

Magis Identity Management System 1.5
ITS / Enterprise Architecture Group
July 17, 2006
Document Version 1.2
Technical Audience - Specifications
Jh

Saint Louis University uses an Identity Management System (IDMS) named “Magis” to provide a single source of sign-on for enterprise applications.

Business Specifications

Information Technology Services is responsible for management of the IT Enterprise within the guidelines of regulatory compliance and University policy and procedure. Specific regulatory compliance issues (HIPAA) addressed by **Magis IDMS** include the following:

1. Information Access Control
2. Internal Audit
3. Personnel Security
4. Termination Procedures
5. Assigned Security Responsibility
6. Access Control
7. Audit Controls
8. Authorization Control
9. Data and Entity Authentication

The Banner database is the entry point and central repository for Faculty, Staff, and Student data at Saint Louis University. The Magis IDMS system presents that identity information, in combination with guest account information, as a central point for authentication.

The data steward for student information is the University Registrar. The data steward for Staff data is the Human Resources division. The data steward for Faculty information is the Provost.

Functional Specifications

Faculty, Staff, and Student data is entered through the Banner interface under the supervision of the respective stewards of that data.

Guest data is entered into a Banner Oracle table by the ITS Customer Service Center. Other technical accounts can also be created by the Server Team with the authorization of the Server Team lead.

Technical Specifications

Magis IDMS consists of three components:

1. A proprietary Microsoft SQL application which pulls user data from a view in the Banner Oracle database. This application has a web interface through which temporary accounts can be entered. This collection is done by a dirXML driver provided by Novell. The current version (1.5) is pulling only Faculty and Staff data once a day at 6 am.

The structure of data coming from Banner is as follows:

| Field | Data Type | Sample Value |
|--------------------|-----------|--------------------------------|
| Banner_ID | text 9 | 000049671 |
| Full_Email_Address | text 38 | kappjd@slu.edu |
| Net_ID | text 30 | kappjd |
| Last_Nm | text 25 | Kapp |
| First_Nm | text 15 | Jeffrey |
| Middle_Nm | text 15 | D |
| Sort_Nm | text 30 | Kapp, Jeffrey D |
| Orgn | text 6 | Z604 |
| Orgn_Name | text 30 | ITS-Enterprise Resources |
| Lev1 | text 6 | E75 |
| Lev1_Org_Name | text 30 | VP & Chief Information Officer |
| Lev2 | text 6 | S43 |
| Lev2_Org_Name | text 30 | Information Technology Service |
| Lev3 | text 6 | D056 |
| Lev3_Org_Name | text 30 | Information Technology Service |
| Lev4 | text 6 | Z605 |
| Lev4_Org_Name | text 30 | ITS-Enterprise Resources |

2. A Novell eDirectory (SLUID) which collects user entity data from the SQL data base through a JDBC driver provided by Novell.
3. A Novell eDirectory (Magis) which pulls information from the SLUID eDirectory and places it into Organizational Units (OUs) that is representational of the Saint Louis University organizational structure as stored in Banner. Magis currently supports Sign-In and desktop management (ZenWorks) for the Billiken Information Shield environment, and is capable of authenticating users for any system compliant with OpenLDAP. The CMS and enterprise web servers are slated to use Magis for authenticating beginning the week of 7/24.
4. Timing - Data is pulled from Banner once per day. Data is pushed into eDirectory (Magis) every thirty seconds.
5. Passwords – Default passwords in the directory are <null>. (needs to be verified)