Trusted Access Platform Training Use Cases

Training Coming Soon!

This course series will explore solutions for four common identity and access management Problem and Solution sets:

(A) Managing Access

Whether you are on a campus, with a research organization, or a company, managing access to multiple resources can quickly overwhelm you and other staff members. Higher Education in particular has the complex situation of having many people with many roles that require a large variety of access rights to it's resources.

Using groups as the primary means for access means having a group management system that is intuitive and easy to use.

The Grouper software component of the Trusted Access Platform facilitates enterprise-level access management and authorization by grouping uniq ue institutional identities (UIDs) into groups that can be associated with classes, class materials, and other resources. It also provides many powerful features for managing the access rights of the identities easily over time with little effort.

The Scenario

Stephen Hawking is a new student in your system. His interview for enrollment identified him as being highly proficient in math and the faculty would like him to assist them with updating math faculty resources.

The Math Faculty must facilitate adding all of the new math students to the basic curriculum resources and additionally they would like to give Stephen the ability to update curriculum resources and access some student information for tutoring purposes.

Using Grouper the Math Faculty can be added to a group with delegated authority for adding or removing student identities from groups associated with Math Faculty Resources. Then any of the Math Faculty members can add Stephen to groups that have R/W access to those resources and read access to certain students who have Opted-In for tutoring.

Now the Math "team" would be able to manage access and authorization to these resources independently from Central IT.

Replicate that across all departmental resources and applications and you can realize a large optimization in people's time and effort.

The Demonstration / Training

Bring up an instance of Grouper pre-populated with Math Faculty, groups representing admin for certain resources (this could be spaces), and groups representing students, students who opt-in for tutoring

(B) Creating Collaboration Infrastructure for Research and Scholarship

Research organizations and virtual organizations have similar issues - people coming from various places bringing an identity with them, and needing access to various tools and ways to collaborate.

The Scenario

Imagine researchers and administrators working together on a groundbreaking research effort while being based at numerous different universities and research institutes. To facilitate their teamwork, these collaborators need to share documents, set up institution-independent mailing lists, coordinate calendars, and use a protected wiki to capture their efforts. Their collaboration needs to be protected, but the focus needs to be on the collaboration, not the technology.

The Demonstration / Training

Bring up an instance of COmanage, Confluence, Grouper pre-populated with Faculty Researchers from several fake institutions, groups representing admin for certain resources (this could be spaces), and groups representing researchers working on 3 or 4 different aspects of a project with associated mailing lists to communicate. They can all have access to the protected wiki but there will be several pages specific to the different aspects details.

(C) Guest Systems

Many organizations would like a way to manage guest (affiliation) access that doesn't require creating accounts and provisioning guests through the normal ERP system. This session will provide a solution.

Overview of the Colorado State University Guest System

(D) Identity Onboarding and LifeCycle Management

Identifying users in a unique way that can then be used to provide access to institutional resources, and later change or withdraw that access can be a challenging process and prone to many problems. Students are the most problematic as there are vast numbers of them and what they should or should not have access to and what level of access may frequently change during their enrollment time and even afterwards as alumni. Staff and faculty, though smaller in number, have similar issues.

The Trusted Access Platform can be integrated with existing systems of record SOR, such as HR, such that events like hiring, student admissions, etc. will trigger the creation of a unique institutional identity (UID) and associate that identity with basic known attributes from the SOR and then store the identity in a registry with those attributes.

Additionally, the identity can also be added to groups associated with access to classes, course materials, applications and other resources automatically (provisioning).

Similarly, additional events triggered by changes in HR or other SORs can change or revoke the identity access rights automatically (de-provisioning).

The Scenario

Stephen Hawking is a new student in your system. His interview for enrollment identified him as being highly proficient in math and the faculty would like him to assist them with updating math faculty resources.

The Demonstration / Training

As a part of the normal business process for students assisting faculty, Stephen will be hired as a research assistant in the HR system. Stephen will appear to be a new person to the HR person, so it will send a message to midPoint to create Stephen in the registry. The registry discovers Stephen already exists by running its search match process, and updates the registry with the HR system identifier. An updated person message is sent out by the registry, prompting Grouper to retrieve information about Stephens employee status and department and adds Stephen to basis groups resulting in an employee affiliation. Midpoint receives a message about the employee group affiliation and adds the employee role to Stephen.

After two semesters, Stephen decided to stop working to focus on studying, the HR system marked Stephen as terminated. A message from the HR system about the termination is sent to midPoint which marks Stephen as inactive for the HR resource and published an updated person message. Grouper retrieves this message, and processes changes to basis groups resulting in the loss of employee affiliation. A message about this change is picked up by midPoint, which removes the employee role from Stephen.

Students will work through an integrated demo environment and learn how InCommon Trusted Access Platform components can work together to solve common IAM challenges.

(E) Federating Organizational Applications (SPs)

Many times institutions that support many of their own applications would like to provide secure access to those applications such that outside Faculty or Student can collaborate on projects or in other way through those applications. Managing many inside and outside user accounts /passwords is cumbersome and time consuming. Federating those applications as Service Providers (SPs) provides a means to securely provide access by verifying users via Federated Identity Providers (IdPs) both internally and for select external institutions or organizations.

The Scenario

write this

The Demonstration / Training

write this