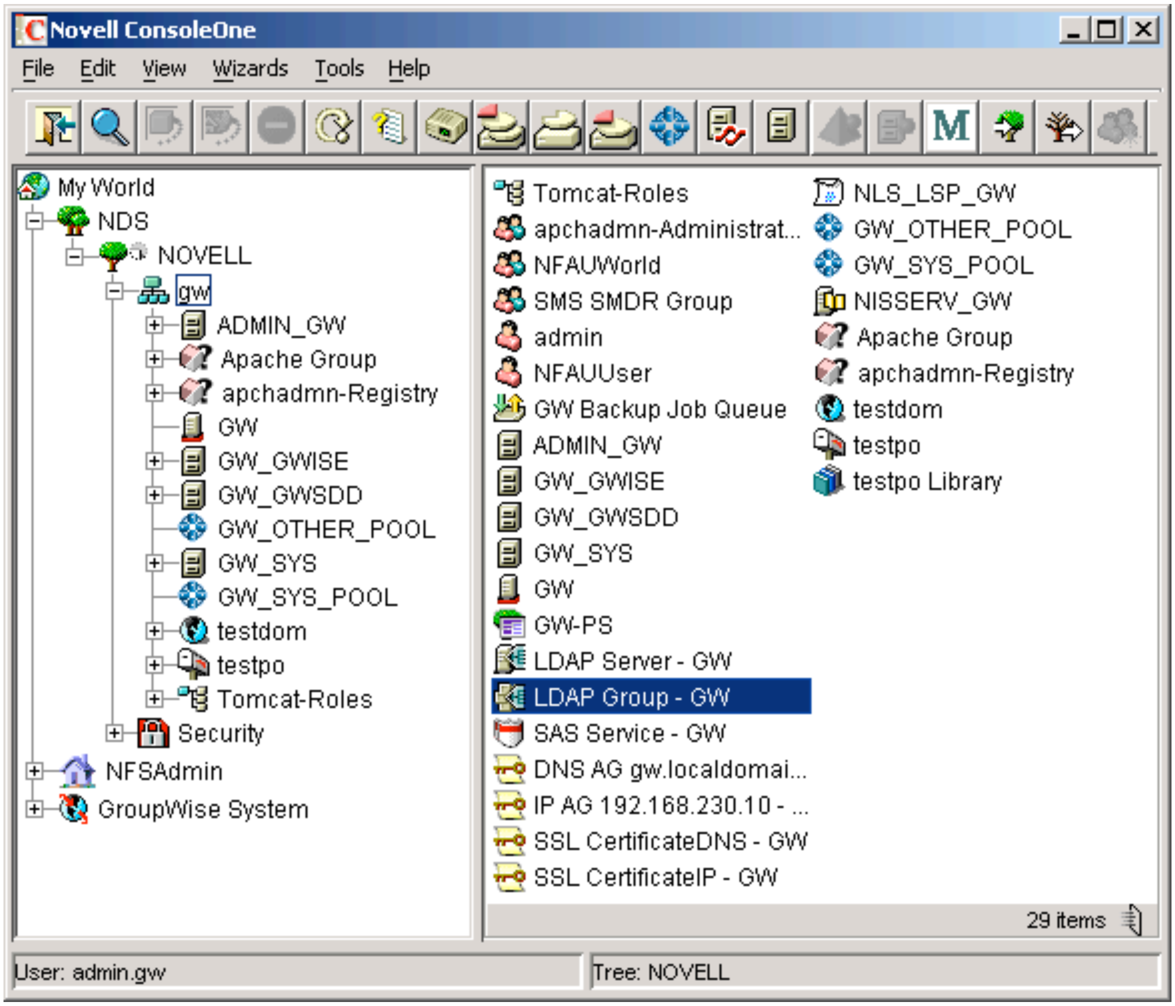
Configuring GroupWise version 7.x/8.x for SSL encrypted LDAP authentication.

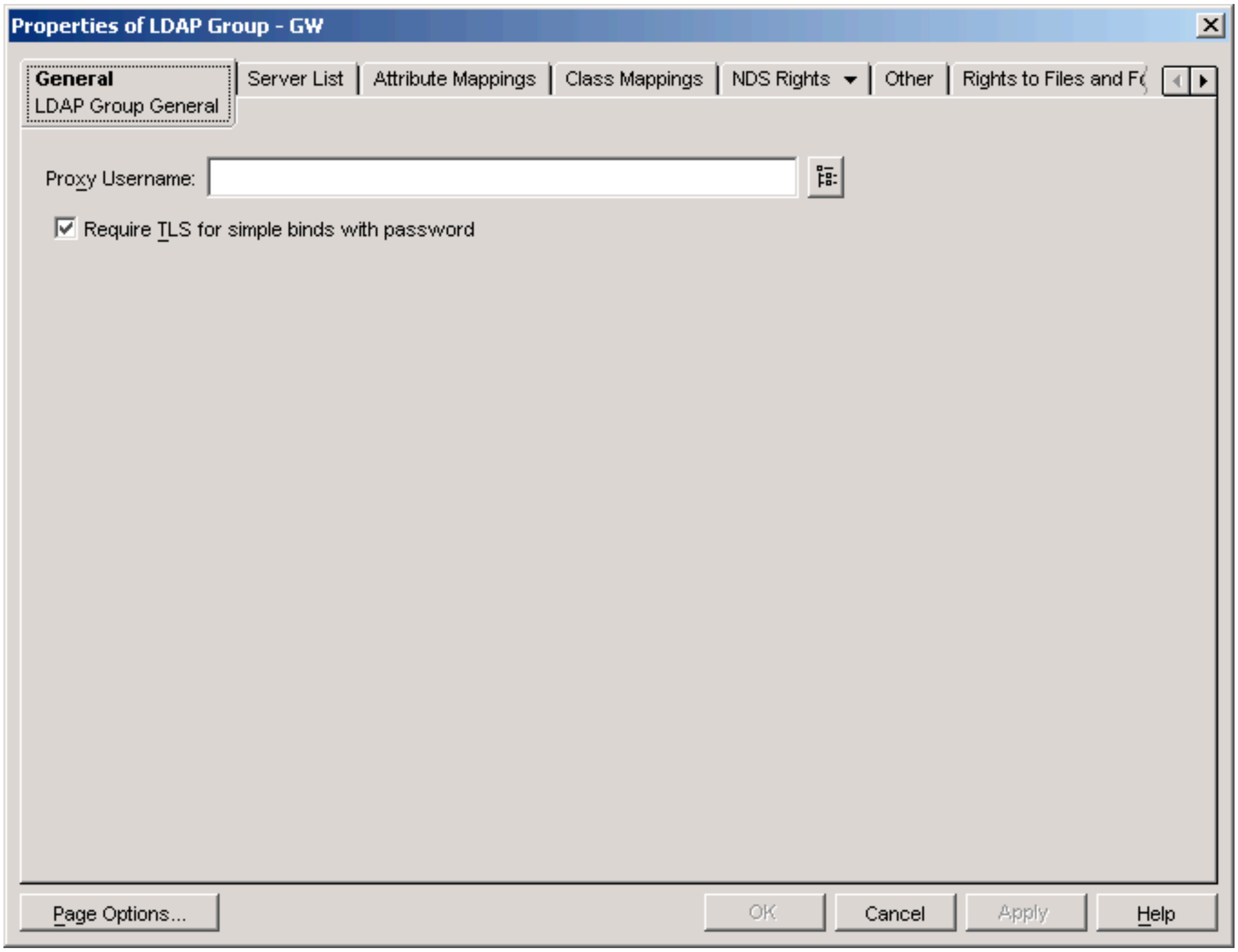
The advantage of enabling LDAP authentication on your GroupWise post office is that your users eDirectory passwords will now be used for GroupWise authentication. If you have password change policies in effect for your eDirectory users, they will now be enforced for GroupWise as well since they are using the same password.

In the following setup example our tree and server information is as follows:

Tree Name: NOVELL
OU: gw
Server Name: GW
GroupWise server IP address: 192.168.230.10



The first step for configuring GroupWise for LDAP access over SSL is to bring up the properties of the GroupWise server's LDAP Group to ensure that TLS is required so we're not sending un-encrypted passwords over the wire. This is the default behavior of the LDAP Group but it is best to verify this setting.



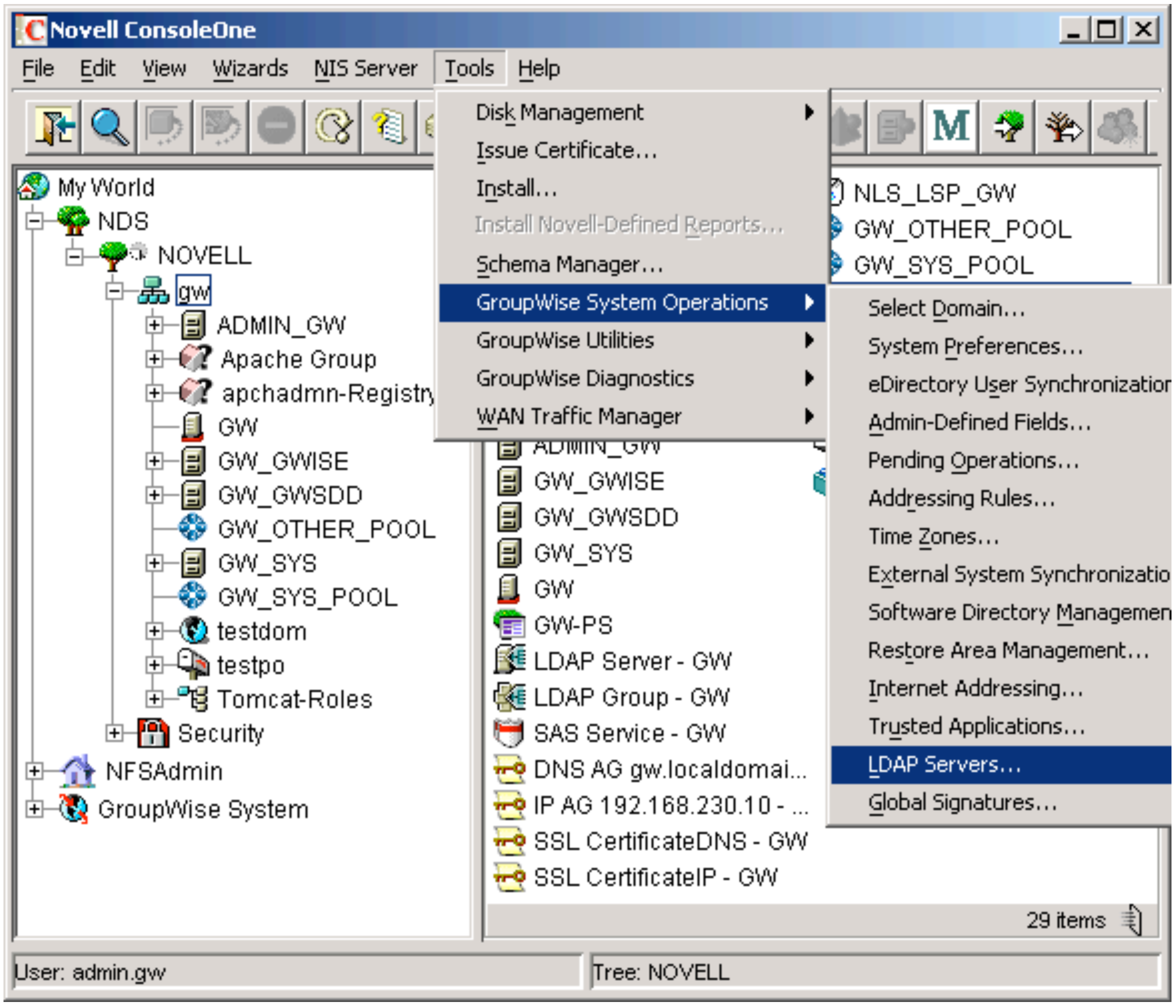
Proxy Username:

☑ Require TLS for simple binds with password

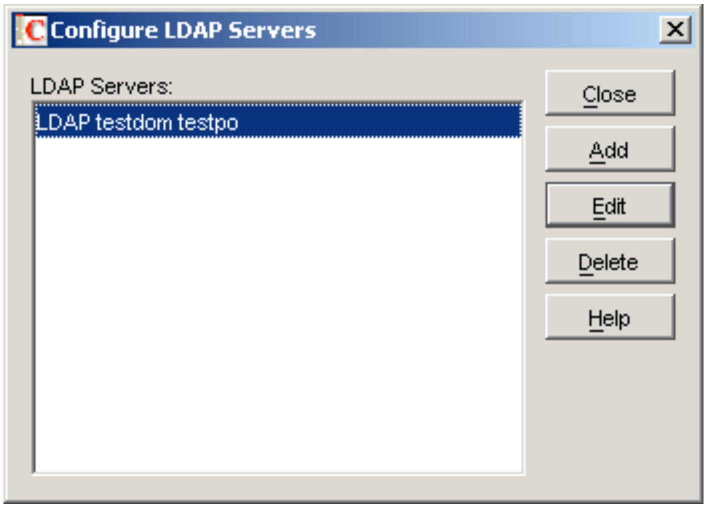
If the "Require TLS for simple binds with password" is not checked, talk to your local network administrator to see why this has been changed. Chances are somebody either got lazy or there is a specific app that requires clear text passwords to be sent over the wire for LDAP authentication.

Next we want to copy our SSL root certificate (default is RootCert.der) from sys:public to the directory where we installed the GroupWise post office agent. By default this is in sys:system on NetWare and /opt/novell/groupwise/agents on Linux

Now that we have the preliminaries out of the way, it's time to set up SSL access to the LDAP server(s). In ConsoleOne select "Tools|GroupWise System Operations|LDAP Servers"



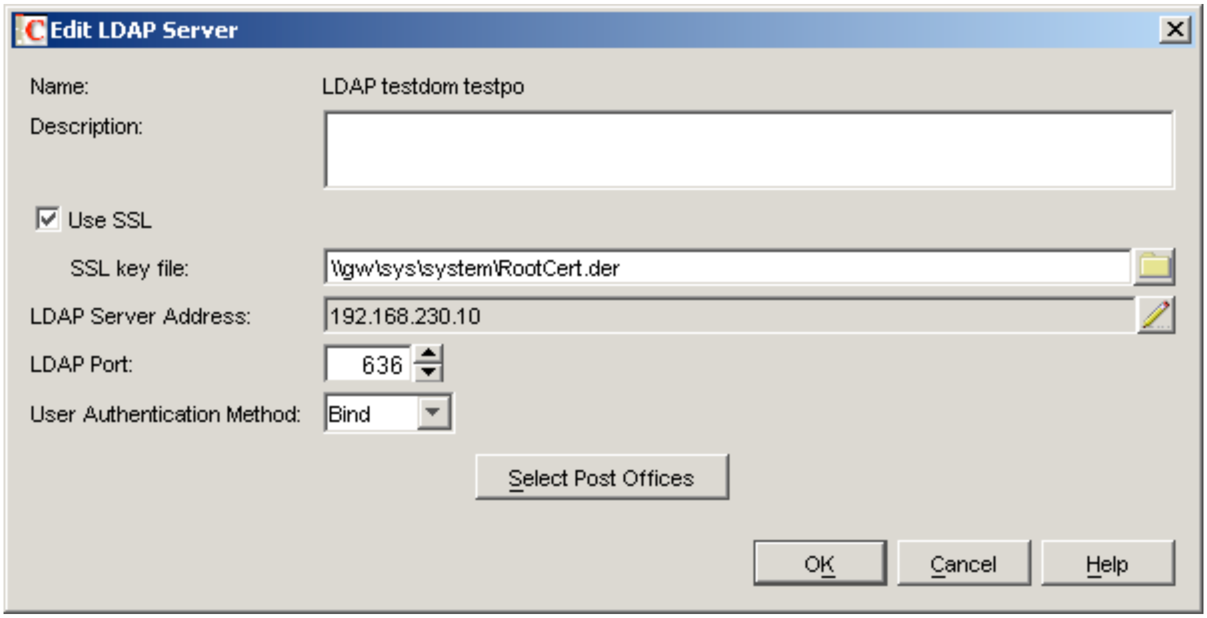
This will bring up the following dialog box



LDAP Servers:

LDAP testdom testpo

If you don't see any LDAP servers listed you can click "Add" and put in your LDAP server information, otherwise click "Edit".



Name: LDAP testdom testpo

Description:

☑ Use SSL

SSL key file: `\\gw\sys\system\RootCert.der`

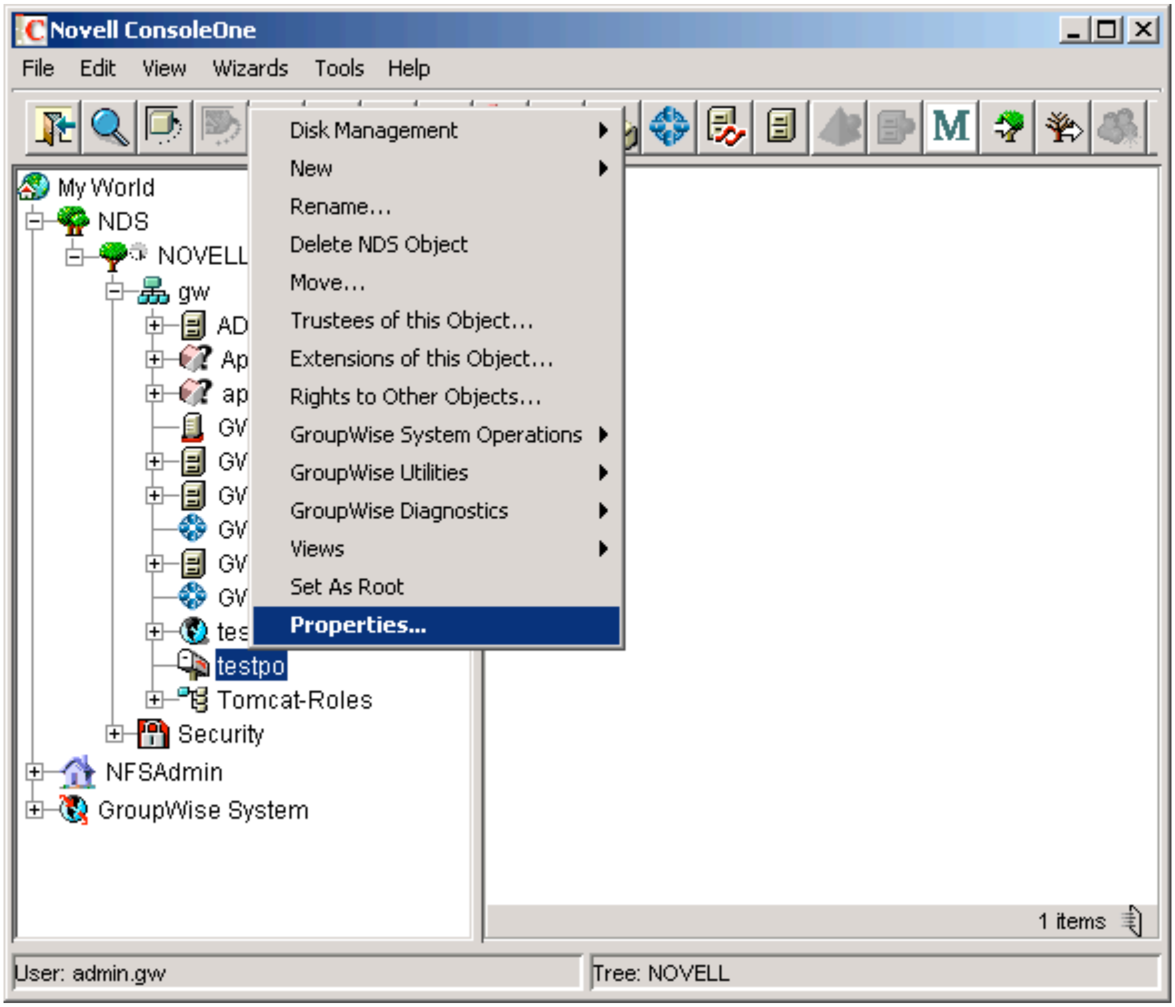
LDAP Server Address: 192.168.230.10

LDAP Port: 636

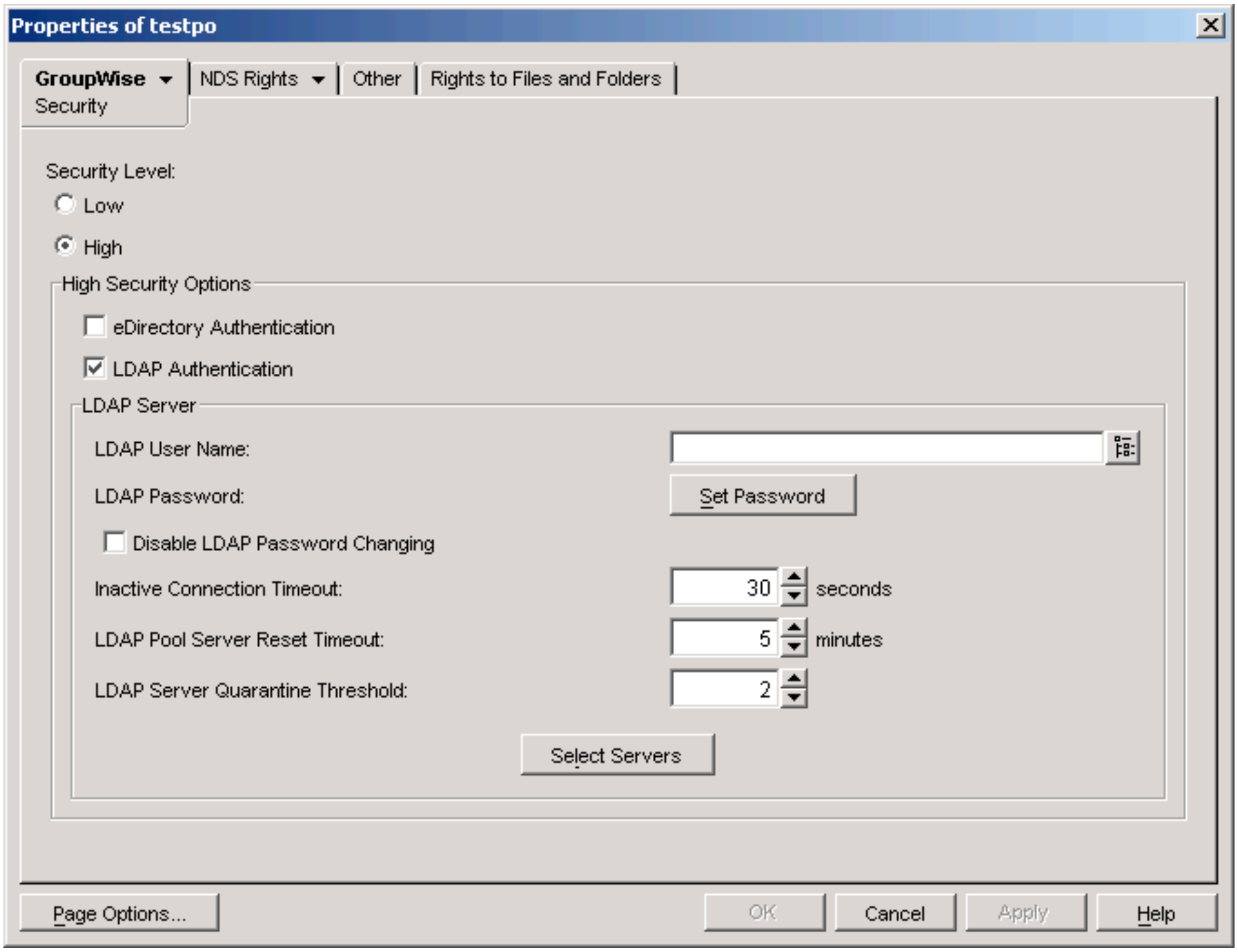
User Authentication Method: Bind

Check the "Use SSL" checkbox. Put in the path to your SSL certificate and specify the IP address or DNS name of your LDAP server.

Now that we've got our LDAP servers defined we need to change the post office to use LDAP authentication. Right click on the PO object in ConsoleOne, in our case this is called testpo, and click "Properties".



Click “Security Settings” from the GroupWise tab drop down box. If your PO security level is set to “Low” select “High”. The ramifications of this change is that users must be logged on to the network in order to access a mailbox that has a blank password.

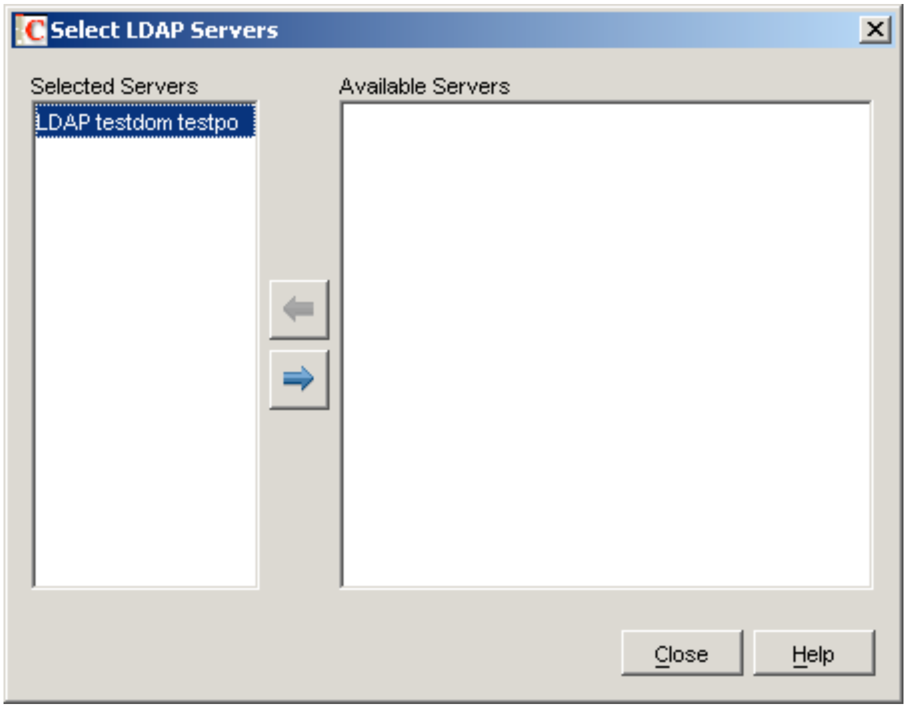


Security Level:
○ Low
● High

High Security Options
□ eDirectory Authentication
☑ LDAP Authentication

LDAP Server
LDAP User Name:
LDAP Password: Set Password
□ Disable LDAP Password Changing
Inactive Connection Timeout: 30 seconds
LDAP Pool Server Reset Timeout: 5 minutes
LDAP Server Quarantine Threshold: 2

Next we want to select “LDAP Authentication” and then click “Select Servers”.



If your server is in the list of selected servers then you are all set. If not, highlight the LDAP server from the list of available servers on the right and click the left arrow button to move it under “Selected Servers” and then click “Close”. After clicking on “Apply” for the properties of the PO a message will be sent to the post office to do a restart with the new settings. No server or PO restart is required. Once the PO has processed the update message your users will now be logging in to GroupWise with their eDirectory passwords.

Potential problems

Root Certificates

The SSL root certificate needs to be in the same directory as the post office agent. The reason is that the agent needs full access to the file. The PO agents wouldn't normally be able to access it in the sys:public directory without permission changes. One thing that you must keep in mind is that when the certificate is renewed, you must then copy the updated certificate to the PO agent directory again.

LDAP SSL authentication failing

If the agents aren't installed to the default location keep in mind that you will need to copy the following LDAP NLM files to the agent directory:

ldaphdlr.nlm
ldapsdk.nlm
ldapssl.nlm
ldapx.nlm
ldapxs.nlm

If these files are not present you will not be able to make an SSL connection to the LDAP server.

Password changes

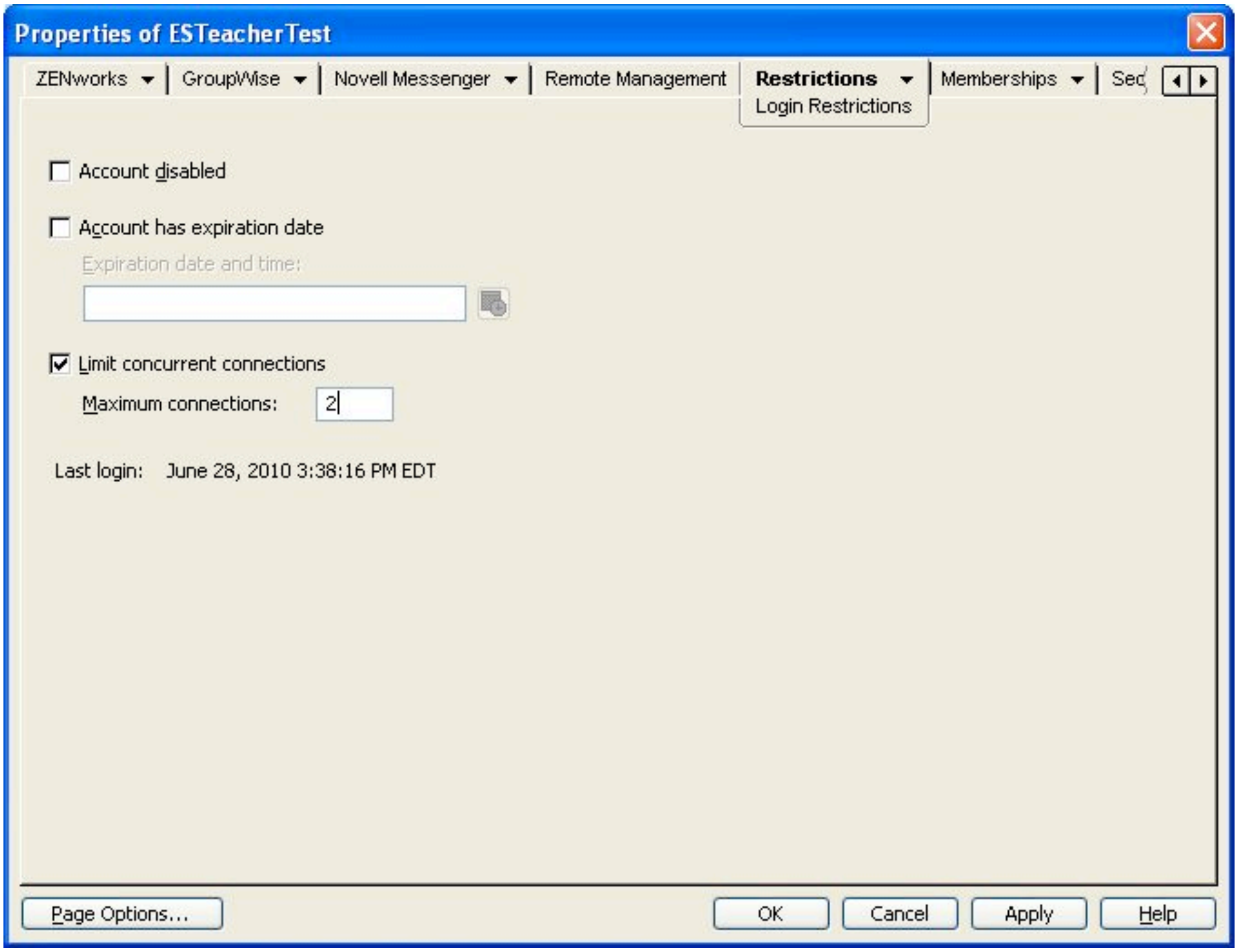
Bear in mind that users can now change their eDirectory password from their email client. This also includes the webmail interface. It is documented in the dialog boxes that allow changing of the password in both the GroupWise client and in web access, but we all know how well users read warning messages.

External entities

External entities are not affected by this change, they will continue to use the GroupWise passwords that are currently assigned.

Concurrent connections

If you are limiting concurrent connections you will want to add an additional login for your user accounts in ConsoleOne (or iManager) since GroupWise authentication will now be consuming an extra connection.



□ Account disabled

□ Account has expiration date

Expiration date and time:

☑ Limit concurrent connections

Maximum connections: 2

Last login: June 28, 2010 3:38:16 PM EDT