



www.turbotag.com

TurboTag® User Manager Software
Version 1.3.0.0
Setup and Operating Instructions

Table of Contents

Electronic Signatures and Administration of <i>Session Manager DB</i> Software	2
Installation and Initialization of Software	3
Operating User Manager Software	5
<i>Viewing Users</i>	6
<i>Adding New Users</i>	7
<i>Editing User Profiles</i>	9
User Roles	15
Database Tables Affected by <i>User Manager</i>	16
Database Backup and Restore	19
Administrator Access Recovery	23

Electronic Signatures and Administration of *Session Manager DB* Software

Session Manager DB software is intended for users that require all temperature monitoring operations to be compliant with standards that require electronic signatures in their system.

This software and hardware system is specifically designed to be in conformance with the US Food and Drug Administration specification known as 21 CFR Part 11. This regulatory specification requires that all operations be limited to authorized users, that each fundamental operation is associated with a known user identification (protected by a password), and that only tag data derived from tags that are validated for use with the system be detected and entered into database memory as a compliant data set.

This information system consists of two software installation packages (installed simultaneously):

- (1) *TurboTag*[®] *User Manager* software
- (2) *Session Manager DB* software

Both software programs communicate with the installed *TurboTag*[®] database. *Session Manager DB* performs reading and writing operations with T-700 tags and associates these operations with an electronic signature that is activated by user login. This login is validated against a registered User Name and Password that can only be set by a User.

TurboTag[®] *User Manager* Software records electronic signature events in the same database that contains data from validated T-700 tags and associated non-tag data. A summary record of user status and profile information is displayed in *TurboTag*[®] *User Manager* software, and certain aspects of this can be edited.

This user profile information includes date the profile was created, last login, date of last password change, date of password reset and date locked (if locked), role assignments, and *TagMate USB*[®] assignments.¹

TurboTag[®] *User Manager* Software is typically installed on each user machine,² but only accessible to administration level personnel.

¹ *TagMate USB*[®] is a handheld device for processing tags (see separate instructions). It can be operated under user access control for CFR compliance.

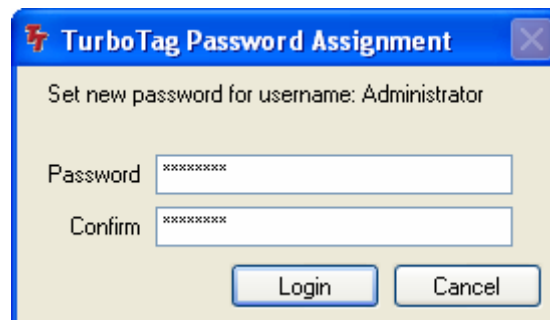
² A single copy of the database can be shared over a network. In this case, *User Manager* is only installed once in connection with the server installation; a client version of *Session Manager DB* is used for all workstation installations.

Installation and Initialization of Software

The installation of the *User Manager* software is part of the *Session Manager DB* installation process.

- Insert the *Session Manager DB* Software Installation CD and select Install.
- Follow all on-screen prompts. Accept license terms and default options.
- When the installation processes are complete, you will have a *TurboTag*® *Session Manager DB* icon on your desktop.
- There is no icon for User Manager software – it may be accessed via the Windows® Start menu (Start → Programs → TurboTag → User Manager).

When ready to manage users, it is first necessary to set up the administrator-level user logins. This is done via *User Manager* software. Upon opening this software, a special login screen appears for first-time use, prompting for creation of a password for the user called “Administrator”:



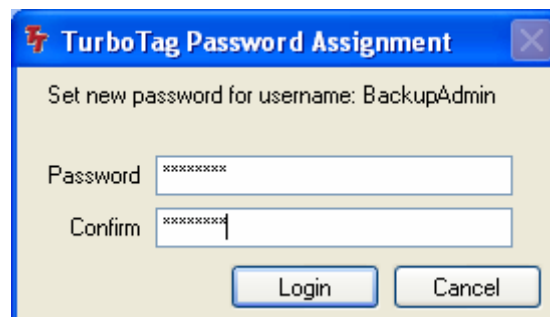
The screenshot shows a dialog box titled "TurboTag Password Assignment". The text inside reads "Set new password for username: Administrator". There are two input fields: "Password" and "Confirm", both containing eight asterisks. At the bottom, there are two buttons: "Login" and "Cancel".

Type and re-type an 8-character password and click the Login button.

Note:

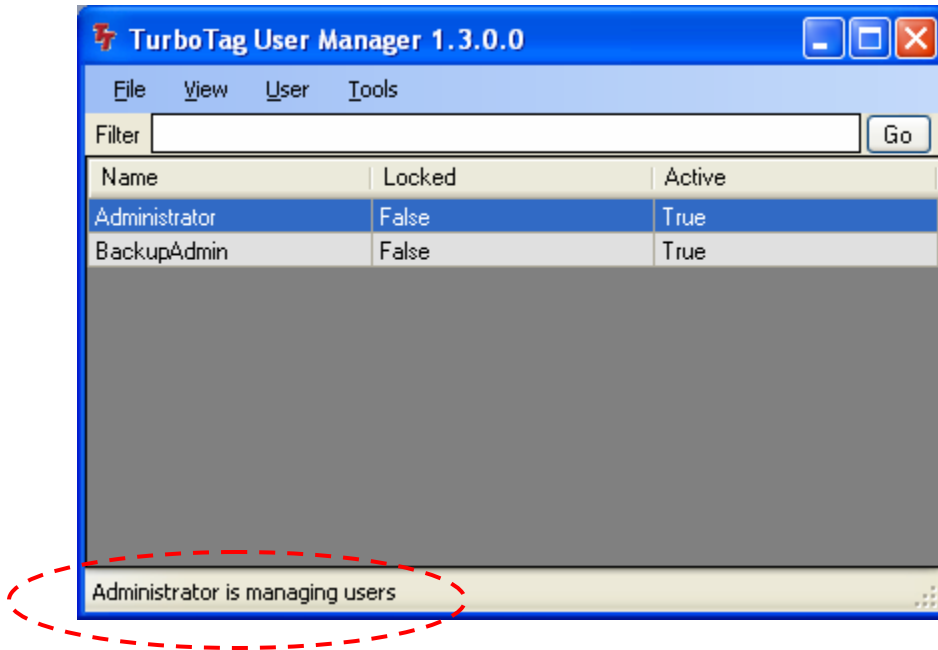
Good practice for setting difficult-to-guess passwords (e.g., mixing upper and lower case text, and mixing numbers and letters) should be followed at all times. Make sure that Caps Lock is not on during this process. MAKE SURE that you remember this password!

After setting the “Administrator” user’s password, a confirmation message appears. Then the process repeats for the user called “BackupAdmin”:



The screenshot shows a dialog box titled "TurboTag Password Assignment". The text inside reads "Set new password for username: BackupAdmin". There are two input fields: "Password" and "Confirm", both containing eight asterisks. At the bottom, there are two buttons: "Login" and "Cancel".

After setting the passwords for both of these users the software screen is displayed, showing these two users:



The purpose behind these pre-defined users is as follows:

- **Administrator:** Serves as a default user in all software operations, including *Session Manager DB* in cases where other users are not needed. Serves as the main user administrator only in cases where other users are created for using *Session Manager DB* (recommended).
- **BackupAdmin:** Serves as a backup user administrator, as the name implies. This user should not be used for *Session Manager DB* operations—other users should be created as needed for that purpose. This user is reserved for a specific purpose: to reset the password for the **Administrator** user. Resetting of passwords, and lockout circumstances are described below.

Note that, in the screen above (red circle) an indication as to the currently logged-in user is given. The logged-in user is Administrator in any case were the Password Assignment dialog box was encountered at startup.

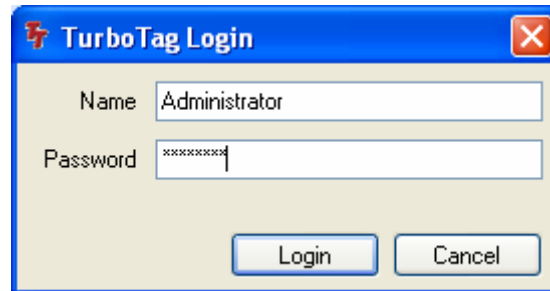
From the screen above, it would be possible to start operating the software as described below. For the sake of familiarization, it is recommended that the software be closed at this point, then re-opened per the instructions given below for regular use.

Operating User Manager Software

For initial use, following the initialization process described above.

The *User Manager* application can be run from the Windows® Start Menu (Programs → TurboTag → User Manager), or by clicking on the application icon for User Manager, stored in the folder named C:\Program Files\TurboTag.

The Login screen will appear:



The example shown above shows the Administrator user logging in.

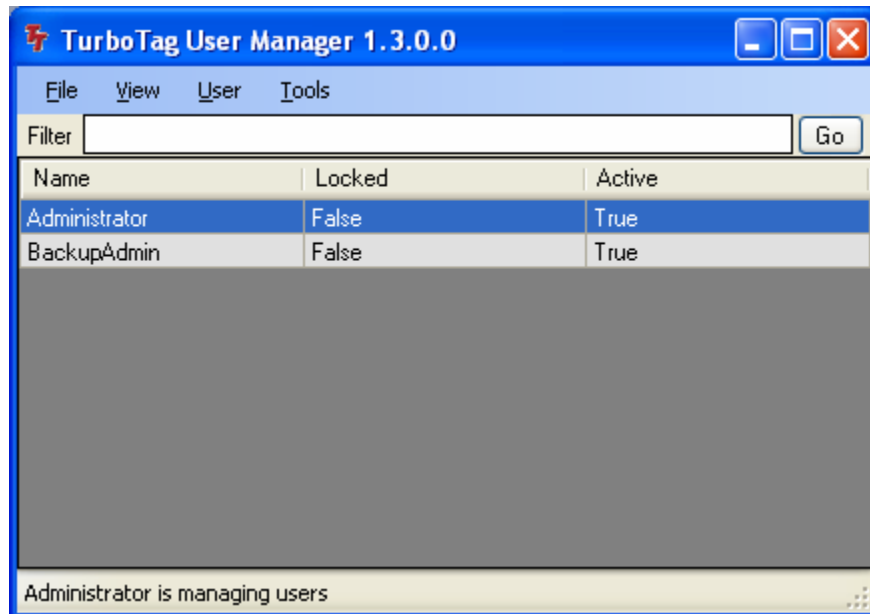
The following notes apply to the login process:

- User names and passwords are shared between both *Session Manager DB* and *User Manager*.
- Not all *Session Manager DB* users will have access to *User Manager*, but all users will have login access to *Session Manager DB* (see discussion of user roles and access limitations given below).
- The only pre-defined users are “Administrator” and “BackupAdmin”. All others are created within *User Manager* by a user administrator.
- Passwords can only be set and changed in *Session Manager DB*.

In addition to being one of the pre-defined users in the database, the “Administrator” is the only user that can restore the database to a previously backed-up version (see ***Database Backup and Restore*** below).

Viewing Users

After clicking on the Login button, the following program window will appear:



The listing above contains the two pre-defined users, Administrator and BackupAdmin, as would be the case on first entry into the program. The name of the user (Administrator) who logged in is displayed in the status bar at the bottom of the screen, and the software version number is displayed at the top of the screen.

As new users are created, they will become visible in this listing, which allows viewers to filter it by either (or both), of two methods:

- Entry of text into the Filter box (then clicking the “Go” button) to limit to User Names to those containing the text entered. This feature helps you to search for certain user names and/or to shorten the displayed list of users. To restore the unfiltered view, delete the entry in the Filter box and click “Go” again.
- Updating the View menu selection. The View menu provides three pre-defined view filters (All; Active Only; Inactive Only). The software default is “Active Only”, and this setting is re-established on each startup.

Note that the Active status of a user is displayed in the listing along with the Locked status of the user. The significance of these attributes is as follows: if a user is inactive (Active = False) or locked out (Locked = True), he cannot log in to *User Manager* or *Session Manager DB*.

Although these two status flags may seem redundant in terms of their consequences, they are different in terms of their causes:

- A user can only be made inactive (Active = False) by someone else, specifically, by an administrator-type user having access to *User Manager* Software. Whenever a user is made inactive, he is also locked out.
- An active user can cause himself to be locked out (Locked = True) by more than nine consecutive failed login attempts in *Session Manager DB* software.

Changes in the Locked and Active status made from within *User Manager* are recorded in the companion database along with identification information for the user affected and the user making the change. The log of these actions can be viewed from within *Session Manager DB* software (see separate user guide for that software, discussion on viewing non-tag audit trail events).

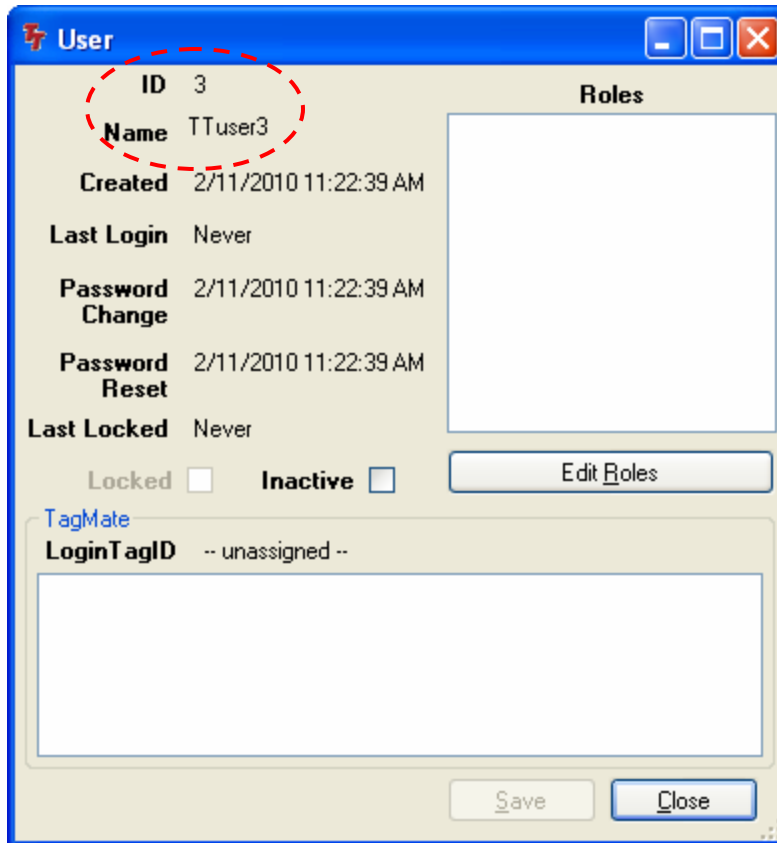
Adding New Users

Upon startup, the first task will be the creation of more Users. The creation of new users is initiated by the menu command (User → New... or Ctrl+N). This brings up the (New) User screen:

The screenshot shows a 'User' dialog box with the following fields and controls:

- ID:** 1
- Name:** TTuser3
- Created:** 2/11/2010 11:17:27 AM
- Last Login:** Never
- Password Change:** 2/11/2010 11:17:27 AM
- Password Reset:** 2/11/2010 11:17:27 AM
- Last Locked:** Never
- Locked:**
- Inactive:**
- Roles:** To assign Roles, Save User
- Edit Roles:** Button
- TagMate:** LoginTagID -- unassigned --
- Save:** Button
- Cancel:** Button

In the example above, a new user name has been entered ("TTuser3"). Clicking the Save button will lead to an updated User screen, as shown below. Note the fact that the ID number has been updated and the user name can no longer be edited:



As seen above, newly created users have no assigned Roles unless further editing of their profile is carried out, as described below. A lack of assigned Roles means that a user will have only limited access to *Session Manager DB* and no access to *User Manager*.

Note that the User screen can be used to check the recent history of a user. Time of User Creation, along with most recent Login (*Session Manager DB*) / Password Change / Password Reset / Lockout events are displayed in this screen, as is the Inactive / Locked status.

Note also that there is a TagMate area at the bottom showing LoginTagID (unassigned). There are no entries in the box below it; this box would show any assigned *TagMate*[®] USB handhelds. *TagMate*[®] USB assignments and LoginTagID are not editable in *User Manager*, but rather in *Session Manager DB*.

Immediately after their creation, new users are in a "Password Reset" state, which is not evident in the screen above. This state allows one *Session Manager DB* login within three days of the reset. During this login, the user will be required to set a new password. If the user fails to login within the three day period, the user will be locked out and another reset will be necessary in *User Manager*. The procedure for resetting a password is described below.³

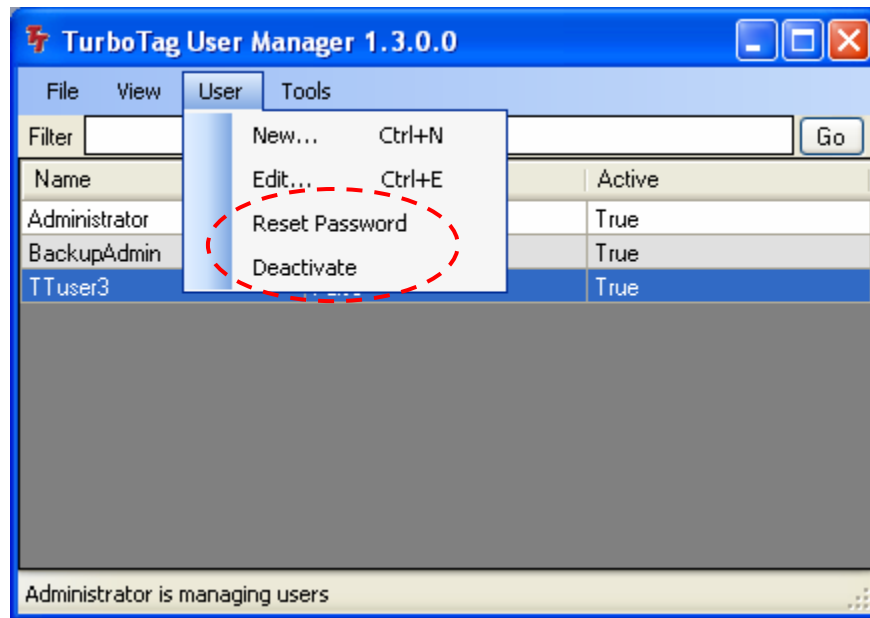
³ It is possible to reset the password for the Administrator and BackupAdmin users, as with any other users, and it is also possible to set the new passwords in *Session Manager DB*, as with other users. In contrast, however, these two pre-defined users' new passwords can be supplied directly in *User Manager* at startup, by the so-called initialization process described above.

Editing User Profiles

In *User Manager*, existing user profiles may be modified in the following ways:

- (1) Reset Password
- (2) Deactivate
- (3) Re-activate
- (4) Edit Roles

The first two modifications can be carried out from the Main listing screen, acting upon whichever user is highlighted. These two processes are under the User menu, as shown in the screen below:

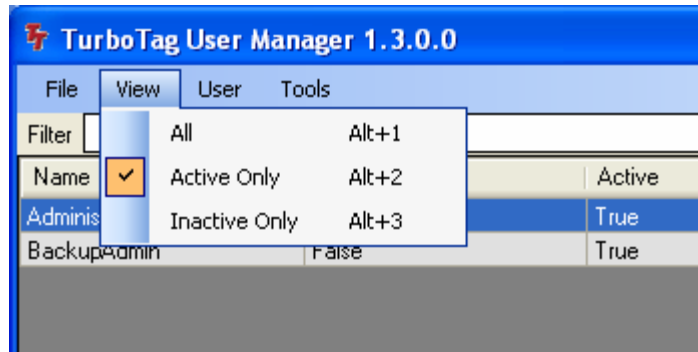


The following notes apply to these two menu actions:

- These commands would be disabled for inactive users AND for the currently logged-in user (Administrator, in this case).
- Unless the current viewing filter is set to "All" via the View menu, de-activation of a user will cause the name to disappear from the listing. Re-activation is described below.

The remaining two options are to re-activate a user or to edit the user's Roles.

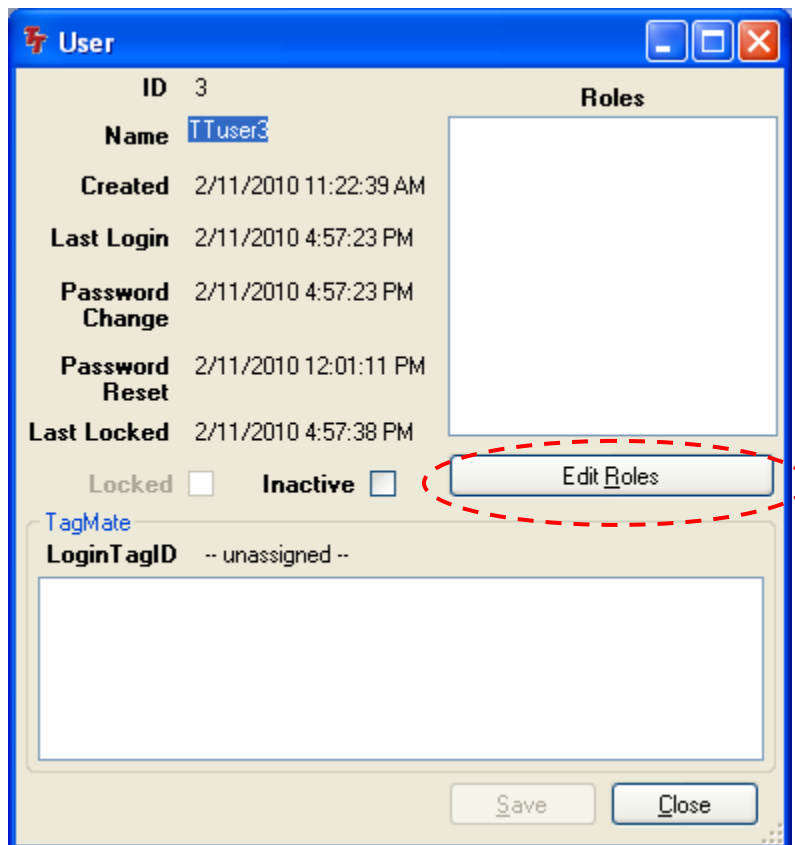
The only way to access users in need of re-activation on the listing is to change the viewing filter (View menu selection, see below) from its default value of "Active Only" to "All" or "Inactive Only".



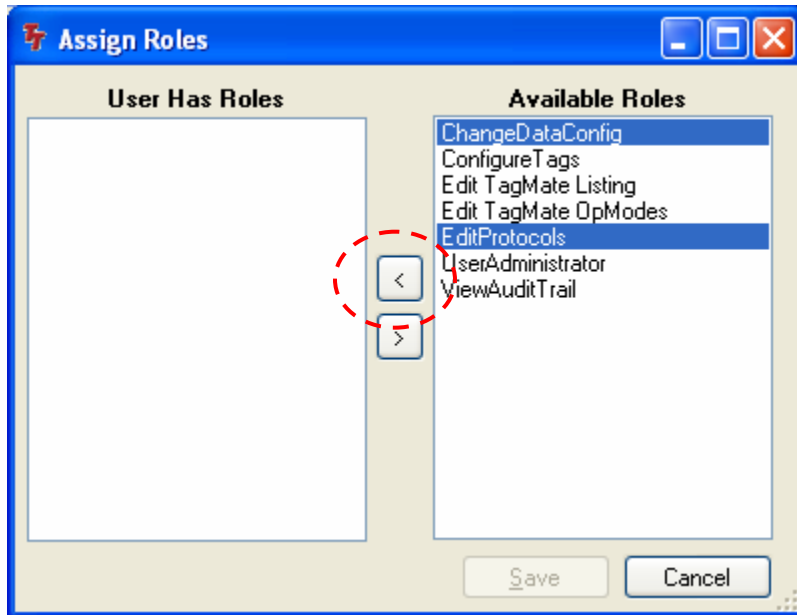
In order to re-activate a user or to update Role assignments, double-click the user name in the listing, or single-click to select the user, then select the menu command (User → Edit... or Ctrl+E). This will bring up the User screen for the selected user.

Editing Roles

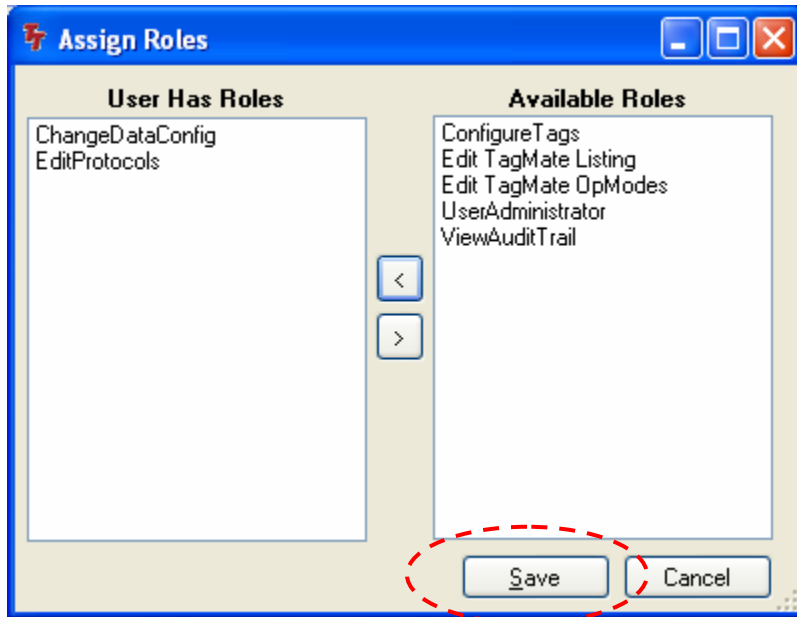
In the example shown below, the user “TTuser3” was selected for editing and the User screen has appeared:



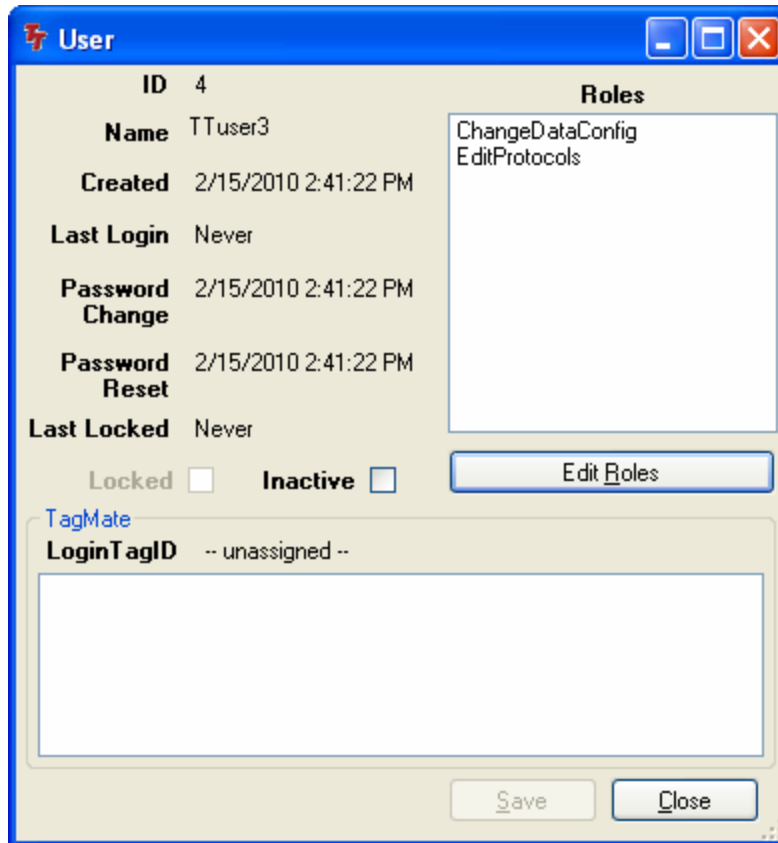
Note that this user has “Active, Unlocked” status (note also that only the Active status can be edited from the User screen, by checking / un-checking the “Inactive” box). This user has no assigned Roles. Clicking on “Edit Roles” brings up a second window:



In this example, two Roles have been selected for addition in the window on the left. Clicking the “<” button transfers these roles to the box on the left and removes them from the box on the right:



Clicking “Save” will return to the User screen, now with the three new Roles added, as shown below:



A similar sequence can be used to remove existing Roles.

User Re-Activation

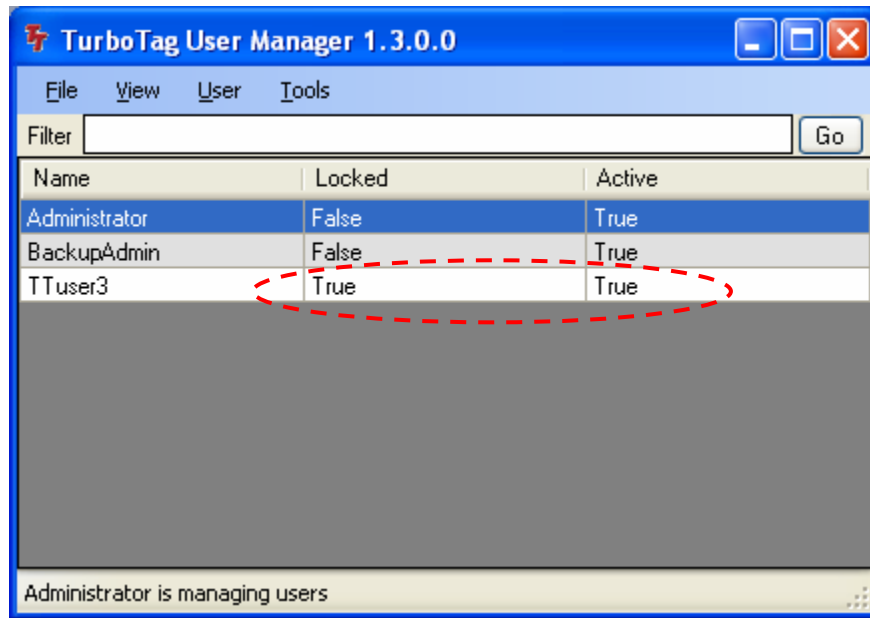
In the following example, the user “TTuser3” is being edited. As the User display shows, this user has been Deactivated, and (concurrently) Locked Out. Note that both of these status consequences follow from the User → Deactivate command described above.

The process of re-activating a User involves two steps. The first step is the un-check the “Inactive” box in the User screen and click “Save”:

The screenshot shows a window titled "User" with the following details:

- ID:** 4
- Name:** TTuser3
- Created:** 2/15/2010 2:41:22 PM
- Last Login:** Never
- Password Change:** 2/15/2010 2:41:22 PM
- Password Reset:** 2/15/2010 2:41:22 PM
- Last Locked:** 2/15/2010 2:43:38 PM
- Locked:**
- Inactive:** (highlighted with a red dashed circle)
- Roles:** ChangeDataConfig, EditProtocols
- TagMate LoginTagID:** -- unassigned --
- Buttons:** Edit Roles, Save (highlighted with a red dashed circle), Close (highlighted with a red dashed circle)

Returning to the User listing (below), it can be seen that TTuser3 now has Active = True, but also Locked = True. In order to restore the ability of TTuser3 to log in to *Session Manager DB*, the Locked status must be changed to False.



This is done with the previously-described Reset Password Menu command, as follows:

- Click on TTuser3 in the listing to select it.
- Select the User → Reset Password command.
- When the password has been reset, a dialog confirms this action:



Remember that resetting is not complete until the user logs in to *Session Manager DB*. This must be done within three days or the user will be locked out again and need to be reset again in *User Manager*.

Note:

This section has described several ways to edit user profiles. It should be noted, however, that the options presented did NOT include deleting users, as this is not possible, just as it is not possible to delete any event records from the companion database. The only similar option is to de-activate users. Also, it is not possible to modify a User Name, so as to ensure correct interpretation of audit trail records over time.

User Roles

The following table summarizes the function of each of the Roles that can be assigned to Users using *User Manager*:

Role	Software Command	Software Function
ChangeDataConfig	<i>Session Manager DB</i> Database Event Log → Configure button off of Main Screen	Controls access to a dialog for changing the active event log fields and their settings.
ConfigureTags	<i>Session Manager DB</i> Mode selector on Main Screen (START)	Controls access to the radio button cluster for start mode in the START screen. If no access is given, this cluster is set to "Start Only".
Edit TagMate Listing	<i>Session Manager DB</i> TagMate USB → Device Listing menu command off of Main Screen	Controls access to a dialog for addition/removal of TagMates, assignment of operating modes to TagMates, and assignment of users (sub-dialog).
Edit TagMate OpModes	<i>Session Manager DB</i> TagMate USB → Operating Modes menu command off of Main Screen	Controls access to a dialog for creation and editing of operating modes for TagMate USBs.
EditProtocols	<i>Session Manager DB</i> Protocols → Update button off of Main Screen (START)	Controls access to the protocol creation dialog accessed via the START screen.
ViewAuditTrail	<i>Session Manager DB</i> View Audit Events button on the Tag Record Set Selector screen (accessed via READ screen with DB=> button).	Controls access to the screen used for viewing tag-processing-related and user-management-related audit trail history.
UserAdministrator	<i>User Manager</i> Login window <i>Session Manager DB</i> TagMate → User ID Tags menu command off of Main Screen Edit Users button off of TagMate Listing Screen	Controls ability to login. If no access is given, login box displays a "Permission Denied" message and stays open. Assignment of ID tags to users. These tags are used with TagMate USB handhelds when carrying out CFR-compliant operations. Assignment of users to TagMates for CFR-compliant operations.

Details about the affected operations of each Role for *Session Manager DB* are found in the companion user guide for *Session Manager DB*.

Database Tables Affected by User Manager

Note:

The following information is for general reference, but is not required for proper operation of User Manager software.

The companion database is shared between *User Manager* and *Session Manager DB* Software. This database contains three tables that are modified by *User Manager* operations described above. These tables are: **dbo.User**, **dbo.AuditTrail**, and **dbo.User_Role**.

The table **dbo.User** contains a snapshot of each User's profile and history, as displayed in *User Manager's* User screen. Its fields comprise the following:

Field Name	Value	Purpose
UserId	Integer	User identification number
UserName	Alphanumeric	User name
Password	Alphanumeric 32 characters	Encrypted password value
LoginTagID	Alphanumeric 16 hex digits	ID code from assigned TagMate USB login tag
CreateDate	Date/Time (UTC)	Date/Time User was first generated
LastLoginDate	Date/Time (UTC)	Date/Time of last login to <i>Session Manager DB</i>
LastPasswordChange	Date/Time (UTC)	Date/Time of last password change in <i>Session Manager DB</i>
LastPasswordReset	Date/Time (UTC)	Date/Time of last password reset operation in <i>User Manager</i>
IsLockedOut	Binary True/False	Locked Out state

LastLockoutDate	Date/Time (UTC)	Date/Time of last lockout event caused in the <i>Session Manager DB™</i> login screen.
Failed Password	Integer 0→9	Counter for consecutive failed login attempts in <i>Session Manager DB™</i>
FailedPasswordWindowStart	Date/Time (UTC)	Unused field (RFU)
IsActive	Binary True/False	Active state

This table is populated with all of the users, active and inactive, that have been entered using *User Manager* software.

Roles are linked to users in the **dbo.User_Role** table. For each instance of an association of a User with a Role, a record is created.

Field Name	Value	Purpose
UserId	Integer	Linking field to User table
RoleId	Integer	Linking field to table of User Roles (dbo.Role).

Logging of certain actions in *User Manager* is carried out via the table **dbo.AuditTrail**. The events that are logged are:

- User Creation
- User Activation
- User Deactivation
- Password Resetting

These events accompany a number of events that are logged into this same table by *Session Manager DB™* software. All of these events can be viewed in *Session Manager DB™* Software, subject to access control associated with Roles. The table fields are listed below:

Field Name	Value	Purpose
AuditTrailId	GUID (string)	System-generated ID field <i>not displayed</i>

SystemId	Alphanumeric	Hardware address (MAC address of an Ethernet adapter) <i>not displayed</i>
SoftwareVersion	Alphanumeric	Version number for <i>User Manager</i> or <i>Session Manager DB</i> <i>not displayed</i>
SoftwareSerial	Alphanumeric	<i>Session Manager DB</i> serial number (not used by <u>User Manager</u>) <i>not displayed</i>
UserId	Integer	Linking field to User table; this is the User performing the action.
CFREvent	Binary True/False	Flag for electronic signature active (only CFR events are logged presently) <i>not displayed</i>
EventType	Integer	Linking field to static table of event types (dbo.Event_Type).
EventDetails	Alphanumeric	Additional information (generally the User Name of the affected User).
CreateDate	Date/Time(UTC)	Date/Time of event.
Checksum	Alphanumeric 32 characters	Data integrity check value, created by Session Manager and User Manager. <i>not displayed</i>

Database Backup and Restore

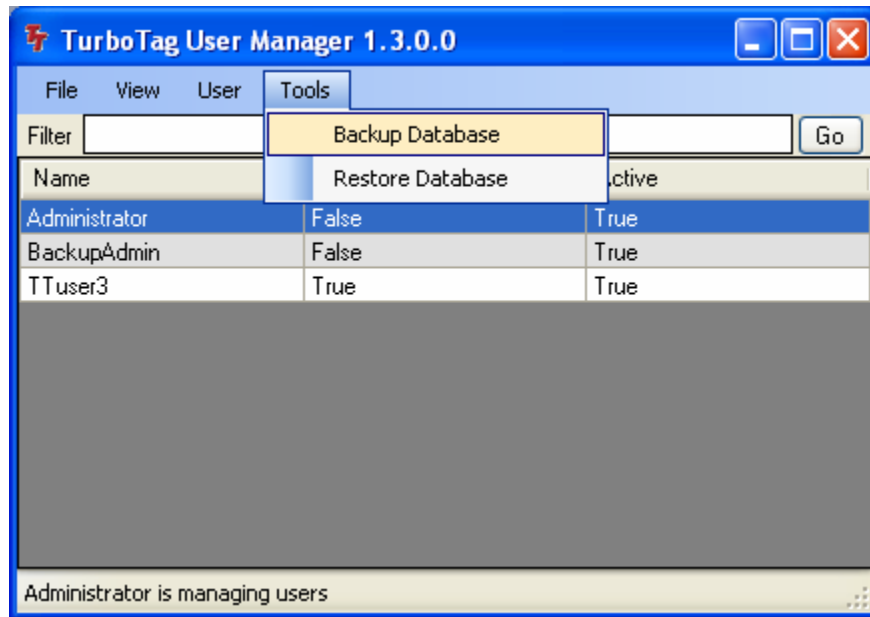
The entire *Session Manager* database (user profiles, protocols, TagMate settings, and tag data) can be backed up as often as desired, then restored to a previous version if it becomes necessary to deal with data loss or corruption. This process is not unlike saving a file and then re-loading it later.

Note:

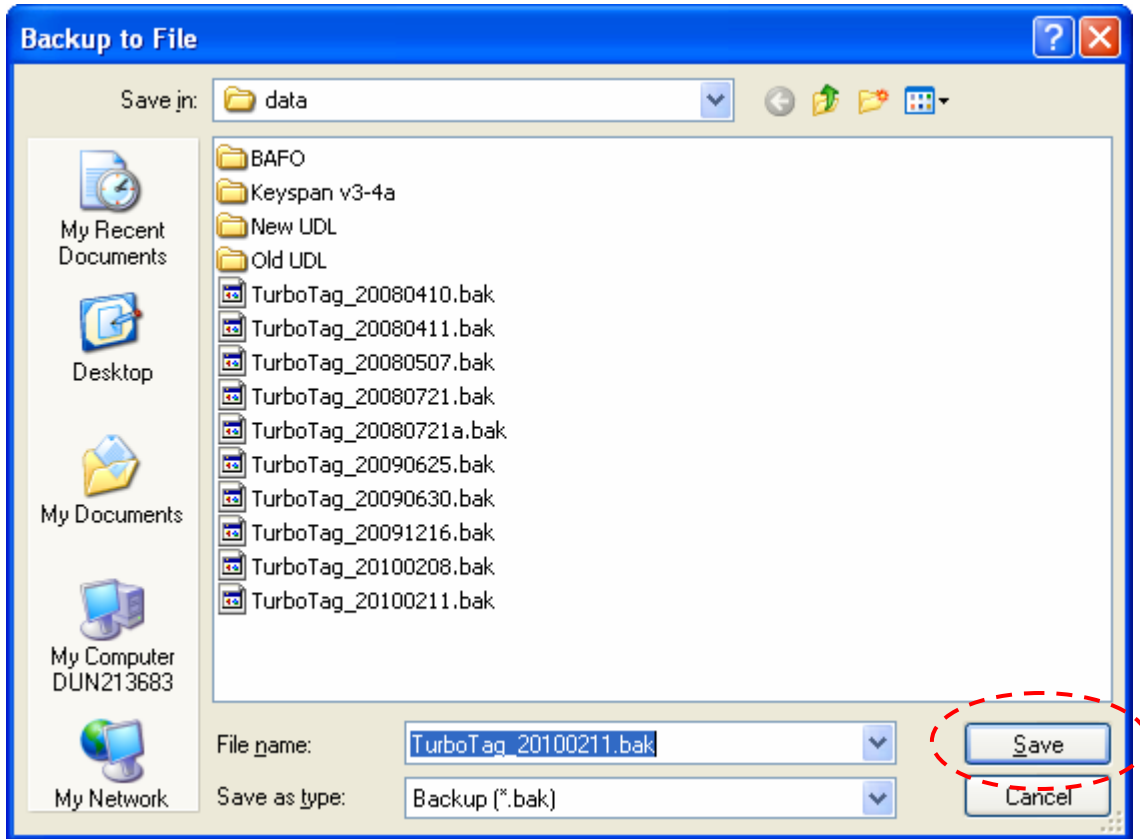
Restoring to a previous database version affects user tables as well as data tables. User status will revert to the status as of the backup—it is possible that passwords will have expired; some users may not exist, etc. Some recent tag data may be lost as well. It is best to backup frequently so that any restore operation will have minimal impact on data.

Backup

The process of backing up can be carried out by any user logged into *User Manager*. It is accessed via the Tools menu, as shown below.



The result of selecting this command is a dialog prompt for file creation. Click "Save" to complete the operation (a confirmation screen appears). Do not change the file name or folder name.



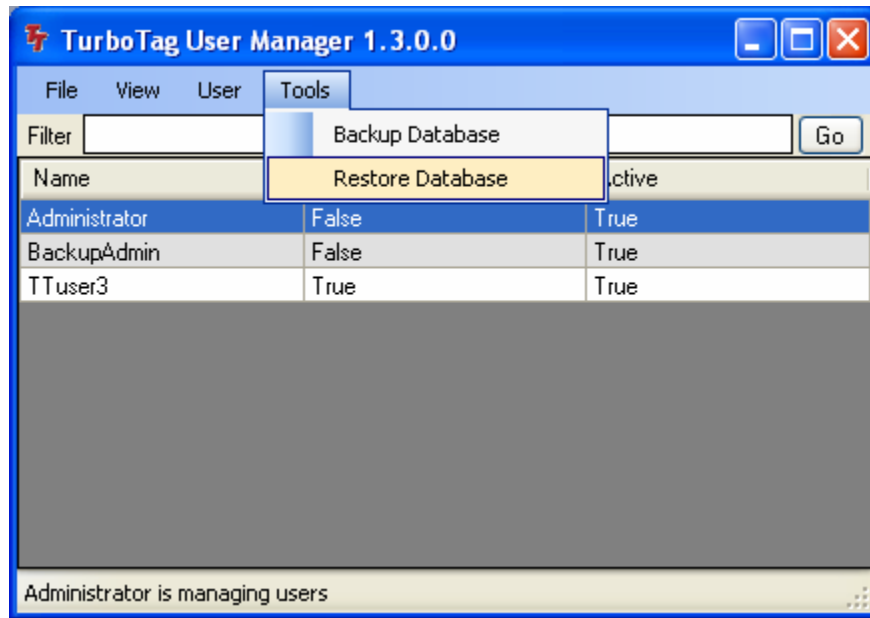
Restore

The process of restoring from a backup file (previous section) can ONLY be carried out by the "Administrator" user. This ensures that the database is not restored to a version for which that user did not exist (the Administrator is the one pre-defined user, and like all users, cannot be deleted). This process is expected to be done infrequently or never, and will cause a loss of all data added after the creation of the backup copy being used.

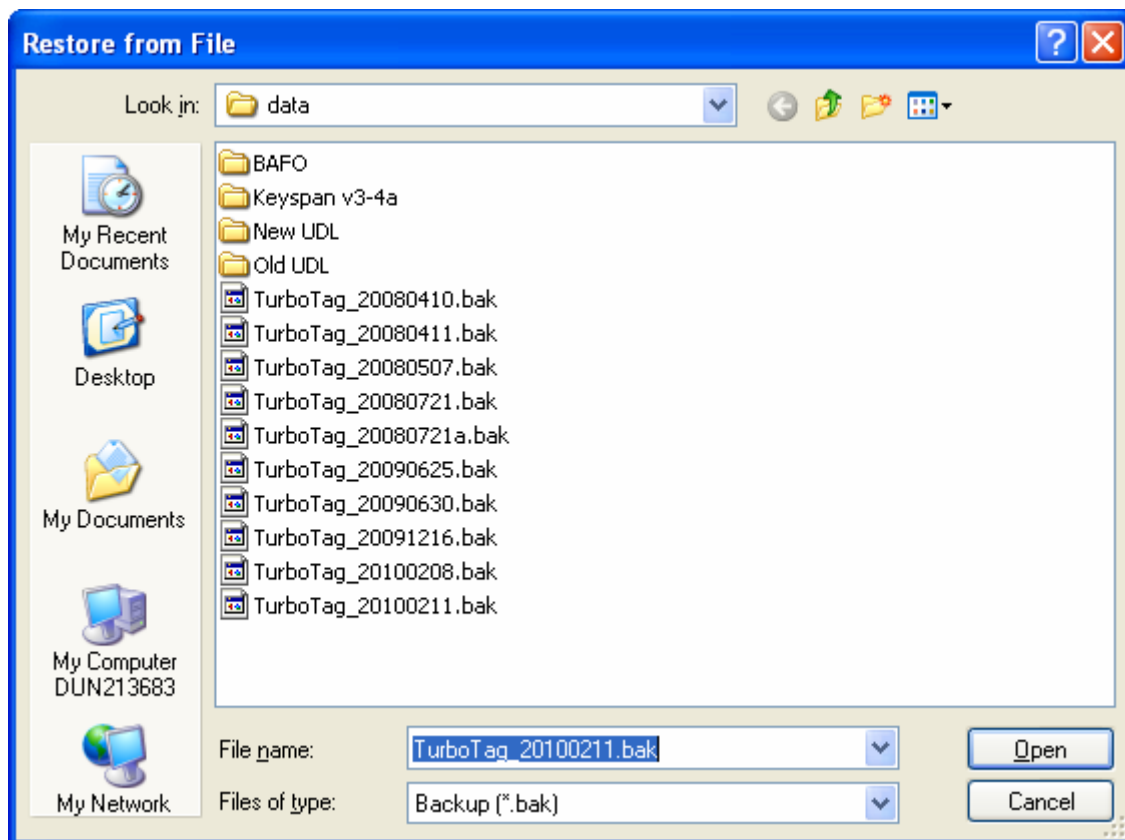
Note:

Unless there is corrupted data, it is best to backup the database immediately before restoring it to an earlier state. This offers the only means to "undo" the restore action and recover the current state.

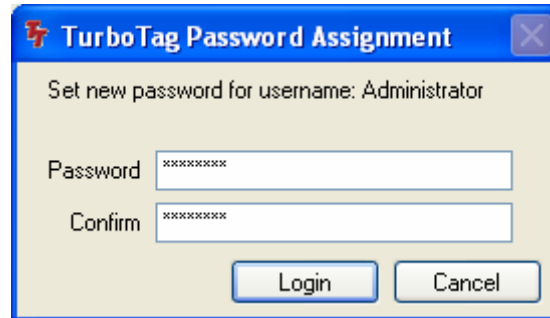
The process of restoring starts from the Tools menu (Restore Database command):



This brings up a dialog for file selection, defaulting to the most recent file:



After file selection, click “Open” to activate the restore function (NOT undo-able; see Note above). A confirmation screen appears. Immediately after this, a login will appear for re-setting the Administrator password. It is OK to re-use the password which was supplied at the original login:



The image shows a Windows-style dialog box titled "TurboTag Password Assignment". The dialog has a blue title bar with a close button (X) on the right. The main area has a light beige background. At the top, it says "Set new password for username: Administrator". Below this, there are two text input fields. The first is labeled "Password" and contains seven asterisks. The second is labeled "Confirm" and also contains seven asterisks. At the bottom of the dialog, there are two buttons: "Login" and "Cancel".

This re-setting of the password is used to ensure that at least one active user having a *known password* is active after the restore operation, with that user being *Administrator*. Other users may have expired or different passwords due to the time that elapsed since the backup had been created. In this case, they may be prompted to change passwords when logging into *Session Manager DB*, or may require re-setting of their password in *User Manager* as described above.

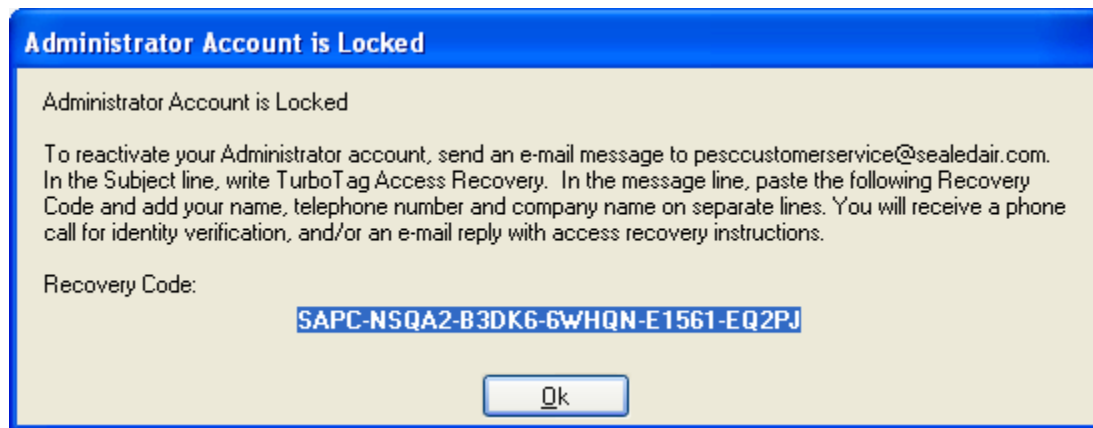
Administrator Access Recovery

Note:

The following procedure is not expected to be necessary if the BackupAdministrator login can be used for resetting the Administrator password, as described above. It is provided as a last resort only.

The lockout of the Administrator user is a special circumstance in *User Manager*.

Whenever a login is attempted as Administrator, and this user is already locked out (a status that arises from >9 successive failed login attempts in *Session Manager DB*), the following access recovery screen appears instead of the usual lockout error message:



This leads to an email-based recovery process whereby, after identity verification, a return email is sent to provide a temporary login (user name and password). This temporary login will be followed by the usual prompt for setting the Administrator password, restoring access of this user to *User Manager*.