# Microsoft SQL Server Always Encrypted

SQL Server 2016 / 2017 / 2019

## Integration Guide

# CryptoServer

SecurityServer 4.45.1

utimaco®

## Imprint


| | |
|---|---|
| Copyright 2026 | Utimaco IS GmbH<br>Krefelder Straße 220<br>52070 Aachen<br>Germany |
| Phone | AMERICAS +1-844-UTIMACO (+1 844-884-6226)<br>EMEA +49 800-627-3081<br>APAC +81 800-919-1301 |
| Internet | https://support.hsm.utimaco.com/ |
| e-mail | support@utimaco.com |
| Document Version | 1.0.0 |
| Date | 2026-03-23 |
| Status | PUBLISHED |
| Document No. | IG-2026-0018 |

# Table of Contents

# 1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle.

All Utimaco SecurityServer product documentation is available from Utimaco's website at https://utimaco.com/.

## 1.1 About This Guide

This guide describes how to enable HSM integration with Microsoft SQL Server Always Encrypted. For more detailed information regarding Microsoft SQL Server and Always Encrypted, please refer to the documentation provided by Microsoft.

### 1.1.1 Target Audience for This Guide

This guide is intended for administrators of Microsoft SQL Server and of Utimaco HSMs.

### 1.1.2 Document Conventions

The following conventions are used in this guide:

| Convention | Use | Example |
|---|---|---|
| Bold | Items of the Graphical User Interface (GUI), e.g., menu options | Press **OK** |
| `Monospaced` | Code that is given for explanation or as an example, file paths | `chsm-create` |
| *Italic* | References and important terms | See *Sample Chapter* in the *CryptoServer - Sample Manual* |

Table 1: Document Conventions

We use special icons to highlight the most important notes and information.

Here, you find important safety information that should be followed.

Here, you find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

### 1.1.3 Abbreviations

The following abbreviations are used in this guide:

| Abbreviation | Meaning |
|---|---|
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| CA | Certificate Authority |
| CEK | Column Encryption Key |
| CMK | Column Master Key |
| CNG | Cryptography API Next Generation |
| CSAR | Cloud Service Architecture |

| Abbreviation | Meaning |
|---|---|
| CSP | Cryptographic Service Provider |
| DBA | Database Administration |
| DES | Data Encryption Standard |
| FIPS | Federal Information Processing Standards |
| GUI | Graphical User Interface |
| HSM | Hardware Security Module |
| MBK | Master Backup Key |
| RSA | Rivest-Shamir-Adleman |
| SQL | Structured Query Language |
| TDE | Transparent Data Encryption |

Table 2: Abbreviations

# 2 Overview

## 2.1 Microsoft SQL Server Always Encrypted

Always Encrypted is a feature in Windows SQL Server 2019 designed to protect sensitive data both at rest and in flight between an on-premises client application server and Azure or SQL Server database(s).

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 Transparent Data Encryption; however, TDE is NOT a requisite for implementing Always Encrypted.

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

- A Column Master Key – The CMK, is an asymmetric RSA encryption key of size 2048 bits
- One or more Column Encryption Key(s) - A CEK, is a symmetric AES key of size 256 bits

The CEK is responsible for encrypting the database column data while the CMK is protected by the Utimaco HSM and is responsible for wrapping (encrypting) the CEK. The Column Master Key is generated using the Utimaco CNG provider via the HSM and stored in an encrypted state within the HSM.

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 encryptions, 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, example 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.

## 2.2 Utimaco SecurityServer HSM

SecurityServer is a hardware security module developed by Utimaco IS GmbH. SecurityServer is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

# 3 Integration Requirements and Prerequisites

Ensure the system environment you will be using meets the following hardware and software requirements.

## 3.1 Tested Versions

The integrations that have been successfully tested with different versions of Microsoft Windows Server, Microsoft SQL Server, Utimaco SecurityServer product and Utimaco HSMs are shown in the following configurations below:

| Microsoft Windows Server | Microsoft SQL Server | Utimaco Security Server Version | Utimaco HSM |
|---|---|---|---|
| Windows Server 2019<br><br>Windows Server 2016 | SQL Server 2019<br><br>SQL Server 2017<br><br>SQL Server 2016 | SecurityServer 4.45.1 or higher | CryptoServer<br><br>CSe-Series/Se-Series<br><br>u.trust Anchor Se40k and<br><br>u.trust Anchor CSAR |

Table 3: List of Tested Versions

For SecurityServer 4.50 onwards, you must download 32-bit Utimaco CNG Library from the support portal and copy it under C:\Windows\SysWOW64 post installation of SecurityServer software.

## 3.2 Software Requirements

| Software | Software Requirements |
|---|---|
| Java | Version 8, Update 271 or higher |

| Software | Software Requirements |
|---|---|
| HSM Interfaces | SecurityServer CNG Provider |

Table 4: List of Software Requirements

## 3.3 Hardware Requirements

| Hardware | Hardware Requirements |
|---|---|
| Utimaco LAN HSM | CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.45.1 or higher<br><br>u.trust Anchor Se40k and u.trust Anchor CSAR |
| Utimaco PCI-e HSM | CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.45.1 or higher<br><br>u.trust Anchor Se40k and u.trust Anchor CSAR |

Table 5: List of Hardware Requirements

Setup an account on the Utimaco support portal and request download access at the following URL. https://support.hsm.utimaco.com

## 3.4 Prerequisites

Before you begin, please ensure that you have:

- Set up and configured SecurityServer. Refer to the SecurityServer documentation to set up the HSM.
- Created and stored the MBK onto each HSM. Refer to the SecurityServer documentation to set up the MBK.
- Replaced the SecurityServer Default Admin with a new admin user.
- Installed and set up the operating system listed in Tested Versions.

- Installed and set up the SQL Server listed in Tested Versions.
- Installed and set up SQL Server Management Studio.
- Installed and set up the SecurityServer version listed in Tested Versions with the SecurityServer CNG provider.
- Set up a cryptographic user on that SecurityServer.

You should also be familiar with SQL statements, as this guide makes intensive use of them.

After the successful SecurityServer setup, you should find these files on your system for use with the SecurityServer CNG provider:

`cs2cng.dll and cs2csp.dll`

The former is the provider library that will be loaded into SQL Server, and the latter is required by it. These files are located in C:\Windows\SysWOW64 which must be in system PATH.

`cs_cng.cfg`

This file contains the parameters that the SecurityServer CNG provider will use when communicating with the HSM. Please see the next sections for details.

# 4 Software Download and Installation

This section describes the process of installing Utimaco HSM software with the CNG provider for Microsoft SQL Server.

## 4.1 Download Utimaco Software

If you have not already done so, please create and request an Utimaco Support Portal Account. This will allow you to download the software components needed for this installation.

If you have purchased an HSM from Utimaco, locate the included product bundle, which contains the Windows software packages.

Install the latest version of the SecurityServer software as described in the SecurityServer Manual for the HSM. We recommend that you uninstall any SecurityServer software before installing the new software.

# 5 Configuring the CNG Provider

## 5.1 Introduction of the CSP

A CSP (Cryptographic Service Provider) is a general-purpose cryptography standard developed by Microsoft. On one side it defines a cryptographic interface to be used by applications (CryptoAPI). On the other side it defines an interface to be used by manufacturers in order to integrate their cryptographic hardware.

A CNG (Cryptography API Next Generation) is the second-generation cryptographic interface developed by Microsoft. It offers updated cryptographic algorithms and is intended for a long-term replacement of CSP.

## 5.2 Installation

1. The initial task is to run the SecurityServer install wizard to install administration tools, documentation and the CSP/CNG interface. The SecurityServer Setup install wizard can be found on the supplied product CD.

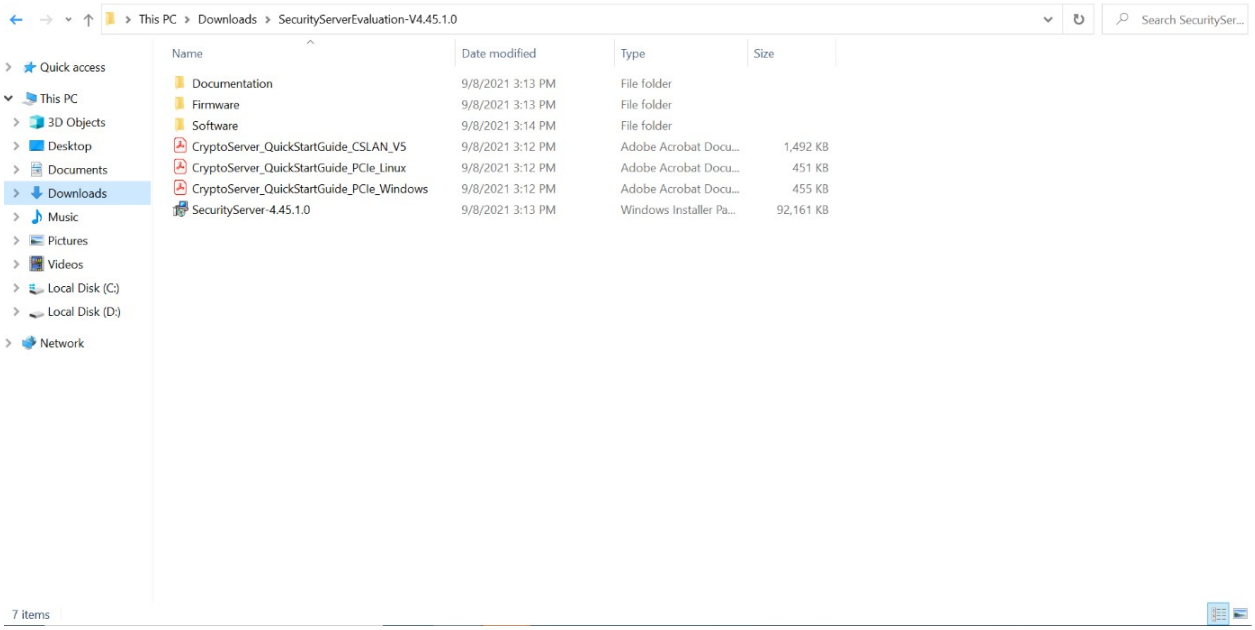


Figure 1 : SecurityServer Setup Installer

2. On the first screen you will be able to choose where SecurityServer should be installed.

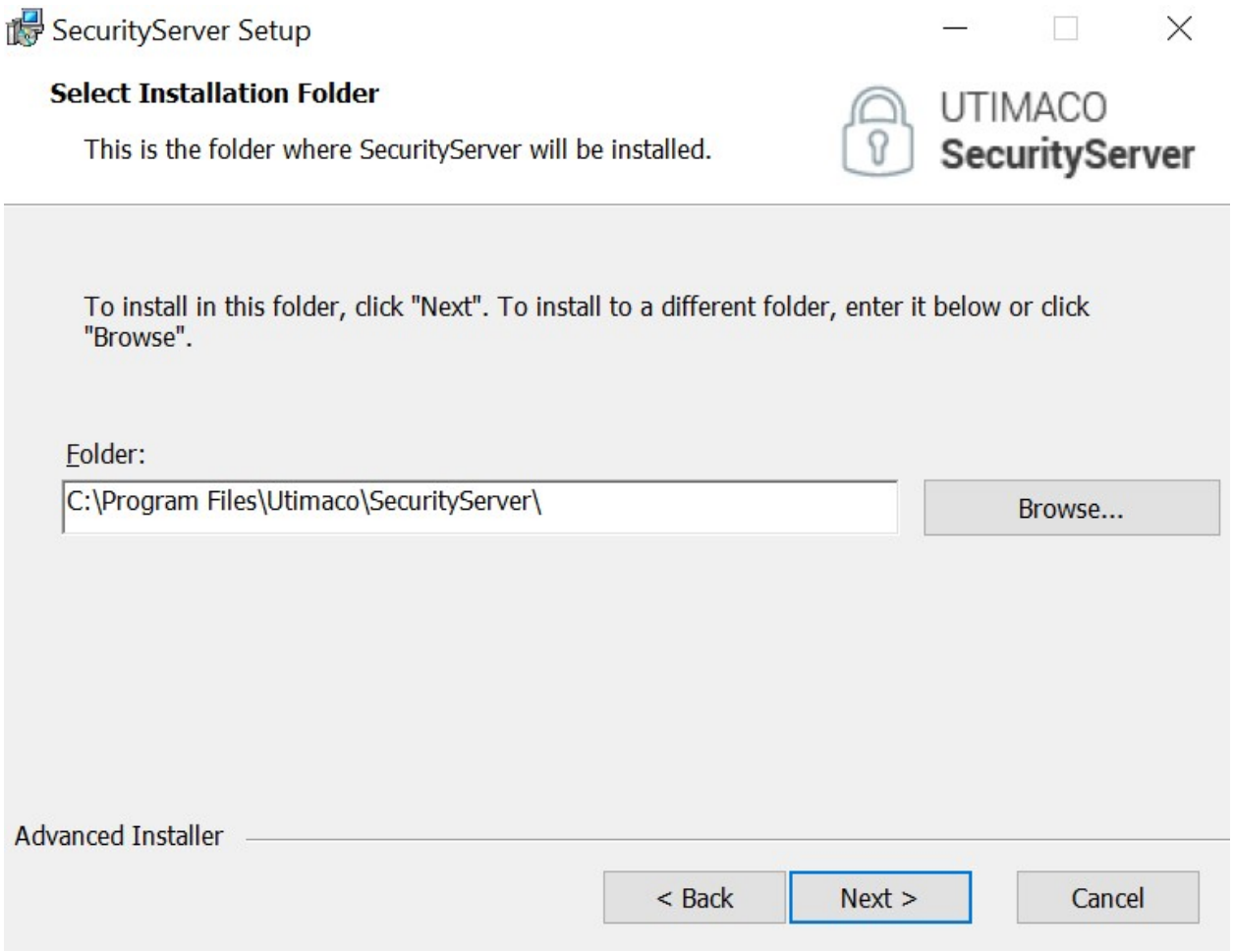


Figure 2 : SecurityServer Destination Location

3. Once you clicked "Next", Select the Custom Setup Type.

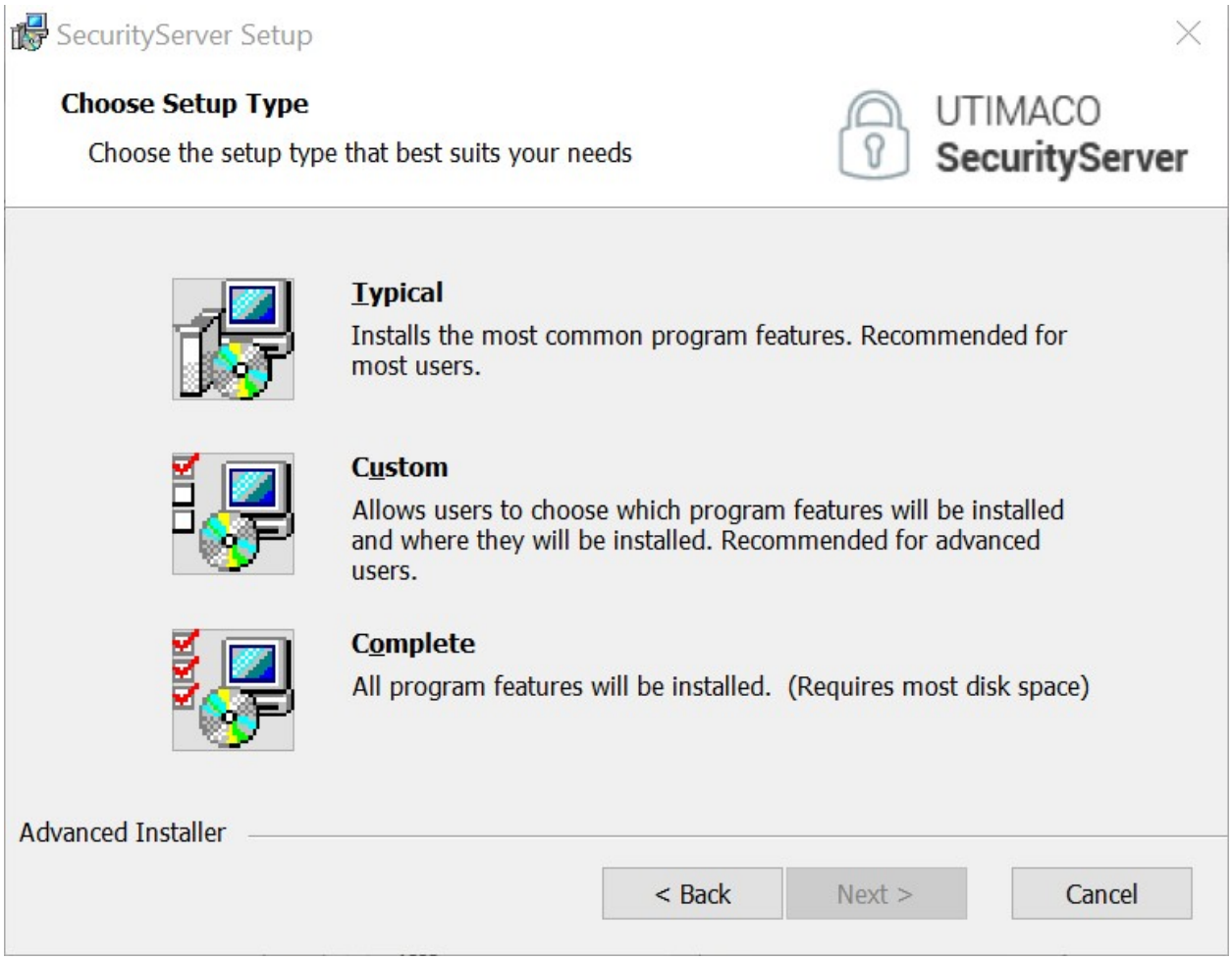


Figure 3 : Setup Window

4. The user can choose which components should be installed. SecurityServer Administration Tools and Documentation are recommended. The CSP/CNG interface is required.

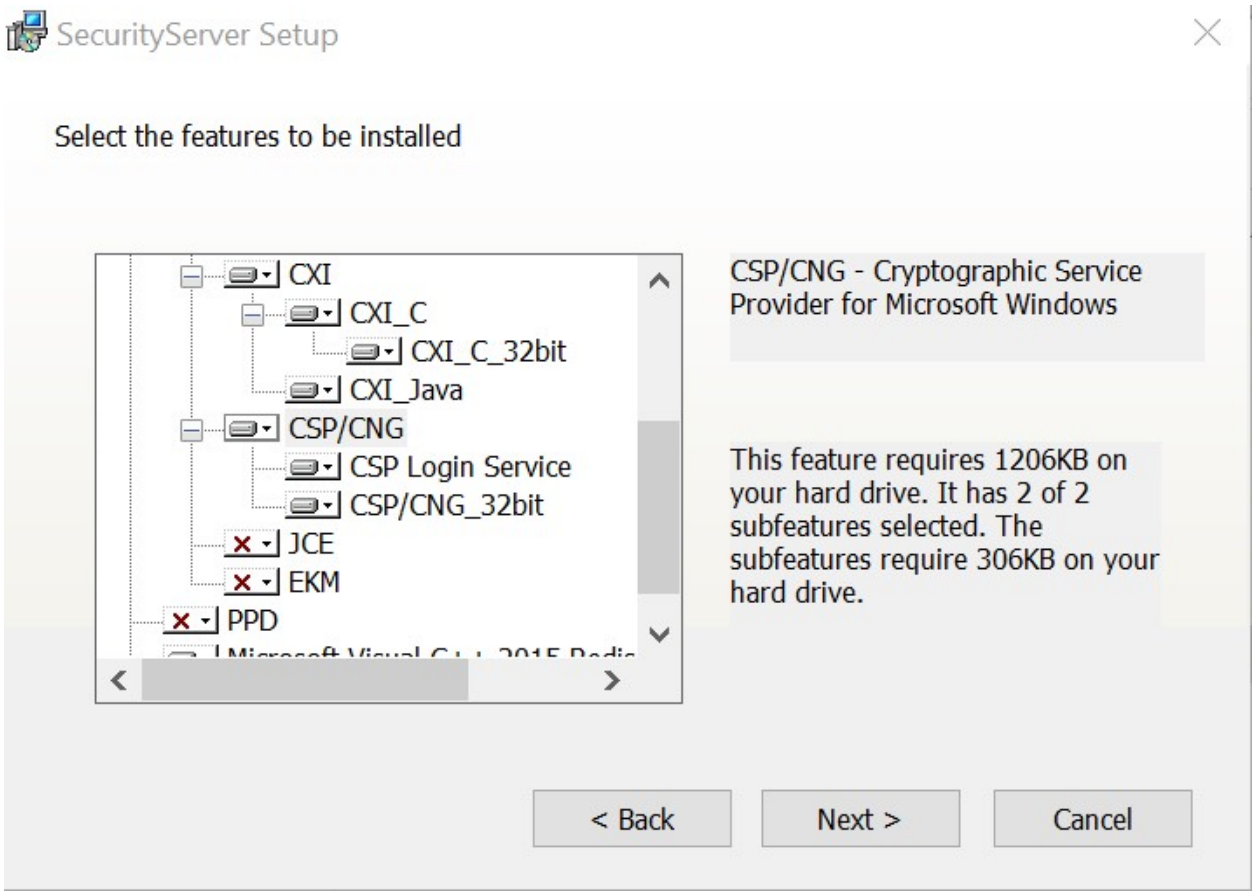


Figure 4 : Setup Window

5. Click Next for other one window.

Once the installation is done, you will see a screen stating the successful installation.

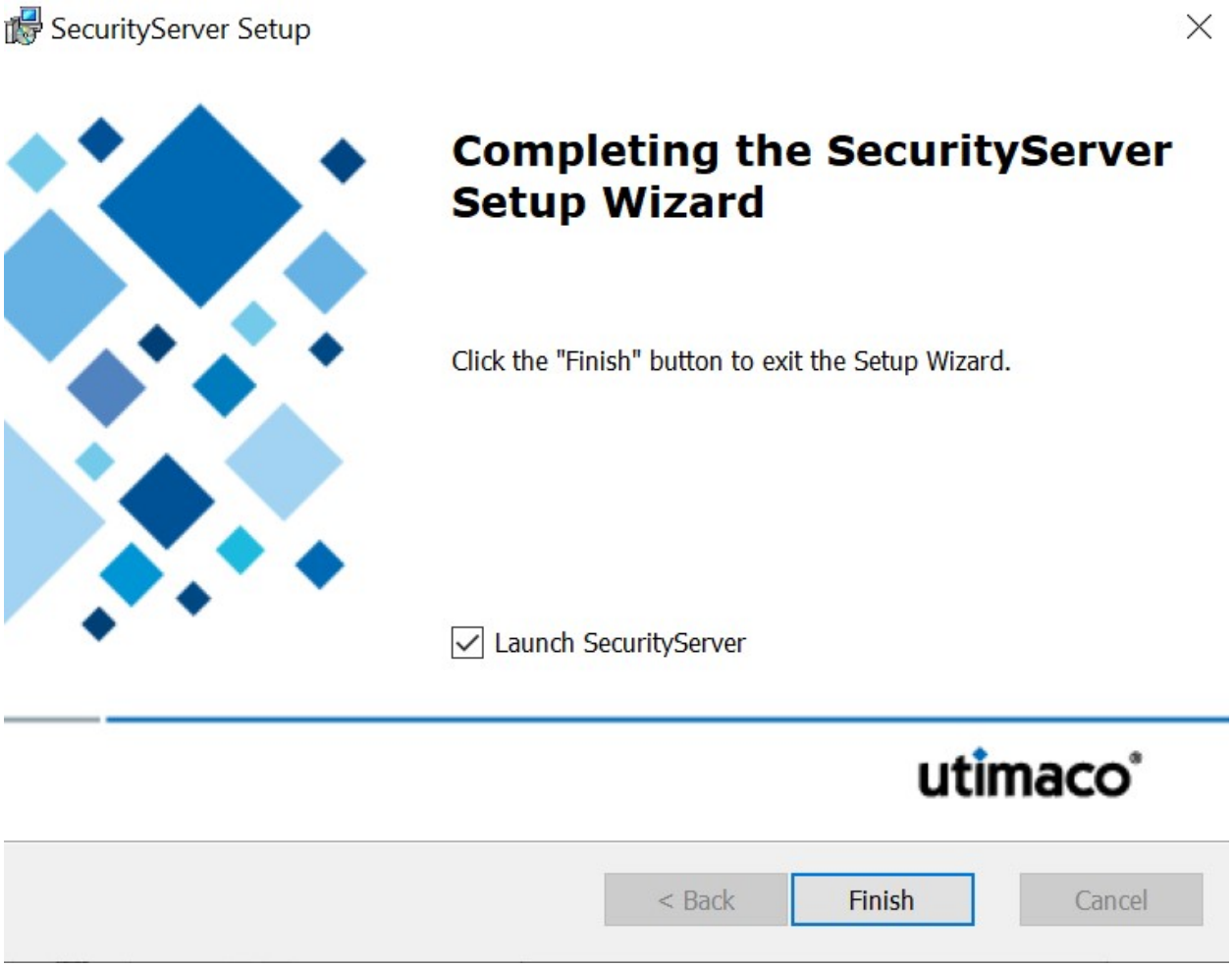


Figure 5 : Desktop Shortcut

For SecurityServer 4.50 onwards, you must download 32-bit Utimaco CNG Library from the support portal and copy it under C:\Windows\SysWOW64 post installation of SecurityServer software.

## 5.3 Creating a Cryptographic User

Create a user for performing cryptographic operation with permission level 00000002 along with a CXI_GROUP with CAT Tool.

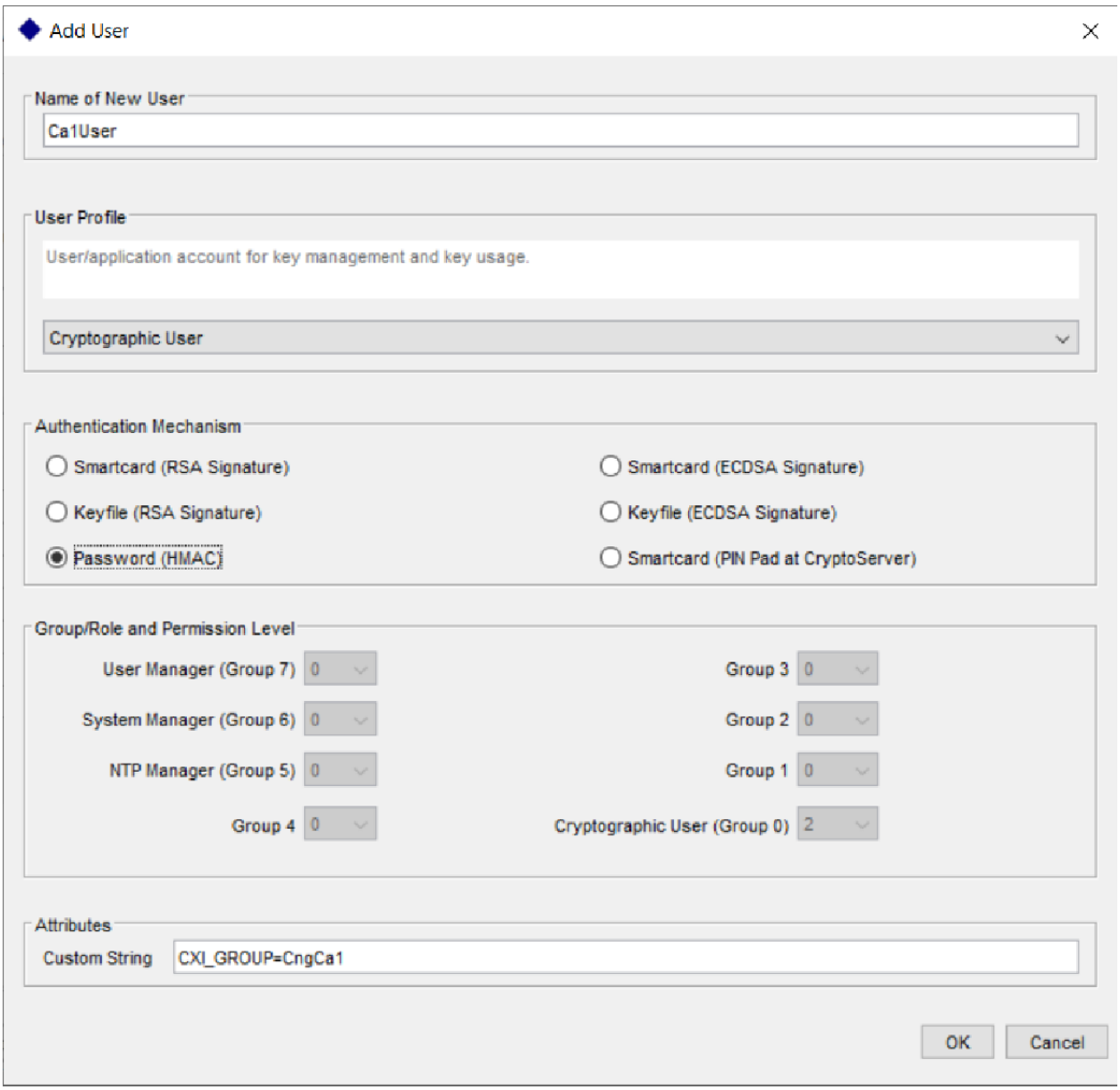


Figure 6 : Creating a Crypto User

Based on the user you can use Password, Smart Card or KeyFile.

## 5.4 Setting up the CNG Provider

The CS_CNG_CFG environment variable contains the path and name of the configuration file. By default, it is located at C:\ProgramData\Utimaco\CNG\cs_cng.cfg.

1. Open the cs_cng.cfg file with an appropriate text editor.

For more advanced configuration, refer to [CspCng].

›_ Console

```
> notepad %CS_CNG_CFG%
```

2. For this installation set the path to the log file and set the log level to "TRACE".

cs_cng.cfg file

```
# Path to the logfile (name of logfile is attached by the API)
Logpath = C:\ProgramData\Utimaco\CNG\log
# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 1
```

3. Set the IP address of the HSM.

cs_cng.cfg file

```
# default device and fallback devices
Device = 10.44.223.141
```

4. Set the Login. In this case, the name of the Cryptographic User is "Ca1User" with an HMAC password "Utimaco".

cs_cng.cfg file

```
# Login = username,HMACPwd=password
Login = Ca1User,HMACPwd=Utimaco
```

5. The Configuration File used in this document.

cs_cng.cfg file

```
# Maximum size of the logfile in bytes
Logsize = 8mb

# Keys are stored in an external or internal database
KeysExternal = false

# Path to the external keystore. Directory must be given, not file!
#KeyStore = C:\ProgramData\Utimaco\CNG\keys

# Export policy for newly created keys: 0=allow all, 1=deny plain export
(standard), 2=deny all
ExportPolicy = 1

# Prevents expiring session after inactivity of 15 minutes
KeepAlive = true

# Timeout of the open connection command in ms
ConnectionTimeout = 3000

# Timeout of command execution in ms
CommandTimeout = 60000

# CXI group for all keys. The user has to have access to this group.
Group = CngCa1
```

### 5.4.1 Testing Connection

1. To enumerate providers, use the following command:

›_ Console

```
> cngtool EnumProvider
Microsoft Key Protection Provider
Microsoft Passport Key Storage 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
Utimaco CryptoServer Key Storage Provider
```

2. To get the provider information, use the following command:

›_ Console

```
>cngtool ProviderInfo
------------------------------------------------------------
Provider : Utimaco CryptoServer Key Storage Provider
Device : 10.44.223.140
Group : CngCa1
Mode : Internal Key Storage

------------------------------------------------------------
Name : Utimaco CryptoServer Key Storage Provider
Version : 0x02030100
Impl.-Type : 0x00000011
MaxNameLength : 0x00000104
Device : 10.44.223.140
Group : CngCa1
Mode : Internal Key Storage
```

3. To get the list of all keys, use the following command (at first this list should be empty):

›_ Console

```
>cngtool ListKeys
------------------------------------------------------------
Provider : Utimaco CryptoServer Key Storage Provider
Device : 10.44.223.140
Group : CngCa1
Mode : Internal Key Storage
------------------------------------------------------------
Index AlgId Size Group Name Spec
------------------------------------------------------------------------
```

# 6 Always Encrypted

## 6.1 Creating the Always Encrypted Column Master Key

1. Open the Microsoft SQL Server Management Studio and then create a utimacoDB database.

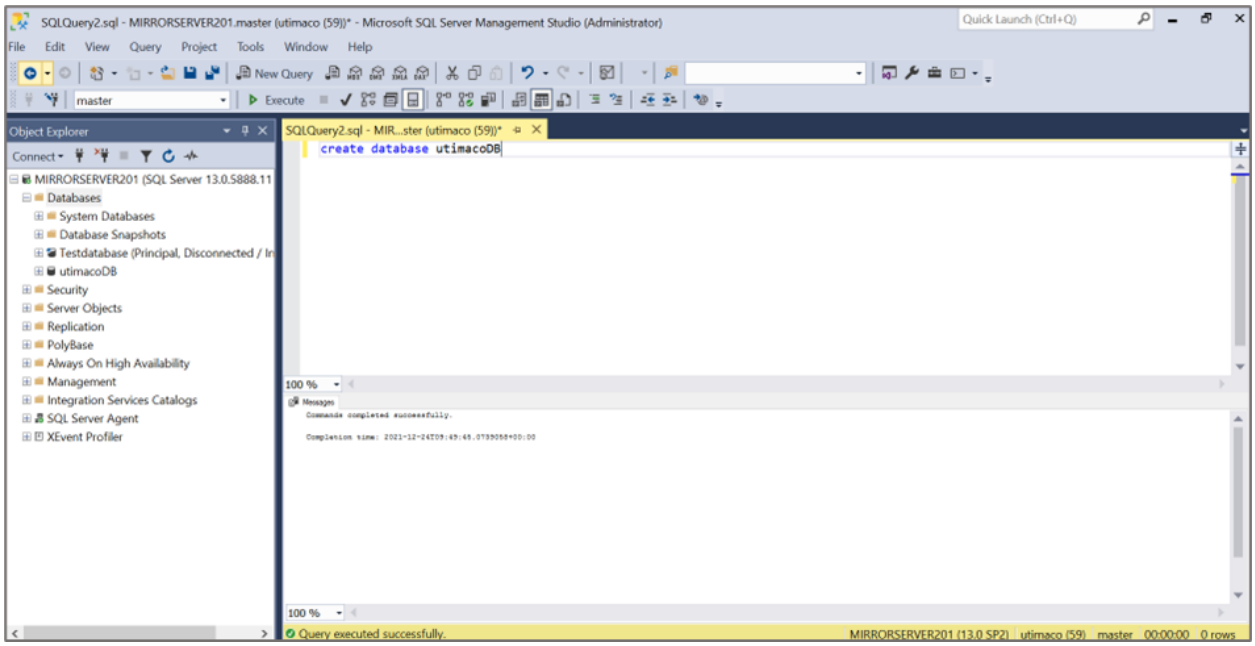


Figure 7 : Creating Database window

2. Create a table name as `Vehicle`.

SQL Statement

```
USE utimacoDB
CREATE TABLE [dbo].[Vehicle] (
ID int NOT NULL,
VehicleName varchar (255) NOT NULL,
VehicleNumber varchar (255) NOT NULL,
Dates varchar(255) NOT NULL
)
GO
```

3. Insert values of respective columns.

SQL Statement

```
INSERT INTO Vehicle VALUES ('One', ‘Alan’, ‘MH 12 FG 4767’,’30 Oct 2021’ );
INSERT INTO Vehicle VALUES (‘Two’, ‘James’, ‘MH 43 WD 7837’,’12 April 2021’);
INSERT INTO Vehicle VALUES ('Three', ‘Mark’, ‘MH 22 GI 8963’,’7 May 2021’ );
```

4. To List the database table content use below query.

SQL Statement

```
Select * from Vehicle
```

5. Create a new key using cngtool command as below.

›_ Console

```
cngtool Name=<Key_Name> CreateKey=<Algorithm,KeySize>
```

6. The user will get this output after executing the above command.

›_ Console

```
>cngtool Name=utimacoKey CreateKey=RSA,2048
-------------------------------------------------------------
Provider: Utimaco CryptoServer  Key Storage Provider
Device : 10.44.223.140
Group : CngCa1
Mode : Internal Key Storage
-------------------------------------------------------------
C:\Users>cngtool ListKeys
-------------------------------------------------------------
Provider : Utimaco CryptoServer  Key Storage Provider
Device : 10.44.223.140
Group : CngCa1
Mode : Internal Key Storage
-------------------------------------------------------------------------
Index     AlgId          Size         Group         Name           Spec
-------------------------------------------------------------------------
1         RSA            2048         CngCa1        utimacoKey       0
```

7. Using Object Explorer, select the Security directory under the desired Database (in the example below this can be seen as “utimacoDB”). 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… the “New Column Master Key” dialogue box will open.

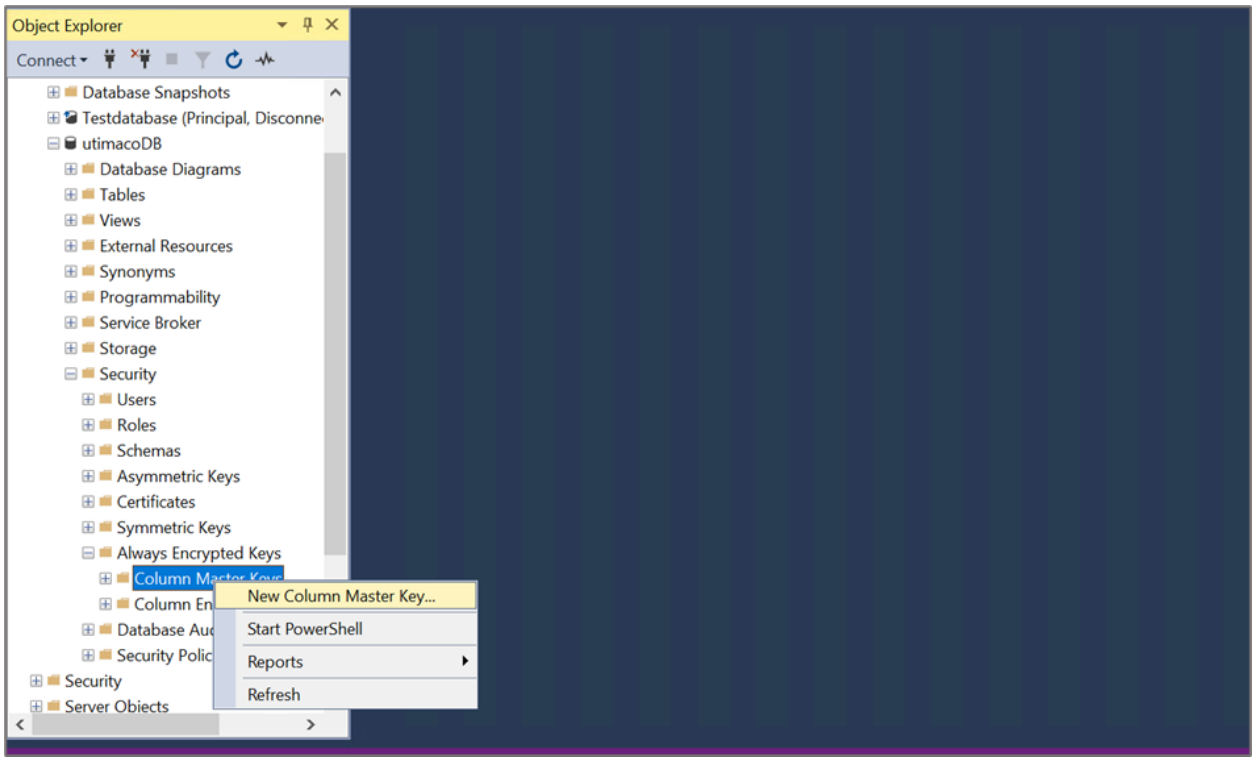


Figure 8 : New Column Master Key

8. Enter the name of the Master Key, e.g., Utimaco-CMK.

9. Select Key store as Key Storage Provider CNG, in this case for the current user or local machine. Select a provider as "Utimaco CryptoServer Key Storage Provider" then click OK.

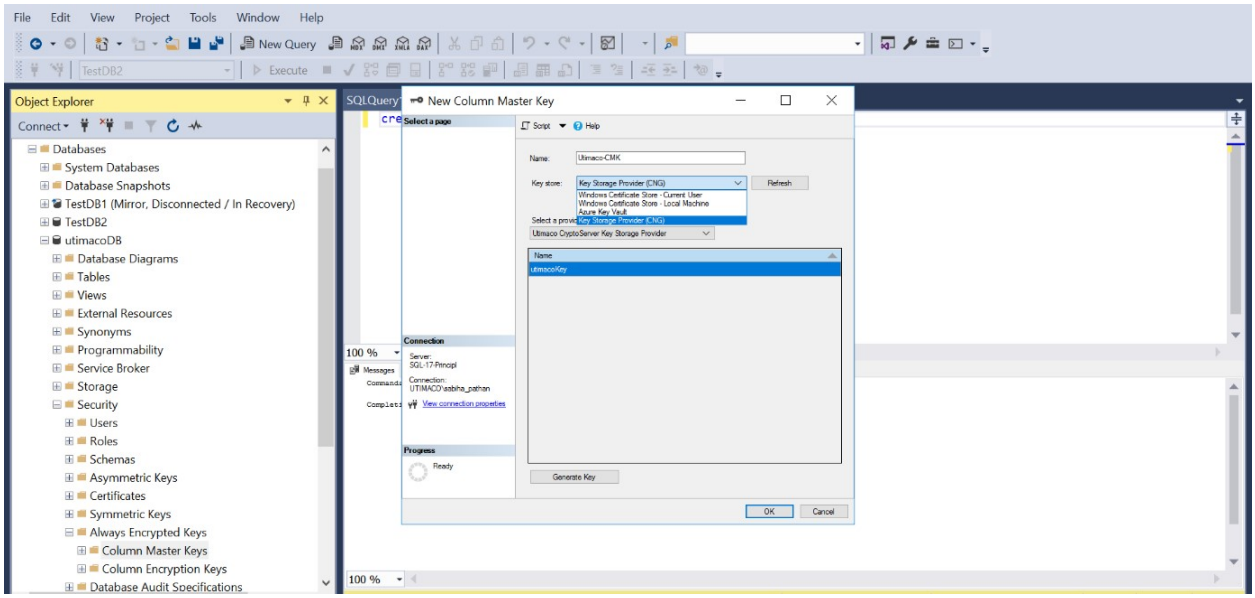


Figure 9 : Creating New Column Master Key window

10. 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).

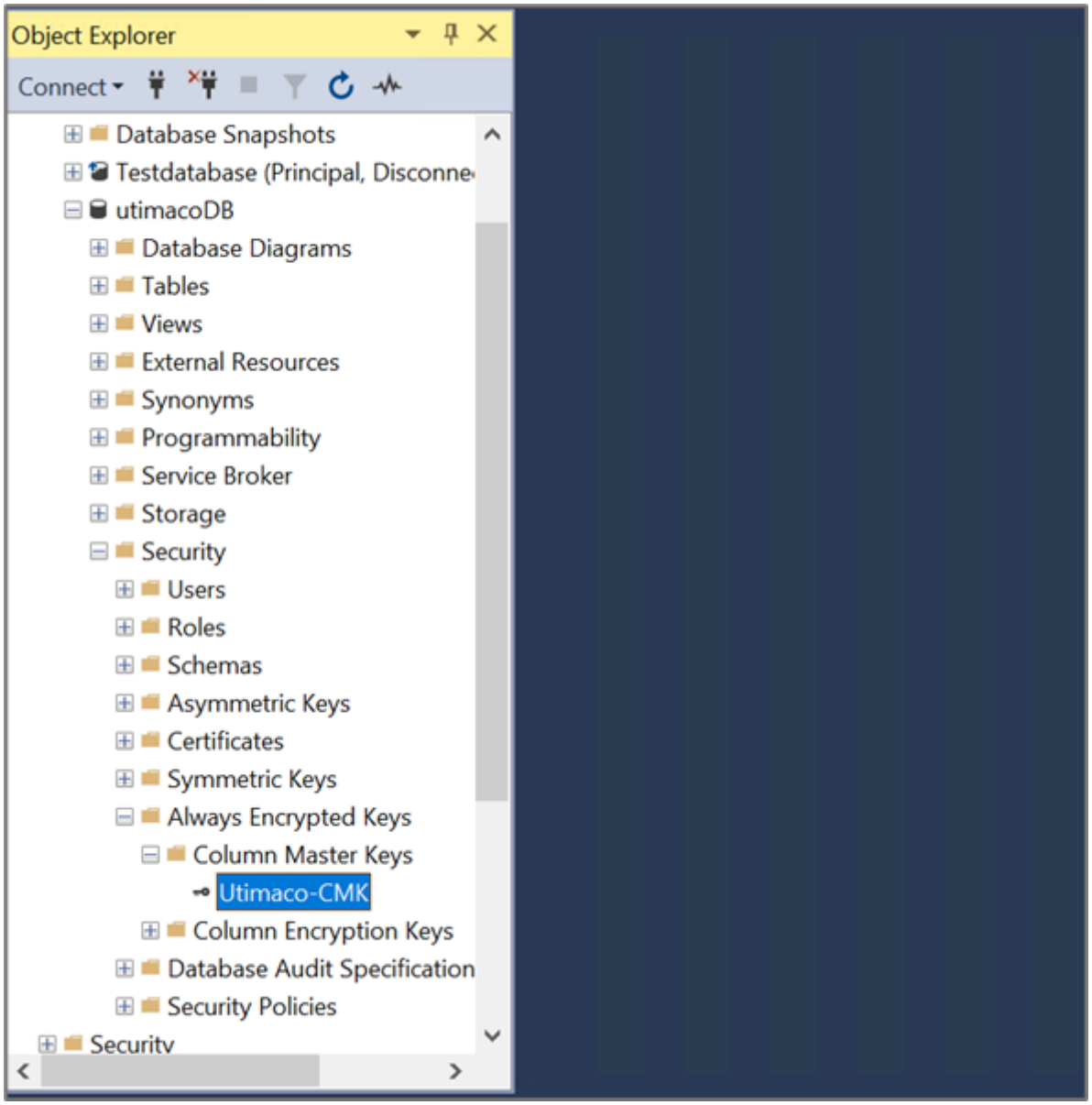


Figure 10 : New Column Master Key

## 6.2 Enable Always Encrypted

1. To Enable Always Encrypted and generate a Column Encryption Key, right-click on the Database Name in Object Explorer Menu and select TASK.

2. Select Encrypt Column... This will open the Always Encrypted wizard.

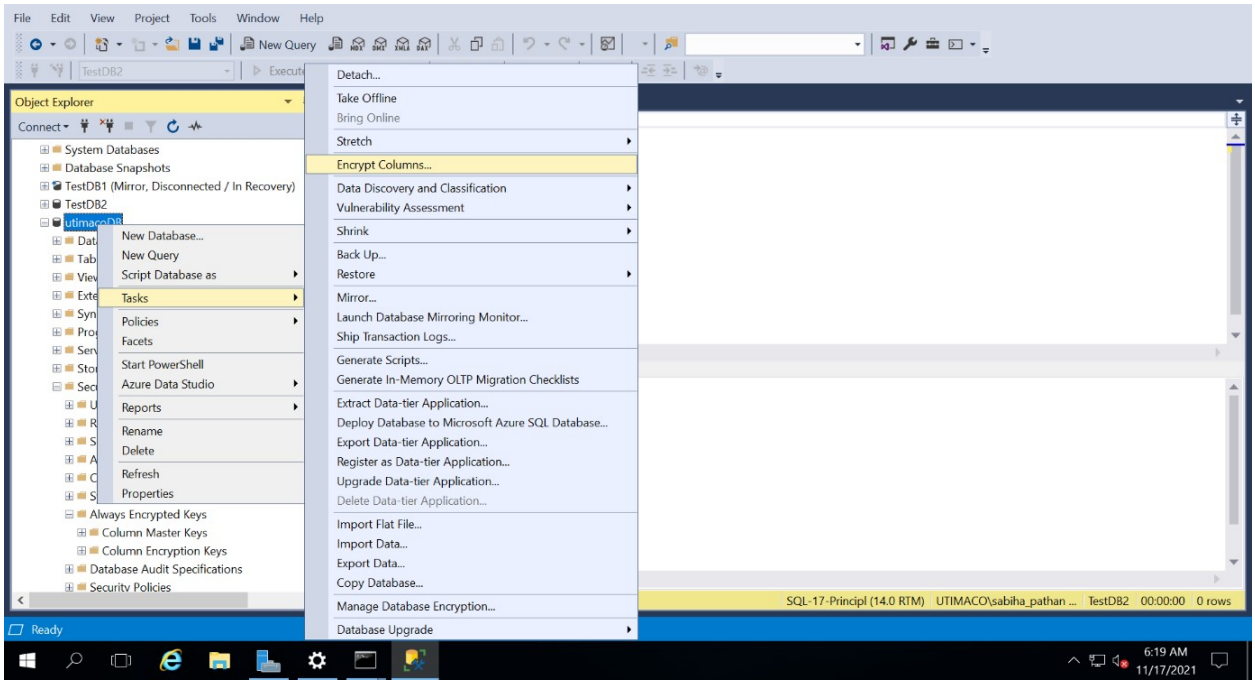


Figure 11 : Apply Always Encrypted window

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

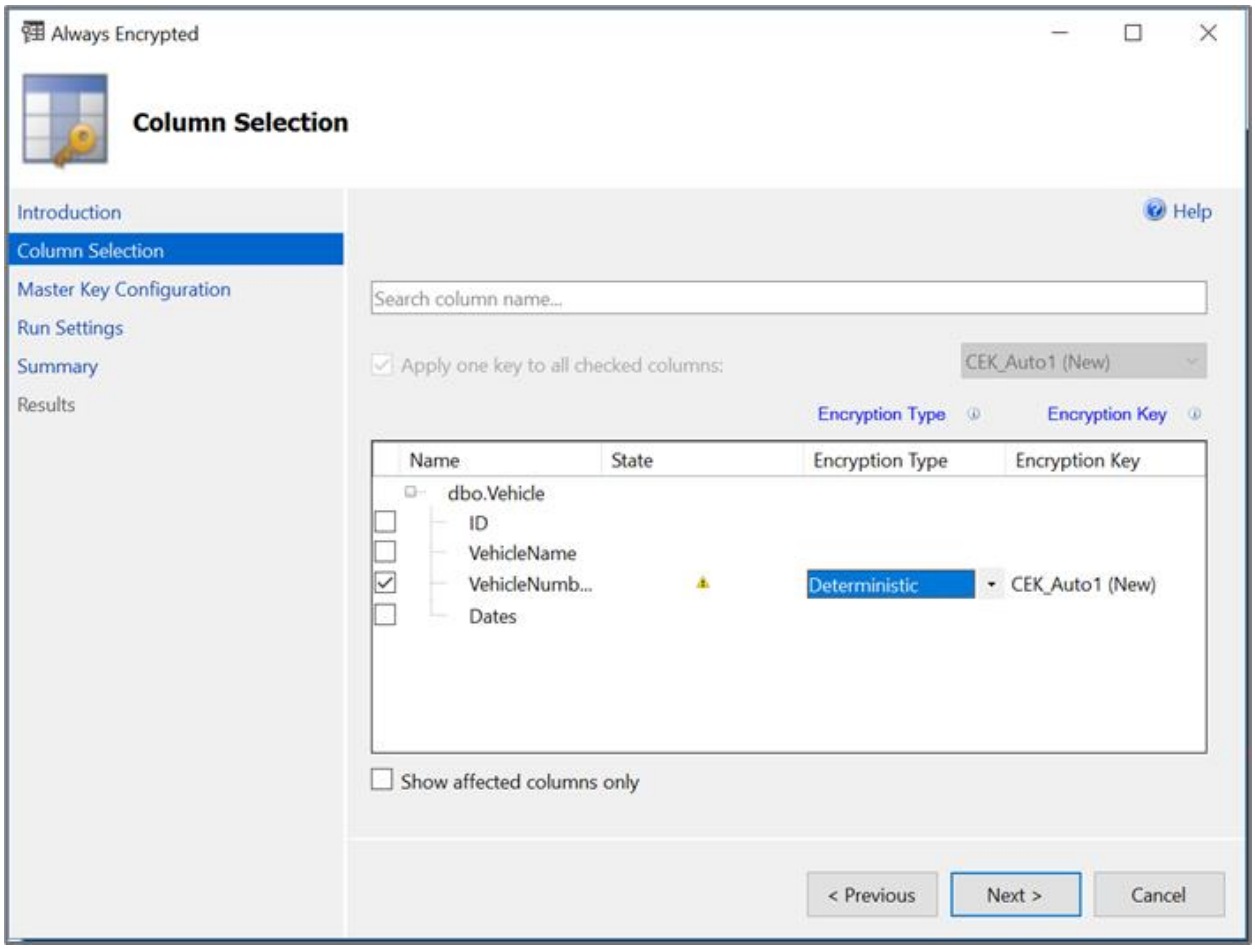


Figure 12 : Column Selection window

The “Apply one key to all checked columns” is shaded out until 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 beneath the “Encryption Key” option.

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
- Randomized
- Plaintext (only available to revert encrypted columns to an unencrypted state)

4. Click Next.

5. On the Master Key Configuration page, make sure that you select the CMK that was generated using the Utimaco Key Storage Provider and protected by the HSM and click Next.

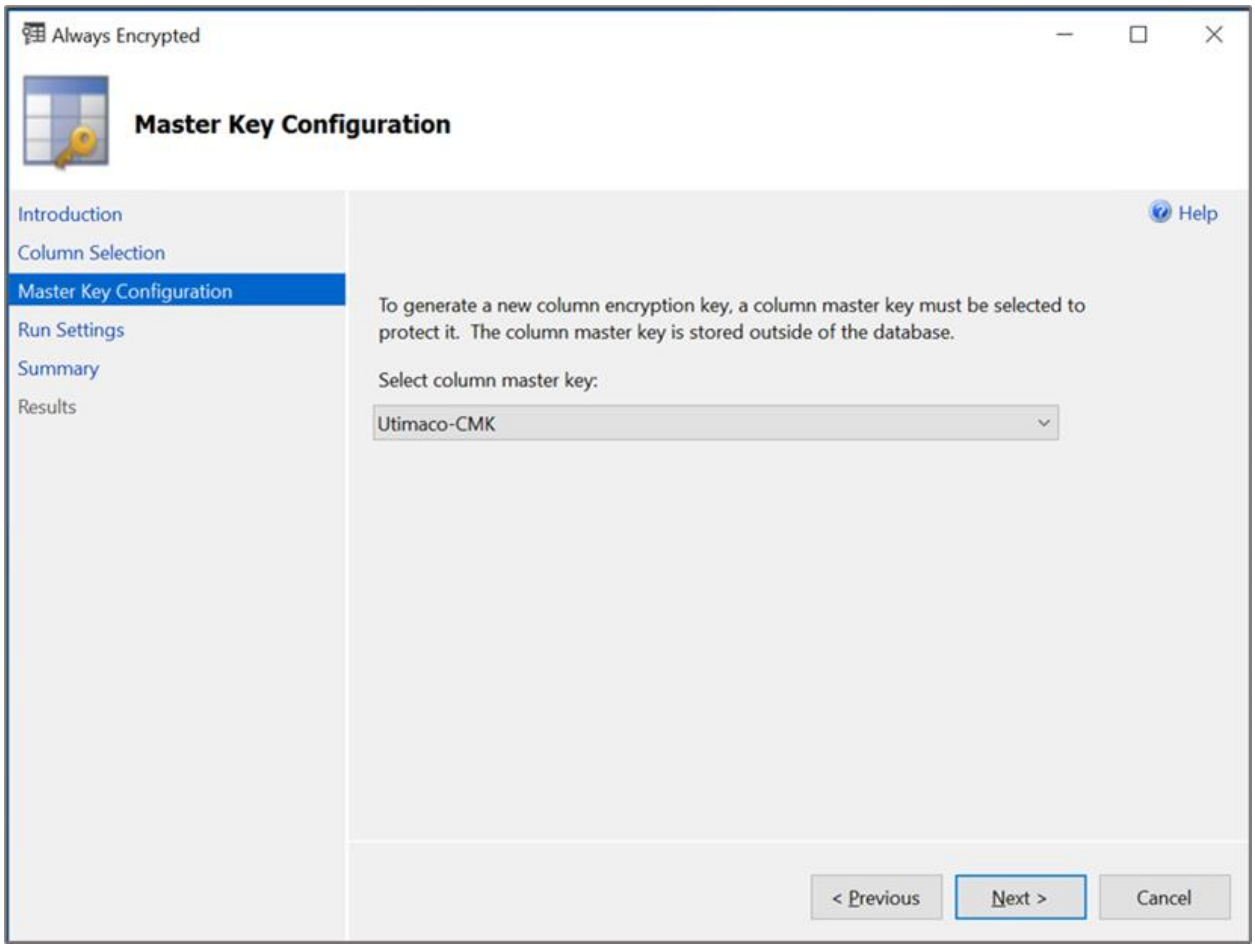


Figure 13 : Column Selection window

6. 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 back up the database and to only perform this activity when the database is off-line.

7. In this case we will continue and run the encryption straight away. Select the option “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 Summary page.

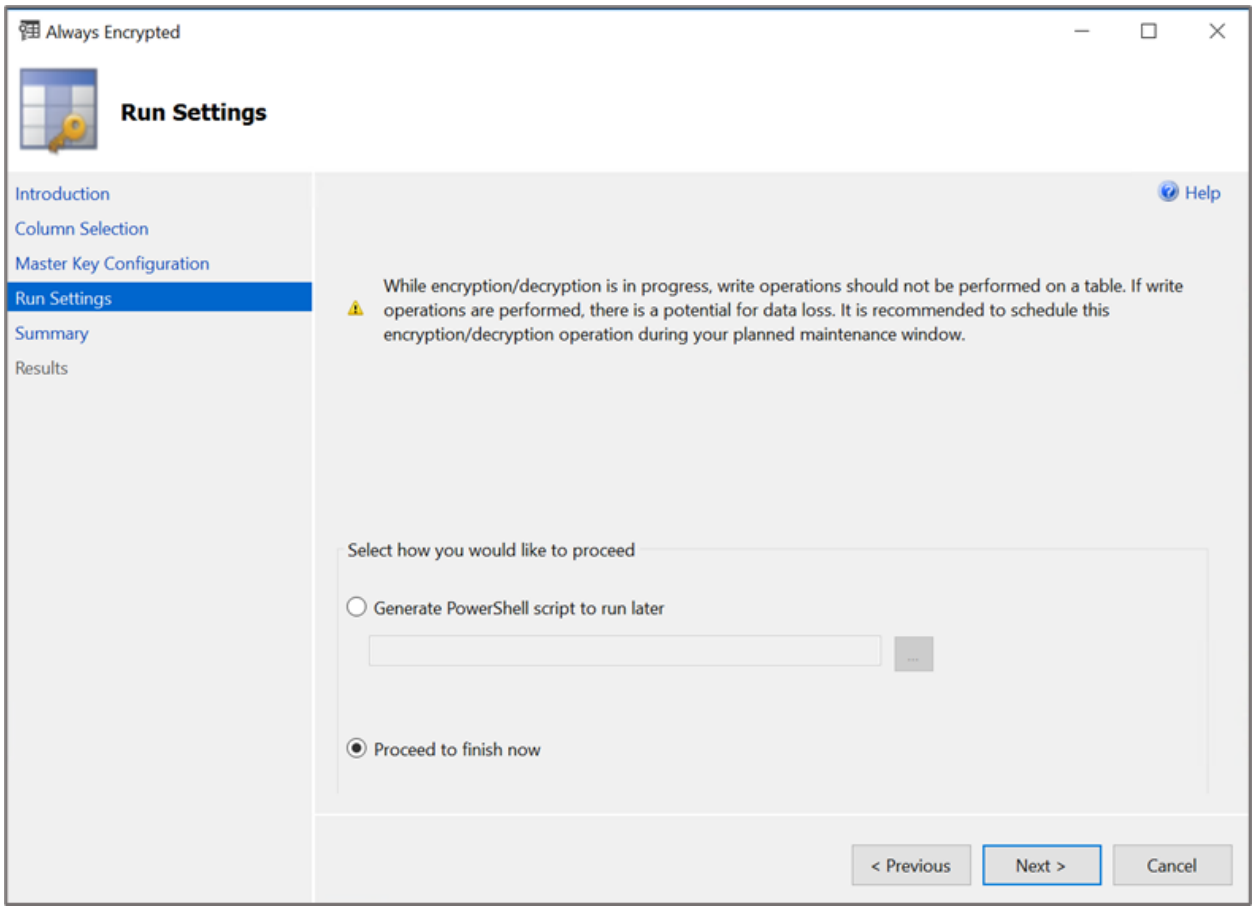


Figure 14 : Run Settings window

8. Verify the summary of settings and click Finish.

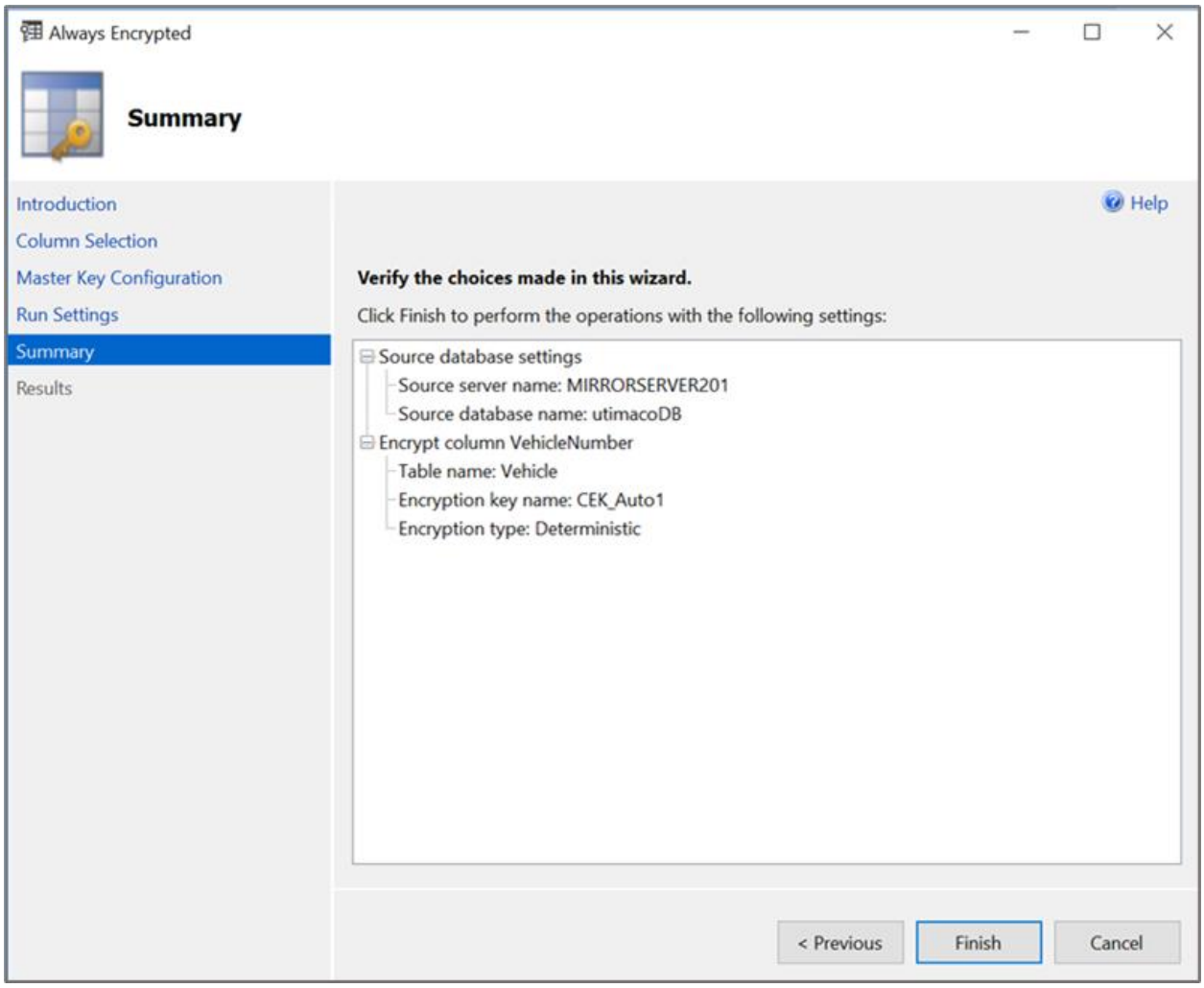


Figure 15 : Summary window

9. The Results page will report the requested / specified columns are now encrypted. The user can now click “Close” to exit the Always Encrypted Column Encryption Key wizard.

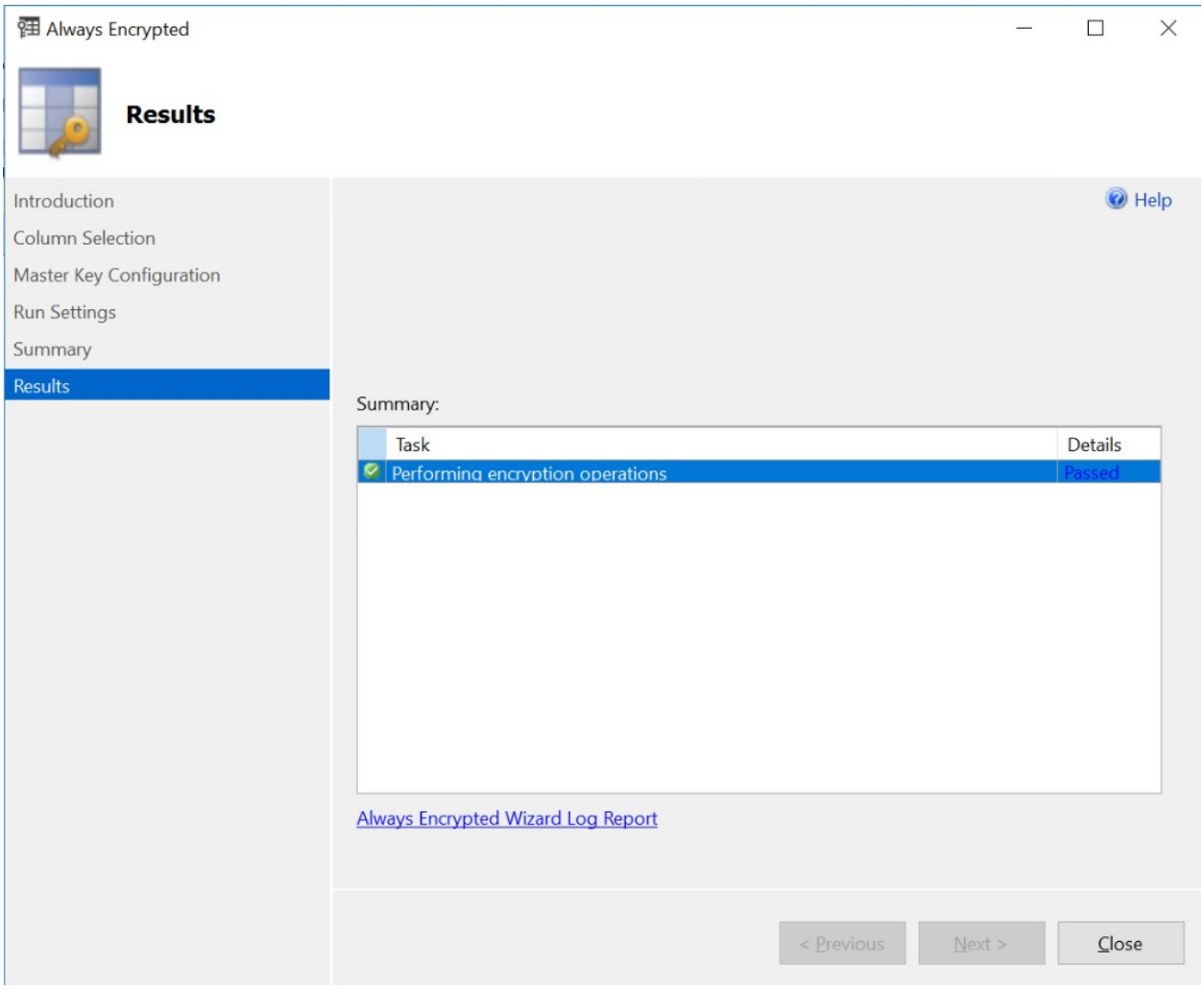


Figure 16 : Results window

10. Query the table using select query and view the encrypted column. Expected output should be the encrypted column values will be visible in encrypted format.

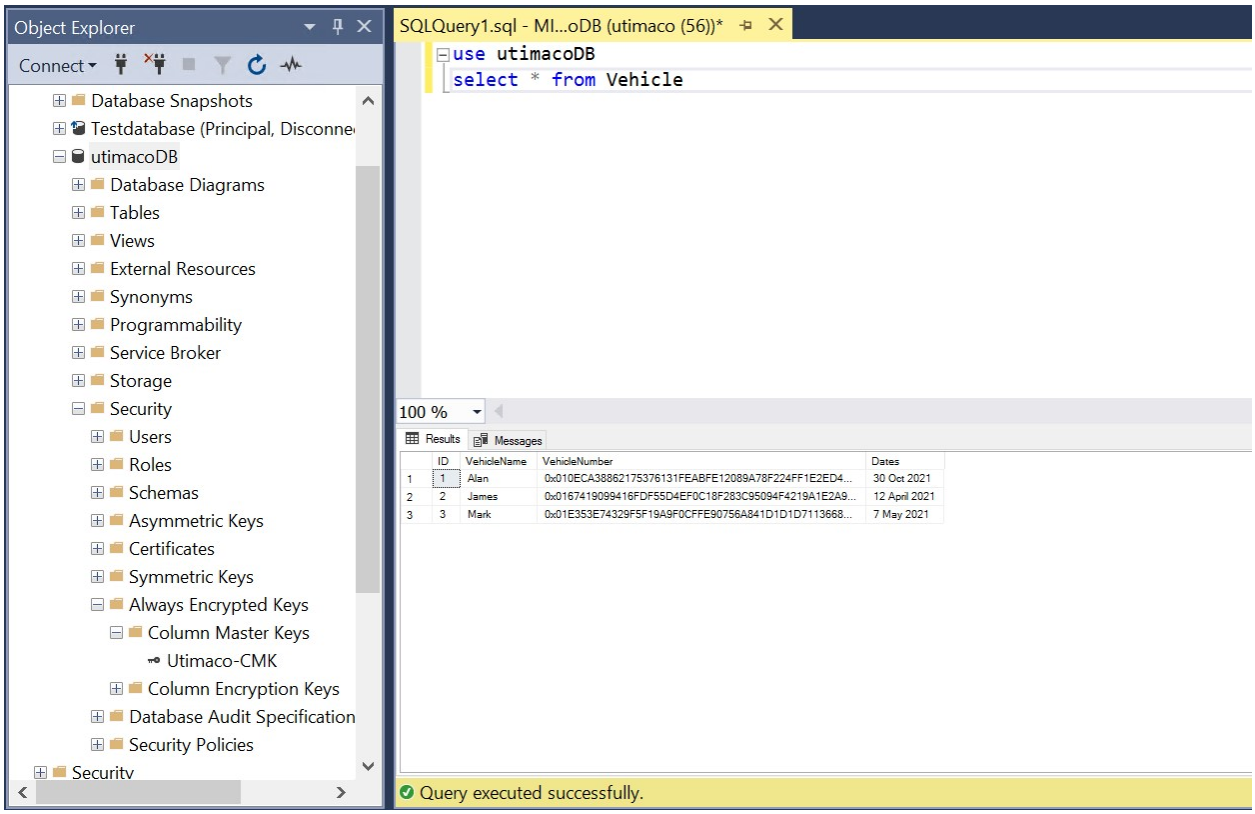


Figure 17 : Always Encrypted Output window

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 “Column Encryption Setting = enabled” (without parenthesis “”) and then click “Connect”.

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

## 6.3 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.

1. 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”.

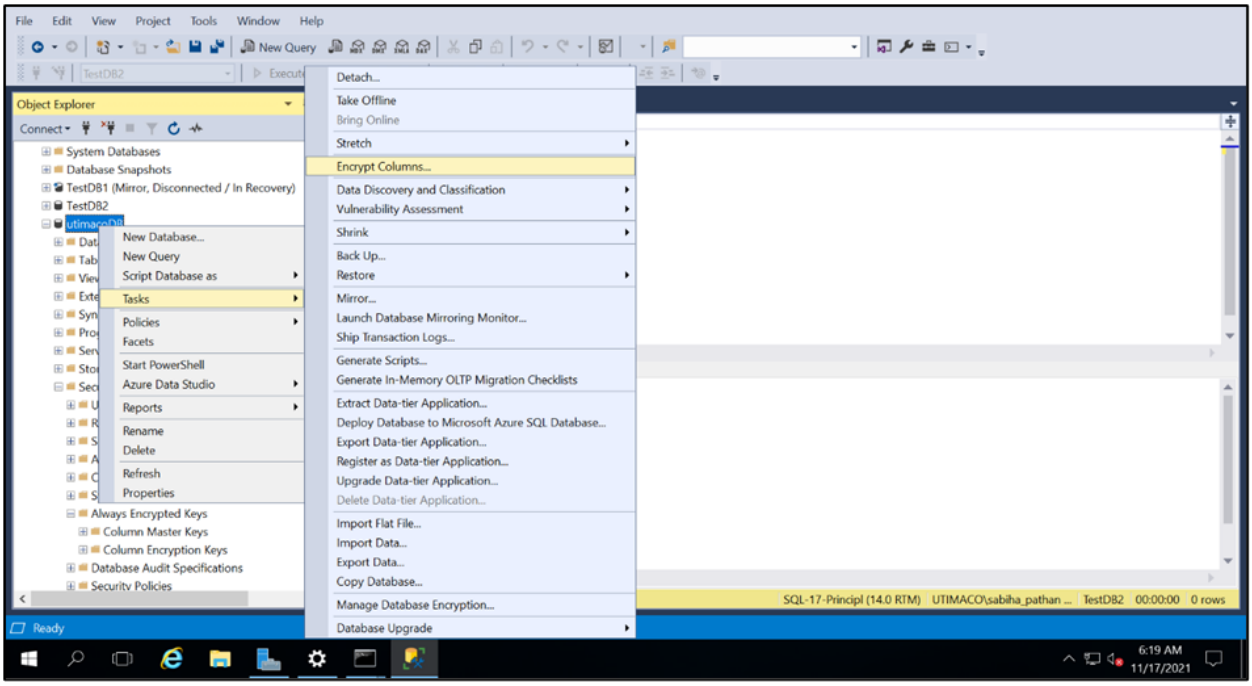


Figure 18 : Removing Always Encryption Window

2. From the Introduction screen, select “Next” to get to the Column Selection page. Click on the field “Encryption Type” to enter your preferred option for this value.

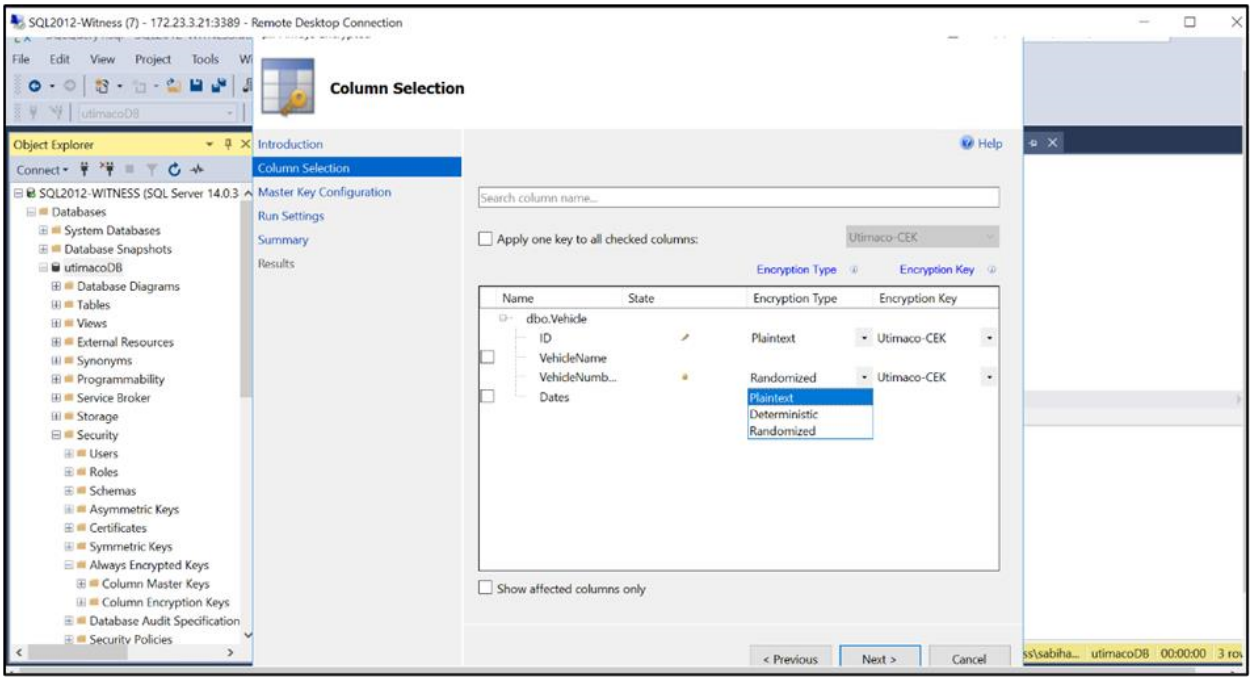


Figure 19 : Encryption Type Selection window

3. From the drop-down list select “Plaintext” then 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 offline before proceeding to remove the column encryption.

4. Select “Proceed to finish now” and click Next.

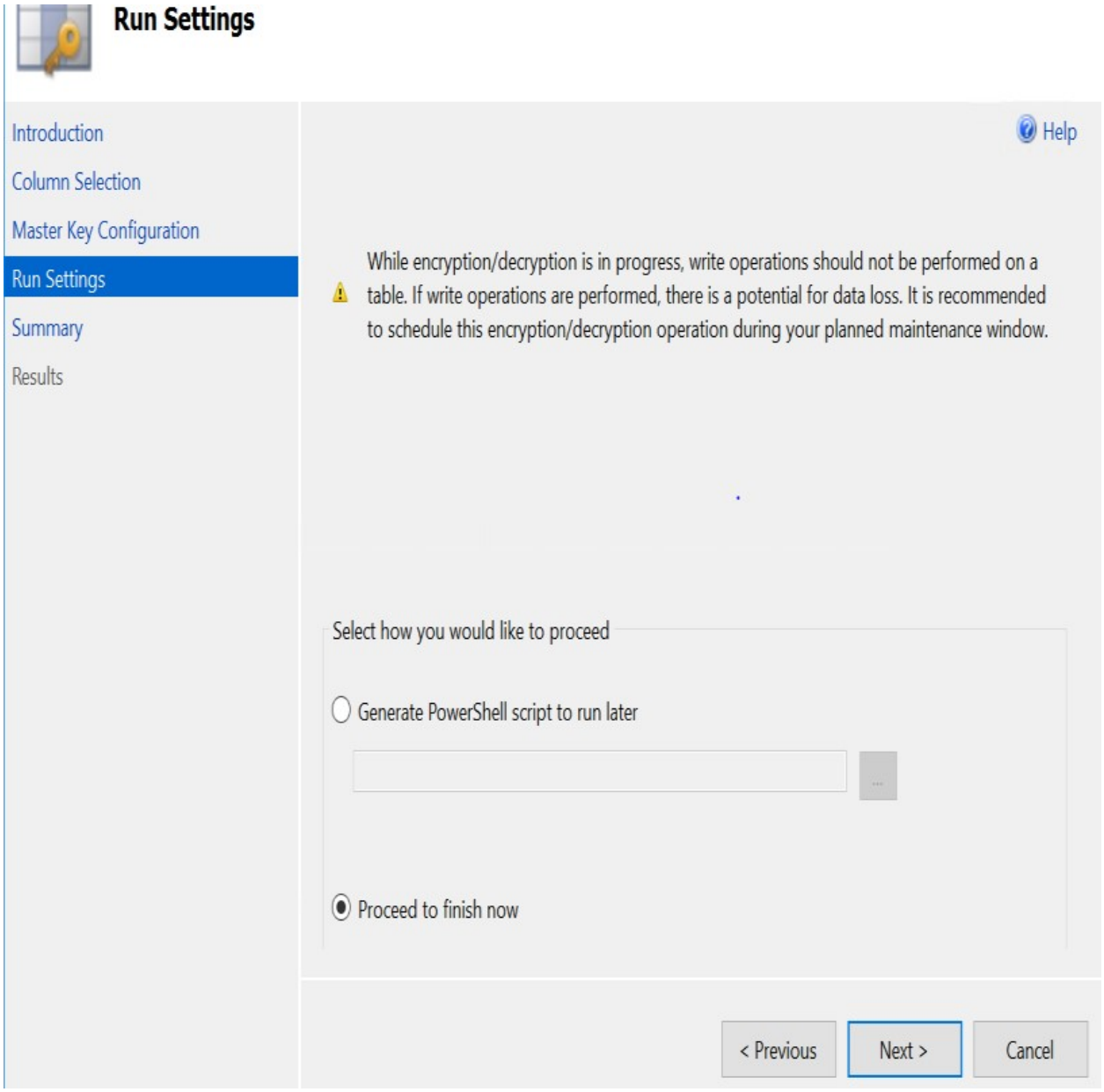


Figure 20 : Run Setting Window

5. The following page will provide a review summary for the requested operations.

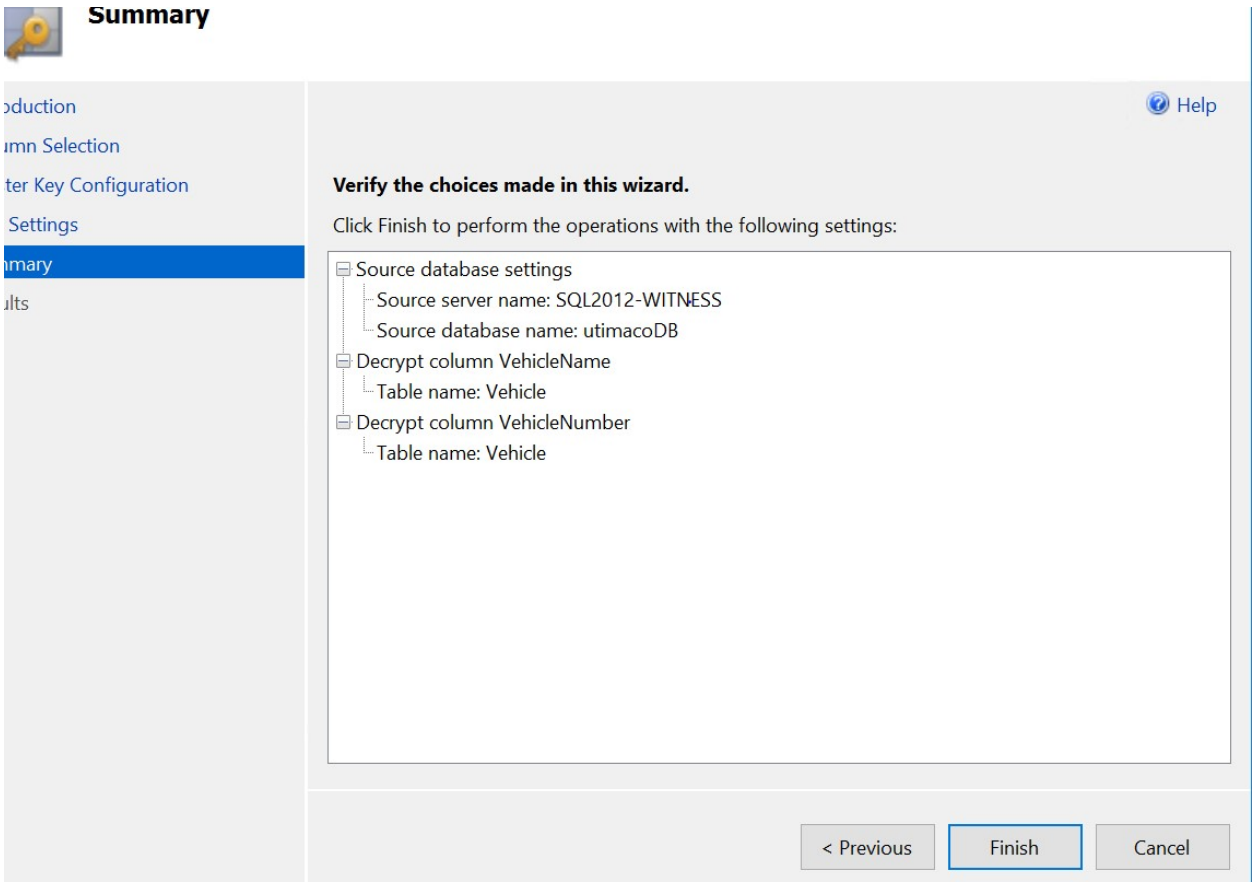


Figure 21 : Summary window

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

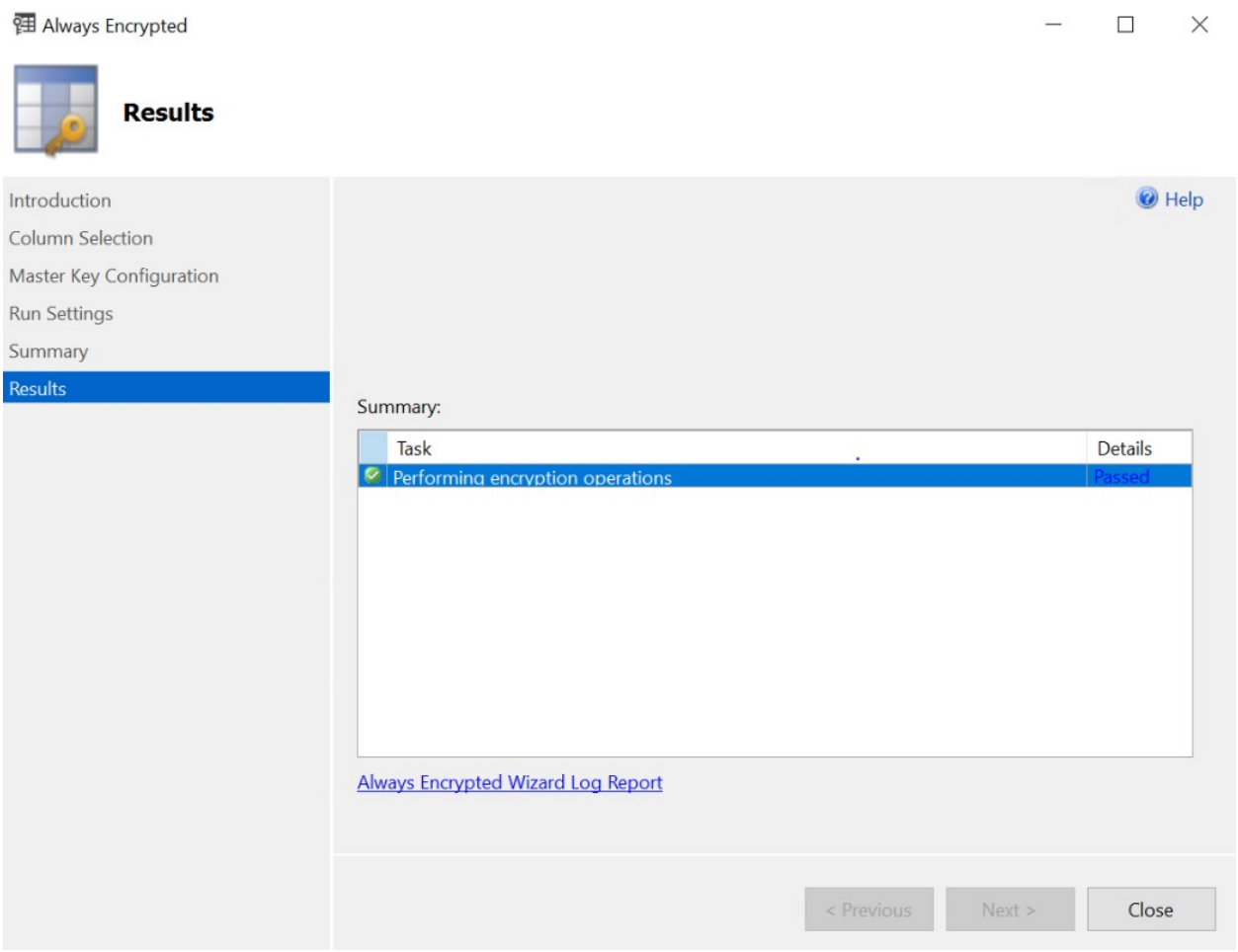


Figure 22 : Results window

7. You have successfully removed Always Encrypted column encryption from your database. When you next log into the database you can remove the Column Encryption Setting = enabled string from 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).

This completes the Integration for Microsoft SQL Always Encrypted with Utimaco SecurityServer.

# 7 Troubleshooting

| Error | Diagnosis |
|---|---|
| Cannot continue the execution because the session is in the kill state.<br><br>A severe error occurred on the current command. The results, if any, should be discarded. | 1. Check if Security Server Application is Up & Running if the user is using simulator<br>2. Check if the Configuration File (cs_cng.cfg) has correct HSM IP Address configured. |
| Error B0680103<br><br>CryptoServer module<br><br>CXI FIPS mode<br><br>Algorithm not available in FIPS mode | RSA Algorithm is not supported in FIPS Mode. |
| While user is trying to create a key using cngtool command line utility, following error is seen:<br><br>E: NCryptOpenStorageProvider [Utimaco CryptoServer Key Storage Provider] returned: Error 0x80090011<br><br>Object was not found.<br><br>CreateKey= returned: Error 0x80090011<br><br>Object was not found. | 1. Check if HSM is accessible.<br>2. Verify if the correct port number is used to connect to HSM. |

| Error | Diagnosis |
| --- | --- |
| While user is trying to create a key using cngtool command line utility, following error is seen:<br>E: NCryptEnumKeys returned: Error 0x80090010<br>Access denied.<br>ListKeys returned: Error 0x80090010<br>Access denied. | 1. Check if correct Crypto User credentials are used.<br>2. User may not have the permission to access the key from specific group. |
| While user is trying to create a key using cngtool command line utility, following error is seen:<br>E: unsupported algorithm: AES<br>CreateKey= returned: Error 0x80090027<br>The parameter is incorrect. | Check if the supported algorithm type and size are mentioned while creating the key while using cngtool command line utility. |

Table 6: List of Errors and their Diagnoses

# 8 Further Information

This document forms a part of the information and support which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website: https://utimaco.com/

For more information regarding Microsoft SQL Server Always Encrypted documentation, please see the following link:

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

# 9 References

| Reference | Title/Company | Document No. |
|---|---|---|
| [CSADMIN] | CryptoServer – csadm Manual/Utimaco IS GmbH | 2009-0003 |
| [CSADMIN2] | CryptoServer_csadm_Manual_Systemadministrators.pdf | 2009-0003 |
| [CSLAN] | CryptoServerLAN_V5_Manual_Systemadministrators.pdf | 2018-0010 |
| [CSP-CNG] | CryptoServer_Manual_CSP_CNG.pdf | 2008-0002 |

Table 7: References

# 10 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

### RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

### Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.