

# Active Directory Users, Groups and OUs

8/2008

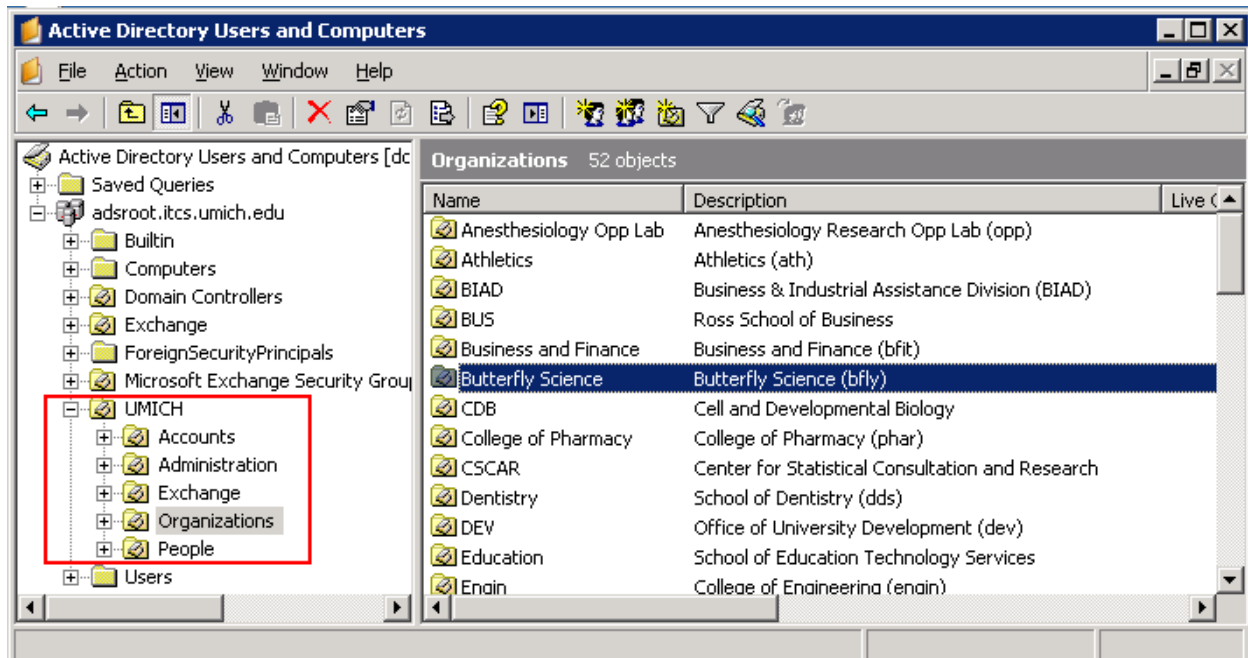
## Organizational Units (OUs)

OUs are containers that hold other AD objects. They have 3 main purposes:

- Visually organize objects.
- Different Group Policies can be assigned to different OUs.
- Permissions can be delegated to different OUs so they can be managed by a subset of administrators.

Unlike some other systems, OUs are not security principles so that that you cannot assign a common set of permissions to all the users in an OU. You can only assign permissions to users and groups.

## UMROOT OUs



## People OU

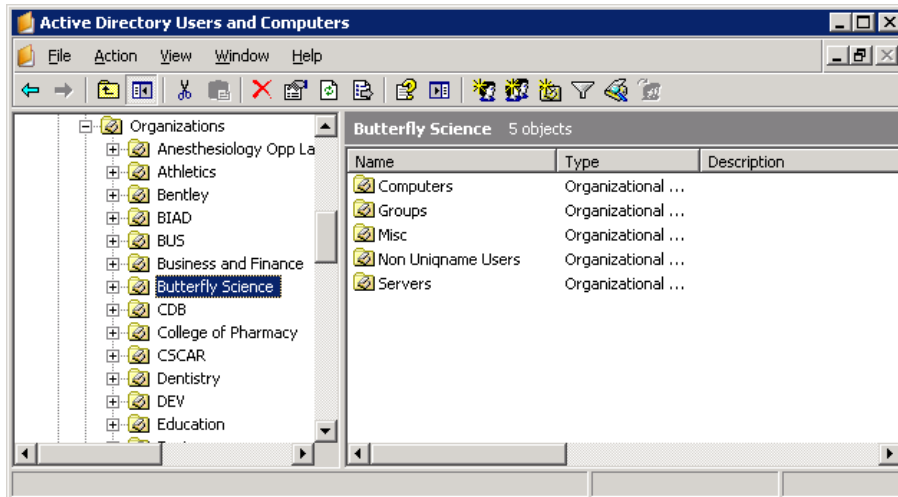
The People OU contains a synchronized copy of all the users in the U-M Online Directory so you don't need to create any unique user accounts. There are several ways to manage these users that will be

explained below. There are currently approximately 300,000 users in the People OU.

Note: Passwords are NOT the same as the user's Kerberos passwords and needs to be set. See below.

## Organizations OU

Each unit that joins Active Directory will have an Organizations OU.



Unit administrators can create additional OUs, computers and server objects, groups, and non-unique name users and in their Organizations OU. All objects except OUs must conform to the naming conventions of **dept-whatever**.

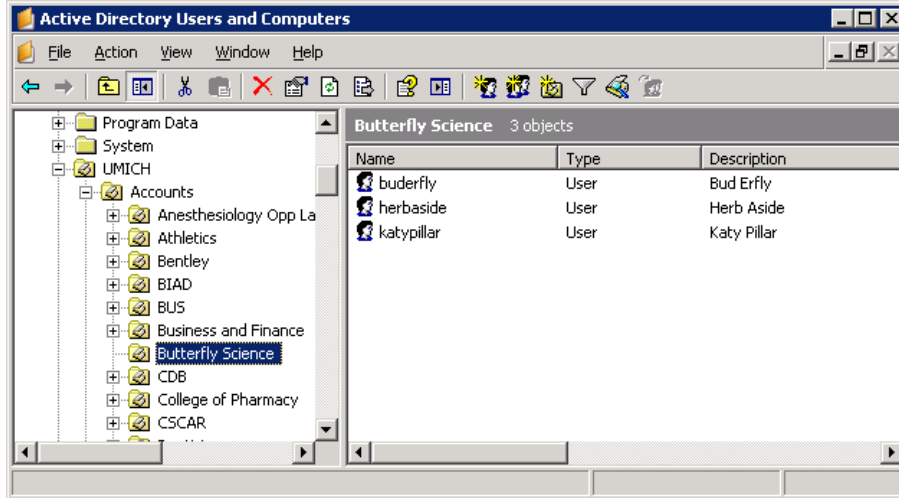
You are not allowed to create user objects with unique names or using the unique name naming convention of 3-8 alphabetic characters. You must create user objects that follow the above naming convention. For administrative accounts there is an exception that allows you to add a number to the end of a unique name to create a user name.

Group Policies can be applied to your Organizations OU or any of the sub OUs.

## Accounts OU (Optional)

Each unit that joins Active Directory will have an Accounts OU. Using this OU is optional and many units will choose to not use it to simplify their administration.

A more complex and detailed use of these users and their attributes can be accomplished by choosing to fully manage your users. In many cases, this is unnecessary and extra work. See the following for an explanation. <http://www.umich.edu/~lannos/windows/central-accounts.html>



## Managing Users

All users with uniqnames are already provisioned in the People OU of Active Directory. You can manage many aspects of these users without needing to manage the users in your Accounts OU.

- User's can reset their own passwords using a web page if they know their Kerberos password.
- Users can be added by OU Administrators to groups you create in your Organizations OU.
- Permissions can be assigned by OU Administrators to your resources to any users, although we recommend always applying permissions to groups.
- Group Policies, including Logon Scripts, can be applied by OU Administrators to any users logging onto your computers by using Loopback Policies.
- Exchange mailboxes can be assigned to any user by ITCOM Admins if you are a Full Serve Exchange unit.

## Resetting Passwords

- User can access web page: <https://accounts.itcs.umich.edu/kpasswd-bin/kpasswd.cgi>
- Select Windows Active Directory tab at top.
- Enter Kerberos uniqname and password
- Enter a new Windows Active Directory password.  
Note: Password restrictions are more stringent than Kerberos. See the instructions on the web page. Although it is not the best security, users may want to use the same password in Kerberos and Windows.
- Users should always log on to Windows resources using the following format:  
**umroot\uniqname**

## Managing Groups

It is best to assign permissions to groups rather than individuals. As an OU Admin, you can create Security Groups, add users, and then assign permissions to resources. To create groups:

- Using Active Directory Users and Computers, navigate to your OU and then to the Groups OU.
- Right click and select New Group. The default Global Security Group is fine for most purpose.
- Enter the group name which must follow one of the two naming conventions:
  - **unit-any-thing** using AD prefix assigned to your unit when you requested your OU:  
example: hsg-assistants
  - **Unit Any Thing**  
example: Housing Assistants  
This type of group is better suited if you plan on using Exchange and want to use the group as a distribution list and have it show up in the Global Address List.
- Don't mail enable the group unless you are using the ITCS Exchange service. See <http://www.itd.umich.edu/exchange/> for more info.
- Open the newly created group and add members.
- Assign permissions to group. This step depends on what permissions you want to give the group.