THALES

Thales Luna HSM Client 10.2.0 for Luna PCIe HSM

CUSTOMER RELEASE NOTES

Issue Date: 25 June 2021

Document Part Number: 007-000556-002 Rev. C

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 PCIe HSM secures your sensitive data and critical applications by storing, protecting and managing your cryptographic keys in a high-assurance, tamper-resistant, low-profile PCIe card that offers market-leading performance. Luna PCIe HSM provides applications with dedicated access to a purpose-built, high-performance cryptographic processor. You can quickly embed this cost-efficient solution directly into your servers and security appliances for FIPS 140-2 validated key security.

Luna PCIe HSM is installed directly into an application server to provide PKCS#11-compliant cryptographic services.

Release Description

Luna HSM Client release 10.2.0 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 10.2.0 for Luna PCIe HSM introduces the following new features and enhancements:

New Luna HSM Client Operating System Support

Luna HSM Client 10.2.0 can be installed on the following new operating systems:

- Windows Server Core 2016/2019
- Red Hat Enterprise Linux 8 (including variants like CentOS 8)

Support for New Mechanisms in Luna HSM Firmware 7.4.2

Luna HSM Client 10.2.0 includes support for Luna HSM firmware 7.4.2 mechanisms.

- 3GPP Cryptography for 5G Mobile Networks
- SM2/SM4 Support
- SHA-3 Function Support

> **NOTE** Refer to "Special Considerations for PED-Authenticated Luna HSMs" on page 8 before installing Luna HSM firmware 7.4.2.

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.

Red Hat Enterprise Linux / CentOS 6 Will Not be Supported in Future Releases

Luna HSM Client 10.2.0 is the last version that will support RHEL 6 and related operating systems. If you plan to install future client updates, consider updating your clients to RHEL 7 or 8.

Luna HSM Firmware 7.4.1 is No Longer Available

Luna HSM firmware 7.4.1 is no longer available for download from the Thales Customer Portal. Thales recommends that all customers using HSM firmware version 7.4.1 update to 7.4.2 or higher.

Luna HSM Client 7.5 is No Longer Available

Luna HSM Client 7.5 is no longer available for download from the Thales Customer Portal. Thales strongly recommends that all customers using version 7.5 update their client software to 10.1 or higher.

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.

Support for 32-bit OS Platforms is Ending

Starting with Luna HSM Client 10.1.0, 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, or 7.4), 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-7585: 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.

In cases where a derived key must be extractable, add the following line to the **java.security** file:

```
com.safenetinc.luna.provider.createExtractablePrivateKeys=true
```

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 PCIe 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**.

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.

Supported Operating Systems

This section lists the supported operating systems for the Luna HSM Client and Remote PEDserver.

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 10.2.0 on the following 64-bit operating systems:

Operating System	Version	Secure Boot	DPoD HSM on Demand
Windows	10	Yes	Yes

Operating System	Version	Secure Boot	DPoD HSM on Demand
Windows Server	2019 (Standard/Core)	Yes	Yes
	2016 (Standard/Core)	Yes	Yes
	2012 R2	No	Yes
Red Hat Enterprise Linux (including variants like CentOS and Oracle Enterprise Linux)	8	No	Yes
	7	No	Yes
SuSe Linux (minimal client only)	12.4	No	No
	11.4	No	No
Ubuntu *	14.04	No	No
	18	No	No

* 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 and newer requires the advanced version of Oracle Java 7/8.
- JCA within OpenJDK 7/8/9/10/11
- OpenSSL
- Microsoft CAPI
- Microsoft CNG

Server Compatibility

The Luna PCIe HSM conforms to the PCIe 2.0 standard and requires a PCIe x4 or higher slot. There are no known incompatible servers at this time.

> **NOTE** Do not install the Luna PCIe HSM into a slot reserved for a dedicated function, such as video. If you do, the host system might not boot successfully.

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.
- 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	10.2.0
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
	7.3.3, 7.4.0, 7.4.1	7.4.2*
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 PED-Authenticated Luna HSMs" on the next page 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 PED-Authenticated Luna HSMs" below)
- Luna firmware v. 7.0.3 (factory-shipped version)
- Luna firmware v. 7.0.2 (see F5 note, below)

Special Considerations for PED-Authenticated Luna HSMs

Refer to the following table for special firmware 7.3.3 and 7.4.2 update procedures for PED-authenticated HSMs. These procedures apply depending on what firmware version was used to create the application partitions. The install paths described in "Valid Update Paths" on the previous page apply.

Luna HSM Client 10.2.0, or a patched version of Luna HSM Client 7.4.0, is required to make full use of firmware 7.4.2 capabilities.

Partition created in HSM at firmware version	Procedure
7.0.3, 7.3.3	Normal firmware update procedure (refer to HSM documentation)
7.1.0, 7.2.0, 7.3.0, or 7.4.0 with Partition Policy 15 set to ON*	Normal firmware update procedure (refer to HSM documentation) - EXCEPT the Partition SO must reset the challenge secret(s) after the firmware update, so that partition objects become accessible again.
7.1.0, 7.2.0, 7.3.0, or 7.4.0 with Partition Policy 15 set to OFF*	1. Before updating firmware, back up your partition contents. This step is essential as access to the partition will be lost after the firmware update. 2. Update your HSM to firmware version 7.3.3 or 7.4.2 (refer to "Valid Update Paths" on the previous page). 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.

Recommended Minimum Versions

Generally, Thales recommends that you always keep your HSM firmware 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	Luna HSM Firmware
Luna PCIe HSM 7 Minimum Recommended Configuration	7.2	7.2.0
		7.0.3
Luna PCIe HSM 6 Minimum Recommended Configuration for migration to Luna HSM 7	7.2	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 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: List of known issues from Luna HSM Client 10.2.0

Issue	Synopsis
LUNA-14009	**Problem:** When running **cmu verifyhsm**, the interactive mode does not prompt for a challenge string, and fails with "**Parameters missing**". **Workaround:** Always specify a challenge string: **cmu verifyhsm -challenge "**<string>**"**
LUNA-13907	**Problem:** When requesting a certificate (**cmu requestcertificate**) using the wrong attribute to specify the private key, an incorrect error message is thrown ("**Signing key not found**"). **Workaround:** Use **-privatehandle** to specify a key on a Luna partition, and **-privateouid** on an HSMoD service.
LUNA-13762	**Problem:** The Windows Device Manager sometimes displays incorrect driver version **10.2.0.1** for Luna PCIe HSM and Luna Backup HSM. **Workaround:** Can be safely ignored. The correct driver version is **10.2.0.111**.
LUNA-13144	**Problem:** Using Luna HSM Client 10.2.0, some of the new mechanisms available in Luna firmware 7.4.2 appear in LunaCM and **ckdemo** as "Unknown Mechanism Type". They are listed correctly in **multitoken**. **Workaround:** In the Luna API, you can always call mechanisms by name or by vendor code. The unknown mechanisms are listed by vendor code below: CKM_SM2DSA 0x80000b21 CKM_SM3_SM2DSA 0x80000b22 CKM_SHA1_SM2DSA 0x80000b23 CKM_SHA224_SM2DSA 0x80000b24 CKM_SHA256_SM2DSA 0x80000b25 CKM_SHA384_SM2DSA 0x80000b26 CKM_SHA512_SM2DSA 0x80000b27
LUNA-11367	**Problem:** On Solaris, attempting to perform operations on an HSM in Secure Transport Mode returns an unhelpful error (CKR_UNKNOWN) instead of the correct CKR_CMD_NOT_ALLOWED_HSM_IN_TRANSPORT. **Workaround:** Refer to the documentation for instructions on recovering the HSM from STM.

Issue	Synopsis
SH-4987	**Problem:** When creating a self-signed certificate with **cmu selfsigncertificate**, additional characters are added to the specified serial number. **Workaround:** None. Use **cmu getattribute** to note the actual serial number assigned to the certificate.

Table 2: List of known issues from previous releases

Issue	Synopsis
LUNA-13780	**Problem:** Importing a DSA public key to a partition using **cmu import** fails with "Certificate invalid" error. **Workaround:** None.
LUNA-13761	**Problem:** On Linux clients, when running **cmu selfsigncertificate** with no arguments specified, **cmu** fails to prompt the user for the relevant object handles/OUIDs, even if multiple valid keypairs exist on the partition. **Workaround:** Always specify the object handles/OUIDs of the desired keypair using **-publichandle** and **-privatehandle** or **-publicouid** and **-privateouid**.
LUNA-13176	**Problem:** On Linux, selecting only the PEDserver component during client installation installs all available client components. **Workaround:** Uninstall the undesired components.
LUNA-13175	**Problem:** Code comment mistakenly appears in the output for some **vtl** commands: `Note: Aux cert printing function deprecated in OpenSSL 1.1.0 - reimplement` **Workaround:** Message can be safely ignored.
LUNA-12822	**Problem:** CKDEMO option **(39) Get OUID** reports object OUIDs with extra zeroes appended. **Workaround:** Use option **(24) Get Attribute** to view the correct OUID.
LUNA-12471	**Problem:** In LunaProvider, some operations prohibited in FIPS mode (insufficient key size, for example) fail with an unhelpful **NULL** error. **Workaround:** Consult documentation for permitted FIPS mode operations.
LUNA-11724	**Problem:** When setting up a DPoD HSM on Demand service on Windows, running the **setenv** script by right-clicking and selecting "Run as Administrator" causes the operation to fail with the error: ``The argument `setenv.ps1` to the -File parameter does not exist. Provide the path to an existing `.ps1` file as an argument to the -File parameter`` **Workaround:** Run the **setenv** script in an already-open Administrator command prompt. On Windows Server, the command prompt is always opened with Administrator privileges.

Issue	Synopsis
LUNA-11448	**Problem:** Occasionally, after uninstalling the client software, client binaries remain in the installation directory. **Workaround:** These can be safely deleted. To keep your configuration when updating to a new client version, do not delete the following files/directories: > **/cert** > **/PedClient_service** > **/softtoken** > **crystoki.ini/Chrystoki.conf**
LUNA-11269	**Problem:** When an HSMoD service is a member of an HA group, some events (such as the HSMoD member being dropped and its connection then re-established) are not recorded in the HA log file. **Workaround:** None.

LUNA-11229	**Problem:** Occasionally, changing the active slot in LunaCM results in objects not being correctly displayed by lunacm:>**partition contents**, even though the Crypto Officer remains logged in on that slot.
	`The 'Crypto Officer' is currently logged in. Looking for objects`
	`accessible to the 'Crypto Officer'.`
	`No objects viewable to 'Crypto Officer' are currently stored in the partition.`
	Workaround: Log in as Crypto Officer again and retry lunacm:>**partition contents**.

LGX-2032	**Problem:** The Luna G7 Backup HSM driver fails to uninstall on Windows, causing subsequent client install/uninstall issues. **Workaround:** If you encounter this issue, contact Thales Customer Support ("Support Contacts" on page 17).
LUNA-11117	**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	**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	**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	Synopsis
LUNA-11017 SH-4282	**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	**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	**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.
LKX-5545	**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 (lunacm:>**hsm restart**).
LKX-5353	**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	**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	**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	**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.
LKX-4868	**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	**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.

Issue	Synopsis
LKX-4776	**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 the **fmrecover** utility, and restart the FM application if necessary.
LKX-4266	**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	**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-11230	**Problem:** After enabling FMs by turning on HSM policy 50, the user is unable to re-initialize the HSM. **Workaround:** Manually add the following entry to the **Misc** section of th client configuration file (**crystoki.ini**/**Chrystoki.conf**): `LoginAllowedOnFMEnabledHSMs=1`
LUNA-7438	**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	**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-3108	**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	**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	**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	**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 PCIe HSM appliance.

Issue	Synopsis
LUNA-2445	**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-2268	**Problem:** The deprecated LunaCM command **hsm reset** can still be run on a PCIe HA slot, causing LunaCM to crash. **Workaround:** If you encounter this crash, restart LunaCM. Use **hsm restart** instead.
LUNA-2261	**Problem:** "CKR_DATA_INVALID" on wrap/unwrap with **multitoken** on AIX and Solaris clients. **Workaround:** None.
LUNA-2252	**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	**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	**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	**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	**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	**Problem:** When trying to run the **HALogin.java** script, a CKR_UNKNOWN error is returned. **Workaround:** None. Do not use the **HALogin.java** sample.
CPP-2368	**Problem:** The **hagroup list** command returns an error. **Workaround:** Run the **hagroup list** command again. The second attempt should be successful.
CPP-632 LUNA-7429	**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	Synopsis
CPP-626 CPP-624	**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	**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-5372	**Problem:** Partition utilization metrics reports a different serial number (hardware SN) for the admin partition than other LunaCM commands. **Workaround:** This information can be safely ignored.
LKX-4942	**Problem:** When the HSM is in a tampered state, the **ctfm** utility produces a confusing error (CKM_INVALID_ENTRY_TYPE). **Workaround:** Check for and clear any tamper state before using **ctfm**.
LKX-4817	**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	**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-3511	**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	**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-2103	**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-218	**Problem:** You cannot add a host or network route using the LunaSH **network route add** command without including the gateway value. **Workaround:** None.

Issue	Synopsis
CPP-3404	**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-2960	**Problem:** LunaCM hangs on exit on Windows 2016. **Workaround:** End the LunaCM instance using the Task Manager.
CPP-2925	**Problem:** When the **cklog** library is configured, an **error.txt** file containing extraneous messages may be created. **Workaround:** None.
CPP-2380	**Problem:** When running the **MiscCSRCertificateDemo.java** sample, a null pointer exception occurs. **Workaround:** None.
CPP-1249 LUNA-1681	**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	**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 3: List of resolved issues

Issue	Synopsis
LGX-1295	**Problem:** When using a one-time password to initialize the Luna G7 Backup HSM's RPV (orange PED key), including the **-pwd** option before **-ip** or **-hostname** causes the command to fail. **Resolved:** Fixed in Luna HSM Client 10.2.0.
LUNA-11616	**Problem:** If the client fails to resolve the DPoD service's DNS hostname, other client slots fail to load in LunaCM. **Resolved:** Fixed in Luna HSM Client 10.2.0.
LUNA-11447	**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. **Resolved:** Fixed in Luna HSM Client 10.2.0.

Issue	Synopsis
LGX-1844	**Problem:** Luna G7 Backup HSM does not appear as a slot in LunaCM if **ShowAdminTokens = no** in the Luna HSM Client configuration file (**Chrystoki.conf/crystoki.ini**). **Resolved:** Fixed in Luna HSM Client 10.2.0.
LGX-1149	**Problem:** When backing up objects to a G7-based Backup HSM from user partitions hosted on HSMs running older firmware, differences in the size of the metadata associated with the objects may cause the backup partition to become full before all of the objects are backed up, resulting in the following error message before all of the objects have been backed up: <CKR_CONTAINER_OBJECT_STORAGE_FULL> **Resolved:** Fixed in Luna HSM Client 10.2.0.

Revision History

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

Revision A: 14 April 2020

> Initial Release

Revision B: 28 May 2020

> Added to **Advisory Notes**:

- "Red Hat Enterprise Linux / CentOS 6 Will Not be Supported in Future Releases" on page 3
- Clarified **java.security** fix to "Resolved Issue LUNA-7585: Java DERIVE and EXTRACT flag settings for keys injected into the HSM" on page 4

> Added to **Resolved Issues**: "LGX-1295" on the previous page

Revision C: 25 June 2021

> Revised **Advisory Note**:

- "Older JAVA versions require patch/update" on page 3

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).