WVM Ethos Identity Project Overview
Topics

- Terminology
- Ellucian Ethos Identity
- BEIS / BEP Overview
- ADAP Configurations
- Active Directory Attributes
- User Roles
- Student / Staff Roles
- Account Creation Process
- Banner Data Push
- Functional overview
- Questions
Terminology

▪ ADAP (Active Directory Account Provisioning)
  – has the ability to synchronize users from Banner into AD using BEIS.

▪ BEIS (Banner Enterprise Identity Services)
  – A collection of Banner components that support the district’s identity and access management architecture.

▪ BEP (Banner Event Processing)
  – A required component of Ellucian BEIS that publishes events in a standard XML format, when Banner data changes.

▪ SSO (Single sign-on)
  – Allows a user to securely access multiple systems with a single login account.

▪ SSO Manager
  – is a BEIS component that relies on a central access manager (such as CAS or the EIS) to authenticate a user and assert the user’s identity.

▪ SPML (Service Provisioning Markup Language)
  – the XML message is used to update the AD server for that particular user.

▪ UDC Identifier (UDCID)
  – A globally unique identifier that is assigned to each Banner user and is stored in an external data store, like Active Directory
Ellucian Ethos Identity Overview
Ellucian Ethos Identity

- Ellucian Ethos Identity is an enterprise middleware solution for institutions seeking to implement, simplify, or improve an identity and access management infrastructure.

- It is the driver behind policies and practice of ID Management and Single Sign On to different Banner and non Banner related applications.
BEIS / BEP Overview
The Banner Enterprise Identity Services (BEIS) with the Banner Event Publisher (BEP) provide mechanisms to help institutions to achieve their identity management goals, including enabling Ellucian applications to work with a 3rd party IDM, and supporting account provisioning from Banner (where Ellucian Banner ERP is the authoritative source for identities) or to Banner (where Banner is the non-authoritative source).

The following is a graphical representation of this architecture:
ADAP Configuration
ADAP Configuration

The ADAP components were deployed on two domains – one for Staff (the parent domain) and one for student (the child domain). There were two ADAP adapter web archives deployed to handle SPML messages for each roles from Banner (student and staff). Each of these web archives are registered as end points in BEIS Proxy.

The following is a graphical representation of this architecture:
Active Directory Attributes
Staff Attributes

- **extensionAttribute1**: Contains a person’s campus, and is used to auto generate mailing list membership. This should only be edited by HR through Banner. This is based on primary job.
- **extensionAttribute2**: E Class Code. This is also used to generate email lists, but in addition it is used for licensing in Office 365. This should only be edited by HR through Banner. This is based on primary job.
- **extensionAttribute4**: This denotes an employee, and is used to determine which employee active directory accounts are to be synced to the Office 365 cloud. This should only be edited by HR through Banner.
- **extensionAttribute7**: Fund Org information. Used by PageDNA. Controlled by Banner and Finance.
- **extensionAttribute8**: Fund Org information. Used by PageDNA. Controlled by Banner and Finance.
- **extensionAttribute9**: Contains a person’s UDCID. Without the correct UDCID present a person will not have access to any Banner applications, or their access could be to the wrong applications/records. This attribute is controlled by Banner, and should never be changed or deleted.
- **extensionAttribute13**: Used as a flag to activate licensing in Office 365.
- **company**: Contains a description of which part of the organization you work for. WVC, MC or the District. This is based on Primary Job. This should only be edited by HR through Banner.
- **department**: Contains a person’s department based on primary job. This should only be edited by Applications Staff through Banner.
- **title**: A person’s job title based on their primary job. This should only be edited by HR through Banner.
- **employeeID**: Contains the G Number. This should only be edited by Applications Staff through Banner.
- **employeeNumber**: Contains the old Colleague ID. This should only be edited by Applications Staff through Banner.
- **telephoneNumber**: Contains the phone number. This data is written to the account by the Shoretel system, and should only be updated through Shoretel Director. If a person has an incorrect office number, it will need to be updated in ShoreTel.

A person’s name, username, and address are all written by Banner. If a person’s name changes they need to change it through HR. Email information is maintained by the email system.
Student Attributes

- **extensionAttribute4**: This contains a student’s CCCID. This is the student’s unique CCCID for Federated Identity.

- **extensionAttribute10**: This contains a flag Office365. This is used to sync student AD accounts to the cloud.

- **extensionAttribute12**: This attribute contains a flag “Registered” OR “NotRegistered” that is used to assign a license for Office Pro Plus. Only students who are enrolled in classes in the current or the next term will receive “Registered” status for Office Pro Plus.

- **extensionAttribute13**: This contains a flag denoting Student or Alumni. This is used for licensing in the office cloud.

- **department**: This is used to denote a student’s campus, and will be used to redirect a student to the correct portal site.

All of these are managed by Banner and should not be changed. A student’s identity data is managed by A&R through Banner.
User Roles
User Roles

- Every ‘eligible’ staff and student in Banner will be assigned a role – Example – EMPLOYEE and STUDENT

- These roles are assigned if a person fulfills criteria set in pre defined rules

- These roles are the main driver behind establishing user access and determine how a person’s ID is created and what systems they can access

- They are created in Banner via a process which reads the pre defined rules and determines if a person is eligible – it also removes a role from a persons profile if a person no longer meets the criteria
Student / Staff Role
Student / Staff Role

Student
- Active (AS) status in SGASTDN
- Latest term code greater than or equal to 201730 (no ‘9’ terms included)
- Student type not equal to E

Student O365 Register Flag
- Calculate current term based on system date
- Check if registered for current term or greater
- If yes then ‘Registered’ else ‘Not Registered’

Staff
- Active status in PEAEMPL
- Exclude – PO, V1, CD, ND, RT
Account Creation Process
Account Creation Process

- The ADAP system will create and update accounts in an Organizational Unit (OU) related to a person’s role.
- When an event occurs in Banner – meaning a data change on one of the database table columns that are pre-marked – it triggers creation of an XML message that has all the data elements sent to a middleware server (ADAP server) using a SPML (Service Provisioning Markup Language) format.
- The XML message is then used to update the AD server for that particular user.
- This is all done online near real time.
- It includes creation of a new AD ID or updates to existing IDs.
- This process will run 5 times a day – 10am, 12pm, 2pm, 4pm, and 8pm.

Note – These actions only effect data changes for IDs that have a role defined in Banner.
Banner Data Push
Banner Data Push

- Banner will be the main source of data for all new AD IDs here on now. Previously these IDs were manually created in AD.

- Once the ID is created, all future changes to key data items are monitored and pushed to AD via ADAP, as long as the ID has the role defined.

- I.S. will not control the data in Banner, it will be maintained by HR and Student functional data owners respectively.

- HR and Student departments will work closely with I.S. and develop policies and practices for user management and access.

- They should be trained on some key data elements in Banner which are used in rules created to manage AD.

- Incorrect or missing information may have an impact on a user’s business processes and will impact a user AD access.
Functional Overview
Functional Overview – Create Staff / Student

Banner
- New Staff or Student created or updated
- Job to create roles based on rules
- Role table populated with data
- Fire BEP Triggers to generate XML with Banner data based on rules

BEIS / ADAP
- ID Gateway
- ID Proxy - Generate SPML Message from Banner data
- ADAP (different server) – SPML message and determine domain (Staff or Student)
- Send data to AD

Active Directory
- Receive data
- Create or Update AD Object and populate attributes
- Manage account security
- Forward to Office 365 for email etc.
Questions?