SafeNet Authentication Service

INTEGRATION GUIDE

THALES LUNA HSM

Document Information

Document Part Number	007-000451-001
Revision	B
Release Date	9 September 2020

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

This document provides you the steps for integrating SafeNet Authentication Service (SAS) with a Luna HSM. It demonstrates how to configure a SafeNet Authentication Service (SAS) to secure the AES encryption key within a Luna HSM. Thales Luna HSM is an external hardware security module that is available for use with SafeNet Authentication Service (SAS). Luna HSM with SAS is used to secure encryption keys that protect sensitive data. Multiple Luna HSMs can be configured as a High Availability (HA) group with SAS that ensure the availability of encryption keys.

The benefits of using a Luna HSM to generate the encryption key to protect sensitive data for SafeNet Authentication Service (SAS) include:

- Secure generation, storage and protection of the private keys on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of the keys.
- HSM audit trail.
- Significant performance improvements by off-loading cryptographic operations from servers.

Supported Platforms

List of the platforms which are tested with the following HSMs:

Thales Luna HSM: Thales Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

The Thales Luna HSM on premise offerings include the Luna Network HSM, PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

The following platforms are supported:

Platforms Tested	SafeNet Authentication Service (SAS)
Windows Server 2016 Standard	SAS PCE/SPE 3.10.1
Windows Server 2016 Standard	SAS PCE/SPE 3.8.1

NOTE: Any Luna HSM version is subjected to support this integration if it is used with supported Luna Client.

Prerequisites

Before you proceed with the integration, complete the following tasks:

Configure Luna HSM

If you are using a Luna HSM, ensure the following:

1. Ensure the HSM is set up, initialized, provisioned and ready for deployment. Refer to the Luna HSM Product Documentation for more information.
2. Create a partition on the Luna HSM for use with SafeNet Authentication Service (SAS).
3. If you are using a Luna Network HSM, register a client for the system and assign the client to each partition to create an NTLS connection for the three partitions. Initialize the Crypto Officer and Crypto User roles for each registered partition.
4. Ensure that each partition is successfully registered and configured. The command to see the registered partitions is:

   ```
   C:\Program Files\SafeNet\LunaClient>lunacm.exe

   lunacm (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights
   reserved.


           Available HSMs:

           Slot Id ->              0

           Label ->                SAS_PCE_Par

           Serial Number ->        1238696045103

           Model ->                LunaSA 7.4.0

           Firmware Version ->     7.4.0

           Configuration ->        Luna User Partition With SO (PW) Key Export

           with Cloning Mode

           Slot Description ->     Net Token Slot

           FM HW Status ->         FM Ready

           Current Slot Id: 0
   ```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

   > **NOTE:** Follow the Network Luna HSM documentation for detailed steps for creating NTLS connection, initializing the partitions, and various user roles.

Configuring Luna HSM HA (High-Availability)

Please refer to the Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM appliances on Windows and UNIX systems. You must enable the HAOnly setting in HA for failover to work so that if primary stop functioning for some reason, all calls automatically routed to secondary till primary starts functioning again.

> **NOTE:** This integration is tested in both HA and FIPS mode.

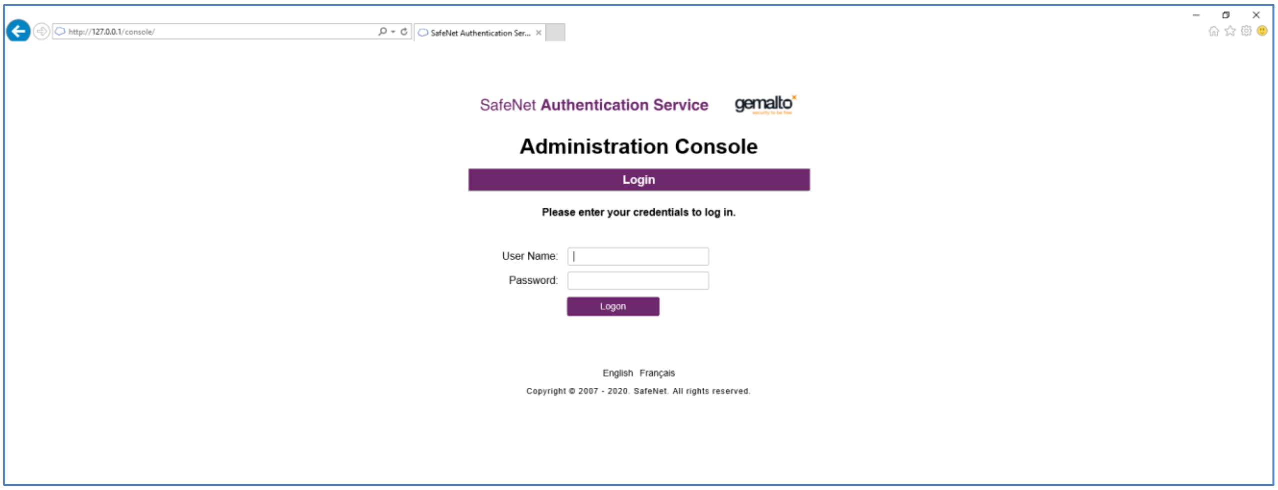
Set up SafeNet Authentication Service (SAS)

Please refer to the *SafeNet Authentication Service (SAS) Documentation* for installing and configuring the product. You can download SafeNet Authentication Service (SAS) from the Thales support site using the link given below:

https://supportportal.thalesgroup.com/csm

After installation, ensure that SAS service is running successfully by accessing the URL:

https://<hostname or IP address>/console


http://127.0.0.1/console/
SafeNet Authentication Ser...
SafeNet Authentication Service
gemalto
Administration Console
Login
Please enter your credentials to log in.
User Name:
Password:
Logon
English Français
Copyright © 2007 - 2020. SafeNet. All rights reserved.

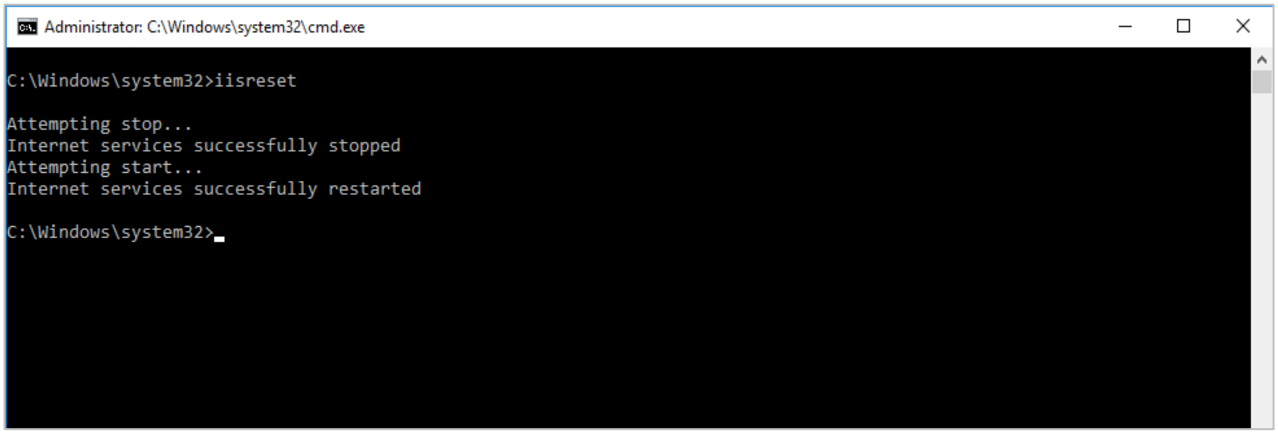
Configuring Luna HSM for SafeNet Authentication Service

This integration assumes that SAS is installed and running. Complete the following to configure the Luna HSM with SAS.

> **NOTE:** For existing SAS setups, the untouched data is not encrypted till a modification call is made. Once the data is modified, the HSM encryption is applied to it. Any existing data will remain unencrypted until it is changed.

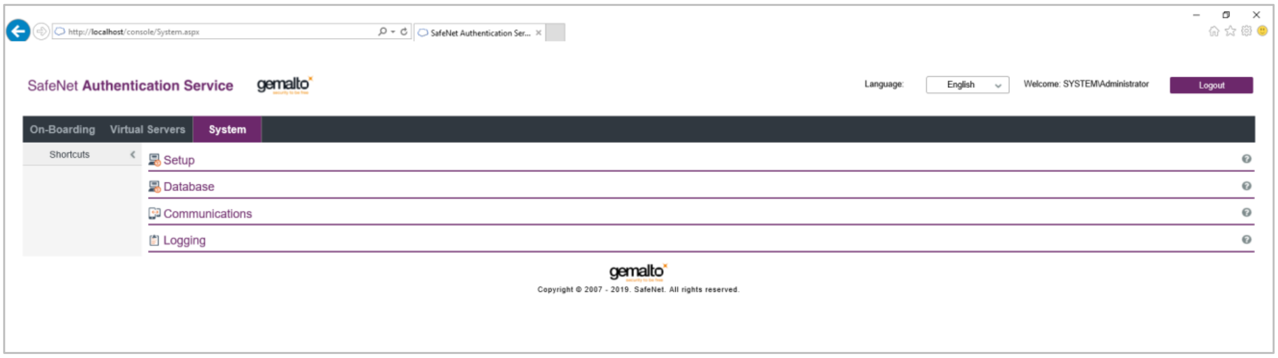
To configure Luna HSM for SafeNet Authentication Service:

1. Login to the system as an Administrator where SAS is running.
2. Copy the **cryptoki.dll** from **C:\Program Files\SafeNet\LunaClient** folder to the **C:\Windows\System32** folder.
3. Open the command prompt and run the **iisreset** command to reset IIS.

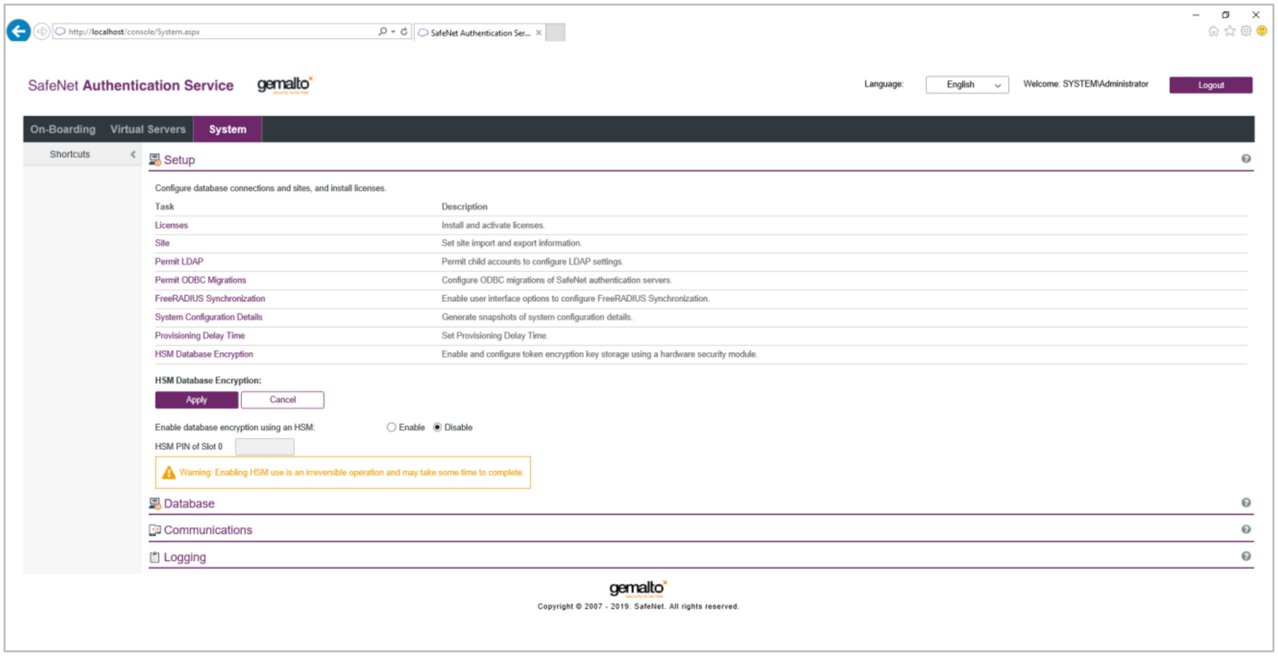


```
C:\Windows\system32>iisreset

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

C:\Windows\system32>_
```

Launch SAS Manager Console and log in to the SAS Manager Console as an Administrator.
http://localhost/console


http://localhost/console/System.aspx
SafeNet Authentication Ser...
SafeNet Authentication Service
gemalto
Language:
English
Welcome: SYSTEM\Administrator
Logout
On-Boarding
Virtual Servers
System
Shortcuts
Setup
Database
Communications
Logging
Copyright © 2007 - 2019. SafeNet. All rights reserved.

4. Navigate to **System** > **Setup** > **HSM Database Encryption**.


http://localhost/console/System.aspx
SafeNet Authentication Ser...
SafeNet Authentication Service
gemalto
Language:
English
Welcome: SYSTEM\Administrator
Logout
On-Boarding
Virtual Servers
System
Shortcuts
Setup

Configure database connections and sites, and install licenses.

Task	Description
Licenses	Install and activate licenses.
Site	Set site import and export information.
Permit LDAP	Permit child accounts to configure LDAP settings.
Permit ODBC Migrations	Configure ODBC migrations of SafeNet authentication servers.
FreeRADIUS Synchronization	Enable user interface options to configure FreeRADIUS Synchronization.
System Configuration Details	Generate snapshots of system configuration details.
Provisioning Delay Time	Set Provisioning Delay Time.
HSM Database Encryption	Enable and configure token encryption key storage using a hardware security module.

HSM Database Encryption:

Apply Cancel

Enable database encryption using an HSM: ○ Enable ● Disable

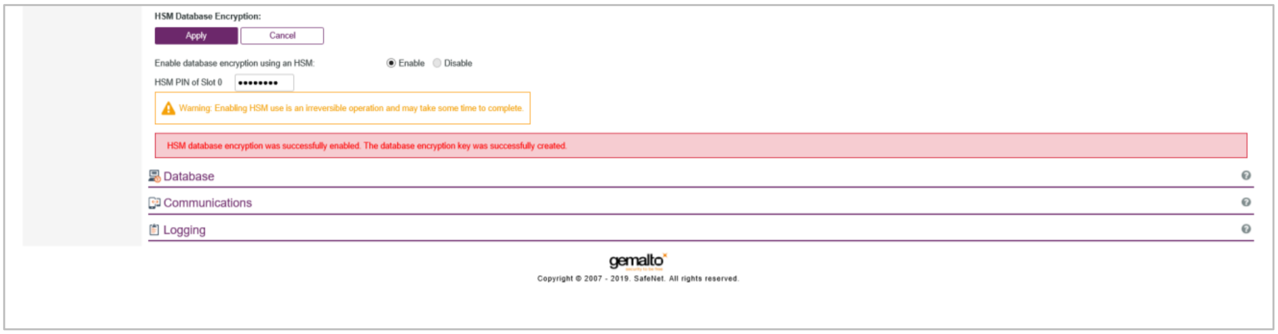
HSM PIN of Slot 0

Warning: Enabling HSM use is an irreversible operation and may take some time to complete.

5. Click **Enable** to **Enable database encryption using an HSM**.

6. Enter the Crypto Officer PIN of the HSM partition in the **HSM PIN of Slot 0** input field.

7. Click the **Apply** button. You will see the following message: **HSM database encryption was successfully enabled. The database encryption key was successfully created.** In case a key is already present in the HSM or in the case of a PIN update, an appropriate message will be displayed.


HSM Database Encryption:

Apply Cancel

Enable database encryption using an HSM: ● Enable ○ Disable

HSM PIN of Slot 0 ••••••••

Warning: Enabling HSM use is an irreversible operation and may take some time to complete.

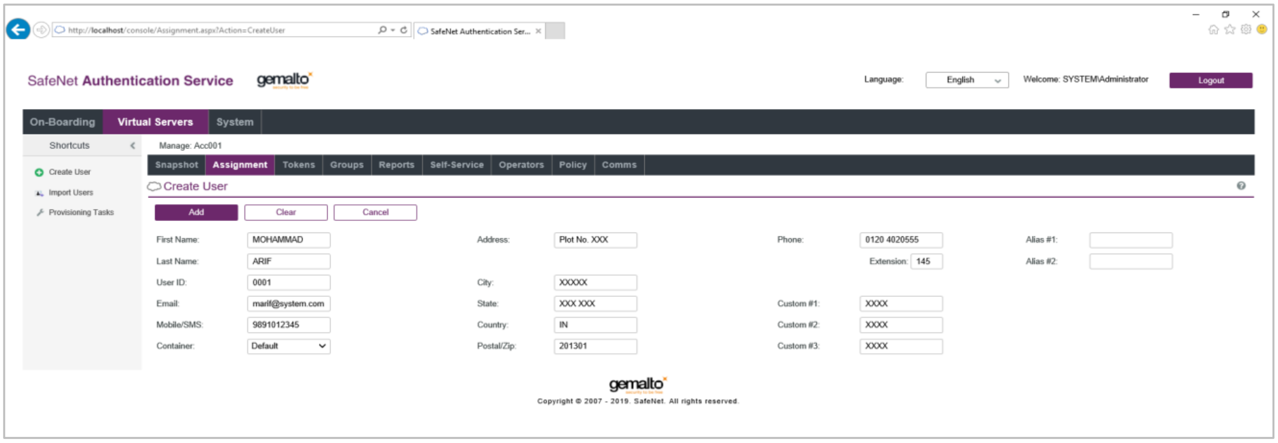
HSM database encryption was successfully enabled. The database encryption key was successfully created.

> **NOTE:** If the AES key with Label: HSM_KEY_AES_ENCRYPTION_VER_13 exists in Luna HSM partition, then it will use the existing key. If there is no key with this label, it will generate a new key.

Verifying Encryption on SafeNet Authentication Service

You can verify if SafeNet Authentication Service encryption is operating and using an encryption key provided by the Luna HSM. To verify encryption on SafeNet Authentication Service:

1. Create a new user, or update an existing user.

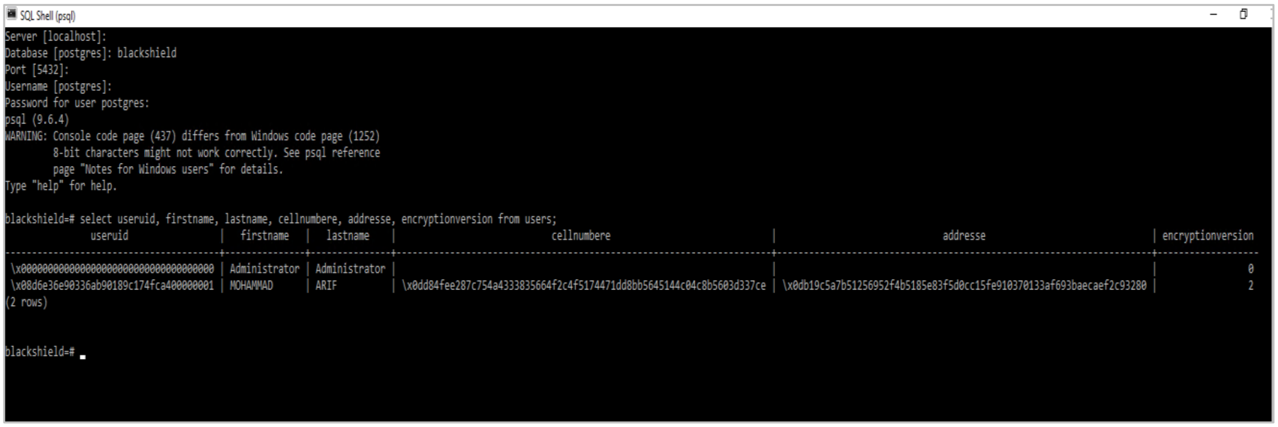


First Name: MOHAMMAD
Last Name: ARIF
User ID: 0001
Email: marif@system.com
Mobile/SMS: 9891012345
Container: Default
Address: Plot No. XXX
City: XXXXX
State: XXX XXX
Country: IN
Postal/Zip: 201301
Phone: 0120 4020555
Extension: 145
Custom #1: XXXX
Custom #2: XXXX
Custom #3: XXXX
Alias #1:
Alias #2:

2. Check the value of the **encryptionVersion** column in SAS database.

```
# select useruid, firstname, lastname, cellnumbere, addresse, encryptionversion
from users;
```

If the value of the **encryptionVersion** column is set to **2**, it means that the encryption is achieved.



```
Server [localhost]:
Database [postgres]: blackshield
Port [5432]:
Username [postgres]:
Password for user postgres:
psql (9.6.4)
WARNING: Console code page (437) differs from Windows code page (1252)
         8-bit characters might not work correctly. See psql reference
         page "Notes for Windows users" for details.
Type "help" for help.

blackshield=# select useruid, firstname, lastname, cellnumbere, addresse, encryptionversion from users;
               useruid                |   firstname   |   lastname    |                             cellnumbere                              |                              addresse                              | encryptionversion
--------------------------------------+---------------+---------------+----------------------------------------------------------------------+--------------------------------------------------------------------+-------------------
 \x00000000000000000000000000000000000 | Administrator | Administrator |                                                                      |                                                                    |                 0
 \x08d6e36e90336ab90189c174fca400000001 | MOHAMMAD      | ARIF          | \x0dd84fee287c754a4333835664f2c4f5174471dd8bb5645144c04c8b5603d337ce | \x0db19c5a7b51256952f4b5185e83f5d0cc15fe910370133af693baecaef2c93280 |                 2
(2 rows)


blackshield=# 
```

SafeNet Authentication Service now uses the Luna HSM key to encrypt all sensitive data. This completes the Luna HSM integration with SafeNet Authentication Service.

Contacting Customer Support

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. 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 to this service is governed by the support plan arrangements made between Thales 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.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository 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 Thales 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.DIS@thalesgroup.com.