FASTPATH

Minimizing the use of ‘sa’ in Microsoft Dynamics GP

Jeff Soelberg, CRISC

Synopsis:

Out of the box, Microsoft Dynamics GP creates the 'sa' user with full privileges to create, modify and delete any and all data within the SQL database and the GP application. There is a common misconception that this approach is the best and/only way to manage administrative level security. This document is designed to explain the access rights and risks of the 'sa' user as well as the best practice approach for setting up administrative rights to create a more secure environment.

The Problem:

When installing Microsoft Dynamics GP, the Microsoft SQL Server environment on which the databases are installed must use mixed mode authentication. In this environment, the 'sa' user is required and has full access to the entire SQL Server environment. This user has full privileges including creating and dropping databases, users, and tables.

In addition, the out of the box 'sa' user is assigned to the SQL fixed server role of sysadmin. This assignment makes the 'sa' user the only GP user who is able to create users and assign them to GP companies as well as create new companies and assign users to those new GP companies.

The dependence on the 'sa' account creates significant financial, system and organizational risk. First, 'sa' is a generic account name and not a named account. This makes it difficult to isolate who used the 'sa' account to make critical changes and verify if those changes were authorized. Second, the 'sa' account can view, update and delete data from within Dynamics GP, SQL Server Management Studio and any other tools that provide database connectivity including Microsoft Excel. Finally, 'sa' access enables the user to make sweeping and powerful changes to critical data. This increases the risk of malicious or unintentional database catastrophes.

There is a common conception that the 'sa' account is required to create users, create companies and perform various maintenance processes within Microsoft Dynamics GP. This is false and the remainder of this document is designed as a guide to minimizing the use of, access to and reliance on the 'sa' account.

The Solution:

Before reducing 'sa' privileges from the Dynamics GP environment, it is necessary to grant a Dynamics GP named user the access required to perform provisioning and administrative tasks.

Ideally, to achieve segregation of duties, the GP user provisioning would be divided amongst 3 users: one to create the user and add that user to a company database, one to assign security roles to a user and one to maintain role and task definitions.

Using additional controls such as activity tracking or audit trails, the provisioning may divided between 2 users. The remainder of this document will describe the 2 user scenario using a GP Security Administrator and a GP Access Administrator.

The GP Security Administrator is a named GP user responsible for:

a. Assigning Users to Roles, as well as their Mod-Alt profile

b. Assigning Tasks to Roles and creating or deleting Roles
c. Assigning Windows and Reports to Tasks and creating or deleting Tasks
d. Managing Mod-Alt profile setups
e. This user should NOT have the ability to create GP Users, or assign them to GP Companies
f. Activity of this user should be tracked by Audit Trails, or Activity Tracking.

The GP Access Administrator is a named GP user responsible for:

a. Creating and deleting all Dynamics GP users
b. Assigning users to companies in your Dynamics GP environment
c. Resetting forgotten user passwords
d. This user should NOT have access to assign security rights from within Dynamics GP.

Setup GP Security Administrator

Required Dynamics GP Application Access

The GP Security Administrator is a Dynamics GP user with limited GP access. Create a named user in Dynamics GP with access to all Dynamics companies.

Assign this user access to the following Dynamics GP forms:

a. User Security
b. Security Tasks
c. Security Roles
d. Alternate/Modified Forms and Reports

Ensure that this user does not have access to the following Dynamics GP forms:

a. User Setup
b. User Access

The user may be assigned other access outside of the forms listed above.

Setup GP Access Administrator

Required Dynamics GP Application Access

The GP Access Administrator is a Dynamics GP user with limited GP access. Create a named user in Dynamics GP with access to all Dynamics companies.

Assign this user access to the following Dynamics GP forms:

a. User Setup
b. User Access

Ensure that this user does not have access to the following Dynamics GP forms:

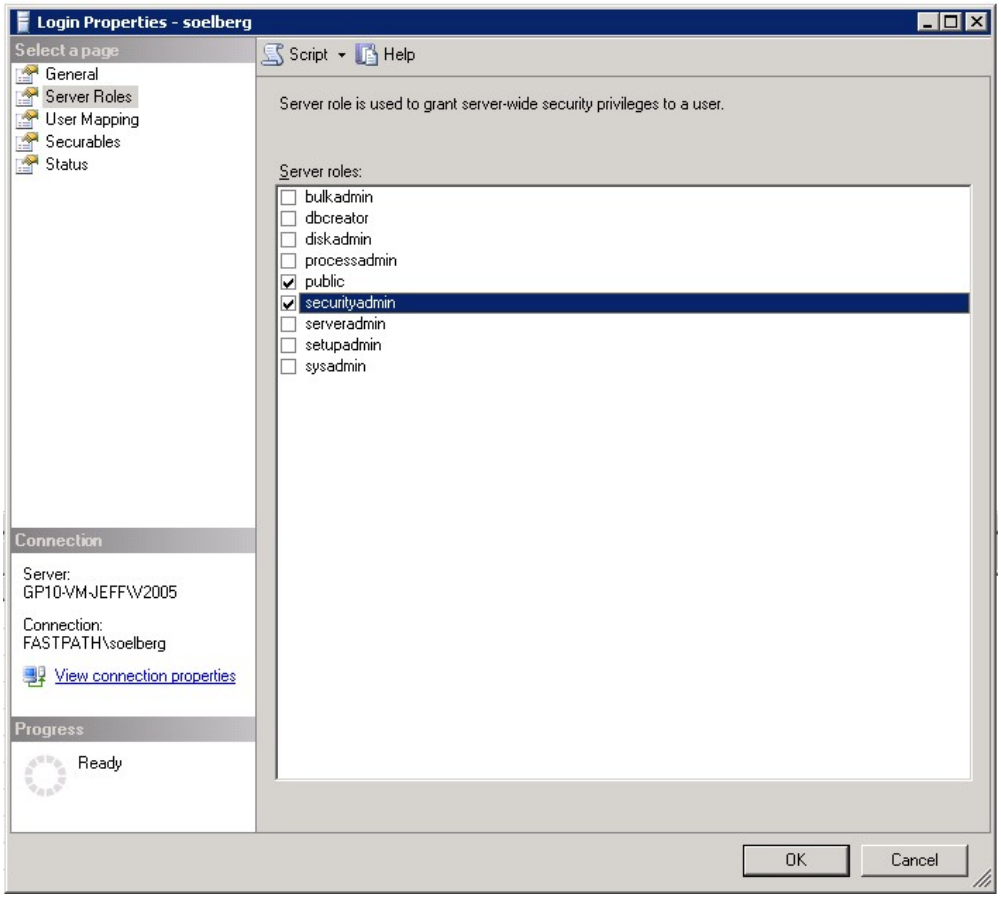
a. User Security
b. Security Tasks
c. Security Roles
d. Alternate/Modified Forms and Reports
e. Any access that would allow maintenance of GP data through the GP client. Examples include: VBA, Modifier, Smartlist Builder

The user may be assigned other access outside of the forms listed above.

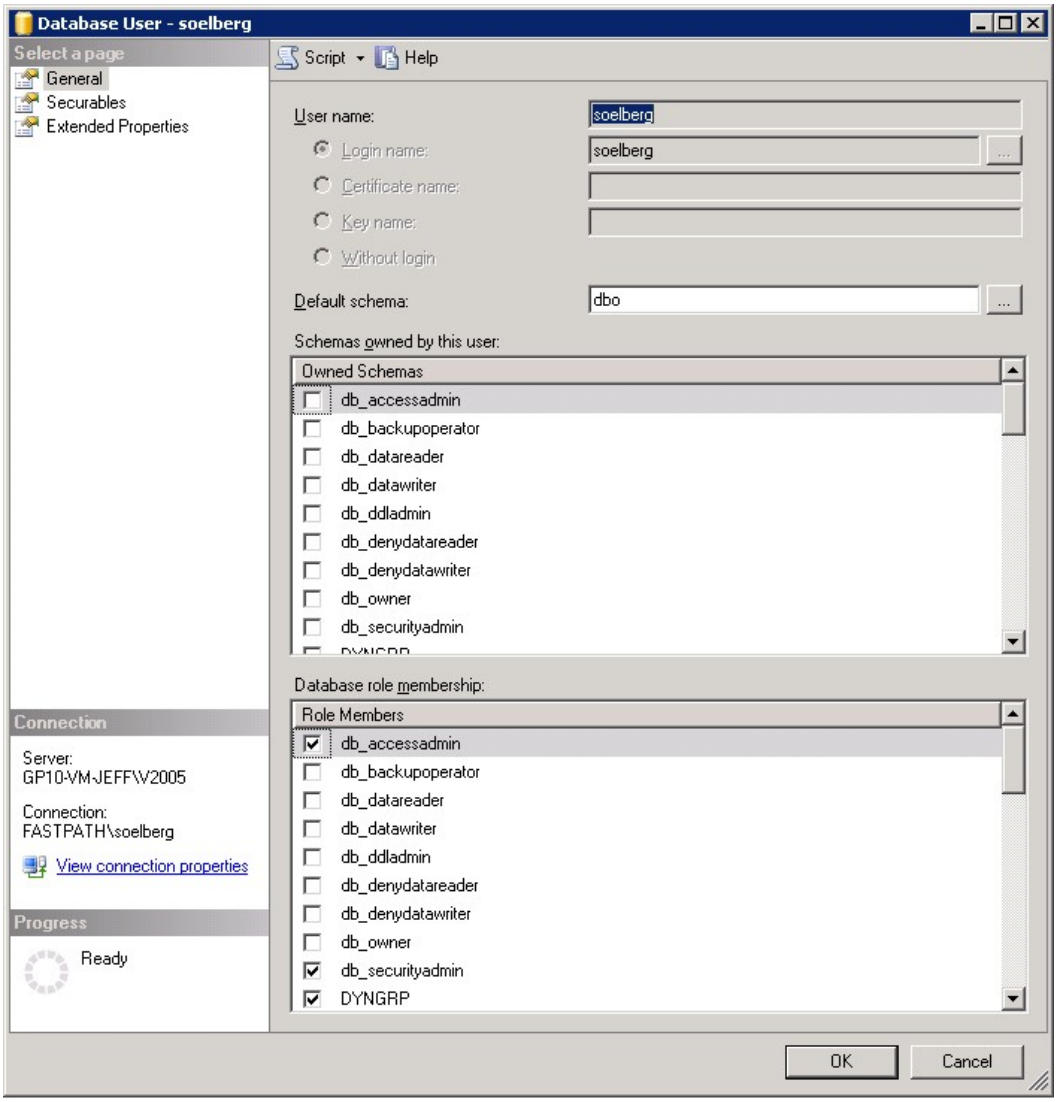
Required Microsoft SQL Server Access

This user will require elevated SQL Server permissions. Because GP encrypts the SQL passwords for all GP application users except 'sa' the GP Access Administrator user will not have access to financial data via applications like SQL Server Management Studio, Microsoft Access, Microsoft Excel, or any other connection via ODBC.

Grant the SQL Login associated to the GP Access Administrator user the securityadmin SQL fixed server role. In addition, the SQL User needs to have db_securityadmin, db_accessadmin, and the DYNGRP roles assigned in the **DYNAMICS** database and **All** GP company database. The DYNGRP role is automatically assigned when the user is created in Dynamics GP.
To assign the user's login to the **securityadmin** role in SQL Server, open **Microsoft SQL Server Management Studio**, maximize the **Security** folder and the **Logins** subfolder. Double-click on the user login to open the **Login Properties** window. Select the **Server Roles** page and mark the **securityadmin** role.



To assign the user's login to the **db_securityadmin** and the **db_accessadmin** role in SQL Server, open **Microsoft SQL Server Management Studio**, maximize the **database, Security** folder, and the **Users** subfolder. Double-click on the user to open the **Database User** window. Mark the **db_securityadmin** and **db_accessadmin** roles.



Since the SQL user you are granting the SQL fixed sever roles is a Dynamics GP user with an encrypted password, this user cannot gain direct access to the SQL environment or the SQL tables. The only way for this user to access the SQL data is via the Dynamics GP application.

Setup 'sa' access to Dynamics GP

By default, the 'sa' user is assigned the Dynamics GP application role 'Poweruser'.

'Poweruser' is a programmatic role meaning that it provides access to all areas of Dynamics GP and is not subject to application security. Users assigned 'Poweruser' will not appear in the standard GP security reports. Because of this risk, it is recommended that no user be assigned the 'Poweruser' role.

A new role titled ‘Administrator’ should be created and all tasks should be assigned to this role as required.

It is not required to assign the ‘sa’ account ‘Poweruser’ role or an ‘Administrator’ role.

The ‘sa’ account is only required in and should be limited to the following places in Dynamics GP:

a. Performing 3rd party upgrades (Not all 3rd parties require ‘sa’)
b. Using Professional Services Tools Library

The following are functions that do not require the ‘sa’ account:

a. Creating an ODBC connection
b. Creating reports using Smartlist Builder
c. Creating new GP companies
d. Upgrading GP, or apply service packs

Any member of the SysAdmin fixed server role can upgrade from a previous release or install Microsoft Dynamics GP. The SysAdmin fixed server role should be granted by the SQL Server administrator to a GP user on an as needed basis, and should be revoked after the task is complete.