

SafeNet Authentication Service

INTEGRATION GUIDE
SAFENET LUNA HSM



Document Information

Document Part Number	007-000451-001
Release Date	June 2019

Revision History

Revision	Date	Reason
A	June 2019	First Release

Trademarks, Copyrights, and Third-Party Software

© 2019 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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.

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- > The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE	5
Scope	5
Document Conventions.....	5
Command Syntax and Typeface Conventions	6
Support Contacts	7
Customer Support Portal	7
Telephone Support	7
Email Support	7
CHAPTER 1: Introduction	8
Third Party Application Details.....	8
Supported Platforms	8
Prerequisites	9
Configure SafeNet Luna HSM	9
Set up SafeNet Authentication Service (SAS).....	9
CHAPTER 2: Integrating SafeNet Luna HSM with SafeNet Authentication Service	10
Configuring the SafeNet Luna HSM for SafeNet Authentication Service	10
Verifying Encryption on SafeNet Authentication Service	13

PREFACE

This document is intended to guide administrators through the steps for integrating SafeNet Authentication Service (SAS) with a SafeNet Luna HSM. This guide provides the necessary information to configure SafeNet Authentication Service (SAS) to secure the AES encryption key for encrypting sensitive data using a SafeNet Luna HSM.

Scope

This guide demonstrates configuring a SafeNet Authentication Service (SAS) test environment that secures the AES encryption key within a SafeNet Luna HSM.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Notes contain important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION! Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

****WARNING**** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury

Command Syntax and Typeface Conventions

Convention	Description
bold	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Window titles (On the Protect Document window, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italic</i>	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[a b c] [<a> <c>]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.
{ a b c } { <a> <c> }	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Support Contacts

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 [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 a 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.

CHAPTER 1: Introduction

The SafeNet Luna HSM is an external hardware security module, which is available for use with SafeNet Authentication Service (SAS). You can use the SafeNet solution with SAS to secure AES keys used for protecting sensitive data. You can integrate multiple HSMs as a High Availability (HA) group with SAS.

The benefits of using a SafeNet Luna HSM to generate the AES key for protecting sensitive data in 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.

Third Party Application Details

This integration uses the following third party applications:

- > SafeNet Authentication Service (SAS)

You can download SafeNet Authentication Service (SAS) from the Gemalto support site using the link given below:

<https://supportportal.gemalto.com/csm/>

Supported Platforms

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

SafeNet Luna HSM: SafeNet 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. SafeNet Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs. SafeNet 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)	SafeNet HSM
Windows Server 2016 Standard	SAS PCE/SPE 3.8.1	SafeNet Luna SA 7.3.0 Firmware 7.3.0 SafeNet Luna Client 7.3.0

NOTE: SafeNet Authentication Service (SAS) is supported with Luna Clients in HA & FIPS Mode.

Prerequisites

Before you proceed with the integration, complete the following:

Configure SafeNet Luna HSM

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

1. Ensure the HSM is set up, initialized, provisioned and ready for deployment. Refer to the SafeNet Luna HSM Product Documentation for more information.
2. Create a partition on the SafeNet Luna HSM for use with SafeNet Authentication Service (SAS).
3. If you are using a SafeNet 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.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

Available HSMs:

Slot Id ->                0
Label ->                  SAS
Serial Number ->          1280780175888
Model ->                  LunaSA 7.3.0
Firmware Version ->      7.3.0
Configuration ->         Luna User Partition With SO (PW) Key Export With
Cloning Mode
Slot Description ->      Net Token Slot
Current Slot Id: 0
```

NOTE: Follow the *SafeNet Luna Network HSM Product Documentation* for detailed steps for creating the NTLS connection, initializing the partitions, and initializing the Security Officer, Crypto Officer, and Crypto User roles.

Set up SafeNet Authentication Service (SAS)

Please refer to the *SafeNet Authentication Service (SAS) Documentation* for installing and configuring the product.

CHAPTER 2: Integrating SafeNet Luna HSM with SafeNet Authentication Service

SafeNet Luna HSM integrates with SafeNet Authentication Service (SAS) to secure the AES encryption key for encrypting sensitive data.

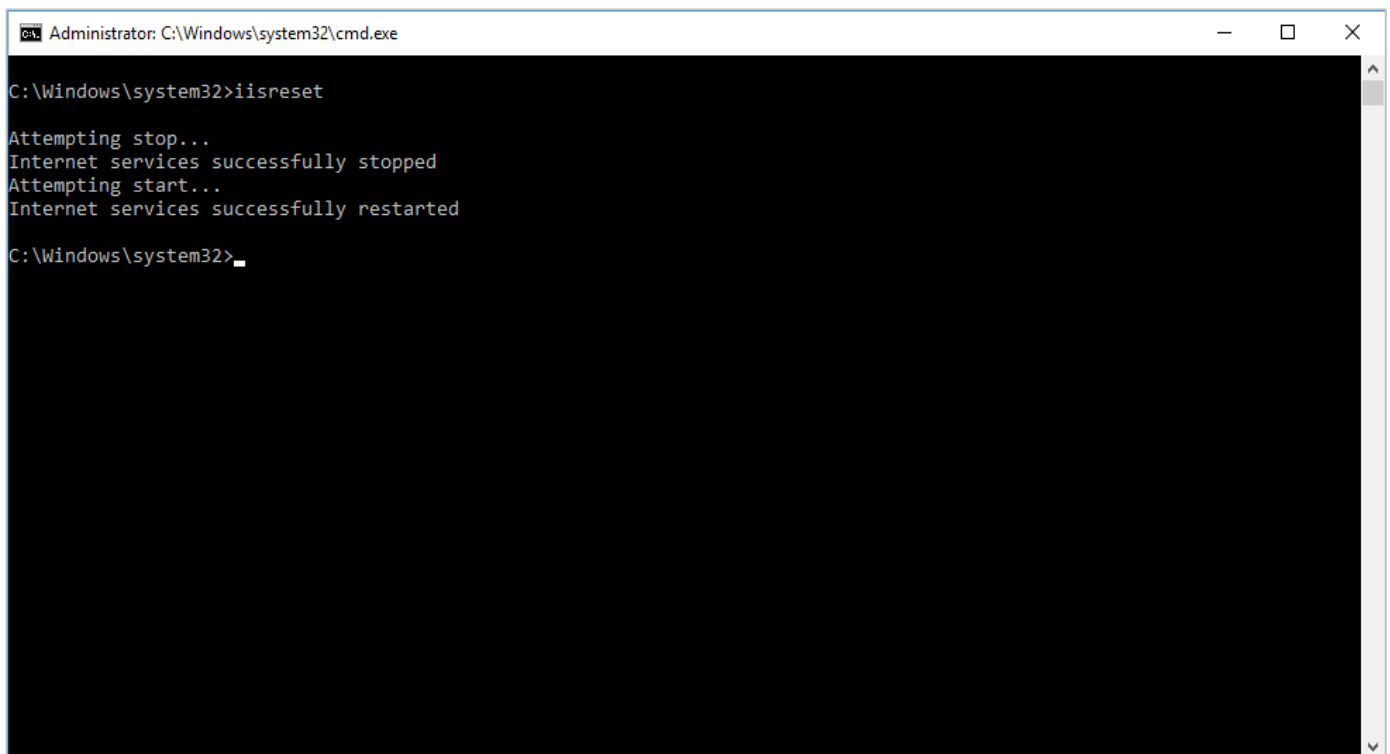
Configuring the SafeNet Luna HSM for SafeNet Authentication Service

This integration assumes that SAS is installed and enabled. Complete the following to configure the SafeNet Luna HSM for use 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 the SafeNet Luna HSM for SafeNet Authentication Service

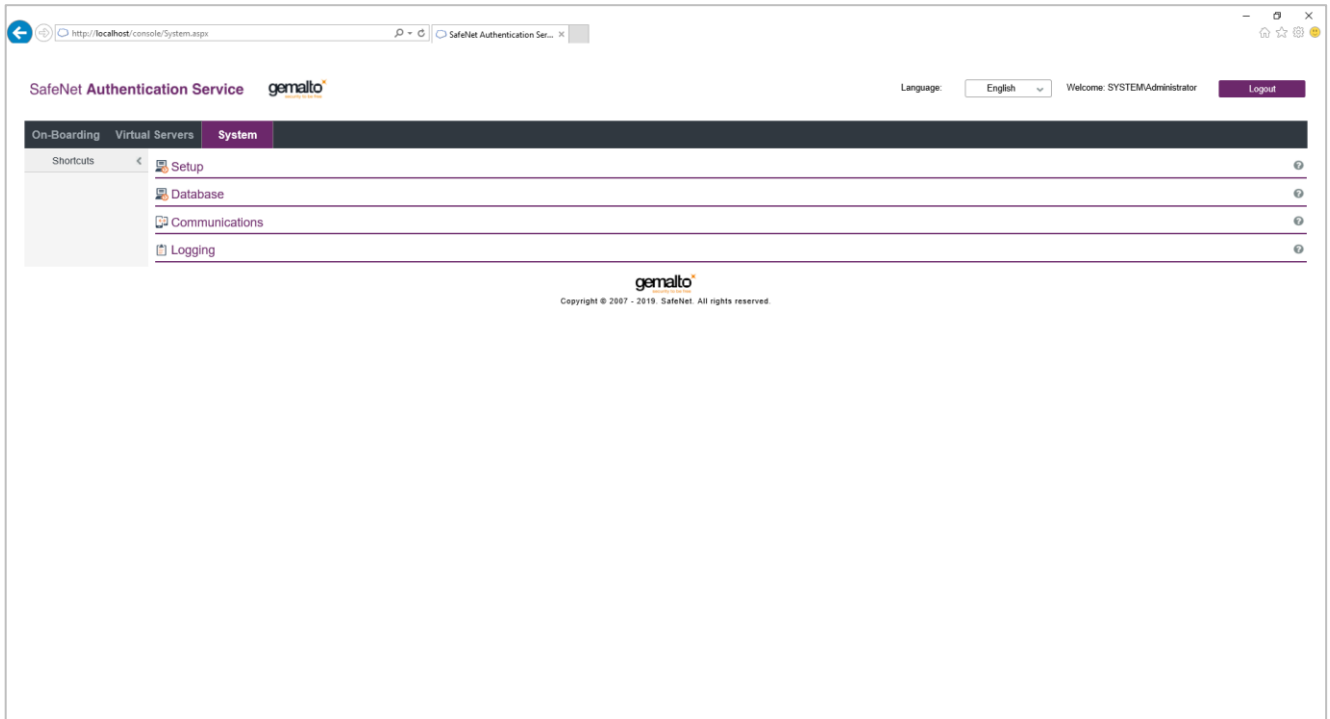
1. Copy the **cryptoki.dll** from **C:\Program Files\SafeNet\LunaClient** folder to the **C:\Windows\System32** folder.
2. Open the command prompt and run the **iisreset** command to reset IIS.



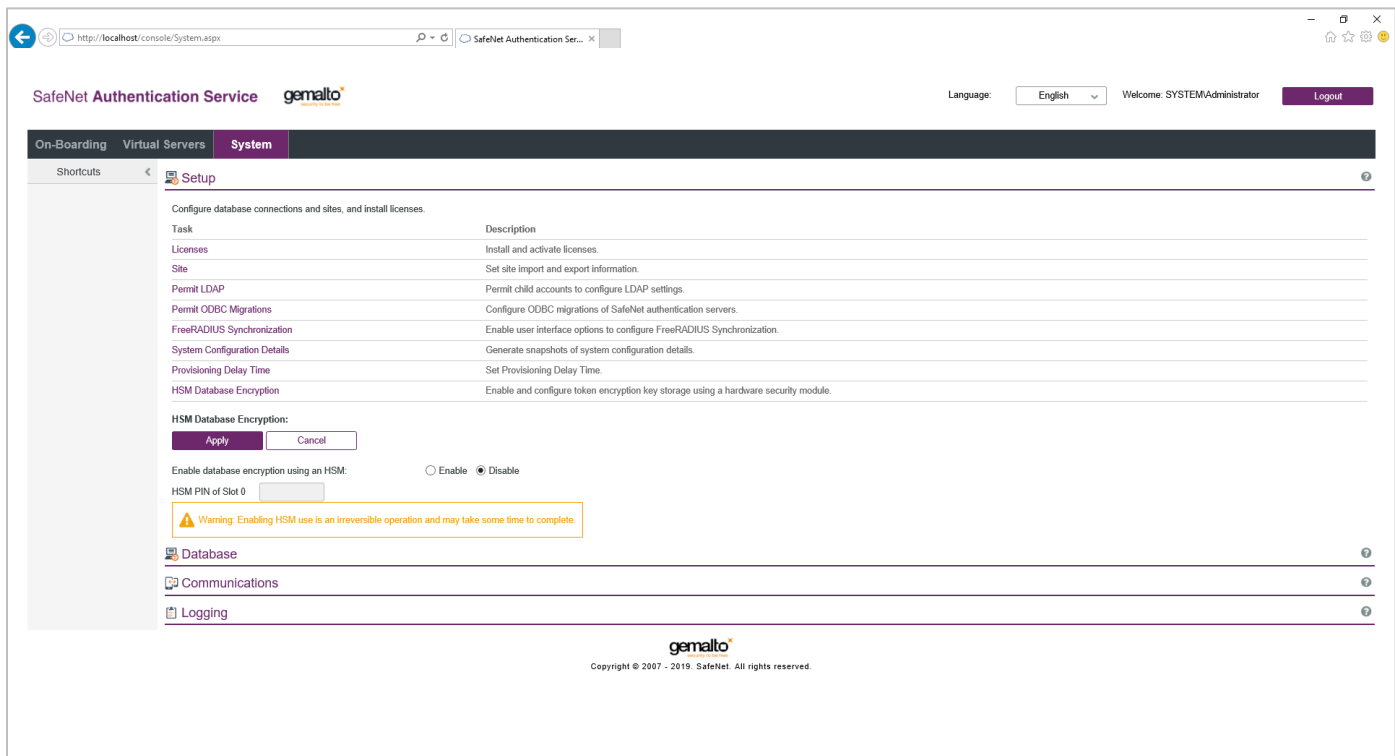
```
Administrator: C:\Windows\system32\cmd.exe
C:\Windows\system32>iisreset
Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
C:\Windows\system32>
```

3. Launch SAS Manager Console and login to the SAS Manager Console as an Administrator.

<http://localhost/console>

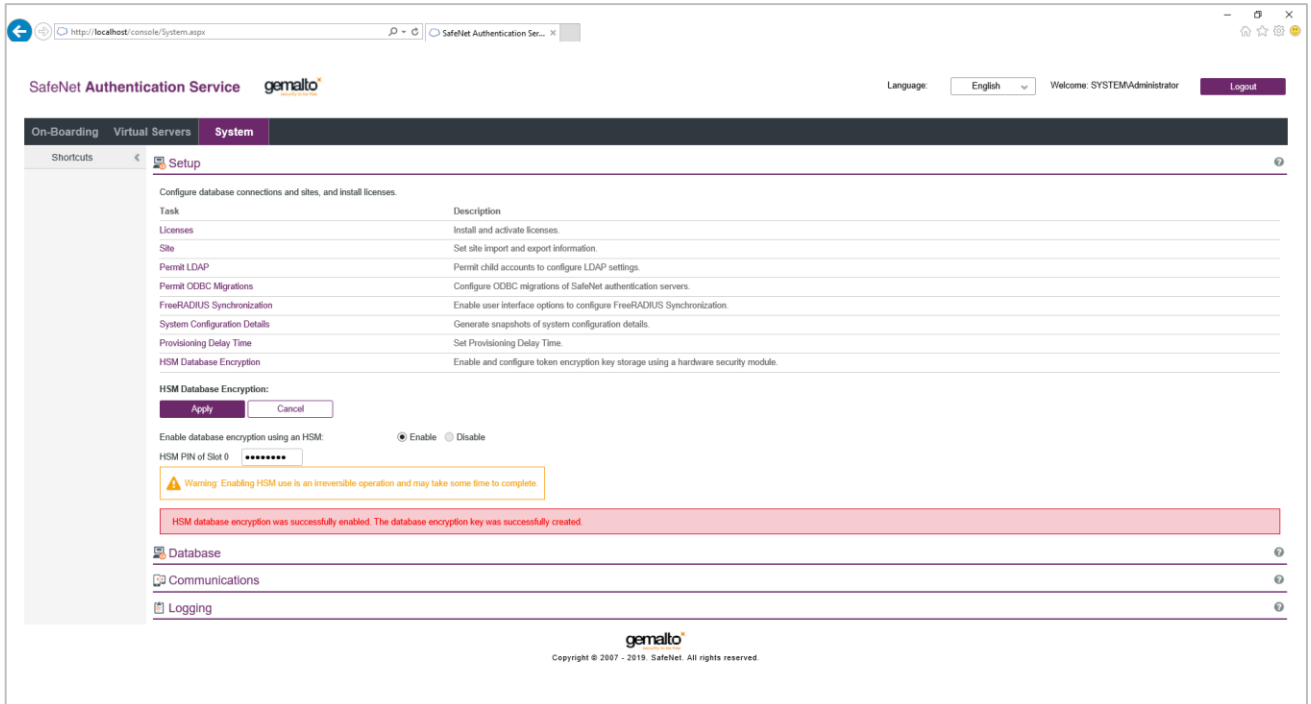


4. Navigate to **System > Setup > HSM Database Encryption**.



5. Select **Enable** and provide the Crypto Officer PIN of the HSM partition.
6. Click **Apply**.

The message, **HSM database encryption was successfully enabled. The database encryption key ...** will be displayed. If a key is already present in the HSM (or in the case of a PIN update), an appropriate message(s) will be displayed.



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 SafeNet Luna HSM.

To verify encryption on SafeNet Authentication Service

1. Create a new user (or update an existing user).

The screenshot shows the 'Create User' form in the SafeNet Authentication Service web interface. The form is titled 'Create User' and includes several input fields for user details. The fields are organized into two columns. The left column contains: First Name (MOHAMMAD), Last Name (ARIF), User ID (0001), Email (marif@system.com), Mobile/SMS (9891012345), and Container (Default). The right column contains: Address (Plot No. XXX), City (XXXXX), State (XXX.XXX), Country (IN), Postal/Zip (201301), Phone (0120 4020555), Extension (145), and three Custom fields (XXXX). There are also fields for Alias #1 and Alias #2. The interface includes a navigation menu with options like 'On-Boarding', 'Virtual Servers', and 'System'. The top right shows the user is logged in as SYSTEM/Administrator.

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

```

SQL Shell (psql)
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 userid, firstname, lastname, cellnumbere, addresse, encryptionversion from users;
   userid   |  firstname  |  lastname  | cellnumbere | addresse | encryptionversion
-----|-----|-----|-----|-----|-----
 \x00000000000000000000000000000000 | Administrator | Administrator |             |          | 0
 \x0806e30e90336ab901174fc4400000001 | MOHAMMAD    | ARIF       | \x0dd84fee287c754a433835664f2c4f5174471dd8bb5645144c04c8b5083d337ce | \x0db19c5a7b51256952f4b5185e83f5d0cc15fe910370133af693baecaef2c93208 | 2
(2 rows)

blackshield=#

```

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