

PRODUCT OVERVIEW

ARMS—Workflow

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

deploys solutions for issues of security policy compliance, by keeping a history of who has access, when the access was granted, and when the access will expire or need re-attestation.

When implemented the Workflow Module begins as a blank slate, administrators will then custom define the workflow paths and build the resource definitions. This provides the organization total control over what resources can be requested, and who can request them. The path through which requests are approved is also defined at this time, the process of approval can be as simple or complex as desired. Requests can have pool of users that can approve a resource or it can be required that the workflow go through a number of stages to meet the requirements for approval. At each and every stage email messages can be dispatched to keep an accurate time line of events for each request made. Finally the expiration of access is defined, ensuring that accounts are properly maintained and deprovisioned when no longer needed.

FAST FACTS

What you need to know about Workflow

- ⇒ Automated mechanism to request resources
- ⇒ Dashboard showing all assigned resources
- ⇒ Provides auditable trail for compliance
- ⇒ Delegates responsibilities to function owners
- ⇒ Integrations with DSS and other ARMS modules
- ⇒ Cross-platform browser based access

Module provides 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 Workflow Module of ARMS provides organizations an interface that displays instant state of access information across the entire work environment. All levels of the organization's hierarchy can access the tool to view their current permissions. An individual can view what they currently have access to and what requests are active and can be made in the future. Department managers can view their team, and administrators and help group can search and view the access for any user in the organization. Both physical resources and electronic credentials can be tracked, requested, and either approved or denied. The Workflow Module

The Workflow Module can be configured to track the access to, or possession of any resource the organization provides. This can include access to information systems such as email or customer management software, or can be physical items including keys, computers, and mobile phones. When leveraged through an identity management solution, Workflow can automatically provision users into network resources once the request for access has been approved. For physical resources that are tracked by the Workflow Module email can be sent to the distributor of the resource once the request for the item in question has been approved. Email can also be utilized by Workflow to provide updates and documentation for all requests managed with the module.

The ARMS Workflow Module provides a simple, transparent solution for access and resource management. It's automation of access approval along with an accurate history of requests made and their current status gives a complete picture of who has access, who owns the access, and where the organization's resources are right now.



IDENTITY, DATA AND ACCESS MANAGEMENT SPECIALISTS

WWW.IDENTITYAUTOMATION.COM : INFO@IDENTITYAUTOMATION.COM