ORACLE
DATABASE

Oracle Advanced Security
Transparent Data Encryption (TDE)

Frequently Asked Questions (FAQ)

APRIL 2016

ORACLE

Product Overview

Q. What does Transparent Data Encryption (TDE) provide?

A: TDE transparently encrypts data at rest in Oracle Databases. It stops unauthorized attempts from the operating system to access database data stored in files, without impacting how applications access the data using SQL.

TDE can encrypt entire application tablespaces or specific sensitive columns. Tablespace encryption is useful when you want to encrypt all data irrespective of columns. With tablespace encryption, you do not need to consider column characteristics such as indexes and constraints. Column encryption is useful in cases where only a handful of sensitive columns must be encrypted.

TDE is fully integrated with Oracle database. Encrypted data remains encrypted in the database, whether it is in tablespace storage files, temporary tablespaces, undo tablespaces, or other files that Oracle Database 12*c* relies on such as redo logs. Also, TDE can encrypt entire database backups and Data Pump exports. Oracle Recovery Manager (RMAN) and Data Pump Export/Import both integrate with TDE encryption to pass through previously encrypted data.

Q. How are TDE encryption keys managed?

A: TDE creates and manages multiple keys used for encryption. These keys must be protected because, if an attacker obtains encrypted data and matching keys, they can easily decrypt to see clear data.

TDE has a two-tier key architecture, with data encryption keys that are wrapped by a single database master key. Data encryption keys are managed by Oracle Database 12*c* behind the scenes. The master key is separated from encrypted data, stored outside of the database, and directly managed by the database security administrator in a keystore.

Two keystore options are available for TDE to support diverse customer environments. By default, TDE stores its master key in an Oracle Wallet, a PKCS#12 standards-based key storage file. Wallets provide an easy solution for small numbers of encrypted databases. Customers with many Oracle databases and other encrypted Oracle servers can leverage Oracle Key Vault, a security hardened software appliance that provides centralized key and wallet management for the enterprise. It uses industry standard OASIS Key Management Interoperability Protocol (KMIP) for communications. Customers can keep their local Oracle Wallets and Java Keystores, using Key Vault as a central location to periodically back them up, or they can remove keystore files from their environment entirely in favor of always-on Key Vault connections. All network connections between Key Vault and database servers are encrypted and mutually authenticated using SSL/TLS.

TDE master keys can be rotated periodically according to your security policies with zero downtime and without having to re-encrypt any stored data. Historical master keys are retained in the keystore in case encrypted database backups must be restored later. Master keys in the keystore are managed using a set of SQL commands (introduced in Oracle Database 12*c*). For separation of duties, these commands are accessible only to security administrators who hold the new SYSKM administrative privilege or higher. In addition to using SQL commands, you can manage TDE master keys using Oracle Enterprise Manager 12*c* or 13*c*.

Q. How does TDE impact database performance?

A: For Oracle Database 12*c* systems with modern hardware, the performance overhead from TDE typically is very low and not noticeable to end-users. The TDE page on Oracle Technology Network links to several real-world customer testimonials describing how TDE performs in live production environments.

TDE tablespace encryption leverages cryptographic circuitry present in most modern Intel® and Oracle SPARC processors and cores to accelerate encrypt and decrypt operations by 5-10 times. Oracle Database 12*c* further caches decrypted tablespace data to make repeated queries faster. For applications that run full table scans, the performance impact may be higher. More memory and bigger caches will improve performance in these

situations. As TDE works at tablespace level, one could consider moving all non-sensitive tables to a clear tablespace.

TDE column encryption can be narrowed to certain columns containing your most sensitive data to minimize overall performance impact. In this approach, only a few columns must be decrypted – even for complex analytical queries that scan large data sets. Column encryption also leverages CPU cryptographic acceleration.

Q. How transparent is TDE to business applications?

A: TDE is transparent to business applications and does not require application changes. Encryption and decryption occur at the database storage level, with no impact to the SQL interface that applications use (neither inbound SQL statements, nor outbound SQL query results).

Note that TDE is certified for use with common packaged applications. These certifications are mainly for profiling TDE performance under different application workloads and for capturing application deployment tips, scripts, and best practices.

Q. How transparent is TDE to database operations?

A: TDE is tightly integrated with frequently used Oracle Database 12*c* technologies to make it transparent to your database operations. For example, it is integrated with Oracle Advanced Compression, Oracle Real Application Clusters (RAC), Oracle Data Guard, Oracle Active Data Guard (primary/standby), Oracle Golden Gate (replication), and Oracle Multitenant (pluggable databases). Note that for unattended startup in database cluster configurations, TDE provides a key management option, auto-login wallet that allows the database to open its keystore and access its master key without a human operator.

Q. How does TDE integrate with Oracle Exadata?

A: TDE tablespace encryption leverages Oracle Exadata to further boost performance. For example, Exadata Smart Scans parallelize cryptographic processing across multiple storage cells, resulting in faster queries on encrypted data. TDE also benefits from support of hardware cryptographic acceleration on server processors in Exadata. TDE integration with Exadata Hybrid Columnar Compression (EHCC) compresses data first, improving cryptographic performance by greatly reducing the total amount of data to encrypt and decrypt.

Deployment Considerations

Q. What is the process to set up TDE?

As TDE is part of the database kernel, no separate installation is required. To deploy and configure TDE: 1) Setup a keystore and create an initial master key, 2) Enable encryption for tablespaces or columns in your database.

All steps can be executed using SQL commands or Oracle Enterprise Manager 12*c* or 13*c* GUI. All data that is added to those encrypted tablespaces is automatically encrypted. Column encryption however, can be applied to both new and existing tables. See the next question for information about encrypted existing clear data. For detailed information about setup steps, tuning, and migration, please refer to the product documentation for TDE.

Q. How do I migrate existing clear data to TDE encrypted data?

A: TDE provides multiple techniques to migrate existing clear data to encrypted tablespaces or columns. Solutions are available for both online and offline migration.

For tablespace encryption, you can copy existing clear data into a new encrypted tablespace with Oracle Online Table Redefinition (DBMS_REDEFINITION). It copies in the background with no downtime. This approach works for both 11*g* and 12*c* databases. This approach includes certain restrictions described in Oracle Database 12*c* product documentation.

Customers with Oracle Data Guard can use Data Guard and Oracle Data Pump to encrypt existing clear data with near zero downtime (see details here). This procedure encrypts on standby first (using DataPump Export/Import), switches over, and then encrypts on the new standby. Database downtime is limited to the time it takes to perform Data Guard switch over. Multiple synchronization points along the way capture updates to data from queries that executed during the process.

If you plan to migrate to encrypted tablespaces offline during a scheduled maintenance period, then you can use Data Pump to migrate in bulk. You also can use SQL commands such as ALTER TABLE MOVE, ALTER INDEX REBUILD (to move an index), and CREATE TABLE AS SELECT to migrate individual objects.

With TDE column encryption, you can encrypt an existing clear column in the background using a single SQL command such as ALTER TABLE MODIFY. This is a fully online operation.

Q. How much extra storage space is needed for TDE encrypted data?

A: For TDE tablespace encryption, the storage overhead is practically none.

The storage overhead associated with TDE column encryption is between 1 and 52 bytes per row for each encrypted column, depending on the following factors:

- Padding [Mandatory] - Padding to the next 16 bytes (for AES). With 3DES168, padding is to the next 8 bytes. For example, if a value requires 9 bytes of storage, then encrypting this value with 3DES168 requires an additional 7 bytes of storage.
- MAC [Optional] - If MAC is specified on the encrypted column, then 20 bytes are added to each value to support integrity checking using SHA. MAC is on by default.
- SALT [Optional] - If SALT is specified for TDE column level encryption, then an additional 16 bytes per value is added. Randomly generated 16 bytes SALT is on by default.

These numbers are important for storage planning. Note that when a column is marked as encrypted, any cryptographic expansion of the cipher data is handled by TDE transparently.

Q. Does TDE support Hardware Security Modules (HSM)?

A: TDE customers optionally may store their master keys in an external device such as HSM using the PKCS #11 interface. In this setup, master keys are stored directly in the third-party device rather than in Oracle Key Vault or Oracle Wallet.

When using PKCS #11, the third-party vendor provides the storage device, PKCS #11 software client library, secure communication from the device to the PKCS #11 client (running on the database server), authentication, auditing, and other related functionality. The vendor also is responsible for testing and ensuring high-availability of the master encryption key in diverse database server environments, configurations, and versions. Customers should contact the device vendor to receive assistance for any related issues. We do not certify or validate third-party HSMs due to the above challenges.

Standards and Compliance

Q. Which encryption algorithms does TDE support?

A: TDE encryption uses international standards such as Advanced Encryption Standard (AES) and 3DES. Customers can choose their preferred data encryption algorithm and key length.

Q. What industry standards key management does TDE use?

A: TDE master key management uses standards such as PKCS #12 and PKCS #5 for Oracle Wallet keystore. Oracle Key Vault uses OASIS Key Management Interoperability Protocol (KMIP) and PKCS #11 standards for communications. Customers can choose Oracle Wallet or Oracle Key Vault as their preferred keystore.

Q. What security certifications and validations does TDE have?

A: The cryptographic library that TDE uses in Oracle Database 12c is validated for U.S. FIPS 140-2. See here for the library's FIPS 140 certificate (search for the text "Crypto-C Micro Edition"; TDE uses version 4.0). Also, see here for up-to-date summary information regarding Oracle Database certifications and validations.

Q. How does TDE help customers comply with Payment Card Industry (PCI) standards, healthcare data privacy laws (U.S. HIPAA/HITECH), and other security regulations?

A: TDE is an important database security control that helps Oracle customers comply with diverse standards, laws, and regulations that mandate data privacy and security. It provides essential encryption for data at rest in Oracle Databases, enabling customers to address a growing list of regulations in different geographies and industries and remain in compliance as regulations evolve. TDE often is deployed in conjunction with its key management options (Oracle Key Vault and Oracle Wallet) to address specific terms of PCI-DSS Requirement #3 - Protect Stored Cardholder Data. In healthcare context for HIPAA, customers use TDE to encrypt sensitive patient data stored in the database.

Comparison to Other Approaches

Q. How does TDE compare to encrypting in the application tier?

Encrypting in the application tier may be desirable for certain extremely sensitive columns where it is essential that only the application be able to access the data. However, this approach requires high-cost custom coding for proper encryption/decryption and management of keys. Furthermore, all application server nodes need to access the encryption keys making their management and protection difficult. It also increases the chances of corruption if users or the application can update any row/column without appropriate control.

Encryption in the application tier also adversely impacts core database query capabilities because you can only use the database to perform equivalency searches on encrypted columns. Common analytical queries that match against data ranges or computed values will not work. Application tier encryption does not benefit from Oracle Database In-Memory and Exadata high performance architecture.

TDE can be used to encrypt very diverse data all at once in database storage files and does not have these limitations.

Q. How does TDE compare to encrypting host directories or volumes?

Encrypting Oracle Database 12*c* tablespace files using file or volume encryption software running on the host may initially seem desirable with its support for diverse use cases and platforms; however, because these

technologies are not tuned for high I/O database operations, they can have dramatic impact on core database components. For example, if you attempt to store database redo logs in an encrypted directory or volume, this redo component will incur performance overhead, leading to increasing wait times for log switches, delayed archive file writes, accelerating memory consumption, and possible database stoppage (see details on My Oracle Support).

If you use third-party products that require installing invasive operating system and/or file system modules, this software can crash the database host. These modules may conflict with other running security programs (e.g. anti-virus, intrusion detection) and lead to system crashes. They may also disrupt your patching policies, preventing you from applying a critical patch to the host operating system or file system until a matching patch is available from the encryption vendor. Sensitive data in encrypted file storage may be presented as clear data to non-database programs and users running on the host, exposing your sensitive information to attacks that circumvent the database.

In addition, these solutions cannot limit encryption overhead to specific sets of database tables or columns, and they do not benefit from Oracle Database In-Memory and Exadata high performance architecture.

Note that TDE is fully supported on all operating system platforms including Oracle engineered systems. For addressing data at rest encryption outside of Oracle Databases, TDE can be paired with complementary Oracle technologies.

If a third-party vendor solution causes problems with your database environment, Oracle Support may request you to decrypt data, uninstall third-party software, and reproduce your issue before providing assistance. For questions about third-party encryption products or any support inquiries, you will be asked to consult with your vendor. Oracle provides no support for third-party solutions encrypting tablespace files on Oracle engineered systems such as Oracle Exadata and Oracle Database Appliance.

Q. How does TDE compare to encrypting in disk drives or SAN?

A: Encrypting Oracle Database 12*c* tablespace files using encryption features of disk drives or SAN storage arrays may seem desirable due to their support for diverse use cases outside of Oracle Databases. However, sensitive data in encrypted disks or SAN may be presented as clear data to non-database programs and users running on the host, exposing your sensitive information to attacks that circumvent the database. These solutions cannot limit encryption overhead to specific sets of database tables or columns, and they do not benefit from Oracle Database In-Memory and Exadata architectures. You typically must purchase new premium price hardware and/or software with optional add-ons. Troubleshooting data I/O issues becomes nearly impossible on encrypted storage arrays.

Complementary Technologies

Q. Can TDE be paired with other data at rest encryption technologies?

A: Oracle provides additional data at rest encryption technologies that can be paired with TDE to protect unstructured file data, storage files of non-Oracle databases, and more as shown in the table below.

Use Case	Oracle Technology
Encrypt files (non-tablespace) using Oracle file systems and operating systems	• Oracle ZFS - An encrypting file system for Solaris and other operating systems • Oracle ACFS - An encrypting file system that runs on Oracle Automatic Storage Management (ASM)

	• Oracle Linux native encryption modules including dm-crypt and eCryptFS
Encrypt files (non-tablespace) using Oracle Database 12*c*	Oracle Secure Files in combination with TDE. Support for Secure File LOBs is a core feature of the database
Encrypt data programmatically in the database tier	Oracle Database package encryption toolkit (DBMS_CRYPTO) for encrypting database columns using PL/SQL
Encrypt data programmatically in the application tier	Oracle Java (JCA/JCE), application tier encryption may limit certain query functionality of the database. Consider suitability for your use cases in advance

Table 1 – Complementary Oracle Data at Rest Encryption Technologies

Oracle provides solutions to encrypt sensitive data in the application tier – although this has implications for databases that you must consider in advance (see details here). Note that TDE is the only recommended solution specifically for encrypting data stored in Oracle Database 12*c* tablespace files.

Q. What security controls typically are configured alongside TDE?

A: It is recommended to use TDE in combination with other detective and preventive security controls available for Oracle Database 12*c*.

Preventive controls help you stop many common threats. Good prevention starts by granting only appropriate privileges and roles to database user accounts, following the security principle of least privilege. You also should encrypt database network connections using SQLNet encryption or built-in support for SSL/TLS. Next, you can add restrictions for privileged user accounts, limit display of sensitive application data, and sanitize copies of production data used in testing and development environments. Details about these preventive controls are shown below.

Preventive Control	**Description**
Oracle Database Vault	Reduces risk exposure coming from powerful database users such as DBA and privileged application connections. Restricts operations these privileged accounts can perform
Oracle Data Redaction	Redacts sensitive data from query results prior to display by applications. Enforces redaction at runtime, with low overhead, and according to conditions set in policies. Part of the same license as TDE (Oracle Advanced Security)
Oracle Data Masking and Subsetting	Makes it easy to create masked and subsetted copies of production data for use in non-production environments such as testing and development databases. Available as an add-on pack for Oracle Enterprise Manager
Oracle Label Security	Implements Multi-Level Security (MLS) enabling rows with differing sensitivity to reside in the same table. Explicitly labels rows with group, compartment, and sensitivity levels – then matches them with user labels

Table 2 – Oracle Database Preventive Controls Typically Used In Combination with TDE

Detective controls start with database auditing to capture records of database actions. You can deploy Oracle Audit Vault and Database Firewall to move audit information to a central repository where you can run database activity reports, detect anomalies, and generate security alerts. Oracle Audit Vault and Database Firewall also provides database firewall and monitoring capabilities that track inbound SQL statements, giving you early warning of unauthorized database activity and blocking threats before they cause harm.

Please refer to the Oracle Database Security page on Oracle Technology Network for more information about database security controls to use alongside TDE.

More Information

Q. How is TDE licensed?

TDE is part of Oracle Advanced Security license for Oracle Database Enterprise Edition. For on-premises databases, Advanced Security can be licensed by server core count or by named user plus (see pricing information here).

The Advanced Security license includes data redaction, tablespace encryption, column encryption, and wallet-based master key management. Centralized key and wallet management using Oracle Key Vault is licensed separately. Note that creating encrypted database backups (RMAN) and Data Pump exports also requires a license for Advanced Security if you do not already have one.

Q. Where can I learn more about TDE?

A: For more information about the benefits of TDE, please see the product page on Oracle Technology Network. A variety of helpful information is available on this page including product data sheet, customer references, videos, tutorials, and more.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US


blogs.oracle.com/oracle


facebook.com/oracle


twitter.com/oracle


oracle.com

Integrated Cloud Applications & Platform Services