



HARVARD UNIVERSITY
Information Technology

Overview of IAM Group Services

December 22, 2017

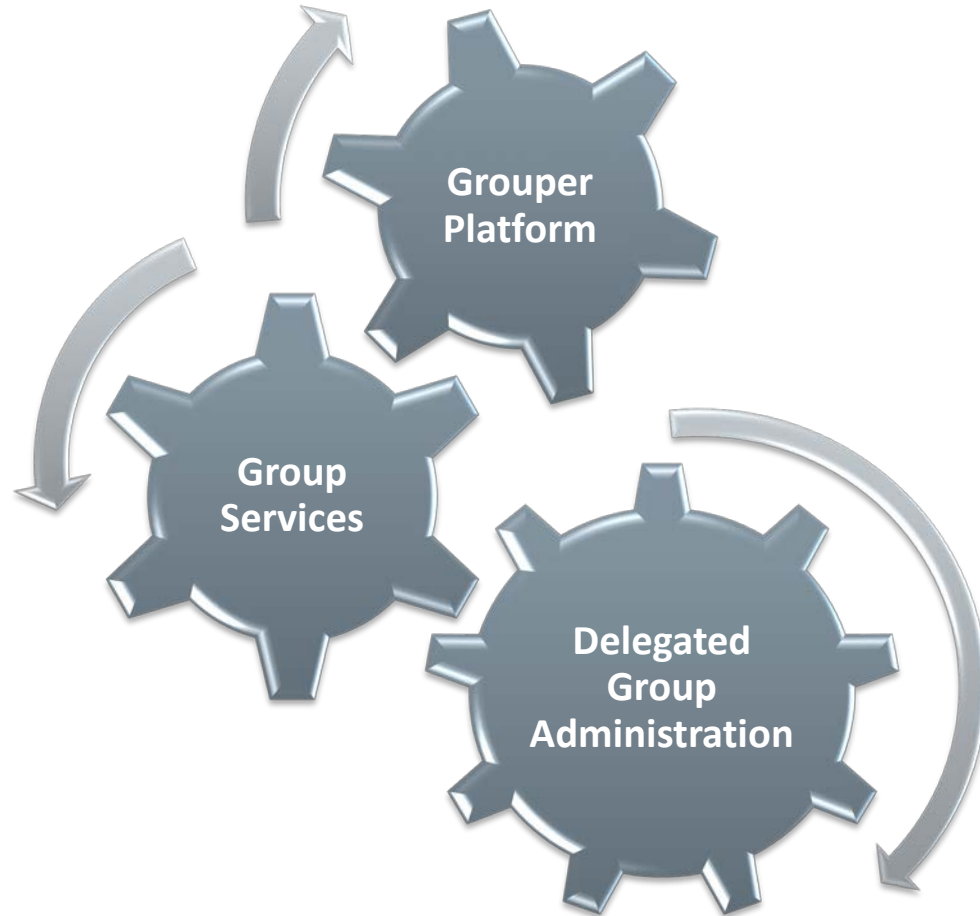
Groups Enable Other IT Services

Groups are a critical component of these IT Services

Access Control (available now)	<ul style="list-style-type: none">• Enable application access for eligible users (authorization)• Authorization options through HarvardKey & API• Automatically removes access as eligibility ends
Communication (start in FY19)	<ul style="list-style-type: none">• Email or texting messaging to targeted audiences• Broadcast Communications
Collaboration (future)	<ul style="list-style-type: none">• Simplify document sharing to collaborators• Enable controlled file sharing (individuals and groups)

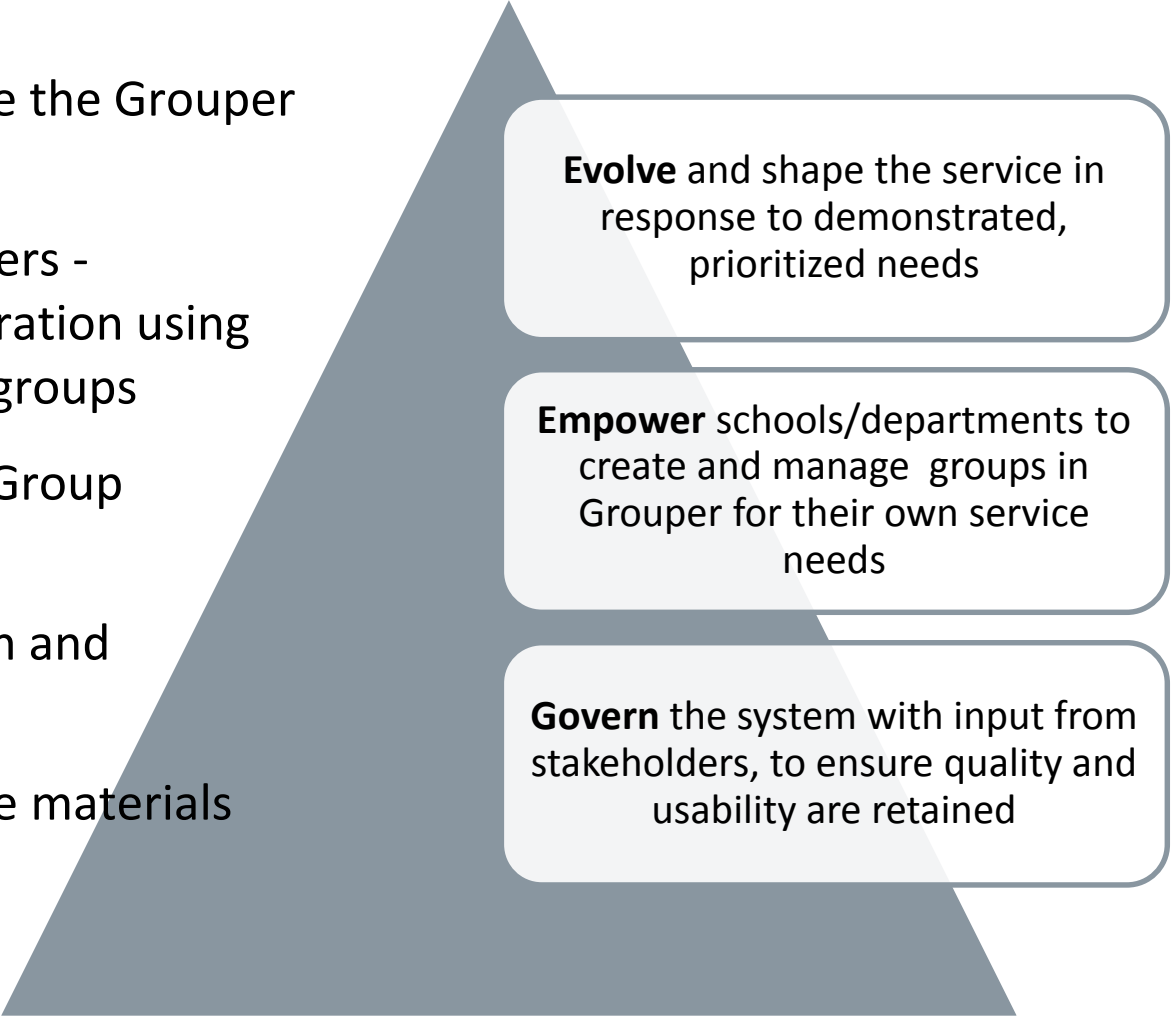
IAM Group Services Overview

Group Services drives the evolution of the **Grouper Platform** and the adoption of **Delegated Group Administration** by schools and departments



Group Services Activities and Guiding Principles

- Build and operate the Grouper Platform
- Onboard customers - application integration using HarvardKey and groups
- Train Delegated Group Administrators
- Perform outreach and consulting
- Provide reference materials
- Tier 2-3 support

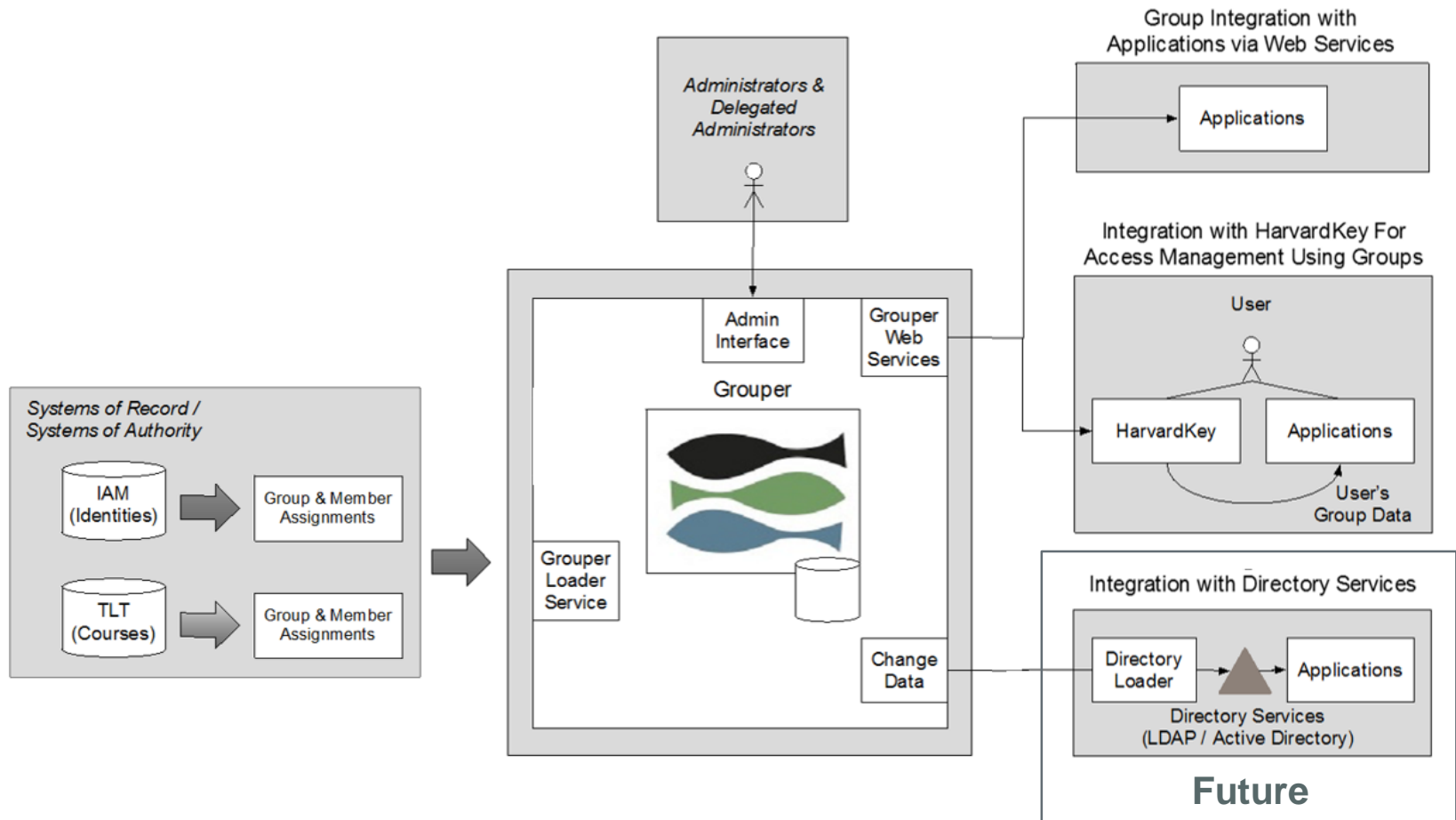


Evolve and shape the service in response to demonstrated, prioritized needs

Empower schools/departments to create and manage groups in Grouper for their own service needs

Govern the system with input from stakeholders, to ensure quality and usability are retained

Groups Services Platform



Grouper



A group management system;

- An open-source application provided by the Internet2 consortium; used widely among universities - <https://www.internet2.edu/products-services/trust-identity/grouper/>
- Integrated with IAM identity and TLT course data so that group memberships are updated automatically
- Used by school and department IT Service Providers to manage groups directly or via API for application authorization access
- A web tool for delegated group administrators to manage groups for their local needs

Grouper is NOT directly accessible to faculty, staff and students at this time

HarvardKey Integration with Group Services

Used for web-based application authorization for **CAS** or **SAML** clients.

Two methods which can be used alone or together.

Group Authorization Filter –

After authentication, HarvardKey checks if the person is in a particular group, e.g., authorized-users-omni. If so, then access to the application is granted.

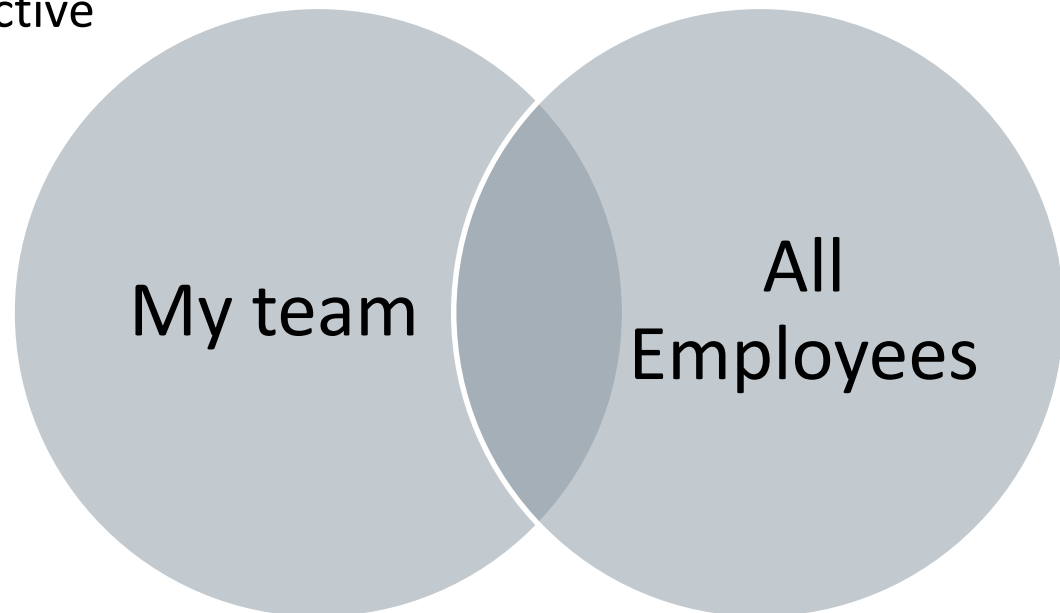
Group Attribute Release –

CAS or SAML release the groups a person is a member of in their response back to the application. The application then determines what to do with that information. Can be used for more granular level of permissions, e.g. standard or superuser permission.

The Value of Reference Groups

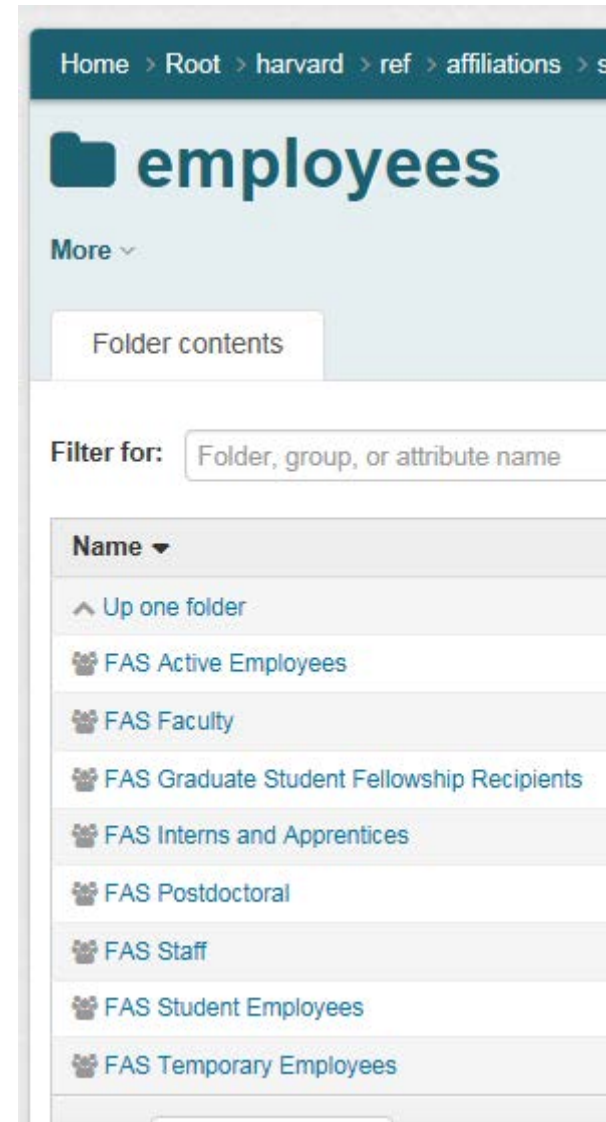
Reference groups are automatically updated daily based on the system of record feeds to IAM and TLT

- Using reference groups, you get “only current members” and this supports authorization objectives
- By intersecting reference groups with your own custom groups, you can ensure that the membership of your custom managed groups is automatically updated to remove people who are no longer active



Reference Groups Build-out

- Reference groups are automatically updated daily based on the system of record feeds to IAM and TLT
- Today reference groups are only built out to the school – high level department depth
- We have 400+ reference groups available today
- Additional reference groups are built out upon request (e.g. at the department level)

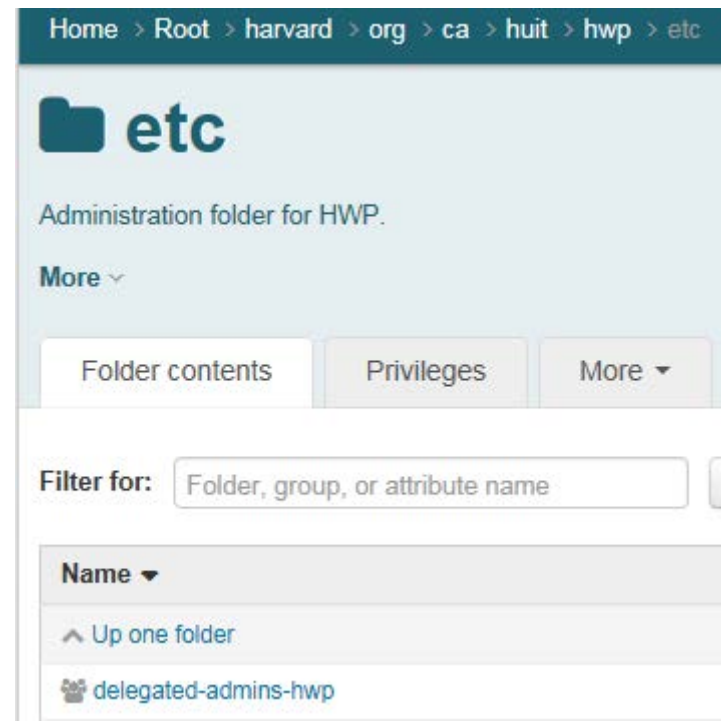


Delegated Group Administration

Grouper is ... designed for the highly ***distributed management environment*** and heterogeneous information technology environment common to universities [Internet2].

Delegated Group Administrators

- Interacts directly with Grouper to create and manage groups
- Receives training and observes IAM group conventions
- Provides Tier 1 support for their school/department
- May designate additional delegated administrators



Group Services - Point Persons

- Anne Margulies asked all CIOs to designate a point person for group services
- To date we have point persons in most of the schools. Those we don't have are represented at the monthly Group Services Workgroup
- Point persons have access to Grouper and are responsible for the management of the groups beneath their organization folder within Grouper
- Point persons determine who are delegate group administrators for their organization.



How Can I Use The Service

IAM Product Operations supports the Group Service.

Group Service	How To Use The Service
Access Control for Web Applications using HarvardKey and Groups	iam_help@harvard.edu Submit a request to integrate an application with HarvardKey. http://iam.harvard.edu/files/iam/files/cas-saml-spusagerequest-form.pdf
Delegated Group Administration	Depending on your application needs we will provide consultation, training and onboarding for you to manage groups as you need.
Custom Group By Request	Users are directed to iam_help@Harvard.edu from within Open Scholar and Wiki

Service catalog listing and related documentation projects are in progress.