THALES

www.thalesesecurity.com

THALES E-SECURITY

Microsoft SQL Server 2016 Always Encrypted

Integration Guide

Version: 1.2
Date: 31 May 2017

Table of Figures and Diagrams

Always Encrypted and Thales nShield HSMs

Introduction to Always Encrypted

Always Encrypted is a feature in Windows Server 2016 designed to protect sensitive data both at rest and in flight between an on-premises client application server and Azure or SQL Server databases.

Data protected by Always Encrypted remains in an encrypted state until it has reached the on–premises client application server, this effectively mitigates man in the middle attacks and provides assurances against unauthorized activity from rogue DBAs or admins with access to Azure / SQL server Databases. Always Encrypted was designed to be used in conjunction with TDE however; TDE is **NOT** a requisite for implementing Always Encrypted.

Configuring Always Encrypted involves creating and provisioning cryptographic keys, specifically:

- A **C**olumn **M**aster **K**ey – The CMK, is an asymmetric RSA encryption key of size 2048 bits
- One or more **C**olumn **E**ncryption **k**ey(s) - A CEK, is a symmetric AES key of size 256 bits.

The CEK is responsible for encrypting the database column while the CMK is protected by the HSM and is responsible for wrapping (encrypting) the CEK.

The table below shows current support for the different data operations.

Task	SSMS	T-SQL
Provisioning column master keys, column encryption keys and encrypted column encryption keys with their corresponding column master keys	Yes	No
Creating key metadata in the database	Yes	Yes
Creating new tables with encrypted columns	Yes	Yes
Encrypting existing data in selected database columns	Yes	No

The Column Master Key is generated using the Thales nCipher CNG provider via the HSM and the key(s) stored in an encrypted state on the on-premises client application server in the kmdata\local folder.

Note: It is recommended that the server configured with Always Encrypted be located on a different server than that on which the database resides.

Always Encrypted supports two named types of encryption, **Deterministic** and **Randomized**. Selecting deterministic encryption means that the same encrypted value will be produced from the same plaintext value each time encryption occurs, this allows for point lookups, equality joins, grouping and indexing on encrypted columns. However, this has implications on the security of the data as it potentially allows an attacker to ‘guess’ the plaintext from the recurring cipher text through emerging patterns within the encrypted columns. Deterministic encryption should not really be used where a small set of values are presented, e.g. True / False, Yes / No etc. Randomized encryption is more secure, as it produces different cipher text values from the same plaintext every time the data is encrypted, eliminating the predictable aspects associated with deterministic encryption, however, this also removes the ability to perform any search operations on the encrypted data in situ.

Although columns encrypted with Always Encrypted are never revealed in Plaintext (in the clear) on the database server, it is still possible to perform limited queries on some types of data within the database engine itself, depending on the initial encryption method used.

Requirements

This integration uses the Always Encrypted wizard to create and provision the keys and was performed and tested using the following configuration:

- Microsoft Windows 2012 R2
- SQL Server 2016
- SQL Server Management Studio 17 (SSMS)
- .NET Framework 4.6.1
- Thales nShield HSM with Security World software 12.30
- Thales nShield Hardware Security module (nShield Solo +; nShield Connect +)

The integration process was performed using SQL Server Management Studio 17 (as supplied with SQL server 2016) to query the database table(s).

You must install .NET Framework 4.6.1 on the on-premises client server before installing SQL Server Management Studio (SSMS). The download can be obtained via the Microsoft website:

https://www.microsoft.com/en-us/download/details.aspx?id=49982

Using multiple on-premises client servers

In order for multiple on-premises client application servers to share and decrypt database columns encrypted with HSM assisted Always Encrypted, there is a requirement that each client server wanting access to the contents of data encrypted with a given Column Encryption key(s) protected by a specific Column Master Key that the server must have access to an HSM in the same Security World and have a copy of the Column Master Key stored on its local drive in “C:\ProgramData\nCipher\Key Management Data\local”.

The default location for all nShield Security World data (this includes the HSM generated Column Master Key) can be found in the “C:\ProgramData” folder, by default this is a hidden folder. To view this folder open an explorer window go to the “View” tab and tick the check box named “Hidden items”

For more information about:

- Configuring a Thales nShield HSM, see the Installation Guide for your HSM
- Security World Configuration, see the appropriate User Guide for your HSM

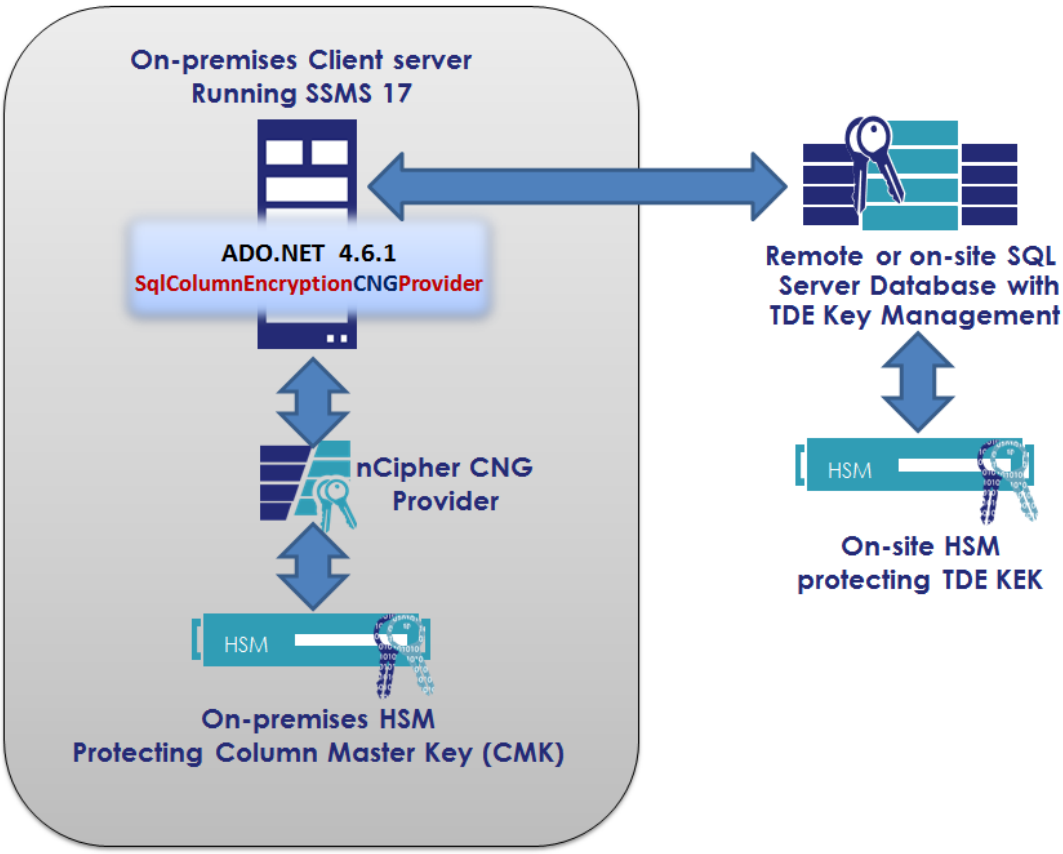


Figure 1: Always Encrypted using HSM to protect CMK

The Thales Security World Software must be installed onto the on-premises application server being used for Always Encrypted.

Note: If you are running TDE with nShield HSMs the same security world can be used or if preferred an entirely different Security World can be implemented. If you prefer to use a different Security World you will need further HSMs as the nShield HSM can only host a single Security World instance at any one time.

Security Worlds and key protection

This section covers the options for Security World when using Always Encrypted. Always Encrypted uses the nCipher CNG provider; There are certain restrictions on the use of these providers concerning methods of authentication and operations that are available. The table below shows the restrictions on HSM key protection methods available when using the Thales nCipher CNG provider.

Security world Type	Protection / Credential	Supported	Works in Pool mode
FIPS 140-2 Level 2 (Default)	Module	Yes	Yes
	SoftCard	No	No
	Operator Card Set 1/ n	Yes	No
	Operator Card Set k / n	Yes	No

Table 1: Supported key protection methods for nCipher CNG provider

Configuring nShield Hardware Security Modules for use with Always Encrypted

Ensure that the Thales Security World software is installed on the on-premises server that will be used as an Always Encrypted client.

Install and register the CNG provider

Once the Security World Software has been installed you must run the CNG install wizard to install and register the Thales Key Storage Provider (KSP). This can be performed via the CNG install wizard that can be found in the "Apps By name" screen of the Desktop.

Click the start button and then click on the  to access all applications. Look for the recently installed nCipher utilities.

Figure 2: Install and register nShield provider

Double click the CNG configuration wizard. (If the User Access Control prompt pops up click "YES" to continue.)

Figure 3: CNG install Welcome screen

The following screen prompts you to enable Pool Mode. Leave the default value with the check box unticked and click "Next".

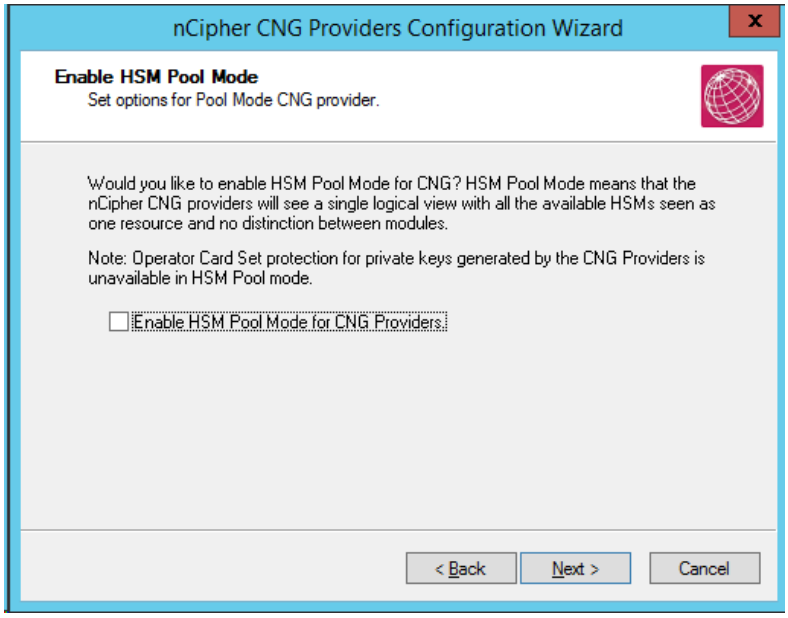


Figure 4: Select to enable / Disable Pool Mode

If you already have a security world that you intend to use for Always Encrypted The next screen will prompt you to select that via the "**Use the existing security world**" button. If you do not currently have a security world or would like to create a new security world then check the "**Create a new security world**" radio button and click "Next".

Ensure that the Set Module States show the available modules as

- Mode = operational
- State = usable

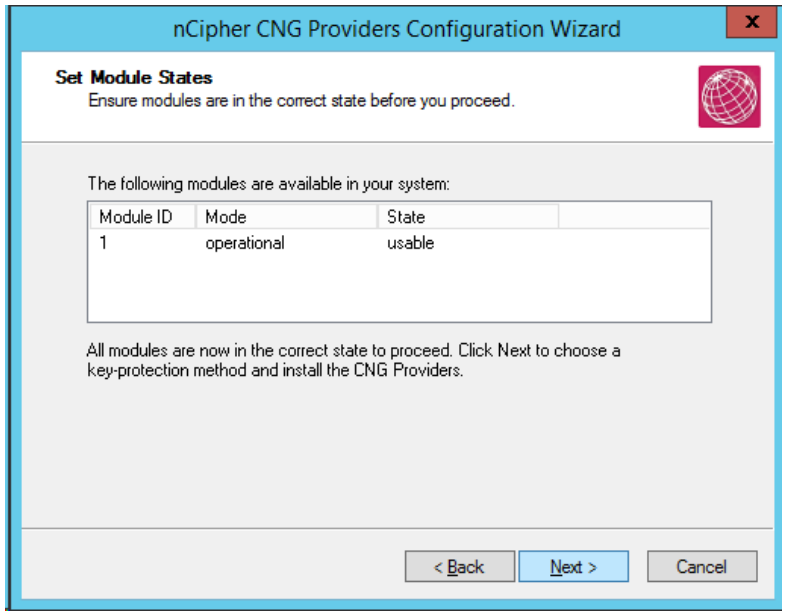


Figure 5: Set Module States

Click "Next".

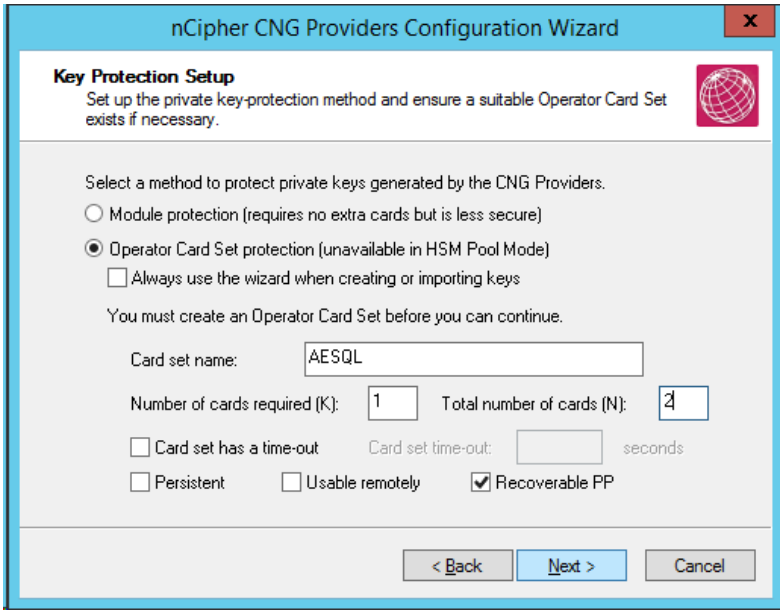


Figure 6: Set Key Protection

Proceed to create an Operator Card Set by selecting "Operator Card Set protection" and enter a name for your Card set, ensure that the "Always use the wizard when creating or importing keys" is **deselected**. Enter the card set name (this field is mandatory) then enter the required K of N value; (consult your security policy document for details on correct values to enter here). Carefully consider which of the optional values to set for the Operator Card set Please refer to the description in the table below for further details. Please note that by default the OCS is created as non-persistent.

Click "Next" to proceed to create the Operator Card Set.

By,:

Term	Definition
Card set name	Card set name must be supplied, unlike naming of individual cards which is optional.
Number of cards required	This relates to *K* of *N* where the value [*K*] = the necessary number of cards required to complete authentication (the quorum) and *[N]* = the total number of cards available. The value for *K* should be less than *N*. We do not recommend creating card sets in which *K* is equal to *N* because an error on one card would render the whole card set unusable.
Card set has a time-out	This allows a specified period of time, in seconds, where keys protected by any given OCS remain loaded in the HSM for use by your application. Once the time period has expired, all keys loaded under the OCS will be forcible removed from the HSM such that they are no longer available. Time-outs operate independently of OCS persistence
Persistent	Keys protected by a persistent card set can be used for as long as the application that loaded the OCS remains connected to the hardware security device (unless that application removes the keys).
Non-persistent	keys protected by a non-persistent card set can only be used while the last required card of the quorum remains loaded in the smart card reader of the Thales hardware security device. The keys protected by this card are removed from the memory of the device as soon as the card is removed from the smart card reader.
Usable remotely	The Remote Operator feature enables the contents of a smart card inserted into the slot of one module (the attended module, such as a client module) to be securely transmitted and loaded onto another module (an unattended module, such as the nShield Connect or netHSM). This is usefulwhen you need to load an OCS-protected key onto a machine to which you do not have physical access (because, for example, it is in a secure area). This feature is deprecated in favour of Remote Administration which was launched with version 12.00 of the Thales nShield Security World software.
Recoverable PP	The option allows the recovery of a lost or forgotten pass phrase. For further details on recovery operations and Security World settings please refer to the HSM documentation supplied on the Security World CD.

If you wish to give a name to each card, do so here, select to enter a pass phrase if required, enter and confirm the pass phrase before clicking on “Next” to create the OCS.

Note: you must have the *N* value of cards available for this operation before you commence. Insert a card into the attached HSM card reader or the TVD (Trusted Verification Device) if you are using the Remote Administration feature, when you are prompted to do so.

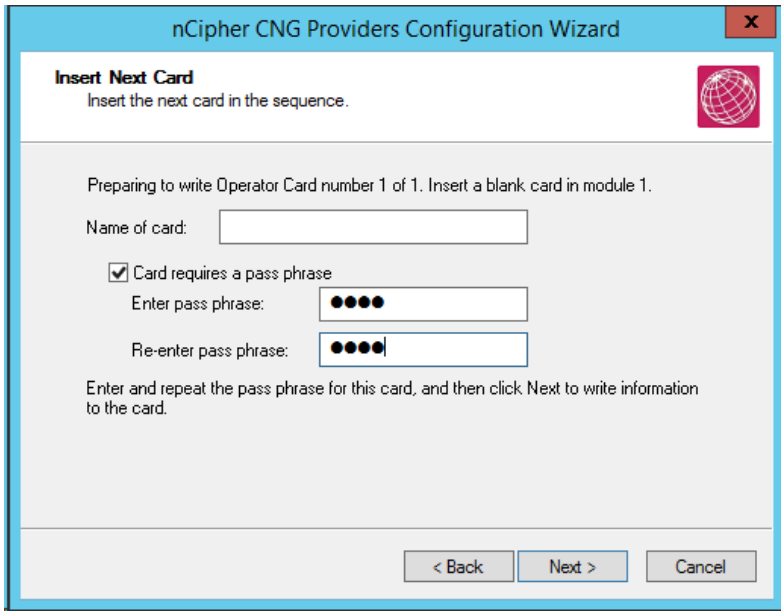


Figure 7: Writing the Operator Card Set

You do not have to give individual cards names, but if you wish, enter the name of the card in the appropriate field. Similarly, you do not have to give the cards a pass phase, but enter one if appropriate for your security policy. Click “Next”.

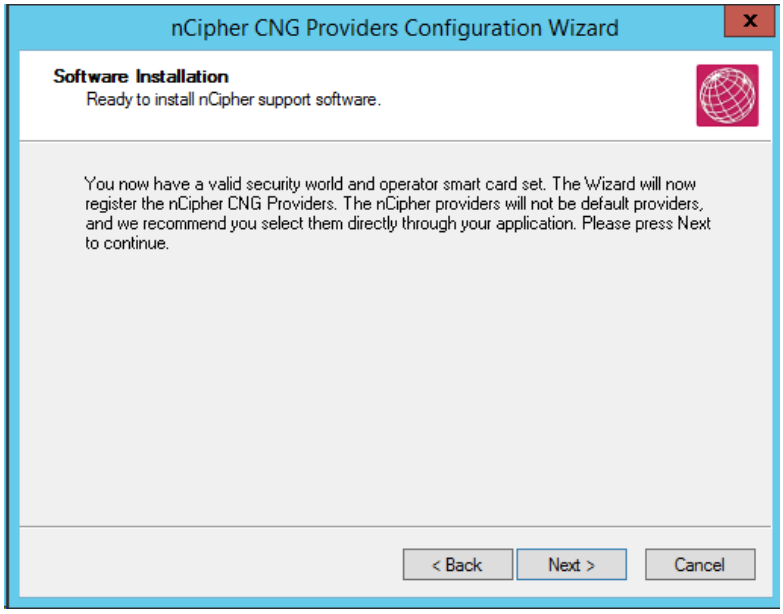


Figure 8: Register CNG Providers

The Thales nCipher CNG providers will now be installed and the key Storage Provider will be registered. To confirm that the KSP has been successfully registered open a Command Line Interface (right click and “Run as Administrator”) and run the following command:

```
C:\Program Files (x86)\nCipher\nfast\bin>cnglist.exe --list-providers
Microsoft Key Protection Provider
Microsoft Platform Crypto Provider
Microsoft Primitive Provider
Microsoft Smart Card Key Storage Provider
Microsoft Software Key Storage Provider
Microsoft SSL Protocol Provider
Windows Client Key Protection Provider
nCipher Primitive Provider
nCipher Security World Key Storage Provider

C:\Program Files (x86)\nCipher\nfast\bin>
```

You should see the nCipher Security World key Storage Provider listed (highlighted in Bold above)

Installing the nCipher Key Storage Provider using the CLI.

If preferred, it is possible to install and register the Thales nCipher CNG provider via the Thales supplied utilities from the command line.

Install and register the CNG provider using `cnginstall.exe` (for 32 bit applications) or `cnginstall64.exe` (for 64 bit applications

```
C:\Program Files (x86)\nCipher\nfast\bin>cnginstall.exe –i
```

Once the provider .dll has been installed you must register the provider using `cngregister.exe`

```
C:\Program Files (x86)\nCipher\nfast\bin>cngregister.exe
```

Creating the Always Encrypted Column Master Key using the nCipher KSP

Once you have successfully installed the nCipher CNG Key Storage Provider you can begin to configure Always Encrypted.

From the “Apps by name” desktop environment, select the Microsoft SQL Server Management Studio and connect to the desired database. Once connected to the database the first thing you will need to do is create a Column Master Key. This key will encrypt all subsequent Column Encryption keys (CEKs).

First create the **CMK**. Using Object Explorer, select the Security directory under the desired Database (In the example below this can be seen as “TestDatabase”). Click to expand “Always Encrypted Keys”.

Select: <Your database> > Security > Always Encrypted Keys > Column Master Keys.

Right click on “Column Master Keys” and select > New Column Master Key…

A dialogue box will open.

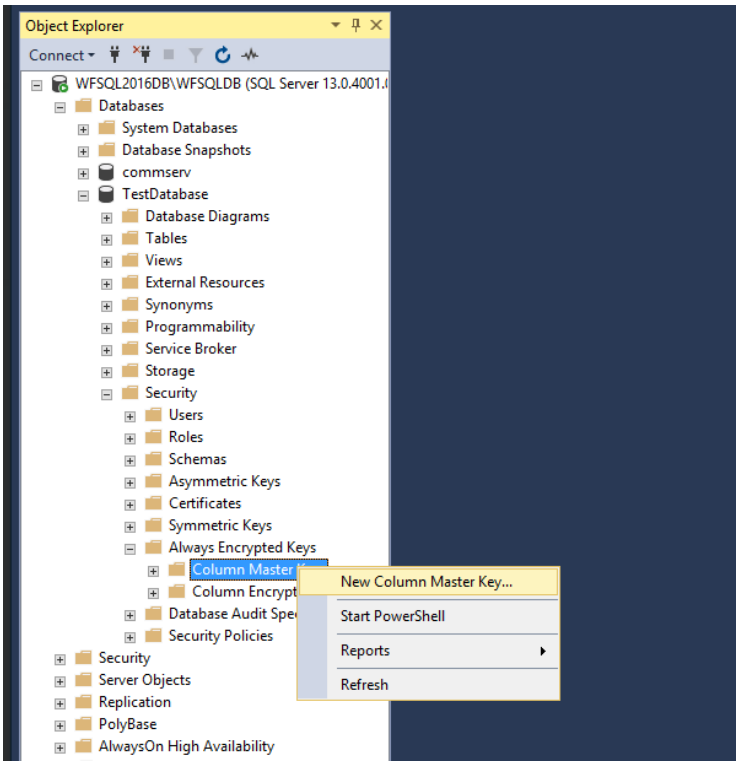


Figure 9: New Column Master Key

In the **Name** field, enter a meaningful name for the CMK, e.g. MyAECMK

From the drop down list select the “Key Storage Provider (CNG)” option. This will then present the option to “**Select a provider”**. Choose the “nCipher Security World Key Storage Provider” from the drop down list and click Generate Key to create a new CMK using the nShield HSM and CNG KSP.

If the “nCipher Security World Key Storage Provider” is not visible you will need to ensure that you have correctly installed and registered the Thales Key Storage Provider.

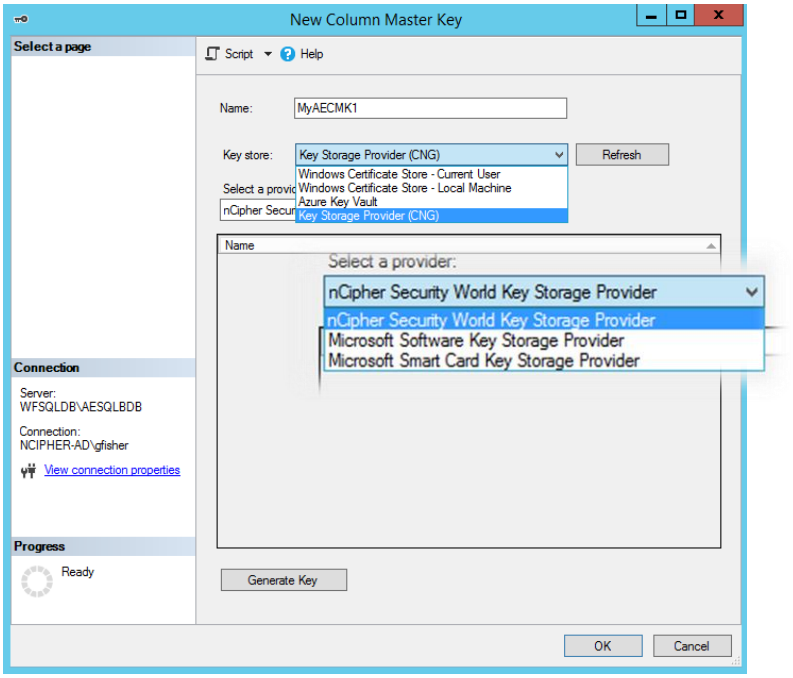


Figure 10: Generate new CMK

The nCipher Key Storage Provider – Create key dialogue will open.

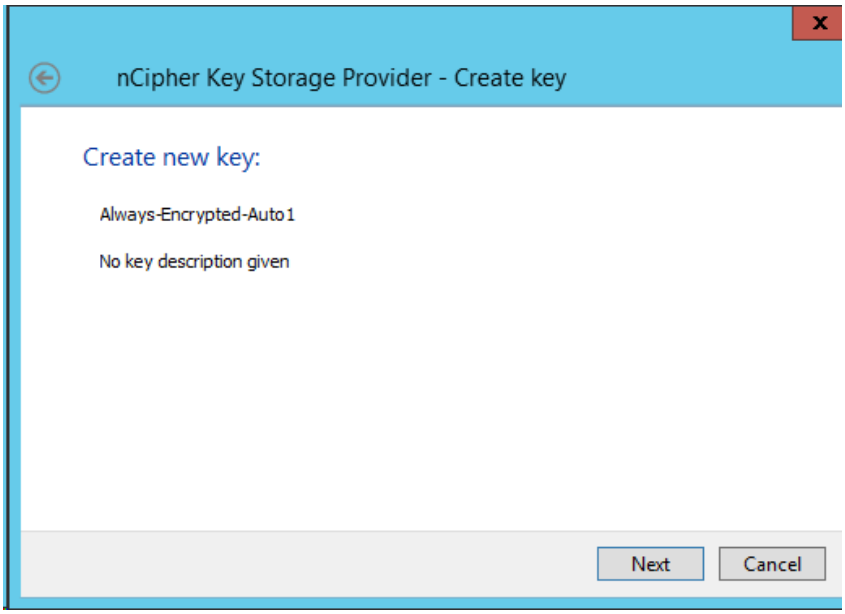


Figure 11: nCipher KSP - Create key

Click “Next” to select key generation options to use either Module or Operator Card Set.

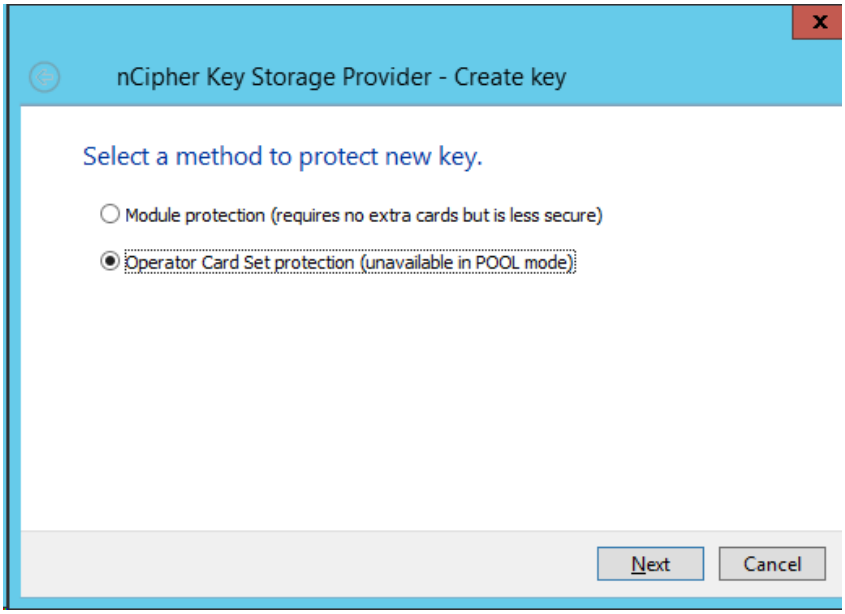


Figure 12: Select module or OCS

The following screen will prompt you to select which Operator Card Set to use for the CMK. Current Card sets will be listed in the left hand field.

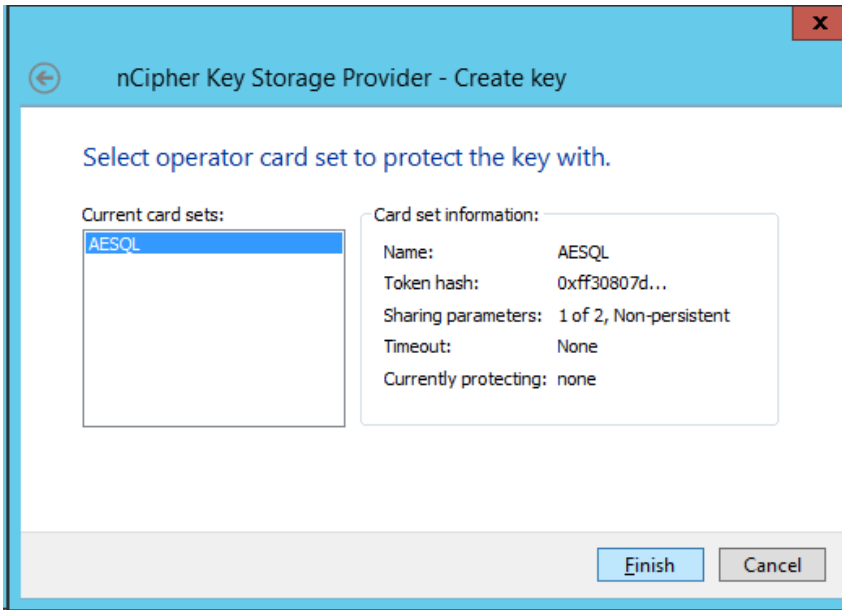


Figure 13: Select card set by name

Select the required OCS that you want to use and click “Finish” the next two screens will prompt you to enter the pass phrase for the selected OCS if one exists and confirm card reading completed successfully.

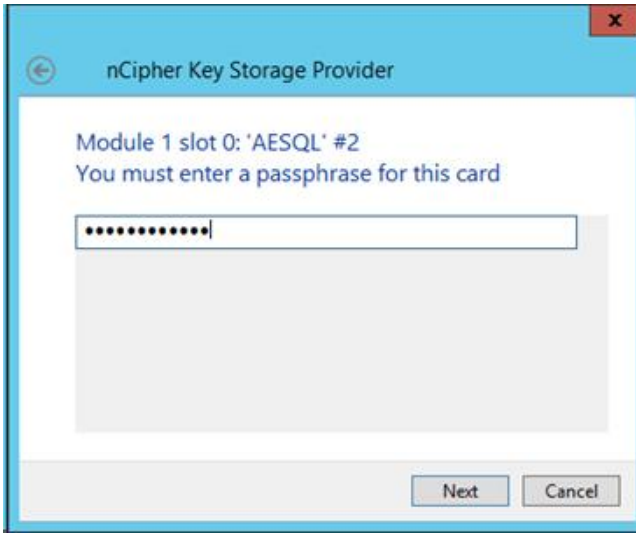


Figure 14: Enter pass phrase

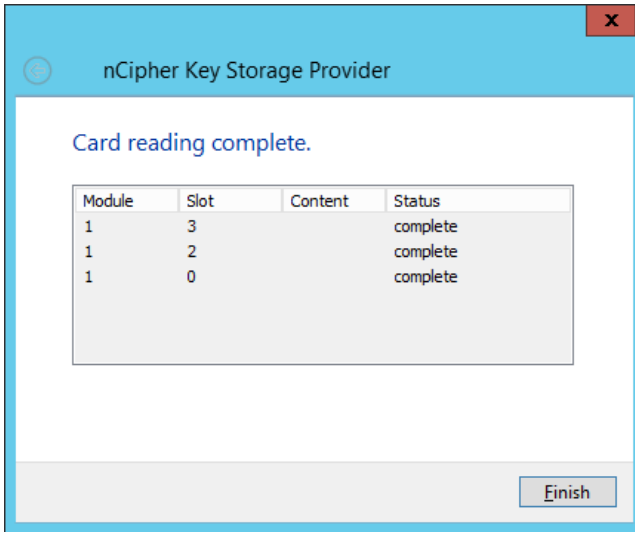


Figure 15: Card reading complete

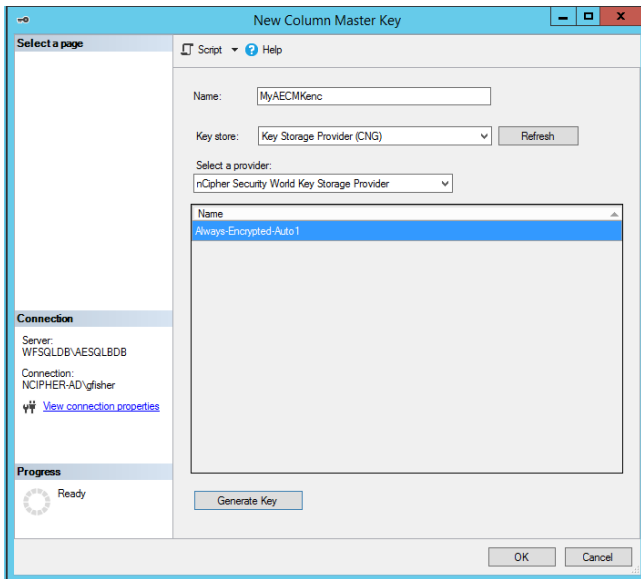


Figure 16: New CMK generated

You will now have a Column Master Key called MyAECMK protected by the card set, AESQL. The newly generated CMK will be visible in the Name field.

To confirm the key has been successfully created using the Thales nShield Key Storage Provider open a **cmd** shell (this should be done with elevated permissions, right click and select "Run as Administrator") navigate to `%nfast_home%\bin` and run the Thales utility `nfkminfo.exe` with the `-k` argument. You should see something similar to the output, given below.

```
C:\Program Files (x86)\nCipher\nfast\bin>nfkminfo.exe -k

Key list - 1 keys
 AppName caping                Ident s-1-5-21-527237240-1202660629-1708537768-767
0--b7a3ff6552ecfa07c463867b3bc131f473d93ca5
```

Click OK, the database now has a Column Master Key protected by the Security World under OCS protection.

To view the new Column Master Key use the SQL Object Explorer. Navigate to the relevant database and expand by clicking the + sign. Expand the "Security" folder and then expand the "Always Encrypted Keys" Folder. You will find two folders, one for the Column Master Key(s) and one for the Column Encryption Key(s)

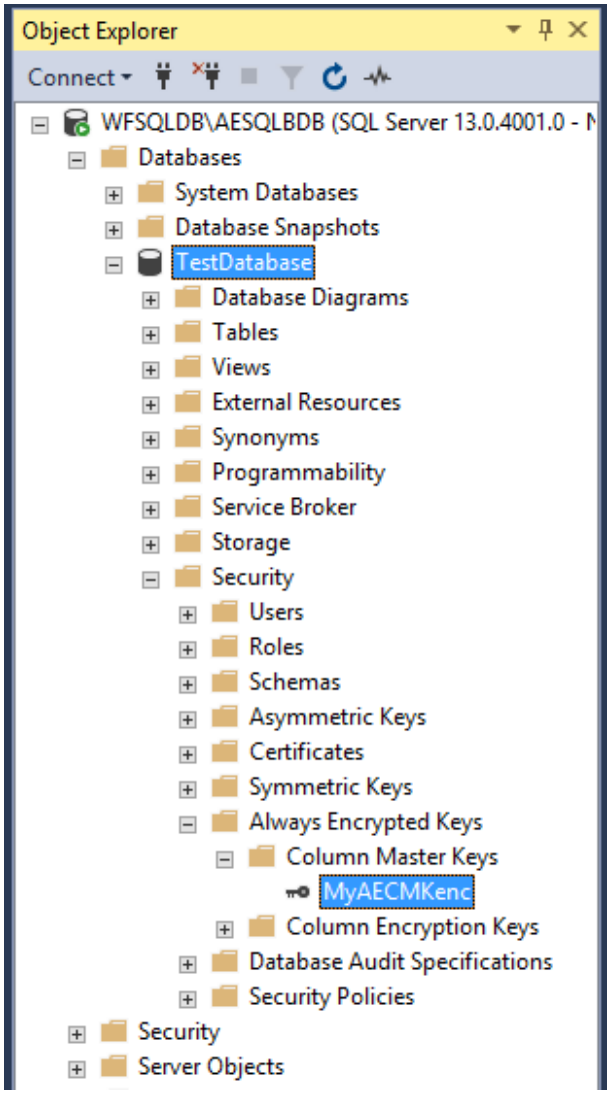


Figure 17: New CMK

Enable Always Encrypted.

To Enable Always Encrypted and generate a Column Encryption Key, right click on the required database, in this example we shall use TestDatabase, right click and in the “Tasks” tab select to “Encrypt Columns…” this will open the Always Encrypted wizard.

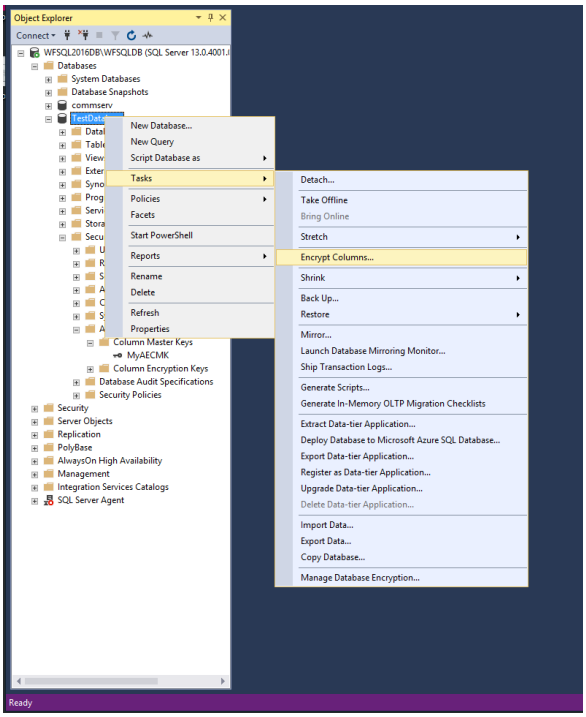


Figure 18: Encrypt Columns

If you don’t want the Introduction screen presented each time you run the wizard, check the “Do not show this page again” box. Click “Next”

The Column Selection screen allows you to choose the type of Column Encryption Key and specify the columns you want to encrypt.

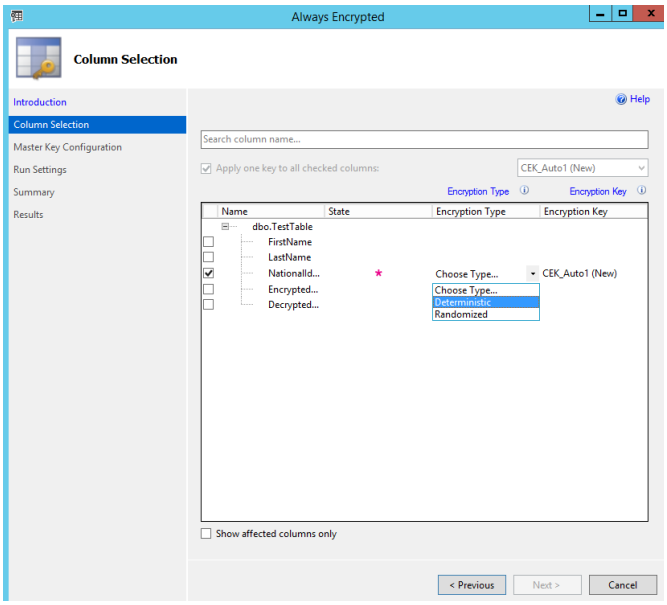


Figure 19: Column Selection and encryption type

Note: The “Apply one key to all checked columns” is shaded out until such time as you have two or more CEKs available. You will then also have the option to select the CEK for any given column via the drop down list.

Under “Encryption Type” click to select the column(s) to encrypt by checking the appropriate box to the left of the column name, you can then select the encryption method from the drop down box beneath “Choose Type” Encryption is either:

- Deterministic
- Randomised

Click “Next”.

On the Master key Configuration page, Make sure that you select the CMK that was generated using tha nCipher Key Storage Provider and protected by the HSM and click next.

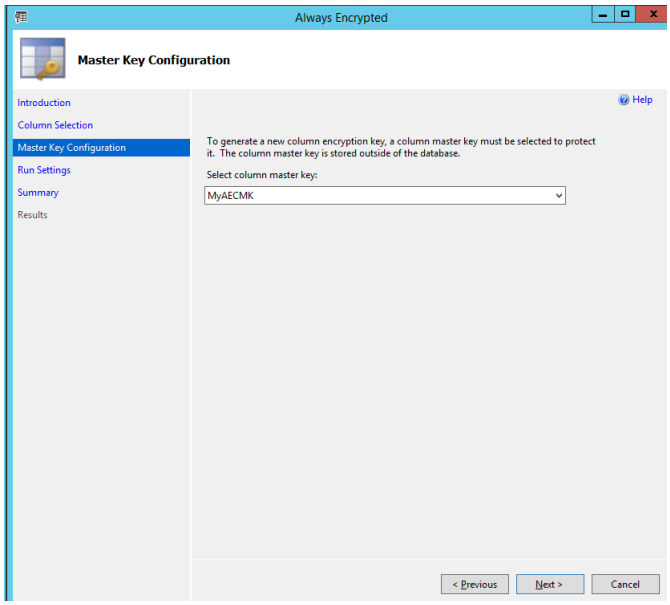


Figure 20: Select CMK to use

N.B. ***Run Settings***: It is recommended that maintenance downtime be scheduled for this activity.

The process of encrypting your database records can take a considerable amount of time, depending on the size / quantity of data. To mitigate the possibility of data corruption occurring as records are encrypted whilst being updated, it is advisable to only perform this activity when the database is off-line.

In this case we will continue and run the encryption straight away. Select the radio button ”Proceed to finish now” this will begin the process of creating the CEK and using it to encrypt the specified column in the database. Click “Next” to view the Summery page.

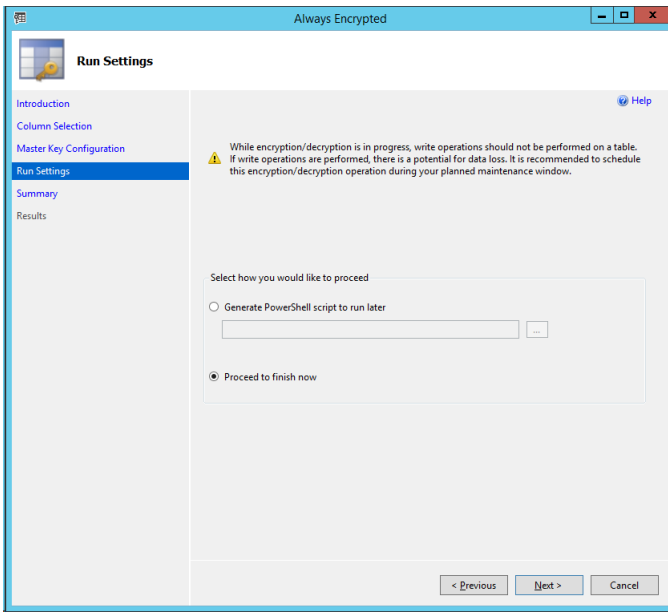


Figure 21: Run Settings

This page allows you to verify your configuration choices and amend if necessary.

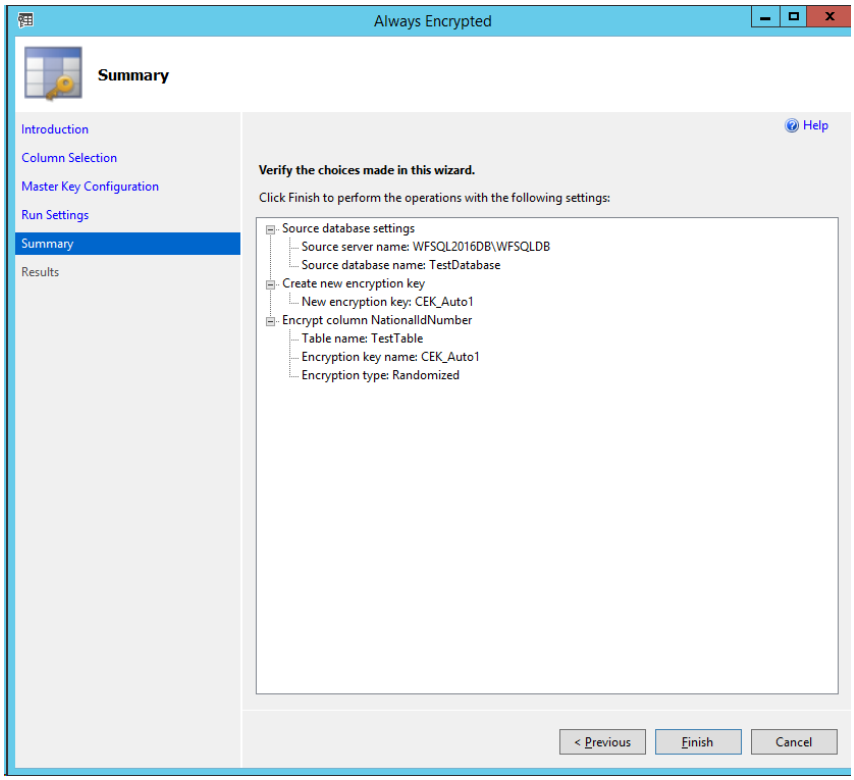


Figure 22: Verify Settings

The next operation requires the Operator Card Set quorum to be available.

Before you can create a CEK you must first load the CMK. The following screen will prompt you to present the OCS protecting the Column Master Key. Present the OCS quorum and enter the passphrase, continue by clicking "Finish".

Figure 23: Load CMK

You will be prompted for the Operator Card passphrase, enter the passphrase and click “Next”.

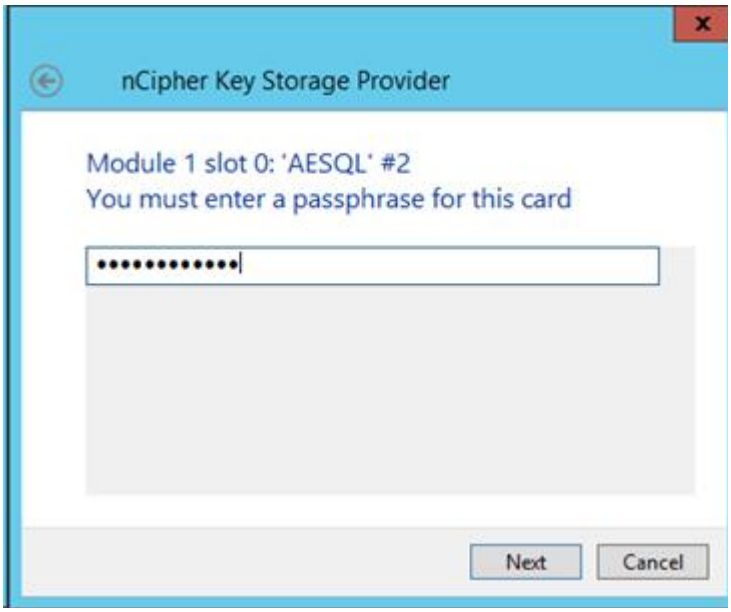


Figure 24: Enter passphrase for OCS protecting the CMK

Click “Finish” to complete the loading of the CMK into the memory of the HSM this will allow it to securely encrypt the Column Encryption Key.

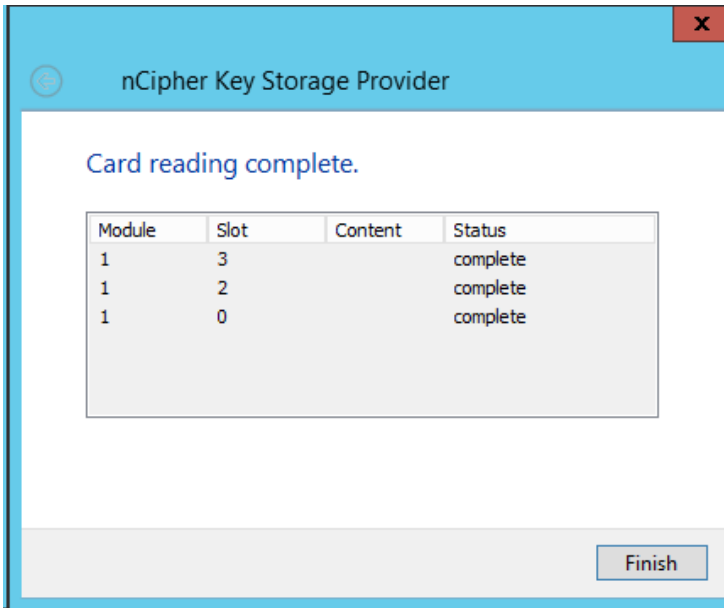


Figure 25: Confirmation of card reading

Next, the CEK shall be generated and protected by an OCS protected Column Master Key.

Click “Finish” to proceed.

Figure 26: key Load

Insert the quorum from the Operator Card set and enter the passphrase(s) when prompted.

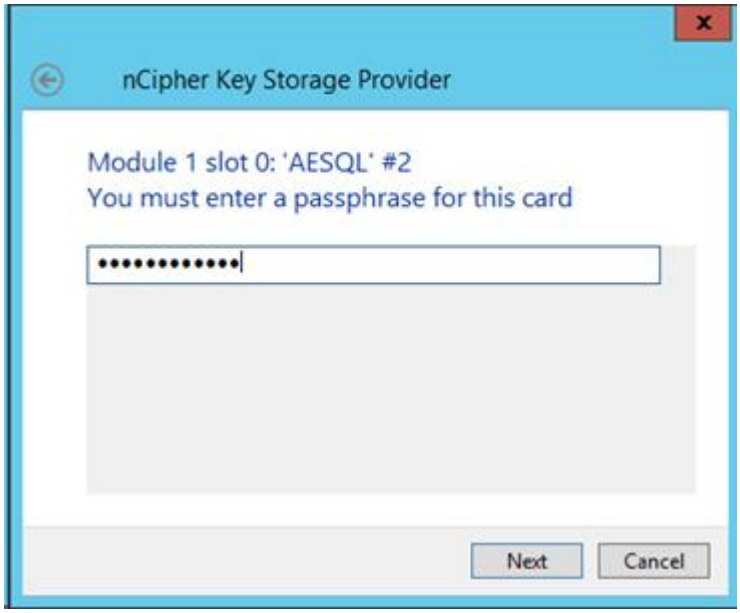


Figure 27: Enter passphrase

The following screen reports on the status of the Operator Card reading operation.

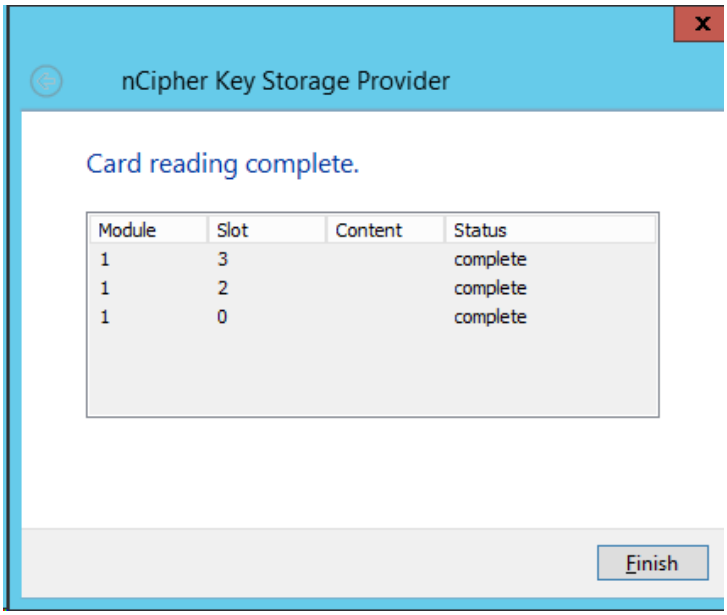


Figure 28: Card reading complete

Providing the Operator Card(s) where correctly read the CEK will have been created.

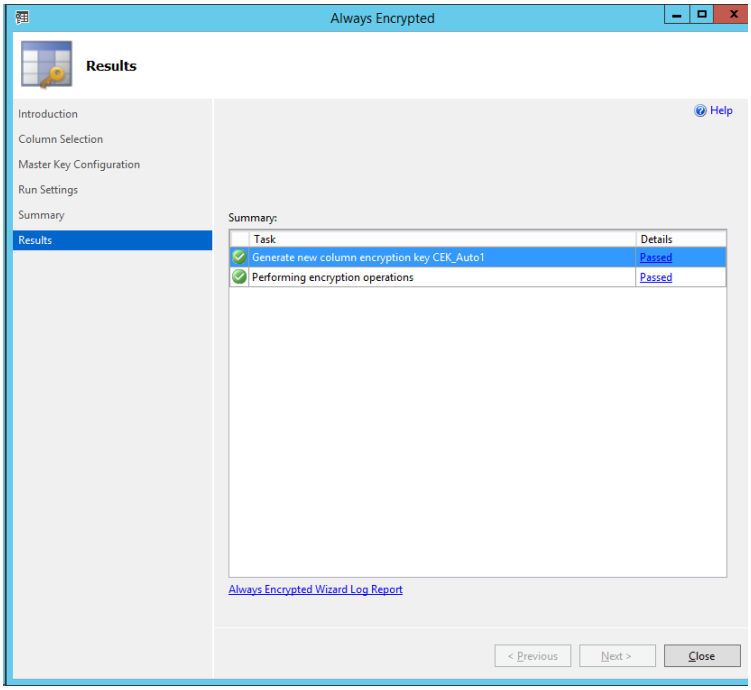


Figure 29: CEK successfully encrypted Column

The Results page will report that the “CEK was generated and the requested / specified columns are now encrypted. You can now click “Close” to exit the Always Encrypted Column Encryption Key wizard.

If you now open the table by right clicking on the dbo.Table and selecting “Select Top 1000 Rows” you will see that the column that was chosen for encryption now appears as ciphertext.

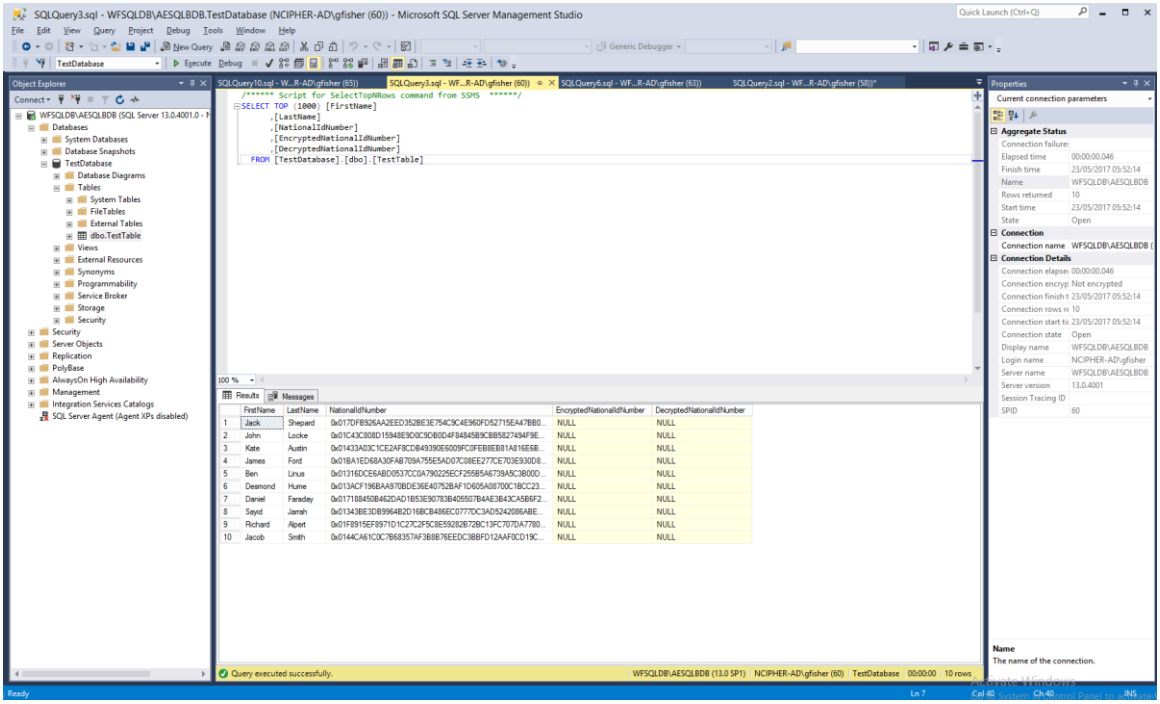
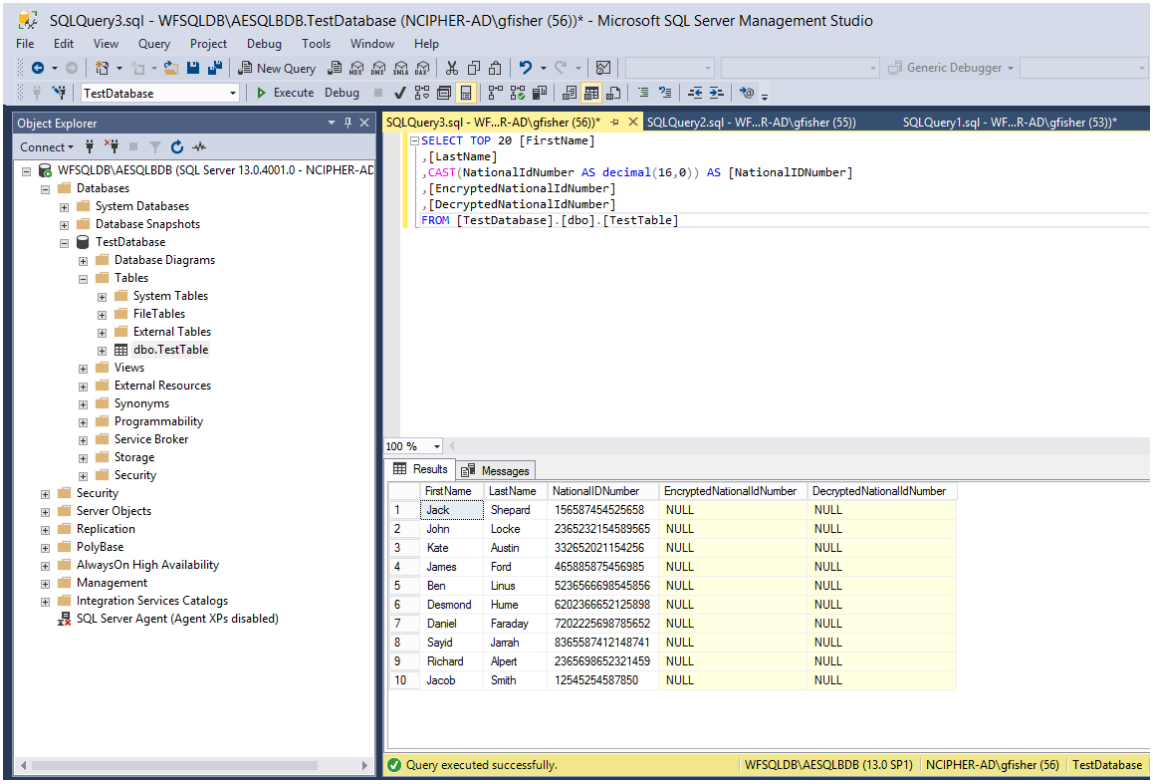


Figure 30: Showing encrypted columns

To show the encrypted columns in plaintext (i.e. Decrypted) you should disconnect from the database and reconnect with the given additional connection parameter. This is entered from the “Connect to Database Engine” logon screen. Select the required server name and click on “Options>>” Go to “additional Connection Parameters” and add the connection string (without parenthesis) “Column Encryption Setting = enabled” and then Connect.

When you now run the query on the table you will now see the original values decrypted by the Column Encryption Key.



	FirstName	LastName	NationalIDNumber	EncryptedNationalIdNumber	DecryptedNationalIdNumber
1	Jack	Shepard	156587454525658	NULL	NULL
2	John	Locke	2365232154589565	NULL	NULL
3	Kate	Austin	332652021154256	NULL	NULL
4	James	Ford	465885875456985	NULL	NULL
5	Ben	Linus	5236566698545856	NULL	NULL
6	Desmond	Hume	6202366652125898	NULL	NULL
7	Daniel	Faraday	7202225698785652	NULL	NULL
8	Sayid	Jarrah	8365587412148741	NULL	NULL
9	Richard	Alpert	2365698652321459	NULL	NULL
10	Jacob	Smith	12545254587850	NULL	NULL

Figure 31: Example of encrypted Column using Always Encrypted CEK

Removing column encryption

If you want to remove the protection provided by Always Encrypted column encryption this can be done using the SQL Server Management Studio Object Explorer.

To remove Column Encryption from a specific or multiple data column(s):

Right click on the required database and in the “Tasks” menu select “Encrypt Columns”

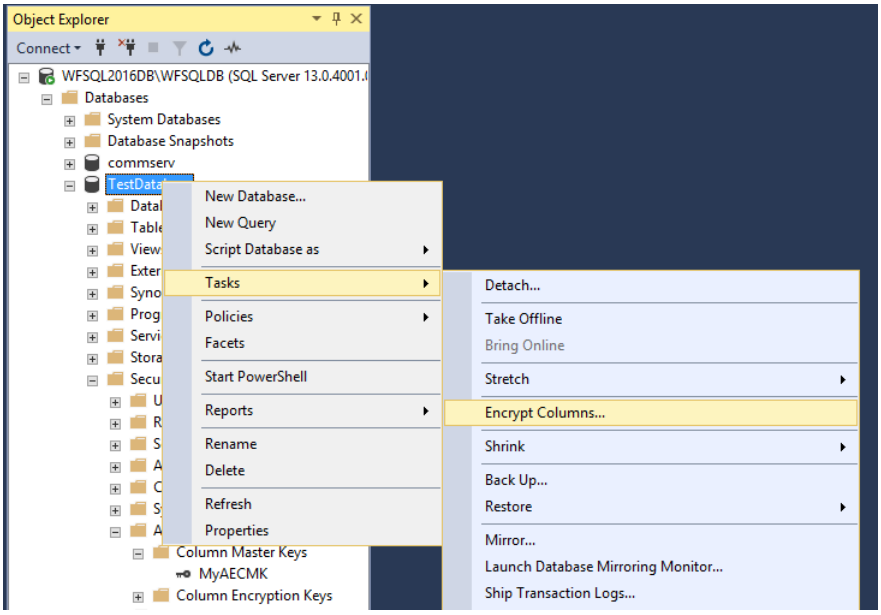


Figure 32: Select Encrypt Columns...

Select “Next” to get to the Column Selection page, and click on the field “Encryption Type”

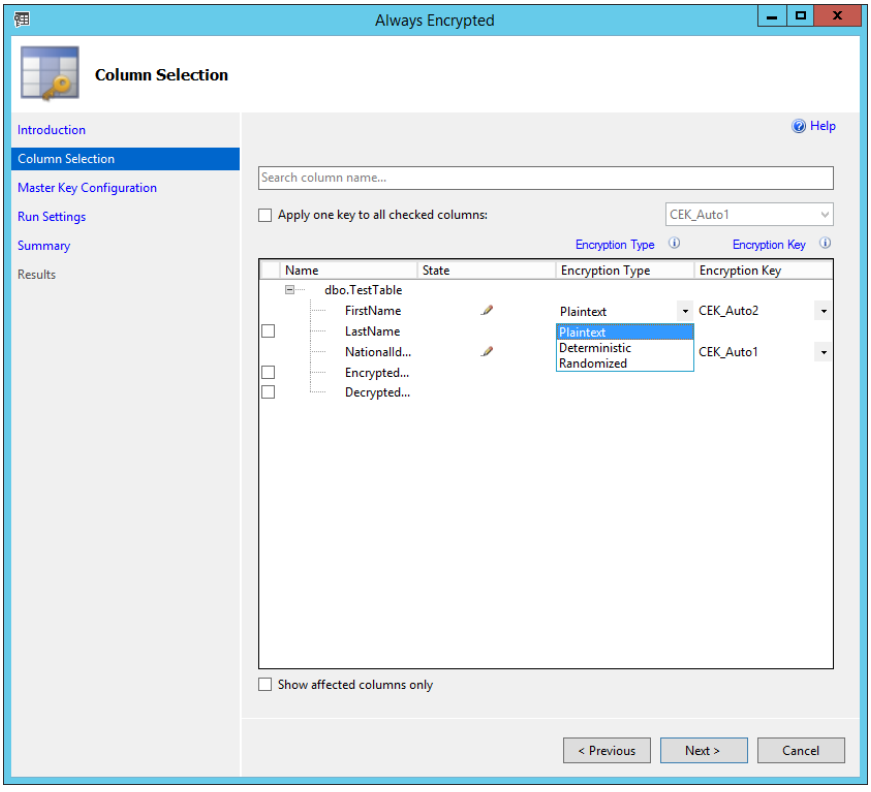


Figure 33: Choose the option - Plaintext

From the drop down list select “Plaintext” Click “Next”.

As there is no key to configure this time click “Next” to proceed straight to the ***Run Settings*** page. If the database is live at this point, you should first take it off-line before proceeding to remove the column encryption. Either generate the required PowerShell script to run later, or as we will do here, select “Proceed to finish now”

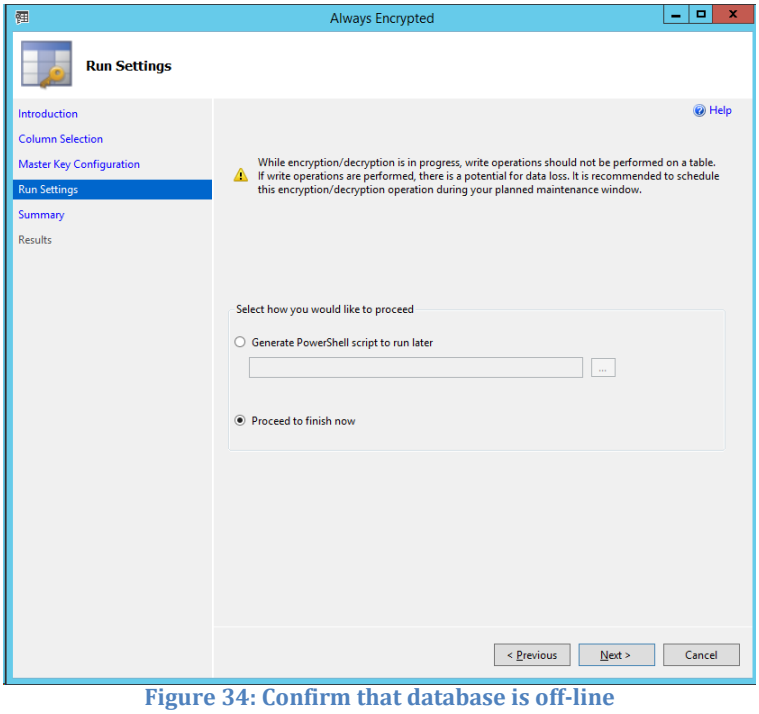


Figure 34: Confirm that database is off-line

The next page will provide a review summery for the requested operations

.

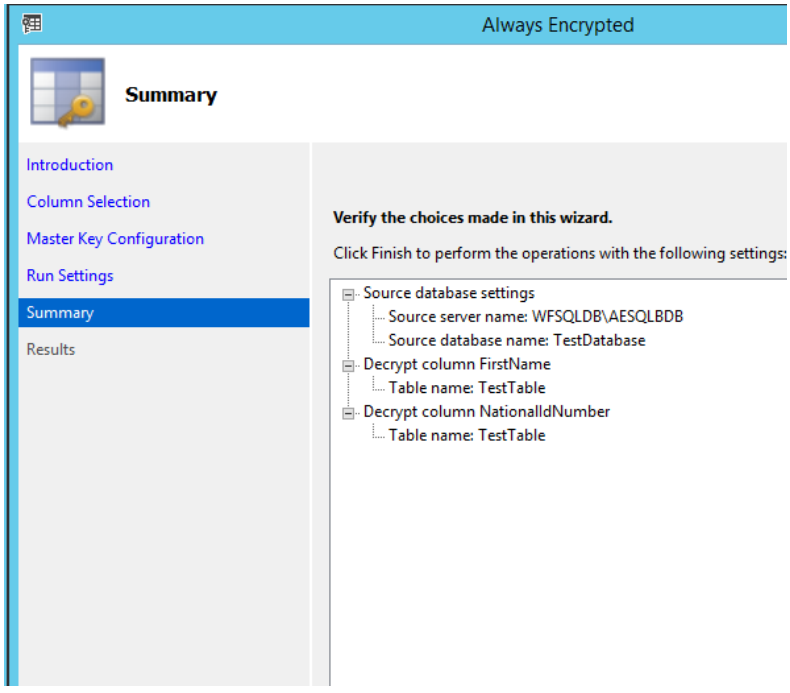


Figure 35: Review column decryption state

Check to ensure that the correct Decrypt column(s) are listed and click “Finish” The “Performing encryption operations” should show as Passed.

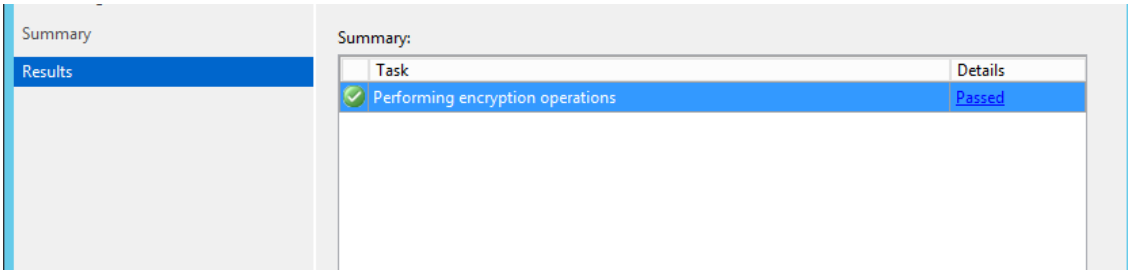


Figure 36: Successfully removed Always Encrypted column encryption

You have successfully removed Always Encrypted column encryption from you database. When you next log into the database you can remove the "Column Encryption Setting = enabled" string form the "Additional Connection Parameters" field of the database login screen. When you now view your database table via, "Select Top 1000 Rows" you should see all columns in plaintext (i.e. an unencrypted state).

THALES

www.thalesesecurity.com

About Thales e-Security

Thales e-Security is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales e-Security is part of Thales Group.

Follow us on:

Americas – 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101-03, 41/F., Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com