

Setting up your Active Directory Environment

8/2008

Join Active Directory as a Delegated OU

The first step in using Active Directory is to fill out a form to join as a Delegate Organizational Unit.

<http://www.umich.edu/~lannos/windows/central-accounts-JoinForestAsOU.html>

The Bootstrap Computer

The bootstrap computer is specified in your request for an Organizational Unit above and should follow the naming convention DEPT-ANYTHING. It needs to be joined to the domain and configured to access and administer Active Directory before you can add additional computers and servers or manage users, groups and other objects in Active Directory. The bootstrap computer can be any modern Windows computer such as XP, Vista, or a Windows 2003 Server. (It could also be a Window 2008 server. We don't currently support that configuration although it should work.)

The simplest solution today is to use a Windows 2003 R2 Server because it can serve multiple purposes:

- Active Directory Management Server
This server can contain all the Active Directory Management tools you need to manage your environment. All your administrators can then access this server with their OU Admin credentials using Remote Desktop so they don't need to install them on all their desktops.
Note: Only two admins can connect to Remote Desktop at a time unless you install Terminal Services.
- File Server, Application Server or Whatever
In a single server or multiple server environment, you can run your applications on this same server or servers.

If you choose to install your Active Directory tools on a workstation(s), there are several things to keep in mind:

- Do not logon to your workstation as an OU Admin. This is a bad security practice.
- Logon as a regular user and then use the "Run As" function to launch the necessary tools which your OU Admin credentials.

Once you installed Active Directory tools on any other computer in your OU, the bootstrap computer is no longer important and can be kept or deleted as you choose. You can administer AD from servers, workstations or both.

Join the Bootstrap Computer to the Domain

- Go to Control Panel > System > Computer Name. Select Change button.
- Make sure the computer name exactly matches the bootstrap computer name in your request.
Note: If you need to change the computer name, make this change and reboot before proceeding.
- Test that you can ping the domain, **adsroot.itcs.umich.edu**.
- Select Member of domain radio button and enter **adsroot.itcs.umich.edu**.
- When prompted, enter *your* OU Admin username and password with the following format: **umroot\dept-ouadminN**, where N=1,2,3 etc., and dept is your assigned department/unit prefix.
- You should see a “Welcome to the UMROOT Domain” message and then reboot.

Administrator Configuration

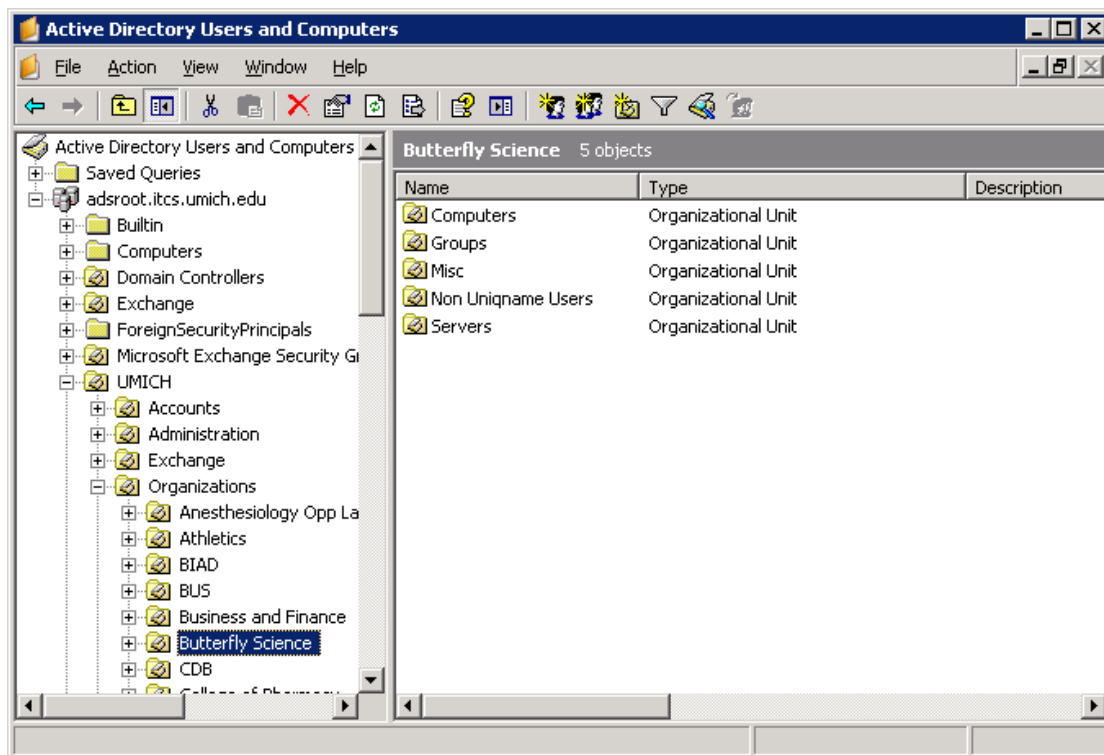
- Change **Log on to** drop down menu to **DEPT-ANYTHING (this computer)** and logon as **Administrator**. This is the local Administrator account you created when installing the computer OS, not your OU Admin account.
- Start > Administrative Tools > Computer Management.
Select Local Users and Groups
Select Groups
Select Administrators
Select Add...
Enter *your* OU Admins group, **umroot\dept-ouadmins** and select Check Names
Exit Computer Management.
- Logoff
- Change **Log on to** drop down menu to **UMROOT** and this time logon as *your* OU Admin account, **umroot\dept-ouadminN**. You will now be logged onto the server as a Local Administrator and to the domain as your department/unit OU Admin.

Install Active Directory Tools

- Download and install the correct Active Directory Administration Tools for your Operating System. See Appendix for a list of current downloads.
- (Optional) Download and install the Group Policy Management Console with Service Pack 1.
<http://www.microsoft.com/downloads/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&DisplayLang=en>
- (Optional) Download and install Windows Server 2003 Service Pack 2 32-bit Support Tools.
<http://www.microsoft.com/downloads/details.aspx?FamilyID=96a35011-fd83-419d-939b-9a772ea2df90&DisplayLang=en>

Start Managing Active Directory

- Start > Administrative Tools > Active Directory Users and Computers.
- Navigate to UMICH > Organizations > Your_OU
- Create top level OUs for:
 - Users
 - Groups
 - Servers
 - Computers
- Most units create some or all of the following top level OUs. You can browse other departments OUs to see what they have done.
- (Optional) You can now drag your bootstrap computer to the correct OU.
- See Active Directory 101 documentation for more information.



Appendix – Active Directory Administration Tools

Window 2003 R2

- Windows 2003 R2 Administration Tools Pak for x86
<http://www.microsoft.com/downloads/details.aspx?FamilyID=9bfb44f5-232a-4fb5-bc14-45bfd81b7ac1&DisplayLang=en>
- Windows 2003 R2 Administration Tools Pak for x64
<http://www.microsoft.com/downloads/details.aspx?FamilyID=8f7df3a5-e738-44b4-91eb-4907511f87c6&DisplayLang=en>

Windows 2003 SP2 and XP

- Windows Server 2003 Service Pack 2 Administration Tools Pack for x86 editions
<http://www.microsoft.com/downloads/details.aspx?familyid=86B71A4F-4122-44AF-BE79-3F101E533D95&displaylang=en>
- Windows Server 2003 Service Pack 2 Administration Tools Pack for x64 editions
<http://www.microsoft.com/downloads/details.aspx?FamilyID=514bd06e-f3bc-4054-8429-c49f51e2190b&DisplayLang=en>

Vista

- Microsoft Remote Server Administration Tools for Windows Vista (KB941314)
<http://www.microsoft.com/downloads/details.aspx?FamilyID=9ff6e897-23ce-4a36-b7fc-d52065de9960&DisplayLang=en>
- Microsoft Remote Server Administration Tools for Windows Vista for x64-based Systems (KB941314)
<http://www.microsoft.com/downloads/details.aspx?familyid=D647A60B-63FD-4AC5-9243-BD3C497D2BC5&displaylang=en>