IAM Project Overview

&

Milestones

TABLE OF CONTENTS

IAM Project Success Factors:

1. Establish one University credential (ID and Password) for the average end-user
2. Require single sign-on for all Campus and UA web accessible technology
    - Reduce the number of times a credential request is presented to a user during a routine session
3. Provide the self-service functionality to allow University and external colleagues to request and revoke access to University and external resources
4. Protect the privacy of the members of the University community
    - Allow individuals some dimension of control over their personal information
    - Provide complete transparency over the University's use of one's personal information in accordance with federal, state, and University guidelines and laws
5. Understand and manage the risk to the University data environment
    - Raise our confidence in establishing and managing a person's identity and the rigor of one's credentials
    - Reduce the number of entry points for University systems
6. Establish stronger and longer relationships with members of the University community
    - Retain an end-user identity for life
7. Provide a central authentication system to support applications across a variety of platforms and scope including mobile, departmental, and central supported.
    - Asking ourselves--How much work will it be for departmental staff to use the new central authentication system? -- Objective has been accomplished on December 8, 2012

Project Scope:

In Scope

1. Courion core product installation and integration with authoritative systems (e.g. Banner, iCard)
    a. Document criteria used for defining authoritative systems
2. Password management including a central password service (central password policy) and password synchronization across the main password stores at the University of Illinois:
    - Enterprise LDAP (EAS)
    - UIS AD
    - UIC AD
    - UIC OpenLDAP
    - UIC PhoneBook
    - UofI AD
    - ICS/Novell Directory
    - Chicago Medical Center AD
3. Design a process for managing Non-system affiliates. This will include:
    a. The management of identities that are not in an authoritative system, such as guest accounts, Intensive English Institute (IEI), Osher Lifelong Learning Institute (OLLI) Scholars, etc.

    b. A streamlined repository for storing all identities at the University of Illinois
    c. Create a process for:
        i. associating identities with specific affiliation types

        ii. requesting the addition of new identity types

        iii. easily requesting access for non-system affiliates

        iv. automated provisioning identities similar to authoritative system affiliated identities
4. Replace existing Identity Provisioning/De-Provisioning processes that includes:
    a. Identity creation and registration
    b. Common account name creation and access provisioning/de-provisioning
    c. ID claiming process
    d. Profile registration
5. Provisioning to University and Campus-wide systems such as:
        - University directories (i.e. EAS, UofI AD, UIC AD, UIC Open LDAP, UIC Phonebook, UIS AD, and Urbana ICS)
        - Additional service provisioning to be included for Email/Exchange, Lync, and Banner.
        - Identity change processes including changes to Identity affiliation and attributes. This includes changes such as roles, departments, identity information, etc.
6. Access auditing and compliance control - automated compliance processes for use in the review of current user access and the ability to revoke access no longer required.
7. Role mining and role management workflows - automated enterprise role development processes for use with access fulfillment, and maintenance of enterprise roles defining user access levels for access fulfillment and access certification.
8. Deploy a modernized process for authentication (logon) and managing access to the University systems. This process will include:
    a. Deploying a University-wide authentication infrastructure based on SiteMinder
    b. Implementing a process for requesting and adding new applications to the new authentication system
    c. Deploying a single web page where all users are authenticated to use University systems
    d. Implementing a process for managing Federation with the University, to be integrated with SiteMinder as the identity provider. The federation implementation will comply with NIST and InCommon.
    e. Providing the needed training to both system admins and end users to help improve the adoption rate of the new systems
9. The provisioning and de-provisioning of Primary Accounts are in-scope
10. Implementing Integrated Windows Authentication (IWA) for supported hardware or applications where applicable and allowed by policy

Out of Scope

1. Integration with systems other than those listed as in scope for provisioning and de-provisioning of identities

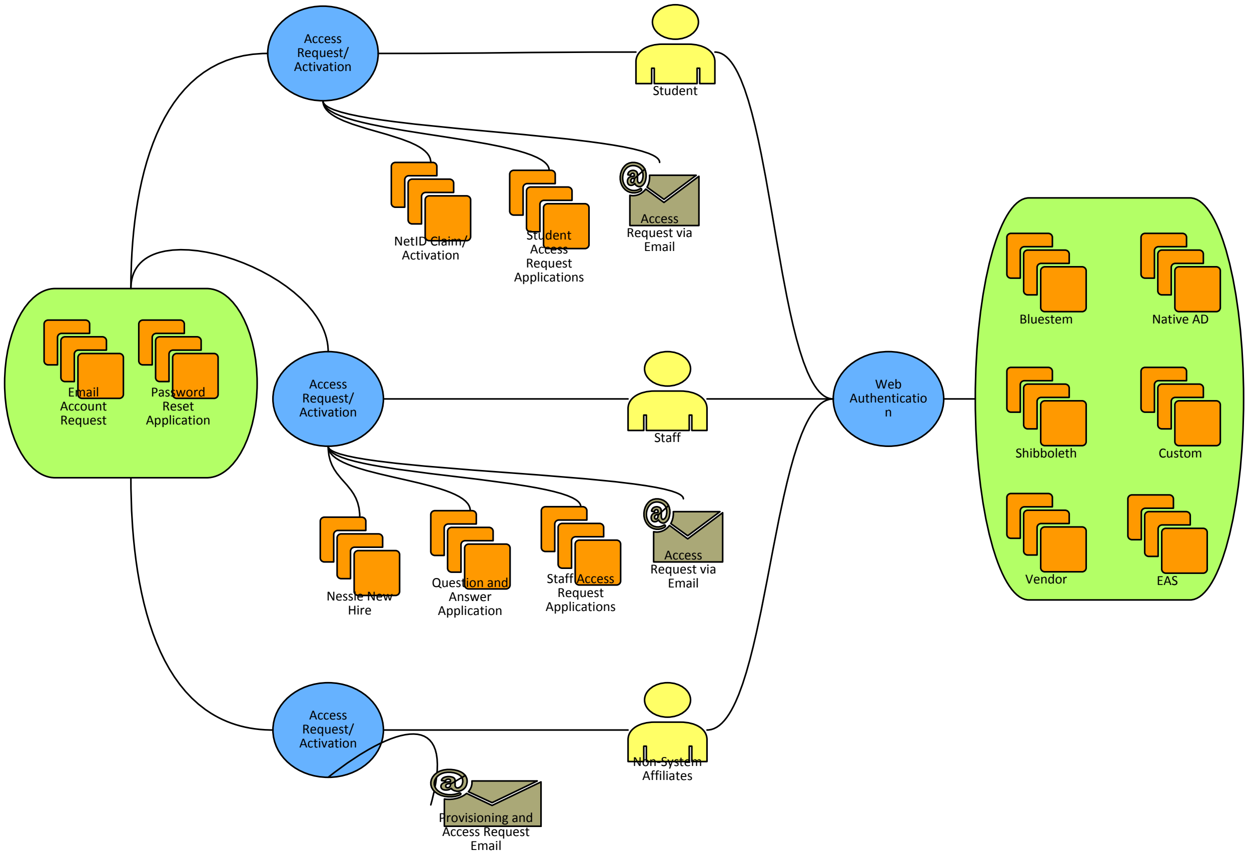
2. The provisioning and de-provisioning of administrative/service accounts
3. Changing the format of the University ID Number (UIN). This is a numeric number and cannot be changed to alphanumeric due to its tie to bank routing numbers and their requirement that they be numeric.
4. The decommissioning of University systems whose functionality will be replaced. Such systems may include:
    a. Decommissioning Enterprise (EAS) LDAP
    b. Decommissioning Bluestem
    c. Decommissioning EAS
    d. Decommissioning Tivoli, Chicago PhoneBook and Springfield's scripts for creating identities

Although these projects are out of scope of the actual IAM project, they are the responsibility of the campus IT departments. The decommissioning of these technologies is important for rationalization of future IAM processes and to realize the documented cost savings. The IAM project will make it possible to decommission these systems.

5. Implementing Integrated Windows Authentication (IWA) for non-supported hardware or applications

IAM Now vs. Future

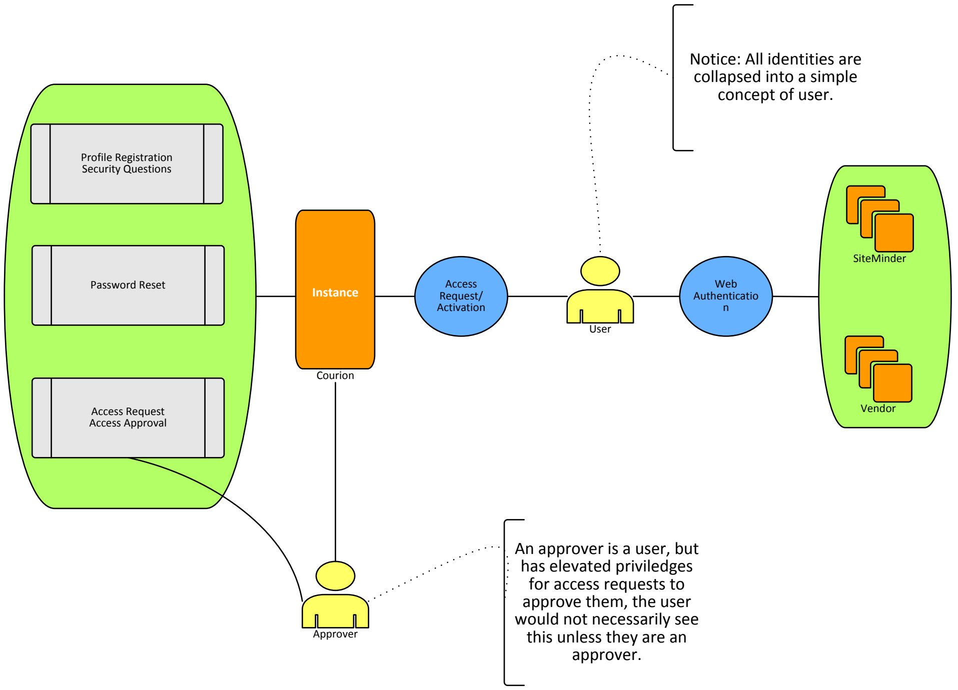
IAM Now


Access Request/ Activation
Student
NetID Claim/ Activation
Student Access Request Applications
Access Request via Email
Email Account Request
Password Reset Application
Access Request/ Activation
Staff
Nessie New Hire
Question and Answer Application
Staff Access Request Applications
Access Request via Email
Access Request/ Activation
Non-System Affiliates
Provisioning and Access Request Email
Web Authentication
Bluestem
Native AD
Shibboleth
Custom
Vendor
EAS

The picture describes the current state of IAM at the University of Illinois. This includes:

- Identity generation process and provisioning, which happens separately at each campus. This process causes the following issues:
  - Duplication of identities: Users may exist in multiple authoritative user stores in each campus and UA
  - Different credentials: When users have multiple identities, their user ids and passwords are different. In other words, users are forced to remember multiple user IDs and passwords to logon to the various applications. Some effort has been made in the past to synchronize the user ids between the campuses and UA.
  - User ID conflict: Some user accounts get assigned to two or more people. In other words, a Chicago person may own the same NetID as an Urbana person.
  - Difficult to collaborate: Users find it difficult to collaborate and assign access between the campuses and external entities. It is not easy for Chicago faculty to share access with Urbana faculty in SharePoint. IT normally has to get involved with these requests.
  - Non-System Affiliation problems: There is no simple process for requesting access for guests, visitors, contractors, students of special programs such OLLI and ESL students, etc.
  - Bad Business process: To grant access to non-System affiliates, the University uses a process by which people are created as 0% employees with 0% appointments, which is a violation of HR practices.
  - Identity and user access is terminated when users leave the University.
- User Activation and Access process is distributed and different from campus to campus. Sometime this process is also different from Department to department in a single campus. This causes the following issues:
  - End User Confusion: The identity claiming process, where the users need to go to get their ID activated, is difficult and confusing for the end users.
  - Inconsistent Processes: Users who are both Chicago and Urbana students (or employees) are asked to provide different information to claim their identities.
  - Password Resets: Passwords resets are managed differently from Campus to Campus. The password rules are not the same, which has created security exposures in the past. In addition, the password management is the mostly costly service expense at the three campuses and UA.
- System Logon:
  - Multiple logons: Users still get prompted to logon multiple times when they go from one application to another. There is not University Wide Single Sign-On.
  - Logon is distributed: There is no one place where University users are asked to logon to web applications. Not only is this practice confusing, it also makes it easier to hack user credentials

IAM in the Future:



Notice: All identities are collapsed into a simple concept of user.

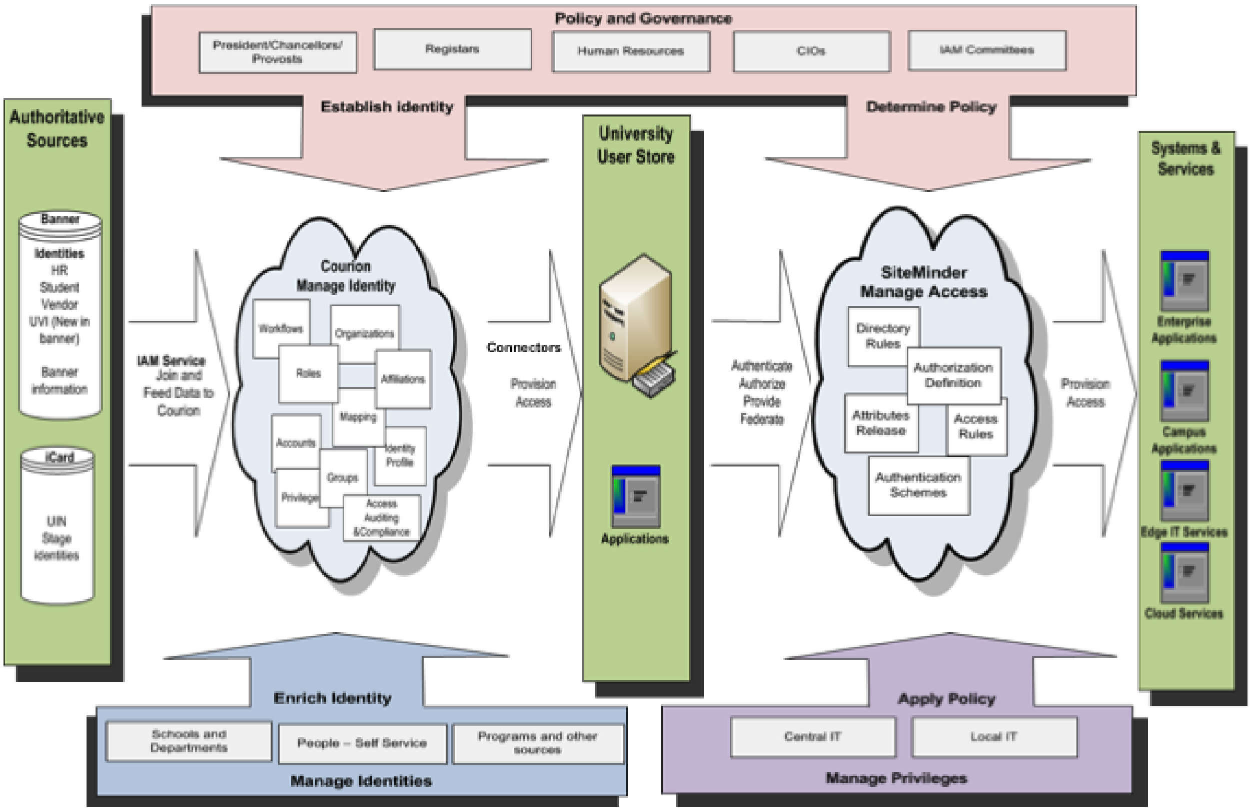
An approver is a user, but has elevated priviledges for access requests to approve them, the user would not necessarily see this unless they are an approver.

The future IAM project will provide the following changes:

- Identity generation process and provisioning will be streamlined and made easier. Users will be created automatically in the IAM system based on business events such as student admission process, HR hiring process, vendor relationship, etc. This means:
    - Users can access and claim their identities much sooner and faster
    - No duplication of identities. Each person will only have on authoritative record in the IAM system.
    - Users will not need to remember more than one user id and password. The same account can be used to access any university resources. Urbana employees can use their one user id/password to access Springfield, Chicago and UA systems if they have the appropriate permissions.
    - User ID conflicts will be significantly reduced or eliminated
    - The new system will provide facility to easily request access for guests, lecturers, distinguished scholars, etc.
    - The new infrastructure will make it easier for users to request and manage access for collaborative systems.
    - This project will allow for the retirement of bad business practices for managing user access
    - User identities and some access will be retained at the University for life.
- User Activation and Access process is streamlined across the entire University.
    - The user activation will be easier for end users. They do it once and they get access to all their accounts.

  - The IAM project will provide a more streamlined and consistent self-service password management process, which is projected to be significantly made easier for users to change their password.
- System Logon:
  - The deployment of SiteMinder will allow a user from Urbana to logon once at the central University logon service and access any resources in Chicago and Springfield without being prompted to logon again.
  - SiteMinder will make it easier for system admins and application developers to integrate with the University logon service. By simplifying the process, the hope is that the adoption rate is high, which will make the Single Sign-On more successful.

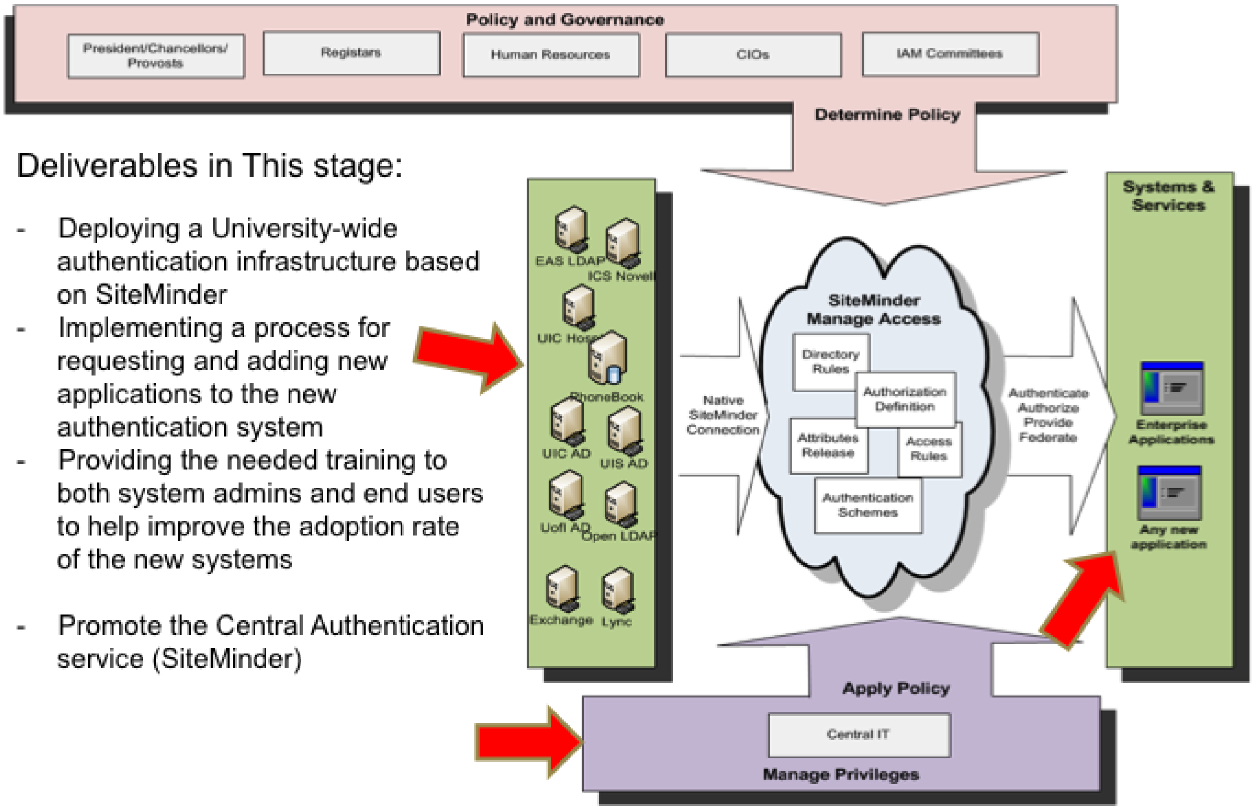
IAM Project End State:



Access Management:

Authentication:

This stage is complete and SiteMinder is currently in Production. This environment is available for all University admins and application developers. Although, campus IT will be coordinating the transition of applications from Bluestem to SiteMinder, interested parties can choose to transition to SiteMinder as they are ready. A more detailed description of SiteMinder integration at the University is as follows:



Deliverables in This stage:

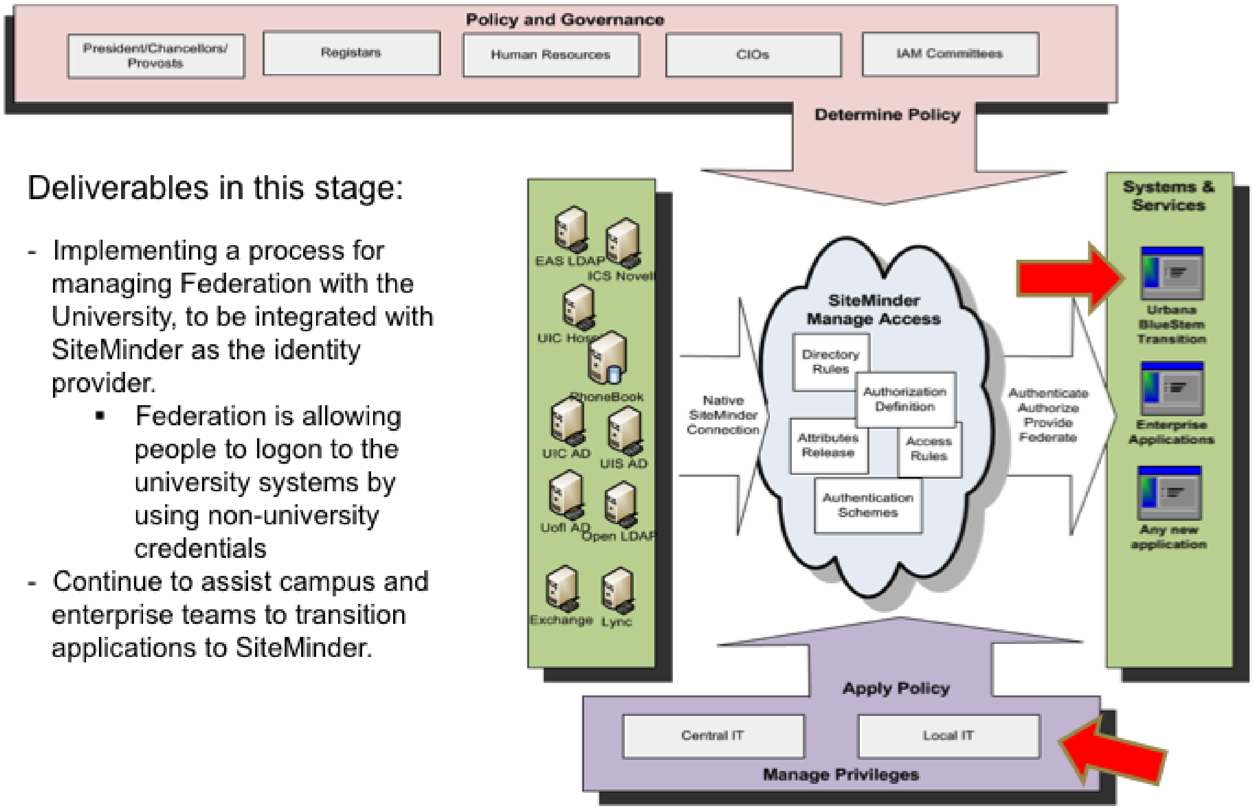
- Deploying a University-wide authentication infrastructure based on SiteMinder
- Implementing a process for requesting and adding new applications to the new authentication system
- Providing the needed training to both system admins and end users to help improve the adoption rate of the new systems
- Promote the Central Authentication service (SiteMinder)

Impact:

- End User:
  - End user impact is minimal at this stage. As applications move to SiteMinder, users may see slightly different EAS and Bluestem login pages.
  - Users will continue to use their current user id and passwords for accessing the campus and the enterprise applications
- Campus and central IT:
  - Central IT can begin to move applications to SiteMinder as soon as possible by following the process outlined on the IAM website.
  - Central IT can begin the plans for decommissioning legacy authentication systems such as EAS and Bluestem.
  - Address issues related to legacy EAS and Bluestem issues such as PWF file, doc.cgi, etc.
- Local IT:

        - Local IT can begin to move applications to SiteMinder as soon as possible by following the process outlined on the IAM website.
- Business offices Impact:
    - As applications move to SiteMinder, application owners may be contacted to test and/or sign off on the transition of applications to SiteMinder.
    - Some applications such as Nessie and the campus portal may need more coordination to transition to SiteMinder.

SiteMinder Federation and Agent Installations:



Deliverables in this stage:

- Implementing a process for managing Federation with the University, to be integrated with SiteMinder as the identity provider.
    - Federation is allowing people to logon to the university systems by using non-university credentials
- Continue to assist campus and enterprise teams to transition applications to SiteMinder.

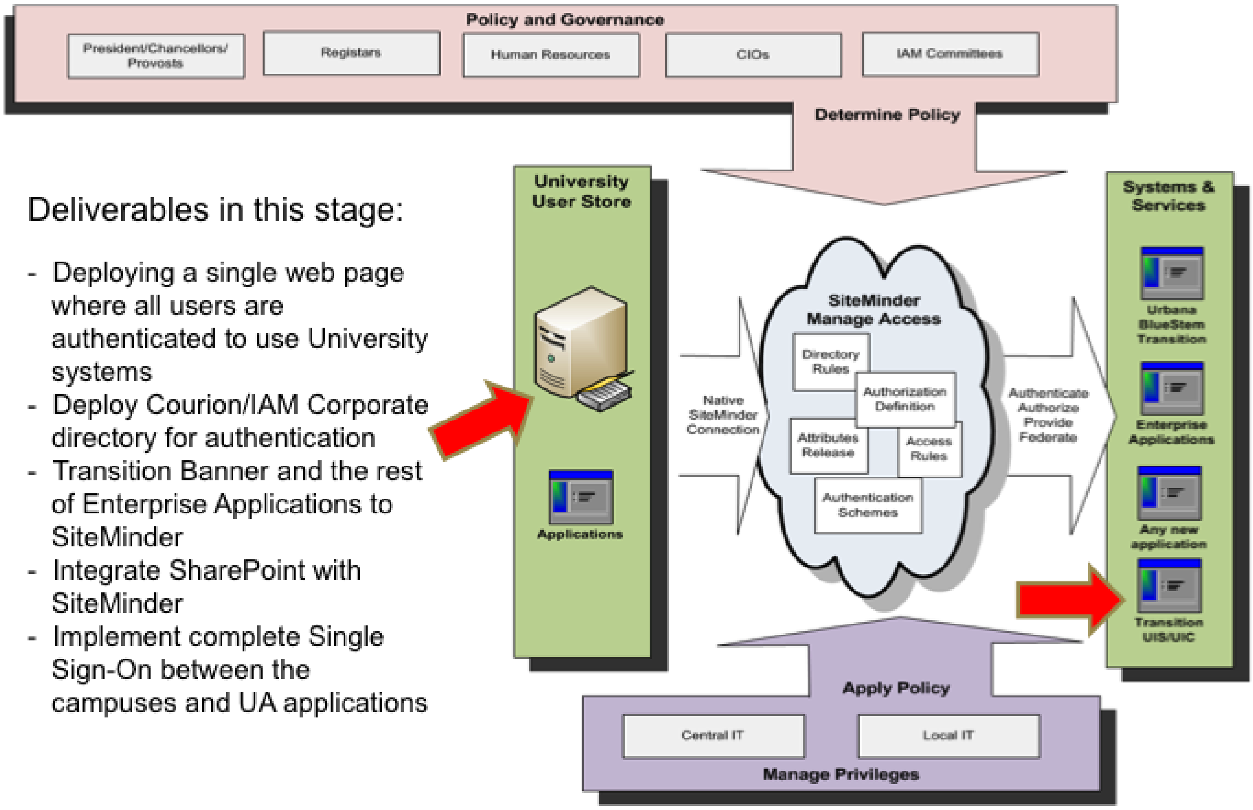
Impact:

- End User:
    - Same impact as the SiteMinder Stage1
- Campus and central IT:
    - Shibboleth instances will be changed to allow the for the SiteMinder authentication
    - Applications that require federation services can start using SiteMinder authentication processes. If the applications are already using Shibboleth, the Shibboleth Application will continue. Users of such applications will be automatically directed back to SiteMinder for authentication.
- Local IT:

    - Applications that require federation services can start using SiteMinder authentication processes. If the applications are already using Shibboleth, the Shibboleth Application will continue. Users of such applications will be automatically directed back to SiteMinder for authentication.

- Business offices Impact
    - As applications move to SiteMinder, application owners may be contacted to test and/or sign off on the transition of applications to SiteMinder.

SiteMinder Integrations and Single Login Page:



Deliverables in this stage:

- Deploying a single web page where all users are authenticated to use University systems
- Deploy Courion/IAM Corporate directory for authentication
- Transition Banner and the rest of Enterprise Applications to SiteMinder
- Integrate SharePoint with SiteMinder
- Implement complete Single Sign-On between the campuses and UA applications

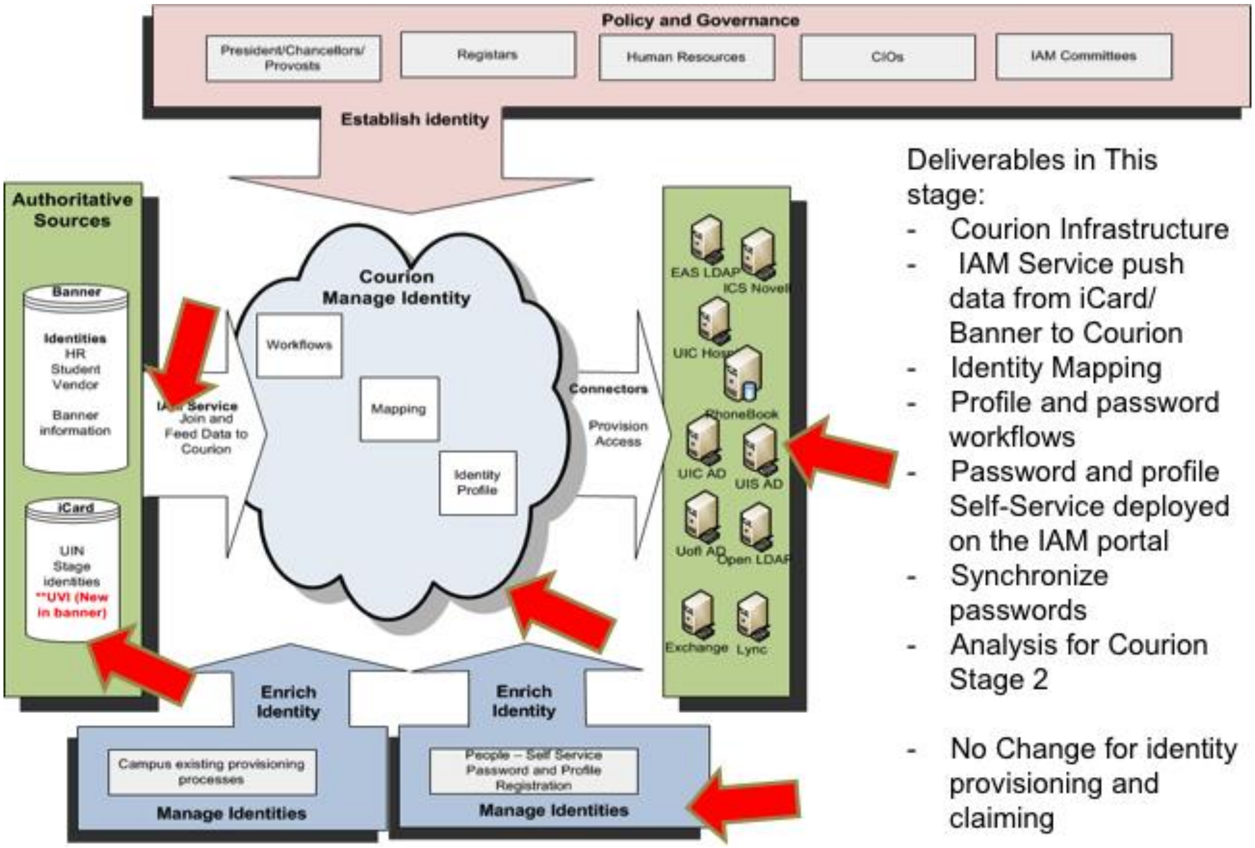
Impact:

- End User
    - Users will start using a new page that is designed to replace all central login pages
    - This page will include a user prompt, real estate for login instructions and password management, new area for communicating important University information and update branding.
- Campus and central IT
    - Continue to help local admins with the transitioning applications to SiteMinder
    - Help with the transition to the central Courion authentication directory
    - Retire legacy logon systems

- Local IT
    - Continue to transition applications to SiteMinder
- Business offices Impact
    - As applications move to SiteMinder, application owners may be contacted to test and/or sign off on the transition of applications to SiteMinder.

Identity Provisioning and Administration:

Profile Registration and Password Management:



Deliverables in This stage:

- Courion Infrastructure
- IAM Service push data from iCard/ Banner to Courion
- Identity Mapping
- Profile and password workflows
- Password and profile Self-Service deployed on the IAM portal
- Synchronize passwords
- Analysis for Courion Stage 2

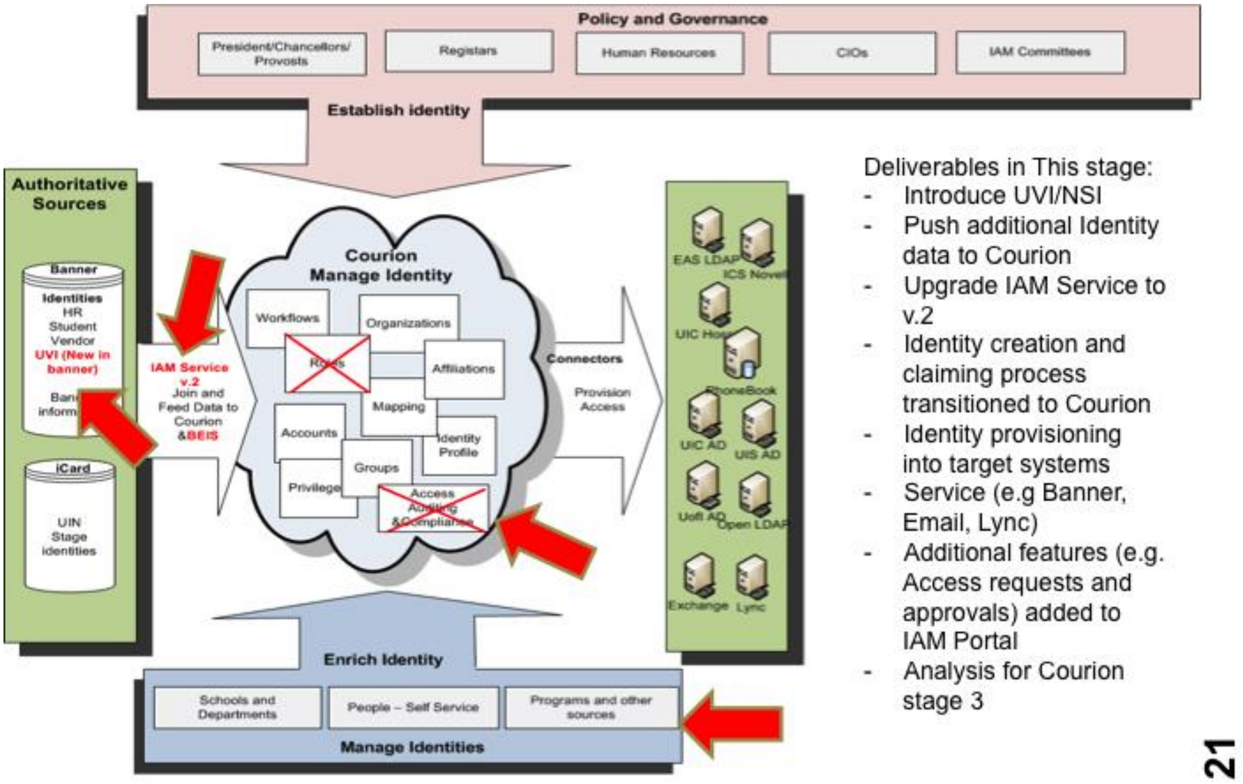
- No Change for identity provisioning and claiming

Impact:

- End User:
    - Users will be asked to logon to the new IAM Portal to Register their profile and change their passwords.
    - Users will be asked to create and answer security questions for password management purposes. They will also be asked to provide a non-university email address as well as cell phone number that can be used to recover passwords in the future.

  - New Chicago users will be directed to Courion to claim their user accounts
- Campus and central IT:
  - Urbana-CITES, Chicago-ACCC, Springfield-ITS and UA-AITS are all expected to change their current user id claiming process to introduce the Courion profile registration and password change function
  - The IAM team will be deploying a new user id claiming process for Chicago.
  - Change the current password pages to redirect users to Courion for password management
  - Identify and determine, which systems should be retired at this stage (e.g. MIT Kerberos, Bluestem, Chicago current ID claiming process)
- Local IT:
  - As the trusted IT personnel at the local department, the role of local IT will be critical in communicating the new password and profile registration features. This will reduce confusion and assure people that they are not being hacked.
- Business offices Impact
  - Since the new profile registration and password interface is going to change across the University, business documentation and web sites will need to be updated to reflect the new changes. For instance if the admission office publish information about user accounts and password management, this type of documents will need to change. Additionally, the different process for claiming NetID/EID can be changed.

Identity Provisioning/De-Provisioning:



Deliverables in This stage:
- Introduce UVI/NSI
- Push additional Identity data to Courion
- Upgrade IAM Service to v.2
- Identity creation and claiming process transitioned to Courion
- Identity provisioning into target systems
- Service (e.g Banner, Email, Lync)
- Additional features (e.g. Access requests and approvals) added to IAM Portal
- Analysis for Courion stage 3

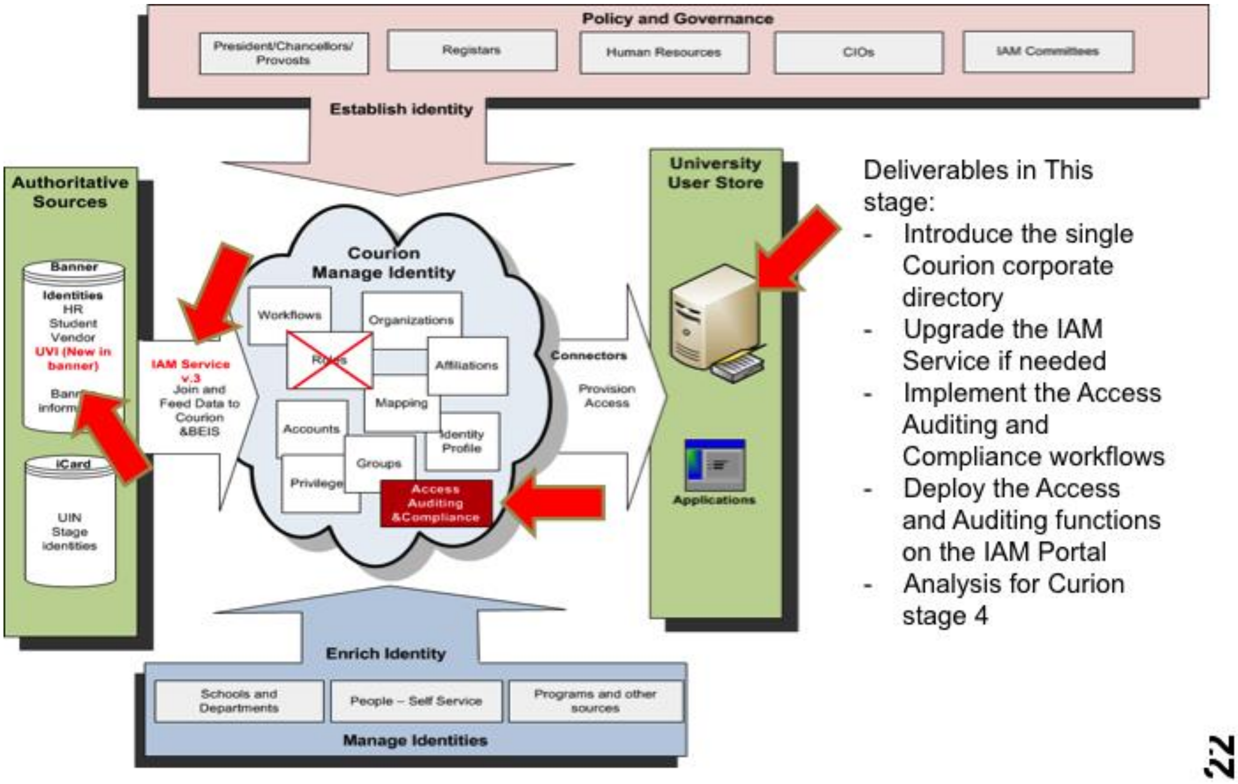
Impact:

- End User:
  - Users will be notified with the new changes and trained in the following:
    - New Id claiming process
    - New IAM portal for requesting, changing, removing and approving access
    - New process for managing non-System affiliates

- Campus and central IT:
  - Switch off access for the current campus user id claiming applications in order to deploy the new system
  - Configure Courion to provision existing user stores (AD and LDAP servers). Courion will be used to create new user IDs and password, email accounts, Banner access, and Lync
- Local IT:
  - Local admins will begin to use Courion for creating non-system affiliates, provisioning and de-provisioning user access.
- Business offices Impact
  - Since user creation, claiming and provisioning processes are being completely replaced, business documentation and web sites will need to be updated to reflect the new changes.

  - University Security Contacts (USCs) will be trained to request and approve access for users in their departments
  - University Security Contacts (USCs) will be trained create and manage non-system affiliates.

Access, Auditing and Compliance Control:



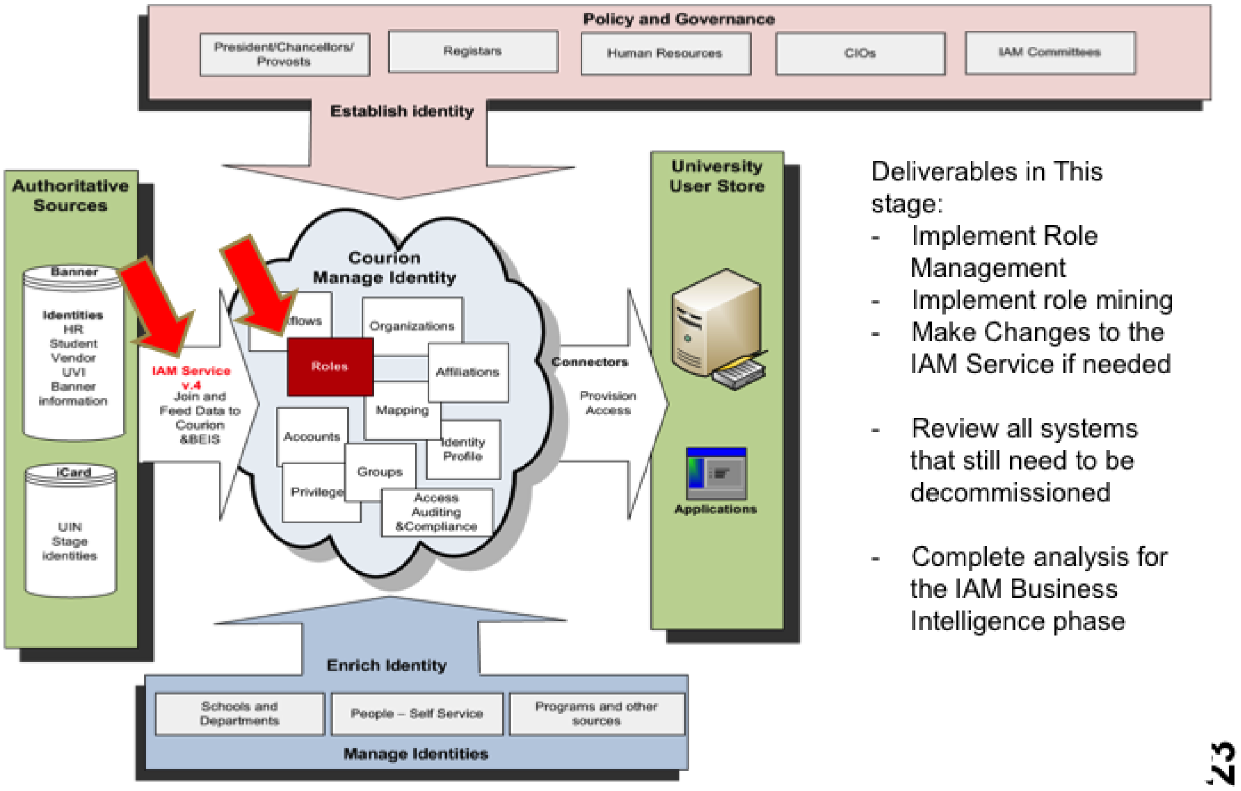
Deliverables in This stage:

- Introduce the single Courion corporate directory
- Upgrade the IAM Service if needed
- Implement the Access Auditing and Compliance workflows
- Deploy the Access and Auditing functions on the IAM Portal
- Analysis for Curion stage 4

Impact:

- End User:
  - As the user access auditing process is updated and automated as part of this stage, users might be contacted for changes related to their current access
- Campus and central IT:
  - IT Personnel will be trained to review and remediate users accesses
  - Implement changes to address security concerns in the campus directory servers
- Local IT:
  - IT Personnel will be trained to review and help remediate user access for users in their departments.
- Business offices Impact
  - University Security Contacts will be trained to use the new software to review and remediate access for users in their departments

Role Mining and Role Management:



Deliverables in This stage:

- Implement Role Management
- Implement role mining
- Make Changes to the IAM Service if needed
- Review all systems that still need to be decommissioned
- Complete analysis for the IAM Business Intelligence phase

Impact:

- End User:
  - As Courion introduces role mining and role management, users could be contacted to make further changes to their access.
- Campus and central IT:
  - IT Personnel will be contacted to help with changes related to groups and role management. This includes assigning and removing users from roles and groups.
  - Additional IAM related legacy systems can be decommissioned at this stage
- Local IT:
  - IT Personnel will be contacted to help with changes related to groups and role management. This includes assigning and removing users from roles and groups.
- Business offices Impact

    - University Security Contacts (USCs) will be contacted to help with changes related to groups and role management. This includes assigning and removing users from roles and groups.

REVISION CONTROL

Document title	**IAM Project Overview & Milestones**
Author	**Amin Kassem**
File reference	**SharePoint**

Date	**By**	**Action**	**Pages**
5-15-13	**Amin Kassem**		**32**
7-3-13	**Rachel Buller**		**17**