SeniorSystems

System Administration
Release Bulletin

December 2008

In this release bulletin, the latest enhancements to the **System Administration** module are described.

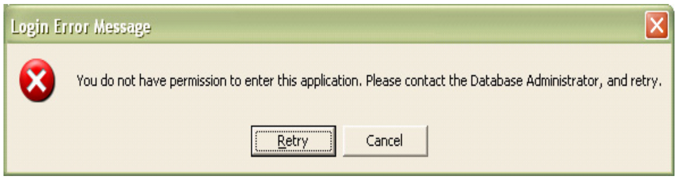
In this Issue...

SINGLE SIGN-ON FOR SENIOR SYSTEMS APPLICATIONS

The **System Administrator** can now allow all users or just some users, single sign-on capability for **Senior Systems** applications. If a user has single sign-on capability, then they can log into an application like **Accounts Receivable** as they normally would, by entering their username and password. Then, if later in the day they need to go into **General Ledger** they can select the shortcut or executable and the application will open without requiring a login.

As long as a **Senior Systems** application is open on their desktop, subsequent applications will not require the user to enter their username and password. If all the applications have been closed, then the next application they select will require them to re-enter their username and password.

Application access rights are in effect with single sign-on. If the user attempts to access an application they don't have assigned rights to, they will be denied entry and receive the following message:

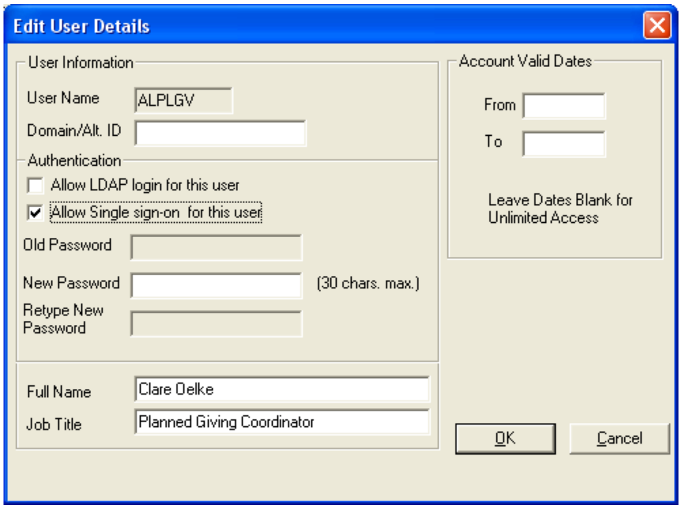


You do not have permission to enter this application. Please contact the Database Administrator, and retry.

FIGURE 1. **Login Error Message**

To activate single sign-on for a user, follow these steps:

1. Log into **System Administration** as **SENIORDB**.
2. From the **File** menu, select **User Maintenance** > **Edit User Profiles**.
3. Select the user you wish to modify click **Edit**.
4. When the **Edit User Details** menu (figure 2) appears, select the **Allow Single sign-on for this user** checkbox, then click **OK**.



User Name: ALPLGV
Domain/Alt. ID:
□ Allow LDAP login for this user
☑ Allow Single sign-on for this user
Old Password:
New Password: (30 chars. max.)
Retype New Password:
Full Name: Clare Oelke
Job Title: Planned Giving Coordinator
From:
To:
Leave Dates Blank for Unlimited Access

FIGURE 2. **Edit User Details**

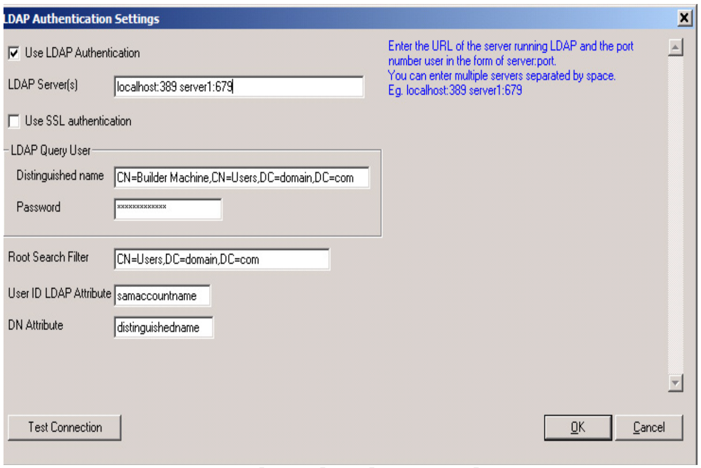
You can then notify the user that single sign-on is now available. Once this is activated, if they leave their desk unattended for a period of time, for security purposes, they should close all **Senior Systems, Inc.** applications, requiring them to log back in upon their return.

SETTING UP LDAP AUTHENTICATION

By setting up LDAP Authentication, users of **Senior Systems, Inc.** applications can now login using only their local domain passwords. Users will have fewer passwords to remember and network administrator can force regular **Senior Systems, Inc.** password changes by forcing a network password change.

To enable LDAP authentication for users, follow these steps:

1. Log into **System Administration** as **SENIORDB**.
2. From the **File** menu, select **Security Options** > **LDAP Authentication** > **LDAP Authentication Settings**. The **LDAP Authentication Settings** menu (figure 3) appears.



☑ Use LDAP Authentication
LDAP Server(s): localhost:389 server1:679
□ Use SSL authentication
Distinguished name: CN=Builder Machine,CN=Users,DC=domain,DC=com
Password: *************
Root Search Filter: CN=Users,DC=domain,DC=com
User ID LDAP Attribute: samaccountname
DN Attribute: distinguishedname

Enter the URL of the server running LDAP and the port number user in the form of server:port.
You can enter multiple servers separated by space.
Eg. localhost:389 server1:679

FIGURE 3. **LDAP Authentication Settings**

3. Select the **Use LDAP Authentication** checkbox.

   You can then select which users will be allowed to use LDAP Authentication and enable your Web Users.

4. In the **LDAP Server(s) field**, enter the URL of the server(s) running LDAP and the port number used in this format: *server.port*

   You can enter multiple servers by separating each string of *server:port* with a space between each entry.

5. If your active directory uses SSL, select the **Use SSL Authentication** checkbox. Otherwise, leave the box unchecked.
6. For the **LDAP Query User**, enter the **Distinguished name** of a user that can connect to the directory.
7. Enter the **Password** used by the LDAP Query User.
8. In the **Root Search Filter**, enter the name of the root node in LDAP for user search. For example,

   CN=users,dc=domain,dc=com

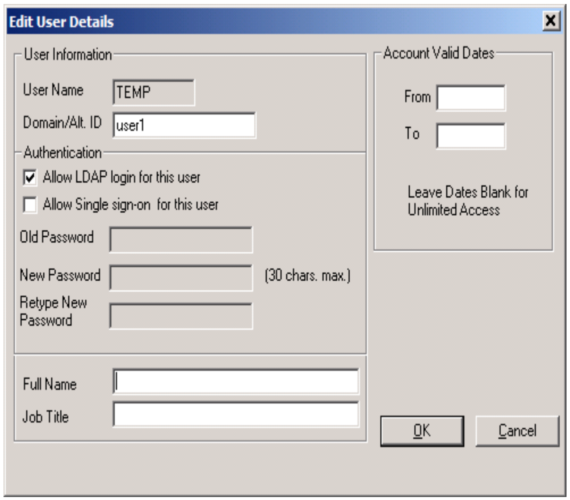
9. In the **User ID LDAP Attribute** field, enter the attribute that the LDAP Authentication module will search for in the Active Directory and return to match the UID in the Directory Server. If you are using Active Directory, the most common value is **sAMAccountName.** Check with your network administrator to determine if there is a different value.

10. Enter the **DN Attribute** that LDAP Authentication will use to query the distinguished name of a user. If you are using Active Directory, the most common value is **distinguishedname**.
11. Click **Test Connection** to try out your settings, then click **OK** when you are done.

Enabling Users for LDAP Authentication

Now that you have created your LDAP settings, you can enable specific users LDAP Authentication for logins.

1. From the **File** menu, select **User Maintenance > Edit User Profiles**.
2. From the **User Maintenance** window, select a user and click **Edit**.
3. In the **Edit User Details** menu (figure 4), in the **Domain/Alt. ID** field, enter the domain username. The username does not contain the @ sign or domain name.



Edit User Details

User Information

User Name: TEMP

Domain/Alt. ID: user1

Authentication

☑ Allow LDAP login for this user

☐ Allow Single sign-on for this user

Old Password:

New Password: (30 chars. max.)

Retype New Password:

Full Name:

Job Title:

Account Valid Dates

From:

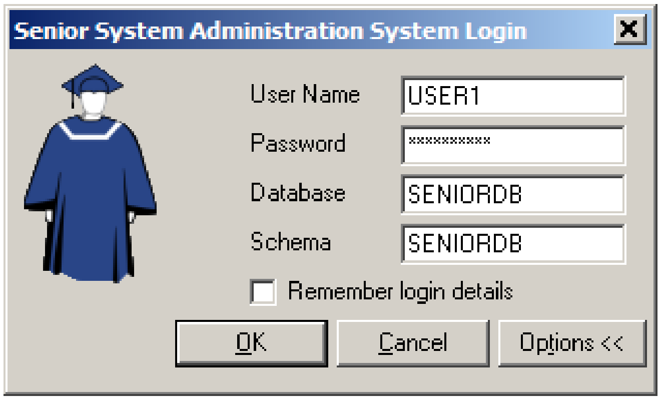
To:

Leave Dates Blank for Unlimited Access

FIGURE 4. **Edit User Details**

4. Select the **Allow LDAP login for this user** checkbox, then click **OK**.

   The user can now use their domain username and password in the login screen (figure 5).



Senior System Administration System Login

User Name: USER1

Password: ***********

Database: SENIORDB

Schema: SENIORDB

☐ Remember login details

FIGURE 5. **System Login**

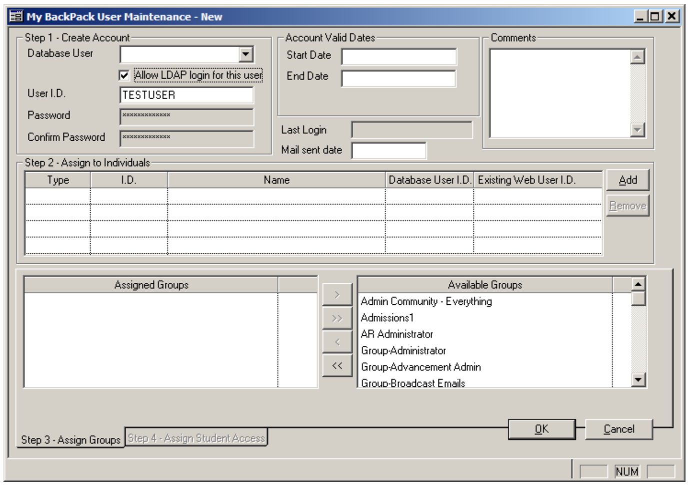
Setting up Web Users for LDAP Authentication

If you use any of the **Senior Systems, Inc. My Backpack** modules, then many of your web users can also benefit from LDAP Authentication.

For teachers that do their grade entry through the **My Backpack Faculty Community**, many of these teachers do not have regular database usernames, therefore, their Web User account settings need to be altered to allow the LDAP Authentication. If your teachers do have standard database usernames, by mapping the database username to the Web User account and enabling LDAP Authentication for the standard database username, the Web User account can access **My Backpack** using the domain username and password.

If students have access to the **My Backpack Student Community** and have usernames on your domain, you can also allow them access to LDAP Authentication.

1. From the **My BackPack** menu, select **My BackPack User Maintenance**.
2. Select a user and click **Edit**.
3. In the **My BackPack User Maintenance - New** (figure 6) window, select the **Allow LDAP login for this user** checkbox, then click **OK**.



☑ Allow LDAP login for this user

User I.D. TESTUSER

Password ************

Confirm Password ************

Available Groups:

- Admin Community - Everything
- Admissions1
- AR Administrator
- Group-Administrator
- Group-Advancement Admin
- Group-Broadcast Emails

FIGURE 6. **My BackPack User Maintenance**

The user will now be able to login to **My BackPack** communities with his/her domain username and password.