THALES

Thycotic Secret Server

INTEGRATION GUIDE

THALES LUNA NETWORK HSM

THALES DATA PROTECTION ON DEMAND

Document Information

Document Part Number	007-000480-001
Release Date	7 May 2020

Revision History

Revision	Date	Reason
A	July 24, 2019	Initial release
B	7 May 2020	Update

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales Group 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 Thales' 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, Thales 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, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales 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 Thales 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.

Thales 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 Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales 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

This document describes steps to integrate Thycotic Secret Server with a Thales Luna Network HSM or a Thales Data Protection On Demand (DPOD) service. It contains the following chapters:

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure, including Luna Network HSM users and security officers, key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Document Conventions

This section provides information on the conventions used in this template. The information presented is to instruct the writer on how to use the template and can be removed if you do not wish to include it in your customer-facing document. For example, you may wish to remove the “Hyperlinks” sections but keep the “Notifications” section.

Notifications

This template uses notes, cautions, and warnings to alert you to important information that may help you to complete your task, or prevent personal injury, damage to the equipment, or data loss.

Notes

Notes are used to alert you to important or helpful information.

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

Cautions

Cautions are used to alert you to information that may help prevent unexpected results or data loss.

> **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.

> ****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	The bold attribute is used to indicate the following: > 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**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* 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> | <b> | <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> | <b> | <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.

Related Documents

The following documents contain related or additional information:

Thales Luna Network HSM Product Documentation

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 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.

CHAPTER 1: Getting Started

This chapter explains the setup that you require for integrating Thycotic Secret Server with a Thales Luna Network HSM or a DPOD service. It includes the following sections:

Using a Compatible Device

This integration is verified with:

> Thales Luna Network HSM on Windows 2016 Server operating system
> Thales DPOD on Windows 2016 Server operating system

This integration is also compatible with:

> Thales Luna PCIe HSM on Windows 2016 Server operating system
> Thales Luna USB HSM on Windows 2016 Server operating system

Configuring Luna Network HSM

Before you begin the integration process:

1. Ensure that the HSM is setup, initialized, provisioned, and ready for deployment.
2. Create a partition on the HSM that will be later used by Thycotic Secret Server.
3. Register a client for the system and assign the client to the partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is registered and configured. The command to see the registered partition is:

```
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

Available HSMs:

Slot Id ->              0
Label ->                Thycotic
Serial Number ->        1280780175917
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 steps mentioned in *Thales Luna Network HSM Documentation* for creating NTLS connection, initializing the partition, and various user roles.

Using Luna Network HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the Luna Network HSM in FIPS mode, you have to make the following change to the configuration file:

```
[Misc]

RSAKeyGenMechRemap = 1;
```

This setting redirects the older calling mechanism to a new approved mechanism when Luna Network HSM is in FIPS mode.

Setting up Thales Luna Network HSM HA

Refer to the *Thales Luna Network HSM Product Documentation* for steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work.

Provisioning DPOD Service

This DPOD service provides your client machine with access to an HSM Application Partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share a single application partition.

To use the DPOD service, you need to provision your application partition by initializing the following roles:

- **Security Officer (SO)** - responsible for setting the partition policies and for creating the Crypto Officer.
- **Crypto Officer (CO)** - responsible for creating, modifying, and deleting crypto objects within the partition. The CO can use the crypto objects and create an optional, limited-capability role called Crypto User that can use the crypto objects but cannot modify them.
- **Crypto User (CU)** - optional role that can use crypto objects while performing cryptographic operations.

Resolving Issues with DPOD Services

Enabling DPOD Service in Non-FIPS mode: DPOD services operate in a FIPS and non-FIPS mode. Ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your DPOD service. The FIPS mode is enabled by default. Refer to the *Mechanism List* in the *SDK Reference Guide* for more information about available FIPS and non-FIPS algorithms.

Verifying DPOD <slot> value: LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using DPOD services, you need to verify the slot on the DPOD service for sending the commands. If there is more than one slot, then use the **slot set** command to direct a command to a specified slot. You can use slot list to determine which slot numbers are currently in use by the DPOD service.

Setting up Thycotic Secret Server

Install Thycotic Secret Server on the target machine. Refer to *Thycotic Documentation* for detailed instructions.

CHAPTER 2: Integrating Thycotic Secret Server with a Luna Network HSM

Integrating Thycotic Secret Server with a Luna Network HSM involves the following steps:

> Configuring the SafeNet Key Storage Provider

> Enabling HSM

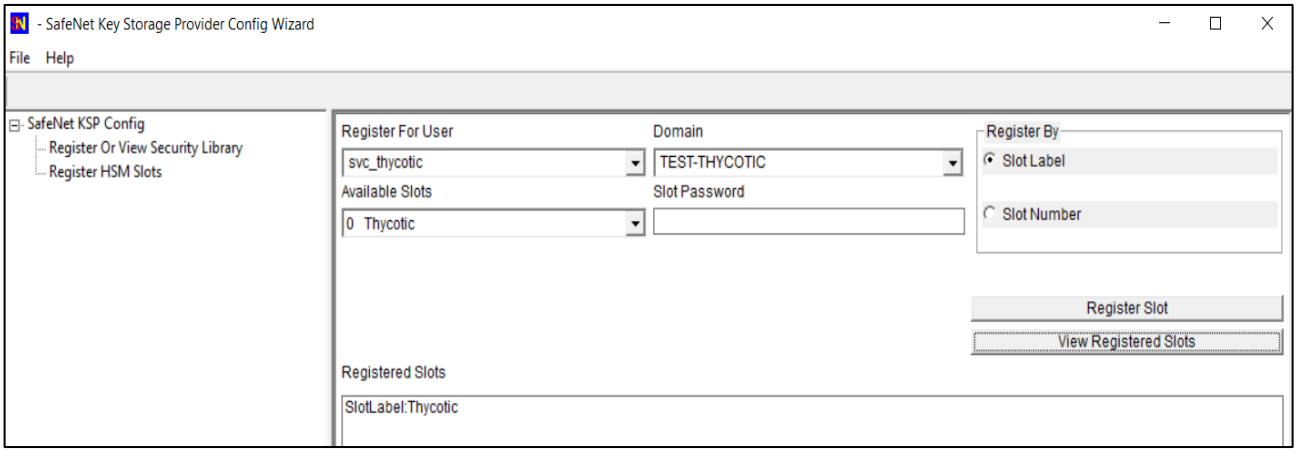
Configuring the SafeNet Key Storage Provider

To configure the SafeNet Key Storage Provider:

1. Navigate to the **<Luna HSM Client installation Directory>\KSP** directory. If you are using a DPOD service, the **\KSP** folder is available in the service client package.
2. Double-click **KspConfig.exe**. The SafeNet KSP configuration wizard will appear on your screen.
3. Double-click **Register or View Security Library** on the left side of the pane.
4. Click **Browse** and select a cryptographic library such as **<Luna HSM Client installation Directory>\cryptoki.dll>.**
5. Click **Register**. If using a DPOD service client, the cryptographic libraries are available in the service client package. On successful registration, you will see the following message:

   "**Success registering the security library**"
6. Double-click **Register HSM Slots** and enter the **Slot (Partition) password**.
7. Click **Register Slot** to register the slot for **Domain** and **Service Account** that has access to database and running the IIS Application Pool(s) dedicated to Secret Server. On successful registration, you will see the following message:

   “The slot was successfully and securely registered.”

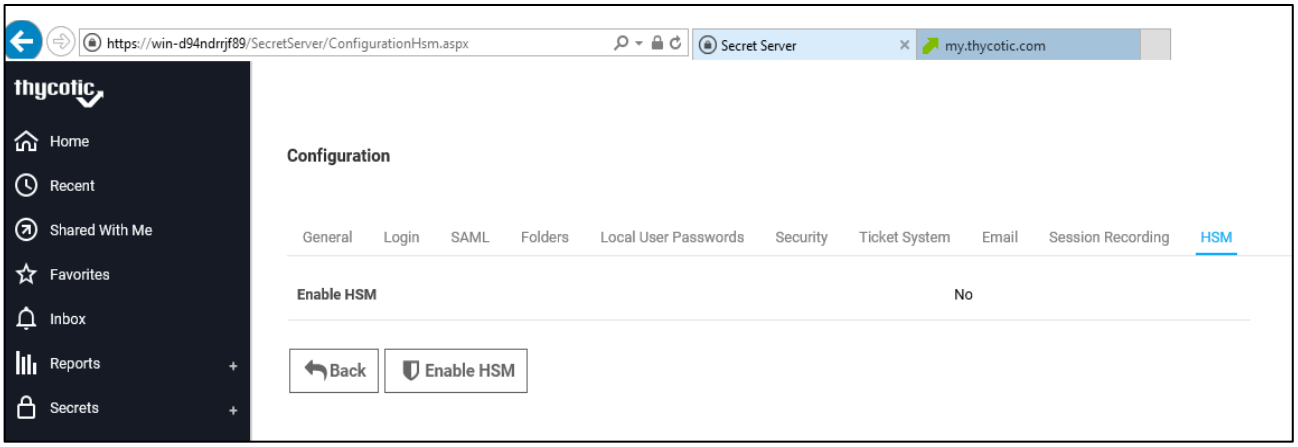


8. Register the same slot for **NT_AUTHORITY\SYSTEM**.
9. Place **SafeNetKSP.dll** in service client package under **C:\Windows\System32**, if you are using a DPOD service client.
10. Restart the IIS after registering KSP for changes to take effect.

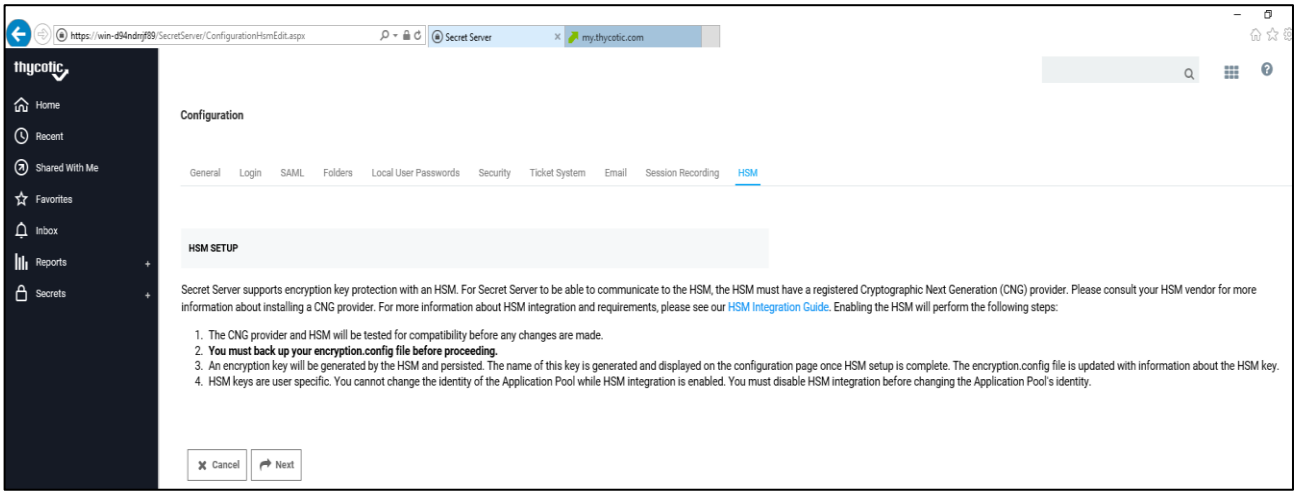
Enabling HSM

To configure the HSM, complete the following steps:

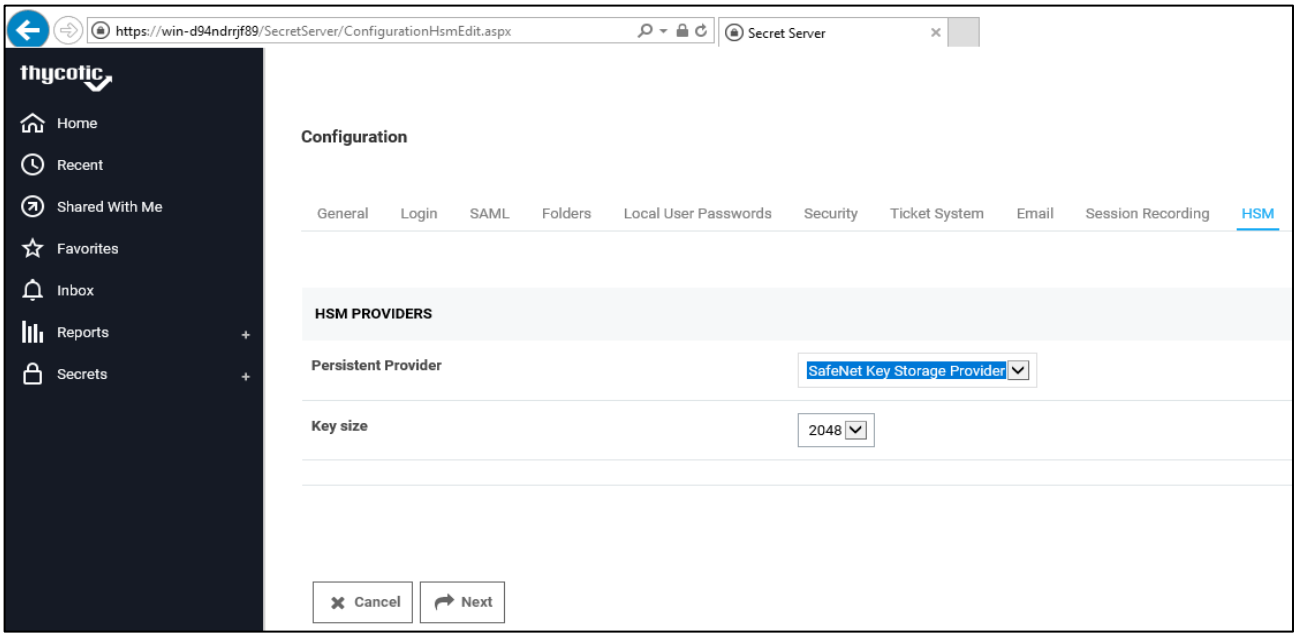
1. Go to the **Admin** menu and click **Configuration**.
2. Select the **HSM** tab.
3. Click **Enable HSM** to initiate the HSM configuration process.



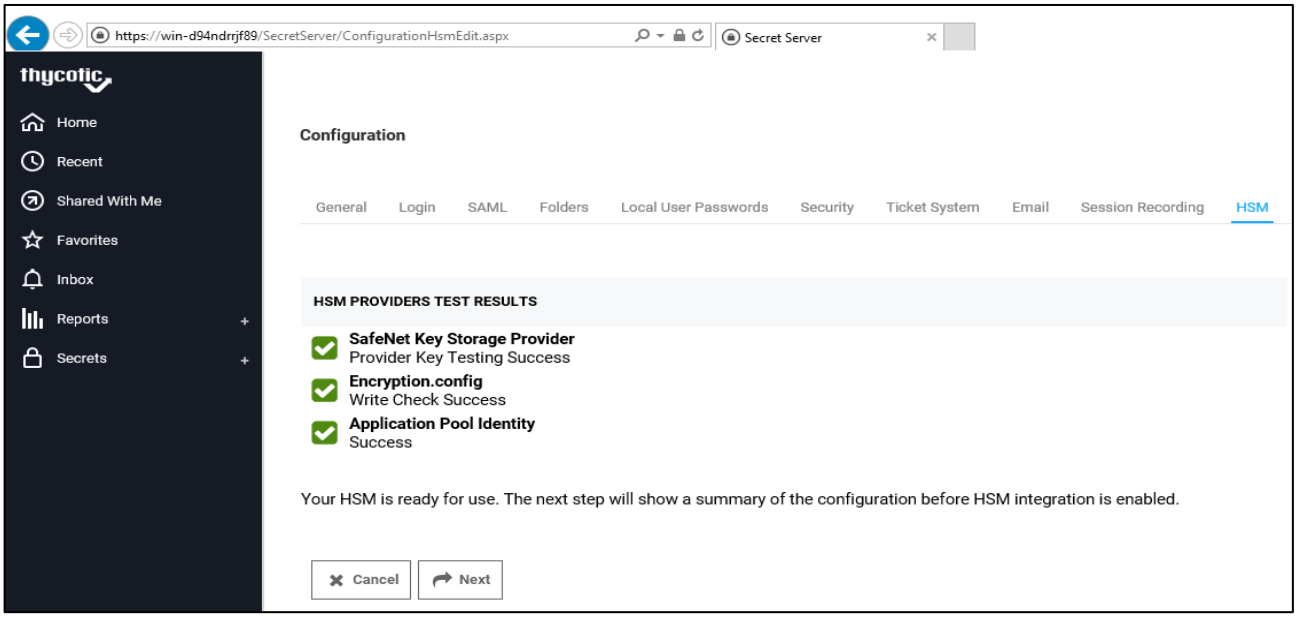
4. Click **Next**.



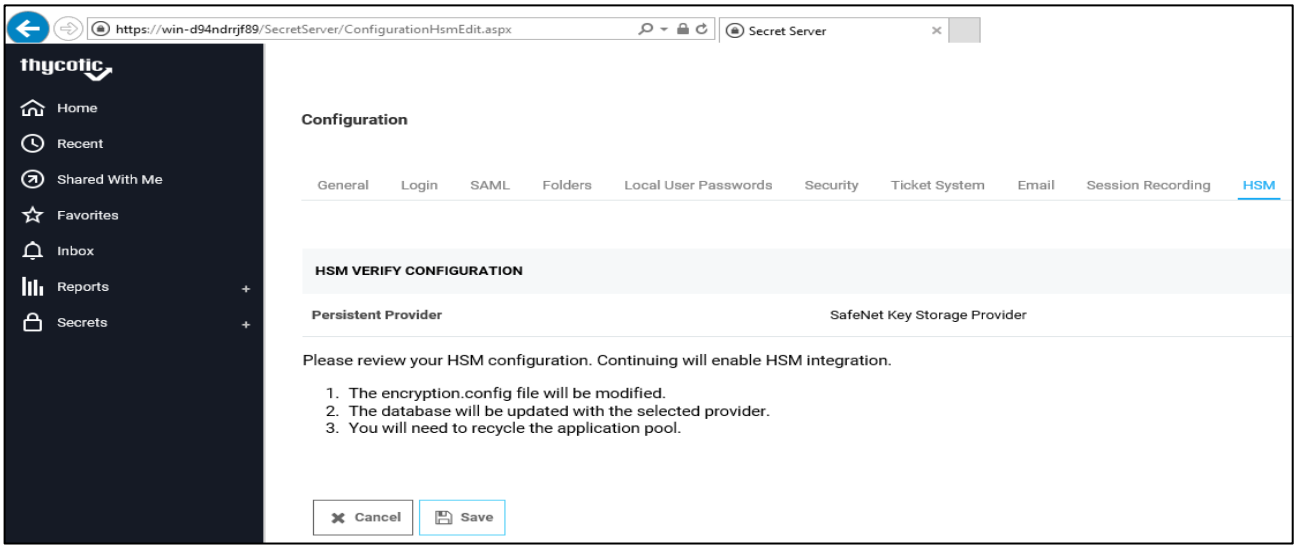
5. Select **SafeNet Key Storage Provider** from **Persistent Provider** drop down box under **HSM PROVIDERS** section and select key size of RSA from **Key size** drop down box.
6. Click **Next**. After this, Secret Server will simulate encryption and decryption operations.



7. Verify whether the configuration has been successful by checking the details under the **HSM PROVIDERS TEST RESULTS** section.

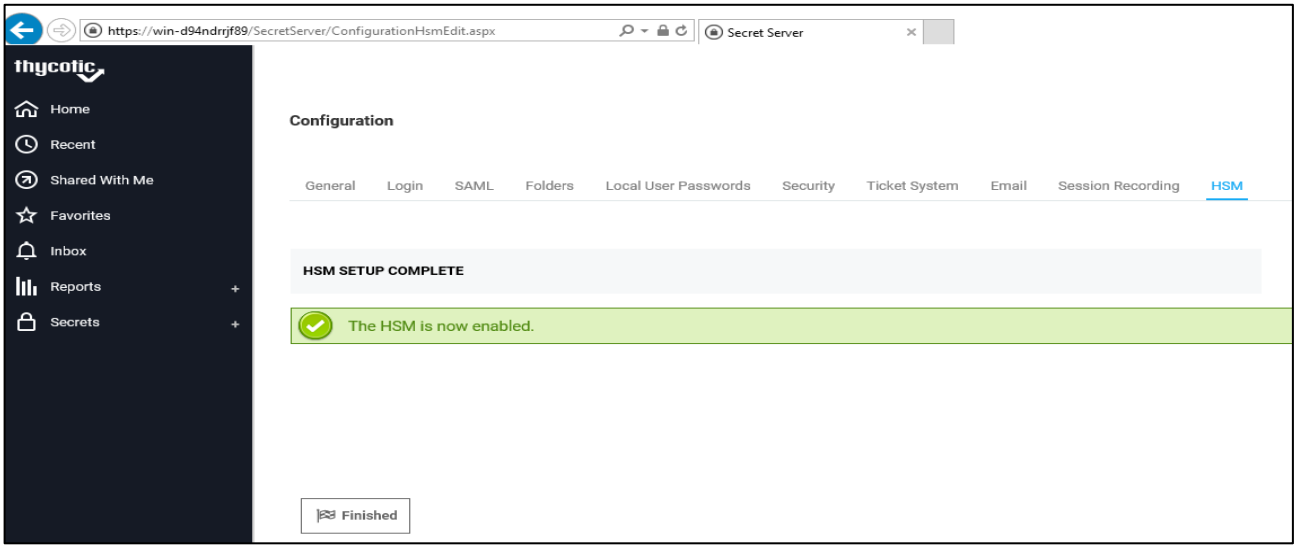


8. Click **Next** to access the **HSM VERIFY CONFIGURATION** section. Review HSM configuration and then click **Save** to enable the HSM.

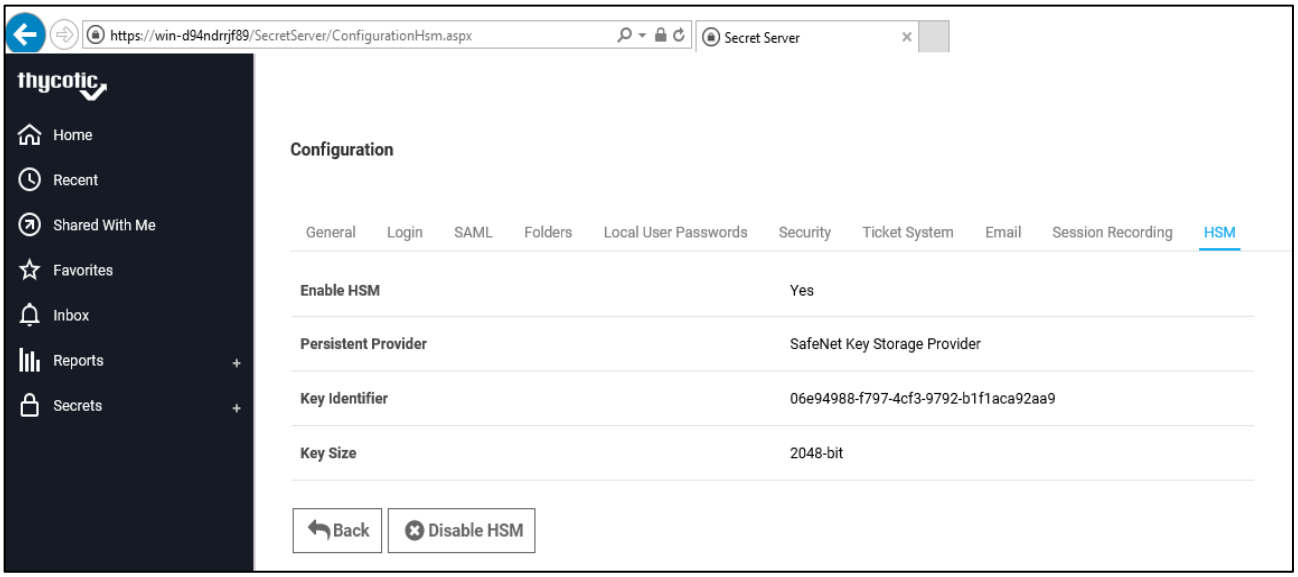


9. Click **Finished** after you see the following message under the **HSM SETUP COMPLETE** section:

   "The HSM is now enabled."



10. Restart the IIS for configuration changes to take effect. You can now view the HSM configuration details under the **HSM** tab. The Secret Server encryption key is now stored on Luna Network HSM partition.



11. Verify the key using the lunacm utility.

```
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 ->                Thycotic
        Serial Number ->        1280780175917
        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

lunacm:> role login -n co

        enter password: ********

Command Result : No Error

lunacm:> partition contents

        The 'Crypto Officer' is currently logged in. Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:          f81597e9-b459-4a4e-89c5-d5c3af22821b
        Handle:         325
        Object Type:    Private Key
        Object UID:     4c09000018000003cb640800

        Label:          f81597e9-b459-4a4e-89c5-d5c3af22821b
        Handle:         186
        Object Type:    Public Key
        Object UID:     4b09000018000003cb640800


        Number of objects:  2

Command Result : No Error
```

This completes the integration of Thycotic Secret Server with Thales Luna Network HSM or Thales Data Protection On Demand Service. Secrets created in Thycotic Secret Server will now use encryption keys residing in HSM partition.

CHAPTER 3: Integrating Thycotic Secret Server Cluster with a Luna Network HSM

Integrating Thycotic Secret Server Cluster with a Luna Network HSM involves the following steps:

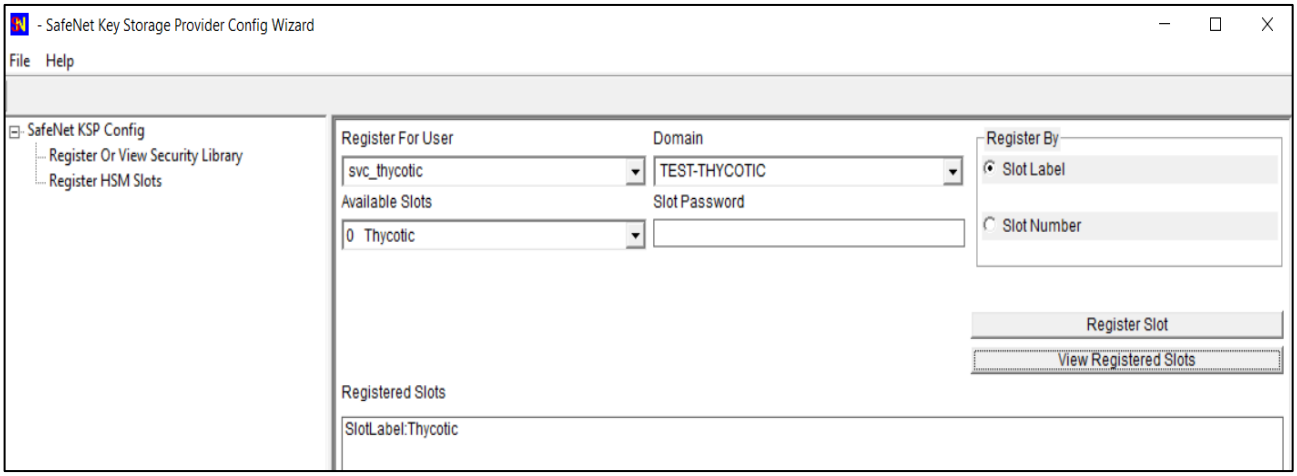
> Configuring the SafeNet Key Storage Provider

> Enabling HSM

Configuring the SafeNet Key Storage Provider

Perform the following steps on all the nodes of the Thycotic Secret Server Cluster:

1. Navigate to the **<Luna HSM Client installation Directory>\KSP** directory.
2. Double-click **KspConfig.exe**. The SafeNet KSP configuration wizard displays.
3. Double-click **Register or View Security Library** on the left side of the pane.
4. Click **Browse** and select a cryptographic library such as **<Luna HSM Client installation Directory>\cryptoki.dll>.**
5. Click **Register**. On successful registration, you will see the following message: "**Success registering the security library**" displays.
6. Double-click **Register HSM Slots** on the left side of the pane.
7. Enter the **Slot (Partition) password**.
8. Click **Register Slot** to register the slot for **Domain** and **Service Account** that has access to database and running the IIS Application Pool(s) dedicated to Secret Server. On successful registration, you will see the following message: **"The slot was successfully and securely registered"**



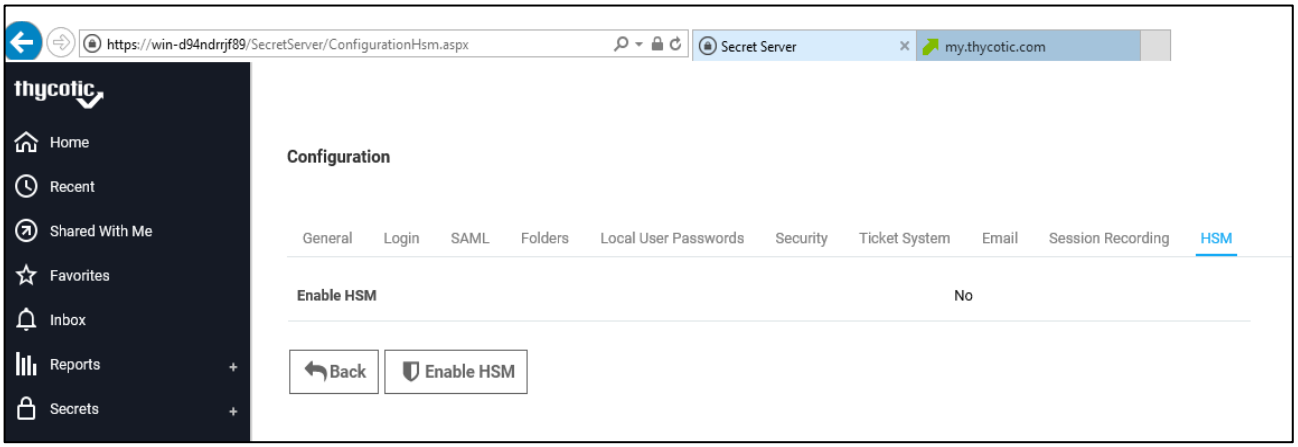
9. Register the same slot for **NT_AUTHORITY\SYSTEM**.
10. Restart the IIS after registering KSP for changes to take effect.

Enabling HSM

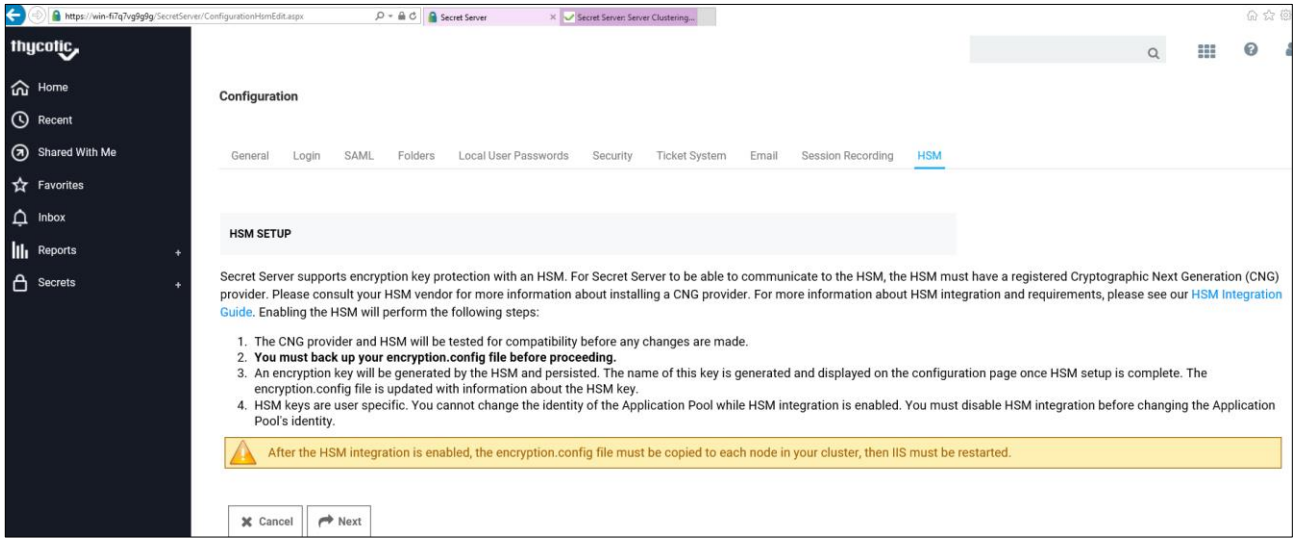
To configure the HSM, complete the following steps on only one of the node of cluster:

1. Log in to Secret Server from browser : http://localhost:80/SecretServer
2. Go to the **Admin** menu and click **Configuration**.
3. Select the **HSM** tab. This initiates the HSM configuration, which guides the process of selecting the HSM's CNG provider.
4. Click **Enable HSM** to initiate the configuration process.

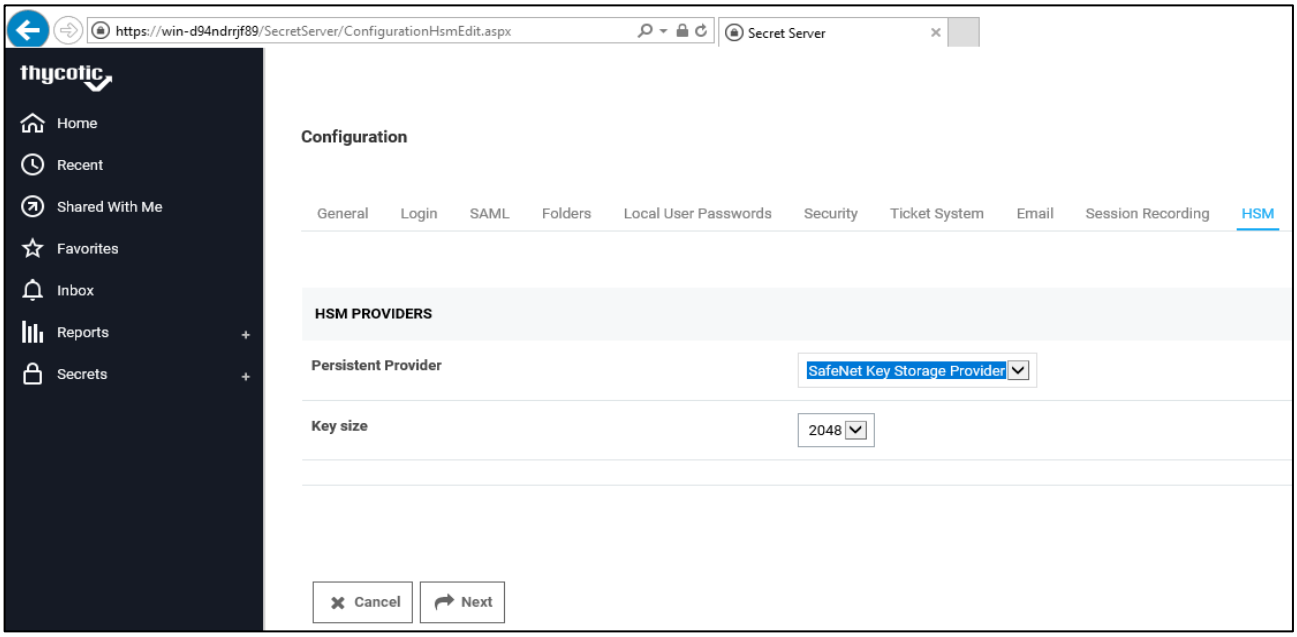
> **NOTE:** Back up the encryption.config before proceeding to enable HSM.



5. Click **Next**.

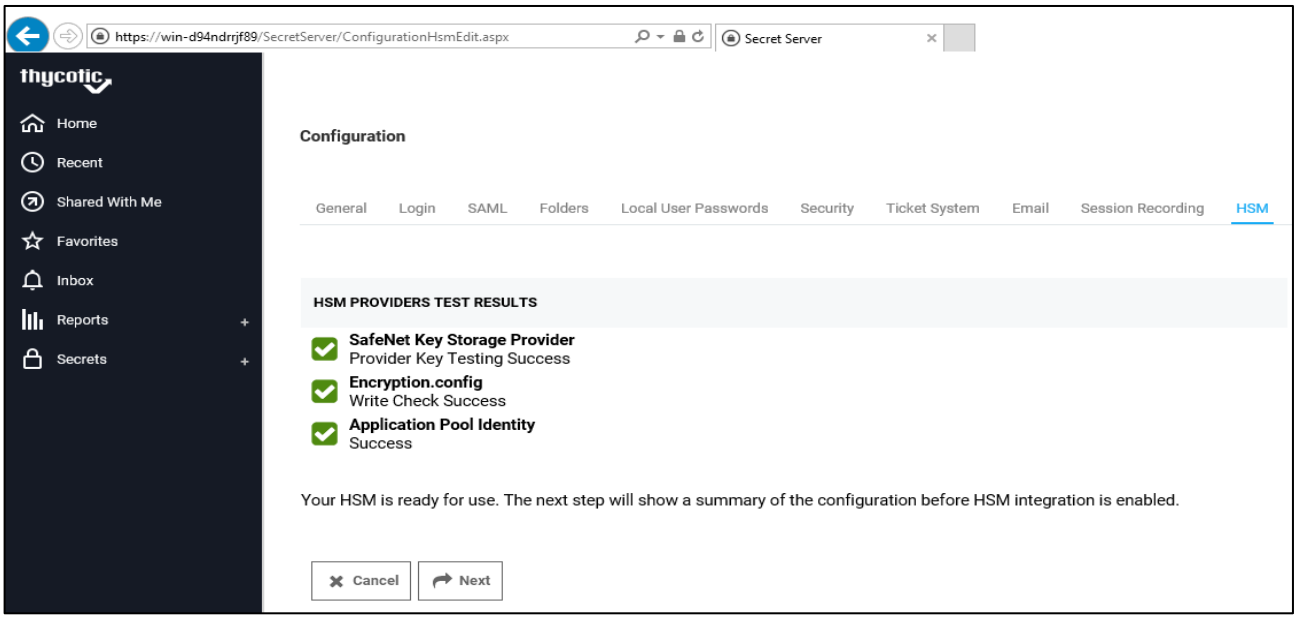


6. Select **SafeNet Key Storage Provider** from the **Persistent Provider** drop down box under the **HSM PROVIDERS** section and select key size of RSA from **Key size** drop down box.

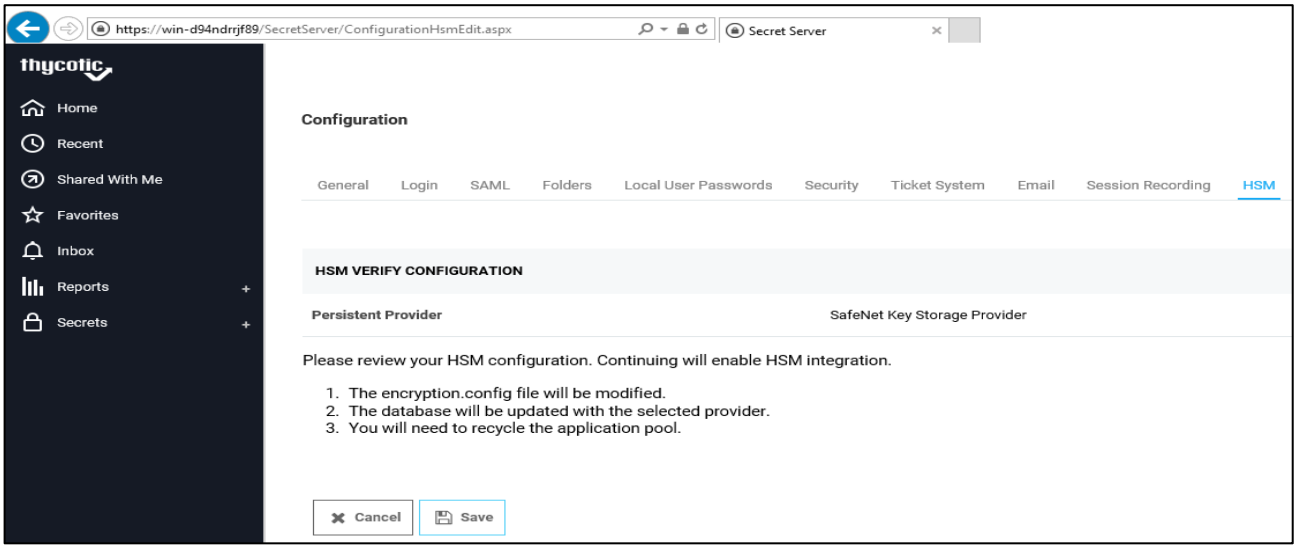


7. Click **Next**. After this, Secret Server will simulate encryption and decryption operations.

8. Verify whether the configuration has been successful by checking the details under the HSM PROVIDERS TEST RESULTS section.

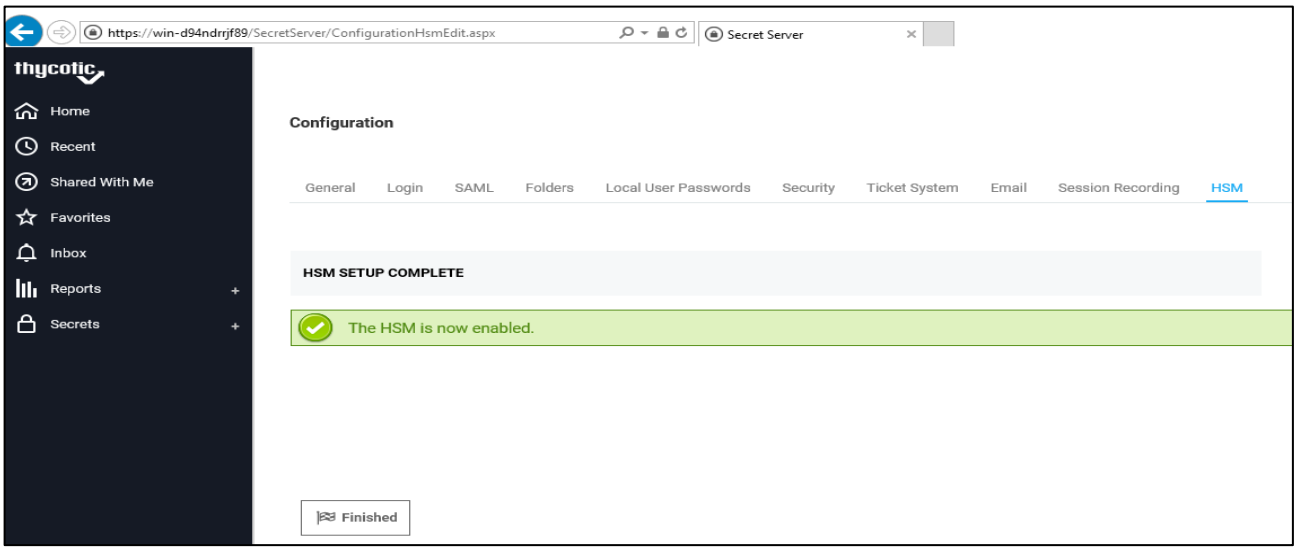


9. Click **Next**. Review your HSM configuration under the **HSM VERIFY CONFIGURATION** section.



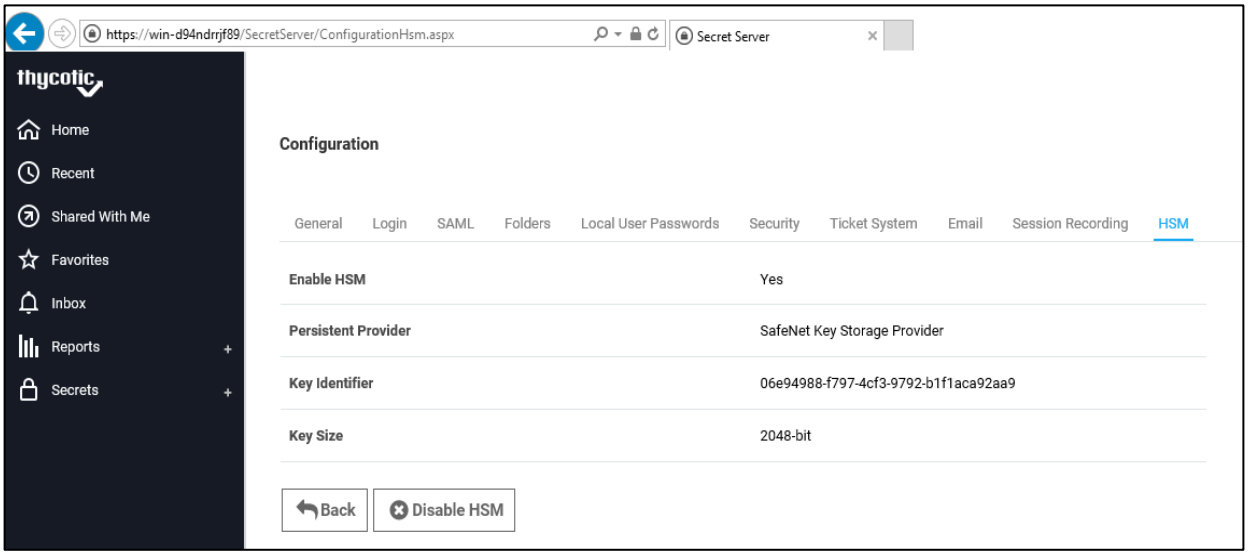
10. Click **Save** to complete the HSM setup. You will see the following message on the screen:

"The HSM is now enabled."



11. Click **Finished** and then restart the IIS for configuration changes to take effect.

12. The HSM configuration is saved and can be viewed under **HSM** tab. The Secret Server encryption key is now stored on Luna Network HSM partition.



13. Verify the key using the lunacm utility:

```
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 ->                Thycotic
        Serial Number ->        1280780175917
        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


lunacm:> role login -n co

        enter password: ********

Command Result : No Error


lunacm:> partition contents

        The 'Crypto Officer' is currently logged in. Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:          f81597e9-b459-4a4e-89c5-d5c3af22821b
        Handle:         325
        Object Type:    Private Key
        Object UID:     4c09000018000003cb640800

        Label:          f81597e9-b459-4a4e-89c5-d5c3af22821b
        Handle:         186
        Object Type:    Public Key
        Object UID:     4b09000018000003cb640800


        Number of objects:  2


Command Result : No Error
```

14. Copy **encryption.config** file from this node to all other nodes.

15. Restart each nodes' Application Pool for the changes to take effect.

16. Log in to Secret Server from any node and verify that the HSM is enabled and key identifier displayed is correct. This completes the integration of Thycotic Secret Server Cluster with a Thales Luna Network HSM. Secrets created in Thycotic Secret Server Cluster from any node will now use encryption keys residing in the HSM partition.