Genesys Security Deployment Guide

Encrypted Data in Databases

6/13/2026

Contents

- 1 Encrypted Data in Databases
  - 1.1 Security Benefits
  - 1.2 Supporting Components
  - 1.3 Feature Description
  - 1.4 Feature Configuration

Encrypted Data in Databases

This feature uses the data transparency and encryption functionalities provided by a Database Management System (DBMS) to encrypt data contained in a database.

> **Important**
>
> If database encryption is not in place, database passwords used by Database Access Points, and the values of any configuration options named **password**, such as those used with SNMPv3, will be automatically encrypted using AES 128. This is a failsafe measure only; Genesys strongly recommends that you encrypt all data in the database.

Security Benefits

By default, data in a database is stored as plain text, and is easily read by anyone (or anything) accessing it. Encrypting this data makes that data nearly impossible to read without the corresponding decryption mechanism. In effect, this feature provides a second level of protection should an unauthorized user get access to the database itself.

Supporting Components

Databases in the following Genesys products support this feature:

- Genesys Administrator Extension (GAX)
- Management Framework
- Outbound Contact
- eServices
- Universal Contact Server
- Genesys Voice Platform
- Genesys Interactive Insights
- Performance Management Advisors
- Genesys Info Mart
- Interaction Concentrator
- Workforce Management

- Pulse

Feature Description

Data in a database is stored as plain text by default, and therefore is easily read by anyone (or anything) accessing it. This feature uses the data transparency and encryption functionalities provided by a DBMS to encrypt that data, so that it cannot be read or understood without the corresponding decryption capabilities.

Feature Configuration

This feature is supported by Genesys only if the DBMS also supports encrypted data. Currently, only the data encryption mechanisms of the following DBMS are supported:

- MS SQL 2008 R2 and later
- Oracle 11g R1 and later
- Oracle 10.2 and later

MS SQL 2008 R2 and Later

Genesys provides transparent access to databases based on MS SQL 2008 R2 and later with the Transparent Data Encryption (TDE) feature enabled. The TDE feature is fully described, with implementation instructions, on the Microsoft Developer Network website at http://msdn.microsoft.com/en-us/library/bb934049.aspx.

Deployment of TDE must follow MS SQL documentation, and basically consists of the following steps:

1. Create a master key.
2. Create or obtain a certificate protected by the master key.
3. Create a database encryption key (in the existing Genesys database) and protect it with this certificate.
4. Configure the database to use encryption.

Before implementing this feature, first create (or convert) your database with a schema compatible with the release of your Genesys software that supports this feature. Then deploy encryption.

Oracle 11g R1 and Later

Genesys provides transparent access to Oracle 11g R1 and later encrypted tablespaces.

Deployment of TDE must follow Oracle 11g documentation. It includes the following steps:

1. Set up Oracle 11g encryption:
    a. Create a system encryption key.

b. Load the master key at database restart.

c. Initialize the autologin wallet to keep the master key accessible across restarts of this instance of the database.

2. Set up the Genesys database:

a. Create the tablespace with encryption.

b. Make it the default tablespace with [unlimited] quote for a user account used by Genesys applications.

c. Create database schemas in the encrypted tablespace.

For more details and examples, see the Oracle-Base article at http://www.oracle-base.com/articles/11g/TablespaceEncryption_11gR1.php.

Deploy encryption on the Genesys tablespace before creating the database schema compatible with the release of your Genesys software that supports this feature. If the database tables already exist and reside in unencrypted tablespace, move the tables to an encrypted tablespace using tools provided by Oracle.

Oracle 10.2 and Later

Genesys provides transparent access to databases based on Oracle 10.2 and later with the Transparent Data Encryption (TDE) feature enabled on database columns that support it.

Important

- A list of column types that are supported by Oracle 10.2 and later is included in the Oracle documentation.
- Columns that contain BLOB and CLOB data cannot be encrypted.

For details about the schema of the databases for which you want to encrypt the data, contact your Genesys representative. For example, the help file Framework Configuration Database Schema Reference contains the database schema for the Configuration Database.

Deployment of TDE must follow Oracle 10 documentation. It includes the following steps:

1. Set up the TDE feature:

a. Create a system encryption key.

b. Load the master key at database restart.

c. Initialize the autologin wallet to keep the master key accessible across restarts of this instance of the database. For details, see the Oracle-Base articles starting at http://www.oracle-base.com/articles/10g/transparent-data-encryption-10gr2.php.

2. In the Genesys database, alter the database tables by setting up columns with transparent encryption to encrypt the data in those columns, as follows:

a. Stop the server that uses the database that you want to alter. For example, if you are going to

encrypt data in the Configuration Database, stop Configuration Server.

b. Run the script to alter the table. For example, to add encryption to the password column of a Person object, alter the Configuration Server 8.1.1 database table definition as follows:

```
ALTER TABLE cfg person MODIFY (password ENCRYPT);
```

c. Restart the server.