# SafeNet HSM 6.2.2

## CUSTOMER RELEASE NOTES

**Issue Date:** 27 January 2017

**Document Part Number:** 007-012225-008 Rev.C

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

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

SafeNet PCIe HSM is a PCIe 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 PCIe HSM are available – password authenticated and PED authenticated - in two performance variants, the SafeNet PCIe HSM-1700 or PCIe-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 Release 6.2.2 is:

- a replacement Client, which improves robustness of the HA implementation and includes bug fixes, and
- a field upgrade of the SafeNet Network HSM which upgrades the included OpenSSL version and
- a firmware upgrade that includes some important fixes.

# New Features and Enhancements

The following are summaries of features new to SafeNet HSM in release 6.2.2.

## HA Auto-Reconnect

The HA feature now includes the ability of the Client to reconnect and resume application operation, without intervention, after completely losing contact with the HA group of HSMs. Context is retained, and token object states are preserved.

Login is hands-free.

**[Requires SafeNet HSM Client 6.2.2; no firmware dependency]**

## HA Failover withstands member deactivation and reconnects on activation of member partition

The following scenarios are addressed in 6.2.2 Client:

- When an application starts up the HA system ensures that the partition is activated.
- If a member has failed, during recovery the system checks that the partition is activated and confirms activation before the member is added back to the group.
- When a new member is being added to an HA group, the system checks whether or not the new member partition is activated and subsequently ensures activation before the member is successfully added to the HA group.

**[Requires SafeNet HSM Client 6.2.2; no firmware dependency]**

## Network HSM gets OpenSSL upgrade

The SafeNet Network HSM receives enhanced OpenSSL to address the vulnerability described in CVE-2016-6304.

**[Requires SafeNet Network HSM appliance software version 6.2.2; no client or firmware dependency]**

## Updates

One critical issue involves a rare condition that would prevent an HSM from recovering after reboot.
The issue exists from SafeNet HSM firmware 6.22.0 and newer; customers are strongly advised to upgrade to firmware version 6.24.3.
FIPS-validated firmware 6.10.9 is unaffected.

**[Complete coverage requires firmware version 6.24.3]**

Other updates - see "Resolved Issues" on page 27.

# Advisory Notes

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

## Crypto Command Center

SafeNet Crypto Command Center is a web-based application that provides centralized management of your HSM infrastructure. With SafeNet Crypto Command Center, you can place some, or all, of your SafeNet Network HSM devices into a common device repository, provision cryptographic services (HSM partitions) on these devices, and then make these cryptographic services available to application owners, on an organizational basis, for use with their cryptographic applications.

Download a trial version of Crypto Command Center here;

http://www2.gemalto.com/crypto-command-center/freemium-form.html

 

## Terminology Change

The feature formerly called SIM is now called Scalable Key Storage. The Capability Update now appears under that name when capabilities are listed. The terminology has also been updated throughout the documentation where appropriate.

## Create a new SSL/NTLS Certificate on first use

All SafeNet Network HSMs come from the factory with the same SSL (NTLS) key. For proper security, run the **sysconf regencert** command before configuring your system for first use.

## After SRK is enabled lunacm reports transport mode disabled

If Lunacm **srk show** command does not show the expected state for SRK after you run this command, the cache might not have been updated, following the most recent change. Exit and re-launch lunacm to see the current state of SRK.

## 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. Use CKDemo option 98, sub-option 16. If it is set to "enhanced roles", select it to set it to "legacy Luna roles". The setting is a toggle, and flips every time you see it.

## SSH problem after appliance upgrade

Due to SSH security enhancements made to the SafeNet Network HSM appliance, the updated appliance now requires that Windows users employ PuTTY v0.67 for secure communication. PuTTY version 0.67 is provided with release 6.2.1 and newer Clients. Discontinue using PuTTY versions that accompanied earlier Client installations and replace with the newer version.

The newer version of PuTTY is backward compatible, and can negotiate to communicate with older HSM appliances, but updated HSM appliances are required to comply with the newer, more stringent security supported only by the newer PuTTY client.

## 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.

## Modification to DES3 Algorithm for NIST Compliance

NIST standard SP 800-67 specifies Triple-DES (a.k.a DES3), and is a static document. NIST SP 800-131A specifies adjustments to that original standard and to others, and is a living document updated periodically.

Per NIST document SP 800-131A Revision 1, that came into effect 01 January 2016, when the HSM is in FIPS mode, 16-byte two-key DES3 is now restricted to legacy operations (decryption, unwrapping, and CMAC verification). All other

operations for DES3 must use the 24-byte three-key variant. However, the restriction **also** applies to one form of 24-byte 3-key DES3.

**Note:** Three-key triple DES has two options:
- The first option has three keys such that K1≠K2≠K3 (all three keys unique), which is accepted by the HSM when it is in FIPS mode, for non-legacy operations.

- The second option has K1=K3≠K2 (only two keys are unique), which is considered to be the security equivalent of 2-key DES3, and therefore not acceptable for non-legacy operations.

Only when the HSM is **not** in FIPS mode, can the 2-key and the equivalent-to-2-key DES3 variants be used freely.

## SQL 2016 Support

Firmware 6.10.9 supports SQL 2016 in both FIPS and non-FIPS modes, but firmware 6.24.3 supports SQL 2016 only in non-FIPS mode.

## Scalable Key Storage Migration Patch

If you want to migrate a Scalable Key Storage-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 support SFF backup only on PED-authenticated HSMs, not password-authenticated HSMs.

## HTL is deprecated

The HTL feature is now deprecated, and will be discontinued in a future release. If you have been using HTL, please plan for configuration and work-flow that does not make use of it.

# Compatibility and Upgrade Information

This section provides upgrade paths and compatibility information for SafeNet HSM 6.2.2 software and firmware versions.

## Upgrade Paths

| Component | Directly from version | To version |
|---|---|---|
| SafeNet HSM client software | Any | 6.2.2 |
| SafeNet Network HSM appliance software | 5.4.7, 6.0.0, 6.1.0, 6.2.0, 6.2.1 [see Note 1] | 6.2.2 |
| HSM firmware | 6.2.x, 6.10.x, 6.20.x, 6.21.x, 6.22.x, 6.23.0, 6.24.0, 6.24.2 [see Note 2] | 6.24.3 |
| 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 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 6.24.3. 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, newer versions of PED firmware are needed. For example, SFF requires PED firmware 2.6.0. 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 at the test lab, not yet submitted to NIST: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140IUT.pdf
- Modules in Process at NIST (lab test report was submitted): 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 is compatible with virtual environments. SafeNet PCIe HSMs are not supported in virtual environments. See note below about USB HSM with ESXi.

| 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<br>**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 |
| | 2016 | 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 |

  

| 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 |
|---|---|---|---|---|---|
| SuSE Enterprise Linux (SEL) | 10 | Yes | Yes | Yes | Yes |
| | 11 | Yes | Yes | Yes | Yes |
| Debian | 6 | Yes | No | No | Yes |
| | 7 | Yes | No | No | Yes |
| | 8 | Yes | No | No | Yes |
| FreeBSD<br>**Note**: FreeBSD is supported only for SafeNet Network HSM. | 8.3, 8.4 | Yes | Yes | Yes | Yes |
| | 9 | Yes | Yes | Yes | Yes |
| | 10 | 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<br>**Note:** Only SafeNet Network HSM is supported; SafeNet USB HSM and SafeNet PCIe HSM are not supported with AIX for this release. | 6.1 | Yes | Yes | Yes | No |
| | 7.1 | Yes | Yes | Yes | No |

## ESXi

SafeNet USB HSM (formerly Luna G5) is supported in pass-through mode, connected to an ESXi host.

| Item | Versions |
|---|---|
| ESXi | 5.5 and 6.0 |
| LunaClient versions | 5.4.1, and above |
| HSM firmware | 6.10.9 and above |
| Virtual Machines | Windows 2012 R2 and RHEL 7 |

## 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 2016
- 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

### Installing Advanced Configuration Upgrades

More detailed instructions can be found in the Administration Guide of the product documentation.

0. Before proceeding, backup all HSM partition contents that you wish to preserve.

For all three SafeNet HSM types, any Advanced Configuration Upgrade is a capability update file (CUF) and a text file with the required authentication code.

For SafeNet PCIe HSM and SafeNet USB HSM the .CUF file and authcode file are positioned manually, and you apply using a SafeNet utility that comes with LunaClient.

1. Acquire the capability update (normally in an archive file) from Gemalto, and copy or move the unpacked .CUF and .authcode files to the desired location.

2. Run lunacm, select the slot representing the Admin Partition of the desired HSM, and log in as HSM SO with the **role login** command.
3. Use command **hsm updateCap** providing the filename of the capability update file and the filename of the authcode file. Lunacm installs the upgrade.

For SafeNet Network HSMs, the operating system is not directly available, so the same CUF is transferred to the appliance wrapped in a Secure Package (spkg) that lunash recognizes and can unpack in the correct location to be applied to the HSM. The authcode file is retained at your location so the text inside can be manually typed in during package update on the HSM.

1. Acquire the capability update (normally in an archive file) from Gemalto, and unpack the archive.
2. Use a text editor to view the authentication code in the .authcode file.
3. Use scp or pscp to copy the unpacked secure package file to the "admin" account on the selected Network HSM appliance, or to a named account on the appliance that has appliance administrator role privileges.
4. Connect via SSH and log into a Luna Shell session (lunash) on the SafeNet Network HSM appliance as the same administrative user to which you sent the secure package.
5. Use lunash command **hsm login** to log into the HSM as the HSM SO.
6. Run command **package update** <package-name>.spkg **-authcode** <authcode> (type in the authentication code that you read from the <package-name>.auth file).
7. Run command **hsm update capability -capability** <capabilityname>
   Lunash installs the upgrade.

## Server Compatibility

The SafeNet PCIe 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 | With one processor configured in the server, only Slots 2 and 3 are enabled. Therefore, Slot 1 does not detect an HSM card. |

### SafeNet PCIe HSM Server Compatibility

The SafeNet PCIe 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 6.2.2 Overview that is included with your HSM documentation.

## RADIUS Compatibility

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

# Update Instructions

## Reasons for Upgrade

If you have any SafeNet HSM at release 5.4.7 or newer, you can upgrade to version 6.2.2 to obtain the value of newer features and fixes. See "The following are summaries of features new to SafeNet HSM in release 6.2.2." on page 3 earlier in this document for brief summaries of new features in release 6.2.2. Refer to the respective Customer Release Notes for earlier releases, to learn about features added or modified in those releases that became available since the version that you currently have installed.

**Note:** For any customer running SafeNet General Purpose HSM release 6.0, or 6.1, or 6.2.1 you are highly recommended to upgrade to release 6.2.2.

If HSM firmware is currently at version 6.22.0 or higher, we highly recommend that you update to firmware version 6.24.3.

If FIPS compliance is a requirement of your security policy, keep your HSM firmware at version 6.10.9 until a newer version achieves FIPS validation.

## Upgrade Paths

Refer to the section "Compatibility and Upgrade Information" on page 7 earlier in this document.

**Note:** When you install SafeNet Network HSM software, you displace the firmware version that was previously in standby. So, if you need FIPS validation and do not have firmware 6.10.9 in your appliance, simply contact Gemalto and download a stand-alone firmware 6.10.9 upgrade package.

## Component Firmware Versions

The following table lists the supported firmware versions for the various components supported in SafeNet HSM 6.2.2.

| Component | Version |
|---|---|
| SafeNet Network HSM and SafeNet PCIe HSM firmware | 6.24.3 * |
| SafeNet Remote Backup HSM firmware | 6.10.9 * |
| SafeNet USB HSM firmware | 6.24.3 * |
| SafeNet PED 2 | 2.4.0-3 through 2.6.0 |
| SafeNet PED 2 Remote (Remote PED - requires PED workstation s/w on PC) [optional] | 2.4.0-3 through 2.6.0 |

*You can upgrade SafeNet HSM Client and (for SafeNet Network HSM) the appliance software to version 6.2.2 while leaving the HSM firmware at lower firmware versions, but several SafeNet HSM 6.2.2 features are not supported

  

| Component | Version |
|---|---|
| without the latest firmware. Refer to the list of new features, which indicates which ones are software-only, and which ones require firmware 6.24.3.<br>We recommend that you upgrade 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. | |

# Preparing for the Upgrade

Before attempting to upgrade to SafeNet HSM 6.2.2, ensure that you have satisfied the following prerequisites:

- you have the upgrade software (downloaded from the Gemalto Service Portal).
- you have the authentication credentials required to perform the upgrade.
- you have prepared your HSMs for the upgrade.

Each of these prerequisites is discussed in detail in the following sections.

## Obtaining the Upgrade Software

All of the software and firmware required to upgrade to SafeNet HSM 6.2.2 is available via download from the Gemalto Service Portal (formerly Customer Connection Center or C3).

**Note:** Authorization codes are required to install firmware. To obtain the authorization codes for your firmware, contact SafeNet Technical Support.

The following packages are included in the upgrade software:

- SafeNet HSM 6.2.2 client software
- SafeNet Network HSM 6.2.2 appliance software
- SafeNet HSM 6.24.3 firmware (suitable for SafeNet USB HSM, SafeNet PCIe HSM and SafeNet Network HSM)
- PED firmware (Refer to the readme.txt file included in the SafeNet HSM 6.2.2 client software for more information)

## Required Authentication Credentials

You must be able to log in to the HSM as the security officer (SO) to perform the upgrade. On PED-authenticated HSMs, you need the blue PED key. On password-authenticated HSMs, you need the SO password. On SafeNet Network HSM, you also need to be able to log in to the appliance using an admin-level account before you can log in to the HSM as the SO.

To install the SafeNet HSM Client software on a computer, you must run the installer with root/super-user privileges (Linux/UNIX) or Administrator privileges (Windows), or be able to launch the installer from an “Administrator: Command Prompt” (Windows).

## Preparing your HSMs for the Upgrade

Perform the following tasks to prepare your HSM for the upgrade:

**Note:** Generally, the following actions can be performed remotely for PED-Authenticated HSMs, as long as you have already imprinted an orange Remote PED Key for that HSM, and have that orange key available to use at a Remote PED workstation (see the main SafeNet HSM customer documentation for instructions to configure and use the Remote PED feature).

1. Ensure that your appliance software (for SafeNet Network HSM only), and firmware are at a starting version listed in the "Upgrade Paths" section above. (The installed Client software version does not matter, because the Client software installs in place of any previous version, with no dependencies on any previous version.)
2. Connect your HSM appliance or host computer to an uninterruptible power supply (UPS), if available. Although this is not a requirement, use of a UPS is strongly recommended to ensure successful completion of all upgrade activities.
3. Ensure that your USB devices (SafeNet USB HSM, SafeNet Remote Backup HSM) are connected using a USB cable, to the computer on which you are installing the Luna software. If the USB devices are not connected to the host computer, the USB drivers do not install successfully. This issue applies to Windows 2008 only.
4. If the Secure Recovery Key (SRK) on the HSM is enabled, it must be disabled before you can upgrade the HSM firmware. The SRK carries an external split of the HSM's Master Tamper Key (MTK) that is imprinted on the purple PED key. When you disable the SRK, the SRV (Secure Recovery Vector) portion of the MTK is returned to the HSM, so that the SRV is no longer external to the HSM. It is only in this state that you can upgrade the HSM firmware. After you upgrade the firmware, you can re-enable SRK, if desired, to re-imprint a purple PED key with the SRV.
5. Backup the content of your HSM or HSM partitions to SafeNet Backup HSMs, or to Small Form-Factor Backup devices (if you have the SFF Backup option).
6. Copy the SafeNet HSM 6.2.2 upgrade software package (the downloaded tar file) to the client computer and use your favorite archiving program to untar the archive.
7. Stop all applications and services that are using the HSM.
8. Disable HSM policy 39 (Allow Secure Trusted Channel). You can re-enable this policy after upgrade.

# Performing the Upgrade

Depending on the product you are upgrading you might need to upgrade the client software, appliance software, and/or the HSM firmware, as specified in the following table:

| Product | Client software upgrade | Appliance software upgrade | HSM firmware upgrade |
|---|---|---|---|
| SafeNet Network HSM | X | X | X |
| SafeNet PCIe HSM | X | | X |
| SafeNet USB HSM | X | | X |
| SafeNet Backup HSM | X | | X |

Upgrade the software/firmware in the following order:

1. Client software
2. Appliance software (SafeNet Network HSM only)
3. HSM firmware *

  

**Note:** * If your current HSM has a firmware version that supports newer attributes for HSM objects, AND you have created objects with those newer attributes, then you must **update the SafeNet Backup HSM firmware before you backup the source HSM**. The purpose is to prevent those newer attributes from being stripped off your objects by a Backup HSM whose firmware is too old to support the existence of newer attributes.
If you are using the Small Form-Factor Backup option, this is not an issue, because the storage format on SFF tokens is different.

## Upgrading the Client Software

**Note:** Upgrade the client software before upgrading the appliance software or HSM firmware.

**Overview** - upgrading your client software consists of the following main steps:

1. Ensure that all applications using the SafeNet HSM software libraries are stopped.
2. Uninstall your old client software. When you uninstall your old SafeNet HSM client software, backups of your existing configuration file (all SafeNet HSM types), and certificates (SafeNet Network HSM only), are retained so that they may be restored. Any other custom files/directories found in the client installation directory/folder that are not part of the standard client installation are also retained.
3. Install the SafeNet HSM 6.2.2 client software. On Linux/Unix, your backup configuration file and certificates are automatically restored. On Windows, your configuration file and certificates are retained.

### To upgrade the client software to SafeNet HSM 6.2.2

1. Uninstall the currently installed SafeNet HSM client software. The method you use is platform specific, as follows:
   - **Windows** Use the Windows uninstaller (Start > Control Panel > Programs and Features) to uninstall SafeNet HSM Client, which removes all of the SafeNet HSM Client software components.
   - **AIX/Linux** Run the /usr/safenet/lunaclient/bin/uninstall.sh script.
   - **HP-UX/Solaris** Run the /opt/safenet/lunaclient/bin/uninstall.sh script.
2. Install the SafeNet HSM 6.2.2 software. The method you use is platform specific, as follows:
   - **Windows** Run the LunaClient.msi installation program and respond to the prompts as they appear.
   - **Linux/Unix** Run the install.sh installation script and respond to the prompts as they appear.

## Upgrading the SafeNet Network HSM Appliance Software

If you do not have a SafeNet Network HSM Appliance, skip this section.

**Note:** Upgrade the SafeNet Network HSM appliance software before you upgrade the SafeNet Network HSM firmware. The appliance software can be applied only to the SafeNet Network HSM appliance.

**Note:** Appliance software upgrade is a one-way operation. There is currently no way to downgrade the appliance software once a new version is applied. This contrasts with

- SafeNet HSM Client software, which can be replaced by any version, simply by uninstalling

  

the current version and installing a desired version, and

- SafeNet HSM firmware, which can be rolled back to the version that was installed before the currently-installed version. This applies only to versions since firmware rollback was enabled.

### To upgrade the SafeNet Network HSM Appliance software to Luna HSM 6.2.2

1. Copy the SafeNet HSM 6.2.2 appliance package file (.spkg) to the SafeNet Network HSM appliance you want to upgrade:
   - Windows pscp <path>\<partnum>.spkg admin@<LunaSA_hostname>:
   - Unix/Linux scp <path>/<partnum>.spkg admin@<LunaSA_hostname>:
2. Stop all client applications that are connected to the SafeNet Network HSM.
3. At the console, log in to the SafeNet Network HSM appliance using an admin-level account. The default account is admin.
4. Log in to the SafeNet Network HSM as the HSM Security Officer:

   lunash :> hsm login
   - For SafeNet Network HSM with PED authentication, the blue PED Key is required.
   - For SafeNet Network HSM with Password Authentication, you are prompted for the HSM Admin (SO) password.
5. (Optional) Verify that the upgrade package file that you copied is present:

   lunash :> package listfile
6. (Optional) Verify the upgrade package:

   lunash :> package verify <partnum>.spkg -authcode <authorization_code>

   Verification requires approximately 90 seconds.
7. Install the upgrade package:

   lunash :> package update <partnum>.spkg -authcode <authorization_code>

   The installation/upgrade process takes approximately 90 seconds. During that time, a series of messages are displayed that detail the progress of the upgrade. At the end of this process, the message “Software upgrade completed!” is displayed.

## Upgrading the HSM Firmware

**Note:** Upgrade the HSM firmware only after you have upgraded the client software (and – for SafeNet Network HSM – the appliance software). This ensures that the correct version is ready to be installed.

**Note:** For any customer running SafeNet General Purpose HSM release 6.0, or 6.1, or 6.2.1 you are highly recommended to upgrade to release 6.2.2.

If HSM firmware is currently at version 6.22.0 or higher, we highly recommend that you update to

  

firmware version 6.24.3.

If FIPS compliance is a requirement of your security policy, keep your HSM firmware at version 6.10.9 until a newer version achieves FIPS validation.

On SafeNet Network HSM, use LunaSH (the Luna Shell) to upgrade the firmware. On SafeNet PCIe HSM, SafeNet USB HSM and SafeNet Remote Backup HSM, use LunaCM to upgrade the firmware.

## HSM Firmware 6.24.3 and FIPS 140-2

Firmware 6.24.3 implements some of the features of release 6.2.2, but is not currently FIPS-validated. Contact your Gemalto representative, or visit the NIST site for information about SafeNet HSM versions that have certificates, and for progress updates on HSM (and firmware) versions that are in the validation process.

For SafeNet Network HSM, when you update to SafeNet HSM 6.2.2 software on the appliance, you have the option to also immediately update the firmware to 6.24.3, or to place 6.24.3 firmware on standby, available to be installed later. If you decide not to update the firmware to 6.24.3 because you wish to use FIPS validated firmware, we strongly recommend upgrading to 6.10.9. You can obtain a stand-alone 6.10.9 upgrade package from Gemalto's service portal. It is possible to upgrade to higher firmware versions to obtain desired features, but doing so loses the appliance's FIPS validated status.

**Note:** If you have a PKI bundle including a SafeNet Network HSM and an attached SafeNet USB HSM running in PKI mode, often the SafeNet USB HSM has earlier firmware than the SafeNet Network HSM. Upgrade the SafeNet Network HSM first, following the above upgrade paths. Then, when you upgrade the firmware on the associated SafeNet USB HSM, the SafeNet USB HSM upgrades to the same firmware version as is installed on the SafeNet Network HSM.

## Upgrading SafeNet Network HSM firmware

On SafeNet Network HSM, use LunaSH (the Luna Shell) to upgrade the firmware.

1. Log in to the HSM as the HSM admin user if you are not already logged in.

   lunash :> hsm login

2. Run the firmware upgrade command. The HSM will reset when the upgrade is complete:

   lunash :> hsm update firmware

3. Use the hsm show command to verify that the firmware upgrade was successful:

   lunash :> hsm show

   If the upgrade was successful, the firmware version is displayed as 6.24.3.

**Note:** If you did not reboot the appliance before upgrading the firmware (remote PED case) the following error message is displayed:
Error: Unable to communicate with HSM.
Please run 'hsm supportInfo' and contact customer support.

You can ignore the error message.

4. If you disabled the SRK prior to performing the firmware upgrade, re-enable it if desired. Refer to the SafeNet HSM documentation for details. If you attempted to upgrade the firmware without disabling the SRK, the firmware upgrade

  

fails with the following error:

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

5. If you logged into the HSM using a remote PED, ensure that all client connections are terminated and then enter the following command to reboot the appliance:

   sysconf appliance reboot

## Upgrading the SafeNet PCIe HSM or SafeNet USB HSM/SafeNet Backup HSM firmware

To upgrade the firmware on a SafeNet PCIe HSM or SafeNet USB HSM/SafeNet Backup HSM, launch the LunaCM utility on a SafeNet HSM client computer

- that contains a copy of the firmware upgrade (.fuf) file with its associated firmware authentication code (.txt) file, and
- contains the SafeNet PCIe HSM, or
- is connected to the SafeNet USB HSM/SafeNet Backup HSM that you want to upgrade.

1. Copy the firmware file (<fw_filename>.fuf) from the firmware folder on the software CD to the SafeNet HSM client root directory:
   - Windows: C:\Program Files\SafeNet\LunaClient
   - Linux/AIX: /usr/safenet/lunaclient/bin
   - Solaris/HP-UX: /opt/safenet/lunaclient/bin
2. Obtain the firmware authorization code:
   a. Contact SafeNet Customer Support (support@safenet-inc.com). The firmware authorization code is provided as a .txt file.
   b. Copy the <fw_auth_code>.txt file to the SafeNet HSM client root directory:
   - Windows: C:\Program Files\SafeNet\LunaClient
   - Linux/AIX: /usr/safenet/lunaclient/bin
   - Solaris/HP-UX: /opt/safenet/lunaclient/bin
3. Launch the LunaCM utility:

   **Windows**

   a. Open a Command Prompt window

      (Start > Programs > Accessories > Command Prompt).

   b. Change to the SafeNet HSM client root directory:

      cd C:\Program Files\SafeNet\LunaClient

   c. Enter the following command

      Lunacm

   **Linux/AIX**

   a. Open a terminal window and change to the SafeNet HSM client root directory:

      /usr/safenet/lunaclient/bin

   b. Enter the following command:

      ./lunacm

   **HP-UX/Solaris**

a. Open a terminal window and change to the SafeNet HSM client root directory:

   /opt/safenet/lunaclient/bin

b. Enter the following command:

   ./lunacm

4. Enter the following command to log in to the HSM. Note that the password is not required on PED-based systems:

   hsm login [-password <password>]

5. Enter the following command to upgrade the firmware on an attached SafeNet USB HSM:

   hsm –updateFirmware –fuf <fw_filename>.fuf –authcode <fw_authcode_filename>.txt

### Additional Tasks for Java Users

You must copy the Java library (LunaAPI.dll) and jar file (LunaProvider.jar) from the client installation folder to the jre/lib/ext folder.

## Returning the HSM to Operation

After performing the upgrade, you must reactivate the HSM partitions (if applicable) and re-register the SafeNet HSM client to return the HSM to operation.

**To return the HSM to operation**

1. If updating from firmware below 6.22.0, the upgrade separates SafeNet USB HSM and SafeNet PCIe HSM administration partition and client application partitions, which causes client applications to see them as separate slots. This is a change from previous behavior. Make any necessary adjustments to your scripts and application settings.
2. If updating from firmware below 6.22.0, upgrading can change slot numbering, specifically the starting slot number in a slot listing. Refer to the "Slot Numbering and Behavior" section in the *HSM Administration Guide*. Other than that adjustment, for SafeNet PCIe HSM or SafeNet USB HSM your HSM is ready as soon as the firmware update is done.
3. Reactivate all partitions that were activated before the upgrade (applies to SafeNet Network HSM with PED Authentication).

# Migration Notes

SafeNet HSM 6.2 introduces significant changes to the way in which the product operates. This section describes the tasks you might need to perform to successfully migrate your HSMs to SafeNet HSM 6.2.x, if you are starting from a firmware version lower than 6.22.0.

## SafeNet PCIe HSM or SafeNet USB HSM HA groups

**Note:** This section only applies if you are upgrading from a firmware version lower than 6.22.0 to a firmware version that is 6.22.0 or higher.

Firmware 6.22.0 and above changes how you see your SafeNet PCIe HSM and SafeNet USB HSMs. In previous releases, each slot represented a physical HSM. With 6.22.0 or higher firmware, each physical HSM is divided into two distinct partitions, as follows:

- an Admin partition. The Admin partition is reserved for the HSM SO role, and uses the original (pre-6.22.0), HSM Serial Number.
- a User partition. The User partition is used by the Partition Owner/Crypto Officer for cryptography. It is assigned a new serial number, created by appending 3 digits to the original serial number.

Virtual slots, used to configure HA groups, are also viewed as user partitions, and are therefore also assigned new serial numbers.

If you are using SafeNet PCIe HSM and SafeNet USB HSMs in HA mode, you must edit your **Chrystoki.conf** (Linux/Unix) or **Crystoki.ini** (Windows) file to update the partition serial numbers for the HA group members.

## Behavior with firmware older than 6.22.0

Before firmware version 6.22.0, LunaCM did not make SafeNet PCIe HSM and SafeNet USB HSM user partitions visible. The following example shows how LunaCM displays PCIe HSM, GUSB HSM, and HA virtual slots with pre-6.22.0 firmware. Note that the HA group is shown at Slot Id 5.

### Example

```
Available HSMs:

Slot Id ->              0
Tunnel Slot Id ->       1
HSM Label ->            pcie_hsm1
HSM Serial Number ->    155316
HSM Model ->            K6 Base
HSM Firmware Version -> 6.21.0
HSM Configuration ->    Luna PCI (PED) Signing With Cloning Mode
HSM Status ->           OK

Slot Id ->              1
Tunnel Slot Id ->       2
HSM Label ->            pcie_hsm2
HSM Serial Number ->    155317
HSM Model ->            K6 Base
HSM Firmware Version -> 6.21.0
HSM Configuration ->    Luna PCI (PED) Signing With Cloning Mode
HSM Status ->           OK

Slot Id ->              5
HSM Label ->            PCIHA
HSM Serial Number ->    1155316
HSM Model ->            LunaVirtual
HSM Firmware Version -> 6.21.0
HSM Configuration ->    Luna Virtual HSM (PED) Signing With Cloning Mode
HSM Status ->           N/A - HA Group
```

### HA group definition in the Chrystoki.conf/Crystoki.ini file

The members of the HA group shown in slot 5 are defined in the **VirtualToken** section of the **Chrystoki.conf**/**Crystoki.ini** file, as illustrated below:

```
VirtualToken = {
VirtualToken00Label = PCIHA;
VirtualToken00SN = 1155316;
VirtualToken00Members = 155316,155317;
}
```

## Behavior with 6.22.0 or higher firmware

With firmware 6.22.0 or higher, LunaCM makes the user partition visible: it has its own serial number derived from the HSM's serial number. The following example shows the output of LunaCM for the same hardware after upgrading to the 6.22.0 firmware.

Note the user partition labeled **Cryptoki User** with serial number **155316014** is distinct from the HSM partition with label **pcie_hsm1** and serial number **155316**. Note also that LunaCM does not identify the HA group. This is because the serial number of the HSM user partition changed, and no longer matches the value in the HA members list in the **Chrystoki.conf** or **Crystoki.ini** file.

### Example

```
Available HSMs:

Slot Id ->              0
Tunnel Slot Id ->       6
Label ->                Cryptoki User
Serial Number ->        155316014
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->     User Token Slot

Slot Id ->              5
Tunnel Slot Id ->       6
Label ->                pcie_hsm1
Serial Number ->        155316
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->     Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK

Slot Id ->              6
Tunnel Slot Id ->       12
Label ->                Cryptoki User
Serial Number ->        155317014
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->     User Token Slot

Slot Id ->              11
Tunnel Slot Id ->       12
Label ->                pcie_hsm2
Serial Number ->        155317
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->     Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK
```

### Changes required to the Chrystoki.conf/Crystoki.ini file to restore the HA group definition

To restore the HA group configuration, you must edit the **Chrystoki.conf**/**Crystoki.ini** file to update the virtual token slot serial numbers to include the three extra digits added to the user slot serial numbers after upgrading to firmware 6.22.0 or above (in this example, the extra digits are **014**). You must add the three digits to the **VirtualToken**<nn>**SN** and **VirtualToken**<nn>**Members** entries, as shown in the following example:

  

**Before upgrading to firmware 6.22.0 or above**

```
VirtualToken = {
VirtualToken00Label = PCIHA;
VirtualToken00SN = 1155316;
VirtualToken00Members = 155316,155317;
}
```

**After upgrading to firmware 6.22.0 or above**

```
VirtualToken = {
VirtualToken00Label = PCIHA;
VirtualToken00SN = 1155316014;
VirtualToken00Members = 155316014,155317014;
}
```

## Updating Your HA Group Configurations After Upgrading to Firmware 6.22.0 or above

The following procedure describes, in detail, the steps you need to perform to reconfigure your HA group definitions in the **Chrystoki.conf**/**Crystoki.ini** file after upgrading to firmware 6.22.0 or above.

### To update your HA group definitions

1. Update all members of the HA group to firmware 6.22.0 or above.
2. Ensure that you have write access to **/etc/Chrystoki.conf** (Linux/UNIX) or **chrystoki.ini** (Windows, in the SafeNet HSM client installation directory).
3. Edit the **Chrystoki.conf**/**Crystoki.ini** file and navigate to the **VirtualToken** section. Each virtual token is defined by three entries, as follows:
   - **VirtualToken**<nn>**Label**. For example, `VirtualToken00Label`
   - **VirtualToken**<nn>**SN**. For example, `VirtualToken00SN`
   - **VirtualToken**<nn>**Members**. For example, `VirtualToken00Members`

   where <nn> starts at 00 and increments by one for each HA group

   You will need to modify the value of **VirtualToken**<nn>**Members** for each virtual token in the file to reflect its new serial number.
4. In LunaCM, enter the **partition list** command to determine the new serial numbers for the HA group members:

```
Available HSMs:
Slot Id ->              0
Tunnel Slot Id ->       6
Label ->                Cryptoki User
Serial Number ->        155316014
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->     User Token Slot

Slot Id ->              5
Tunnel Slot Id ->       6
Label ->                pcie_hsm1
Serial Number ->        155316
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->     Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK

Slot Id ->              6
```

  

```
Tunnel Slot Id ->       12
Label ->                Cryptoki User
Serial Number ->        155317014
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->     User Token Slot

Slot Id ->              11
Tunnel Slot Id ->       12
Label ->                pcie_hsm2
Serial Number ->        155317
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->     Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK
```

5. For each serial number in **VirtualToken**<nn>**Members** find the slot with the matching serial number prefix, and take note of the three additional digits. Look for this information in slots with `Slot Desciption ---> User Token Slot.`

   For example, for `VirtualToken00Members = 155316,155317`, the new serial numbers displayed in LunaCM are 155316**014** and 155317**014**.

6. Add the last portion (**014** in our example) to the serial number for each virtual token member. In our example the new values after the modifications are:

   ```
   VirtualToken00Members = 155316014,155317014;
   ```

7. Next adjust the value of **VirtualToken**<nn>**SN** in a similar manner. In our example, the adjusted value is 1155316014.

8. When you have updated the serial number for all virtual tokens and members, save the file.

9. If the HSMs are PED-AUTH, log in to each user partition slot (where Slot Description --> User Token Slot), one at the time, and enter the following LunaCM commands to activate the partition (the activation policy remains on after firmware update).

   **slot set -slot** <slot_id>
   **role login -n "Crypto Officer"**

   You will be prompted for the challenge in LunaCM, and for the black key at the attached PED device. Successful login will activate your partition.

10. You should now be able to see your virtual token (HA group). First, restart LunaCM in one of following two ways:

    - Exit from LunaCM by typing **exit** and launch LunaCM again
    - From the lunacm:> prompt, enter **clientconfig restart -force**

    LunaCM output for our example now shows:

    ```
    Available HSMs:
    Slot Id ->              0
    Tunnel Slot Id ->       6
    Label ->                Cryptoki User
    Serial Number ->        155316014
    Model ->                K6 Base
    Firmware Version ->     6.22.0
    Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
    Slot Description ->     User Token Slot

    Slot Id ->              5
    ```

```
Tunnel Slot Id ->       6
Label ->                pcie_hsm1
Serial Number ->        155316
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->     Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK

Slot Id ->              6
Tunnel Slot Id ->       12
Label ->                Cryptoki User
Serial Number ->        155317014
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->     User Token Slot

Slot Id ->              11
Tunnel Slot Id ->       12
Label ->                pcie_hsm2
Serial Number ->        155317
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->     Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK

Slot Id ->              8
HSM Label ->            PCIHA
HSM Serial Number ->    1155316014
HSM Model ->            LunaVirtual
HSM Firmware Version -> 6.22.0
HSM Configuration ->    Luna Virtual HSM (PED) Signing With Cloning Mode
HSM Status ->           N/A - HA Group
```

# 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 |
|---|---|---|
| LHSM-36894: lunacm HA list command doesn't always show the correct HA sync state | H | **Problem:** LunaCM HA sync code will not always detect out-of-sync condition between HA member.<br>To reproduce, use ckdemo to create a data object on the HA virtual slot and then create another data object on one of the physical HA member slots only. With this setup, the HA slot should be out of sync but HA list command will report that the HA slot is in-sync.<br>.<br>**Workaround:** Avoid writing directly to individual (physical) member slots when HA is active. |
| LHSM-31236: Ckdemo: token serial number does not match with the partition serial number in 6.1 and above | H | **Problem:** *Steps to reproduce:*<br>1. assign one partition to remote Luna Client<br>2. from lunaclient check the slot infor by vtl v<br>3. ckdemo check the token infor (option 12)<br>*Expecting:*<br>The token serial number from ckdemo to match with the partition serial number that shows from the vtl v.<br>*Actual result:*<br>The token serial number does NOT match with the partition serial number.<br>`LunaClient 6.2.0-15-Linux 64`<br>`vtl v`<br>`Slot Serial # Label`<br>`==== ================ =====`<br>`1 1072743706450 P1SA1`<br>`2 1107440122459 P1SA3`<br>`ckdemo option 12`<br>`Token label -> P1SA1`<br>`Token Manufacturer -> Safenet, Inc.`<br>`Token Model -> LunaSA`<br>`Token Serial Number -> 3296849746`<br>`Token label -> P1SA3`<br>`Token Manufacturer -> Safenet, Inc.`<br>`Token Model -> LunaSA`<br>`Token Serial Number -> 3633527387`<br>**Workaround:** None for CKDemo at this time. Functions properly in lunacm. |
| LHSM-41016: Cannot upgrade FW on backup HSM with partition | M | **Problem:**<br>1. Start with a backup HSM with FW 6.10.9<br>2. Partition backup some objects to the backup HSM<br>3. Try to do firmware upgrade on the backup HSM<br>4. It fails and complains<br>`lunacm:> hsm uf -u fwupdateG5_realCert_6.24.2_RC6.FUF -a authcodeG5_realCert_6.24.2_RC6.TXT`<br>`You are about to update the firmware.`<br>`The HSM will be reset.`<br>`Are you sure you wish to continue?`<br>`Type 'proceed' to continue, or 'quit' to quit now -> proceed` |

| Issue | Severity | Synopsis |
|---|---|---|
| | | Updating firmware. This may take several minutes.<br>Number of Partitions found: 1<br>New Partition Headers are larger. Checking for free space to accommodate this.<br>Partition #: 1 Name: backup1 Status: Failed<br>Current Free: 0 bytes Required: 7164 bytes<br>Objects must be deleted from 'Failed' Partitions before FW Upgrade can be applied.<br><br>Command Result : 0x80000903 (CKR_UNKNOWN)<br>.<br><br>**Workaround:** Avoid updating the Backup HSM firmware past the recommended version 6.10.9. Or clear objects from any existing partition, or delete the backup partition before performing firmware upgrade to a version newer than 6.10.9. |
| LHSM-32337: After disabling the "HA auto-synchronization" mode, it still shows "need sync no". | M | **Problem:** Steps to reproduce:<br>1. Perform the network setup on two SafeNet Network HSM<br>2. Ensure that the Allow Cloning and Allow Network Replication policies are “On” in hsm showPolicies.<br>3. Create a partition on each SafeNet Network HSM. They must have the same password.<br>4. Create a Network Trust Link between the Client and the Appliance<br>5. Register client computer with both SafeNet Network HSMs<br>6. On client machine, run the lunacm utility. It must show the registered partitions.<br>7. Run hagroup create command:<br>`lunacm:> haGroup creategroup -serialNumber <serial number> -l <label> -p <password>`<br>The serial number must be of the partition which will be added to the hagroup as first member. The label given will be the name of hagroup.<br>8. Run hagroup addmember command to add another member to the HA group:<br>`lunacm:> hagroup addMember-serialNumber <serial number> -group <groupname> -password <password>`<br><br>9. Similarly create one more HA group.<br>10. Run ha listgroup to check auto-sync enabled on both groups.<br>11.Disable ha-sync on one of ha group<br>12. Run ha listgroup to verify autosync is disable on one of ha group<br>13. Start two traffic on both ha group slot with 100 threads, running for a while, then stop traffic<br>14. check sync state on both ha group<br>Expected:<br>One HA group should be sync, another should not<br>Actual Output:<br>Shows sync required : NO<br><br>**Workaround:** None. |

 

| Issue | Severity | Synopsis |
|---|---|---|
| LHSM-31213: HA member doesn't show it is alive even after auto-recovery | M | **Problem:** When a member of an HA group is removed and brought back after auto-recovery is done, the log messages says that the recovery attempt is successful but lunacm does not show that the recovered member is alive or up.<br>**Workaround:** Restart lunacm to update the slot list. |

# Resolved Issues

This section lists issues fixed 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-41768 LHSM-41630 bonding is disabled after reboot (reboot is part of configuring bonding) | C | **Problem:** When configuring port bonding, the user is expected to restart the appliance in order to complete the configuration. However, once the appliance is restarted bonding goes disabled and does not work<br><br>**Fixed:** Fixed in SafeNet Network Appliance software version 6.2.2. |
| LHSM-41609 LHSM-31155 HSM unrecoverable crash after Network HSM Appliance reboot | C | **Problem:** A rare HSM condition could cause the HSM to enter an unrecoverable state after rebooting.<br>This issue can be present in SafeNet HSM firmware versions from 6.22.0 through 6.24.2.<br><br>**Fixed:** Requires firmware update to version 6.24.3 |
| LHSM-41622 Luna SA6.2.2: CVE-2016-6304 OpenSSL | H | **Problem:** To address CVE-2016-6304 OpenSSL vulnerability an update to the *OpenSSL appliance version is required from existing SafeNet Network HSM 6.2.1. |

| Issue | Severity | Synopsis |
|---|---|---|
| vulnerability appliance patch | | **Fixed:** Appliance software 6.2.2 updates OpenSSL. |
| LHSM-41162 SA 6.2.1 windows client will crash after C_Finalize call if HA is configured for active recovery mode | H | **Problem:** A bug causes HA active recovery to continue after C_Finalize is called by the client application, which can crash an application that does not exit shortly after C_Finalize.<br><br>**Fixed:** Fixed in 6.2.2 client library. |
| LHSM-37045 Large data fails signature in 6.24.0 | H | **Problem:** Attempts to sign data in the megabyte data size range can result in CKR_DEVICE_MEMORY error.<br><br>**Fixed:** Fixed in 6.2.2 client library. |
| LHSM-37038 Register a Luna SA to the client will fail if the Luna Client CAFile.pem is empty | H | **Problem:** If the CAFile.pem is empty, an attempt to register a SafeNet Network HSM to the client fails with:<br>Error: Could not register the server's certificate. Please ensure filename provided is correct and that the current user has read and write privileges to the files and directory at: /usr/safenet/lunaclient/cert/server/CAFile.pem. (-2)<br><br>**Fixed:** Fixed in 6.2.2 client library. |

# Support Contacts

| Contact method | Contact |
|---|---|
| **Address** | SafeNet, Inc.<br>4690 Millennium Drive<br>Belcamp, Maryland 21017<br>USA |

| Contact method | Contact | |
|---|---|---|
| **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<br>Provides access to the SafeNet Knowledge Base and quick downloads for various products. | |
| **Technical Support Customer Portal** | https://serviceportal.safenet-inc.com<br>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. | |

  