



# Progeny Security Features

Your Data is Reliably Secure and Easy to Manage

## User Identification and Authentication

The User ID and encrypted password control who has access to a database.

## Auditing

This feature helps you maintain a record of actions on the database. The database engine has extensive auditing available including log file operations. Progeny additionally includes the option to maintain a history (the date, time, user, and previous value) of every change made to individual data or sample data.

## Database Encryption

Database encryption features allow you to choose the level of database encryption. You can choose to secure your database either with simple encryption, or with strong encryption. Simple encryption is equivalent to obfuscation. Strong encryption renders the database completely inaccessible without an encryption key.

## Transport-Layer Security

You can use transport-layer security to authenticate communications between client applications and the database server. Transport-layer security uses simple, elliptic curve, or RSA encryption technology. Separately licensable components are required for RSA and elliptic curve encryption.

## Discretionary Access Control Features

The actions that a user can carry out while connected to a database are defined within the User ID.

## User and User-Class Definitions

Users are assigned to class definitions to determine the roles and permissions throughout the software. General permissions such as access to spreadsheets, the data warehouse, markers, and form design are also assigned to the User ID. Integrated login is available for environments where it is required.

## Field Level Security

Class based security can be defined even at the field level. Roles and permissions can be setup to determine what rights a given category of users has to modify or view data fields.

## **Folder Level Security**

The ability to read, add, delete, and modify is controlled at the folder level. Security applies to folders throughout the software including data field folders. This flexibility is ideal for setting up scenarios where one group of users is not able to read or to modify another group's data. Folder level security makes it possible for several institutions or groups to share a single database. Each institution may be unaware of the other members.

## **Pedigree Level Security**

Read and write access can be assigned to an individual pedigree. The permissions are assigned via the user class.

## **Database Level Security**

The user can set the level of security on the database by restricting functions such as the ability to add, delete, or modify a pedigree or individual folder as well as the ability to add, delete, or modify a data folder.

## **Password Expiration**

Passwords have a forced expiration every 180 days after which they must be changed. The new password is validated to not contain the old password.

## **Password Naming Conventions Enforced**

Passwords are required to be 6 characters long, contain both letters and numbers, and cannot include the User ID.

## **External Access Protection**

Access to the Progeny database from outside the Progeny application is restricted to the Progeny administrator User ID.

## **Login Auditing**

Each login to the database is audited. The User ID, operating system, application, host name, login date, and logout date are recorded for every successful and unsuccessful login.

## **C2 Certification**

C2 is a set of security guidelines established by the U.S. government to maintain consistency within their organization. If you have the appropriate hardware, you can set up your machine to run in a C2 certified manner.