

Updating Passwords on a Gentrans System

Last revised: 10/24/03
Shane Cargal

Sterling Commerce
An IBM Company

The information contained in this document represents the current view of Sterling Commerce on the issue discussed as of the date of publication. Because Sterling Commerce must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Sterling Commerce, and Sterling Commerce cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. STERLING COMMERCE MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS DOCUMENT.

© 2000 Sterling Commerce. All rights reserved.

TABLE OF CONTENTS

Purpose	3
Background	3
Windows Integrated Authentication	3
Standard Security (SQL Server Authentication or Oracle RDBMS).....	3
Solution Steps	4
Gentran.....	4
Database	11
Data Source Name (DSN).....	11
Microsoft SQL Server	11
Oracle	11
Windows	13
Windows 2000	13
Windows NT	15
Distributed COM Configuration (DCOM)	16
Verification	19

Purpose

Provide an overview of all the areas that need to be updated, when a password change is required for the user id used to start the Gentran Server for Windows services (Release 3.01 and higher).

Background

There are many possible areas that can be affected by a password change to the Windows user id that is used to start the Gentran Server for Windows services, such as the database, Gentran, and DCOM access.

Not all areas need to be updated, but for the sake of keeping the User ID and password consistent across all areas, it is suggested that the password is updated in all areas. Specifically, the database user id and password, and the Gentran's ODBC access user id and password do not have to be updated when the Windows user id has been updated when using Windows integrated authentication.

It is strongly suggested that a network administrator make all changes regarding the Windows user id and password, along with the changes to the user id and password for the services. It is also recommended that a database administrator make any changes to a password for the database user id.

As always, before making any changes to a production machine, make sure that a current backup has been made, and verify the backup is valid.

Windows Integrated Authentication

When using Windows integrated authentication with Microsoft SQL Server, the passwords in Microsoft SQL Server and in Gentran Server for Windows' ODBC access areas do not have to be updated. In fact, the password fields are unavailable from within Microsoft SQL Server when using Windows integration authentication.

Standard Security (SQL Server Authentication or Oracle RDBMS)

When using Standard Security with Microsoft SQL Server (SQL Server authentication) or Oracle, the passwords do not have to be updated unless the ODBC access areas in Gentran have been updated, or vice versa. It is a good idea to update the password in all areas to keep user id and password in sync with the ones used in Windows.

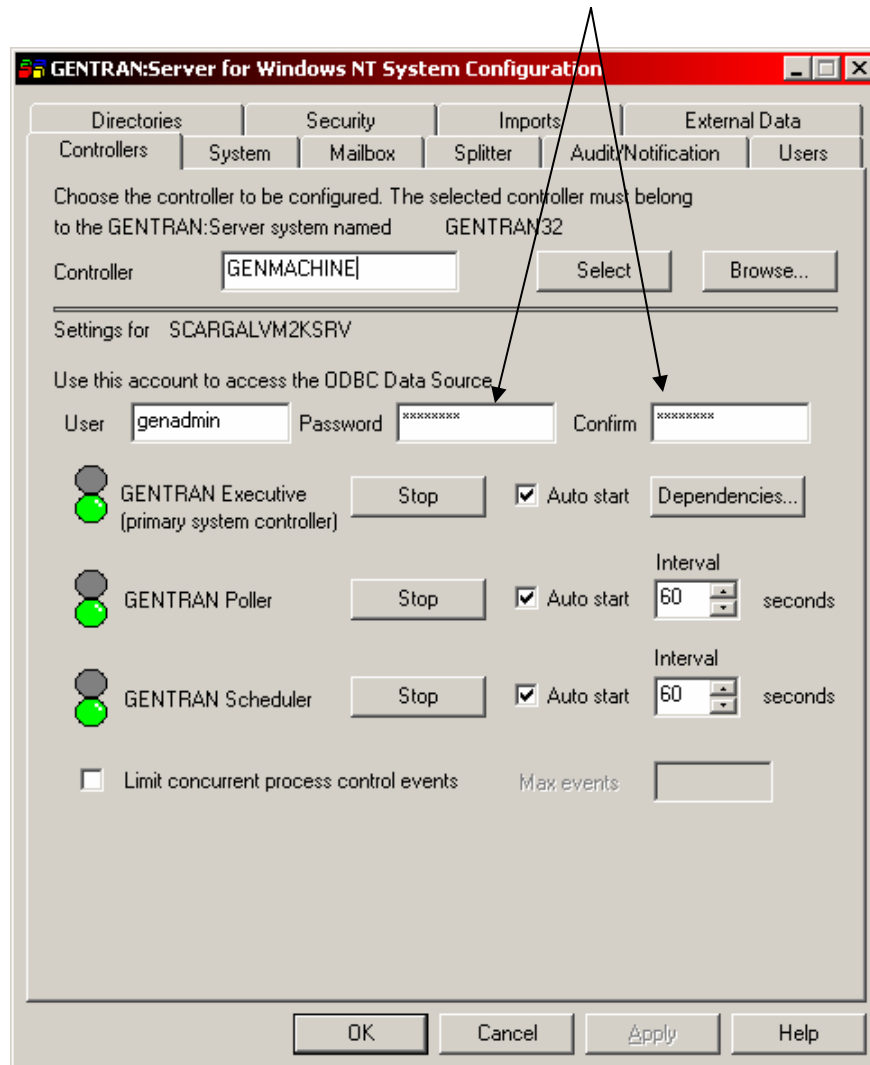
Solution Steps

Gentran

When the password is to be updated in the database, the first place to update it will be in the Gentran Server for Windows ODBC access areas of the Gentran Server System Configuration and then the Gentran Server Mailbox properties.

- 1) Open Gentran Server Configuration.
- 2) Enter the new password in the 'Password' and 'Confirm' fields.

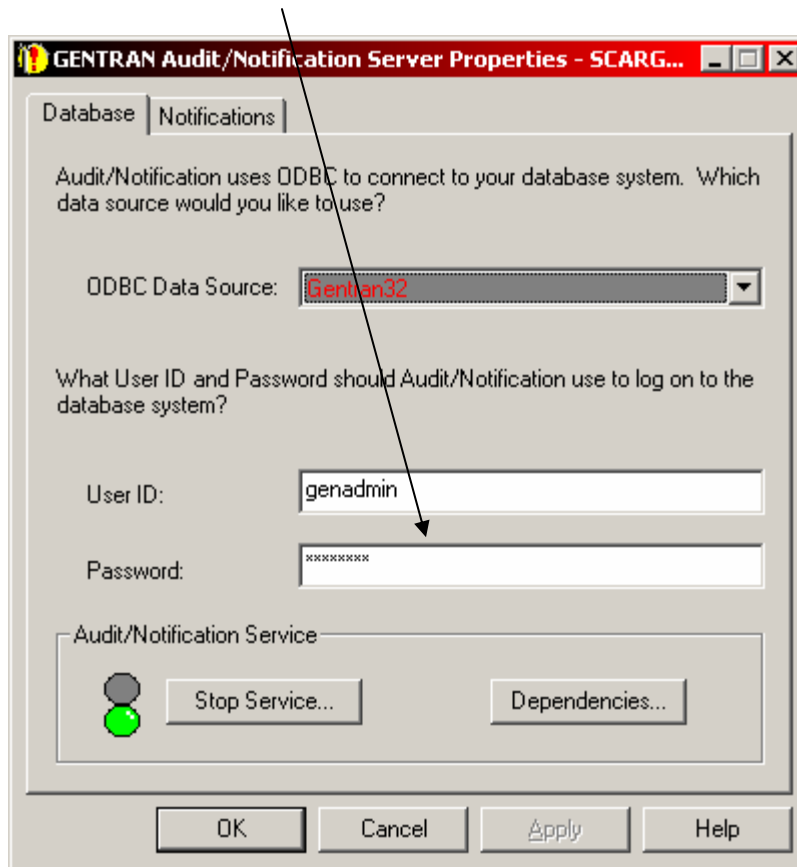
This changes the ODBC database login password for the GENTRAN Server Executive service.



In Gentrans Server Configuration (cont.):

- 1) Click on the 'Audit/Notification' tab.
- 2) Click on the 'Server' button.
- 3) Enter the new password in the 'Password' field.

This changes the ODBC database login password for the Gentrans Audit Notification service.



Next the password must be changed in the Gentrans Server for Windows Mailbox properties.

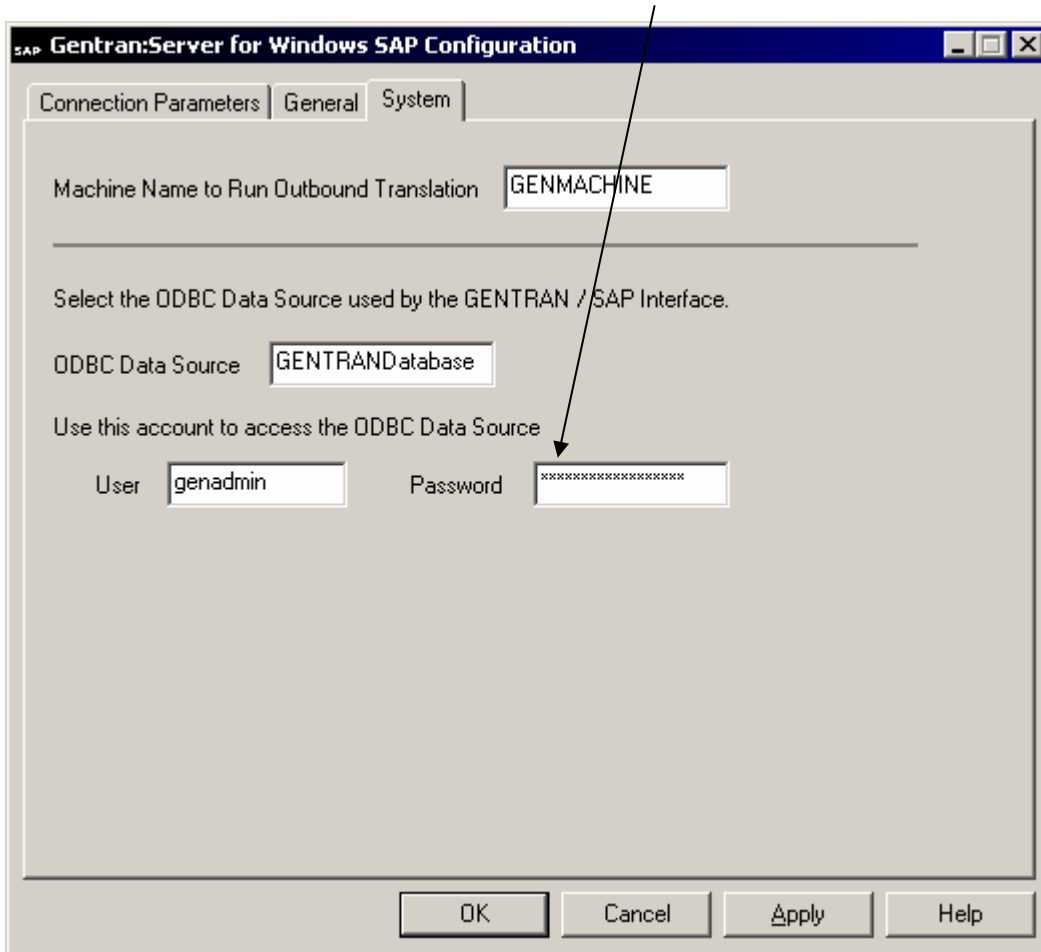
- 1) Open Gentrans Server Mailbox Server Manager.
- 2) Right click on the server name, and select 'Properties.'
- 3) On the 'Database' tab enter the new password in the 'Password' field.

This changes the ODBC database login password for the Gentrans Server Mailbox service.



When using the SAP Extension for Gentrans Server for Windows, the password will need to be updated within the Gentrans Server for Windows SAP Configuration.

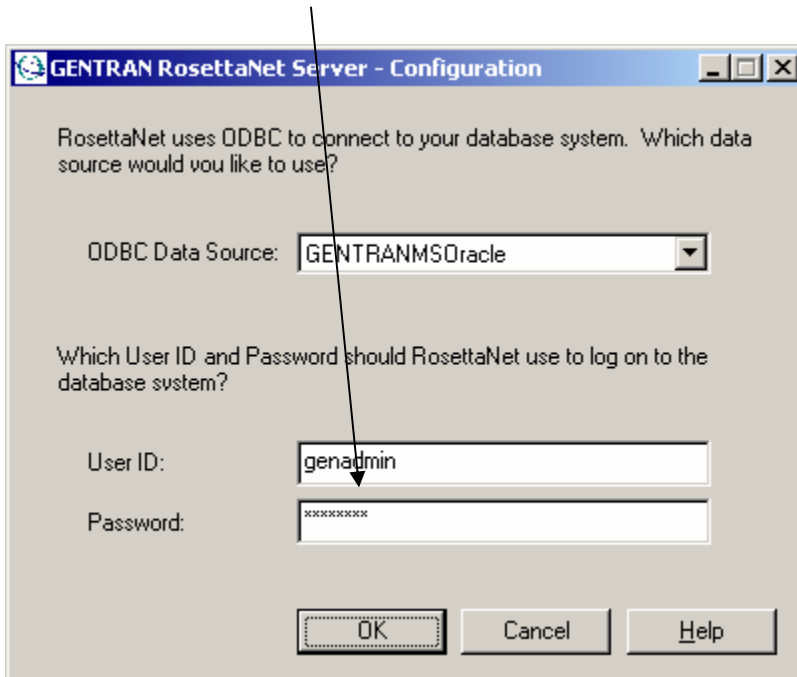
- 1) Open Gentrans Server for Windows SAP Configuration.
- 2) Click on the 'System' tab.
- 3) Enter the new password in the 'Password' field.



The screenshot shows the 'SAP Gentrans:Server for Windows SAP Configuration' dialog box with the 'System' tab selected. The 'Machine Name to Run Outbound Translation' field contains 'GENMACHINE'. Below this, the instruction 'Select the ODBC Data Source used by the GENTRAN / SAP Interface.' is followed by the 'ODBC Data Source' field containing 'GENTRANDatabase'. Underneath, the instruction 'Use this account to access the ODBC Data Source' is followed by the 'User' field containing 'genadmin' and the 'Password' field containing a masked password 'xxxxxxxxxxxx'. An arrow points from the top of the dialog to the password field. At the bottom, there are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

When using RosettaNet for Gentrans Server for Windows version 3.1.1 and 3.2, the password will need to be updated in the Gentrans RosettaNet Server Configuration screen.

- 1) Open Gentrans RosettaNet Server Configuration.
- 2) Enter the new password in the 'Password' field.



GENTRAN RosettaNet Server - Configuration

RosettaNet uses ODBC to connect to your database system. Which data source would you like to use?

ODBC Data Source: GENTRANMSOracle

Which User ID and Password should RosettaNet use to log on to the database system?

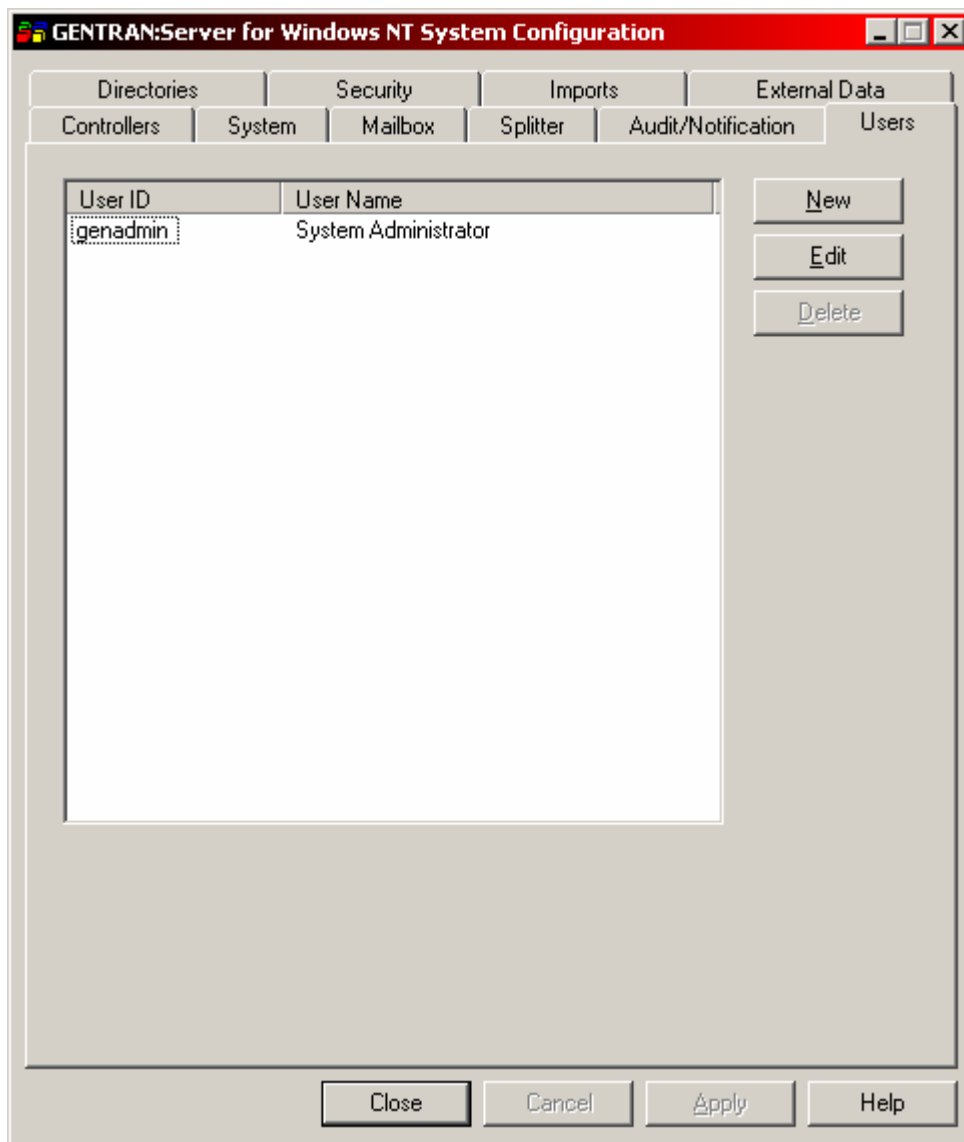
User ID: genadmin

Password: xxxxxxx

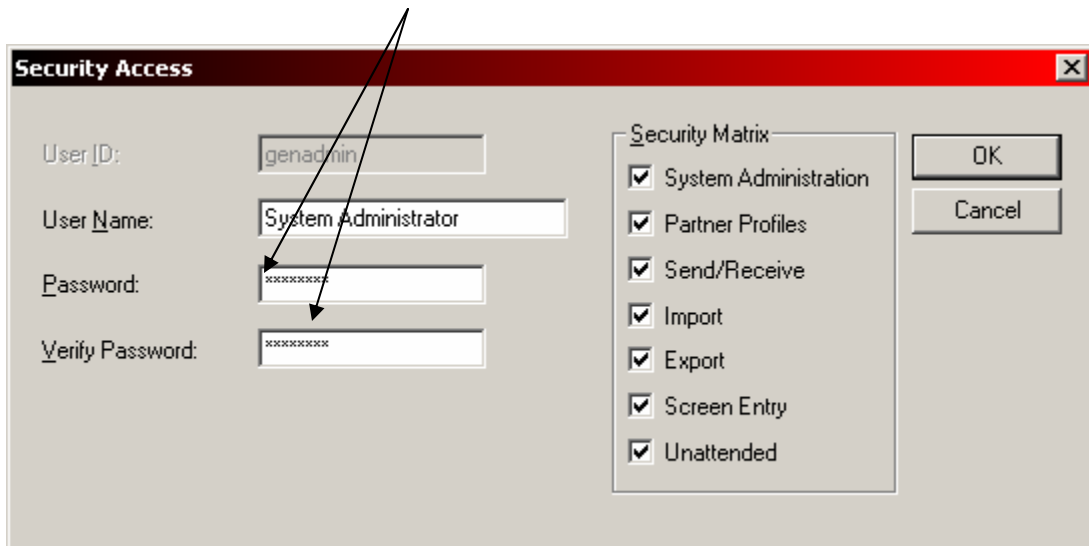
OK Cancel Help

If the User ID that is used to start the Gentrans Services is also used to log into Gentrans and Gentrans is setup to use Windows Integrated Security or Mixed Security, then the password will need to be updated within the Users tab of Gentrans Server Configuration. When using Standard Security the password does not have to be updated, however it is suggested to keep all the passwords same.

- 1) Open Gentrans Server Configuration.
- 2) Click on the 'Users' tab.
- 3) Select the User Id and click 'Edit.'



- 4) Enter the new password in the 'Password' and 'Verify Password' fields.



The screenshot shows a 'Security Access' dialog box with the following fields and options:

- User ID: genadmin
- User Name: System Administrator
- Password: [Redacted]
- Verify Password: [Redacted]
- Security Matrix:
 - System Administration
 - Partner Profiles
 - Send/Receive
 - Import
 - Export
 - Screen Entry
 - Unattended
- Buttons: OK, Cancel

Two arrows point from the top of the dialog box to the Password and Verify Password fields, indicating where to enter the new password.

Database

After the password has been updated in the Gentran Server for Windows' ODBC access areas, the password will need to be updated in the database.

When using Microsoft SQL Server the password can be updated from within Microsoft SQL Server Enterprise Manager. When using Oracle 8i the password can be changed from within DBA Studio, or when using Oracle 9i the password can be changed from within Oracle Enterprise Manager.

For more information regarding changing or updating passwords in the database, see the database vendor software documentation or a database administrator.

Data Source Name (DSN)

Microsoft SQL Server

When using Microsoft SQL Server, the ODBC Data Source name (DSN) contains a User ID and password area. This user id and password entry is only used during an ODBC test for the DSN when using Standard Security (SQL Server Authentication). This user id and password is not used during normal operations and processing.

For the test to be successful when using Standard Security, the password will need to be updated prior to performing an ODBC test.

****Please note:** Any entry in the password field of the DSN setup is not saved once the DSN configuration is closed, and must be re-entered prior to a DSN test. As mentioned before, these user id and password fields are used only when testing the DSN from the DSN setup applet. The user id and password fields here in the DSN setup are only used during the testing of the DSN when using Standard Security, and they are not used by Gentran to access the database.

Oracle

The DSN setup for Oracle 8i and 9i do not require a password, so the DSN will not need

to be modified. The user id and password in the DSN are used only when testing the DSN.

Windows

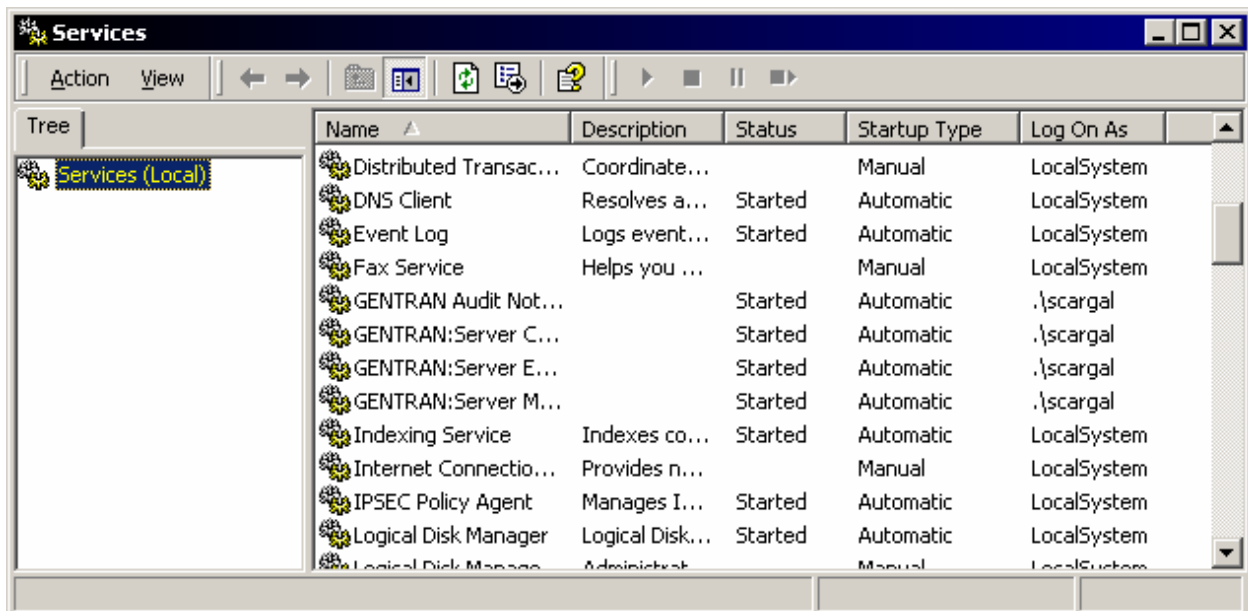
After updating the password for the database access and Gentran Server for Windows' ODBC access areas then the Windows user id and password will need to be updated. The Windows user id that is used to start the Gentran Server for Windows services can be a local user or a domain user. In either case, this user's password will need to be updated.

It is suggested that a network or administrator make any changes regarding any local or domain user accounts.

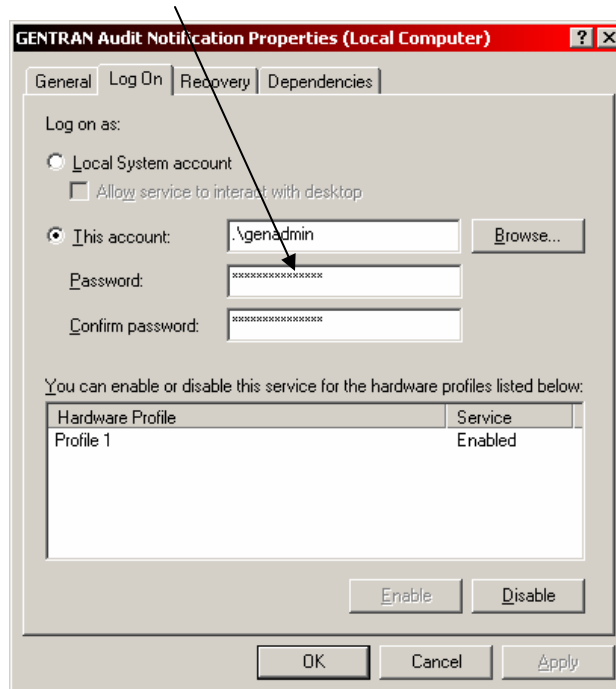
This Windows user id's password will first need to be updated. Once the password for that id has been updated, then the new password for will need to be entered for each of the Gentran Server for Windows services using the steps below.

Windows 2000

- 1) Open the Microsoft Management Console for Services. This is located within Administrative Tools.



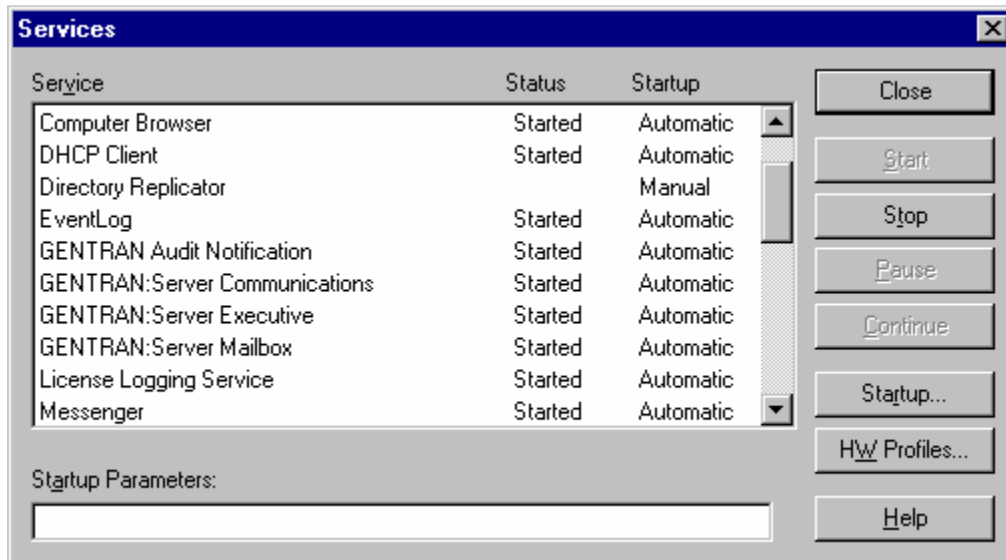
- 1) Double click Gentran Audit Notification.
- 2) Click the 'Log On' tab
- 3) Enter the new password in the 'Password' and 'Confirm password' fields.



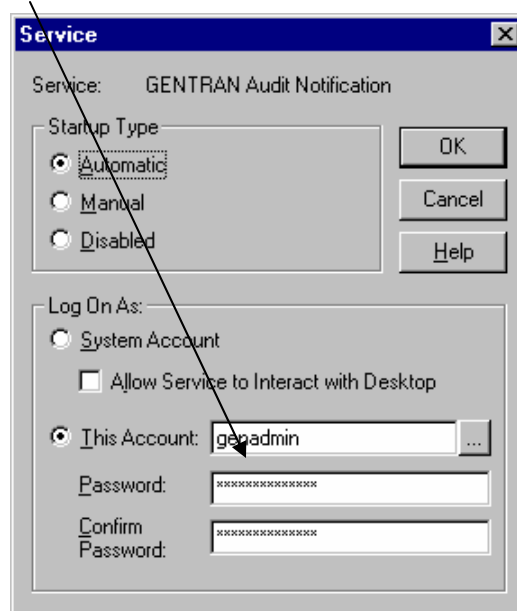
- 4) Repeat the steps above for Gentran Server Mailbox and Gentran Server Executive, and if installed, Gentran Server Communications and RosettaNet Server PIP services.

Windows NT

- 1) Open the Services console from within the Control Panel.



- 2) Double click Gentrans Audit Notification.
- 3) Enter the new password in the 'Password' and 'Confirm password' fields.



- 4) Repeat the steps above for Gentrans Server Mailbox and Gentrans Server Executive, and if installed, Gentrans Server Communications and RosettaNet Server PIP services.

Distributed COM Configuration (DCOM)

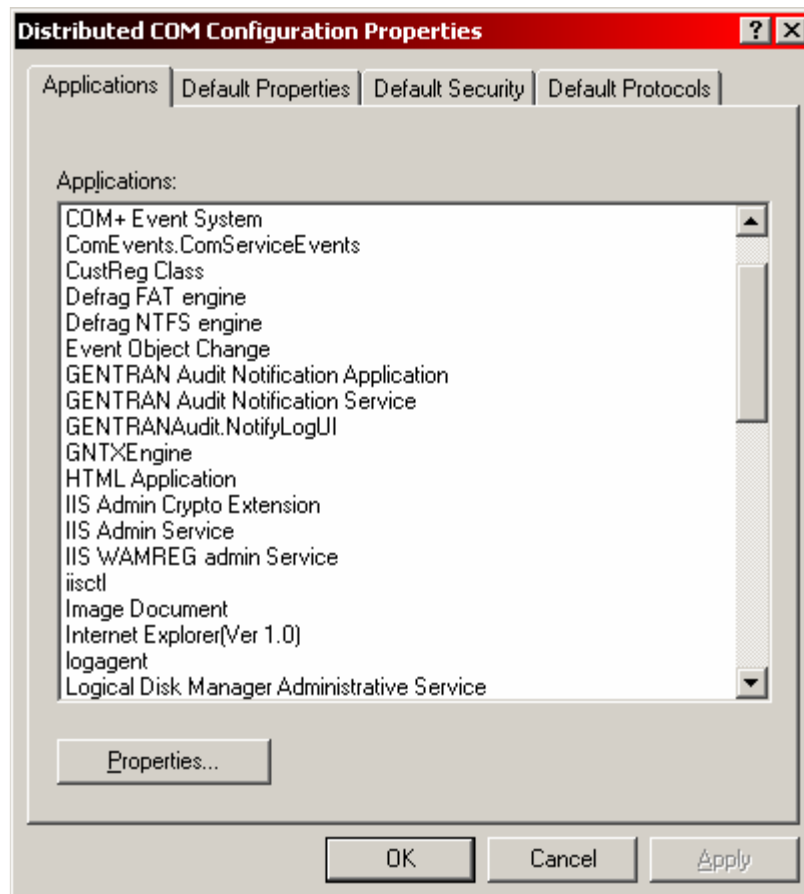
After the password has been updated in Windows for the user id that is used to start the Gentran Server for Windows services, the password will then need to be changed within Distributed COM Configuration.

The user id and password that will be updated within Distributed COM Configuration is the exact same user id and password that is used to start the Gentran services, so the user id and password here has to be the same as the one used before when updating the user id that starts the services (Windows user id).

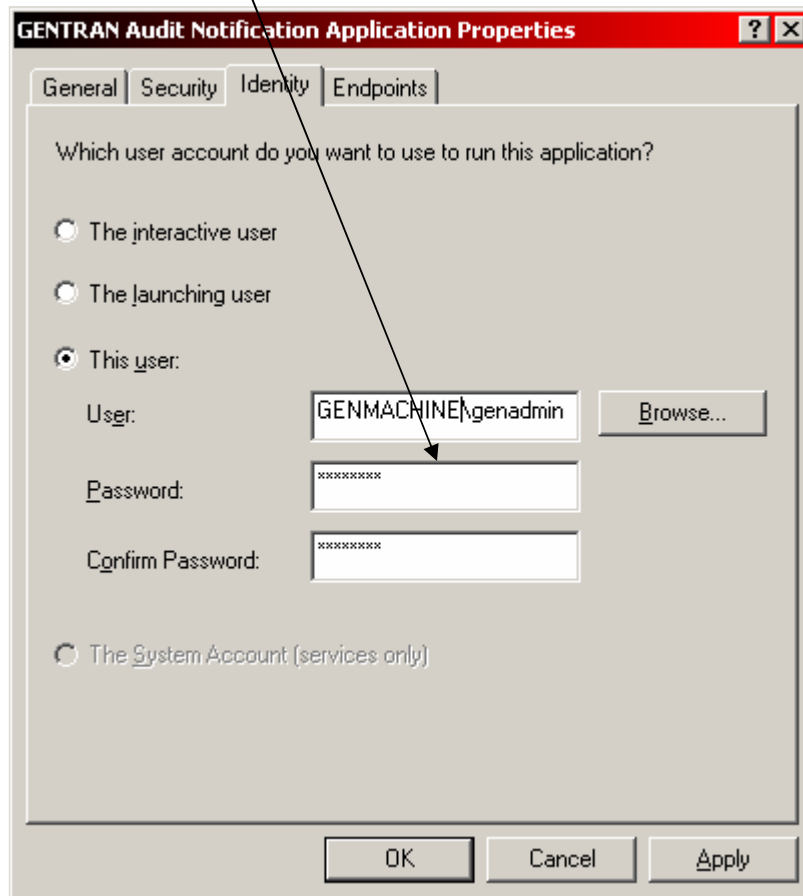
It is suggested that network administrator make the necessary changes in the Distributed COM configurations.

To update the password for the id being used in the Distributed COM configuration, follow the instructions below.

- 1) Click on the Windows 'Start' button.
- 2) Select 'Run'.
- 3) Type DCOMCNFG, and click 'OK' to open the Distributed COM Configuration Properties.



- 4) Highlight Gentrans Audit Notification Application in the list of Applications on the 'Applications' tab and click the 'Properties' button.
- 5) Select the 'Identity' tab, and enter the new password in the 'Password' and 'Confirm Password' fields in the 'This user' area.

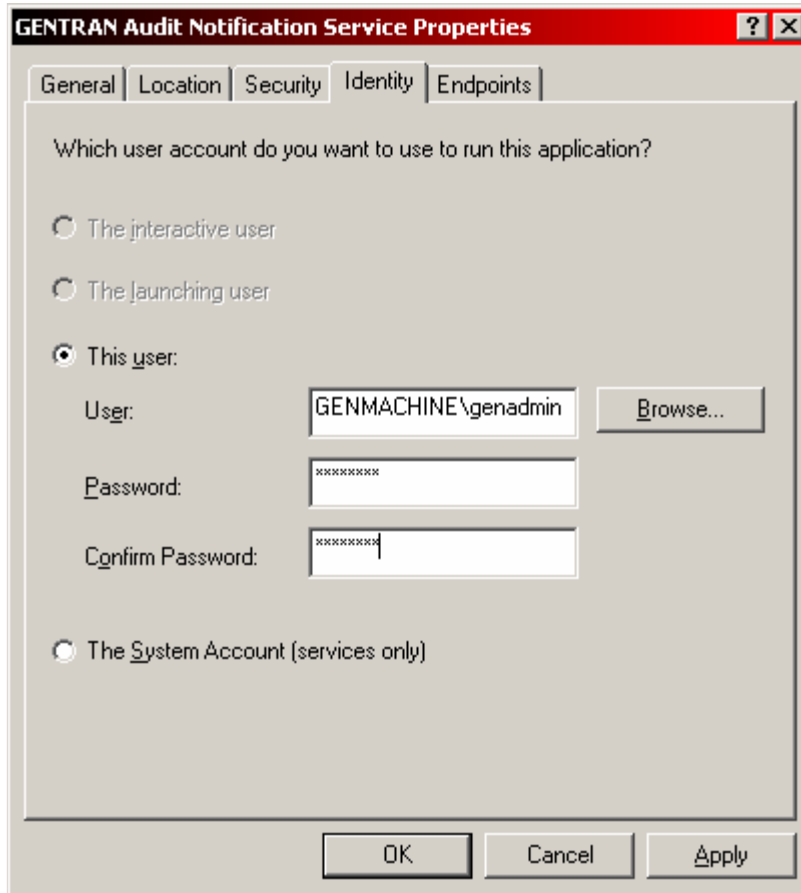


The screenshot shows the 'GENTRAN Audit Notification Application Properties' dialog box with the 'Identity' tab selected. The dialog has four tabs: 'General', 'Security', 'Identity', and 'Endpoints'. The 'Identity' tab contains the following elements:

- Question: "Which user account do you want to use to run this application?"
- Radio buttons for user selection:
 - The interactive user
 - The launching user
 - This user:
 - The System Account (services only)
- Fields for the selected user:
 - User: GENMACHINE\genadmin (with a 'Browse...' button to the right)
 - Password: [masked with asterisks]
 - Confirm Password: [masked with asterisks]
- Buttons at the bottom: OK, Cancel, and Apply.

An arrow points from the top of the dialog to the 'User' field.

- 6) Highlight Gentran Audit Notification Service in the list of Applications on the 'Applications' tab and click the 'Properties' button.
- 7) Select the 'Identity' tab, and enter the new password in the 'Password' and 'Confirm Password' fields in the 'This user' area.
 - a. If the 'This User' radio button is not selected, select 'This User', click the 'Browse' button and select the correct User ID, and enter the password in the 'Password' and Confirm Password' fields.



The screenshot shows the 'GENTRAN Audit Notification Service Properties' dialog box with the 'Identity' tab selected. The dialog has a red title bar with a question mark and close button. Below the title bar are tabs for 'General', 'Location', 'Security', 'Identity', and 'Endpoints'. The main area contains the question 'Which user account do you want to use to run this application?' and four radio button options: 'The interactive user', 'The launching user', 'This user:', and 'The System Account (services only)'. The 'This user:' option is selected. Below it are three input fields: 'User:' containing 'GENMACHINE\genadmin' with a 'Browse...' button to its right, 'Password:' containing '*****', and 'Confirm Password:' containing '*****'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Verification

The password has now been updated in all areas required for Gentran Server for Windows; the machine must be rebooted to test. Verify all services start up correctly as well as testing Gentran's access to other applications, process control events, communications etc.