Avaya CM Login with Windows Active Directory Services

Objective 2

Installing Active Directory Services on a Windows 2003 Server 2

Installing Windows Service for UNIX on Windows 2003 Active Directory Server 6

Creating Profiles and Groups in the Active Directory for CM Login profiles 10

Creating and Configuring Users in Active Directory for CM Logins 15

Installing and Configuring Softerra LDAP Browser 20

Verifying Active Directory Schema for SFU Using LDAP Browser 25

Preparing the CM for LDAP Authentication 26

Configuring the Avaya CM for LDAP Active Directory User Authentication 27

Logging into the CM using Active Directory Users 33

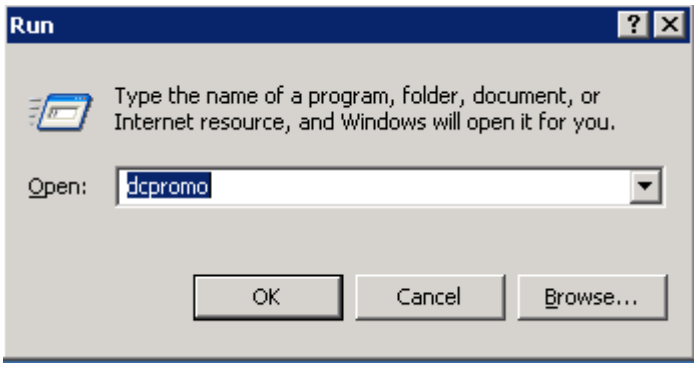
Objective

The purpose of this document is to describe how to log in to the Avaya Communication Manager 5.X using User account logins in a Windows 2003 Active Directory Server. This document will cover how to install and configure Active Directory Services on a Windows 2003 Server, install and configure Services for UNIX for Active Directory, install and configure an LDAP Browser (i am using Softerra LDAP Browser which is free), create and manage CM Users and Admins, configuring User Profiles in the Avaya CM to provide granular control to the CM User base, configuring the Avaya CM to utilize Active Directory credentials as a first method of authentication and then using local user authentication.

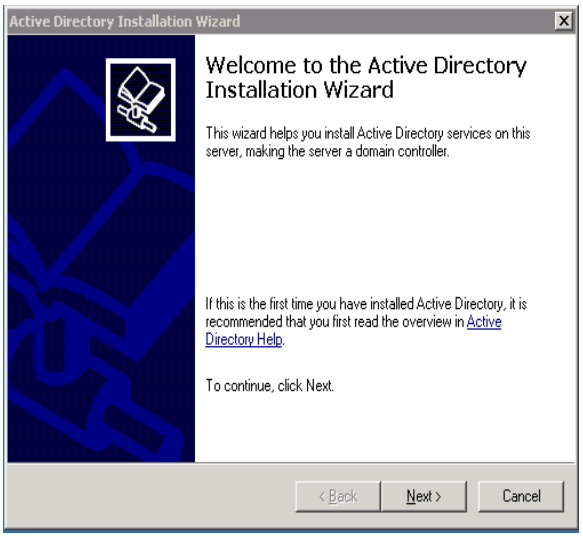
Installing Active Directory Services on a Windows 2003 Server

If you already have an Active Directory Server, please skip to the next section.

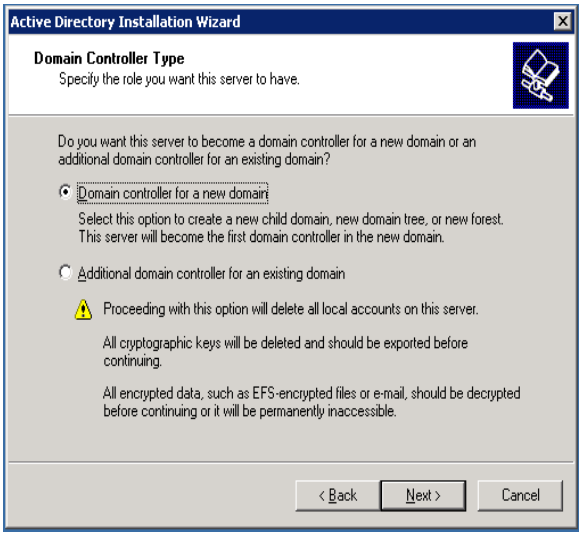
For the purpose of this document, we will assume that we are creating a domain controller for a brand new domain (TESTDOMAIN). If you already have a domain controller, you can simply install Active Directory Services on the same or another server without creating a brand new domain. On the Windows 2003 Server, open **START > RUN** and type **dcpromo** in the Open Window and hit OK (you may need to insert the Windows 2003 Server CD in the CDROM Drive or ISO MOUNT to the Server)

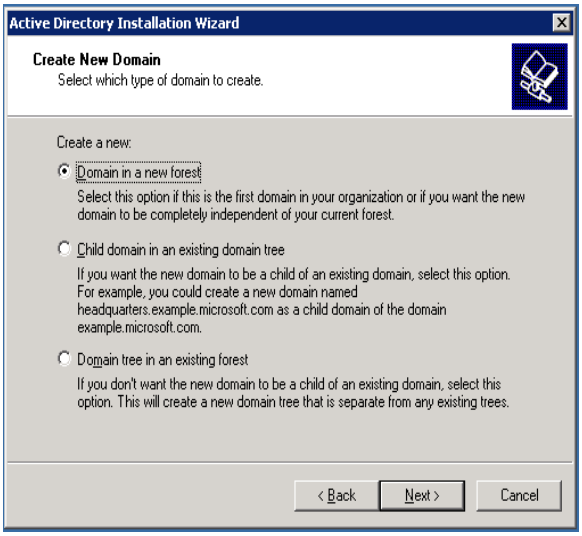


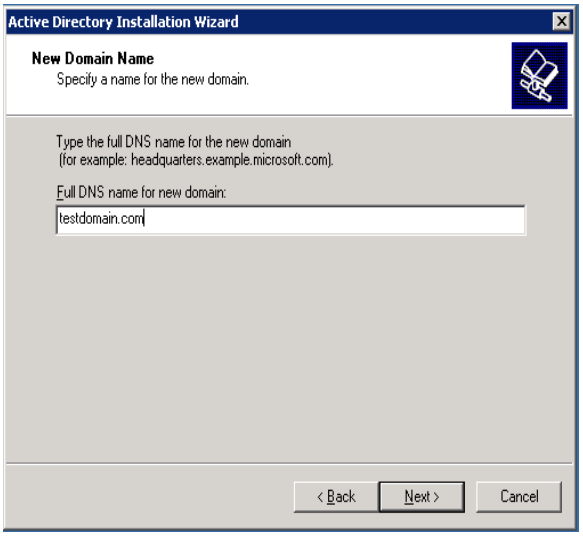
Go through the Active Directory installation wizard as follows:

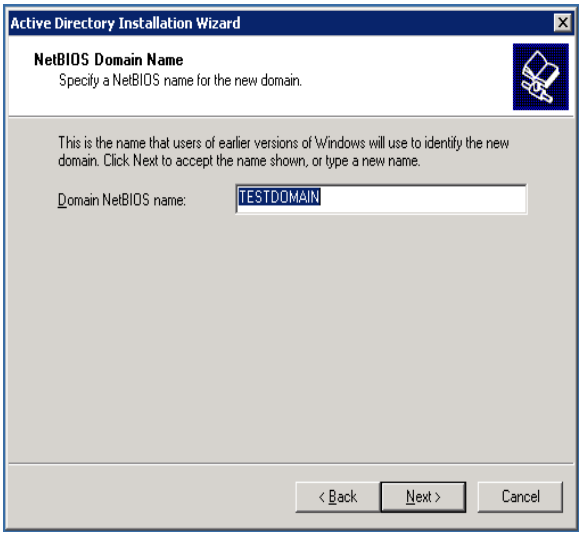

Active Directory Installation Wizard
Welcome to the Active Directory Installation Wizard
This wizard helps you install Active Directory services on this server, making the server a domain controller.
If this is the first time you have installed Active Directory, it is recommended that you first read the overview in Active Directory Help.
To continue, click Next.
< Back
Next >
Cancel

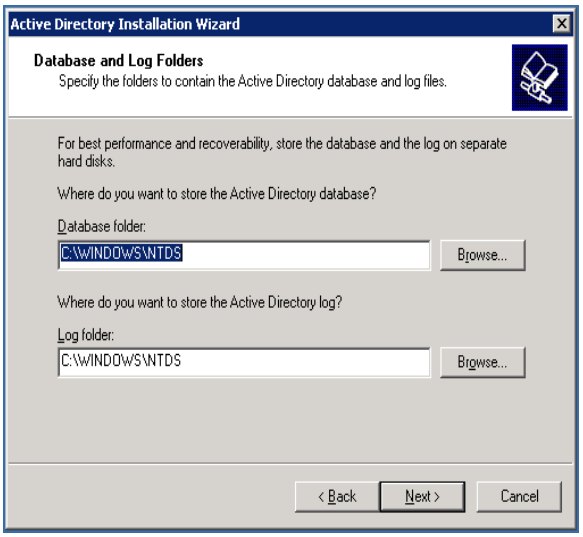

Active Directory Installation Wizard
Operating System Compatibility
Improved security settings in Windows Server 2003 affect older versions of Windows.
Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.
Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 or earlier, do not meet these requirements. Similarly, some non-Windows systems, including Apple Mac OS X and SAMBA clients, might not meet these requirements.
For more information, see Compatibility Help.
< Back
Next >
Cancel

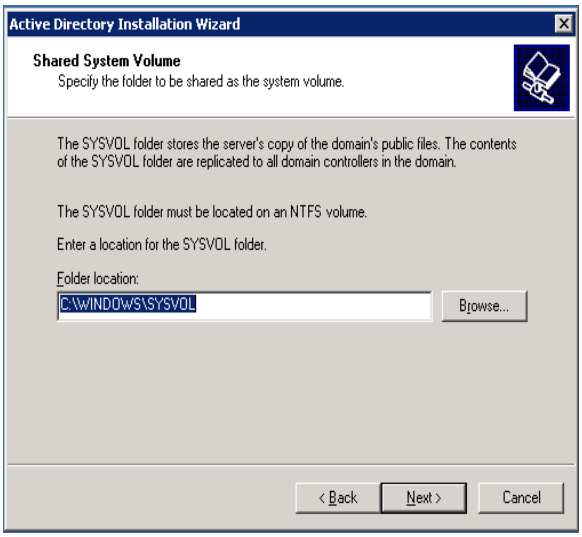

Active Directory Installation Wizard
Domain Controller Type
Specify the role you want this server to have.
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?
Domain controller for a new domain
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
Additional domain controller for an existing domain
Proceeding with this option will delete all local accounts on this server.
All cryptographic keys will be deleted and should be exported before continuing.
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
< Back
Next >
Cancel

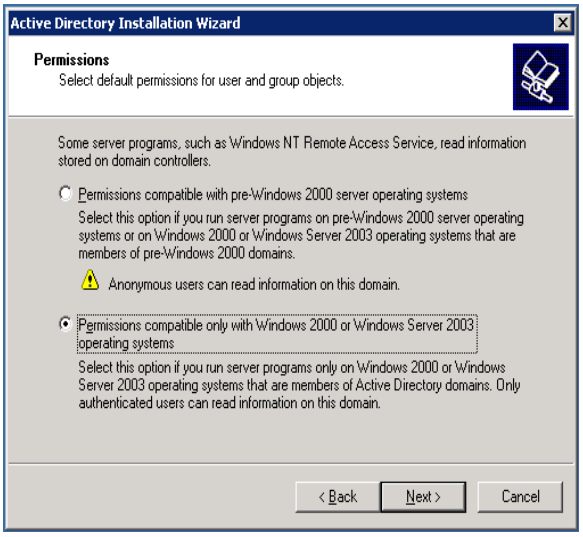

Active Directory Installation Wizard
Create New Domain
Select which type of domain to create.
Create a new:
Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
< Back
Next >
Cancel

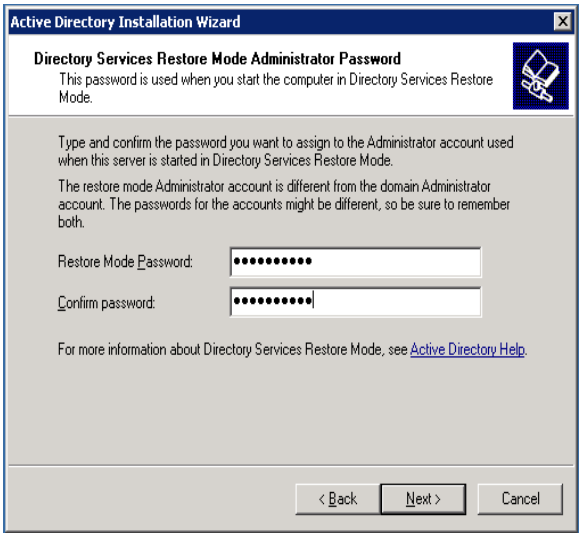

Active Directory Installation Wizard
New Domain Name
Specify a name for the new domain.
Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).
Full DNS name for new domain:
testdomain.com
< Back
Next >
Cancel

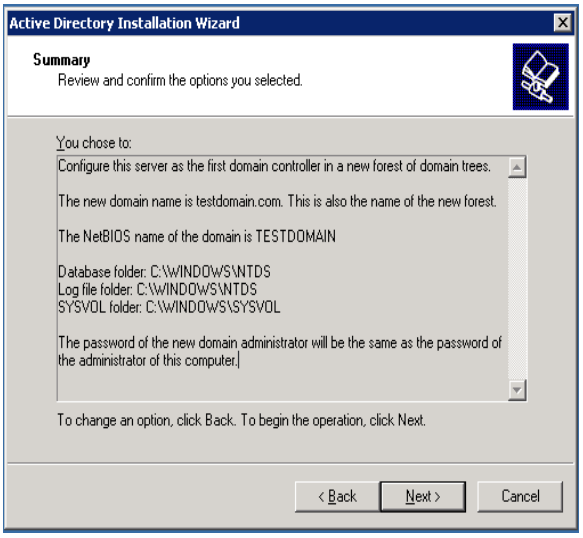

Active Directory Installation Wizard
NetBIOS Domain Name
Specify a NetBIOS name for the new domain.
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.
Domain NetBIOS name:
TESTDOMAIN
< Back
Next >
Cancel

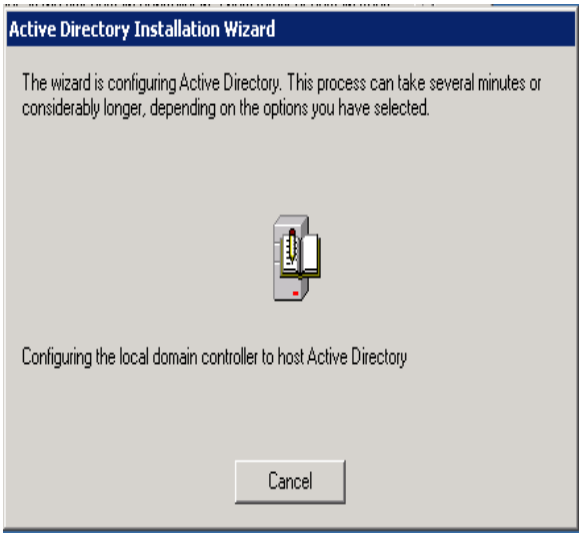

Active Directory Installation Wizard
Database and Log Folders
Specify the folders to contain the Active Directory database and log files.
For best performance and recoverability, store the database and the log on separate hard disks.
Where do you want to store the Active Directory database?
Database folder:
C:\WINDOWS\NTDS
Browse...
Where do you want to store the Active Directory log?
Log folder:
C:\WINDOWS\NTDS
Browse...
< Back
Next >
Cancel

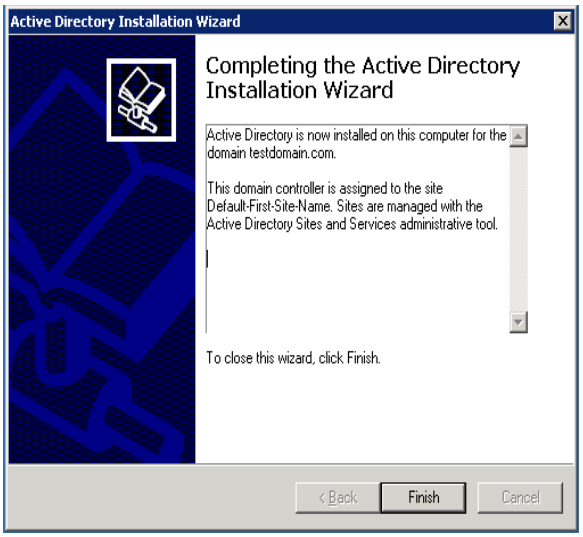

Active Directory Installation Wizard
Shared System Volume
Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Folder location:
C:\WINDOWS\SYSVOL
Browse...
< Back
Next >
Cancel


Active Directory Installation Wizard
Permissions
Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
Permissions compatible with pre-Windows 2000 server operating systems
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
Anonymous users can read information on this domain.
Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
< Back
Next >
Cancel


Active Directory Installation Wizard
Directory Services Restore Mode Administrator Password
This password is used when you start the computer in Directory Services Restore Mode.
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.
Restore Mode Password:
Confirm password:
For more information about Directory Services Restore Mode, see Active Directory Help.
< Back
Next >
Cancel


Active Directory Installation Wizard
Summary
Review and confirm the options you selected.
You chose to:
Configure this server as the first domain controller in a new forest of domain trees.
The new domain name is testdomain.com. This is also the name of the new forest.
The NetBIOS name of the domain is TESTDOMAIN
Database folder: C:\WINDOWS\NTDS
Log file folder: C:\WINDOWS\NTDS
SYSVOL folder: C:\WINDOWS\SYSVOL
The password of the new domain administrator will be the same as the password of the administrator of this computer.
To change an option, click Back. To begin the operation, click Next.
< Back
Next >
Cancel


Active Directory Installation Wizard
The wizard is configuring Active Directory. This process can take several minutes or considerably longer, depending on the options you have selected.
Configuring the local domain controller to host Active Directory
Cancel



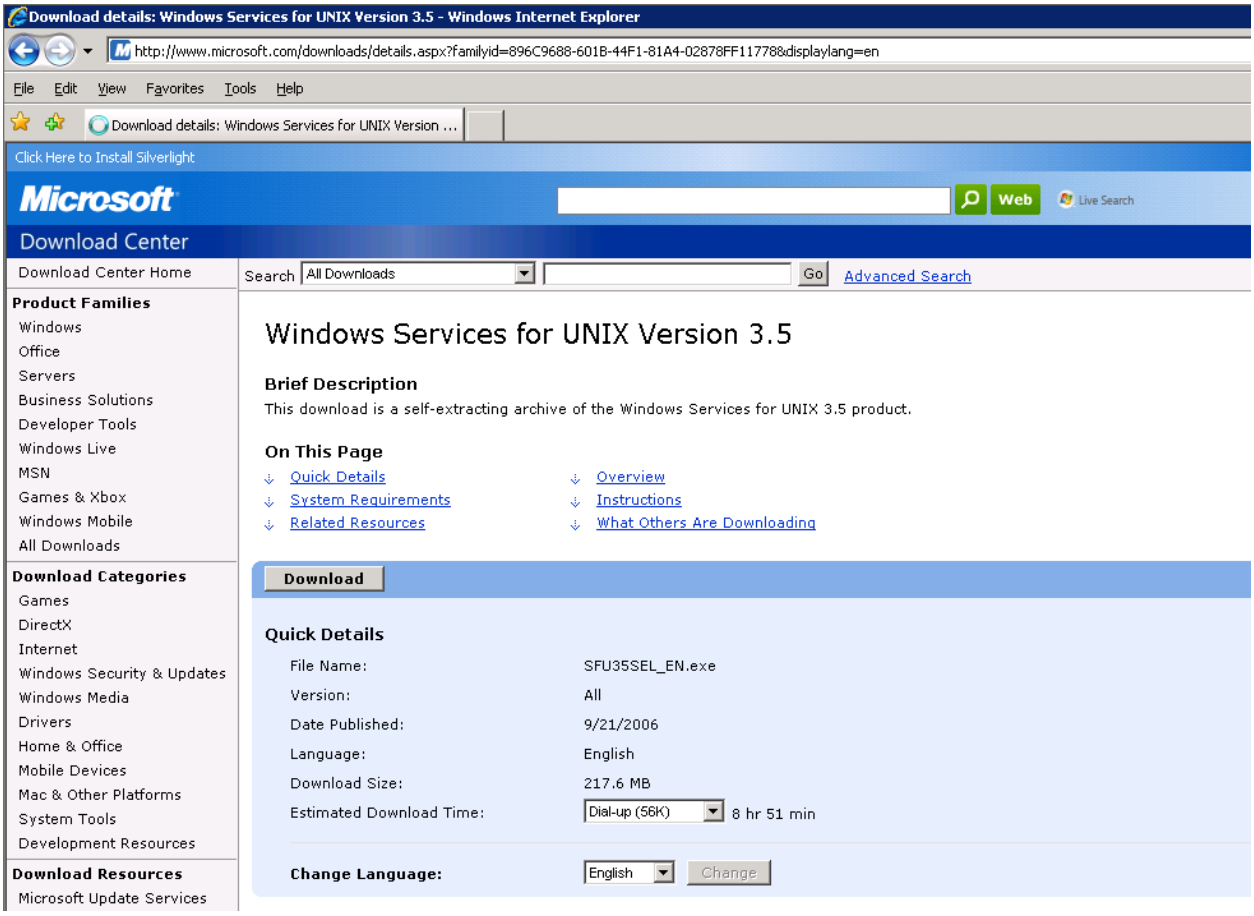
Now you should see the Active Directory icons under **START > PROGRAMS > ADMINISTRATIVE TOOL** Menu



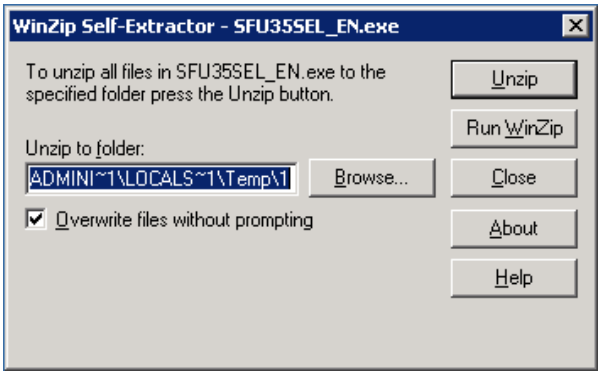
Installing Windows Service for UNIX on Windows 2003 Active Directory Server

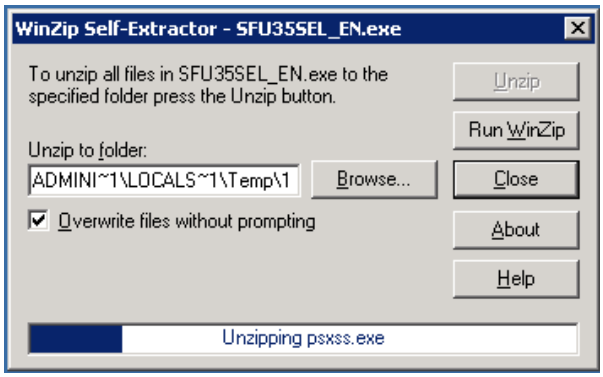
If you already have Windows Services for UNIX installed on your Windows 2003 Server, please skip to the next section.

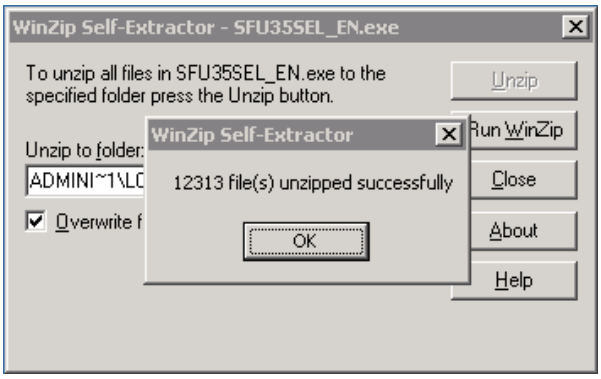
Download the latest version of Windows Services for UNIX from the microsoft.com website.

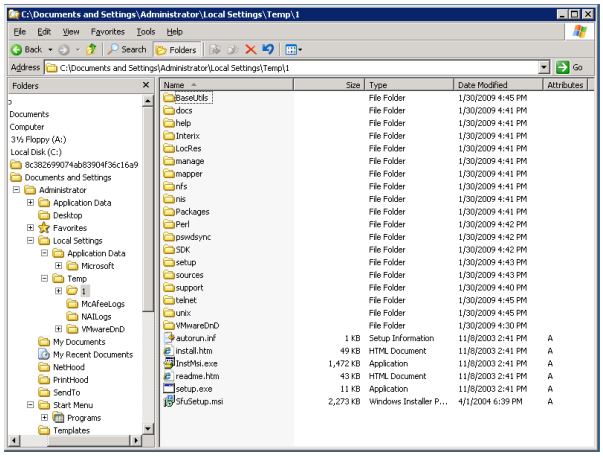


Double-click on the .EXE file downloaded and unzip the contents to a known location.

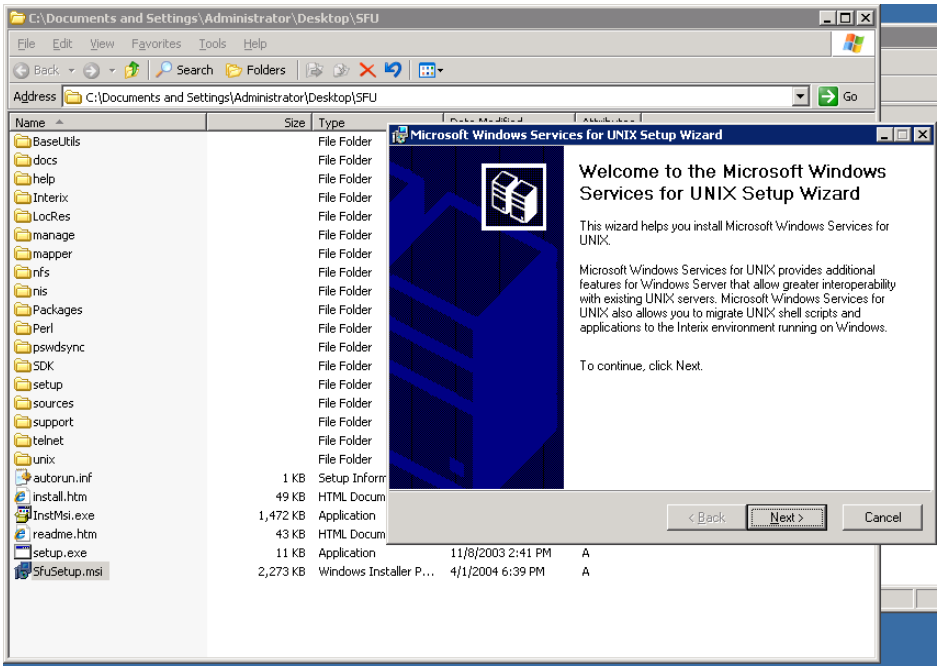


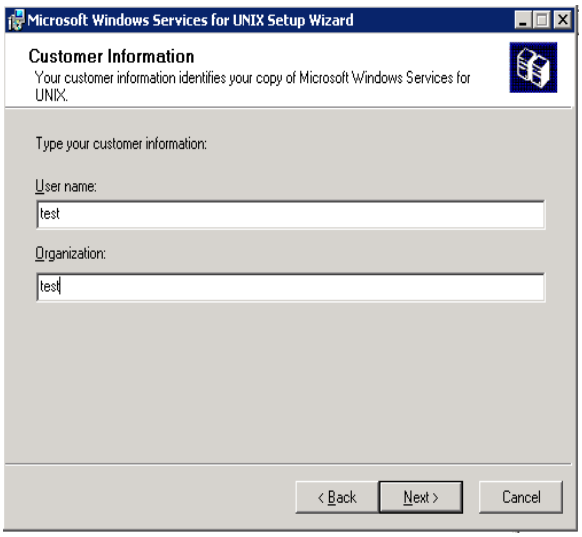


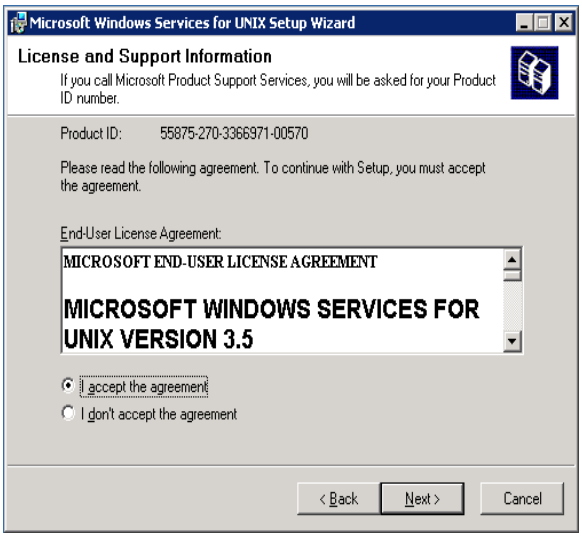


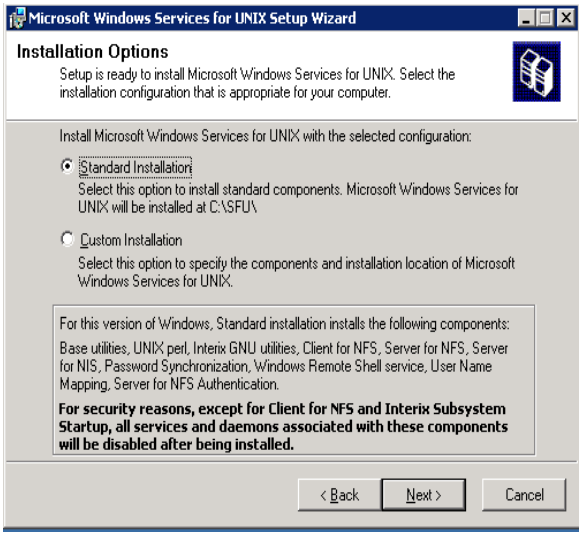


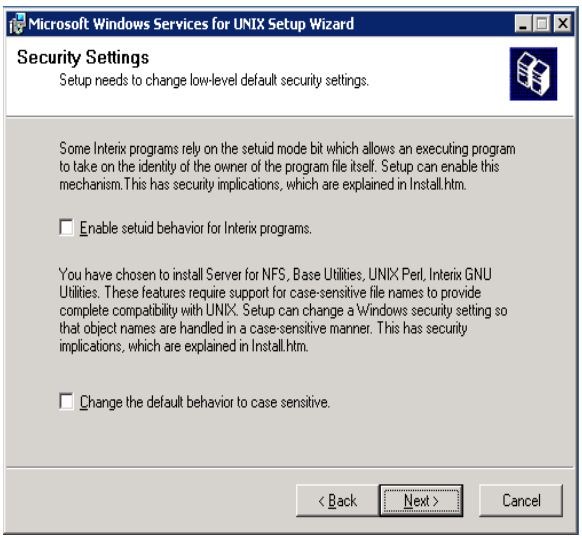
Double-click on the SfuSetup.msi file and install the SFU on the Windows 2003 server as follows:

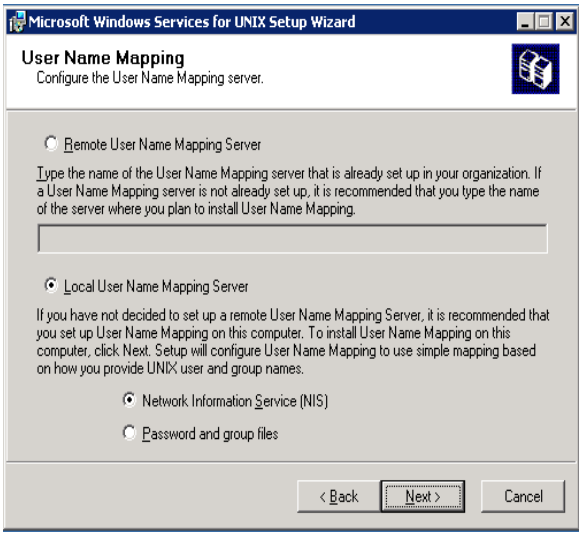


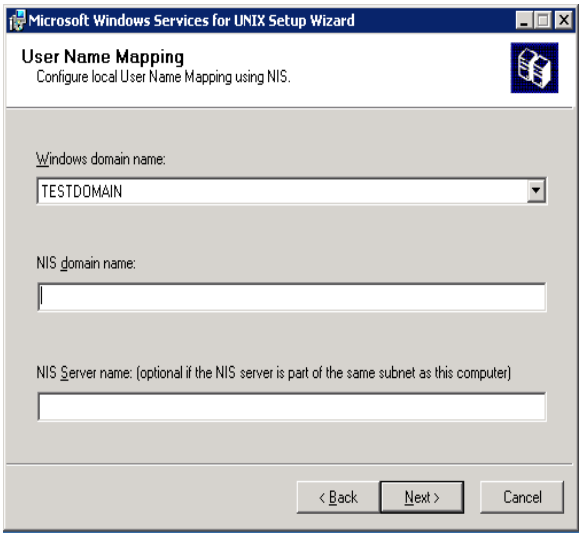

Microsoft Windows Services for UNIX Setup Wizard
Customer Information
Your customer information identifies your copy of Microsoft Windows Services for UNIX.
Type your customer information:
User name:
test
Organization:
test
< Back
Next >
Cancel

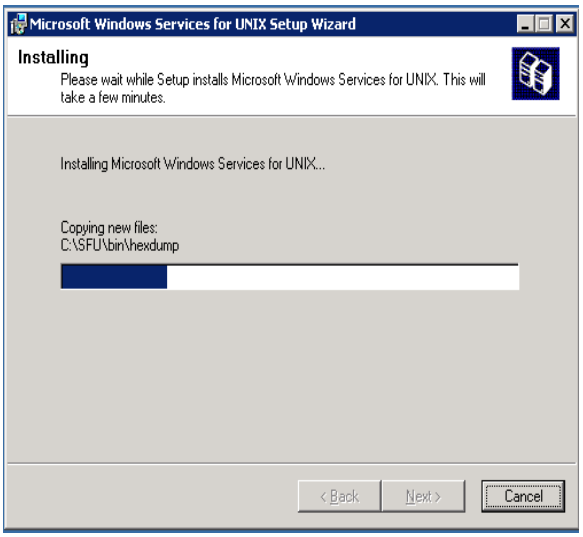

Microsoft Windows Services for UNIX Setup Wizard
License and Support Information
If you call Microsoft Product Support Services, you will be asked for your Product ID number.
Product ID: 55875-270-3366971-00570
Please read the following agreement. To continue with Setup, you must accept the agreement.
End-User License Agreement:
MICROSOFT END-USER LICENSE AGREEMENT
MICROSOFT WINDOWS SERVICES FOR UNIX VERSION 3.5
I accept the agreement
I don't accept the agreement
< Back
Next >
Cancel

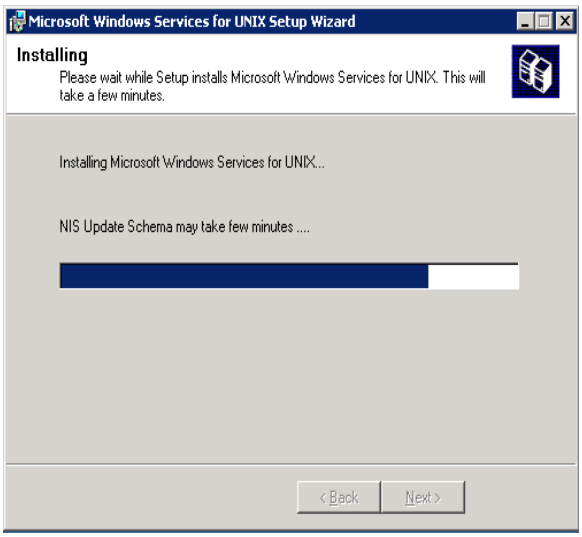

Microsoft Windows Services for UNIX Setup Wizard
Installation Options
Setup is ready to install Microsoft Windows Services for UNIX. Select the installation configuration that is appropriate for your computer.
Install Microsoft Windows Services for UNIX with the selected configuration:
Standard Installation
Select this option to install standard components. Microsoft Windows Services for UNIX will be installed at C:\SFU\
Custom Installation
Select this option to specify the components and installation location of Microsoft Windows Services for UNIX.
For this version of Windows, Standard installation installs the following components:
Base utilities, UNIX perl, Interix GNU utilities, Client for NFS, Server for NFS, Server for NIS, Password Synchronization, Windows Remote Shell service, User Name Mapping, Server for NFS Authentication.
For security reasons, except for Client for NFS and Interix Subsystem Startup, all services and daemons associated with these components will be disabled after being installed.
< Back
Next >
Cancel

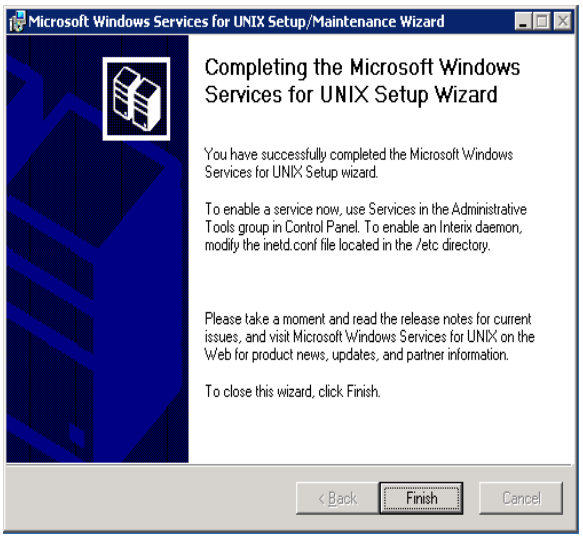

Microsoft Windows Services for UNIX Setup Wizard
Security Settings
Setup needs to change low-level default security settings.
Some Interix programs rely on the setuid mode bit which allows an executing program to take on the identity of the owner of the program file itself. Setup can enable this mechanism.This has security implications, which are explained in Install.htm.
Enable setuid behavior for Interix programs.
You have chosen to install Server for NFS, Base Utilities, UNIX Perl, Interix GNU Utilities. These features require support for case-sensitive file names to provide complete compatibility with UNIX. Setup can change a Windows security setting so that object names are handled in a case-sensitive manner. This has security implications, which are explained in Install.htm.
Change the default behavior to case sensitive.
< Back
Next >
Cancel


Microsoft Windows Services for UNIX Setup Wizard
User Name Mapping
Configure the User Name Mapping server.
Remote User Name Mapping Server
Type the name of the User Name Mapping server that is already set up in your organization. If a User Name Mapping server is not already set up, it is recommended that you type the name of the server where you plan to install User Name Mapping.
Local User Name Mapping Server
If you have not decided to set up a remote User Name Mapping Server, it is recommended that you set up User Name Mapping on this computer. To install User Name Mapping on this computer, click Next. Setup will configure User Name Mapping to use simple mapping based on how you provide UNIX user and group names.
Network Information Service (NIS)
Password and group files
< Back
Next >
Cancel


Microsoft Windows Services for UNIX Setup Wizard
User Name Mapping
Configure local User Name Mapping using NIS.
Windows domain name:
TESTDOMAIN
NIS domain name:
NIS Server name: (optional if the NIS server is part of the same subnet as this computer)
< Back
Next >
Cancel


Microsoft Windows Services for UNIX Setup Wizard
Installing
Please wait while Setup installs Microsoft Windows Services for UNIX. This will take a few minutes.
Installing Microsoft Windows Services for UNIX...
Copying new files:
C:\SFU\bin\hexdump
< Back
Next >
Cancel


Microsoft Windows Services for UNIX Setup Wizard
Installing
Please wait while Setup installs Microsoft Windows Services for UNIX. This will take a few minutes.
Installing Microsoft Windows Services for UNIX...
NIS Update Schema may take few minutes ....
< Back
Next >


Microsoft Windows Services for UNIX Setup/Maintenance Wizard
Completing the Microsoft Windows Services for UNIX Setup Wizard
You have successfully completed the Microsoft Windows Services for UNIX Setup wizard.
To enable a service now, use Services in the Administrative Tools group in Control Panel. To enable an Interix daemon, modify the inetd.conf file located in the /etc directory.
Please take a moment and read the release notes for current issues, and visit Microsoft Windows Services for UNIX on the Web for product news, updates, and partner information.
To close this wizard, click Finish.
< Back
Finish
Cancel


Microsoft Windows Services for UNIX Installer Information
You must restart your system for the configuration changes made to Microsoft Windows Services for UNIX to take effect. Click Yes to restart now or No if you plan to manually restart later.
Yes
No

Creating Profiles and Groups in the Active Directory for CM Login profiles

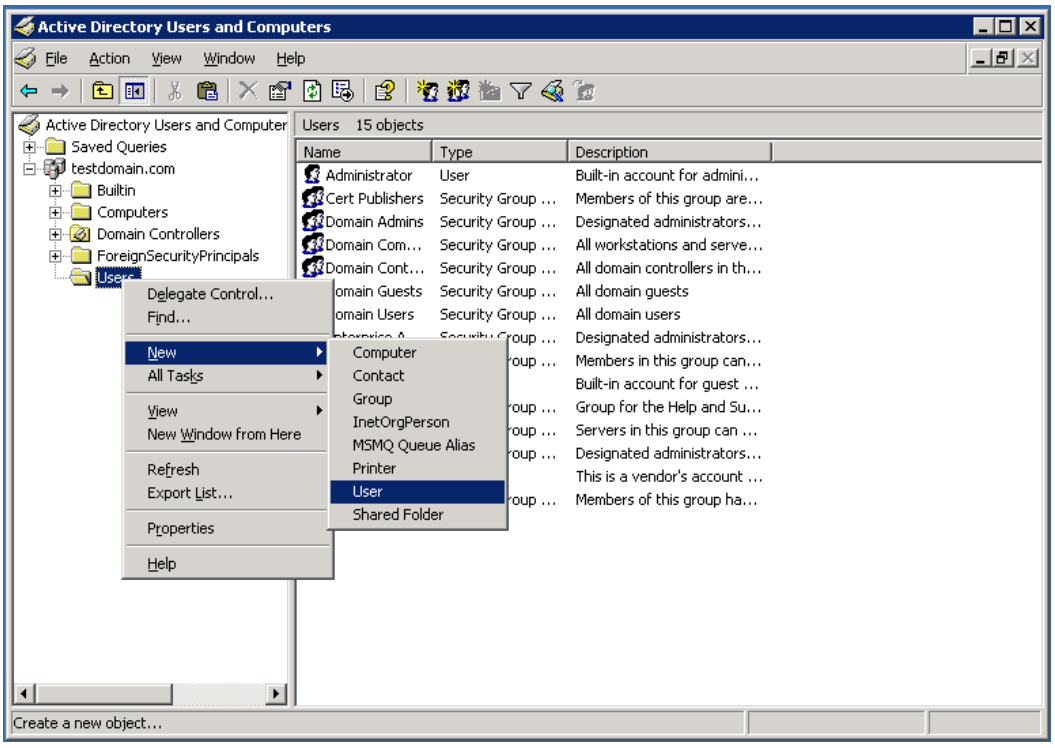
For the sake of this document, I will assume that we have two types of users: admins and non-admin type users. One can create multiple type of users based on their business needs which will follow the same concepts as described below.

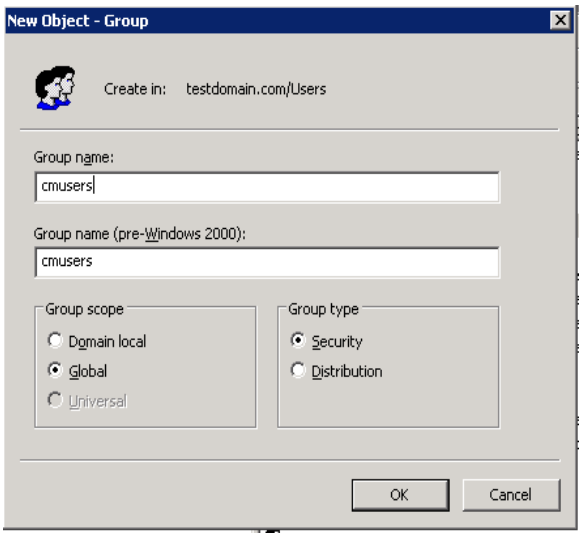
For the two types of users mentioned above, we need to create two groups in the Active directory, one for normal users or *cmusers* and one for admins or *susers*. We also need to create two additional groups which will be associated with the **USER-PROFILES** in the Avaya CM corresponding to the *cmusers* and *susers* groups. By default, profile 18 or *prof18* is associated with susers group and we can create a custom profile (in our example *prof20*) for *cmusers*.

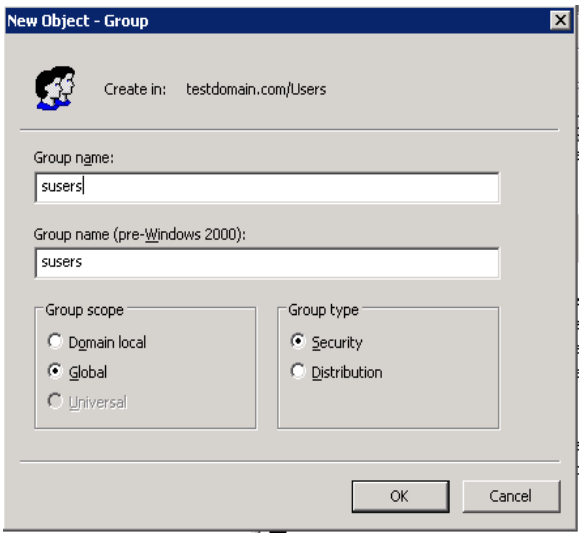
From the **START > PROGRAMS > ADMINISTRATIVE TOOLS** Menu, select Active Directory Users and Computers for the AD Users snap-in.

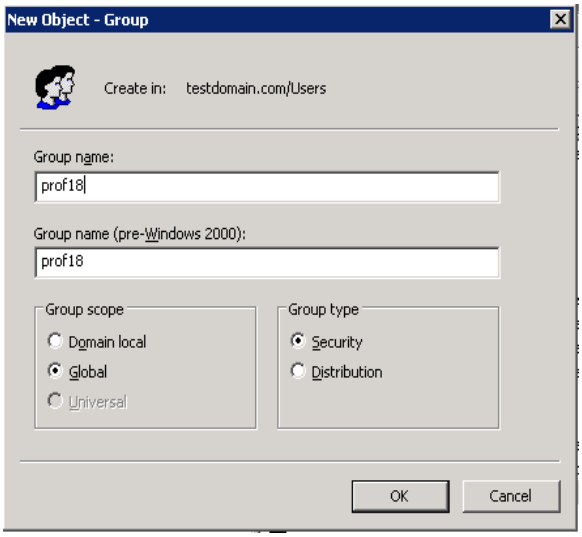
Create the following four groups as follows:
cmusers, susers, prof18 and *prof20*

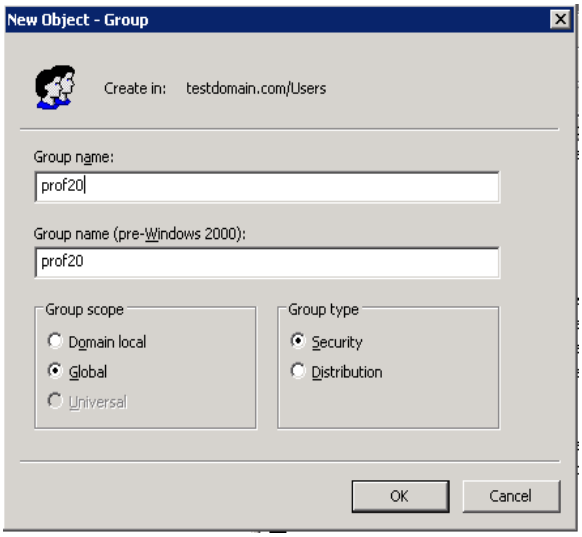
In the AD Users and Computers snap-in, under the **testdomain.com** drop-down menu, right-click on the **Users** icon, select **New** and then **Group**







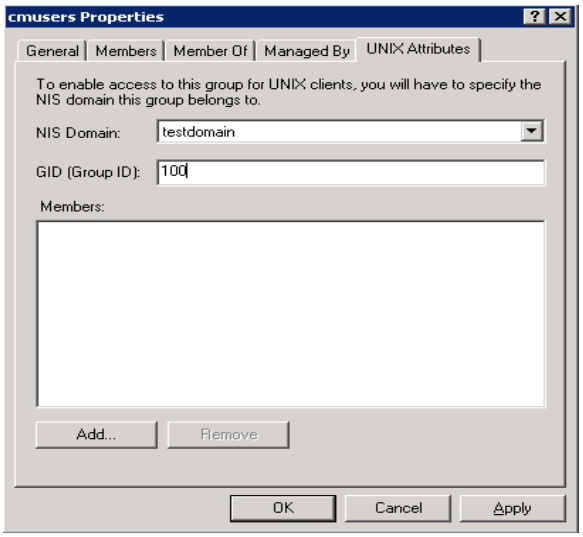


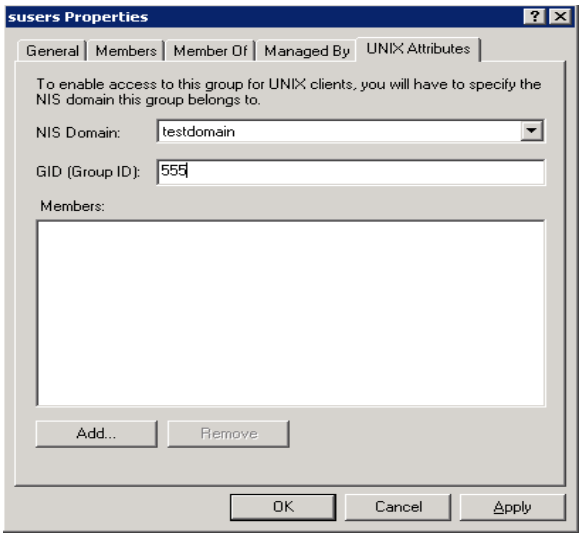


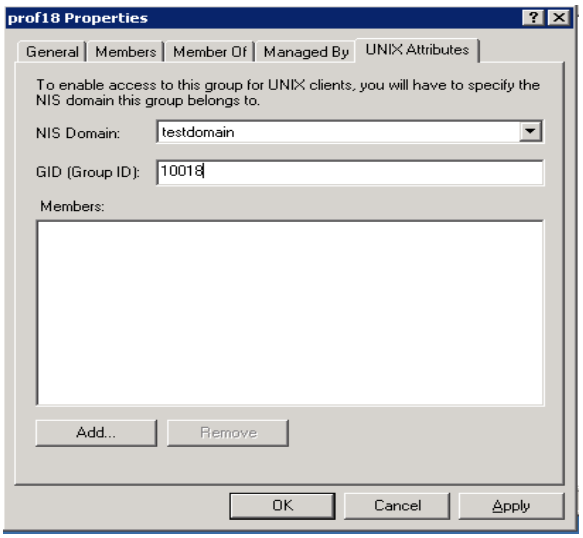
After creating the four required **Security Groups**, right-click on each and go to the Unix Attribute tabs or each and set the values as follows:

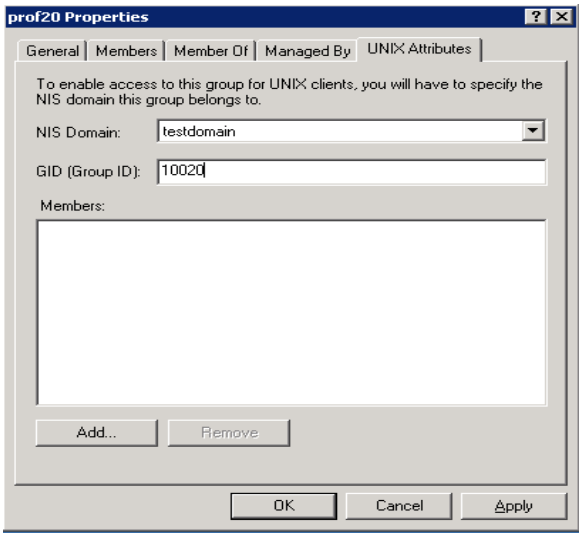
For *cmusers* Group, set the NIS Domain to testdomain (from the drop-down menu) and the GID value to 100
For susers Group, set the NIS Domain to testdomain and the GID value to 555
For *prof18* Group, set the NIS Domain to testdomain, and the GID value to 10018
For *prof20* Group, set the NIS Domain to testdomain, and the GID value to 10020

NOTE: for various profiles, the formula to use is 10000 plus the numerical value of the profile so for example prof54 will have the GID value of 10054 etc.

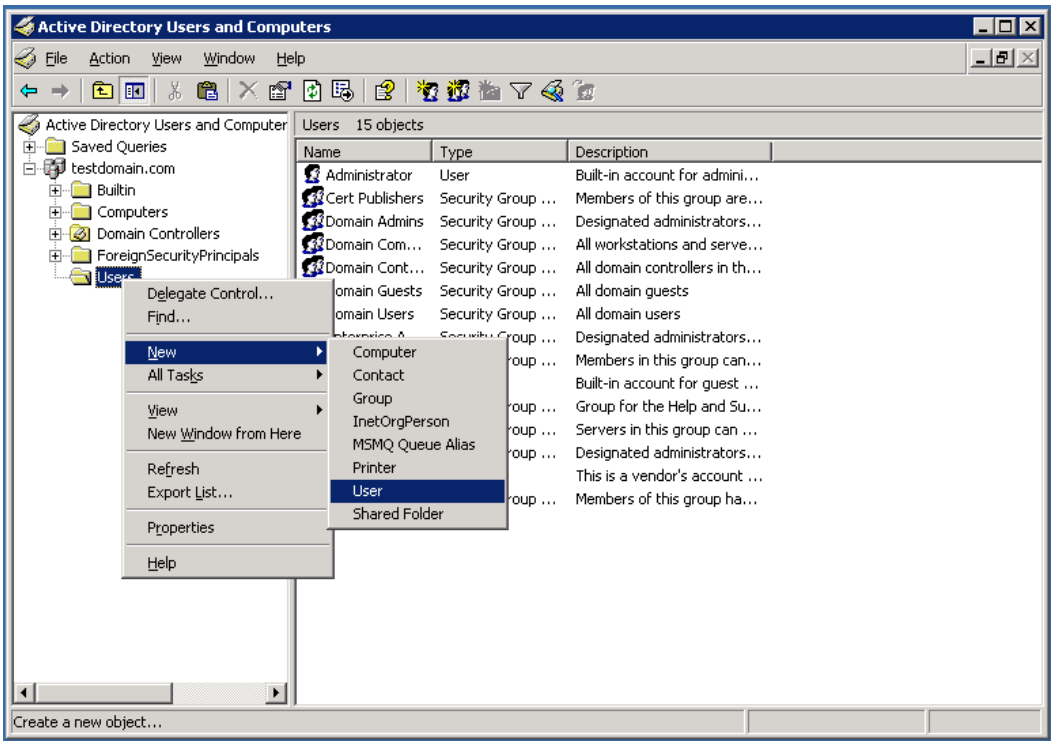




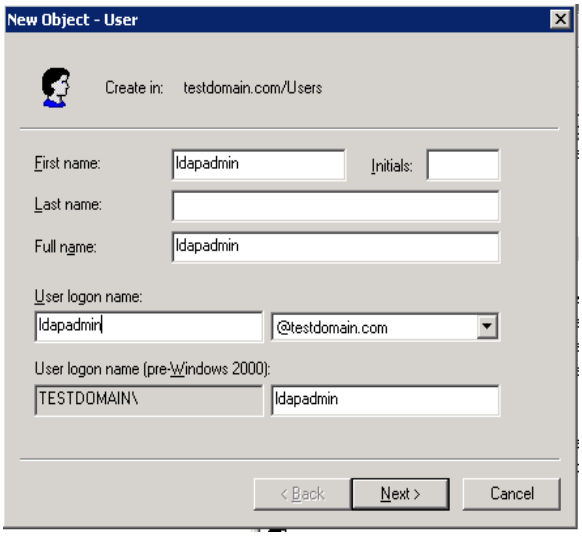


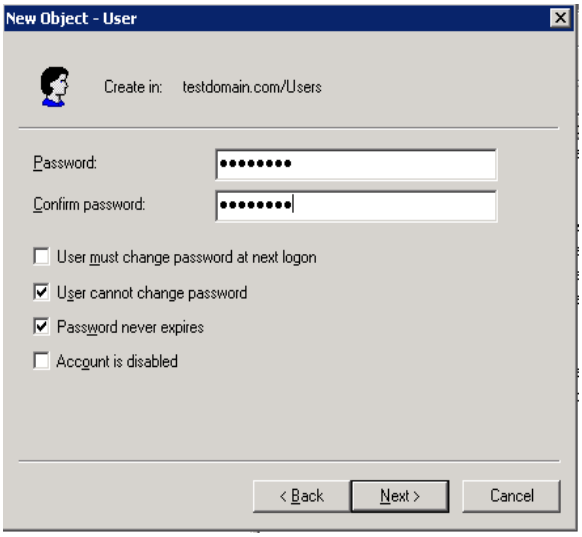


Lastly, we need to create an Admin user for the CM to be able to access the AD. We will call this user *ldapadmin*. Right-click on the **Users** under testdomain.com and select, **New** and then **User**

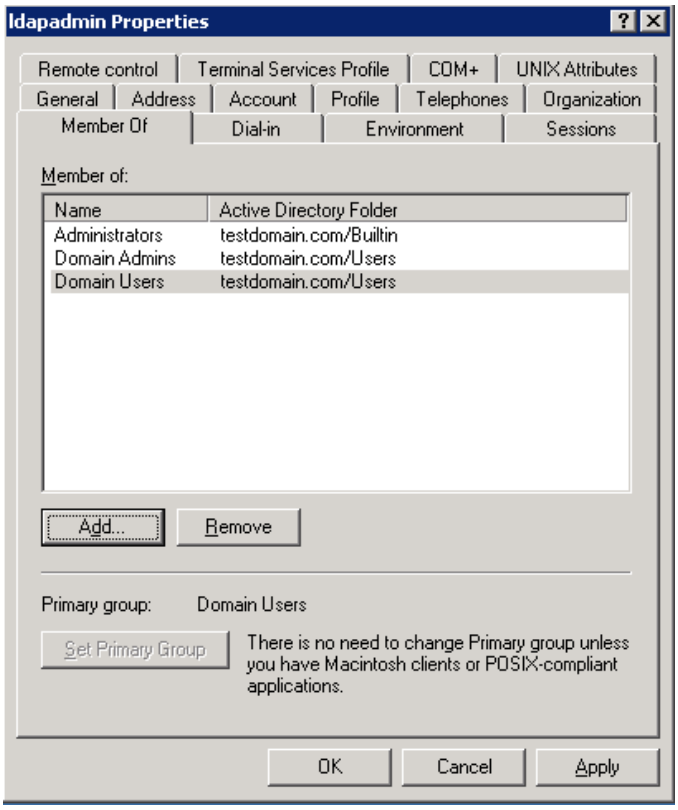


Create a new user as follows:





After creating the *ldapadmin* user, double-click on the *ldapadmin* user and go to the **Member Of** tab, click Add and make him a member of **Administrators** and a **Domain Admins** group.



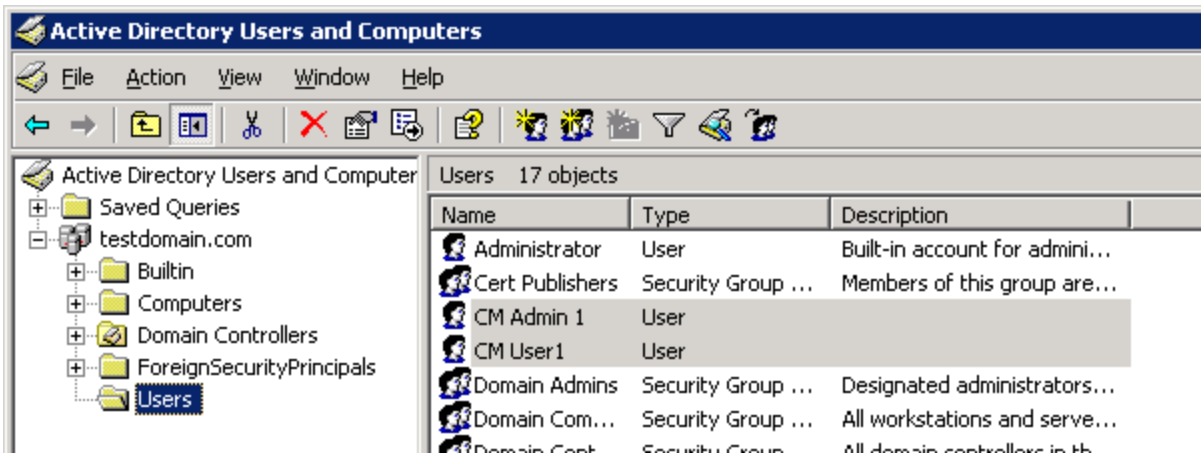
This account has **Administrator** privileges to the domain **testdomain**. In this example, the password for this account is set to Avaya123!

Creating and Configuring Users in Active Directory for CM Logins

If you already have Users configured in your Active Directory server, you can skip to the portion where we edit the user for UNIX Attributes.

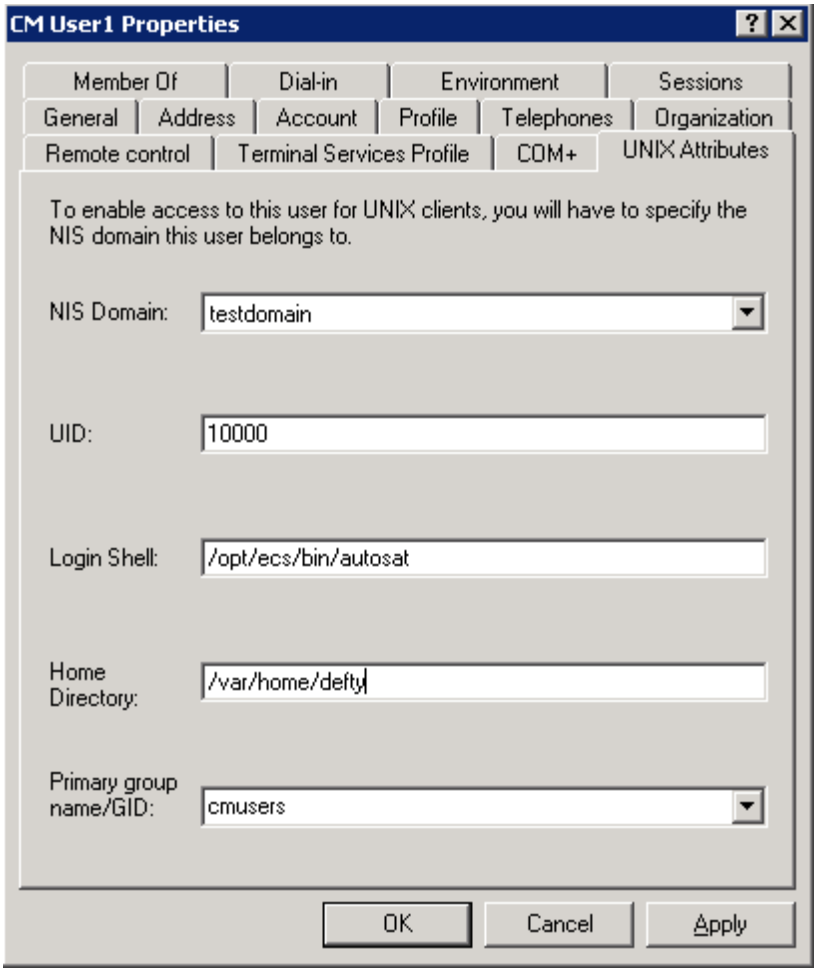
For this example, we will create two users, one for non-admin use called *cmuser1* and one for admin use called *cmadmin1*

Create two Users called *cmuser1* and *cmadmin1* exactly the same way as you created *ldapadmin* User only **DO NOT** make them part of the **Administrators** or **Domain Admins** group. By default, they will be placed in the **Domain Users** group.



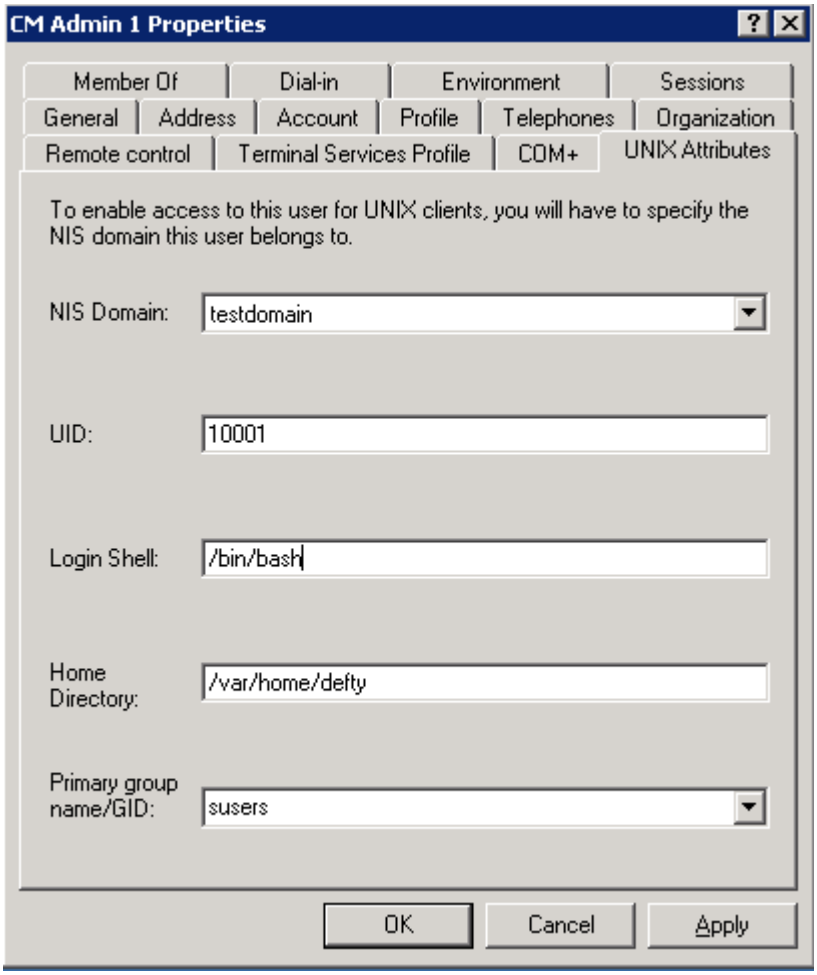
Double Click on the *cmuser1* User and go to the **UNIX Attribute** tab. Set the Values as follows:

NIS Domain = **testdomain**
UID has to be a distinct number for each user, this could be any number as long as it is different for each user.
Login Shell = /opt/ecs/bin/autosat
NOTE: This allows ONLY SAT access to the CM, since these are non-admin users, we do not ant to give them shell access to the CM UNIX side.
Home Directory = /var/home/defty
Primary Group name/GID = **cmusers**

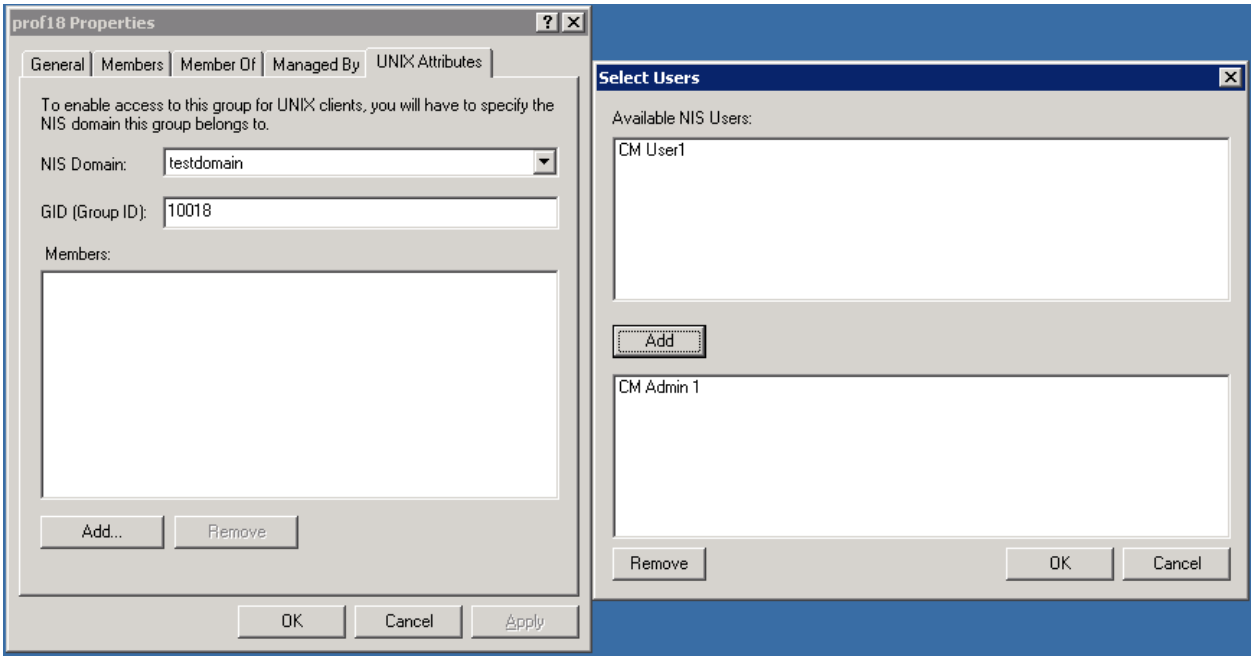


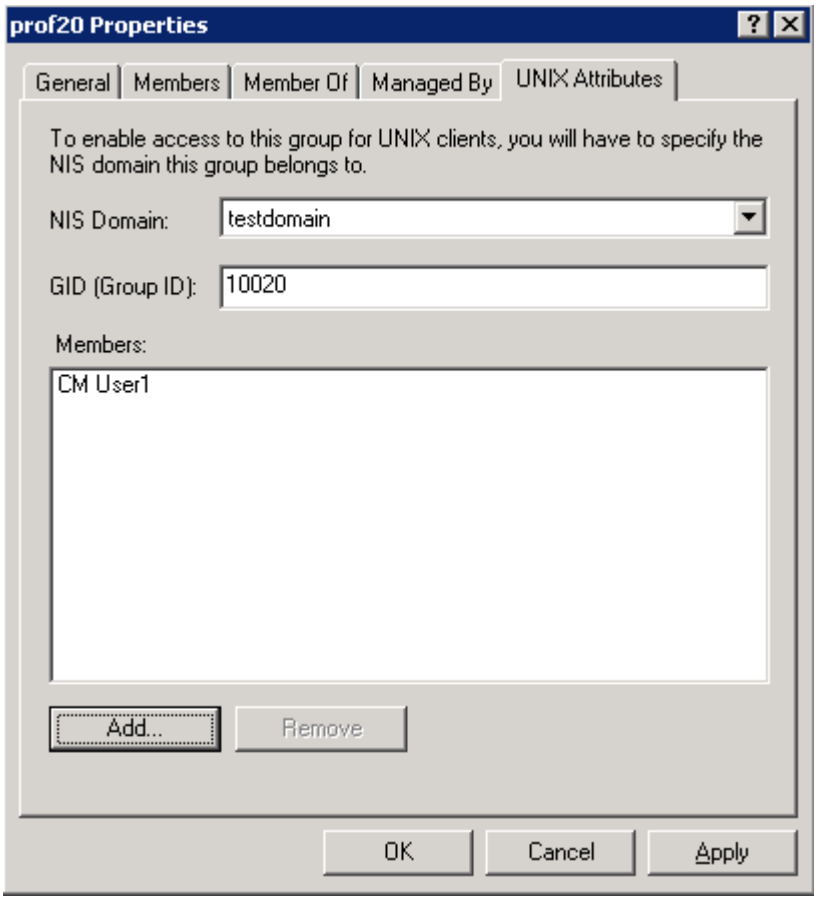
For the User *cmadmin1*, on the **UNIX Attribute** tab, set the values as follows:

NIS Domain = **testdomain**
UID has to be a distinct number for each user, this could be any number as long as it is different for each user.
Login Shell = /bin/bash
NOTE: This allows FULL BASH shell access to the CM, since these are admin users, we can allow SHELL access to the CM, if you don't want to give them SHELL access, set the login shell value to the previous value as stated in the cmuser1 profile.
Home Directory = /var/home/defty
Primary Group name/GID = **susers**

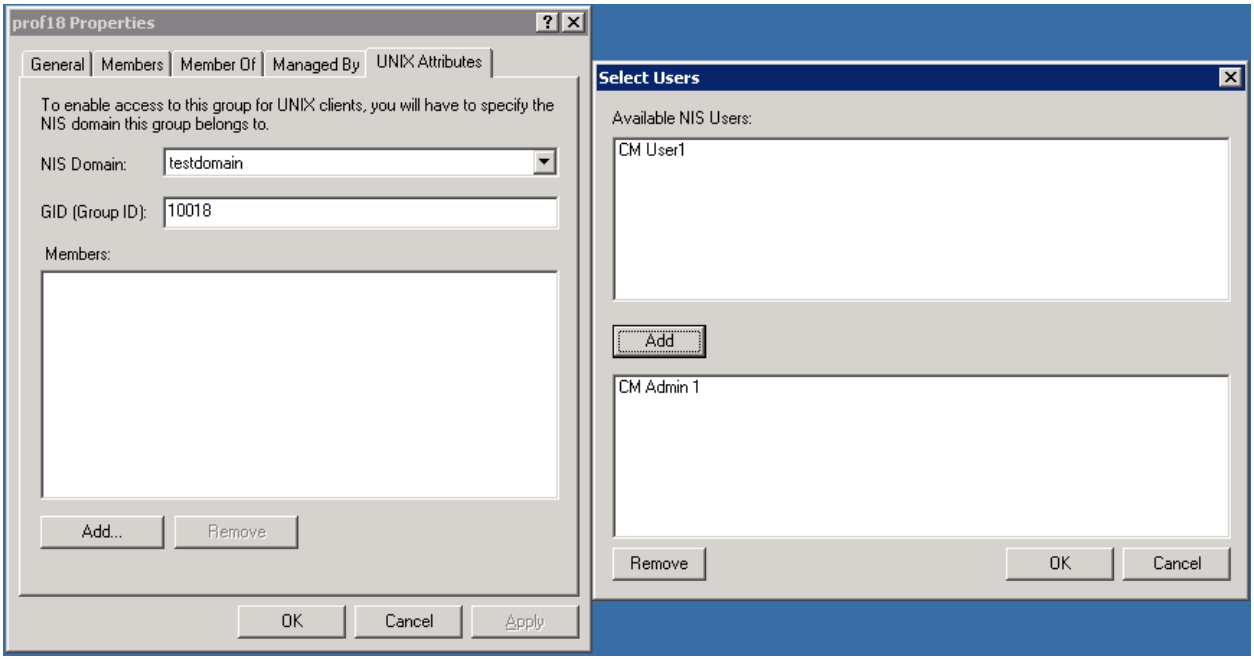


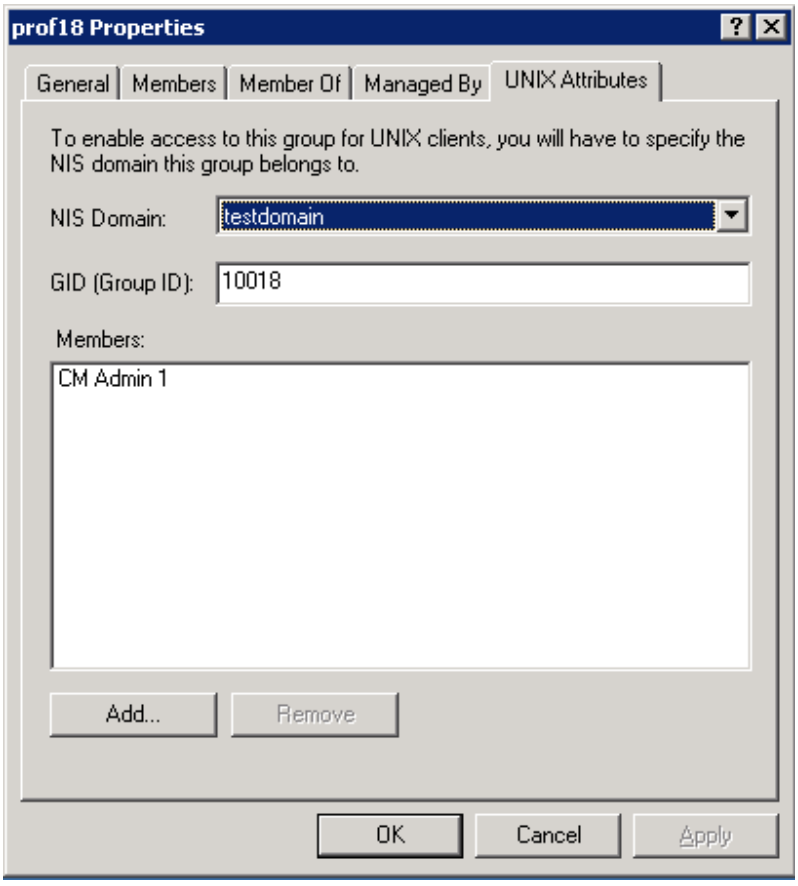
Hit **Apply** and **OK** for both Users.
Double-click on *prof18* Group and go to the **UNIX Attribute** tab, Click **Add** under the **Members** window and add *cmuser1* as a member of this Group.
NOTE: You cannot do this under the Member Of tab.


prof18 Properties
General
Members
Member Of
Managed By
UNIX Attributes
To enable access to this group for UNIX clients, you will have to specify the NIS domain this group belongs to.
NIS Domain:
testdomain
GID (Group ID):
10018
Members:
Add...
Remove
OK
Cancel
Apply
Select Users
Available NIS Users:
CM User1
Add
CM Admin 1
Remove
OK
Cancel


prof20 Properties
General
Members
Member Of
Managed By
UNIX Attributes
To enable access to this group for UNIX clients, you will have to specify the NIS domain this group belongs to.
NIS Domain:
testdomain
GID (Group ID):
10020
Members:
CM User1
Add...
Remove
OK
Cancel
Apply

Double-click on *prof20* Group and go to the **UNIX Attribute** tab, Click **Add** under the **Members** window and add *cmadmin1* as a member of this Group.
NOTE: You cannot do this under the Member Of tab.

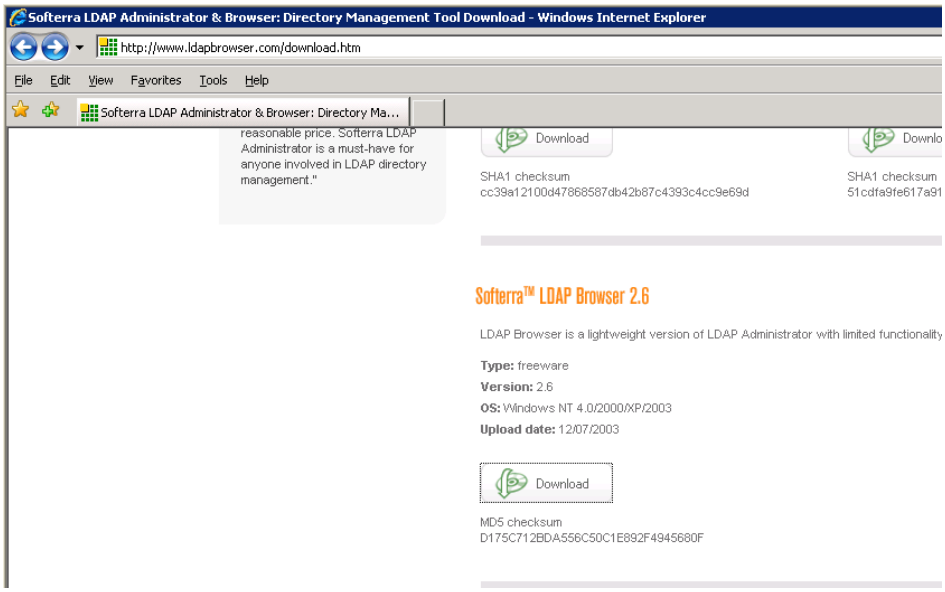




Installing and Configuring Softerra LDAP Browser

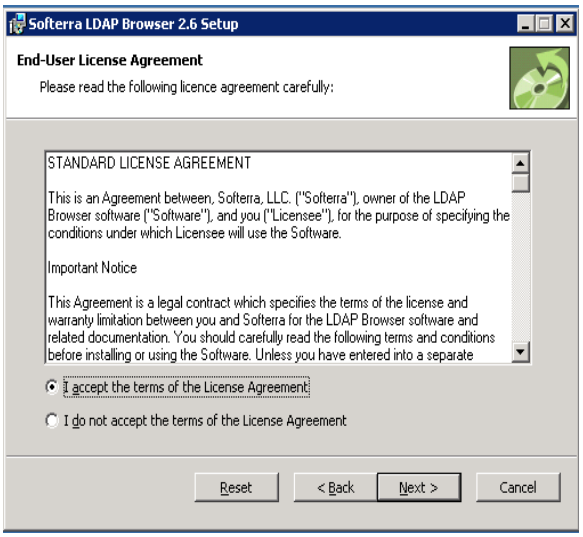
If you already have an LDAP Browser installed on your PC or the Windows 2003 server, please skip to the next step.

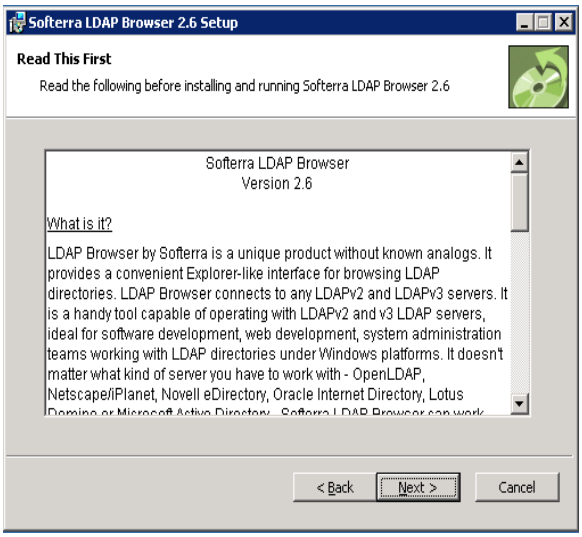
Download the Softerra LDAP Browser from the softerra website (it is free) and install on your PC and/or the Windows 2003 server, for this document, I will be installing it on the Windows 2003 Server.

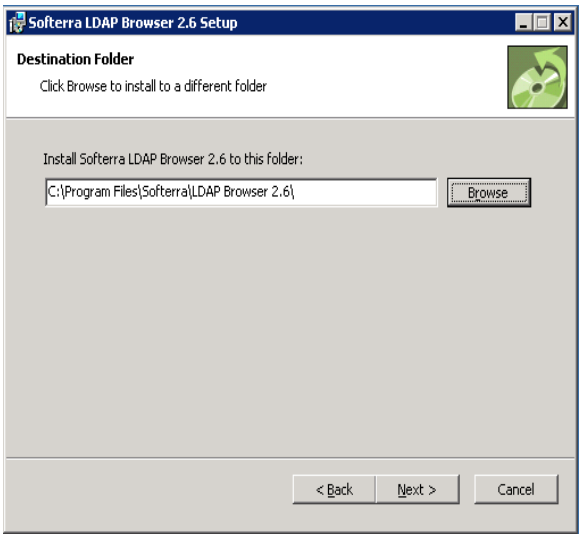


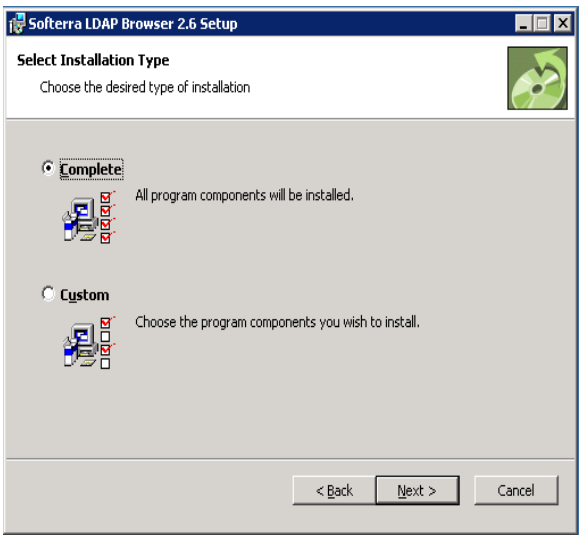


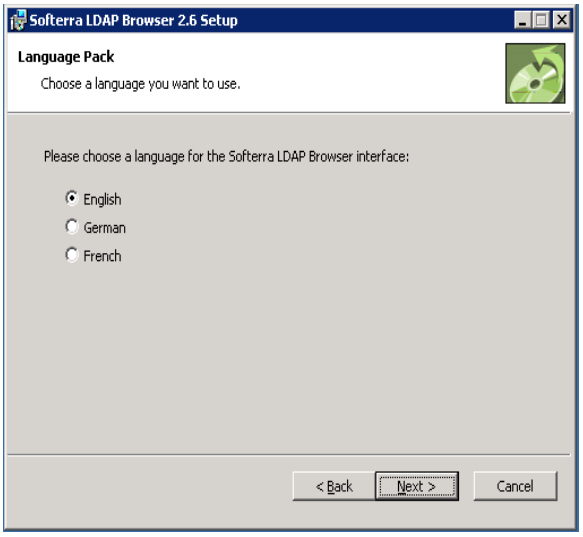


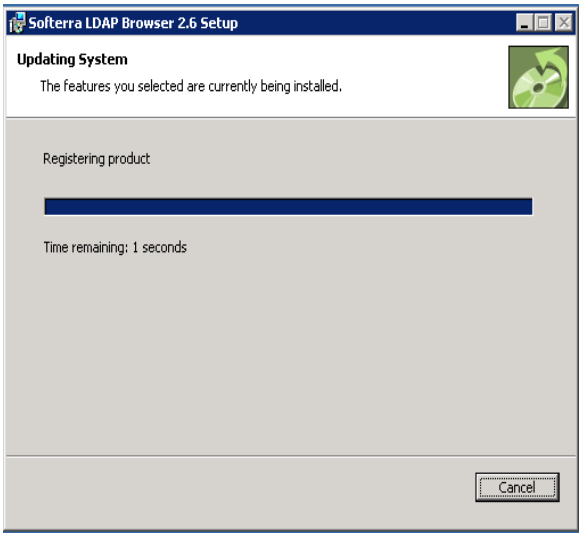

Softerra LDAP Browser 2.6 Setup
End-User License Agreement
Please read the following licence agreement carefully:
STANDARD LICENSE AGREEMENT
This is an Agreement between, Softerra, LLC. ("Softerra"), owner of the LDAP Browser software ("Software"), and you ("Licensee"), for the purpose of specifying the conditions under which Licensee will use the Software.
Important Notice
This Agreement is a legal contract which specifies the terms of the license and warranty limitation between you and Softerra for the LDAP Browser software and related documentation. You should carefully read the following terms and conditions before installing or using the Software. Unless you have entered into a separate
I accept the terms of the License Agreement
I do not accept the terms of the License Agreement
Reset
< Back
Next >
Cancel


Softerra LDAP Browser 2.6 Setup
Read This First
Read the following before installing and running Softerra LDAP Browser 2.6
Softerra LDAP Browser
Version 2.6
What is it?
LDAP Browser by Softerra is a unique product without known analogs. It provides a convenient Explorer-like interface for browsing LDAP directories. LDAP Browser connects to any LDAPv2 and LDAPv3 servers. It is a handy tool capable of operating with LDAPv2 and v3 LDAP servers, ideal for software development, web development, system administration teams working with LDAP directories under Windows platforms. It doesn't matter what kind of server you have to work with - OpenLDAP, Netscape/iPlanet, Novell eDirectory, Oracle Internet Directory, Lotus
< Back
Next >
Cancel


Softerra LDAP Browser 2.6 Setup
Destination Folder
Click Browse to install to a different folder
Install Softerra LDAP Browser 2.6 to this folder:
C:\Program Files\Softerra\LDAP Browser 2.6\
Browse
< Back
Next >
Cancel

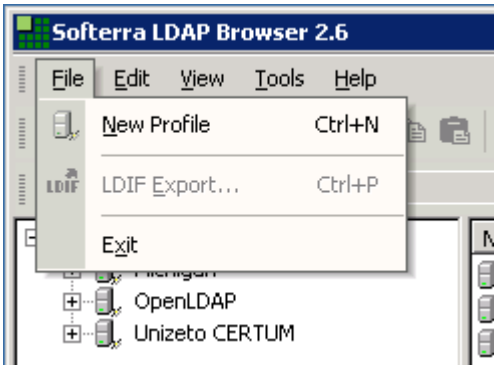

Softerra LDAP Browser 2.6 Setup
Select Installation Type
Choose the desired type of installation
Complete
All program components will be installed.
Custom
Choose the program components you wish to install.
< Back
Next >
Cancel

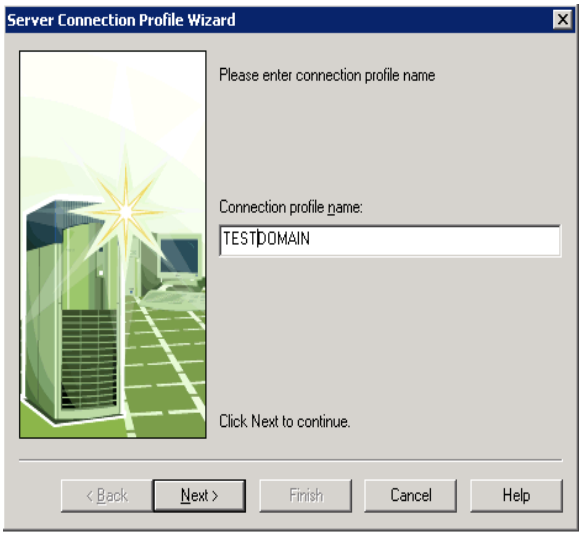

Softerra LDAP Browser 2.6 Setup
Language Pack
Choose a language you want to use.
Please choose a language for the Softerra LDAP Browser interface:
English
German
French
< Back
Next >
Cancel

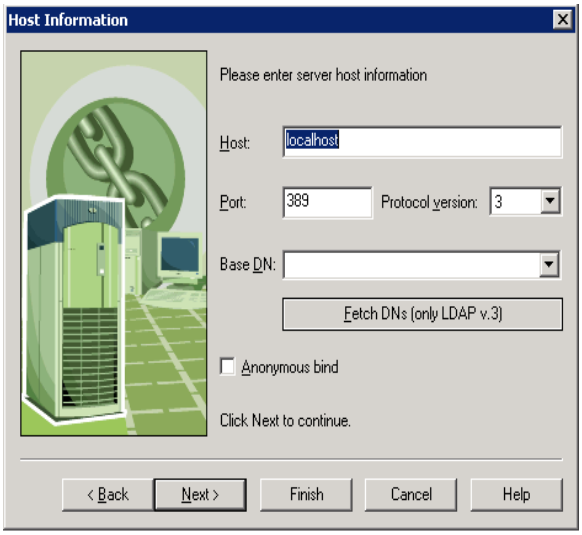

Softerra LDAP Browser 2.6 Setup
Updating System
The features you selected are currently being installed.
Registering product
Time remaining: 1 seconds
Cancel

After installing the LDAP Browser, start it from the Programs Menu.

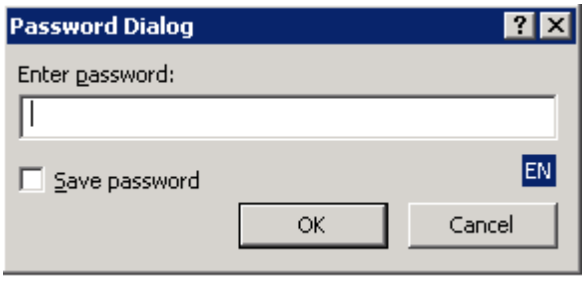
Create a new profile for TESTDOMAIN as follows:





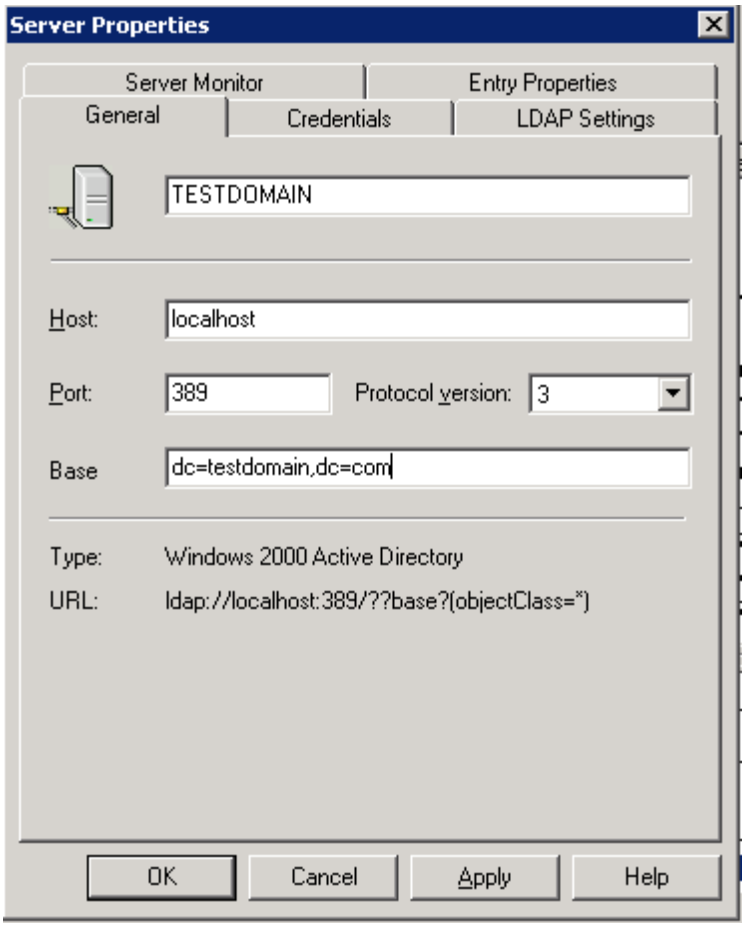


NOTE: If you did not install LDAP Browser on the Windows 2003 server itself, please put the IP address of your Server under the Host.

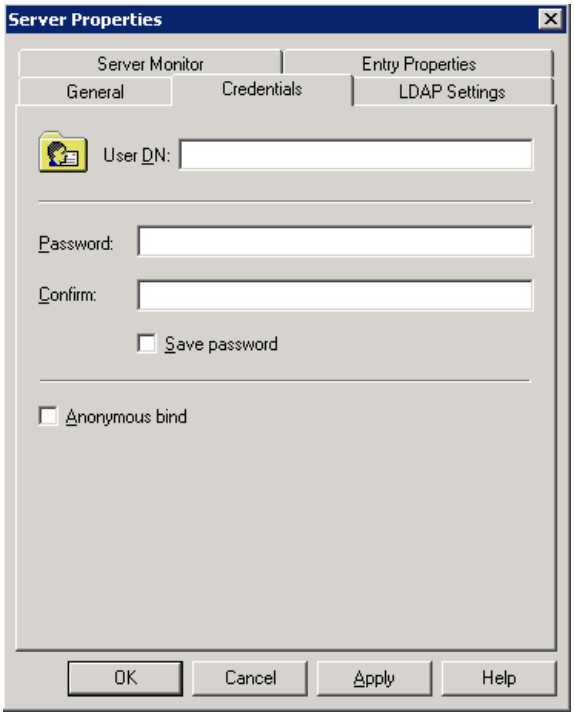


Enter the Domain Administrator password

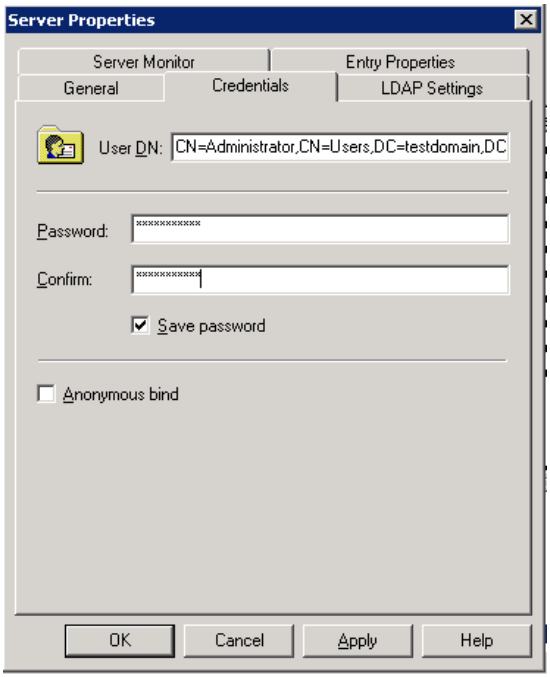
Since we did not put a Base DN in the previous screen, you will probably get a Operation Error based on Invalid Credentials. Select TESTDOMAIN from the **Browser Root** drop-down Menu and Select **VIEW > PROPERTIES**, make sure the Base is correct in the General tab.



Go to the Credentials Tab



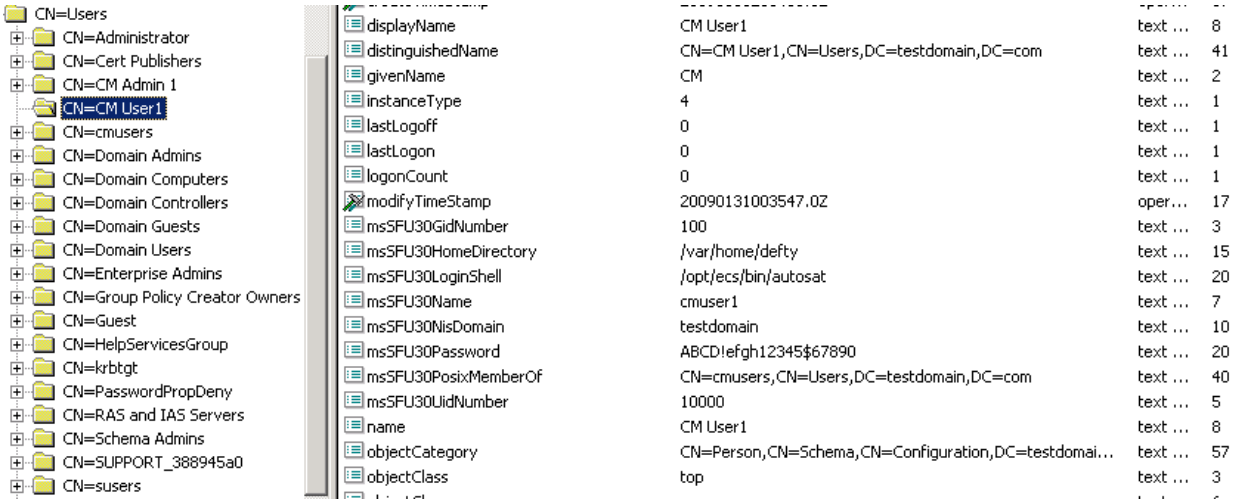
Enter your UserDN, in this case, the UserDN will be
CN=Administrator,CN=Users,DC=testdomain,DC=com
NOTE: You can use the *ldapadmin* account and password here as well.
And enter the Administrator password and confirm password, save password for ease of use in the future if you would like.



It should now allow you to Browse your LDAP Active Directory.

Verifying Active Directory Schema for SFU Using LDAP Browser

Click on a user for example cmuser1 in the Softerra LDAP Browser and observer the UNIX Schema.

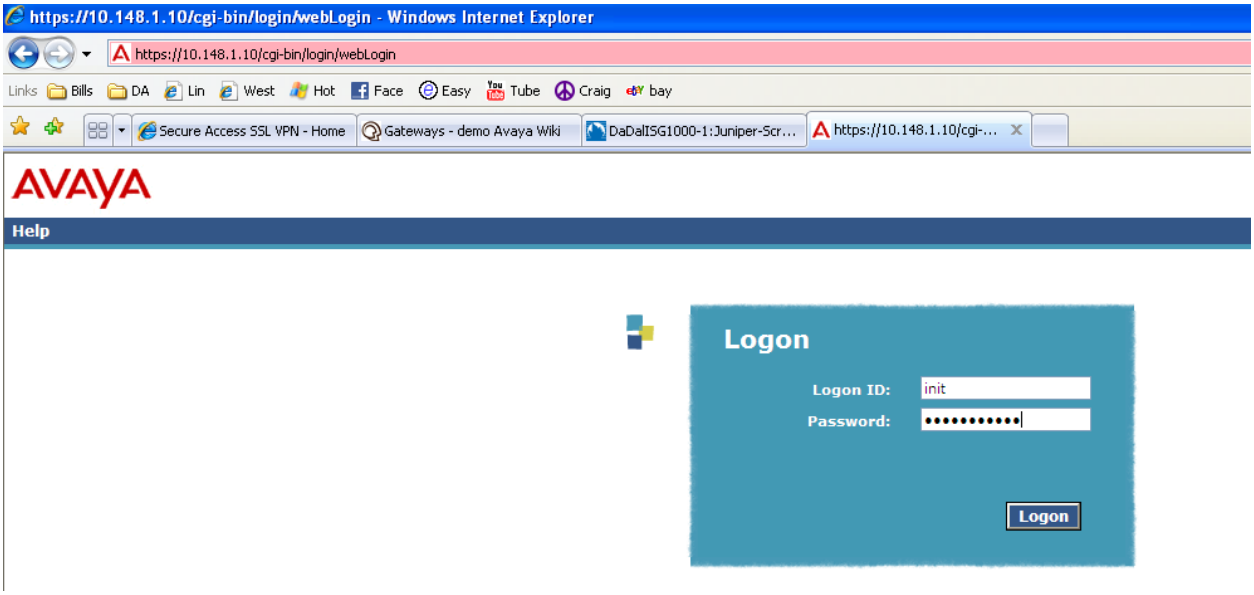


We can deduce that we are using the **msSFU30** schema for UNIX Services, this will come into play later when we configure the CM UNIX for LDAP Authentication.

Preparing the CM for LDAP Authentication

In order for the CM to send/receive LDAP User authentication requests, we have to ALLOW AD ports in the CM Firewall.

Web into the CM using the *init* login.



Click **Launch Maintenance Web Interface**

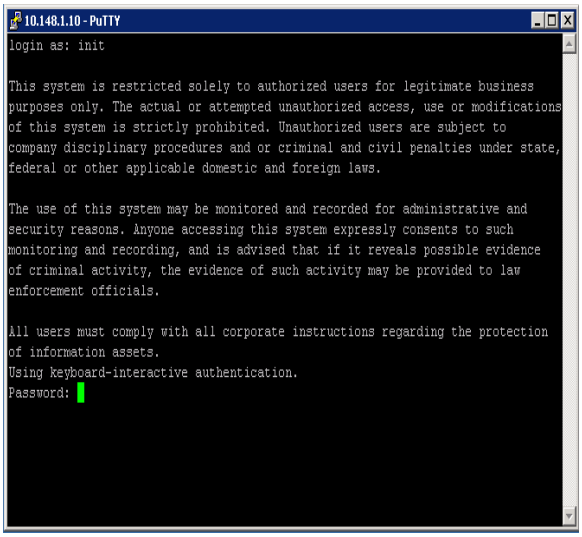
Under **Security**, click on **Firewall,** check the ldap port tcp389 to ALLOW

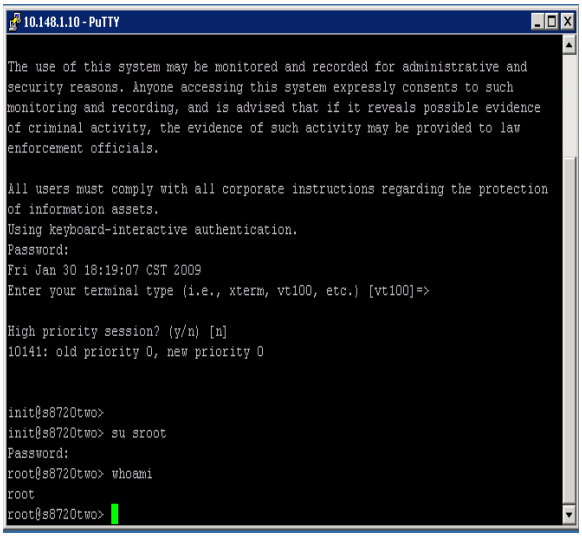


Configuring the Avaya CM for LDAP Active Directory User Authentication

We will need to manipulate four files in total. We will need puTTY or any other SSH client and network connectivity to the CM including the init credentials.

Using PuTTY, or any SSH capable client, SSH into the CM SHELL using the *init* user. su to *sroot* user as shown and type the root password (default is **sroot01**), type whoami to confirm that you are **root** on the machine.





First file we need to manipulate is **mv-auth** file which is located in the **/etc/pam.d** directory.
cd to /etc/pam.d directory by typing **cd /etc/pam.d**

vi mv-auth file

```
root@s8720two> vi mv-auth
# <MESA:01:@(#):MdrcesfPgfX0:r6:43.1.12.1:20061222100700:drces:1 42 63101:MESA>
#%PAM-1.0

auth       required     /lib/security/pam_env.so
auth       required     /lib/security/pam_tally.so unlock_reset deny=5 unlock_
time=600
auth       required     /opt/ecs/lib/pam_root_login.so
auth       sufficient   /lib/security/pam_asg.so

# External AAA uncomment as and when needed
# auth      sufficient   /lib/security/pam_radius_auth.so use_first_pass
#auth       sufficient   /lib/security/pam_ldap.so use_first_pass
#auth       sufficient   /lib/security/pam_safeword.so use_first_pass
#auth       sufficient   /lib/security/pam_securid.so use_first_pass

auth       sufficient   /lib/security/pam_unix.so  try_first_pass
auth       required     /lib/security/pam_deny.so

#
# Account modules
#
account    required     /lib/security/pam_unix.so
account    required     /lib/security/pam_access.so
#account    required     /lib/security/pam_time.so
account    required     /lib/security/pam_tally.so

# External AAA uncomment as and when needed
#account    sufficient   /lib/security/pam_localuser.so
#account   [default=die success=ok user_unknown=ignore service_err=ignore authin
fo_unavail=ignore]      /lib/security/pam_ldap.so
#account    sufficient   /lib/security/pam_radius.so
#account    required     /lib/security/pam_access.so

#
# Password modules
#
password   sufficient   /lib/security/pam_asg.so
password   required     /lib/security/pam_cracklib.so retry=3 minlen=6
password   sufficient   /lib/security/pam_unix.so use_authtok

# External AAA uncomment as and when needed
#password   sufficient   /lib/security/pam_ldap.so use_authtok
password   required     /lib/security/pam_deny.so


#
# Session modules
```

```
#
#session      required     /lib/security/pam_limits.so
#session     required     /lib/security/pam_lastlog.so never
#session     required     /lib/security/pam_motd.so
session     required      /lib/security/pam_unix.so
~
# auth      sufficient    /lib/security/pam_radius_auth.so use_first_pass
#auth       sufficient    /lib/security/pam_ldap.so use_first_pass
#auth       sufficient    /lib/security/pam_safeword.so use_first_pass
#auth       sufficient    /lib/security/pam_securid.so use_first_pass

auth        sufficient    /lib/security/pam_unix.so  try_first_pass
auth        required      /lib/security/pam_deny.so

#
# Account modules
#
account     required      /lib/security/pam_unix.so
account     required      /lib/security/pam_access.so
#account    required      /lib/security/pam_time.so
account     required      /lib/security/pam_tally.so

# External AAA uncomment as and when needed
#account    sufficient    /lib/security/pam_localuser.so
#account   [default=die success=ok user_unknown=ignore service_err=ignore
authinfo_unavail=ignore]       /lib/security/pam_ldap.so
#account    sufficient    /lib/security/pam_radius.so
#account    required      /lib/security/pam_access.so

#
# Password modules
#
password    sufficient    /lib/security/pam_asg.so
password    required      /lib/security/pam_cracklib.so retry=3 minlen=6
password    sufficient    /lib/security/pam_unix.so use_authtok

# External AAA uncomment as and when needed
#password   sufficient    /lib/security/pam_ldap.so use_authtok
password    required      /lib/security/pam_deny.so


#
# Session modules
#
#session      required     /lib/security/pam_limits.so
#session     required     /lib/security/pam_lastlog.so never
#session     required     /lib/security/pam_motd.so
session     required      /lib/security/pam_unix.so
~
```

Save this file just in case you need to revert your changes back by typing:

cp mv-auth mv-auth-old

Replace the contents of the OLD mv-auth file with the following, you can use VI to do this or create it in a windows box as a TXT document and copy it over to the CM.

NEW mv-auth file:

```
auth        required      /lib/security/pam_env.so
auth        required      /lib/security/pam_tally.so unlock_reset deny=5 unlock_time=600
auth        required      /opt/ecs/lib/pam_root_login.so
auth        sufficient    /lib/security/pam_asg.so

# External AAA uncomment as and when needed
auth        sufficient    /lib/security/pam_ldap.so  try_first_pass
auth        sufficient    /lib/security/pam_unix.so  try_first_pass
auth        required      /lib/security/pam_deny.so

#
# Account modules
#
account     required      /lib/security/pam_unix.so
account     required      /lib/security/pam_access.so
account     required      /lib/security/pam_tally.so

# External AAA uncomment as and when needed
account    sufficient    /lib/security/pam_localuser.so
#account           required      /lib/security/pam_ldap.so
account   [default=die success=ok user_unknown=ignore service_err=ignore
authinfo_unavail=ignore]       /lib/security/pam_ldap.so

#
# Password modules
#
password    sufficient    /lib/security/pam_asg.so
password    required      /lib/security/pam_cracklib.so retry=3 minlen=6
password    sufficient    /lib/security/pam_unix.so use_authtok md5

# External AAA uncomment as and when needed
password   sufficient    /lib/security/pam_ldap.so use_authtok
password    required      /lib/security/pam_deny.so

#
# Session modules
#
session         required        /lib/security/pam_mkhomedir.so
session     required      /lib/security/pam_unix.so
~
```

Notice the contents of the new mv-auth file highlighted in bold allow the CM to first look at the User credentials in an outside LDAP server and then it goes to the internal UNIX logins created locally on the CM, lastly it denies anything that does not fit those two choices.

Second and third file that needs to be modified is the *ldap.conf* file, this is located in two locations: under the **/etc** directory and under the **/etc/openldap** directory.

type **cd /etc**
vi ldap.conf
this is the original content of the ldap.conf file:

root@london8500> vi ldap.conf
#
 # LDAP Defaults
#

 # See ldap.conf(5) for details
 # This file should be world readable but not world writable.

#BASE dc=example, dc=com
#URI ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT 12
#TIMELIMIT 15
#DEREF never
HOST 127.0.0.1
BASE dc=example,dc=com

Copy this file as a backup if you need to revert your changes back just like before by typing

cp ldap.conf ldap.conf-old

Type cd /etc/openldap
backup the ldap.conf file (this is the same file as before)

cp ldap.conf ldap.conf-old

vi both ldap.conf files in the two locations (/etc and /etc/openldap) and copy the new contents as follows:

uri ldap://10.148.1.69 ##IP ADDRESS OF THE AD SERVER##
base dc=testdomain,dc=com
ldap version 3
binddn cn=ldapadmin,cn=Users,dc=testdomain,dc=com
bindpw Avaya123!
scope sub
timelimit 10
ssl off
nss_base_passwd cn=Users,dc=tesdomain,dc=com

nss_base_shadow cn=Users,dc=tesdomain,dc=com
nss_base_group cn=Users,dc=testdomain,dc=com
nss_map_objectclass posixAccount user
nss_map_objectclass shadowAccount user
nss_map_attribute uid sAMAccountName
nss_map_attribute uidNumber msSFU30UidNumber
nss_map_attribute gidNumber msSFU30GidNumber
nss_map_attribute loginShell msSFU30LoginShell
nss_map_attribute gecos name
nss_map_attribute userPassword msSFU30Password
nss_map_attribute homeDirectory msSFU30HomeDirectory
nss_map_objectclass posixGroup Group
nss_map_attribute uniqueMember msSFU30PosixMember
nss_map_attribute cn cn
pam_login_attribute sAMAccountName
pam_filter objectclass=user
pam_member_attribute msSFU30PosixMember
 # pam_groupdn cn=susers,cn=Users,dc=demotest,dc=com
pam_password ad

 # this is the /etc/ldap.conf file for the CM side of active directory

Notice the *nss_map_attributes* highlighted in bold on the new ldap.conf file, they should correspond with the UNIX schema found via the Softerra LDAP Browser. Also, notice the use of the *ldapadmin* account and the password in the file as well.

Lastly, we need to modify the **nsswitch.conf** file which is located in the **/etc** directory.

cd /etc
vi nsswitch.conf

I am omitting the full output of the vi, but there should be three lines in that file which will look like

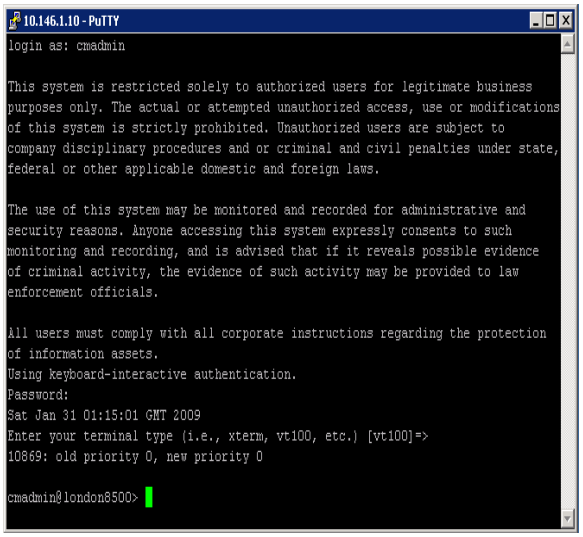
passwd: files
shadow: files
group: files

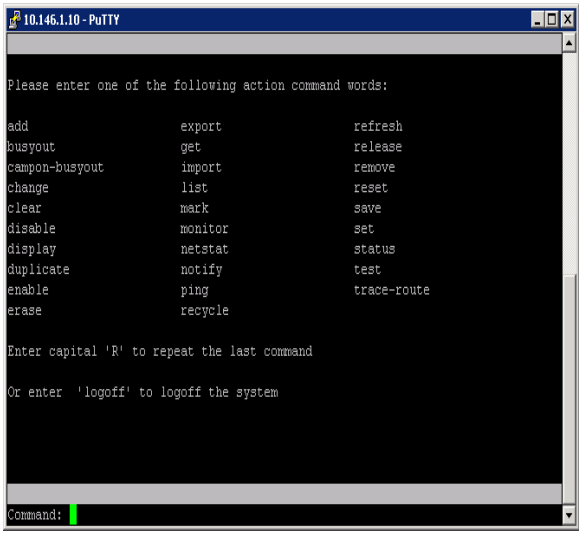
change these lines to look like

passwd: files ldap
shadow: files ldap
group: files ldap

Logging into the CM using Active Directory Users

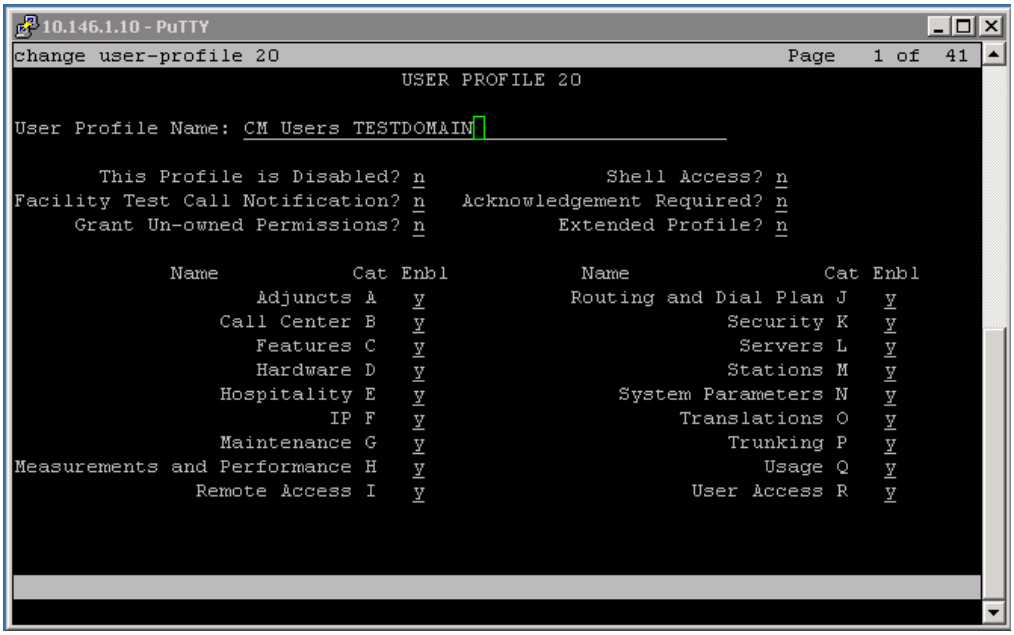
Log into the CM using PuTTY or any other SSH client on port 22. First use the *cmadmin1* user and password. It will log you into the BASH SHELL. You can type autosat at the prompt to go to the SAT Terminal and select the terminal of your choice (i prefer W2KTT). Type **help** and you will see a list of all command:



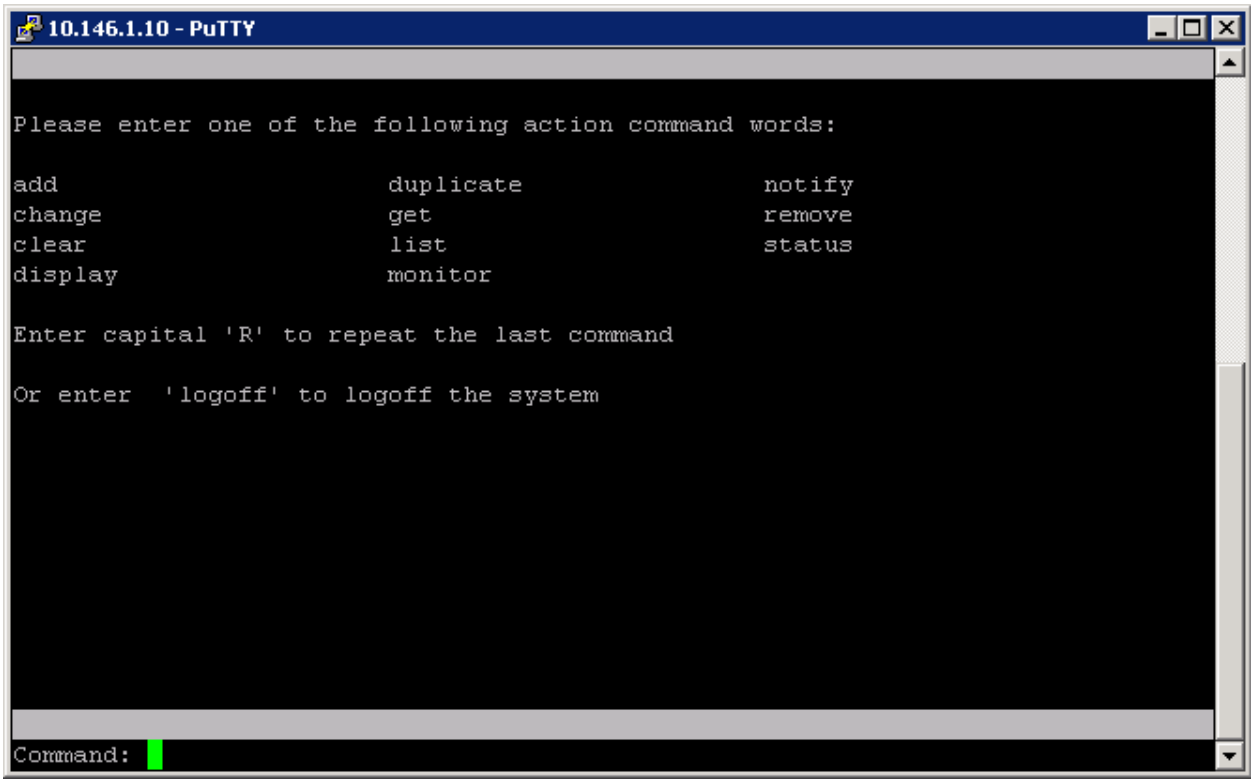


Hence you have full admin privileges to this CM including SHELL access.

Create a user-profile in CM by typing **change user-profile 20** (for user prof20), set this profile to ONLY allow read access to everything. Hit ESC-E to ENTER (this is in the W2KTT terminal, if you selected a different terminal, this will be different).



Log out of the CM and log back in using cmuser1 user, use SSH and port 5022 (default SAT port). It will take you directly to the SAT terminal without going to the SHELL. type **help**



You will notice that now you have only a limited number of commands to the CM since this is a non-admin user.

For any questions, please contact the author by way of email at ameer@avaya.com