IOWA STATE UNIVERSITY
IT Services Technical Notes

Windows Enterprise
OU Administrator Policy and Procedures
Managing Users Within a College/Departmental Organizational Unit

Steven L. Kunz
August 17, 2016

This document describes how to manage user objects within a college or departmental “Organizational Unit” (“OU”) in the Iowa State Windows Enterprise domain (“iastate.edu”).

Departmental and college OU managers are allowed to request that their “faculty”, “staff”, and “affiliate” user objects be moved into their OU structure. This allows IT staff to apply user Group Policy, reset passwords, assign home directory and roaming profile storage, etc. When an OU is initially created the bulk of the departmental faculty/staff can be moved shortly after the OU manager becomes familiar with the policies and procedures outlined in this document. After the initial “bulk move” the “auto-drop” process will correctly deposit future users into the correct OU (based on official university department code). See “OU User Placement Logic” at http://tech.its.iastate.edu/windows/admin/OUUserLogic.pdf for more info on this process.

There is provision for OU managers to ask for a few faculty/staff/affiliate user objects outside their department to be moved into their OU. See the section titled “Requesting Faculty/Staff/Affiliate Users Outside Your OU” at the end of this document.

It is VERY IMPORTANT that OU managers understand the two types of user objects (“NetID-based” and “Windows Exception”) and how each type can be managed within their OU.

Types of User Objects

There are two main types of user objects within college or departmental OUs.

The first type of user object is an “ISU NetID User Object”. These are created when the user registers for an ISU NetID with the Acropolis “register” function. These are the PRIMARY usernames used by users within the ISU enterprise. The ISU NetIDs (a.k.a. “usernames” or “logon names”) and associated passwords are kept “in synch” between Windows Active Directory and the enterprise Kerberos servers (used by many other systems on campus). The account synchronization process does the “mastering” of the Active Directory data for certain fields. OU managers must follow certain guidelines in dealing with these user objects (since they are “mastered” somewhere else).

Departmental OU admins requiring additional usernames should create a sponsored NetID via http://asw.iastate.edu (IT Administration/Manage Sponsored Net-IDs). These sponsored accounts have MyFiles storage, an Exchange mailbox, etc. and provisioned by all standard account provisioning processes.

The second type of user object is a “Windows Exception User Object”. These are created directly by an OU manager using Windows “Active Directory and Computers”. This type of account is strongly discouraged at this time. These usernames only exist in Windows Active Directory (and are not populated to/from ISU NetIDs). They are not assigned university resources typically given a provisioned NetID such as MyFiles storage and an Exchange mailbox. They must follow a special naming convention but otherwise are under complete control of the OU manager.

Managing ISU NetID User Objects

ISU NetID User Objects should be considered “owned by the enterprise” since that is where they are created, altered, and inactivated/deleted of when the user leaves the university. The Active Directory design process revealed the need for OU managers to have a certain amount of control over these user objects (in order to change passwords, set roaming profile paths, home directory paths, etc) for their faculty/staff users. As a result, “enterprise” objects for faculty and staff users are placed in departmental OUs. Remember that certain guidelines must be followed for ISU NetID-based user objects in your OU:

1. DON’T DELETE, RENAME, DISABLE or ENABLE ISU NetID-based user objects. DON’T change the “login names”. The existence (and enabled/disabled status) of ISU NetID-based user objects is synchronized with the master status of these users (see next topic). Deleted user objects will just "reappear" with a different GUID whenever the user changes their ISU NetID password. A process regularly runs that will check the Acropolis “suspended/active” status of each NetID-based user object and disable/enable the Windows user to match. Changing the disabled/enabled status will not “stick”.

   If someone in your OU leaves your department or the university do NOT delete or disable them. You should move the user object(s) to the “iastate.edu/Relocation” container and send email to its-ad-admins@iastate.edu. In the email provide a list of the usernames you moved into the “Relocation” OU and a brief reason as to “why”. They will be moved back into the general user pool. You should NOT disable or delete these users since they may come back as students or employees somewhere else in the university at a later date.

   IMPORTANT: If you move usernames out of your OU and into the “Relocation” container, remember to remove them from any Security Groups you may have added them to. Group membership (and the access control provided by any security groups) will follow the user object wherever it is moved to!

   If you have security issues (hacking or other malicious activity) that force you to disable a NetID-based user object in your Windows OU the action should be reported immediately to the ITS Security Office (abuse@iastate.edu). An investigation can be initiated to see if action is warranted on all other campus access.

2. Be aware that Acropolis master functions will enable/disable (and eventually delete, if they leave the university) NetID-based user objects. These actions are based on the user's official status with the university (based on Human Resources and Registrar records). Refer to "The Care and Feeding of ISU NetIDs" for complete information on this process (Old ITS Handout GGS 317, http://www.tech.its.iastate.edu/windows/admin/ggs317.pdf - archive document – not current information).

   Remember, while you may have the ability to enable/disable ISU NetID-based user objects within your OU you should not do it. A process regularly runs that will check the Acropolis "suspended/active" status of each NetID-based user and disable/enable the Windows user to match. The action will not "stick".

   If you want to easily determine the official "enabled/disabled" status of an existing NetID (to determine if the Windows user object was disabled by Acropolis master functions, for example) you can use the "ShowUserDept" script (available at http://tech.its.iastate.edu/windows/admin/ShowUserDept.zip). The response for an Acropolis-suspended NetID will have the term "[inactive]" appended to the response. You may also contact the Solution Center (195 Durham Center, 294-4000) with questions/problems relating to ISU NetIDs.

3. 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:

   a) 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.
   b) 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.

4. OU managers can right-click users with "Active Directory Users and Computers" and set their password. This password will be synched back up to the ISU NetID. 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 all other services (UNIX and others) within the enterprise.

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

General Tab
First name, Initials, Last name
Display name
Description
Office
Telephone number
Email

Address Tab
Street
P.O. Box
City/
State/province
Zip/Postal Code
Country/region

Account Tab
User logon name
User logon name (pre-Windows 2000)
Account options
Account expires

Telephones Tab
Home telephone number
Fax telephone number
IP phone number

Organization Tab
Job Title
Department
Company

Other attributes you should NOT change:
uidNumber
gidNumber
unixHomeDirectory
loginShell
employeeType
division
departmentNumber
homeDirectory
homeDrive
profilePath

The enterprise central directory of official university data masters most of this information. In the future access control lists may lock out changes to fields mastered somewhere else. For now, if you change these they will get "re-synched" by the account synchronization process.

If you want the above information 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 is the master for this data.

6. Some of the user objects may have "Change password to use" as the Active Directory "Description". This means the user has not changed their Acropolis NetID password since April 2000 (when we started synching the users down to Active Directory on password changes). These users need to change their Acropolis password to enable the account to be used in Windows 2000. 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 bring their staff ID to the Solution Center and the staff there will reset it for them.
    - They can come to you (or one of your departmental OU admins -members of the group “!<dept> Admins” which control of your OU has been delegated to). Find the username in your OU with "Active Directory Users and Computers", right-click the username, and select "Change password". The admin should supply a 5-char, two-character-set password and tell them what it is. This will reset their password in both Windows AND Unix. They should then use this to connect to http://asw.iastate.edu and reset the temporary password from there to something else. This latter step is necessary because password sets by an admin from Windows will NOT reset the “Description” – it must come from Acropolis.

    Make sure your users understand that when they change their own password (whether on a Unix system or a Windows system that is a member of the "iastate.edu" domain) the password will be changed in both places automatically.

Sponsored Accounts (Instead of Bang-accounts)

In the past OU managers were instructed to create bang-accounts for non-centrally provisioned user needs. **Bang-accounts are strongly discouraged at this time.** ITS is beginning a year-long phase-out of bang-accounts (OU manager directly-created accounts with the format "!<username>"). Bang-accounts are being replaced by sponsored Net-IDs for accountability/auditing reasons.

ASW (http://asw.iastate.edu) can be used to create new sponsored Net-IDs (using the "Manage Sponsored Net-IDs" selection). OU managers should do this instead of directly creating a bang-account.

ASW can also be used to convert existing bang-accounts to sponsored Net-IDs (Campus IT Staff Administrative Functions -> Manage Users -> Convert an AD-only bang-user to a Net-ID). This action must be performed by an OU manger with rights to the bang-account. A conversion done in this way is a "rename" to a centrally provisioned Net-ID so the account retains its unique identity used for group memberships, access control, etc.

The current timeline for the bang-account phase-out is:

1. July 1, 2014 – An email warning will begin to be issued every time an IT admin creates a new bang-account or enables a previously created/disabled bang account.

2. January 1, 2015 – Bang-accounts will no longer be allowed to be created.

3. June 1, 2015 – All bang-accounts should be gone.

Requesting Faculty/Staff/Affiliate Users Outside Your OU

Sometimes a faculty or staff person may have an official university department code that places them in an OU where there is either no IT manager or it is not the OU where the IT technology for that person is managed. In many cases the department code can be corrected (through the Personnel Office) to reflect the correct employment status of the person. For more information see "Master Directory Sources" at http://tech.its.iastate.edu/windows/admin/EnterpriseMastering.pdf .

Sometimes a departmental code correction is not possible (or desirable). In these cases (when only one or a few faculty/staff user objects are desired) then departmental IT admin may request the user object to be placed in their OU.

The first step in a special request for a user objects is to ALWAYS find out:

1) What type of user object you are requesting. You can only request "faculty", "staff", and "affiliate" user objects. You can find this information out using the following script: http://tech.its.iastate.edu/windows/admin/ShowUserDept.zip . After supplying a NetID this script will show you the official department code, faculty/staff/affiliate status, and abbreviations for the college/department based on official university data for the user.

2) Where the user object currently resides. You can find this out from “Active Directory Users and Computers” on the “Object” tab for the user object. If you cannot see the “Object” tab make sure “Advanced Features” is checked on the “View” menu.

Knowing the official department of the user (and the fact they ARE a “faculty”, “staff”, or “affiliate” user) and their location you can now decide who to ask. Depending on where the user objects currently resides it may be either a departmental IT admin or an Enterprise Administrator. Make this decision and request as follows:

1) The Enterprise Administrators will NEVER move a user object that is already placed into a departmental OU to another OU. This is because that user object is already under direct control by someone, and may have departmental resources (such as home directory and roaming profile storage) allocated their IT staff. To get that user object moved you must directly contact the OU manager where the object current resides and work with them. When they have cleaned up the settings required they can move the user object to the “Relocation” container where you can pick them up. Enterprise Administrators seldom need to be involved (or even aware of) this process. If you don’t know who the OU manager is, look at the membership of the group that has control of the OU. This group is generally named “!<OU-name> Admins”.

2) The Enterprise Administrators will generally honor requests for a few faculty or staff user objects outside the official department as long as they reside in the general “Users” container. This is where all faculty and staff user objects reside if they do not have a managed departmental OU. These user objects will never have departmental resources associated with them. Requests are made via email to: its-ad-admins@iastate.edu

3) When users leave a department, it may take some time for their official university department data to be updated to their new department of employment. These users are moved to a container called “UsersInFlux”. This container is outside the normal “auto-drop” process and prevents users with “old department data” from being automatically moved back into the old department (which would happen if they were placed back in the general “Users” container). Departmental IT managers can request a faculty or staff user object from this container. Requests are made via email to: its-ad-admins@iastate.edu

4) User objects marked as “affiliate” accounts currently have no departmental data associated with them. Because of this they cannot be auto-dropped into any department (even the sponsoring department). Currently ALL affiliate accounts must be requested for manual moves. Requests are made via email to: its-ad-admins@iastate.edu

5) Requests for large numbers of users from other departments should result in the creation of a new OU for that department (based on the official department

abbreviation for the users). This OU can have control delegated to someone not in the department (the case where one IT manager may manage multiple departments). Such requests should be made as per the normal OU request process documented in "Requesting a Departmental/College Organizational Unit" at http://tech.its.iastate.edu/windows/admin/RequestDeptOU.pdf

Requesting Student Users Outside Your OU

Requests for moves of student user objects into departmental OUs are never honored. Student user objects can have "service-oriented" fields set by college level IT admins as per the "Student User Object Policy and Procedures" document at http://tech.its.iastate.edu/windows/admin/StudentObjects.pdf