Groups Service Basics

Contents

This page presents basic introductory information about the UW Groups Service to give context for use through its browser interface (groups.uw.edu) and via the Groups Service API.

Similar information is available in the UW Groups article in IT Connect.

Overview

The UW groups service is a central location in which groups can be created, managed, and then reused in other services and applications. Groups can be created from various sources of group information and used in a wide variety of integrated services and applications, as illustrated in Figure 1.

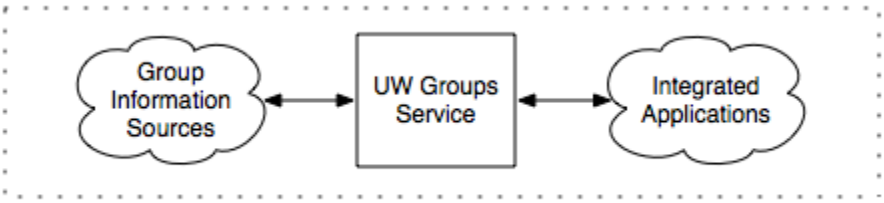

Figure 1. Groups service relationship to information sources and applications.

Some groups are managed by individual people and teams for ad hoc purposes such as collaboration, communication, or access control. Other groups are managed by UW organizations or institutional processes such as UW course enrollments or UW employee appointments.

This diversity of group information sources and varied application uses is enabled by a delegated model of management authority: any member of the UW community can use the service to manage groups under his/her authority and delegate that authority to others as needed. Individuals can do this by themselves or as part of a team or organization.

You can access the web browser interface by logging in using your personal UW NetID. Access using shared UW NetIDs (also known as supplemental accounts) is not supported. However, you can use your shared UW NetID to name and identify groups.

Programmatic access to the REST API requires client authentication using a X.509 certificate issued by the UW Services CA. Once authenticated, applications can create, read, update, and delete groups for which they are authorized to do so.

Groups may be classified according to UW Administrative Policy Statement 2.6 (Information Security Controls and Operational Practices). All groups are assigned "unclassified" status until an administrator has intentionally applied a "Public", "Restricted", or "Confidential" classification.

Groups Usage

Groups are well suited to applications involving lists of identifiers for people (or other entities), where the application needs to know whether someone is a member of a group or needs to obtain the entire membership of the group.

Common uses of groups in applications include email, collaboration, calendaring, access control, purchasing, sharing, voting, scheduling, federating, surveying, and polling.

Purpose / Usage	Description
Email	Communicating via email with a group
Collaboration	Communicating and sharing resources among a group
Calendaring	Scheduling events and/or sharing calendars with a group
Access Control	Managing and reviewing access to resources based on a group
Purchasing	Providing software and other resources for purchase to an eligible group
Sharing	Distributing resources to a group
Voting	Putting choices to a vote by a group
Scheduling	See Calendaring
Federating	Asserting group membership to 3rd party applications via federation
Surveying	Conducting surveys with a group
Polling	See Surveying

UW Group IDs

The UW groups service uses a structured namespace for group identifiers, known as UW Group IDs, permitting UW people and organizations to create and manage groups independently. Each group has a unique UW Group ID. Systems and applications using UW Groups typically refer to groups using UW Group IDs.

UW Group IDs consist of lower-case letters (a-z), digits (0-9), dash ("-"), dot (".") and underscore ("_"). The underscore character is used to separate components of group IDs, much like slash ("/") or backslash ("\") is used in URLs or filenames. Refere to the UW Groups Naming Plan for more information.

If you want to create a new group, you can do so if you have appropriate permission (see Access Controls below) on an existing group. You can see what groups you administer using the "My groups" tab (instructors also see their courses via My groups). For example, if you have Admin or Create access to the "uw_pavesci_admin" group, you could create a group called "uw_pavesci_admin_fulltime". You should choose a UW Group ID appropriate for the expected use of the group, bearing in mind that the group may be used by many people for a long time.

If you need to create a new namespace for UW Group IDs in the UW groups service for your organization, refer to the Home Groups page to learn more.

Group Memberships

In the UW groups service, individual groups may include members using several types of identifiers:

Identifier Type	Example	Comment
UW NetID	bob234	Any type of UW NetID may be used as a group member
Federated ID	bob456@example.edu	An ID from some non-UW identity service provider, in user@domain format
DNS name	sys789.org.washington.edu	Any DNS name, typically subject names in UW CA-issued X.509 certificates
UW Group ID	uw_org789_all_tmp	Other UW Group IDs can be members of groups.
UWWI Computer	luke$	The netbios name of a computer joined to UWWI followed by a "$" character

When adding members, the groups service verifies that member entries are valid, except for federated ID values; to add a UW Group ID as a member, you must have permission to view the membership of the member group.

Some systems and applications using the service may be limited in the types of members they can handle. For example, the use of federated IDs for access control wouldn't apply in an application that only accepts logins by UW NetID.

When viewing group memberships, "direct" members are those members that are listed in a group's membership, directly; while "effective" members include all direct members, plus members of any groups listed as members, recursively.

Administrators, subgroup creators, and member managers are not automatically added as group members.

Members can join and leave group memberships on their own if they're permitted to do so by the group administrators use of the opt-in and opt-out permissions.

Viewing the memberships of groups classified "Confidential" requires a valid 2-factor login session.

Access Controls

The UW groups service provides controls to manage who can create, update, and delete group information. All groups have these controls:

Control	Role Name	Purpose
Admin	Administrator	Permits all operations on the group, including update, delete, create subgroup, manage members, and view members
Create	Subgroup creator	Permits new subgroup creation; i.e. new UW Group IDs using this group's ID as the prefix
Update	Member manager	Permits adding and removing members of the group
Member View	Membership viewer	Permits restricting who can view a group's membership, including no restrictions
Opt-in	Opt-in population	Permits individuals to join a group membership on their own
Opt-out	Opt-out population	Permits individuals to leave a group membership on their own

Access control entries can have any of the types of identifiers that group memberships can have: UW NetID, UW Group ID, federated ID, DNS name, or UWWI computer.

An organizational home group has an initial set of users with Admin control, as requested by the organization. You have Admin access to your personal home group when it is created. These controls can be modified at any time so you can control access as needed.

The creator of a group is automatically added as an Admin of the group. In those cases where this isn't desirable, return to the Edit page after group creation and remove the entry. Make sure that at least one other person or group is listed as an administrator.

Changing access controls on a group affects only that group. It has no effect on controls in any other existing groups.

Enhanced Security

Each group has an security attribute that controls whether or not a valid 2-factor login session is required to administer the group. This attribute is located under the administrators control, enabled via an "enable enhanced security" checkbox.

Any administrator of a group can enable enhanced security, but doing requires a valid 2-factor login session.

With enhanced security enabled, editing group information, deleting, moving/renaming, and changing membership requires a valid 2-factor session, except for groups with opt-in/opt-out enabled, in which case users can join/leave without doing 2-factor authentication.

Since application clients currently have no way to perform strong (higher-assurance) authentication, programmatic clients of the GWS REST API cannot update/delete groups with enhanced security enabled. For the same reason, the enhanced security attribute itself cannot be enabled or disabled via the GWS REST API, although it will be present in representations retrieved via the REST API.

Further Reading

Now that you're familiar with the basics of the service, you may want to browse the user interface by signing in to groups.uw.edu using your personal UW NetID.

For further reading on some of topics mentioned above refer to these pages:

Home Groups
UW Group Naming Plan
Groups Service Architecture
Institutional Groups