FORTANIX TECHNICAL DOCUMENTATION

Fortanix

Integration Guide

USING DATA SECURITY MANAGER WITH MSSQL SERVER TDE – STANDALONE SERVER

VERSION 1.0



TABLE OF CONTENTS

1.0		2
2.0	ENABLING SQL FEATURES	2
3.0	CREATING CRYPTOGRAPHIC PROVIDER	3
4.0	CREATING CREDENTIALS (SYSADMIN)	4
5.0	CREATING ASYMMETRIC KEYS (MEK)	7
6.0	CREATING CREDENTIALS (DB ENGINE)	8
7.0	CREATING LOGIN (DB ENGINE)	9
8.0	CREATING SAMPLE DATABASE	10
9.0	CREATING DATA ENCRYPTION KEY (DEK)	11
10.0	ENABLING TDE ON DATABASE	12
11.0	MONITORING TDE PROGRESS	12
12.0	DOCUMENT INFORMATION	14
12.1	Document Location	14
12.2	Document Updates	14

1.0 INTRODUCTION

This document is a step-by-step guide to implement Microsoft SQL Transparent Data Encryption (TDE) using the Fortanix DSM.



NOTE: Ensure that you have performed the steps from *Data Security Manager with MSSQL TDE Integration Guide – Before You Begin Guide.*

2.0 ENABLING SQL FEATURES

Run the following commands if Extensible Key Management (EKM) is not supported or enabled in the SQL Server Edition:

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



FIGURE 1: RUN COMMANDS FOR ERROR SCENARIO

3.0 CREATING CRYPTOGRAPHIC PROVIDER

Run the following commands to use the correct location of the EKM DLL:

```
CREATE CRYPTOGRAPHIC PROVIDER EKM_Prov
FROM FILE = 'C:\Program Files\Fortanix\KmsClient\FortanixKmsEkmProvi
der.dll';
GO
```

Where,

• EKM Prov refers to the name of the provider defined by the user.



FIGURE 2: CREATE CRYPTOGRAPHIC PROVIDER

4.0 CREATING CREDENTIALS (SYSADMIN)

This section describes the steps to create the credentials to generate the Master Encryption Key (MEK) on the Fortanix DSM using the SQL administrator.

The SQL administrator requires permission to connect to Fortanix DSM to generate the key.

- 1. Perform the following steps to get the API key:
 - a. Log in to the Fortanix DSM.
 - b. From the UI left panel, click the **Apps** tab.
 - c. Click **COPY API KEY** to copy the API key of your application and then paste the DSM API key as the value for the SECRET parameter in the next command.

MS-SQL Demo default / REST API		
D. e1893d42-ed10-4995-b464-d7df7e851dc6 D		
vity chart 🗸		
O SECURITY OBJECTS USAGE		
Enabled 🖑 (No description) 🖉		
ADI Key		Activity Logs 🕑 Last updated: 12:28 pm
MF LINGY	use to create applications	Last login: Never
bick provides cools, compliers, needers, noral res, code samples, and a new nep system checkeveropers can	use to create applications.	
COPY API KEY		
Change authentication method 🗸		
Groups	App permissions:	
基 MS-SQL Demo Default group 원	A	
	EDIT GROUPS	
OAuth		
Using OAuth users can authorize this app to perform actions on their behalf		
OAuth enabled		
	EDIT	
All Developer Resources	EDIT	
All Developer Resources DSM developer resources DSM developer resources provides libraries, example code and documentation that developers can use to integrate their ap following link to whit DSM resources page.	EDIT	
All Developer Resources DSM developer resources provides libraries, example code and documentation that developers can use to integrate their ap librowing link to visit DSM resources page.	EDIT	

FIGURE 3: COPY API KEY

2. Run the following commands to create a credential using the copied API key in your SQL Server Studio that will be used by the system administrators:

```
CREATE CREDENTIAL sa_ekm_tde_cred
WITH IDENTITY = 'Identity1',
SECRET = '<DSM API KEY>'
```

```
FOR CRYPTOGRAPHIC PROVIDER EKM_Prov ;

GO

SQLQuey7xql-M.17MMSQL2017(53)" * ×

CREATE CREDENTIAL sa_ekm_tde_cred

WITH IDENTITY = 'Identity1',

SECRET = 'NTEyMDJmN2QtNTkyMi002DdhLTg0MDUtODg1MTY2YmYxZDhi0lQ2N3FaU2JGdFUwRDRVZWtKdXNK

FOR CRYPTOGRAPHIC PROVIDER EKM_Prov ;

GO

Solution for the second successfully.

Solution for the second successfully.

SSQL2017(14.0 RTM) MSSQL2017(53) MSSQLLAB 000000 0rows
```

FIGURE 4: CREATE CREDENTIAL

3. Add the credential to a high privileged user such as your own domain login in the

format [DOMAIN\login]:

```
ALTER LOGIN "<Domain>\Administrator"
ADD CREDENTIAL "sa_ekm_tde_cred";
GO
```

Run the following commands in case there is no domain, and the machine is part of a workgroup or standalone:

```
ALTER LOGIN "LOCALHOST\Administrator"
ADD CREDENTIAL "sa_ekm_tde_cred";
GO
```



FIGURE 5: COMMAND FOR NO DOMAIN

If you are not an administrator and hence unable to alter the login, open the Object

Explorer and map the credentials as shown in the following image:

2. 52.172.32.101 (ms2014ent)	3. 62.172.140.254 (MSSQL2017)	(3)						Ø
X Detach tab Q Toggle scaling 50 Fulso	reen 💷 Fit to window size 🔍 Set conne	ction password 🕴 Hide bar	X Disconnect					
45	SQLQuery15.sq	I - SQL2014Enterpr.master (SQL2014Enterpr\ms2014er	nt (58))* - Microsoft SQL Server M	Management Studio	o (Administrator)		= 0 X
File Edit View Project Debug Tools	Window Help							
🗄 🔂 • 🔄 • 😅 🛃 🥔 🔔 New Query 📋	B & & B & B	(四·马) (四) > (- 109	· Q3** .			
1 3/ 12/ master - 1	Execute > Debug = > 10 = 1	174000122	連課 44 。					
Object Explorer 🔹 🕴 🗙	SQLQuery15.sql - Srpr\ms2014ent (58))	0	Login Properties - SQL2	014Enterpr\ms2014ent	_ 0 X		- Properties	- # ×
Connect * 2 2 = 7 2 3	ALTER LOGIN "SQL2014Enters ADD CREDENTIAL sa_ekm_tde	Select a page	🔄 Script 👻 🚺 Help				Current connection	parameters •
Databases	60	Server Roles	Login name:	SGL2014Enterprism2014ent	Search.		Aggregate State	u.
🗄 🧰 Logins		Status	 Windows authentication 				Elanced time	00-00-00.015
##MS_PolicyEventProcessingLogin			 SQL Server authentication 				E Finish time	12/24/2019 8:00:18 AM
A NT AUTHORITY/SYSTEM			Password:				Name	SQL2014Enterpr
A NT Service\MSSQLSERVER			Confirm password				Rows returned	0
A NT Service\SQLlaaSExtensionQuery			Specify old password				Start time	12/24/2019 8:00:18 AM
A NT SERVICE/SQLSERVERAGENT			Old password.				State	Open
A NT SERVICE (SQLWIRE)	100 % • <		Enforce password polic	9		3	Connection nam	e SOL2014Enterpr (SOL20
📥 sa	La Messages		Enforce password expir	ation			 Connection Det 	ails
SQL2014Enterpr\ms2014ent	Msg 33042, Level 16, State		User must change pain	oword at next login			Connection elap	s- 00:00:00.015
E Server Roles	Cannot add credential becaus		O Mapped to certificate		~		Connection finis	h 12/24/2019 8:00:18 AM
at sa ekm tde cred			O Mapped to asymmetric key		~		Connection rows	+ 0
a 🔄 Cryptographic Providers		Connection	Map to Credential		▼ Add		Connection start	1 12/24/2019 0:00:10 AM
KM_Prov		Secure	Mapped Credentials	Condential Provider			Display name	SQL2014Enterpr
Audits	1	SQL2014Enterpr		sa_ekm_tde_cred EKM_Prov		• ·	Login name	SQL2014Enterpr\ms2014
Server Objects		Connection:					Server name	SQL2014Enterpr
3 Replication	100 % ~ <	SQL2014Enterpr/ms2014ent				>	Server version	12.0.6329
AlwaysOn High Availability	Duery completed with errors.	Vew connection properties				ns2014e master 00:00:00 0 rows	SPID	58
Output		Progress			Remove	- a	×	
Show output from: Debug	- 3 S	Ready	Default database:	master	~			
Auto-attach to process '[2936] [50	L] SQL2014Enterpr' on machine 'S	100	Default language:	English	~		^	
The thread 'SQL2014Enterpr [55]' (0x4dc) has exited with code 0 (0			19 - 22 - 19 - 19 - 19 - 19 - 19 - 19 -				
The program '[2936] [SQL] SQL2014E	nterpr: SQL2014Enterpr' has exit			OK	Cancel			
	1						-	
							Name	
							The name of the con	inection.
						/		
Ready								
							• Re 10	ENG 12/24/2019
500	A. 11							12 24 2017

FIGURE 6: MAP CREDENTIALS

5.0 CREATING ASYMMETRIC KEYS (MEK)

The MSSQL admin has the credentials associated with creating the Master Encryption Key (MEK) on Fortanix DSM. This section describes the steps to create the asymmetric keys.

Run the following commands to create an asymmetric key stored inside the EKM provider:

```
USE master;
GO
CREATE ASYMMETRIC KEY ekm_login_key
FROM PROVIDER [EKM_Prov]
WITH ALGORITHM = RSA_2048,
PROVIDER_KEY_NAME = 'SQL_Server_Key';
GO
```

Where,

- ekm login key refers to the master key alias on the MSSQL database.
- EKM Prov refers to the Fortanix EKM Provider.
- SQL Server Key refers to the key created on the Fortanix DSM.



For example:

USE master; GO CREATE ASYMMETRIC KEY ekm_login_key_v1 FROM PROVIDER [EKM_Prov] WITH ALGORITHM = RSA_2048, PROVIDER_KEY_NAME = 'SQL_Server_Key_v1'; GO

5	SQLQuery11.sql - SQL2014Enterpr.master (SQL2014Ente	rpr\ms2014ent (55))* - Microsoft SQL Se	rver Management Studio (Administ	trator)
File Edit View Query Project Debug	Fools Window Help			
🗄 🛅 🔻 🕮 😁 🎯 🛃 🥥 🔔 New Query 📑	📸 📸 👗 🖦 🚵 🥙 - (* - 🚚 - 🖳 🌌 🕨	- 12	- 🔩 🕾 🎠 🖬 - 🖕	
1 💀 🙀 🛛 master 🔹 🕴	Execute 🕨 Debug 🔲 🗸 📅 🖷 🔒 📅 🖷 🍪 🖉 🍋 🚍 😫 🛱 🛱 🗸			
Object Explorer 👻 🕂 🗙	SQLQuery11.sql - Srpr\ms2014ent (55))* × SQLQuery20.sql - Srpr\ms2014ent (61))*	SQLQuery19.sql - Srpr\ms2014ent (56))*	SQLQuery18.sql - Srpr\ms2014ent (60))*	-
Connect · · · · · · · · · · · · · · · · · · ·	USE master ; GO ECREATE ASYMMETRIC KEY ekm_login_key FROM PROVIDER EKM_Prov WITH ALGORITHM = RS_2048, PROVIDER_KEY_MANE = "FORTANIX" ; GC			
F Security				N
🖃 🧰 Logins	100 % - <			>
##MS_PolicyEventProces	Messages			
TH AUTHORN System NT AUTHORN SysTeM NT Service/MSSQLSERVE NT Service/SQLasEXten NT SERVICE/SQLSERVER/ NT SERVICE/SQLSWriter NT SERVICE/SQLSWriter NT SERVICE/SQLSWriter NT SERVICE/SQLSWriter NT SERVICE/SQLSWriter NT SERVICE/SQLSWriter NT SERVICE/SQLSWriter	Command(s) completed successfully.			=
A SQL2014Enterpr\ms2014e				~
Server Roles	100 % - <			>
Credentials	Ouery executed successfully.	SQL2014Enter	pr (12.0 SP3) SQL2014Enterpr\ms2014e	master 00:00:01 0 rows
Output				- ₽ >
Show output from: Debug	- 2 2 3 3 -			
Auto-attach to process '[2936] [SQL]30[2014Enterppr' on machine 'SQL2014Enterpr' succeeded. The thread 'SQL2014Enterpr [55]' (0x4dc) has exited with code θ (0x0). The thread 'SQL2014Enterpr' [55]' (0x4dc) has exited with code θ (0x0). The program '[2936] [SQL] SQL2014Enterpr' has exited with code θ (0x0). ====================================				
<				× ×

FIGURE 7: CREATE ASYMMETRIC KEY

6.0 CREATING CREDENTIALS (DB ENGINE)

Run the following commands to create a credential that will be used by the database engine:

```
USE master;
CREATE CREDENTIAL ekm_tde_cred
WITH IDENTITY = 'Identity2',
SECRET = '<DSM API KEY>'
FOR CRYPTOGRAPHIC PROVIDER EKM Prov;
```

Where,

- ekm tde cred refers to the name of the credentials.
- Identity2 refers to the identity name. The value can be any name.
- EKM Prov refers to the Fortanix EKM Provider.
- SECRET refers to the Fortanix DSM API Key. *Refer to the "Section 4- Creating Credentials (SysAdmin)" to get the DSM API Key.*

	SQLQuery16.sql - SQL2014Enterpr.master (SQL2014	Enterpr\ms2014ent (59))* - Microsoft SQL Server Managen	nent Studio (Administrator)				
File Edit View Query Project Debug	Tools Window Help						
🗄 📷 🕶 🖅 🚅 🛃 🍠 🔔 New Query 👔	(1) * 回 * (2) J Mew Query) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1						
1 32 14 master • 1	Execute 🕨 Debug 😑 🗸 🎇 🖉 😓 🏋 🐴 🍈 🦉 🍈 🗮 😫 🗒 🚎						
			C) 2014 (51))+				
Uget taplorer Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 = 7 2 3 Connect → 2 2 2 2 = 7 2 3 Connect → 2 2 2 2 2 2 2 Connect → 2 2 2 2 2 2 2 2 Connect → 2 2 2 2 2 2 2 2 2 Connect → 2 2 2 2 2 2 2 2 Connect → 2 2 2 2 2 2 2 2 Connect → 2 2 2 2 2 2 2 Connect → 2 2 2 2 2 2 2 Connect → 2 2 Connect → 2 2 2 Connect → 2 2 Con	SULGuerylosq! - Sprimscilent(SM) X SULGuerylosq! - Sprimscilent(SM) BUSE asster ; ECREATE CREDENTITA = damity2', SECRET = 'UTEYMOTAW2QHITkylio27dHiLTg0HDutcog1MTY2YmYXZDhiOl FOR CRYPTOGRAPHIC PROVIDER EKM_Prov ;)* SQLQuery11sql-Srprivmsc014ent (55))* SQLQuery20sql- Q2N3FaU23GdFUwRDRVZNtKdXNOZXg4anVFYNU4HU03cN83LXRpQmdBV	Srpr/mx20146mt (b1))*				
ENCRYPTION RET			×				
E Logins	100 % • <	ш	>				
##MS_PolicyEventProces	Messages						
🎄 ##MS_PolicyTsqlExecutic	Command(s) completed successfully.		^				
M IN AU IHURI ITYSTIEM MT Service/MSSQLSERVE MT Service/SQLIAsExten MT SERVICE/SQLSERVER4 MT SERVICE/SQLWriter MT SERVICE/SQLWriter MT SERVICE/Winmgmt Sa			-				
SQL2014Enterpr\ms2014e			~				
E Server Roles	100 % - <		>				
Credentials	Query executed successfully.	SQL2014Enterpr (12.0 SP3) SC	22014Enterpr\ms2014e master 00:00:00 0 rows				
Output			* # X				
Show output from: Debug							
Auto-attach to process '[2936] [SC	DL1 SOL2014Enterpr' on machine 'SOL2014Enterpr' succeeded.						
The thread 'SQL2014Enterpr [55]' (The thread 'SQL2014Enterpr [55]' (The program '[2936] [SQL] SQL2014E	(0x4dc) has exited with code 0 (0x0). (0x4dc) has exited with code 0 (0x0). nterpr: SQL2014Enterpr' has exited with code 0 (0x0).		=				
1							
4			V				

FIGURE 8: CREATE CREDENTIAL FOR DATABASE ENGINE

7.0 CREATING LOGIN (DB ENGINE)

Run the following commands to create a login from an asymmetric key and map credentials to the login:

```
CREATE LOGIN EKM_Login
FROM ASYMMETRIC KEY ekm_login_key;
GO
ALTER LOGIN EKM_Login
ADD CREDENTIAL ekm_tde_cred;
GO
```

Where,

• ekm_login_key refers to the master key alias on MSSQL database. This key is already
created in "Section 5- Creating Asymmetric keys".

- EKM Login refers to the login name.
- ekm_tde_cred refers to the key created on the Fortanix DSM. This credential is already
 created in "Section 6- Creating Credentials".

56 - Carlos Carl	SQLQuery17.sql - SQL2014Enterpr.master	(SQL2014Enterpr\ms2014ent (57))* - Microsoft S	QL Server Management Studio (Administrator)	
File Edit View Query Project Debug	Tools Window Help			
🗄 🚼 🔻 🔠 🖉 🚅 🍠 🔔 New Query 📋	🖌 🖓 🖉 🖉 - 🕫 - 🖉 - 🖉 🖓 🖓		- 🔩 🕾 🏷 🖬 - 🖕	
1 💷 🔐 master 🔹 🕴	Execute 🕨 Debug 🔲 🗸 📅 👼 🔜 📅 🍓 🎧 🦉 🏠 🚍 😩	連連 私。		
Object Explorer 👻 후 🗴	SQLQuery17.sql - Srpr\ms2014ent (57))* × SQLQuery16.sql - Srpr\ms	2014ent (59))* SQLQuery15.sql - Srpr\ms2014ent (58))* SQLQuery11.sql - Srpr\ms2014ent (55))*	÷
Connect · · · · · · · · · · · · · · · · · · ·	CREATE LOGIN EW_Login FROM ASYMMETRIC KEY ekm_Login_key ; GO BAITER LOGIN EW/Login ADO CREDENTIAL ekm_tde_cred ; GO	ev nem (zz)) — secedarci, i znaji - smiph mozennem (zz)) – Jackach (Triagh - am (Printzek mein (22))	
ENCRYPTION KEY Security				~
😑 🚞 Logins	100 % * <			>
##MS_PolicyEventProces	🛅 Messages			
A = #WS_Poilery seprecutic A IT AUTHORYSYSTEM TY AUTHORYSYSTEM NT Service/MSSQLSERVE A IT Service/SQLsERVER A IT SERVICE/SQLEWriter A IT SERVICE/SQLEWriter A IT SERVICE/SQLEWriter A Sa	Command(s) completed successfully.			
SQL2014Enterpr\ms2014e				~
Gerdentials	100 % • <			>
	Query executed successfully.	SQL20	14Enterpr (12.0 SP3) SQL2014Enterpr\ms2014e master 00:0	00:00 0 rows
Output				- 4 ×
Show output from: Debug	- Q Q 🙀 🖃			
Auto-attach to process '[2396] [SQ The thread 'SQL2014Enterpr [55]' (The thread 'SQL2014Enterpr [55]' (The program '[2936] [SQL] SQL2014E	[1] SQL2014Enterpr' on mechine 'SQL2014Enterpr' succeeded. &vAdc) has exited with code 0 (0x0). 0x4dc) has exited with code 0 (0x0). nterpr: SQL2014Enterpr' has exited with code 0 (0x0).			
<				>
Ready				Ln 6

FIGURE 9: ADD NEW CREDENTIAL TO LOGIN

8.0 CREATING SAMPLE DATABASE

This section describes the steps for creating sample database to enable TDE.

1. Run the following commands to create database employee:

CREATE DATABASE employee

2. 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
```

殿	SQLQuery18.sql - SQL2014Enterpr.master (SQL2014Ente	rpr\ms2014ent (60))* - Microsoft SQL Server M	Aanagement Studio (Administrator)	
File Edit View Query Project Debug	Tools Window Help			
🗄 🛅 🕶 📨 🧀 🛃 🥥 🔔 New Query 🎲	📸 📸 🕹 🛍 🛍 🤊 - 🗠 - 💭 - 🖏 🚧 🕨	~ M	- 🟹 😤 🎾 🖬 - 🖕	
🕴 🔡 🔤 master 🔹 🕴 📍	Execute 🕨 Debug 😑 🧹 🎁 🖻 🔒 📅 🐴 🚳 🦉 🏹 🔲 🗮 😫 🛊 🗱 🖏			
Object Explorer 👻 म 🗙	SQLQuery18.sql - Srpr\ms2014ent (60))* × SQLQuery17.sql - Srpr\ms2014ent (57))*	SQLQuery16.sql - Srpr\ms2014ent (59))* SQLQu	ery15.sql - Srpr\ms2014ent (58))*	
Connect 🕶 🛃 🗒 🖉 👩 🎿	□CREATE TABLE employee (first_name VARCHAR(128),last_name VARCHAR	(128),empID DECIMAL,salary DECIMAL(6));		÷
🖃 🔀 SQL2014Enterpr (SQL Server 12.0.632 🔨	CREATE DATABASE employee			^
🖃 🚞 Databases	GO			
SQL2014Enterpr (SQL Server 12.0.6329.1 - 5	iQL2014Enterpr\ms2014ent)			
⊞ <mark>U</mark> master				-
🛞 📙 model				=
i i i i i i i i i i i i i i i i i i i				
Database Snapshots				
🗉 📋 employee 🗮 🗮				
ENCRYPTION KEY				_
🖃 🚞 Security	100.96			~
E Dogins				· · · · · · · · · · · · · · · · · · ·
##MS_PolicyEventProces	Messages Command(a) completed successfully			
NT AUTHORITY/SYSTEM	command(s) completed successfully.			Ê
A NT Service\MSSQLSERVE				
A NT Service\SQLIaaSExten				
NT SERVICE\SQLSERVER4				=
A NT SERVICE\SQLWriter				
MT SERVICE\Winmgmt				
58 S8				
Separ Poler				~
Credentials	100 % • (
< 111 >	Query executed successfully.	SQL2014Enterpr (12.	0 SP3) SQL2014Enterpr\ms2014e master 0	0:00:00 0 rows
Output				- 4 ×
Show output from: Debug	- \$ \$ \$ 🙀 🛒			
Auto-attach to process '[2936] [SQL] SQL2014Enterpr' on machine 'SQL2014Enterpr' succeeded.			^
The thread 'SQL2014Enterpr [55]' (0) The thread 'SQL2014Enterpr [55]' (0)	ix4dc) has exited with code 0 (0x0).			
The program '[2936] [SQL] SQL2014Er	hterpr: SQL2014Enterpr' has exited with code 0 (0x0).			=
1				
<				>

FIGURE 10: CREATE TABLE

9.0 CREATING DATA ENCRYPTION KEY (DEK)

Run the following commands to create the Data Encryption Key (DEK) that will be used for TDE:

```
USE employee
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER ASYMMETRIC KEY ekm_login_key ;
GO
```

Where,

- employee refers to the database name.
- ekm_login_key refers to the master key alias on the MSSQL database.

10.0 ENABLING TDE ON DATABASE

Run the following commands to alter the database to enable Transparent Data Encryption (TDE):

ALTE	ER	DATABASE	emp	oloyee
SET	ΕN	ICRYPTION	ON	;
GO				



FIGURE 11: ENABLE TDE

11.0 MONITORING TDE PROGRESS

SQL Server keeps track of the encryption progress, and we can pull that information by querying sys.dm_database_encryption_keys. Particularly 'Percent_Complete' and 'encryption_state' are the two columns that are required to understand the progress of TDE. 'encryption_state' column returns an integer value (0-6) which indicates the encryption status of the database and 'percent_complete' column tells us the percent completed of the DB encryption state change.

Encryption_state (int)	Description
0	No database encryption key present, no encryption
1	Unencrypted
2	Encryption in progress
3	Encrypted
4	Key change in progress
5	Decryption in progress
6	Protection changes in progress (The certificate or asymmetric key that is encrypting the database encryption key is being changed).

The following T-SQL statement can be used to monitor TDE progress or status:

```
SELECT DB_NAME(database_id) AS DatabaseName, encryption_state,
encryption state desc =
CASE encryption_state
        WHEN '0' THEN 'No database encryption key present, no enc
ryption'
        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'
         WHEN '6' THEN 'Protection change in progress (The certifi
cate or asymmetric key that is encrypting the database encryption ke
y is being changed.) '
        ELSE 'No Status'
        END,
percent complete, encryptor thumbprint, encryptor type FROM sys.dm d
atabase encryption keys
```

The output of this query comes handy to manage TDE.

12.0 DOCUMENT INFORMATION

12.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/12716572654228-Data-Security-Manager-with-Microsoft-SQL-Server-TDE-Guide-Standalone-Server

12.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com

© 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.