

PRODUCT OVERVIEW

ARMS—Account Management

The Access Request Management System (ARMS) is the premier end-user facing Identity Management tool on the market. ARMS combines an intuitive, simple to use interface, with the power and functionality to manage identity and access in the most complex environments. ARMS is a suite of tools made up of three modules, each designed to handle specific facets of the Identity life cycle. These modules are seamlessly integrated to provide flow from one module to the next. The Account Management Module provides

FAST FACTS

What you need to know about Account Management

- ⇒ Provides user self-service facility
- ⇒ Recover passwords on any smartphone
- ⇒ Policy based password complexity enforcement
- ⇒ Integrations with DSS and other ARMS modules
- ⇒ Cross-platform browser based access

end-users with self-service functionality as well as providing managers, help desk users and other delegates with delegated administration capabilities. Requesting, approving, tracking and re-attesting access are all provided with the Workflow Module. Lastly, the Sponsorship Module allows IT to delegate the lifecycle management of external accounts to the hiring manager while enabling policies to ensure compliance. With the addition of DSS, ARMS is fully integrated into an organization's identity management infrastructure, giving IT administrators single point, cradle to grave control over all users in the system.

The Account Management Module harnesses the full capabilities of a unified identity management solution. Through the interface, accounts can easily be kept current and the changes will be pushed out to all of the systems connected to the IDM architecture. Passwords across all resources can be set and managed from this solution allowing security policies to be set in one place and at one level, superseding less desirable password requirements. The Whitepages is an example of a custom delegation that provides contact information to everyone in the system, through a simple, searchable interface.

The key feature of the Account Management Module of ARMS is its granular, top down delegation of profile maintenance. Administrators are able to grant modification rights to all levels of users within a system. These delegations of authority can be as general or precise as desired. Each field of the user profile can have change/update authority granted to anyone in the organization that would need to maintain the account. For example, employee accounts can be organized by departments and IT can then delegation actions to the department manager for their respective group of users.

End users can be delegated the ability to keep their digital identity up to date, and are able to reset their forgotten password via a self-service application that is challenged based which removes the need to contact the help desk for password issues. Organizations that deploy the ARMS Account Management Module can define custom delegations to meet specific requirements. For instance, school districts can leverage custom delegation definitions to provide teachers with the ability to assist their students with password resets. Department managers can be given authority over their entire team, giving them easy self-supportability on matters of user information. This type of delegation reduces downtime for the workforce and it reduces burden on the IT department. The help desk role members can view and maintain all users in the system from the same interface.

Additionally, the Account Management Module of ARMS has the added functionality of a mobile application available for smart phones including iPhone, Android, Blackberry and Windows Mobile platforms. This gives users the flexibility to reset their password from a mobile device when they are unable to authenticate to a PC and access the ARMS web interface.

The ARMS Account Management Module provides a simple, transparent solution for profile and password maintenance. Its delegation of self-service responsibility to users and group leaders frees IT staff from the need to constantly maintain the present, and allows organizations to leverage their technology staff on projects that look to the future.



IDENTITY, DATA AND ACCESS MANAGEMENT SPECIALISTS

WWW.IDENTITYAUTOMATION.COM : INFO@IDENTITYAUTOMATION.COM