

SafeNet Luna Network HSM 7.3

CUSTOMER RELEASE NOTES

Issue Date: 18 July 2019

Document Part Number: 007-013580-005 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 | 2 |
| Release Description | 2 |
| New Features and Enhancements | 2 |
| HSM Firmware version 7.3.3 is FIPS 140-2 validated. | 2 |
| Appliance Re-Image | 2 |
| Partition Utilization Metrics | 2 |
| BIP32 Algorithm | 3 |
| JavaSP support for ECC Curve 25519 | 3 |
| Fixes | 3 |
| Advisory Notes | 3 |
| HSM Firmware version 7.3.3 caveats | 3 |
| Luna 7.3 Appliance Software Does Not Support 10G Optical Ethernet | 4 |
| Resolved Issue LUNA-7533: Java DERIVE and EXTRACT flag settings for keys injected into the HSM | 4 |
| PED Upgrade Required for Currently-Owned PEDs | 4 |
| New USB-powered PED | 5 |
| STC over IPv6 is Unavailable | 5 |
| Remote Backup Over IPv6 is Unavailable | 5 |
| HSM Logs Sent to Messages Log | 5 |
| Supported Operating Systems | 6 |
| SafeNet Luna HSM Client | 6 |
| Remote PEDserver | 6 |
| Supported Cryptographic APIs | 7 |
| Update Considerations | 7 |
| Valid Update Paths | 7 |
| FIPS-Validated Firmware Versions | 8 |
| Recommended Minimum Versions | 8 |
| Known Issues | 8 |

| | |
|------------------------|----|
| Resolved Issues | 16 |
| Revision History | 18 |
| Support Contacts | 18 |

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 7.3 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.

New Features and Enhancements

SafeNet Luna Network HSM 7.3 introduces the following new features and enhancements:

HSM Firmware version 7.3.3 is FIPS 140-2 validated.

Firmware 7.3.3 update incorporates the features and fixes supported by firmware versions 7.1, 7.2 and 7.3, and is now the preferred FIPS-validated SafeNet Luna HSM firmware version.

CMVP Certificate #3205

See the ["HSM Firmware version 7.3.3 caveats " on the next page](#) in the Advisory Notes section, below.

Appliance Re-Image

SafeNet Luna Network HSM 7.3 allows you to re-image the appliance to a pre-installed baseline version. This procedure formats the SafeNet Luna Network HSM file system, zeroizes the HSM, erases the appliance configuration, and resets the appliance software to Luna 7.2 and the HSM firmware to version 7.0.3. This capability is useful if you are re-purposing an HSM for a project that has standardized on an earlier software/firmware configuration, or if you need to format the appliance completely and remove all trace of its prior configuration (requires firmware 7.3.0).

Partition Utilization Metrics

SafeNet Luna Network HSM 7.3 allows the HSM SO to access utilization records for all partitions on the HSM. This information is restricted to operation counts, and shows which partitions are using the HSM's resources. Information about which keys are being used for which operation is still restricted to the Auditor (requires firmware 7.3.0).

BIP32 Algorithm

SafeNet Luna Network HSM 7.3 includes new mechanisms that use the BIP32 cryptographic algorithm. This allows SafeNet Luna Network HSM to support applications that use Hierarchical Deterministic Wallets, used in Bitcoin and blockchain transactions (requires firmware 7.3.0).

JavaSP support for ECC Curve 25519

The SafeNet Java Provider now includes support for mechanisms using ECC Curve 25519.

Fixes

Issues addressed in this release are listed in ["Resolved Issues" on page 16](#).

Advisory Notes

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

HSM Firmware version 7.3.3 caveats

Firmware 7.3.3 update incorporates the features and fixes supported by firmware versions 7.1, 7.2 and 7.3, and is now the preferred FIPS-validated SafeNet Luna HSM firmware version.

The firmware version shipped from the factory remains 7.0.3. Version 7.3.3 is a field-installable update.

Update paths and considerations

| From f/w version | To f/w version | Comment or caveat |
|---|----------------|--|
| <i>PASSWORD-AUTHENTICATED</i> | | |
| 7.0.3, 7.1.0, 7.2.0, 7.3.0 | 7.3.3 | Normal firmware update procedure (see Updates and Upgrades section of main HSM documentation) - no issues. |
| <i>PED-AUTHENTICATED</i> | | |
| 7.0.3 | 7.3.3 | Normal firmware update procedure (see Updates and Upgrades section of main HSM documentation) - no issues. |
| partition created in HSM at one of f/w versions 7.1, 7.2, or 7.3.0 with Partition Policy 15 set to ON | 7.3.3 | Normal firmware update procedure (see Updates and Upgrades section of main HSM documentation) - EXCEPT you must reset the challenge secret, after f/w update, so that partition objects become accessible again. |

| From f/w version | To f/w version | Comment or caveat |
|--|----------------|---|
| Partition created in HSM at one of f/w versions 7.1, 7.2, or 7.3.0 with Partition Policy 15 set to OFF (*) | 7.3.3 | <ol style="list-style-type: none"> 1. Before updating firmware, back up your partition contents. 2. Update your HSM to firmware version 7.3.3. 3. Your existing partition is no longer accessible -- re-initialize the existing partition. 4. Restore your partition objects from backup. |

(* By default, Partition Policy 15 is off. Turning Policy 15 ON is destructive.)

Luna 7.3 Appliance Software Does Not Support 10G Optical Ethernet

The SafeNet Luna Network HSM with 10G optical ethernet capability is not supported by the Luna 7.3.x appliance software. If you have a 10G-ready appliance, update appliance software to version 7.4 or higher only.

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.

Resolved Issue LUNA-7533: Java DERIVE and EXTRACT flag settings for keys injected into the HSM

Formerly, the DERIVE and EXTRACT flags were forced to "true" in the JNI, which overrode any values passed by applications via Java. This is resolved in Luna 7.3 release.

As of release 7.3:

- > The default values for the DERIVE and EXTRACT flags are set to "false" (were set to "true" in previous releases.
- > JNI accepts and preserves values set by applications via the following Java calls:

```
LunaSlotManager.getInstance().setSecretKeysDerivable( true );
LunaSlotManager.getInstance().setPrivateKeysDerivable( true );
LunaSlotManager.getInstance().setSecretKeysExtractable( true );
LunaSlotManager.getInstance().setPrivateKeysExtractable( true );
```

NOTE If you have existing code that relies on the DERIVE and EXTRACT flags being automatically defined by the JNI for new keys, you will need to modify your application code to set the flag values correctly.

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 7.3 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 | No | No |
| Solaris (SPARC/x86) * | 11 | Yes | No | 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

Detailed procedures for installing the SafeNet Luna Network HSM 7.3 software and firmware updates can be found in the product documentation. Before you install any of the updates, consider the following guidelines:

- > 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.
- > For firmware 7.3.3 see "[Update paths and considerations](#) " on page 3 in case your HSM is affected by a special case.

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 | 7.3 |
| SafeNet Luna Network HSM appliance software | 7.0, 7.1 | 7.2 |
| | 7.2 | 7.3 |
| SafeNet Luna HSM firmware | 7.0.1, 7.0.2 | 7.0.3, 7.2.0 |
| | 7.0.3, 7.1.0, 7.2.0, 7.3.0 | 7.3.3* |
| 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 |

(* Check the CRN "Advisory Notes" section, to see if any caveat applies to your HSM)

(** Note that firmware 6.24.7 is the latest FIPS-validated version for the Backup HSM. FIPS validation might not be strictly necessary for a Backup HSM because it does not perform cryptographic operations with contained objects, but some audit checklists might not make that distinction.)

FIPS-Validated Firmware Versions

The following firmware versions are all FIPS-140-2 Level 3 certified per certificate #3205:

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3205>

- > Luna firmware v. 7.3.3 (recommended)
- > Luna firmware v. 7.0.2 (see F5 note, below)
- > Luna firmware v. 7.0.3

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 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.

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. |

| Severity | Classification | Definition |
|----------|----------------|------------------------|
| L | Low | Low severity problems. |

Table 2: List of known issues in release 7.3

| Issue | Severity | Synopsis |
|-----------|----------|---|
| LKX-4868 | H | <p>Problem: On a 64-bit client operating system, running multitoken with different BIP32 modes against an STC HA virtual slot causes multitoken to fail with an error (CKR_TOKEN_NOT_PRESENT).</p> <p>Workaround: Do not use BIP32 modes with STC HA groups; use NTLS instead.</p> |
| LKX-4543 | H | <p>Problem: After a firmware update, duplicate entries are produced in the audit logs. These duplicate entries cause log verification to fail with an error (CKR_LOG_BAD_RECORD_HMAC).</p> <p>Workaround: There is no way to avoid the duplicate entries. However, the other entries in the log file can be verified without error. When verifying the logs, specify a range that excludes the duplicate entries:</p> <p>lunash:>audit log verify -file <log_file> -start <first_entry> -end <last_entry></p> |
| LUNA-7438 | H | <p>Problem: When using CKdemo to perform a multipart sign/verify operation with a key that has exceeded its specified usage count, an expected error is returned (CKR_KEY_NOT_ACTIVE). The next sign/verify operation with an active key fails with an unexpected error (CKR_OPERATION_ACTIVE).</p> <p>Workaround: Restart CKdemo and attempt the operation again.</p> |
| LUNA-7436 | H | <p>Problem: Encrypt operations using DES3_CBC_PAD and specifying a NULL buffer fail (CKR_BUFFER_TOO_SMALL).</p> <p>Workaround: Manually specify a buffer size for these operations.</p> |
| LKX-4852 | M | <p>Problem: Reset timestamp displayed when reporting metrics via LunaSH or REST can vary, each time the commands are used, by approximately 6s.</p> <p>Workaround: Reset the timers. This causes the value to be written to a file, so that the reported reset time remains constant until the next reset.</p> |
| LKX-4250 | M | <p>Problem: CA_DeriveKeyAndWrap does not handle AES_KW, AES_KWP, or AES_CTR mechanisms.</p> <p>Workaround: None.</p> |
| LUNA-7418 | M | <p>Problem: When logged in to LunaSH as a custom user, resetting the appliance users to factory condition (lunash:>sysconf config factoryreset -service users) does not delete the currently logged-in user.</p> <p>Workaround: Log in to LunaSH as admin to reset the appliance user configuration.</p> |

| Issue | Severity | Synopsis |
|------------------------|----------|--|
| LUNA-7164 | M | <p>Problem: When a bad remote logging host is added, existing hosts that were functioning correctly stop receiving logs.</p> <p>Workaround: Ensure that all remote logging hosts are reachable and configured correctly before adding them.</p> |
| LUNA-7074 | M | <p>Problem: In LunaCM, when switching the active slot between partitions on different HSMs, ped connect and ped get sometimes report an active Remote PED connection, even though the connection is broken. Authentication commands fail.</p> <p>Workaround: Use ped disconnect on the active slot before switching to a different slot and running ped connect.</p> |
| LUNA-4134 | M | <p>Problem: When the SafeNet Luna Network HSM is configured for IPv6 connections, a missing file error is displayed in the output from <code>lunash:>network show</code> (<code>/usr/lunasa/lush/Lroot/Cnetwork/network_utility_common: line 63: /usr/lunasa/bin/getIPv6Prefix: No such file or directory</code>).</p> <p>Workaround: This error can be safely ignored.</p> |
| LUNA-4133 | M | <p>Problem: NTLS connection fails when the appliance has the default hostname <code>local_host</code>.</p> <p>Workaround: Assign a unique hostname to the appliance (<code>lunash:>network hostname <hostname></code>).</p> |
| LUNA-7430 | L | <p>Problem: When running commands in some Luna utilities on Windows 10, password characters are duplicated.</p> <p>Workaround: Contact Gemalto Customer Support.</p> |
| LUNA-7194 RAPI-1416 | L | <p>Problem: Webserver starts even if no SSL key/cert exists, but is not accessible.</p> <p>Workaround: Generate the SSL key/cert before starting the webserver.</p> |

Table 3: List of known issues from prior releases

| Issue | Severity | Synopsis |
|----------|----------|--|
| LKX-3184 | M | <p>Applies to firmware 7.0.3 only. This issue has been fixed in firmware 7.2.0 and later.</p> <p>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).</p> <p>Workaround: None. If you are using STC, or have enabled HSM policy 39 in the past, do not roll back the HSM firmware.</p> |
| LKX-2634 | M | <p>Problem: Cannot back up curve25519 key types to the SafeNet Luna Backup HSM.</p> <p>Workaround: Use cloning or HA to back up your curve25519 key types to another SafeNet Luna 7.x HSM.</p> |

| Issue | Severity | Synopsis |
|-----------|----------|--|
| LUNA-3691 | M | <p>Problem: When resetting the HSM to factory conditions with audit logging enabled and an existing audit log file, new events are not logged after the Auditor role is re-initialized.</p> <p>Workaround: None.</p> |
| LUNA-3683 | M | <p>Problem: On Linux clients, when a non-root user attempts to uninstall the Luna HSM Client software, the process fails and the client software remains installed, but "Uninstall of the Luna HSM Client 7.3.0-165 completed" is displayed in the command output.</p> <p>Workaround: Ignore this message and log in as the root user to uninstall the Luna HSM Client software.</p> |
| LUNA-3554 | M | <p>Problem:The appliance remains disconnected from the network, even though the appliance itself is back online and fully functional.</p> <p>Workaround: Reboot the appliance.</p> |
| LUNA-3423 | M | <p>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.</p> <p>Workaround: If you are checking logs for one of these exact errors, ensure that you search for the error associated with your connection type.</p> |
| LUNA-3429 | M | <p>Problem: Error: pedClient is not currently running error is displayed when trying to connect with PEDserver using lunash:>hsm ped connect, even though the cbs service is shown to be running.</p> <p>Workaround: Restart the cbs service on the appliance.</p> |
| LUNA-3422 | M | <p>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.</p> <p>Workaround: If you are checking logs for one of these exact errors, ensure that you search for the error associated with your connection type.</p> |
| LUNA-3421 | M | <p>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.</p> <p>Workaround: None.</p> |
| LUNA-3416 | M | <p>Problem: When performing AES encryption on an HA group using AIX and SPARC clients, failover occasionally fails with an error (CKR_TOKEN_NOT_PRESENT).</p> <p>Workaround: None.</p> |
| LUNA-3414 | M | <p>Problem: One-step Network Trust Link (NTLS) setup fails on Windows with error code CKR_CANCEL when SO Login Enforcement is enabled.</p> <p>Workaround: Use the multi-step NTLS setup procedure to create a connection to the SafeNet Luna Network HSM appliance.</p> |

| Issue | Severity | Synopsis |
|-----------|----------|--|
| LUNA-3343 | M | <p>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.</p> <p>Workaround: Restart the client application, and the error will clear.</p> |
| LUNA-3307 | M | <p>Problem: In LunaCM, clientconfig deploy (one-step NTLS) fails if the partition name contains spaces.</p> <p>Workaround: Use the multi-step NTLS connection procedure to assign the partition to the client.</p> |
| LUNA-3291 | M | <p>Problem: When you uninstall the Luna HSM Client software and reinstall it in a custom directory, existing IPv6 NTLS connections are broken. The existing client IPv6 certificates are not copied to the new client certificate directory.</p> <p>Workaround: Manually copy the IPv6 certificates to the new client certificate directory.</p> |
| LUNA-3108 | M | <p>Problem: If you uninstall Luna HSM Client and reinstall it in a custom directory, HA logging stops working.</p> <p>Workaround: Open crystoki.conf/crystoki.ini and edit <code>haLogPath</code> = to match the new client path.</p> |
| LUNA-3107 | M | <p>Problem: If you uninstall Luna HSM Client and reinstall it in a custom directory, RBS stops working.</p> <p>Workaround: Copy the two certificate files serverkey.pem and server.pem from the original rbs directory to the new rbs directory.</p> |
| LUNA-3070 | M | <p>Problem: vtl cklog enable/disable command not working if LibUNIX and LibUNIX64 are in different folders.</p> <p>Workaround: Enable cklog manually by editing Chrystoki.conf/crystoki.ini. Refer to the <i>SDK Reference Guide</i> for details.</p> |
| LUNA-2646 | M | <p>Problem: One-step NTLS can fail after installing, uninstalling, and reinstalling the Luna HSM Client on Windows.</p> <p>Workaround: Use the multi-step NTLS setup procedure to create a connection to the SafeNet Luna Network HSM appliance.</p> |
| LUNA-2445 | M | <p>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.</p> <p>Workaround: Manually set the HA log maximum file size using <code>lunacm:>hagroup halog -maxlength <bytes></code> the first time you configure HA logging.</p> |
| LUNA-2261 | M | <p>Problem: "CKR_DATA_INVALID" on wrap/unwrap with multitoken on AIX and Solaris clients.</p> <p>Workaround: None.</p> |

| Issue | Severity | Synopsis |
|-----------|----------|---|
| LUNA-2252 | M | <p>Problem: Invalid options are displayed on Solaris installer.</p> <p>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.</p> |
| LUNA-2224 | M | <p>Problem: When you initialize an STC partition by applying a partition policy template, a confusing error (CKR_TOKEN_NOT_PRESENT) is returned.</p> <p>Workaround: None.</p> |
| LUNA-2199 | M | <p>Problem: LunaCM occasionally freezes in Windows 2016 when a new slot is created or deleted.</p> <p>Workaround: End the LunaCM instance with Task Manager and restart LunaCM.</p> |
| LUNA-2007 | M | <p>Problem: Unable to establish NTLS connection using the one-step NTLS procedure on Solaris x86 when there are more partitions(10~15).</p> <p>Workaround: Use the multi-step NTLS connection procedure on a Solaris client.</p> |
| LUNA-1927 | M | <p>Problem: Unable to add new member to HA group after removing primary member.</p> <p>Workaround: Manually delete the serial number of the deleted Network HSM's partition from the <code>VirtualToken00Members</code> field in the Chrystoki.conf (Linux/UNIX) 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.</p> |
| LUNA-1725 | M | <p>Problem: In LunaCM, partition archive restore -replace does not replace DUPLICATED objects in target partition.</p> <p>Workaround: Remove all duplicate objects from the target partition prior to running partition archive restore -replace.</p> |
| LUNA-1592 | M | <p>Problem: When trying to run the HALogin.java script, a CKR_UNKNOWN error is returned.</p> <p>Workaround: None. Do not use the HALogin.java sample.</p> |
| RAPI-1211 | M | <p>Problem: In REST API, GET /api/lunasa/hsms may return an empty list.</p> <p>Workaround: Another attempt may return a populated list if an HSM is available.</p> |
| RAPI-383 | M | <p>Problem: REST API does not verify the NTLS client's IP against the certificate.</p> <p>Workaround: None.</p> |
| CPP-3261 | M | <p>Problem: After performing sysconf config factoryreset, the appliance host name is not reset.</p> <p>Workaround: None.</p> |

| Issue | Severity | Synopsis |
|-----------------------|----------|---|
| CPP-3241 | M | <p>Problem: Untarred audit log files are not visible to the user.</p> <p>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>.</p> |
| CPP-3191 | M | <p>Problem: After rebooting the appliance, occasionally clients cannot see partitions on the first connection attempt.</p> <p>Workaround: Run the vtl verify command again. The second attempt should be successful.</p> |
| CPP-2954 LUNA-3352 | M | <p>Problem: The hsmCriticalEvent and hsmNonCriticalEvent counters incorrectly track HSM events.</p> <p>Workaround: None. SNMP hsmCriticalEvent and hsmNonCriticalEvent counters are not implemented in this release and will always remain 0.</p> |
| CPP-2505 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 network dns add {-nameserver <IP_address> -searchdomain <net_domain>}.</p> |
| CPP-2368 | M | <p>Problem: The hagroup list command returns an error.</p> <p>Workaround: Run the hagroup list command again. The second attempt should be successful.</p> |
| CPP-1339 | M | <p>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.</p> <p>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.</p> |
| CPP-632 LUNA-7429 | M | <p>Problem: When using CKdemo with HA groups, an Attribute type invalid error is returned.</p> <p>Workaround: If you plan to use HA groups, change your CKdemo settings to use legacy role logins. To do this, select Role Support from the 98) Options in the OTHERS menu.</p> |
| CPP-626 CPP-624 | M | <p>Problem: If you zeroize an HSM hosting an HA group member partition, all running cryptographic operations against the HA group fail.</p> <p>Workaround: Remove any member partition from the HA group before zeroizing the host HSM.</p> |
| LUNA-3511 | L | <p>Problem: Audit logging -- hsm zeroize is not logged after performing a factory reset of the HSM, since the audit configuration is erased during factory reset.</p> <p>Workaround: None.</p> |

| Issue | Severity | Synopsis |
|-----------------------|----------|---|
| LUNA-3276 | L | <p>Problem: When installing the Luna HSM Client software to a custom directory with spaces in the directory name, the installer creates a new named directory that ignores everything after the first space.</p> <p>Workaround: Do not use spaces when naming your custom install directory.</p> |
| LUNA-3126 | L | <p>Problem: After running <code>lunash:> hsm ped connect</code> on an uninitialized SafeNet Luna Network HSM, <code>hsm ped show</code> may incorrectly display <code>Number of Connected PED Server : 0</code>.</p> <p>Workaround: None necessary; this behavior does not affect the functioning of Remote PED.</p> |
| LUNA-2103 | L | <p>Problem: If you enter duplicate policies (policies with the same ID) in the partition policy template, the partition will take the last value.</p> <p>Workaround: Avoid duplicate policy IDs in partition policy template files.</p> |
| LUNA-2022 | L | <p>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."</p> <p>Workaround: None. You cannot bind SSH to a bond slave.</p> |
| LUNA-2015 | L | <p>Problem: Default <code>ntlsOperStatus</code> for SNMP is incorrectly set to 0 (correct value: 3). This can lead to errors in applications that adhere to syntax strictly.</p> <p>Workaround: None.</p> |
| LUNA-339 | L | <p>Problem: Some appliance sensor information is missing or incorrectly reported via SNMP.</p> <p>Workaround: Use the LunaSH command status sensors to obtain this information.</p> |
| LUNA-218 | L | <p>Problem: You cannot add a host or network route using the LunaSH network route add command without including the gateway value.</p> <p>Workaround: None.</p> |
| RAPI-1096 | L | <p>Problem: After modifying the webserver settings the apiversion under <code>/api/lunasa</code> becomes 0.</p> <p>Workaround: Restart the webserver service.</p> |
| CPP-3404 | L | <p>Problem: CMU may crash or report a memory allocation error when using a non-FIPS signing mechanism in FIPS mode.</p> <p>Workaround: Specify a FIPS-approved signing mechanism such as sha256withRSA.</p> |
| CPP-3384 LUNA-1585 | L | <p>Problem: After zeroization or factory reset, the STC cipher option is set to <code>NULL_ENC</code>. Output from hsm stc status includes "Cipher Name: No Cipher".</p> <p>Workaround: Run the LunaSH command hsm stc cipher enable -all to enable all available STC ciphers.</p> |

| Issue | Severity | Synopsis |
|-----------------------|----------|---|
| CPP-3235 | L | <p>Problem: In LunaCM, the partition clone command fails the first time if the Partition SO is logged in to the target slot.</p> <p>Workaround: Run the partition clone command again. The second attempt should be successful.</p> |
| CPP-2960 | L | <p>Problem: LunaCM hangs on exit on Windows 2016.</p> <p>Workaround: End the LunaCM instance using the Task Manager.</p> |
| CPP-2925 | L | <p>Problem: When the cklog library is configured, an error.txt file containing extraneous messages may be created.</p> <p>Workaround: None.</p> |
| CPP-2380 | L | <p>Problem: When running the MiscCSRCertificateDemo.java sample, a null pointer exception occurs.</p> <p>Workaround: None.</p> |
| CPP-1249 LUNA-1681 | L | <p>Problem: Remote backup through TCP/IP via the LunaCM command partition archive backup -slot remote -hostname <hostname> -port <portnum> is not recognized.</p> <p>Workaround: Use RBS to backup partitions remotely.</p> |
| CPP-932 | L | <p>Problem: If the configured audit logging directory is not found, the PEDclient service fails with error LOGGER_init failed.</p> <p>Workaround: Ensure that the directory you configure for audit logging exists.</p> |

Resolved Issues

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

Table 4: List of resolved issues

| Issue | Severity | Synopsis |
|-----------|----------|---|
| LUNA-7000 | H | <p>Problem: Using REST API, open application IDs sometimes cause the HSM to stop responding.</p> <p>Resolved: Fixed in REST API 7.0.0.</p> |
| LUNA-3254 | H | <p>Problem: Calls to CA_OpenApplicationID fail when certain sequences of calls are run, for example:</p> <ol style="list-style-type: none"> 1. CA_SetApplicationID(x,y) 2. C_OpenSession() 3. C_CloseSession() 4. CA_OpenApplicationID(x,y) <p>Resolved: Fixed in Luna release 7.3.</p> |

| Issue | Severity | Synopsis |
|------------------------|----------|--|
| LUNA-7533 | M | <p>Problem: Java DERIVE and EXTRACT flag settings for keys injected into the HSM. The DERIVE and EXTRACT flags were forced to "true" in the JNI, which overrode any values passed by applications via Java.</p> <p>Resolved: Fixed in Luna release 7.3.</p> |
| LUNA-7258 | M | <p>Problem: When running cmu commands on Windows 10, password characters are duplicated.</p> <p>Resolved: Fixed in Luna release 7.3.</p> |
| LUNA-3364 | M | <p>Problem:After running sysconf appliance reboot from LunaSH, the appliance occasionally gets stuck with a "Rebooting" message on the LCD screen.</p> <p>Resolved: Fixed in Luna release 7.3.</p> |
| LUNA-3275 | M | <p>Problem: When using CKdemo to query an application partition, the Crypto Officer password is entered in visible plaintext.</p> <p>Resolved: Fixed in Luna release 7.3.</p> |
| LUNA-3298 | M | <p>Problem: When installing Backup HSM and Luna 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.</p> <p>Resolved: Fixed in Luna HSM Client release 7.3.</p> |
| LUNA-3167 | M | <p>Problem: Cannot migrate keys using MS2Luna.exe for CSP.</p> <p>Resolved: Fixed in Luna release 7.3.</p> |
| LUNA-3071 | M | <p>Problem: When LunaCM is launched in Luna Minimal Client, an unexpected error is displayed (Error: Failed to initialize remote PED support).</p> <p>Resolved: Fixed in Luna HSM Client release 7.3.</p> |
| LUNA-2983 | M | <p>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.</p> <p>Resolved: Fixed in Luna HSM Client release 7.3.</p> |
| RAPI-1248 | L | <p>Problem: REST API web client shows wrong logout result.</p> <p>Resolved: Fixed in REST API 7.0.0.</p> |
| RAPI-1062 | L | <p>Problem: In REST API, POST /auth/logout does not return Access-Control-Allow-Credentials and Access-Control-Allow-Origin in the response headers.</p> <p>Resolved: Fixed in REST API 7.0.0.</p> |
| RAPI-1027 LUNA-3621 | L | <p>Problem: REST API partition actions contain actions that should be deprecated.</p> <p>Resolved: Fixed in REST API 7.0.0.</p> |

| Issue | Severity | Synopsis |
|-----------|----------|---|
| CPP-3326 | L | Problem: Webserver starts even if no SSL key/cert exists, but is not accessible. |
| RAPI-1416 | | Resolved: Fixed in REST API 7.0.0. |
| LUNA-7194 | | |

Revision History

Revision A: 21 September 2018

- > Initial Release

Revision B: 02 May 2019

- > Added to **Advisory Notes:** ["Luna 7.3 Appliance Software Does Not Support 10G Optical Ethernet" on page 4](#)

Revision C: 20 July 2019

- > Added to **Advisory Notes:** ["HSM Firmware version 7.3.3 is FIPS 140-2 validated." on page 2](#)
- > Added to **Advisory Notes:** ["HSM Firmware version 7.3.3 caveats " on page 3](#)
- > Updated **Valid Update Paths** table in ["Update Considerations" on page 7](#)

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

The support portal also lists telephone numbers for voice contact. ([KB0013367](#))

Email Support

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