

**Windows Enterprise
OU Administrator Policy and Procedures
Student User Object Policy and Procedures**

June 12, 2006

Last Update: August 17, 2016

Summary

College IT admins have requested the ability to provide “logon script”, “home directory”, and “roaming profile” support for their students. This ability is now provided by grouping all students into OUs by college and delegating control of the “service oriented” fields to college IT admins (total control of the student user object is not granted). The depositing of students into the proper OU and the daily movement between college OUs as students change majors is automated as much as possible based on official university data from the Registrar’s Office.

Procedures in Place

1. Students are placed into a “Students” OU structure according to college. One OU exists within the “Students” OU for each college (named “Students/<college>” using the official abbreviation of the college).
2. Newly registered students are “auto-dropped” into the Students OU structure into the appropriate college (based on their major at the time).
3. College IT admins have the ability to change certain “service oriented” AD fields for the students in their “Student/<college>” OU. These fields are for logon script, roaming profile storage, and home directory storage (items on the “Profile” tab of the user object). Exchange support may be provided in the future. Specific AD field names are:

- homeDrive (for home directory)
- homeDirectory (for home directory)
- profilePath (for roaming profile)
- scriptPath (for logon script)
- extensionattribute5 (for any use by the College of Engineering)

Once a college has the ability to alter “service oriented” fields for students it is termed a “managed OU”.

College IT admins are granted the power to change these fields by being a member of a security group given access to the fields as follows:

- AG - !Ag Student OU Admins
- BUS - !Bus Student OU Admins
- DSN - !Dsn Student OU Admins
- ENGR - !ENGR_Student_OU_Admins

H SCI - !H_SCI_Student_OU_Admins
LAS - !LAS_Student_OU_Admins
V MED - !V_MED_Student_OU_Admins

College IT admins have full control the membership of these lists, and can therefore grant anyone the power to control the service-oriented fields (including college IT admins outside their own college).

4. Students who change majors within the same college need similar resources provided by the college, so no user movement is done and no “exit strategy” is needed.
5. Students who change majors to a different college need to be moved from one “Student/<college>” OU to another. Three inter-college move cases exist:
 - a) Between two unmanaged OUs: There are no “exit strategy” issues. Such moves can be performed daily and immediately.
 - b) From an unmanaged OU to a managed OU: There are no “exit strategy” issues. Such moves can be performed daily and immediately.
 - c) From a managed OU to any other OU: There are “exit strategy” issues. See next section (“User Movement Out of a Managed OU”).

User Movement Out of a Managed OU

1. An automated “daily user movement” process will handle moves out of managed and unmanaged student college OUs as follows:

```
IF the user object is from a managed OU THEN
  Examine the service-oriented fields
  IF they are all cleared OR
    the homeDirectory and profilePath point to MyFiles server and others are clear THEN
    Move them to the new OU
  ELSE
    Do not move them to the new OU
    Include the username in daily notification to the college student OU admins
  ENDIF
ELSE
  Move them to the new OU
ENDIF
```

2. Notification of pending user moves will be done by email to a mailing list of the college IT admin’s choice. The format of the mail will be body-only (no attachments) with the subject “Pending <college-abbrev> Student Moves”. The body will contain pending moves of the following format (one per line):

```
<netid> -- <user-type> -- <college> to <next-ou> -- <field1>[,<field2>,...]
```

Where:

<netid> is the NetID (Windows login username) of the user with a pending move.

<user-type> is “student”, “faculty”, “staff”, or “affiliate”.

<college> is the college abbreviation of current student OU.

<next-ou> is the college abbreviation of the next student OU
(or “Users” if no longer a student)

<fieldn> is the name of a service-oriented field that is set to a non-null value

Example:

```
joeuser -- student -- ENGR to BUS—homeDrive, homeDirectory, scriptPath
```

3. Assuming the college student OU admins get daily notification of required user moves then the automated process will move them as soon as the service-oriented fields are cleared by the college admins. No communication of "I did this user - you can move them now" from the college staff back to ITS needs to be done. As soon as the fields are cleared by college staff the next daily user move will automatically move them to their proper OU (and they will be removed from the list of users that need attention by that college).
4. When a student is hired by a department they become “staff”. However, if they their user object currently lives in a managed student OU the above logic still applies. The staff user will not be moved until the college IT admin clears the service-oriented fields.
5. Whenever a college should have a user object but it is locked out from movement due to uncleared “service oriented fields” in a managed OU, the two college IT admins will be placed in contact with each other for coordination.

College Export Procedures

Since colleges already deal with students leaving college IT computing environments, existing college procedures will be used. It is the college’s responsibility to communicate with the student moving out of their IT management as to what resources can be taken with them and how they may be transported to their new environment.

Students Changing Majors After Classes Have Started

It is recognized that there will be a certain point in any semester when students are no longer likely to change classes even though that may formally change majors. A change of major can occur after the last day to add/drop a course, when the student probably wishes to complete the current coursework before taking courses in their new major next semester. If the student is changing majors within the same college it is a “no movement” issue. However, if they change majors to a different college AND they have “service oriented” fields set for the “current college” the pending move email will begin to be sent daily to the current college IT admins for the remainder of the semester.

It will be up to the discretion of the “current college” IT admins to allow the user to be moved (by clearing the “pending” fields noted above). If the “current college” IT admins choose to ignore the “pending move” email they will simply continue to receive it daily. Any request by the “new college” IT admins to gain control of the service oriented fields for the student in question will be referred to the “current college” IT admins for coordination.

Group Policy Needs for Roaming Profiles

As colleges implement roaming profiles for their students (on that particular college’s file servers) the question arises as to what happens when students with roaming profiles roam to various departments on campus. Preventing the roaming profile storage from growing without bounds is a problem as various applications deposit their information in the roaming profile. The “local cache” space on systems around campus can also grow as huge local caches of roaming profiles begin to be deposited.

An attempt at solving this issue involves two policy settings on “public” systems that people may “roam” to. These settings are enabled: “Only allow local user profiles” and “Prevent Roaming Profile changes from propagating to the server”. See the following document for more information: <http://tech.ait.iastate.edu/windows/admin/GPforRoamingProfiles.pdf>

Double Majors

Students with double majors in two different colleges will result in the student being placed in one of the college’s “Students” OU structure. Cooperation between the college IT admins will be necessary since both may desire to grant roaming profile, home directory, and logon script services.