Guest Management Systems at Colorado State University

Contents

CSU Overview and Populations

Colorado State University is a public, land-grant, research university founded in 1870.

It has three campuses: CSU Fort Collins, CSU Pueblo, and CSU Online.

It has approximately 30,000 students including 4,000 graduate students, 7,500 employees including 1,600 faculty, and 200,000 active alumni.

- Members include students, faculty, staff, emeritus and retirees.
- Affiliates include student applicants, research associates, affiliates, federal associates, guest associates and visiting associates.
- Guests include alumni, parents, family, donors, vendors, and library patrons.

Middleware and Identity and Access Management (IAM) is a department in Academic Computing and Networking Services under the Vice President for Information Technology.

CSU Identity and Access Management Architecture

- **CSU eID** (electronic identity) is a locally-developed system that currently manages identities of most Fort Collins internal identities, including members and affiliates.
    - Data comes from two sources:
        - The **Human Resources Management System (HRMS)** contains faculty, staff and affiliate data in Oracle HR. (Data is retrieved through the CSU Operational Data Store (ODS).)
        - **Banner** is the Student Information System which contains instructor, student, course, and enrollment data in Oracle.
    - Data is stored in a SQL Server database
    - Data is accessed via an ASP.NET/C# web application.
- **COmanage** currently stores both internal and external identities.
- The **CSU Patron Registry** is a locally-developed system that currently manages library patrons who are community members but not CSU members.
    - **Alma** is the library catalog, which also stores and manages patron accounts.
    - **Primo** is a website to search the library catalog, request, borrow and renew books and materials, pay fines and fees.
    - Library patrons can also log in with their patron ID to use library computers and printers.
- **MidPoint** is expected to replace eID, the Patron Registry, and COmanage to store internal identities for members and affiliates of all three campuses in 2019 or 2020.
- **Shibboleth** is used for single sign-on to log in to CSU systems using CSU eID.
- The **Cirrus Identity Social-SAML Gateway** is used by external users to log in to CSU systems using their social accounts (Google, Microsoft and /or Facebook).
- **Active Directory** and **OpenLDAP** are LDAP implementations used for authentication and storing local credentials and group memberships.
- **Grouper** is increasingly used by CSU applications for authorization and distributed group management.
- **Microsoft Azure Service Bus** and **RabbitMQ** are cloud-based message queue systems used in COmanage, Grouper and LDAP provisioning.
- **Visual Cron** is process scheduling software that is run on Windows Server.

Colorado State University IAM Core Architecture
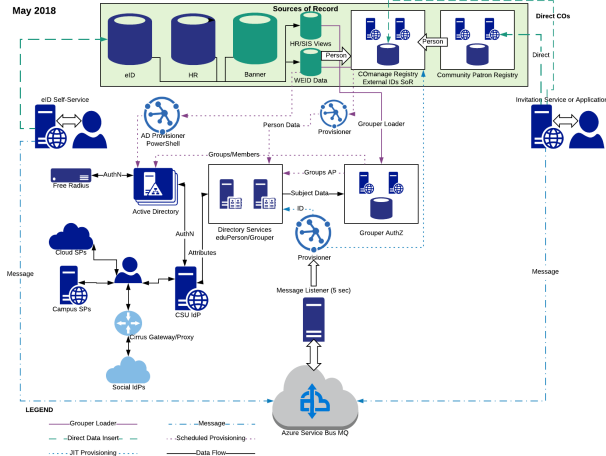
CSU IAM Strategy 2018
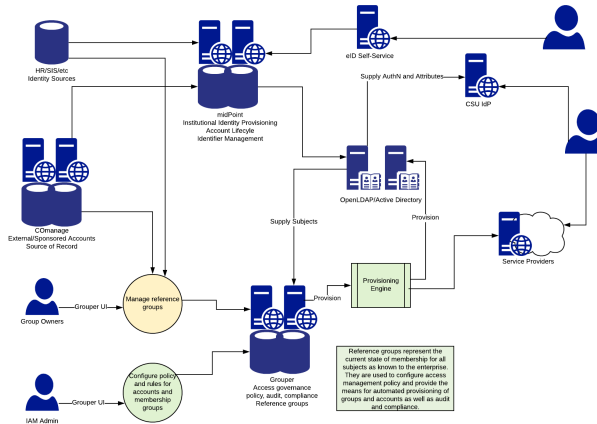
CSU Invitation Management System

The CSU Invitation Management System is a locally-developed system to store and manage invitations of external users who are invited to be authorized to use CSU-managed web applications.

General Workflow

1. A CSU member uses a CSU application to request that an an external person be granted access to a CSU application.
2. The CSU application sends a message to the message queue.
3. A console application processes each message in the message queue. It validates the message data, creates an invitation in the database, and sends an invitation email to the external person.
4. The external person reviews the invitation email and clicks the invitation link.
5. A web page prompts the external person to log in using either their CSU eID or their social account.
6. A web page displays a brief summary of the invitation (requester, invitee, application, and status).
7. The external person checks a box accepting the terms of use, and clicks a button to accept the invitation.
8. The application stores the acceptance in the database, checks for an existing record, creates or updates a COmanage account, creates or updates an LDAP record, and displays a link to the application.
9. The external person clicks the link to the application and logs in (if not already logged in).

Architecture

- The **Invitations message listener** processes and validates message queue requests, creates invitations, and sends invitations via email. It is a C# console application.
- The **Invitations website** can create, display, and accept user invitations, and allows application and Middleware admins to view and manage the invitations, requesters, invitees and applications for which they are authorized. It is an ASP.NET/C# web application.
- The **Invitations database** is a SQL Server database which stores information about invitations, requesters, invitees, and applications.
- **Visual Cron** is used to run the message listener every minute.
- The **Microsoft Azure Service Bus** is used to receive, queue and dequeue messages containing invitation requests.
- **Shibboleth** and the **Cirrus Social-SAML Gateway** allow users to sign in using their CSU or non-CSU credentials.
- **COmanage** and **OpenLDAP** store data about the external person, including names, CSU and non-CSU identifiers and email addresses, and groups.

- **Grouper** contains a group of admins for each CSU application using the invitation system, and a group listing Middleware admins of those groups.

CSU applications currently using the invitation system

Alumni: RAMrecords

Provides alumni access to their student records.

Alumni can view grades, transcripts, billing, tax info, and test scores.

Parents: FAMweb

Provides access to student records to people the student trusts and invites, including parents and other family members.

Students can authorize them to view the student's grades, transcripts, class schedule, financial aid, tax and billing information, and pay the student's bills.
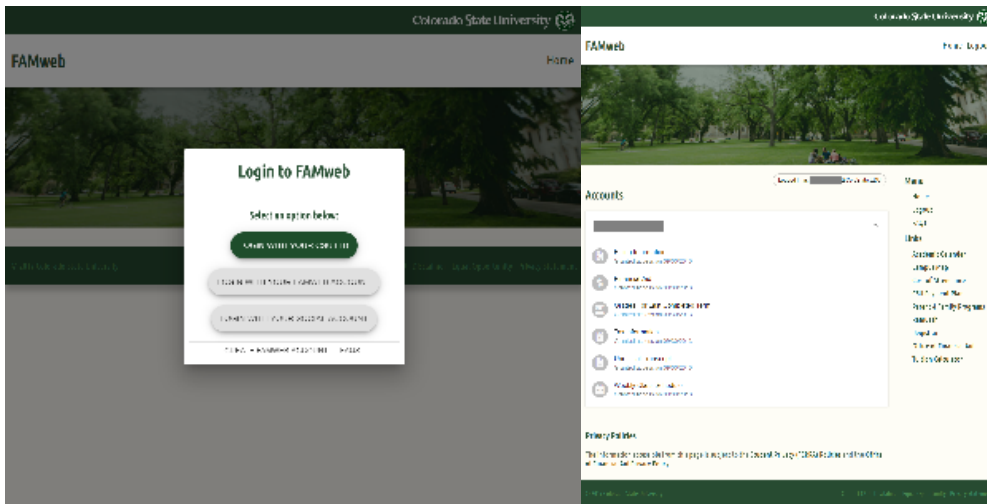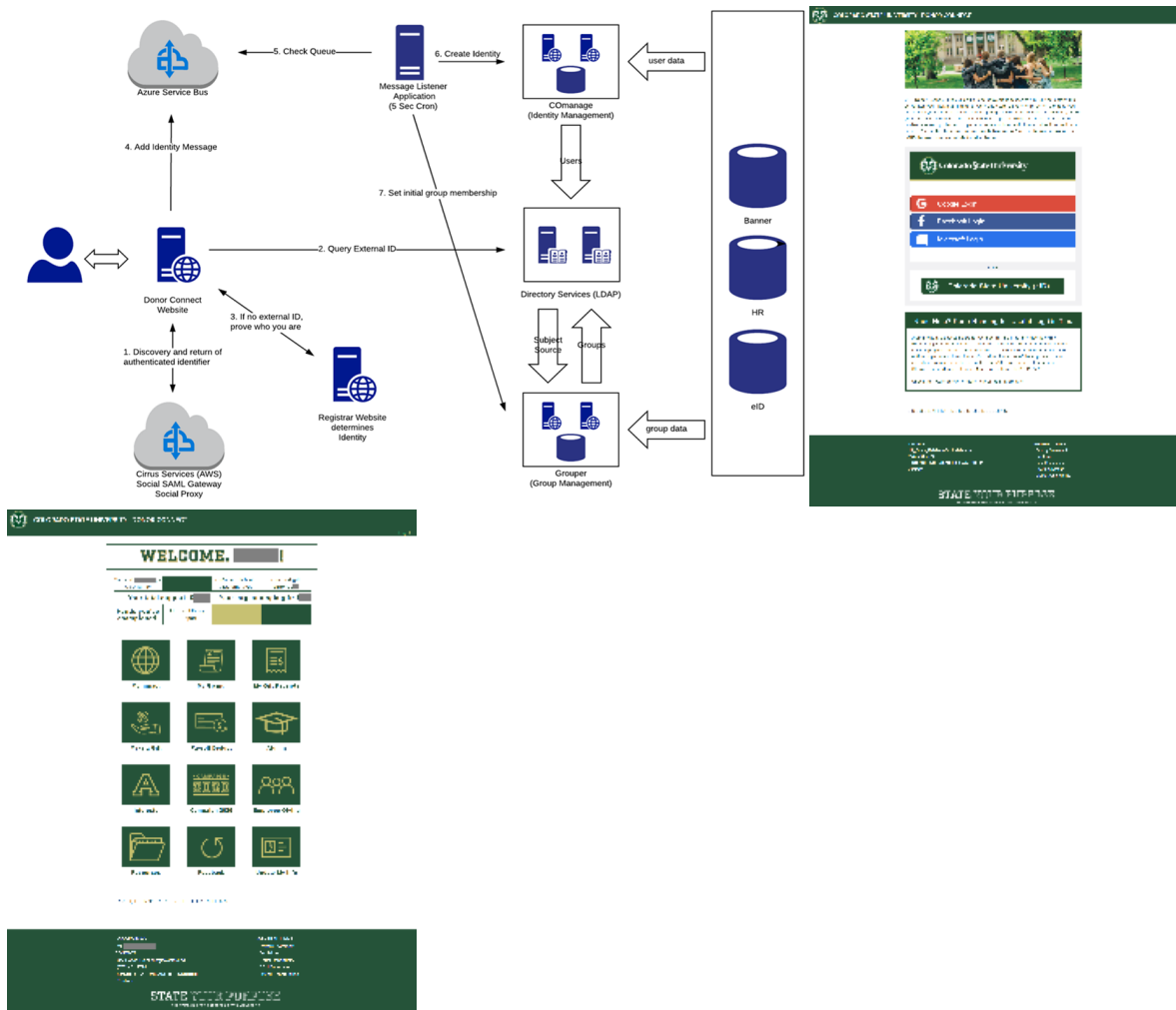
How-to-Add-an-...New-RAMweb.pdf

Activating-Your-F...er-Directions.pdf

Donors: Advancement Donor Connect

Provides donors with access to their accounts.

Donors can make donations, payroll deduction, view donation history/receipts, and get emails about areas of interest.

Vendors: **BFS**

Provides vendors who work with CSU with access to Business and Financial Services accounts.