

# Authenticating Ubuntu via Active Directory with Samba/Winbind

(CISS-150 William Jojo)

Make sure your IP address is static on Ubuntu and not set for DHCP. If the address changes or you have a short lease, the IP address will change and so will `/etc/resolv.conf` which will render this procedure useless even during the setup.

- Install the following packages:  

```
sudo apt-get install openssh-server
sudo apt-get install samba samba-common samba-doc
sudo apt-get install winbind krb5-user
sudo apt-get install slapd ldap-utils
```

*Choose and admin password and confirm if prompted for slapd*
- Reconfigure LDAP slapd:  

```
sudo dpkg-reconfigure slapd
```

*Choose no for Omit OpenLDAP server configuration*  
*Set the DNS Domain name (can be the same as the AD domain)*  
*Choose an Organization name.*  
*Enter and confirm admin password. You will need this later!*  
*Select Ok for Database configuration*  
*Select BDB.*  
*Select yes for database removal on purge.*  
*Select yes for move old database if asked.*  
*Select no for Allow LDAPv2 protocol.*
- Setup schema data for LDAP:  

```
sudo cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema
sudo gzip -d /etc/ldap/schema/samba.schema.gz
```
- Edit `/etc/ldap/slapd.conf` (add lines under existing includes):  

```
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/samba.schema
```
- Restart LDAP  

```
sudo /etc/init.d/slapd restart
```

- Create data file to make a container for IDMAP data:  

```
sudo gedit /tmp/ou.ldif
```

*(add the following lines)*  

```
dn: ou=idmap,dc=mothra,dc=local
objectclass: organizationalunit
ou: idmap
```
- Load the container into LDAP:  

```
ldapadd -x -D cn=admin,dc=mothra,dc=local -W -f /tmp/ou.ldif
```

*Enter ldap admin password you setup earlier.*
- Stop samba services:  

```
sudo /etc/init.d/samba stop
sudo /etc/init.d/winbind stop
```
- Create new `/etc/samba/smb.conf` (make sure this reflects *your* domain data):  

```
[global]
workgroup = MOTHRA
security = ADS
encrypt passwords = yes
realm = MOTHRA.LOCAL
client use spnego = yes
winbind separator = +
log level = 2
interfaces = 192.168.153.129/24
wins server = 192.168.153.131
winbind enum users = yes
winbind enum groups = yes
template shell = /bin/bash
ldap admin dn = cn=admin,dc=mothra,dc=local
idmap domains = MOTHRA
idmap config MOTHRA:default = yes
idmap config MOTHRA:backend = ldap
idmap config MOTHRA:ldap_base_dn = ou=idmap,dc=mothra,dc=local
idmap config MOTHRA:ldap_user_dn = cn=admin,dc=mothra,dc=local
idmap config MOTHRA:ldap_url = ldap://127.0.0.1/
idmap config MOTHRA:range = 200000-500000
idmap alloc backend = ldap
idmap alloc config:ldap_base_dn = ou=idmap,dc=mothra,dc=local
idmap alloc config:ldap_user_dn = cn=admin,dc=mothra,dc=local
idmap alloc config:ldap_url = ldap://127.0.0.1/
idmap alloc config:range = 200000-500000
```

```
[netlogon]
path = /netlogon
```
- Check Samba configuration:  

```
sudo testparm -v
```

*(look for warnings or errors)*

- Configure Samba to know about the LDAP admin password:  

```
sudo smbpasswd -w ldapadminpass
sudo net idmap secret MOTHRA ldapadminpass
sudo net idmap secret alloc ldapadminpass
```
- Create a new `/etc/krb5.conf` to configure the default realm and the Key Distribution Center server (*make sure this reflects **your** domain data*):

```
[libdefaults]
    default_realm=MOTHRA.LOCAL

[realms]
    MOTHRA.LOCAL = {
        kdc = 192.168.153.131
    }
```

- Double check your `/etc/resolv.conf` that it shows the W2k3 server ip address and the correct domain name.
- Add to `/etc/hosts` (*make sure this reflects **your** domain data*):  

```
192.168.153.131 w2k3svr.mothra.local w2k3svr
192.168.153.129 ubuntu.mothra.local ubuntu
```
- Make sure the Windows 2003 server and Ubuntu times are in sync:  

```
sudo ntpdate w2k3name
```
- Get s Kerberos ticket:  

```
sudo kinit administrator
```

*Enter password of w2k3 server.*
- Attempt to join Samba to Active Directory  

```
net ads join -U administrator@MOTHRA.LOCAL
```
- Edit `/etc/pam.d/common-auth` (add **before** `pam_unix` line):  

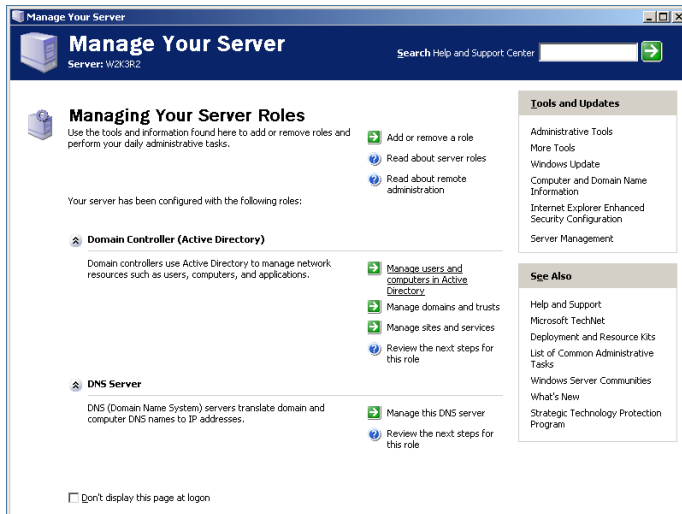
```
auth sufficient    pam_winbind.so
```

*(add use\_first\_pass to end of pam\_unix line)*

- Edit `/etc/pam.d/common-account` (add **before** `pam_unix` line):  
`account sufficient pam_winbind.so`  
*(add `use_first_pass` to end of `pam_unix` line)*
- Edit `/etc/pam.d/common-session` (add **after** `pam_unix` line):  
`session required pam_mkhomedir.so umask=0022 skel=/etc/skel`
- Edit `/etc/nsswitch.conf`:  
*Add winbind to the end of the password and group lines.*
- Start samba services:  
`sudo /etc/init.d/samba start`  
`sudo /etc/init.d/winbind start`
- Check users and groups are retrieved by winbind:  
`wbinfo -u`  
`wbinfo -g`
- Check users and groups appear to system:  
`getent passwd`  
`getent group`
- Check that Samba is storing SID mapping in LDAP (*make sure this reflects **your** domain*):  
`ldapsearch -x -D cn=admin,dc=mothra,dc=local -W -b dc=mothra,dc=local "(sambasid=*)"`
- Test ssh to local system:  
`ssh mothra+username@localhost`  
*(Enter password of user from Active Directory)*
- Look for the home directory to be created:  
`ls -al /home/MOTHRA/username`

If you can login to Ubuntu via ssh with an Active Directory user, this portion is complete.

# Configuring Active Directory Users to Retrieve Roaming Profile from Samba



On the Windows 2003 server, from the Manage Your Server window, select **Manage Users and Computers in Active Directory**.

Illustration 1: Manage Your Server window.

Select the **Users** folder, then right click on a user and select **Properties**.

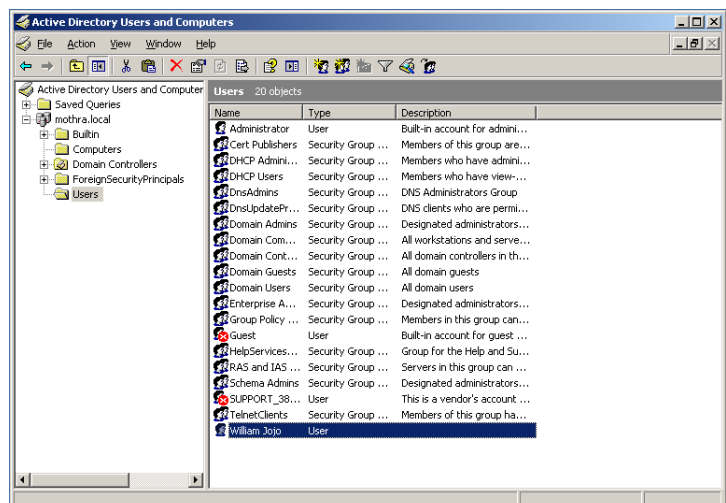
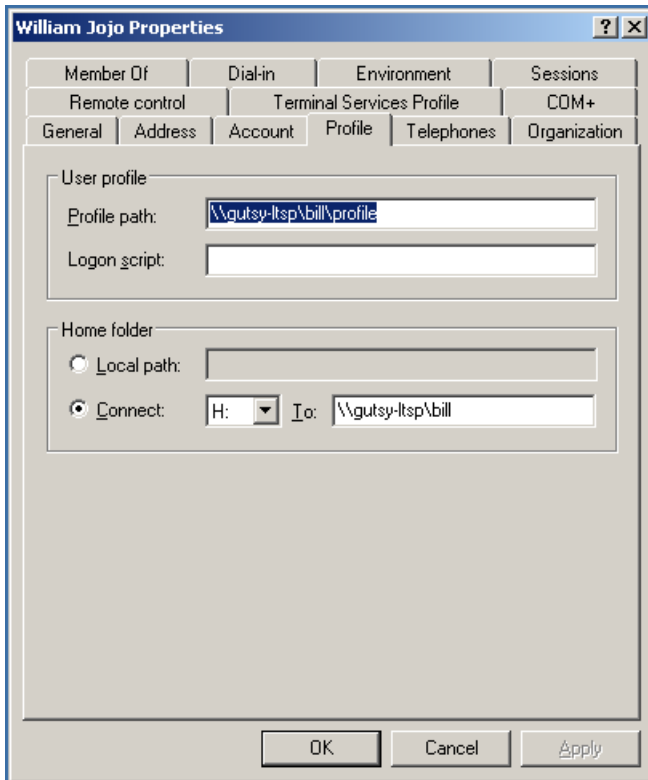


Illustration 2: Selecting a user from the Users folder.



Enter the **Profile path** as

**\\*ubuntuserver*\*username*\profile** where *ubuntuserver* is the name of the Samba server and *username* is the name of the Windows user.

Select **Connect** and a drive letter (H:) and enter the **To** value as **\\*ubuntuserver*\*username***.

You will likely get a message about access to the server. You can simply select **OK**.

Select **OK**.

*Illustration 3: Setting up the profile path and home folder.*

- On Ubuntu, Edit `/etc/samba/smb.conf` and add the following new section:

```
[homes]
    comment = Home Directories
    read only = no
    path = %H
```

- Log on to Windows XP with a user in the Active Directory domain. If successful, logout.
- On Ubuntu determine if the profile roamed by looking in the directory:  
`ls -al /home/MOTHRA/username/profile`