THALES

gemalto
a Thales company

SafeNet Luna Network HSM 7.2

CUSTOMER RELEASE NOTES

Issue Date: 20 June 2019

Document Part Number: 007-013580-004 Rev. C

The most up-to-date version of this document is posted to the Technical Support Customer Portal at https://supportportal.gemalto.com

Contents

Product Description

The SafeNet Luna Network HSM secures your sensitive data and critical applications by storing, protecting and managing your cryptographic keys in a high-assurance, tamper-resistant, network-attached appliance that offers market-leading performance. The SafeNet Luna Network HSM meets compliance and audit needs for FIPS 140, HIPAA, PCI-DSS, eIDAS, GDPR, and others, in highly-regulated industries including Financial, Healthcare, and Government.

The SafeNet Luna Network HSM offers up to 100 HSM partitions, high-availability configuration options, remote management, PED, backup, and dual hot-swappable power supplies.

Release Description

SafeNet Luna Network HSM 7.2 is a field update release of Gemalto's 7.x SafeNet Luna Network HSM. It includes Client software with drivers and tools, appliance software update, and new firmware for the HSM.

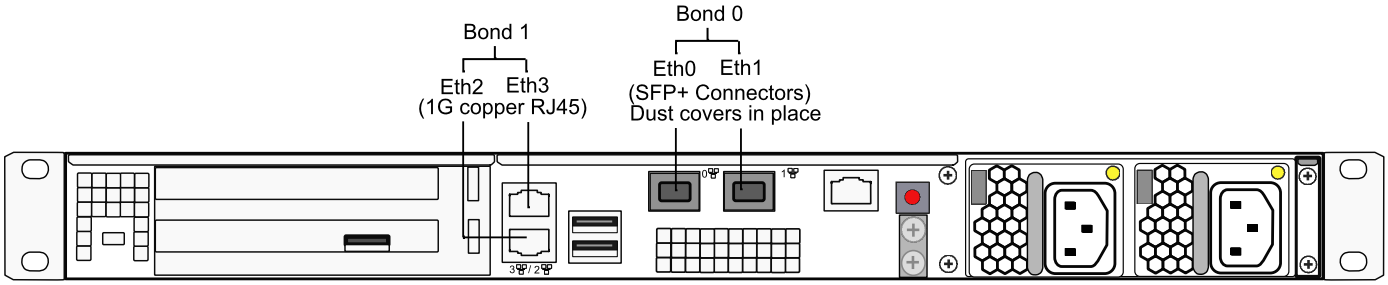
SafeNet Luna Network HSM 7.2 is a factory release of Gemalto's 7.x SafeNet Luna Network HSM. It includes 10Gbps Optical Ethernet hardware and appliance software.

Important Notices for SafeNet Luna Network HSM 7.2 Optical Ethernet Release

Gemalto is pleased to announce the availability of the 10 Gbps optical NIC SafeNet Luna Network HSM. This product variant provides two 10G optical network interfaces and two 1G copper network interfaces, as opposed to the standard 1G model which provides four 1G copper network interfaces.

The 10G SafeNet Luna Network HSM provides two 10G SFP optical Ethernet network interfaces (labeled 0 and 1), and two 1G copper RJ45 network interfaces (labeled 2 and 3), as illustrated below. You can optionally bond eth0 and eth1 to bond0, or eth2 and eth3 to bond1, to provide a redundant active/standby virtual interface.

The 10G model is functionally equivalent to the standard 1G model, except on the following five points:



- Two of the Ethernet ports (see the middle, upper portion of the diagram, just above the ventilation grid) have 10Gbps Optical Ethernet SFP+ connectors, while the two Ethernet ports (stacked vertically beside the HSM slot) retain 1Gbps copper RJ-45 sockets.
- The small form-factor pluggable (SFP) transceiver modules are packed in their own independent packaging to avoid possible damage and dust during shipping and handling, and those must be inserted into the SFP+ connectors on the appliance during appliance installation. (See the Installation Guide in the main product documentation)
- The logical Ethernet port assignments are different from the standard appliance, such that the 10Gbps optical ports are designated Eth0 and Eth1, while the 1Gbps copper ports are designated Eth2 and Eth3.
- The output of the Luna Shell (lunash:>) command **network show -verbose** displays "FIBRE" and the 10000baseT/Full option, when the appliance has optical Ethernet ports.
- Port bonding is allowed only between Ethernet ports of the same type and speed.

Appliance Software Updates

The 10G SafeNet Luna Network HSM model ships with Luna 7.2 appliance software and Luna 7.0.3 HSM firmware installed. You can use the 10G optical ethernet ports with the installed software, or update to Luna 7.4 or higher.

> **CAUTION! Do not update the 10G appliance to Luna 7.3.x.**
>
> The port mapping will revert to the 1G configuration and you will lose 10G support. The appliance might require RMA to fix the port mapping.

The notices below apply to either hardware version.

Important Notices for SafeNet Luna Network HSM 7.2 Release

Please consider the following important information before updating to this release.

SafeNet Luna Network HSM 7.2 Update Packages

Note that there are TWO (2) separate update packages available on the Gemalto Customer Support Portal for the SafeNet Luna Network HSM 7.2 release:

- SafeNet Luna Network HSM 7.2 appliance software, with update to firmware **7.2.0**

  Select this update if you do NOT require FIPS-validated firmware and/or require the bug fixes from the newer version.
- SafeNet Luna Network HSM 7.2 appliance software, with update to firmware **7.0.3**

Select this update if you DO require FIPS-validated firmware; firmware 7.0.3 is Gemalto's newest FIPS-validated version for Luna 7 HSMs.

> **NOTE** If you require firmware 7.0.3, you MUST upgrade your appliance to software version 7.2. Refer to the following sections for more information:
>
> > "Valid Update Paths" on page 9
> > "Recommended Minimum Versions" on page 10
> > "Special Instructions for Installing Firmware 7.0.3 if Your Current Firmware Version is 7.1.0" on page 10

Check that you have downloaded the appropriate package for your use case before proceeding with the update.

Resolved Issue LKX-3338

Gemalto has identified an issue with asymmetric digest-and-sign, or digest-and-verify mechanisms when the data length exceeds 64KB, for all SHAxxx_RSA_xxx, SHAxxx_DSA and SHAxxx_ECDSA mechanisms.

Please note:

- Simple (i.e. not combined with digest) RSA/ECDSA/DSA sign/verify operations are NOT affected, and work as expected for all HSM models.
- This issue only affects HSMs with standard- and enterprise-level performance (*700 and *750 models). Maximum-performance (*790) models are not affected.

This issue is resolved in both firmware 7.2.0 and 7.0.3.

Gemalto strongly recommends that you update to firmware 7.2.0 or firmware 7.0.3 to avoid this issue in the future.

New Features and Enhancements

SafeNet Luna Network HSM 7.2 introduces the following new features and enhancements:

Improved Luna HSM Client

Release 7.2 adds improvements to the Luna HSM Client software:

- **Enhanced Version Compatibility for Luna HSM Client** — Version 7.2 and newer Luna HSM Client can be used with HSMs running Luna 6.2.1 or higher, or any Luna 7 version, without conflict. Luna HSM Client 7.2 and newer versions can coexist in large deployments. You can schedule client roll-outs at your convenience, without need to match versions across your organization. Future HSM features that do not have client-version dependencies will function without issue. See also "Supported Operating Systems" on page 8.
- **Mixed-Version HA Groups** — HA groups containing both SafeNet Luna Network HSM 6 and 7 partitions are now supported using SafeNet Luna HSM Client 7.2 or newer. This mixed-version configuration is useful for migrating keys to a new SafeNet Luna Network HSM 7, or to gradually upgrade your production environment from Luna 6 to Luna 7.
- **Improved Client Installer with User-Defined Install Paths (Windows)** — Luna HSM Client can be installed at user-selected locations (file paths with sufficient space), and installed Client software can be modified without uninstalling and reinstalling.

- **User-Defined Client Install Paths (Linux)** — Linux root-level users can install the Luna HSM Client software to an installation directory of their choice.
- **Minimal Client (Linux)** — The SafeNet Luna Minimal Client for Linux provides only the files needed to use an application with a partition on a SafeNet Luna Network HSM for deployment in Docker containers and similar microservice environments. The Luna Minimal Client can be installed on a workstation without root access.

Configurable Cipher Suites

You can now configure the TLS cipher suites used by NTLS, STC, and PEDserver on the SafeNet Luna Network HSM. This new capability allows administrators to select and configure cipher strength to meet their internal security objectives and compliance requirements.

The cipher suites are configured using the new **sysconf tls cipher** LunaSH commands. The available set of ciphers is displayed in default order. Users can choose which ciphers from the set to use, as well as the order of preference for TLS cipher-suite negotiation. The modified cipher list and order can also be exported as a template; the template can then be used to configure TLS cipher suites on multiple HSMs.

Customizable System Logging

You can now customize local and remote system logging according to message severity. There is no limit on the number of remote logging servers you can add, and you can configure the severity level for each server and log type independently. For example, you could send all log entries produced by the appliance to one remote server, and only entries marked **critical** or higher to another. Storing only the most severe (infrequent) entries locally on the appliance can prevent the syslog directory from filling up over time.

Rename/Relabel Partitions

The HSM SO can now change the name assigned to a partition on creation. This does not affect the label set by the Partition SO during initialization and is only visible in LunaSH. This allows partitions to be created ahead of time and renamed to something more suitable later, when they are allocated for a particular purpose (Requires firmware 7.2.0).

The Partition SO can now change the label of an initialized partition (Requires firmware 7.2.0).

Initialize the Orange RPV Key Remotely

You can now initialize the Remote PED Vector (orange key) using a Luna PED connected to a remote workstation running PEDserver. A one-time numeric password is used to authenticate the Remote PED to the HSM before initializing the RPV. This optional method is useful if the HSM SO only has remote SSH access to the appliance. The HSM must be in a zeroized state (uninitialized), for security. Your firewall settings must allow an HSM-initiated Remote PED connection (Requires firmware 7.2.0).

Crypto User Can Clone Public Objects

The Crypto User (CU) role has always been able to create public objects, but not clone them. In HA mode, this would cause the replication and subsequent object creation operations to fail. Firmware 7.2.0 allows the CU to clone public objects, and therefore to perform operations on HA groups without Crypto Officer authentication (Requires firmware 7.2.0).

Auto-Enabled HA Logging

Luna HSM Client now automatically enables HA logging, either when you create the first HA group, or when you update the Luna HSM Client to 7.2 and it detects a previously-configured HA group. If you manually turn HA logging off, logging is not auto-enabled for new HA groups.

SCP03 Encoding

The SCP03 encoding scheme, as defined in NIST SP 800-108, is now supported for Global Platform.

REST API 6.0

REST API 6.0 is included with the SafeNet Luna Network HSM7.2 release. Customers who update their appliance software to version 7.2 will automatically receive the REST API 6.0 update. REST API 6.0 contains the following new features:

- **Appliance Upgrade Management** — Manage Gemalto Licensing Portal partition upgrade packs using REST API.
- **Package and Firmware Update Management** — Update, verify, list, and delete secure packages with REST API, including firmware updates.
- **Multi-Part Upload Requests** — Upgrade your HSMs via a single REST API call, improving performance and efficiency.
- **Configurable REST API Users and Roles** — Manage REST API users and roles (add, remove, modify, show, list) using REST API.
- **Configurable REST API Access Control List** -- Modify role access using REST API, by importing and exporting lists of available resources.

Fixes

Issues addressed in this release are listed in "Resolved Issues" on page 18.

Advisory Notes

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

PED Upgrade Required for Currently-Owned PEDs

If you have older PEDs that you intend to use with SafeNet Luna HSM 7.0 or later, you must upgrade to firmware 2.7.1 (or newer). The upgrade and accompanying documentation (007-012337-003_PED_upgrade_2-7-1-5.pdf) are available from the Gemalto Support Portal.

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 enables the PED to be USB-powered; 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 model number on the manufacturer's label identifies the refreshed PED: PED-06-0001.

To use the new USB-powered PED

1. Ensure the SafeNet Luna HSM Client software is installed on the Windows computer that will provide PED authentication for your SafeNet Luna Network HSM. Installing the Remote PED component of the SafeNet Luna HSM client installs the required driver.
2. Connect the PED to the computer where you installed the Remote PED component of the SafeNet Luna HSM client using the USB micro connector on the PED and a USB socket on your computer.
3. 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 listed below:

   BOOT V.1.1.0-1

   CORE V.3.0.0-1

   Loading PED...

   Entering...
4. After the boot process is complete, the PED displays **Local PED mode** and the **Awaiting command...** prompt. Your new PED is now ready for use.
5. To enter Remote PED mode, if needed, exit Local PED mode with the "<" key, and from the **Select Mode** menu, select option **7 Remote PED**.

STC over IPv6 is Unavailable

STC client-partition links are not available over an IPv6 network.

Remote Backup Over IPv6 is Unavailable

Network connections from the SafeNet Luna HSM Client to a Remote Backup Server must use IPv4.

> **NOTE** Network connections, from the client to the HSMs you want to backup using RBS, can use IPv6. Only the connection from the client to the RBS server requires IPv4.

HSM Logs Sent to Messages Log

The **hsm.log** file has been removed from Luna 7. The HSM logs are now sent to the **messages** log.

> **NOTE** Although it is ignored, the **hsm** option appears in the syntax for some **syslog** commands (such as **syslog tail -logfiles**).

Supported Operating Systems

This section lists the supported software, hardware, and optional upgrades for the HSM.

SafeNet Luna HSM Client

You can install the SafeNet Luna HSM Client 7.2 on the following operating systems:

Operating System	Version	64-bit applications on 64-bit OS	32-bit applications on 64-bit OS	32-bit applications on 32-bit OS
Windows	10	Yes	Yes	No
	2012 R2	Yes	Yes	No
	2016	Yes	Yes	No
Redhat-based Linux (including variants like CentOS and Oracle Enterprise Linux)	6	Yes	Yes	Yes
	7	Yes	Yes	Yes
AIX *	7.1	Yes	Yes	No
Solaris (SPARC/x86) *	11	Yes	Yes	No
Ubuntu **	14.04	Yes	No	Yes

* Although the AIX and Solaris installers display the options, SafeNet Luna PCIe and USB HSMs are not supported in this release. Select only **SafeNet Luna Network HSM** during installation.

** The Linux installer for Luna HSM Client software is compiled as .rpm packages. To install on a Debian-based distribution, such as Ubuntu, **alien** is used to convert the packages. We used **build-essential**:

apt-get install build-essential alien

If you are using a Docker container or another such microservice to install the Luna Minimal Client on Ubuntu, and your initial client installation was on another supported Linux distribution as listed above, you do not require **alien**. Refer to the product documentation for instructions. You might need to account for your particular system and any pre-existing dependencies for your other applications.

Remote PEDserver

The PEDserver software is included with the SafeNet Luna HSM Client software. You must install the SafeNet Luna HSM Client, with the PEDserver option, on each workstation used to host a remote PED. The PEDserver software is supported on the following operating systems:

- Windows 10 (64-bit)
- Windows 2016
- Windows 2012 R2

Supported Cryptographic APIs

Applications can perform cryptographic operations using the following APIs:

- PKCS#11 2.20
- Java 7/8/9
- OpenSSL
- Microsoft CAPI
- Microsoft CNG

Update Considerations and Procedures

Detailed procedures for installing the SafeNet Luna Network HSM7.2 software and firmware updates can be found in the product documentation. Before you install any of the updates, consider the following guidelines:

- If it applies to you, refer to "Special Instructions for Installing Firmware 7.0.3 if Your Current Firmware Version is 7.1.0" on the next page.
- Back up all important cryptographic material. Refer to the product documentation for backup procedures.
- Stop all client applications running cryptographic operations on the HSM.
- If you are using STC on the HSM Admin channel, disable it by running lunash:> **hsm stc disable** before you update the HSM firmware.
- Use an uninterruptible power supply (UPS) to power your HSM. There is a small chance that a power failure during an update could leave your HSM in an unrecoverable condition.

Valid Update Paths

The following table provides tested paths for updating to the current software/firmware versions.

Component	Directly from version	To version
SafeNet Luna HSM Client software	Any	7.2
SafeNet Luna Network HSM appliance software	7.0, 7.1	7.2
SafeNet Luna HSM firmware	7.0.1, 7.0.2, 7.0.3, 7.1.0	7.2.0
	7.0.1, 7.0.2	7.0.3 (FIPS-certified)
SafeNet Backup HSM firmware	6.10.9, 6.26.0	6.27.0
SafeNet Luna PED firmware	2.7.1	N/A
	2.8.0	N/A

FIPS-Validated Firmware Versions

The following firmware versions are all FIPS 140-2, overall level 3, certified per certificate #3205 (https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3205):

- Luna firmware v. 7.0.3 (recommended)
- Luna firmware v. 7.0.2 (see F5 note, below)
- Luna firmware v. 7.0.1

For details on the scope of the FIPS certificate and applicable configurations, please refer to the product Security Policy posted alongside the certificate at the link above.

Recommended Minimum Versions

Generally, Gemalto recommends that you always keep your HSM firmware, appliance software, and client software up to date, to benefit from the latest SafeNet features and bug fixes. If regular updates are not possible or convenient, the following table lists the recommended minimum firmware and software versions for use with SafeNet Luna 7 HSMs. If you are running an earlier version, Gemalto advises upgrading to the version(s) below (or later) to ensure that you have critical bug fixes and security updates.

	Luna HSM Client	Appliance Software	Luna HSM Firmware
SafeNet Luna Network HSM 7 Minimum Recommended Configuration	7.2	7.2	7.2.0
			7.0.3

> **NOTE** Customers who wish to use Luna 7 HSMs with F5 Network BIG-IP 13.1 appliances should follow F5 guidelines for Supported SafeNet client and HSM versions (https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-safenet-hsm-version-interoperability-matrix.html). At the time of this release, F5's supported versions for Luna 7 are Luna HSM Client 7.1 with appliance software 7.1 and firmware 7.0.2.

Special Instructions for Installing Firmware 7.0.3 if Your Current Firmware Version is 7.1.0

Firmware 7.0.3 is Gemalto's latest FIPS-certified Luna firmware. If you are using firmware 7.0.1 or 7.0.2, you can proceed with the standard update procedure. If you previously updated to firmware 7.1.0, and you wish to use firmware 7.0.3, follow this procedure to ensure a successful update.

SafeNet Luna Network HSM does not allow you to update the firmware from a higher-numbered to a lower-numbered version. Therefore, if you are currently running firmware 7.1.0, you must first perform a firmware rollback.

> **CAUTION!** Firmware rollback is destructive; earlier firmware versions might have older mechanisms and security vulnerabilities that a new version does not. Back up any important materials before rolling back the firmware. This procedure zeroizes the HSM and all cryptographic objects are erased.
>
> If you are using STC, or have ever enabled HSM policy 39, you may encounter a known issue (see "LKX-3184" on the next page). If this is the case, do not roll back the HSM firmware.

To install firmware 7.0.3 on an HSM running firmware 7.1.0:

1. Check the previous firmware version that is available on the HSM. The firmware available for rollback must be 7.0.1 or 7.0.2.

   lunash:>**hsm firmware show**
2. Back up any important cryptographic objects currently stored on the HSM.
3. Log in as HSM SO.

   lunash:>**hsm login**
4. Perform a firmware rollback.

   lunash:>**hsm firmware rollback**
5. Initialize the HSM and log in as HSM SO.
6. Install the SafeNet Luna Network HSM 7.2 update that includes firmware 7.0.3, as described in the product documentation.
7. Update the firmware to version 7.0.3, which is now stored on the appliance.

   lunash:>**hsm firmware upgrade**
8. Recreate your application partition(s) and restore the contents from backup.

Known Issues

This section lists the issues known to exist in the product at the time of release. Workarounds are provided where available. The following table defines the severity level assigned to each listed issue.

Table 1: Issue severity definitions

Severity	Classification	Definition
H	High	Reasonable workaround exists.
M	Medium	Medium severity problems.
L	Low	Low severity problems.

Table 2: List of known issues in release 7.2

Issue	Severity	Synopsis
LKX-3184	M	**Applies to firmware 7.0.3 only. This issue has been fixed in firmware 7.2.0.** **Problem**: If HSM policy 39: Enable Secure Trusted Channel has been set to **1** (ON) at any time, attempting a firmware rollback will cause the HSM to fail with an error (Unable to communicate with HSM). **Workaround:** None. If you are using STC, or have enabled HSM policy 39 in the past, do not roll back the HSM firmware.

Issue	Severity	Synopsis
LUNA-8620	H	**Problem:** NTLS failover on 10G optical ports (bond0) sometimes fails. **Workaround:** None. Troubleshooting: Luna Network HSM supports active-backup bonding mode only. This mode does not require any specific configuration of the switch. If this problem (Bond0 failover unsuccessful) is encountered, we recommend to: 1. Trace the packet in the network to ensure that the network interface in the Luna Network HSM is discovered properly. 2. Ensure that ARP entry is not incorrectly cached in the network. Such problem could be resolved through manual ping-out from the appliance (**network ping** command). To execute such command, the operator must directly connect to the Luna Network HSM through the serial port.
LUNA-3554	M	**Problem:**The appliance remains disconnected from the network, even though the appliance itself is back online and fully functional. **Workaround:** Reboot the appliance.
LUNA-3429	M	**Problem:**'Error: pedClient is not currently running' error is displayed when trying to connect with a ped server using 'hsm ped connect' command, even though the cbs service is shown to be running. **Workaround:** Restart the cbs service on the appliance.
LUNA-3423	M	**Problem:** A failed C_WrapKey call on an STC partition configured for Cloning returns the error CKR_BUFFER_TOO_SMALL, while the same failure on an NTLS Cloning partition returns the error CKR_KEY_NOT_WRAPPABLE. **Workaround:** If you are checking logs for one of these exact errors, ensure that you search for the error associated with your connection type.
LUNA-3422	M	**Problem:** A failed C_WrapKey call on an STC partition configured for Key Export returns the error CKR_BUFFER_TOO_SMALL, while the same failure on an NTLS Cloning partition returns the error CKR_MECHANISM_INVALID. **Workaround:** If you are checking logs for one of these exact errors, ensure that you search for the error associated with your connection type.
LUNA-3421	M	**Problem:** A C_CloseAllSessions call on an STC partition configured for Key Export returns CKR_UNKNOWN, while the same call on an NTLS Key Export partition returns CKR_OK. **Workaround:** None.
LUNA-3416	M	**Problem:** When performing AES encryption on an HA group using AIX and SPARC clients, failover occasionally fails with an error (CKR_TOKEN_NOT_PRESENT). **Workaround:** None.
LUNA-3414	M	**Problem:** One-step Network Trust Link (NTLS) setup fails on Windows with error code CKR_CANCEL when SO Login Enforcement is enabled. **Workaround:** Use the multi-step NTLS setup procedure to create a connection to the SafeNet Luna Network HSM appliance.

Issue	Severity	Synopsis
LUNA-3364	M	**Problem:**After running **sysconf appliance reboot** from LunaSH, the appliance occasionally gets stuck with a "Rebooting" message on the LCD screen. **Workaround:** Remove all power from the appliance (by removing the cable from the power supply units), then reconnect power and restart the appliance.
LUNA-3343	M	**Problem:** When using STC in a high traffic or high multi-threaded application scenario, the error CKR_STC_RESPONSE_REPLAYED is occasionally generated and causes subsequent commands to fail. **Workaround:** Restart the client application, and the error will clear.
LUNA-3307	M	**Problem:** In LunaCM, **clientconfig deploy** (one-step NTLS) fails if the partition name contains spaces. **Workaround:** Use the multi-step NTLS connection procedure to assign the partition to the client.
LUNA-3298	M	**Problem:** When installing Backup HSM and/or PED drivers from Luna HSM Client software on a host machine with a fresh, non-upgraded version of Windows 10, Windows reports an error with the driver signatures. **Workaround:**Download and install Luna client patch 7.2.1 from the Gemalto Customer Support Portal (DOW0003077). Alternatively, disable Windows 10 driver signature enforcement before installing the Luna HSM Client.
LUNA-3108	M	**Problem:** If you uninstall Luna HSM Client and reinstall it in a custom directory, HA logging stops working. **Workaround:** Open **crystoki.conf**/**crystoki.ini** and edit `haLogPath =` to match the new client path.
LUNA-3107	M	**Problem:** If you uninstall Luna HSM Client and reinstall it in a custom directory, RBS stops working. **Workaround:** Copy the two certificate files **serverkey.pem** and **server.pem** from the original **rbs** directory to the new **rbs** directory.
LUNA-3071	M	**Problem:** When LunaCM is launched in Luna Minimal Client, an unexpected error is displayed (Error: Failed to initialize remote PED support). **Workaround:** Edit Chrystoki.conf/crystoki.ini and remove **Toolsdir** form the **Misc** section.
LUNA-3070	M	**Problem:vtl cklog enable**/**disable** command not working if LibUNIX and LibUNIX64 are in different folders. **Workaround:** Enable **cklog** manually by editing Chrystoki.conf/Chystoki.ini. Refer to the *SDK Reference Guide* for details.

Issue	Severity	Synopsis
LUNA-2983	M	**Problem:** CMU Export Public Key - Incorrect formatting of exported key. A public key, exported with command **cmu export -handle** <handle#> **-outputfile** <filename> **-key** has incorrect header and footer text. **Workaround:** Edit the exported public key file, replacing `----- BEGIN CERTIFICATE -----` and `----- END CERTIFICATE -----` with `----- BEGIN PUBLIC KEY -----` and `----- END PUBLIC KEY -----` respectively.
LUNA-2646	M	**Problem:** One-step NTLS can fail after installing, uninstalling, and reinstalling the Luna HSM Client on Windows. **Workaround:** Use the multi-step NTLS setup procedure to create a connection to the SafeNet Luna Network HSM appliance.
LUNA-2445	M	**Problem:** The default maximum length for HA log files is incorrectly set to 40000 bytes, and misreported in LunaCM as 262144 bytes (the intended minimum). This can lead to many small HA log files being rotated frequently. **Workaround:** Manually set the HA log maximum file size using lunacm:>**hagroup halog -maxlength** <bytes> the first time you configure HA logging.
LUNA-2007	M	**Problem:** Unable to establish NTLS connection using the one-step NTLS procedure on Solaris x86 when there are more partitions(10~15). **Workaround:** Use the multi-step NTLS connection procedure on a Solaris client.
RAPI-1211	M	**Problem:** In REST API, **GET /api/lunasa/hsms** may return an empty list. **Workaround:** Another attempt may return a populated list if an HSM is available.
RAPI-383	M	**Problem:** REST API does not verify the NTLS client's IP against the certificate. **Workaround:** None.
LUNA-3126	L	**Problem:** After running lunash:> **hsm ped connect** on an uninitialized SafeNet Luna Network HSM, **hsm ped show** may incorrectly display `Number of Connected PED Server : 0`. **Workaround:** None necessary; this behavior does not affect the functioning of Remote PED.
RAPI-1248	L	**Problem:** REST API web client shows wrong logout result. **Workaround:** Use the Custom I/O to manually log out.
RAPI-1096	L	**Problem:** After modifying the webserver settings the **apiversion** under **/api/lunasa** becomes 0. **Workaround:** Restart the webserver service.
RAPI-1062	L	**Problem:** In REST API, **POST /auth/logout** does not return Access-Control-Allow-Credentials and Access-Control-Allow-Origin in the response headers. **Workaround:** None.

Issue	Severity	Synopsis
RAPI-1027	L	**Problem:** REST API partition actions contain actions that should be deprecated. **Workaround:** Do not call these resources.
CPP-3326 RAPI-1416	L	**Problem:** Webserver starts even if no SSL key/cert exists, but is not accessible. **Workaround:** Generate the SSL key/cert before starting the webserver.

Table 3: List of known issues from prior releases

Issue	Severity	Synopsis
LKX-2634	M	**Problem:** Cannot back up curve25519 key types to the SafeNet Luna Backup HSM. **Workaround:** Use cloning or HA to back up your curve25519 key types to another SafeNet Luna 7.0 HSM.
LUNA-2261	M	**Problem:** "CKR_DATA_INVALID" on wrap/unwrap with **multitoken** on AIX and Solaris clients. **Workaround:** None.
LUNA-2252	M	**Problem:** Invalid options are displayed on Solaris installer. **Workaround:** Only the SafeNet Luna Network HSM is supported for Solaris; drivers for the PCIe HSM and USB HSM options are not provided at this time. If multiple options appear when installing Luna HSM Client on Solaris, choose Network HSM only.
LUNA-2224	M	**Problem:** When you initialize an STC partition by applying a partition policy template, a confusing error (CKR_TOKEN_NOT_PRESENT) is returned. **Workaround:** None.
LUNA-2199	M	**Problem:** LunaCM occasionally freezes in Windows 2016 when a new slot is created or deleted. **Workaround:** End the LunaCM instance with Task Manager and restart LunaCM.
LUNA-1927	M	**Problem:** Unable to add new member to HA group after removing primary member. **Workaround:** Manually delete the serial number of the deleted Network HSM's partition from the "VirtualToken00Members" field in the "Chrystoki.conf" (Linux/UNIX) file or "Crystoki.ini" (Windows) file and then add the new partition to the existing HA group. It is added successfully, and the old entry from the lunacm HA list is also removed.
LUNA-1725	M	**Problem:** In LunaCM, **partition archive restore -replace** does not replace DUPLICATED objects in target partition. **Workaround:** Remove all duplicate objects from the target partition prior to running **partition archive restore -replace**.
LUNA-1592	M	**Problem:** When trying to run the **HALogin.java** script, a CKR_UNKNOWN error is returned. **Workaround:** None. Do not use the **HALogin.java** sample.

Issue	Severity	Synopsis
CPP-3261	M	**Problem:** After performing **sysconf config factoryreset**, the appliance host name is not reset. **Workaround:** None.
CPP-3241	M	**Problem:** Untarred audit log files are not visible to the user. **Workaround:** Untarred audit log files will not appear in the list of log files generated by the LunaSH command **my file list**, but they can still be verified using **audit log verify -file** <filename> **-serialsource** <serialnum>.
CPP-3191	M	**Problem:** After rebooting the appliance, occasionally clients cannot see partitions on the first connection attempt. **Workaround:** Run the **vtl verify** command again. The second attempt should be successful.
CPP-2954 LUNA-3352	M	**Problem:** The hsmCriticalEvent and hsmNonCriticalEvent counters incorrectly track HSM events. **Workaround:** None. SNMP hsmCriticalEvent and hsmNonCriticalEvent counters are not implemented in this release and will always remain 0.
CPP-2505 LUNA-132	M	**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. **Workaround:** Configure the name server and search domain manually, using the LunaSH command **network dns add** {**-nameserver** <IP_address> | **-searchdomain** <net_ domain>}.
CPP-2368	M	**Problem:** The **hagroup list** command returns an error. **Workaround:** Run the **hagroup list** command again. The second attempt should be successful.
CPP-1339	M	**Problem:** In LunaSH, **sysconf config restore** does not restore the SSH password for the admin user. If the password is not reset immediately, the admin user will be unable to log in to the appliance in subsequent SSH sessions. **Workaround:** Use **sysconf config clear** to reset the admin password to the default. You must do this in the same session that you used to run the **sysconf config restore** command.
CPP-626 CPP-624	M	**Problem:** If you zeroize an HSM hosting an HA group member partition, all running cryptographic operations against the HA group fail. **Workaround:** Remove any member partition from the HA group before zeroizing the host HSM.
LUNA-2347	L	**Problem:** Deprecated `PartitionPolicyTemplatePath` entry is present in the **MISC** section of **Chrystoki.conf**/**crystoki.ini**. **Workaround:** Ignore. This entry is not used by Luna 7 policy templates.

Issue	Severity	Synopsis
LUNA-2103	L	**Problem:** If you enter duplicate policies (policies with the same ID) in the partition policy template, the partition will take the last value. **Workaround:** Avoid duplicate policy IDs in partition policy template files.
LUNA-2022	L	**Problem:** Incorrect warning displayed when changing ssh restriction to bond slave device. Message displayed is "Warning: SSH is already restricted to the specified ip address / ethernet card. No changes made." **Workaround:** None. You cannot bind SSH to a bond slave.
LUNA-2015	L	**Problem:** Default ntlsOperStatus for SNMP is incorrectly set to **0** (correct value: **3**). This can lead to errors in applications that adhere to syntax strictly. **Workaround:** None.
LUNA-339	L	**Problem:** Some appliance sensor information is missing or incorrectly reported via SNMP. **Workaround:** Use the LunaSH command **status sensors** to obtain this information.
LUNA-218	L	**Problem:** You cannot add a host or network route using the LunaSH **network route add** command without including the gateway value. **Workaround:** None.
CPP-3404	L	**Problem:** CMU may crash or report a memory allocation error when using a non-FIPS signing mechanism in FIPS mode. **Workaround:** Specify a FIPS-approved signing mechanism such as **sha256withRSA**.
CPP-3384 LUNA-1585	L	**Problem:** After zeroization or factory reset, the STC cipher option is set to NULL_ENC. Output from **hsm stc status** includes "Cipher Name: No Cipher". **Workaround:** Run the LunaSH command **hsm stc cipher enable -all** to enable all available STC ciphers.
CPP-3235	L	**Problem:** In LunaCM, the **partition clone** command fails the first time if the Partition SO is logged in to the target slot. **Workaround:** Run the **partition clone** command again. The second attempt should be successful.
CPP-2960	L	**Problem:** LunaCM hangs on exit on Windows 2016. **Workaround:** End the LunaCM instance using the Task Manager.
CPP-2925	L	**Problem:** When the **cklog** library is configured, an **error.txt** file containing extraneous messages may be created. **Workaround:** None.
CPP-2380	L	**Problem:** When running the **MiscCSRCertificateDemo.java** sample, a null pointer exception occurs. **Workaround:** None.

Issue	Severity	Synopsis
CPP-1249 LUNA-1681	L	**Problem:** Remote backup through TCP/IP via the LunaCM command **partition archive backup -slot remote -hostname** <hostname> **-port** <portnum> is not recognized. **Workaround:** Use RBS to backup partitions remotely.
CPP-932	L	**Problem**: If the configured audit logging directory is not found, the **PEDclient** service fails with error **LOGGER_init failed**. **Workaround**: Ensure that the directory you configure for audit logging exists.

Resolved Issues

This section lists issues that have been resolved for the current release.

Table 4: List of resolved issues

Issue	Severity	Synopsis
LKX-3338	H	**Problem:** On Luna HSM *700 and *750 models, asymmetric digest-and-sign or digest-and-verify mechanisms produce the wrong result when the data length exceeds 64 kB. **Fixed:** Fixed in firmware 7.2.0 and 7.0.3.
LKX-3233 LKX-3201	H	**Problem:** Value for HSM policy 46 (Disable Decommission) cannot be changed. Attempting to change it returns an error (CKR_CONFIG_FAILS_DEPENDENCIES). **Fixed:** Fixed in firmware 7.2.0.
LUNA-3015	H	**Problem:** Appliance command **sysconf config factoryReset** does not remove port bonding. **Fixed:** Fixed in release 7.2.
LUNA-2663	H	**Problem:** In LunaSH, **hsm firmware upgrade** fails with errors (LUNA_RET_ UNKNOWN_COMMAND and RC_GENERAL_ERROR) if STC is enabled on the Admin channel. It is then necessary to decommission the HSM in order to upgrade the firmware. **Fixed:** Fixed in release 7.2.
LUNA-2230	H	**Problem:** If HSM policy 39 (Allow Secure Trusted Channel) is turned off while STC is enabled on the admin channel, the HSM SO is unable to log in using **hsm login**. **Fixed:** Fixed in release 7.2.
LKX-3184	M	**Problem**: If HSM policy 39: Enable Secure Trusted Channel has been set to **1** (ON) at any time, attempting a firmware rollback will cause the HSM to fail with an error (Unable to communicate with HSM.) **Fixed:** Fixed in firmware 7.2.0. However, this issue still exists in firmware 7.0.3. See .
LUNA-2947	M	**Problem:** When using SafeNet Luna Network HSM appliance software 7.2 with earlier SafeNet Luna HSM Client software, **cmu getpkc** fails with an error ("Could not retrieve the PKC"). **Fixed:** Fixed in Luna HSM Client 7.2.

Issue	Severity	Synopsis
LUNA-2677	M	**Problem:** Unable to change CKA_EXTRACTABLE key attribute via Java (LunaProvider/JSP). **Fixed:** Fixed in Luna HSM Client 7.2.
LUNA-2081	M	**Problem:** Multipart AES_KW operations on non-block-sized-data returns incorrect error code CKR_DEVICE_ERROR. **Fixed:** Fixed in release 7.2.
LUNA-2077	M	**Problem:** On Windows, one-step NTLS is very slow and takes almost four minutes to complete the NTLS connection setup. **Fixed:** One-step NTLS performance has been improved in release 7.2.
LKX-3178	M	**Problem:** When you use an older client, and query partition-level capabilities and policies, the HSM returns incorrect policy numbers. **Fixed:** Fixed in firmware 7.2.0.
LKX-3159	M	**Problem:** In LunaCM, **hsm information monitor** incorrectly reports HSM utilization. **Fixed:** Fixed in firmware 7.2.0.
RAPI-1446	M	**Problem:** Webclient sample cannot complete tasks. **Workaround:** Fixed in REST API 6.0.0.
LKX-3042 LKX-2989	L	**Problem:** When partition policy 39: Allow start/end date attributes is enabled, all start dates must be later than January 01, 1970. **Fixed:** Fixed in firmware 7.2.0.

Revision History

Revision A: 07 May 2018

> Initial Release

Revision B: 17 August 2018

> Added to "New Features and Enhancements" on page 4:

- Version 7.2 and newer Luna HSM Client can be used with HSMs running Luna 6.2.1 or higher without conflict.
- The improved Luna HSM Client can be used to create mixed-version HA groups with Luna 6/7 partitions.

Revision C: 20 June 2019

> Added "Important Notices for SafeNet Luna Network HSM 7.2 Optical Ethernet Release" on page 2 about the factory-orderable option for 10 Gbps Optical Ethernet

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.