New Access Provisioning Tool (APT) Coming Very, Very Soon!

We have previously written about a new APT Request User Interface. The time has come to again bring this to your attention, as we enter the testing and implementation planning phase of development. EAST is actively testing the new solution, exercising the user interface features. We anticipate completion of development before Closure, with some testing lingering in the first few weeks of 2014. The APL Advisory Group, who contributed to the design, will have an opportunity to exercise the training materials and new user interface prior to rollout, providing initial feedback. General training and rollout will begin late in January.

Some of the new features you can look forward to:

- Ability to create a single request per user, addressing multiple systems and subject areas
- Ability to start a request and finish later
- Ability to select the APL from a list
- Comprehensive display of prerequisite training information (e.g. FERPA, UAccess Agreement, Elevated Privileges)
- Ability to scroll through Role Descriptions for all systems directly in the APT Request User Interface, while keeping the request open

This is a very exciting release; making use of PeopleSoft lays the groundwork for future improvements to the overall request and provisioning process.

Please look for January communications regarding training. We thank you for your participation in the process, as we move forward with this rollout.
Updates to APT and Security Dashboards

In recent months, minor improvements were made to the APT, through your suggestions:

- **In the Approve and Monitor application, searches for tickets by NetID are now possible.** Searches by NetID will return tickets where the NetID matches the Requestor, Subject, or Department Approver. Searches by Name are still possible as well. For additional instructions and tips for searching tickets, please see the document 'General Steps to Search For and Monitor Requests' on the Access Provisioning Documentation site.

- **UAccess Analytics > Security > All Roles (as well as Person Roles, My UAccess Roles) now includes security information for UAccess Student – Reporting environment.**

- **A new Role Details dashboard is available** by clicking the Technical Role Name on UAccess Analytics > Security > All Roles. The Role Details dashboard provides a Role Description, training requirements, and APT request selections. See the 'Quick Reference – Using the All Roles Dashboard' on the Access Provisioning Documentation site.

ISO-P702M Compliance Work

The ISO-P702M is a University procedure for Enterprise Applications Account Access, which defines the steps to authorize, monitor, and control access to UAccess systems, and as such, drives many of EAST’s tasks and projects. (Read this procedure and related policies here.)

Since the inception of the Access Provisioning Liaison (APL) program, we have completed various 702M-driven assignments, such as reviewing UAccess Student users and roles granted during implementation, and implementing Elevated Privilege Training as a repeatable operation. But there are assignments on which we as an institution have not yet focused. One of these open assignments was mentioned in the 2013 Financial Audit: the comprehensive review of access at least one time every three years.

Compliance with the 702M is an institutional responsibility. EAST can facilitate compliance by providing reporting and working with Data Stewards and APLs to collect the necessary documentation needed for compliance verification, but success will rely on collaboration and our collective participation.

EAST will create a process to facilitate the review; Data Stewards will be asked to review the scope of access and permissions allowed through each Role. APLs will be asked to review individuals assigned that Role, confirming an ongoing business need for the Role. Data Stewards will provide a final sign-off approval, after APLs have reconfirmed a User’s need for a given Role. All Roles must be reviewed. We will begin with UAccess Employee Roles.

Please look for more on this topic in Q1 of the coming calendar year.

MSS I-9 Implementation

As many of you know, the paper I-9 form is being converted to an MSS online form by Systems Control. This functionality is planned to go-live in January 2014.

The release of this functionality will necessitate the provisioning of new roles for HR Department Approver and College Reviewer/Approver for I-9 transactions. Just like previous MSS releases, Systems Control is working with departments as we speak to identify I-9 Approvers per department/college, and Systems Control will in turn provide this information to EAST for provisioning.

This pre-provisioning process will include a new requirement, however: completion of Elevated Privileges training. Because the I-9 form includes sensitive data, these roles will be considered Elevated Privileges. As such, Systems Control will be sharing this training requirement with department representatives as the user lists are gathered. You can help by ensuring the users identified to have I-9 Approver roles have completed Elevated Privileges training in the past year. Refer to the UAccess Analytics > Security > Prereqs dashboard, making note of the ‘Priv. Agree.’ column.
APL Advisory Group and EAST Collaborations

Ever wonder about who EAST works with, and how we get feedback? EAST receives comments from the campus community, in addition to those we receive from you, and your colleagues – other APLs. We also interact regularly with a smaller group of APLs, stemming from early meetings with the Council of Academic Business Officers (CABO). These individuals, whom we now refer to as the “APL Advisory Group,” were instrumental in identifying the need for the APL program, and the need to have representation from all of campus with regard to Access and Provisioning. We also regularly include the Workshop and Training Team (WaTT) and of course, the Data Stewards, inviting them to participate in discussions and to complete required work. For instance, the APL Advisory Group was instrumental in the rollout plan for Elevated Privilege Training (we just finished our second annual big push – again very successful thanks to all of your support). And similarly, we have been relying on this group for input on the new APT Request User Interface, from a requirements perspective, prioritization of features, and the overall design of the user interface. For Role related concerns, we also interact with the UITS Business Analysts for UAccess systems who work directly with administrative business units.

EAST relies on these resources to vet ideas and receive early feedback on issues or challenges we face. We appreciate working with these groups, and their willingness to help shape our services. If you would like more information about our interaction with these groups, please contact me using the contact information listed below.

Laurel Wadlund
Assistant Director, Production Integrity
ITIL® Foundation Certified
520-626-9949, UITS 306
wadlund@email.arizona.edu

Q and A with EAST

APL Question: How do I request access for Instructor Center?

EAST Answer: Access to Instructor Center – which provides access for Instructors to class rosters and to post grades – is automatically granted for Instructors who are assigned to a course according to UAccess Student. (This is a similar concept to the automatic provisioning of the Employee Self Service role for employees in UAccess Employee.) There is no need to request Instructor access through APT. Instead, confirm the instructor has been assigned to the course(s) for which he or she is teaching with your department’s course scheduler. Then, advise the Instructor to sign in to Instructor Center via http://uaccess.arizona.edu/. Instructor Center access will be granted behind the scenes, and an email will be sent to the Instructor that provides more information on the use of Instructor Center.
Going On Vacation?

How to delegate your approval tasks

With the holidays and Winter Closure upon us, please take a moment to consider if you will need to delegate your access request/approval tasks to another APL, Dean, or Department Head. A vacation ‘rule’ can be created in the UAccess Access Provisioning Tool by following these instructions:

1) Access the [UAccess Access Provisioning Tool](https://request.uaccess.arizona.edu), and click Approve and Monitor Requests.
2) From the Approval dashboards, on the far upper right, click the link for Preferences.
3) On the Vacation page, set the dates of your vacation and Save.
4) Click Create to begin creating your vacation rule.
5) Give the rule a name; this can be whatever is meaningful for you.
6) Leave the default checkbox ‘Rule should only apply from [your vacation] dates’ checked, and click Create.
7) Do not add a Condition. Instead, skip down to ‘Task the following action:’ and select the Delegate to option.
8) Specify your Delegate by NetID. If you do not know your Delegate’s NetID, use the flashlight icon to look it up.
9) Save your updates.

If possible, we recommend setting up your vacation rule a day or two prior to leaving the office, so you can verify with your Delegate that it is working as you both expect. Keep in mind you will continue to be notified of and have the ability to approve requests routed to you during the dates you have set for your vacation rule.

APL Roles and Responsibilities

Because new APLs are delegated on a continuing basis, this space will be reserved for Liaison Roles and Responsibilities.

**Liaison Roles**

- Act as a Primary Contact for the college/business unit for Access related work and issues with regard to Access Provisioning/Access Reviews/Changes/Removals/Related Activity
- Become the college/department local subject matter expert in the area of Access Provisioning
- Understand, communicate and champion security concerns as they relate to the end user and the access they have been privileged to receive

**Liaison Responsibilities**

- Act as the Primary Contact for receiving, reviewing, distributing and collecting necessary information relating to access
- Participate in the work flow for overseeing/approving/requesting access or access removals
- Monitor Department User training needs as they relate to Access Provisioning
- Monitor and insure department users who have elevated privileges complete necessary annual security training and acknowledgements and/or agreements
- Review and disseminate Access Provisioning Communications to appropriate college/department personnel and users