

## Windows Enterprise Design OU User Placement Logic

September 6, 2002

Updated: January 20, 2012

Prior to the creation of college and/or departmental Organizational Units (OUs) all users (faculty/staff/students) were placed into the "iastate.edu/Users" container at the time they change their ISU NetID password. This "Acropolis AD NetID Population" process has been happening since April of 2000.

As the creation of college and/or departmental OUs (based on "official university names") occurs, faculty/staff users (but NOT students) can be moved into college or departmental OUs as soon as the OU administrator indicates they are ready for their faculty/staff users. Once this is done, the departmental OU administrators can reset passwords, home directories, profile storage, and other such tasks for their faculty and staff. The initial move (from the general "Users" pool into the OU) is a "mass move" done by an enterprise administrator (moving those existing faculty/staff with the matching college/department attributes from the general "Users" container into the proper departmental OU).

As new users for the college/departmental OU are created (via the automated "Acropolis AD NetID Population" process) they are not placed into the general "Users" pool. An attempt is made to automatically place them in their correct OU. The logic that is applied (as each new user is created) is the following:

Note: "college" can be either a college (like "Business", "LAS" or "Engineering") or a major operating-unit (like "AIT")

```
Look up official "college" and "dept" for the username from university data
IF the user is a "student" THEN
  Place the user in the "iastate.edu/Students/<college>/Users" container
ELSE /* the user is "faculty" or "staff" */
  IF a "<college>/<dept>/Users" OU exists THEN
    Place the user in the "iastate.edu/<college>/<dept>/Users" OU
  ELSE /* No departmental Users container */
    IF a "<college>/Users" OU exists THEN
      Place the user in the "iastate.edu/<college>/Users" OU
    ELSE /* No college Users container */
      Place the user in the "iastate.edu/Users" OU
    ENDIF
  ENDIF
ENDIF
ENDIF
```

As you can see, it is important for the college/departmental OU administrators to make sure a “Users” container (created at the time the OU is set up) is present at the college or departmental level. As new users are deposited there, they may be moved elsewhere in the departmental OU (no automated process will move them back to the original “drop” location). However, if the college or departmental “Users” OU is deleted the above logic will cause new departmental users to be placed in the general “iastate.edu/Users” container (out of reach of the OU administrator).

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

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