

# UCLA Grouper Page

<a href="#">Wiki Home</a>	<a href="#">Deploying Grouper</a>	<a href="#">Grouper Guides</a>	<a href="#">Grouper Deployment Guide</a>	<a href="#">Community Contributions</a>	<a href="#">Internal Developer Resources</a>
---------------------------	-----------------------------------	--------------------------------	--	---	--

## UCLA Grouper Deployment

- [Overview](#)
- [IAMUCLA Deployment Use Cases](#)
- [Application-Specific Deployment Use cases](#)
- [Architecture and Design](#)
- [Presentations](#)

### Overview

UCLA's enterprise identity management program (IAMUCLA) deploys Grouper as a strategic component of its role and access management solution. Grouper is at the center of all group-like (role, access control list, service eligibility, distribution list) management activities on the IAMUCLA roadmap.

We are actively working with campus data stewards to identify/define institutional roles (types of students, types of employees, types of visitors/guests, etc.) in order to source and automate book-of-record group/role provisioning. As opportunities arise, we work with service providers to streamline and automate role-based access for existing and future applications.

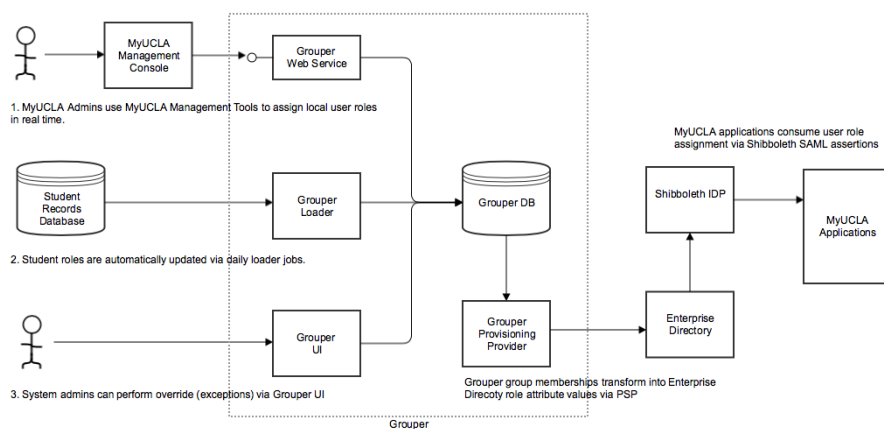
The sections below highlights several sample Grouper integration use cases at UCLA:

## IAMUCLA Deployment Use Cases

### Student Portal (MyUCLA) Role-Based Access

**Type:** Application Role-Based Access Control

**MyUCLA** is UCLA Student services portal. Rather a traditional portal where content is collected and delivered via widgets on a single platform, MyUCLA is made up of several distinct web applications. Each of these applications is managed by a different department at UCLA. MyUCLA produces a coherent user experience through coordinated design, development, and a set of back-end data sharing/exchange interfaces. In particular, all MyUCLA applications share a common set of Grouper-managed user roles and access memberships. Group membership is managed via a mix of book-of-record data feeds and direct updates via Grouper web service. The membership assignment in turn maps to role attribute values. All applications under the MyUCLA umbrella consume role attributes via Shibboleth to determine user access at run time.



### Campus ID Card / Door Access Management (BruinCard)

**Type:** ACL-Based Access Control

BruinCard is UCLA's employee and student photo ID card. It is a physical door access token, a debit card, and is used for meals and access to events on campus. When we replaced the BruinCard technology stack in 2015, we integrated BruinCard systems with Grouper. Grouper is now the engine behind most of BruinCard's group and role management needs. These include:

- Door access assignment - delegated function to let departmental door administrators manage door access in the departments
- Door administrator role assignment - manage who is a door administrator, and for which unit
- Photo API access - manages the ACL for BruinCard photo downloads

The diagram illustrates the BruinCard system architecture, showing the flow of data and control between various components. The system is divided into three main sections: External Applications, the Grouper Ecosystem (enclosed in a dashed box), and the BruinCard System.

**External Applications:**

- Department Door Administrators:** Use the **BruinCard BCDors Application** to assign departmental door access.
- Source Databases:** **Student Records**, **Payroll**, and **Housing** databases provide data to the **Grouper Loader**.
- System Admins:** Use the **Grouper UI** to manage access to BC Doors and the BruinCard Photos API.

**Grouper Ecosystem (Dashed Box):**

- The **BruinCard BCDors Application** connects to the **Grouper Web Service**.
- The **Grouper Web Service** interacts with the **Grouper DB** and the **Custom Provisioning Service Provider**.
- The **Grouper Loader** feeds data into the **Grouper DB**.
- The **Grouper UI** interacts with the **Grouper Web Service**.
- The **Custom Provisioning Service Provider** is a custom SQL PSP that provisions BruinCard related group memberships to the BruinCard System.

**BruinCard System:**

- Receives data and control from the **Custom Provisioning Service Provider**.
- Manages door access and controls data release via the **BruinCard Photos API**.

```

graph LR
    subgraph External
        Admin[1. Department Door Administrators] --> BCDors[BruinCard BCDors Application]
        DBs[(Student Records, Payroll, Housing)] --> Loader[Grouper Loader]
        Admin2[3. System admins] --> UI[Grouper UI]
    end

    subgraph Grouper_Ecosystem [Grouper]
        BCDors --> GWS[Grouper Web Service]
        GWS <--> GDB[(Grouper DB)]
        GWS <--> CUSP[Custom Provisioning Service Provider]
        Loader --> GDB
        UI --> GWS
    end

    CUSP --> BCSystem[BruinCard System]
    style BCSystem fill:none,stroke:none

```

## Faculty Information System (Opus)

Separate from the Enterprise IAM deployment, UCLA's [Faculty Information System Project \(Opus\)](#) has adopted Grouper as an application-specific, academic hierarchy driven, role-based access management solution.

Opus intends to operate a separate Grouper instance from the enterprise instance at its initial launch. Plans to migrate/converge with the enterprise instance is TBD.

## Architecture and Design

- [UCLA Group Naming Guide](#)
- [UCLA Grouper Folder Registry](#)

## Presentations