FORTANIX TECHNICAL DOCUMENTATION

# Administration Guide

**Fortanix**<sup>®</sup>

USING DATA SECURITY MANAGER WITH MSSQL SERVER – ALWAYS ENCRYPTED

VERSION 1.0

Fortanix, Inc. | 3910 Freedom Circle | Suit 104 | Santa Clara, CA 95052 | United States of America | +1 (628) 400-2043 |

#### TABLE OF CONTENTS

| 1.0   |  | 2  |
|-------|--|----|
| 1.1 P | Prerequisites                                | 2  |
| 2.0   | DEFINITIONS                                  | 3  |
| 3.0   | SQL SERVER ALWAYS ON SETUP                   | 5  |
| 3.1   | Supported Versions                           | 5  |
| 4.0   | INTEGRATION STEPS                            | 5  |
| 4.1   | Configuring Fortanix DSM                     | 5  |
| 4.1.1 | Creating Groups                              | 5  |
| 4.1.2 | 2 Creating Apps                              | 7  |
| 4.2   | Fortanix CNG Client                          | 7  |
| 4.2.1 | 1 Installation                               | 8  |
| 4.2.2 | 2 Configuring CNG Client                     | 8  |
| 4.3   | SQL Always Encrypted                         | 9  |
| 4.3.1 | 1 Create Sample Database                     | 9  |
| 4.3.2 | 2 Create Column Master key                   | 10 |
| 4.3.3 | 3 Create Column Encryption Key               | 12 |
| 4.3.4 | 4 Encrypt Columns Using Always Encrypted Key | 13 |
| 4.3.5 | 5 Verify Always Encrypted Columns            |    |
| 4.3.6 | 6 Rotate Always Encrypted Key                | 19 |
| 5.0   | DOCUMENT INFORMATION                         | 25 |
| 5.1   | Document Location                            | 25 |
| 5.2   | Document Updates                             | 25 |

#### 1.0 INTRODUCTION

This document describes the steps to integrate the Fortanix Data Security Manager (DSM) with Microsoft SQL Always Encrypted Server.

For more information, refer to the <u>https://learn.microsoft.com/en-us/sql/relational-</u> <u>databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver15</u>

#### 1.1 **PREREQUISITES**

Ensure the following:

• The port 443 must be accessible from the SQL target machine to Fortanix DSM.

| PROTOCOL | INBOUND/ | PORT   | LOAD     | PURPOSE                             |
|----------|----------|--------|----------|-------------------------------------|
|          | OUTBOUND | NUMBER | BALANCER |                                     |
|          |          |        | USE      |                                     |
|          |          |        | (YES/NO) |                                     |
| ТСР      | Outbound | 443    | No       | HTTPS – Used for calling REST API.  |
|          |          |        |          | MS-SQL server will access the       |
|          |          |        |          | cluster/SaaS URL on this port.      |
|          |          |        |          | Each individual node will also need |
|          |          |        |          | this port open.                     |

- The SQL Server must be installed and configured on the target machine.
- Administrators are privileged to access SQL Server Management Studio from the target machine.

#### 2.0 **DEFINITIONS**

#### • Fortanix Data Security Manager -

Fortanix DSM is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

#### • Accounts -

A Fortanix DSM account is the top-level container for security objects managed by the Fortanix DSM. An account is generally associated with an organization, rather than an individual. Security objects, groups, and applications belong to exactly one account. Different accounts are fully isolated from each other. *See <u>support</u> for more information.* 

• Users -

Users are associated with an email address. A user can be a member of one or more accounts. Depending on permissions, users can:

- Perform management operations like adding or modifying users or groups
- Create security objects
- Change properties of security objects
- Review logs of Fortanix DSM activity

## Users cannot perform cryptographic operations. Only applications can perform cryptographic operations.

• Groups -

A group is a collection of security objects created by and accessible by users and applications which belong to the group. The user who creates a group automatically gets assigned the role of the group administrator. You can add more users to the group in the role of administrators or auditors. You can also add applications to the group to enable the applications to create and use security objects in that group. *See <u>support</u> for more information.* 

Access policies are set at the group level, so all security objects in a group share the same access policy. Any number of users and/or applications can be assigned to a group. *Some examples of usage of groups are given in the <u>Authorization</u> section.* 

Quorum policies can also be set at group level. A Quorum policy mandates that all security sensitive operations in that group would require a quorum approval. Such operations include using a key for cryptographic operations or deleting or updating a group. *See <u>Quorum Policy</u> for more information.* 

#### • Applications -

An application (app) can use Fortanix DSM to generate, store, and use security objects, such as cryptographic keys, certificates, or an arbitrary secret. Applications can authenticate to Fortanix DSM using an API key (a secret token) or a TLS client certificate. An application can interact with Fortanix DSM using the REST APIs or using the PKCS#11, JCE, or CNG providers. *See support for more information.* 

#### • Fortanix Data Security Manager Security Objects -

A security object is any datum stored in Fortanix DSM (for example a key, a certificate, a password, or other security objects). Each security object is assigned to exactly one group. users and applications assigned to the group have permission to see the security object and to perform operations on it. *See <u>support</u> for more information.* 

## **Fortanix**°

#### 3.0 SQL SERVER ALWAYS ON SETUP

This integration uses the following setup to demonstrate the Always Encrypted with Fortanix DSM:

- 1. A Windows Server machine, as a Domain Controller.
- 2. A Windows Server machine, with SQL Server and Fortanix CNG 32-bit client installed.
- 3. A Windows 10 Professional machine with Fortanix CNG 64-bit client install to the test column decryption.

#### 3.1 SUPPORTED VERSIONS

This SQL Always Encrypted integration is tested on the following versions:

- Microsoft SQL Server 2019
- Microsoft Server Management Studio 19 (v19.1)
- Fortanix DSM 4.19
- Fortanix CNG Client 4.19 (32-bit)

#### 4.0 INTEGRATION STEPS

#### 4.1 CONFIGURING FORTANIX DSM

Perform the following tasks to configure Fortanix DSM:

#### 4.1.1 CREATING GROUPS

A Fortanix DSM group is a collection of security objects created by and accessible by users and applications that belong to the group. The user who creates a group automatically gets assigned the role of group administrator. You can add more users to the group in the role of administrators or auditors. You can also add applications to the group to enable the applications to create and use security objects in that group.

To add a group, specify the following:

- The title of the group (required).
- A short description for the group (not mandatory).
- Users in your account as members.

- Applications in your account to add to the group so that they can use the security objects in the group. *Refer to "Section 4.1.2- Creating Apps" to know the steps for creating the app.*
- Add a quorum approval policy (optional). A group administrator may enable a quorum approval policy for a group, which mandates that all security-sensitive operations in that group would require a quorum approval.

| GROUPS EXTERNAL ROLES CUSTOM GROUP ROLES   |   |  |
|--|---|--|
| Groups   |   |  |
| Adding new group   |   |  |
| Sea site for your me group<br>MSSQL_Demo_Group   | Example: DSM Team<br>You can change the tide lear     |  |
| Add the description for your group here  | This would help you to blandly groups in your system. |  |
| Add Group Quorum Policy<br>Quorum approxi data an easi level of protection to all objects in the group. At survitive expensions with lags and pugines within the group will require<br>expresse excenting to the pulsio. | ADD QUORUM POLICY                                     |  |
| Configure as HSM/External KMS group  | LINK HSM/EXTERNAL KMS                                 |  |
| Configure a KEK from an existing group<br>Bross al election in the proof with the selected KEK.  | CONFIGURE A KEK                                       |  |
|  | CANCEL  |  |

FIGURE 1: ADDING NEW GROUP

#### 4.1.2 CREATING APPS

An application can use Fortanix DSM to generate, store, and use security objects, such as cryptographic keys, certificates, or an arbitrary secret. Examples of applications include web servers, PKI servers, key vaults, and so on. An application can interact with Fortanix DSM using the REST APIs or the PKCS#11, JCE, or CNG providers.

To add an application, specify the following:

- Name of the application (required).
- Type of the application. Select the value as **interface**.
- A short description of the application.
- Select the authentication method as **API key**.
- Assign the app to the MSSQL group as created in the "Section 4.1.3- Creating Group".

After the application has been added, you can use the API key to authenticate the CNG client to Fortanix DSM and start making calls to do cryptographic operations.

| Apps                    |                              |                              |                        |                  |                      |           |                      |              |
|-------------------------|------------------------------|------------------------------|------------------------|------------------|----------------------|-----------|----------------------|--------------|
| Adding ne               | w app                        |                              |                        |                  |                      |           |                      |              |
| App name<br>MS-SQL Demo |                              |                              |                        |                  |                      |           | Interface (optional) | *            |
| O ADD DES               | CRIPTION                     |                              |                        |                  |                      |           |                      |              |
| Authentic               | ation method                 | i                            |                        |                  |                      |           |                      |              |
| APIKey                  | O Certificate                | O Trusted CA                 | Google Service Account | O JSON Web Token | O External Directory | O AWS IAM |                      |              |
| Set and secret key      | 2.28                         |                              |                        |                  |                      |           |                      |              |
| OAuth                   |                              |                              |                        |                  |                      |           |                      |              |
| Enable C                | n authorize that app to pert | term actions on their behalf |                        |                  |                      |           |                      |              |
| Assigning th            | e new app to gr              | roups                        |                        |                  |                      |           |                      | Time         |
|                         |                              |                              |                        |                  |                      |           | 🚊 MS-SQL Demo        | <b>III</b> B |
|                         |                              |                              |                        |                  |                      |           | Solution             |              |
|                         |                              |                              |                        |                  |                      |           |                      |              |
|                         |                              |                              |                        |                  |                      |           |                      |              |
|                         |                              |                              |                        |                  |                      |           |                      |              |
|                         |                              |                              |                        |                  |                      |           |                      |              |
|                         |                              |                              |                        |                  |                      |           |                      |              |
|                         |                              |                              |                        |                  |                      |           |                      |              |
|                         |                              |                              | DREATE NEW (           | CROUP            |                      |           |                      |              |
|                         |                              |                              |                        |                  |                      |           |                      | CANCEL       |

FIGURE 2: ADDING NEW APP

#### 4.2 FORTANIX CNG CLIENT

The Fortanix CNG Provider must be installed on every target machine. Refer to

https://support.fortanix.com/hc/en-us/articles/360018084132-CNG-EKM (32-bit) to download the CNG

Provider.

FortanixKmsClient.msi installs the Fortanix CNG Provider, as well as an EKM provider and the PKCS#11 library. Next, to configure the CNG client Fortanix CNG Provider communicates with Fortanix DSM for crypto operations.

#### 4.2.1 INSTALLATION

Perform the following steps to complete the installation on your machine:

- 1. On the **Fortanix KMS Client Setup** dialog box, click the **Next** button.
- 2. Select the checkbox for **I accept the terms in the License Agreement** and click the **Next** Button.
- Enter the location for installing the Fortanix KMS Client as C:\Program Files\Fortanix\KMS Client\.
- 4. Click the **Install** button to install the Fortanix KMS client.
- 5. After the installation is done, click the **Finish** button.

#### 4.2.2 CONFIGURING CNG CLIENT

The Fortanix KMS Server URL and proxy information are configured in the Windows registry for the current user.

1. Run the following command to navigate to FortanixKmsClientConfig.exe file:

cd C:\Program Files (x86)\Fortanix\KmsClient\

2. The user key store uses the current user configuration.

For example, run the following command to configure the Fortanix KMS Server URL for the current user:

FortanixKmsClientConfig.exe user --api-endpoint {KMS\_URL}

#### Where,

- KMS\_URL refers to the Fortanix DSM URL. On-premises customers use KMS URL and SaaS. The customers can use the following URLs based on the region.
  - Europe: <u>https://eu.smartkey.io/</u>
  - o APAC: <u>https://apac.smartkey.io/</u>



• United States of America: <u>https://amer.smartkey.io/</u>

For example,

```
FortanixKmsClientConfig.exe user --api-endpoint https://<fortanix
_dsm_url>
```

- To configure proxy information, add --proxy http://proxy.com or --proxy none to unconfigure proxy.
- 4. Run the following command to configure the API key as created in *Section 4.1.2: Creating Apps* for the user keystore:

FortanixKmsClientConfig.exe user --api-key <api\_key>

#### 4.3 SQL ALWAYS ENCRYPTED

#### 4.3.1 CREATE SAMPLE DATABASE

For testing the integration, a sample database is created. However, you can use the existing database table to encrypt the required column.

- 1. Open the SQL Server Management Studio and connect to the database.
- 2. Run the following commands to create database employee:

```
CREATE DATABASE employee
```

3. Run the following commands to create table employee:

```
USE employee
CREATE TABLE employee (first_name VARCHAR(128),last_name VARCHAR(
128),empID DECIMAL,salary DECIMAL(6));
GO
```

4. Run the following commands to insert data into the table:

```
Fortanix
```

```
insert into employee values ('Adam','Parker','1','5000')
insert into employee values ('John','Doe','2','4500')
insert into employee values ('Peter','Williams','2','4500')
GO
```

#### 4.3.2 CREATE COLUMN MASTER KEY

The column master keys are key-protecting keys that are used to encrypt the column encryption keys. The column master keys will be stored on the Fortanix DSM. The database only contains metadata about the column master keys such as type of key store and location. The column master key metadata is stored in the

sys.column\_master\_keys (Transact-SQL) catalog view.

- Log in to the Fortanix DSM user interface and create an RSA key with the following permissions, such as Always\_Encrypted\_Key\_Database\_Name.
  - Encrypt
  - Decrypt
  - Sign
  - Verify



| ② Dashboard   | pre utare dedennated destroyed                             |  |
|---|--|--|
| ி Integrations  | Always_Encrypted_Key_Database_Name                         |  |
| 品 Groups  |  |  |
| 🗁 Apps  | UUID: f9bda536-e86c-4240-83d9-cab664c35112                 |  |
| Security Objects<br>Keys, Secrets, Certs  | Activity chart 🗸   |  |
| Users     Users |  |  |
| Plugins   | INFO ATTRIBUTES/TAGS KEY ROTATION KEY ACCESS JUSTIFICATION |  |
| 🕑 Tasks   | Enabled ③  |  |
| 🕼 Audit Log   | (No description) Ø   |  |
| ී Settings  | Type RSA $\odot$ Size 2048 bits KCV O                      | Activity Logs C Last upo                                 |
|   | 😤 DOWNLOAD PUBLIC KEY 🧳 REMOVE PRIVATE KEY                 | DSM will keep a full audit log for this op               |
|   | Public key published                                       |  |
|   | Padding Policy   | App "MS-SQL Demo" used key<br>ON Jun 27, 2023 1:43:22 am |
|   | Encryption OAEP Hashing Algorithm all                      | App "MS-SQL Demo" used key<br>ON Jun 27, 2023 1:43:22 am |
|   | EDIT   | App "MS-SQL Demo" used key<br>ON Jun 27, 2023 1:43:22 am |
|   | Group  | App "MS-SQL Demo" used key<br>OI Jun 27, 2023 1:43:07 am |
|   | 品 MS-SQL Demo  | App "MS-SQL Demo" used key                               |

FIGURE 3: CREATE KEY

- 2. After the key is created, log in to the SQL Server Management Studio.
- Navigate to the Databases → employee → Security → Always Encrypted Keys →
   Column Master Keys. Right click on the folder Column Master Keys and select the
   New Column Encryption Key option to create the Column Master Keys.
- 4. Enter the following details:
  - **Name:** Enter the required name of the key.
  - **Key Store:** Select the **Key Storage Provider (CNG)** option from the drop down menu.
  - Select a provider: Select the Fortanix KMS CNG Provider option from the drop down menu.



| Object Explorer 👻 म 🗙                                    |                              |   |      |      |
|--|------------------------------|---|------|------|
| Connecta # X# = X & A                                    |                              |   |      |      |
|  |                              |   |      |      |
| CZAMAZ-OLC/ETC (SQL Server 15.0.4201.1 - ECZAMAZ-OLC/ETC |                              |   |      |      |
| Databases  | *** New Column Master Key    |   |      | ×    |
| System Databases   | New Column Musici Key        |   |      | ~    |
|  | Select a page                | 🖵 Script 👻 😯 Help                           |      |      |
| employee   |                              |   |      |      |
|  |                              |   |      |      |
|  |                              | Name: Fortanix_CMK                          |      |      |
| Views     Views  |                              |   | _    |      |
|  |                              | Key store: Key Storage Provider (CNG) V Ref | resh |      |
| Programmability  |                              |   |      |      |
| Service Broker   |                              |   |      |      |
| Storage  |                              | Select a provider:                          |      |      |
| Security   |                              | Fortanix KMS CNG Provider 🗸                 |      |      |
| licers   |                              |   |      |      |
| Roles  |                              | Name  |      | -    |
| Schemas  |                              | Always_Encrypted_Key_Database_Name          |      |      |
| Asymmetric Keys  |                              |   |      |      |
| Certificates   |                              |   |      |      |
| Symmetric Keys   |                              |   |      |      |
| Always Encrypted Keys                                    |                              |   |      |      |
| 🗉 📕 Column Master Keys                                   |                              |   |      |      |
| 😠 🛑 Column Encryption Keys                               | Connection                   |   |      |      |
| 🕀 📁 Database Audit Specifications                        | Service .                    |   |      |      |
| 🗉 🛑 Security Policies                                    | EC2AMAZ-OLC7E1L              |   |      |      |
| 🗉 🗐 Security   | Connection                   |   |      |      |
| 🗉 💼 Server Objects                                       | EC2AMAZ-OLC7E1L\Administrato |   |      |      |
| 🕀 💼 Replication  | View connection properties   |   |      |      |
| 🗉 📁 PolyBase   | TT Men connector properties  |   |      |      |
| 🗉 🚎 Always On High Availability                          |                              |   |      |      |
| 🗉 📁 Management   |                              |   |      |      |
| 🗉 🛑 Integration Services Catalogs                        | Progress                     |   |      |      |
| 🗉 县 SQL Server Agent                                     |                              |   |      |      |
|  | Heady                        |   |      |      |
|  |                              | Generate Key                                |      |      |
|  |                              |   |      |      |
|  |                              | ок  | Car  | ncel |
|  |                              |   |      |      |

FIGURE 4: COLUMN MASTER KEYS

#### 5. Click the **OK** button.

#### 4.3.3 CREATE COLUMN ENCRYPTION KEY

The column encryption keys are content-encryption keys used to encrypt the data in the database columns. You can encrypt one or more columns with the same column encryption key or use multiple column encryption keys depending on your application requirements. The column encryption keys are themselves encrypted, and only the encrypted values of the column encryption keys are stored in the database (as part of the column encryption key metadata). The column encryption key metadata is stored in the sys.column encryption keys (Transact-SQL) and

sys.column\_encryption\_key\_values (Transact-SQL) catalog views. The column encryption keys used with the AES-256 algorithm are 256-bit long.

- 1. Navigate to the **Databases**  $\rightarrow$  **employee**  $\rightarrow$  **Security**  $\rightarrow$  **Always Encrypted Keys**  $\rightarrow$  **Column Encryption Keys** to create the Column Encryption Keys.
- 2. Enter the following details:
  - **Name:** Enter the name of the column encryption key.



Column master key: Select the same column master key as created in *Section* 4.2.2 – Create Column Master Key. For example, select Fortanix\_CMK key from the drop down menu.

| Object Explorer  |   |                      |   |         |     |
|--|---|----------------------|---|---------|-----|
| Connect - ¥ ¥ = ∀ C →                                      |   |                      |   |         |     |
| EC2AMAZ-OLC7E1L (SQL Server 15.0.4261.1 - EC2AMAZ-OLC7E1L) |   |                      |   |         |     |
| 😑 💼 Databases  |   |                      |   |         |     |
| 🗉 💼 System Databases                                       | al New Column Encryption Ke   | у                    | -   |         | ×   |
|  | Select a page   | 🗖 Societ 📼 🙆 Hele    |   |         |     |
| 🗉 🗎 employee   |   | 🔄 Script - 🔂 Help    |   |         |     |
| Database Diagrams  |   |                      |   |         |     |
| I ables  |   | Name:                | Fortanix CEK  |         |     |
| Views  |   | Hume.                | . order of the second                                     |         |     |
| External Resources   |   | Column master key:   | Fortanix_CMK ~  | Refresh |     |
| Synonyms     Programmability                               |   |                      |   |         |     |
| Frogrammability     Service Broker                         |   |                      |   |         |     |
| Storage  |   | Column encryption k  | eys protect your data, and column master keys protect you | column  |     |
| E Security   |   | encryption keys. Thi | s lets you manage fewer keys.                             |         |     |
| 🕀 🗰 Users  |   | To create a new col  | umn masterkey, use the "New Column MasterKey" page.       |         |     |
| 🗉 🛑 Roles  |   |                      |   |         |     |
| 🗉 📁 Schemas  |   |                      |   |         |     |
| 🗉 📕 Asymmetric Keys  |   |                      |   |         |     |
| 😠 💼 Certificates   |   |                      |   |         |     |
| 😠 🛑 Symmetric Keys   |   |                      |   |         |     |
| 😑 📁 Always Encrypted Keys                                  |   |                      |   |         |     |
| 🗉 🛑 Column Master Keys                                     |   |                      |   |         |     |
| - Fortanix_CMK   | Connection  |                      |   |         |     |
| Column Encryption Keys                                     | Server:   |                      |   |         |     |
| Database Audit Specifications                              | EC2AMAZ-OLC7E1L   |                      |   |         |     |
| Security Policies  | Connection:   |                      |   |         |     |
| Security     Security                                      | EC2AMAZ-OLC/E1L\Administrator   |                      |   |         |     |
| Benlistien   | Vew connection properties   |                      |   |         |     |
|  |   |                      |   |         |     |
| 🗉 🧧 Folybase   |   |                      |   |         |     |
| Management   |   |                      |   |         |     |
| Integration Services Catalogs                              | Progress  |                      |   |         |     |
| 田 易 SQL Server Agent                                       | Ready   |                      |   |         |     |
| XEvent Profiler  | We and We are a second |                      |   |         |     |
|  |   |                      |   |         |     |
|  |   |                      | OK  | Can     | cel |
|  |   |                      |   |         |     |

FIGURE 5: COLUMN MASTER ENCRYPTION KEY

3. Click the **OK** button.

#### 4.3.4 ENCRYPT COLUMNS USING ALWAYS ENCRYPTED KEY

Perform the following steps:

 Navigate to the Databases → employee → Tables. Right click the required table and select the Encrypt Columns option to encrypt the columns.



| 0-0 12-1-4                              | New Query 🗿 🔊 🖓 🕰                | டி ஃ சி வி ? - ் - 🕅 - 📁 - 📮 - 🖓 🔎 🏛 🖸 - 🖕   |
|---|----------------------------------|--|
| 🕴 🛱 🔤 employee                          | ▶ Execute     ■     √            | B [29 28 20] 요즘 10 [ 14 24 ] 14 54 ] 16 5  |
| Object Explorer                         | + ‡ ×                            | SQLQuery2.sql - ECAdministrator (63))* 🍝 🗙 SQLQuery1.sql - ECAdministrator (60))   |
| Connect - 🕴 🍟 = 🝸 🖒 🚸                   |                                  | select* from employee  |
| 😑 😸 EC2AMAZ-OLC7E1L (SQL Serve          | er 15.0.4261.1 - EC2AMAZ-OLC7I ^ | SELECT * FROM sys.column_encryption_keys;  |
| 🖃 📁 Databases                           |                                  |  |
| System Databases     Database Spanshots |                                  |  |
| employee                                |                                  |  |
| 🗉 🛑 Database Diagrams                   |                                  |  |
| 😑 🗰 Tables                              |                                  |  |
| 🕀 💼 System Tables                       |                                  |  |
| 🕀 🇰 FileTables                          |                                  |  |
| Graph Tables                            |                                  |  |
|   |                                  |  |
| 🗉 📶 Colui                               | New Table                        |  |
| 🕀 💼 Keys 🛛 🛛                            | Design                           |  |
| E Cons S                                | elect Top 1000 Rows              |  |
| E Index                                 | dit Top 200 Rows                 |  |
| 🛞 🗰 Statis S                            | icript Table as                  |  |
| 🗉 🗰 Views 🛛 V                           | /iew Dependencies                |  |
| 🕀 💼 External Reso 🛛 N                   | Memory Optimization Advisor      |  |
|   | ncrypt Columns                   |  |
| 😠 🗰 Service Brok 🛛 🖡                    | ull-Text index                   | 100 % - <  |
| B Storage Security S                    | itorage 🕨                        | III Results @# Messages  |
| B Users p                               | Policies +                       | name column_encryption_key_idcreate_date modify_date<br>1 Entryption_FEX_2 2022_06_26 [1:1:10:0.94] 2022_06_26 27.45.27.45.7 |
| E Roles F                               | acets                            |  |
| i i Schemas<br>i i Asymme S             | itart PowerShell                 |  |
| E Certificat                            | leports +                        |  |
| B Always E R                            | lename                           |  |
| B Colui                                 | Delete                           |  |
|   | lefresh                          |  |
| 😑 📕 Colui 🛛 p                           | Properties                       |  |
| al Fortanix_C                           | CEK                              |  |
| Database Audit S     Security Policies  | opecifications                   |  |
| Security Policies                       |                                  | <u>а</u>   |

FIGURE 6: ENCRYPT COLUMN

2. On the **Introduction** screen, click the **Next** button.

| 館 Always Encrypted       | –  |
|--------------------------|--|
| Introduction             | _  |
| Introduction             | 🧭 Help   |
| Column Selection         |  |
| Master Key Configuration |  |
| Run Settings             |  |
| Summary                  | Always Encrypted is designed to protect sensitive information - such as credit card numbers -<br>stored in SQL Server databases. It enables clients to encrypt data inside client applications and |
| Results                  | never reveal the encryption keys to SQL Server.  |
|                          |  |
|                          | Do not show this page again.   |
|                          | < Previous Next > Cancel   |
|                          |  |

FIGURE 7: INTRODUCTION



- 3. On the **Column Selection** screen, select the following:
  - a. Encryption Type: Chose the required option from the drop down menu:
    - **Deterministic encryption** always generates the same encrypted value for a given plaintext value.
    - **Randomized encryption** uses a method that encrypts data in a less predictable manner.
  - b. **Encryption Key:** Chose the same key name as created in *Section 4.2.3: Create Column Encryption Key.*

|                              |   |           |                 |                 |              |            | _     |        |
|------------------------------|---|-----------|-----------------|-----------------|--------------|------------|-------|--------|
| 열표 Always Encrypted          |   |           |                 |                 |              | _          |       | ×      |
| Column Selection             |   |           |                 |                 |              |            |       |        |
| Introduction                 |   |           |                 |                 |              |            | 0 H   | lelp   |
| Column Selection             |   |           |                 |                 |              |            |       | _      |
| Master Key Configuration     | Search column name  |           |                 |                 |              |            |       |        |
| In-Place Encryption Settings | Apply one key to all cl   | necked    | columns:        |                 | Fortanix_CEK |            |       | $\sim$ |
| Run Settings                 |   |           |                 | Encryption Type | <b>(i)</b>   | Encryption | Key   | (j)    |
| Summary                      | Name  | State     | Encryption Type | Encry           | ption Key    |            |       |        |
| Results                      | <ul> <li>dbo.emplo</li> <li>first_na</li> <li>last_na</li> <li>emplD</li> <li>salary</li> </ul> | J Is only | Randomized      | • Forta         | nix_CEK      |            |       | •      |
|                              | _   | ĺ.        |                 |                 |              |            |       |        |
|                              |   |           |                 | < Previous      | Next         | >          | Cance | I      |

#### FIGURE 8: COLUMN SELECTION

- 4. Click the **Next** button.
- On the Run Settings screen, select the Proceed to finish now radio button and click the Next button.



| 🖽 Always Encrypted           | - 🗆 X  |
|------------------------------|--|
| Run Settings                 |  |
| Introduction                 | 🔞 Help   |
| Column Selection             |  |
| Master Key Configuration     | While encryption/decryption is in progress, write operations should not be performed on a table.       |
| In-Place Encryption Settings | this encryption/decryption operation during your planned maintenance window.                           |
| Run Settings                 |  |
| Summary                      |  |
| Results                      |  |
|                              | Select how you would like to proceed O Generate PowerShell script to run later O Proceed to finish now |
|                              | < Previous Next > Cancel   |

FIGURE 9: RUN SETTINGS

6. On the **Summary** screen, wait until the results are processing.



| _  |  |     |        |      |
|--|--|-----|--------|------|
| Malways Encrypted  |  | -   |        | ×    |
| Introduction<br>Column Selection<br>Master Key Configuration<br>In-Place Encryption Settings<br>Run Settings<br>Summary<br>Results | Verify the choices made in this wizard.<br>Click Finish to perform the operations with the following settings:<br>Source database settings<br>Source database name: employee<br>Generate PowerShell script<br>Script location: C:\Users\Administrator\Documents\<br>Script name: decrypt_generated.ps1<br>Encrypt column salary<br>Table name: employee<br>Encryption key name: Fortanix_CEK<br>Encryption type: Randomized<br>Oversting media Clinat into |     | @ H    | lelp |
|  | Coperation mode: Client-side   | ich | Cancel |      |
|  | < Previous Fini  | ish | Cancel | 1    |

FIGURE 10: SUMMARY

7. Click the **Finish** Button to view the results.

#### **Fortanix**



FIGURE 11: RESULTS

#### 4.3.5 VERIFY ALWAYS ENCRYPTED COLUMNS

Perform the following steps on the testing server or the application server to view

encrypted columns in plain text format:

**NOTE:** Ensure that the Fortanix CNG 64-bit client must be installed and configured with Fortanix endpoint and API key.

- 1. Log into the Windows 10 professional machine.
- 2. Install Fortanix Client 64-bit CNG Client. For more information, refer to *Section 4.2: Fortanix CNG Client*.
- 3. Run the following command to install the SQL Server PowerShell module:

install-Module -Name SqlServer -AllowClobber

4. Use the following sample script to decrypt the data:

```
# Import the SqlServer module.
Import-Module "SqlServer"
# Connect to your database.
$serverName = "<server_name>"
```



```
$databaseName = "<database_name>"
# Change the authentication method in the connection string, if
needed.
$connStr = "Data Source=$serverName;Initial
Catalog=employee;Integrated Security=True;Column Encryption Setting
= Enabled"
#Tesing using SQL login
#$pwd = read-host -AsSecureString -Prompt "Password"
#$connStr = "Data Source=$serverName; User Id=applogin;Initial
Catalog=$databaseName; Password
=Fortanix123!;TrustServerCertificate=true;Column Encryption Setting
= Enabled"
# Invoke the query to view the encrypted data
Invoke-Sqlcmd -ConnectionString $connStr -Query "SELECT * FROM
dbo.employee" | Format-Table -AutoSize
```

PS C:\Users\Administrator\Documents> .\decrypt.ps1

| У |
|---|
| - |
| 0 |
| 0 |
| 0 |
| 0 |
|   |

#### 4.3.6 ROTATE ALWAYS ENCRYPTED KEY

Rotating the Always Encrypted Keys is the process of replacing an existing key with a new one. You may need to rotate a key if it has been compromised, or to comply with your organization's policies or compliance regulations that mandate that the cryptographic keys must be rotated regularly.

- **Rotate column encryption key**: This involves decrypting the existing data with current key and re-encrypting it using the new column encryption key.
- Rotate column master key: This involves decryption the column encryption key and protecting it with new column master key. For more information, refer to <u>https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/rotate-</u> <u>always-encrypted-keys-using-ssms?view=sql-server-ver16</u>. Perform the following steps:
  - 1. **Creating New Column Master Key:** Create new security object in Fortanix DSM as described in *Section 4.2.2: Create Column Master Key*.

| ← → C 🔒 sdkms.fortar                     | nix.com/#/sobjects/7c7ffb8e-5903-48b4-9f62-2a829aa8c370                                 |  |
|--|---|--|
| Fortanix<br>Data Security Manager        | Account Administration  |  |
| ② Dashboard                              | jacijem y i Savetlje Openi V Sevanski poljen<br>pre-vetire active deschvated destrinjed |  |
| Integrations                             | Always_Encrypted_Key_Database_Name_v2   |  |
| 品 Groups                                 |   |  |
| 🗁 Apps                                   | UUID: 7c7ffb8e-5903-48b4-9f62-2a829aa8c370 D COPY ID V ①                                |  |
| Security Objects<br>Keys, Secrets, Certs | Activity chart  |  |
| ③ Users                                  |   |  |
| Plugins                                  | INFO ATTRIBUTES/TAGS KEY ROTATION KEY ACCESS JUSTIFICATION                              |  |
| ි Tasks                                  | Enabled 💿   |  |
| 🗿 Audit Log                              | (No description) 🖉  |  |
| ⊗ <sup>®</sup> Settings                  | Type RSA ③ Size 2048 bits KCV -   | Activity Logs C Less updated: 11:33 pm<br>Less used: June 26th 2023, 11:32:04 pm   |
|  | 🙄 DOWNLOAD PUBLIC KEY 🤣 REMOVE PRIVATE KEY  | Keep detailed log for the object   |
|  | Dublic key published  | USM will keep a full audit log for this object. You can disable logging to increas |
|  | Padding Policy  | App "MS-SQL Demo" created key "Always_Encrypted_Key_Datab.                         |
|  | Encryption 🛛 PKCS1v15, 🖾 Raw (Decryption only), 🖾 OAEP Hashing Algorithm all            |  |
|  | Signature 🗹 PKCS1v15, 🗹 PSS Hashing Algorithm all                                       |  |
|  | EDIT  |  |
|  | Group   |  |
|  | P Massi a   |  |

FIGURE 12: KEY CREATED ON FORTANIX DSM



| Object Explorer 👻 🕂 🗙   | SQLQuery2.sql - ECAdministrator (63))*          |  |  |
|---|---|--|--|
| Connect - # ×# = ⊤ ¢ →  | select* from employee                           |  |  |
| C R EC20M07-01-C7511 (SOL Server 15.0.4261.1 - EC20M07-01-C78.+ |   |  |  |
| Databases   |   |  |  |
| System Databases  | P New Column Master Key - X                     |  |  |
| Database Spanshots  |   |  |  |
|   | Setect a page I Script 👻 🕜 Help                 |  |  |
|   |   |  |  |
| E Tables  |   |  |  |
| 🕫 📕 System Tables   | Name: Fortanc_CMK_V2                            |  |  |
| 🕫 🛑 FileTables  |   |  |  |
| 🕫 📕 External Tables   | Key store: Key storage trovider (LNG) V Hetresh |  |  |
| 🗑 🛑 Graph Tables  |   |  |  |
|   |   |  |  |
| 🗑 🛑 Columns   | Select a provider:                              |  |  |
| 🕀 💼 Keys  | Fortanix KMS CNG Provider V                     |  |  |
| 🕀 📁 Constraints   |   |  |  |
| 🗉 💼 Triggers  | Name  |  |  |
| Indexes   | Always_Encrypted_Key_Database_Name              |  |  |
| E Statistics  | Aways_Encrypted_Key_Database_Name_v2            |  |  |
| Uiews   |   |  |  |
| External Resources  |   |  |  |
| 🗉 📕 Synonyms  |   |  |  |
| 🗉 📁 Programmability   |   |  |  |
| 🛞 🗰 Service Broker  | 100 % - Connection                              |  |  |
| 🗉 💼 Storage   | III Results All Messages Server                 |  |  |
| 😑 🗰 Security  | first name emplo                                |  |  |
| 😠 💼 Users   | 1 Alam Poles 1 Connection                       |  |  |
| 🗉 💼 Roles   | 2 Advan Parkar 1 EC2AMA2-OLC7E1L\Administrato   |  |  |
| 🗉 💼 Schemas   | 2 Julia Das 2 Mil Vew connection properties     |  |  |
| 🗉 💼 Asymmetric Keys   |   |  |  |
| E Certificates  | 4 Peter Villams 2                               |  |  |
| 😠 🛑 Symmetric Keys  |   |  |  |
| Always Encrypted Keys   | Progress  |  |  |
| 🖂 📕 Column Master Keys  | de Park   |  |  |
| # Fortanix_CMK  | Preduy Control March 1                          |  |  |
| 😑 🗰 Column Encryption Keys                                      | Generate Key                                    |  |  |
| a <sup>g</sup> Fortanix_CEK                                     |   |  |  |
| Database Audit Specifications                                   | OK Capel  |  |  |
| Secunty Policies  |   |  |  |
| Security  |   |  |  |
| Server Objects  |   |  |  |
| Explication   |   |  |  |
| 🗉 🔲 Polybase  |   |  |  |
| Always Un High Availability                                     |   |  |  |
|   |   |  |  |

FIGURE 13: KEY CREATED ON SQL SERVER

- 2. **Rotating the Key:** After the key is rotated, the affected column encryption key will have two encrypted values: one value encrypted with the existing column master key, and a new value encrypted with the new column master key.
  - a. Navigate to the Security  $\rightarrow$  Always Encrypted Keys  $\rightarrow$  Column Master Keys folder and locate the column master key that you want to rotate.
  - b. Right-click on the column master key and select the **Rotate** option.
  - c. In the Column Master Key Rotation dialog box, select the name of your new column master key that you created in *Step 1: Creating New Column Master Key in the Target field*.
  - d. Review the list of the column encryption keys, protected by the existing column master keys. These keys will be affected by the rotation.
  - e. Click the **OK** button.

#### DSM INTEGRATION WITH MSSQL SERVER ALWAYS ENCRYPTED



FIGURE 14: ROTATE THE KEY

- 3. Configure Application with New Column Master Key: Ensure that all your client applications query database columns that are protected with the rotated Fortanix column master key can access the new column master key. The column master key is stored in Fortanix DSM, the application must be implemented so that it can authenticate to Fortanix DSM and has permission to access the new column master key.
- 4. **Cleaning Up:** After you have configured all your applications to use the new column master key, remove the values of column encryption keys that are encrypted with the old column master key from the database. Removing old values will ensure that you are ready for the next rotation.

**NOTE:** Each column encryption key is protected with a column master key to be rotated, must have exactly one encrypted value.

**WARNING:** If you remove the value of a column encryption key before its corresponding column master key has been made available to an application, the application will no longer be able to decrypt the database column.



- a. Navigate to the **Security**  $\rightarrow$  **Always Encrypted Keys** folder and locate the existing column master key that you want to replace.
- b. Right-click on your existing column master key and select the **Cleanup** option.
- c. Review the list of column encryption key values to be removed.
- d. Click the **OK** button.

| Object Explorer 👻 म 🗙   | SQLQuery2.sql - ECAdministrator ( | 53))* 😐 🗙 SQLQuery1.sql - EC                    | Administrator (60))   |
|---|-----------------------------------|---|---|
| Connect - ∓ ×∓ = ⊤ C →  | select* from employee             |   |   |
| R FC2AMA7-01 C7E1L (SOL Server 15 0 4261 1 - FC2AMA7-01 C7L A |                                   |   |   |
| Databases   |                                   |   |   |
| System Databases  |                                   | - Column Master Key Cleanu                      | ip - Fortanix_CMK — 🗆 🗙   |
| 🗉 📕 Database Snapshots  |                                   | Select a page                                   |   |
| employee  |                                   | Selecta page                                    | Script ▼ (2) Help   |
| 🕢 📁 Database Diagrams   |                                   |   |   |
| 😑 💼 Tables  |                                   |   | Cleaning up after a column master key rotation will delete all key values already   |
| 🗉 🗰 System Tables   |                                   |   | encrypted with a second master key. Ensure that the second column master key is   |
| 😠 🗰 FileTables  |                                   |   | deployed to all necessary computers before performing this step, as all computers still<br>using the first master knowill be lenger be able to depart data protected using its column |
| 🕢 💼 External Tables   |                                   |   | using the inscritaster key will no longer be able to decrypt data protected using its column  |
| 😠 🗰 Graph Tables  |                                   |   | Retiring column master key: Fortanix_CMK  |
| dbo.employee  |                                   |   | A Values in hold will be cleaned up:  |
| 🕢 🗰 Columns   |                                   |   |   |
| 🕀 💼 Keys  |                                   |   | Name Encrypted Value 1 Encrypted Value 2  |
| E Constraints   |                                   |   | Fortanix_CEK Fortanix_CMK: 0x0178002 Fortanix_CMK_V2: 0x017E00780   |
| Triggers  |                                   |   |   |
| 🛚 🗰 Indexes   |                                   |   |   |
| E Mathematics   |                                   |   |   |
| E Views   |                                   |   |   |
| External Resources  |                                   |   |   |
| B Synonyms  |                                   |   |   |
| Programmability   | 100.84 - 4                        | C   |   |
| Service broker  | 100 /8 -                          | Connection                                      |   |
| Scorage     Scorage   | Hesults Bill Messages             | Server:   |   |
| - Security  | first_name last_name empli        | BCZAMIAZ-OLC/ETC                                |   |
| Roler   | 1 Adam Parker 1                   | Connection:<br>EC20M07 OL C7E1L) Administration |   |
| Schemas   | 2 Adam Parker 1                   | Lezzon ze occore ne o dana na data              |   |
| Asymmetric Keys   | 3 John Doe 2                      | YT View connection properties                   |   |
| Certificates  | 4 Peter Williams 2                |   |   |
| Symmetric Keys  |                                   |   |   |
| Always Encrypted Keys   |                                   | Program   |   |
| 😑 💼 Column Master Keys  |                                   | Trogress  |   |
| + Fortanix_CMK  |                                   | Ready   |   |
| +     Fortanix_CMK_V2   |                                   | 10 A B B.                                       |   |
| 🖃 🛑 Column Encryption Keys                                    |                                   |   |   |
| B Fortanix_CEK  |                                   |   | OK Cancel   |
| Database Audit Specifications                                 | UK Lancel                         |   |   |
| B Security Policies   |                                   |   |   |
| Escurity  |                                   |   |   |
| Server Objects  |                                   |   |   |
| Keplication   |                                   |   |   |

FIGURE 15: CLEAN UP

5. After Rotation: To verify if that rotation is done successfully, refer to the

following figures:

a. Column Master Key:

#### DSM INTEGRATION WITH MSSQL SERVER ALWAYS ENCRYPTED

| Object Explorer 👻 👎 🗙  | SQLQueryZ.sql - ECAdministrator (63))* + × SQLQuery1.sql - ECAdministrator (60))   |  |   |
|--|--|--|---|
| Connect - ₩ ×₩ = ▼ C →   | select* from employee  |  |   |
| EC2AMAZ-OLCTELL (SOL Server 15.0.4261.1 - EC2AMAZ-OLCTLA   |  |  |   |
| Databases  |  |  |   |
| 🕞 🛑 System Databases   | ** Column Master Key Properti  |  | ties - Fortanix_CMK_V2 - 🗆 🗙  |
| Database Snapshots   |  | Calculation and  |   |
| employee   |  | Select a page  | 💭 Script 🔻 😯 Help   |
| 🛞 🛑 Database Diagrams  |  |  |   |
| 😑 📁 Tables   |  |  | Name: Epitanix CMK V2   |
| 🗉 🗰 System Tables  |  |  | Created: 6/26/2023 11:34:56 PM  |
| FileTables   |  |  | Key store provider: MCSOL CNG STOPE                                       |
| 😠 🛑 External Tables  |  |  | Key adde provider. Middae_chica_aronec                                    |
| 🕀 🗰 Graph Tables   |  |  | Ney pair. Forcerix Nets Creat Forder Away8_DICtypted_Ney_Database_Name_V2 |
| 😑 🎹 dbo.employee   |  |  |   |
| 🕀 🗮 Columns  |  |  | Encrypted column encryption keys  |
| 🗉 🗰 Keys   |  |  | Name Algorithm Encrypted Value  |
| E Constraints  |  |  | Endoring CEK BSA DAER 0x017E0000 A540CA7D5E89265214144CEE9812895          |
| 🕀 💼 Triggers   |  |  |   |
| Indexes  |  |  |   |
| E Matistics  |  |  |   |
| Views  |  |  |   |
| External Resources   |  |  |   |
| B Synonyms   |  |  |   |
| Programmability  | 100.86   | Constant   |   |
| Service broker   | 100 /8 1   | Connection   |   |
| E Storage  | Hesuts B Messages  | Server:  |   |
| B Blogr  | first_name last_name empl  | DECZAMAZIOLC/ETC   |   |
| Boler  | 1 Adam Parker 1  | Connection:<br>EC20M0Z/OLC7E1L\Administrato  |   |
| Schemas  | 2 Adam Parker 1  | U II   |   |
| Asymmetric Keys  | 3 John Doe 2   | View connection properties   |   |
| Certificates   | 4 Peter Williams 2   |  |   |
| 🗉 🛑 Symmetric Keys   |  |  |   |
| Always Encrypted Keys  |  | Program  |   |
| 🗉 📁 Column Master Keys   |  | Trogress   |   |
| +• Fortanix_CMK  |  | Ready  |   |
| - Fortanix_CMK_V2  |  | .04B.0.  |   |
| 😑 📁 Column Encryption Keys   |  |  |   |
| B <sup>®</sup> Fortanix_CEK  |  |  | OK Commit   |
| 🗉 🛑 Database Audit Specifications  |  |  | OK Cancel   |
| 🛞 🗰 Security Policies  |  |  |   |
| 🗉 📕 Security   |  |  |   |
| B Server Objects   |  |  |   |
| <ul> <li>Stonge</li> <li>Stonge</li> <li>Securty</li> <li>Uses</li> <li>Reles</li> <li>Schemas</li> <li>Azymmetric Keys</li> <li>Certificates</li> <li>Symmetric Keys</li> <li>Certificates</li> <li>Symmetric Keys</li> <li>Column Matter Keys</li> <li>Fortanic, CMK</li> <li>Fortanic, CMK</li> <li>Column Comption Keys</li> <li>Schemary Security Policies</li> <li>Security</li> <li>Security</li> </ul> | Time         Peak.org         Set Messages           fmt_rame         bst_rame         expl           1         Adam         Parker         1           2         Adam         Parker         1           3         John         Parker         2           4         Peter         Williams         2 | Sever:<br>ECJMA2OLC7E1L<br>Corrector:<br>ECJMA2OLC7E1LV4ministrato<br>₩ Mex.connection procedies<br>Progress<br>Progress | OK Cancel   |

FIGURE 16: COLUMN MASTER KEY

#### b. Column Encryption Key:

| Object Explorer 👻 🖣 🗙  | SQLQuery2.sql - ECAdministrator                         | (63))* 😐 🗶 SQLQuery1.sql - EC.   | Administrator (60))  |
|--|---|--|--|
| Connect - ₩ ×₩ = ▼ C ++                                      | select* from employee                                   |  |  |
| □ ■ EC2AMA7+0LC7E1L(SOL Server 15.0.4261.1 + EC2AMA7+0LC7E A |   |  |  |
| Databases  |   |  |  |
| 🗑 🛑 System Databases   | 📲 Column Encryption Key Properties - Fortanix_CEK – 🗆 🗙 |  | operties - Fortanix_CEK - 🗆 🗙  |
| 🗉 📁 Database Snapshots                                       |   | Selectanore  |  |
| 😑 🗑 employee   |   | bereet a page  | 👖 Script 🔻 🚱 Help  |
| 🛞 💼 Database Diagrams  |   |  |  |
| 😑 💼 Tables   |   |  | Name: Fortanix CEK   |
| 🗉 🗰 System Tables  |   |  | Constant: 6/26/2022 E-12-00 EM                                       |
| 🕀 💼 FileTables   |   |  | Created. 0/20/2023 0.13.00 PM  |
| 🕀 📁 External Tables  |   |  | Last modified: 6/28/2023 7:03:07 AM                                  |
| 🕀 💼 Graph Tables   |   |  | Economical values  |
| dbo.employee   |   |  | Colors   |
| E Columns  |   |  | Master Key Algorithm Encrypted Value                                 |
| E 📫 Keys   |   |  | Enderix CMK V2_RSA_04EP0x017E00000166006E007200740061006E00690078002 |
| Constraints  |   |  |  |
| Triggers   |   |  |  |
| Indexes  |   |  |  |
| Statistics   |   |  |  |
| Views  |   |  |  |
| External Resources   |   |  |  |
| Synonyms     Beersmanhility                                  |   |  |  |
| E Service Broker   | 100 % + 4   | Connection   |  |
| G Storage  | TTT Dan de roll Manager                                 | Connection   | Economian columna  |
| E Security   | III Houdio El Messages                                  | EC2AMAZ-OLC7E1L  | Colora Column  |
| 🕀 📁 Users  | first_name_last_name_empl                               | Constant of Consta | Column Encryption Type Agontim                                       |
| 🕀 🗰 Roles  | 1 Adam Parker 1   | EC2AMAZ-OLC7E1L\Administrato   | [salary] Randomized AEAD_AES_256_CBC_HMA                             |
| 🕀 📕 Schemas  | 2 Adam Parker 1   | Was connection properties  |  |
| Asymmetric Keys  | 3 John Doe 2  | TT IST SOTTONIC PRODUCT  |  |
| E Certificates   | 4 Peter Williams 2                                      |  |  |
| 🕀 🗰 Symmetric Keys   |   |  |  |
| 🖃 📕 Always Encrypted Keys                                    |   | Progress   |  |
| 😑 🚞 Column Master Keys                                       |   | ATTA Baady   |  |
| * Fortanix_CMK   |   |  |  |
| +     Fortanix_CMK_V2  |   | -0-  |  |
| Column Encryption Keys                                       |   |  |  |
| B* PORTANO_CEK   |   |  | OK Cancel  |
| Database Audit Specifications                                |   |  |  |
| Security Fondes  |   |  |  |
| Security     Security  |   |  |  |
| Replication  |   |  |  |
| PolyBase   |   |  |  |
| Always On High Availability                                  |   |  |  |
| Management   |   |  |  |
| Integration Services Catalogs                                |   |  |  |
|  | Query executed successfully.                            |  | EC2AM  |
|  |   |  |  |

#### FIGURE 17: COLUMNS ENCRYPTION KEY

#### 5.0 DOCUMENT INFORMATION

#### 5.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL: <u>https://support.fortanix.com/hc/en-us/articles/16916974311700-Fortanix-Data-Security-Manager-</u> <u>with-Microsoft-SQL-Server-Always-Encrypted</u>

#### 5.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle. For any urgent document updates, send an email to: <a href="mailto:support@fortanix.com">support@fortanix.com</a>

© 2016 – 2023 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc. All other trademarks are the property of their respective owners.

**NOTICE**: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform <u>info@fortanix.com</u> immediately.