Setting ServicePrincipalName (SPN) for NTLM based SSO

One requirement for the NTLM Authorization type for Single Sign-On (SSO) is that the GTX service is installed on a Windows based computer that is a member of a Windows Active Directory Domain.

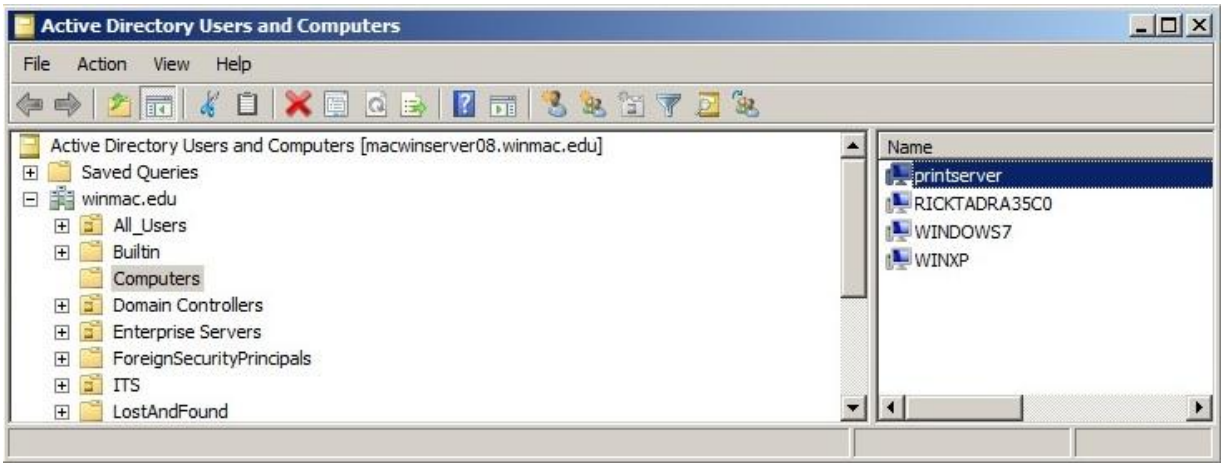
By default the GTX service runs as the Local System account. The registration steps for this are detailed below for this configuration. In some cases, the GTX service may be configured to run using a domain service account. For this case, the domain service account will need to be registered instead of the computer account. The process to register a service user account is identical except the domain user account is used instead of the computer account.

Important: once SSO is enabled any current GoPrint admin accounts will not be able to login to Control Center unless they are actual Active Directory user accounts and have been added to the proper Admin Class. Refer to the troubleshooting section for more information.

Steps for registering SPN on – GTX service running on a local system account

To verify that the GTX server computer account is trusted for delegation

1. Open Active Directory Users and Computers
2. Find the computer account for the GTX server
3. Right-click the computer account, and then click Properties

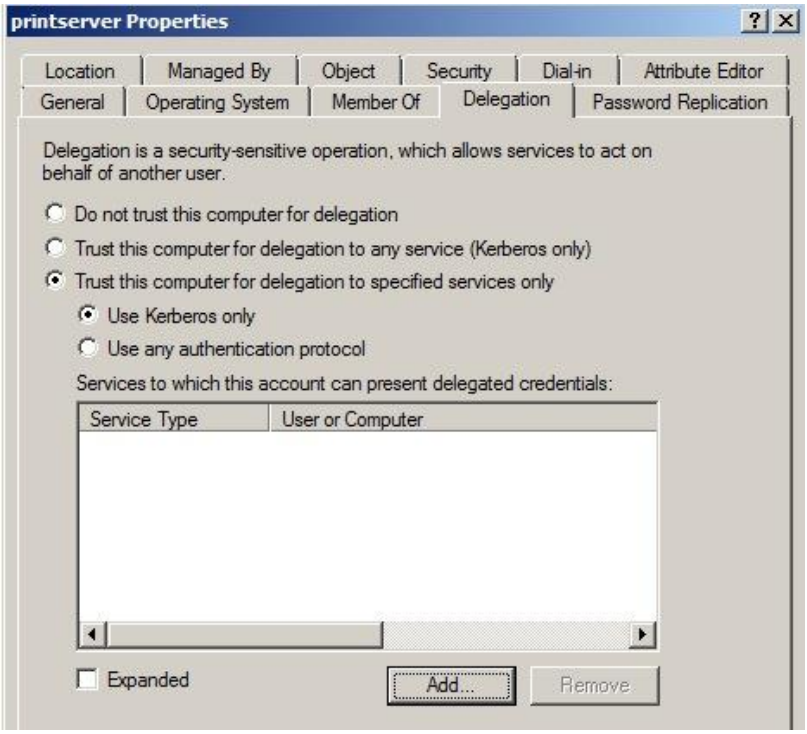


On the **Delegation** tab, if **Do not trust this computer for delegation** then select:

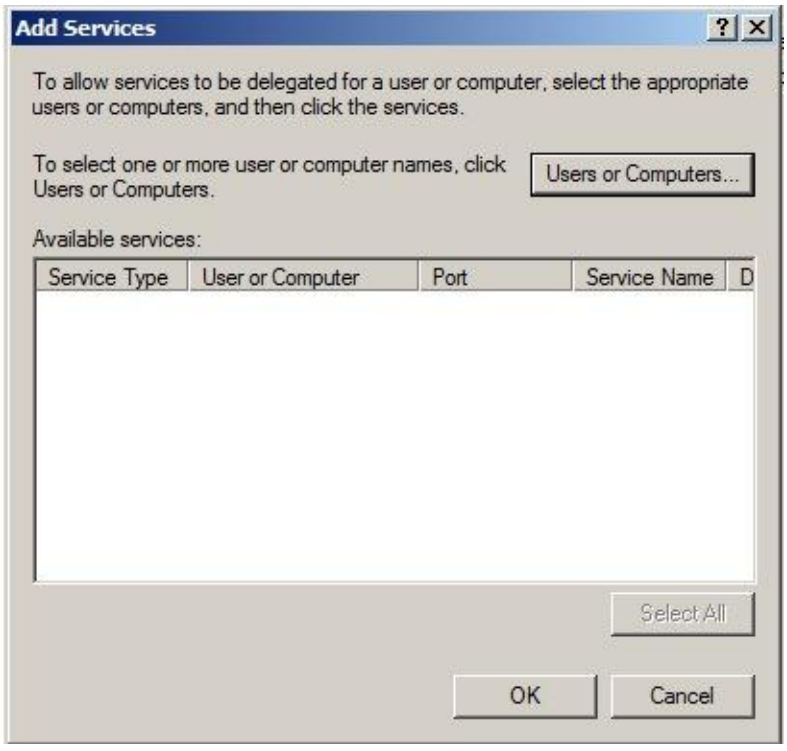
4. **Trust this computer for delegation to specified services only**

   A. Use Kerberos only

   B. Click the **Add** button to set the **http** service type to trusted:



5. In the Add Services dialog click on the **Users or Computers** button

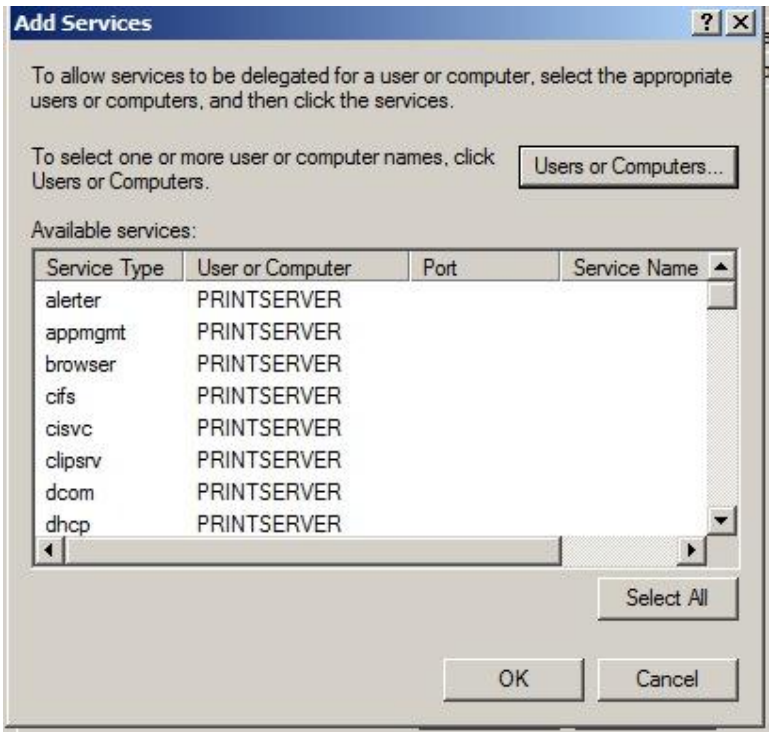


6. Enter the GTX server computer account in the domain accounts prompt

Once the computer account is added the list of service types will appear:

7. Select http and hit ok

8. Click Apply on the account properties dialog



Register the Service Principal Name on the GTX server

Using the setspn.exe command line utility, register the fully qualified domain name of the GTX server URL to the GTX server's computer account:

1. On the GTX server, open the command prompt and add a http service by typing SPN for each GTX service URL

   setspn –A http/<GTX_URL> <COMPUTER_ACCOUNT_NAME>

   For example, if the base URL for the GTX is http://printserver.winmac.edu:7768 and the computername is printserver then the command is:

   setspn –A http//printserver.winmac.edu:7768 printserver

```
C:\Users\Administrator>setspn -A http://printserver.winmac.edu:7768 PRINTSERVER
Registering ServicePrincipalNames for CN=printserver,CN=Computers,DC=winmac,DC=e
du
        http://printserver.winmac.edu:7768
Updated object
```

Repeat the listing command on step 1 to confirm the SPN is registered:

```
C:\Users\Administrator>setspn -A https://printserver.winmac.edu:7773 PRINTSERVER
Registering ServicePrincipalNames for CN=printserver,CN=Computers,DC=winmac,DC=edu
        https://printserver.winmac.edu:7773
Updated object
```

```
C:\Users\Administrator>setspn -A https://printserver.winmac.edu:7770 PRINTSERVER
Registering ServicePrincipalNames for CN=printserver,CN=Computers,DC=winmac,DC=edu
        https://printserver.winmac.edu:7770
Updated object
```

List the currently registered ServicePrincipalNames (SPN) for the GTX server:

setspn –L <COMPUTER_ACCOUNT_NAME>

```
C:\Users\Administrator>setspn -l PRINTSERVER
Registered ServicePrincipalNames for CN=printserver,CN=Computers,DC=winmac,DC=edu:
        https://printserver.winmac.edu:7773
        https://printserver.winmac.edu:7770
        http://printserver.winmac.edu:7768
        WSMAN/printserver
        WSMAN/printserver.winmac.edu
        RestrictedKrbHost/PRINTSERVER
        HOST/PRINTSERVER
        RestrictedKrbHost/PRINTSERVER.winmac.edu
        HOST/PRINTSERVER.winmac.edu
```

Enable SS0 in Control Center

1. Navigate to System – System Policy

2. Click the Security tab

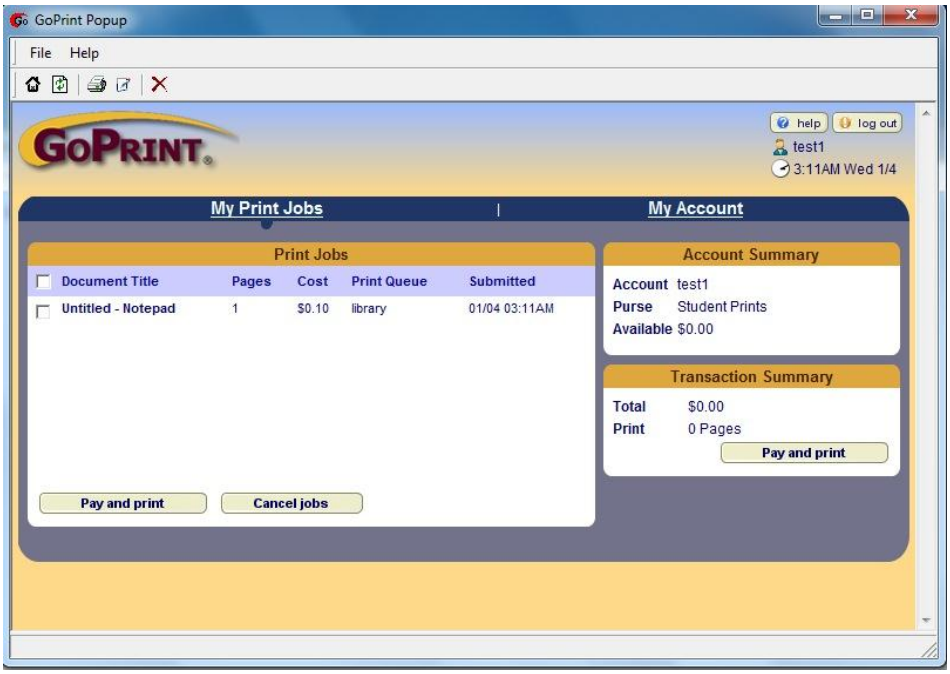
3. Scroll down to Single Sign-On (SSO) section and from the drop down menu select NTLM Authorization.

Your configuration is now complete

Test using the Web Client

1. Log in to a workstation with a domain user account
2. Send and print job

   At this point, the user bypasses the Web Client login screen and is automatically logged in displaying the My Print Jobs main page screen.



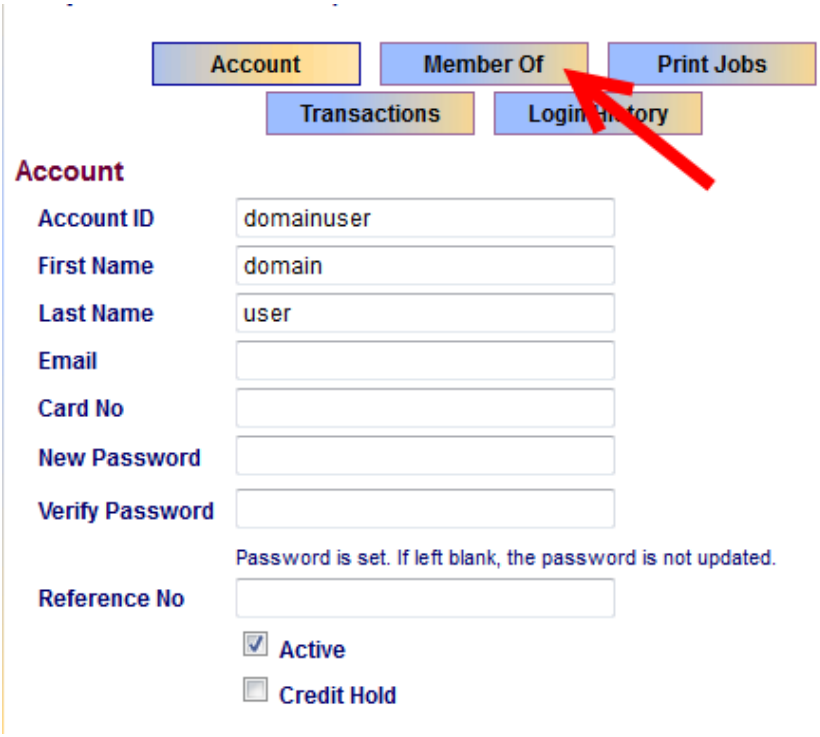
Control Center Login

Once SSO is enabled all GoPrint admin accounts are authenticated against SSO and must match an Active Directory account. If the account, was manually created within GoPrint the account will no longer be able to login. To resolve you must disable SSO and log in to Control Center and add the domain user to the proper Admin Class.

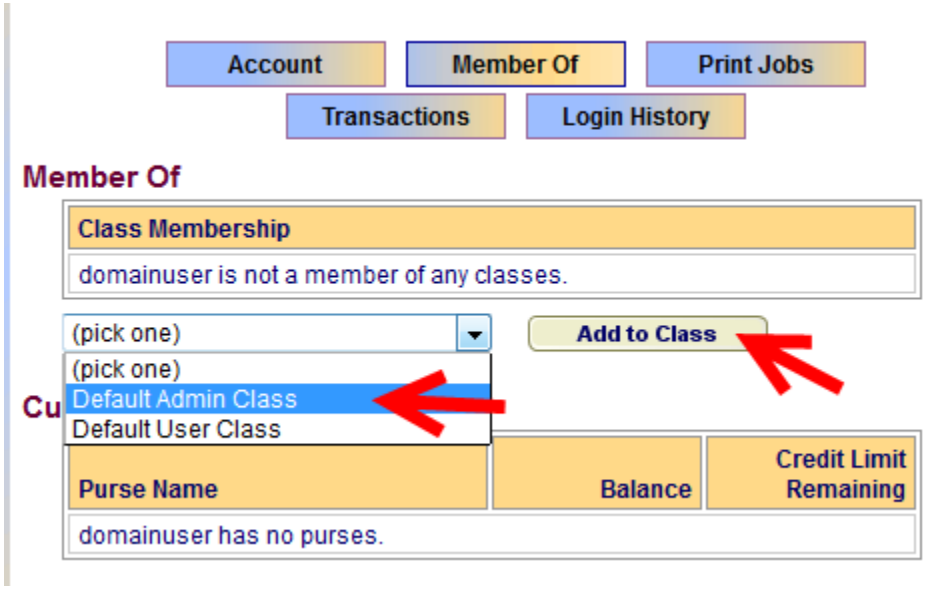
Accounts – Manage Users

Search for the user and once found, click on their username in the search results

Select the Member Of tab



From the Class Membership drop down menu - Select the appropriate Admin Class then press Add to Class



Note: You may create custom Admin Classes and apply a specific level of User Rights. To do so, navigate to Accounts – Class Definitions.

For additional information, refer to the Administrator Accounts documentation at http://www.goprintsupport.com/support.html

The results display the user as a member of the Default Admin Class: