



ENTRUST

Microsoft SQL Server TDE and nShield® HSM

Integration Guide

2026-04-27

Member of
Microsoft Intelligent
Security Association

Table of Contents

1. Introduction	1
1.1. Product configurations	1
1.2. Supported nShield hardware and software versions	1
1.3. Supported nShield SQLEKM provider:	1
1.4. Supported nShield functionality	2
1.5. Requirements	2
1.6. Terms	2
2. Test database	4
3. Install and configure the Entrust nShield HSM	5
3.1. Install the Entrust nShield HSM	5
3.2. Install the Security World software and create a Security World	5
3.3. Install the nShield nDSOP	6
3.4. Install the hotfix for TAC-1266	6
3.5. Select the protection method	7
3.6. Create the Operator Card Set (OCS) or Softcard	7
4. Configure SQL EKM	10
4.1. Enable EKM and register the SQLEKM provider	10
4.2. Verify the SQLEKM provider configuration	11
4.3. Create the user SQL Server credential	13
5. Configure TDE	16
5.1. Create a TDEKEK	16
5.2. Create a TDE login and credential	17
5.3. Create the TDEDEK and switch on encryption	20
5.4. Key rotation - Replace the TDEKEK	22
5.5. Key rotation - Replace the TDEDEK	25
6. Column level encryption	27
6.1. Create a new key	27
6.2. Import an existing key	28
6.3. Encrypt a column with a symmetric key	30
6.4. Encrypt a column with an asymmetric key	32
6.5. Encrypt a column with the imported asymmetric key	33
7. Perform backup and recovery	35
7.1. Back up the Security World	35
7.2. Restore the Security World	35
7.3. Back up the database	35
7.4. Restore the database	37
8. Upgrade nDSOP from v1.0 to v2.1.0	40

8.1. Versions	40
8.2. Procedure	40
9. Upgrade nDSOP from v2.1.0 to v2.1.1	46
9.1. Versions	46
9.2. Procedure	46
10. Troubleshoot	51
10.1. Microsoft SQL Server, Error: 15209 while rotating the TDEKEK	51
11. Additional resources and related products	52
11.1. nShield HSMs	52
11.2. nShield as a Service	52
11.3. nShield Database Option Pack	52
11.4. Entrust products	52
11.5. nShield product documentation	52

Chapter 1. Introduction

This document describes how to integrate Microsoft SQL Server TDE with the nShield Database Security Option Pack (nDSOP) using an Entrust nShield hardware security module (HSM) as a Root of Trust. Entrust nShield HSMs (referred to as HSM in this guide) provide FIPS certified solutions to generate and secure the keys used to encrypt and decrypt the database.

1.1. Product configurations

Entrust tested the integration with the following versions:

Product	Version
Base OS	Windows Server Datacenter 2025
SQL Server	Microsoft SQL Server Enterprise 2025
Microsoft SQL Server Management Studio (SSMS)	v22.5.0

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

HSM	Security World Software	Firmware	Netimage
Connect XC	13.6.15	12.72.4 (FIPS 140-2 certified)	13.6.15
nShield 5c	13.6.15	13.4.5 (FIPS 140-3 certified)	13.6.15

Security World Software v13.6.8 is the first release supporting Window Server 2025.

1.3. Supported nShield SQLEKM provider:

Product	Version
nDSOP	v2.1.1
Hotfix	TAC-1266

1.4. Supported nShield functionality

Functionality	Support
FIPS 140 Level 3	Yes
Key Management	Yes
Key Generation	Yes
Key Recovery	Yes
1 of N Card Set	Yes
Softcards	Yes
Module Only Key	No
Fail Over	Yes
Load Balancing	Yes
nSaaS	Yes

1.5. Requirements

You must have access to the [Entrust TrustedCare Portal](#). This portal is available to customers with an active maintenance agreement. To request an account, contact nshield.support@entrust.com.

Familiarize yourself with the following documentation:

- The Microsoft SQL Server features and documentation.
- The Microsoft SQL Server Management Studio features and documentation.
- The T-SQL language. The minimum requirement for T-SQL is a basic understanding of SQL tasks such as creating a database or tables.
- Database security concepts and practices.
- The [nShield Documentation](#).

1.6. Terms

Acronym	Definition
SQLEKM	SQL Server Extensible Key Management
TDEKEK	TDE Key Encryption Key
TDEDEK	TDE Database Encryption Key

Chapter 2. Test database

Microsoft SQL Server was deployed as a stand-alone instance on a single machine. A database named TestDatabase was created for the purpose of this integration. The following SQL query creates TestDatabase and displays a view of TestTable.

```
USE master
GO

-- Create database named "TestDatabase".
CREATE DATABASE TestDatabase;
GO

-- Create table named "TestTable" and populate it with some values.
USE TestDatabase
GO
CREATE TABLE TestTable (FirstName varchar(50), LastName varchar(50), Email varchar(320), Password nvarchar(50));
GO
INSERT INTO TestTable (FirstName, LastName, Email, Password) VALUES ('Firstname1', 'Lastname1',
'Firstname1.Lastname1@testserver.com', 'Password1');
INSERT INTO TestTable (FirstName, LastName, Email, Password) VALUES ('Firstname2', 'Lastname2',
'Firstname2.Lastname2@testserver.com', 'Password2');
INSERT INTO TestTable (FirstName, LastName, Email, Password) VALUES ('Firstname3', 'Lastname3',
'Firstname3.Lastname3@testserver.com', 'Password3');
INSERT INTO TestTable (FirstName, LastName, Email, Password) VALUES ('Firstname4', 'Lastname4',
'Firstname4.Lastname4@testserver.com', 'Password4');
INSERT INTO TestTable (FirstName, LastName, Email, Password) VALUES ('Firstname5', 'Lastname5',
'Firstname5.Lastname5@testserver.com', 'Password5');
GO

--Grants permissions to <DOMAIN>/Administrator.
USE TestDatabase;
GRANT ALTER ANY COLUMN ENCRYPTION KEY TO "INTEROP\Administrator";
GRANT ALTER ANY COLUMN MASTER KEY TO "INTEROP\Administrator";
GRANT VIEW ANY COLUMN ENCRYPTION KEY DEFINITION TO "INTEROP\Administrator";
GRANT VIEW ANY COLUMN MASTER KEY DEFINITION TO "INTEROP\Administrator";
GO
```

The screenshot shows the Microsoft SQL Server Enterprise Manager interface. The Object Explorer on the left shows the TestDatabase folder expanded, with the TestTable table visible. The SQL Query window on the right contains the following query:

```
SELECT TOP (1000) [FirstName]
,[LastName]
,[Email]
,[Password]
FROM [TestDatabase].[dbo].[TestTable]
```

The Results pane shows the following data:

FirstName	LastName	Email	Password
Firstname1	Lastname1	Firstname1.Lastname1@testserver.com	Password1
Firstname2	Lastname2	Firstname2.Lastname2@testserver.com	Password2
Firstname3	Lastname3	Firstname3.Lastname3@testserver.com	Password3
Firstname4	Lastname4	Firstname4.Lastname4@testserver.com	Password4
Firstname5	Lastname5	Firstname5.Lastname5@testserver.com	Password5

The status bar at the bottom indicates: "Qu... MSSQLNSHIELD25\MSSQLNSHIELD... | INTEROP\Administrator ... TestDatabase 00:00:00 Row: 1, Col: 1 | 5 rows".

Chapter 3. Install and configure the Entrust nShield HSM

Prerequisites:

- A Windows Server with Microsoft SQL server.
- SQL Server Management Studio installed.
- The database `TestDatabase` has been created and is available for the integration.

3.1. Install the Entrust nShield HSM

Install the nShield Connect HSM locally, remotely, or remotely via the serial console. Condensed instructions are available in the following Entrust nShield Support articles.

- [How To: Locally Set up a new or replacement nShield Connect.](#)
- [How To: Remotely Setup a new or replacement nShield Connect.](#)
- [How To: Remotely Setup a new or replacement nShield Connect XC Serial Console Model.](#)

For detailed instructions see the [nShield v13.6.15 Hardware Install and Setup](#). Guides.

3.2. Install the Security World software and create a Security World

1. Install the Security World software. For detailed instructions see the [nShield Security World Software v13.6.15 Installation Guide](#).
2. Add the Security World utilities path to the system path. This path is typically `C:\Program Files\nCipher\ncfast\bin`.
3. Open the firewall port 9004 for the HSM connections.
4. If using remote administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).
5. Open a command window and run the following to confirm that the HSM is **operational**:

```
>enquiry
Server:
  enquiry reply flags  none
  enquiry reply level Six
  serial number       810B-03E0-D947 92C8-8591-52EB
  mode                 operational
  version              13.6.15
```

```

...
Module #1:
enquiry reply flags UnprivOnly
enquiry reply level Six
serial number      810B-03E0-D947
mode               operational
version           12.72.4
...
Module #2:
enquiry reply flags UnprivOnly
enquiry reply level Six
serial number      92C8-8591-52EB
mode               operational
version           13.4.5
...

```

6. Create your Security World if one does not already exist or copy an existing one. Follow your organization's security policy for this. For more information see [Create a new Security World](#).



ACS cards cannot be duplicated after the Security World is created. You may want to create extras in case of a card failure or a lost card.

7. Confirm that the Security World is "Usable*":

```

> nfkminfo
World
generation 2
state      0x3737000c Initialised Usable ...
...
Module #1
generation 2
state      0x2 Usable
...
Module #2
generation 2
state      0x2 Usable
...

```

3.3. Install the nShield nDSOP

To install the nShield nDSOP:

1. Mount the `nDSOP_Windows-x.x.x.iso` file.
2. Launch the `setup` file and follow the instructions.

3.4. Install the hotfix for TAC-1266

1. Request the hotfix for TAC-1266 from the Entrust support portal.

2. Install the hotfix according to the included instructions.

```
>ncversions
Comp      Output      Version      Build Details
-----
caping    user        13.6.12+     TAC1266-564420ed
csps     user        13.6.15+     387-54fe04d9
...
```

3. Reboot the server.

3.5. Select the protection method

The OCS or Softcard and associated passphrase will be used to authorize access to specific keys protected by the SQLEKM provider.

- Operator Cards Set (OCS) are smartcards that are presented to the physical smartcard reader of an HSM. For more information on OCS use, properties, and K-of-N values, see [Operator Card Sets \(OCS\)](#).
- Softcards are logical tokens (passphrases) that protect they key and authorize its use. For more information on Softcards use see [Softcards](#).

Follow your organization’s security policy to select an authorization access method.

3.6. Create the Operator Card Set (OCS) or Softcard

Typically, an organization’s security policies dictate the use of one or the other.

3.6.1. Create the OCS

A SQL Server credential (as used for EKM) maps one protecting token to one stored passphrase. It can store information for only one token at a time. Therefore an OCS card set does need to have a quorum K of one.

Recovering from a power failure requires the OCS to be inserted in the HSM or the TVD.

1. Edit file `C:\ProgramData\nCipher\Key Management Data\config\cardlist` to add the serial number of the card(s) to be presented or the wildcard value.
2. Open a command window as administrator.
3. Run the `createocs` utility as described below. Enter a passphrase or password at the prompt. Use the same passphrase for all the OCS cards in the set (one for each person with access privilege, plus the spares). In this example note that slot 2, remote via a

TVD, is used to present the card.



After an OCS card set has been created, the cards cannot be duplicated. You may want to create extras in case of a card failure or a lost card.



Add the **-p** (persistent) option to the command below to be able to encrypt/decrypt the database after the OCS card has been removed for safe storage from either the HSM front panel slot or from the TVD. See the [Preload Utility](#) for more information.

```
> createocs -m1 -s2 -N testOCS -Q 1/1

FIPS 140-2 level 3 auth obtained.

Creating Cardset:
Module 1: 0 cards of 1 written
Module 1 slot 0: Admin Card #1
Module 1 slot 2: blank card
Module 1 slot 3: empty
Module 1 slot 2:- passphrase specified - writing card
Card writing complete.

cardset created; hkltu = edb3d45a28e5a6b22b033684ce589d9e198272c2
```

The authentication provided by the OCS as shown in the command line above is non-persistent and only available while the OCS card is inserted in the HSM front panel slot or the TVD. If the TVD loses connection to the Remote Administration client the database will be inaccessible.

4. Verify the OCS created:

```
> nfkminfo -c
Cardset list - 1 cardsets: (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
Operator logical token hash          k/n timeout name
edb3d45a28e5a6b22b033684ce589d9e198272c2 1/1 none-NL testOCS
```

3.6.2. Create the Softcard

A SQL Server credential (as used for EKM) maps one protecting token to one stored passphrase. Softcards are singular and do not have a quorum, so the SQL Server credential matches them quite well.

Unlike OCS protection, which requires a smart card and a passcode, a softcard does not require additional input for recovery after a power failure.

1. Ensure the **C:\Program Files\nCipher\ncfast\cknfastrc** file exists with the following

content. Otherwise, create it.

```
> type "C:\Program Files\Cipher\fast\cknfastrc"
CKNFAST_LOADSHARING=1
```

2. Execute the following command. Enter a passphrase at the prompt.

```
> ppmk -n testSC

Enter new pass phrase:
Enter new pass phrase again:
New softcard created: HKLTU 925f67e72ea3c354cae4e6797bde3753d24e7744
```

3. Verify the Softcard created:

```
> nfkminfo -s
SoftCard summary - 1 softcards:
Operator logical token hash          name
925f67e72ea3c354cae4e6797bde3753d24e7744 testSC
```

The **rocs** utility shows the OCS and Softcard created:

```
> rocs
`rocs` key recovery tool
Useful commands: `help`, `help intro`, `quit`.
rocs> list cardset
No. Name                Keys (recov) Sharing
  1 testOCS              0 (0)           1 of 5
  2 testSC                0 (0)           (softcard)
rocs> quit
```

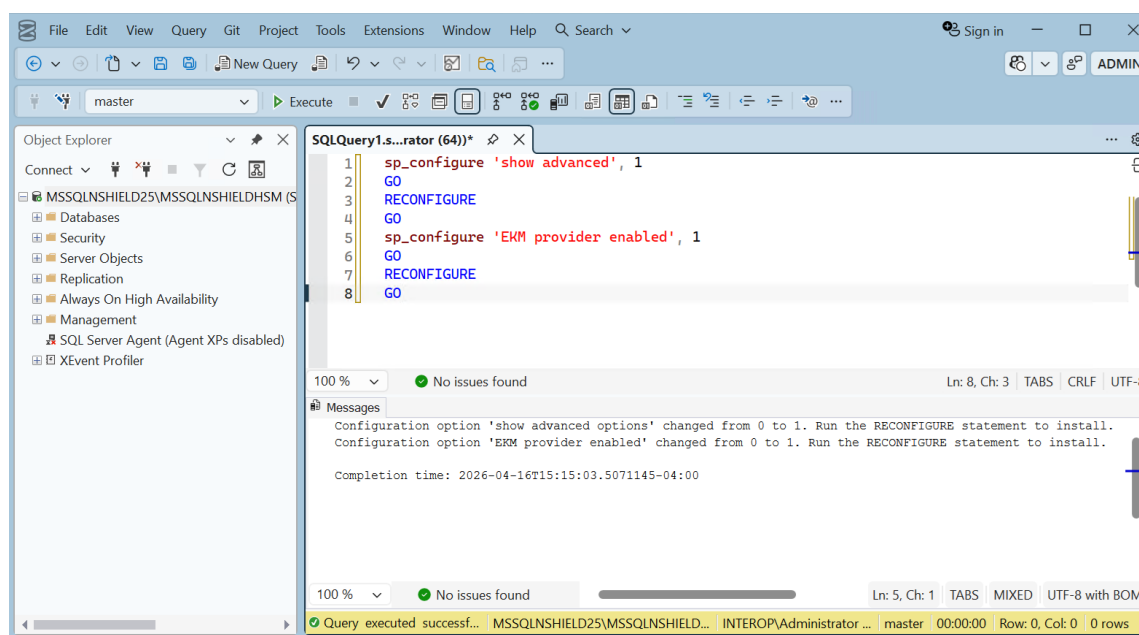
Chapter 4. Configure SQL EKM

4.1. Enable EKM and register the SQLEKM provider

To enable EKM and register the SQLEKM provider:

1. Launch the SQL Server Management Studio GUI.
2. Enable EKM by executing the following query:

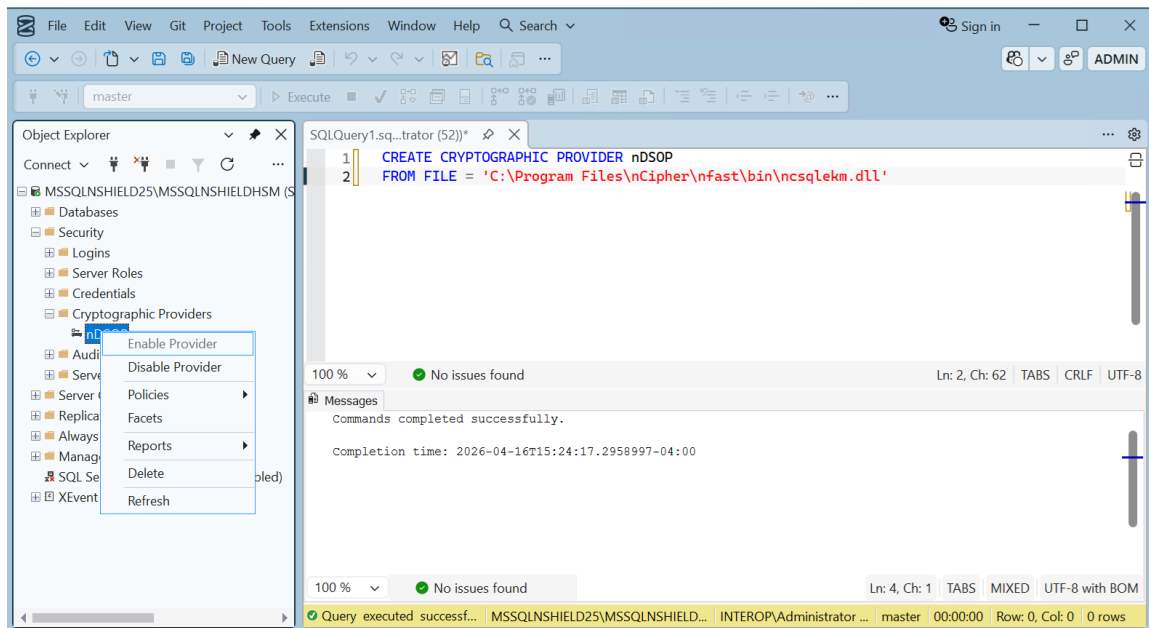
```
sp_configure 'show advanced', 1
GO
RECONFIGURE
GO
sp_configure 'EKM provider enabled', 1
GO
RECONFIGURE
GO
```



3. Register the SQLEKM provider with the SQL Server by executing the following query:

```
CREATE CRYPTOGRAPHIC PROVIDER nDSOP
FROM FILE = 'C:\Program Files\nCipher\fast\bin\ncsqlm.dll'
```

4. Check the SQLEKM provider is listed in the SQL Server Management Studio GUI. Go to **Security > Cryptographic Providers**. nDSOP should be visible. Right-click it to verify that it is enabled.

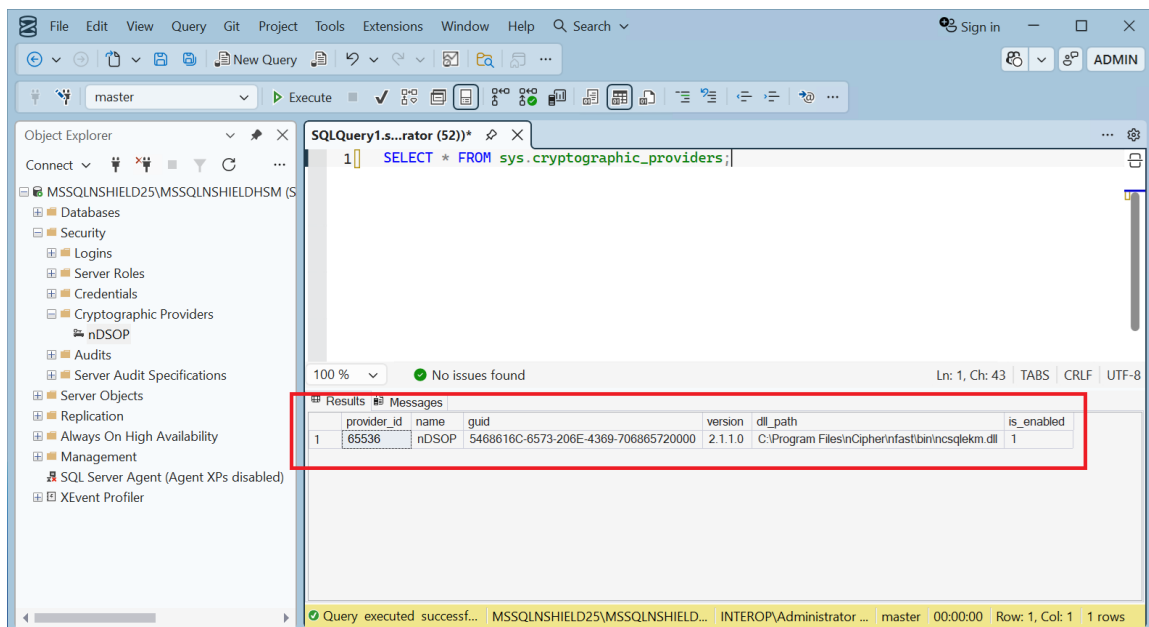


4.2. Verify the SQLEKM provider configuration

To verify the SQLEKM provider configuration:

1. Run the following query:

```
SELECT * FROM sys.cryptographic_providers;
```



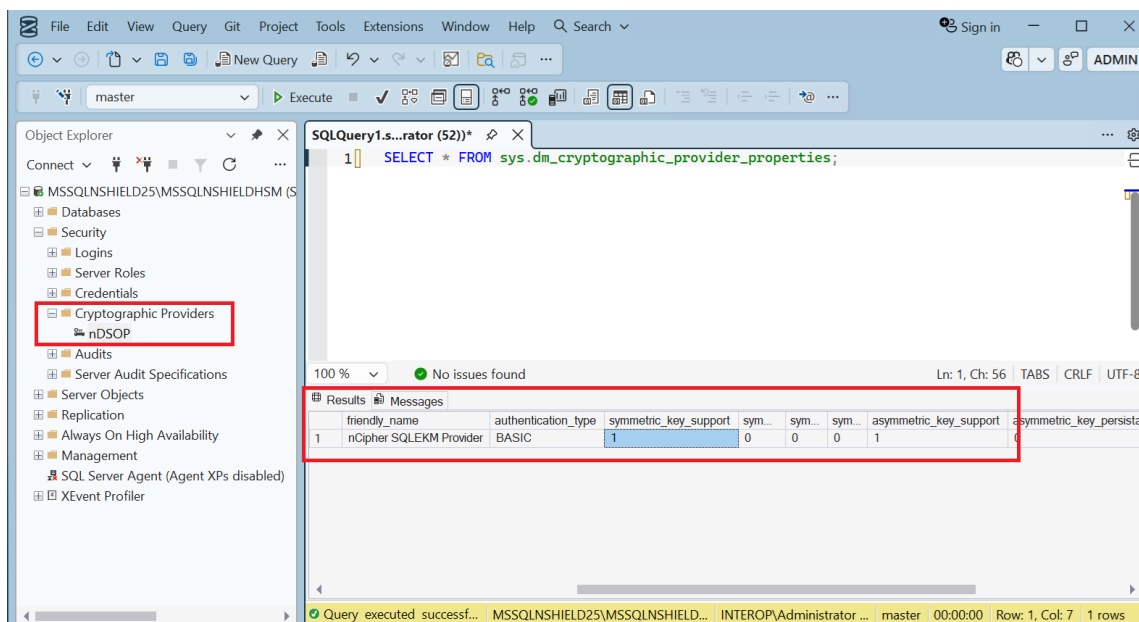
Verify the following:

- The version matched that of the nDSOP installation **is**o.

- Path to **dll** is correct.
- **is_enabled** column set to **1**.

2. Run the following query:

```
SELECT * FROM sys.dm_cryptographic_provider_properties;
```

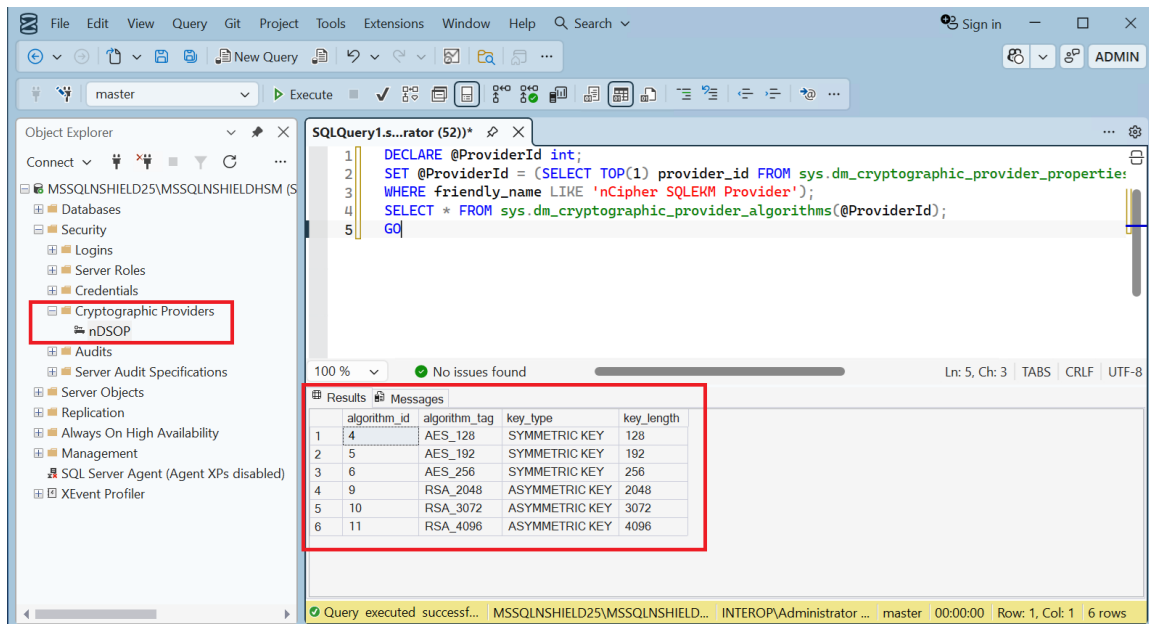


Verify the following:

Column	Value
friendly_name	nCipher SQLEKM Provider
authentication_type	BASIC
symmetric_key_support	1
asymmetric_key_support	1

3. Verify the supported cryptographic algorithms can be queried by running the following query:

```
DECLARE @ProviderId int;
SET @ProviderId = (SELECT TOP(1) provider_id FROM sys.dm_cryptographic_provider_properties
WHERE friendly_name LIKE 'nCipher SQLEKM Provider');
SELECT * FROM sys.dm_cryptographic_provider_algorithms(@ProviderId);
GO
```



Notice each key type has its set of valid algorithms.

Key Type	Algorithm
Symmetric	AES_128, AES_192, ASE_256
Asymmetric	RSA_2048, RSA_3072, RSA_4096

4.3. Create the user SQL Server credential

To create the user SQL Server credential:

1. Verify the OCS or Softcard created above:

```

> nfkminfo -c
Cardset list - 1 cardsets: (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
Operator logical token hash k/n timeout name
edb3d45a28e5a6b22b033684ce589d9e198272c2 1/5 none-NL testOCS

> nfkminfo -s
SoftCard summary - 1 softcards:
Operator logical token hash name
925f67e72ea3c354cae4e6797bde3753d24e7744 testSC

```

2. Insert the OCS in the HSM slot or TVD. If using Softcard protection, no action is needed.
3. Navigate to **Security > Credentials** in SQL Server Management Studio.
4. Right-click **Credentials**, then select **New Credential**.
5. Under **New Credential**:

- a. Enter the **Credential name**.
- b. For **Identity**, enter the OCS card or Softcard name.
- c. Enter the **passphrase** of the OCS card or Softcard.
- d. Select **Use Encryption Provider**.
- e. For **Provider**, select **nDSOP**.
- f. Select **OK**.

The screenshot shows the 'New Credential' dialog box with the following fields and options:

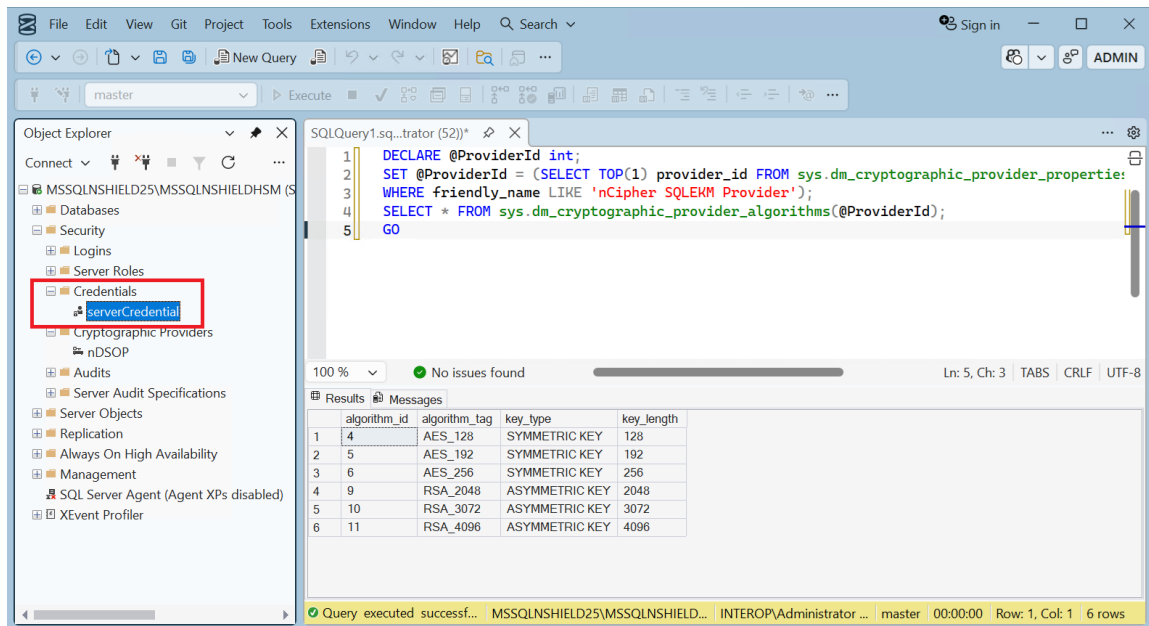
- Credential name:** serverCredential
- Identity:** testOCS
- Password:** [masked]
- Confirm password:** [masked]
- Use Encryption Provider
- Provider:** nDSOP

The 'Connection' section displays:

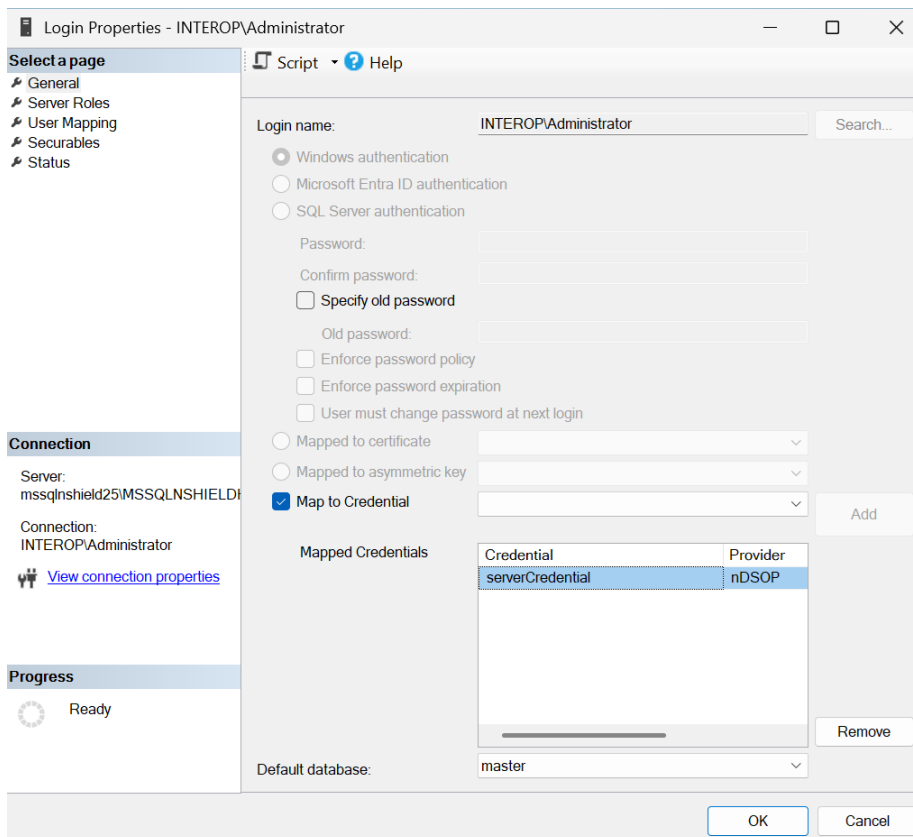
- Server: mssqlshield25\MSSQLNSHIELD
- Connection: INTEROPAdministrator
- [View connection properties](#)

The 'Progress' section shows a 'Ready' status.

6. Verify the new credential in **Security > Credentials**. You may need to right-click and select **Refresh**.



7. Navigate to **Security > Logins**. Right-click the login used to access the TestDatabase and select **Properties**.
8. Check **Map to Credentials** in the dialog. Select the server credential created above in the drop-down to the right. Then select **Add**, and select **OK**.



Chapter 5. Configure TDE

The TDE Database Encryption Key (TDEDEK) is a symmetric key that is used to perform the actual encryption of the database and are unique to a given database. It is created by SQL Server and cannot be exported from the database, meaning it cannot be created or directly protected by the SQLEKM provider (nShield HSM).

The TDEDEK is protected within the database by encrypting it with a wrapping key. The wrapping key is called the TDE Key Encryption Key (TDEKEK). The TDEKEK is an asymmetric key protected by the SQLEKM provider in the nShield HSM. It is possible to have a single TDEKEK for multiple databases, or different TDEKEKs for different databases.

The TDEKEK must be created under the `tdeLogin/tdeCredential`. However, the current user does not have to use the `tdeCredential`, so long as the user credential is using the same OCS or Softcard as the `tdeCredential`.

5.1. Create a TDEKEK

To create a TDEKEK in the master database:

1. Insert the OCS in the HSM slot or TVD. If using Softcard protection, no action is needed.
2. Run the following query:

```
USE master;
CREATE ASYMMETRIC KEY "<name_of_key_in_database>"
FROM PROVIDER "<SQLEKM_provider>"
WITH
PROVIDER_KEY_NAME = '<name_of_key_in_SQLEKM_provider>',
CREATION_DISPOSITION = CREATE_NEW,
ALGORITHM = <asymmetric_algorithm_desc>;
GO
```

Where:

name_of_key_in_database	Name given to the key in the database.
name_of_key_in_SQLEKM_provider	Name given to the key in the SQLEKM provider.
asymmetric_algorithm_desc	A valid asymmetric key algorithm descriptor.

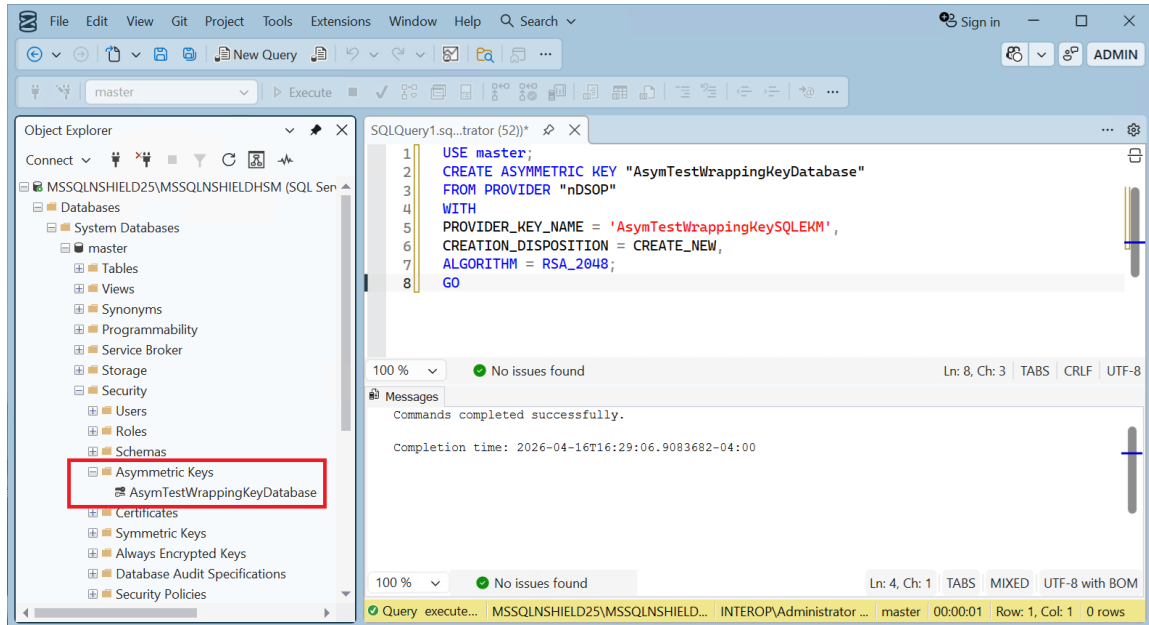
For example:

```

USE master;
CREATE ASYMMETRIC KEY "AsymTestWrappingKeyDatabase"
FROM PROVIDER "nDSOP"
WITH
PROVIDER_KEY_NAME = 'AsymTestWrappingKeySQLEKM',
CREATION_DISPOSITION = CREATE_NEW,
ALGORITHM = RSA_2048;
GO

```

Notice the newly created key highlighted in the object explorer.



3. The key generated can also be verified using a CLI command:

```

>nfkminfo -l

Keys protected by cardsets:
key_simple_sqlekm-edb3d45a28e5a6b22b033684ce589d9e198272c2-026abe8f340d2c124f68f006a8ee37fd58a2cc26
'AsymTestWrappingKeySQLEKM'

```

The `rocs` utility shows the names and protection methods of the keys.

```

>rocs
'rocs' key recovery tool
Useful commands: 'help', 'help intro', 'quit'.
rocs> list keys
  No. Name                               App      Protected by
  --- --
   1 AsymTestWrappingKeySQLEK simple    test0CS
rocs> quit

```

5.2. Create a TDE login and credential

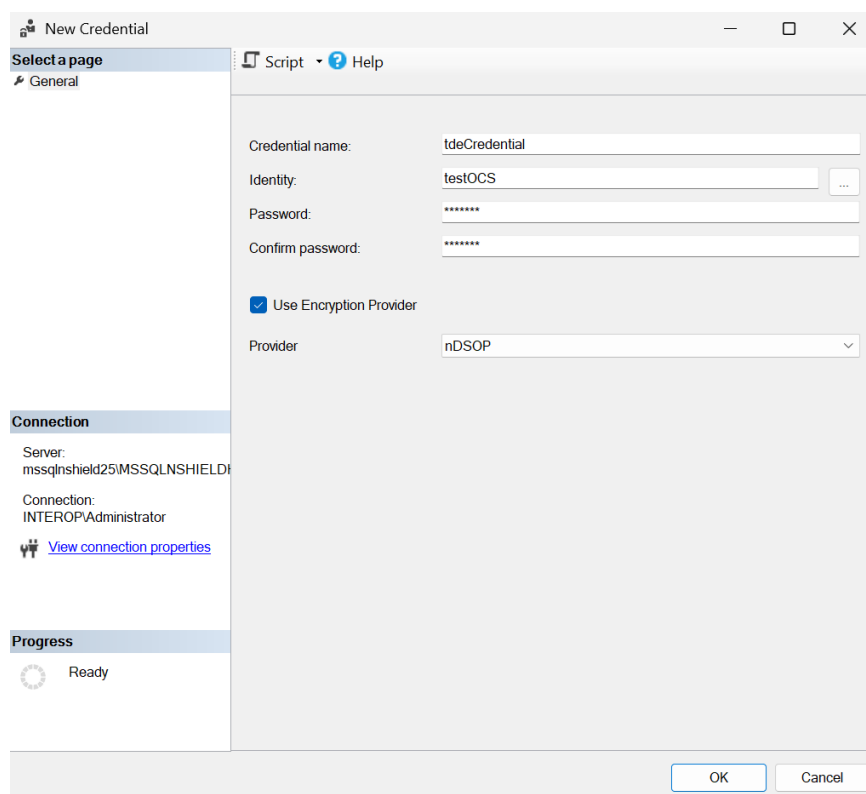
A `tdeLogin` and `tdeCredential` allows an ordinary database user, who is fully authorized to

use the database, but has no SQLEKM credentials of their own, to perform query operations using a TDE encrypted database. Without the tdeLogin and tdeCredential, then every user would need their own credentials. It is beyond the scope of this document to provide an example of how to use these credentials, only on how to create them.

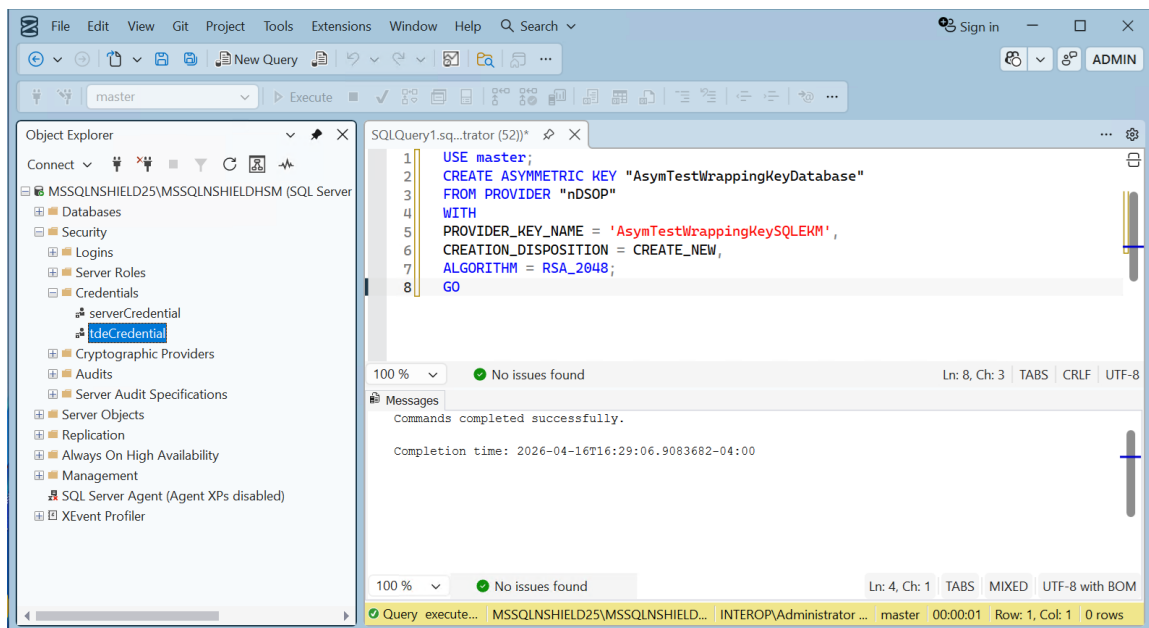
5.2.1. Create a TDE credential

To create a TDE credential:

1. Insert the OCS in the HSM slot or TVD. If using Softcard protection, no action is needed.
2. In SQL Server Management Studio, navigate to **Security > Credentials**.
3. Right-click **Credentials**, then select **New Credential**.
4. Under **New Credential**:
 - a. Enter the **Credential name**.
 - b. For **Identity**, enter the OCS card or Softcard name.
 - c. Enter the **passphrase** of the OCS card or Softcard.
 - d. Select **Use Encryption Provider**.
 - e. For **Provider**, select **nDSOP**.
 - f. Select **OK**.



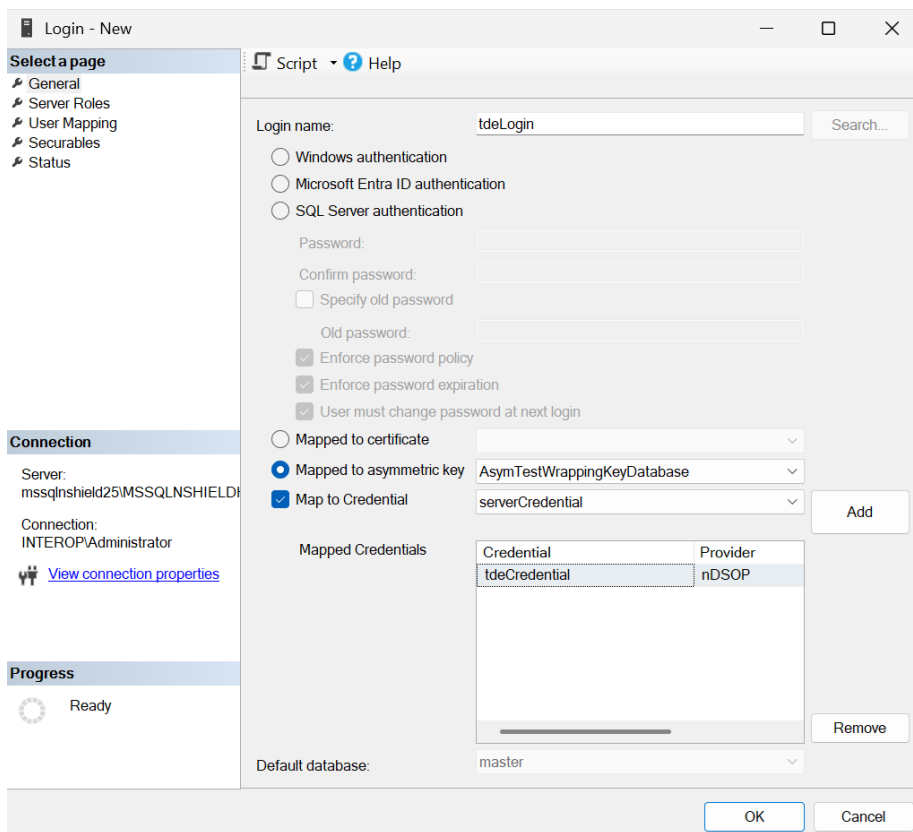
5. Notice the credential created.



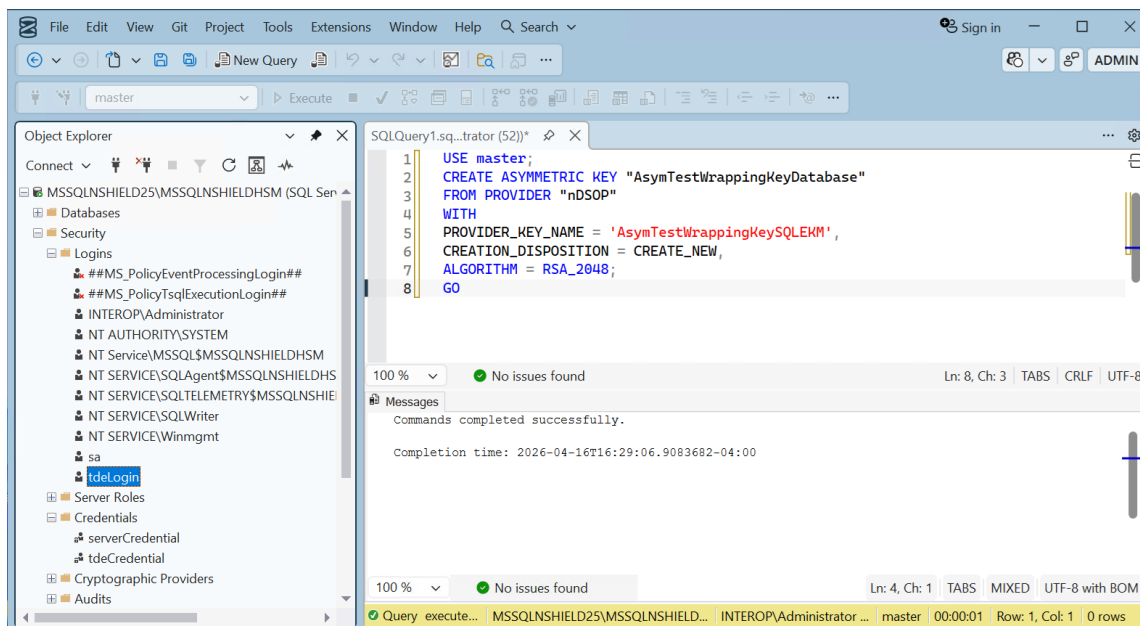
5.2.2. Create a TDE login

To create a TDE login:

1. In SQL Server Management Studio, navigate to **Security > Logins**.
2. Right-click **Logins**, then select **New Login**.
3. Enter the **Login name**.
4. Select **Mapped to asymmetric key**. Then select the TDEDEK created in [Create a TDEKEK](#).
5. Select **Map to Credential**. Then select the TDE credential created in [Create a TDE credential](#). Then select **Add**.
6. Select **OK**.



7. Notice the login created.

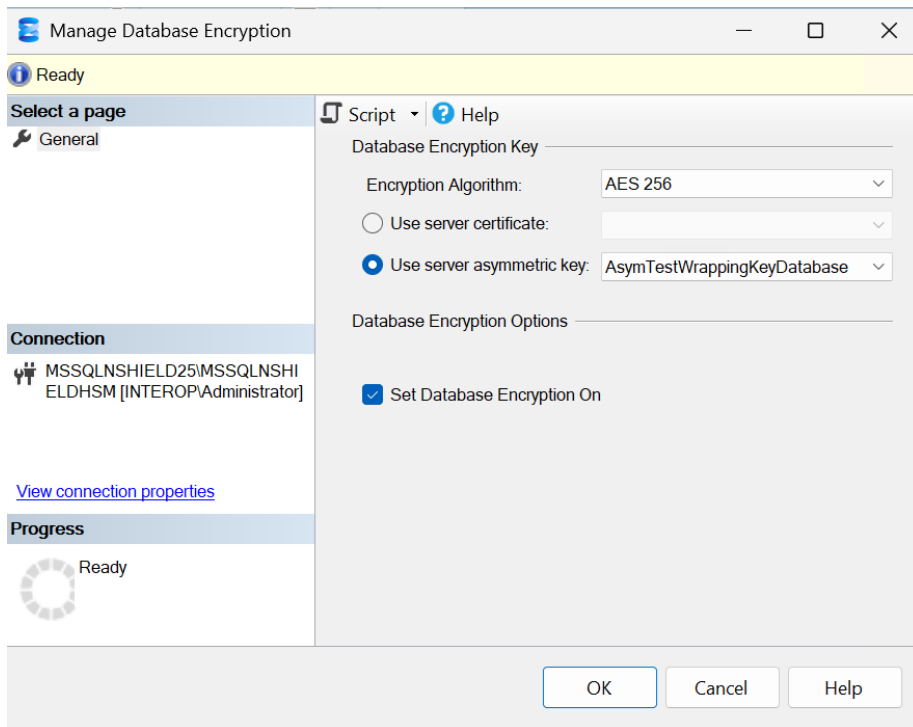


5.3. Create the TDEDEK and switch on encryption

To create the TDEDEK and switch on encryption:

1. In SQL Server Management Studio, navigate to **Databases > TestDatabase**.

2. Right-click TestDatabase, then select **Tasks > Manage Database Encryption**.
3. Set **Encryption Algorithm** to **AES 256** or your choice.
4. Select **Use server asymmetric key**. Then select the TDEDEK created in [Create a TDEDEK](#).
5. Select **Set Database Encryption On**. If using OCS protection, present the card at this point. Then select **OK**.

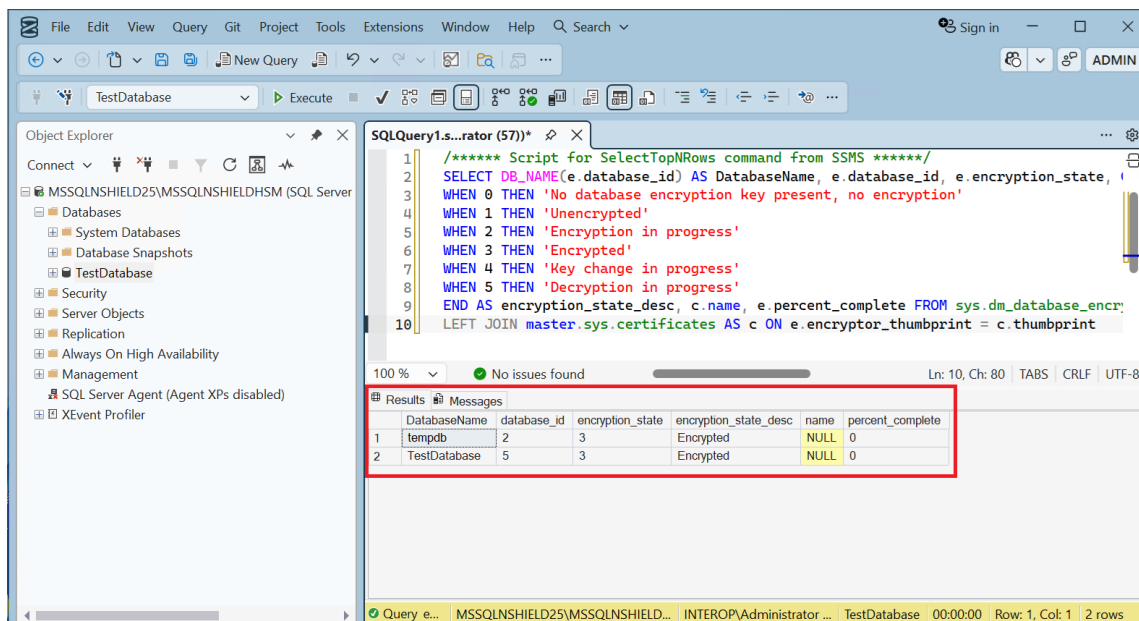


6. Run the following query to verify the encryption state:

```

/***** Script for SelectTopNRows command from SSMS *****/
SELECT DB_NAME(e.database_id) AS DatabaseName, e.database_id, e.encryption_state, CASE e.encryption_state
WHEN 0 THEN 'No database encryption key present, no encryption'
WHEN 1 THEN 'Unencrypted'
WHEN 2 THEN 'Encryption in progress'
WHEN 3 THEN 'Encrypted'
WHEN 4 THEN 'Key change in progress'
WHEN 5 THEN 'Decryption in progress'
END AS encryption_state_desc, c.name, e.percent_complete FROM sys.dm_database_encryption_keys AS e
LEFT JOIN master.sys.certificates AS c ON e.encryptor_thumbprint = c.thumbprint

```



The following table shows the value returned for encryption state and the meaning.

Encryption state	Meaning
0	Encryption disabled (or no encryption key)
1	Unencrypted or Decrypted
2	Unencrypted or Decrypted
3	Encrypted
4	Key change in progress
5	Decryption in progress
6	Protection change in progress (The certificate or asymmetric key that is encrypting the database encryption key is being changed)

7. Turn encryption off and on by toggling **Set Database Encryption On** in the steps above, each time running the query to verify the encryption state.

5.4. Key rotation - Replace the TDEKEK

This section performs a key rotation by replacing the TDEKEK, an asymmetric key protected by the SQLEKM provider in the nShield HSM.

1. Create a new asymmetric TDEKEK. Follow the procedure in [Create a TDEKEK](#). For

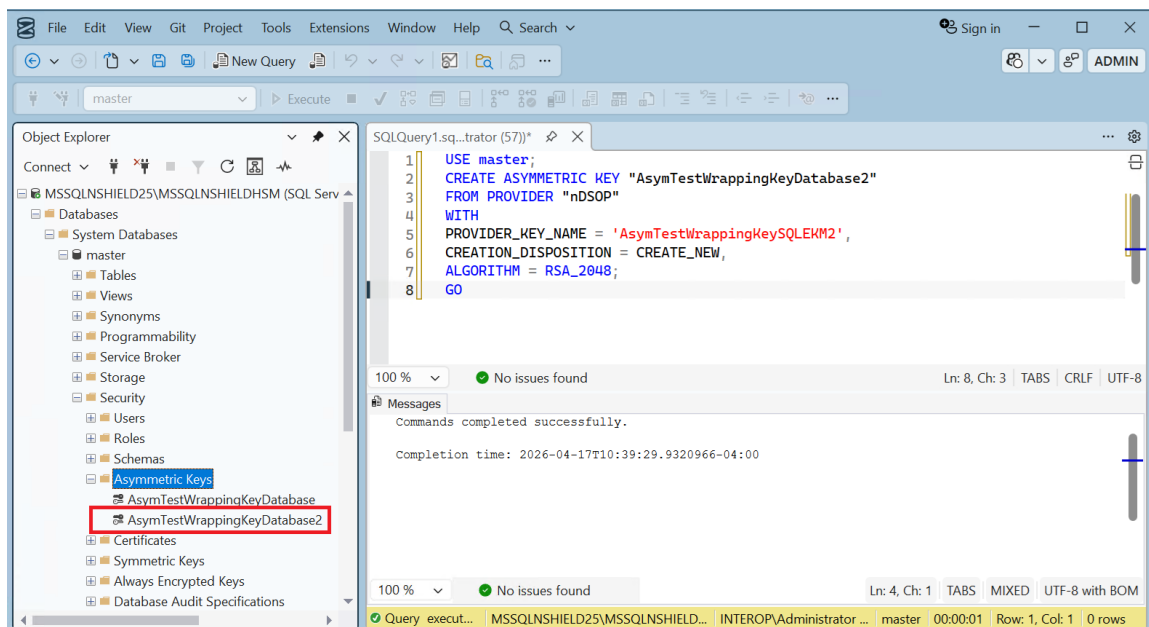
example:

```
USE master;
CREATE ASYMMETRIC KEY "AsymTestWrappingKeyDatabase2"
FROM PROVIDER "nDSOP"
WITH
PROVIDER_KEY_NAME = 'AsymTestWrappingKeySQLEKM2',
CREATION_DISPOSITION = CREATE_NEW,
ALGORITHM = RSA_2048;
GO
```

```
> nfkminfo -l
```

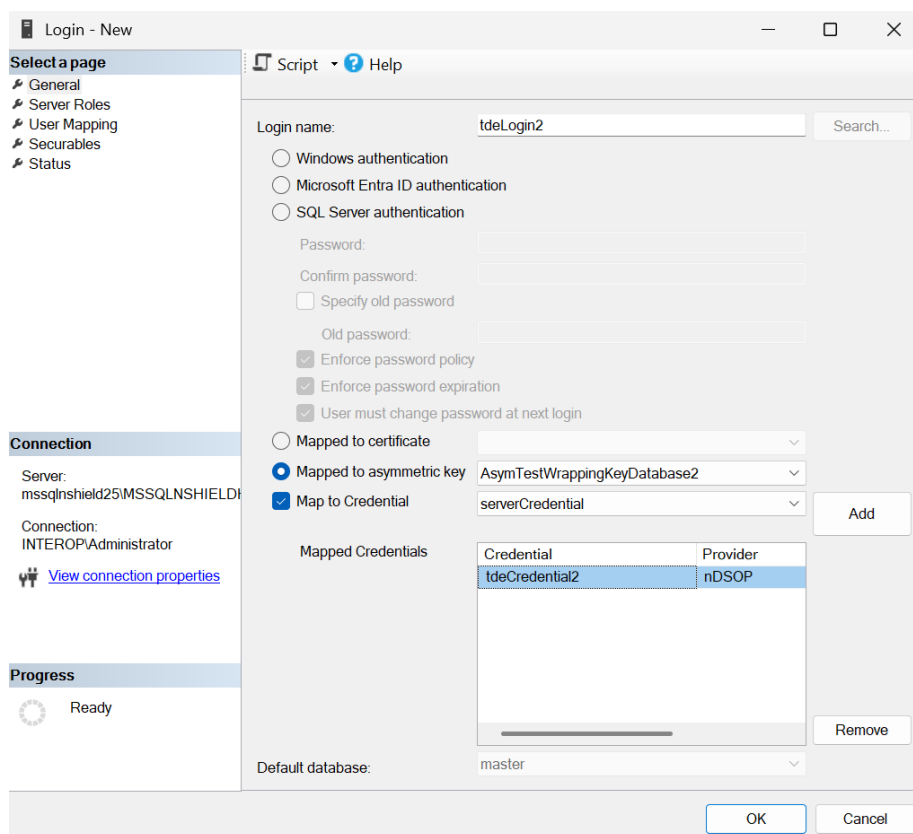
Keys protected by cardsets:

```
key_simple_sqlekm-edb3d45a28e5a6b22b033684ce589d9e198272c2-026abe8f340d2c124f68f006a8ee37fd58a2cc26
'AsymTestWrappingKeySQLEKM'
key_simple_sqlekm-edb3d45a28e5a6b22b033684ce589d9e198272c2-b08737c94cff5a51a3483c60c7ff883bb6e998c9
'AsymTestWrappingKeySQLEKM2'
```

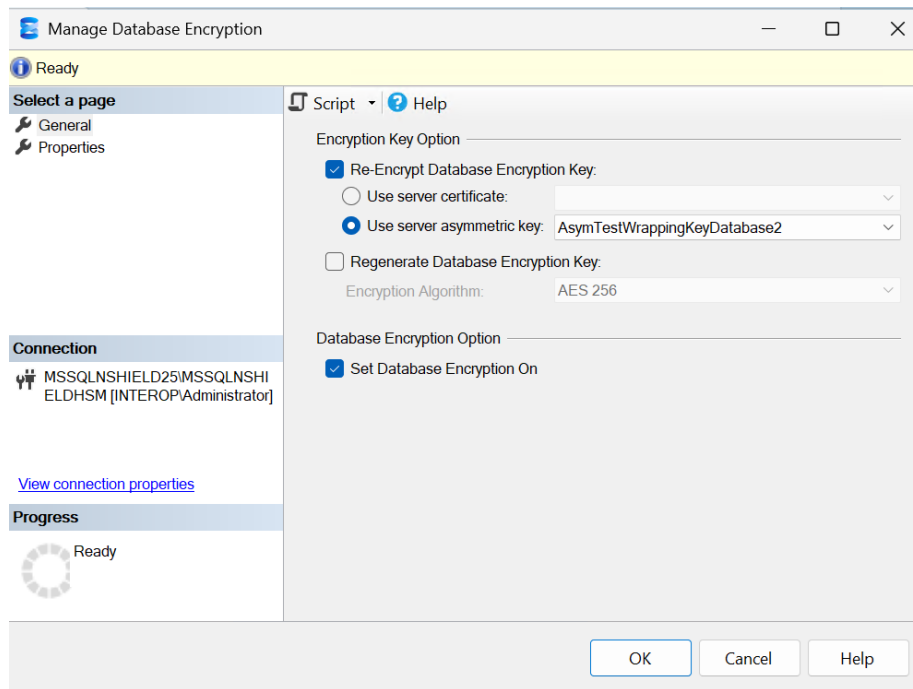


2. Create a new TDE credential. Follow the procedure in [Create a TDE credential](#).
3. Create a new TDE login mapped to the new asymmetric key and credential created above. Follow the procedure in [Create a TDE login](#).

For example:



4. In SQL Server Management Studio, navigate to **Databases > TestDatabase**.
5. Right-click TestDatabase, then select **Tasks > Manage Database Encryption**.
6. Select **Re-Encrypt Database Encryption Key** and **Use server asymmetric**.
7. Select the newly created asymmetric key **AsymTestWrappingKeyDatabase2**.
8. Deselect **Regenerate Database Encryption Key**.
9. Select **Set Database Encryption On**.
10. Select **OK**.

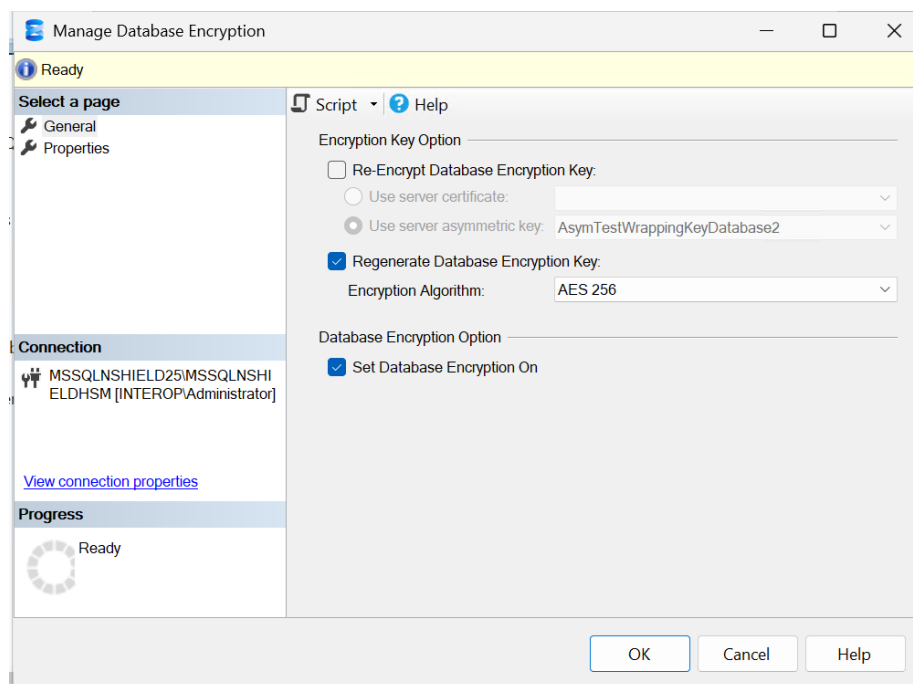


11. Verify the encryption state as shown in [Create the TDEDEK and switch on encryption](#).

5.5. Key rotation - Replace the TDEDEK

This section performs a key rotation by replacing the TDEDEK, a symmetric key used to perform the actual encryption of the database. This key is created by SQL Server and cannot be exported from the database. It is protected within the database by encrypting it with a wrapping key TDEKEK.

1. In SQL Server Management Studio, navigate to **Databases > TestDatabase**.
2. Right-click TestDatabase, then select **Tasks > Manage Database Encryption**.
3. Deselect **Re-Encrypt Database Encryption Key**.
4. Select **Regenerate Database Encryption Key**.
5. Select **AES 256**.
6. Select **Set Database Encryption On**.
7. Select **OK**.



8. Verify the encryption state as shown in [Create the TDEDEK and switch on encryption](#).

Chapter 6. Column level encryption

Table column data can be protected by an Entrust nShield HSM protected key. These nDSOP EKM keys can encrypt/decrypt data in a column.

6.1. Create a new key

Create a new key within the SQL Server database to encrypt a column. This key will be protected by the Entrust nShield HSM.

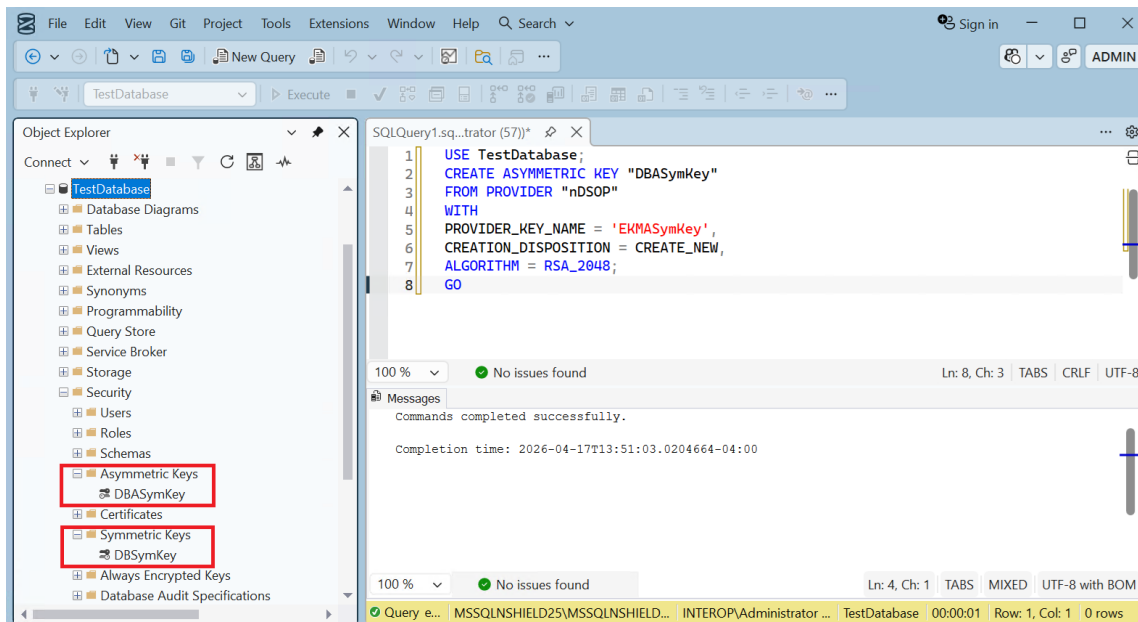
1. Insert the OCS in the HSM slot or TVD. If using Softcard protection, no action is needed.
2. To create an symmetric key, run the following query:

```
USE TestDatabase;
CREATE SYMMETRIC KEY "DBSymKey"
FROM PROVIDER "nDSOP"
WITH
PROVIDER_KEY_NAME = 'EKMSymKey', IDENTITY_VALUE = '$DBSymKey',
CREATION_DISPOSITION = CREATE_NEW,
ALGORITHM = AES_256;
GO
```

3. To create a asymmetric key, run the following query:

```
USE TestDatabase;
CREATE ASYMMETRIC KEY "DBASymKey"
FROM PROVIDER "nDSOP"
WITH
PROVIDER_KEY_NAME = 'EKMASymKey',
CREATION_DISPOSITION = CREATE_NEW,
ALGORITHM = RSA_2048;
GO
```

4. Verify the keys created above.



```

> nfkminfo -l

Keys protected by cardsets:
key_simple_sqllekm-edb3d45a28e5a6b22b033684ce589d9e198272c2-026abe8f340d2c124f68f006a8ee37fd58a2cc26
'AsymTestWrappingKeySQLEKM'
key_simple_sqllekm-edb3d45a28e5a6b22b033684ce589d9e198272c2-4fb51bde7597bbf997f6a2c918d1a751651b1e36
'EKMASymKey'
key_simple_sqllekm-edb3d45a28e5a6b22b033684ce589d9e198272c2-aadcea7a00fca427316e483cb5168f7a1a0dc515
'EKMSymKey'
key_simple_sqllekm-edb3d45a28e5a6b22b033684ce589d9e198272c2-b08737c94cff5a51a3483c60c7ff883bb6e998c9
'AsymTestWrappingKeySQLEKM2'
    
```

6.2. Import an existing key

The Entrust nShield HSM utility **generatekey** will be used to create an asymmetric key. Then this key will be imported in the SQL Server.

1. Run the utility **generatekey** interactive as show below:



The **ident: Key identifier?** [] must begin with **sqllekm-**, and may not contain upper case characters.

```

> generatekey simple
protect: Protected by? (token, softcard, module) [token] >
slot: Slot to read cards from? (0-5) [0] >
recovery: Key recovery? (yes/no) [yes] >
type: Key type? (AES, DES2, DES3, DH, DHEX, DSA, EC, ECDH, ECDSA, HMACSHA1,
HMACSHA256, HMACSHA384, HMACSHA512, Rijndael, RSA) [RSA]
>
size: Key size? (bits, minimum 1024) [2048] >
OPTIONAL: pubexp: Public exponent for RSA key (hex)? []
>
ident: Key identifier? [] > sqllekm-ekmexistingasymkey
plainname: Key name? [] > EKMEExistingASymKey
    
```

```

nvrnm: Blob in NVRAM (needs ACS)? (yes/no) [no] >
key generation parameters:
operation      Operation to perform      generate
application    Application                simple
protect        Protected by               token
slot           Slot to read cards from   0
recovery       Key recovery               yes
verify         Verify security of key    yes
type           Key type                   RSA
size           Key size                   2048
pubexp         Public exponent for RSA key (hex)
ident          Key identifier             sqlckm-ekmexistingasymkey
plainname      Key name                   EKMEExistingASymKey
nvrnm          Blob in NVRAM (needs ACS) no

Loading cardset(s):
Module 1 slot 2: 'testOCS' #2
Module 1 slot 0: empty
Module 1 slot 3: empty
Module 1 slot 4: empty
Module 1 slot 5: empty
Module 1 slot 2:- passphrase supplied - reading card
Card reading complete.

Key successfully generated.
Path to key: C:\ProgramData\ncipher\Key Management Data\local\key_simple_sqlckm-ekmexistingasymkey

```

2. Notice the newly created key.

```

> nfkminfo -l

Keys protected by cardsets:
key_simple_sqlckm-edb3d45a28e5a6b22b033684ce589d9e198272c2-026abe8f340d2c124f68f006a8ee37fd58a2cc26
'AsymTestWrappingKeySQLCKM'
key_simple_sqlckm-edb3d45a28e5a6b22b033684ce589d9e198272c2-4fb51bde7597bbf997f6a2c918d1a751651b1e36
'EKMASymKey'
key_simple_sqlckm-edb3d45a28e5a6b22b033684ce589d9e198272c2-aadcea7a00fca427316e483cb5168f7a1a0dc515
'EKMSymKey'
key_simple_sqlckm-edb3d45a28e5a6b22b033684ce589d9e198272c2-b08737c94cff5a51a3483c60c7ff883bb6e998c9
'AsymTestWrappingKeySQLCKM2'
key_simple_sqlckm-ekmexistingasymkey `EKMEExistingASymKey'

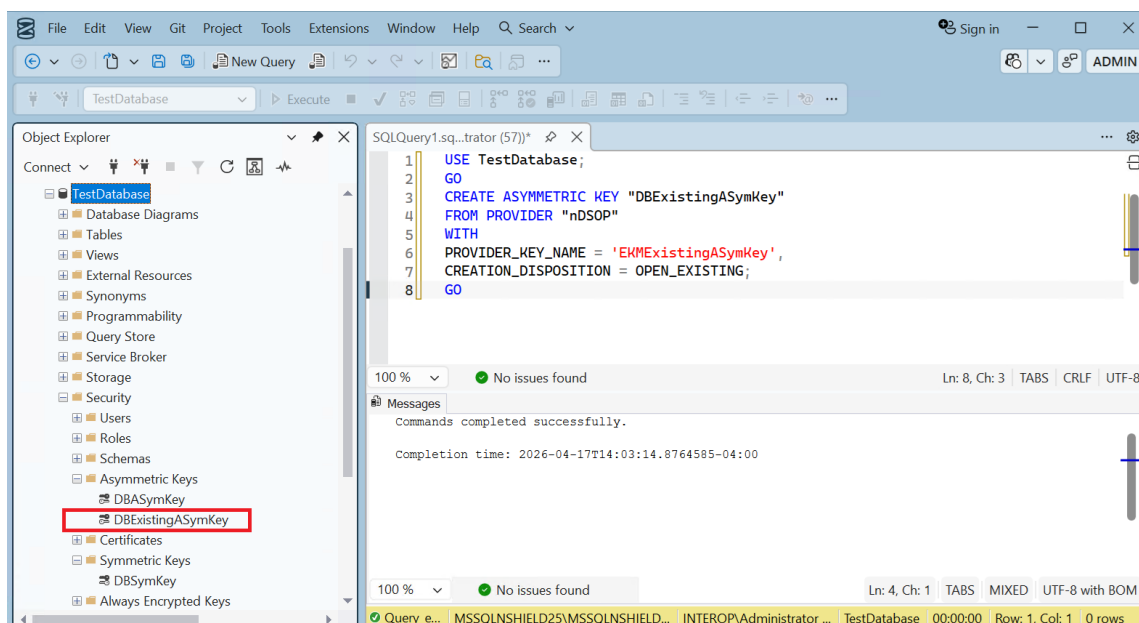
```

3. Import the newly created key by running the following query. Re-start the SSMS if the key is not found.

```

USE TestDatabase;
GO
CREATE ASYMMETRIC KEY "DBExistingASymKey"
FROM PROVIDER "nDSOP"
WITH
PROVIDER_KEY_NAME = 'EKMEExistingASymKey',
CREATION_DISPOSITION = OPEN_EXISTING;
GO

```



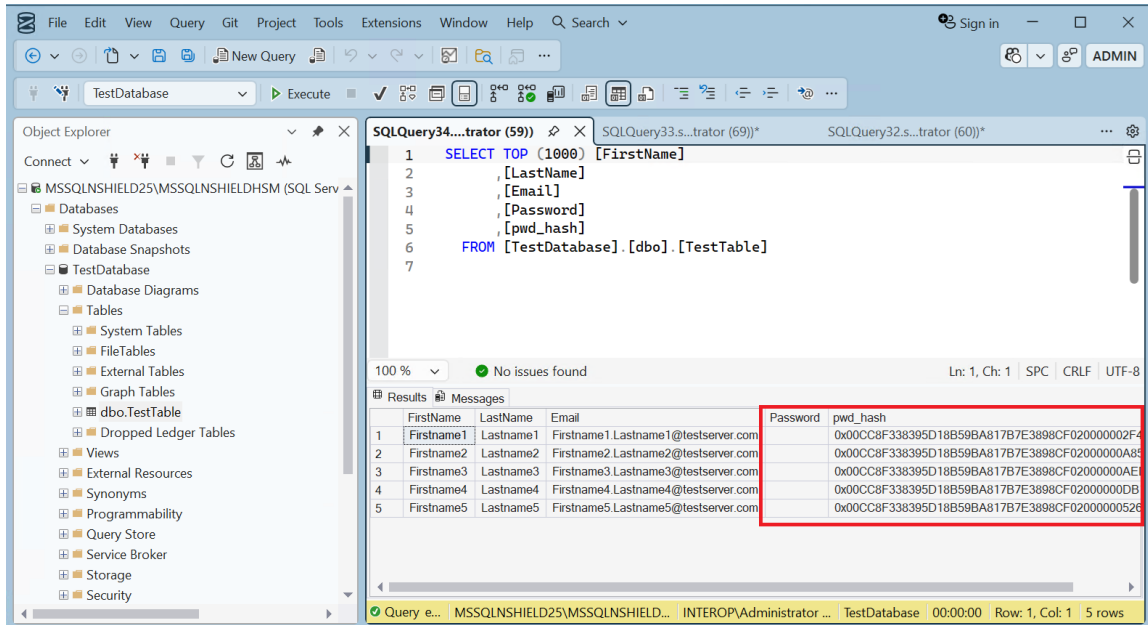
6.3. Encrypt a column with a symmetric key

To encrypt a column with a symmetric key:

1. Run the following query to create a new **pwd_hash** column that contains the encrypted passwords using the symmetric key created earlier. Populate the **Password** column with blank values.

```
USE TestDatabase;
ALTER TABLE TestTable
ADD pwd_hash VARBINARY (256);
GO
UPDATE TestTable
SET pwd_hash = ENCRYPTBYKEY(KEY_GUID('DBSymKey'), Password);
UPDATE TestTable
SET Password = '';
GO
```

2. Notice the new **pwd_hash** column containing the encrypted passwords.

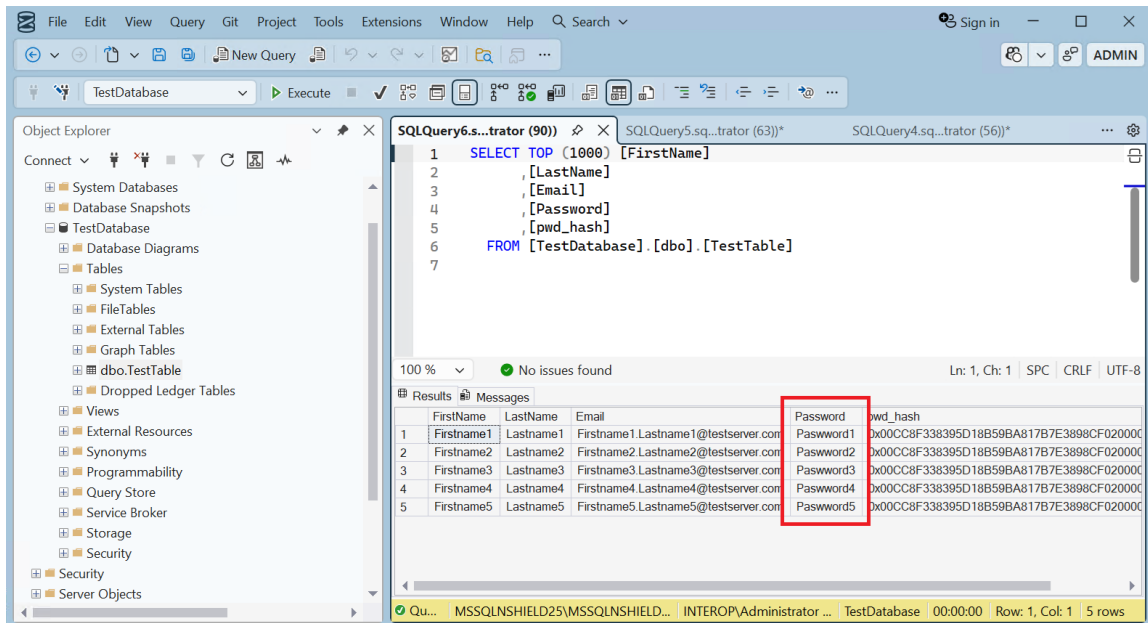


Clear the "Invalid column name 'pwd_hash'" error by selecting **Toolbar > Edit > IntelliSense > Refresh Local Cache**.

3. Run the following query to decrypted the column above.

```
USE TestDatabase;
UPDATE TestTable
SET Password = DecryptByKey(pwd_hash);
GO
```

4. Notice the **Password** column is now populated with the decrypted password.



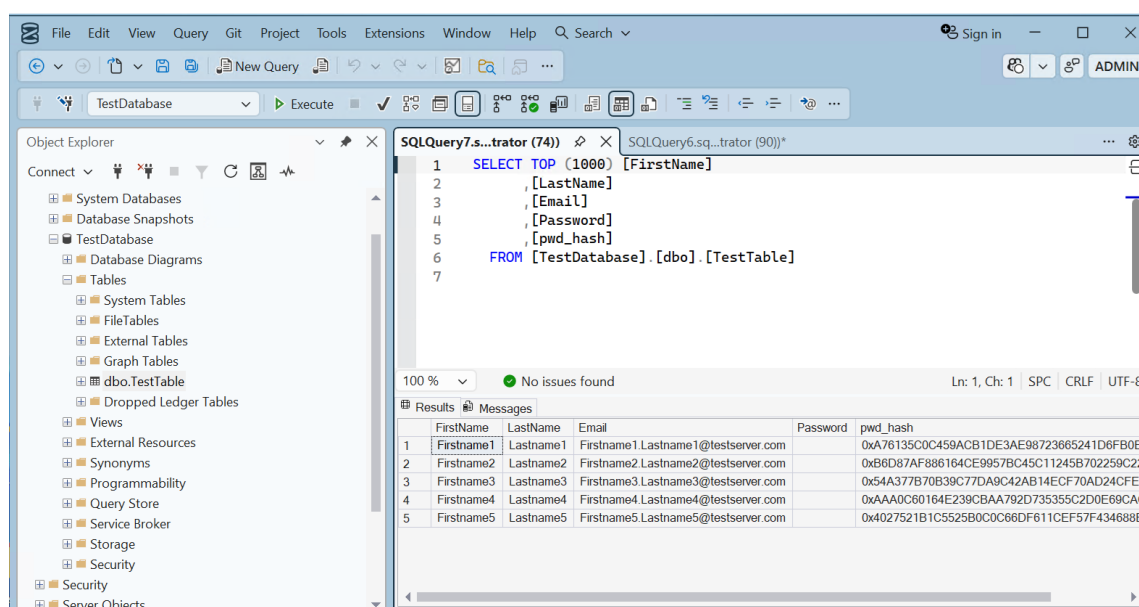
6.4. Encrypt a column with an asymmetric key

To encrypt a column with an asymmetric key:

1. Run the following query to encrypt the passwords with the asymmetric key created above, and populate the **Password** column with blanks.

```
USE TestDatabase;
UPDATE TestTable
SET pwd_hash = ENCRYPTBYASYMKEY(ASYMKEY_ID('DBASymKey'), Password);
UPDATE TestTable
SET Password = '';
GO
```

2. Notice the **pwd_hash** column has new values corresponding to the asymmetric key.

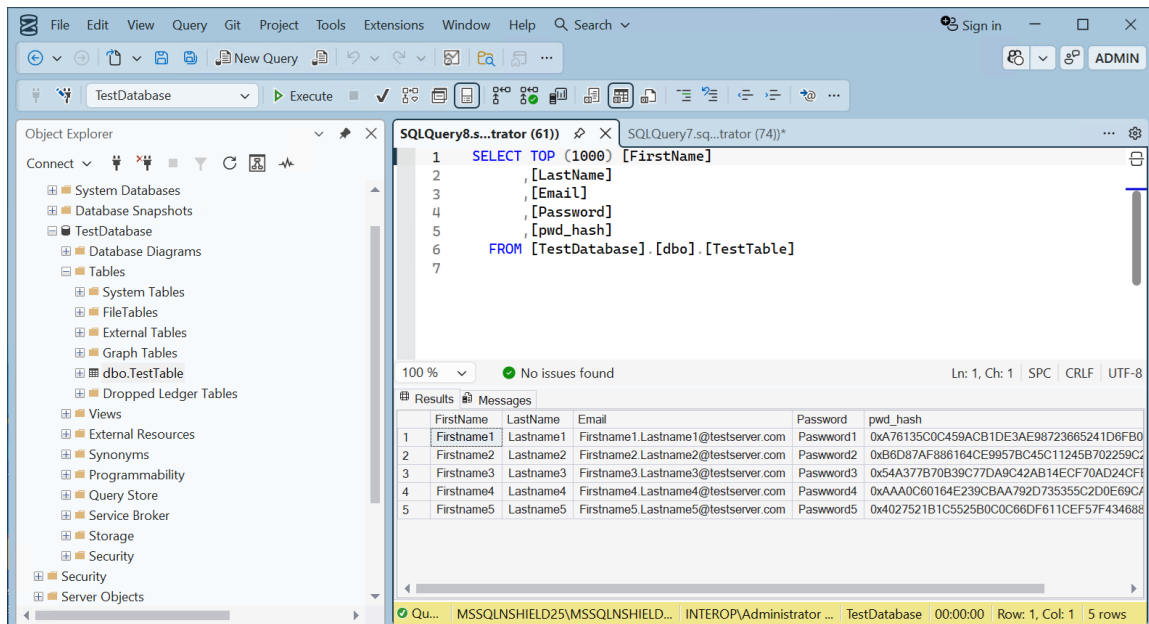


	FirstName	LastName	Email	Password	pwd_hash
1	Firstname1	Lastname1	Firstname1.Lastname1@testserver.com		0xA76135C0C459ACB1DE3AE98723665241D6FB0E
2	Firstname2	Lastname2	Firstname2.Lastname2@testserver.com		0xB6D87AF886164CE9957BC45C11245B702259C22
3	Firstname3	Lastname3	Firstname3.Lastname3@testserver.com		0x54A377B70B39C77DA9C42AB14ECF70AD24CFEE
4	Firstname4	Lastname4	Firstname4.Lastname4@testserver.com		0xAAA0C60164E239CBAA792D735355C2D0E69CAC
5	Firstname5	Lastname5	Firstname5.Lastname5@testserver.com		0x4027521B1C5525B0C0C68DF611CE57F434688B

3. Run the following query to decrypted the column above.

```
USE TestDatabase;
UPDATE TestTable
SET Password = DECRYPTBYASYMKEY(ASYMKEY_ID('DBASymKey'), pwd_hash);
GO
```

4. Notice the **Password** column is now populated with the decrypted password.



6.5. Encrypt a column with the imported asymmetric key

To encrypt a column with the imported asymmetric key:

1. Run the following query to encrypt the passwords with the imported asymmetric, and populate the **Password** column with blanks.

```

USE TestDatabase;
UPDATE TestTable
SET pwd_hash = ENCRYPTBYASYMKEY(ASYMKEY_ID('DBExistingASymKey'), Password);
UPDATE TestTable
SET Password = '';
GO

```

2. Notice the **pwd_hash** column has new values corresponding to the imported key.

SQLQuery9.s...trator (58)

```

1 SELECT TOP (1000) [FirstName]
2     ,[LastName]
3     ,[Email]
4     ,[Password]
5     ,[pwd_hash]
6 FROM [TestDatabase].[dbo].[TestTable]
7

```

FirstName	LastName	Email	Password	pwd_hash
1	Firstname1	Lastname1	Firstname1.Lastname1@testserver.com	0xA6498FF6E568132A492194753E29271A9F8D3664
2	Firstname2	Lastname2	Firstname2.Lastname2@testserver.com	0x0ED80CBC00951374C2DBE2CD68F43E2FA6B1C1
3	Firstname3	Lastname3	Firstname3.Lastname3@testserver.com	0x80187A4986BD497935707160C1AB1FA34D15CD
4	Firstname4	Lastname4	Firstname4.Lastname4@testserver.com	0x4F9DA4C0BA29A4EF4BDAFD23DDE838D81757F
5	Firstname5	Lastname5	Firstname5.Lastname5@testserver.com	0x21BA9F4545645A7123682D8B54A39C6E2C649A6

3. Run the following query to decrypted the column above.

```

USE TestDatabase;
UPDATE TestTable
SET Password = DECRYPTBYASYMKEY(ASYMKEY_ID('DBExistingASymKey'), pwd_hash);
GO

```

4. Notice the **Password** column is now populated with the decrypted password.

SQLQuery10....trator (82)

```

1 SELECT TOP (1000) [FirstName]
2     ,[LastName]
3     ,[Email]
4     ,[Password]
5     ,[pwd_hash]
6 FROM [TestDatabase].[dbo].[TestTable]
7

```

FirstName	LastName	Email	Password	pwd_hash
1	Firstname1	Lastname1	Firstname1.Lastname1@testserver.com	0xA6498FF6E568132A492194753E29271A9F8D3664
2	Firstname2	Lastname2	Firstname2.Lastname2@testserver.com	0x0ED80CBC00951374C2DBE2CD68F43E2FA6B1C1
3	Firstname3	Lastname3	Firstname3.Lastname3@testserver.com	0x80187A4986BD497935707160C1AB1FA34D15CD
4	Firstname4	Lastname4	Firstname4.Lastname4@testserver.com	0x4F9DA4C0BA29A4EF4BDAFD23DDE838D81757F
5	Firstname5	Lastname5	Firstname5.Lastname5@testserver.com	0x21BA9F4545645A7123682D8B54A39C6E2C649A6

Chapter 7. Perform backup and recovery

A rigorous backup regimen is recommended to provide a means to recover both the database and associated keys used for encryption. Consult your corporate IT and security team for best practice and corporate policy requirements.

7.1. Back up the Security World

The Security World data is inherently encrypted and does not require any further encryption operation to protect it. It can only be used by someone who has access to a quorum of the correct ACS cards, or the OCS card, Softcard, their passphrases, an nShield HSM and nShield Security World Software. Therefore, backup simply consists of making a copy of the Security World files and saving the copy in a safe location, as necessary to restore the keys used by the database.

1. Back up `C:\ProgramData\nCipher\Key Management Data`.
2. Securely store and keep a record of ACS and OCS cards associated with each Security World, preferable using the serial number on the cards.
3. The Softcard, used instead of OCS, resides in the `Key Management Data` folder. It is backed up at `C:\ProgramData\nCipher\Key Management Data`.
4. Keep a record of which database and which Security World backups correspond to each other.

7.2. Restore the Security World

Restoring a Security World simply means restoring a backup copy of the Security World folder `C:\ProgramData\nCipher\Key Management Data`.

The ACS is required if the Security World being restored is not already loaded onto the HSM. See the *Installation Guide* and the *User Guide* for the HSM. A shorter version of this procedure is available at [How to: Locally set up a new or replacement nShield Connect](#).



Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

7.3. Back up the database

To back up the database:

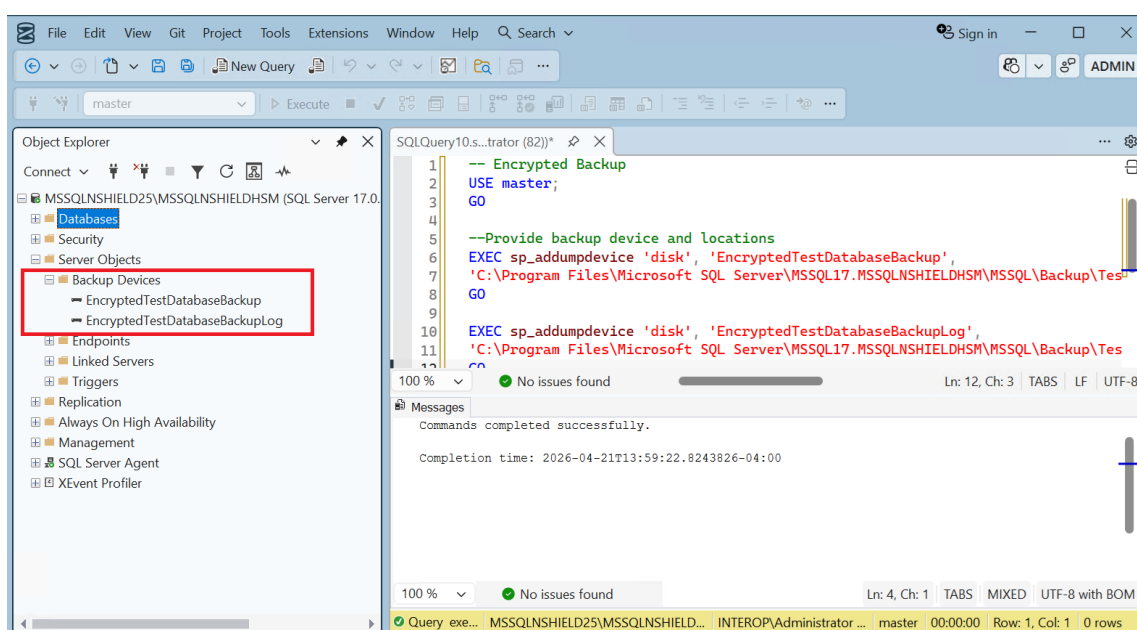
1. Create the backup devices by running the following query:

```
-- Encrypted Backup
USE master;
GO

--Provide backup device and locations
EXEC sp_addumpdevice 'disk', 'EncryptedTestDatabaseBackup',
'C:\Program Files\Microsoft SQL Server\MSSQL17.MSSQLNSHIELDHSM\MSSQL\Backup\TestDatabaseEncrypted.bak';
GO

EXEC sp_addumpdevice 'disk', 'EncryptedTestDatabaseBackupLog',
'C:\Program Files\Microsoft SQL Server\MSSQL17.MSSQLNSHIELDHSM\MSSQL\Backup\TestDatabaseEncryptedLog.bak';
GO
```

2. Notice the devices created.



3. Create the backup by running the following query:

```
-- Encrypted Backup
USE master;
GO

ALTER DATABASE TestDatabase
SET RECOVERY FULL;
GO

-- Back up the encrypted database
BACKUP DATABASE TestDatabase TO EncryptedTestDatabaseBackup;
GO

-- Back up the encrypted log
BACKUP LOG TestDatabase TO EncryptedTestDatabaseBackupLog;
GO
```

4. Notice the backup files created.

```

C:\Program Files\Microsoft SQL Server\MSSQL17.MSSQLNSHIELDHSM\MSSQL\Backup>dir
Volume in drive C has no label.
Volume Serial Number is 1425-A148

Directory of C:\Program Files\Microsoft SQL Server\MSSQL17.MSSQLNSHIELDHSM\MSSQL\Backup

04/21/2026  02:02 PM  <DIR>          .
04/16/2026  10:28 AM  <DIR>          ..
04/21/2026  02:02 PM                5,136,896 TestDatabaseEncrypted.bak
04/21/2026  02:02 PM                86,528 TestDatabaseEncryptedLog.bak
                2 File(s)      5,223,424 bytes
                2 Dir(s)  43,416,313,856 bytes free

```

If the database is encrypted, the backup will also be encrypted. If the database is not encrypted, then the backup will not be encrypted. If you want to create an encrypted backup from a non-encrypted database, you will have to create the non-encrypted backup file, and then encrypt the file using an independent encryption tool.

7.4. Restore the database

Restore a TDE encrypted database in a similar manner as an un-encrypted database. But for TDE encrypted database the Security World needs to be restored before restoring the encrypted database. The OCS, if used, needs to be inserted in the HSM before restoring the encrypted database. Otherwise, the restored database will appear as **(Restore Pending)**.

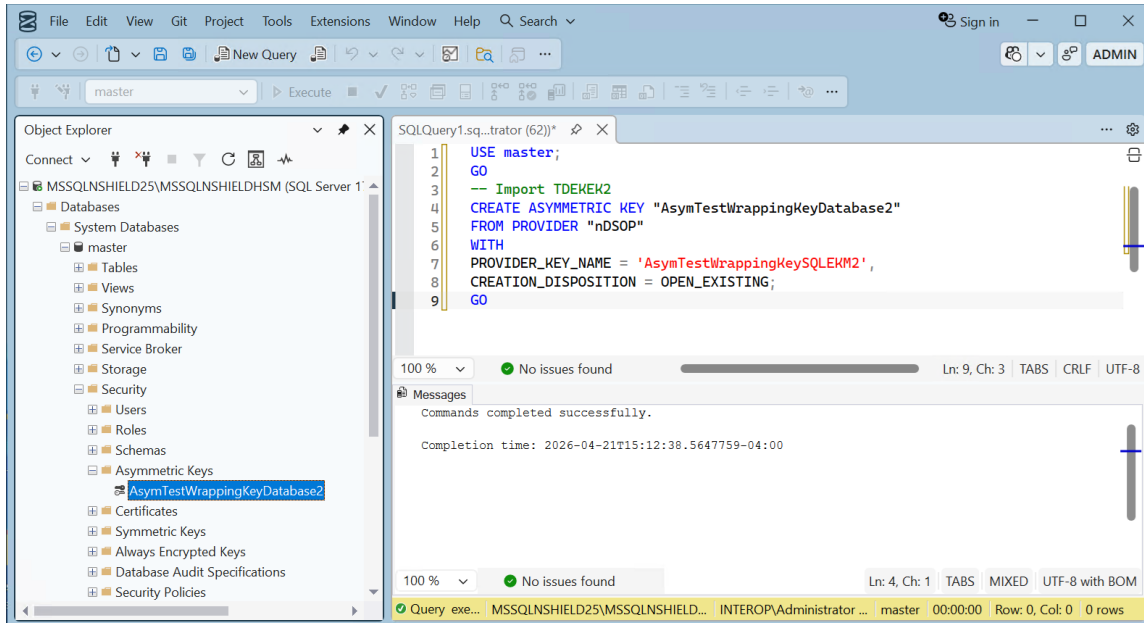
1. Install the Security World software and the nShield nDSOP if rebuilding the server. Do not create a Security World.
2. Restore the Security World.
3. Insert the OCS in the HSM front panel slot, or the TVD if using OCS protection.
4. Enable EKM and register the SQLEKM provider if rebuilding the server.
5. Create the SQL Server credential if rebuilding the server. The OCS and Softcard are in the restored Security World.
6. Verify the SQLEKM provider configuration if rebuilding the server.
7. Import the database wrapping key (TDEKEK) into the master database by running the following query. This is the TDEKEK last used to encrypt the database. This key should already exist in the restored Security World.

```

USE master;
GO

-- Import TDEKEK
CREATE ASYMMETRIC KEY "AsymTestWrappingKeyDatabase2"
FROM PROVIDER "nDSOP"
WITH
PROVIDER_KEY_NAME = 'AsymTestWrappingKeySQLEKM2',
CREATION_DISPOSITION = OPEN_EXISTING;
GO

```



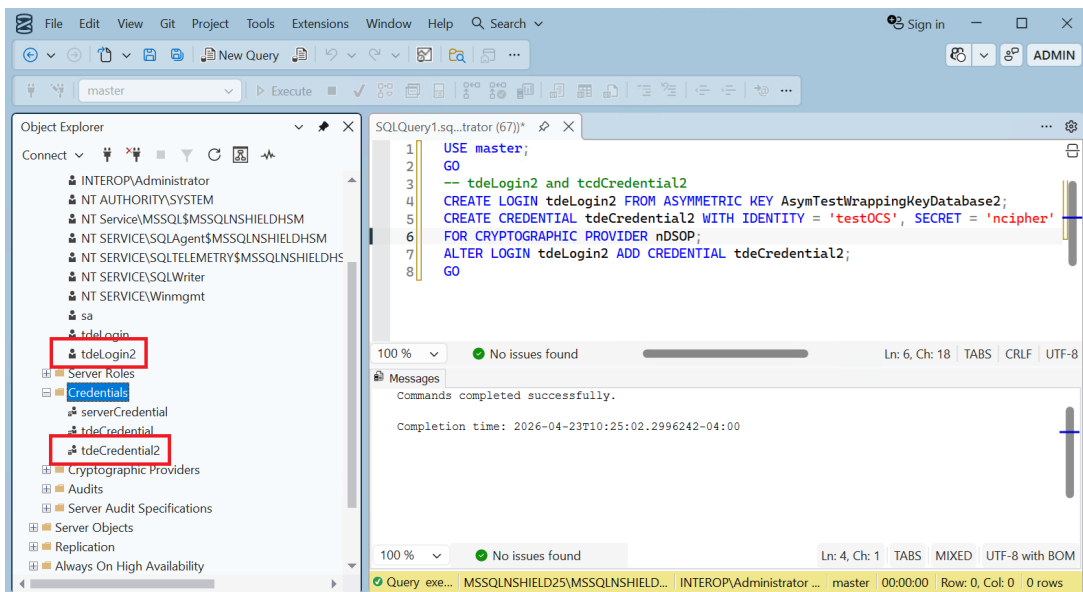
8. Recreate the TDE login and credential by running the following query. These are the TDE login and credential last used to encrypt the database. Notice the name of the OCS (**nDSOPocs**), and Softcard (**nDSOPsoftcard**) created earlier.

- OCS:

```

USE master;
GO

-- tdeLogin2 and tdcCredential2
CREATE LOGIN tdeLogin2 FROM ASYMMETRIC KEY AsymTestWrappingKeyDatabase2;
CREATE CREDENTIAL tdeCredential2 WITH IDENTITY = 'testOCS', SECRET = 'ncipher'
FOR CRYPTOGRAPHIC PROVIDER nDSOP;
ALTER LOGIN tdeLogin2 ADD CREDENTIAL tdeCredential2;
GO
    
```



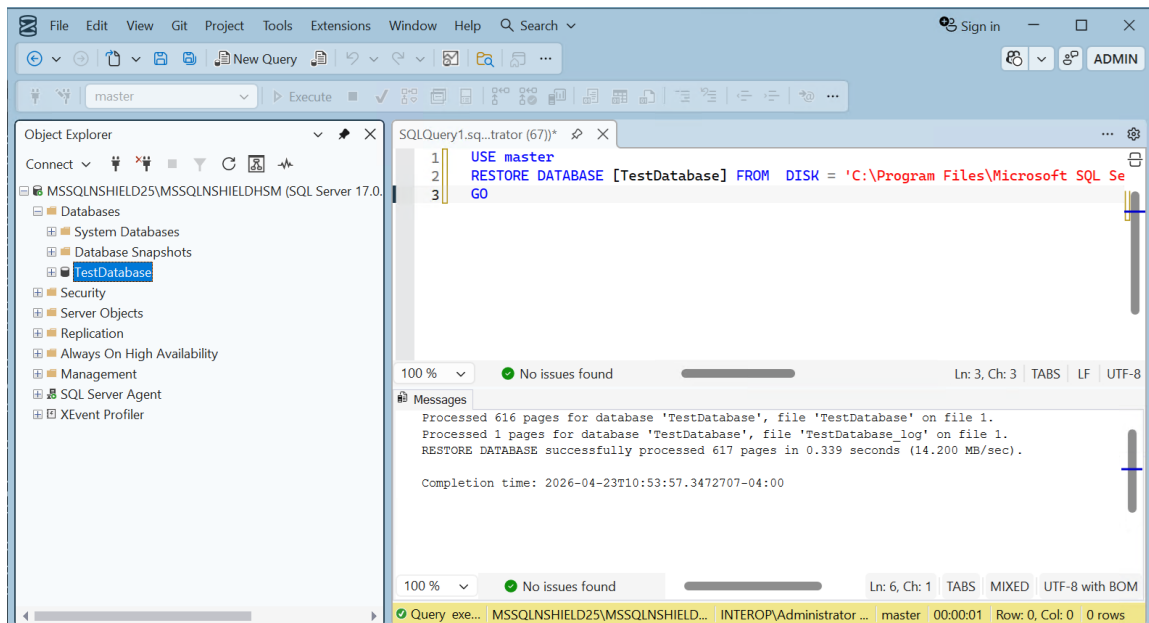
◦ Softcard:

```
USE master;
GO

-- tdeLogin2 and tdeCredential2
CREATE LOGIN tdeLogin2 FROM ASYMMETRIC KEY AsymTestWrappingKeyDatabase2;
CREATE CREDENTIAL tdeCredential2 WITH IDENTITY = 'testSC', SECRET = 'ncipher'
FOR CRYPTOGRAPHIC PROVIDER nDSOP;
ALTER LOGIN tdeLogin2 ADD CREDENTIAL tdeCredential2;
GO
```

9. Restore the database by running the following query:

```
USE master
RESTORE DATABASE [TestDatabase] FROM DISK = 'C:\Program Files\Microsoft SQL
Server\MSSQL17.MSSQLNLSHIELDHSM\MSSQL\Backup\TestDatabaseEncrypted.bak'
GO
```



10. Return to multiple user mode by running the following script:

```
USE master;
ALTER DATABASE TestDatabase SET
MULTI_USER;
GO
```

Chapter 8. Upgrade nDSOP from v1.0 to v2.1.0

8.1. Versions

From version	To version
v1.0	v2.1.0 (hotfix-Z166345-TAC1058)

Product configurations

Product	Version
Base OS	Windows Server 2016 Datacenter
SQL Server	Microsoft 2016 Enterprise with Service Pack 2
Microsoft SQL Server Management Studio	v18.8

Tested nShield hardware and software versions

HSM	Security World	Firmware	Netimage
Connect XC	12.60.11 with v2 Compatibility Package	12.50.11 (FIPS 140-2 Certified)	12.60.10

8.2. Procedure

A database called TestDatabase has been created and encrypted and will be used in this procedure.

1. [Back up the Security World.](#)
2. [Back up the database.](#)
3. Run the following query to verify the encryption state.

```

/***** Script for SelectTopNRRows command from SSMS *****/
SELECT DB_NAME(e.database_id) AS DatabaseName, e.database_id, e.encryption_state, CASE e.encryption_state
WHEN 0 THEN 'No database encryption key present, no encryption'
WHEN 1 THEN 'Unencrypted'
WHEN 2 THEN 'Encryption in progress'
WHEN 3 THEN 'Encrypted'
WHEN 4 THEN 'Key change in progress'

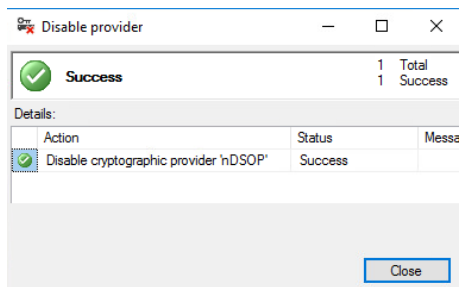
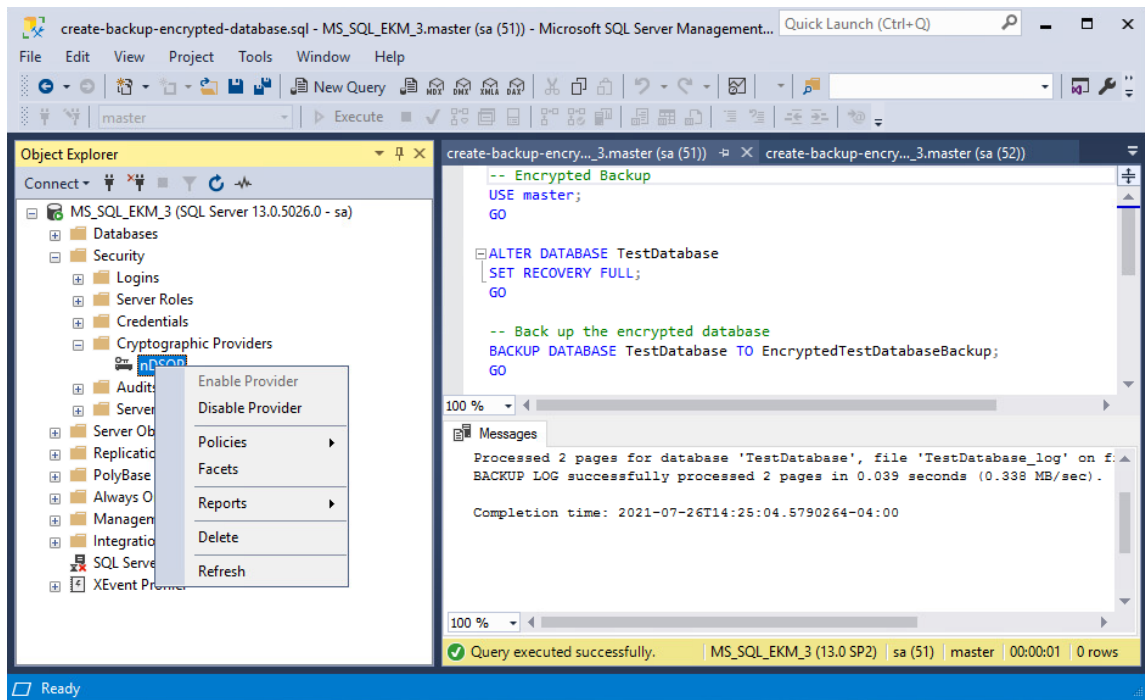
```

```

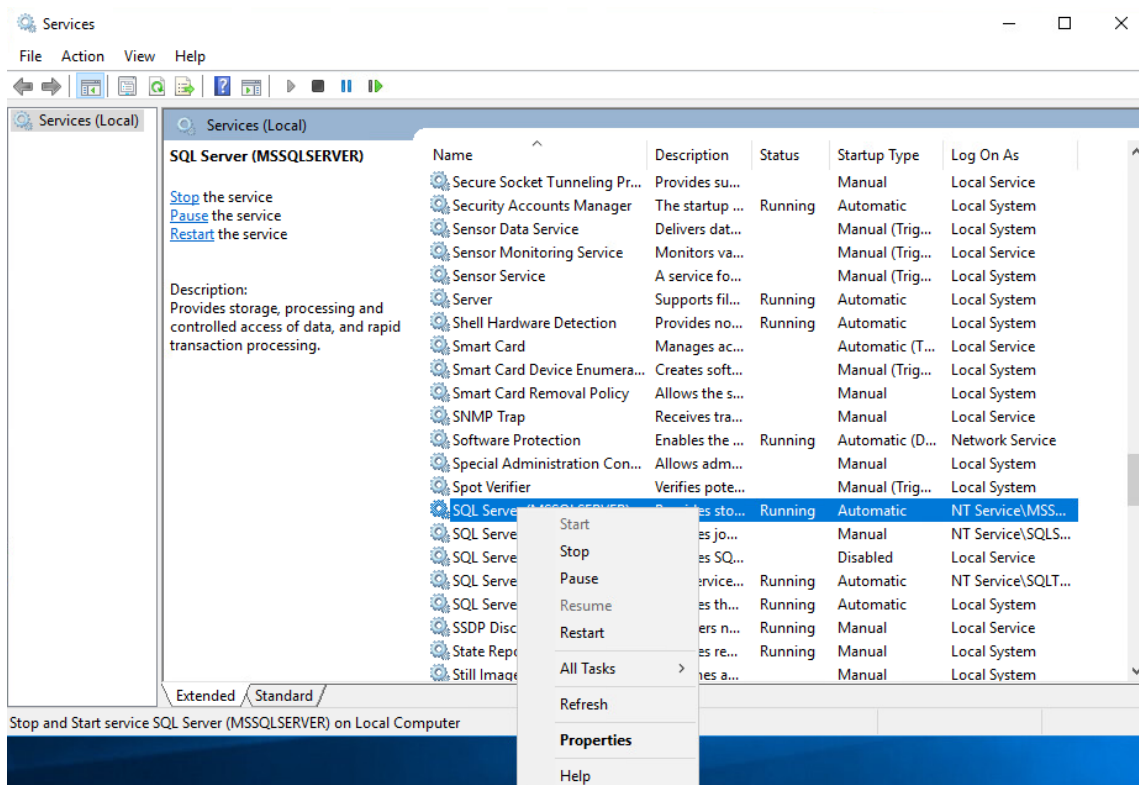
WHEN 5 THEN 'Decryption in progress'
END AS encryption_state_desc, c.name, e.percent_complete FROM sys.dm_database_encryption_keys AS e
LEFT JOIN master.sys.certificates AS c ON e.encryptor_thumbprint = c.thumbprint

```

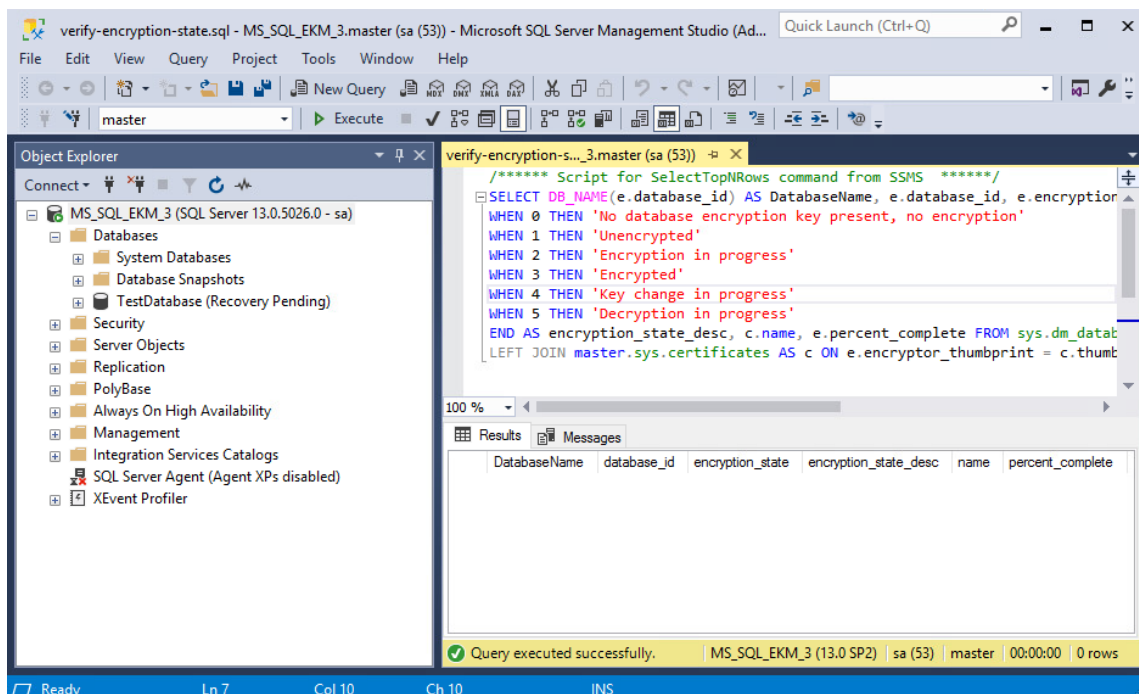
4. Disable the EKM provider. Select **Security Cryptographic Providers**. Right-click on the provider and select **Disable**.



5. Restart the SQL Server from the Windows MSSMS or services.



6. Wait for 60 seconds after the restart. Then check the database status. Notice **Recovery Pending** next to **TestDatabase**.



7. Un-install nDSOP v1.0 EKM provider using the Windows **Control Panel > Programs > Programs and Features**.

8. Install nDSOP v2.1.0 EKM provider by mounting the **.iso** file and double-clicking **setup**.

9. Insert the OCS in the HSM slot or TVD. No action is needed if you are using Softcard protection.
10. Retarget the keys by running the `sqladm_retarget_keys` command:

```
C:\Users\Administrator>nfkminfo -k

Key list - 2 keys
AppName pkcs11          Ident uc79dfaf7c3311d22d240a7257e5e760ede89fbc70-
56ac051fb249f91e641b065dc12fec8a9fea2419
AppName pkcs11          Ident uc79dfaf7c3311d22d240a7257e5e760ede89fbc70-
c88b06f02bdca29f2a98b9c9352daf9191fc8afd

C:\Users\Administrator>sqladm_retarget_keys --all
Found 2 keys to retarget
Retargetted: key_pkcs11_uc79dfaf7c3311d22d240a7257e5e760ede89fbc70-c88b06f02bdca29f2a98b9c9352daf9191fc8afd
Retargetted: key_pkcs11_uc79dfaf7c3311d22d240a7257e5e760ede89fbc70-56ac051fb249f91e641b065dc12fec8a9fea2419

C:\Users\Administrator>nfkminfo -k

Key list - 4 keys
AppName pkcs11          Ident uc79dfaf7c3311d22d240a7257e5e760ede89fbc70-
56ac051fb249f91e641b065dc12fec8a9fea2419
AppName pkcs11          Ident uc79dfaf7c3311d22d240a7257e5e760ede89fbc70-
c88b06f02bdca29f2a98b9c9352daf9191fc8afd
AppName simple          Ident sqladm-79dfaf7c3311d22d240a7257e5e760ede89fbc70-
b1844c5bb4eadbdb1166dccb64f4c5d59e4e408c
AppName simple          Ident sqladm-79dfaf7c3311d22d240a7257e5e760ede89fbc70-
fa9380a3e111df122b0e02dd37c1233da89b8e16
```

11. Open the `C:\ProgramData\nCipher\Key Management Data\local` folder. Move all `pkcs11` keys to another folder. Leave the `simple` keys in the current folder.

```
C:\ProgramData\nCipher\Key Management Data>mkdir local_pkcs11_keys

C:\ProgramData\nCipher\Key Management Data>move local\key_pkcs11* local_pkcs11_keys\
C:\ProgramData\nCipher\Key Management Data\local\key_pkcs11_uc79dfaf7c3311d22d240a7257e5e760ede89fbc70-
56ac051fb249f91e641b065dc12fec8a9fea2419
C:\ProgramData\nCipher\Key Management Data\local\key_pkcs11_uc79dfaf7c3311d22d240a7257e5e760ede89fbc70-
c88b06f02bdca29f2a98b9c9352daf9191fc8afd
    2 file(s) moved.

C:\ProgramData\nCipher\Key Management Data>nfkminfo -k

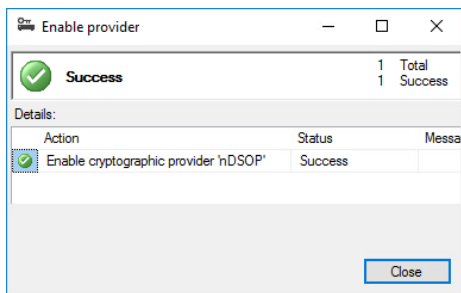
Key list - 2 keys
AppName simple          Ident sqladm-79dfaf7c3311d22d240a7257e5e760ede89fbc70-
b1844c5bb4eadbdb1166dccb64f4c5d59e4e408c
AppName simple          Ident sqladm-79dfaf7c3311d22d240a7257e5e760ede89fbc70-
fa9380a3e111df122b0e02dd37c1233da89b8e16
```

12. Set the new provider by running the following query:

```
--ChangeToNewProvider.sql

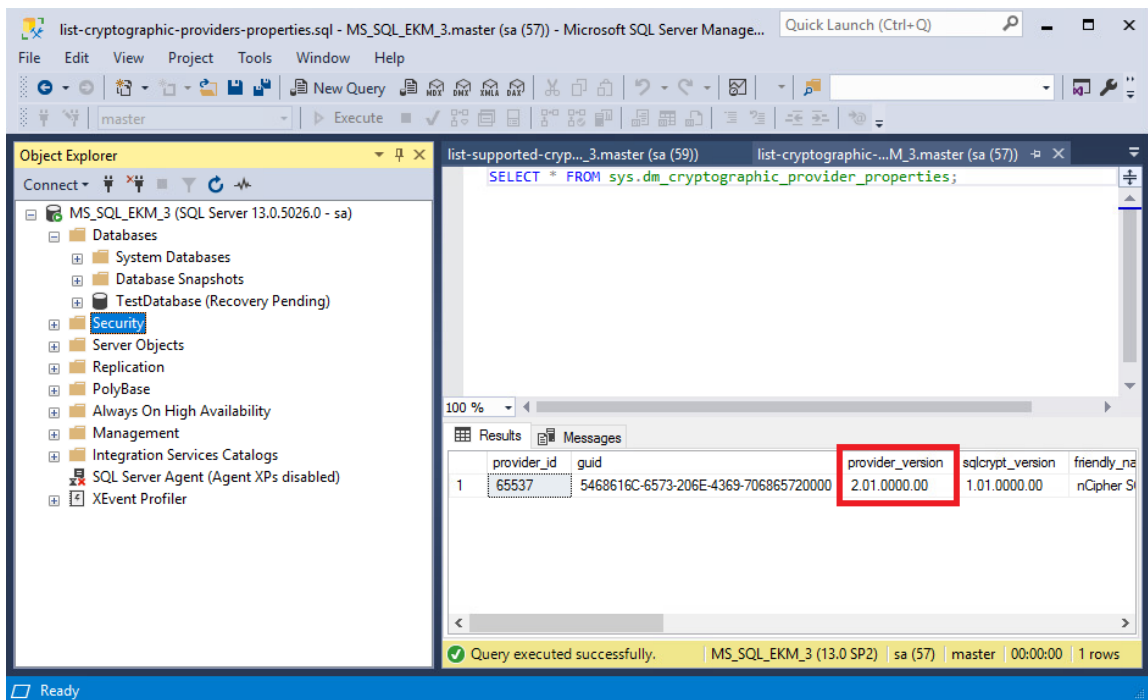
ALTER CRYPTOGRAPHIC PROVIDER nDSOP
FROM FILE = 'C:\Program Files\nCipher\nfast\bin\ncsqladm.dll';
GO
```

- 13. Enable the EKM provider. Select **Security > Cryptographic Providers**. Right-click the provider and select **Enable**.



- 14. Verify the new EKM provider version by running the following query. Notice the **provider_version**.

```
SELECT * FROM sys.dm_cryptographic_provider_properties;
```



- 15. Restart the SQL Server from the Windows MSSMS or services. Wait for 60 seconds after the restart.
- 16. Check and refresh database status. Notice the **Recovery Pending** message next to the TestDatabase goes away.
- 17. Verify the encryption state by running the following query. Notice the **encryption_state_desc** shown as **Encrypted**.

```
/***** Script for SelectTopNRRows command from SSMS *****/  
SELECT DB_NAME(e.database_id) AS DatabaseName, e.database_id, e.encrypted_state, CASE e.encrypted_state  
WHEN 0 THEN 'No database encryption key present, no encryption'  
WHEN 1 THEN 'Unencrypted'
```

```

WHEN 2 THEN 'Encryption in progress'
WHEN 3 THEN 'Encrypted'
WHEN 4 THEN 'Key change in progress'
WHEN 5 THEN 'Decryption in progress'
END AS encryption_state_desc, c.name, e.percent_complete FROM sys.dm_database_encryption_keys AS e
LEFT JOIN master.sys.certificates AS c ON e.encryptor_thumbprint = c.thumbprint

```

The screenshot shows the Microsoft SQL Server Management Studio interface. The Object Explorer on the left shows the server instance 'MS_SQL_EKM_3 (SQL Server 13.0.5026.0 - sa)'. The main window displays a query window with the following SQL script:

```

/***** Script for SelectTopNRows command from SSMS *****/
SELECT DB_NAME(e.database_id) AS DatabaseName, e.database_id, e.encryptor_thumbprint AS EncryptorThumbprint
WHEN 0 THEN 'No database encryption key present, no encryption'
WHEN 1 THEN 'Unencrypted'
WHEN 2 THEN 'Encryption in progress'
WHEN 3 THEN 'Encrypted'
WHEN 4 THEN 'Key change in progress'
WHEN 5 THEN 'Decryption in progress'
END AS encryption_state_desc, c.name, e.percent_complete FROM sys.dm_database_encryption_keys AS e
LEFT JOIN master.sys.certificates AS c ON e.encryptor_thumbprint = c.thumbprint

```

The Results pane shows the following data:

DatabaseName	database_id	encryption_state	encryption_state_desc	name	percent_complete
tempdb	2	3	Encrypted	NULL	0
TestDatabase	5	3	Encrypted	NULL	0

The status bar at the bottom indicates: Query executed successfully. MS_SQL_EKM_3 (13.0 SP2) | sa (52) | master | 00:00:00 | 2 rows

Chapter 9. Upgrade nDSOP from v2.1.0 to v2.1.1

9.1. Versions

From version	To version
v2.1.0 (hotfix-Z166345-TAC1058)	v2.1.1

Product configurations

Product	Version
Base OS	Windows Server 2022 Datacenter
SQL Server	Microsoft SQL Server Enterprise 2022
Microsoft SQL Server Management Studio	v20.2.1

Tested nShield hardware and software versions

HSM	Security World	Firmware	Netimage
nShield 5c	13.3.2	13.4.5 (FIPS 140-3 certified)	13.6.7

9.2. Procedure

A database called TestDatabase has been created and encrypted and will be used in this procedure.

1. [Back up the Security World.](#)
2. [Back up the database.](#)
3. Run the following query to verify the encryption state.

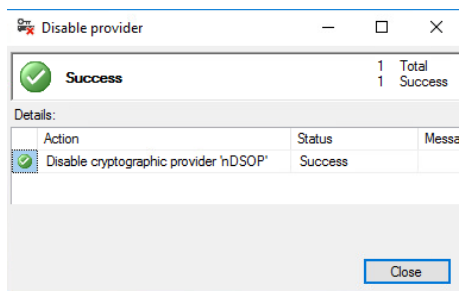
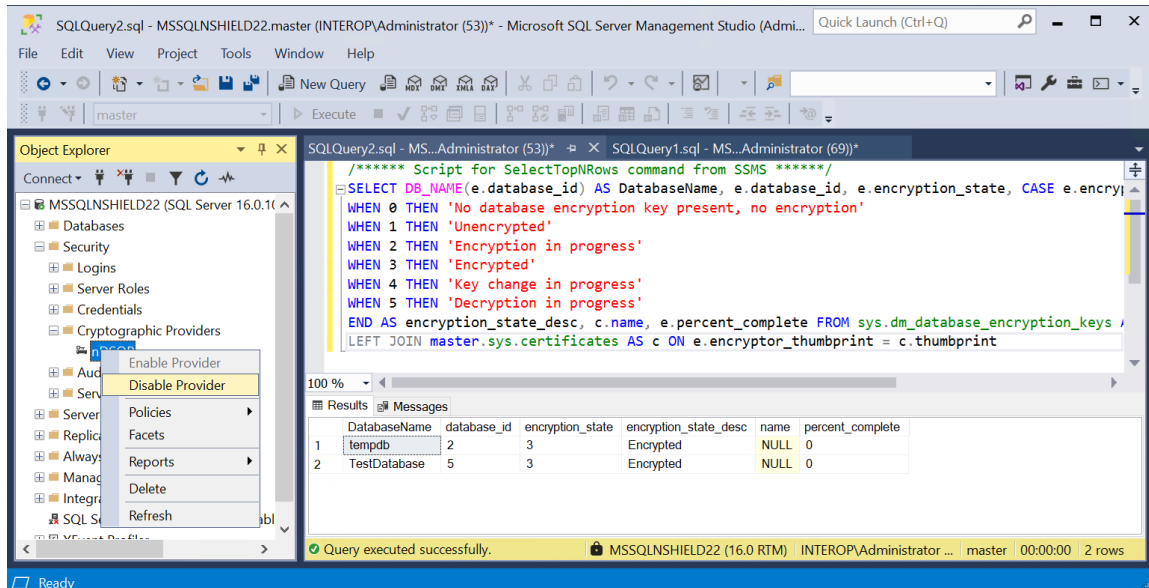
```

/***** Script for SelectTopNRows command from SSMS *****/
SELECT DB_NAME(e.database_id) AS DatabaseName, e.database_id, e.encryption_state, CASE e.encryption_state
WHEN 0 THEN 'No database encryption key present, no encryption'
WHEN 1 THEN 'Unencrypted'
WHEN 2 THEN 'Encryption in progress'
WHEN 3 THEN 'Encrypted'
WHEN 4 THEN 'Key change in progress'
WHEN 5 THEN 'Decryption in progress'
END AS encryption_state_desc, c.name, e.percent_complete FROM sys.dm_database_encryption_keys AS e

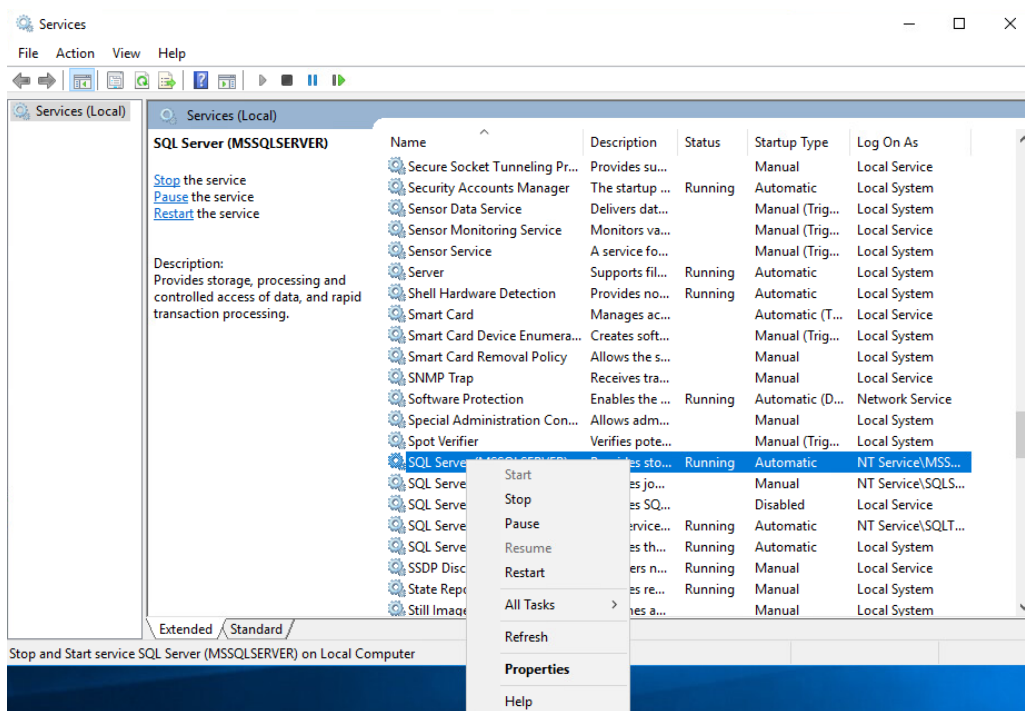
```

```
LEFT JOIN master.sys.certificates AS c ON e.encryptor_thumbprint = c.thumbprint
```

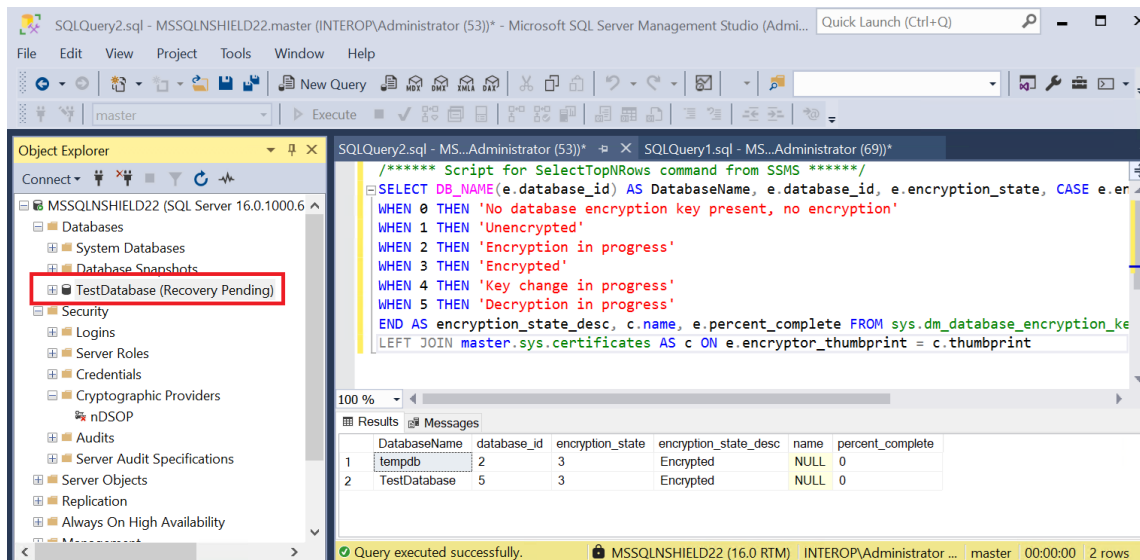
4. Disable the EKM provider. Select **Security Cryptographic Providers**. Right-click on the provider and select **Disable**.



5. Restart the SQL Server from the Windows MSSMS or services.



6. Wait for 60 seconds after the restart. Then check the database status. Notice **Recovery Pending** next to **TestDatabase**.



7. Un-install nDSOP v2.1.0 EKM provider using the Windows **Control Panel > Programs > Programs and Features**.

8. Install nDSOP v2.1.1 EKM provider by mounting the **.iso** file and double-clicking **setup**.

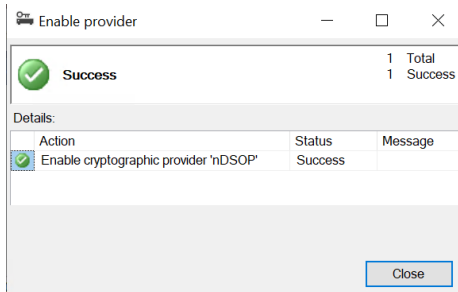
9. Insert the OCS in the HSM slot or TVD. No action is needed if you are using Softcard protection.

10. Set the new provider by running the following query:

```
--ChangeToNewProvider.sql
```

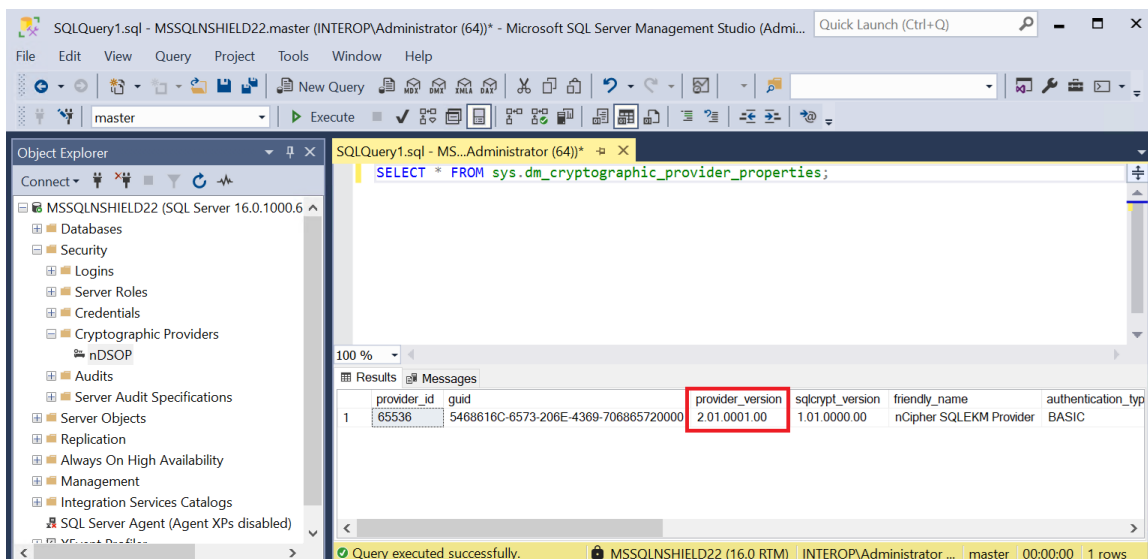
```
ALTER CRYPTOGRAPHIC PROVIDER nDSOP
FROM FILE = 'C:\Program Files\nCipher\ncfast\bin\ncsqllekm.dll';
GO
```

11. Enable the EKM provider. Select **Security > Cryptographic Providers**. Right-click the provider and select **Enable**.



12. Verify the new EKM provider version by running the following query. Notice the **provider_version**.

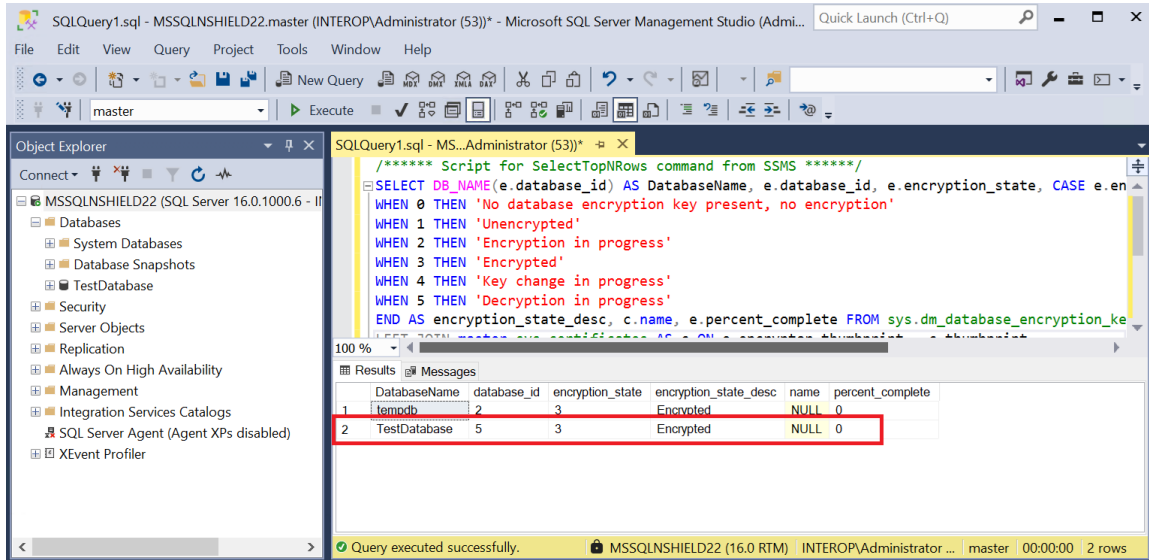
```
SELECT * FROM sys.dm_cryptographic_provider_properties;
```



13. Restart the SQL Server from the Windows MSSMS or services. Wait for 60 seconds after the restart.
14. Check and refresh database status. Notice the **Recovery Pending** message next to the TestDatabase goes away.
15. Verify the encryption state by running the following query. Notice the **encryption_state_desc** shown as **Encrypted**.

```
/****** Script for SelectTopNRows command from SSMS *****/
SELECT DB_NAME(e.database_id) AS DatabaseName, e.database_id, e.encrypted_state, CASE e.encrypted_state
WHEN 0 THEN 'No database encryption key present, no encryption'
```

```
WHEN 1 THEN 'Unencrypted'  
WHEN 2 THEN 'Encryption in progress'  
WHEN 3 THEN 'Encrypted'  
WHEN 4 THEN 'Key change in progress'  
WHEN 5 THEN 'Decryption in progress'  
END AS encryption_state_desc, c.name, e.percent_complete FROM sys.dm_database_encryption_keys AS e  
LEFT JOIN master.sys.certificates AS c ON e.encryptor_thumbprint = c.thumbprint
```



Chapter 10. Troubleshoot

10.1. Microsoft SQL Server, Error: 15209 while rotating the TDEKEK

1. Restart the database.
2. Try again to rotate the TDEKEK.

Chapter 11. Additional resources and related products

11.1. nShield HSMs

11.2. nShield as a Service

11.3. nShield Database Option Pack

11.4. Entrust products

11.5. nShield product documentation