



SafeNet HSM 6.3

CUSTOMER RELEASE NOTES

Issue Date: 06 October 2017

Document Part Number: 007-012225-011 Rev.C

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

http://www.securedbysafenet.com/releasenotes/luna/cm_luna_hsm_6-3-0.pdf

Contents

| | |
|---|----------|
| Product Description | 3 |
| SafeNet Network HSM | 3 |
| SafeNet PCIe HSM | 3 |
| SafeNet USB HSM | 3 |
| Release Description | 3 |
| New Features and Enhancements | 3 |
| New USB-powered PED | 4 |
| New 6.3.1 Client Adds Support for the CKM_RSA_PKCS_PSS Mechanism to the Java LunaProvider | 7 |
| Client Support for Windows Server 2016 | 7 |
| IPV6 support | 8 |
| Technology Preview Features are Mainstreamed | 8 |
| Partition Renaming using LunaSH | 8 |
| Crypto User Can Clone Public Objects | 8 |
| External Power Supply for SafeNet Backup HSM and SafeNet USB HSM | 8 |
| Advisory Notes | 8 |
| SafeNet Luna Client Installation on Windows Server 2012/2012R2 | 8 |
| REST API | 9 |
| NTLS Keys-in-Hardware Feature is Deprecated | 9 |
| Crypto Command Center | 9 |
| Terminology Change | 9 |
| Create a New SSH Certificate on First Use | 9 |
| After SRK is Enabled, LunaCM reports Transport Mode Disabled | 9 |
| CKDemo Requires Additional Configuration with Firmware Older than 6.22.0 | 9 |
| SSH Problem After Appliance Upgrade | 10 |
| New Objects Visible in PPSO User Partition | 10 |

| | |
|--|-----------|
| Minimum Recommended Firmware for SafeNet Remote Backup HSM | 10 |
| Modification to DES3 Algorithm for NIST Compliance | 10 |
| SQL Server 2016 Support | 10 |
| Luna SA4 SIM Migration Patch | 11 |
| Small Form Factor (SFF) Backup Support Notes | 11 |
| HTL is deprecated | 11 |
| Compatibility and Upgrade Information | 12 |
| Upgrade Paths | 12 |
| About FIPS Validation | 13 |
| About Common Criteria | 13 |
| Supported Operating Systems | 13 |
| Remote PED Server | 15 |
| Supported APIs | 15 |
| Advanced Configuration Upgrades | 15 |
| Server Compatibility | 16 |
| RADIUS Compatibility | 16 |
| Update Instructions | 17 |
| Upgrade Paths | 17 |
| Component Firmware Versions | 17 |
| Preparing for the Upgrade | 18 |
| Obtaining the Upgrade Software | 18 |
| Required Authentication Credentials | 18 |
| Preparing your HSMs for the Upgrade | 18 |
| Performing the Upgrade | 19 |
| Upgrading the Client Software | 20 |
| Upgrading the SafeNet Network HSM Appliance Software | 20 |
| Upgrading the HSM Firmware | 21 |
| Returning the HSM to Operation | 24 |
| Migration Notes | 24 |
| SafeNet PCIe HSM or SafeNet USB HSM HA groups | 24 |
| Known Issues | 29 |
| Issue Severity Definitions | 29 |
| Known Issues | 30 |
| Resolved Issues | 33 |
| List of Resolved Issues | 33 |
| Support Contacts | 34 |

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 6.3 is:

- a replacement Client that supports IPv6
- a field upgrade of the SafeNet Network HSM 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 6.3.

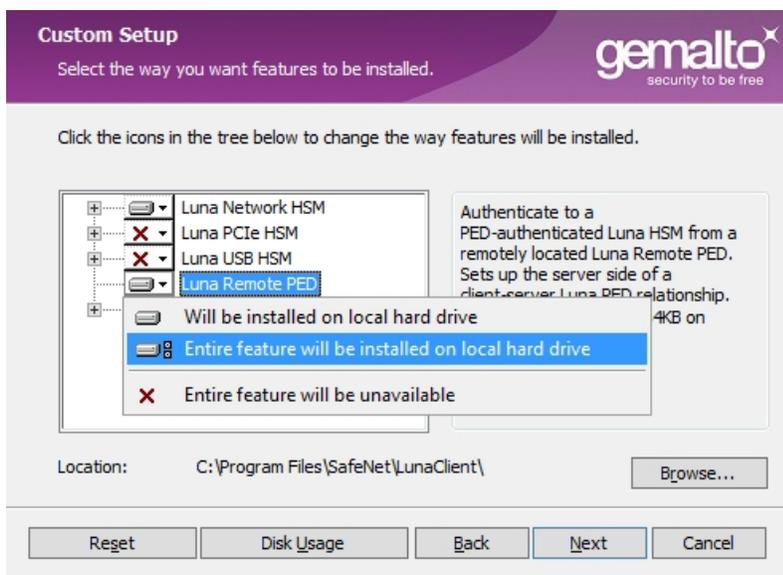
New USB-powered PED

Gemalto is pleased to announce the availability of SafeNet Luna HSM Pin Entry Device (PED) v2.8. The v2.8 PED contains new hardware that supports the ability to be USB-powered, a feature frequently requested in the past. With the new PED, there is no longer a requirement for an external DC power Adapter. PED v2.8 is functionally equivalent to your existing (pre-generation) PEDs and is compatible with HSM versions, 5.x, 6.x, and 7.x.

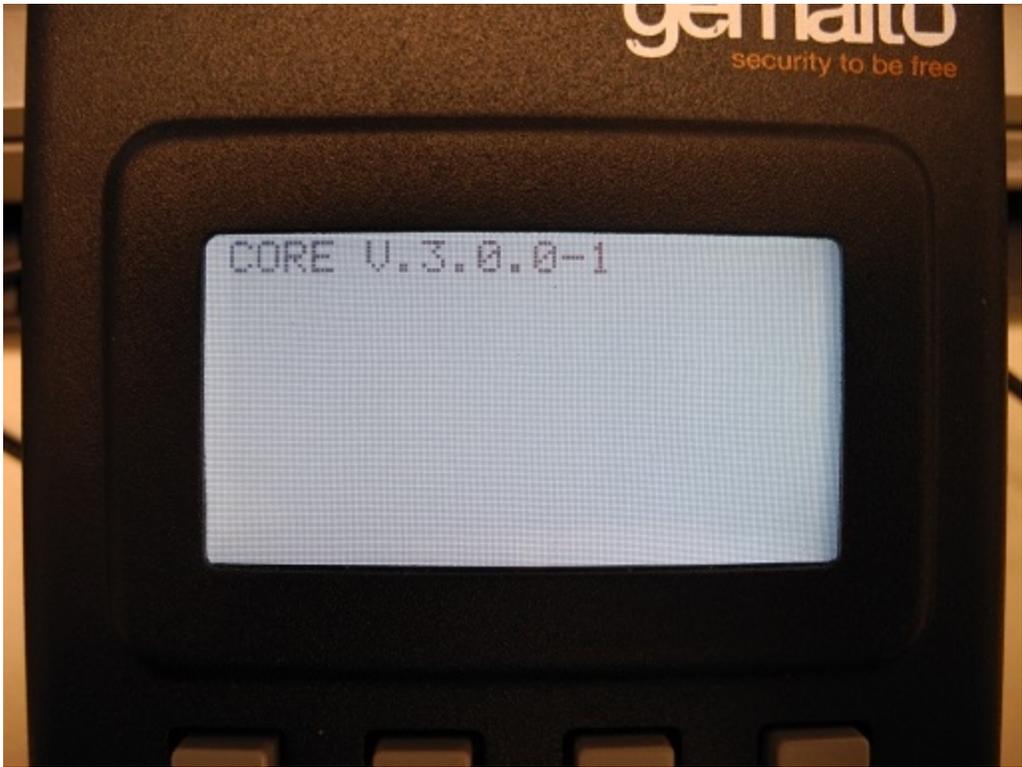
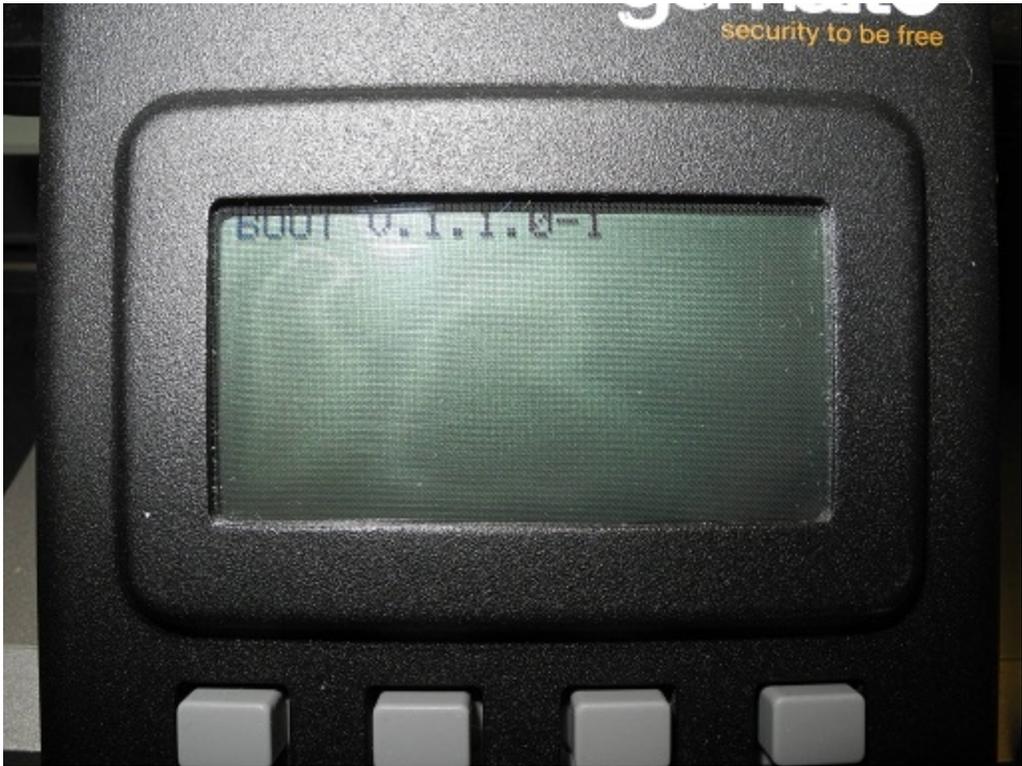
PED v2.8 ships with firmware 2.8.0. Note that you cannot upgrade existing PEDs to the 2.8.0 version; existing PEDs continue to need a separate DC power adapter for remote PED and upgrade use. The part number on the manufacturer's label identifies the refreshed PED: 808-000060-002 or 808-000060-003.

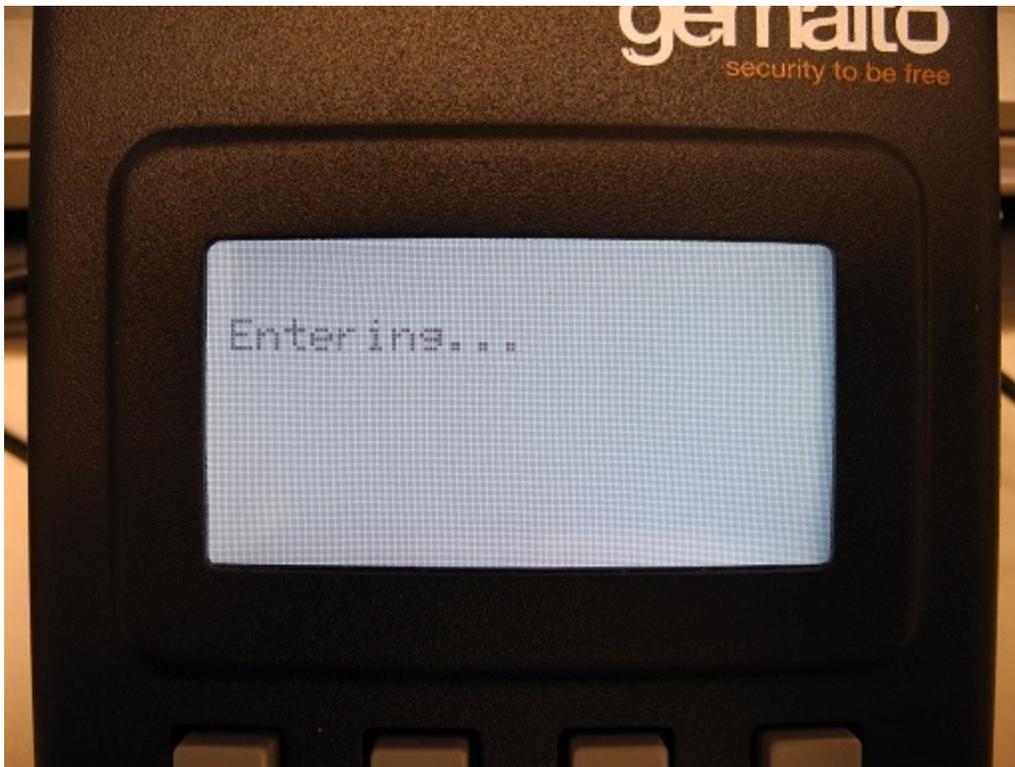
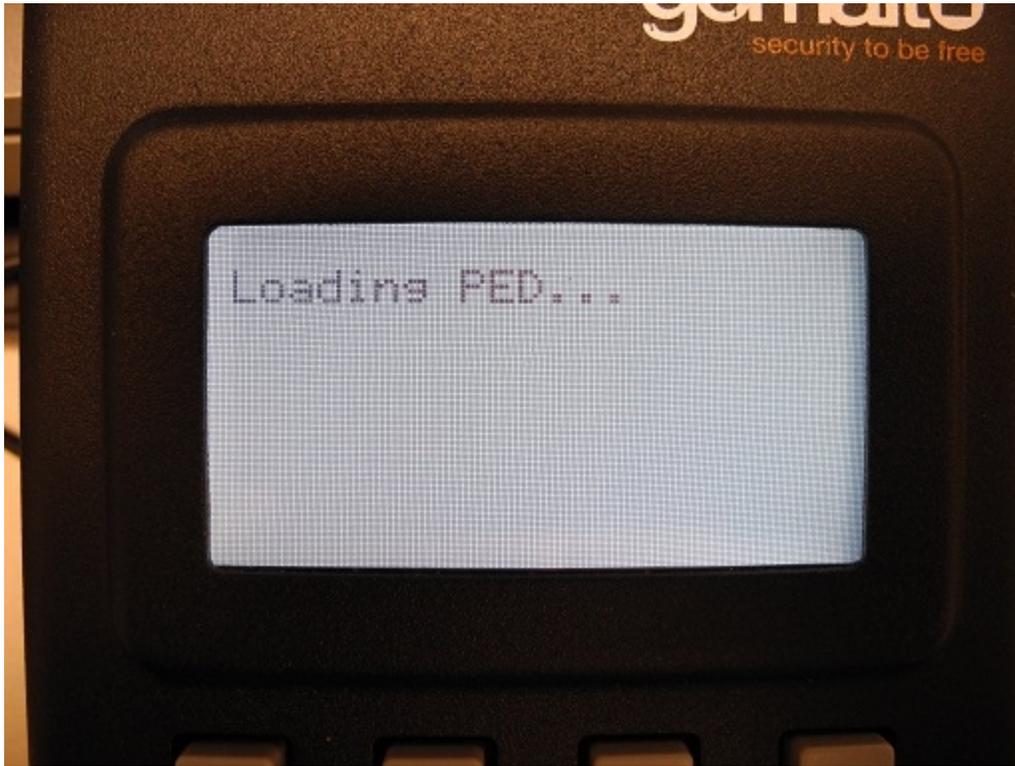
To use the new USB-powered PED

1. Download the SafeNet Luna client from the Gemalto Service Portal, if necessary.
2. Install the Remote PED component of the SafeNet Luna client on any client computer that will use the new PED (either in Local or Remote mode). Installing the Remote PED component of the SafeNet Luna client installs the required driver.

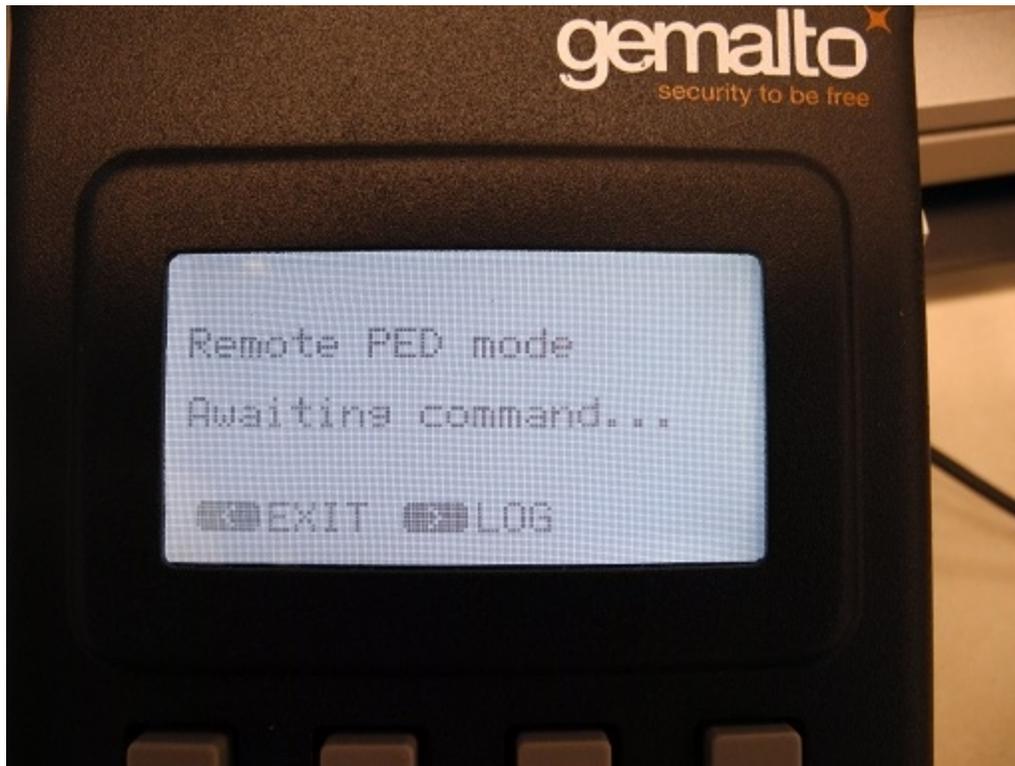


3. Connect the PED to the computer where you installed the Remote PED component of the SafeNet Luna client:
 - For Local PED - Use the PED cable provided, connected to the PED's SCP port.
 - For Remote PED and PED firmware upgrades - Use the USB cable provided, connected to the PED's USB port.
4. After you connect the PED to the host computer, it will take 30 to 60 seconds for initial boot-up, during which time a series of messages are displayed, as illustrated below:





5. After boot up is complete, the PED displays the mode (**Remote PED mode** or **Local PED mode**) and the **Awaiting command...** prompt, as illustrated below. Your new PED is now ready for use.



New 6.3.1 Client Adds Support for the CKM_RSA_PKCS_PSS Mechanism to the Java LunaProvider

The 6.3.1 client, for 64-bit Linux only, adds support for the CKM_RSA_PKCS_PSS mechanism to the Java LunaProvider. All other functionality is identical to the 6.3 client.

To deploy the 6.3.1 client

1. Download the 6.3.1 SafeNet Luna client from the Gemalto Service Portal.
2. Install the 6.3.1 SafeNet Luna client on any Linux 64-bit client computer used to host Java applications that require the CKM_RSA_PKCS_PSS mechanism. Refer to the *Installation Guide* for detailed uninstallation/installation instructions.
 - a. Uninstall the existing SafeNet Luna client, if applicable.
 - b. Install the 6.3.1 SafeNet Luna client, including the Java components, and configure your Java environment as required. Refer to the *Installation Guide* for details.
3. Update your Java applications as required to use the CKM_RSA_PKCS_PSS mechanism.

Client Support for Windows Server 2016

The SafeNet Luna client is now supported on Windows Server 2016. See "[SafeNet Luna HSM 6.3 Client](#)" on page 13 for a complete list of supported operating systems.

IPV6 support

The SafeNet Network HSM appliance now supports the use of secure shell and cryptographic operations over IPV6, in addition to IPV4.

[Requires SafeNet HSM Client 6.3 and Network HSM appliance software 6.3; no firmware dependency]

Technology Preview Features are Mainstreamed

The features originally previewed in release 6.2.1 have been extensively verified and are now considered mainstream product features, with the exception of port bonding enhancements.

[Requires SafeNet HSM Client 6.3; SafeNet Network HSM software 6.3, and firmware 6.27.0]

Partition Renaming using LunaSH

Partitions can be created and configured with generic names (any name you wish), and can be renamed at a later time, when deployed to other entities (customers, departments, business units, etc.)

[Requires SafeNet HSM Client 6.3; SafeNet Network HSM software 6.3, and firmware 6.27.0]

Crypto User Can Clone Public Objects

The Crypto User has always been able to create public objects, but when HA mode was in operation, the replication operation would fail, causing the object creation operation to also fail. As of firmware 6.27.0 the HSM does not block cloning operations on objects that the Crypto User role was allowed to create.

[Requires SafeNet Network HSM appliance software version 6.3, and firmware 6.27.0]

External Power Supply for SafeNet Backup HSM and SafeNet USB HSM

The SafeNet Backup HSM and SafeNet USB HSM ship with an external power supply, making the appliance more easily serviceable if it is left unpowered for long periods of time. See the manufacturer's documentation for more information.

Advisory Notes

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

SafeNet Luna Client Installation on Windows Server 2012/2012R2

To successfully install the SafeNet Luna Client on Windows Server 2012/2012R2, you must satisfy the following prerequisites:

- Install .NET framework version 3.5.
- Install the Microsoft Universal C Runtime (Universal CRT) update and its prerequisite Windows updates.

Refer to the *Installation Guide* for a detailed list of the required updates, and their order of installation.



Note: Depending on the update level of your server, some updates may fail. If so, simply install the next update in the list of required updates until all of the updates are installed.

REST API

If you upgrade to 6.3, the REST API Version 4.0 update is also installed on the Network HSM appliance. For more information, refer to the [REST API 4.0 CRN](#) or find it on the Support Portal.

NTLS Keys-in-Hardware Feature is Deprecated

The feature whereby NTLS keys can be stored within the HSM (inside the SafeNet Network HSM appliance) is deprecated and will be officially discontinued in an upcoming release. Any customers using the feature should begin making alternate plans now.

Crypto Command Center

SafeNet Crypto Command Center is a web-based application that provides centralized management and monitoring 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. You can download a trial version of Crypto Command Center at <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 SSH Certificate on First Use

All SafeNet Network HSMs come from the factory with the same SSH 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

We recommend that you update the SafeNet Backup HSM firmware to version 6.10.9. This is the current FIPS-validated HSM firmware version.

Release 6.3 comes with newer firmware version 6.27.0. Upgrading to firmware 6.27.0 increases Backup HSM storage capacity to 32MB.

Use of firmware 6.27.0 with Backup HSM is supported for use with appliance version 6.3 and RBS Client 6.3.

Upgrade to appliance 6.3 is necessary for use with Backup HSM with firmware version 6.27.0.

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 $K1 \neq K2 \neq K3$ (all three keys unique), which is accepted by the HSM when it is in FIPS mode, for non-legacy operations.
 - The second option has $K1 = K3 \neq K2$ (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 Server 2016 Support

Firmware 6.10.9 supports SQL Server 2016 in both FIPS and non-FIPS modes, but firmware 6.27.0 supports SQL Server 2016 only in non-FIPS mode.

Luna SA4 SIM Migration Patch

If you want to migrate a Luna SA4 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 Notes

1. We support SFF backup only on PED-authenticated HSMs, not password-authenticated HSMs.
2. Due to the End of Life announcement for the SafeNet eToken 7300 (as announced at [SafeNet Luna HSM SFF backup no longer available for sale](#)) the Luna Small Form Factor Backup solution is no longer available for sale. Gemalto will continue to support existing Small Form Factor Backup deployments and recommends all other customers use the SafeNet Backup HSM solution.

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 6.3 software and firmware versions.

Upgrade Paths

| Component | Directly from version | To version |
|--|--|----------------|
| SafeNet HSM client software | Any | 6.3 |
| SafeNet Network HSM appliance software | 5.3.5, 5.4.7, 6.0.0, 6.1.0, 6.2.0, 6.2.1 [see Note 1], 6.2.2 | 6.3 |
| 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] | 6.27.0 |
| | 6.0.8 [See Note 3] | 6.2.1 |
| SafeNet Backup HSM firmware | 6.10.9 | 6.27.0 |
| | 6.0.8 [See Note 4] | 6.10.9, 6.27.0 |
| SafeNet Local PED/Remote PED firmware | 2.4.0-3, 2.5.0-3 [see Note 5] | 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 6.27.0. Refer to the earlier upgrade documentation provided by SafeNet Technical Support.]

[NOTE 3: If you are updating from firmware version 6.0.8 and your SafeNet HSM appliance is nearly full of cryptographic objects, you must clear space (up to 15% of the maximum storage) before updating the firmware. Otherwise, the HSM may be left in a bad state.

[NOTE 4: 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.

Use of firmware 6.27.0 with Backup HSM is supported for use with appliance version 6.3 and RBS Client 6.3. Upgrade to appliance 6.3 is necessary for use with Backup HSM with firmware version 6.27.0.]

[NOTE 5: 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.

Firmware 6.10.9 is fully supported by release 6.3 (except for features dependent on newer firmware).

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/140-1/140InProgress.pdf>
- Completed Validations - Vendor List:
<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm>

About Common Criteria

Common Criteria is the most widely recognized, longest running, and most established benchmark for assessing product security available today. The foundation of the certification is a mutually agreed set of 'Common Criteria' recognized by 28 participating nations. Common Criteria provides a robust market independent path to developing independent 3rd party assurance of security and life-cycle claims made by a vendor against a product.

Gemalto is committed to certifying its products in support of our customers compliance and audit requirements, and is pleased to announce that SafeNet Luna HSM versions 5/6 running firmware 6.10.9 is Common Criteria certified to EAL4 augmented with ALC_FLR.2 and AVA_VAN.4

Information concerning the Common Criteria certification for SafeNet Luna HSM version 5/6 can be found on the Common Criteria Portal at the following locations.

- <https://www.commoncriteriaportal.org/products/#DG> (listed under the "products for Digital Signatures section")
- [https://www.commoncriteriaportal.org/files/epfiles/\[CR\]%20NSCIB-CC-38671-CR.pdf](https://www.commoncriteriaportal.org/files/epfiles/[CR]%20NSCIB-CC-38671-CR.pdf) (certification report)
- [https://www.commoncriteriaportal.org/files/epfiles/\[ST\]%20CR-3524_18%20\(Relase%20Version\)%20-%20Security%20Target.pdf](https://www.commoncriteriaportal.org/files/epfiles/[ST]%20CR-3524_18%20(Relase%20Version)%20-%20Security%20Target.pdf) (security target)

Supported Operating Systems

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

SafeNet Luna HSM 6.3.1 Client

The 6.3.1 client is available for 64-bit Linux only. It adds support for the CKM_RSA_PKCS_PSS mechanism to the Java LunaProvider. All other functionality is identical to the 6.3 client.

SafeNet Luna HSM 6.3 Client

To ensure trouble-free installation and operation, it is recommended that you keep your operating system up to date by installing any recommended updates provided by the operating system vendor.



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 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 |

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 |

Note: For ESXi operation, your USB HSM must have bootblock version 1.8. If the bootblock is older, contact your Gemalto Sales Representative to return and exchange or RMA the unit. In Linux systems, the bootblock version appears in system messages. In Windows, you would need to run DebugView.

The version can be discovered in log messages similar to this:



```
Feb 18 22:09:12 localhost kernel: lunauhd0: LOG: Hardware serial number: 3444.6157.152a.8087
Feb 18 22:09:12 localhost kernel: lunauhd0: LOG: Hardware revision 1
Feb 18 22:09:12 localhost kernel: lunauhd0: LOG: Boot block revision G5 1.8
Feb 18 22:09:12 localhost kernel: lunauhd0: LOG: Date: Apr 30 2013
Feb 18 22:09:12 localhost kernel: lunauhd0: LOG: Time: 14:09:47
Feb 18 22:09:12 localhost kernel: lunauhd0: LOG: 64MB FLASH memory
```

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, 20, 35, 50, 75, or 100 partitions)
- 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.



Note: 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 6.3 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 5.3.5 or newer, you can upgrade to version 6.3 to obtain the value of newer features and fixes. See "[The following are summaries of features new to SafeNet HSM in release 6.3.](#)" on page 3 earlier in this document for brief summaries of new features in release 6.3. 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, or 6.2.2 you are recommended to upgrade to release 6.3.

– If HSM firmware is currently at version 6.22.0 or higher, we recommend that you update to firmware version 6.27.0.

– 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 12 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 6.3.

| Component | Version |
|---|-----------------------|
| SafeNet Network HSM and SafeNet PCIe HSM firmware | 6.27.0 * |
| SafeNet Remote Backup HSM firmware | 6.10.9 * or 6.27.0 |
| SafeNet USB HSM firmware | 6.27.0 * |
| 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 6.3 while leaving the HSM firmware at lower firmware versions, but several SafeNet HSM 6.3 features are not supported without the latest firmware. Refer to the list of new features, which indicates which ones are software-only, and which ones

| Component | Version |
|--|---------|
| require firmware 6.27.0. | |
| 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 6.3, 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 6.3 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 6.3 client software
- SafeNet Network HSM 6.3 appliance software
- SafeNet HSM 6.27.0 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 6.3 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 6.3 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 6.3 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 6.3

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 6.3 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 6.3

1. Copy the SafeNet HSM 6.3 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, or 6.2.2, you are recommended to upgrade to release 6.3.

– If HSM firmware is currently at version 6.22.0 or higher, we recommend that you update to firmware version 6.27.0.

– 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 6.27.0 and FIPS 140-2

Firmware 6.24.3 implements some of the features of release 6.3, 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 6.3 software on the appliance, you have the option to also immediately update the firmware to 6.27.0, or to place 6.27.0 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 6.27.0.



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 6.27.0, 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 6.27.0, 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 6.3.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/Chrystoki.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/Chrystoki.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
```

- 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 Description ---> User Token Slot.

For example, for VirtualToken00Members = 155316,155317, the new serial numbers displayed in LunaCM are **155316014** and **155317014**.

- 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;
```

- Next adjust the value of **VirtualToken**<nn>**SN** in a similar manner. In our example, the adjusted value is **1155316014**.
- When you have updated the serial number for all virtual tokens and members, save the file.
- 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.

- 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 |
|-----------|----------|---|
| LUNA-1403 | M | <p>Problem: USB HSM docs incorrectly state that auto-activation is not supported</p> <p>Workaround: Ignore.</p> |
| LUNA-1356 | M | <p>Problem: Luna shell command hsm checkcertificates fails</p> <p>Workaround: For firmware versions 6.22.0 and above, create two partitions and re-run the command. For firmware versions prior to 6.22.0, use the cmu utility to verify the HSM (example: cmu verifyhsm.) Refer to the 6.3 product documentation on cmu usage.</p> |
| LUNA-1274 | M | <p>Problem: PCI driver signature not trusted on Enterprise Servers Win 2008 R2 Gemalto provides drivers signed with SHA-256-based certificate. Without a Windows update, Windows 2008 R2 expects the older SHA-1, and is unable to validate driver software signed with newer mechanisms. "Windows cannot verify the digital signature for the drivers required for this device. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source. [Code 52]"</p> <p>Workaround: See Microsoft Security Advisory 3033929 Availability of SHA-2 Code Signing Support for Windows 7 and Windows Server 2008 R2 https://technet.microsoft.com/en-us/library/security/3033929 and install the appropriate update before installing Luna Client software on Windows 2008 R2 servers.</p> |
| LUNA-1210 | M | <p>Problem: got "LUNA_RET_KCV_PARAMETER_MISSING" error during restore objects from PCM backup to partition of Network HSM key migration</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. backup objects from Luna SA 4 to PCMCIA Luna Backup token FW 4.8.7 2. connect Luna Dock II to Luna SA 5.4.7 with FW 6.10.9 3. set legacydomain on partition of Luna SA 5.4.7 4. restore objects from PCMCIA Luna Backup Token to Luna SA 5.4.7 5. upgrade Luna SA 5.4.7 appliance software to 6.3 6. upgrade FW from version 6.10.9 to version 6.27.0 |
| LUNA-1205 | M | <p>Problem: Can't ping IP outside of subnet though bonding port after upgraded from 6.2.2 to 6.3</p> <p>Workaround: Use port bonding mode 0</p> |
| LUNA-1159 | M | <p>Problem: Clearing HSM tamper shows confusing error if hsm was configured for STC Logging in to clear the tamper mentions Error: 'hsm login' failed. (80000E00 : Unknown ResultCode value) Future hsm login attempts succeed.</p> <p>Workaround: Login again.</p> |
| LUNA-1091 | M | <p>Problem: After upgrading the Luna HSM firmware to version 6.27.0, older versions of LunaCM and CKDEMO (6.2.x) report an incorrect firmware version.</p> <p>Workaround: Upgrade all Luna Client software to the latest 6.3.x version.</p> |
| LUNA-960 | M | <p>Problem: Pedclient disconnect after idling too long, but does not reconnect on next</p> |

| Issue | Severity | Synopsis |
|----------|----------|---|
| | | <p>command..</p> <p>Workaround: If a previously working remote PED connection has stopped, disconnect and then reconnect (ped disconnect followed by ped connect -ip <pedserver ip> . If that fails, try stopping and restarting the pedserver, and then re-issue ped connect.</p> |
| LUNA-958 | M | <p>Problem: Ped client does not connect to ped server on PCI when host is rebooted When client workstation with PCI card(s) is rebooted, starting LunaCm and executing commands that attempt to reconnect with a Pedserver resulted in Command Result : 0x5 (CKR_GENERAL_ERROR)</p> <p>Workaround: Restart the pedclient service.</p> |
| LUNA-827 | M | <p>Problem: libCryptoki library should not call HSM when an application attempts to get length w/ a NULL pointer During key wrapping/unwrapping, calling with a NULL data pointer to get the data length causes the key to be used twice. This causes issues with the key usage count.</p> <p>Workaround: None. The key is called twice and is counted twice - once to get the required buffer size, and once for the wrapping/unwrapping operation.</p> |
| LUNA-817 | M | <p>Problem: cmu selfsigncertificate command fails for SECP256K1 key pair</p> <p>Workaround: none</p> |
| LUNA-812 | M | <p>Problem: Can cause crypto failure in bonding active backup mode by unplugging/plugging eth0 a few times Set bonding mode 1 (active backup). Started symmetric crypto from the client I unplug and plug back in eth0 cable a few times (fairly rapidly), crypto fails on the client</p> <p>Workaround: Use bonding mode 0 (rather than 1, active backup mode)</p> |
| LUNA-801 | M | <p>Problem: On Windows, a system crash can occur when you disconnect a SafeNet Luna Backup HSM from the computer while the PedClient service is running.</p> <p>Workaround: Stop the PedClient service before disconnecting the Backup HSM. From a command line, run pedclient mode stop.</p> |
| LUNA-798 | M | <p>Problem: IPv6: Cannot start pedserver.exe after using IPv6 address with pedserver -m config command</p> <p>Workaround: Start the pedserver with an IPv6 address if you use the alternative command: pedserver -m start -ip 2018:1:2:3:f046:3807:68b7:2afc</p> |
| LUNA-795 | M | <p>Problem: ipv6: lush doesn't display gateway at 'net show' cmd on Network HSM</p> <p>Workaround:get the default gateway from the routing table output</p> <p>For IPv6, the default route it is the destination with "::/0":</p> <pre>Kernel IPv6 routing table Destination Next Hop Flags Metric Ref Use Iface 2018:1:2:3::/64 :: UA 256 0 0 eth1 fe80::/64 :: U 256 0 0 eth1 ::/ fe80::c800:5ff:fedc:8 UGDA 1024 0 0 eth1 ::1/128 :: U 0 0 1 lo ff00::/8 ::</pre> |
| LUNA-792 | M | <p>Problem: "Unknown ResultCode value" on lunash command "partition changepw" on a legacy STC partition</p> |

| Issue | Severity | Synopsis |
|----------------------------------|----------|---|
| | | <p>Steps to reproduce:</p> <ol style="list-style-type: none"> 1. create legacy partition on SA 2. create challenge on the partition, and change password 3. enable policies 22 and 23 4. configure and setup STC connection between client and this partition following doc 5. make sure partition can be seen from client through STC 6. add this partition info a HA group 7. attempt change password, get failure message. <p>Workaround: Perform the password change operation from lunacm on the client, or in LunaSH on the Network HSM appliance, run hsm stc enable and then perform the password change in LunaSH.</p> |
| LUNA-782 LUNA-858 | M | <p>Problem: Windows: vdumpit failing to execute Workaround: Use the 32-bit version of vdumpit, or LunaDiag can be used to dump the dualport contents for Tech Support</p> |
| LUNA-760 | M | <p>Problem:HA log name for rotated log wrong and is missing ".txt" extension The date portion of the filename is not zero-padded and might be difficult to parse or sort. Workaround: Add ".txt" extension to filename. Add zero padding to date portion of the filename</p> |
| LUNA-715 LUNA-850 CPP-1249 | M | <p>Problem:Lunacm: "partition archive backup -slot remote " command does not work Workaround: Use RBS method for Remote Backup.</p> |
| LUNA-675 | H | <p>Problem: "partition rename" fails on SA 6.3 with error "10A0B : LUNA_RET_OPERATION_RESTRICTED" The lunash "partition rename" operation fails if the HSM has ever had a firmware version between versions 6.22.0 and 6.26.4, inclusive. Workaround:</p> <ul style="list-style-type: none"> • If you created any partitions with firmware earlier than 6.22.0 and have not updated, update directly to firmware 6.27.0 (or newer), and rename freely. • Any partitions with firmware from 6.22.0 through 6.26.4, OR any partition created with earlier firmware, where you have since updated to any PSO -capable firmware (from 6.22.0 through 6.26.4), cannot be renamed. Use "hsm factoryReset", then update your HSM firmware to version 6.27.0 and recreate the partitions; you will then be able to rename them at any time. |
| LUNA-664 | M | <p>Problem: warning about "eth0 primary device has no effect" when using round-robin load balancing mode Workaround: cosmetic issue - has no effect on functionality - ignore.</p> |
| LUNA-359 | M | <p>Problem: HA failover does not work when a member partition is deactivated with partition deactivate, resulting in failure of cryptographic operations. Workaround: To safely deactivate a member partition, first use the LunaCM command hagroup removemember to remove the member from the HA group.</p> |

| Issue | Severity | Synopsis |
|----------|----------|--|
| LUNA-132 | M | <p>Problem: When configuring a network device for IPv6 using SLAAC or DHCPv6, the IPv6 address is retrieved, but the name server and search domain are not.</p> <p>Workaround: Configure the name server and search domain manually, using the LunaSH command <code>network dns add {nameserver <IP_address> searchdomain <net_domain>}</code>.</p> |
| LUNA-107 | M | <p>Problem: Remote PED (<code>pedserver -m show</code>) is slow to show</p> <p>The interval from establishing a Remote PED client-server link, until "PedServer -mode show" returns proper, updated output is an arbitrary length of time, ranging from approximately a minute to several minutes.</p> <p>Workaround: wait for the command to complete.</p> |
| LUNA-63 | M | <p>Problem: When using CKDEMO to create objects with Option 98, Sub-option 10: Object Usage Counters set to "selectable", CKDEMO prompts for a CKA_USAGE_LIMIT value during object creation. An incorrect value is then applied to the attribute.</p> <p>Workaround: Leave Sub-option 10: Object Usage Counters set to "disabled". Set the CKA_USAGE_LIMIT attribute for each object after creating it, using Option 25: Set Attribute.</p> |

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-41102 | M | <p>Problem: 6.0:SA6 STC: running multitoken rsasigver on STC causes CKR_STC_SEQUENCE_NUM_INVALID</p> <p>Fixed: Now provide a unique sequence number counter to each thread.</p> |
| LHSM-41070 | M | <p>Problem: Partition Clear failed to delete all objects through LunaCM</p> <p>Fixed: Now clears all objects.</p> |
| LHSM-37195 | M | <p>Problem: One step ntlis: Client gets added twice in the slot list if the deploy runs twice with first time failed.</p> <p>These steps can reproduce the issue:</p> <ol style="list-style-type: none"> 1. Having a valid ntlis connection between the client and server (using hostname) by |

| Issue | Severity | Synopsis |
|------------|----------|--|
| | | <p>running command</p> <pre>ccfg deploy -n serverHostName -c 192.20.15.145 -par P1SA3 -pw 1q@W3e\$R1</pre> <ol style="list-style-type: none"> Go to the server folder (cert/server) and delete the CAFile.pem Now setup the ntlm connection between the client and server again but this time using the ip address. <pre>ccfg deploy -n 192.20.23.133 -c 192.20.15.145 -par P1SA3 -pw 1q@W3e\$R1</pre> <ol style="list-style-type: none"> Now you will see the issue. <p>The root cause of the issue is that there are now two server entries in the Chrystoki.conf file (one using hostname , one using ip address) using the same cert entry in CAFile.pem</p> <p>Workaround: Edit the Chrystoki.conf file (Crystoki.ini in Windows) and delete one server entry.</p> |
| LHSM-25147 | M | <p>Problem: Luna Shell: adding snmp user with special characters in name succeeds, but user is invalid</p> <p>Fixed: This issue has been fixed in this release.</p> |

Support Contacts

| Contact method | Contact | |
|--|---|------------------|
| Phone (Subject to change. An up-to-date list is maintained on the Technical Support Customer Portal) | Global | +1 410-931-7520 |
| | Australia | 1800.020.183 |
| | 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 | https://safenet.gemalto.com | |
| Customer Support Portal | https://supportportal.gemalto.com Existing customers with a Gemalto Customer Support Portal account can log in to manage incidents, get the latest software upgrades, and access the Knowledge Base. | |