Thales Luna HSM Client 10.1.0 for Luna Network HSM

CUSTOMER RELEASE NOTES

Issue Date: 25 June 2021

Document Part Number: 007-000554-001 Rev. D

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

Contents

Product Description

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. 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.

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

Release Description

Luna HSM Client release 10.1 includes Client software with drivers and tools. You can view, administer, and access via API, both password-authenticated Luna HSM application partitions and Luna Cloud HSM services from Data Protection on Demand, with the ability to securely clone objects between the two (see "Advisory Notes" on the next page for provisos).

New Features and Enhancements

Luna HSM Client 10.1.0 for Luna Network HSM introduces the following new features and enhancements:

Luna HSM Client 10.1 Supports Both Luna HSMs and Luna Cloud HSM Services From Data Protection on Demand

Luna HSM Client can now be used with Luna Cloud HSM services provided by Thales Data Protection on Demand. This allows you to migrate keys from a password-authenticated Luna HSM partition to a Luna Cloud HSM service or vice-versa, set up High-Availability (HA) groups that include both password-authenticated Luna partitions and Luna Cloud HSM services, and operate your local (Luna PCIe), remote (Luna Network), and cloud HSM solutions on the same client workstation.

Luna Cloud HSM client compatibility is limited to Windows and Red Hat Enterprise Linux 7-based operating systems in this release.

Luna G7 Backup HSM

Thales is pleased to announce the availability of the Luna G7 Backup HSM – a full-featured, hand-held, USB-attached backup HSM that includes an informational full-color display.

You can use the Luna G7 Backup HSM to backup your Luna HSM 5.x, 6.x, and 7.x user partitions.

The Luna G7 Backup HSM connects easily to a client workstation using the included USB 3.0 Type C cable, and includes a universal 5V external power supply, which may be required to power the device in some instances.

> **NOTE** The smart card slot located at the bottom front of the unit is reserved for future use and has been disabled in this release.

Models

The Luna G7 Backup HSM is available in the following models. All models can be initialized in PED or password-authenticated mode for backing up either PED or password authenticated partitions. In-field storage upgrades are not available.

B700	32 MB storage, up to 100 partitions of the same authentication type
B750	128 MB storage, up to 100 partitions of the same authentication type
B790	256 MB storage, up to 100 partitions of the same authentication type

To use the Luna G7 Backup HSM, you must upgrade to Luna HSM Client 10.1, a client-only field update for Linux and Windows. Luna HSM Client 10.1 provides the drivers and software updates you need to use the Luna G7 Backup HSM.

Remote PED Support on Linux

You can now host Remote PED services on a Linux workstation.

Client Certificates Signed by a Trusted Certificate Authority

Luna HSM Client 10.1 allows you to use client certificates signed by a trusted Certificate Authority (CA), which can be a commercial third-party CA or your organization's own signing station.

Windows Secure Boot Support

The drivers included with the Luna HSM Client software for Luna PCIe HSMs, Luna Backup HSMs, Luna USB HSMs, and Luna PEDs now support Windows Secure Boot.

Fixes

Issues addressed in this release are listed in "Resolved Issues" on page 21.

Advisory Notes

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

Luna HSM Client 10.1 Replaces Version 7.5

Luna HSM Client 10.1 includes bug fixes and additional functionality for the Luna G7 Backup HSM. Thales strongly recommends that all customers using version 7.5 update their client software to 10.1 or newer. Luna HSM Client 7.5 is no longer available for download from the Thales Customer Portal.

Older JAVA versions require patch/update

The .jar files included with the Luna HSM Client have been updated with a new certificate, signed by the Oracle JCE root certificate. This certificate validation requires a minimum Oracle JDK/JRE version.

- If your application relies on Oracle Java 7 or 8, you must update to the advanced version provided by Oracle. You require (at minimum) version **7u131** or **8u121**. Please refer to Oracle's website for more information: https://www.oracle.com/technetwork/java/java-se-support-roadmap.html
- If your application relies on IBM Java 7 or 8, you must install a patch from IBM before updating to Luna HSM Client 10.x (see APAR IJ25459 for details).

"CKR_MECHANISM_INVALID" messages in mixed DPoD implementations

When using DPoD with Luna HSM Client, you might encounter errors like "CKR_MECHANISM_INVALID" or "Error NCryptFinalizeKey" during some operations in Hybrid HA and FIPS mode (3DES Issue). This can occur if firmware versions differ between a Luna Network HSM partition and a DPoD service in an HA group when you invoke a mechanism that is supported on one but not the other. Similarly, if one member is in FIPS mode, while the other is not, a mechanism might be requested that is allowed for one member, but not the other. For example, the **ms2luna** tool can fail when 3DES operations are invoked.

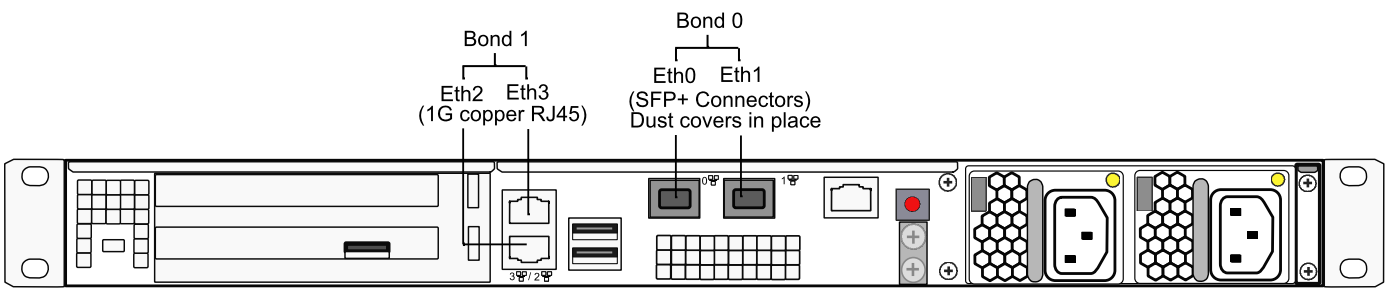
Important note about 10 Gbps Optical Ethernet modules

The Network HSM Appliance is shipped from the factory with FIPS-validated firmware installed, and can be purchased with one of two options for Ethernet ports:

- 1Gbps copper-only RJ-45 connectors for all four physical Ethernet ports, or
- 10Gbps Optical Ethernet on two of the ports and 1Gbps RJ-45 connections on the other two ports.

The first option was already the standard, factory-delivered appliance.

The second option behaves identically to the first, in all respects, except 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.

> **CAUTION!** To use 10 Gbps optical Ethernet, update Luna Network HSM appliance software to version 7.4 or higher. Do not attempt to update a 10G-ready appliance to version 7.3.x.

Support for 32-bit OS Platforms is Ending

As of this release, 32-bit libraries are no longer provided. If you have a 32-bit application or integration, remain with a previous client release (such as 7.2, 7.3, 7.4, or 7.5), or migrate to 64-bit platform.

Resolved Issues LKX-2832/LUNA-956: CKA_EXTRACTABLE Default Setting

Formerly, the CKA_EXTRACTABLE attribute on new, unwrapped, and derived keys was incorrectly set to TRUE by default. This was resolved in Luna HSM firmware 7.0.2 and higher. In firmware 7.0.2 and higher, the CKA_EXTRACTABLE attribute on new, unwrapped, and derived keys is set to FALSE by default.

> **NOTE** If you have existing code or applications that expect keys to be extractable by default, you must modify them to explicitly set the CKA_EXTRACTABLE attribute value to TRUE.

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 release 7.3 and higher.

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 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 Thales Support Portal.

New USB-powered PED

Gemalto is pleased to announce the availability of 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 Luna HSM Client software is installed on the Windows computer that will provide PED authentication for your Luna Network HSM. Installing the Remote PED component of the Luna HSM Client installs the required driver.
2. Connect the PED to the computer where you installed the Remote PED component of the 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 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.

Luna HSM Client

Luna HSM Client 7.2 and newer 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.

You can install the Luna HSM Client 10.1.0 on the following 64-bit operating systems:

Operating System	Version
Windows	10 (Secure Boot Mode supported)
Windows Server	2019 (Secure Boot Mode supported)
	2016 (Secure Boot Mode supported)
	2012 R2
Red Hat Enterprise Linux (including variants like CentOS and Oracle Enterprise Linux)	7
	6 (HSMoD not supported)
AIX *	7.1 (HSMoD not supported)
Solaris (SPARC/x86) *	11 (HSMoD not supported)
SuSe Linux	12.4 (minimal client only)
	11.4 (minimal client only)
Ubuntu **	14.04 (HSMoD not supported)

* Although the AIX and Solaris installers display the options, 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 Luna HSM Client software. You must install the Luna HSM Client, with the PEDserver option, on each workstation used to host a remote PED. The PEDserver software is supported on Windows and Linux (see "Supported Operating Systems" on the previous page).

Supported Cryptographic APIs

Applications can perform cryptographic operations using the following APIs:

- PKCS#11 2.20
- JCA within Oracle Java 7*/8*/9/10/11

  *Luna HSM Client 10.1 requires the advanced version of Oracle Java 7/8.
- JCA within OpenJDK 7/8/9/10/11
- OpenSSL
- Microsoft CAPI
- Microsoft CNG

Update Considerations

Detailed procedures for installing the software and firmware updates can be found in the product documentation. Before you install any 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.

Valid Update Paths

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

Component	Directly from version	To version
Luna HSM Client software	Any	10.1
Luna Network HSM appliance software	7.0, 7.1	7.2
	7.2, 7.3	7.4

Component	Directly from version	To version
Luna HSM firmware	7.0.1, 7.0.2	7.0.3, 7.1.0, 7.2.0
	7.0.3, 7.1.0, 7.2.0, 7.3.0	7.3.3*, 7.4.0
Luna Backup HSM (G5) firmware	6.10.9, 6.24.7, 6.26.0	6.27.0**
Luna Backup HSM (G7) firmware	7.3.2	N/A
Luna PED firmware	2.7.1	N/A
	2.8.0	N/A

* See "Special Considerations for Updating to Luna Firmware 7.3.3" below to see if any caveat applies to your HSM.
** Note that firmware 6.24.7 is the latest FIPS-validated version for the Luna Backup HSM (G5). 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, see "Special Considerations for Updating to Luna Firmware 7.3.3" below)
- Luna firmware v. 7.0.3 (factory-shipped version)
- Luna firmware v. 7.0.2 (see F5 note, below)

Special Considerations for Updating to Luna Firmware 7.3.3

Firmware 7.3.3 update incorporates the features and fixes supported by firmware versions 7.1.0, 7.2.0 and 7.3.0, and is now the preferred FIPS-validated Luna Network HSM firmware version. Refer to the following table for special update procedures.

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

From f/w version	To f/w version	Procedure
PASSWORD-AUTHENTICATED		
7.0.3, 7.1.0, 7.2.0, 7.3.0	7.3.3	Normal firmware update procedure (refer to main HSM documentation)
PED-AUTHENTICATED		
7.0.3	7.3.3	Normal firmware update procedure (refer to main HSM documentation)

From f/w version	To f/w version	Procedure
Partition created in HSM at one of f/w versions 7.1.0, 7.2.0, or 7.3.0 with Partition Policy 15 set to ON*	7.3.3	Normal firmware update procedure (refer to main HSM documentation) - EXCEPT you must reset the challenge secret after the f/w update, so that partition objects become accessible again
Partition created in HSM at one of f/w versions 7.1.0, 7.2.0, or 7.3.0 with Partition Policy 15 set to OFF*	7.3.3	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.
Network appliance with appliance software 7.4.0 and HSM at f/w 7.4.0	7.3.3	Must first roll back f/w to one of 7.0.3, 7.1.0, 7.2.0, 7.3.0 before updating to f/w 7.3.3

***** By default, Partition Policy 15 is OFF. Turning Policy 15 ON is destructive.

Recommended Minimum Versions

Generally, Thales 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 Luna 7 HSMs. If you are running an earlier version, Thales 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
Luna Network HSM 7 Minimum Recommended Configuration	7.2	7.2	7.2.0
			7.0.3
Luna Network HSM 6 Minimum Recommended Configuration for migration to Luna HSM 7	7.2	6.3	6.10.9

> **NOTE** Customers who wish to use Luna 7 HSMs with F5 Network BIG-IP 13.1 appliances should follow F5 guidelines for supported Luna HSM 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.
L	Low	Low severity problems.

Table 2: List of known issues from Luna HSM Client release 10.1

Issue	Severity	Synopsis
LUNA-11616	M	**Problem:** If the client fails to resolve the DPoD service's DNS hostname, other client slots fail to load in LunaCM. **Workaround:** Ensure that your DNS network is stable before deploying HSMoD in an HA group. Ideally, configure multiple DNS nameservers for failover.
LUNA-11447	M	**Problem:** If an application running against an HA group fails over to the HSMoD member and the DNS hostname does not resolve, a segmentation fault can occur. **Workaround:** Ensure that your DNS network is stable before deploying HSMoD in an HA group. Ideally, configure multiple DNS nameservers for failover.
LUNA-11363	M	**Problem:** When using an HA group made up of Luna STC partitions and an HSMoD service and restarting the STC service, login to another STC partition in the same session can fail with an error (CKR_STC_NO_CHANNEL). **Workaround:** Restart LunaCM.
LUNA-11117	M	**Problem:** When using an HSM on Demand service with an Entrust integration on Windows, the **entsh** session times out after 4 minutes (this does not occur on Linux). **Workaround:** Log in to the Entrust session again and rerun the command.
LUNA-11141	M	**Problem:** If you installed the Windows client downloaded from the DPoD portal, LunaCM returns a missing DLL error (**MSVCP140.dll**). **Workaround:** Use the Luna HSM Client 10.1 installer, which includes all prerequisite files. Otherwise, refer to the DPoD documentation (**Services > HSM on Demand Services > HSMoD service supported client platforms**) for prerequisites to install manually.
SH-4571	M	**Problem:** If you exceed the recommended maximum number of objects cloned to/from an HSMoD service in a single cloning operation, the operation sometimes fails with an unhelpful error (CKR_DEVICE_ERROR). In the case of HA groups, this could include key creation operations, since objects are then cloned to the HSMoD service. **Workaround:** Expected behavior. Refer to the Luna HSM Client documentation for the recommended maximums.

Issue	Severity	Synopsis
LUNA-11017 SH-4282	M	**Problem:** When using an HA group made up of Luna partitions and an HSMoD service in FIPS mode, if the Luna partition is unavailable, **ms2luna** fails to migrate keys from the Microsoft CA to the HA slot. **Workaround:** Ensure that all HA group members are available before you run **ms2luna**.
SH-4194	M	**Problem:** If you perform **cmu getpkc** on an HSMoD service to confirm a public key, the operation can sometimes fail. **Workaround:** To confirm your key pair's origins and security in an HSM, run CKDemo's Display Object (27) function. If the CKA_NEVER_EXTRACTABLE attribute is present, this confirms that the private key was created in the HSM and never extracted.
LUNA-10992	M	**Problem:** When using an HA group made up of Luna partitions and an HSMoD service in FIPS mode, if the Luna partition is unavailable, 3DES keygen fails with CKR_MECHANISM_INVALID error. **Workaround:** Ensure that all HA group members are available before initiating 3DES keygen.

Table 3: List of known issues from prior releases

Issue	Severity	Synopsis
LKX-5545	M	**Problem:** When simultaneously running a combination of FM and non-FM applications with the HSM, an error: `Unable to communicate with HSM` can occasionally occur under very high operation loads. **Workaround:** Restart the HSM to clear the error (lunash:>**hsm restart**).
LKX-5353	M	**Problem:** When a Remote PED connection times out, lunacm:>**role login** fails with a confusing error (CKR_FUNCTION_FAILED). **Workaround:** Run lunacm:>**ped disconnect** before **ped connect**.
LKX-5351	M	**Problem:** When **partition policy 29: Perform RSA signing without confirmation** is set to **0** (OFF), all RSA sign operations fail with an error (CKR_DATE_LEN_RANGE). **Workaround:** If you use RSA signing, do not turn off partition policy 29.
LKX-5263	M	**Problem:** When audit logs fill up the HSM memory, HSM functions continue when they should be halted until audit logging is properly configured. Affects FM log entries only. **Workaround:** Configure audit logging on the HSM as described in documentation to prevent HSM memory from filling up.
LKX-5259	M	**Problem:** FM Capability license can be applied on non-FM-ready hardware. **Workaround:** Ensure your hardware is FM-ready before applying an FM license to the HSM.

Issue	Severity	Synopsis
LKX-4868	M	**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). **Workaround:** Do not use BIP32 modes with STC HA groups; use NTLS instead.
LKX-4852	M	**Problem:** Reset timestamp displayed when reporting metrics via LunaSH or REST can vary, each time the commands are used, by approximately 6s. **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.
LKX-4776	M	**Problem:** When running a combination of high-traffic FM and standard Luna applications, a rare SMFS failure can occur. Standard Luna processes are unaffected. **Workaround:** Erase the SMFS using lunash:>**hsm fm recover -erase smfs**, and restart the FM application if necessary.
LKX-4266	M	**Problem:** LunaCM incorrectly allows the user to add FM-enabled partitions to the same HA group as non-FM partitions. **Workaround:** HA groups with a combination of FM and non-FM members are not supported.
LKX-2634	M	**Problem:** Cannot back up curve25519 key types to the Luna Backup HSM. **Workaround:** Use cloning or HA to back up your curve25519 key types to another Luna 7.x HSM.
LUNA-8789	M	**Problem:** Restricting SSH traffic to an IPv6-configured ethernet port with lunash:>**sysconf ssh device** <eth#> still allows SSH connection via IPv4. **Workaround:** None.
LUNA-8760	M	**Problem:** Registering an IPv6 NTLS client with REST API by POSTing to **/api/lunasa/ntls/clients** fails with an `HTTP 400` error. **Workaround:** None. Register NTLS clients with LunaSH to avoid this issue.
LUNA-8756 HAPP-267	M	**Problem:** An FM-ready Luna Network HSM with appliance software version 7.4.0 and HSM firmware 7.0.3 incorrectly displays "**Non-FM**" in the output from lunash:>**hsm show**. LunaCM slot information for a partition on this HSM correctly displays "FM Ready". **Workaround:** Ignore the incorrect output. You must upgrade the HSM firmware to 7.4.0 to use FMs.
LUNA-8739	M	**Problem:** When an ethernet bond is active, lunash:>**sysconf config factoryreset** produces an incorrect error: `Error: bond1 is still active.` **Workaround:** The bond is actually reset and this error can be safely ignored.

Issue	Severity	Synopsis
LUNA-8695 LKX-5745	M	**Problem:** When a Remote PED connection times out, lunacm:>**ped connect** and lunacm:>**ped get** indicate that there is an active PED connection, but operations requiring PED authentication produce an error (CKR_CALLBACK_ERROR). **Workaround:** Run lunacm:>**ped disconnect** before **ped connect** or **ped get**.
LUNA-8620	M	**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 (lunash:> **network ping**). To execute such command, the operator must directly connect to the Luna Network HSM through the serial port.
LUNA-8619	M	**Problem:** During HSM initialization, if the PED operation to create the red domain key fails or times out, subsequent attempts to re-initialize the HSM will not prompt you to create the red domain key. **Workaround:** Zeroize the HSM with lunash:>**hsm zeroize** before re-initializing.
LUNA-8566	M	**Problem:** If a tamper state exists on the HSM, the appliance re-image procedure fails without providing a reason. **Workaround:** Clear any tamper state before executing lunash:>**sysconf reimage start**.
LUNA-8548	M	**Problem:** When port bonding is configured on the appliance, SSH service is sometimes lost after an appliance reboot. This issue occurs more often if the appliance is directly connected to a managed switch. **Workaround:** Log in to LunaSH using a serial connection. Ping any IP using lunash:>**network ping** <IP> to restore SSH service.
LUNA-8512	M	**Problem:** When a client is connected to multiple FM-enabled HSMs, and one HSM goes down for maintenance, is rebooted, or is busy with a long FM process, new FM processes on other HSMs experience a performance slowdown. Existing processes are unaffected. **Workaround:** None. The slowdown only lasts as long as the HSM is down, rebooting, or busy.
LUNA-8348	M	**Problem:** When adding a DNS server using REST API, configured port bonds are broken. If there is no other ethernet interface configured, you must use a serial connection to reconfigure the port bond. **Workaround:** None. Use LunaSH to configure the DNS servers.

Issue	Severity	Synopsis
LUNA-7438	M	**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). **Workaround:** Restart **CKdemo** and attempt the operation again.
LUNA-7436	M	**Problem:** Encrypt operations using DES3_CBC_PAD and specifying a NULL buffer fail (CKR_BUFFER_TOO_SMALL). **Workaround:** Manually specify a buffer size for these operations.
LUNA-7418	M	**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. **Workaround:** Log in to LunaSH as **admin** to reset the appliance user configuration.
LUNA-4134	M	**Problem:** When the Luna Network HSM is configured for IPv6 connections, a missing file error is displayed in the output from lunash:>**network show** (`/usr/lunasa/lush/Lroot/Cnetwork/network_utility_common: line 63: /usr/lunasa/bin/getIPv6Prefix: No such file or directory`). **Workaround:** This error can be safely ignored.
LUNA-4133	M	**Problem:** NTLS connection fails when the appliance has the default hostname `local_host`. **Workaround:** Assign a unique hostname to the appliance (lunash:>**network hostname** <hostname>).
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-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.

Issue	Severity	Synopsis
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 Luna Network HSM 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-3291	M	**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. **Workaround:** Manually copy the IPv6 certificates to the new client certificate directory.
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-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/crystoki.ini. Refer to the *SDK Reference Guide* for details.
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 Luna Network HSM appliance.

Issue	Severity	Synopsis
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-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 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-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.
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) 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.
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.

Issue	Severity	Synopsis
RAPI-383	M	**Problem:** REST API does not verify the NTLS client's IP against the certificate. **Workaround:** None.
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-632 LUNA-7429	M	**Problem:** When using CKdemo with HA groups, an **Attribute type invalid** error is returned. **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.

Issue	Severity	Synopsis
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.
LKX-5396	L	**Problem:** When creating an RSA key using CKDEMO, the user is mistakenly prompted for the Derive attribute (RSA key derivation is not allowed). **Workaround:** None. The value entered is dropped and can be safely ignored.
LKX-4817	L	**Problem:** FM sample applications built on a Windows platform do not automatically locate the Cryptoki library. **Workaround:** Move or copy the sample **.exe** to the main Lunaclient directory where the library is located.
LKX-4716	L	**Problem:** The **wrapcomptest** sample application hangs if it is used to query a non-FM slot or an invalid slot number. **Workaround:** Interrupt the hanging application with CTRL+C. Use the correct slot for the FM partition.
LUNA-8782	L	**Problem:** Attempting to change a destructive HSM policy to an already-existing setting (**0** to **0** or **1** to **1**) results in partitions being renamed to "**unknown1**", "**unknown2**", etc. The partitions remain intact and are usable by clients. **Workaround:** Ensure that your policy change commands are correct. If you did not mean to change the destructive policy and want to keep your existing partitions, you can rename them with lunash:>**partition rename**.
LUNA-3511	L	**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. **Workaround:** None.
LUNA-3276	L	**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. **Workaround:** Do not use spaces when naming your custom install directory.
LUNA-3126	L	**Problem:** After running lunash:> **hsm ped connect** on an uninitialized 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.
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.

Issue	Severity	Synopsis
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.
RAPI-1096	L	**Problem:** After modifying the webserver settings the **apiversion** under **/api/lunasa** becomes 0. **Workaround:** Restart the webserver service.
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.

Issue	Severity	Synopsis
CPP-2380	L	**Problem:** When running the **MiscCSRCertificateDemo.java** sample, a null pointer exception occurs. **Workaround:** None.
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
LUNA-8881	H	**Problem:** Application cannot change CKA_EXTRACTABLE default value via JSP. **Resolved:** Fixed in Luna HSM Client 10.1.
LUNA-10915 SH-3162	M	**Problem:** When you delete a key from an HSMoD service, CKlog displays an incorrect object handle. **Resolved:** Fixed in Luna HSM Client 10.1.
LUNA-8780	M	**Problem:** One-step NTLS fails when the appliance's SSH host key changes or when connecting for the first time. **Resolved:** Fixed in Luna HSM Client 10.1.
LUNA-8758	M	**Problem:** Command output of **vtl examineCert** and **vtl fingerprint** are reversed. **Resolved:** Fixed in Luna HSM Client 10.1.
LUNA-8810	L	**Problem:** Minimal Luna HSM Client tar file has an additional character that could affect customer scripts. **Resolved:** Fixed in Luna HSM Client 10.1.

Revision History

This section describes revisions made to this CRN since the initial release.

Revision A: 30 October 2019

> Initial Release

Revision B: 03 December 2019

> Correction: Windows 10, Server 2016, and Server 2019 device drivers included with Luna HSM Client 10.1 are signed by Microsoft and fully compatible with Windows Secure Boot.

Revision C: 09 January 2020

> Added to **Advisory Notes**: "Luna HSM Client 10.1 Replaces Version 7.5" on page 4

> Clarification: Luna Network HSM and HSM on Demand support different client operating systems. Refer to "Supported Operating Systems" on page 7 for details.

> BIP32 keys can now be cloned between Luna partitions and HSMoD services.

Revision D: 25 June 2021

> Revised **Advisory Note**:

- "Older JAVA versions require patch/update" on page 4

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 Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access is governed by the support plan negotiated between Thales and your organization. Please consult this plan for details regarding your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems and create and manage support cases. It offers 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.

> **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 (Contact Us).