IOWA STATE UNIVERSITY
IT Services Technical Notes

IT

Windows Enterprise
OU Administrator Policy and Procedures
Creating a Departmental Sub-OU and Delegating Full Control

Steven L. Kunz
September 6, 2002

This document describes how to create a "sub-OU" within your departmental OU and delegate full control to a group of individuals.

IMPORTANT: You should only do this when you want to apply different security policy to objects in the OU. A "deep" OU tree created without a reason (i.e. "just because that is the way we are organized" without group policy application) results in increased login and access control times.

IMPORTANT: It is VERY IMPORTANT that the "security rights" for whatever OU you move NetID-based user objects into be correct. You MUST NOT lock out enterprise "Administrators" access in an OU where university information (and passwords) must be synchronized from the enterprise level. Specifically:

1) The "IASTATE/Administrators" group must have full rights to objects in the "<your OU>/Users" container to add/update/delete the NetID-based user objects that were placed there when your faculty/staff were populated into your OU.
2) If you move NetID-based user objects from "<your OU>/Users" to another OU within your OU, you must remember to grant the "IASTATE/Administrators" group full rights to objects in that container, also, or updates will break.

Instructions to Create a "Sub-OU" Within an OU You Manage

Assume your OU is named "MY OU"
Assume the new sub-ou is named "NEW OU"

Using "Active Directory Users and Computers":

1. LOG everything you do - so you can later see what you did and can undo something that may have gone wrong.
2. Right-click your OU ("MY OU") and pick "New->Organizational Unit"
3. Supply "NEW OU" for the name
4. Right-click the "NEW OU" OU, and pick "New->Group"
5. Supply "!NEW OU Admins" as the name and leave it the default "Global Security" group type.
6. Add Windows 2000 usersname to the membership of the "!NEW OU Admins" group.
7. Delegate full control of the new OU to the "!NEW OU Admins" group

- Under "Active Directory Users and Computers" make sure "View->Advanced" is checked
- Right-click the "NEW OU" OU and select "Properties"
- Click the "Security" tab
- Click the "Advanced" button
- Click the "Add" button
- Supply "!NEW OU Admins" for the "Name:" to "add"
- Check "Full Control" in the "Allow" column on the "Object" tab (Don't change any other settings)
- Check "Read All Properties" and "Write All Properites" in the "Allow" column on the "Properties" tab (Don't change any other settings)
- Click "OK" enough to close out all window

8. Get the full DNS hostname of the Windows 2000 system the initial OU administrator will use to administer the OU. The LEFTMOST term (everything to the left of the first ".") is the hostname you will use to "pre-create" the computer in the OU for the administrator.
9. Right-click the "NEW OU" OU and pick "New->Computer". Supply the hostname (not the full DNS name) for the system. IMPORTANT! Change the "The following user or group can join this computer to a domain" to indicate the "!NEW OU Admins" can do the function. Don't leave it the default ("Domain Admins") since very few people are "Domain Admins" (and they are all in AIT/ADP).
10. Supply (or tell the admin how to get) the AdminPak (in the I386 folder on the Windows 2000 Server CD) for Windows 2000 so they can manage the OU.

You (and your sub-OU admins) will have to both remember that as you add computers to your OUs, you will have to make sure the details in Step 8 are followed (or you won't be able to add the system to the proper place).