SafeNet HSM 6.3.1

TECHNICAL NOTE

Issue Date: 31 October 2018

Document Part Number: 007-000241-001 Rev. A

Contents

Product Description

The SafeNet HSM (hardware security module) family provides FIPS-certified, PKCS#11-compliant cryptographic services in a high-performance, ultra-secure, and tamper-proof hardware package. By securing your cryptographic keys in hardware, SafeNet HSMs provide robust protection for your secure transactions, identities, and applications. They also offer high-performance encryption, decryption, authentication, and digital signing services. SafeNet HSMs are available in the following form factors which offer multiple levels of performance and functionality:

SafeNet Network HSM

SafeNet Network HSM is a network-based, Ethernet-attached HSM appliance that offers up to 100 HSM partitions, high-availability configuration options, remote management PED and backup, and dual hot-swappable power supplies. SafeNet Network HSM provides cryptographic services for network clients that are authenticated and registered against HSM partitions. Two models of SafeNet Network HSM are available – password authenticated and PED authenticated - in two performance variants, the SafeNet Network HSM-1700 and SafeNet Network HSM-7000, which are capable of 1700 and 7000 (RSA 1024-bit) signings per second respectively.

Release Description

SafeNet HSM Release 6.3.1 is a field update of the SafeNet Network HSM version 6.3 that includes new features and fixes.

We recommend that you update to appliance software version 6.3.1 if any of the following apply:

- You require the ability to configure the TLS cipher suite used in NTLS and other communication services
- You require the ability to configure the NTLS port on the appliance from the default 1792 to another port number more suitable for your deployment scenario (such as deploying in a cloud environment)
- You require a security update to address a potential NTP vulnerability (covered in CVE-2018-7183)
- You are experiencing issues with SNMP traps not logging IPMI events, such as fan or power supply failures, on your 6.3 appliance

New Features and Enhancements

The following are summaries of features new to SafeNet HSM in release 6.3.1.

Configurable NTLS port

You can now change the default NTLS listening port on the Network HSM. This gives administrators more flexibility and allows them to set the listening port to one that is more in line with their internal requirements for their deployment environment. The default NTLS port can be configured to a new port number, using the new "ntls port" command.

See "Configure the NTLS listening port on a Network HSM appliance" on page 6 for more detailed information.

[Requires SafeNet Network HSM appliance software 6.3.1; no firmware dependency]

Configurable cipher suites

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

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

See "Configure TLS cipher suites on a Network HSM Appliance " on page 7 for more detailed information.

[Requires both **the SafeNet Network HSM software 6.3.1** and **Luna HSM Client 7.2; no firmware dependency]**

Updated NTP version

The NTP version is updated to version 4.2.8p12. This addresses the potential NTP vulnerability described by CVE-2018-7183. The applicable open-source licenses for NTP version 4.2.8p12 are :

- •MIT license: MIT (https://opensource.org/licenses/mit-license.php)
- •BSD-4-Clause (http://www.gnu.org/licenses/license-list.html#OriginalBSD)

[Requires SafeNet Network HSM appliance software 6.3.1; no firmware dependency]

Advisory Notes

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

Release 6.3.1 applies an update to the appliance software only; there is no change to the firmware. In other words, after applying this patch, your currently installed firmware within the appliance remains unchanged.

The patch is intended to be applied to an existing 6.3 appliance. If your appliance has a different version of software, you must upgrade the appliance to software version 6.3 before applying this patch.

We recommend that you install this patch on all applicable HSM appliances.

Luna HSM Client version 7.2 required

Appliance software 6.3.1 is tested and verified with Luna HSM Client version 7.2 (the common client for use with both 6.3 and 7.x HSMs).

NOTE Luna client version 7.2 is required if you plan to use ‘Configurable Cipher Suites’.

Diffie-Hellman TLS Cipher Suites

After you update to 6.3.1 and reboot the appliance, the appliance will begin generating the parameters for 4096-bit DHE ciphers. This operation can take several hours, but it occurs only once for each Network HSM appliance. You will need to wait until the DH parameter generation is complete before you can use them for TLS connections.

See section "Configure TLS cipher suites on a Network HSM Appliance " on page 7 for more details.

NTP Server Might Take Slightly Longer to Connect/Disconnect After Updating to Luna 6.3.1

If you are using NTP, after you update to Luna 6.3.1 you might find that the SafeNet Network appliance takes longer to synchronize with the NTP server.

To reduce the synchronization time, specify the [-iburst] option when adding an NTP server:

sysconf ntp addserver <hostname_or_ipaddress> **-iburst**

This causes the server to more rapidly synchronize when first connecting/reconnecting.

Instructions for New Functionality

This section describes how to use the new features included in appliance software 6.3.1.

Configure the NTLS listening port on a Network HSM appliance

The default value for the NTLS listening port on the Network HSM is 1792. You can use the **ntls port** commands to view and set the NTLS listening port to a different value. The table at "APPENDIX: Network HSM Appliance standard ports " on page 17 indicates default port values for other HSM appliance services, so you know which values to avoid. It is up to you to sort out port numbers dictated by your application programs, firewall rules, etc.

Overview of steps

The overall procedure is:

1. Login to your appliance as the administrator and use the LunaSH commands to set the NTLS listening port value on the appliance.
2. Update the configuration file for each Luna client that connects to the appliance to refer to the new port value.

Viewing and Setting the NTLS listening port on the appliance

To view the current NTLS listening port value

1. Log into the appliance as "admin" or "operator" or "monitor".
2. Run the following command in LunaSH:

   lunash:> **ntls port show**

To modify the current NTLS listening port value

1. Log into the appliance as "admin" or "operator".
2. Run the following command in LunaSH:

   lunash:> **ntls port set -port** <port number>

Updating the client configuration file settings for NTLS port

On *each* client that connects to the Network HSM appliance, edit the crystoki.ini file (Windows) or the Chrystoki.conf file (Linux/UNIX).

Under the "LunaSA Client" section, modify the setting below to match the value that was set on the appliance in the previous step with the **ntls port set** command.

`ServerPortXX=<portnumber>` (where XX is the server port ID, a two-digit number with leading zero if needed)

NOTE Clients will not be able to connect to the Network appliance until you update their configuration file as noted above. The value for the ServerPort in the configuration file, and on the appliance, must be in the range 1792-65535.

Configure TLS cipher suites on a Network HSM Appliance

TLS cipher suites are used by several of the Network HSM services and features, when secure communication links are required. When a Luna client attempts to establish a TLS link with the SafeNet Luna Network HSM, the appliance negotiates with the client to find a cipher that is supported in both the Network HSM's and the client's respective lists of available/acceptable ciphers. The appliance starts with the first cipher on its list and proceeds down that list until a match is achieved with a cipher acceptable to the client.

You can use the **sysconf tls cipher** commands:

- to display the current cipher list, used by the SafeNet Luna Network HSM appliance,
- to reorder the list (placing preferred ciphers earlier in the negotiation order - that is, closer to the top of the list),
- to remove ciphers from availability (shorten the list), or
- to reset to the default cipher list.

Prerequisites

To make use of TLS ciphers, you will need Luna Client version 7.2 or greater.

Overview of Steps

The overall procedure is:

1. Update your client to Luna Client version 7.2 or greater.
2. Update your appliance to version 6.3.1 and reboot to start the TLS parameter generation. See note on Diffie-Hellman TLS cipher suites if you plan to use these.
3. Configure the desired TLS ciphers.
4. Restart NTLS, PED (or cbs) and STC services for the new TLS cipher settings to take effect.

NOTE First-time Use of Diffie-Hellman (DHE) TLS Cipher Suites After Upgrade to version 6.3.1

After updating to 6.3.1 is complete and the appliance is rebooted, the appliance begins generating the parameters for 4096-bit DHE ciphers. This operation can take approximately four hours, but it occurs only once for each Network HSM appliance. You will need to wait until the Diffie-Hellman parameter generation is complete before you can use them for TLS connections.

Please make special note of the following:

- If you restart the services before DHE parameter generation is complete, then operation resumes where it left off and continues to completion.
- If you reboot the appliance before the DHE parameter generation is complete, the parameter generation process will start over from the beginning.

Viewing and Configuring the TLS Cipher List

To view the current cipher list in use by the appliance

1. Log into the appliance as "admin" or "operator" .
2. Run the following command in LunaSH:

   lunash:> **sysconf tls cipher show**

To reorder the list, or to remove ciphers, using a command-line list

1. Log into the appliance as "admin" .
2. Run the following command in LunaSH:

   lunash:> **sysconf tls cipher set -list** <ciphername1:ciphername2:...>

Configuring the TLS Cipher List Using a Template

To export the current cipher list to a template file

1. Log into the appliance as "admin" or "operator".
2. Run the following command in LunaSH:

   lunash:> **sysconf tls cipher show -exportTemplate** <templatefilename>

To reorder the list, or to remove ciphers, using a template file

1. Log into the appliance as "admin".
2. Run the following command in LunaSH:

   lunash:> **sysconf tls cipher set -applyTemplate** <templatefilename>

Resetting the TLS Cipher List

To reset the current cipher list to match the "available" cipher list

1. Log into the appliance as "admin" .
2. Run the following command in LunaSH:

   lunash:> **sysconf tls cipher reset**

Compatibility and Upgrade Information

Release 6.3.1 is an update patch to SafeNet Network HSM appliance software 6.3.0, only. There is no firmware version dependency.

We recommend using Luna HSM Client version 7.2 (common client) with this software update, as some items in this release have a Luna HSM Client version dependency. See sections on "New Features and Enhancements" on page 3 and "Advisory Notes" on page 4 for more details.

Upgrade Paths

Component	Directly from version	To version
SafeNet HSM client software	Any	7.2.0
SafeNet Network HSM appliance software	6.3.0	6.3.1

Supported Operating Systems for SafeNet HSM Client 7.2 and Greater

This section lists the supported operating systems for the SafeNet HSM client 7.2 and greater and Remote PED server.

SafeNet Luna HSM Client

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

Operating System	Version	64-bit applications on 64-bit OS	32-bit applications on 64-bit OS	32-bit applications on 32-bit OS
Windows	10	Yes	Yes	No
	2012 R2	Yes	Yes	No
	2016	Yes	Yes	No
Redhat-based Linux (including variants like CentOS and Oracle Enterprise Linux)	6	Yes	Yes	Yes
	7	Yes	Yes	Yes

Remote PED Server

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

The PEDserver software for SafeNet Luna HSM Client version 7.2 and greater is supported on the following operating systems:

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

Supported APIs

The following APIs are supported :

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

Update Instructions

Upgrade Paths

Refer to the section "Compatibility and Upgrade Information" on page 10 earlier in this document.

NOTE When you install SafeNet Network HSM software, you displace the firmware version that was previously in standby. So, if you need FIPS validation and do not have firmware 6.10.9 in your appliance, simply contact Gemalto and download a stand-alone firmware 6.10.9 upgrade package.

Component Firmware Versions

If your SafeNet Network HSM appliance worked with appliance software 6.3.0 and whatever firmware version you have installed, then it will work with appliance software updated to 6.3.1.

Preparing for the Upgrade

Before attempting to upgrade to SafeNet HSM 6.3.1, ensure that you have satisfied the following prerequisites:

- you have the upgrade software (downloaded from the Gemalto Service Portal).
- you have the authentication credentials required to perform the upgrade.
- you have prepared your HSMs for the upgrade.

Each of these prerequisites is discussed in detail in the following sections.

Obtaining the Upgrade Software

All of the software and firmware required to upgrade to SafeNet HSM 6.3.1 is available via download from the Gemalto Support Portal (https://supportportal.gemalto.com).

NOTE Authorization codes are required to install firmware. To obtain the authorization codes for your firmware, contact SafeNet Technical Support.

The following packages are included in the upgrade software:

- SafeNet Network HSM 6.3.1 appliance software

Preparing your HSMs for the Upgrade

Perform the following tasks to prepare your HSM for the upgrade:

1. Ensure that your appliance software (for SafeNet Network HSM only)is at a starting version listed in the "Upgrade Paths" section above.
2. Connect your HSM appliance to an uninterruptible power supply (UPS), if available. Although this is not a requirement, use of a UPS is strongly recommended to ensure successful completion of all upgrade activities.

3. Backup the content of your HSM or HSM partitions to SafeNet Backup HSMs, or to Small Form-Factor Backup devices (if you have the SFF Backup option).
4. Copy the SafeNet HSM 6.3.1 upgrade software package (the downloaded tar file) to the client computer and use your favorite archiving program to untar the archive.
5. Stop all applications and services that are using the HSM.
6. Disable HSM policy 39 (Allow Secure Trusted Channel). You can re-enable this policy after upgrade.

Performing the Upgrade

Depending on the product you are upgrading you might need to upgrade the client software, appliance software, and/or the HSM firmware, as specified in the following table:

Product	Client software upgrade	Appliance software upgrade	HSM firmware upgrade
SafeNet Network HSM	See NOTE below	**Yes**	No
SafeNet PCIe HSM	No	n/a	No
SafeNet USB HSM	No	n/a	No
SafeNet Backup HSM	No	n/a	No

NOTE: Updating appliance software to version 6.3.1 also requires that you *update all Luna HSM Client instances to 7.2* (common client) in order to have the requisite ciphers available at both ends.

Upgrading the SafeNet Network HSM Appliance Software

NOTE Appliance software upgrade is a one-way operation. There is currently no way to downgrade the appliance software once a new version is applied.

NOTE Appliance software 6.3.1 is tested and verified only with Luna HSM Client version 7.2 (the common client for use with both 6.3 and 7.x HSMs).

To upgrade the SafeNet Network HSM Appliance software to Luna HSM 6.3.1

1. Copy the SafeNet HSM 6.3.1 appliance package file (.spkg) to the SafeNet Network HSM appliance you want to upgrade:
   - Windows **pscp** <path>\<partnum>**.spkg admin@**<LunaSA_hostname>:
   - Unix/Linux **scp** <path>/<partnum>**.spkg admin@**<LunaSA_hostname>:
2. Stop all client applications that are connected to the SafeNet Network HSM.
3. At the console, log in to the SafeNet Network HSM appliance using an admin-level account. The default account is admin.
4. Log in to the SafeNet Network HSM as the HSM Security Officer:

   lunash :> **hsm login**

- For SafeNet Network HSM with PED authentication, the blue PED Key is required.
- For SafeNet Network HSM with Password Authentication, you are prompted for the HSM Admin (SO) password.

5. (Optional) Verify that the upgrade package file that you copied is present:

   lunash :> **package listfile**

6. (Optional) Verify the upgrade package:

   lunash :> **package verify** <partnum>**.spkg -authcode** <authorization_code>

   Verification requires approximately 90 seconds.

7. Install the upgrade package:

   lunash :> **package update** <partnum>**.spkg -authcode** <authorization_code>

   The installation/upgrade process takes approximately 90 seconds. During that time, a series of messages are displayed that detail the progress of the upgrade. At the end of this process, the message “Software upgrade completed!” is displayed.

Returning the HSM to Operation

After performing the upgrade, you must reactivate the HSM partitions (if applicable) to return the HSM to operation.

To return the HSM to operation

1. Reactivate all partitions that were activated before the upgrade (applies to SafeNet Network HSM with PED Authentication).
2. Re-enable HSM policy 39 (Allow Secure Trusted Channel), if required.

Known Issues & Resolved Issues

The known issues for this release are the same as those listed in the SafeNet Network Appliance release 6.3.0 CRN available from the Gemalto Support Portal (https://supportportal.gemalto.com).

Resolved Issues

This section lists issues that have been resolved for the current 6.3.1 release.

List of Resolved Issues

Issue	Severity	Synopsis
LUNA-7486	H	**Problem:** SafeNet Network HSM appliance 6.3 is unable to log any IPMI event. **Fixed:** Fixed in 6.3.1 update.
LUNA-7501	M	**Problem:** Address NTP vulnerability CVE-2018-7183 **Fixed:** Fixed in 6.3.1 update.

The resolved issues for the SafeNet Luna Network Appliance release 6.3.0 are in the 6.3.0 CRN available from the Gemalto Support Portal (https://supportportal.gemalto.com).

Support Contacts

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

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

Customer Support Portal

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

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

Telephone Support

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

Email Support

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

APPENDIX: Network HSM Appliance standard ports

The following table shows the default port assignments for various services. Some can be reassigned to different port values, in case of conflict with your applications or network rules.

Port	Protocol	Feature	Configurable	Session Initiation
22	TCP	Secure Shell (SSH)	Yes	inbound
123	UDP	Network Time Protocol (NTP)	No	outbound
161	UDP	Simple Network Management Protocol (SNMP) daemon	No	inbound
162	UDP	Simple Network Management Protocol (SNMP) trap	No	outbound
514	UDP	Remote Syslog Service	Yes	outbound
1501	TCP	Callback Service (CBS)	No	inbound
9697	TCP	Callback Service (CBS) (Remote PED enhanced)	No	inbound
1503	TCP	Remote PED multi-factor authentication	Yes	outbound
1792	TCP	NTLS (Network Trust Link Service)	Yes	inbound
1867	TCP	Host Trust Link (HTL)	No	inbound
5656	TCP	Secure Trusted Channel (STC) Application traffic SafeNet Luna HSM Client Utilities cmu, vtl, your application(s), etc. See "Secure Trusted Channel (STC)" in the *Administration Guide* for more information.	No	inbound
8443	TCP	REST API webserver	Yes	inbound