Windows Enterprise Design
ListSync
Official University Lists as Global Security Groups

November 3, 2009
Last Update: April 16, 2012

ListSync Overview

"ListSync" is a feature of the Windows Enterprise Domain. ListSync is a process that automatically populates "official university lists" into Active Directory as "Windows Global Security Groups". These Global Security Groups contain as their membership the NetIDs (which are also login accounts in the Windows Enterprise Domain) of the people who are on that "official list".

Windows Global Security Groups can be used for access control of resources (just as lists can be used to control access to UNIX resources). Access to files, printers, desktop systems, etc. can be controlled based on "security" permissions given to an individual or a Global Security Group. Since official lists are automatically updated as people come and go from those "official areas", the day to day maintenance of the "official" groups is greatly reduced for departmental IT administrators, faculty and staff.

The Global Security Groups created in the Windows Enterprise domain are synched with the Unix-style lists (sometimes called "Moira lists"). For example, a list of all the people with an "Art" undergraduate major can be seen on a UNIX system with the "chlist –m art_ugrad" command. This same list is pushed down as a Global Security Group named "art_ugrad" within the Windows Enterprise Domain. All the official university lists are stored in the "AutoLists" OU, broken down into sub-OUs by their type (ClassLists, CollegeLists, DeptLists, and MajorLists). There is only ONE exception to the "identical naming convention", and that is "instructor" lists for classes. In UNIX, the name will be similar to "class/instructors". Since the "forward slash" is problematic is Windows, the name is translated to "class-instructors" when it is created as a Windows Global Security Group.

Class lists are a special case. FERPA regulations are very strict about privacy issues relating to disclosing what classes a student is taking. As a result, a special structure is created for a class list that allows anybody to use the name of the class's Global Security Group for access control, but only the "instructors of record" can actually view the membership of the class. This structure also prevents anyone from seeing what classes a student is taking by viewing the "Member Of" tab (in "Active Directory Users and Computers"). Any class-list based groups they are a member of will appear as "hsg-<nnnnnnnn>" (obfuscating the actual name of each class they are taking).

Types of Lists Processed

The following lists are pushed down to Active Directory as Global Security Groups:

- College Lists – Members of each college
- Major Lists – Members of each major
- Class Lists – Members of each class. These are only pushed down if the instructor has elected to have the computer class list created. Creating a class list is covered in the following IT Services FAQ:
  http://www.it.iastate.edu/faq/view.php?id=250
- Department Lists – Member of each department (based on which department processes the employee's "Vacation and Sick Leave" cards).

Private lists (created via ASW or UNIX "chlist" commands, for example) are never synchronized down in the Windows Enterprise Domain.

IMPORTANT Rules for Departmental OU Administrators

There are a couple aspects of the official-list-based "Global Security Groups" that OU Administrators should be aware of.

OU managers are strongly advised to place a "!" in front of group names they create. This is covered in section 8 of the "Enforced Conventions for User and Group Names" document at:

http://tech.its.iastate.edu/windows/admin/enforced.conventions.pdf

If you create a conflict with one of the official class list names you will break the synchronization process and IT Services will be contacting you to change the name of your group. If ITS cannot contact you a "!" will be placed in front of the group for you (to let the automatic synch process continue). Duplicate names should not be much of a problem as the official names are long and ugly enough discourage this mistake. Avoid the naming convention used for the official lists in all cases (and always use a preceding "!" in your group names).

OU managers are STRONGLY cautioned to NEVER delete a NetID-based user object (those whose login name does not start with a "!"). This will remove the user object AND remove it from all security groups it is a member of (including the official college, major, department, and class groups). Having the user recreate the user object (by changing the password in ASW) WILL NOT repopulate all the group memberships! Staff often leave departments and come back as students (or employees in other areas). Repopulating official groups is a manual process and there may be considerable delay until the official groups are repopulated. Private list

membership is never recovered (unless each group owner adds the individual user back to each group). Follow the guidelines in the "Managing Users Within a College/Departmental Organizational Unit" document at:

http://tech.its.iastate.edu/windows/admin/UserMgmtInOUs.pdf

ListSync Update Schedules

The time at which a change to an official university list gets reflected within the Windows list-based global security groups varies from "minutes" to "overnight", depending on the type of change. An overnight process (called the "Master Update" in this document) handles many changes in a batch process. This nightly process runs after midnight, every night. As a result, when the Registrar's Office records a "class add/drop" for a student the change will generally not appear in the security groups until the next day. The various types of changes and their update schedules follow.

Administrative Changes

The most common "administrative change" is for someone to become (or be removed as) an "Instructor of Record" for a class. These updates happen during the nightly Master Update.

List Creation Changes

When an "Instructor of Record" uses ASW to create a class list for the first time, the class-list-based security group is created and populated with the members of the class within several minutes*. The membership is defined by the previous nightly Master Update.

College, Major, and Department lists are created automatically at the "master" level.

List Membership Changes

Note: In all cases, membership of a class-list-based group depends on an "Instructor of Record" having created it previously (see previous section).

- New student registering for NetID for the first time

  These students are made members of their college, major, and class lists within several minutes* based on the information available at the previous nightly Master Update.

- Student with NetID who adds/drops a class (and/or changes majors)

These updates happen during the nightly Master Update.

- Student who drops out of school

  These updates happen during the nightly Master Update.

- Employee changes within a department (new hires/termination)

  These updates happen during the nightly Master Update. The Master Update data can only be kept up to date based on how soon and how correctly the departments enter their data to Human Resources.

  Sometimes there is a considerable lag in the time an employee leaves the university and they are removed as a member of the department. ITS is looking into this issue.

* "several minutes" is dependant on other list processing requests going on at the time. Requests are queued for processing and if a large number of simultaneous requests exist it may take many minutes for a request to complete.

Frequently Asked Questions

Why are the names of the groups so strange and long?

The names are based off the official university abbreviations for the college, majors, and departments. Class list names are based off the course number, section, and semester of offering. Remember – you can always nest the "official group" within your own private security group to use a shorter name. Remember to use a "!" as the first character of your group name!

How do I get a person on or off an official departmental group after they are hired or leave?

Since the membership of these groups is based off official university records, the official university information has to be in place. Sometimes a delay is caused if the proper "Personnel Action Form" is not completed. In general this involves Human Resources for Department lists. Your departmental secretary may assist you in getting this changed. Once the official university information is changed it will filter into the official university lists (and security groups) within a day or two.

A staff person is listed in the wrong department! How do I fix this?

Since the membership of these groups is based off official university records, the official university information has to be changed. In general this involves Human Resources for Department lists. The "official" department associated with a staff person is generally the department that processes the employee's "Vacation and Sick Leave" cards. Sometimes this is not the department an employee really wants to be seen as their "official affiliation". Your departmental secretary may assist you in getting this changed. Once the official university information is changed it will filter into the official university lists (and security groups) within a day or two.

I am an instructor. How do I create a class-list-based global security group for my class?

Creating a class list is covered in the following IT Services FAQ:

http://www.it.iastate.edu/faq/view.php?id=250

I am an instructor. How do I manage daily adds/drops to my class-list based security group?

Since the membership of these groups is based off official university records, the official university information has to be changed. In general this involves the Registrar's Office for students (College, Major, and Class lists). Once the official university information is changed it will filter into the official university lists (and security groups) within a day or two.

How can I view the membership of class lists?

FERPA privacy guidelines mandate the privacy of what classes a student is taking. You must be made an "instructor of record" by your department to be placed on the "instructors" group for the class. Once you are an "instructor of record" you will be able to view (but not update) the membership of a class-list based security group. In general your departmental secretary can assist in making someone an "instructor of record" for a class.

If I cannot view the membership of hidden class lists, how can I write a login script that makes decisions to mount drives based on class group membership?

Use the "ifmember.exe" program from Microsoft and check for membership in the visible class-name group. Documentation on getting and using "ifmember.exe" is available here:

http://tech.its.iastate.edu/windows/admin/groupawarescripts.pdf

What about students with double-majors?

Double majors are handled correctly. The person will appear in each college and major list for each major. Persons with more than two majors will have only two

majors processed into official university lists/groups. The rules as to which two are selected are not researched at this time.

How often are updates done?

When a NEW user registration happens, the user status present the previous night determines their security group membership. For changes to EXISTING users, the updates are done nightly (so a change during the day will appear the following day).

Are these lists mailing lists?

All Class and Major lists are also mailing lists. Take the list name, append "@iastate.edu" to the end, and it will function as a mailing list. College lists are never mailing lists (to avoid easy SPAM generation to a wide audience). Department lists are by default NOT mailing lists, but the department can request them to be a mailing list. This information is covered in the following IT Services FAQ:

http://www.it.iastate.edu/faq/view.php?id=250

Can I cause a list I created to be synchronized as a Windows security group?

Yes. See http://tech.its.iastate.edu/windows/admin/ListSyncUserReq.pdf

References

Managing User and Group Objects in Departmental OUs

Enforced Conventions for User and Group Names
http://tech.its.iastate.edu/windows/admin/enforced.conventions.pdf

Managing Users Within a College/Departmental Organizational Unit
http://tech.its.iastate.edu/windows/admin/UserMgmtInOUs.pdf

FERPA Privacy Guidelines

- What Faculty and Staff Need to Know About FERPA
  http://www.registrar.iastate.edu/info/ferpa.pdf
- FERPA Notification of Rights
  http://www.registrar.iastate.edu/info/ferpanotice.html

NetIDs

Master Directory Sources
http://tech.its.iastate.edu/windows/admin/EnterpriseMastering.pdf

The Care and Feeding of Iowa State Net-IDs (archive document – not current information)
http://www.tech.its.iastate.edu/windows/admin/ggs317.pdf

Using Class Groups in Login Scripts

Creating Group-Aware Logon Scripts
http://tech.its.iastate.edu/windows/admin/groupawarescripts.pdf