Fortanix®

Integration Guide

USING DATA SECURITY MANAGER WITH MSSQL SERVER TDE – BEFORE YOU BEGIN

VERSION 1.0

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052| United States of America | +1 (650) 943-2484 |
info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

This document describes the steps that must be performed before integrating Fortanix Data Security Manager (DSM) with Microsoft SQL Transparent Data Encryption (TDE).

1.1 PREREQUISITES

Ensure the following:

- The Fortanix CNG Client must be installed and configured.
- The port 443 must be accessible from the SQL target machine to Fortanix DSM.

PROTOCOL	INBOUND/ OUTBOUND	PORT NUMBER	LOAD BALANCER USE (YES/NO)	PURPOSE
TCP	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.

1.2 LIMITATIONS AND RESTRICTIONS

- You must be a highly privileged user (such as a system administrator) to create a database encryption key and encrypt a database. That user must be able to be authenticated by the EKM module.
- Upon startup, the database engine must open the database. To do this, you should create a credential that will be authenticated by the EKM and add it to a login that is based on an asymmetric key. Users cannot sign in using that login, but the database engine will be able to authenticate itself with the EKM device.
- If the asymmetric key stored by EKM Provider (Fortanix DSM) is lost, the database will not be able to be opened by SQL Server. Hence, it is recommended to never delete or edit SQL Server managed keys from Fortanix DSM manually. Even after key rotation, it is recommended to keep the old keys, so that older backups can be used in contingency scenarios.
- Access to install the Fortanix KMS Server file to configure it on the machine and user.

1.3 PERMISSIONS

This document uses the following permissions:

- To change a configuration option and run the `RECONFIGURE` statement, you must be granted the `ALTER SETTINGS` server-level permission. The `ALTER SETTINGS` permission is implicitly held by the System Administrator and the Server Administrator who hold fixed server roles.
- Requires `ALTER ANY CREDENTIAL` permission.
- Requires `ALTER ANY LOGIN` permission.
- Requires `CONTROL` permission on the database to encrypt the database.
- Requires `CREATE ASYMMETRIC KEY` permission.

2.0 FORTANIX CNG PROVIDER

The Fortanix CNG Provider must be installed on every target machine. Refer to https://support.fortanix.com/hc/en-us/articles/360018084132-CNG-EKM 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.

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.

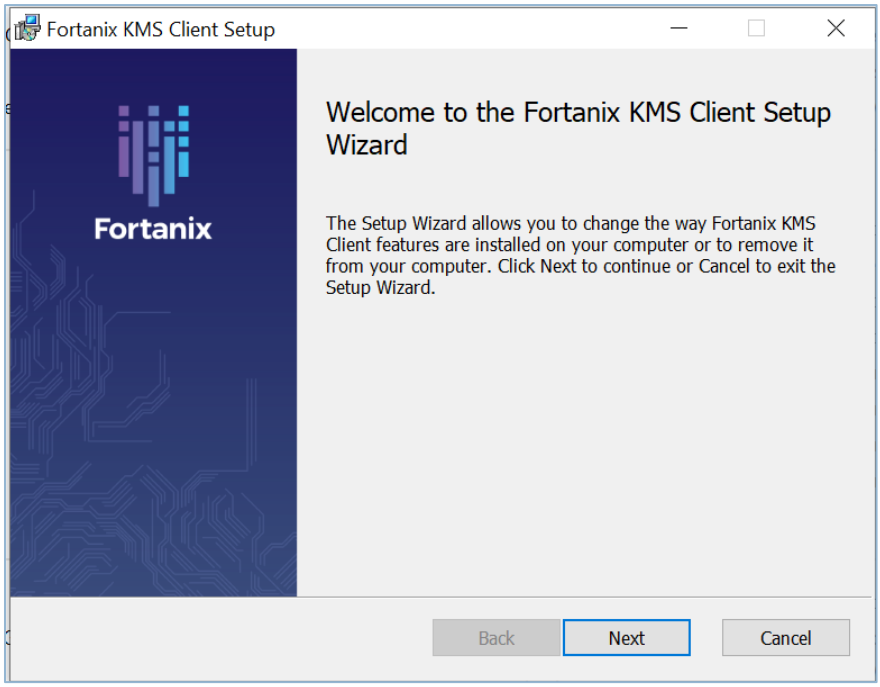

FIGURE 1: FORTANIX KMS CLIENT SETUP

2. Select the checkbox for **I accept the terms in the License Agreement** and click the **Next** Button.

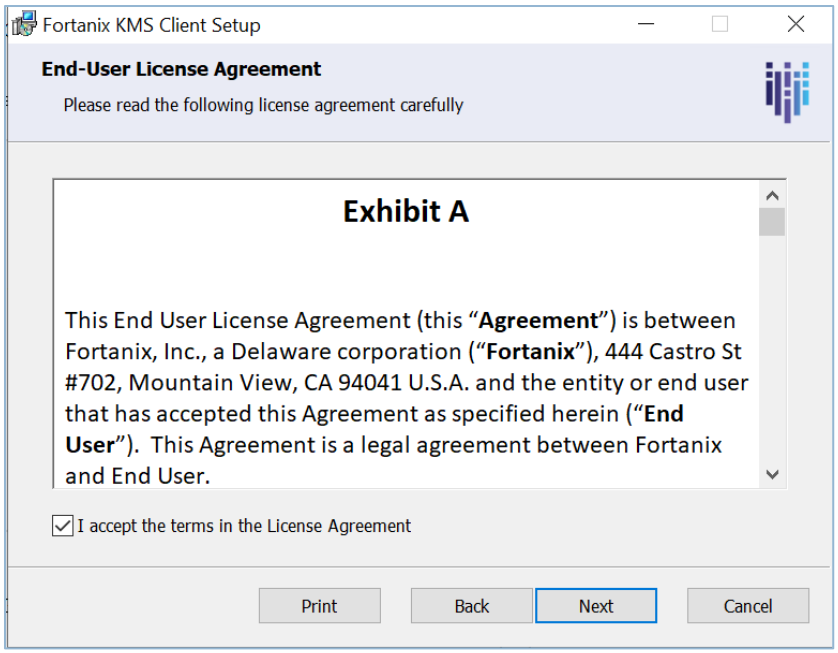

FIGURE 2: FORTANIX KMS CLIENT SETUP

3. Enter the location for installing the **Fortanix KMS Client** as **C:\Program Files\Fortanix\KMS Client**.

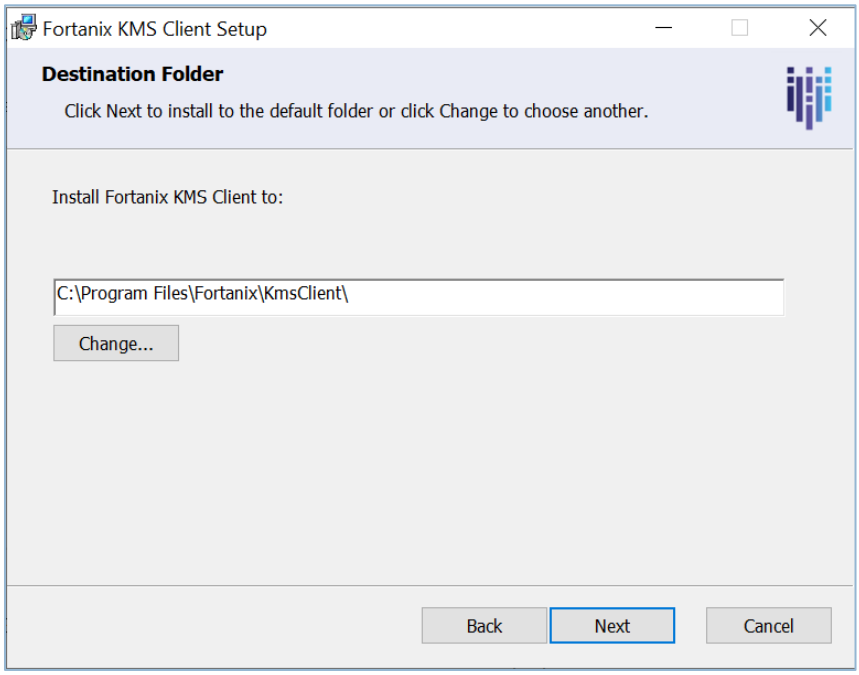

FIGURE 3: FORTANIX KMS CLIENT SETUP

4. Click the **Install** button to install the Fortanix KMS client.

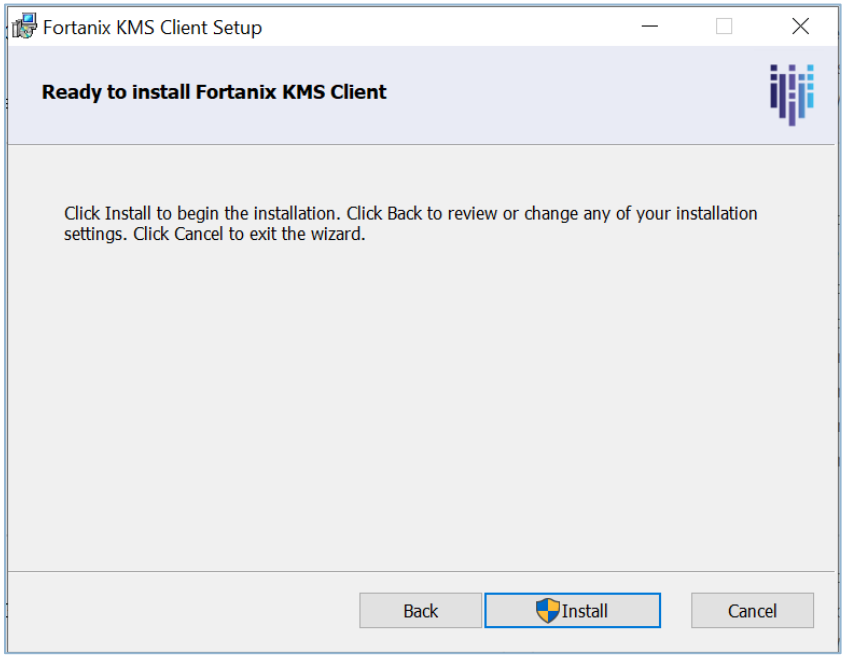

FIGURE 4: FORTANIX KMS CLIENT SETUP

5. After the installation is done, click the **Finish** button.

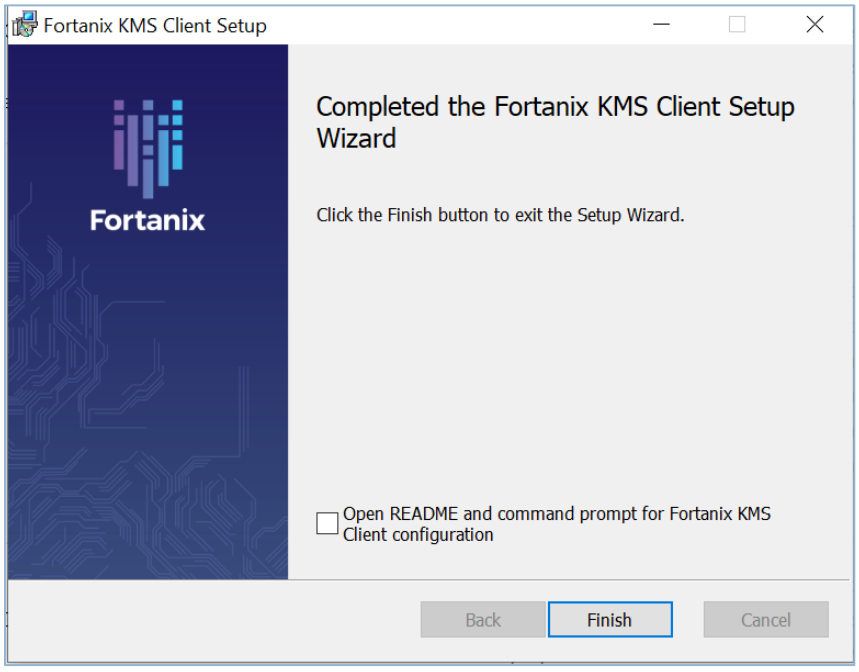

FIGURE 5: FORTANIX KMS CLIENT SETUP

2.2 CONFIGURING CNG CLIENT

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

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

```
cd C:\Program Files\Fortanix\KmsClient\
```

The machine key store uses the local machine configuration, and the user key store uses the current user configuration.

For example, run the following command to configure the Fortanix KMS Server URL for the local machine:

```
FortanixKmsClientConfig.exe machine --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: https://eu.smartkey.io/
    - APAC: https://apac.smartkey.io/
    - United States of America: https://amer.smartkey.io/

For example,

```
FortanixKmsClientConfig.exe machine --api-endpoint https://<fortanix
_dsm_url?
```

Run the following command to configure the Fortanix KMS Server URL for the current user:

```
FortanixKmsClientConfig.exe user --api-endpoint {KMS_URL}
```

To configure proxy information, add `--proxy http://proxy.com` or `--proxy none` to unconfigure proxy.

2.3 CREATING GROUPS

A 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 2.4- 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.

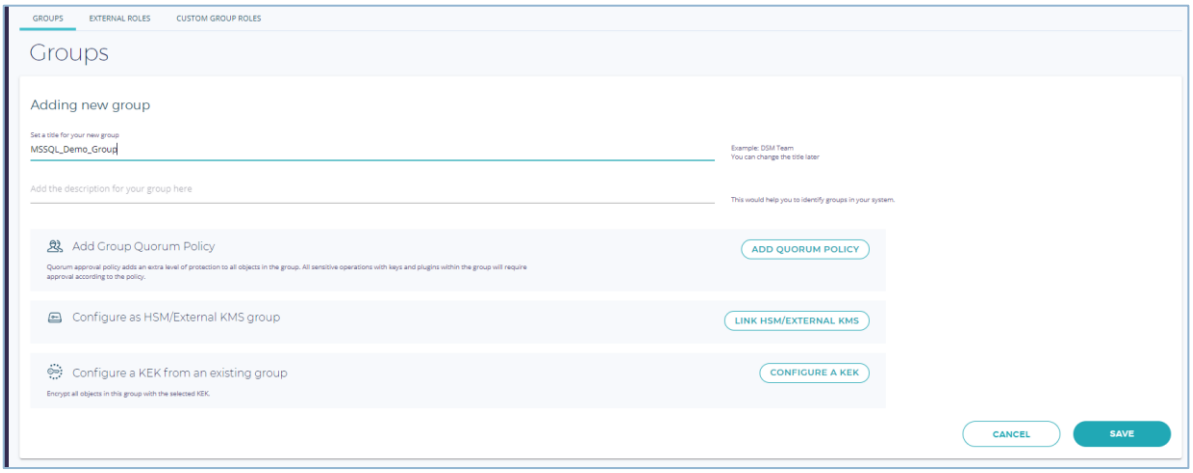

FIGURE 6: ADDING NEW GROUP

2.4 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 2.3- 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.

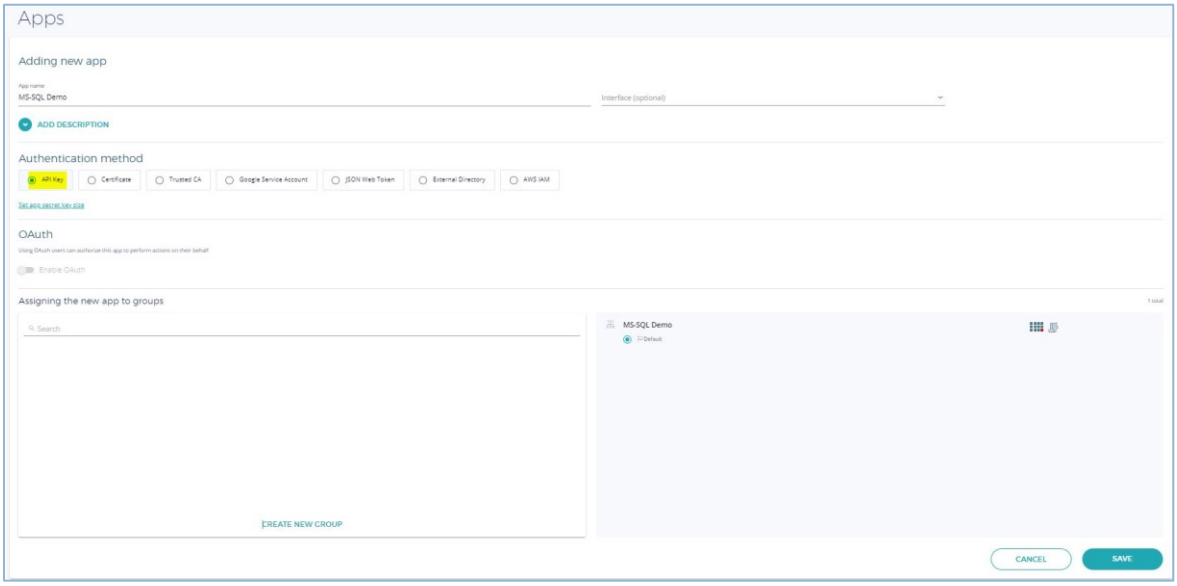

FIGURE 7: ADDING NEW APP

3.0 REFERENCE DOCUMENTS

Refer to the following documents to know the integration procedure in the same sequence as mentioned:

1. Data Security Manager with Microsoft SQL TDE Integration - Standalone Server Integration
2. Data Security Manager with Microsoft SQL TDE Integration - AOG Server Integration
3. Data Security Manager with Microsoft SQL TDE Integration - Key Rotation
4. Data Security Manager with Microsoft SQL TDE Integration - Backup & Restore
5. Data Security Manager with Microsoft SQL TDE Integration - Advanced

4.0 DOCUMENT INFORMATION

4.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/12715831971988-Data-Security-Manager-with-Microsoft-SQL-Server-TDE-Guide-Before-You-Begin

4.2 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