

System Administration Security

Authentication / Authorization and
LDAP on campus

Overview

- Security Status
- State Campus Status
- Community College Status
- eduPerson Discussion

Security Administrators

- Security Administrators needed for:

- Cayuga
- Corning
- Dutchess
- Erie
- FIT
- Finger Lakes
- Fulton-Montgomery
- Herkimer
- Mohawk Valley
- Monroe
- Nassau
- North Country
- Orange
- Schenectady
- Sullivan
- Tompkins/Cortland
- Ulster

State Campuses

- LDAP ready:
 - Albany
 - Buffalo College
 - Empire State College
 - Geneseo
 - Downstate Medical
 - Maritime
 - Morrisville
 - Old Westbury
 - Oswego
 - Purchase
 - Stony Brook

CC Distributed Authentication

- Clinton, Ulster – Complete
- Adirondack, Monroe, Rockland – Testing
- Finger Lakes, Fulton-Montgomery, Genesee, Jamestown, Mohawk Valley, Niagara, North Country, Orange, Schenectady, Tompkins/Cortland, Westchester – Communicating
- All others – No feedback

Distributed Authentication

- Coordinate LDAP configuration
- Firewall configuration
- Testing / Test User
- Notify Users
- Security Administrator

Security Working Committee

- The Suggested SUNY standard attributes are the result of a collaborative effort of the SUNY Security Working Committee (SWC). The SWC has representative members from SUNY campuses, System Administration, ITEC, Research Fund, SICAS, SLN and Library Services. The following individuals are the participating members of the SWC:

Chuck Dunn	University at Buffalo
Richard Reeder	Stony Brook University
Brian Gaon	SUNY Downstate Medical Center
Lesley Bidwell	SUNY at Oneonta
Bill Wagoner	Monroe Community College
James Dutcher	Orange County Community College
Chris Bordeleau	ITEC
Patrick Masson	SUNY Online Learning Environments
Kathleen Paranya	SICAS
Christine Carpenter	Research Fund
Jeremy Binger Dave Powalyk	System Administration

Security Working Committee

- Attributes proposed in IdM Spec 10/12/2006
 - eduPersonPrincipalName
 - eduPersonNickname
 - eduPersonOrgDN
 - eduPersonOrgUnitDN
 - eduPersonPrimaryOrgUnitDN
 - eduPersonAffiliation
 - eduPersonPrimaryAffiliation
 - eduPersonScopedAffiliation
 - eduPersonEntitlement
 - mail
 - displayName
 - telephoneNumber
 - postalAddress
 - sunyPersonId
 - sunyStudentId

Security Working Committee

- Defined attributes to expose
- Definition of attributes was not stated

Shared Attributes

- Campuses want to know how to set required attributes
- Proposed standard definitions
- System Administration Provided Examples

eduPersonPrincipalName

● Definition

- A uniquely valued identifier in the form of “user@scope” where scope defines the local security domain.

● SA Example:

- sAMAccountName represents the user in Active Directory
- Part of user setup in the SA LAN
- sAMAccountName@sysadmin.suny.edu

eduPersonNickname

● Definition

- Person's informal name or nickname

● SA Example:

- Already available in Active Directory via displayName or givenName
- Part of user setup in the SA LAN
- Example: John

eduPersonOrgDN

● Definition

- The distinguished name (DN) of the entry representing the institution the person is associated with

● SA Example:

- No organizational specific location

eduPersonAffiliation

● Definition:

- The person's relationship to the institution.

● Permissible values

- Faculty
- Student
- Staff
- Alum
- Member
- Affiliate
- Employee

eduPersonAffiliation

● Suggested U-Wide standard definition:

- **Faculty:** An active teaching instructor, for current course sections in the current term. Applications should source the Student Information System for this data.
- **Student:** An individual currently enrolled in one or more course sections in the current term. Current course sections include online learning courses, and zero-credit courses. Applications should source the Student Information System for this data.
- **Staff:** Any employee not categorized as faculty.
- **Alum:** An individual who received a degree in a program of study from the university. Applications should source the Student Information System for this data.
- **Member:** Any individual receiving services from the university (includes library card holder, parking pass holder, etc.)
- **Affiliate:** Any individual not directly associated with the university (vendor, auditor, etc.)
- **Employee:** Any individual working for the institution that has an active job record in the state, Research Foundation or FSA. Applications should source the Employment System as one source for this data.

eduPersonEntitlement

● Definition:

- URI that indicates a set of rights to specific resources. Roles and Accounts could be defined through entitlement

● SA Example:

- Currently <NULL>
- Future Use for distributed campus roles

mail

● Definition:

- The e-mail address of the user

● SA Example:

- Already available in Exchange via Active Directory
- Part of user setup in the SA LAN

displayName

● Definition:

- The way the user's name is displayed in the system

● SA Example:

- Already set in Active Directory
- Part of user setup in the SA LAN
- Example: Dave Powalyk

telephoneNumber

● Definition:

- The office or campus phone number of the user

● SA Example:

- Already available in Active Directory
- Part of user setup in the SA LAN
- Example: +1 518 555 1234

postalAddress

● Definition:

- The campus or office address

● SA Example:

- Street, City, Zip already available in directory
- Part of user setup in the SA LAN
- streetName + "\$" + | + "," + st + " " + postalCode
- State University Plaza\$Albany, NY 12246

sunyPersonId

● Definition:

- The user's SUNY ID as defined in the HR Person System

● SA Example:

- Currently <NULL>
- Will be assigned by System Administration HR application
- Campus must store value in directory
- Available via:
 - Feedback File
 - Web Service Query

sunyStudentId

● Definition:

- A SUNY ID assigned to a student by the IR office

● SA Example:

- Currently <NULL>
- Will be assigned by System Administration IR application
- Campus must store value in directory
- Available via:
 - Feedback File (Data Transfer System Process)
 - Web Service Query

Questions?



