vSEC CMS with Luna 7 HSM and DPoD

Integration Guide

gemalto
a Thales company

Contents

Preface

This document is intended to guide security administrators through the steps for the vSec CMS *S Series* Integration with SafeNet Network HSM and HSMoD service, and also covers the necessary information to install, configure and integrate vSEC CMS with SafeNet Network HSM and HSMoD.

Scope

This document outlines the steps to integrate vSEC CMS with SafeNet HSM. SafeNet HSM is used to secure the Master Encryption Key for vSEC CMS.

Revisions

Name	Date	Reason for change	Version
Akhil Babal	06/08/2019	Document created	1.0

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	**New product name**
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna Client	SafeNet HSM Client

NOTE: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

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. Contains 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	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**.)

Convention	Description
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read 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.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

Overview

This document is intended to guide security administrators through the steps for the vSEC CMS Integration with SafeNet Luna 7 HSM and DPoD (HSM on demand service), and also covers the necessary information to install, configure and integrate vSEC CMS with SafeNet Luna HSM.

A HSM can be used to store the master key(s) used when performing administration key operations with the *S-Series* such as registering a smart card token or PIN unblock operations. The *S-Series* makes use of the PKCS#11 interface available in the HSM. All management functions around the master key stored on the HSM should be managed by the HSM key management tools available with LunaClient or DPoD service client.

NOTE: It is expected that the HSM PKCS#11 module is installed and configured to connect to the HSM on the server where the *S-Series* is installed. It is required that the 32 bit version (dll) of the HSM PKCS#11 module is available. The *S-Series* will search in the system path for the PKCS#11 module.

3rd Party Application Details

- vSEC CMS S Series 5.4

Supported Platforms

The following platforms are tested with SafeNet Luna HSM:

vSEC CMS S Series 5.4

Platforms Tested	SafeNet Luna HSM Client Software Version	SafeNet Network HSM Appliance S/W version	SafeNet Network HSM Appliance F/W version
Windows 2016	7.3	7.3.0-165	7.3.0

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding the configuration and setup of the box on Windows systems. Before you get started ensure the following:

- SafeNet Network HSM appliance and a secure admin password.
- SafeNet Network HSM, and a hostname, suitable for your network.
- SafeNet Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Network HSM appliance.
- Create and exchange certificates between the SafeNet Network HSM and your Client system.
- Create a partition on the HSM, remember the partition password that will be later used by vSEC CMS.
- Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Network HSM. The general form of command is “C:\Program Files\SafeNet\LunaClient> vtl verify” for Windows.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Data Protection on Demand (DPoD) HSM service Setup

Refer to SafeNet Data Protection on Demand Documentation for service client setup steps and details.

https://gemalto.na.market.dpondemand.io/docs/tenant_admin/Content/dpod/services/hsmod/hsmod.html

Before you get started ensure the following:

- SafeNet DPOD subscription is available.
- HSM on Demand tile is available under Tenant Account.
- Application owner account is created and has access to HSMoD service tile.
- HSMoD service client is configured.
- HSMoD service is accessible using the service client.
- Partition is initialized using LunaCM tool.
- Partition roles are initialized and password for Crypto Office is created. This CO password will be required in vSEC settings.

vSEC CMS Prerequisites for Installation

Before installing vSEC CMS on a Windows Server, ensure that the system chosen meets the necessary operating system, hardware, software, and communications requirements.

For the installation requirements for data server products, see Appendix.

vSEC CMS Installation and Configuration

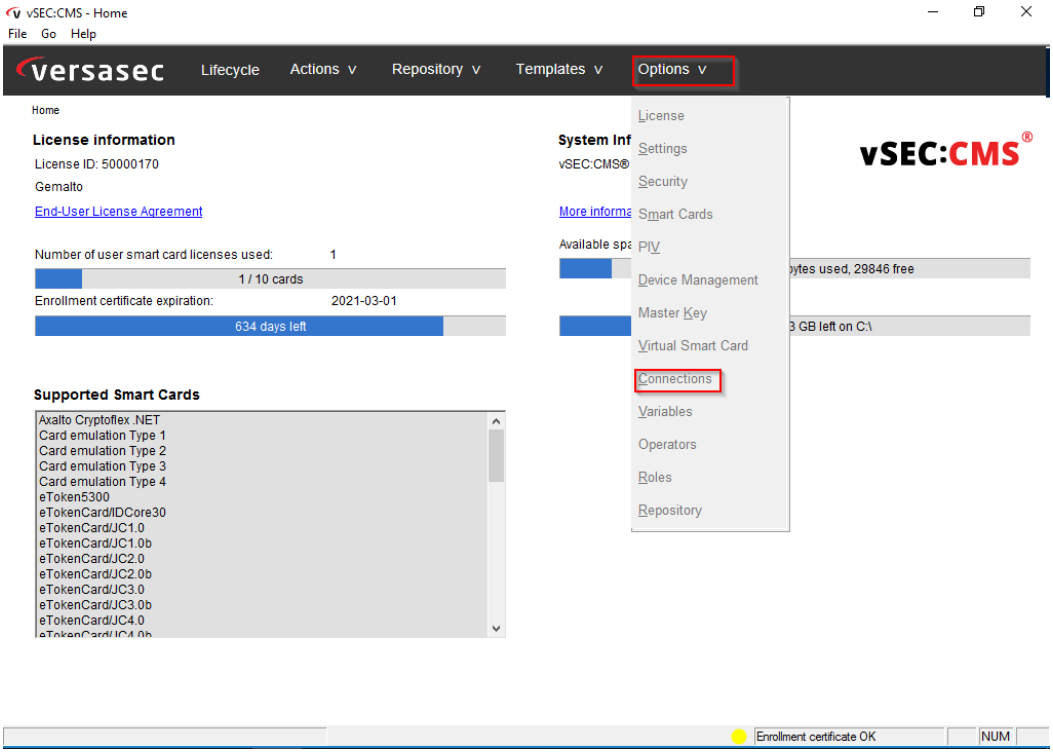
vSEC CMS must be installed on the target machine to carry on with the integration process. For a detailed installation procedure of vSEC CMS refer to the Versasec Documentation, reference of the same is provided in Appendix.

2
Integrating SafeNet Luna HSM with vSEC CMS

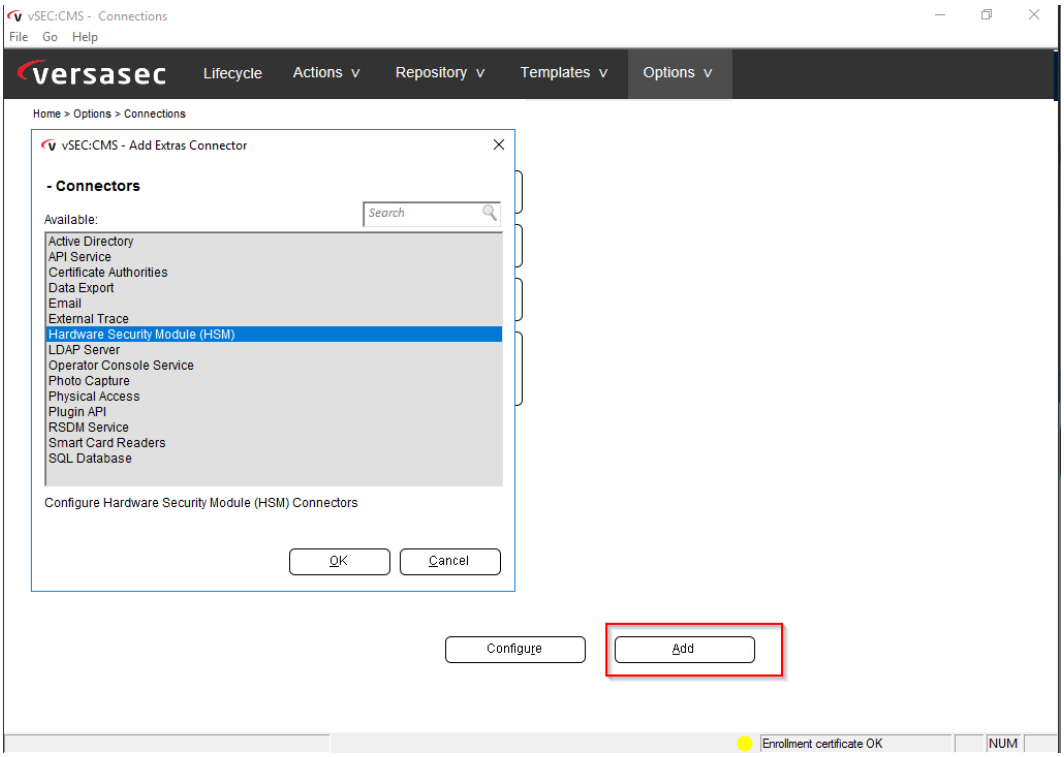
Creating a Connection with HSM from vSEC CMS

Follow these steps to create a connection with Luna 7 after vSEC CMS is installed using System Owner card.

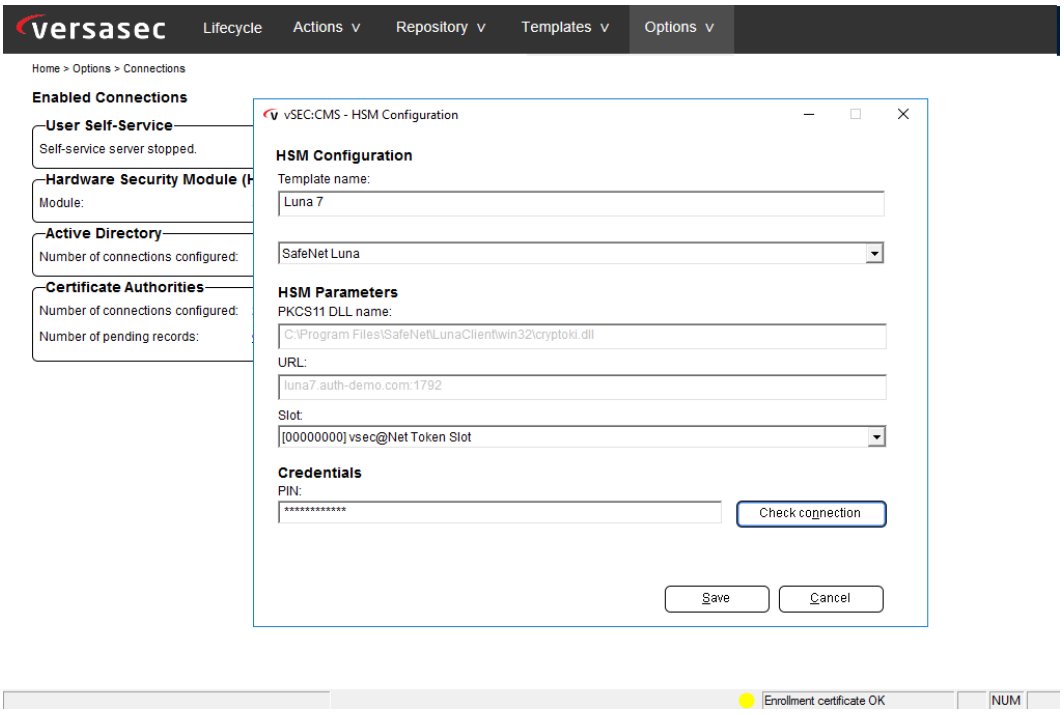
1. Navigate to Options> Connections option



2. To create a new connection, select Add and then Hardware Security Module (HSM)

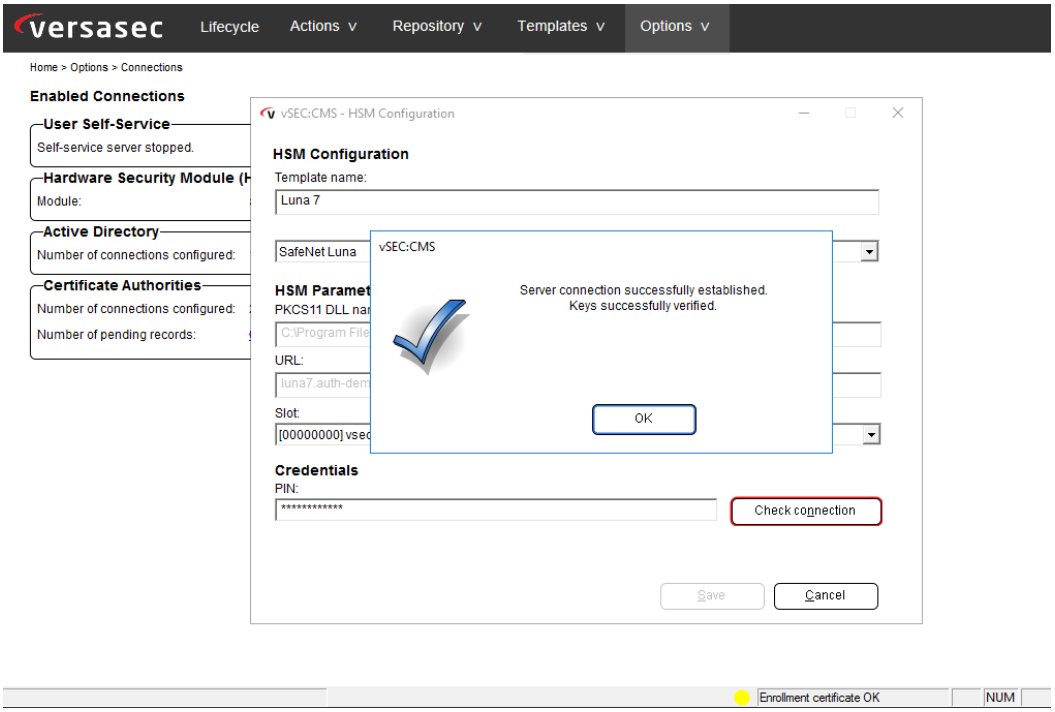


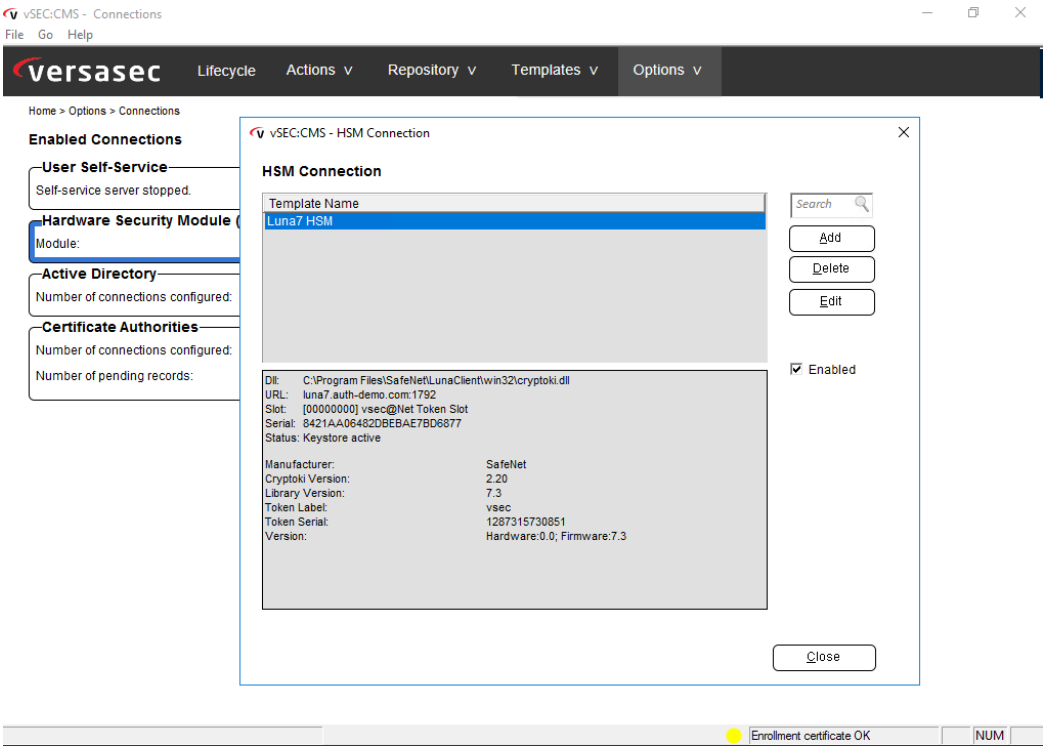
3. Create a Template name and select SafeNet Luna from the drop down list.



4. Notice that if the Luna client is correctly installed on the vSEC CMS server and configured properly with Luna 7 HSM, the PKCS11 DLL and server details will auto populate. Select your slot ID and provide the

Cypto Officer password in the fields and check connection to verify CMS can connect to the partition on Luna HSM.

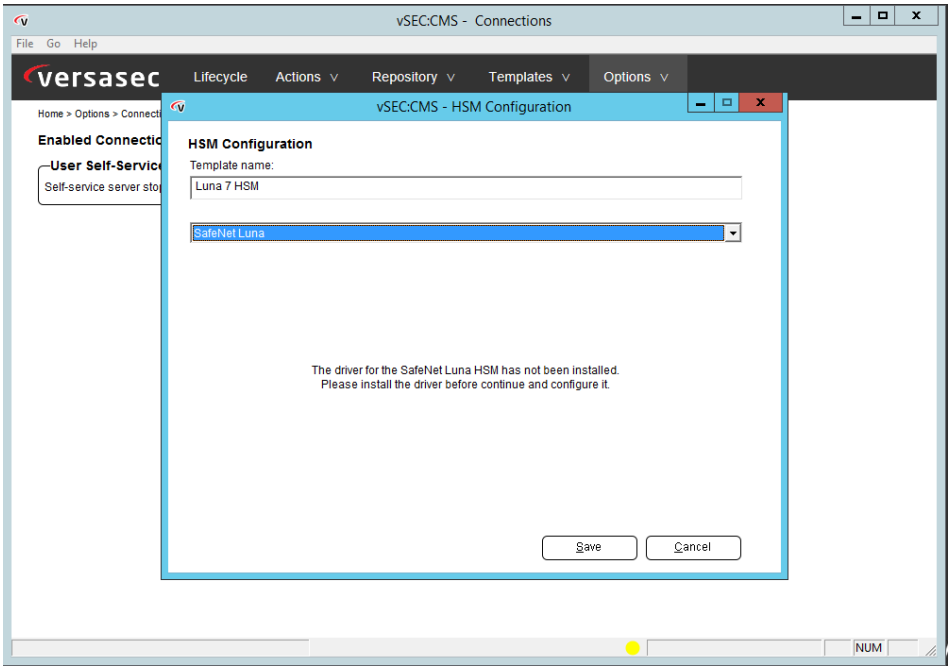


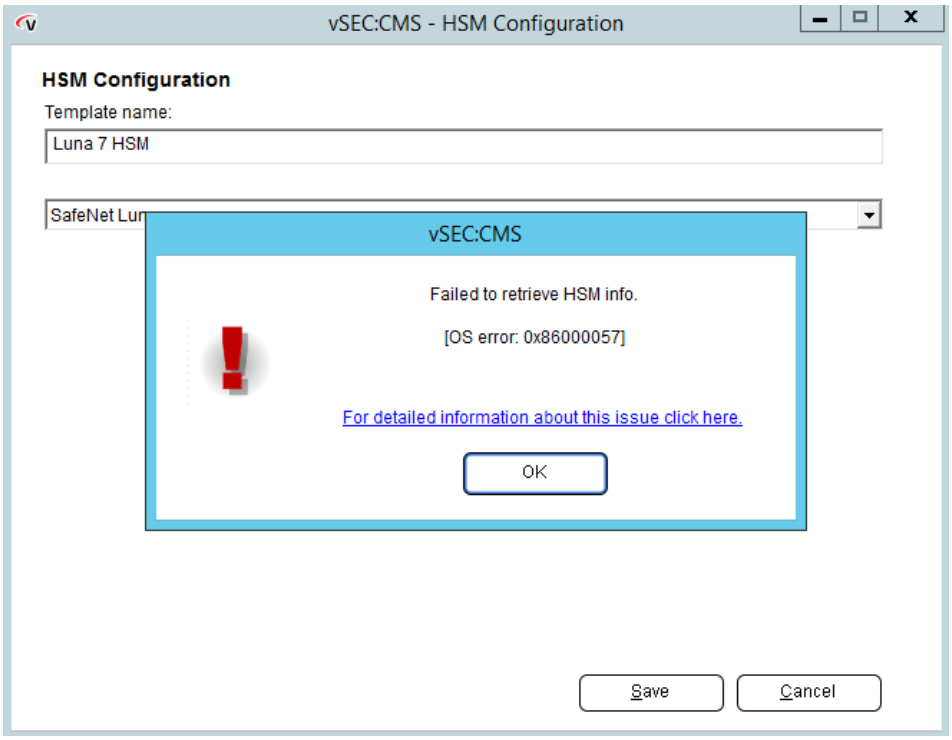


Troubleshooting Tip>

If the Luna Client is not correctly configured then it is warranted to run into errors.

When selecting SafeNet Luna HSM from the drop down list while adding a HSM connection, if you run into below shown error messages

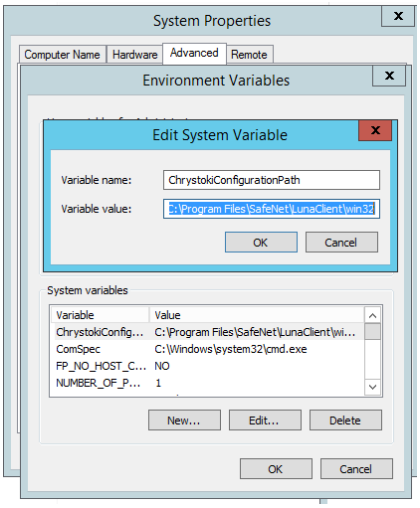




The reason is by default Luna Client does not set ChrystokiConfigurationPath in System Environment Variables to point to 32 bit library

NOTE: It is expected that the HSM PKCS#11 module is installed and configured to connect to the HSM on the server where the *S-Series* is installed. It is required that the 32 bit version (dll) of the HSM PKCS#11 module is available. The *S-Series* will search in the system path for the PKCS#11 module.

When you modify and update the path in env variable then error will be resolved.

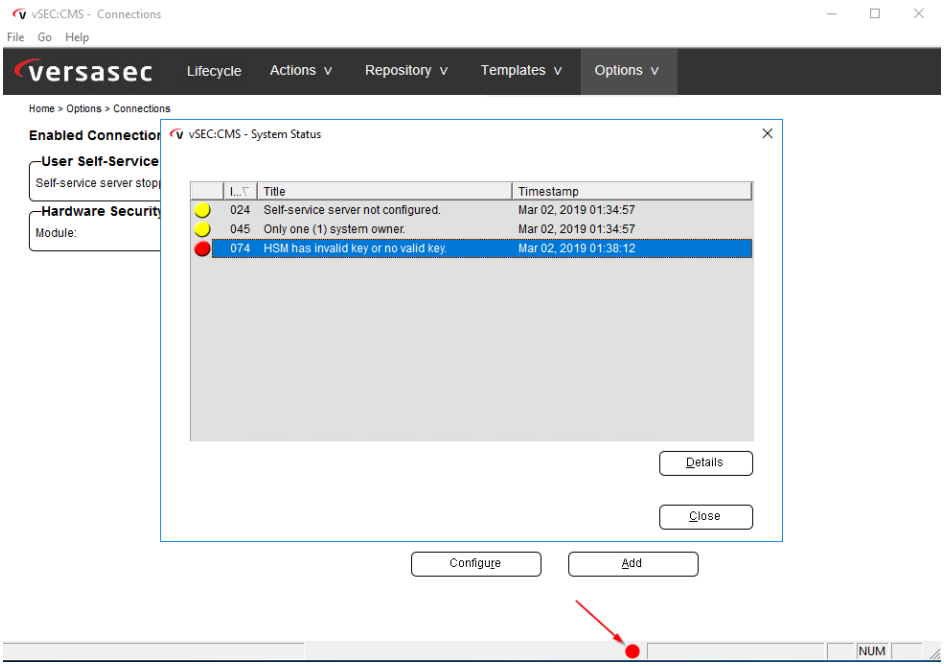


Generate New Master Key

If it is required to generate a new master key, either on the operator token or on the HSM follow the instruction here.

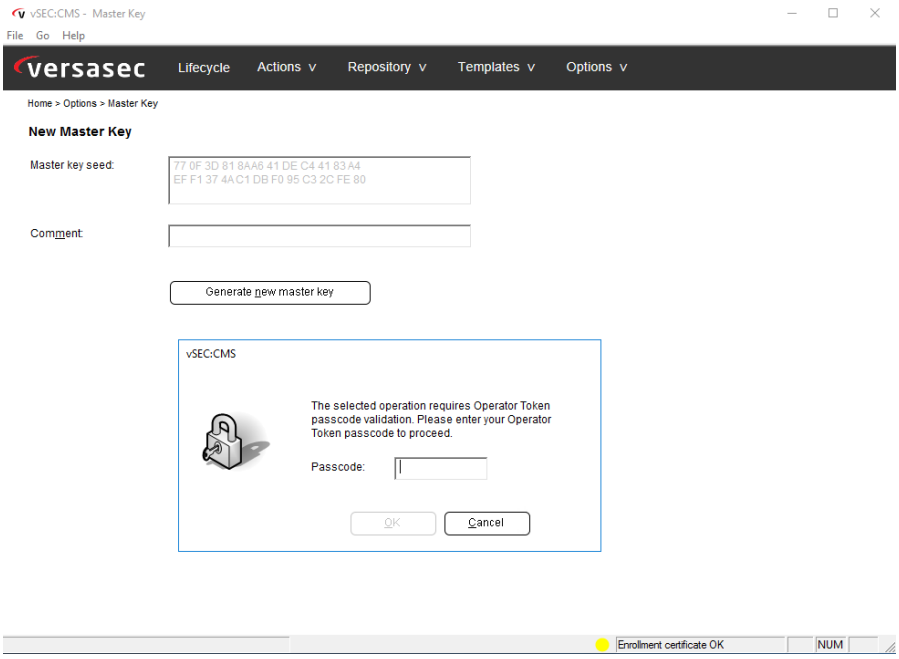
WARNING: It is important to remember that any new user smart card administration key will be diversified from the newly generated master key. Any user smart card administration key diversified from the old administration key of the *S-Series* application will remain operable. However, it is recommended to re-register those user cards issued from the old administration key of the *S-Series*. This will update the user's smart card administration key so that it is diversified from the new master key.

For a new installation of vSEC CMS after successfully creating a HSM connection explained in previous section it is required to generate a new Master Key. This is shown as under System Status too



Follow these steps to generate a new Master Key

1. From **Options – Master Key** click the **Generate new master key** button to start the process. A



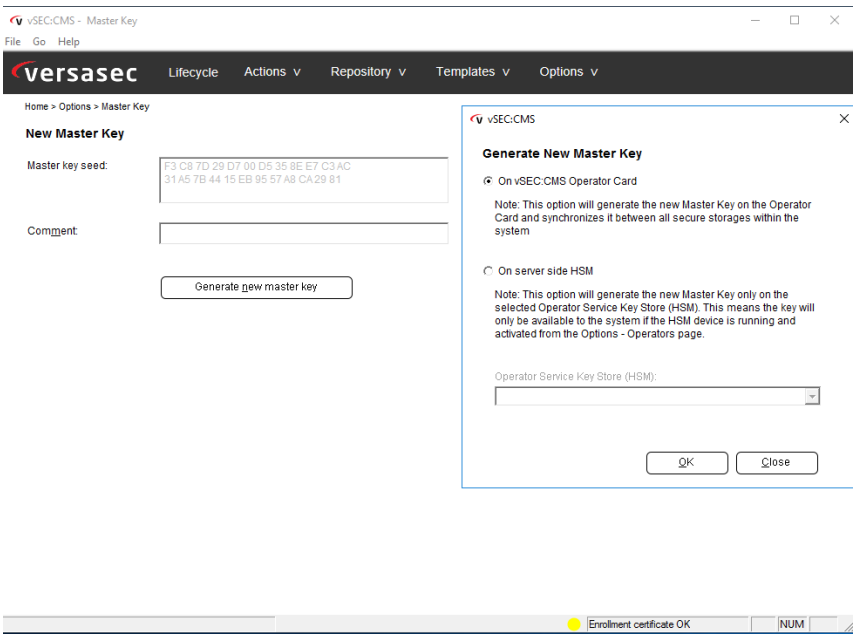
A dialog will be displayed.

2. Select **On vSEC:CMS Operator Card** if it is required that the new master key is generated on the connected full-featured operator token. The new master key will also be migrated to the HSM and any

other full-featured operator token(s) used in the *S-Series*. For a full-featured operator token the migration will take place the next time an operator logs onto the **S-Series**

3. Select the option **On server side HSM** if it is required that the new master key should be generate on the HSM only. In this case the new master key will only be available on the HSM. Therefore, all operations that require master key access to the newly generated master key will need to use the HSM.

   NOTE: For any smart card that was previously managed by the *S-Series* with a full-featured operator token that used an older master key that was not generated by the HSM it will be possible to continue to manage these cards but it is recommended to update these cards so that they will be managed by the newly created master key.

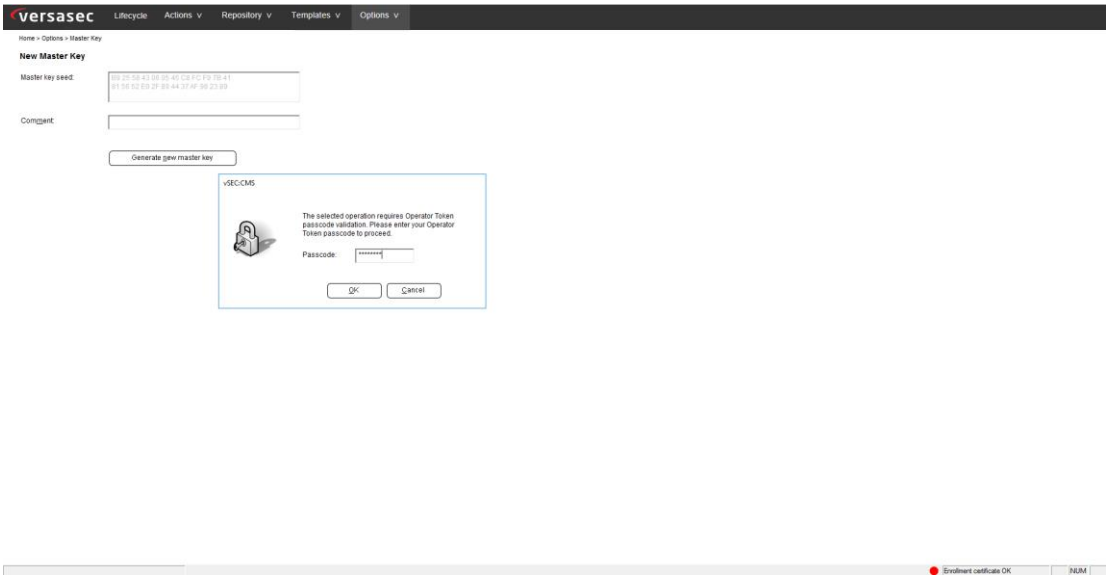


As shown in the screen shot above the option to select **On Server side HSM** is unavailable. This will mean that the OSKS will need to be activated from the **Options - Operators** page. Instructions to create Operator Service Key Store (OSKS), see Appendix.

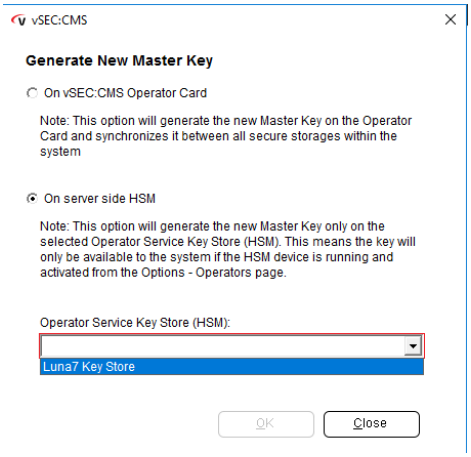
It is required to create OSKS before you follow next steps. Please see Appendix.

4. After generating, creating and enabling the OSKS the next step is to generate the new master key.

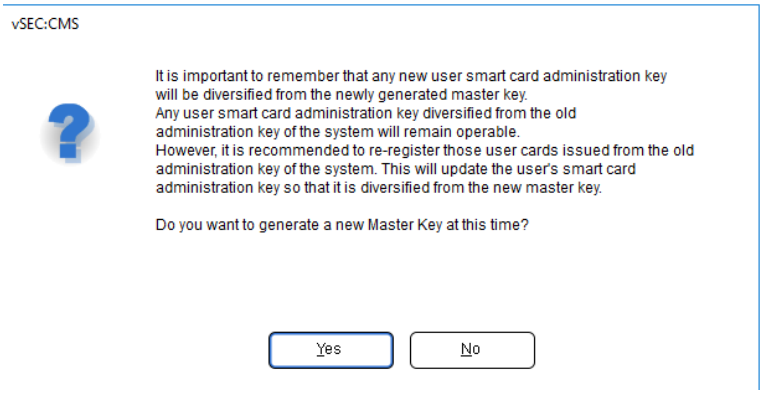
   From **Option > Master Key**, select **Generate new master key** option and provide operator card login



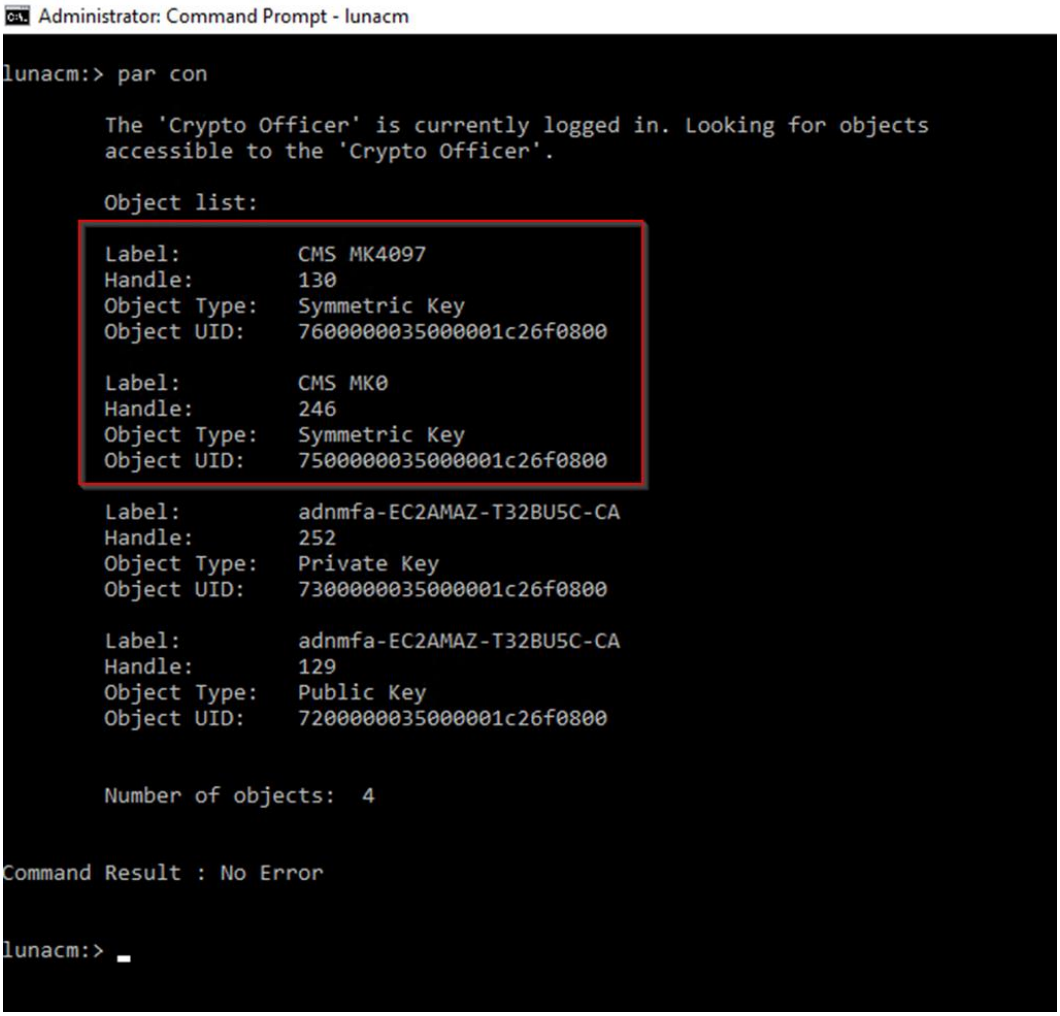
Select **On server side HSM** option and select key store added in step 3 (instruction in Appendix)



Please read the warning message carefully and select yes.



After selecting yes, the new master keys will be created on the HSM as you can see via lunacm



Notice two symmetric keys are available, one was generated and one was migrated from your operator card in to HSM as explained in one of the steps in OSKS configuration.

At this stage, vSEC CMS is correctly configured with master key generated on the HSM.

3
Integrating DPoD with vSEC CMS

Steps to integrate vSEC CMS with HSM on Demand service are exactly same as they are explained in integration HSM with vSEC CMS (Chapter 2).

NOTE: It is expected that the HSM PKCS#11 module is installed and configured to connect to the HSM on the server where the *S-Series* is installed. It is required that the 32 bit version (dll) of the HSM PKCS#11 module is available. The *S-Series* will search in the system path for the PKCS#11 module.

WARNING: DPoD client by default only provides 64-bit version dlls. However, for vSEC integration it is required that 32 bit version dll of cryptoki.dll (PKCS#11 module) is available. Please contact Technical support team to request 32 bit version of dlls for DPoD client.

Creating a Connection with DPoD from vSEC CMS

Refer to the steps mentioned in integration with HSM, previous section. The steps are exactly same.

Important>

Once 32 bit version dlls are available, copy the win32 folder to DPoD client location and follow these steps before creating a connection in vSEC CMS.

1. Ensure to retain the original crystoki.ini created using DPoD client by running ***setenv***
2. Crystoki.ini initially created using ***setenv*** must be available to the location where 32 bit version dlls are located.
3. Accordingly update the System and user environment variable to update the ChrystokiConfigurationPath to location where 32 bit version cryptoki.dll is located.
4. In vSEC CMS while creating the connection select SafeNet Luna as option to add DPoD HSM on Demand to generate a new master key.

4
Appendix

1. The installation requirements for vSEC CMS products are listed in:

https://versasec.zendesk.com/hc/en-us/articles/115000766453-S-Series-Overview

2. The installation procedure of vSEC CMS is described in:

https://versasec.zendesk.com/hc/en-us/articles/115000402934-Install-and-Configure-S-Series-on-First-Use

3. Procedure to create Operator Service Key Store:

   Follow the instructions in this section on how to configure the *S-Series* to use an HSM for OSKS. During this process, the master key stored on the operator smart card token will be migrated to the HSM.

Important: It will be required to RDP to the server where the *S-Series* is installed to perform all the steps below.

Important: The OSKS in this case is an encrypted component that runs as a service which is accessible only by the *S-Series*.

Important: The Operator needs to use a Full-Featured Operator Card that has a role of System Administrator in order to carry out this process.

Important: It will be necessary to have setup a connection to the HSM from Options - Connections before starting this setup.

From vSEC CMS version 5.3 onwards **Activator Tool (AT)** is available. The activator tool can be used to Generate **Operator Service Key Store (OSKS)** installer.
The AT is a standalone application that is located in the **tools** folder of the *S-Series* installation. The AT is named **Versasec-Activator.exe** in this folder. The AT requires internet access so it may be necessary to copy the AT to a host that has internet access if the *S-Series* is installed in a restricted environment.

Generate OSKS Installer

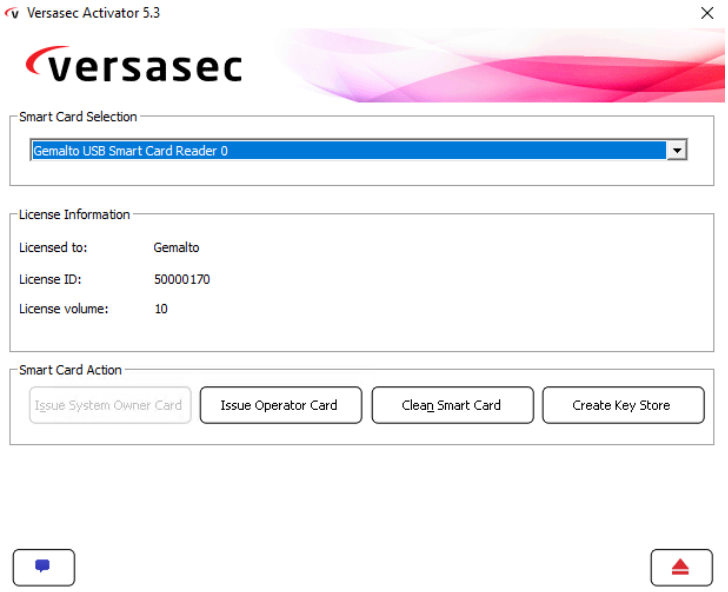
The OSKS is used by the S-Series to perform administration key operations. In order to set this up it will be firstly required to generate an OSKS installer.

Important: It will be required to use the SO to perform this task.

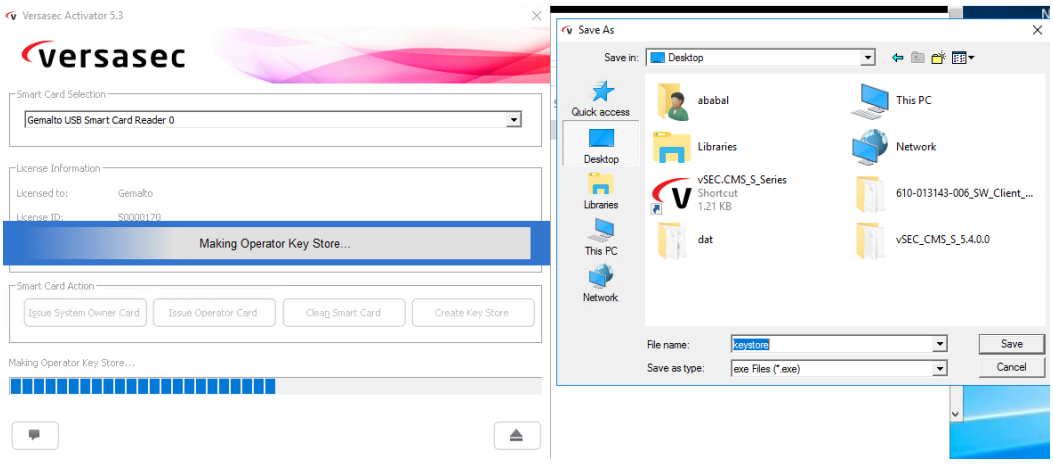
Important: It will be required to have the latest version of the Gemalto minidriver installed on the host where you are running the AT from.

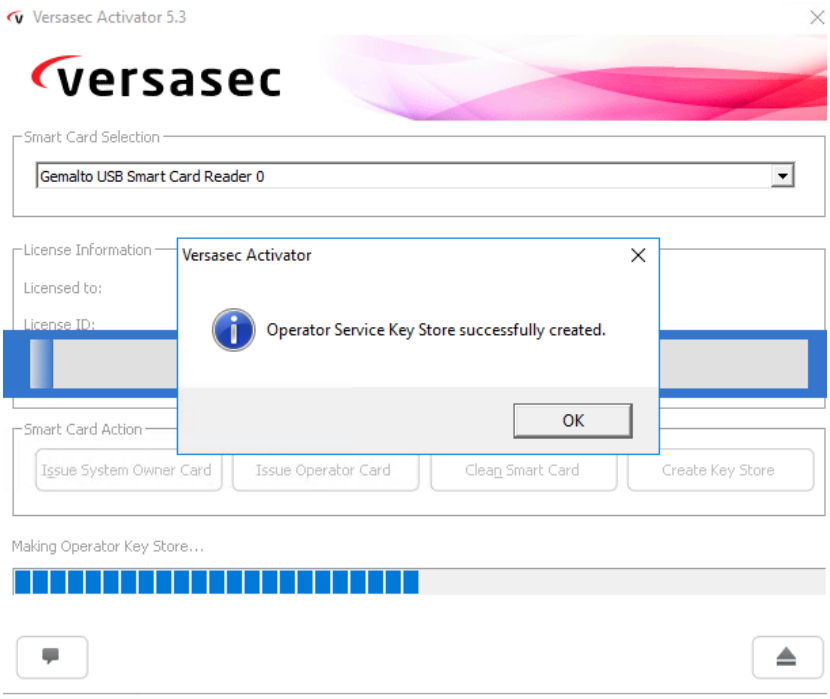
Important: The host where you are running the AT from will need to have an internet connection.

In order to generate the OSKS installer start the AT. Attach the SO token and from the **Smart Card Selection** select the reader from the drop-down list that the SO is inserted into.



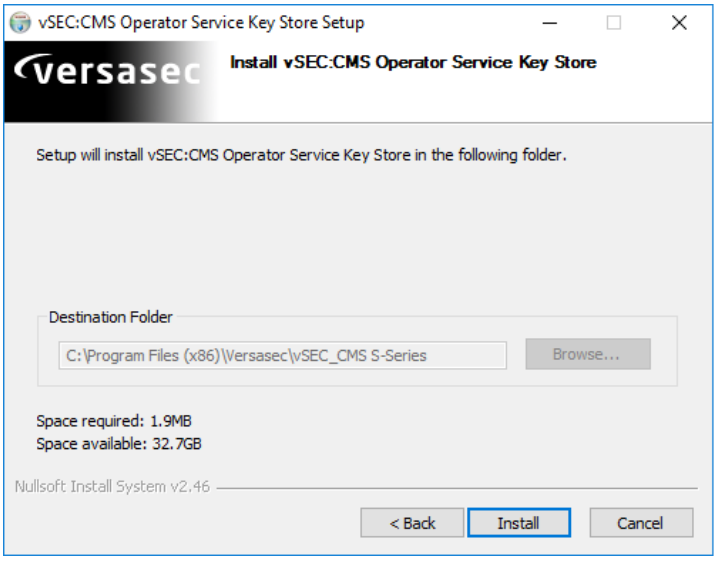
Click the **Create Key Store** button. Enter the PIN for the SO when prompted. At the end of the process you will be prompted to save the OSKS installer. Save the installer to complete this process.





Then you should move this installer to the server where the *S-Series* is installed.

Copy the installation package to the *S-Series* server. Make sure to close any open *S-Series* consoles and start the installation.

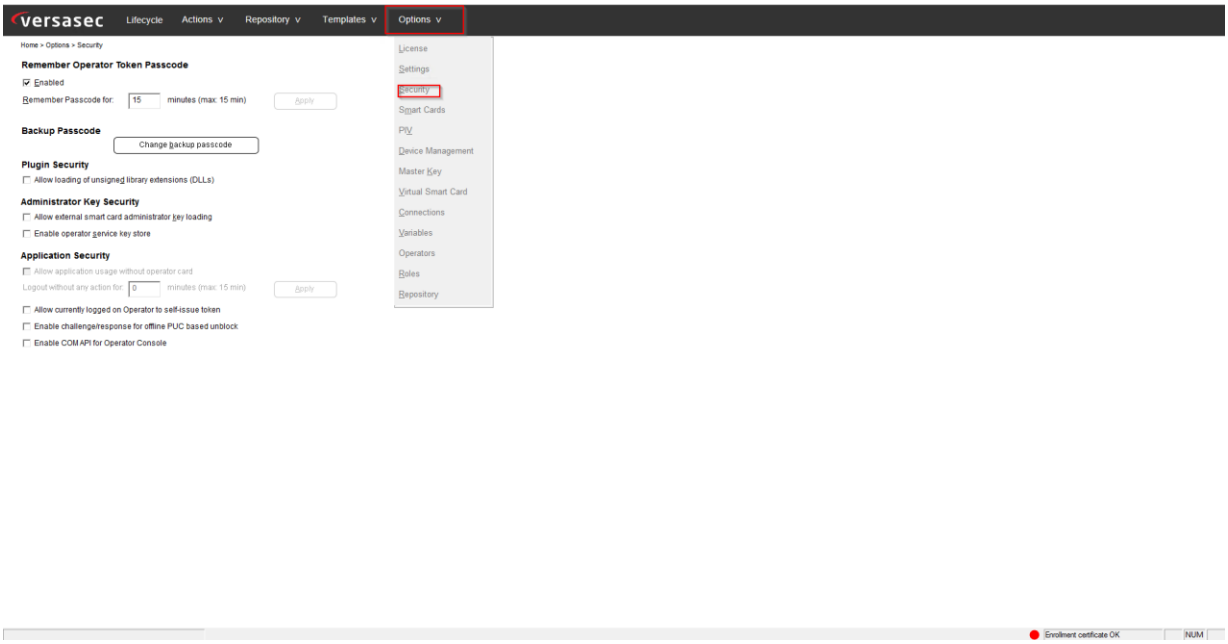


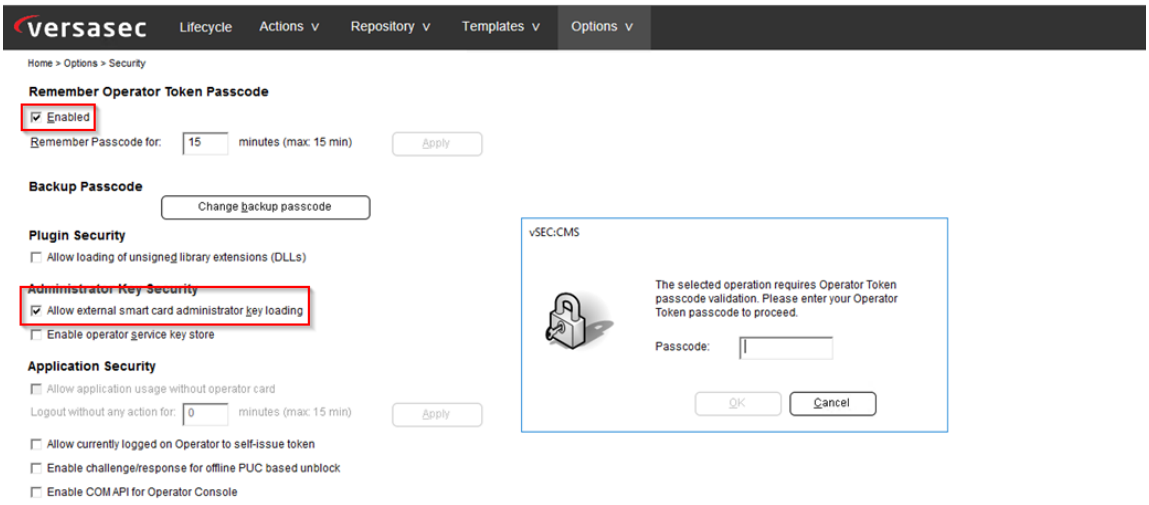
Enable OSKS on vSEC CMS

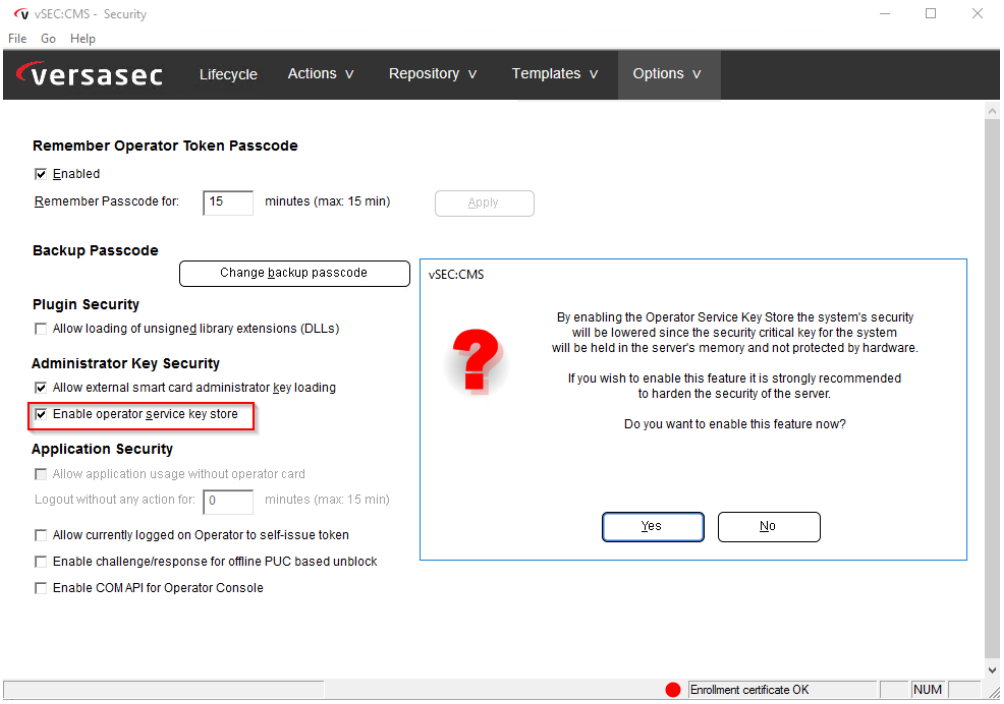
When the installation completes log onto the *S-Series* application with the full-featured operator token used in step 1 or the System Owner token if you are using the **Activator Tool**.

Important: You should see a message dialog informing the Operator that the package was successfully installed. If you do not see this message dialog then the installation was not successful.

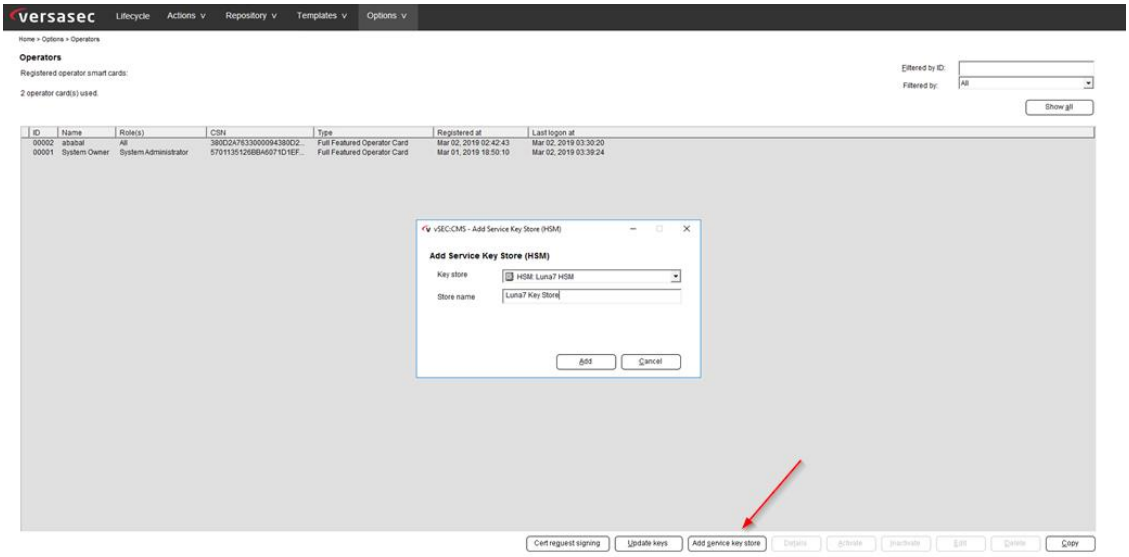
Start the *S-Series* application and from the **Options - Security** page enable **Allow external smart card administration key loading** and **Enable operator service key store** check boxes.



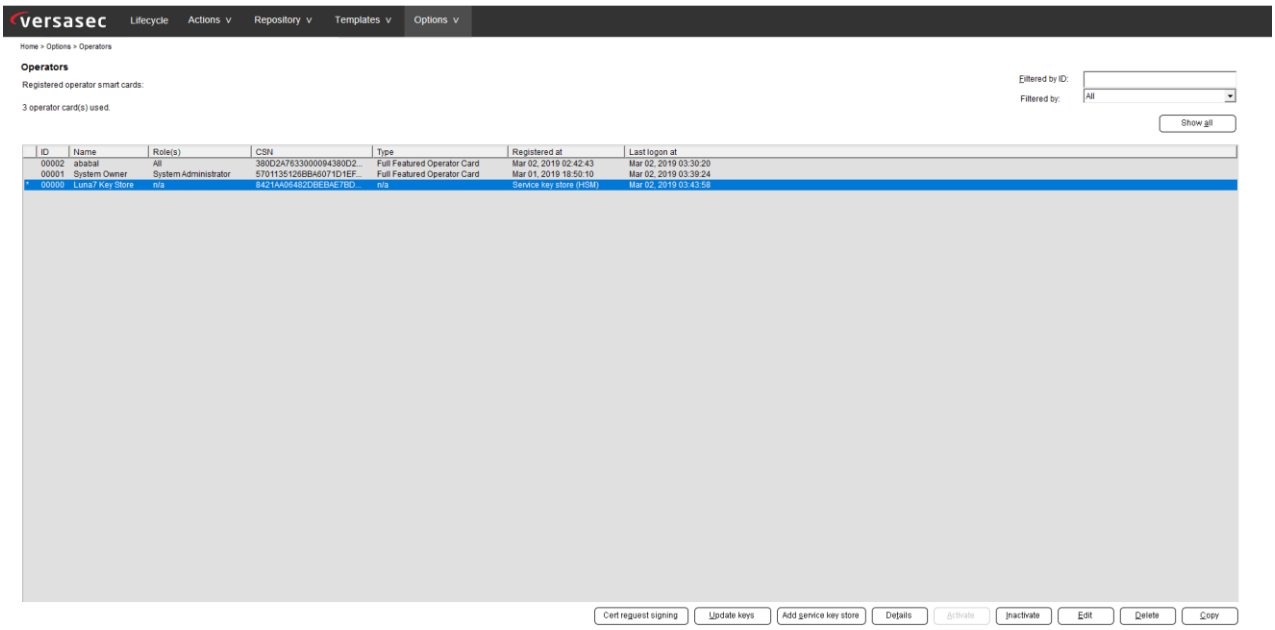




From the **Options - Operators** page click the **Add service key store** button. You should see that the **Key store** field is automatically populated with HSM. Enter a name for the **Store name** field and click the **Add** button to create the key store.



When complete you will see that the service key store is added and that it is active. This completes the setup. The *S-Series* will use the master key stored in the HSM for any operations requiring administration key operations.


versasec
Lifecycle
Actions v
Repository v
Templates v
Options v
Home > Options > Operators
Operators
Registered operator smart cards:
3 operator card(s) used.
Filtered by ID:
Filtered by:
All
Show all
ID
Name
Role(s)
CSN
Type
Registered at
Last logon at
00002 ababal All 380D2A7633000094380D2... Full Featured Operator Card Mar 02, 2019 02:42:43 Mar 02, 2019 03:30:20
00001 System Owner System Administrator 5701135126BB46071D1EF... Full Featured Operator Card Mar 01, 2019 18:50:10 Mar 02, 2019 03:39:24
00000 Luna7 Key Store n/a 8421AA06482DBEBAE7BD... n/a Service key store (HSM) Mar 02, 2019 03:43:58
Cert request signing
Update keys
Add service key store
Details
Activate
Inactivate
Edit
Delete
Copy