



ENTRUST

Microsoft SQL Server TDE and Entrust CSP Key Management Vault

Integration Guide

2026-04-22

Member of
Microsoft Intelligent
Security Association

Table of Contents

1. Introduction	1
1.1. Product configurations	1
1.2. Requirements	1
2. Test setup	2
3. Configure the Entrust CSP Vault	3
4. Integrate the MS SQL Server with the Entrust CSP Vault	6
4.1. Get the vault information	6
4.2. Install the policy agent client on the MS SQL Server host	7
4.3. Register the MS SQL Server with your vault	8
4.4. Enable TDE on the MS SQL Server	10
4.5. Create a TDE database keyset to hold the cloud keys	11
4.6. Create the database connector	12
4.7. Load the EKM provider on Microsoft SQL Server	14
4.8. Create a master key in the Entrust CSP vault	15
4.9. Create the TDE key and login on Microsoft SQL Server	16
5. Test the integration	18
5.1. Test the database encryption	18
5.2. Rotate the key manually in the Entrust CSP Vault	19
5.3. Shut down encryption on the database and remove credentials	19
6. Additional resources and related products	21
6.1. Entrust CSP Key Manager	21
6.2. Entrust products	21
6.3. nShield product documentation	21

Chapter 1. Introduction

This document describes the procedure for integrating the Entrust Cryptographic Security Platform (CSP) Vault with Microsoft SQL Server. The Entrust CSP Vault becomes the Extensible Key Management (EKM) provider for Microsoft SQL Server TDE.

1.1. Product configurations

Entrust has successfully tested the Microsoft SQL Server TDE integration with the Entrust CSP Vault in the following configurations:

Product	Version
Microsoft SQL Server	Enterprise Edition 2025
SQL Server Management Studio	22.4.1
Entrust CSP Vault	10.5.1
Operating System	Windows Server 2025

1.2. Requirements

Access to the [Entrust TrustedCare Portal](#). This portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

Familiarize yourself with the following documentation:

- [CSP Compliance Manager 10.5.1](#) documentation.
- [Cryptographic Security Platform Vault v10.5.1 Online Documentation Set](#) documentation.

Chapter 2. Test setup

The test setup consisted of four virtual machines:

- Entrust CSP Compliance Manager server.
- Entrust CSP Vault server (two nodes).
- Windows Server hosting the SQL database server and management tools.

The Entrust CSP Compliance Manager server was deployed and configured as described in [CSP Compliance Manager 10.5.1 - Installation and Administration](#).

The Entrust CSP Vault was implemented as a 2-node cluster. The cluster was deployed and configured as described in [Cryptographic Security Platform Vault v 10.5.1 Online Documentation Set](#).

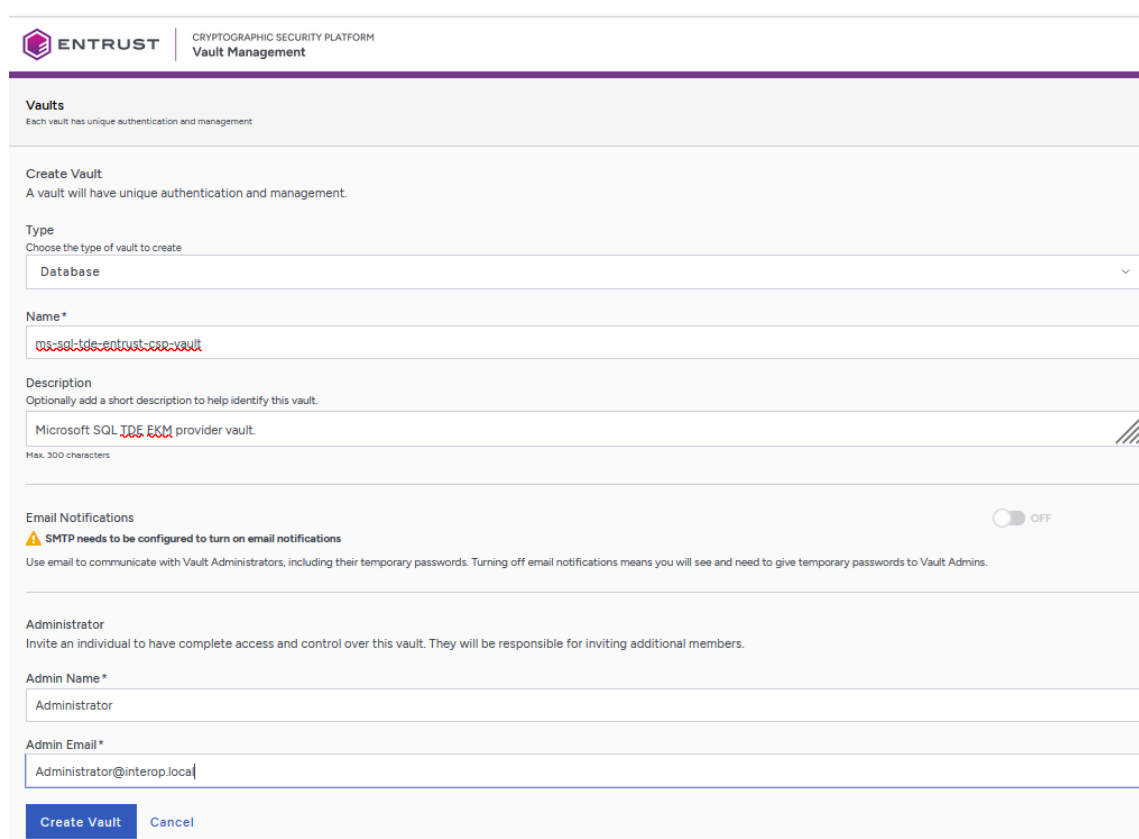
The Microsoft SQL Server was deployed as a stand-alone instance on a single machine. A database named TestDatabase was created for the purpose of this integration.

Chapter 3. Configure the Entrust CSP Vault

To create and configure a vault.

1. Sign in to the Entrust CSP Vault management web GUI.
2. Select the **+ Create Vault** icon.
3. For **Type**, select **Database** from the drop-down menu.
4. Enter a vault name and description, an administrator name and email, and then select **Create Vault**.

For example:



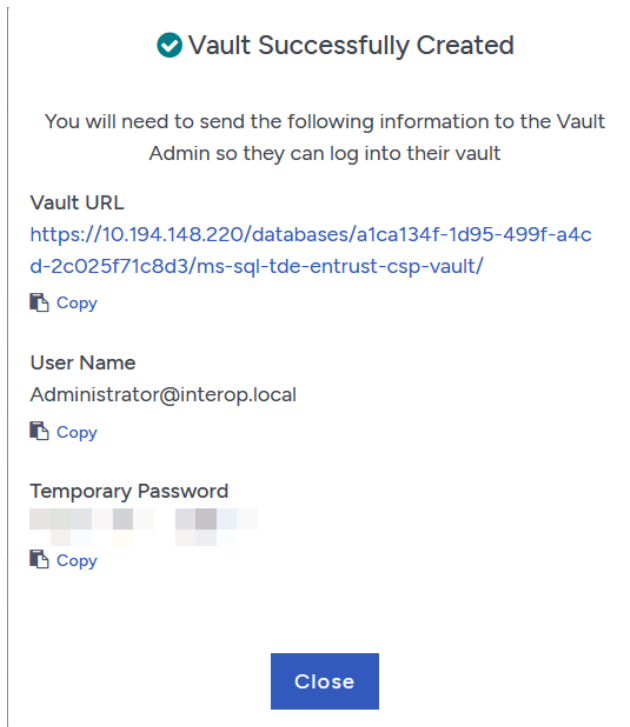
The screenshot shows the 'Create Vault' form in the Entrust CSP Vault Management web GUI. The form is titled 'Create Vault' and includes the following fields and options:

- Type:** A dropdown menu with 'Database' selected.
- Name*:** A text input field containing 'ms-sql-tde-entrust-csp-vault'.
- Description:** A text input field containing 'Microsoft SQL TDE EKM provider vault'.
- Email Notifications:** A toggle switch set to 'OFF'. A warning icon and text state: 'SMTP needs to be configured to turn on email notifications. Use email to communicate with Vault Administrators, including their temporary passwords. Turning off email notifications means you will see and need to give temporary passwords to Vault Admins.'
- Administrator:** A section for inviting an administrator, with the following fields:
 - Admin Name*:** A text input field containing 'Administrator'.
 - Admin Email*:** A text input field containing 'Administrator@interop.local'.
- Buttons:** 'Create Vault' (blue) and 'Cancel' (grey).

This creates the vault.

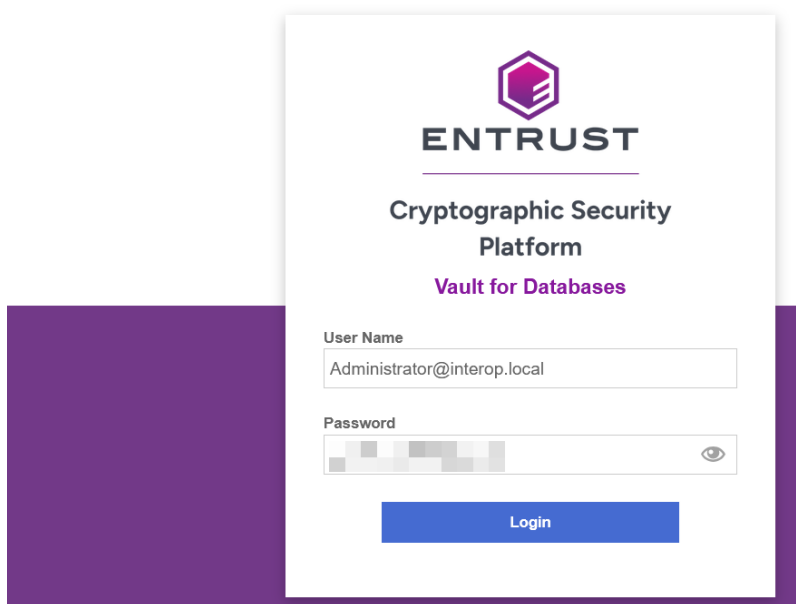
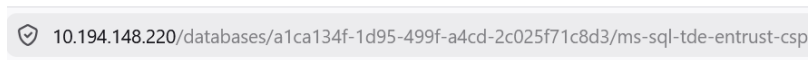
5. Copy and save the **Vault URL** and **Temporary Password**.

For example:



- 6. Bookmark your vault URL in the browser on the MS SQL Server host.
- 7. Sign in to your vault for the first time with your temporary administrator credentials.

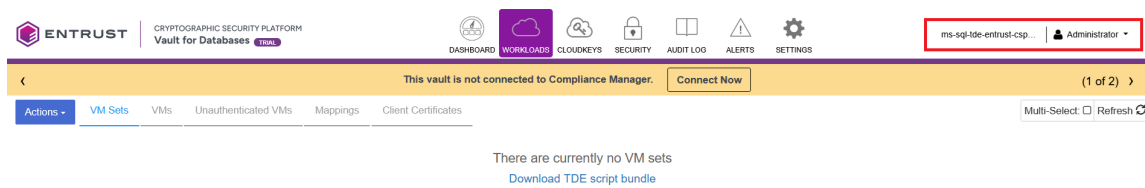
For example:



- 8. Enter the new administrator password. Then select **Close**.
- 9. Sign in again with your new password.

The vault name appears at the top of the screen.

For example:



Chapter 4. Integrate the MS SQL Server with the Entrust CSP Vault

For reference, see [Microsoft SQL Server Manual Installation and Configuration](#).

1. [Get the vault information](#)
2. [Install the policy agent client on the MS SQL Server host](#)
3. [Register the MS SQL Server with your vault](#)
4. [Enable TDE on the MS SQL Server](#)
5. [Create a TDE database keyset to hold the cloud keys](#)
6. [Create the database connector](#)
7. [Load the EKM provider on Microsoft SQL Server](#)
8. [Create a master key in the Entrust CSP vault](#)
9. [Create the TDE key and login on Microsoft SQL Server](#)

4.1. Get the vault information

1. Sign in to the MS SQL Server host.
2. From the MS SQL Server host, sign in to your vault web GUI.
3. In the top left, under **Administrator**, select **About** from the drop-down menu.

For example:

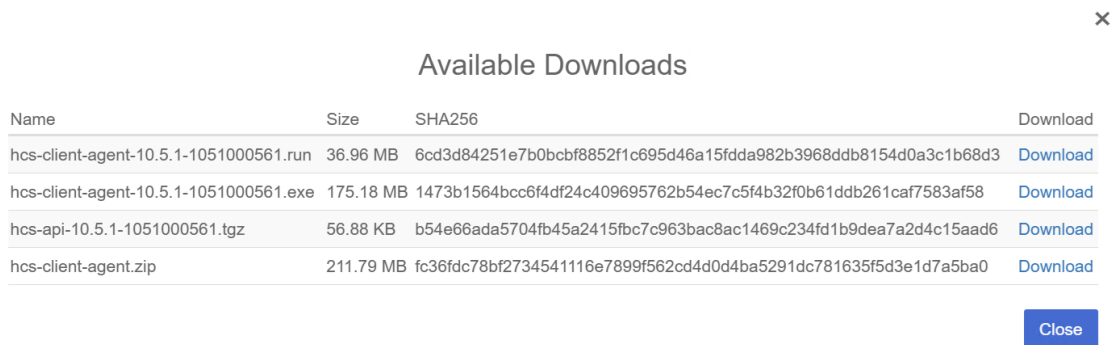


4. Make a note of the **Vault ID**.

4.2. Install the policy agent client on the MS SQL Server host

1. Sign in to the MS SQL Server host.
2. From the MS SQL Server host, sign in to your vault web GUI.
3. In the toolbar select **WORKLOADS**.
4. Select **Actions**, then select **Download Policy Agent** from the drop-down menu.

For example:



Name	Size	SHA256	Download
hcs-client-agent-10.5.1-1051000561.run	36.96 MB	6cd3d84251e7b0bcbf8852f1c695d46a15fdda982b3968ddb8154d0a3c1b68d3	Download
hcs-client-agent-10.5.1-1051000561.exe	175.18 MB	1473b1564bcc6f4df24c409695762b54ec7c5f4b32f0b61ddb261caf7583af58	Download
hcs-api-10.5.1-1051000561.tgz	56.88 KB	b54e66ada5704fb45a2415fbc7c963bac8ac1469c234fd1b9dea7a2d4c15aad6	Download
hcs-client-agent.zip	211.79 MB	fc36fdc78bf2734541116e7899f562cd4d0d4ba5291dc781635f5d3e1d7a5ba0	Download

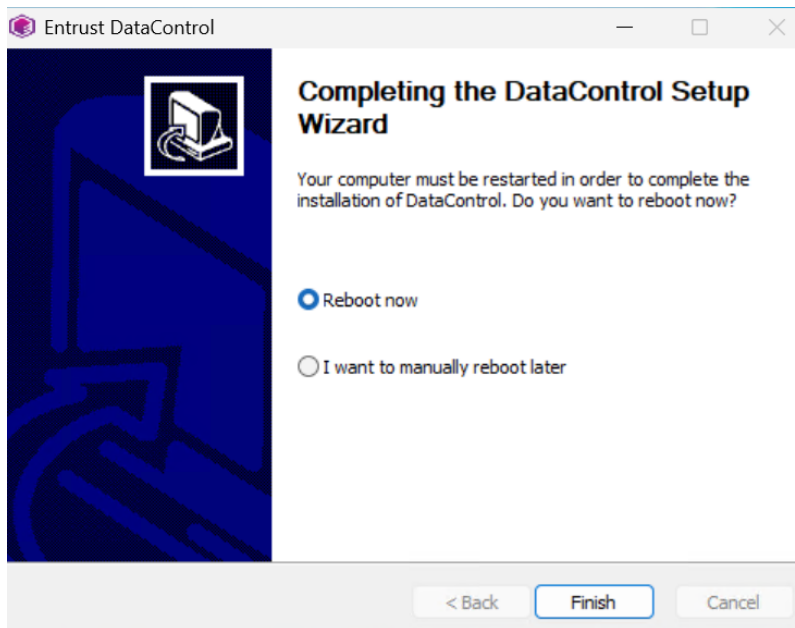
5. Select **Download** next to the `hcs-client-agent-<version>.exe` file.

Alternatively, download the `hcs-client-agent.zip` file and then extract the Windows executable.

6. Select **Close**.
7. Run the downloaded file, `hcs-client-agent-<version>.exe`.

Alternatively, open the `ZIP` file and navigate to the `hcs-client-agent\windows` folder and then run the executable.

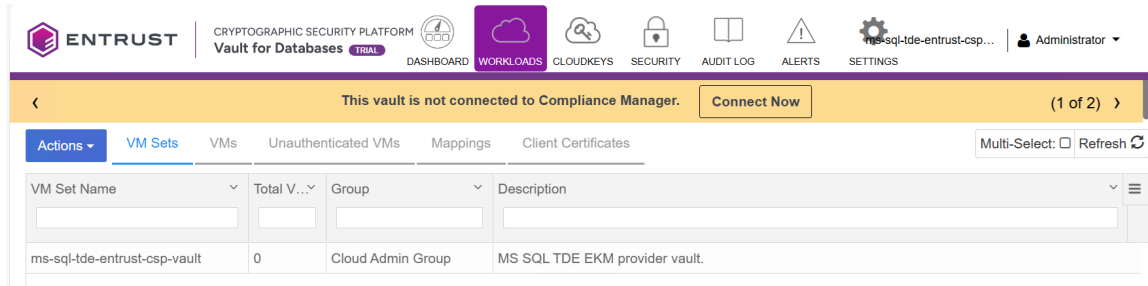
8. Complete the install process using the default options.
9. Upon completion, select **Reboot now**, then select **Finish**.



4.3. Register the MS SQL Server with your vault

1. On the MS SQL Server host, sign in to your vault web GUI.
2. In the toolbar, select **WORKLOADS**.
3. Select **Actions**, then select **Create New Cloud VM Set** from the drop-down menu.
4. In the **Create Cloud VM set** window, enter a **Name** and **Description**, then select **Create** and **Close**.

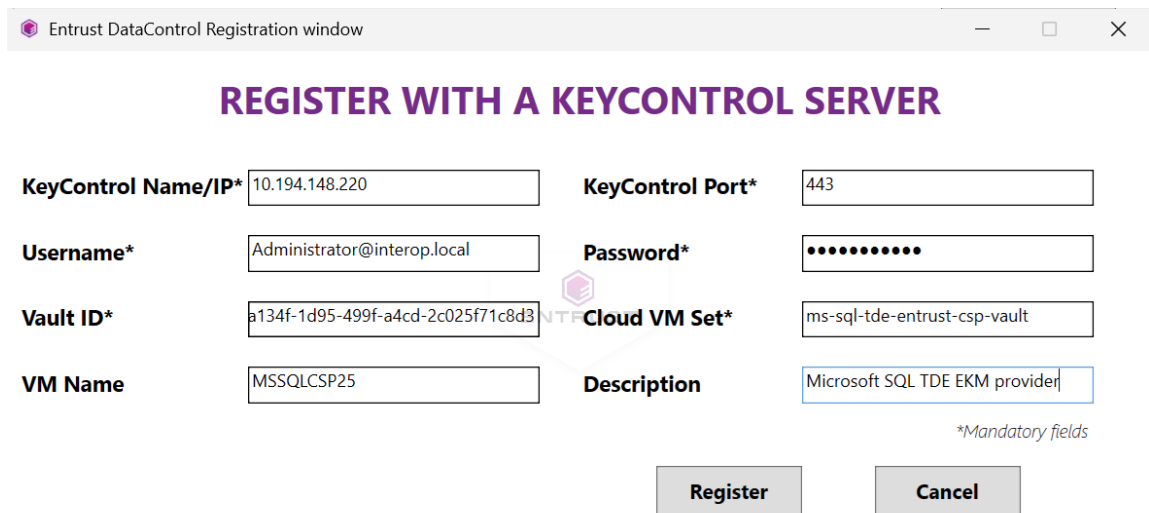
The new cloud VM set appears.



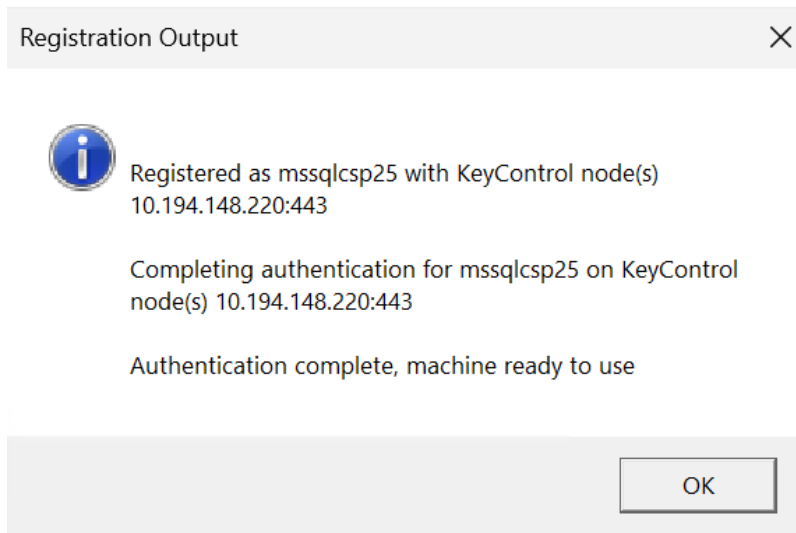
5. Select the **Start** menu in the MS SQL Server host and navigate to **Entrust DataControl**.
6. Select **Register**.
7. In the **Register** window, enter the information as follows, then select **Register** and **OK**.

For example:

Parameter	Value
Name / IP	First node of the Entrust CSP Vault cluster
Username	User created in Configure the Entrust CSP Vault
Password	User created in Configure the Entrust CSP Vault
Vault ID	See Get the vault information
Cloud VM set	Name of cloud VM set created above

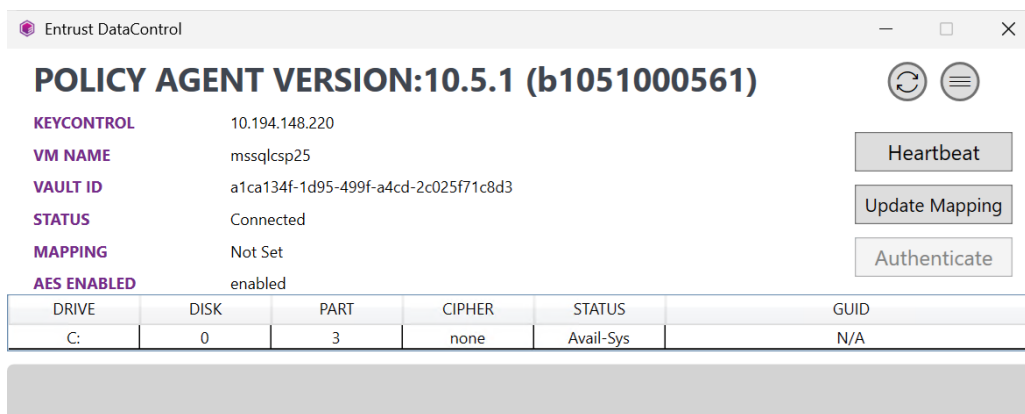


8. After registration succeeds, select **OK**.



The Entrust DataControl window now shows **STATUS Connected**.

9. Close the window.



4.4. Enable TDE on the MS SQL Server

1. On the MS SQL Server host, open a command window as an administrator.
2. Run the following command to enable TDE on the server:

```
C:\Users\Administrator.INTEROP>hcl tde status

TDE is not enabled on this VM

C:\Users\Administrator.INTEROP>hcl tde enable
Enabling tde will change permissions of some Files.
Do you want to proceed? (y/n) y

If you are enabling TDE for an Oracle database, follow the steps mentioned below from the Administrator
Guide.
"Administration Guide > KeyControl Vault for Databases > KeyControl with Oracle TDE > Configuring the
Oracle Server Database"

C:\Users\Administrator.INTEROP>hcl tde status
```

TDE is enabled on this VM

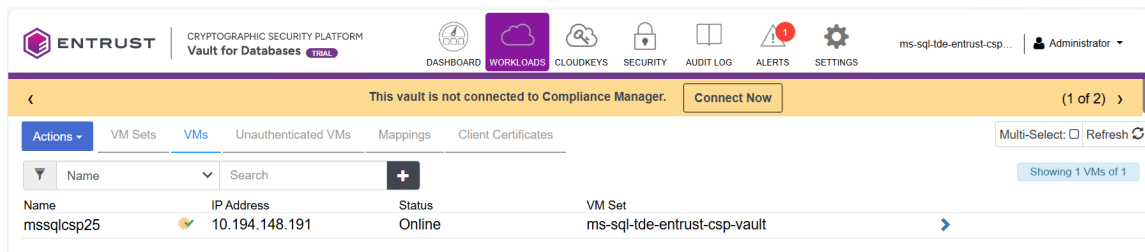
```
C:\Users\Administrator.INTEROP>hcl status
```

Summary

```
-----  
KeyControl: 10.194.148.220:443  
KeyControl list: 10.194.148.220:443  
Vault ID: a1ca134f-1d95-499f-a4cd-2c025f71c8d3  
Status: Connected  
Last heartbeat: Mon Apr 6 11:11:05 2026 (successful)  
Certificate Expiration: Apr 6 14:42:47 2027 GMT
```

3. Sign in to your vault web GUI.
4. In the toolbar select **WORKLOADS**, then select the **VM** tab.

The Microsoft SQL Server host now appears.



4.5. Create a TDE database keyset to hold the cloud keys

1. On the MS SQL Server host, sign in to your vault web GUI.
2. In the toolbar select **CLOUDKEYS**.
3. Select **Actions**, then select **Create Key Set** from the drop-down menu.
4. In the **Create Key Set** window, on the **Details** tab, enter the details as follows, then select **Continue**.

For example:

Create Key Set ✕

Details HSM

Name *

Description

Admin Group *

Database Type *

5. Enter the HSM information, if provisioned, then select **Apply**.
6. After the keyset is successfully created, select **Close**.

✔ **Key Set Created Successfully** ✕

What's Next?

Connect Key Set with a Microsoft SQL Server VM using Actions > Create Connector under key set details.

Make sure you have created and registered a VM with the database.

[? Learn more about registering a VM](#)

4.6. Create the database connector

1. On the MS SQL Server host sign in to your vault web GUI.
2. In the toolbar, select **CLOUDKEYS**, then select the **Key Sets** tab.
3. Select your keyset created in [Create a TDE database keyset to hold the cloud keys](#).

4. Scroll down and select the **Database Connectors** tab.
5. Select **Create Connector Now**.
6. In the **Create Database Connector** window, select your Microsoft SQL Server host from the drop-down menu.
7. Enter a name and select the expiration, then select **Create**. In this integration, we configure the connector to never expire.

For example:

Create Database Connector ×

Create a connection to the database VM. You will need to make sure that the database has TDE enabled. [How do I enable TDE on the VM?](#)

Associate this connection with the following VM:

VM Name *
mssqlcsp25 (ms-sql-tde-entrust-csp-vault) ▼
[Don't see a VM to use?](#)

Connector Name *
ms-sql-tde-entrust-csp-vault

Expiration *
 Never Choose a date

Cancel Create

8. Check the box next to the Database Connector created, then, from the **Actions** drop-down menu, select **Generate Access Token**.
9. In the **Generate Access Token** window, select **Generate Token**.

The access token is generated.

10. Copy and save the **Identity** and **Secret**.

For example:

Generate Access Token ✕

Generate an access token and copy Identity and Secret to be used in SQL Server for configuring Cryptographic Provider. [Learn More](#)

VM Name: **mssqlcsp25 (Cloud VM Set: ms-sql-tde-entrust-csp-vault)**

Generate Token

Identity Copy

ms-sql-tde-entrust-csp-vault

Secret Copy

Copy Config

Close

4.7. Load the EKM provider on Microsoft SQL Server

1. Launch Microsoft SQL Server Management Studio and connect to the SQL Server.
2. Run the following query to enable the EKM provider:

```

USE master
GO

-- Enable EKM provider
sp_configure 'show advanced options', 1 ;
GO
RECONFIGURE;
GO

sp_configure 'EKM provider enabled', 1 ;
GO
RECONFIGURE;
GO
        
```

100 % ▾
✔ No issues found

Messages

Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
 Configuration option 'EKM provider enabled' changed from 0 to 1. Run the RECONFIGURE statement to install.

Completion time: 2026-04-06T14:26:22.8086912-04:00

100 % ▾
✔ No issues found

3. Run the following query to load the EKM provider library:

```
-- Load cryptographic provider
CREATE CRYPTOGRAPHIC PROVIDER Entrust_CSP_Vault
FROM FILE = 'C:\Program Files\hcs\bin\htsqlckm_provider.dll';
GO
```

- Using the **Identity** and **Secret** from section [Create the database connector](#), create a credential file in JSON format. Place this file where it is accessible to the SQL Server, for example `C:\Users\Administrator\sqlcred.conf`.

```
{
  "identity" : "ms-sql-tde-entrust-csp-vault",
  "secret" :
  "WsZdrsP0mpbrTVtZSLGs6sU0Zy1q0cB0FmpyN17nNwiuN3PbjSThQj59eACZCg3IYZo/dtFn5Acr6FceJ+a/NAAhqS7keQ0T5cgXswjHVZ
z4gYrkqTPfMeUI8vM6z79E6qvVp/Fyr840nlhz1e1nSKiVohD85Dmued40dRvOqFy4iKuNWEwBEk9bs35P1La1iYz1ANDm31QH0akhT6+C9
sON0tSHSzs1JoZphNnPDN2PULJVIXkdo+yhbF+xBfW3P6N4JaQWK1aL09qIin/dX+Y/nBmeXbkNkyiBJend05jjSrRFMvkhZBNjEALkdUuc
IaPBpoe2m6~NRT3gkHo/jSJ6dgKy9GpvcyLguFDLzfz8jEfZuLKenfhSp5E75mJmFYqApuhBK566fqPH+sp2NmhSdXyMcixE+6u+HLy/3VN
Tnf9HezmrFMPNq1NF6NZBB9dQyz6KBFZ9zjPpNu6H2kJFbH3jwkYkfvnKBM9vC+ki25RTWNMOTQchf43LC3vaxup3QG6NcBfUWqXFWxsmTS
kSY04K3B+oDXVr77Io0GT59Fi6LhHv4ncEMr5w1dK2svRyf8W8iRebi0d1VsKbtgPg4KwoWdMp7U/VRxon16BeXvZgJ3YUFdsaCZL3eghjn
FEWOHP/v33Sx8EtzL53oT/5xCJprze1U="
}
```

- Run the following query to create login credentials for the administrator:

```
-- Create credential for system administrator
CREATE CREDENTIAL sa_entrust_csp_vault
WITH IDENTITY = 'file:C:\Users\Administrator\sqlcred.conf',
SECRET = 'ignore'
FOR CRYPTOGRAPHIC PROVIDER Entrust_CSP_Vault;
GO

-- Add this credential to the system administrator login
ALTER LOGIN [INTEROP\Administrator]
ADD CREDENTIAL "sa_entrust_csp_vault";
GO
```




We recommend pointing to the `sqlcred.conf` file in the query instead of simply listing the actual identity and secret. The former is required for SQL Server clusters.

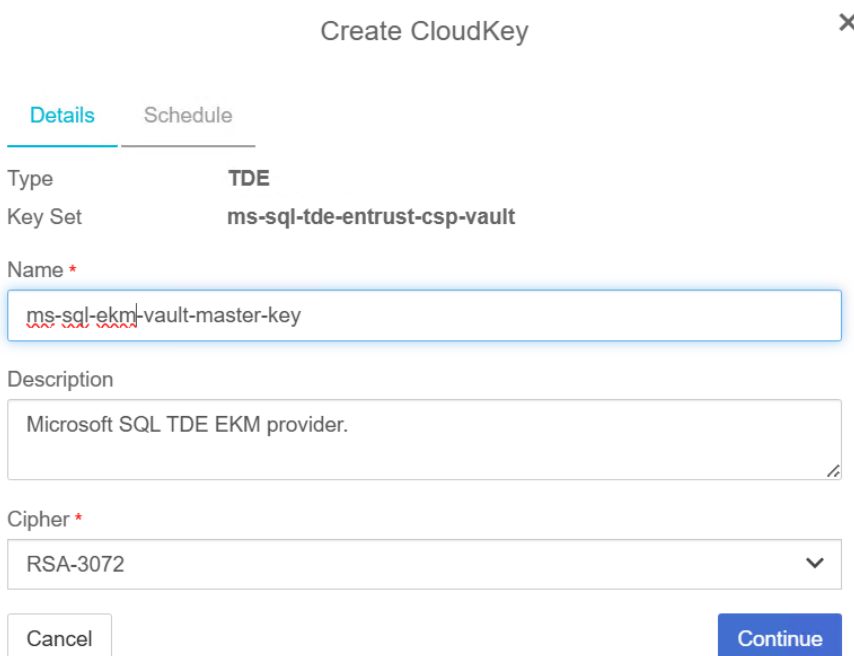
4.8. Create a master key in the Entrust CSP vault

- On the MS SQL Server host, sign in to your vault web GUI.
- In the toolbar select **CLOUDKEYS**, then select the **Cloud Keys** tab.
- In the **Key Set** drop-down menu, select your keyset created in [Create a TDE database keyset to hold the cloud keys](#).
- Select **Actions > Create CloudKey**.
- In the **Create CloudKey** window **Details** tab, enter a **Name** and **Description**.

6. Select the **Cypher** per your application requirements, then select **Continue**.

 SQL Server supports a maximum of 3072 bits for the **Cypher**.

For example:



Create CloudKey [X]

Details | Schedule

Type: **TDE**

Key Set: **ms-sql-tde-entrust-csp-vault**

Name *
ms-sql-ekm-vault-master-key

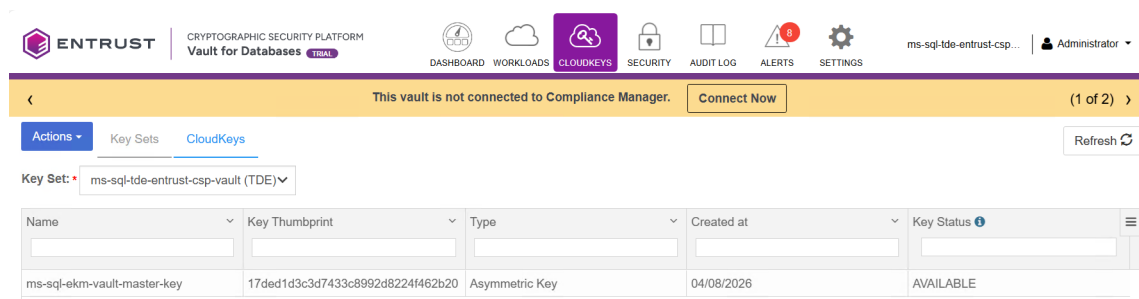
Description
Microsoft SQL TDE EKM provider.

Cipher *
RSA-3072

Cancel [Continue]

7. In the **Schedule** tab, select the required options, then select **Apply** and **Close**.

The master key is created.



ENTRUST CRYPTOGRAPHIC SECURITY PLATFORM Vault for Databases TRIAL

DASHBOARD WORKLOADS CLOUDKEYS SECURITY AUDIT LOG ALERTS SETTINGS

ms-sql-tde-entrust-csp... Administrator

This vault is not connected to Compliance Manager. [Connect Now] (1 of 2)

Key Set: ms-sql-tde-entrust-csp-vault (TDE)

Name	Key Thumbprint	Type	Created at	Key Status
ms-sql-ekm-vault-master-key	17ded1d3c3d7433c8992d8224f462b20	Asymmetric Key	04/08/2026	AVAILABLE

4.9. Create the TDE key and login on Microsoft SQL Server

1. Launch Microsoft SQL Server Management Studio and connect to the SQL Server.
2. Run the following query to create a TDE key protected by the EKM provider vault master key created in [Create a master key in the Entrust CSP vault](#).

```
USE master;  
CREATE ASYMMETRIC KEY TDE_Key  
FROM PROVIDER Entrust_CSP_Vault WITH
```

```
PROVIDER_KEY_NAME = 'ms-sql-ekm-vault-master-key',  
CREATION_DISPOSITION = OPEN_EXISTING;  
GO
```

3. Run the following query to create a login for the TDE user:

```
-- Create login for TDE user  
CREATE LOGIN TDE_Login  
FROM ASYMMETRIC KEY TDE_Key ;  
GO
```

4. Run the following query to create a credential for the TDE login:

```
-- Create credential for the TDE user  
CREATE CREDENTIAL tde_entrust_csp_vault  
WITH IDENTITY = 'file:C:\Users\Administrator\sqlcred.conf',  
SECRET = 'ignore'  
FOR CRYPTOGRAPHIC PROVIDER Entrust_CSP_Vault;  
GO  
  
-- Add this credential to the TDE user login  
ALTER LOGIN TDE_Login  
ADD CREDENTIAL "tde_entrust_csp_vault";  
GO
```

Chapter 5. Test the integration

1. [Test the database encryption](#)
2. [Rotate the key manually in the Entrust CSP Vault](#)
3. [Shut down encryption on the database and remove credentials](#)

5.1. Test the database encryption

The following queries test encryption on a database named `TestDatabase` created in section [Test setup](#).

1. Launch Microsoft SQL Server Management Studio and connect to the SQL Server.
2. Run the following query to create a database encryption key (DEK) wrapped with the TDE key named `TDE_Key` created in [Create the TDE key and login on Microsoft SQL Server](#).

```
USE TestDatabase
GO

CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER ASYMMETRIC KEY TDE_Key;
GO
```

3. Run the following query to enable encryption on `TestDatabase`:

```
ALTER DATABASE TestDatabase
SET ENCRYPTION ON;
GO
```

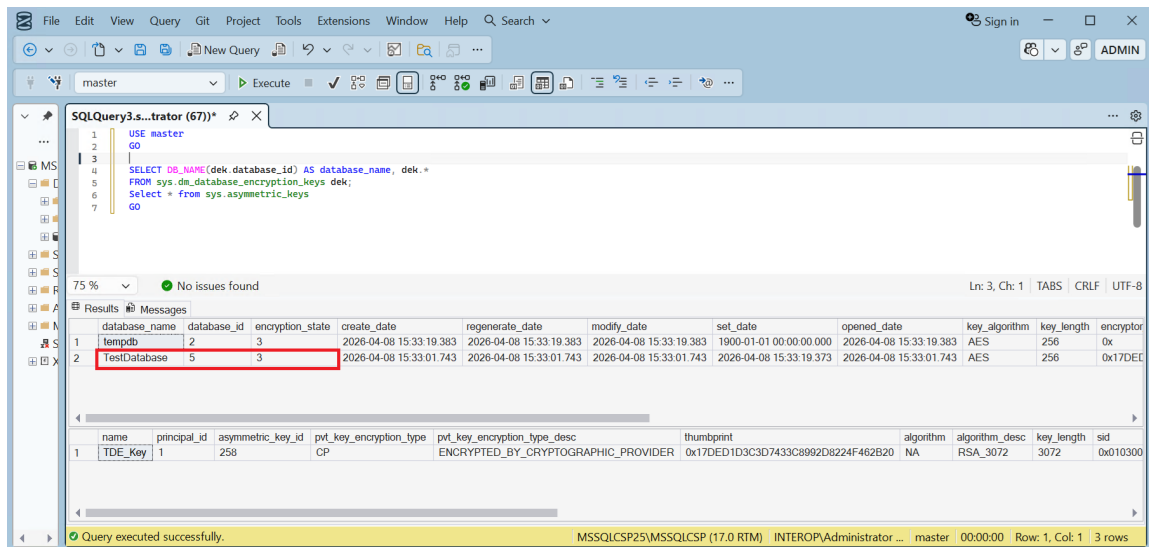
4. Check the state of keys and encryption.

The thumbprints should be matching for each query. The **encryption_state** of **3** signifies "encrypted". See [sys.dm_database_encryption_keys \(Transact-SQL\)](#) for reference.

For example:

```
USE master
GO

SELECT DB_NAME(dek.database_id) AS database_name, dek.*
FROM sys.dm_database_encryption_keys dek;
Select * from sys.asymmetric_keys
GO
```



5.2. Rotate the key manually in the Entrust CSP Vault

The Entrust CSP Vault v10.5.1 supports reusing the same key name upon a key rotation. The asymmetric key object continues to resolve to the new cloud key after a key rotation. It is sufficient to rotate the cloud key in the Entrust CSP Vault. No action is needed in the Microsoft SQL Server.

1. (Recommended) Back up your database before performing key rotation.
2. Sign in to your vault web GUI.
3. In the toolbar select **CLOUDKEYS**, then select the **Cloud Keys** tab.
4. In the **Key Set** drop-down menu, select your keyset created in [Create a TDE database keyset to hold the cloud keys](#).
5. Select your key created in [Create a master key in the Entrust CSP vault](#).
6. Scroll down and select **Rotate Now**.

A new version of the key is created. You can see this new version in the **Key Thumbprints** tab, marked with a star in front of it.

Details			Tags	Key Thumbprints	Actions
Key Thumbprint	Expires	Key Status			
★ 8e48969f761f490dbdb0718a615ed189	Never	AVAILABLE			
□ 17ded1d3c3d7433c8992d8224f462b20	Never	AVAILABLE			

5.3. Shut down encryption on the database and remove credentials

1. Launch Microsoft SQL Server Management Studio and connect to the SQL Server.
2. Run the following query to shut down encryption.

```
ALTER DATABASE TestDatabase
SET ENCRYPTION OFF;
GO

USE TestDatabase
DROP DATABASE ENCRYPTION KEY
GO

USE master
GO

DROP ASYMMETRIC KEY TDE_Key
GO

ALTER LOGIN TDE_Login
DROP CREDENTIAL tde_ekm_cred
GO

DROP LOGIN TDE_Login
DROP CREDENTIAL tde_ekm_cred
GO
```

3. Run the following query to remove the credential from the admin login:

```
ALTER LOGIN [INTEROP\Administrator]
DROP CREDENTIAL sa_entrust_csp_vault;
GO

DROP credential sa_ekm_tde_cred
GO
```

Chapter 6. Additional resources and related products

6.1. [Entrust CSP Key Manager](#)

6.2. [Entrust products](#)

6.3. [nShield product documentation](#)