

QCommission Single Sign on – Integration with Windows ADS

Overview

Single Sign is a method of access control that enables a user to authenticate once and gain access to the resources of multiple software applications.

Users have only one identity (User Ids and Passwords) to maintain. When the users are authenticated at the OS level (example windows) they need not be authenticated again to use QCommission.

Objective

1. Maintain a single source of authentication information for all users in an organization and that single source can be an existing directory of user names and passwords, such as Active Directory or LDAP, for QCommission users
2. Use an existing directory of user names and passwords, such as Active Directory or LDAP, for QCommission users
3. Allow seamless sign-on to Qcommission applications, eliminating the need for explicit user log on actions.
4. One userid and password to remember between the applications. i.e QCommission Client and QCommission Webportal.

Benefits

Business owners will have the peace of mind that all entry points to applications and data are kept at one single location within a secure AD Directory of the windows with the company's user policy, password-policy in mind. This helps user policies should be dictated by the business owners not by the software vendors.

The Single Sign On feature enables users to log in to the QCommission using their user-account credentials from the Active Directory service provider, based on their Active Directory group membership.

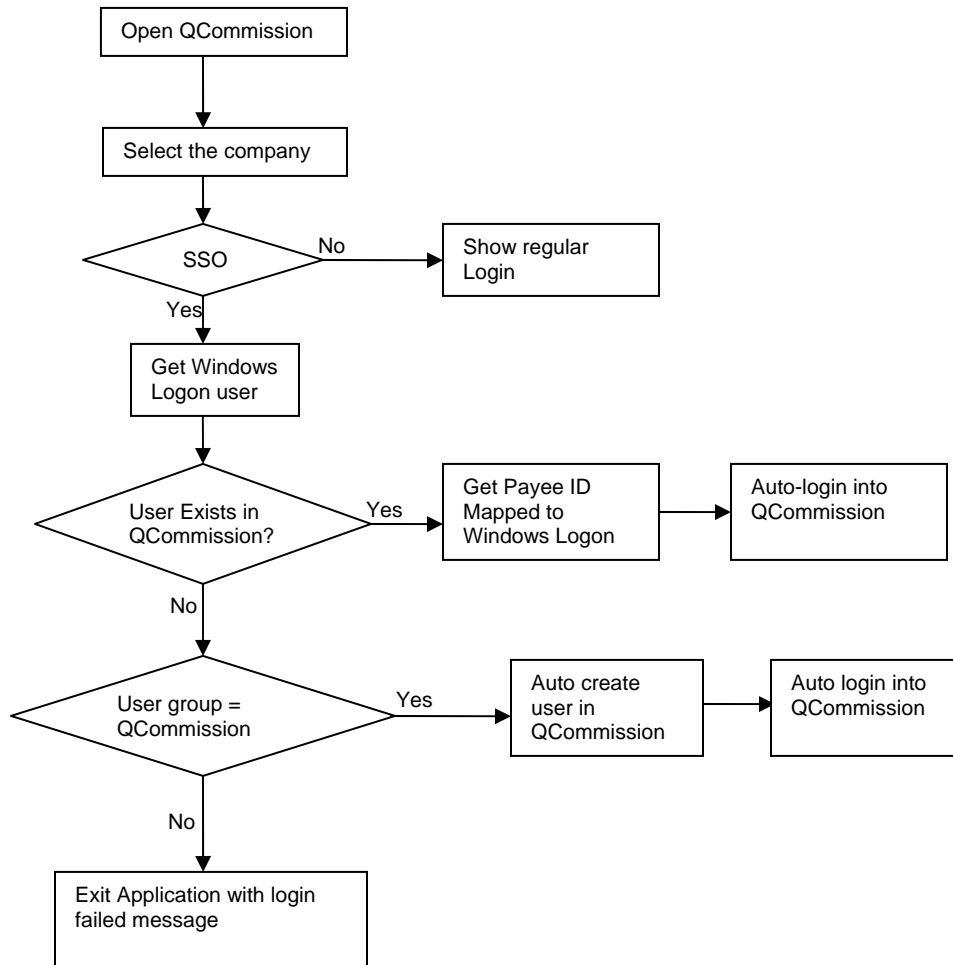
How it works

When QCommission is launched, it should check to see if SSO is active for the company at the database level. (Check the option if SSO is enabled. If disabled is should follow the normal process)

Follow these steps when SSO is enabled.

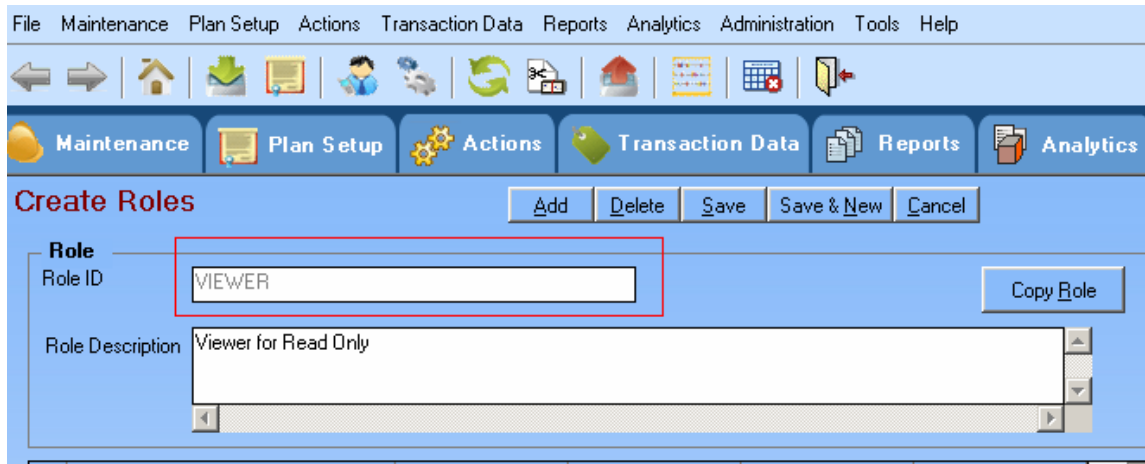
1. Launch QCommission and select the company to login
2. Inquire the system for the current logged on user's information from Active directory services.
3. Check if the logged in user record matches with the QCommission user record.
4. If the user record exists, then the user login dialog is skipped. The user gets into the application. The identity of the user is obtained by querying the user table to get the payee id associated with this userid. In case of web portal this step will help to show his, own commission statement.
5. If the user record does not exist, the domain group associated to this user is queried from the Active directory services. If his domain group matches with one of the role that exists in QCommission the user is auto created in Qcommission.

Process Flow

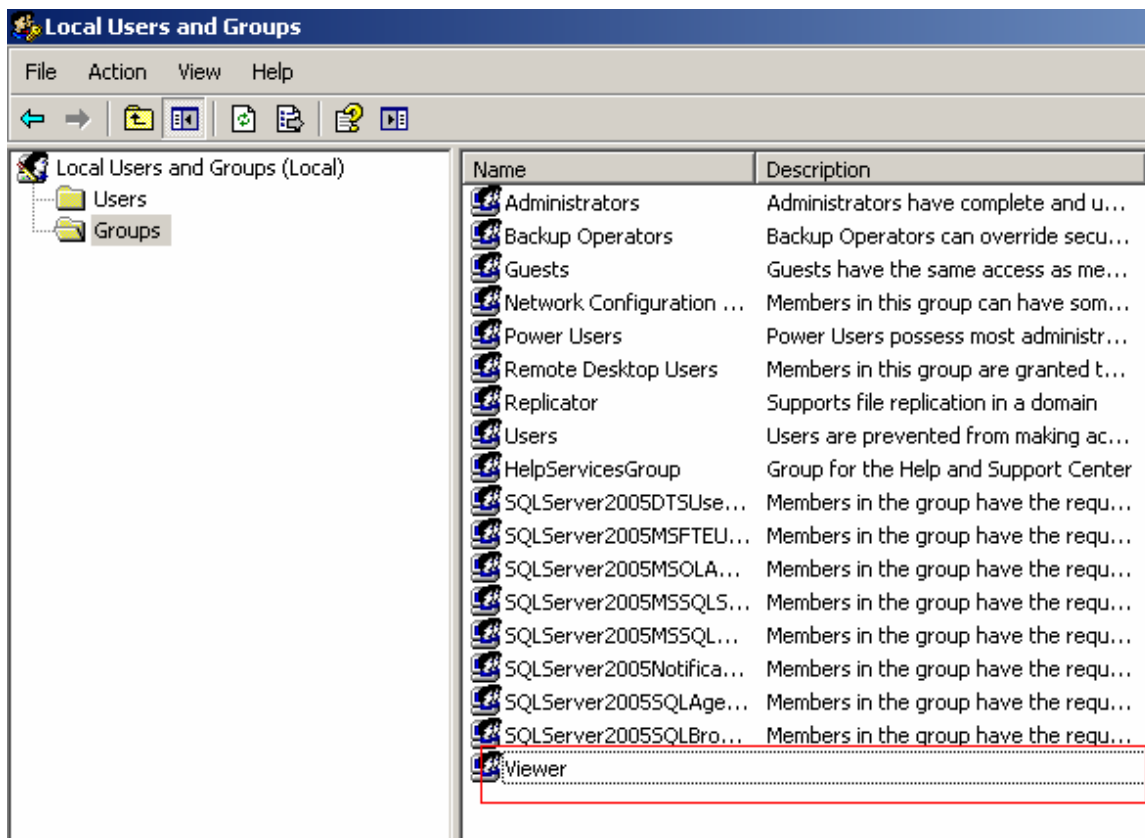


Implementation Requirements

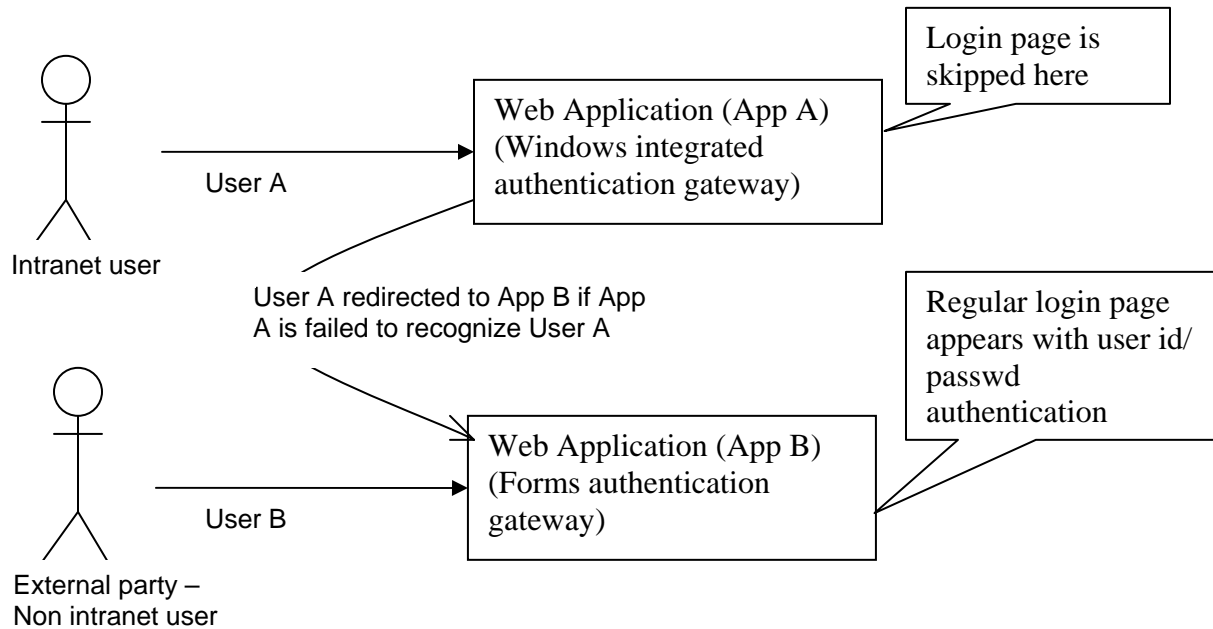
1. Create a group in the domain server with group name matching with the role in QCommission.



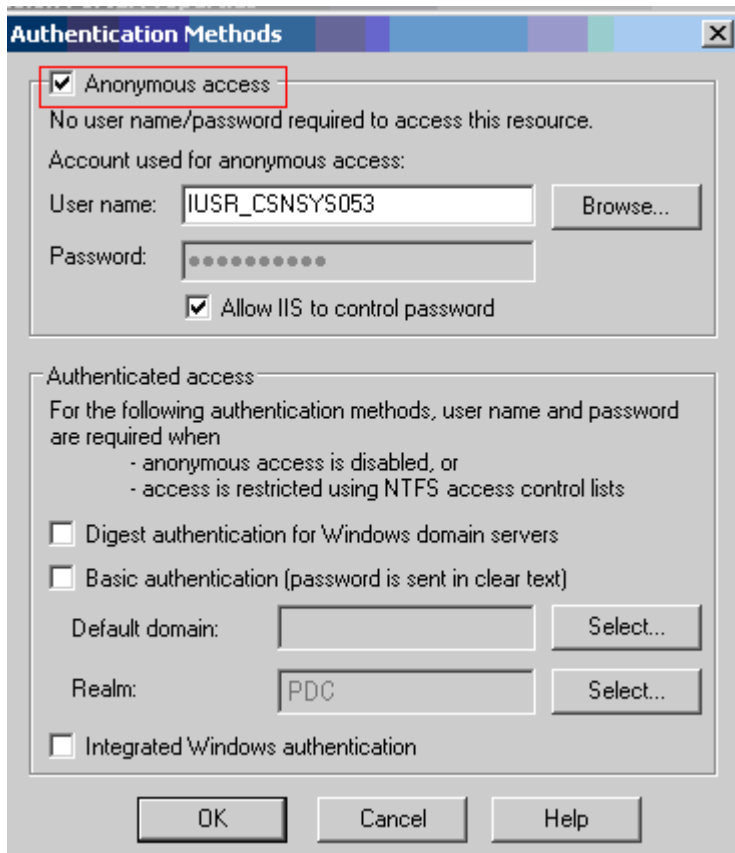
Matching Domain group (Viewer) in ADS



Qcommission Portal – Single sign on implementation



IIS Directory settings for App A



IIS Directory settings for App B

Authentication Methods

Anonymous access
No user name/password required to access this resource.
Account used for anonymous access:
User name: IUSR_CSNSYS053 Browse...
Password:
 Allow IIS to control password

Authenticated access
For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

Digest authentication for Windows domain servers
 Basic authentication (password is sent in clear text)

Default domain: Select...
Realm: PDC Select...

Integrated Windows authentication

OK Cancel Help

User id mapped to Payee ID

Add User Add Delete Save Save & New Cancel K < > |

User ID: Brady
Password: *****
Confirm Password: *****
Change Password
Hint Question: [dropdown]

Payee Id: Jenifer
Expiry Date: [dropdown]
Status: [dropdown]
Role ID: [dropdown]

Brady	Brady
Jenifer	Jenifer
Robbie Allen	Robbie Allen
Robert	Robert
Sandy	Sandy