



WPC-LDAP Integration Setup Guide

Table of Contents

<i>WPC-LDAP Integration Setup Guide</i>	4
1. Introduction	4
<i>Configuring WPC</i>	5
2. Configuration in Login.wpcs	5
3. Configuration through lookup table	5
<i>Configuring Novell eDirectory Server</i>	9
4. Configure LDAP schema for users and roles	9
4.1 Create a new Organization	9
4.2 Create a new user	10
4.3 Create a new group.....	11
5. Configuration Notes	12
5.1 Password Encryption Support.....	12
6. SSL Setup	14
6.1 Steps to extract self signed certificate for client:	14
6.2 SSL Setup – Client Side (WPC end).....	18
7. Changes required in the Login Script for Novell (DIGEST-MD5)	19
<i>Configuration requirement for SUNONE Directory Server</i>	20
8. Creating a Directory Tree	20
8.1 For Simple Bind	20
8.2 For SASL Bind	20
8.3 For SSL	20
<i>Configuring Microsoft Active Directory Server</i>	26
9. Configure LDAP schema for users and roles	26
9.1 Create a new Domain.....	26
9.2 Create a new Organization	26
9.3 Create a new user	27
9.4 Create a new group	29
10. Configuration Notes:	31
10.1 Configuring Microsoft Active Directory for SSL access and Extract Self Signed Certificate for client	31
<i>Configuring Lotus Domino Server 6.5</i>	33
11. Configure LDAP schema for users and roles	33
11.1 Create a new Person	33
11.2 Create a new group.....	34
11.3 Configuration Notes	36
11.4 SSL Setup.....	36
<i>Configuring Tivoli Directory Server</i>	37
12. Configure LDAP schema for users and roles	37
12.1 Create a new realm.....	37
12.2 Create a new user template	38

12.3 Create a new user -----	39
12.4 Create a new group -----	40
13. SASL - CONFIGURING DIGEST-MD5 on TDS-----	42
-----	43
13.1 Configuration Notes -----	43
13.2 SSL Setup -----	44
13.3 SSL Setup – Client Side (WPC end) -----	47
<i>Configuring Z/OS-----</i>	48
14. Creating Users and Groups:-----	48
14.1 Create a new user:-----	48
14.2 Create a new Group:-----	51

WPC-LDAP Integration Setup Guide

1.Introduction

The Lightweight Directory Access Protocol (LDAP) is an open industry standard. LDAP defines a standard method for accessing and updating information in a directory. LDAP is gaining a wide acceptance as the directory access method of the Internet and is therefore also becoming strategic within corporate intranets.

WPC has traditionally managed its own authentication strategy. However as WPC evolves into a middleware solution that is a component of a larger customer strategic enterprise integration with the other components is core requirement. One such component is the directory server which maintains the enterprise wide business critical User information.

The WPC 5.3 provides integration with the LDAP server using customizable Login & Logout script, it satisfies the IBM directory integration compliance requirements, and it can become interoperable with another directory server.

The WPC-LDAP integration is a two setup process involving changes in the WPC end and at LDAP server end. This document will detail out the setup and configuration steps that are required for various LDAP servers and also the changes need to be made on WPC end for successful WPC-LDAP integration.

Configuring WPC

2. Configuration in Login.wpcs

We need to modify the following configurations in Login.wpcs

- 1) wpcOnlyAuthentication – Flag that identifies the authentication mechanism. Set to false in case ldapAuthentication is required
Default value is true.
- 2) logger_name - The logger variable configure in log.xml
Default value is ldap.

3. Configuration through lookup table

The other configurations to be done for LDAP server is moved from Login.wpcs to a lookup Table (LDAP Properties for English locale). Also the user attributes required to be fetched using LDAPUserDataFetch.wpcs have been moved to this lookup table.

If we are using multiple LDAP URLs, Each ldap url should contain row with the relevant values filled in.

The description of each attributes for LDAP server is given below.

Attribute Names	Description Of Attributes
LDAP URL	Ldap Server url. PK of the lookup table entry. The values are for the ldap server given.
LDAP User Naming Attr	The naming attribute for the users in this LDAP Server
LDAP Group Naming Attr	The naming attribute for the groups in this LDAP Server
User Parent DNs	The Pipe () delimited Parent DNs where the users are likely to be found (Can be set to "") if you do not know the Parent DN
Group Parent DNs	The Pipe () delimited Parent DN where the groups are

	likely to be found (Can be set to "") if you do not know the Parent DN
Root Entry DN	The root user's entrydn in the ldap
Root Password	The password of the root user
Bind Type	The bind type could be one of simple/sasl/ssl. This is provided as an enum.
SSL Bind Type	The subtypes allowed in ssl bind. One of simple/DIGEST-MD5.This is provided as an enum.
personClassNames	The person class name in the LDAP server
groupClassNames	The groups class name in the LDAP server
keystore	The location of the cacerts file that has been imported in to the JVM
supportedSaslMechanisms	Subset of server Supported sasl mechanisms using which the customer wants to authenticate LDAP users if the Bind Type is sasl. The list of mechanisms should be delimited by space character .
First Name Attribute	The user attribute which represents first name in ldap. E.g givenname in Tivoli.
Last Name Attribute	The user attribute which represents last name in ldap. E.g sn in Tivoli.
Full Name Attribute	The user attribute which represents full name in ldap. E.g cn in Tivoli.
Mail ID Attribute	The user attribute which represents mail ID in ldap. E.g mail in Tivoli.
Telephone Number Attribute	The user attribute which represents telephone number in ldap. E.g telephonenumber in Tivoli.
FAX Number Attribute	The user attribute which represents fax number in ldap. E.g facsimiletelephonenumber in Tivoli.
Postal Address Attribute	The user attribute which represents postal address in ldap. E.g postaladdress in Tivoli.
Title Attribute	The user attribute which represents title in ldap. E.g title in Tivoli.

Sample Configuration Values for Various Directory Servers

	Sun-One	Novell	Notes Domino
LDAP URL	ldap://9.184.114.57:3537	ldap://9.184.112.116:389	ldap://9.182.149.115:389
LDAP User Naming Attr	Uid	Cn	Cn
LDAP Group Naming Attr	Cn	Cn	Cn
User Parent DNs	dc=in,dc=ibm,dc=com (Mandatory)		
Group Parent DNs	dc=in,dc=ibm,dc=com (Mandatory)		
Root Entry DN	uid=admin, ou=administrators, ou=topologymanagement, o=netscaperoot	Cn=admin,o=company	cn=SanjayIBM_User
Root Password	trinitron	root1234	wpcldap
Bind Type	simple	Simple	simple
personClassNames	inetOrgPerson	Inetorgperson	inetorgPerson
groupClassNames	groupOfUniqueNames	groupofUniqueNames	groupOfUniqueNames
keystore			
supportedSaslMechanisms			



	Tivoli	Z/OS	Microsoft
LDAP URL	ldap://9.184.114.80:389	ldap://tvt1003.tivlab.raleigh.ibm.com:389	ldap://9.182.149.46:389
LDAP User Naming Attr	Cn	Cn	cn
LDAP Group Naming Attr	Cn	Cn	cn
User Parent DNs	Cn=localhost (Mandatory)	cn=admin,cn=wpctreeeroot,dc=tvt1003	dc=wpc,dc=com (Mandatory)
Group Parent DNs	Cn=localhost (Mandatory)	cn=admin,cn=wpctreeeroot,dc=tvt1003	dc=wpc,dc=com (Mandatory)
Root Entry DN	Cn=root	Bryan	CN=wpcuser,OU=isl,OU=ibm,dc=wpc,dc=com
Root Password	root	secret	root1234
Bind Type	simple	Simple	Simple


personClassNames	inetOrgPerson	Inetorgperson	person
groupClassNames	groupOfUniqueNames	groupofUniqueNames	group
keystore			
supportedSaslMechanisms			

LDAP Properties ...

Common Attributes

Primary Key, Display

LDAP URL  

LDAP Properties Spec 

LDAP User Naming Attr

LDAP Group Naming Attr

User Parent DNs

Group Parent DNs

Root Entry DN

Root Password

Bind Type

SSL Bind Type

personClassNames

groupClassNames

Keystore

supportedSaslMechanisms

First Name Attribute

Last Name Attribute

Full Name Attribute

Mail ID Attribute

Telephone Number Attribute

FAX Number Attribute

Postal Address Attribute

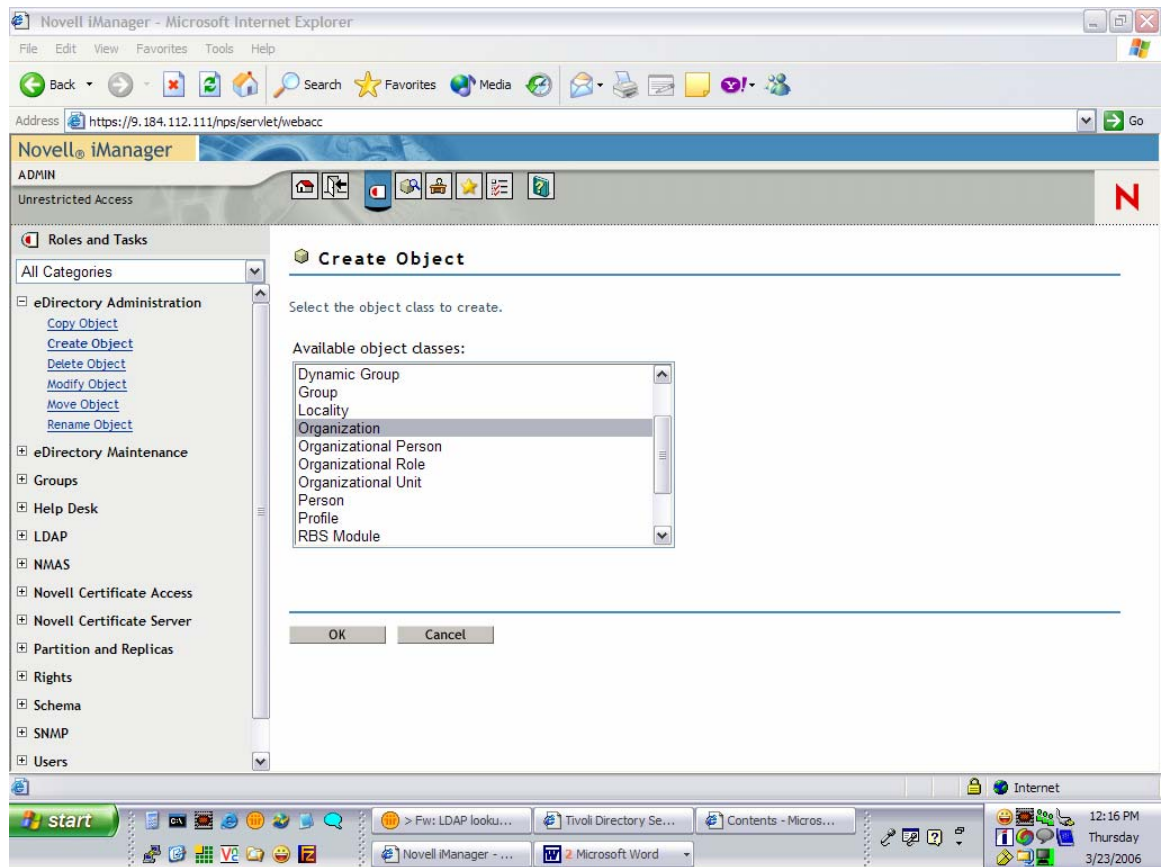
Title Attribute

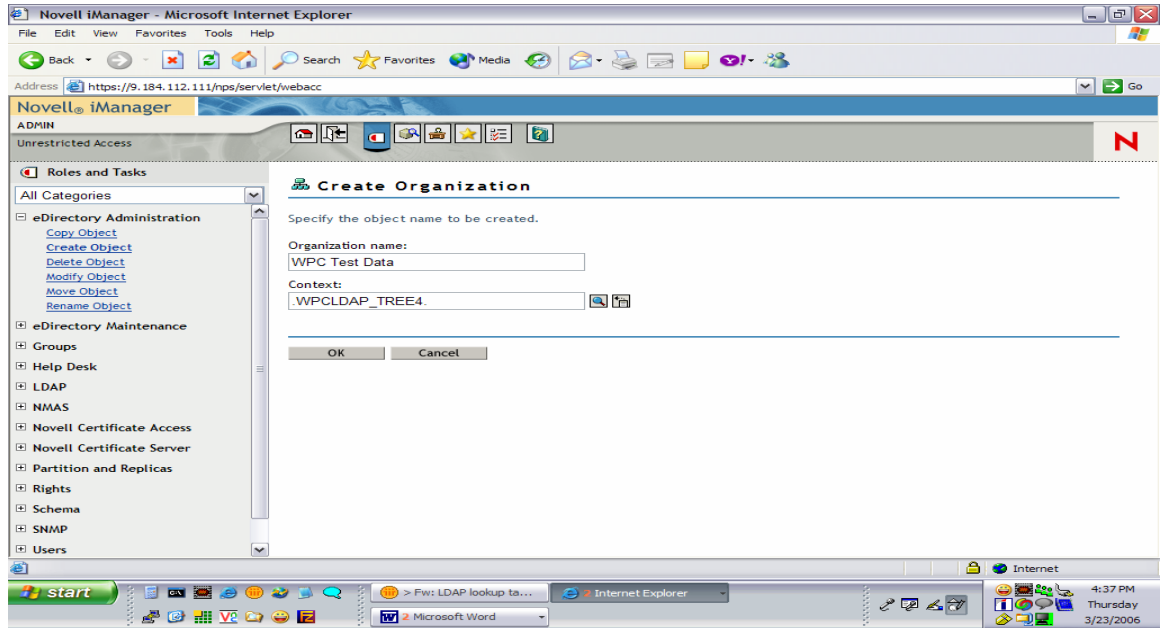
Configuring Novell eDirectory Server

4. Configure LDAP schema for users and roles

4.1 Create a new Organization

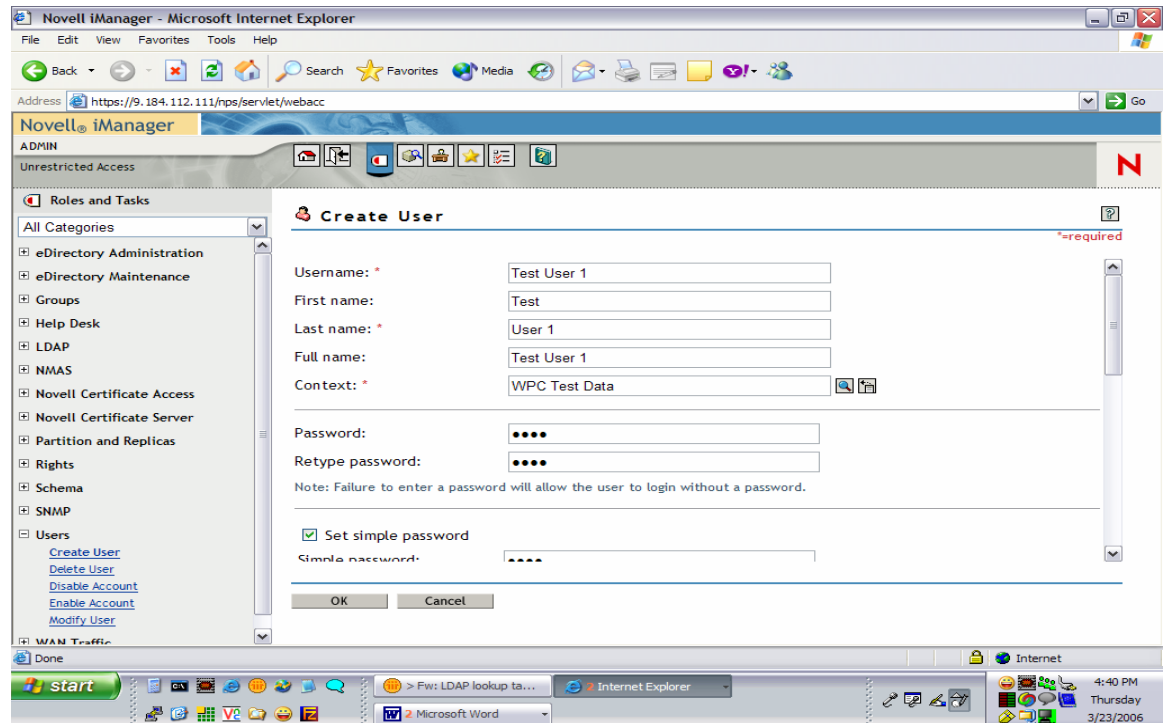
1. Create a new Organization from Novell iManager web console using eDirectory Administration > Create Object option.
2. Give organization name and context in which Organization should reside.





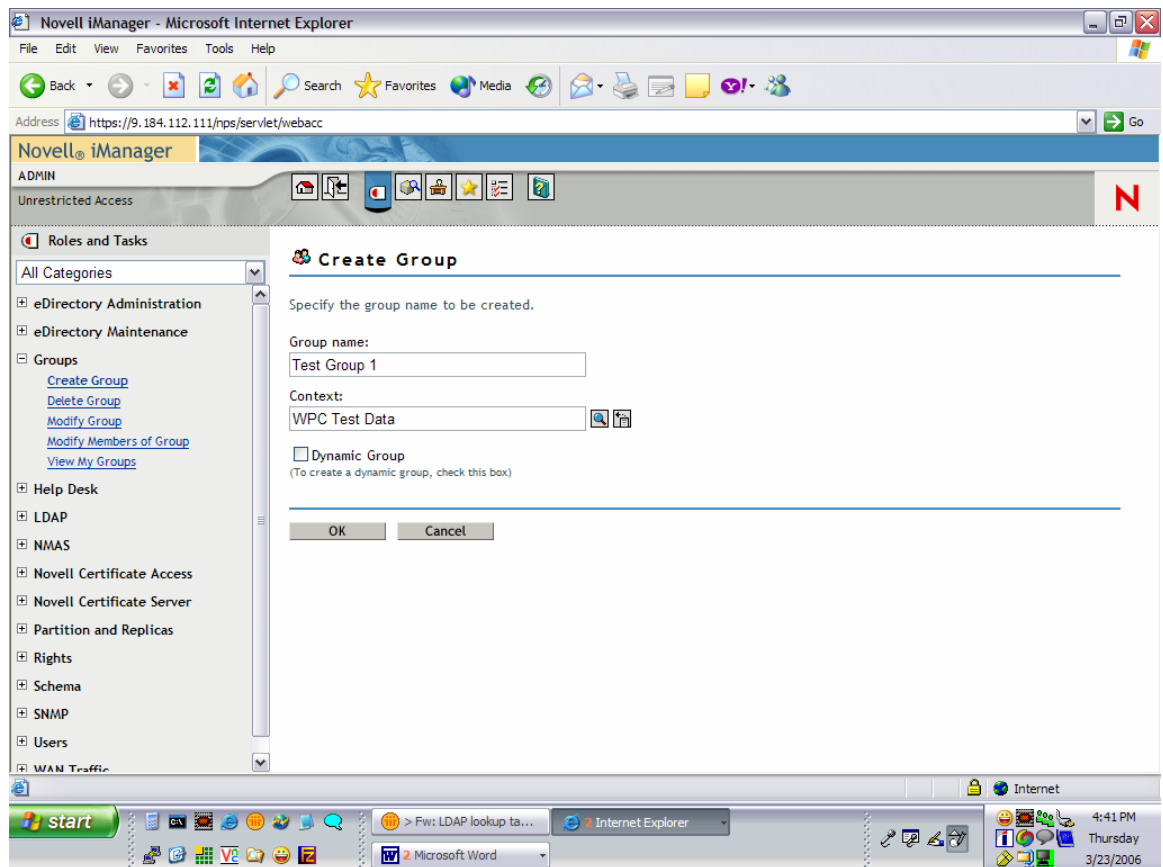
4.2 Create a new user

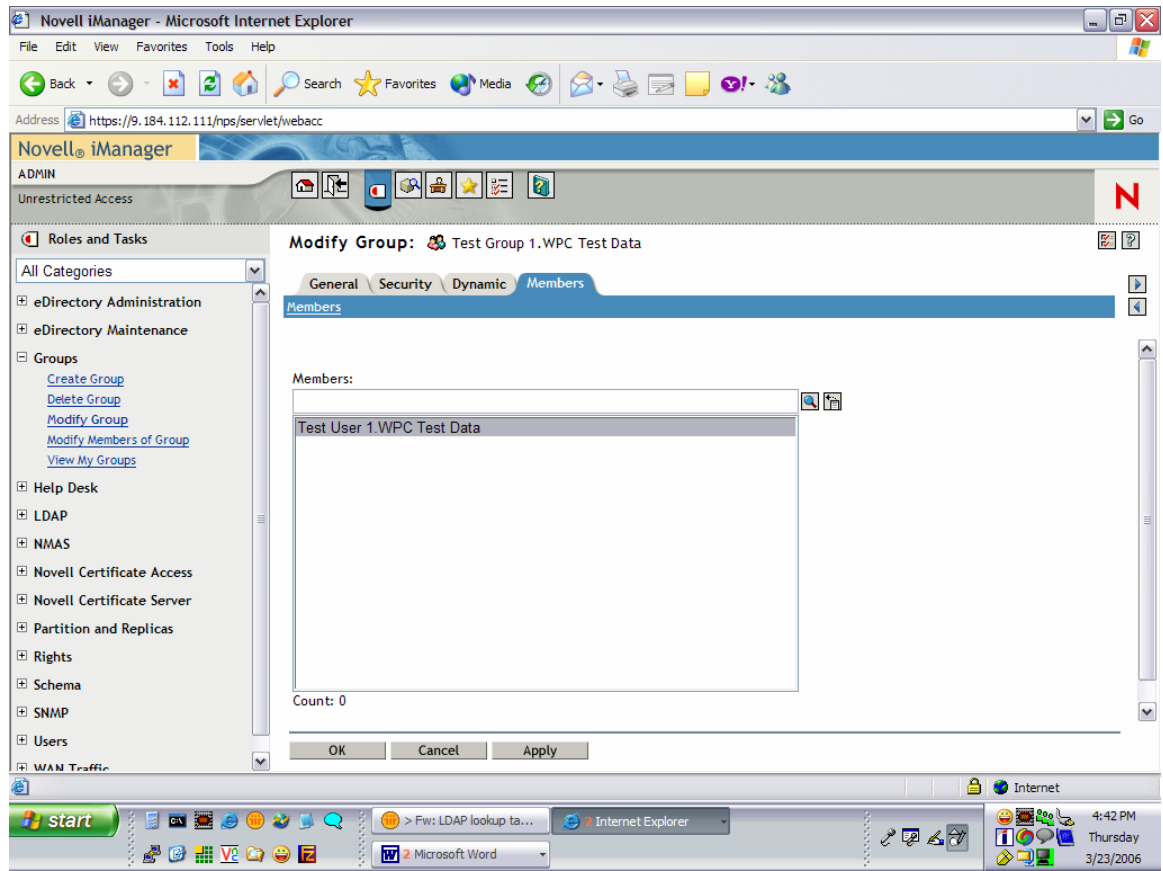
1. Create a new User from the Novell iManager web console using the menu path **Users > Create User**.
2. Select the above-created Organization for this user.
3. Set NDS Password and Simple Password.



4.3 Create a new group

1. Create a new Group from the Novell iManager web console using the menu path **Groups > Create Group**.
2. Select the above-created Organization for this group.
3. Modify the Group and associate the Users to Groups.



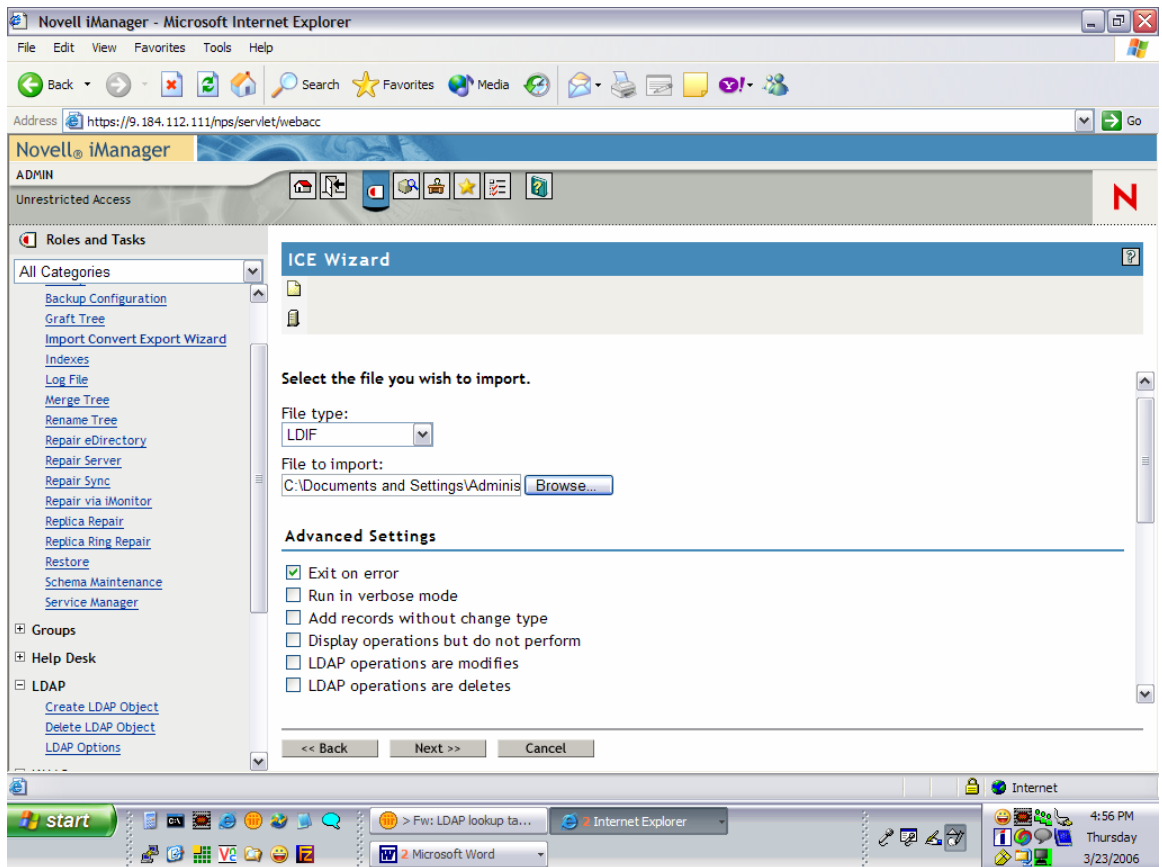
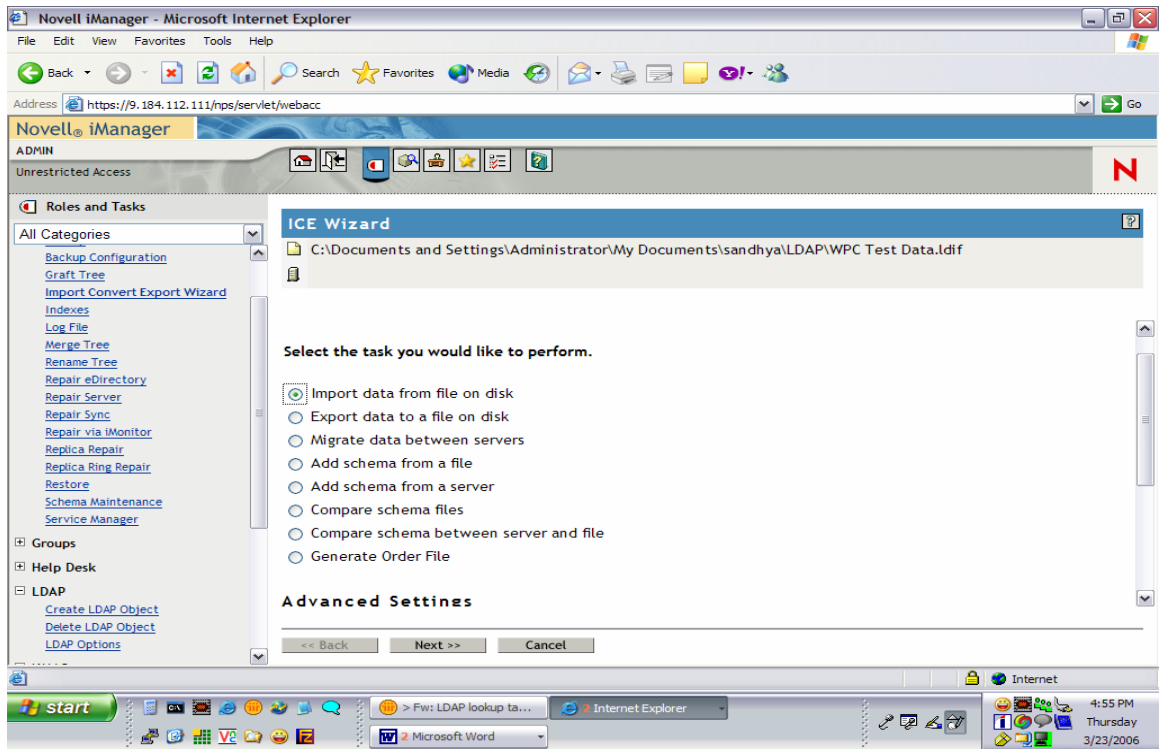


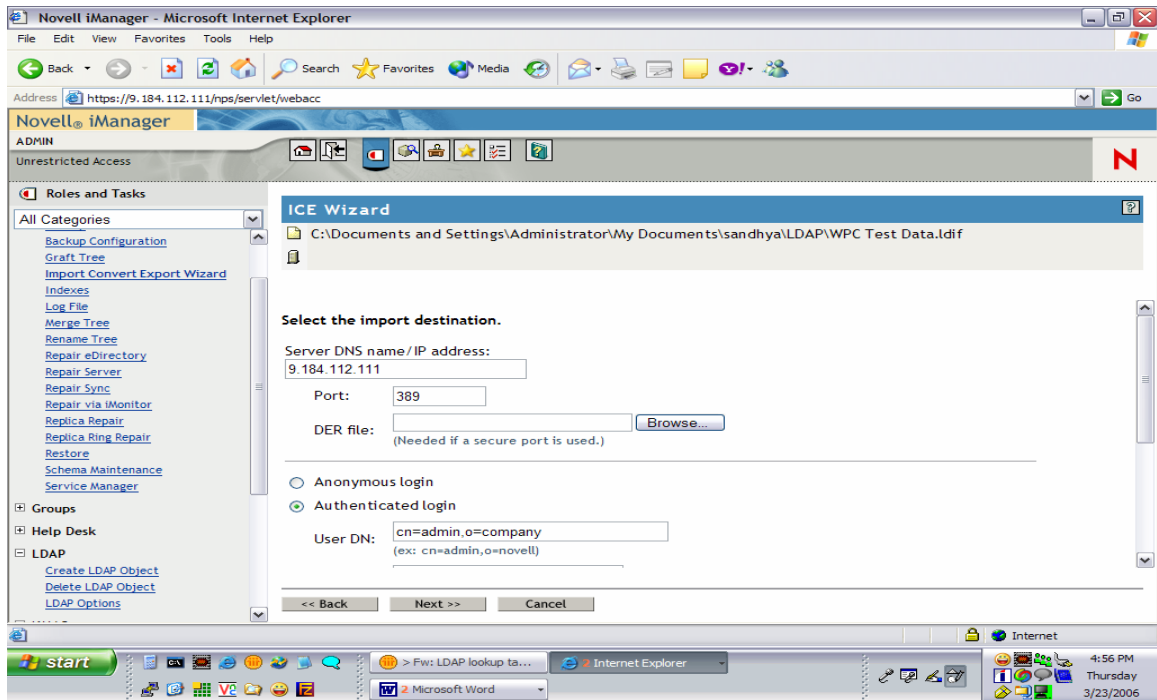
5. Configuration Notes

5.1 Password Encryption Support

SHA-1 and Crypt Password encryptions are tested by importing the LDIF which has user objects with SHA/Crypt encrypted password through iManager web console.

- Go to eDirectory Maintenance -> Import Convert Export Wizard.
- Select Import data from file on disk and click next.
- Browse the file from disk to be imported and click next.
- Give the destination IP address and the login details. In the advanced settings select Allow forward references.

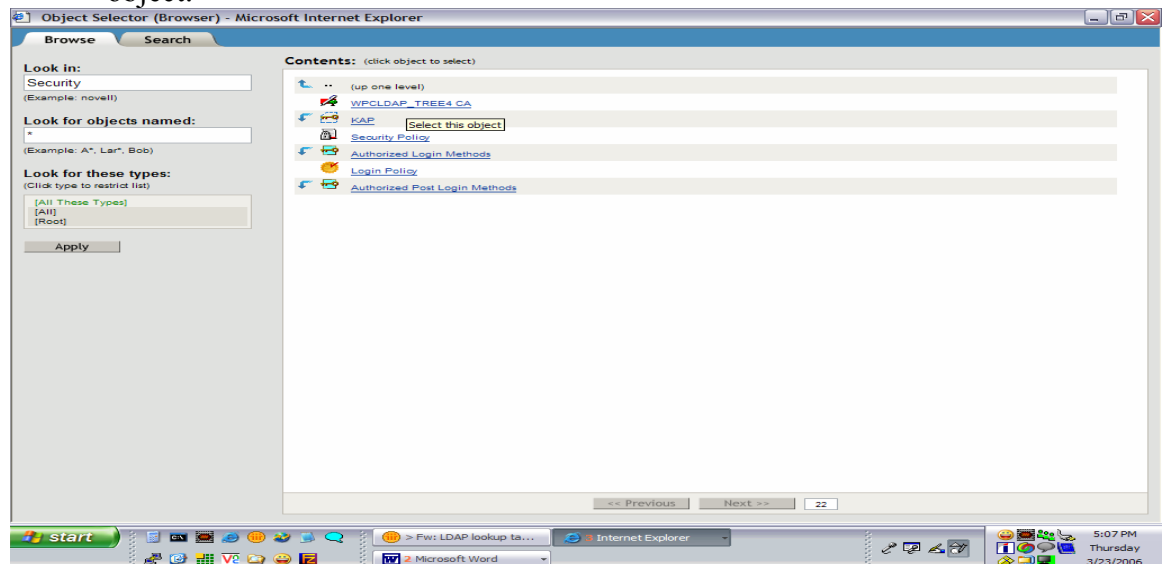


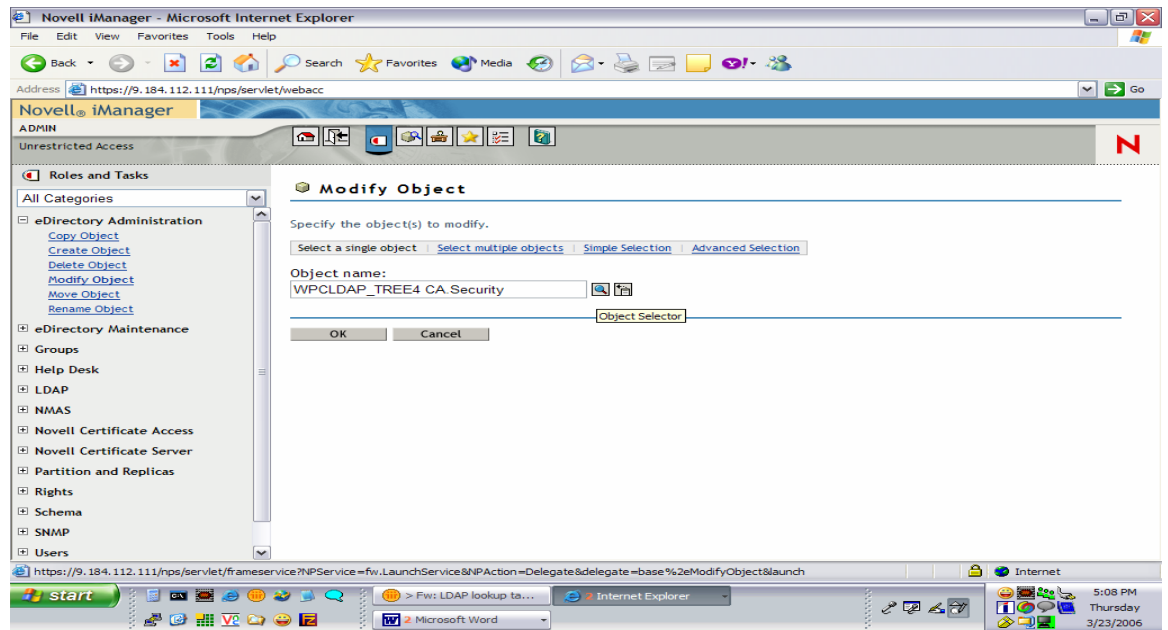


6. SSL Setup

6.1 Steps to extract self signed certificate for client:

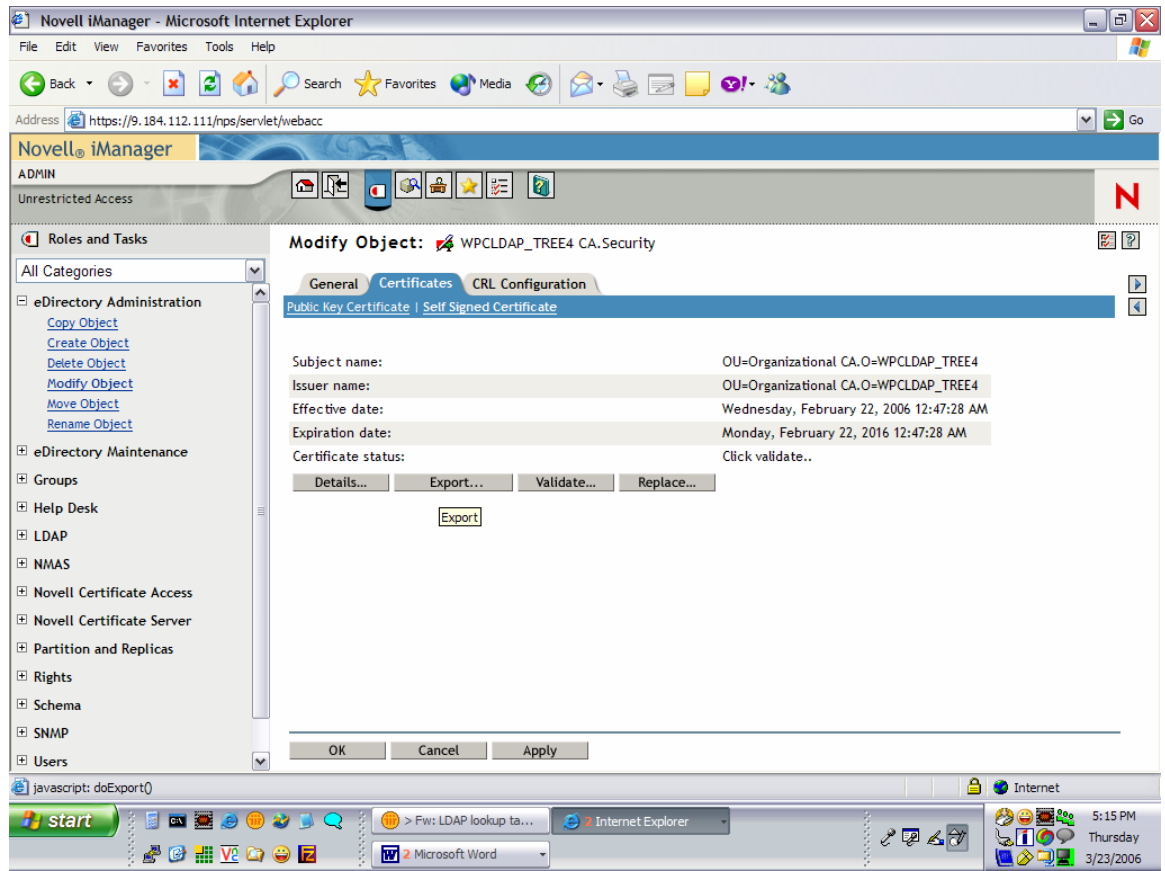
1. Go to eDirectory Administrator -> Modify Object.
 - i. Object name is selected from the Object Selector window. Click Object Selector.
 - ii. Select the <Tree>CA object, for example: WPCLDAP_TREE4 CA object.



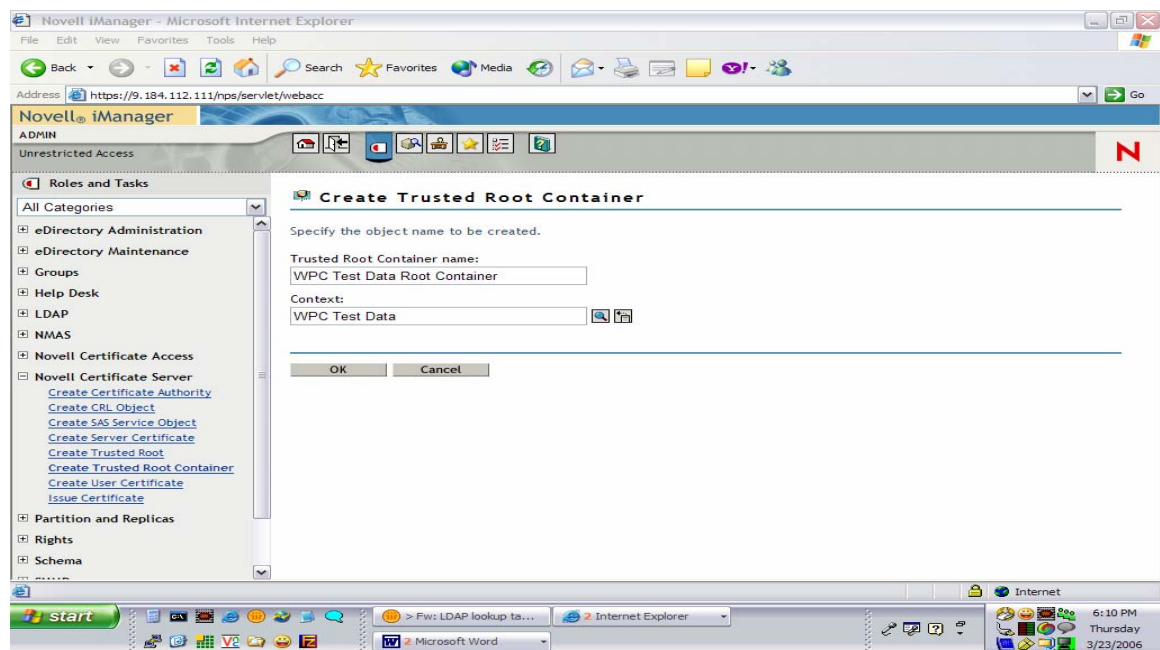


2. Go to Certificates -> Self Signed certificate -> Export.

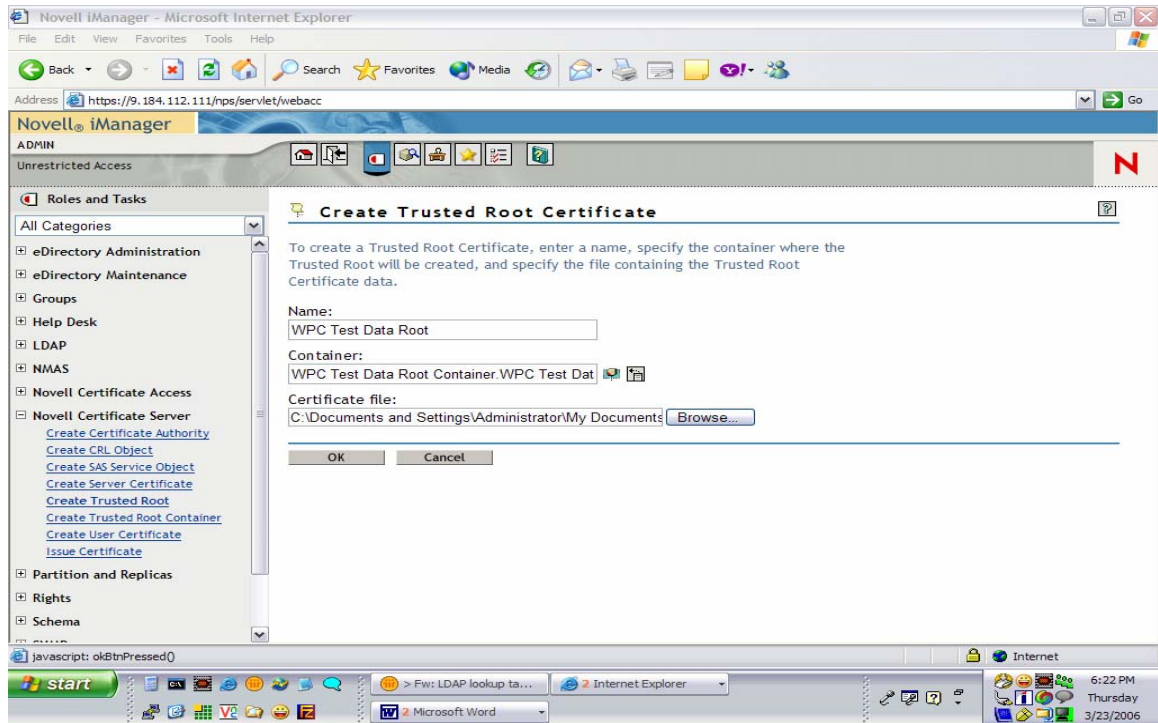
- i. Do you want to export the private key with the certificate? No
- ii. Select an output format. File in Base64 format.
- iii. Click “Save the exported certificate to a file” -> Save the file.



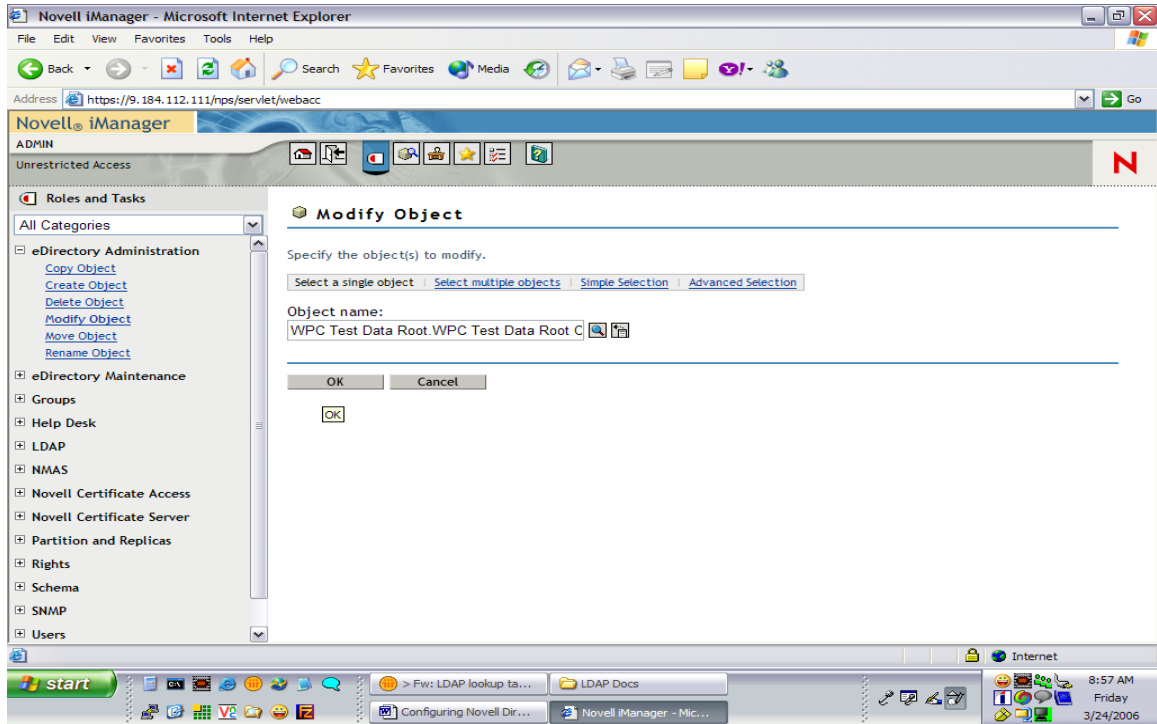
3. Go to Novell Directory Server -> Create Trusted Root Container -> Give a Trusted Root Container name and Context.



4. Create a Trusted Root with the above container and certificate file created in step2.



5. Go to eDirectory Administration -> Modify Object -> Modify the Trusted Root object (which will be under Trusted root container).
 - Export the certificate in Base 64 format and save the certificate.



6. You have now created a file that holds your own root certificate. This must be imported to all communication partners that will connect to the server through SSL.

6.2 SSL Setup – Client Side (WPC end)

1. Get the .b64 file generated in the above steps in to the WPC environment.
2. Use the keytool command to import this in to the JVM.


```
keytool -import -trustcacerts -keystore cacerts -storepass changeit -noprompt -alias mycert -file <cert_file_generated>
```
3. Change the location of the cacerts file in the keystore variable in the login script. If the file that was generated in the step2 was in /home/sgopan/cert/cacerts, make the value for the keyStore variable to this location.

Note: Set the bindType variable to ssl and sslBindType to either simple or DIGEST-MD5.

7. Changes required in the Login Script for Novell (DIGEST-MD5)

The login script has appropriate sections that describe the steps to be followed to enable SASL Bind for Novell.

Novell expects the principal to be prefixed with dn;, followed by the entryDn unlike Tivoli where the just the naming attributes value would be sufficient for the SASL Bind.

Configuration requirement for SUNONE Directory Server

8. Creating a Directory Tree

Follow the instructions given in the link <http://docs.sun.com/source/816-6698-10/suffixes.html> to create a directory tree structure.

8.1 For Simple Bind

1. In the login script the parentDN for the users and for the groups should be set atleast to the top level DN e.g “o=IBM”.

8.2 For SASL Bind

1. The changes done in the login script for SASL Bind are similar to the changes done for Novell eDirecotry. The Context.SECURITY_PRINCIPAL should have the full entry DN with prefix as “dn:”.
2. In the login script the parent DN value should have atleast the top level dn. For e.g. “o=IBM”.
3. The fully qualified host name of the server should be entered in the etc/hosts file of the client machine. The provider url should be the fully qualified host name of the server. Using IP address for provider url will throw protocol error.

Following are the changes required to be done in the login script for SUN ONE Directory Server :

The login script has appropriate sections that describe the steps to be followed to enable SASL Bind for Sun-One.

Sun-One like Novell expects the principal to be prefixed with dn: , followed by the entryDn unlike Tivoli where the just the naming attributes value would be sufficient for the SASL Bind.

8.3 For SSL

Refer the the following url : <http://docs.sun.com/source/816-6704-10/ssl.html>.

Follow the steps given below for server side setup :

1. Request for a certificate for the certifying authority. E.g <https://www.verisign.com/products-services/security-services/ssl/index.html>.
2. To request for a certificate you need to generate a CSR(Certificate Signing Request).
3. Go to Tasks -> Manage Certificates -> Server Certs (Tab)
Enter the details required for generating the certificate like the hostname of the server, company name, organization name, city, country etc.

The screenshot shows a 'Certificate Request Wizard' window with the following details:

- Server name: 2fdibm412.in.ibm.com
- Organization: IBM
- Organizational unit: WPC-GDS
- City/locality: Bangalore
- State/province: Karnataka
- Country/region: IN India

Buttons at the bottom: < Back, Next >, Cancel, Help, Show DN.

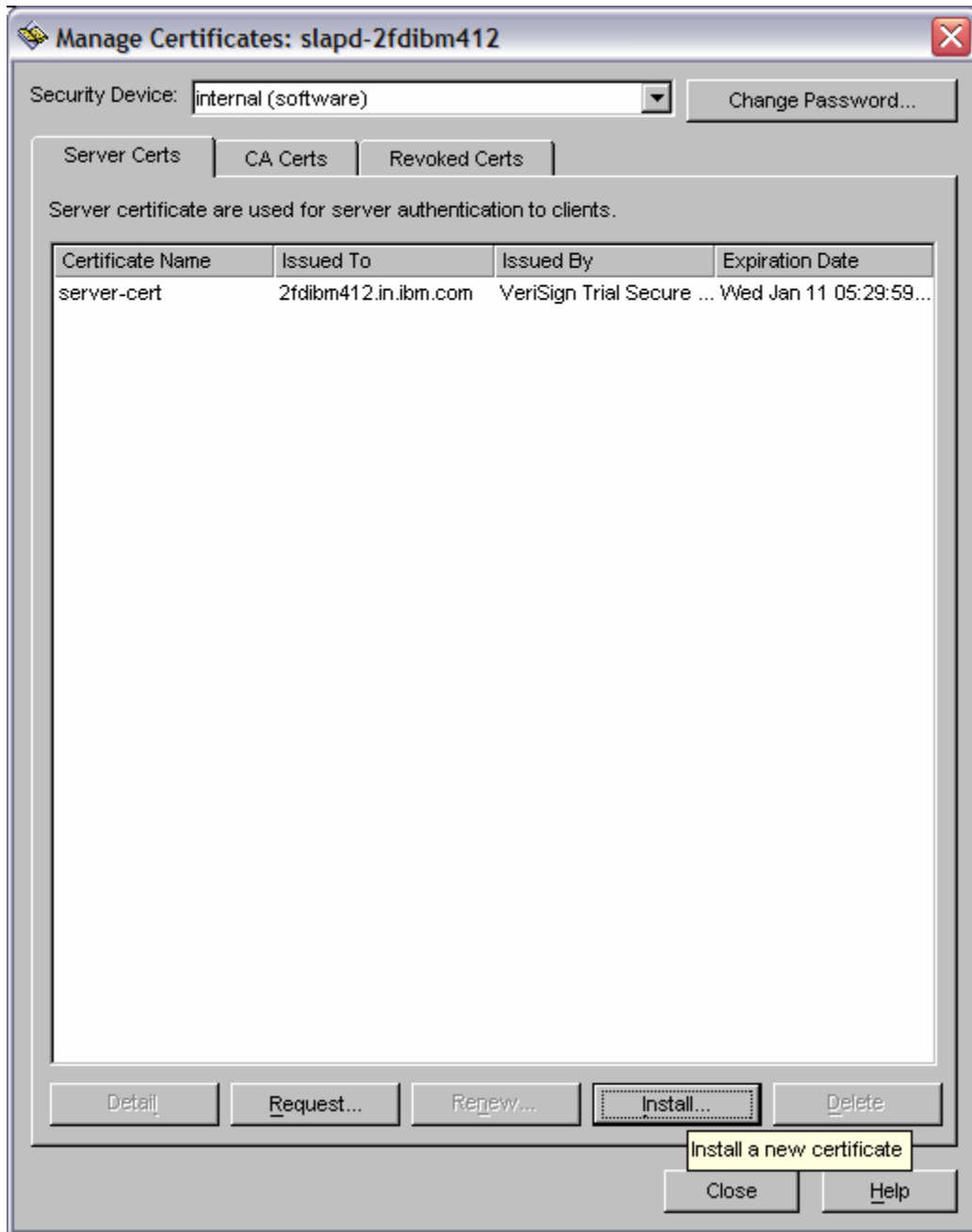
4. After going through these steps a CSR will be generated. This CSR can be used to request a certificate from Verisign.
5. A mail will be sent to you with a certificate of 15 day validity period. The certificate would be as below. It includes the header and the footer.

```
-----BEGIN CERTIFICATE-----
MIIEOjCCA6OgAwIBAgIQN77E+RcOX6hx5pJXsfNqIjANBgkqhkiG9w0BAQUFADCB
jDELMakGA1UEBhMCVVMxZzAVBGNVBAoTD1Zlcm1TaWduLCBjbmuMTAwLgYDVQQQL
EydGb3IyVGVzdCBQdXJwb3NlcyBpbm5LiAgTm8gYXNzdXJhbmNlcy4xMjAwMjE1
BAMTKVZlcm1TaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIyVGVzdCBSc290IENBMB4X
DTA1MTIyNzAwMDAwMFoXDTA2MDExMDIzNTk1OVowgbAxCzAJBgNVBAYTAlOMRIw
EAYDVQQIEwllYXJhYXRha2EExEjaQBGNVBAUCUJhbmdbG9yZTEEMMAoGA1UEChQD
SUJNMRAwDgYDVQQLFAdXUEMTR0RTMTowOAYDVQQLFDFUZXJtcyBvZiB1c2UgYXQg
d3d3LnZlcm1zaWduLmNvbS9jcHMvdGVzdGNhIChjKTA1MR0wGwYDVQQDFBQyZmRp
Ym00MTIuaW44aWJtLmNvbTcBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEAAs1YP
QtIIQu44aU55YmAkblD96SUIoLk3wYfmQ1gW21c2LiHc8IfqGOH7r9HMjppq78TOZ
2c/FB3awI1U8uB1239wMTbneiKbP2jWnO/YCAk0z53Bt2UZhdCxaGMyjNnoxVD9C
```

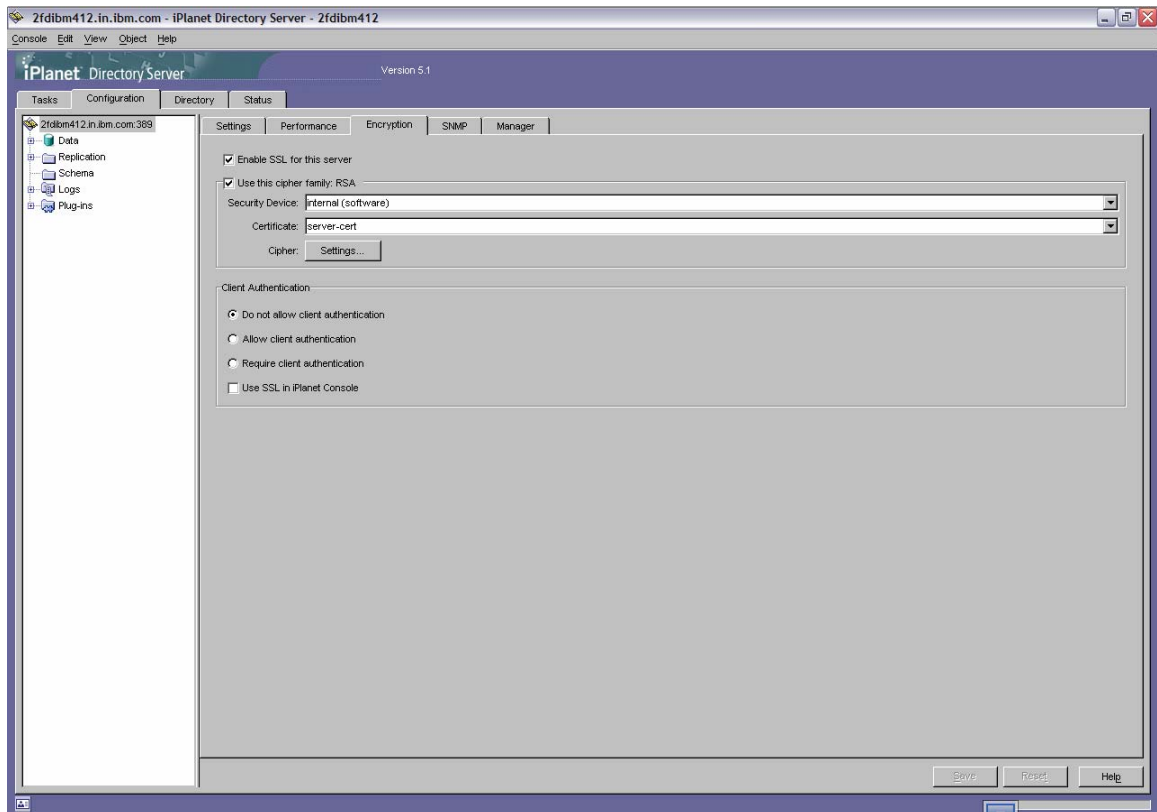
HxRZJ34d9EqolFcuyNLFvLTfgvc/fYAMwrlXM78CAwEAAaOCAXUwggFxmAkGA1Ud
EwQCMAAwCwYDVR0PBAQDAgWgMEcGA1UdHwRAMD4wPKA6oDiGNmh0dHA6Ly9TVlJT
ZWN1cmUtY3JsLnZlcm1zaWduLmNvbS9TVlJUcm1hbFJvb3QyMDA1LmNybDBKBgNV
HSAEQzBBMD8GCmCGSAGG+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cu
dmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EwHQYDVR0lBBYwFAYIKwYBBQUHAWEGCCsG
AQUFBwMCMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
dmVyaXNpZ24uY29tMG0GCCsGAQUFBwEMBGEwX6FdoFswWTBXMfUWCWltYWdlL2dp
ZjAhMB8wBwYFKw4DAhoEFI/10xqGrI2Oa8PPgGrUSBgsexkuMCUWI2h0dHA6Ly9s
b2dvLnZlcm1zaWduLmNvbS92c2xvZ28uZ2lmMA0GCSqGSIB3DQEBBQUAA4GBAJkH
7bLGW4CDUyc1bG0dIg/cl5Ab/5fd+MhVss1RsGZEEvevjkbqbwktKtGTQGR4til
sffCc0Xh6ksRBOTdObf7jch0z3tTe92EHY++YcgPXYOVdKNi4MPKZ+bRMJr7r5Ry
mINY3LXU2JLGSf3ZInInu44y9jqbTEXC7oqG07M

-----END CERTIFICATE-----

6. Install this certificate in your server. To do this you need to go to
Tasks -> Manage Certificates -> Server Certs (Tab) -> Install (button).



7. After installing the certificate you need to enable SSL in the server. To do this go to Configuration (Tab) -> Encryption (Tab) .



The “Enable SSL” checkbox should be checked. Check the “Use this cipher family” checkbox and select the certificate which you have installed. Under “Client Authentication” section, select “Do not allow client authentication”.

Follow are the steps below for client side setup :

1. Save the certificate which you had obtained from verisign in a file. Save it in a folder where you want to generate your keystore.
2. Use certutil for creating a certificate database.

`certutil -N -d certdir` (Where *certdir* is the directory where certificate db is to be generated. For eg the current directory).

This will generate `cert7.db` and `key3.db` in the directory specified with `-d` option.

3. Import the certificate which you have saved as part of step 2 in the certificate database using the following command.

```
certutil -A -n nameoftheserver -t trustargs -i cerfile -d certdir
```

Eg `certutil -A -n "2fdibm412.in.ibm.com" -t "C,C,C" -i iplanetcert.cert -d .`

4. To check if the certificate has been imported properly. Use the following command.

```
certutil -L -n "2fdibm412.in.ibm.com" -d .
```

5. Get the binary format for the certificate using the following command.

```
certutil -L -n "2fdibm412.in.ibm.com" -d . -r > checkcert
```

This will generate the file checkcert which is the binary format of the certificate.

6. Using keytool import the certificate in keystore.

```
keytool -import -trustcacerts -keystore cacerts -storepass changeit -noprompt -alias ipcrt -file checkcert
```

Configuring Microsoft Active Directory Server

9. Configure LDAP schema for users and roles

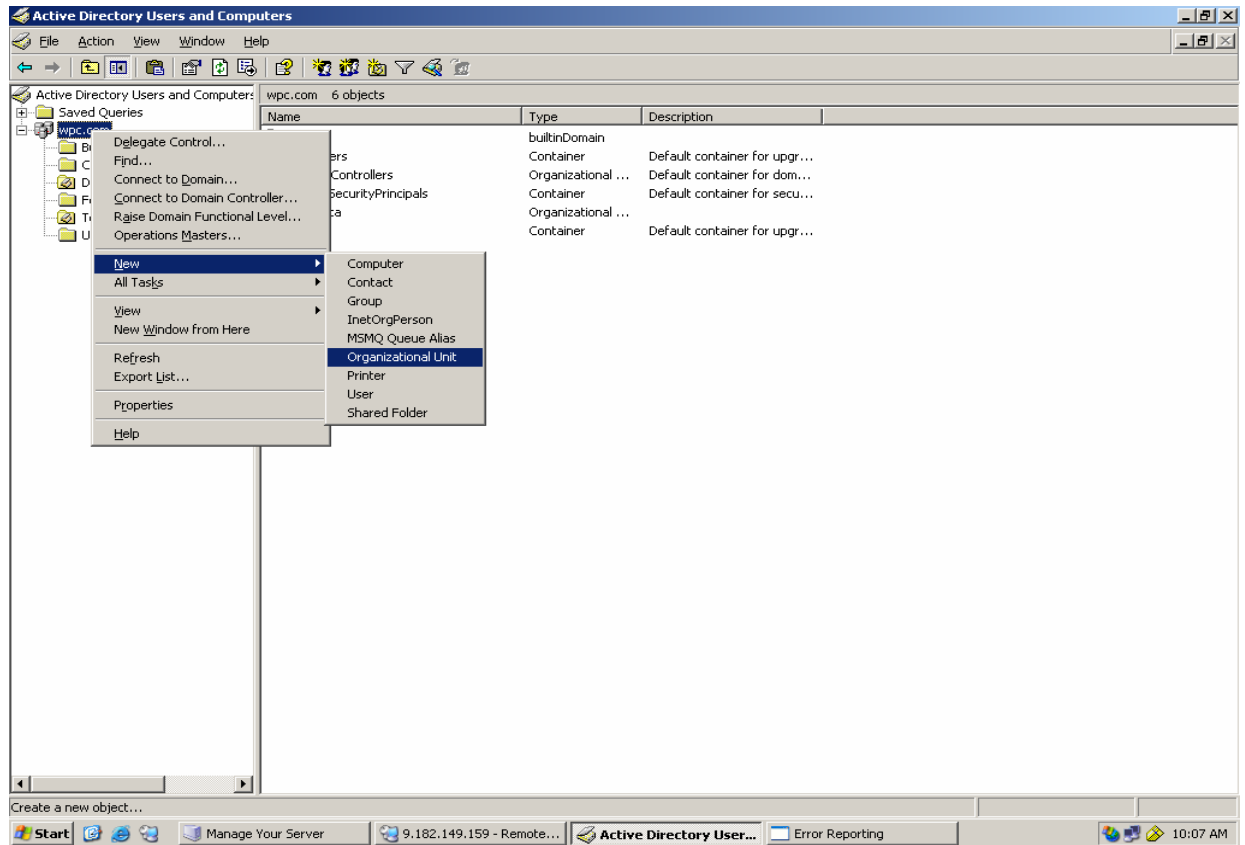
9.1 Create a new Domain

A new domain is created by creating the first domain controller. To do this, install Active Directory on a member server running Windows Server 2003 by using the Active Directory Installation Wizard. The wizard uses the information that you provide to create the domain controller and create the domain within the existing domain structure of your organization. Depending on the existing domain structure, the new domain could be the first domain in a new forest, the first domain in a new domain tree, or a child domain of an existing domain tree.

A domain controller provides the Active Directory Server's directory services to network users and computers, stores directory data, and manages user and domain interactions, including user logon processes, authentication, and directory searches.

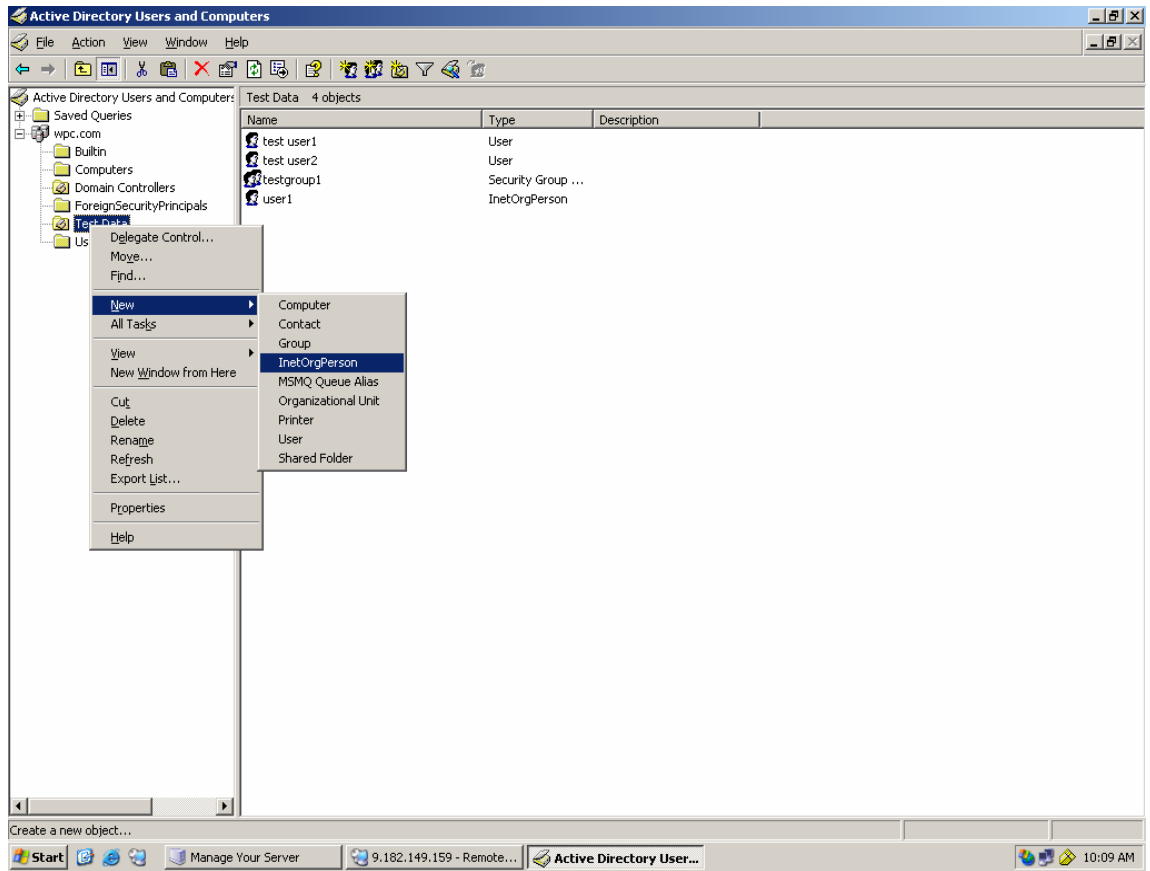
9.2 Create a new Organization

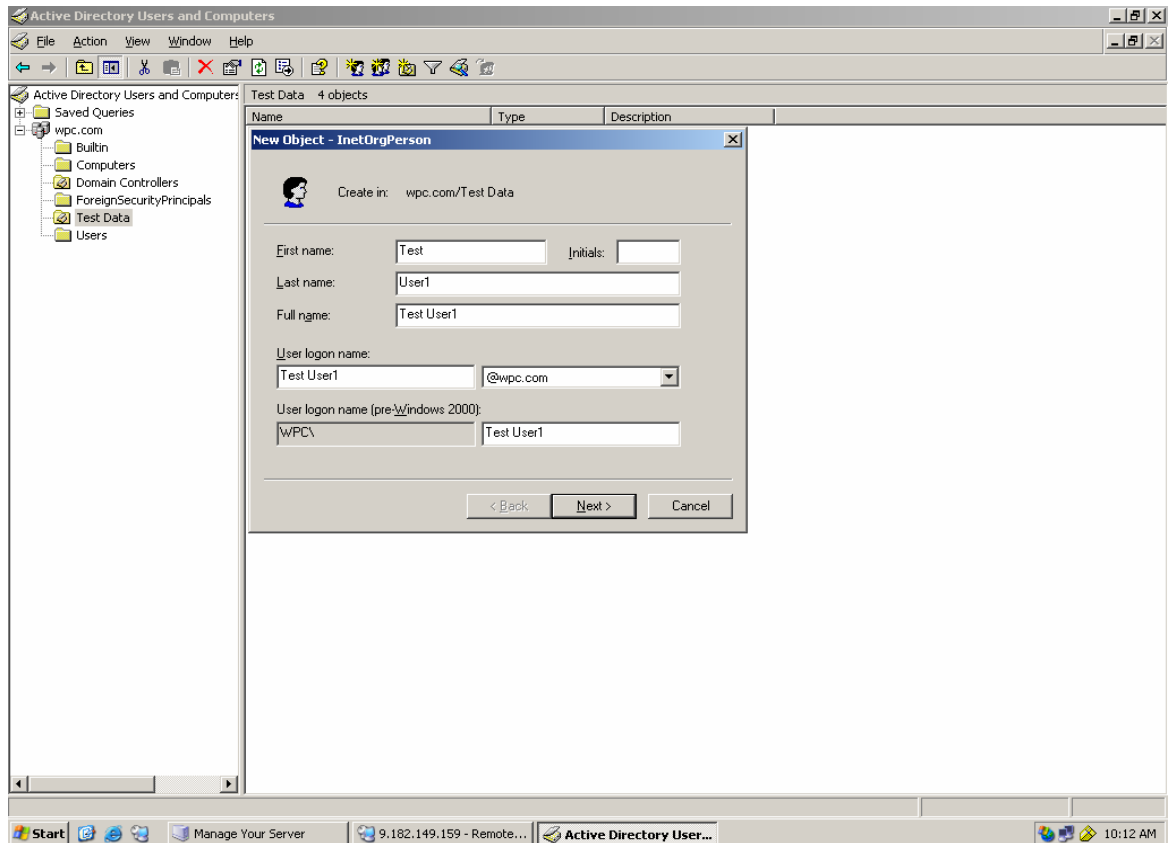
1. Create a new Organization from Microsoft Management Console (MMC) by selecting the domain and right clicking and choosing new OrganisationalUnit.
2. Fill in the name of the organization.



9.3 Create a new user

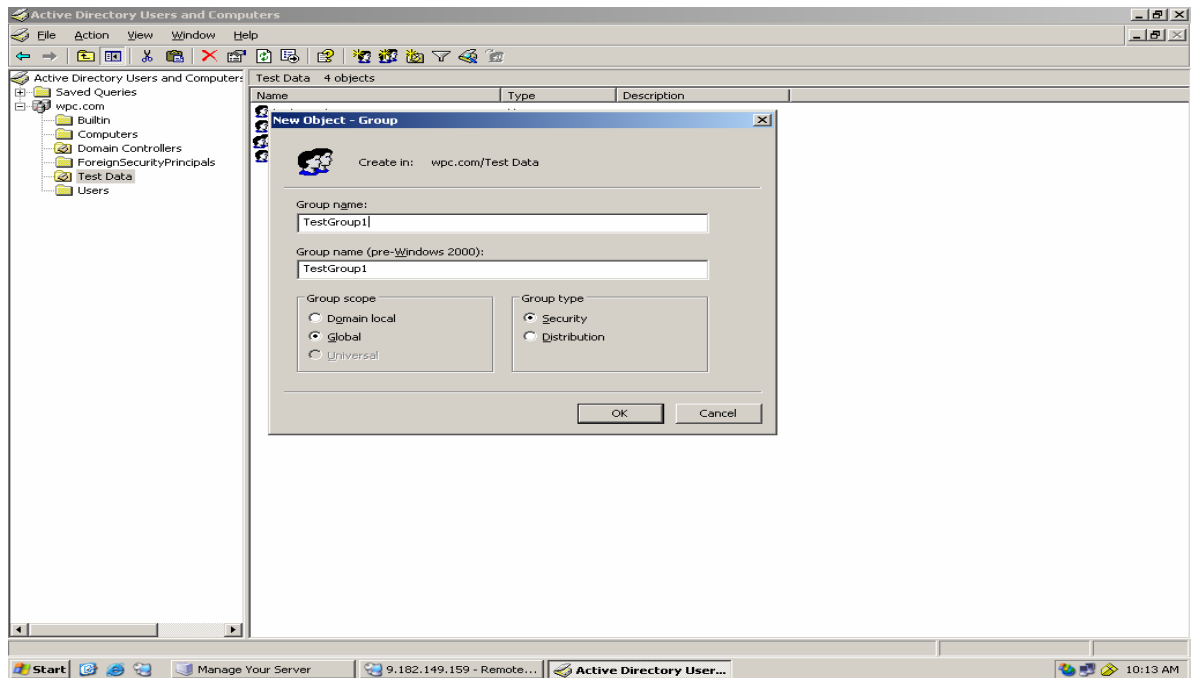
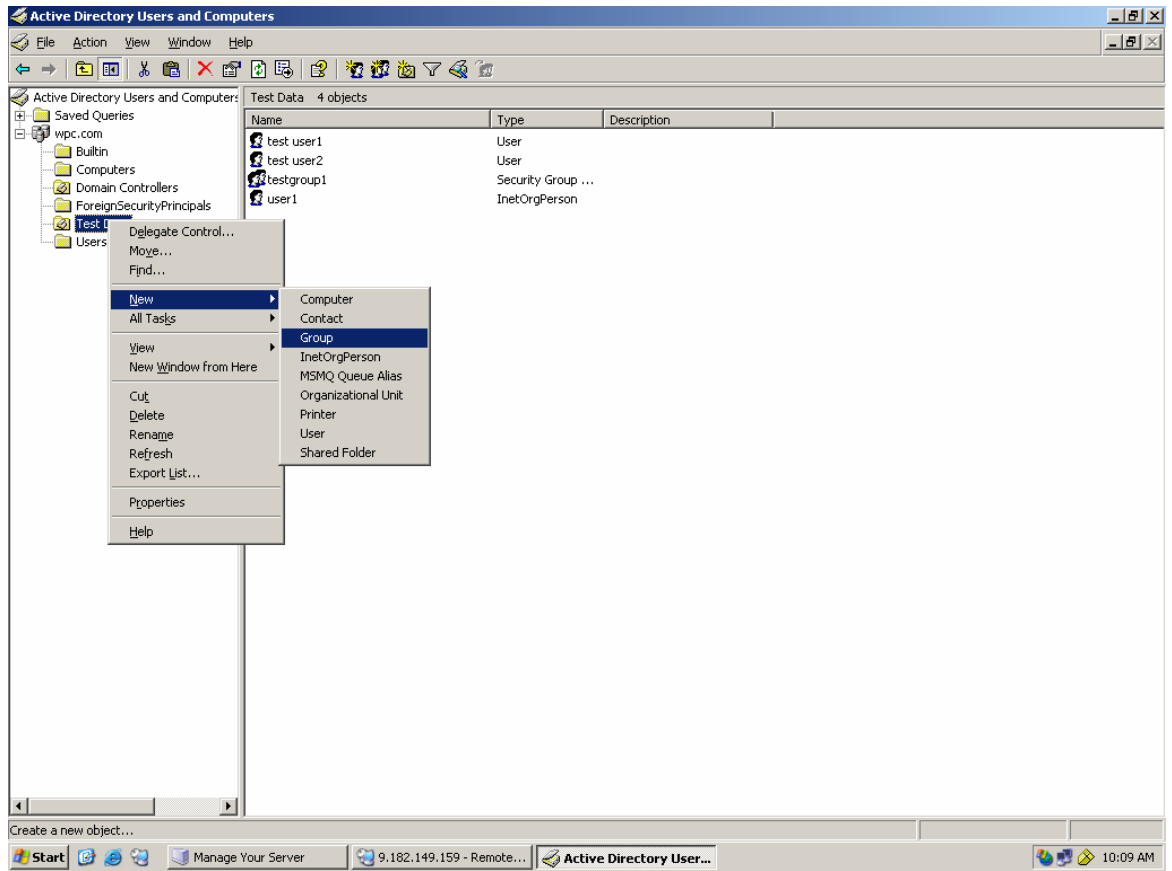
1. Create a new User from MMC by selecting the OrganizationalUnit created above and right clicking and choosing new InetOrgPerson
2. Complete the process by filling in the details.





9.4 Create a new group

1. Create a new Group from MMC by selecting the OrganizationalUnit created and right clicking and choosing new Group
2. Complete the process by filling in the details.



10. Configuration Notes:

10.1 Configuring Microsoft Active Directory for SSL access and Extract Self Signed Certificate for client

Ensure that the Active Directory domain is set up and Certificate Authority (CA) is installed on the system.

If the Certificate Authority (CA) is not installed, you can install it on your Active Directory server as follows:

1. Click **Start -> Control Panel -> Add or Remove Programs**.
2. Click **Add/Remove Windows Components** and select **Certificate Services**.
3. Follow the procedure provided to install the **Certificate Services CA**.

10.1.1 Verifying that SSL is enabled on the Active Directory server

To verify that SSL has been enabled on the Active Directory server, do the following:

1. Ensure that Windows Support Tools is installed on the Active Directory machine. The **suptools.msi** setup program is located in the \Support\Tools directory on your Windows installation CD.
2. Select **Start -> All Programs -> Windows Support Tools -> Command Prompt**. Start the **ldp** tool by typing **ldp** at the command prompt.
3. From the **ldp** window, select **Connection -> Connect** and supply the host name and port number (**636**). Also select the SSL check box.

Note:

Ensure that you type the Active Directory domain server name correctly.

If successful, a window is displayed listing information related to the Active Directory SSL connection. If the connection is unsuccessful, restart your system, and repeat this procedure.

10.1.2 Exporting the certificate from the Active Directory server

To export the CA certificate from the Active Directory server, follow these steps:

1. Log on as a Domain Administrator to the Active Directory domain server
2. Export the certificate from the Active Directory server to a file. To do so, follow these steps:

- a. Click **Start -> Control Panel -> Administrative Tools -> Certificate Authority** to open the CA Microsoft Management Console (MMC) GUI.
- b. Highlight the CA machine and right-click to select **Properties** for the CA.
- c. From General menu, click **View Certificate**.
- d. Select the **Details** view, and click the **Copy to File** button on the lower-right corner of the window.
- e. Use the Certificate Export Wizard to save the CA certificate in a file.

Note: You can save the CA certificate in either DER Encoded Binary X-509 format or Based-64 Encoded X-509 format.

10.1.3 Importing the certificate in WPC environment

- a) Get the file generated in the above steps in to the WPC environment
- b) Use the keytool command to import this in to the JVM
`keytool -import -trustcacerts -keystore cacerts -storepass changeit -noprompt -alias mycert -file <cert_file_generated>`
- c) Change the location of the cacerts file in the keystore variable in the login script. If the file that was generated in the step b was in /home/sgopan/cert/cacerts, make the value for the keyStore variable to this location.

Set the bindType variable to ssl and sslBindType to either simple or DIGEST-MD5

Note:

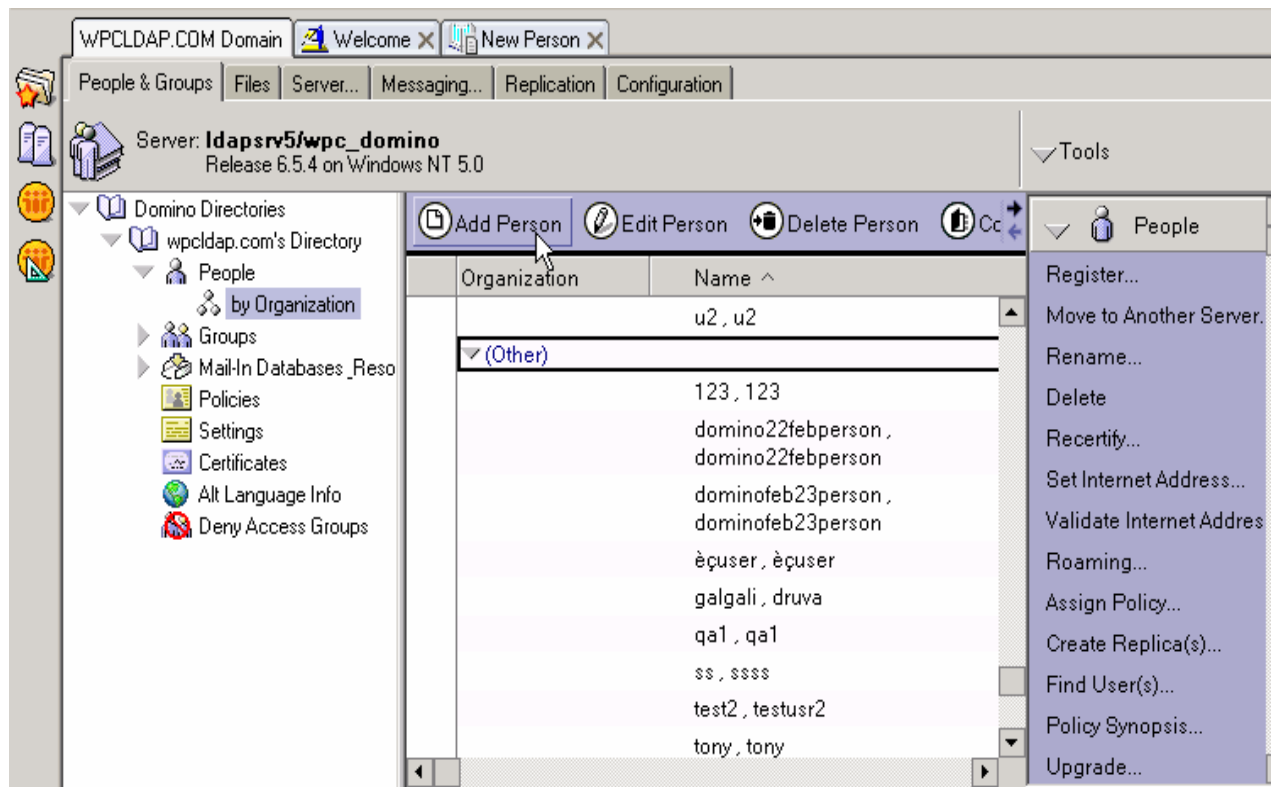
1. For DIGEST-MD5 to work, the user's password has to be stored in reversible encryption format.
2. User and Group parent DN fields are mandatory, and has to be filled up with domain names E.g. dc=wpc,dc=com is a valid DN for wpc.com domain.

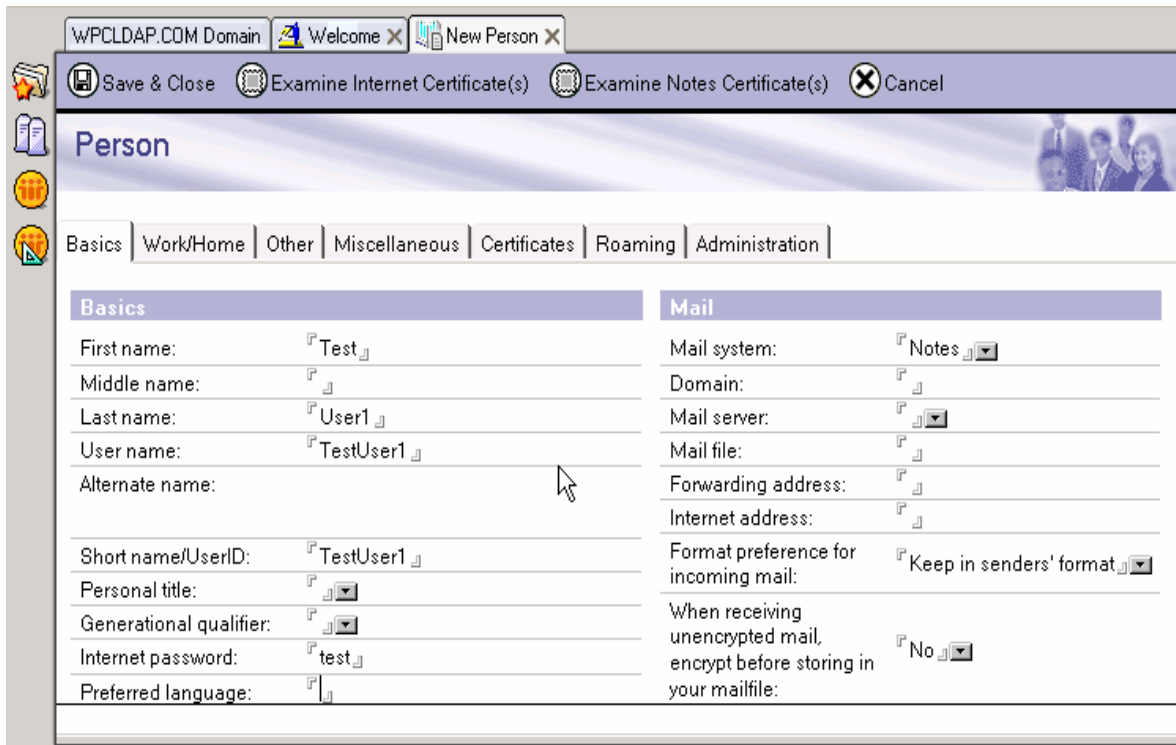
Configuring Lotus Domino Server 6.5

11. Configure LDAP schema for users and roles

11.1 Create a new Person

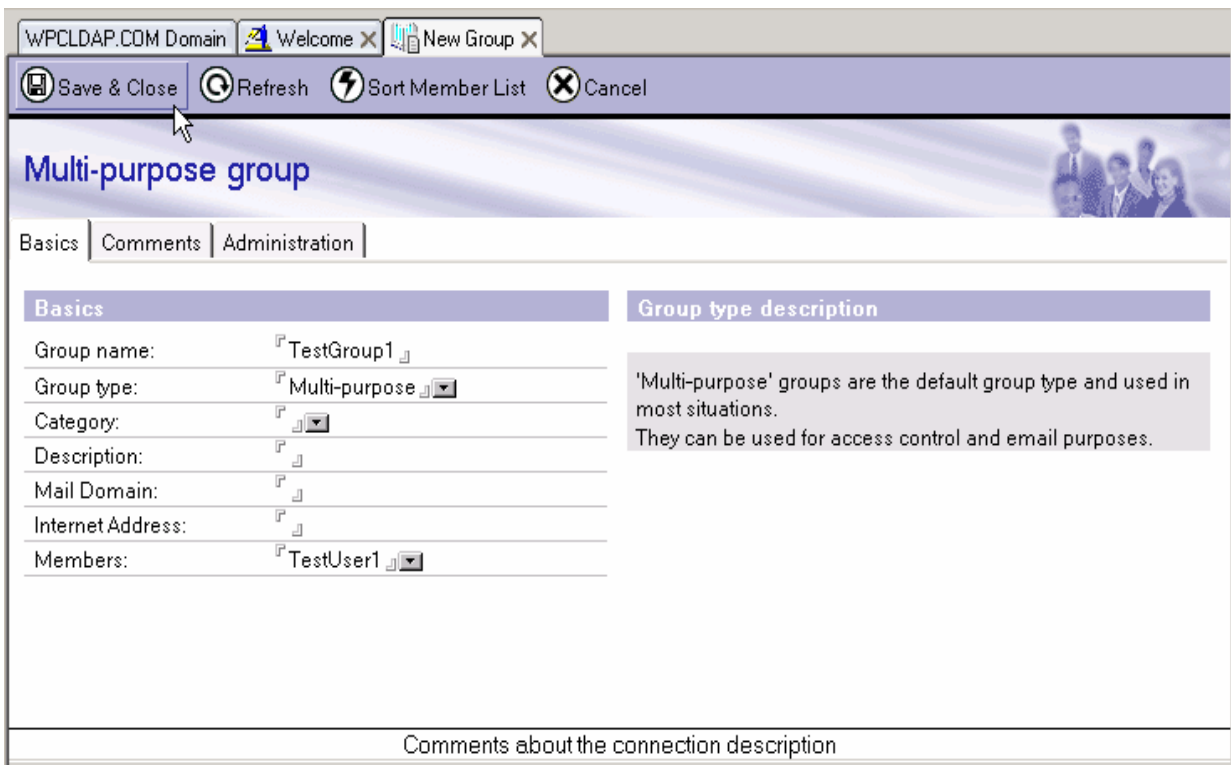
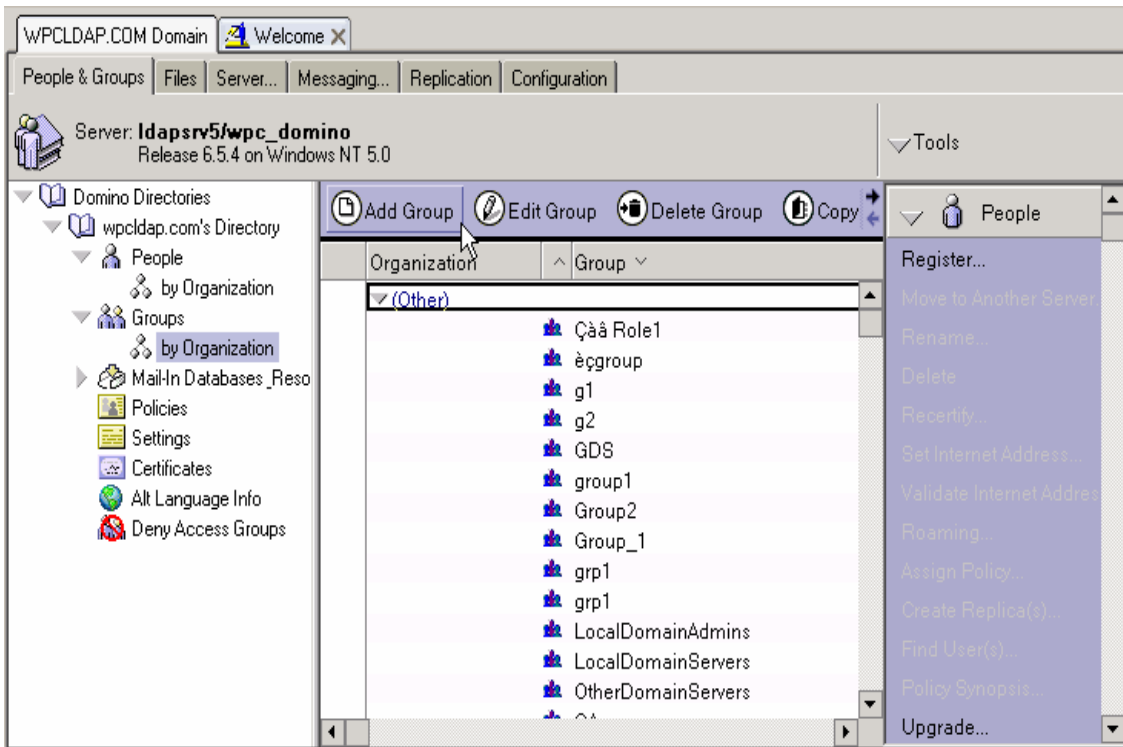
1. Create a new Person (User) using the menu path **People > Add Person**.
2. Enter details like user id first name, last name and Password.





11.2 Create a new group

4. Create a new Group from Lotus client using the menu path **Groups > Add Group**.
5. Modify the Group and associate the Users to Groups.



11.3 Configuration Notes

Password Encryption Support

Lotus notes do not support password encryption.

11.4 SSL Setup

11.4.1 Steps to set up the SSL at the server side:

- 1) Create a key ring
- 2) Create a certificate request.
- 3) Get a trial certificate or full fledged certificate from the verisign or any other CA.
- 4) Install the certificate which has been obtained from the CA. If the CA is not trusted then the certificate of CA needs to be installed prior to installation of server certificate.
- 5) Go to Admin-→port---internet port input the key ring file which contains the server certificate and key pair of server.
- 6) Go to Admin-→port---internet port---Directory- Enable the SSL.

11.4.2 SSL Setup – Client Side (WPC end)

- d) Use the server side trial certificate for importing to the client side jvm
- e) Use the ikey man/keytool command to import this in to the JVM
keytool -import -trustcacerts -keystore cacerts -storepass changeit -noprompt -alias mycert -file <cert_file_generated>
- f) Change the location of the cacerts file in the keystore variable in the login script. If the file that was generated in the step **b** was in /home/ksanjay/cert/cacerts, make the value for the keyStore variable to this location.

Use the standard script for testing the SSL and simple binding.

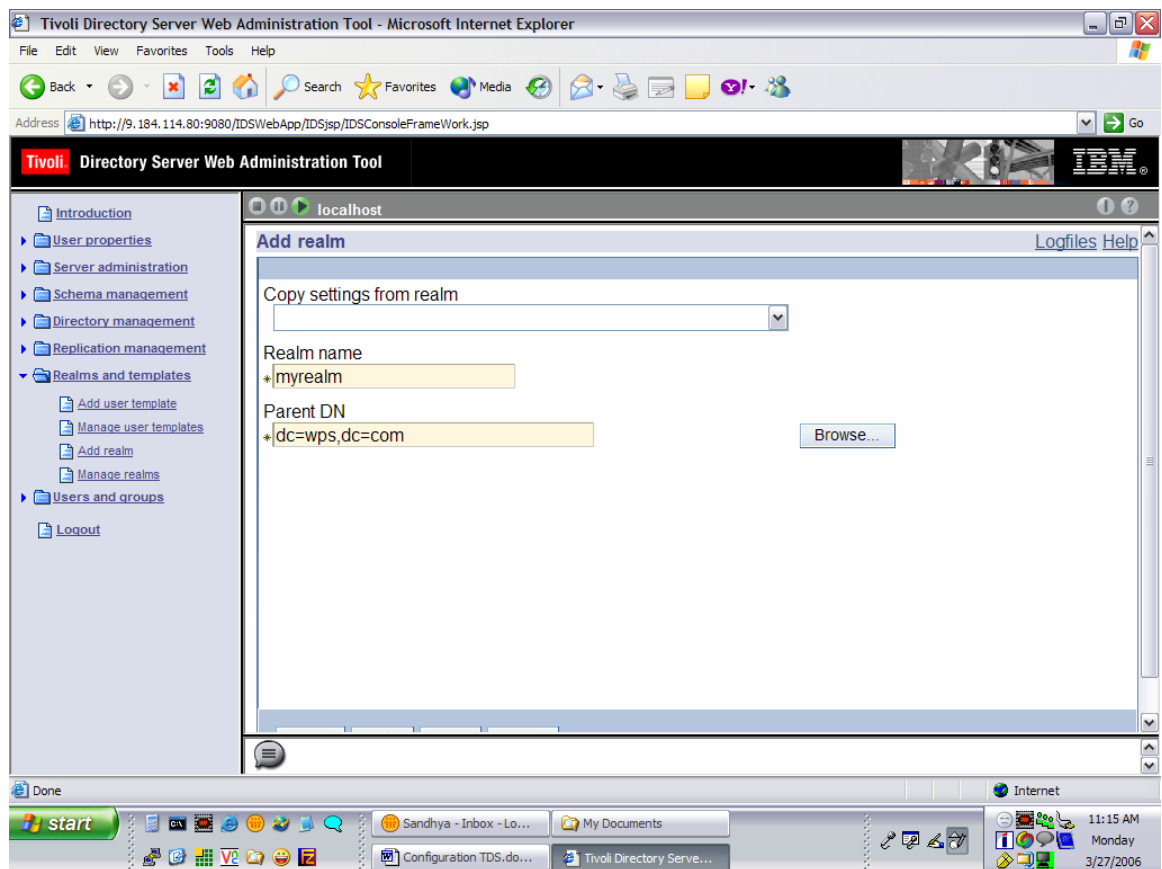
Lotus does not support SASL.

Configuring Tivoli Directory Server

12. Configure LDAP schema for users and roles

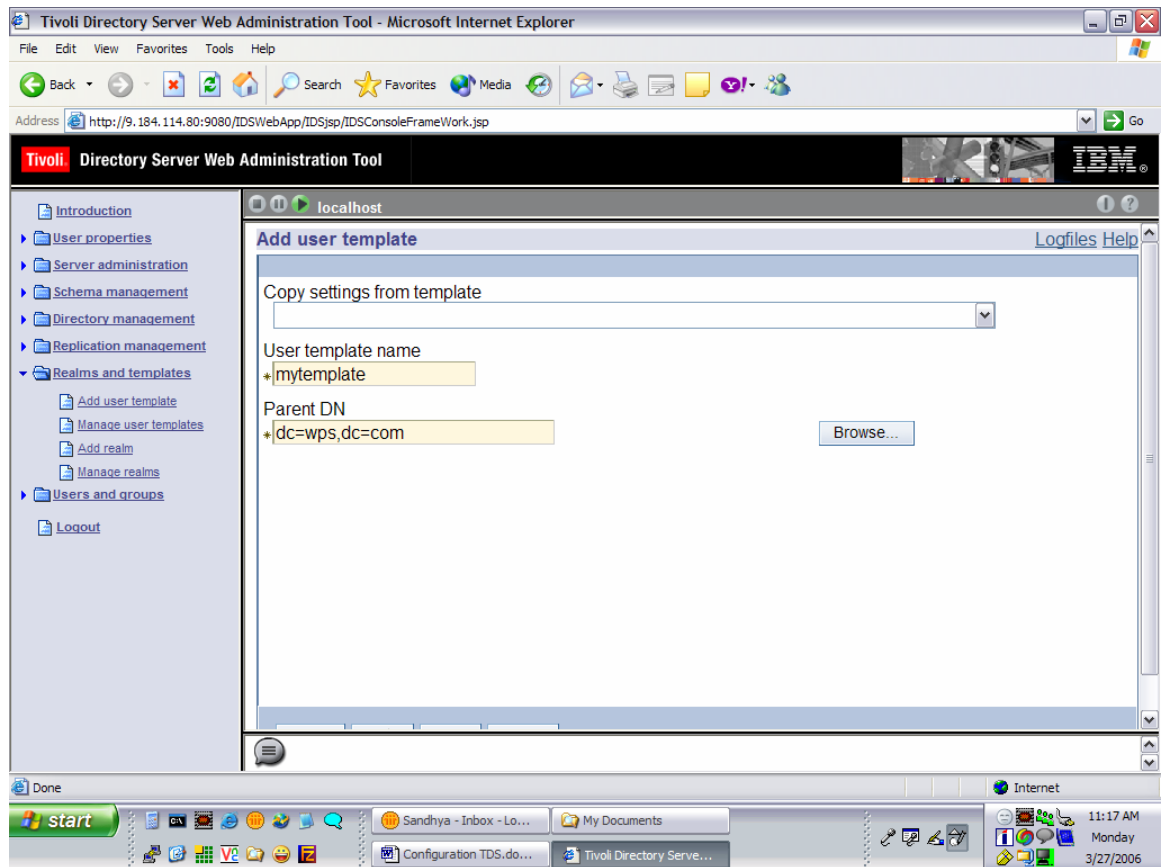
12.1 Create a new realm

- i. Create a new Realm from the IBM Tivoli Directory Server Web Administration Tool using the menu path **Realms and Templates > Add Realm**.
- ii. Complete all the required fields.
- iii. Select the Object Class *domain* as the Parent DN.



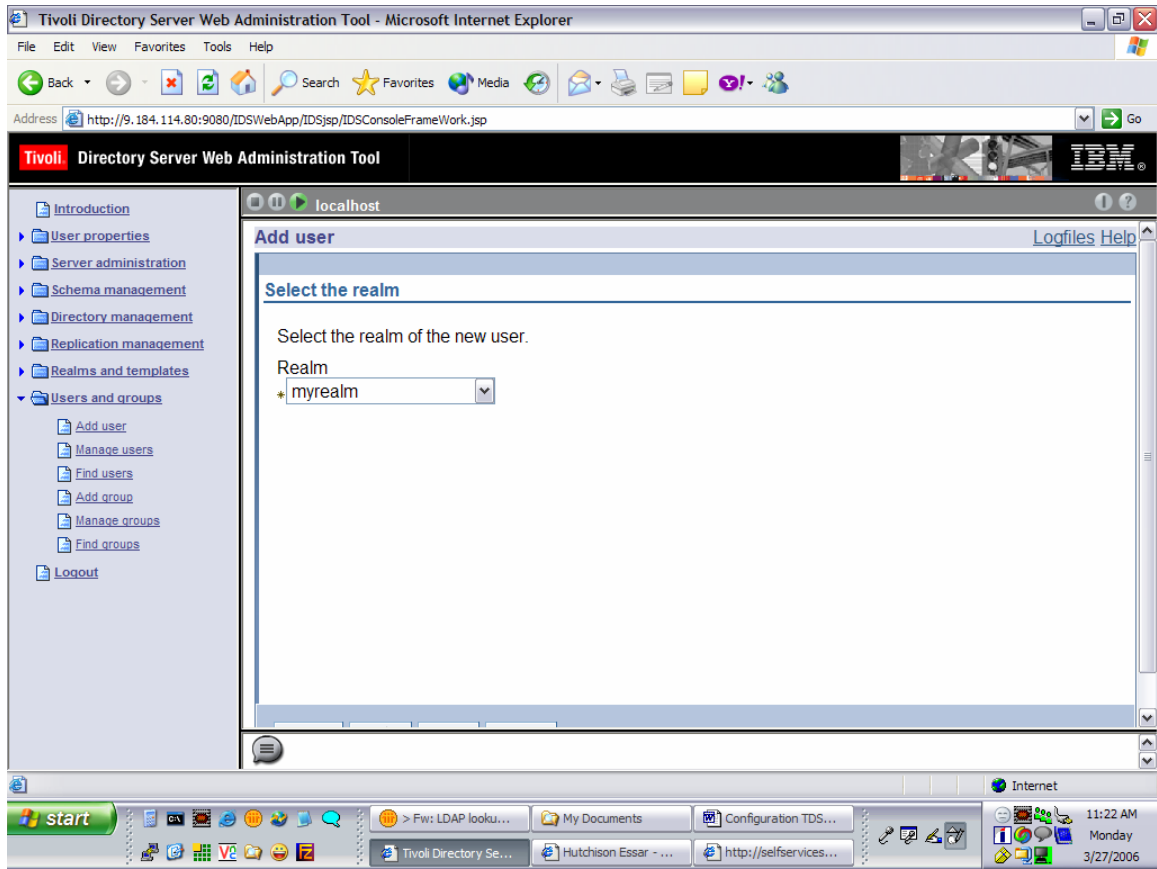
12.2 Create a new user template

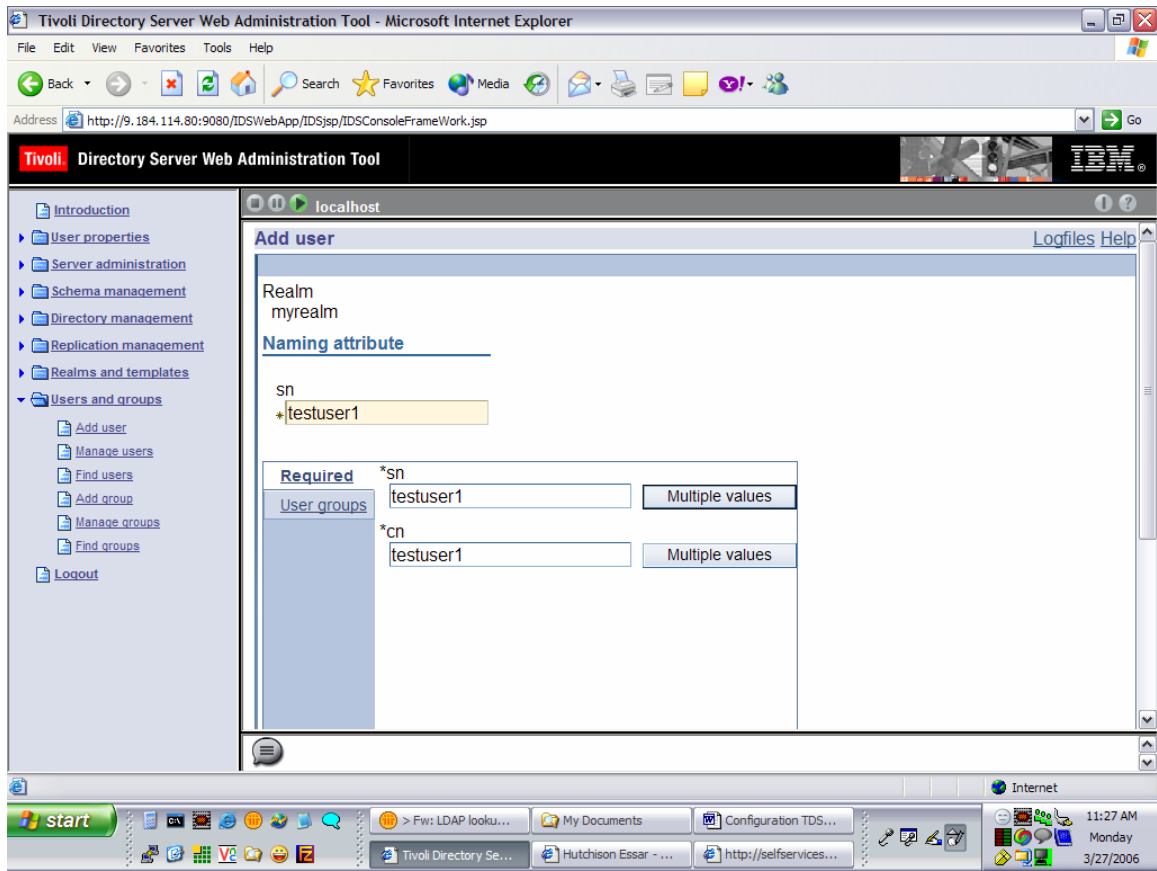
- i. Create a new User Template from the IBM Tivoli Directory Server Web Administration Tool by clicking **Realms and Templates > Add User Template**.
- ii. Key in above created realm entry as the Parent DN. Select the Structural object class as *inetOrgPerson*.
- iii. Edit the Required attribute tab to include all the following list of required attributes:
 - Cn
 - Sn
 - Uid (This is the Naming Attribute)
 - Mail
 - TelephoneNumber
 - TelexNumber
 - postalAddress
- iv. Associate this User Template with the above created Realm using the menu path Realms and Templates > Manage Realms > Edit.



12.3 Create a new user

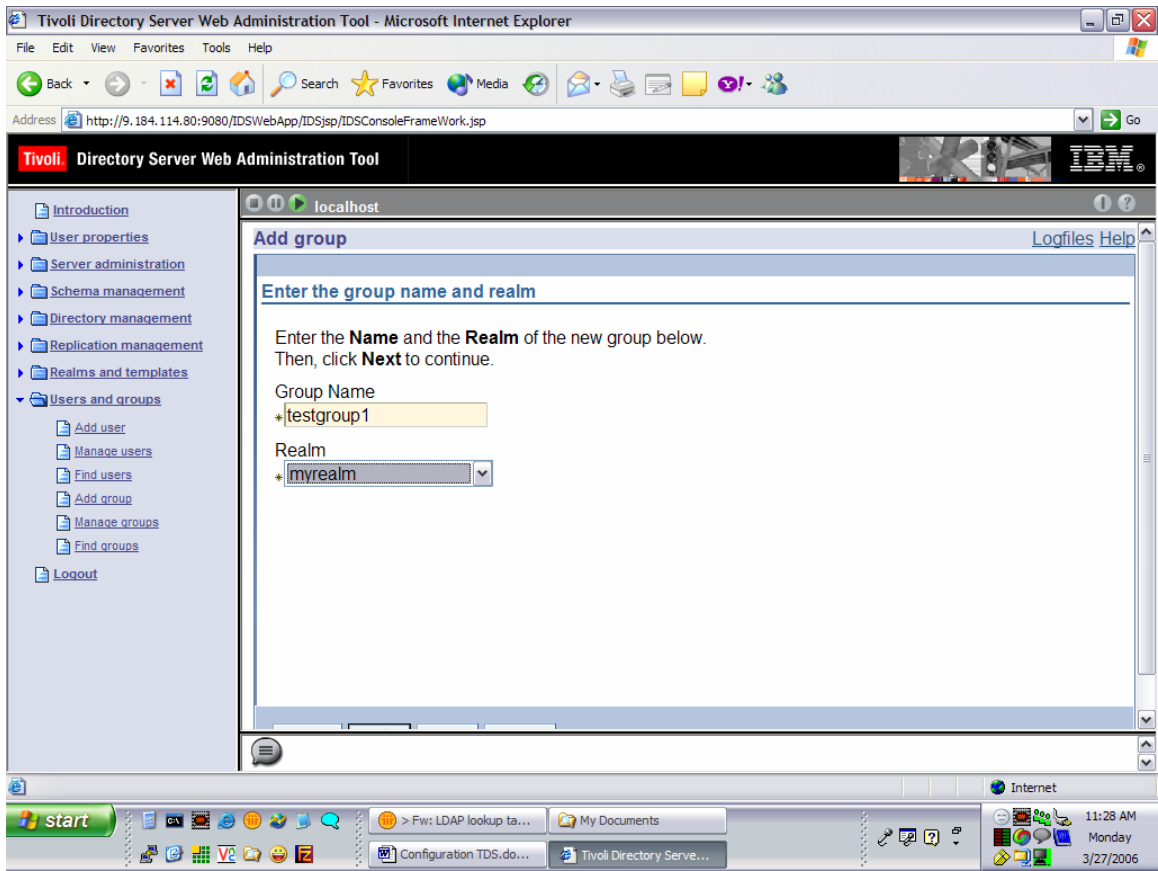
- i. Create a new User from the IBM Tivoli Directory Server Web Administration Tool using the menu path **Users and Groups > Add User**.
- ii. Select the above-created realm as Realm for this user.
- iii. Key in the "Required" attribute tab to include all the above-mentioned attributes.

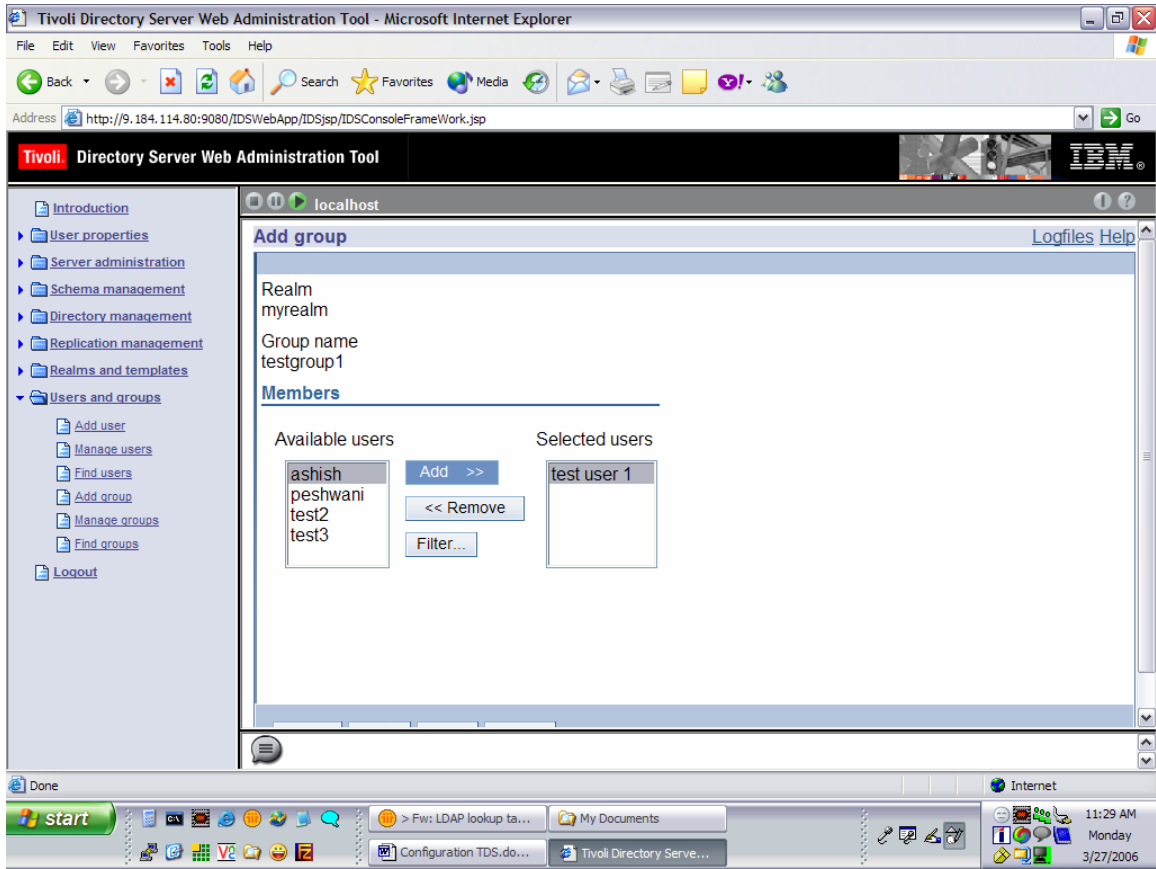




12.4 Create a new group

- i. Create a new Group from the IBM Tivoli Directory Server Web Administration Tool using the menu path **Users and Groups > Add Group**.
- ii. Select the previously created realm as Realm for this group. The Object class for the group is groupOfNames.
- iii. Associate the Users to Groups.





13. SASL - CONFIGURING DIGEST-MD5 on TDS

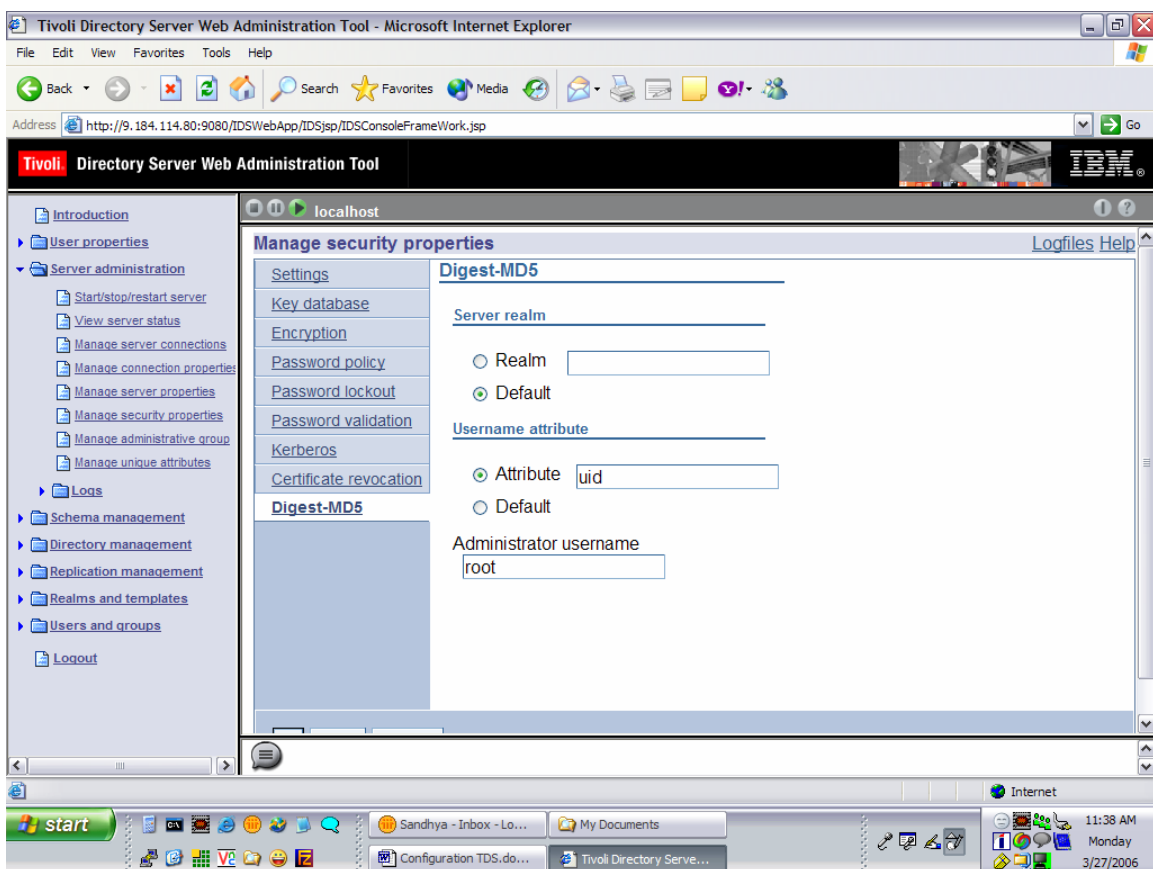
Under Server administration in the Web Administration console, expand the Manage security properties category in the navigation area of the Web Administration Tool, select the DIGEST-MD5 tab.

- a) Under Server realm, you can use the pre selected Default setting, which is the fully qualified host name of the server, or you can click Realm and type the name of the realm that you want to configure the server as.

Note:

If the `ibm-slapd Digest Realm` attribute in the configuration entry is set, the server uses that value instead of the default for the realm. In this case, the Realm button is pre selected and the realm value is displayed in the field. This realm name is used by the client to determine which user name and password to use.

- b) Under Username attribute, you can use the pre selected Default setting, which is uid, or you can click Attribute and type the name of the attribute that you want the server to use to uniquely identify the user entry during DIGEST-MD5 SASL binds.
- c) IF you are logged in as the directory administrator, under Administrator username, type the administrator username. This field cannot be edited by members of the administrative group. If the username specified on a DIGEST-MD5 SASL bind matches this string, the user is has the administrator.
- d) When you are finished, click Apply to save your changes without exiting, or click OK to apply your changes and exit, or click Cancel to exit this panel without making any changes.



13.1 Configuration Notes

1. Password Encryption Support

The DIGEST-MD5 mechanism authenticates clients by comparing a hashed value sent by the client with a hash of the user's password. However, because the mechanism must read user passwords, all users wishing to be authenticated through DIGEST-MD5 must have {CLEAR} passwords in the directory. When

storing {CLEAR} passwords in the directory, you must ensure that access to password values is properly restricted through ACIs. You may wish to further protect {CLEAR} passwords by configuring attribute encryption in that suffix, as described in Encrypting Attribute Values.

Refer - <http://docs.sun.com/source/817-7613/ssl.html#wp14354>

2. Client Side Configuration

The hostname of the Tivoli Server should be entered in the hosts file of the Server.

13.2 SSL Setup

To enable security with server authentication, you can follow one of the given steps:

i. SSL Setup – Certificate from a Certifying Authority (CA) Self Signed Certificate

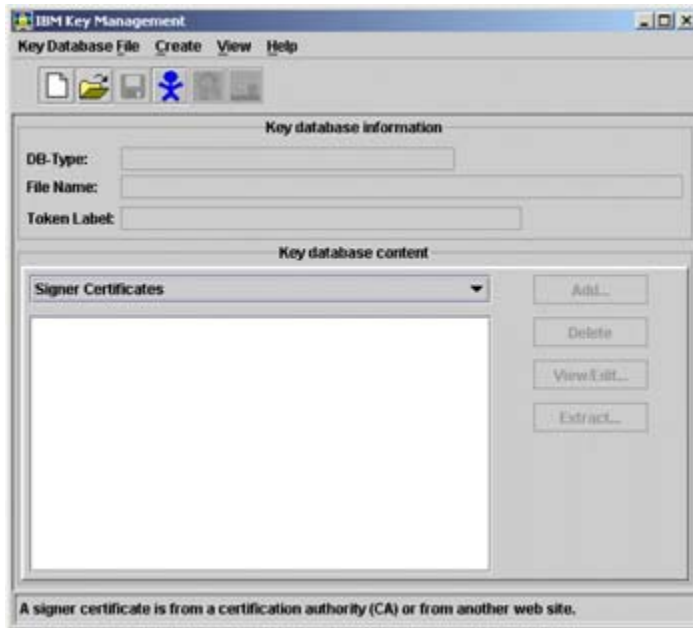
Create a public/private key pair and obtain and store a certificate from one of the predefined (well-known) Certificate Authorities. This procedure requires less setup because the key ring file is preconfigured with the CA root certificates required to identify the CAs from whom the certificate is issued.

ii. SSL Setup – Self Signed Certificate

To enable SSL security we can create a self-signed root certificate and store the certificate in the database and class files. To ensure maximum security for your site, you should only use a self-signed certificate for server authentication until you receive a CA-issued certificate.

You can use the ikmgui (IBM Key Management GUI) utility to create a self-signed certificate to enable SSL sessions between clients and servers. The steps are essentially the same except that, in this case, you are the CA for the keys you will be creating, and you will be creating your own root certificate. The advantage of using this type of certificate is a quick start, it is free, and you have no dependencies on other organizations. The drawback, on the other hand, is that each client or server using this kind of certificate needs to have the new root certificate imported, which may impose some administrative burden.

1. Create server key database (.kdb file).
 - a. Click **Key Database File**



b. Click New, from that dropdown that appears in point a. above.

c. On the dialog window that pops up, select **CMS key database** file in the Key database type selection list and then type in the name and location of the key database file to be created. This file has an extension of .kdb, as, for example, in ldap_key.kdb. Then, click **OK** to close the dialog panel.

d. A new dialog pops up that requests your input for a password for the key database file, an optional expiration time, and whether or not the password is to be stashed to a file. Enter a password, an optional expiration time, and make sure that you check the check box next to Stash the password to a file? otherwise, you have to enter the password manually in the configuration file of the directory server. Click **OK** to close

this dialog. The password is then encrypted and stored in a file with the same name as the key database file but with an extension of .sth.

2. Create a self-signed certificate.

a. Select **New Self-Signed Certificate...** from the Create pull-down menu in the main window. In the dialog window that shows up, you will have to fill in the following information:

- Key label (a clear, descriptive label for the certificate)
- Key Version (normally X.509 V3, unless you have reasons for other versions)
- Key size (512 or 1024, depending upon security requirements and country version of the ikmGUI utility)
- Common name

- Organization and other pertinent information to identify the owner of the certificate
- Validity period in days

3. Click **OK** to create the request. The .arm file so created contains the certificate request.

4. From the certificate just created above, you need to extract the root certificate that is necessary for other communication partners (clients and/or servers) to recognize the newly created certificate. Here are the steps for exporting the root certificate:

- a. Select the new certificate's entry in the Personal Certificate list and click **Extract Certificate** at the bottom right on the main window.
- b. Select **Base64-encoded ASCII data** from the Data type list and enter a file name (with a .arm extension) and a location (directory) for the new root certificate to be exported to. Then click **OK** to export the root certificate. (If
You have now created a file that holds your own root certificate. This must be imported to all communication partners that will connect to the server through SSL.

5. Use the following steps for importing the new root certificate into others' key database (using ikmgui):

- a. Make sure that the certificate extracted above, in the previous step, is made available to all the communication partners. You can transfer the file using ftp or a diskette or any other suitable media.
- b. Invoke the ikmgui utility on the receiving system.
- c. If not already done, create a key database file (see first step above for creating a self-signed certificate).
- d. In the Key database content portion of the window, select Signer Certificates from the selection list and click Add... on the right.
- e. Select Base64-encoded ASCII data from the Data type list and type the Certificate file name and location into the appropriate fields. Then, click **OK** to import the certificate.
- f. On the upcoming dialog, supply a label for this certificate and click **OK**.

The steps as described above need to be done on each machine that will communicate using this certificate with the machine from which the certificate was exported.

Each LDAP server should have its own certificate. Sharing certificates across multiple LDAP servers is not recommended. By using different certificates and

private keys for each server, your security exposure is minimized should a keyring file for one of the servers be compromised.

13.3 SSL Setup – Client Side (WPC end)

- a. Get the .arm file generated in the above steps in to the WPC environment
- b. Use the keytool command to import this in to the JVM
 - i. `keytool -import -trustcacerts -keystore cacerts -storepass changeit -noprompt -alias mycert -file <cert_file_generated>`
- c. Make an entry in hosts file to point to the SSL Tivoli instance.
- d. Change the location of the cacerts file in the keystore variable in the login script. If the file that was generated in the step2 was in /home/sgopan/cert/cacerts, make the value for the keyStore variable to this location.

Set the bindType variable to ssl and sslBindType to either simple or DIGEST-MD5.

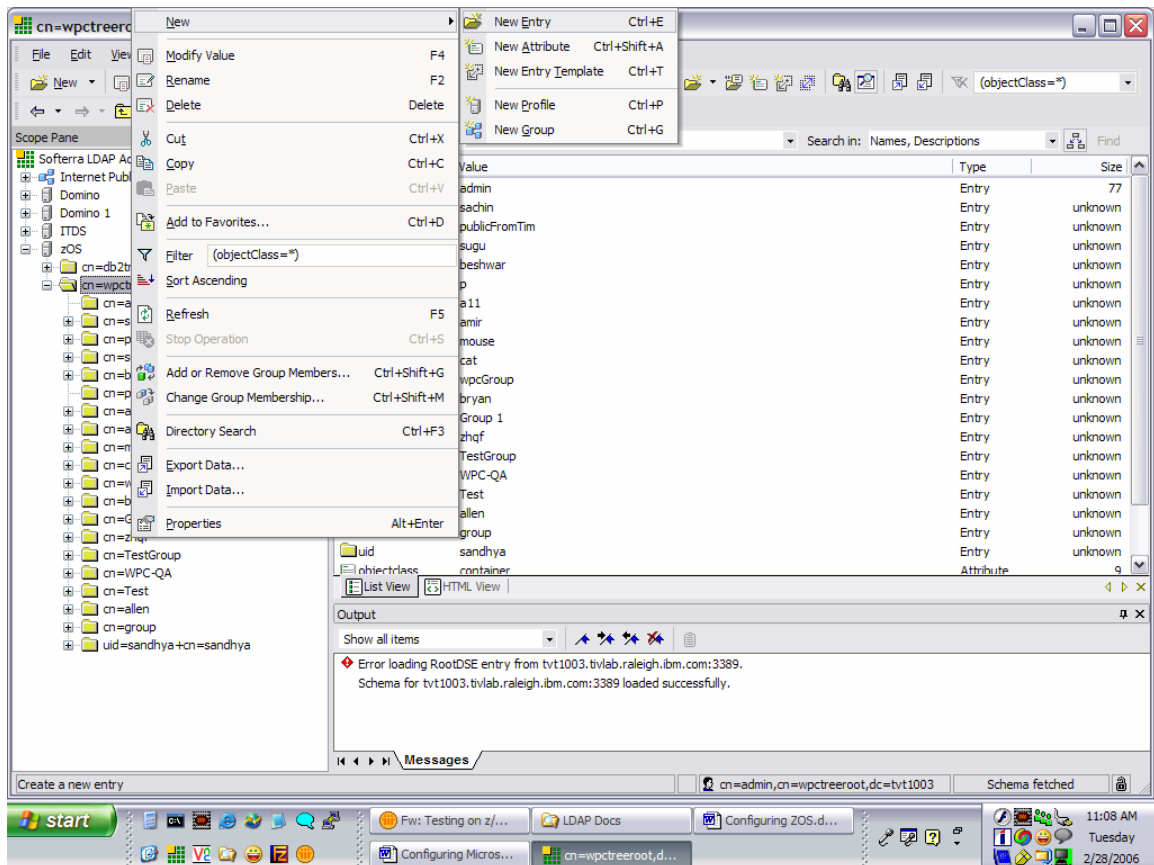
Configuring Z/OS

14. Creating Users and Groups:

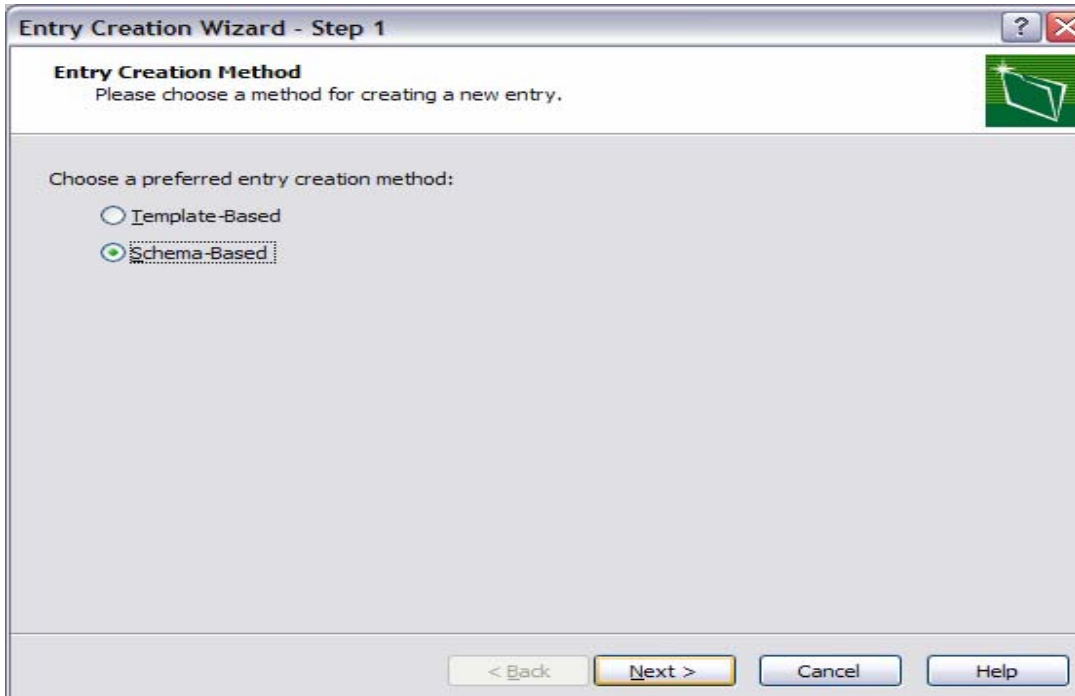
Use Softerra LDAP Administrator 3.3.1 to connect to the Z/OS server.

14.1 Create a new user:

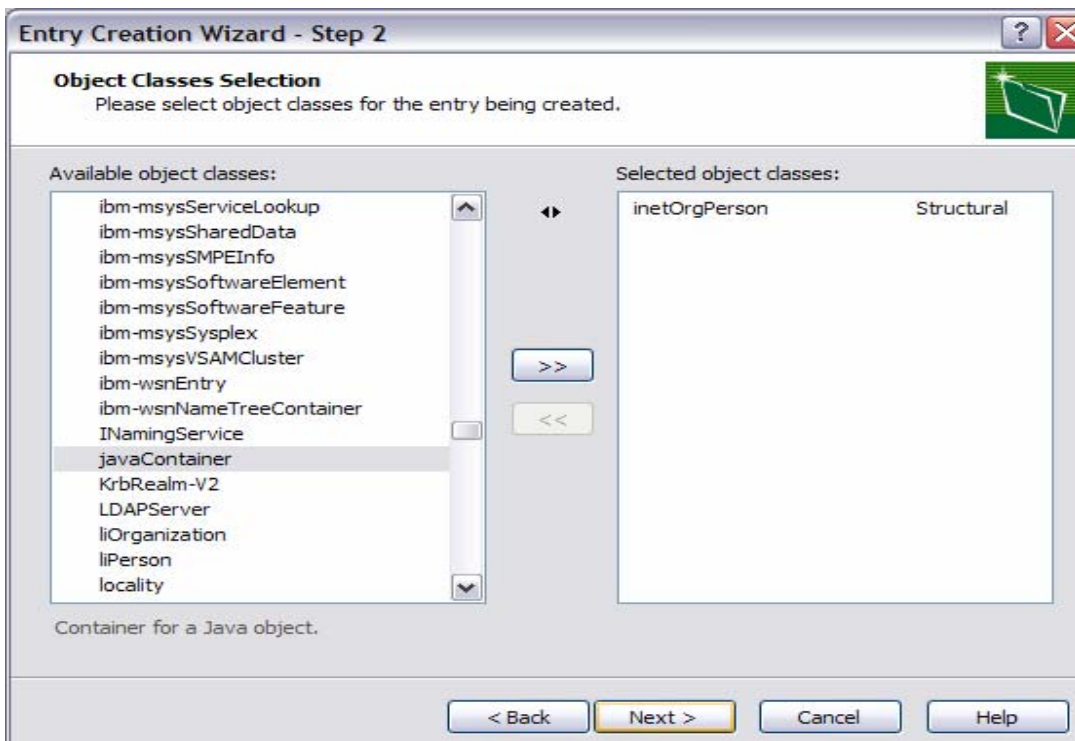
1. Create a new user through LDAP Administrator by selecting a container (say cn=wpcreot) and right clicking and choosing New -> New entry.



2. Choose the entry creation method as “Schema based”, in the Entry Creation Wizard-Step 1.



3. Select inetOrgPerson in the Object class selections of Entry Creation Wizard-Step2.



4. Enter the RDN as cn=testuser1 in the Entry Creation Wizard-step3.

The screenshot shows the 'Entry Creation Wizard - Step 3' dialog box. The title bar reads 'Entry Creation Wizard - Step 3'. The main heading is 'Entry RDN' with the instruction 'Please specify an RDN for the entry.' Below this, a sub-instruction says 'Please specify the entry RDN. You can specify a multi-valued RDN by clicking on the 'Add Value' link.' There are two input fields: 'Type:' with a dropdown menu showing 'cn' and 'Value:' with a text box containing 'testuser1'. An 'Add Value' link is positioned below the 'Type:' field. At the bottom left, an 'RDN Preview' shows 'cn=testuser1'. At the bottom right, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

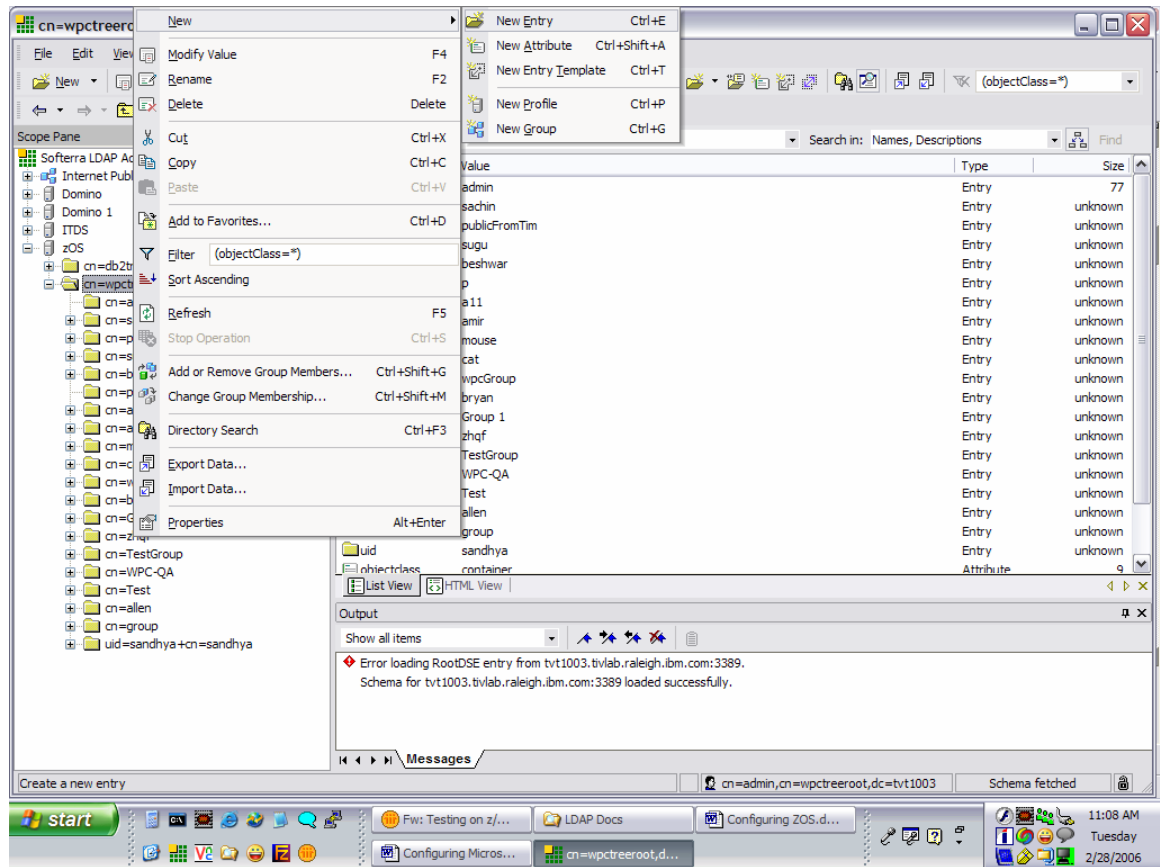
5. Add values to the attributes like sn, uid, user password and more in the Entry creation Wizard-Step4 and click finish.

The screenshot shows the 'Entry Creation Wizard - Step 4' dialog box. The title bar reads 'Entry Creation Wizard - Step 4'. The main heading is 'Adding Attributes and Their Values' with the instruction 'Please select attributes for the new entry and specify their values.' Below this, a sub-instruction says 'Please fill in attribute values:'. A table lists various attributes with their corresponding values. The 'cn' attribute has the value 'testuser 1' and the 'objectclass' attribute has the value 'inetOrgPerson'. The 'sn' attribute also has the value 'testuser 1'. Other attributes listed include 'audio', 'businessCategory', 'carLicense', 'departmentNumber', 'description', 'destinationIndicator', 'displayName', 'employeeNumber', 'employeeType', 'facsimileTelephoneNum...', 'givenName', 'homePhone', and 'homePostalAddress'. To the right of the table are buttons for 'Add Attribute', 'Remove Attribute', 'Add Value', and 'Remove Value'. At the bottom right, there is a 'Save Template...' button. At the bottom left, there is a checkbox labeled 'Don't close the wizard after the entry has been added'. At the bottom right, there are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'.

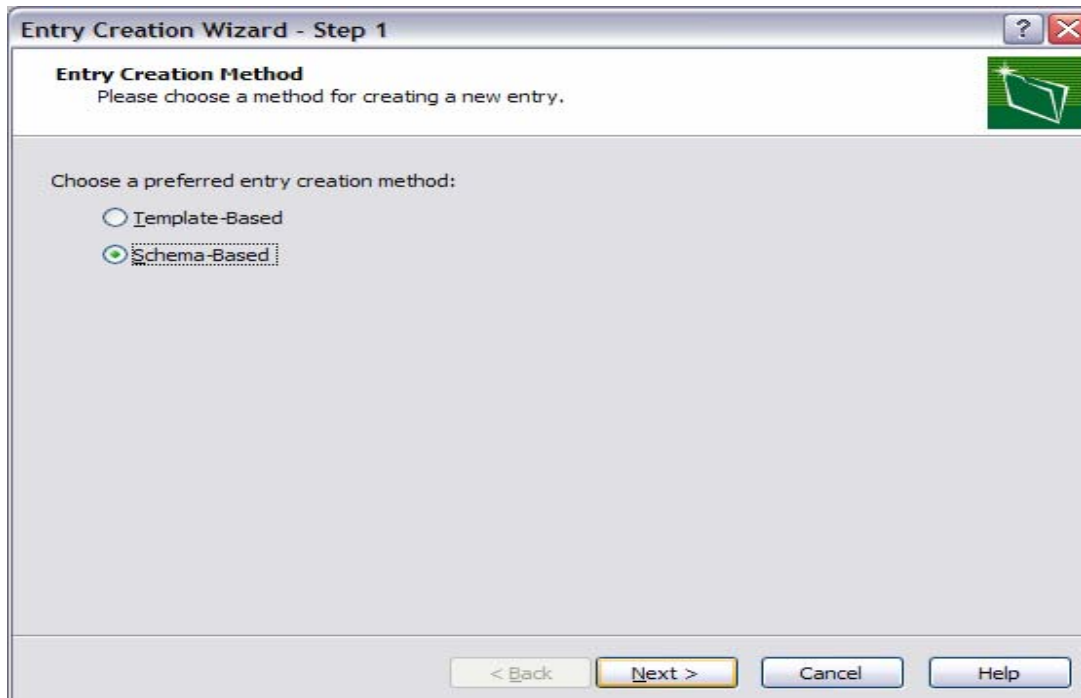
Attribute	Value
cn	testuser 1
objectclass	inetOrgPerson
sn	testuser 1
audio	
businessCategory	
carLicense	
departmentNumber	
description	
destinationIndicator	
displayName	
employeeNumber	
employeeType	
facsimileTelephoneNum...	
givenName	
homePhone	
homePostalAddress	

14.2 Create a new Group:

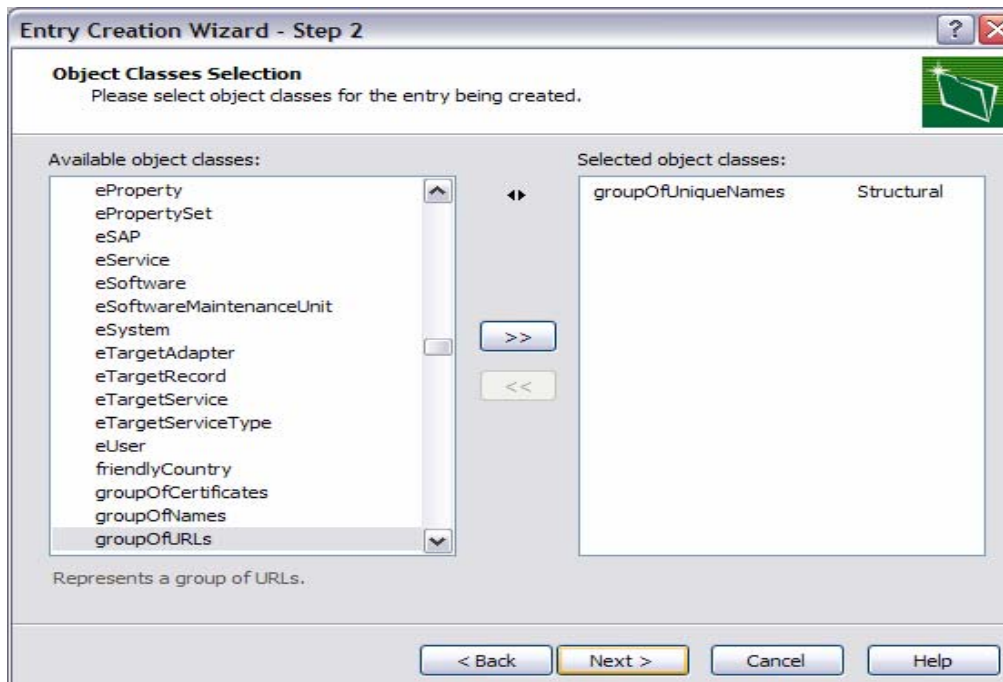
1. Create a new group through LDAP Administrator by selecting a container (say cn=wpcreot) and right clicking and choosing New -> New entry.



2. Choose the entry creation method as "Schema based", in the Entry Creation Wizard-Step 1.



3. Select groupOfUniqueNames in the Object class selections of Entry Creation Wizard-Step2.



1. Enter the RDN as cn=testgroup1 in the Entry Creation Wizard-step3.

Entry RDN
Please specify an RDN for the entry.

Please specify the entry RDN. You can specify a multi-valued RDN by clicking on the 'Add Value' link.

Type: **cn** = Value: **testgroup1**

[Add Value](#)

RDN Preview: cn=testgroup1

< Back Next > Cancel Help

5. Enter the Unique member of the group and click finish.

Adding Attributes and Their Values
Please select attributes for the new entry and specify their values.

Please fill in attribute values:

cn	testgroup1
objectclass	groupOfUniqueNames
uniqueMember	testuser1
businessCategory	
description	
o	
ou	
owner	
seeAlso	

Buttons: Add Attribute, Remove Attribute, Add Value, Remove Value, Save Template...

Don't close the wizard after the entry has been added

< Back Finish Cancel Help

Note:

- For SASL bind, user's password must be clear passwords.
- Uid field must be populated with a unique value across the sub tree for SASL to work.
- For SASL only the principal has to be supplied in the lookup table.