

	Quarterly Reporting	Production Schedule	Product Roadmap	Marketing Plans	Performance Data	Sales Records	Workforce Data	
41			1					Abner, Mark
		5			5	1		Aloe, Vera
	1	34						Ander, Cori
	1		12			39		Agebrandt, Angie
		14			1			Baer, Roy
4	1							Becher, Joe Kurt
	13		1			9		Borg, Angie
				12		1		Busch, Burkhard
			1		3			Dampf, Hans
		2		21	1			Dee, Dan
		1				17		Frido, Fleia
			3		1			G...
1								n



 eBOOK

Access Rights Manager: Evaluation Guide

Purpose of this document

We're glad you decided to evaluate SolarWinds® Access Rights Manager (ARM) to analyze, document, monitor, and change access rights in your company. You can download the free trial [here](#). The trial version is a full-featured version of the product, functional for 30 days. After the evaluation period, you can easily convert your evaluation license to a production license by obtaining and applying a license key.

This document will get you started with Access Rights Manager and help you explore for yourself how ARM's features work in your environment. It will guide you through installation and initial discovery, and provide an overview of key features and functionalities.

If you require further information or troubleshooting, do not hesitate to contact sales@solarwinds.com or visit our Success Center, particularly the Installation Guide and Getting Started Guide.

WHY YOU MAY NEED AN ACCESS RIGHTS MANAGEMENT SOLUTION

Common symptoms indicating you might need to consider an access rights management tool:

- » Your Active Directory® structure has grown constantly and you are lost in its structure
- » You don't know who has access to your file servers, Exchange™, or SharePoint® resources
- » You have no idea about the as-is processes in Active Directory and your file and Exchange servers
- » Your organization has no processes and responsibilities implemented for a secure ARM tool
- » Changes to important accounts and folders remain under the radar
- » You are still managing your access rights by hand and documenting changes in Excel

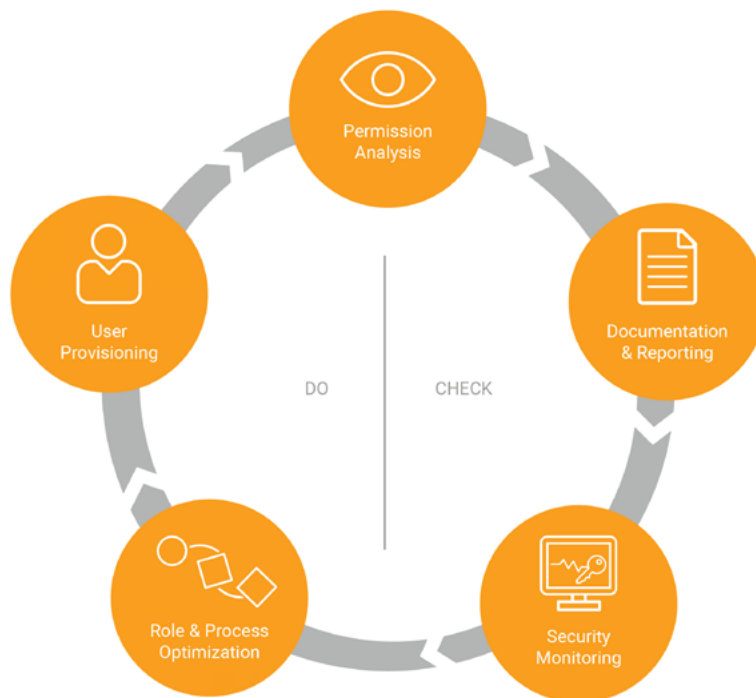


Figure 1: Five Central Disciplines of Access Rights Manager

Access Rights Manager is focused around five central disciplines. Together, they make up a clear and easily implementable system of safe and easy Access Rights Management.

PERMISSION ANALYSIS Displays a comprehensive overview of the access rights situation to resources in your organization

DOCUMENTATION & REPORTING Records any access rights activity in our logbook and creates audit-ready reports

SECURITY MONITORING Monitors security-relevant actions in Active Directory and on your file servers

ROLE & PROCESS OPTIMIZATION Shortens your access rights management process and involves only the most important actors

USER PROVISIONING Sets rules for the creation of new user accounts, provisioning of rights, and editing of account details

	ARM FEATURE	ARM BENEFITS
PERMISSION ANALYSIS	AD Graph	Get a comprehensive view on your Active Directory by clicking through the group structures. Identify nested groups, and see where you have to remove memberships without affecting wanted permissions.
	Resource View	Get a comprehensive view on all your resources (Active Directory, file servers, Exchange, SharePoint, and the users with access to it). You can also select one user and identify all access rights assigned to the account. Furthermore, you can check out multiple access paths to folders and remove them.
	Risk Assessment Dashboard	<p>Incorrect permissions and settings can cause security risks. The Risk Assessment Dashboard visualizes the top risk factors with the highest security impact.</p> <p>ARM displays the following risk factors:</p> <ul style="list-style-type: none"> » Noncompliant user accounts » Accounts with passwords that never expire » Directories with deviating access rights » Unresolved SIDs in directories » Globally accessible directories » Groups in recursion » Inactive accounts
DOCUMENTATION & REPORTING	Reports	The access rights situation, as well as the process of assigning access rights, is fully documented in a large variety of well-structured reports. These are crucial for fulfilling requirements in regulations such as GDPR, SOX, PCI DSS, HIPAA, and more.
	Logbook	Track all the activities in an easy-to-comprehend and adjustable Logbook.
	Comment Window	Every change must be documented. Besides the automatic tracking of the account and action, the user must always enter a comment. This way, you know (even after years) why the change had to be made.
SECURITY MONITORING	Logging	The ARM Loggers deepen the level of security within Active Directory and file and Exchange servers. Instead of only showing the current situation, you get full insight into the as-is processes performed in your systems. The AD analysis shows changes made with Windows native tools. In this way, temporary group memberships for quick data theft become immediately transparent. The file server Logger provides insights into who did what in sensitive folders. The Exchange Logger displays if anyone accessed a sensitive email account.
	Alerting	ARM informs you (proactively via the alerts feature) if someone attempts to manipulate user accounts, group memberships, or file server directories. The threshold functionality alerts users in charge when typical incident behavior (such as data theft) is being performed on file servers. After an alert has been released, a script tailored to the incident can be executed.

ARM FEATURE		ARM BENEFITS
ROLE & PROCESS OPTIMIZATION	The ARM Self-Service Portal	Employees often need access to resources from other departments. With the ARM Self-Service Portal, the needed access can be ordered. The Data Owner can easily confirm the request, and the right will be delivered automatically. This way, ARM bridges the gap between IT and business. Depending on the organizational structure and demand, a workflow can be designed for each resource individually.
	Periodic Review of Access Rights	Through periodic reviews, the data owner can add and remove permissions, or leave them unchanged, even without any specific IT knowledge. SolarWinds Access Rights Manager will perform the changes automatically. This way, you achieve one important milestone in data security: The Access rights to your directories are maintained based on the Principle of Least Privilege.
	User Cockpits	SolarWinds Access Rights Manager offers User Cockpits. Every role in the company has its own view and instruments in an easy to comprehend web client. The functionality is primarily made for Help Desk Agents as they are often assigned to handle standard Active Directory operations, such as password reset. By using the web client, ARM ensures no damage can be done to Active Directory. All functionalities can be made available according to the user's qualification.
USER PROVISIONING	Joiner, Mover, & Leaver Process	ARM is designed to help address the user provisioning process across three phases—joiners, movers, and leavers. Create a new Active Directory account based on a template for a certain unit or function of your company. You can specify the creation of mailboxes and distribution groups and automatically execute a script after the account has been created (e.g., for creating a set of working folders for the user). If the user changes into another department, just assign a different department profile to the account, and the user will get a basic set of permissions relevant for their new job. In case the employee leaves, you want to make sure sensitive data stays in your organization. Easily deactivate the user with "soft delete," and the account is transferred to an organizational unit with a strictly limited group policy.
	Group Wizard	If you modify file server rights with ARM, Active Directory groups are set up in the background automatically. Therefore, the assignment of rights follows Microsoft® best practice.
	Automatic List Rights Provisioning	ARM builds list rights automatically. This way, users can move freely in the entire directory structure to the folder they have access to.
	Scheduled Provisioning	In many cases, it makes sense to only grant access rights for a certain time period. With "Scheduled Provisioning," the administrator makes sure a consultant or trainee only has access until a project is over. ARM will automatically remove the given rights on the desired date.

Evaluators' guide

Install and Configure

PLANNING AND PREREQUISITES

Your ARM server sizing is impacted by:

- » Number of domains and users
- » Number of resources and size (file servers and folders, Exchange and mailboxes, SharePoint and sites)
- » The time span in which scan and log data is stored

ARM installations on virtual machines are supported. The virtual machine requirements are identical to the physical server requirements.

System requirements can be found [here](#).

INSTALLATION

You'll find a detailed walkthrough of the installation in the [Install & Configuration Manual](#)

In short, follow these three steps:

1. Download the [free trial of ARM](#)
2. Copy the downloaded setup.exe into a local folder on your ARM server (do not use a network folder); start the setup
3. Select all options except FS Logga. Click "Install."

WEB CONFIGURATION

The configuration of the web components starts automatically after the setup.

1. For evaluation, leave the server name and port as default
2. Select the desired certificate; for evaluation purposes, you can use a self-signed certificate

BASIC CONFIGURATION

The basic configuration screen is displayed automatically after starting the ARM configuration module for the first time.

1. Enter credentials to connect to Active Directory
2. Enter SQL server connection parameters

For evaluation purposes, you can use SQL Server® Express Edition.

SCAN CONFIGURATION

With the scan configuration, you can add resources to ARM. Possible resources include:

- » Active Directory (AD)
- » File servers
- » Exchange (online and on-premises)
- » SharePoint (online and on-premises)

Always start with an AD scan, then add more resources as you wish.

Scans are noninvasive and perform no changes to resources. Scans have minimal impact on the performance of resource systems. For example, a file server scan typically generates less than 5% CPU load.

For a useful evaluation, we strongly recommend you include productive systems. Add resources gradually, and limit the file server scan scope and depth at the beginning for quick results.

In ARM, you can use the graphical user interface to analyze the access rights situation and create reports for added resources.

Find more information about configuring scans in the [Install & Configuration Manual](#).

CHANGE CONFIGURATION

To test the User Provision features, you must set up the change configuration for the different resources.

With Group Wizard and automatic list rights assignment, ARM offers an enormous increase in efficiency in the assignment of permissions, especially for file servers.

You find the change configuration on the home screen of the configuration menu.

For more information, check the [Install & Configuration Manual](#).

LOGGA CONFIGURATION

ARM scans the permission information of the configured resources at scheduled intervals. To continuously monitor changes to resources, you must configure and activate the ARM Logga modules. ARM provides logging for file servers, Exchange servers and Active Directory. This allows you to capture activities and changes that have been made, for example, with Windows native tools.

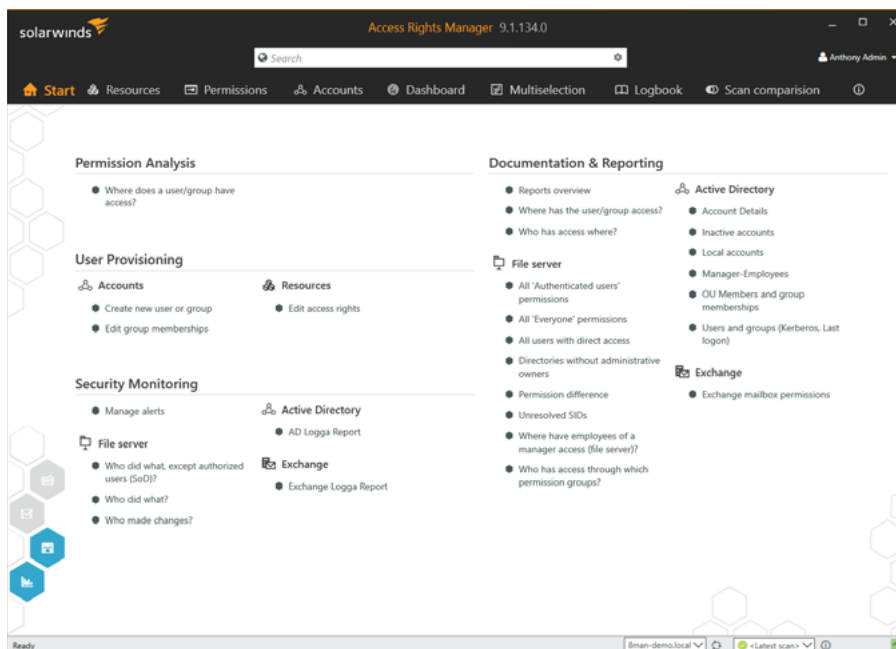
You configure the Logga modules in the ARM configuration menu in the “Scans” section.

For more information, check the [Install & Configuration Manual](#).

EXPLORE SOLARWINDS ARM FEATURES

ARM START PAGE

After a successful installation and configuration, you can access the rich client landing page. All the product’s core services can be triggered from here. Try the search bar, as it is the quickest way to find a user or resource.



ARM ACCOUNTS VIEW

By searching for a specific user (e.g., Helena Help Desk) in the search bar, you get automatically directed into the Accounts View, where you can identify the user's group structure with the AD Graph.

The screenshot shows the SolarWinds Access Rights Manager 9.1.134.0 interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', and 'Scan comparison'. The 'Accounts' tab is active. The central 'Graph' pane shows a hierarchical structure of groups and users. On the left, a 'Parents' pane lists various groups like 'Domain Users' and 'Users'. On the right, a 'Children' pane shows details for the selected user 'Helena Helpdesk', including attributes like Name, Email Address, and Organizational Name.

ARM RESOURCE VIEW

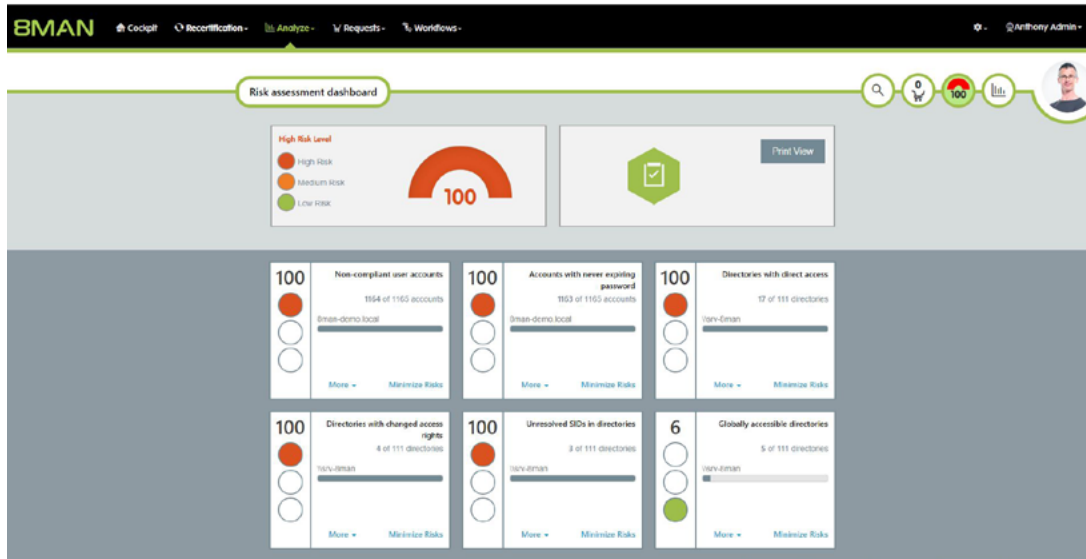
By searching for a specific resource (e.g., Marketing) in the search bar, you get automatically directed into the Resource View. All users with permissions to the folder are listed on the lower right side.

The screenshot shows the SolarWinds Access Rights Manager 9.1.134.0 interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', and 'Scan comparison'. The 'Resources' tab is active. The left pane lists resources under 'Active Directory' and 'File server'. The right pane shows the 'Marketing' resource with a table of permissions for various users and groups.

Name	how often granted	Inheritance
Abbey O'Flaherty (Bman-demo\Abbey O'Flaherty)	1	
Abdul-Hadi Deeb (Bman-demo\Abdul-Hadi Deeb)	1	
Adalino Contreras (Bman-demo\Adalino Contreras)	1	
Adam Adminmanager (Bman-demo\Adam Adminmanager)	2	1x
Adalugo Buchi (Bman-demo\Adalugo Buchi)	1	
Administrator (Bman-demo\Administrator)	2	1x
Adolfsee Bonenfant (Bman-demo\Adolfsee Bonenfant)	1	
Adrienn Foldesi (Bman-demo\Adrienn Foldesi)	1	
Agatha Melo (Bman-demo\Agatha Melo)	1	
Ahmad Khoury (Bman-demo\Ahmad Khoury)	1	
Al Tao (Bman-demo\Al Tao)	1	
Aida Spuren (Bman-demo\Aida Spuren)	1	

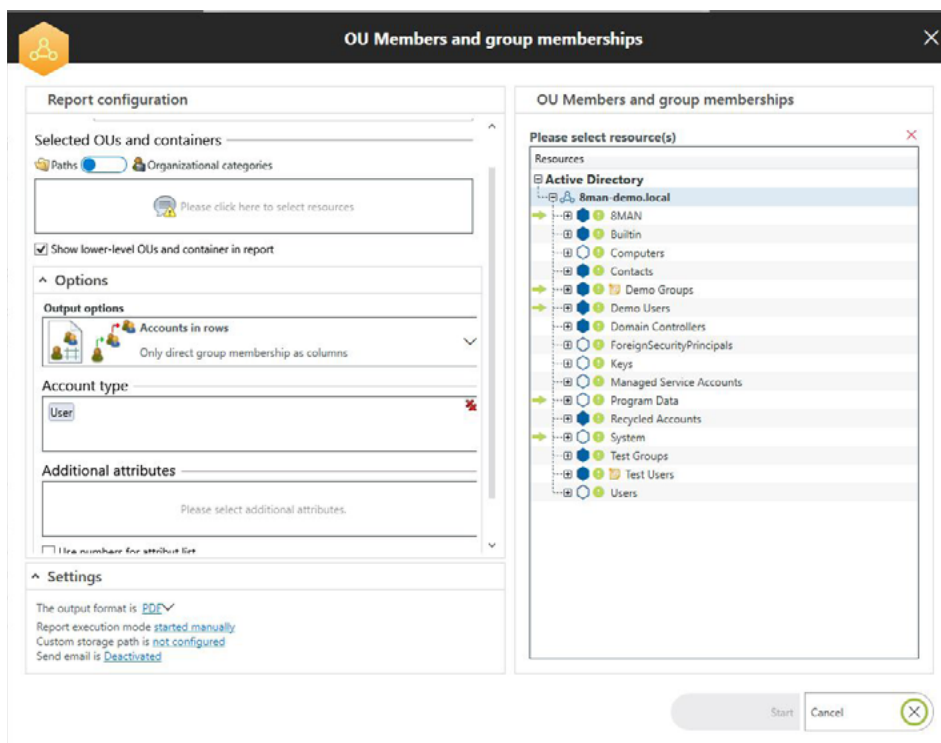
RISK ASSESSMENT DASHBOARD

Access Rights Manager has many functionalities in the web client. Check out the Risk Assessment Dashboard to see the core threats in your system. Click on a Risk and let ARM identify all issues automatically.



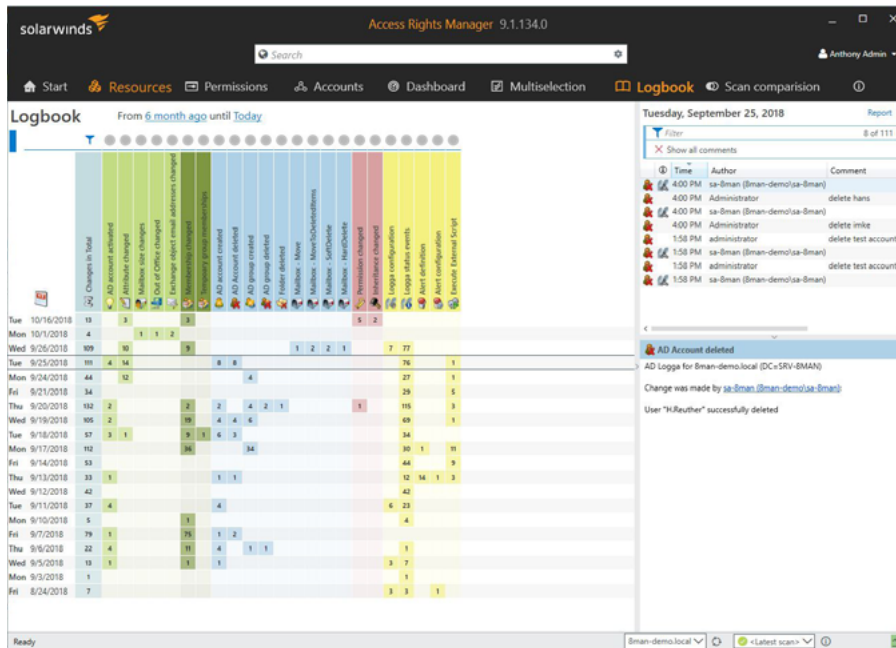
REPORTS

Easily configure your own Reports. Schedule them and let them automatically be sent to the people in charge.



LOGBOOK

See all changes in your system in an easy-to-comprehend calendar view. In the example, you have a list of all accounts deleted on Thursday, September 25. In the upper right corner, you see all accounts in a list.



COMMENT WINDOW

Easily document your changes. This way, you know the reason a change was made—even after years.

The screenshot shows the 'Change access rights' dialog box. The path is \\srv-8man\Organization\Marketing. The owner is Domain Admins (8man-demo\Domain Admins). The inheritance is set to On. The file server credentials are 8man-demo\sa-8man. The active directory change credentials are 8man-demo\sa-8man. The 'Access right changes' section shows a warning: 'Emily Employee (8man-demo\Emily Employee) already had the access right Modify.' The 'Group Wizard options' section includes a text input field with 'Ticket: A12RX54' and buttons for 'Immediately' and 'Close'.

LOGGING

Get instant knowledge about the activities in your sensitive directories. Choose the actions and the users you want to track, and get a report instantly.

The screenshot shows the 'Who did what?' configuration window. It has a dark header with a home icon and a close button. The main area is divided into two panels. The left panel, titled 'Report configuration', contains fields for 'Title' and 'Comment', a 'Reference period' dropdown set to 'Fixed time span 9/24/2018 3:19 PM - 9/26/2018 3:19 PM', a 'Resource' field with the path 'D:\Projects\Top Secret Project Z (SRV-SMAN)', and a 'Monitored actions' section with a placeholder text. Below this is an 'Authors' section with a placeholder text. At the bottom of the left panel is a 'Settings' section with a dropdown for 'The output format is PDF', a status for 'Report execution mode started manually', a status for 'Custom storage path is not configured', and a status for 'Send email is Deactivated'. The right panel, titled 'Who did what?', contains a 'Monitored actions' list with a filter input and a count of 6. The list includes: 'Directory / file created', 'Directory / file deleted', 'Directory / file moved or renamed', 'File read', 'File written', and 'Permission (ACL) changed'. At the bottom of the window are 'Start' and 'Cancel' buttons.

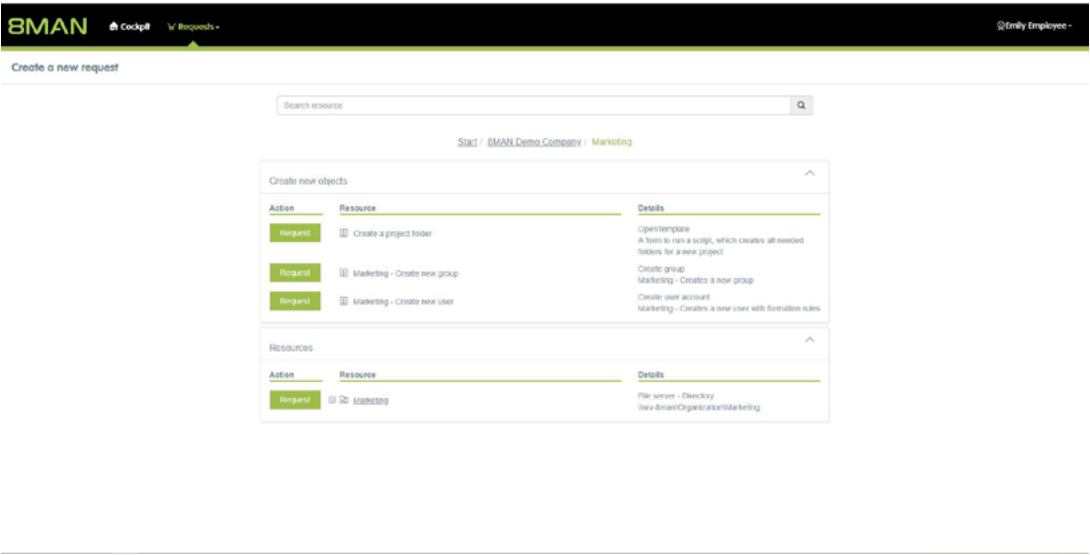
ALERTING

Easily create alerts for Active Directory & file server changes.

The screenshot shows the 'Edit alert' configuration window. It has a dark header with a home icon and a close button. Below the header is a subtitle: 'Edit an automatically executed alert for "Domain Admins (Bman-demo\Domain Admins)".'. The main area is a table with columns: 'ALERT NAME', 'EVENT', 'THRESHOLD', 'ACTIONS', and 'CATEGORY'. The first row shows: 'Group memberships changed' (with a green checkmark), a bell icon (with a green checkmark), a bell icon (with a green checkmark), a bell icon, and a dropdown set to 'Warning'. Below the table is a section titled 'DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT' with a bell icon. This section contains a 'Send email' checkbox (checked), a 'To' field with three email addresses, a 'Language' dropdown set to 'English', a 'Time zone' dropdown set to '(UTC) Coordinated Universal Time', and a 'Write to Windows event log' checkbox (unchecked). At the bottom is a 'Please add a comment' text area with a yellow warning icon, a user profile picture, and 'Apply' and 'Close' buttons.

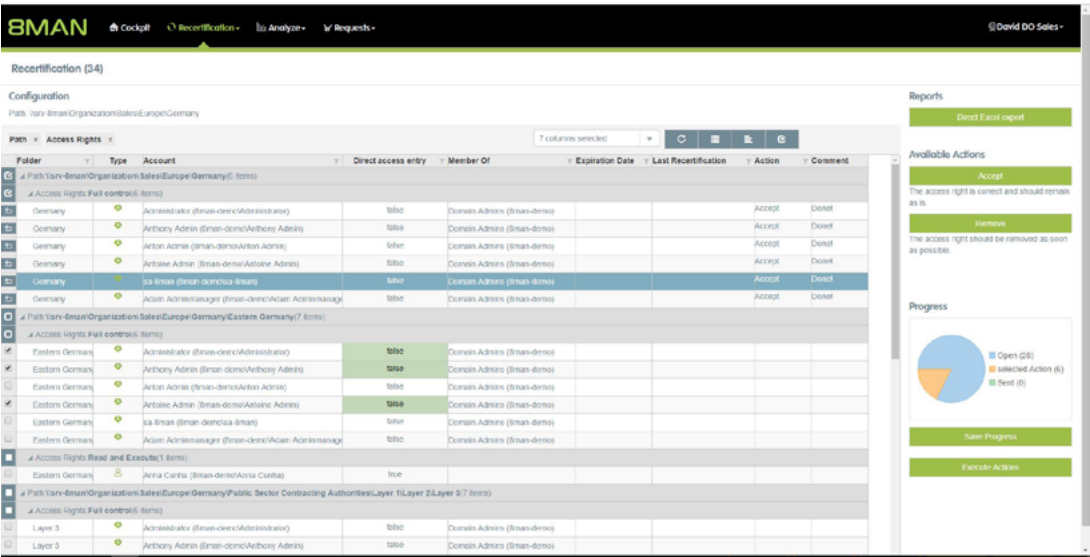
THE ARM SELF-SERVICE PORTAL

Employees simply order their access rights and further resources in the ARM Self-Service Portal.



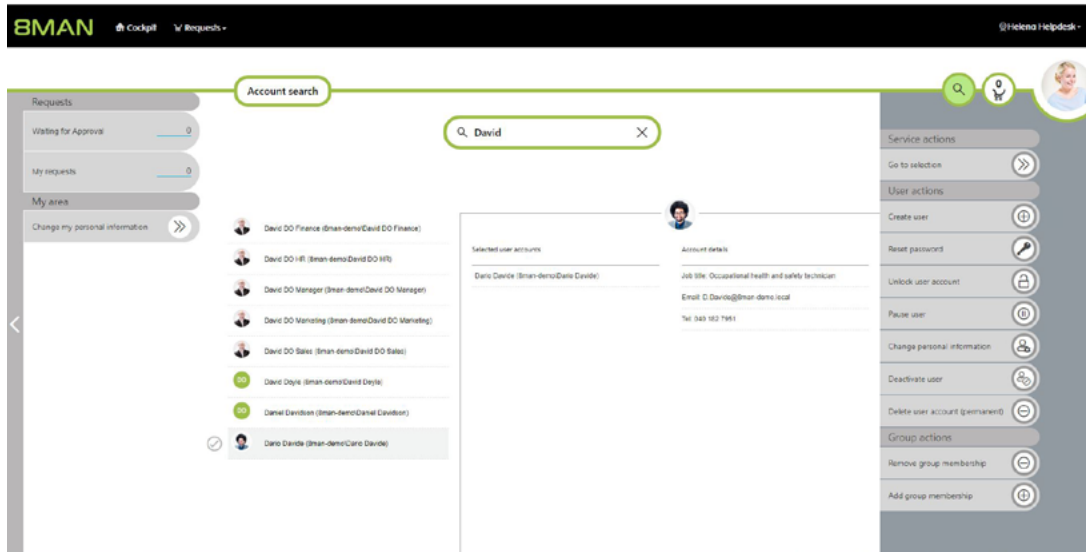
PERIODIC REVIEW OF ACCESS RIGHTS

Get a well-maintained access rights situation by letting the heads of every department check the permission status. A simple yes/no answer is enough, and changes are made automatically.



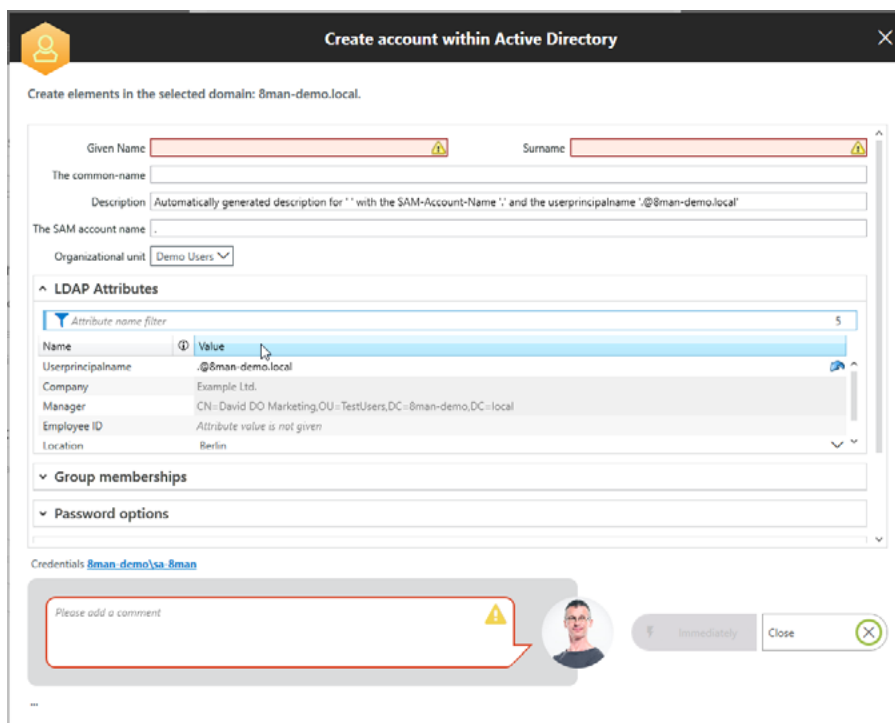
USER COCKPITS

Delegate standard operations to the help desk. The Agent works in a cockpit with limited access and actions to changeable resources.



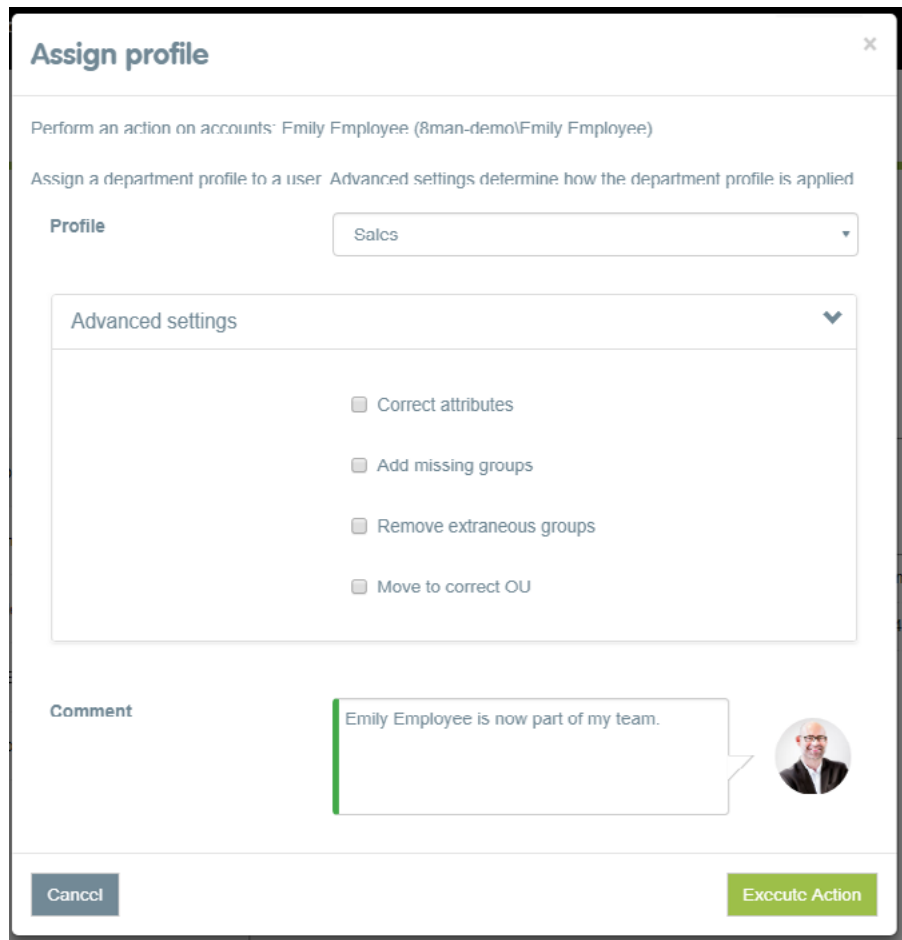
THE JOINER PROCESS

Predefine templates for all departments and thereby get coherent roles in your organization. The help desk only fills in the employee's master data. ARM will create the account and a mailbox automatically.



THE MOVER PROCESS

When an employee changes departments, it is an easy move for the new manager. The manager can easily assign the department profile, including all the basic permissions, to the employee.



Assign profile [X]


Perform an action on accounts: Emily Employee (8man-demo\Emily Employee)

Assign a department profile to a user. Advanced settings determine how the department profile is applied.

Profile Sales

Advanced settings [v]

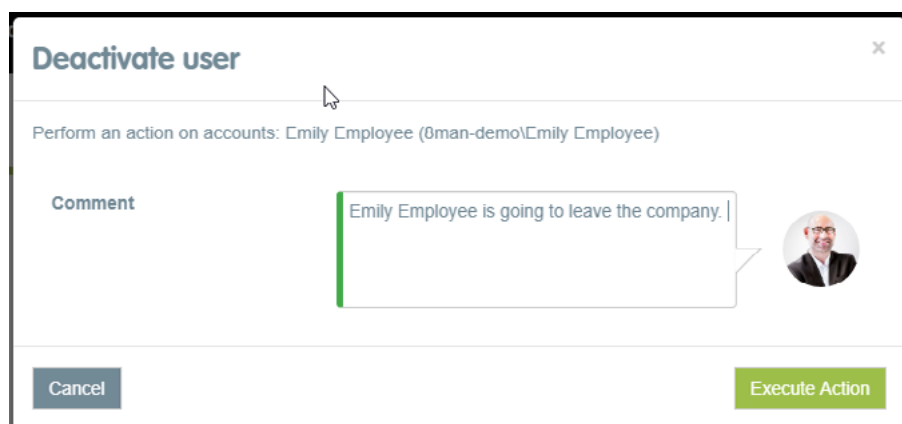
- ☐ Correct attributes
- ☐ Add missing groups
- ☐ Remove extraneous groups
- ☐ Move to correct OU

Comment Emily Employee is now part of my team. 

Cancel Execute Action


THE LEAVER PROCESS

If an employee leaves the company, deactivating the user account quickly is key. With ARM, the department lead can deactivate or pause the account easily.



Deactivate user [X]

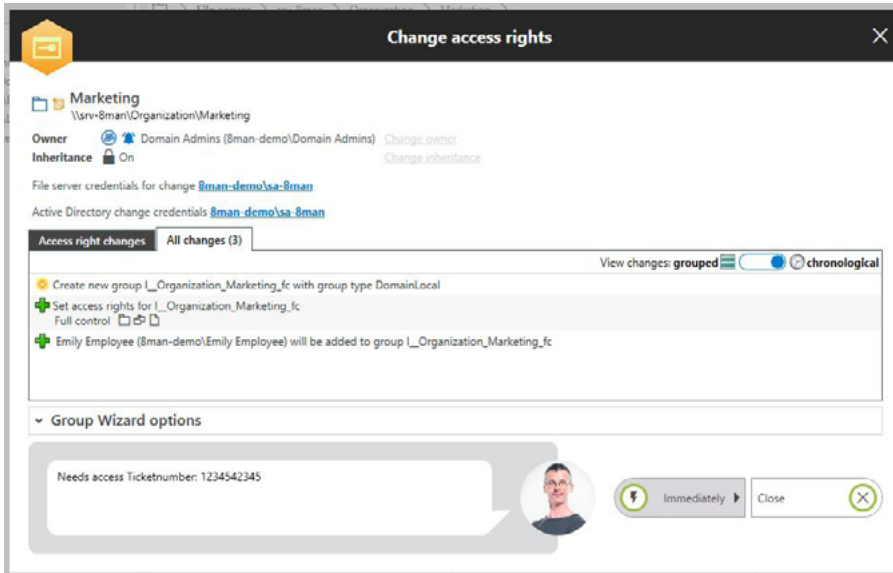
Perform an action on accounts: Emily Employee (8man-demo\Emily Employee)

Comment Emily Employee is going to leave the company. 

Cancel Execute Action

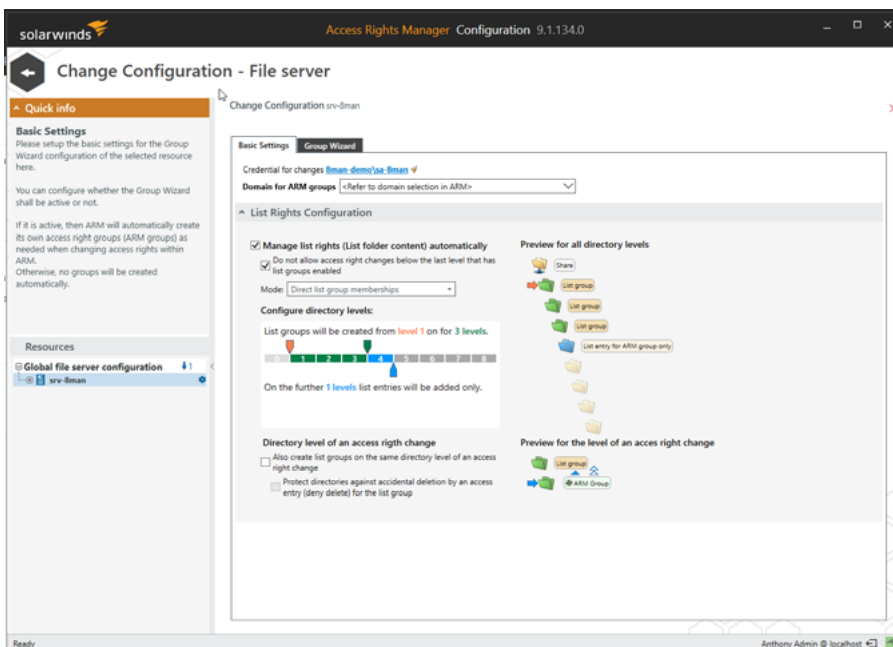
THE GROUP WIZARD

Give a user access in a simple drag-and-drop interface. The Group Wizard will create the needed AD Groups and list rights automatically.



AUTOMATIC LIST RIGHTS PROVISIONING

ARM builds list rights automatically according to your needs. This way, users can navigate to the folder they have access to.



SCHEDULED PROVISIONING

If you know the collaboration will only be temporary, just mark the expiration date of the account before it is even created.

The screenshot shows a 'Create account within Active Directory' window. At the top, it says 'Create elements in the selected domain: 8man-demo.local.' Below this, there are several sections: 'Group memberships' with a search bar and a list of groups; 'Password options'; 'User activation' with a date picker set to '11/17/2018 12:00 AM' and a 'Do not activate' option; 'Create an Exchange mailbox'; and 'Scripting'. At the bottom, there is a 'Credentials' field set to '8man-demo\sa-8man' and a 'Please add a comment' field. The window has a close button in the top right corner.

VALUE OF AN ACCESS RIGHTS MANAGEMENT SOLUTION

The benefits of an access rights management solution ultimately come down to:

- » Internal security
- » Compliance conformity
- » Cost savings

INTERNAL SECURITY

SolarWinds Access Rights Manager provides the tools for internal security. You can safeguard your most valuable capital: data, information, and knowledge.

COMPLIANCE CONFORMITY

A clear documentation of access rights is top priority for many regulations, such as GDPR, HIPAA, PCI DSS, ISO, or BSI. By implementing ARM, you can automatically implement standardized and transparent processes within your organization.

COST SAVINGS

Identifying, documenting, and provisioning access rights is a time-consuming task. By delegating ARM tasks to a help desk, administrators can focus on complex projects.

Through the self-service portal, all the work is done automatically, and it is no longer necessary to involve administrators or the help desk. The whole technical process is converted into a single management decision.



*For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx*

© 2018 SolarWinds Worldwide, LLC. All rights reserved.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.