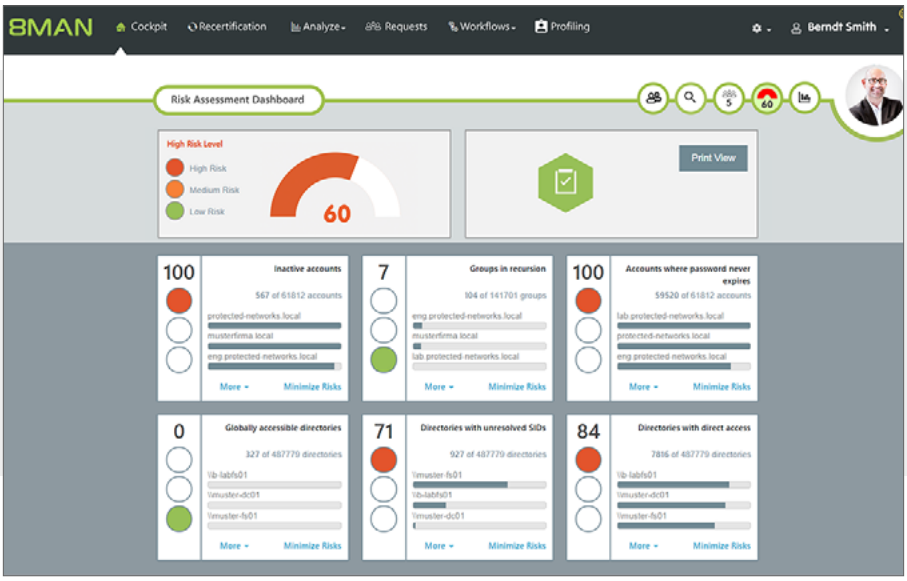
DATASHEET

solarwinds

Access Rights Manager

Manage and audit user access rights across your IT infrastructure



SolarWinds® Access Rights Manager (ARM) is designed to assist IT and security admins to quickly and easily provision, deprovision, manage and audit user access rights to systems, data, and files so they can help protect their organizations from the potential risks of data loss and data breaches. By analyzing user authorizations and access permission you get visualization of who has access to what and when they accessed it. With just a few clicks, customized reports can be generated to demonstrate compliance with most regulatory requirements. Provision and deprovision users using role-specific templates to help assure conformity of access privilege delegation in alignment with security policies.

ACCESS RIGHTS MANAGER BENEFITS AT-A-GLANCE

- Helps improve security posture and mitigate insider threats.
- Help demonstrate compliance with built-in customizable reports.
- Easily manage user permissions.
- Designed to enhance productivity.

FEATURES

Monitoring of Active Directory

Enhance security by monitoring, analyzing, and auditing Active Directory® and Group Policy to see what changes have been made, by whom, and when those changes occurred.

Auditing of Windows File Share

Help prevent data leaks and unauthorized changes to sensitive files and data through visualization of permissions on file servers.

Monitoring of Microsoft® Exchange

Simplify Exchange™ monitoring and auditing to help prevent data breaches. Track changes to mailboxes, mailbox folders, calendars, and public folders. Help improve compliance and detect unauthorized Exchange changes.

SharePoint™ access monitoring and management

Display SharePoint permissions in a tree structure and quickly see who is authorized to access a given SharePoint resource. Using the scan comparison report, you can find out who has made changes to permissions and what they were.

User Provisioning and Management

Set up and manage new user accounts generally in seconds with standardized role-specific templates that provide access to file servers, and Exchange.

User Permissions Analysis

Help protect from internal security threats by analyzing user access to services and file servers with visibility into group memberships from Active Directory and file servers.

Custom Report Generation

Create and generate management and auditor-ready reports that help demonstrate regulatory compliance showing user access rights in just a few clicks. Log activities in Active Directory and file servers by user.

Self-service Permissions Portal

Put access rights of data directly in the hands of the data owner instead of the administrator with a web-based, self-service permissions portal.

SERVER REQUIREMENTS	UP TO 1000 USERS	1001-4000 USERS	MORE THAN 4000 USERS
Hard Drive	30 GB	40 GB	40 GB
Memory	4 GB	8 GB	16 GB
CPU	Dual Core Processor or better		
Operating System	Microsoft Windows Server® 2008 SP1 (32- bit and 64-bit), 2008 R2, 2012, 2012 R2 and 2016.		
Databases	SQL Server® 2008 SP1, 2012, 2014, 2016 (32-bit and 64-bit).		
.NET Framework	.NET 3.5 SP1 and .NET 4.5.2 (or higher) is required.		
COLLECTOR REQUIREMENTS			
Hard Drive	5 GB		
CPU	Dual-core processor or better		
Memory	4 GB		
Operating System	Microsoft Windows Server 2008 SP1 (32- bit and 64-bit), 2008 R2, 2012, 2012 R2 and 2016.		
.NET Framework	.NET 3.5 SP1 and .NET 4.5.2 (or higher) is required.		