

# OU Manager's Handbook

## Tips for the ISU OU Manager

By the

Iowa State University  
Information Technology Services

# Table of Contents

Table of Contents .....	ii
About this Document .....	2
ISU Net-ID's .....	2
Using ISU Net-ID's on Your Systems .....	2
Key Concepts .....	3
Directory Services .....	3
Organizational Units (OU's) .....	3
Getting Started .....	4
Send a Request to Become OU Administrator .....	4
Getting Your Active Directory Tools .....	5
Server Administration Tools .....	5
Group Policy Management Console .....	6
Windows Vista and Windows 7 .....	6
Windows XP .....	6
Active Directory Enumerator .....	6
Adding Computers to Your OU .....	6
The First Computer in Your OU .....	6
Adding Other Computers to Your OU .....	8
An important word about system security .....	8
Managing Users in Your OU .....	9
Moving Your First Users into Your OU .....	10
New Users in Your Department .....	10
Users Transferring from Other Departments .....	10
Users Leaving Your OU .....	11
Managing ISU Net-ID User Objects .....	11
Special Net-ID Accounts .....	14
Local Accounts .....	15
Password Management .....	16
Password Changes .....	16
Why is it important to follow the naming conventions for usernames on local accounts? .....	16
Password Expiration .....	17
Security Groups and Mailing Lists .....	17
Creating Your Own Groups .....	17
Using Official University Lists as Security Groups .....	18
Using an ASW List as a Security Group .....	19
Using Mail Lists as Global Address List Contacts .....	19
Creating and Delegating in Sub-OUs .....	20
How Do I Create a Sub-OU? .....	20
How Do I Delegate Authority in a Sub-OU? .....	21
Changing OU Management .....	22
Using the ISU WSUS Server .....	22

Group Policy .....	24
Linking a Group Policy Object to Your OU .....	24
Creating Your Own Group Policy Objects .....	24
Activation of Windows Vista and Windows 7 .....	25
Key Management Service (KMS).....	28
Multiple Activation Key (MAK) .....	28
Appendix A -- Learning More .....	29
ITS Windows-related Websites .....	29
Windows Administrators Support Group .....	29
Microsoft Support Resources.....	29

## About this Document

This document is intended for use by Iowa State University computer support staff who plan to participate in the ISU implementation of Microsoft's Active Directory product. Those who participate in Active Directory can use campus Net-IDs and group policy to administer their computers and users. A wide variety of administration options are available.

The portion of Active Directory that you will administer is called an *Organizational Unit*. This term is universally abbreviated as "OU". In this document and most Microsoft documents, you will see OU referenced instead of "Organizational Unit".

This document contains all of the information you need to request an OU and to begin managing it. Additional information can be found in the many good trade publications.

## ISU Net-ID's

Nearly every student, faculty or staff member has an ISU Net-ID. New students are asked to register for a Net-ID during new student orientation. Most faculty and staff members have created a Net-ID in order to have an e-mail account.

A Net-ID is used in many ways. For example, you can use it to:

- Access your e-mail using Outlook, Entourage, Thunderbird or Outlook Web Access.
- Login to the ISU network using the secure VPN (virtual private network).
- Register computers and other networked devices on the campus network.
- Download site-licensed software from [www.sitelicensed.iastate.edu](http://www.sitelicensed.iastate.edu) and [software.iastate.edu](http://software.iastate.edu).
- Create campus-wide mail lists.
- Connect to campus AFS file servers using the OpenAFS client.
- Log in to computers in labs maintained by ITS and in many campus locations. Macs, Windows and UNIX systems are supported.
- Encrypt terminal sessions to participating UNIX systems.
- Charge printed output to your university bill in many computer labs.

## Using ISU Net-ID's on Your Systems

Computer administrators can also use ISU Net-ID's to authenticate users on computers that they manage. Once you have configured your computers, you will:

- Eliminate the need to create most user accounts on your systems. Your users can use their ISU Net-ID to login to Windows, Mac OS X and many UNIX systems.
- Be able to use Group Policy, SMS and SCCM to centrally manage most features of your Windows computers.
- Use campus Net-ID's and groups of Net-ID's to grant collaborators access to computers, file shares and printers.
- Retain the ability to solve common account problems for your faculty and staff. (For example, you can reset passwords.)

# Key Concepts

## ***Directory Services***

ISU uses directory services to store information about students, faculty and staff. Four directory types are in common use:

1. A Red Hat Directory Server acts as the authoritative directory server. This server is LDAP compliant and is used for any new LDAP-compliant applications. Among other things, this directory contains a record for every student, staff and faculty member.
2. Windows Active Directory (AD) is synchronized with the LDAP server and as such contains a record for every student, staff and faculty member. AD is used to administer workstations and printers and is also used as the user database for ISU's Microsoft Exchange mail servers.
3. Moira is our legacy UNIX directory service. It also contains a record for every student, staff and faculty member. Moira data is one of the key sources that helps build the LDAP directory. Since the Moira database is modified using Account Services on the Web (ASW) it is often referred to as the "ASW database".
4. NDS, Novell's directory service is used by departments with Novell servers and clients. It is possible to synchronize your NDS users with the LDAP directory service.

Directory service technology enables ISU to offer a single campus Net-ID. If you are administering Windows systems, you can use the directory services offered by Microsoft's Active Directory too.

## ***Organizational Units (OU's)***

The ISU Active Directory lets IT support personnel administer collections of people and computers called *Organizational Units (OU's)*. If you decide to use AD to administer your computers and clients, you will become an OU administrator.

OU's are organized along departmental and college political lines. An organizational chart for ISU would look very much like the ISU OU structure. When you apply to be an OU administrator, an OU will be created that matches your scope of responsibility.

OU setup is not difficult. The initial steps require that you:

1. Be named as the OU administrator for your department or group. This involves sending a request to an AD enterprise administrator.
2. Add your computers to your OU. You must specify which computers are joining the OU and then accept admission to the OU on each of the client systems. As soon as you admit a computer to your OU, you will be able to use the campus Net-ID to authenticate users on it.
3. Verify that the correct faculty and staff accounts have been automatically moved into your OU for you.
4. Create appropriate group policies to manage your newly created groups of users and computers.

## Getting Started

### ***Send a Request to Become OU Administrator***

The OU administrator should be the IT manager for a department, college or operating unit. The name of your OU will be assigned by enterprise domain management, and is the official “short abbreviation” of your unit. Your OU will be placed within the “college/major-operating-unit” OU according to the official university structure. For example, the English department OU is named “ENGL” and is within the LAS college OU.

To request an OU, send an email request with the following information to:

[w2k-root-admin@iastate.edu](mailto:w2k-root-admin@iastate.edu)

All requests should include the following items:

- 1) The name of your department.
- 2) The full DNS hostname of a Windows system (Windows XP, Windows Vista, Windows 7 or Windows Server 2003/2008) you will use to administer your OU.
- 3) Your name, position, and phone number

Your request will be handled as fast as time permits (generally a day or two). A short phone call is usually made to make sure all requests are handled properly. For example, your OU may really be a departmental sub-OU, with the request more properly handled by an existing departmental or college level OU administrator.

When your OU is created, the following things are done at the enterprise level:

- 1) The OU is created with the official university departmental short name.
- 2) A security group is created within the OU named “!**<your-OU-name> Admins**”. Your Net-ID is placed as the first member in that group.
- 3) Complete control for the OU is delegated to the security group created in the previous step. Members of this group can add/delete/change all objects, including users, computers, sub-OUs, and groups. Initially, this is only you, but you can extend this complete authority to anyone else you choose by making them a member of that security group.
- 4) The Windows administrative system you supplied will be “pre-created” in the ISU domain and placed in your OU. The ability to add/remove this computer from the domain will be delegated to the “!**<your-OU-name> Admins**” security group.
- 5) A **Users** container will be created in your OU. For the time being it will be EMPTY. DO NOT remove it. Eventually, you (and all your departmental users) will be placed in this container.

After your OU is created you will receive an email reply indicating it is ready for you.

## Getting Your Active Directory Tools

You should have four basic tools to administer your new OU:

1. One computer running Windows 7, Windows Vista SP1 (or higher), or Windows XP Professional SP1 (or higher). Add this computer to your OU using the instructions in the next section, entitled “The First Computer in Your OU”.
2. Either the Remote Server Administration Tools or the Windows 2003 Server Administration Tools (depending on your version of Windows), a collection of programs that enable you to manage your OU.
3. The Group Policy Management Console, a program which centralizes the various group policy management tools which came with Windows Server and places them in a single user interface.
4. The Active Directory Enumerator, a locally-written tool that can be used to easily view a large amount of information about Active Directory objects in a single window.

### Server Administration Tools

To install the Remote Server Administration Tools on Windows 7, download and follow the installation instructions at

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d>, or go to the Microsoft Download Center at <http://www.microsoft.com/downloads> and search for “Remote Server Administration Tools for Windows 7”. Note that there are separate downloads for 32-bit Windows (x86) and 64-bit Windows (x64); be sure to download the correct package for the version of Windows you are running. Read and follow the instructions on Microsoft’s page carefully, as simply installing the package won’t give you the tools; you must enable them in the Programs and Features control panel.

To install the Remote Server Administration Tools on Windows Vista 32-bit with Service Pack 1 or higher, download and follow the installation instructions at

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=9ff6e897-23ce-4a36-b7fc-d52065de9960>, or go to the Microsoft Download Center at <http://www.microsoft.com/downloads> and search for “Microsoft Remote Server Administration Tools for Windows Vista”.

To install the Remote Server Administration Tools on Windows Vista 64-bit with Service Pack 1 or higher, download and follow the installation instructions at

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=D647A60B-63FD-4AC5-9243-BD3C497D2BC5>, or go to the Microsoft Download Center at <http://www.microsoft.com/downloads> and search for “Microsoft Remote Server Administration Tools for Windows Vista for x64-based Systems”.

To install the Windows Server 2003 Active Directory tools on Windows XP SP1 (or higher) systems issue the command:

```
msiexec /i \\software.iastate.edu\OUmgr\ADTools2003\adminpak.msi  
ADDLOCAL=FeADTools /qb
```

Note that this command should be typed as a single line.

## **Group Policy Management Console**

The Group Policy Management Console (GPMC) is used to create and manage Group Policy objects and link them to OUs in the Active Directory. How it's installed depends on the version of Windows your administrative machine is running.

### **Windows Vista and Windows 7**

In Windows Vista and Windows 7 the Group Policy Management console is installed along with the Remote Server Administration Tools; however, it will not appear in the Administrative Tools control panel until you do the following:

1. Choose Start -> Control Panel -> Programs and Features -> Turn Windows features on or off.
2. Expand "Remote Server Administration Tools".
3. Expand "Feature Administration Tools".
4. Check "Group Policy Management Tools".
5. Click OK.
6. Close the Programs and Features window.

### **Windows XP**

The version of GPMC available to Windows XP is not as full-featured as later versions; you cannot, for example, change the owner of a group policy object. On the ISU campus you can install the Group Policy management console with the command:

[\\software.iastate.edu\OUMgr\gpmc\gpmc.msi](http://software.iastate.edu\OUMgr\gpmc\gpmc.msi)

### **Active Directory Enumerator**

The Active Directory Enumerator, written by Mark Bland of ITS, allows you to find out and modify (if you have sufficient privileges) information about an Active Directory user like groups belonged to, Exchange server, last password change, etc. in a single convenient user interface. It is available with documentation from [\\software.iastate.edu\OUMgr\AdToolsMisc\ADE](http://software.iastate.edu\OUMgr\AdToolsMisc\ADE).

If you are having trouble locating the Active Directory tools, contact OU support ([OUSupport@iastate.edu](mailto:OUSupport@iastate.edu)).

## **Adding Computers to Your OU**

Active Directory and the iastate.edu domain become accessible when you add computers to your new OU. You and your users will be able to login with their campus Net-ID as well as the local usernames. You will be able to manage these computers with group policy and other tools.

### ***The First Computer in Your OU***

The first computer in your OU will be the computer that you specified in your OU request. It is pre-added to your OU when your OU is created and is ready to become a member of your OU.

You must accept this membership at the console of that computer. To do so:

1. Logon as a local administrator-equivalent user on the system.
2. Check the system time and reset it if necessary. The system time must be within five minutes of the correct time, or the system will not be able to connect to the domain.
3. Right-click the **My Computer** icon and select **Properties**.
4. Click the **Network Identification** tab and select **Properties**.
5. Select **Domain** and enter `iastate.edu` as the domain.
6. You will be asked for the **name and password of an account with permission to join the domain**. Supply your campus Net-ID and password. (Your Net-ID has been given permission to add this computer to the IASTATE domain because it is a member of the **!<your-ou-name> Admins** group.)

## Adding Other Computers to Your OU

Each of the machines to be added to your OU will need a NetBIOS name and an IP number. The NetBIOS name is found in the properties of My Computer, under the Computer Name tab; click “Change” to change it. The NetBIOS name is arbitrary; it must be no more than fifteen characters long and must be unique on the IASTATE domain. An easy way to check a name’s uniqueness is simply to look it up in Active Directory Enumerator. If a machine with the same name exists, ADE will find a computer object and display its location in the Active Directory.

There are two ways to obtain an IP address:

1. An address can be obtained automatically via DHCP. While it is possible to simply connect a machine to the network, start a web browser and fill out the form that appears, it gives you better control to register a departmental machine manually in ASW.
  - a. Determine the machine’s MAC address. On the new machine, start a command prompt, and type “ipconfig /all”. Each network interface on the machine will display a “Physical Address” in the form “00-00-00-00-00-00”. Record this address with the machine’s NetBIOS name.
  - b. From your administrative machine, log in to <http://asw.iastate.edu>. You can do this with your regular Net-ID, but for continuity it’s best to log in with an administrative Net-ID obtained specifically for this purpose (see the section on “Special Net-ID Accounts” later in this document).
  - c. Choose “Campus IT Admin Functions”, then “Administer NetReg”, then “Add a Host”.
  - d. Fill out the form, including the following:
    - Ethernet Addr:** the physical address you found in step 1.
    - Hostname:** again an arbitrary name, but many areas use the NetBIOS name for the first section. The second section will automatically be set to the abbreviation for your department.
    - NAT Protected:** check this if you do not want the machine to be visible from outside the campus network; it will be assigned an IP address beginning with 10.24 or 10.25.
  - e. Click “Register System”.
2. For servers and other machines that need fixed IP addresses, you will need to apply for a static IP address.
  - a. From your administrative machine, log in to <http://asw.iastate.edu>.
  - b. Choose “Request for Services”, then “Domain Name Service (DNS)”, then “IP Request”.
  - c. Fill out the form.

### An important word about system security

Any computer you add to your OU should follow standard Windows security practices. Each computer should have the latest service packs and hotfixes. All local user accounts should have strong passwords (especially any accounts with administrative power). Antivirus and anti-spyware software should be installed with automatic updates and regular scans scheduled. Software firewalls (like the built-in Windows firewall) should be enabled. File shares that can be written by anyone without a strong password should never be used.

An easy way to perform a preliminary security check on each computer within your OU would be to run the “ISU Computer Inspector” on each computer. This product will run some basic checks and produce a report of any weaknesses found. Methods to correct the problem are provided by a web interface. Run the ISU Computer Inspector from this URL:

<https://asw.iastate.edu/cgi-bin/acropolis/inspect>

You will receive an IP address and other necessary information via e-mail.

Once you have obtained IP numbers and set the NetBIOS names of your computers, you are ready to pre-add them to your OU and the iastate.edu domain using your newly added Active Directory tools. Use the following steps to add a computer:

1. Locate the **Active Directory Users and Computers** management console in the **Administrative Tools** control panel.
2. Open the iastate.edu domain, and then open your OU.
3. Right-click your OU, then choose **New -> Computer**.
4. Enter the NetBIOS name that you set earlier under “Computer name”. Make sure that “Computer name (pre-Windows 2000) matches “Computer name”.
5. Click the **Change** button and change who can “*join this computer to a domain*”. Change the default Domain Admins to your “!*<your-ou-name>Admins*” security group. This is important both because you are not a Domain Admin and because only those that you specify can perform the task.
6. Click **Next**.
7. Skip the “managed computer” dialogue. Click **Next**, then **Finish**.
8. Repeat steps 3 through 7 for each computer that you are adding to the domain.

Once you have pre-added all of your computers to the Active Directory, you must visit each computer and accept membership in the iastate.edu domain in the same way as you did for the first computer you added to the domain. After each system is admitted to the “iastate.edu” domain, your users can login with their ISU Net-ID and password.

It is also possible to add computers with dialup or DSL connections to your OU. You may find such computers to be useful when you want to remotely administer your OU. These computers can be pre-added and accepted to your OU in almost the same way as your office systems. To login to the iastate.edu domain via dialup, select **login using a dialup connection** when you are logging in to your system.

## Managing Users in Your OU

Active Directory enables you to manage more than equipment. You can perform limited management of faculty and staff accounts. For example, you are able to set the Net-ID password for users in your OU; the change will occur in both Active Directory and ASW.

It’s important to know that there are two types of users that can appear in your OU:

### 1. ISU Net-ID User Objects

These users are associated with an ISU Net-ID. They are created when a person registers for an ISU Net-ID with the ASW “Register” function, and are the primary usernames used by people within the ISU enterprise. The ISU Net-IDs and their associated passwords are synchronized between Windows Active Directory and the enterprise Kerberos servers used by many other systems on campus (and managed through the ASW web interface). The account synchronization process creates and maintains the

Active Directory data for certain fields based on data from Human Resources and the Registrar's office.

Existing Net-ID users for your department will be moved into your OU on your request. When new people in your department register for Net-IDs, they will automatically be placed into your OU. Exception and administrative accounts created through the ASW "Request for Services -> Net-ID" process are placed into the OU of the requesting sponsor.

## 2. **Windows Exception User Objects**

Windows Exception users can be created directly by an OU manager using Windows Active Directory and Computers. They exist only in the Active Directory and are not associated with ISU Net-IDs at all. To avoid conflicts with existing and future Net-IDs, they must follow a special naming convention (names must begin with an exclamation point) but otherwise are under complete control of the OU manager.

### ***Moving Your First Users into Your OU***

When you are ready to start managing your users, send a request to Steve Kunz, [skunz@iastate.edu](mailto:skunz@iastate.edu). He will run an automated process that moves your faculty and staff to the **Users** container in your OU. Before he runs that process, he will send you a proof copy of the faculty and staff that will be moved. It is important to double-check this list. We have found a number of accounts that have been misclassified. It is important to resolve as many mistakes as possible before your faculty and staff are moved.

### ***New Users in Your Department***

New faculty and staff in your department are automatically placed in the **Users** container for your OU when they register for their Net-ID. You shouldn't need to do anything. Occasionally new users will wind up in the iastate.edu/Users container instead; if this happens, send mail to [w2k-root-admin@iastate.edu](mailto:w2k-root-admin@iastate.edu) and they can be moved to the correct location.

### ***Users Transferring from Other Departments***

Some faculty and staff may transfer to your department from another department and need to be placed in your OU. This activity can be handled by you and their former OU administrator. The container "iastate.edu/**Relocation**", a top-level object, is used to transfer the user object from one OU to another. You can see this container by opening **Active Directory Users and Computers** management console. All OU Admins have rights to move objects in and out of this container. Do the following:

1. Look in the iastate.edu/Relocation container to see if the user has already been moved there. Good administrators will move the users to Relocation as soon as they leave the department. If they're already there, skip to step 5.
2. Determine the OU that the user is currently in. The easiest way to do this is to look up the user's Net-ID in Active Directory Enumerator. The location of the user object is given under "Location"; the OU name is the section just before the final "Users". For

example, the user “sccconcl” is at the location “iastate.edu/ITS/Users/sccconcl”, so the user is in the ITS OU.

3. Determine the administrators of that OU.
  - a. Each OU is supposed to have a group named “!OUName Admins”. Search for that group in Active Directory Enumerator; the members of that group will appear in the “Members” field.
  - b. If that group does not exist, find the OU object in Active Directory Users and Computers. Right-click on it, choose Properties, then click the Security tab. Look for a group named “!OUName Admins” having Full Control permissions on that object. Look that group up in ADE and find the members of that group.
4. Send mail to the OU administrators explaining the situation and asking them to move the user object to the Relocation container.
5. Once the object has been moved to Relocation, open the iastate.edu/Relocation container in Active Directory Users and Computers, find the user object, and move it to your Users container.

### ***Users Leaving Your OU***

If someone in your OU leaves your department or the university do NOT delete or disable their Net-ID. Instead, do the following:

1. Using Active Directory Users and Computers, remove the user from any security groups you may have added them to. Any rights you’ve granted in this way will move with them to the new location, and you probably don’t want them to have access to your printers and machines.
2. Move the user object to the “iastate.edu/Relocation” container.
3. Send email to [w2k-root-admin@iastate.edu](mailto:w2k-root-admin@iastate.edu). In the email provide a list of the usernames you moved into the “Relocation” OU and why.

The users leaving your department will be moved back into the general user pool. You should NOT disable or delete these users. Net-ID policies allow even users who have left the university to have access to their online information for several months. Since they may come back as students or employees somewhere else in the university at a later date it is important that their login is available to them.

### ***Managing ISU Net-ID User Objects***

ISU Net-ID User Objects should be considered “owned by the enterprise.” They are created, altered, and inactivated when the user leaves the University by automated processes that are controlled by information in Human Resources and Registrar records. (For more complete information on this process, refer to “The Care and Feeding of ISU Net-IDs”, available from <http://www.it.iastate.edu/pub/ggs317/ggs317.pdf>.)

We recognize that OU administrators need to have a certain amount of control over their user objects to change passwords, apply group policy, set roaming profile paths, set home directories, etc. In order to keep things running smoothly, you must follow the following guidelines:

1. ***DO NOT DELETE, RENAME, DISABLE OR ENABLE ISU Net-ID-based user objects.*** DO NOT change the “login names”. The existence and enabled/disabled status of Net-ID-based users is dependent on user data outside the Active Directory. Enabling or disabling a user will not stick; an automated process checks the ASW status of each Net-ID and disables or enables the Active Directory object to match. If you delete a user, that object will simply reappear with a different GUID when the user changes their Net-ID password.

If someone in your OU leaves your department or the University, do not delete or disable them. Instead, move their user object into the Relocation folder and send mail to [w2k-root-admin@iastate.edu](mailto:w2k-root-admin@iastate.edu).

If you have security issues (like hacking or other malicious activity) that force you to disable a Net-ID-based user in your OU, report the action immediately to the ITS Security Office ([abuse@iastate.edu](mailto:abuse@iastate.edu)). An investigation will determine if the user should be blocked from other campus resources.

You can determine the enabled/disabled state of a user by looking them up in Active Directory Enumerator. The “Disabled” field will be “False” for active users and “True” if the user has been disabled. You may also contact the Solution Center (195 Durham Center, 294-4000) with questions/problems relating to ISU Net-IDs.

2. It is ***VERY IMPORTANT*** that the "security rights" for whatever OU you move Net-ID-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:
  - The "IASTATE/Administrators" group must have full rights to objects in the "<yourOU>/Users" container to add/update/delete the NetID-based user objects that were placed there when your faculty/staff were populated into your OU.
  - If you move NetID-based user objects from "<yourOU>/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.
3. OU managers can reset the passwords of users in their OU. Either
  - Right-click on the user in "Active Directory Users and Computers" and choose “Reset Password”.
  - Look up the user in Active Directory Enumerator and click the “Set Password” button.

Passwords must have a minimum of eight characters and a maximum of 127 characters and must contain two different character classes (upper/lower/digit/punctuation). Spaces may be used in passwords. Changing the Windows AD password automatically changes the ISU Net-ID password. Be aware of the responsibility you are granting anyone in your OU administrators group. By resetting a password (possibly to deny access on Windows systems) you are also denying them access to many other services (e-mail, WebCT, UNIX and others) within the enterprise.

4. Avoid changing things on the "General", "Address", "Account", "Telephones", and "Organization" tabs for the ISU NetID user. Specifically, do NOT change the following:

<b>General Tab</b>	First name, Initials, Last name Display name Description Office Telephone number Email
<b>Address Tab</b>	Street P.O. Box City/ State/province Zip/Postal Code Country/region
<b>Account Tab</b>	User logon name User logon name (pre-Windows 2000) Account options Account expires
<b>Telephones Tab</b>	Home telephone number Fax telephone number
<b>Organization Tab</b>	Title Department Company
<b>Other attributes</b>	employeeType uidNumber gidNumber unixHomeDirectory loginShell

All of these items are mastered in the enterprise central directory of official university data and are managed by Human Resources for staff and the Registrar's office for students. If you change them in Active Directory, they will be reset to their original values later by the account synchronization process. If you want the above items changed or suppressed, your user must change the university information. The document "Master Directory Sources" (<http://tech.its.iastate.edu/windows/admin/EnterpriseMastering.pdf>) contains information on which university office must be contacted to make these changes.

5. Some of the user objects may have "Change password to use" as the Active Directory "Description". This means the user has not changed their Net-ID password using ASW since April 2000 (when we started synchronizing the user information with Active Directory on password changes). These users need to change their ASW password to enable the account to be used in Windows. This will also reset their "Description" to their proper name. The password can be set in one of three ways:

- If they remember their old password, they can go to <http://asw.iastate.edu>, login, and change it there.
- If they cannot remember their old password, they can contact the Solution Center and the staff there will reset it for them.
- You or one of the members of the group “!<yourOU> Admins” to which control of your OU has been delegated can change the password for them. Using either of the techniques described above, change the password for their Net-ID to a temporary password with a minimum of eight characters and two different character classes (upper/lower/digit/punctuation). This will reset their password in both AD *and* ASW. They *must* then use this password to log in to <http://asw.iastate.edu> and reset the temporary password from there to something else. This second step is necessary because password changes by an admin from Windows will NOT reset the “Description” – it must come from ASW.

Make sure that your users understand that when they change their own password, whether on ASW or through Windows, that the password will be changed in both places automatically.

### **Special Net-ID Accounts**

Net-IDs are automatically created when students or eligible staff join the University, but it’s also possible to create Net-IDs for special purposes. These special accounts come in two different types:

- Exception accounts are commonly used for visiting scholars, interns, hourly employees and participants in various short-time educational institutes; persons who have an academic requirement for access to computing resources but who do not normally qualify. Exception accounts may be sponsored by any permanent faculty or staff member who qualifies for a standard Net-ID; they are reviewed every semester and the sponsor can continue to renew the account as long as necessary. To create an exception account, log in to <http://asw.iastate.edu> and choose Request for Services -> Net-ID (Account) -> Request an Exception Account.
- Administrative accounts are special accounts created for special needs. Unlike an exception account, an administrative account is owned by a department, not an individual. Such an account might be the owner of a Web page or AFS file system, or could be used to register computers in the NetReg registration system. If such things are owned by an individual and that individual leaves the University, the ownership must be transferred to someone else or the objects will disappear when the person’s Net-ID is disabled. If these objects are owned by an administrative account, anyone with access to that Net-ID and password can administer them and they won’t go away as long as the administrative account is renewed annually. Administrative accounts are also used for student employees so that they can be given Exchange mail and Windows file storage separate from their regular Net-ID accounts. To create an administrative account, log in to <http://asw.iastate.edu> and choose Request for Services -> Net-ID (Account) -> Request an Administrative Account.

When an exception or administrative account is created, the user object is moved into the OU of the sponsoring Net-ID. If for some reason the departmental affiliation doesn't happen correctly, the new account will appear in "iastate.edu/Users". Send a request to [w2k-root-admin@iastate.edu](mailto:w2k-root-admin@iastate.edu) and the user will be moved into the Users container in your OU.

## **Local Accounts**

Local accounts that you create exist only in your OU. They do not have a corresponding Net-ID and are not part of the formal university account structure. They're sometimes referred to as "bang accounts" because the required naming convention says that the local account name must begin with an exclamation point (*aka* "bang"). Local accounts have several uses:

- IT administrators often use local accounts with enhanced privileges for administration, to help limit the damage possible if their regular Net-ID account is compromised. (Make sure you use different passwords on your Net-ID and admin accounts, just in case the two can be associated in some way.)
- Student employees are sometimes given local accounts so that work-related privileges can be kept separate from their regular Net-ID accounts. (This only works if they have no need for electronic mail or access to network file servers; these things are not given to local accounts.)
- Vendors and third-party tech support personnel are sometimes given local accounts to provide support for particular machines or software. (If you do this, make sure that non-University people have access only to those parts of your OU that they absolutely need to access.)

You should not attempt to use local accounts as the permanent accounts for faculty and staff; have them use their regular Net-ID instead. Local accounts will not be given access to Exchange mail or storage. Unlike Net-ID accounts, local accounts have no mechanism for identifying who created them or why, and no automatic process removing them when they are no longer required.

To create a local account, do the following:

1. Open the **Active Directory Users and Computers** management console.
2. Right-click on your OU and choose New -> User.
3. Enter first name, middle initial and last name.
4. Enter the logon name. The logon name **MUST** follow the ISU naming convention for local accounts. Logon names (unlike Net-IDs) may be up to twenty characters long and contain periods and spaces, but they *must* begin with an exclamation mark "!". This distinguishes local accounts from campus Net-IDs; campus Net-IDs NEVER have the special character and therefore will not conflict with any local account. For example, if you need to create "joeuser" for a visiting professor, then it must be created as "!joeuser". Make sure that the primary "user logon name" and the "pre-windows 2000 user logon name" are the same and ALWAYS start with a "!" character.
5. Click Next.
6. Enter a password in the "Password" and "Confirm password" fields and click Next.
7. Click Finish.

The user you have created will have to change their password at their first login.

## Why is it important to follow the naming conventions for usernames on local accounts?

The naming convention avoids conflicts with the centrally managed campus Net-IDs that are created in both ASW and Active Directory. If you inadvertently create a username that violates the naming standard, you could have a naming conflict and a resulting headache.

For example, suppose you create a local account for a visitor and name it “bobsmith” instead of “!bobsmith”. If someone else subsequently registers for a permanent account using the same username, “bobsmith”, an account enforcement process will take place. The campus Net-ID creation process looks for an existing Windows username and finds it in the Windows namespace. It synchronizes the newly registered user’s password and personal information with the existing Active Directory username. Your bobsmith loses the ability to log in and a stranger gains access to all their resources and privileges.

## *Password Management*

### **Password Changes**

Passwords in Active Directory are subject to rules. The password can be between 8 and 127 characters long, and must contain at least two of the following character classes:

- Lowercase letters
- Uppercase letters
- Numbers
- Punctuation

Passwords may be changed in a variety of ways:

1. Users logged in to a Windows computer on the IASTATE domain can press {Ctrl/Alt/Del} and click **Change Password**.
2. You can right-click on the user object for any user in your OU in Active Directory Users and Computers and choose “Reset Password”.
3. Users with regular Net-IDs (but not local accounts) who forget their password can contact the Solution Center and have the password reset. Call the Solution Center at 515-294-4000 or come to 195 Durham Center.
4. Users with regular Net-IDs (but not local accounts) can log in to the web site <http://asw.iastate.edu> and select **Manage User -> Change your password**.
5. Users with regular Net-IDs (but not local accounts) who forget their password and who have created a challenge question or registered their cell phone number can change their password. To do this, go to <http://asw.iastate.edu> and click "Forgot your password". Enter your Net-ID, your ISU ID Card Number and your birth date, and click on "Submit Data". The next screen will show two choice areas. Your Challenge Question will be displayed; to change password this way, enter the response and click “Submit Response”. If your response is correct you will be able to change your password. To reset via text

message, click “Text Me”. A verifier code will be sent to your cell phone; enter that code on the web page and click “Verify”, and you will be able to change your password.

Changes made to regular Net-ID accounts with any of these methods will be synchronized on both Active Directory and ASW.

## **Password Expiration**

Microsoft Active Directory makes no provision for differing password expiration rules within an organization. At ISU, differing password expiration requirements have been mandated by auditors and contractual agreements. Some units need 30 day expiration, others want 180 days and still others want no expiration.

Microsoft’s password expiration facility has been circumvented in the following way.

- By default, new users created by the ASW registration process have non-expiring passwords. This matches the current policy for ASW.
- You can switch your users to have expiring passwords. The default expiring password will expire in 180 days. To do this, follow these steps:
  1. In Active Directory Users and Computers, right-click on the user and choose Properties.
  2. Click the Account tab.
  3. Uncheck “Password never expires”.
  4. Click OK.
- You can use a password utility to enforce shorter password expiration for your users. Pswdutil is a program that checks user objects in an OU for password age. The program and documentation are available in the archive file <http://tech.its.iastate.edu/windows/admin/PswdUtil.v1.0.zip>.

## **Security Groups and Mailing Lists**

### ***Creating Your Own Groups***

The same naming standard used for local accounts applies to departmental groups that OU administrators create. Group names must begin with an exclamation point to avoid conflicts with ASW groups being populated down into the Windows environment. (ASW groups include departmental, class, major, and college lists, which can be used in Windows as security groups for resource control.)

To create a group, do the following:

1. Open the Active Directory Users and Groups management console.
2. Right-click on your OU and choose New Group.
3. Enter a group name beginning with an exclamation point. For example, a departmental security group of lab managers might be called “!My Dept Lab Managers”.
4. Choose a group scope and a group type. Generally the defaults of “Global” and “Security” are correct.
5. Click OK.

To add users to a group, do the following:

1. Right-click on the group and choose Properties.
2. Click the Members tab.
3. Click Add.
4. Enter the Net-ID or login name of the user to add and press {Enter}.
5. Repeat the previous two steps until all the users are added.
6. Click OK.

### **Using Official University Lists as Security Groups**

It is not necessary for you to create security groups for all of the people in your college or department, or for majors and classes in your department. These lists are already maintained by Human Resources and the Registrar's office and propagated automatically into the Active Directory whenever changes occur. All of these lists appear in the AutoLists OU in the Active Directory and are divided as follows:

- CollegeLists – groups for all of the people in a college divided by group, with names like “dept\_coll\_group”. For example, faculty in the College of Agriculture are members of the group “agri\_coll\_faculty”.
- DeptLists – staff in a department divided by group with names in the form “department\_group”. Professional and scientific staff in the department of Agronomy appear in the group “agronomy\_profsci”.
- MajorLists – students divided by major and type (undergraduate vs. graduate). There are four types of major lists:
  - Lists including all undergraduate or graduate students with a major, like “chem\_ugrad”.
  - Students currently enrolled in a major, like “current\_chem\_ugrad”.
  - Students who have pre-registered for a major but have not begun classes, like “future\_chem\_ugrad”.
  - Students who have changed away from a major, like “past\_chem\_ugrad”.
- ClassLists – groups for a specific section of a specific class. There are two lists for each class section:
  - The students list has a name of the form “semester.dept.number.section”. Because of security concerns, the students group contains only hidden objects and will not appear to have any members.
  - The instructors list has a name of the form “semester.dept.number.section.instructors”.


All of these lists may be used as security groups to control access to resources. All but college lists can also be used as mailing lists; send e-mail to *listname@iastate.edu*.

For more information, see <http://tech.its.iastate.edu/windows/admin/ListSync.pdf>, “Official University Lists as Global Security Groups”.

## Using an ASW List as a Security Group

Lists created in ASW can be connected to AD security groups, letting multiple people maintain a security group with a simple Web-based interface. Creating a security group from an ASW list can occur when the list is created or afterwards.

To make an ASW list a security group, view the Properties page for the list and check “Windows Active Directory Security Group” as shown here.

Properties: 

Status	Synchronized Into ...
<input type="checkbox"/> Disabled	<input type="checkbox"/> AFS
<input type="checkbox"/> Hidden	<input type="checkbox"/> NFS/NAS
<input type="checkbox"/> Public	<input checked="" type="checkbox"/> Mail
<input checked="" type="checkbox"/> Sticky	<input type="checkbox"/> Without Inbound SPAM filtering
Expiry Date	<input type="checkbox"/> Managed by Mailman
	<input checked="" type="checkbox"/> Included in the Exchange GAL
	as Win Admin Meeting   [ITSYS]   <input type="text"/>
Institutional?	<input checked="" type="checkbox"/> Windows Active Directory Security Group
No <input type="text"/>	

(properties in red are protected)

Changes in the ASW list will be synchronized with a corresponding group in AD. Net-IDs in the list will be converted to the appropriate Windows user object. Lists may be members of lists, but “Windows Active Directory Security Group” must also be checked in the properties of the sub-lists. Strings in the ASW list like “STRING:[someuser@gmail.com](mailto:someuser@gmail.com)” will not be pushed to the AD list.

If “Hidden” is not checked, the list will appear in the OU “AutoLists/UserReqLists”, and the members of the list will be visible in the Active Directory. If “Hidden” is checked, the list will appear in the OU “AutoLists/UserReqHMLists” and the members will *not* be visible.

Be careful not to uncheck the “Windows Active Directory Security Group” box. When you do, the Windows group will be deleted, and any Windows resources with access controls referencing that group will lose their connection. Recreating the group by checking the box again will create a group with a new GUID, and you will have to connect that new group to all of your resources again.

For more information, see <http://tech.its.iastate.edu/windows/admin/ListSyncUserReq.pdf>, “User Requested Lists as Global Security Groups”.

## Using Mail Lists as Global Address List Contacts

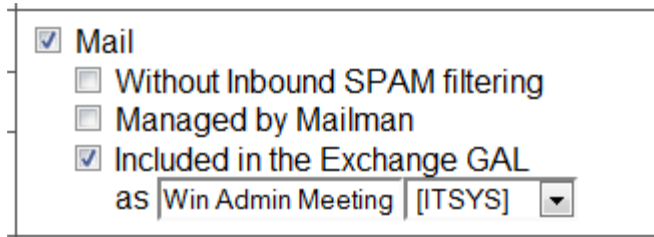
Lists created in ASW can also be used as mailing lists complete with entries in the Windows Global Address List, letting multiple people maintain an Exchange mailing list with a simple Web-based interface. This can be done when the list is created or afterwards by setting the list’s properties in ASW.

Log in to <http://asw.iastate.edu> and choose Manage Lists -> View/Update a List’s Properties. On the list’s properties page, set the mailing properties as shown below:

- The Mail check box creates an ASW mailing list. Address the mail to [lastname@iastate.edu](mailto:lastname@iastate.edu). This list can contain ISU Net-IDs, other ASW mailing lists (in the

form "LIST:*listname*") or STRING objects of the form "STRING:*username@hostname*", to include addresses of people off-campus.

- Checking "Included in the Exchange GAL" creates a contact list in "AutoLists/Contacts" which appears in the Global Address List and can be used from Outlook, Entourage, etc. This box is only available to faculty, staff and affiliate exception accounts; students and "NetReg-only" accounts cannot create an Exchange contact list.
- The name field under "Included in the Exchange GAL" is initially the name of the list, but can be changed to a more descriptive name. It must not match an existing contact list; the creation of the contact list will fail and you'll be notified by e-mail if this happens.
- The field at the end of the list name is the department code and will initially be set to the owner's department. You may select a different department code from the pull-down menu if this is appropriate.



Mail  
 Without Inbound SPAM filtering  
 Managed by Mailman  
 Included in the Exchange GAL  
as Win Admin Meeting | [ITSYS] ▼

The Exchange contact list contains only the member [listname@iastate.edu](mailto:listname@iastate.edu); it does not contain the members of the list. For more information, see <http://tech.its.iastate.edu/windows/admin/ListSyncMailLists.pdf>, "Mail Lists as Global Address List Contacts".

## Creating and Delegating in Sub-OUs

### *How Do I Create a Sub-OU?*

You may find that you have a need to administer different groups of computers and users, well, differently. Perhaps you need to manage faculty computers and a student computer lab, which have very different requirements. It is appropriate to create separate OUs for this task. But before you create a sub-OU, be warned; you should only do this when you want to apply different security policy to objects in the sub-OU. A "deep" OU tree results in increased login and access control times. Do not create a sub-OU simply to mirror the organization of your department. You need a good technical reason to create a sub-OU.

Before you start, find a notebook or open a Word document. It is a good idea to keep a log of everything you do. In doing this, you can later see what you did and can undo something that may have gone wrong.

In the following example, we will create two OUs, one for faculty computers and one for a student computer lab. Assume your OU is named "SAMP":

1. Open the Active Directory Users and Groups management console.
2. Right-click your OU ("SAMP") and choose New -> Organizational Unit

3. Enter "SAMP-Student\_lab" for the name and press {Enter}.
4. Right-click your OU ("SAMP") and choose New -> Organizational Unit
5. Enter "SAMP-Faculty\_computers" for the name and press {Enter}.

You can now drag computer objects for faculty and the computer lab into the appropriate folders. Your two OUs are now ready for separate management with separate group policies.

### ***How Do I Delegate Authority in a Sub-OU?***

You may have a group that is not only different, but fiercely independent. Perhaps you have a research lab with computer needs that are very different from your standard office computers. The people in that group would like to manage their own machines. If these needs are important enough to warrant separate administration, you can create a separate sub-OU within your OU. This sub-OU would provide a structure for separate administration of this research lab.

In this section, we'll demonstrate how to create a sub-OU and assign permissions to a different group of people. We'll assume your OU is named "SAMP", and we'll create a sub-OU for the research lab named "SAMP-RESEARCHLAB". Next, we'll create an administrators group for the sub-OU, and set the properties of the OU so that the administrators group has full control of the OU.

1. Start the **Active Directory Users and Computers** management console.
2. First, we'll create the sub-OU. Right-click your OU ("SAMP") and choose **New -> Organizational Unit**.
3. Enter "SAMP-RESEARCHLAB" for the OU name and press {Enter}.
4. Now we'll create an administrators security group within that OU to manage it. Right-click the "SAMP-RESEARCHLAB" OU, and choose **New -> Group**.
5. Enter "!SAMP-RESEARCHLAB Admins" as the group name, verify that the group scope is **Global** and group type is **Security**, then click **OK**. (Notice that we've used the same naming convention as ITS-created admin groups, and *don't forget the exclamation point!*)
6. Add Windows usernames to the membership of the **!SAMP-RESEARCHLAB Admins** group. These usernames will be able to administer your new sub-OU.
  - a. Right-click the **!SAMP-RESEARCHLAB Admins** group and choose **Properties**.
  - b. Select the **Members** tab, then click the **Add** button.
  - c. For each user that you want to add to the **!SAMP-RESEARCHLAB Admins** group, click **Add**, enter a Net-ID or username, and press {Enter}.
  - d. When you are done adding Net-ID's, click **OK** to leave the properties of **!SAMP-RESEARCHLAB Admins** group.
7. Delegate full control of the new OU to the **!SAMP-RESEARCHLAB Admins** group
  - a. The following instructions presume that the **Active Directory Users and Computers** management console is in its "advanced view". Click the **View** menu and verify that **Advanced Features** is already checked; select it if it isn't.
  - b. Right-click the "SAMP-RESEARCHLAB" OU and choose **Properties**.
  - c. Click the **Security** tab.
  - d. Click the **Advanced** button.
  - e. Click the **Add** button.

- f. Enter “!SAMP-RESEARCHLAB Admins” in the large entry field and click **OK**. A permissions window will display.
  - g. Click the **Object** tab. Check **Full Control** in the **Allow** column (Don't change any other settings)
  - h. Click the **Properties** tab. Check **Read All Properties** and **Write All Properties** in the **Allow** column (don't change any other settings).
  - i. Click "**OK**" enough times to close out all windows and return to the **Active Directory Users and Computers** management console.
8. The administrators of your new sub-OU will need to have computers in their new sub-OU. If those computers are already part of your OU, drag the computer objects from your OU and drop them in the sub-OU. Then they can be administered by the new administrators of the sub-OU.
- If the computers have yet to be added to your OU, you should add at least one computer to the new sub-OU. This should be the new sub-OU administrator's computer. They will need at least one computer to get started. Right click on the new sub-OU; select **NEW** then **Computer**. Add this computer in the same manner as you did all of the other computers in your OU. Be sure to specify that the *!SAMP-RESEARCHLAB Admins* group can add this computer to the domain.
9. Help the new sub-OU administrators get the Active Directory tools (as described above in the *Getting your Active Directory Tools* section) so they can manage the sub-OU.
10. Make sure ALL your administrators understand policies relating to the management of ISU Net-IDs as outlined in this document.

## Changing OU Management

Your OU has been set up so the Windows enterprise administration never needs to be involved in the transfer of power within your department. OU management can be transferred simply by adding and removing users from the “!<YourOU> Admins” security group.

In the event the management of your OU changes (a departmental OU manager assumes new duties or leaves the department) the remaining OU manager(s) should perform the following tasks:

1. Add any new OU manager(s) to the “!<YourOU> Admins” security group. This gives the new admin(s) the same powers the existing OU managers have.
2. Add the new OU manager(s) to any other appropriate security groups created by the department to manage their OU structure.
3. Remove the exiting managers from appropriate departmental security groups.

If the OU manager is leaving the department the remaining OU manager(s) should move the user object to the “Relocation” container and email [w2k-root-admin@iastate.edu](mailto:w2k-root-admin@iastate.edu) once all necessary cleanup activities have been performed.

## Using the ISU WSUS Server

ITS maintains the Enterprise WSUS server, a local mirror of the Microsoft Windows Updates server. Rather than having thousands of ISU machines contacting Microsoft's server daily, we

have those updates downloaded locally to reduce network bandwidth. This server automatically approves all updates as they are received from Microsoft. There is no testing, delay or filtering of updates other than that described below. If you would prefer to test updates first or want more granularity in selecting the updates being deployed, you may want to look into providing your own WSUS server.

A machine may be configured to use the ISU WSUS server either individually or through Group Policy.

1. Start either “Local Security Policy” or “OU Group Policy”.
2. Open Local Computer Policy -> Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update.
3. Configure the following settings under Windows Update:

<b>Configure Automatic Updates</b>	Enabled
Configure automatic updating:	4 – Autodownload and schedule the install (recommended)
Scheduled install day:	0 – Every day (recommended)
Scheduled install time:	Sometime after 4 PM (our WSUS server synchronizes with Microsoft’s update servers at about 4 PM)
<b>Specify intranet Microsoft update service location</b>	Enabled
Set the intranet update service for detecting updates	<a href="http://sus.iastate.edu">http://sus.iastate.edu</a>
Set the intranet statistics server	<a href="http://sus.iastate.edu">http://sus.iastate.edu</a>
<b>Enable client-side targeting</b>	Enabled only if you want to choose a client-side targeting group other than the default.
Target group name for this computer	One of the choices in the table below.

The client-side targeting groups allow all or parts of the Windows updates to be excluded from being installed automatically. The pre-defined groups are as follows:

<b>Group Name</b>	<b>Description</b>
Unassigned Computers	Receives all updates except “Drivers”. This is the default.
All	Receives all updates including drivers
SC	Receives only “Critical”, “Security”, “Service Packs”, “Update Rollups” and “Definitions” updates. Does not receive “Drivers” or optional updates.
None	Does not automatically install any updates (usually used only for servers where updates should be tested before manual deployment)

If you enable automatic updates but do not enable client-side targeting, your machines will receive all updates except those categorized as “Drivers”.

Microsoft documentation on configuring a client (either joined to the Enterprise domain or not) is available here:

<http://technet2.microsoft.com/windowsserver/en/library/8b786951-a481-49a6-a0e6-69189e58f2ab1033.mspx>

A good overview of the entire WSUS process is available here:

<http://www.microsoft.com/technet/technetmag/issues/2005/11/HandsOn/default.aspx>

## **Group Policy**

### ***Linking a Group Policy Object to Your OU***

Group Policy can be used to configure and install software on the machines in your OU from your administration machine. All OU Admins have the rights to create and link to Group Policy Objects (GPOs) on the IASTATE domain.

The full use of Group Policy is beyond the scope of this document. However, it is relatively easy to link your OU to GPOs that have been created by other administrators, and the enterprise administrators have created GPOs designed to be used by anyone on the IASTATE domain. These can be used for deploying Forefront Endpoint Protection 2010, the Microsoft SCCM client, and Vista TN3270 as well as a wide variety of useful settings.

All of the Group Policy objects created on the IASTATE domain appear in the “Group Policy Objects” folder in the Group Policy Management console. Group Policy objects designed for all IASTATE domain machines have names beginning with “ISU”.

To link your OU to a GPO, do the following:

1. Start Group Policy Management (in the Administrative Tools section of your Control Panel).
2. Right-click on your OU and select “Link an existing GPO”.
3. Scroll through the list of Group Policy objects, highlight the one you want to link to, and click OK.

The policies in that object will be applied to computers at next restart, and to users at their next login.

### ***Creating Your Own Group Policy Objects***

If you create Group Policy objects, there are several things you can do that will make life simpler for everyone.

1. All domain group policy objects must live in the same folder. Please begin the names of your GPOs with the name of your OU so everyone can tell the context for which they were designed.
2. The groups “Enterprise Admins” and “Domain Admins” must have full access (edit/delete/modify) to all GPOs, and the group “ENTERPRISE DOMAIN CONTROLLERS” must have read access. Please do not remove or modify these permissions.
3. When you create a GPO, delegate full access to your “!<your-OU> Admins” group:
  - a. In the Group Policy Management console, select the GPO, then select the “Delegation” tab.
  - b. Use the “Add” button to add “!<your-OU> Admins” with the power to edit settings, delete and modify security on that GPO.
  - c. Highlight your own entry and click “Remove”.
  - d. Click “Advanced”.
  - e. Highlight “!<your-OU> Admins”, turn on “Full Control” under the Allow column, and click “Apply”.
  - f. If you are using Windows Vista or Windows 7 on your administrative machine, change the ownership of the new group policy object to your Admins group instead of yourself. (You can’t do this step if you’re using Windows XP.)
    - i. Click “Advanced” again.
    - ii. Click the “Owner” tab.
    - iii. Click “Other Users and Groups”.
    - iv. Enter “!<your-OU> Admins” and click OK.
    - v. Highlight “!<your-OU> Admins” in the list and click “OK” to change the ownership to the “!<your-OU> Admins” group.
  - g. Click OK until the dialog boxes are all closed and you’ve returned to the Group Policy Management window.

If you reset the ownership to a group it will not be necessary for the domain admins to reassign ownership when the current owner leaves the University.

For more information on use of Group Policy at ISU, see <http://tech.its.iastate.edu/windows/admin/GPO.procedures.pdf>. More information on the use of Group Policy is available at <http://technet.microsoft.com/en-us/library/bb742376.aspx>.

## CyFiles

As of August 2011, every NetID-based account (but not local accounts) is given 5 GB of free online file storage through CyFiles. This storage is available through CIFS and NFS to Windows, Mac OS X and Linux clients, and is attached to the user, not to the department. People moving from department to department may see changes in their department-related file storage, but the contents of their CyFiles share will still be the same.

The following Active Directory attributes are set on user objects that have been provisioned for CyFiles:

Attribute	Description
homeDirectory	Set to the user's CyFiles path: <a href="#">\\cyfiles.iastate.edu\##\##\netID</a> where "##\##" is a series of numbers based on the user's UID
homeDrive	U:
profilePath	The user's CyFiles path plus a profile directory depending on Windows version: <a href="#">\\cyfiles.iastate.edu\##\##\netID\.profile</a> (Windows XP) <a href="#">\\cyfiles.iastate.edu\##\##\netID\.profile.V2</a> (Windows Vista and 7)

When a Windows user logs in to any Windows computer connected to the IASTATE domain their CyFiles space will be mapped to drive U. This will not interfere with any other drive mappings you may have configured on login.

If your department or college does not want new faculty/staff users you manage to have CyFiles provisioned for them you can request that your OU be exempted; send email to [storage@iastate.edu](mailto:storage@iastate.edu). In this case, the CyFiles user space will still be created, but no U drive will be mapped automatically and the Active Directory attributes will not be set. You may also change the "homeDirectory", "homeDrive" and "profilePath" attribute settings on users in your OU, but bear in mind that if you do you may need to work with them to transfer any items in their CyFiles space to an accessible location.

### **CyFiles and Roaming Profiles**

Roaming profiles allow user documents and settings to be automatically stored on a file server. Folders like "Documents" and "Contacts" are automatically redirected to the network share, and the user doesn't have to think about where they're actually stored. No matter which machine they log in to, their files are just there.

The default group policy on the IASTATE domain ("Default Domain Policy") disables roaming profiles. However, you can enable roaming profiles on computers in your OU via Group Policy. You could create a group policy for this purpose, or you could simply link the OU to the ISU group policy objects below:

Group Policy Object	Description
ISU – Enable Roaming Profiles	This enables the use of roaming profiles on the machine.
ISU – Disable Offline Files	Link to this GPO if you do not wish to have the user's profile mirrored on the local machine, but only on CyFiles. Use this for lab machines and other computers primarily for "transient" users.

With those settings, users logging in to your computers will have their profiles redirected to the .profile or .profile.V2 directories in their CyFiles space. If you'd prefer that they find profile folders like Documents at the top level of their CyFiles directory, link the OU containing your users to one of the following as appropriate:

Group Policy Object	Description
ISU – CyFiles Folder Redirection All	This redirects all of the user’s profile folders to top-level CyFiles folders: AppData(Roaming), Contacts, Desktop, Documents, Downloads, Favorites, Links, Music, Pictures, Saved Games, Searches and Videos.
ISU – CyFiles Folder Redirection Essentials	This redirects only Desktop, Documents, and Favorites to top-level CyFiles folders.
ISU – CyFiles Folder Redirection for Windows XP	Designed for Windows XP machines, this redirects Application Data, Desktop and Documents to top-level folders compatible with Windows Vista/7 logins. Music, Pictures and Videos appear in the Documents folder as they do in Windows XP.

If your users log in to machines on the IASTATE domain that do not have roaming profiles enabled, their folders will not be redirected; however, their files will still be available through the U drive.

## Secunia Corporate Software Inspector

The Secunia Corporate Software Inspector (CSI) is a system which extends Microsoft’s WSUS update system to include updates to third-party software. An agent installed on a Windows machine reports the software installed to the CSI server; this is compared to a list of vulnerable software maintained by Secunia, and patches are produced for vulnerable products. These patch packages are then placed on the WSUS server, and machines belonging to the Secunia client-side targeting groups retrieve the third-party software patches from the WSUS server along with regular Windows updates.

Iowa State University has a license for CSI and has installed it on the central WSUS server, sus.iastate.edu. To use CSI to supply third-party updates to your machines, simply link the OU containing the machines to the following group policy objects:

Group Policy Object	Description
ISU WSUS – CSI	Installs the CSI agent and the digital certificates necessary to install third-party updates.
<b>In addition, you must link to one of the following:</b>	
ISU WSUS-SCPlusSecunia	Machines will receive Microsoft “Critical”, “Security”, “Service Packs”, “Update Rollups” and “Definitions” updates, plus all third-party software updates.
ISU WSUS-NoDriversPlusSecunia	Receives all Microsoft updates except hardware drivers, plus all third-party updates.
ISU WSUS-AllPlusSecunia	Apply all Microsoft and third-party software updates.

These group policy objects do not set the Windows update schedule. You will still need to configure automatic updates. You may link to the GPOs “ISU AutoUpdate 12 PM” or “ISU AutoUpdate 5 PM” if those choices fit into your schedule or create your own GPO.

You can also receive vulnerability reports on the computers running the CSI agent in your OUs. To request reports, send email to [secunia-admins@iastate.edu](mailto:secunia-admins@iastate.edu) containing the following information:

- Your name
- Your department
- The email address to send reports to (can be a mailing list)
- The OUs you want reports on.

Reports for each OU will be sent weekly in the form of a CSV file.

## **Activation of Windows Vista and Windows 7**

Iowa State University is a signatory to the Microsoft Campus Agreement. As a result, a wide variety of Microsoft software is available for any machines owned or leased by Iowa State University and used exclusively by faculty or staff or in open access computer labs at no additional charge. Desktop machines may be upgraded to any version of Windows including Windows 7 Enterprise as long as they have a legitimate license for some version of Windows. (This does not apply to servers.) For more information on the Microsoft Campus Agreement, see <http://www.it.iastate.edu/mca/>.

Installations of Windows Vista and Windows 7 must be activated to remain fully functional. There are two ways to do this: Key Management Service and Multiple Activation Keys.

### ***Key Management Service (KMS)***

Machines using KMS automatically activate when connected to the IASTATE domain, and machines not connected to the domain can be activated manually. To comply with the MCA, KMS activation only works for machines on the campus network. It will not work with machines that are:

- Off-campus;
- Connecting via PPP or VPN connections;
- Using IP numbers assigned to Residence Halls;
- From “guest” IP connections.

We recommend that you use KMS activation for most departmentally-owned machines. KMS activation need only happen every six months; even for laptops that are taken off-campus, they will usually be returned to campus often enough to stay activated.

### ***Multiple Activation Key (MAK)***

For machines that are permanently located off the campus network, or off campus for more than six months at a time, we recommend the use of a MAK license. Iowa State has a MAK number, which gives us a limited number of activations. Re-imaging a machine requires the use of an additional activation. ITS staff monitors the number of MAK activations so that we can order more licenses when necessary.

For more information on using KMS and MAK, see <http://www.it.iastate.edu/vista/> or contact [mca@iastate.edu](mailto:mca@iastate.edu).

## Appendix A -- Learning More

### ***ITS Windows-related Websites***

ITS maintains a number of web pages pertaining to the ISU Windows Enterprise Domain. These are available online at the links below:

OU Administration FAQ	<a href="http://tech.its.iastate.edu/windows/admin/OUAdminFAQ.pdf">http://tech.its.iastate.edu/windows/admin/OUAdminFAQ.pdf</a>
OU Administrator Support	<a href="http://tech.its.iastate.edu/windows/admin/ouadmin.shtml">http://tech.its.iastate.edu/windows/admin/ouadmin.shtml</a>
Windows Enterprise Domain homepage	<a href="http://tech.its.iastate.edu/windows/">http://tech.its.iastate.edu/windows/</a>
Windows Support for IT Administrators	<a href="http://tech.its.iastate.edu/windows/admin/">http://tech.its.iastate.edu/windows/admin/</a>
Windows System Security information	<a href="http://tech.its.iastate.edu/windows/admin/security.shtml">http://tech.its.iastate.edu/windows/admin/security.shtml</a>
Windows Desktop User Support	<a href="http://tech.its.iastate.edu/windows/user/">http://tech.its.iastate.edu/windows/user/</a>
Windows Software Distribution	<a href="http://tech.its.iastate.edu/windows/downloads/downloads.shtml">http://tech.its.iastate.edu/windows/downloads/downloads.shtml</a>

### ***Windows Administrators Support Group***

This group meets monthly to discuss topics of interest to Windows consultants on campus, particularly those pertinent to Microsoft servers and systems. In addition to regular meetings, there is also a mailing list that is used for Windows-related questions and announcements. To join the Windows Administrators email list, send a request to Steve Kunz ([skunz@iastate.edu](mailto:skunz@iastate.edu)). Meeting notes can be found at <http://www.tech.its.iastate.edu/windows/admin/meetings.shtml>.

### ***Microsoft Support Resources***

Microsoft makes a number of technical resources available:

Microsoft Support (Solution Centers for products, KnowledgeBase)	<a href="http://support.microsoft.com">http://support.microsoft.com</a>
Microsoft TechNet (manuals, training, videos and forums for IT professionals)	<a href="http://technet.microsoft.com/en-us/default.aspx">http://technet.microsoft.com/en-us/default.aspx</a>
Microsoft Download Center (downloadable software and updates)	<a href="http://www.microsoft.com/downloads/en/default.aspx">http://www.microsoft.com/downloads/en/default.aspx</a>
Microsoft Learning (training and certification information, some free training but most for pay)	<a href="http://www.microsoft.com/learning/en/us/default.aspx">http://www.microsoft.com/learning/en/us/default.aspx</a>