Bioreactor Single Sign-On Configuration Guide

PBS Vertical Wheel® Bioreactor Control Software

1. Purpose

This document was created to provide the necessary information for configuration of Single Sign-On for PBS Bioreactors and integration with a User's Active Directory database.

2. Scope

This document will cover permission groups that bioreactors will require in order to appropriately assign bioreactor functions to Active Directory users, configuration of the bioreactor, and basic testing. This document only applies to bioreactors running PBS Control software v4.1 and above.

3. Target Audience

This document is to be used by experienced IT professionals only. If you do not have experience with Active Directory, please contact your IT staff and have them review this document. PBS Biotech is not responsible for configuration of the User's network or ensuring compliance with the User's SOPs, IT Policies, or applicable standards such as 21 CFR Part 11.

4. Overview of Single Sign On

PBS Bioreactors provide Single Sign-On by integrating directory with the User's Active Directory (AD) database via the Lightweight Directory Access Protocol (LDAP). Permissions are assigned by creating AD Groups corresponding to each bioreactor permission ("Permission Groups") and assigning AD User accounts to those groups.

When an AD User uses their domain credentials to log into the PBS Bioreactor, the User's AD Group memberships are queried to build the list of permissions assigned to the user during that login session. Permissions may be granted by assigning users directly to Permission Groups or through the group hierarchy by "member-of" relationships:

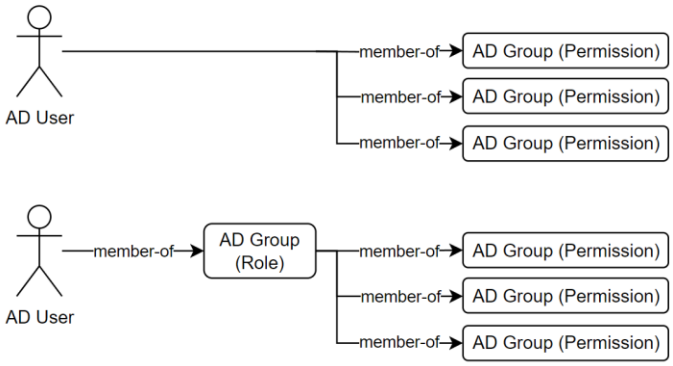

Figure 1: Example of direct (top) vs. indirect (bottom) Permission Group assignment.

5. Domain Configuration

5.1. Active Directory Configuration

The following AD Permission groups must be created and assigned to users to grant bioreactor permissions via Single Sign-On. Permission group names are case-insensitive but must otherwise exactly match:

Bioreactor Permission	AD Permission Group Name
Controls	PBS_Controls
Acknowledge Alarms	PBS_Acknowledge_Alarms
Start Sequence	PBS_Start_Sequence
End Sequence	PBS_End_Sequence
Main Light	PBS_Main_Light
Activate Alarm Settings	PBS_Activate_Alarm_Settings
Activate Logger Settings	PBS_Activate_Logger_Settings
Activate System Variables	PBS_Activate_System_Variables
Batch Events	PBS_Batch_Events
Reports	PBS_Reports
Process Calibration	PBS_Process_Calibration
Sequence Editor	PBS_Sequence_Editor
Email Settings	PBS_Email_Settings
Alarm Settings Editor	PBS_Alarm_Settings_Editor
System Variables Editor	PBS_System_Variables_Editor
Logger Settings Editor	PBS_Logger_Settings_Editor
Equipment Calibration	PBS_Equipment_Calibration
Account Management	PBS_Account_Management
Backup Configuration	PBS_Backup_Configuration
System Management	PBS_System_Management
Map Drive	PBS_Map_Drive

5.2. Bioreactor Configuration

Bioreactors are delivered with SSO disabled by default. Perform the following steps to enable SSO:

1. Connect the bioreactor to a network able to contact the configured Domain Controller.
2. Log into the bioreactor UI as a local admin.
3. Configure SSO Settings from Side Menu -> Administration -> Single Sign-On:
    a. Enable SSO by checking the box.
    b. Configure the default domain. Domain can be a domain name or IP address.
    c. Click the “Test Domain” button to confirm that the domain controller is accessible.
    d. (optional) Configure the credential binding method. We recommend leaving this at the default of Negotiate.
    e. (optional) Configure a default inactivity timeout. The system accepts any value from 2 – 60 minutes.
4. Save and log out when complete.

5.3. Testing Single Sign-On

After configuring the Domain Controller and bioreactor, SSO can be tested by logging into the bioreactor and confirming the list of permissions assigned to the user:

1. Click the UI to open the login screen and confirm that the Domain option is visible.
2. Enter credentials for a valid user with permissions assigned in the domain controller.
    a. **Note:** The username field should contain just the account's username with no prefix or suffix. For example: "johnsmith" instead of "test\johnsmith" or "johnsmith@test.com"
3. Click login and confirm login is successful. Login may fail for the following reasons:
    a. Invalid username or password.
    b. The account is locked or disabled (note: will be reported as invalid credentials).
    c. No PBS permissions are assigned to the AD User Account.
    d. Error contacting domain controller. This can occur due to an issue with network connectivity, domain name, or server configuration.

6. Additional Considerations

6.1. Domain Admins

The SSO feature allows a domain account to be assigned the "Account Management" permission, allowing it to configure local bioreactor users and groups. To prevent the possibility of using domain and local admins to mutually lock all admins from the system, special behaviors were implemented for configuring Administration settings:

- The last local admin account cannot be disabled, deleted, or have its group reassigned.
- The Account Management permission cannot be removed from a group if it results in removing admin access for the last local admin(s).
- SSO cannot be disabled by a domain admin.
- If SSO is not enabled and no local admins exist when the system starts, then SSO will be enabled automatically. **Note**: that this is only possible if the files are deliberately modified by users outside of the application's control.

6.2. Local Fallback Accounts

The SSO feature requires a connection to the Domain Controller to be established for each user login. It does not perform any local caching of user credentials or permissions. If the Domain Controller is not accessible, SSO login attempts will fail.

PBS Biotech recommends at least one generic, local fallback account to be available to allow system access in the event of a network outage (e.g., "Operator"). Note that Users are responsible for implementing and using such accounts in compliance with their own SOPs, Policies, and applicable standards.

6.3. Network Encryption

Encryption is handled automatically by the underlying connection using Negotiate authentication. In a modern Active Directory environment, network traffic will be encrypted using Kerberos.

The LDAP Binding Options setting allows selection of the method used for credential validation. Use of the default Negotiate is preferred for compatibility. Simple Bind requires the server's SSL certificate to be installed on the bioreactor if the SSL option is selected or the server requires secure simple binding.

If Simple Bind fails due to secure binding requirements or SSL certificate is not installed, the UI error message will indicate "Invalid username or password". If Simple Bind (SSL) fails due to SSL certificate not being installed, the UI error message will indicate "Error contacting Domain Controller or querying Authorization Groups".

7. Example Implementation

This section contains an example implementation based on PBS Biotech's internal test environment. It is provided **for reference only** as an example of how an environment might be configured.

7.1. Role-Based Group Assignments

The table below shows permissions assigned to each of four AD Groups used to define roles for users of the PBS Bioreactor system. For each group defining a user role was assigned as "member-of" the corresponding list of Permission Groups.

Lab_Advanced_Users	Lab_Account_Manager	Lab_Regular_Users	Lab_Limited_Users
PBS_Controls	PBS_Account_Management	PBS_Controls	PBS_Main_Light
PBS_Acknowledge_Alarms		PBS_Acknowledge_Alarms	PBS_Reports
PBS_Start_Sequence		PBS_Start_Sequence	
PBS_End_Sequence		PBS_End_Sequence	
PBS_Main_Light		PBS_Main_Light	
PBS_Activate_Alarm_Settings		PBS_Activate_Alarm_Settings	
PBS_Activate_Logger_Settings		PBS_Activate_Logger_Settings	
PBS_Activate_System_Variables		PBS_Activate_System_Variables	
PBS_Batch_Events		PBS_Batch_Events	
PBS_Reports		PBS_Reports	
PBS_Process_Calibration		PBS_Sequence_Editor	
PBS_Sequence_Editor		PBS_Email_Settings	
PBS_Email_Settings		PBS_Alarm_Settings_Editor	
PBS_Alarm_Settings_Editor		PBS_System_Variables_Editor	
PBS_System_Variables_Editor		PBS_Logger_Settings_Editor	
PBS_Logger_Settings_Editor			
PBS_Equipment_Calibration			
PBS_Backup_Configuration			
PBS_System_Management			
PBS_Map_Drive			

7.2. Example Security Group Screenshot

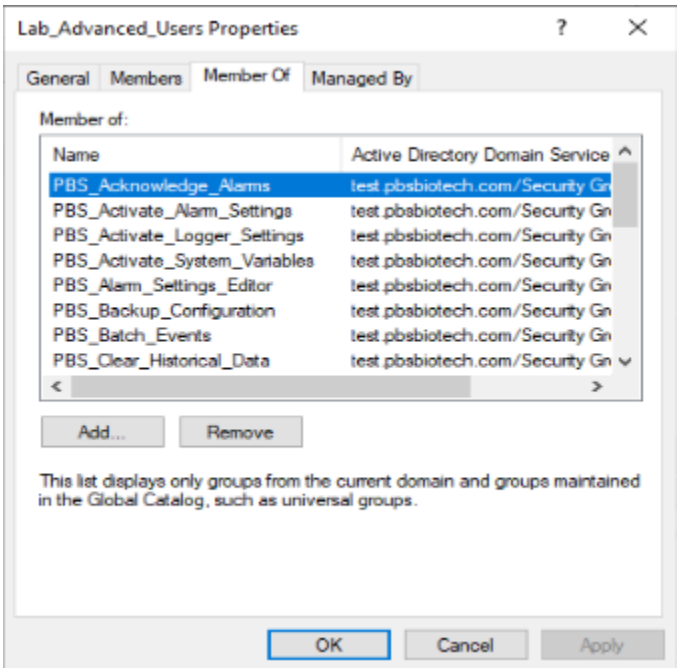

Figure 2: Properties dialog of an AD Group defining the Lab_Advanced_Users role. The "Member Of" tab shows the list of Permission Groups associated with the Security Group.

7.3. Example Permission Group Screenshot

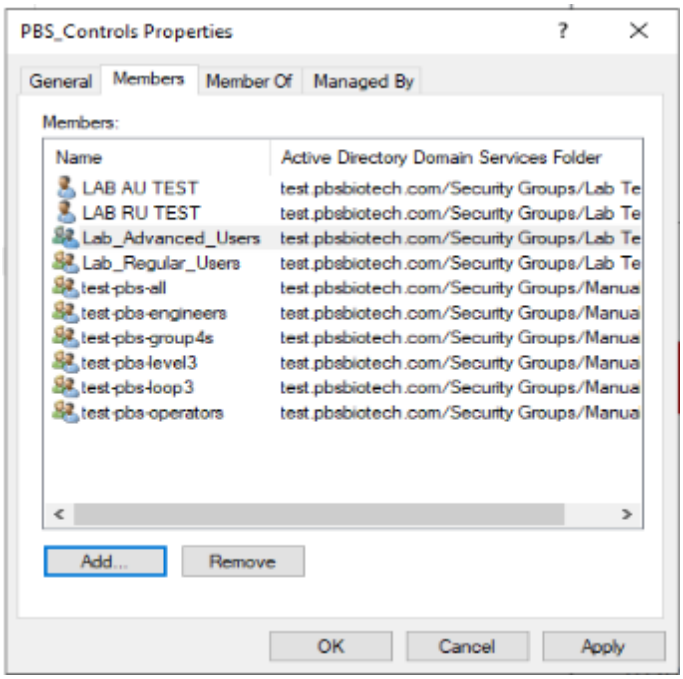

Figure 3: Properties dialog of a Permission Group. The "Members" tab shows all Security Groups and Users that are directly assigned that permission.