WHITE PAPER

Joiner, Mover, Leaver:

User Provisioning with SolarWinds Access Rights Manager

Joiner, Mover, Leaver: User Provisioning with SolarWinds Access Rights Manager

The flexibility of today's working world requires a well thought-through user provisioning process. Whether for a new user, a short-term assignment, department changes or temporary projects, the expectations of an IT group are to accurately and quickly provision users while helping to maintain data security.

IT departments are typically responsible for securing a network, managing access to resources and keeping an overview of permissions and access rights policies. Therefore, they should use a provisioning framework. SolarWinds® Access Rights Manager (ARM) is designed to help address the user provisioning process across three phases—joiners, movers and leavers.

THE JOINER PHASE

The joiner phase encompasses the onboarding process. How quickly can a user and their email account be generated? Has the correct information been entered? Has the employee been added to all mailing lists? Mistakes can be expensive and wreak havoc on collaboration with partner organizations or related activities.

User creation

ARM is built to automate and optimize the process workflow by allowing HR to create new user accounts through a self-service portal. Instead of sending user information to IT, HR can enter and create a new account in one step. The help desk only has to check and approve the requested changes. Through templates, which can be defined by IT and administrators, the overall permissions concept can be maintained.

Depending on the defined role, new employees receive a batch of basic permissions based on templates defined by departments and compliance managers. Any additional permissions on file servers and Microsoft® SharePoint® can be granted directly by the data owner. These data owners can control the field of play for their employees, helping ensure that each role is fit for the right purpose.

Mailbox management

ARM is designed to make managing Microsoft Exchange® mailboxes within ARM simple, allowing you to:

- Enable mailboxes
- Manage email addresses—assign to and remove multiple email addresses from mailboxes, distribution groups and contacts

- Change permissions
- Manage of out-of-office notices
- Manage mailbox and email size
- Manage distribution groups, memberships and permissions

THE MOVER PHASE

When employees switch to a different department, access rights can be revoked or granted directly by the data owner. The new manager will receive a new employee account with only basic permissions, and can then provide the appropriate access rights for that specific role. If the employee requires additional access rights beyond their new department, they can request those rights from the appropriate data owner.

Recertification of existing access rights

Modern, robust security requirements usually demand the implementation of the principle of least privilege. This is why data owners should periodically check the access rights of their resources and employees. A recertification processes is meant to help you check and change access rights for your resources.

Requesting file server access rights from data owners

Employees can request access rights to file server directories from data owners using the ARM self-service portal. You can configure a variety of different processes and involve the relevant decision makers, depending on your security requirements.

Moving objects in Active Directory

ARM is built to help you move objects—meaning user accounts, group accounts and computers—from one organizational unit (OU) to another. This may be required if one of your users moves their location or if new group policies are applicable.

Modifying group and user attributes

ARM is designed to help you easily manage attributes for user accounts via a flat list. The system will automatically document any actions you take.

Resetting passwords

Resetting passwords is a common task performed by help desks. ARM is designed to allow an easy and safe way of resetting passwords. Sensitive actions are documented in a log book. If an employee uses native tools to reset a password and illegally tries to access that user account, the system will capture the incident.

THE LEAVER PHASE—USER DEPROVISIONING

When an employee leaves the organization, HR informs the help desk. The help desk can then decommission the user by using the "soft delete" (for example, during parental leave) or by irrevocably deleting the user account.

Deactivating a user account

If you deactivate an account with ARM, this is equivalent to a normal deactivation in Active Directory®. The user account remains in the OU.

Deleting a user account by using the "soft delete" feature

When deleting a user with "soft delete," their access rights remain intact. The account is moved to a "Recycle-OU" status, and deactivated. This account can no longer be used, since the "Recycle-OU" is part of a strictly limited group policy.

Removing a user and their permissions

ARM is built to allow you to delete users from Active Directory and remove their access rights on the file server in one easy action.

SEE HOW SOLARWINDS ACCESS RIGHTS MANAGER WORKS IN YOUR ENVIRONMENT

Want to see just what ARM can do for you? Simply download a free 30-day trial, or give us a call and one of our specialists will arrange a personalized demo.

For a free trial, visit solarwinds.com/access-rights-manager/registration

To contact sales, visit solarwinds.com/company/contact-us

This document is provided for informational purposes only. SolarWinds makes no warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information contained herein.