



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# User's Guide

## Security and Authentication

# Security and Authentication

**Purpose:** Gathers together topics relating to security, encryption, authentication, and the like.

## Contents

- **1 Security and Authentication**
  - 1.1 Database Encryption
  - 1.2 Security Log Filtering
  - 1.3 TLS
  - 1.4 Authentication
  - 1.5 Role-Based Access Control

## Database Encryption

For database encryption, Genesys recommends using Transparent Data Encryption (TDE):

- Oracle 11—Tablespace-level; see [http://www.oracle-base.com/articles/11g/TablespaceEncryption\\_11gR1.php](http://www.oracle-base.com/articles/11g/TablespaceEncryption_11gR1.php).
- MSSQL Server 2008—Database-level; see [http://msdn.microsoft.com/en-us/library/cc278098\(SQL.100\).aspx](http://msdn.microsoft.com/en-us/library/cc278098(SQL.100).aspx).

Do not use column-level encryption.

## Security Log Filtering

You can use configuration options in the **log-filter** and **log-filter-data** sections to control how or whether user data keys appear in the logs.

## TLS

UCS/CS supports Transport Layer Security (TLS) in various ways:

- For UCS, see **Using TLS with UCS** and related pages. The procedures described also apply to E-mail Server.
- For clients of UCS, see **Using TLS with UCS Clients**.
- UCS/CS also supports secure connections to Configuration Server.

## Authentication

When clients connect to UCS, there are two possible modes of authentication, specified by configuration options in the **authentication** section.

- Single-user—Clients connect using the user name and password specified by the UCS options `username` and `password`. This means all UCS clients must use the same credentials. To enable single-user authentication, give the `mode` option a value of `single-user`.
- Multi-User—Clients are configured as Persons in the Configuration Layer, and connect to UCS using the user name and password specified by their Person object. This means that each client can have its own credentials. To enable multi-user authentication, give the `mode` option a value of `multi-user`.

These and all other UCS/CS options are described on the **Configuration Options** page.

## Role-Based Access Control

Role-based access control is available in UCS/CS starting in release 8.1.0. See

- [UCS Role Privileges](#) in this User's Guide.
- [Role-Based Access Control](#) in the Context Services Developer's Guide.