Luna SA 5.1.5

CUSTOMER RELEASE NOTES

Document part number: 007-011137-002 Revision G
Release notes issued on: 17 November 2015

The most up-to-date version of the Luna SA 5.1 Customer Release Notes document is at:
http://www.securedbysafenet.com/releasenotes/luna/crn_luna_sa_5-1.pdf

Contents

Product description

SafeNet Luna SA is a network-attached hardware security appliance providing cryptographic acceleration, hardware key management, and multiple configuration profiles.

About these release notes

Luna HSM 5.1.5 Security Patch

This firmware patch for Luna G5 and Luna PCI-E and Luna SA to firmware version 6.2.5 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 SA 5.1.4

Luna HSM 5.1.4 is a Luna SA-only release, 630-010165-017, which includes the previous 5.1.x releases and patches.

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.

See HSMAN-125 in the Luna SA Addressed Issues table.

Luna SA 5.1.3

(Limited distribution)

Luna SA 5.1.2

Fix for Luna SA NTLS crash problem.

Luna SA 5.1.0 and 5.1.1

Applies to Luna SA 5.1 (appliance and client) and the Luna SA 5.1.1 patch (client only). The issues that apply to the 5.1.1 release are listed in separate tables in the "Known issues" and "Addressed Issues" sections below.

Reason for this revision

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 7 for more information.

Applying the 5.1.1 Luna SA client patch

The 5.1.1 client update fixes some HA-related issues that exist in the 5.1 client software. If you are using your Luna SA appliances in HA mode, it is highly recommended that you install this update.

The update, including update instructions, is available for download. The release 5.1 client must be installed before you can apply the update.

New features and enhancements

Luna SA Version	Reason for Update
5.1.4	• Fix for BASH vulenarabilities (Shellshock)
5.1.3	• (Limited distribution)
5.1.2	• Fix for appliance NTLS crash
5.1.1	• HA-related bug fixes (client-only patch)
5.1	• Numerous bug fixes • Introduction of the entry-level Luna SA-1700 • SIM key migration from Luna SA 4 via the Luna Dock2 card reader
5.0	• New internal HSM (the SafeNet Luna K6 card) • Completely new appliance, with redundant, "hot-swappable" power supplies, removable/replaceable chassis fans, Emergency Decommission button, Gigabit Ethernet, three USB ports • Secure Transport Mode – prevents interference while appliance is in transit • PKI and Key migration • All sensitive cryptographic operations (such as NTLS) can take place inside the HSM (user configurable) • Remote system logging – Luna SA can be configured to transfer all logs to another server for collection, parsing, and automatic notifications

Component versions

Component	Version
HSM:	K6
Appliance	5.1.4
HSM Firmware:	6.2.5*
Luna Remote Backup HSM	6.0.8
Luna G5 (for PKI bundle)	6.0.8
PED Workstation software (requires Remote PED) [optional]	1.0.5
Luna PED2 (local only)	2.4.0
Luna PED2 Remote (requires PED workstation s/w on PC) [optional]	2.4.0
IKey	1000
Client	5.1 or 5.1.1

(* Formerly 6.2.1; see section “Luna HSM 5.1 Security Patch”, above.)

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)

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
- FIPS 140-2 Level 3
  - certificate # 1957 update of existing cert now lists f/w 6.2.5)

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/

Notes about release 5.1.x

Java 7 support

The Luna SA Java API now supports Java 5, 6, and 7.

No Luna SX

Luna SX is not tested with Luna SA 5.1.

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.

Remote PED and Backup Not Virtual

For the time being, the Luna SA Remote PED and Backup functions are not supported in virtualized environments (such as VMWare, XEN, Hyper-V, etc.). Remote PED, for example, is a USB device that must be controlled by a single instance of pedServer.exe. Efforts are ongoing with virtualization vendors to achieve standardized ways for connected USB devices that are not in the class HID (human interface device) to be allotted/shared/managed from a physical machine that hosts multiple virtual environments.

Backup and Restore – difference in tracking object sizes

The data structures used to represent objects in different firmware versions have different sizes. The following example shows the discrepancy between firmware 6.0.8 (on the Luna Backup HSM) and firmware 6.2.1 (on the K6 HSM inside Luna SA).

1 Generate 120 RSA 2048 bit keys (60 pairs) on a Luna SA (firmware 6.2.1) partition. The storage reading of the partition is:

Total=102701, Used=101520, Free=1181

1 Backup the keys to a Luna Backup HSM (G5, firmware 6.0.8). The storage reading of the Luna Backup HSM partition is:

Total=101520, Used=98940, Free=2580

2 Restore the keys back to the SA. The storage reading of the partition is:

Total=102701, Used=101520, Free=1181

In the rare situation where the partition on the Luna Backup HSM appears nearly full, if you attempt to restore onto a Luna SA HSM of the same nominal size, the Luna SA could say that it lacks sufficient space to perform the restore operation. The same absolute size of data appears to take more space because the firmware 6.2.1 Luna SA tracks object sizes using more parameters than did the firmware 6.0.8 Luna Backup HSM.

There is no other negative impact on the backup/restore operations.

Legacy HSM firmware

Luna SA 5 includes firmware 4.8.6 image for token HSMs. If you intend to migrate the contents of your G4 token HSMs to Luna SA 5.1 partitions, first perform the firmware update of each token. If you intend to continue using your G4 token HSMs (Luna CA4), then do not update their firmware, and instead leave them at firmware version 4.6.8.

Migration is a one-way operation. You cannot “restore” objects from a Luna SA 5.x partition to a legacy token.

See also “M of N” below if you are migrating.

Upgrade Paths

This section shows the upgrade paths permitted for each revision, starting with the most recent.

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.

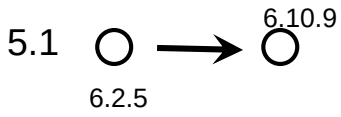
Upgrade Paths for Secure Firmware

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
5.1 / 6.2.1	6.2.1	6.2.5	Validated

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



Upgrade Paths for 5.1.4

Upgrade to version 5.1.4 from Luna SA 5.1.x. No upgrade path is provided from previous-generation Luna SA products.

Component	From version...	To version...
Appliance software	5.1.0, 5.1.2, or 5.1.3	5.1.4

Upgrade Paths for 5.1.0 or 5.1.1

Upgrade to this version from either Luna SA 5.0 or Luna SA 5.0.1. No upgrade path is provided from previous-generation Luna SA products.

Component	From version...	To version...
Client software	5.0 or 5.0.1	5.1
Appliance software	5.0 or 5.0.1	5.1
HSM firmware	6.0.8 or 6.1.6	6.2.1

Notes for upgraders

All of the concepts described in this section are explained in much greater detail in the Luna SA Help (on the Documentation CD that came with your Luna SA 5.1 appliance.

Domains

In earlier Luna SA versions, the cloning domain was a single HSM-wide secret, regulating cloning between HSMs with identical domains (same red PED Key). In Luna SA 5.x, it is possible to apply domains independently to HSM Partitions. A Luna SA with 20 partitions could therefore have twenty different domains.

MofN

In earlier Luna SA versions (4.x, as well as other legacy HSM products) MofN split-knowledge, multi-person access control was an additional secret, optionally applied at initialization time, and requiring a set of green PED Keys. The MofN secret (if invoked) applied to the entire HSM, and could be cached and cloned independently of the blue key (SO) and black key (Partition User/Owner) secrets. MofN was a command-line option for the HSM initialization command.

With Luna SA 5, MofN splitting is applied (optionally) to the individual authentication secrets (any of the blue, black, red, orange, or purple keys) and is an individual choice during PED interaction – no command-line involvement. Thus you can choose to split (MofN) any of the individual secrets associated with your HSM, and not others, at your discretion, on the same HSM. Because MofN is now a PED-only interaction, Luna SA 5.x no longer has the legacy concepts of separate MofN activation or of MofN cloning.

PKI

You can use a Luna CA4 token (in a Luna DOCK 2 card reader, connected to the USB port of the appliance) with Luna SA 5.1. From your client's perspective, it appears as another slot.

Performance

Luna SA 5.1 requires that at least 50 software threads be run against the HSM for maximum performance. This differs from the previous generation Luna SA, which required only ten threads to fully exercise the HSM.

Summary of release support

Any Windows or Linux version listed as supporting Luna SA 5 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 client software in a virtualized environment.

Luna SA 5.1 or 5.1.1 client software

Operating System	O/S kernel architecture	32-bit library	64-bit library
Windows Server 2003 SP2	32 bit	Yes	No
	64 bit	Yes	Yes
Windows Server 2008 R2	32 bit	No	No
	64 bit	No	Yes
Solaris 9 SPARC	32 bit	Yes	No
	64 bit	Yes	Yes
Solaris 10 SPARC	32 bit	No	No
	64 bit	Yes	Yes
Solaris 10 x86	32 bit	Yes	No
	64 bit	Yes	Yes
AIX 5.3	32 bit	Yes	No
	64 bit	Yes	Yes
AIX 6.1	32 bit	No	No

	64 bit	No	Yes
HP-UX 11i PA-RISC	32 bit	No	No
	64 bit	Yes	Yes
HP-UX 11i V2 Itanium	32 bit	No	No
	64 bit	Yes	Yes
HP-UX 11i V3 Itanium	32 bit	No	No
	64 bit	Yes	Yes
Redhat Enterprise Linux 5	32 bit	Yes	No
	64 bit	Yes	Yes
Redhat Enterprise Linux 6	32 bit	Yes	No
	64 bit	Yes	Yes
SUSE Linux Enterprise Server 10 Power PC	32 bit	No	No
	64 bit	Yes	Yes
SUSE Linux Enterprise Server 11	32 bit	No	No
	64 bit	Yes	Yes

Remote PED Server OS Support

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

OS	Driver	App
Windows 2003 Standard / Enterprise	32/64 bit	32/64 bit
Windows 2008 R2	64 bit	64 bit
Windows XP	32/64 bit	32/64 bit
Windows 7	32/64 bit	32/64 bit

Firmware versions

Supported firmware versions

HSM/Token	Luna SA Version	
	5.0/5.0.1	5.1
Luna SA KeyCard firmware	6.0.8/6.1.6	6.2.1
Luna SA (G3 and G4) Backup Token firmware	6.0.8	6.0.8

Addressed issues

Issue severity

The following table defines the severity of the known and addressed issues listed in the tables above.

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

Disclaimer

Although we have attempted to make this document as complete, accurate, and useful as possible, we cannot guarantee it contents. Errors or omissions will be corrected, as they are identified, in succeeding releases of the product.

The following tables list the issue addressed in the 5.1.x releases. Separate tables are provided for release 5.1, 5.1.1, and release 5.1.4. See "Issue severity" above for a description of the severity code assigned to an issue.

Issues addressed in the Luna SA 5.1.4 client patch

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 5.1.4 fixes the vulnerability as a field update, and in all 5.x versions shipped from the factory.

Issues addressed in the Luna SA 5.1.1 client patch

Issue	Severity	Synopsis
(153050) Error when using ssh on a 64-bit HPUX IA V2 client	M	**Problem:** The following error is displayed when attempting to use ssh on a 64-bit HPUX IA V2 client: /usr/lib/hpux64/dld.so: Unsatisfied code symbol 'seteuid' in load module './ssh'. **Fixed:** This issue has been fixed in the 5.1.1 Luna client.
(151610) Error when performing load balancing operations when HA Sync is disabled.	H	**Problem:** The following error is displayed when attempting to perform load balancing operations with HA Sync disabled: Error 0x82 (CKR_OBJECT_HANDLE_INVALID) **Fixed:** This issue has been fixed in the 5.1.1 Luna client
(150967) Unable to create an HA group on 32-bit HPUX PA-RISC client running on a 64-bit OS	H	**Problem:** Unable to create an HA group on a 32-bit HPUX PA-RISC client running on a 64-bit OS. **Fixed:** This issue has been fixed in the 5.1.1 Luna client.

Issues addressed in Luna SA 5.1

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.
(143883) Custom upgrades only available as post-delivery add-ons	M	**Problem:** In previous releases, any upgrades to the standard Luna SA configuration (RAM, etc) had to be ordered separately and installed after the appliance was delivered. **Fixed:** As of release 5.1 customers can specify custom upgrades as part of the ordering process. The custom upgrades are factory installed and configured prior to the appliance being shipped. For more information, please contact sales or customer support.

Issue	Severity	Synopsis
(142495) CA4 PKI bundle predeployed with MofN on SA4 can't be used on SA5 as PKI bundle	H	**Problem:** CA4 PKI bundle predeployed with MofN enabled on Luna SA 4 cannot be used on Luna SA 5. **Fixed:** This problem has been fixed in this release.
(139623) PE1746Enabled flag no longer required in Chrystoki.conf	L	**Problem:** Since PE1746 is enabled by default, the PE1746Enabled flag is no longer required in the Chrystoki.conf file. **Fixed:** The flag has been removed from the Chrystoki.conf file.
(139190) CSP/KSP key counter support	L	**Problem:** The Luna CSP/KSP does not support key counting. **Fixed:** CSP/KSP key counting support has been added in this release.
(139187) CSP/KSP OAEP padding support	L	**Problem:** The Luna CSP/KSP does not support OAEP padding. **Fixed:** OAEP padding support has been added in this release.
(138607) cmu enhancements	L	**Problem:** The cmu utility needs to be enhanced to ensure compatibility with third-party software. **Fixed:** cmu has been enhanced to fix compatibility issues. See the help for details.
(138523) NTLS "Keys in Hardware" fails if activation policy for the "Cryptoki User" partition is "On"	M	**Problem:** If the activation policy for the "Cryptoki User" partition is "On", then the "Keys in Hardware" feature will fail. **Fixed:** This problem has been fixed in this release.
(138504) Sample Chrystoki.conf file for enabling cklog on HPUX is incorrect	M	**Problem:** The sample Chrystoki.conf file describing how to enable cklog on HPUX is incorrect and does not work. **Fixed:** This problem has been fixed in this release.
(138245) No way to determine current setting for NTLS keys in HW	M	**Problem:** None of the available NTLS commands provide information for the current NTLS keys in HW setting. **Fixed:** The **ntls show** command now provides this information.
(137125) Cannot Import/export configuration information to/from Luna Remote Backup Token	H	**Problem:** Cannot Import/export configuration information to/from a Luna Remote Backup Token **Fixed:** Import/export of configuration information to/from a Luna Remote Backup Token is now supported.
(135531) Slot order incorrect (vtl listslot or ckdemo)	H	**Problem:** The slot list displayed using vtl slotlist or ckdemo places the LunaNet slots after the Luna UHD slots. LunaNet slots should appear first. **Fixed:** The LunaNet slots are now enumerated before the Luna UHD slots.
(131906) SSH keys not unique on different Luna SAs	M	**Problem:** The SSH keys are set to a factory default, resulting in the keys being the same on all new Luna SA 5 platforms. **Fixed:** The SSH keys are no longer set at the factory, but are now set during customer personalization of the Luna SA.
(130451) KCDSA capability is included by default, although it is now an orderable option	M	**Problem:** KCDSA capability is included by default, although it should be included only if ordered as an upgrade option. **Fixed:** KCDSA capability is now included only if ordered.

Issue	Severity	Synopsis
(129035) Setting or changing the time requires SO login	M	**Problem:** You must login as the security officer to set or change the time. **Fixed:** SO login is no longer required to set or change the time.
(126679) The **server.pem** file is accessible only by the admin user that created it	M	**Problem:** Running the **sysconf regencert** command creates a **server.pem** file in the home directory of the (admin role) user that created it. This file is not accessible to other admin role users, preventing them from creating clients. **Fixed:** All admin role users can now access the **server.pem** file.
(126478) ARIA key generation mechanisms have incorrect implementation	H	**Problem:** The ARIA key generation mechanisms were implemented incorrectly in firmware 6.0.8 and earlier. The following mechanisms were not implemented correctly: #define CKM_ARIA_ECB 0x00000561 #define CKM_ARIA_CBC 0x00000562 #define CKM_ARIA_MAC 0x00000563 #define CKM_ARIA_MAC_GENERAL 0x00000564 #define CKM_ARIA_CBC_PAD 0x00000565 #define CKM_ARIA_ECB_ENCRYPT_DATA 0x00000566 #define CKM_ARIA_CBC_ENCRYPT_DATA 0x00000567 **Fixed:** Fixed in firmware 6.2.1. Any ARIA keys that have been generated or derived on any firmware version are still valid and can continue to be used with any firmware. Any data, however, that was signed/encrypted/wrapped using the older firmware must be resigned, re-encrypted, re-wrapped with the new firmware. To support migration, the following mechanisms are included in firmware 6.2.1. They use the incorrect implementation and can be used to migrate from the old (incorrect) implementation to the new (correct) implementation. #define CKM_ARIA_L_ECB (CKM_VENDOR_DEFINED + 0x130) #define CKM_ARIA_L_CBC (CKM_VENDOR_DEFINED + 0x131) #define CKM_ARIA_L_CBC_PAD (CKM_VENDOR_DEFINED + 0x132) #define CKM_ARIA_L_MAC (CKM_VENDOR_DEFINED + 0x133) #define CKM_ARIA_L_MAC_GENERAL (CKM_VENDOR_DEFINED + 0x134) **Note:** These mechanisms can only be used for migration: • The ECB, CBC, CBC_PAD mechanisms can only be used for decryption. • The MAC and MAC_GENERAL can only be used to verify signatures.
(124524) Cannot integrate Luna libraries with Adobe SDK	M	**Problem:** The format of the EKU list returned by the Luna provider does not match what is expected by the Adobe SDK, preventing integration. **Fixed:** The EKU list is now generated in the correct format.
(123422) Syslog messages may not be received under DISK FULL: ALERT! conditions	L	**Problem:** In certain instances, messages are not received under a DISK FULL: ALERT! condition. **Fixed:** This problem has been fixed in this release.
(123171) Configured log levels unclear	L	**Problem:** The output of the **syslog show** command displays some configured log levels as "*". The meaning of "*" is unclear. **Fixed:** The following note has been added to the output of the **syslog show** command: **Note: '*' means all log levels.**
(122822) Weak defaults for NTP autokey	L	**Problem:** The default key size and algorithm used by NTP Autokey are weak (RSA-MD5, RSA, 512). **Fixed:** The defaults have been strengthened to use RSA-SHA1, RSA, 2048. Affected commands are **sysconf ntp autokey generate** and **sysconf ntp autokey update**.

Issue	Severity	Synopsis
(122820) Key generation in HA environment is slow	M	**Problem:** The methods used to generate keys in an HA environment are slow and need optimization. **Fixed:** The methods have been optimized, resulting in performance improvements.
(121583) Utilities included with the Luna SA client use dynamic linking.	L	**Problem:** The utilities included with the Luna SA client use dynamic linking, which may result in customers using untested configurations. **Fixed:** The utilities now use static linking, ensuring that all configurations are tested.
(119970) Not all jar files are signed	L	**Problem:** Not all of the jar files shipped with the Luna SA client are signed to verify their authenticity. **Fixed:** All of the jar files are now signed.
(119379) Slow Java provider certificate validation	M	**Problem:** Certificate validation using the Java provider is slow. **Fixed:** Performance has been improved.
(119378) jMultitoken key algorithm needs enhancement	M	**Problem:** jMultitoken does not include DH, ECDH, and ECDHC key derive operations. **Fixed:** jMultitoken now supports DH, ECDH, and ECDHC key derive operations.
(119072) Manually Zeroized flag not set to "No" after decommission	M	**Problem:** After decommissioning and initializing the Luna SA Manually Zeroized flag is set to Yes. This is incorrect. **Fixed:** The flag is now reset to No.
(118826) Luna shell (lush) output needs improvement	L	**Problem:** The output from the Luna shell is difficult to understand. **Fixed:** The Luna shell includes numerous changes to make commands clearer and output more meaningful.
(113923) Output of **hsm factoryReset** command says RPV erased, when it is not	M	**Problem:** The output of the **hsm factoryReset** command states that the operation erased the remote PED vector (RPV). The **hsm factoryReset** command does not erase the RPV. **Fixed:** The output for the **hsm factoryReset** command now accurately reports status of remote PED vector.
(113797) Performance-based licensing introduced in Luna SA 5.1	C	**Problem:** Luna SA 5.1 introduces a new lower-performance variant (Luna SA-1700). High performance versions of Luna SA require the **621-000021-001 Performance Level 15** license. **Fixed:** The high performance license is installed automatically when existing Luna SA 5.0 customers upgrade to Luna SA 5.1. To verify that the new license is installed, enter the **hsm displayLicenses** command. The **621000021-001 Performance level 15** license should be listed.
(113766) cryptoki.h and examples refer to CK_USHORT	L	**Problem:** cryptoki.h and examples refer to CK_USHORT, which has been removed from PKCS#11 v2 **Fixed:** In the "cryptoki_v2.h" file, "CK_USHORT" is flagged as "deprecated" and so applications that use this type will be warned at compile time. This change will not affect the compiled applications that continue to use CK_USHORT. They will behave as in previous releases. The change will only be evident during compilation. If an application continues to use "CK_USHORT", a warning will be displayed at compile time.
(110919) PKCS#11 version number is incorrectly encoded	L	**Problem:** The PKCS#11 version number is incorrectly encoded. This breaks any code which checks the version number to determine which API features and behaviors are supported. **Fixed:** The PKCS#11 version number is now encoded correctly.

Issue	Severity	Synopsis
(110913) Library reports errors to stderr	L	**Problem:** Without configuring the system (i.e. accepting the default configuration and not putting in place a NTL configuration) calls to C_Initialize return CKR_UNABLE_TO_CONNECT and also report “Unable to load certificate” to stderr. A library should never report errors to stderr. **Fixed:** This problem has been fixed in this release.
(110755) The LunaProvider.jar file is not sealed.	L	**Problem:** The LunaProvider.jar file is not sealed allowing access to package-private methods by declaring a new class inside an existing jar. **Fixed:** The LunaProvider.jar file is now sealed.
(110737) KSP provider does not support IsEphemeral	M	**Problem:** The KSP provider does not support the IsEphemeral operation needed by .NET applications. **Fixed:** KSP now supports IsEphemeral.
(110459) jMultitoken does not support signature verification	M	**Problem:** jMultitoken does not support signature verification. **Fixed:** Two checkboxes have been added under Test Type: "sign" and "verify". These checkboxes are only enabled when Signature is selected. At least one of these must be selected before the Signature test is started. When both "sign" and "verify" are selected, the whole sign+verify sequence is counted as one operation for the purposes of the performance display.
(109460) Help text for sysconf command does not differentiate between regenCert and hwRegenCert	L	**Problem:** Help text for sysconf command does not differentiate between regenCert and hwRegenCert **Fixed:** Help now reads as follows: Name (short) Description --- regenCert r Generate Server Certificate In Software hwRegenCert h Generate Server Certificate In Hardware
(107982) Poor SHA384withECDSA signing performance when using the Java provider	H	**Problem:** The ECDSA signing performance is poor when using the SHA384withECDSA algorithm through the Java provider. **Fixed:** The non-sensitive ECDSA parameters are now cached, resulting in performance that lies within the expected target range.
(104849) HA auto - reconnect interval is not configurable	M	**Problem:** The HA auto-reconnect interval is hardcoded at 60 seconds. **Fixed:** You can now use the **vtl haadmin** command to set the HA reconnect interval to a value between 60 and 1200 seconds.
(104848) HA standby members should not be used until all non-standby members have failed.	L	**Problem** Standby members in an HA group should not be used until all non-standby members have failed. **Fixed:** Standby members in an HA group are not used until all non-standby members have failed. When a non-standby member returns, the standby is dropped. All writes go to every member, but reads only go to non-standbys.
(101700) Using the Close Access API to close a session opened with another client may cause "Session Handle Invalid" message	M	**Problem:** If you open a session on slot *n* using client 1, use client 2 to close the client 1 session using the close access API, and then use client 3 to open another session on slot *n* with a new APP ID, login will fail with a "Session Handle Invalid" message. **Fixed:** The close access API now removes all session handles.
(101613) Cannot Import/export appliance configuration data to/from Luna Remote Backup HSM.	H	**Problem:** Cannot import/export appliance configuration data to/from Luna Remote Backup HSM **Fixed:** Import/export of appliance configuration data to/from Luna Remote Backup HSM is now supported.

Issue	Severity	Synopsis
(101301) HA sync of 3rd member clones the keys properly but client vtl gives error of sync not completed	L	**Problem:** In a 3-member HA group, when attempting to synchronize device C where devices A and B are already in sync, device A syncs to device C, then device B tries to sync with objects that now already exist from the synchronization with device A. The vtl error message LUNA_RET_OH_OBJECT_ALREADY_EXISTS", 68610 decimal is displayed. **Fixed**: This problem has been fixed in this release.
(101285) Setting SNMP trap causes firewall block of SNMP port 161	L	**Problem:** Setting the SNMP trap causes the firewall to block of SNMP port 161. **Fixed:** This problem has been fixed in this release.
(101190) uninstall.sh script doesn't uninstall JSP and SDK if uninstall script issued not from /usr/lunasa/bin on linux client	M	**Problem:** The uninstall.sh script on the linux client did not uninstall JSP and SDK if issuing uninstall script from any location other than /usr/lunasa/bin. **Fixed.** This problem has been fixed in this release.
(101124) HA retry polling applies only to HSM that were running at application startup.	L	**Problem:** HA retry polling is done only for the Luna SA HSMs in the HAgroup that are up and running at application start. **Fixed:** The HA retry count has been changed from 500 (20 second intervals) to infinite so that if a Luna HSM in the HA group restarts after application startup, it will be included in the retry polling.
(99914) Client installers do not install all available Java samples	M	**Problem:** All of the available Java samples are not installed by some client installers. **Fixed:** All of the client installers now install all of the available Java samples.
(99902) LunaProvider: PriorityWrap sample app causes JVM segfault	L	**Problem**: The PrivateWrap Java sample app crashes the JVM when it's run against an HSM without the key wrapping capability. It should fail, but in a more controlled way. **Fixed:** This problem has been fixed in this release.
(99822) Unexpected ShortBufferException in JMultitoken for RSA OAEP 8k key cipher	M	**Problem**: Get an Unexpected ShortBuffer exception trying to run RSA OAEP encryption with 1 thread for an 8K key size... data size = 16 bytes. This is a Java message, not from the crypto library or the device. The C multitoken tool performs the same operation successfully. **Fixed**: This problem has been fixed in this release.
(99260) Java key generators should provide valid default key parameters	L	**Problem:** Many of our Java key generators do not supply a default set of initialization parameters. When someone tries to use an uninitialized generator, they will get an exception of some kind. The Java crypto spec has this to say: "In case the client does not explicitly initialize the KeyGenerator (via a call to an init method), each provider must supply (and document) a default initialization." The classes that are affected are: • all subclasses of LuneKeyGeneratorSecret • LunaKeyPairGeneratorDh • LunaKeyPairGeneratorEc **Fixed:** This problem has been fixed in this release.
(98835) Enhanced logging of more events: impending NTLS certificate expiry	M	**Problem:** Syslog does not include messages regarding the operational status and state of the NTLS certificate. **Fixed:** Syslog messages are now generated for the NTLS certificate monitor.

Issue	Severity	Synopsis
(98828) Strengthened SNMP traps by removing V2 parameters	L	**Problem:** SNMP trap parameters for the **sysconf snmp trap set** command include v2 options. Traps should always be sent in V3 format. **Fixed:** This problem has been fixed in this release.
(98785) Corrected DSA tools to allow migration from SA 4.x to SA 5.x	M	**Problem:** Luna SA 4 DSA tools fail on Luna SA 5. **Fixed:** This problem has been fixed in this release.
(96130) Added ability to backup PKI bundle partitions via the remote backup feature	M	**Problem:** Cannot use remote backup to backup to a G5 PKI token partition. **Fixed:** This problem has been fixed in this release.
(96051) Return of configuration settings to factory state made more extensive.	M	**Problem:** Several configuration attributes do not get reset to their default values when the **sysconf config factoryReset** command is executed. **Fixed:** A complete factory reset requires using the **sysconf config factoryReset** and hsm **factoryReset** commands. See the Luna SA 5.1 Help for details.
(95822) NTLS keys-in-hardware feature more resilient after appliance restart.	M	**Problem:** NTLS restart following an appliance reboot generates an RC_SOCKET_ADDRESS_IN_USE error. **Fixed:** This problem has been fixed in this release.
(95540) Extraneous message file log entries	L	**Problem:** The messages file contains extraneous (for example, login time out) messages. **Fixed:** This problem has been fixed in this release.
(94993) Client installer prompts for reboot when additional components are not yet installed	M	**Problem:** When installing the client, if you choose to install more than one component, the installer prompts you to reboot after the client is installed. If you do reboot, the other items you selected are not installed. **Fixed:** This problem has been fixed in this release.
(94426) Cannot specify label during vtl backup token init	L	**Problem:** There is no option in the **vtl backup token init** command to specify a label. **Fixed:** This problem has been fixed in this release.
(93576) Restoring large objects from the Luna Remote Backup HSM fails.	L	**Problem**: Restoring large objects from a Luna G5 remote backup HSM fails with a LUNA_RET_DEVICE_ERROR. **Fixed:** This problem has been fixed in this release.
(91914) Remote PED requires both interfaces to have static IP addresses	M	**Problem**: Remote PED requires both interfaces to have static IP addresses **Fixed:** This problem has been fixed in this release. Remote PED no longer requires both interfaces to have static IP addresses.
(90668) **vtl haadmin** subcommands are case sensitive	L	**Problem**: All subcommands under **vtl haadmin** are case sensitive, affecting usability. **Fixed:** This problem has been fixed in this release. The subcommands are no longer case sensitive.

Issue	Severity	Synopsis
(88308) Java provider KeyFactory classes are limited	L	**Problem**: Wider support required for Java provider KeyFactory classes. **Fixed:** The Java provider now supports KeyFactory classes for the following key types: • DH (KeyFactory) • DSA (KeyFactory) • RSA (KeyFactory) Generic/AES/ARIA (SecretKeyFactory) • DES (SecretKeyFactory) • DES3 (SecretKeyFactory)
(88307) Partition backup procedure requires improvement	L	**Problem:** The partition backup procedure is cumbersome and requires improvement. **Fixed:** The procedure has been streamlined. Refer to the Luna SA 5.1 Help for details.
(73481) Java samples do not include an ECDSA example	L	**Problem:** Java code samples do not include an ECDSA example. **Fixed:** The Java samples now include an ECDSA signature example.
(24195) Java applications cannot reinitialize the cryptoki library	M	**Problem:** Cannot use a Java application to reinitialize the cryptoki library. **Fixed:** The closeAllSessions method now invalidate the master session on a slot as well. A new method, LunaSlotManager.reinitialize() has been added that does all the Finalize/Init/close-sessions steps. This method also invalidates any LunaTokenObject objects that refer to session objects on the HSM which were removed during the C_Finalize.

Known issues

The following tables list the known issues at time of release. Separate tables are provided for release 5.1 and release 5.1.1. Workarounds are provided where available. See "Issue severity" on page 7 for a description of the severity code assigned to an issue.

Known issues in the Luna SA 5.1.1 client patch

Issue	Severity	Synopsis
(153576) 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.
(153569) 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.
(153052) 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 **Workaround:** Ignore the word "not" in the log message.

Issue	Severity	Synopsis
(153049) 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. This issue will be addressed in a future release.
(152642) Deleting the HA group does not delete HA entries in the client configuration file	M	**Problem:** Deleting the HA group does not delete HA entries in the client configuration file. **Workaround:** None. This issue will be addressed in a future release.
(151071) Certificate autoenrollment fails when using KSP with OCSP.	M	**Problem:**. Certificate autoenrollment fails when using KSP with OCSP. **Workaround:**.None. This issue will be addressed in a future release.

Known issues in Luna SA 5.1

Issue	Severity	Synopsis
(152754) The **user delete** and **user role delete** commands do not request confirmation before deleting a user/role	M	**Problem:** The **user delete** and **user role delete** commands perform the requested operation without first requesting confirmation. This may result in accidental deletion of a user or role. **Workaround:** Use caution when using these commands to ensure that you do not accidentally delete a user or role. This problem will be fixed in a future release.
(152659) The **sysconf ntp deleteserver** command allows deletion of the NTP psuedo IP (127.127.1.0)	M	**Problem:** If NTP loses synchronization with the remote server, it will synchronize against itself using psuedo IP address 127.127.1.0 until it can start synchronizing with the remote server again. Although you should be prevented from deleting this psuedo 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 psuedo IP address (127.127.1.0).
(152510) The **my file delete** and **my public-key delete** commands do not request confirmation before deleting a file/key	M	**Problem:** The **my file delete** and **my public-key delete** commands perform the requested operation without first requesting confirmation. This may result in accidental deletion of a file or key. **Workaround:** Use caution when using these commands to ensure that you do not accidentally delete a file or key. This problem will be fixed in a future release.
(150544) 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. This issue will be resolved in a future release.
(150533) The csp does not allow the firmware to enforce key wrapping	L	**Problem:** The csp enforces private key wrapping as not allowable. This prevents using the csp to allow private key wrapping **Workaround:** None. The csp will be changed in a future release to allow the firmware to enforce key wrapping.
(148292) 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.

Issue	Severity	Synopsis
(146783) 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. This issue will be resolved in a future release.
(144528) ECIES does not work	H	**Problem:** ECIES does not work in this release. **Workaround:** None. This issue will be resolved in a future release.
(144389) 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.
(144229) Time set using **sysconf time** does not persist after a power off	L	**Problem:** If the time is set using the sysconf time command, and the Luna SA is subsequently powered off, the time set does not persisit when the Luna SA is powered back on. **Workaround:** None. This issue will be resolved in a future release.
(142122) 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.
(141370) lunash PED key prompts are unclear for partition backup	L	**Problem:** With Luna SA 5.x, When backing up a Luna SA partition you need blue/red/black keys for the HSM partition, and blue/red/black keys for the backup HSM. The prompts within lunash are unclear as to which keys are required at which time. **Workaround:** None. This issue will be resolved in a future release.
(140653) 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.
(138779) Cannot create a certificate after installing client on Windows 2003 (32-bit) or Windows 2008 (64-bit)	M	**Problem:** Attempting to create a certificate after installing the client on Windows 2003 (32-bit) or Windows 2008 (64-bit) produces the following error: • Error: Unable to open the SafeNet-INC configuration file for read. Please check your file permissions. The user running vtl must have at least read permissions for the crystoki.ini file. (Usually the Administrator, or someone with Administrator privileges runs vtl.) **Workaround:** Logout, log back in, and retry.
(138363) 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. This issue will be resolved in a future release.
(137534) Poor signing performance using sha256RSA	M	**Problem:** The signing performance for sha256RSA is slower than the RSA signing performance, by an order of magnitude. **Workaround:** None. This issue will be resolved in a future release.

Issue	Severity	Synopsis
(137144) LunaProvider: LunaKeyStore doesn't support some JCA features	L	**Problem:** The following methods are not supported by LunaKeyStore: • entryInstanceOf() • getEntry() • load(KeyStore.LoadStoreParameter) • setEntry() • store(KeyStore.LoadStoreParameter) **Workaround:** None. This issue will be addressed in a future release.
(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. **Workaround:** If searching for terms that include an underscore, omit the portion of the string that includes the underscore.
(128393) X9.31 with SHA2 signatures and FIPS 186-3 RSA key generation are not supported	H	**Problem:** X9.31 with SHA2 signatures and FIPS 186-3 RSA key generation are not supported in this release. **Workaround:** None. This issue will be addressed in a future release.
(118902) PED client and server startup information is inconsistent	L	**Problem:** The startup information for the PED connection that is logged for the PED client and PED server is not consistent. The client log also contains extraneous information. **Workaround:** None. This issue will be addressed in a future release.
(99065) Token PKI command result displays incorrect slot number	M	**Problem:** The slot number displayed in PKI command result is always displayed as the actual slot number decreased by 1. See example below. [myluna] lunash:>token pki changepin -s 777002 Please type "proceed" to continue, anything else to abort: proceed ********** * * * About to change the partition password * * Please pay attention to the PED * * * ********** Please enter the current user challenge: Please enter the new user challenge: Please re-enter the new user challenge: Success changing the user password for the slot 0 ! SHOULD BE slot 1 ! Command Result : 0 (Success) **Workaround**: None. This is working as designed. The logical slot numbers start at zero (0), similar to operating system dialogs that refer to ports (such as Ethernet ports) starting at logical slot zero, which is equivalent to physical slot/device 1. Simply be aware that this is how it works.
(97966) RSA with MGF1 is missing from jMultitioken	M	**Problem:** RSA with MGF1 algorithms were missing from jMultitoken cross all supported clients. **Workaround:** RSA with MGF1 is not supported in the jMultitoken tool for this release. The general Luna Java api still supports RSA with MGF1 for key sizes larger than 1024-bit.

Issue	Severity	Synopsis
(93128) Need large number of threads to push up performance for multitoken	M	**Problem:** In Luna SA 5.0, in order to reach maximum performance during performance measurement, we need a large number of threads on multitoken (normally 50 or more threads). In previous releases only 10 threads were sufficient to get the system working near maximum performance. **Workaround:** To ensure maximum performance, ensure that your clients invoke at least 50 threads on the HSM.

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
Email	support@safenet-inc.com	
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.

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