

UAccess Student – Overview and Access Request Workflow

Overview

UAccess Student requests are typically more complex than other Access Provisioning Tool (APT) requests, primarily due to the following:

- Wide Variety of Subject Areas and Roles
- Row Level Security Requirements
- Composite Roles
- Training Prerequisites

Wide Variety of Subject Areas and Roles

UAccess Student consists of a wide variety of subject areas including:

- Academic Advising
- Financial Aid
- Room and Course
- Admissions
- Financial Aid Composites (applies to Internal/Central Admin Units only)
- Student Financials
- Campus Community
- Graduate College
- Student Records
- Course and Fee Management
- Transfer credit

Within each Subject Area, there are numerous roles available that are designed to provide specific user functionality while protecting data and systems. Since each subject area contains roles which may be applicable to either Campus Community or Internal/Central Admin Users, they have been divided into following two Systems within APT to aid requestors in making the appropriate selections:

- UAccess Student – Campus Users
- UAccess Student – Internal/Central Admin Units

Access Request Workflow

The workflow used to manage UAccess Student requests includes additional steps needed for Quality Assurance of any [Row Level Security](#) requests as well as verification of training for those roles with training prerequisites. Department Approvers play a vital role in the UAccess Student workflow as they are the first person in the approval chain and are in the best position to determine the validity of requests. The workflow for UAccess Student requests is as follows:

1. **Subject User** needs access to UAccess Student.
2. The **Access Requestor** (typically the Subject User's supervisor) requests access on behalf of the Subject User.
3. The **Department Approver** (i.e., an Access Provisioning Liaison, Dean, Director, or Department Chair) reviews the request. The Department Approver may approve or deny the request at their discretion. If approved, the request moves forward in the workflow.



4. A UITS **Business Analyst (BA)** may review the Role and Row Level Security requested depending upon the System / Subject Area, performing a level of Quality Assurance on the request. The Row Level Security complexity makes this review necessary.
 - a. If the BA modifies the request, they will include comments describing the change made.
 - b. When the BA is satisfied with the requested data, they will approve / advance the request in the workflow.

5. The **Authorizing Agent** for the System / Subject Area will receive the request and may approve or deny it at their discretion. The Authorizing Agent may request additional information or may delegate the request to another Authorizing Agent.

6. After an Authorizing Agent has approved the Request, the **Security Administrator** will review the request. The Security Administrator may approve or deny the request at their discretion.

7. Access will provision by the Security Administrator upon verification that the Subject User has completed all prerequisites (typically training). If prerequisites are not completed within 42 days of the initial request, the request will automatically expire.