

SafeNet Authentication Service

INTEGRATION GUIDE THALES LUNA HSM

Document Information

Document Part Number	007-000451-001
Revision	C
Release Date	13 July 2023

Trademarks, Copyrights, and Third-Party Software

Copyright © 2023 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

CONTENTS

Overview	4
Supported Platforms	4
Prerequisites	5
Configure Luna HSM	5
Set up SafeNet Authentication Service (SAS)	6
Configuring Luna HSM for SafeNet Authentication Service	6
Verifying Encryption on SafeNet Authentication Service	9
Contacting Customer Support	10
Customer Support Portal	10
Telephone Support	10

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:

- > Ensuring secure key generation, storage, and protection through FIPS 140-2 level 3 validated hardware.
- > Providing full life cycle management of the keys.
- > Maintaining an audit trail through HSM.
- > Achieving significant performance enhancements by offloading cryptographic operations from application servers.

Supported Platforms

The following platforms are certified for integrating SafeNet Authentication Service with Luna Cloud HSM:

Platforms Tested	SafeNet Authentication Service (SAS)
Windows Server 2022 Datacenter Windows Server 2019 Standard	SAS PCE/SPE 3.18
Windows Server 2016 Standard	SAS PCE/SPE 3.10.1
Windows Server 2016 Standard	SAS PCE/SPE 3.8.1

NOTE: This integration will work properly and be compatible with any Luna HSM device, provided the Luna HSM device is supported and used in conjunction with a compatible Luna Client.

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

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 <u>Luna HSM</u> <u>Documentation</u> for more information.
- 2. Create a partition on the Luna HSM for use with SafeNet Authentication Service (SAS).
- 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
                         Luna User Partition With SO (PW) Key Export
Configuration ->
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 <u>Luna HSM documentation</u> for detailed steps for creating NTLS connection, initializing the partitions, and various user roles.

Configuring Luna HSM HA (High-Availability)

Please refer to the <u>Luna HSM documentation</u> 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)

For detailed instructions on installing and configuring the SafeNet Authentication Service (SAS), please consult the official SAS Documentation. To download the SAS software, visit the Thales support site by following the provided link:

https://supportportal.thalesgroup.com/csm

Once the installation is complete, verify the successful operation of the SAS service by accessing the following URL:

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

SafeNet Authentication Service x +	~	- 0 ×
← → C ▲ Not secure 10.164.76.12/console/	6 \$	* 🛛 🚳 :
🧧 Get Ready to Deplo 📎 download 🚦 Using Smart Cards 🚦 BitLocker: How to e TN Hosting the Windo 🔋 Direct Access 🚦 Yeal World' Direct 💿 jtt-consulting: Direc 💽 Securing Stored Us	30	Other bookmarks
SafeNet Authentication Service		
Administration Console		
Login		
Please enter your credentials to log in.		
Email:		
Password:		
Logon		
English Francais		
Copyright © 2007 - 2023 Thales Group. All rights reserved.		
	^ '■ @ ⊄	5:27 PM

Configuring Luna HSM for SafeNet Authentication Service

This integration assumes that SAS is installed and running. Complete the following steps 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.
- 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.

Administrator: C:\Windows\system32\cmd.exe		×
C:\Windows\system32>iisreset		^
Attempting stop Internet services successfully stopped Attempting start Internet services successfully restarted		
C:\Windows\system32>_		

4. Launch SAS Manager Console and log in to the SAS Manager Console as an Administrator. https://<hostname.or IP address>/console

SafeNet Authentication Service	+	0	2	-	3 ×	
← → C ▲ Not secure 1	0.164.76.12/console/System.aspx	6 1	àr -	* 🛙	🌝 E	
Statket Authentication Service ★ ★ Cet Reary to Depto. It in 64.76.12/console/System.aspx It is in 5 mark Cards. It is in 6 mark Cards. It is						
SafeNet Authen	tication Service Language: English ~ Welcome: SYSTEMIAdministrator			Logout		
On-Boarding Virtual	Servers System					
Shortcuts 🕺	Setup				0	
Image: State Image: English Image: English <td>0</td>		0				
	Communications				0	
	Logging				0	
	THALES					
	Copyright © 2007 - 2023 Thales Group. All rights reserved.					

5. Navigate to System > Setup > HSM Database Encryption.

10.164.76.12/console/System.as:	× +		v -	0
← → C ▲ Not secure	10.164.76.12/console/System.aspx		e 🗙 🛊	0 🚳
📑 Get Ready to Deplo 🚷 downlo	ad 📑 Using Smart Cards 📑 BitLocker: How to e TN	Hosting the Windo 📙 Direct Access 📲 'Real World' Direct 📵 jtt-consulting: [Dire 🥃 Securing Stored Da	* <mark>8</mark> 0	ther bookma
SafeNet Auther	tication Service	Language: English v Welcome: SYSTEMAdministrator	Logout	
On-Boarding Virtua	Servers System			
Shortcuts 🦿	Setup			0
	Configure database connections and sites, and insta	ill licenses.		
	Task	Description		
	Licenses	Install and activate licenses.		
	Site	Set site import and export information.		
	Permit LDAP	Permit child accounts to configure LDAP settings.		
	Software Token Push OTP Setting	Enable Push OTP communication with MobilePass+		
	Permit ODBC Migrations	Configure ODBC migrations of SafeNet authentication servers.		
	Agent Communication with JWT token	Enable additional agent communication through the use of a JWT token.		
	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:	C Enable Disable		

- 6. Click Enable to Enable database encryption using an HSM.
- 7. Enter the Crypto Officer PIN of the HSM partition in the HSM PIN of Slot 0 input field.
- 8. 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.

😵 10.164.76.12/console/System.as; 🗙	+		~ - O ×
← → C ▲ Not secure 10	0.164.76.12/console/System.aspx		@ \$ \$ 0 () :
📑 Get Ready to Deplo 🔇 download	d 🚦 Using Smart Cards 🚦 BitLocker: How to e TN Hosting	a the Windo 🧧 Direct Access 📲 'Real World' Direct 😰 itt-consulting: [Dire 🧰 Securing Stored Da	» 🧧 Other bookmarks
	Permit I DAP	Permit child accounts to configure I DAP settings	
	Software Token Push OTP Setting	Enable Push OTP communication with MobilePass+	
	Permit ODBC Migrations	Configure ODBC migrations of SafeNet authentication servers	
	Agent Communication with JWT token	Enable additional agent communication through the use of a . WT token	
	System Configuration Details	Generate snanchots of system configuration details	
	Provisioning Delay Time	Set Provisioning Delay Time	
	HSM Database Encrution	Enable and configure taken encryption key storage using a hardware security module	
	Tom Database Encrypton	Linube and configure over energypoor key denage during a minumare accordy module.	
	HSM Database Encryption: Apply Cancel		
	Enable database encryption using an HSM:	Enable Disable	
	HSM PIN of Slot 0		
	A Warning: Enabling H3M use is an irreversible operation	on and may take some time to complete.	
	HSM database encryption was successfully enabled. The	e database encryption key was successfully created.	
	Database		0
	Communications		Ø
	Logging		0
		THALES	
	Copyrig	ht © 2007 - 2023 Thales Group. All rights reserved.	
📲 🗄 🔂 🧔	📑 🥶 💷 🖉 🔮 🦄	🦻 🛂 📲	へ 🛎 🧟 (小) 😚 6:03 PM 7/6/2023 💀

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.

9. Verify that the key is being created. To view the key created on Luna HSM partition, run the "cmu list" command.



Verifying Encryption on SafeNet Authentication Service

To verify encryption on SafeNet Authentication Service:

1. Create a new user or update the information of an existing user.

SafeNet Authentication Service	× 💡 592k/S11, :	Subhani Khera Rd, Di 🗙 📔 🕂						33	~	- 0	x c
← → C ▲ Not secure	10.164.76.12/consc	ole/Assignment.aspx?Action=Det	be					ß	¢ 1	N 🛛	() :
📑 Get Ready to Deplo 🔗 downlo	ad 🚦 Using Smar	rt Cards 🚦 BitLocker: How to e	TN Hosting the	Windo 📙 Direct Access	Real World' Direct	jtt-consulting: [Dire 🧧 Secu	ring Stored Da		*	Other	bookmarks
SafeNet Auther	ntication S	Service			Language: E	inglish 👽 Welcome:	SYSTEM/administrator		Log	jout	
On-Boarding Virtu	al Servers	System									
Shortcuts 《	Manage: Adm	ninistrator									
Create User	Snapshot	Assignment Tokens	Groups Re	ports Self-Service	Operators Policy	Comms					
👢 Import Users	User Detail	l : tuser								0	
	Apply First Name Last Name User ID: Email: Mobile/SMS: Container: Authenticat	Cancel Test User tuser tuser@localhost.com 1234567890 Default vition Methods	Address: City: State Country: Postal/Zip:	Berger Tower Nolda Uttar Pradesh India 201301	Phone: Emergency: Custom #1 : Custom #2 : Custom #3 :	Extension:	Allas #1: Allas #2:				*
	Assign Assign Passw	vord	Change L	pg					Passwo	urd]

2. Check the value of the encryptionVersion column in SAS database by executing the following query:

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

If the value of the **encryptionVersion** column is set to **2**, it indicates that the encryption has been successfully implemented.

SQLQuery1sql - 10.164.76.44.BlackShield File Edit Yiew Query Project Ioo O O O Y BlackShield P P	(Ba (66)** Microsoft SGL Server Management Studio (Administrator) bi Wickow Lefe # Overy 単命 奈 奈 奈 奈 永 () つ う つ・つ 割 ・) 声 # Covery 単奈 奈 奈 奈 奈 秋 () つ う つ・つ 割 ・) 声 # Covery 単 奈 奈 奈 奈 秋 () 日 () つ う つ ・ ○ 割 ・) 声 # Covery 単 奈 奈 奈 奈 秋 () 日 () つ う つ ・ ○ 割 ・) 声 # Covery 単 奈 奈 奈 奈 奈 秋 () 日 () つ う つ ・ ○ 割 ・) 声 # Covery 単 赤 の ・ ○	aunch (Ctrl+Q) 👂 🕳 🛷	×
Polject Epslorer ● # × Connect ● # Y ● ■ ♥ Ø ◆ ■ 01016774505 Server 15020005-ss ■ 901016774505 Server 15020005-ss ■ 95erver Objects ■ 95erver Objects ■ Reprint Color ■ 849000 Server Objects ■ 85000 Server Objects ■ 10169200 Server Objects	SQLQary1ag-10_lacShed (g 66)/ * X ure BlacShield; 60 select Useruid, firstname, lastname, cellnumbere, addresse encryptionversion from users) 100% *		* 1 × 1
	Bit Netsages Sector S	europtionesten 0 2 2 vate Windows	
۲	© Query excuted successfully. 10.164.76.44 (15.0 RTA	4) sa (66) BlackShield 00:00:00 3 rows	
🗇 Ready	Lin 4 Col 90 Ch 90 MS		

The integration of the Luna HSM with SafeNet Authentication Service is now finalized as the SafeNet Authentication Service employs the Luna HSM key for encrypting all sensitive data.

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 <u>Thales Customer Support</u>. 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 <u>https://supportportal.thalesgroup.com</u>, 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.