



Technology for Communication, Collaboration and Productivity

Identity Access Management



Portal Solutions



Custom Application Development

2009 Product Catalog

Friday, April 03, 2009

IDW-200 Identity Workflow

▶ IDW-200-1 AppointLink Identity Workflow (AIW)

The Identity Workflow Application is a complete user access management system that allows organizations to effectively and efficiently control access by a diverse user population to corporate resources. The system provides the following:

- Self Service Access Requests for New User, Change User, Request Status, Task List, and Data Cleanup.
- Request Workflow Processing
- Rule based Provisioning/De-Provisioning
- Automatic Access Provisioning for AD, EPIC, eDir, email, directory access, etc. LDAP
- Authoritative connections to HR Systems
- User Access and Compliance Reporting
- Data Cleanup Utilities

Key benefits of AIW:

- Allows organizations to enforce access policies at the corporate, entity, department, or application levels.
- Provides mechanisms to standardize all requests for resource access.
- Automatically de-provisions users after termination or transfer.
- Facilitates and automates request approval processing.
- AIW provides tools to accurately measure the timeliness of approvals and provisioning tasks.
- Allows management to measure provisioning workload across the organization and compare provisioning performance between entities and applications.
- Provides automated escalation of delayed approval and provisioning tasks.
- Maintains detailed records of approved user access levels at the application level providing a basis for audits of downstream systems.

▶ IDW-200-1-FP1 AIW Advanced Provisioning Feature Pack

This feature pack provides more sophisticated workflow provisioning features to the base product. These features allow complex dependencies between applications, sequencing based on approval and provisioning status, and custom conditions and events based on user defined SQL Server functions.

▶ IDW-200-1-FP2 AIW Feature Pack 2 - Enhanced Reporting

This Feature Pack adds reporting to 1) measure provisioning and approval workload, 2) compare provisioning efficiency between organizations, 3) provide more detailed auditing reports and 4) provide detailed active request analysis.

▶ IDW-200-1-FP3 AIW Feature Pack 3 - Advanced Provisioning Notes and Non-Employee Workflows

This feature pack provides a new workflow and updates to tasks to allow operation with or without connection to a help desk systems (i.e. Remedy) as a provisioning method. This feature pack adds a new workflow to allow end users to change non-employee records to employee records. Updates to the task list include options for provisioners and approvers to add more detailed comments when tasks are complete. This feature pack also updates the batch import process to automatically create both AD and IChain accounts as part of the normal import.

IDW-200 Identity Workflow

▶ **IDW-200-2**
AIW-SAP Authoritative Connector

The SAP Authoritative Connector reads a data feed from SAP and converts the feed into events that are applied to the user information in the Identity Workflow Database. The connector processes new user, user termination, user transfer, and name change events from SAP.

▶ **IDW-200-3**
AIW-JDBC/NOVELL Connector

The connector provides event generation code and JDBC driver configuration settings necessary to manage user objects in the eDir vault.

IDW-120 Faculty / Staff Access Management

▶ IDW-120-1 Faculty/Staff Object Manager

The Faculty/Staff Object Manager system provides functions to monitor an authoritative source for new or changed faculty/staff information. The system will create, update, move, and optionally delete faculty/staff objects stored in an eDir directory based on client specific policies. Installation of the driver includes analysis of existing policies and configuration of the database components to ensure object management complies with these policies. This product includes all Faculty/Staff Object Manager database components, installation and configuration of the JDBC drivers, technical documentation, administrator training and maintenance plans. This product requires the selection of at least one of the Faculty/Staff Object Manager authoritative connectors (IDW-100-2).

▶ IDW-120-2-1 Faculty/Staff Authoritative Connector-CIMS

The Faculty/Staff Authoritative Connector - CIMS module provides a bidirectional connection between the Faculty/Staff Object Manager database and the CIMS faculty/staff information system. This module gathers faculty/staff attributes from the CIMS faculty/staff tables and forwards updates to the Faculty/Staff Object Manager. The module can be configured to update fields in the CIMS system from data in the Faculty/Staff Object Manager database or connected directories.

▶ IDW-120-2-2 Faculty/Staff Authoritative Connector-SQL Server

The Faculty/Staff Authoritative Connector - SQL module provides a bidirectional connection between the Faculty/Staff Object Manager database and any SQL Server database. This module gathers faculty/staff attributes from SQL tables and forwards updates to the Faculty/Staff Object Manager. The module can be configured to update fields in SQL Server from data in the Faculty/Staff Object Manager database or connected directories.

▶ IDW-120-3-1 Faculty/Staff eDir-eDir Driver

The Faculty/Staff eDir-eDir driver configuration provides synchronization between the faculty/staff object vault and the production eDir directory.

▶ IDW-120-3-2 Faculty/Staff AD Driver

The Faculty/Staff AD Driver synchronizes the faculty/staff objects in either the vault or production directories with Active Directory.

IDW-120 Faculty / Staff Access Management

▶ IDW-120-4 Faculty/Staff Group Manager

The Faculty/Staff Group Management Application automates the creation and maintenance of groups for faculty/staff based on course enrollment, section, faculty, and school. The application takes a data field from the authorization system and then establishes group membership based on configured rules. Group membership can be based on simple one to one mappings from attributes to group names or on sophisticated mapping rules that allow AND, OR, and NOT conditions. The system also rolls up disconnected subsets into a single group.

The application includes all linkage to automatically provision groups from the database into the vault. Additional components allow downstream provisioning into additional edit vaults and Active Directory. The group rule database table can be exposed to other client applications allowing precise timing of group creation and expiration. System includes audit reporting which allows administrator to track what users were in what groups at what time.

IDW-100 Student Access Management

▶ IDW-100-1 Student Object Manager

The Student Object Manager system provides functions to monitor an authoritative source for new or changed student information. The system will create, update, move, and optionally delete student objects stored in an eDir directory based on client specific policies. Installation of the driver includes analysis of existing policies and configuration of the database components to ensure object management complies with these policies. This product includes all Student Object Manager database components, installation and configuration of the JDBC drivers, technical documentation, administrator training and maintenance plans. This product requires the selection of at least one of the Student Object Manager authoritative connectors (IDW-100-2).

▶ IDW-100-2-1 Student Authoritative Connector - CIMS

The Student Authoritative Connector - CIMS module provides a bidirectional connection between the Student Object Manager database and the CIMS student information system. This module gathers student attributes from the CIMS student tables and forwards updates to the Student Object Manager. The module can be configured to update fields in the CIMS system from data in the Student Object Manager database or connected directories.

▶ IDW-100-2-2 Student Authoritative Connector - SQL Server

The Student Authoritative Connector - SQL module provides a bidirectional connection between the Student Object Manager database and any SQL Server database. This module gathers student attributes from SQL tables and forwards updates to the Student Object Manager. The module can be configured to update fields in SQL Server from data in the Student Object Manager database or connected directories.

▶ IDW-100-2-3 Student Authoritative Connector - Banner

The Student Authoritative Connector - Banner module provides a connection between the Student Object Manager database and Banner views of student data. This module gathers student attributes from Banner views and forwards updates to the Student Object Manager.

▶ IDW-100-3-1 Student eDir-eDir Driver

The Student eDir-eDir driver configuration provides synchronization between the student object vault and the production eDir directory.

▶ IDW-100-3-2 Student AD Driver

The Student AD Driver synchronizes the student objects in either the vault or production directories with Active Directory.

IDW-100 Student Access Management

▶ IDW-100-3-3 Student LDAP Driver

This module connects to the Student Access Manager database and synchronized user groups in a single LDAP directory based on changes to group membership. This .NET application requires credential on the LDAP directory with permissions to search for user objects and update group settings.

▶ IDW-100-4 Student Group Manager

The Student Group Management Application automates the creation and maintenance of groups for students based on course enrollment, section, faculty, and school. The application takes a data field from the authorization system and then establishes group membership based on configured rules. Group membership can be based on simple one to one mappings from attributes to group names or on sophisticated mapping rules that allow AND, OR, and NOT conditions. The system also rolls up disconnected subsets into a single group.

The application includes all linkage to automatically provision groups from the database into the vault. Additional components allow downstream provisioning into additional eDir vaults and Active Directory. The groups rule database table can be exposed to other client application allowing precise timing of group creation and expiration. The system includes audit reporting which allows administrators to track what users were in what groups at what time.

IDW-090 Identity Workflow Utilities

▶ IDW-090-3 Data Prep Utility

The Data Prep Utility provides security managers with functions to quickly validate and classify user information extracted from other systems. As security managers integrate provisioned systems with the identity management processes there are often discrepancies between authoritative credentials found in the Identity Workflow database and islands of user data found in systems that existed before implementation of the Identity Workflow Solution. This utility allows the batch import of user credentials from these other systems and outputs an MS Excel report with potential matches to the authoritative data set. These potential matches are ranked by probability of an exact match allowing the user to select or adjust the record that will be used in the final import into the Identity Workflow Solution. The Data Prep Utility will export a file format that can then be imported into the Identity Workflow Data Import Utility.

▶ IDW-090-4 Data Cleanup Utility

The Data Clean-up Utility provides security managers with functions to quickly validate and classify user information in the AIW system that violates business rules. As security managers integrate provisioned systems with the identity management processes there are often discrepancies with user information found in the Identity Workflow database. This utility allows the manager to determine if a user record should or should not be used in the Identity Workflow Solution. The Data Clean-up Utility will also merge the records that have been selected to be used back into the Identity Workflow Data system.

Platform: The Data Clean-up Utility is a Windows - MS Access 2003 application with linked tables to Identity Workflow user data tables.

Data Input: The data used in this application will be user records selected from the AIW system that violate the business rules (i.e. duplicates, invalid character in User ID, missing employee number for user with occupations codes, etc.) *The duplication scenarios will be limited to User Record scenarios defined in the Data Cleanup Scenarios document as of 1/31/09.*

Data Output: The user records that have been reviewed in the Data Clean-up Utility and approved for use in the AIW system will be merged back into the Identity Workflow database.

Prerequisites: This application requires windows XP or Vista and MS Access 2003. The user's machine must meet the minimum requirements for the operating system and MS Access 2003 to run this application.