Access Provisioning Liaison Newsletter

What We’ve Been Up To

Several updates to the Access Provisioning Tool (APT) have been released in recent months:

- **Access Removals** can now be requested for all UAccess Systems by choosing the option UAccess Systems – Access Removals from the main system request page. See the article “How Do I Request Access Removal” on page 4.
- **UAccess Financials** has been added to the tool. See the article “Notes on UAccess Financials” on page 4 for additional information regarding UAccess Financials provisioning.
- **UAccess Student** has been added to the tool, replacing the previous email request process. See the article “UAccess Student Now Available for Request via APT” on page 2.
- **New Manager Self-Service roles** have been added to the tool, to support functionality that has been released for approving Personal Information Requests.
- **The main APT landing page** has been redesigned. Of particular note is a new link for Training and Documentation, which opens an Access Provisioning Documentation page in a new window. All of the documentation previously available on the APT site, as well new documentation in support of the new UAccess Student request process is available here.
- **Approval Authority (APL) dashboard** in UAccess Analytics will be cleaned up. We will be working in the coming months to clean up the data, remove “mistaken” delegations, and separate the history data from the current data.
UAccess Student Now Available for Request via APT!

As announced recently through the APL listserv, UAccess Student may now be requested via the APT. This replaces the email request process that has been used since the UAccess Student Implementation, and will allow requests for access for all UAccess systems to be made using a single tool. In addition, the configuration of UAccess Student Roles in the APT will remove manual processes, provide complete records of approvals, and improve the accuracy and timeliness of UAccess Student provisioning.

It’s important to note the business rules and prerequisites for gaining access to UAccess Student have not changed. UAccess Student requests will continue to require:

1. FERPA training
2. User agreement to the UAccess Acceptable Use Policy
3. APL approval
4. Data Steward or Authorizing Agent approval per Role/Access Level requested.
5. User Training per Role/Access Level where required.

One of the key differences in the provisioning process for UAccess Student compared to other UAccess systems is the likelihood that role(s) being requested require formal training (either online or instructor-led). In general, roles that allow update access to the system require training. Common examples are creating/approving Financial Aid External Awards, Course Scheduling, Enrollment, or updating Service Indicators. APLs and their delegates are encouraged to become familiar with the roles that require training and where to sign up. Check out our new UAccess Student - Campus Training Catalog, which maps Role Names to required training course and contact information. Keep in mind the following:

- Roles that require training are not granted until the training requirement is satisfied.
- APT requests have a life of 42 days. Please consider whether or not training requirements can be completed within that timeframe before submitting requests for access.

To assist you in becoming familiar with the roles, training prerequisites, and other terms associated with UAccess Student, several Access Provisioning Hands-On Labs were offered through UITS Workshops. The sessions were well-attended with great feedback and participation! If you were not able to attend, please contact us. With enough interest, we can schedule additional sessions now or later in the academic year. We’re also happy to visit you in your department.

Finally, documentation pertaining to the new UAccess Student request process is provided via our main UAccess Application Access Provisioning site under the Training and Documentation Links heading. Please review and let us know your feedback!
What is Row-Level Security?

Row-Level Security is a term used to describe a layer of security in addition to that provided by Roles within a software system or database. While Roles provide the User access to pages within UAccess Student or UAccess Employee, Row-Level Security provides the User access to specific rows of data for which he or she is authorized.

In UAccess Employee, access to data by Department (dept id) is controlled using Row-Level Security. Consider Manager Self-Service (MSS); MSS Users can only perform transactions for employees within the Department(s) for which they are authorized. On the other hand, in UAccess Student, Row-Level Security does not secure access to Department data, but rather data pertaining to certain actions or functions within a Subject area. Review these common examples:

- For Course Scheduling, the scheduling Roles provide access to the pages under Schedule of Classes, while Row-Level Security provides access to the specific (course) Subjects for which the User is authorized to schedule courses.
- For Financial Aid External Awards, the awarding Role provides access to the pages that allow the creation or approval of external awards, while Row-Level Security provides access to the accounts (or Item Types) for which the User is authorized to award.

Why is this important to understand? For many roles, the Row-Level Security required for a given User is unique, and EAST must collect this information from you at the time of request, so that it can be approved along with the Roles. Where Row-Level Security is necessary for a given Role, the APT has been configured to request this information from you.

In UAccess Student, it is also common for Users to have a need to request additional Row-Level Security corresponding to a Role he or she already has. In these scenarios, it is not necessary to request the Role again. Instead, a Row-Level Security Only option is available within each relevant UAccess Student Subject in APT. Use this option to request just the additional Row-Level Security needed for Users who already have access to perform the applicable transaction(s).
Notes on UAccess Financials

Since the UAccess Financials go-live in early October, EAST has received many inquiries regarding UAccess Financials access provisioning. Please note the following:

- The **Financial Systems User** role available for request in the APT is the same as what has been referred to as Role 54. It provides access for users to serve as Fiscal Officers/Delegates, create salary transfers, manage capital assets, chart of accounts and workflow.
- The Financial Systems User role (Role 54) is the only UAccess Financials role provisioned by EAST. Permissions for Groups or workflow routings are managed within the department, and EAST has no authority to facilitate these types of requests.
- However, permissions for Groups often carry the prerequisite that the user has Role 54. Use the UAccess Analytics > Financials > General – Security dashboard to check whether or not a user has Role 54.
- For UAccess Analytics, there is just one level of Financials access at this time, and it has been categorized under Base Analytics access.
- Additional resources:
  - Mosaic UAccess Financials Go Live Information and Updates
  - Your College/Department’s UAccess Financials Super User

How Do I Request Access Removal?

Access Removal can now be requested via the APT by selecting a new request option on the main system selection page: UAccess Systems – Access Removals. By selecting this option, the APT screens that follow allow you to request Access Removal in these scenarios:

- Terminations
- Transfers
- Job Duty Changes

To accommodate all of these scenarios, the Access Removal option allows you to select access removal for all UAccess systems, for a single UAccess system, by individual Role, as well as for Department-specific Row-Level Security. Please contact us if you are unsure of the option which best fits your individual need.

The workflow routing and notifications for Access Removals are slightly different than that of Access Requests:

- Only the approval of the APL is required.
- Only the Requestor is notified when the request is complete. No notification is sent to the Employee.

Finally, the Access Removal system no longer checks for the employee’s active status or completion of the UAccess Acceptable Use Policy.