SafeNet HSM 5.4.9 Client

TECHNICAL NOTE

Contents

Release Description

This client software patch release introduces some new features and updates.

Note: Client Release 5.4.9 accumulates changes since release 5.4.2 (patch on 5.4.1), including the features described below, and in the Resolved Issues table.

For Windows, patch release 5.4.9 can be applied to Client version 5.4.1 or 5.4.2, using the installer (LunaClient.msi), or can be installed on a computer with no pre-existing LunaClient.

For Linux, install.sh installs the full LunaClient on a system that does not currently have LunaClient installed.

DELTA: Revision B of this document replaces Revision A because the Linux installer has been updated (January 2017) to a full client installation, replacing the original patch-only installer (December 2016).

This patch is tested for 64-bit client on Windows and Linux 64-bit platforms only.

Features and Updates

OpenSSL version is updated

An updated version of openssl is installed on the client, for improved security and to satisfy dependencies.

HA actively monitors appliance recovery

HA now performs active monitoring of appliance recovery and re-adds the HA member to the group without waiting for the next crypto operation.

HA Failover withstands member deactivation and reconnects on activation of member partition

The following scenarios are addressed in 5.4.9 Client:

- When an application starts up the HA system ensures that the partition is activated.
- If a member has failed, during recovery the system checks that the partition is activated and confirms activation before the member is added back to the group.
- When a new member is being added to an HA group, the system checks whether or not the new member partition is activated and subsequently verifies activation before the member is successfully added to the HA group.

RHEL 7.x is supported

RedHat Enterprise Linux 7.x is now supported for SafeNet 5.4.9 and newer.

RNG/GetRandom is parallelized

GetRandom and HSM Random Number Generation operation is now parallelized to support load balancing in HA configurations. Performance improvements appear to be approximately linear with additional HA group members.

Windows Installer Updates

The Windows installer now allows the option to patch an existing LunaClient, and does not require a separate unistall action prior to installation of the 5.4.9 client. The same Windows client installer can also perform a full installation where no previous LunaClient exists.

Support for CK_GCM_PARAMS

Use of CK_GCM_PARAMS is supported , and a previously used proprietary ID for the AES/GCM cipher mechanism is replaced by the standard value 0x1087 (formalized with PKCS#11 v2.3).

Updates

See "Resolved Issues" on page 5, for issues addressed in this patch release.

Advisory Notes

At this time, we are examining an issue where the library can crash due to a collision when a client application attempts to re-initialize or to perform cryptographic operations and also to run C_Finalize at the same time. The PKCS#11 standard notes that C_Finalize behavior is undefined if it is called while other threads of the application are making crypto calls.

Customers using the JavaSP library should note that calling reinitialize() on a LunaSlotManager instance incorporates calling C_Finalize(). Thus, precautions must be taken when developing a client application using JavaSP library.

Upgrade Procedure

Upgrade Paths

The following tables demonstrate the supported upgrade paths. For Windows users only, if your client software is at a version lower than the indicated starting version, you should simply uninstall your existing client and install the 5.4.9 patch as a completely new LunaClient installation. For Linux users, if any version of LunaClient software is installed, uninstall it before running install.sh.

Client Software

Starting Client Software Version	End Client Software Version
5.4.1 or 5.4.2	5.4.9

Compatible Components

Component	Version
Luna SA appliance software	5.3.13
Luna SA HSM firmware	6.10.9 (FIPS validated; not all features available) or 6.20.2 (feature support; not FIPS validated)

Supported Platforms

Operating System	Version	64-bit client
Windows	2008 R2	Yes
	2012 R2	Yes
Redhat Enterprise Linux (includes variants like CentOS)	5.x	Yes
	6.x	Yes
	7.x	Yes

Upgrade Outcomes

The 5.4.9 patch release changes only the LunaClient software version. HSM firmware, and Network Appliance software are not affected.

Upgrading the Client Software

For Linux, ensure that the operator performing the update has root privilege.

The 5.4.9 patch package consists of these files:

a. Install-patch.sh

b. sw-patch.tar

For Windows, ensure that the operator performing the update has Administrator privilege.

To upgrade the client software to SafeNet HSM 5.4.9

1. Backup any important configuration settings, logs or other material that must be preserved. The patch software is designed to preserve settings, and files that have been changed or added since the original client software installation, but it is always prudent to perform your own backup before making software changes.
2. Stop any application that is using SafeNet HSM(s).
3. Install the SafeNet HSM 5.4.9 patch software. The method you use is platform specific, as follows:
   - **Windows** Run the LunaClient.msi installation program and respond to the prompts as they appear. Choose the desired software components from the list.
   - **Linux/Unix** Change directory to the folder where the patch package is located, run the install.sh installation script (without arguments) and respond to the prompts as they appear.
4. Reboot the client host computer to clear the old drivers from memory and launch updated drivers.
5. For Windows hosts, you can verify that the patch installed successfully by looking at Control Panel > Programs and Features; it shows the new version number.
   For Linux hosts, the patch script provides success messages as each step completes.
6. After reboot, restart your applications.

Known Issues

This patch collects several fixes, along with the feature improvements. Fixes are listed below, in the Resolved Issues section. Any issues not addressed there are still outstanding; refer to the Release 5.4 Customer Release Notes, Known Issues table (crn_luna_hsm_5-4.pdf).

Resolved Issues

This section lists issues fixed in the product at the time of release. The following table defines the severity of the issues listed in this section.

Priority	Classification	Definition
C	Critical	No reasonable workaround exists.
H	High	Reasonable workaround exists.
M	Medium	Medium level priority problems.
L	Low	Lowest level priority problems.

List of Resolved Issues

Issue	Severity	Synopsis
LHSM-32292	C	**Problem:** Issues with IIS and TLS 1.1 and TLS 1.2. Websites stop

Issue	Severity	Synopsis
Issues with IIS and TLS 1.1 and TLS 1.2. Websites stop working when SSL 2.0, SSL 3.0 and TLS 1.0 are disabled in IE..		working when SSL 2.0, SSL 3.0 and TLS 1.0 are disabled in IE.. **Fixed:** Fixed in one of the patches delivered in SafeNet LunaClient software version 5.4.9.
SPCD-306 Client Propagation: LunaProvider is unusable in an environment where the provider is dynamically loaded.	H	**Problem:** Users of cryptographic modules in an application server environment want their application to load the LunaProvider dynamically rather than having it as part of the java.security list. This affords the ability to ensure other applications running in the application server do not accidentally use the HSM. **Fixed:** Fixed in SafeNet LunaClient software version 5.4.9.
SPCD-167 Integration With NDES over SCEP protocol	H	**Problem:** Generating a certificate request that uses a challenge response generated from the NDES web enrollment fails. Unwrapping any other self generated cert on the HSM is successful but when NDES tries to do so, it fails. **Fixed:** Fixed in SafeNet LunaClient software version 5.4.9.
LHSM-32258 Luna KSP freezes after creating 251 key pairs.	H	**Problem:** Luna KSP freezes after creating 251 key pairs. **Fixed:** Fixed in one of the patches delivered in SafeNet LunaClient software version 5.4.9.
SPCD-161 LunaProvider JAR, keyStore.setKeyEntry) Operation of updating certificate chain results in all the old certificates being present on the HSM as well as the new ones.	H	**Problem:** With LunaSA 5.2 and above, LunaProvider JAR, keyStore.setKeyEntry) Operation of updating certificate chain results in all the old certificates being present on the HSM as well as the new ones. **Fixed:** Fixed in SafeNet LunaClient software version 5.4.9.
SPCD-557 HA - monitor failures related to partition deactivation	M	**Problem:** Ensure that any HSM that is introduced as part of the HA group has the partition activated. **Fixed:** Added to SafeNet LunaClient software version 5.4.9.
SPCD-556 HA Active Monitoring	M	**Problem:** HA must actively monitor appliance recovery HA should perform active monitoring of appliance recovery and re-add the HA member to the group without waiting for the next crypto operation. **Fixed:** Added to SafeNet LunaClient software version 5.4.9.

Issue	Severity	Synopsis
SPCD-199 Client patch Installer	M	**Problem:** Allow customers to easily apply Luna client patch by using an automated installer. **Fixed:** Added to SafeNet LunaClient software version 5.4.9.
SPCD-173 upgrade OpenSSL	M	**Problem:** Upgrade the OpenSSL version for security and compatibility. **Fixed:** Fixed in SafeNet LunaClient software version 5.4.9.
SPCD-166 random number generation is not load balanced in HA	M	**Problem:** When in HA the random number generation is no faster than a single device. **Fixed:** Fixed in SafeNet LunaClient software version 5.4.9.
SPCD-164 JVM Crashes because of an uninitialized variable	M	**Problem:** A bug in the HA recovery code leads to an uninitialized variable being used during a CA_DestroyMultipleObjects call, which causes our library to crash. **Fixed:** Fixed in SafeNet LunaClient software version 5.4.9.
SPCD-162 SA5.x: SSL with Luna java provider is much slower compared to SA4 performance	M	**Problem:** Upgrade the OpenSSL version for security and compatibility. **Fixed:** Fixed in SafeNet LunaClient software version 5.4.9.
SPCD-116 Support 5.3 or 5.4 client on RHEL 7.x	M	**Problem:** Customer needs official support for 5.3 or 5.4 Luna client on RHEL 7.x. **Fixed:** Fixed in SafeNet LunaClient software version 5.4.9.
LHSM-25647 NTE_BAD_FLAGS error when AlternateSignatureAlgorithm = true in policy file	M	**Problem:** AlternateSignatureAlgorithm configures the CA to support the PKCS#1 V2.1 signature format for both the CA certificate and certificate requests. PKCS#1 V2.1 implies RSA-PSS. In general, the CSP and KSP should support both RSA-PSS and RSA-OAEP. **Fixed:** Fixed in one of the patches delivered in SafeNet LunaClient software version 5.4.9.
LHSM-19364 Support CK_GCM_ PARAMS (which was added by the 2.3 p#11 spec), so that it can be used with the AES/GCM cipher mechanism	M	**Problem:** Original SafeNet-Gemalto support for GCM was based on PKCS11 v2.20 amendment 5 Draft 1. Need to support CK_GCM_PARAMS (which was added by the PKCS#11 version 2.3 spec), so that it can be used with the AES/GCM cipher mechanism, and replace Safenet's proprietary mechanism ID for the AES/GCM cipher (0x80000113) with the standard ID, which is 0x1087.

Issue	Severity	Synopsis
		Fixed: Fixed in one of the patches delivered in SafeNet LunaClient software version 5.4.9.
HSMAI-363 Issue with IIS 8.5 integration with Luna 6.0 on WIndows 2008R2 & Windows 2012 R2	M	**Problem:** IIS integration with Luna 6.0 on Windows 2008 R2 & Windows 2012 R2 works fine with default configuration, but problems appear when applying script to restrict insecure cipher suites. Fixes in CSP and KSP to be researched. **Fixed:** Fixed in one of the patches delivered in SafeNet LunaClient software version 5.4.9.

Support Contacts

Contact method	Contact	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	Global	+1 410-931-7520
	Australia	1800.020.183
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.1302.029
	Singapore	800.863.499
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608

Contact method	Contact
Web	www.safenet-inc.com
Support and Downloads	www.safenet-inc.com/support Provides access to the Gemalto Knowledge Base and quick downloads for various products.
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.