SafeNet Luna HSM 6.x

FIRMWARE VERSION 6.24.7 UPGRADE INSTRUCTIONS

Contents

007-000025-001 Rev. B 29 August 2018

Release Description

Firmware 6.24.7 is the latest FIPS-validated firmware for SafeNet HSM 6.x

This upgrade is for:

- SafeNet Network HSM
- SafeNet PCIe HSM
- SafeNet USB HSM
- SafeNet Backup HSM

The FIPS certificates for firmware versions 6.24.6 and 6.24.7 are as follows:

SafeNet PCIe Hardware Security Module and **SafeNet PCIe Hardware Security Module for SafeNet Network HSM**

- Trusted Path (PED) Authentication overall Level 3 - FIPS Certificate-3268)
- Password Authentication overall Level 2 - FIPS Certificate-3208

SafeNet USB Hardware Security Module

- Trusted Path (PED) Authentication overall Level 3 - FIPS Certificate-3211
- Password Authentication overall Level 2 - FIPS Certificate-3210

SafeNet Backup Hardware Security Module

- Trusted Path (PED) Authentication overall Level 3 - FIPS Certificate-3209

Changes Included in Firmware 6.24.7

- Support is added for GlobalPlatform Secure Channel Protocol 03 (SCP03) encoding schemes.
- For non-FIPS mode, some restrictions around DER encoding of data with CKM_RSA_PKCS are eased, to prevent problems with TLSv1.1 and earlier.
- The KDM_PRF derivation mechanism (CKM_NIST_PRF_KDF) now allows derived keys to have "Extractable" set to True.
- PKCS rule usage for mechanisms like ECDH is corrected, such that derived keys are extractable if the parent key is extractable.

Download Availability

Go to the Gemalto Support Portal https://supportportal.gemalto.com to download the relevant tar files containing the updates that you need for your HSMs.

See "Content" on page 4 to match a DOW number with the downloadable content.

Valid Update Paths

HSM	Appliance or Client version	From firmware	To firmware
SafeNet Network HSM	6.2.1, 6.2.2, or 6.3	6.10.9	6.24.7
		6.24.2	6.24.7
		6.24.3	6.24.7
		6.27.0	6.24.7 (requires firmware rollback before upgrading to 6.24.7)
SafeNet PCIe HSM	6.2.1, 6.2.2, or 6.3	6.10.9	6.24.7
		6.24.2	6.24.7
		6.24.3	6.24.7
		6.27.0	6.24.7 (requires firmware rollback before upgrading to 6.24.7)
SafeNet USB HSM	6.2.1, 6.2.2, or 6.3	6.0.8 or 6.10.9	6.24.7
		6.27.0	6.24.7 (requires firmware rollback before upgrading to 6.24.7)
SafeNet Backup HSM*	6.2.1, 6.2.2, or 6.3	6.0.8 or 6.10.9	6.24.7
		6.27.0	6.24.7 (requires firmware rollback before upgrading to 6.24.7)

NOTE Upgrade from previous firmware is supported, provided you are using one of the listed clients.

NOTE Luna SKS appliance versions 6.2.3/6.2.4 with firmware 6.25.0/6.25.1 are *not* part of the supported update paths for this firmware release.

NOTE *Refer to an important note in the upgrade instructions for the Backup HSM.

Upgrade Procedure

Prerequisites

For Network HSMs, this firmware can be applied *only* on SafeNet HSM appliances at version 6.2.1, 6.2.2, 6.3.

> ⚠ **CAUTION!** For PCIe or USB or Backup HSMs, this firmware *must* be applied from a Client version 6.2.1 or 6.2.2, or 6.3 only. If you have a previous client installed, be sure to uninstall that first, and install a supported Client version before performing the firmware upgrade.

If your firmware is newer than 6.24.7, you must perform a firmware rollback before applying the 6.24.7 firmware, as described in "If Your Firmware is Newer Than 6.24.7" on page 7.

Content

The downloadable tar files are presented via the Gemalto Support Portal, each one under a Knowledge Base (KB<number>) number/link, with an associated downloadable DOW<number> contain the following:

> DOW0002850 downloads 630-010430-023_SPKG_NetworkHSM_fwupdate_6.24.7_RevA.tar, which contains the following:

- a secure package (SPKG) for SafeNet Network HSMs (630-010430-023_SPKG_NetworkHSM_fwupdate_6.24.7_RevA.spkg)
- the authorization code (630-010430-023_SPKG_NetworkHSM_fwupdate_6.24.7_RevA.auth)

> DOW0002851 downloads 621-000019-040_fwupdate_6.24.7_PCI_HSM_RevA.tar, which contains the following:

- a firmware upgrade file (FUF) for SafeNet PCIe HSM (621-000019-040_fwupdate_6.24.7_PCI_HSM_RevA.FUF)

> DOW0002852 downloads 621-000020-038_fwupdate_6.24.7_USB_HSM_RevA.tar, which contains the following:

- a firmware upgrade file (FUF) for SafeNet USB HSM or SafeNet Backup HSM (621-000020-038_fwupdate_6.24.7_USB_HSM_RevA.FUF)

> **NOTE** Contact Technical Support for the authorization codes for the PCIe HSM or for the USB HSM / Backup HSM updates.

Upgrading the HSM Firmware

On SafeNet Network HSM, use LunaSH (the Luna Shell) to upgrade the firmware. On SafeNet PCIe HSM, SafeNet USB HSM and SafeNet Remote Backup HSM, use LunaCM to upgrade the firmware.

> **NOTE** Ensure that you have a complete backup of all cryptographic material on the HSM, before performing any upgrade. Use of a UPS is strongly recommended, to ensure successful completion of all upgrade activities.

If the Secure Recovery Key (SRK) on the HSM is enabled, it must be disabled before you can upgrade the HSM firmware. The SRK carries an external split of the HSM's Master Tamper Key (MTK) that is imprinted on the purple PED key.

When you disable the SRK, the SRV (Secure Recovery Vector) portion of the MTK is returned to the HSM, so that the SRV is no longer external to the HSM. It is only in this state that you can upgrade the HSM firmware.

After you upgrade the firmware, you can re-enable SRK, if desired, to re-imprint a purple PED key with the SRV.

To upgrade SafeNet Network HSM firmware

On SafeNet Network HSM, use LunaSH (the Luna Shell) to upgrade the firmware.

1. Copy the SafeNet HSM 6.24.7 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 HSM as the HSM admin user if you are not already logged in.

   lunash :> **hsm login**
5. Run the firmware upgrade command. The HSM will reset when the upgrade is complete:

   lunash :> **hsm update firmware**
6. Use the hsm show command to verify that the firmware upgrade was successful:

   lunash :> **hsm show**

   If the upgrade was successful, the firmware version is displayed as 6.24.7.

   NOTE If you did not reboot the appliance before upgrading the firmware (remote PED case) the following error message is displayed:

   ```
   Error:    Unable to communicate with HSM.
   Please run 'hsm supportInfo' and contact customer support.
   ```

   You can ignore the error message.
7. If you disabled the SRK prior to performing the firmware upgrade, re-enable it if desired. Refer to the SafeNet HSM documentation for details.

   If you attempted to upgrade the firmware without disabling the SRK, the firmware upgrade fails with the following error:

   ```
   Error:  'hsm update firmware' failed. (10A0B : LUNA_RET_OPERATION_RESTRICTED)
   ```
8. If you logged into the HSM using a remote PED, ensure that all client connections are terminated and then enter the following command to reboot the appliance:

   sysconf appliance reboot

To upgrade the SafeNet PCIe HSM or SafeNet USB HSM firmware

To upgrade the firmware on a SafeNet PCIe HSM, or the SafeNet USB HSM/SafeNet Backup HSM, launch the LunaCM utility on a SafeNet HSM client computer that satisfies the following conditions:

> It contains a copy of the firmware upgrade (.fuf) file with its associated firmware authentication code (.txt) file, and

> It contains the SafeNet PCIe HSM, or is connected to the SafeNet USB HSM/SafeNet Backup HSM, that you want to upgrade.

1. Copy the firmware file (<fw_filename>.fuf) from the firmware folder on the software CD to the SafeNet HSM client root directory:
   - Windows: C:\Program Files\SafeNet\LunaClient
   - Linux/AIX: /usr/safenet/lunaclient/bin
   - Solaris/HP-UX: /opt/safenet/lunaclient/bin
2. Obtain the firmware authorization code:
   a. Contact SafeNet Customer Support (support@safenet-inc.com). The firmware authorization code is provided as a .txt file.
   b. Copy the <fw_auth_code>.txt file to the SafeNet HSM client root directory:
      - Windows: C:\Program Files\SafeNet\LunaClient
      - Linux/AIX: /usr/safenet/lunaclient/bin
      - Solaris/HP-UX: /opt/safenet/lunaclient/bin
3. Launch the LunaCM utility:

Windows	1. Open a Command Prompt window: (Start > Programs > Accessories > Command Prompt). 2. Change to the SafeNet HSM client root directory: cd C:\Program Files\SafeNet\LunaClient 3. Enter the following command **Lunacm**
Linux/AIX	1. Open a terminal window and change to the SafeNet HSM client root directory: /usr/safenet/lunaclient/bin 2. Enter the following command: ./**lunacm**
HP-UX/Solaris	1. Open a terminal window and change to the SafeNet HSM client root directory: /opt/safenet/lunaclient/bin 2. Enter the following command: ./**lunacm**

3. Enter the following command to log in to the HSM. Note that the password is not required on PED-based systems:

   hsm login [**-password** <password>]

4. Enter the following command to upgrade the firmware on an attached SafeNet USB HSM:

   hsm –updateFw –fuf <fw_filename>.fuf **–authcode** <fw_authcode-filename>.txt

To upgrade the SafeNet SafeNet Backup HSM firmware

It is recommended to continue to use the factory-shipped firmware, version 6.10.9, because it is also a FIPS-validated firmware.

If you wish to upgrade to firmware 6.24.7 for access to new features, all existing partitions on the Backup HSM must be deleted prior to the upgrade. New deployments can upgrade directly.

If Your Firmware is Newer Than 6.24.7

If you have an HSM with newer firmware (example HSM Appliance 6.3 with firmware 6.27.0) and you wish to install the FIPS-validated 6.24.7 firmware, you must perform a firmware rollback, which is a destructive operation (all partitions and cryptographic objects are destroyed.

> ⚠ **CAUTION!** The rollback operation is destructive to application partitions and contents, so perform backups, as necessary, before rolling back.
>
> After rollback, the no-longer-valid client/partition assignment configuration files remain, and must be cleared before you create any new partitions. HSM initialization clears those files and is a **required** operation following firmware rollback.

In the Network HSM appliance, you can have an uploaded newer firmware version on the appliance file system, ready to install.

For SafeNet PCIe HSM and SafeNet USB HSM, you can have newer firmware in the host file system, ready to install.

To roll back Network HSM firmware

1. In Luna Shell, use command **hsm firmware show** to verify the HSM's current firmware version and the available rollback version:

```
lunash:>hsm firmware show

   Current Firmware:                  6.27.0
   Rollback Firmware:                 6.10.9
   Upgrade Firmware:                  N/A

Command Result : 0 (Success)
```

2. Run the **hsm firmware rollback** command:

```
lunash:>hsm firmware rollback

WARNING: This operation will rollback your HSM to the previous firmware version !!!

         (1) This is a destructive operation.
         (2) You will lose all your partitions.
         (3) You might lose some capabilities.
         (4) You must re-initialize the HSM.
         (5) If the PED use is remote, you must re-connect it.
```

```
Type 'proceed' to continue, or 'quit' to quit now.

> proceed
Proceeding...

Rolling back firmware.  This may take several minutes.

Command Result : 0 (Success)
```

3. Verify the rollback with the **hsm show** command:

```
lunash:>hsm show

   Appliance Details:
   ==================
   Software Version:               6.3.0

   HSM Details:
   ============
   HSM Label:                         mysa6
   Serial #:                          7000022
   Firmware:                          6.10.9
   HSM Model:                         K6 Base
   Authentication Method:             PED keys
   HSM Admin login status:            Not Logged In
   HSM Admin login attempts left:     3 before HSM zeroization!
   RPV Initialized:                   Yes
   Audit Role Initialized:            No
   Remote Login Initialized:          No
   Manually Zeroized:                 No

   Partitions created on HSM:
   ==========================

.... (snip)...

Command Result : 0 (Success)
```

4. Following rollback, initialize the HSM with command **hsm init** :

```
lunash:> hsm init -label mysa6

CAUTION:  Are you sure you wish to re-initialize this HSM?
All partitions and data will be erased.
Type 'proceed' to initialize the HSM, or 'quit' to quit now.
> proceed

Luna PED operation required to initialize HSM - use Security Officer (blue) PED Key
'hsm -init successful'

Command result : 0 (Success)
```

To roll back PCIe HSM firmware

1. Ensure that the host computer and, if applicable, any attached USB HSM or Backup HSM, are connected to an uninterruptible power supply.
2. Launch LunaCM.
3. Use **slot list** command to see the slot number for the desired HSM.

4. Use **slot set** command to select the slot corresponding to the HSM that is to have its firmware rolled back.
5. Use the **hsm showinfo** command to see the current firmware version and the rollback firmware version:

```
lunacm:> hsm showinfo  lunacm:> hsm showinfo

        Partition Label -> mypcie6
        Partition Manufacturer -> Safenet, Inc.
        Partition Model -> K6 Base
        Partition Serial Number -> 150022
        Partition Status -> OK
        Token Flags ->
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> Yes
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 000000000000000064a0200

        Partition Storage:
                Total Storage Space:  262144
                Used Storage Space:   0
                Free Storage Space:   262144
                Object Count:         0
                Overhead:             9280

        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***

        Firmware Version -> 6.27.0
        Rollback Firmware Version -> 6.10.9
        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   174288
                Free Storage Space:   1922864
                Allowed Partitions:   1
                Number of Partitions: 1

        License Count -> 9
                1. 621000026-000 K6 base configuration
                1. 620127-000 Elliptic curve cryptography
                1. 620114-001 Key backup via cloning protocol
                1. 620109-000 PIN entry device (PED) enabled
                1. 621010358-001 Enable a split of the master tamper key to be
stored externally
                1. 621010089-001 Enable remote PED capability
                1. 621000021-001 Performance level 15
                1. 621000079-001 Enable Small Form Factor Backup
                1. 621000099-001 Enable per-partition Security Officer

Command Result : No Error

lunacm:> hsm showinfo  lunacm:> hsm showinfo

        Partition Label -> myusbhsm
        Partition Manufacturer -> Safenet, Inc.
        Partition Model -> G5 Base
```

```
        Partition Serial Number -> 150022
        Partition Status -> OK
        Token Flags ->
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> Yes
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 000000000000000064a0200

        Partition Storage:
                Total Storage Space:  262144
                Used Storage Space:   0
                Free Storage Space:   262144
                Object Count:         0
                Overhead:             9280

        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***

        Firmware Version -> 6.27.0
        Rollback Firmware Version -> 6.10.9
        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   174288
                Free Storage Space:   1922864
                Allowed Partitions:   1
                Number of Partitions: 1

        License Count -> 9
                1. 621000026-000 K6 base configuration
                1. 620127-000 Elliptic curve cryptography
                1. 620114-001 Key backup via cloning protocol
                1. 620109-000 PIN entry device (PED) enabled
                1. 621010358-001 Enable a split of the master tamper key to be s
tored externally
                1. 621010089-001 Enable remote PED capability
                1. 621000021-001 Performance level 15
                1. 621000079-001 Enable Small Form Factor Backup
                1. 621000099-001 Enable per-partition Security Officer

Command Result : No Error
```

6. Login if you have not already done so, and run the **hsm rollbackfw** command.

```
lunacm:> hsm login

Please attend to the PED.

Command Result : No Error

lunacm:> hsm rollbackFW

You are about to rollback the firmware.
The HSM will be reset.
Are you sure you wish to continue?
```

```
Type 'proceed' to continue, or 'quit' to quit now -> proceed

Rolling back firmware. This may take several minutes.

Firmware rollback passed. Resetting HSM

Command Result : No Error
```

7. Following rollback, initialize the HSM with command **hsm init** :

```
lunacm:> hsm init -label myLuna
```

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. If you are updating from firmware below 6.22.0, the upgrade operation separates SafeNet USB HSM and SafeNet PCIe HSM administration partition and client application partitions, which causes client applications to see them as separate slots. This is a change from previous behavior. Make any necessary adjustments to your scripts and application settings.
2. If you are updating from firmware below 6.22.0, then upgrading can change slot numbering, specifically the starting slot number in a slot listing. Refer to the "Slot Numbering and Behavior" section in the *HSM Administration Guide*. Other than that adjustment, for SafeNet PCIe HSM or SafeNet USB HSM your HSM is ready as soon as the firmware update is done.
3. Reactivate all partitions that were activated before the upgrade (applies to SafeNet Network HSM with PED Authentication).

Known Issues

Issue	Severity	Synopsis
LUNA-3055	M	**Problem:** Partition serial number got cut off in firmware 6.10.9 with LunaClient 6.3.0 **Workaround:** Fixed in firmware 6.24.7. Option 1. Update the conf or ini file with correct serial number after firmware upgrade. Option 2. Remove the affected HA member and re-add to the HA group after firmware upgrade.
LUNA-3043	M	**Problem**: Objects on Backup HSM must be deleted before firmware can be updated from 6.10.9 to 6.24.7 **Workaround**: If your Backup HSM is at firmware 6.10.9, it can remain at that version (which is FIPS-validated). Firmware 6.24.7 is needed for features and fixes that are useful on cryptographic HSMs, and provide no advantage for Backup HSMs.

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.