SafeNet HSM 6.2

CUSTOMER RELEASE NOTES

Issue Date: 04 January 2016

Document Part Number: 007-012225-006 Rev. A

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

http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_6-2.pdf

Contents

Product Description

The SafeNet HSM (hardware security module) family provides FIPS-certified, PKCS#11-compliant cryptographic services in a high-performance, ultra-secure, and tamper-proof hardware package. By securing your cryptographic keys in hardware, SafeNet HSMs provide robust protection for your secure transactions, identities, and applications. They also offer high-performance encryption, decryption, authentication, and digital signing services. SafeNet HSMs are available in the following form factors which offer multiple levels of performance and functionality:

SafeNet Network HSM

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

SafeNet PCI-E HSM

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

SafeNet USB HSM

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

Release Description

SafeNet HSM 6.2 is a field upgrade which introduces some features to improve the scalability and enhance the ability to work in multi-tenant environments.

Product Rebranding

In early 2015, Gemalto NV completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna PED	SafeNet PED
Luna Client	SafeNet HSM Client

Old product name	New product name
Luna Backup HSM	SafeNet Backup HSM
Luna CSP	SafeNet CSP
Luna JSP	SafeNet JSP
Luna KSP	SafeNet KSP

Note: The Luna name is retained for some SafeNet HSM software tools, such as LunaCM, LunaSH, LunaProvider, and Lunadiag. The device names displayed by these tools will also use the old names.

New Features and Enhancements

The following are summaries of features new to SafeNet HSM in release 6.2.

Derive Templates

Derive templates are an optional extension to the PKCS#11 C_DeriveKey function which provide additional security by restricting important attributes in the resulting derived key. Derive templates are offered in our PKCS#11 and JCPROV software development kits, and our CKDemo and multitoken utilities.

[Requires firmware version 6.24.0]

Unwrap Templates

We now support unwrap templates as outlined in the PKCS#11 v. 2.20 standard. Unwrap templates are offered in our PKCS#11 and JCPROV software development kits, and our CKDemo and multitoken utilities.

[Requires firmware version 6.24.0]

Partition Policy Templates

Application partition policy templates can be created, edited, stored by name, and assigned to new application partitions for rapid, consistent deployment.

[Requires firmware version 6.24.0]

Parallelized PED Operations

SafeNet HSMs can now run PED operations simultaneously with other operations. PED operations acting on a partition no longer block other operations occurring on other partitions. For example, parallelized PED operations allow you to create new partitions or backups while running cryptographic operations on a separate partition. In this way, you can perform maintenance and configuration on your HSM without interrupting client applications. PED operations might still block cryptographic operations occurring on the same partition, especially high volumes of write object requests.

[Requires firmware version 6.24.0]

Expanded CKM_RSA_PKCS_OAEP Support in JSP

The JSP API now supports multiple hashing options for RSA OAEP. The supported algorithms are SHA1, SHA224, SHA256, SHA384 and SHA512.

[Requires firmware version 6.24.0]

Fix for HA Recovery Login

The CA_HAGetLoginChallenge() function in the cryptoki library now functions properly.

[Does not require firmware version 6.24.0]

Advisory Notes

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

Do Not Use "sysconf config factoryReset" LunaSH Command

The "sysconf config factoryReset" command restores system settings but does not include files and folders, only pointers. Because the factory version is 5.x, a factory reset from 6.x causes major conflicts with directory structures which cannot be resolved. The system can enter an indeterminate state and require return to Gemalto. Instead of using factory reset, create an equivalent configuration fallback using "sysconf config backup" at the lower version, and use "sysconf config restore -file <baseline name>" to restore the backup. Consult the *Configuration Guide*'s Optional Configuration Tasks chapter for more information.

CKDemo Requires Additional Configuration with Firmware Older than 6.22.0

If you use CKDemo in a new client with firmware older than 6.22.0, you might encounter the error CKR_TEMPLATE_INCONSISTENT. Try CKDemo option 98, sub-option 16. If it is set to "enhanced roles", try selecting it to set it to "legacy Luna roles". The setting is a toggle, and flips every time you see it.

New Objects Visible in PPSO User Partition

Some new objects are visible in PPSO user partitions, including Clock and Monotonic Counter. These are standard PKCS#11 objects. Refer to PKCS#11 documentation for more information on these objects.

Minimum Recommended Firmware for SafeNet Remote Backup HSM

With firmware older than version 6.10.9, 'ped connect' fails to work properly. The LunaCM command returns "No Error, but the PED ID remains set to 1 and PedServer "Client Information" shows "Not Available". We recommend that you update the SafeNet Backup HSM firmware to version 6.10.9.

RSA Key Sizes and FIPS

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

Modification to DES3 Algorithm for NIST Compliance

Per the NIST document SP 800-131A Revision 1, when the HSM is in FIPS mode, two-key DES3 is now restricted to legacy operations (decryption, unwrapping, and CMAC verification). All other operations for DES3 must use the three-key variant.

SIM Migration Patch

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

Small Form Factor (SFF) Backup Support

We only support SFF backup on PED-authenticated HSMs, not password-authenticated HSMs.

Be Cautious With Using HTL with HA Configurations

In several situations, the HTL service hangs while deployed with HA. Issue LHSM-25697 in the Known Issues list details some known failures, but is not exhaustive. When the HTL service hangs, a full appliance reboot is required to return to production. Therefore, we do not recommend deploying the HTL service in an HA configuration.

HSM Admin Partition Erroneously Displayed

On SafeNet HSM client with Windows 32 libraries, if you establish an NTLS connection to a SafeNet Network HSM, a slot is displayed with the Configuration "Luna HSM Admin Partition" and the Slot Description "Net Admin Token Slot". Ignore this slot. You cannot access or edit the partition. If you run the vtl verify command, you see two partitions with the same label; log in to LunaCM to determine which slot is invalid.

Compatibility and Upgrade Information

This section provides upgrade paths and compatibility information for SafeNet HSM 6.2.0 software and firmware versions.

Upgrade Paths

Component	Directly from version	To version
SafeNet HSM client software	Any	6.2
SafeNet Network HSM appliance software	5.4.7, 6.0.0, 6.1.0 [see Note 1]	6.2
HSM firmware	6.2.x, 6.10.x, 6.20.x, 6.21.x, 6.22.x, 6.23.0 [see Note 2]	6.24.0
SafeNet Backup HSM firmware	6.0.8	6.10.9 [See Note 3]
SafeNet Local PED/Remote PED firmware	2.4.0-3, 2.5.0-3 [see Note 4]	2.6.0
[NOTE 1: If your SafeNet Network HSM appliance software is not listed, contact SafeNet Technical Support to		

Component	Directly from version	To version
upgrade.]		
[NOTE 2: If your HSM firmware is older than version 6.2.1, you must update to firmware version 6.2.1 before updating to firmware 6.24.0. Refer to the earlier upgrade documentation provided by SafeNet Technical Support.]		
[NOTE 3: We recommend that you upgrade the SafeNet Remote Backup HSM to 6.10.9, which is a FIPS-validated version. Follow the same upgrade procedure as for a SafeNet USB HSM. It is not necessary to upgrade SafeNet Remote Backup HSMs beyond 6.10.9, as they work to backup and restore newer-firmware HSMs.]		
[NOTE 4: Version 2.4.0-3 is the PED version required for basic PED and Remote PED function with SafeNet HSM 5.x or 6.x. For newer options like SFF backup, newer versions of PED firmware are needed. Refer to the table in the *HSM Administration Guide*, on the page "Using the PED", under heading "Versions".]		

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, use firmware version 6.10.9, which is the validated version 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 SafeNet 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

About Common Criteria

Some organizations specify Common Criteria evaluation for equipment and systems that they deploy. We submit fewer products/versions for CC evaluation than we do for FIPS validation, due to relative demand, cost, and the much longer time-frames involved. Completed CC evaluations: http://www.commoncriteriaportal.org/products/ Firmware version 6.10.9 is currently under evaluation.

Supported Operating Systems

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

SafeNet HSM Client

Note: The SafeNet HSM client works in virtual environments. SafeNet USB HSM and PCI-E are not supported in virtual environments.

Operating system	Version	64-bit client installer on 64-bit OS	32-bit applications on 64-bit OS	32-bit client installer on 64-bit OS	32-bit client installer on 32-bit OS
Windows **Note:** The 64-bit Windows installer also installs the 32-bit libraries for compatibility with 32-bit client applications. No standalone 32-bit SafeNet HSM client is available.	2008 R2	Yes	Yes	No	No
	2012 and 2012 R2	Yes	Yes	No	No
	10	Yes	Yes	No	No
Redhat-based Linux (including variants like CentOS and Oracle Enterprise Linux)	5	Yes	Yes	Yes	Yes
	6	Yes	Yes	Yes	Yes
	7	Yes	Yes	Yes	Yes
OpenSuse Linux	11.4	Yes	Yes	Yes	Yes
	12	Yes	Yes	Yes	Yes
	13	Yes	Yes	Yes	Yes
Debian	6	Yes	No	No	Yes
	7	Yes	No	No	Yes
	8	Yes	No	No	Yes
FreeBSD	8.3, 8.4	Yes	Yes	Yes	Yes
	9	Yes	Yes	Yes	Yes
Solaris (SPARC/x86)	10	Yes	Yes	Yes	No
	11	Yes	Yes	Yes	No
HP-UX	11.31	Yes	Yes	Yes	No
AIX **Note:** Only SafeNet Network HSM is supported; SafeNet USB HSM and SafeNet PCI-E HSM are not supported with AIX for this release.	6.1	Yes	Yes	Yes	No
	7.1	Yes	Yes	Yes	No

Remote PED Server

The remote PED server must be installed on any workstation used to host a remote PED. The remote PED server software is supported on the following Windows operating systems only:

- Windows 2012 and 2012 R2
- Windows 2008 R2
- Windows 10
- Windows 7 (64-bit)

Supported APIs

The following APIs are supported :

- PKCS#11 2.20
- Java 7
- Java 8
- OpenSSL
- Microsoft CAPI
- Microsoft CNG

Advanced Configuration Upgrades

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

- SafeNet Network HSM partition upgrades (5 , 10, 15, 20, 50, or 100 compatible with SafeNet Backup HSM, 35 or 75 not compatible with Safenet Backup HSM)
- Partition SO (PSO)
- Maximum memory
- ECIES acceleration
- Korean algorithms

Server Compatibility

The SafeNet PCI-E HSM card and SafeNet USB HSM are tested for compatibility with some commonly used servers. Specifically, we have noticed compatibility problems with the following:

Server	Slot(s)	Failure
Dell R720	1	HSM card not detected in slot 1 (but works in slots 2 and 3)

SafeNet PCI-E HSM Server Compatibility

The SafeNet PCI-E HSM card is designed to the PCIe 1.1 standard, for use in servers with PCIe x4 slots. For further information and compatibility options, refer to the SafeNet HSM 6.2 Overview that is included with your HSM documentation.

RADIUS Compatibility

For this release, we only support the use of one RADIUS server.

Known Issues

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

Issue Severity Definitions

The following table defines the severity of the issues listed in this section.

Priority	Classification	Definition
C	Critical	No reasonable workaround exists.
H	High	Reasonable workaround exists.
M	Medium	Medium level priority problems.
L	Low	Lowest level priority problems.

Known Issues

Issue	Severity	Synopsis
LUC-691: Remote PED fails to connect to G5 (Solaris Sparc)	H	**Problem:** Attempting to establish a host trust link (HTL) connection fails on UNIX and Linux platforms. **Workaround:** After generating the one-time token (OTT), wait for about 30 seconds before transferring it to the client. Note that you must transfer the token before it expires. Use the htl show command to view the OTT expiry time.
LHSM-30622 Duplicate partitions seen in Windows 32 bit with different serial numbers in 6.2	H	**Problem:** On SafeNet HSM client with Windows 32 libraries, if you establish an NTLS connection to a SafeNet Network HSM, a slot is displayed with the Configuration "Luna HSM Admin Partition" and the Slot Description "Net Admin Token Slot". If you run the vtl verify command, you see two partitions with the same label; **Workaround:** Log in to LunaCM to determine which slot is invalid. Ignore this slot. You cannot access or edit the partition.
LHSM-25697 HTL can crash or hang when HA failover should occur	H	**Problem:** HTL service can sometimes hang in HA configurations: - if the primary HA member (first on the list in the config file) fails while HTL is configured, the HTL service can hang, with the primary or secondary member stuck in the grace period - if the primary HSM appliance's time is adjusted into what should be its grace period, the HTL service on both primary and secondary will hang - service shows running, but status remains in grace period - if the network is unplugged for 15-to-30 seconds (less than the grace period), HTL service hangs, and logs can fill with beacon messages. **Workaround:** In all cases appliance reboot allows service to resume. Avoid using HTL with HA configurations.
LHSM-25096 NTLS connection	H	**Problem:** You cannot establish an NTLS connection between LunaClient 5.x and SafeNet Network HSM 6.x. **Workaround:** None. At the time of this writing, we do not support connecting

Issue	Severity	Synopsis
between SafeNet HSM Client 5.4.0 and SafeNet Network HSM 6.2.0 (6.24.0 fw) cannot be established.		SafeNet Network HSMs to a SafeNet HSM client at a lower version.
LHSM-16838 SafeNet Network HSM 6.0: STC K6 crashed after 7 days with LUNA_RET_DEVICE_ERROR	H	**Problem:** Uptime of just 7 days and K6 crashed. Nothing heavy running. Just STC enabled. **Workaround:** None. If you are testing STC, SafeNet Technical Support would appreciate a capture of the logs and of dual-port dump, if this occurs.
LHSM-16776 PKI bundles: partition restore failed with CA4 for migration test	H	**Problem:** For SafeNet Network HSM, in order to migrate a pre-existing Luna CA4 (on Luna DOCK) PKI bundle to SafeNet USB HSM, the first step is normally to restore the desired object(s) from the Luna CA4 HSM to a partition on the SafeNet Network HSM, and then clone to the SafeNet USB HSM. However, on Luna HSM 6.0 the initial "restore" step fails with "RC_DATA_INVALID" (even though "set legacydomain" succeeded). **Workaround:** If possible, migrate before you upgrade to Luna HSM 6.0.
LHSM-15016 SafeNet Network HSM 6.0: STC hsm soft init fails with "Error: 'hsm init' failed. (80000000 : LUNA_RET_ERROR)"	H	**Problem:** When issuing an 'HSM initialize' or 'HSM zeroize' command through lunash or lunacm, the command succeeds, but returns: 'LUNA_RET_ERROR' for lunash or 'CKR_GENERAL_ERROR' for lunacm. LunaCM then needs a restart. This is a result of the active STC link through which the command is issued being dropped unilaterally by the HSM as a result of the zeroize / factory reset actions. **Workaround:** Restart lunacm.
LHSM-15004 SafeNet Network HSM 6.0: STC hsm soft init fails with "Error: 'hsm init' failed. (80000000 : LUNA_RET_ERROR)"	H	**Problem:** When running initialization/zeroize for HSM with STC: - For soft Zeorize – i.e. 'HSM init' of already initialized HSM (original defect report) will work properly and return OK. - For hard zeorize – 'HSM zeroize' command will succeed but report "CKR_GENERAL_ERROR" - For factory reset – 'HSM factoryreset' command will succeed but report "CKR_GENERAL_ERROR" – HSM will not crash **Workaround:** Be aware that init/zeroize of the HSM generates error messages if STC was active, even though the init/zeroize finished smoothly, without error. The errors are from STC, which loses contact when the HSM zeroizes.
LHSM-14992 After successfully enabling SRK	H	**Problem:** On an HSM with firmware 6.22.0, if you enable SRK and successfully imprint a purple PED Key, lunacm still shows SRK as disabled. This is a display error that has not caught up with the actual state of the HSM, but can be worrisome

Issue	Severity	Synopsis
lunacm reports transport mode disabled		and might not be acceptable to an auditor. **Workaround:** Restart lunacm to update the cache of hsm capabilities and policies. The correct state of SRK is then visible.
LHSM-14210 Performance loss of RSA, ECDSA, Digest, AES/DES3 and DSA	H	**Problem:** Comparing to SafeNet Network HSM 5.4, we have performance slow-down on test cases with RSA, ECDSA, Digest, AES/DES3 (PE1746 is disabled) and DSA. The range is about 5-10%. Detailes are attached as spreadsheets. AES/DES3 with PE1746 Enabled have over 20% slowing down. **Workaround:** None. If performance is critical, do not update at this time.
(LHSM-13408) Diminished performance after upgrading to 6.22.0 firmware.	H	**Problem**: After upgrading the firmware on a SafeNet USB HSM to 6.22.0, HSM performance is reduced. **Workaround**: Run the **ureset** utility (located in the SafeNet HSM client root directory) to reset the USB driver after performing the firmware upgrade.
LHSM-11637 SafeNet USB HSM performance slowing down around 50% with ECC and ECDH, etc.	H	**Problem:** Comparing to release 5.4, SafeNet USB HSM release 6.0 performance numbers are reduced with: RSA Encrypt/Decrypt ECDSA ECDH ECIES HMAC ARIA KCDSA **Workaround:** None. If performance is critical, do not update at this time.
(LHSM-8424 MKS190409) The PED client service does not start on Solaris 11 Sparc T-5120 server.	H	**Problem:** The PED client service from 32-bit binaries does not start on Solaris 11 Sparc T-5120 server. **Workaround:** None
(LHSM-8406 MKS190450) Client tools fail to detect SafeNet USB HSM on 'unplug and re-plug' operations.	H	**Problem:** When SafeNet USB HSM 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
(LHSM-5804 MKS180345 and 170626) change of	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

Issue	Severity	Synopsis
PED related timeout setting requires pedclient restarting, which has impact on audit logging		logging, restarting has an impact on audit logging. Pedclient should pick up the change without restarting. **Workaround:** None. For SafeNet PCI-E HSM, audit logging is affected when the restart is performed. In SafeNet Network HSM, there is no provision to restart pedclient, and therefore no way to make a timeout change effective.
(LHSM-5797 MKS182827) SafeNet USB HSM HA autorecovery does not work	H	**Problem:** If you enable HA autorecovery on SafeNet USB HSM, members of the HA group that go down might not be autorecovered when they come back online. **Workaround:** Do not use the autorecover feature. If one of your HA members goes down, restart your applications to manually restore the member.
LUC-705: Unable to establish an HTL connection (UNIX/Linux)	M	**Problem:** Attempting to establish a host trust link (HTL) connection fails on UNIX and Linux platforms. **Workaround:** After generating the one-time token (OTT), wait for about 30 seconds before transferring it to the client. Note that you must transfer the token before it expires. Use the htl show command to view the OTT expiry time.
LHSM-30091 SW shows an odd character on the Appliance's LCD when displaying system status code.	M	**Problem:** The SafeNet Network HSM does not display the system status code properly on the LCD screen. **Workaround:** To view the system status code in LunaSH, run "status sysstat show".
LHSM-29888 STC firmware upgrade fails	M	**Problem:** If you attempt to upgrade to firmware 6.24.0 and HSM policy 39 (Allow Secure Trusted Channel) is enabled, the upgrade fails. **Workaround:** Disable HSM policy 39 and re-attempt firmware upgrade.
LHSM-27567 HA slot performance is slower than a single slot over symmetric key at big data size	M	**Problem:** When encrypting a large data size with a symmetric key, encryption is 25% slower on an HA slot as compared to a single slot. **Workaround:** If you notice a large performance slowdown on an HA slot for requests of this type, perform these requests on a single slot.
LHSM-25763 STC admin channel with NULL_ENC fails to verify spkg	M	**Problem:** If the STC admin channel is enabled with all the ciphers disabled, secure package capability updates do not install. **Workaround:** Enable at least one cipher.
LHSM-25676 Cannot run java on HPUX	M	**Problem:** You cannot run the SafeNet HSM 6.2 Java SDK with the HP-UX operating system by default. **Workaround:** SafeNet HSM Client 5.4 and below can run Java with HP-UX. You can apply SafeNet HSM Client 5.4 files to make Java work with HP-UX through the following steps: 1. With SafeNet HSM Client 5.4 installed, back up the following folders: /opt/safenet/lunaclient/jsp /opt/safenet/lunaclient/jcprov

Issue	Severity	Synopsis

		2. Uninstall SafeNet HSM Client 5.4.
		3. Install SafeNet HSM Client 6.2.
		4. Keep the 5.4 Luna Provider and Library in the <java home>/jre/lib/ext directory
		5. Change the following settings in the /etc/Chrystoki.ini file by adding the bolded sections.
		`Misc = {`
		`PE1746Enabled = 0;`
		`ToolsDir = /opt/safenet/lunaclient/bin;`
		`PartitionPolicyTemplatePath = /opt/safenet/lunaclient/data/partition_policy_templates;`
		`FunctionBindLevel = 2;`
		`}`
		`Presentation = {`
		`OneBaseSlotId = 1;`
		`}`

LHSM-25244: "error is c0000001, RC_MEMORY_ALLOCATION" using NTLS with STC HSM policy 39 ON	M	**Problem:** If you use NTLS with HSM policy 39 (Allow Secure Trusted Channel) set to ON, an error "c0000001, RC_MEMORY_ALLOCATION" sometimes appears. **Workaround:** Exit and log back in to LunaCM. The error no longer displays.
LHSM-25155 PPT partition policy 37 stc is allowed to be ON on create with hsm policy 39 still OFF	M	**Problem:** You can appear to set partition policy 37 (Force Secure Trusted Channel) to ON in a partition policy template. This option should not be displayed; if you set a partition policy template to ON, and then use the template to create a new partition, the new partition has partition policy 37 set to OFF. You cannot set partition policy 37 to ON through a partition policy template, because this action would bypass proper STC registration and risk lock out from the new partition. **Workaround:** You must enable partition policy 37 manually for a newly created partition following proper STC registration steps, outlined in the Secure Trusted Channel chapter of the *HSM Administration Guide*. Note that PPSO-style partitions only allow the partition SO to edit policies, not the HSM SO.
LHSM-25147 Adding snmp user with special characters in name succeeds, but user is invalid	M	**Problem:** If you use LunaSH to create an SNMP user with a hyphen (-) or underscore (_) in the user name, the user is invalid. **Workaround:** Avoid hyphens and underscores for SNMP user names. As a best practice, use only letters and numbers.
LHSM-25081 Changing RPED timeout value from default 1800 seconds seems to be ignored.	M	**Problem:** Changing the remote PED timeout value from the default of 1800 seconds has no effect. **Workaround:** If the remote PED times out before you expected, re-connect the PED server.
LHSM-25049 HA	M	**Problem:** When you set an HA member to standby, it still displays as "alive".

Issue	Severity	Synopsis
Standby Member Shows Wrong Status		**Workaround:** If you want to determine if an HA member is in standby mode, run the LunaSH command "hsm information show" on that member. The "Crypto Operations Requests" value does not increase as you send cryptographic requests to the HA group.
LHSM-20625 DOC: sysconf config factoryReset will fail to see HSM if STC is ON.	M	**Problem:** If you perform a factory reset with the STC policy on, the HSM is unreachable from LunaSH. **Workaround:** Make sure STC policy is turned off before performing a factory reset. If you have a backup of the sysconf config before performing a factory reset with STC on, you can restore the backup.
LHSM-20536 DOC: Utilities Reference Guide > CKdemo > Using the ckdemo Menu list is still from 5.x	M	**Problem:** The CKDemo command list in the SafeNet HSM documentation is out of date. **Workaround:** If you need help with CKDemo, contact customer support.
LHSM-20393 cmu selfsigncertificate command fails for SECP256K1 key pair	M	**Problem:** You cannot run "cmu selfsigncertificate" on an ECDSA key pair with the curve secp256k. **Workaround:** None.
LHSM-19307 SafeNet HSM Client DA login utility with STC: Able to open and close multiple sessions with the same ID.	M	**Problem:** In the SafeNet HSM Client 'salogin' utility with STC, you are able to open multiple sessions with the same ID without any warning message; 'salogin' is unable to close the sessions. This is because these sessions do not share login access as each run of the utility is assigned a unique STC link. **Workaround:**None. The 'salogin' utility is not currently compatible with STC.
LHSM-19128 LunaSH command 'hsm information reset' sometimes fails	M	**Problem:** If, in LunaSH, you run "service stop sysstat" and then quickly run "hsm information reset" the HSM Event Counters might not all be reset to zero. **Workaround:** After running the two commands, run "hsm information show" to check the HSM Event Counters. If any of the counters are above zero, run "service status sysstat" to ensure that sysstat is stopped, then re-run "hsm information reset".
LHSM-19089 ppso audit role unlock displays wrong message	M	**Problem:** If after three failed attempts to login the PPSO Auditor role in LunaCM, you wait 60 seconds and login with the correct credentials, LunaCM displays an inaccurate warning that the Auditor is locked. In fact, the command succeeds and the Auditor is not locked. **Workaround:** This is a display issue, and can be ignored. If you want to confirm the state of the Auditor, run "role show -name Auditor".
LHSM-18991 lunacm 'help audit export' does not	M	**Problem:** The "help audit export" command in LunaCM does not work and instead runs "audit export." **Workaround:** Refer to SafeNet HSM documentation for information on the "audit

Issue	Severity	Synopsis
work on SafeNet USB HSM/SafeNet PCI-E HSM		export" command.
LHSM-18380 lunacm HA API extension commands do not work in FIPS mode, 6.22.x firmware	M	**Problem:** The lunacm HA API extension commands do not work with 6.22.0 or above firmware in FIPS mode. **Workaround:** Use ckdemo to manually generate an RSA 186-3 or aux prime 2048 bit keypair on one slot, clone the keypair to the other slot, and then use ckdemo to initialize HA on either slot.
LHSM-18348 HTL generation of ott does not put the token into the non-admin lush_files directory	M	**Problem:** If you login as a non-default admin user such as manager, and generate an OTT file for HTL, the OTT is placed in /home/admin/lush_files instead of the directory for the current admin user. **Workaround:** None. Only the admin user can store the token when OTT is generated.
LHSM-18312 SafeNet Network HSM 6.0: STC with HA haonly and 1746 enabled in the client fails with (CKR_DATA_ LEN_RANGE) on C_EncryptInit	M	**Problem:** If HA-only is set, STC fails if you attempt to enable PE1746 usage. **Workaround:** When using STC, either avoid using HA-only, or avoid specifying PE1746.
LHSM-18310 'ped connect' doesn't work with G5Base FW 6.0.8 and 6.2.3	M	**Problem:** With SafeNet USB HSM having firmware 6.0.8 or 6.2.3, 'ped connect' command in lunacm returns No Error but the PED ID is set to 1. On the PedServer side, however, the "Client Information:" shows "Not Available". **Workaround:** Update firmware to 6.10.x or newer.
LHSM-18302 STC Status command is displaying incorrect current key life value when executed in SO owned partition.	M	**Problem:** The STC key life, as shown by the STC status command is too small by several orders of magnitude. **Workaround:** None.
LHSM-18299 Confusing "hsm stc status" information for admin channel.	M	**Problem:** [sa97] lunash:>hsm changePo -po 39 -v 1 'hsm changePolicy' successful. Policy Allow Secure Trusted Channel is now set to value: 1 Command Result : 0 (Success) [sa97] lunash:>hsm stc status HSM STC: Enabled Enabled: No

Issue	Severity	Synopsis
		Workaround: Be aware that the first instance does not really deal with enabling, but rather with whether the policy is set or not, so "HSM STC: Enabled" should say "HSM STC: Allowed". The second "Enabled: No" is the STC admin channel turned on or off by command. We will try to make it less confusing in future.
LHSM-18295 RemotePED: G5 with legacy fw and SA can not share the same remote PED	M	**Problem:** A SafeNet Network HSM with firmware 6.22.0 and above cannot share a remote PED with a G5 with legacy 6.21.0 firmware. **Workaround:** Upgrade the firmware on both devices to 6.22.2 or above.
LHSM-18283 pedclient relies on deprecated net-tools package	M	**Problem:** When installing the 6.0.0 SafeNet HSM Client on a CentOS 7.1 system with a minimal install, the pedclient fails to start; the ifconfig and various other system commands have been deprecated and are not installed by default. **Workaround:** yum -y install net-tools
LHSM-18281 'token backup init' command failed due to LUNA_ RET_INVALID_ ENTRY_TYPE	M	**Problem:** The first 'token backup init' command after 'token backup factoryReset' always fails with LUNA_RET_INVALID_ENTRY_TYPE. However, the second 'token backup init' command succeeds. **Workaround:** Repeat the command.
LHSM-18231 Updating "Ignore Idle Connection Timeout" by 'pedClient mode config set' command changes "Idle Connection Timeout"	M	**Problem:** Attempting to to enable "Ignore Connection Time out" but the setting of "Idle Connection Timeout (seconds)" is updated instead. **Workaround:** Edit the config file manually (contact Technical Support).
LHSM-18230 CKR_FUNCTION_ FAILED for 'par crp -l user_PCI' command after PED has been switched from remote to local	M	**Problem:** 1. Initialize HSM. 2. Generate RPV. 3. Connect the Remote PED. Verify the connection via PedServer. 4. Initialize HSM and create a user partition. 5. Disconnect the Remote PED. Verify the [dis]connection via PedServer. 6. Initialize HSM and create a user partition. lunacm:>par crp -l user_PCI Please attend to the PED. Error in execution: CKR_FUNCTION_FAILED. Command Result : 0x6 (CKR_FUNCTION_FAILED) **Workaround:** Exit lunacm and relaunch lunacm.

Issue	Severity	Synopsis
LHSM-18096 Remote PED does not work with SafeNet Backup HSM attached to a SafeNet Network HSM	M	**Problem:** The PED for the SafeNet Backup HSM can be successfully disconnected, but when connecting to the Remote PED, gets 0X300207 (Unknown ResultCode value) error. **Workaround:** Update the SafeNet Backup HSM firmware to version 6.10.9.
LHSM-18031 Cannot change legacy CU challenge when partition activation policy set	M	**Problem:**For PED-auth SafeNet Network HSM, cannot change legacy CU challenge when partition activation policy is set. **Workaround:** Switch the activation policy off before changing the Crypto User challenge secret: lunash:>partition changepolicy -policy 22 -value 0 -partition mypar1 'partition changePolicy' successful. Policy "Allow activation" is now set to: 0 Command Result : 0 (Success) lunash:>partition changepw -partition mypar1 -cu -oldpw /W5W4dLbAWKLGCxW -newpw cuserpin SafeNet PED operation required to activate partition on HSM - use User or Partition Owner (black) PED key. 'partition changePw' successful. lunash:>partition changepolicy -policy 22 -value 1 -partition mypar1
LHSM-17804 SafeNet Network HSM 6.0: HA manual sync fails with 'ha sync -g <group>' if -password parameter is not used	M	**Problem:** HA manual sync fails if password parameter is not provided. **Workaround:** Provide the password at the command line.
LHSM-17755 and LHSM-14857 Lunacm "partition clone" logs out current user after successful OR unsuccessful operation.	M	**Problem:** After logging in CO and cloning objects, the CO is logged out of the current working slot for no apparent reason. **Workaround:** Log in again.
LHSM-17181 LunaCM: par ar r didn't handle properly with -replace option	M	**Problem:** 1. have couple of objects pre-created in the user partition 2. restore from backup with -replace option turned on 3. expecting the existing objects will be deleted, then replaced with the backup objects. 4. it turns out, the restore process just skips the existing objects without replacing them.

Issue	Severity	Synopsis
		Workaround: If in doubt, delete objects on the target partition before restoring from archive.
LHSM-16825 Lunacm: partition archive backup -slot remote does not work	M	**Problem:** "partition archive backup -slot remote" command returns "(invalid arguments)" error, regardless of options that are provided. **Workaround:** None.
LHSM-16315 HA: ha sync up with PKI bundle not performed with two members one having 0 objects.	M	**Problem:** 1. Pre-deploy, then deploy SafeNet USB HSMs, have two SafeNet USB HSMs from each SafeNet Network HSM 2. Assign each G5 bundle to the same client 3. From client, create HA group using both partitions from PKI bundles. 4. Create some objects in one HA member and leave the other one with 0 objects in it. 5. Order synchronization of the objects within the HA group, get "No synchronization performed/needed". 6. Remove the 0 object member from HA group and add it back in, then attempt sync again. Same result, "no sync performed". **Workaround:** None. HA is not working for PKI bundle.
LHSM-16311 When enable bonding false negative error message	M	**Problem:** When port bonding is enabled, the dialog returns an error like: Error adding address 172.20.10.179 for bond0. **Workaround:** Ignore. Bonding is successful, despite the spurious error.
LHSM-16238 PKI bundle: token pki resetPin failed with creating challenge	M	**Problem:** For SafeNet USB HSMs connected to SafeNet Network HSM: FW 6.22.0 - has the challenge created in the PED screen, but after pressing Enter on the PED, got message "Failed to create new challenge!" in the lunash. FW 6.2.4 - failed the resetPin right away without displaying the new challenge in the PED. **Workaround:** If necessary to change the challenge secret on a PKI bundle SafeNet USB HSM, temporarily attach the SafeNet USB HSM to a SafeNet HSM Client host computer, perform the operation in lunacm, and then return the SafeNet USB HSM to the SafeNet Network HSM.
LHSM-16237 partition backup append replace does not work	M	**Problem:** Backing up a partition to SafeNet USB HSM and then attempting to back it up again to the same partition with the append and replace options, no items are backed up, they are just skipped. **Workaround:** Avoid using the "append" and "replace" options in the same command.
LHSM-15991 PKI bundle: Failed to deploy token pki on FW 6.10.1	M	**Problem:** 1. Predeployed the SafeNet USB HSM with FW 6.10.1 2. Performed the changepin operation 3. Deploy fails with "Can not locate the token". **Workaround:** None.

Issue	Severity	Synopsis
LHSM-15975 PKI bundle: token active failed in lunash after deactive from SafeNet HSM client	M	**Problem:** On SafeNet Network HSM 6.0, with attached SafeNet USB HSM having f/w 6.22.0: 1. Assigned the PKI token (the SafeNet USB HSM) to client 2. Deactivated the token 3. When activated from lunash, failed with error code 65535. **Workaround:** None. But the activation from lunash was observed to work for firmware 6.2.4
LHSM-15964 SafeNet Network HSM 6.0: sysconf config factoryReset complains of 'hsm [4411]: Unable to locate client token library configured in 'ClientTokenLib' if STC enabled	M	**Problem:** With STC enabled, perform a "sysconf config factoryReset -s all -f" lunash does not see the hsm. **Workaround:** Restore previous configuration with lunash:>sysconf config restore -s all -fi <config filename>.tar.gz.
LHSM-15960 "sysc ssh device eth1" hung on bonded NIC (PED-auth SafeNet Network HSM)	M	**Problem:** On a PED-authenticated SafeNet Network HSM with bonded Ethernet ports, run "sysconf ssh device eth1". The command hangs, with no return. **Workaround:** Close the SSH terminal session and start again.
LHSM-15417 PKI bundle: token pki update capability broken	M	**Problem:** The command 'token pki update capability' is broken, returning RC_FILE_ERROR. **Workaround:** Disconnect the SafeNet USB HSM from the SafeNet Network HSM appliance, and connect to a SafeNet HSM Client computer. Use lunacm to apply the capability update. Return the updated SafeNet USB HSM to its place connected to the SafeNet Network HSM appliance for PKI Bundle operation.
LHSM-15017 'sysconf regenCert' returns 'ERROR. Partition named "Cryptoki User" not found'	M	**Problem:** When running an ordinary 'sysconf RegenCert' the dialog talks about being unable to find Cryptoki User partition, which would be expected if running a 'sysconf hwregencert'. **Workaround:** Ignore.
LHSM-14848 hsm init from lunacm on a PED-auth HSM should warn when password and domain are provided	M	**Problem:** For a PED-authenticated SafeNet HSM with older firmware, if you offer a password or domain when initializing, you are told that they are being ignored. On a PED-authenticated HSM with firmware 6.22.0, if both pw and domain are provided, the initialization just works, but without notifying about ignored parameters. However, if an unnecessary password is provided, but the unnecessary domain is not provided, the command simply fails. It should not. **Workaround:** When initializing a PED-authenticated SafeNet HSM with lunacm:> hsm init, DO NOT provide password, domain, or default domain. Simply run the command "hsm init -label <some label>" and respond to the SafeNet PED prompts.

Issue	Severity	Synopsis
LHSM-14761 CKR_DEVICE_ ERROR during RC4 key gen	M	**Problem:** Key gen (CKM_RC4_KEY_GEN) fails with a CKR_DEVICE_ERROR and renders the HSM unresponsive. The same HSM/test combination ran for weeks without issue. **Workaround:** Restart the HSM. This is a very rare occurrence, and a fix is being tested.
LHSM-14333 SafeNet Network HSM 6.0: HA using java does not recover and does not terminate/clean up session	M	**Problem:**Setup: Two SafeNet Network HSM appliances Java with HA HAOnly 1. Run jMultitoken 2. Shut down the interface of 1 member 3. After four attempts at recovering, restart the interface (notice the error code of 0xC0000102 4. After reaching max retries, perform manual recover The client sets up a session with the appliance but HA is never recovered. **Workaround:** Reboot.
(LHSM-13949) Long pauses (5 minutes) during SFF restore of existing objects	M	**Problem:** When restoring existing objects from an SFF token to an SA partition, existing objects are found and skipped, as expected, every 5-6 seconds or so. However, on occasion, there may be a lengthy pause (5 minutes or so), between objects. **Workaround:** None. If you notice a pause, please be patient.
LHSM-13421 Changing logpath of audit log while services stopped causes SafeNet USB HSM to not respond when services restarted	M	**Problem:**Logged in as the Auditor, set log level to log nothing. Stopped the SafeNet HSM client services - HTL, SNMP, PED Server. Renamed the "logtest" directory to something else. Restarted the 3 services stopped earlier. At this point the SafeNet USB HSM froze with its green light on. I couldn't get it back to life without a ureset. Definitely an unlikely edge case, but interesting. **Workaround:** Perform ureset to get SafeNet USB HSM going again.
LHSM-12575 Running ssh lush commands immediately after port bonding forces bonding in Fault-Tolerance	M	**Problem:**Calling any lunash commands immediately after bonding enable or disable causes bonding to go into Fault-Tolerance mode causing unexpected behavior. **Workaround:** None.
LHSM-11659 First hsm login after tamper is ignored	M	**Problem:**Tamper a SafeNet Network HSM. Reboot. Perform hsm login - I and get "success" from lunash. Note that the hsm still isn't really logged in, and requires a second login before I can do things that require SO authentication. **Workaround:** After a tamper event, perform 'hsm login' twice.
(LHSM-10615) KSP does not	M	**Problem:** KSP is only logging failures. It should also record successes, for auditing purposes.

Issue	Severity	Synopsis
record success messages		**Workaround:** None.
(LHSM-10594) KSP unable to set usage limits	M	**Problem:** kspcmd.exe has an option to specify a usage limit. The command appears to work and generates a registry entry that sets the limit specified for any key created via KSP (i.e. CA, etc.). However, when keys/certs are created via CA, the KSP log records error CKR_ATTRIBUTE_TYPE_INVALID. Reviewing the keys attributes in ckdemo does not show attributes CKA_USAGE_LIMIT or CKA_USAGE_COUNT. Without these set, the keys can be used an infinite number of times. **Workaround:** After creating your CA, or after every renewal, launch ckdemo and manually add the usage limit attribute.
(LHSM-10162) No way to put SafeNet Backup HSM into FIPS approved operation mode on SafeNet Network HSM	M	**Problem:** SafeNet Backup HSM with firmware 6.10.2 is undergoing FIPS evaluation. To conform to FIPS evaluation, it must be used in FIPS approved operation mode. By default this HSM policy is OFF. There is no way to turn it on via lunash. **Workaround:** Connect the Backup HSM to a standalone host computer and use lunacm to change the policy, then reconnect the Backup HSM to the SafeNet Network HSM. Or perform remote backup.
(LHSM-10161) token backup show needs to show whether Backup HSM is in FIPS approved mode or not	M	**Problem:** SafeNet Backup HSM with f/w 6.10.2 is undergoing FIPS evaluation. To conform to FIPS requirements, it must be used in FIPS approved operation mode and there must be a way to visually confirm this configuration. There is no way via Lunash to query whether this HSM policy is on or off for a SafeNet Backup HSM. **Workaround:** Connect the Backup HSM to a standalone host computer and use lunacm to view the status, then (if acceptable) reconnect the Backup HSM to the SafeNet Network HSM. Or perform remote backup.
(LHSM-10160) Attempt to backup to non-existent partition on Backup HSM gives warning but no way to back out	M	**Problem:** Attempting to perform a backup with "replace" option to a partition on the SafeNet Backup HSM that does not exist, Lunash prompts with a warning, but then gives no opportunity to back out of the command: [192.20.9.127] lunash:>partition backup -partition John1 -password userpin -serial 7000627 -replace -tokenpar Warning: 'replace' mode specified, but no partition named FIPSBackup exists on the backup token. A new partition will be created. Warning: You will need to connect SafeNet PED to the SafeNet Backup HSM to complete this operation. You may use the same SafeNet PED that you used for SafeNet Network HSM. Please type 'proceed' and hit <enter> when you are ready to proceed> quit Please type 'proceed' and hit <enter> **Workaround:** Close the session, open a new SSH session to the SafeNet HSM appliance, login to the HSM and try the backup again with a correct, existing partition name.
(LHSM-9888)	M	**Problem:** Steps to reproduce:

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

Issue	Severity	Synopsis
		OR Command Result : 0x80000024 (CKR_TIMEOUT) --> If the PED prompt went to a PED other than yours and nobody inserted the expected black key and pressed <ENTER>. **Workaround:** For Remote PED authentication or remote Small Form-factor Backup of SafeNet Network HSM, first run "hsm ped disconnect" from lunash, then run "ped connect and perform Small Form-factor Backup (or other PED-using operations) from lunacm.
(LHSM- 9712) PED SCP communication problem	M	**Problem:** Occasional errors or timeout occurred during local-PED data transfers (using SCP connection). This was probably always present, but went unnoticed during authentication operations due to the small data transactions. However, when PED is used in local mode for lengthy transactions, such as occur in SFF backup and restore operations, the instability is revealed. **Workaround:** Use Remote PED SFF backup when backing up and restoring larger amounts of partition data. (Remote PED SFF backup operations have proven reliable over a reliable network.)
(LHSM-8423, MKS190597) System is rebooted on issuing **hsm reset** command when running HA on Solaris Sparc 11 Netra T5440.	M	**Problem:** System gets rebooted when **hsm reset** command is issued on a G5 HA, running Solaris Sparc 11 (64-bit) Netra T5440 server. **Workaround:** It is recommended to stop any running applications before issuing **hsm reset** command in lunacm.
(LHSM-7696 MKS190048) RBS host app crashes on access when SafeNet Backup HSM removed	M	**Problem:** If a SafeNet 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 SafeNet Backup HSM.
(LHSM-7052/2863) Auto and manual	M	**Problem:** When a system is configured for auto-recovery, running the manual vtl haAdmin recovery option causes errors randomly.

Issue	Severity	Synopsis
recovery conflict during recovery		**Workaround:** Avoid manual recovery when system is configured for HA auto-recovery.
LHSM-5812 Crypto-User cannot create objects when using an HA group (MKS #176840)	M	**Problem:** Firmware allows only Crypto-Officer to clone objects. Currently, Crypto-User is not allowed to do cloning The HA logic for object creation is to create on the primary and then propagate (using the cloning operation) to other members. **Workaround:** Use Crypto Officer when using HA.
(LHSM-5768) Windows installer - when modifying existing SafeNet HSM Client, extra selected components are not installed	M	**Problem:** When trying to modify an already-installed SafeNet HSM Client on Windows we have the option to select any extra component we want, but the selected additional components are not actually installed. The installer gives no error message. **Workaround:** When modifying an existing installed SafeNet HSM Client, on Windows, choose to install a Luna Product and ALL its sub-features. THEN deselect any that are not needed, and the remaining desired files are installed correctly.
(LHSM-2864) HA Key gens do not recover properly when recovering the primary.	M	**Problem:** In an HA environment, configure for auto-recovery. Launch multitoken with 10 threads performing key gens Fail the secondary and recover - everything works. Fail the primary - it switches over to do the key gens on the secondary. Recover the primary and wait; the app fails with CKR_CANCEL **Workaround:** None. Can be avoided if you do not have multiple clients connected to the HA slot.
LHSM-30099 ntls in show displays "Operational Status down"	L	**Problem:** After you update the firmware, and run the command "ntls information show" sometimes the Operational Status erroneously displays as down. This is only a display error; NTLS is still running. **Workaround:** Restart the appliance. The NTLS Operational Status then displays properly.
LHSM-27566 HA member still displayed after server removed	L	**Problem:** If, on SafeNet HSM client, you remove an HA member from the list of trusted servers, and then start LunaCM, the removed member is still displayed. **Workaround:** This is a display issue only; the HA member is no longer in the group. If you want to correct the display, run the LunaCM command "**haGroup removeMember -serialNumber** <serial number> **-slot** <slot number> **-group** <grouplabel>".
LHSM-25117 partitions order reversed in lush after firmware upgrade to 6.24.0 from 6.22.0	L	**Problem:** After upgrading firmware to 6.24.0, when you run "hsm show", the order in which partitions display is reversed. **Workaround:** This is a cosmetic issue. There is no workaround.
LHSM-19278 lunacm cache	L	**Problem:** If you apply a 100 partition capability update in LunaCM, and immediately try to create an additional partition, the operation fails.

Issue	Severity	Synopsis
needs to be cleared (restart lunacm) after updating partition license or else you can't create additoinal partitions		**Workaround:** After applying the capability update, exit and start LunaCM for the change to take effect. Then you can create additional partitions.
LHSM-18062 lunash "partition sff showcontent" output not giving full command	L	**Problem:** lunash command "partition sff showcontent" output "'partition sff sho' successful.", should readback the full command "partition sff showcontent" rather than the short form. **Workaround:** Cosmetic; ignore.
(LHSM-10633) SafeNet HSM Client on Debian requires libcryptoki library purge to reset to the default Chrystoki.conf version on uninstall	L	**Problem:** In some instances, it might be desirable to perform a complete re-install of the SafeNet HSM client, including replacing the current Chrystoki.conf file with the default version. Doing this on a Debian OS requires, after uninstalling the client, that the libcryptoki library be purged before the Chrystoki.conf.debsave backup file is deleted. **Workaround:** Workaround: To re-install the SafeNet HSM client with the default Chrystoki.conf file on a Debian OS 1. Uninstall the SafeNet HSM 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 SafeNet HSM client: <path>/install.sh
(LHSM-10163) SFF remote backup - Unknown Command Displayed on PED	L	**Problem:** During SFF backup over Remote PED, "Unknown Command" is observed on the PED followed by "Get Version". This should be a message like "write to token..." **Workaround:** Ignore.
(LHSM-10154) "cmu selfsign" fails to display key handler for new generated key	L	**Problem:** Running "cmu selfsign" ends with generating a key. If the command runs successfully, cmu is expected to display the new generated key handler, but it does not. **Workaround:** Issue "cmu list" to verify that the new key has been created.
(LHSM-10153) windows Client - cmu importkey gives wrong error message	L	**Problem:** The cmu utility returns "Buffer too small" instead of "wrong password" against "cmu importkey" cmd. **Workaround:** Be aware that the message is wrong, and re-try with the correct password.

Issue	Severity	Synopsis
(LHSM-9889) User loses pub key authentication after sysconf backup/restore	L	**Problem:** After: 1) Run sysconf config backup 2) Run sysconf config factoryReset any existing named user is no longer able to log in with public key authentication. **Workaround:** Recreate the named user (see issue LHSM-9888). Upload a public key and re-establish public key authentication for each such user.
(LHSM-9816) All other crypto ops to same HSM halt during init phase of SFF backup, recover slightly during object backup phase	L	**Problem:** When performing any kind of multitoken cryptographic operation, and a Small Form Factor Backup operation is started on the same HSM, all other cryptographic operation ceases during the eToken initialization phase of the operation. This can take 2-3 minutes. After the eToken initialization stage, crypto operations recover somewhat, but not to full speed, until backup completes. **Workaround:** Simply be aware that SafeNet PED operations and prompting have always blocked crypto operations on the attached HSM, and this continues with PED-mediated Small Form Factor Backup.
(LHSM-9681) Incorrect error when attempting to backup symmetric keys with symmetric SFF turned off.	L	**Problem:** Attempted to back up 2 symmetric keys with SFF symmetric policy turned off for the partition. The objects did not backup, but an overall message said success backing up 2 objects. lunacm:> par archive backup -slot eToken -label G5Backup WARNING: continuing the backup operation will wipe out all keys on the backup token! Are you sure you wish to continue? Type 'proceed' to continue, or 'quit' to quit now -> proceed Operation in progress, please wait. (1/2): Backing up object with handle 22... Failure (2/2): Backing up object with handle 25... Failure WARNING: Errors occurred while backup up one or more keys. Backup Complete. 2 objects have been backed up to partition G5Backup on the backup device Command Result : 0x63 (CKR_KEY_TYPE_INCONSISTENT) lunacm:> If some objects do not backup due to policy settings, a better message should be presented, such as "Some or all objects failed to backup due to policy restrictions on the current partition" or similar. This should replace the current bad grammar warning: "WARNING: Errors occurred while backup up one or more keys." **Workaround:** Ignore messages like “2 objects have been backed up to partition” when other messages indicate individual failures.
(LHSM-6986) Warning from install script on Debian 6/64 client install	L	**Problem:** During the full client install in Debian 6 this warning/error appeared: Unpacking lunajmt (from lunajmt_5.3.0-9_amd64.deb) ... Setting up lunajmt (5.3.0-9) ... Adding new version of lunajcprov

Issue	Severity	Synopsis
		/usr/safenet/lunaclient/debian_pkgs Use of uninitialized value $postinst in length at /usr/share/perl5/Alien/Package/Deb.pm line 741. **Workaround:** The error appears to be a harmless coding issue in /usr/share/perl5/Alien/Package/Deb.pm which comes with the alien package. Ignore the message.
(LHSM-6945 MKS160706) Handling of PEDId parameter is inconsistent or confusing	L	**Problem:** Currently, whether an application uses the remote or the local PED is determined by the existence of the PEDId=[0|1] parameter in the 'Luna' section of Crystoki.conf. If this parameter does not exist, applications will always try to use the local PED, even if one is not attached. There is currently no way of setting this through any of the applications (lunacm or ckdemo), so the user must manually edit this file - not a preferred method. Lunacm, ckdemo, and multitoken all allow the user to specify the PED id, either on the command line or via a menu selection, but this works only for one specific session in the given application. Also, commands initrpv and deleterpv are executed only on a locally-attached PED. However, the applications which invoke these functions will simply use whatever PED id is currently specified for that session (or the default from Crystoki.conf). So these commands might incorrectly attempt to invoke a remote PED. **Workaround:** Modify the configuration file, or specify at the command line for each instance.

Resolved Issues

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

Priority	Classification	Definition
C	Critical	No reasonable workaround exists.
H	High	Reasonable workaround exists.
M	Medium	Medium level priority problems.
L	Low	Lowest level priority problems.

List of Resolved Issues

Issue	Severity	Synopsis
LHSM-20527 SDK JSP Samples differ between Linux and Windows installations.	M	**Problem:** The Windows installation for SDK JSP Samples does not include SM3Demo. **Resolution:** Fixed. The Windows installshield now includes SM3Demo.

Issue	Severity	Synopsis
LHSM-19368 JavaSP Samples are not in the correct directory for all Unix clients	M	**Problem:** The Java sample cases do not compile for Unix clients because the Java Samples are placed in the wrong directory during installation. **Resolution:** Fixed. The Java sample cases are now placed in the correct directory.
LHSM-19077 lunacm partition init command does not update label name on AIX	M	**Problem:** On SafeNet HSM Client for AIX, the LunaCM command "partition init" does not update the slot label. **Resolution:** Fixed. The "partition init" command now functions properly.
LHSM-18229 SafeNet Network HSM 6.0: on reboot of SafeNet Network HSM, the Backup HSM is not detected.	M	**Problem:** Backup HSM attached directly into the appliance. Reboot the SafeNet Network HSM After reboot, the Backup HSM is not detected. **Resolution:** Fixed.
LHSM-18483 SNMP unable to access Cryptoki library	M	**Problem:** SNMP is unable to access the Cryptoki library after uptimes of 22 days or longer. **Resolution:** Fixed.
LHSM-17857 when installing CA Safenet provider options are not available after ksp registrations	M	**Problem:** Upon registration of ksp partitions using kspconfig.exe, a restart is sometimes necessary when installing your CA, as the SafeNet provider options for the cryptographic algorithms sometimes do not show up in the drop down menu without the restart. **Resolution:** Fixed.
LHSM-16830 Remote backup server cannot connect to Remote PED when in external LunaCM session	M	**Problem:** SafeNet Client connection to SafeNet Network HSM on one computer and a SafeNet Remote Backup HSM with RBS session on a second computer. Assign the Backup HSM as a Remote Backup device for the SafeNet Network HSM. First computer lunacm instance can now see both the SafeNet Network HSM partition and the backup HSM. Attempting "ped connect" against the Backup HSM's slot via lunacm on the first computer fails. Running "ped connect" on the second computer FOR the Backup HSM connected to that computer, succeeds. **Resolution:** Fixed. A remote backup server can now connect to remote PED through an external LunaCM session.
(LHSM-10152) windows Client – lunacm : Cannot load library	M	**Problem:** After installing SafeNet HSM Client on windows server 2008 RC2, tried to run lunacm. Got "Cannot load library: The specified module could not be found". **Resolution:** Fixed.

Support Contacts

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