



ADMINISTRATOR GUIDE

# Access Rights Manager

Version 2019.4

© 2019 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

# Table of Contents

<b>Configuration</b> .....	<b>16</b>
Start the configuration application .....	16
Login .....	16
Advanced login options .....	18
Basic configuration .....	19
Enter ARM server credentials .....	19
Enter SQL server credentials .....	22
Identify the SQL server instance name .....	24
SQL Express 2017 and ARM .....	25
SQL Express integration .....	26
Switch database recovery mode .....	28
SQL Server database maintenance .....	28
Shrink database logs .....	29
Shrink database .....	30
Complete and save basic configuration .....	31
License and server status .....	33
Switch from an evaluation license to a production license .....	33
Online activation .....	37
Offline activation .....	40
Transfer a license to another server .....	46
Assign licenses to AD objects .....	47
Identify logged in users .....	53
Switch from 8MAN to SolarWinds licensing .....	54
Load the license file and check covered features .....	56
Collectors .....	58
Install additional collectors .....	60
Add collectors using setup .....	60
Add collectors or install via push method .....	63

Update collectors .....	66
Run collectors in foreign (non-trusted) domains .....	66
Remove collectors .....	67
Verify collector connection status .....	67
Perform a simple connection check .....	67
Test a connection to the collector with the browser .....	68
Configure scans and Logga .....	68
Active Directory (AD) scans .....	69
Add AD scans .....	69
Configure AD scans .....	71
AD change configuration .....	73
Load additional LDAP attributes .....	75
Customize AD attributes properties .....	80
Start AD scans .....	87
Delete AD scan configurations .....	88
File server (FS) scans .....	89
Add FS scans .....	89
Configure FS scans .....	94
Start FS scans .....	101
Delete FS scan configurations .....	102
Exchange scans .....	103
Prepare exchange scans .....	103
Configure Exchange scans .....	109
Advanced Exchange scan settings in the configuration files .....	116
SharePoint scans .....	120
Required accounts and permissions for a SharePoint scan .....	120
Add a SharePoint on-premise scan .....	121
Add a SharePoint Online scan .....	127
Configure additional properties .....	129
Customize a SharePoint scan configuration .....	138

SAP scans .....	138
Required accounts and permissions for an SAP scan .....	138
Add an SAP scan .....	139
Customize an SAP scan configuration .....	143
Configure additional SAP properties .....	144
Prepare Office 365 integration .....	146
Azure AD scans .....	159
Required accounts and permissions for an Azure AD scan .....	159
Add Azure AD scans .....	159
OneDrive scans .....	164
Required accounts and permissions for a OneDrive scan .....	165
Add OneDrive scans .....	165
Configure additional OneDrive scan properties .....	170
Configure AD Logga .....	171
Configure audit policies for the domain controllers (DC) .....	171
Set audit permissions in the AD object SACLs .....	181
Configure the Windows firewall for AD Logga .....	187
Add an AD Logga configuration .....	188
Activate or deactivate AD Logga .....	189
Customize an AD Logga configuration .....	190
Filter AD Logga events .....	190
Delete an AD Logga configuration .....	198
Configure the File Server (FS) Logga .....	199
Prepare Windows file servers .....	199
Prepare NetApp 7-mode file servers .....	201
Prepare NetApp clustered data ONTAP file servers .....	205
Prepare EMC file servers .....	213
Add a FS Logga configuration .....	220
Complete a FS Logga configuration .....	224
FS Logga settings in the pnTracer.config.xml file .....	238

Troubleshooting .....	242
Configure Exchange Logga .....	243
Add an Exchange Logga configuration .....	244
Customize an Exchange Logga configuration .....	245
Select the mailboxes to be monitored .....	246
Filter the Exchange Logga events .....	249
Enable or disable the Exchange Logga .....	252
Configure OneDrive Logga .....	252
Configure SharePoint Online Logga .....	258
Scan local accounts .....	264
Adding local accounts scans .....	265
Assign resources to a domain .....	266
Integrate Easy Connect resources .....	267
Alerts .....	270
Enable or disable alert sensors .....	271
Manage alerts .....	271
Manage ARM users .....	274
Add ARM users .....	275
Use groups as ARM users .....	276
Assign a role to ARM users .....	277
Define ARM user roles .....	278
Simplified rights management .....	280
Change configuration .....	281
Customize the Active Directory (AD) change configuration .....	282
Configuring new user default settings .....	283
Select available LDAP attributes .....	285
File Server (FS) change configuration .....	286
Manage global settings for FS changes .....	287
Basic settings .....	288
Set AD group types for the Group Wizard .....	293

Select access categories available in ARM .....	300
Define ARM group names .....	305
Blacklist - exclude users and groups from use .....	307
Apply a file server change configuration .....	313
Define file server and share specific change settings .....	313
Exchange change configuration .....	326
Create an Exchange change configuration .....	326
Customize an Exchange change configuration .....	328
Delete an Exchange change configuration .....	332
SharePoint change configuration .....	333
Add a SharePoint change configuration .....	334
Modify a SharePoint change configuration .....	335
Delete a SharePoint change configuration .....	339
Azure Active Directory (AAD) change configuration .....	340
Add an AAD change configuration .....	341
Modify an AAD change configuration .....	342
Delete an AAD change configuration .....	343
OneDrive change configuration .....	344
Add a OneDrive change configuration .....	345
Modify a OneDrive change configuration .....	346
Delete a OneDrive change configuration .....	347
Data owner .....	348
Create organizational categories .....	349
Assign a Data Owner to an organizational category .....	352
Assign resources to an organizational category .....	355
Assign specific group wizard settings to organizational categories .....	358
Activate or deactivate simple approvals for Data Owners .....	359
Data Owner configuration and GrantMA .....	362
Import or export Data Owner configurations .....	365
Create a Data Owner configuration report .....	366

Server .....	368
Configure the web client URL .....	368
Set the display duration for comment icons .....	369
Configure email settings .....	370
Configure storage of scans settings .....	373
Determine server thresholds .....	379
Display the server health check .....	384
Server event logging .....	385
Determine the logging level .....	385
Retrieve ARM log files .....	385
Logfile types .....	387
Set Syslog servers .....	388
Scripting .....	389
Configure scripts .....	389
DEEP DIVE: Pass parameters to a script via JSON or CSV .....	398
Disable a user via GrantMA .....	399
Pass parameters to a script via JSON or CSV .....	408
Jobs overview .....	413
Display jobs grouped by status .....	415
Display jobs grouped by category .....	416
Configure and view reports .....	417
Configure report options .....	418
Configure the blacklist for views and reports .....	419
Open Order .....	421
Define the requestable technologies and resources .....	421
Set technology .....	423
Define resources .....	425
Predefined icons .....	427
Descriptions .....	428
Validate an XML configuration file .....	429



Integrate Open Order templates in GrantMA .....	431
Enter the template's call into the XML resource configuration .....	431
Upload an XML resource configuraton to the Data Owner configuration .....	433
Set the Open Order resource to requestable .....	435
Configure web components .....	438
Generate a self-signed certificate .....	441
Bind a certificate to a site .....	443
Configuration in the web client .....	446
Set analyze options .....	446
Configure recertifications .....	447
Activate and deactivate recertifications .....	447
Deadlines and intervals .....	448
Activate recertifications in the Data Owner configuration .....	449
Customize notification emails .....	450
Test notification emails for recertification .....	451
Configure display settings .....	453
GrantMA settings .....	454
Resource owners .....	457
Activate the Resource Owner feature .....	457
Assign resource owners using the web client .....	458
Import or export resource owner configurations .....	462
<b>Using ARM .....</b>	<b>468</b>
Permission analysis .....	468
Cross-resource .....	468
Identify the permissions of a user .....	468
Identify access rights on a resource .....	472
Identify multiple access paths .....	475
Identify deviating access rights in the tree structure .....	477
Analyze historical access rights situations .....	480
Compare two different access rights situations (Scan Comparison) .....	482

Get an overview of the environment in the Web Dashboard .....	486
Determine permissions deviating from the department profile (compliance check) (web client)	492
Active Directory .....	496
Visualize nested group structures .....	496
Identify overprivileged users based on Kerberos token size .....	499
Identify the depth of group nesting .....	501
View members of different groups in one list .....	503
Identify empty groups .....	504
Identify recursive groups .....	506
Identify recursive groups (web client) .....	510
Identify users with never expiring passwords .....	513
Identify users with never expiring password (web client) .....	516
Identify inactive accounts (web client) .....	519
Identify expiring user accounts .....	522
Identify the most recent actions on an account .....	524
File server .....	528
Identify globally accessible directories (web client) .....	528
Identify corrupted inheritance .....	531
Identify folders with special protection .....	534
Identify the latest activities on a directory .....	537
Identify share permissions .....	540
Exchange .....	542
Identify access rights on mailboxes .....	542
Identify mailbox properties .....	544
Identify access rights on public folders .....	546
Identify permissions on distribution groups .....	548
Identify members of distribution groups .....	550
OneDrive .....	553
Identify shared directories and files on OneDrive .....	553
Documentation & Reporting .....	556

Cross-resource .....	556
Report: Who has access where? .....	556
Flexible reports (web client) .....	563
Where do users and groups have access? .....	566
Report on ARM Access Rights Management activities (Logbook report) .....	568
Active Directory .....	570
Employees of a manager .....	570
Group memberships and account details .....	573
Find inactive accounts (users or computers) .....	576
OU members and group memberships .....	580
Users and groups report .....	582
Report on local accounts .....	587
Organizational help for administrators .....	589
File server .....	596
Where do employees of a manager have access? .....	596
Who has access through which permission groups? .....	598
Report on direct permissions .....	602
Report on unresolved SIDs .....	605
Report on the usage of "everyone" .....	608
Report on the usage of "Authenticated Users" .....	612
Report on directories whose owners are not administrators .....	614
Permission differences .....	617
Exchange .....	619
Report on mailbox permissions .....	619
Who has access to what in Exchange? .....	622
OneDrive .....	624
Create a report about directories and files shared on OneDrive .....	624
Security Monitoring .....	627
Cross-resource .....	628
Manage alerts .....	628

Active Directory Logga .....	630
Analyze AD Logga events with the logbook .....	631
Report on changes in Active Directory .....	634
Report on temporary group memberships .....	640
Report on locked user accounts .....	642
Report on password resets .....	644
Set alerts for groups .....	646
Set alerts for user accounts .....	652
Set alerts for OUs/domains .....	658
File Server Logga .....	665
Monitor access to sensitive file server data .....	665
Enable alerts for file server directories .....	669
Enable alerts for suspected data theft (file server) .....	677
Enable alerts for data deletion (file server) .....	687
Enable alerts for suspected cases on ransomware on file servers .....	696
Exchange Logga .....	705
View activities in mailboxes, calendars, and contacts in logbook .....	705
Report activities on mailboxes, calendars, and contacts .....	708
OneDrive Logga: Report activities on OneDrive .....	711
SharePoint Online Logga: Report activities on SharePoint Online .....	714
Role & Process Optimization .....	717
Delegation of tasks .....	717
Apply an ARM account to a specific security role or data owner .....	718
Assign the administration of access rights to a Data Owner .....	723
Delegate user provisioning processes to help desk .....	727
Create approval processes .....	729
The simple authorization process - approving and rejecting actions as an administrator .....	729
GrantMA: Design approval processes .....	733
Data Owner: Recertification of existing access rights .....	741
Email notifications for recertification .....	745

ARM GrantMA: workflows for employees .....	746
Manage my requests (cockpit) .....	746
Request file server access rights .....	748
Request group memberships .....	756
Request directories .....	762
Create a user account as an HR employee .....	765
Order script-based services .....	771
ARM GrantMA: workflows for data owner/administrators .....	775
Approve or reject requests (cockpit) .....	775
Inform approvers of new requests via email .....	779
User Provisioning .....	780
Active Directory .....	781
Administrator .....	781
Helpdesk .....	846
Data Owner/Manager .....	865
File server .....	893
Grant and remove file server access rights .....	893
Remove multiple access paths to file server directories .....	898
Create a protected file server directory .....	905
Remove direct permissions .....	913
Remove direct permissions in bulk (web client) .....	916
Remove corrupted inheritance .....	920
Identify errors in inheritance and fix them in bulk (web client) .....	925
Identify and delete unresolved SIDs .....	928
Remove unresolved SIDs in bulk (web client) .....	933
Remove "everyone" permissions in bulk (web client) .....	936
Change directory ownership .....	939
Exchange .....	941
Create a mailbox (email enable accounts) .....	941
Create a mailbox in Exchange Online (assign an Office 365 license) .....	944

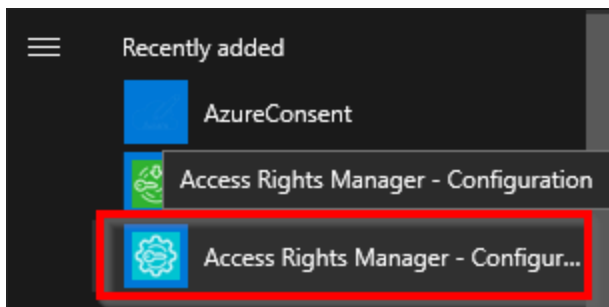
Change mailbox permissions .....	947
Manage out of office notices .....	951
Manage mailbox and email size .....	954
Manage email addresses .....	957
Manage distribution group memberships .....	960
Manage distribution group permissions .....	963
Modify moderation of distribution groups .....	967
Change the manager of distribution groups .....	970
Create and delete contacts .....	973
SharePoint .....	975
Manage SharePoint permissions .....	975
Create SharePoint groups .....	975
<b>Customize ARM templates .....</b>	<b>981</b>
Take advantage of customized templates .....	981
Load templates in ARM .....	982
Edit and name templates .....	984
All templates - the header of the template .....	984
Availability of input types .....	985
Basic structure of an input option .....	986
Frequent properties .....	986
Constraints .....	988
Multilanguage templates .....	989
Creation rules .....	990
Hide input fields .....	996
TextField .....	997
TextArea .....	998
MultiValue Text .....	998
DropDownList .....	999
FixedValue .....	1000
Checkbox .....	1001

Customize templates for new users .....	1001
Enter Name and OU .....	1002
Enter additional LDAP attributes .....	1004
Assign group memberships .....	1005
Run an external program .....	1006
Enter password options .....	1007
Activation options .....	1009
Create an Exchange mailbox .....	1010
Customize templates for new groups .....	1016
Preset group options (group type/scope) .....	1016
Preset group members .....	1018
Enable email (create distribution group) in Exchange .....	1019
Customize templates for new contacts .....	1021
Make templates for users/groups/contacts available in the Web client .....	1023
Open order templates .....	1025
Structure of an Open Order template .....	1026
Create an input option .....	1027
Specific Open Order input options .....	1027
AccountSearchTextField .....	1027
Radio Buttons .....	1029
Include open order templates in the ARM GrantMA .....	1030
Enter the template's call into the XML resource configuration .....	1031
Upload an XML resource configuration to the Data Owner configuration .....	1032
Set the open order resource to requestable .....	1034

# Configuration

This section provides detailed information on configuring ARM.

## Start the configuration application



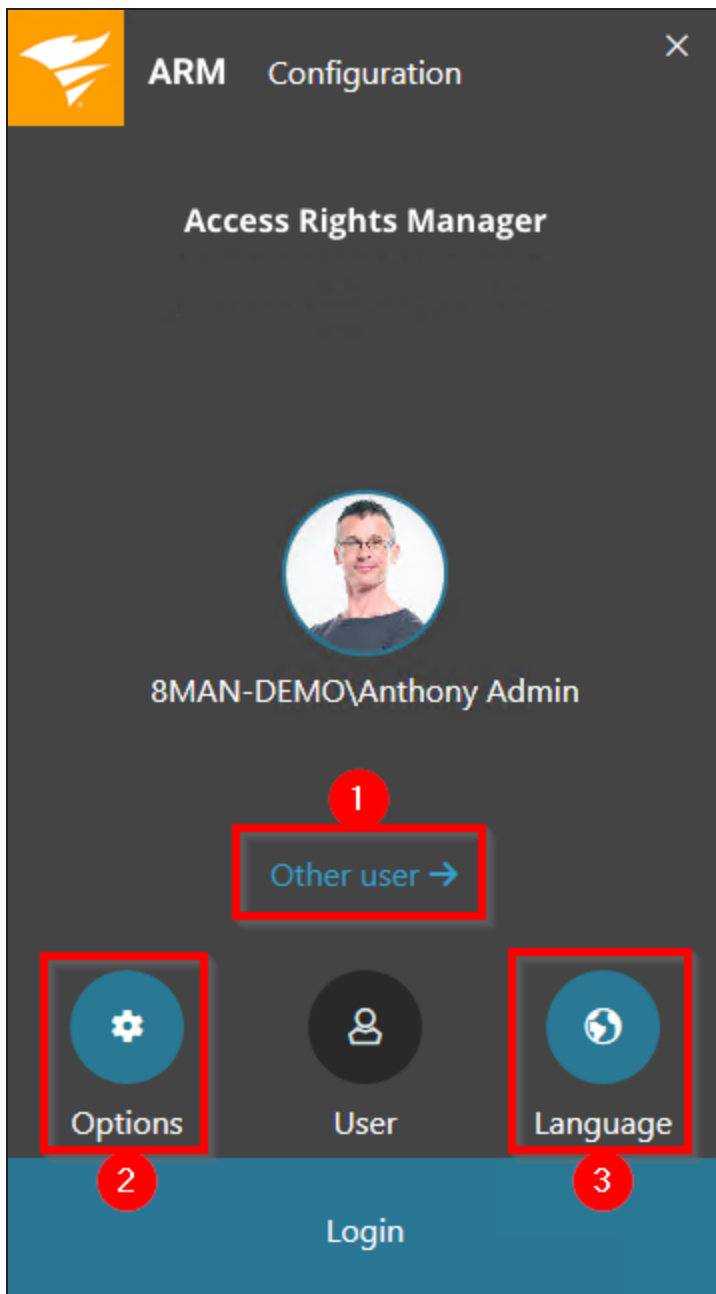
Start the configuration module.

## Login

After a new installation, there is only one user who can log into ARM: the user who performed the installation.

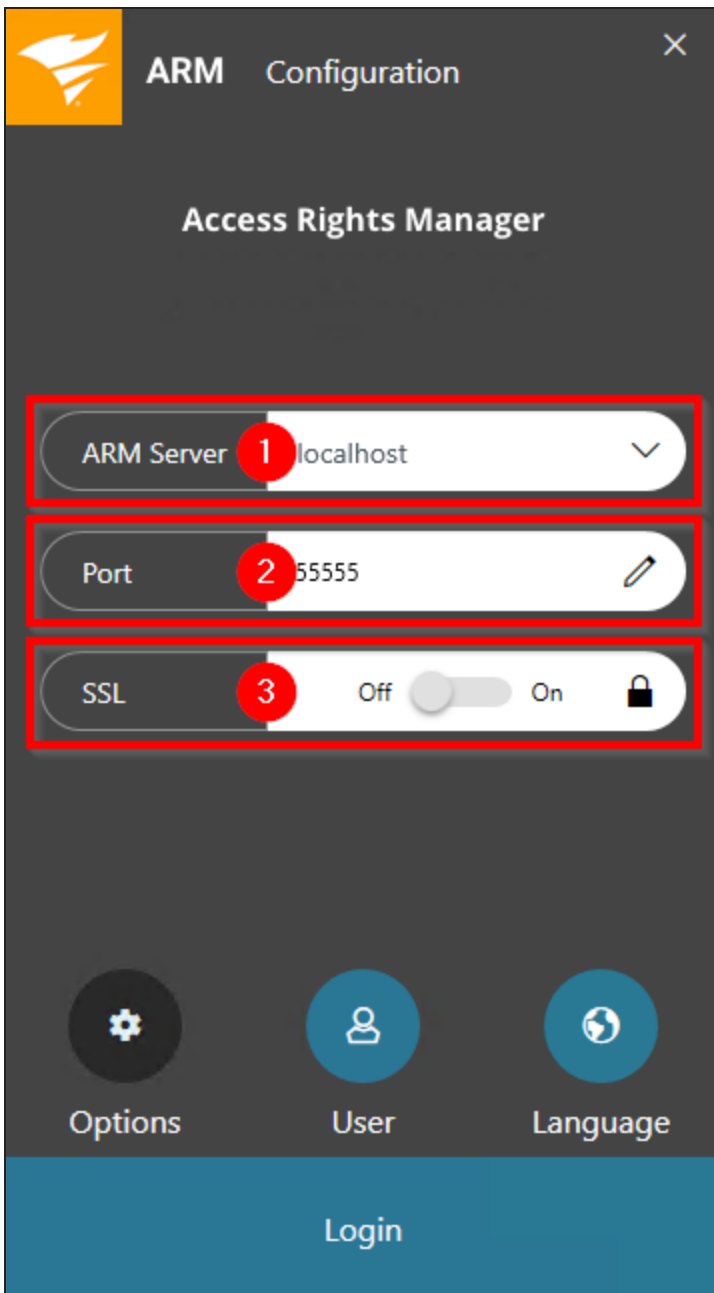
 More information on adding ARM users can be found at [ARM user management](#).





1. If additional users have already been added you can use their credentials.
2. Switch to advanced login options.
3. Change the language of the user interface. Available languages are English, German and French.

## Advanced login options



1. Enter the name of the ARM server, for example "srv-ARM" (without "\\"). If working locally on the ARM server you may also use "localhost". It is also possible to reference an IP address.
2. By default, the communication between ARM server and GUI uses port 55555. Please also refer to the chapter on [firewall settings](#). If you want to change the port please see the knowledge base article: [Configure ARM client apps to use a custom port](#).
3. If you activate the SSL option, all communication between ARM server and GUI will be encrypted. Encryption must be configured first. Please see the following knowledge base article: [How to enable SSL encryption](#).

## Basic configuration

In the basic configuration, you specify which credentials the ARM service uses to request the Active Directory.


ARM requires an SQL database to store data. In the basic configuration you specify:

- SQL Server Name
- SQL Server Instance
- SQL Server authentication method and credentials

Select Basic Configuration on the ARM configuration application start page.

## Enter ARM server credentials

The ARM server is a service that runs with local permissions. The ARM server requires credentials to log on to Active Directory and the SQL server (if Windows authentication is used).

 The Active Directory credentials are proposed by default for newly created scan configurations.

ARM Access Rights Manager Configuration

## Basic Configuration

**ARM Server**  
Credentials for Active Directory and SQL Server access

User name: sa-8man

Password: ••••••

Domain: 8MAN-DEMO

**SQL Server**

SQL Server name: localhost

SQL Server instance: SQLEXPRESS

SQL Database name: \_8ManDB

Suggested recovery mode: Simple

Use Integrated Security (Windows Authentication)

SQL Server user name: \_\_\_\_\_

SQL Server password: \_\_\_\_\_

**Configuration Status**

- ARM Server credentials: Test not yet executed!
- SQL Server settings: Test not yet executed!

**Complete configuration**  
Configuration successfully loaded!

Ready Anthonyv Admin @ 127.0.0.1

Enter the login credentials for Active Directory.

SolarWinds recommends the use of [service accounts](#).

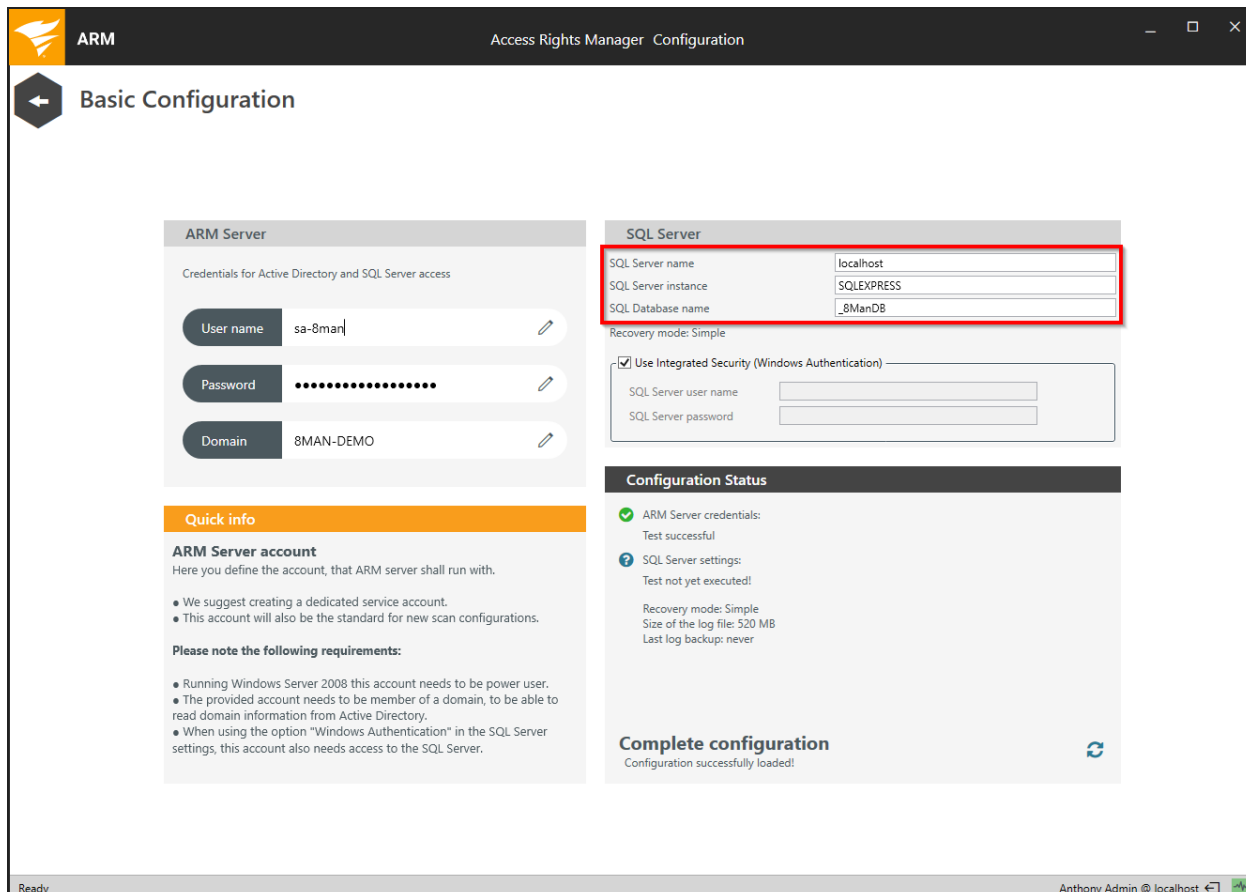
The screenshot displays the 'Basic Configuration' window in the Access Rights Manager (ARM) application. The window is titled 'ARM Access Rights Manager Configuration' and features a navigation pane on the left with a back arrow and the text 'Basic Configuration'. The main content area is divided into several sections:

- ARM Server:** A section for configuring credentials for Active Directory and SQL Server access. It includes three input fields: 'User name' (sa-8man), 'Password' (masked with dots), and 'Domain' (8MAN-DEMO).
- SQL Server:** A section for configuring SQL Server settings. It includes input fields for 'SQL Server name' (localhost), 'SQL Server instance' (SQLEXPRESS), and 'SQL Database name' (\_8ManDB). The 'Recovery mode' is set to 'Simple'. A checkbox for 'Use Integrated Security (Windows Authentication)' is checked, with corresponding empty input fields for 'SQL Server user name' and 'SQL Server password'.
- Configuration Status:** A section showing the results of the configuration tests. A red box highlights the 'ARM Server credentials: Test successful' message. Below it, the 'SQL Server settings: Test not yet executed!' message is shown. Additional details for SQL Server settings include 'Recovery mode: Simple', 'Size of the log file: 520 MB', and 'Last log backup: never'.
- Complete configuration:** A section at the bottom right with a blue refresh icon and the text 'Configuration successfully loaded!'.

The Windows taskbar at the bottom shows the system is 'Ready' and the user is 'Anthony Admin @ localhost'.

If valid credentials are entered, ARM will display the message "Test successful". Successful means that the credentials are valid for Active Directory login.

## Enter SQL server credentials



The screenshot shows the 'Basic Configuration' window of the Access Rights Manager (ARM). The 'SQL Server' section is highlighted with a red box, showing the following fields:

Field	Value
SQL Server name	localhost
SQL Server instance	SQLEXPRESS
SQL Database name	8ManDB

Below the 'SQL Server' section, the 'Configuration Status' shows:

- ARM Server credentials: Test successful
- SQL Server settings: Test not yet executed!

Recovery mode: Simple  
Size of the log file: 520 MB  
Last log backup: never

**Complete configuration**  
Configuration successfully loaded!

Enter the SQL server name, the name of the instance and the data base (no spaces allowed). Please note additional information to the [SQL instance name](#).

**i** By default, the simple recovery mode (recommended) is configured for the ARM data base. Switching to the full recovery mode is only possible once the initial configuration has been completed (also see: [switch data base recovery mode](#)).

The screenshot displays the 'Basic Configuration' window for the Access Rights Manager (ARM). It is divided into several sections:

- ARM Server:** Contains fields for 'User name' (sa-8man), 'Password' (masked), and 'Domain' (8MAN-DEMO).
- SQL Server:** Contains fields for 'SQL Server name' (localhost), 'SQL Server instance' (SQLEXPRESS), and 'SQL Database name' (\_8ManDB). Below these is a checkbox for 'Use Integrated Security (Windows Authentication)' which is checked and highlighted with a red box. Underneath are fields for 'SQL Server user name' and 'SQL Server password'.
- Quick info:** Provides information about the 'ARM Server account' and lists requirements for the account, such as being a power user or domain member.
- Configuration Status:** Shows a green checkmark for 'ARM Server credentials: Test successful' and a question mark for 'SQL Server settings: Test not yet executed!'. It also lists 'Recovery mode: Simple', 'Size of the log file: 520 MB', and 'Last log backup: never'.
- Complete configuration:** A button to save the configuration, with the text 'Configuration successfully loaded!' below it.

Specify the type of logon to the SQL server.

### Option enabled

Windows authentication is used with the credentials of the ARM server (on the left-hand side)

### Option disabled

SQL server authentication is used. Enter user name and password to log into the SQL server.

Please refer to the notes on the use of [service accounts](#).

**ARM Server**

Credentials for Active Directory and SQL Server access

User name: sa-8man

Password: [Redacted]

Domain: 8MAN-DEMO

**SQL Server**

SQL Server name: localhost

SQL Server instance: SQLSERVER

SQL Database name: \_8ManDB

Recovery mode: Simple

Use Integrated Security (Windows Authentication)

SQL Server user name: [Redacted]

SQL Server password: [Redacted]

**Configuration Status**

- ARM Server credentials: Test successful
- SQL Server settings: Test successful

Recovery mode: Simple  
Size of the log file: 520 MB  
Last log backup: never

**Complete configuration**  
Configuration successfully loaded!

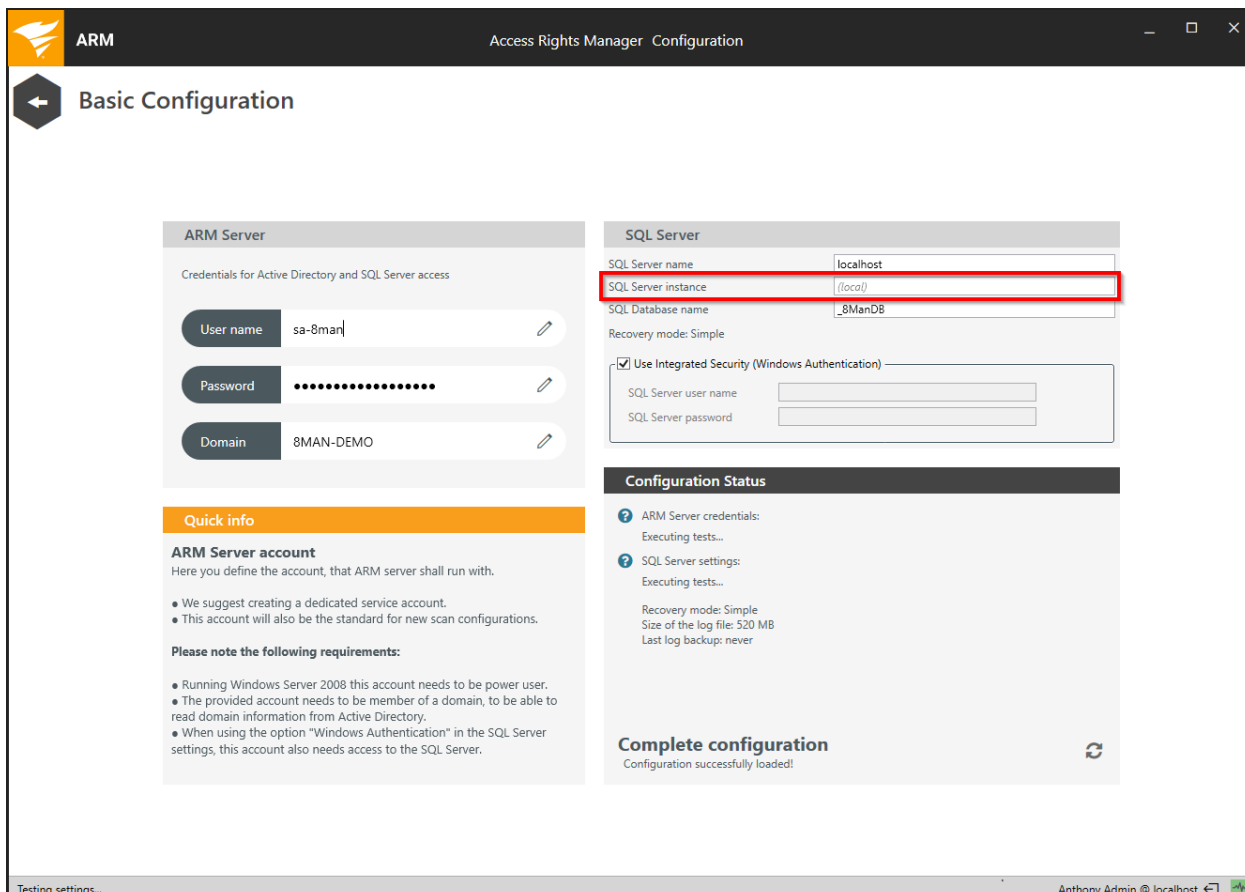
1. Click the button to verify the connection to the SQL server.
2. If valid credentials have been entered, ARM displays the message "Test successful".

## Identify the SQL server instance name

Name	Description	Status	Startup Type	Log On As
SNMP Trap	Receives trap messag...	Stopped	Manual	Local Service
Software Protection	Enables the download...	Running	Automatic (Delayed Start, Trigger Start)	Network S...
Special Administration Console Helper	Allows administrators...	Running	Manual	Local Syste...
Spot Verifier	Verifies potential file s...	Stopped	Manual (Trigger Start)	Local Syste...
SQL Service (MSSQLSERVER)	Provides storage, pro...	Running	Automatic	NT Service...
SQL Server Agent (MSSQLSERVER)	Executes jobs, monito...	Running	Manual	NT Service...
SQL Server Browser	Provides SQL Server c...	Running	Automatic	Local Service
SQL Server VSS Writer	Provides the interface...	Running	Automatic	Local Syste...
SSDP Discovery	Discovers networked ...	Stopped	Disabled	Local Service
Still Image Acquisition Events	Launches application...	Stopped	Manual	Local Syste...
Storage Tiers Management	Optimizes the placem...	Running	Manual	Local Syste...
Superfetch	Maintains and improv...	Running	Manual	Local Syste...
System Event Notification Service	Monitors system even...	Running	Automatic	Local Syste...
System Events Broker	Coordinates executio...	Running	Automatic (Trigger Start)	Local Syste...
Task Scheduler	Enables a user to conf...	Running	Automatic	Local Syste...
TCP/IP NetBIOS Helper	Provides support for t...	Running	Automatic (Trigger Start)	Local Service

The instance name can be identified by using the services console:



**EXCEPTION:**

A standard SQL server (or higher) can be installed without assigning an instance name. This is then displayed in the Services Console as "SQL Server (MSSQLSERVER)". In this case, the SQL Server Instance field must remain empty. The word "(local)" is displayed in gray as a placeholder.

## SQL Express 2017 and ARM

Microsoft SQL-Server Express Edition 2017 has the following limitations:

- 10 GB maximum data base size -> only a limited number of scans can be stored
- ca. 1.4 GB maximum RAM use -> poor performance in large environments
- 4 cores maximum -> poor performance in large environments

ARM allows you to configure your settings in order to optimize data storage:

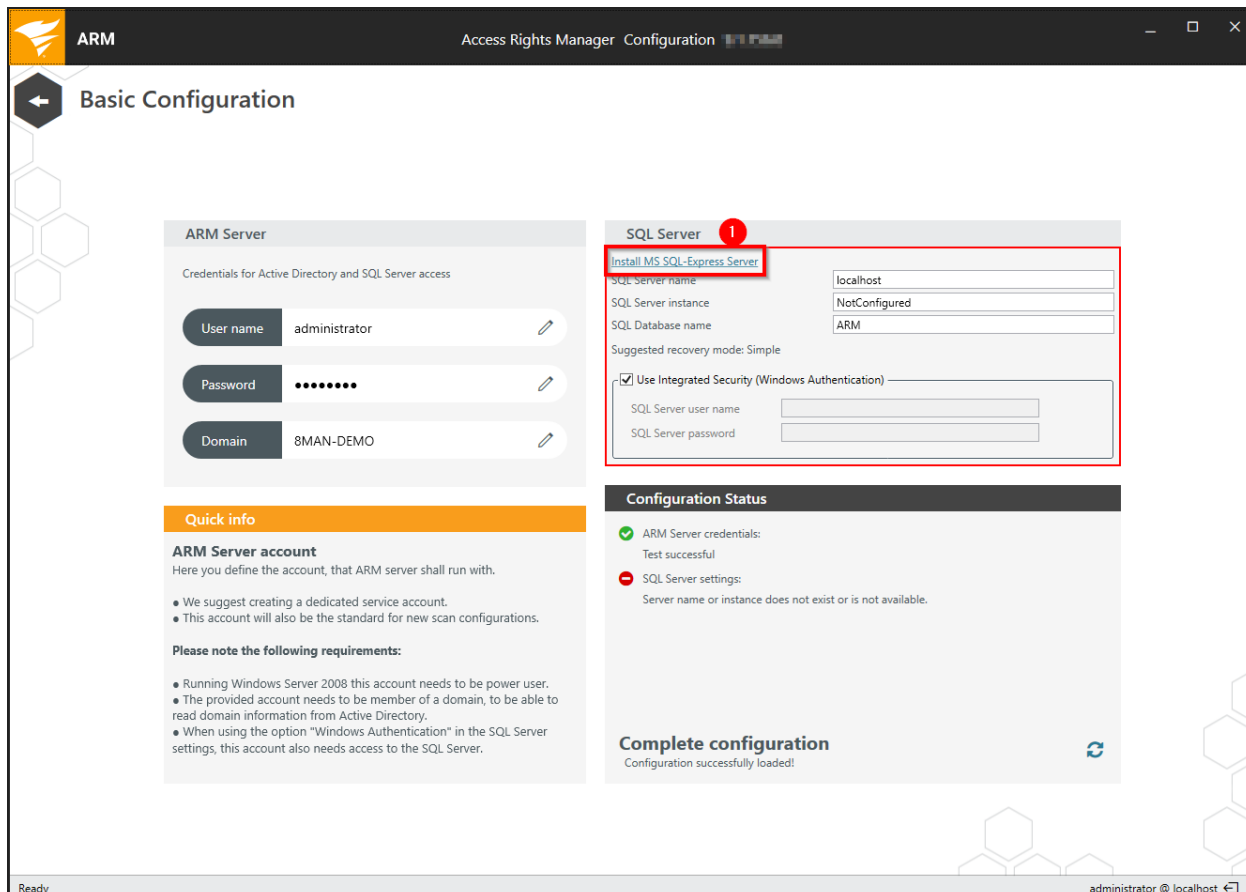
Information on actual data base size can be found in the [Server health check](#).

Details on reducing data base size can be found in the following topics: [storage of scans](#) and [SQL-Server data base maintenance](#).

You can find additional information in the article [Available SQL Server 2017 editions](https://www.microsoft.com/en-us/sql-server/sql-server-2017-editions). (© 2020 Microsoft, <https://www.microsoft.com/en-us/sql-server/sql-server-2017-editions>, obtained on January 29, 2020).

## SQL Express integration

For a simpler installation, especially for evaluation purposes, you can perform a SQL Express installation directly from the basic configuration. All necessary SQL logins are automatically generated and entered into the ARM basic configuration.



The screenshot displays the 'Basic Configuration' window for the Access Rights Manager (ARM). The window is titled 'ARM Configuration' and shows the following sections:

- ARM Server:** Credentials for Active Directory and SQL Server access. Fields include User name (administrator), Password (masked), and Domain (8MAN-DEMO).
- SQL Server:** Configuration for the SQL Server instance. Fields include SQL Server name (localhost), SQL Server instance (NotConfigured), and SQL Database name (ARM). A red box highlights the 'SQL Server' section, and a red circle with the number '1' is placed above the 'Install MS SQL-Express Server' link.
- Configuration Status:** Shows the status of the configuration. A green checkmark indicates 'ARM Server credentials: Test successful'. A red minus sign indicates 'SQL Server settings: Server name or instance does not exist or is not available'.
- Complete configuration:** A button labeled 'Complete configuration' with a refresh icon, and a message 'Configuration successfully loaded!'.

Click on the link to perform an SQL Express installation on the ARM server.

The screenshot shows the 'Basic Configuration' window for ARM. The 'SQL Server' section is highlighted with a red box, showing the following settings:

- SQL Server name: localhost
- SQL Server instance: SOLARWINDS\_ARM
- SQL Database name: ARM
- Suggested recovery mode: Simple
- Use Integrated Security (Windows Authentication)
- SQL Server user name: ARMService
- SQL Server password: [Redacted]

The 'Configuration Status' section shows two successful tests:

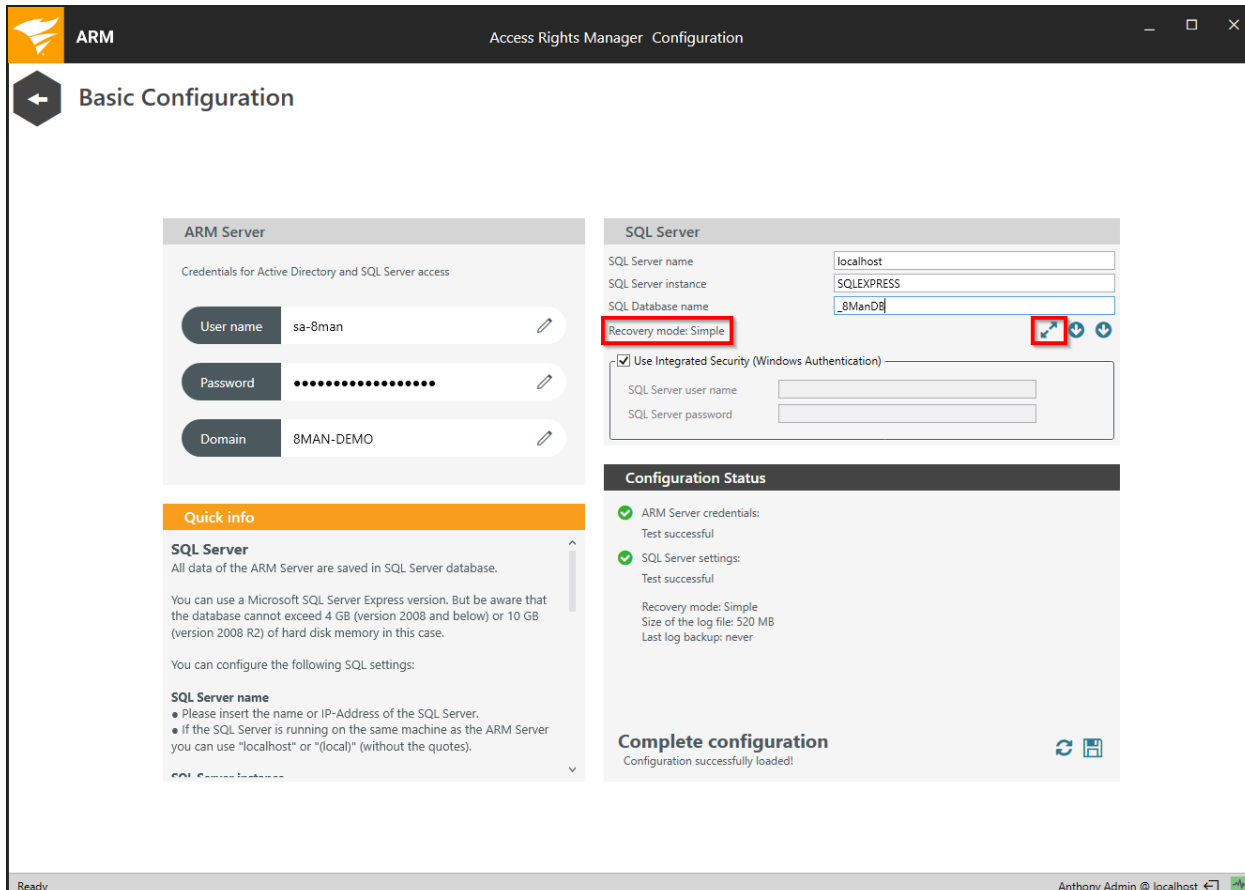
- ARM Server credentials: Test successful
- SQL Server settings: Test successful

The 'Complete configuration' section indicates 'Configuration successfully loaded!' with a refresh and save icon.

After successful installation of SQL Express, the required credentials are already entered.

**i** The administrator who performs the installation is the owner of the SQL Express instance. You can use the administrator's credentials to log on to the instance.


## Switch database recovery mode




The screenshot shows the 'Basic Configuration' page for the Access Rights Manager. It is divided into several sections:

- ARM Server:** Contains fields for 'User name' (sa-8man), 'Password', and 'Domain' (8MAN-DEMO).
- SQL Server:** Contains fields for 'SQL Server name' (localhost), 'SQL Server instance' (SQLEXPRESS), and 'SQL Database name' (8ManDB). The 'Recovery mode: Simple' dropdown is highlighted with a red box, and a 'Change' button next to it is also highlighted with a red box.
- Configuration Status:** Shows two green checkmarks indicating successful tests for 'ARM Server credentials' and 'SQL Server settings'. Below this, it lists the current settings: 'Recovery mode: Simple', 'Size of the log file: 520 MB', and 'Last log backup: never'.
- Complete configuration:** A message at the bottom right states 'Configuration successfully loaded!' with a refresh icon.

The recovery mode can only be changed after the initial configuration has been completed and the message "Test successful" has been displayed. You can switch the recovery mode from "simple" to "full" and back again.

 The simple mode is strongly recommended.

The change is performed immediately after clicking the "Change button". You do not need to save the configuration again.

 For more information about recovery mode, see the article [Recovery Models \(SQL Server\)](https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/recovery-models-sql-server?view=sql-server-2017). (© 2020 Microsoft, <https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/recovery-models-sql-server?view=sql-server-2017>, obtained on January 29, 2020)

## SQL Server database maintenance

Every morning at 5 am the ARM server completes scheduled maintenance by removing and archiving old scans from the ARM data base. These settings can be managed in the menu item server in the [storage of scans](#) section.

Scheduled data base maintenance is only performed if all ARM user interfaces are closed. You can [identify logged in users](#) in the menu item server status.

## Shrink database logs

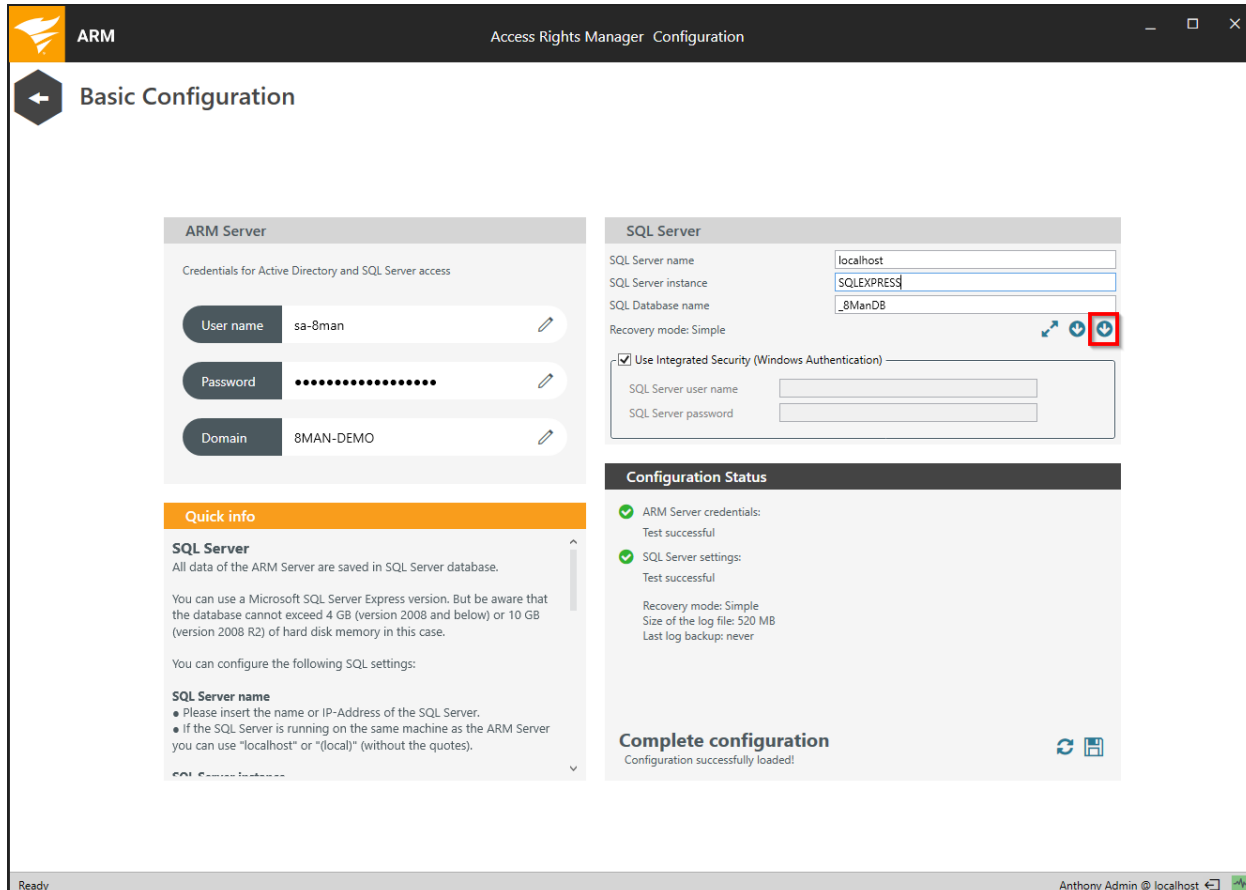
The screenshot shows the 'Basic Configuration' window in the Access Rights Manager (ARM) application. The window is titled 'ARM Access Rights Manager Configuration'. It is divided into several sections:

- ARM Server:** Contains fields for 'User name' (sa-8man), 'Password', and 'Domain' (8MAN-DEMO).
- SQL Server:** Contains fields for 'SQL Server name' (localhost), 'SQL Server instance' (SQLEXPRESS), and 'SQL Database name' (\_8ManDB). There is a 'Recovery mode: Simple' dropdown menu with a red circle '1' around the 'Simple' option.
- Configuration Status:** Shows a list of configuration items with their status: 'ARM Server credentials: Test successful', 'SQL Server settings: Test successful', and 'Recovery mode: Simple: Size of the log file: 520 MB' (with a red circle '2' around the text).
- Complete configuration:** A message stating 'Configuration successfully loaded!' with a refresh icon.

The bottom of the window shows the system tray with 'Ready' and 'Anthony Admin @ localhost'.

1. Shrinking of data base logs frees up disk space. The action is performed immediately after clicking the button.
2. The actual size of logs is shown.


## Shrink database




The screenshot shows the 'Basic Configuration' window for the Access Rights Manager. It is divided into several sections:

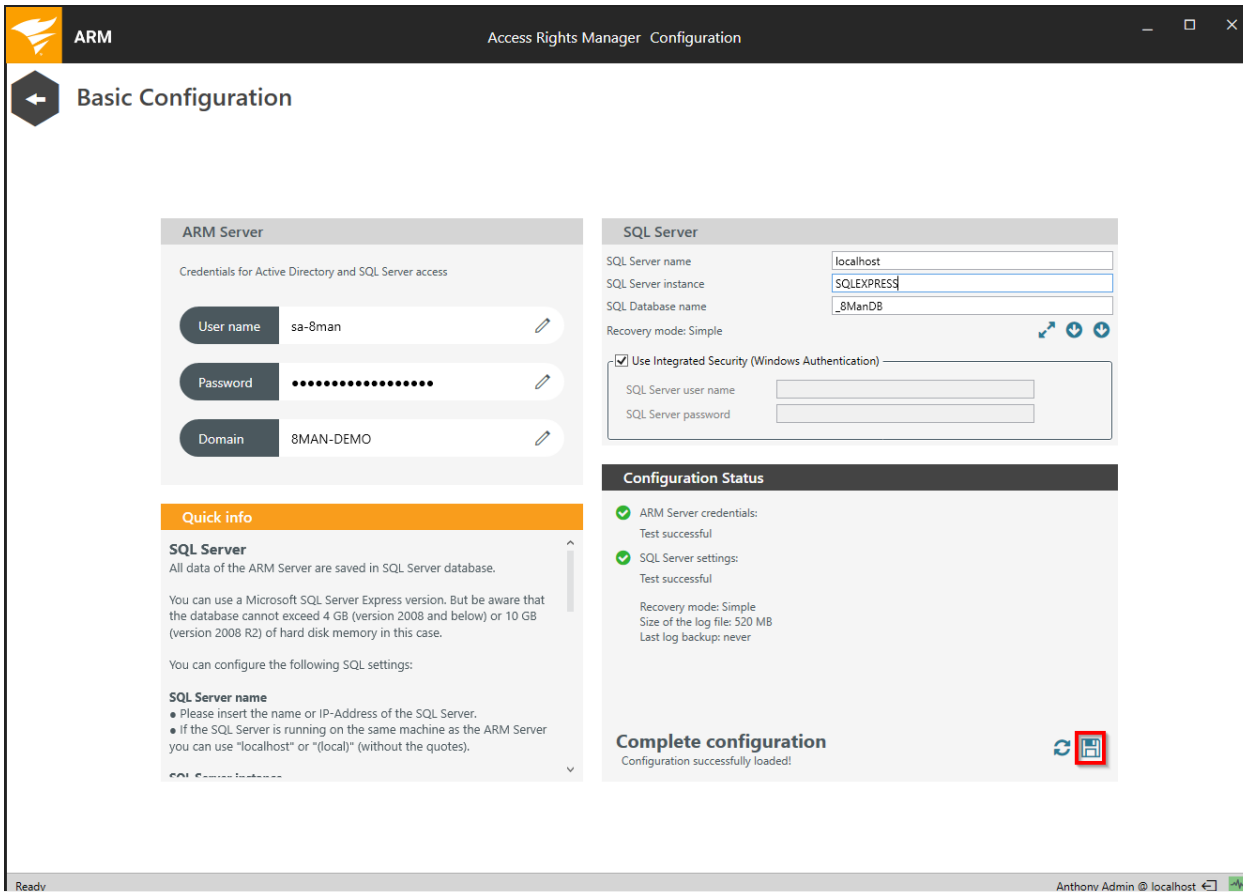
- ARM Server:** Contains fields for 'User name' (sa-8man), 'Password' (masked), and 'Domain' (8MAN-DEMO).
- SQL Server:** Contains fields for 'SQL Server name' (localhost), 'SQL Server instance' (SQLEXPRESS), and 'SQL Database name' (\_8ManDB). Below these is a 'Recovery mode: Simple' section with a 'Shrink Database' button highlighted by a red box.
- Configuration Status:** Shows two successful test results: 'ARM Server credentials: Test successful' and 'SQL Server settings: Test successful'. It also lists 'Recovery mode: Simple', 'Size of the log file: 520 MB', and 'Last log backup: never'.
- Complete configuration:** A message stating 'Configuration successfully loaded!' with refresh and save icons.

Shrinking the database frees up disk space. This action is performed immediately when clicking the button.

 For more information on data base size or available disk space please see: [Server Health-Check](#).

 Please see additional notes on [SQL Express Edition](#).

## Complete and save basic configuration



ARM Access Rights Manager Configuration

### Basic Configuration

**ARM Server**

Credentials for Active Directory and SQL Server access

User name: sa-8man

Password: [Redacted]

Domain: 8MAN-DEMO

**SQL Server**

SQL Server name: localhost

SQL Server instance: SQLEXPRESS

SQL Database name: 8ManDB

Recovery mode: Simple

Use Integrated Security (Windows Authentication)

SQL Server user name: [Redacted]

SQL Server password: [Redacted]

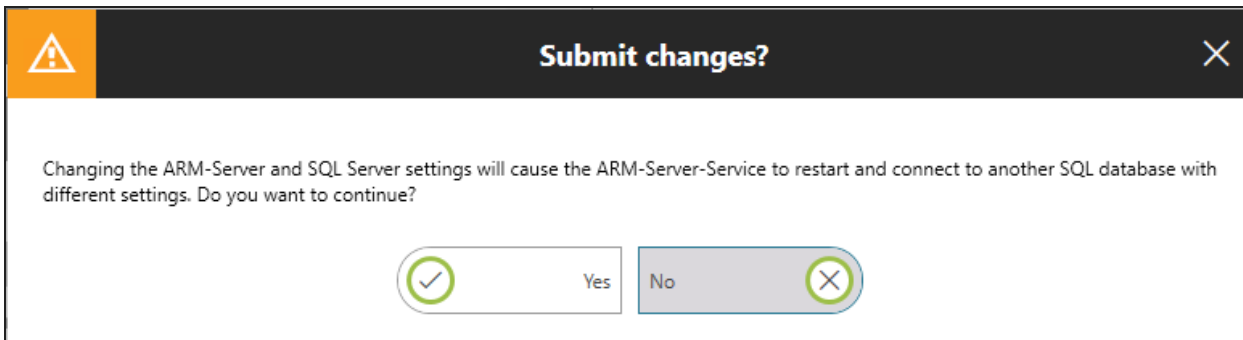
**Configuration Status**

- ARM Server credentials: Test successful
- SQL Server settings: Test successful

Recovery mode: Simple  
Size of the log file: 520 MB  
Last log backup: never

**Complete configuration**  
Configuration successfully loaded!

If all login credentials have been entered and tested successfully, you can save the configuration.

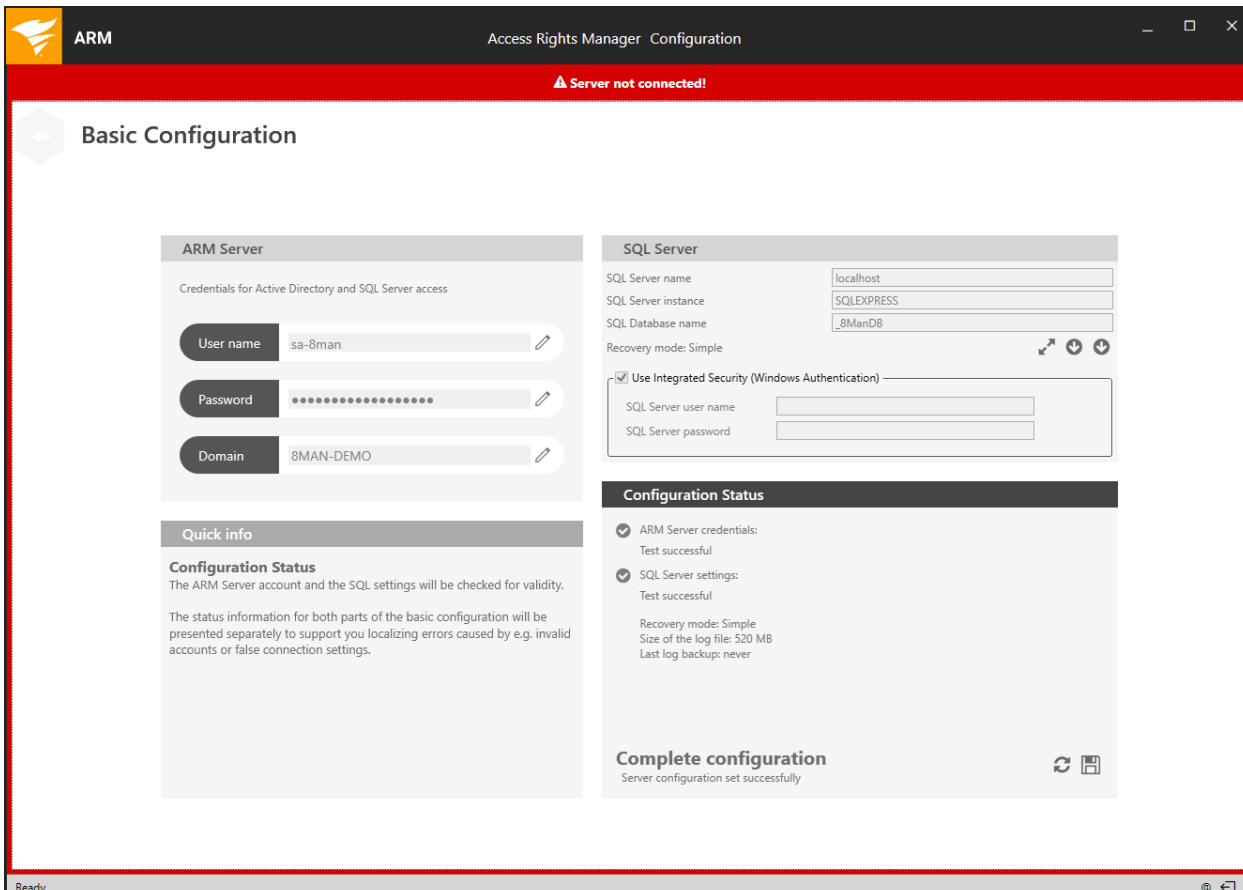


**Submit changes?**

Changing the ARM-Server and SQL Server settings will cause the ARM-Server-Service to restart and connect to another SQL database with different settings. Do you want to continue?

Yes No

Confirm the changes.



ARM Access Rights Manager Configuration

**Server not connected!**

### Basic Configuration

#### ARM Server

Credentials for Active Directory and SQL Server access

User name: sa-8man

Password: [REDACTED]

Domain: 8MAN-DEMO

#### SQL Server

SQL Server name: localhost

SQL Server instance: SQLEXPRESS

SQL Database name: \_8ManDB

Recovery mode: Simple

Use Integrated Security (Windows Authentication)

SQL Server user name: [REDACTED]

SQL Server password: [REDACTED]

#### Quick info

##### Configuration Status

The ARM Server account and the SQL settings will be checked for validity.

The status information for both parts of the basic configuration will be presented separately to support you localizing errors caused by e.g. invalid accounts or false connection settings.

#### Configuration Status


- ARM Server credentials:  
Test successful
- SQL Server settings:  
Test successful

Recovery mode: Simple  
Size of the log file: 520 MB  
Last log backup: never

#### Complete configuration

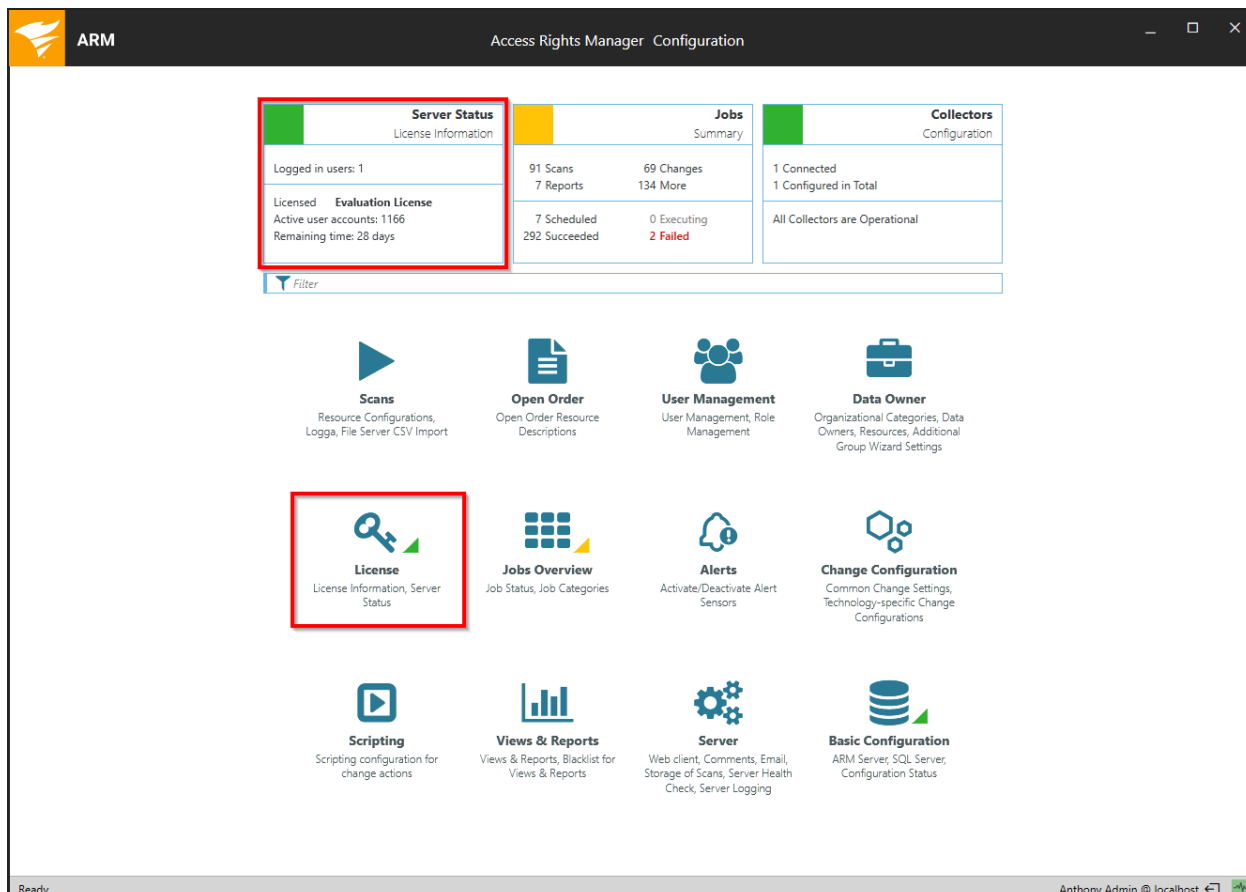
Server configuration set successfully

If you have confirmed by clicking "yes" the desired changes will be applied.

 The connection between ARM server and ARM GUI is inactive while the ARM service is being restarted. The connection will be automatically reactivated. This may take a while.



# License and server status



The screenshot shows the ARM Configuration interface. At the top, there are three summary tiles: 'Server Status' (License Information), 'Jobs Summary', and 'Collectors Configuration'. The 'Server Status' tile is highlighted with a red box and contains the following information:

Server Status
License Information
Logged in users: 1
Licensed <b>Evaluation License</b>
Active user accounts: 1166
Remaining time: 28 days

Below the summary tiles is a 'Filter' dropdown. The main area contains a grid of 12 functional tiles, each with an icon and a description of its capabilities. The 'License' tile is also highlighted with a red box.

- Scans**: Resource Configurations, Logga, File Server CSV Import
- Open Order**: Open Order Resource Descriptions
- User Management**: User Management, Role Management
- Data Owner**: Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**: License Information, Server Status
- Jobs Overview**: Job Status, Job Categories
- Alerts**: Activate/Deactivate Alert Sensors
- Change Configuration**: Common Change Settings, Technology-specific Change Configurations
- Scripting**: Scripting configuration for change actions
- Views & Reports**: Views & Reports, Blacklist for Views & Reports
- Server**: Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**: ARM Server, SQL Server, Configuration Status

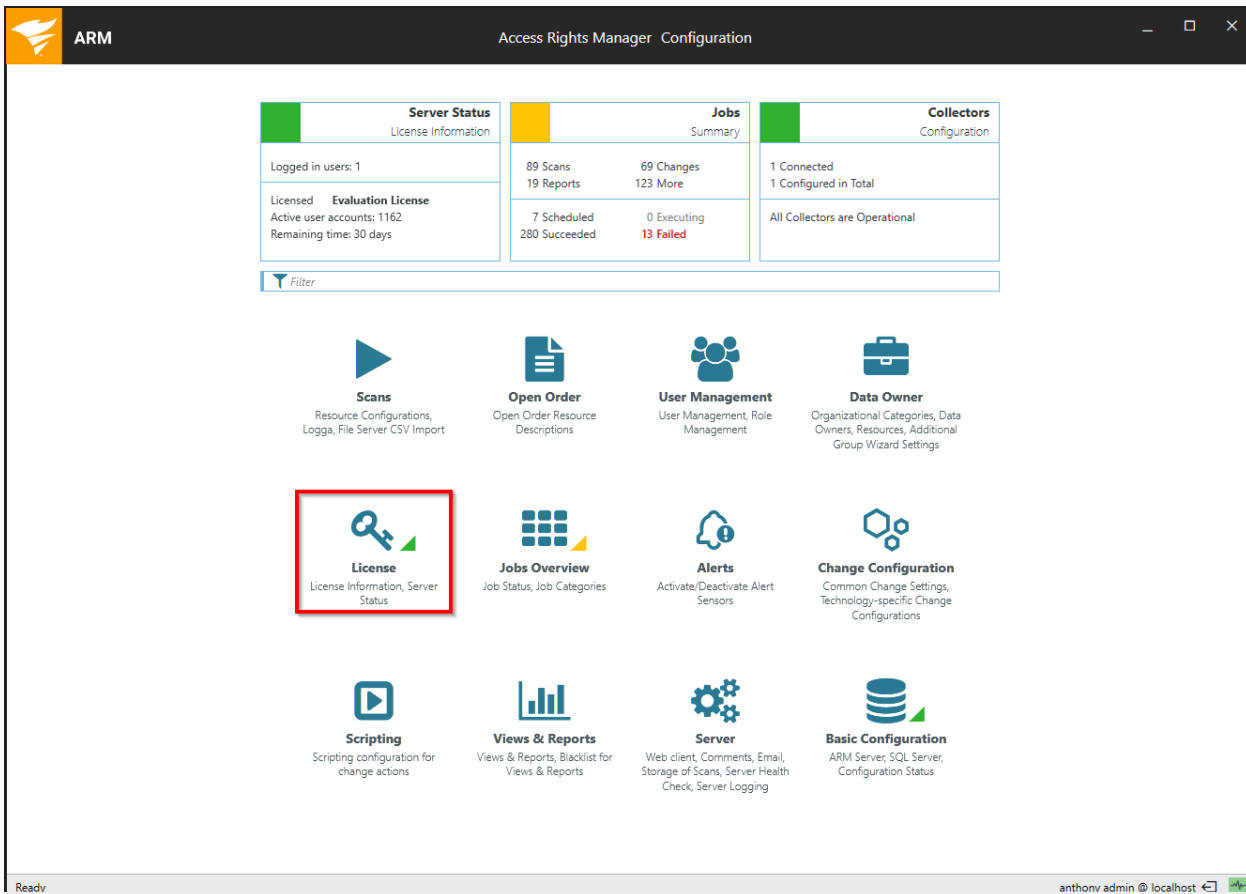
The ARM configuration home page displays information about the "Server Status" including license information.

Click on the tile "Server Status" or the category "License" for more details on the server status.

## Switch from an evaluation license to a production license

To convert your evaluation license into a permanent production license, complete the following steps. You will need a purchased license and access to the SolarWinds customer portal.

Activating a license binds your purchased license to a single installation. Please refer to the chapter [transfer a license to another server](#) if needed.



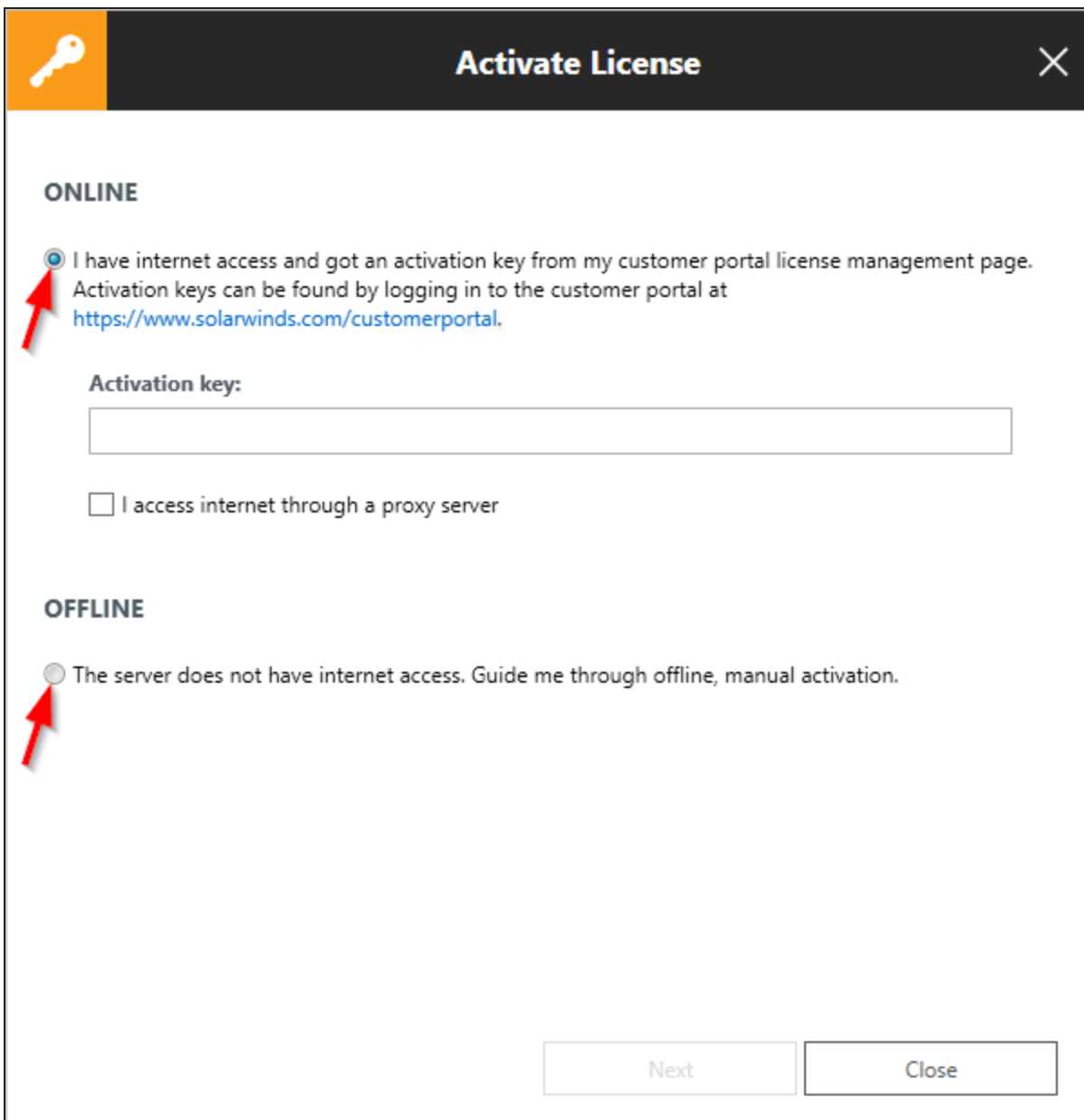
Start the ARM configuration application and click "License".

The screenshot displays the 'License Information and Server Status' page in the SolarWinds Access Rights Manager Configuration tool. The interface is divided into several sections:

- License Information:** A table showing details about the current license, including Customer (Trial), Evaluation version? (Yes), Remaining time (30 days), Licensed? (Yes), and Product (Enterprise). A red box highlights the 'Activate' button. Below the table is a link for 'Load 8MAN license'.
- Technologies:** A table listing various technologies and their status, such as Domains (\*), Licensed user count (unlimited), and various Logga counts (99).
- Features:** A table listing features like GrantMA, Programming Interface, Alerts, and Analyze and Act, all of which are enabled (Yes).
- Server Status:** Shows system uptime (41 hours) and version (9.1.164.0). Below this is a 'Logged in users: 1' section with a table listing the user 'anthony admin' and their associated components.
- Documentation:** A section with expandable links for 'Easy Connect - SQL' and 'Easy Connect - CSV', each with sub-links for documentation and example files.

The status bar at the bottom indicates the system is 'Ready' and the user is 'anthony admin @ localhost'.

Click "Activate".



**Activate License**

**ONLINE**

I have internet access and got an activation key from my customer portal license management page. Activation keys can be found by logging in to the customer portal at <https://www.solarwinds.com/customerportal>.

Activation key:

I access internet through a proxy server

**OFFLINE**

The server does not have internet access. Guide me through offline, manual activation.

Next Close

Decide how you want to perform the license activation.

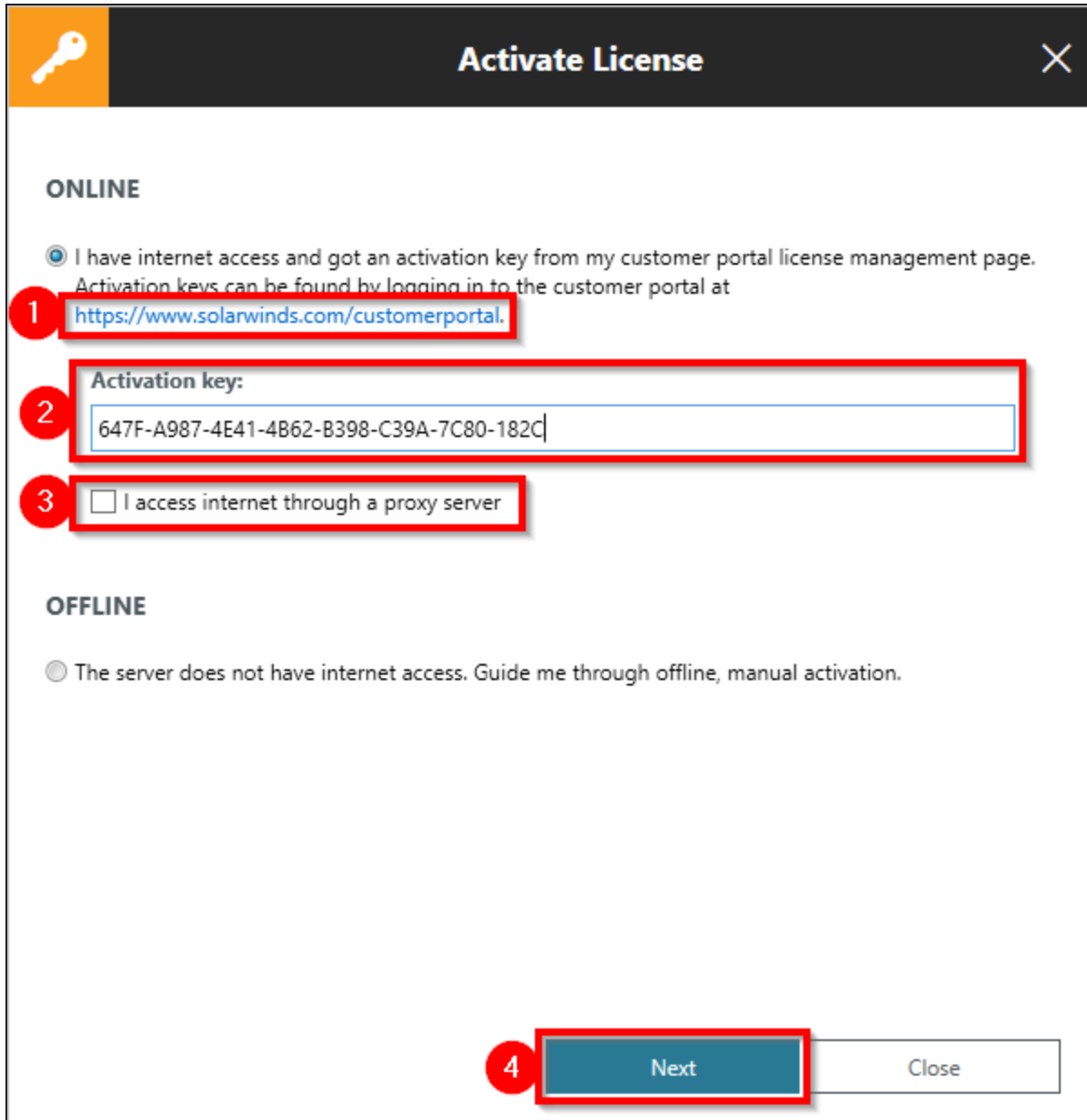
**ONLINE**

Recommended. The ARM server needs an internet connection.

**OFFLINE**

Use offline if the ARM server has no internet connection.

## Online activation



**Activate License**

**ONLINE**

I have internet access and got an activation key from my customer portal license management page. Activation keys can be found by logging in to the customer portal at <https://www.solarwinds.com/customerportal>.

**1** <https://www.solarwinds.com/customerportal>.

**2** Activation key:  
647F-A987-4E41-4B62-B398-C39A-7C80-182C


**3**  I access internet through a proxy server

**OFFLINE**

The server does not have internet access. Guide me through offline, manual activation.

**4** Next Close

1. Log in to the SolarWinds customer portal. You can use the link. You will find the appropriate activation key in the entry for your purchased ARM license.
2. Copy the activation key from the customer portal into the input field.
3. Optional: Activate this option if the Internet connection is established via a proxy server.
4. Click "Next".



## Activate License ×

**PLEASE REGISTER YOUR PRODUCT** 1

**First Name**

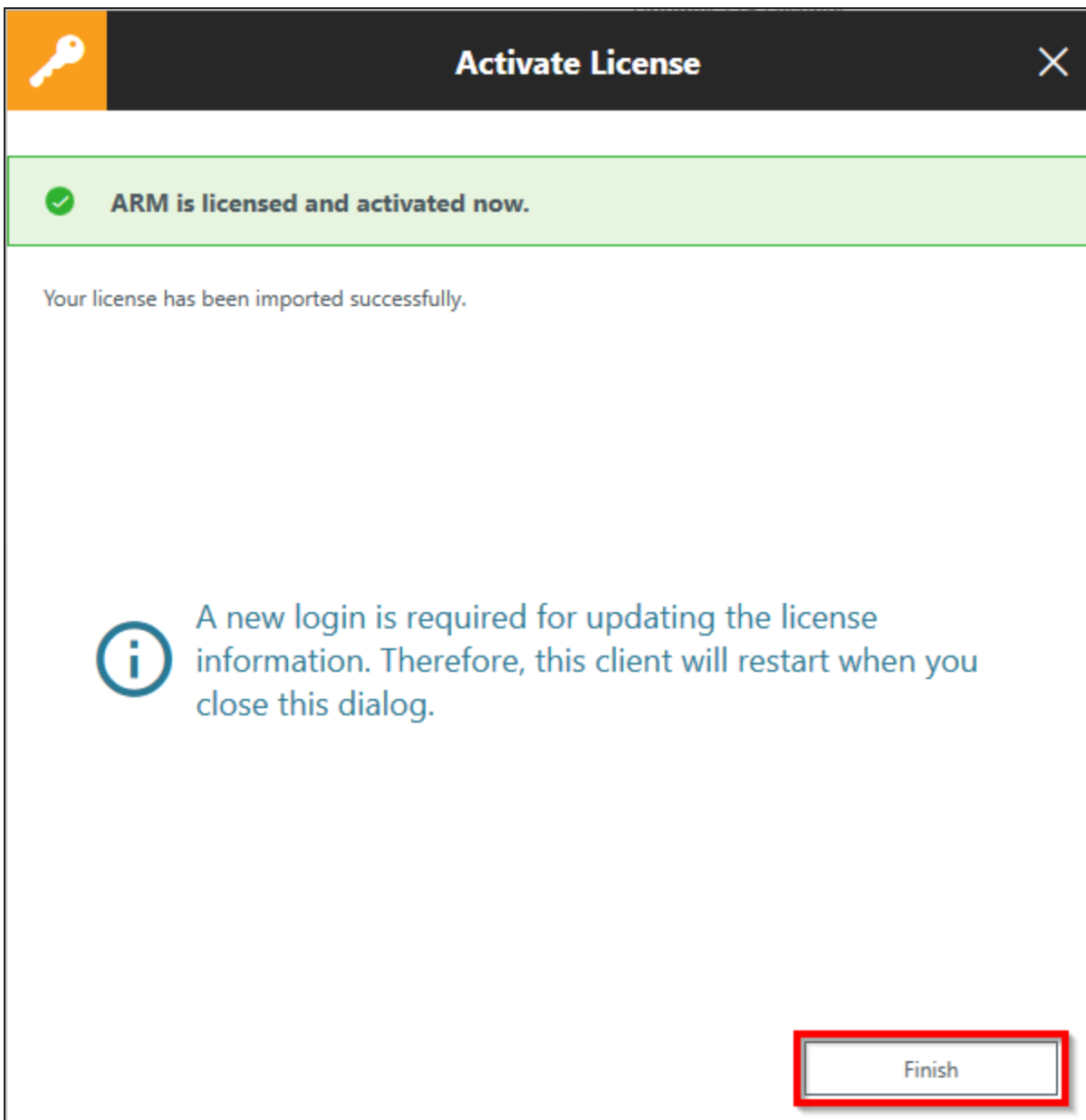
**Last Name**

**Email (required)**

**Phone Number**

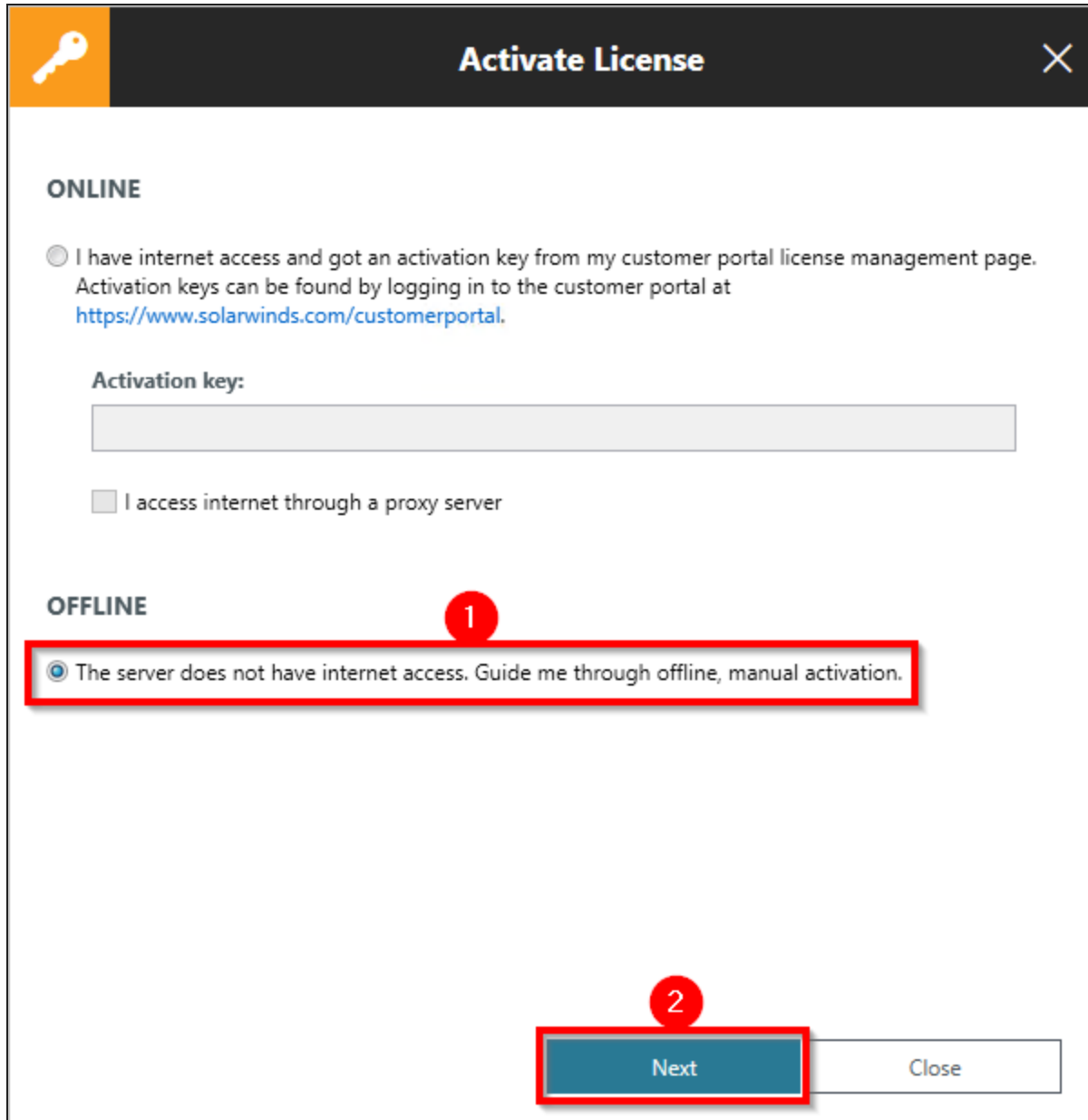
 2/> 

1. Specify to whom the product should be registered. You must enter at least one email address.
2. Click "Activate".



Click "Finish". The ARM configuration application will then restart to update the license information.

## Offline activation



**Activate License**

**ONLINE**

I have internet access and got an activation key from my customer portal license management page. Activation keys can be found by logging in to the customer portal at <https://www.solarwinds.com/customerportal>.

Activation key:

I access internet through a proxy server

**OFFLINE**

The server does not have internet access. Guide me through offline, manual activation.

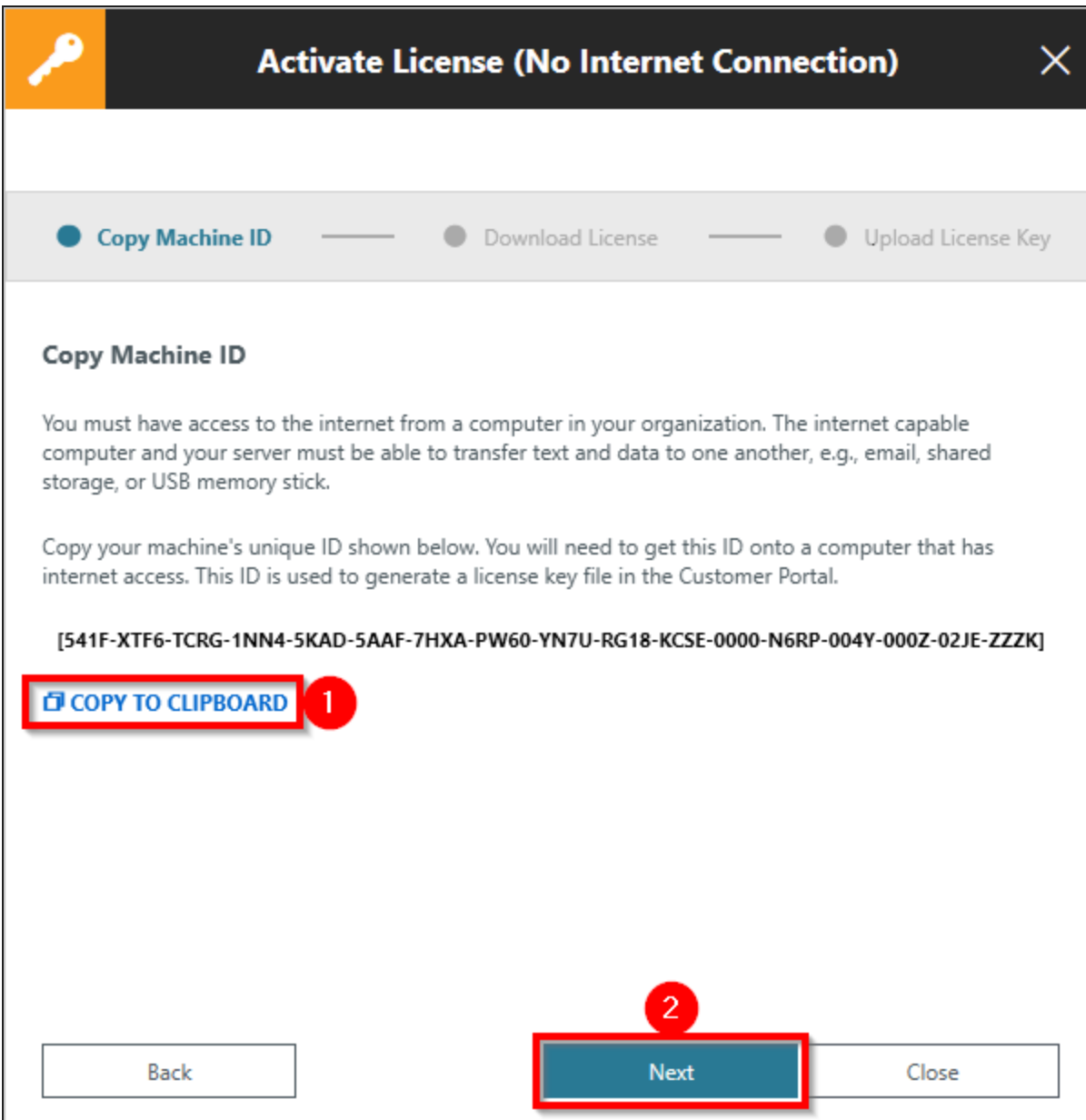
Next Close

1. Select "Offline" activation.
2. Click "Next".

For offline activation you need to transfer data between the ARM server and a computer with internet access. Typically you can use:

- clipboard shared with guest and host
- shared folders
- email
- USB memory stick etc.





**Activate License (No Internet Connection)**

● **Copy Machine ID** — ● Download License — ● Upload License Key

### Copy Machine ID

You must have access to the internet from a computer in your organization. The internet capable computer and your server must be able to transfer text and data to one another, e.g., email, shared storage, or USB memory stick.

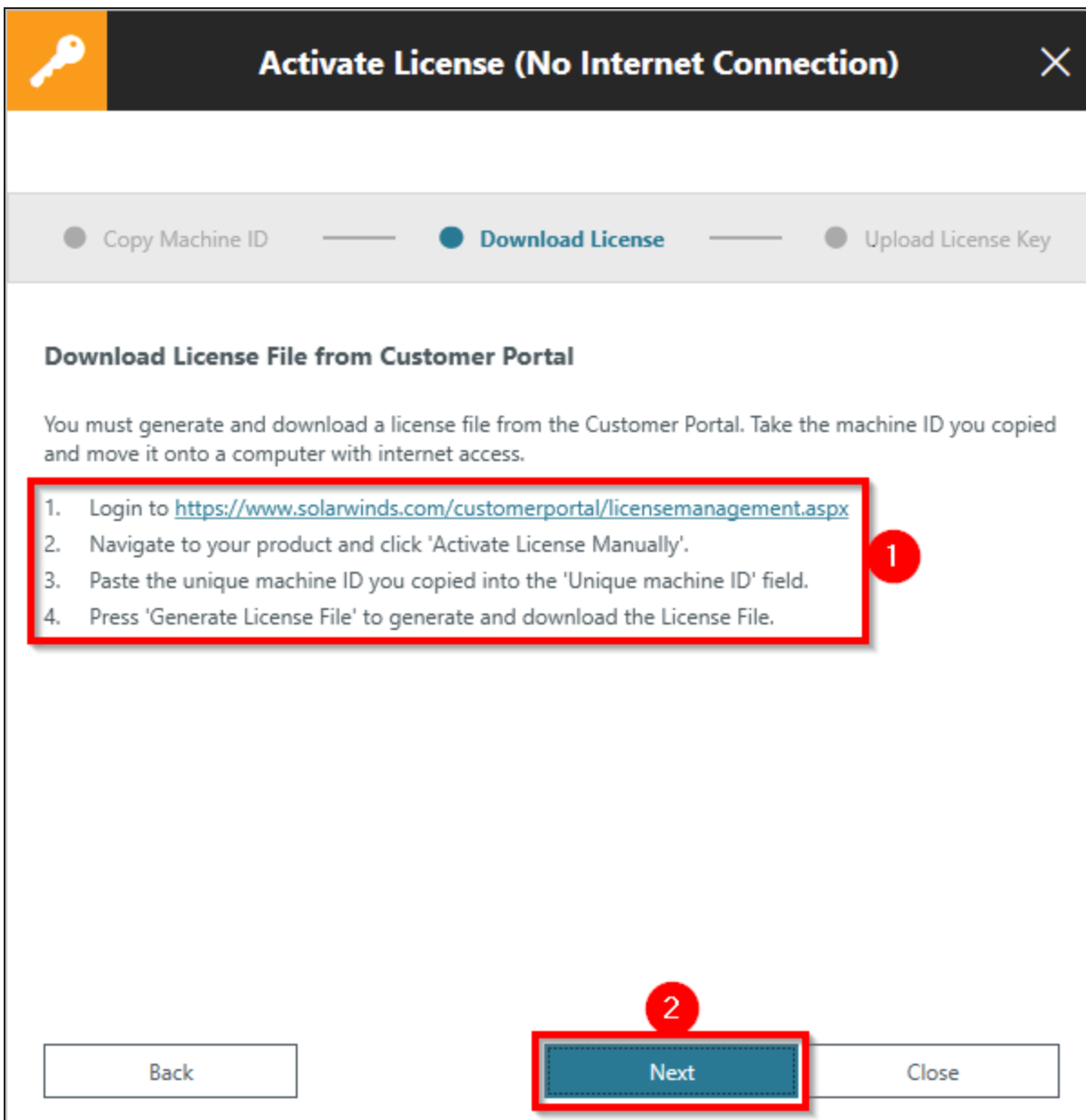
Copy your machine's unique ID shown below. You will need to get this ID onto a computer that has internet access. This ID is used to generate a license key file in the Customer Portal.

[541F-XTF6-TCRG-1NN4-5KAD-5AAF-7HXA-PW60-YN7U-RG18-KCSE-0000-N6RP-004Y-000Z-02JE-ZZZK]

**COPY TO CLIPBOARD** 1

Back **Next** 2 Close

1. Click "Copy to clipboard".
2. Click "Next".



**Activate License (No Internet Connection)**

● Copy Machine ID — ● **Download License** — ● Upload License Key


**Download License File from Customer Portal**

You must generate and download a license file from the Customer Portal. Take the machine ID you copied and move it onto a computer with internet access.

1. Login to <https://www.solarwinds.com/customerportal/licensemanagement.aspx>
2. Navigate to your product and click 'Activate License Manually'.
3. Paste the unique machine ID you copied into the 'Unique machine ID' field.
4. Press 'Generate License File' to generate and download the License File.

Back **Next** Close

1. Follow the instructions on the screen.
2. Click "Next".



## Activate License (No Internet Connection) ×

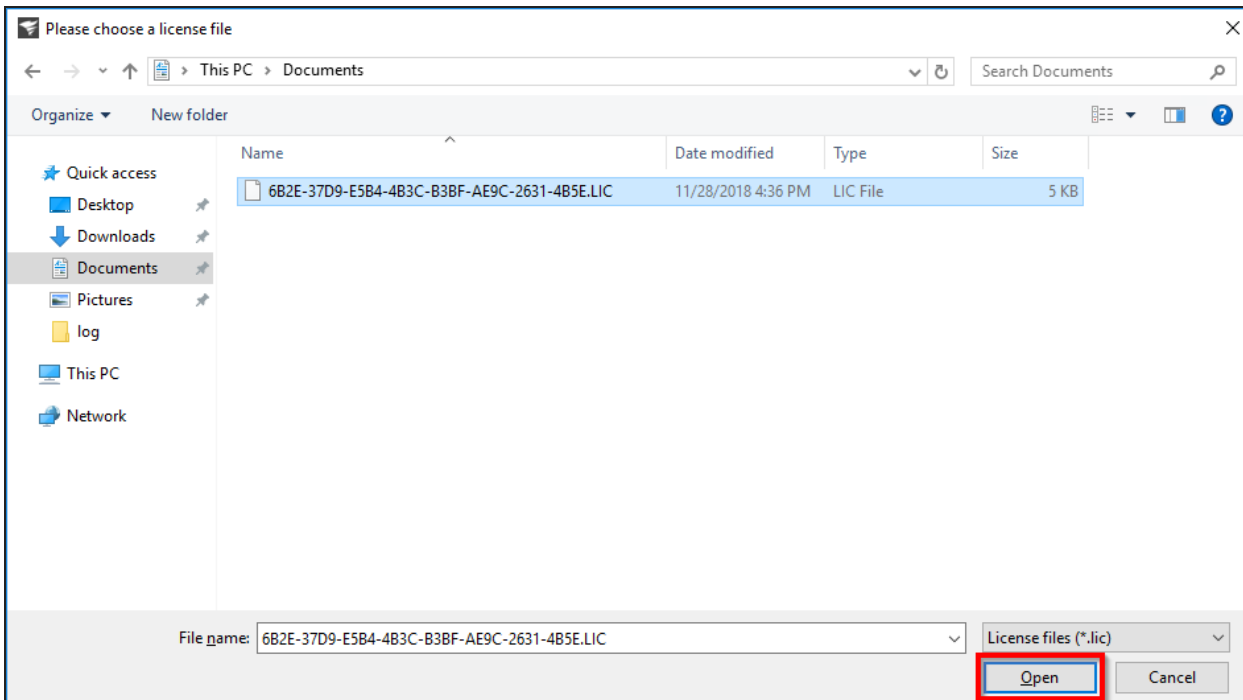
● Copy Machine ID    ● Download License    ● **Upload License Key**

### Upload License Key to ARM Server



On the machine you copied the machine ID from, upload the license key file you downloaded from the Customer Portal.

**Browse** No file selected yet.

Click "Browse".



Navigate to the location where your \*.LIC file from the customer portal is stored. Click "Open".

 **Activate License (No Internet Connection)** 

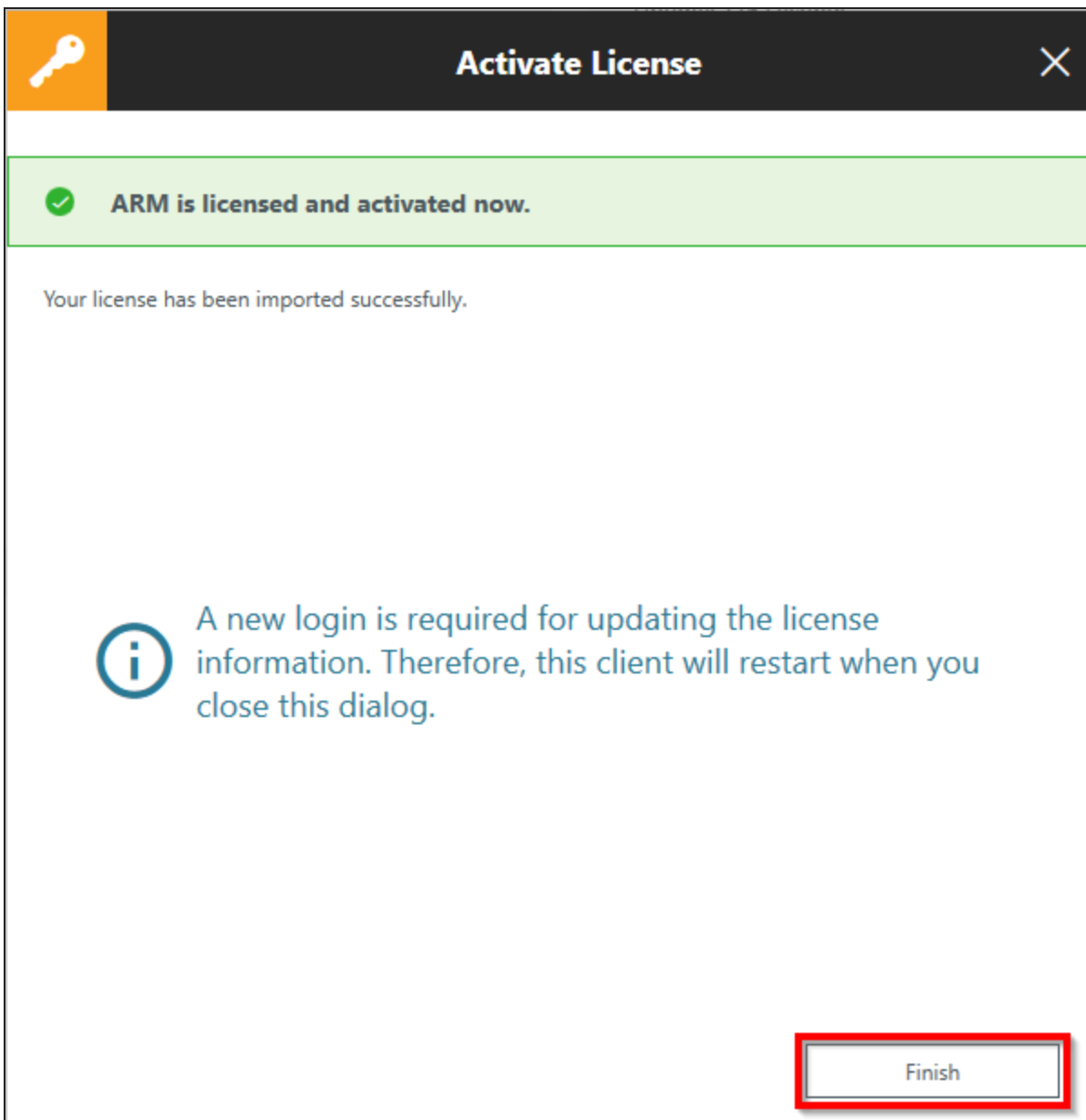
Copy Machine ID     Download License     **Upload License Key**

### Upload License Key to ARM Server

On the machine you copied the machine ID from, upload the license key file you downloaded from the Customer Portal.

C:\Users\Anthony Admin\Documents\6B2E-37D9-E5B4-4B3C-B3BF-AE9C-2...

Click "Activate" to complete the license activation.



Click "Finish". The ARM configuration application will then restart to update the license information.

## Transfer a license to another server

The ARM license is bound to the ARM server by activation. If you want to transfer the license to a new server, you must first deactivate the license on the old server and then activate it again on the new server.

The screenshot displays the 'License Information and Server Status' page in the ARM Configuration application. The 'License Information' section shows the current license is 'Enterprise' and includes 'Deactivate' and 'Activate' buttons. The 'Server Status' section shows the system is up for 26 seconds and version 9.1.150.0. The 'Logged in users' table shows one user logged in. The 'Technologies' and 'Features' sections provide additional system details.

License Information	
Customer	Yes
Licensed:	Yes
Product	Enterprise
	<input type="button" value="Deactivate"/> <input type="button" value="Activate"/>

Technologies	
Domains	*
Licensed user count	200 (in use 82049)
File server count	99
Active Directory Logga count	99
File server Logga count	99
Exchange Logga count	99
Exchange Forests	99

Features	
GrantMA	Yes
Programming Interface	Yes (read and modify)
Alerts	Yes
Analyze and Act	Yes

Server Status	
Uptime:	26 seconds
Version:	9.1.150.0

Logged in users: 1			
Name	Domain	Host	ARM Component
*	*	*	Configuration

Documentation

- ^ Easy Connect - SQL
  - [How to documentation](#)
  - [Example SQL command files](#)
- ^ Easy Connect - CSV
  - [How to documentation](#)
  - [Example CSV files](#)

In the ARM configuration application under "License," click "Deactivate."

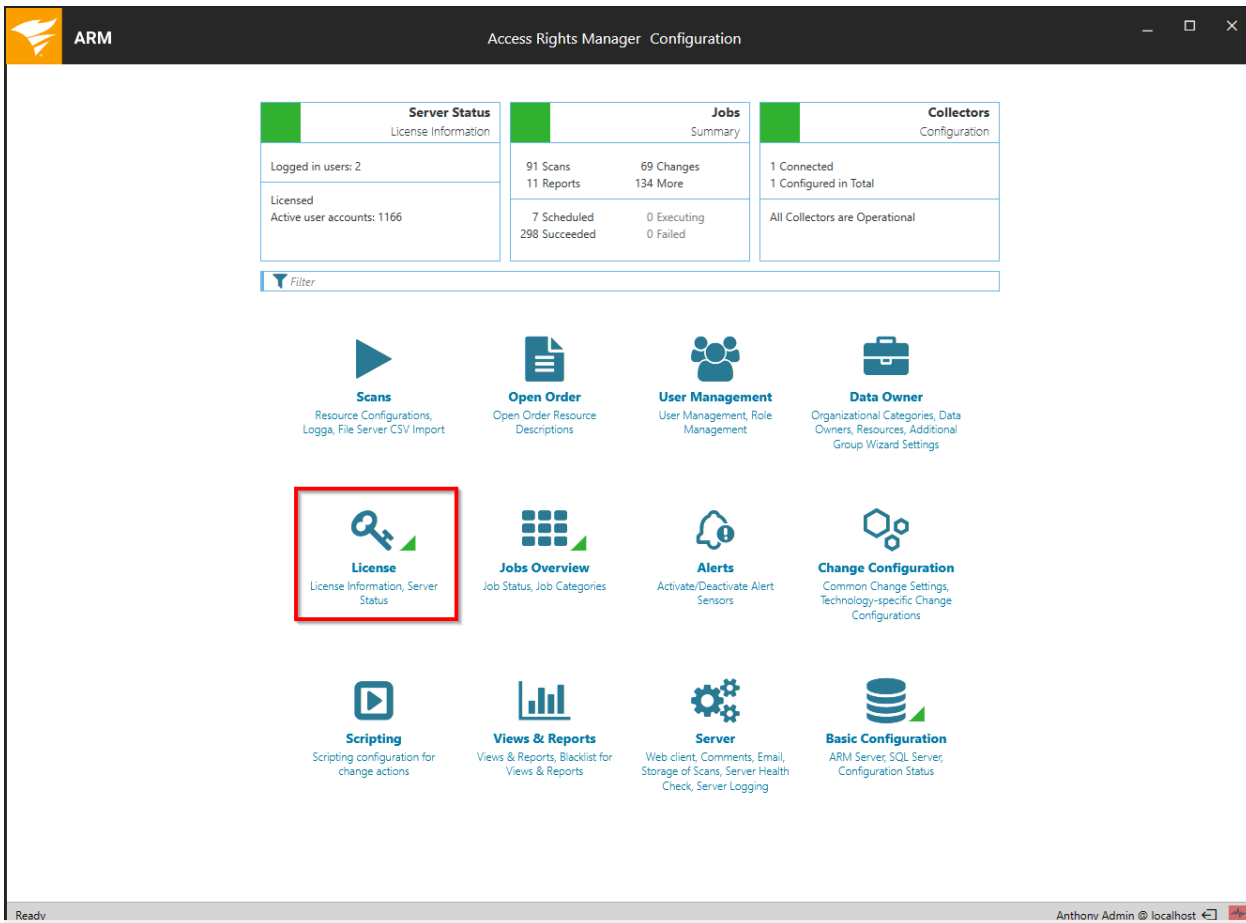
The activation is described in the topic [Switch from an evaluation license to a production license](#).

## Assign licenses to AD objects

**⚠** This chapter is only relevant to the SolarWinds licensing mechanism, not for the legacy 8MAN licensing.

Use the assignment of licenses in case you have more active users in your domains than in your license scope.

If you have a license coverage for all users in your domains, you do not need to make an assignment.



In the ARM configuration application click "License".



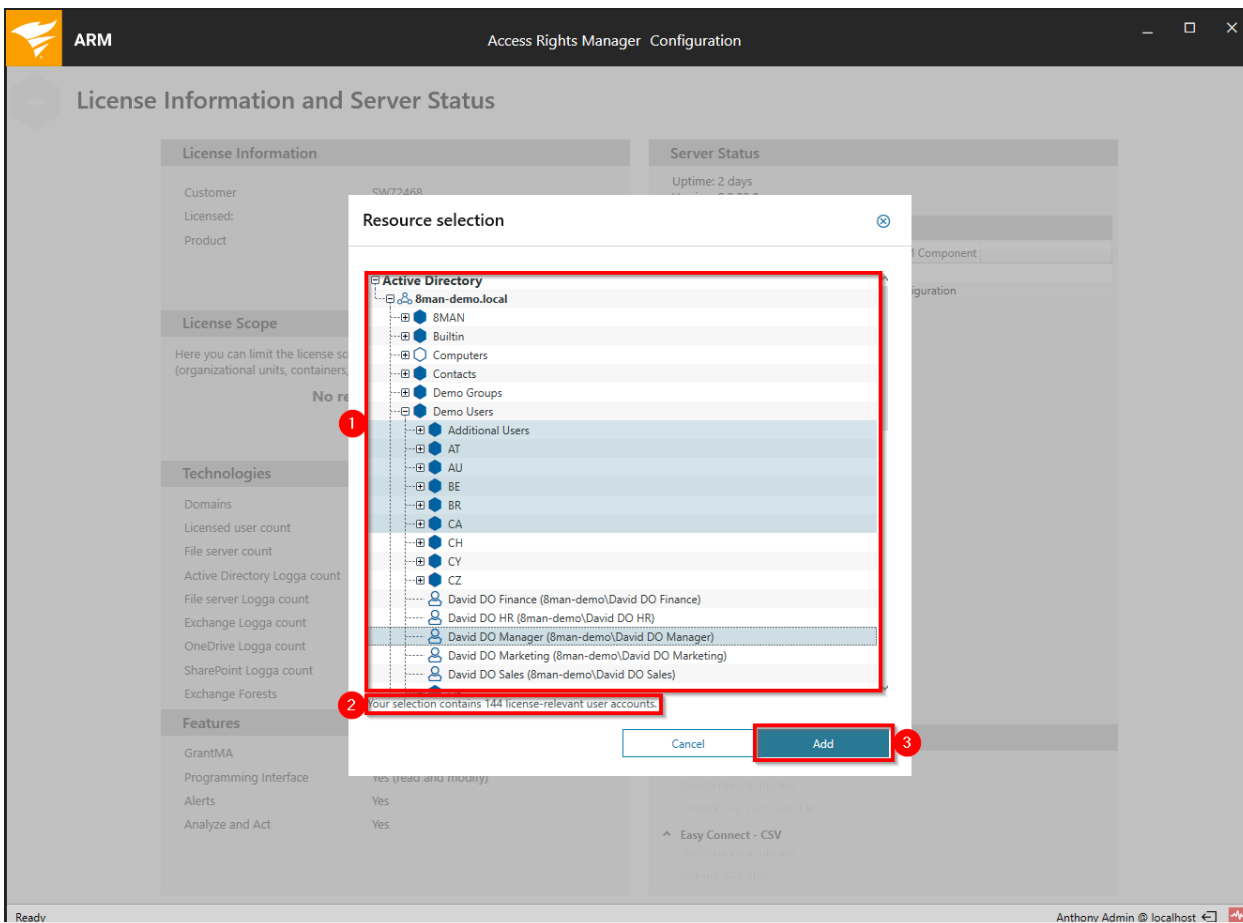
The screenshot displays the 'License Information and Server Status' page in the SolarWinds Access Rights Manager Configuration console. The page is divided into several sections:

- License Information:** Shows Customer (SW72468), Licensed (Yes), and Product (Enterprise). A 'Deactivate' button is present.
- License Scope:** Includes the text 'Here you can limit the license scope to individual Active Directory resources (organizational units, containers, user and group accounts)'. Below this, it states 'No resources are defined' and features a red-bordered 'Add' button.
- Technologies:** Lists various technologies and their counts, such as Domains (\*), Licensed user count (3000), and File server count (unlimited).
- Features:** Lists features like GrantMA, Programming Interface, Alerts, and Analyze and Act, all marked as 'Yes'.
- Server Status:** Shows Uptime (2 days) and Version (9.2.32.0).
- Logged in users:** A table with 2 users:

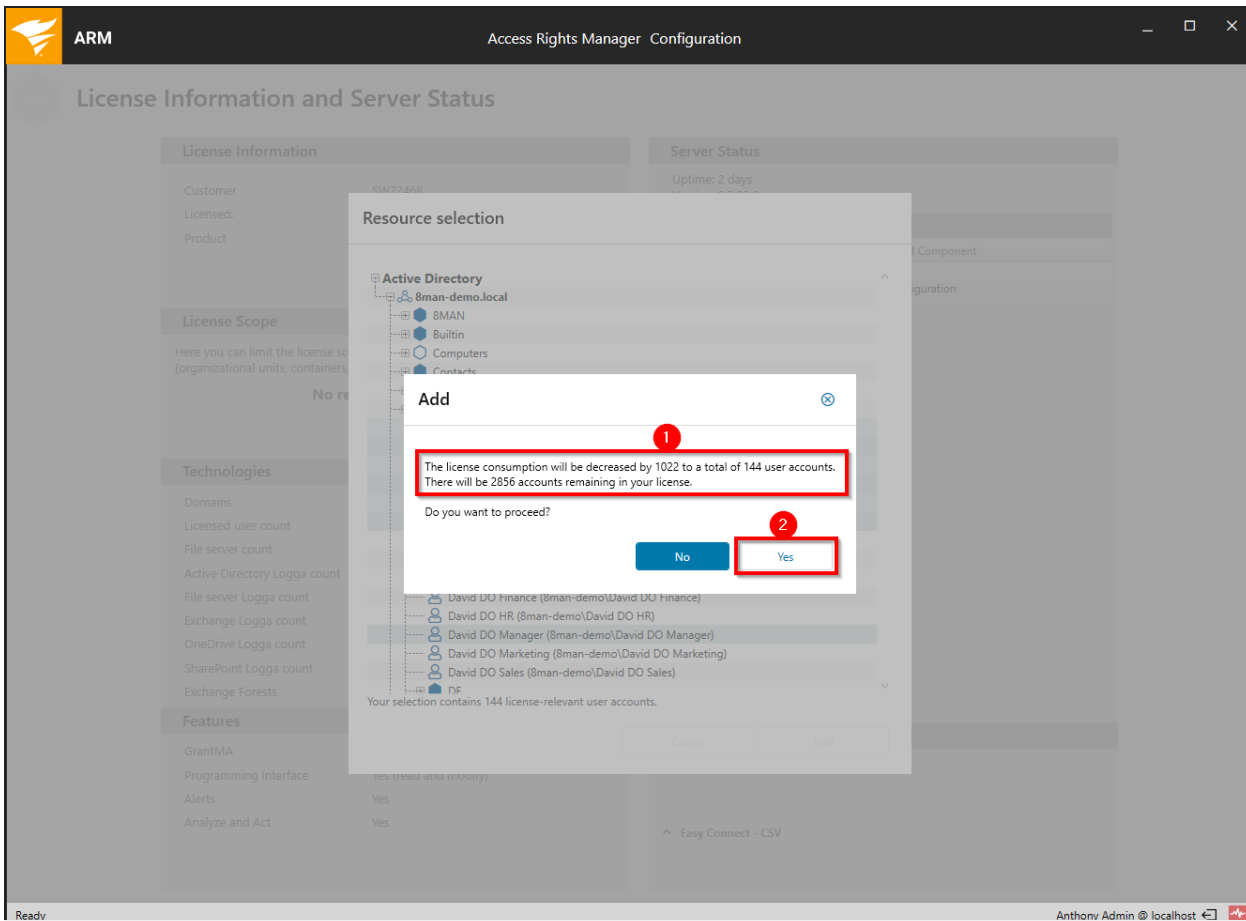
Name	Domain	Host	ARM Component
anthony admin	8MAN-DEMO	SRV-8MAN	ARM
anthony admin	8MAN-DEMO	SRV-8MAN	Configuration
- Documentation:** Contains links for 'Easy Connect - SQL' and 'Easy Connect - CSV', each with sub-links for 'How to documentation' and 'Example' files.

The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Under License Scope click "Add".



1. Select domains, OUs or users. You can use multi-select.
2. ARM shows you how many license-relevant users are selected.
3. Click "Add".



1. ARM shows you how many licenses will be assigned and how many will remain.
2. Click "Yes" to proceed.

**License Information**

Customer: SW72468  
 Licensed: Yes  
 Product: Enterprise  
 [Deactivate]

**License Scope**

Here you can limit the license scope to individual Active Directory resources (organizational units, containers, user and group accounts).

Name

- Additional Users (OU=Additional Users,OU=Demo Users,DC=8man-demo,DC=local)
- AT (OU=AT,OU=Demo Users,DC=8man-demo,DC=local)
- AU (OU=AU,OU=Demo Users,DC=8man-demo,DC=local)
- BE (OU=BE,OU=Demo Users,DC=8man-demo,DC=local)
- BR (OU=BR,OU=Demo Users,DC=8man-demo,DC=local)
- CA (OU=CA,OU=Demo Users,DC=8man-demo,DC=local)
- David DO Manager (8man-demo)David DO Manager (CN=David DO Manager,...

[Remove] [Add]

**Server Status**

Uptime: 2 days  
 Version: 9.2.32.0

**Logged in users: 2**

Name	Domain	Host	ARM Component
anthony admin	8MAN-DEMO	SRV-8MAN	ARM
anthony admin	8MAN-DEMO	SRV-8MAN	Configuration

**Technologies**

Domains: \*

Licensed user count: 3000 (in use 144)

File server count: unlimited

Active Directory Logga count: unlimited

File server Logga count: unlimited

Exchange Logga count: unlimited

OneDrive Logga count: unlimited

SharePoint Logga count: unlimited

Exchange Forests: unlimited

**Features**

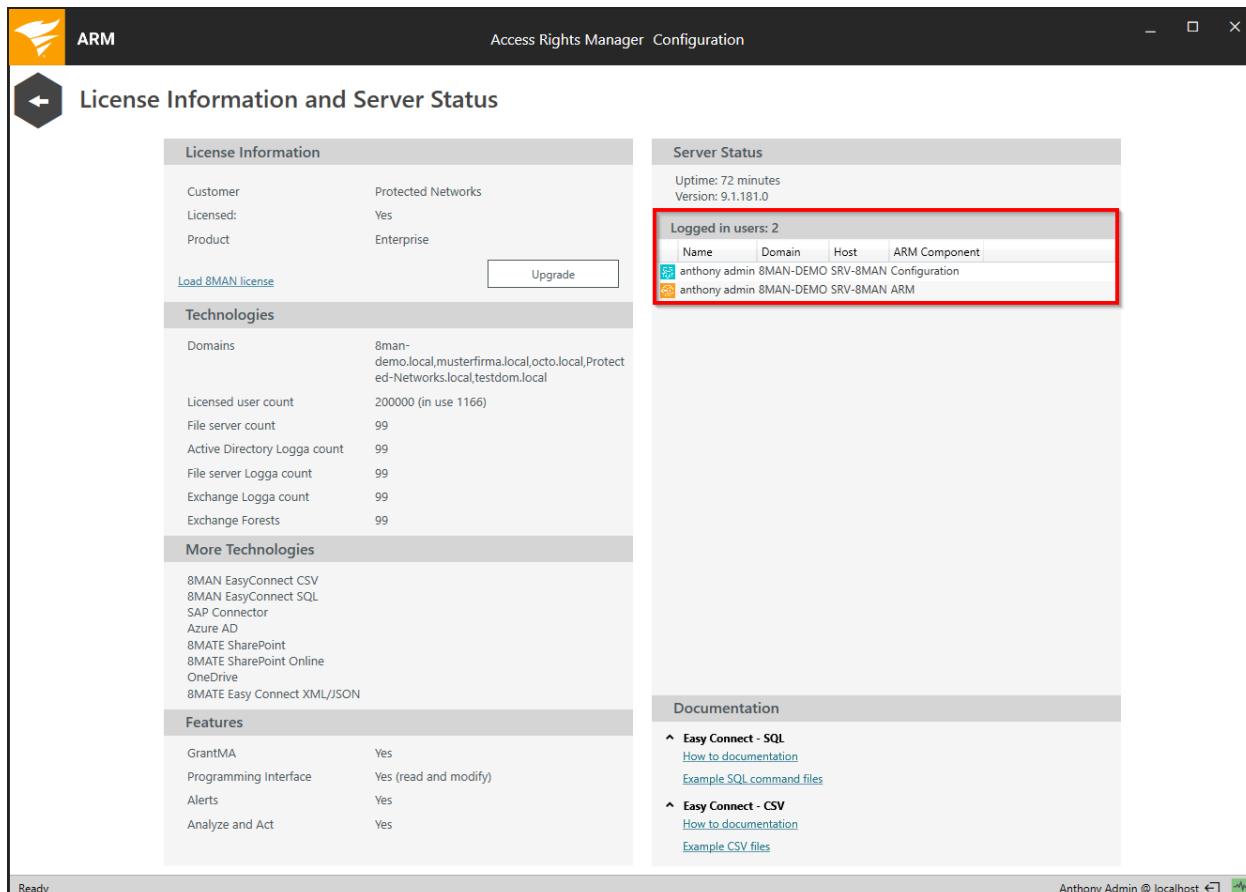
GrantMA: Yes

**Documentation**

- Easy Connect - SQL
  - [How to documentation](#)
  - [Example SQL command files](#)
- Easy Connect - CSV
  - [How to documentation](#)
  - [Example CSV files](#)

1. ARM shows you your currently assigned AD objects.
2. Select an object and click "Remove" to remove an assignment.

# Identify logged in users



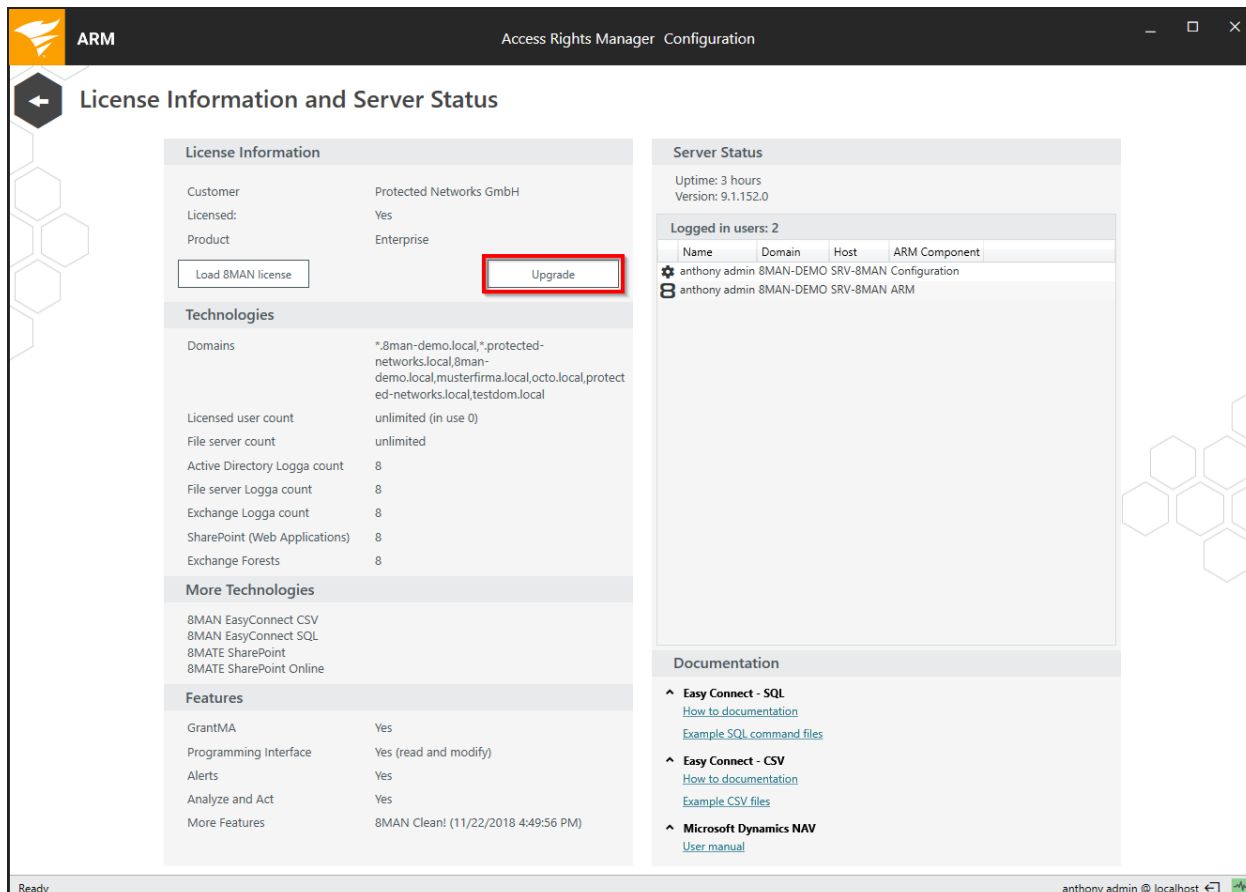
The screenshot displays the 'Access Rights Manager Configuration' window. The main content is divided into two columns. The left column contains 'License Information' and 'Technologies' sections. The right column contains 'Server Status' and 'Documentation' sections. A red box highlights the 'Logged in users: 2' section within the 'Server Status' area, which contains a table of active users.

Name	Domain	Host	ARM Component
anthony admin	8MAN-DEMO	SRV-8MAN	Configuration
anthony admin	8MAN-DEMO	SRV-8MAN	ARM

In the Server status section you can see which users are currently logged in.

**i** The ARM application can be opened multiple times - even multiple instances on the same computer. Only one user can be logged in to the ARM configuration application.

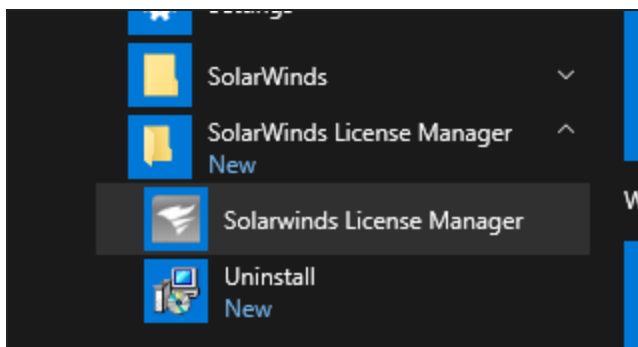
## Switch from 8MAN to SolarWinds licensing



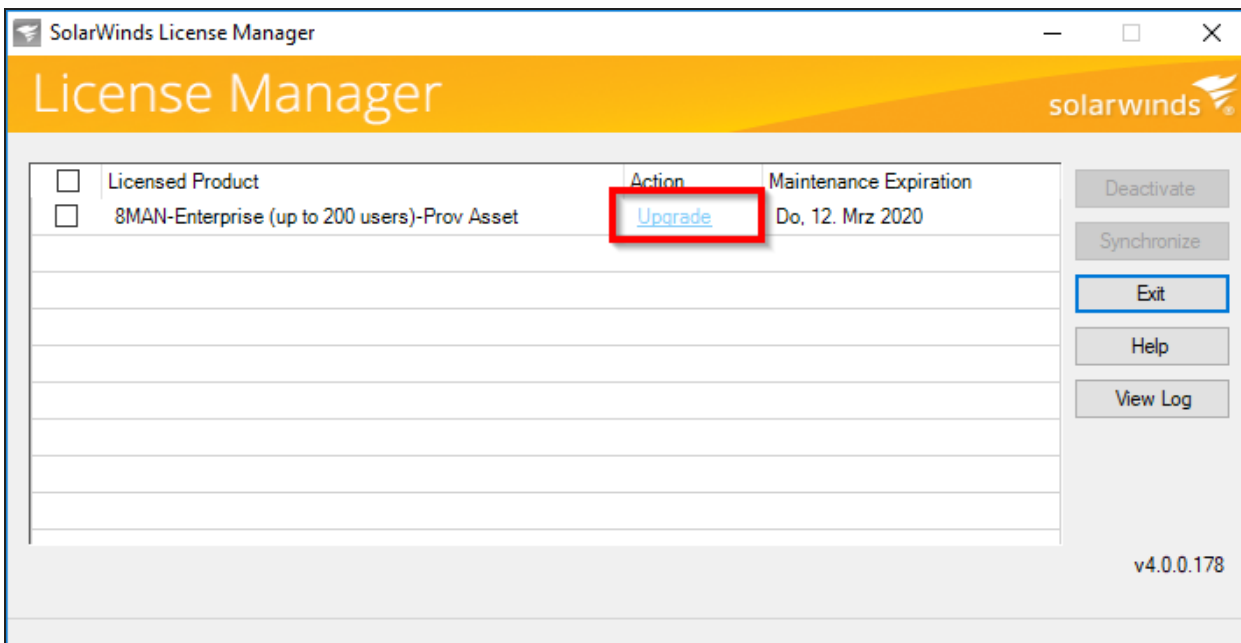
In the ARM configuration application under "License," click "Upgrade."

For the first license key use the same procedure as described in the chapter [Switch from an evaluation license to a production license](#).

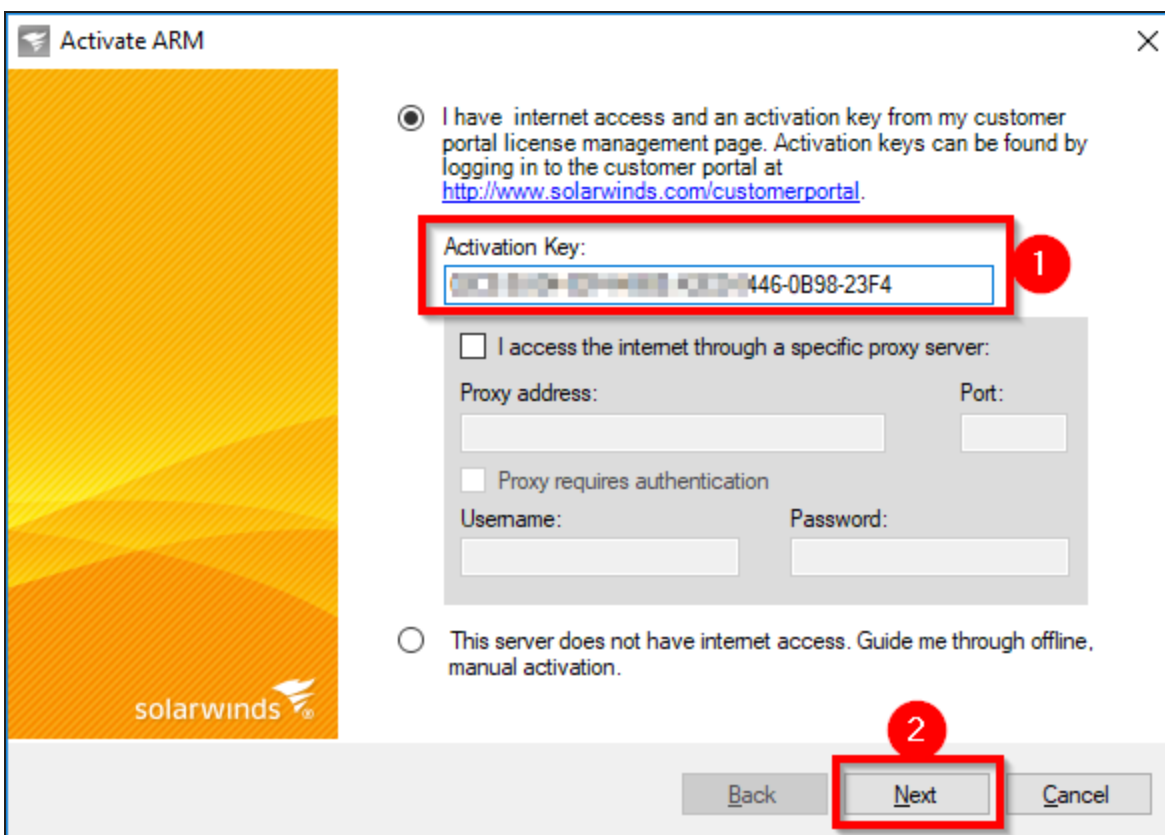
If you have more than one license key to activate follow these steps for your further license keys:



Start the SolarWinds License Manager. This is a standalone application included in the ARM setup.



Click "Upgrade".



1. Copy the next license key into the license manager.
2. Click "Next" and follow the instructions on the screen.

Repeat the steps until all your license keys are activated.

The screenshot displays the 'License Information and Server Status' page in the Access Rights Manager Configuration 9.2.1 application. The 'License Information' section shows the following details:

Customer	[Redacted]
Licensed:	Yes
Product	Enterprise

Below this, there is a 'Load 8MAN license' link and an 'Upgrade' button. The 'Technologies' section is highlighted with a red box and contains the following data:

Domains	*
Licensed user count	200 (in use 87027)
File server count	16
Active Directory Logga count	available
File server Logga count	2

The 'Features' section is also highlighted with a red box and contains the following data:


GrantMA	Yes
Programming Interface	Yes (read and modify)
Alerts	Yes
Analyze and Act	Yes

The 'Server Status' section on the right shows 'Uptime: 11 minutes' and 'Version: 9.2.1'. Below it, a table titled 'Logged in users: 1' lists one user:

Name	Domain	Host	ARM Component
[Redacted]	[Redacted]	[Redacted]	Configuration

Double check under "Features" and "Technologies" all your licensed features.

## Load the license file and check covered features

 This chapter is only relevant to customers with the legacy 8MAN licensing mechanism.



The screenshot shows the 'Access Rights Manager Configuration' window. The 'License Information' section includes fields for Customer (Trial), Evaluation version? (Yes), Remaining time (28 days), Licensed? (Yes), and Product (Enterprise). A red box highlights the 'Load 8MAN license' button. Below this are 'Deactivate' and 'Activate' buttons. The 'Technologies' section lists various counts, and the 'Features' section lists GrantMA, Programming Interface, Alerts, and Analyze and Act. The 'Server Status' section shows Uptime (46 minutes) and Version (9.1.181.0). A table shows 'Logged in users: 1' with columns for Name, Domain, Host, and ARM Component, listing 'anthony admin 8MAN-DEMO SRV-8MAN Configuration'. The 'Documentation' section has links for 'Easy Connect - SQL' and 'Easy Connect - CSV'.

Ready Anthony Admin @ localhost

Click "Load 8MAN license".

The screenshot shows a file explorer window titled 'Please choose a license file'. The address bar shows the path: Local Disk (C:) > ProgramData > protected-networks.com > 8MAN > licenses. A search box contains 'Search licenses'. The file list shows a single file: '8Man\_20161117125549.license' with a date modified of '11/17/2016 1:55 PM', type 'LICENSE File', and size '8 KB'. The 'File name' field at the bottom contains '8Man\_20161117125549.license' and the file type is set to 'License files (\*.license)'. 'Open' and 'Cancel' buttons are visible.

Select the path where your license key is stored. 8MAN license files have the file extension ".license".

After clicking on open, the license key will be copied to

```
%ProgramData%\protected-networks.com\8MAN\licenses
```

All licensed features are activated immediately.

The screenshot shows the 'Access Rights Manager Configuration' window. The 'License Information and Server Status' page is displayed. The 'License Information' section is highlighted with a red box and contains the following data:

License Information	
Customer	Protected Networks
Licensed:	Yes
Product	Enterprise
<a href="#">Load 8MAN license</a> <input type="button" value="Deactivate"/> <input type="button" value="Upgrade"/>	
Technologies	
Domains	8man-demo.local,musterfirma.local,octo.local,Protected-Networks.local,testdom.local
Licensed user count	200000 (in use 1166)
File server count	99
Active Directory Logga count	99
File server Logga count	99
Exchange Logga count	99
Exchange Forests	99
More Technologies	
8MAN EasyConnect CSV 8MAN EasyConnect SQL SAP Connector Azure AD 8MATE SharePoint 8MATE SharePoint Online OneDrive 8MATE Easy Connect XML/JSON	
Features	
GrantMA	Yes
Programming Interface	Yes (read and modify)
Alerts	Yes
Analyze and Act	Yes

The 'Server Status' section on the right shows:

- Uptime: 53 minutes
- Version: 9.1.181.0
- Logged in users: 1
- Table with columns: Name, Domain, Host, ARM Component. One user is listed: anthony admin 8MAN-DEMO SRV-8MAN Configuration.
- Documentation links for Easy Connect - SQL and Easy Connect - CSV.

If the license file has been successfully loaded you will see detailed information on licensed features.

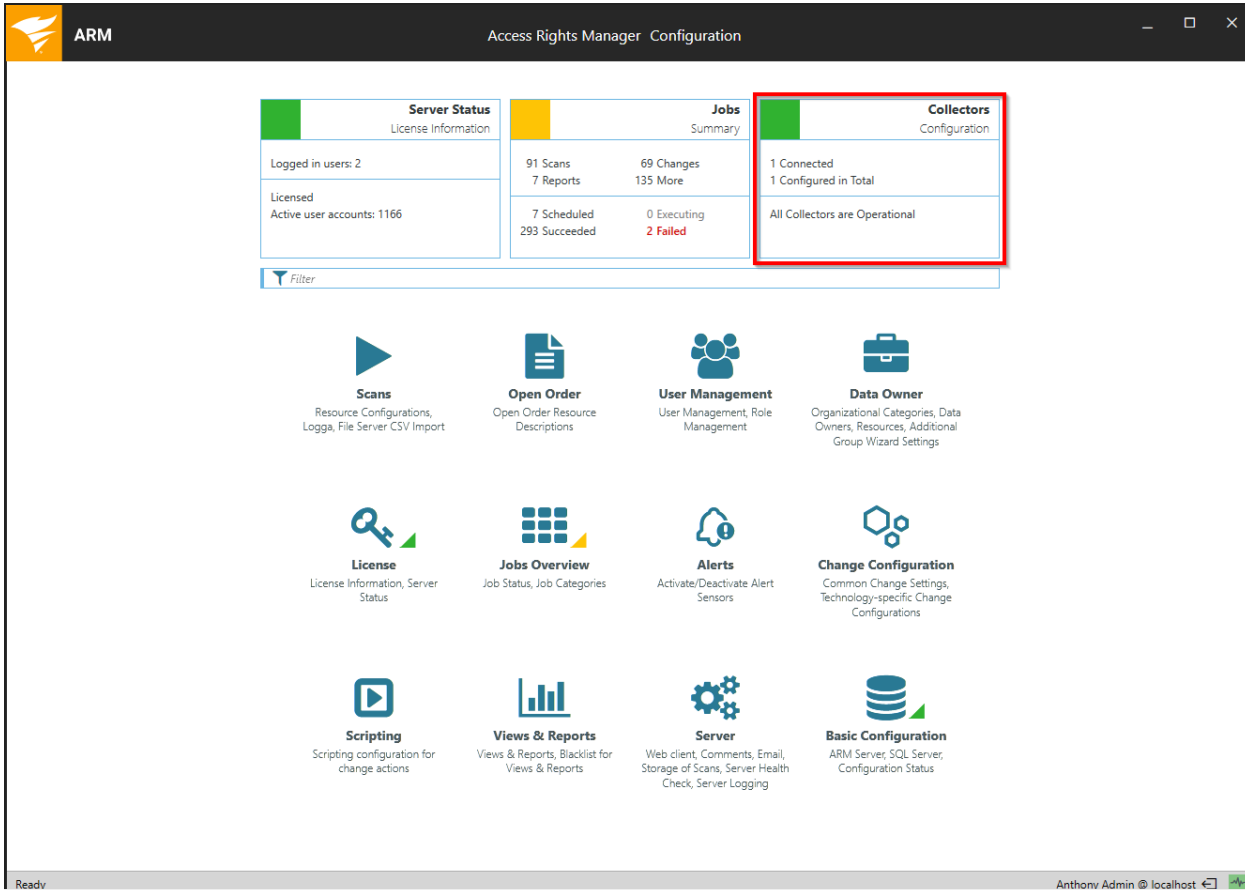
## Collectors

After the installation there is already a first collector: the ARM server itself.

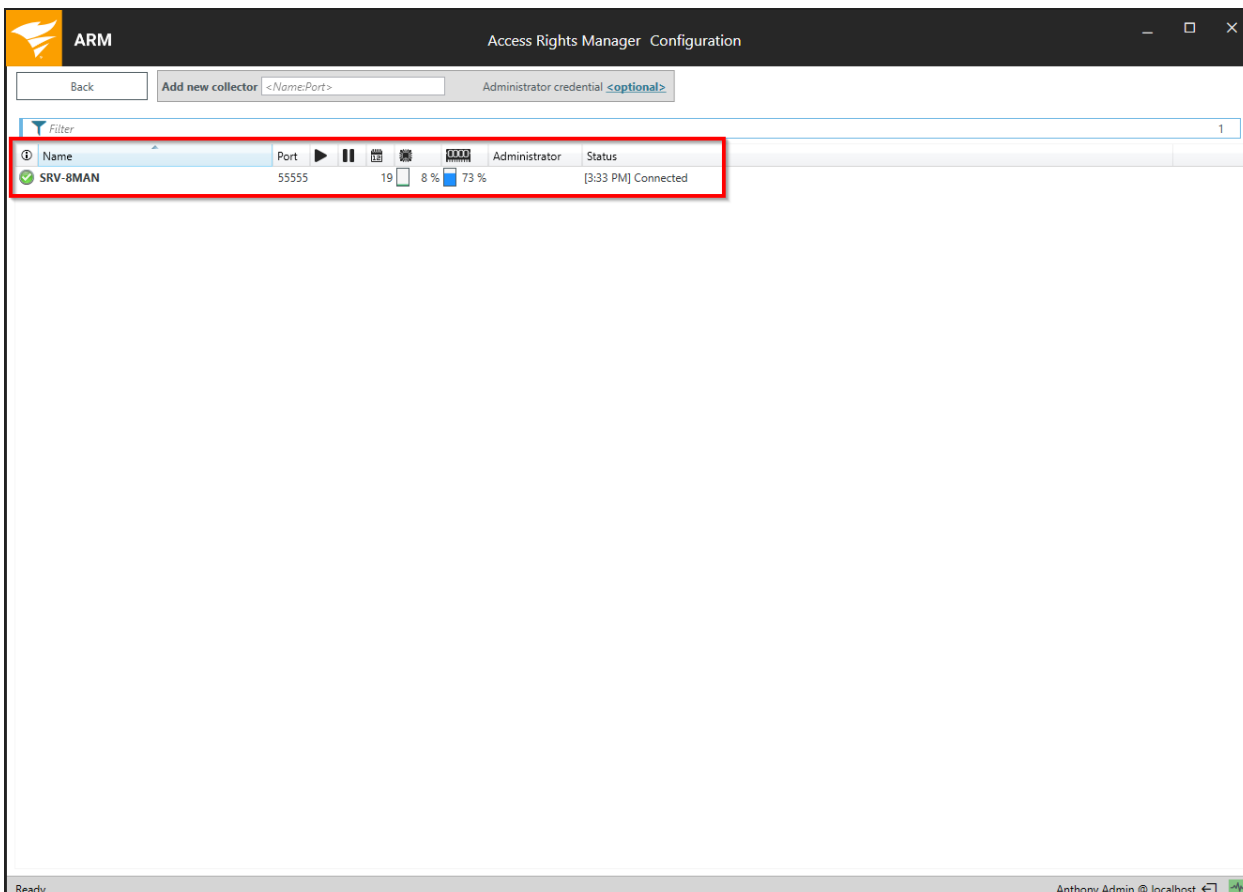
Additional collectors may be installed for the following reasons:

1. You want to connect remote resources. Installing collectors on remote systems reduces the WAN footprint and improves performance when executing scans or making access rights changes.
2. Some resource types and features require the installation of additional collectors, for example FS Logga for Windows Fileserver.
3. Load balancing.


4. To incorporate foreign domains (non-trusted) a collector must be installed. Please see [Collectors in foreign domains \(non-trusted\)](#) for more details.



Click on the tile for displaying information on the configured collectors or add new ones.



The list of collectors contains more detailed information on the selected port, storage and CPU workload, number of scheduled jobs, connection status.

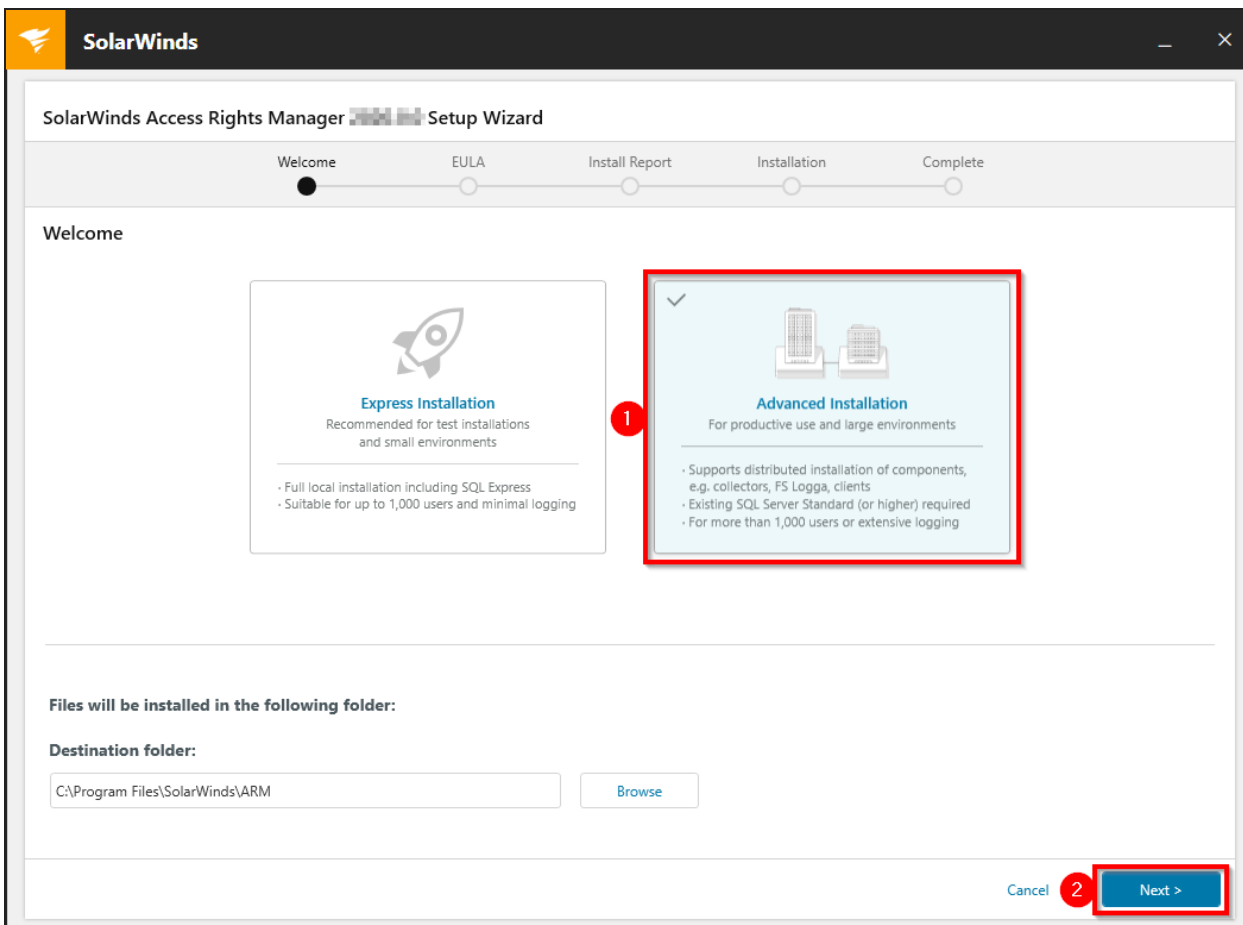
 If you are having problems with the connection please see [Firewall settings](#).

## Install additional collectors

### Add collectors using setup

If there is no trust between the ARM server (domain) and a resource (domain), this method of installing a collector must be used.

Log on to the desired system and copy the setup.exe file into a local folder (do not use a network folder). Start the file with administrator rights.

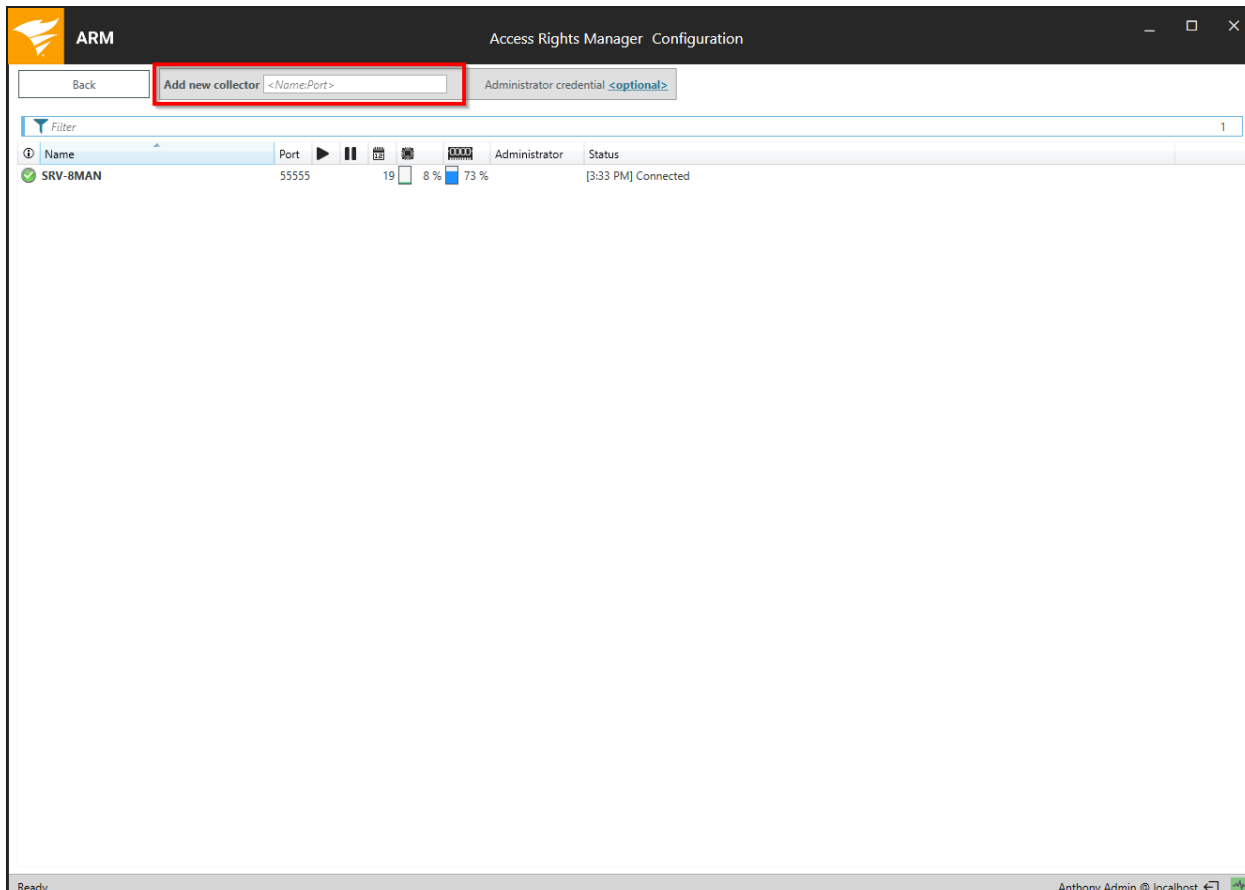


1. On the welcome page select production installation.
2. Click Next.

1. Select Custom Installation.
2. Enable ARM Collector.
3. Click Next and follow the instructions on the screen.

**i** After the installation is complete the collector must be added to the ARM configuration (please see next paragraph).

## Add collectors or install via push method

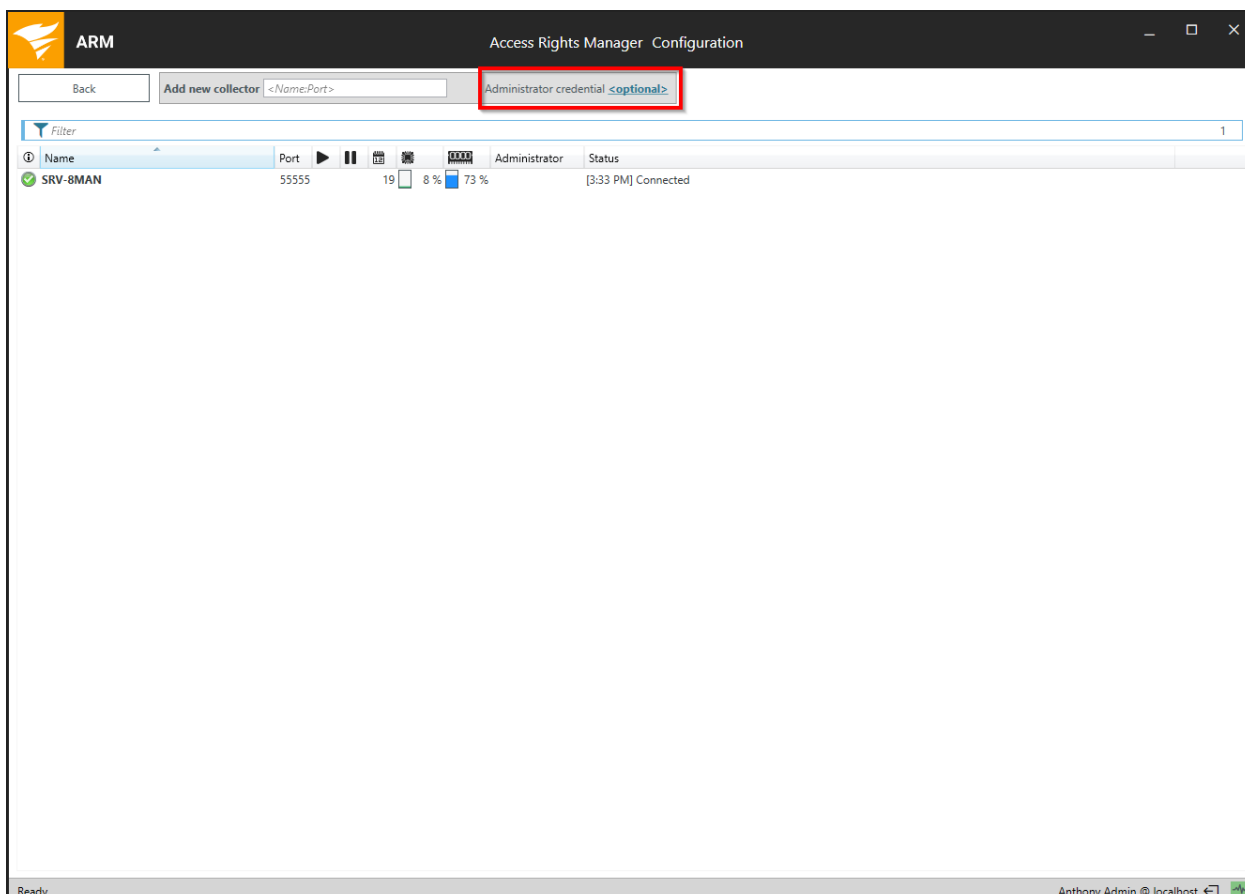


Enter the name of the desired server. Enter a port number after the name, if you don't use the default port "55555".

If the target system already has a collector installed, it will be added to a lists of collectors and establish a connection. You do not need to enter any login credentials.

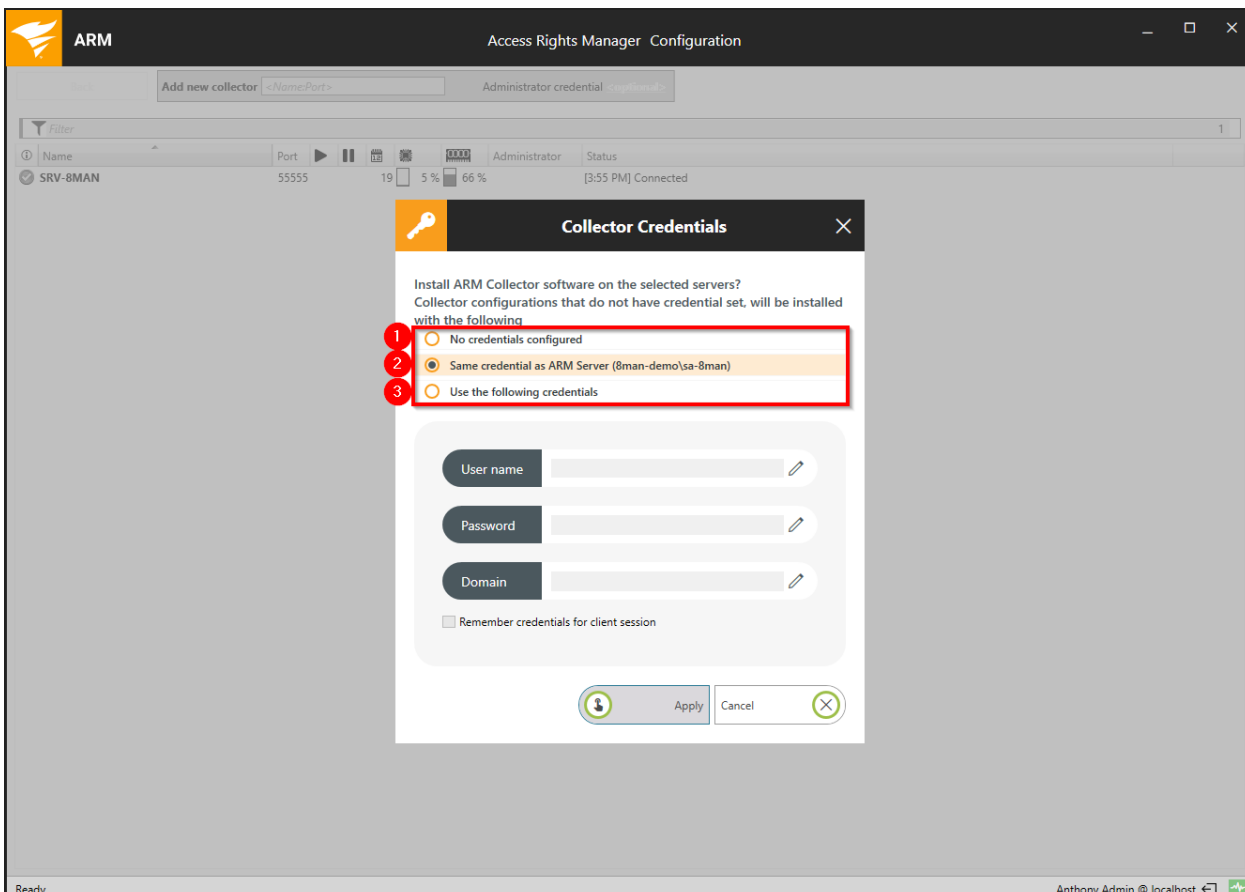
If the target system is in a foreign domain (non-trusted), please note the section: [Run collectors in foreign domains \(non-trusted\)](#).

If you are having connection problems please see: [Firewall settings](#).

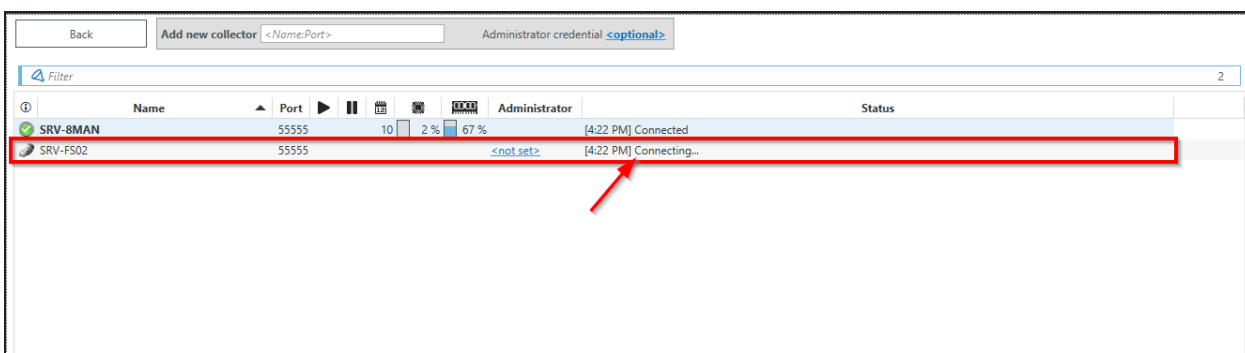


If a collector has not been installed on the target system an installation will be attempted through the push method. Click the link "<optional>" and enter your login credentials, that are required for setup execution on the target system.





1. Select "No credentials" if you would like to remove previously entered credentials.
2. The installation is performed using the credentials from the basic configuration.
3. Enter any additional credentials you would like to use for collector installation.



Information on the progress of the installation process are shown in the column "Status".

If the target system is in a foreign domain (non-trusted), please note the section: [Run collectors in foreign domains \(non-trusted\)](#).

If you are having connection problems please see: [Firewall settings](#).

## Update collectors

To ensure successful communication between the ARM server and collector both components must be present in the same version.

ARM performs automatic updates of all collectors automatically (via push method), as long as a network connection is active.

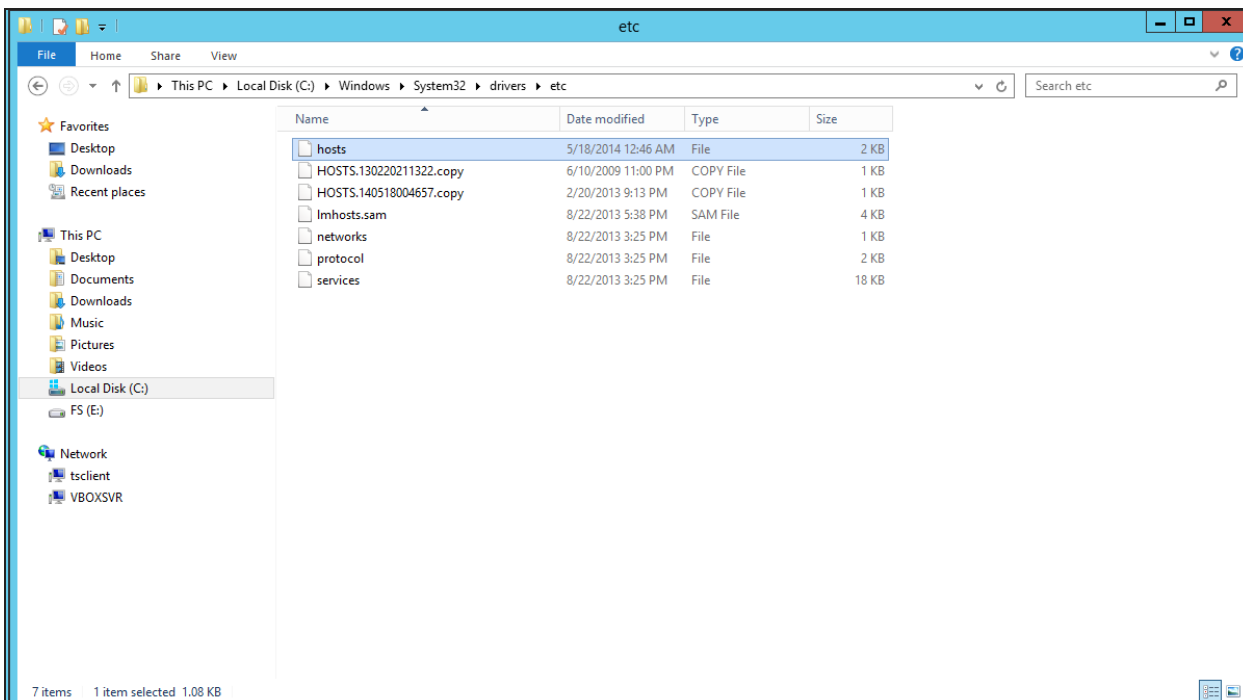
Up to 2 collectors are updated simultaneously.

## Run collectors in foreign (non-trusted) domains

To include resources from non-trusted domains in ARM, a collector is required in the non-trusted domain.

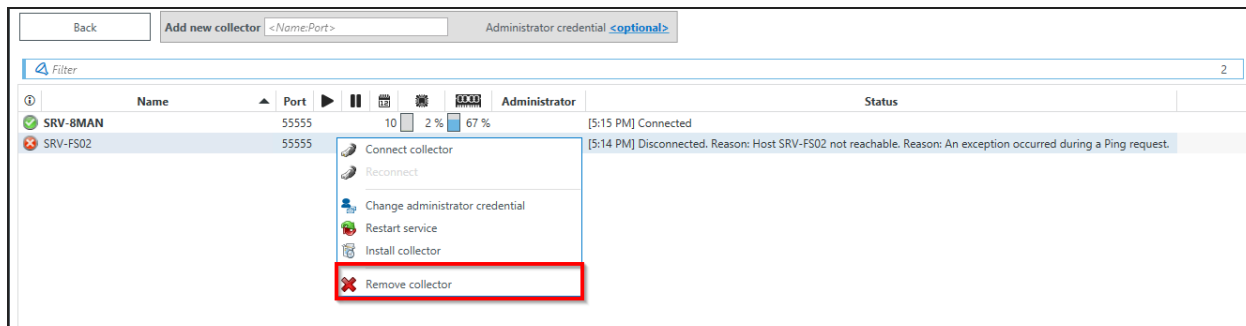
Depending on your network configuration, the automatic update mechanism for collectors may not work. In such cases the installation of this collector must be performed manually by using the setup, as described in [Install additional collectors](#).

Once installed, the collector must be added to the configuration. Collectors in foreign domains can be added immediately via the IP address.



To be able to use a name for the collector in foreign domains (non-trusted), you must extend the hosts files on both computers involved, that is, on the ARM server and on the collector server in the foreign domain.

## Remove collectors

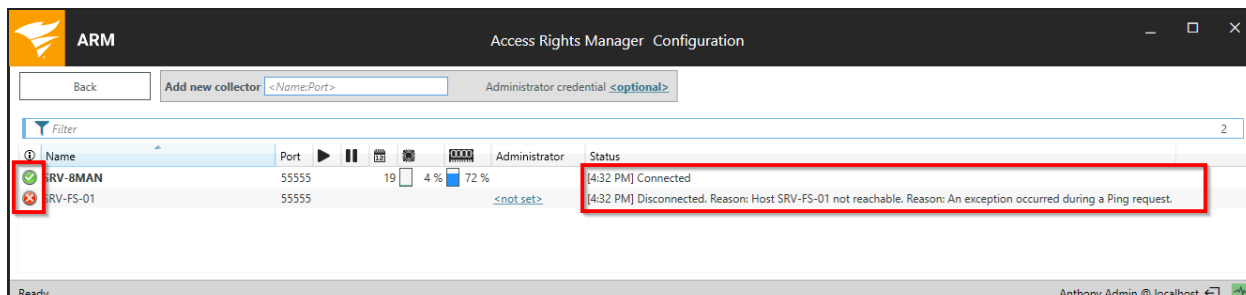


You can remove a collector by right-clicking on it and selecting "Remove collector" from the context menu.

**i** The installation on the target system remains intact. To remove the collector software from the target system, use the Windows control panel on the target system.

## Verify collector connection status

Start the [ARM Configuration application](#) and click the [Collectors](#) tile on the home screen.



ARM displays more details on the current connection status. If you see a red symbol in the first column, the collector is not available.

**i** Connection problems are mostly caused by firewalls. Please reference [firewall settings \(used ports overview\)](#).

## Perform a simple connection check

A simple check can be done by `ping`. If the ping was executed successfully, a firewall can still block the communication on port "55555".

The `tracert` command can be used to track where packets may be blocked. "External" firewalls can be identified in this way.

## Test a connection to the collector with the browser

Start a browser on the ARM server and call the address of the collector with port "55555".

*Example:*


```
"http://srv-fs01:55555"
```

*Communication blocked:*

After a timeout, you receive an error message that the page cannot be displayed.

*Communication successful:*

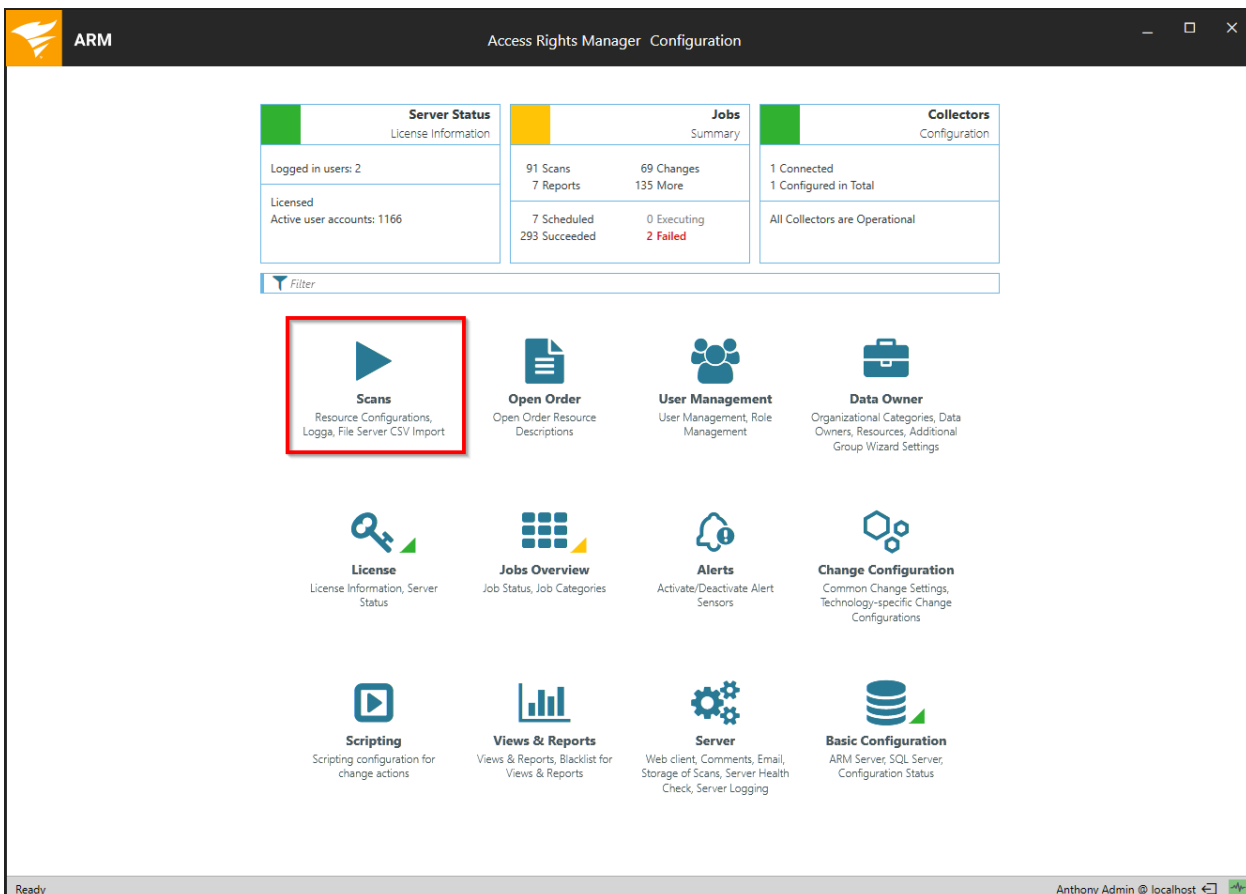
You will receive a message starting with ".Net..." and further containing "...expecting preamble...". This error message is generated by the ARM service.

 Run the browser test in both directions. Call the collector from the ARM server and vice versa. Communication must be possible bidirectionally.

## Configure scans and Logga

ARM scans access rights structures from different resource systems in configurable intervals. The scan results are stored in an SQL data base. Users can access these results quickly via the ARM GUI, as they are already located in the data base.

Events that occur in between scans are captured by the Logga features.

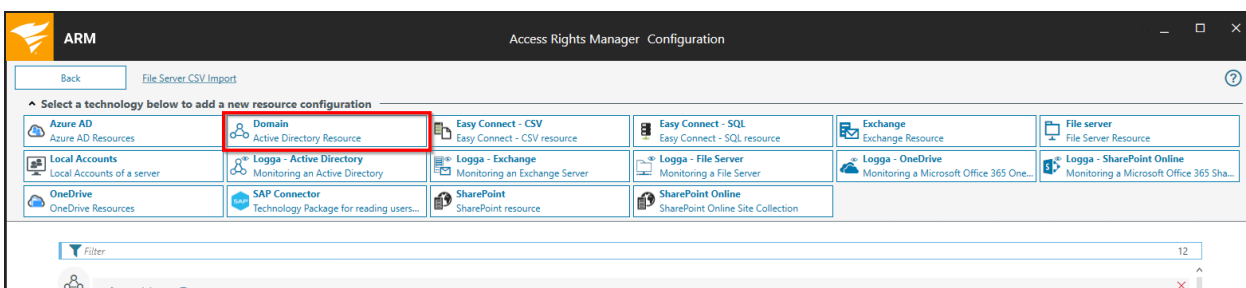


Click on "Scans" to configure resource scans and Logga settings.

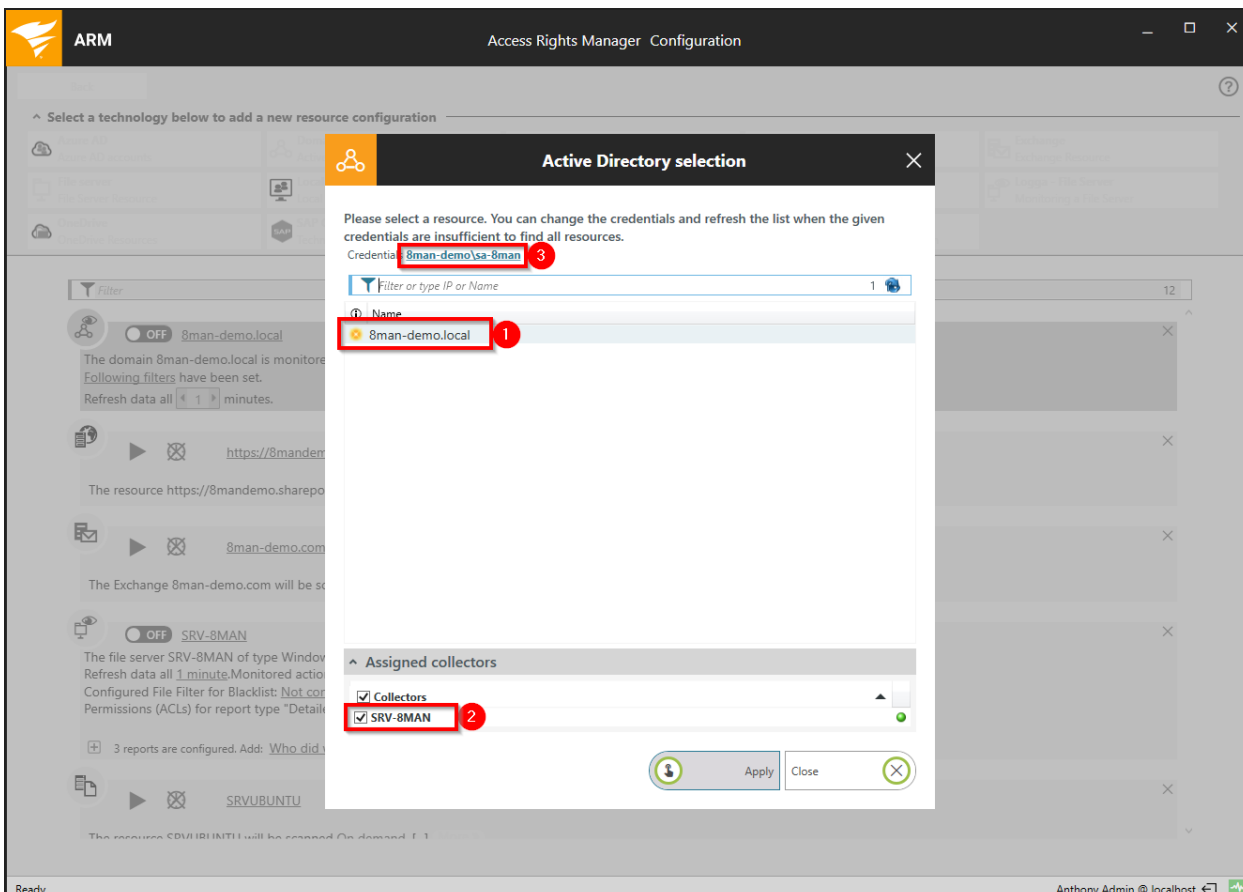
## Active Directory (AD) scans

### Add AD scans

On the start page of the configuration application, click on "Scans".



Click on Domain to add an AD scan.

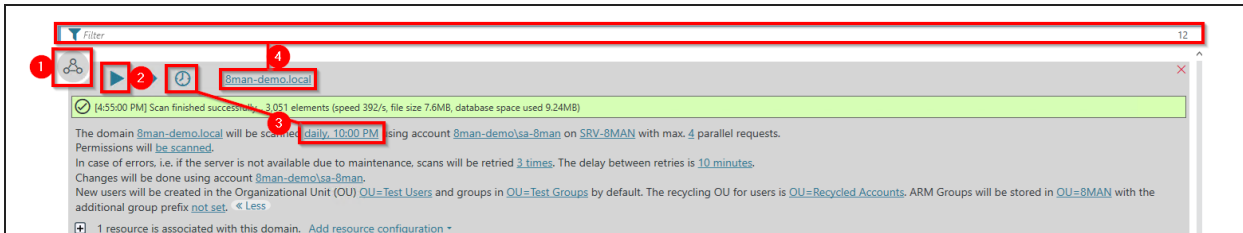


1. Select the desired domain for the AD scan.
2. Select a collector for the AD scan.
3. By default the credentials from the ARM server basic configuration will be used. You can specify different credentials.

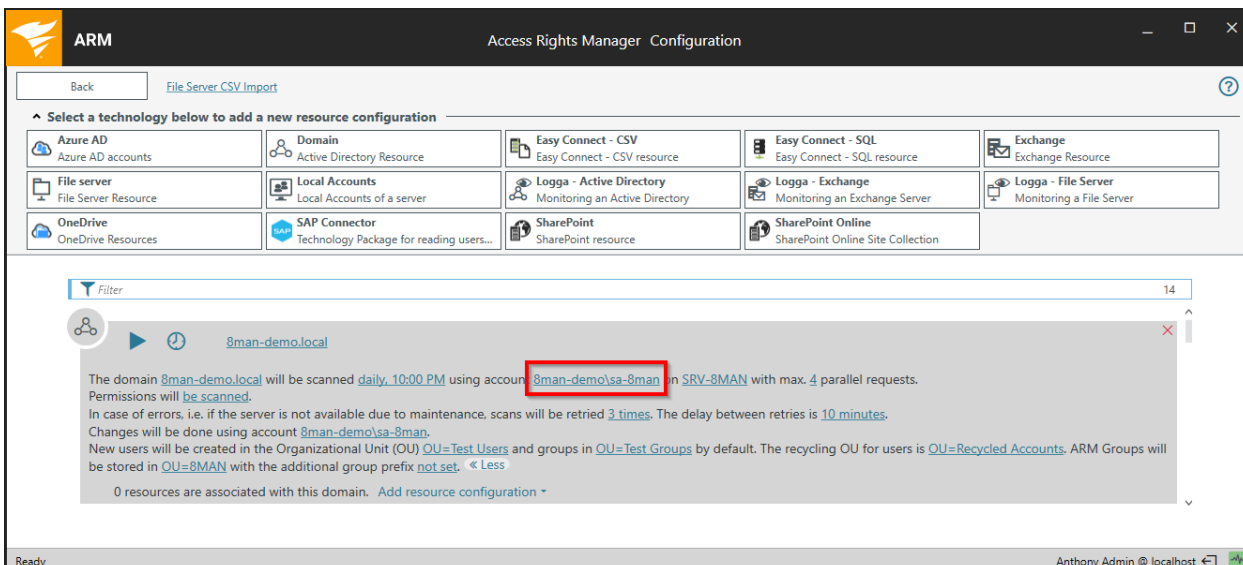
If the desired domain is not shown please check the following:

1. Are the credentials for the desired domain valid? Correct the entered information if necessary.
2. 8MAN licensing only: Is the desired domain included in the license? See: [License information](#)
3. Are the requirements for scanning foreign (non-trusted) domains met?
  - Is the collector service in the foreign domain running? See: [Collectors in foreign domains](#)
  - Is there a valid collector configuration? See: [Verify collector connection status](#)

## Configure AD scans



1. This icon is used for easy recognition of an AD scan configuration.
2. Start/Stop an AD scan. During and after a scan you can find information on the progress and the success of a scan in the light green box. Saved information about the scans of the last 14 days can be found in the [Job overview](#).
3. Set the schedule for the AD scan or disable the scheduled execution.
4. You can change the name of the Scan Configuration. If you have configured many resource scans, you can use the filter to quickly find a configuration.



Specify the credentials that will be used to perform the AD scan.

Follow our recommendation for [using service accounts](#).

ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

<b>Azure AD</b> Azure AD accounts	<b>Domain</b> Active Directory Resource	<b>Easy Connect - CSV</b> Easy Connect - CSV resource	<b>Easy Connect - SQL</b> Easy Connect - SQL resource	<b>Exchange</b> Exchange Resource
<b>File server</b> File Server Resource	<b>Local Accounts</b> Local Accounts of a server	<b>Logga - Active Directory</b> Monitoring an Active Directory	<b>Logga - Exchange</b> Monitoring an Exchange Server	<b>Logga - File Server</b> Monitoring a File Server
<b>OneDrive</b> OneDrive Resources	<b>SAP Connector</b> Technology Package for reading users...	<b>SharePoint</b> SharePoint resource	<b>SharePoint Online</b> SharePoint Online Site Collection	

Filter 14

8man-demo.local

The domain [8man-demo.local](#) will be scanned [daily, 10:00 PM](#) using account [8man-demo\sa-8man](#) or [SRV-8MAN](#) with max. [4](#) parallel requests. Permissions will be scanned.

In case of errors, i.e. if the server is not available due to maintenance, scans will be retried [3 times](#). The delay between retries is [10 minutes](#).

Changes will be done using account [8man-demo\sa-8man](#).

New users will be created in the Organizational Unit (OU) [OU=Test Users](#) and groups in [OU=Test Groups](#) by default. The recycling OU for users is [OU=Recycled Accounts](#). ARM Groups will be stored in [OU=8MAN](#) with the additional group prefix [not set](#). < Less

0 resources are associated with this domain. [Add resource configuration](#)

Ready Anthony Admin @ localhost

Determine which collector performs the scan.

You can select several collectors. ARM then automatically decides which collector will run the scan based on CPU load and memory usage.

ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

<b>Azure AD</b> Azure AD accounts	<b>Domain</b> Active Directory Resource	<b>Easy Connect - CSV</b> Easy Connect - CSV resource	<b>Easy Connect - SQL</b> Easy Connect - SQL resource	<b>Exchange</b> Exchange Resource
<b>File server</b> File Server Resource	<b>Local Accounts</b> Local Accounts of a server	<b>Logga - Active Directory</b> Monitoring an Active Directory	<b>Logga - Exchange</b> Monitoring an Exchange Server	<b>Logga - File Server</b> Monitoring a File Server
<b>OneDrive</b> OneDrive Resources	<b>SAP Connector</b> Technology Package for reading users...	<b>SharePoint</b> SharePoint resource	<b>SharePoint Online</b> SharePoint Online Site Collection	

Filter 14

8man-demo.local

The domain [8man-demo.local](#) will be scanned [daily, 10:00 PM](#) using account [8man-demo\sa-8man](#) on [SRV-8MAN](#) with max. [4](#) parallel requests. Permissions will be scanned.

In case of errors, i.e. if the server is not available due to maintenance, scans will be retried [3 times](#). The delay between retries is [10 minutes](#).

Changes will be done using account [8man-demo\sa-8man](#).

New users will be created in the Organizational Unit (OU) [OU=Test Users](#) and groups in [OU=Test Groups](#) by default. The recycling OU for users is [OU=Recycled Accounts](#). ARM Groups will be stored in [OU=8MAN](#) with the additional group prefix [not set](#). < Less

0 resources are associated with this domain. [Add resource configuration](#)

Ready Anthony Admin @ localhost

You can configure the number of parallel requests. The more parallel requests the faster the scan (non-linear) and the higher the CPU load.

Possible values are 1 (no parallel requests) to 128.



The screenshot shows the ARM Access Rights Manager Configuration window. At the top, there is a navigation bar with 'Back' and 'File Server CSV Import'. Below this is a section titled 'Select a technology below to add a new resource configuration' with a grid of 15 options: Azure AD, Domain, Easy Connect - CSV, Easy Connect - SQL, Exchange, File server, Local Accounts, Logga - Active Directory, Logga - Exchange, Logga - File Server, OneDrive, SAP Connector, SharePoint, and SharePoint Online. Below the grid is a filter bar showing 'Filter' and '14'. The main content area displays a configuration summary for the domain '8man-demo.local'. The text includes: 'The domain 8man-demo.local will be scanned daily, 10:00 PM using account 8man-demo\sa-8man on SRV-8MAN with max. 4 parallel requests. Permissions will be scanned.' (where 'be scanned.' is highlighted with a red box), 'In case of errors, i.e. if the server is not available due to maintenance, scans will be retried 3 times. The delay between retries is 10 minutes.', 'Changes will be done using account 8man-demo\sa-8man.', and 'New users will be created in the Organizational Unit (OU) OU=Test Users and groups in OU=Test Groups by default. The recycling OU for users is OU=Recycled Accounts. ARM Groups will be stored in OU=8MAN with the additional group prefix not\_set. < Less'. At the bottom, it says '0 resources are associated with this domain. Add resource configuration +'. The status bar at the bottom shows 'Ready' and 'Anthony Admin @ localhost'.

Specify for which Active Directory object classes the permissions are read.

This option is useful if you are working with delegation in AD.

## AD change configuration

This screenshot is identical to the one above, but with a red box highlighting the AD change configuration section. The highlighted text is: 'Changes will be done using account 8man-demo\sa-8man. New users will be created in the Organizational Unit (OU) OU=Test Users and groups in OU=Test Groups by default. The recycling OU for users is OU=Recycled Accounts. ARM Groups will be stored in OU=8MAN with the additional group prefix not\_set. < Less'.

The marked area shows the AD change configuration.

The screenshot shows the ARM Configuration window with the following resource configuration options:

<b>Azure AD</b> Azure AD accounts	<b>Domain</b> Active Directory Resource	<b>Easy Connect - CSV</b> Easy Connect - CSV resource	<b>Easy Connect - SQL</b> Easy Connect - SQL resource	<b>Exchange</b> Exchange Resource
<b>File server</b> File Server Resource	<b>Local Accounts</b> Local Accounts of a server	<b>Logga - Active Directory</b> Monitoring an Active Directory	<b>Logga - Exchange</b> Monitoring an Exchange Server	<b>Logga - File Server</b> Monitoring a File Server
<b>OneDrive</b> OneDrive Resources	<b>SAP Connector</b> Technology Package for reading users...	<b>SharePoint</b> SharePoint resource	<b>SharePoint Online</b> SharePoint Online Site Collection	

The detailed view for the domain `8man-demo.local` shows the following configuration:

- The domain `8man-demo.local` will be scanned **daily, 10:00 PM** using account `8man-demo\sa-8man` on `SRV-8MAN` with max. **4** parallel requests. Permissions will be **scanned**.
- In case of errors, i.e. if the server is not available due to maintenance, scans will be retried **3 times**. The delay between retries is **10 minutes**.
- Changes will be done using account `8man-demo\sa-8man`.
- New users will be created in the Organizational Unit (OU) `OU=Test Users` and groups in `OU=Test Groups` by default. The recycling OU for users is `OU=Recycled Accounts`. ARM Groups will be stored in `OU=8MAN` with the additional group prefix `not set`.

Specify logon information that ARM uses to apply changes to the AD.

If you leave the option set to "not set", the credentials will be prompted for each change.

Follow our recommendation for [using service accounts](#).

The screenshot shows the ARM Configuration window with the same resource configuration options as above. The detailed view for the domain `8man-demo.local` shows the following configuration:

- The domain `8man-demo.local` will be scanned **daily, 10:00 PM** using account `8man-demo\sa-8man` on `SRV-8MAN` with max. **4** parallel requests. Permissions will be **scanned**.
- In case of errors, i.e. if the server is not available due to maintenance, scans will be retried **3 times**. The delay between retries is **10 minutes**.
- Changes will be done using account `8man-demo\sa-8man`.
- New users will be created in the Organizational Unit (OU) `OU=Test Users` and groups in `OU=Test Groups` by default. The recycling OU for users is `OU=Recycled Accounts`. ARM Groups will be stored in `OU=8MAN` with the additional group prefix `not set`.

Configure in which OU you want ARM to create new users and groups.

If you leave this configuration on "not set" the user will need to chose the OU the first time they create a new user or group. ARM will memorize the choice depending on the user and will suggest it again the next time.

ARM Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

Azure AD Azure AD accounts	Domain Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource
File server File Server Resource	Local Accounts Local Accounts of a server	Logga - Active Directory Monitoring an Active Directory	Logga - Exchange Monitoring an Exchange Server	Logga - File Server Monitoring a File Server
OneDrive OneDrive Resources	SAP Connector Technology Package for reading users...	SharePoint SharePoint resource	SharePoint Online SharePoint Online Site Collection	

Filter 14

8man-demo.local

The domain 8man-demo.local will be scanned daily, 10:00 PM using account 8man-demo\sa-8man on SRV-8MAN with max. 4 parallel requests. Permissions will be scanned. In case of errors, i.e. if the server is not available due to maintenance, scans will be retried 3 times. The delay between retries is 10 minutes. Changes will be done using account 8man-demo\sa-8man. New users will be created in the Organizational Unit (OU) OU=Test Users and groups in OU=Test Groups by default. The recycling OU for users is OU=Recycled Accounts. ARM Groups will be stored in OU=8MAN with the additional group prefix not set. < Less

0 resources are associated with this domain. Add resource configuration +

Ready Anthonyv Admin @ localhost

Determine a recycling OU. The OU is used for the "soft delete" function.

ARM Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

Azure AD Azure AD accounts	Domain Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource
File server File Server Resource	Local Accounts Local Accounts of a server	Logga - Active Directory Monitoring an Active Directory	Logga - Exchange Monitoring an Exchange Server	Logga - File Server Monitoring a File Server
OneDrive OneDrive Resources	SAP Connector Technology Package for reading users...	SharePoint SharePoint resource	SharePoint Online SharePoint Online Site Collection	

Filter 14

8man-demo.local

The domain 8man-demo.local will be scanned daily, 10:00 PM using account 8man-demo\sa-8man on SRV-8MAN with max. 4 parallel requests. Permissions will be scanned. In case of errors, i.e. if the server is not available due to maintenance, scans will be retried 3 times. The delay between retries is 10 minutes. Changes will be done using account 8man-demo\sa-8man. New users will be created in the Organizational Unit (OU) OU=Test Users and groups in OU=Test Groups by default. The recycling OU for users is OU=Recycled Accounts. ARM Groups will be stored in OU=8MAN with the additional group prefix not set. < Less

0 resources are associated with this domain. Add resource configuration +

Ready Anthonyv Admin @ localhost

If using the group wizard, you can determine into which OU automatically created ARM groups are placed.

You are also able to add an ARM group prefix.

## Load additional LDAP attributes

This chapter details integrating additional Active Directory LDAP attributes into ARM that are not loaded by default.

The screenshot shows the 'Configuration - Active Directory' window in the ARM application. It is divided into several sections:

- Required properties:**
  - SAM account name:** Includes 'Users', 'Administrators', and 'Service accounts' tabs. The 'Users' tab is active, showing 'Preset' and 'Custom' options. A dropdown menu shows 'GIVENNAME Surname'. Below, a text box contains '{givenname} {sn}'. A note states: 'For the fictional user "Ulrike User" e. g. the following SAM account name will be suggested according to your rule definition: Ulrike User'.
  - Password options:** Includes 'Initial password' (1n17141P455w0rd), 'Hide password' checkbox, and 'Generate a new password with a length of 8 characters'. There are three checkboxes: 'The user must change the password at next logon' (checked), 'The user cannot change his password' (unchecked), and 'The password never expires' (unchecked).
- Quick info:** A section titled 'LDAP attributes' with a note: 'In this section you can select LDAP attributes that are optional for users and groups. Please select all attributes which shall be configurable when creating new users and group. Entries that you uncheck here will not appear in the Create User/Group overlay in ARM.'
- LDAP Attributes:** A section with 'Users', 'Groups', and 'Computers' tabs. The 'Users' tab is selected and highlighted with a red box. Below the tabs is a search filter 'Attribute name filter' with the value '27'. A table lists various LDAP attributes with checkboxes, aliases, creation rules, and validation rules.
 

Attribute	Alias	Creation Rule	Validation Rule
Account Expires (account...)			
Common Name (cn)			^.*w+.*\$
Comment (comment)			
Company (company)			
Department (department)			
Description (description)			
Display Name (displaynam...)			
Employee Id (employeeid)			
Job Category (employeey...)			
Given Name (givenname)			
Home Directory (homedir...)			
Home Drive (homedrive)			[a-zA-Z]:
Home Phone (homephone)			{1,64}
Information (info)			
Initials (initials)			
Email Address (mail)			
Manager (manager)			^[c][Nn]=.*\$
Mobile (mobile)			

In the ARM configuration application under Change Configuration > Active Directory you find all the attributes for users, groups and computers that are already loaded.

To add further attributes the `pnServer.config.xml` configuration file has to be edited. The file is located under:

```
%ProgramData%\protected-networks.com\8MAN\cfg
```

## Examples

The following example loads the additional attributes `employeetype` and `wWWHomePage`:

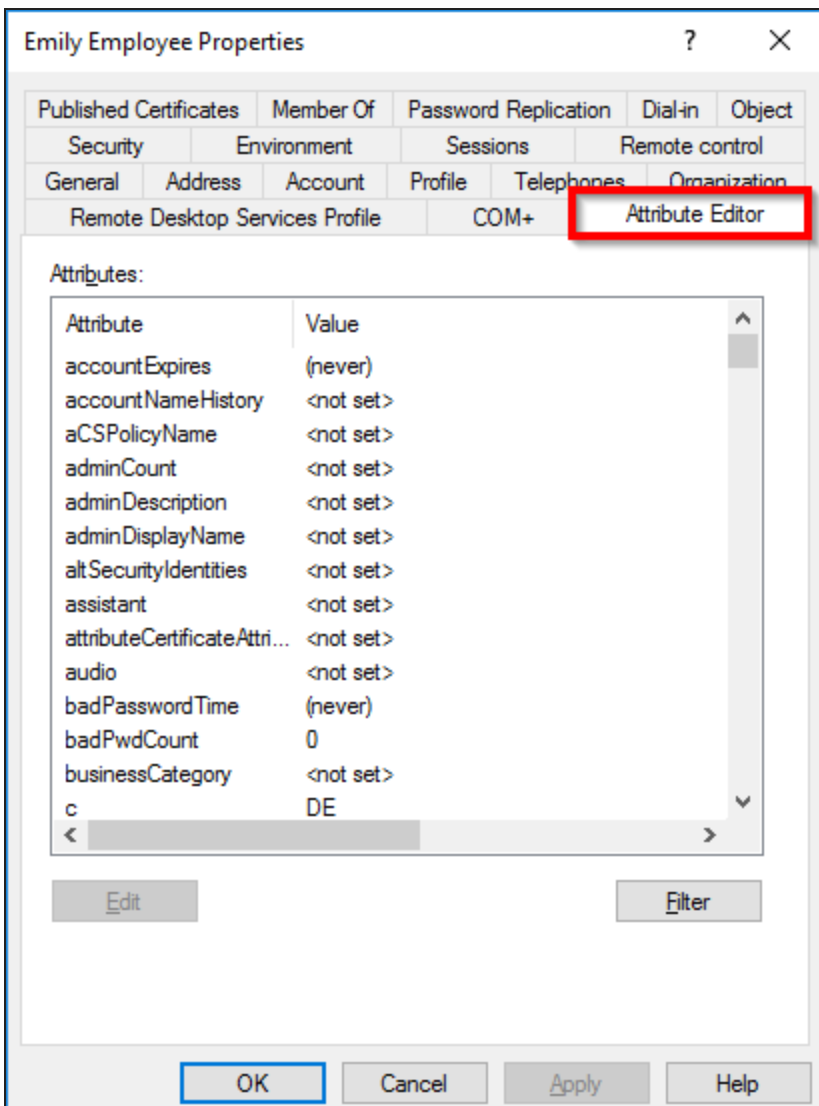
```
<changeConfiguration>
<activeDirectory>
<PropertiesToLoad
type="System.String">employeetype;wWWHomePage</PropertiesToLoad>
<PropertiesDetails>
<employeetype>
<AliasDisplayName type="System.String">Job Category</AliasDisplayName>
</employeetype>
```

```
<wWWHomePage>  
<AliasDisplayName type="System.String">Website</AliasDisplayName>  
</wWWHomePage>  
</PropertiesDetails>  
</activeDirectory>  
</changeConfiguration>
```

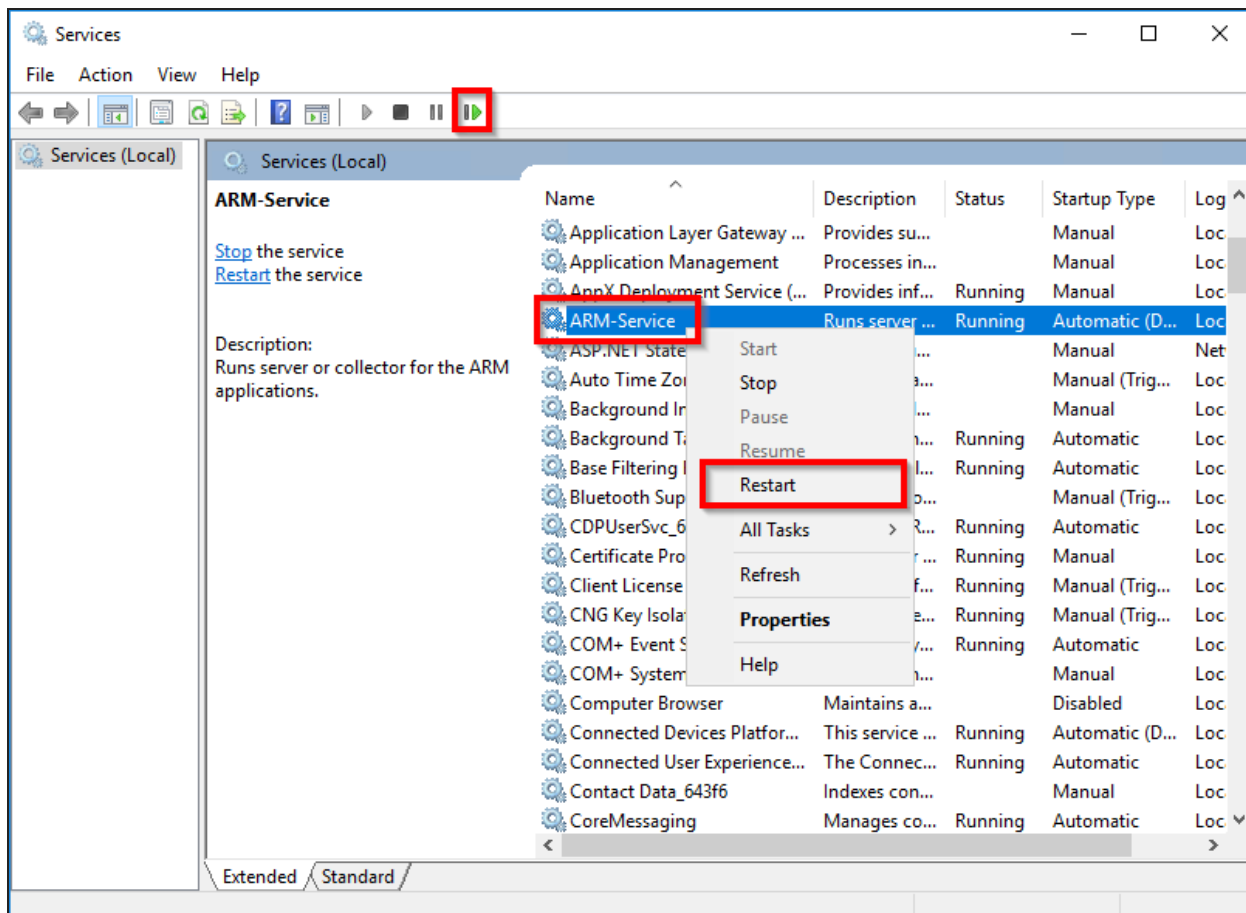
It is also possible to load attributes of type boolean:

```
<changeConfiguration>  
<activeDirectory>  
<PropertiesToLoad  
type="System.String">msExchHideFromAddressLists</PropertiesToLoad>  
<PropertiesDetails>  
<msExchHideFromAddressLists>  
<TypeInfo>System.Boolean</TypeInfo>  
<AllowOnlyDefinedValues type="System.String">>true</AllowOnlyDefinedValues>  
<DefinedValues type="System.String">FALSE;TRUE</DefinedValues>  
<IsChangeable type="System.String">>true</IsChangeable>  
<CreationRule type="System.String">FALSE</CreationRule>  
</msExchHideFromAddressLists>  
</PropertiesDetails>  
</activeDirectory>  
</changeConfiguration>
```





Under the tab "Attribute Editor" you will find the attribute names that must be used.



After saving the changes of the `pnServer.config.xml` file the ARM service must be restarted. The next AD scan will include the additional attributes.

In order to be able to use the additionally loaded attributes, these must be set as available. This is done for the ARM application in the AD [Change configuration](#) by setting the checkboxes there.

How to set the attributes available in the Web client is described in the following chapter: [Set attributes available to web client scenarios](#).

## Customize AD attributes properties

You can define "properties details" to AD attributes to standardize and simplify the process of creating new AD objects.

**⚠** Note that values entered with customized templates are not subject to the restrictions defined here.

The following properties are available:



## AliasDisplayName

Sets an alternate display name for the use in ARM.

*Example:*

```
<1>  
<AliasDisplayName type="System.String">City</AliasDisplayName>  
</1>
```

## AllowOnlyDefinedValues

Only predefined values can be selected. Use it together with `DefinedValues`.

*Example:*

```
<postalCode>  
<AllowOnlyDefinedValues type="System.String">true</AllowOnlyDefinedValues>  
<DefinedValues type="System.String">12345;67890</DefinedValues>  
</postalCode>
```

## DefinedValues

The predefined values for the attribute, separated by semicolons. The values are available in ARM as a drop down list. Use it together with `AllowOnlyDefinedValues`.

*Example:*

```
<postalCode>  
<AllowOnlyDefinedValues type="System.String">true</AllowOnlyDefinedValues>  
<DefinedValues type="System.String">12345;67890</DefinedValues>  
</postalCode>
```

## CreationRule

Defines a creation rule for the attribute.

*Example:*


```
<mail>  
<CreationRule type="System.String">{givenname}.{sn}@[fqdn]</CreationRule>  
</mail>
```

## ValidationRule

Regular expression for checking the entered value. Use it together with `ValidationInformation`.

*Example:*

```
<telephoneNumber>
<ValidationRule type="System.String">^[+]\d{1,4}[ ][^0]\d{1,5}[ ]\d{1,32}[-]\d{1,8}</ValidationRule>
<ValidationInformation type="System.String">The phone number does not match the requirements.</ValidationInformation>
</telephoneNumber>
```

 For help with regular expressions we recommend <https://regex101.com>.

## ValidationInformation

Displays a help text for the validation rule. Use it together with `ValidationRule`.

*Example:*

```
<telephoneNumber>
<ValidationRule type="System.String">^[+]\d{1,4}[ ][^0]\d{1,5}[ ]\d{1,32}[-]\d{1,8}</ValidationRule>
<ValidationInformation type="System.String">The phone number does not match the requirements.</ValidationInformation>
</telephoneNumber>
```

## IsRequired or Essential

The input is mandatory.

*Example:*

```
<streetAddress>
<IsRequired type="System.String">true</IsRequired>
</streetAddress>
```

## IsHidden

The Attribute is hidden in all ARM views and reports.

*Example:*

```
<streetAddress>
```

```
<IsHidden type="System.String">true</IsHidden>  
</streetAddress>
```

### IsChangeable

If set to true the value can not be modified within ARM. Not valid for creating objects. See also: [IsInitialConfigurable](#)

*Example:*

```
<streetAddress>  
<IsChangeable type="System.String">true</IsInitialConfigurable>  
</streetAddress>
```

### IsInitialConfigurable

If set to true the value can be modified during creating objects. See also: [IsInitialConfigurable](#)

*Example:*


```
<streetAddress>  
<IsInitialConfigurable type="System.String">true</IsInitialConfigurable>  
</streetAddress>
```

### SortIndex

Allows you to define the display order of the properties in the Account view, Creation overlay, and Edit overlay using an integer value. The smaller the value, the higher the attribute is placed.

*Example:*

```
<streetAddress>  
<SortIndex type="System.String">1500</SortIndex>  
</streetAddress>
```

 Please refer to the list of default LDAP properties and sort index values below.

### IsObjectSearchable

If set to true, the attribute is included in the ARM search for AD objects.

*Example:*

```
<streetAddress>  
<IsObjectSearchable type="System.String">true</IsObjectSearchable>
```

```
</streetAddress>
```

LDAP attributes that are read by default, and their sort index values

The following LDAP attributes ARM reads by default during an AD scan:

LDAP ATTRIBUTE	SORTINDEX DEFAULT
"accountexpires"	1000
"admincount"	2000
"cn"	3000
"comment"	4000
"company"	5000
"dc"	6000
"department"	7000
"description"	8000
"distinguishedname"	9000
"displayname"	10000
"employeeid"	11000
"employeeype"	11500
"flags"	12000
"givenname"	13000
"grouptype"	14000
"homedirectory"	15000
"homedrive"	16000
"homephone"	17000
"info"	18000
"initials"	19000
"jpegphoto"	50000
"thumbnailphoto"	51000
"lastlogon"	20000

LDAP ATTRIBUTE	SORTINDEX DEFAULT
"lastlogontimestamp"	21000
"managedby"	21250
"manager"	21500
"mail"	22000
"member"	23000
"memberof"	24000
"mobile"	25000
"name"	26000
"objectclass"	27000
"objectguid"	28000
"objectsid"	29000
"operatingsystem"	30000
"operatingsystemsservicepack"	31000
"operatingsystemversion"	32000
"ou"	33000
"personaltitle"	34000
"primarygroupid"	35000
"profilepath"	36000
"proxyaddresses"	36500
"samaccountname"	37000
"samaccounttype"	38000
"scriptpath"	39000
"sidhistory"	40000
"sn"	41000
"subrefs"	42000
"systemflags"	43000
"telephonenumber"	44000

LDAP ATTRIBUTE	SORTINDEX DEFAULT
"title"	45000
"useraccountcontrol"	46000
"userprincipalname"	47000

Set attributes available to web client scenarios


For the action "Change personal information" - available in the cockpit and some web client scenarios - ARM loads a standard set of attributes. The standard set is the same for all roles. You can adjust which attributes are available for each ARM role.

To do this, you need to extend the `pnservice.config.xml` located at the following location:

```
%programdata%\protected-networks.com\8MAN\cfg
```

 The changes will be applied without restarting the ARM service.

## Example

 The line numbers are for explanation purposes only.

```
01 <WebClient.Cockpit.ChangeAttributes.Manager>
02 postalCode;physicalDeliveryOfficeName;telephoneNumber;facsimileTelephoneNumber
03 </WebClient.Cockpit.ChangeAttributes.Manager>
```

### Line 01 and 03

Specify which role the configuration should apply to. The following roles are possible:

*ARM role*

```
WebClient.Cockpit.ChangeAttributes.Administrator
WebClient.Cockpit.ChangeAttributes.JuniorAdministrator
WebClient.Cockpit.ChangeAttributes.DataOwner0
WebClient.Cockpit.ChangeAttributes.DataOwner1
WebClient.Cockpit.ChangeAttributes.DataOwner2
WebClient.Cockpit.ChangeAttributes.DataOwner3
WebClient.Cockpit.ChangeAttributes.DataOwner4
WebClient.Cockpit.ChangeAttributes.Read
```

WebClient.Cockpit.ChangeAttributes.Requester

WebClient.Cockpit.ChangeAttributes.Manager

*Self Service in the cockpit: "Change my personal information"*

WebClient.Cockpit.ChangeAttributes.SelfService

## Line 02

List of attributes to be available. You can only use attributes that are included in the AD scan.

## Start AD scans

The screenshot shows the ARM Configuration window. At the top, there's a navigation bar with 'ARM' and 'Access Rights Manager Configuration'. Below that, there's a 'Back' button and a 'File Server CSV Import' link. A section titled 'Select a technology below to add a new resource configuration' contains a grid of options: Azure AD, Domain, Easy Connect - CSV, Easy Connect - SQL, Exchange, File server, Local Accounts, Logga - Active Directory, Logga - Exchange, Logga - File Server, OneDrive, SAP Connector, and SharePoint Online. Below this grid is a 'Filter' input field with '14' items. A red box highlights a play button icon next to the domain '8man-demo.local'. Below the play button, a green bar indicates a successful scan: '[11:59:31 AM] Scan finished successfully... 2,996 elements (speed 351/s, file size 7.39MB, database space used 9.12MB)'. The main content area contains detailed scan configuration information, including the account used, scan frequency, and error handling. At the bottom, it shows '0 resources are associated with this domain' and a link to 'Add resource configuration'.

Start/cancel an AD scan. Typically AD scans only take a couple of minutes.

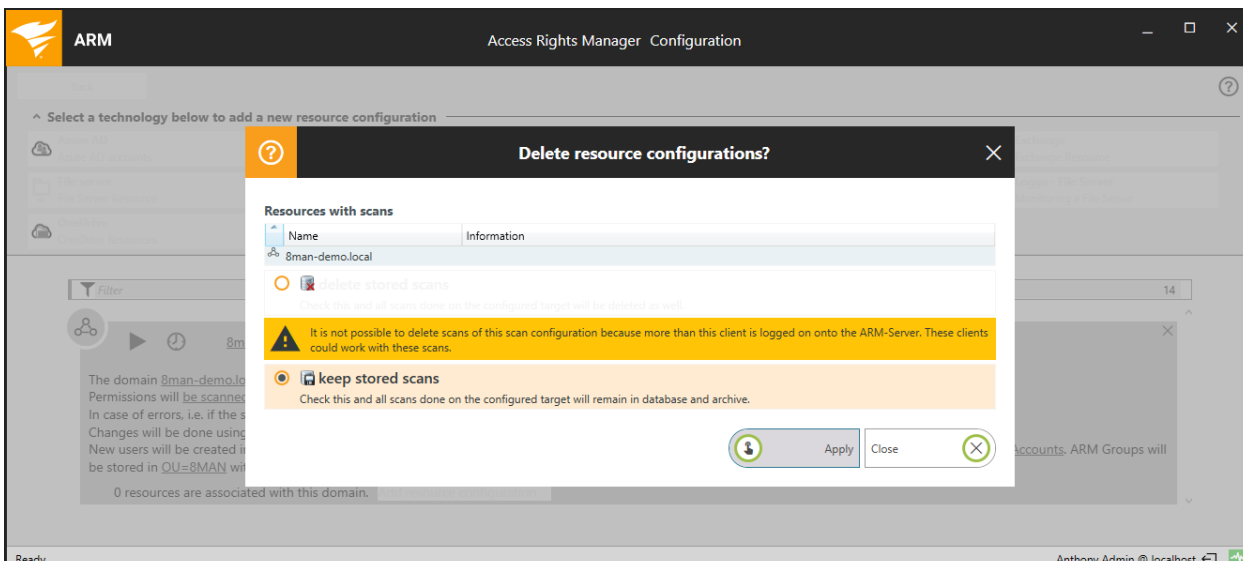
Status information is shown during and after the AD scan.

**i** These are no longer shown if you leave and re-enter the scan menu. You can find the information in [Job overview](#).

### Delete AD scan configurations

Delete an AD scan configuration.



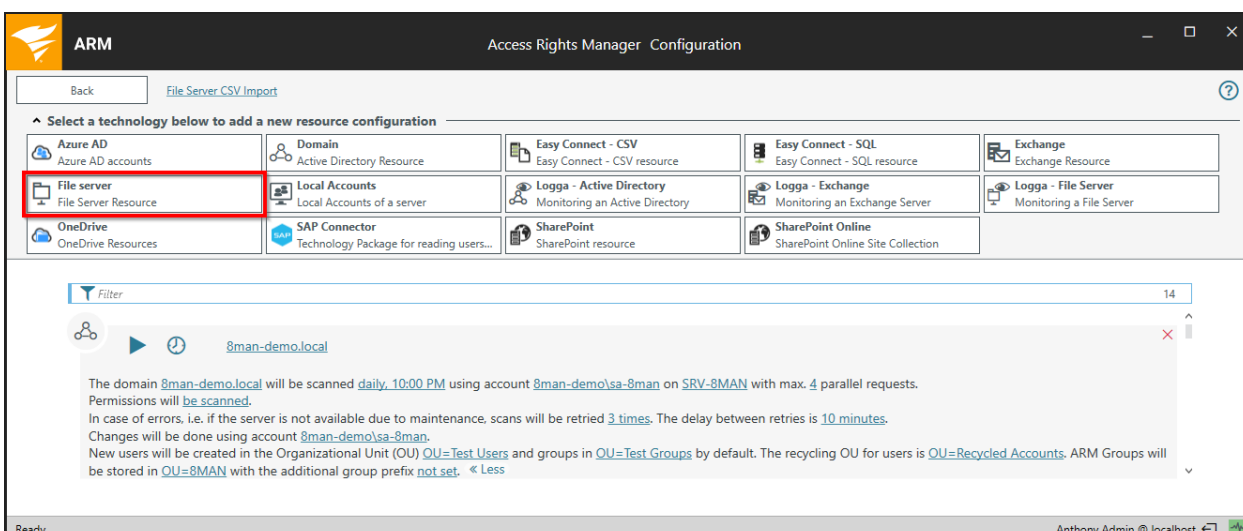


If you delete a scan configuration, you can either keep or delete the stored scan data.

**i** Deleting is only possible if all other ARM applications are closed. You can [identify logged in users](#) in the Server status section.

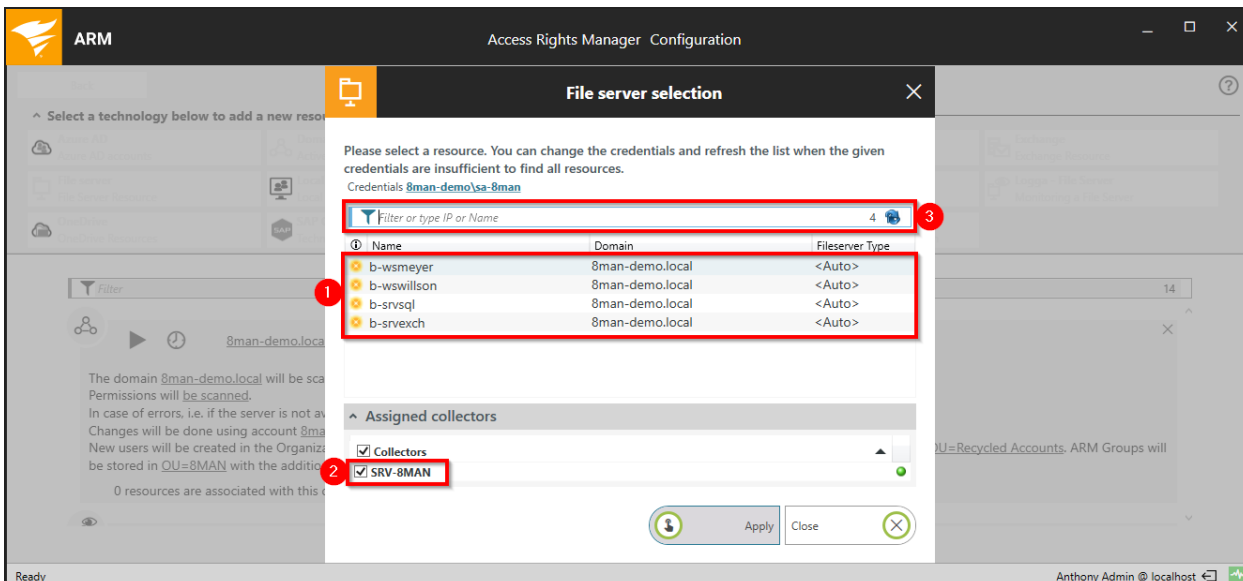
## File server (FS) scans

### Add FS scans

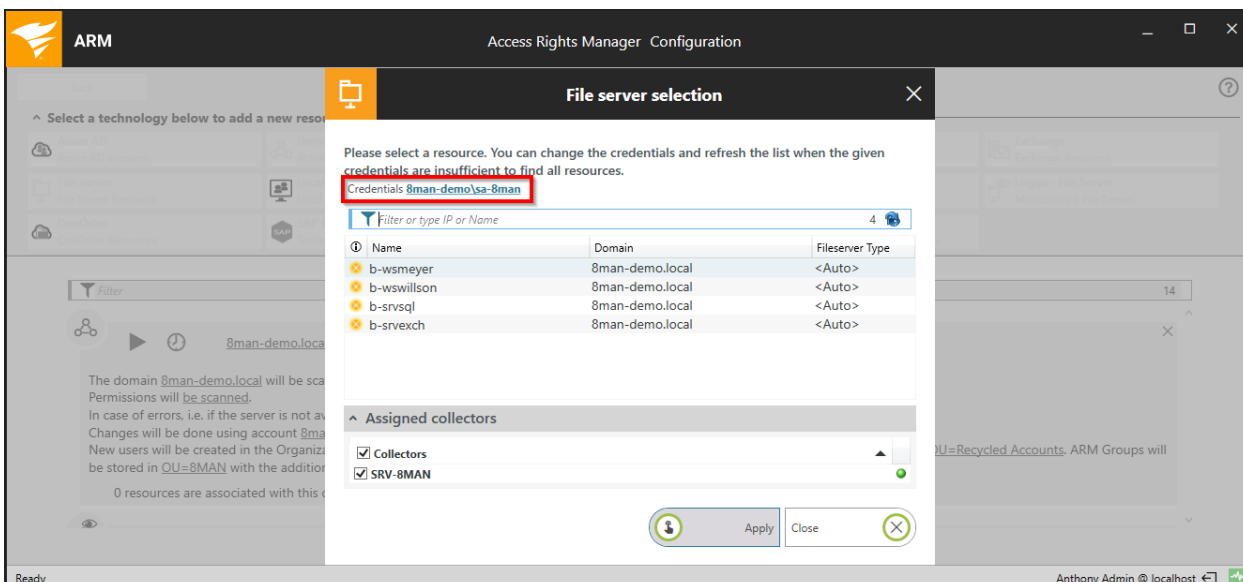


Click on "File server" to add an FS scan.

**i** To scan file servers in foreign (non-trusted) domains, a collector is mandatory in the foreign domain. See [Collectors in foreign domains](#).



1. Select the desired file server. The list of computers is loaded from AD (no AD scan needed).
2. Select a collector for the FS scan.
3. You can also enter a (not listed) name into the filter / search field.



By default the [ARM server basic configuration](#) credentials will be used.

If the desired file server is not shown please check the following:

- Are the credentials for the desired domain valid? Change the entered information if necessary.
- If the requirements for scanning in foreign (non-trusted) domains are adhered to: [Scan file servers in foreign \(non-trusted\) domains](#)

**i** If the scan configuration is invalid you will see an error message at the start of the scan. This will also be recorded in a [Logfile](#).

## Import FS scan configurations

The screenshot shows the 'Access Rights Manager Configuration' window. The 'File Server CSV Import' option is highlighted in a red box. Below the navigation menu, there is a grid of technology options for adding new resource configurations. A detailed configuration card for '8man-demo.local' is visible, showing scan frequency, account, and other settings.

Select a technology below to add a new resource configuration				
<b>Azure AD</b> Azure AD accounts	<b>Domain</b> Active Directory Resource	<b>Easy Connect - CSV</b> Easy Connect - CSV resource	<b>Easy Connect - SQL</b> Easy Connect - SQL resource	<b>Exchange</b> Exchange Resource
<b>File server</b> File Server Resource	<b>Local Accounts</b> Local Accounts of a server	<b>Logga - Active Directory</b> Monitoring an Active Directory	<b>Logga - Exchange</b> Monitoring an Exchange Server	<b>Logga - File Server</b> Monitoring a File Server
<b>OneDrive</b> OneDrive Resources	<b>SAP Connector</b> Technology Package for reading users...	<b>SharePoint</b> SharePoint resource	<b>SharePoint Online</b> SharePoint Online Site Collection	

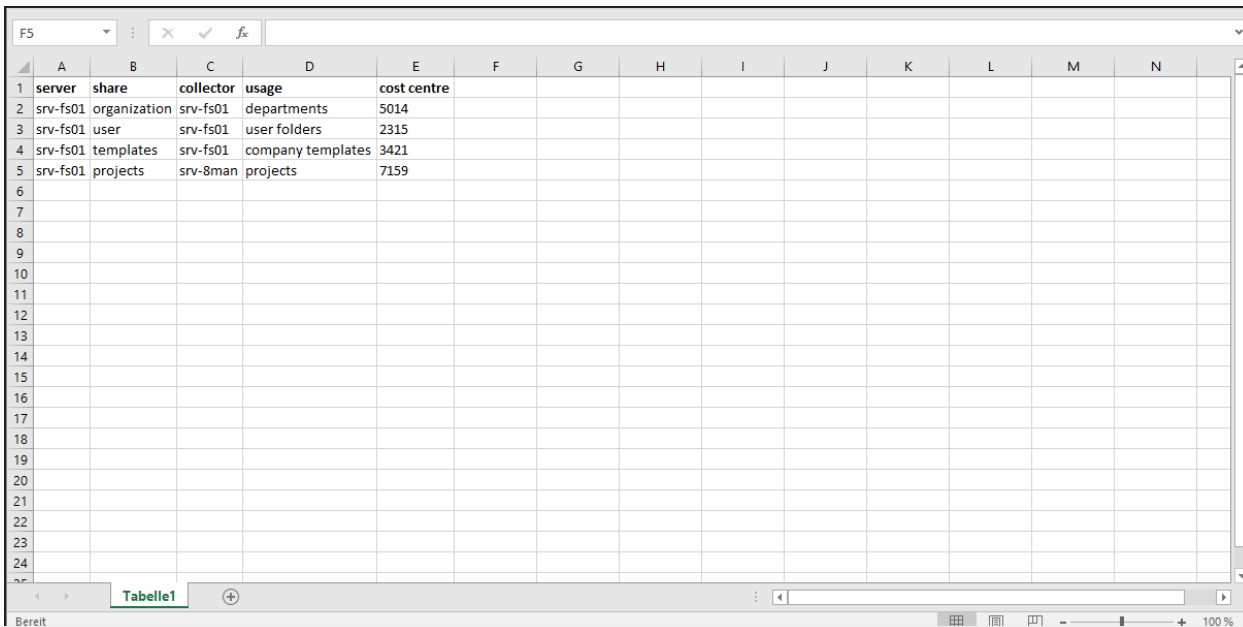
**8man-demo.local**

The domain **8man-demo.local** will be scanned **daily, 10:00 PM** using account **8man-demo\sa-8man** on **SRV-8MAN** with max. **4** parallel requests. Permissions will **be scanned**.  
 In case of errors, i.e. if the server is not available due to maintenance, scans will be retried **3 times**. The delay between retries is **10 minutes**.  
 Changes will be done using account **8man-demo\sa-8man**.  
 New users will be created in the Organizational Unit (OU) **OU=Test Users** and groups in **OU=Test Groups** by default. The recycling OU for users is **OU=Recycled Accounts**. ARM Groups will be stored in **OU=8MAN** with the additional group prefix **not set**. [« Less](#)

0 resources are associated with this domain. [Add resource configuration](#)

Click on "File server CSV import" to import a file server configuration file.

We recommend using the CSV import functionality to manage a large number of FS scan configurations and add these to ARM with just a few clicks.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	server	share	collector	usage	cost centre									
2	srv-fs01	organization	srv-fs01	departments	5014									
3	srv-fs01	user	srv-fs01	user folders	2315									
4	srv-fs01	templates	srv-fs01	company templates	3421									
5	srv-fs01	projects	srv-8man	projects	7159									
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														


The CSV file must contain, at minimum, the following columns:


- "Server"
- "Share" or "freigabe"

Optional columns:

- "Collector" or "kollektor"
- additional descriptions

Choose tab or semi-colon as a delimiter.

 If the column "collector" is not created, then the collector defined in the import dialog will be used for all scan configurations.

 Do not use the following descriptions as column headers: "Bemerkung", "description", "Präfix", "prefix"

**File server CSV import**

This is a preview of the shares which will be imported. Please make sure everything is correct and specify some common settings to use for all scans.

Server	Share	Collector	usage	cost centre
srv-fs01	organization	srv-fs01	departments	5014
srv-fs01	user	srv-fs01	user folders	2315
srv-fs01	templates	srv-fs01	company te...	3421
srv-fs02	projects	srv-8man	projects	7159

**Settings:**

Collector:   
(Only if not set in CSV file)

Start time:  
 On demand  
Do not schedule, the task will only be started on demand.

**Daily** **Settings**

Weekly

Monthly

Quarterly

Yearly

Hour:  Minute:

Time zone:

User account:  
Credentials:  
User name:   
Password:   
Domain:

Max. parallel requests:


File server type:  
 Detect automatically  
 Windows  EMC  
 NetApp  DFS

Delete all existing file server resources

**keep stored scans**  
Check this and all scans done on the configured target will remain in database and archive.

Determine the import settings:

- which collector(s) perform(s) scans (only required if not included in the CSV file)
- at what time the scans are performed
- how many parallel requests are performed
- file server type
- if previously entered scan configurations should be deleted

 The settings in the import dialog are valid for all shares.

## Configure FS scans

ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

<b>Azure AD</b> Azure AD accounts	<b>Domain</b> Active Directory Resource	<b>Easy Connect - CSV</b> Easy Connect - CSV resource	<b>Easy Connect - SQL</b> Easy Connect - SQL resource	<b>Exchange</b> Exchange Resource
<b>File server</b> File Server Resource	<b>Local Accounts</b> Local Accounts of a server	<b>Logga - Active Directory</b> Monitoring an Active Directory	<b>Logga - Exchange</b> Monitoring an Exchange Server	<b>Logga - File Server</b> Monitoring a File Server
<b>OneDrive</b> OneDrive Resources	<b>SAP Connector</b> Technology Package for reading users...	<b>SharePoint</b> SharePoint resource	<b>SharePoint Online</b> SharePoint Online Site Collection	

Filter 14

srv-8man

The file server `srv-8man` of type `Windows` will be scanned `daily, 10:10 PM` using account `8man-demo\sa-8man` on `SRV-8MAN` with max. `4` parallel requests. The following shares will be scanned during the scheduled scans: `Organization, Projects, Templates, Test, Users`. The depth of the file server scan will be `unlimited`. From a depth of `8` and on only different rights will be reported. In case of errors, i.e. if the server is not available due to maintenance, scans will be retried `3 times`. The delay between retries is `10 minutes`.

The change account and the list right management have moved to [File Server change configuration](#). < Less

Ready Anthony Admin @ localhost

Edit the name of the FS scan configuration.

ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

<b>Azure AD</b> Azure AD accounts	<b>Domain</b> Active Directory Resource	<b>Easy Connect - CSV</b> Easy Connect - CSV resource	<b>Easy Connect - SQL</b> Easy Connect - SQL resource	<b>Exchange</b> Exchange Resource
<b>File server</b> File Server Resource	<b>Local Accounts</b> Local Accounts of a server	<b>Logga - Active Directory</b> Monitoring an Active Directory	<b>Logga - Exchange</b> Monitoring an Exchange Server	<b>Logga - File Server</b> Monitoring a File Server
<b>OneDrive</b> OneDrive Resources	<b>SAP Connector</b> Technology Package for reading users...	<b>SharePoint</b> SharePoint resource	<b>SharePoint Online</b> SharePoint Online Site Collection	

Filter 14

srv-8man

The file server `srv-8man` of type `Windows` will be scanned `daily, 10:10 PM` using account `8man-demo\sa-8man` on `SRV-8MAN` with max. `4` parallel requests. The following shares will be scanned during the scheduled scans: `Organization, Projects, Templates, Test, Users`. The depth of the file server scan will be `unlimited`. From a depth of `8` and on only different rights will be reported. In case of errors, i.e. if the server is not available due to maintenance, scans will be retried `3 times`. The delay between retries is `10 minutes`.

The change account and the list right management have moved to [File Server change configuration](#). < Less

Ready Anthony Admin @ localhost

Schedule the FS scan by clicking on the clock icon or the link in the text. You can also deactivate the scheduling functionality.

ARM Access Rights Manager Configuration

Back File\_Server\_CSV\_Import

Select a technology below to add a new resource configuration

Azure AD Azure AD accounts	Domain Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource
File server File Server Resource	Local Accounts Local Accounts of a server	Logga - Active Directory Monitoring an Active Directory	Logga - Exchange Monitoring an Exchange Server	Logga - File Server Monitoring a File Server
Logga - OneDrive Monitoring a Microsoft Office 365 One...	Logga - SharePoint Online Monitoring a Microsoft Office 365 Sha...	OneDrive OneDrive Resources	SAP Connector Technology Package for reading users...	SharePoint SharePoint resource

Filter 14

srv-8man

The file server **srv-8man** of type **Windows** will be scanned **daily, 10:10 PM** using account **8man-demo\sa-8man** on **SRV-8MAN** with max. **4** parallel requests. The following shares will be scanned during the scheduled scans: **Organization, Projects, Templates, Test, Users**. The depth of the file server scan will be **unlimited**. From a depth of **8** and on only different rights will be reported. In case of errors, i.e. if the server is not available due to maintenance, scans will be retried **3 times**. The delay between retries is **10 minutes**.

The change account and the list right management have moved to [File Server change configuration](#). < Less

Ready Anthony Admin @ localhost

You can change the file server for which this scan configuration is valid.

ARM Access Rights Manager Configuration

Select a technology below to add a new resource configuration

Filter 14

srv-8man

The file server **srv-8man** of type **Windows** will be scanned **daily, 10:10 PM** using account **8man-demo\sa-8man** on **SRV-8MAN** with max. **4** parallel requests. The following shares will be scanned during the scheduled scans: **Organization, Projects, Templates, Test, Users**. The depth of the file server scan will be **unlimited**. From a depth of **8** and on only different rights will be reported. In case of errors, i.e. if the server is not available due to maintenance, scans will be retried **3 times**. The delay between retries is **10 minutes**.

The change account and the list right management have moved to [File Server change configuration](#).

Ready Anthony Admin @ localhost

**Scan options**

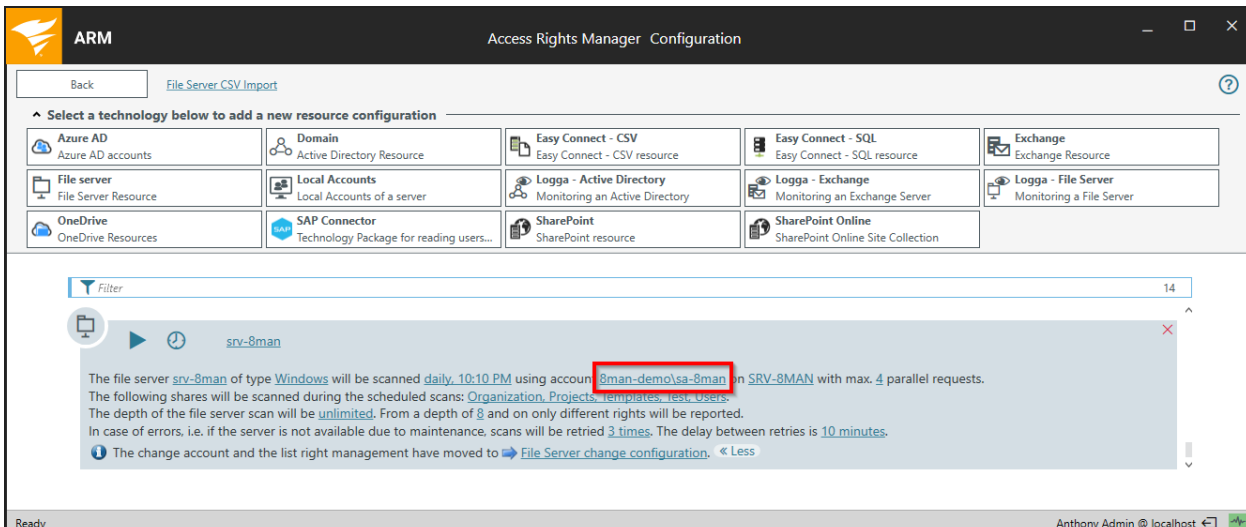
Max. parallel requests  
4 You can change the number of parallel requests during scans. This may speed up the scan process.

File server type  
 Detect automatically  
 Windows  EMC  
 NetApp  DFS

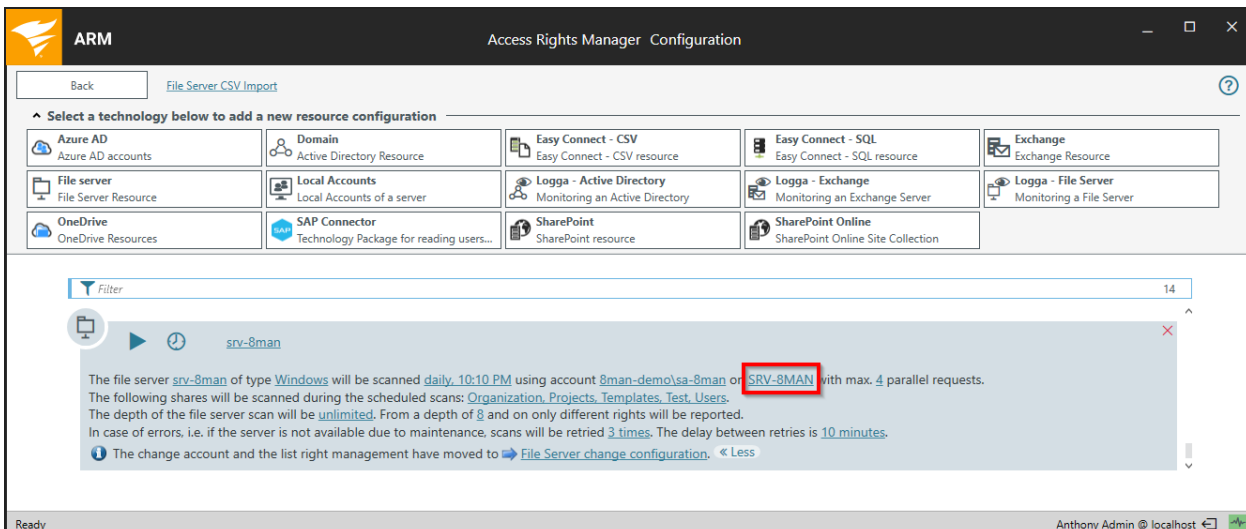
Apply Close

1. Configure the number of parallel requests. The more parallel requests the faster the scan and the higher the CPU load. Possible values are 1 (no parallel requests) to 128.
2. Set the file server type.

**NOTE:** ARM detects Windows/DFS file server types automatically. For NetApp and EMC, you must set the correct type for optimal performance.



Determine which credentials are used to perform the FS scan.  
Please reference the following section: [Service accounts](#).



Determine which collectors are used to perform the scan. If you have configured several collectors, ARM will automatically determine which collector to use based upon CPU load and RAM usage.



ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

Azure AD Azure AD accounts	Domain Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource
File server File Server Resource	Local Accounts Local Accounts of a server	Logga - Active Directory Monitoring an Active Directory	Logga - Exchange Monitoring an Exchange Server	Logga - File Server Monitoring a File Server
OneDrive OneDrive Resources	SAP Connector Technology Package for reading users...	SharePoint SharePoint resource	SharePoint Online SharePoint Online Site Collection	

Filter 14

srv-8man

The file server `srv-8man` of type `Windows` will be scanned `daily, 10:10 PM` using account `8man-demo\sa-8man` on `SRV-8MAN` with max. `4` parallel requests.  
 The following shares will be scanned during the scheduled scans: `Organization, Projects, Templates, Test, Users`.  
 The depth of the file server scan will be `unlimited`. From a depth of `8` and on only different rights will be reported.  
 In case of errors, i.e. if the server is not available due to maintenance, scans will be retried `3` times. The delay between retries is `10` minutes.

The change account and the list right management have moved to [File Server change configuration](#). < Less

Ready Anthony Admin @ localhost

Determine the shares that will be scanned.

ARM Access Rights Manager Configuration

Select a technology below to add a new resource configuration

Depth of scan

Please specify to what depth to be scanned.  
 To save disk space, you can specify from which scan depth on only paths with changed permissions will be stored in the database.

Maximum depth of scan

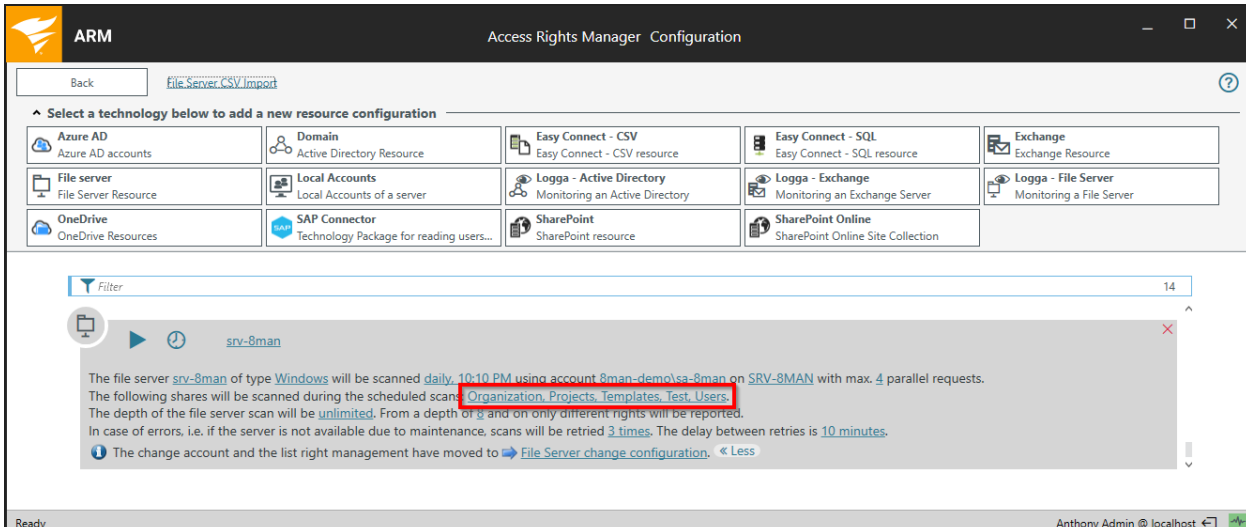
Depth of scan after which only changes will be saved

Apply Cancel

Ready Anthony Admin @ localhost

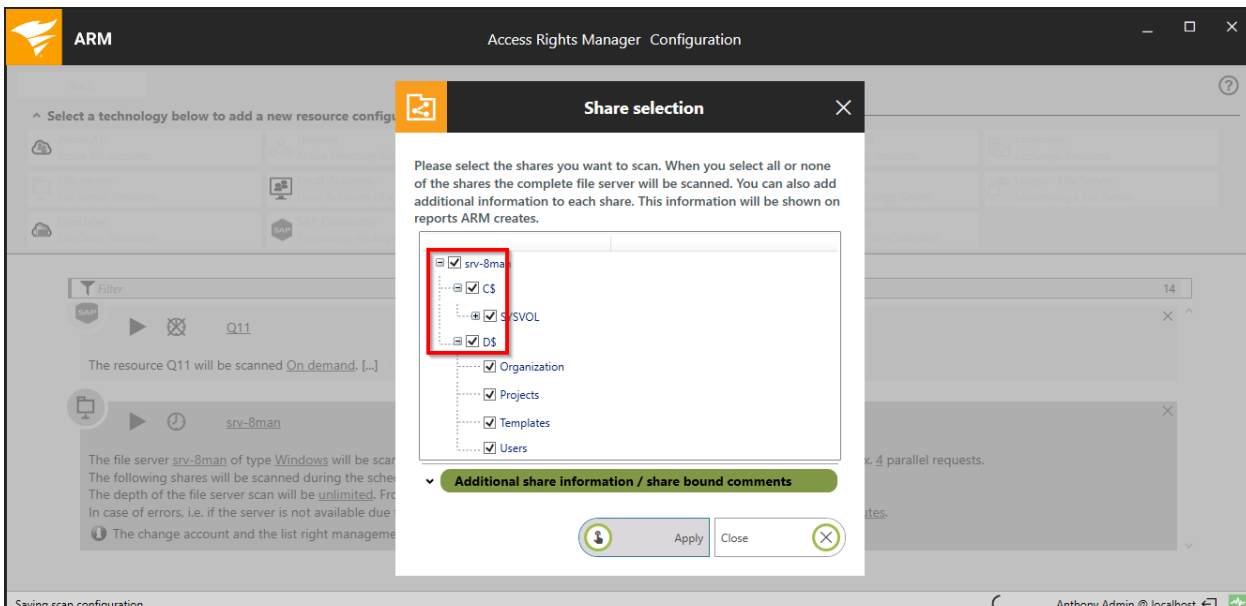
1. Determine the scan depth.
2. To save storage space, you can specify from which depth only paths with deviating permissions are stored.

## Select shares



To ensure optimal results for reports and viewing information in the ARM resource view, consider the following points when selecting shares.

## Unfavorable



A selection of these shares will result in the following resource view:

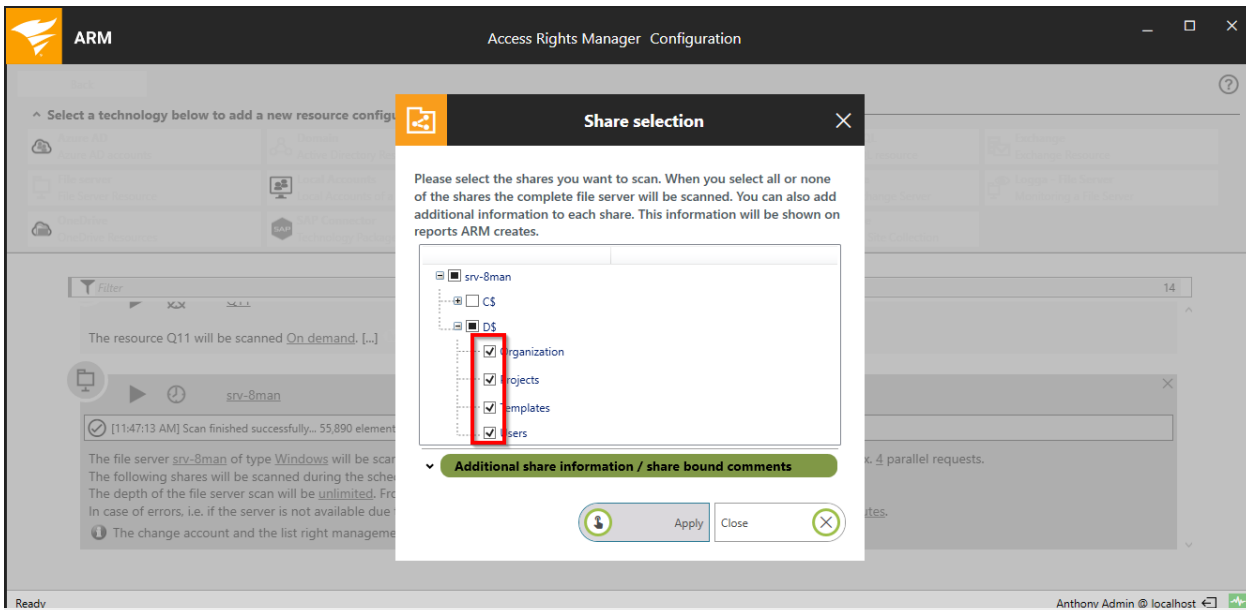
The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main window shows a tree view of resources under the 'File server' section. The 'Organization' folder is highlighted in red in the tree view, and its full path, '\\srv-8man\D\$\Organization', is also highlighted in red in the right-hand pane. A red arrow points from the 'Organization' folder in the tree view to the 'Organization' folder in the right-hand pane. The right-hand pane shows the 'Organization' folder's properties, including its full path, owner, inheritance, and access rights.

Name	how often granted	Inhe
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	
Administrator (8man-demo\Administrator)	1	
Anthony Admin (8man-demo\Anthony Admin)	1	
Antoine Admin (8man-demo\Antoine Admin)	1	
Anton Admin (8man-demo\Anton Admin)	1	
NT AUTHORITY\SYSTEM	1	
sa-8man (8man-demo\sa-8man)	1	

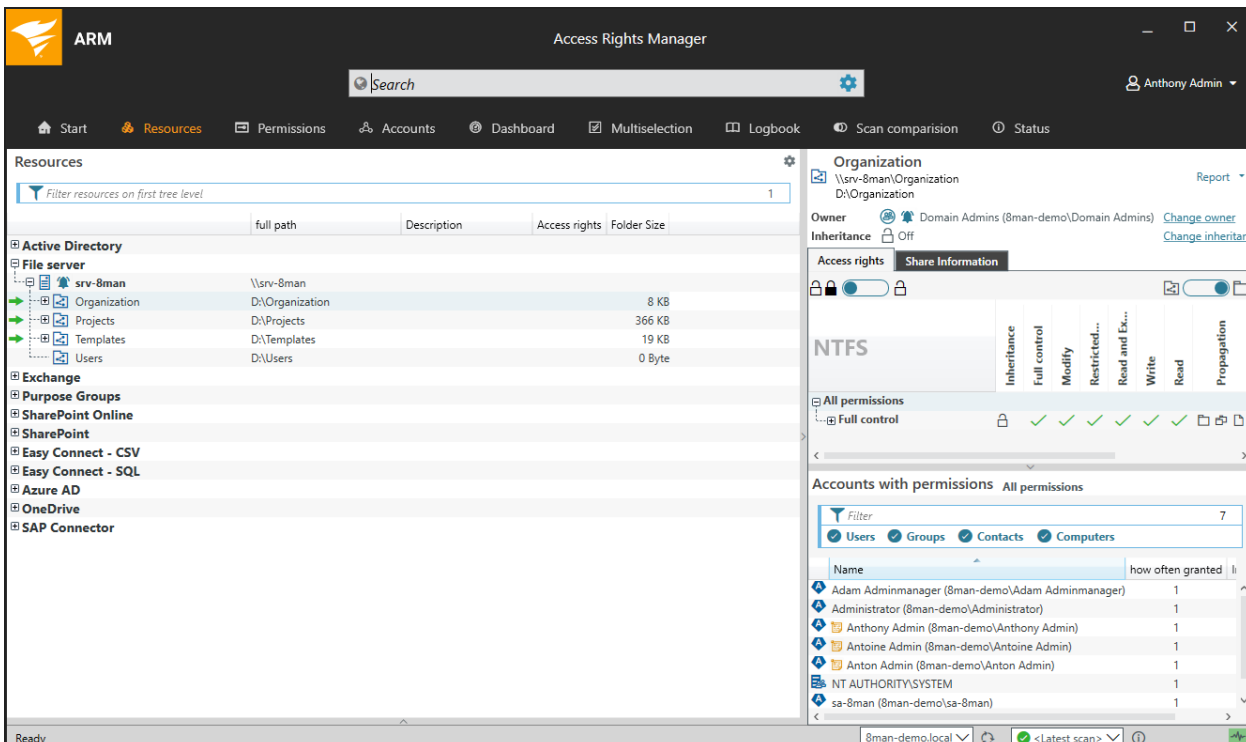
Folders are shown twice (for example "Organization").

This may result in confusing access group names created by the group wizard, as well as unclear and confusing reports and views.

## Ideal

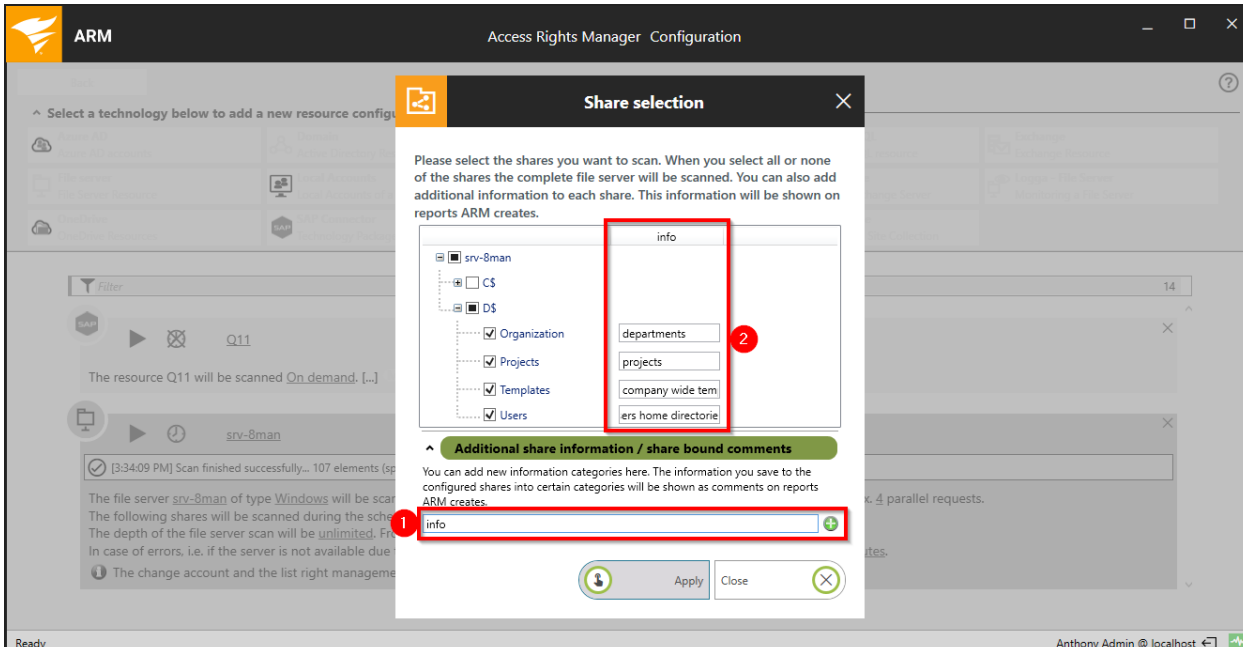


Only select shares, which are entry points and visible/relevant for users.



The permissions are displayed in the usual manner in the ARM resource view.

## Label shares

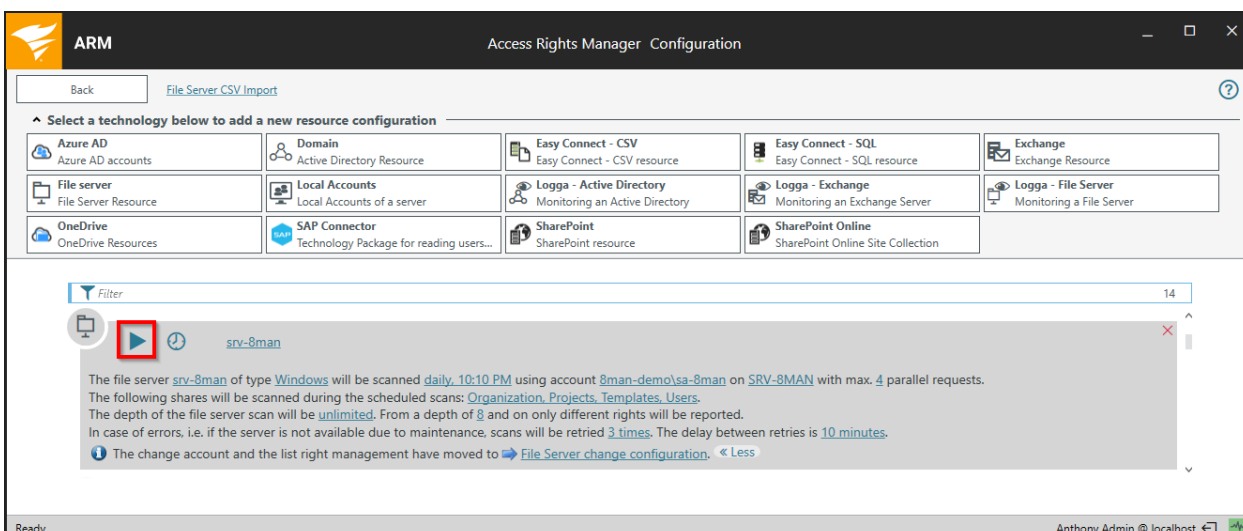


You can add descriptions and additional information to shares.

1. Enter a column description into the appropriate field. Click on the plus icon. This creates a new description column.
2. Enter a description for the shares.

The descriptions are shown in ARM reports.

## Start FS scans



Start/cancel the FS scan.

**i** FS scans may take a long time depending on your file server performance and load, network load, and most significantly the number of file server directories that need to be scanned. Initially you can limit your scans on a few shares and lesser scan depth.

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there's a 'Back' button and a 'File Server CSV Import' link. Below that, a section titled 'Select a technology below to add a new resource configuration' displays a grid of various connectors like Azure AD, Domain, Easy Connect, Exchange, File server, Local Accounts, Logga, OneDrive, SAP Connector, and SharePoint. The main area shows a scan log for 'srv-8man' with a green success message: '[4:56:45 PM] Scan finished successfully... 107 elements (speed 136/s [File Count 11], file size 0.03MB, database space used 0.7MB)'. Below the message, details are provided: 'The file server srv-8man of type Windows will be scanned daily, 10:10 PM using account 8man-demo\sa-8man on SRV-8MAN with max. 4 parallel requests. The following shares will be scanned during the scheduled scans: Organization, Projects, Templates, Users. The depth of the file server scan will be unlimited. From a depth of 8 and on only different rights will be reported. In case of errors, i.e. if the server is not available due to maintenance, scans will be retried 3 times. The delay between retries is 10 minutes.' A red box highlights the success message. At the bottom, the status is 'Ready' and the user is 'Anthony Admin @ localhost'.

Status information is shown during and after the FS scan.

These are no longer shown if you leave and re-enter the scan menu. You can find the information in [Jobs overview](#).

## Delete FS scan configurations


The screenshot shows the same 'Access Rights Manager Configuration' window as above. The scan log for 'srv-8man' is visible, but the success message is no longer highlighted. A red 'X' icon is present in the top right corner of the log entry area, indicating that the configuration can be deleted. The rest of the interface, including the connector grid and status bar, remains the same.


Delete an FS scan configuration.

### Delete resource configurations? ⊗


**Resources with scans**

Name	Information
srv-8man	

 **delete stored scans**  
Check this and all scans done on the configured target will be deleted as well.

 **keep stored scans**  
Check this and all scans done on the configured target will remain in database and archive.

If you delete a scan configuration, you can either store or delete the scan information. Deleting is only possible if all other user interfaces are closed.

 [Identify logged in users](#) in users in the server status section.

## Exchange scans

The Exchange feature allows you to integrate Exchange resources into the Access Rights Manager.

All [system requirements](#) must be met.

An overview of the required permissions can be found in the chapter: [Service account permissions](#). There are some more settings required as described on the following pages.


### Prepare exchange scans

ARM reads information from the Exchange server via a remote PowerShell connection.

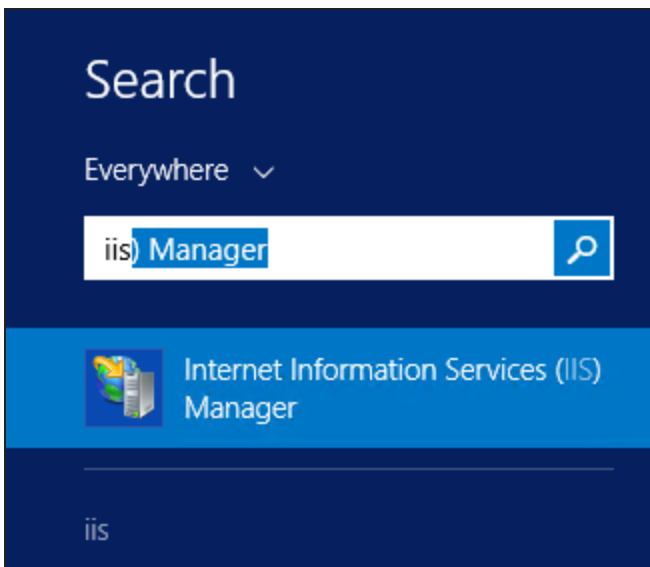
An Exchange scan can be performed by any collector.

The connection is established using a client access server (CAS) or a database availability group (DAG).

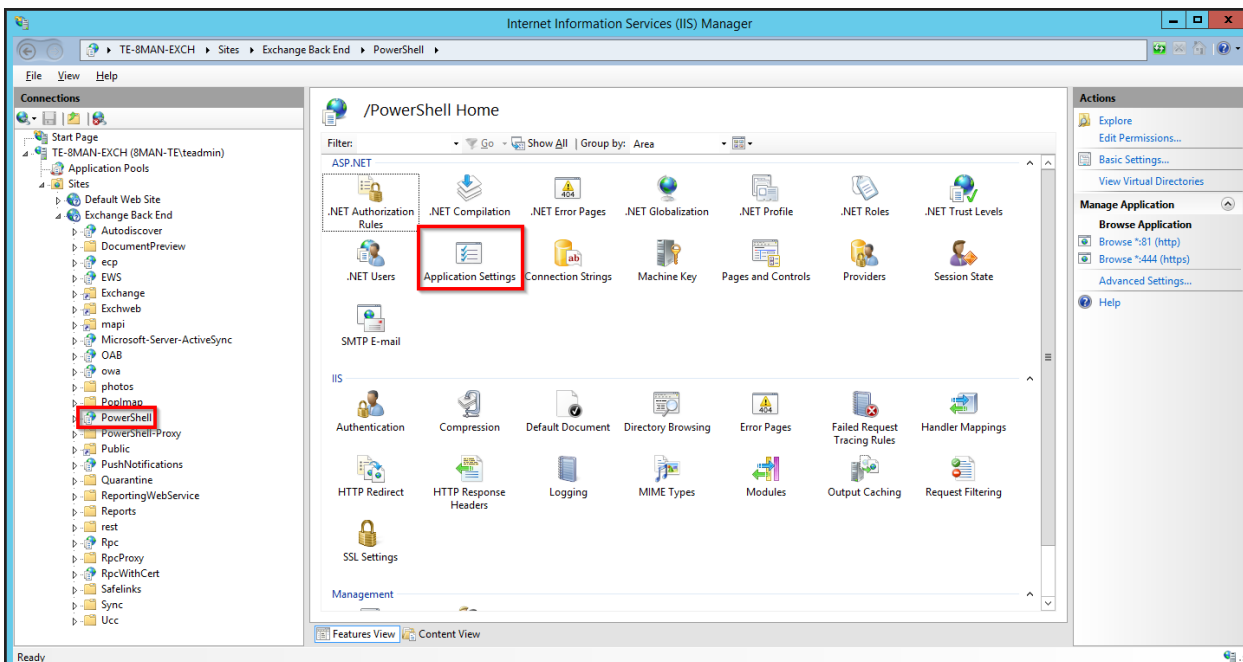
Prepare the PowerShell website

 The steps described in this section are not required for Exchange Online.

The Exchange Client Access Server (CAS) hosts a site within the IIS, that allows users to access the Exchange Server. It is called "Default Web Site" (2010) or "Exchange Back End" (2013 and higher) and includes the sub-site "PowerShell". This must be configured to allow ARM access to Exchange.



Start the IIS Manager on the CAS.



Navigate to "Powershell". In Exchange 2010 this can be found under "Default Web Site". In Exchange 2013 it is found under "Exchange Back End". Double-click "Application Settings".



Internet Information Services (IIS) Manager

TE-BMAN-EXCH > Sites > Exchange Back End > PowerShell

Connections: TE-BMAN-EXCH (BMAN-TE\teadmin) > Application Pools > Sites > Exchange Back End > PowerShell

### Application Settings

Use this feature to store name and value pairs that managed code applications can use at runtime.

Group by: No Grouping

Name	Value	Entry Type
CAS_MaxTimeInMinutes	720	Local
DisableADSettingsCache...	true	Local
LogEnabled	true	Local
LogSubFolderName	Powershell-Proxy	Local
ProvisioningCacheIdenti...	Powershell-Proxy	Local
<b>PSLanguageMode</b>	<b>FullLanguage</b>	Local
RequestMonitor.Enabled	true	Local
RoutingUpdateModule.P...	Powershell	Local
SidsCacheTimeoutInHours	24	Local

Actions: Add..., Edit..., Remove, Help

#### Edit Application Setting

Name: PSLanguageMode

Value: FullLanguage

OK Cancel

Configuration: 'Exchange Back End/PowerShell' web.config

1. Select "PS LanguageMode"
2. Click "Edit"
3. Enter the value "FullLanguage".

⚠ Please note that cumulative Exchange updates may reset this setting!

Internet Information Services (IIS) Manager

TE-BMAN-EXCH > Sites > Exchange Back End > PowerShell

Connections: TE-BMAN-EXCH (BMAN-TE\teadmin) > Application Pools > Sites > Exchange Back End > PowerShell

### Authentication

Group by: No Grouping


Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Enabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Actions: Help

Configuration: 'Exchange Back End/PowerShell' web.config

Activate the desired authentication method.


You must later select the same authentication method in the [Exchange scan configuration](#) that you activate here.

 For additional information see the article [IIS for Beginners Part 4: Authentication and Authorization with the IIS](#) (© 2020 Microsoft, <https://blogs.technet.microsoft.com/bernhardfrank/2011/04/08/iis-fr-einsteiger-teil-4-authentifizierung-und-autorisierung-mit-dem-iis/>, obtained on January 29, 2020).

Alternatively you can activate the authentication with PowerShell.

For example: Activate Windows-authentication (Kerberos)

```
Get-PowerShellVirtualDirectory | Set-PowerShellVirtualDirectory -  
WindowsAuthentication $true
```

 You must restart the IIS in order to apply any changes.

For example in the command prompt or PowerShell:

```
iisreset
```

Set up required permissions

The service account that is used to scan Exchange requires the following access rights:

1. Membership in the Exchange security group "View-Only Organization Management"
2. Read permissions in Active Directory (During the scan distinguished names are resolved and access rights are partially read from the mailbox user)
3. Impersonation rights to scan deputy rules, mailbox folders. See the section: [Exchange Web Service - impersonation](#)
4. Its own mailbox to scan public folders

The service account that you want to use to modify Exchange requires additional different rights:

1. Membership in the Exchange security group "Organization Management"

 Deny rights applied to mailbox content may hinder successful scans.

For Exchange Online, create a user (with an email address) that is "Global Administrator" on the server and does not need to be licensed. Add the user to the group "View-Only Organization Management" for read only access, "Organization Management" for modify access.

## Exchange Web Services - Impersonation

PowerShell allows you to load administrative information from Exchange, such as the structure and permissions of objects, e.g. mailboxes and public folders. The Exchange Web Service allows you to access their content. Substitution rules can only be read via the Exchange Web Service.

**⚠** Before you decide to read and view mailbox folders, you should ensure that this adheres to your company data security policy. You may be able to view sensitive information by only viewing mailbox folder structures.

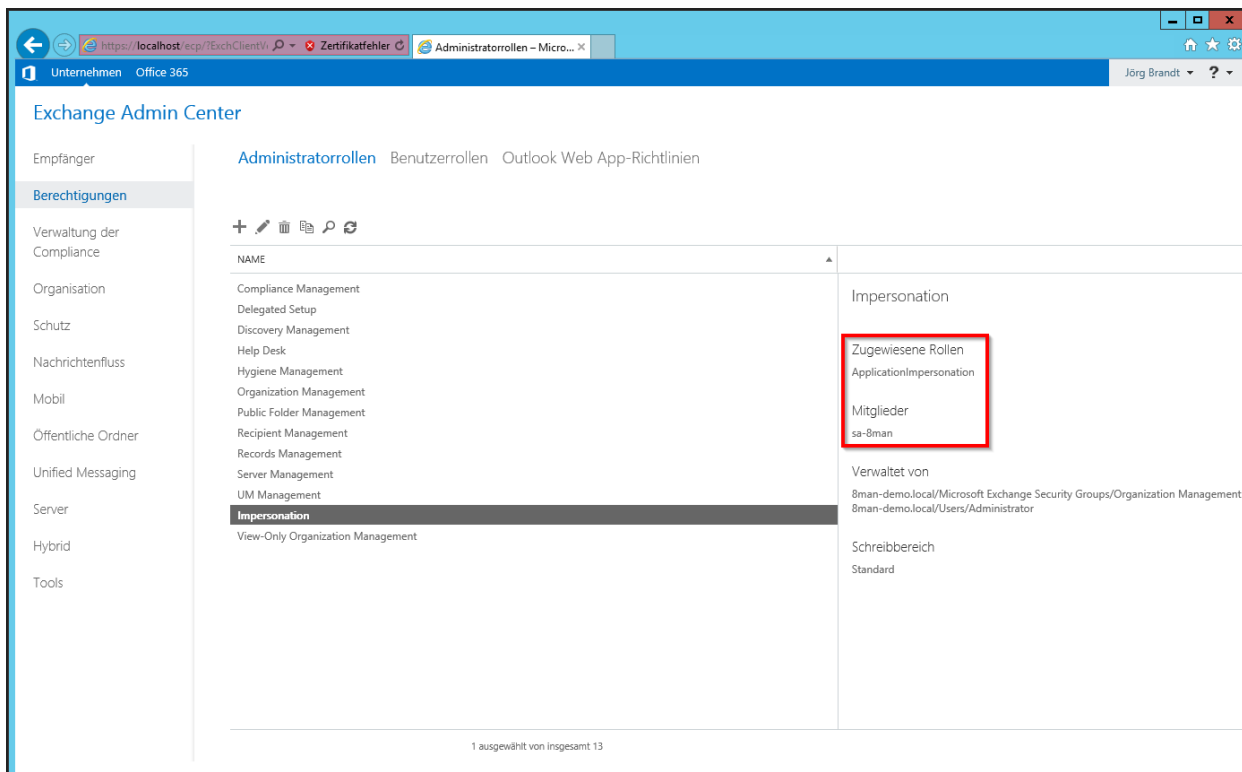
Access to the Exchange Web Service always happen in context with the mailbox user. This requires that the scan account (service account) has the right to impersonate.

**i** Impersonation only works with active Active Directory accounts.

Examples for the configuration of impersonations via PowerShell can be found here:

- Exchange 2010: [Configuring Exchange Impersonation in Exchange 2010](https://docs.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2010/bb204095(v=exchg.140)) (© 2020 Microsoft, [https://docs.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2010/bb204095\(v=exchg.140\)](https://docs.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2010/bb204095(v=exchg.140)), obtained on January 29, 2020).
- Exchange 2013 or higher, online and Office 365: [How to: Configure impersonation](https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-configure-impersonation) (© 2020 Microsoft, <https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-configure-impersonation>, obtained on January 29, 2020).

Alternatively to the process described by Microsoft you can use the GUI of the Exchange Admin Center:



The screenshot displays the Exchange Admin Center interface. The left-hand navigation pane shows the 'Impersonation' role selected under 'Berechtigungen'. The main content area shows the configuration for the 'Impersonation' role. The 'Zugewiesene Rollen' (Assigned Roles) section is highlighted with a red box and contains the following roles:

- ApplicationImpersonation
- Mitglieder sa-8man

The 'Verwaltet von' (Managed by) section shows the role is managed by '8man-demo.local/Microsoft Exchange Security Groups/Organization Management' and '8man-demo.local/Users/Administrator'. The 'Schreibbereich' (Mailbox) is set to 'Standard'.

You can define a new Administrator role (Group) in the Exchange Admin Center. Assign "ApplicationImpersonation" to the new role.

Alternatively, you can also assign "ApplicationImpersonation" to the built-in role "Discovery Management".

Add the service account as a member of the appropriate role.

Summary: The scan account must be assigned a management role, including the explicit impersonation right.

Test the connection to Exchange PowerShell

Use the following process to test the connection to PowerShell:

1. Start a power shell console with the credentials that are also used for the remote session. (CTRL+SHIFT+right-click on the PowerShell-Icon -> "Run as different user")
2. Create a credential object:  
`$cred = get-credential`
3. Create a SessionOption object (turn off all checks for the test):  
`$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck`
4. Create a session. Adjust the URI, Authentication (authentication mechanism) and encryption http(s):  
`$session = New-PSSession -configurationname Microsoft.Exchange -connectionURI https://srv-ex01/PowerShell/ -Credential $cred -SessionOption $so -Authentication Default`
5. Enter the session. You can execute cmdlets (which ones, depends on their rights):  
`Enter-PSSession $session`

## Configure Exchange scans

The screenshot displays the ARM Configuration interface. At the top, the title bar reads 'ARM Access Rights Manager Configuration'. The main content area is divided into three summary cards:

- Server Status** (License Information): Logged in users: 2; Licensed Active user accounts: 1166.
- Jobs** (Summary): 91 Scans, 7 Reports, 69 Changes, 135 More; 7 Scheduled, 293 Succeeded; 0 Executing, 2 Failed.
- Collectors** (Configuration): 1 Connected, 1 Configured in Total; All Collectors are Operational.

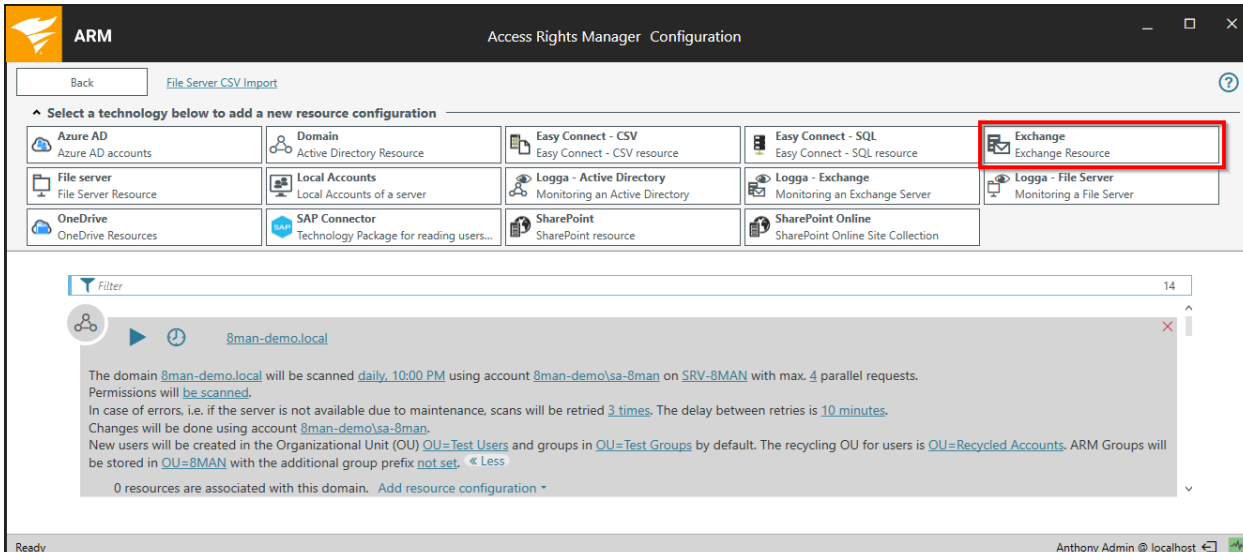
Below the summary cards is a 'Filter' dropdown. The main area contains a grid of 12 configuration options, each with an icon and a description:

- Scans** (highlighted with a red box): Resource Configurations, Logga, File Server CSV Import.
- Open Order**: Open Order Resource Descriptions.
- User Management**: User Management, Role Management.
- Data Owner**: Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings.
- License**: License Information, Server Status.
- Jobs Overview**: Job Status, Job Categories.
- Alerts**: Activate/Deactivate Alert Sensors.
- Change Configuration**: Common Change Settings, Technology-specific Change Configurations.
- Scripting**: Scripting configuration for change actions.
- Views & Reports**: Views & Reports, Blacklist for Views & Reports.
- Server**: Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging.
- Basic Configuration**: ARM Server, SQL Server, Configuration Status.

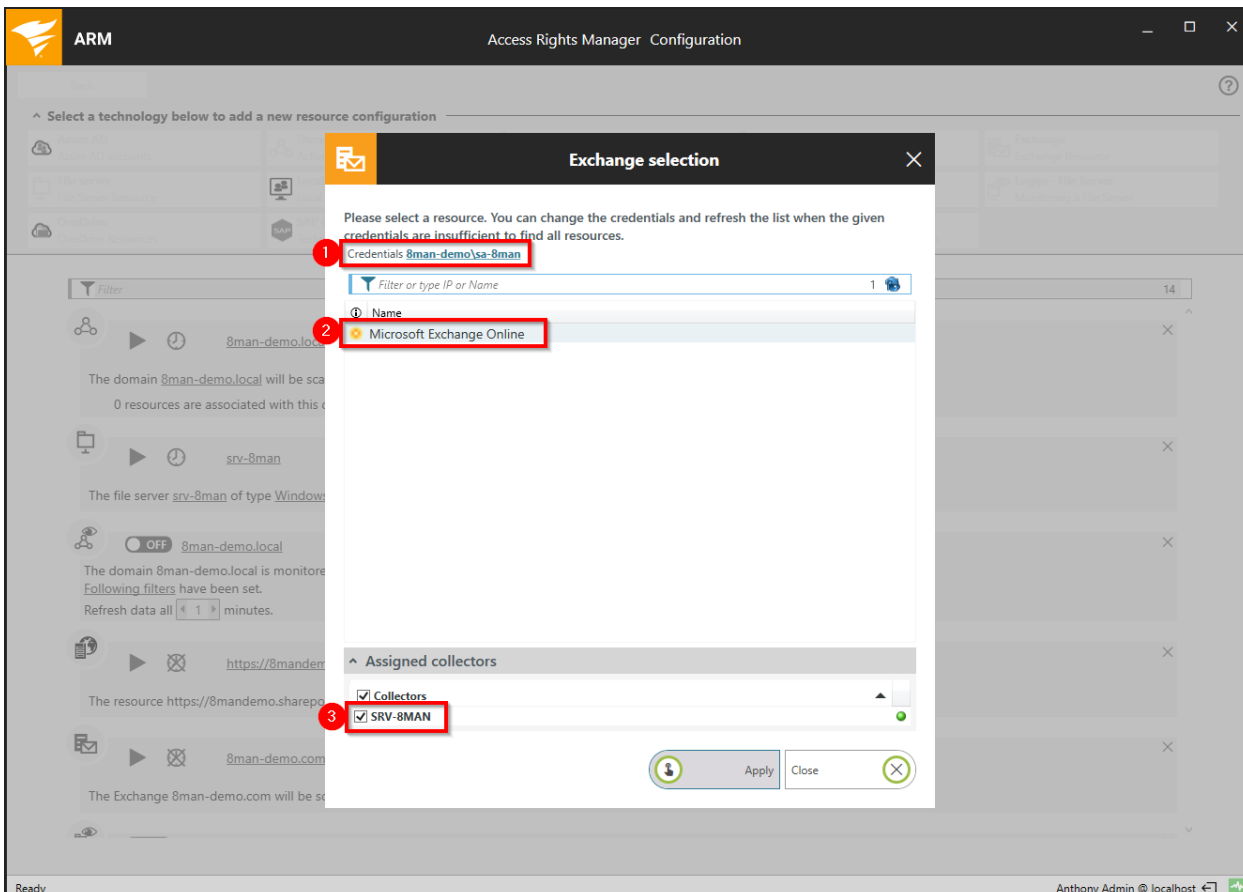
The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Select "Scans" from the home page of the configuration application.

## Add an Exchange scan



Select "Exchange".



1. Enter the account information for the account that should be used to execute the Exchange scan.

The credentials from the [basic configuration](#) will be suggested automatically.

2. Select the Exchange Server. All DAGs\* or servers that are contained in the current Active Directory site will be listed. Enter the desired server into the search field (this is possible even when it is not listed).
3. Assign a collector.

### Special considerations for Exchange Online:

1. The credentials displayed here are not relevant for Exchange Online. They must be adjusted later in the scan configuration.
2. Exchange Online is always shown.
3. For Exchange Online the collector requires internet access.

\* ARM can connect to DAG servers (Database Availability Groups) and execute scans on them. You are able to select the DAG server directly in the scan configuration. Please note that you have to adjust the settings described in the section [Preparing the PowerShell Website](#) on every involved DAG Exchange server. The decision, which server the collector establishes a connection with is made by the DAG during the initial connection build up. This means that successive scans may take place on different servers.


**i** Since IP less DAGs (from Exchange 2016 Default Setting, optional in Exchange 2013) do not have an Administrative Access Point (AAP), the Exchange server cannot be managed via this DAG. In this case, specify an Exchange server directly or use the load balancing namespace.

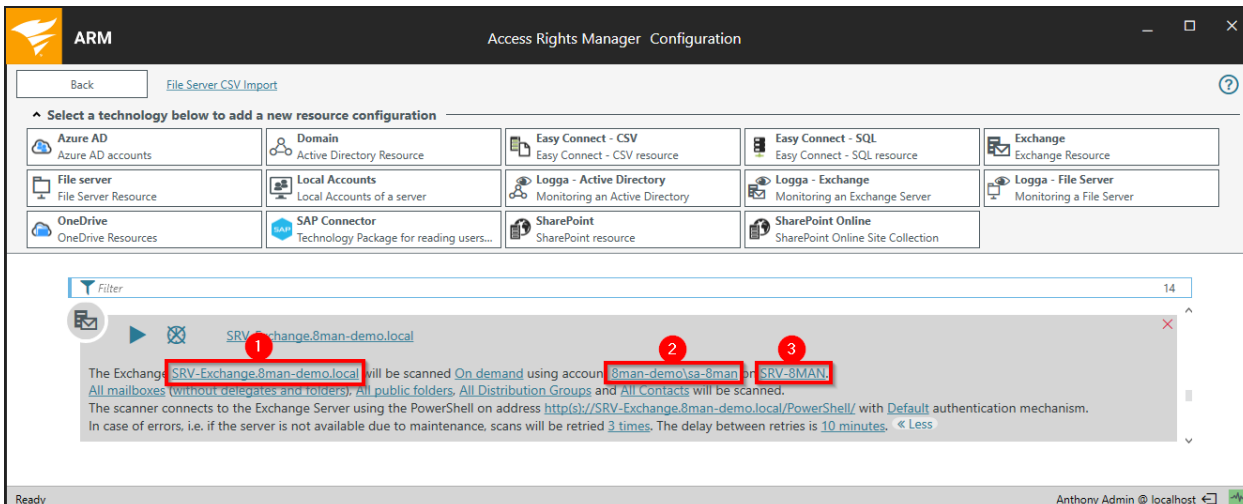
### Customize an Exchange scan configuration

The screenshot shows the ARM Configuration window. At the top, there's a 'Back' button and a 'File Server CSV Import' link. Below that, a section titled 'Select a technology below to add a new resource configuration' contains a grid of options including Azure AD, Domain, Easy Connect - CSV, Easy Connect - SQL, Exchange, File server, Local Accounts, Logga - Active Directory, Logga - Exchange, Logga - File Server, OneDrive, SAP Connector, SharePoint, and SharePoint Online. A search filter is applied to the 'Exchange' category, showing 'SRV-Exchange.8man-demo.local'. A red box highlights the search results, and a red arrow points to the 'On demand' scan type. Below the search results, a detailed configuration card is visible, showing the server name, scan type, and authentication details.

1. Start/cancel an Exchange Scan.
2. Schedule regular scans.

## 3. Change the name of the configuration.

 The typical scan speed is around 10 elements per second.

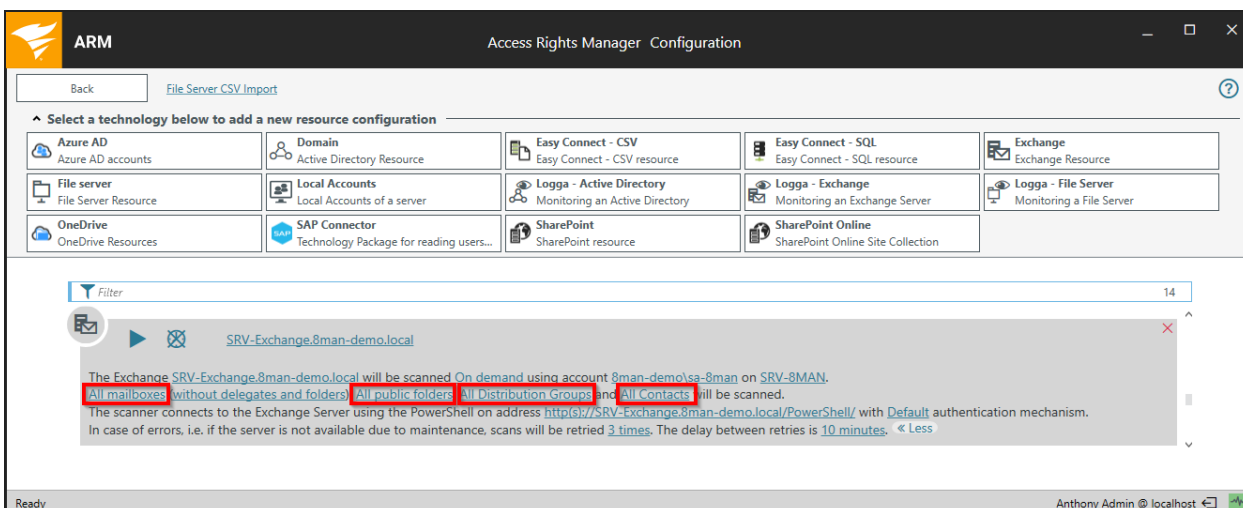


The screenshot shows the ARM Configuration window for 'File Server CSV Import'. A configuration for 'SRV-Exchange.8man-demo.local' is selected. The configuration details are as follows:

- 1. The Exchange server to be scanned: SRV-Exchange.8man-demo.local
- 2. The account used for scanning: 8man-demo\sa-8man
- 3. The collector server: SRV-8MAN

The configuration details also include: 'On demand' scanning, 'All mailboxes (without delegates and folders), All public folders, All Distribution Groups and All Contacts' to be scanned, and a PowerShell address: http(s)://SRV-Exchange.8man-demo.local/PowerShell/ with Default authentication mechanism. Scans will be retried 3 times with a 10-minute delay.

1. Change the Exchange Server that you want to scan.
2. Change the credentials that are used to execute the scan.
3. Switch the collector server. Please note that the collector server requires internet access when using Exchange Online.



The screenshot shows the ARM Configuration window for 'File Server CSV Import'. A configuration for 'SRV-Exchange.8man-demo.local' is selected. The configuration details are as follows:

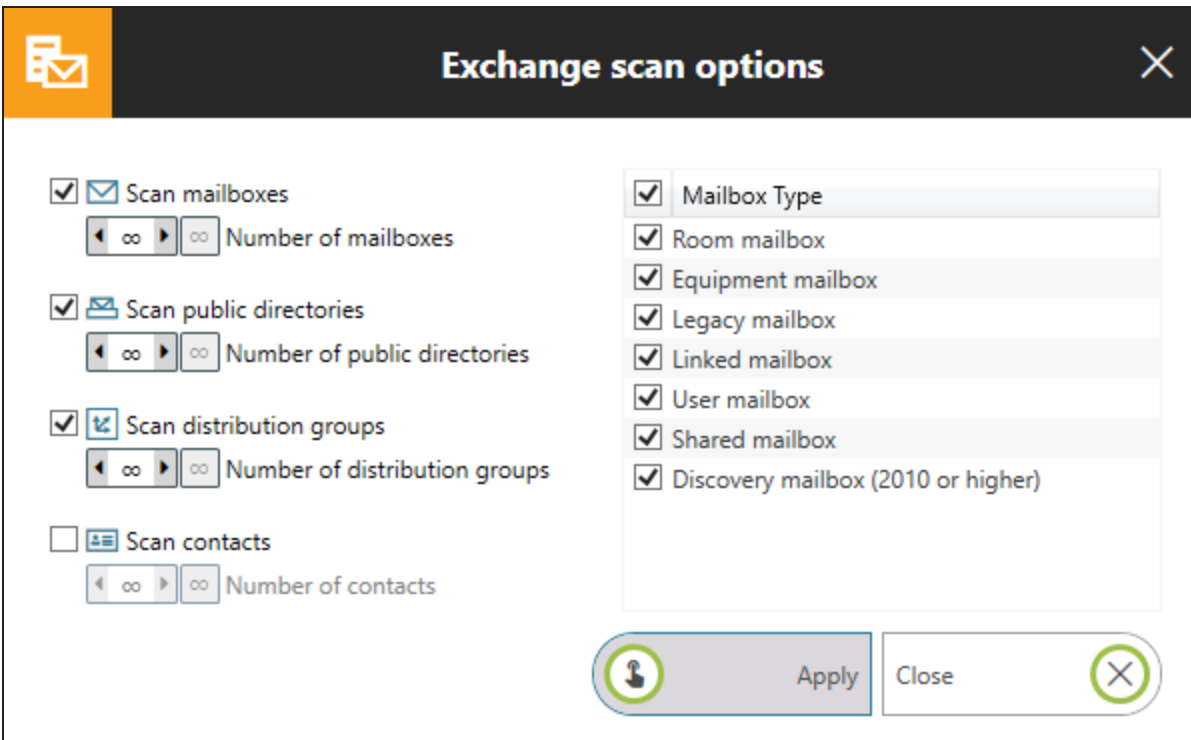
- The Exchange server to be scanned: SRV-Exchange.8man-demo.local
- The account used for scanning: 8man-demo\sa-8man
- The collector server: SRV-8MAN

The configuration details also include: 'On demand' scanning, 'All mailboxes (without delegates and folders), All public folders, All Distribution Groups and All Contacts' to be scanned, and a PowerShell address: http(s)://SRV-Exchange.8man-demo.local/PowerShell/ with Default authentication mechanism. Scans will be retried 3 times with a 10-minute delay.

Define the range of the scan.

All the links lead to the following dialog:





**Exchange scan options**

Scan mailboxes  
 ◀ ∞ ▶ ∞ Number of mailboxes

Scan public directories  
 ◀ ∞ ▶ ∞ Number of public directories

Scan distribution groups  
 ◀ ∞ ▶ ∞ Number of distribution groups

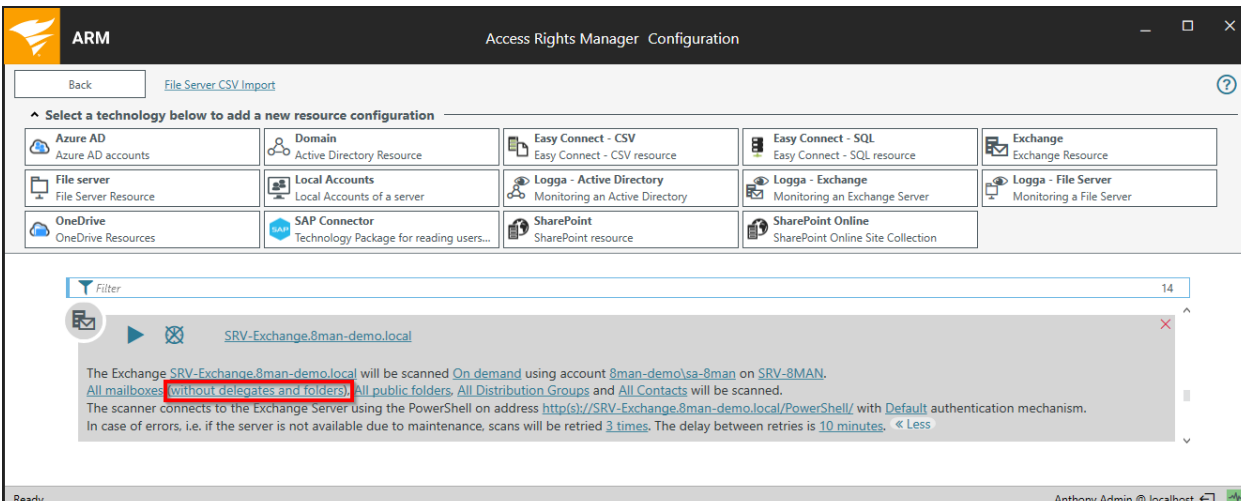
Scan contacts  
 ◀ ∞ ▶ ∞ Number of contacts

Mailbox Type

- Room mailbox
- Equipment mailbox
- Legacy mailbox
- Linked mailbox
- User mailbox
- Shared mailbox
- Discovery mailbox (2010 or higher)

Apply Close

If you select only a subset of folders for readable public folders, then no statistical data will be available. Administrative permissions to public folders are not available (since Exchange 2013). A filter is applied to the mailbox property "RecipientTypeDetails", to select the mailbox type.



ARM Access Rights Manager - Configuration

Back File Server.CSV.Import

Select a technology below to add a new resource configuration

Azure AD Azure AD accounts	Domain Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource
File server File Server Resource	Local Accounts Local Accounts of a server	Logga - Active Directory Monitoring an Active Directory	Logga - Exchange Monitoring an Exchange Server	Logga - File Server Monitoring a File Server
OneDrive OneDrive Resources	SAP Connector Technology Package for reading users...	SharePoint SharePoint resource	SharePoint Online SharePoint Online Site Collection	

Filter 14

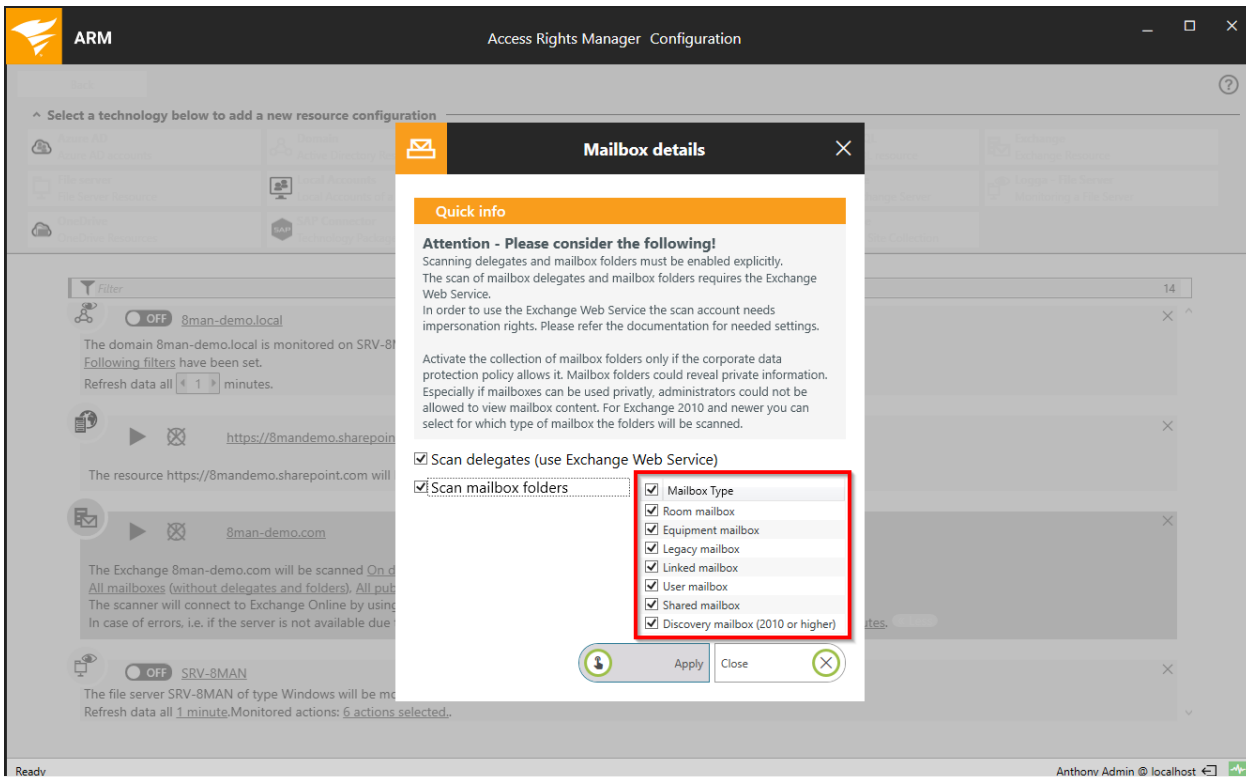
SRV-Exchange.8man-demo.local

The Exchange SRV-Exchange.8man-demo.local will be scanned On demand using account 8man-demo\sa-8man on SRV-8MAN. All mailboxes without delegates and folders. All public folders. All Distribution Groups and All Contacts will be scanned. The scanner connects to the Exchange Server using the PowerShell on address http(s)://SRV-Exchange.8man-demo.local/PowerShell/ with Default authentication mechanism. In case of errors, i.e. if the server is not available due to maintenance, scans will be retried 3 times. The delay between retries is 10 minutes. < Less

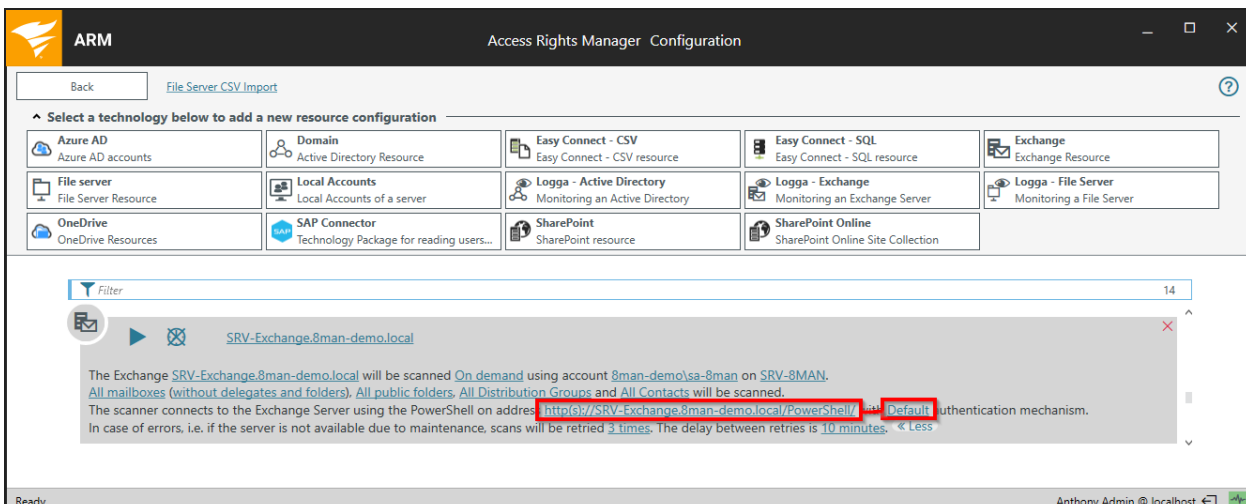
Ready Anthonyv Admin @ localhost

You can determine if substitution rules and mailbox folders are read.

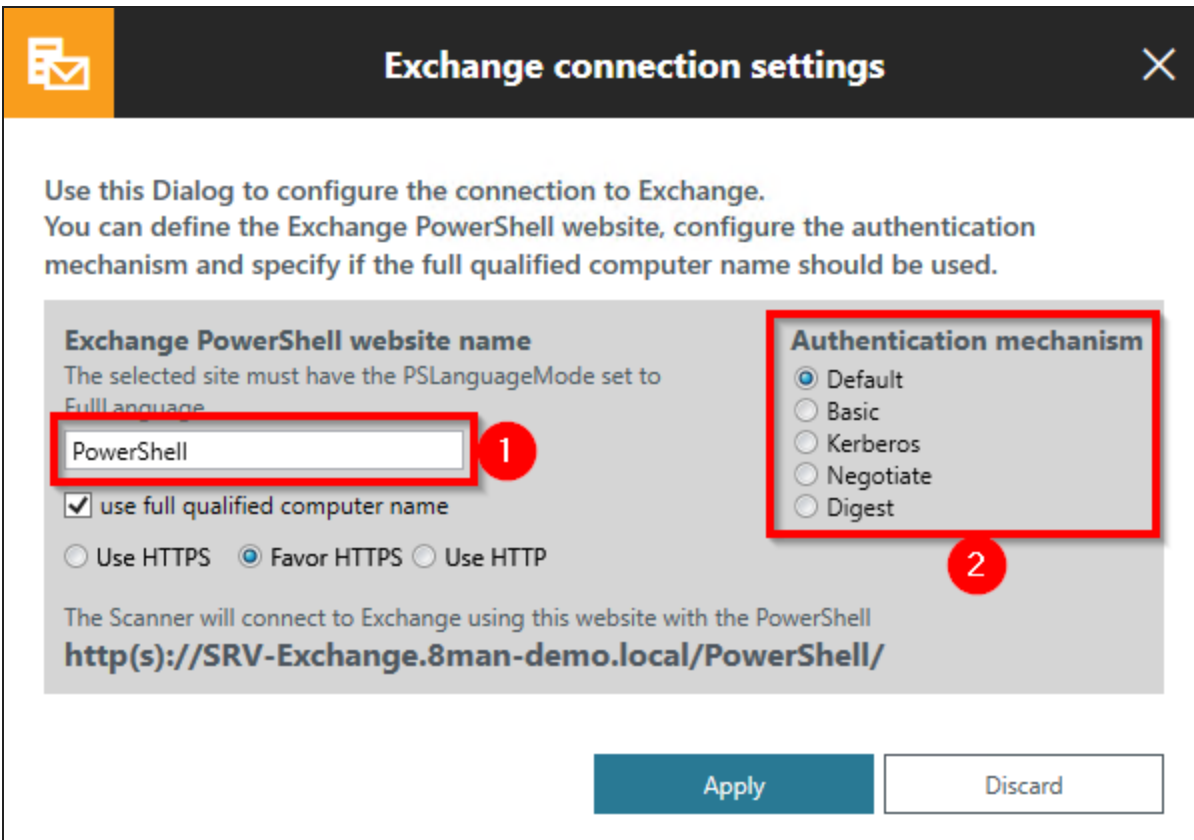
Please note that [Exchange Web Services - Impersonation](#) is used.



Determine the range in which mailbox details are read with Exchange Web Service (EWS).  
 The selection of mailbox type is independent for scans with PowerShell and EWS. This means that you can determine which [mailbox types are scanned](#) and for which mailbox types the mailbox folders are scanned.



Click one of the links to configure the connections settings for the Exchange scan.




The dialog box is titled "Exchange connection settings" and contains the following elements:

- Exchange PowerShell website name:** A text input field containing "PowerShell". A red box highlights this field with a red circle containing the number "1".
- Authentication mechanism:** A group box containing five radio button options: "Default" (selected), "Basic", "Kerberos", "Negotiate", and "Digest". A red box highlights this group with a red circle containing the number "2".
- Other options:** A checked checkbox for "use full qualified computer name" and radio buttons for "Use HTTPS", "Favor HTTPS" (selected), and "Use HTTP".
- Preview:** A text area showing the connection URL: `http(s)://SRV-Exchange.8man-demo.local/PowerShell/`.
- Buttons:** "Apply" and "Discard" buttons at the bottom.

The following settings must match those of the IIS-website. These are described in the section [Preparation of the PowerShell website](#).

1. Enter the name of the Exchange PowerShell website. In standard settings this is "PowerShell".
2. Select an authentication mechanism. For Exchange Online select "Basic".


Exchange connection settings
✕

Use this Dialog to configure the connection to Exchange.  
You can define the Exchange PowerShell website, configure the authentication mechanism and specify if the full qualified computer name should be used.

**Exchange PowerShell website name**  
The selected site must have the PSLanguageMode set to FullLanguage.

**Authentication mechanism**

Default

Basic

Kerberos

Negotiate

Digest

use full qualified computer name

Use HTTPS  Favor HTTPS  Use HTTP


The Scanner will connect to Exchange using this website with the PowerShell  
**http(s)://SRV-Exchange.8man-demo.local/PowerShell/**

Apply
Discard

1. In some cases the client access server is not reachable via the fully qualified computer name. In this scenario, deactivate this option. Please note the preview.
2. Select if an encrypted connection should be used. This setting must match those of the PowerShell website.

## Advanced Exchange scan settings in the configuration files

Some settings can not be made in the graphical configuration application. Advanced settings must be adjusted in the configuration files.

 The settings described below are only effective after a new scan.

Change the attribute for the creation of mailbox categories

By default ARM sorts mailboxes into categories, upwards of 1,000 mailboxes, according to the Active Directory property "sn".

The selected property can be changed to any desired text attribute from Active Directory, via the configuration file.

## Configuration file

pnJob.config.xml

## Computer

Collector server which is configured for the Exchange Scan.

## Path

%ProgramData%\protected-networks.com\8MAN\cfg

If the file is not available, copy the "template" from the following path, delete the content and enter the code.

old: %ProgramFiles%\Protected Networks\8MAN\etc

new: %ProgramFiles%\solarwinds\ARM\etc

## Code

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <collector.scanner.exchange.sortingProperty
Type="System.String">sn</collector.scanner.exchange.sortingProperty>
</config>
```

## Possible Values

Replace "sn" with any desired AD text (single line) attribute.

Change the cut-off rules for the mailbox categories

By default the category descriptions are generated from the first 10 characters of the first and last mailbox. You can change the length of utilized descriptions.

## Configuration file

pnServer.config.xml

## Computer

ARM-Server

## Path

%ProgramData%\Protected Networks\8MAN\cfg

## Code

in the section <config>

```
<exchange.CategoryLength type="System.Int32">10</exchange.CategoryLength>
```

## Possible values

1 to 500

Prevent the formation of mailbox categories

By default ARM sorts mailboxes into categories, upwards of 1,000 mailboxes. You can turn off the creation of categories.

## Configuration file

pnServer.config.xml

## Computer

ARM-Server

## Path

%ProgramData%\Protected Networks\8MAN\cfg

## Code

in the section <config>

```
<exchange.makeMailBoxCategories  
type="System.Boolean">false</exchange.makeMailBoxCategories>
```

## Possible values


false no categories (flat list of mailboxes in the resource view)

true use categories

Adjust the throttling factor

The Exchange Web-Service is used for the scanning of delegations. The scan works with the given throttling settings of the Exchange server.

The scan can be accelerated with an optimal throttling setting.

 For additional information see the article [Set-ThrottlingPolicy](https://docs.microsoft.com/en-us/powershell/module/exchange/server-health-and-performance/Set-ThrottlingPolicy?view=exchange-ps). (© 2020 Microsoft, <https://docs.microsoft.com/en-us/powershell/module/exchange/server-health-and-performance/Set-ThrottlingPolicy?view=exchange-ps>, obtained on January 29, 2020)

The setting "EWSMaxConcurrency" is important. It affects the number of parallel requests used by the scan to read delegations.

By default ARM uses the maximum number of possible parallel requests allowed by the throttling policy. If the throttling policy allows for an unlimited number of parallel requests, then the number of processors is multiplied by 8. You are able to change this value.

### Configuration file

pnJob.config.xml

### Computer

Collector server that is configured for the Exchange scan.

### Path

%ProgramData%\Protected Networks\8MAN\cfg

### Code

```
<?xml version="1.0" encoding="utf-8"?>
<config>
<collector.scanner.exchange.processormultiplierForUnlimitedThrottling
type="System.Int32">
8</collector.scanner.exchange.processormultiplierForUnlimitedThrottling>
</config>
```

### Possible values

Replace the value "8" with your desired number. The entered number will be multiplied with the number of processors.

## SharePoint scans

Integrate SharePoint as a resource into ARM Access Rights Management was possible in two ways:

### **OLD: 8MATE for SharePoint up to version 9.0**

- uses the Server Side Object Model (SSOM)
- Requires a local installation on the SharePoint server
- Supports only the SharePoint versions 2010 and 2013 (on premise)

### **NEW: ARM SharePoint integration using the CSOM from version 8.0**

- uses the Client Side Object Model (CSOM)
- No installation on the SharePoint server is required
- Supports SharePoint versions 2010, 2013, 2016, and SharePoint Online

The system requirements must be fulfilled. See section [SharePoint requirements](#).

## Required accounts and permissions for a SharePoint scan

For a SharePoint scan, two accounts are to be configured:

### Process Account

The "Process account" is used to execute the scan process on the selected collector. This account must have local administrative rights and interactive logon privileges on the collector.

### Scan Account

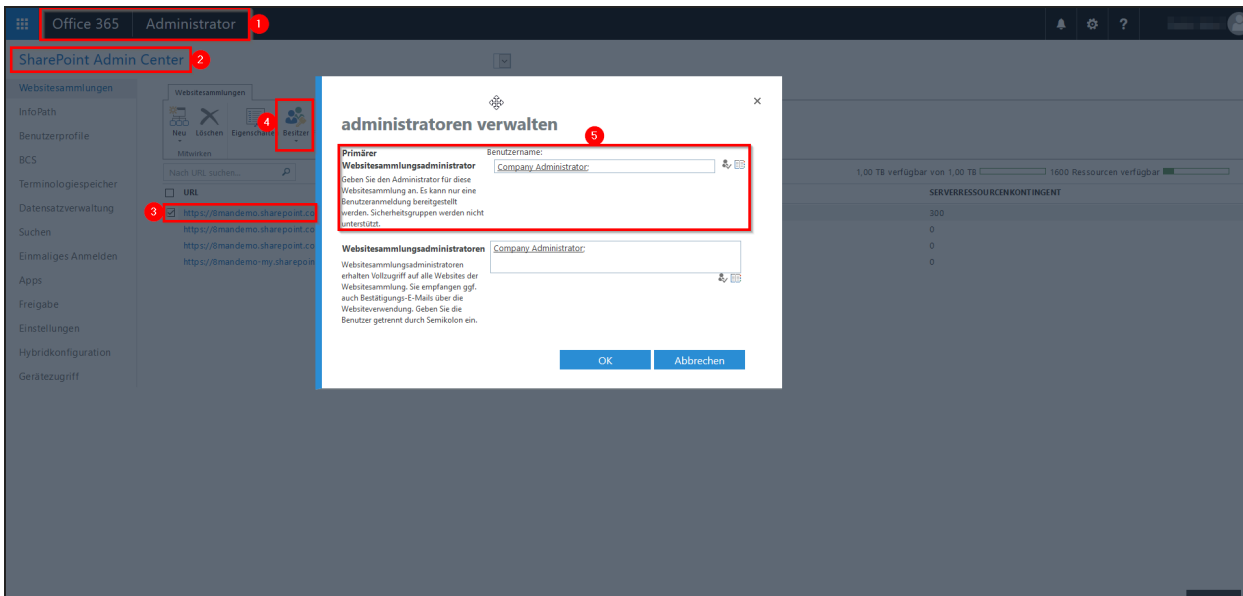
The "scan account" is used for the actual scan. This account must always be the same as the owner account registered for the site collection (= primary site collection administrator). The corresponding user account is defined when a site collection is created and can only be viewed or changed via the SharePoint central administration.

Navigate in the Central Administration to:

application management -> site collections -> Change site collection administrators -> Selection of the site collection -> Primary site collection administrator



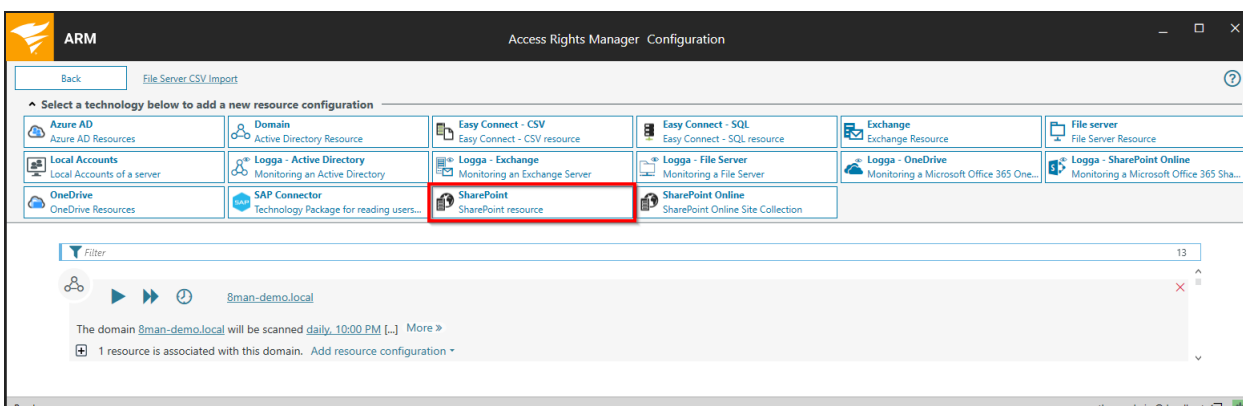
## Identify the primary site collection administrator in SharePoint Online



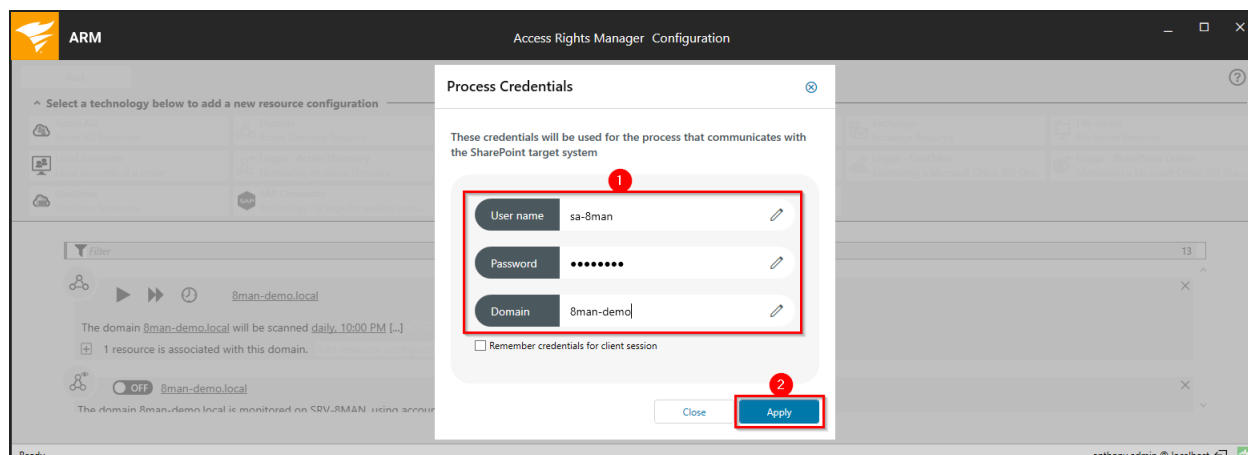
1. Log into your Office 365 environment as an administrator.
2. Go to the SharePoint Admin Center.
3. Select the collection to be scanned (set the checkmark).
4. Click Owner-> Manage Administrators.
5. You will see the primary site collection administrator.

The placeholder "Company Administrator" stands for all global Office 365 administrators.

## Add a SharePoint on-premise scan



Click the button to add a SharePoint on-premise resource.

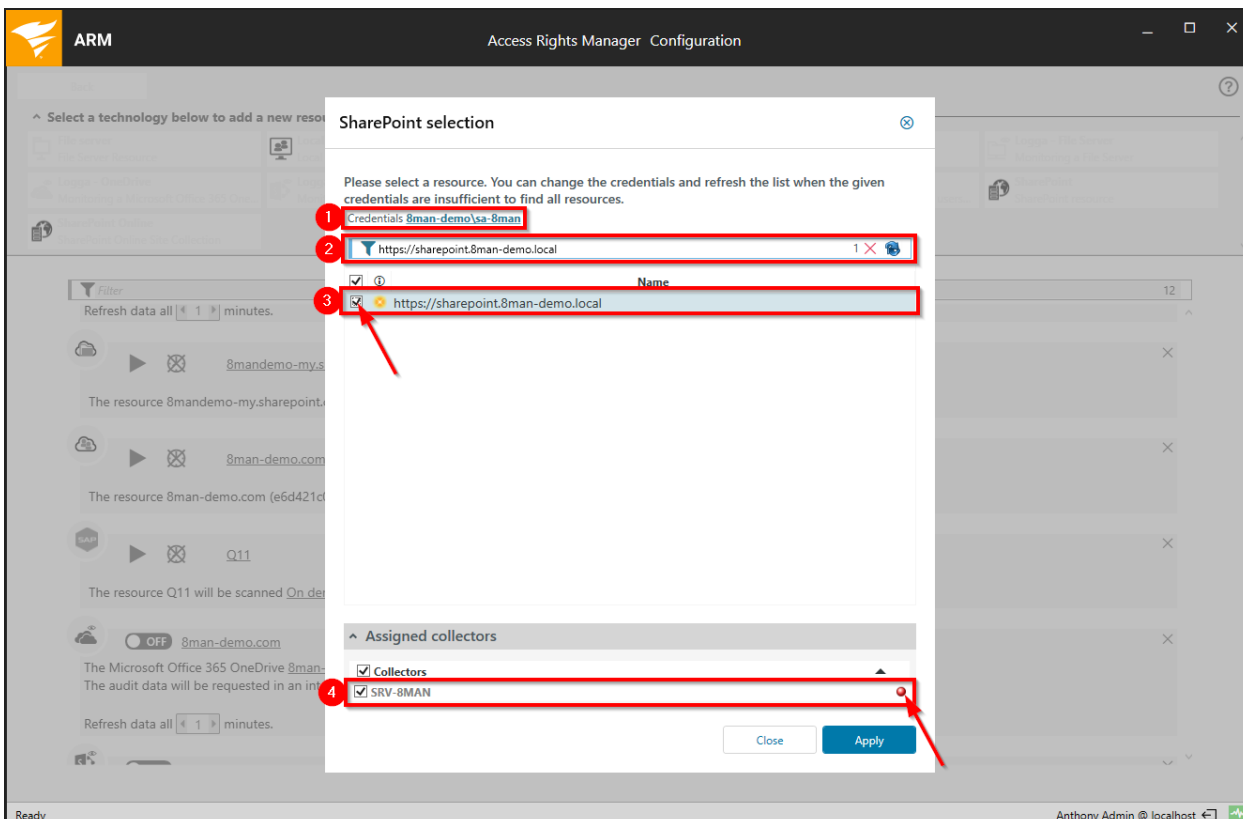


1. Specify the credentials for the "[Process Account](#)". We recommend to use the ARM service account.

**i** The account is preset to scan the SharePoint items. You can change the "[Scan Account](#)" later, as described in the chapter "[Customize a SharePoint scan configuration](#)".

2. Click Apply.

ARM checks the specified credentials. Once the check is successful, the selection of available resources opens.



1. If necessary, change the account used to read the SharePoint resources. Preset is the "Process account".
2. Specify the SharePoint server name (recommended) or a URL of a SharePoint element. Confirm your entry with the ENTER key.

**i** If you specify the name of the server you can later conveniently [select the elements to be integrated](#).  
 For this feature, [WinRM must be configured and CredSSP must be enabled in the additional SharePoint properties](#).

This feature is only available for SharePoint on-premise and **not** for SharePoint Online.

3. Select the added entry (set the checkmark).
4. Select one or more collectors to perform the scan.

**i** **Collector indicator green:**

A connection to the specified SharePoint server was successful.

**Collector indicator red:**

Unable to successfully connect to the specified SharePoint server. You can still save the settings and correct them later.

In certain configurations, the indicator remains red and the SharePoint server can still be successfully scanned with the specified credentials.

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there is a 'Back' button and a 'File Server CSV Import' link. Below this is a section titled 'Select a technology below to add a new resource configuration' with a grid of options including Azure AD, Domain, Easy Connect, Exchange, File server, Local Accounts, Logga, OneDrive, SAP Connector, SharePoint, and SharePoint Online. The main area displays a list of resources. A red box highlights a warning for the resource 'http://demo-sitecollection'. The warning text reads: 'The resource http://demo-sitecollection will be scanned daily, 1:00 AM. The communication will be established using account 8man-demo\sa-8man. Scans will be performed using account 8man-demo\sa-8man on SRV-8MAN. The following SharePoint elements will be scanned: <select SharePoint elements>. In case of errors, i.e. if the server is not available due to maintenance, scans will be retried once. The delay between retries is 10 minutes. ⚠ The additional properties have not completely been configured. < Less'.

You have created a new SharePoint configuration.

The warning indicates that you must [configure additional properties](#) before you can successfully perform a scan.

Select SharePoint on-premise elements to be integrated

**i** The selection feature is only available for SharePoint on-premise, **not** for SharePoint Online.

ARM Access Rights Manager Configuration

Back File\_Server\_CSV\_Import

Select a technology below to add a new resource configuration

<b>Azure AD</b> Azure AD accounts	<b>Domain</b> Active Directory Resource	<b>Easy Connect - CSV</b> Easy Connect - CSV resource	<b>Easy Connect - SQL</b> Easy Connect - SQL resource	<b>Exchange</b> Exchange Resource
<b>File server</b> File Server Resource	<b>Local Accounts</b> Local Accounts of a server	<b>Logga - Active Directory</b> Monitoring an Active Directory	<b>Logga - Exchange</b> Monitoring an Exchange Server	<b>Logga - File Server</b> Monitoring a File Server
<b>Logga - OneDrive</b> Monitoring a Microsoft Office 365 One...	<b>Logga - SharePoint Online</b> Monitoring a Microsoft Office 365 Sha...	<b>OneDrive</b> OneDrive Resources	<b>SAP Connector</b> Technology Package for reading users...	<b>SharePoint</b> SharePoint resource

Filter 13

in case of errors, i.e. if the server is not available due to maintenance, scans will be retried [3 times](#). The delay between retries is [10 minutes](#). < Less

**SRV-8MAN** OFF

The file server SRV-8MAN of type Windows will be monitored on SRV-8MAN  
Refresh data all [10 minutes](#). Monitored actions: [6 actions selected](#).  
Configured File Filter for Blacklist: [Not configured](#). Whitelist: [Not configured](#)  
Permissions (ACLs) for alerts and for report type "Detailed permission changes" will be read using account [not set](#)

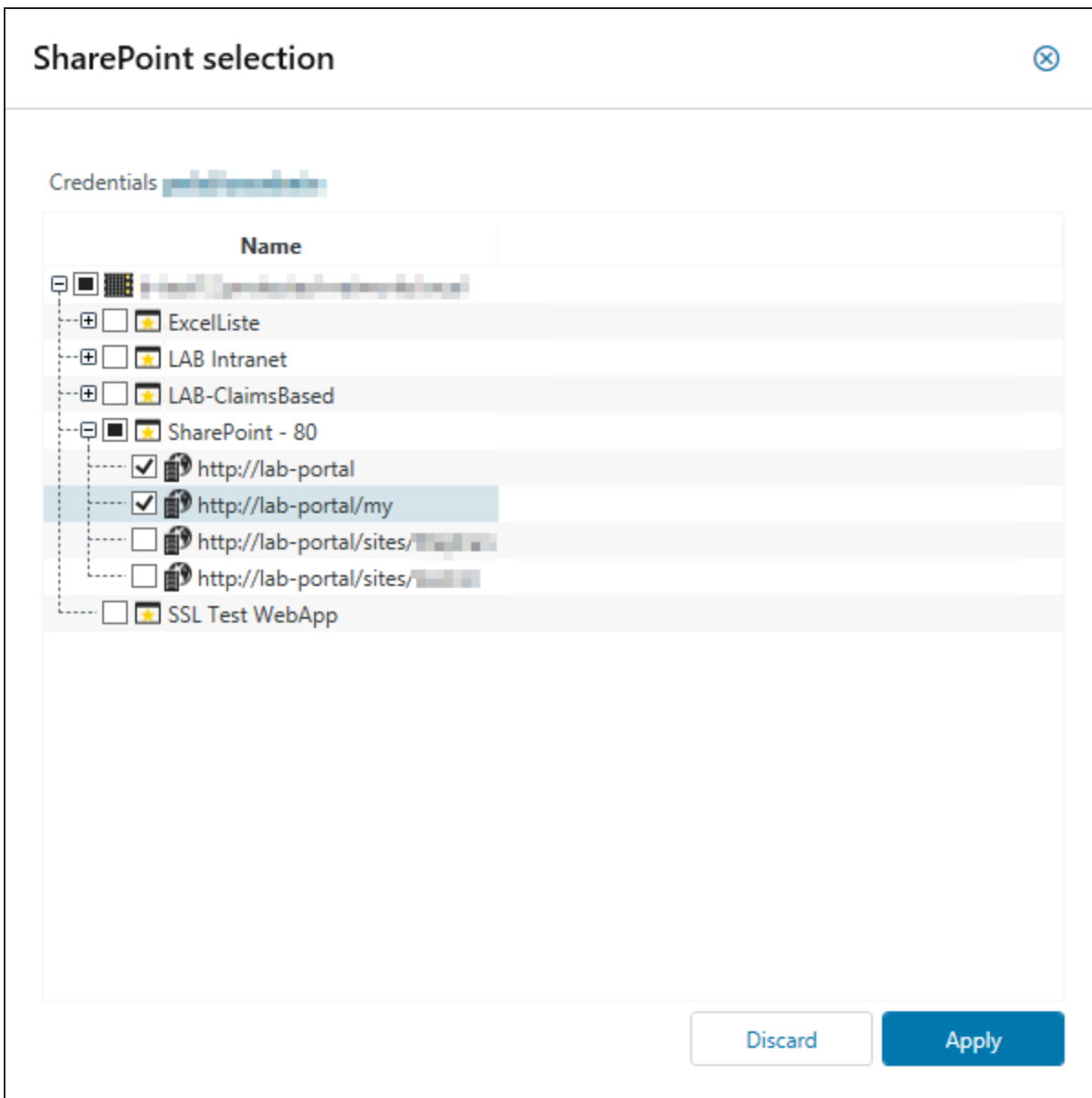
3 reports are configured. Add: [Who did what?](#) [Who made changes?](#) [Who did what, except authorized users \(SoD\)?](#) [Detailed permission changes](#)

**SharePoint-Demo**

The resource SharePoint-Demo will be scanned [On demand](#). The communication will be established using account [8man-demo\administrator](#). Scans will be performed using account [8man-demo\administrator](#) on SRV-8MAN .  
The following SharePoint elements will be scanned [<select SharePoint elements>](#).  
In case of errors, i.e. if the server is not available due to maintenance, scans will be retried [once](#). The delay between retries is [10 minutes](#).  
The [additional properties have completely](#) been configured. < Less

Ready Anthony Admin @ localhost

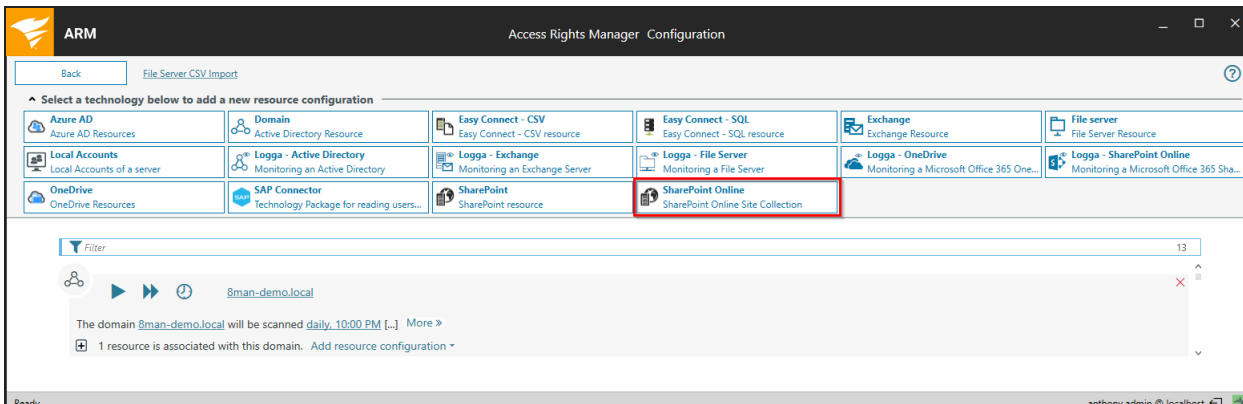
Click on "Select SharePoint elements" in the SharePoint configuration.



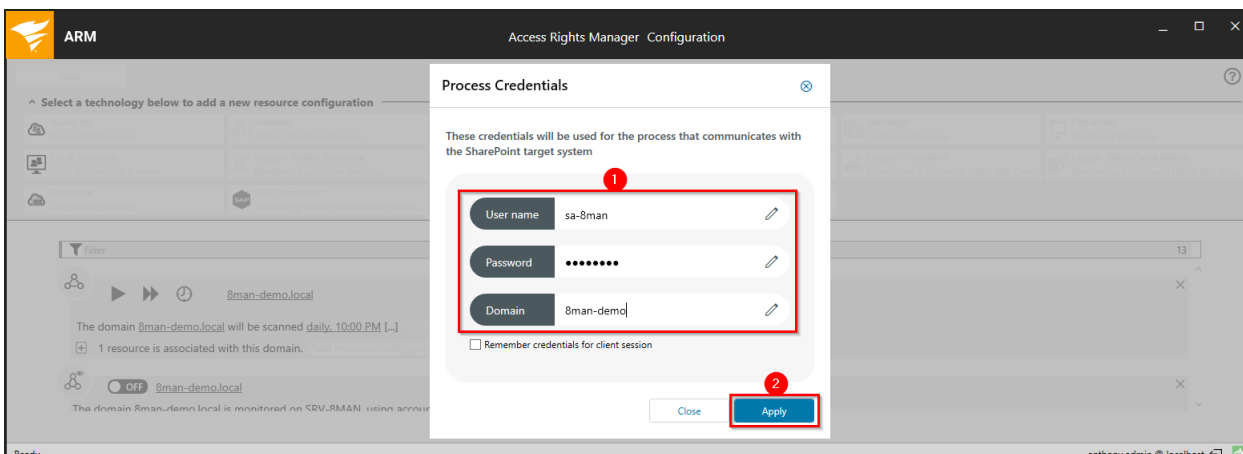
Select the elements to be integrated.

 This option is only working if [WinRM is configured and CredSSP in the additional SharePoint properties is enabled](#).

## Add a SharePoint Online scan



Click the button to add a SharePoint Online resource.

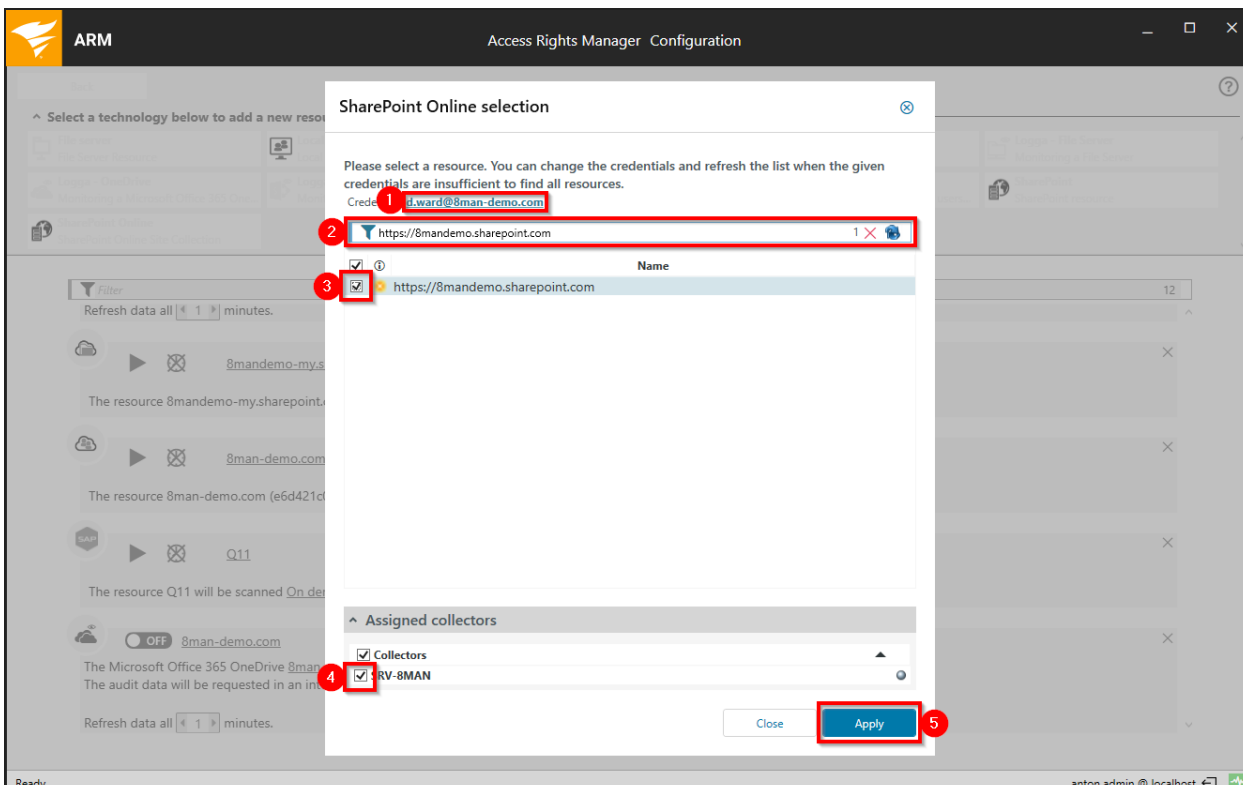


1. Specify the credentials for the "[Process Account](#)". We recommend to use the ARM service account.

**i** The account is not used to scan the SharePoint elements. The scan account will be set up in a later step.

2. Click Apply.

ARM checks the specified credentials. Once the check is successful, the selection of available resources opens.



1. Specify the credentials with which SharePoint Online will be scanned.
2. Specify the URL of the element that you want to add to SharePoint. Confirm the entry with the Enter key.

**⚠** Please be careful, the entry is not checked for validity at this point.

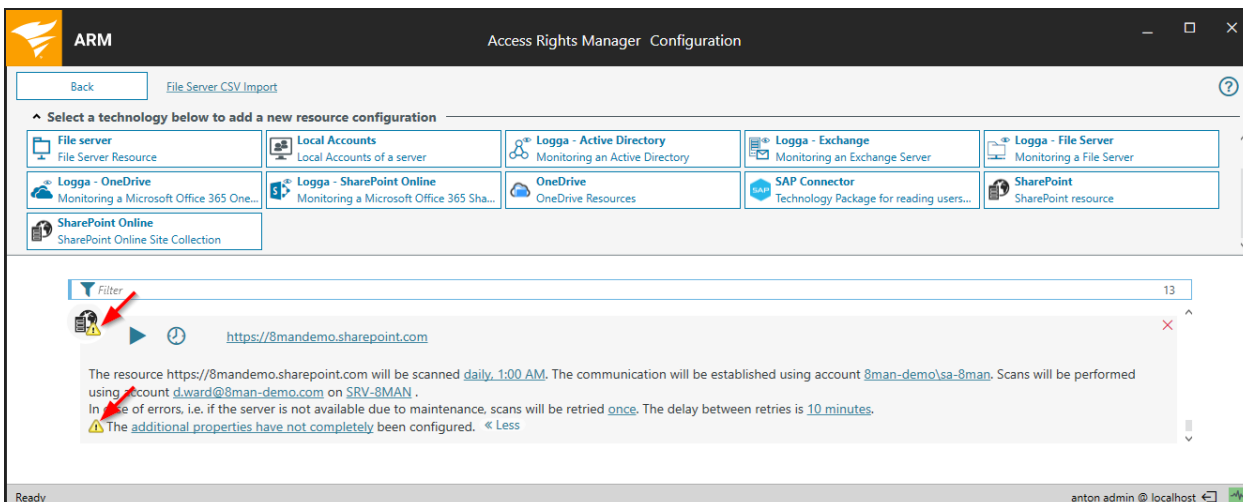
**i** Contrary to SharePoint on-premise, it is **not** possible to specify a server name and select the elements to be scanned later.

3. Select the desired element by activating the check mark.
4. Select a collector to run the scan through.

**i** The collector server must have an Internet connection for the scan.

5. Click Apply.

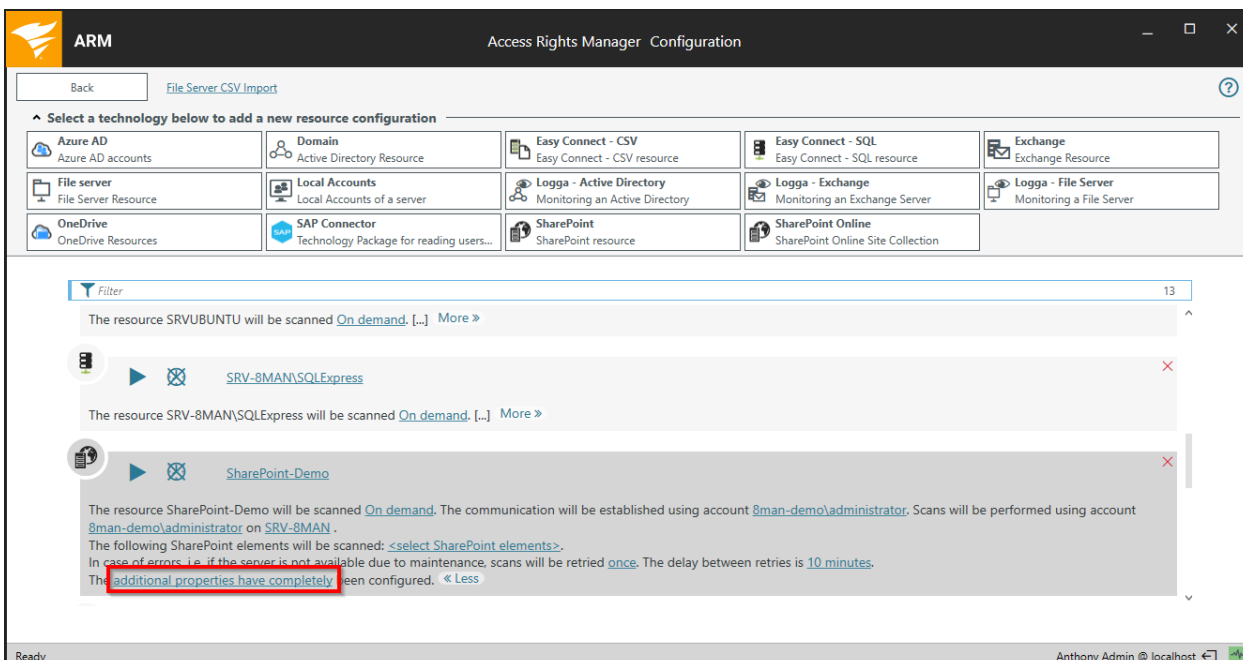




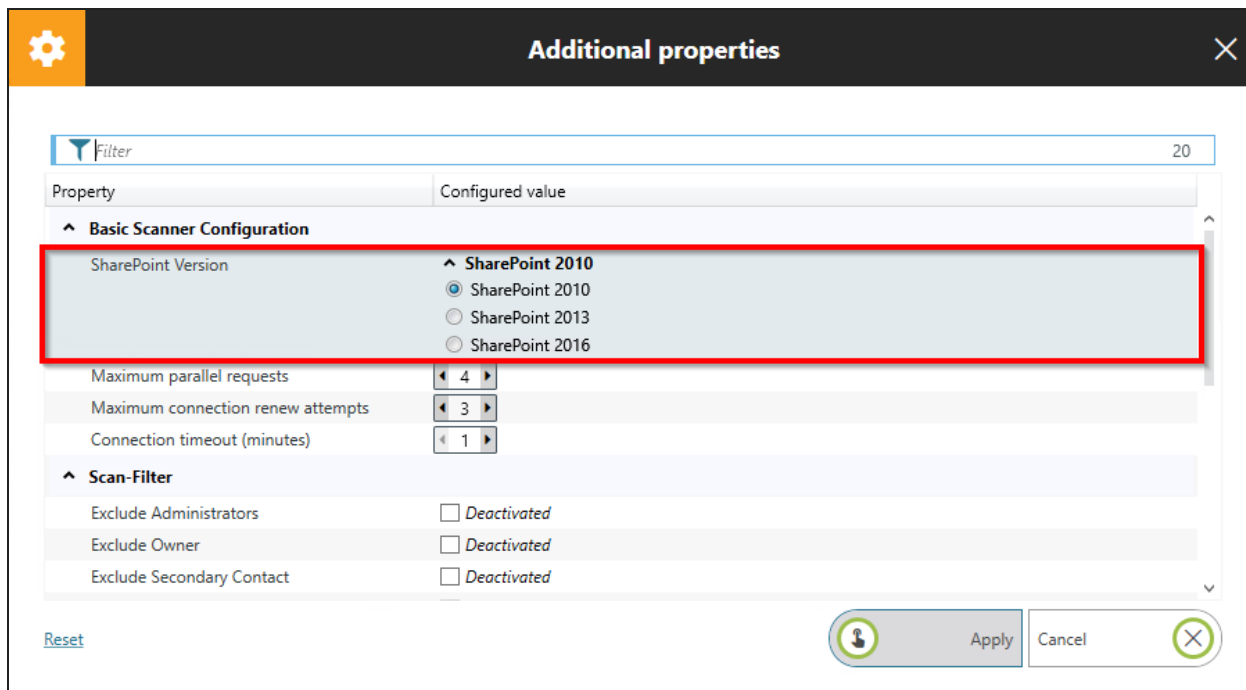
You have successfully created a SharePoint Online scan configuration. The symbols (arrows) indicate that the additional options still need to be set. This procedure is identical for SharePoint Online and SharePoint on-premise and is described in the chapter [Configuring additional SharePoint properties](#).

How to customize a SharePoint Online scan configuration is described in the chapter [Customize a SharePoint Scan Configuration](#).

## Configure additional properties



Click the link.



**Additional properties**

Filter 20

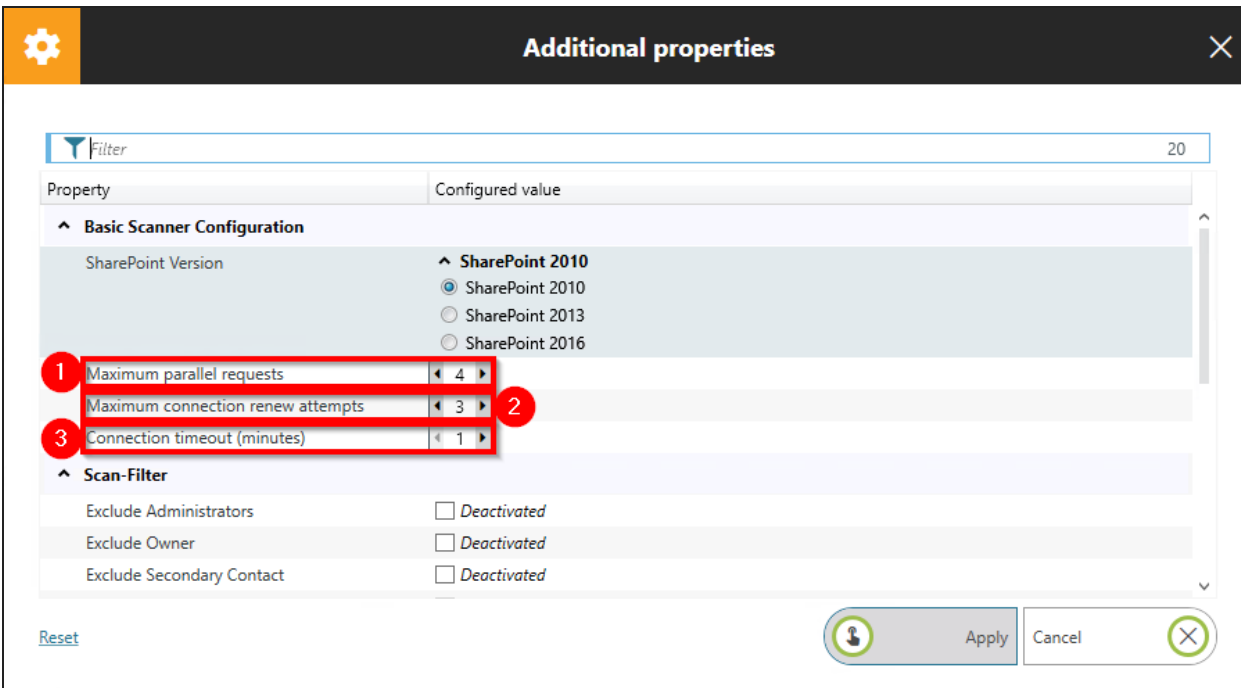
Property	Configured value
<b>Basic Scanner Configuration</b>	
SharePoint Version	<b>SharePoint 2010</b> <input checked="" type="radio"/> SharePoint 2010 <input type="radio"/> SharePoint 2013 <input type="radio"/> SharePoint 2016
Maximum parallel requests	4
Maximum connection renew attempts	3
Connection timeout (minutes)	1
<b>Scan-Filter</b>	
Exclude Administrators	<input type="checkbox"/> Deactivated
Exclude Owner	<input type="checkbox"/> Deactivated
Exclude Secondary Contact	<input type="checkbox"/> Deactivated

[Reset](#) Apply Cancel

Select the SharePoint version.

For SharePoint 2019 please select SharePoint 2016.

**i** To communicate with the SharePoint system, ARM uses Microsoft components that are specific to the version of the SharePoint system that is used. Specifying the correct SharePoint version ensures that all information is shared correctly with the SharePoint system. If the configured version of SharePoint differs from the actual version, this may result in incomplete or incorrect data.



Property	Configured value
<b>Basic Scanner Configuration</b>	
SharePoint Version	<input checked="" type="radio"/> SharePoint 2010 <input type="radio"/> SharePoint 2013 <input type="radio"/> SharePoint 2016
Maximum parallel requests	4
Maximum connection renew attempts	3
Connection timeout (minutes)	1
<b>Scan-Filter</b>	
Exclude Administrators	<input type="checkbox"/> Deactivated
Exclude Owner	<input type="checkbox"/> Deactivated
Exclude Secondary Contact	<input type="checkbox"/> Deactivated

1. Determine how many maximum parallel requests the scan will perform. The higher the number, the higher the scanning speed and the load on the SharePoint server.  
Possible values: 1 to 10
2. Specify how often an attempt is made to connect to the SharePoint server.
3. Specify how long ARM waits for the connection to the SharePoint Server or the result of a query.  
Possible values: 1 to 120 min,  
Recommended for systems with lists and libraries < 5,000 elements: 10 min  
Recommended for systems with lists and libraries > 5,000 elements: 60 min

**Additional properties**

Filter 16

Property	Configured value
<b>Scan-Filter</b>	
Exclude Administrators	<input checked="" type="checkbox"/> Deactivated
Exclude Owner	<input checked="" type="checkbox"/> Deactivated
Exclude Secondary Contact	<input type="checkbox"/> Deactivated
Exclude Limited Access	<input checked="" type="checkbox"/> Activated
Exclude hidden lists	<input type="checkbox"/> Deactivated
Exclude list items	<input type="checkbox"/> Deactivated
Include list items with unique rights only	<input type="checkbox"/> Deactivated
Maximum element scan attempts	3
List view threshold	2,000
<b>Diagnostic settings</b>	
Detailed logging	<input checked="" type="checkbox"/> Deactivated

Reset Apply Cancel

1. **Option enabled:** ARM excludes administrators from the scan. They are not available in views and reports.
2. **Option enabled:** ARM excludes owner from the scan. They are not available in views and reports. This option is not effective for SharePoint 2010. Microsoft does not provide the information about the owner in this release.

**Additional properties**

Filter 16

Property	Configured value
<b>Scan-Filter</b>	
Exclude Administrators	<input type="checkbox"/> Deactivated
Exclude Owner	<input type="checkbox"/> Deactivated
Exclude Secondary Contact	<input type="checkbox"/> Deactivated
Exclude Limited Access	<input checked="" type="checkbox"/> Activated
Exclude hidden lists	<input type="checkbox"/> Deactivated
Exclude list items	<input type="checkbox"/> Deactivated
Include list items with unique rights only	<input type="checkbox"/> Deactivated
Maximum element scan attempts	3
List view threshold	2,000
<b>Diagnostic settings</b>	
Detailed logging	<input checked="" type="checkbox"/> Deactivated

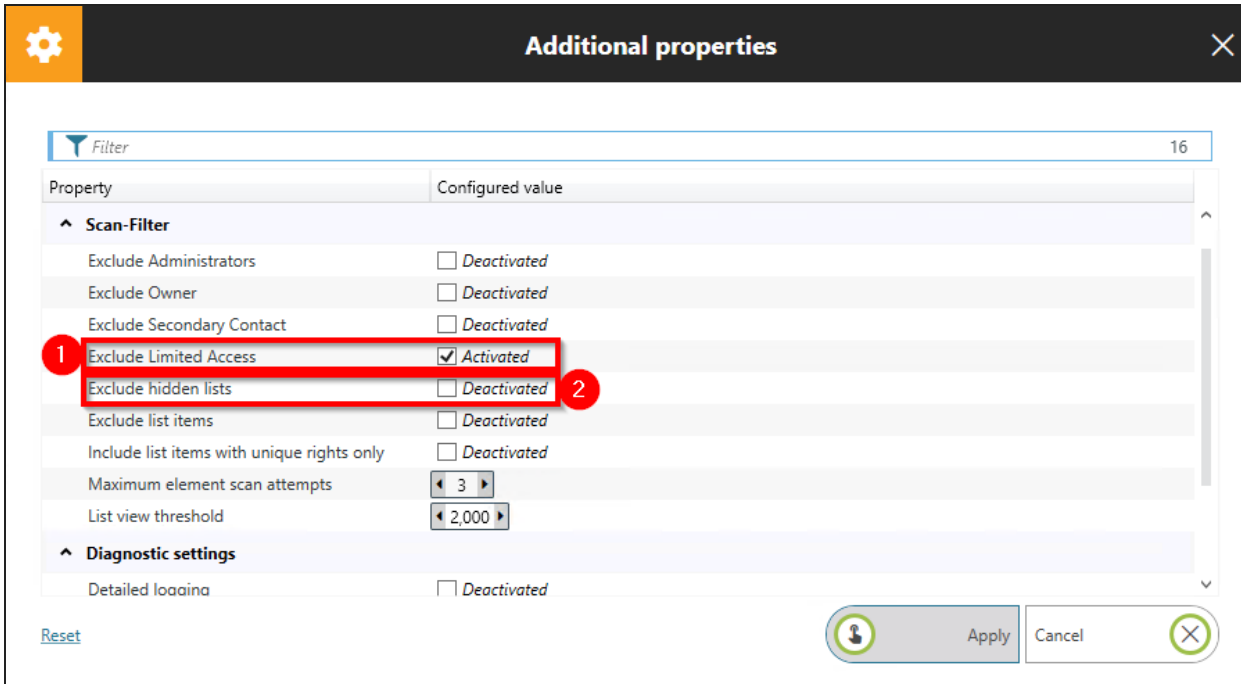
Reset Apply Cancel

**Option enabled:**

ARM excludes secondary contacts from the scan. They are not available in views and reports.

The secondary contact is optional in SharePoint. The option is ineffective if no secondary contact is entered.

This option is not effective for SharePoint 2010. Microsoft does not provide the secondary contact information in this release.



Property	Configured value
<b>Scan-Filter</b>	
Exclude Administrators	<input type="checkbox"/> Deactivated
Exclude Owner	<input type="checkbox"/> Deactivated
Exclude Secondary Contact	<input type="checkbox"/> Deactivated
Exclude Limited Access	<input checked="" type="checkbox"/> Activated
Exclude hidden lists	<input type="checkbox"/> Deactivated
Exclude list items	<input type="checkbox"/> Deactivated
Include list items with unique rights only	<input type="checkbox"/> Deactivated
Maximum element scan attempts	3
List view threshold	2,000
<b>Diagnostic settings</b>	
Detailed logging	<input type="checkbox"/> Deactivated

- Option enabled:** ARM excludes the limited access from the scan. This information is not available in views and reports.  
Limited access is automatically granted by the SharePoint system to a large extent, ensuring that SharePoint users can navigate through the system.
- Option enabled:** ARM excludes hidden lists from the scan. They are not available in views and reports.

**Additional properties**

Filter 16

Property	Configured value
<b>Scan-Filter</b>	
Exclude Administrators	<input type="checkbox"/> Deactivated
Exclude Owner	<input type="checkbox"/> Deactivated
Exclude Secondary Contact	<input type="checkbox"/> Deactivated
Exclude Limited Access	<input checked="" type="checkbox"/> Activated
Exclude hidden lists	<input type="checkbox"/> Deactivated
Exclude list items	<input type="checkbox"/> Deactivated
Include list items with unique rights only	<input type="checkbox"/> Deactivated
Maximum element scan attempts	3
List view threshold	2,000
<b>Diagnostic settings</b>	
Detailed logging	<input type="checkbox"/> Deactivated

Reset Apply Cancel

1. Option enabled: ARM excludes list items from the scan. They are not available in views and reports.
2. Determine whether only list elements or documents with specific permissions (interrupted inheritance) will be scanned.

**Additional properties**

Filter 16

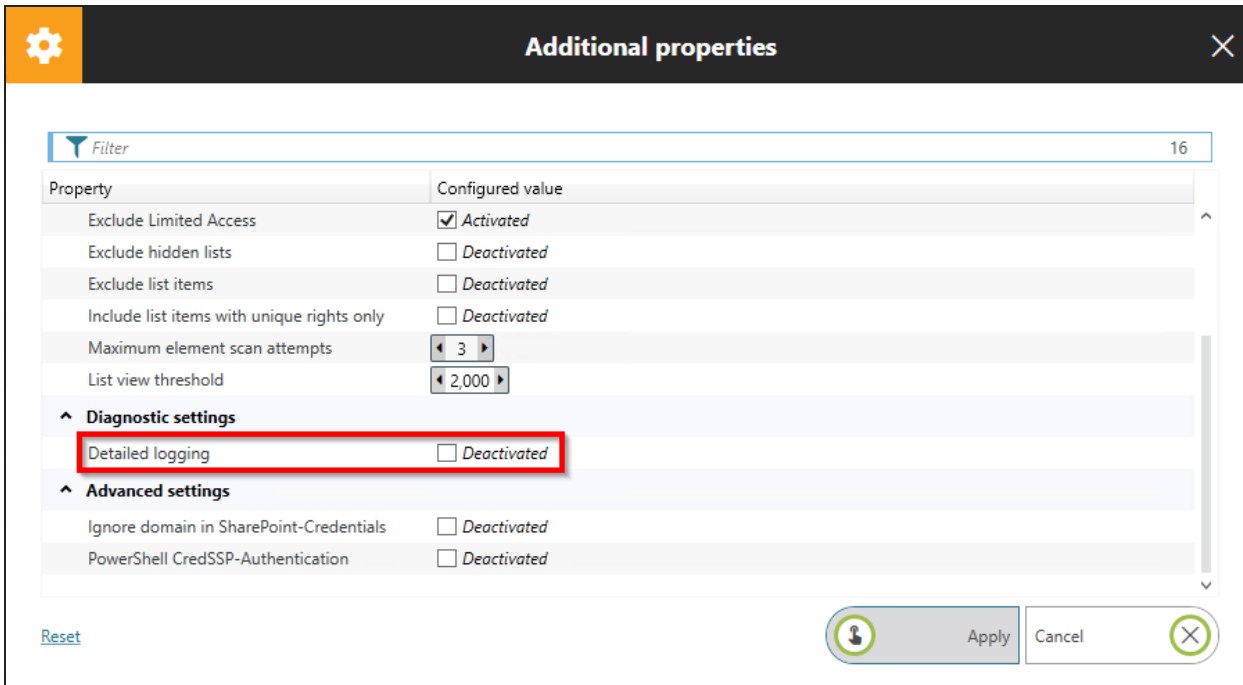
Property	Configured value
<b>Scan-Filter</b>	
Exclude Administrators	<input type="checkbox"/> Deactivated
Exclude Owner	<input type="checkbox"/> Deactivated
Exclude Secondary Contact	<input type="checkbox"/> Deactivated
Exclude Limited Access	<input checked="" type="checkbox"/> Activated
Exclude hidden lists	<input type="checkbox"/> Deactivated
Exclude list items	<input type="checkbox"/> Deactivated
Include list items with unique rights only	<input type="checkbox"/> Deactivated
Maximum element scan attempts	3
List view threshold	2,000
<b>Diagnostic settings</b>	
Detailed logging	<input type="checkbox"/> Deactivated

Reset Apply Cancel

1. Determine the maximum number of attempts after which the scan of a specific SharePoint object

is canceled. Possible values: 1 to 5, Recommended: 3

2. With the threshold value for reading list elements, you determine how many list elements are read at maximum.



The screenshot shows the 'Additional properties' dialog box. At the top, there is a gear icon and the title 'Additional properties' with a close button. Below the title is a filter bar with a dropdown arrow and the text 'Filter' and '16'. The main area contains a table with two columns: 'Property' and 'Configured value'. The table lists several properties, including 'Exclude Limited Access' (checked), 'Exclude hidden lists' (unchecked), 'Exclude list items' (unchecked), 'Include list items with unique rights only' (unchecked), 'Maximum element scan attempts' (3), and 'List view threshold' (2,000). Under the 'Diagnostic settings' section, the 'Detailed logging' property is highlighted with a red box and is currently 'Deactivated'. Under the 'Advanced settings' section, 'Ignore domain in SharePoint-Credentials' and 'PowerShell CredSSP-Authentication' are both 'Deactivated'. At the bottom, there is a 'Reset' link, an 'Apply' button, and a 'Cancel' button with a close icon.

Property	Configured value
Exclude Limited Access	<input checked="" type="checkbox"/> <i>Activated</i>
Exclude hidden lists	<input type="checkbox"/> <i>Deactivated</i>
Exclude list items	<input type="checkbox"/> <i>Deactivated</i>
Include list items with unique rights only	<input type="checkbox"/> <i>Deactivated</i>
Maximum element scan attempts	3
List view threshold	2,000
<b>Diagnostic settings</b>	
Detailed logging	<input type="checkbox"/> <i>Deactivated</i>
<b>Advanced settings</b>	
Ignore domain in SharePoint-Credentials	<input type="checkbox"/> <i>Deactivated</i>
PowerShell CredSSP-Authentication	<input type="checkbox"/> <i>Deactivated</i>

Enable the option for extended error analysis only. If this option is enabled, the scan speed will slow down and the size of the log file of the ARM server will increase faster.

The screenshot shows the 'Additional properties' dialog box with a table of properties. The 'Ignore domain in SharePoint-Credentials' property is highlighted with a red box. The table has two columns: 'Property' and 'Configured value'.

Property	Configured value
Exclude Limited Access	<input checked="" type="checkbox"/> <i>Activated</i>
Exclude hidden lists	<input type="checkbox"/> <i>Deactivated</i>
Exclude list items	<input type="checkbox"/> <i>Deactivated</i>
Include list items with unique rights only	<input type="checkbox"/> <i>Deactivated</i>
Maximum element scan attempts	3
List view threshold	2,000
<b>Diagnostic settings</b>	
Detailed logging	<input type="checkbox"/> <i>Deactivated</i>
<b>Advanced settings</b>	
Ignore domain in SharePoint-Credentials	<input type="checkbox"/> <i>Deactivated</i>
PowerShell CredSSP-Authentication	<input type="checkbox"/> <i>Deactivated</i>

Buttons: [Reset](#), Apply, Cancel,

### Only for SharePoint on-premise:

Activate this property if the system to be scanned is not operated in the local network infrastructure (e.g. by an external service provider) and the account name is used in the form abc@xyz.com.

The screenshot shows the 'Additional properties' dialog box with a table of properties. The 'PowerShell CredSSP-Authentication' property is highlighted with a red box. The table has two columns: 'Property' and 'Configured value'.

Property	Configured value
Exclude Limited Access	<input checked="" type="checkbox"/> <i>Activated</i>
Exclude hidden lists	<input type="checkbox"/> <i>Deactivated</i>
Exclude list items	<input type="checkbox"/> <i>Deactivated</i>
Include list items with unique rights only	<input type="checkbox"/> <i>Deactivated</i>
Maximum element scan attempts	3
List view threshold	2,000
<b>Diagnostic settings</b>	
Detailed logging	<input type="checkbox"/> <i>Deactivated</i>
<b>Advanced settings</b>	
Ignore domain in SharePoint-Credentials	<input type="checkbox"/> <i>Deactivated</i>
PowerShell CredSSP-Authentication	<input type="checkbox"/> <i>Deactivated</i>

Buttons: [Reset](#), Apply, Cancel,

This option is relevant for scanning an **entire** SharePoint farm.



**i** This Option must be enabled if you want to use the [ARM integrated site selection](#) for scanning SharePoint on-premise servers.

Enable it if SharePoint is running in a multi-server environment, i.e. if dedicated servers are used for front end and database.

In order for the scanner to work properly, you must first configure WinRM and prepare PowerShell to use CredSSP authentication.

Prepare SharePoint to use CredSSP

**!** First configure all SharePoint servers and then the ARM server. The ARM server needs to access SharePoint already during the configuration.

### SharePoint frontend server

1. Start the SharePoint Management Shell with local administrator privileges.
2. Activate Remoting for PowerShell  
`Enable-PSRemoting -Force`
3. Activate MultiHop support in WinRM  
`Enable-WSManCredSSP -Role "Server" -Force`

### ARM server

1. Start PowerShell as administrator
2. Activate MultiHop support in WinRM  
`Enable-WSManCredSSP -Role "Client" -DelegateComputer "FQDN-SharePoint-FrontEnd-Server-Name" -Force`  
Replace the yellow marked text with the Fully Qualified Domain Name of your SharePoint frontend server.

For more information please visit [Microsoft](#).

## Customize a SharePoint scan configuration

1. Change the SharePoint Scan configuration name.
2. Change scheduling for scanning.
3. Change the "[Process Account](#)".
4. Change the "[Scan Account](#)".
5. Change the collector server that runs the scan.

## SAP scans

### Required accounts and permissions for an SAP scan

Two accounts must be configured for an SAP scan:

#### Process account

The "Process account" is used to execute the scan process on the selected collector. This account must have local administrator rights and interactive login rights on the collector.

#### Scan-Account

The "scan account" is used for the actual scan. This account must have read access to the following tables:

- UST04
- UST10S
- AGR\_1016b
- USR12

- UST12
- TOBJ

**i** To access the tables, the SAP component "SAP Connector for Windows 64bit" is required, which you can download from the SAP download portal (login required).

The needed files are (64bit versions):

sapnco\_utils.dll

sapnco.dll

The components are contained in the downloaded package.

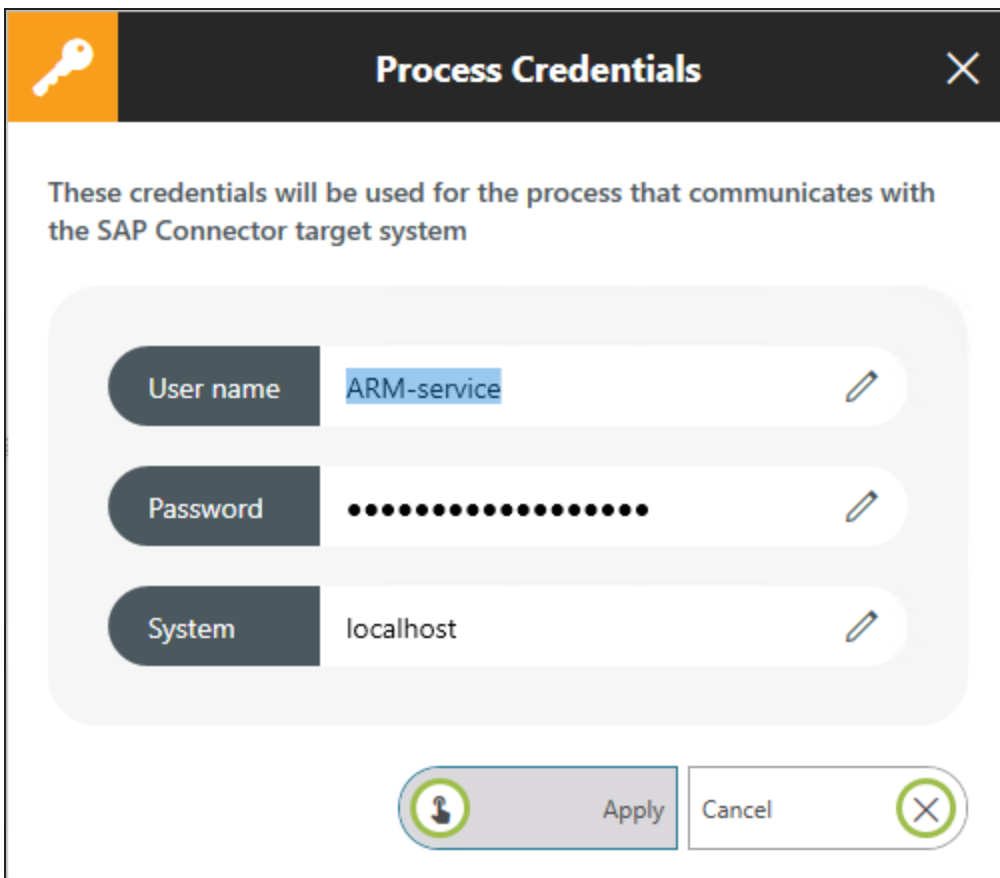
Copy the missing files to the following target directory on the ARM server:

```
%ProgramData%\protected-networks.com\8MAN\technologies\server\[YourDatabase-Id]\63732467f6d84a659c85e7cdaa0f3cde\server\bin
```

## Add an SAP scan


The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there is a navigation bar with 'Back' and 'File Server CSV Import'. Below this is a section titled 'Select a technology below to add a new resource configuration'. A grid of technology options is displayed, with 'SAP Connector - technology Package for reading users...' highlighted by a red box. Other technologies include Azure AD, Logga, OneDrive, Exchange, File server, and SharePoint. Below the grid, a list of existing configurations is shown, including domains like '8man-demo.local' and resources like 'https://8mandemo.sharepoint.com' and 'SRV-8MAN'. The status of each configuration is indicated by a play button and a toggle switch.


In the ARM Configuration Application click Scans > SAP Connector to add an SAP resource.






**Process Credentials** ✕

These credentials will be used for the process that communicates with the SAP Connector target system

User name  

Password  

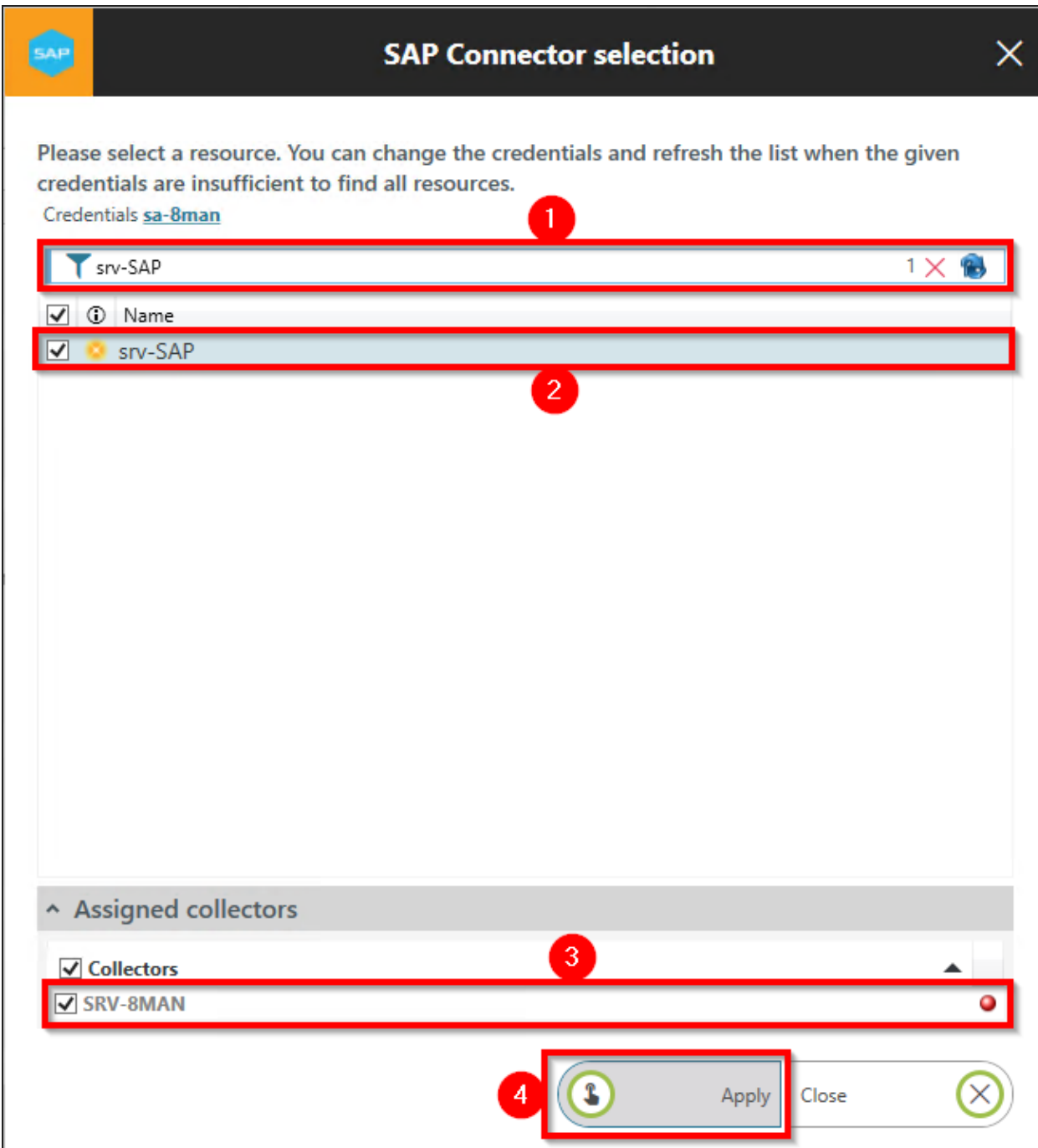
System  

 Apply  

Specify the credentials for the "[Process account](#)".

The account is not used to scan SAP permissions. The "Scan account" is set up in a later step.

After the "Process Account" has been successfully checked, the selection of available resources opens.



**SAP Connector selection**

Please select a resource. You can change the credentials and refresh the list when the given credentials are insufficient to find all resources.

Credentials [sa-8man](#)

srv-SAP

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	srv-SAP

Assigned collectors

<input checked="" type="checkbox"/>	Collectors
<input checked="" type="checkbox"/>	SRV-8MAN

Apply Close

1. Enter the name or IP address of the SAP server. Confirm your input with the ENTER key.
2. Activate the added entry (check the box).
3. Select one or more collectors to scan through.
4. Click "Apply".

The screenshot shows the ARM Configuration window with a list of scan configurations. A red box highlights the configuration for 'srv-SAP'. The configuration details are as follows:

- Resource: srv-SAP
- Scanned: daily, 1:00 AM
- Communication: established using account ARM-service
- Scans performed using account: ARM-service in SRV-SMAN
- Retries: scans will be retried once if the server is not available due to maintenance
- Delay between retries: 10 minutes
- Warning: The additional properties have not completely been configured.

You have created a new SAP scan configuration.

1. The warning indicates that you need to [configure additional properties](#) before you can successfully run a SAP scan.
2. The credentials for the "Scan Account" are prefilled with those of the "Process Account". Click on the link to add different credentials for the [scan account](#).

# Customize an SAP scan configuration

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there's a navigation bar with 'Back' and 'File Server: CSV Import'. Below that is a section 'Select a technology below to add a new resource configuration' with various icons for different technologies like Azure AD, Logga, SharePoint Online, Domain, Easy Connect, Exchange, File server, Local Accounts, etc. The main area displays a list of scan configurations. The configuration for 'srv-SAP' is highlighted in grey and has three red boxes with numbers: 1 is over the play/pause button, 2 is over the schedule 'daily, 1:00 AM', and 3 is over the account 'sa-8man'.

1. Start or stop a scan.
2. Change the schedule for periodic scanning.

This screenshot shows the same 'srv-SAP' configuration as the previous one, but with different red boxes and numbers. Number 1 points to the 'ARM-service' account in the text 'The communication will be established using account sa-8man'. Number 2 points to the 'ARM-service' account in the text 'Scans will be performed using account sa-8man on SRV8MAN'. Number 3 points to the 'SRV8MAN' account in the same text.

1. Change the process account.
2. Change the scan account.

3. Specify which collector is to be used for the scan.

### Configure additional SAP properties

The screenshot shows the 'Access Rights Manager - Configuration' window. At the bottom, the 'srv-SAP' resource is selected. A red box highlights the text: "If additional properties have completed, see configured." Below this text, there are buttons for 'Apply' and 'Cancel'.

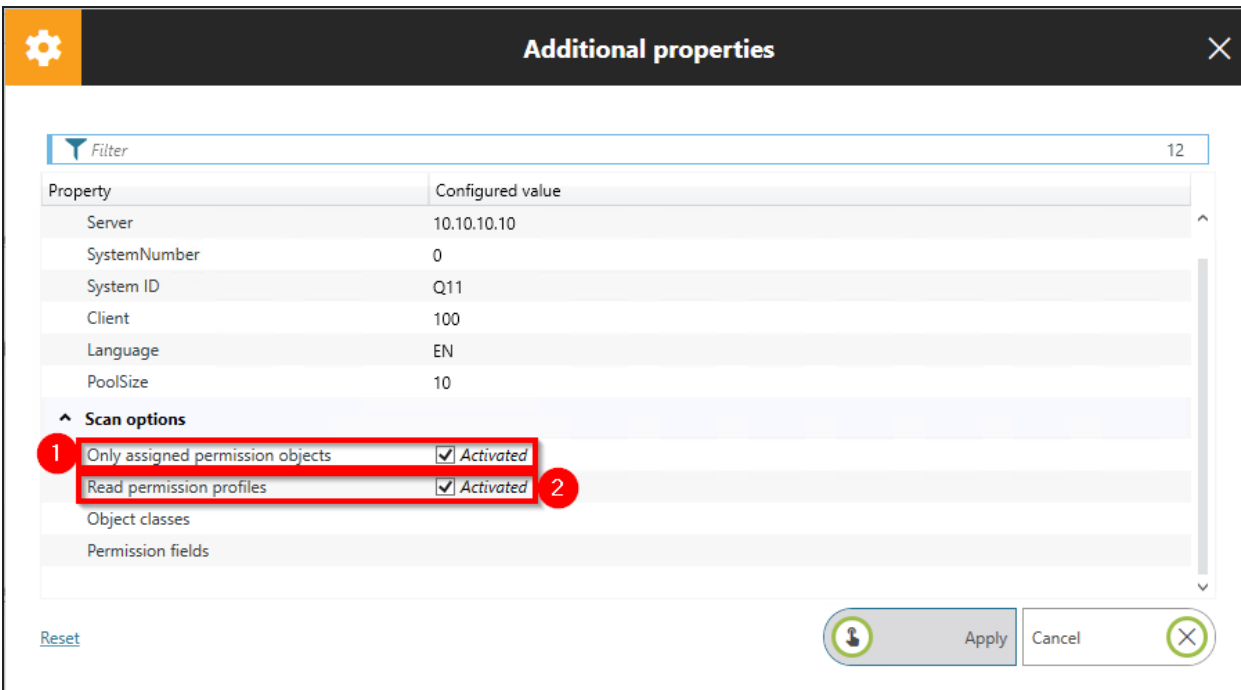
Click on the link to configure the additional properties.

The 'Additional properties' dialog box is shown. The 'Connection settings' section is expanded, and a red box highlights the 'Server' field with the value '10.10.10.10'. Other fields include 'SystemNumber' (0), 'System ID' (Q11), 'Client' (100), 'Language' (EN), and 'PoolSize' (10). The 'Scan options' section is also visible with 'Only assigned permission objects' and 'Read permission profiles' checked and activated.

Property	Configured value
<b>Connection settings</b>	
Server	10.10.10.10
SystemNumber	0
System ID	Q11
Client	100
Language	EN
PoolSize	10
<b>Scan options</b>	
Only assigned permission objects	<input checked="" type="checkbox"/> Activated
Read permission profiles	<input checked="" type="checkbox"/> Activated
Object classes	
Permission fields	

Enter the access data for your SAP system.

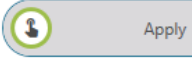





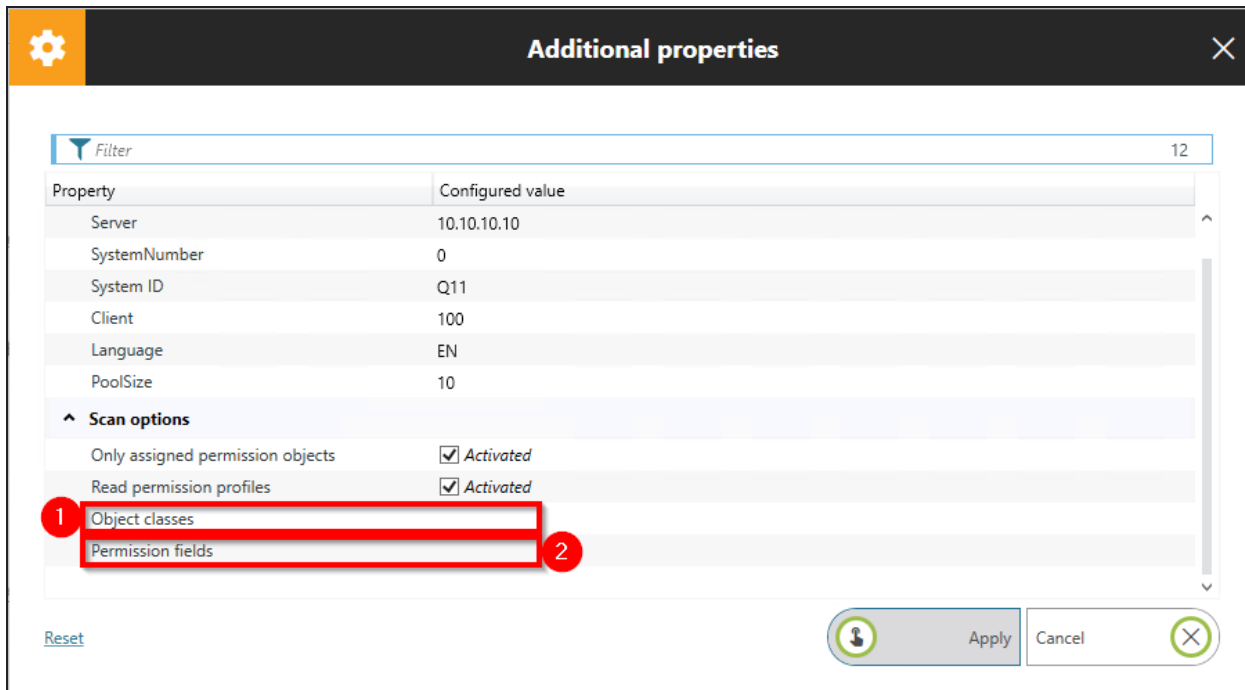
**Additional properties**

Filter 12

Property	Configured value
Server	10.10.10.10
SystemNumber	0
System ID	Q11
Client	100
Language	EN
PoolSize	10
<b>Scan options</b>	
1 Only assigned permission objects	<input checked="" type="checkbox"/> Activated
Read permission profiles	<input checked="" type="checkbox"/> Activated 2
Object classes	
Permission fields	

[Reset](#)  

1. Activate this option if you only want to include objects in the analysis that have been assigned permissions.
2. Activate this option to read authorization profiles and include them in the analysis. If you assign authorizations using roles and SAP automatically generates corresponding authorization profiles, activating this option can lead to the display of duplicate authorization paths. In this case, deactivate the option.



**Additional properties**

Filter 12

Property	Configured value
Server	10.10.10.10
SystemNumber	0
System ID	Q11
Client	100
Language	EN
PoolSize	10

**Scan options**

- Only assigned permission objects  Activated
- Read permission profiles  Activated
- Object classes
- Permission fields

Reset Apply Cancel

1. **Optional:**

Use a list of object classes separated by semicolons to specify which object classes are to be read. This restricts the area to be read. Leave the field empty to read all object classes.

2. **Optional:**

Use a list of authorization fields separated by semicolons to specify which authorization fields are to be read. This restricts the area to be read. Leave the field empty to read all authorization fields.


## Prepare Office 365 integration

ARM uses the Microsoft Graph API to access Azure AD and OneDrive.

The following permissions are required:

- Application.ReadWrite.OwnedBy
- Directory.ReadWrite.All
- Files.ReadWrite.All
- Group.ReadWrite.All
- Member.Read.Hidden
- User.ReadWrite.All
- Sites.FullControl.All

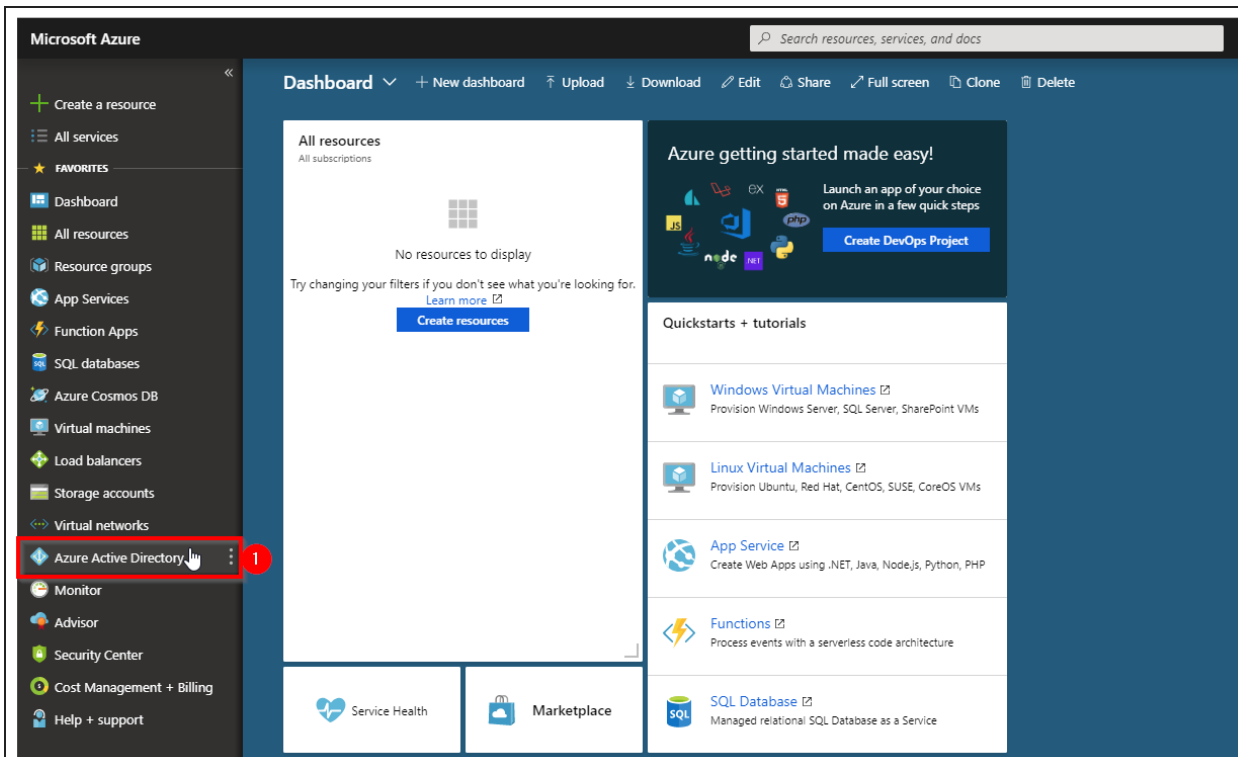
ARM uses the Office 365 Management API to access OneDrive and SharePoint Online events.

 To retrieve events, Office 365 auditing must be enabled. How to enable auditing can be found at [Microsoft](#).

The following permissions are required:

- ActivityFeed.Read
- ServiceHealth.Read

To assign the required permissions, perform the following steps.



Go to the Azure Portal Website (<https://ms.portal.azure.com>) and log in with admin credentials.

1. Click "Azure Active Directory".

The screenshot shows the Microsoft Azure portal interface. On the left, there is a navigation pane with various service categories. Under the 'App registrations (Preview)' category, the option is highlighted with a red box and a mouse cursor. The main content area shows the 'Overview' page for a directory named 'Protected Networks GmbH', with options for 'Switch directory' and 'Delete directory'. Below this, there are sections for 'Sign-ins' and 'What's new in Azure AD'.

Click "App registrations (Preview)".

The screenshot shows the 'App registrations (Preview)' page in the Azure portal. The page title is 'Protected Networks GmbH - App registrations (Preview)'. At the top, there are navigation links for 'New registration', 'Endpoints', and 'Troubleshooting'. The 'New registration' button is highlighted with a red box and a mouse cursor. Below this, there is a banner indicating that the preview experience is being used. The main content area shows a search bar and a list of applications under the 'Owned applications' tab. The list includes three entries with their respective display names and icons.

Add a new app registration.

Home > [App registrations \(Preview\)](#) > Register an application

## Register an application

PREVIEW

### \* Name

The user-facing display name for this application (this can be changed later).

  **1**

### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only ([Learn more about this account type](#))
- Accounts in any organizational directory
- Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

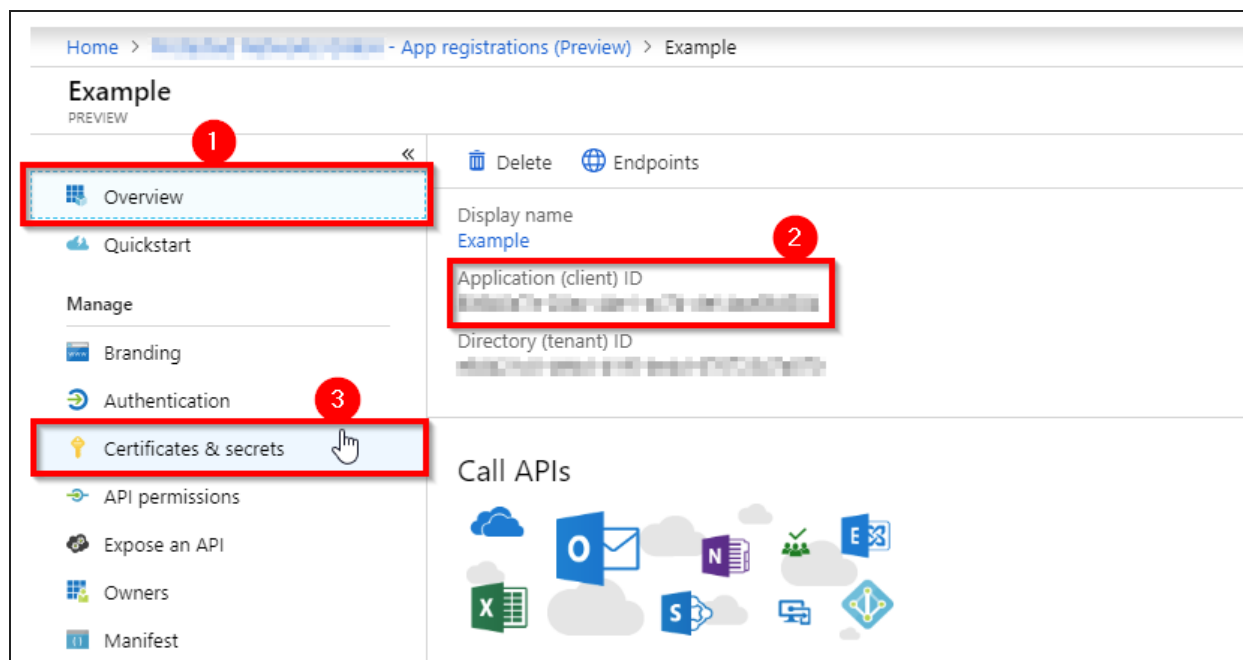
[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URL after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

   **2**

1. Assign a name to the registration.
2. Click "Register".



Home > App registrations (Preview) > Example

### Example

PREVIEW

Overview (1)

Quickstart

Manage

Branding

Authentication

Certificates & secrets (3)

API permissions

Expose an API

Owners

Manifest

Delete Endpoints

Display name  
Example

Application (client) ID (2)  
[Redacted]

Directory (tenant) ID  
[Redacted]

### Call APIs

[Icons for various services: Office 365, Azure, etc.]

1. Click "Overview".
2. Copy the Application ID to a file. The Application ID will later be used as the user name to access Azure/O365 resources.
3. Click "Certificates & secrets".

### Example - Certificates & secrets

PREVIEW

- Overview
- Quickstart
- Manage
  - Branding
  - Authentication
  - Certificates & secrets**
  - API permissions
  - Expose an API
  - Owners
  - Manifest
- Support + Troubleshooting
  - Troubleshooting
  - New support request

Credentials enable applications to identify themselves to the authentication service when receiving a level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

#### Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token.

[Upload certificate](#)

THUMBPRINT	START DATE
------------	------------

#### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE
-------------	---------	-------

Add a new "Client secret".

### Example - Certificates & secrets

PREVIEW

- Overview
- Quickstart
- Manage
  - Branding
  - Authentication
  - Certificates & secrets**
  - API permissions
  - Expose an API
  - Owners
  - Manifest
- Support + Troubleshooting
  - Troubleshooting
  - New support request

#### Add a client secret

Description  1

Expires

In 1 year

In 2 years

Never 2

[Add](#) 3 [Cancel](#)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE
-------------	---------	-------

1. Enter a description.
2. Set the expiration date to "Never".
3. Click "Add".

Example - Certificates & secrets  
PREVIEW

Overview  
Quickstart  
Manage  
Branding  
Authentication  
Certificates & secrets  
API permissions  
Expose an API  
Owners  
Manifest  
Support + Troubleshooting  
Troubleshooting  
New support request

Copy the new client secret value. You won't be able to retrieve it after you leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates  
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

THUMBPRINT	START DATE	EXPIRES
------------	------------	---------

Client secrets  
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

DESCRIPTION	EXPIRES	VALUE
Example description	12/31/2299	[Redacted]

Save the value to a file. The Client secret will later be used as the password to access Azure/O365 resources.

Example - Certificates & secrets  
PREVIEW

Overview  
Quickstart  
Manage  
Branding  
Authentication  
Certificates & secrets  
API permissions  
Expose an API  
Owners  
Manifest  
Support + Troubleshooting  
Troubleshooting  
New support request

Copy the new client secret value. You won't be able to retrieve it after you leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates  
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

THUMBPRINT

Client secrets  
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

DESCRIPTION	VALUE
Example description	[Redacted]

Click "API permissions".



**Example - API permissions**  
PREVIEW

Overview  
Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- API permissions**
- Expose an API

### API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent p

**+ Add a permission**

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▼ Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. [See best practices for requesting permissions](#)

Click "Add a permission".

Home > Example - API permissions

**Example - API permissions**  
PREVIEW

Overview  
Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- API permissions**
- Expose an API
- Owners
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

### Request API permissions

PREVIEW

Select an API

Microsoft APIs | APIs my organization uses | My APIs

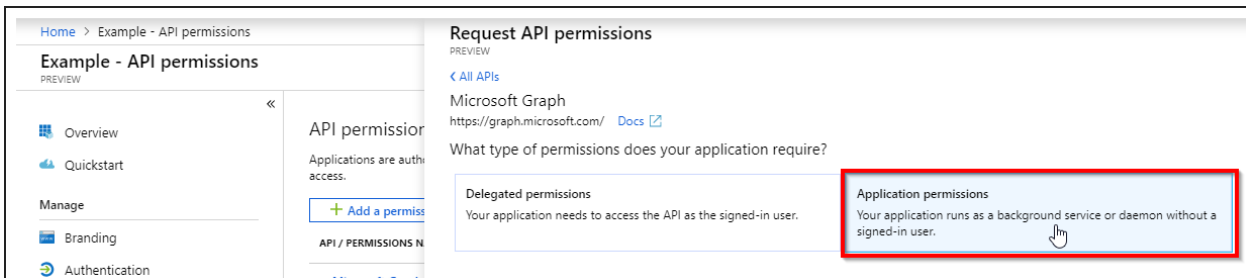
Commonly used Microsoft APIs

**Microsoft Graph**

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

<b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets	<b>Azure Rights Management Services</b> Allow validated users to read and write protected content	<b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal
<b>Data Export Service for Microsoft Dynamics 365</b> Export data from Microsoft Dynamics CRM organization to an external destination	<b>Dynamics CRM</b> Access the capabilities of CRM business software and ERP systems	<b>Flow Service</b> Embed flow templates and manage flows
<b>Intune</b> Programmatic access to Intune data	<b>Office 365 Management APIs</b> Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity	<b>OneNote</b> Create and manage notes, lists, pictures, files, and more in OneNote notebooks

Click "Microsoft Graph".



Click "Application permissions".

## Request API permissions

PREVIEW

[< All APIs](#)

Microsoft Graph  
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
▶ AccessReview	
▼ Application (1)	
<input type="checkbox"/> Application.ReadWrite.All Read and write all applications ⓘ	Yes
<input checked="" type="checkbox"/> Application.ReadWrite.OwnedBy Manage apps that this app creates or owns ⓘ	Yes
▶ AuditLog	
▶ Calendars	
▶ Calls	
▶ ChannelMessage	
▶ Chat	
▶ Contacts	
▶ Device	
▼ Directory (1)	
<input type="checkbox"/> Directory.Read.All Read directory data ⓘ	Yes
<input type="checkbox"/> Directory.ReadWrite.All	

[Add permissions](#) [Discard](#)

1. Enable **all** of the following permissions:

- Application.ReadWrite.OwnedBy
- Directory.ReadWrite.All
- Files.ReadWrite.All
- Group.ReadWrite.All
- Member.Read.Hidden

- User.ReadWrite.All
  - Sites.FullControl.All
2. Save your settings.

Home > App registrations (Preview) > Example - API permissions (Preview)

### Request API permissions

PREVIEW

Select an API

Microsoft APIs | APIs my organization uses | My APIs

#### Commonly used Microsoft APIs

**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Rights Management Services**  
Allow validated users to read and write protected content

**Azure Service Management**  
Programmatic access to much of the functionality available through the Azure portal

**Flow Service**  
Embed flow templates and manage flows

**Intune**  
Programmatic access to Intune data

**Office 365 Management APIs**  
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

**OneNote**

**Power BI Service**

**SharePoint**

Click "Office 365 Management APIs".

### Request API permissions

PREVIEW

< All APIs

**Office 365 Management APIs**  
<https://manage.office.com/> Docs

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.


**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

Select "Application permissions".

## Request API permissions

PREVIEW

[All APIs](#)

 Office 365 Management APIs  
<https://manage.office.com/> [Docs](#)

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

Select permissions 1 expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
<b>ActivityFeed (1)</b> <span>2</span>	
<input checked="" type="checkbox"/> ActivityFeed.Read Read activity data for your organization ⓘ	Yes
<input type="checkbox"/> ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data ⓘ	Yes
<b>ActivityReports</b>	
<input type="checkbox"/> ActivityReports.Read Read activity reports for your organization ⓘ	Yes
<input type="checkbox"/> ActivityReports.Read Read activity reports for your organization ⓘ	Yes
<b>ServiceHealth (1)</b> <span>3</span>	
<input checked="" type="checkbox"/> ServiceHealth.Read Read service health information for your organization ⓘ	Yes
<b>ThreatIntelligence</b>	
<input type="checkbox"/> ThreatIntelligence.Read Read threat intelligence data for your organization ⓘ	Yes
<input type="checkbox"/> ThreatIntelligence.Read Read threat intelligence data for your organization ⓘ	Yes

4 Add permissions Discard

1. Click "expand all".
2. Enable "ActivityFeed.Read".
3. Enable "ServiceHealth.Read".
4. Click "Add permissions".

Home > Example - API permissions

### Example - API permissions

PREVIEW

Permissions have changed. Users and/or admins will have to consent even if they have already done so previously.

#### API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Microsoft Graph (7)			
Application.ReadWrite.OwnedBy	Application	Manage apps that this app creates or owns	Yes ⚠ Not granted for Protec...
Directory.ReadWrite.All	Application	Read and write directory data	Yes ⚠ Not granted for Protec...
Files.ReadWrite.All	Application	Read and write files in all site collections	Yes ⚠ Not granted for Protec...
Group.ReadWrite.All	Application	Read and write all groups	Yes ⚠ Not granted for Protec...
Member.Read.Hidden	Application	Read all hidden memberships	Yes ⚠ Not granted for Protec...
User.Read	Delegated	Sign in and read user profile	- ✓
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes ⚠ Not granted for Protec...

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. [See best practices for requesting permissions](#)

#### Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

[Grant admin consent for \[Application Name\]](#)

Click "Grant admin consent for...".

### Example - API permissions

PREVIEW

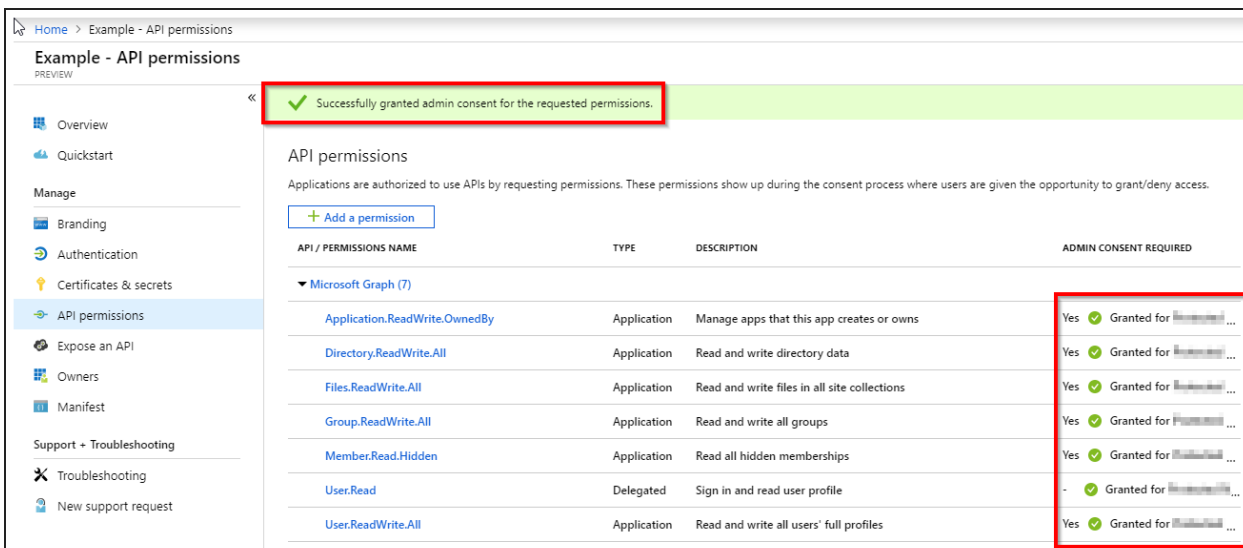
Do you want to grant consent for the requested permissions for all accounts in Protected Network?

**Yes** No

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

[+ Add a permission](#)

Confirm the dialog box.



Example - API permissions

PREVIEW

Successfully granted admin consent for the requested permissions.

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Microsoft Graph (7)			
Application.ReadWrite.OwnedBy	Application	Manage apps that this app creates or owns	Yes <input checked="" type="checkbox"/> Granted for [redacted] ...
Directory.ReadWrite.All	Application	Read and write directory data	Yes <input checked="" type="checkbox"/> Granted for [redacted] ...
Files.ReadWrite.All	Application	Read and write files in all site collections	Yes <input checked="" type="checkbox"/> Granted for [redacted] ...
Group.ReadWrite.All	Application	Read and write all groups	Yes <input checked="" type="checkbox"/> Granted for [redacted] ...
Member.Read.Hidden	Application	Read all hidden memberships	Yes <input checked="" type="checkbox"/> Granted for [redacted] ...
User.Read	Delegated	Sign in and read user profile	- <input checked="" type="checkbox"/> Granted for [redacted] ...
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes <input checked="" type="checkbox"/> Granted for [redacted] ...

If the approval has been given successfully, the Application ID and Client secret can be used to configure Azure resources in ARM.

## Azure AD scans

### Required accounts and permissions for an Azure AD scan

To perform an Azure AD scan, you must configure two accounts:


#### Process Account

The "Process account" is used to execute the scan process on the selected collector. This account must have local administrative rights and interactive logon privileges on the collector.

#### Scan Account

The "scan account" is used for the actual scan. This account must have the permissions described in the section "[Prepare Office 365 integration](#)".

### Add Azure AD scans

 You must at first [set up access in the Azure portal](#) to be able to configure an Azure AD scan completely.

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there are navigation buttons for 'Back' and 'File Server CSV Import'. Below this is a section titled 'Select a technology below to add a new resource configuration'. This section contains a grid of options:

- Azure AD** (highlighted with a red box): Azure AD accounts
- Domain**: Active Directory Resource
- Easy Connect - CSV**: Easy Connect - CSV resource
- Easy Connect - SQL**: Easy Connect - SQL resource
- Exchange**: Exchange Resource
- File server**: File Server Resource
- Local Accounts**: Local Accounts of a server
- Logga - Active Directory**: Monitoring an Active Directory
- Logga - Exchange**: Monitoring an Exchange Server
- Logga - File Server**: Monitoring a File Server
- OneDrive**: OneDrive Resources
- SAP Connector**: Technology Package for reading users...
- SharePoint**: SharePoint resource
- SharePoint Online**: SharePoint Online Site Collection

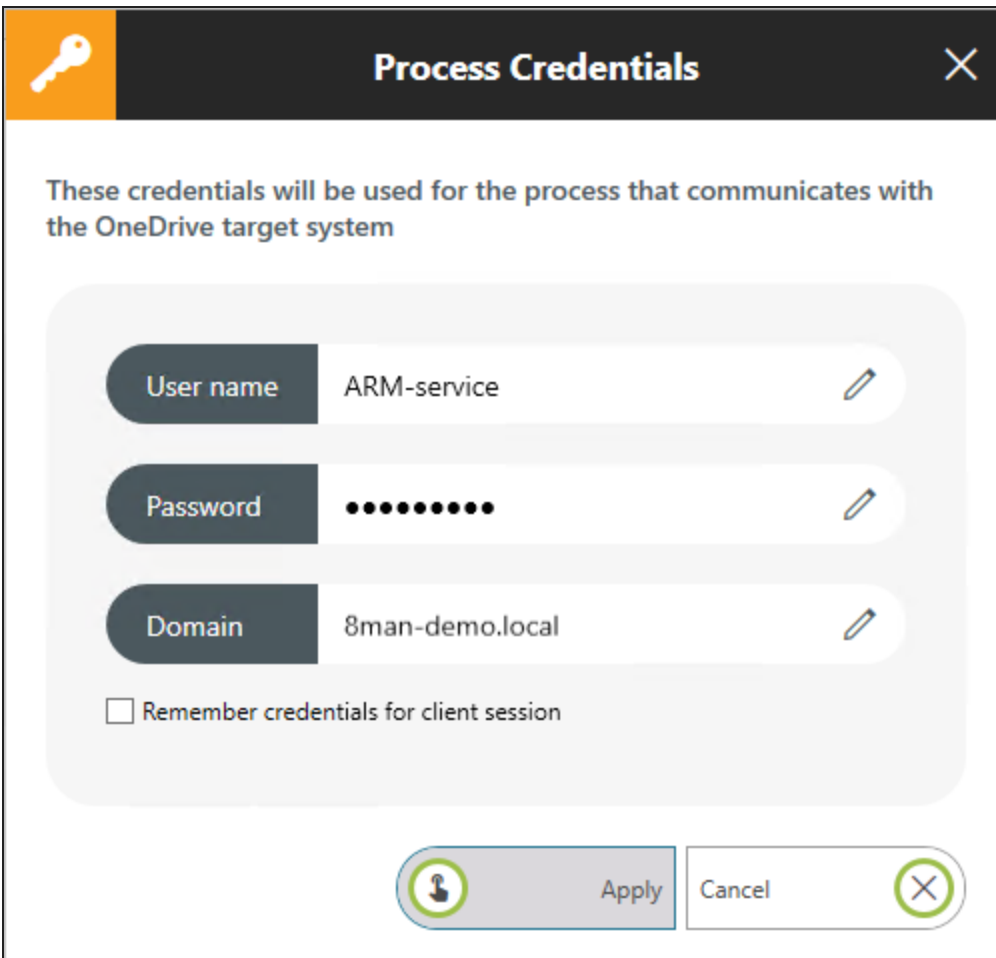
Below the grid is a 'Filter' input field with the value '13'. The main area displays a list of resources:

- 8man-demo.local**: The domain 8man-demo.local will be scanned **daily, 10:00 PM** [...] More »  
1 resource is associated with this domain. Add resource configuration +
- 8man-demo.local** (OFF): The domain 8man-demo.local is monitored on SRV-8MAN using account 8man-demo\sa-8man. Following filters have been set. Refresh data all 1 minutes.
- https://8mandemo.sharepoint.com**: The resource https://8mandemo.sharepoint.com will be scanned **On demand**, [...] More »

At the bottom left, it says 'Ready'. At the bottom right, it says 'Anthony Admin @ localhost'.

From the ARM Configuration Application > Scans, click "Azure AD".





**Process Credentials**

These credentials will be used for the process that communicates with the OneDrive target system

User name ARM-service

Password

Domain 8man-demo.local

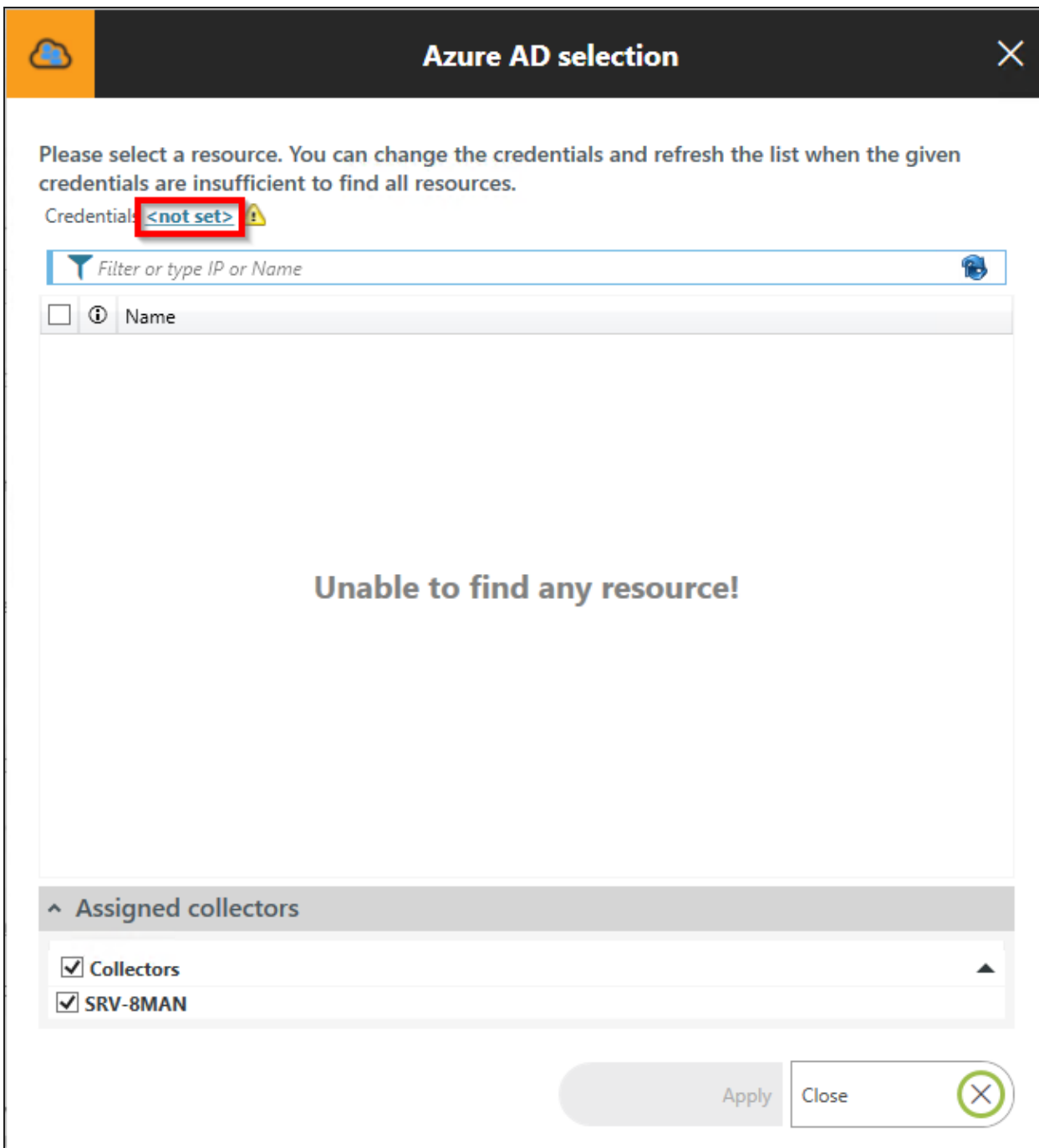
Remember credentials for client session

Apply Cancel

Specify the credentials for the "[Process Account](#)".


The account will not be used to scan the Azure AD. This account will be set up in a later step.


After successfully verifying the "Process Account", the available resources selection opens.




**Azure AD selection** ✕


Please select a resource. You can change the credentials and refresh the list when the given credentials are insufficient to find all resources.


Credential: <not set> 



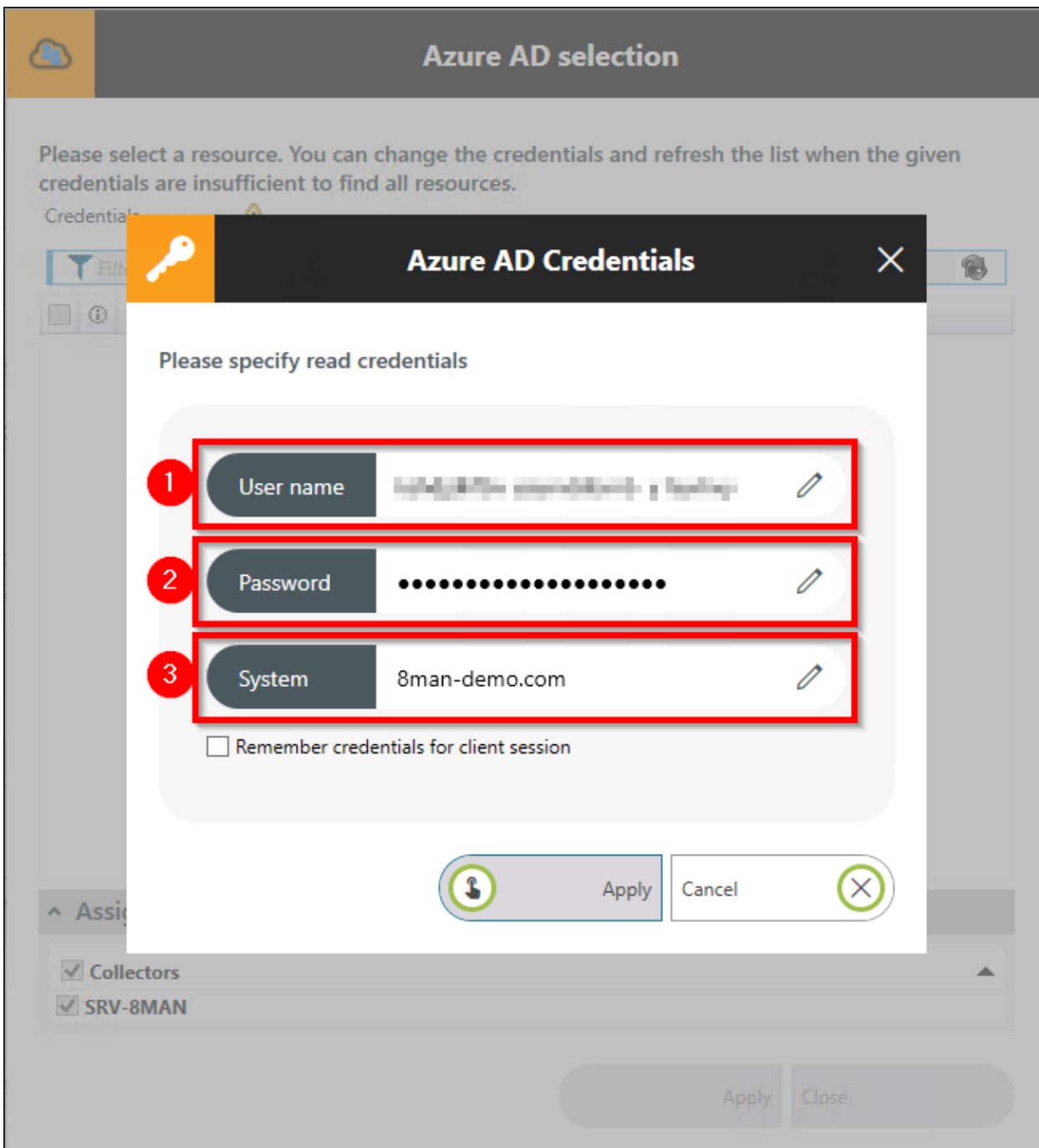
<input type="checkbox"/>	 Name
<b>Unable to find any resource!</b>	

^ Assigned collectors

- Collectors 
- SRV-8MAN

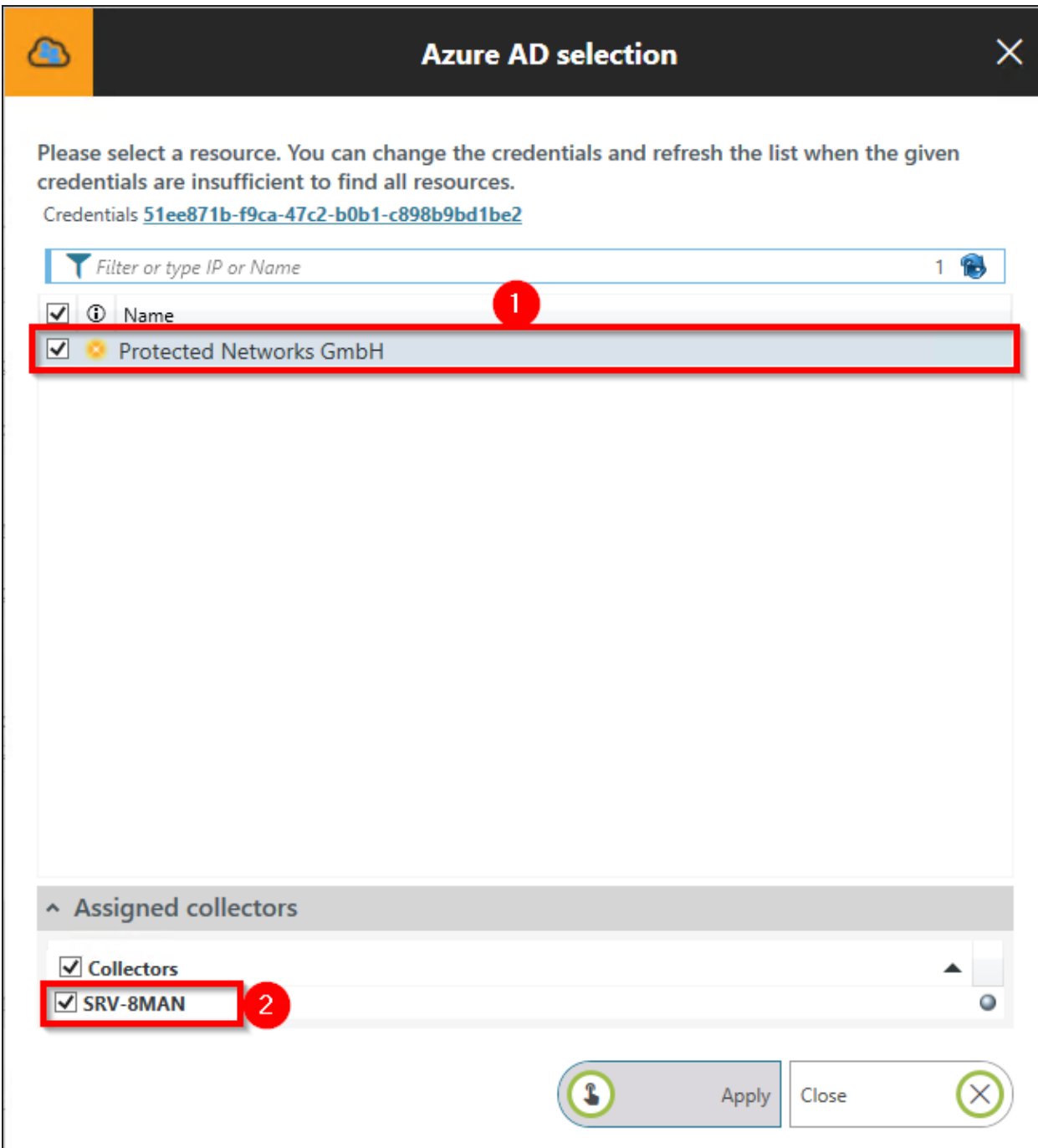
Apply Close 

Click the link.



Enter the access data that you created during [preparation](#) on the Azure portal.

1. Enter the [application ID](#) as the user name.
2. Enter the [client secret](#) as the password.
3. Enter the online domain.



**Azure AD selection**

Please select a resource. You can change the credentials and refresh the list when the given credentials are insufficient to find all resources.

Credentials [51ee871b-f9ca-47c2-b0b1-c898b9bd1be2](#)

Filter or type IP or Name 1

<input checked="" type="checkbox"/>	ⓘ	Name
<input checked="" type="checkbox"/>	★	Protected Networks GmbH

Assigned collectors

<input checked="" type="checkbox"/>	Collectors
<input checked="" type="checkbox"/>	SRV-8MAN

Apply Close

1. Activate the required resource (check the box).
2. Select one or more collectors. Note that the collector servers must have an Internet connection.

## OneDrive scans

## Required accounts and permissions for a OneDrive scan

To perform a OneDrive scan, you must configure two accounts:

### Process Account

The "Process account" is used to execute the scan process on the selected collector. This account must have local administrative rights and interactive logon privileges on the collector.

### Scan Account

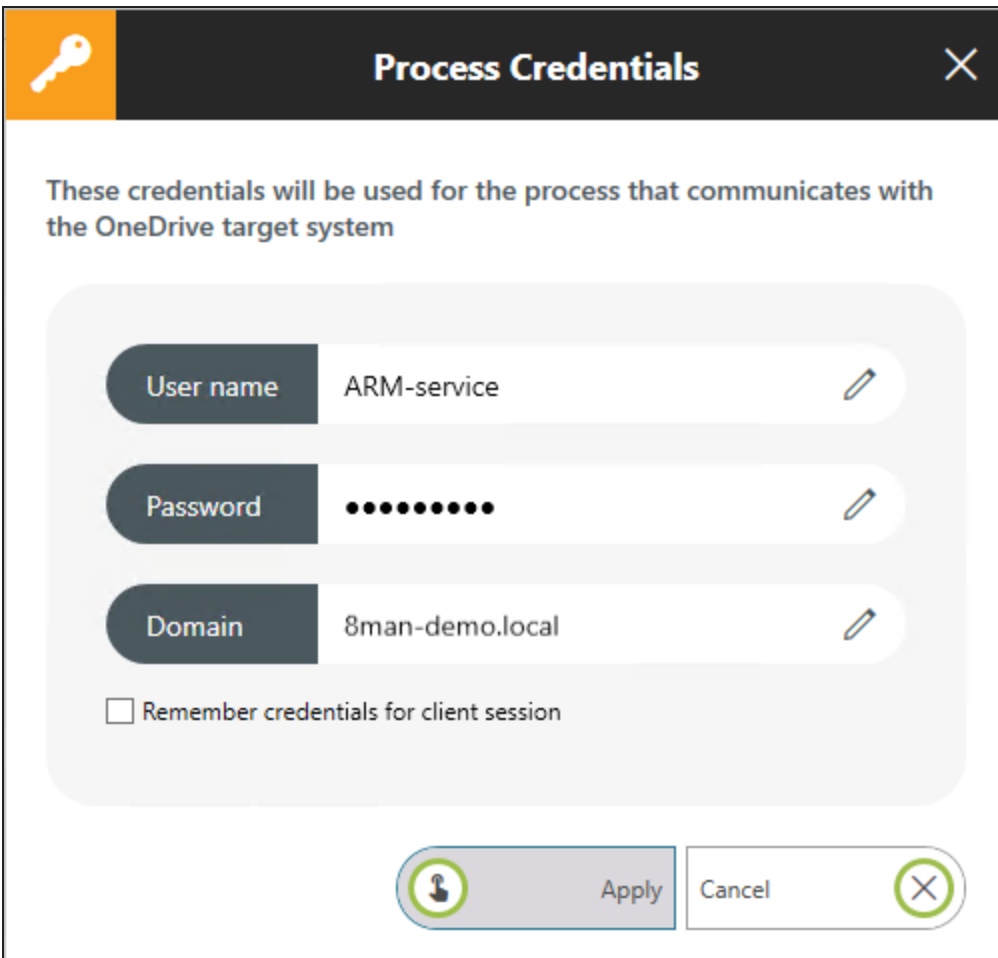
The "scan account" is used for the actual scan. This account must have the permissions described in the section "[Prepare Office 365 integration](#)".

## Add OneDrive scans

**!** You must at first [set up access in the Azure portal](#) to be able to configure a OneDrive scan completely.

The screenshot shows the ARM Configuration application interface. At the top, there's a navigation bar with 'Back' and 'File Server CSV Import'. Below that, a section titled 'Select a technology below to add a new resource configuration' contains several icons for different technologies. The 'OneDrive OneDrive Resources' icon is highlighted with a red box. Below this, a list of resources is displayed, including '8man-demo.local', 'https://8mandemo.sharepoint.com', '8man-demo.com', 'SRV-8MAN', and 'SRVUBUNTU'. Each resource entry includes a play button, a refresh icon, and a 'More >' link. The 'SRV-8MAN' entry has a 'OFF' toggle and detailed configuration information.

In the ARM Configuration Application > Scans, click "OneDrive" to add a OneDrive resource.



**Process Credentials**

These credentials will be used for the process that communicates with the OneDrive target system

User name ARM-service

Password

Domain 8man-demo.local


Remember credentials for client session

Apply Cancel

Specify the credentials for the "[Process Account](#)".


The account will not be used to scan the OneDrive permissions. This account will be set up in a later step.



After successfully verifying the "Process Account", the available resources selection opens.



## OneDrive selection ✕


Please select a resource. You can change the credentials and refresh the list when the given credentials are insufficient to find all resources.


Credential **<not set>** 

  
  Name

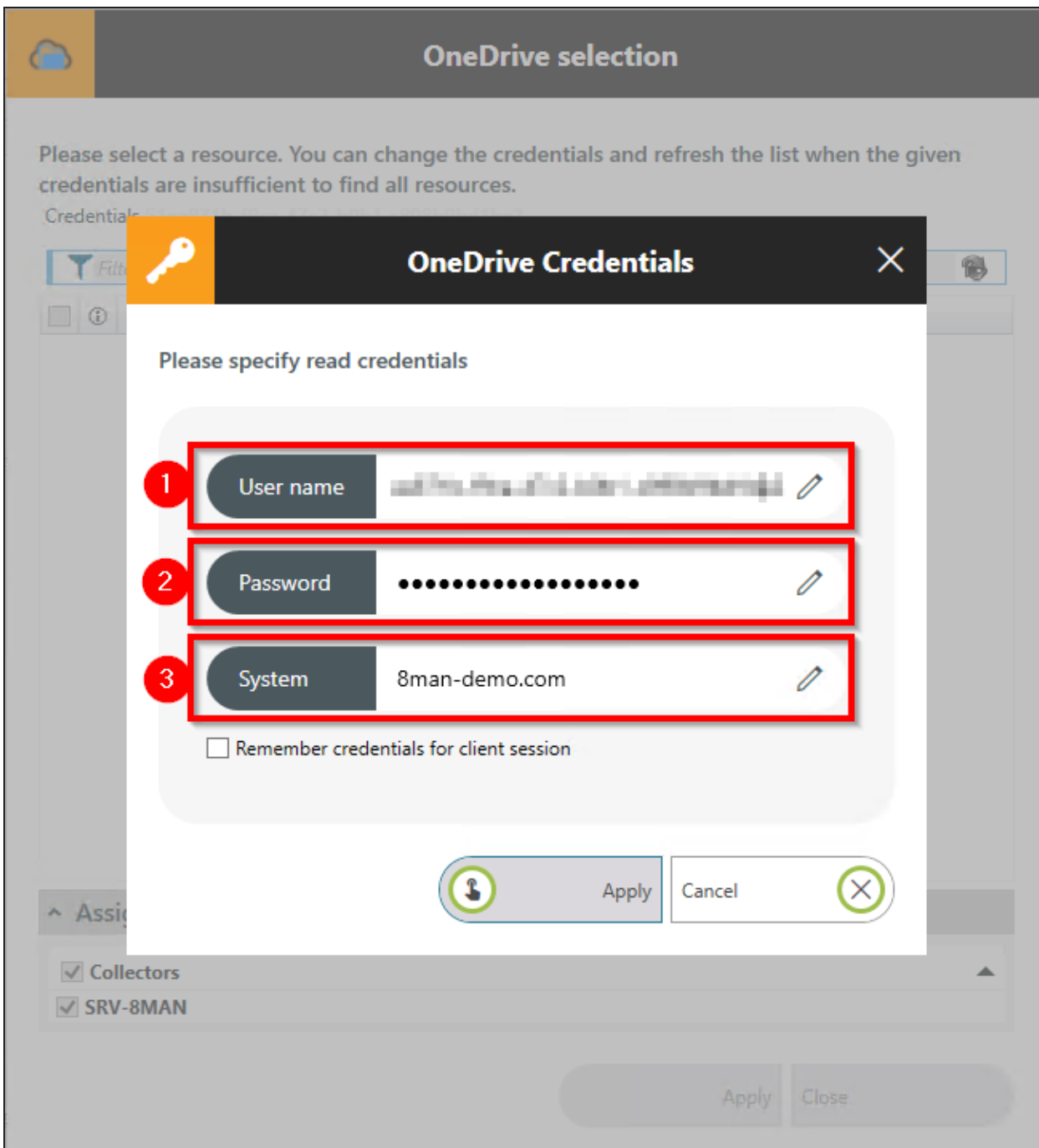
### Unable to find any resource!

^ Assigned collectors

- Collectors 
- SRV-8MAN

Apply Close 

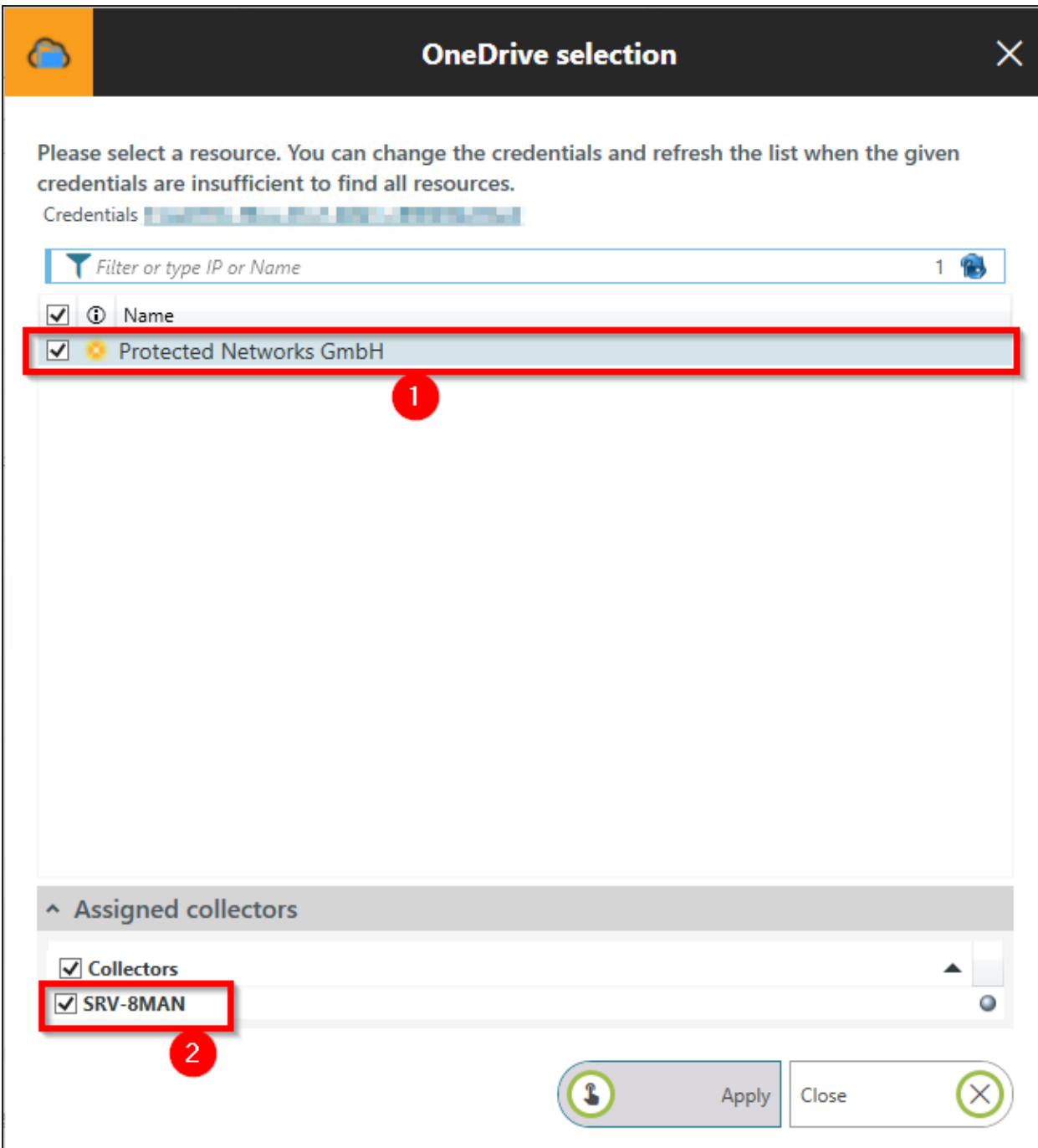
Click the link.



Enter the access data that you created during [preparation](#) on the Azure portal.

1. Enter the [application ID](#) as the user name.
2. Enter the [client secret](#) as the password.
3. Enter the online domain.








**OneDrive selection**

Please select a resource. You can change the credentials and refresh the list when the given credentials are insufficient to find all resources.



Credentials

Filter or type IP or Name 1 

<input checked="" type="checkbox"/>	 Name
<input checked="" type="checkbox"/>	 Protected Networks GmbH

**Assigned collectors**

<input checked="" type="checkbox"/> Collectors
<input checked="" type="checkbox"/> SRV-8MAN

 Apply  

1. Activate the required resource (check the box).
2. Select one or more collectors. Note that the collector servers require an Internet connection.

## Configure additional OneDrive scan properties

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there's a 'Back' button and a 'File Server CSV Import' link. Below that, a section titled 'Select a technology below to add a new resource configuration' displays a grid of options including Azure AD, Domain, Easy Connect - CSV, Easy Connect - SQL, Exchange, File server, Local Accounts, Logga - Active Directory, Logga - Exchange, Logga - File Server, OneDrive, SAP Connector, SharePoint, and SharePoint Online.

Below the grid, a list of resources is shown with a filter bar. The resources listed are 'Q11' and 'Protected Networks GmbH'. The 'Protected Networks GmbH' resource is highlighted, and its scan settings are visible: 'On demand', '10 minutes', and 'additional properties have completely been configured'. A red box highlights the text 'additional properties have completely been configured'.

Click the link.

The screenshot shows the 'Additional properties' dialog box. It has a filter bar at the top with the number '3'. Below the filter, there's a table with two columns: 'Property' and 'Configured value'. The table contains two rows under the 'Scan settings' section:

Property	Configured value
Max. parallel requests	16
Scan files	<input checked="" type="checkbox"/> Activated

Red boxes and numbers highlight the 'Max. parallel requests' field (1) and the 'Scan files' checkbox (2). At the bottom of the dialog, there are 'Reset', 'Apply', and 'Cancel' buttons.

1. Specify the maximum number of parallel requests to be sent to OneDrive.  
Recommended value: 16
2. Recommended: Enable this option to scan folders **and** files.

## Configure AD Logga

### Configure audit policies for the domain controllers (DC)

To access AD Logga functionality you must activate specific audit policies.

If you want to make changes to audit policy you must be a member of the appropriate domain admin or organization admin group.

Configure audit policies for DCs on Server 2008

 Before configuring audit policies you can [verify](#) if all required categories may already be activated.

You can activate the required audit policies by running the following commands on every DC with admin rights:

For "Monitor policy changes":

```
auditpol /set /subcategory:{0CCE922F-69AE-11D9-BED3-505054503030} /success:enable
```

For "Directory service changes":

```
auditpol /set /subcategory:{0CCE923C-69AE-11D9-BED3-505054503030} /success:enable
```

For "Managing User Accounts", "Managing computer accounts", "Managing security groups", "Managing distribution groups", "Managing application groups" and "other account management events":

```
auditpol /set /subcategory:{0CCE9235-69AE-11D9-BED3-505054503030} /success:enable
```


```
auditpol /set /subcategory:{0CCE9236-69AE-11D9-BED3-505054503030} /success:enable
```

```
auditpol /set /subcategory:{0CCE9237-69AE-11D9-BED3-505054503030} /success:enable
```

```
auditpol /set /subcategory:{0CCE9238-69AE-11D9-BED3-505054503030} /success:enable
```

```
auditpol /set /subcategory:{0CCE9239-69AE-11D9-BED3-505054503030} /success:enable
```

```
auditpol /set /subcategory:{0CCE923A-69AE-11D9-BED3-505054503030} /success:enable
```

 Repeat this process for every DC!

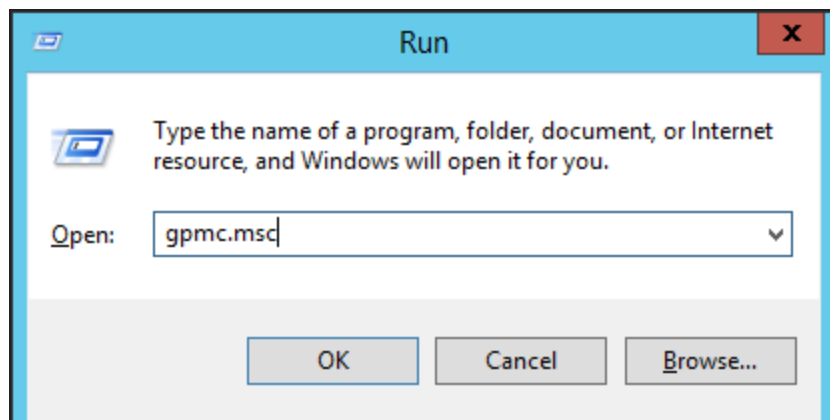
Configure audit policies for DCs on Server 2008 R2 or higher

You can use the group policy editor to manage audit policy on server 2008 R2 or higher. This means you only need to implement the policy once rather than having to repeat it for every DC.

Please note that the activation of audit policy may be delayed on the domain controllers (DCs) depending on your replication interval.

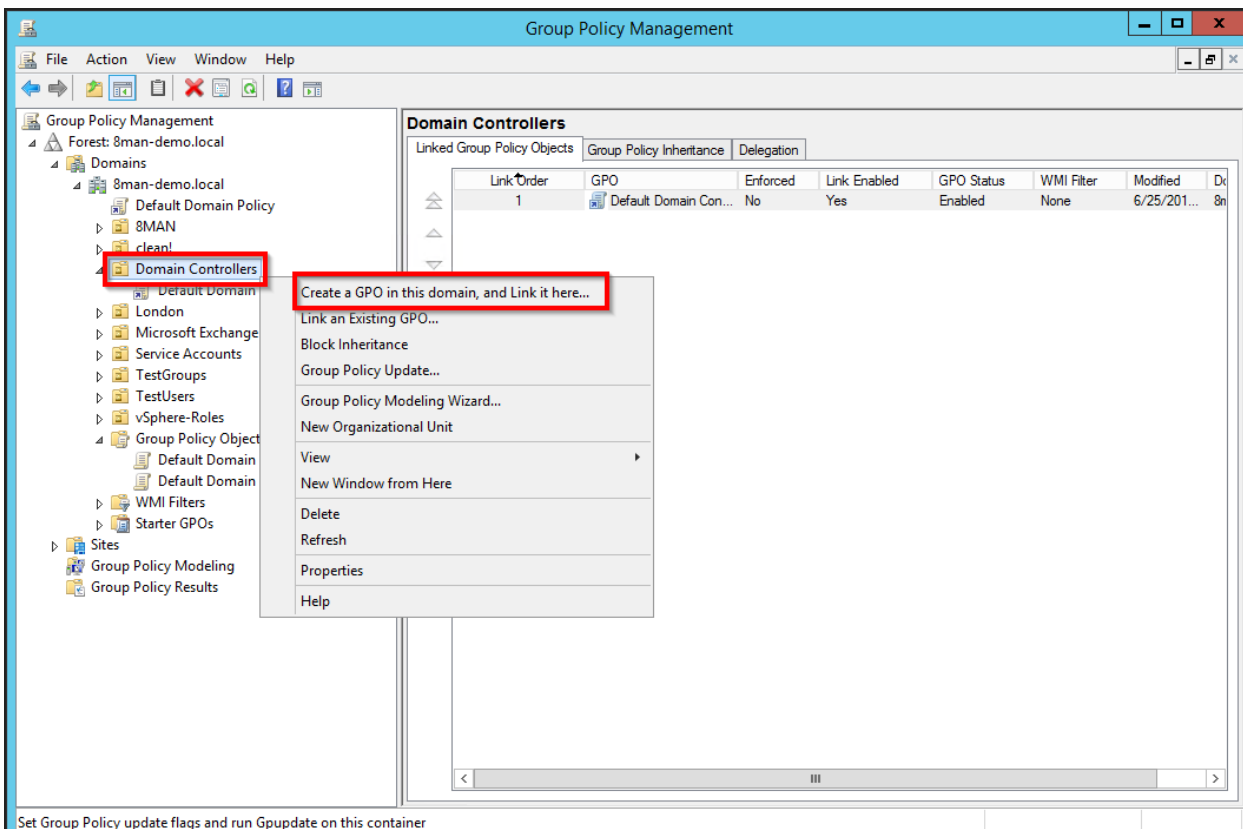
Once you have completed these settings:

- complete a manual policy update with the command "gpupdate /force"
- [Verify the audit policies settings](#)



Start managing group policies, by opening:


```
gpmmc . msc
```

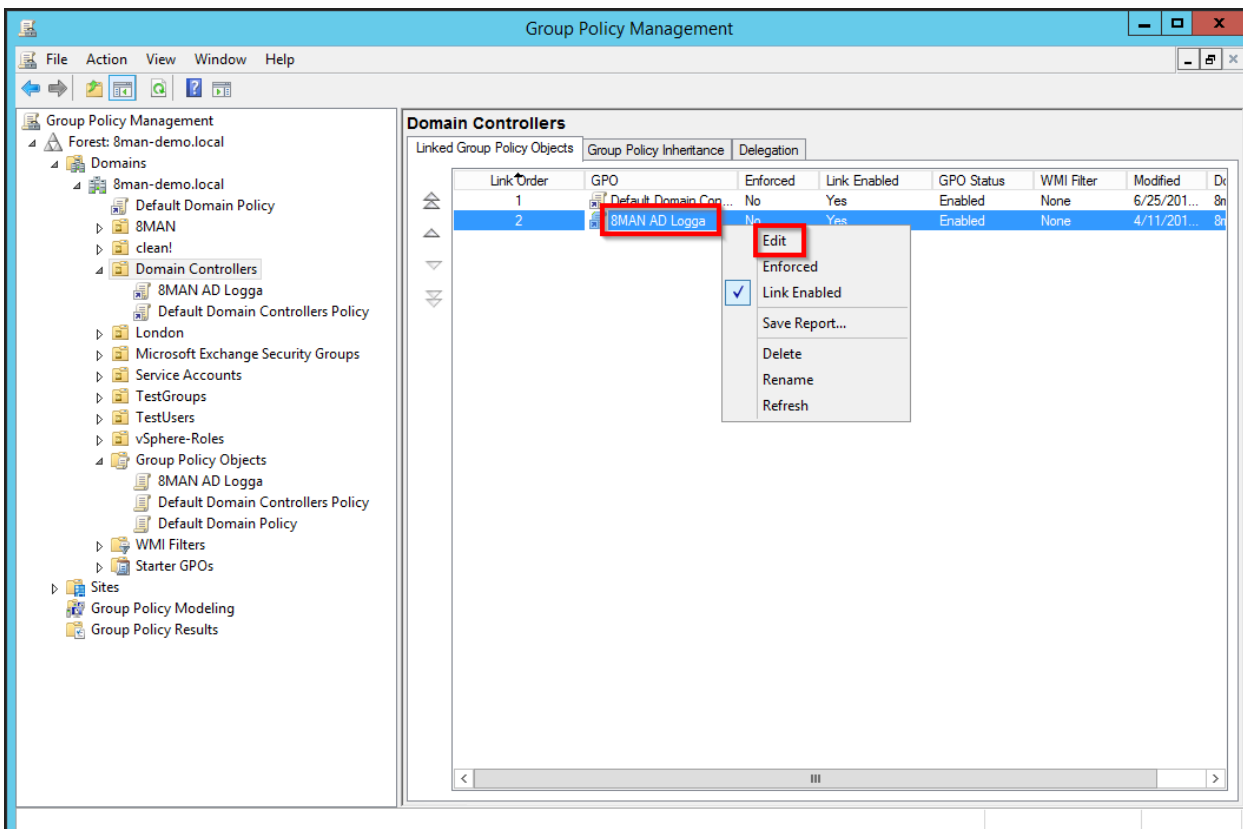


Create a new group policy.

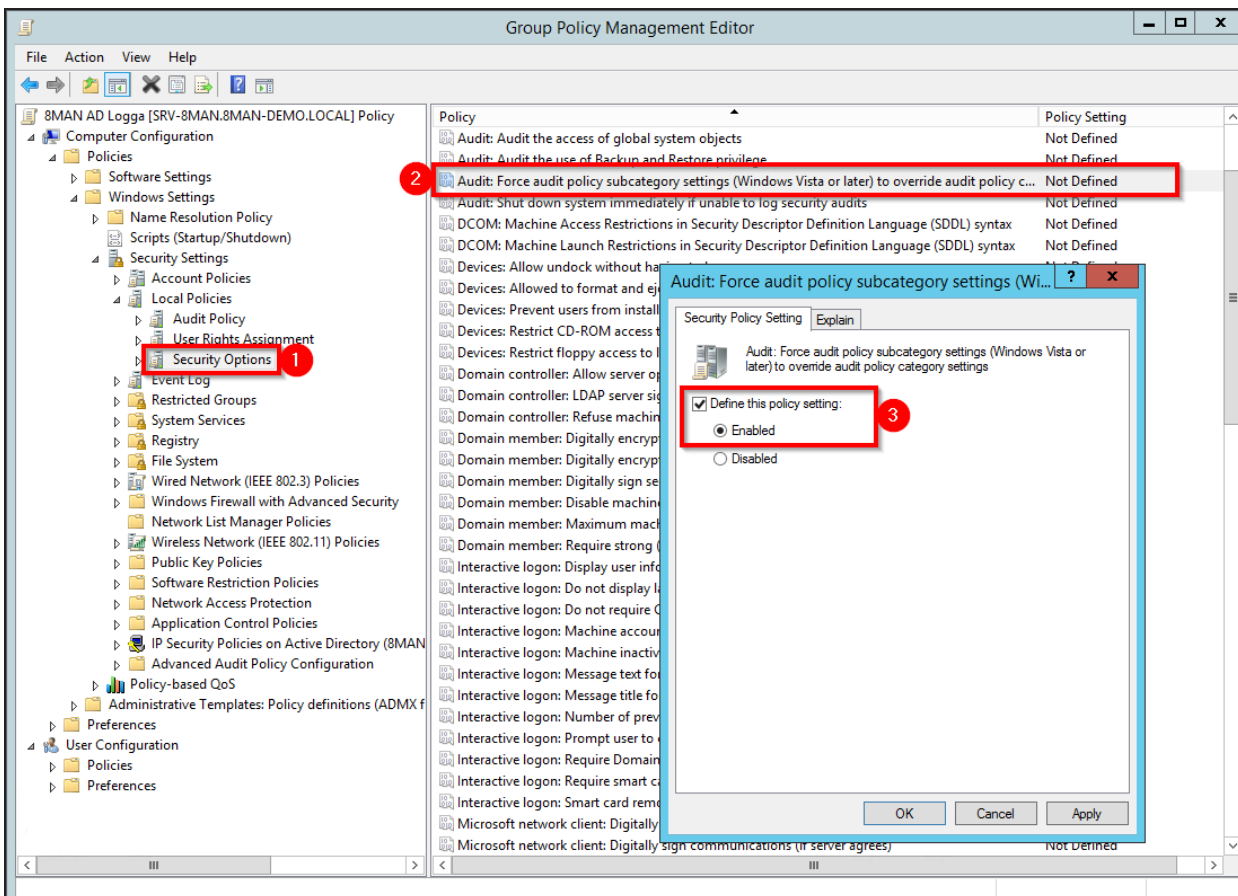
Select the OU in which the DC computer accounts are located. By default they are located in the OU "Domain Controllers".

Ensure that the newly created policy is applied/winning to the appropriate DCs (hierarchy and order).

 The order in which you set the options affects the effectiveness of the policy. Follow the order given here!

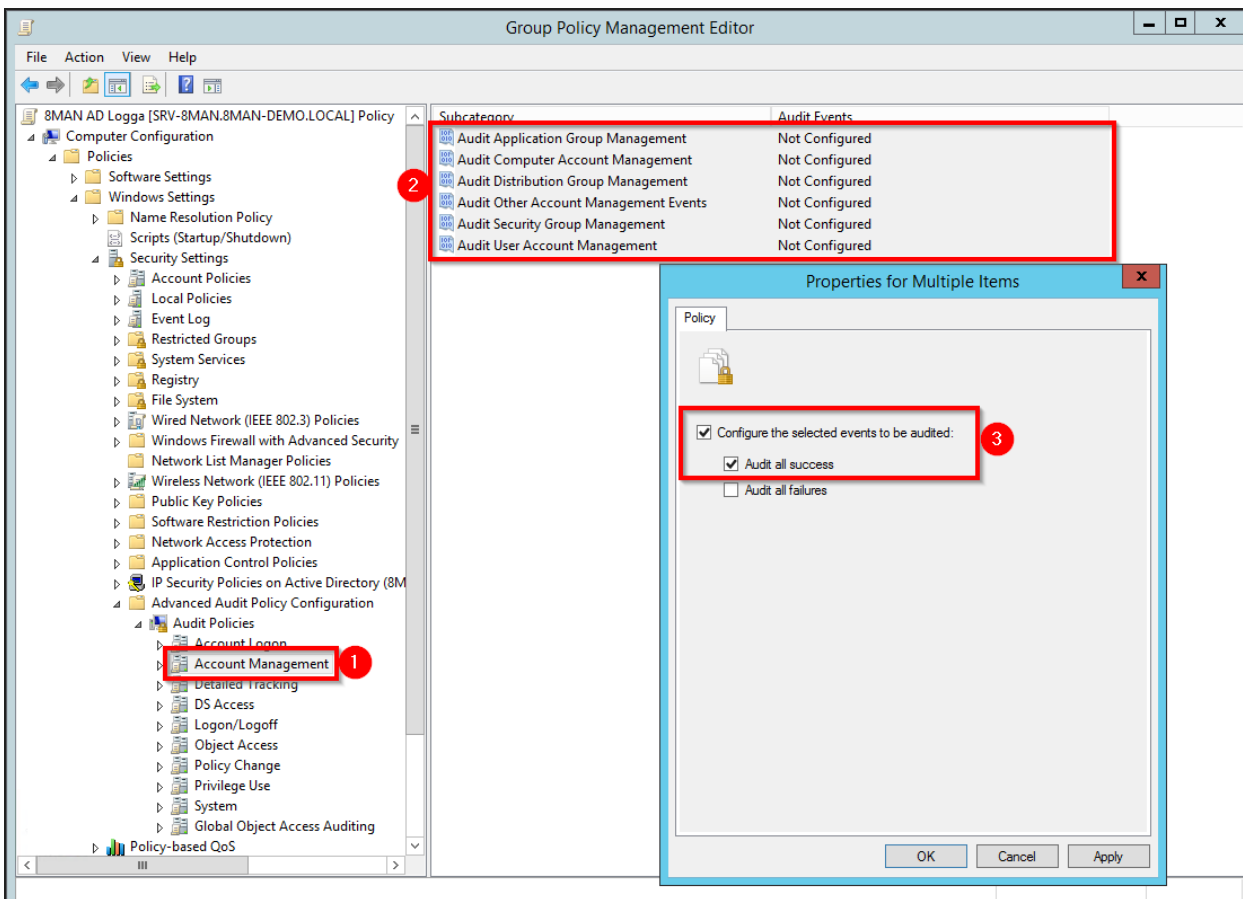


Select the newly created group policy by right clicking and selecting "edit".



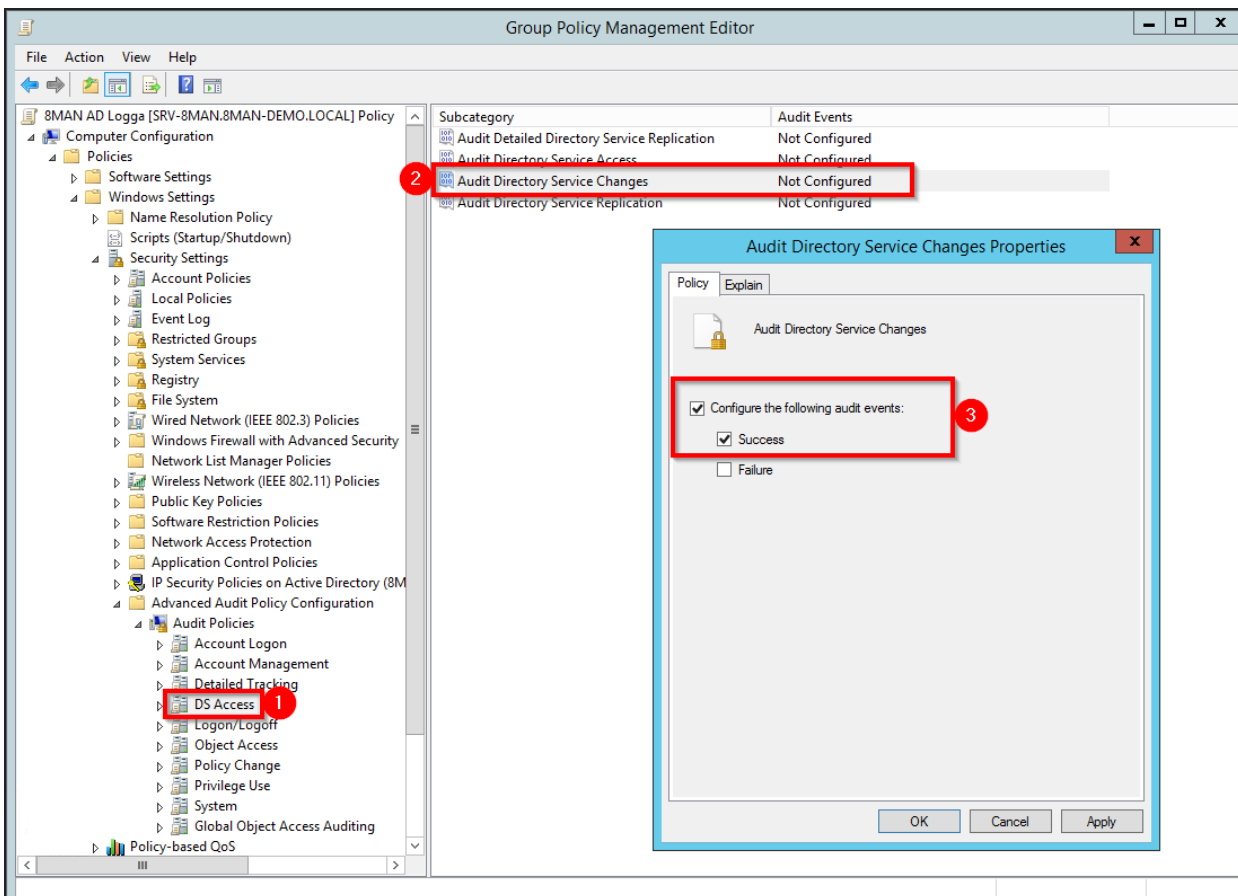
1. Navigate to "security options".
2. Double-click the policy "Audit: Force audit policy...".
3. Activate the security policy as shown in the screenshot.

**!** The order in which you set the options affects the effectiveness of the policy. Follow the order given here!

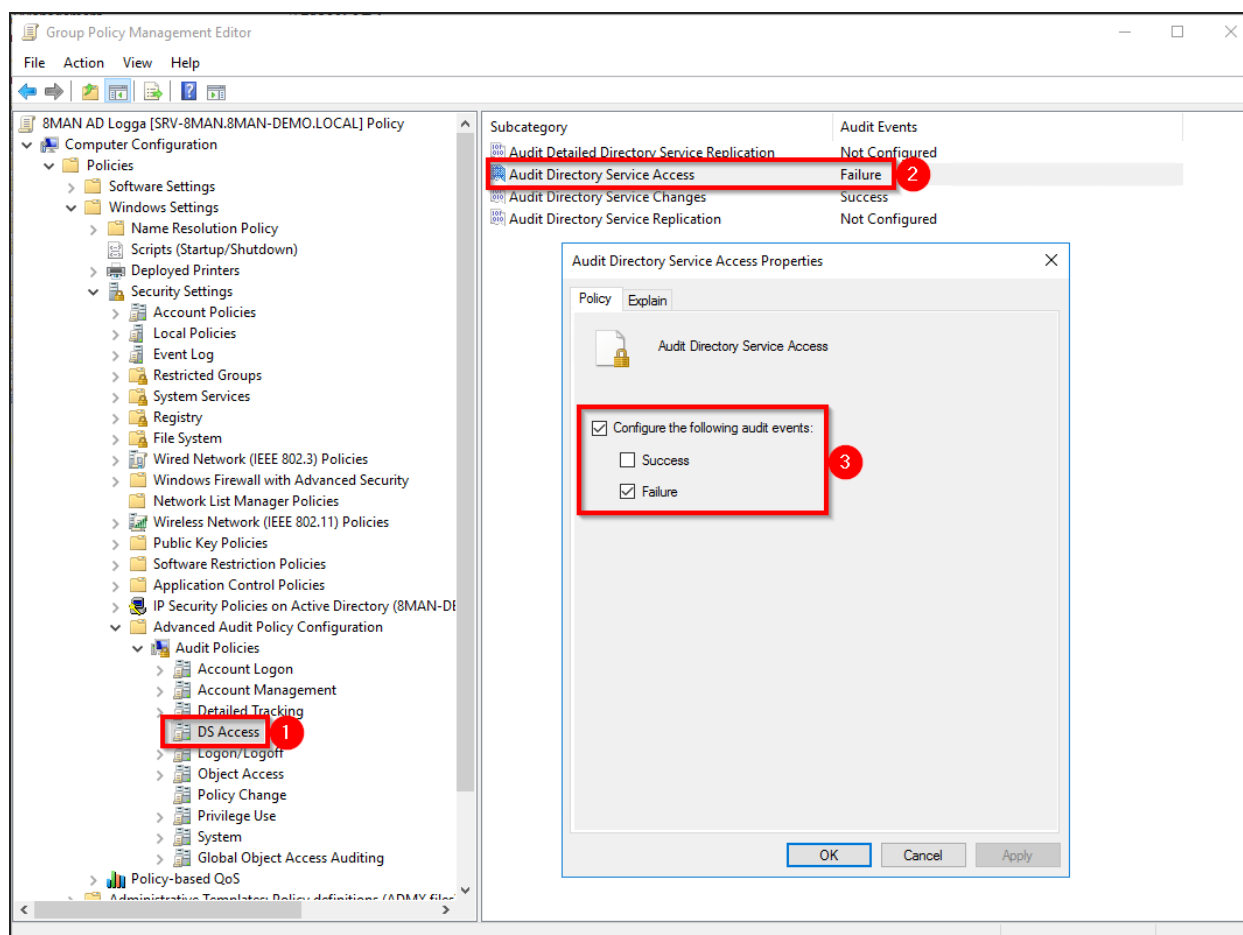


1. Navigate to account management.
2. Use multi-select and select **all** subcategories.
3. Activate the audit by right-clicking and selecting "Properties", as shown in the diagram.

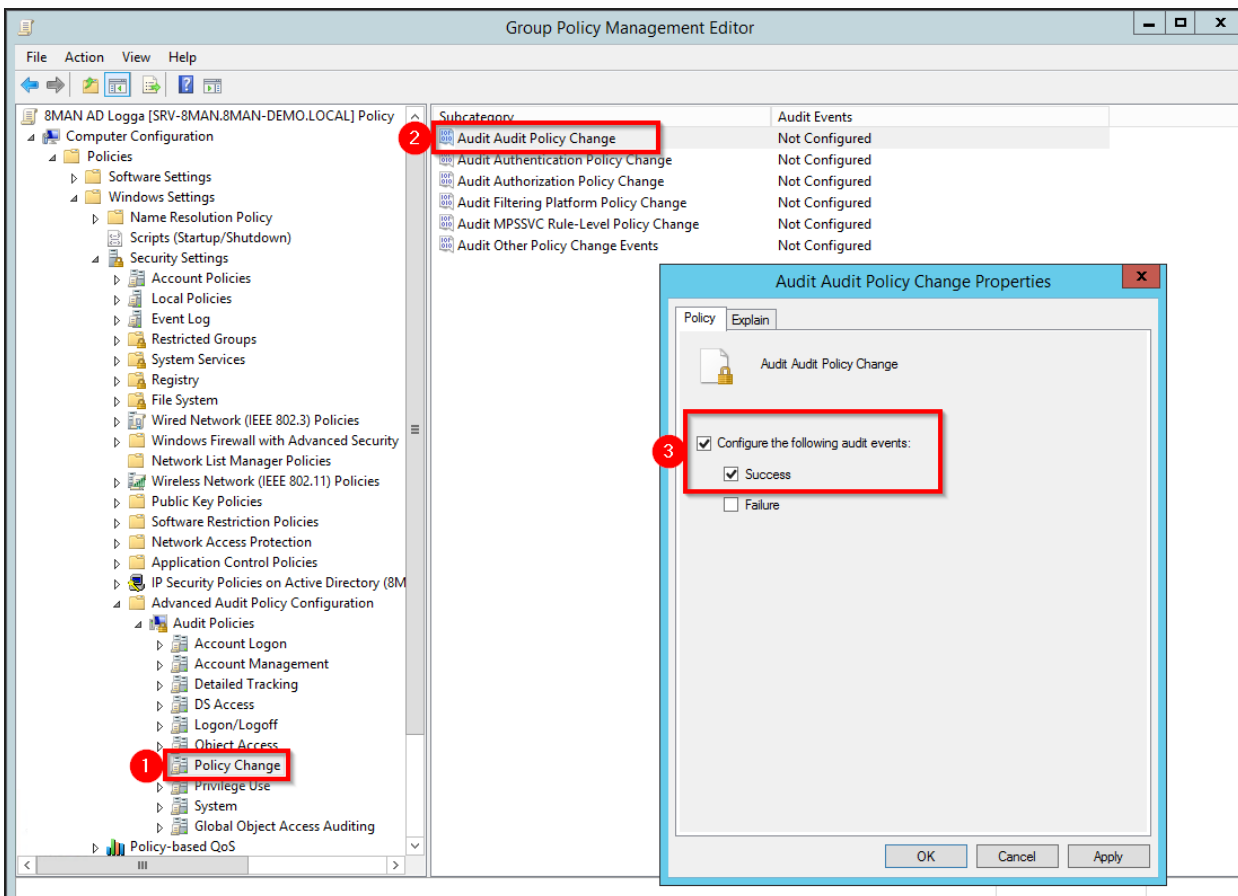




1. Navigate to "DS Access".
2. Double-click the subcategory "Audit Directory Service Changes".
3. Activate the audit as shown in the screenshot.



1. Navigate to "DS Access".
2. Double-click the subcategory "Audit Directory Service Access".
3. Activate the audit in case of failure, as shown in the screenshot.



1. Navigate to "Policy Change".
2. Double-click the subcategory "Audit Audit Policy Change".
3. Activate the audit as shown in the screenshot.

Once you have completed these settings:

- complete a manual policy update with the command `gpupdate /force`
- Verify the audit policies settings

Configure the AD Logga disk space requirement

1000 events require approximately 0.57 MB of storage in the data base.


By default the storage period of AD Logga events is set to 30 days and can be managed under server -> [storage of scans](#).

Set the size of the Windows event log

To ensure that you don't "lose" any events, you must configure the maximum size for security event logs appropriately. For audit policy settings the storage requirements is roughly 1KB per event.

*For example:*

For a server outage or maintenance time (of the collector server selected for the AD Logga) of one hour, with approximately 1000 events per hour, the absolute minimum security event log size would be 1MB. Considering the low storage space requirements for 1000 events, the uncertainty of outage times as well as the potential relevance of individual security events we highly recommend that you ensure that enough storage space is available.

 For more information about recovery mode, see the article [Set Maximum Log Size](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc748849(v=ws.11)). (© 2020 Microsoft, [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc748849\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc748849(v=ws.11)), obtained on January 29, 2020)

Verify the audit policy settings

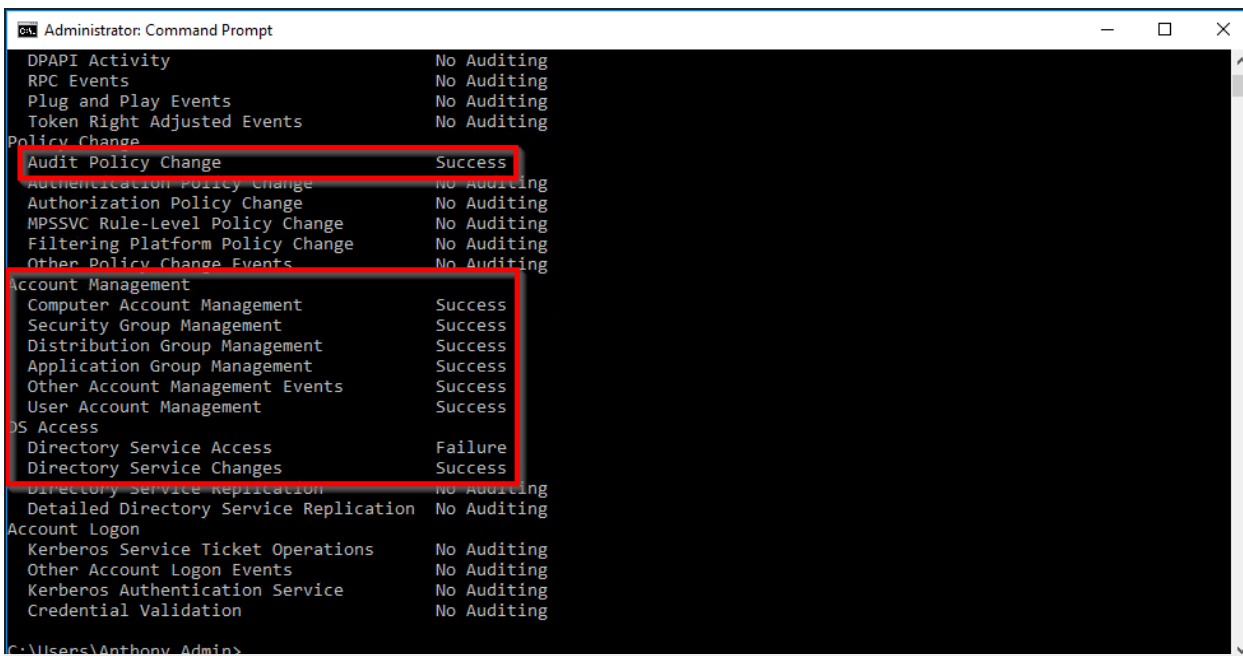
You can verify the effectiveness of audit policies by starting the command prompt with admin rights and entering the following command:

**For english servers**

```
auditpol /get /category:"policy change,account management,ds access"
```

**For all languages**

```
auditpol /get /category:*
```




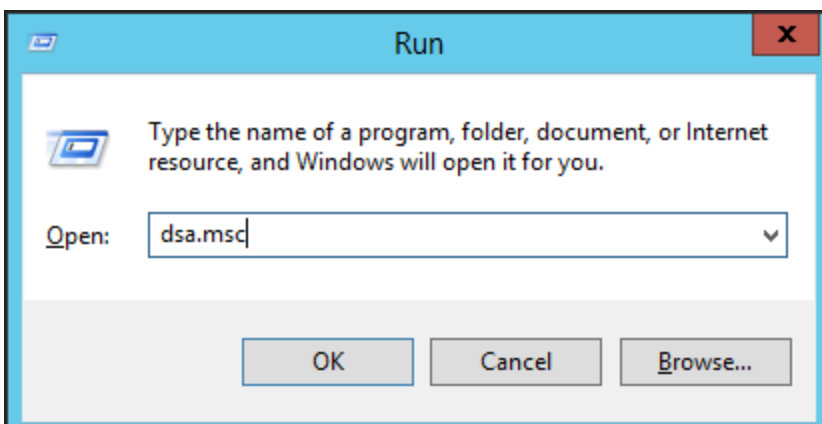
The marked subcategories must be set to "Success" or "Failure" as shown.

## Set audit permissions in the AD object SACLs

After activating the audit policies you must set the audit permissions for AD objects (SACL) accordingly.

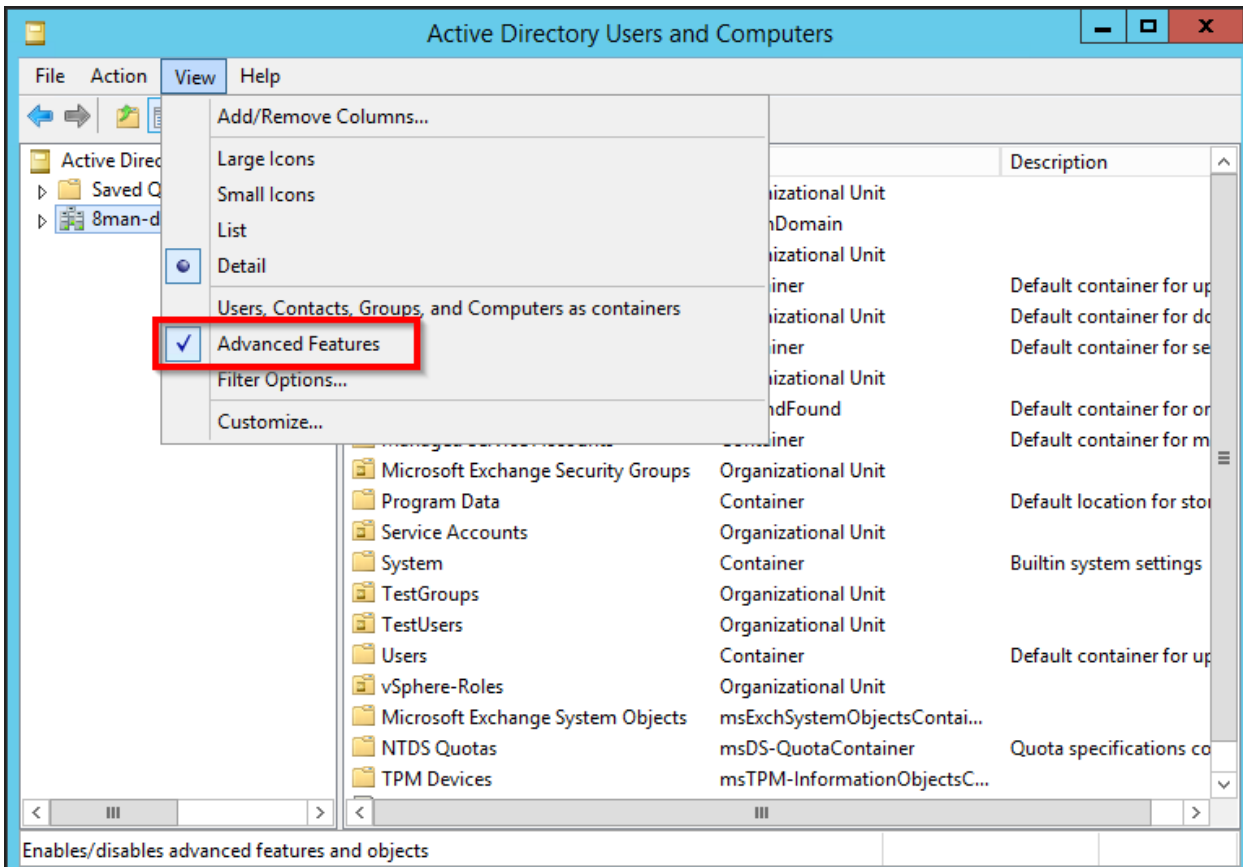
The user right "Manage auditing and security log" is required for the configuration of the SACL (this corresponds to the privilege "SeSecurityPrivilege"). You must be a member of the "event log reader" or domain admin group.

 The configuration of the SACL is only required for one of the domain controllers. All other DCs receive the configuration via replication.

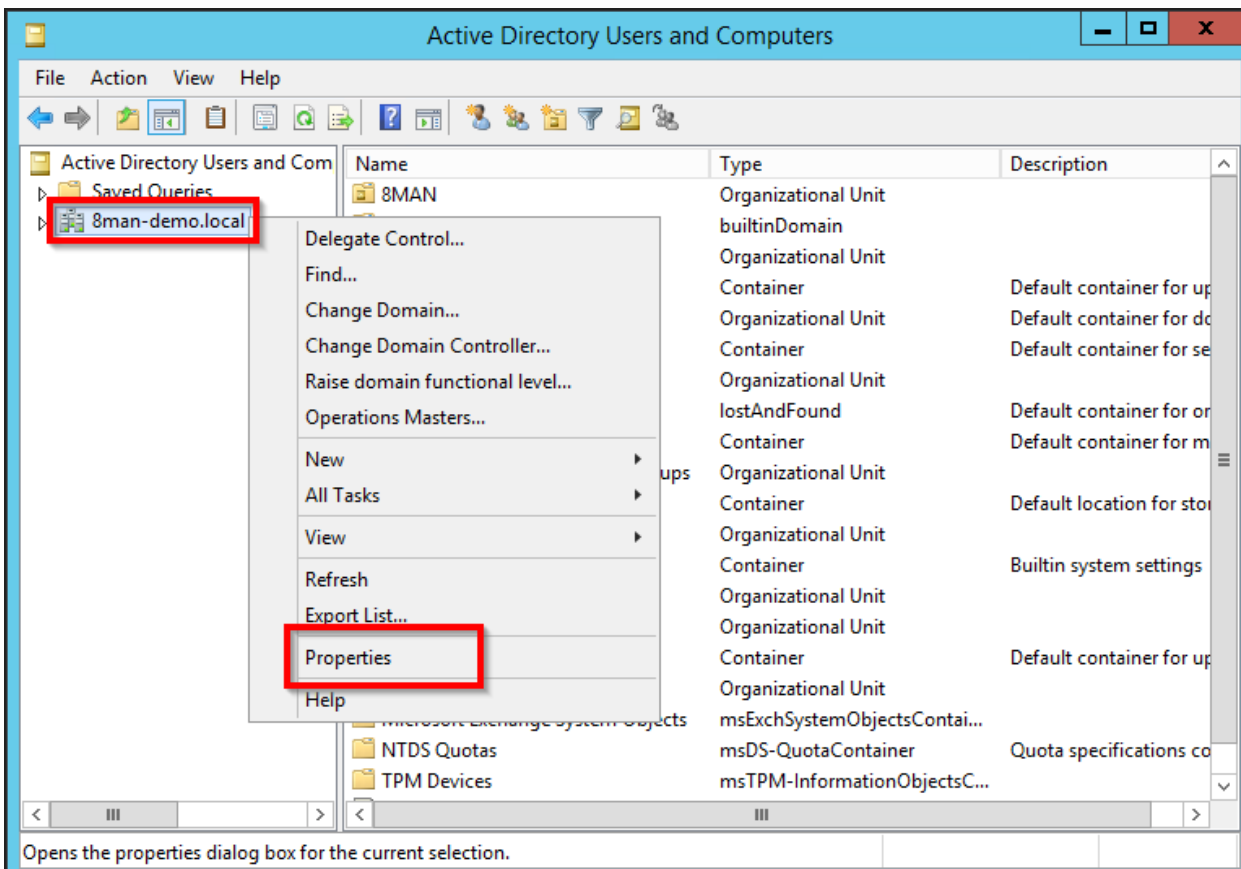


Start the management of Active Directory users and computers on a DC by opening

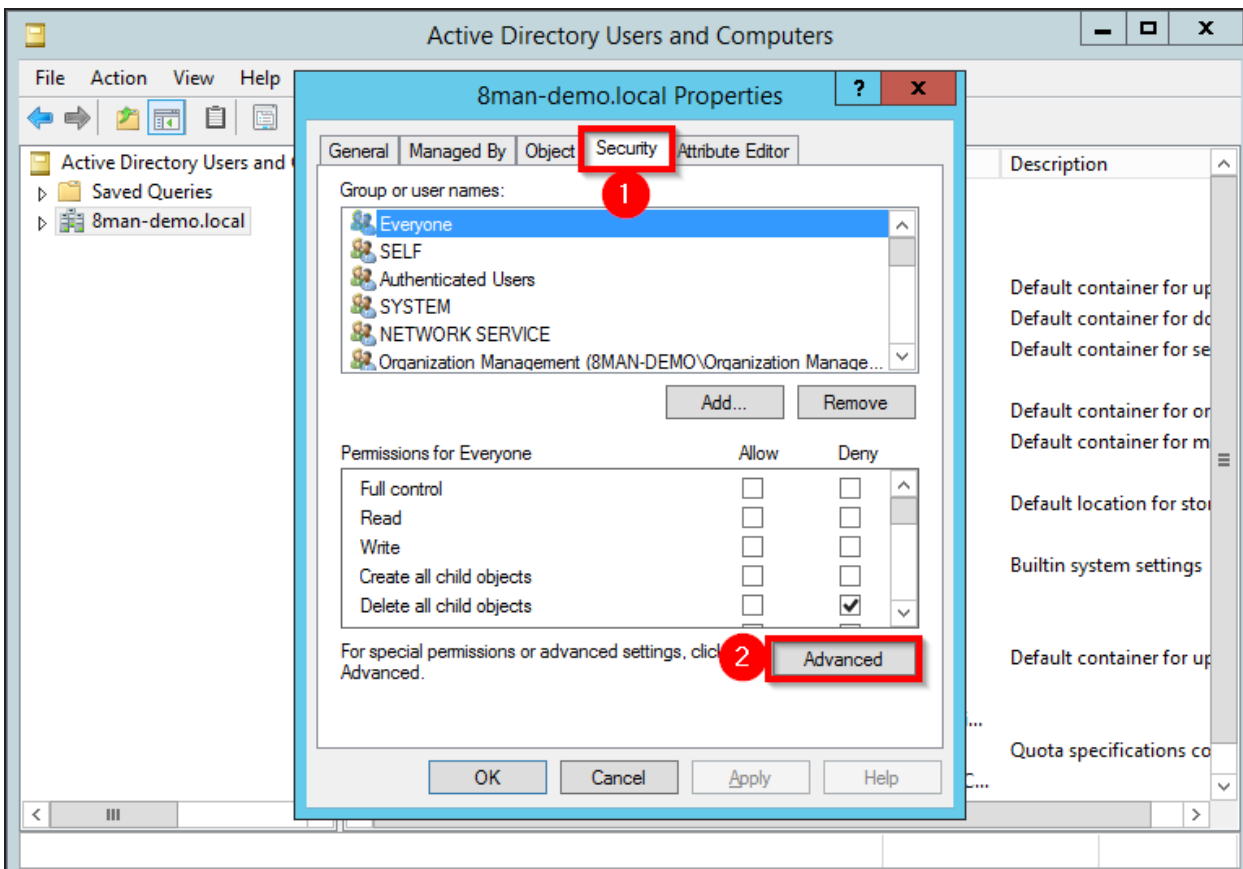
dsa.msc



Activate the option "Advanced Features".

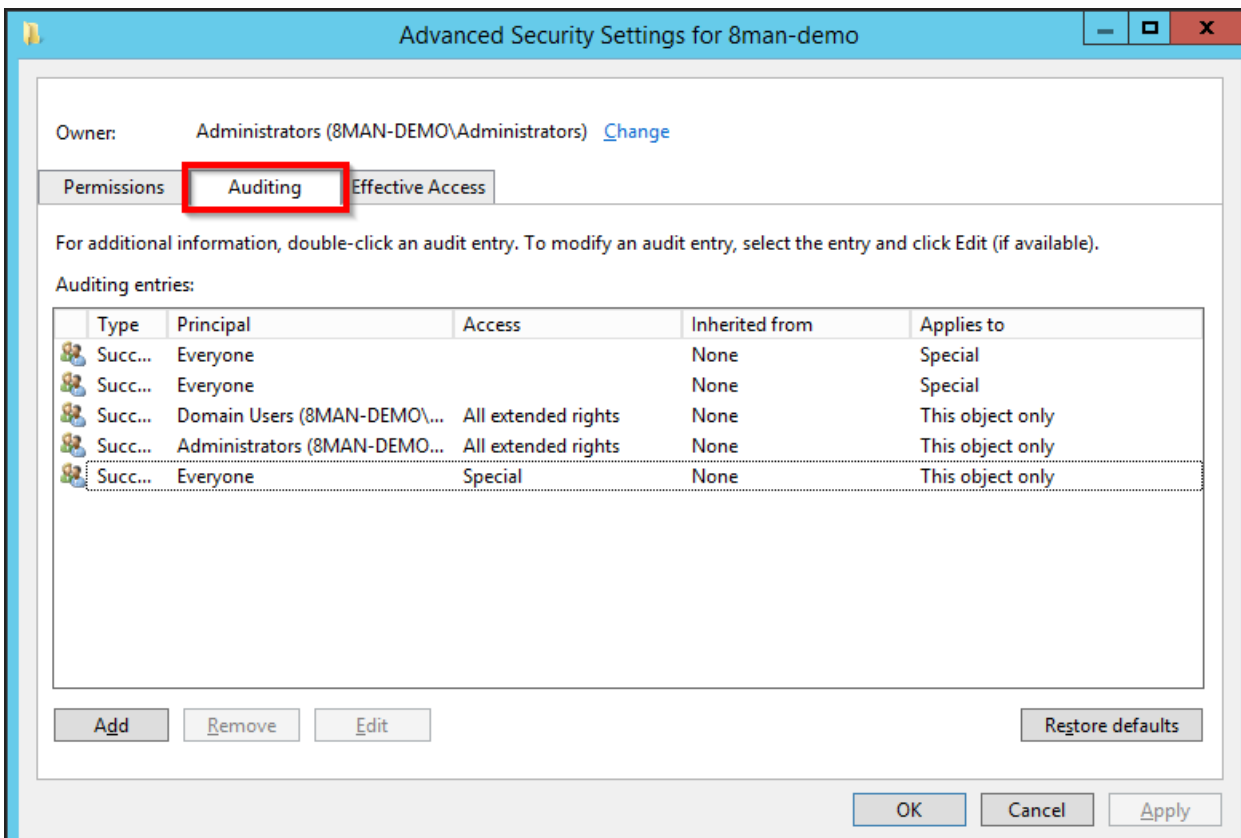


Select the domain that you want to monitor by right-clicking on it and selecting "Properties".



In the properties window, select the tab "Security" and then click on "Advanced".

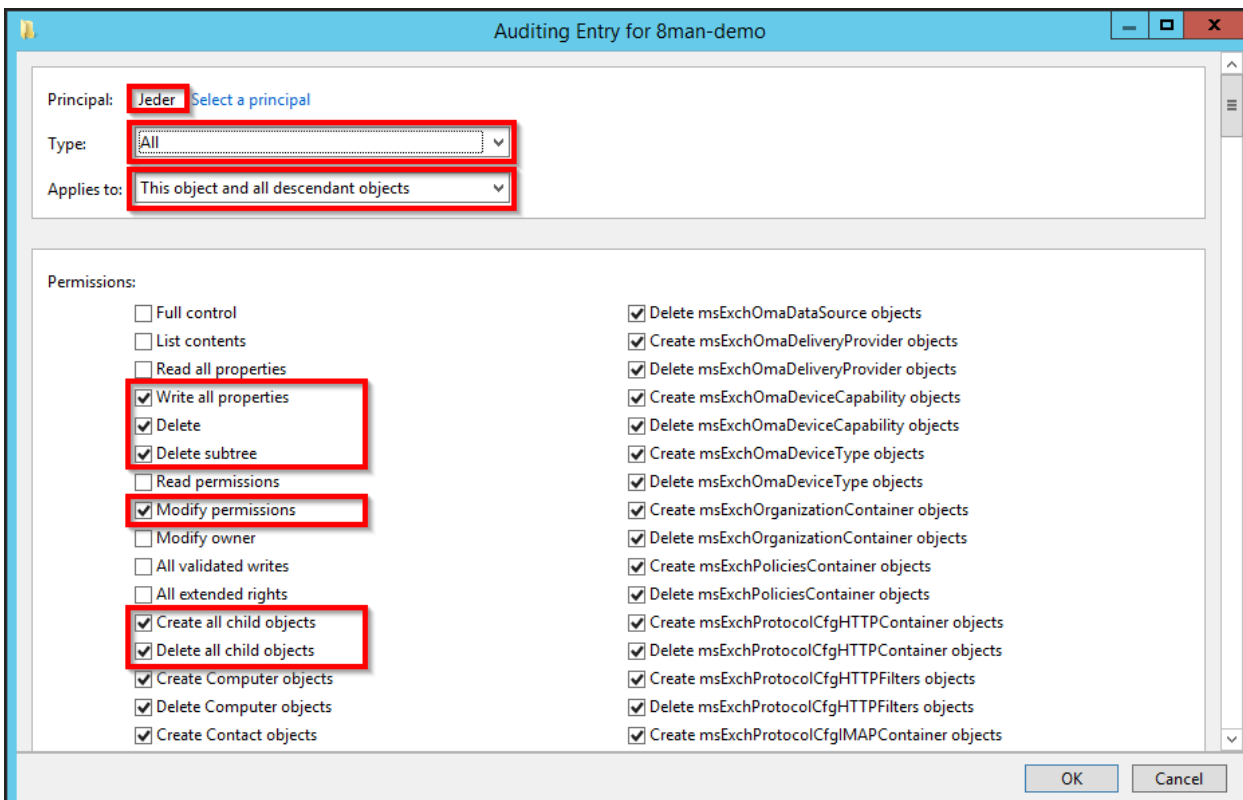




Select the tab "Auditing".

Analyze the existing access rights. Perhaps the required permissions already exist.

If required, expand the access rights of an existing "Everyone" principal or add the desired entry.



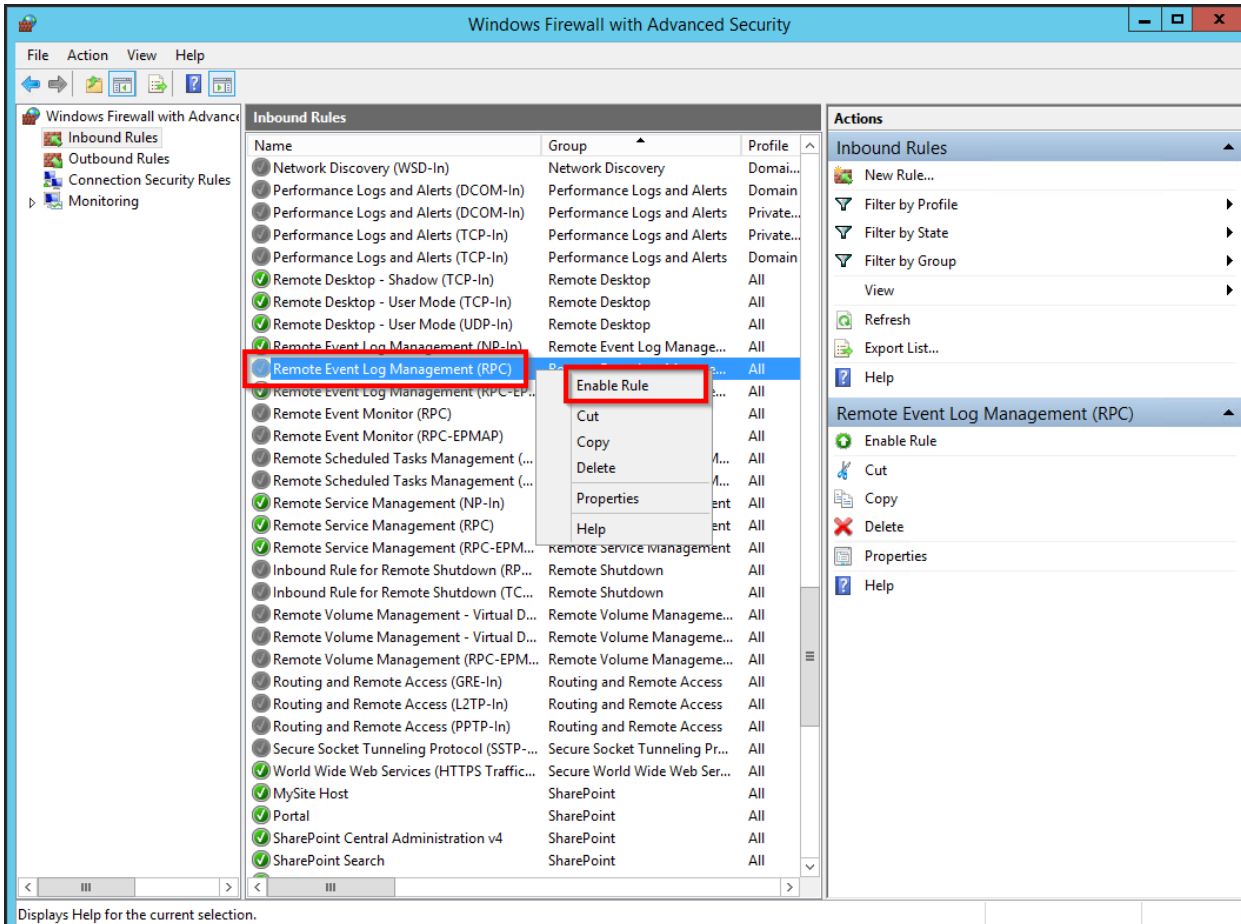
At minimum, the following is required:

- Principal: "Everyone"
- Type: "All"
- Apply to: "This object and all descendant objects"

Permissions:

- Write all properties
- Delete
- Delete subtree
- Modify permissions
- Create all child objects
- Delete all child objects

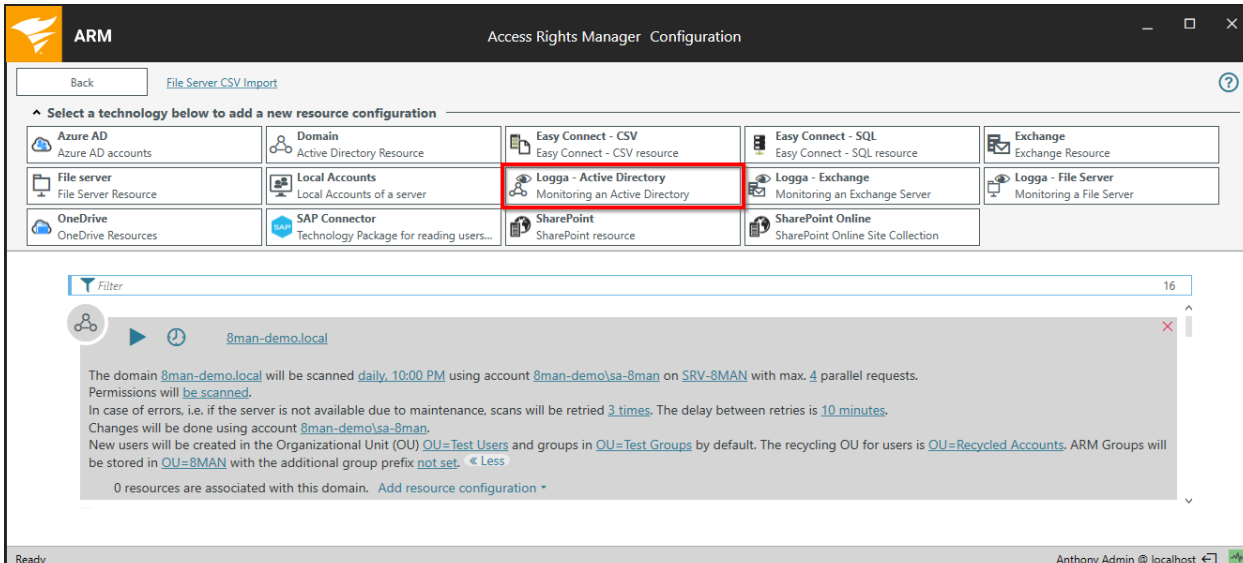
## Configure the Windows firewall for AD Logga



If the Windows firewall is activated on the DC that you would like to monitor, then a pre-defined Microsoft rule "Remote Event Log Management (RPC)" must be enabled.

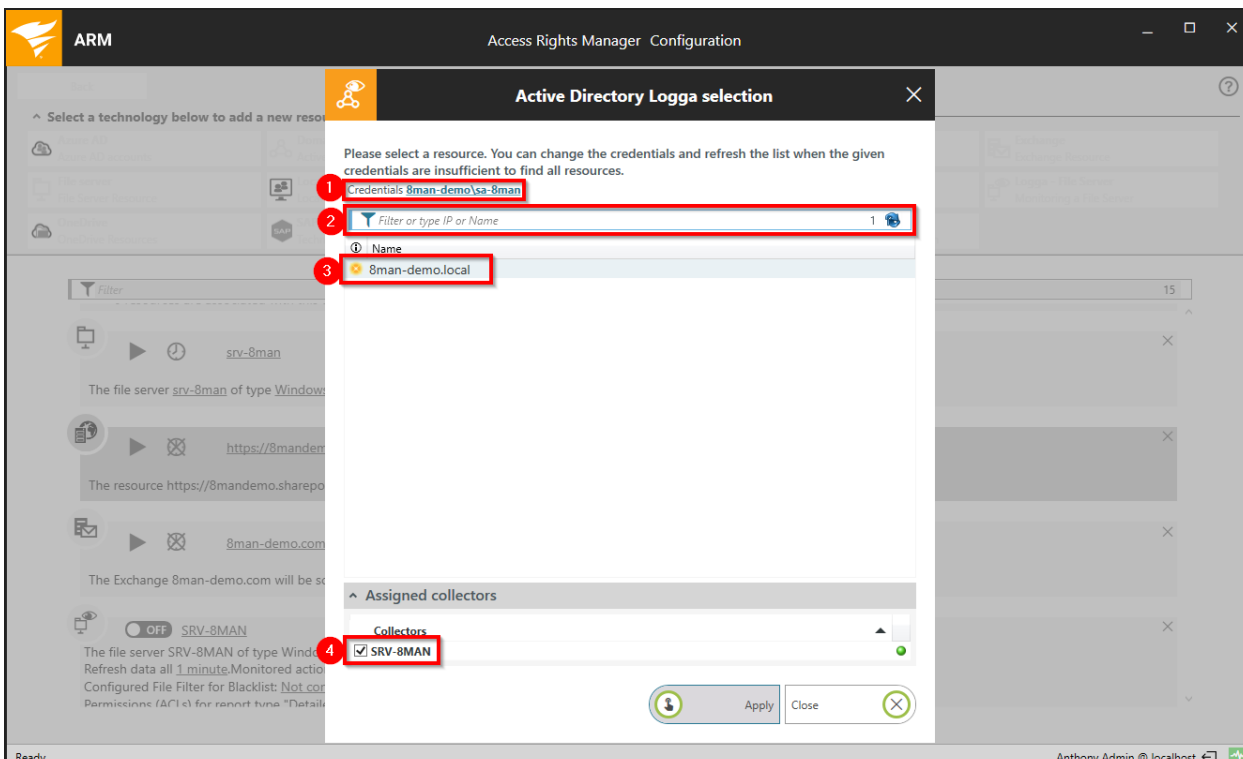
⚠ Repeat the procedure for each DC to be monitored.

## Add an AD Logga configuration



On the configuration home page select "Scans".

Select "Logga - Active Directory".



1. Enter valid credentials for the domain that you want to monitor.

2. Use the filters to find the desired domains.

3. Select a domain. Child domains are not monitored. Every domain must be configured separately
4. Select a collector server. You can only select one collector per domain.

**i** After adding an AD Logga configuration, it initially remains deactivated. You must [activate the AD Logga](#) to record events.

## Activate or deactivate AD Logga

The screenshot shows the 'Access Rights Manager Configuration' window. Under the 'Scans' section, there is a list of domains. The domain '8man-demo.local' is shown with a switch icon that is currently turned off (OFF). A red box highlights this switch icon. Below the domain name, there is a note: 'The domain 8man-demo.local is monitored on SRV-8MAN using account 8man-demo\sa-8man. Following filters have been set. Refresh data all 10 minutes.'

On the configuration home page select "Scans".

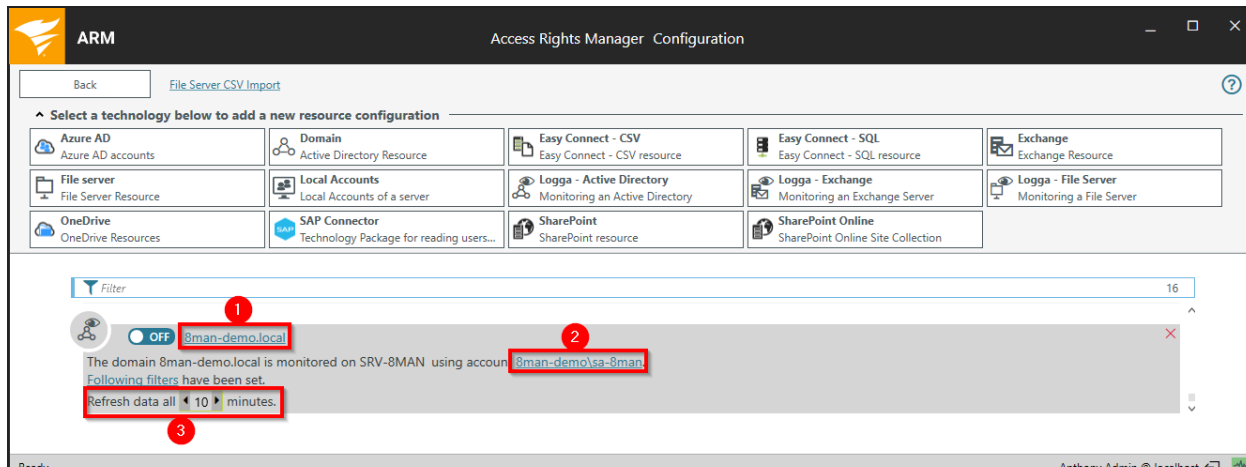
Click on the switch icon to activate or deactivate AD Logga.

**i** AD Logga events are stored by default for 30 days. See [Configure storage of scans settings](#).

The screenshot shows the 'Start logging' dialog box overlaid on the configuration page. The dialog box contains the following text: 'Please confirm the Start of the Active Directory Logga with a comment. The start event will be logged in the ARM logbook.' Below this text is a text input field with a placeholder 'Please add a comment' and a yellow warning icon. To the right of the input field is a profile picture of a man. At the bottom of the dialog box are two buttons: 'Apply' and 'Close'. The 'Apply' button is highlighted with a red box.

You must enter a comment.

## Customize an AD Logga configuration



1. Rename the configuration.
2. Set the account used by AD Logga to read events from the domain controller.  
The account must be a member of the group "event log readers" or "domain admins". You can only change this setting when the Logga is turned off.
3. Determine how frequently Logga data is updated. Events are cached by the collector and transferred to the data base via the ARM server in configured intervals.  
Default setting: 10 minutes  
Possible values: 1 to 60 minutes

### Filter AD Logga events

You can filter out desired events in order to focus on specific and relevant entries. Filtering means that filtered events will not be recorded.

This allows you to significantly improve your overview and reduce data volume. A typical example are frequent attribute changes of the Exchange server.

**i** You are only able to configure filters if at least one AD scan is stored in the database.

## Understand the filter principles for AD Logga

The AD Logga filter is considered a blacklist filter. In this case, blacklist means: The AD Logga records all possible events. You can determine which results are excluded.


By default the filter is set to the object classes "Service-Connection-Point" and "Print-Queue".

The filter criteria work cumulatively. An event is excluded if criteria 1, or criteria 2, or criteria 3 is fulfilled, or multiple criteria simultaneously.

The filter criteria do not correlate to each other. The events are evaluated by the AD Logga consecutively based upon the entered criteria. If one of the criteria is fulfilled, the AD Logga immediately excludes the result independent of whether any other criteria have been evaluated.

For example:

- If User A is configured as a filter, then all changes made by him will be excluded, even if the object classes or attributes that he made changes to are not configured as a filter. Changes that affect User A are still included.
- If object class X is configured as a filter, then all events, that include this object class explicitly will be excluded, even if the event author or changed attribute is not configured as a filter. This also applies to attribute filters.

 Not all security log entries include affected object classes or attributes. For example changes to group memberships will not be excluded, even if the object classes "User" and "Group" and the attribute "Member" are configured as filters.

## Configure the event filters

ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

Azure AD Azure AD accounts	Domain Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource
File server File Server Resource	Local Accounts Local Accounts of a server	Logga - Active Directory Monitoring an Active Directory	Logga - Exchange Monitoring an Exchange Server	Logga - File Server Monitoring a File Server
OneDrive OneDrive Resources	SAP Connector Technology Package for reading users...	SharePoint SharePoint resource	SharePoint Online SharePoint Online Site Collection	

Filter 16

8man-demo.local OFF

The domain 8man-demo.local is monitored on SRV-8MAN using account 8man-demo\sa-8man. Following filters have been set. Refresh data all 10 minutes.

Ready Anthony Admin @ localhost

Click the link.

ARM Access Rights Manager Configuration

Active Directory Logga Filter Configuration

SET FILTER CRITERIAS TO LIMIT THE AMOUNT OF DATA COLLECTED BY THE ACTIVE DIRECTORY LOGGA

Available event authors 1178

Filtered out Event authors 1

Abdul-Hadi Deeb (8man-demo\Abdul-Hadi Deeb)

Active Directory Events

Event authors 1

Computer event authors

Object classes 2

Attributes

Logga monitoring

Use groups as event authors

ARM allows to configure groups as event authors. All direct and indirect members of the configured groups will be selected as event authors to be filtered out. Using groups needs additional configuration for group membership changes.

Please add a comment

Apply Close

Ready Anthony Admin @ localhost

1. Filter events related to specific users.
2. Use the filter to find the desired user. You can search for either display name or CommonName.
3. Select the desired user and add him with drag&drop or double-click.



ARM

Access Rights Manager Configuration

Active Directory Logga Filter Configuration

SET FILTER CRITERIAS TO LIMIT THE AMOUNT OF DATA COLLECTED BY THE ACTIVE DIRECTORY LOGGA

Active Directory Events

Event authors

Group event authors

Computer event authors

Object classes

Attributes

Logga monitoring

Available event authors

Filter 1672

Groups

Name

8man-demo complete (8man-demo\8man-demo complete)

Access Control Assistance Operators (Access Control Assis...)

Account Operators (Account Operators)

Administrators (Administrators)

Admins (8man-demo\Admins)

All employees (8man-demo\All employees)

Allowed RODC Password Replication Group (8man-demo\...

Backup Operators (Backup Operators)

BigGlobalGroup\_0 (8man-demo\BigGlobalGroup\_0)

BigLocalDomainGroup\_0 (8man-demo\BigLocalDomainGr...

BigUniversalGroup\_0 (8man-demo\BigUniversalGroup\_0)

BUILTIN\Power Users

C-Level (8man-demo\C-Level)

Cafeteria (8man-demo\Cafeteria)

Filtered out Group event authors

Filter

Use groups as event authors

ARM allows to configure groups as event authors. All direct and indirect members of the configured groups will be selected as event authors to be filtered out. Using groups need additional configuration or group membership changes.

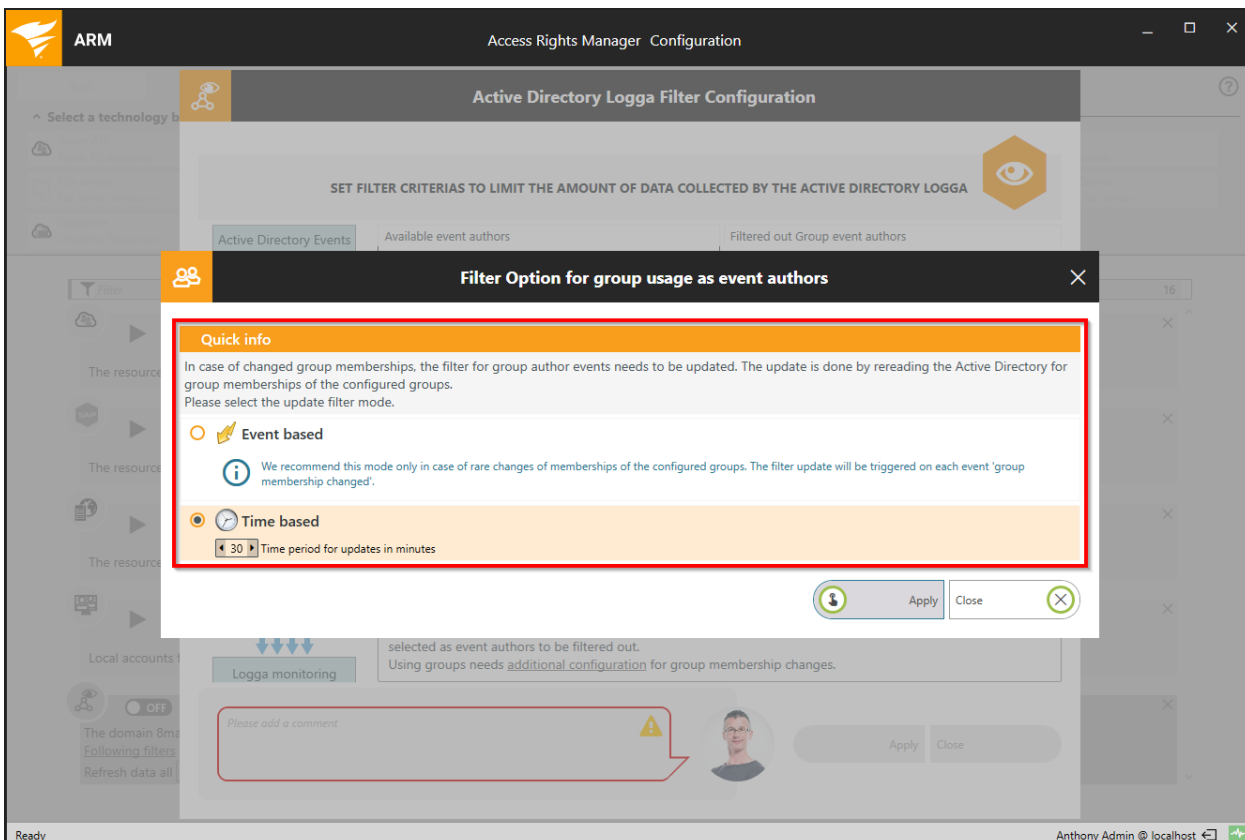
Please add a comment

Apply Close

Ready

Anthony Admin @ localhost

1. You can filter groups as event authors. Activate the option.
2. The filter level is shown. By moving groups into the right hand column with drag & drop, all events of users who are direct or indirect members of that group are filtered and excluded.
3. Click on "additional configuration".



Determine which mode is used by the filter to update group memberships.

Please note the information in the displayed dialog.

Only use "event-based" if memberships in the filtered groups change rarely.

The update interval for the "time-based" option can be set between 10 and 1440 min (24h). The shorter the interval, the higher the load on your AD.

The screenshot shows the 'Active Directory Logga Filter Configuration' window in SolarWinds ARM. The window title is 'Active Directory Logga Filter Configuration'. The main heading is 'SET FILTER CRITERIAS TO LIMIT THE AMOUNT OF DATA COLLECTED BY THE ACTIVE DIRECTORY LOGGA'. The interface is divided into several sections:

- Active Directory Events:** A vertical flow of blue arrows pointing down, representing the filter criteria.
- Event authors:** A dropdown menu with a filter icon and the number '1'.
- Group event authors:** A vertical flow of blue arrows pointing down.
- Computer event authors:** A dropdown menu with a filter icon and the number '2'. This section is highlighted with a red box.
- Object classes:** A dropdown menu with a filter icon and the number '2'.
- Attributes:** A vertical flow of blue arrows pointing down.
- Logga monitoring:** A vertical flow of blue arrows pointing down.

On the right side, there are two panels:

- Available event authors:** A list of event authors with a filter icon and the number '4'. The 'Computers' category is selected. Below the list is a table with the following data:

Name
b-srvexch (8man-demo\B-SRVEXCH\$)
b-srvsql (8man-demo\B-SRVSQL\$)
b-wsmeyer (8man-demo\B-WSMEYERS)
b-wswillson (8man-demo\B-WSWILLSON\$)
- Filtered out Computer event authors:** A panel with a filter icon and the number '0'.

At the bottom of the window, there is a checkbox labeled 'Filter out events from all computer accounts' which is currently unchecked. Below this is a comment field with the placeholder text 'Please add a comment', a warning icon, a user profile picture, and 'Apply' and 'Close' buttons.

Filter events for selected or all computer accounts.

The screenshot shows the 'Active Directory Logga Filter Configuration' dialog. The main title is 'SET FILTER CRITERIAS TO LIMIT THE AMOUNT OF DATA COLLECTED BY THE ACTIVE DIRECTORY LOGGA'. The dialog is divided into several sections:

- Active Directory Events:** A section with a funnel icon and a count of 245.
- Event authors:** A section with a funnel icon and a count of 1.
- Group event authors:** A section with a funnel icon and a count of 1.
- Computer event authors:** A section with a funnel icon and a count of 1.
- Object classes:** A section with a funnel icon and a count of 2. This section is highlighted with a red box and a '1'.
- Attributes:** A section with a funnel icon and a count of 1.
- Logga monitoring:** A section with a funnel icon and a count of 1.

The 'Object classes' section contains a list of object classes. Two classes are highlighted with a red box and a '2': 'Print-Queue (printQueue)' and 'Service-Connection-Point (serviceConnectionPoint)'. The 'Filtered out Object classes' section shows a count of 2, corresponding to these two classes.

At the bottom right, there is a 'rescan' button highlighted with a red box and a '3'. Below the 'rescan' button is a text box that says 'Update the information of attributes and object classes by rescan of Active Directory.'.

At the bottom left, there is a comment box with the text 'Please add a comment' and a warning icon.

At the bottom right, there are 'Apply' and 'Close' buttons.

1. Filter the events of specific object classes.
2. By default events relating to the two selected object classes will be filtered.
3. The initial loading (and a rescan) of object classes from AD may take some time. After that the object classes will be loaded from the data base. Click "rescan" to update the object classes, e.g. after a schema change.

Active Directory Logga Filter Configuration

SET FILTER CRITERIAS TO LIMIT THE AMOUNT OF DATA COLLECTED BY THE ACTIVE DIRECTORY LOGGA

Active Directory Events

Event authors

Group event authors

Computer event authors

Object classes

Attributes

Attributes selection

ms-exch 4 of 1497

Filtered out Attributes

Filter 4

Update the information of attributes and object classes by [rescan](#) of Active Directory.

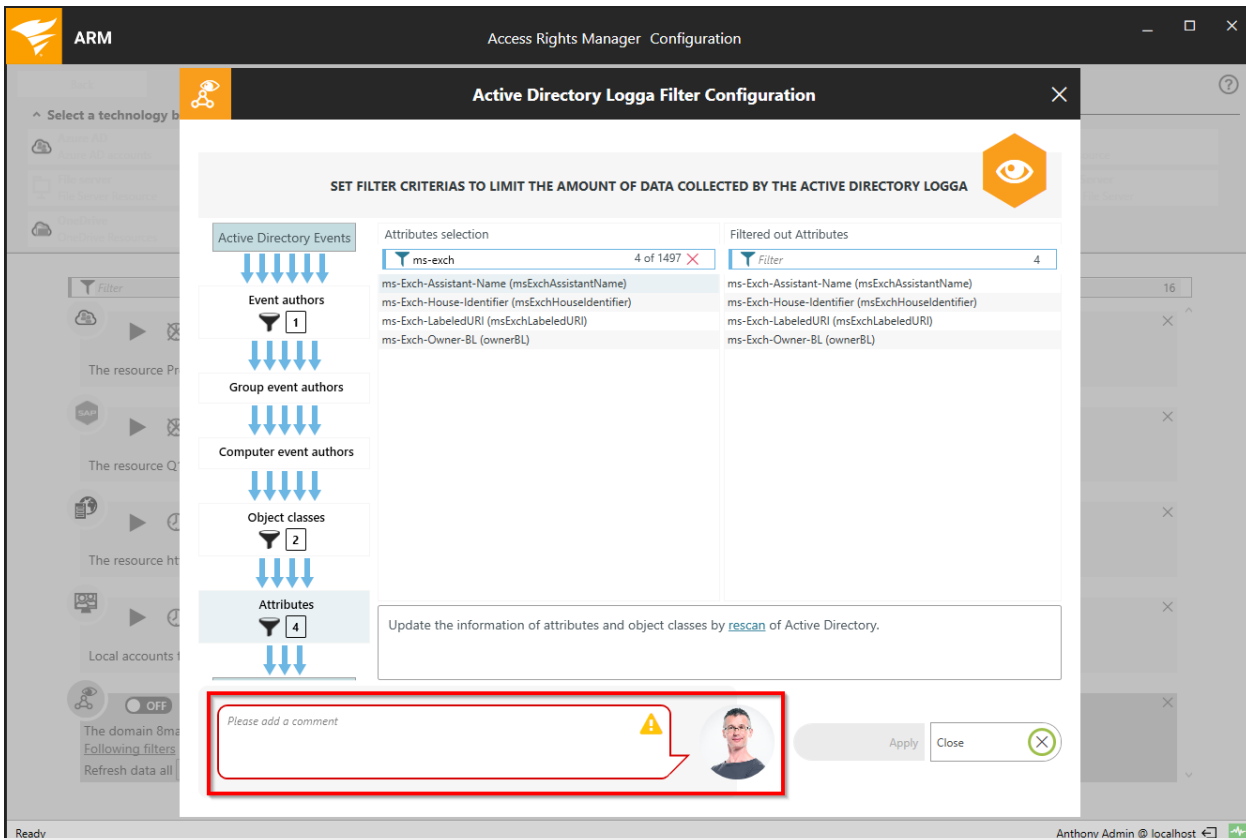
Please add a comment

Apply Close

Filter events related to specific attributes.

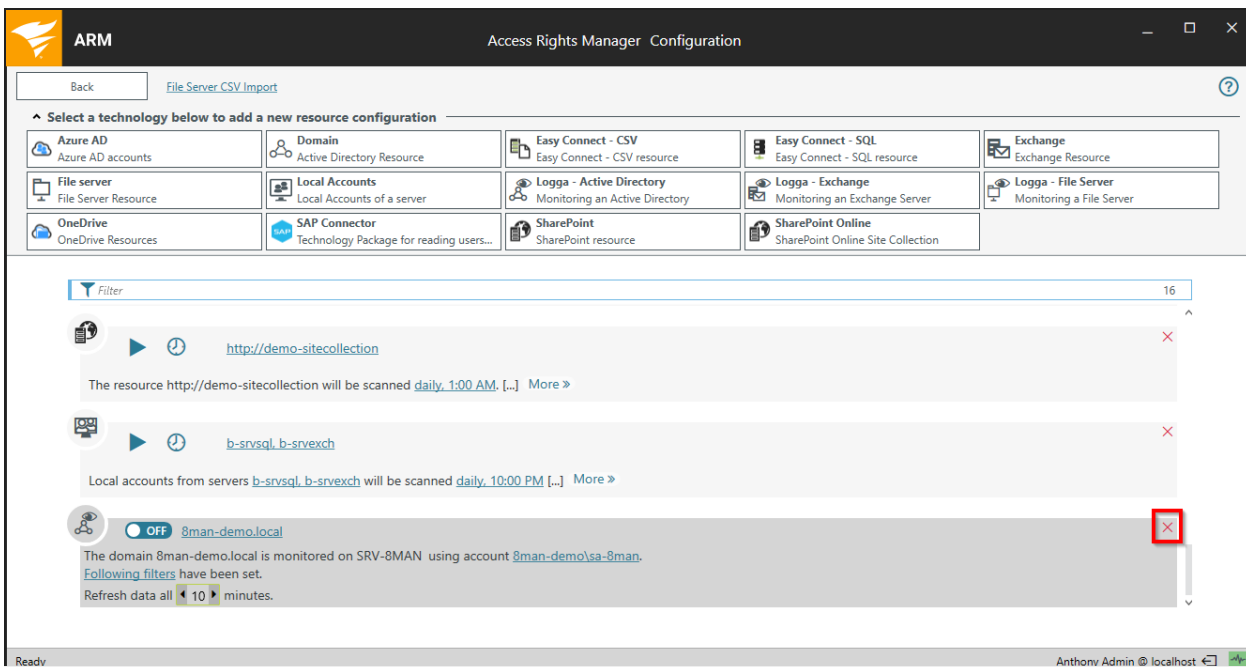
For example:

All events related to attributes that include "ms-exch" are filtered out / excluded.

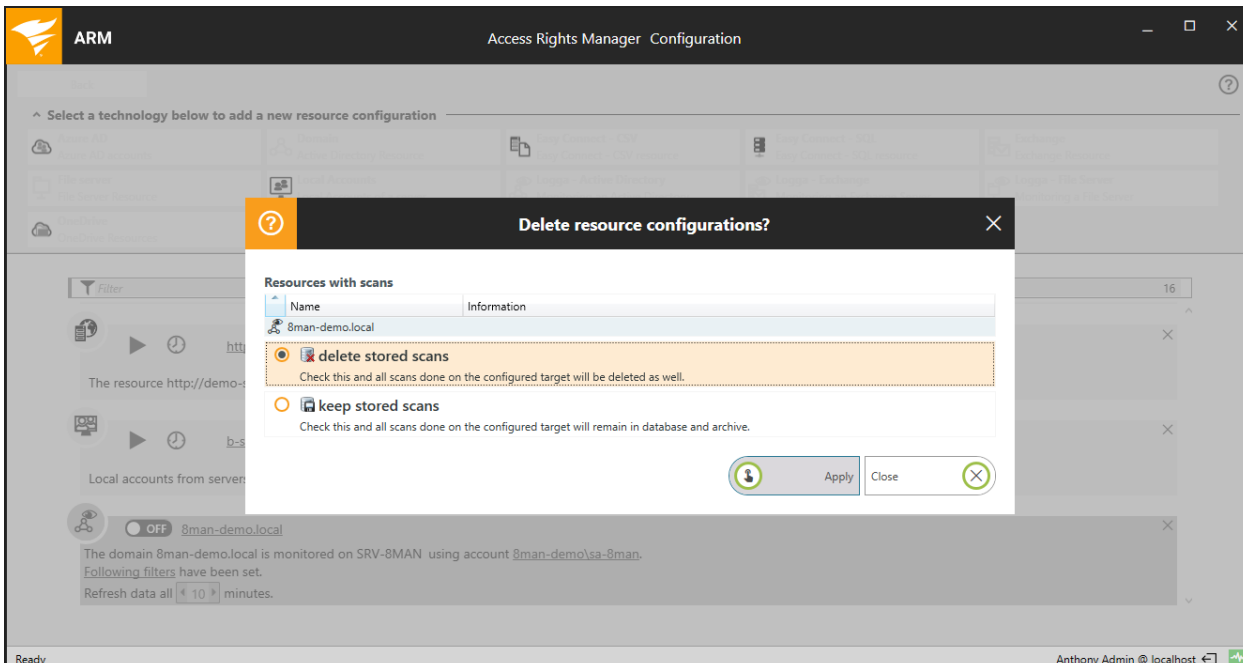


You must enter a comment to apply any changes made to filter settings.

### Delete an AD Logga configuration



Select the desired AD Logga configuration. Click on the red "X".



You can decide if you would like to keep or delete the stored Logga data.

Deleting is only possible if all user interfaces are closed.

You can [identify logged in users](#) in the server status menu.

## Configure the File Server (FS) Logga

**i** The configuration of file server alerts is described in the chapter [Enable alerts for file server directories](#).

### Prepare Windows file servers


Running the FS Logga on a Windows file server requires an installation of the following components on the file server:

- filter driver
- collector

When monitoring Windows file servers, no dedicated (external) collector server is required. The file server itself works as a collector.

The components are included in the setup file and can be installed in one step.

**i** If Windows Failover Cluster resources should be monitored you have to install both components on each node of the cluster.


 When replacing hard disks or when mounting other hard disks (setting up Volume Mount Points), the FS-Logga must be switched off before (ON/OFF button in the ARM configuration) and switched on again after the change.

Install the FS Logga on Windows file servers

The FS Logga requirements must be fulfilled.

In short:

- Windows Server 2008 R2 or higher
- Ports 55555 and 5671 TCP must be open bidirectionally between ARM server and Collectors
- .NET 4.8

 .NET 4.8 is included in the ARM setup. The installation of .NET 4.8 in most cases requires a reboot.


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

1. Copy ARM setup.exe into a local folder (do not use a network folder).
2. To start the installation, run the file with administrator rights.

The setup language is automatically selected to match the language of the operating system for the following languages: German, English, French. Otherwise English is used.

3. On the Setup Wizard home page, select "Advanced Installation".
4. In the second step of the wizard select "Custom Installation" and activate the two options "Collector" **and** "FS Logga" **only**.


Follow the instructions of the wizard and complete the setup.

 The collector service and the FS Logga filter driver must be installed on **every** Windows file server that you would like to monitor.

After the installation the collector must be added to the ARM configuration.

In short:

1. Log in to the ARM configuration application.
2. Click the collectors tile in the upper right corner.
3. Enter the name or the IP-address of the collector (no credentials needed).

 If you want to use the server name then make sure that the server name can be resolved by DNS or edit the hosts files. See also [Collectors in foreign domains \(non-trusted\)](#).

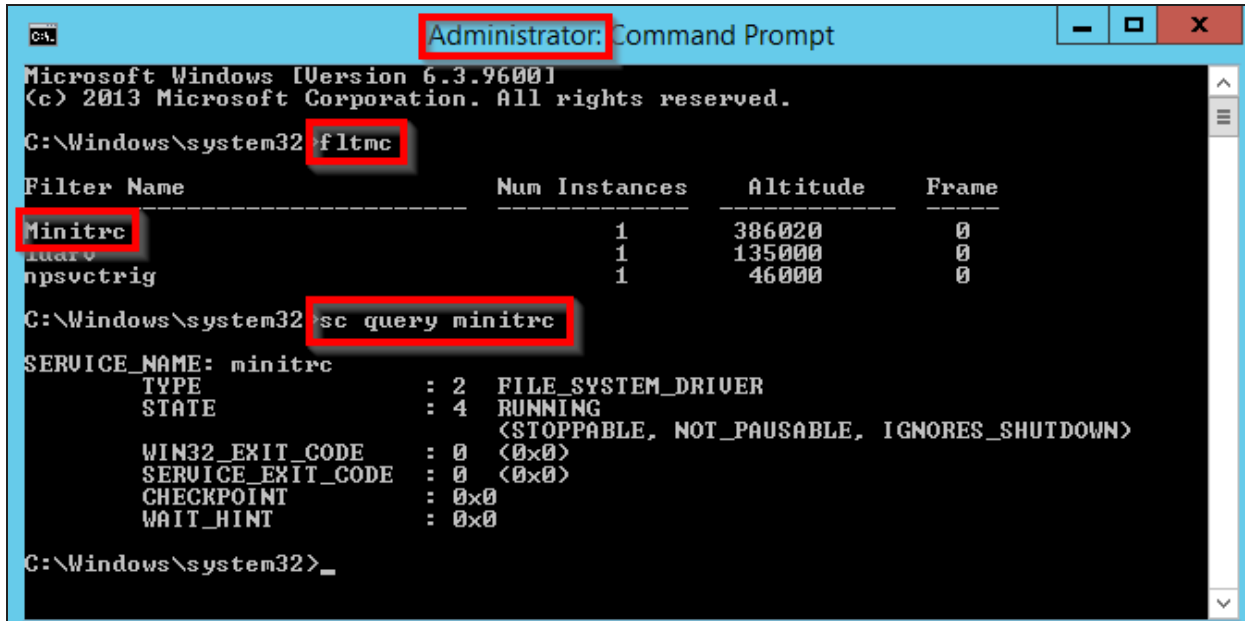


4. Click the plus icon to add the collector to the ARM configuration.
5. Check the connection status.

Detailed instructions and additional information can be found in the chapter [Install additional collectors](#).

### Verify filter driver activity

You can check the activity of the filter driver from the command prompt. To execute the commands, you must run the command prompt with administrator privileges.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>fltmc
Filter Name                               Num Instances  Altitude      Frame
-----
Minitrc                                   1              386020        0
fslogga                                   1              135000        0
npsvcstrig                                1              46000         0
C:\Windows\system32>sc query minitrc
SERVICE_NAME: minitrc
        TYPE               : 2  FILE_SYSTEM_DRIVER
        STATE                : 4  RUNNING
                        (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
C:\Windows\system32>
```

You can list loaded filter drivers with the following command:

```
fltmc
```

The filter driver of the FS logga will respond with "Minitrc". The number of instances must be at least 1. A number of 0 instances is possible, indicating that no report is configured or no alert is active.


You can see details of the filter driver with the following command:


```
sc query minitrc
```


## Prepare NetApp 7-mode file servers

### Collectors for NetApp file servers

Collectors for NetApp file servers are dedicated Windows servers with the collector service running.

 We strongly recommend that you use a Collector server within the same network segment as the NetApp file server, otherwise performance and routing problems may occur.


 Each 7-Mode NetApp needs its own collector.

 The FS Logga for NetApp file servers does **not** require a filter driver installation like on Windows file servers.

## Set NetApp file servers findable

In Active Directory registered NetApp file servers have a typical value set in the LDAP attribute `operatingSystem`. This property is used by the collector to detect NetApp file servers and mark it as NetApp file server type in the FS Logga configuration.

By default, the `operatingSystem` value of the NetApp file servers is set to `OnTap` or `NetApp` in the collector configuration file. If your NetApp file servers use different values for the `operatingSystem` property, you can adjust the search parameters.

 If your NetApp file server is not registered in Active Directory, you must create a computer account and set the `operatingSystem` attribute accordingly.

## Configuration file

`pnCollector.config.xml`

## Computer

Collector server which is configured for the NetApp file server.

## Path

`%ProgramData%\protected-networks.com\8MAN\cfg`

If the file does not exist, copy the "template" from the following path:

old: `%ProgramFiles%\Protected Networks\8MAN\etc`

new: `%ProgramFiles%\solarwinds\ARM\etc`

## Code

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<config>
```

```
  <tracer>
```

```
    <netapp>
```

```
      <NetappOperatingSystems>OnTap, NetApp</NetappOperatingSystems>
```

```
</netapp>
```

```
</tracer>
```

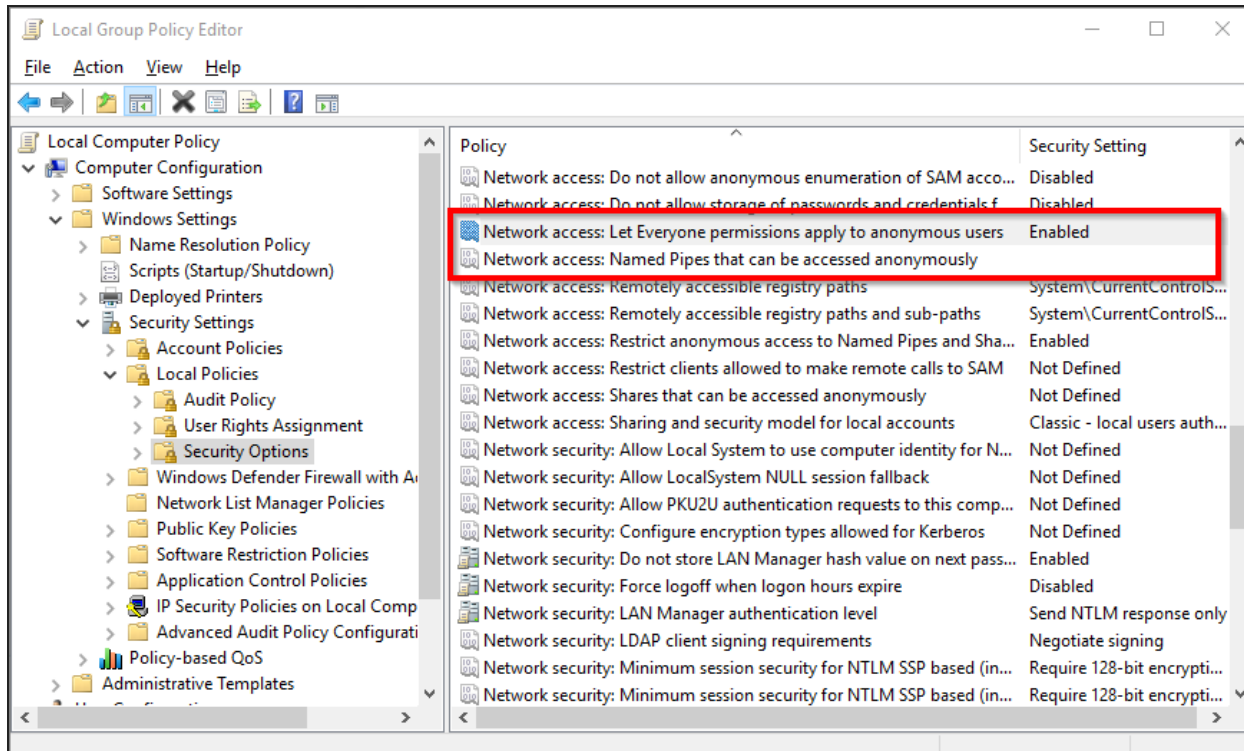
```
</config>
```

## Possible Values

Add your operatingSystem values comma-separated.

If your NetApp file servers have different values for the property “operatingSystem” then insert all these values separated by comma. If no or not all NetApp file servers register the property “operatingSystem” in the Active Directory leave the entry empty in the collectors configuration file. With an empty entry you will get all non-EMC or non-Windows computer accounts from Active Directory visible for the used account.

Set local security policies on collectors



To enable communication between NetApp and the collector, you must configure the following policy settings on the collector server.

### SECURITY OPTION

### VALUE

Network access: Let Everyone permissions apply to anonymous users

Enabled

SECURITY OPTION	VALUE
Network access: Named Pipes that can be accessed anonymously	ntapfprq_<netapp name> (<netapp name> is the name of the NetApp file server)

FPolicy feature

The FS-Logga for NetApp file server uses the NetApp FPolicy feature. Therefore it has to be activated and properly configured.


#### *Activation of the FPolicy feature*

```
options fpolicy.enable on
```

#### *Configuration of the FPolicy*

```
fpolicy create 8ManLogga screen
fpolicy enable 8ManLogga
fpolicy options 8ManLogga cifs_setattr on
```

The value **8ManLogga** of the FPolicy has to match with the value in the configuration file.

 The configuration file only needs to be edited if you want to use a value other than the default value.

### **Configuration file**

```
pnTracer.config.xml
```

### **Computer**

Collector server which is configured for the NetApp file server.

### **Path**

```
%ProgramData%\protected-networks.com\8MAN\cfg
```

If the file does not exist, copy the "template" from the following path:

```
old: %ProgramFiles%\Protected Networks\8MAN\etc
```

```
new: %ProgramFiles%\solarwinds\ARM\etc
```


## Code

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <netapp>
      <policy>8ManLogga</policy>
    </netapp>
  </tracer>
</config>
```

## Possible Values

The value has to match with the name of the created FPolicy.

Default value: 8ManLogga

 The configuration file only needs to be edited if you want to use a value other than the default value.

## Domain accounts

The collector server's computer account must become a member of the Backup Operators group on the NetApp file server.

```
useradmin domainuser add <domain\computer-account> -g "Backup Operators"
```

To be able to read the complete paths of the shares a user account is needed, that is member of the "Power Users" group on the NetApp file server:

```
useradmin domainuser add <domain\user> -g "Power Users"
```

## Prepare NetApp clustered data ONTAP file servers

### Collectors for NetApp file servers

Collectors for NetApp file servers are dedicated Windows servers with the collector service running.

**⚠** We strongly recommend that you use a Collector server within the same network segment as the NetApp file server, otherwise performance and routing problems may occur.

**i** The FS Logga for NetApp file servers does **not** require a filter driver installation like on Windows file servers.

### Set NetApp file servers findable

In Active Directory registered NetApp file servers have a typical value set in the LDAP attribute `operatingSystem`. This property is used by the collector to detect NetApp file servers and mark it as NetApp file server type in the FS Logga configuration.

By default, the `operatingSystem` value of the NetApp file servers is set to `OnTap` or `NetApp` in the collector configuration file. If your NetApp file servers use different values for the `operatingSystem` property, you can adjust the search parameters.

**i** If your NetApp file server is not registered in Active Directory, you must create a computer account and set the `operatingSystem` attribute accordingly.

### Configuration file

`pnCollector.config.xml`

### Computer

Collector server which is configured for the NetApp file server.

### Path

`%ProgramData%\Protected Networks\8MAN\cfg`

If the file does not exist, copy the "template" from the following path:

old: `%ProgramFiles%\Protected Networks\8MAN\etc`

new: `%ProgramFiles%\solarwinds\ARM\etc`

### Code

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<config>
```

```
  <tracer>
```

```
    <netapp>
```

```
<NetappOperatingSystems>OnTap, NetApp</NetappOperatingSystems>
  </netapp>
</tracer>
</config>
```


## Possible Values

Add your operatingSystem values comma-separated.

If your NetApp file servers have different values for the property “operatingSystem” then insert all these values separated by comma.

If no or not all NetApp file servers register the property “operatingSystem” in the Active Directory leave the entry empty in the collectors configuration file. With an empty entry you will get all non-EMC or non-Windows computer accounts from Active Directory visible for the used account.

Set up encrypted data transfer on the collector

 The following steps are only necessary if communication between NetApp and the collector is to be encrypted.

If you have configured encrypted data transfer (see chapter [Creating the External Engine Configuration](#)) you also have to adapt the pnTracer.config.xml file on the collector server. For each file server (CIFS server on the NetApp) to be monitored on this collector, the following entry have to be added under

```
<tracer><netapp><ssl><cifsServers>
```

```
<name of cifs server>
```

```
  <switchOn type="System.Boolean">true</switchOn>
```


```
  <protocol type="System.Int32">5</protocol>
```

```
  <serverCertificateName>name of certificate from certificate store to use</serverCertificateName>
```

```
</name of cifs server>
```

The certificate must be installed in the computers certificate store.


For <protocol> the following values are possible: TLS = 1, TLS1.1 = 2, TLS1.2 = 3, SSL2 = 4, SSL3 = 5. Default is SSL3 (5).

 Choose a protocol available on both collector and NetApp.

## FPolicy feature

The FS-Logga for NetApp file server uses the NetApp FPolicy feature. Therefore it has to be activated and properly configured via CLI.


To configure the FPolicy feature you have to use an account of role admin or vsadmin on the NetApp.

 In all following CLI commands the parameter “<vserver\_name>” has to be replaced by the name of the SVM (Storage Virtual Machine).

## Creating the event configuration

The event configuration determines:

- which events will be monitored
- which events will not be monitored
- which protocol is used (only the CIFS protocol is supported by FS Logga)

 Change only the parameter “<vserver\_name>”. All other changes may lead to missing events in the reports or to higher load of collector and NetApp because of processing of not used events.

## Command

```
fpolicy policy event create -vserver <vserver_name> -event-name event_8manlogga_  
cifs -file-operations create, create_dir, delete, delete_dir, read, write,  
rename, rename_dir, setattr, open -protocol cifs -filters first-read, first-  
write, open-with-delete-intent
```

## Replace:

<vserver\_name> - name of the SVM (Storage Virtual Machine)

With the following command you can check the result:

```
fpolicy policy event show
```

## Creating the External Engine Configuration

The External Engine Configuration determines to which server (defined by IP address and port) the events has to be sent by the NetApp. The IP address has to be an address of the FS-Logga collector reachable by the NetApp. The port must be a free and reachable port on the collector.



## Command

```
fpolicy policy external-engine create -vserver <vserver_name> -engine-name  
engine_8manlogga -primary-servers <collector-ip> -port 2002 -extern-engine-type  
asynchronous -ssl-option <ssl-option>
```

### Replace:

<vserver\_name> - name of the SVM (Storage Virtual Machine)

<collector-ip> - IP address of the collector

<ssl-option>

- "no-auth" - no encryption
- "server-auth" - use encryption

If you want to use encryption, it must be configured on the [collector](#) and on the [NetApp](#).

With the following command you can check the result:

```
fpolicy policy external-engine show
```

## Creating the FPolicy Configuration

The FPolicy Configuration is the assembly of Event- and External Engine Configuration.

## Command

```
fpolicy policy create -vserver <vserver_name> -policy-name 8manlogga -events  
event_8manlogga_cifs -engine engine_8manlogga -is-mandatory false
```

### Replace:

<vserver\_name> - name of the SVM (Storage Virtual Machine)

With the following command you can check the result:

```
fpolicy policy show
```

Creating the scope for the FPolicy

Use the following command to specify the volumes to be monitored, including their shares, directories, and files.

### Command

```
fpolicy policy scope create -vserver <vserver_name> -policy-name 8manlogga -  
volumes-to-include "*" "
```

### Optional: Replace

```
"* "
```

If only certain volumes are to be monitored, we recommend specifying a comma-separated list of these volumes instead of the wildcard ("\*"). This reduces the load on the NetApp file server and on the collector.

Enable FPolicy


If all of the above steps were successful, you need to activate the policy. Even if only one policy is defined, the system requires a sequence number.

### Command

```
fpolicy enable -vserver <vserver_name> -policy-name 8manlogga -sequence-number 1
```

### Replace:

<vserver\_name> - name of the SVM (Storage Virtual Machine)

 The sequence number must always be specified, even if there is only one FPolicy. It determines the order in which the FPolicies are processed.

With the following command you can check the result:

```
fpolicy show-enabled
```

Domain accounts

To read the shares local paths an account is needed which is member of the local group "Power Users" on the NetApp SVM. With this account the Logga has to be configured later.

## Command

```
vserver cifs users-and-groups local-group add-members -vserver <vserver_name> -  
group-name "BUILTIN\Power Users" -member-names <domain\user>
```

### Replace:

<vserver\_name> - name of the SVM (Storage Virtual Machine)

<domain\user> - User account used to configure FS Logga within ARM

The Logga uses the ONTAP API to read FPolicy data and request the NetApp to start Logging for the external engine. For this the Logga needs an account with restricted access rights on the NetApp. Therefore a new role should be created and the rights of this role will be defined.

## Commands

```
security login role create -role 8manrole -vserver <vserver_name> -cmd "vserver  
fpolicy"
```

```
security login role create -role 8manrole -vserver <vserver_name> -cmd "volume"  
-access readonly
```

```
security login role create -role 8manrole -vserver <vserver_name> -cmd "vserver"  
-access readonly
```

```
security login role create -role 8manrole -vserver <vserver_name> -cmd "version"  
-access readonly
```

### Replace:

<vserver\_name> - name of the SVM (Storage Virtual Machine)

With the following command you can check the result:

```
security login role show
```

Assign the new role to the account used by the Logga

```
security login create -username <domain\username> -application ontapi -  
authmethod domain -role 8manrole -vserver <vserver_name>
```

### Replace:

<vserver\_name> - name of the SVM (Storage Virtual Machine)

<domain\username> - User account used to configure FS Logga within ARM

With the following command you can check the result:

```
security login show
```

### Firewall configuration

The Logga uses the ONTAP API via https to read FPolicy data and to request the NetApp to start logging for the external engine. The service https must be configured on a LIF (Logical Interface) of the SVM. This LIF must be reachable by the collector.

Use the following command to see the service that is active on which SVM firewall policy:

```
system service firewall policy show
```

The assignment of firewall policies to LIF of a certain SVM can be checked with:

```
network interface show -vserver <vserver_name> -fields firewall-policy
```

*Replace:*

<vserver\_name> - name of the SVM (Storage Virtual Machine)

If a firewall policy with the service https is already active on a LIF of the SVM, then you only need to change the 'allow-list':

```
system services firewall policy modify -vserver <vserver_name> -policy <current_firewall_policy> -service https -allow-list <collector-ip/32>
```

*Replace:*

<vserver\_name> - name of the SVM (Storage Virtual Machine)

<current\_firewall\_policy> - already activated firewall policy

<collector-ip/32> - IP address of the collector

If you do not want to change the current firewall policy, you can create a copy of this firewall policy, perform the necessary changes, and then assign this new firewall policy to the appropriate LIF:

```
system services firewall policy clone -vserver <vserver_name> -policy <current_firewall_policy> -destination-policy 8manlogga_fp
```

*If the https service **already exists** in the cloned firewall policy:*

```
system services firewall policy modify -vserver <vserver_name> -policy 8manlogga_fp -service https -allow-list <collector-ip/32>
```

*If the https service is not present in the cloned firewall policy:*

```
system services firewall policy create -vserver <vserver_name> -policy  
8manlogga_fp -service https -allow-list <collector-ip/32>  
  
network interface modify -vserver <vserver_name> -lif <lif> -firewall-policy  
8manlogga_fp
```

*Replace:*

<vserver\_name> - name of the SVM (Storage Virtual Machine)

<current\_firewall\_policy> - already activated firewall policy

<collector-ip/32> - IP address of the collector

<lif> - Name of the Logical Interface

Certificate configuration for encrypted event data transfer

If you have configured encrypted event data transfer between NetApp and Logga (see "[Creating the External Engine Configuration](#)") then the public certificate of certificate authority that is used to sign the collector certificate has to be installed on the SVM:

```
security certificate install -vserver <vserver_name> -type client-ca
```

*Replace:*

<vserver\_name> - name of the SVM (Storage Virtual Machine)


Use the following command to verify that the certificate has been installed:


```
security certificate show
```

## Prepare EMC file servers

Collectors for EMC file servers

Collectors for EMC file servers are dedicated Windows servers with the collector service running.

 We strongly recommend that you run the Collector and the EMC file server within the same network segment, otherwise performance and routing problems may occur. The Collector service should preferably be installed on the same Windows server on which the [Common Event Enabler](#) (CEE) is installed.

 The FS Logga for EMC file servers does **not** require a filter driver installation like on Windows file servers.

Set EMC Celerra/VNX file servers findable

In Active Directory registered EMC file servers have a set operatingSystem attribute. This attribute is used by the collector to detect EMC file servers and mark it as EMC file server type in the FS Logga configuration.

By default, the operating systems of the EMC file servers are set to "EMC File Server" and "EMC Celerra File Server" in the collector configuration file. If your EMC file servers use different values for the operatingSystem property, you can adjust the search parameters.

## Configuration file

pnCollector.config.xml

## Computer

Collector server which is configured for the EMC file server.

## Path

%ProgramData%\Protected Networks\8MAN\cfg

If the file does not exist, copy the "template" from the following path:

old: %ProgramFiles%\Protected Networks\8MAN\etc

new: %ProgramFiles%\solarwinds\ARM\etc

## Code

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <emc>
      <EmcOperatingSystems>EMC File Server,EMC Celerra File
Server</EmcOperatingSystems>
    </emc>
  </tracer>
</config>
```

## Possible Values

Add your operatingSystem values comma-separated.

If your EMC file servers have different values for the property "operatingSystem" then insert all these values separated by comma. If no or not all EMC file servers register the property "operatingSystem" in the Active Directory leave the entry empty in the collectors configuration file. With an empty entry you will get all non-NetApp or non-Windows computer accounts from Active Directory visible for the used account.

Set EMC Isilon file servers findable

The Isilon cluster does not register the CIFS file server in Active Directory. If the FS Logga searches for resources to be monitored, it will not find any EMC resource. You must use the cluster name as a resource name or manually add a computer account to Active Directory that is used as a CIFS server to access the shares on Isilon. In this case, you must also add a corresponding DNS record for routing.

Set for the manually created computer account the operatingSystem attribute for example to "EMC Isilon" and modify the configuration file to find the computer accounts with the special operatingSystem attribute as shown below.

## Configuration file

pnCollector.config.xml

## Computer

Collector server which is configured for the EMC file server.

## Path

%ProgramData%\protected-networks.com\8MAN\cfg

If the file does not exist, copy the "template" from the following path:

old: %ProgramFiles%\Protected Networks\8MAN\etc

new: %ProgramFiles%\solarwinds\ARM\etc

## Code

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <emc>
      <EmcOperatingSystems>EMC Isilon</EmcOperatingSystems>
    </emc>
  </tracer>
</config>
```

```
</config>
```

## Possible Values

Set the value to the same value as the operatingSystem attribute in Active Directory.

Alternatively, you can leave the EmcOperatingSystems value empty. With the empty EmcOperatingSystems entry, the Logga displays all available all non-NetApp or non-Windows AD computer accounts so that you can select the manually created ones.

## Common Event Enabler (CEE)

The Common Event Enabler (CEE) for Windows, is a necessary component provided by EMC to enable monitoring. We recommend that you install both the CEE and the collector on the same Windows server.

The Common Event Enabler (CEE) must be published to EMC, enable EMC to forward the events. We recommend to install and start the CEE before configuring the EMC. This way you can check immediately if these components are connected.

## Installation of the CEE

The collector installation needs another EMC specific framework installation. This framework called "CEE" covers the communication between EMC Data Mover and EMC CEE framework. The actual installation documents can be found in the EMC documentation center.

ARM supports the CEE up to version 6.6 or 8.6.1 or higher.

## ARM specific changes for the CEE

For optimal performance, the collector and CEE should run on the same server.


The connection between collector and CEE framework client is controlled by Windows registry entries. To apply these changes you need administrator rights. In registry editor navigate to:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP]
```

Create or change the following entries.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] Enabled=(REG_DWORD) 0x00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] EndPoint=(REG_SZ) "SolarWindsARM"
```

 The new values will be active after restarting the CEE service "emc cava".



Creating and editing cepp.conf file

Create a file named cepp.conf with following content:


```
cifsserver=  
surveytime=10  
ft level=0  
msrpcuser=<the account the CEE service is running under>  
pool name=pool1 \  
servers=<IP address or hostname of the Windows server running the CEE service> \  
postevents=* \  
option=ignore \  
reqtimeout=1000 \  
retrytimeout=500
```

Copy this file to the root directory of the EMC Data Mover:

```
$ server_file <movername> -put cepp.conf cepp.conf
```

Administer rights of the account of CEE service

For verification of the account the CEE service is running under, on the EMC you have to administer the rights of this account accordingly.

 The installation of the MMC snap-in is described in the EMC document "Installing Management Applications on VNX for File".

Procedure according to the document [Using the Common Event Enabler on Windows](https://www.delltechnologies.com/en-us/collaterals/unauth/technical-guides-support-information/products/storage-3/docu48055.pdf) (© 2020 Dell Inc, <https://www.delltechnologies.com/en-us/collaterals/unauth/technical-guides-support-information/products/storage-3/docu48055.pdf>, obtained on January 29, 2020):

1. Click Start and select Settings > Control Panel > Administrative Tools > EMC VNX File CIFS Management. The EMC VNX File CIFS Management window appears.
2. Perform one of the following:
  - a. If a Data Mover is already selected (name appears after Data Mover Management), go to step 4.
  - b. If a Data Mover is not selected:
    - Right-click Data Mover Management and select Connect to Data Mover.
    - In the Select Data Mover dialog box, select a Data Mover by using one of the following methods:

- i. In the Look in: list box, select the domain in which the Data Mover that you want to manage is located and select the Data Mover from the list. Or
  - ii. In the Name box, type the computer name, IP address, or the NetBIOS name of the Data Mover.
3. Double-click Data Mover Management, and double-click Data Mover Security Settings.
4. Click User Rights Assignment. The assignable rights appear in the right pane.
5. Double-click EMC Event Notification Bypass. The Security Policy Setting dialog box appears.
6. Click Add. The Select Users or Groups dialog box appears.
7. If necessary, choose the server from the Look in drop-down list. Select the user from the list box.
8. Click Add, and then click OK to close the Select Users or Groups dialog box.
9. Click OK to close the Security Policy Setting dialog box.
10. In the User Rights Assignment list, double-click EMC Virus Checking. The Security Policy Setting dialog box appears.
11. Click Add. The Select Users or Groups window appears.
12. If necessary, choose the server from the Look in drop-down list. Select the user from the list box.
13. Click Add, and then click OK to close the Select Users or Groups dialog box.
14. Click OK to close the Security Policy Setting dialog box.
15. Close the EMC VNX File CIFS Management window.

#### Starting the Common Event Publishing Agent (CEPA)

The last step is starting and checking CEPA on EMC.

- **Start**  

```
$ server_cepp <movername> -service -start
```

in which:  
<movername> = name of the Data Mover

result:  
<movername> : done
- **Check CEPA status:**  

```
$ server_cepp <movername> -service -status
```

result:  
<movername>: CEPP Started
- **Detailed info:**  

```
$ server_cepp <movername> -pool -info
```

result:  
<movername>:  
pool\_name = <pool name>  
server\_required = no  
access\_checks\_ignored = 0  
req\_timeout = 500 ms  
retry\_timeout = 50 ms

```
pre_events =
post_events = CreateFile,DeleteFile, RenameFile, FileRead ...
post_err_events =
CEPP Servers:
IP = <CEE IP>, state = ONLINE, vendor = Unknown
```

Configure Isilon file servers

Configuration of auditing for Isilon is done via CLI.

### Set the necessary event types

```
isi audit settings modify --audit-success create,delete,read,rename,set_
security,write
```

### Set the <hostname>

Use the server name that is used to access the shares on the Isilon. This name must be identical to the resource name selected in the ARM configuration for logging.

```
isi audit settings global modify --hostname=<hostname>
```


### Set the CEE URI

```
isi audit settings global modify --add-cee-server-uris=<CEE_server_URI>
```

 The CEE URI looks like `http://cee.example.com:12228/cee`. Port 12228 is the CEE default port.

### Set zones to monitor

Zones define the shares or directories for which the Isilon sends the events to CEE (and finally to the FS Logga).

 This setting is the basis for the [selection of the directories](#) to be monitored in the FS Logga Reports. If you select a directory for an FS Logga report that is not included in a monitored zone, the report will contain no events.

```
isi audit settings global modify --audited-zones <zone>
```

### Enable auditing

```
isi audit settings global modify --protocol-auditing-enabled on
```

## Add a FS Logga configuration

**Server Status**  
License Information

Logged in users: 1

Licensed  
Active user accounts: 1175

**Jobs**  
Summary

138 Scans  
14 Reports

190 Changes  
149 More

7 Scheduled  
482 Succeeded

0 Executing  
2 Failed

**Collectors**  
Configuration

1 Connected  
1 Configured in Total

All Collectors are Operational

Filter

**Scans**  
Resource Configurations, Logga, File Server CSV Import

**Open Order**  
Open Order Resource Descriptions

**User Management**  
User Management, Role Management

**Data Owner**  
Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings

**License**  
License Information, Server Status

**Jobs Overview**  
Job Status, Job Categories

**Alerts**  
Activate/Deactivate Alert Sensors

**Change Configuration**  
Common Change Settings, Technology-specific Change Configurations

**Scripting**  
Scripting configuration for change actions

**Views & Reports**  
Views & Reports, Blacklist for Views & Reports

**Server**  
Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging

**Basic Configuration**  
ARM Server, SQL Server, Configuration Status

Ready Anthony Admin @ localhost

Log in to the ARM configuration application. Click Scans.

The screenshot shows the SolarWinds Access Rights Manager (ARM) Configuration interface. At the top, the title bar reads "ARM Access Rights Manager Configuration". Below the title bar, there is a navigation bar with "Back" and "File\_Server\_CSV\_Import" buttons. The main content area is titled "Select a technology below to add a new resource configuration". It features a grid of technology options:

<b>Azure AD</b> Azure AD accounts	<b>Domain</b> Active Directory Resource	<b>Easy Connect - CSV</b> Easy Connect - CSV resource	<b>Easy Connect - SQL</b> Easy Connect - SQL resource	<b>Exchange</b> Exchange Resource
<b>File server</b> File Server Resource	<b>Local Accounts</b> Local Accounts of a server	<b>Logga - Active Directory</b> Monitoring an Active Directory	<b>Logga - Exchange</b> Monitoring an Exchange Server	<b>Logga - File Server</b> Monitoring a File Server
<b>Logga - OneDrive</b> Monitoring a Microsoft Office 365 One...	<b>Logga - SharePoint Online</b> Monitoring a Microsoft Office 365 Sha...	<b>OneDrive</b> OneDrive Resources	<b>SAP Connector</b> Technology Package for reading users...	<b>SharePoint</b> SharePoint resource

The "Logga - File Server" option is highlighted with a red border. Below the grid, there is a "Filter" input field with a value of "13". The main list shows several configurations for the domain "8man-demo.local":

- 8man-demo.local**: The domain 8man-demo.local will be scanned daily, 10:00 PM [...]. 0 resources are associated with this domain.
- srv-8man**: The file server srv-8man of type Windows will be scanned daily, 10:10 PM [...].
- 8man-demo.local** (OFF): The domain 8man-demo.local is monitored on SRV-8MAN using account 8man-demo\sa-8man. Following filters have been set. Refresh data all 10 minutes.
- https://8mandemo.sharepoint.com**: The resource https://8mandemo.sharepoint.com will be scanned On demand [...].
- 8man-demo.com**: The Exchange 8man-demo.com will be scanned On demand [...].
- SharePoint-Demo**: (No description visible)


The bottom status bar shows "Ready" on the left and "Anthony Admin @ localhost" on the right.

Click Logga - File Server.

### File Server Logga selection ⊗

Please select a resource. You can change the credentials and refresh the list when the given credentials are insufficient to find all resources.


Credentials **8man-demo\sa-8man** 1

▼ Filter or type IP or Name 3 

Name	Cluster	Fileserver Type
<input checked="" type="radio"/> netapp-demo		NetApp C-Mode
<input checked="" type="radio"/> emc-isilon		EMC
<input checked="" type="radio"/> SRV-8MAN		NTFS

2

^ Assigned collectors

▼ Collectors ▲ 

SRV-8MAN ●

Close
Apply
4

1. Set credentials for reading computer accounts from Active Directory.
2. List of computer accounts from Active Directory. The list is filtered by presumed file servers.

i For Windows failover clusters, please refer to the [following notes](#).

i If you are missing NetApp file servers, please see [Set NetApp file server findable](#).

**i** If you are missing EMC file servers, please see [Set EMC file servers findable](#).

3. Select a collector server.

**i** For Windows file servers you can only select the collector that is installed on the file server.

**i** For Windows failover clusters, please refer to the [following notes](#).

**i** For NetApp or EMC file servers, we strongly recommend 1:1 collector to file server mapping.

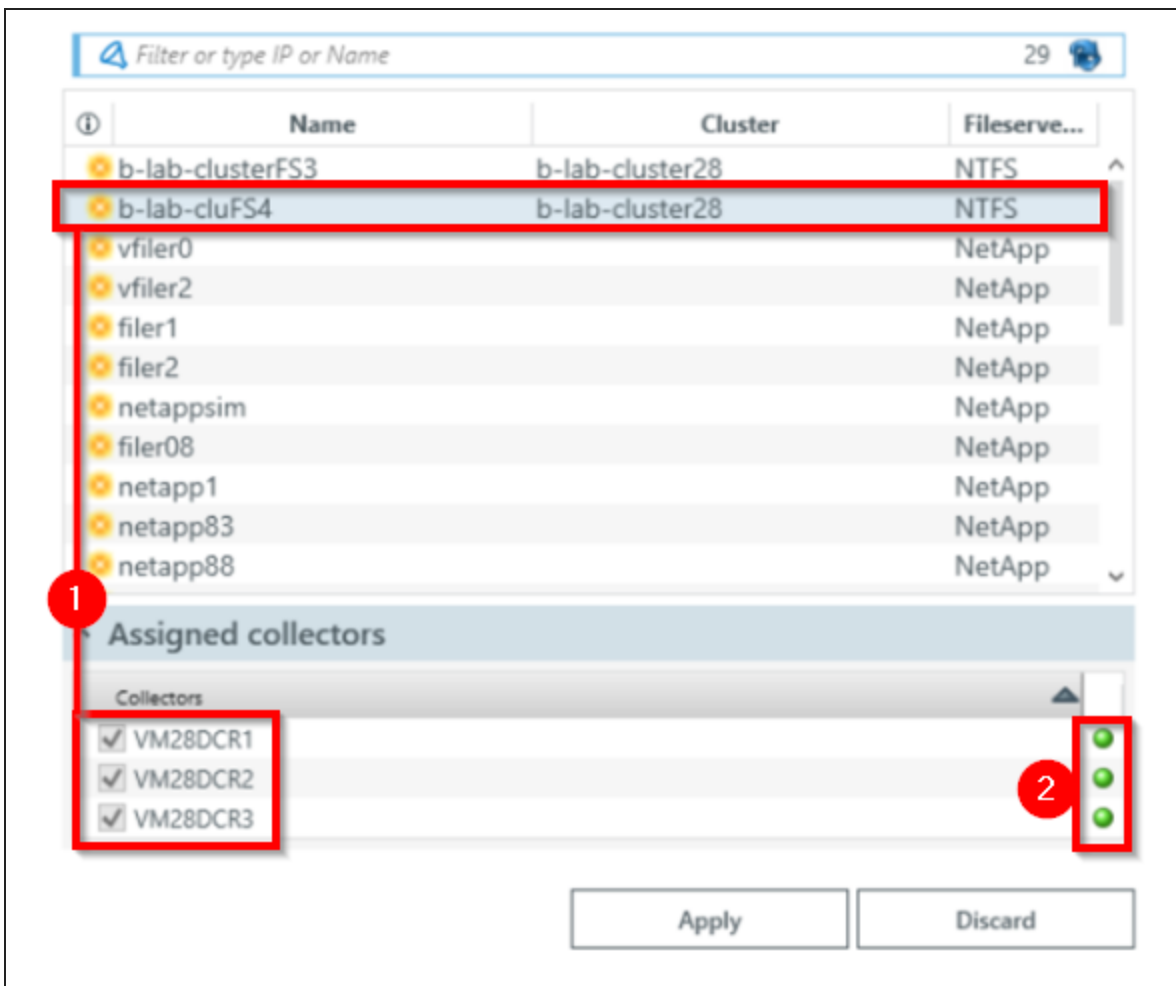
4. Click Apply.

## Windows failover cluster

If the Windows Failover Cluster feature is active on a file server, ARM displays the active Services/Roles instead of the of the file server name.

To successfully configure a FS Logga for a Windows failover cluster, the following requirements must be met:

- The FS Logga filter driver is installed on every node.
- The collector service is installed and running on every node.
- Every node collector service is connected to the ARM server and configured by name and **not** by IP address. See also [Verify collector connection status](#)



The screenshot displays the SolarWinds Access Rights Manager interface. At the top, there is a search bar with the text "Filter or type IP or Name" and a user profile icon showing "29". Below this is a table with columns for "Name", "Cluster", and "Fileserve...". The table lists several resources, with "b-lab-cluFS4" highlighted in blue and a red box around it. Below the table is a section titled "Assigned collectors" with a sub-section "Collectors" containing three entries: "VM28DCR1", "VM28DCR2", and "VM28DCR3", each with a checked checkbox and a green status icon. A red box highlights the checkboxes, and another red box highlights the green status icons. At the bottom of the interface are "Apply" and "Discard" buttons. Red circles with numbers "1" and "2" are placed next to the highlighted resource and status icons, respectively.

Name	Cluster	Fileserve...
b-lab-clusterFS3	b-lab-cluster28	NTFS
b-lab-cluFS4	b-lab-cluster28	NTFS
vfiler0		NetApp
vfiler2		NetApp
filer1		NetApp
filer2		NetApp
netappsim		NetApp
filer08		NetApp
netapp1		NetApp
netapp83		NetApp
netapp88		NetApp

Assigned collectors

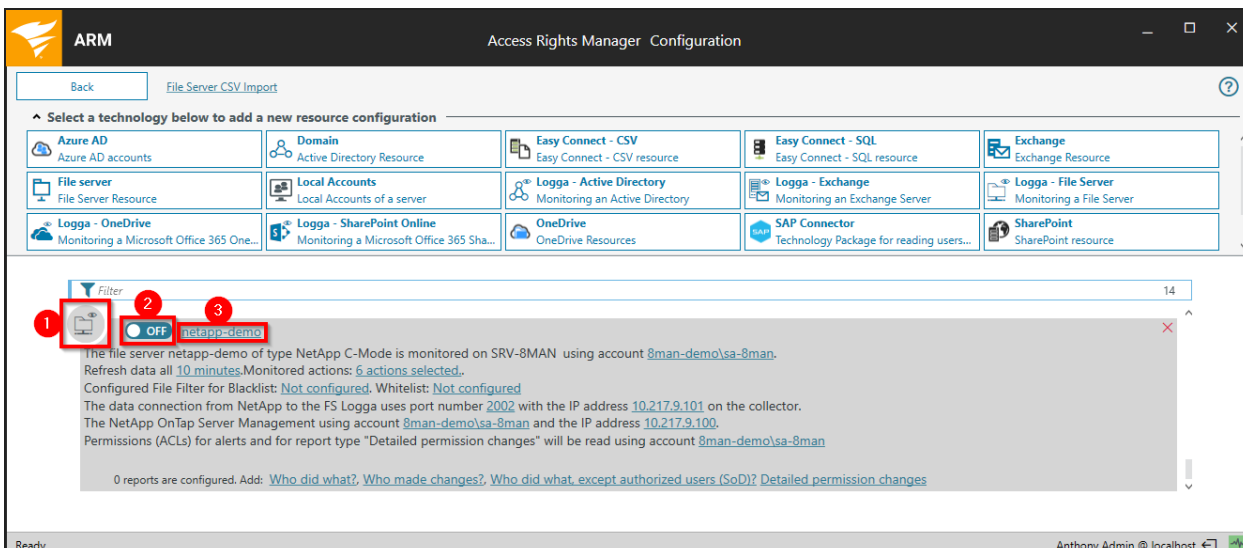
Collectors
<input checked="" type="checkbox"/> VM28DCR1
<input checked="" type="checkbox"/> VM28DCR2
<input checked="" type="checkbox"/> VM28DCR3

Apply Discard

1. If you select a Windows cluster resource, all collectors involved are already preselected. You will not be able to change the selection.
2. All collectors must be available, indicated by the green icons. Otherwise you will not be able to create the FS Logga configuration.

## Complete a FS Logga configuration



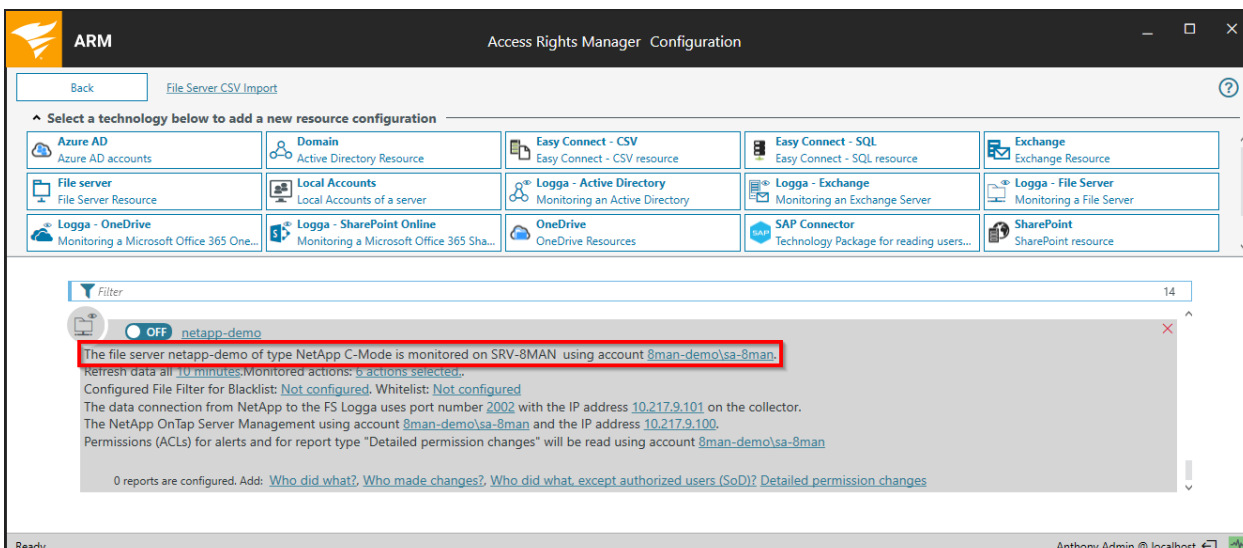


1. The folder icon with the eye indicates a FS Logga configuration.
2. Turn the FS Logga on or off. You must enter a comment to perform the action. The event and the comment is recorded in the ARM logbook.

Use the logbook to verify that the FS Logga has been turned on successfully.

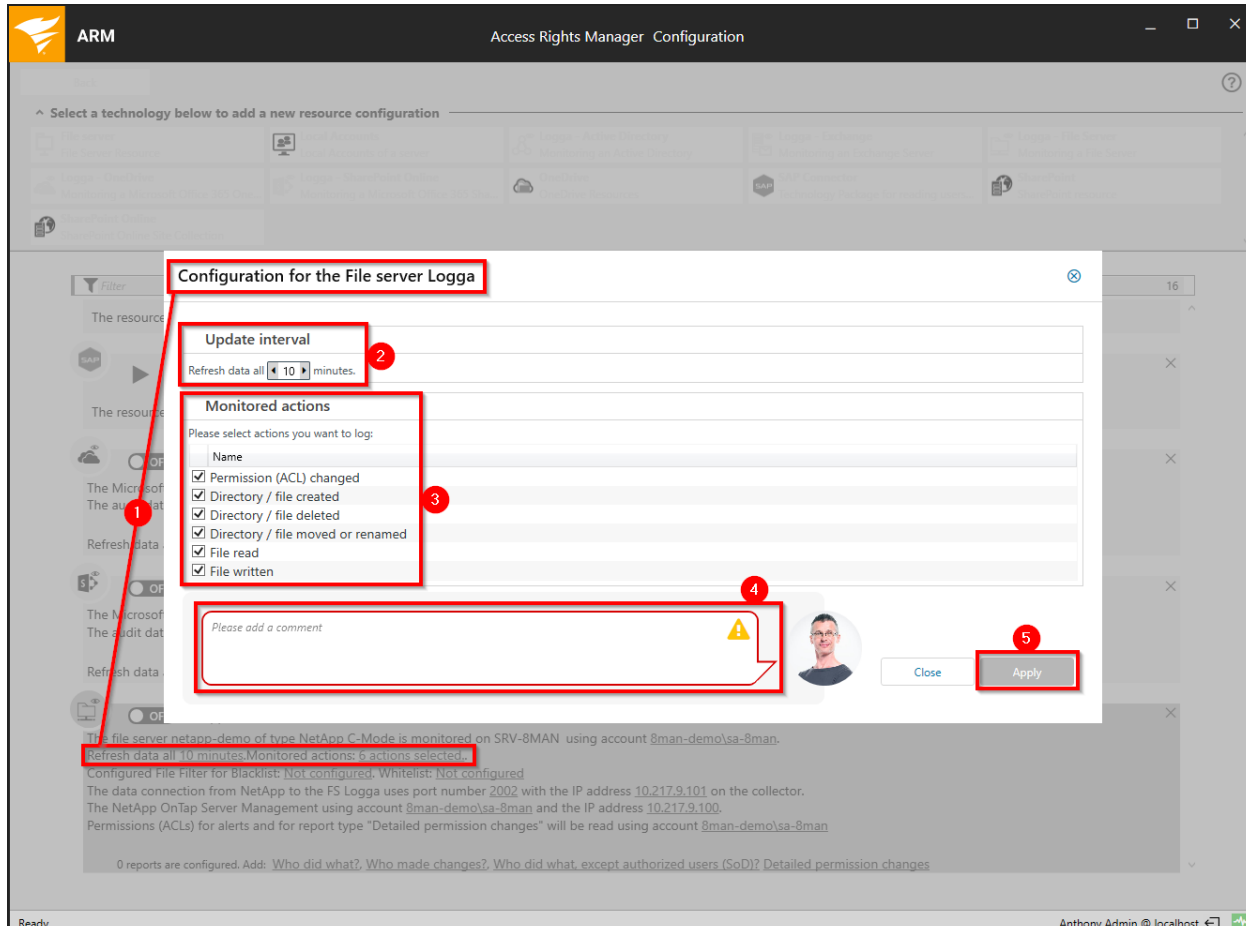
You cannot change credentials if the FS Logga is turned on.

3. You can change the name of the configuration. The name has no impact on the FS Logga function.



ARM shows you the file server name and type and the collector that is used. For NetApp and EMC you can change the account that is used for monitoring.

## Monitored actions and data refresh interval



1. Click on one of the links to open up this dialog.
2. Specify the interval at which the Logga data is written from the collector to the ARM database. The default value is 10 minutes, minimum is 1 minute, maximum 60 minutes.
3. With monitored actions you can filter what type of events are recorded. Disable not needed actions to reduce the amount of recorded data in the data base.
4. You must enter a comment.
5. Click Apply.

## File filter configuration

The screenshot displays the 'Access Rights Manager - Configuration' window. At the top, there's a 'Back' button and a 'File Server CSV Import' link. Below this is a section titled 'Select a technology below to add a new resource configuration' with a grid of options including Azure AD, Domain, Easy Connect, Exchange, File server, Local Accounts, Logga, Microsoft Dynamics NAV, OneDrive, SAP Connector, and SharePoint.

The main content area shows a filter for 'SRV-8MAN' which is currently 'OFF'. The configuration details for this filter are as follows:

- Resource: SRV-8MAN
- File server: SRV-8MAN of type Windows will be monitored on SRV-8MAN
- Refresh data: all 1 minute
- Monitored actions: 6 actions selected
- Configured File Filter for Blacklist: **Not configured**, Whitelist: **Not configured**
- Permissions (ACLs) for report type: Detailed permission changes will be read using account [not set](#)

Below the configuration details, there are three reports configured, with links to view details: [Who did what?](#), [Who made changes?](#), and [Who did what, except authorized users \(SoD\)? Detailed permission changes](#).

At the bottom, a resource URL is listed: <http://srv-8man.8man-demo.local:7047/DynamicsNAV90/WS/CRONUS%20AG/Page/>, which will be scanned [On demand](#).

Filtering is based on either the blacklist or whitelist method. Click one of the links.

1. Blacklist entries: Define for which files no events are recorded.
2. Whitelist entries: Define for which files events are recorded.
3. You can use wildcards "\*", "?" or regular expressions.
4. Delete a filter entry.
5. Add a filter entry.

The FS-Logga first applies the blacklist entries, then the whitelist entries.

The filter configuration shown here is illogical and is for demonstration purposes only.

### Record detailed permission changes

FS Logga enables you to create a report on permission changes details. File servers just deliver the event, that an ACL (access control list) has changed. To see what has changed in detail, much more effort is needed. The permissions of all monitored directories and files have to be scanned and stored in the database. After a changed ACL event has happened the permissions of the regarding object have to be read again and compared to the permissions before. This process consumes storage space and CPU power.

We strongly recommend to use this function for sensitive files and directories only. Which resources are monitored is defined by the [report configuration](#).

**i** This feature is not available for Windows failover cluster resources.

ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

<b>Azure AD</b> Azure AD accounts	<b>Domain</b> Active Directory Resource	<b>Easy Connect - CSV</b> Easy Connect - CSV resource	<b>Easy Connect - SQL</b> Easy Connect - SQL resource	<b>Exchange</b> Exchange Resource
<b>File server</b> File Server Resource	<b>Local Accounts</b> Local Accounts of a server	<b>Logga - Active Directory</b> Monitoring an Active Directory	<b>Logga - Exchange</b> Monitoring an Exchange Server	<b>Logga - File Server</b> Monitoring a File Server
<b>Logga - OneDrive</b> Monitoring a Microsoft Office 365 One...	<b>Logga - SharePoint Online</b> Monitoring a Microsoft Office 365 Sha...	<b>OneDrive</b> OneDrive Resources	<b>SAP Connector</b> Technology Package for reading users...	<b>SharePoint</b> SharePoint resource

Filter 14

**netapp-demo** OFF

The file server netapp-demo of type NetApp C-Mode is monitored on SRV-8MAN using account 8man-demo\sa-8man.  
 Refresh data all 10 minutes. Monitored actions: 6 actions selected.  
 Configured File Filter for Blacklist: Not configured. Whitelist: Not configured  
 The data connection from NetApp to the FS Logga uses port number 2002 with the IP address 10.217.9.101 on the collector.  
 The NetApp OnTap Server Management using account 8man-demo\sa-8man and the IP address 10.217.9.100.  
 Permissions (ACLs) for alerts and for report type "Detailed permission changes" will be read using account 8man-demo\sa-8man

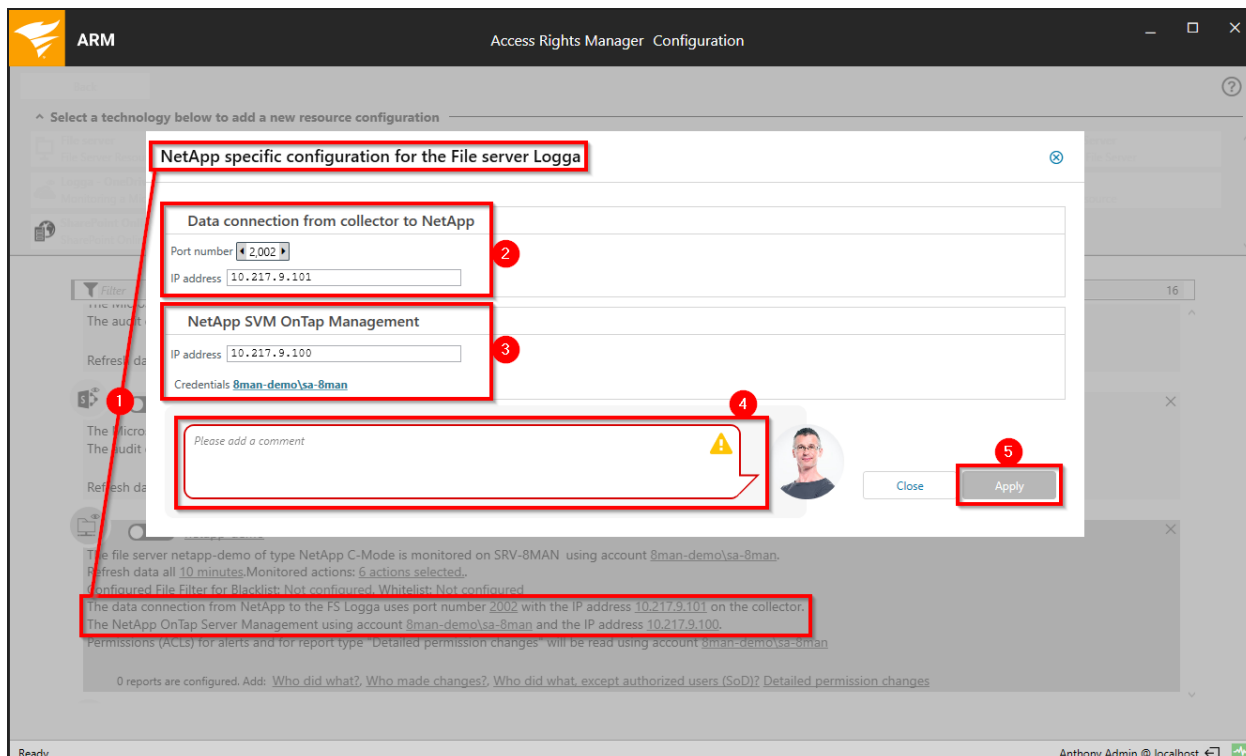
0 reports are configured. Add: Who did what?, Who made changes?, Who did what, except authorized users (SoD)? Detailed permission changes

Ready Anthony Admin @ localhost

Click on the link to enter the credentials of the account that is used for reading the ACLs.

## NetApp Clustered Data ONTAP configuration

**i** The following section applies only to NetApp Clustered Data ONTAP.



1. Click on one of the links to open up this dialog.

2. **Connection from collector to NetApp**

Enter the IP address and port of the dedicated collector. The values must match to those configured during the [Preparation of NetApp clustered data ONTAP file servers](#).

**i** The IP address and port is used to receive the events from the NetApp and therefore must be available.

3. **NetApp SVM management**

Enter the IP address of the LIF (Logical Interface) of the SVM (Storage Virtual Machine) on which the file server to be monitored is running.

The LIF to set here must match the configured one. See [Firewall configuration](#).

The credentials must match the account configured in chapter [Domain accounts](#).

4. You must enter a comment.

5. Click Apply.

## Report configuration

Events captured by the FS Logga are recorded in the ARM database. To view the information recorded, you must create a report.

Report configurations define the scope of the FS Logga. Only file server events that are happening in an area that is covered by a report configuration will be recorded. Also the event types that are recorded are defined by the report configuration.

ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

- File server: File Server Resource
- Local Accounts: Local Accounts of a server
- Logga - Active Directory: Monitoring an Active Directory
- Logga - Exchange: Monitoring an Exchange Server
- Logga - File Server: Monitoring a File Server
- Logga - OneDrive: Monitoring a Microsoft Office 365 One...
- Logga - SharePoint Online: Monitoring a Microsoft Office 365 Sha...
- OneDrive: OneDrive Resources
- SAP Connector: Technology Package for reading users...
- SharePoint: SharePoint resource
- SharePoint Online: SharePoint Online Site Collection

Filter 16

netapp-demo OFF

The file server netapp-demo of type NetApp C-Mode is monitored on SRV-8MAN using account 8man-demo\sa-8man. Refresh data all 10 minutes. Monitored actions: 6 actions selected. Configured File Filter for Blacklist: Not configured. Whitelist: Not configured. The data connection from NetApp to the FS Logga uses port number 2002 with the IP address 10.217.9.101 on the collector. The NetApp OnTap Server Management using account 8man-demo\sa-8man and the IP address 10.217.9.100. Permissions (ACLs) for alerts and for report type "Detailed permission changes" will be read using account 8man-demo\sa-8man

0 reports are configured. Add: Who did what?, Who made changes?, Who did what, except authorized users (SoD)? Detailed permission changes

Ready Anthonyv Admin @ localhost

Click one of the links to create a report configuration.

Configure the "Who did what?" report

ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

- Azure AD: Azure AD accounts
- Domain: Active Directory Resource
- Easy Connect - CSV: Easy Connect - CSV resource
- Easy Connect - SQL: Easy Connect - SQL resource
- Exchange: Exchange Resource
- File server: File Server Resource
- Local Accounts: Local Accounts of a server
- Logga - Active Directory: Monitoring an Active Directory
- Logga - Exchange: Monitoring an Exchange Server
- Logga - File Server: Monitoring a File Server
- Logga - OneDrive: Monitoring a Microsoft Office 365 One...
- Logga - SharePoint Online: Monitoring a Microsoft Office 365 Sha...
- OneDrive: OneDrive Resources
- SAP Connector: Technology Package for reading users...
- SharePoint: SharePoint resource

Filter 17

netapp-demo OFF

The file server netapp-demo of type NetApp C-Mode is monitored on SRV-8MAN using account 8man-demo\sa-8man. Refresh data all 10 minutes. Monitored actions: 6 actions selected. Configured File Filter for Blacklist: Not configured. Whitelist: Not configured. The data connection from NetApp to the FS Logga uses port number 2002 with the IP address 10.217.9.101 on the collector. The NetApp OnTap Server Management using account 8man-demo\sa-8man and the IP address 10.217.9.100. Permissions (ACLs) for alerts and for report type "Detailed permission changes" will be read using account 8man-demo\sa-8man

0 reports are configured. Add: Who did what?, Who made changes?, Who did what, except authorized users (SoD)? Detailed permission changes

SRV-8MAN OFF

The file server SRV-8MAN of type Windows will be monitored on SRV-8MAN. Refresh data all 10 minutes. Monitored actions: 6 actions selected. Configured File Filter for Blacklist: Not configured. Whitelist: Not configured. Permissions (ACLs) for alerts and for report type "Detailed permission changes" will be read using account srv-8man\localsystem

1 reports are configured. Add: Who did what?, Who made changes?, Who did what, except authorized users (SoD)? Detailed permission changes

Report "Who did what?" HR file server activity

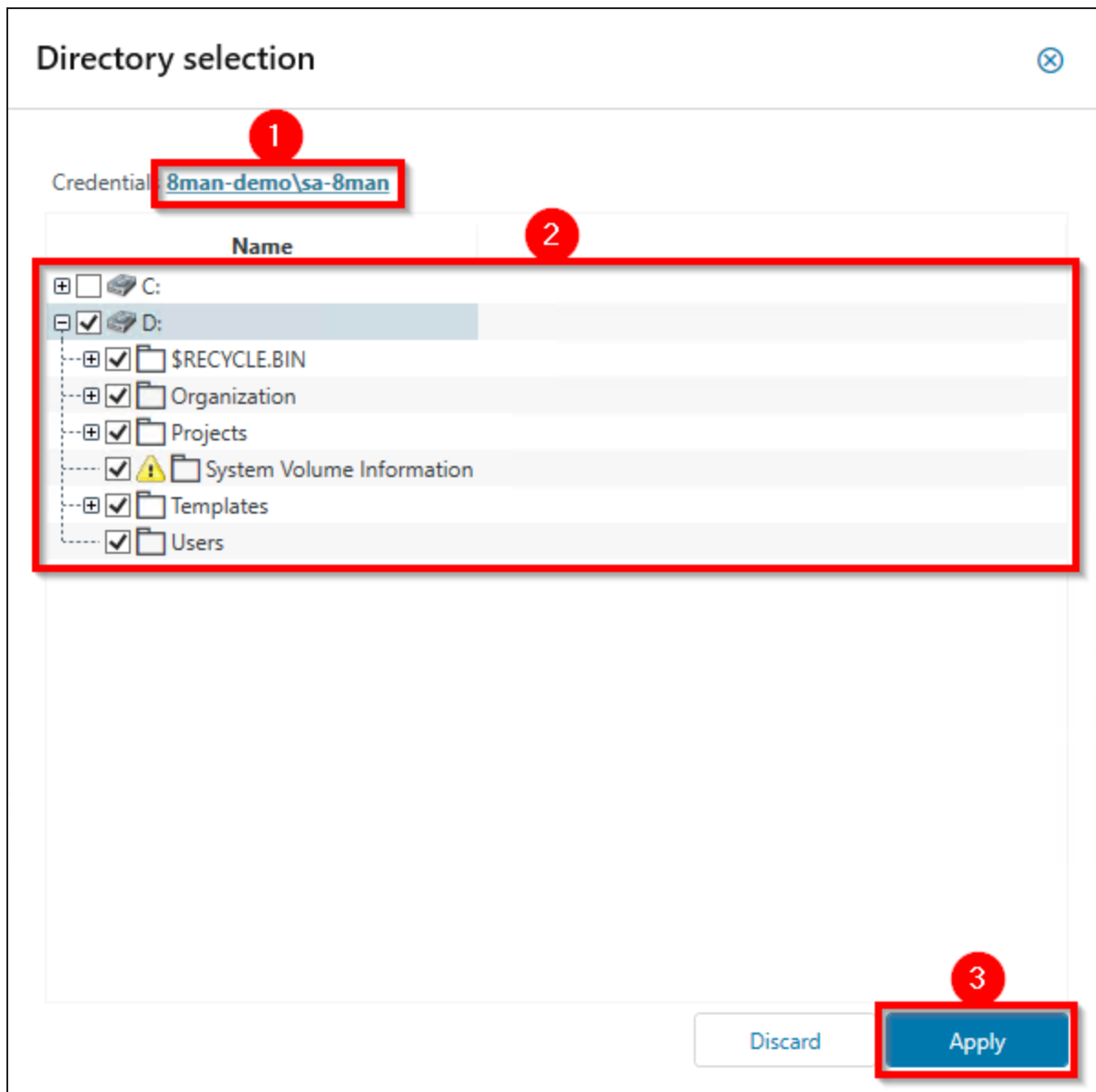
The following directories will be monitored: DA\Organization\Human Resources

emc-isilon OFF

Ready Anthonyv Admin @ localhost

1. Click "Who did what?".
2. Name the FS Logga report configuration.

3. Select the directories to be monitored.



1. Use credentials of an account that is allowed to read file server paths. On NetApp the account has to be a member of the Power User group. See [NetApp clustered](#) or [NetApp 7-mode](#).
2. Select the directories to be monitored. Subdirectories and files are included.
3. Click Apply.

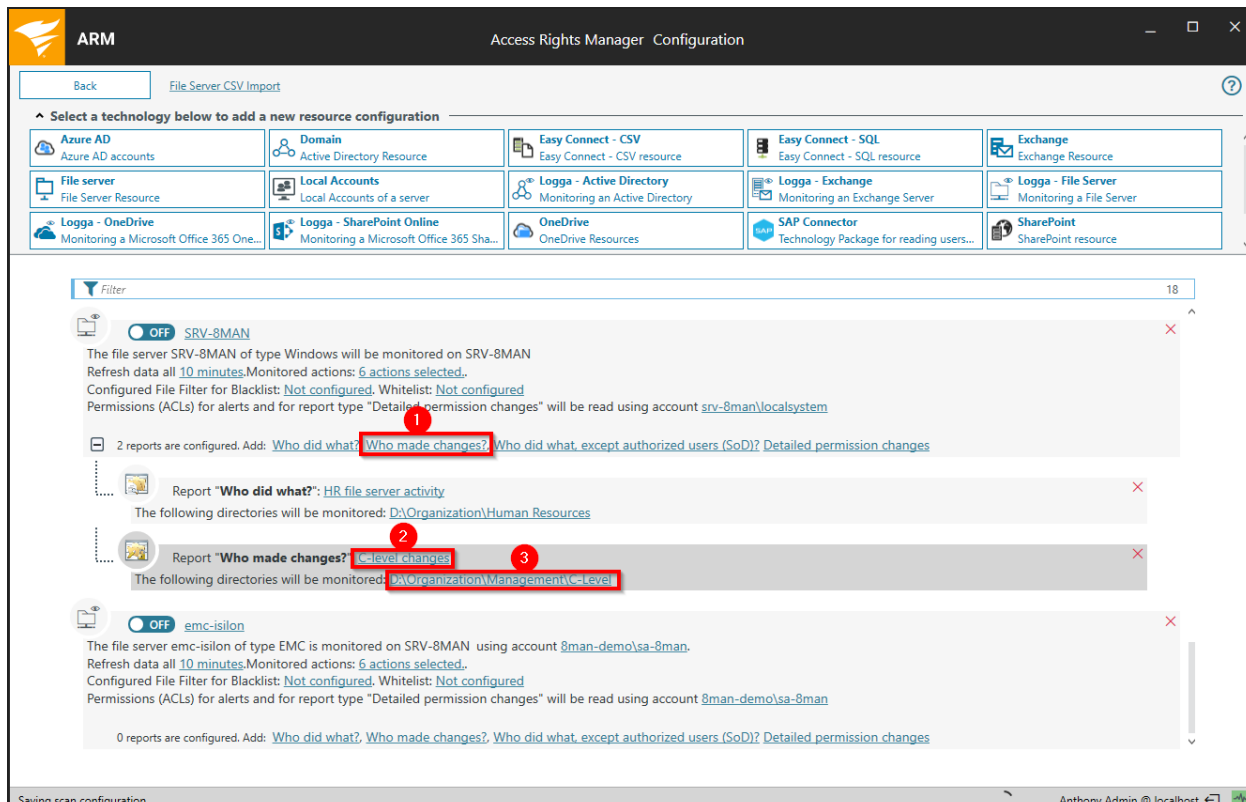
For the selected directories, subdirectories and the files in there are the following operations recorded:

- File read
- File written
- Directory or file created



- Directory or file deleted
- Directory or file moved or renamed
- ACL changed
- ACL read (switched off by default, activation in the `pnTracer.config.xml` file possible, not available for NetApp and EMC file server)

Configure the "Who made changes?" report



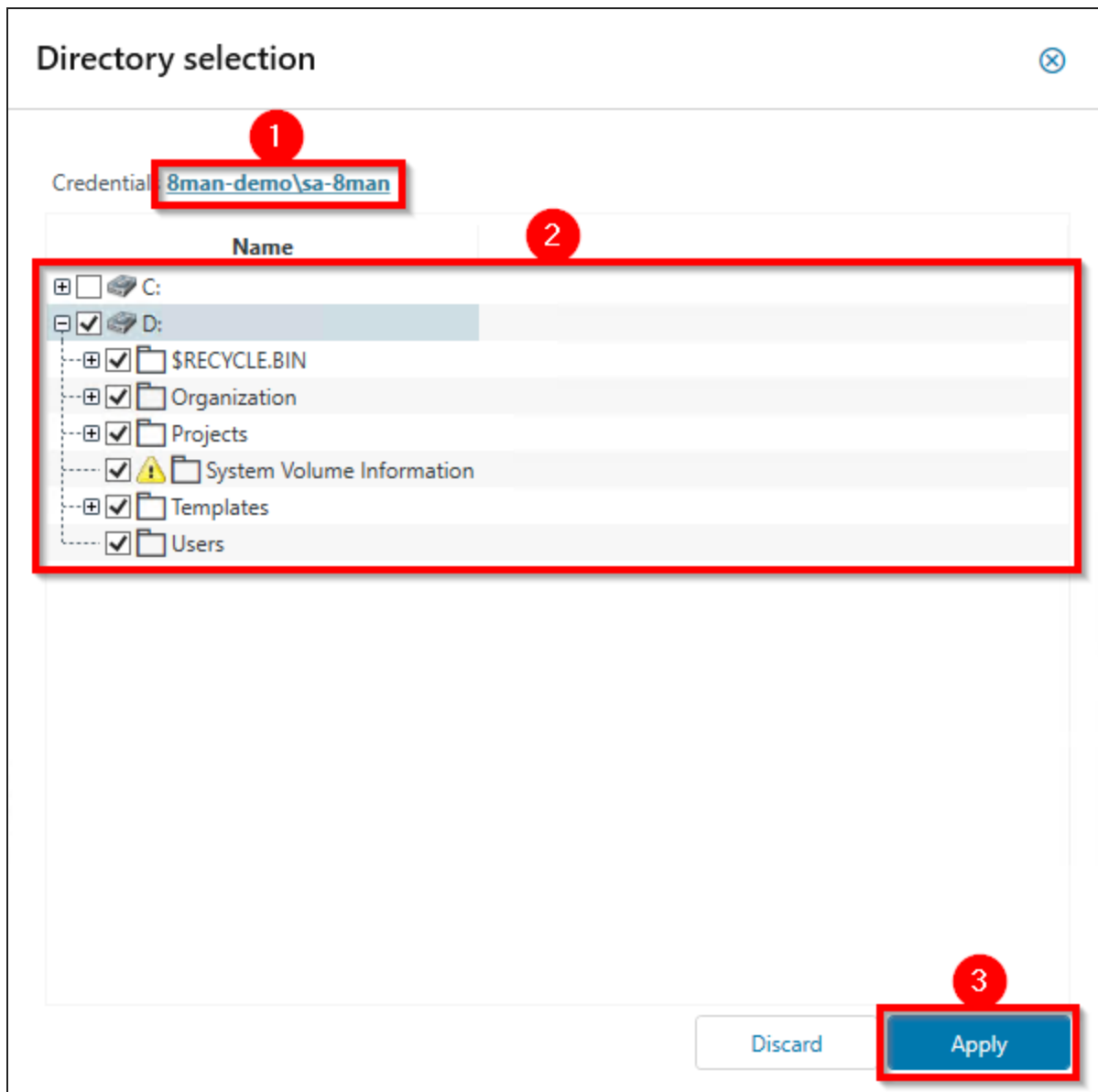
The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there's a 'File Server: CSV Import' section with a 'Back' button. Below this is a grid of technology options to add a new resource configuration, including Azure AD, Domain, Easy Connect, Exchange, File server, Local Accounts, Logga, OneDrive, and SharePoint.

The main area shows two configurations:

- SRV-8MAN:** A file server of type Windows. It is currently turned OFF. The configuration shows 2 reports are configured. One report, "Who made changes?", is highlighted with a red box and a red circle labeled '1'. Below it, another report "Who did what?" is shown. The configuration also lists monitored directories: `D:\Organization\Human Resources`.
- emc-ision:** A file server of type EMC. It is also turned OFF. The configuration shows 0 reports are configured. A report "Who made changes?" is highlighted with a red box and a red circle labeled '2'. Below it, the configuration lists monitored directories: `D:\Organization\Management\C-Level`, which is also highlighted with a red box and a red circle labeled '3'.

At the bottom of the window, it says "Saving scan configuration..." and the user is identified as "Anthony Admin @ localhost".

1. Click "Who made changes?".
2. Name the FS Logga report configuration.
3. Select the directories to be monitored.



1. Use credentials of an account that is allowed to read file server paths. On NetApp the account has to be a member of the Power User group. See [NetApp clustered](#) or [NetApp 7-mode](#).
2. Select the directories to be monitored. Subdirectories and files are included.
3. Click Apply.

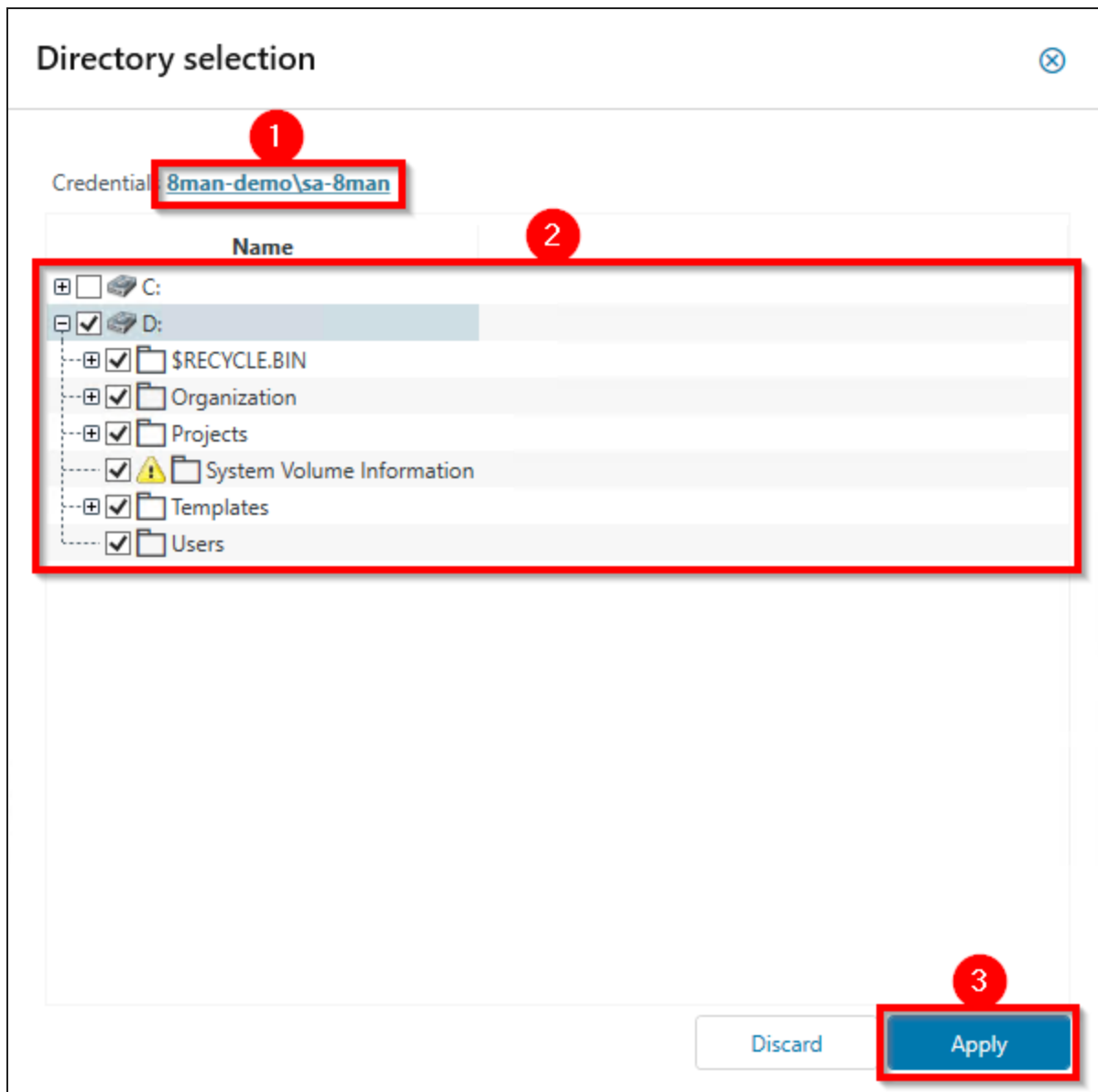
For the selected directories, subdirectories and the files in there are the following operations recorded:

- File written
- ACL changed

## Configure the "Who did what, except authorized users (SoD)?" report


The screenshot shows the ARM Configuration window for 'Access Rights Manager'. The interface includes a navigation bar with 'Back' and 'File Server CSV Import' buttons. Below this is a grid of technology options for configuration, including Azure AD, File server, Logga - OneDrive, Domain, Local Accounts, Logga - SharePoint Online, Easy Connect - CSV, Easy Connect - SQL, OneDrive, Logga - Active Directory, Logga - Exchange, SAP Connector, Exchange, Logga - File Server, and SharePoint. A filter bar shows 19 items. The main content area displays three configurations for the SRV-8MAN file server, each with a toggle switch and a red 'X' icon. The first configuration is for 'SRV-8MAN' with a report 'Who did what, except authorized users (SoD)?' selected. The second configuration is for 'HR file server activity' with a report 'Who did what?'. The third configuration is for 'emc-isilon' with a report 'Who did what, except authorized users (SoD)?'. Red boxes and numbers 1, 2, and 3 highlight the report name, the report name, and the monitored directories, respectively.

1. Click "Who did what, except authorized users (SoD)?".
2. Name the FS Logga report configuration.
3. Select the directories to be monitored.



1. Use credentials of an account that is allowed to read file server paths. On NetApp the account has to be a member of the Power User group. See [NetApp clustered](#) or [NetApp 7-mode](#).
2. Select the directories to be monitored. Subdirectories and files are included.
3. Click Apply.

For the selected directories, subdirectories and the files in there are the following operations recorded:

 The selection of authorized users and groups is done when the report is created.

- File read
- File written
- Directory or file created
- Directory or file deleted

- Directory or file moved or renamed
- ACL changed
- ACL read (switched off by default, activation in the `pnTracer.config.xml` file possible, not available for NetApp and EMC file server)

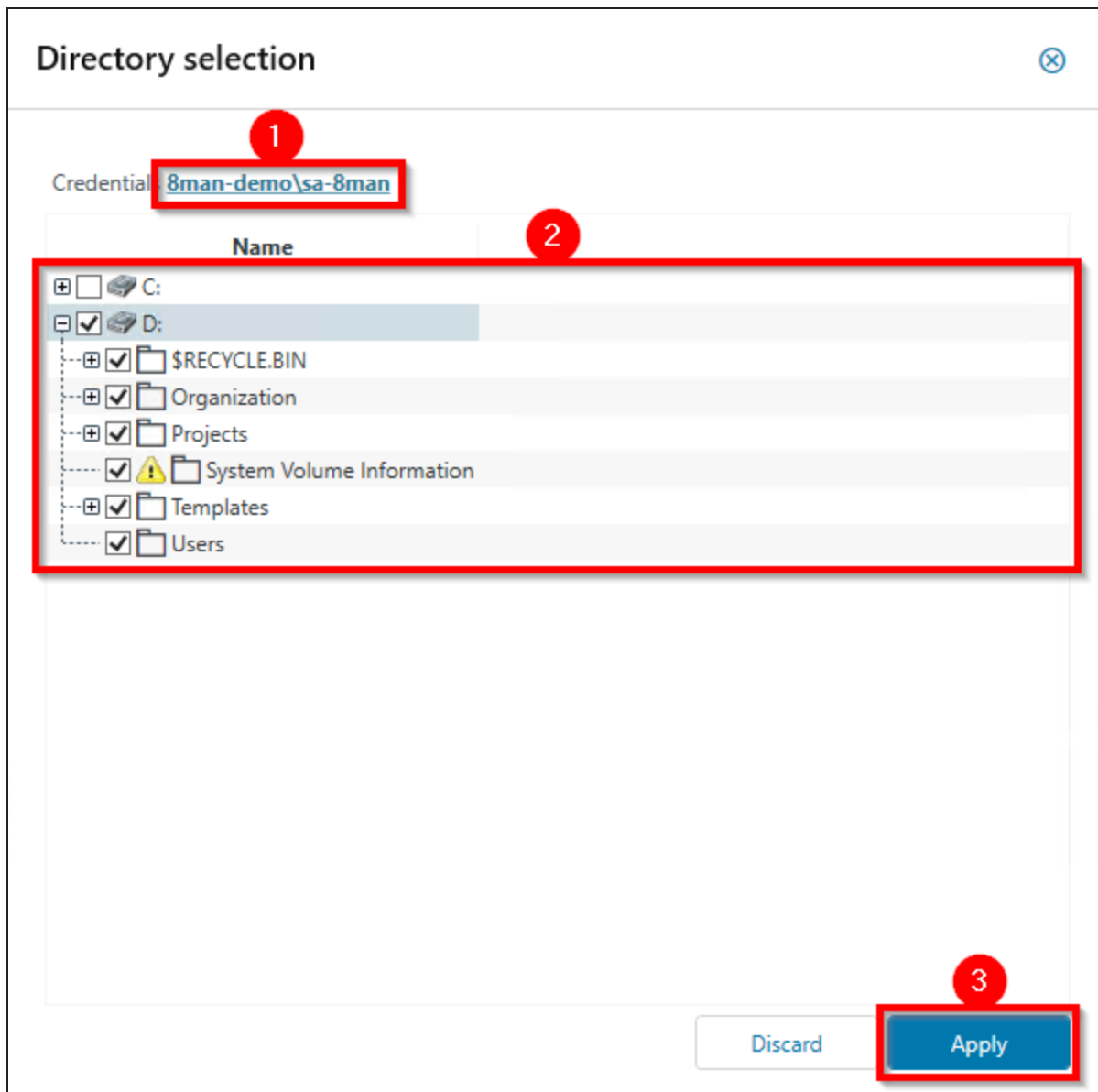
Configure the "Detailed permission changes" report

This report type is not available for Windows Failover cluster resources.

We strongly recommend to use this function for sensitive files and directories only. The extended use of this function can result in a high CPU load on the monitored file server and the assigned collector server.

The screenshot shows the ARM Configuration window for a File Server CSV Import. Under "Select a technology below to add a new resource configuration", various options like Azure AD, File server, and Logga are listed. The main area shows a configuration for SRV-8MAN with 4 reports. The "Detailed permission changes" report is highlighted, and the "DAUsers" directory is selected for monitoring. A warning message is displayed at the bottom of the report configuration.

1. Click "Detailed permission changes".
2. Name the FS Logga report configuration.
3. Select the directories to be monitored.



1. Use credentials of an account that is allowed to read file server paths. On NetApp the account has to be a member of the Power User group. See [NetApp clustered](#) or [NetApp 7-mode](#).
2. Select the directories to be monitored. Subdirectories and files are included.
3. Click Apply.

## FS Logga settings in the pnTracer.config.xml file

Filter out redundant events to reduce the amount of data collected

User actions such as browsing directories or opening a file with an application often involve multiple reads or writes. These redundant operations can be ignored by the FS-Logga if they occur within a specified time period.

You can configure:

- Enable (default) or disable the redundant events handling, separately for read and write events
- The time frame within which the FS Logga classifies events as redundant events.

## Configuration file

pnTracer.config.xml

## Computer

Collector server which is configured for the file server.

## Path

%ProgramData%\Protected Networks\8MAN\cfg

If the file does not exist, copy the "template" from the following path:

old: %ProgramFiles%\Protected Networks\8MAN\etc

new: %ProgramFiles%\solarwinds\ARM\etc

## Code

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <fileserver>
      <redundantEntriesHandling>
        <removeRead type="System.Boolean">true</removeRead>
        <removeWrite type="System.Boolean">true</removeWrite>
        <!-- maximum time-diff in seconds to ignore read or write,
default 10 -->
        <maxTimeDiffForReads
type="System.Int32">10</maxTimeDiffForReads>
        <maxTimeDiffForWrites
type="System.Int32">10</maxTimeDiffForWrites>
      </redundantEntriesHandling>
    </fileserver>
  </tracer>
```

```
</config>
```

## Possible Values

*removeRead and removeRight*

**true** - as redundant classified operations are **not** recorded (default)


**false** - all operations are recorded (not recommended)

*maxTimeDiffForReads and maxTimeDiffForWrites*


minimum **1** second

default **10** seconds

maximum **60** seconds

 After saving the pnTracer.config.xml file you have to stop and then start the FS Logga so that the changes can take effect.

Disable the default non-recording of operations for certain security IDs (SIDs)


 This section applies to Windows file servers only.

The default non-recording of operations for the following security IDs (SIDs) helps to reduce the amount of recorded data.

S-1-5-18 NT-AUTHORITY\SYSTEM

S-1-5-19 NT-AUTHORITY\ LOCAL SERVICE

S-1-5-20 NT-AUTHORITY\ NETWORK SERVICE

 The non-recording of operations for individual SIDs is not possible.

You can turn the filtering off so that all events of the listed SIDs will be recorded.

## Configuration file

pnTracer.config.xml

## Computer

Collector server which is configured for the file server.



## Path

%ProgramData%\Protected Networks\8MAN\cfg

If the file does not exist, copy the "template" from the following path:

old: %ProgramFiles%\Protected Networks\8MAN\etc

new: %ProgramFiles%\solarwinds\ARM\etc


## Code

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <windows>
      <suspendfilter type="System.Boolean">true</suspendfilter>
    </windows>
  </tracer>
</config>
```

## Possible Values

**true** - events of the listed SIDs are **not** recorded (default)

**false** - events of the listed SIDs are recorded (not recommended)

 After saving the pnTracer.config.xml file you have to stop and then start the FS Logga so that the changes can take effect.

Change the directory for temporary files of the Logga

By default temporary files of the Logga are store under

%ProgramData%\Protected Networks\8MAN\

You can change the location by editing the configuration file.

## Configuration file

pnTracer.config.xml

## Computer

Collector server which is configured for the file server.

## Path

%ProgramData%\Protected Networks\8MAN\cfg

If the file does not exist, copy the "template" from the following path:

old: %ProgramFiles%\protected-networks.com\8MAN\etc


new: %ProgramFiles%\solarwinds\ARM\etc

## Code

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <localStoragePath>E:\other\directory</localStoragePath>
  </tracer>
</config>
```

## Possible Values

Enter the local storage path.

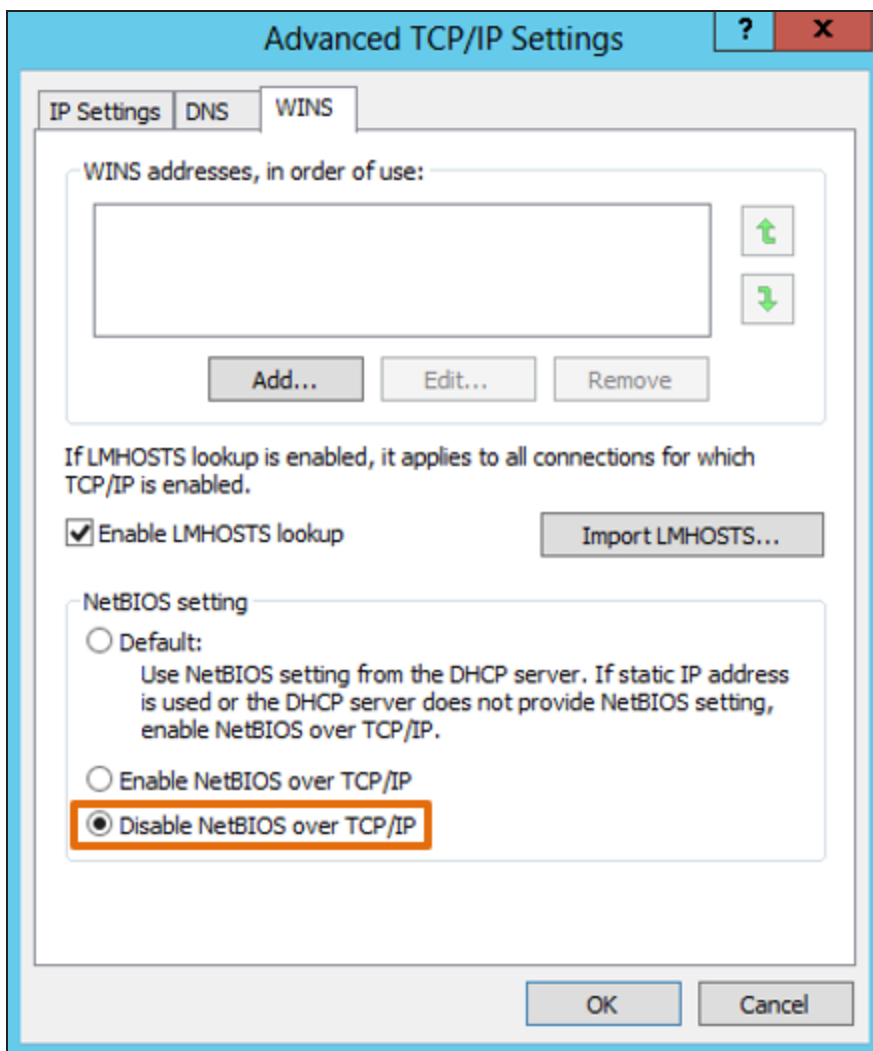
 After saving the pnTracer.config.xml file you have to stop and then start the FS Logga so that the changes can take effect.

## Troubleshooting

Problems connecting Logga and NetApp

### Disable the NetBIOS over TCP/IP setting

A possible solution to network connection problems is to disable the NetBIOS over TCP/IP setting.



On the collector server open the following dialog:

Start → Control Panel → Network and Internet → Network and Sharing Center → Change adapter settings → Ethernet properties → Internet Protocol Version 4 (TCP/IPv4) → Properties → Advanced → WINS → Disable NetBIOS over TCP/IP

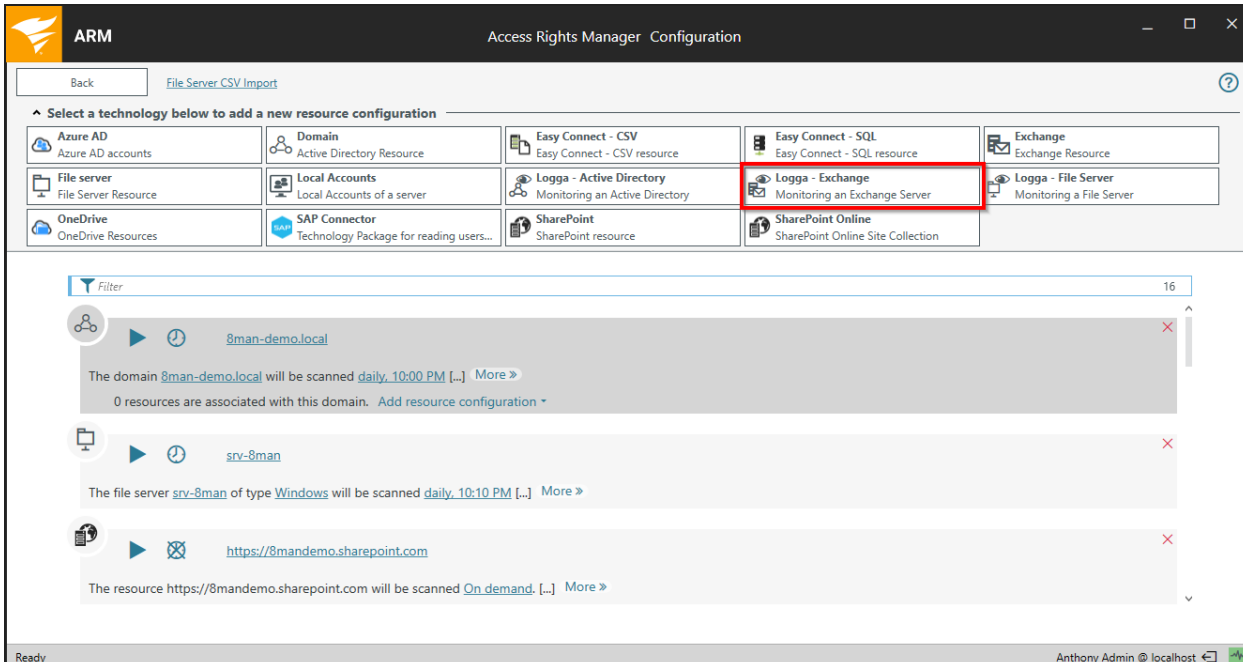
Empty report for Windows failover cluster resource

Switching file server resources from one node to another node due to cluster service shutdown or node shutdown can cause connection problems between Logga and Windows system components. This may result in a missing data delivery to the Logga.

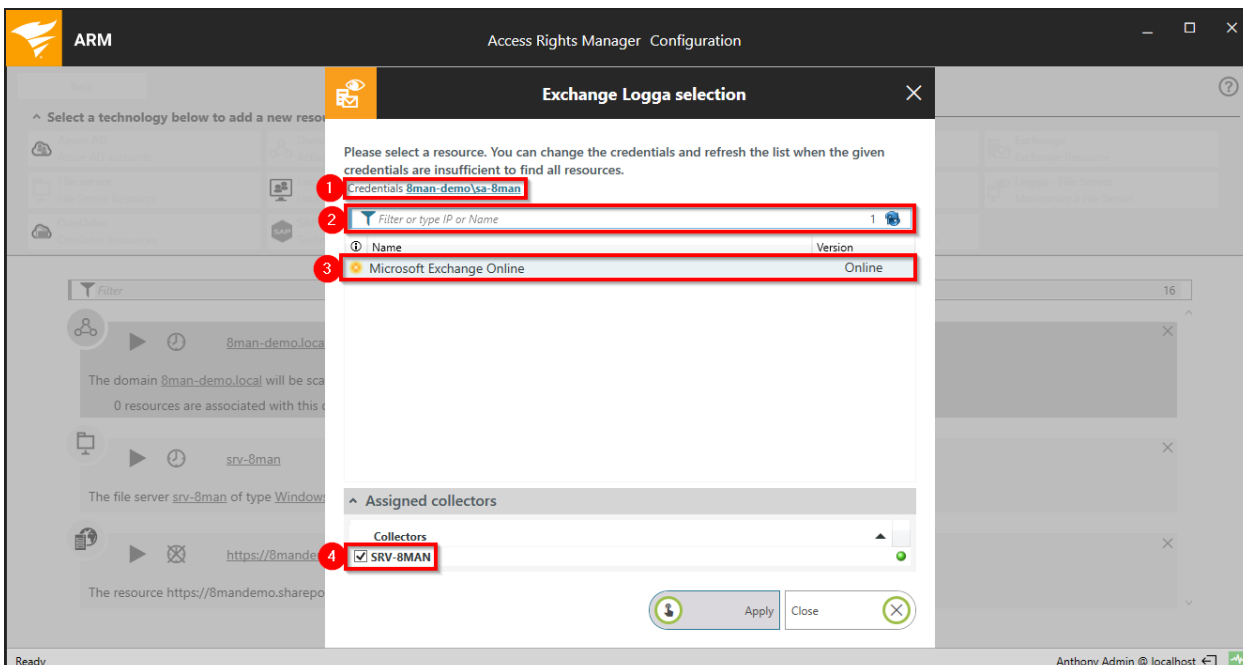
To solve this problem, turn the logga off and on again after 10 seconds.

## Configure Exchange Logga

## Add an Exchange Logga configuration



Select "Logga - Exchange".



1. Specify valid credentials for the Exchange to be monitored. See also: [required permissions](#).
2. Optional: Use the filter to find the desired server.
3. Select a server.

#### 4. Choose a collector server. You can only select one collector per Exchange.

If you have added an Exchange Logga configuration, the Logga is initially disabled. You must [enable the Exchange Logga](#) to record events.

### Customize an Exchange Logga configuration

The screenshot shows the ARM Configuration window for 'Logga - Exchange'. The configuration is currently disabled (OFF). The configuration name is '8man-demo.com'. The account used for monitoring is 'sa-8manscan@8man-demo.com'. The authentication mechanism is 'Basic'. The refresh interval is set to 1 minute.

1. Rename the configuration.
2. Change the credentials used by the Exchange Logga to read the events from the Exchange Server. See also: [required permissions](#).
3. Optional: [Put filters](#).

The screenshot shows the ARM Configuration window for 'Logga - Exchange'. The configuration is now enabled (ON). The authentication mechanism is 'Basic'. The refresh interval is set to 1 minute.


1. Choose the authentication method that must match the [PowerShell website](#) configuration.

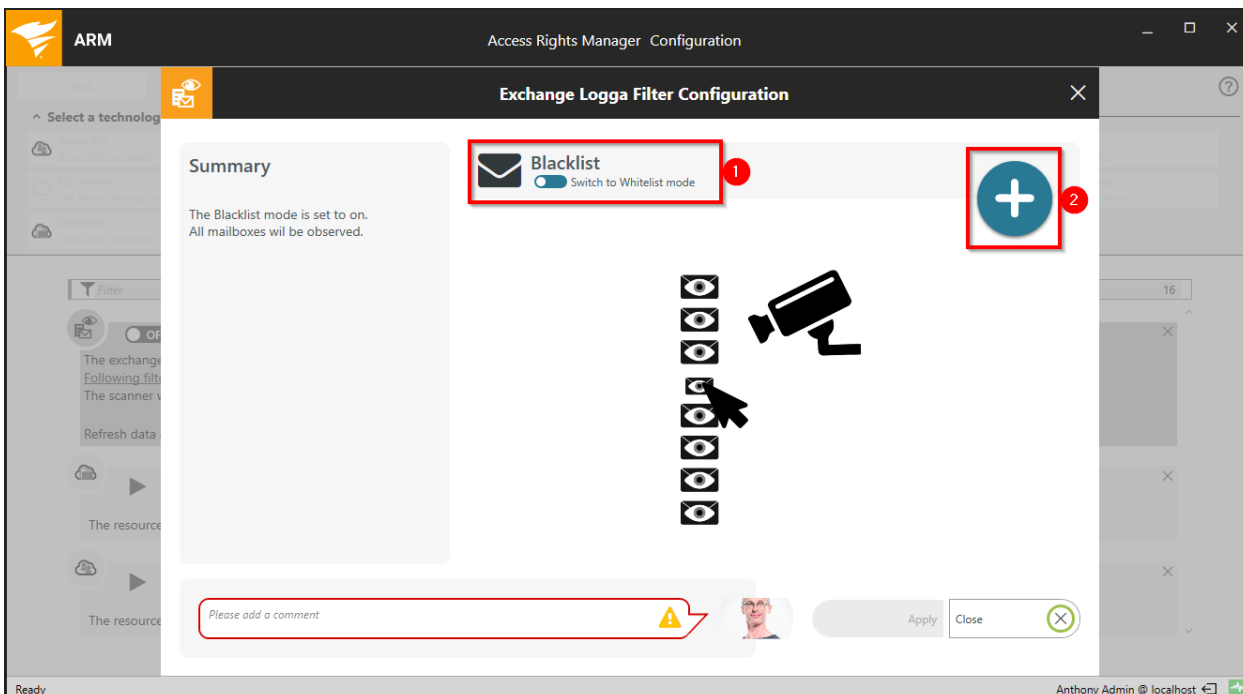
2. Set the interval for the data refresh. The events are collected by the collector and passed to the ARM server in the defined interval. Default value (recommended): 10 minutes.

## Select the mailboxes to be monitored

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there is a 'Back' button and a 'File Server CSV Import' link. Below this is a section titled 'Select a technology below to add a new resource configuration' with a grid of options including Azure AD, Domain, Easy Connect, Exchange, File server, Local Accounts, Logga, OneDrive, SAP Connector, SharePoint, and SharePoint Online. Below the grid is a 'Filter' section with a search bar containing '16'. A red box highlights an Exchange icon next to a toggle switch labeled 'OFF' and the text '8man-demo.com'. Below this, a text box contains the following information: 'The exchange server 8man-demo.com (ExchangeOnline) is monitored on SRV-8MAN using account sa-8manscan@8man-demo.com. Following filters have been set: All mailboxes will be monitored. The scanner will connect to Exchange Online by using authentication mechanism Basic. Refresh data all 1 minutes.' The status bar at the bottom shows 'Ready' and the user 'Anthony Admin @ localhost'.

1. The symbol indicates an Exchange Logga configuration.
2. Click on the link.

 By default, all mailboxes are monitored.



1. Select a mode:

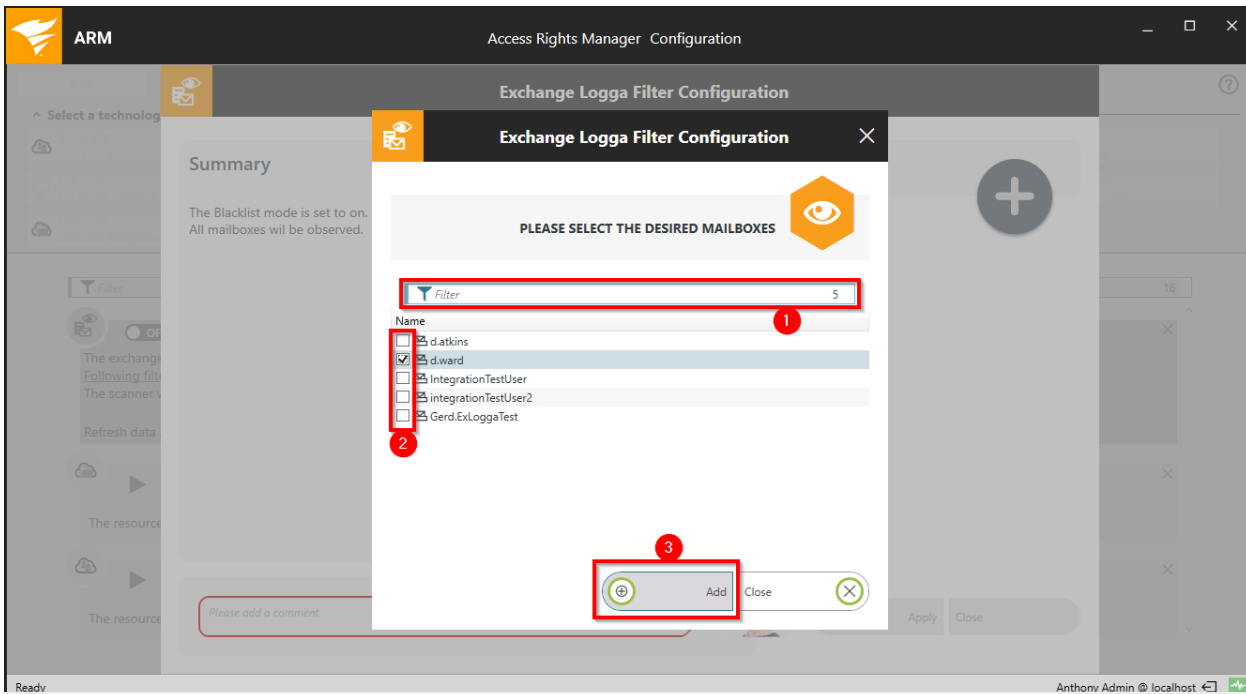
- **Blacklist**

By default all mailboxes will be monitored, including those added in the future. You specify which mailboxes are excluded from monitoring.

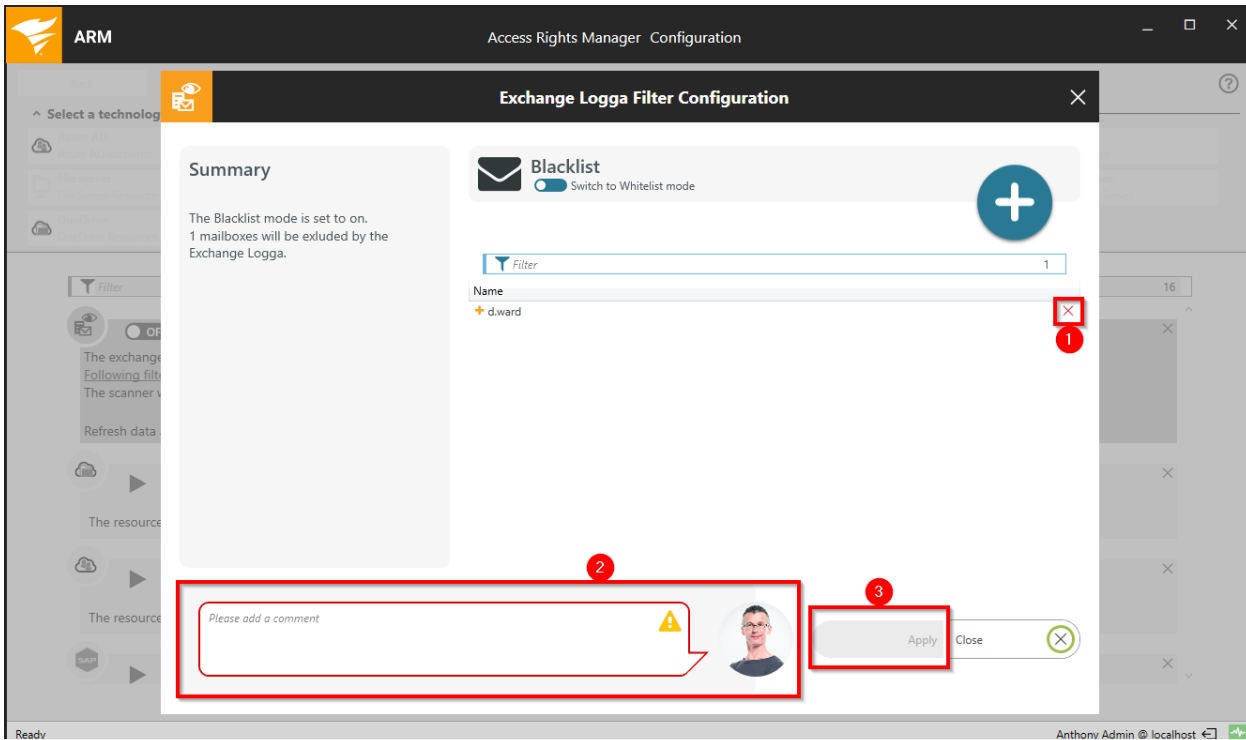
- **Whitelist**

You explicitly specify which mailboxes are monitored.

2. Click on the plus icon to add entries.



1. Use the search to find desired mailboxes.
2. Select the desired mailboxes.
3. Click "Add".



1. Click on the "X" to remove entries.



2. You must enter a comment.
3. Click "Apply" to save the configuration.

## Filter the Exchange Logga events

Filter out uninteresting events to record only relevant entries. Filtering here means that filtered out events are not recorded.

This significantly increases the overview and reduces data volumes.

### Understand the filter principles for Exchange Logga

The Exchange Logga Filter is designed as a blacklist filter. Blacklist means here: The Exchange Logga records to the maximum extent. You determine which events are not recorded (discarded).

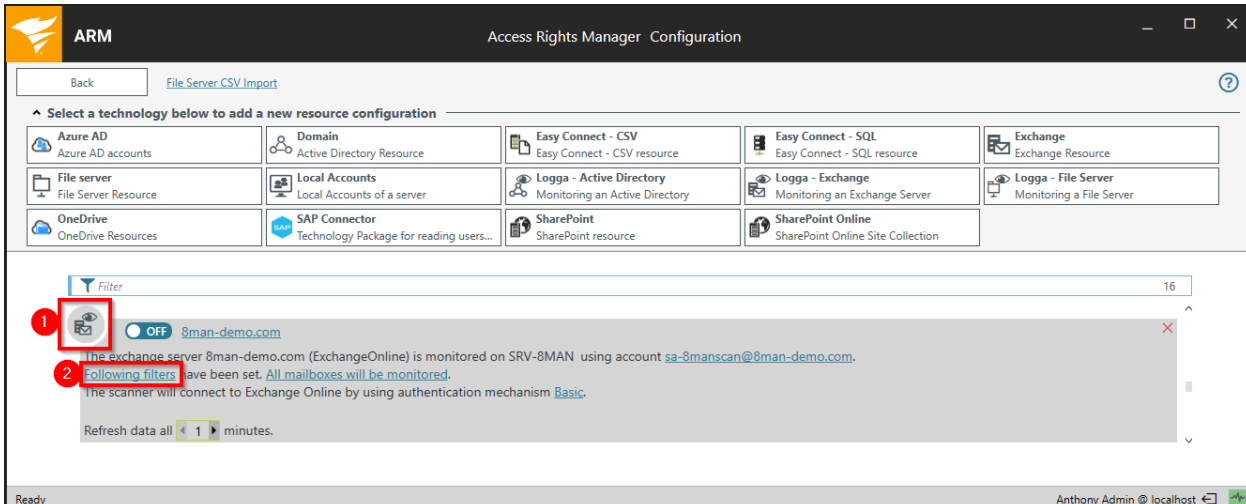
The filter criteria work additively. An event is rejected if criterion 1 or criterion 2 or criterion 3 applies, or several criteria simultaneously.

The filter criteria are not correlated with each other. The events are evaluated by the Exchange Logga one after the other according to the criteria. In the case of a hit, the event is immediately rejected and no longer checked, regardless of whether another criterion has already been evaluated or not.

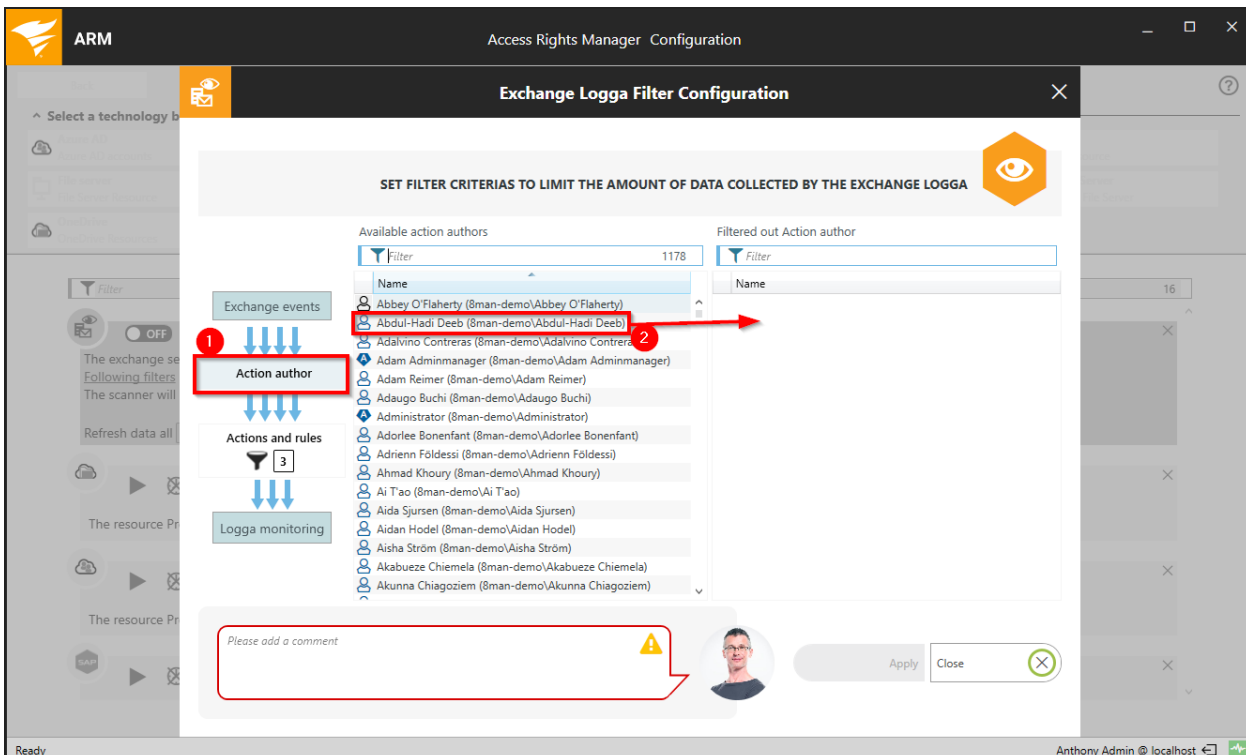
### *Example:*

If user A is configured as an "action author" filter, all changes made by him in Exchange will be discarded, even if the actions or roles he has performed are not configured as a filter.

## Configure the event filters for an Exchange Logga



1. The symbol indicates an Exchange Logga configuration.
2. Click on the link.



1. Filter events from users.
2. Select one or more users and drag them to the right column. Events triggered by these users are not recorded (blacklist).

Exchange Logga Filter Configuration

SET FILTER CRITERIAS TO LIMIT THE AMOUNT OF DATA COLLECTED BY THE EXCHANGE LOGGA

	Administrator	Delegate	Owner	
select all / deselect all				
Copy				
Create				
FolderBind	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
HardDelete				
MailboxLogin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
MessageBind		<input type="checkbox"/>	<input type="checkbox"/>	
Move				
MoveToDeletedItems				
SendAs			<input type="checkbox"/>	
SendOnBehalf				
SoftDelete				
Update				

Please add a comment

Apply Close

1. Filter events based on specific login types or actions.
2. Actions (lines) of login types (columns) with an eye icon are recorded.
3. You must enter a comment to save changes to the filter settings.

For more information about the monitored events, please see [Mailbox audit logging in Exchange Server](https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/mailbox-audit-logging?view=exchserver-2019) (© 2020 Microsoft, <https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/mailbox-audit-logging?view=exchserver-2019>, obtained on January 29, 2020).

## Enable or disable the Exchange Logga

The screenshot shows the ARM Configuration window for version 9.1.181.0. The interface includes a navigation bar with 'Back' and 'File\_Server.CSV Import' buttons. Below is a grid of technology options for adding a new resource configuration. The 'Logga - Exchange' option is selected, showing details for the server '8man-demo.com'. A red box highlights the Exchange icon (1) and the 'OFF' toggle switch (2). The configuration details include the account 'sa-8manscan@8man-demo.com' and a refresh interval of 1 minute.

1. The symbol indicates an Exchange Logga configuration.
2. In the desired Exchange Logga configuration, click the switch to enable or disable the Exchange Logga.

You must enter a comment to enable or disable the Exchange Logga.

**i** AD Logga events are stored by default for 30 days. See [Configure storage of scans settings](#).

## Configure OneDrive Logga

**!** To enable the OneDrive Logga, you must have completed the [preparation for Office 365 integration](#) in the Azure Portal.

ARM Access Rights Manager Configuration

Server Status License Information	Jobs Summary	Collectors Configuration
Logged in users: 1	91 Scans 7 Reports	1 Connected 1 Configured in Total
Licensed Active user accounts: 1166	7 Scheduled 293 Succeeded	0 Executing 0 Failed

Filter

- Scans**  
Resource Configurations, Logga, File Server CSV Import
- Open Order**  
Open Order Resource Descriptions
- User Management**  
User Management, Role Management
- Data Owner**  
Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**  
License Information, Server Status
- Jobs Overview**  
Job Status, Job Categories
- Change Configuration**  
Common Change Settings, Technology-specific Change Configurations
- Scripting**  
Scripting configuration for change actions
- Views & Reports**  
Views & Reports, Blacklist for Views & Reports
- Server**  
Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**  
ARM Server, SQL Server, Configuration Status

Ready Anthony Admin @ localhost

Start the ARM configuration application and click "Scans".

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there is a 'Back' button and a 'File Server CSV Import' link. Below this is a section titled 'Select a technology below to add a new resource configuration'. This section contains a grid of 15 options:

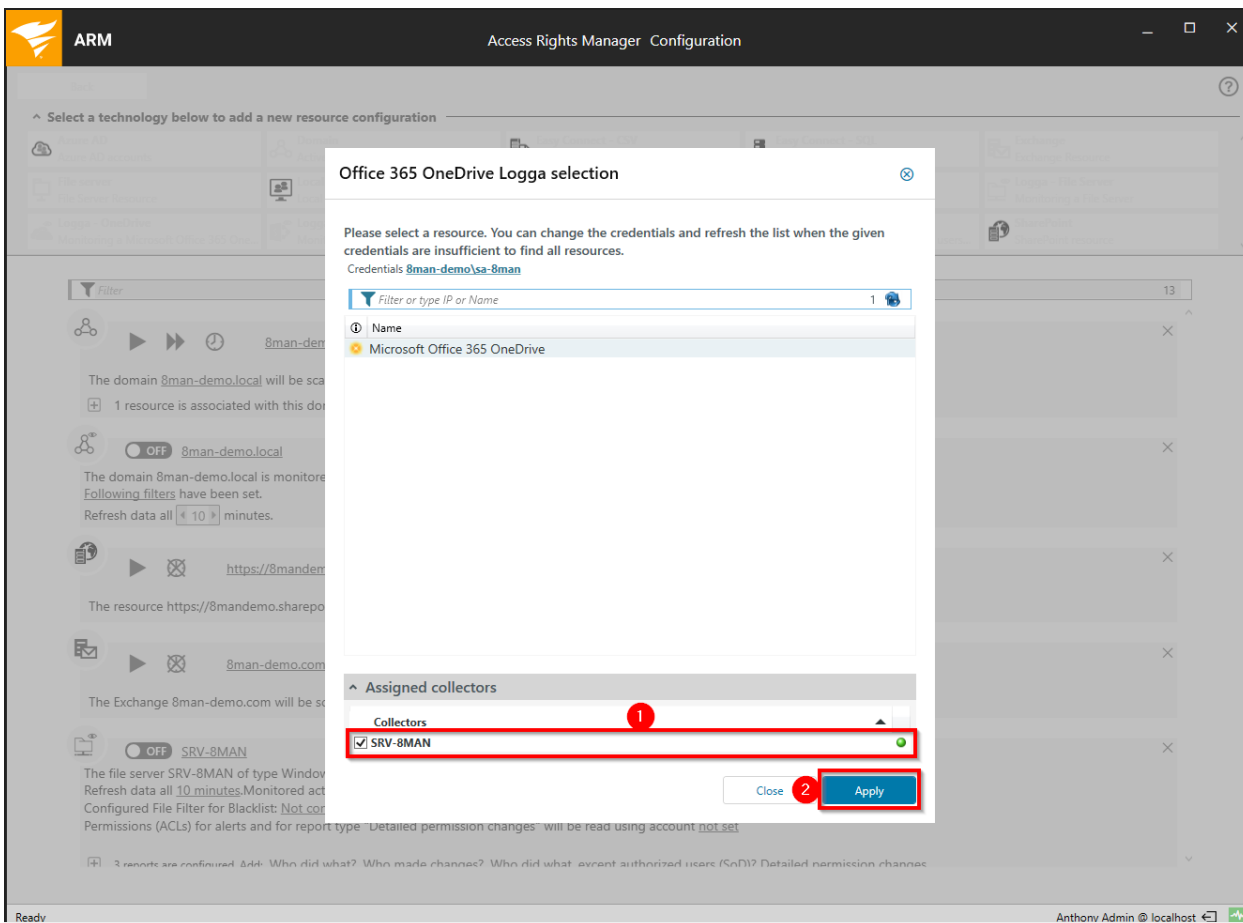
- Azure AD (Azure AD accounts)
- Domain (Active Directory Resource)
- Easy Connect - CSV (Easy Connect - CSV resource)
- Easy Connect - SQL (Easy Connect - SQL resource)
- Exchange (Exchange Resource)
- File server (File Server Resource)
- Local Accounts (Local Accounts of a server)
- Logga - Active Directory (Monitoring an Active Directory)
- Logga - Exchange (Monitoring an Exchange Server)
- Logga - File Server (Monitoring a File Server)
- Logga - OneDrive (Monitoring a Microsoft Office 365 OneDrive Resource)** - This option is highlighted with a red box.
- Logga - SharePoint (Monitoring a Microsoft Office 365 SharePoint Resource)
- OneDrive (OneDrive Resources)
- SAP Connector (Technology Package for reading users...)
- SharePoint (SharePoint resource)

Below the grid is a list of existing configurations for the domain '8man-demo.local'. Each entry includes a play button, a refresh icon, and a close button. The entries are:

- 8man-demo.local: The domain 8man-demo.local will be scanned daily, 10:00 PM [...]. 1 resource is associated with this domain.
- 8man-demo.local: The domain 8man-demo.local is monitored on SRV-8MAN using account 8man-demo\sa-8man. Refresh data all 10 minutes.
- https://8mandemo.sharepoint.com: The resource https://8mandemo.sharepoint.com will be scanned On demand [...].
- 8man-demo.com: The Exchange 8man-demo.com will be scanned On demand [...].
- SRV-8MAN: The file server SRV-8MAN of type Windows will be monitored on SRV-8MAN. Refresh data all 10 minutes. Monitored actions: 6 actions selected. Configured File Filter for Blacklist: Not configured. Whitelist: Not configured. Permissions (ACLs) for alerts and for report type "Detailed permission changes" will be read using account not set.

At the bottom of the window, the status bar shows 'Ready' and the user 'Anthony Admin @ localhost'.

Select "Logga - OneDrive".



1. Select a collector server. Note, that the collector server needs internet access to pull OneDrive events.
2. Click "Apply".

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there's a 'Back' button and a 'File\_Server\_CSV Import' link. Below that, a section titled 'Select a technology below to add a new resource configuration' displays a grid of various monitoring technologies like Azure AD, Domain, Easy Connect, Exchange, File server, Local Accounts, Logga, OneDrive, SAP Connector, and SharePoint. The main area shows a list of 14 resources. The resources listed are: 8man-demo.com (ExchangeOnline), Protected Networks GmbH (two entries), Q11, and Microsoft Office 365 OneDrive. The OneDrive resource is highlighted with a red box and has a warning icon. Red numbers 1-4 are placed on the interface: 1 points to the resource title, 2 to the scan frequency, 3 to the warning icon, and 4 to the 'not set' Client ID field.

1. Newly added resources are always at the bottom.
2. You have created a OneDrive Logga configuration.
3. The warning indicates that not all required settings are made.
4. Click one of the links.



ARM Access Rights Manager Configuration

Select a technology below to add a new resource configuration

Filter

8man-demo.com

The exchange server 8man-demo.com (Exchange) has been set. Following filters have been set. All mailboxes will be scanned. The scanner will connect to Exchange Online by using the following filters.

Refresh data all 10 minutes.

Protected Networks GmbH

The resource Protected Networks GmbH will be scanned on demand. [...]

Q11

The resource Q11 will be scanned on demand. [...]

Microsoft Office 365 OneDrive

The Microsoft Office 365 OneDrive 8man-demo.com with Client ID 51ee871b-f9ca-47c2-b0b1-c898b9bd1be2 is monitored on SRV-8MAN. The audit data will be requested in an interval of 60 seconds.

Refresh data all 10 minutes.

Ready Anthony Admin @ localhost

1. Enter the tenant, for example "mycompany.com".
2. Enter the application ID.
3. Enter the client secret.

**i** The application ID and the client secret were created during the [preparation for Office 365 integration](#).

4. Determine the interval for pulling events from OneDrive to the collector server.
5. You must enter a comment.
6. Click "Apply".

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there is a 'Back' button and a 'File Server CSV Import' link. Below this is a section titled 'Select a technology below to add a new resource configuration' with a grid of options including Azure AD, Domain, Easy Connect - CSV, Easy Connect - SQL, Exchange, File server, Local Accounts, Logga - Active Directory, Logga - Exchange, Logga - File Server, Logga - OneDrive, Logga - SharePoint, OneDrive, SAP Connector, and SharePoint. The main area displays a list of configurations for the domain '8man-demo.com'. The 'Logga - OneDrive' configuration is highlighted with a red box and numbered 1. The 'Refresh data all' interval is set to 10 minutes and is also highlighted with a red box and numbered 2. The 'Logga - OneDrive' configuration is currently turned off, indicated by a red 'X' icon and a red circle with the number 3.

1. Give the OneDrive Logga configuration a new name.
2. Specify the interval at which the Logga data is written from the collector to the ARM database.
3. Turn on the Logga.

**i** Please note that when you enable logging for the first time, Microsoft states that it can take up to 12 hours for the first events to be recorded.

## Configure SharePoint Online Logga

**!** To enable the SharePoint Online Logga, you must have completed the [preparation for Office 365 integration](#) in the Azure Portal.

**Server Status**  
License Information

Logged in users: 1

Licensed  
Active user accounts: 1166

**Jobs**  
Summary

91 Scans 7 Reports	69 Changes 133 More
7 Scheduled 293 Succeeded	0 Executing 0 Failed

**Collectors**  
Configuration

1 Connected  
1 Configured in Total

All Collectors are Operational

Filter

**Scans**  
Resource Configurations, Logga, File Server CSV Import

**Open Order**  
Open Order Resource Descriptions

**User Management**  
User Management, Role Management

**Data Owner**  
Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings

**License**  
License Information, Server Status

**Jobs Overview**  
Job Status, Job Categories

**Change Configuration**  
Common Change Settings, Technology-specific Change Configurations

**Scripting**  
Scripting configuration for change actions

**Views & Reports**  
Views & Reports, Blacklist for Views & Reports

**Server**  
Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging

**Basic Configuration**  
ARM Server, SQL Server, Configuration Status

Ready Anthony Admin @ localhost

Start the ARM configuration application and click "Scans".

ARM Access Rights Manager Configuration

Back File Server CSV Import

Select a technology below to add a new resource configuration

Azure AD Azure AD accounts	Domain Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource
File server File Server Resource	Local Accounts Local Accounts of a server	Logga - Active Directory Monitoring an Active Directory	Logga - Exchange Monitoring an Exchange Server	Logga - File Server Monitoring a File Server
Logga - OneDrive Monitoring a Microsoft Office 365 One...	Logga - SharePoint Monitoring a Microsoft Office 365 Sha...	OneDrive OneDrive Resources	SAP Connector Technology Package for reading users...	SharePoint SharePoint resource

Filter 14

8man-demo.local

The domain 8man-demo.local will be scanned daily, 10:00 PM [...] More »

1 resource is associated with this domain. Add resource configuration +

8man-demo.local

The domain 8man-demo.local is monitored on SRV-8MAN using account 8man-demo\sa-8man. Following filters have been set. Refresh data all 10 minutes.

https://8mandemo.sharepoint.com

The resource https://8mandemo.sharepoint.com will be scanned On demand, [...] More »

8man-demo.com

The Exchange 8man-demo.com will be scanned On demand [...] More »

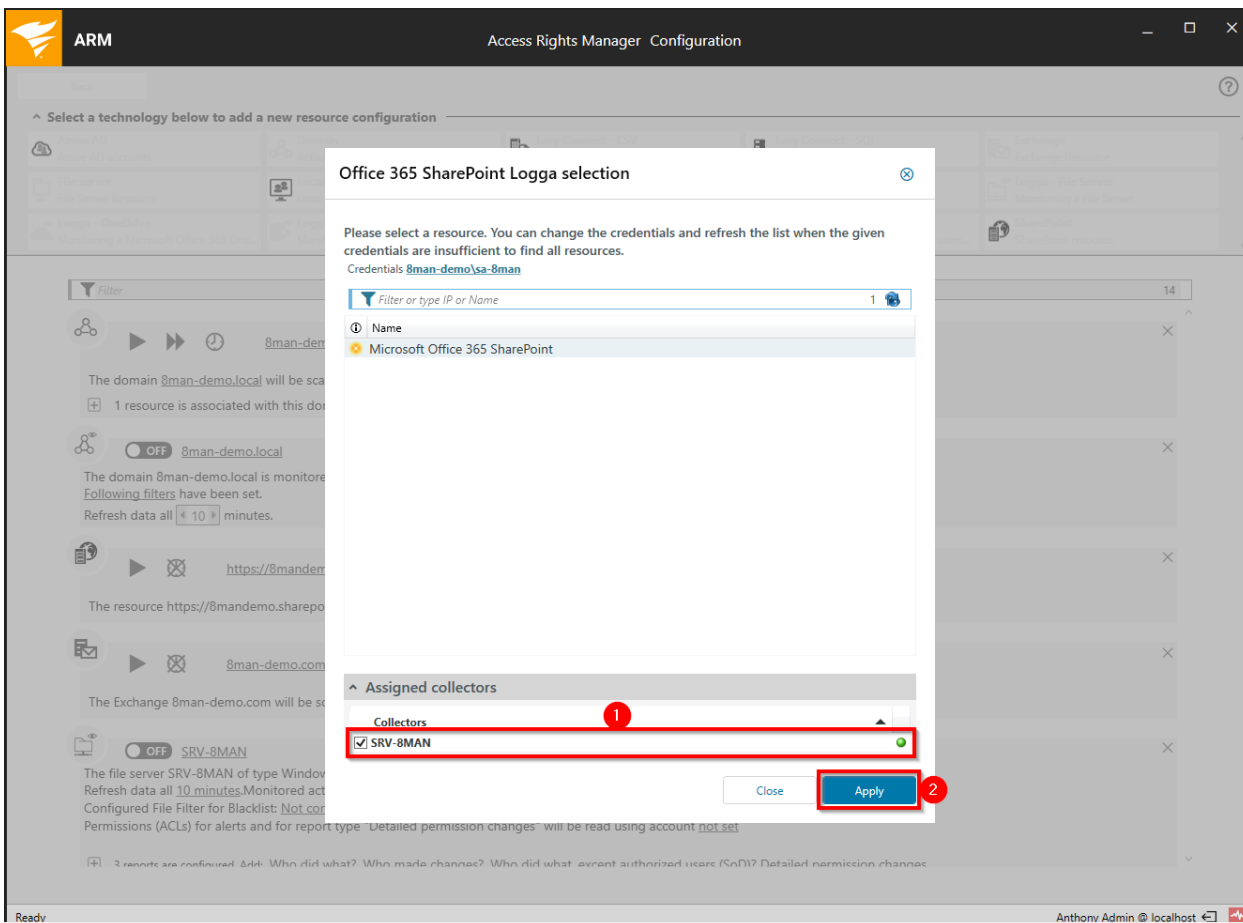
SRV-8MAN

The file server SRV-8MAN of type Windows will be monitored on SRV-8MAN Refresh data all 10 minutes. Monitored actions: 6 actions selected. Configured File Filter for Blacklist: Not configured. Whitelist: Not configured Permissions (ACLs) for alerts and for report type "Detailed permission changes" will be read using account not set

3 reports are configured. Add: Who did what? Who made changes? Who did what - event authorized users (SoD)? Detailed permission changes

Ready Anthony Admin @ localhost

Select "Logga - SharePoint Online".



1. Select a collector server. Note, that the collector server needs internet access to pull SharePoint Online events.
2. Click "Apply".

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there is a 'Back' button and a 'File\_Server\_CSV Import' link. Below this is a section titled 'Select a technology below to add a new resource configuration' with a grid of options including Azure AD, Domain, Easy Connect - CSV, Easy Connect - SQL, Exchange, File server, Local Accounts, Logga - Active Directory, Logga - Exchange, Logga - File Server, Logga - OneDrive, Logga - SharePoint, OneDrive, SAP Connector, and SharePoint.

The main area displays a list of resources. The resource 'Microsoft Office 365 SharePoint' is highlighted with a red box. It has a warning icon and a message: 'The Microsoft Office 365 SharePoint [not set] with Application ID [not set] is monitored on SRV-8MAN. The audit data will be requested in an interval of 60 seconds.' Red annotations include: 1. A circle around the resource name, 2. A circle around the 'not set' text, 3. An arrow pointing to the warning icon, and 4. A circle around a link in the message.

1. Newly added resources are always at the bottom.
2. You have created a SharePoint Online Logga configuration.
3. The warning indicates that not all required settings are made.
4. Click one of the links.

ARM Access Rights Manager Configuration

Select a technology below to add a new resource configuration

Filter

8man-demo.com

The exchange server 8man-demo.com (Exchange) Following filters have been set. All mailboxes will be scanned. The scanner will connect to Exchange Online by using the following filters.

Refresh data all 10 minutes.

Protected Networks GmbH

The resource Protected Networks GmbH will be scanned on demand. [...]

Protected Networks GmbH

The resource Protected Networks GmbH will be scanned on demand. [...]

Q11

The resource Q11 will be scanned on demand. [...]

Microsoft Office 365 SharePoint

The Microsoft Office 365 SharePoint not set with Application ID not set is monitored on SRV-8MAN. The audit data will be requested in an interval of 60 seconds.

Refresh data all 10 minutes.

Ready Anthony Admin @ localhost

1. Enter the tenant, for example "mycompany.com".
2. Enter the application ID.
3. Enter the client secret.

**i** The application ID and the client secret were created during the [preparation for Office 365 integration](#).

4. Determine the interval for pulling events from SharePoint Online to the collector server.
5. You must enter a comment.
6. Click "Apply".

1. Give the SharePoint Online Logga configuration a new name.
2. Specify the interval at which the Logga data is written from the collector to the ARM database.
3. Turn on the Logga.

**i** Please note that when you enable logging for the first time, Microsoft states that it can take up to 12 hours for the first events to be recorded.

## Scan local accounts

ARM is able to read local accounts of computers (and not just file servers).



## Adding local accounts scans

The screenshot shows the 'Access Rights Manager Configuration' window. In the 'Select a technology below to add a new resource configuration' section, the 'Local Accounts' option is highlighted with a red box. Below this, the configuration for the domain '8man-demo.local' is shown, including a scan schedule of 'daily, 10:00 PM' and a list of filters.

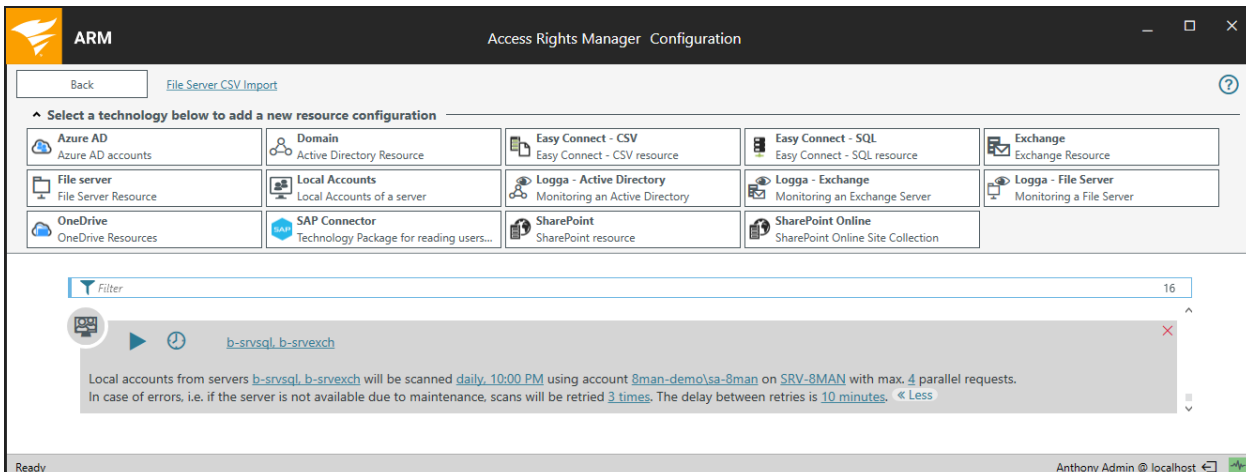
Select "Local Accounts".

The 'Local Accounts selection' dialog box is open, showing a list of file servers to be scanned for local accounts. The list includes the following entries:

Name	Domain
<input type="checkbox"/> srv-8man	8man-demo.local
<input type="checkbox"/> b-wsmeyer	8man-demo.local
<input type="checkbox"/> b-wswillson	8man-demo.local
<input checked="" type="checkbox"/> b-srvsql	8man-demo.local
<input checked="" type="checkbox"/> b-srvexch	8man-demo.local

The 'Assigned collectors' section shows 'Collectors' and 'SRV-8MAN' selected. The 'Apply' and 'Close' buttons are visible at the bottom of the dialog.

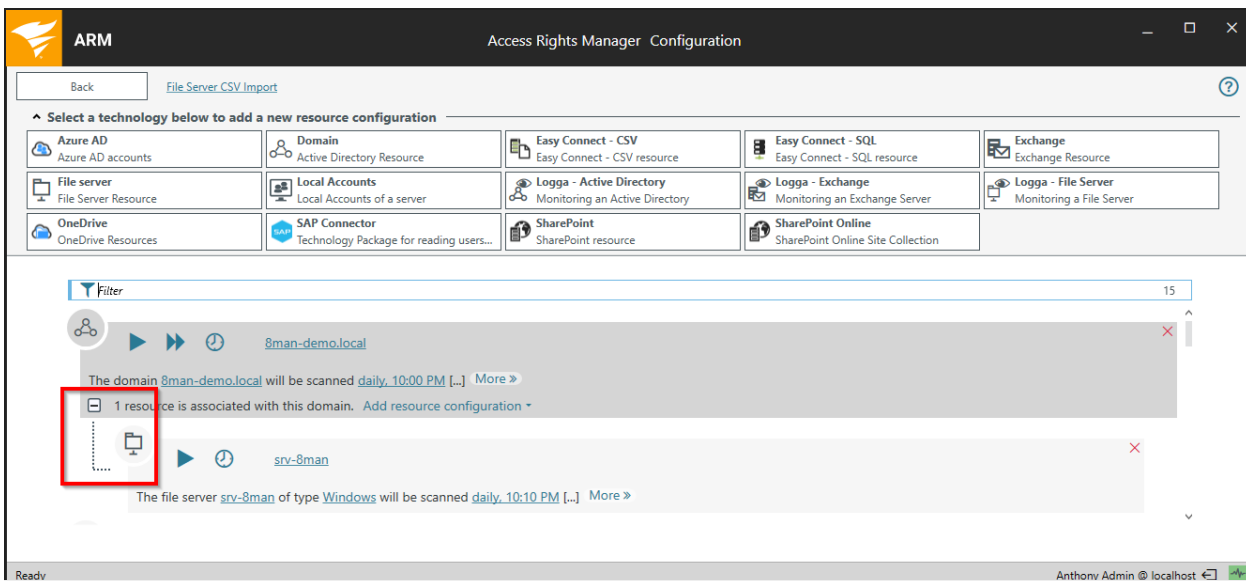
Select the computers for which you want to read local accounts.



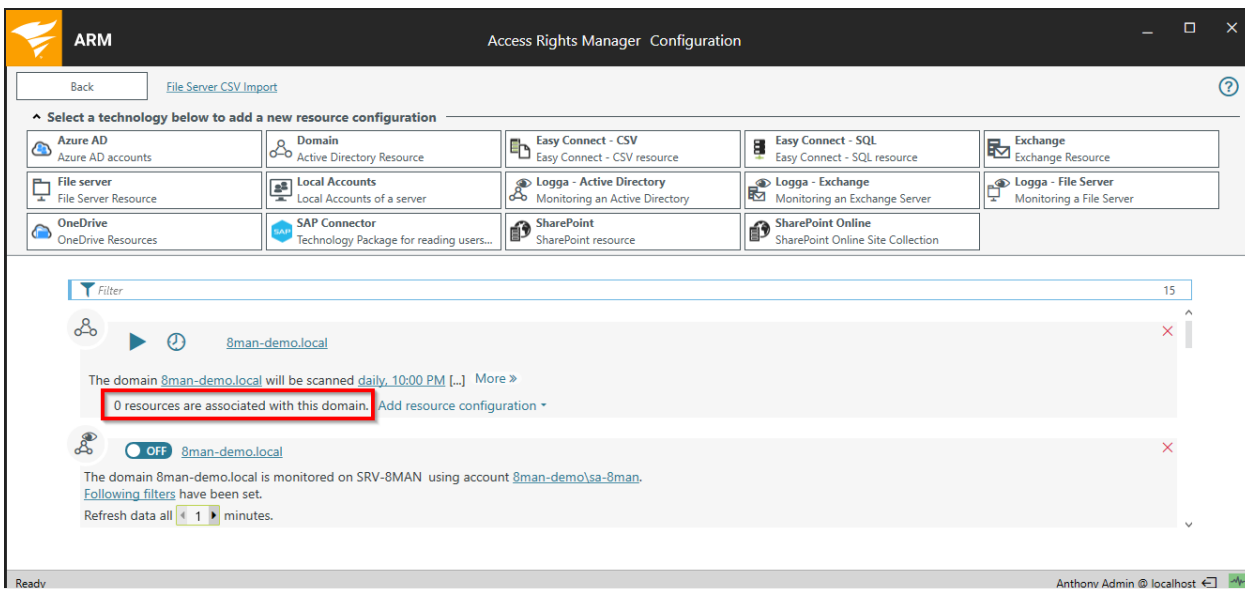
The available configuration options are the same as with an [AD-scan](#).

## Assign resources to a domain

You can assign a file server, Exchange or SharePoint scan to a domain. Use drag & drop in order to make this assignment, or to remove it.

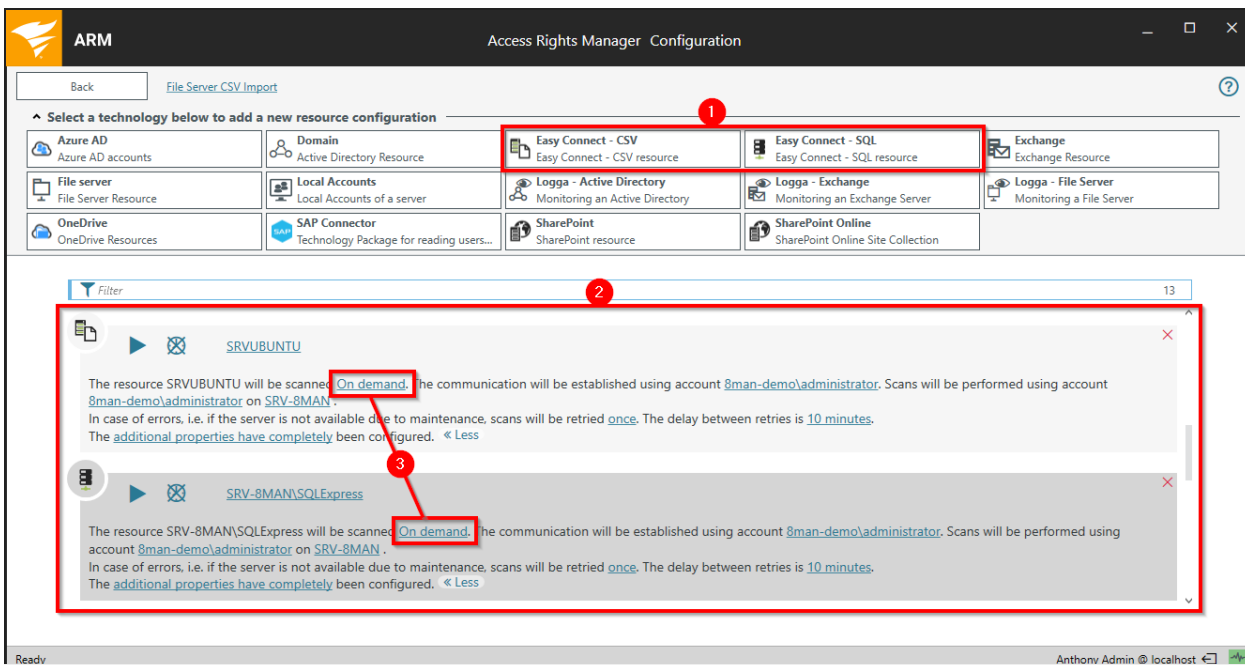


ARM displays assigned resources in the ARM application only if the appropriate domain has been selected.



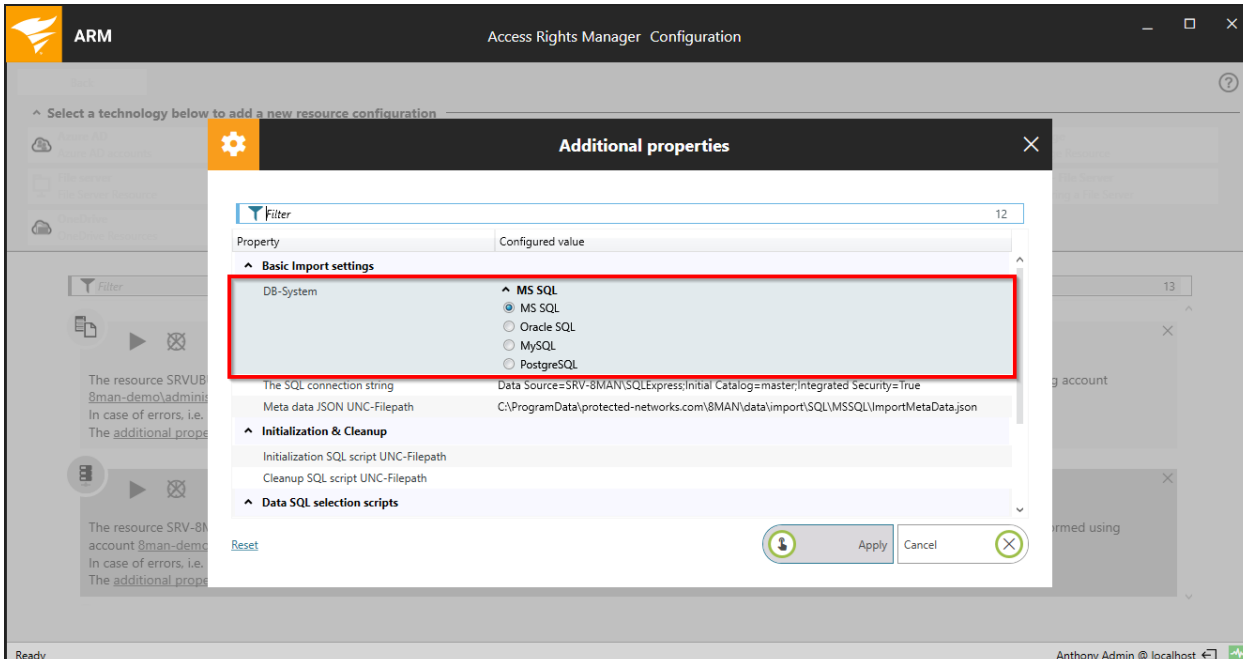
Unassigned resources are always displayed in the ARM application, regardless of the domain selected by the current user.

## Integrate Easy Connect resources



Click "Scans" on the ARM configuration application homepage.

1. Add an Easy Connect resource.
2. The configuration is seamlessly integrated.
3. Configure a regularly import.



ARM supports the following SQL-server:

- Microsoft SQL
- Oracle SQL
- MySQL
- PostgreSQL

The screenshot displays the 'License Information and Server Status' page in the ARM Configuration application. The page is divided into several sections:

- License Information:** Shows Customer (Protected Networks), Licensed (Yes), and Product (Enterprise). It includes a 'Load 8MAN license' link and an 'Upgrade' button.
- Technologies:** Lists domains (8man-demo.local, musterfirma.local, octo.local, Protected-Networks.local, testdom.local), licensed user count (200000), and various Logga counts (99).
- More Technologies:** Lists supported technologies like 8MAN EasyConnect CSV, SAP Connector, Azure AD, etc.
- Features:** Lists features like GrantMA, Programming Interface, Alerts, and Analyze and Act, all with 'Yes' status.
- Server Status:** Shows Uptime (19 hours) and Version (9.1.181.0). It includes a 'Logged in users: 1' table with columns for Name, Domain, Host, and ARM Component. The user 'anthony admin' is listed with domain '8MAN-DEMO' and host 'SRV-8MAN Configuration'.
- Documentation:** A red box highlights this section, which contains links for 'Easy Connect - SQL' (How to documentation, Example SQL command files) and 'Easy Connect - CSV' (How to documentation, Example CSV files).

The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Find a detailed documentation on required CSV-file structure and example files under "License" in the configuration application.

# Alerts

The screenshot displays the SolarWinds Access Rights Manager (ARM) Configuration interface. At the top, the title bar reads "ARM Access Rights Manager Configuration". Below the title bar, there are three summary cards:

- Server Status** (License Information): Logged in users: 2; Licensed Active user accounts: 1166.
- Jobs** (Summary): 91 Scans, 8 Reports, 69 Changes, 136 More; 7 Scheduled, 297 Succeeded, 0 Executing, 0 Failed.
- Collectors** (Configuration): 1 Connected, 1 Configured in Total; All Collectors are Operational.

Below the summary cards is a "Filter" dropdown. The main area contains 12 category tiles, each with an icon and a list of sub-items:

- Scans**: Resource Configurations, Logga, File Server CSV Import
- Open Order**: Open Order Resource Descriptions
- User Management**: User Management, Role Management
- Data Owner**: Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**: License Information, Server Status
- Jobs Overview**: Job Status, Job Categories
- Alerts** (highlighted): Activate/Deactivate Alert Sensors
- Change Configuration**: Common Change Settings, Technology-specific Change Configurations
- Scripting**: Scripting configuration for change actions
- Views & Reports**: Views & Reports, Blacklist for Views & Reports
- Server**: Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**: ARM Server, SQL Server, Configuration Status

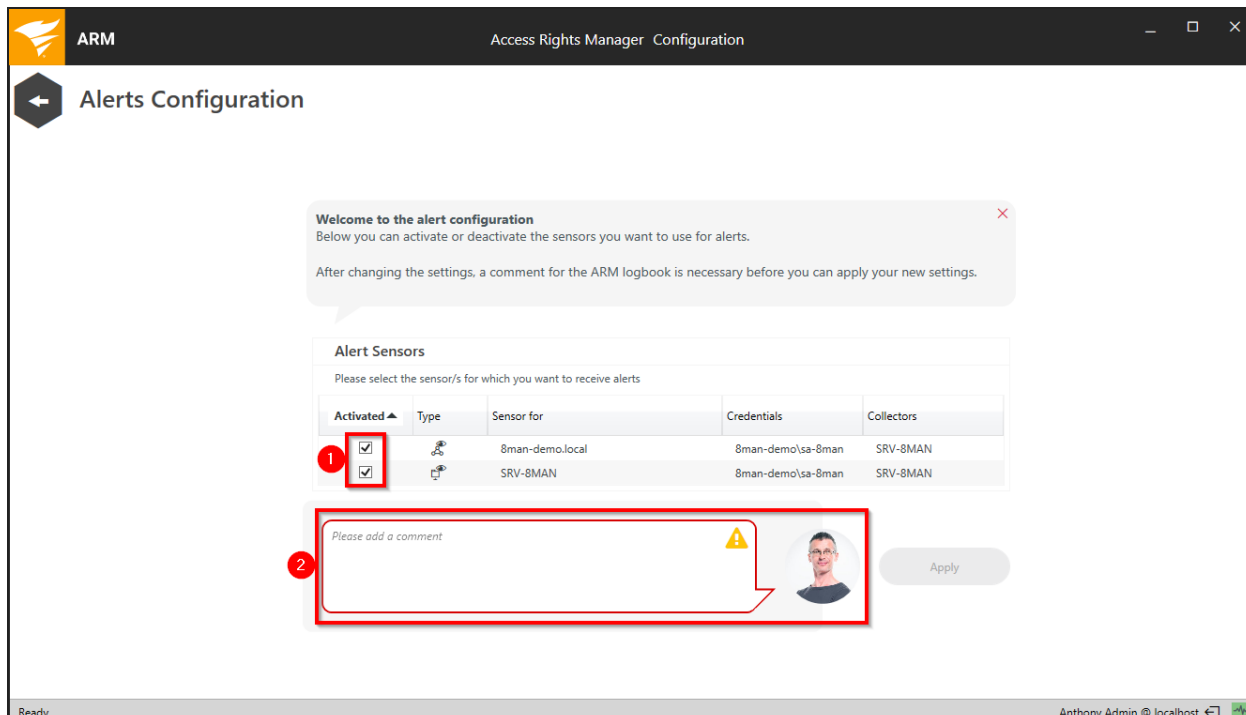
The system tray at the bottom shows "Ready" and the user "Anthony Admin @ localhost".

You activate and deactivate the alarm sensors in the "Alarms" category.

With active alert sensors, you can create alerts for [groups](#), [users](#), [domains](#) or [file servers](#).

[FS Logga](#) or [AD Logga](#) must be enabled for activating the alert sensors.

# Enable or disable alert sensors





ARM Access Rights Manager Configuration



## Alerts Configuration

Welcome to the alert configuration  
Below you can activate or deactivate the sensors you want to use for alerts.  
After changing the settings, a comment for the ARM logbook is necessary before you can apply your new settings.


### Alert Sensors

Please select the sensor/s for which you want to receive alerts

Activated	Type	Sensor for	Credentials	Collectors
<input checked="" type="checkbox"/>		8man-demo.local	8man-demo\sa-8man	SRV-8MAN
<input checked="" type="checkbox"/>		SRV-8MAN	8man-demo\sa-8man	SRV-8MAN

Please add a comment  

1. Enable/disable alert sensors.
2. You must enter a comment.

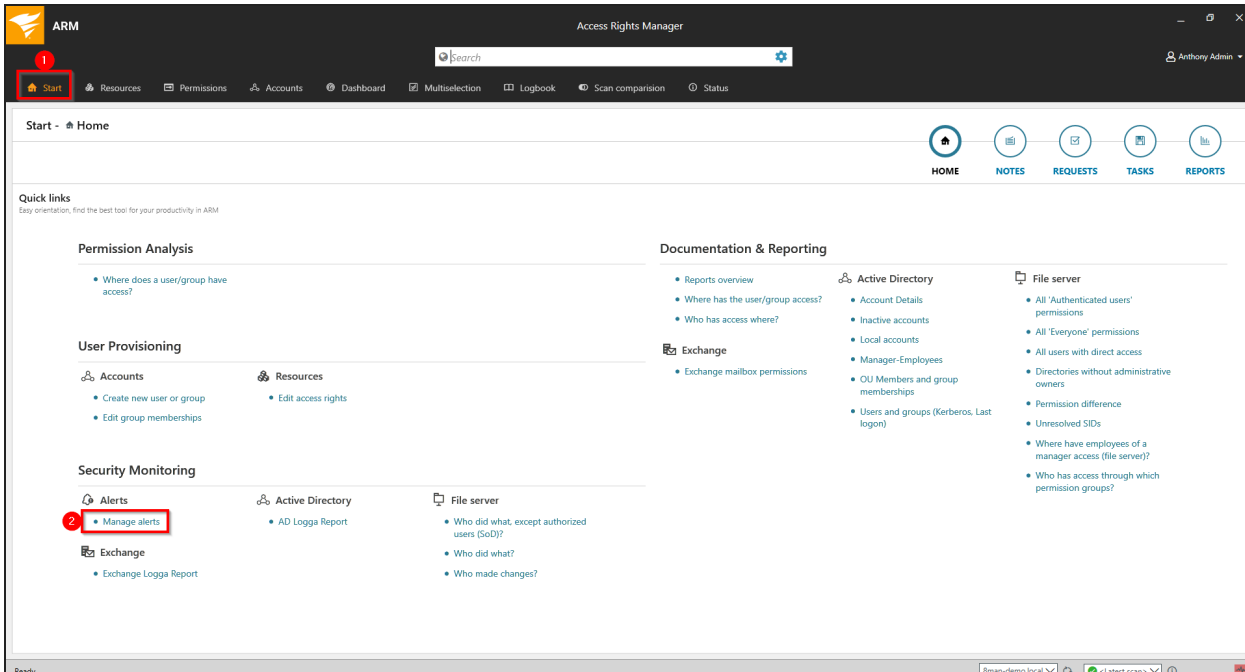
 The alert configurations are only effective with active sensors.

## Manage alerts

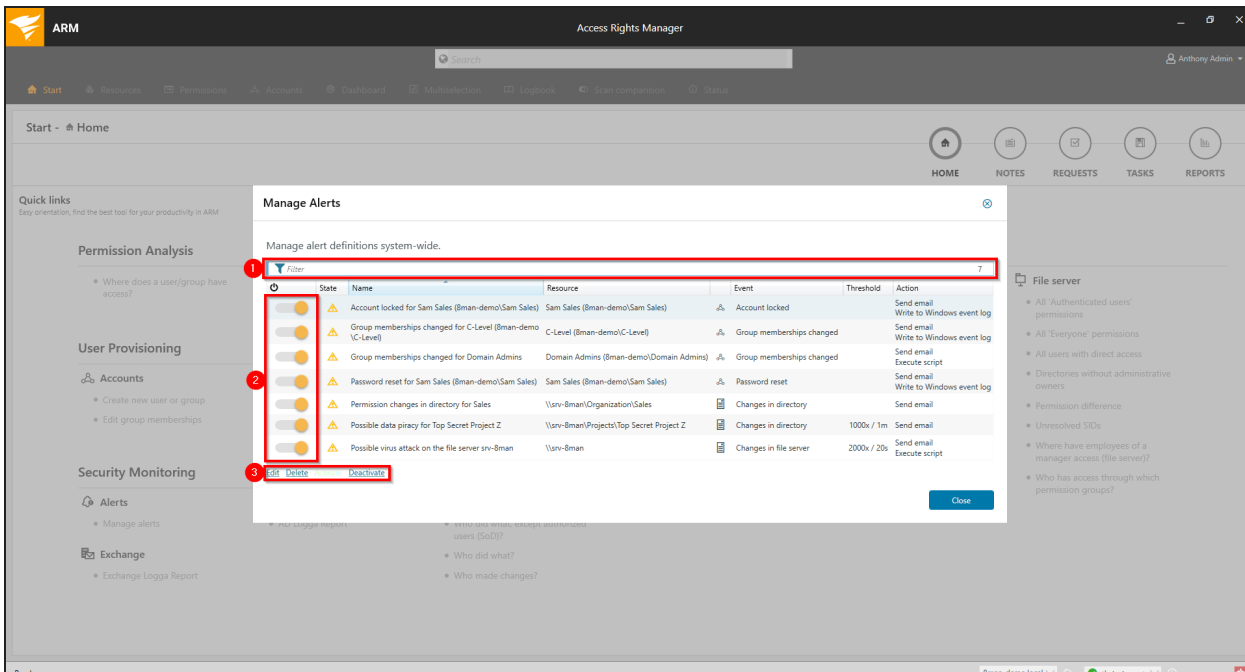
### Background / Value

Saved alert configurations can be modified at any time via the ARM home page.

## Step-by-step process



1. Select "Start".
2. Click "Manage alerts".



ARM shows you all alert configurations.



1. Search for an alert configuration.
2. Turn alerts on or off.
3. Use the links to edit, delete or enable/disable the selected alert configuration. Alternatively you can right-click an entry and use the context menu.

# Manage ARM users

Server Status License Information	Jobs Summary	Collectors Configuration
Logged in users: 2	91 Scans 7 Reports	69 Changes 132 More
Licensed Active user accounts: 1166	7 Scheduled 292 Succeeded	0 Executing 0 Failed
		1 Connected 1 Configured in Total
		All Collectors are Operational

Filter

- Scans**  
Resource Configurations, Logga, File Server CSV Import
- Open Order**  
Open Order Resource Descriptions
- User Management**  
User Management, Role Management
- Data Owner**  
Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**  
License Information, Server Status
- Jobs Overview**  
Job Status, Job Categories
- Alerts**  
Activate/Deactivate Alert Sensors
- Change Configuration**  
Common Change Settings, Technology-specific Change Configurations
- Scripting**  
Scripting configuration for change actions
- Views & Reports**  
Views & Reports, Blacklist for Views & Reports
- Server**  
Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**  
ARM Server, SQL Server, Configuration Status

Ready Anthony Admin @ localhost

Click "User Management" to add ARM-Users and assign roles.

## Add ARM users

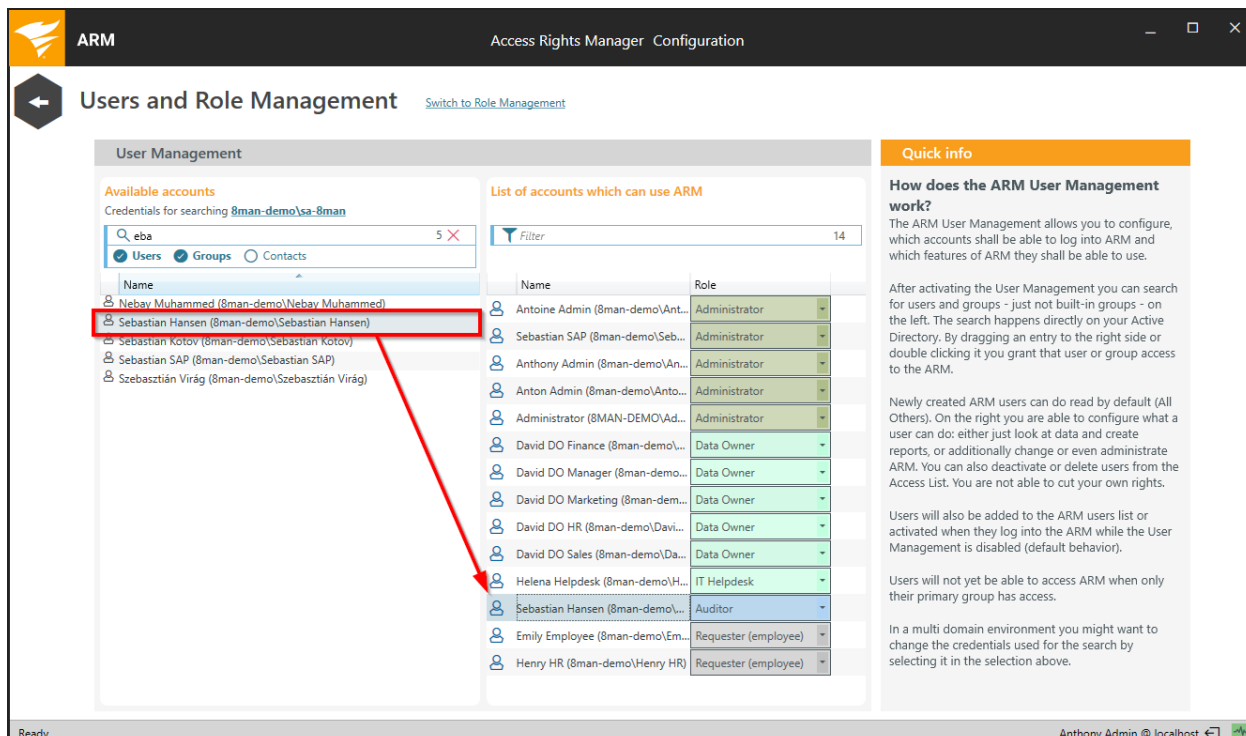
The screenshot shows the 'Users and Role Management' configuration page in the ARM console. At the top, there is a navigation bar with the ARM logo and the title 'Access Rights Manager Configuration'. Below this, a breadcrumb trail shows 'Users and Role Management' with a 'Switch to Role Management' button. The main content area is divided into two columns. The left column, titled 'User Management', contains a search box for 'Available accounts' with the text 'Credentials for searching 8man-demo\sa-8man' and a search field containing 'domain2\another.user'. Below the search field are radio buttons for 'Users' and 'Groups'. A red box highlights the search field and the 'Users' radio button. The right column, titled 'List of accounts which can use ARM', contains a table with columns for 'Name' and 'Role'. The table lists 13 accounts with roles such as Administrator, Data Owner, and Requester. A red box highlights the 'Name' column header. To the right of the table is a 'Quick info' sidebar with the heading 'How does the ARM User Management work?' and several paragraphs of text explaining the functionality.

1. Use the link to switch between user and role management.
2. ARM triggers a live request to your AD when adding an ARM user. It is therefore not required to perform an AD scan prior to adding a user.

### Available search options:

- If no prefixed domain is entered in the search field, ARM reads from the domain from which the credentials originate.
- If a domain is entered (for example: "domain2\another.user"), then ARM will search that domain.

**⚠** When assigning a user to a change role - such as data owner - that user initially has access to all resources. If you want to limit their access further you must do this via the [Data Owner configuration](#).



**ARM** Access Rights Manager Configuration

**Users and Role Management** [Switch to Role Management](#)

**User Management**

**Available accounts**  
 Credentials for searching 8man-demo\sa-8man  
 Search: eba 5 X  
 Users  Groups  Contacts

**List of accounts which can use ARM**

Name	Role
Antoine Admin (8man-demo\Ant...	Administrator
Sebastian SAP (8man-demo\Seb...	Administrator
Anthony Admin (8man-demo\An...	Administrator
Anton Admin (8man-demo\Anto...	Administrator
Administrator (8MAN-DEMO\Ad...	Administrator
David DO Finance (8man-demo\...	Data Owner
David DO Manager (8man-demo...	Data Owner
David DO Marketing (8man-dem...	Data Owner
David DO HR (8man-demo\Davi...	Data Owner
David DO Sales (8man-demo\Da...	Data Owner
Helena Helpdesk (8man-demo\H...	IT Helpdesk
Sebastian Hansen (8man-demo\...	Auditor
Emily Employee (8man-demo\Em...	Requester (employee)
Henry HR (8man-demo\Henry HR)	Requester (employee)

**Quick info**

**How does the ARM User Management work?**  
 The ARM User Management allows you to configure, which accounts shall be able to log into ARM and which features of ARM they shall be able to use.

After activating the User Management you can search for users and groups - just not built-in groups - on the left. The search happens directly on your Active Directory. By dragging an entry to the right side or double clicking it you grant that user or group access to the ARM.

Newly created ARM users can do read by default (All Others). On the right you are able to configure what a user can do: either just look at data and create reports, or additionally change or even administrate ARM. You can also deactivate or delete users from the Access List. You are not able to cut your own rights.

Users will also be added to the ARM users list or activated when they log into the ARM while the User Management is disabled (default behavior).

Users will not yet be able to access ARM when only their primary group has access.

In a multi domain environment you might want to change the credentials used for the search by selecting it in the selection above.

Ready Anthony Admin @ localhost


Once you have found the desired user you can add him via drag & drop or by double-clicking.

## Use groups as ARM users

You can use AD groups as ARM users. The process is identical to adding an ARM user. Please note the following:

### Nested groups

If nested group memberships should be resolved, please follow the instructions in the knowledgebase article [Configure ARM for the use of nested groups in the ARM user management](#).

 Using complex group structures will increase login time significantly.

## Hierarchy of role assignments

By using groups, it is possible to assign several roles to a user. In this scenario the login mechanism verifies role columns from left to right and uses the first match. There is no combination of roles.

## Assign a role to ARM users

**ARM** Access Rights Manager Configuration

**Users and Role Management** [Switch to Role Management](#)

**User Management**

**Available accounts**  
 Credentials for searching 8man-demo\sa-8man  
 Search: eba 5 X  
 Users  Groups  Contacts

**List of accounts which can use ARM**  
 Filter: 14

Name	Role
Antoine Admin (8man-demo\Ant...	Administrator
Sebastian SAP (8man-demo\Seb...	Administrator
Anthony Admin (8man-demo\An...	Administrator
Anton Admin (8man-demo\Anto...	Administrator
Administrator (8MAN-DEMO\Ad...	Administrator
David DO Finance (8man-demo\...	Data Owner
David DO Manager (8man-demo...	Data Owner
David DO Marketing (8man-dem...	Data Owner
David DO HR (8man-demo\Davi...	Data Owner
David DO Sales (8man-demo\Da...	Data Owner
Helena Helpdesk (8man-demo\H...	IT Helpdesk
Sebastian Hansen (8man-demo\...	Auditor
Emily Employee (8man-demo\Em...	Administrators
Henry HR (8man-demo\Henry HR)	Data Owner

**Quick info**

**How does the ARM User Management work?**  
 The ARM User Management allows you to configure, which accounts shall be able to log into ARM and which features of ARM they shall be able to use.

After activating the User Management you can search for users and groups - just not built-in groups - on the left. The search happens directly on your Active Directory. By dragging an entry to the right side or double clicking it you grant that user or group access to the ARM.

Newly created ARM users can do read by default (All Others). On the right you are able to configure what a user can do: either just look at data and create reports, or additionally change or even administrate ARM. You can also deactivate or delete users from the Access List. You are not able to cut your own rights.

Users will also be added to the ARM users list or activated when they log into the ARM while the User Management is disabled (default behavior).

Users will not yet be able to access ARM when only their primary group has access.

environment you might want to  
 tials used for the search by

- Data Owner
- IT Helpdesk
- Benutzerdefinierte Rolle
- User defined
- User defined

Administrators  
 Full access to ARM

Data Owner  
 Read, change and create reports

Auditor  
 Read and create reports

Requester (employee)  
 Request access to resources in web client

No access  
 No access to ARM

Ready Anthony Admin @ localhost

Use the drop down menu to assign a role to an ARM user.

For more information on how to define roles please reference the chapter: [define ARM user roles](#).

## Define ARM user roles

The screenshot shows the 'Users and Role Management' configuration page in the ARM console. The main area is a table with columns for roles and rows for different ARM components. A red box highlights the role names in the first column. The roles are: Administrator, Junior Administrator, Data Owner, IT Helpdesk, Benutzerdefinierte Rolle, User defined, User defined, Auditor, Manager (defined in AD), and Requester (employee). The table shows permissions (green checkmarks for 'yes', red minus signs for 'no') for various ARM Applications and Views.

**Role Management**

Filter for functions and descriptions

**Quick info**

**Role Management**  
With the User Roles Management you can define which type of user should be able to use which feature.

**ARM Applications**

- Configuration Client**  
Allows users to use the ARM configuration client.
- ARM Application**  
Allows to use the ARM client.
- ARM Web client**  
Allows to use the web client.

**Views - ARM-Application**

- Dashboard**  
Shows some statistics and analyses concerning Active Directory.
- Accounts**  
Shows users, groups and other accounts in graphical form.
- Multi selection**  
Shows Active Directory in tabular form to allow the selection of multiple objects.
- Scan comparison**  
Allows ARM users to compare two scans.
- Resources**  
Shows all resources and the corresponding access rights.
- Resources with Active Directory access rights**  
Show access rights for Active Directory objects in the Resource View.
- Modify access rights**  
Shows the access rights of resources and allows modifying them.
- Simplified rights management**  
Reduce the complexity of access right management, by hiding technical details. The ARM user will be presented with a view that is reduced to the configured access right categories and

ARM provides different user role types (from left to right):

- 2 Administrator-roles
- 5 Change-roles
- 1 Read only-role
- 1 Manager Role
- 1 Requester Role

**i** The Manager Role can not be assigned by the ARM user management. It is assigned by the AD attribute "Manager".

**i** You can change the name of the role by clicking on the pen icon.

**i** Only the first administrator role (leftmost column) can use the user management.

The screenshot shows the 'Role Management' section of the Access Rights Manager Configuration tool. A search filter 'paus' is applied to the role list. A red box highlights a section of the check box matrix. The matrix columns represent roles: Administrator, Junior Administrator, Data Owner, IT Helpdesk, Benutzerdefinierte Rolle, User defined, User defined, Auditor, and Manager (defined in AD). The rows represent various ARM features, including ARM Applications, Configuration Client, ARM Application, ARM Web client, Views - ARM-Application (Dashboard, Accounts, Multi selection, Scan comparison), Resources, Resources with Active Directory access rights, Modify access rights, and Simplified rights management.

Use the "check box matrix" to determine which role can use which views and functions. Unlicensed views and features are grayed out (legacy 8MAN licensing model only).

The screenshot shows the same 'Role Management' interface, but with the search filter 'paus' applied to the role list. The 'IT Helpdesk' role is highlighted in blue. The check box matrix shows permissions for 'Actions - Web client' and 'Pause staff member'. The 'Pause staff member' row shows a green checkmark for the 'IT Helpdesk' role and red crosses for other roles.

Use the filter to quickly find the desired option.

⚠ Please note that certain functions require specific access and views. For example the functionality "reset user password" requires either the "Accounts" or the "Resource" view.

ℹ The changes take effect immediately without requiring users to log in again.

## Simplified rights management

The screenshot shows the 'Users and Role Management' configuration page in the Access Rights Manager. A search filter 'simpl' is applied to the 'Role Management' table. Below the table, the 'Views - ARM-Application' section is highlighted with a red box. In this section, the 'Simplified rights management' checkbox is unchecked, and a red circle with the number '1' points to it. The 'Quick info' panel on the right explains that Role Management allows defining user types for specific features.

1. With the simplified rights management, certain details are hidden to simplify operation. This option is suitable for non-technical data owners.

## Limitations of simplified rights management

- The Group Wizard creates groups and members. The Group Wizard must be activated when using simplified user management. It is possible to enable this option with deactivated Group Wizard, however an error message will be shown.
- The option "apply to all" is not available in the Group Wizard, meaning that existing direct access rights can not be turned into group memberships.
- The detailed list of planned changes is hidden.
- Only the content of ARM groups is displayed. Existing access rights (direct or via other non-ARM groups) as well as "Applies to" information (propagation) is hidden.



# Change configuration

ARM Access Rights Manager Configuration

Server Status License Information	Jobs Summary	Collectors Configuration
Logged in users: 2	91 Scans 7 Reports	1 Connected 1 Configured in Total
Licensed Active user accounts: 1166	69 Changes 132 More	All Collectors are Operational
	7 Scheduled 292 Succeeded	
	0 Executing 0 Failed	

Filter

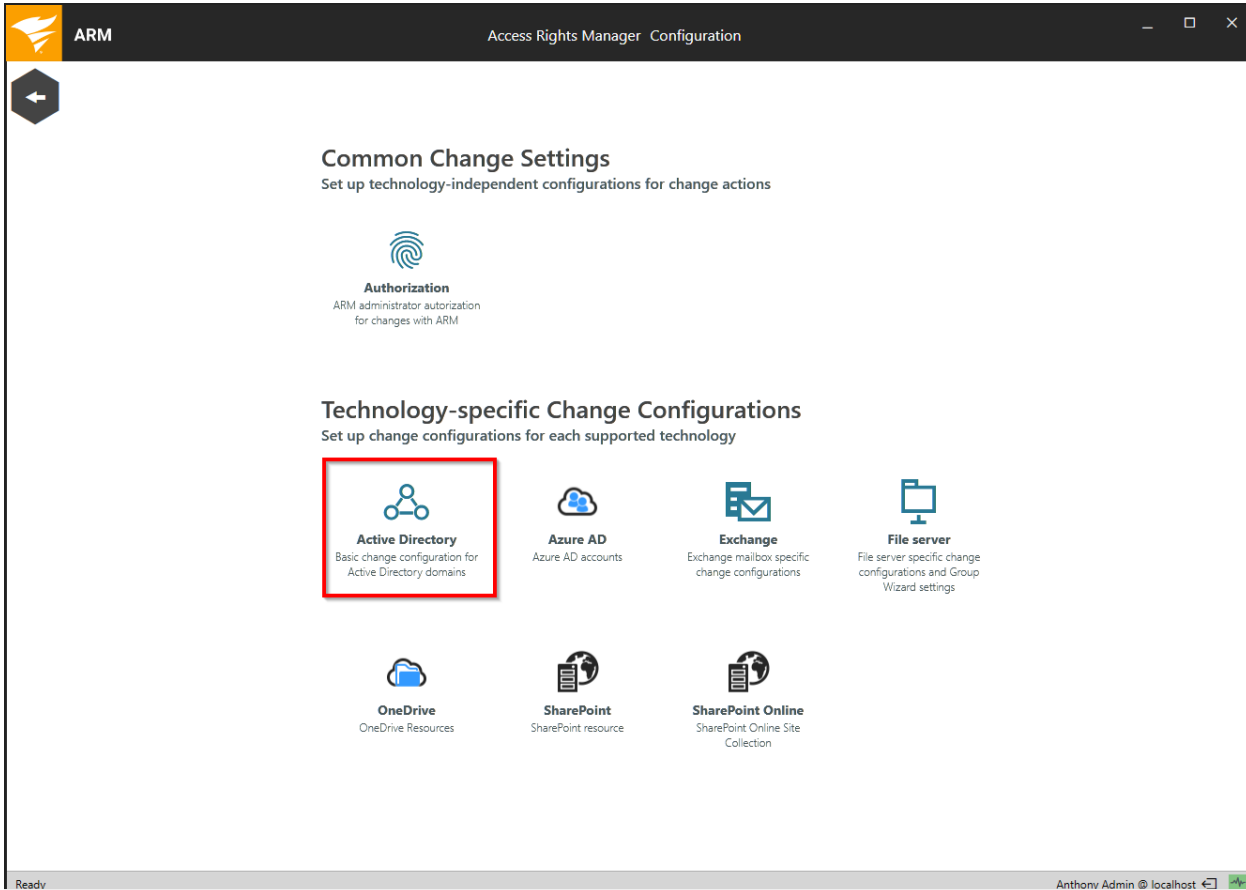
- Scans**  
Resource Configurations, Logga, File Server CSV Import
- Open Order**  
Open Order Resource Descriptions
- User Management**  
User Management, Role Management
- Data Owner**  
Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**  
License Information, Server Status
- Jobs Overview**  
Job Status, Job Categories
- Alerts**  
Activate/Deactivate Alert Sensors
- Change Configuration**  
Common Change Settings, Technology-specific Change Configurations
- Scripting**  
Scripting configuration for change actions
- Views & Reports**  
Views & Reports, Blacklist for Views & Reports
- Server**  
Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**  
ARM Server, SQL Server, Configuration Status

Ready Anthony Admin @ localhost

Click on "Change configuration".

**i** If you are using the ARM Audit Edition (or legacy 8MAN Visor) the chapter "Change configuration" is not relevant.

# Customize the Active Directory (AD) change configuration



Click on "Active Directory".

## Configuring new user default settings

The screenshot shows the 'Configuration - Active Directory' window in the ARM application. The 'Required properties' section is highlighted with a red box. It contains the following elements:

- SAM account name:** Three tabs are visible: 'Users', 'Administrators', and 'Service accounts'. The 'Users' tab is selected, showing a 'Preset' dropdown set to 'Givenname Surname' and a 'Custom' field containing the template '{givenname} {sn}'. Below this, a note states: 'For the fictional user "Ulrike User" e. g. the following SAM account name will be suggested according to your rule definition: Ulrike User'.
- Password options:** Includes an 'Initial password' field with the value '1n17141P455w0rd', a 'Hide password' checkbox, and a 'Generate a new password' button with a length of 8 characters. Three checkboxes are present: 'The user must change the password at next logon' (checked), 'The user cannot change his password' (unchecked), and 'The password never expires' (unchecked).

The 'Quick info' section on the right provides details on attribute functions:

- `<ToUpperCase>(ARGUMENT)` - converts the determined argument into capital letters.
- `<ToLowerCase>(ARGUMENT)` - converts the determined argument into lower case letters.
- `<firstLetter>(ARGUMENT)` - only takes the first letter of the determined argument.
- `<subst>(ARGUMENT)` - substitutes a couple of letters from the given argument, with examples like 'a' to 'ae', 'o' to 'oe', etc.

The 'LDAP Attributes' section at the bottom shows a table with columns for 'Attribute', 'Alias', 'Creation Rule', and 'Validation Rule'. A list of attributes is shown with checkboxes, including 'Account Expires (account...)', 'Common Name (cn)', 'Comment (comment)', 'Company (company)', 'Department (department)', 'Description (description)', 'Display Name (displaynam...', 'Employee Id (employeeid)', and 'Job Category (employeety...').

You can determine default settings that are applied to newly created users in the ARM application.

The naming conventions for user names can be applied differently for users, administrators and service accounts. You can manage these settings in the appropriate tabs.

**Required properties**

SAM account name

Users Administrators Service accounts

Preset

Givename Surname

Custom

{givenname} {sn}

For the fictional user "Ulrike User" e. g. the following SAM account name will be suggested according to your rule definition:

Ulrike User

Password options

Initial password

1n17141P455w0rd

Hide password

Generate a new password with a length of 8

The user must change the password at next logon

The user cannot change his password

The password never expires

**Quick info**

These functions are used to format the password according to the attributes. Functions are marked by angle brackets followed by the argument in round brackets:

<toUpperCase>(ARGUMENT) - converts the determined argument into capital letters,

<toLowerCase>(ARGUMENT) - converts the determined argument into lower case letters,

<firstLetter>(ARGUMENT) - only takes the first letter of the determined argument.

<subst>(ARGUMENT) - substitutes a couple of letters from the given argument, 'a'->'ae', 'o'->'oe', 'u'->'ue', 'A'->'Ae', 'O'->'Oe', 'U'->'Ue', 'B'->'ss', 'r'->'r' 'space'->' 'e'->'e'

**LDAP Attributes**

Users Groups Computers

Attribute name filter 31

Attribute	Alias	Creation Rule	Validation Rule
Account Expires (account...)			
Common Name (cn)			^.*\w+.*\$
Comment (comment)			
Company (company)			
Department (department)			
Description (description)			
Display Name (displaynam...)			
Employee Id (employeeid)			
Job Category (employeeety...)			

Different possibilities for naming rules are described in the "Quick info" section.

## Select available LDAP attributes

The screenshot shows the 'Configuration - Active Directory' window in the ARM application. The 'LDAP Attributes' section is highlighted with a red box. It contains a table with the following columns: Attribute, Alias, Creation Rule, and Validation Rule. The table lists various LDAP attributes, some of which are marked with green checkmarks in the first column, indicating they are mandatory. The 'Attribute' column also includes a star icon for some attributes.

Attribute	Alias	Creation Rule	Validation Rule
Account Expires (account...)			
Common Name (cn)			^.*\w+.*\$
Comment (comment)			
Company (company)			
Department (department)			
Description (description)			
Display Name (displaynam...)			
Employee Id (employeeid)			
Job Category (employeety...)			
Given Name (givenname)			
Home Directory (homedir...)			
Home Drive (homedrive)			[a-zA-Z]:
Home Phone (homephone)			(1,64)
Information (info)			
Initials (initials)			
Location (l)	Ort		
lockouttime (lockouttime)			
Email Address (mail)			
Manager (manager)			^([a-zA-Z0-9-@_+])+\$

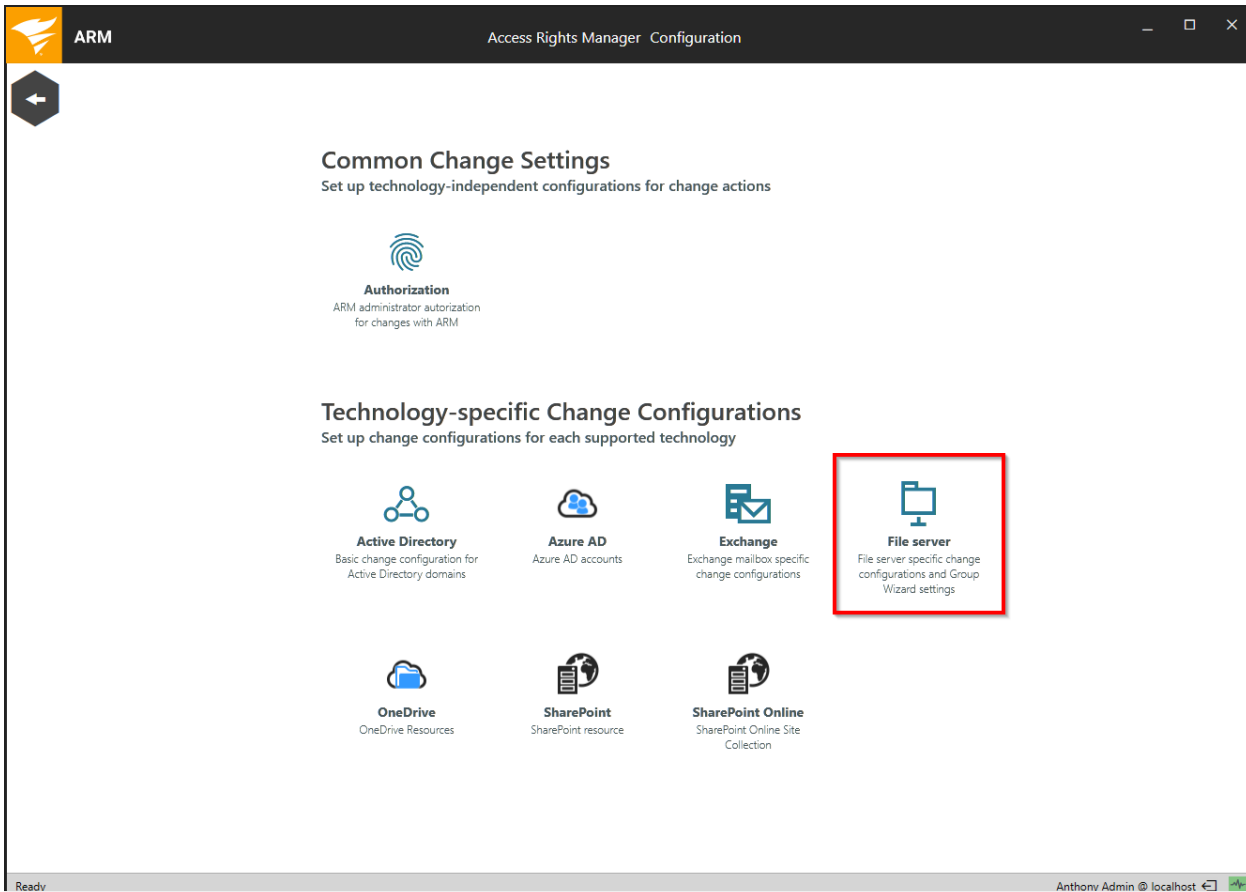
You can select which LDAP attributes are available in the ARM application for the creation of new users and groups.

Attributes that are marked with a green check in the first column can not be deselected.

Attributes with an additional green check in the second column are mandatory fields that must be filled in.

**i** ARM reads and displays a standard set of LDAP attributes. If you would like to use additional attributes, please refer to [load additional LDAP attributes](#) and [customize LDAP attributes properties](#).

# File Server (FS) change configuration



Click on "File server".

## Manage global settings for FS changes

ARM Access Rights Manager Configuration

### Change Configuration - File server

**Quick info**

**Resources**  
You can set up change configurations and the Group Wizard for each resource.  
Please select a resource to setup its change configuration.

**Resources**

- Global file server configuration

**Configuration Status**

- Group Wizard Settings: Configuration successfully loaded.
- Configuration Check: The configuration is valid.

**Basic Settings**

- Enable Group Wizard
- Simulate changes only (simulation mode)
- Enable scheduled removing of access rights (Comfort Feature):  
Earliest run after 2 day(s) at 12:00 a.m.
- Use following domain groups:  
 local  global  universal  local and global  Create global groups within the account domain
- Performs an initial check of the access right changes on the affected resources before additional options will be provided (e.g. Group Wizard usage or the name of access right groups).

**Access Categories**

**Naming Conventions for ARM Groups**

**Blacklist**

Ready Anthony Admin @ localhost

Click "Global file server configuration" in the "Resources" section.

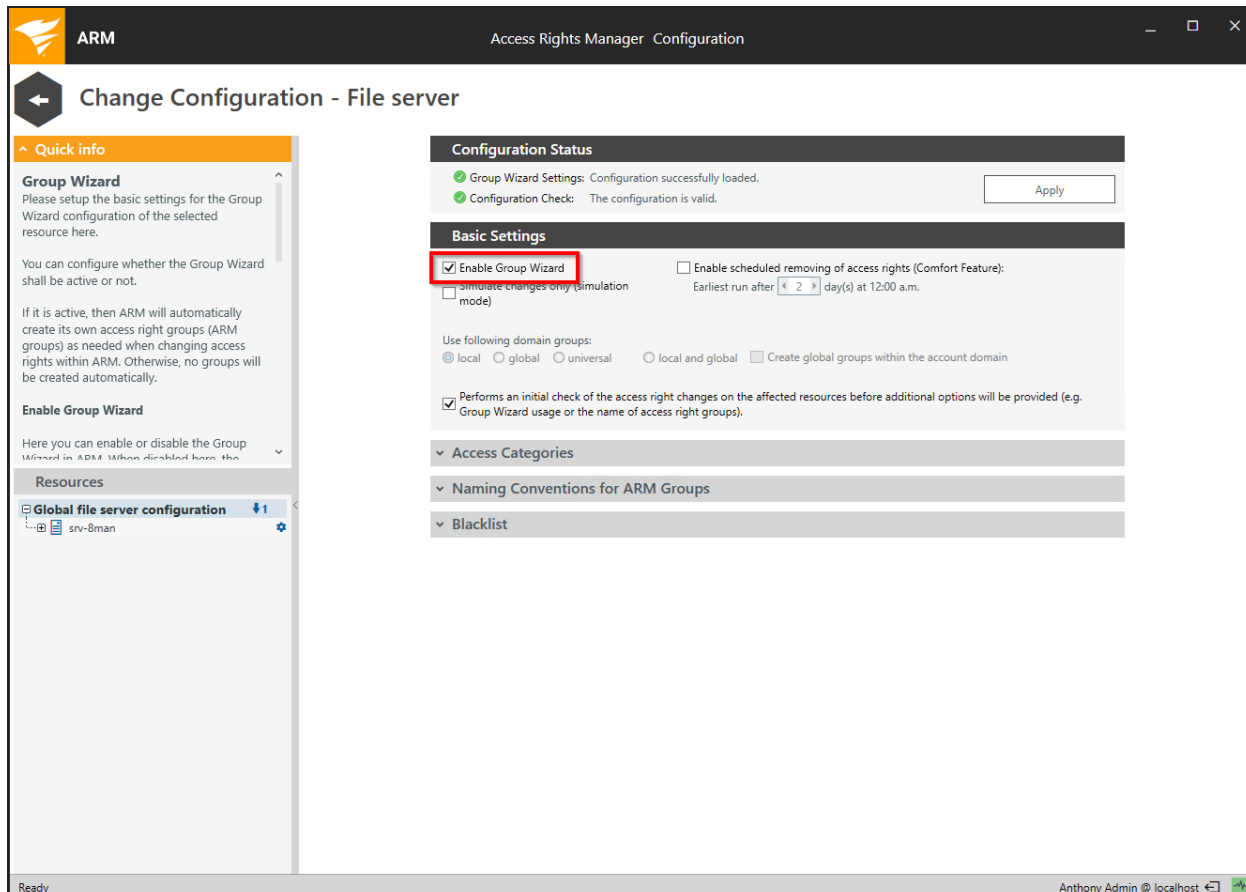
## Basic settings

The screenshot shows the 'Access Rights Manager Configuration' window for a 'File server'. The main title is 'Change Configuration - File server'. On the left, there is a 'Quick info' section with a 'Group Wizard' subsection. The 'Group Wizard' section contains text explaining its function and an 'Enable Group Wizard' checkbox. Below this is a 'Resources' section with a tree view showing 'Global file server configuration' and 'srv-8man'. The main area on the right is titled 'Configuration Status' and 'Basic Settings'. The 'Configuration Status' section shows two green checkmarks: 'Group Wizard Settings: Configuration successfully loaded.' and 'Configuration Check: The configuration is valid.', with an 'Apply' button. The 'Basic Settings' section is highlighted with a red box and contains the following options: 'Enable Group Wizard' (checked), 'Simulate changes only (simulation mode)' (unchecked), 'Enable scheduled removing of access rights (Comfort Feature):' (unchecked), 'Earliest run after' (2 days), 'Use following domain groups:' (radio buttons for local, global, universal, local and global, and a checkbox for 'Create global groups within the account domain'), and 'Performs an initial check of the access right changes on the affected resources before additional options will be provided (e.g. Group Wizard usage or the name of access right groups):' (checked). Below the 'Basic Settings' are sections for 'Access Categories', 'Naming Conventions for ARM Groups', and 'Blacklist'. The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Determine the basic settings for Group Wizard, comfort feature and sandbox.



## Use the Group Wizard



The Group Wizard is one of the most powerful features of ARM.

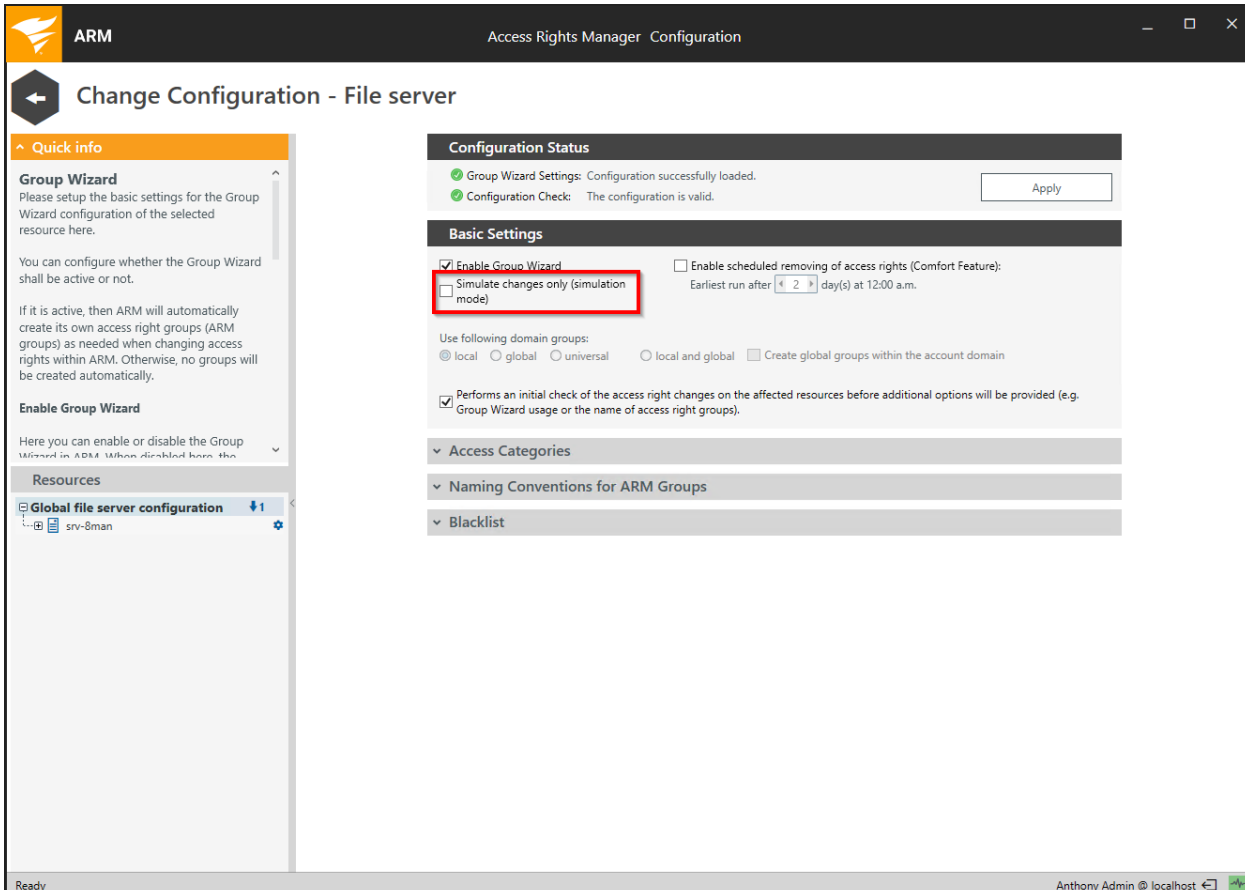
### Option disabled

File server access rights changes made with ARM are written directly into the ACL (Access Control List). If you do this with users and not with groups, this procedure contradicts Microsoft's recommended best practices.

### Option enabled

ARM automatically creates and removes permission groups (ARM groups). Users and groups are then assigned memberships in these ARM groups.

## Use the simulation mode



The screenshot shows the 'Change Configuration - File server' window in the Access Rights Manager (ARM) application. The window title is 'Access Rights Manager Configuration'. The main content area is divided into several sections:

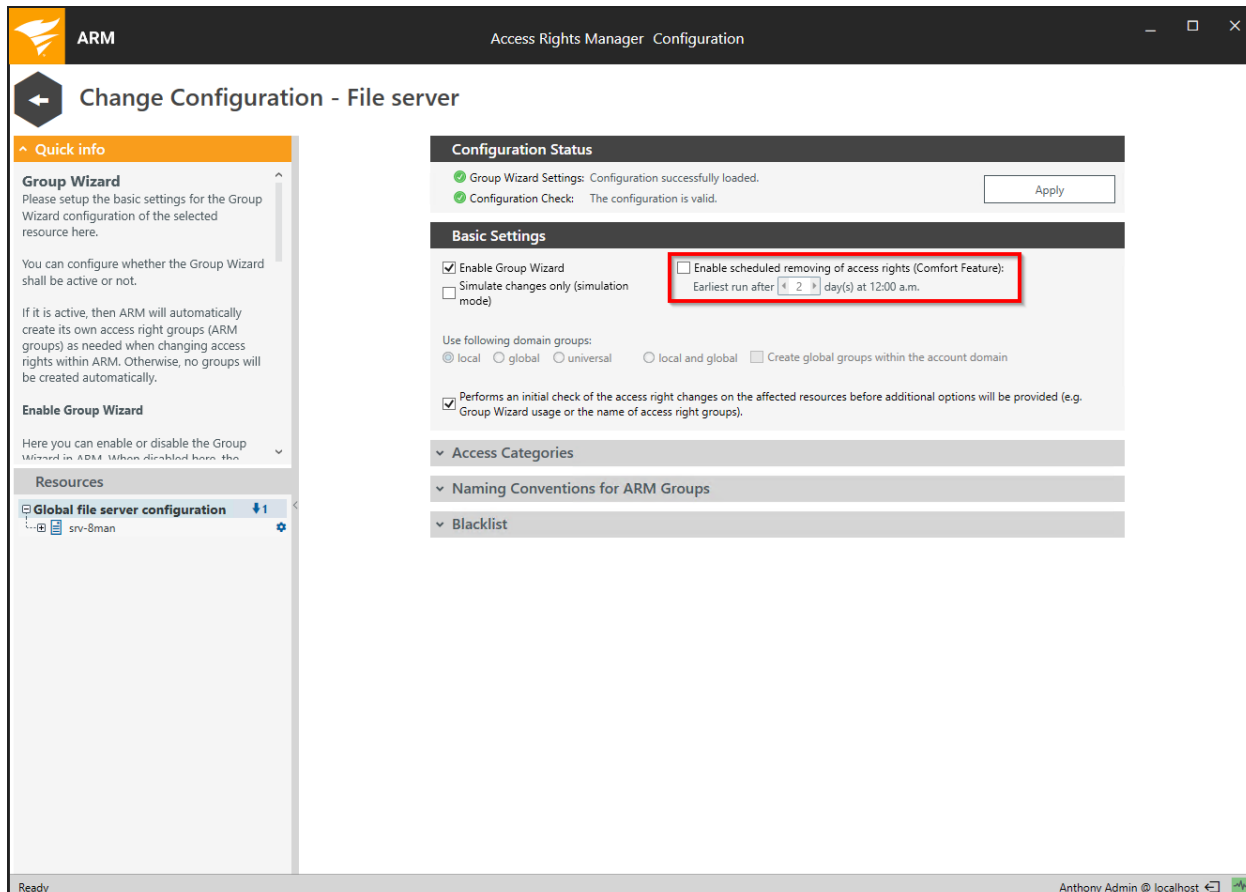
- Quick info:** Contains information about the Group Wizard and its settings.
- Configuration Status:** Shows two green checkmarks indicating that the Group Wizard Settings are successfully loaded and the configuration is valid. An 'Apply' button is present.
- Basic Settings:** Contains several checkboxes and options:
  - Enable Group Wizard
  - Simulate changes only (simulation mode) - This option is highlighted with a red box.
  - Enable scheduled removing of access rights (Comfort Feature): Earliest run after 2 day(s) at 12:00 a.m.
  - Use following domain groups: local (selected), global, universal, local and global, Create global groups within the account domain.
  - Performs an initial check of the access right changes on the affected resources before additional options will be provided (e.g. Group Wizard usage or the name of access right groups).
- Access Categories:** A section with a dropdown arrow.
- Naming Conventions for ARM Groups:** A section with a dropdown arrow.
- Blacklist:** A section with a dropdown arrow.

The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Activate the simulation mode to preview all planned changes, for example, which groups would be created. You can not apply changes in this mode.

If you want to execute changes with ARM, the simulation mode must be deactivated.

## Use the comfort feature



The screenshot shows the 'Access Rights Manager Configuration' window. The title bar reads 'ARM Access Rights Manager Configuration'. The main window title is 'Change Configuration - File server'. On the left, there is a 'Quick info' section for the 'Group Wizard' and a 'Resources' list containing 'Global file server configuration'. The main area is divided into 'Configuration Status' and 'Basic Settings'. Under 'Configuration Status', there are two green checkmarks: 'Group Wizard Settings: Configuration successfully loaded.' and 'Configuration Check: The configuration is valid.', with an 'Apply' button. Under 'Basic Settings', the 'Enable Group Wizard' checkbox is checked. The 'Enable scheduled removing of access rights (Comfort Feature):' checkbox is unchecked and highlighted with a red box. Below it, the 'Earliest run after' is set to '2' days at '12:00 a.m.'. Other options include 'Simulate changes only (simulation mode)', 'Use following domain groups' (radio buttons for local, global, universal, local and global, and a checkbox for 'Create global groups within the account domain'), and 'Performs an initial check of the access right changes on the affected resources before additional options will be provided (e.g. Group Wizard usage or the name of access right groups.)' which is checked. Below these are sections for 'Access Categories', 'Naming Conventions for ARM Groups', and 'Blacklist'. The system tray at the bottom shows 'Ready' and 'Anthony Admin @ localhost'.

When users register on the network, their group memberships are verified and added to the Kerberos token. When assigning permissions with the Group Wizard via group memberships, they only become active after the user logs out of and into the system again.

By activating the "comfort feature", users temporarily receive direct access rights. These are active immediately and are automatically removed after a configurable time. This allows the user to access required resources immediately without having to log out and in again.

**i** ARM does not set temporary list permissions. Users may not be able to navigate to the folders.

## Activate or deactivate an initial test

The screenshot shows the 'Change Configuration - File server' window in the Access Rights Manager (ARM) application. The window title is 'Access Rights Manager Configuration'. The main content area is titled 'Change Configuration srv-8man'. There are two tabs: 'Basic Settings' and 'Group Wizard'. The 'Group Wizard' tab is active, showing an information icon and a message: 'Configure the global Group Wizard settings on the "Global file server configuration" top node. You can configure different settings for subordinated file servers or shares here.' Below this, there are two sections: 'Configuration Status' and 'Basic Settings'. The 'Configuration Status' section shows two green checkmarks: 'Group Wizard Settings: Configuration successfully loaded. No group strategy has been chosen yet.' and 'Configuration Check: The configuration is valid.' There is an 'Apply' button. The 'Basic Settings' section has several options: 'Enable Group Wizard' (checked), 'Simulate changes only (simulation mode)' (unchecked), 'Enable scheduled removing of access rights (Comfort Feature):' (unchecked), and 'Use following domain groups:' with radio buttons for 'local', 'global' (selected), 'universal', and 'local and global'. There is also a checkbox for 'Create global groups within the account domain' (unchecked). A red box highlights the option 'Perform an initial check of the access right changes on the affected resources before additional options will be provided (e.g. Group Wizard usage or the name of access right groups)', which is checked. Below this are expandable sections for 'Access Categories', 'Naming Conventions for ARM Groups', and 'Blacklist'. The bottom status bar shows 'Ready' and 'Anthony Admin @ localhost'.

**Option enabled**

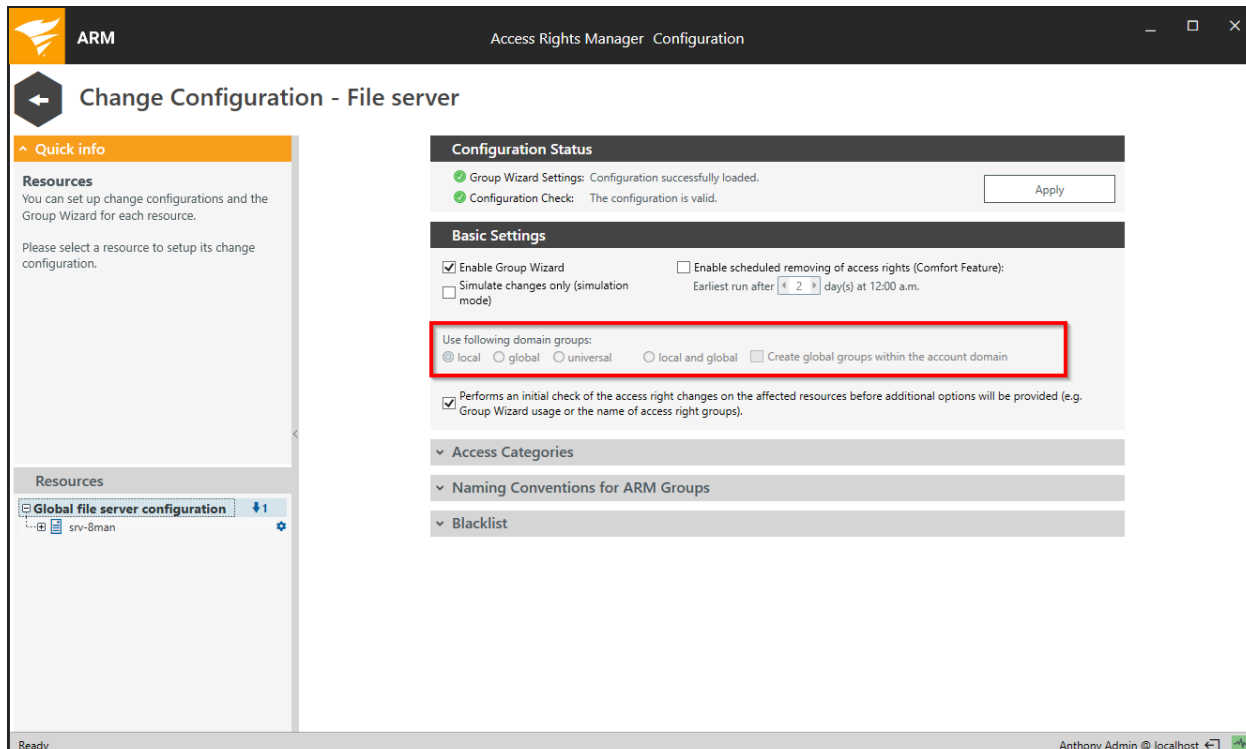
The Group Wizard will determine all required steps for access rights changes in the ARM application immediately after clicking on "Apply".

**Option disabled**

Before determining the required changes, a dialog box will open, allowing you to make changes to Group Wizard options.

This can save a lot of time, especially if you want to perform complex access rights changes with non-standard Group Wizard options.

## Set AD group types for the Group Wizard



Specify the model according to which the Group Wizard creates groups.

**!** After you have selected a model and saved the configuration you can not change it. It can be extremely cumbersome to make any changes to the model after it has been saved so please select carefully!

**i** More information regarding the use of AD groups can be found on the following pages and in the article [Understanding Groups](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd861330(v=ws.11)) (© 2020 Microsoft, [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd861330\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd861330(v=ws.11)), obtained on January 30, 2020).

Use local AD groups

**A -> DL -> P**

A - account (user account)

DL - domain local group (local AD group)

P - permission

1. ARM creates AD groups with the type local.
2. ARM adds the required users to this group.
3. ARM assigns permissions to file server resources for this group.

## ADVANTAGES

Users and groups from other domains or forests can be a member of a local AD group and thereby be assigned permissions.

## DISADVANTAGES

Membership in a local group requires 40 bytes of storage in the Kerberos token. This can cause the maximum permitted Kerberos token size to be exceeded, especially in large environments where users have a large number of group memberships.

Local AD groups are only visible and usable in the corresponding domain.

Use global AD groups

**A -> G -> P**

A - account (user account)

G - global group (global AD-group)

P - permission

The screenshot shows the 'Change Configuration - File server' dialog in the SolarWinds Access Rights Manager. The 'Group Wizard' tab is selected, and the 'global' radio button under 'Use following domain groups' is highlighted with a red box. The 'Configuration Status' section indicates that the configuration is valid. The 'Basic Settings' section includes options to 'Enable Group Wizard' and 'Enable scheduled removing of access rights (Comfort Feature)'. The 'Access Categories', 'Naming Conventions for ARM Groups', and 'Blacklist' sections are collapsed.

1. ARM creates AD groups of the type global.
2. ARM adds the required users to this group.
3. ARM assigns permissions to file server resources for this group.

## ADVANTAGES

Membership in a global AD-group requires only 8 bytes of storage space in the Kerberos token.

This is the most "frugal" group-type, in case you are having issues with Kerberos token limits.

## DISADVANTAGES

Only users and groups of the corresponding domain can be members of global AD-groups. Therefore, this approach is unsuitable for multi-domain environments.

Use universal AD groups

**A -> U -> P**

A - account (user-account)

U - universal group (universal AD-group)

P - permission

The screenshot shows the 'Change Configuration - File server' dialog in the Access Rights Manager Configuration window. The 'Group Wizard' tab is selected, and the 'universal' radio button under 'Use following domain' is highlighted with a red box. The 'Configuration Status' section shows that the configuration is valid. The 'Basic Settings' section includes options for enabling the Group Wizard, simulating changes, and enabling scheduled removing of access rights. The 'Access Categories' section is expanded, showing 'Naming Conventions for ARM Groups' and 'Blacklist'.

1. ARM creates AD groups with the type universal.
2. ARM adds the required users to this group.
3. ARM assigns permissions to file server resources for this group.



**ADVANTAGES**

Membership in a universal group requires 8 bytes (foreign domain) or 40 bytes (own domain) of storage in the Kerberos token. A universal group can be a member on foreign domains as long as these belong to the same forest. It is therefore possible to use a group in multiple domains within the same forest.

**DISADVANTAGES**

Universal AD-groups may not have local AD-groups as members. Nested grouping (parent - child relationships) are part of this restriction.

Universal groups can not be used across multiple forests. Therefore this approach is unsuitable in multi-forest environments.

---

Use local and global AD groups

**A -> G -> DL -> P**

A - account (user-account)

G - global group (global AD-group)

DL - domain local group (local AD-group)

P - permission

Consider all groups created by the group wizard as file server resource groups. You should not use these groups for other purposes (for example: VPN access).

1. ARM creates a group of the type global for users.
2. ARM adds the desired users to the global group.
3. ARM creates another group of the type local.
4. ARM nests the group. The global group (child) becomes a member of the local group (parent).
5. ARM gives the local group access rights to file server resources.

## Example

"Sam Sales" (A) -> "g\_fs01\_share01\_sales\_md" (G) -> "l\_fs01\_share01\_sales\_md" (DL) -> permission (P) "Modify" on the folder "Sales".

The screenshot shows the 'Change Configuration - File server' dialog box in the SolarWinds ARM Configuration tool. The 'Group Wizard' tab is selected. Under 'Configuration Status', there are two green checkmarks: 'Group Wizard Settings: Configuration successfully loaded. No group strategy has been chosen yet.' and 'Configuration Check: The configuration is valid.' Below this, under 'Basic Settings', the 'Enable Group Wizard' checkbox is checked. Under 'Use following domain groups:', the 'local and global' radio button is selected, and the 'Create global groups within the account domain' checkbox is checked and highlighted with a red box. Other options include 'Simulate changes only (simulation mode)', 'Enable scheduled removing of access rights (Comfort Feature)', and 'Perform an initial check of the access right changes on the affected resources before additional options will be provided (e.g. Group Wizard usage or the name of access right groups)'. The dialog also has sections for 'Access Categories', 'Naming Conventions for ARM Groups', and 'Blacklist'.

### Option enabled (recommended)

The global group is created in every domain that members are located in (this including possibly multiple times). Only by activating this function can you assign access rights across multiple domains.

### Option disabled

The global group is only created in the domain that the resource is located in. In this scenario it is not possible to assign access rights across multiple domains.

## ADVANTAGES

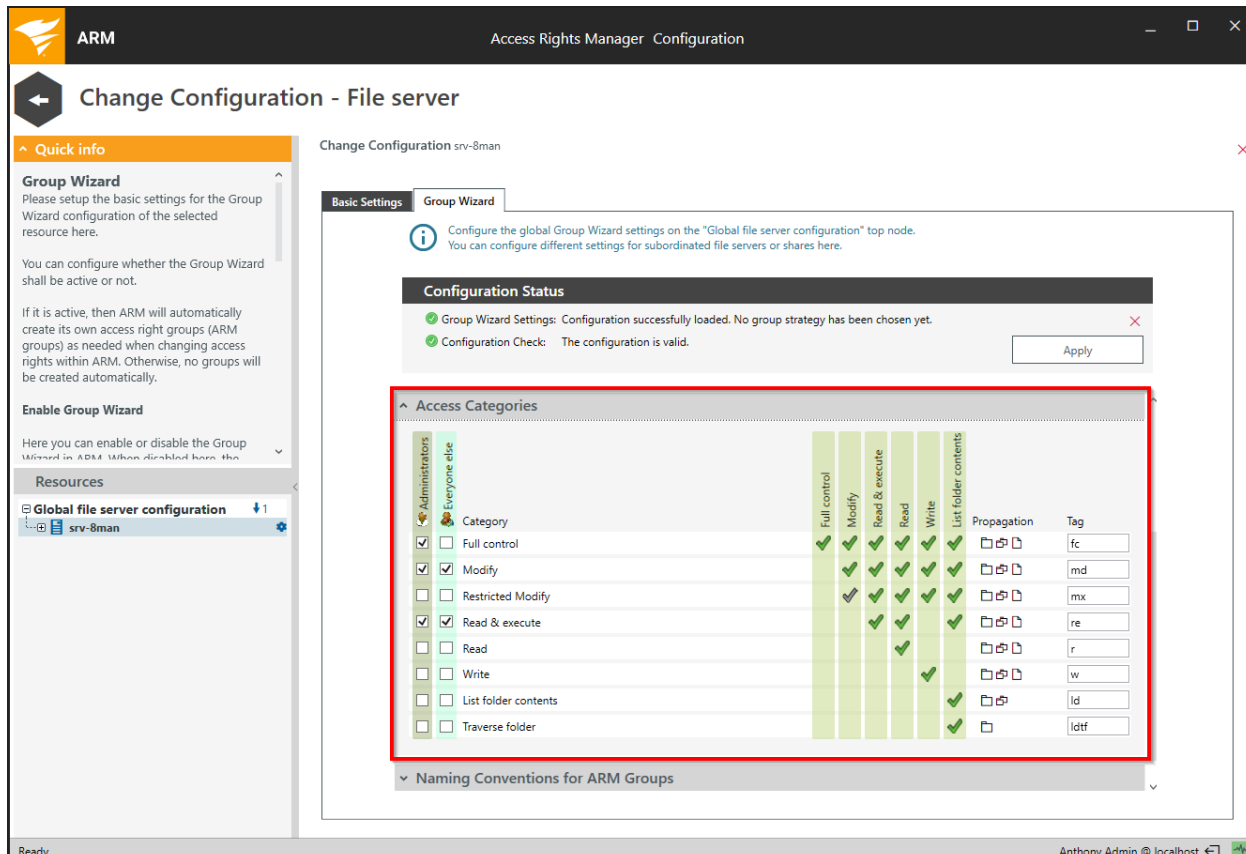
The A-G-DL-P-principle ensures a variety of different options and approaches in multi-domain and multi-forest environments.

## DISADVANTAGES

Users require two or more group memberships for their permissions. Therefore this approach may lead to issues with token size.

## Select access categories available in ARM

ARM bundles the Microsoft permission combinations into access categories. This allows for a simplification of access rights assignment.



The screenshot shows the 'Change Configuration - File server' window in the ARM application. The 'Access Categories' section is highlighted with a red box. It displays a table of permissions and their corresponding tags. The table has columns for 'Full control', 'Modify', 'Read & execute', 'Read', 'Write', 'List folder contents', 'Propagation', and 'Tag'. The 'Full control' column is highlighted in green, indicating it is selected. The 'Read & execute' and 'List folder contents' columns are also highlighted in green, indicating they are selected. The 'Tag' column shows the corresponding tags for each permission.

Category	Full control	Modify	Read & execute	Read	Write	List folder contents	Propagation	Tag
<input type="checkbox"/> Full control	✓	✓	✓	✓	✓	✓	☐ ☐ ☐	fc
<input checked="" type="checkbox"/> Modify	✓	✓	✓	✓	✓	✓	☐ ☐ ☐	md
<input type="checkbox"/> Restricted Modify		✓	✓	✓	✓	✓	☐ ☐ ☐	mx
<input checked="" type="checkbox"/> Read & execute	✓	✓	✓	✓	✓	✓	☐ ☐ ☐	re
<input type="checkbox"/> Read			✓	✓	✓	✓	☐ ☐ ☐	r
<input type="checkbox"/> Write					✓	✓	☐ ☐ ☐	w
<input type="checkbox"/> List folder contents						✓	☐ ☐ ☐	ld
<input type="checkbox"/> Traverse folder						✓	☐	ldtf

Select the access category that you would like to make available in ARM.

Selected access categories will then be visible as columns in the ARM application.

The screenshot shows the 'Change Configuration - File server' window in SolarWinds ARM. The 'Group Wizard' tab is active, displaying configuration status and a table of access categories. A red box highlights the 'Administrators' and 'Everyone else' roles in the 'Access Categories' table.

**Configuration Status:**

- Group Wizard Settings: Configuration successfully loaded. No group strategy has been chosen yet.
- Configuration Check: The configuration is valid.

**Access Categories Table:**

Category	Full control	Modify	Read & execute	Read	Write	List folder contents	Propagation	Tag
Full control	✓	✓	✓	✓	✓	✓	☐ ☐ ☐	fc
Modify	✓	✓	✓	✓	✓	✓	☐ ☐ ☐	md
Restricted Modify	✓	✓	✓	✓	✓	✓	☐ ☐ ☐	mx
Read & execute	✓	✓	✓	✓	✓	✓	☐ ☐ ☐	re
Read	✓	✓	✓	✓	✓	✓	☐ ☐ ☐	r
Write	✓	✓	✓	✓	✓	✓	☐ ☐ ☐	w
List folder contents	✓	✓	✓	✓	✓	✓	☐ ☐	ld
Traverse folder	✓	✓	✓	✓	✓	✓	☐	ldtf

Determine which access categories should be available for which ARM-user roles.

You can configure these settings so that the administrator role can manage different access categories than the other ARM-user roles.

**Change Configuration - File server**

Change Configuration srv-8man

**Group Wizard**

Configure the global Group Wizard settings on the "Global file server configuration" top node. You can configure different settings for subordinated file servers or shares here.

**Configuration Status**

- Group Wizard Settings: Configuration successfully loaded. No group strategy has been chosen yet.
- Configuration Check: The configuration is valid.

**Access Categories**

Category	Full control	Modify	Read & execute	Read	Write	List folder contents	Propagation	Tag
Full control	✓						☐ ☐	fc
Modify		✓	✓	✓	✓	✓	☐ ☐	md
Restricted Modify			✓	✓	✓	✓	☐ ☐	mx
Read & execute			✓	✓	✓	✓	☐ ☐	re
Read				✓			☐ ☐	r
Write					✓		☐ ☐	w
List folder contents						✓	☐ ☐	ld
Traverse folder						✓	☐	ldtf

**Naming Conventions for ARM Groups**

Determine the abbreviations for the individual access categories. The abbreviations can also be used for the naming convention of ARM-groups.

Default abbreviations have the following significance:

- fc - full control
- md - modify
- mx - restricted modify
- re - read & execute
- r - read
- w - write
- ld - list directory
- ldtf - list directory this folder (only)

# Traverse folder

Change Configuration - File server

Change Configuration srv-8man

**Basic Settings** | **Group Wizard**

**Configuration Status**

- Group Wizard Settings: Configuration successfully loaded. No group strategy has been chosen yet.
- Configuration Check: The configuration is valid.

**Access Categories**

Category	Full control	Modify	Read & execute	Read	Write	List folder contents	Propagation	Tag
<input checked="" type="checkbox"/> Full control	✓	✓	✓	✓	✓	✓	📁📁📁	fc
<input checked="" type="checkbox"/> Modify		✓	✓	✓	✓	✓	📁📁📁	md
<input type="checkbox"/> Restricted Modify		✗	✓	✓	✓	✓	📁📁📁	mx
<input checked="" type="checkbox"/> Read & execute			✓	✓	✓	✓	📁📁📁	re
<input type="checkbox"/> Read				✓			📁📁📁	r
<input type="checkbox"/> Write					✓		📁📁📁	w
<input type="checkbox"/> List folder contents						✓	📁📁	ld
<input type="checkbox"/> Traverse folder						✓	📁	ldtf

**Naming Conventions for ARM Groups**

"Traverse folder" is a special combination of access rights where the user only has rights to traverse the folder for navigation (Applies to: this folder only).

**i** This access category is not visible to users if ARM manages list rights automatically.

## Restricted modify

The screenshot shows the 'Change Configuration - File server' window in the ARM Configuration tool. The 'Group Wizard' tab is selected, displaying configuration status and access categories. The 'Restricted Modify' permission is highlighted with a red box.

Category	Full control	Modify	Read & execute	Read	Write	List folder contents	Propagation	Tag
Full control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	fc
Modify	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	md
Restricted Modify	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	mx
Read & execute	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	re
Read	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	r
Write	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	w
List folder contents	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ld
Traverse folder	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ldtf

Restricted modify is a special combination of permissions where users have modify rights to folders and sub-folders but are not able to delete this folder (keep it as parent for inheritance).

Three permissions are assigned:

- Modify (applies to: this folder, subfolders and files)
- Deny Delete (applies to: this folder only)
- Delete (applies to: subfolders and files)



## Define ARM group names

The screenshot shows the 'Change Configuration - File server' window in the SolarWinds Access Rights Manager. The 'Group Wizard' tab is selected, and the 'Configuration Status' section indicates that the configuration is valid. The 'Group-specific characters' section is highlighted with a red box, showing the following settings:

- Global groups:  Local groups:  Universal groups:  List groups:  Delimiter:
- List group Suffix:

The 'Path usage in group names' section is also highlighted, showing the following settings:

- Complete path:
- Path relative to server:  All directories
- Limit to the first  directories:
- Limit to the first  and the last  directories:

The 'Name format' section is also highlighted, showing the following settings:

- 1st Element:  Delimiter:
- 2nd Element:  Delimiter:
- 3rd Element:  Delimiter:
- 4th Element:

The 'Preview' section shows the resulting group name: `g_8GP_Share_Folder1_Folder2_Folder3_Folder4_fc`.

Determine how names of ARM groups are build.

Please note the preview in the bottom section.

Change ARM group names automatically

By default ARM group names are build according to the defined naming convention.

## Option enabled

When changing folder names, ARM-groups are automatically renamed the next time access rights are changed (except list groups).

Users are not able to change the name of the ARM-group in the ARM application.

## Option disabled

When changing folder names, ARM-groups are not automatically renamed.

Users are able to change the name of the ARM-group in the ARM application.

## Blacklist - exclude users and groups from use

ARM Access Rights Manager Configuration

### Change Configuration - File server

Change Configuration srv-8man

**Quick info**

#### Blacklist

The Blacklist allows you to define users and groups whose access rights you will not be able to manage within ARM. You may either search for a specific user name or just enter the SID of an account.

**Resources**

- Global file server configuration
- srv-8man

**Basic Settings** **Group Wizard**

Configure the global Group Wizard settings on the "Global file server configuration" top node. You can configure different settings for subordinated file servers or shares here.

**Configuration Status**

- Group Wizard Settings: Configuration successfully loaded. No group strategy has been chosen yet.
- Configuration Check: The configuration is valid.

**Blacklist**

Credentials for searching 8man-demo\sa-8man

Available users/groups/Well-known SIDs:

Search:

Users  Groups

The blacklist contains the following entries: 39

Internal entries  Custom entries

Name
Administrator
BUILTIN\Account Operators
BUILTIN\Administrators
BUILTIN\Backup Operators
BUILTIN\Domain
BUILTIN\Guests
BUILTIN\Network Configuration Operators
BUILTIN\Power Users
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Print Operators
BUILTIN\Remote Desktop Users
BUILTIN\Replicators

Also search for well-known SIDs. [Restore default entries](#)

Determine which users and groups are excluded from usage within ARM for granting and removing access.

## Add entries to the blacklist

The screenshot shows the 'Change Configuration - File server' window in the ARM Configuration tool. The 'Blacklist' section is expanded, showing a search field with the text 'Credentials for searching 8man-demo\sa-8man'. Below the search field, there are radio buttons for 'Users' and 'Groups', both of which are selected. The search results list various system users and groups, including 'Administrator', 'BUILTIN\Account Operators', 'BUILTIN\Administrators', 'BUILTIN\Backup Operators', 'BUILTIN\Domain', 'BUILTIN\Guests', 'BUILTIN\Network Configuration Operators', 'BUILTIN\Power Users', 'BUILTIN\Pre-Windows 2000 Compatible Access', 'BUILTIN\Print Operators', 'BUILTIN\Remote Desktop Users', and 'BUILTIN\Replicators'. The search field and the search options are highlighted with red boxes and red circles with the numbers 1 and 2, respectively.

1. You can determine which domain is searched based upon the login credentials. By default the credentials from the [basic configuration](#) are used.
2. When searching for users and groups a "live-request" is sent to the Active Directory. This search works independently of existing AD scans. Legacy 8MAN licensing: The search only works in licensed domains.

## Available search options:

- If no domain is entered into the search field, the domain is selected based upon the credentials.
- If a domain is entered (for example: domain2\another.user"), ARM will search that domain (domain2).

ARM Access Rights Manager Configuration

## Change Configuration - File server

Change Configuration srv-8man

**Quick info**

**Blacklist**  
This list shows all users, groups or well-known SIDs that fit your search input and that you can add to the Blacklist.

**Resources**

- Global file server configuration
- srv-8man

**Basic Settings** **Group Wizard**

Configure the global Group Wizard settings on the "Global file server configuration" top node. You can configure different settings for subordinated file servers or shares here.

**Configuration Status**

- Group Wizard Settings: Configuration successfully loaded. No group strategy has been chosen yet.
- Configuration Check: The configuration is valid.

**Blacklist**

Credentials for searching 8man-demo\sa-8man

Available users/groups/Well-known SIDs: 5

The blacklist contains the following entries: 39

Filter: Internal entries Custom entries

Users Groups

Name

- Daniel Araujo (8man-demo\Daniel Araujo)
- Daniel Davidson (8man-demo\Daniel Davidson)
- Daniel Russell (8man-demo\Daniel Russell)
- Danielle Ingram (8man-demo\Danielle Ingram)
- Ghenet Daniel (8man-demo\Ghenet Daniel)

Select all Ctrl+A

Copy Ctrl+C

Add selection

Also search for well-known SIDs.

Restore default entries

Ready Anthony Admin @ localhost

To add a user or group to the blacklist you can:

- Double-click
- Use drag&drop
- Right-click on the object and select from the context menu
- Use the green plus icon

## Remove entries from the blacklist

The screenshot shows the 'Change Configuration - File server' window in the ARM Configuration tool. The 'Blacklist' section is expanded, showing a list of users and groups. The entry 'Daniel Davidson (8man-demo\Daniel Davidson)' is selected, and a context menu is open over it, with the 'Delete' option highlighted. A red 'X' icon is visible in the bottom right corner of the configuration window.

Filter the entries and remove the desired entry by

- right-clicking on the object and selecting from the context menu,
- drag & drop onto the recycle bin icon or
- the red X icon.

Please note that default entries with the "internal" type can not be removed.

## Restore default blacklist entries

The screenshot shows the 'Change Configuration - File server' window in the SolarWinds Access Rights Manager. The window is titled 'Change Configuration - File server' and has a sub-title 'Change Configuration srv-8man'. The main content area is divided into two tabs: 'Basic Settings' and 'Group Wizard'. The 'Group Wizard' tab is active, showing a 'Configuration Status' section with two green checkmarks indicating that the configuration is valid. Below this is the 'Blacklist' section, which is expanded to show a list of available users/groups and a list of current blacklist entries. The 'Available users/groups/Well-known SIDs' list contains 11 entries, and the 'The blacklist contains the following entries:' list contains 40 entries. A 'Restore default entries' button is highlighted in red at the bottom of the blacklist list.

In factory settings the blacklist contains 39 default entries. These are Microsoft built in/predefined accounts and should not be used in conjunction with ARM.

You are able to remove and restore the entries with the green dot. This may be required if you need to remove "Everyone" access rights, for example.

When restoring the blacklist only the removed standard entries are added again. Any individual additional entries remain stored in the blacklist.

"Internal entries" are marked with a lock and gray font and can not be removed.



## Apply a file server change configuration

1. You must confirm changes in the file server change configuration by clicking "Apply".
2. If you click "Back" instead, a warning appears and you can discard all changes if necessary.

## Define file server and share specific change settings

You can configure specific settings for each file server and configured shares:

- the account used to make the changes
- in which domain the ARM groups are stored
- the Group Wizard Settings (access categories, group naming conventions, blacklist)
- how the list rights are managed.

**i** If you do not set any optional Group Wizard settings, the parent level settings will be used.

ARM Access Rights Manager Configuration

## Change Configuration - File server

**Quick info**

**Resources**  
You can set up change configurations and the Group Wizard for each resource.  
Please select a resource to setup its change configuration.

**Resources**

- Global file server configuration
  - srv-8man
  - Organization** 1
  - Projects
  - Templates
  - Users

**Configuration**  
Change Configuration \\srv-8man\Organization

**Group Wizard**

Configure the global Group Wizard settings on the "Global file server configuration" top node.  
You can configure different settings for subordinated file servers or shares here.

Create a configuration different from the parent element 2

Ready Anthony Admin @ localhost

1. Select the desired file server or share in the "Resources" area. How to add a file server is described in the chapter [Add FS scans](#). Newly added file servers and shares do not have a configuration.
2. Create a new configuration.

The screenshot displays the SolarWinds Access Rights Manager (ARM) Configuration window. The main title is "Change Configuration - File server". The interface is divided into several sections:

- Quick info:** A section on the left providing information about configuration status.
- Configuration status:** A section on the left with the text: "These messages deal with operations like loading and saving the configuration."
- Resources:** A tree view on the left showing the hierarchy: "Global file server configuration" (with a gear icon and a "2" above it), "srv-8man", "Organization" (with a gear icon and a "1" above it), "Projects", "Templates", and "Users".
- Change Configuration \\\srv-8man\Organization:** The main content area, titled "Group Wizard", containing:
  - An information icon and text: "Configure the global Group Wizard settings on the 'Global file server configuration' top node. You can configure different settings for subordinated file servers or shares here."
  - Configuration Status:** A section with two green checkmarks: "Group Wizard Settings: Configuration successfully loaded. No group strategy has been chosen yet." and "Configuration Check: The configuration is valid." An "Apply" button is present.
  - Basic Settings:** A section with various options:
    - Enable Group Wizard
    - Simulate changes only (simulation mode)
    - Enable scheduled removing of access rights (Comfort Feature):
      - Earliest run after:  day(s) at 12:00 a.m.
    - Use following domain groups:  local,  global,  universal,  local and global,  Create global groups within the account domain
    - Performs an initial check of the access right changes on the affected resources before additional options will be provided (e.g. Group Wizard usage or the name of access right groups).
  - Access Categories:** A collapsed section.
  - Naming Conventions for ARM Groups:** A collapsed section.
  - Blacklist:** A collapsed section.

ARM shows you how many configurations exist below (arrow with number) and where they are (gear).

## Configure the FS change account

Change Configuration - File server

Change Configuration srv-8man

Basic Settings Group Wizard

Credential for changes 8man-demo\sa-8man

Domain for ARM groups <Refer to domain selection in ARM>

List Rights Configuration

Resources

- Global file server configuration
- srv-8man
  - Organization
  - Projects
  - Templates
  - Users

Ready Anthony Admin @ localhost

Determine which account is used to apply changes to the selected file server resource. If you don't enter credentials these will be requested in the ARM application.

## Determine the domain for ARM groups

The screenshot displays the 'Change Configuration - File server' window in the SolarWinds Access Rights Manager (ARM) application. The window title is 'Access Rights Manager Configuration'. On the left, there is a 'Quick info' section titled 'Domain for ARM groups' with a description: 'This setting defines the domain in which the ARM groups controlling access to this file server are created. This is usually the hosting domain of the file server.' Below this is a 'Resources' tree view showing 'Global file server configuration' expanded to 'srv-8man', which includes sub-items for 'Organization', 'Projects', 'Templates', and 'Users'. The main configuration area has two tabs: 'Basic Settings' (selected) and 'Group Wizard'. Under 'Basic Settings', there is a 'Credential for changes' field set to '8man-demo\sa-8man' and a 'Domain for ARM groups' dropdown menu. The dropdown menu is highlighted with a red box and shows the text '<Refer to domain selection in ARM>'. Below the dropdown is a section for 'List Rights Configuration' which is currently empty. The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Select the domain in which the ARM groups are stored.

If you don't enter a domain, the ARM-groups will automatically be stored in the domain that the user has selected in the ARM application.

## Configure automatic list rights management

**Change Configuration - File server**

Change Configuration srv-8man

**Basic Settings** | **Group Wizard**

Credential for changes: 8man-demo\sa-8man

Domain for ARM groups: <Refer to domain selection in ARM>

**List Rights Configuration**

Manage list rights (List folder content) automatically

Do not allow access right changes below the last level that has list groups enabled

Mode: Direct list group memberships

Configure directory levels:

List groups will be created from level 1 on for 3 levels.

On the further 1 levels list entries will be added only.

Directory level of an access righth change

Also create list groups on the same directory level of an access right change

Protect directories against accidental deletion by an access entry (deny delete) for the list group

Preview for all directory levels

Preview for the level of an access right change

The list right configuration includes several options for determining how ARM automatically ensures that users can navigate to the folders that they have access to.

Compared to Microsoft native tools you can avoid many cumbersome and error prone administrative steps.

ARM Access Rights Manager Configuration

## Change Configuration - File server

Change Configuration srv-8man

**Basic Settings** | Group Wizard

Credential for changes: 8man-demo\sa-8man

Domain for ARM groups: <Refer to domain selection in ARM>

### List Rights Configuration

**Manage list rights (List folder content) automatically**

Do not allow access right changes below the last level that has list groups enabled

Mode: Direct list group memberships

**Configure directory levels:**

List groups will be created from level 1 on for 3 levels.

On the further 1 levels list entries will be added only.

Directory level of an access righth change

Also create list groups on the same directory level of an access right change

Protect directories against accidental deletion by an access entry (deny delete) for the list group

Preview for all directory levels

Preview for the level of an access right change

Ready Anthony Admin @ localhost

Activate the automatic list rights management.

Use the sliders to determine the level of folder depth that ARM manages.

## Level 0

Level 0 is the shared folder (share level). This folder is visible to users based on share rights. An assignment of list rights on this level is not required.

## green levels

ARM creates list groups for every level. The access rights groups become members of list groups.

## blue levels

ARM does not create list groups for these levels. Access groups are provisioned by entering list rights directly into the Access Control List (ACL). This way overall less groups are created and Kerberos token size is minimized. On the other hand more ACL entries are required which may cause file server performance issues.



ARM Access Rights Manager Configuration

## Change Configuration - File server

Change Configuration srv-8man

**Basic Settings** | **Group Wizard**

Credential for changes: 8man-demo\sa-8man

Domain for ARM groups: <Refer to domain selection in ARM>

### List Rights Configuration

**Manage list rights (List folder content) automatically**

Do not allow access right changes below the last level that has list groups enabled

Mode: Direct list group memberships

**Configure directory levels:**

List groups will be created from **level 3** on for 2 levels.

On the further 1 levels list entries will be added only.

**Directory level of an access righth change**

Also create list groups on the same directory level of an access right change

Protect directories against accidental deletion by an access entry (deny delete) for the list group

**Preview for all directory levels**

**Preview for the level of an access right change**

Move the orange slider to exclude folder levels from the automatic creation of list groups. This is useful if users already have list rights to these folder levels.

ARM Access Rights Manager Configuration

## Change Configuration - File server

Change Configuration srv-8man

**Basic Settings** | Group Wizard

Credential for changes: `8man-demo\sa-8man`

Domain for ARM groups: <Refer to domain selection in ARM>

### List Rights Configuration

**Manage list rights (List folder content) automatically**

Do not allow access right changes below the last level that has list groups enabled

Mode: Direct list group memberships

**Configure directory levels:**

List groups will be created from level 3 on for 2 levels.

On the further 1 levels list entries will be added only.

**Directory level of an access righth change**

Also create list groups on the same directory level of an access right change

Protect directories against accidental deletion by an access entry (deny delete) for the list group

Preview for all directory levels

Preview for the level of an access right change

Activate this option to prevent access rights changes with ARM below the lowest "list-rights-level" plus one (for example level 7, as in the screenshot).

You should activate this option to prevent users from gaining access to levels that they are not able to navigate to.

ARM Access Rights Manager Configuration

## Change Configuration - File server

Change Configuration srv-8man

**Basic Settings** | **Group Wizard**

Credential for changes **8man-demo\sa-8man**

Domain for ARM groups <Refer to domain selection in ARM>

### List Rights Configuration

**Manage list rights (List folder content) automatically** **Preview for all directory levels**

Do not allow access right changes below the last level that has list groups enabled

Mode: Direct list group memberships

**Configure**

**Cascade list groups**  
ARM groups will be each added as member to their corresponding list group. The list rights to all upper directory levels will be established by cascading the list groups (each list group is member of the one above).

**Direct list group memberships**  
ARM groups will be each added as member to their corresponding list groups in all upper directory levels to establish list rights to these directories.

On the further **1 levels** list entries will be added only.

**Directory level of an access righth change**

Also create list groups on the same directory level of an access right change

Protect directories against accidental deletion by an access entry (deny delete) for the list group

Preview for the level of an acces right change

Ready Anthony Admin @ localhost

Select a list group mode.

**i** This setting has no impact on Kerberos token size.

The screenshot shows the 'Change Configuration - File server' window in the SolarWinds Access Rights Manager. The 'List Rights Configuration' section is active, showing the following settings:

- Basic Settings:** Credential for changes is `8man-demo\sa-8man`. Domain for ARM groups is set to `<Refer to domain selection in ARM>`.
- List Rights Configuration:**
  - Manage list rights (List folder content) automatically
  - Do not allow access right changes below the last level that has list groups enabled
  - Mode: Direct list group memberships
  - Configure directory levels: List groups will be created from level 3 on for 2 levels. A progress bar shows levels 0-8, with level 3 highlighted in red and level 5 in blue.
  - On the further 1 levels list entries will be added only.
  - Preview for all directory levels: A tree diagram shows a 'Share' folder with subfolders, including 'List group' and 'List entry for ARM group only'.
  - Directory level of an access righth change:**
    - Also create list groups on the same directory level of an access right change
    - Protect directories against accidental deletion by an access entry (deny delete) for the list group
  - Preview for the level of an access right change: A diagram shows a 'List group' folder with an 'ARM Group' icon.

The 'Resources' sidebar on the left shows the 'Global file server configuration' tree with 'srv-8man' selected, containing 'Organization', 'Projects', 'Templates', and 'Users'.

You can use these options to prevent the deletion of folders that are to be retained as parents for inheritance.

**i** It is more beneficial to protect folder levels by assigning "[restricted modify](#)", as these require fewer group memberships.

## Delete a file server- and share-specific change configuration

ARM Access Rights Manager Configuration

## Change Configuration - File server

Change Configuration srv-8man

**Basic Settings** | Group Wizard

Credential for changes 8man-demo\sa-8man

Domain for ARM groups <Refer to domain selection in ARM>

### List Rights Configuration

**Manage list rights (List folder content) automatically**

Do not allow access right changes below the last level that has list groups enabled

Mode: Direct list group memberships

**Configure directory levels:**

List groups will be created from level 3 on for 2 levels.

On the further 1 levels list entries will be added only.

**Directory level of an access righth change**

Also create list groups on the same directory level of an access right change

Protect directories against accidental deletion by an access entry (deny delete) for the list group

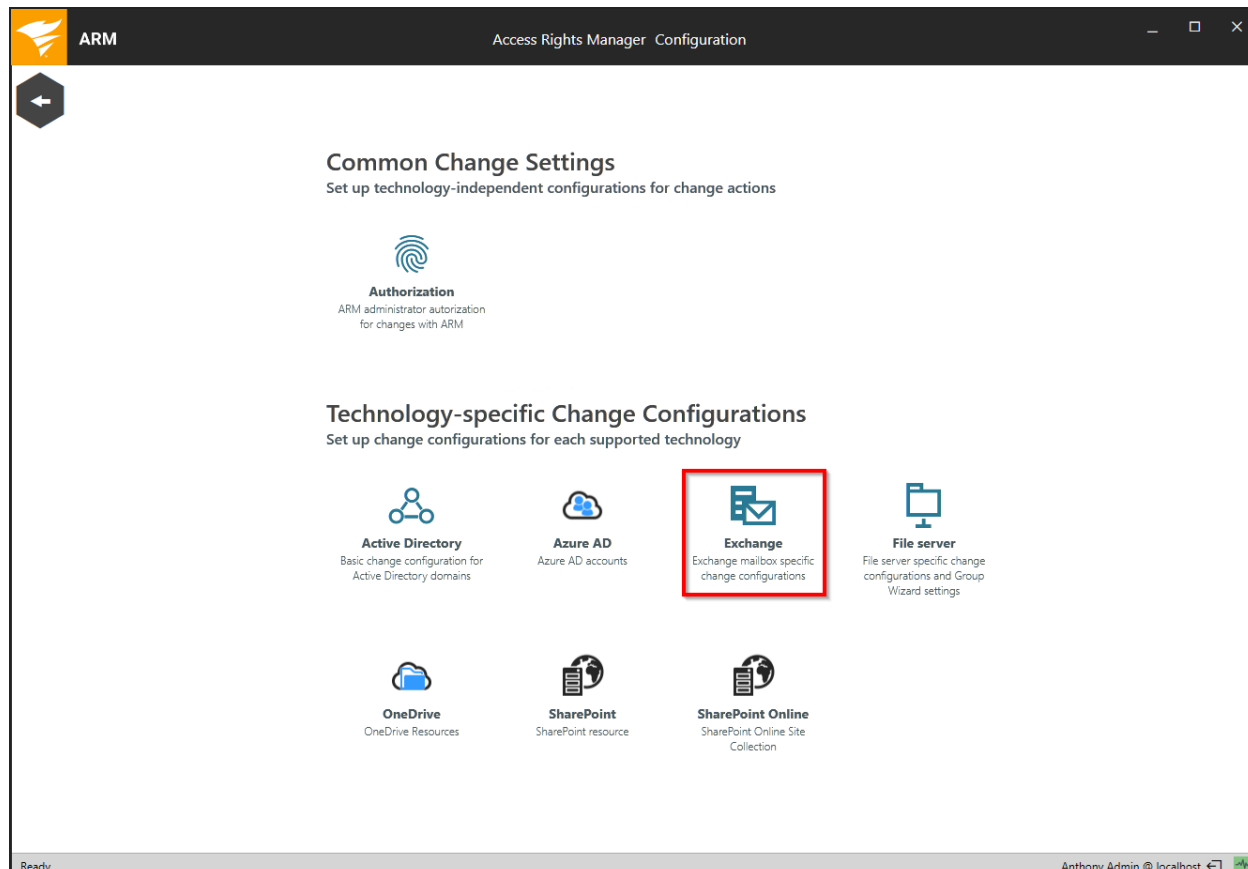
**Preview for all directory levels**

**Preview for the level of an acces right change**

Ready Anthony Admin @ localhost

Click the red X to remove a change configuration.

## Exchange change configuration



Select "Change configuration" from the ARM Configuration application home menu.  
Click "Exchange".

### Create an Exchange change configuration

In order to create an Exchange Change configuration, complete the following steps first:

1. [Create an Exchange Scan configuration.](#)
2. Have ARM complete at least one Exchange scan.

The screenshot shows the 'Change Configuration - Exchange' window in the ARM console. The window title is 'ARM Access Rights Manager Configuration'. On the left, there is a 'Quick info' section with 'Basic Settings' instructions. Below that is a 'Resources' list containing two Exchange servers: '8man-demo.com' and 'SRV-Exchange.8man-demo.L...'. A red box highlights the 'SRV-Exchange.8man-demo.L...' entry, with a red circle containing the number '1' next to it. In the center of the main area, a message states 'This element has no configuration yet.' with a 'Create new configuration' link. A red box highlights a blue plus icon in a circle, with a red circle containing the number '2' next to it.

1. Select an (already scanned) Exchange server.
2. Click the plus icon.

## Customize an Exchange change configuration

1. Enter the desired credentials to make changes to Exchange. Please note additional information in the following sections: [Service accounts](#).  
If you don't enter any credentials, ARM-users will be prompted to enter this information for every change.
2. Specify the settings for creating a mailbox (email-enable an user account).

**i** For creating mailboxes for Exchange Online please see [Create a mailbox in Exchange Online \(assign an Office 365 license\)](#) and [Create a user account in Azure Active Directory](#).



Determine how email addresses for mailing lists are built.


### Option activated:

E-Mail-Addresses are automatically built based on Exchange policies. When activating emails for mailing lists the email address can not be changed.

### Option deactivated:

Email addresses are generated based upon the defined settings. For example, you can use the OU instead of the group name. You may define email addresses differently than allowed by default Exchange policies.

When activating email of the distribution group, the email address can be changed.

 Creating distribution groups in Exchange Online is not supported.

ARM Access Rights Manager Configuration

## Change Configuration - Exchange

Change Configuration SRV-Exchange.8man-demo.local

### Quick info

#### Access Category Tag

Here you can configure access categories that will be used when modifying access rights in ARM. Enabled categories you will find in the "Modify access rights" represented by columns or rows.

There you can easily change the access rights of users and groups via drag and drop.

For each category you can also define,

- which indicator should be added to the default names of related ARM groups
- whether administrators as well as
- all non-administrators can use it in ARM.

### Resources

- Exchange
  - 8man-demo.com
  - SRV-Exchange.8man-demo.L...

### Basic Settings

Credential for changes [optional](#)

#### Enable mailbox

#### Distribution group - enable

#### Mailbox Access Categories

Administrators	Everyone else	Category
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full Access
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Send As
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Receive As
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Send On Behalf

#### Distribution Groups Access Categories

#### Mailbox Settings

Determine which mailbox access categories are available to ARM users.

**i** The category "Receive As" is not supported by Exchange Online.

ARM Access Rights Manager Configuration

## Change Configuration - Exchange

Change Configuration SRV-Exchange.8man-demo.local

**Quick info**

**Access Category Tag**  
Here you can configure access categories that will be used when modifying access rights in ARM. Enabled categories you will find in the "Modify access rights" represented by columns or rows.  
There you can easily change the access rights of users and groups via drag and drop.  
For each category you can also define,  
- which indicator should be added to the default names of related ARM groups  
- whether administrators as well as  
- all non-administrators can use it in ARM.

**Resources**

- Exchange
- 8man-demo.com
- SRV-Exchange.8man-demo.L...

**Basic Settings**

Credential for changes [optional](#)

Enable mailbox

Distribution group - enable

Mailbox Access Categories

**Distribution Groups Access Categories**

Category	Send As	Receive As	Send On Behalf
Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Everyone else	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Mailbox Settings**

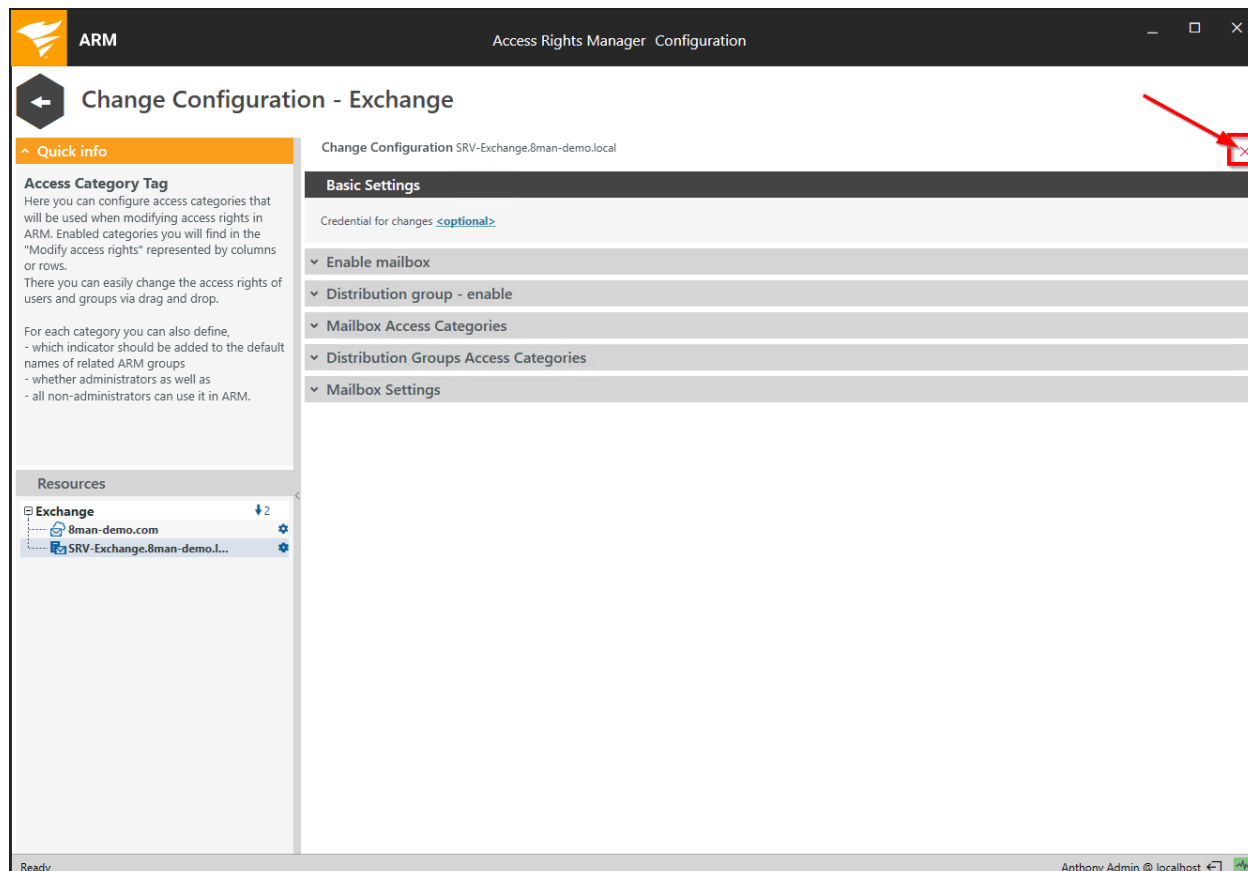
Mailbox Size

Quota increase step

1,024 MB On mailbox size (quota) increase provide the user with 1.00 GB additional space

1. Determine which distribution group access categories are available to ARM users.
2. Determine the increments that will be used to increase mailbox size.

## Delete an Exchange change configuration



ARM Access Rights Manager Configuration

### Change Configuration - Exchange

Change Configuration SRV-Exchange.8man-demo.local

**Quick info**

**Access Category Tag**  
Here you can configure access categories that will be used when modifying access rights in ARM. Enabled categories you will find in the "Modify access rights" represented by columns or rows.  
There you can easily change the access rights of users and groups via drag and drop.  
For each category you can also define,  
- which indicator should be added to the default names of related ARM groups  
- whether administrators as well as  
- all non-administrators can use it in ARM.

**Resources**

- Exchange
  - 8man-demo.com
  - SRV-Exchange.8man-demo.L...

**Basic Settings**

Credential for changes [optional](#)

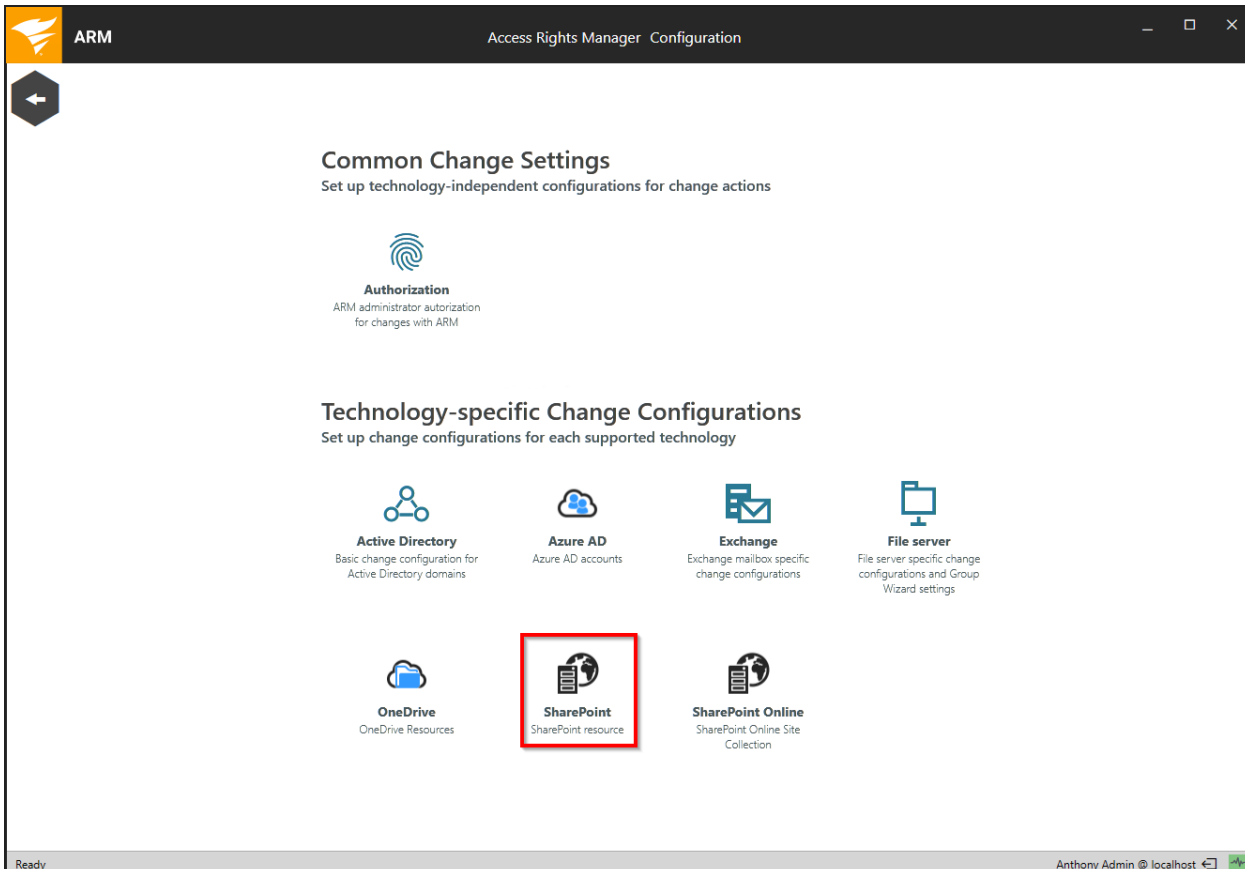
- Enable mailbox
- Distribution group - enable
- Mailbox Access Categories
- Distribution Groups Access Categories
- Mailbox Settings

Ready Anthony Admin @ localhost


Click the red cross.

If you delete an Exchange change configuration you lose all customized settings and can create a new configuration with default settings.

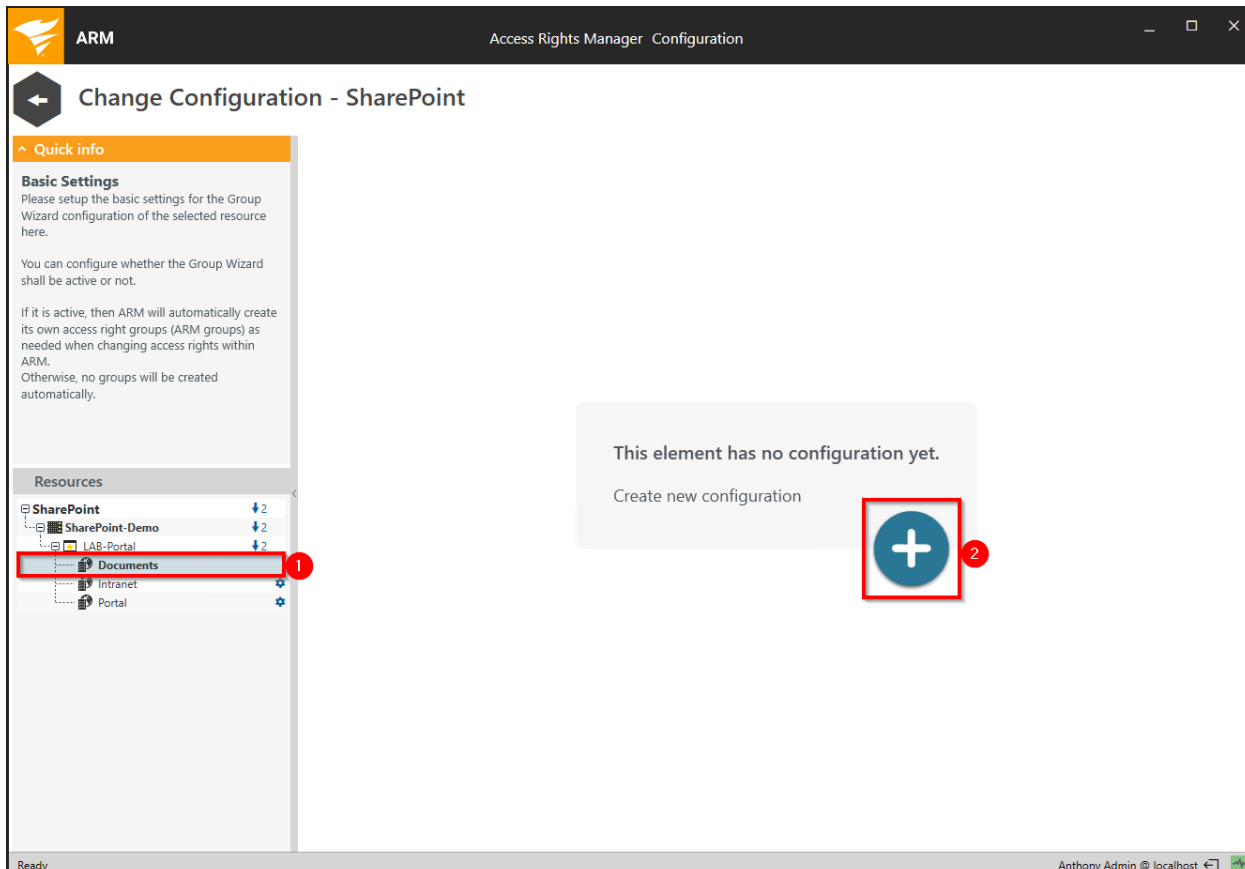
# SharePoint change configuration



In the ARM Configuration application, navigate to "Change Configuration" -> "SharePoint".

 You must have run at least one SharePoint scan to create a change configuration.

## Add a SharePoint change configuration



The screenshot shows the 'Change Configuration - SharePoint' interface. On the left, under 'Resources', the 'Documents' resource is selected, highlighted with a red box and a red circle containing the number 1. The main area displays a message: 'This element has no configuration yet.' Below this message is a 'Create new configuration' link and a plus icon (+) inside a blue circle, which is also highlighted with a red box and a red circle containing the number 2.

1. Select a SharePoint resource.
2. Click the plus icon.

## Modify a SharePoint change configuration

**Quick info**

**Access Category Tag**  
Here you can configure access categories that will be used when modifying access rights in ARM. Enabled categories you will find in the "Modify access rights" represented by columns or rows.  
There you can easily change the access rights of users and groups via drag and drop.  
For each category you can also define,  
- which indicator should be added to the default names of related ARM groups  
- whether administrators as well as  
- all non-administrators can use it in ARM.

**Resources**

- SharePoint
  - SharePoint-Demo
  - LAB-Portal
  - Documents
    - Intranet
    - Portal

**Change Configuration Documents**

**Basic Settings**

Credential for changes (optional):

**Access Categories**

Category	Administrators	Everyone else
Approve	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Contribute	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Design	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage Hierarchy	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Restricted Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Group Wizard**

1. Specify which credentials are used to make changes to the SharePoint resource. If you do not specify any, the ARM users are prompted for each change. You must enter credentials if you want to enable the SharePoint Group Wizard.
2. Determine which access categories are available for ARM users to change access rights. Define a set for ARM administrators and another for all ARM modify user roles (See also: [manage ARM users](#)).

The screenshot shows the 'Change Configuration - SharePoint' window in the Access Rights Manager (ARM) application. The window title is 'Access Rights Manager Configuration'. The main content area is titled 'Change Configuration Documents'. Under the 'Basic Settings' section, the 'Group Wizard' is expanded, and the 'Enable Group Wizard' checkbox is checked. A red box highlights this checkbox with a red '1'. Below this, a dropdown menu is open, showing a list of systems to manage ARM resource groups. The 'Documents (SharePoint-Demo)' option is selected and highlighted with a red box and a red '2'. Other options include 'Intranet (SharePoint-Demo)', 'Portal (SharePoint-Demo)', and 'Teamwebsite (https://8mandemo.sharepoint.com)'. The 'Documents (SharePoint-Demo)' option has a warning icon and the text 'No credentials set in Change Configuration'. An 'Apply' button is visible at the bottom right of the dropdown menu.

### 1. Option enabled

ARM automatically creates permission groups when assigning permissions using drag & drop in the ARM application.

### 2. Determine where the permission groups are stored.



ARM Access Rights Manager Configuration

## Change Configuration - SharePoint

Change Configuration Documents

### Basic Settings

Credential for changes `8man-demo\sa-8man`

### Access Categories

#### Group Wizard

Enable Group Wizard

Please select the system in which ARM resource groups shall be managed:

Documents (SharePoint-Demo)

Create a new SharePoint group

Owner: own

- SharePoint Online Accounts (0)
- SharePoint Accounts (1)
- Documents Owners (SharePoint-Demo) Name: Documents Owners Display Name: Documents Owners

Resources

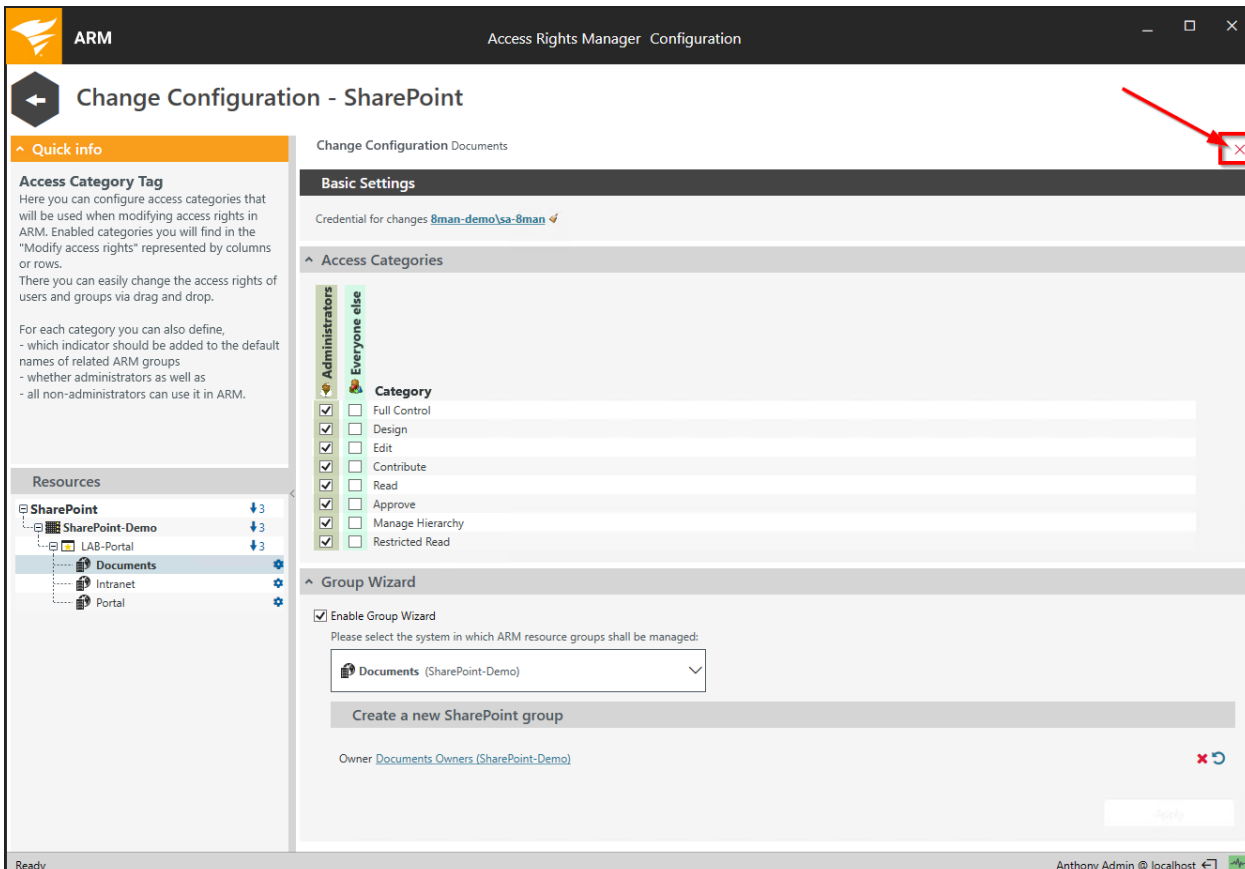
- SharePoint
  - SharePoint-Demo
    - LAB-Portal
    - Documents
    - Intranet
    - Portal

SharePoint groups must have an owner. Use the search to specify a SharePoint account which will be the owner of the automatically created permission groups.

**i** Enter a space in the search box to get a list of all available accounts.

Click "Apply" to save your SharePoint Group Wizard settings.

## Delete a SharePoint change configuration



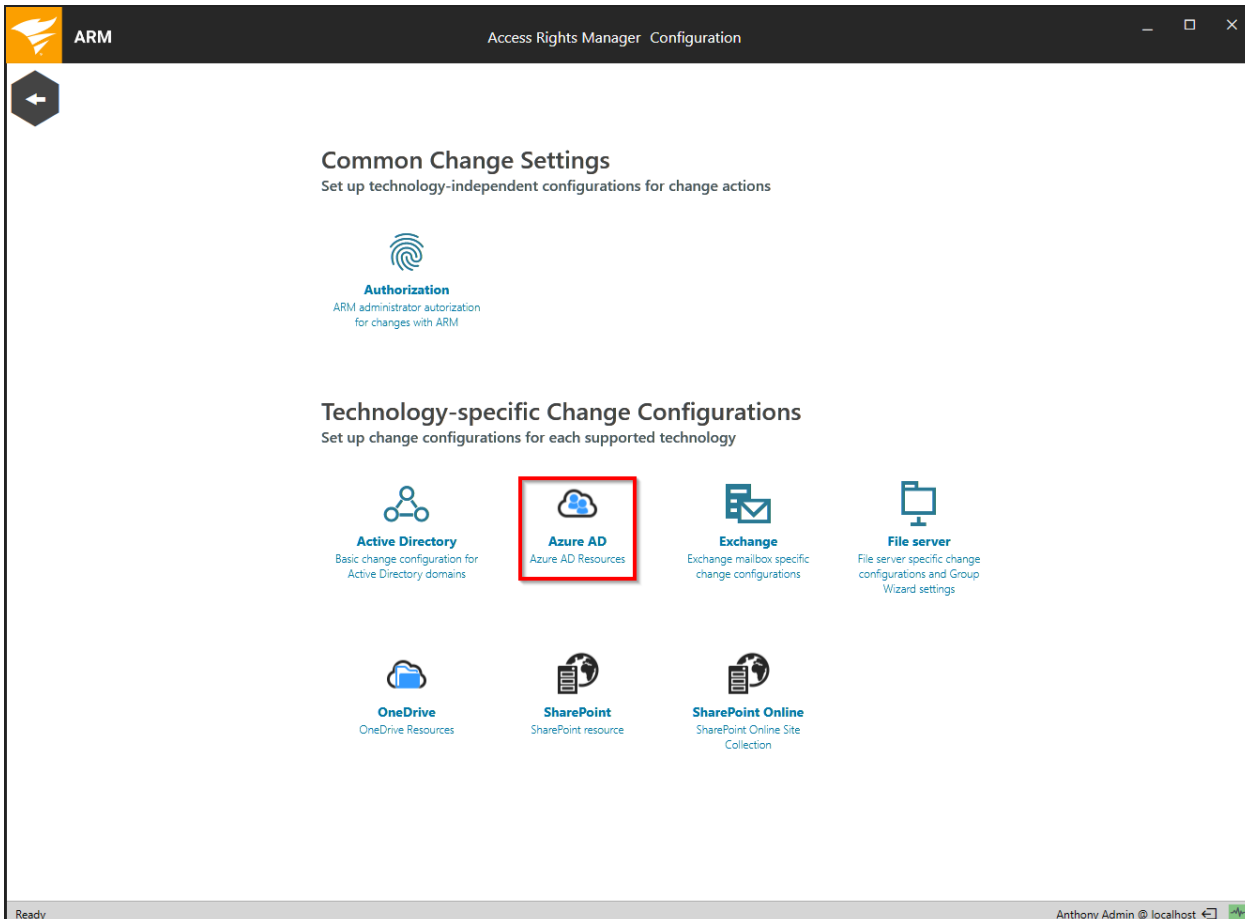
The screenshot displays the SolarWinds Access Rights Manager (ARM) Configuration interface. The main window title is "Change Configuration - SharePoint". The interface is divided into several sections:

- Quick info:** Provides instructions on how to configure access categories and change rights of users and groups.
- Resources:** A tree view showing the hierarchy of resources, including SharePoint, SharePoint-Demo, LAB-Portal, Documents, Intranet, and Portal.
- Change Configuration Documents:** The main configuration area, which includes:
  - Basic Settings:** Shows the credential for changes as "8man-demo\sa-8man".
  - Access Categories:** A list of categories with checkboxes for various permissions. The "Everyone else" category is selected, and its permissions are listed: Full Control, Design, Edit, Contribute, Read, Approve, Manage Hierarchy, and Restricted Read.
  - Group Wizard:** A section for creating new groups, with "Enable Group Wizard" checked and "Documents (SharePoint-Demo)" selected as the system for group management.

A red arrow in the top right corner of the window points to the close button (X).

Delete a SharePoint change configuration.

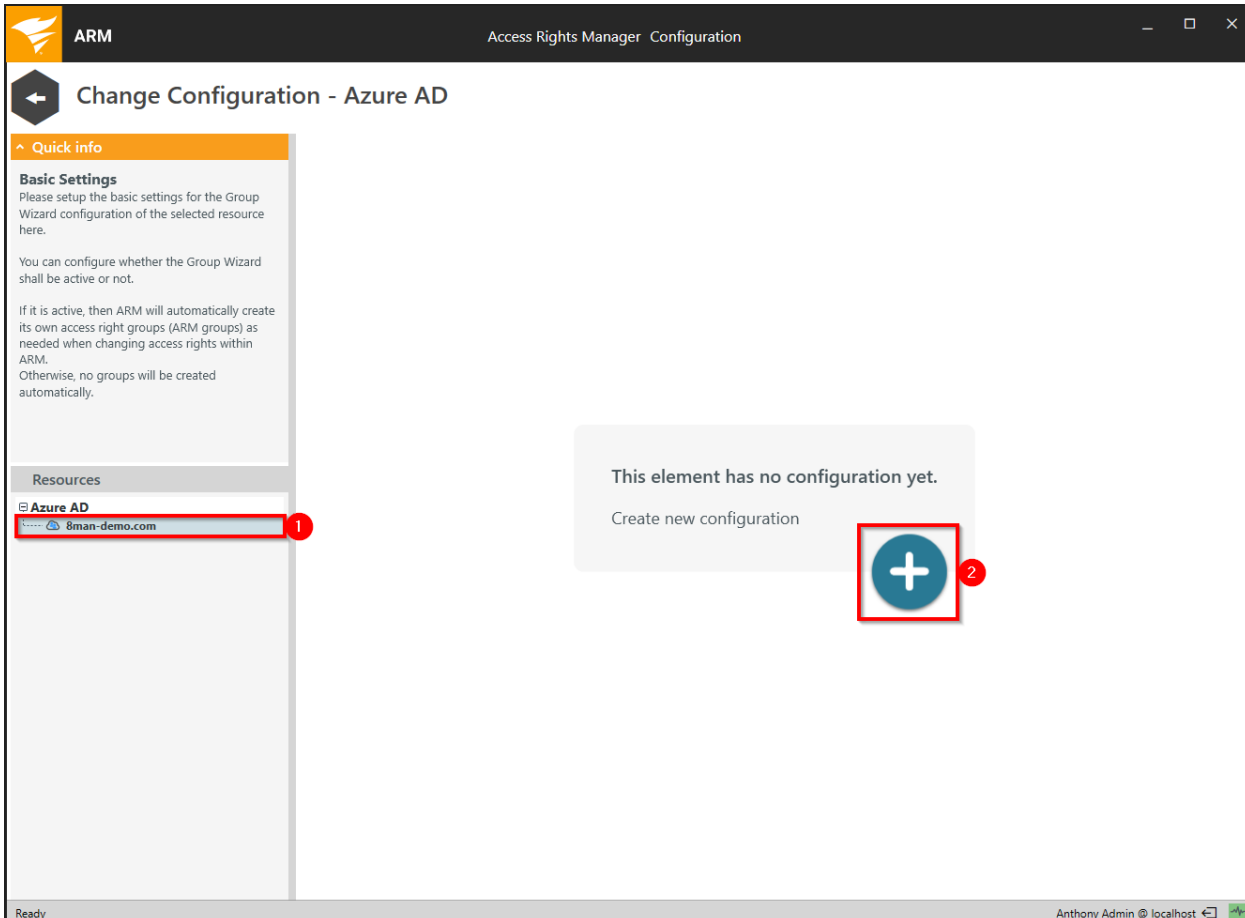
# Azure Active Directory (AAD) change configuration



In the ARM configuration application, navigate to Change Configuration > Azure AD.

**i** You must have run at least one AAD scan to create a change configuration.

## Add an AAD change configuration



ARM Access Rights Manager Configuration

### Change Configuration - Azure AD

**Quick info**

**Basic Settings**  
Please setup the basic settings for the Group Wizard configuration of the selected resource here.

You can configure whether the Group Wizard shall be active or not.

If it is active, then ARM will automatically create its own access right groups (ARM groups) as needed when changing access rights within ARM.  
Otherwise, no groups will be created automatically.

**Resources**

- Azure AD
- 8man-demo.com

This element has no configuration yet.

Create new configuration

Ready Anthony Admin @ localhost

1. Select an AAD resource.
2. Click the plus icon.

## Modify an AAD change configuration

ARM Access Rights Manager Configuration

### Change Configuration - Azure AD

**Quick info**

**Credential for changes**  
This credential will be used for any changes being made within the selected resource.  
If no credential were set here, they will be requested later whenever they are needed.

**Resources**

- Azure AD
- 8man-demo.com

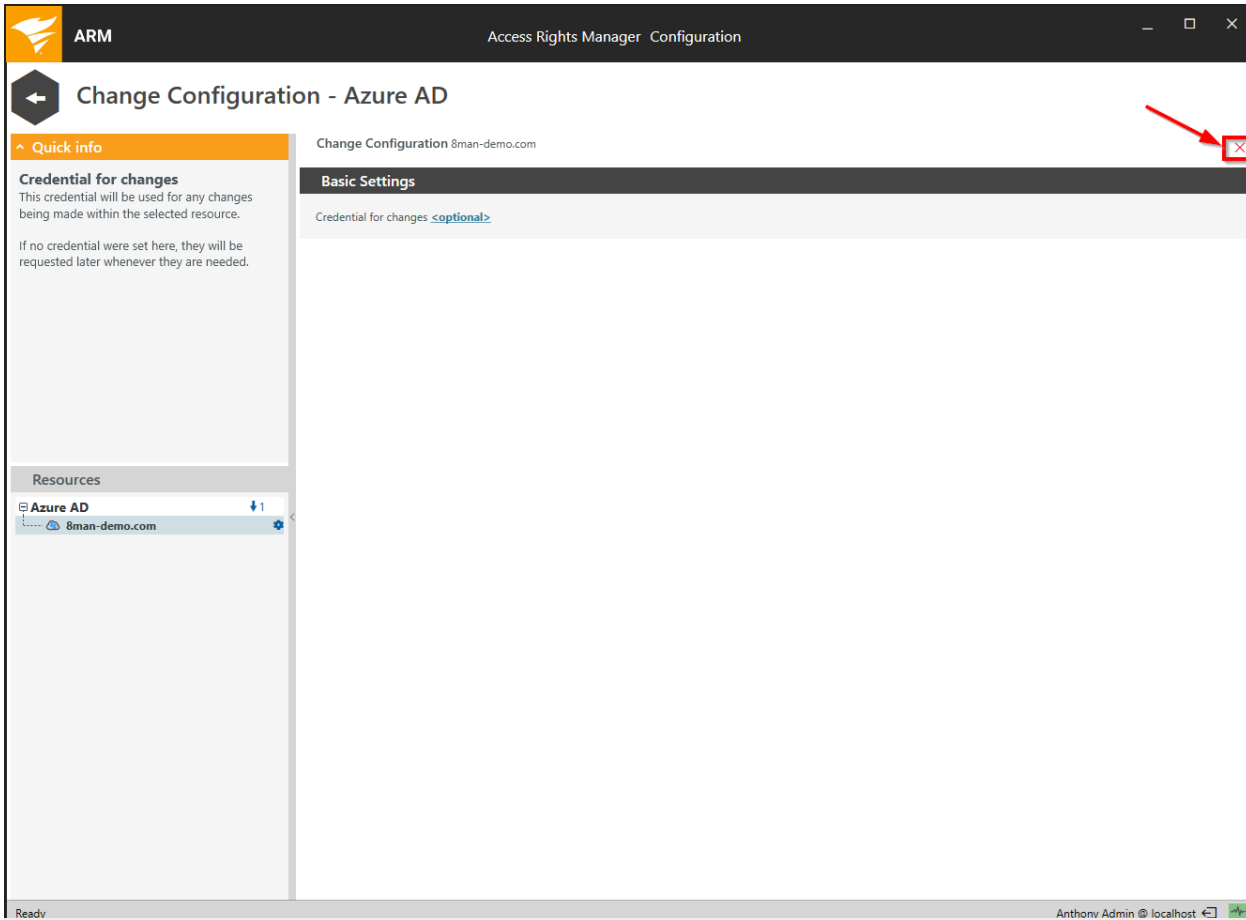
**Basic Settings**

Credential for change: **<optional>**

Ready Anthony Admin @ localhost

Specify which credentials are used to make changes to the AAD resource. If you do not specify any, ARM users are prompted for each change.

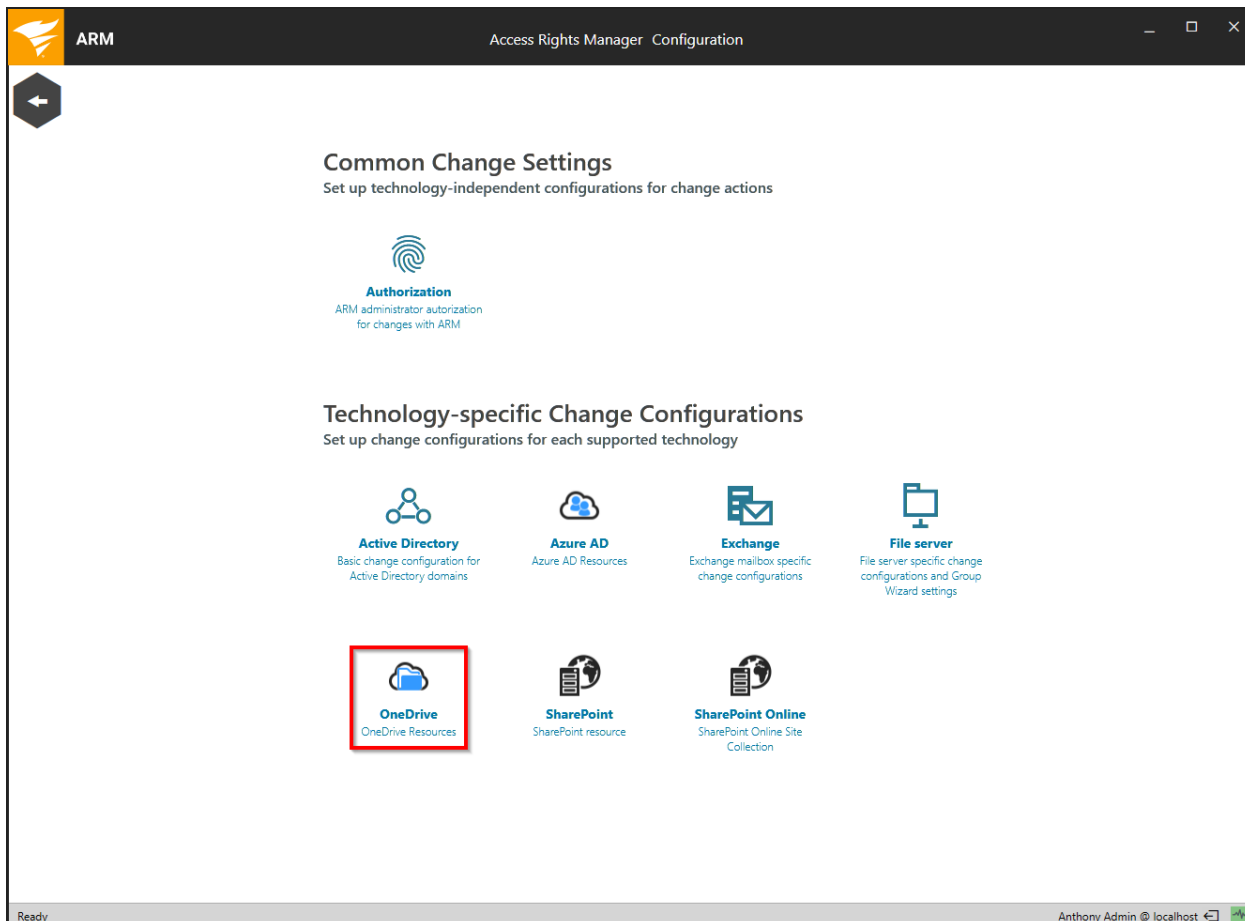
## Delete an AAD change configuration



The screenshot shows the ARM Configuration interface. The main heading is "Change Configuration - Azure AD". On the left, there is a "Quick info" section with the title "Credential for changes" and a "Resources" section listing "Azure AD" with a sub-item "8man-demo.com". The main content area is titled "Basic Settings" and contains a link for "Credential for changes" with the text "\_optional>". A red arrow points to a red "X" icon in the top right corner of the configuration card, which is used to delete the configuration.

Click on the red cross to delete an AAD Change configuration.

# OneDrive change configuration



In the ARM configuration, navigate to Change Configuration > OneDrive.

**i** You must have run at least one OneDrive scan to create a change configuration.



## Add a OneDrive change configuration

The screenshot shows the 'Change Configuration - OneDrive' window in the Access Rights Manager (ARM) Configuration tool. The window title is 'ARM Access Rights Manager Configuration'. The main content area is titled 'Change Configuration - OneDrive'. On the left, there is a 'Quick info' section with the following text: 'Resources You can set up change configurations and the Group Wizard for each resource. Please select a resource to setup its change configuration.' Below this is a 'Resources' list containing one item: 'OneDrive 8mandemo-my.sharepoint...'. A red box highlights this resource, with a red circle containing the number '1' next to it. In the center of the main area, there is a message: 'This element has no configuration yet. Create new configuration'. Below this message is a blue circular button with a white plus sign, which is also highlighted with a red box and a red circle containing the number '2' next to it. The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

1. Select a OneDrive resource.
2. Click the plus icon.

## Modify a OneDrive change configuration

ARM Access Rights Manager Configuration

### Change Configuration - OneDrive

Change Configuration 8mandemo-my.sharepoint.com

**Quick info**

**Access Category Tag**  
Here you can configure access categories that will be used when modifying access rights in ARM. Enabled categories you will find in the "Modify access rights" represented by columns or rows. There you can easily change the access rights of users and groups via drag and drop.

For each category you can also define,  
- which indicator should be added to the default names of related ARM groups  
- whether administrators as well as  
- all non-administrators can use it in ARM.

**Resources**

OneDrive  
8mandemo-my.sharepoint...

**Basic Settings**

Credential for change:  1

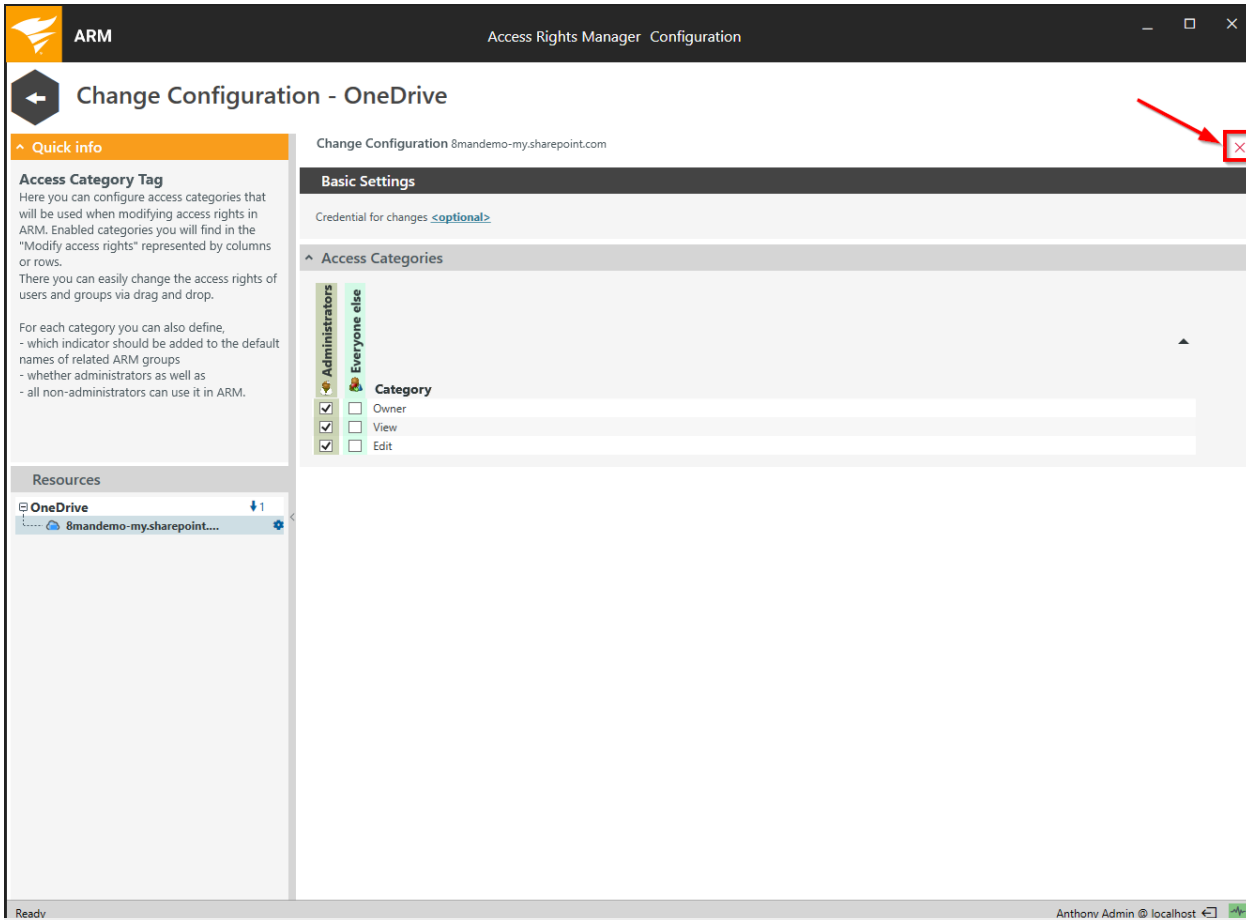
**Access Categories**

Category	Owner	View	Edit
Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Everyone else	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Ready Anthony Admin @ localhost

1. Specify which credentials are used to make changes to the OneDrive resource. If you do not specify any, the ARM users are prompted for each change.
2. Determine which access categories are available for ARM users to change access rights. Define a set for ARM administrators and another for all ARM modify user roles (See also: [manage ARM users](#)).

## Delete a OneDrive change configuration



The screenshot shows the 'Change Configuration - OneDrive' page in the Access Rights Manager (ARM) Configuration interface. The page title is 'Change Configuration - OneDrive' and the URL is 'Change Configuration 8mandemo-my.sharepoint.com'. A red arrow points to a red 'X' icon in the top right corner of the configuration card, indicating the delete action.

**Quick info**

**Access Category Tag**  
Here you can configure access categories that will be used when modifying access rights in ARM. Enabled categories you will find in the "Modify access rights" represented by columns or rows. There you can easily change the access rights of users and groups via drag and drop.

For each category you can also define,

- which indicator should be added to the default names of related ARM groups
- whether administrators as well as
- all non-administrators can use it in ARM.

**Resources**

**OneDrive** ↓ 1

- 8mandemo-my.sharepoint...

**Basic Settings**

Credential for changes [optional](#)

**Access Categories**

Administrators	Everyone else	Category
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Owner
<input checked="" type="checkbox"/>	<input type="checkbox"/>	View
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit

Click on the red cross to delete a OneDrive change configuration.

# Data owner

The screenshot displays the ARM Configuration window. At the top, there are three summary cards:

- Server Status** (License Information): Logged in users: 1, Licensed Active user accounts: 0.
- Jobs** (Summary): 91 Scans, 7 Reports, 69 Changes, 130 More, 7 Scheduled, 290 Succeeded, 0 Executing, 0 Failed.
- Collectors** (Configuration): 1 Connected, 1 Configured in Total, All Collectors are Operational.

Below the summary cards is a 'Filter' section. The main area contains 12 configuration tiles:

- Scans**: Resource Configurations, Logga, File Server CSV Import
- Open Order**: Open Order Resource Descriptions
- User Management**: User Management, Role Management
- Data Owner** (highlighted): Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**: License Information, Server Status
- Jobs Overview**: Job Status, Job Categories
- Alerts**: Activate/Deactivate Alert Sensors
- Change Configuration**: Common Change Settings, Technology-specific Change Configurations
- Scripting**: Scripting configuration for change actions
- Views & Reports**: Views & Reports, Blacklist for Views & Reports
- Server**: Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**: ARM Server, SQL Server, Configuration Status

The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Data Owners, from an ARM perspective are persons or roles in an organization that know, which employees need access to specific resources to do their jobs.

You create organizational categories in the data owner configuration. You can determine which users are assigned the Data Owner role and which rights they can assign.

# Create organizational categories

The screenshot shows the 'Data Owner configuration' for the 'Europe' category. The 'Organizational Categories' sidebar on the left is highlighted with a red box and shows a tree structure under '8MAN Demo Company' with sub-categories: Finance, Human Resources, Marketing, Sales, Asia, Europe (selected), France, Germany, and Great Britain.

The main area is titled 'Europe' and contains the following sections:

- Data Owners:** A table with columns 'Name', 'Inherited from', and 'User role'. It lists two entries: 'David DO Sales (... 8MAN Demo Compan...)' and 'David DO Manag... 8MAN Demo Company', both with the role 'Data Owner'.
- Requesters:** A table with columns 'Name', 'Inherited from', and 'User role'. It lists two entries: 'Emily Employ...' and 'Henry HR (8m... 8MAN Demo Com...', both with the role 'Requester (employee)'.
- Resources:** A table with columns 'Name', 'Alias', 'Inherited from', and 'Access'. It lists resources under three categories:
  - Active Directory (2):** 'Demo Groups (OU=Demo Groups,DC=8man-de-...' and 'Demo Users (OU=Demo Users,DC=8man-demo-...'.
  - File server (3):** 'France (\srv-8man\Organization\Sales\Europe\Fr...', 'Germany (\srv-8man\Organization\Sales\Europe...', and 'Great Britain (\srv-8man\Organization\Sales\Eur...'.
  - Template (2):** 'Sales - Create new group (8man)' and 'Sales - Create new user (8man)'.
- User & Group selection:** A search interface for users in the '8man-demo.local' domain. It lists several users including 'Caroline Berggren', 'Domain Users', 'Emily Employee', 'Ludvig Karlsson', and 'Marketing'.
- Resource selection:** A search interface for resources, listing categories like 'Active Directory', 'File server', 'Exchange', 'Template', 'Hardware', 'Software', 'SharePoint Online', 'SharePoint', 'Easy Connect - CSV', 'Easy Connect - SQL', 'Azure AD', 'OneDrive', and 'SAP Connector'.

You use the organizational categories to bundle resources in containers that the data owners manage. Create structures and hierarchies similar to your companies org chart. You can add a description to all organizational categories.

The screenshot displays the 'Data Owner configuration' for the 'Europe' organizational category. The interface is divided into several sections:

- Organizational Categories:** Located on the left, it shows a tree view with categories like Finance, Human Resources, Marketing, Sales, Asia, Europe, France, Germany, and Great Britain. A context menu is open over 'Europe', showing 'New', 'Edit', and 'Delete' options.
- Data Owners:** A table with columns for Name, Inherited from, and User role. It lists David DO Sales and David DO Manag...
- Requesters:** A table with columns for Name, Inherited from, and User role. It lists Emily Employ... and Henry HR (8m...).
- Resources:** A table with columns for Name, Alias, Inherited from, and Access. It lists Active Directory, File server, and Template resources.
- User & Group selection:** A panel on the right showing a search bar and a list of users and groups.
- Resource selection:** A panel on the right showing a search bar and a list of resource types like Active Directory, File server, Exchange, etc.

Create as many organizational categories as you like. You can do this by using the symbols on the top or by right-clicking and using the context menu.

Move the organizational categories with drag & drop.

The screenshot shows the 'Data Owner configuration' for the 'Europe' organizational category. The interface is divided into several sections:

- Organizational Categories:** A search bar with 'Include content' checked (highlighted in red). Below it is a tree view of categories: 8MAN Demo Company, Finance, Human Resources, Marketing, Sales, Asia, Europe (selected), France, Germany, and Great Britain.
- Data Owners:** A table with columns: Name, Inherited from, User role. It lists David DO Sales and David DO Manag...
- Requesters:** A table with columns: Name, Inherited from, User role. It lists Emily Employ... and Henry HR (8m...).
- Resources:** A table with columns: Name, Alias, Inherited from, Access. It lists Active Directory (2), File server (3), and Template (2) entries.
- User & Group selection:** A search bar and a list of users/groups including Caroline Berggren, Domain Users, Emily Employee, and Ludvig Karlsson.
- Resource selection:** A search bar and a list of resource types including Active Directory, File server, Exchange, Template, Hardware, Software, SharePoint Online, SharePoint, Easy Connect - CSV, Easy Connect - SQL, Azure AD, OneDrive, and SAP Connector.

Search the organizational categories.

**Option "Include content" deactivated:**

The search is only applied to names and descriptions of the organizational category.

**Option "Include content" activated:**

The search also includes Data Owners and resources.

## Assign a Data Owner to an organizational category

The screenshot shows the 'Data Owner configuration' window for the 'Sales' category. The interface is divided into three main sections: 'Data Owners', 'Requesters', and 'Resources'. Each section has a search and filter bar and a 'Show inherited entries' button. The 'Data Owners' and 'Requesters' sections currently show 'No Data Owners to show...' and 'No requesters to show...' respectively. The 'Resources' section shows 'No resources to show...'. On the right side, there is a 'User & Group selection' panel with a search bar containing 'david' and a list of results. A red arrow points from the search results to the 'Data Owners' section. The 'User & Group selection' panel also includes a 'Resource selection' section with a search bar and a list of resources.

1. Use the search and filter options to find the desired users and groups.
2. Use drag & drop to add the selected entries as data owners.



The screenshot shows the 'Data Owner configuration' window in the ARM interface. A modal dialog box titled 'Insert accounts into ARM user management' is displayed. The dialog contains the following information:

**1 account could not be configured as Data Owners**  
 Accounts cannot be configured as Data Owner unless they are part of the user management

List of accounts that will be added as Data Owner

Account	State
Augustyn Symanski (8man-demo)Augustyn Sy...	Account will be added automatically to the use...

Do you want ARM to automatically apply the necessary user role to the pending accounts?  
 The required user role "Data Owner" will be applied to the accounts. Afterwards, these accounts will be added to the organizational category.

Buttons: Apply, Close

Data Owners must have either a "change" or a "read" user role in the [ARM user management](#).

If you want to assign Data Owners that do not own the required role, then this the dialogue box is shown. When clicking on "Apply" the required change role is assigned to the user. You can change the role afterwards in the [ARM user management](#).

**i** ARM-Admin roles can not be configured as Data Owners.

The screenshot displays the 'Data Owner configuration' window for the 'Europe' category. The 'Data Owners' table is as follows:

Name	Inherited from	User role
David DO Sales (8man-de...	8MAN Demo Company/Sales	Data Owner

The 'Requesters' section is empty, displaying 'No requesters to show...'. The 'Resources' section is also empty, displaying 'No resources to show...'. The 'User & Group selection' sidebar shows the domain '8man-demo.local' and a list of users including Augustyn Symanski and David DO Sales. The 'Resource selection' sidebar lists various resources such as Active Directory, File server, Exchange, Template, Hardware, Software, SharePoint Online, SharePoint, Easy Connect - CSV, Easy Connect - SQL, Azure AD, OneDrive, and SAP Connector.

### Hierarchy rule:

Data Owners are able to manage the assigned organizational category and all sub-categories.

1. You can activate the option "Show inherited entries".
2. The column "inherited from" shows the origin.

## Assign resources to an organizational category

The screenshot shows the 'Data Owner configuration' window for the 'Europe' organizational category. The interface is divided into several sections:

- Organizational Categories:** A sidebar on the left with a search bar and a list of categories including 8MAN Demo Company, Finance, Human Resources, Marketing, Sales, Asia, and Europe (selected).
- Data Owners:** A table with columns for Name, Inherited from, and User role. It shows one entry: David DO Sales (8man-de...) with an inherited role of 8MAN Demo Company/Sales and a user role of Data Owner.
- Requesters:** A section that is currently empty, displaying 'No requesters to show...'
- Resources:** A section that is currently empty, displaying 'No resources to show...'
- User & Group selection:** A sidebar on the right with a domain dropdown set to '8man-demo.local' and a list of users including Augustyn Symanski and David DO Sales.
- Resource selection:** A sidebar on the right, highlighted with a red box, containing a search bar and a list of resources: Active Directory, File server, Exchange, Template, Hardware, Software, SharePoint Online, SharePoint, Easy Connect - CSV, Easy Connect - SQL, Azure AD, OneDrive, and SAP Connector.

Select the desired resource and add it to the organizational category via drag & drop or by double-clicking on it.

**i** You can only add resources which have been scanned.

Open order resources such as "template", "hardware" or "software" can only be added if:

- you have the required license
- you have imported an open order configuration.

The screenshot shows the 'Data Owner configuration' for 'Europe' in the Access Rights Manager. The interface is divided into several sections:

- Organizational Categories:** A sidebar on the left showing a tree view of categories like Finance, Human Resources, Marketing, Sales, Asia, and Europe.
- Data Owners:** A table with columns for Name, Inherited from, and User role. One entry is visible: 'David DO Sales (8man-de...)' under '8MAN Demo Company/Sales' with the role 'Data Owner'.
- Requesters:** A section that currently displays 'No requesters to show...'
- Resources:** A section with a table listing resources. One resource is shown: 'File server (1)' with the path 'Sales (\srv-8man\Organization\Sales)'. A red box highlights the icons for this resource, with numbered callouts:
  - 1: Remove resource icon (X)
  - 2: Assign aliases and description icon (ABC)
  - 3: Enable/disable re-certification icon (refresh)
  - 4: Enable/disable orderability icon (list)
  - 5: Enable/disable visibility icon (eye)
  - 6: Enable/disable changeability icon (pencil)
- User & Group selection:** A section on the right for selecting users and groups, showing a search bar and a list of users like 'Augustyn Symanski' and 'David DO Sales'.
- Resource selection:** A section on the right for selecting resources, showing a search bar and a tree view of resources under 'Active Directory' and 'File server', including 'Organization', 'Development', 'Facility Management', 'Finance', 'Human Resources', 'Management', 'Marketing', 'Production', 'Research', 'Sales', 'Projects', 'Templates', and 'Users'.

Select a resource to perform the following functions in the flyout:

1. Remove resource.
2. Assign aliases and description to simplify ordering in GrantMA.
3. Enable/disable re-certification. To be able to re-certificate a resource, visibility (5) and changeability (6) is also necessary.
4. Enable/disable orderability in GrantMA. To be able to order a resource, visibility (5) and changeability (6) is also necessary.
5. Enable/disable visibility.
6. Enable/disable changeability.

The screenshot displays the 'Data Owner configuration' for the 'Sales' organizational category. The interface is divided into several sections:

- Organizational Categories:** A sidebar on the left showing a hierarchy: 8MAN Demo Company > Finance > Human Resources > Marketing > Sales > Asia > Europe.
- Sales Configuration:** The main area shows 'Additional Group Wizard Settings' (Keep standard settings) and 'Assigned workflow' (Single Step Data Owner Authorization). It includes sections for 'Data Owners' (listing David DO Sales) and 'Requesters' (empty).
- Resources:** A table listing resources. One resource is shown: 'File server (1)' with path '\srv-8man\Organization\Sales\Europe'. The 'Inherited from' column for this resource is highlighted with a red box and labeled '2'. The 'Show inherited entries' checkbox is also highlighted with a red box and labeled '1'.
- User & Group selection:** A sidebar on the right showing the domain '8man-demo.local' and a list of users: Augustyn Symanski and David DO Sales.
- Resource selection:** A sidebar on the right showing a tree view of resources, with 'Europe' selected.

### Hierarchy rule:

Resources are available in the assigned organizational category and all higher categories (from bottom to top as opposed to Data Owner and NTFS rights inheritance).

1. Activate the option "Show inherited entries" to display inherited entries in gray.
2. The column "inherited from" shows the origin.

# Assign specific group wizard settings to organizational categories

The screenshot shows the Access Rights Manager Configuration interface. The main window is titled "Data Owner configuration" and displays "8MAN Demo Company" as the selected organizational category. A dialog box titled "Group Wizard Configuration for 8MAN Demo Company" is open, prompting the user to select Group Wizard settings. The dialog box contains the following text:

Please select the Group Wizard settings you want to use  
ARM groups created by the Group Wizard in the Data Owner context of this organization will be put under a specific OU with a specific ARM group prefix (BGP) according to the selected Group Wizard settings.

**Keep standard settings**  
The Group Wizard settings defined in the Scan Configuration will be applied when performing changes on resources.

**Use custom settings**  
The custom Group Wizard settings defined here will be applied when performing changes on resources.

2. Creating groups under <Root>  
in the domain 8man-demo.local

3. Define a ARM group prefix (BGP) that will be added to all groups created by ARM.

Additional ARM group prefix

The dialog box has "Close" and "Apply" buttons.

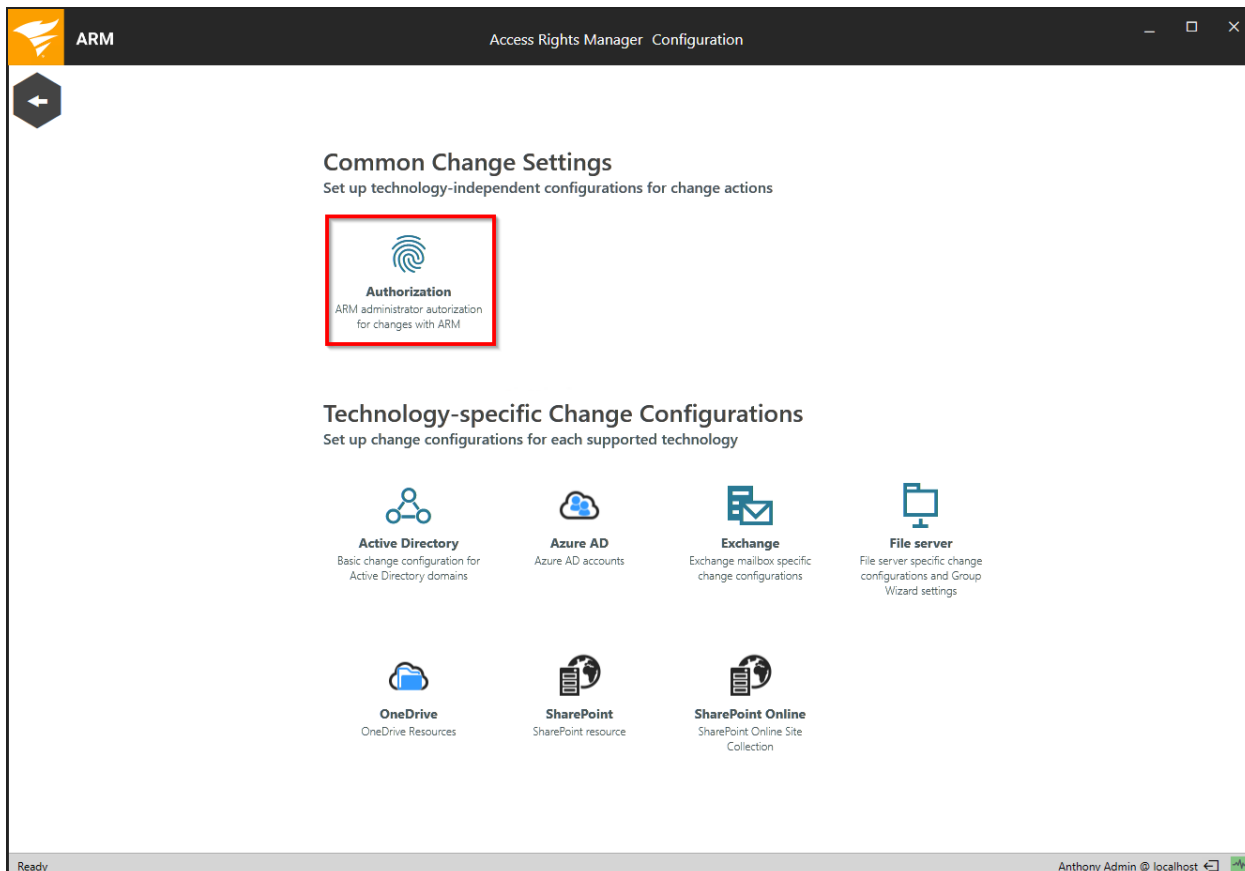
1. You can modify the group wizard configuration for every organizational category.

This allows you to use


2. separate OUs and
3. specific prefixes for group names

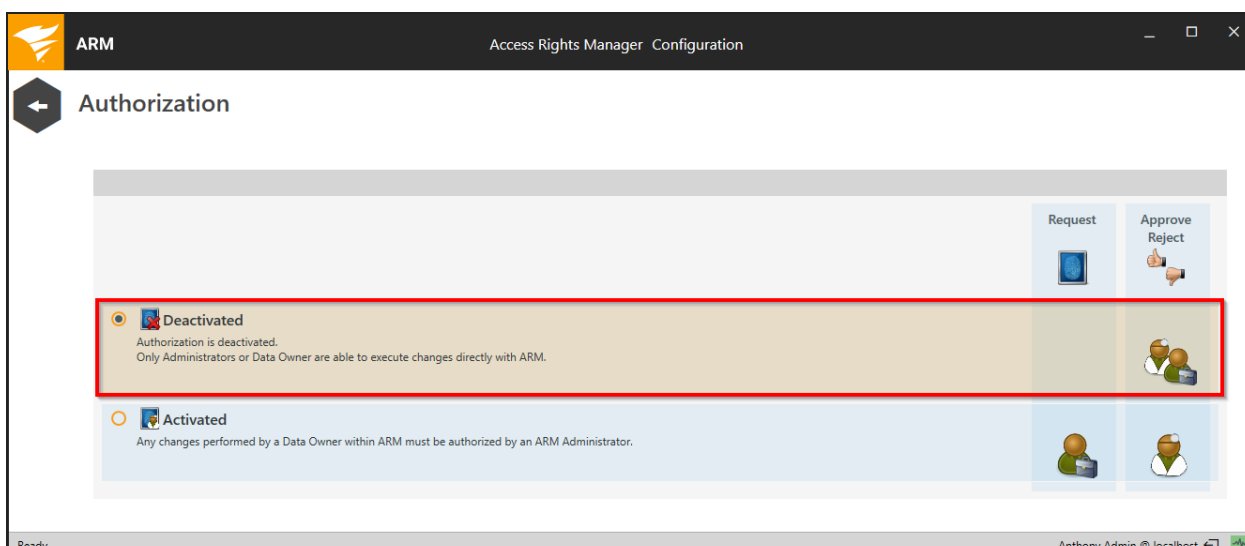
for ARM groups that are created by Data Owners.

# Activate or deactivate simple approvals for Data Owners



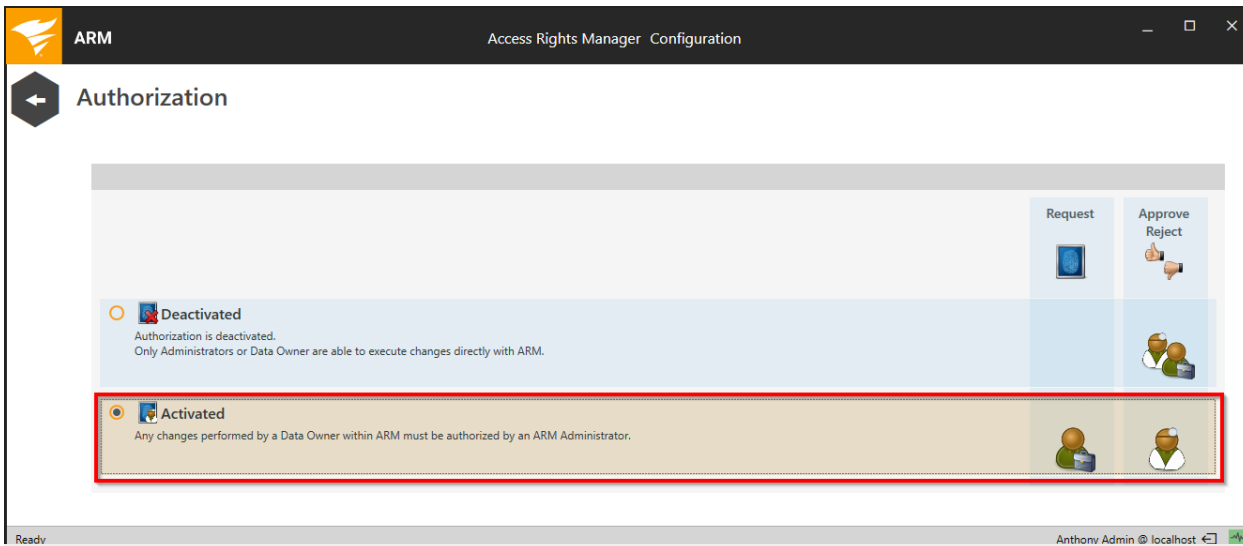
In the ARM Configuration application, click Change Configuration > Authorization.

 The authorization settings do not affect GrantMA workflows.



**Option "Deactivated":**

ARM executes changes made by data owners without further approval.




### Option "Activated":

Changes made by Data Owners must be approved by an ARM Administrator.



The screenshot shows the SolarWinds Access Rights Manager (ARM) application interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. Below the navigation bar, there are five main navigation buttons: HOME, NOTES, REQUESTS, TASKS, and REPORTS. The REQUESTS button is highlighted with a red box. The main content area is divided into several sections: Permission Analysis, User Provisioning, Security Monitoring, and Documentation & Reporting. The Documentation & Reporting section is further divided into Active Directory, File server, and Exchange categories, each with a list of related reports and actions.

ARM administrators must log on to the ARM application and click on "Requests" on the start page to find open approval requests.

 Simple approvals without GrantMA do not include any active notification functionality.

## Data Owner configuration and GrantMA

The screenshot displays the 'Data Owner configuration' window in the Access Rights Manager. The main area shows the 'Sales' category with 'Data Owners' and 'Requesters' lists. A red box highlights the 'Assigned workflow' field, which is currently set to '(inherited from \*8MA...'. A modal dialog titled 'Assign a workflow' is open, prompting the user to select a workflow. The dialog lists several options: '<No workflow>', 'Immediate execution', 'HR (3 steps approval)', 'Marketing (2 steps approval)', 'Resource Owner', and 'Single Step Data Owner Authorization'. The background interface shows organizational categories like Sales, Finance, and Marketing, and a list of resources on the right.

Assign a workflow for an organizational category. In this way, you can use different workflows with different approval steps for each organizational category.

**i** Workflows are created in the GrantMA web interface. See: [GrantMA: Design approval processes](#)

The screenshot shows the 'Data Owner configuration' window in the ARM interface. The 'Sales' category is selected. The 'Requesters' table is empty, and the 'User & Group selection' panel is open, showing a list of users and groups. A red box highlights the 'User & Group selection' panel, and a red arrow points to the 'Requesters' table, indicating the steps for selecting a user and adding it to the requesters list.

Name	Inherited from	User role
Emily Employee (8ma...		Requester (employee)

1. Select a user or group from the account selection area.
2. Add your selection to the "Requester" section via drag & drop.

The screenshot displays the 'Data Owner configuration' window in the ARM interface. On the left, a tree view shows organizational categories: 8MAN Demo Company, Finance, Human Resources, Marketing, Sales, Asia, and Europe. The main area is titled 'Europe' and contains sections for 'Data Owners', 'Requesters', and 'Resources'. The 'Resources' section shows a table with columns for Name, Inherited from, and Access. A red box highlights the 'Requestable' icon (a document with a plus sign) in the Resources table. On the right, the 'User & Group selection' panel shows a search for 'Emily Employee (8...)' and a list of users. A red box highlights the 'Requestable' checkbox in the 'Resource selection' list.

Mark the resources as requestable, so they can be ordered in the GrantMA web interface.

# Import or export Data Owner configurations

The screenshot displays the 'Data Owner configuration' window in the ARM console. The main area is titled 'Europe' and shows the following configuration details:

- Organizational Categories:** A sidebar on the left lists categories like 8MAN Demo Company, Finance, Human Resources, Marketing, Sales, Asia, and Europe. The 'Import' button is highlighted in red.
- Data Owners:** A table with columns for Name, User role, and Inherited from. One entry is visible: '8MAN Demo Company' with user role 'Data Owner'.
- Requesters:** A table with columns for Name, Inherited from, and User role. One entry is visible: 'Emily Employee (8MAN Demo...)' with user role 'Requester (employee)'.
- Resources:** A table with columns for Name, Alias, Inherited from, and Access. One entry is visible: 'Europe (\\srv-8man\Organization\Sa...)'.
- User & Group selection:** A panel on the right showing a search for users in the '8man-demo.local' domain. Results include 'Emily Employee (8MAN Demo...)'.
- Resource selection:** A panel on the right showing a list of resources such as Active Directory, File server, Exchange, Template, Hardware, Software, SharePoint Online, SharePoint, Easy Connect - CSV, Easy Connect - SQL, Azure AD, OneDrive, and SAP Connector.

You can export an existing Data Owner configuration in order to be able to perform bulk operations or a transfer to and from other systems (for example from testing to productive).

# Create a Data Owner configuration report

The screenshot shows the 'Data Owner configuration' window in the Access Rights Manager (ARM) application. The interface is divided into several sections:

- Organizational Categories:** A sidebar on the left with a search bar and a 'Report' button highlighted in red. It lists categories like '8MAN Demo Company', 'Finance', 'Human Resources', 'Marketing', 'Sales', 'Asia', and 'Europe'.
- Data Owners:** A table with columns for Name, User role, and Inherited from. It shows one entry: '8... Data Owner'.
- Requesters:** A table with columns for Name, Inherited from, and User role. It shows one entry: 'Emily Employee (8ma... 8MAN Demo... Requester (employe...)'.
- Resources:** A table with columns for Name, Alias, Inherited from, and Access. It shows one entry: 'Europe (\\srv-8man\Organization\Sal...'.
- User & Group selection:** A panel on the right with a search bar and a list of users including 'Augustyn Symanski', 'David DO Sales', and 'Emily Employee'.
- Resource selection:** A panel on the right with a search bar and a list of resource types including 'Active Directory', 'File server', 'Exchange', 'Template', 'Hardware', 'Software', 'SharePoint Online', 'SharePoint', 'Easy Connect - CSV', 'Easy Connect - SQL', 'Azure AD', 'OneDrive', and 'SAP Connector'.

You can create a Data Owner configuration report in CSV format.

	A	B	C	D	E	F	G	H
1	Organization Unit		DO Name	User	Resource Type	Resource		Resource Size
2	marketing		8MAN-DEMO\PWillis		FileServer	\\srv-8man\Organization\Marketing		408 Bytes
3					ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)		
4					FileServer	\\srv-8man\Organization\Marketing		408 Bytes
5					ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)		
6					FileServer	\\srv-8man\Organization\Marketing		408 Bytes
7								
8	manufacturing		8man-demo\ASTillwell		ActiveDirectory	Agco Corp Global Group 1 (8man-demo.local: CN=Agco Corp Global Group 1,OU=TestGroups,DC=8man-demo,DC=local)		
9					SharePoint	http://portal.8man-demo.com (SRV-8MAN)		
10					ActiveDirectory	Agco Corp Global Group 1 (8man-demo.local: CN=Agco Corp Global Group 1,OU=TestGroups,DC=8man-demo,DC=local)		
11					SharePoint	http://portal.8man-demo.com (SRV-8MAN)		
12					ActiveDirectory	Agco Corp Global Group 1 (8man-demo.local: CN=Agco Corp Global Group 1,OU=TestGroups,DC=8man-demo,DC=local)		
13					SharePoint	http://portal.8man-demo.com (SRV-8MAN)		
14								
15	HR		8man-demo\Tom Ahawk		FileServer	\\srv-8man\Organization\HR		344 Bytes
16					FileServer	\\srv-8man\Organization\HR		344 Bytes
17					ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)		
18					FileServer	\\srv-8man\Organization\HR		344 Bytes
19					ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)		
20								
21	SharePoint Site		8MAN-DEMO\Administrator		SharePoint	http://portal.8man-demo.com/Docs (SRV-8MAN)		
22					SharePoint	http://portal.8man-demo.com/Docs (SRV-8MAN)		
23					ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)		
24					SharePoint	http://portal.8man-demo.com/Docs (SRV-8MAN)		
25					ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)		

The last column contains information on data storage of file server resources.

The column users will only contain values if a group has been configured as the Data Owner.

# Server

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there are three summary cards: 'Server Status' (License Information), 'Jobs' (Summary), and 'Collectors' (Configuration). Below these are several configuration categories represented by icons and text:

- Scans**: Resource Configurations, Logga, File Server CSV Import
- Open Order**: Open Order Resource Descriptions
- User Management**: User Management, Role Management
- Data Owner**: Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**: License Information, Server Status
- Jobs Overview**: Job Status, Job Categories
- Alerts**: Activate/Deactivate Alert Sensors
- Change Configuration**: Common Change Settings, Technology-specific Change Configurations
- Scripting**: Scripting configuration for change actions
- Views & Reports**: Views & Reports, Blacklist for Views & Reports
- Server** (highlighted with a red box): Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**: ARM Server, SQL Server, Configuration Status

Click "Server" to manage settings related to comments, email, data storage, health-check and event logs.

## Configure the web client URL

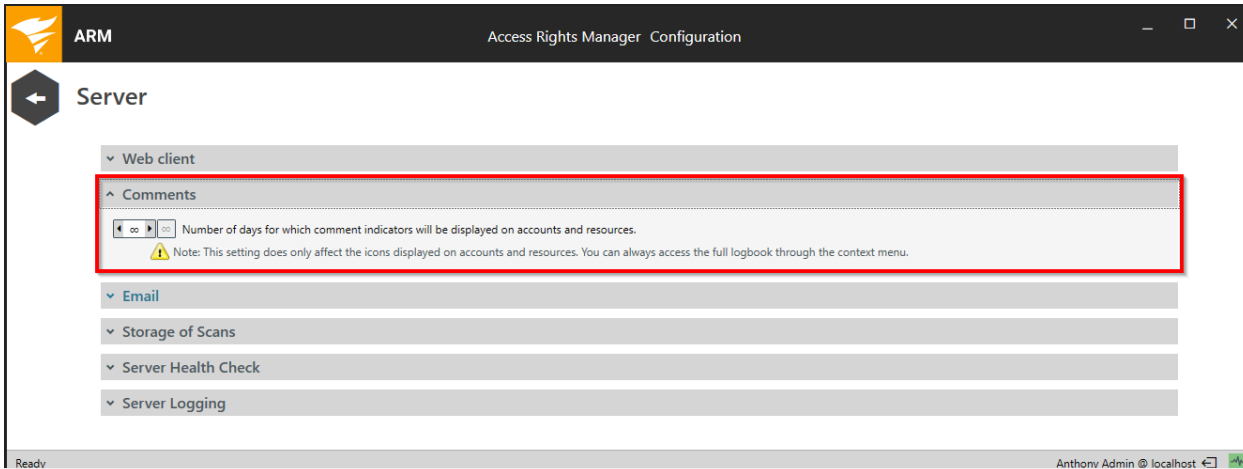
The screenshot shows the 'Server' configuration page in the 'Access Rights Manager Configuration' window. The 'Web client' section is expanded and highlighted with a red box, showing the text: "The base URL to ARM web server is <https://srv-8man.8man-demo.local>". Other sections listed include Comments, Email, Storage of Scans, Server Health Check, and Server Logging.

Specify the URL of the web server running the ARM Website.



This is used for the link in the notification emails.

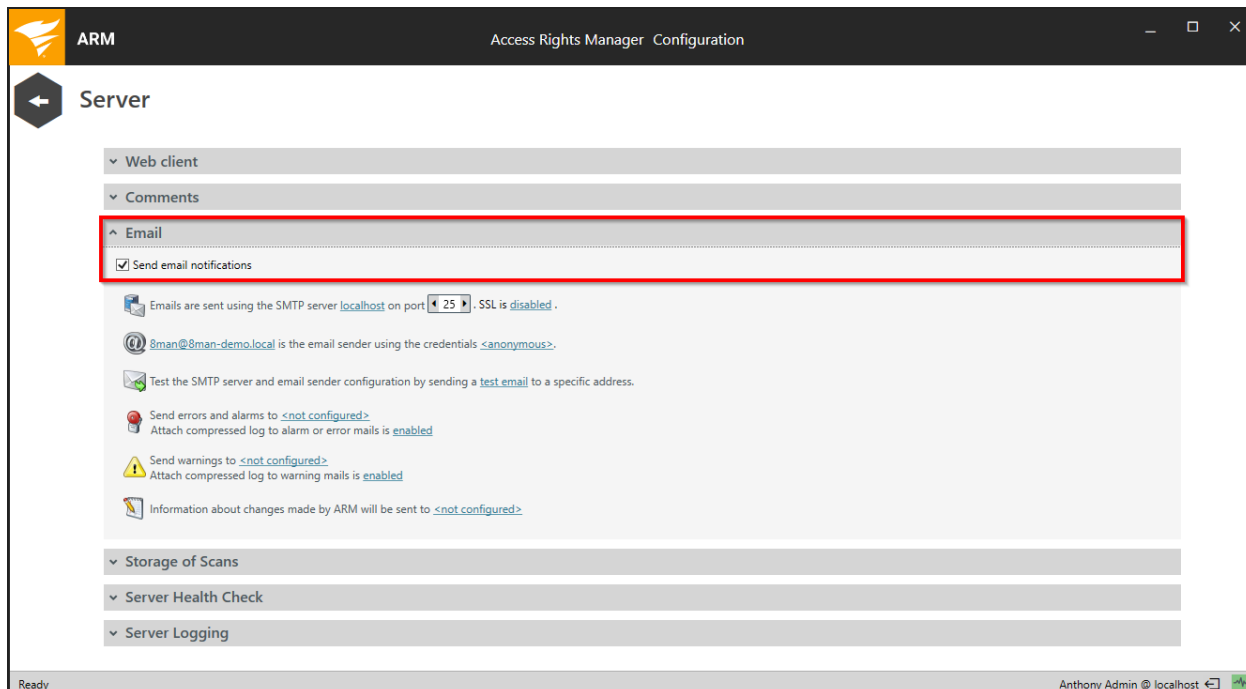
## Set the display duration for comment icons



ARM displays a note icon in the resource or accounts view for stored comments or AD Logga information.

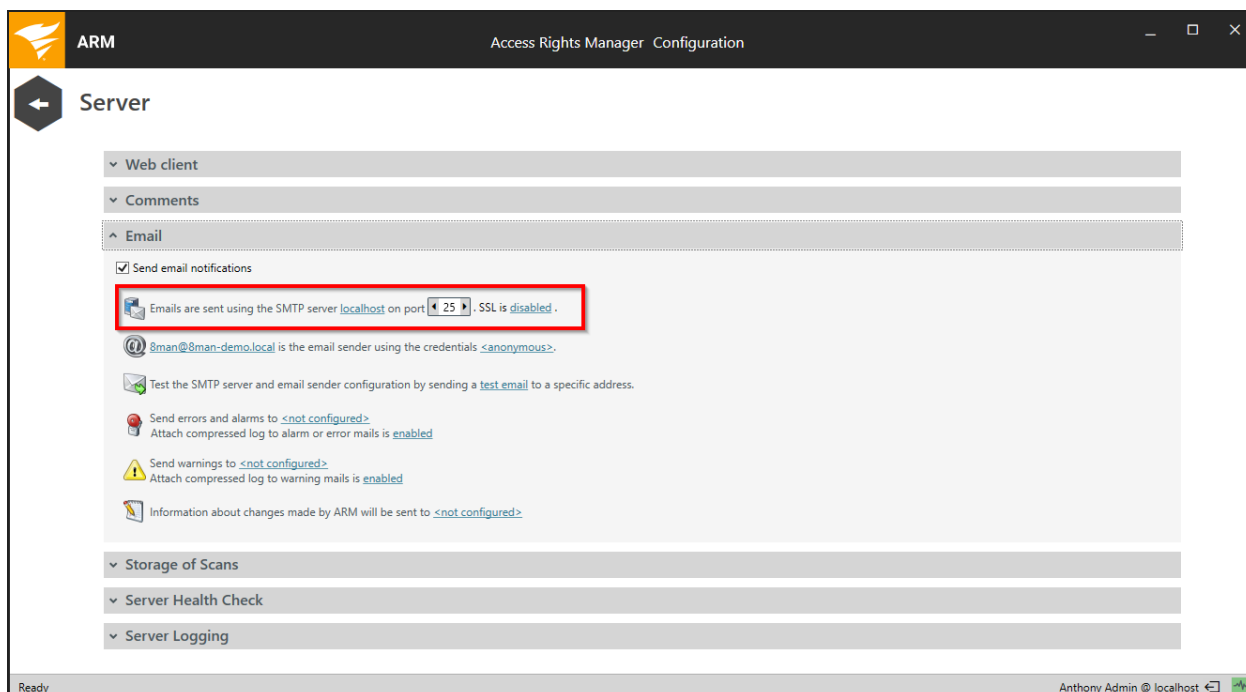
The longer you use ARM, the more notes will be created. You can reduce the length of time that notes are displayed, if you see too many notes.

# Configure email settings




The screenshot shows the 'Server' configuration page in the Access Rights Manager (ARM) interface. The 'Email' section is expanded, and the 'Send email notifications' checkbox is checked and highlighted with a red box. Below this, the SMTP server configuration is shown as 'localhost' on port '25', with 'SSL is disabled'. Other settings include the email sender '@sman@sman-demo.local' using 'anonymous' credentials, and various notification options for errors, warnings, and changes.

Activate email support in ARM.



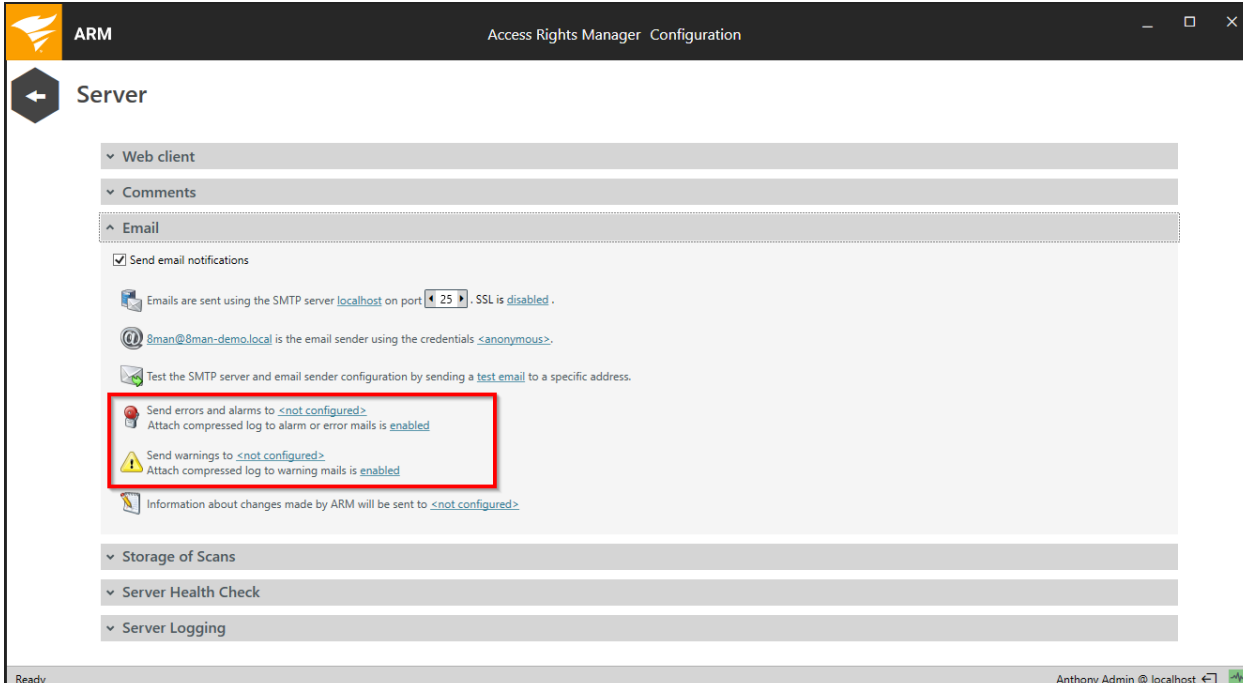
The screenshot shows the 'Server' configuration page in the Access Rights Manager (ARM) interface. The 'Email' section is expanded, and the SMTP server configuration is highlighted with a red box. The configuration shows 'localhost' on port '25', with 'SSL is disabled'. Other settings include the email sender '@sman@sman-demo.local' using 'anonymous' credentials, and various notification options for errors, warnings, and changes.

Configure an SMTP-server for sending emails.

 You can only configure an internal SMTP-server. It is **NOT** possible to configure an external SMTP-server such as smtp.office365.com. You may setup an internal relay server.

Standard ports for SMTP:

- 25 without SSL
- 465 or 587 with SSL/TLS

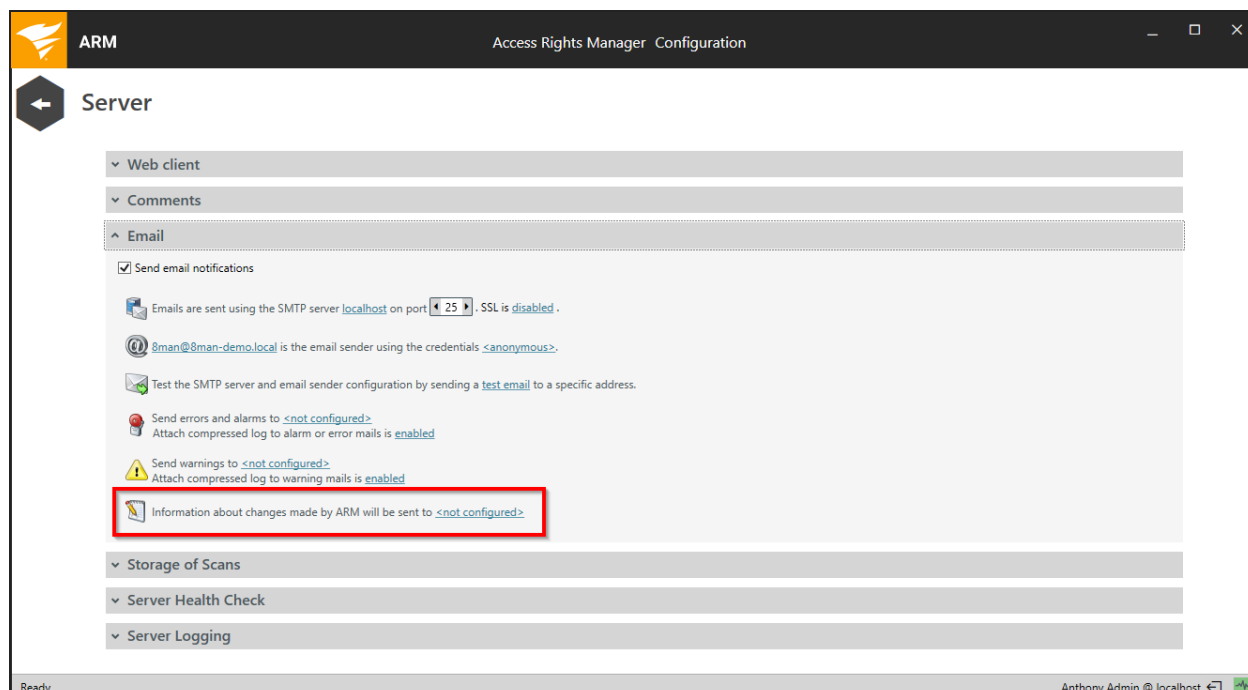


The screenshot shows the 'Server' configuration page in the 'Access Rights Manager' application. The 'Email' section is expanded, showing several options. The option 'Send errors and alarms to <not configured>' is highlighted with a red box. Below it, the option 'Send warnings to <not configured>' is also visible. The status bar at the bottom indicates 'Ready' and 'Anthony Admin @ localhost'.

Sources for errors, alerts and warnings include the following:

- Thresholds from the Server [Health-Check](#)
- Errors when running ARM

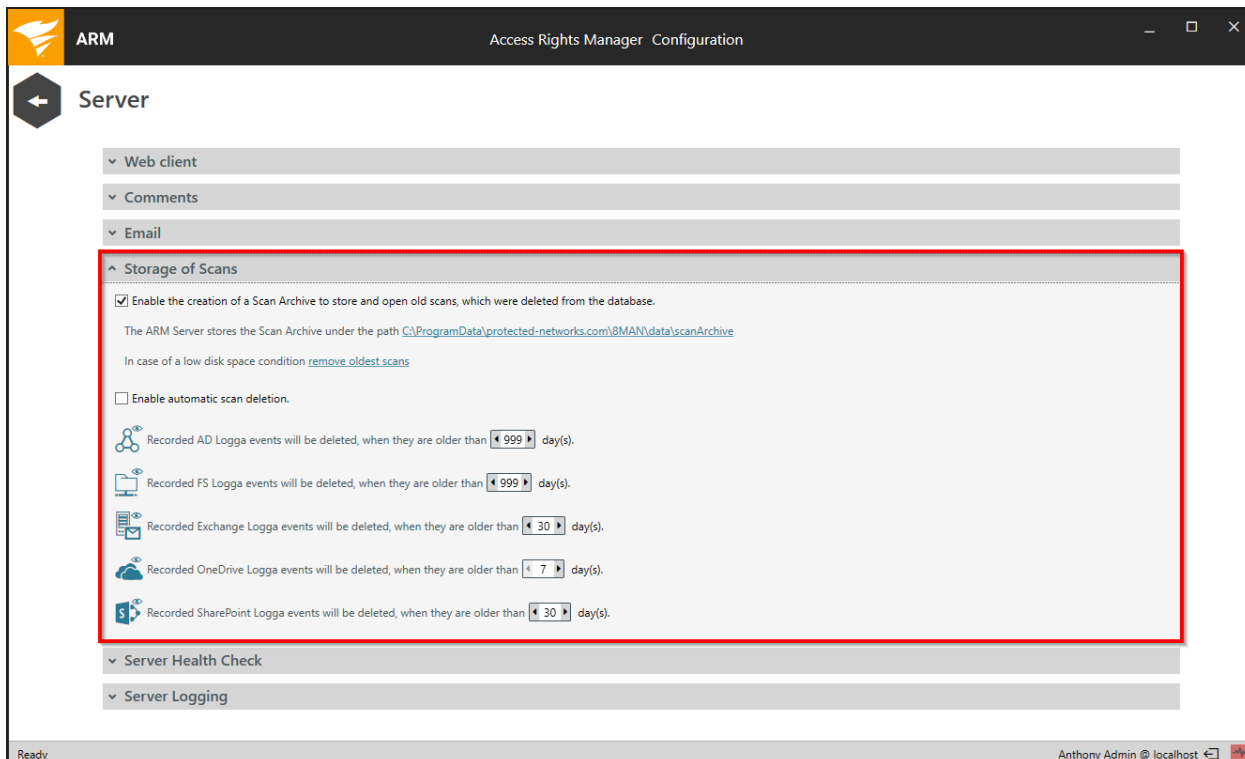
The events of the last 4 hours are summarized in an email.



Enter an email address if you want to be alerted every time a user completes a change with ARM.

⚠ SPAM Alert! Every change generates an email.

## Configure storage of scans settings



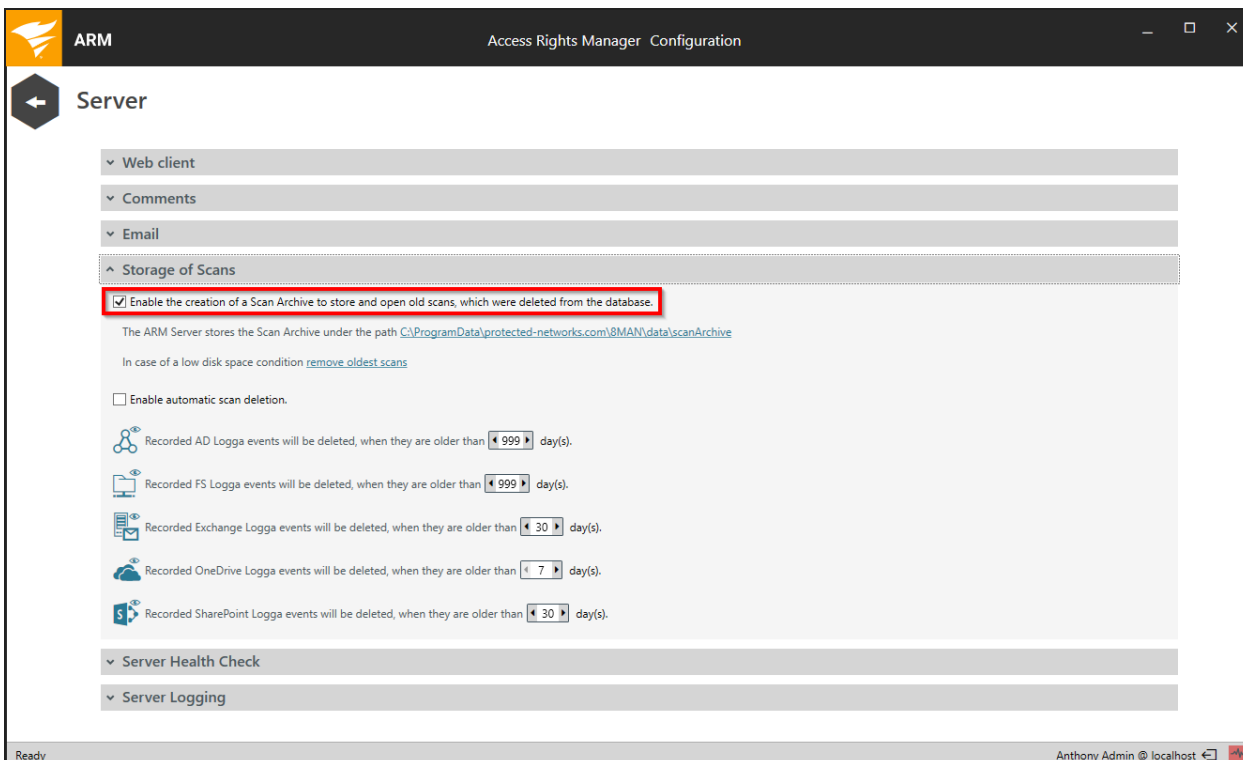
The screenshot shows the 'Server' configuration page in the Access Rights Manager (ARM) interface. The 'Storage of Scans' section is highlighted with a red border. It contains the following settings:

- Enable the creation of a Scan Archive to store and open old scans, which were deleted from the database.  
The ARM Server stores the Scan Archive under the path `C:\ProgramData\protected-networks.com\ARM\data\scanArchive`  
In case of a low disk space condition [remove oldest scans](#)
- Enable automatic scan deletion.
- Recorded AD Logga events will be deleted, when they are older than  day(s).
- Recorded FS Logga events will be deleted, when they are older than  day(s).
- Recorded Exchange Logga events will be deleted, when they are older than  day(s).
- Recorded OneDrive Logga events will be deleted, when they are older than  day(s).
- Recorded SharePoint Logga events will be deleted, when they are older than  day(s).

Below the 'Storage of Scans' section, there are expandable sections for 'Server Health Check' and 'Server Logging'.

The "Storage of Scans" configuration allows you to determine how long scan and Logga data are stored. This affects the size of your data base and required disk storage.

Please refer to the chapter [SQL Express and ARM](#).



The screenshot shows the 'Server' configuration page in the Access Rights Manager (ARM) application. The 'Storage of Scans' section is expanded, and the checkbox for 'Enable the creation of a Scan Archive to store and open old scans, which were deleted from the database.' is checked. Below this, the text indicates that the Scan Archive is stored at the path `C:\ProgramData\protected-networks.com\8MAN\data\scanArchive` and that the `remove_oldest_scans` option is used for low disk space conditions. There is also an unchecked checkbox for 'Enable automatic scan deletion.' and several dropdown menus for setting retention periods for different Logga event types: AD (999 days), FS (999 days), Exchange (30 days), OneDrive (7 days), and SharePoint (30 days). The bottom of the window shows the system tray with 'Ready' and 'Anthony Admin @ localhost'.

**Option activated:**

ARM creates an encrypted and password protected zip file and stores it on the file system. This data can be reloaded in the ARM application even if it has been deleted from the data base. Activate this option when using SQL Express.

**Option deactivated:**

ARM does not create a scan archive. ARM users are only able to access data available in the data base.

The screenshot shows the 'Server' configuration page in the Access Rights Manager (ARM) console. The 'Storage of Scans' section is expanded, showing the following settings:

- Enable the creation of a Scan Archive to store and open old scans, which were deleted from the database.  
The ARM Server stores the Scan Archive under the path `C:\ProgramData\protected-networks.com\8MAN\data\scanArchive`  
In case of a low disk space condition [remove oldest scans](#)
- Enable automatic scan deletion.
- Recorded AD Logga events will be deleted, when they are older than  day(s).
- Recorded FS Logga events will be deleted, when they are older than  day(s).
- Recorded Exchange Logga events will be deleted, when they are older than  day(s).
- Recorded OneDrive Logga events will be deleted, when they are older than  day(s).
- Recorded SharePoint Logga events will be deleted, when they are older than  day(s).

Other sections visible include 'Web client', 'Comments', 'Email', 'Server Health Check', and 'Server Logging'.

Ready

Anthony Admin @ localhost

Determine where the ARM scan archives are stored. For example, you can store the scan archives on another volume.

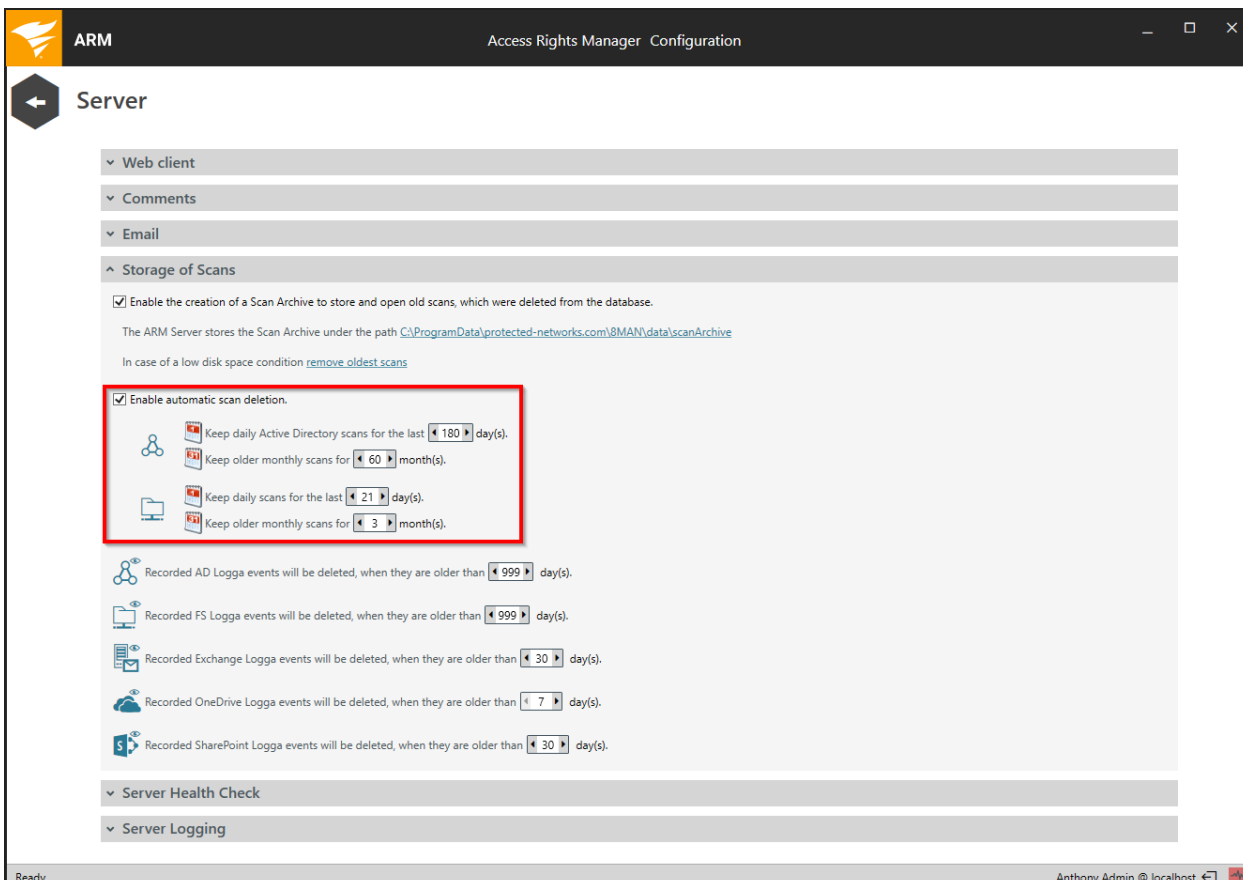
Default path for the scan archives:

```
%ProgramData%\protected-networks.com\8MAN\data\ScanArchive
```

The screenshot shows the 'Access Rights Manager Configuration' window. The 'Server' section is expanded to 'Storage of Scans'. A red box highlights the text 'In case of a low disk space condition'. A dialog box titled 'Action to perform in case of storage limit reached' is overlaid, asking 'How should ARM react if there is not enough free disk space available for the scan archive?' with two radio button options: 'Skip storing new scans (leave old scans untouched)' and 'Remove old scan data until the new scan data can be archived.' The 'Apply' button is highlighted.

Determine how ARM reacts in case of low disk space (volume full).





ARM Access Rights Manager Configuration

Server

- Web client
- Comments
- Email
- Storage of Scans
  - Enable the creation of a Scan Archive to store and open old scans, which were deleted from the database.  
The ARM Server stores the Scan Archive under the path `C:\ProgramData\protected-networks.com\8MAN\data\scanArchive`  
In case of a low disk space condition [remove oldest scans](#)
  - Enable automatic scan deletion.
    - Keep daily Active Directory scans for the last  day(s).
    - Keep older monthly scans for  month(s).
    - Keep daily scans for the last  day(s).
    - Keep older monthly scans for  month(s).
  - Recorded AD Logga events will be deleted, when they are older than  day(s).
  - Recorded FS Logga events will be deleted, when they are older than  day(s).
  - Recorded Exchange Logga events will be deleted, when they are older than  day(s).
  - Recorded OneDrive Logga events will be deleted, when they are older than  day(s).
  - Recorded SharePoint Logga events will be deleted, when they are older than  day(s).
- Server Health Check
- Server Logging

Ready Anthony Admin @ localhost

### Option deactivated:

ARM does not delete any scans from the data base.

### Option activated:

Determine how long ARM retains scans in the database.

Activate this option when using SQL Express and select a short period of retention.

Please see further information in [Data base maintenance](#).

The screenshot shows the 'Server' configuration page in the ARM interface. The 'Storage of Scans' section is expanded, showing options to enable a Scan Archive and automatic scan deletion. A red box highlights the Logga event retention settings:

- Recorded AD Logga events will be deleted, when they are older than 180 day(s).
- Recorded FS Logga events will be deleted, when they are older than 60 month(s).
- Recorded Exchange Logga events will be deleted, when they are older than 21 day(s).
- Recorded OneDrive Logga events will be deleted, when they are older than 3 month(s).
- Recorded SharePoint Logga events will be deleted, when they are older than 999 day(s).
- Recorded FS Logga events will be deleted, when they are older than 999 day(s).
- Recorded Exchange Logga events will be deleted, when they are older than 30 day(s).
- Recorded OneDrive Logga events will be deleted, when they are older than 7 day(s).
- Recorded SharePoint Logga events will be deleted, when they are older than 30 day(s).

Determine how long Logga data is stored.

Default: 30 days

An event generates the following average amount of data:

FS Logga about 43 bytes

AD Logga about 600 bytes

Exchange Logga about 600 bytes

## Determine server thresholds

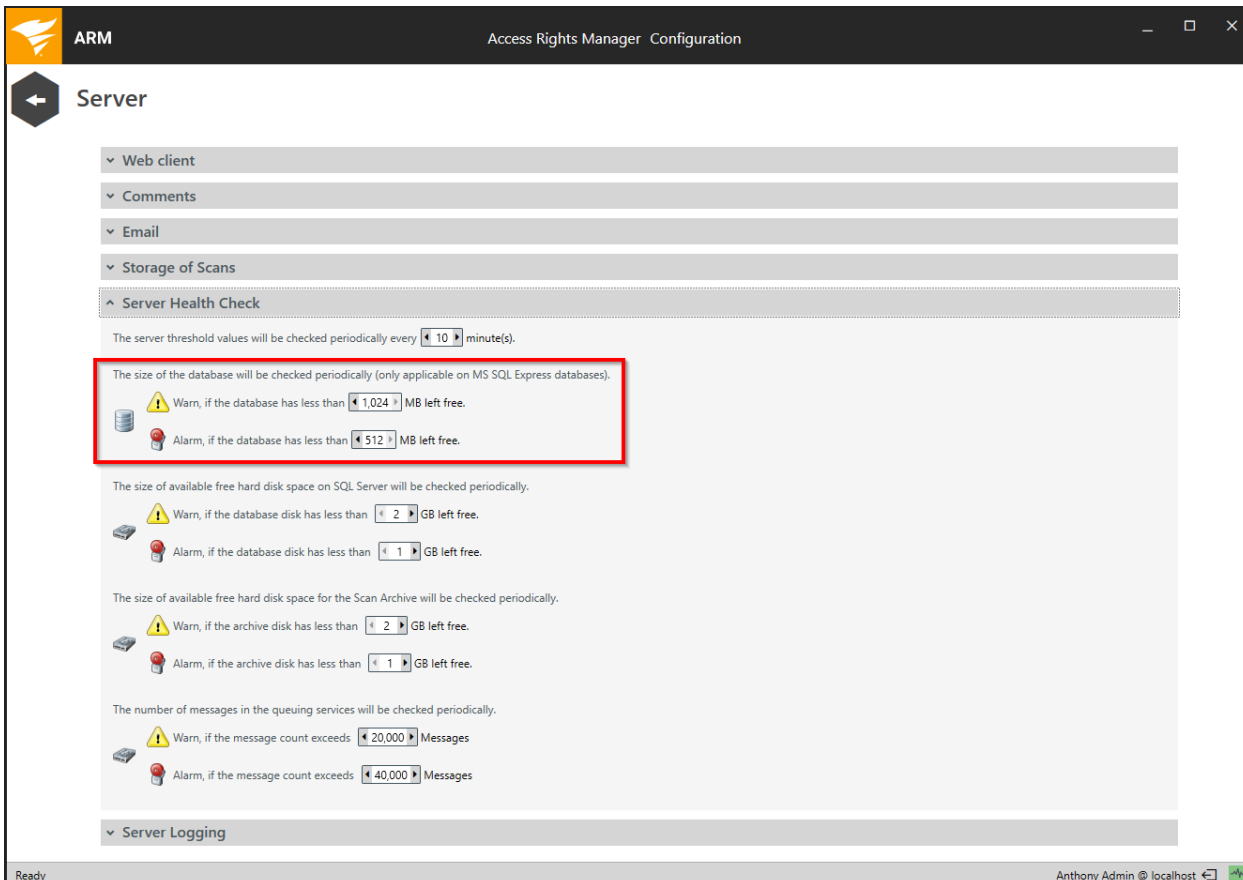
The screenshot shows the 'Server' configuration page in the Access Rights Manager (ARM) interface. The 'Server Health Check' section is highlighted with a red border. It contains the following settings:

- Web client
- Comments
- Email
- Storage of Scans
- Server Health Check**
  - The server threshold values will be checked periodically every  minute(s).
  - The size of the database will be checked periodically (only applicable on MS SQL Express databases).
    - Warn, if the database has less than  MB left free.
    - Alarm, if the database has less than  MB left free.
  - The size of available free hard disk space on SQL Server will be checked periodically.
    - Warn, if the database disk has less than  GB left free.
    - Alarm, if the database disk has less than  GB left free.
  - The size of available free hard disk space for the Scan Archive will be checked periodically.
    - Warn, if the archive disk has less than  GB left free.
    - Alarm, if the archive disk has less than  GB left free.
  - The number of messages in the queuing services will be checked periodically.
    - Warn, if the message count exceeds  Messages
    - Alarm, if the message count exceeds  Messages
- Server Logging

Ready Anthony Admin @ localhost

Determine server thresholds and monitoring frequency.

Please also reference the following chapter: [Display actual server thresholds.](#)



The screenshot shows the 'Server' configuration page in the Access Rights Manager. The 'Server Health Check' section is expanded, showing various monitoring settings. A red box highlights the database size monitoring settings for MS SQL Express databases. The settings include a warning threshold of 1,024 MB left free and an alarm threshold of 512 MB left free. Other settings include disk space monitoring for the database and scan archive, and message count monitoring for queuing services.

ARM

Access Rights Manager Configuration

Server

Web client

Comments

Email

Storage of Scans

Server Health Check

The server threshold values will be checked periodically every 10 minute(s).

The size of the database will be checked periodically (only applicable on MS SQL Express databases).

Warn, if the database has less than 1,024 MB left free.

Alarm, if the database has less than 512 MB left free.

The size of available free hard disk space on SQL Server will be checked periodically.

Warn, if the database disk has less than 2 GB left free.

Alarm, if the database disk has less than 1 GB left free.

The size of available free hard disk space for the Scan Archive will be checked periodically.

Warn, if the archive disk has less than 2 GB left free.

Alarm, if the archive disk has less than 1 GB left free.

The number of messages in the queuing services will be checked periodically.

Warn, if the message count exceeds 20,000 Messages

Alarm, if the message count exceeds 40,000 Messages

Server Logging

Ready Anthonyv Admin @ localhost

ARM identifies automatically whether you are using SQL Express. In this case you can determine thresholds for data base size.

If you are using a "full" SQL server, then these settings are not relevant.

Please refer to the following section for additional information: [ARM and SQL Express](#).

The screenshot shows the 'Server' configuration page in the Access Rights Manager (ARM) interface. The 'Server Health Check' section is expanded, showing various monitoring thresholds. A red box highlights the 'The size of available free hard disk space on SQL Server will be checked periodically' section, which includes a warning threshold of 2 GB and an alarm threshold of 1 GB. Other sections include 'Web client', 'Comments', 'Email', 'Storage of Scans', and 'Server Logging'.

ARM

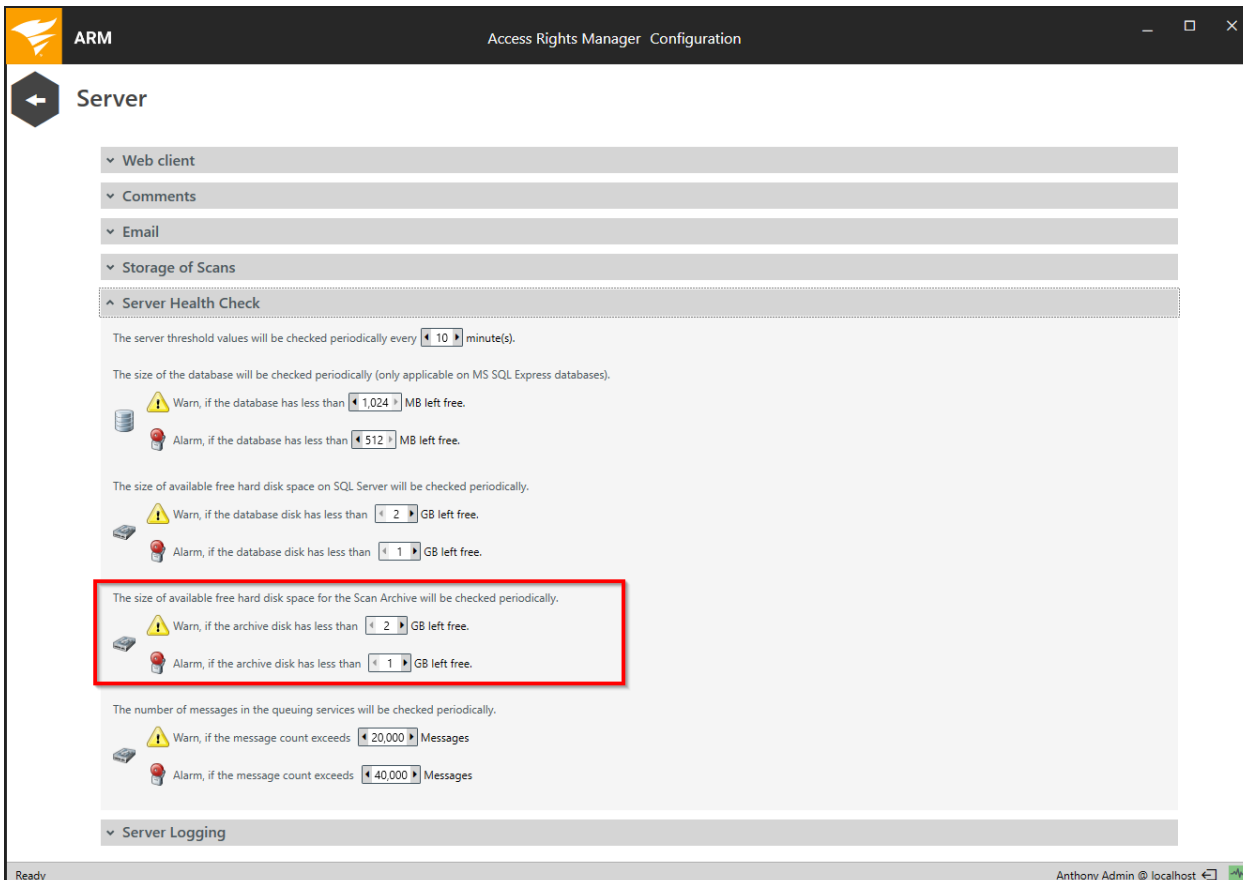
Access Rights Manager Configuration

### Server

- Web client
- Comments
- Email
- Storage of Scans
- Server Health Check**
  - The server threshold values will be checked periodically every  minute(s).
  - The size of the database will be checked periodically (only applicable on MS SQL Express databases).
    - Warn, if the database has less than  MB left free.
    - Alarm, if the database has less than  MB left free.
    - The size of available free hard disk space on SQL Server will be checked periodically.**
      - Warn, if the database disk has less than  GB left free.
      - Alarm, if the database disk has less than  GB left free.
  - The size of available free hard disk space for the Scan Archive will be checked periodically.
    - Warn, if the archive disk has less than  GB left free.
    - Alarm, if the archive disk has less than  GB left free.
  - The number of messages in the queuing services will be checked periodically.
    - Warn, if the message count exceeds  Messages
    - Alarm, if the message count exceeds  Messages
- Server Logging

Ready Anthony Admin @ localhost

ARM automatically determines the available disk space on the volume storing SQL data base files.  
Determine thresholds for available storage space.



The screenshot shows the 'Server Health Check' configuration page in the ARM interface. The page is titled 'Server' and has a navigation arrow on the left. The 'Server Health Check' section is expanded, showing several monitoring settings. The 'Scan Archive' disk space settings are highlighted with a red box. The settings are as follows:

- The server threshold values will be checked periodically every  minute(s).
- The size of the database will be checked periodically (only applicable on MS SQL Express databases).
  - Warn, if the database has less than  MB left free.
  - Alarm, if the database has less than  MB left free.
- The size of available free hard disk space on SQL Server will be checked periodically.
  - Warn, if the database disk has less than  GB left free.
  - Alarm, if the database disk has less than  GB left free.
- The size of available free hard disk space for the Scan Archive will be checked periodically.
  - Warn, if the archive disk has less than  GB left free.
  - Alarm, if the archive disk has less than  GB left free.
- The number of messages in the queuing services will be checked periodically.
  - Warn, if the message count exceeds  Messages
  - Alarm, if the message count exceeds  Messages

The bottom of the window shows the system tray with 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Determine the thresholds for available disk space of the scan archive.

Settings for the scan archive can be found in [Storage of Scans](#).

The screenshot shows the 'Server' configuration page in the Access Rights Manager (ARM) interface. The 'Server Health Check' section is expanded, showing various monitoring settings. A red box highlights the 'The number of messages in the queuing services will be checked periodically' section, which includes a warning threshold of 20,000 messages and an alarm threshold of 40,000 messages.

ARM Access Rights Manager Configuration

## Server

- Web client
- Comments
- Email
- Storage of Scans
- Server Health Check**

The server threshold values will be checked periodically every  minute(s).

The size of the database will be checked periodically (only applicable on MS SQL Express databases).

- Warn, if the database has less than  MB left free.
- Alarm, if the database has less than  MB left free.

The size of available free hard disk space on SQL Server will be checked periodically.

- Warn, if the database disk has less than  GB left free.
- Alarm, if the database disk has less than  GB left free.

The size of available free hard disk space for the Scan Archive will be checked periodically.

- Warn, if the archive disk has less than  GB left free.
- Alarm, if the archive disk has less than  GB left free.

The number of messages in the queuing services will be checked periodically.

- Warn, if the message count exceeds  Messages
- Alarm, if the message count exceeds  Messages

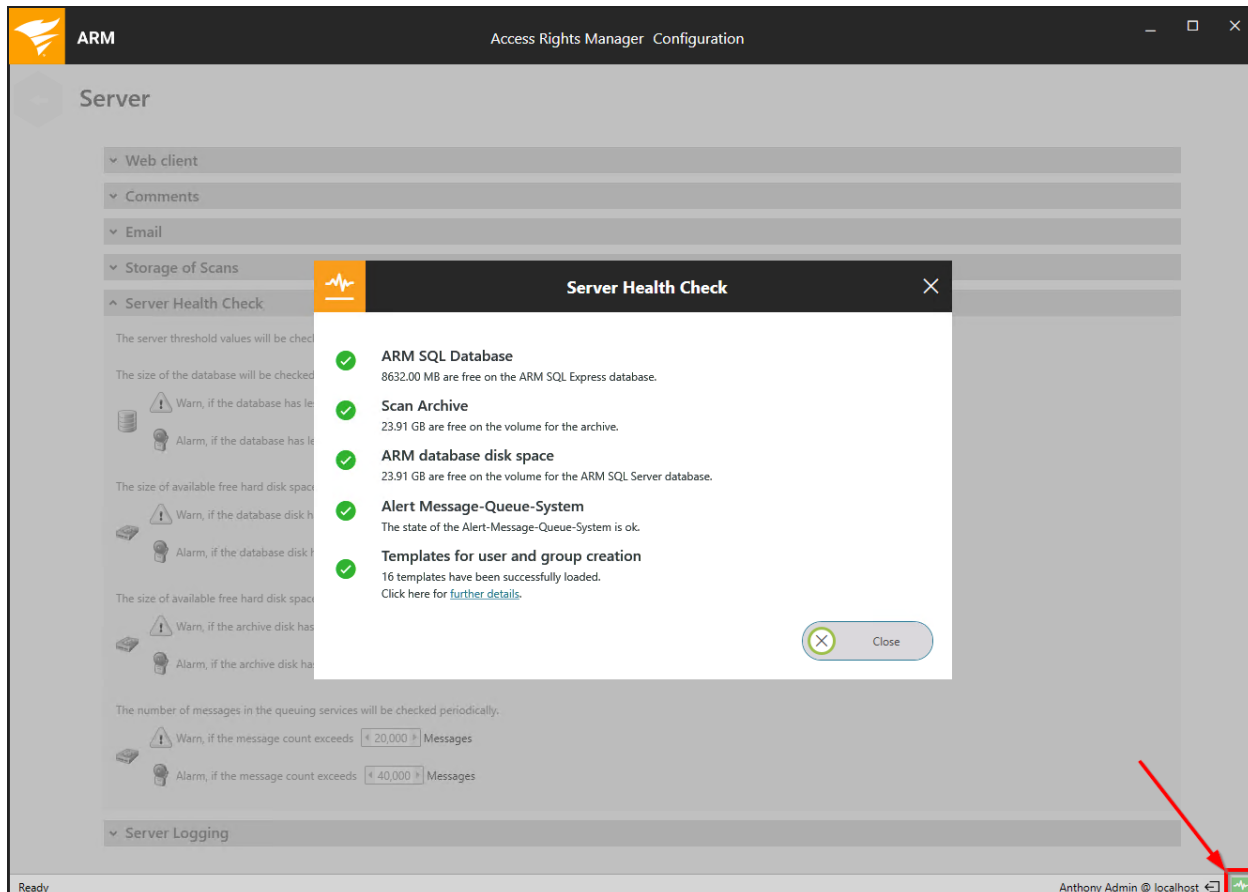
Server Logging

Ready Anthonyv Admin @ localhost

Determine the thresholds for the message queuing.

The settings are only relevant if you use the alerts feature ([alert sensors](#) enabled).

## Display the server health check



The screenshot shows the 'Access Rights Manager Configuration' window with the 'Server' section selected. A 'Server Health Check' dialog box is open, displaying the following information:

- ARM SQL Database**: 8632.00 MB are free on the ARM SQL Express database.
- Scan Archive**: 23.91 GB are free on the volume for the archive.
- ARM database disk space**: 23.91 GB are free on the volume for the ARM SQL Server database.
- Alert Message-Queue-System**: The state of the Alert-Message-Queue-System is ok.
- Templates for user and group creation**: 16 templates have been successfully loaded. Click here for [further details](#).

The dialog box includes a 'Close' button. A red arrow points to a small green plus icon in the status bar at the bottom right of the configuration window.

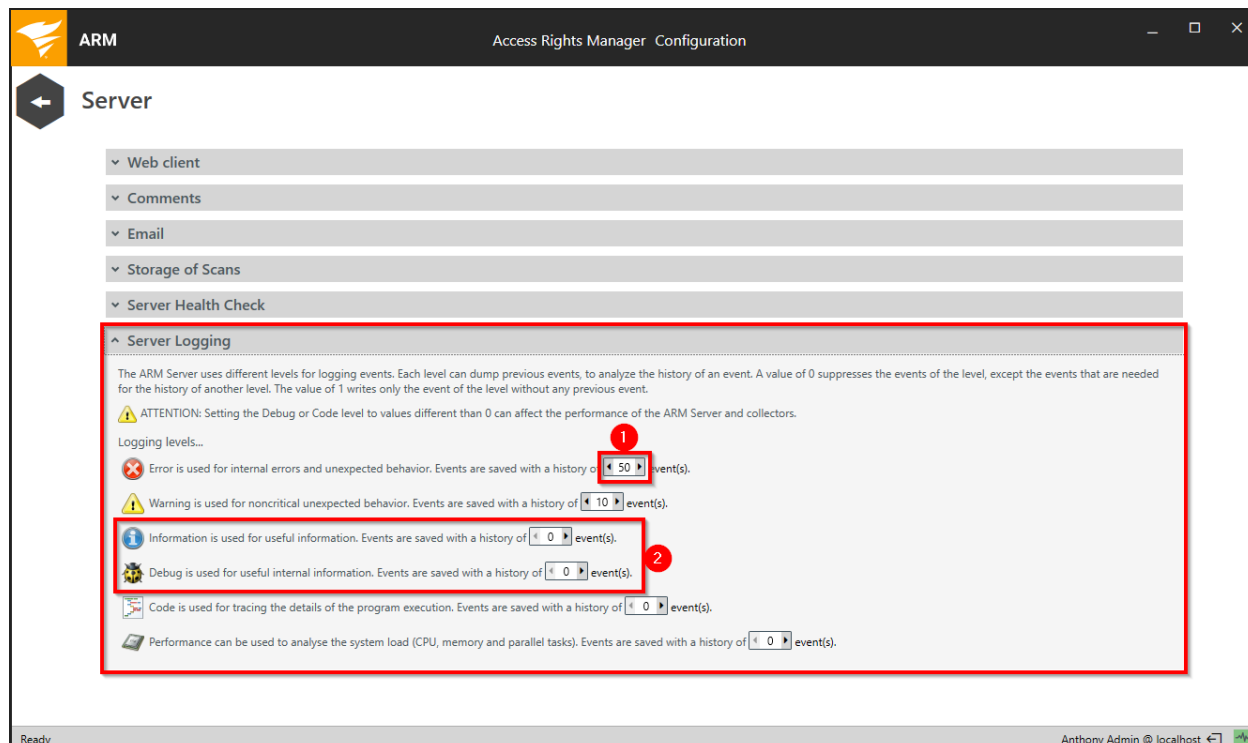
Click on the marked symbol in the status bar to see the current server values.

This works in both ARM applications.



# Server event logging

## Determine the logging level



Determine the level of details that ARM captures in ARM logs.

1. Set the value for the number of stored errors to at least 50.
2. Activate the levels Debug or Code only for the diagnosis of severe issues.

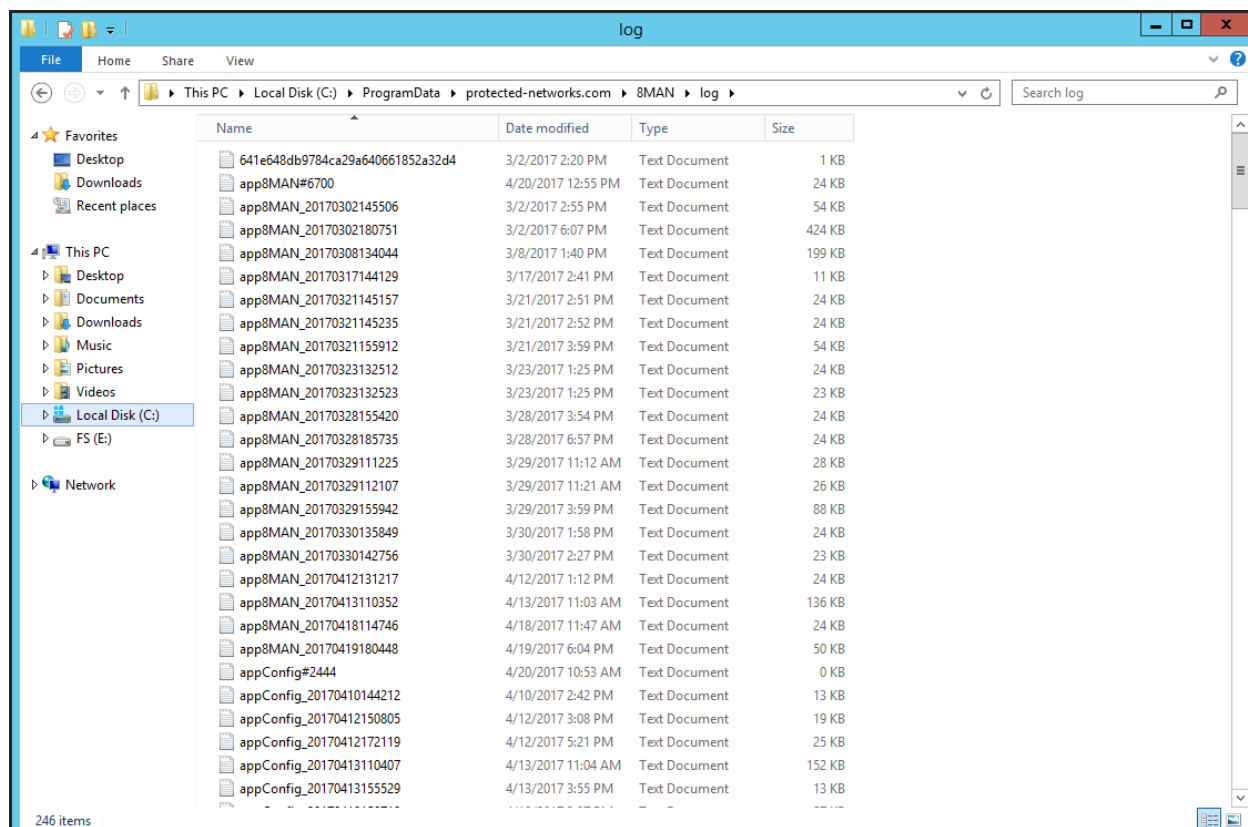
## Retrieve ARM log files

ARM stores all log files in the following folder:

```
%ProgramData%\protected-networks.com\8MAN\log
```

All events are saved centrally on the ARM-server, including events from remote collectors.

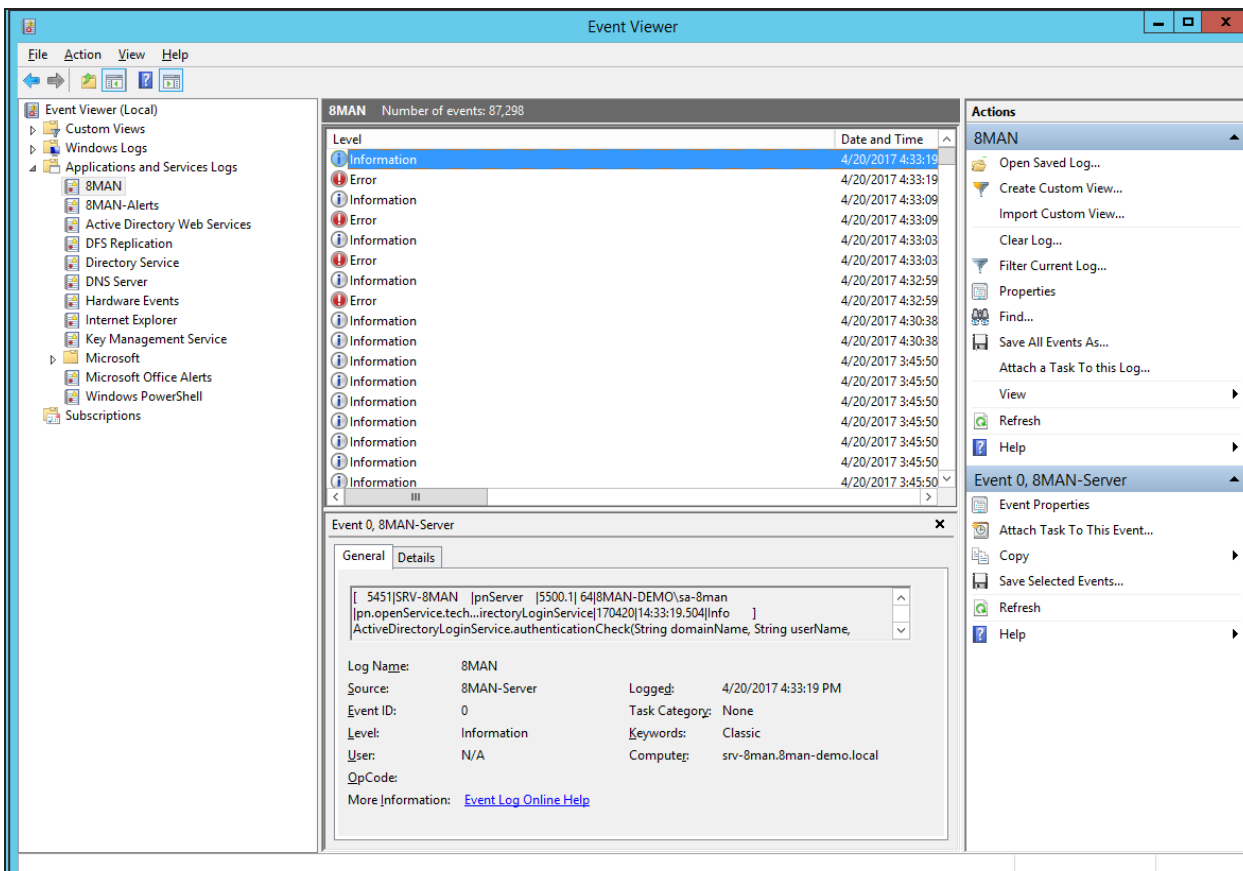
Log files either grow to a size of 50MB or 7 days. When restarting the ARM service a new log file is started. ARM saves a maximum of 20 log files per [type](#).



The current version does not have a time stamp in the file name.

Current log files may be shown with a 0 KB size in Windows Explorer, even if they contain data.

Please zip the files before sending them to [support](#).



The following event types are entered into the Windows event log: "Error", "Warning" and "Information". ARM creates its own node under "Application and Service Logs".

## Logfile types

### FILENAME CONTAINES...

armServer (old: pnServer)	Information on the ARM server, collectors and jobs. Is most frequently used in support requests. Please don't confuse this with pnService. From ARM version 2019.4 the files are named armServer*.log, for older ARM versions they are named pnserver*.log.
pnService	Information relating to the start of the ARM service.
app8MAN	Information on the ARM application (graphical user interface, GUI). Useful in case of program crashes.
appConfig	Information on the configuration application. Useful in case of crashes of the configuration.
pnTracer	Information on Logga.
pnRun	Watchdog for pnServer service.

**F**  
**ILENAME CONTAINES...**

pnAlert	Information about alert engine (FS Logga and AD Logga).
grantMa	Information on GrantMA, webAPI.

## Set Syslog servers

The screenshot shows the 'Server' configuration page in the Access Rights Manager (ARM) interface. The 'SysLog' section is expanded, showing a table with columns for 'Address' and 'UDP Port'. A single entry is visible with 'KIWI' in the Address field and '514' in the UDP Port field. The 'New' and 'Delete' buttons are visible above the table.

Address	UDP Port
KIWI	514

Configure Syslog servers with Name/IP address and port.

This setting is required for sending alert events to Syslog.

You can configure more than one Syslog server. Every event is sent to all servers.

# Scripting

The screenshot displays the ARM Configuration window. At the top, it shows 'ARM' and 'Access Rights Manager Configuration'. The main area contains three summary cards:

- Server Status (License Information):** Logged in users: 2; Licensed Active user accounts: 1166.
- Jobs Summary:** 91 Scans, 7 Reports, 69 Changes, 131 More; 7 Scheduled, 291 Succeeded; 0 Executing, 0 Failed.
- Collectors Configuration:** 1 Connected, 1 Configured in Total; All Collectors are Operational.

Below the summary cards is a 'Filter' dropdown. The main dashboard features 12 functional tiles:

- Scans:** Resource Configurations, Logga, File Server CSV Import.
- Open Order:** Open Order Resource Descriptions.
- User Management:** User Management, Role Management.
- Data Owner:** Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings.
- License:** License Information, Server Status.
- Jobs Overview:** Job Status, Job Categories.
- Alerts:** Activate/Deactivate Alert Sensors.
- Change Configuration:** Common Change Settings, Technology-specific Change Configurations.
- Scripting:** Scripting configuration for change actions (highlighted with a red box).
- Views & Reports:** Views & Reports, Blacklist for Views & Reports.
- Server:** Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging.
- Basic Configuration:** ARM Server, SQL Server, Configuration Status.

The bottom status bar shows 'Ready' and 'Anthony Admin @ localhost'.

Ordering a new user on the GrantMA Self-Service Portal is natively supported by ARM. For example, disabling a user after the approval flow has been completed becomes possible through the use of scripts. The combination GrantMA - Scripts - ARM webAPI opens up a multitude of further possibilities for automating documented processes.

## Configure scripts

Scripts must be stored in the following directory:

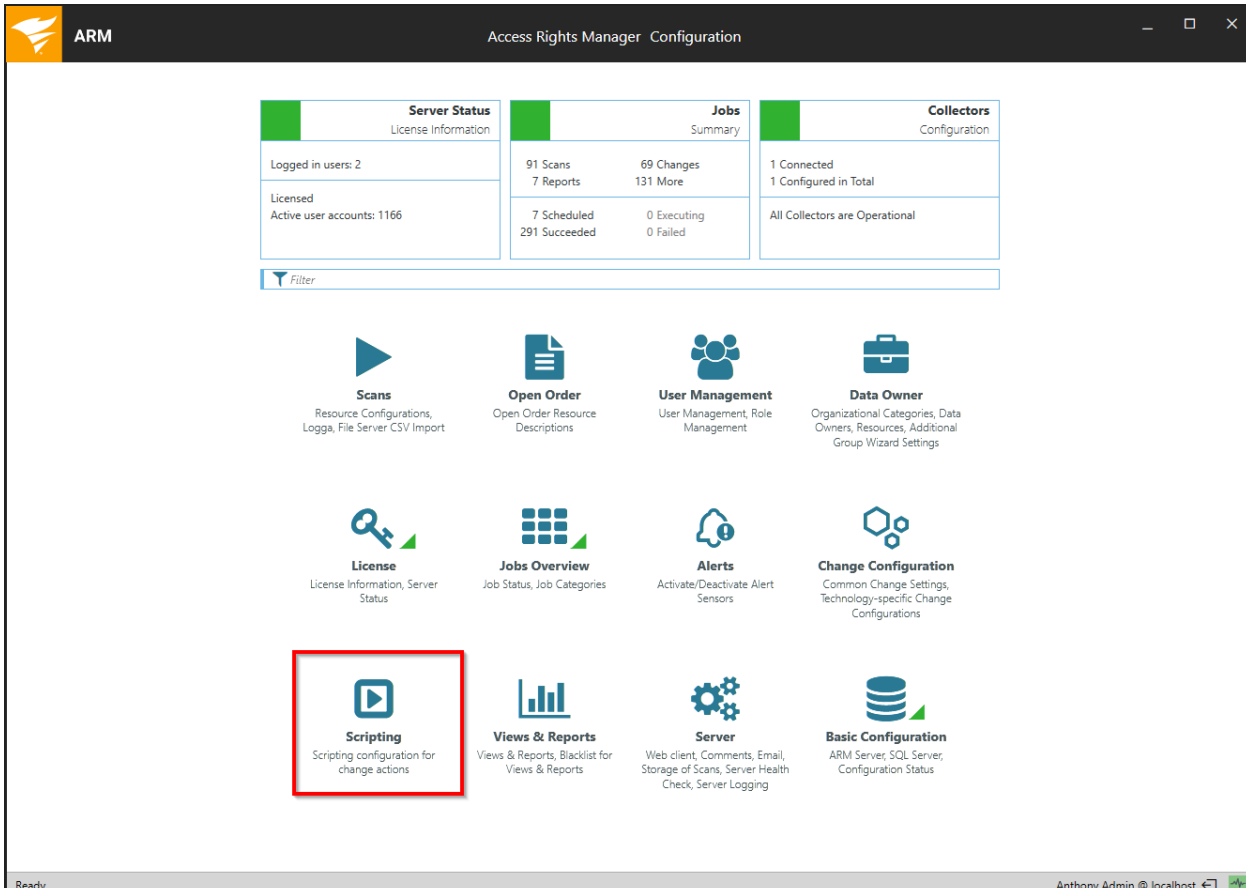
```
%ProgramData%\protected-networks.com\8MAN\scripts\analyze
```

Supported file types are:

- .ps (PowerShell)
- .vbs (VisualBasic)
- .bat
- .cmd

- .js (nodejs.exe)
- .exe

**i** Required PowerShell modules must be installed on the ARM server.



On the start page of the ARM configuration application, click "Scripting".

ARM Access Rights Manager Configuration

## Scripting

**Quick info**

**Scripting Configuration**  
Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, js (nodejs.exe) and .exe. Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Change actions Alerts Order templates / Service actions

New [Add](#)

Execution point	Action	Preselection	Script file on server	Parameters
after change action	Create user account	<input type="checkbox"/>	CreateHomeDir Berlin.ps1	Command line arguments {samaccountname} {department}
after change action	Create user account	<input type="checkbox"/>	CreateHomeDir Hannover.ps1	Command line arguments {samaccountname} {department}
after change action	Create user account	<input type="checkbox"/>	Welcome Package.ps1	Command line arguments {samaccountname} {department} {displayname} {employeeid}
after change action	Move AD Object	<input type="checkbox"/>	ChangeLocation.ps1	JSON object and additional argume -Std Berlin
after change action	Move AD Object	<input type="checkbox"/>	ChangeLocation.ps1	JSON object and additional argume -Std Hannover
after change action	Move AD Object	<input type="checkbox"/>	ChangeDepartment.ps1	Command line arguments {MoveObjectName} {MoveObjectGuid} {TargetOuDomain} {Tar
before change action	Delete user account	<input type="checkbox"/>	DeleteHomeDir Berlin.ps1	CSV object and additional argumer -Server FS-BLN-02
before change action	Delete user account	<input type="checkbox"/>	ArchiveAndDelMail.ps1	JSON object and additional argume {userprincipalname}
before change action	Delete user account	<input type="checkbox"/>	TryRemoveLotusAccount.ps1	Command line arguments {samaccountname}

Ready Anthony Admin @ localhost

Select the area for which you are configuring scripts.

ARM
Access Rights Manager Configuration

## Scripting

**Quick info**

**Scripting Configuration**  
 Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, .js (nodejs.exe) and .exe.

Use the command line preview by clicking the magnifying glass in the right column.

Supported actions and parameters 1

New 2
Change actions
Alerts
Order templates / Service actions

Execution point	Action	Preselection	Script file on server	Parameters
after change action	Create user account	<input type="checkbox"/>	CreateHomeDir Berlin.ps1	Command line arguments {samaccountname} {department}
after change action	Create user account	<input type="checkbox"/>	CreateHomeDir Hannover.ps1	Command line arguments {samaccountname} {department}
after change action	Create user account	<input type="checkbox"/>	Welcome Package.ps1	Command line arguments {samaccountname} {department} {displayname} {employeeid}
after change action	Move AD Object	<input type="checkbox"/>	ChangeLocation.ps1	JSON object and additional argume -Std Berlin
after change action	Move AD Object	<input type="checkbox"/>	ChangeLocation.ps1	JSON object and additional argume -Std Hannover
after change action	Move AD Object	<input type="checkbox"/>	ChangeDepartment.ps1	Command line arguments {MoveObjectName} {MoveObjectGuid} {TargetOuDomain} {Tar
before change action	Delete user account	<input type="checkbox"/>	DeleteHomeDir Berlin.ps1	CSV object and additional argumen -Server FS-BLN-02
before change action	Delete user account	<input type="checkbox"/>	ArchiveAndDelMail.ps1	JSON object and additional argume {userprincipalname}
before change action	Delete user account	<input type="checkbox"/>	TryRemoveLotusAccount.ps1	Command line arguments {samaccountname}

Apply

1. ARM shows you a list of all the supported change actions before or after which scripts can be executed, as well as available parameters.
2. Create a new script configuration.



ARM Access Rights Manager Configuration

## Scripting

**Quick info**

**Scripting Configuration**  
Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, .js (nodejs.exe) and .exe. Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Change actions Alerts Order templates / Service actions

New Delete

Execution point	Action	Preselection	Script file on server	Parameters
after change action	Create user account	<input type="checkbox"/>	CreateHomeDir Berlin.ps1	Command line arguments [samaccountname] (department)
after change action	Create user account	<input type="checkbox"/>	CreateHomeDir Hannover.ps1	Command line arguments [samaccountname] (department)
after change action	Create user account	<input type="checkbox"/>	Welcome Package.ps1	Command line arguments [samaccountname] (department) [displayname] (employeeid)
after change action	Move AD Object	<input type="checkbox"/>	ChangeLocation.ps1	JSON object and additional argume -Std Berlin
after change action	Move AD Object	<input type="checkbox"/>	ChangeLocation.ps1	JSON object and additional argume -Std Hannover
after change action	Move AD Object	<input type="checkbox"/>	ChangeDepartment.ps1	Command line arguments [MoveObjectName] (MoveObjectGuid) (TargetOuDomain) (TargetOuName)
before change action	Delete user account	<input type="checkbox"/>	DeleteHomeDir Berlin.ps1	CSV object and additional argumer -Server FS-BLN-02
before change action	Delete user account	<input type="checkbox"/>	ArchiveAndDelMail.ps1	JSON object and additional argume [userprincipalname]
after change action	Please select actions	<input type="checkbox"/>	TryRemoveLotusAccount.ps1	Command line arguments [samaccountname]

Apply

Ready Anthony Admin @ localhost

1. Select whether to run the script before or after the action. Your selection filters the available actions (column 2).
2. Select an action for which you want to make a script available.
3. If you have several scripts available for an action, specify the default settings for the ARM users in the drop-down menu.

ARM Access Rights Manager Configuration

## Scripting

**Quick info**

**Scripting Configuration**  
Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, js (nodejs.exe) and .exe. Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Change actions Alerts Order templates / Service actions

Action	Preselection	Script file on server	Parameters
Create user account	<input type="checkbox"/>	CreateHomeDir Berlin.ps1	Command line arguments {samaccountname} {department}
Create user account	<input type="checkbox"/>	CreateHomeDir Hannover.ps1	Command line arguments {samaccountname} {department}
Create user account	<input type="checkbox"/>	Welcome Package.ps1	Command line arguments {samaccountname} {department} {displayname} {employeeid} {givenname} {sn} {Password} {u
Move AD Object	<input type="checkbox"/>	ChangeLocation.ps1	JSON object and additional argume -Std Berlin
Move AD Object	<input type="checkbox"/>	ChangeLocation.ps1	JSON object and additional argume -Std Hannover
Move AD Object	<input type="checkbox"/>	ChangeDepartment.ps1	Command line arguments {(MoveObjectName) (MoveObjectGuid) (TargetOuDomain) (TargetOuGuid)}
Delete user account	<input type="checkbox"/>	DeleteHomeDir Berlin.ps1	CSV object and additional argumer -Server FS-BLN-02
Delete user account	<input type="checkbox"/>	ArchiveAnc...ail.ps1	JSON object and ...sonal argume {userprincipalname}
Create user account	<input type="checkbox"/>	CreateHomeDir Berlin.ps1	Command line arguments {samaccountname}

Ready Anthony Admin @ localhost

1. Select a script file.
2. Select how ARM passes the parameters to the script.

You can select the parameters directly or pass them as JSON or CSV objects.

ARM
Access Rights Manager Configuration

## Scripting

**Quick info**

**Scripting Configuration**

Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, .js (nodejs.exe). Use the command line preview by clicking the magnifying glass in the right column.

**Change actions** | Alerts | Order templates / Service actions


Arguments	[samaccountname] (department)
Arguments	[samaccountname] (department)
Arguments	[samaccountname] (department) [displayname] [employeeid] [givenname] [sn] [Password] [userprincipalname]
Additional argument	-Std Berlin
Additional argument	-Std Hannover
Arguments	[MoveObjectName] [MoveObjectGuid] [TargetOuDomain] [TargetOuGuid]
Additional argument	-Server FS-BLN-02
Additional argument	[userprincipalname]
Arguments	[samaccountname]

accountexpires  
admincount  
AuthorComment  
AuthorName  
cn  
comment  
CommonName  
company  
Deactivated  
department  
description  
displayname  
distinguishedname  
DomainController  
DomainName  
employeeid  
employeetype  
givenname  
homedirectory  
homedrive  
homephone  
info  
initials  
JobCreationTime  
JobName  
jpegphoto  
l  
lastlogon  
lastlogontimestamp  
lockouttime  
mail  
manager  
mobile  
name  
NewObjectGuid  
objectclass

in folder "%ProgramData%\protected-

[Supported actions and parameters](#)

Name		
man Create HomeDirectory Berlin	A	Q
man Create HomeDirectory Hannover	A	Q
man Welcome Package	A	Q
man Change Location Berlin	A	Q
man Change Location Hannover	A	Q
man Change Department	A	Q
man Delete HomeDirectory Berlin	A	Q
man Archive and Delete Mail	A	Q
man 8man-demo\sa-8man Delete IBM Notes Account	A	Q

 Apply

Select the command line parameters.

ARM
Access Rights Manager Configuration

## Scripting

Quick info

**Scripting Configuration**

Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, .js (nodejs.exe) and .exe. Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Change actions
Alerts
Order templates / Service actions

	Parameters		Credentials	Name
in.ps1	Command line arguments	{samaccountname} {department}	8man-demo\sa-8man	Create Hor
mover.ps1	Command line arguments	{samaccountname} {department}	8man-demo\sa-8man	Create Hor
s1	Command line arguments	{samaccountname} {department} {displayname} {employeeid} {givenname} {sn} {Password} {userprincipalname}	8man-demo\sa-8man	Welcome P
	JSON object and additional argume	-Std Berlin	8man-demo\sa-8man	Change Lo
	JSON object and additional argume	-Std Hannover	8man-demo\sa-8man	Change Lo
ps1	Command line arguments	{MoveObjectName} {MoveObjectGuid} {TargetOuDomain} {TargetOuGuid}	8man-demo\sa-8man	Change De
in.ps1	CSV object and additional argumen	-Server FS-BLN-02	8man-demo\sa-8man	Delete Hor
ps1	JSON object and additional argume	{userprincipalname}	8man-demo\sa-8man	Archive anc
ount.ps1	Command line arguments	{samaccountname}	8man-demo\sa-8man	Delete IBM

Apply

Select the type of data transfer to the script. Using a JSON or CSV object as a selection causes the script to provide a temporary file that contains the object data in the selected format.

ARM Access Rights Manager Configuration

## Scripting

**Quick info**

**Scripting Configuration**  
Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, js (nodejs.exe) and .exe.  
Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Change actions Alerts Order templates / Service actions

		Credentials	Name	
Arguments	[samaccountname] (department)	8man-demo\sa-8man	Create HomeDirectory Berlin	[A] [Q]
Arguments	[samaccountname] (department)	8man-demo\sa-8man	Create HomeDirectory Hannover	[A] [Q]
Arguments	[samaccountname] (department) [displayname] [employeeid] [givenname] [sn] [Password] [userprincipalname]	8man-demo\sa-8man	Welcome Package	[A] [Q]
Additional argument	-Std Berlin	8man-demo\sa-8man	Change Location Berlin	[A] [Q]
Additional argument	-Std Hannover	8man-demo\sa-8man	Change Location Hannover	[A] [Q]
Arguments	[MoveObjectName] [MoveObjectGuid] [TargetOuDomain] [TargetOuGuid]	8man-demo\sa-8man	Change Department	[A] [Q]
Additional argument	-Server FS-BLN-02	8man-demo\sa-8man	Delete HomeDirectory Berlin	[A] [Q]
Additional argument	[userprincipalname]	8man-demo\sa-8man	Archive and Delete Mail	[A] [Q]
Arguments	[samaccountname]	8man-demo\sa-8man	Delete IBM Notes Account	[A] [Q]

Ready Anthony Admin @ localhost

1. Specify credentials to run the script. If you do not specify any, the credentials from the [basic configuration](#) are used.
2. Give the script assignment a unique name for the selection in the ARM applications.
3. Optional but recommended: Leave a description.

The screenshot shows the ARM Configuration window with the 'Scripting' section active. A 'Command line preview' dialog is overlaid, showing a PowerShell command for running a script. The command is: `powershell.exe -executionpolicy bypass -inputformat none -File C:\ProgramData\protected-networks.com\8MAN\scripts\analyze\ArchiveAndDelMail.ps1 -json {jsonfile} {userprincipalname}`. Below the command is a 'Copy to clipboard' link and a 'Close' button. A vertical search bar is visible on the right side of the dialog.

Get a command line preview at any time.

## DEEP DIVE: Pass parameters to a script via JSON or CSV

In the "Deep Dive" you learn how exactly parameters are transferred to a script via JSON or CSV file.

The following chapters describe:

1. General: Include a template with a script call in ARM. Described using the example "[Disable a user via GrantMA](#)".
2. In detail: [Pass the parameters to the script via JSON or CSV](#).

## Disable a user via GrantMA

### Background / Value

Ordering a new user on the GrantMA Self-Service Portal is natively supported by ARM. Disabling a user after the order workflow has been completed becomes possible through the use of scripts. The combination GrantMA - Scripts - ARM webAPI opens up a multitude of further possibilities to automate documented processes.

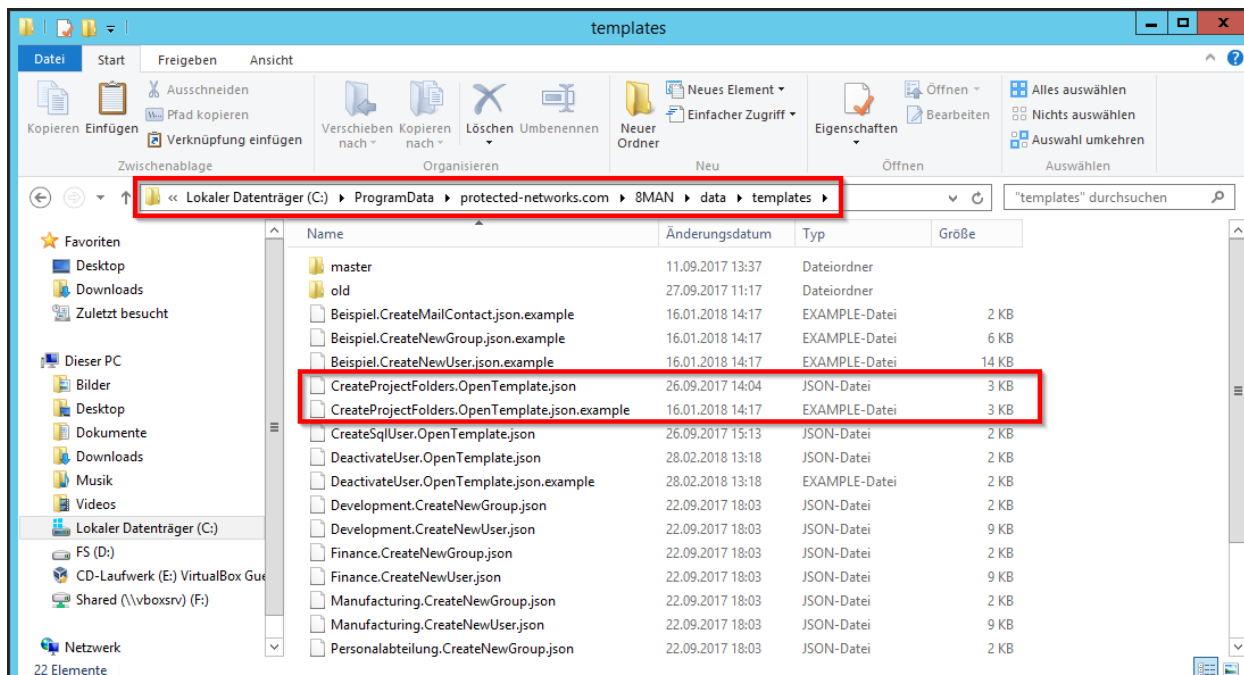
An example is the option described below of ordering the deactivation of a user:

1. Define an open template and ask for required values in a request in GrantMA.
2. After approval, the values are passed to a script.
3. The script controls ARM via the webAPI to perform the required action in ARM.
4. ARM executes the action and logs it in the ARM logbook.

### Related features

[Create a user account as an HR employee](#)

### Step-by-step process



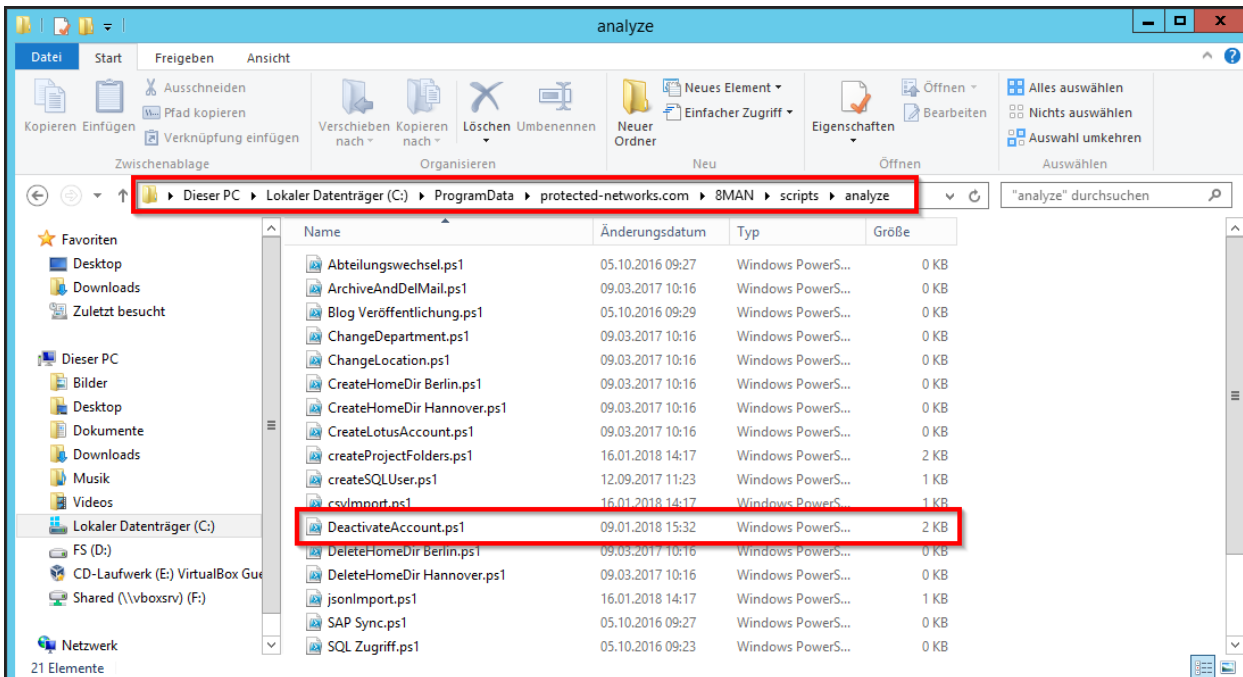
In the directory

```
%programdata%\Protected Networks\8MAN\data\templates
```

ARM provides a sample template for disabling users.

Copy the sample file, remove the suffix ".example" and make adjustments as needed. For more information, see the "[Customize ARM Templates](#)" section.

The template will be loaded automatically. Errors while loading the template are displayed in the [server health check](#).



In the directory

OLD: %programdata%\Protected Networks\8MAN\scripts\analyze

NEW: %programdata%\SolarWinds\ARM\scripts\analyze

ARM provides a sample script for disabling users.



**ARM** Access Rights Manager Configuration

## Scripting

**Quick info**

### Scripting Configuration

Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, .js (nodejs.exe) and .exe. Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Change actions Alerts **Order templates / Service actions**

New Delete

Usage	Preselection	Script file on server	Parameters	Cre
Template	<input type="checkbox"/>	createProjectFolders.ps1	JSON object and additional argume	8rr
Template	<input type="checkbox"/>	createSQLUser.ps1	Command line arguments	8rr
Template	<input type="checkbox"/>	DeactivateAccount.ps1	Command line arguments	8rr

Apply

Ready Anthony Admin @ localhost

On the start page of the ARM configuration select "Scripts".

1. Click on the tab "Order templates / Service actions".
2. Choose "Template".
3. Select the script, in this example here "DeactivateAccount.ps1".

ARM
Access Rights Manager Configuration

## Scripting

**Quick info**

**Scripting Configuration**  
 Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, .js (nodejs.exe) and .exe. Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Change actions | Alerts | Order templates / Service actions

Parameters	Credentials	Name
JSON object and additional arguments	8man-demo\sa-8man	createProjectFolders
Command line arguments: -UserName {UserName} -Password {Password} -DataSource {SqlServerInstanz}	8man-demo\sa-8man	createSQLUser
Command line arguments: -authZToken {UserAuthZToken} comment {UserComment} targetDate {Zieltermin} -accountDn {KontoDn}	<optional>	deactivateUser

- Department
- Folders
- Password
- ProjectName
- SqlServerInstanz
- TargetPath
- UserAuthZToken
- UserComment
- UserName
- WebApiBaseUrl

Apply

Specify which parameters are passed to the script.

In the example here, the authentication token and the comment are passed.

ARM Access Rights Manager Configuration

## Scripting

**Quick info**

### Scripting Configuration

Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, js (nodejs.exe) and .exe. Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Change actions	Alerts	Order templates / Service actions
ipt file on server	Parameters	Credentials
stateProjectFolders.ps1	JSON object and additional argume	8man-demo\sa-8man
stateSQLUser.ps1	Command line arguments	8man-demo\sa-8man
activateAccount.ps1	Command line arguments	<optional>

```
DeactivateUser.OpenTemplate.json - Visual Studio Code [Administrator]
File Edit Selection View Go Debug Tasks Help
DeactivateUser.OpenTemplate.json x
23 {
24   "Key": "TargetDate",
25   "value": {
26     "Type": "DatePicker",
27     "Label": "Date of deactivation",
28     "IsRequired": true,
29     "ScriptParameterFormat": "0"
30   }
31 },
32 {
33   "Key": "AccountDn",
34   "value": {
35     "Type": "TextField",
36
```

In addition, the values queried in the template are passed to the script:

- The name of the account to be deactivated
- The date on which the account should be deactivated

The screenshot displays the ARM Configuration window for the 'Scripting' section. It includes a 'Quick info' area with 'Scripting Configuration' details and a table of scripts. A red box highlights the 'DeactivateUser' script in the table, and a red arrow points to its corresponding JSON template in a Visual Studio Code window.

Object and additional arguments	Credentials	Name
<input type="text"/>	8man-demo\sa-8man	createProjectFolders
<input type="text" value="-UserName (UserName) -Password (Password) -DataSource (SqlServerInstanz)"/>	8man-demo\sa-8man	createSQLUser
<input type="text" value="-authZToken (UserAuthZToken) -comment (UserComment) -targetDate (TargetDate) -accountDn (AccountDn)"/>	<optional>	DeactivateUser

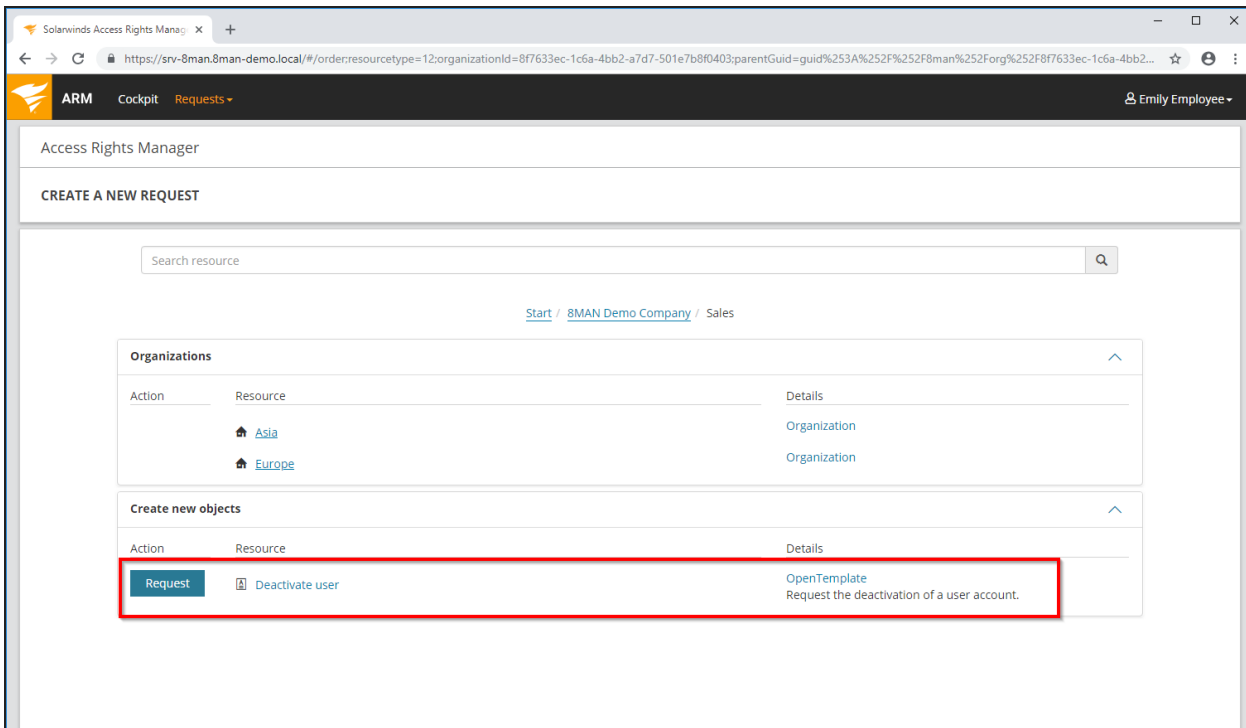
```
1  [{"Version": 1,
2  "TemplateType": "OpenTemplate",
3  "Id": "bb3bd40e-911d-4180-8520-bba4beca2c5e",
4  "DisplayName": "Deactivate user",
5  "Description": "Request the deactivation of a user account.",
6  "ManualInteractionRequired": "false",
7  "ScriptToExecute": "DeactivateUser",
8  "Form": {
9    "Type": "Container",
10   "Label": "Request to deactivate a user",
11   "Templates": [{"Key": "User", "Value": {
```

Enter the name of the script. The name must match the call in the template.

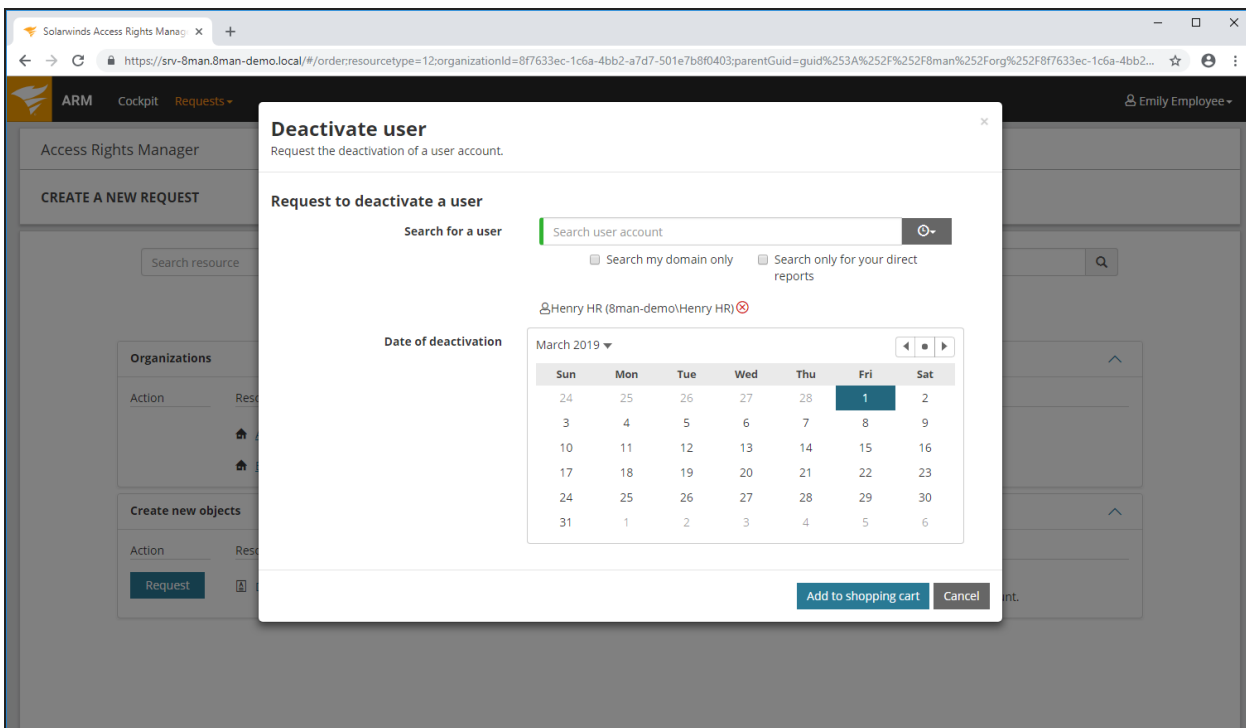
The screenshot displays the 'Data Owner configuration' window in the ARM interface. The 'Sales' organizational category is selected. The 'Resources' table lists various resources, including Active Directory groups, File servers, and Templates. The 'Template (3)' section is expanded, showing 'Deactivate user (8man)'. A red box highlights this template, and a red arrow points to its entry in the Resources table. Another red box highlights the 'Deactivate user' template in the 'Resource selection' pane on the right. The 'User & Group selection' pane shows a list of users and groups, with 'Marketing (8man-demo)\Marketing' selected.

In the Data Owner configuration you set the template to requestable.

1. Use Drag & Drop to add the template to an organizational category.
2. The template must be requestable (default) and modifiable.



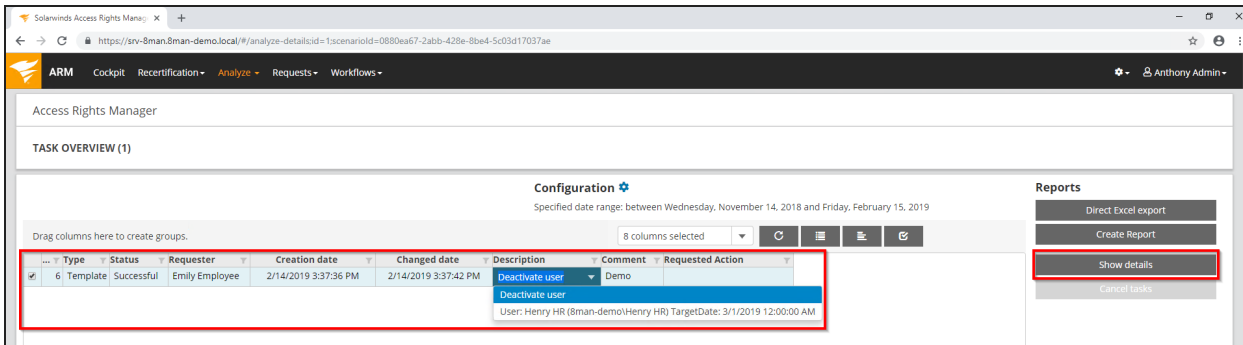
Start the request in GrantMA.



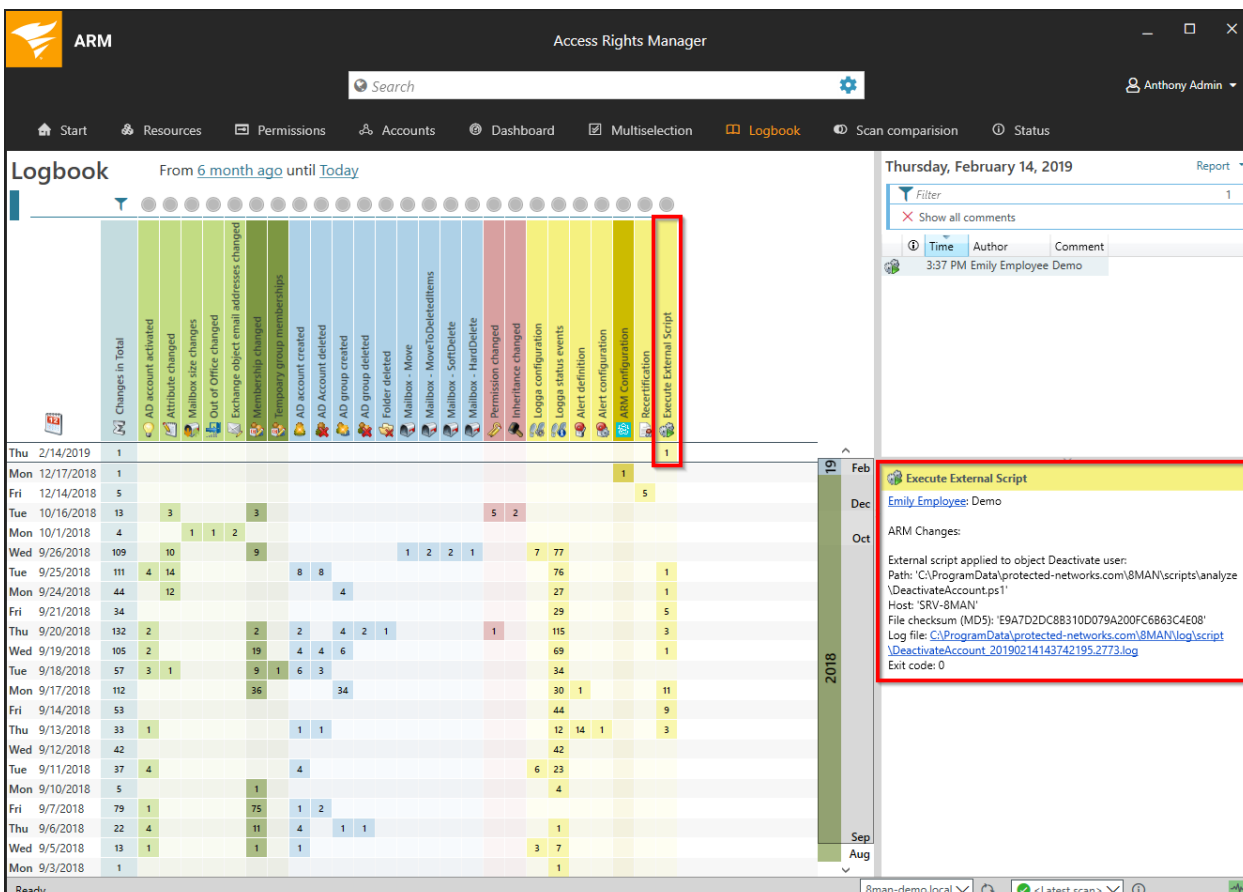
The freely configurable template queries the values that will later be passed as parameters to the script. In the example here:

- The account to be deactivated.
- The date on which the account should be deactivated.

After completing and approving the order as usual, the script will be executed automatically.



In the task overview, you can see details about job execution. Successful job execution here means that the script started successfully.



For information about the script execution, see the ARM Log.

To diagnose script execution errors, use the linked log file.

## Pass parameters to a script via JSON or CSV

The transfer of parameters to the script can be done either directly or through a JSON or CSV file. The direct entry is described in the previous section "[Disabling a user via GrantMA](#)".

Using a JSON or CSV file is especially convenient if you want to pass many parameters to a script. In particular, the JSON format in Powershell can be used immediately as an object.

Here's a sample PowerShell script that simply outputs the parameters passed by JSON.

### Location

```
%ProgramData%\Protected Networks\8MAN\scripts\analyze\jsonImport.ps1
```

### Code

```
param(  
    [string]$json  
)  
  
# example for reading json formatted data addressed by $json over command line  
# Read all data from json file into an object  
Write-Host $json  
  
(Get-Content $json) -join "`n" | ConvertFrom-Json | Write-Host  
  
# here you can alternatively assign and compute the object
```



## Configuration of the script

**ARM** Access Rights Manager Configuration

## Scripting

**Quick info**

### Scripting Configuration

Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, .js (nodejs.exe) and .exe. Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Change actions Alerts Order templates / Service actions

New Delete

Usage	Preselection	Script file on server	Parameters	Create
Template	<input type="checkbox"/>	createProjectFolders.ps1	JSON object and additional argume	
Template	<input type="checkbox"/>	createSQLUser.ps1	Command line arguments	
Template	<input type="checkbox"/>	jsonImport.ps1	JSON object and additional argume	

Apply

Ready Anthony Admin @ localhost

1. Enter the name of the script.
2. Select "JSON object and additional parameters" dropdown.
3. Optional: Specify additional parameters that will be passed to the script in addition to those contained in the JSON file.

The screenshot displays the 'Scripting' configuration page in the ARM interface. It includes a 'Quick info' section with 'Scripting Configuration' details. Below this is a table for configuring scripts, with columns for 'Name', 'Credentials', and 'Script'. A red box highlights the 'DeactivateUser' script in the table. Below the table, a Visual Studio Code window shows the JSON template for 'DeactivateUser.OpenTemplate.json', with a red box highlighting the 'ScriptToExecute' field set to 'DeactivateUser'.

**Scripting Configuration**

Using scripts that can supplement ARM

- executed change actions and automate the steps that precede or follow an action
- trigger specific actions if alerts occur
- define actions for order templates

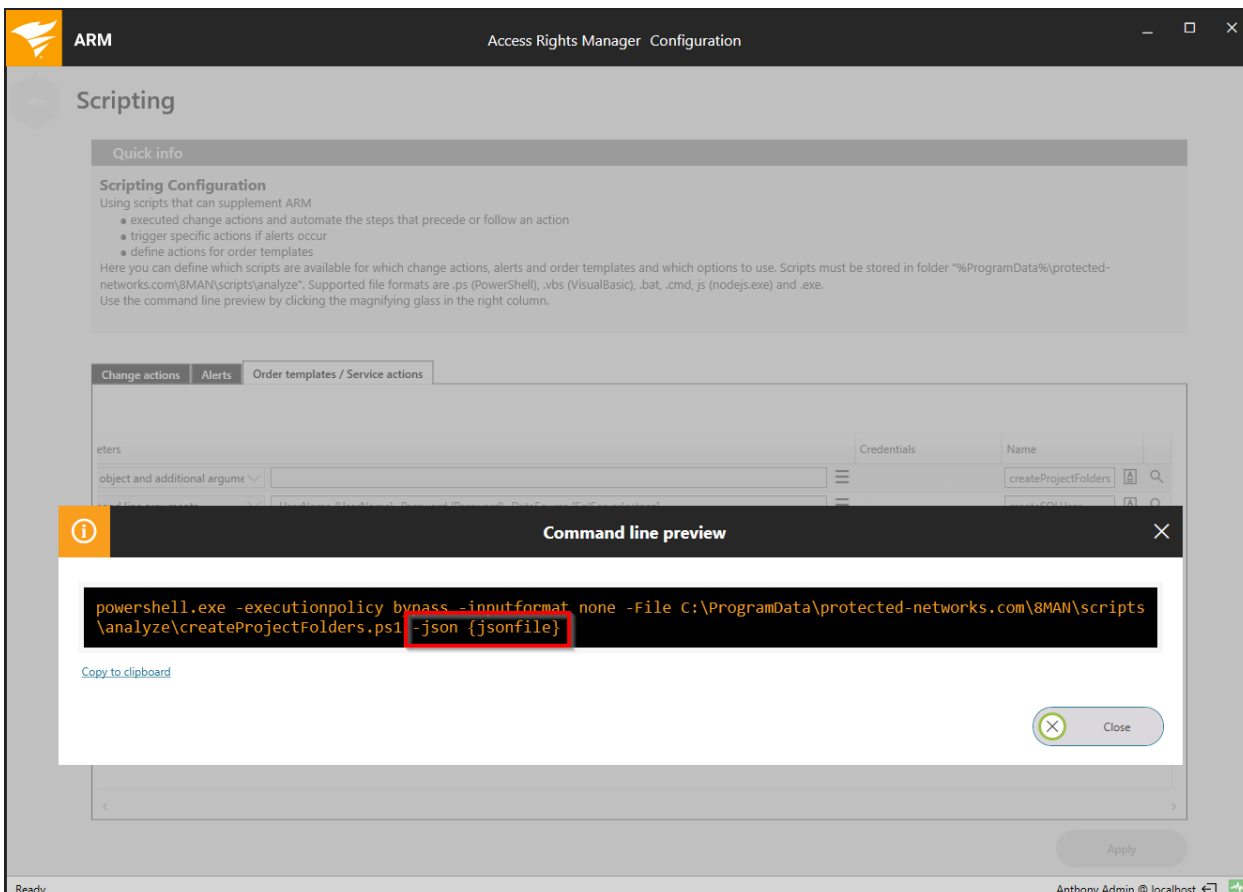
Here you can define which scripts are available for which change actions, alerts and order templates and which options to use. Scripts must be stored in folder "%ProgramData%\protected-networks.com\8MAN\scripts\analyze". Supported file formats are .ps (PowerShell), .vbs (VisualBasic), .bat, .cmd, js (nodejs.exe) and .exe. Use the command line preview by clicking the magnifying glass in the right column.

[Supported actions and parameters](#)

Object and additional arguments	Credentials	Name
<input type="text"/>	8man-demo\sa-8man	createProjectFolders
<input type="text"/>	8man-demo\sa-8man	createSQLUser
<input type="text"/>	<optional>	DeactivateUser

```
DeactivateUser.OpenTemplate.json - Visual Studio Code [Administrator]
File Edit Selection View Go Debug Tasks Help
DeactivateUser.OpenTemplate.json x
1  [{"Version": 1,
2  "TemplateType": "OpenTemplate",
3  "Id": "bb3bd40e-911d-4180-8520-bba4beca2c5e",
4  "DisplayName": "Deactivate user",
5  "Description": "Request the deactivation of a user account.",
6  "ManualInteractionRequired": "false",
7  "ScriptToExecute": "DeactivateUser",
8  "Form": {
9    "Type": "Container",
10   "Label": "Request to deactivate a user",
11   "Templates": [
12     {
13       "Key": "User",
14       "Value": {
```

Enter the name of the script. The name must match the call in the template.



In the command line preview, you will see the call of the JSON file.

The JSON file is temporarily stored here after filling in the template:

`%ProgramData%\protected-networks.com\8MAN\tmp\script\`

and gets a file name with timestamp, for example:

`jsonImport_param_20180318130028263.json`

The variable `{jsonfile}` can be used as the filename on the command line.

Supported field types / input options from the templates

Textfield

Returns the text content. If the field is empty, it will not be transported.

DropDown

Returns the value of the selection, not the display value.

### Checkbox

Returns the text "True" if the box was selected, otherwise "False".

### DatePicker

Returns the text of the selected time. The output format can be influenced by the parameter "ScriptParameterFormat" ([.net definitions](#)).

### RadioButton

Returns the text of the selected radio button. The key is the Radio GroupId.

### Example JSON-File

```
{
  "OnBoardingUser": "Horst Peter (arm-demo\\H.Peter)",
  "FirstName": "Horst",
  "LastName": "Peter",
  "LoginName": "H.Peter",
  "VPN2": "False",
  "VPN": "True",
  "WLAN": "True",
  "Teamwarp": "True",
  "Jira": "False",
  "HomeDir": "True",
  "When": "2018-03-28T22:00:00.0000000Z",
  "DropDownValue": "Value B",
  "UserComment": "LOL"
}
```

# Jobs overview

The screenshot shows the SolarWinds ARM Configuration interface. At the top, there are three summary tiles: Server Status, Jobs, and Collectors. The Jobs tile is highlighted with a red box and contains the following data:

Jobs Summary	
91 Scans	69 Changes
7 Reports	132 More
7 Scheduled	0 Executing
292 Succeeded	0 Failed

Below the summary tiles is a grid of functional tiles. The 'Jobs Overview' tile is also highlighted with a red box. It contains the following information:

- Jobs Overview**
- Job Status, Job Categories

Other visible tiles include Scans, Open Order, User Management, Data Owner, License, Alerts, Change Configuration, Scripting, Views & Reports, Server, and Basic Configuration.

The job overview contains a variety of information including scan speed and the amount of collected data.

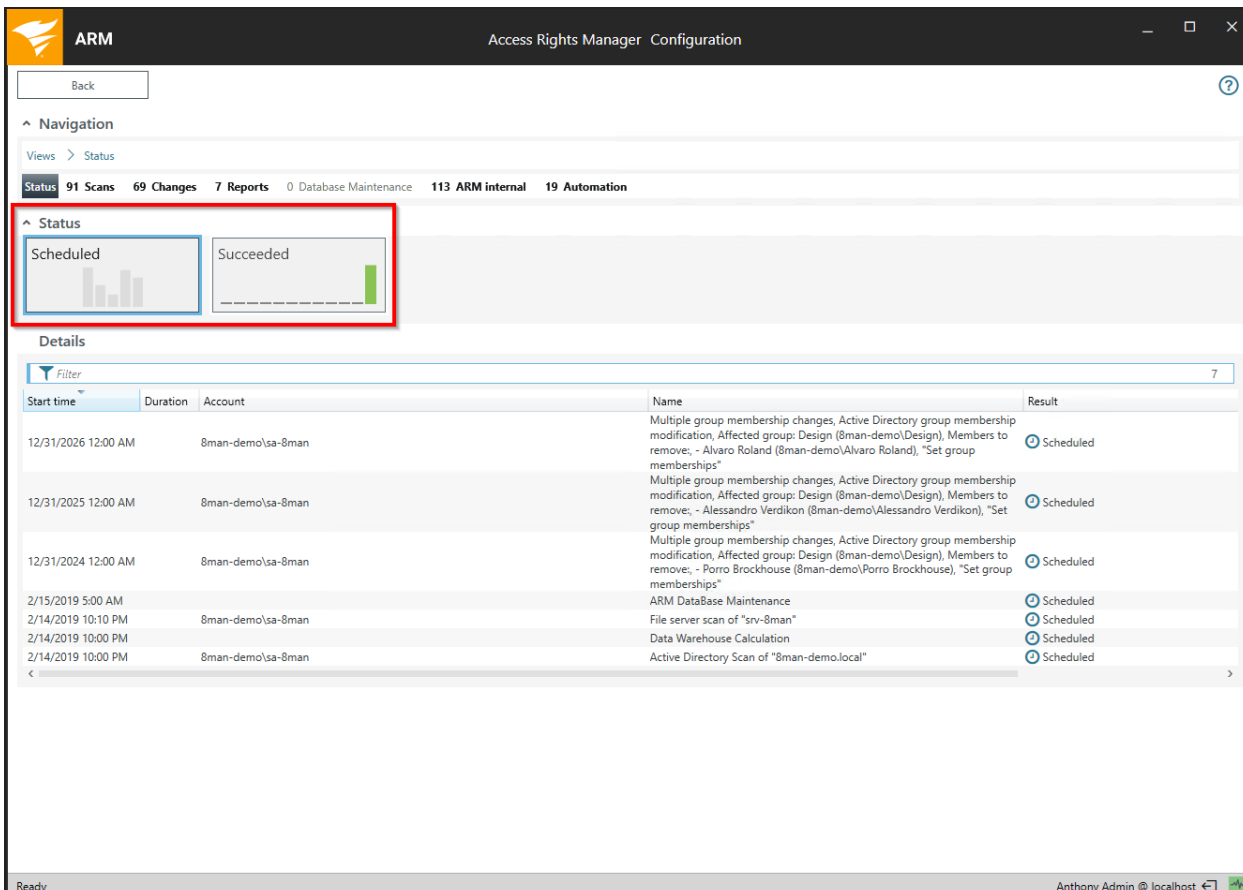
You are not able to edit or configure the displayed information in the job overview tile. Successful jobs are displayed for 2 weeks, failed jobs for 4 weeks.

Click the tile for more details.

The screenshot displays the SolarWinds Access Rights Manager (ARM) Configuration page. At the top, there is a navigation bar with the ARM logo and the title 'Access Rights Manager Configuration'. Below this is a 'Back' button and a help icon. A navigation menu is visible, with 'Views' highlighted in a red box. The menu includes 'Categories' and 'Status'. Below the navigation menu, there is a status summary section with two cards: 'Scheduled' and 'Succeeded'. The 'Scheduled' card shows a bar chart with four bars of increasing height. The 'Succeeded' card shows a bar chart with one bar. The main content area is mostly empty, with a message: 'Please select a job history diagram to view details...'. At the bottom of the interface, the status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Select between two views.

## Display jobs grouped by status



The screenshot shows the SolarWinds Access Rights Manager (ARM) Configuration interface. The top navigation bar includes a 'Back' button and a help icon. Below the navigation bar, there is a 'Views > Status' breadcrumb. The main content area is titled 'Status' and displays a summary of job counts: 91 Scans, 69 Changes, 7 Reports, 0 Database Maintenance, 113 ARM internal, and 19 Automation. A red box highlights the 'Status' section, which contains two bar charts: 'Scheduled' and 'Succeeded'. The 'Scheduled' chart shows a distribution of bars representing different job statuses, while the 'Succeeded' chart shows a single bar representing the count of successful jobs. Below the charts, there is a 'Details' section with a filter bar and a table of job details. The table has columns for Start time, Duration, Account, Name, and Result. The table lists several jobs, all of which are 'Scheduled'.

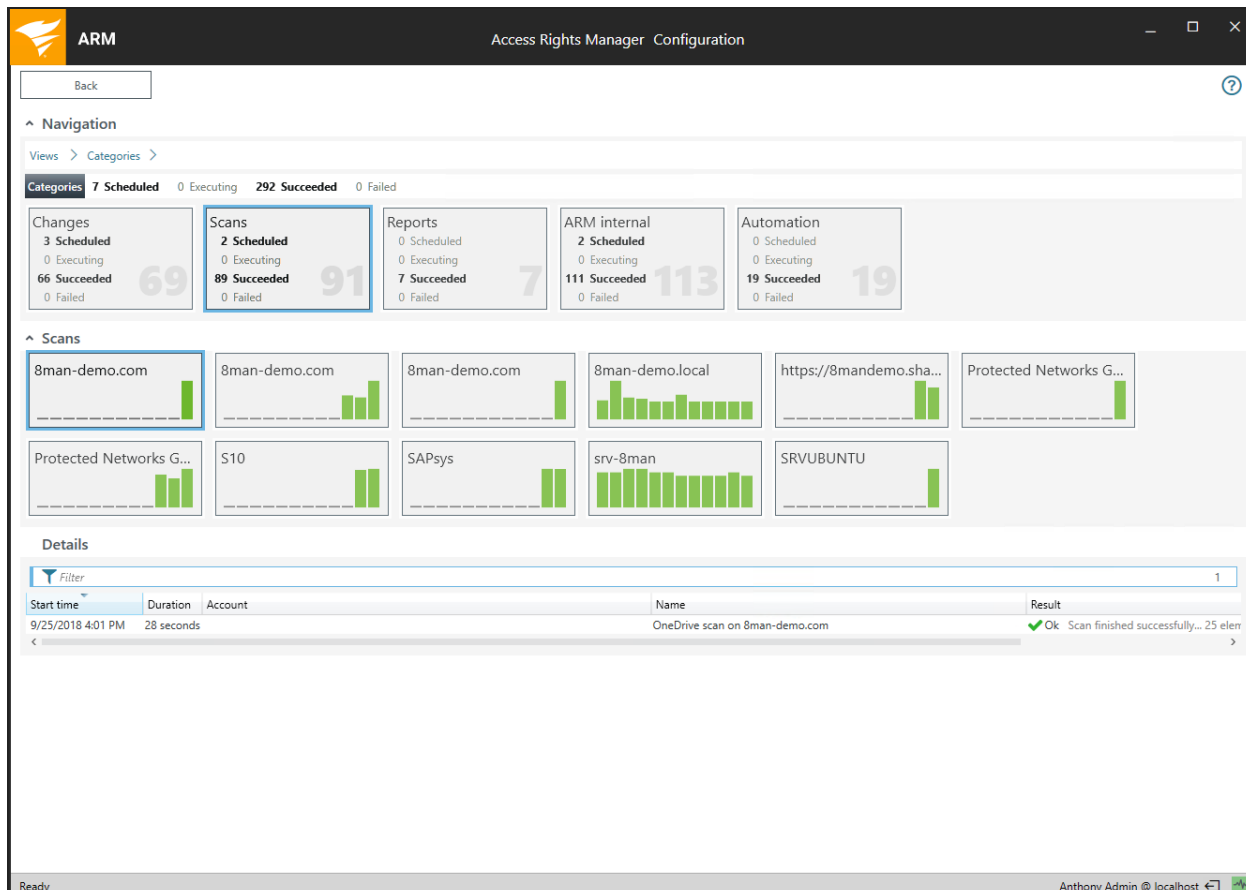
Start time	Duration	Account	Name	Result
12/31/2026 12:00 AM		8man-demo\sa-8man	Multiple group membership changes, Active Directory group membership modification, Affected group: Design (8man-demo\Design), Members to remove; - Alvaro Roland (8man-demo\Alvaro Roland), "Set group memberships"	Scheduled
12/31/2025 12:00 AM		8man-demo\sa-8man	Multiple group membership changes, Active Directory group membership modification, Affected group: Design (8man-demo\Design), Members to remove; - Alessandro Verdikon (8man-demo\Alessandro Verdikon), "Set group memberships"	Scheduled
12/31/2024 12:00 AM		8man-demo\sa-8man	Multiple group membership changes, Active Directory group membership modification, Affected group: Design (8man-demo\Design), Members to remove; - Porro Brockhouse (8man-demo\Porro Brockhouse), "Set group memberships"	Scheduled
2/15/2019 5:00 AM			ARM DataBase Maintenance	Scheduled
2/14/2019 10:10 PM		8man-demo\sa-8man	File server scan of "srv-8man"	Scheduled
2/14/2019 10:00 PM			Data Warehouse Calculation	Scheduled
2/14/2019 10:00 PM		8man-demo\sa-8man	Active Directory Scan of "8man-demo.local"	Scheduled

You can see a job progress diagram for every status.

Click on a diagram to view the associated jobs.

Hover over the bars in the diagram to receive a quick preview.

## Display jobs grouped by category



The screenshot shows the 'Access Rights Manager Configuration' window. The 'Categories' view is active, displaying a summary of job counts for various categories. The 'Scans' category is highlighted with a blue border.

**Categories Summary:**

Category	Scheduled	Executing	Succeeded	Failed
Changes	3	0	66	0
Scans	2	0	89	0
Reports	0	0	7	0
ARM internal	2	0	111	0
Automation	0	0	19	0

**Scans Category Details:**

Target	Progress
8man-demo.com	High (Green bars)
8man-demo.com	Medium (Green bars)
8man-demo.com	Low (Green bars)
8man-demo.local	Medium (Green bars)
https://8mandemo.sha...	Low (Green bars)
Protected Networks G...	Low (Green bars)
Protected Networks G...	Low (Green bars)
S10	Low (Green bars)
SAPsys	Low (Green bars)
srv-8man	Medium (Green bars)
SRVUBUNTU	Low (Green bars)

**Details Table:**

Start time	Duration	Account	Name	Result
9/25/2018 4:01 PM	28 seconds		OneDrive scan on 8man-demo.com	✓ Ok: Scan finished successfully... 25 eler

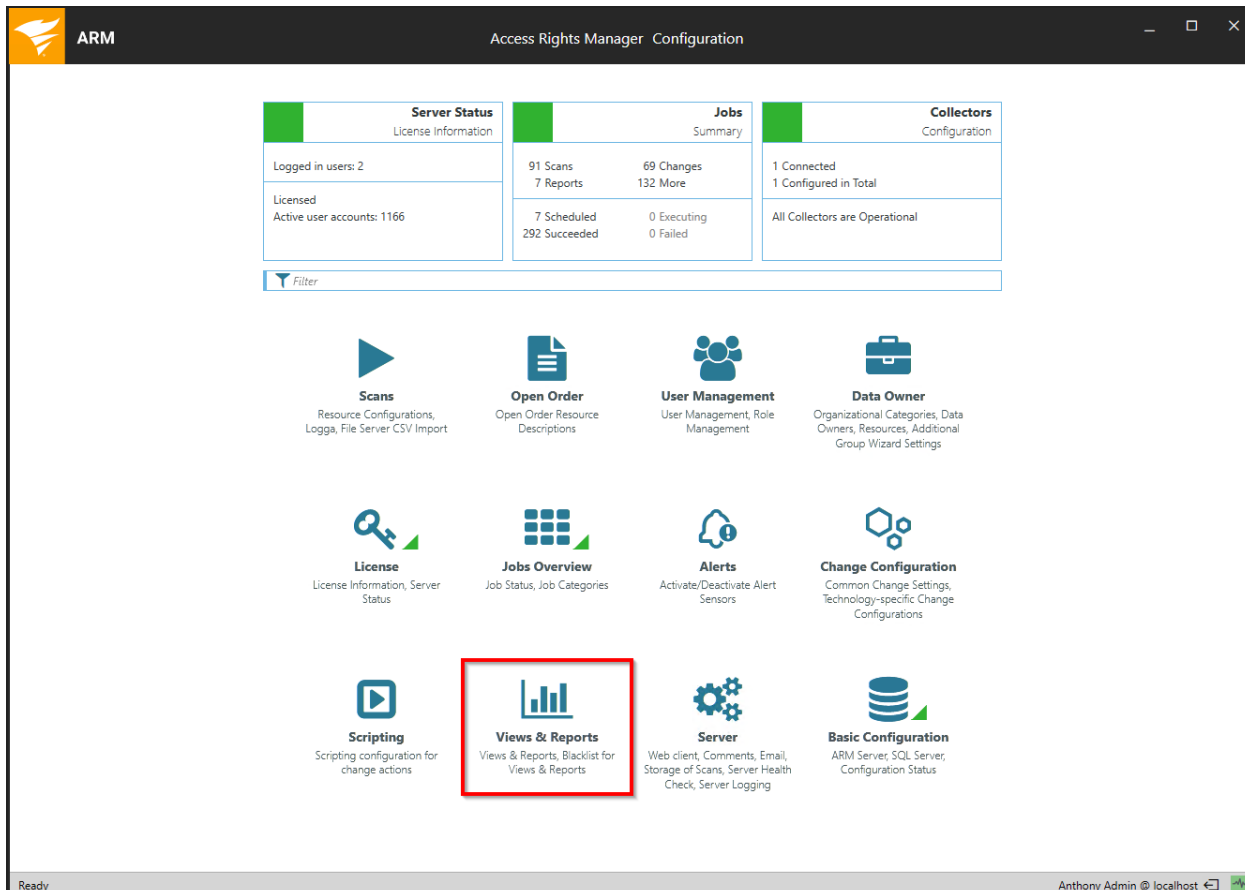
In the category view the jobs are listed in more granularity.

ARM provides job progress diagrams for each category.

Click on a diagram to list the associated jobs.



# Configure and view reports



The screenshot displays the ARM Configuration interface. At the top, there are three summary cards:

- Server Status** (License Information): Logged in users: 2; Licensed Active user accounts: 1166.
- Jobs** (Summary): 91 Scans, 7 Reports, 69 Changes, 132 More; 7 Scheduled, 292 Succeeded, 0 Executing, 0 Failed.
- Collectors** (Configuration): 1 Connected, 1 Configured in Total; All Collectors are Operational.

Below the summary cards is a 'Filter' button. The main area contains several configuration tiles:

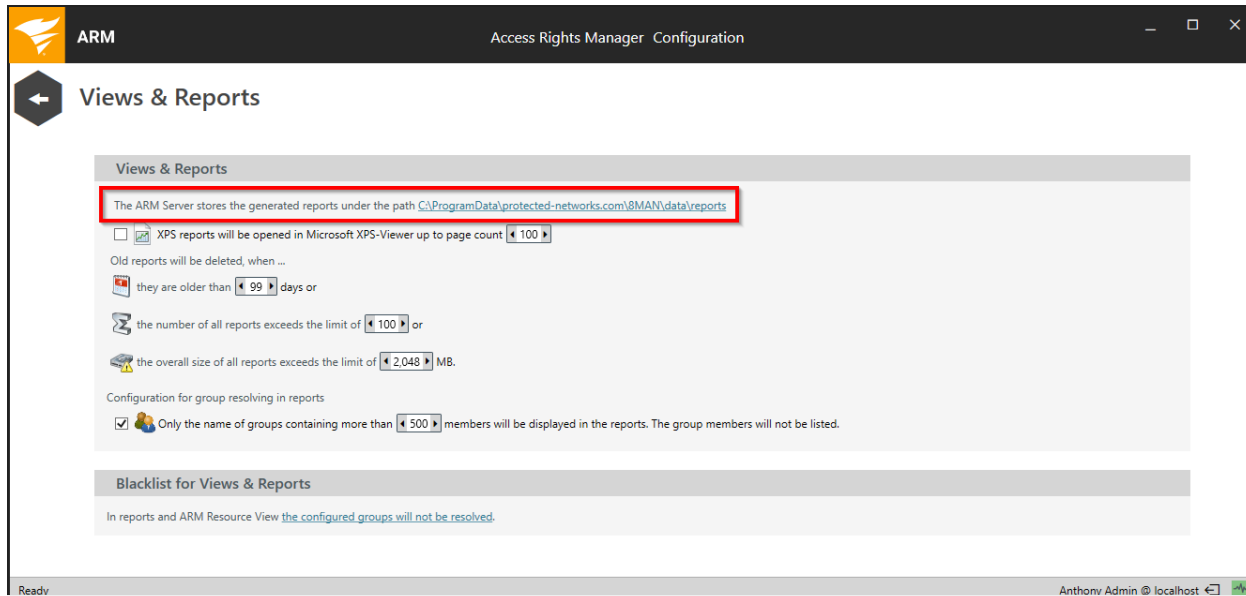
- Scans**: Resource Configurations, Logga, File Server CSV Import.
- Open Order**: Open Order Resource Descriptions.
- User Management**: User Management, Role Management.
- Data Owner**: Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings.
- License**: License Information, Server Status.
- Jobs Overview**: Job Status, Job Categories.
- Alerts**: Activate/Deactivate Alert Sensors.
- Change Configuration**: Common Change Settings, Technology-specific Change Configurations.
- Scripting**: Scripting configuration for change actions.
- Views & Reports** (highlighted with a red box): Views & Reports, Blacklist for Views & Reports.
- Server**: Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging.
- Basic Configuration**: ARM Server, SQL Server, Configuration Status.

The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Determine the options for report creation, views and blacklists.

Click on "Views & reports".

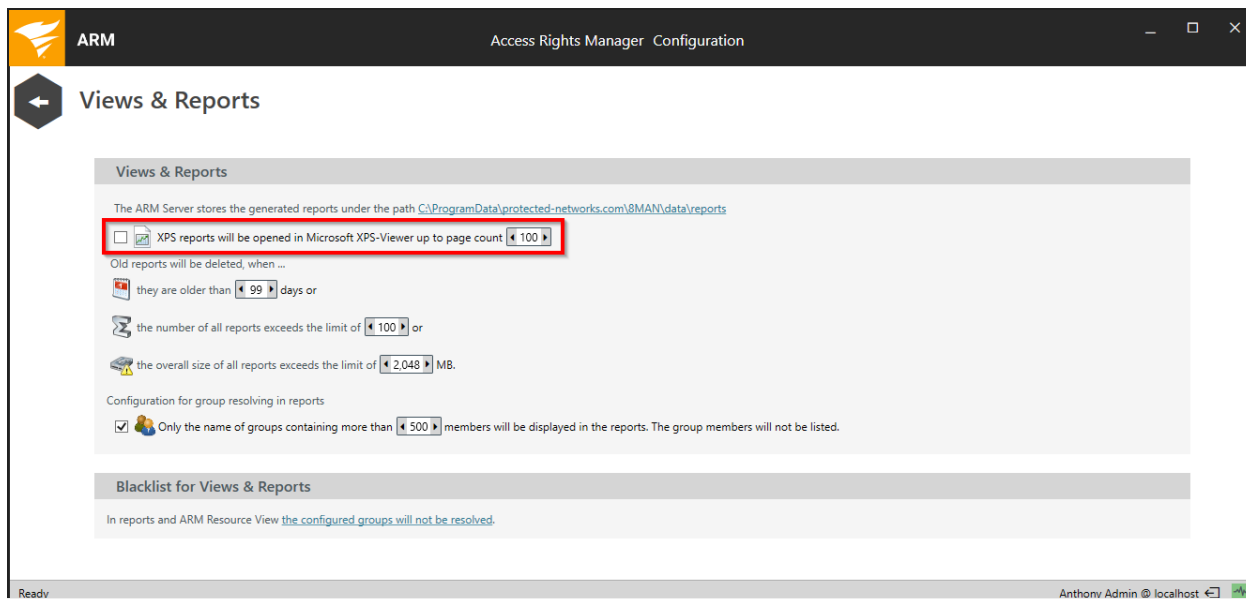
## Configure report options



Click the link to determine where ARM stores reports.

The default path is:

```
%ProgramData%\protected-networks.com\8MAN\data\reports
```



**i** From 8MAN/ARM version 8 on reports will no longer be created in XPS format. For compatibility reasons the XPS viewer will stay included to view earlier created reports in XPS format.

By default ARM uses its own XPS viewer when opening files in an XPS format. The ARM user interface is locked when displaying XPS reports.

Please use the Microsoft XPS viewer if you require the simultaneous availability of both report and ARM user interface.

## Configure the blacklist for views and reports

You can determine the groups for which members are not resolved in the views and reports. This allows for a better overview, especially for groups with large numbers of users. Affected are:

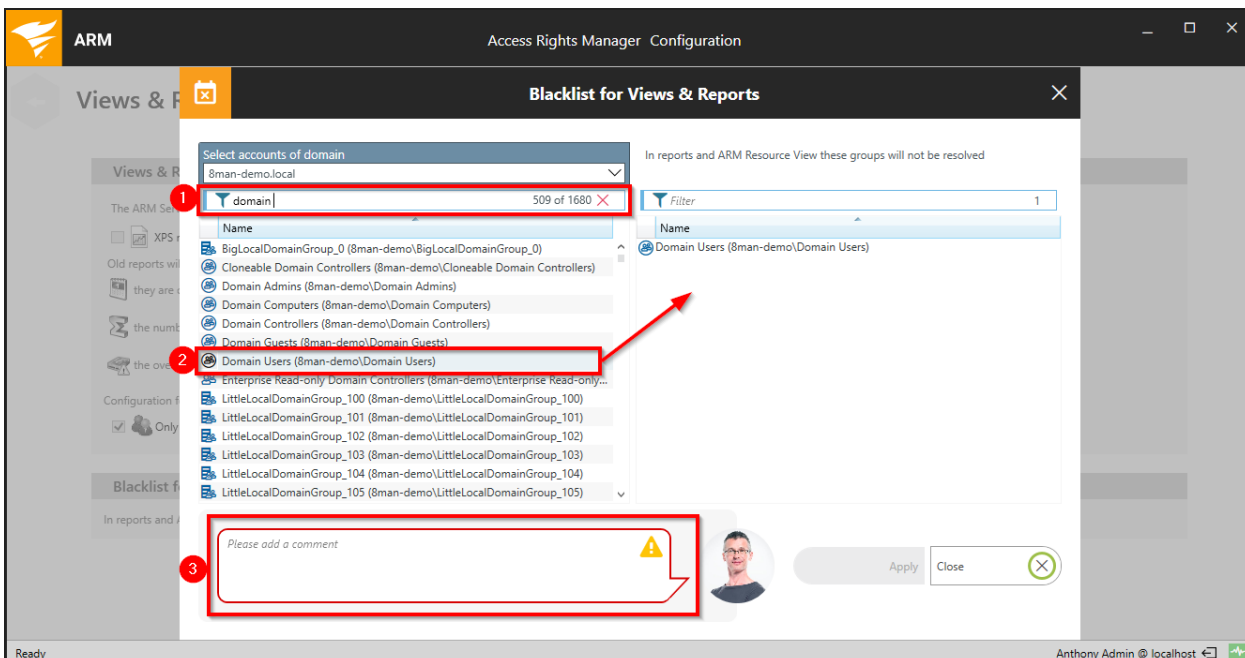
- reports
- views in ARM application
- Analyze&Act web interface

Examples:

- Domain users - This groups includes all users in the applied domain.
- Users (predefined) - This group includes all users within a selected context (for example domain, file server)

Hiding group memberships may also be required in order to ensure compliance with company regulations and guidelines.

Groups included in the blacklist are indicated with a blacklist icon in the resource view of the ARM application. Their members are not displayed.



1. Use the search to find the desired accounts.
2. Move accounts in and out of the blacklist via drag & drop.
3. You must enter a comment for the log book in order to be able to apply these changes.

# Open Order

The screenshot displays the ARM Configuration window. At the top, there are three summary cards:

- Server Status (License Information):** Logged in users: 2; Licensed Active user accounts: 1166.
- Jobs Summary:** 91 Scans, 7 Reports, 69 Changes, 132 More; 7 Scheduled, 292 Succeeded; 0 Executing, 0 Failed.
- Collectors Configuration:** 1 Connected, 1 Configured in Total; All Collectors are Operational.

Below the summary cards is a 'Filter' dropdown. The main area contains a grid of 12 tiles:

- Scans:** Resource Configurations, Logga, File Server CSV Import
- Open Order:** Open Order Resource Descriptions (highlighted with a red border)
- User Management:** User Management, Role Management
- Data Owner:** Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License:** License Information, Server Status
- Jobs Overview:** Job Status, Job Categories
- Alerts:** Activate/Deactivate Alert Sensors
- Change Configuration:** Common Change Settings, Technology-specific Change Configurations
- Scripting:** Scripting configuration for change actions
- Views & Reports:** Views & Reports, Blacklist for Views & Reports
- Server:** Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration:** ARM Server, SQL Server, Configuration Status

The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

With Open Order, you use GrantMA workflows for orders that are not executed with ARM after completion.

You define the available technologies and resources in an XML file, e.g. Hardware, software, or permissions for systems not integrated into ARM.

Customize the order with customizable templates (see [Customizing templates](#)).

## Define the requestable technologies and resources

Define the requestable technologies and resources in an XML file.

The XML file has the following structure:

1. [Set technology](#)
2. Define technology
  - [Define permissionsets](#)
  - [Summarizing permissions for types](#)
3. Describe resources
  - [Define resource root](#)
  - [Define resources](#)

## Example

```
<?xml version="1.0" encoding="utf-8"?>

<!-- do not change -->
<resourceImport Version="3">

<!-- technology definition -->
<technology Id="D54C16F2-42C1-477A-BD20-3285158F68D3" Name="Hardware" IconId="2"
Color="#0000be">
<definitions>
<permissionSets>
<permissionSet PermissionSetId="1" Description="['en-US:Buy','de-DE:Kaufen']" />
<permissionSet PermissionSetId="2" Description="['en-US:Lease','de-DE:Leasen']"
/>
<permissionSet PermissionSetId="3" Description="['en-US:Rent','de-DE:Mieten']"
/>
</permissionSets>
<types>
<type Id="1" Description="['en-US:Hardware','de-DE:Hardware']"
IconId="Container" PermissionSetIds="[]" />
<type Id="3" Description="['en-US:Desktop','de-DE:Desktop']" IconId="Computer"
PermissionSetIds="[1,2,3]" />
</types>
</definitions>

<!-- resource definition -->
<data>
<root Id="6CE9B526-9FFD-46A5-9ED0-36FB4E1303B5" Name="Computer" TypeId="1"
Merge="no">
<resource Name="Desktop PCs" TypeId="3" Description="['en-US:Stationary PC','de-
DE:Stationäre Arbeitsplatz-PCs']">
<resource Name="Desktop-PC simple" TypeId="3" />
<resource Name="Desktop-PC default" TypeId="3" />
```

```
<resource Name="Desktop-PC customizable" TypeId="3" TemplateID="E3865726-6FDF-489E-A7D5-4ABBA5B2BF83" />
</resource>
</root>
</data>
</technology>
</resourceImport>
```

## Set technology

An OpenOrder XML configuration can contain several technologies. In the first line of a technology section, specify the ID, name, and icon.

### Example

```
<!-- technology definition -->
<technology Id="D54C16F2-42C1-477A-BD20-3285158F68D3" Name="Hardware"
IconId="2">
```

### Id

Identifies the technology and must be unique within Open Order. Our recommendation: Use a GUID, e.g. from [guidgen.com](http://guidgen.com)

### Name

Display name of the technology.

### IconId

Displayed icon for the DataOwner configuration (not for GrantMA). See [predefined icons](#).

Define permission sets

In the **permissionSets** section, you define the technology's permission sets.

### Example

```
<permissionSets>
```

```
<permissionSet PermissionSetId="1" Description="['en-US:Buy','de-DE:Kaufen']" />
<permissionSet PermissionSetId="2" Description="['en-US:Lease','de-DE:Leasen']"
/>
<permissionSet PermissionSetId="3" Description="['en-US:Rent','de-DE:Mieten']"
/>
</permissionSets>
```

### PermissionSetId

Assign an integer that identifies the entry in the permission set.

### Description

Optionally provide a [description](#) of the permission set.

Define types

A type definition of a technology contains 0 to n permissions and an icon.

### Example

```
<types>
<type Id="1" Description="['en-US:Hardware','de-
DE:Hardware']" IconId="Container" PermissionSetIds="[]" />
<type Id="3" Description="['en-US:Desktop','de-DE:Desktop']" IconId="Computer"
PermissionSetIds="[1,2,3]" />
</types>
```

### Id

Assign an integer that identifies the type.

### Description

The displayed [description](#) of type.

### IconId

Displayed icon for the DataOwner configuration (not for the GrantMA). See [predefined icons](#).



## PermissionSetIds

A list of possible permissions for the type. An empty list of PermissionSetIds implies that a resource with the authorization type can not be ordered.

## Define resources

You define the resources in the data section. A resource node begins with a root entry. You then specify the resources that can be requested.

Define root

With a node entry (root), you define the topmost entry of a resource.

## Example

```
<data>
<root Id="6CE9B526-9FFD-46A5-9ED0-36FB4E1303B5" Name="Computer" TypeId="1"
Merge="no">
<resource Name="Desktop PCs" TypeId="3" Description="['en-US:Stationary PC','de-
DE:Stationäre Arbeitsplatz-PCs']">
<resource Name="Desktop-PC simple" TypeId="3" />
<resource Name="Desktop-PC standard" TypeId="3" />
<resource Name="Desktop-PC customizable" TypeId="3" TemplateID="E3865726-6FDF-
489E-A7D5-4ABBA5B2BF83" />
</resource>
</root>
</data>
```

## Id

Assign an ID to the top node. The ID must be unique within Open Order. Our recommendation: Use a GUID, e.g. from [guidgen.com](http://guidgen.com)

## Name

Assign an display name for the node.

## TypeId

Specify the type of the top node.

## Merge

Set the update behavior if you re-upload the XML configuration.

*Merge="no"*

An existing configuration of the same root ID is removed and replaced by the new upload.

*Merge="yes"*

For an existing root ID:

- new entries (new name) will be added
- same entries (same name) will be added creating duplicates
- old entries will be kept

Define resource

Within the root, you define the resources in the **resource** section. You can nest the resources as much as you want.

## Example

```
<data>
<root Id="6CE9B526-9FFD-46A5-9ED0-36FB4E1303B5" Name="Computer" TypeId="1"
Merge="no">
<resource Name="Desktop PCs" TypeId="3" Description="['en-US:Stationary PC','de-
DE:Stationäre Arbeitsplatz-PCs']">
<resource Name="Desktop-PC simple" TypeId="3" />
<resource Name="Desktop-PC standard" TypeId="3" />
<resource Name="Desktop-PC customizable" TypeId="3" TemplateID="E3865726-6FDF-
489E-A7D5-4ABBA5B2BF83" />
</resource>
</root>
</data>
```

## Name

Displayed name of the resource.

## TypeId

Mandatory: Assign a type to the resource.

## Description

Optionally provide a [description](#) of the resource.

## Predefined icons








To display the technologies and resources in the data owner configuration, use predefined icons.

Use either the ID or the tag (tags are case-insensitive).

## Example

IconId="1" or IconId="Server" or IconID="SERVER"

TAG (CASE-INSENSITIVE)	ID	ICON	TOOLTIP GERMAN	TOOLTIP ENGLISH	NOTES
Unknown	0		Unbekannt	Unknown	(1)
Server	1		Server	Server	(2)
Domain	2		Domäne	Domain	
OrganizationalUnit	3		Organisationseinheit	Organizational Unit	
Container	4		Container	Container	
Computer	5		Computer	Computer	
Share	6		Freigabe	Share	
Directory	7		Verzeichnis	Directory	
File	8		Datei	File	
Contact	9		Kontakt	Contact	
Item	10		Element	Item	
Group	11		Gruppe	Group	

TAG (CASE-INSENSITIVE)	ID	ICON	TOOLTIP GERMAN	TOOLTIP ENGLISH	NOTES
User	12		Benutzer	User	
Memorystick	13		Memorystick	Memorystick	
BoxSoftware	14		Softwarebox	Software box	
Cd	15		CD	CD	
Laptop	16		Laptop	Laptop	
Smartphone	17		Smartphone	Smartphone	
Printer	18		Drucker	Printer	

(1) Default for resources if no or an invalid value (tag or ID) was specified.

(2) The default setting for resource nodes (root), if no or an invalid value (tag or ID) was specified.


## Descriptions

Descriptions can be given in several languages.

### Example

```
Description="['en-US:Buy', 'de-DE:Kaufen', 'fr-FR:Acheter']
```

You can add additional languages. Use the Windows Language Code Identifier (LCID).

 If you need to use an apostrophe (escape character) within the description text, this must be quoted:

```
Description="['en-US:PC&quot;']
```

## Validate an XML configuration file

At the latest when uploading to ARM, your XML configuration is validated. You can already check the structure of your XML data in the editor for validity.

The screenshot shows the ARM Configuration application interface. The top bar displays the ARM logo and the title 'Access Rights Manager Configuration'. Below the title bar, there are three summary cards: 'Server Status', 'Jobs Summary', and 'Collectors Configuration'. The 'Server Status' card shows 'Logged in users: 2' and 'Licensed Active user accounts: 1166'. The 'Jobs Summary' card shows '91 Scans', '7 Reports', '69 Changes', and '132 More'. The 'Collectors Configuration' card shows '1 Connected' and '1 Configured in Total'. Below these cards is a 'Filter' dropdown menu. The main area contains a grid of icons for various functions: 'Scans', 'Open Order' (highlighted with a red box), 'User Management', 'Data Owner', 'License', 'Jobs Overview', 'Alerts', 'Change Configuration', 'Scripting', 'Views & Reports', 'Server', and 'Basic Configuration'. Each icon has a corresponding title and a brief description of its function. The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

In the ARM configuration application, click "Open Order".

The screenshot displays the 'Open Order Configuration' page within the Access Rights Manager (ARM) Configuration window. The page is divided into two main sections: 'Open Order Resource Descriptions' and 'Quick info'.

**Open Order Resource Descriptions:**

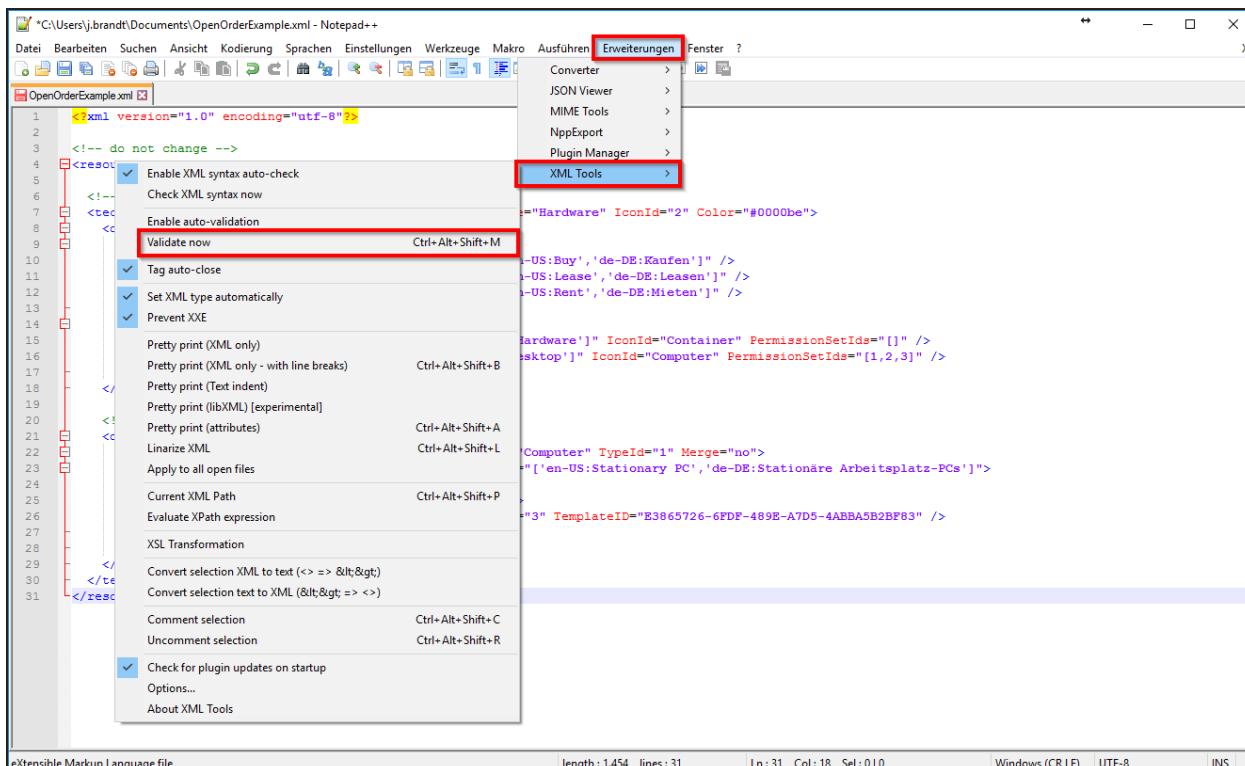
- Import File:** A section with the instruction 'Select a valid XML file which contains open order resource descriptions for import.' and an 'Upload' button.
- XML schema:** A section with the instruction 'The XML schema will be used to verify that the import file is valid. It also serves as documentation for creating an import file. You can download the schema [here](#).' The word 'here' is highlighted with a red box.
- Resource Categories:** A list of categories including 'Hardware' and 'Software', each with a corresponding icon.

**Quick info:**

- Open Order Configuration:** A section explaining that users can manage external resource descriptions of several Open Order technologies. It states: 'Here you can manage external resource descriptions of several Open Order technologies. Use the Open Order technologies in the Data Owner configuration in order to assign your requestable resources.'
- Functions:** A list of actions:
  - Import Open Order resource descriptions from XML file
  - Remove loaded Open Order resource descriptions

The bottom of the window shows the system tray with 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Click the link to download the XML schema file (.xsd).



Example: In Notepad++ with XML Tools enabled, you can perform a schema validation.

Click Plugins > XML Tools > Validate Now.

## Integrate Open Order templates in GrantMA

To integrate Open Order Templates, follow these steps:

1. [Enter the template's call into the XML resource configuration](#)
2. [Upload an XML Open Order resource configuration to ARM](#)
3. [Set the Open Order resource to requestable](#)

Enter the template's call into the XML resource configuration

Assign the [unique ID](#) of the OpenOrderTemplate to one or more resources.

### Example

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<resourceImport Version="3">
```

```
<technology Id="D54C16F2-42C1-477A-BD20-3285158F68D3" Name="Hardware" IconId="2"
Color="#0000be">
```

```
<definitions>
<permissionSets>
<permissionSet PermissionSetId="1" Description="['en-US:Buy','de-DE:Kaufen']" />
<permissionSet PermissionSetId="2" Description="['en-US:Lease','de-DE:Leasen']"
/>
<permissionSet PermissionSetId="3" Description="['en-US:Rent','de-DE:Mieten']"
/>
</permissionSets>
<types>
<type Id="1" Description="['en-US:Hardware','de-DE:Hardware']"
IconId="Container" PermissionSetIds="[]" />
<type Id="3" Description="['en-US:Desktop','de-DE:Desktop']" IconId="Computer"
PermissionSetIds="[1,2,3]" />
</types>
</definitions>
<data>
<root Id="6CE9B526-9FFD-46A5-9ED0-36FB4E1303B5" Name="Computer" TypeId="1"
Merge="no">
<resource Name="Desktop PCs" TypeId="3" Description="['en-US:Stationary PC','de-
DE:Stationäre PCs']">
<resource Name="Desktop-PC Simple" TypeId="3" />
<resource Name="Desktop-PC Standard" TypeId="3" />
<resource Name="Desktop-PC Custom" TypeId="3" TemplateID="E3865726-6FDF-489E-
A7D5-4ABBA5B2BF83" />
</resource>
</root>
</data>
</technology>
</resourceImport>
```



## Upload an XML resource configuraton to the Data Owner configuration

The screenshot displays the ARM Configuration application interface. At the top, there are three summary cards:

- Server Status** (License Information): Logged in users: 2, Licensed Active user accounts: 1166.
- Jobs** (Summary): 91 Scans, 7 Reports, 69 Changes, 132 More, 7 Scheduled, 292 Succeeded, 0 Executing, 0 Failed.
- Collectors** (Configuration): 1 Connected, 1 Configured in Total, All Collectors are Operational.

Below the summary cards is a 'Filter' dropdown menu. The main area contains a grid of menu items:

- Scans**: Resource Configurations, Logga, File Server CSV Import.
- Open Order**: Open Order Resource Descriptions (highlighted with a red box).
- User Management**: User Management, Role Management.
- Data Owner**: Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings.
- License**: License Information, Server Status.
- Jobs Overview**: Job Status, Job Categories.
- Alerts**: Activate/Deactivate Alert Sensors.
- Change Configuration**: Common Change Settings, Technology-specific Change Configurations.
- Scripting**: Scripting configuration for change actions.
- Views & Reports**: Views & Reports, Blacklist for Views & Reports.
- Server**: Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging.
- Basic Configuration**: ARM Server, SQL Server, Configuration Status.

The bottom status bar shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

In the ARM configuration application, click "Open Order".

The screenshot shows the 'Open Order Configuration' page in the Access Rights Manager Configuration window. The page is divided into two main sections: 'Open Order Resource Descriptions' and 'Quick info'.

**Open Order Resource Descriptions:**

- Import File:** A section with the text 'Select a valid XML file which contains open order resource descriptions for import.' Below this text is a red-bordered 'Upload' button.
- XML schema:** A section with the text 'The XML schema will be used to verify that the import file is valid. It also serves as documentation for creating an import file. You can download the schema [here](#).' Below this text is a downward-pointing arrow.
- Hardware:** A section with a folder icon and the text 'Hardware'.
- Software:** A section with a folder icon and the text 'Software'.

**Quick info:**

- Open Order Configuration:** A section with the text 'Here you can manage external resource descriptions of several Open Order technologies. Use the Open Order technologies in the Data Owner configuration in order to assign your requestable resources.'
- Functions:** A list of functions:
  - Import Open Order resource descriptions from XML file
  - Remove loaded Open Order resource descriptions

The status bar at the bottom of the window shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Click "Upload" to import the XML Resource Configuration.

After successful import, the resources are available in the Data Owner configuration and can be assigned to organizational categories (see next chapter).

**i** A copy of the XML configuration is stored in `%programdata%\protected-networks.com\8MAN\openOrder`. You can use these to change your configuration. Note the [merge settings](#) for repeated imports.

## Set the Open Order resource to requestable

ARM Access Rights Manager Configuration

Server Status License Information	Jobs Summary	Collectors Configuration
Logged in users: 2	91 Scans 7 Reports	1 Connected 1 Configured in Total
Licensed Active user accounts: 1166	7 Scheduled 292 Succeeded	All Collectors are Operational

Filter

- Scans**  
Resource Configurations, Logga, File Server CSV Import
- Open Order**  
Open Order Resource Descriptions
- User Management**  
User Management, Role Management
- Data Owner**  
Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**  
License Information, Server Status
- Jobs Overview**  
Job Status, Job Categories
- Alerts**  
Activate/Deactivate Alert Sensors
- Change Configuration**  
Common Change Settings, Technology-specific Change Configurations
- Scripting**  
Scripting configuration for change actions
- Views & Reports**  
Views & Reports, Blacklist for Views & Reports
- Server**  
Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**  
ARM Server, SQL Server, Configuration Status

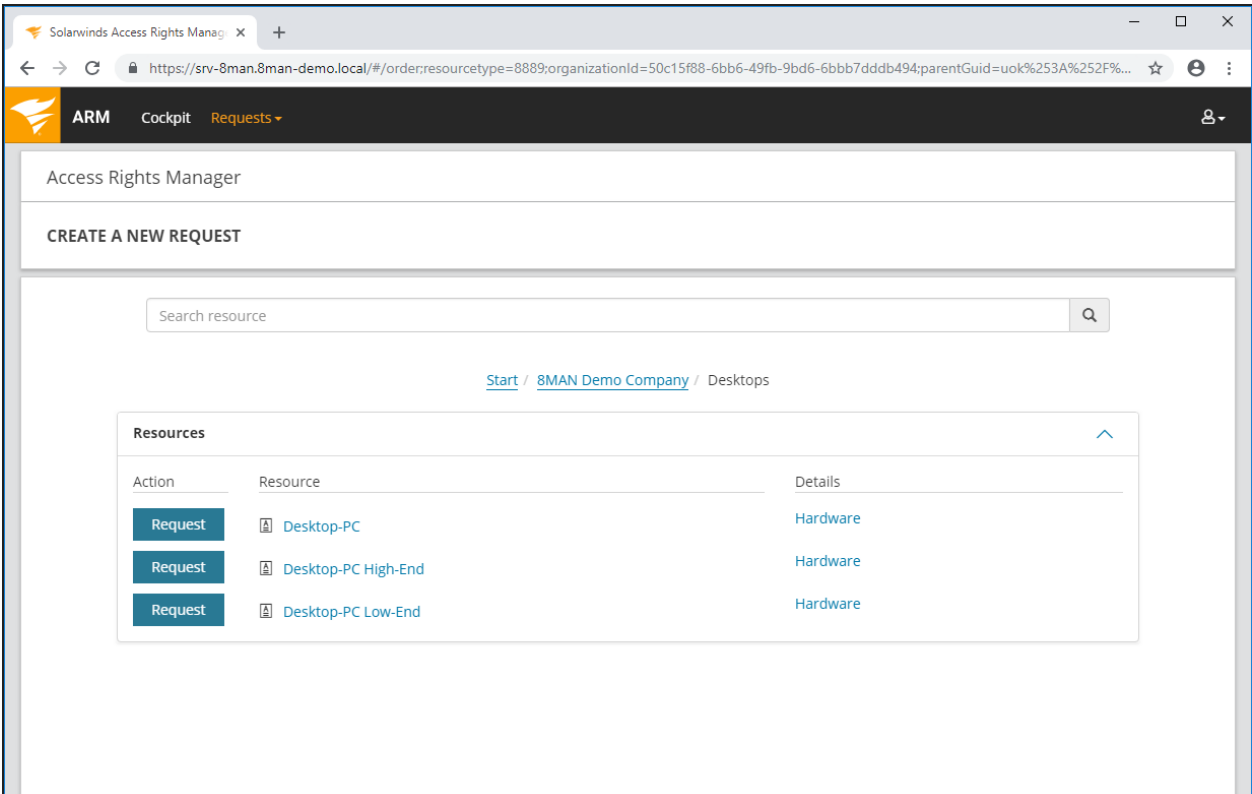
Ready Anthonyv Admin @ localhost

In the ARM configuration application, click "Data Owner".

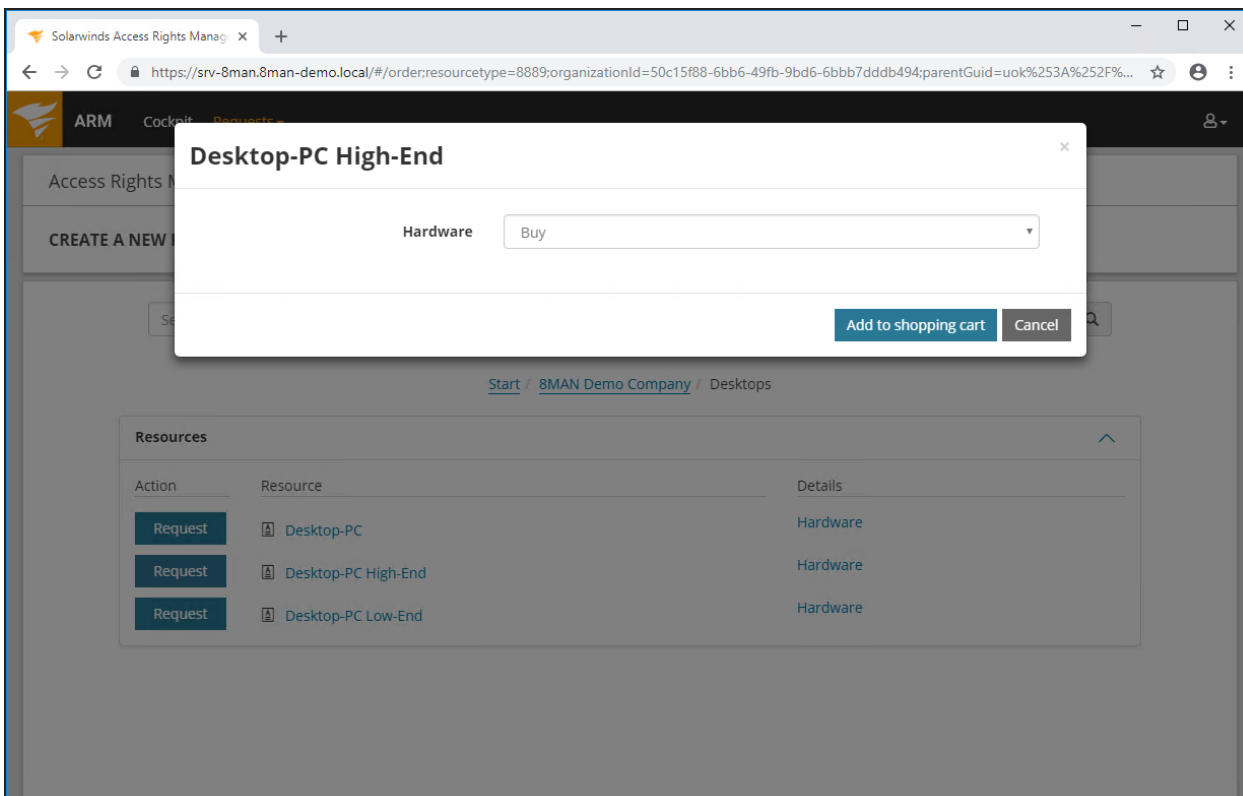
The screenshot shows the 'Data Owner configuration' for 'Human Resources'. On the left, there's a sidebar with 'Organizational Categories' including Finance, Human Resources, Marketing, and Sales. The main area is divided into several sections:

- Data Owners:** A table with columns 'Name', 'Inherited from', and 'User role'. It lists 'David DO HR (8man-demo)' and 'David DO Manag... 8MAN Demo Company'.
- Requesters:** A table with columns 'Name', 'Inherited from', and 'User role'. It lists 'Emily Employ...' and 'Henry HR (8man-demo)'.
- Resources:** A table with columns 'Name', 'Alias', 'Inherited from', and 'Access'. It lists various resources like 'Active Directory (2)', 'File server (1)', 'Template (2)', and 'Hardware (1)'. A red arrow points to the 'Desktop PCs' resource under 'Hardware (1)', which is highlighted with a red box and a '2' in a red circle.
- User & Group selection:** A search bar and a list of users and groups, including 'Caroline Berggren', 'Domain Users', 'Emily Employee', 'Ludvig Karlsson', and 'Marketing'.
- Resource selection:** A search bar and a tree view of resources. 'Desktop PCs' is highlighted with a red box and a '1' in a red circle.

1. Add the desired resource by drag & drop.
2. The resource is automatically marked as requestable.




The requester can find the resource available via Open Order.

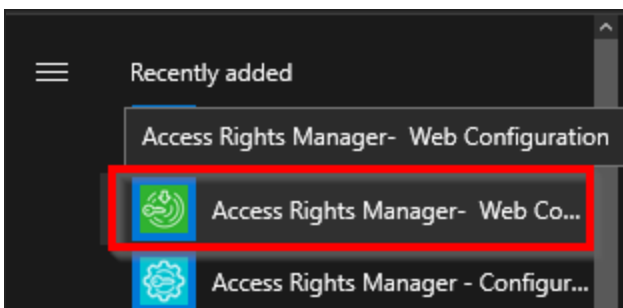


Example for an template based Open Order request.

## Configure web components

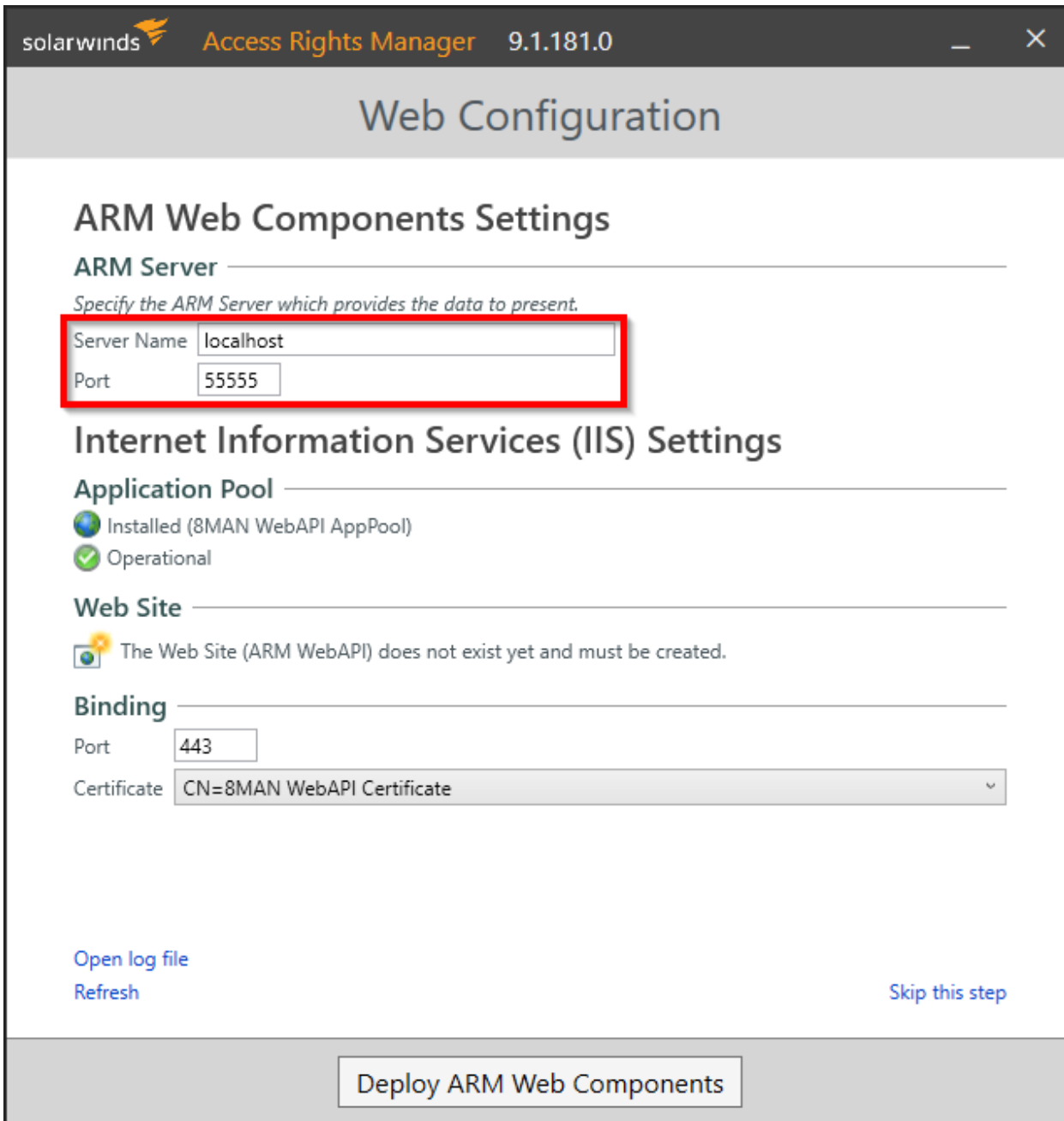
 ARM web components are pre-configured during an evaluation installation with default values.


For a production installation you may install ARM web components on a different server (not recommended). With the ARM web configurator you set the web server name, port and certificate bindings.



Open the ARM web configuration application.

**i** After a Production Installation with enabled web components the web configuration application starts automatically.



solarwinds  Access Rights Manager 9.1.181.0

## Web Configuration

### ARM Web Components Settings

#### ARM Server


Specify the ARM Server which provides the data to present.


Server Name

Port


### Internet Information Services (IIS) Settings

#### Application Pool

 Installed (8MAN WebAPI AppPool)

 Operational

#### Web Site

 The Web Site (ARM WebAPI) does not exist yet and must be created.

#### Binding

Port

Certificate

[Open log file](#)

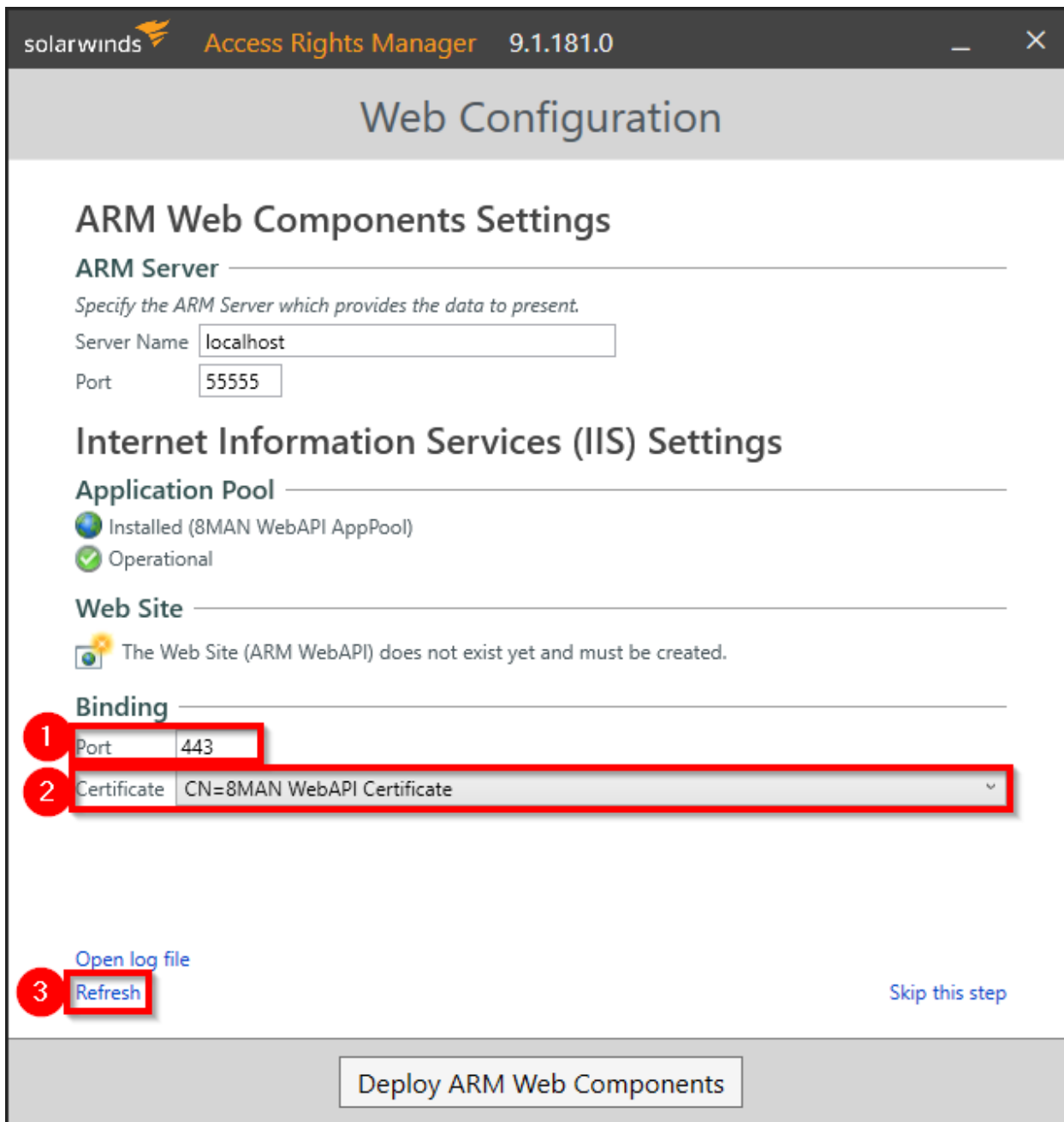
[Refresh](#)


[Skip this step](#)

**Deploy ARM Web Components**

Enter the name of the ARM server. If you are running both Web Components and the ARM server on the same computer, you can use localhost.

Enter the port of the ARM server. By default the ARM server communicates through port "55555".



solarwinds  Access Rights Manager 9.1.181.0

## Web Configuration

### ARM Web Components Settings

**ARM Server**


Specify the ARM Server which provides the data to present.


Server Name

Port


### Internet Information Services (IIS) Settings

**Application Pool**

 Installed (8MAN WebAPI AppPool)

 Operational

**Web Site**

 The Web Site (ARM WebAPI) does not exist yet and must be created.

**Binding**

1 Port

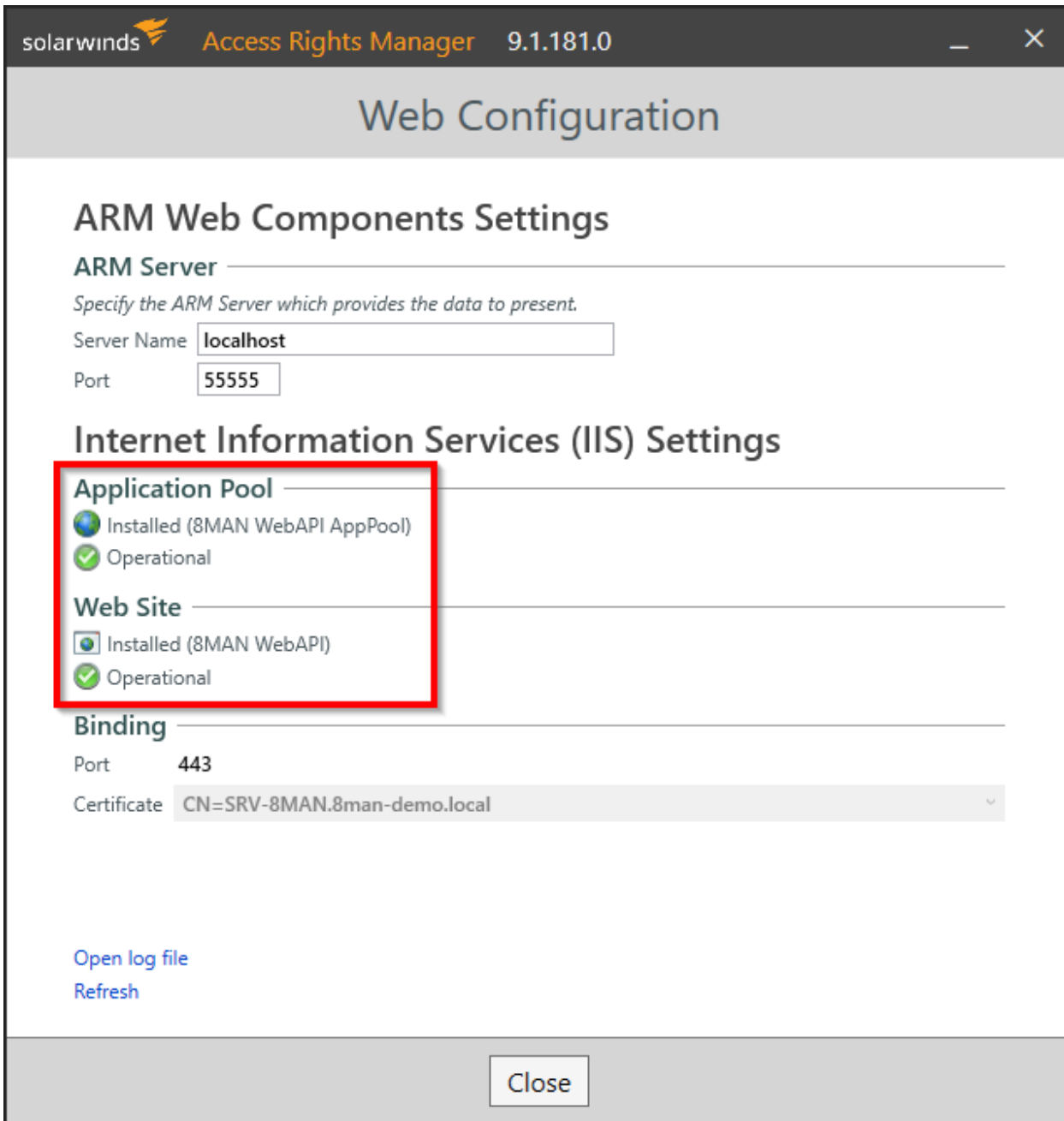
2 Certificate


[Open log file](#)

3  [Skip this step](#)

1. Enter a port for the binding of the certificate to the website. The standard https port is 443. If you enter any other port you must consider this when starting the ARM website (providing the URL to users).
2. Select a certificate. If no certificate is offered, please reference the following chapters: "Generate a self-signed certificate".
3. You can reload the list of available certificates by clicking on "Refresh".





solarwinds  Access Rights Manager 9.1.181.0

## Web Configuration

### ARM Web Components Settings

**ARM Server**



*Specify the ARM Server which provides the data to present.*

Server Name



Port

### Internet Information Services (IIS) Settings

**Application Pool**

-  Installed (8MAN WebAPI AppPool)
-  Operational

**Web Site**

-  Installed (8MAN WebAPI)
-  Operational

**Binding**

Port


Certificate

[Open log file](#)

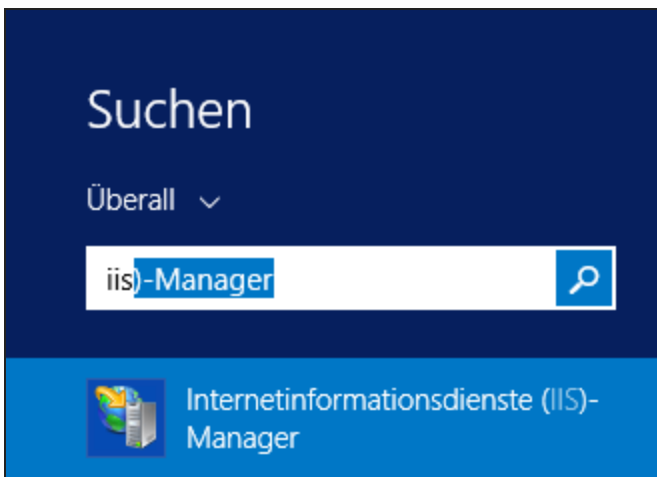
[Refresh](#)

The web components will be available once all settings for "Application Pool" and "Web Site" are shown as operational.

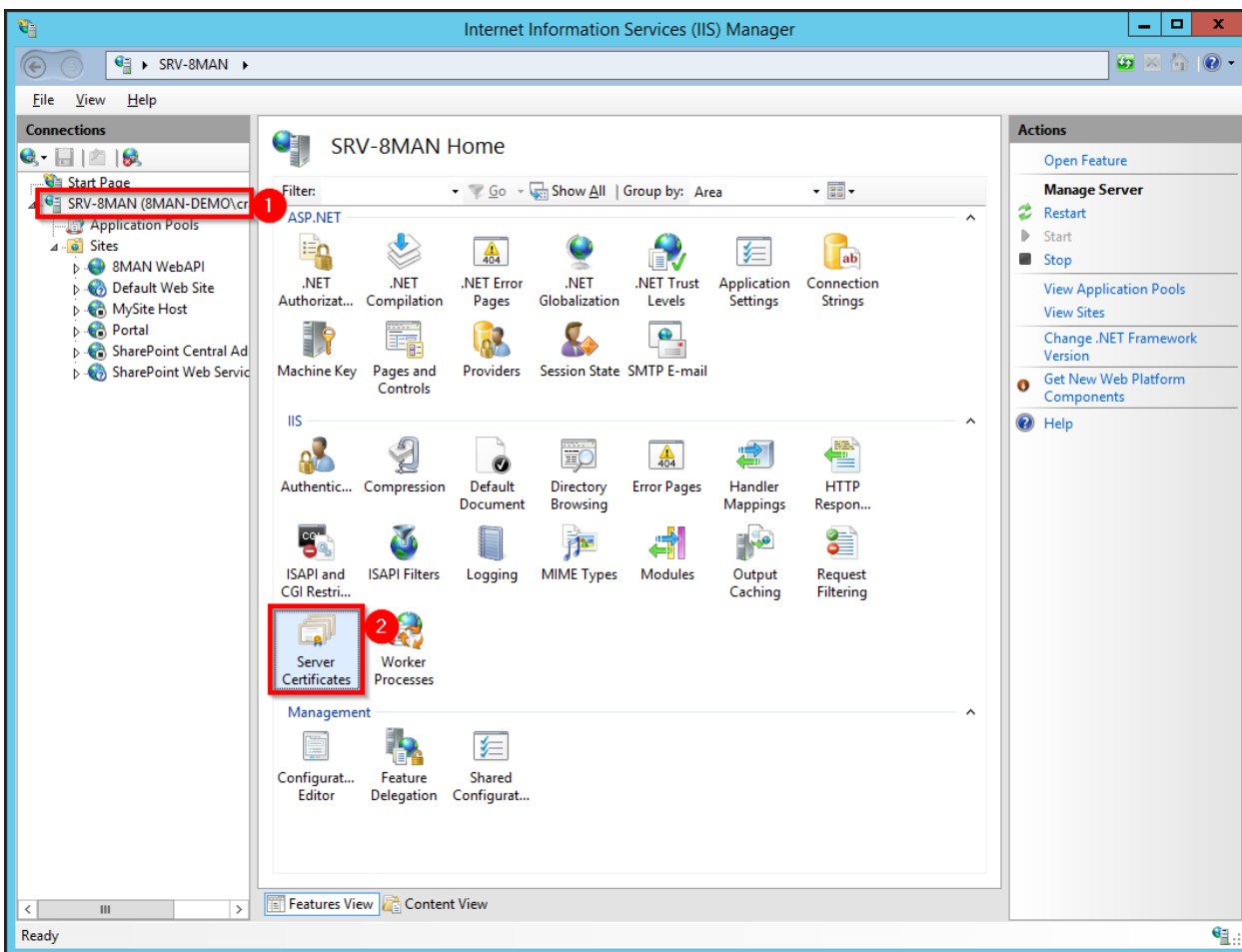
## Generate a self-signed certificate

 The following steps are optional.

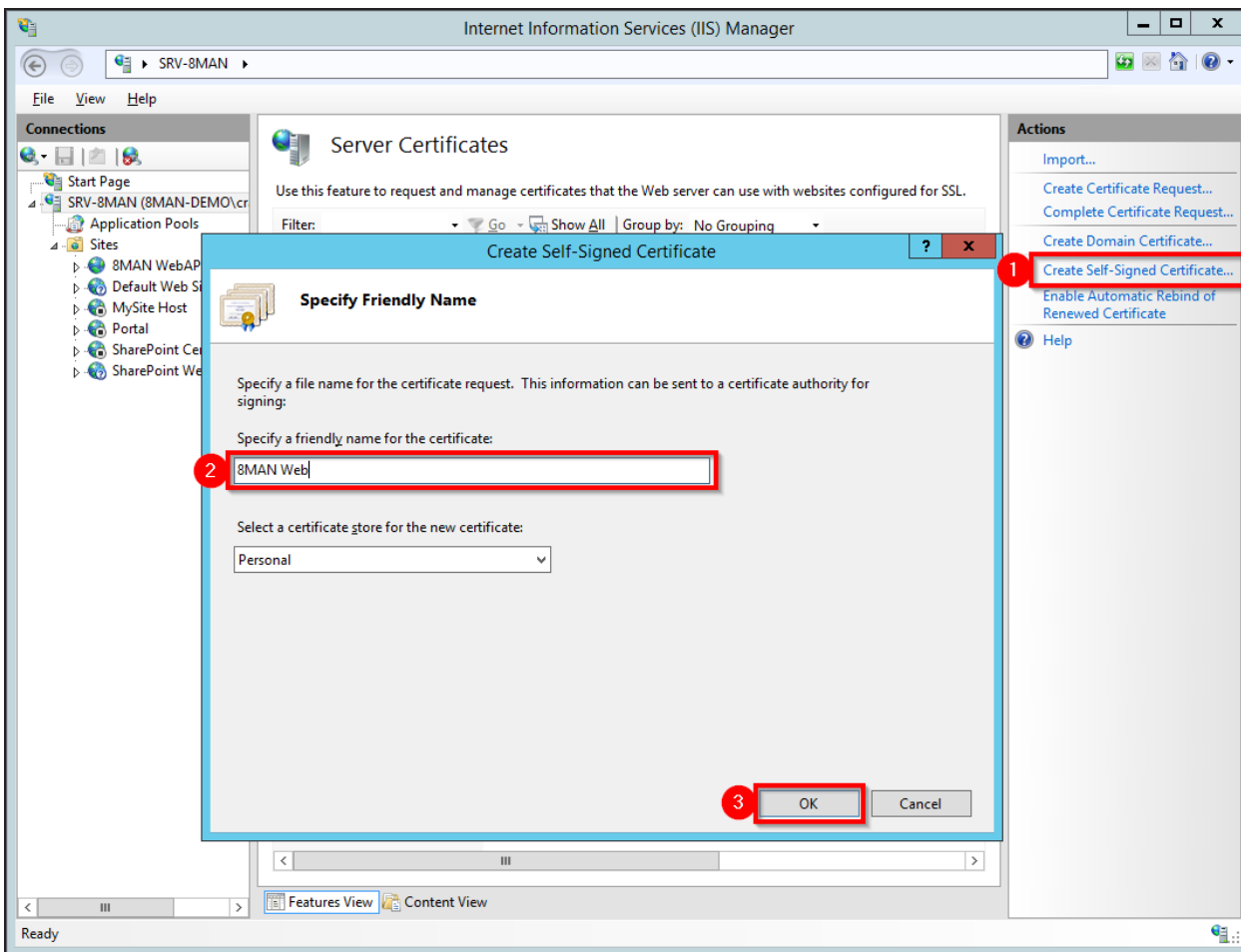
The self-signed certificates described in the following steps create security warnings in various browsers, as an out-of-date SHA-1 based encryption is used. Use certificates with SHA2 / 256 encryption for productive use.



Start the IIS-Manager.



1. Select the server.
2. Double-click "Server Certificates".

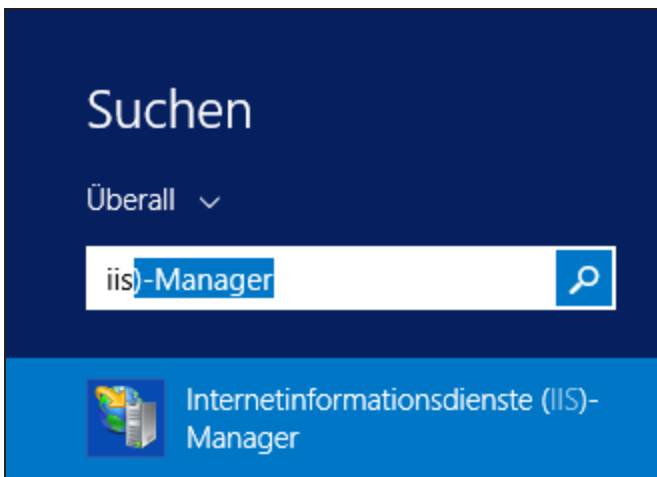


1. Click "Create Self-Signed Certificate".
2. Give the certificate a name.
3. Generate the certificate.

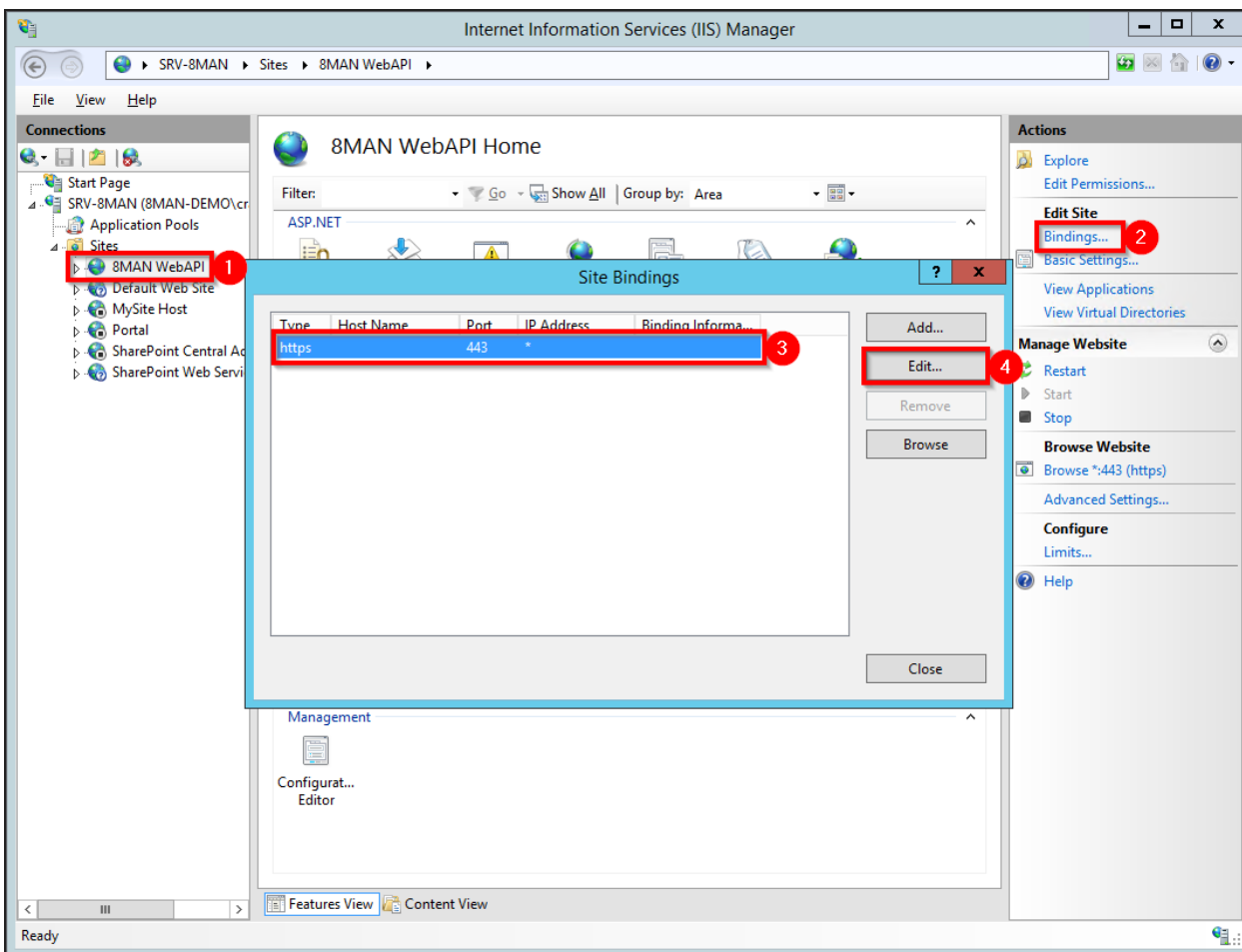
The next step is to bind the certificate to the website.

## Bind a certificate to a site

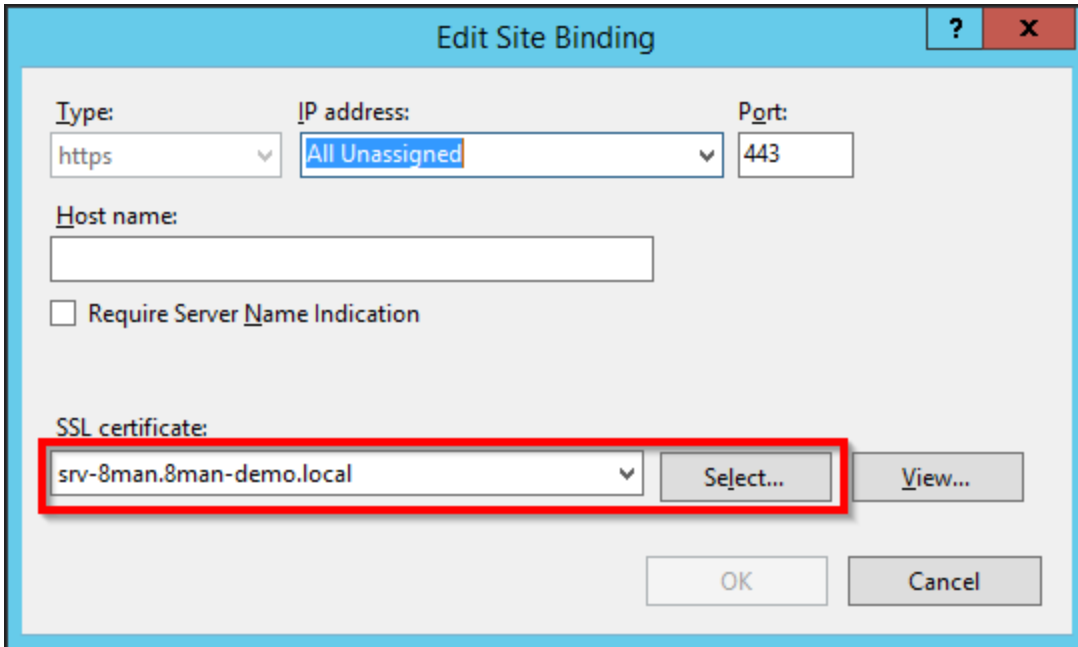
You can add a certificate to the site during the provisioning process. It may be necessary to add another certificate, for example when the old one has expired.



Start the IIS-Manager.



1. Navigate to the site "ARM WebAPI".
2. Click "Bindings...".
3. Select the certificate with type "https" and port "443" (standard settings).
4. Click "Edit...".



**Edit Site Binding** ? X

Type: https IP address: All Unassigned Port: 443

Host name:

Require Server Name Indication

SSL certificate:

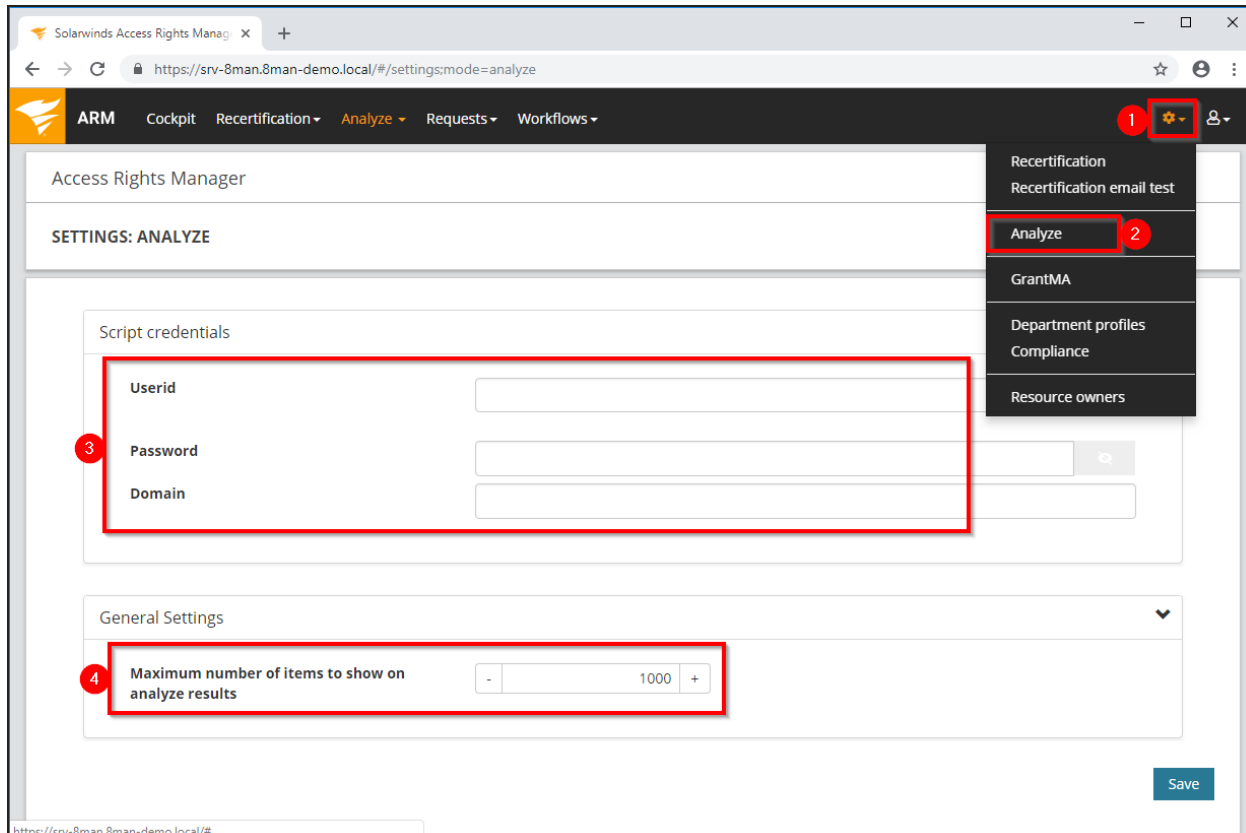
srv-8man.8man-demo.local Select... View...

OK Cancel

Select a certificate. Click "OK" to bind the certificate to the site.

# Configuration in the web client

## Set analyze options



Log into the WebClient as ARM administrator.

1. Click the gear. If you do not see a gear you are not logged in as an ARM administrator.
2. Select Analyze.
3. Specify credentials for the execution of scripts. Specify an account that has the permissions to perform the actions of the scripts.
4. Define the maximum number of lines to be displayed in the scenarios. A high number of lines can lead to performance problems (see [Browser recommendations](#)).

# Configure recertifications

## Activate and deactivate recertifications

The screenshot shows the Solarwinds Access Rights Manager (ARM) interface. The top navigation bar includes 'ARM', 'Cockpit', 'Recertification', 'Analyze', 'Requests', and 'Workflows'. The main content area is titled 'SETTINGS: RECERTIFICATION'. Under the 'Configuration' section, the 'Recertification date range' is configured. The 'Start date' is set to 'December 14, 2018'. A calendar for 'February 2019' is displayed, with the 18th selected. Below the calendar, there is an 'End date' checkbox. The 'Duration' is set to 730 Days, and the 'Frequency' is set to 24 Month. A 'Save' button is located at the bottom right. A red box highlights the 'Recertification' menu item in the top navigation bar, and another red box highlights the 'Recertification date range' configuration area, including the calendar and the 'End date' checkbox.

1. Login with ARM administrator credentials and select "Recertification".
2. Select a start date. Recertification is active from this date on.

**i** The recertification is based on scan data of this date. Permission changes that occur after this date will not be considered by an active recertification.

3. Select an end date. Recertification is deactivated from this date on. There is no other option to deactivate the recertification. All Data Owners with open recertification requests will be informed by email.

These settings are valid globally for all Data Owners.

Which resources need to be certified is specified in the [DataOwner configuration](#).

## Deadlines and intervals

The screenshot displays the 'Settings: Recertification' page in the Solarwinds Access Rights Manager. The 'Configuration' section includes a 'Recertification date range' field with a start date of 'December 14, 2018'. Below this is a calendar for February 2019, with the 18th selected. The 'Duration' field is set to 14 Days, and the 'Frequency' field is set to 6 Month. A 'Save' button is visible at the bottom right.

Notification emails will be sent to all data owners on the start date (during the nightly ARM server maintenance).

1. Determine how long the data owners have time to complete recertification.
2. Determine the frequency of the recertification process.

These settings are valid globally for all Data Owners.



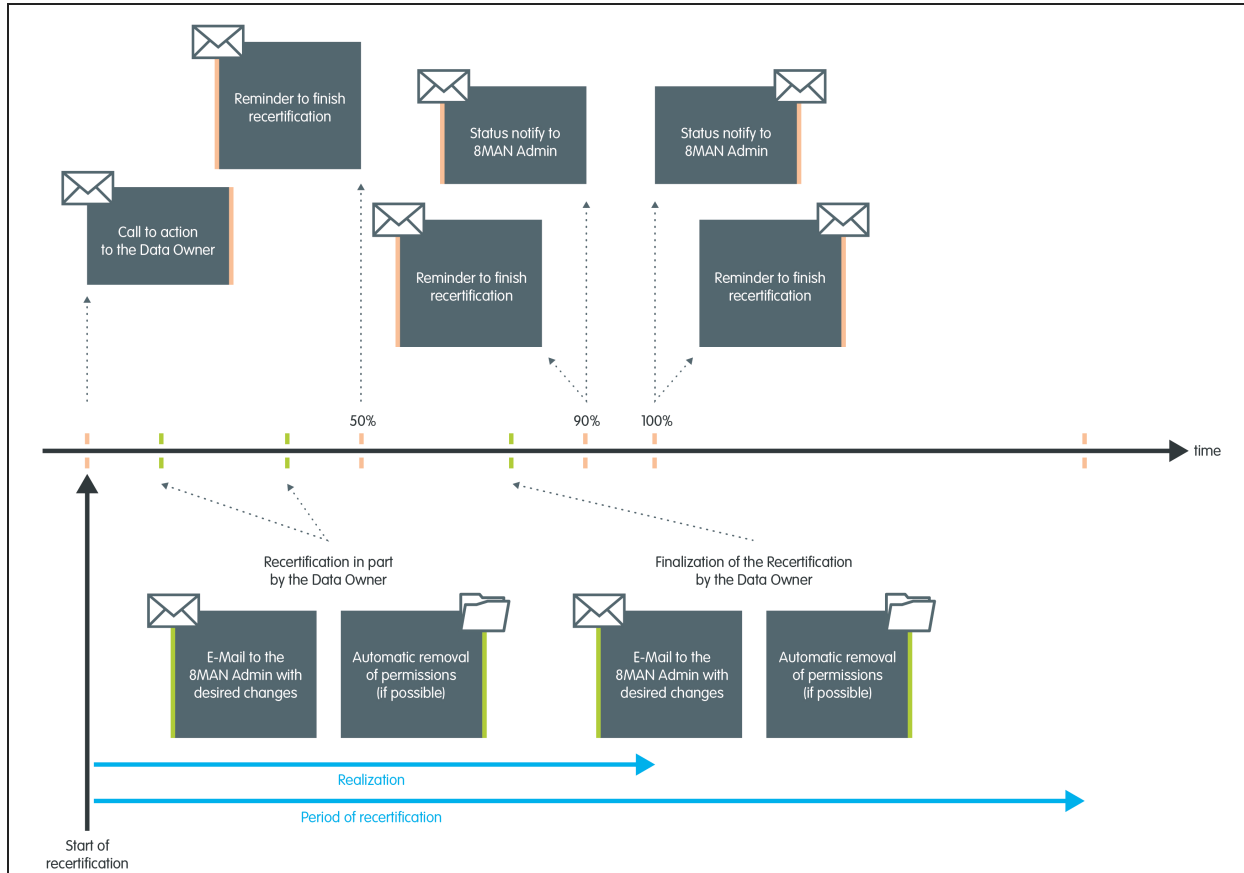
## Activate recertifications in the Data Owner configuration

The screenshot shows the ARM Configuration window for 'Germany'. The 'Resources' section is expanded, showing a list of resources. A red box labeled '1' highlights the flyout menu bar for the 'File server' resource, and a red box labeled '2' highlights the 'File server' resource itself. The 'Resources' table has columns for Name, Alias, Inherited from, and Access. The 'File server' resource is selected, and its flyout menu is open, showing options for 'Recertify' and 'Edit'. The 'User & Group selection' panel on the right shows a list of users and groups, and the 'Resource selection' panel on the bottom right shows a list of resource categories and sub-categories.

1. To make resources appear in the Data Owner recertification process, you must mark them as editable and activate the recertification.
2. Select a resource and use the flyout menu bar to activate the recertification.

## Customize notification emails

### Manage the frequency of email notifications



During the recertification process, email notifications are sent frequently to data owners and ARM administrators.

The timeline diagram visualizes when emails are sent and whom they are sent to. Every email above the timeline (with an orange marking) can be deactivated.

### Adjust content and style of the notification email

ARM offers standard templates in XML stylesheet format. You can find them in the following directory:

```
OLD: %ProgramFiles%\Protected Networks\8MAN\etc\mails\Recertification
NEW: %ProgramFiles%\SolarWinds\ARM\etc\mails\Recertification
```

In case you want to modify these templates, please copy the files (\*.xslt und css.html) to:

```
%ProgramData%\protected-networks.com\8MAN\cfg\mails\Recertification
```

The sub-directory "mails\recertification" must be created in advance.

Adjust the templates in "ProgramData". ARM primarily uses the customized templates in "ProgramData".

When updating to a newer ARM version the data in "ProgramFiles" will be overwritten.

## Test notification emails for recertification

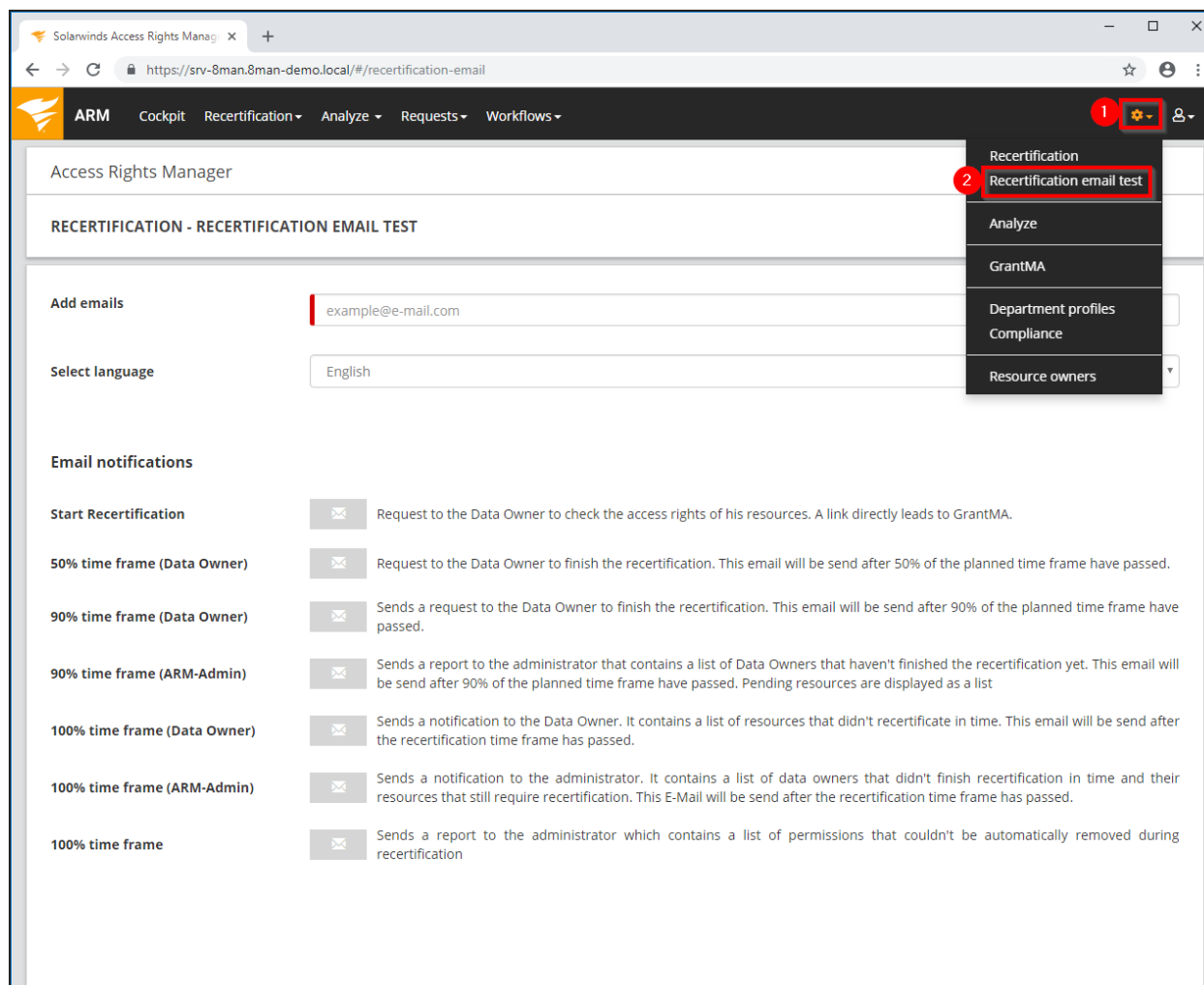
### Background / Value

In the stages of recertification, ARM sends various notification emails. Test the notification emails - including your adjustments if necessary, before you enable recertification.

### Related features

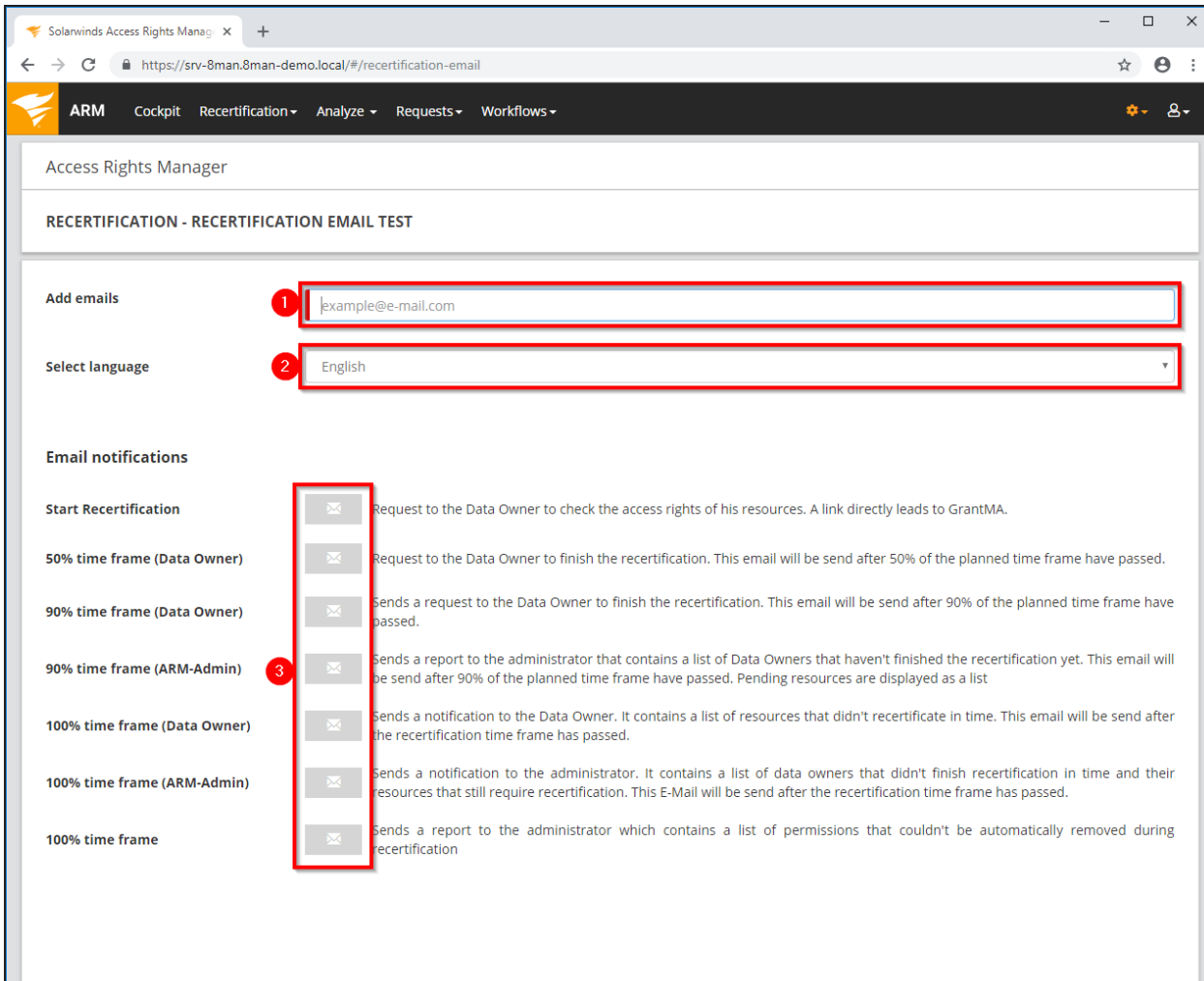
[Customize notification emails for recertification](#) (Administrator)

### Step-by-step process



Log into the web client as an administrator.

1. Click on the gear.
2. Select "Recertification email test".



Solarwinds Access Rights Manager

ARM Cockpit Recertification Analyze Requests Workflows

### RECERTIFICATION - RECERTIFICATION EMAIL TEST

**Add emails** 1

**Select language** 2

**Email notifications**

<b>Start Recertification</b>	<input type="checkbox"/>	Request to the Data Owner to check the access rights of his resources. A link directly leads to GrantMA.
<b>50% time frame (Data Owner)</b>	<input type="checkbox"/>	Request to the Data Owner to finish the recertification. This email will be send after 50% of the planned time frame have passed.
<b>90% time frame (Data Owner)</b>	<input type="checkbox"/>	Sends a request to the Data Owner to finish the recertification. This email will be send after 90% of the planned time frame have passed.
<b>90% time frame (ARM-Admin)</b>	<input checked="" type="checkbox"/> <span>3</span>	Sends a report to the administrator that contains a list of Data Owners that haven't finished the recertification yet. This email will be send after 90% of the planned time frame have passed. Pending resources are displayed as a list
<b>100% time frame (Data Owner)</b>	<input type="checkbox"/>	Sends a notification to the Data Owner. It contains a list of resources that didn't recertificate in time. This email will be send after the recertification time frame has passed.
<b>100% time frame (ARM-Admin)</b>	<input type="checkbox"/>	Sends a notification to the administrator. It contains a list of data owners that didn't finish recertification in time and their resources that still require recertification. This E-Mail will be send after the recertification time frame has passed.
<b>100% time frame</b>	<input type="checkbox"/>	Sends a report to the administrator which contains a list of permissions that couldn't be automatically removed during recertification

1. Enter one or more recipients.
2. Choose the language.
3. Send the desired notification email.

## Recertification

Dear Anthony Admin,

this is a reminder. Half of the period specified has expired and you did not yet finish the recertification. It has to be finished by 3/20/2019.

Please check the permissions on the following resources:

Resource	State
ProjectX (Project X)	Open
ProjectY (Project Y)	Open

Follow the [link](#) to login to the ARM recertification website.

Example of a notification at the beginning of the recertification.

## Configure display settings

Eliminate the display of technical accounts

The recertification process has been designed to check the permissions of real users. Technical accounts (see the following list) are not displayed:

- Creator Owner (S-1-3-0)
- Creator-Group (S-1-3-1)
- Creator-Owner-Server (S-1-3-2)
- Creator group-Server (S-1-3-3)
- All Services (S-1-5-80-0)
- RDT (S-1-5-1)
- Network (S-1-5-2)
- Batch processing (S-1-5-3)
- Interactive (S-1-5-4)
- Domain controller (S-1-5-9)
- Local System (S-1-5-18)
- Local Service (S-1-5-19)
- Network service (S-1-5-20)

Manage display settings for resolving group memberships

Recertifications adopt the settings of the blacklist for views and reports. Please see the section "[Configure the blacklist for views & reports](#)".

## GrantMA settings

The screenshot shows the Solarwinds Access Rights Manager (ARM) settings page for GrantMA. The page is titled "Access Rights Manager" and "SETTINGS: GRANTMA". The "General Settings" section is visible, with the following fields and options:

- The administrator email address for GrantMA is:** anton.admin@8man-demo.local (highlighted with a red box and labeled '3')
- Maximum number of items to show on order overviews:** 1000
- Open requests will expire after:** 14 days
- Send emails to the requester on status updates. (On order, reject, executed or failed)
- Send additional emails to the requester on each approval step.
- Send email on each new approvable request to the Approver
- Allow requesters to browse hierarchical resources (e.g. file system folders).
- Allow approvers to modify order details.
- Legacy mode for resolving workflows and data owner approvers

A dropdown menu is open, showing options like "Recertification", "Analyze", "GrantMA", "Department profiles", "Compliance", and "Resource owners". The "GrantMA" option is highlighted with a red box and labeled '2'. A gear icon in the top right corner is labeled '1'.

Normally, when ordering a resource from an organization category, the workflow of this category is triggered. If this workflow contains the approver role "data owner of the organization category", the data owners of this category have to approve. In the legacy mode, however, the workflow of the first organization category that contains a resource which is (upwards) hierarchically closest to the ordered resource is triggered. If this workflow contains the approver role "data owner of the organization category", the data owners of all organization categories that contain a resource that is closest to the ordered resource have to approve.

Log into the web client as an ARM administrator.

1. Click the gear.
2. Select GrantMA.
3. Specify the administrator's email address for GrantMA. ARM sends emails if errors occur in the order process (not for Recertification and Analyze & Act).

Solarwinds Access Rights Manager

SETTINGS: GRANTMA

General Settings

The administrator email address for GrantMA is

Maximum number of items to show on order overviews **1**

Open requests will expire after **2**  days

**3**  Send emails to the requester on status updates. (On order, reject, executed or failed)

**4**  Send additional emails to the requester on each approval step.

Send email on each new approvable request to the Approver

Allow requesters to browse hierarchical resources (e.g. file system folders).

Allow approvers to modify order details.

Legacy mode for resolving workflows and data owner approvers

Normally, when ordering a resource from an organization category, the workflow of this category is triggered. If this workflow contains the approver role "data owner of the organization category", the data owners of this category have to approve. In the legacy mode, however, the workflow of the first organization category that contains a resource which is (upwards) hierarchically closest to the ordered resource is triggered. If this workflow contains the approver role "data owner of the organization category", the data owners of all organization categories that contain a resource that is closest to the ordered resource have to approve.

1. Define the maximum number of lines to be displayed in the scenarios. A high number of lines can lead to performance problems (see [Browser recommendations](#)).
2. Specify the number of days of unfinished jobs by Data Owners being marked as expired. Administrators see these requests as expired in the order summary. No emails will be sent.
3. Option enabled: The requester receives an email when the status of his order changes.
4. Option enabled: The applicant receives additional emails at each approval step.

Solarwinds Access Rights Manager

ARM Cockpit Recertification Analyze Requests Workflows Anthony Admin

Access Rights Manager

SETTINGS: GRANTMA

General Settings

The administrator email address for GrantMA is

Maximum number of items to show on order overviews

Open requests will expire after  days.

Send emails to the requester on status updates. (On order, reject, executed or failed)

Send additional emails to the requester on each approval step.

1  Send email on each new approvable request to the Approver

2  Allow requesters to browse hierarchical resources (e.g. file system folders).

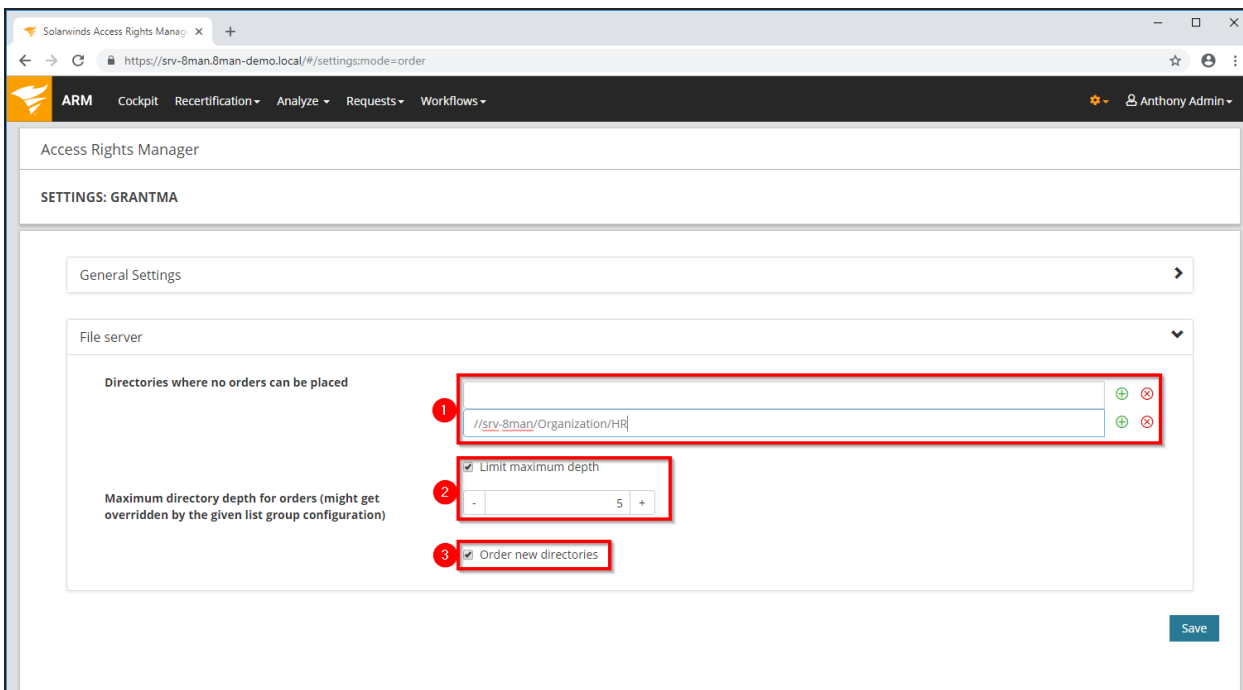
3  Allow approvers to modify order details.

4  Legacy mode for resolving workflows and data owner approvers

Normally, when ordering a resource from an organization category, the workflow of this category is triggered. If this workflow contains the approver role "data owner of the organization category", the data owners of this category have to approve. In the legacy mode, however, the workflow of the first organization category that contains a resource which is (upwards) hierarchically closest to the ordered resource is triggered. If this workflow contains the approver role "data owner of the organization category", the data owners of all organization categories that contain a resource that is closest to the ordered resource have to approve.

1. Option enabled: The approver will receive an email for a new request. We recommend that you enable this option.
2. Option enabled: Requesters can navigate into hierarchical resources, e.g. subdirectories.
3. Option enabled: Approvers can modify a request.
4. If necessary, enable the legacy mode.





1. Define a blacklist for which directories are hidden for orders. Use UNC paths.
2. Define a directory depth up to which users can order.
3. Enable ordering new directories.

## Resource owners

### Activate the Resource Owner feature

The Resource Owner feature is deactivated by default. To activate the feature the pnserv.config.xml file has to be edited.

### Configuration file

pnServer.config.xml

### Computer

ARM-Server

### Path

%ProgramData%\protected-networks.com\8MAN\cfg

## Code

in the section <config>

```
<resourceOwner.enabled type="System.Boolean">true</resourceOwner.enabled>
```

## Possible values


**true** - Resource Owner feature is enabled

**false** - Resource Owner feature is disabled (default)

## Assign resource owners using the web client

### Background / Value

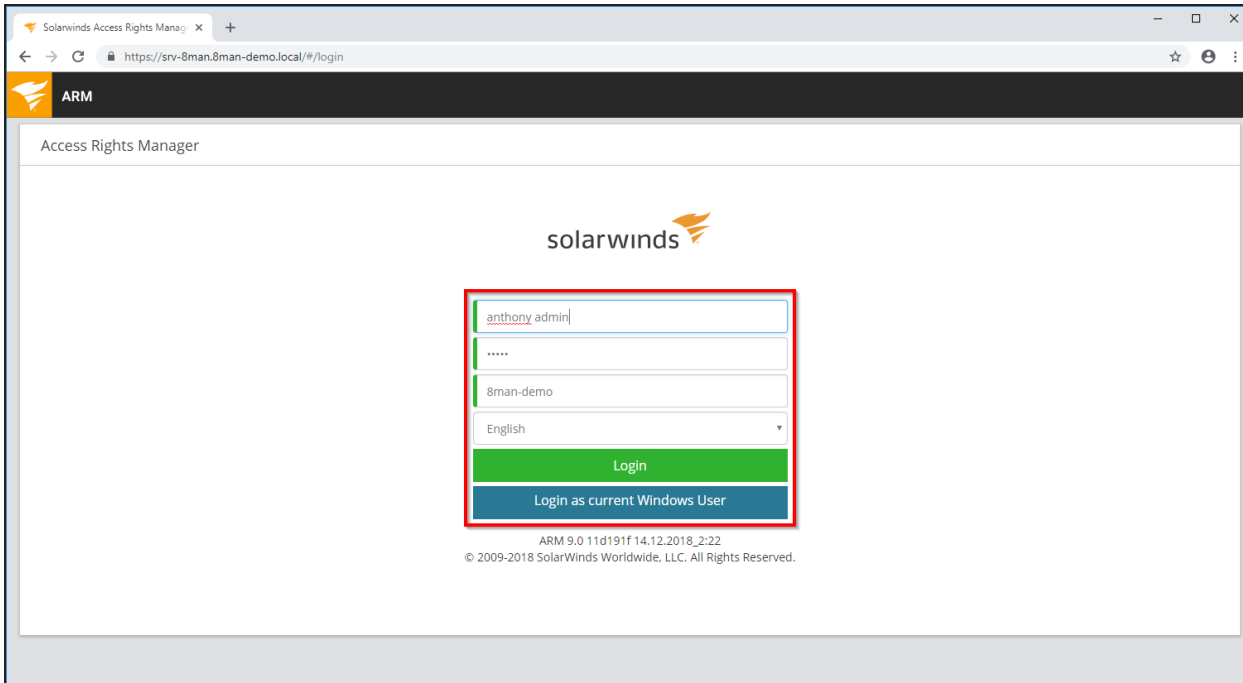
With version 8.0 ARM releases new features to move the GrantMA configuration into the web client. We inserted the new role "Resource Owner". Assign this role completely using the web client. Due to the requirements of our customers we designed a direct assignment between the Resource Owner and the resource - without the need of creating organizational categories in the data owner configuration.

 The functionality is deactivated by default. Please see [Activate the Resource Owner feature](#).

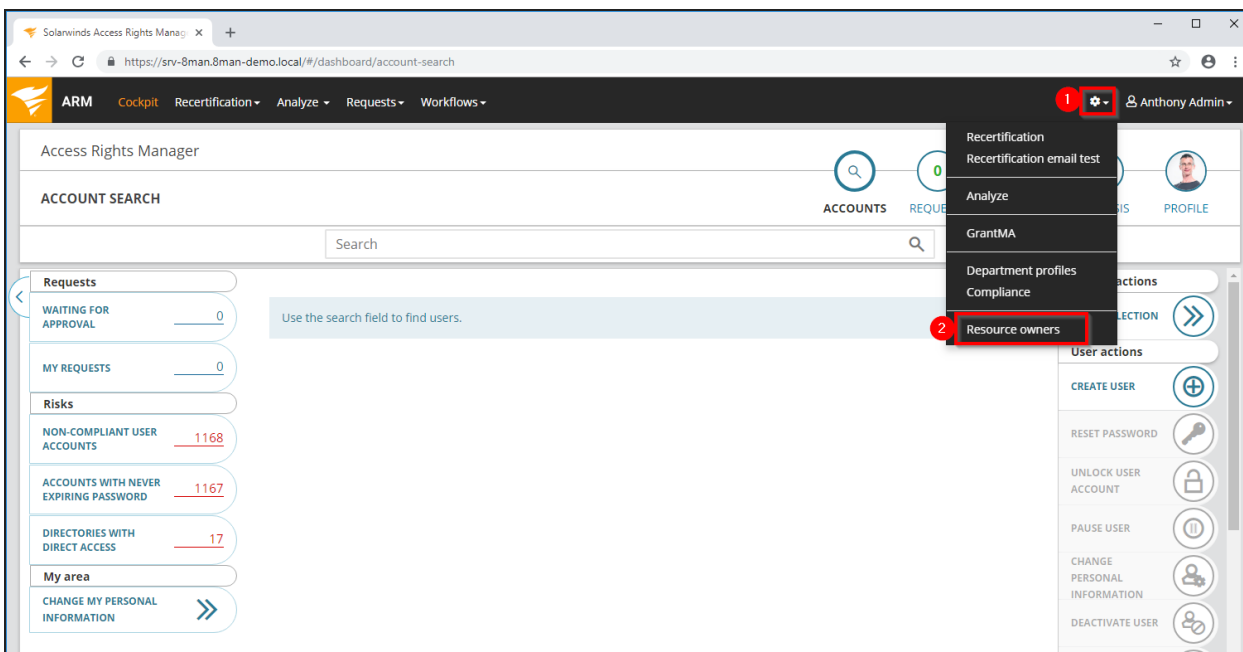
## Related features

[GrantMA: Design approval processes](#) (administrator)

## Step-by-step process



Login to the web interface with admin credentials.



1. Click the gear-wheel.
2. Select "Resource owners".

The screenshot displays the Solarwinds Access Rights Manager (ARM) interface. The top navigation bar includes 'ARM', 'Cockpit', 'Recertification', 'Analyze', 'Requests', and 'Workflows'. The user is logged in as 'Anthony Admin'. The main content area is titled 'Assigned resource owners' and shows a breadcrumb path: 'All Resources / File server / srv-8man / Organization / Human Resources'. A search bar is present on the right side. The left sidebar shows a tree view of resources, with 'Human Resources' highlighted in bold. Red boxes and numbers 1-4 indicate key features: 1. Search bar, 2. Tree view icons, 3. Finance directory (gray text), 4. Human Resources directory (bold text).

1. Search for resources or alternatively navigate through the tree.
2. The icons indicate assignments and assignments in subdirectories.
3. Gray text color indicates that no resource owner is assigned to the directory.
4. Bold text indicates an existing assignment.

Solarwinds Access Rights Manager

SETTINGS: GRANTMA

Search

▼ All Resources

- ▶ Active Directory

▼ File server

▼ srv-8man

▼ Organization

- ▶ Development
- ▶ Facility Management
- ▶ Finance

▶ Human Resources

- ▶ Management
- ▶ Marketing
- ▶ Production
- ▶ Research
- ▶ Sales
- ▶ Projects
- ▶ Templates
- Users

### Assigned resource owners

All Resources / File server / srv-8man / Organization / Human Resources

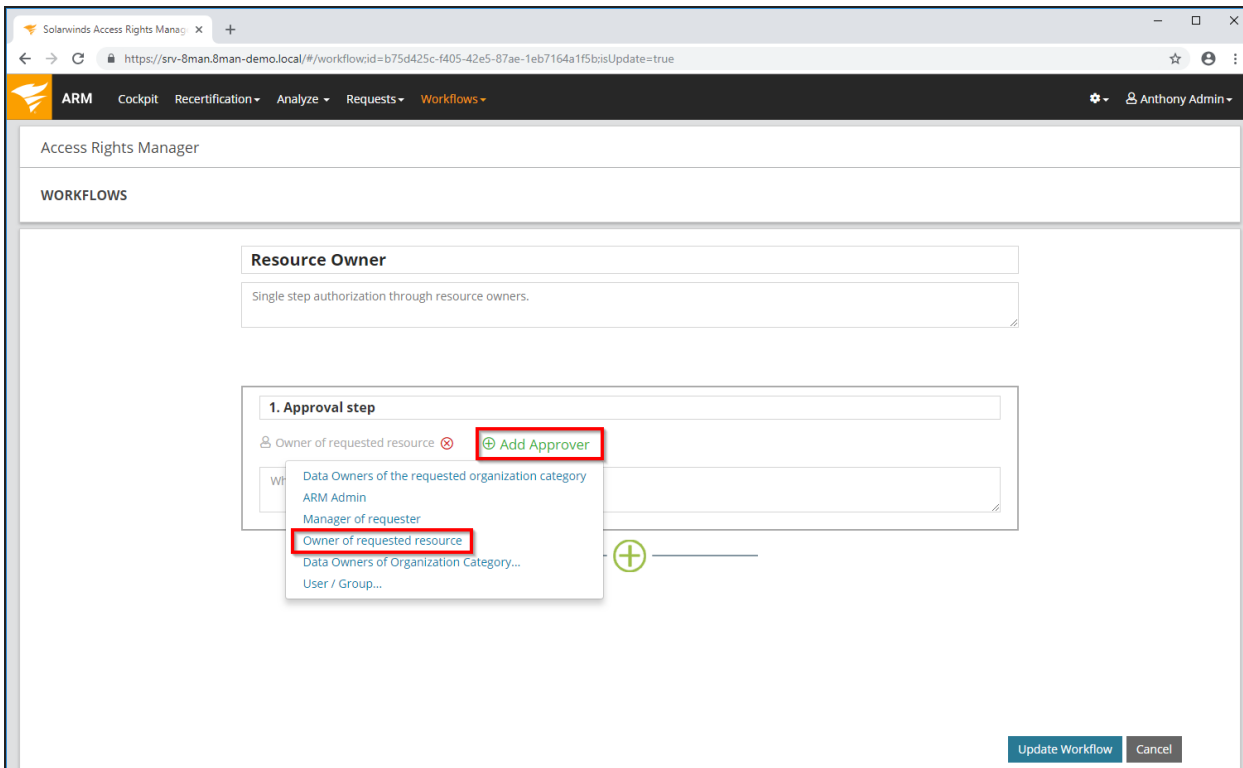
Henry HR (8man-demo\Henry HR)

Search: henr

- Search my domain only
- Search history

- Henry HR (8man-demo\Henry HR)
- Edith Henriksson (8man-demo\Edith Henriksson)
- Anders Henriksen (8man-demo\Anders Henriksen)

1. Find an user or a group.
2. Click a search result to set an assignment.
3. Delete an existing assignment.



Example: Design individual approval flows with the new role resource owner as an approver.

## Import or export resource owner configurations

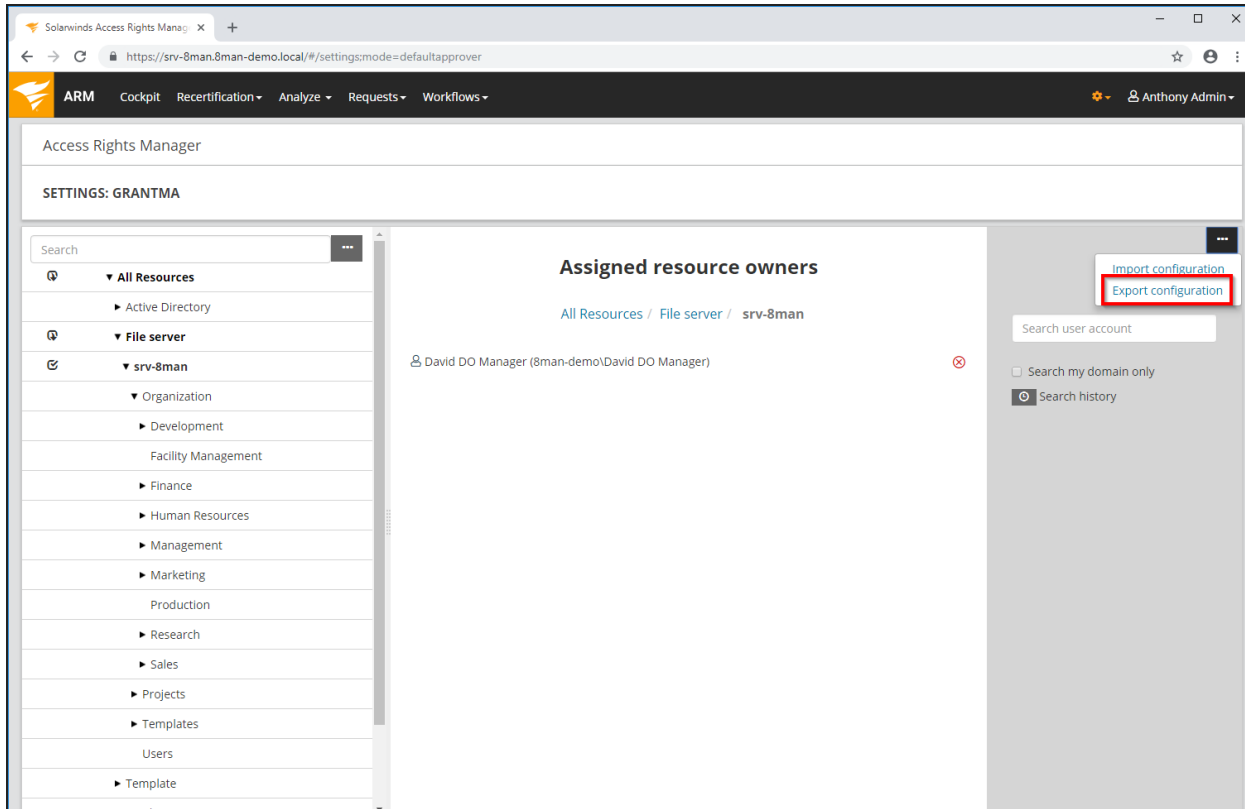
### Background / Value

Automate and accelerate the assignment of resource owners by editing a CSV-file. Import/export the assignments to transfer the configuration from one system to another, for example from a testing to a productive environment.

### Related features

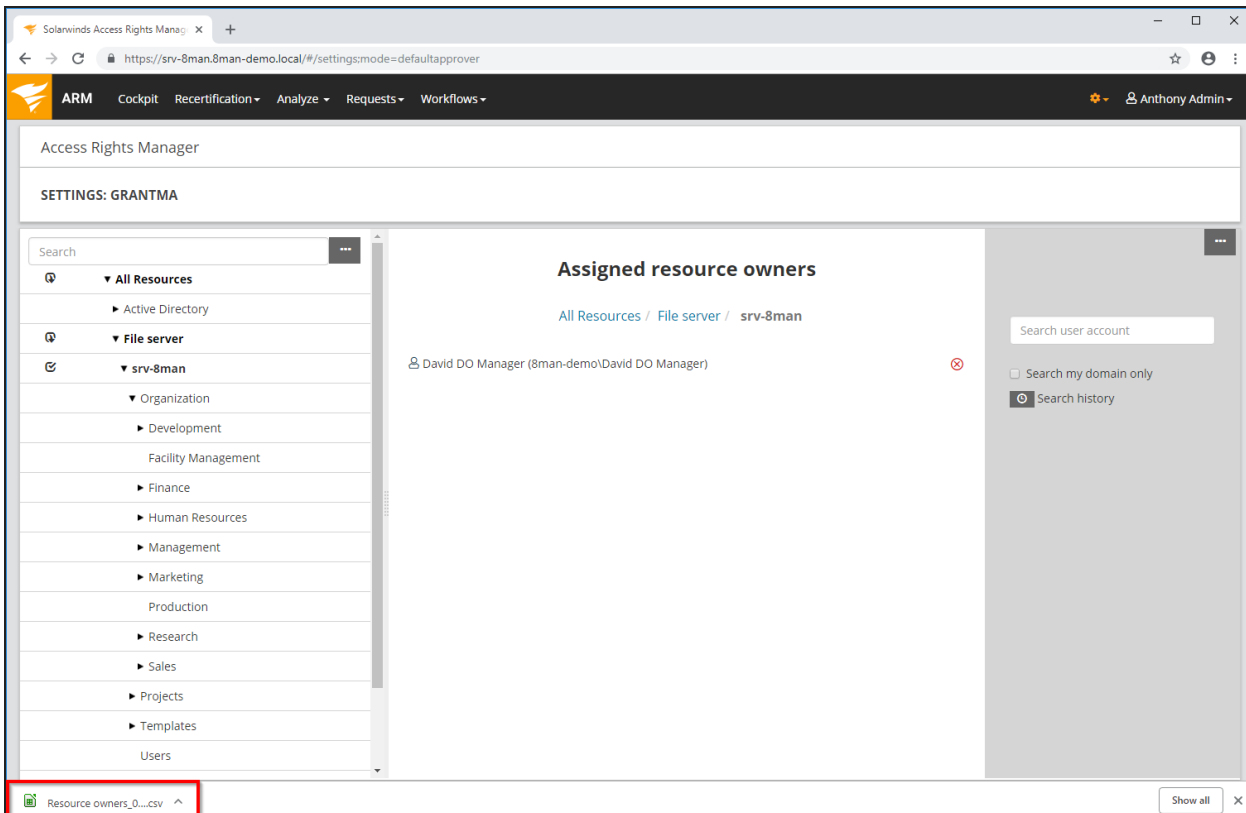
[GrantMA: Design approval processes](#) (administrator)

## Step-by-step process



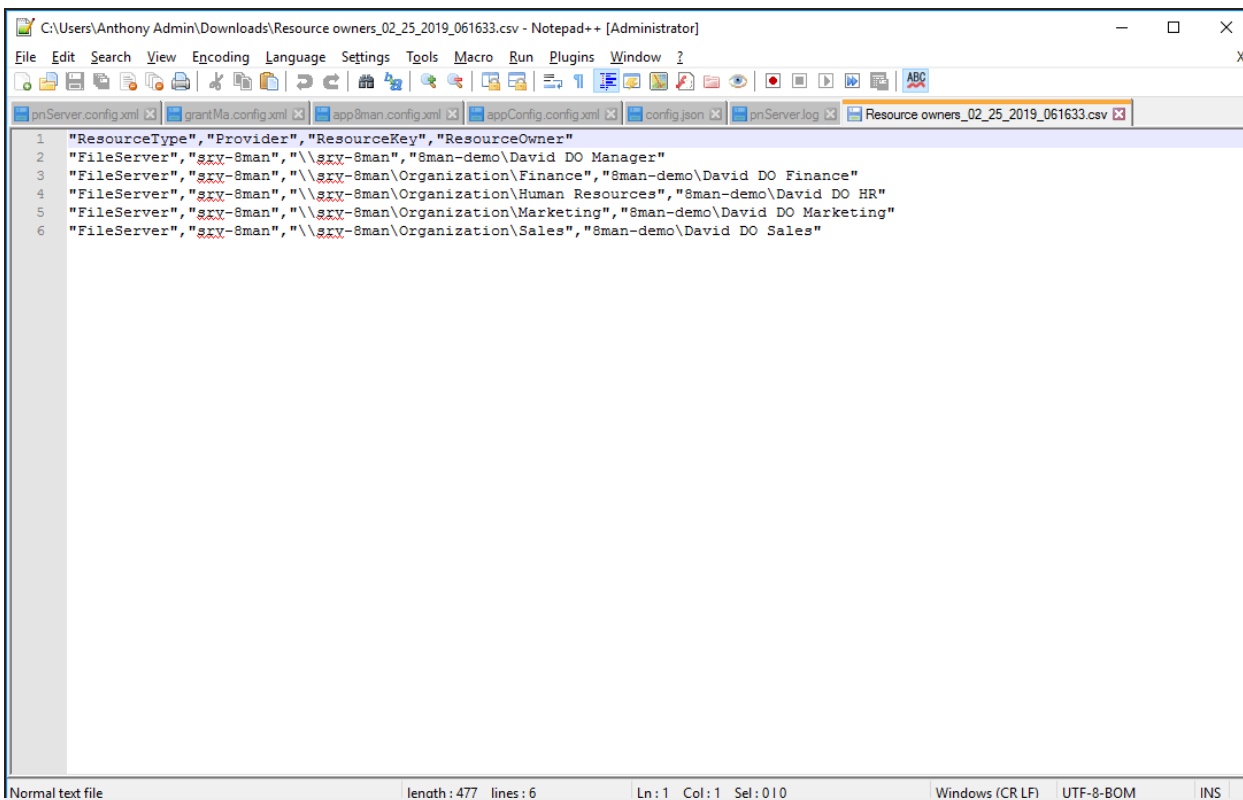
The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The browser address bar indicates the URL: `https://srv-8man.8man-demo.local/#/settings:mode=defaultapprover`. The page title is "Access Rights Manager" and the settings are for "GRANTMA". The main content area is titled "Assigned resource owners" and shows a breadcrumb trail: "All Resources / File server / srv-8man". Below the breadcrumb, a user "David DO Manager (8man-demo\David DO Manager)" is listed with a red "X" icon. On the right side, there are two buttons: "Import configuration" and "Export configuration", with the latter highlighted by a red box. A search bar and search history section are also visible on the right.

Export the configuration to a CSV-file after assigning resource owners. Click "Export configuration".



The export file is handled as a download. Displaying and saving of the file depends on the browser.





```
C:\Users\Anthony Admin\Downloads\Resource owners_02_25_2019_061633.csv - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
pnServer.config.xml x grantMa.config.xml x app8man.config.xml x appConfig.config.xml x config.json x pnServer.log x Resource owners_02_25_2019_061633.csv x
1 "ResourceType","Provider","ResourceKey","ResourceOwner"
2 "FileServer","sxy-8man","\\sxy-8man","8man-demo\David DO Manager"
3 "FileServer","sxy-8man","\\sxy-8man\Organization\Finance","8man-demo\David DO Finance"
4 "FileServer","sxy-8man","\\sxy-8man\Organization\Human Resources","8man-demo\David DO HR"
5 "FileServer","sxy-8man","\\sxy-8man\Organization\Marketing","8man-demo\David DO Marketing"
6 "FileServer","sxy-8man","\\sxy-8man\Organization\Sales","8man-demo\David DO Sales"
Normal text file length: 477 lines: 6 Ln:1 Col:1 Sel:0|0 Windows (CR LF) UTF-8-BOM INS
```

You can edit the CSV-file.

Please note that the assignment must always be one-to-one.

Access Rights Manager

SETTINGS: IMPORT RESOURCE OWNERS

IMPORT RESOURCE OWNERS

Order alias name ▲	Order product specification	Organizational category	Resource owner	Status
FileServer	srv-8man	\\srv-8man\Organization\Finance	8man-demo\David DO Finance	
FileServer	srv-8man	\\srv-8man\Organization\Marketing	8man-demo\David DO Marketing	
FileServer	srv-8man	\\srv-8man\Organization\Human Resour	8man-demo\David DO HR	
FileServer	srv-8man	\\srv-8man\Organization\Sales	8man-demo\David DO Sales	
FileServer	srv-8man	\\srv-8man	8man-demo\David DO Manager	
FileServer	srv-8man	\\srv-8man\Organization\Human Resour	8man-demo\Mama	

Buttons: New (2), Import (3), Load CSV file (1)

1. Load a CSV-file.
2. Clear the loaded list.
3. Click "Import".

Import resource owners

Delete existing configuration before importing (1)

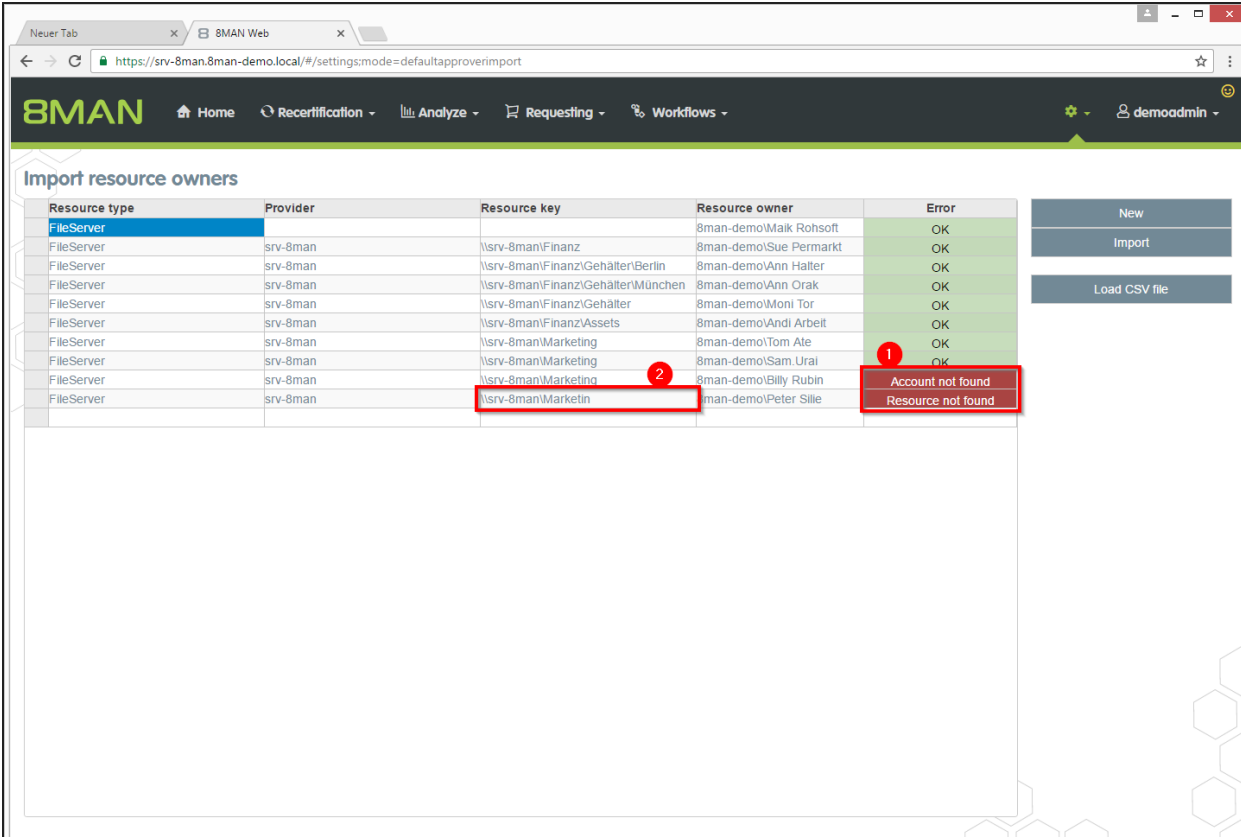
Buttons: Cancel, Import data (2)

1. **Option activated:**  
The existing configuration will be deleted before the import.

**Option deactivated:**

The existing configuration will be retained. The import will be added. No duplicates will be generated.

2. Start the import process.



The screenshot shows the 8MAN web interface with the 'Import resource owners' table. The table has the following columns: Resource type, Provider, Resource key, Resource owner, and Error. The table contains 12 rows of data. The last two rows have error messages in the 'Error' column. Callout 1 points to the error message 'Account not found' and 'Resource not found'. Callout 2 points to the resource key '\srv-8man\Marketin' in the third column of the last row.

Resource type	Provider	Resource key	Resource owner	Error
FileServer	srv-8man	\srv-8man\Finanz	8man-demo\Maik Rohsoft	OK
FileServer	srv-8man	\srv-8man\Finanz\Sue Permarkt	8man-demo\Sue Permarkt	OK
FileServer	srv-8man	\srv-8man\Finanz\Gehälter\Berlin	8man-demo\Ann Halter	OK
FileServer	srv-8man	\srv-8man\Finanz\Gehälter\München	8man-demo\Ann Orak	OK
FileServer	srv-8man	\srv-8man\Finanz\Gehälter	8man-demo\Moni Tor	OK
FileServer	srv-8man	\srv-8man\Finanz\Assets	8man-demo\Andi Arbeit	OK
FileServer	srv-8man	\srv-8man\Marketing	8man-demo\Tom Ale	OK
FileServer	srv-8man	\srv-8man\Marketing	8man-demo\Sam Urai	OK
FileServer	srv-8man	\srv-8man\Marketing	8man-demo\Billy Rubin	Account not found
FileServer	srv-8man	\srv-8man\Marketin	8man-demo\Peter Sille	Resource not found

1. ARM shows you where errors occurred during import.
2. Edit fields directly in the table to fix small errors immediately.

# Using ARM

ARM benefits Access Rights Management in the following five areas. ARM Audit Edition covers Permission Analysis, Documentation & Reporting and Security Monitoring.

## Permission analysis

ARM analyzes the authorization situation in your company and shows who can access a given resource. In a central view, you can see the group memberships from Active Directory and the access rights to your file servers, SharePoint sites, Exchange or other integrated resources. With this knowledge, you are able to take action and protect your company from internal security incidents.

ARM puts you back in control. One click on the Resource view shows the actual condition of a scanned system and the employees with authorizations for it.

## Cross-resource

Many of the ARM Permission Analysis features are available for all configured resources.

## Identify the permissions of a user

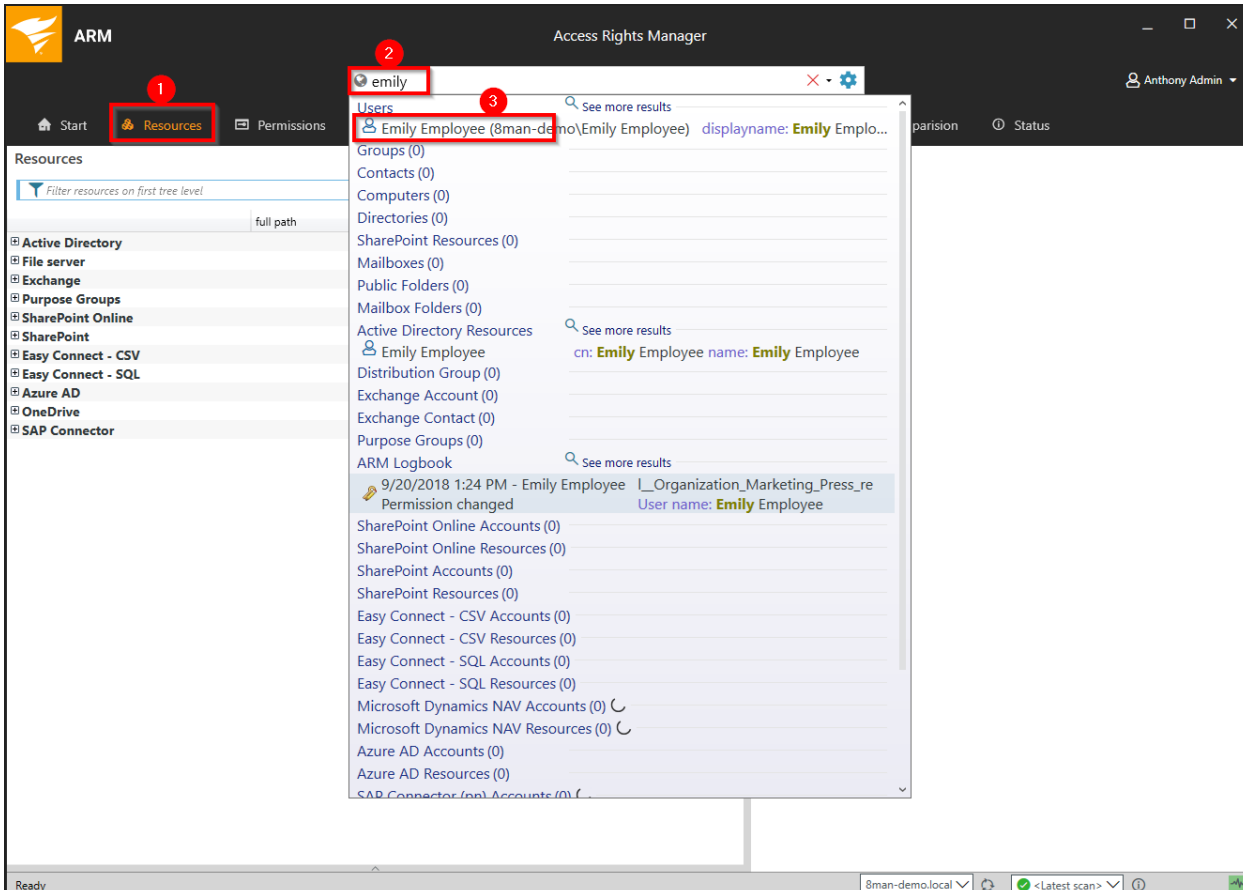
### Background / Value

ARM can also show you the user perspective, and which resources individual users have access to. This is important as it allows you to compare the rights of a given employee to the role that they fill in your organization. Here the "least privilege principle" applies. Employees who have changed departments several times often still have access rights from previous roles that could have been removed after taking on new roles.

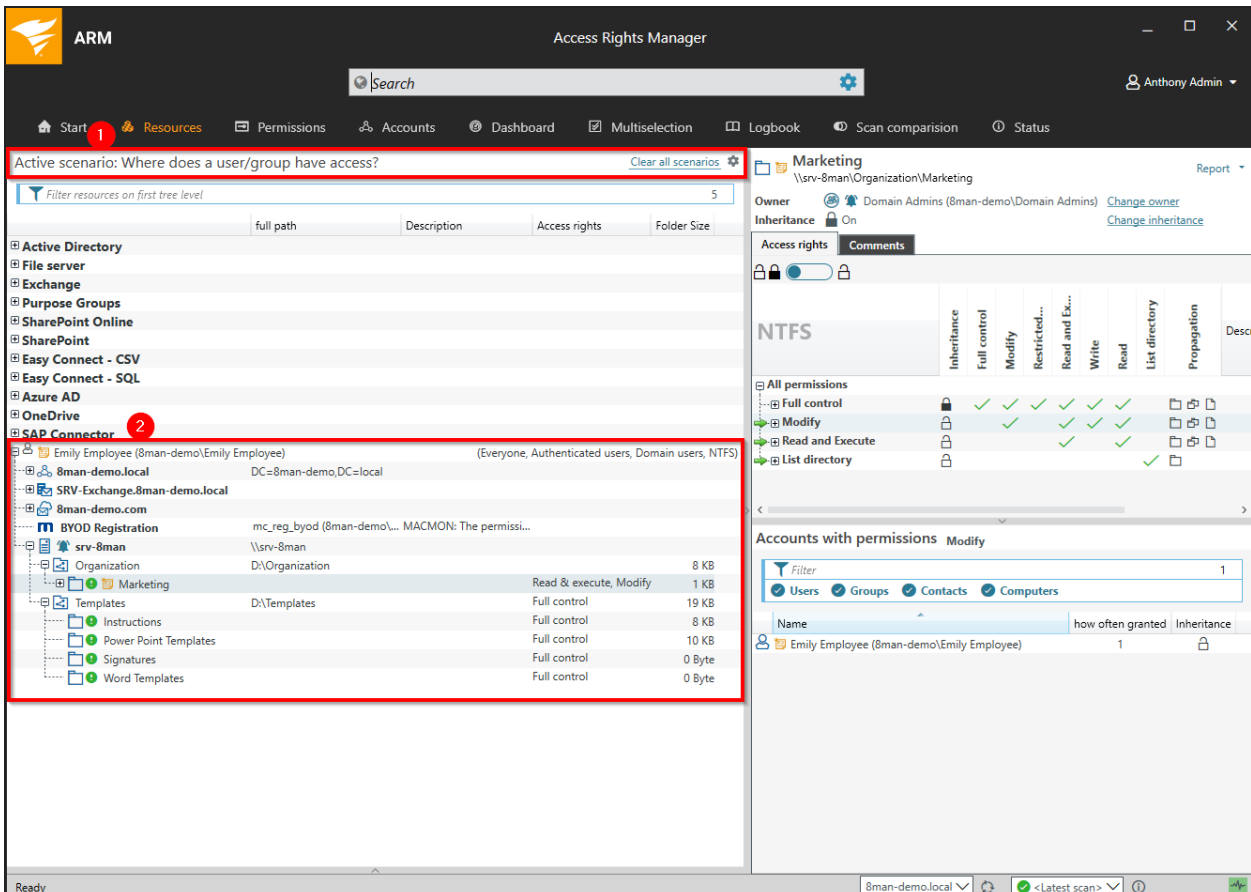
### Related features

Report: [Where do users and groups have access to?](#)

## Step-by-step process



1. Select "Resources".
2. Enter the name of the person whose access rights you want to analyze.
3. Select the desired result in the "User" area.



1. ARM activates the scenario "Where does a user/group have access"
2. ARM shows all resources that "Emily Employee" can access.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The left pane displays a tree view of resources under the 'Marketing' directory, with a green circle and exclamation mark (5) next to the 'Marketing' folder. The right pane shows the 'Marketing' directory's access rights, with a red box highlighting the 'NTFS' permissions table. A green arrow (4) points to the 'Emily Employee' user in the permissions list. A red circle (3) is placed on the 'NTFS' header, and another red circle (2) is on the 'Marketing' folder in the left pane. A red circle (1) is on the 'srv-8man' server in the left pane.

NTFS	Inheritance	Full control	Modify	Restricted...	Read and Ex...	Write	Read	List directory	Propagation	Des
All permissions										
Full control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Modify	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Read and Execute	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
List directory	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1. ARM shows all directories that "Emily Employee" can access on the file server.
2. In this example we have focused on the "Marketing" directory.
3. ARM shows the access rights for the "Marketing" directory.
4. The green arrow indicates the user "Emily Employee". This helps you identify which resources "Emily Employee" can access, based upon the individual permission paths.
5. The green circle with the exclamation mark indicates that the access rights on this directory differ from the "parent" directory.

## Identify access rights on a resource

### Background / Value

ARM quickly shows you all access rights on resources. Initially you should focus on the resources containing the most sensitive data. You simply need to know: Who has access?

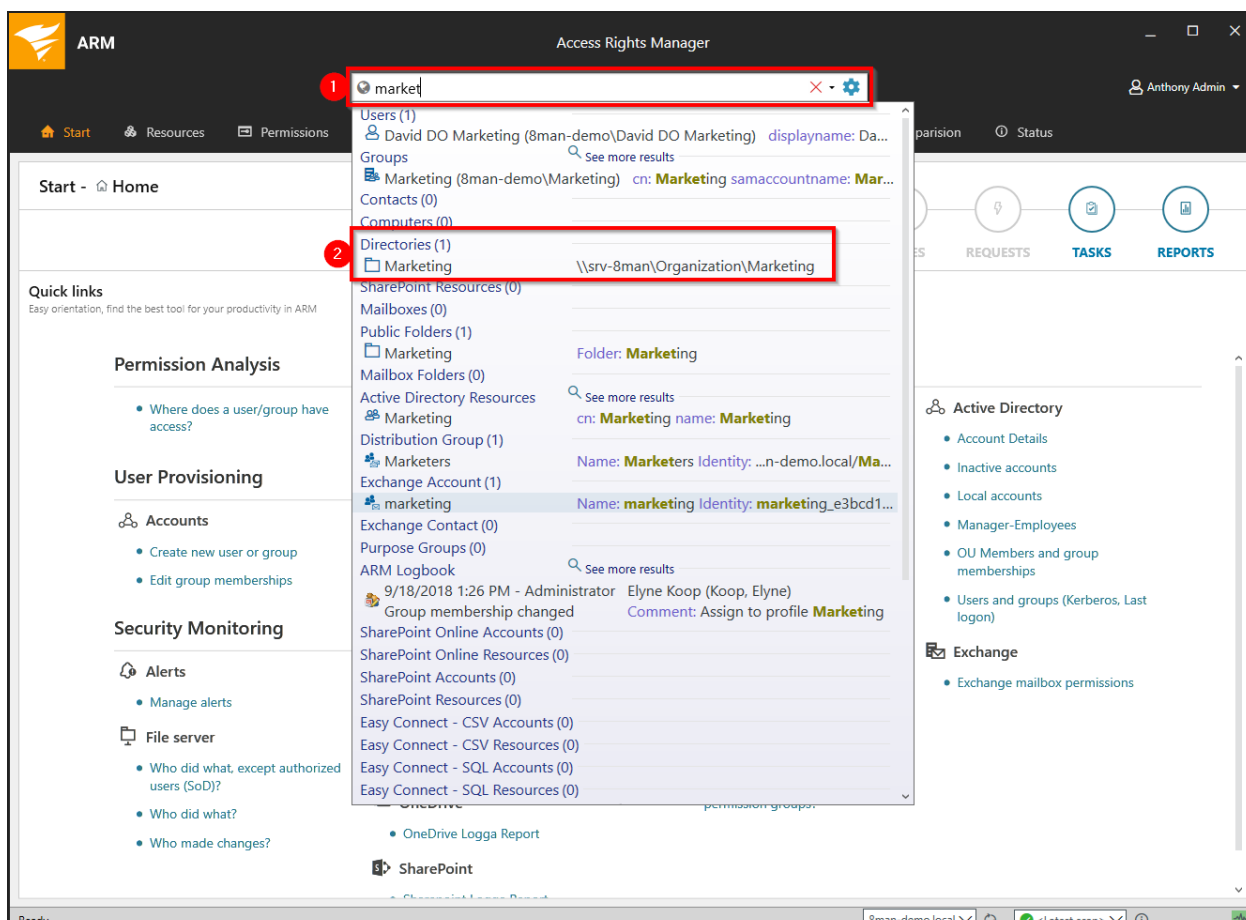
### Related features

[Report: Who has access where?](#)

[Modify directory access rights](#)

[Monitor access to sensitive data](#)

### Step-by-step process



1. Search for the desired directory.
2. You can find your search result in the directory section.



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The 'Resources' tab is selected, and the 'Marketing' directory is expanded in the tree view. The 'Access rights' tab is active, displaying a table of NTFS permissions for the selected directory. The table shows permissions for 'Full control', 'Modify', 'Read and Execute', and 'List directory'. Below the table, a list of accounts with permissions is shown, including 'Adam Adminmanager', 'Administrator', 'Anthony Admin', 'Antoine Admin', 'Anton Admin', 'Caroline Berggren', 'David DO Marketing', 'Domain Users', 'Elyne Koop', 'Emily Employee', and 'Ludvig Karlsson'.

NTFS	Inheritance	Full control	Modify	Restricted...	Read and Ek...	Write	Read	List directory	Propagation
All permissions									
Full control	🔒	✓	✓	✓	✓	✓	✓	✓	📁
Modify	🔒		✓		✓	✓	✓		📁
Read and Execute	🔒				✓		✓		📁
List directory	🔒							✓	📁

Name	how often granted	Inherit
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	🔒
Administrator (8man-demo\Administrator)	1	🔒
Anthony Admin (8man-demo\Anthony Admin)	1	🔒
Antoine Admin (8man-demo\Antoine Admin)	1	🔒
Anton Admin (8man-demo\Anton Admin)	1	🔒
Caroline Berggren (8man-demo\Caroline Berggren)	2	2x ⚠️
David DO Marketing (8man-demo\David DO Marketing)	3	3x ⚠️
Domain Users (8man-demo\Domain Users)	1	🔒
Elyne Koop (8man-demo\Elyne Koop)	2	2x ⚠️
Emily Employee (8man-demo\Emily Employee)	4	4x ⚠️
Ludvig Karlsson (8man-demo\Ludvig Karlsson)	3	3x ⚠️
NT AUTHORITY\SYSTEM	1	🔒

1. ARM switches to the resource view.
2. ARM expands the tree and focuses on the desired directory.
3. ARM displays **all** access rights categories that exist for the chosen directory.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The left pane displays a tree view of resources under 'Active Directory' and 'File server'. The main pane shows the 'Marketing' directory with a table of permissions. The 'Modify' permission is selected, and a list of accounts with permissions is displayed below. Red boxes and numbers 1, 2, and 3 highlight the 'Modify' filter, the list of accounts with permissions, and the filter options respectively.

Account	Inheritance	Full control	Modify	Restricted...	Read and Ex...	Write	Read	List directory	Propagation	Descr
Full control										
Modify										
Alfie Williamson (8man-demo\Alfie Williamson)										
Mattias Blom (8man-demo\Mattias Blom)										
Finn Dunne (8man-demo\Finn Dunne)										
L_Organization_Marketing_...										
Caroline Berggren (8man-...										
David DO Marketing (8m...										

Name	how often granted	Inheritance
Alfie Williamson (8man-demo\Alfie Williamson)	1	
Caroline Berggren (8man-demo\Caroline Berggren)	1	
David DO Marketing (8man-demo\David DO Marketing)	1	
Emily Employee (8man-demo\Emily Employee)	1	
Finn Dunne (8man-demo\Finn Dunne)	1	
George Comer (8man-demo\George Comer)	1	
Louie Findlay (8man-demo\Louie Findlay)	1	
Ludvig Karlsson (8man-demo\Ludvig Karlsson)	1	
Mattias Blom (8man-demo\Mattias Blom)	1	
Nadine Eberhart (8man-demo\Nadine Eberhart)	1	
Okeke Abazu (8man-demo\Okeke Abazu)	1	

1. Select an access category filter. You can expand the tree to analyze how permissions are build. In this example the "Modify" filter has been chosen.
2. ARM lists **all** accounts with "Modify" access rights to the Marketing directory in a flat list - regardless of whether they are assigned directly, through groups, or nested groups.
3. You can add additional filters for users, groups, contacts and computers to narrow down the results further.

## Identify multiple access paths

### Background / Value

Multiple access paths are often a consequence of confusing group structures and direct access rights. Access to resources should only be granted using group memberships.

In practice, it often happens that you remove only one access path and then wonder why the user still has access. With ARM you can see all existing access paths with just a few clicks. This is the basis for completely removing all access paths.

### Related features

[Remove multiple access paths to file server directories](#)


Manage group memberships

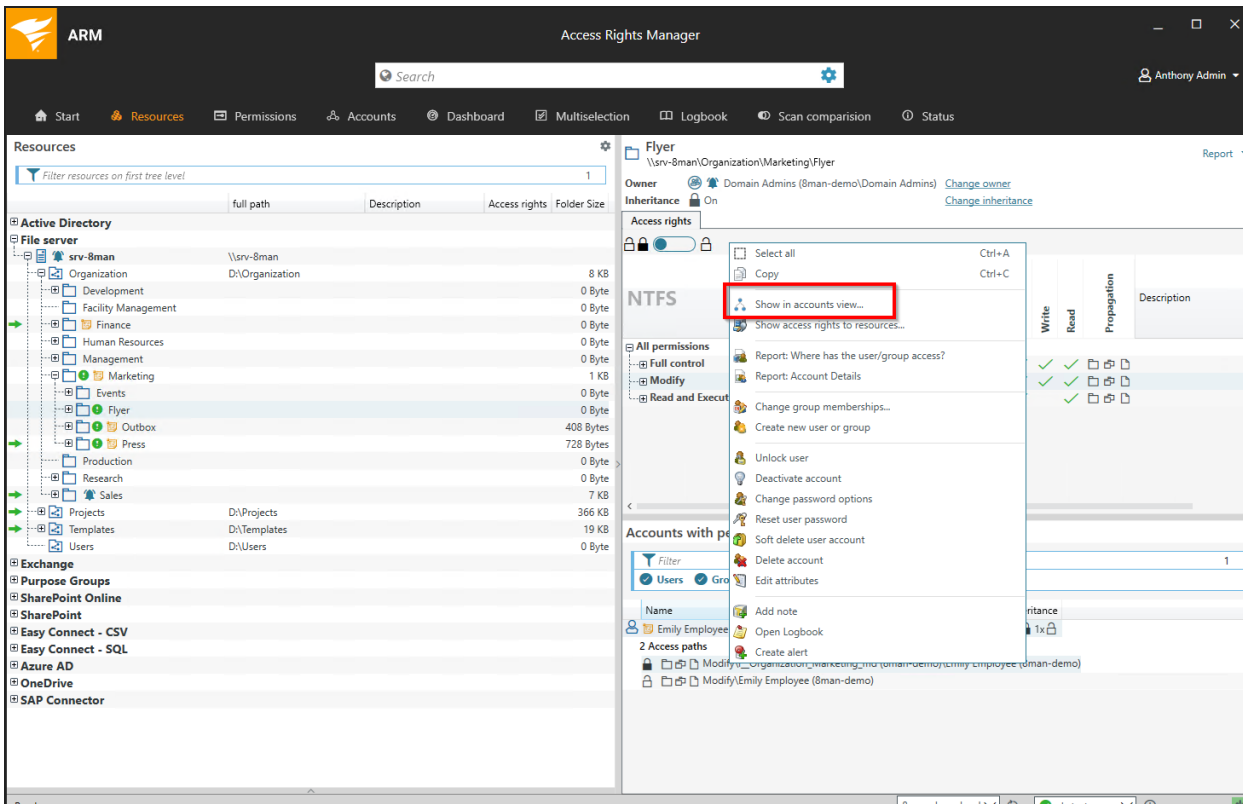
### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The left sidebar displays a tree view of resources under 'File server', with 'Flyer' selected. The main pane shows the 'Flyer' details, including the 'Access rights' table and the 'Accounts with permissions' table. The 'Accounts with permissions' table has a 'how often granted' column, and the 'Emily Employee' entry is highlighted. Below the table, the 'Access paths' section shows multiple paths for the same user.

1. Select "Resources".
2. Select a directory.
3. ARM shows you in the column "how often granted" warnings for multiple access paths.
4. Select an entry.

5. ARM shows you all existing access paths. In this example Emily Employee is granted the modify permission in two ways:
- inherited via the group membership of the permission group
  - via a direct entry to the ACL

 In the resource view you will find many icons and symbols. Hover your mouse over them to get more information and meaning, e.g. inheritance, propagation, group types and so on.



The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main window is titled "Access Rights Manager" and shows a search bar and navigation tabs. The left pane, labeled "Resources", contains a tree view of the file system structure. The right pane, labeled "Flyer", shows the details for the resource, including the owner, inheritance, and access rights. A context menu is open over the "Emily Employee" user, with the option "Show in accounts view..." highlighted in red. The menu also includes options like "Select all", "Copy", "Show access rights to resources...", "All permissions", "Full control", "Modify", "Read and Execute", "Accounts with permissions", and "Access paths".

If you find complicated group structures, we recommend the analysis in the account view. Right-click on the user to open the context menu. Select "Show in accounts view...".

## Identify deviating access rights in the tree structure

### Background / Value

Inheriting permissions is a good way to keep the access rights structure clear and manageable. ARM shows deviating access rights, regardless of whether they were added or removed. If the chain of inheritance is broken, ARM will show this in the tree structure. You can make corrections or leave them as is, if the directory has special protection requirements.

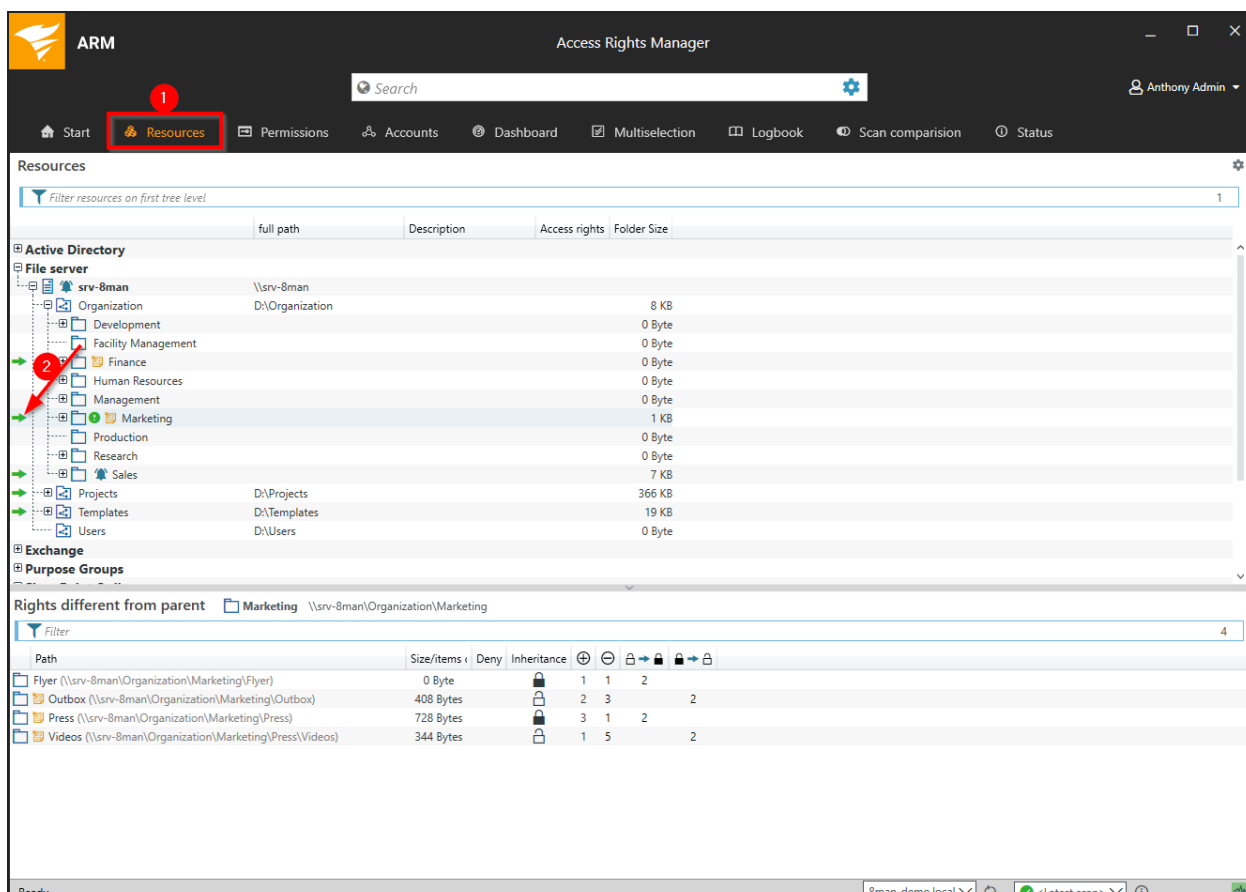
### Related features

Report: [Who has access where?](#)

Report: [Where do users/groups have access?](#)

[Identify corrupted inheritance](#)

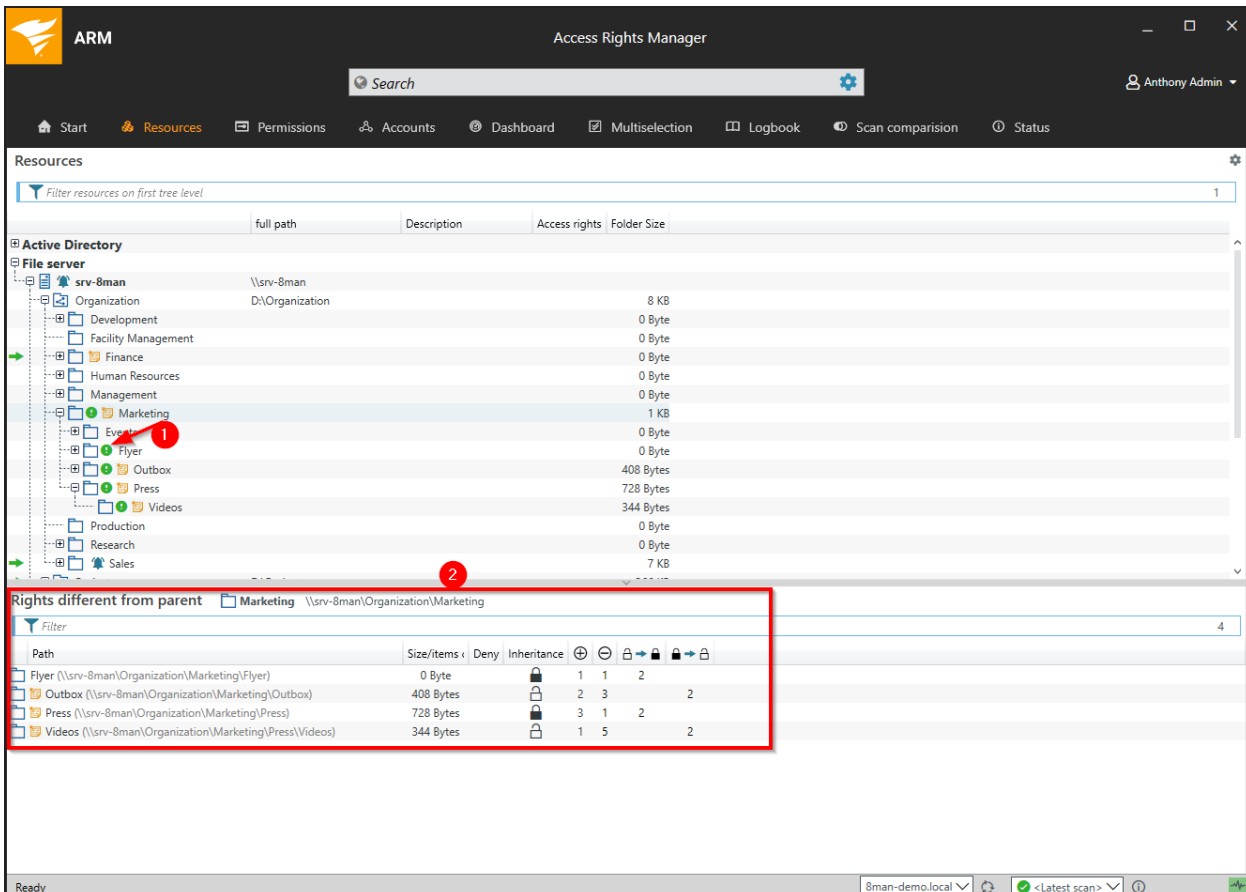
### Step-by-step process



The screenshot shows the Access Rights Manager (ARM) interface. The 'Resources' tab is selected, and the 'Marketing' folder is highlighted. A red arrow points to the 'Marketing' folder, indicating that it contains divergent access rights. The 'Rights different from parent' section shows a table of files with their paths, sizes, and inheritance settings.

Path	Size/items	Deny	Inheritance	+	-	+	-
Flyer (\\srv-8man\Organization\Marketing\Flyer)	0 Byte		1	1	2		
Outbox (\\srv-8man\Organization\Marketing\Outbox)	408 Bytes		2	3	2		
Press (\\srv-8man\Organization\Marketing\Press)	728 Bytes		3	1	2		
Videos (\\srv-8man\Organization\Marketing\Press\Videos)	344 Bytes		1	5	2		

1. Select "Resources".
2. The green arrow indicates that some of the sub-directories contain divergent access rights.



1. The green circle with the exclamation mark indicates that the access rights of this directory differ from its parent.
2. The directories with divergent access rights are listed in a window below with a drill down option.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The main window displays a comparison of access rights between a parent directory and a sub-directory. The interface includes a navigation pane on the left, a search bar at the top, and several data tables. Red boxes and numbers 1-5 highlight specific elements:

- 1. A sub-directory 'Press' in the 'Rights differ from parent' table.
- 2. The 'Access right changes' header and comparison details.
- 3. A list of unchanged access rights for 'Domain Admins' and 'NT AUTHORITY\SYSTEM'.
- 4. A list of added or removed entries for 'Emily Employee', 'li\_Organization\_Marketing\_1st', and 'li\_Organization\_Marketing\_Press\_1st'.
- 5. A list of added or removed inheritance entries for 'I\_Organization\_Marketing\_md' and 'I\_Organization\_Marketing\_re'.

1. Select a sub-directory.
2. ARM shows which directory is compared with which.
3. ARM displays all access rights equal to the parent directory.
4. ARM shows all deviating access rights. A "Plus" signifies added access rights while a "Minus" signifies removed access rights.

## Analyze historical access rights situations

### Background / Value

After the occurrence of data breaches and other security incidents it is often useful to review historical access rights. In this way, you can see who had access at a particular time and who did not. ARM allows you to access historical scans in the usual "Look and Feel" to understand the security implications of access rights at the time of the incident.

### Related features

[Compare two scans from different points in time](#)

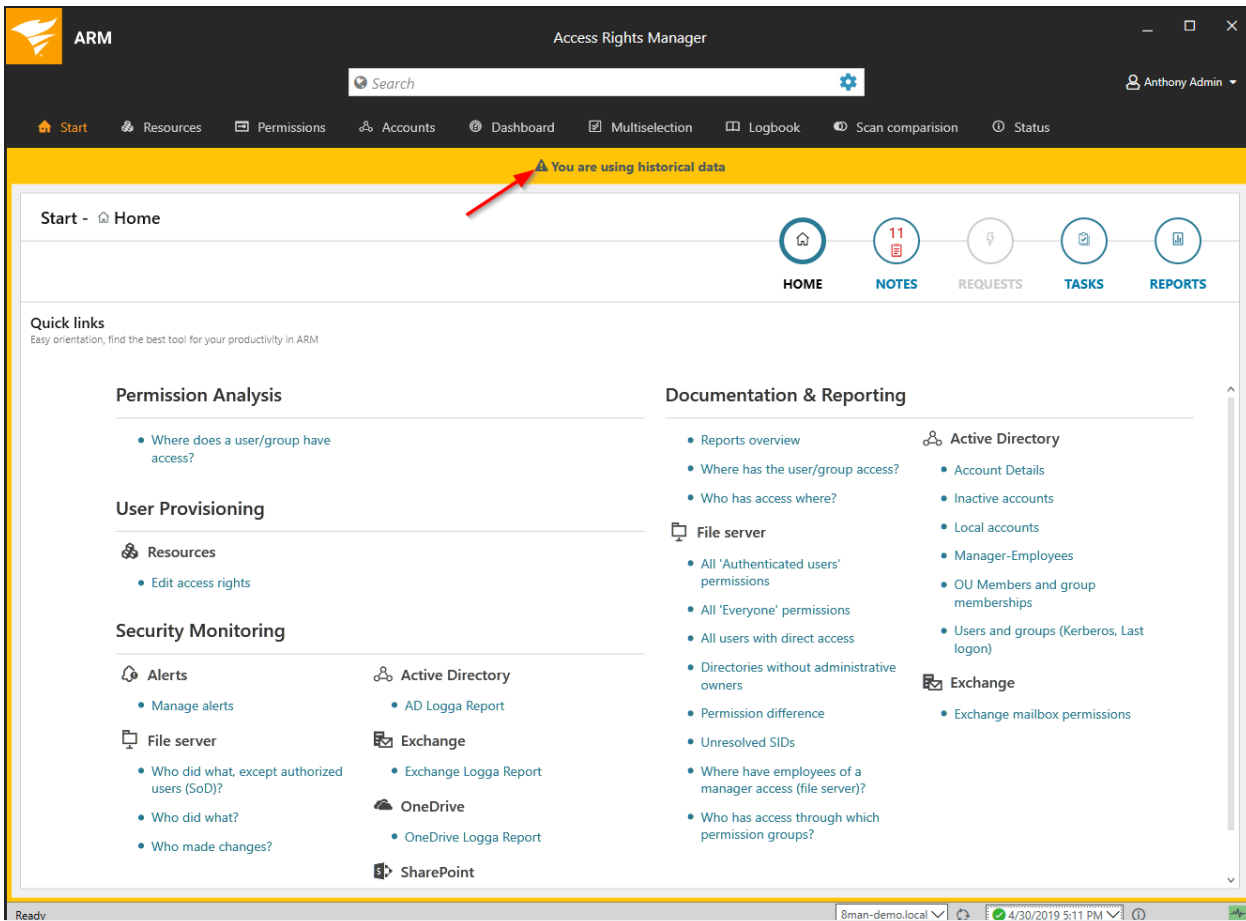
### Step-by-step process

The screenshot shows the ARM web interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The main content area is divided into 'Quick links' and 'Documentation & Reporting'. A dropdown menu is open, showing a list of scan dates. The date '11/7/2019 4:13 PM' is highlighted in orange, indicating it is the selected scan date.

Scan Date
<Latest scan>
11/7/2019 4:13 PM
5/8/2019 10:23 AM
5/7/2019 10:00 PM
5/3/2019 6:15 PM
5/3/2019 3:11 PM
5/3/2019 12:31 PM
5/3/2019 9:50 AM
5/3/2019 8:33 AM
5/2/2019 5:03 PM
5/2/2019 3:20 PM
5/2/2019 3:08 PM
4/30/2019 5:11 PM
4/30/2019 5:07 PM
4/30/2019 5:03 PM
4/29/2019 4:55 PM
12/18/2018 1:26 PM
12/18/2018 8:13 AM
<Latest scan>

Select the desired scan date.





The warning sign and orange frame indicate that you are viewing historical data.

## Compare two different access rights situations (Scan Comparison)

### Background/Value

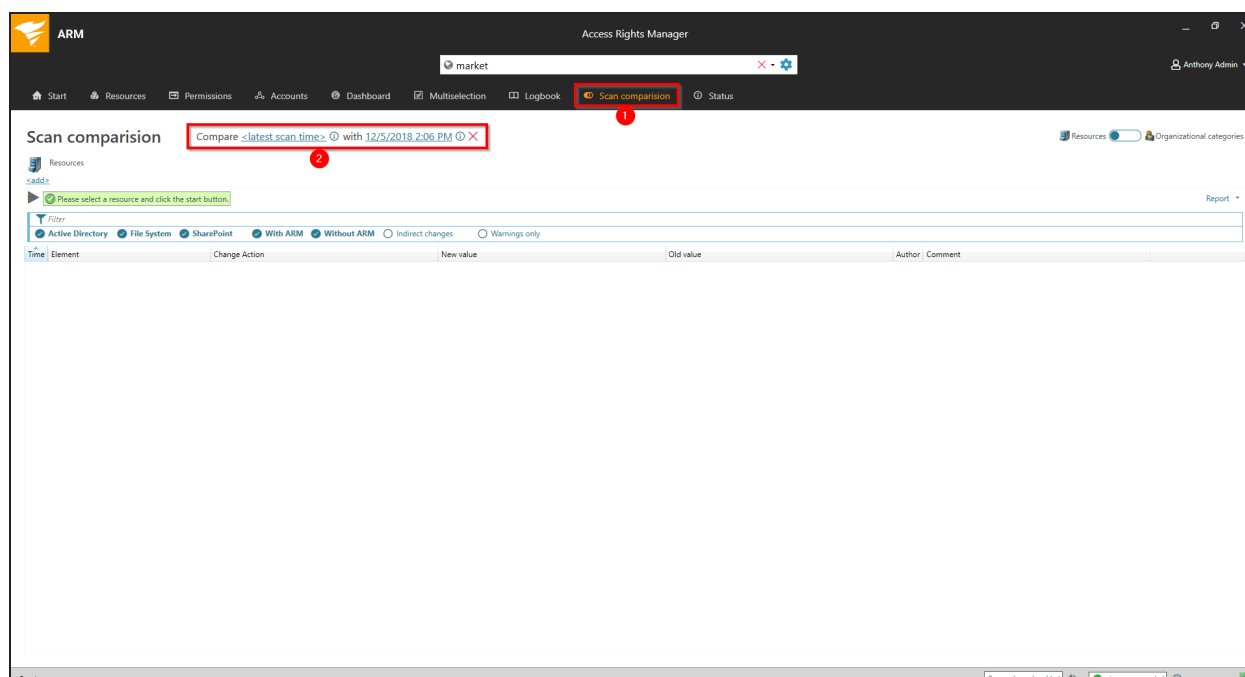
The scan comparison shows the actual states of two authorization situations in the AD and on file servers and compares them with each other. This enables you to determine how the authorization situation has changed.

### Related features


The comparison refers exclusively to two measurement points. Use the Logga reports to analyze all changes of a period.

Use the [Report on permission differences](#) to forward comparison results to other persons.

### Step-by-step process



1. Click on "Scan comparison".
2. Select the two scans that you want to compare.


**Time range for scan comparison**
✕

**End of time range for scan compare**  
Please select an end date for the scan comparison.


◀ December 2018 ▶


Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12			

**Time ( Hour : Minute )**  
◀ 14 ▶ : ◀ 08 ▶

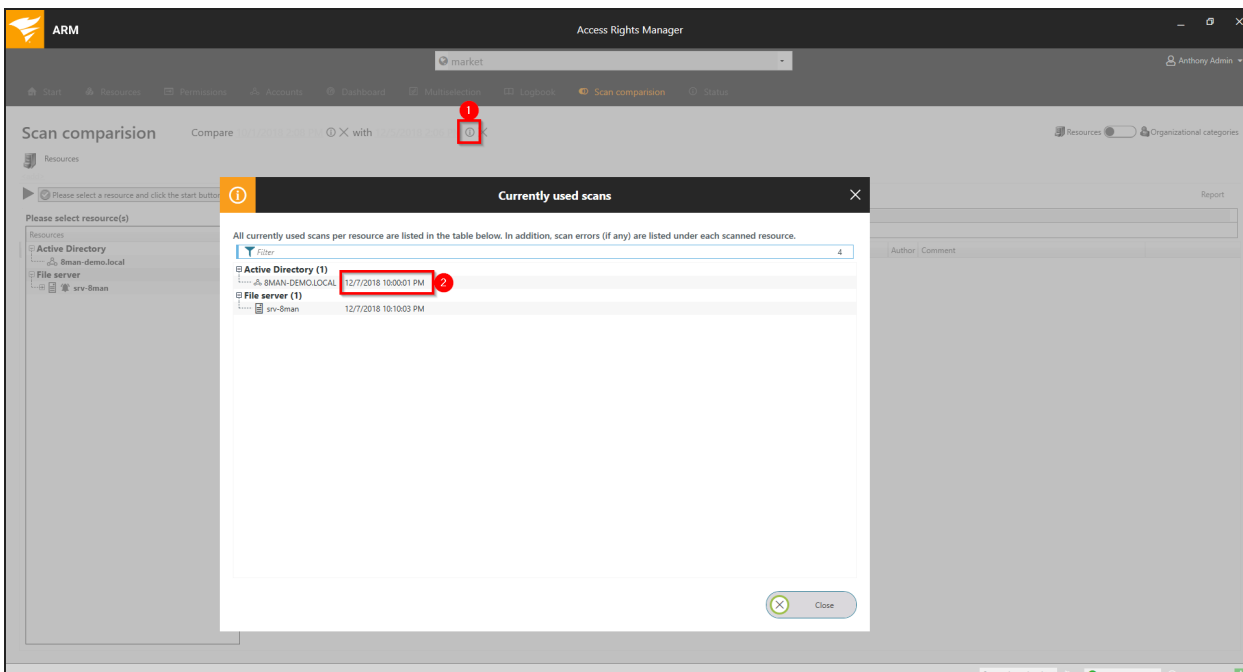
**Time zone**

**Selected date**  
 Wednesday, December 12, 2018 2:08 PM  
 Wednesday, December 12, 2018 1:08 PM [UTC]

 **Apply**

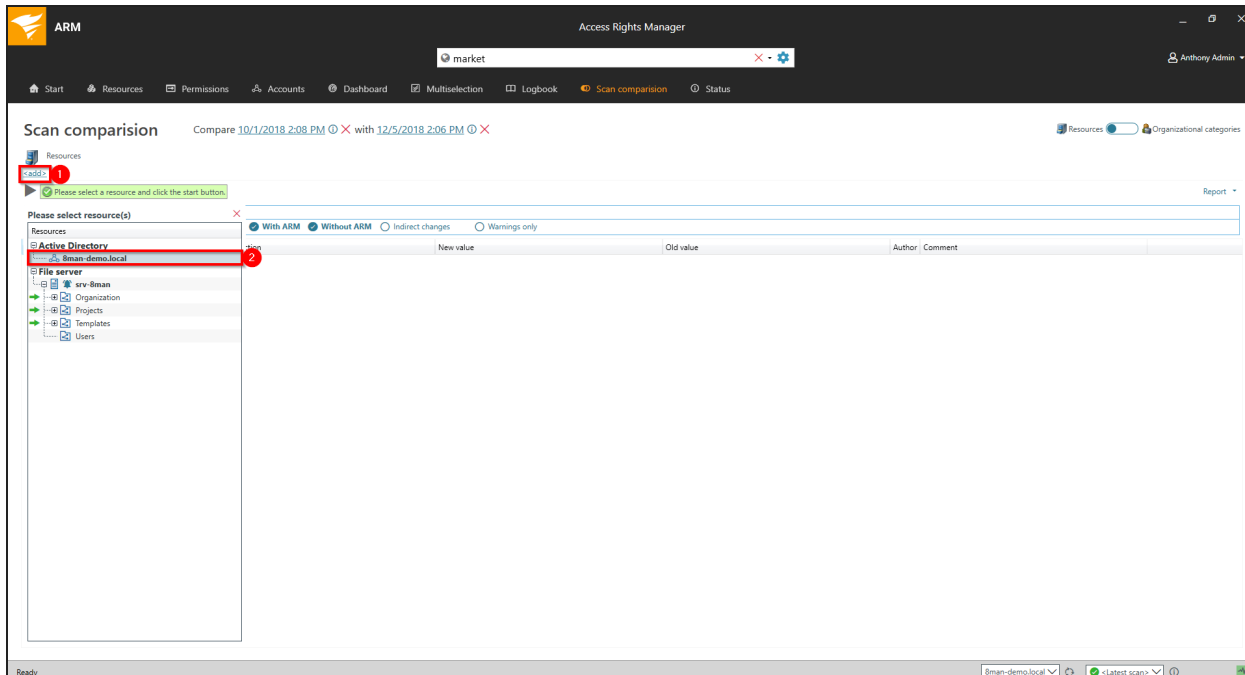
**Cancel** 

Specify the date and time for the start and end points.

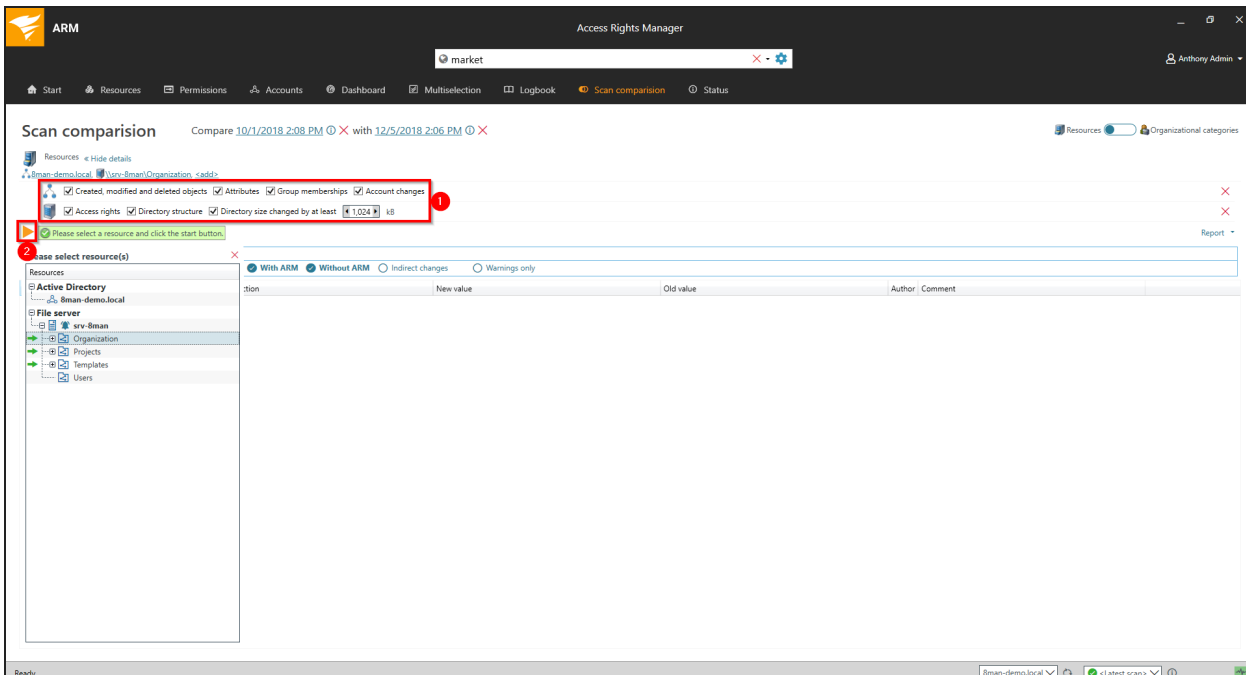


The comparison always compares existing scans.

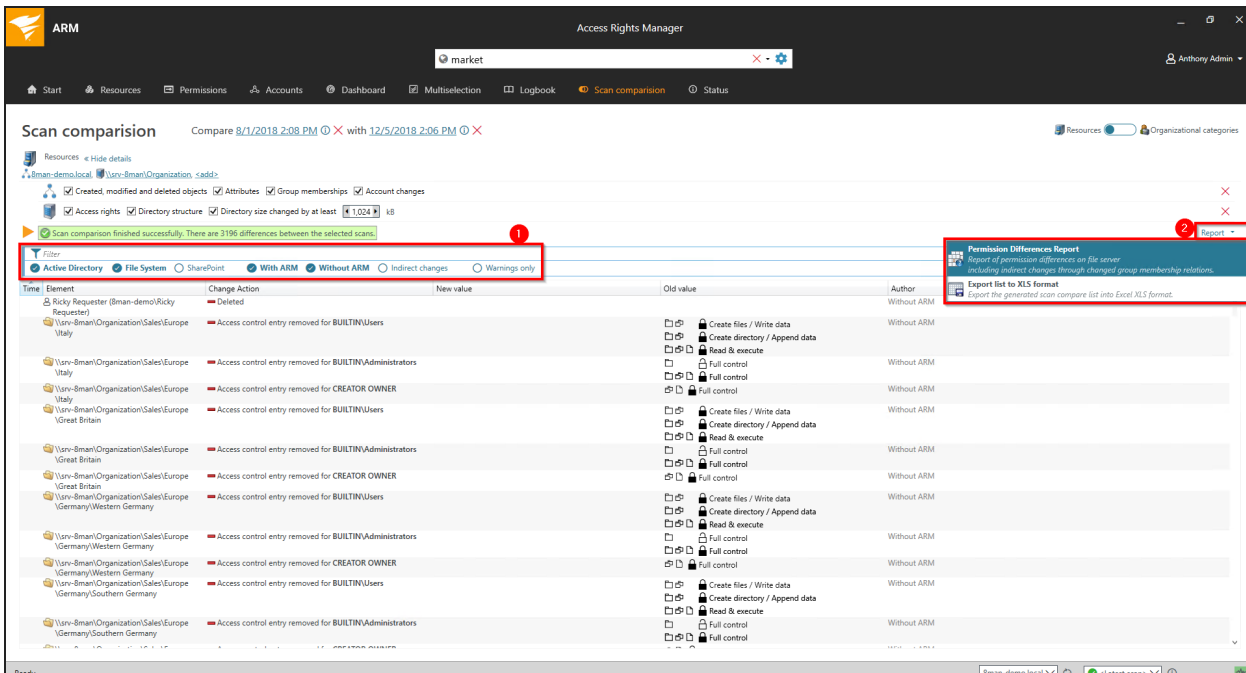
1. Click on the information symbol.
2. Date and time of the selected scan is indicated on the right-hand side.



1. Click "add".
2. Add the desired resource by double clicking on it.



1. Select the range of the comparison.
2. Start the comparison.



1. Use filters to focus on specific actions.
2. Generate a structured "Permission Differences Report" or export the results to .XLS.

## Get an overview of the environment in the Web Dashboard

### Background / Value

Administrators want a quick overview of the current system status in the web client. Key performance indicators of Active Directory, access management risks or the ARM configuration are displayed at a glance.

### Related features

You can find additional useful information in the ARM application (rich client) dashboard, for example depth of group nesting, top 5 Kerberos tokens by size, top 5 oldest logons.

### Step-by-step process

The screenshot displays the ARM Dashboard interface. At the top, there is a navigation bar with tabs for 'ARM', 'Dashboard', 'Cockpit', 'Recertification', 'Analyze', 'Requests', and 'Workflows'. The user 'Anthony Admin' is logged in. The main content area is titled 'ARM Dashboard' and features a 'Quick actions' dropdown. A red box highlights the 'Environment' section, which contains six cards: 'Domains' (1), 'Resources' (3), 'Users' (1178), 'Administrators' (14), 'Computers' (6), and 'Groups' (1706). A red box also highlights the 'Analysis' button in the 'Groups' card. Below the environment summary, there are three main sections: 'Active Directory summary' (showing counts for users, computers, and groups), 'Latest scans' (a table of scan results), and 'Risk assessment' (a table of risk items).

Active Directory state	Count
<b>Users</b>	<b>1178</b>
Disabled users	3
Enabled inactive users	18
Users with never expiring password	0
Expired password	0
<b>Computers</b>	<b>6</b>
Disabled computers	0
Enabled inactive computers	1
<b>All Groups</b>	<b>1706</b>
Empty groups	34
Groups in recursions	24

Status	Type	Resource	Time
✓	✉	8man-demo.com	22 May, 01:23 PM
✓	🏠	8man-demo.local	07 May, 10:00 PM
✓	🖨	srv-8man	03 May, 06:15 PM
✓	🔑	8man-demo.com (e6d421c0-debd-41f6-be4d-67072347...	17 Dec, 08:00 AM
✓	🌐	https://8mandemo.sharepoint.com	01 Oct 2018, 07:43 PM
✓	🏢	Protected Networks GmbH	26 Sep 2018, 01:35 PM

Severity	Title	Resources	Count
----------	-------	-----------	-------

1. Summary of your environment.
2. Jump quickly to the Analyze scenarios.

Solarwinds Access Rights Manager (ARM) Dashboard

Environment

Domains	Resources	Users	Administrators	Computers	Groups
1	3	1178	14	6	1706

**Active Directory summary**

Active Directory state [Analysis](#)

Users	Count
Disabled users	3
Enabled inactive users	18
Users with never expiring password	0
Expired password	0

Computers	Count
Disabled computers	0
Enabled inactive computers	1

All Groups	Count
Empty groups	34
Groups in recursions	24

**Latest scans**

Status	Type	Resource	Time
✓	✉	8man-demo.com	22 May, 01:23 PM
✓	🏠	8man-demo.local	07 May, 10:00 PM
✓	🖨	srv-8man	03 May, 06:15 PM
✓	📄	8man-demo.com (e6d421c0-debd-41f6-be4d-67072347...)	17 Dec, 08:00 AM
✓	🌐	https://8mandemo.sharepoint.com	01 Oct 2018, 07:43 PM
✓	🏢	Protected Networks GmbH	26 Sep 2018, 01:35 PM

**Recent changes (Last 30 days)**

**Risk assessment**

Severity	Title	Resources	Count
----------	-------	-----------	-------

1. Summary of your Active Directory.
2. Jump quickly to the Active Directory Analyze scenarios.

The screenshot shows the ARM Dashboard with the following environment statistics:

- Domains: 1
- Resources: 3
- Users: 1178
- Administrators: 14
- Computers: 6
- Groups: 1706

The 'Latest scans' section is highlighted with a red box and contains the following data:

Status	Type	Resource	Time
✓	✉	8man-demo.com	22 May, 01:23 PM
✓	🏠	8man-demo.local	07 May, 10:00 PM
✓	🖨	srv-8man	03 May, 06:15 PM
✓	📄	8man-demo.com (e6d421c0-debd-41f6-be4d-67072347...)	17 Dec, 08:00 AM
✓	🌐	https://8mandemo.sharepoint.com	01 Oct 2018, 07:43 PM
✓	🏢	Protected Networks GmbH	26 Sep 2018, 01:35 PM

ARM shows you the status of your configured scans of resources.

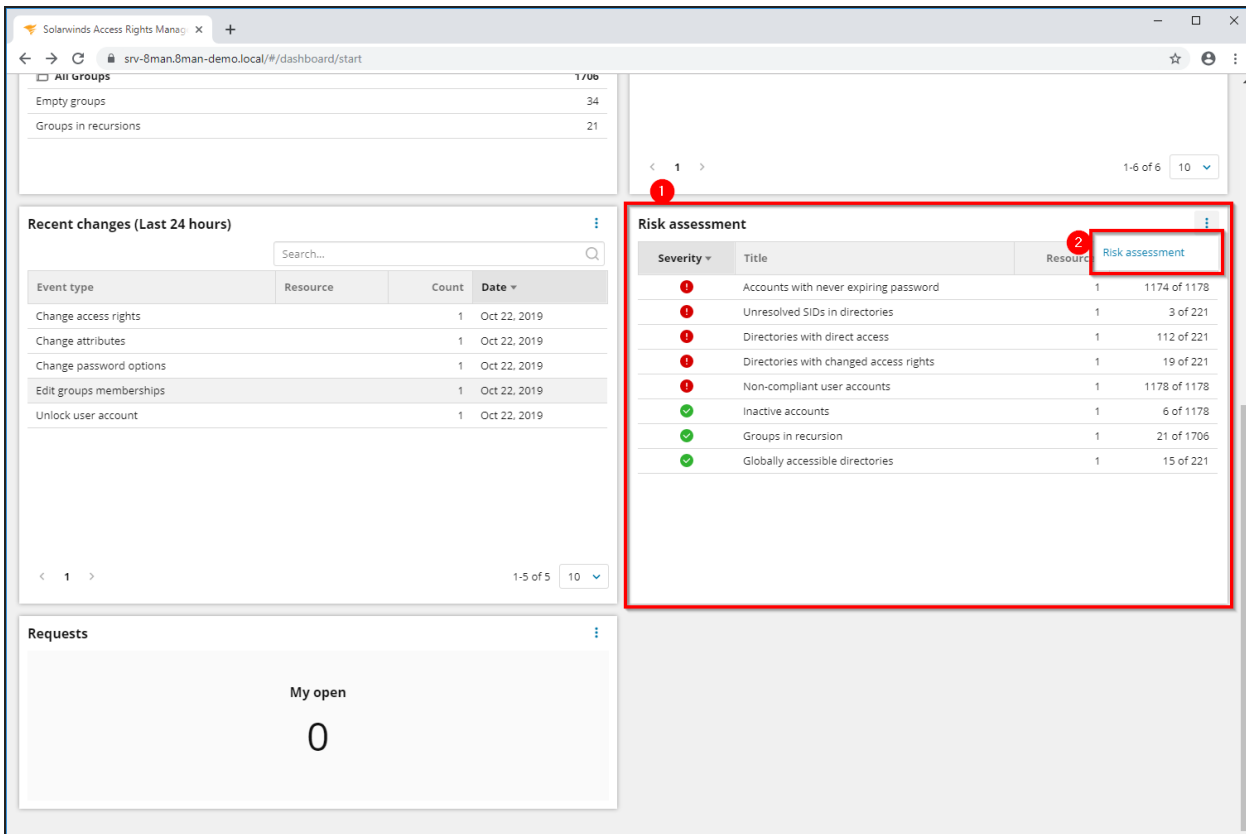
**i** Use the ARM configuration application to find detailed status messages of your scans or to adjust the scan configuration.



The screenshot displays the Solarwinds Access Rights Manager dashboard. The top navigation bar shows the browser address: `srv-8man.8man-demo.local/#/dashboard/start`. The main content area is divided into several sections:

- All Groups:** A summary table showing 1706 total groups, with 34 empty groups and 21 groups in recursions.
- Recent changes (Last 24 hours):** A table with columns for Event type, Resource, and Count. A search bar (3) is at the top. A widget menu (2) is open, showing options for timeframes: Last hour, Last 24 hours, Last 7 days, Last 14 days, and Last 30 days. A red circle (1) highlights the widget title. A specific event is listed: "Unlock user account" with a count of 1 and a date of "Oct 22, 2019".
- Risk assessment:** A table with columns for Severity, Title, Resources, and Count. It lists various security risks, such as "Accounts with never expiring password" (Severity 1, 1 resource, 1174 of 1178) and "Globally accessible directories" (Severity 0, 1 resource, 15 of 221).
- Requests:** A section titled "My open" showing a count of 0.

1. ARM shows you an overview of the latest changes.
2. Use the widget menu to set the time frame.
3. You can use the search to find events of special interest.



1. ARM shows you the risk assessment overview.
2. Jump to the Risk Assessment Dashboard for more details and becoming active on reducing risks.

The screenshot displays the Solarwinds Access Rights Management (ARM) dashboard. The top navigation bar shows the URL `srv-8man.8man-demo.local/#/dashboard/start`. The dashboard is divided into several sections:

- All Groups:** A table showing 1706 total groups, with 34 empty groups and 21 groups in recursions.
- Recent changes (Last 30 days):** A table with columns for Event type, Resource, Count, and Date. It lists five events from Oct 22, 2019, each with a count of 1.
- Risk assessment:** A table with columns for Severity, Title, Resources, and Count. It lists various security risks, some with red warning icons and others with green checkmarks.
- Requests:** A section titled "My open" showing a count of 0. A red box highlights a "Requests" link in the top right corner of this section.

Red circles with numbers 1 and 2 are placed on the page to indicate key actions: 1 points to the "Requests" link in the top right of the "Requests" section, and 2 points to the "Requests" link in the top right of the "My open" section.


1. ARM shows you your open requests.
2. Jump to the requests view to manage your open requests.

Determine permissions deviating from the department profile (compliance check) (web client)

### Background / Value

ARM sets new standards in the field of user provisioning: With the introduction of department profiles, department heads, together with the management and the compliance officer, define the scope of action of employees in the company.

If the employee receives additional permissions that deviate from the standard, a compliance monitor displays the deviating rights to a manager. In the form of bulk operations, the manager can harmonize the user accounts according to the profiles in his department.

 To be able to use the compliance functions, you must have created at least one [department profile](#).

### Related features

[Create a new department profile \(Administrator\)](#)

[Assign a department profile to users](#)

## Step-by-step process

Solarwinds Access Rights Manager

ARM Cockpit Recertification Analyze Requests Workflows Anthony Admin

ANALYSIS

ACCOUNTS 0 REQUESTS 100 RISKS ANALYSIS PROFILE

Search

**Categories**

- AD users
- AD computers
- AD groups
- Orders & tasks
- Compliance**
- Directories

**Scenarios**

- Non-compliant user accounts
- User accounts and department profiles**

Create a list of user accounts and assigned department profiles to create. You can narrow the list down to one profile.

1. Select "Analysis".
2. Click "Compliance".
3. Click on "User Accounts and Department Profiles".

Solarwinds Access Rights Manager

ARM Cockpit Recertification Analyze Requests Workflows Anthony Admin

Access Rights Manager

NEW ANALYZE SESSION

All Scenarios

### User accounts and department profiles

Create a list of user accounts and assigned department profiles to create. You can narrow the list down to one profile.

**Start calculation for your scenario!**

1 Domain name  8man-demo.local

2 Restrict to selected profile < Without restriction >

3  Include accounts without profile assignment

1. Determine which domains are included in your analysis.
2. Choose a departmental profile or all ("without restriction").
3. Optional: Activate this option if you also want to list users with no assigned department profile.
4. Start the scenario.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main content area is titled "Configuration" and shows a table of user accounts under the heading "USER ACCOUNTS AND DEPARTMENT PROFILES (2)". The table has columns for "Domain name", "Type", "Name", "Compliant", "Accepted deviations", and "Unaccepted deviations".

Domain name	Type	Name	Compliant	Accepted deviations	Unaccepted deviations
8man-demo.local		Elyne Koop (8man-demo\Elyne Koop)	Compliant (green circle)		
8man-demo.local		Nick Sandheaver (8man-demo\Nick Sandheaver)	Non-compliant (red circle with X)		The property 'Department' has the wrong value ' ' instead of 'sales'

Red boxes and numbers 1, 2, and 3 are overlaid on the table to highlight the "Compliant", "Accepted deviations", and "Unaccepted deviations" columns respectively.

On the right side of the interface, there is a "Reports" panel with various actions such as "Direct Excel export", "Create Report", "Reset password", "Unlock user account", "Pause user", "Change personal information", "Deactivate user", "Remove group membership", "Add group membership", "Assign profile", "Delete user account (permane...)", "Execute script", "Soft delete user account", "Change password options", "Accept deviations", "Remove department profile", and "Correct profile deviations".

1. ARM shows you which user accounts are compliant.
2. User accounts are compliant when exceptions have been accepted by a controller.
3. User accounts are non-compliant if there are "unaccepted deviations".

## Active Directory

Active Directory is the leading system for administrators in Windows networks. ARM focuses on the analysis of users and groups. ARM can also handle multi-domain environments, regardless of the level of trust.

### Visualize nested group structures

#### **Background/Value**

The central component of every Active Directory (AD) is the group concept. Administrators use groups to assign access rights and resources to individual users or user groups. This results in nesting: For example, the group "Marketing" gives access rights to the corresponding file server directories of the department. At the same time, however, the group is also a member (i.e. nested) of the group "Access Wlan 4th floor". The ARM AD Graph shows the nesting structure in your Active Directory and helps you to recognize grown structures and adjust structural errors.

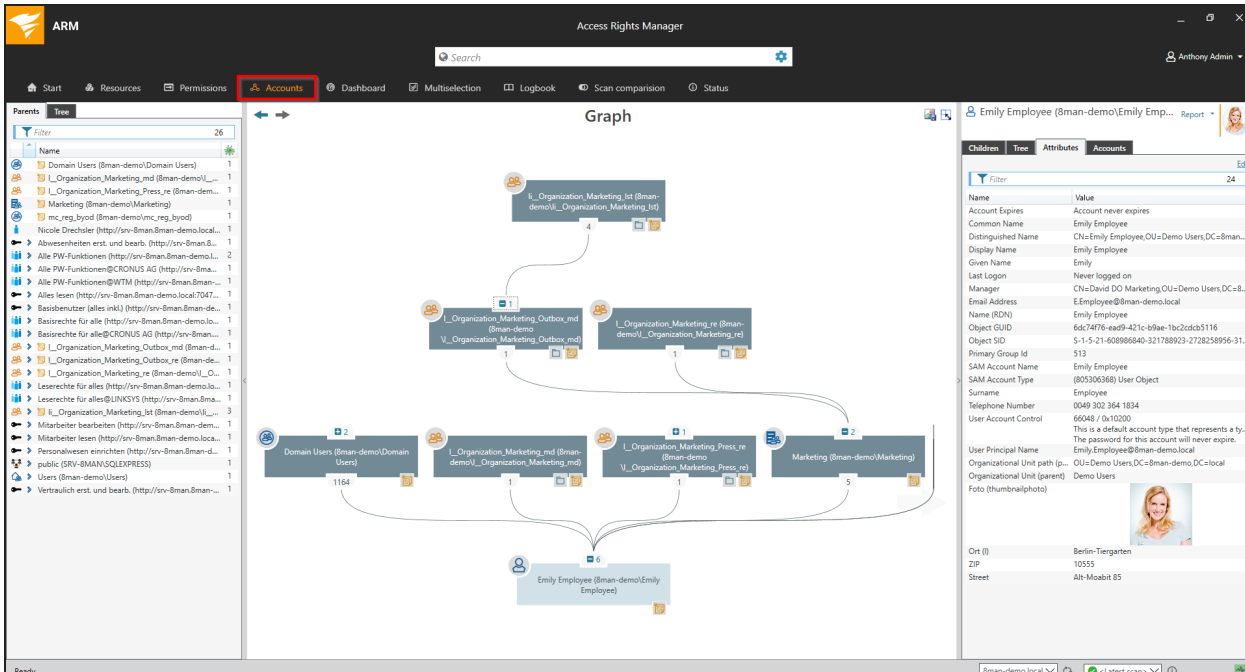
#### **Related features**

[Identify the depth of nesting in your AD](#)

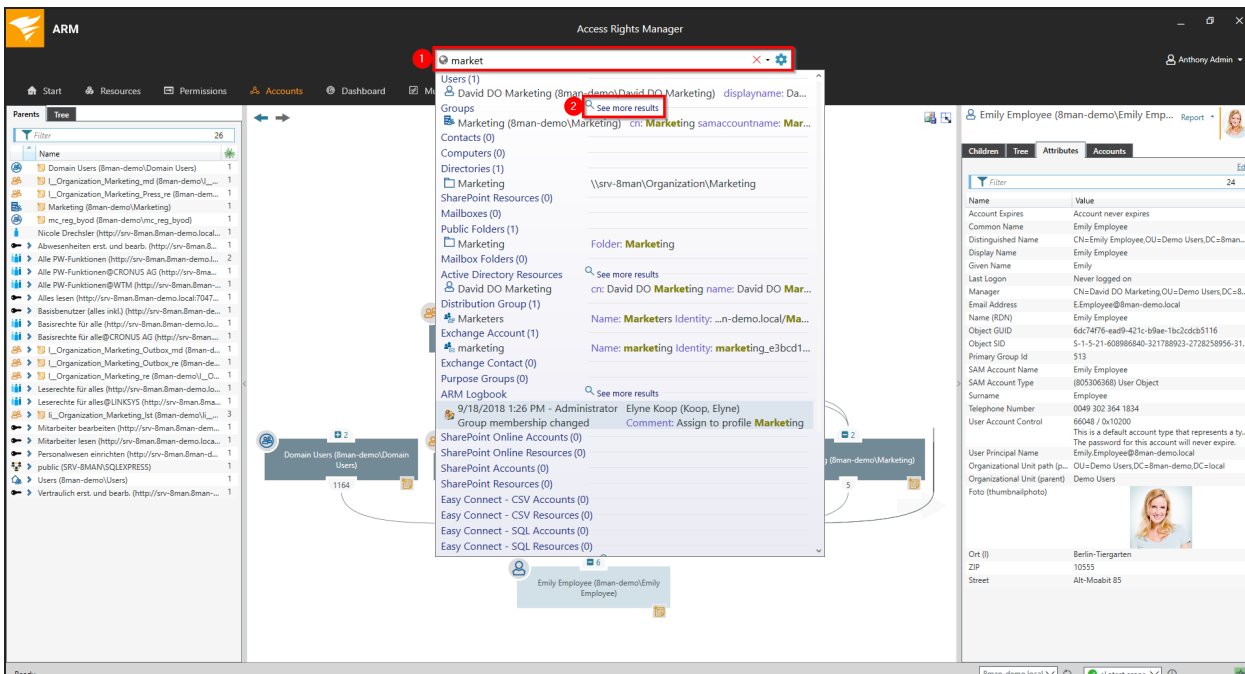
[Identify groups in recursion](#)



## Step-by-step process



Switch to Accounts to see the AD Graph view.



1. Find the AD group by entering its name into the search field. For example: "Marketing". Select the desired result from the Groups section of the drop-down.
2. If you can't find your resource click on "See more results".

1. The "Marketing" group is the focus of the following analysis.
2. Above the group you see other groups in the AD graph that the "Marketing Group is a member in, the so-called "parents". All "parent" groups, both direct and indirect, are listed on the left-hand side. Indirect "parents" are indicated by a blue arrow.
3. On the right hand side you can see the name of the group listed at the top. Underneath it you can see a list of all "children", both direct and indirect, of the group.
4. You can open and close the individual branches on the AD graph by clicking on the icon. The number listed indicates the number of direct "parents" or "children".

# Identify overprivileged users based on Kerberos token size

## Background/Value

The size of a Kerberos token is a good indicator for identifying users with excessive access rights. The more group memberships a user has, the bigger their Kerberos token. Even if a group membership does not automatically grant privileges, it is worthwhile analyzing the listed users.

In addition, there is a risk that users with too many group memberships will no longer be able to login.

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The 'Dashboard' tab is selected in the navigation menu. The main content area displays a list of users and groups. A red box highlights the 'Top 5 Kerberos Tokens [Bytes]' section, which lists five users with their token sizes:

User	Token Size (Bytes)
User96 (@man-demo\User96)	3144
User70 (@man-demo\User70)	3024
User2 (@man-demo\User2)	2992
User39 (@man-demo\User39)	2984
User38 (@man-demo\User38)	2960

1. Select "Dashboard".
2. Double-click on the user in the list "Top 5 Kerberos Tokens".

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. On the left, a 'Parents' list shows 82 entries, with a red box highlighting the list and a red circle labeled '2'. The main 'Graph' view shows a user node 'User96 (Bman-demo\User96)' with a red box and a red circle labeled '1'. Arrows point from various group nodes to the user node, indicating membership. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The user 'Anthony Admin' is logged in.

1. ARM automatically focuses on the selected user in the AD graph view.
2. All "parents", meaning groups in which the selected user is a direct or indirect member of, are shown on the left-hand side. We recommend using this flat list for users with an extremely large number of group memberships.

## Identify the depth of group nesting

### Background/Value

An AD that has grown over years often contains a large number of nested levels. The ARM dashboard shows nested groups up to level 10. According to Microsoft best-practice your AD should contain no more than 3 or 4 levels. ARM allows you to identify these critical areas of your AD and restructure them with minimal effort. In order to achieve low levels of nesting and maintain a well organized AD structure we recommend creating more groups with specific functionalities.

### Related features

[Reduce multiple groups to one group](#)

### Step-by-step process

The screenshot shows the ARM dashboard with the following data points:

- Reporting - Active Directory:**
  - Inactive accounts
  - Local accounts
  - Users and groups (Kerberos, Last logon)
- Reporting - File server:**
  - All 'Authenticated users' permissions: 3
  - All 'Everyone' permissions: 1
  - All users with direct access: 16
  - Directories without administrative owners: 49
  - Unresolved SIDs
- Depth of nested groups:**

Depth	Count
1	1564
2	11
3	3
4	2
5	1
6	1
7	1
- Users and other accounts:**
  - Users: 1169
  - Users (disabled): 3
  - Administrators: 6
  - Administrators (disabled): 0
- Groups:**
  - All Groups: 1660
  - Groups with members (w/o recursions): 1585
  - Empty groups: 41
  - Groups in recursions: 34
  - The largest group (Domain Users (8man-demo\Domain Users)): 1168
  - Built-in security groups: 29
  - Global security groups: 548
  - Universal security groups: 513
  - Local security groups: 557
  - Global distribution groups: 0
  - Universal distribution groups: 13
  - Local distribution groups: 0
- OU / Contacts / More:**
  - Computers: 5
  - Computers (disabled): 0
  - Contacts: 3
  - Foreign users: 0
  - Organizational Units: 45
- Top 5 Kerberos Tokens [Bytes]:**
  - User96 (8man-demo\User96): 3144
  - User70 (8man-demo\User70): 3024
  - User2 (8man-demo\User2): 2992
  - User20 (8man-demo\User20): 2084

1. Select the Dashboard.
2. Click on any of the nesting levels.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a settings icon. The main navigation tabs are Start, Resources, Permissions, Accounts, Dashboard, Multiselection (highlighted with a red box and callout 1), Logbook, Scan comparison, and Status. The 'Multiselection' tab is active, showing a list of groups filtered by 'Depth 4'. The filter bar (callout 2) shows 'All groups with depth of nesting [Depth 4]' and a 'Deactivate scenario' button. The tree view on the right (callout 3) displays a hierarchical structure of sales regions and users, including 'Sales (8man-demo\Sales)', 'Sales Africa', 'Sales Asia', 'Sales Australia', 'Sales Europe', 'Sales France', 'Sales Germany', 'Sales Eastern Germany', 'Sales Northern Germany', 'Sales Southern Germany', 'Sales Western Germany', 'Sales Great Britain', 'Sales Italy', 'Sales Netherlands', 'Sales Poland', 'Sales North America', and 'Sales South America'.

1. ARM automatically shows the Multiselection
2. In this scenario ARM automatically filters the groups by the selected nested level.
3. You can see the nested levels in the tree graph on the right hand side.

## View members of different groups in one list

### Background/Value

With the "Multiselection" you can select several groups and get an overview of all their members.

### Related features

[Reduce several groups to one group](#)


### Step by step process

1. Click Multiselection.
2. Filter by groups.
3. Use the filter to narrow your selection.
4. Select the desired groups.
5. You can see an overview of all "children" of all selected groups. ARM also indicates how often users are in the selected groups, e.g. Poul Rosing three times (arrow).

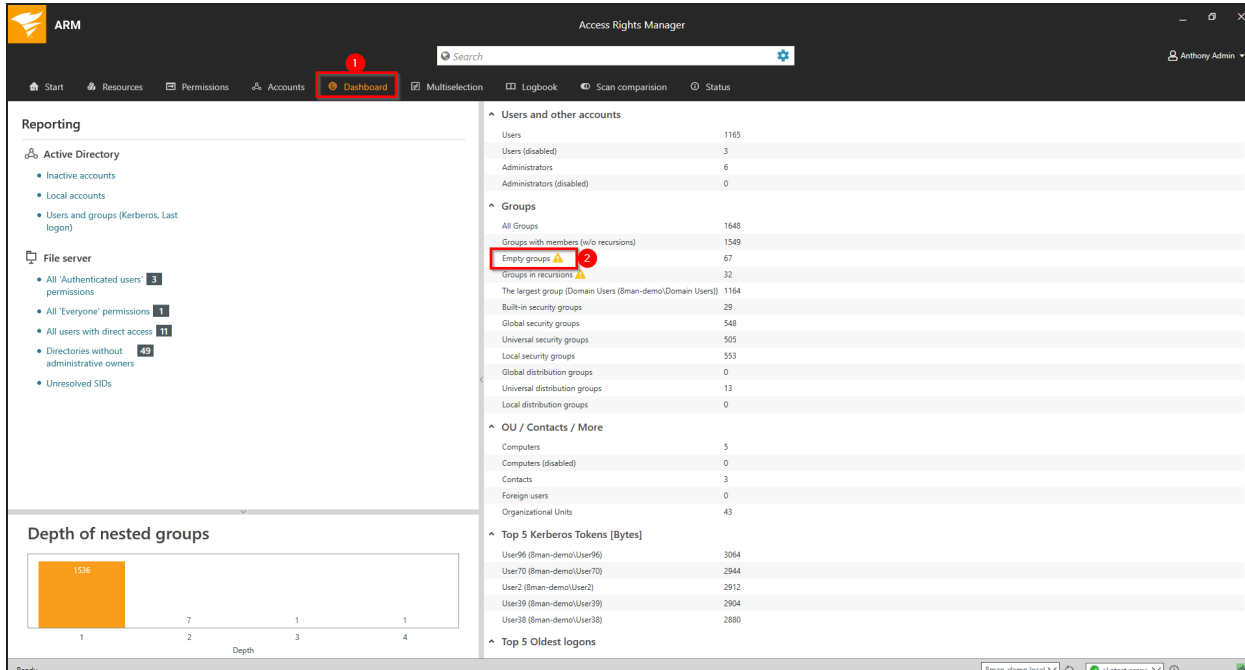
## Identify empty groups

### Background/Value



Over time empty groups often accumulate in an AD structure. These empty groups reduce performance and diminish transparency. We recommend deleting these groups.

 Groups without members can be system groups. You should not delete them.

### Step-by-step process



The screenshot shows the Access Rights Manager (ARM) interface. The 'Dashboard' tab is selected in the top navigation bar. On the left, the 'Reporting' section is visible, with 'Active Directory' and 'File server' categories. The main content area displays a list of groups and accounts. The 'Groups' section is expanded, showing a table with the following data:

Group Name	Count
All Groups	1648
Groups with members (w/o recursions)	1549
Empty groups 	67
Groups in recursions 	32
The largest group (Domain Users (Bman-demo\Domain Users))	1164
Built-in security groups	29
Global security groups	548
Universal security groups	505
Local security groups	553
Global distribution groups	0
Universal distribution groups	13
Local distribution groups	0

The 'Empty groups' row is highlighted with a red box and a red '2' next to it. The 'Dashboard' tab in the top navigation bar is also highlighted with a red box and a red '1' next to it.

1. Select the Dashboard.
2. Double-click "Empty Groups".



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The 'Multiselection' tab is highlighted. Below the navigation bar, the 'Empty groups' scenario is active, and a list of groups is displayed. A red box highlights the 'Multiselection' tab, and a red circle highlights the 'Empty groups' scenario. The right pane shows details for the 'Cafeteria' group, including its name, common name, distinguished name, group type, and other attributes.


Name	Value
Common Name	Cafeteria
Distinguished Name	CN=Cafeteria,OU=Function Groups,OU=Demo Groups...
Group Type	Local group
Name (RDN)	Cafeteria
Object GUID	daaee87f-16e9-419a-9171-b5aaee61d157a
Object SID	S-1-5-21-608986840-321788923-2728258956-3182
SAM Account Name	Cafeteria
SAM Account Type	(538670912) Alias Object
Organizational Unit path (pare...	OU=Function Groups,OU=Demo Groups,DC=Bman-de...
Organizational Unit (parent)	Function Groups

1. ARM automatically switches to "Multiselection".
2. The "Empty groups" scenario is active. All the listed groups are empty.

## Identify recursive groups

### Background/Value

Groups can be members of other groups. Active Directory allows "children" to become "parents" within their own family tree. If the nested group structure loops in a circular way group membership assignments become ineffective and nonsensical. Through these recursions or circular nested groups every user who is a member of any of the recursive groups is granted all of the access rights of all of the groups. The consequence is a confusing mess of excessive access rights. ARM automatically identifies all recursions in your system. We highly recommend removing the recursion by breaking the chain of circular group memberships.

 Administer only with ARM and recursions can no longer happen because ARM does not allow the creation of recursions.

### Related features

The deeper your group structure the more likely you are to have circular nested group structures. We therefore recommend keeping an eye on the number of [nested group levels](#).

[Identify groups in recursion](#) (web client)

Break the circle by [managing group memberships](#) (rich client) or [removing group memberships](#) (web client).

### Step-by-step process

ARM Access Rights Manager

Search

Anthony Admin

Start Resources Permissions Accounts **Dashboard** Multiselection Logbook Scan comparison Status

### Reporting

#### Active Directory

- Inactive accounts
- Local accounts
- Users and groups (Kerberos, Last logon)

#### File server

- All 'Authenticated users' permissions **3**
- All 'Everyone' permissions **1**
- All users with direct access **16**
- Directories without administrative owners **49**
- Unresolved SIDs

#### Depth of nested groups

Depth	Count
1	1564
2	11
3	3
4	2
5	1
6	1
7	1

#### Users and other accounts

Users	1169
Users (disabled)	3
Administrators	6
Administrators (disabled)	0

#### Groups

All Groups	1660
Groups with members (w/o recursions)	1585
Empty groups	41
<b>Groups in recursions</b>	<b>34</b>
The largest group (Domain Users (8man-demo\Domain Users))	1168
Built-in security groups	29
Global security groups	548
Universal security groups	513
Local security groups	557
Global distribution groups	0
Universal distribution groups	13
Local distribution groups	0

#### OU / Contacts / More

Computers	5
Computers (disabled)	0
Contacts	3
Foreign users	0
Organizational Units	45

#### Top 5 Kerberos Tokens [Bytes]

User96 (8man-demo\User96)	3144
User70 (8man-demo\User70)	3024
User2 (8man-demo\User2)	2992
User20 (8man-demo\User20)	2084
User10 (8man-demo\User10)	2084

Ready | 8man-demo.local | <Latest scan>

1. Select the dashboard.
2. Double-click on "groups in recursions".

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection' (highlighted with a red box and number 1), 'Logbook', 'Scan comparison', and 'Status'. The main content area is titled 'Multiselection' (highlighted with a red box and number 2) and shows a list of 'Groups in recursions' (34 total). The list includes various recursive group entries, with one entry highlighted by a red box and number 3. The right-hand pane shows the 'Children' tab (highlighted with a red box and number 4) for the selected group, displaying a list of children groups, with one entry highlighted by a red box and number 5.

1. ARM automatically switches to "Multiselection".
2. The scenario "groups in recursions" is active. ARM lists all groups included in the recursion.
3. Click on a Group.
4. ARM lists all users and groups in the selected recursion.
5. Double-click on a group.


The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts' (highlighted with a red box and a red '1'), 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The main area is titled 'Graph' and shows a hierarchical structure of recursive groups. Three parent nodes at the top are 'Recursive Group 2 Ring 4 (8man-demo \Recursive Group 2 Ring 4)', 'Recursive Group 3 Ring 4 (8man-demo \Recursive Group 3 Ring 4)', and 'Recursive Group 4 Ring 4 (8man-demo \Recursive Group 4 Ring 4)'. These three nodes all point to a single child node at the bottom: 'Recursive Group 1 Ring 4 (8man-demo \Recursive Group 1 Ring 4)'. An orange line connects the three parent nodes to the child node, indicating a recursion. A red arrow with a '2' points to this orange line. The left sidebar shows a 'Parents' tree with a filter set to '4' and a list of recursive groups. The right sidebar shows a 'Children' tree with a filter set to '4' and a list of recursive groups. The bottom status bar shows 'Ready', '8man-demo.local', and '<Latest scan>'.

1. ARM switches to the account view. You can see an example of a recursion.
2. The recursion is indicated by the orange line.

## Identify recursive groups (web client)

### Background/Value

Groups can be members of other groups. Active Directory allows "children" to become "parents" within their own family tree. If the nested group structure loops in a circular way group membership assignments become ineffective and nonsensical. Through these recursions or circular nested groups every user who is a member of any of the recursive groups is granted all of the access rights of all of the groups. The consequence is a confusing mess of excessive access rights. ARM automatically identifies all recursions in your system. We highly recommend removing the recursion by breaking the chain of circular group memberships.

 Administer only with ARM and recursions can no longer happen because ARM does not allow the creation of recursions.

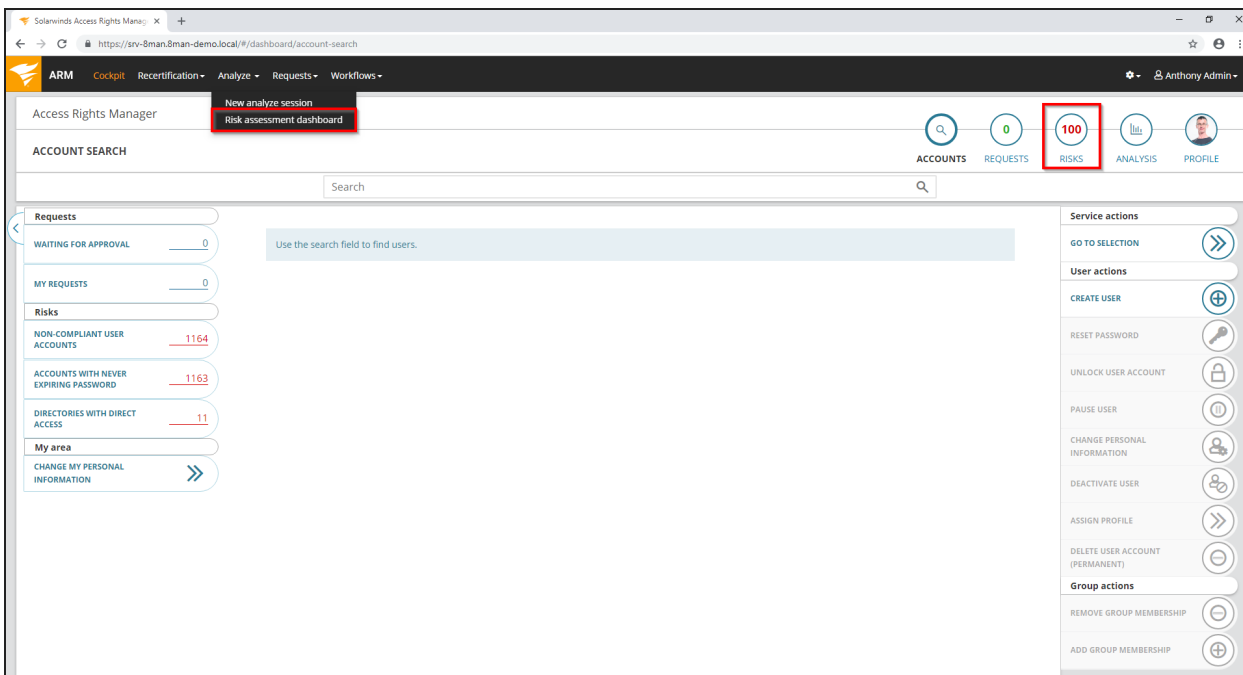
### Related features

The deeper your group structure the more likely you are to have circular nested group structures. Therefore, keep an eye on the [nesting depth](#) of your groups.

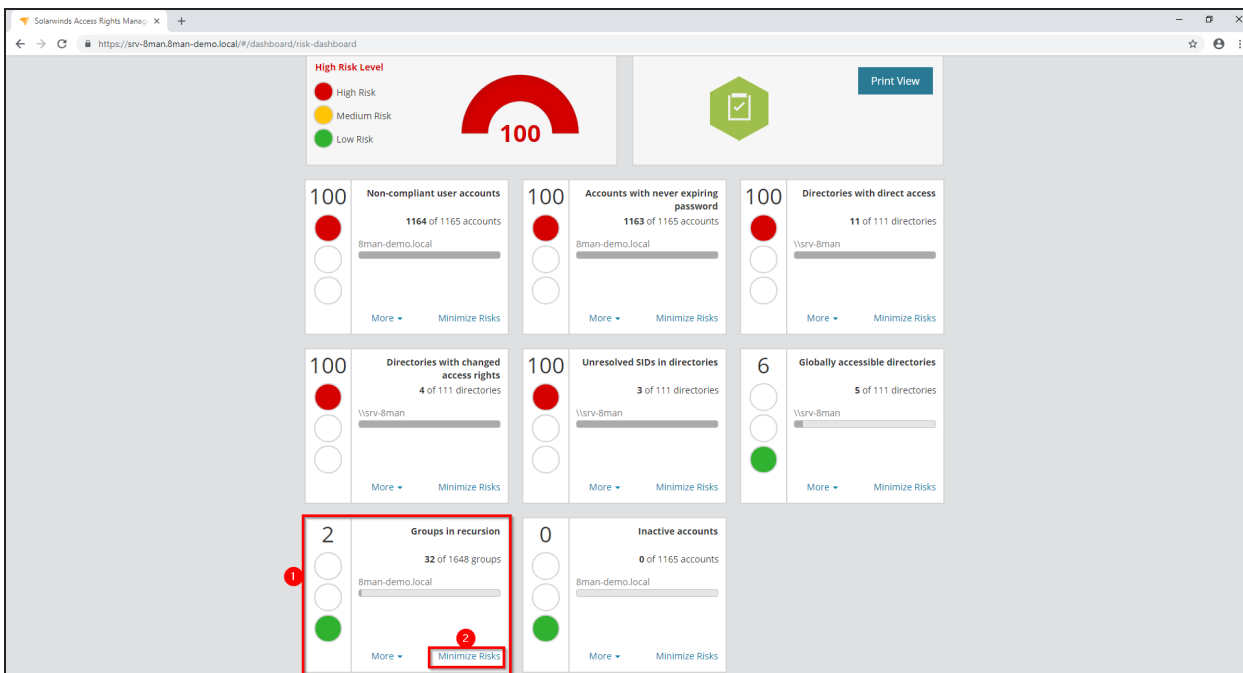
[Identify recursive groups](#) (rich client)

Break the circle by [managing group memberships](#) (rich client) or [removing group memberships](#) (web client).

### Step-by-step process



Go to the Risk Assessment Dashboard.



1. ARM shows a rating for the risk factor "Groups in recursion".
2. Click "Minimize risks".

The tiles are sorted by risk level and may therefore be located in different places.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main heading is "Access Rights Manager". Below it, a red box labeled "1" highlights the text "GROUPS IN RECURSION (32)".

The interface is divided into several sections:

- Configuration:** Shows "Selected resources: 8man-demo.local". A red box labeled "2" highlights the "Domain name" field, which contains "8man-demo.local". A red box labeled "3" highlights the "Type. Name" dropdown menu.
- Table:** A table with columns "Type", "Name", and "Requested Action". The table lists 32 items under the domain "8man-demo.local". The first few rows are:

Type	Name	Requested Action
Recursive Group 1 Ring 1	Recursive Group 1 Ring 1 (8man-demo/Recursive Group 1 Ring 1)	
Recursive Group 1 Ring 2	Recursive Group 1 Ring 2 (8man-demo/Recursive Group 1 Ring 2)	
Recursive Group 1 Ring 3	Recursive Group 1 Ring 3 (8man-demo/Recursive Group 1 Ring 3)	
Recursive Group 1 Ring 4	Recursive Group 1 Ring 4 (8man-demo/Recursive Group 1 Ring 4)	
Recursive Group 10 Ring 1	Recursive Group 10 Ring 1 (8man-demo/Recursive Group 10 Ring 1)	
Recursive Group 10 Ring 2	Recursive Group 10 Ring 2 (8man-demo/Recursive Group 10 Ring 2)	
Recursive Group 10 Ring 3	Recursive Group 10 Ring 3 (8man-demo/Recursive Group 10 Ring 3)	
Recursive Group 2 Ring 2	Recursive Group 2 Ring 2 (8man-demo/Recursive Group 2 Ring 2)	
Recursive Group 2 Ring 1	Recursive Group 2 Ring 1 (8man-demo/Recursive Group 2 Ring 1)	
Recursive Group 2 Ring 3	Recursive Group 2 Ring 3 (8man-demo/Recursive Group 2 Ring 3)	
Recursive Group 2 Ring 4	Recursive Group 2 Ring 4 (8man-demo/Recursive Group 2 Ring 4)	
Recursive Group 3 Ring 1	Recursive Group 3 Ring 1 (8man-demo/Recursive Group 3 Ring 1)	
Recursive Group 3 Ring 2	Recursive Group 3 Ring 2 (8man-demo/Recursive Group 3 Ring 2)	
Recursive Group 3 Ring 3	Recursive Group 3 Ring 3 (8man-demo/Recursive Group 3 Ring 3)	
Recursive Group 4 Ring 1	Recursive Group 4 Ring 1 (8man-demo/Recursive Group 4 Ring 1)	
Recursive Group 4 Ring 2	Recursive Group 4 Ring 2 (8man-demo/Recursive Group 4 Ring 2)	
Recursive Group 4 Ring 3	Recursive Group 4 Ring 3 (8man-demo/Recursive Group 4 Ring 3)	
Recursive Group 5 Ring 1	Recursive Group 5 Ring 1 (8man-demo/Recursive Group 5 Ring 1)	
Recursive Group 5 Ring 2	Recursive Group 5 Ring 2 (8man-demo/Recursive Group 5 Ring 2)	
- Reports:** A sidebar on the right with a red box labeled "4" around the "Direct Excel export" button and a red box labeled "5" around the "Create Report" button. Other buttons include "Execute script" and "Delete group account (permanent)".

1. ARM lists all groups in recursion.
2. Use sorting, filtering and grouping to analyze the data.
3. Select the rows to display in the grid and in the reports.
4. Export the data into Excel.
5. Create a report in PDF- or CSV-format. Save the report or email it.



# Identify users with never expiring passwords

## Background/Value

One key security requirement within any organization is that passwords are changed regularly. ARM scans your domain for user accounts where this requirement has not been activated. You can view this information in our reports for "Users" and "Groups".

## Related features

[Reset passwords](#)

[Change password options](#)

[Identify users with never expiring password](#) (web client)

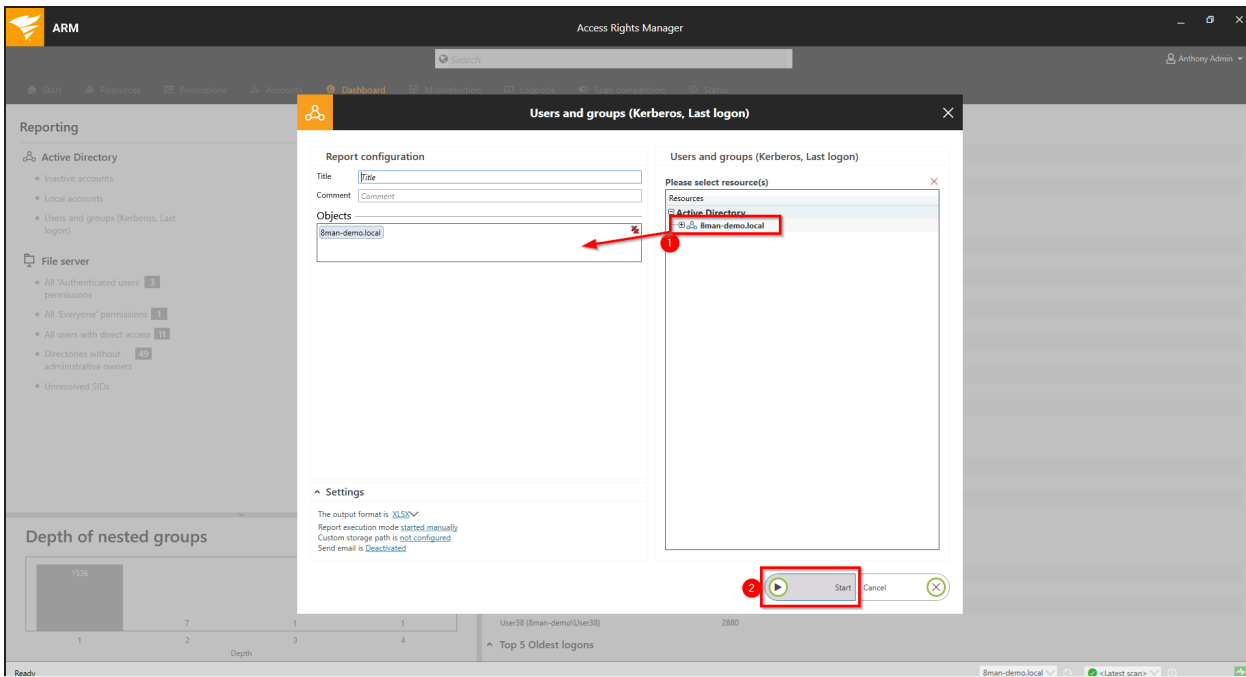
[Change password options in bulk](#) (web client)

## Step-by-step process

The screenshot shows the ARM web interface. The 'Dashboard' menu item is highlighted with a red box and a '1'. In the 'Reporting' section, the 'Users and groups (Kerberos, Last login)' link is highlighted with a red box and a '2'. The main content area displays a list of users and groups with counts.

Category	Count
Users	1165
Users (disabled)	3
Administrators	6
Administrators (disabled)	0
All Groups	1648
Groups with members (w/o recursions)	1549
Empty groups	67
Groups in recursions	32
The largest group (Domain Users (Bman-demo\Domain Users))	1164
Built-in security groups	29
Global security groups	548
Universal security groups	505
Local security groups	553
Global distribution groups	0
Universal distribution groups	13
Local distribution groups	0
Computers	5
Computers (disabled)	0
Contacts	3
Foreign users	0
Organizational Units	43
User96 (Bman-demo\User96)	3064
User70 (Bman-demo\User70)	2944
User2 (Bman-demo\User2)	2912
User39 (Bman-demo\User39)	2904
User38 (Bman-demo\User38)	2880

1. Select the "Dashboard".
2. Click on "Users" and "Groups" in the "Reports" area.



1. Select the range of the report via drag & drop.
2. Run the report.

1	Report of all users for	B	C	D	E	F	G	H	I	J	K	L
2	Display Name	Disabled	Account Expires	PWD don't expire	Last Logon	Last Logon Timestamp	Type	Direct Membership	Indirect Membership	Total Membership	Domain Local Membership	Universal Foreign Membership
3	Abhey O'Flaherty (Bman-demo\Abhey O'Flaherty)	No	Account never expires	Yes	N/A	N/A	User	1	0	0	0	0
4	Abdul-Hadi Deeb (Bman-demo\Abdul-Hadi Deeb)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
5	Adalynno Contreras (Bman-demo\Adalynno Contreras)	No	Account never expires	Yes	N/A	N/A	User	1	3	5	1	0
6	Adam Adromanager (Bman-demo\Adam Adromanager)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
7	Adauge Buchi (Bman-demo\Adauge Buchi)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
8	Adolote Bonenfant (Bman-demo\Adolote Bonenfant)	No	Account never expires	Yes	N/A	N/A	User	2	2	4	2	0
9	Adriano Faldress (Bman-demo\Adriano Faldress)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
10	Agatha Melo (Bman-demo\Agatha Melo)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
11	Ahmad Khoury (Bman-demo\Ahmad Khoury)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
12	Al Tag (Bman-demo\Al Tag)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
13	Aida Suresen (Bman-demo\Aida Suresen)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
14	Aidan Hodel (Bman-demo\Aidan Hodel)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
15	Aisha Syron (Bman-demo\Aisha Syron)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
16	Akubesse Chiemela (Bman-demo\Akubesse Chiemela)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
17	Akuma Chagazem (Bman-demo\Akuma Chagazem)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
18	Alberte Krogh (Bman-demo\Alberte Krogh)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
19	Alberte Lorenzen (Bman-demo\Alberte Lorenzen)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
20	Albina Sorica (Bman-demo\Albina Sorica)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
21	Albino Russo (Bman-demo\Albino Russo)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
22	Aleisha Henderson (Bman-demo\Aleisha Henderson)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
23	Alena Gadjidjari (Bman-demo\Alena Gadjidjari)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
24	Alex Tomaszewski (Bman-demo\Alex Tomaszewski)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
25	Alessandro Verdison (Bman-demo\Alessandro Verdison)	No	Account never expires	Yes	N/A	N/A	User	2	1	3	1	0
26	Alexandre Rodlan (Bman-demo\Alexandre Rodlan)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
27	All Arroyo (Bman-demo\All Arroyo)	No	Account never expires	Yes	N/A	N/A	User	3	1	4	1	0
28	Allie Williamson (Bman-demo\Allie Williamson)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
29	Allons Grabowski (Bman-demo\Allons Grabowski)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
30	Alicia Denshy (Bman-demo\Alicia Denshy)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
31	Alicia Gill (Bman-demo\Alicia Gill)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
32	Alicia Kauppla (Bman-demo\Alicia Kauppla)	No	Account never expires	Yes	N/A	N/A	User	2	4	6	4	0
33	Aline Vallin (Bman-demo\Aline Vallin)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
34	Alice Fekkesa (Bman-demo\Alice Fekkesa)	No	Account never expires	Yes	N/A	N/A	User	1	2	0	0	0
35	Aloisa Bianchi (Bman-demo\Aloisa Bianchi)	No	Account never expires	Yes	N/A	N/A	User	2	4	6	4	0
36	Alvaro Roland (Bman-demo\Alvaro Roland)	No	Account never expires	Yes	N/A	N/A	User	2	1	3	1	0
37	Amabile Caldera (Bman-demo\Amabile Caldera)	No	Account never expires	Yes	N/A	N/A	User	2	4	6	2	0
38	Amanda Christiansen (Bman-demo\Amanda Christiansen)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
39	Amanda Sundegaard (Bman-demo\Amanda Sundegaard)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
40	Amantoni Merviel (Bman-demo\Amantoni Merviel)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
41	Amarsachew Omubiko (Bman-demo\Amarsachew Omubiko)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
42	Ambessa Eftehai (Bman-demo\Ambessa Eftehai)	No	Account never expires	Yes	N/A	N/A	User	2	2	4	2	0
43	Amira Castiglione (Bman-demo\Amira Castiglione)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
44	Andreas Franklin (Bman-demo\Andreas Franklin)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
45	Anna Romani (Bman-demo\Anna Romani)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
46	An Fan (Bman-demo\An Fan)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
47	Andelko Nikolic (Bman-demo\Andelko Nikolic)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0

Open the report in your spreadsheet application.

1. Select the tab "User".
2. Filter the column "PWD don't expire" by positive entries.

We recommend setting your security requirements so that passwords must be changed at least every 90 days.

## Identify users with never expiring password (web client)

### Background / Value

One key security requirement within any organization is that passwords are changed regularly. Use the scenario to find accounts where this requirement has not been activated. View this information in the web interface and create reports.

### Related features

[Reset passwords](#) (rich client)

[Change password options](#) (rich client)

### Step-by-step process

The screenshot shows the Solarwinds Access Rights Manager (ARM) web interface. The top navigation bar includes 'ARM', 'Cockpit', 'Recertification', 'Analyze', 'Requests', and 'Workflows'. The 'RISKS' tab is highlighted in the top navigation bar, and the 'Risk assessment dashboard' link is highlighted in the top left menu. The main content area shows a search field and a list of risk categories on the left sidebar, including 'ACCOUNTS WITH NEVER EXPIRING PASSWORD' with a count of 1163.

Go to the Risk Assessment Dashboard.

Access Rights Manager

RISK ASSESSMENT DASHBOARD

ACCOUNTS REQUESTS RISKS ANALYSIS PROFILE

High Risk Level

- High Risk
- Medium Risk
- Low Risk

100

100 Accounts with never expiring password  
1167 of 1169 accounts  
8man-demo.local  
More Minimize Risks

100 Directories with direct access  
17 of 111 directories  
\\srv-8man  
More Minimize Risks

100 Directories with changed access rights  
4 of 111 directories  
\\srv-8man  
More Minimize Risks

100 Unresolved SIDs in directories  
3 of 111 directories  
\\srv-8man  
More Minimize Risks

6 Globally accessible directories  
5 of 111 directories  
\\srv-8man  
More Minimize Risks

1. ARM shows a rating for the risk factor "Accounts with never expiring password".
2. Click on "Minimize risks".

**i** The tiles are sorted by risk level and may therefore be located in different places.

The screenshot displays the Solarwinds Access Rights Manager (ARM) interface. The main heading is "Access Rights Manager". A red box labeled "1" highlights the text "ACCOUNTS WITH NEVER EXPIRING PASSWORD (1000)". Below this, a "Configuration" section shows "Selected resources: 8man-demo.local". A red box labeled "2" highlights the "Domain name" dropdown menu. A red box labeled "3" highlights the "Type. Name" dropdown menu. A table lists accounts with columns for "Type", "Name", and "Requested Action". A red box labeled "4" highlights the "Direct Excel export" button in the "Reports" sidebar. A red box labeled "5" highlights the "Create Report" button in the "Reports" sidebar.

Type	Name	Requested Action
Domain name: 8man-demo.local (1,000 items)		
David DO Finance (8man-demo\David DO Finance)		
David DO HR (8man-demo\David DO HR)		
David DO Manager (8man-demo\David DO Manager)		
David DO Marketing (8man-demo\David DO Marketing)		
David DO Sales (8man-demo\David DO Sales)		
Emily Employee (8man-demo\Emily Employee)		
Helena Helpdesk (8man-demo\Helena Helpdesk)		
Henry HR (8man-demo\Henry HR)		
Maggy Manager (8man-demo\Maggy Manager)		
Sebastian SAP (8man-demo\Sebastian SAP)		
Anthony Admin (8man-demo\Anthony Admin)		
Antoine Admin (8man-demo\Antoine Admin)		
Anton Admin (8man-demo\Anton Admin)		
DefaultAccount (8man-demo\DefaultAccount)		
sa-8man (8man-demo\sa-8man)		
Guest (8man-demo\Guest)		
User0 (8man-demo\User0)		
User1 (8man-demo\User1)		

1. ARM lists all accounts with never expiring password.
2. Use sorting, filtering and grouping to analyze the data.
3. Select the rows to display in the grid and in the reports.
4. Export the data into Excel.
5. Create a report in PDF- or CSV-format. Save the report or email it.

## Identify inactive accounts (web client)

### Background / Value

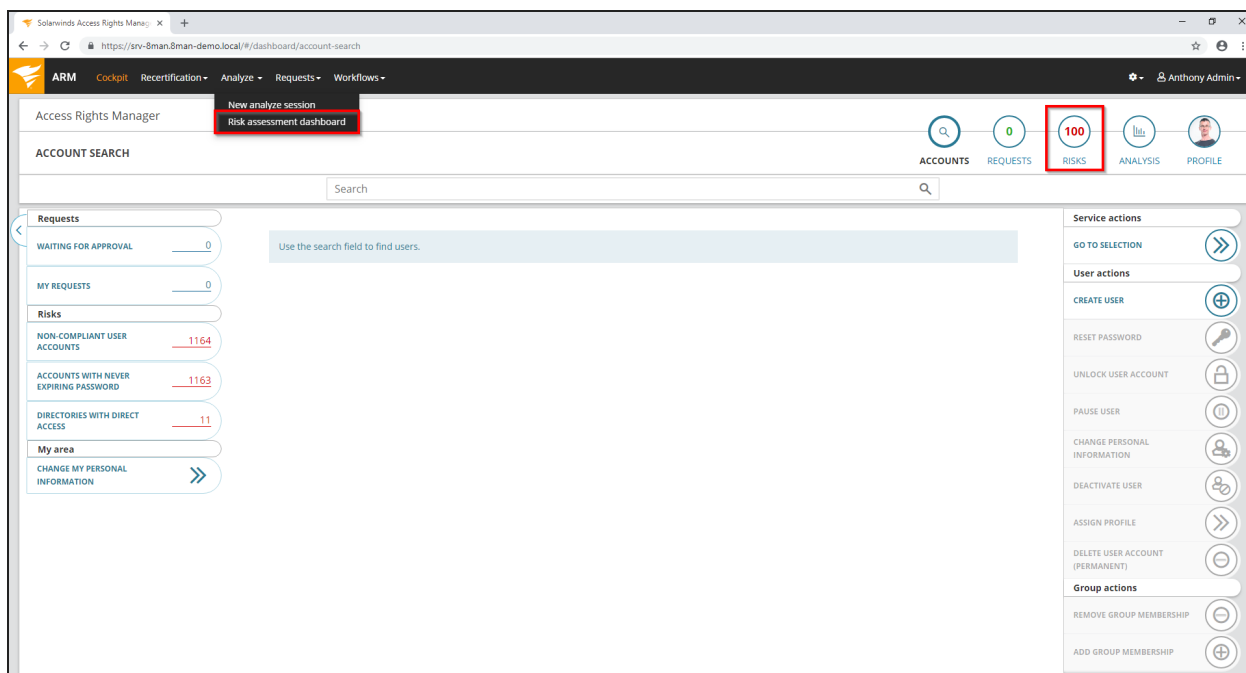
Inactive accounts can be used for data theft and manipulation without being detected. Since most inactive accounts are remnants of past employees, they are often a symptom of a communication problem between HR and IT. ARM displays all inactive accounts in Active Directory with a last logon older than 30 days. Remove or deactivate accounts that are no longer needed.

### Related features

[Report: Inactive accounts](#)

[Deactivate accounts in bulk](#) (web client)

### Step-by-step process

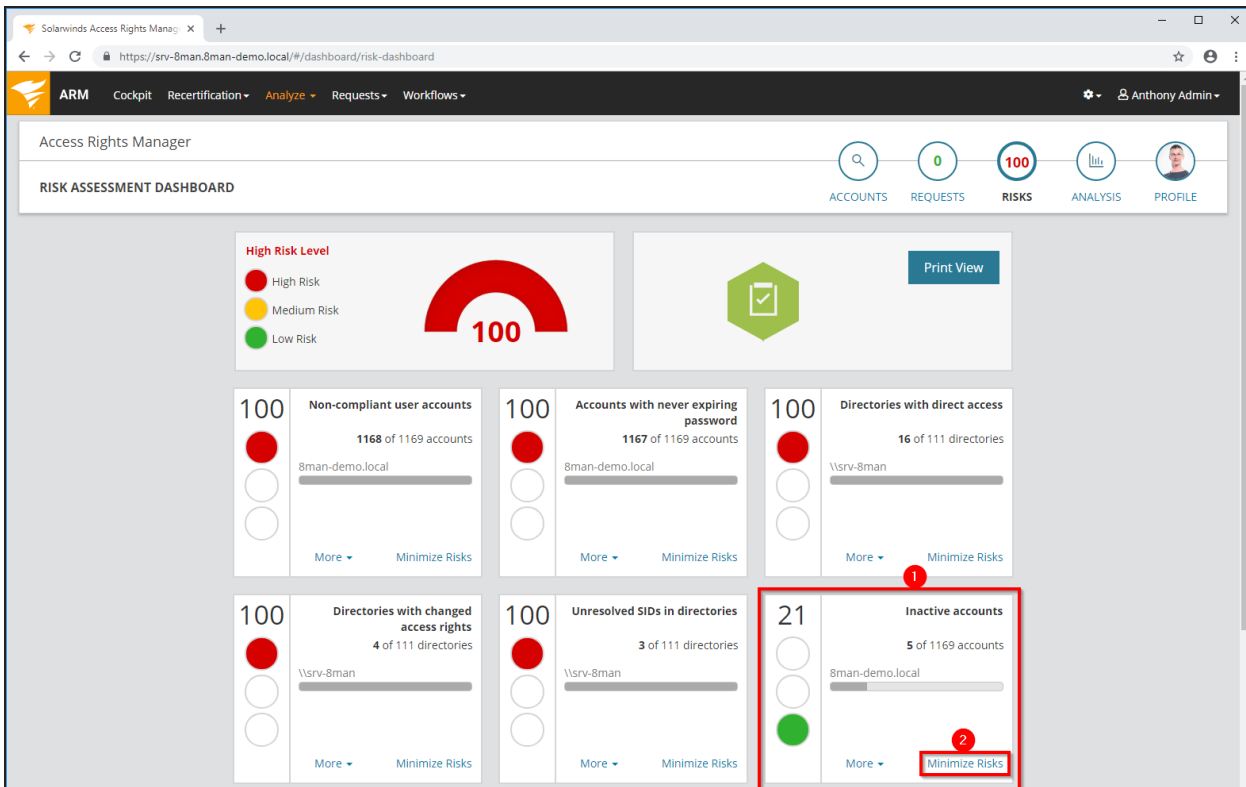


The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'ACCOUNTS', 'REQUESTS', 'RISKS', 'ANALYSIS', and 'PROFILE'. The 'RISKS' button is highlighted with a red box. Below the navigation bar, there is a search field and a 'New analyze session' button. The main content area displays a 'Risks' section with the following data:

Risk Category	Count
NON-COMPLIANT USER ACCOUNTS	1164
ACCOUNTS WITH NEVER EXPIRING PASSWORD	1163
DIRECTORIES WITH DIRECT ACCESS	11

The right sidebar contains 'Service actions' and 'User actions' sections. The 'User actions' section includes: CREATE USER, RESET PASSWORD, UNLOCK USER ACCOUNT, PAUSE USER, CHANGE PERSONAL INFORMATION, DEACTIVATE USER, ASSIGN PROFILE, and DELETE USER ACCOUNT (PERMANENT). The 'Group actions' section includes: REMOVE GROUP MEMBERSHIP and ADD GROUP MEMBERSHIP.

Go to the Risk Assessment Dashboard.



1. ARM shows a rating for the risk factor "Inactive accounts".
2. Click "Minimize risks".

The tiles are sorted by risk level and may therefore be located in different places.



The screenshot displays the Solarwinds Access Rights Manager (ARM) interface. The main heading is "Access Rights Manager" with a sub-heading "INACTIVE ACCOUNTS (5)". Below this is the "Configuration" section, which includes a "Selected resources: 8man-demo.local" and a "Domain name" dropdown menu. A table lists the inactive accounts with columns for "Type", "Name", "Last logon", "Days since last logon", "Is activated", and "Requested Action". The table contains five rows of data. To the right of the table is a "Reports" section with buttons for "Direct Excel export" and "Create Report".

Type	Name	Last logon	Days since last logon	Is activated	Requested Action
	Administrator (8man-demo\Administrator)	12/13/2018	77	true	
	Anthony Admin (8man-demo\Anthony Admin)	12/17/2018	73	true	
	Antoine Admin (8man-demo\Antoine Admin)	12/17/2018	73	true	
	Anton Admin (8man-demo\Anton Admin)	12/17/2018	73	true	
	sa-8man (8man-demo\sa-8man)	12/13/2018	77	true	

1. ARM lists all inactive accounts.
2. Use sorting, filtering and grouping to analyze the data.
3. Select the rows to display in the grid and in the reports.
4. Export the data into Excel.
5. Create a report in PDF- or CSV-format. Save the report or email it.

## Identify expiring user accounts

### Background / Value

User accounts for external employees or interns should only exist temporarily. ARM allows you to maintain an overview of your temporary user accounts. You can view this information in our report for "Users and Groups".

### Step-by-step process

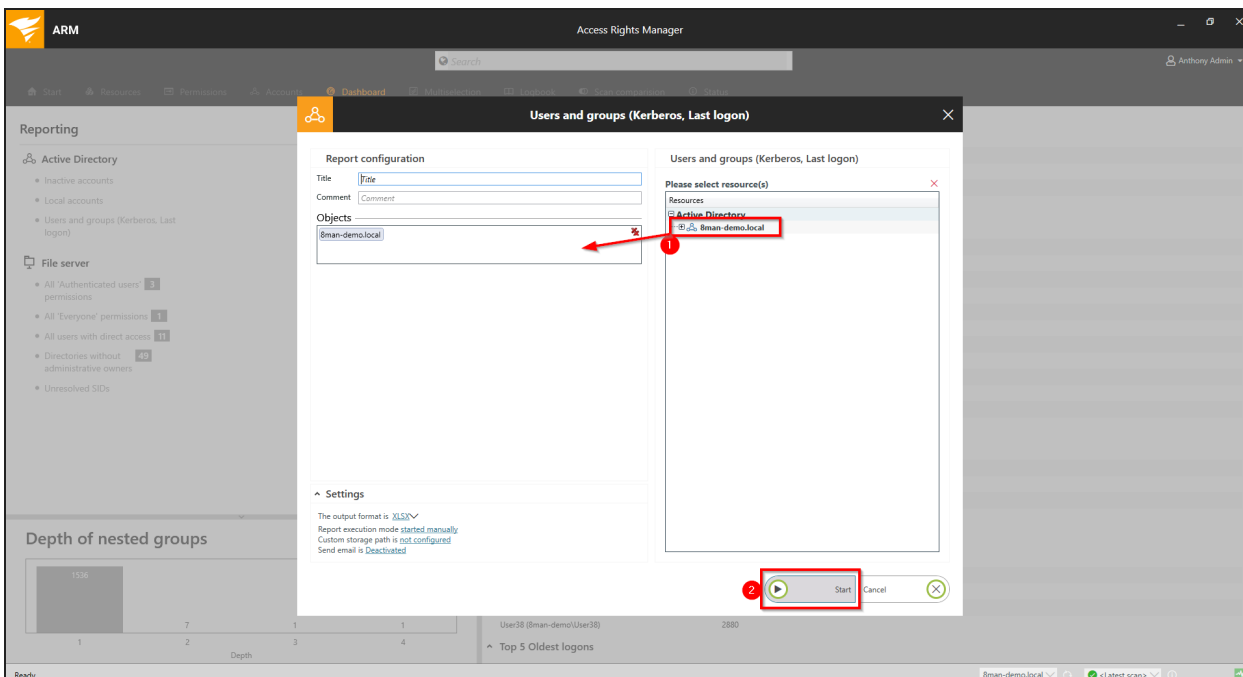
The screenshot shows the ARM interface with the following data:

Category	Item	Count
Users and other accounts	Users	1165
	Users (disabled)	3
	Administrators	6
	Administrators (disabled)	0
Groups	All Groups	1648
	Groups with members (w/o recursions)	1549
	Empty groups	67
	Groups in recursions	32
	The largest group (Domain Users (Bman-demo\Domain Users))	1164
	Built-in security groups	29
	Global security groups	548
	Universal security groups	505
	Local security groups	553
	Global distribution groups	0
OU / Contacts / More	Computers	5
	Computers (disabled)	0
	Contacts	3
Top 5 Kerberos Tokens [Bytes]	User96 (Bman-demo\User96)	3064
	User70 (Bman-demo\User70)	2944
	User2 (Bman-demo\User2)	2912
	User39 (Bman-demo\User39)	2904
	User38 (Bman-demo\User38)	2880

The 'Depth of nested groups' bar chart shows the following distribution:

Depth	Count
1	1536
2	7
3	1
4	1

1. Select the "Dashboard".
2. Click on "Users" and "Groups" in the "Reports" area.



1. Select the range of the report via drag & drop.
2. Run the report.

Report über alle Benutzer für	8man-demo.local	Account Expires	PWD don't expire	Last Logon	Last Logon Timestamp	Type	Direct Memberships	Indirect Memb
27	Azubi_Andy (8man-demo\Andy Azubi)	31.01.2017 00:00:00	ja	N/A	07.03.2016 10:44:09	Benutzer	9	
153	John Doe (8man-demo\John.Doe)	31.12.2016 00:00:00	ja	N/A	N/A	Benutzer	1	

Open the report in your spreadsheet application.

1. Select the tab "User".
2. Filter the column "Account expires" by positive entries.

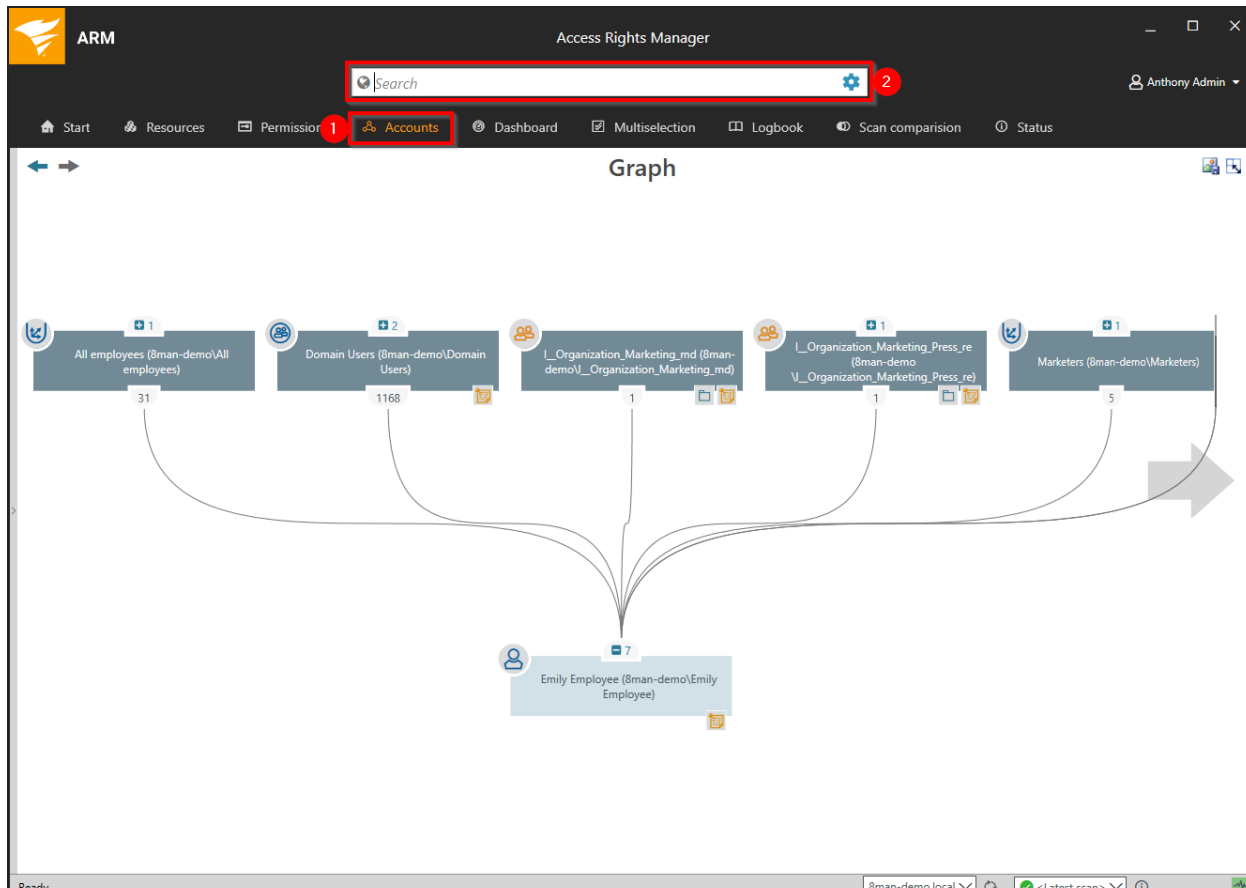
We recommend checking with your HR department if any of these accounts are still needed.

## Identify the most recent actions on an account

### Background / Value

User accounts and AD groups have their own history. This is why it makes sense to review the previously performed actions and changes. ARM shows you a quick view of most recent activities or you can jump directly into the log book to receive a full report.

### Step-by-step process



1. Select "Accounts".
2. Search for the desired user or group.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. At the top, the title bar reads "ARM" and "Access Rights Manager". Below the title bar is a search bar and a user profile for "Anthony Admin". The main navigation bar includes "Start", "Resources", "Permissions", "Accounts", "Dashboard", "Multiselection", "Logbook", "Scan comparison", and "Status".

The central area is titled "Graph" and shows a network of accounts. Five account nodes are visible: "All employees (8man-demo)\All employees)" with 31 members, "Domain Users (8man-demo)\Domain Users)" with 1168 members, "L\_Organization\_Marketing\_md (8man-demo)\L\_Organization\_Marketing\_md)" with 1 member, "L\_Organization\_Marketing\_Press\_re (8man-demo)\L\_Organization\_Marketing\_Press\_re)" with 1 member, and "Marketers (8man-demo)\Marketers)" with 5 members. Red boxes highlight note icons on the "Domain Users" and "L\_Organization\_Marketing\_md" nodes. A large grey arrow points from the logbook comment to the right.

A logbook comment is displayed in the foreground, titled "4 comments" and dated "10/16/2018 11:47 AM, Author: anthony admin". The comment text reads: "anthony admin: Demo ARM Changes: Rights changes in folder '\\srv-8man\Organization\Marketing\Outbox' in chronological order: - New group created: 'L\_Organization\_Marketing\_Outbox\_re' (DomainLocal) - Added access rights entry: L\_Organization\_Marketing\_Outbox\_re: Read & execute - Member Domain Users (8man-demo)\Domain Users) added to group L\_Organization\_Marketing\_Outbox... - Member li\_Organization\_Marketing\_lst added to list group L\_Organization\_Marketing\_Outbox\_re. Used credential: Active Directory changes: 8MAN-DEMO\sa-8man, File System changes: 8MAN-DEMO\sa-8man". Below this, another comment is partially visible, dated "9/7/2018 10:43 AM, Author: Administrator (8man-demo)\Administrator)", mentioning "AD Logga for 8man-demo.local" and "Change was made by Administrator (8man-demo)\Administrator): member 'sa-8man (8man-demo\sa-8man)' added to 'Domain Users'".

The note icon indicates that activities were recorded in the ARM log book. You can hover over the icon to see an overview of the latest activities related to the account.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes the ARM logo, a search bar, and the user name 'Anthony Admin'. The main area is titled 'Graph' and shows a network of accounts and resources. The accounts are represented by blue boxes with icons and labels: 'All employees (8man-demo\All employees)' with 31 members, 'Domain Users (8man-demo\Domain Users)' with 1168 members, 'I\_Organization\_Marketing\_md demo\\_Organization\_Marketi' with 1 member, and 'Marketers (8man-demo\Marketers)' with 5 members. A specific account, 'Emily Employee (8man-demo\Emily Employee)', is highlighted in blue. A context menu is open over this account, listing various actions such as 'Select account', 'Show in Resources View...', 'Report: Where has the user/group access?', 'Change group memberships...', 'Create new user or group', 'Unlock user', 'Deactivate account', 'Change password options', 'Reset user password', 'Soft delete user account', 'Delete account', 'Edit attributes', 'Move object', 'Enable mailbox', 'Add note', 'Open Logbook' (highlighted with a red box), 'Create alert', and 'Copy as path'. The bottom status bar shows 'Ready', the local host '8man-demo.local', and the latest scan status '<Latest scan >'. A large grey arrow points from the 'Open Logbook' option in the context menu towards the right side of the page.

Right-click on the desired object and select "Open Logbook" to view all recorded information.

ARM Access Rights Manager

Search

Anthony Admin

Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparison Status

Overview of the Logbook

Comments for: Emily Employee (8man-demo\Emily Employee)

Filter 8

Only mine

Date & Time	Author
10/16/2018 12:01 PM	anthony admin
10/16/2018 11:58 AM	anthony admin
10/16/2018 11:36 AM	anthony admin
10/16/2018 11:34 AM	anthony admin
9/26/2018 12:10 PM	sa-8man (8man-demo\sa-8man)
9/26/2018 12:10 PM	Administrator
9/20/2018 1:24 PM	Emily Employee
9/20/2018 1:24 PM	sa-8man (8man-demo\sa-8man)

Permission changed

anthony admin: Demo

ARM Changes:

Rights changes in folder "\\\svr-8man\Organization\Marketing\Press\Videos" in chronological order:

- Access rights entry of [Emily Employee \(8man-demo\Emily Employee\)](#) removed (Modify).
- New group created: "[L\\_Organization\\_Marketing\\_Press\\_Videos\\_md](#)" (DomainLocal)
- Added access rights entry: [L\\_Organization\\_Marketing\\_Press\\_Videos\\_md](#): Modify
- Member [Ludvig Karlsson \(8man-demo\Ludvig Karlsson\)](#) added to group [L\\_Organization\\_Marketing\\_Press\\_Videos\\_md](#)
- New group created: "[li\\_Organization\\_Marketing\\_Press\\_1st](#)" (DomainLocal)
- List right access added for [\\svr-8man\Organization\Marketing\Press\](#) on [li\\_Organization\\_Marketing\\_Press\\_1st](#)
- Member [li\\_Organization\\_Marketing\\_Press\\_1st](#) added to list group [L\\_Organization\\_Marketing\\_Press\\_Videos\\_md](#)
- Member [li\\_Organization\\_Marketing\\_1st](#) added to list group [L\\_Organization\\_Marketing\\_Press\\_Videos\\_md](#)
- Member [David DO Marketing \(8man-demo\David DO Marketing\)](#) added to group [L\\_Organization\\_Marketing\\_Press\\_Videos\\_md](#)
- Member [li\\_Organization\\_Marketing\\_Press\\_1st](#) added to list group [L\\_Organization\\_Marketing\\_Press\\_Videos\\_md](#)
- Member [li\\_Organization\\_Marketing\\_1st](#) added to list group [L\\_Organization\\_Marketing\\_Press\\_Videos\\_md](#)

Used credential:  
Active Directory changes: 8MAN-DEMO\sa-8man, File System changes: 8MAN-DEMO\sa-8man

Demo

Add Close

8man-demo.local <Latest scan>

Review past activities related to a user account.

1. You can enter an additional comment at any time into the logbook.
2. The footprint icon indicates that these actions were recorded by AD Logga.

## File server

ARM shows all access rights to file server directories. Many helpful views allow a deep analysis of the permission situation and its occurrence. In addition ARM identifies and highlights security risks such as multiple or direct access rights, corrupted inheritance and unresolved SIDs.

### Identify globally accessible directories (web client)

#### Background / Value

If "Everyone accounts" are used for the assignment of access rights, (almost) everyone has access to the connected resources. The consequence is an excessive assignment of access rights and a high probability for unauthorized access. These go against the principle of least privilege and should therefore not be used. Before deleting permissions you should assign specific groups to the appropriate resources.

"Everyone accounts" are:

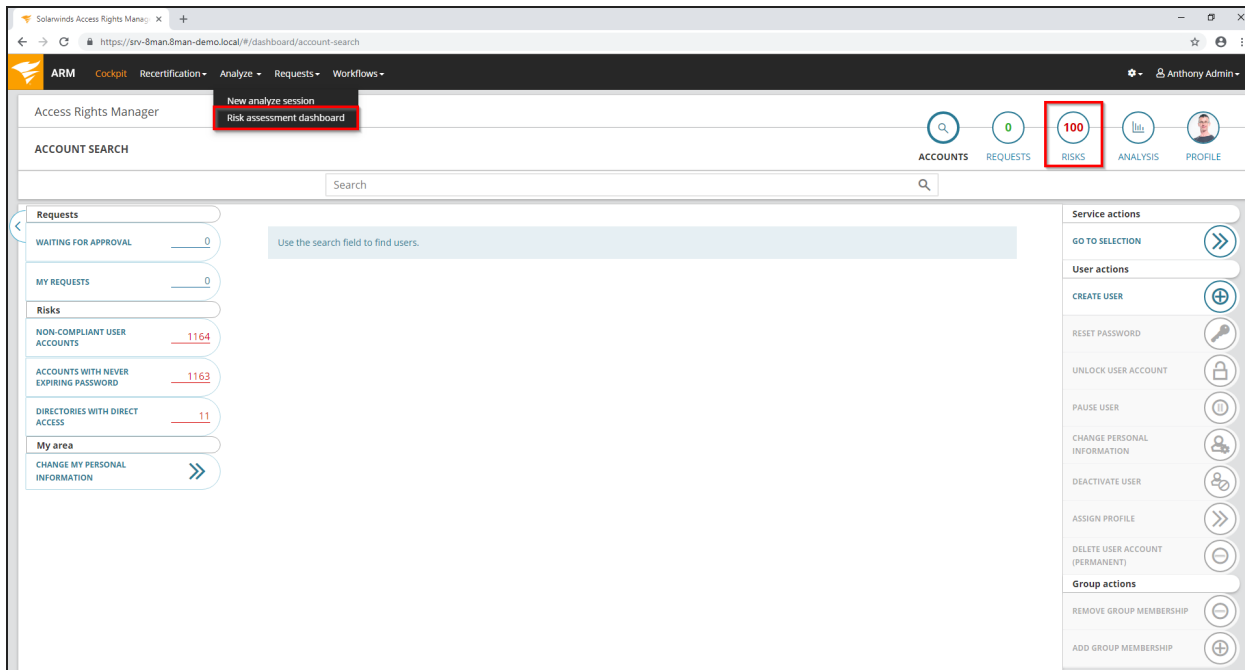
- Everyone
- Authenticated Users
- Domain-Users

#### Related features

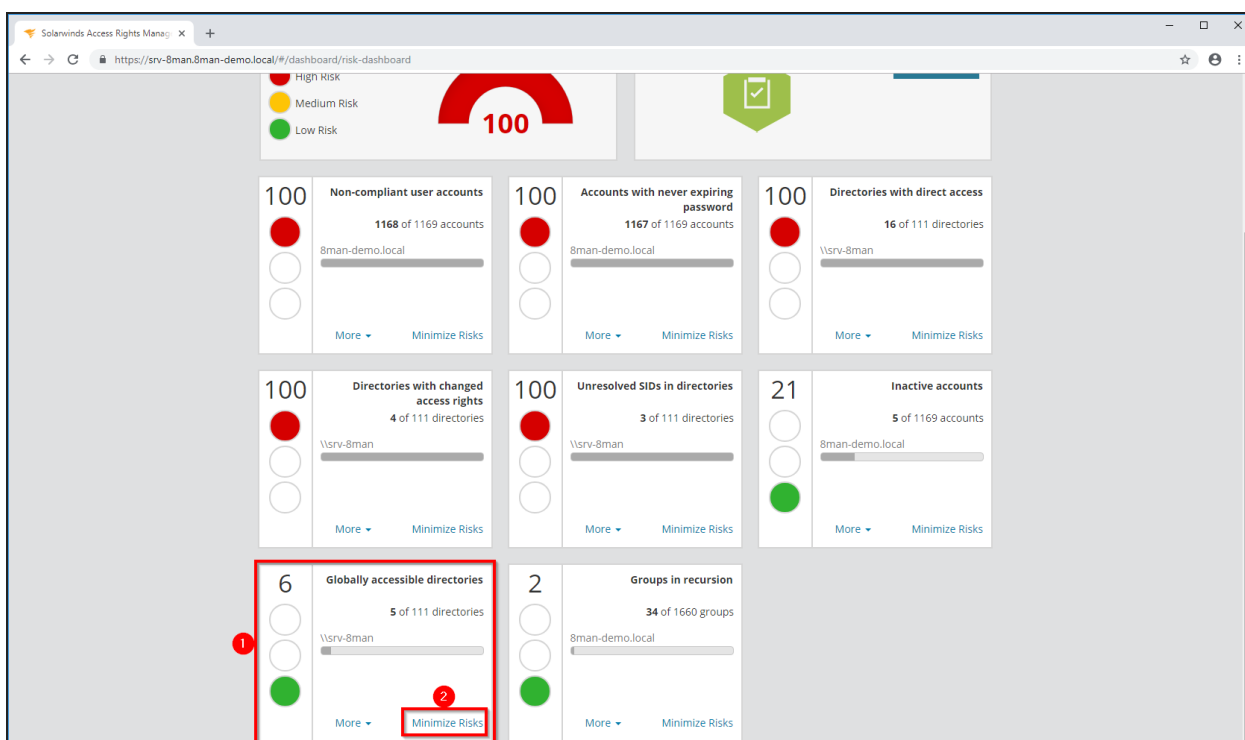
[Remove permissions from globally accessible directories in bulk](#)



## Step-by-step process



Go to the Risk Assessment Dashboard.



1. ARM shows a rating for the risk factor "Globally accessible directories".
2. Click "Minimize risks".

**i** The tiles are sorted by risk level and may therefore be located in different places.

The screenshot displays the Solarwinds Access Rights Manager (ARM) interface. At the top, the navigation bar includes 'ARM', 'Cockpit', 'Recertification', 'Analyze', 'Requests', and 'Workflows'. The main content area is titled 'Access Rights Manager' and shows a section for 'GLOBALLY ACCESSIBLE DIRECTORIES (5)'. Below this, there is a 'Configuration' section with a dropdown menu showing '3 columns selected'. The main table has the following data:

Path	Account	Rights	Requested Action
<input type="checkbox"/> \\srv-8man\Templates	Domain Users	Full control	
<input type="checkbox"/> \\srv-8man\Templates\Instructions	Authenticated Users	Full control	
<input type="checkbox"/> \\srv-8man\Templates\Power Point Templates	Everyone	Full control	
<input type="checkbox"/> \\srv-8man\Templates\Signatures	Authenticated Users	Full control	
<input type="checkbox"/> \\srv-8man\Templates\Word Templates	Authenticated Users	Full control	

On the right side, there are 'Reports' buttons: 'Direct Excel export' and 'Create Report'. Below these are 'Available Actions' buttons: 'Execute script' and 'Remove ACE'.

1. ARM lists all globally accessible directories.
2. Use sorting, filtering and grouping to analyze the data.
3. Select the rows to display in the grid and in the reports.
4. Export the data into Excel.
5. Create a report in PDF- or CSV-format. Save the report or email it.

## Identify corrupted inheritance

### Background / Value

Broken ACLs (Access Control Lists) interfere with the NTFS inheritance on the fileserver. The consequences: The subdirectory does not get the correctly inherited permissions, even though the inheritance is enabled.

ARM shows you broken ACLs in a report.

### Related features

[Remove corrupted inheritance](#)

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The 'Resources' tab is selected, and the 'File server' category is expanded. The file server '\\srv-8man' is selected. The 'Report' button is clicked, and the 'Report on paths with different access rights' report is generated. The report content is displayed on the right side of the interface.

1. Select "Resources".

2. Select the desired file server.

3. Click on "Report".

4. Select "report on all sub-directories with different access rights".

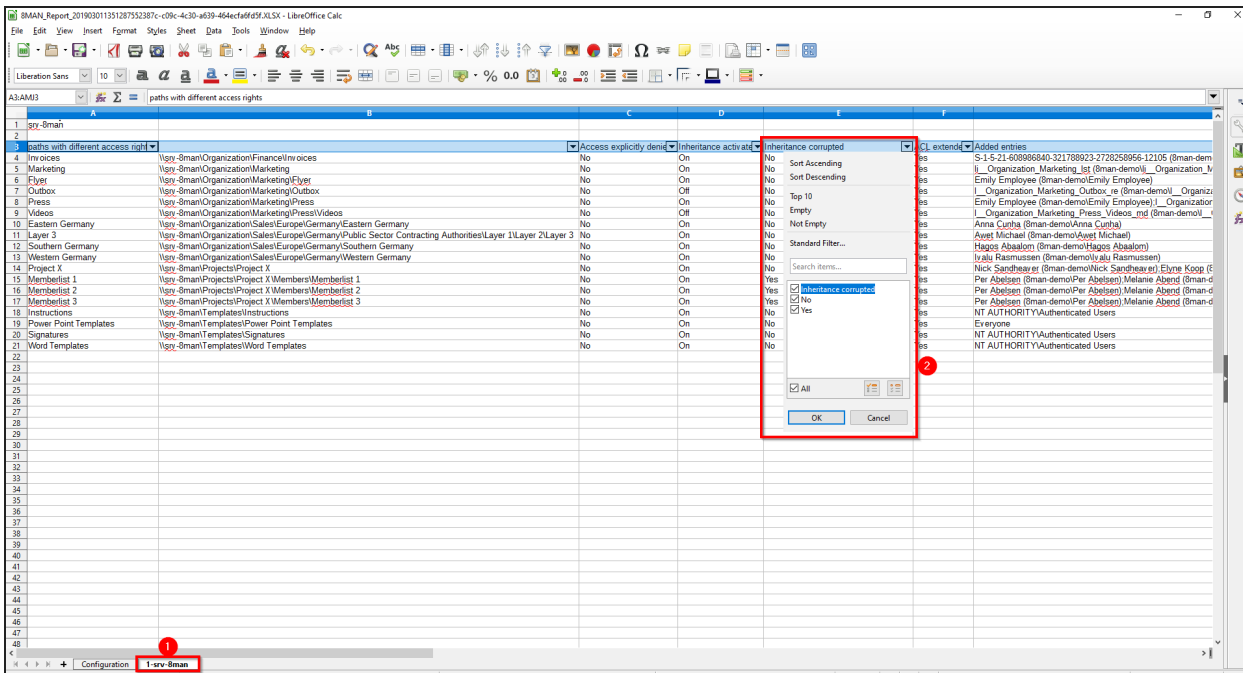
1. Select "Resources".
2. Select the desired file server.
3. Click on "Report".
4. Select "report on all sub-directories with different access rights".

The screenshot shows the 'Report on paths with different access rights' dialog in the Access Rights Manager. The dialog is titled 'Report on paths with different access rights' and has a close button (X) in the top right corner. It is divided into three main sections:

- Report configuration:** This section contains two text input fields: 'Title' and 'Comment'. A red box highlights these fields, and a red circle with the number '1' is placed to the left of the 'Title' field.
- Objects:** This section contains a list of objects. The object 'srv-8man' is selected. A red box highlights this object, and a red circle with the number '2' is placed to the right of the box.
- Report on paths with different access rights:** This section contains a tree view of resources. The tree view shows the following structure:
  - Resources
  - Active Directory
  - File server
    - Organization
    - Projects
    - Templates
    - Users
  - ExchangeA red box highlights the 'File server' section, and a red circle with the number '2' is placed to the right of the box.

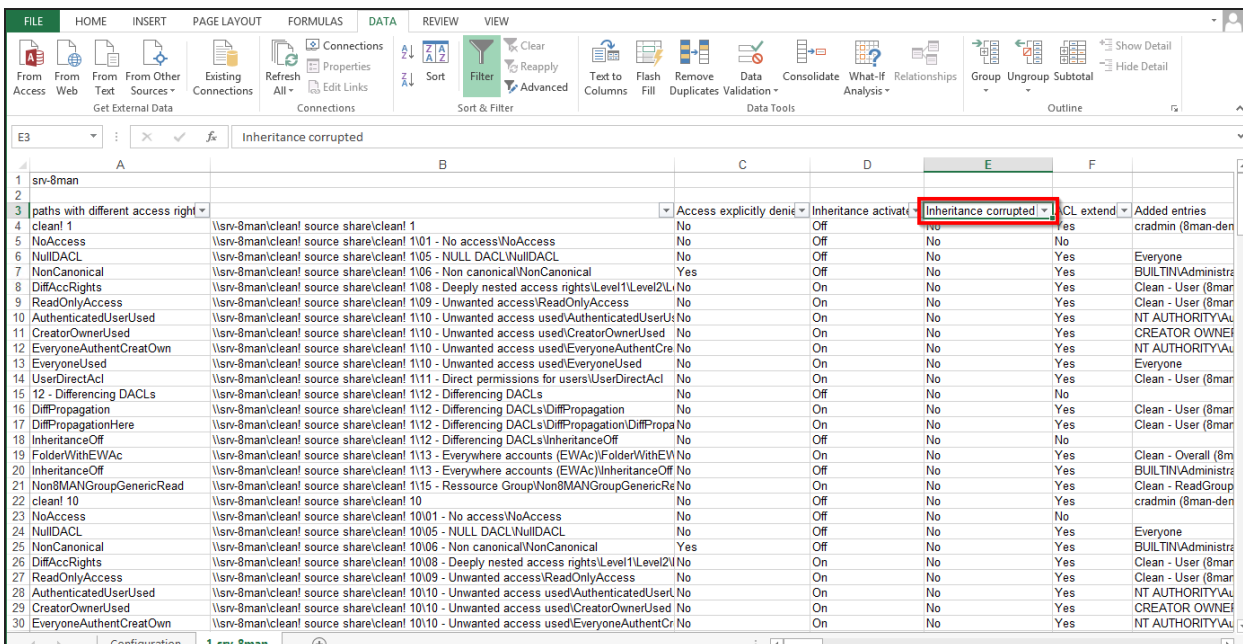
At the bottom of the dialog, there is a 'Start' button with a play icon and a 'Cancel' button. A red box highlights the 'Start' button, and a red circle with the number '3' is placed above the box.

1. You can name the report and add a comment.
2. You can change the range of the report.
3. Start the report creation.



Open the .XLS file with your spreadsheet application.

1. Select the tab of the desired resource.
2. Select the third line and add a filter.



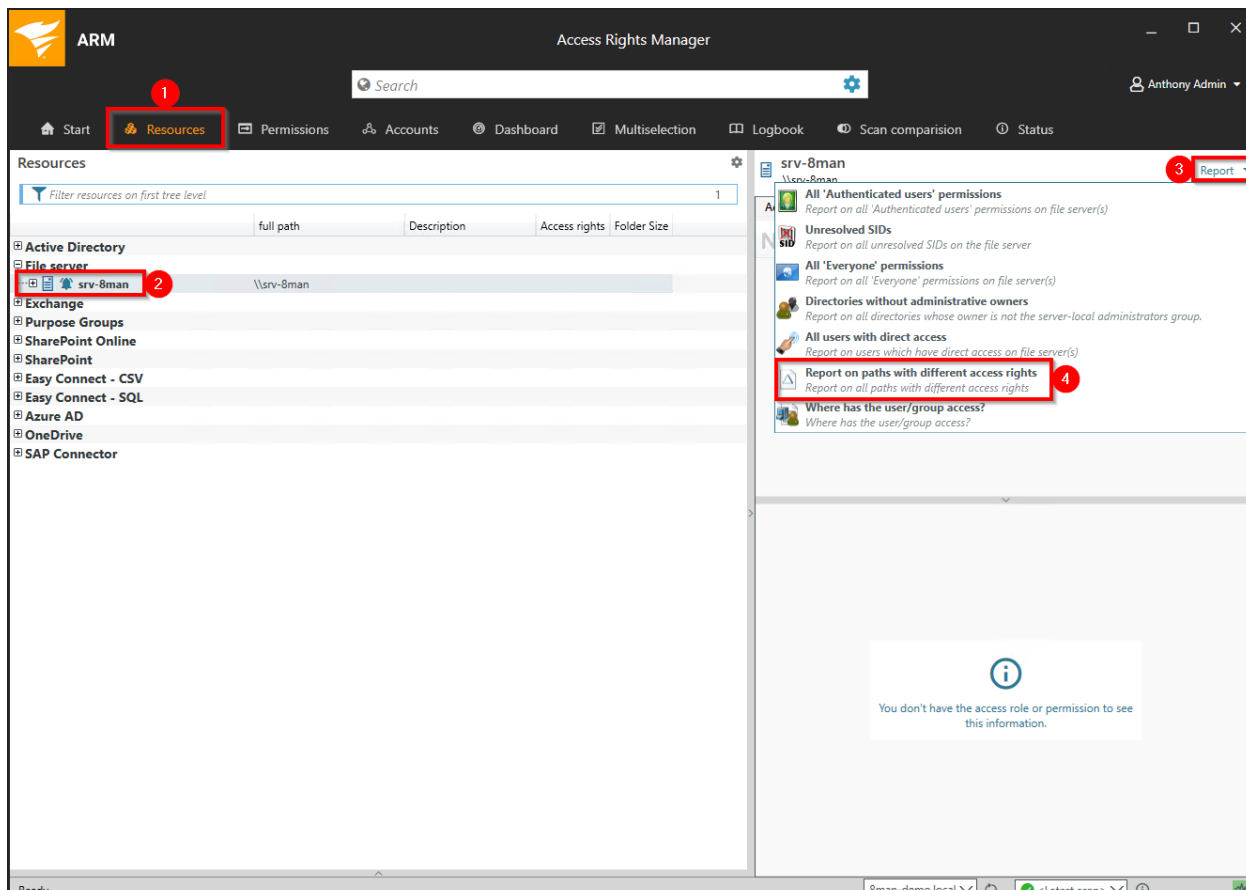
Filter the column "inheritance corrupted" by "yes".

## Identify folders with special protection

### Background / Value

Sub-directories often contain different access rights compared to its "parent" directory. ARM shows all directories where these rights differ. Disabled inheritances are often an indicator of highly restricted directories.

### Step-by-step process



1. Select "Resources"
2. Select the desired file server.
3. Click on "Report"
4. Select the report "Report on paths with different access rights"

ARM Access Rights Manager

Search

Anthony Admin

### Report on paths with different access rights

Resources

Filter resources on file

Active Directory

File server

Exchange

Purpose Groups

SharePoint Online

SharePoint

Easy Connect - CSV

Easy Connect - SQL

Azure AD

OneDrive

SAP Connector

1

**Report configuration**

Title

Comment

**Objects**

srv-8man

2

**Report on paths with different access rights**

Please select resource(s)

Resources

Active Directory

File server

srv-8man

Organization

Projects

Templates

Users

Exchange

3

Start Cancel

Settings

The output format is [XLSX](#)

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

Ready

8man-demo.local <Latest scan>

1. You can name the report and add a comment.
2. If desired you can adjust the range of the report.
3. Start the report.

The screenshot shows a spreadsheet application window titled "BMAN\_Report\_201903011420087ffaff2a-440-40e0-ac37-e89a56642ba.XLSX - LibreOffice Calc". The spreadsheet has a table with the following columns: "paths with different access rights", "Access explicitly denied", "Inheritance activated", "Inheritance corrupted", "ACL extended", and "Added entries". The "Inheritance activated" column is currently set to "Off" for all rows. A context menu is open over this column, showing options: "Sort Ascending", "Sort Descending", "Top 10", "Empty", "Not Empty", "Standard Filter...", "Search items...", "Inheritance activated", "On", and "Off". The "Inheritance activated" option is selected.

paths with different access rights	Access explicitly denied	Inheritance activated	Inheritance corrupted	ACL extended	Added entries
\\sv-Sman		On	o		
\\sv-Sman\Organization\Finance\Inv oices	No	On	o	Yes	S-1-5-21-608986840-32178923-2728258956-12105 (Bman-demo\S-1-5-21-608986840-32178
\\sv-Sman\Organization\Marketing	No	On	o	Yes	_Organization_Marketing_List (Bman-demo\__Organization_Marketing_List)_Organizator
\\sv-Sman\Organization\Marketing\Flyer	No	On	o	Yes	(Emily Employee (Bman-demo\Emily Employee)
\\sv-Sman\Organization\Marketing\Outbox	No	Off	o	Yes	_Organization_Marketing_Outbox_re (Bman-demo\__Organization_Marketing_Outbox_re)
\\sv-Sman\Organization\Marketing\Press	No	On	o	Yes	Emily Employee (Bman-demo\Emily Employee)_Organization_Marketing_Press_re (Bman
\\sv-Sman\Organization\Marketing\Press\Videos	No	Off	o	Yes	_Organization_Marketing_Press_Videos_not (Bman-demo\__Organization_Marketing_Pre
\\sv-Sman\Organization\Sales\Europe\Germany\Eastern Germany	No	On	o	Yes	Anna Curtha (Bman-demo\Anna Curtha)
\\sv-Sman\Organization\Sales\Europe\Germany\Public Sector Contracting Autho	No	On	o	Yes	Aysel Michael (Bman-demo\Aysel Michael)
\\sv-Sman\Organization\Sales\Europe\Germany\Southern Germany	No	On	o	Yes	Hages Abaalon (Bman-demo\Hages Abaalon)
\\sv-Sman\Organization\Sales\Europe\Germany\Western Germany	No	On	o	Yes	Iraku Rasmussen (Bman-demo\Iraku Rasmussen)
\\sv-Sman\Projects\Project X	No	On	o	Yes	Nick Sandbeaer (Bman-demo\Nick Sandbeaer), Elyne Koop (Bman-demo\Elyne Koop)
\\sv-Sman\Projects\Project X\Members\Memberlist 1	No	On	o	Yes	Per Abelsen (Bman-demo\Per Abelsen), Melanie Abend (Bman-demo\Melanie Abend)
\\sv-Sman\Projects\Project X\Members\Memberlist 2	No	On	o	Yes	Per Abelsen (Bman-demo\Per Abelsen), Melanie Abend (Bman-demo\Melanie Abend)
\\sv-Sman\Projects\Project X\Members\Memberlist 3	No	On	o	Yes	Per Abelsen (Bman-demo\Per Abelsen), Melanie Abend (Bman-demo\Melanie Abend)
\\sv-Sman\Templates\Instructions	No	On	o	Yes	NT AUTHORITY\Authenticated Users
\\sv-Sman\Templates\Power Point Templates	No	On	o	Yes	Everyone
\\sv-Sman\Templates\Signatures	No	On	o	Yes	NT AUTHORITY\Authenticated Users
\\sv-Sman\Templates\Word Templates	No	On	o	Yes	NT AUTHORITY\Authenticated Users

1. Open the .XLSX file with your spreadsheet application.
2. Click on the "resource tab".
3. We recommend using "auto filter" to analyze the "Inheritance activated" column. If set to "off" the report shows all directories with disabled inheritance.



## Identify the latest activities on a directory

### Background / Value

File server directories have their own history. This is why it makes sense to review the previously performed actions and changes. ARM shows you a quick view of most recent activities or you can jump directly into the log book to receive a full report.

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The 'Resources' tab is selected, and the 'Marketing' folder is highlighted in the tree view. A red box highlights the 'Marketing' folder in the tree view, and another red box highlights the '2 comments' section in the detailed view. The comments section shows a list of recent actions performed by 'anthony admin' on 10/16/2018 at 11:34 AM, including creating a new group, adding access rights, and adding a member.

1. Select "Resources".
2. The note icon indicates that the object contains comments. You can hover over the note for a quick preview.
3. ARM shows you a quick view of the latest actions.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The left pane shows a tree view of resources under 'Active Directory' and 'File server'. The 'Marketing' directory is selected, and a context menu is open with 'Open Logbook' highlighted. The right pane shows the 'Marketing' directory details, including the owner, inheritance, and a table of NTFS permissions. Below the permissions table is a table of accounts with permissions.

Account	how often granted	Inherit
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	
Administrator (8man-demo\Administrator)	1	
Anthony Admin (8man-demo\Anthony Admin)	1	
Antoine Admin (8man-demo\Antoine Admin)	1	
Anton Admin (8man-demo\Anton Admin)	1	
Caroline Berggren (8man-demo\Caroline Berggren)	2	2x
David DO Marketing (8man-demo\David DO Marketing)	3	3x
Domain Users (8man-demo\Domain Users)	1	
Elyne Koop (8man-demo\Elyne Koop)	2	2x
Emily Employee (8man-demo\Emily Employee)	4	4x
Ludvig Karlsson (8man-demo\Ludvig Karlsson)	3	3x
NT AUTHORITY\SYSTEM	1	

1. Right-click on a directory.
2. Click on "Open Logbook".

ARM

Access Rights Manager

Search

Anthony Admin

Resources

Overview of the Logbook

Filter resources on first

Active Directory

File server

srv-8man

Organization

Development

Facility Manag

Finance

Human Resou

Management

Marketin

Production

Research

Sales

Projects

Templates

Users

Exchange

Purpose Groups

SharePoint Online

SharePoint

Easy Connect - CSV

Easy Connect - SQL

Azure AD

OneDrive

SAP Connector

Comments for: Marketing

Filter 2

Only mine

Date & Time	Author	approved
10/16/2018 11:34 AM	anthony admin	
10/16/2018 11:33 AM	anthony admin	

Permission changed

anthony\_admin: Demo

ARM Changes:

Rights changes in folder "\srv-8man\Organization\Marketing" in chronological order:

- New group created: "L\_Organization\_Marketing\_md" (DomainLocal)
- Added access rights entry: L\_Organization\_Marketing\_md: Modify
- Member Emily Employee (8man-demo\Emily Employee) added to group L\_Organization\_Marketing\_md.

Used credential:

Active Directory changes: 8MAN-DEMO\sa-8man, File System changes: 8MAN-DEMO\sa-8man

Please add a comment

Add Close

Ready

8man-demo.local

1. Check the previous actions on the object.
2. You can also add a comment at any time to the logbook.

## Identify share permissions

### Background / Value

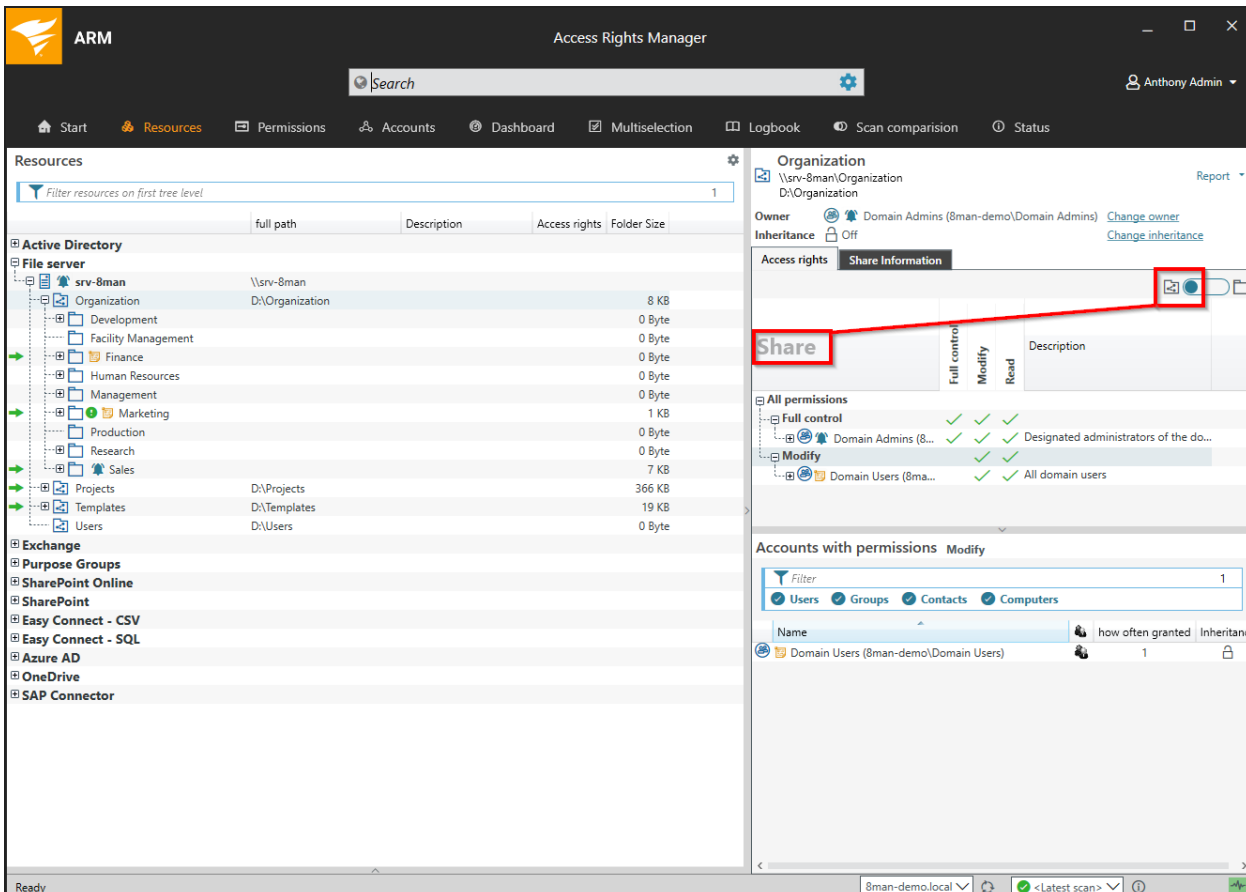
ARM shows both on shared directories: share permissions as well as NTFS permissions. By default NTFS permissions are listed.

### Step-by-step process

The screenshot displays the Access Rights Manager (ARM) interface. The 'Resources' tab is selected in the top navigation bar. In the left pane, the 'Organization' folder under the 'srv-8man' file server is selected. The right pane shows the 'Share Information' tab, which displays 'NTFS' permissions for the selected folder. Below this, a table lists accounts with permissions:

Name	how often granted	Inheritance
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	🔒
Administrator (8man-demo\Administrator)	1	🔒
Anthony Admin (8man-demo\Anthony Admin)	1	🔒
Antoine Admin (8man-demo\Antoine Admin)	1	🔒
Anton Admin (8man-demo\Anton Admin)	1	🔒
NT AUTHORITY\SYSTEM	1	🔒
sa-8man (8man-demo\sa-8man)	1	🔒

1. Select "Resources".
2. Select a shared folder (recognizable by the special folder icon).
3. By default ARM shows NTFS permissions.



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The main window is titled "Access Rights Manager" and shows a search bar and user "Anthony Admin". The left pane displays "Resources" under "Active Directory" and "File server". The "File server" section shows a tree view of folders, with "Organization" selected. The right pane shows the "Organization" folder details, including "Owner" (Domain Admins), "Inheritance" (Off), and "Access rights". A red box highlights the "Share" button in the "Access rights" section. Below the "Share" button is a table with columns "Full control", "Modify", and "Read". The "All permissions" section shows a list of permissions for "Full control" and "Modify". The "Accounts with permissions" section shows a list of accounts with permissions, including "Domain Users (8man-demo\Domain Users)".

Use the toggle button to switch between share and NTFS permissions.

## Exchange

ARM for Exchange integrates Exchange resources. This way the analysis and administration of access rights are standardized across various resources and systems. ARM shows you an overview, where you can see access rights to mailboxes, mailbox folders including calendars and distribution group memberships and properties on one easy to read screen.

### Identify access rights on mailboxes

#### **Background / Purpose**

Who has access to which mailbox? ARM for Exchange shows you all access rights in the resources view.

#### **Related features**

Report: [Who has access where?](#)

Report: [Identify mailbox permissions](#)

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The left sidebar contains a tree view of resources, with the 'Resources' menu item highlighted by a red box and the number '1'. The main pane displays a list of mailboxes under the 'Exchange' section, with the 'Delmar Atkins' mailbox selected, highlighted by a red box and the number '2'. The right pane shows the 'Access rights' tab for the selected mailbox, displaying a table of permissions with columns for Owner, Full Access, Read Permissions, Administrate, and Send As. This table is highlighted by a red box and the number '3'. Below this, the 'Accounts with permissions' section shows a flat list of users/groups with access rights, also highlighted by a red box and the number '4'.

Account	Owner	Full Access	Read Permissions	Administrate	Send As
NT AUTHORITY\SELF	✓				
EURPRD08\Administrator		✓			
EURPRD08\Domain Admini...		✓			
EURPRD08\Enterprise Ad...		✓			
EURPRD08\Organization...		✓			
NT AUTHORITY\SYSTEM	✓				
NT AUTHORITY\NETWORK...			✓		
S-1-5-21-1509316702-20...			✓		
PRDTSB01\UiUsers			✓		
EURPRD08\Public Folder...			✓		

Name	Count	Warning
EURPRD08\Administrator	2	⚠
EURPRD08\Domain Admins	2	⚠
EURPRD08\Enterprise Admins	2	⚠
EURPRD08\Exchange Servers	1	
EURPRD08\Exchange Trusted Subsystem	1	
EURPRD08\Managed Availability Servers	1	
EURPRD08\Organization Management	2	⚠
EURPRD08\Public Folder Management	1	
NT AUTHORITY\NETWORK SERVICE	1	
NT AUTHORITY\SELF	2	⚠

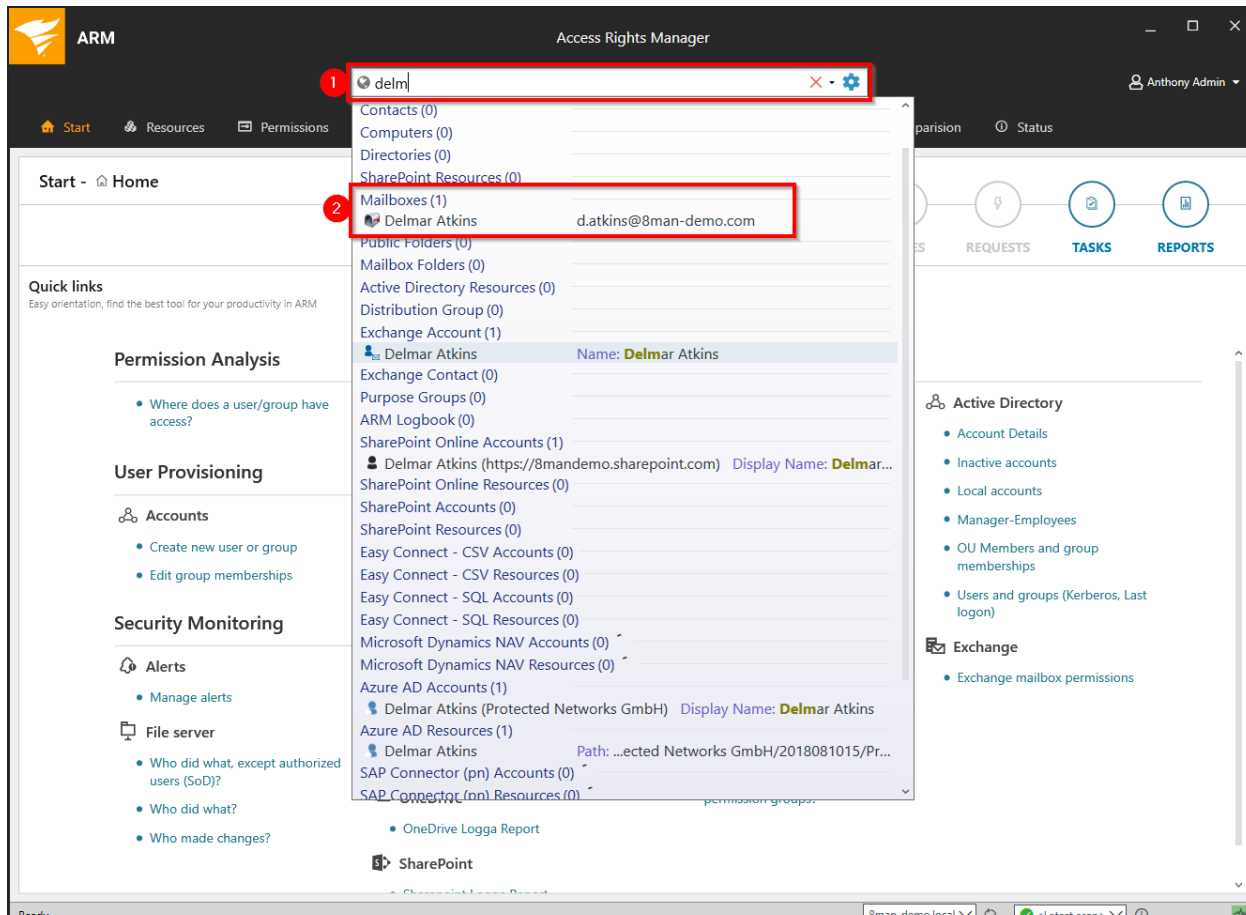
1. Select "Resources".
2. Navigate to the desired mailbox.
3. ARM shows you which users/groups have which rights.
4. ARM shows all accounts with access rights in a flat list.

## Identify mailbox properties

### Background / Purpose

ARM shows the properties of individual mailboxes. Among other things, you will also find out-of-office recipients, delegates and forwards.

### Step-by-step process



Use the search field to find the desired mailbox.



The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources' (highlighted with a red box and a '1'), 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The user 'Anthony Admin' is logged in. The main area is divided into two panes. The left pane, titled 'Resources', shows a tree view of resources under 'Exchange' > '8man-demo.com' > 'Mailboxes'. The mailbox 'Delmar Atkins' is selected and highlighted with a red box and a '2'. The right pane shows the 'Properties' tab for the selected mailbox, with a red box and a '3' highlighting the 'Properties' tab and the list of properties. The properties list includes 'Out of Office' settings, 'Additional attributes' (Identifier, Standard mailbox size), 'Mailbox Quota' (Issue warning quota, Send email prohibited at, Send and receive email prohibited at, Maximum email size), and 'Database Quota' (Issue warning quota, Send email prohibited at, Send and receive email prohibited at, Maximum email size). Other properties include 'email addresses', 'email address policy', 'Item count', 'Database', 'Last logoff timestamp', and 'Last logon timestamp'.

Name	Value
Out of Office	
Recipient	Internal, external contacts
Additional attributes	
Identifier	d.atkins
Standard mailbox size	Not activated
Mailbox Quota (Activated)	
Issue warning quota	50176 MB
Send email prohibited at	50688 MB
Send and receive email prohibited at	51200 MB
Maximum email size (receiving)	37 MB
Maximum email size (Sending)	35 MB
Database Quota	
Issue warning quota	unlimited
Send email prohibited at	unlimited
Send and receive email prohibited at	unlimited
Maximum email size (receiving)	unlimited
Maximum email size (Sending)	unlimited
email addresses	smtp:d.atkinssss@8man-demo.com smtp:d.atkins@8mandemo.onmicrosoft.com SMTP:d.atkins@8man-demo.com SPO-SPO_c20a7426-2ef4-4435-8d3f-3354f5dca7d9... SIP:d.atkins@8man-demo.com
email address policy	Not activated
Item count	34999
Database	EURPR08DG017-db126
Last logoff timestamp	12/17/2018 7:19:11 AM
Last logon timestamp	12/17/2018 6:48:55 AM

1. ARM automatically switches to the resource view.
2. ARM focuses on the desired mailbox.
3. Click on the tab "properties". ARM shows you all mailbox properties.

## Identify access rights on public folders

### Background / Value

Keeping an overview of access rights to public folders can be extremely challenging with native tools. ARM shows you the access rights situation to public folders in the resource view.

### Related features

Report: [Who has access where?](#)

Report: [Identify mailbox access rights](#)

[Create a mailbox](#)

[Change mailbox permissions](#)

[Manage out-of office notices](#)

[Manage mailbox and email size](#)

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The main window is titled "Access Rights Manager" and shows a navigation pane on the left with "Resources" selected. The right pane displays the "Access rights" for the selected resource, "Genes".

1. Select "Resources".

2. Navigate to the desired public folder. Alternatively, you can also use the search function.

3. ARM shows which users/groups have which access rights.

4. ARM shows all accounts with access rights in a flat list view.

The "Access rights" section shows a table with columns for "Author", "None", and "Editor". The "All permissions" section shows a list of permissions with checkmarks indicating they are applied.

The "Accounts with permissions" section shows a list of accounts with their respective access rights:

Name	Access Right
Anonymous (Exchange\Anonymous)	1
Default (Exchange\Default)	1
Eric Zann (8man-demo.com\eric.zann)	1
Jenny Barnes (8man-demo.com\j.barnes)	1

1. Select "Resources".
2. Navigate to the desired public folder. Alternatively, you can also use the search function.
3. ARM shows which users/groups have which access rights.
4. ARM shows all accounts with access rights in a flat list view.

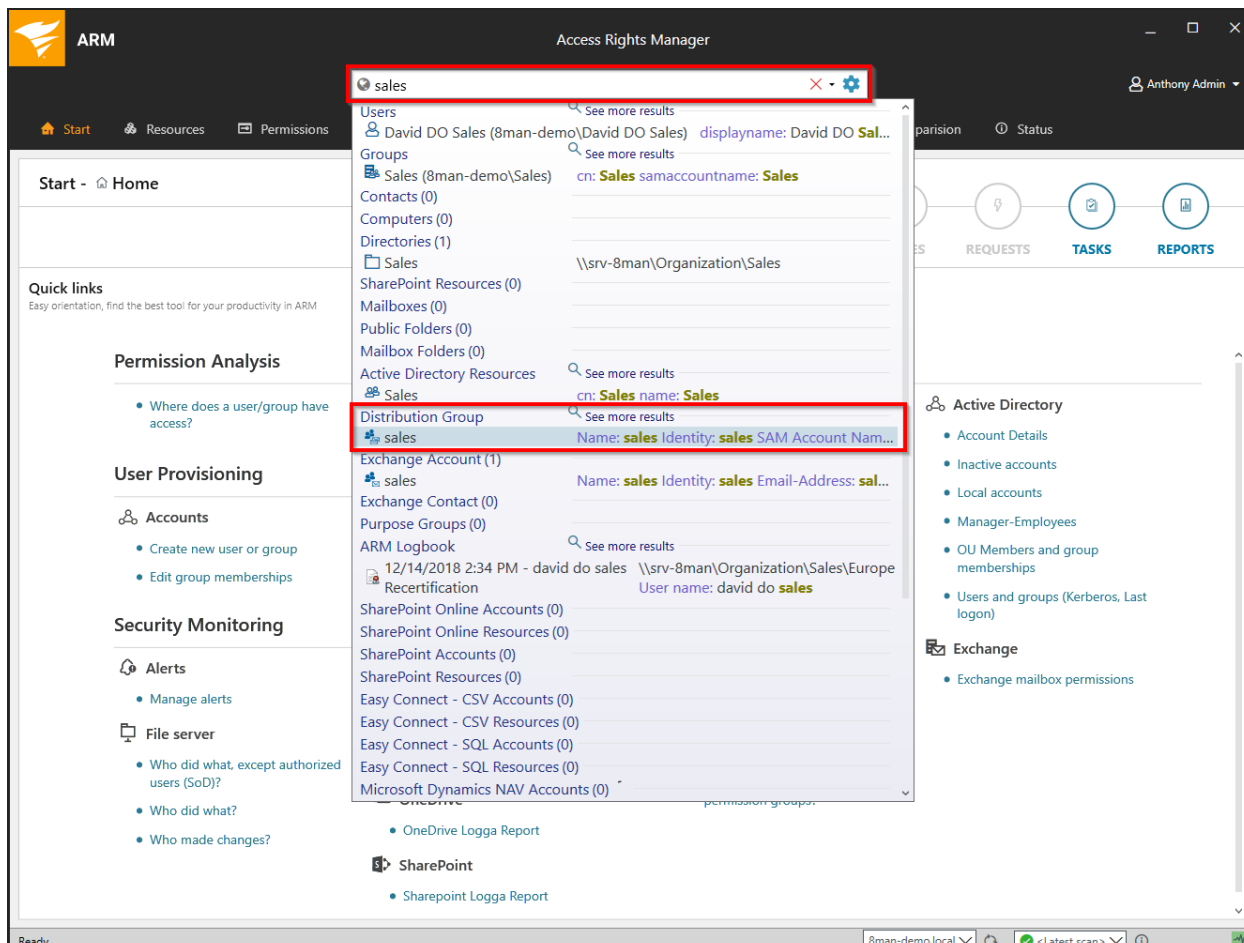
## Identify permissions on distribution groups

### Background / Value

With ARM you can quickly check who is allowed to send emails from which distribution list. The relevant cases are "send as" and "send on behalf of". The former is the most critical, since it is not easy to identify who actually sent the email. In the scenario for "send on behalf" the PA or deputy sending the email is clearly recognizable.

 ARM also works with dynamic Exchange groups.

### Step-by-step process



Use the search field to find the desired Distribution group.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main window is titled 'Access Rights Manager' and shows a search bar and navigation tabs for Start, Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, and Status. The user is logged in as 'Anthony Admin'.

The left pane shows a tree view of resources under 'Exchange' > '8man-demo.com'. The 'sales' account is selected. The right pane shows the 'Access rights' tab for this account, which is highlighted with a red box. It displays a table of permissions and a list of accounts with those permissions.

Account	Permission	Send On Behalf	Send As
Richard Pickman (8man-d...)	All permissions	✓	
h.armitage@8man-demo...	All permissions		✓


Accounts with permissions		
Users/groups with access right: All permissions		
Name	Count	
h.armitage@8man-demo.com	1	
Richard Pickman (8man-demo.com\r.pickman)	1	

ARM shows all access rights on the right-hand side.

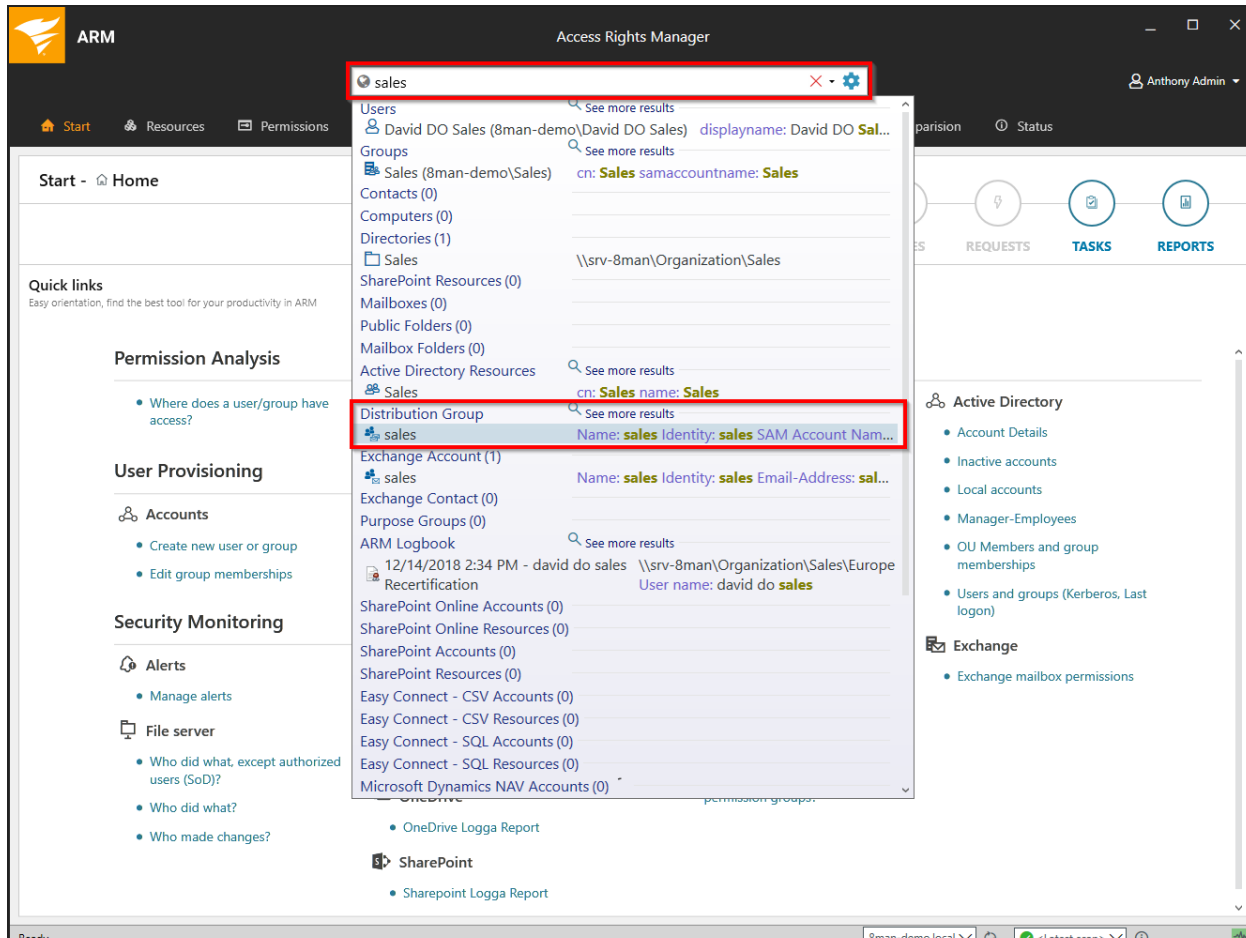
## Identify members of distribution groups

### Background / Purpose

ARM allows you to display all members and / or recipients of distribution lists. In typical ARM style this also includes nested group memberships.

 ARM also works with dynamic Exchange groups.

### Step-by-step process



Use the search field to find the desired distribution group.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main window is titled "Access Rights Manager" and shows a navigation pane on the left with various resource categories like Active Directory, File server, Exchange, etc. The "Exchange" section is expanded, showing a tree view of distribution groups. The "sales" group is selected, and a context menu is open over it, with the "Show in accounts view..." option highlighted. The main pane shows the "Members" tab for the "sales" group, displaying a list of members: Delmar Atkins, Francis Morgan, and Jenny Barnes. The "Children" tab is also visible, showing a flat list of members. The interface includes a search bar, a user profile (Anthony Admin), and a status bar at the bottom.

1. Focus on the desired distribution group.
2. Select the tab "Members".
3. Open the "Children" area.
4. You can then see all members of the distribution group in a flat list.
5. Alternatively you can analyze the group in the accounts view. Right-click on the distribution group and select "Show in accounts view" from the context menu.

The screenshot displays the 'Accounts' view in the Access Rights Manager. The main area shows a 'Graph' of the group structure for 'sales (8man-demo.com\sales)'. The graph is as follows:

- Root Group: sales (8man-demo.com\sales) [2 members]
- Child Groups:
  - DynTestGruppe (8man-demo.com\DynTestGruppe) [19 members]
  - external consultants (8man-demo.com\external consultants) [19 members]
- Child Users:
  - Delmar Atkins (8man-demo.com\d.atkins) [4 members]
  - Francis Morgan (8man-demo.com\f.morgan) [1 member]
  - Jenny Barnes (8man-demo.com\j.barnes) [1 member]

The right-hand pane shows the 'Children' list for the selected group:

Name	Count
Delmar Atkins (8man-demo.com\d.atkins)	1
Francis Morgan (8man-demo.com\f.morg...)	1
Jenny Barnes (8man-demo.com\j.barnes)	1

Use the accounts view to analyze the group structure and memberships.



## OneDrive

OneDrive offers the possibility to store files and folders in the cloud. The advantages of the cloud service are obvious: employees can work together on documents easily and conveniently. The external sharing of documents is particularly critical as it is possible to share documents without authorization for an unlimited period of time.

ARM shows you with its typical simplicity which users shared which files and folders how and with whom.

### Identify shared directories and files on OneDrive

#### **Background/Value**

OneDrive offers the possibility to store files and folders in the cloud. The advantages of the cloud service are obvious: employees can work together on documents easily and conveniently. The external sharing of documents is particularly critical as it is possible to share documents without authorization for an unlimited period of time.

ARM shows you with its typical simplicity which users shared which files and folders how and with whom.

#### **Related features**

[Create a report about directories and files shared on OneDrive](#)

#### **Step-by-step process**

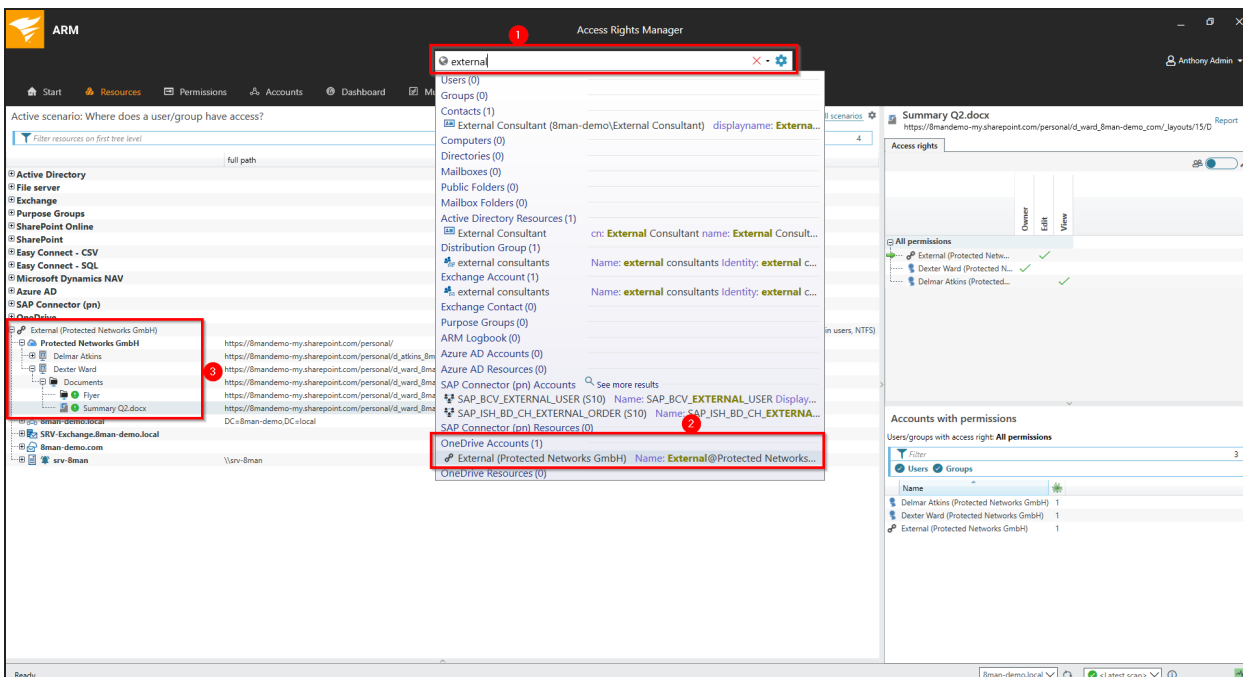
The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The left sidebar contains a tree view of resources, with 'OneDrive' expanded to show a folder structure. The main pane displays details for a document named 'Summary Q2.docx'. The 'Access rights' section shows a table of permissions, and the 'Accounts with permissions' section shows a list of users/groups with their respective access levels.

	Owner	Edit	View
<b>All permissions</b>			
External (Protected Netw...		✓	✓
Dexter Ward (Protected N...	✓		
Delmar Atkins (Protected...			✓

Users/groups with access right: All permissions	
Name	
Delmar Atkins (Protected Networks GmbH)	1
Dexter Ward (Protected Networks GmbH)	1
External (Protected Networks GmbH)	1

1. Select the resource view.
2. Expand OneDrive.
3. Browse the OneDrive structure.
4. ARM displays the permissions.
5. ARM shows you the authorized users.



## External

"External" is used to identify files or folders that are shared externally. OneDrive creates a link (hence the symbol used). Anyone who owns the link can read or change it.

## Internal

"Internal" identifies files or folders that are shared within the organization. When a file or folder is shared with a specific user (by e-mail address) within the organization, that user is granted permission (no link is created).

1. Search for "Internal" or "External".
2. Click on the desired result in OneDrive Accounts.
3. ARM opens up a scenario that displays only internally or externally shared files and folders.

## Documentation & Reporting

ARM offers a wide variety of customizable and easy-to-understand reports about the access rights situation in your organization. With just a few clicks, you can create and schedule reports with safety-critical information. With native tools you would need a great deal of time for those or it would be almost impossible to assemble.

ARM documents the changes in Active Directory, the file servers and all other integrated resources. You can use the Calendar function to view the activities over the course of time. The mandatory comment function takes the burden off the administrator. Since a short note (a ticket number for instance) is stored, every activity is traceable, even a long time after.

### Cross-resource

Many of the ARM Documentation & Reporting features are available for all configured resources.

#### Report: Who has access where?

##### Background / Value

Managers and team leads know best who should have access to what. Having an understanding of your access rights situation is extremely important, especially for sensitive resources. The report "Who has access where?" provides an overview of users and their access.

The report allows responsible managers to make information based decisions in order to answer two central questions:

- Who should have access to what? (increase in data security)
- Which access rights should exist? (improvement of data integrity)

##### Related features

Report: [Where do users and groups have access?](#) (user in focus)

[Modify directory access rights](#)

## Step by step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main content area is divided into several sections: Permission Analysis, User Provisioning, Security Monitoring, and Documentation & Reporting. The 'Start' button in the top navigation bar is highlighted with a red box and a red circle containing the number '1'. In the 'Documentation & Reporting' section, the 'Who has access where?' link is highlighted with a red box and a red circle containing the number '2'.

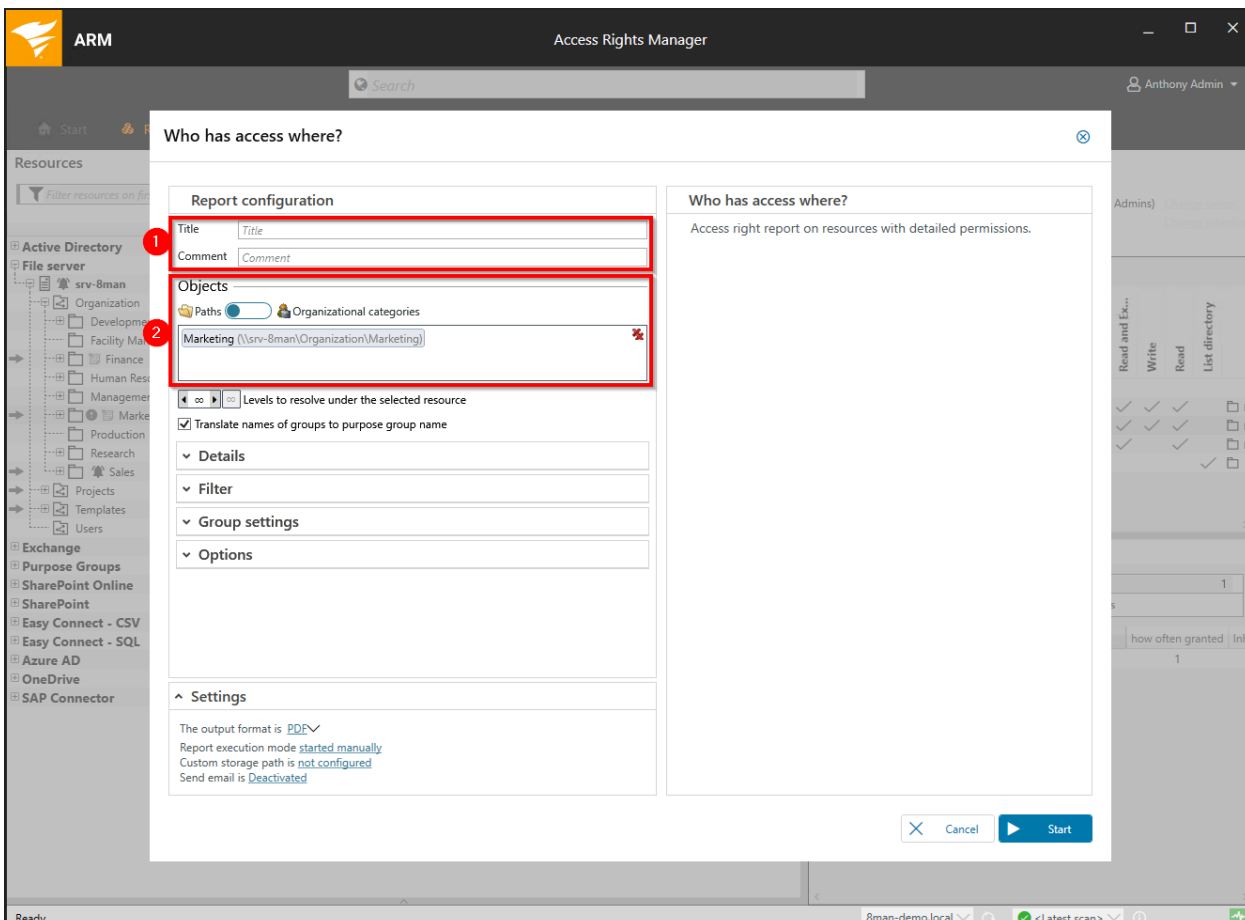
1. Select "Start".
2. Click "Who has access where?".

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The 'Resources' tab is active, showing a tree view of the file system. The 'Marketing' directory is selected, and its context menu is open. The menu items include 'Rescan directory', 'Report: Who has access where?', 'Modify access rights...', 'Create directory', 'Delete directory', 'Change owner', 'Change inheritance', 'Open Logbook', 'Create alert', and 'Copy as path'. The 'Report: Who has access where?' option is highlighted with a red box and a red circle. The right-hand pane shows the 'Marketing' directory details, including the owner (Domain Admins), inheritance (On), and a table of permissions (Full control, Modify, Read and Execute, List directory) with their respective inheritance and control status. Below the permissions table, there is a section for 'Accounts with permissions' showing a list of users and groups with their access counts.

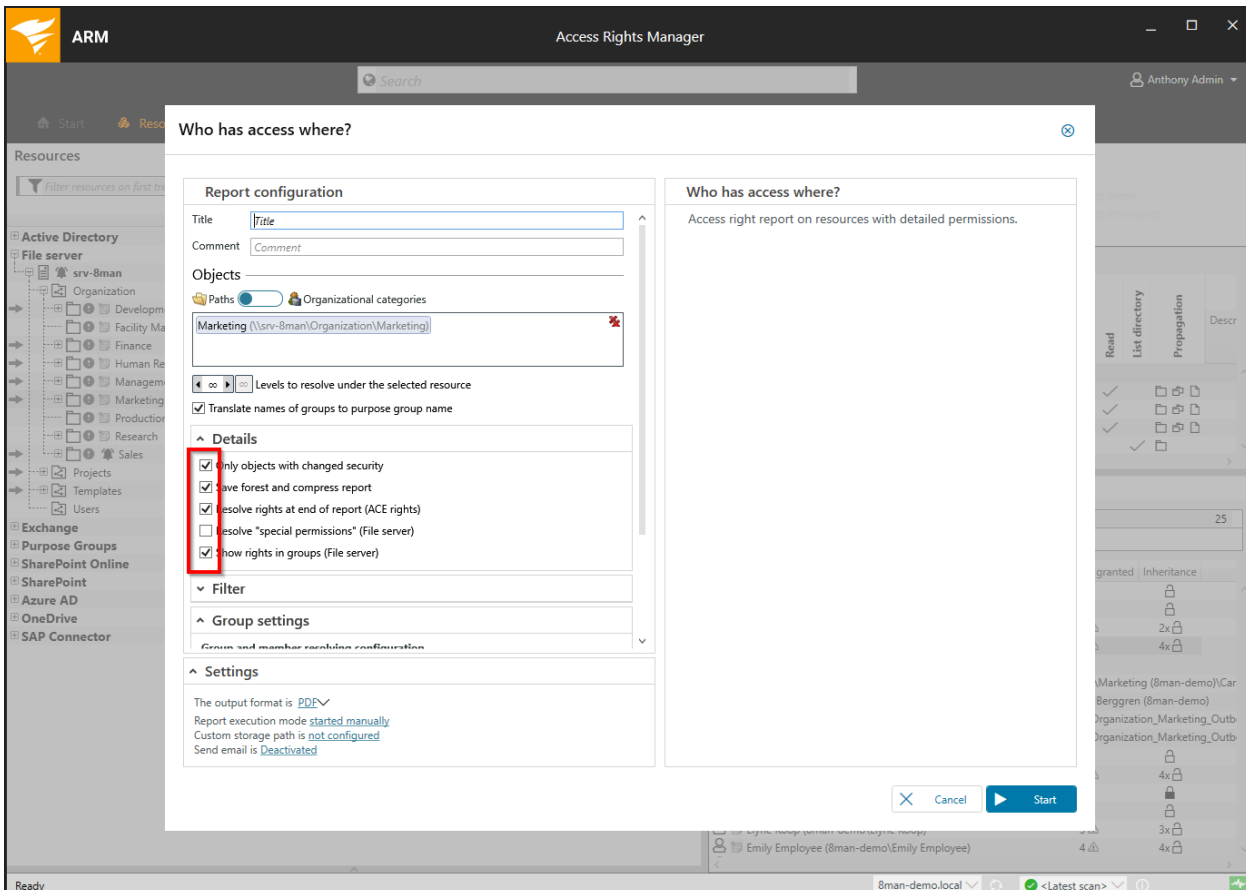
Account	how often granted	Inheritance
Emily Employee (8man-demo\Emily Employee)	1	

Alternative way to start the report:

1. Select "Resources".
2. Right-click on a directory that you are responsible for.
3. Click on "Report: Who has access where?" from the context menu.



1. Name the report and add a comment.
2. The selected resource is automatically included in the list of objects to be analyzed. You can add further resources.



We recommend that you set the options in the details area for a first run as shown above.



ARM Access Rights Manager

Search

Anthony Admin

### Who has access where?

Report configuration

Title

Comment

Objects

Paths  Organizational categories

Levels to resolve under the selected resource

Translate names of groups to purpose group name

Details

Filter

Group settings

Group and member resolving configuration

Usersview  
Groups will be replaced by their members, Listview

Resolve groups in the summary section

Resolve group members up to this level

Settings

The output format is [PDF](#)

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

Cancel Start

1. Open "Group Settings".
2. In order to reduce complexity we recommend selecting the "Usersview".
3. Set the output options. For example, you can schedule the report and set it to be sent regularly by email.
4. Start the report.

ARM Report: Who has access where?			
<b>Title</b>	ARM Report: Who has access where?		
<b>Comment</b>	-		
<b>Used time zone</b>	W. Europe Daylight Time (UTC+02:00:00)		
<b>Scantime</b>	8man-demo.local	Active Directory	5/8/2019 10:23:46 AM
	srv-8man	File server	5/8/2019 10:23:47 AM
<b>Configuration</b>	Selected resources: • Marketing (\\srv-8man\Organization\Marketing)  Number of levels to resolve under the selected resource: All Show only resource objects with changed access rights. Resolve groups at end.		
<b>Scan problems</b>	No scan errors detected.		

### Report for Marketing (\\srv-8man\Organization\Marketing)

Marketing				
\\srv-8man\Organization\Marketing				
Last scan time at 5/10/2019 9:51:30 AM.				
	Full control (This folder, subfolders and files)	Modify (This folder, subfolders and files)	List folder contents (Only this folder)	Read & execute (This folder, subfolders and files)
<b>Full control</b>				
Domain Admins (8man-demo\Domain Admins)	✓	✓		
NT AUTHORITY\SYSTEM	✓	✓		
<b>Modify</b>				
Alfie Williamson (8man-demo\Alfie Williamson)		✓	✓	
Caroline Berggren (8man-demo\Caroline Berggren)		✓	✓	
David DO Marketing (8man-demo\David DO Marketing)		✓	✓	
Emily Employee (8man-demo\Emily Employee)		✓	✓	
Finn Dunne (8man-demo\Finn Dunne)		✓	✓	
George Comer (8man-demo\George Comer)		✓	✓	
Louie Findlay (8man-demo\Louie Findlay)		✓	✓	
Ludvig Karlsson (8man-demo\Ludvig Karlsson)		✓	✓	
Mattias Blom (8man-demo\Mattias Blom)		✓	✓	
Nadine Eberhart (8man-demo\Nadine Eberhart)		✓	✓	

Data owners now can verify whether the listed users should have access.

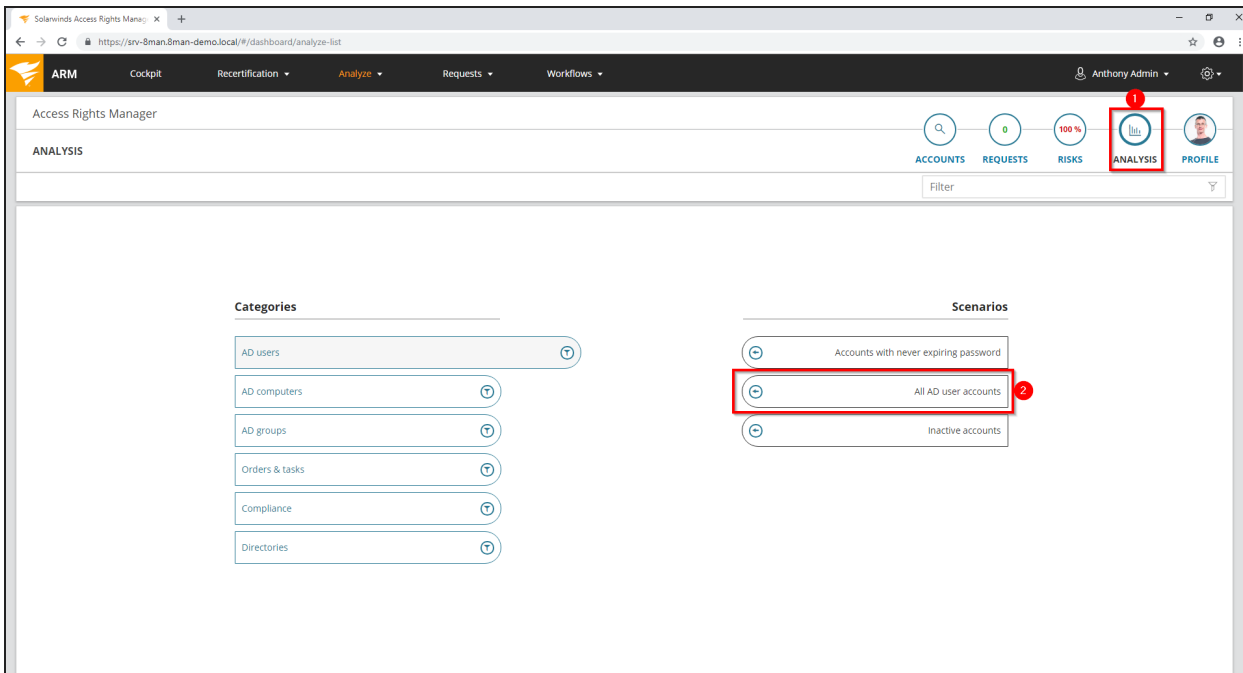
**i** You should also check to see if the access rights of some users can not be reduced for example from "full access" to "read" or "modify". This ensures a higher level of data integrity.

## Flexible reports (web client)

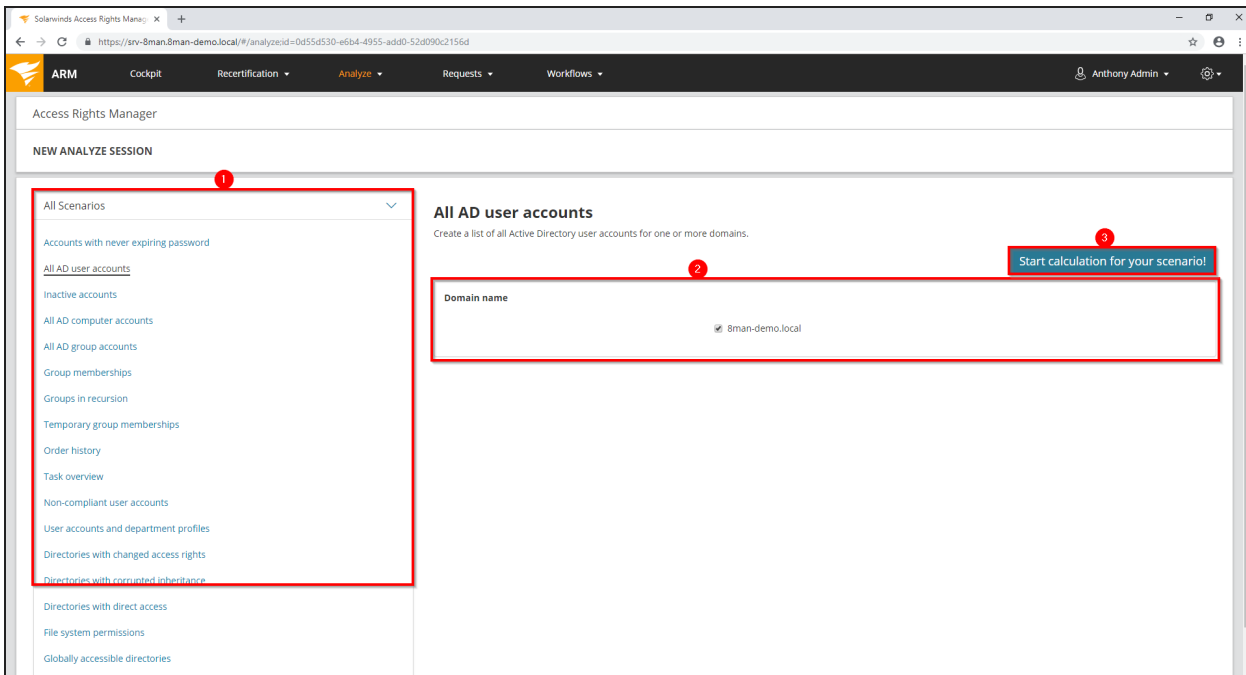
### Background / Value

With Analyze & Act in the web client, you create flexible reports. Design the report with groupings, filters, sorts and the desired columns exactly as you need it. You can then export the finished report directly to the Excel format, for example.

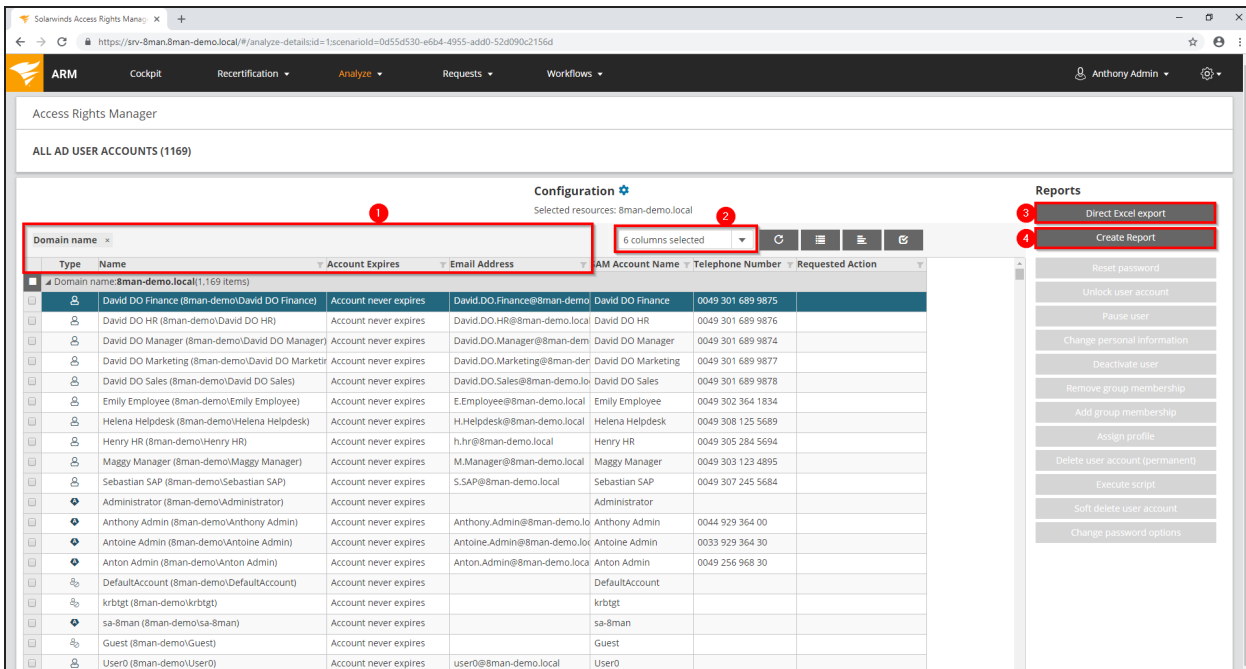
### Step-by-step process



1. Click "Analysis".
2. Click "All AD user accounts" (for example).



1. Optional: Change the scenario.
2. Set options for the scenario.
3. Click "Start calculation".



1. Use groupings, sorts and filters to design the report layout.
2. Add or remove columns to the content.

3. Export the report directly to the Excel format. Layout options will be adopted.
4. Create a report in PDF or CSV format, which you store on the file system or send by email.

## Where do users and groups have access?

### Background / Value

The report "Where has the user/group access?" lists all access rights of users and groups across **all** selected resources (user in focus).

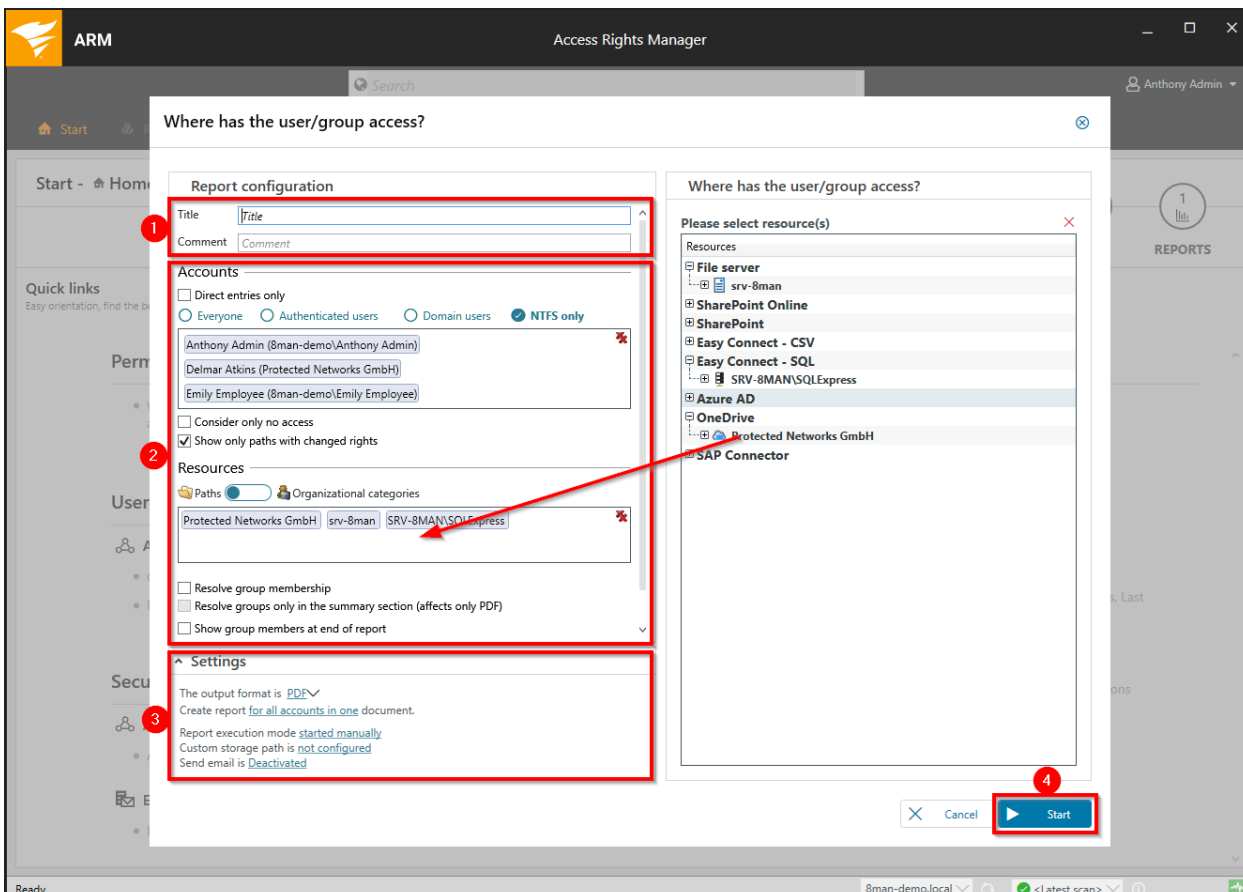
### Related features

Report: [Who has access where?](#) (resource in focus)

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main navigation menu is visible, with the 'Start' button highlighted by a red box and a red circle with the number '1'. Below the navigation bar, the 'Start - Home' page is displayed. The 'Quick links' section is visible, and the 'Documentation & Reporting' section is expanded. The 'Where has the user/group access?' report is highlighted by a red box and a red circle with the number '2'. The interface also shows sections for 'Permission Analysis', 'User Provisioning', and 'Security Monitoring'.

1. Select "Start".
2. Click on "Where has the user/ group access?".



1. Enter a title for the report and add a comment.
2. Define the range and the layout of the report.
3. Define the desired output settings.
4. Start the report.

## Report on ARM Access Rights Management activities (Logbook report)

### Background / Value

All changes made with ARM are automatically recorded in the log book. This ensures compliance with a number of legal and best-practice standards and saves the time of manual documentation. The log book report allows you to capture events by person or event type within any desired time period. This ensures fully transparent processes and documentation.

**i** The logbook covers all changes made with ARM, all AD Logga and Exchange Logga events. FS Logga, OneDrive Logga and SharePoint Online Logga events are only available in their respective reports.

### Related features

[FS Logga Report: Who did what?](#)

### Step-by-step process

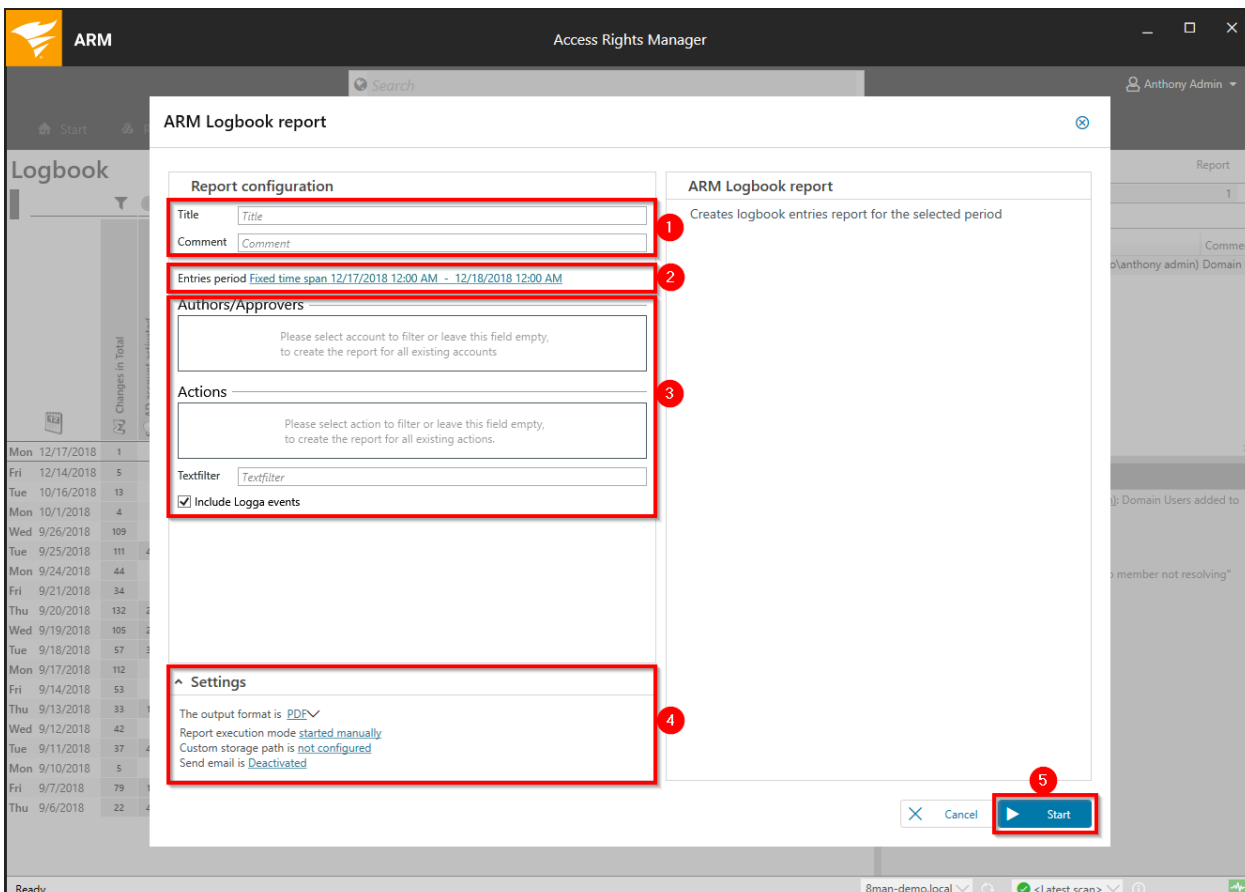
The screenshot shows the Access Rights Manager (ARM) interface. The 'Logbook' tab is selected in the navigation menu (1). In the top right corner, the 'Report' button is highlighted (2). The main area displays a calendar grid for the Logbook, showing events from 6 months ago until today. A right-hand pane shows the details for the selected date, Monday, December 17, 2018, including a list of events like 'ARM Logbook Report' and 'AD Logga Report' (3).

Day	12/17/2018	12/14/2018	10/16/2018	10/17/2018	9/26/2018	9/25/2018	9/24/2018	9/21/2018	9/20/2018	9/19/2018	9/18/2018	9/17/2018	9/14/2018	9/13/2018	9/12/2018	9/11/2018	9/10/2018	9/7/2018	9/6/2018
Mon	1																		
Fri	5																		
Tue	13		3		3														
Mon	4			1 1 2															
Wed	109		10		9														
Tue	111	4 14																	
Mon	44		12																
Fri	34																		
Thu	132	2			2														
Wed	105	2			19														
Tue	57	3 1			9 1 6 3														
Mon	112				36														
Fri	53																		
Thu	33	1																	
Wed	42																		
Tue	37	4																	
Mon	5																		
Fri	79	1																	
Thu	22	4																	

1. Select "Logbook".
2. Click on "Report".



## 3. Select "ARM logbook report".



1. Enter a title for the report and add a comment.
2. Select the desired time-period for the report.
3. Define the range of the report.
4. Define the desired report settings.
5. Start the report.


## Active Directory

ARM lets you create easy to read reports on Active Directory.

### Employees of a manager

#### Background / Value

Data Owners that have some knowledge of Active Directory can view attributes and group memberships of their employees.

 The report utilizes the attribute "manager" in Active Directory.

#### Related features

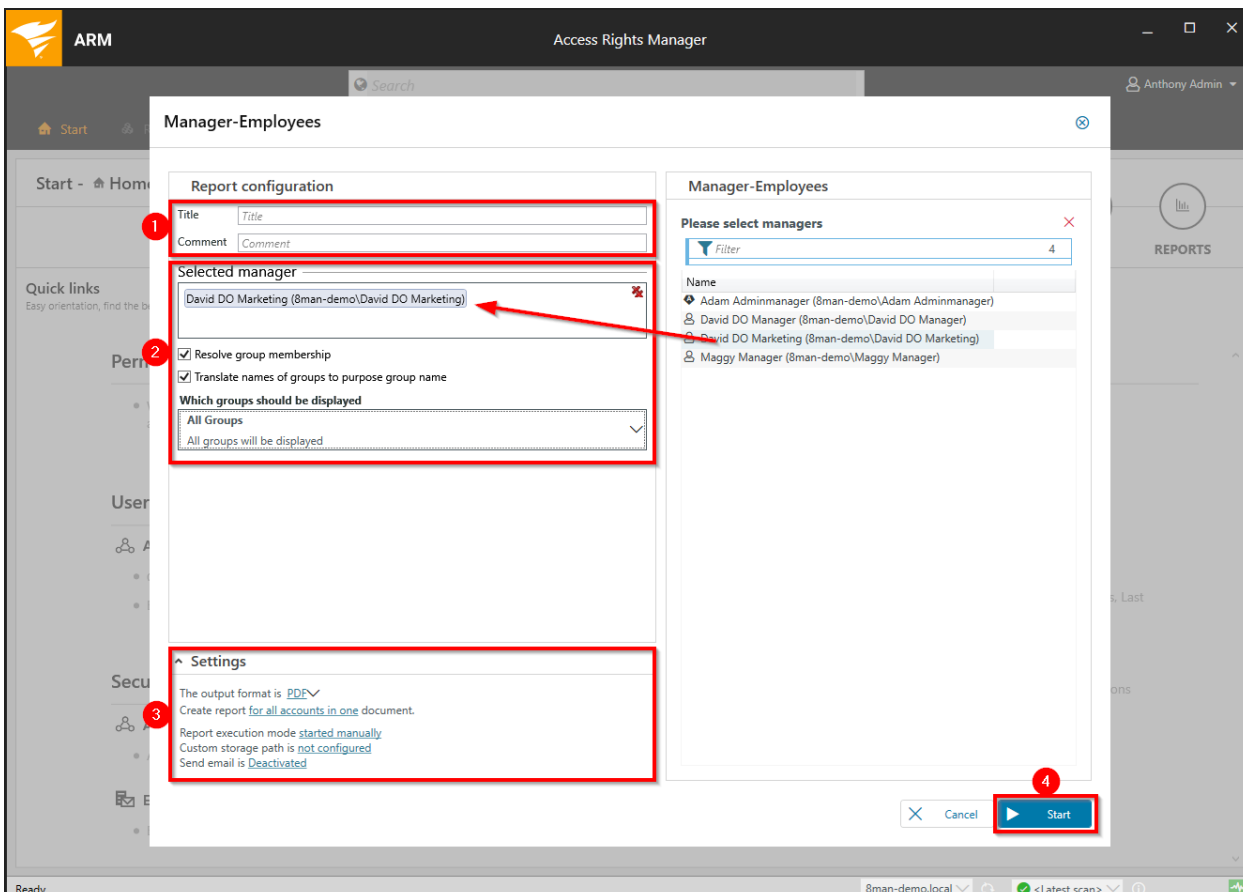
For more detailed information and the inclusion of assigned file server resources we recommend the report:

[Where do employees of a manager have access \(file server\)?](#)

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main content area is divided into several sections: Permission Analysis, User Provisioning, Security Monitoring, and Documentation & Reporting. The 'Start' button in the top navigation bar is highlighted with a red box and a red circle containing the number '1'. In the 'Documentation & Reporting' section, the 'Manager-Employees' link under the 'Active Directory' category is highlighted with a red box and a red circle containing the number '2'.

1. Select "Start".
2. Click on "Manager-Employees".



1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired report settings.
4. Start the report.

## Group memberships and account details

### **Background / Value**

This report provides easy to read group memberships and account details for selected users or groups.

The following account details are shown in the report by default:

- Expiration date of the account
- Display name
- User login name
- Common name
- Defined name
- Email address
- LDAP ADsPath
- Last login
- Object GUID
- Object SID
- SAM Account Name
- SAM Account type
- Group memberships
- Parents + children
- Purpose Group names

### **Related features**

[Report: OU members](#)

## Step-by-step process

The screenshot shows the Access Rights Manager (ARM) web interface. The top navigation bar includes a search box and a user profile for Anthony Admin. Below the navigation bar, there are several menu items: Start, Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, and Status. The 'Start' menu item is highlighted with a red box and a red circle containing the number 1. Below the navigation bar, there are five main sections: HOME, NOTES, REQUESTS, TASKS, and REPORTS. The 'HOME' section is active. Below the main sections, there are several quick links and reports. The 'Account Details' link under the 'Active Directory' section is highlighted with a red box and a red circle containing the number 2.

ARM Access Rights Manager

Start - Home

HOME NOTES REQUESTS TASKS REPORTS

Quick links  
Easy orientation, find the best tool for your productivity in ARM

Permission Analysis

- Where does a user/group have access?

User Provisioning

- Accounts
  - Create new user or group
  - Edit group memberships
- Resources
  - Edit access rights

Security Monitoring

- Active Directory
  - AD Logga Report
- Exchange
  - Exchange Logga Report
- File server
  - Who did what, except authorized users (SoD)?
  - Who did what?
  - Who made changes?

Documentation & Reporting

- Reports overview
- Where has the user/group access?
- Who has access where?
- File server
  - All 'Authenticated users' permissions
  - All 'Everyone' permissions
  - All users with direct access
  - Directories without administrative owners
  - Permission difference
  - Unresolved SIDs
  - Where have employees of a manager access (file server)?
  - Who has access through which permission groups?
- Active Directory
  - Account Details
  - Inactive accounts
  - Local accounts
  - Manager-Employees
  - OU Members and group memberships
  - Users and groups (Kerberos, Last logon)
- Exchange
  - Exchange mailbox permissions

1. Select "Start".
2. Click on "Account Details".

ARM Access Rights Manager

Anthony Admin

### Account Details

**Report configuration**

Title

Comment

**Selected accounts**

Emily Employee (8man-demo\Emily Employee)

Resolve group membership

Translate names of groups to purpose group name

**Settings**

The output format is [PDF](#)

Create report for [all accounts in one](#) document.

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

**Account Details**

Please select users/groups

Search  Filter

Name

- Caroline Berggren (8man-demo\Caroline Berggren)
- Domain Users (8man-demo\Domain Users)
- Emily Employee (8man-demo\Emily Employee)
- Ludvig Karlsson (8man-demo\Ludvig Karlsson)
- Marketing (8man-demo\Marketing)

Cancel Start

1. Enter a title for the report and add a comment.
2. Define the range of the report. Activate the option "Resolve group memberships" to get the memberships listed and resolved in the report.
3. Define the desired output settings.
4. Start the report.

## Find inactive accounts (users or computers)

### Background / Value

Inactive accounts can be used for data theft and manipulation without being detected. Since most inactive accounts are remnants of past employees, they are often a symptom of a communication problem between HR and IT. ARM displays all inactive accounts in Active Directory. You can delete or deactivate old and redundant accounts.

### Related features

[Remove a user and his permissions](#)

["Soft" delete a user account](#)

[Deactivate a user account](#)

[Identify inactive accounts](#) (web client)

[Deactivate user accounts in bulk](#) (web client)



## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard' (highlighted with a red box and a red circle with '1'), 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The left sidebar shows 'Reporting' with 'Active Directory' expanded, where 'Inactive accounts' is highlighted with a red box and a red circle with '2'. Below this is 'File server' with various permission counts. The main content area displays a list of users and groups with their counts:

Category	Count
Users and other accounts	
Users	1169
Users (disabled)	3
Administrators	6
Administrators (disabled)	0
Groups	
All Groups	1660
Groups with members (w/o recursions)	1585
Empty groups	41
Groups in recursions	34
The largest group (Domain Users (8man-demo\Domain Users))	1168
Built-in security groups	29
Global security groups	548
Universal security groups	513
Local security groups	557
Global distribution groups	0
Universal distribution groups	13
Local distribution groups	0
OU / Contacts / More	
Computers	5
Computers (disabled)	0
Contacts	3
Foreign users	0
Organizational Units	45
Top 5 Kerberos Tokens [Bytes]	
User96 (8man-demo\User96)	3144
User70 (8man-demo\User70)	3024
User2 (8man-demo\User2)	2992
User20 (8man-demo\User20)	2084

1. Select "Dashboard".
2. Click on "Inactive accounts".

The screenshot shows the 'Inactive accounts' report configuration dialog in the SolarWinds Access Rights Manager. The dialog is split into two panes. The left pane, 'Report configuration', includes fields for 'Title' and 'Comment', an 'Objects' section with 'Paths' and 'Organizational categories' options, a 'Threshold value (days)' set to 60, a checked 'Exclude deactivated accounts' option, and an 'Inactive Users' dropdown menu. The right pane, 'Inactive accounts', shows a list of resources under 'Active Directory', with '8man-demo.local' selected. A 'Start' button is highlighted in the bottom right corner. Red boxes and numbers 1 through 4 indicate the steps: 1. Title and Comment fields; 2. Objects and Threshold value; 3. Settings section; 4. Start button.

1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired report settings.
4. Start the report.

Days (Difference to current date)							
1	Title	All users of a selected domain					
2	not logged on for a given period.						
3	Comment	-					
4	Author	8MAN-DEMO\cradmin					
5	Used time zone	W. Europe Standard Time (UTC+01:00:00)					
6	Date	2/16/2017 1:02:45 PM					
7	Version	7.6.131.0					
9	Scantime						
10	8man-demo.local	Active Directory		2/14/2017 10:00:03 PM			
12	Configuration						
13		Selected resources:					
14		* 8man-demo.local (DC=8man-demo,DC=local)					
16		Threshold (days): 90					
19	Detected scan problems						
20	No scan errors detected.						
22	Report for	8man-demo.local					
24	Name	Path	Last Logon Timestamp	Days (Difference to current date)			
25	SP_SearchService (8man-demo\SP_SearchService)	CN=SP_SearchService,OU=Service Accounts,DC=8man-demo	5/16/2014 4:37:14 PM	1006			
26	Eric Reid (8man-demo\EReid)	CN=Eric Reid,OU=TestUsers,DC=8man-demo,DC=local	10/10/2014 4:28:02 PM	859			
27	Akbar, Mohammed (8man-demo\Mohammed Akbar)	CN=Mohammed Akbar,OU=TestUsers,DC=8man-demo,DC=local	10/27/2014 9:27:50 AM	843			
28	Quinton Patton (8man-demo\QPatton)	CN=Quinton Patton,OU=TestUsers,DC=8man-demo,DC=local	11/25/2014 3:31:09 PM	813			
29	Adrian Stillwell (8man-demo\AStillwell)	CN=Adrian Stillwell,OU=TestUsers,DC=8man-demo,DC=local	5/27/2015 3:06:13 PM	630			
30	Ali Mente (8man-demo\Ali Mente)	CN=Ali Mente,OU=TestUsers,DC=8man-demo,DC=local	6/24/2015 1:47:33 PM	603			
31	Torrev Smith (8man-demo\TSmith)	CN=Torrev Smith,OU=TestUsers,DC=8man-demo,DC=local	6/24/2015 3:25:49 PM	602			

Review the data in the report. If using historical scan data there may be differences in the days since the last login.

## OU members and group memberships

### Background / Value

ARM allows a quick review of any groups and user contained in an Organizational Unit (OU). This ensures that you can obtain a complete overview of all users and groups within any OU.

### Related features

[Group memberships and account details](#)

### Step-by-step process

The screenshot displays the Access Rights Manager (ARM) web interface. The top navigation bar includes a search box, a settings gear, and the user name 'Anthony Admin'. Below the navigation bar, the 'Start' button is highlighted with a red box and a red circle containing the number '1'. The main content area is divided into several sections: 'Permission Analysis', 'User Provisioning', 'Security Monitoring', 'Documentation & Reporting', 'Active Directory', 'File server', and 'Exchange'. In the 'Active Directory' section, the 'OU Members and group memberships' link is highlighted with a red box and a red circle containing the number '2'. The bottom of the screenshot shows the Windows taskbar with the system tray.

1. Select "Start".
2. Click on "OU members and group memberships".

ARM Access Rights Manager

Anthony Admin

### OU Members and group memberships

**Report configuration**

Title

Comment

**Selected OUs and containers**

Paths  Organizational categories

Demo Users (ou=demo users,dc=8man-demo,dc=local)

Show lower-level OUs and container in report

**Options**

Filter for related objects

**Settings**

The output format is [PDF](#)

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

**Please select resource(s)**

Resources

Active Directory

- 8man-demo.local
  - 8MAN
  - Builtin
  - Computers
  - Contacts
  - Demo Groups
  - Demo Users
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Keys
  - Managed Service Accounts
  - Program Data
  - Recycled Accounts
  - System
  - Test Groups
  - Test Users
  - Users

Cancel Start

1. Enter a title for the report and add a comment.
2. Define the range and the layout of the report.
3. Define the desired output settings.
4. Start the report.

## Users and groups report

### Background / Value

The user and group report shows all users and groups in AD and some of their properties and attributes.

### User accounts

Two key factors shown in this view are the Kerberos token and last logon timestamp. The latter shows you the last login of the AD accounts on your network, across all domain controllers.

The size of the Kerberos token is an expression of the number of group memberships. Many group memberships indicate the possibility of excessive and / or redundant access rights. If the maximum size of 64KB is exceeded, it is no longer possible for the user to log into the network.

In addition the following information is also displayed:

- Account expiry date
- Password expires yes/no
- Admin account yes/no

### Groups

Displays direct and indirect group membership count as well as group scope (local, global, universal)

### Step-by-step process

ARM Access Rights Manager

Search

Anthony Admin

Start Resources Permissions Accounts **Dashboard** Multiselection Logbook Scan comparison Status

### Reporting

- Active Directory
  - Inactive accounts
  - Local accounts
  - Users and groups (Kerberos, Last logon)**
- File server
  - All 'Authenticated users' permissions 3
  - All 'Everyone' permissions 1
  - All users with direct access 16
  - Directories without administrative owners 49
  - Unresolved SIDs

### Depth of nested groups

Depth	Count
1	1564
2	11
3	3
4	2
5	1
6	1
7	1

### Users and other accounts

Users	1169
Users (disabled)	3
Administrators	6
Administrators (disabled)	0

### Groups

All Groups	1660
Groups with members (w/o recursions)	1585
Empty groups	41
Groups in recursions	34
The largest group (Domain Users (8man-demo\Domain Users))	1168
Built-in security groups	29
Global security groups	548
Universal security groups	513
Local security groups	557
Global distribution groups	0
Universal distribution groups	13
Local distribution groups	0

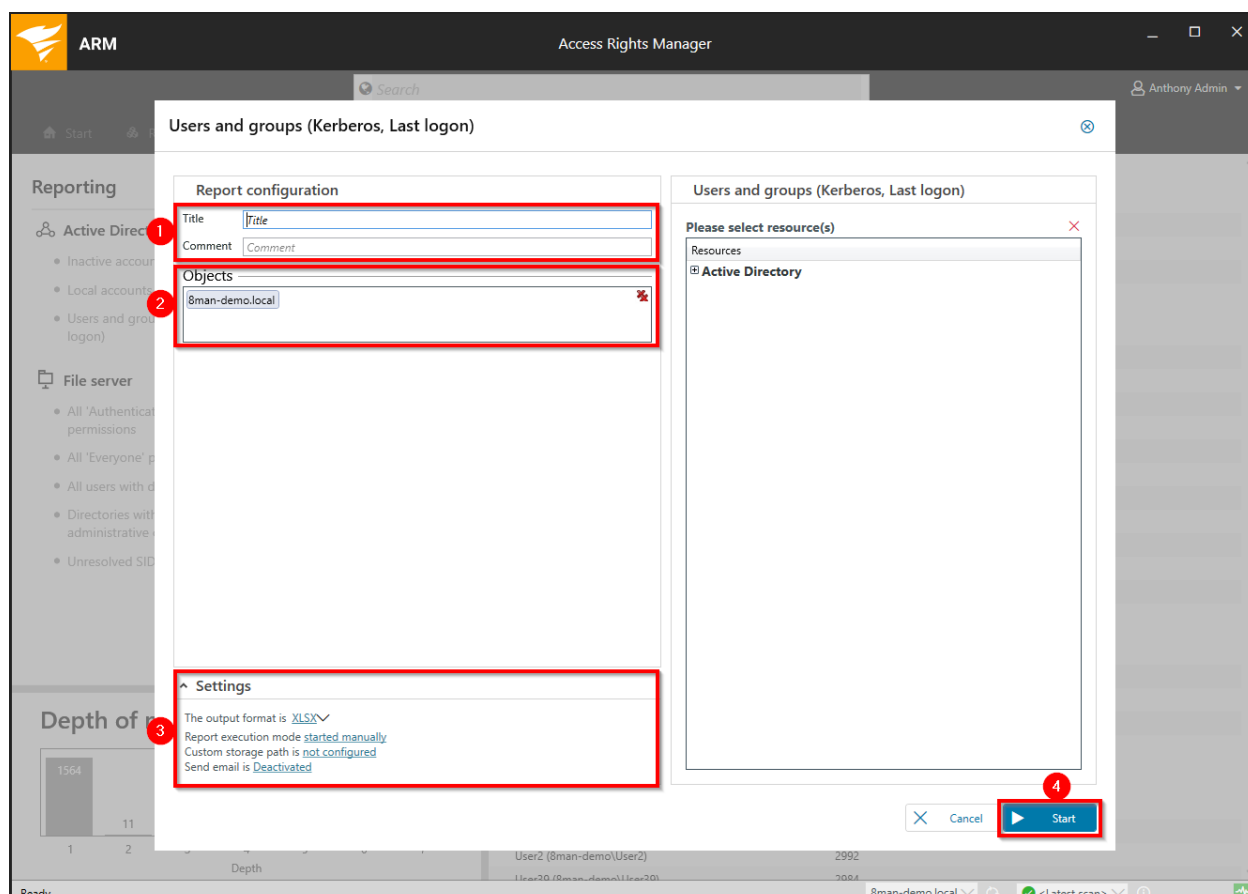
### OU / Contacts / More

Computers	5
Computers (disabled)	0
Contacts	3
Foreign users	0
Organizational Units	45

### Top 5 Kerberos Tokens [Bytes]

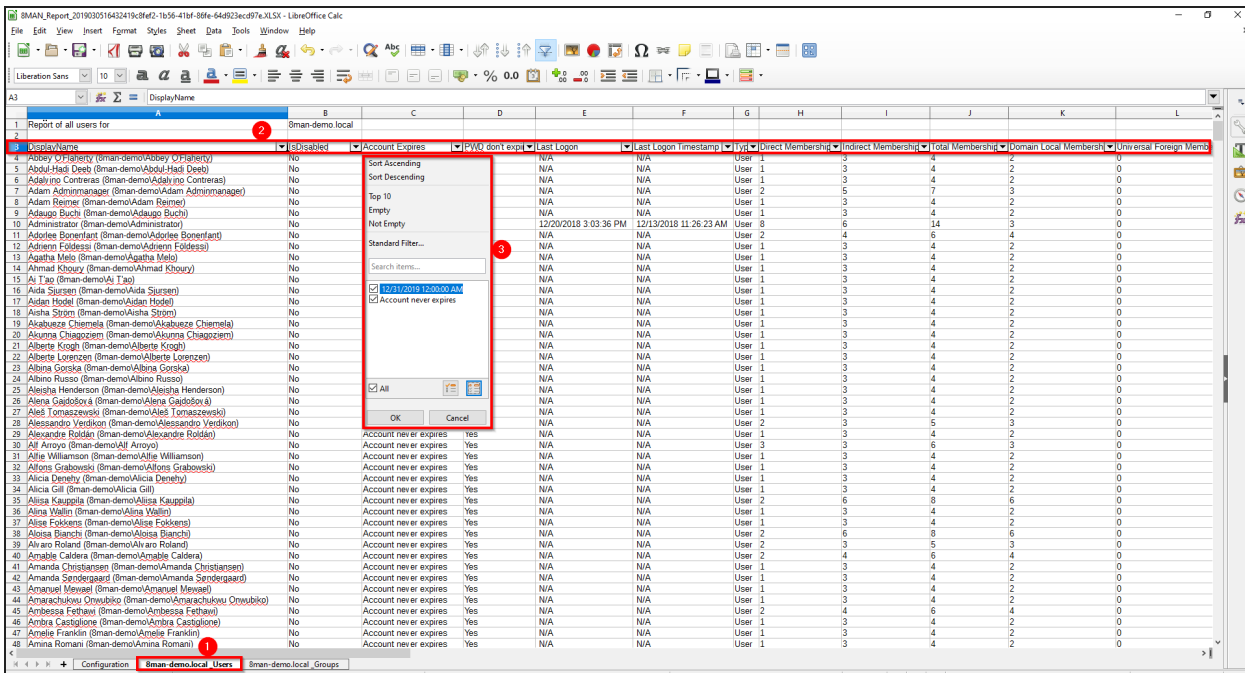
User96 (8man-demo\User96)	3144
User70 (8man-demo\User70)	3024
User2 (8man-demo\User2)	2992
User20 (8man-demo\User20)	2084

1. Select "Dashboard".
2. Click on "Users and groups".



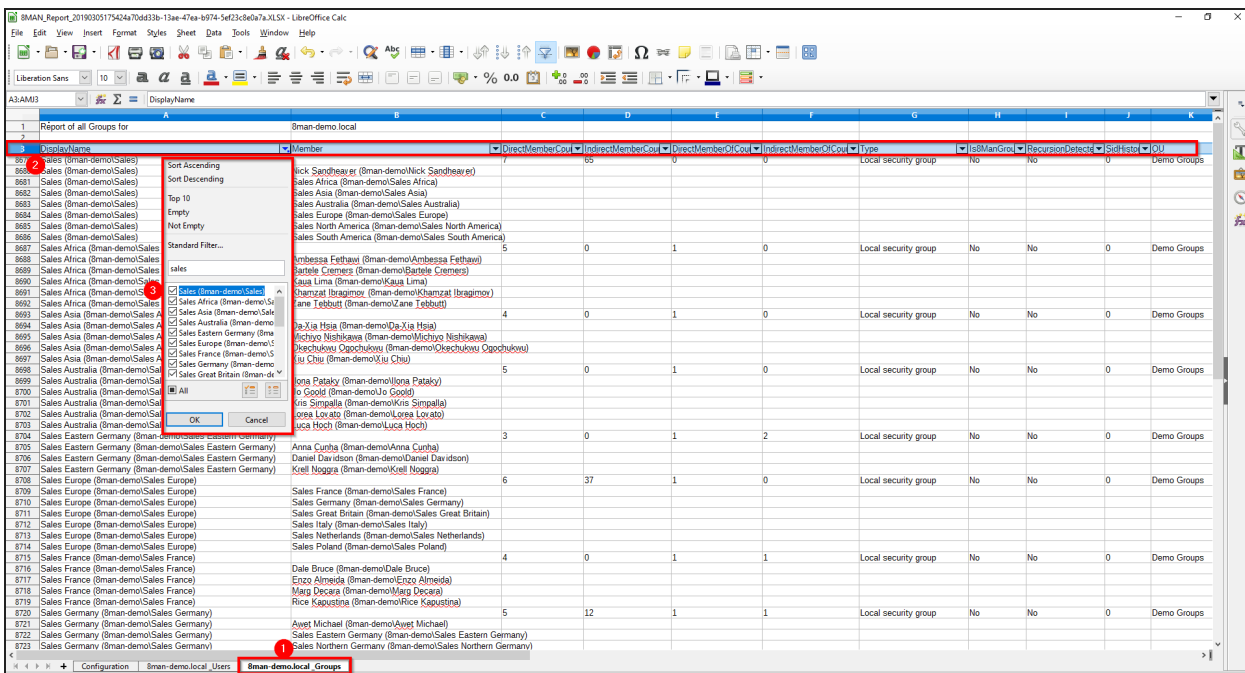
1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired output settings.
4. Start the report.





Open the report in your spreadsheet application.

1. Select the "users" tab.
2. We recommend to apply an auto filter to row 3.
3. Use the auto filter to analyze the user structure, for example to look for expiring accounts.




1. Select the "groups" tab.

2. We recommend to apply an auto filter to row 3.
3. Use the auto filter to analyze the group structure.

## Report on local accounts

### Background / Value

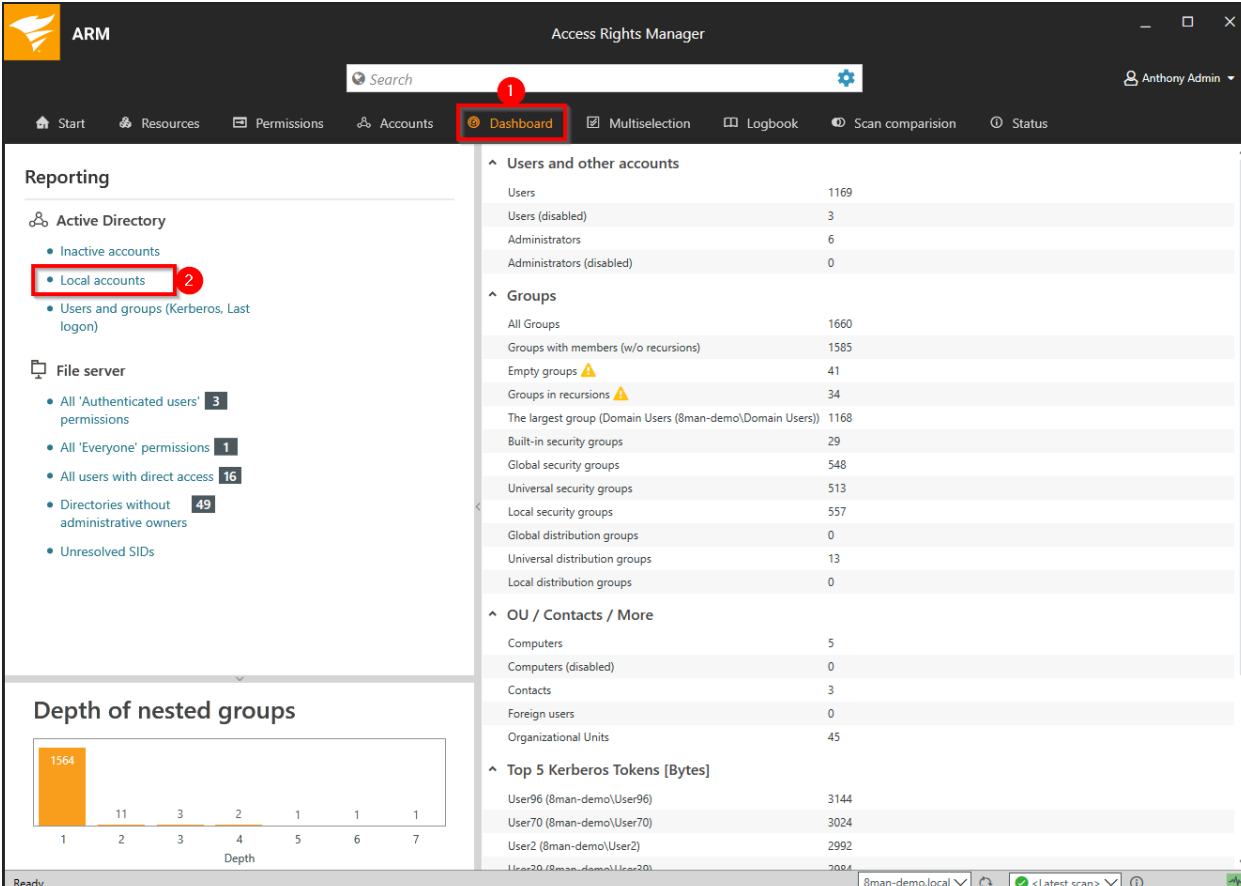
The local account report displays local administrative rights on end points. This way you can see which administrators and users have access to which end point. In this scenario the principle of "least privilege" applies. The report thereby gives you a complete picture regarding access rights in your organization as local accounts are not visible through AD group memberships.

 This report can only show results if you have [configured local accounts scans](#).

### Related features

[Scan local accounts](#) (configuration)

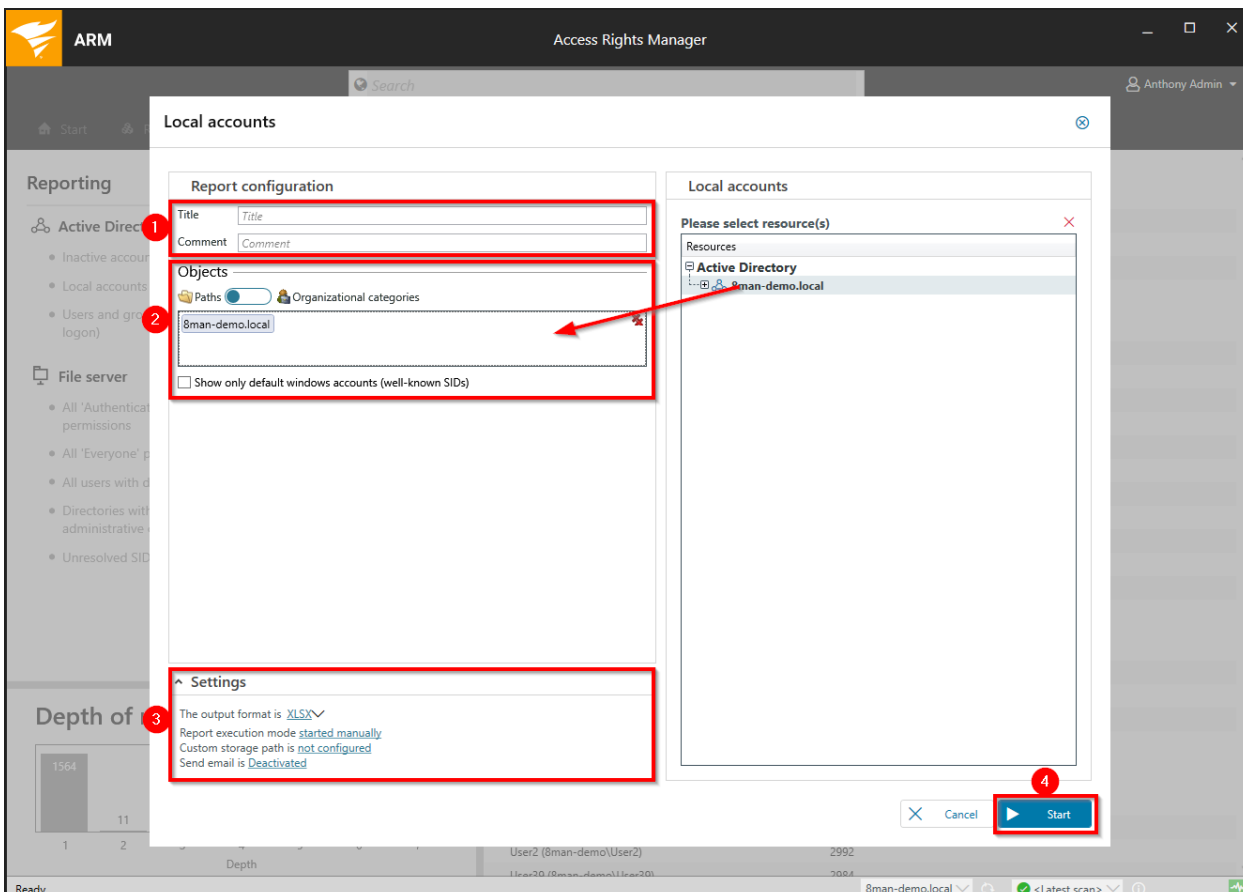
### Step-by-step process



The screenshot shows the Access Rights Manager (ARM) interface. The 'Dashboard' menu item is highlighted with a red box and a red circle containing the number '1'. Below it, in the 'Reporting' section, the 'Local accounts' item is highlighted with a red box and a red circle containing the number '2'. The main content area displays a table of account statistics:

Category	Count
<b>Users and other accounts</b>	
Users	1169
Users (disabled)	3
Administrators	6
Administrators (disabled)	0
<b>Groups</b>	
All Groups	1660
Groups with members (w/o recursions)	1585
Empty groups	41
Groups in recursions	34
The largest group (Domain Users (8man-demo\Domain Users))	1168
Built-in security groups	29
Global security groups	548
Universal security groups	513
Local security groups	557
Global distribution groups	0
Universal distribution groups	13
Local distribution groups	0
<b>OU / Contacts / More</b>	
Computers	5
Computers (disabled)	0
Contacts	3
Foreign users	0
Organizational Units	45
<b>Top 5 Kerberos Tokens [Bytes]</b>	
User96 (8man-demo\User96)	3144
User70 (8man-demo\User70)	3024
User2 (8man-demo\User2)	2992
User20 (8man-demo\User20)	2084

1. Select "Dashboard".
2. Click on "Local accounts".



1. Enter a title for the report and add a comment.
2. Define the range of the report.

**i** You can select a whole domain. The report will contain local computer accounts only.

3. Define the desired output settings.
4. Start the report.

## Organizational help for administrators

Besides automated documentation and reports ARM also includes a number of additional documentation features. These allow you to add post-its to objects manually or give AD groups aliases with the "purpose groups" feature.

Add notes to user accounts and groups

### Background / Value

Flag user and group accounts with post-its. This allows you to add tasks directly to individual objects.

### Step-by-step process

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The 'Accounts' tab is selected in the top navigation bar. The main area shows a 'Graph' view with a tree view on the left and a context menu open over the 'Emily Employee' account. The context menu includes options like 'Select account', 'Show in Resources View...', 'Report: Account Details', and 'Add note'. The 'Add note' option is highlighted with a red box. The right-hand pane shows the 'Attributes' for the 'Emily Employee' account, including fields like Name, Account Expires, Common Name, and Email Address.

Right-click on an account and select "Add note" from the context menu.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. A modal dialog box titled "Add new note" is open, featuring a text input field containing "My special demo note." and a profile picture of a man. A red circle with the number "1" is positioned above the input field, and another red circle with the number "2" is positioned above the "Add" button. The background shows a graph view of the user "Emily Employee (8man-demo\...)" with various attributes and a tree view on the left.

1. Add a note.
2. Click "Add".

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. At the top, there is a navigation bar with a search bar and a user profile for 'Anthony Admin'. Below the navigation bar, there are several icons for navigation: 'HOME', 'NOTES', 'REQUESTS', 'TASKS', and 'REPORTS'. The 'NOTES' icon is highlighted with a red box and a red circle with the number '2'. In the top left corner of the navigation bar, the 'Start' button is highlighted with a red box and a red circle with the number '1'. The main content area is divided into several sections: 'Permission Analysis', 'User Provisioning', 'Security Monitoring', 'Documentation &amp; Reporting', 'Active Directory', 'File server', and 'Exchange'. Each section contains a list of links related to that section. The 'Start' button is located in the top left corner of the navigation bar. The 'NOTES' icon is located in the top right corner of the navigation bar. The 'HOME' icon is located in the top left corner of the main content area. The 'REQUESTS', 'TASKS', and 'REPORTS' icons are located in the top right corner of the main content area. The 'Permission Analysis' section contains a link 'Where does a user/group have access?'. The 'User Provisioning' section contains links for 'Accounts' (Create new user or group, Edit group memberships) and 'Resources' (Edit access rights). The 'Security Monitoring' section contains links for 'Active Directory' (AD Logga Report) and 'Exchange' (Exchange Logga Report). The 'Documentation &amp; Reporting' section contains links for 'Reports overview', 'Where has the user/group access?', and 'Who has access where?'. The 'Active Directory' section contains links for 'Account Details', 'Inactive accounts', 'Local accounts', 'Manager-Employees', 'OU Members and group memberships', and 'Users and groups (Kerberos, Last logon)'. The 'File server' section contains links for 'All \"/&gt;

1. Select "Start".
2. Click "Notes".

The screenshot shows the ARM interface with a navigation bar at the top containing 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The main content area is titled 'Start - Notes' and includes a search bar and a user profile for 'Anthony Admin'. Below this is a section for 'Your ARM notepad' with a table of notes. A right-click context menu is displayed over a note, listing the following actions:

- Show in accounts view...
- Change group memberships...
- Unlock user
- Deactivate account
- Change password options
- Reset user password
- Soft delete user account
- Delete account
- Edit attributes
- Delete note

The list shows all notes. With a right click on the note, you can trigger a number of different functions.

Purpose Groups: Give aliases to groups

## Background / Value

Purpose groups add clear descriptions to AD groups. Often these groups have very technical names and so it is difficult for users or administrators to tell what the purpose of an AD group is. Adding aliases makes the picture much clearer.

**i** The alias descriptions are only visible in the ARM views and reports. There are no changes to Active Directory attributes.



Create a purpose group

## Step-by-step process

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main window is titled 'Graph' and shows a hierarchical tree of Active Directory objects. The root node is '8man-demo complete (8man-demo \8man-demo complete)' with 11 children. Below it is 'C-Level (8man-demo)\C-Level' with 7 children. Two child nodes are visible: 'David DO Finance (8man-demo)\David DO Finance' and 'David DO HR (8man-demo)\HR', each with 3 children. A context menu is open over the 'C-Level' node, listing various actions. The 'Create Purpose Group' option is highlighted with a red box. The right-hand pane shows the 'Attributes' tab for the selected 'C-Level' group, displaying a table of attributes and their values.

Name	Value
Common Name	C-Level
Distinguished Na...	CN=C-Level,OU=Distribution Gr...
Group Type	Universal distribution group
Name (RDN)	C-Level
Object GUID	e752ddfe-d559-4845-8ae2-b351...
Object SID	S-1-5-21-608906640-321788923...
SAM Account Na...	C-Level
SAM Account Type	(268435457) Group Object (non...
Organizational U...	OU=Distribution Groups,OU=De...
Organizational U...	Distribution Groups

Right-click on an AD group. Select "Create Purpose Group" from the context menu.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. A 'Create Purpose Group' dialog box is open, allowing the user to create a new AD group. The dialog has the following fields and buttons:

- Title:** C-Level (8man-demo\C-Level)
- Alias:** Management
- Description:** This group is for managers only
- Buttons:** Close, Create

The background shows a graph view of the AD group hierarchy. The 'C-Level (8man-demo\C-Level)' group is selected, and its children are visible: 'David DO Finance (8man-demo\David DO Finance)', 'David DO HR (8man-demo\David DO HR)', and 'David DO Manager (8man-demo\David DO Manager)'. The 'Create' button is highlighted with a red box and a red circle with the number 2. A red circle with the number 1 is next to the 'Description' field.

1. Give the AD group an alias and add a description for the group.
2. Click on "Create".

## Delete or modify a purpose group

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The 'Resources' tab is active, displaying a list of resources. The 'Purpose Groups' folder is expanded, and the 'C-Level (8man-demo\C-Level)' group is selected. A context menu is open over this group, with 'Delete Purpose Group' and 'Modify Purpose Group' highlighted. The right pane shows the attributes of the selected group, including Name, Value, and Object SID.

Name	Value
Common Name	C-Level
Distinguished Name	CN=C-Level,OU=Distribution Groups,OU=Demo Gr...
Group Type	Universal distribution group
Name (RDN)	C-Level
Object GUID	e752ddfe-d559-4845-8ae2-b3514e73846d
Object SID	S-1-5-21-608906840-321788923-2728258956-3199
SAM Account Name	C-Level
SAM Account Type	(268435457) Group Object (non security)
Organizational Unit path (par...	OU=Distribution Groups,OU=Demo Groups,DC=8m...
Organizational Unit (parent)	Distribution Groups

1. Select "Resources".
2. Expand "Purpose Groups".
3. Select the desired purpose group by right-clicking on it.
4. Select "Delete Purpose Group" or "Modify Purpose Group" from the context menu.

**i** The removal process only affects the purpose group, the added alias in ARM. No changes are made to Active Directory.

## File server

ARM lets you create easy to read reports on file server permissions and security risks.

### Where do employees of a manager have access?

#### Background / Value

ARM includes a special data owner report for file servers. In it, the managers stored in the Active Directory (users with the "Manager" attribute set) are related to the resources stored in the Data Owner configuration.

#### Step-by-step process

The screenshot shows the ARM web interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. Below the navigation bar, there are icons for HOME, NOTES, REQUESTS, TASKS, and REPORTS. The main content area is divided into sections: Permission Analysis, User Provisioning, Security Monitoring, and Documentation & Reporting. The 'Start' button is highlighted with a red box and a '1'. In the 'Documentation & Reporting' section, under 'File server', the link 'Where have employees of a manager access (file server)?' is highlighted with a red box and a '2'.

1. Select "Start".
2. Click on "Where have employees of a manager access (file server)" .

The screenshot shows the 'Where have employees of a manager access (file server)?' report configuration dialog in the SolarWinds Access Rights Manager (ARM) interface. The dialog is divided into two panes. The left pane contains the 'Report configuration' and 'Settings' sections. The right pane contains the 'Please select managers' and 'Disabled manager accounts' sections. Red boxes and numbers 1-4 highlight key steps:

- 1:** Title and Comment fields in the Report configuration section.
- 2:** Selected managers section, including radio buttons for 'Everyone', 'Authenticated users', 'Domain users', and 'NTFS only', and a link 'Please click here to select accounts'.
- 3:** Settings section, including options for output format (PDF), execution mode (started manually), storage path (not configured), and email (Deactivated).
- 4:** Start button at the bottom right of the dialog.

1. Enter a title for the report and add a comment.
2. Define the range of the report. You are only able to add users where the manager attribute has been set and which have a valid Data Owner configuration.
3. Define the desired report settings.
4. Start the report.

## Who has access through which permission groups?

### Background / Value

The report "Who has access through which permission groups?" shows the groups that give access to the selected resource and the users that are members of said groups.

Instead of analyzing individual directories you could also use Organizational Categories of the Data Owner configuration.

### Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and several menu items: Start, Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, and Status. The 'Start' button is highlighted with a red box and a red circle containing the number '1'. Below the navigation bar, there are five main sections: HOME, NOTES, REQUESTS, TASKS, and REPORTS. The 'Quick links' section provides easy orientation. The 'Permission Analysis' section includes a link to 'Where does a user/group have access?'. The 'User Provisioning' section includes links for 'Accounts' (Create new user or group, Edit group memberships) and 'Resources' (Edit access rights). The 'Security Monitoring' section includes links for 'Active Directory' (AD Logga Report) and 'Exchange' (Exchange Logga Report). The 'File server' section includes links for 'Who did what, except authorized users (SoD)?', 'Who did what?', and 'Who made changes?'. The 'Documentation & Reporting' section includes a 'Reports overview' with a red circle containing the number '1', and a list of reports: 'Where has the user/group access?', 'Who has access where?', 'Active Directory' (Account Details, Inactive accounts, Local accounts, Manager-Employees, OU Members and group memberships, Users and groups (Kerberos, Last logon)), 'Exchange' (Exchange mailbox permissions), 'File server' (All 'Authenticated users' permissions, All 'Everyone' permissions, All users with direct access, Directories without administrative owners, Permission difference, Unresolved SIDs, Where have employees of a manager access (file server)?), and 'Who has access through which permission groups?' which is highlighted with a red box and a red circle containing the number '2'.

1. Select "Start".
2. Click on "Access Rights Groups".

The screenshot displays the SolarWinds Access Rights Manager (ARM) web interface. At the top, the title bar reads "ARM Access Rights Manager" with a search bar and the user "Anthony Admin". The main navigation bar includes "Start", "Resources", "Permissions", "Accounts", "Dashboard", "Multiselection", "Logbook", "Scan comparison", and "Status". Below this, a "Start - Home" section contains icons for "HOME", "NOTES", "REQUESTS", "TASKS", and "REPORTS". A "Quick links" section follows. The central focus is a modal dialog box titled "Report: Who has access through which permission groups?". The dialog has a "Title" field (marked with a red '1'), a "Comment" field (marked with a red '2'), and radio buttons for "Paths" (marked with a red '3') and "Organizational categories". A "Show details >" link is also present (marked with a red '4'). At the bottom of the dialog are "Cancel" and "Start" buttons. The background interface shows a "Security Monitoring" section with options for "Active Directory" and "Exchange".

1. Enter a title for the report and add a comment.
2. Define whether the report is organized by individual directories or by organizational categories from the Data Owner configuration.
3. Define the range of the report.
4. Click on "Show details".

**Report: Who has access through which permission groups?**

Title:

Comment:

Paths:  Organizational categories:

Report execution mode: **started manually**

« Hide details

1. **2** Directory levels to resolve under the selected paths  Include selected first level directory

Only directories with changed rights

Use the list of groups, whose members shall not be resolved

Show paths with: Path names  Generic names: 01\_01\_01\_02

Show groups with: Group names  Tag

**Permission groups to report**

	F	M	E	R	W	L	Propagation	Tag
<input type="checkbox"/> Full control	✓	✓	✓	✓	✓	✓	fc	fc
<input checked="" type="checkbox"/> Modify	✓	✓	✓	✓	✓	✓	md	md
<input type="checkbox"/> Read & execute	✓	✓	✓	✓	✓	✓	re	re
<input checked="" type="checkbox"/> Read	✓	✓	✓	✓	✓	✓	r	r
<input type="checkbox"/> Write	✓	✓	✓	✓	✓	✓	w	w
<input type="checkbox"/> List folder contents	✓	✓	✓	✓	✓	✓	ld	ld
<input type="checkbox"/> Traverse folder	✓	✓	✓	✓	✓	✓	ldtf	ldtf
<input type="checkbox"/> Special permissions							sp	sp

**Quick info**

Use path names as column title. The group names will be inserted below.

Report output preview:

	\\b-hadoop\lham\lham	\\b-hadoop\lham\lham	\\b-hadoop\lham\lham	\\b-hadoop\lham\lham
Remutzer 1				
Remutzer 2				
Remutzer 3				

2.   3.

1. To keep the report concise and meaningful, we recommend limiting the number of directory levels.
2. Add more filters and properties to specify the report further.
3. Start the report.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
1	Data Owner's organizational category: Not configured																						
2	Title Demo																						
3	Author 8MAN-DEMO\cradmin																						
4	Date 2/20/2017 10:29																						
5	Comment																						
6																							
7	1 01_01																						
8	md md r md r md r md r md r md r md r md r md r md r md r md r md r md r md																						
9	Adam Administrator	Administrator, Adam (Adam Administrat	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
10	ABoone	Alex Boone (ABoone)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
11	ATime	Anny Time (ATime)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
12	ADavis	Anthony Davis (ADavis)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
13	CCook	Chris Cook (CCook)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
14	EReid	Eric Reid (EReid)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
15	Frank Gore	Gore, Frank (Frank Gore)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
16	JWard	Jimmy Ward (JWard)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
17	JBennett	John Bennett (JBennett)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
18	JThompson	John Thompson (JThompson)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
19	Gareth Jones	Jones, Gareth (Gareth Jones)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
20	Amanda Lynn	Lynn, Amanda (Amanda Lynn)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
21	Mary Chen	Mary Chen	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
22	MBaars	Michael Baars (MBaars)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
23	Patrick.Willis	Patrick Willis (Patrick.Willis)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
24	QPatton	Quinton Patton (QPatton)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
25	RPatrick	Robert Patrick (RPatrick)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
26	TSmith	Torrey Smith (TSmith)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
27																							
28	1 \\srv-8man\Organization																						
29	01_01	\\srv-8man\Organization\Finances																					
30	01_01_01	\\srv-8man\Organization\Finances\Accounts Payable																					

The report contains a list of all user accounts and file server paths, as well as the corresponding access rights groups.

## Report on direct permissions

### Background / Value

Direct access rights should be avoided at all costs and be replaced by group access rights. Firstly, direct access rights are inefficient because every user has to be managed independently. Secondly, each directory needs to be examined individually to ensure the removal of all direct permissions. ARM shows you all direct permissions on your file server(s) in one simple report.

### Related features

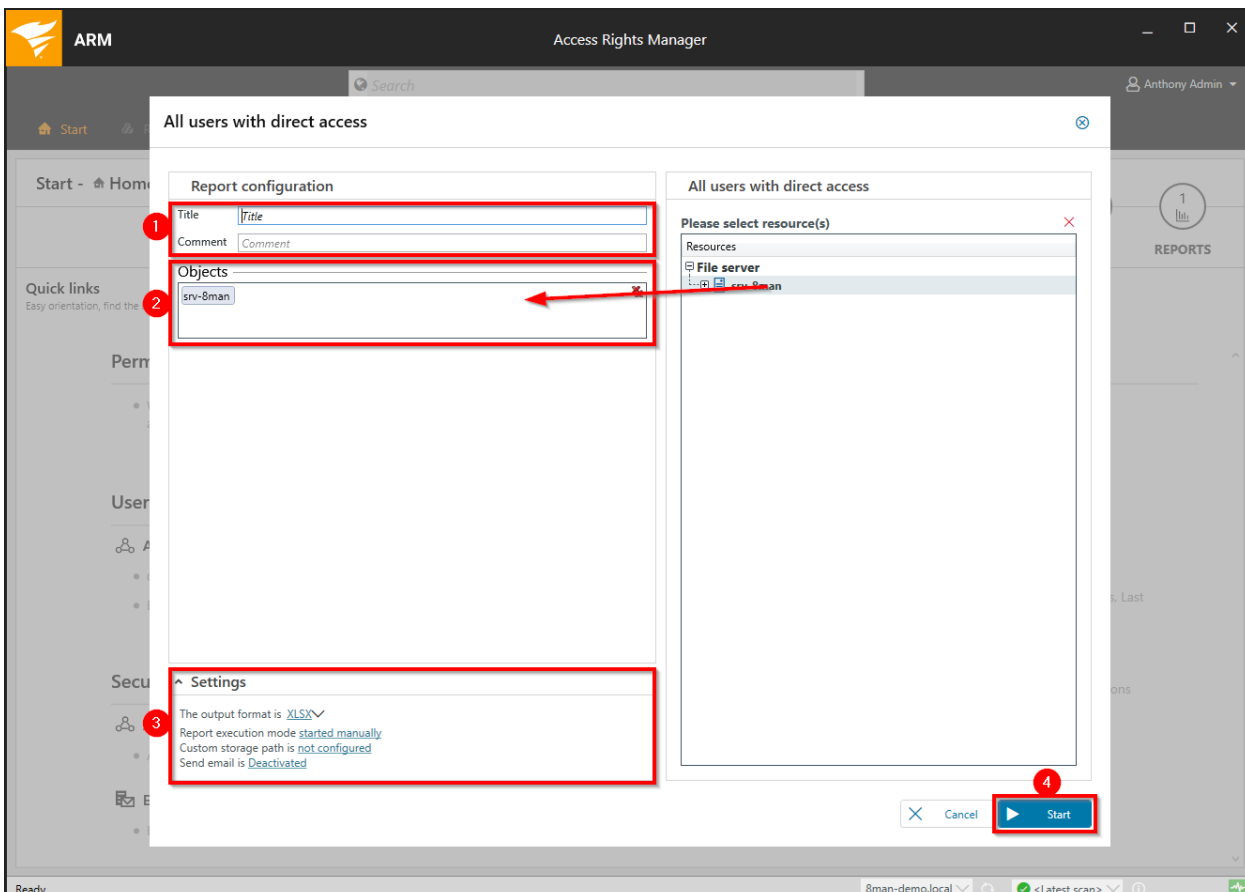
[Remove direct permissions](#) (rich client)

[Remove direct permissions in bulk](#) (web client)

### Step-by-step process

The screenshot shows the ARM web interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The 'Start' button is highlighted with a red box and a '1' in a red circle. Below the navigation bar, there are icons for HOME, NOTES, REQUESTS, TASKS, and REPORTS. The main content area is divided into sections: 'Permission Analysis', 'User Provisioning', 'Security Monitoring', and 'Documentation & Reporting'. The 'Documentation & Reporting' section is further divided into 'Active Directory', 'File server', and 'Exchange'. Under 'File server', the link 'All users with direct access' is highlighted with a red box and a '2' in a red circle.

1. Select "Start".
2. Click on "All users with direct access".



1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired report settings.
4. Start the report.

Path	User name	Right	Dir?
\\srv-8man\Organization\Marketing\Elyse	Emily Employee (8man-demo\Emily Employee)	Modify	
\\srv-8man\Organization\Marketing\Elyse\2016	Emily Employee (8man-demo\Emily Employee)	Modify	
\\srv-8man\Organization\Marketing\Elyse\2017	Emily Employee (8man-demo\Emily Employee)	Modify	
\\srv-8man\Organization\Marketing\Elyse\2018	Emily Employee (8man-demo\Emily Employee)	Modify	
\\srv-8man\Organization\Marketing\Press	Emily Employee (8man-demo\Emily Employee)	Modify	
\\srv-8man\Organization\Sales\Europe\Germany\Eastern Germany	Anna Cupiga (8man-demo\Anna Cupiga)	Read & execute	
\\srv-8man\Organization\Sales\Europe\Germany\Public Sector Contracting Authorities\Layer 1\Layer 2\Layer 3	Ayvet Michael (8man-demo\Ayvet Michael)	Read & execute	
\\srv-8man\Organization\Sales\Europe\Germany\Southern Germany	Hagos Abbaalon (8man-demo\Hagos Abbaalon)	Read & execute	
\\srv-8man\Organization\Sales\Europe\Germany\Western Germany	Julja Rasmussen (8man-demo\Julja Rasmussen)	Read & execute	
\\srv-8man\Projects\Project X	Nick Sandhearer (8man-demo\Nick Sandhearer)	Modify	
\\srv-8man\Projects\Project X	Elyne Koop (8man-demo\Elyne Koop)	Modify	
\\srv-8man\Projects\Project X\Budget	Elyne Koop (8man-demo\Elyne Koop)	Modify	
\\srv-8man\Projects\Project X\Budget	Nick Sandhearer (8man-demo\Nick Sandhearer)	Modify	
\\srv-8man\Projects\Project X\Members	Elyne Koop (8man-demo\Elyne Koop)	Modify	
\\srv-8man\Projects\Project X\Members	Nick Sandhearer (8man-demo\Nick Sandhearer)	Modify	
\\srv-8man\Projects\Project X\Members\Memberlist 1	Per Abelsen (8man-demo\Per Abelsen)	Read & execute	
\\srv-8man\Projects\Project X\Members\Memberlist 1	Melanie Abend (8man-demo\Melanie Abend)	Read & execute	
\\srv-8man\Projects\Project X\Members\Memberlist 2	Per Abelsen (8man-demo\Per Abelsen)	Read & execute	
\\srv-8man\Projects\Project X\Members\Memberlist 2	Melanie Abend (8man-demo\Melanie Abend)	Read & execute	
\\srv-8man\Projects\Project X\Members\Memberlist 3	Per Abelsen (8man-demo\Per Abelsen)	Read & execute	
\\srv-8man\Projects\Project X\Members\Memberlist 3	Melanie Abend (8man-demo\Melanie Abend)	Read & execute	
\\srv-8man\Projects\Project X\Project plan	Elyne Koop (8man-demo\Elyne Koop)	Modify	
\\srv-8man\Projects\Project X\Project plan	Nick Sandhearer (8man-demo\Nick Sandhearer)	Modify	

Open the report in your spreadsheet application. ARM lists all directories with direct access rights.

## Report on unresolved SIDs

### Background / Value

SIDs (Security Identifiers) are character strings that are used to identify user and group accounts in Active Directory. SIDs become unresolved when users or groups with direct access rights are deleted in AD. By using unresolved SIDs insider threats can gain access to sensitive resources.

ARM clearly identifies unresolved SIDs in your system.

### Related features

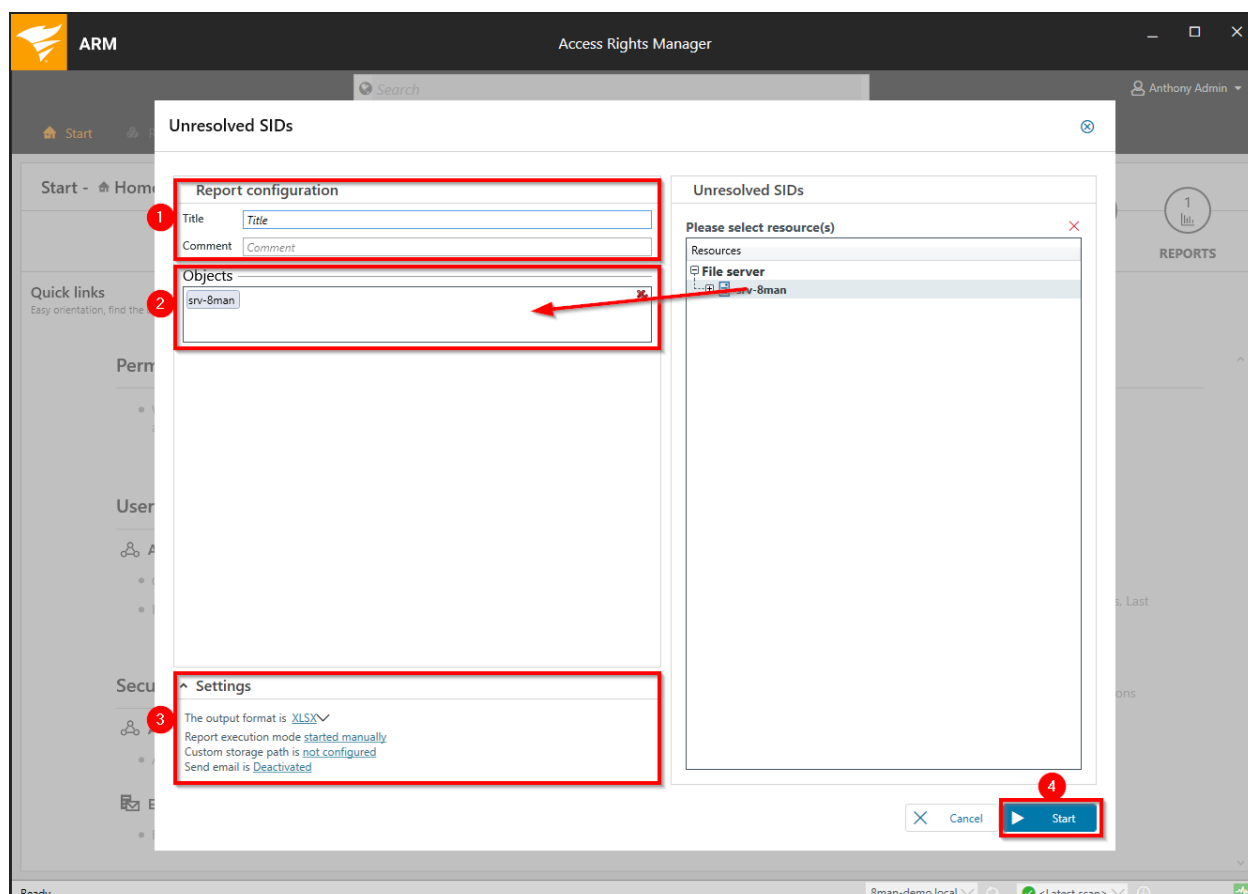
[Identify and delete unresolved SIDs](#) (rich client)

[Remove unresolved SIDs in bulk](#) (web client)

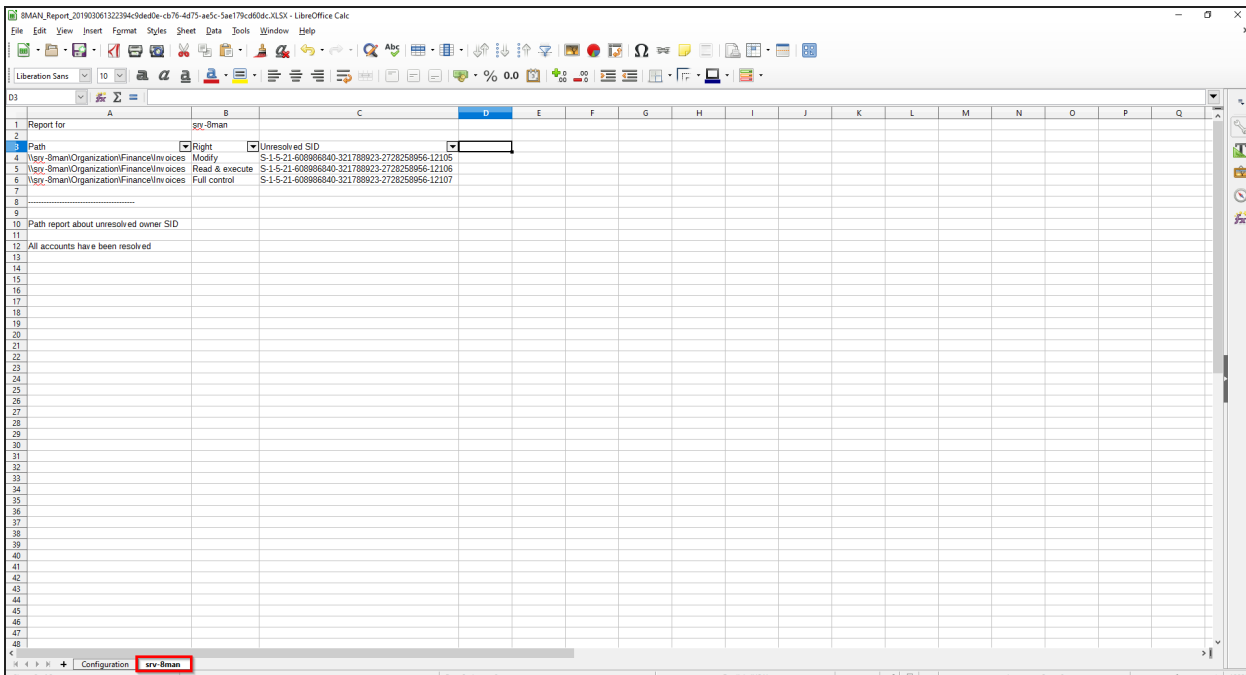
### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) web interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main content area is divided into several sections: 'Permission Analysis', 'User Provisioning', 'Security Monitoring', and 'Documentation & Reporting'. The 'Start' button in the top navigation bar is highlighted with a red box and a '1' in a red circle. In the 'Documentation & Reporting' section, the 'Unresolved SIDs' link is highlighted with a red box and a '2' in a red circle.

1. Select "Start".
2. Click on "Unresolved SIDs".



1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired output settings.
4. Start the report.



Path	Right	Unresolved SID
\\srv-brman\Organization\Finance\Invoices	Modify	S-1-5-21-608986840-321788923-2728258966-12105
\\srv-brman\Organization\Finance\Invoices	Read & execute	S-1-5-21-608986840-321788923-2728258966-12108
\\srv-brman\Organization\Finance\Invoices	Full control	S-1-5-21-608986840-321788923-2728258966-12107

Open the report in your spreadsheet application.

The report lists all unresolved SIDs.

## Report on the usage of "everyone"

### Background / Value

If the "Everyone" account is used for the assignment of access rights, (almost) everyone has access to the connected resources. The consequence is an excessive assignment of access rights and a high probability for unauthorized access. ARM displays all access rights for the "Everyone" account. These go against the principle of least privilege and should therefore not be used.

You can remove "Everyone Permissions" in bulk in the ARM Web Client. Before you remove the permissions, you should assign specific group permissions to the corresponding resources.

### Related features

Also keep an eye on the critical [Authenticated Users](#).

[Identify globally accessible directories](#) (web client)

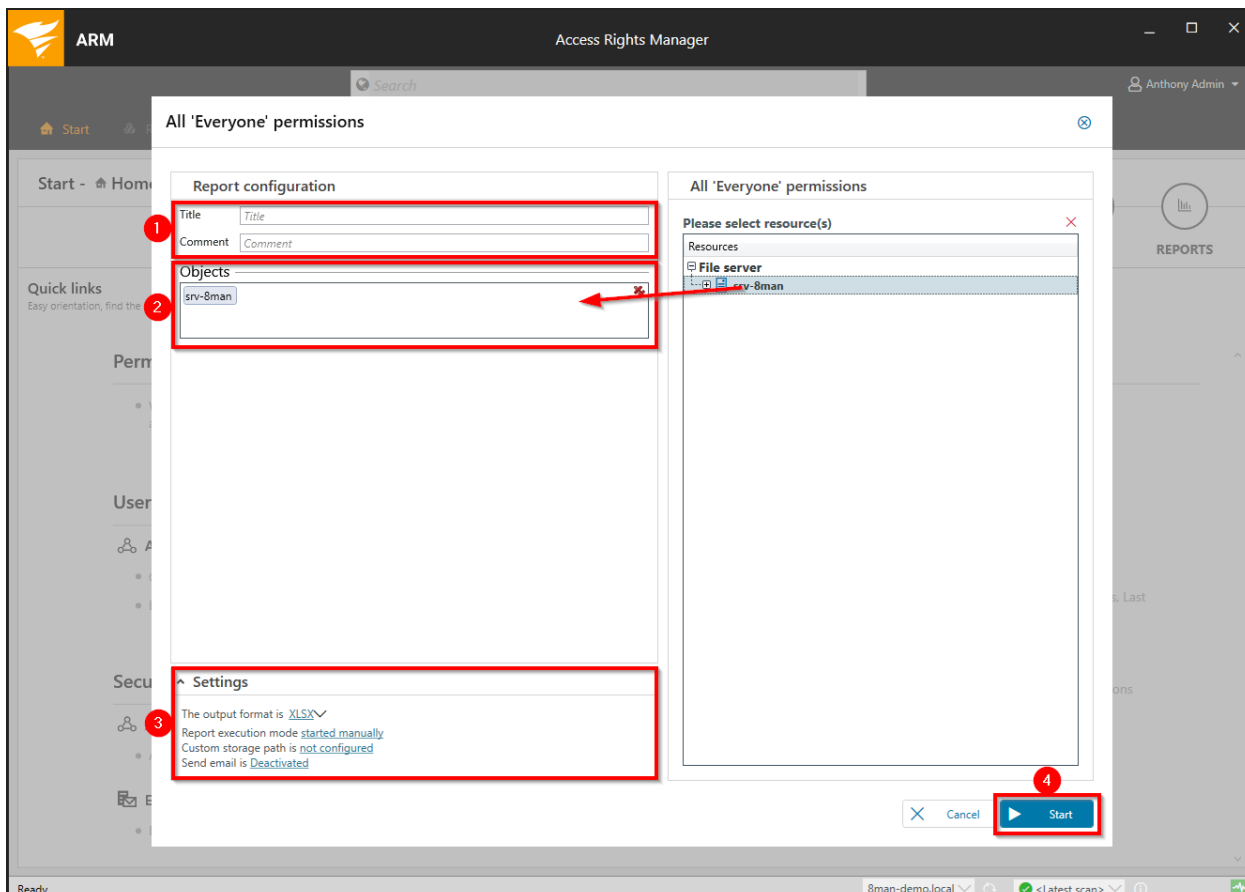
[Remove "everyone" permissions in bulk](#) (web client)



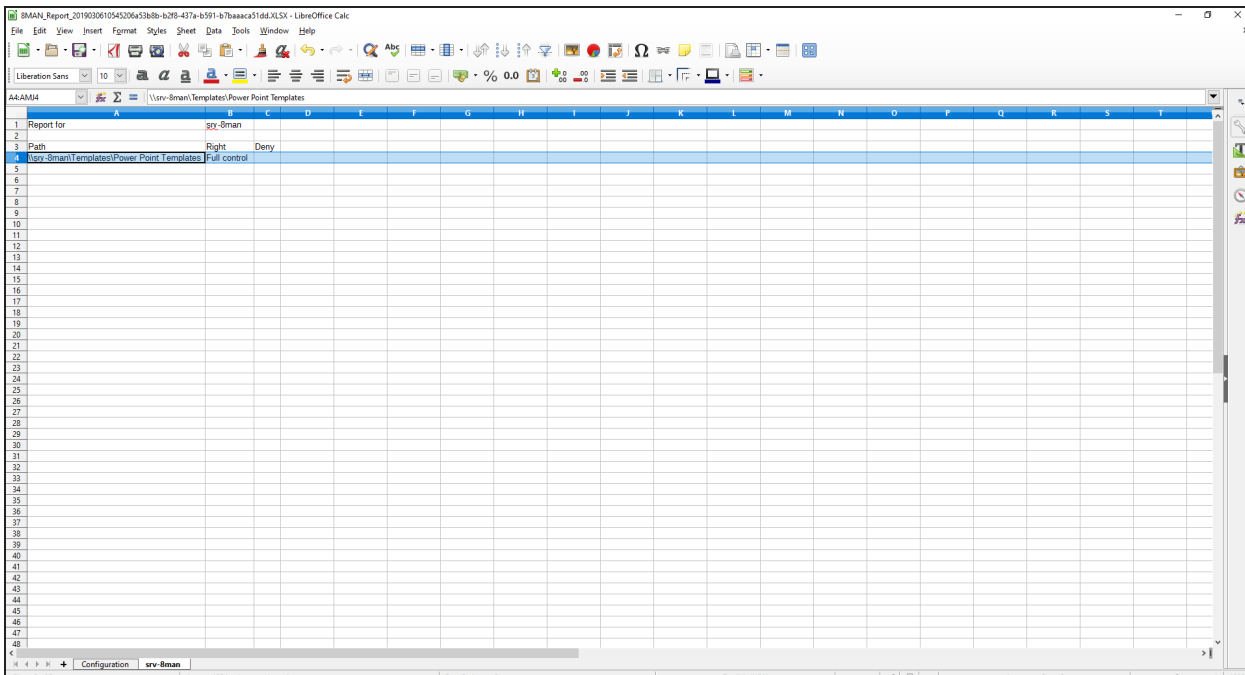
## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main content area is divided into several sections: Permission Analysis, User Provisioning, Security Monitoring, and Documentation & Reporting. The 'Start' button in the top navigation bar is highlighted with a red box and a red circle containing the number 1. In the 'Documentation & Reporting' section, the 'All 'Everyone' permissions' link under the 'File server' category is highlighted with a red box and a red circle containing the number 2.

1. Select "Start".
2. Click on "All 'Everyone' permissions".



1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired report settings.
4. Start the report.



The screenshot shows a spreadsheet application window titled "BMAN\_Report\_2019030610545206a5388b-b28-437a-b591-b7baacca51dd.XLSX - LibreOffice Calc". The spreadsheet contains the following data:

Report for	Path	Permissions
svr-bman	\\svr-bman\Templates\Power Point Templates	Full control

In the example you see directories that everyone has access to.

## Report on the usage of "Authenticated Users"

### Background / Value

The report shows all directories where the account "Authenticated Users" has access. Just like the "Everyone" account, his technical user account should never be used to grant access to sensitive resources. Scan the report for sensitive directories and remove the access rights for "Authenticated Users".

### Related features

[Report on the usage of "everyone"](#)

[Identify globally accessible directories](#) (web client)

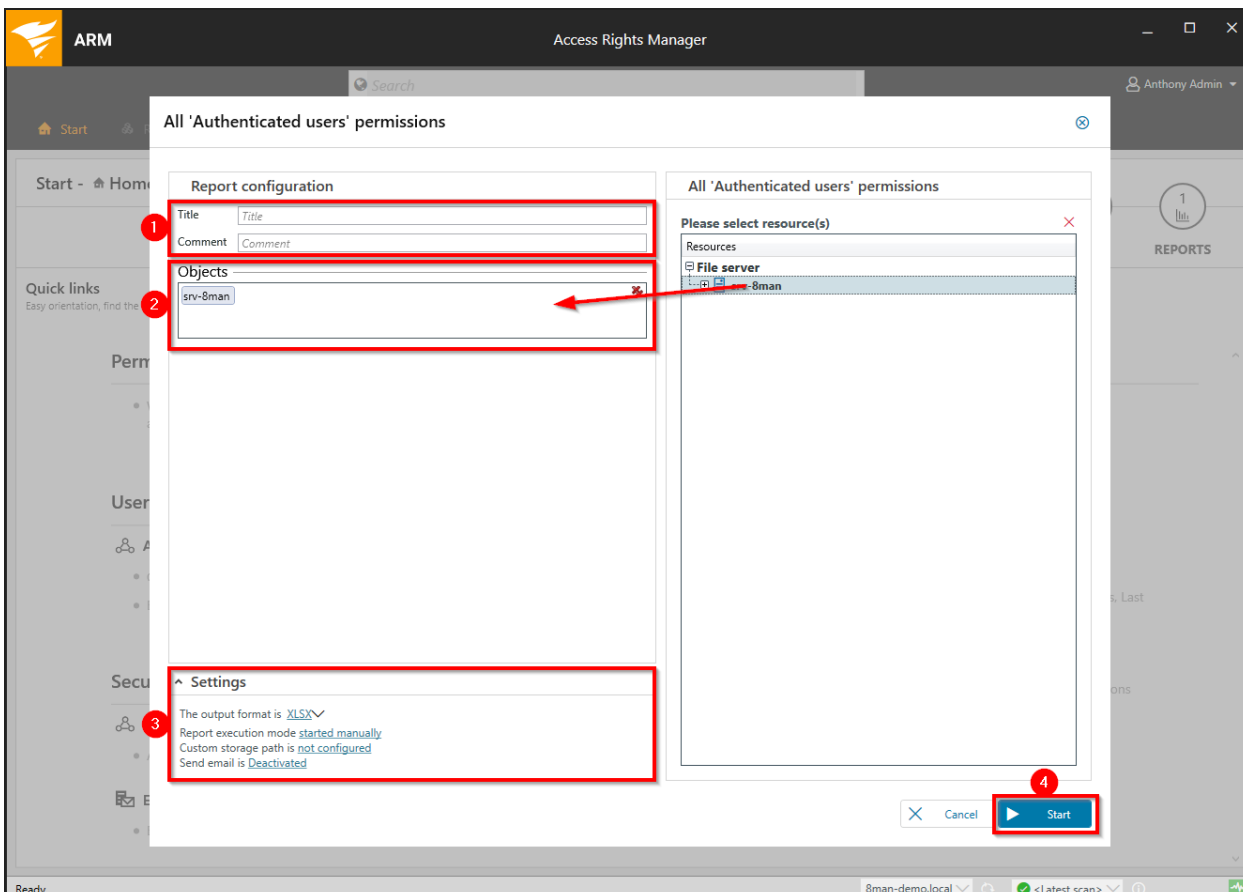
### Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) web interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main content area is divided into several sections:

- Start - Home**: A navigation bar with icons for HOME, NOTES (1), REQUESTS, TASKS, and REPORTS (1).
- Quick links**: A section for easy orientation.
- Permission Analysis**: A section with a link "Where does a user/group have access?".
- User Provisioning**: A section with links for "Accounts" (Create new user or group, Edit group memberships) and "Resources" (Edit access rights).
- Security Monitoring**: A section with links for "Active Directory" (AD Logga Report) and "Exchange" (Exchange Logga Report).
- Documentation & Reporting**: A section with links for "Reports overview" (1), "Where has the user/group access?", and "Who has access where?".
- Active Directory**: A section with links for "Account Details", "Inactive accounts", "Local accounts", "Manager-Employees", "OU Members and group memberships", and "Users and groups (Kerberos, Last logon)".
- Exchange**: A section with a link for "Exchange mailbox permissions".

In the "Documentation & Reporting" section, under the "File server" category, the link "All 'Authenticated users' permissions" is highlighted with a red box and a red circle with the number "2".

1. Select "Start".
2. Click on "All 'Authenticated Users' permissions".



1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired report settings.
4. Start the report.

## Report on directories whose owners are not administrators

### Background / Value

ARM shows you all directories where the owner is not a local administrator. If you exclude users from owning directories, you can prevent unwanted permission changes.

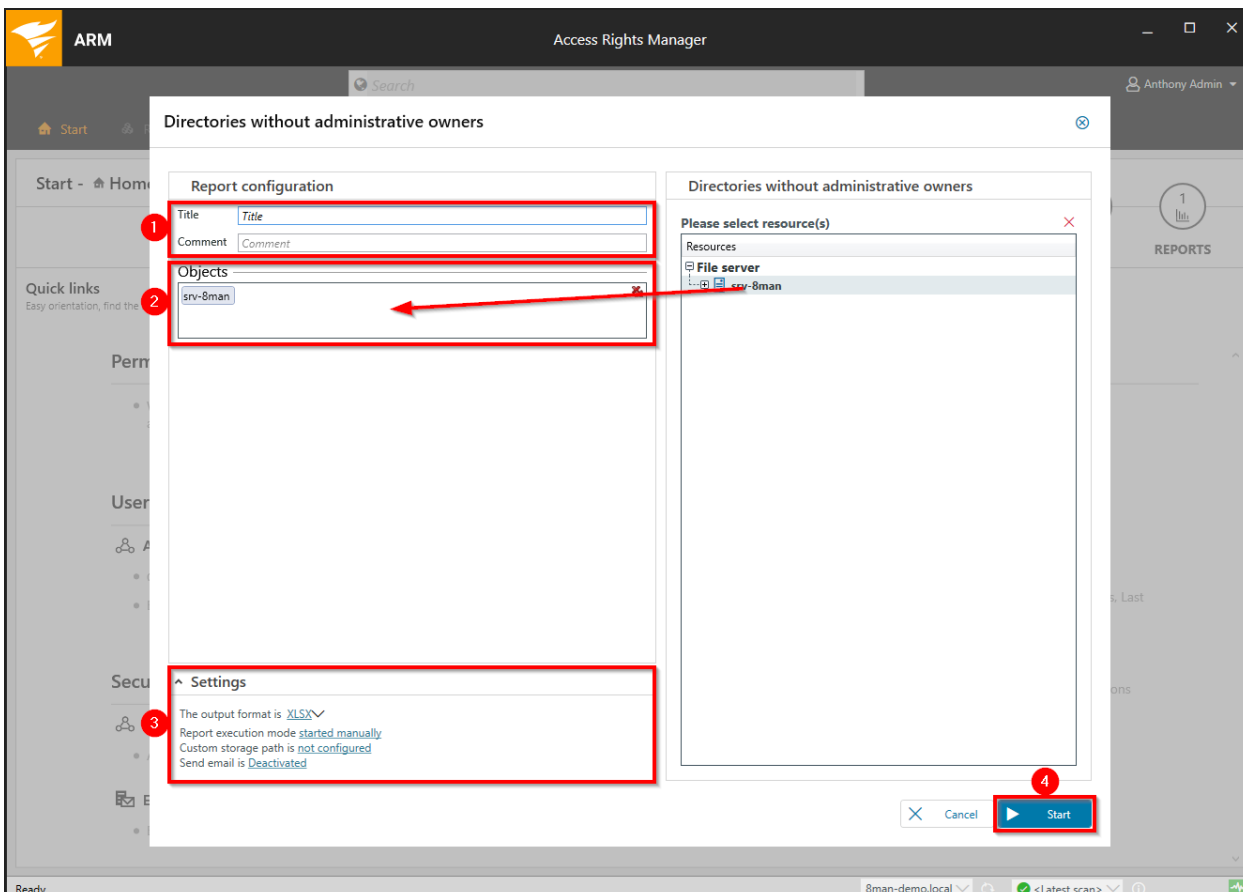
### Related features

[Change directory ownership](#)

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main content area is divided into several sections: Permission Analysis, User Provisioning, Security Monitoring, and Documentation & Reporting. The 'Start' button in the top navigation bar is highlighted with a red box and a red circle containing the number 1. In the 'Documentation & Reporting' section, the 'Directories without administrative owners' item is highlighted with a red box and a red circle containing the number 2.

1. Select "Start".
2. Click on "All owner not administrator".



1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired report settings.
4. Start the report.

Report for	Organization (\srv-8man\Organization)
Path	Owners not Administrators
\srv-8man\Organization	cradmin (8man-demo\cradmin)
\srv-8man\Organization\Finances	Finance (8man-demo\Finance)
\srv-8man\Organization\Finances\Accounts Payable\Accounts Open	cradmin (8man-demo\cradmin)
\srv-8man\Organization\Finances\Accounts Payable\Accounts Paid\New folder	cradmin (8man-demo\cradmin)
\srv-8man\Organization\Marketing\Events\The Art of Security\2011	cradmin (8man-demo\cradmin)
\srv-8man\Organization\Marketing\Events\The Art of Security\2012	cradmin (8man-demo\cradmin)
\srv-8man\Organization\Marketing\Events\The Art of Security\2013	cradmin (8man-demo\cradmin)

Open the report in your spreadsheet application. ARM lists all directories that are not owned by administrators.



## Permission differences

### Background / Value

The "Permission differences" report compares the access rights on your file server at two different points in time and shows you how your access rights situation has changed.

### Related features

[Compare two different access rights situations \(scan comparison\)](#)

[Analyze historical access rights situations](#)

### Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) dashboard. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The main content area is divided into several sections: 'Permission Analysis', 'User Provisioning', 'Security Monitoring', and 'Documentation & Reporting'. The 'Documentation & Reporting' section is further divided into 'Active Directory', 'File server', and 'Exchange'. Under the 'File server' section, the 'Permission difference' option is highlighted with a red box. The taskbar at the bottom shows the system is ready and the current scan is the latest one.

1. Select "Start".
2. Click on "Permission difference".

ARM Access Rights Manager

Search Anthony Admin

### Permission difference

**Report configuration**

Title

Comment

Compared time period [Fixed time span 3/3/2019 10:22 AM - 3/5/2019 10:22 AM](#)

**Selected paths**

Paths  Organizational categories

Replace groups by their members (direct permission changes)

Levels to resolve under the selected resource

**Advanced options**

**Sort and view options**

**Settings**

The output format is [PDF](#)

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

**Permission difference**

Please select resource(s)

Resources

File server

- srv-8man
  - Organization
    - Development
    - Facility Management
    - Finance
    - Human Resources
    - Management
    - Marketing
    - Production
    - Research
    - Sales
    - Projects
    - Templates
    - Users

Cancel Start

1. Enter a title for the report and add a comment.
2. Define the range of the report including the dates and times of comparison.
3. Define the desired output settings.
4. Start the report.

## Exchange

ARM lets you create easy to read reports on mailbox permissions.

### Report on mailbox permissions

#### **Background / Value**

ARM provides a report that shows Exchange mailbox access rights. This includes:

- Mailbox permissions
- Mailbox folder permissions
- Mailbox properties
- Delegates for mailboxes
- Out of office notices

Mailboxes and their folders require a high degree of security. However, in practice they often have excessive access rights. It is important to maintain an overview of these rights as folders often contain sensitive emails.

#### **Related features**

"Send As" access rights are shown in the report "[Who has access where?](#)".

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main content area is divided into several sections: Permission Analysis, User Provisioning, Security Monitoring, and Documentation & Reporting. The 'Start' button in the top navigation bar is highlighted with a red box and a '1' in a red circle. In the 'Documentation & Reporting' section, the 'Exchange mailbox permissions' link is highlighted with a red box and a '2' in a red circle.

1. Select "Start".
2. Click on "Exchange Mailbox permissions" in the "Documentation and Reporting" area.

The screenshot shows the 'Exchange mailbox permissions' report configuration window in the ARM application. The window is titled 'Exchange mailbox permissions' and has a search bar at the top. The main content is divided into three sections:

- Report configuration:** Contains fields for 'Title' (with a red box and number 1) and 'Comment'. Below these are checkboxes for various report options, such as 'Show mailbox folders with their permissions', 'Show standard properties (mailbox size, database, ...)', 'Show extended properties (delegates, out of office, ...)', 'Show only paths with changed rights', 'Save forest and compress report', 'Resolve group membership', and 'Resolve groups only in the summary section (affects only PDF)'. A red box and number 2 highlight the 'Resources' section below.
- Resources:** A tree view showing the directory structure of the Exchange mailbox. A red box and number 2 highlight the selection of 'Delmar Atkins (d.atkins@8man-demo.com)' under the 'Mailboxes' folder. A red box and number 4 highlight the 'Start' button at the bottom right of the dialog.
- Settings:** A section at the bottom with a red box and number 3. It includes settings for 'The output format is PDF', 'Report execution mode started manually', 'Custom storage path is not configured', and 'Send email is Deactivated'.

At the bottom of the dialog, there are 'Cancel' and 'Start' buttons. The 'Start' button is highlighted with a red box and number 4.

1. Enter a title for the report and add a comment.
2. Define the range and the layout of the report.
3. Define the desired output settings.
4. Start the report.

## Who has access to what in Exchange?

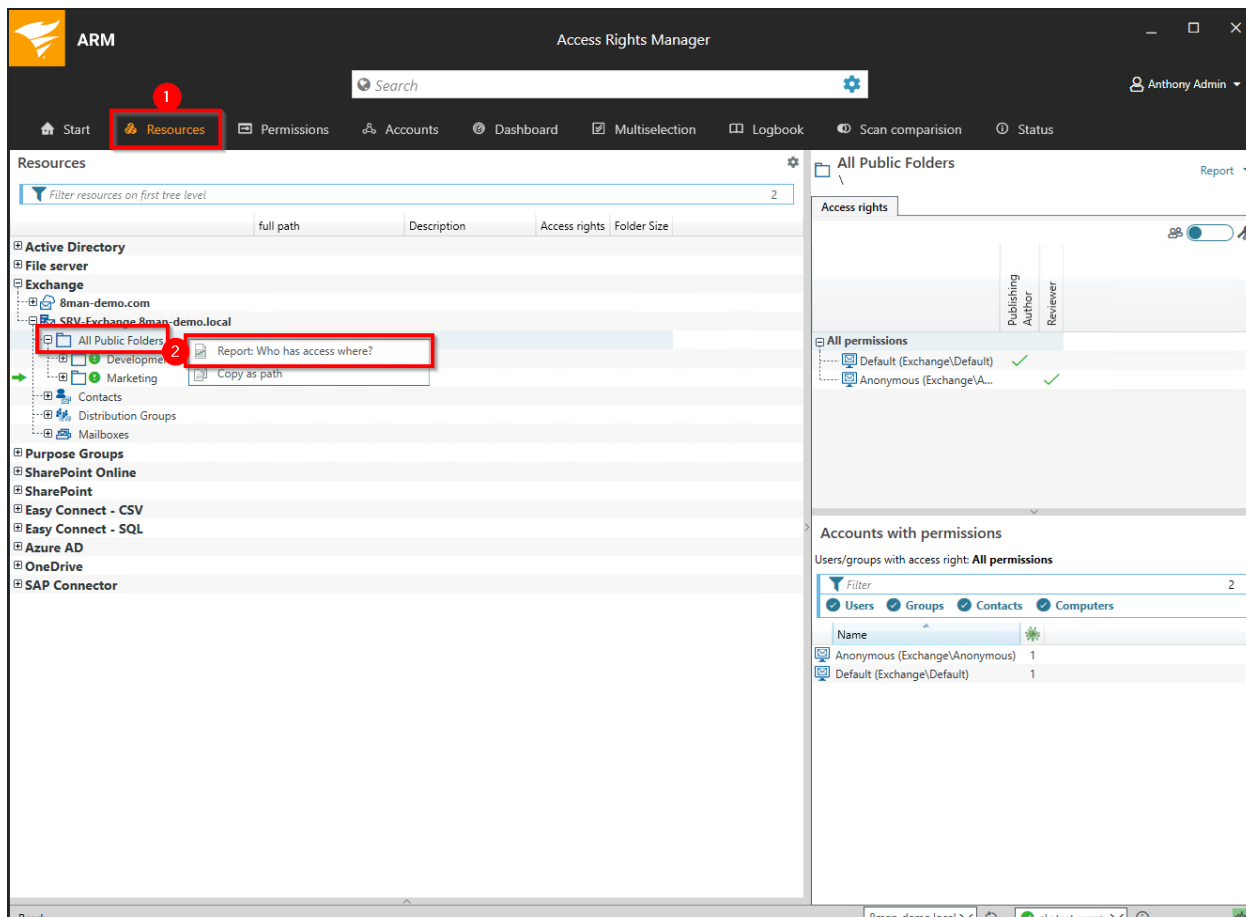
### Background / Value

Managers and team leads know best who should have access to what. Having an understanding of your access rights situation is extremely important, especially for public Exchange folders and mailboxes. The report "Who has access where?" provides an overview of all users and their access to public folders. In addition ARM highlights the access right "send as", due to its potential risk.

### Related features

[Report on mailbox permission](#)

### Step-by-step process



The screenshot shows the Access Rights Manager (ARM) interface. The 'Resources' pane on the left is expanded to show the 'Exchange' section, with 'All Public Folders' selected. A red box highlights the 'Resources' tab in the top navigation bar, and another red box highlights the 'Report: Who has access where?' option in the context menu. The right pane displays the 'All Public Folders' report, showing 'All permissions' and 'Accounts with permissions'.

Name	Count
Anonymous (Exchange\Anonymous)	1
Default (Exchange\Default)	1

1. Select "Resources".
2. Right click on any or all public folders. Select the report "Who has access where?" from the context menu.

1. Enter a title for the report and add a comment.
2. Define the range of the report. In order to reduce complexity, we recommend selecting "user view" in the "group settings" area. All other settings are targeted at expert users.
3. Define the desired output settings.
4. Start the report.

## OneDrive

OneDrive offers the possibility to store files and folders in the cloud. The advantages of the cloud service are obvious: employees can work together on documents easily and conveniently. The external sharing of documents is particularly critical as it is possible to share documents without authorization for an unlimited period of time.

ARM shows you with its typical simplicity which users shared which files and folders how and with whom.

### Create a report about directories and files shared on OneDrive

#### **Background/Value**

A frequently asked question from management is: "Which files have which employees shared externally?" With ARM, you can create a report with just a few clicks that answers exactly this question.

#### **Related features**

[Identify shared directories and files on OneDrive](#)



## Step-by-step-process

The screenshot displays the SolarWinds ARM (Access Rights Manager) interface. The top navigation bar includes 'Start', 'Resources' (highlighted with a red box and '1'), 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The main area is divided into a left pane for 'Resources' and a right pane for 'Protected Networks GmbH'. The 'Resources' pane shows a tree view with categories like Active Directory, File server, Exchange, etc. The 'OneDrive' folder is expanded, and the 'Protected Networks GmbH' resource is selected (2). A context menu is open over the selected resource, and the 'Report: Who has access where?' option is highlighted (3). The right pane shows the 'Access rights' section for the selected resource, which is currently empty, and the 'Accounts with permissions' section below it.

1. Select the Resource view.
2. Expand OneDrive and select a resource.
3. Right-click a resource and select "Report: Who has access where?" from the context menu.

Report configuration

Title

Comment

Objects

Paths  Organizational categories

Protected Networks GmbH

Levels to resolve under the selected resource

Translate names of groups to purpose group name

Details

Filter

Group settings

Options

Settings

The output format is [PDF](#)

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

Who has access where?


Please select resource(s)

Resources

- File server
- Exchange
- SharePoint Online
- SharePoint
- Easy Connect - CSV
- Easy Connect - SQL
- Microsoft Dynamics NAV
- Azure AD
- SAP Connector (pn)
- OneDrive
  - Protected Networks GmbH
    - Delmar Atkins
    - Dexter Ward
    - Gerd ExLoggaTest
    - IntegrationTestUser
    - IntegrationTestUser2

Start Cancel

1. The previously selected resource is preset.
2. Optional: Delete the preselected resources.
3. Use Drag&Drop to add resources.
4. Start the report creation.


**ARM Report: Who has access where?**
Page 1

---

<b>Title</b>	ARM Report: Who has access where?		
<b>Comment</b>	-		
<b>Used time zone</b>	W. Europe Standard Time (UTC+01:00:00)		

<b>Scantime</b>	protected networks gmbh	Azure AD	9/26/2018 1:34:34 PM
	protected networks gmbh	OneDrive	12/4/2018 1:37:43 PM

**Configuration**

Selected resources:  
 - Dexter Ward (Documents)

Number of levels to resolve under the selected resource: All  
 Show only resource objects with changed access rights.  
 Resolve groups at end.

**Scan problems**    No scan errors detected.

### Report for Dexter Ward (Documents)

**Invoices**

[https://8mandemo-my.sharepoint.com/personal/d\\_ward\\_8man-demo\\_com/Documents/Documents/Invoices](https://8mandemo-my.sharepoint.com/personal/d_ward_8man-demo_com/Documents/Documents/Invoices)

	Owner	Edit	View
Dexter Ward (Protected Networks GmbH)	✔	✔	✔
External (Protected Networks GmbH)	✔	✔	✔
marketing (Protected Networks GmbH)	✔	✔	✔
sales (Protected Networks GmbH)	✔	✔	✔

**Summary Q2.docx**

[https://8mandemo-my.sharepoint.com/personal/d\\_ward\\_8man-demo\\_com/\\_layouts/15/Doc.aspx?sourcedoc=%7B2BF5A8F4-9E83-45F8-81B2-919DB190C7B8%7D&file=Summary%20Q2.docx&action=default&mobileredirect=true](https://8mandemo-my.sharepoint.com/personal/d_ward_8man-demo_com/_layouts/15/Doc.aspx?sourcedoc=%7B2BF5A8F4-9E83-45F8-81B2-919DB190C7B8%7D&file=Summary%20Q2.docx&action=default&mobileredirect=true)

	Owner	Edit	View
Delmar Atkins (Protected Networks GmbH)	✔	✔	✔
Dexter Ward (Protected Networks GmbH)	✔	✔	✔
External (Protected Networks GmbH)	✔	✔	✔

**Groups and their members**

marketing (Protected Networks GmbH)

└ This group doesn't have any members.

sales (Protected Networks GmbH)

└ This group doesn't have any members.

**Legend**

Administrator

Example report

## Security Monitoring

A great many employees make changes in Active Directory and to the file server. Security risks can arise without comprehensive monitoring. With our Logga modules you can record security-relevant activities in your company network. This allows you to trace what has been done in the network, by whom and when.

At process levels, you gain complete visibility into Access Rights activities. Changes made outside of ARM are recorded. Based on the information obtained, your Access Rights Management process can be optimized. Alerts (FS and AD Logga) proactively inform you about critical events.

page 627

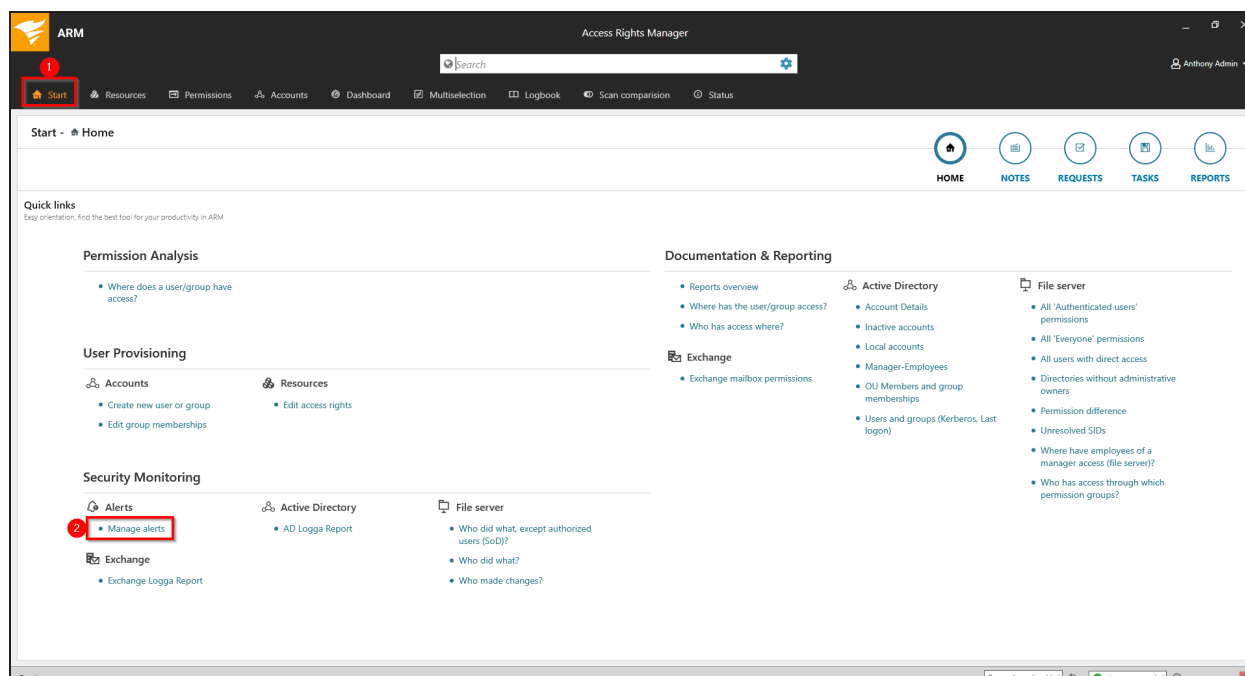
# Cross-resource

## Manage alerts

### Background / Value

Saved alert configurations can be modified at any time via the ARM home page.

### Step-by-step process



1. Select "Start".
2. Click "Manage alerts".

ARM Access Rights Manager

Start - Home

Quick links

Permission Analysis

User Provisioning

Security Monitoring

Manage Alerts

Manage alert definitions system-wide.

State	Name	Resource	Event	Threshold	Action
<input type="checkbox"/>	Account locked for Sam Sales (Bman-demo/Sam Sales)	Sam Sales (Bman-demo/Sam Sales)	Account locked		Send email Write to Windows event log
<input type="checkbox"/>	Group memberships changed for C-Level (Bman-demo/C-Level)	C-Level (Bman-demo/C-Level)	Group memberships changed		Send email Write to Windows event log
<input type="checkbox"/>	Group memberships changed for Domain Admins	Domain Admins (Bman-demo/Domain Admins)	Group memberships changed		Send email Execute script
<input type="checkbox"/>	Password reset for Sam Sales (Bman-demo/Sam Sales)	Sam Sales (Bman-demo/Sam Sales)	Password reset		Send email Write to Windows event log
<input type="checkbox"/>	Permission changes in directory for Sales	\\srv-Bman\Organization\Sales	Changes in directory		Send email
<input type="checkbox"/>	Possible data piracy for Top Secret Project Z	\\srv-Bman\Projects\Top Secret Project Z	Changes in directory	1000x / 1m	Send email
<input type="checkbox"/>	Possible virus attack on the file server srv-Bman	\\srv-Bman	Changes in file server	2000x / 20s	Send email Execute script

File server

- All 'Authenticated users' permissions
- All 'Everyone' permissions
- All users with direct access
- Directories without administrative owners
- Permission difference
- Unresolved SIDs
- Where have employees of a manager access (file server)?
- Who has access through which permission groups?

ARM shows you all alert configurations.

1. Search for an alert configuration.
2. Turn alerts on or off.
3. Use the links to edit, delete or enable/disable the selected alert configuration. Alternatively you can right-click an entry and use the context menu.

## Active Directory Logga

### The problem

Changes to Active Directory or file servers are made by a variety of employees. Without full monitoring, security risks and inconsistencies in the processes are created.

### Security risks

Security risks often occur when group memberships give unauthorized employees access to sensitive documents. If group memberships are revoked again immediately, the security incident is usually not recognized.

### The solution

ARM creates transparency of the access rights situation in Active Directory. The AD Logga expands this transparency to include the entire history of access rights changes in your system. This even includes any changes made outside of ARM. Security relevant temporary group memberships thereby become completely transparent. Through our configurable reports all activities related to user accounts, objects, groups and attributes become fully tracable and transparent.

### This is achieved with the AD Logga

- Giving Administrators a complete picture of all AD activity.
- Auditors recognize security incidents and all involved parties. This way the appropriate remedies can be implemented.
- The management has the certainty: With its monitoring, AD Logga provides the data for internal security and process improvements.
- The AD Logga alerts proactively inform you. Should someone manipulate security-related accounts or groups, the administrator will be informed immediately.

## Analyze AD Logga events with the logbook

### **Background / Value**

By using the reports you can regularly analyze all the tracked events at a detailed level. You can find the information needed much faster by using the logbook.

### **Related features**

[Identify temporary group memberships](#)

[Identify locked user accounts](#)

[Monitor password resets](#)

[Set alerts for groups](#)

[Set alerts for user accounts](#)

## Step-by-step process

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The 'Logbook' tab is active, showing a search filter for 'From 7/1/2018 until Today'. A calendar view shows event counts for various dates, with a red box highlighting a specific row. To the right, a detailed log entry is visible, showing a list of events with columns for Time, Author, and Comment. The log entry shows a sequence of events including NTFS Logga, AD Logga, and Administrator actions.

1. Choose "Logbook".
2. Set the time frame for the logbook analysis.
3. Use the filters to focus on the desired events.
4. Select all events of one day (one row).



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. At the top, there's a search bar and navigation tabs for Start, Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, and Status. The main area is titled 'Logbook' and shows a calendar view from 7/1/2018 to Today. A red box labeled '1' highlights a cell on 9/18/2018. To the right, a detailed view for Tuesday, September 18, 2018, is shown, with a red box labeled '2' highlighting a list of events. A red arrow points to a 'Logga' event. A third red box labeled '3' highlights the detailed view of the 'Membership changed' event for 'AD Logga for 8man-demo.local', showing the change was made by 'sa-8man (8man-demo\sa-8man)' and a member 'Alvaro Roland (8man-demo\Alvaro Roland)' was added to the 'Design' group.

1. Select a cell (an event type) to further narrow down your query.
2. ARM displays all results. The "footstep icon" indicates the AD Logga results. Select a result.
3. ARM displays all details of the event.

## Report on changes in Active Directory

### Background / Value

The AD Logga allows you to monitor current processes in your Active Directory. ARM even captures all changes made with native tools including temporary changes. From a security perspective any actions related to event types and event authors are important.


### Monitoring of event types

*Changes to:*

- Attributes
- Users
- Computers
- Groups
- Passwords
- Accounts
- Members

### Monitoring of event authors

- Users
- Groups
- Computers

 Additionally you are able to filter according to object class and attribute.

### Related features

[Analyze AD Logga events with the logbook](#)

[Set alerts for groups](#)

[Set alerts for user accounts](#)

## Step-by-step process

The screenshot displays the SolarWinds Access Rights Manager (ARM) web interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. A red circle with the number '1' highlights the 'Start' button in the top-left corner. Below the navigation bar, there are five main menu items: HOME, NOTES, REQUESTS, TASKS, and REPORTS. The main content area is titled 'Quick links' and contains several sections: 'Permission Analysis', 'User Provisioning', 'Security Monitoring', and 'Documentation & Reporting'. In the 'Security Monitoring' section, under 'Active Directory', the 'AD Logga Report' link is highlighted with a red box and a red circle with the number '2'. The 'Documentation & Reporting' section lists various reports such as 'Reports overview', 'Where has the user/group access?', and 'Who has access where?'. The bottom of the screenshot shows the Windows taskbar with the system tray.

1. Select "Start".
2. Click on "AD Logga Report".

The screenshot shows the 'AD Logga Report' configuration window in the SolarWinds Access Rights Manager. The window is divided into two panes: 'Report configuration' on the left and 'AD Logga Report' on the right. The 'Report configuration' pane has three red boxes and numbers 1, 2, and 3. Box 1 highlights the 'Title' and 'Comment' fields. Box 2 highlights the 'Report time range' field, which shows a fixed time span from 3/5/2019 11:34 AM to 3/7/2019 11:34 AM. Box 3 highlights the 'Objects' field, which contains '8man-demo.local'. A red arrow points from the 'Objects' field to the 'AD Logga Report' pane, which shows a list of resources under 'Active Directory' with '8man-demo.local' selected. The 'AD Logga Report' pane also has a 'Please select resource(s)' header and a 'Resources' section. At the bottom of the 'Report configuration' pane, there are 'Settings' for output format (XLSX), report creation (all accounts in one document), execution mode (started manually), storage path (not configured), and email (deactivated). The 'AD Logga Report' pane has a 'Save your report configuration' section and 'Cancel' and 'Start' buttons.

1. Enter a title for the report and add a comment.
2. Define the date range of the report.
3. Select domain objects whose events should be captured in the report.

ARM Access Rights Manager

Search

Anthony Admin

### AD Logga Report

Report configuration

Objects: 8man-demo.local

1 **Event Type**  
Please select one or more Event Types.  
To search for all Event Types leave this field empty.

2 **Event Author**  
Please select one or more user.  
To search for events of all users leave this field empty.

3 **Object Class**  
Please select one or more object classes.  
To search for all object classes leave this field empty.

4 **Attribute**  
Please select one or more attributes.  
To search for all attributes leave this field empty.

Settings

The output format is [XLSX](#)

Create report [for all accounts in one document](#).

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

### AD Logga Report

Event Type Filter 19

- Account activated
- Account deactivated
- Account locked
- Account unlocked
- Added attribute
- Changed attribute
- Computer created
- Computer deleted
- Failed change attempt
- Group created
- Group deleted
- Member added
- Member removed
- Other objects created
- Other objects deleted
- Removed attribute
- Reset password
- User created
- User deleted

Save your report configuration

Cancel Start

Define the range of the report by setting filters. By definition filters exclude the selected data.

1. Add the type of events that you would like to include in the report.
2. Add the authors of events that you would like to include in the report.
3. Add all object classes that you would like to include in the report.
4. Add all attributes that you would like to include in the report.

The screenshot displays the 'AD Logga Report' configuration window in the Access Rights Manager. The window is divided into two main sections: 'Report configuration' on the left and 'AD Logga Report' on the right. The 'Report configuration' section includes fields for 'Objects' (containing '8man-demo.local'), 'Event Type', 'Event Author', 'Object Class', and 'Attribute'. The 'AD Logga Report' section shows a 'Please select resource(s)' dialog with 'Active Directory' and '8man-demo.local' selected. Below this, a table lists available templates:

Name	Created on	Author
demo template	3/7/2019 11:51 AM	8MAN-DEMO/Anthony Admin

Below the table are 'Use' and 'Delete' buttons. A 'Save template' dialog is also visible, with 'demo template' as the name and 'New' as the selected option. Two red circles with numbers '1' and '2' are overlaid on the image, pointing to the 'demo template' row in the table and the 'New' radio button, respectively.

By saving AD Logga report configurations as templates you can save valuable time by reusing complex report configurations.

1. Select an existing template.
2. Save the current configuration as a template.

ARM Access Rights Manager

AD Logga Report

Report configuration

Title

Comment

Report time range Fixed time span 7/1/2018 11:34 AM - 3/7/2019 11:34 AM

Show raw data only (affects only CSV)

Objects

8man-demo.local

Event Type

Please select one or more Event Types.  
To search for all Event Types leave this field empty.

Event Author

Please select one or more user.  
To search for events of all users leave this field empty.

Object Class

Please select one or more object classes.  
To search for all object classes leave this field empty.

Settings

The output format is: **CSV**

Create report for all accounts in one document.

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

AD Logga Report

Please select resource(s)

Resources

Active Directory

8man-demo.local

1 Template available

Name	Created on	Author
demo template	3/7/2019 11:51 AM	8MAN-DEMO/Anthony Admin

Use Delete

Save template

Name

Description

Overwrite  
Overwrite the used template with the current report configuration.

New  
Save the current report configuration in a new template.

Cancel Start

1. Define the desired output settings.
2. Option activated and output format set to CSV: The report contains only event data and no report or filter configuration. This can be very helpful for automated post-processing.
3. Start the report.

## Report on temporary group memberships

### Background / Value

AD Logga closes a number of important security gaps. One of the most important one is temporary group memberships. Insider threats grant themselves access to secret directories, copy data and then revert back to the original state after performing their desired actions. Without the AD Logga these types of activities remain undetected.

### Related features

[Analyze AD Logga events with the logbook](#)

[Set alerts for groups](#)

[Set alerts for user accounts](#)

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. Below the navigation bar, there are several menu items: Start, Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, and Status. The 'Start' menu item is highlighted with a red box and a red circle containing the number 1. Below the navigation bar, there are five main sections: HOME, NOTES, REQUESTS, TASKS, and REPORTS. The 'REPORTS' section is highlighted with a red circle containing the number 2. Under the 'REPORTS' section, there are three sub-sections: Active Directory, File server, and Exchange. The 'Active Directory' sub-section is highlighted with a red box and a red circle containing the number 2. Under the 'Active Directory' sub-section, there is a list of reports, including 'AD Logga Report', which is highlighted with a red box and a red circle containing the number 2.

1. Select "Start".
2. Click on "AD Logga Report".



1. Enter a title for the report and add a comment.
2. Define the range of the report. For the event type select "Member added" and "Member removed".
3. Define the desired output settings.
4. Start the report.

## Report on locked user accounts

### Background / Value

In the best case scenario, an attempted login with someone else's account ends with a locked user account. The AD Logga shows you from which computer the attack occurred.

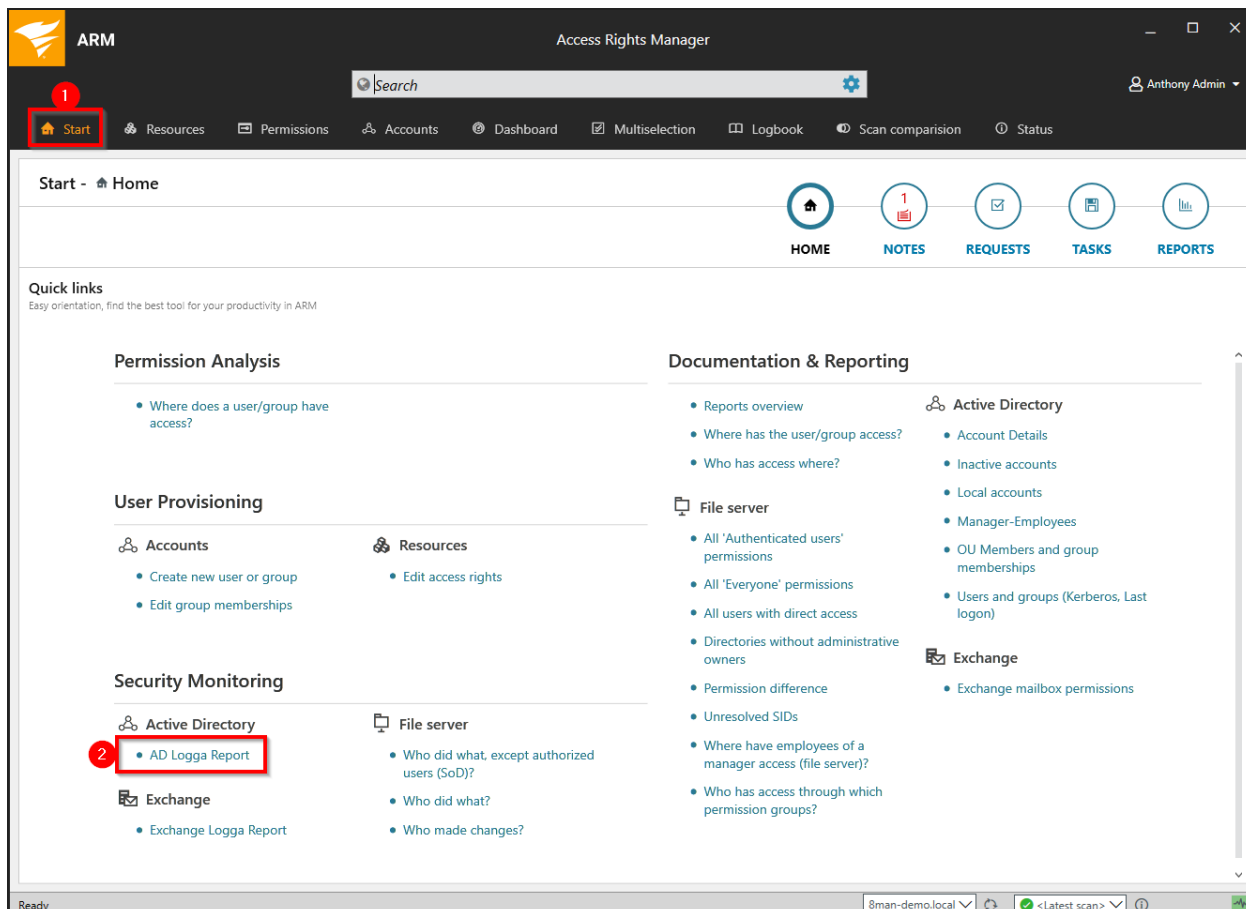
### Related features

[Analyze AD Logga events with the logbook](#)

[Set alerts for groups](#)

[Set alerts for user accounts](#)

### Step-by-step process



1. Select "Start".
2. Click on "AD Logga Report".

The screenshot shows the 'AD Logga Report' configuration window in the SolarWinds ARM interface. The window is split into two main sections. The left section, titled 'Report configuration', contains several input fields and options: 'Title' and 'Comment' (both with placeholder text), 'Report time range' (set to a fixed time span), a checkbox for 'Show raw data only', 'Objects' (with a dropdown showing '8man-demo.local'), 'Event Type' (with a dropdown showing 'Account locked'), 'Event Author' (with instructions to select one or more users), 'Object Class' (with instructions to select one or more object classes), and a 'Settings' section (expanded) showing output format as 'XLSX', report mode as 'started manually', storage path as 'not configured', and email as 'Deactivated'. The right section, titled 'AD Logga Report', displays a list of event types with a filter set to 19. The 'Start' button at the bottom right is highlighted with a red box and a red circle containing the number 4. Red arrows point from the numbered circles to the corresponding configuration elements.

1. Enter a title for the report and add a comment.
2. Define the range of the report. For the event type select "Account locked".
3. Define the desired output settings.
4. Start the report.

## Report on password resets

### Background / Value

With the ARM AD Logga you can monitor the process of resetting passwords. Within this process there is an inherent security risk. For example, if a helpdesk employee secretly resets the password of a manager or executive, they can sign on with a temporary password and gain access to sensitive information. The Manager would probably not notice this and only be confused about why his password is no longer valid, perhaps even thinking that he forgot his password, and then simply request a new one from support.

### Related features

[Analyze AD Logga events with the logbook](#)

[Set alerts for groups](#)

[Set alerts for user accounts](#)

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) web interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main content area is divided into several sections: 'Permission Analysis', 'User Provisioning', 'Security Monitoring', and 'Documentation & Reporting'. The 'Start' button in the top left is highlighted with a red circle and a red '1'. In the 'Security Monitoring' section, the 'AD Logga Report' link is highlighted with a red circle and a red '2'. The 'Documentation & Reporting' section lists various reports such as 'Reports overview', 'Where has the user/group access?', 'Who has access where?', 'Active Directory', 'File server', and 'Exchange'.

1. Select "Start".

## 2. Click on "AD Logga Report".

The screenshot shows the 'AD Logga Report' configuration dialog in the Access Rights Manager (ARM) interface. The dialog is divided into two main sections: 'Report configuration' and 'AD Logga Report'. The 'Report configuration' section includes fields for Title, Comment, Report time range, Show raw data only, Objects, Event Type, Event Author, and Object Class. The 'AD Logga Report' section includes a list of Event Types and a 'Start' button. Red boxes and numbers 1, 2, and 3 highlight the Title/Comment fields, the Event Type selection, and the Settings section respectively. A red arrow points from the 'Reset password' event type in the list to the 'Event Type' field in the configuration section.

1. Enter a title for the report and add a comment.
2. Define the range of the report. For the event type select "reset password".
3. Define the desired report settings.
4. Start the report.

## Set alerts for groups

### Background / Value

Employees receive their access rights through group memberships. Especially sensitive groups grant access to secret folders and other important resources. The AD Logga allows you to actively monitor specific AD groups so that an alert is received if new members are added.

Due to the nested group structures in the Active Directory, it is important to monitor both direct group memberships and indirect memberships.

### Related features

[Set alerts for user accounts](#)

[Set alerts for OUs/domains](#)

[Manage alerts](#)

### Step-by-step process




The screenshot displays the Access Rights Manager (ARM) interface. The search bar at the top is highlighted with a red box and a red '1'. The main area shows a graph view of group memberships. The 'C-Level (8man-demo\C-Level)' group is selected, and its context menu is open. The 'Create alert' option in the context menu is highlighted with a red box and a red '2'. The context menu includes options such as 'Select account', 'Show in Resources View...', 'Show access rights to resources...', 'Report: Where has the user/group access?', 'Report: Account Details', 'Change group memberships...', 'Create new user or group', 'Delete account', 'Edit attributes', 'Move object', 'Create Purpose Group', 'Add note', 'Open Logbook', 'Create alert', and 'Manage alerts'.


1. Use the search to find the desired group.

2. Right-click on the group and select "Create alert" from the context menu.


Create alert ⊗

Create an alert for 'C-Level (8man-demo\C-Level)' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS !	CATEGORY
1 <input type="text" value="Group memberships changed"/> ✓				<input type="text" value="Information"/> ▾

EVENT SETTING FOR 'GROUP MEMBERSHIPS CHANGED' 




2   Direct only  Direct and indirect


Please add a comment  


1. Enter a title for the alert.
2. Select whether only direct or direct and indirect group membership changes (recommended) trigger an alert.

### Create alert ✕

Create an alert for 'C-Level (8man-demo\C-Level)' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Group memberships changed <span style="float: right;">✓</span>	 <span style="float: right;">✓</span>	 <span style="float: right;">✓</span>	 <span style="float: right;">1</span>	Information <span style="float: right;">▼</span>


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 


Send email  

To:  ▼ ▶


Language:  ▼ ⌵ 2


Time zone:  ▼ ⌵

Write to Windows event log  

Execute script  

▼ 4


Please add a comment 


Close Create

#### 1. Choose Actions.

Here you specify which actions are executed when an alert is triggered. You must activate at least one action.

#### 2. Activate the option if an email should be sent in case of an alert.

 The content of the emails can be customized. This is analogous to the [recertification emails](#).




3. The alarm is written to the Windows event log using the categorization. This option is especially useful if you are using a SIEM system that monitors the Windows Event Log.


4. Enable the execution of a script. To be able to activate this option, a [script configuration](#) for alerts must exist.







**Edit alert** ✕


Edit an automatically executed alert for 'C-Level (8man-demo\C-Level)'.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Group memberships changed <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>		Information <input type="checkbox"/>

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 

- Write to Windows event log 
- Execute script   
UndoGroupMemberShipChange
- Write to SysLog 

Please add a comment 



Activate this option to write the event to a Syslog server. Syslog servers need to be configured in the ARM configuration application under Server > [Syslog](#).

### Create alert ✕

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki <span style="color: green;">✔</span>	<span style="color: green;">✔</span>	<span style="color: green;">✔</span>		<div style="border: 1px solid #ccc; padding: 2px;"> <span style="background-color: #f0f0f0; padding: 2px;">Information</span> <span style="font-size: 0.8em;">▼</span>  <span style="padding: 2px;">Information</span>  <span style="padding: 2px;">Warning</span>  <span style="padding: 2px;">Critical</span> </div>

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To:  ▼ ▶

Language:  ▼ ⌂

Time zone:  ▼ ⌚

Write to Windows event log

Execute script




▼


Please add a comment ⚠


Choose a category. This is used when writing to the Windows Event Log and for the email subject.

### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	Information <input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input type="checkbox"/> Critical <input type="checkbox"/>


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 


Send email 



To:

Language:

Time zone:

Write to Windows event log 

Execute script 

1. You must specify a reason for the alert configuration in order to save it.
2. Click on "Create".

## Set alerts for user accounts

### Background / Value

The AD Logga allows you to monitor the process of resetting passwords. Within this process there is an inherent security risk. For example, if a helpdesk employee secretly resets the password of a manager or executive, they can sign on with a temporary password and gain access to sensitive information. In this scenario the designated users are informed.

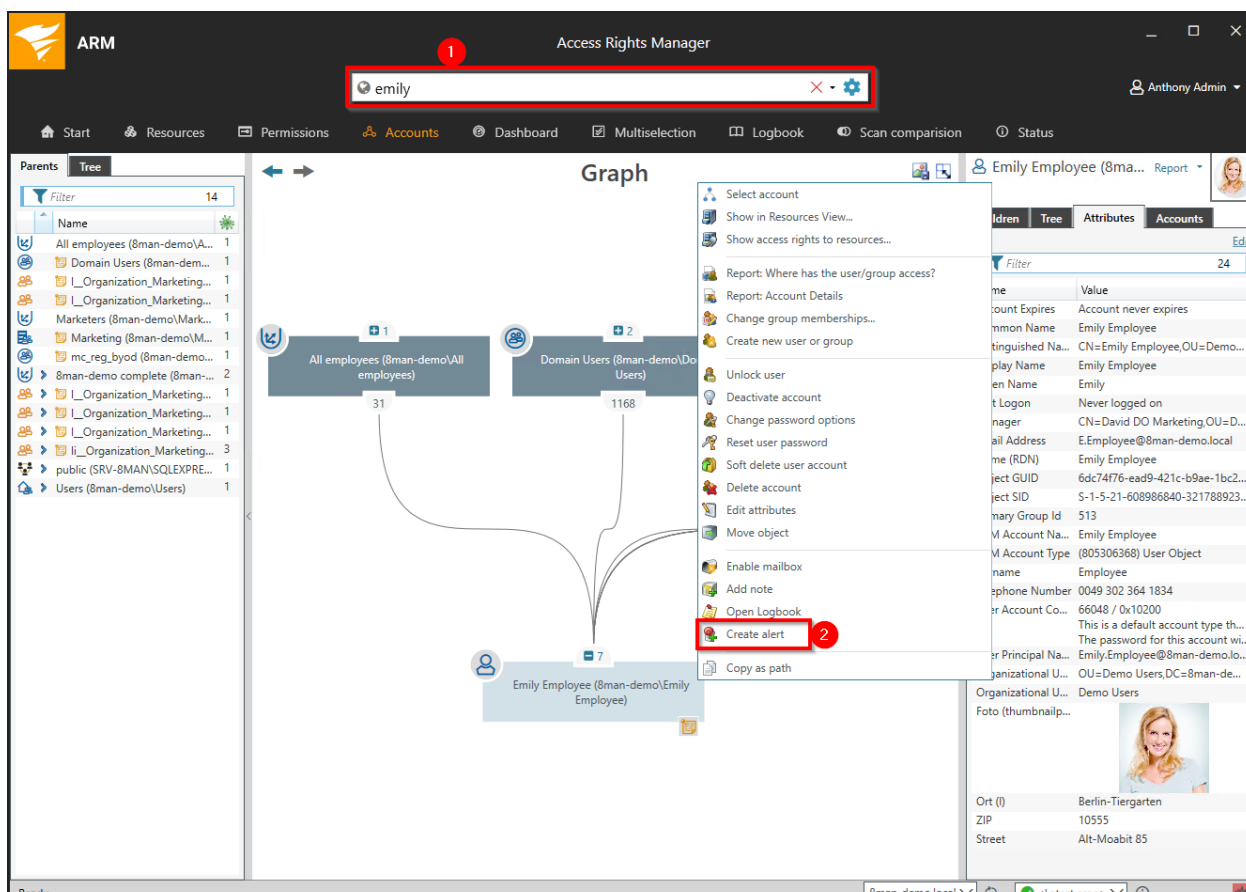
### Related features

[Set alerts for groups](#)

[Set alerts for OUs/domains](#)

[Manage alerts](#)

### Step-by-step process







The screenshot shows the Access Rights Manager (ARM) interface. The search bar at the top contains the name "emily". The main area displays a graph with nodes for "All employees (8man-demo\All employees)" and "Domain Users (8man-demo\Domain Users)". A context menu is open over the "Emily Employee (8man-demo\Emily Employee)" node, with the "Create alert" option highlighted. The right-hand pane shows the user's details, including name, email address, and organizational unit.

1. Find the desired user by entering their name into the search field.
2. Right-click on the user and select "Create alert" from the context menu.

Create alert ✕

Create an alert for 'Emily Employee (8man-demo\Emily Employee)' that will execute the selected actions when occurred.


ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Account locked for Emily Emp <span>✓</span>				Information <span>▼</span>

PLEASE SELECT AN EVENT 

Please select an event

Account locked ▼

Please add a comment ⚠

 Close Create

1. Enter a title for the alert.
2. Select an event type that triggers the alert.

**Create alert**

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki ✓			1	Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To: anthony.admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Write to Windows event log

Execute script

start malware scan

Please add a comment

Close Create

### 1. Choose Actions.

Here you specify which actions are executed when an alert is triggered. You must activate at least one action.

### 2. Activate the option if an email should be sent in case of an alert.




The content of the emails can be customized. This is analogous to the [recertification emails](#).


3. The alarm is written to the Windows event log using the categorization. This option is especially useful if you are using a SIEM system that monitors the Windows Event Log.




4. Enable the execution of a script. To be able to activate this option, a [script configuration](#) for alerts must exist.


**Edit alert** ✕


Edit an automatically executed alert for 'C-Level (8man-demo\C-Level)'.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Group memberships changed <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>		Information <input type="checkbox"/>

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 

- Write to Windows event log 
- Execute script   
UndoGroupMemberShipChange
- Write to SysLog 

Please add a comment 



Activate this option to write the event to a Syslog server. Syslog servers need to be [configured in the ARM configuration application](#) under Server > Syslog.

### Create alert ✕

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki <span style="color: green;">✔</span>	<span style="color: green;">✔</span>	<span style="color: green;">✔</span>		<div style="border: 1px solid #ccc; padding: 2px;"> <span style="background-color: #f0f0f0; padding: 2px;">Information</span> ▾  <span style="padding: 2px;">Information</span>  <span style="padding: 2px;">Warning</span>  <span style="padding: 2px;">Critical</span> </div>

**DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT**

Send email

To:

Language:

Time zone:

Write to Windows event log

Execute script

Please add a comment ⚠




Close
Create


Choose a category. This is used when writing to the Windows Event Log and for the email subject.




### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>		Information <input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input type="checkbox"/> Critical <input type="checkbox"/>


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 


Send email 



To:

Language:

Time zone:

Write to Windows event log 

Execute script 

1. You must specify a reason for the alert configuration in order to save it.
2. Click on "Create".

## Set alerts for OUs/domains

### Background / Value

Sometimes not only a group or a single user is particularly security relevant, but an entire OU or domain. In these cases, you can configure alarms for entire OUs/domains, e.g. if a group membership has been changed, a password reset or an account locked.

### Related features

[Set alerts for user accounts](#)

[Set alerts for groups](#)

[Manage alerts](#)

### Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The 'Resources' tab is selected, and the 'Active Directory' tree is expanded to show the '8man-demo.local' domain. A red box highlights the 'Create alert' option in the context menu for the '8man-demo.local' resource. The right-hand pane shows the 'Access rights' for the selected resource, including a table of permissions and a list of accounts with permissions.




Account	Full control	Read	Special permissions
NT AUTHORITY\Authenticated Users	✓	✓	4
NT AUTHORITY\SYSTEM	✓	✓	
Enterprise Admins (8man-demo.local)	✓	✓	
NT AUTHORITY\ENTERPRISE...	✓	✓	8
Everyone			2
BUILTIN\Administrators			7
BUILTIN\Pre-Windows 20...			17


Name	how often granted
Administrator (8man-demo\Administrator)	1
BUILTIN\Administrators	1
BUILTIN\Incoming Forest Trust Builders	1
BUILTIN\Pre-Windows 2000 Compatible Access	1
CREATOR OWNER	1
Domain Admins (8man-demo\Domain Admins)	1
Everyone	1
NT AUTHORITY\Authenticated Users	2
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	2
NT AUTHORITY\SELF	1
NT AUTHORITY\SYSTEM	1
SRV-BMAN (8man-demo\SRV-BMAN\$)	1

1. Select Resources.
2. Navigate to the desired domain, OU or container. You can alternatively use the search to find the desired AD object. Right-click on it and select "Create alert" from the context menu.

### Create alert

Create an alert for '8man-demo.local' that will execute the selected actions when occurred.


ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Account locked for 8man-demo ✓				Information ▾


PLEASE SELECT AN EVENT 

Please select an event

Account locked ▾

- Account locked
- Group memberships changed
- Password reset

Please add a comment 



Select one of the following event types that can trigger the alert:

- Account locked
- Group membership changed
- Password reset

### Create alert ✕

Create an alert for '8man-demo.local' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Account locked for 8man-demo ✓				Information ▾

**WHEN YOU NEED AN ALERTING FOR A SET NUMBER OF EVENTS WITHIN A SET PERIOD OF TIME, THEN MAKE A THRESHOLD SETTING**

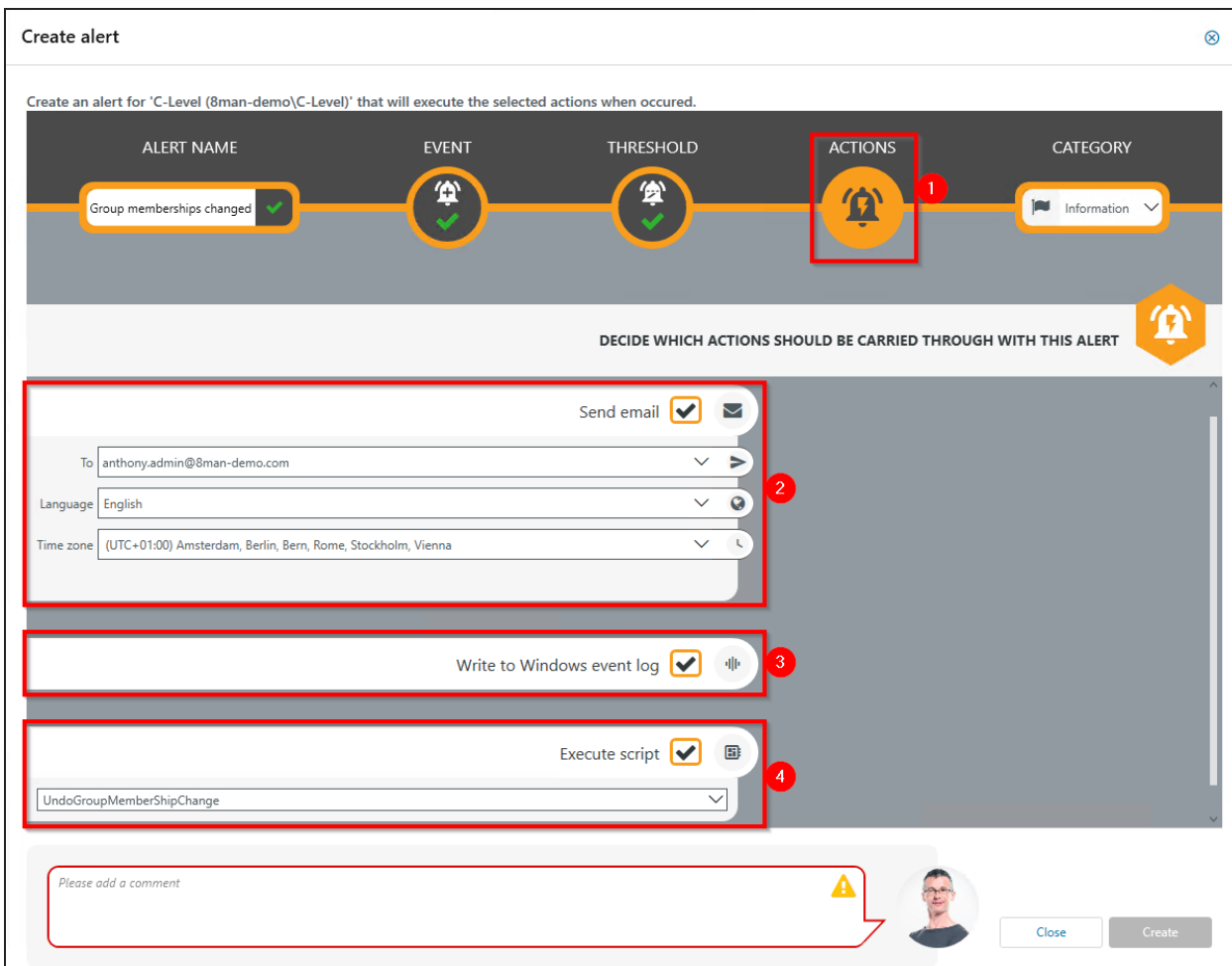
	Off <input checked="" type="checkbox"/> On	Turn threshold on
	No <input type="checkbox"/> Yes	caused by the same initiator
	10 - +	Required number of events to trigger alert
	10 - + Minutes ▾	Limit monitoring to a period of time

Alert when **10 events** are initiated by **different initiators** within a **duration of 10 Minutes** be initiated

**Your threshold is set**

Please add a comment ⚠

You can set a threshold if needed.



Create alert

Create an alert for 'C-Level (8man-demo\C-Level)' that will execute the selected actions when occurred.

ALERT NAME: Group memberships changed ✓


EVENT: ✓

THRESHOLD: ✓

ACTIONS: 1

CATEGORY: Information


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT


Send email  

To: anthony.admin@8man-demo.com


Language: English


Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Write to Windows event log  

Execute script  

UndoGroupMemberShipChange


Please add a comment 



### 1. Choose Actions.

Here you specify which actions are executed when an alert is triggered. You must activate at least one action.

### 2. Activate the option if an email should be sent in case of an alert.

 The content of the emails can be customized. This is analogous to the [recertification emails](#).

### 3. The alert is written to the Windows Event Log. The categorization is used. This option is especially useful if you are using a SIEM system.

### 4. Enable the execution of a script. To activate this option, a [script configuration](#) for alerts must be stored.

**Edit alert**

Edit an automatically executed alert for 'C-Level (8man-demo\C-Level)'.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Group memberships changed ✓				Information ▾

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT




- Write to Windows event log
- Execute script
- UndoGroupMemberShipChange ▾
- Write to SysLog**


Please add a comment


Activate this option to write the event to a Syslog server. Syslog servers need to be configured in the ARM configuration application under Server > [Syslog](#).

### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	<div style="border: 1px solid red; padding: 2px;"><input type="text" value="Information"/>   Information   Warning   Critical</div>


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 


Send email 


To:


Language:

Time zone:

Write to Windows event log 

Execute script 










Choose a category. This is used when writing to the Windows Event Log and for the email subject.

### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Mark <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	Information <input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input type="checkbox"/> Critical <input type="checkbox"/>


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 


Send email 



To:

Language:

Time zone:

Write to Windows event log 

Execute script 

1. You must specify a reason for the alert configuration in order to save it.
2. Click on "Create".



# File Server Logga

## The Problem

Security risks often arise when temporary access rights to sensitive documents are granted to unauthorized employees. These documents can then be read, deleted or even copied. If the access rights are removed immediately thereafter, then the security incident remains undiscovered. Who copied which files can no longer be understood.

## Confusing processes

Confusing access rights assignments can not be improved if the current state can not be analyzed. Who grants rights to whom and why? Where are problems commonplace? Which activities require more coordination? Only by analyzing past mistakes can you implement a sensible access rights process for your organization.

## The solution

ARM creates transparency over the access rights situation on your file server. The FS Logga expands this transparency to the entire access and change history in your system. Even actions performed outside of ARM are captured. Temporary access rights and other changes with security implications become understandable immediately.

By configuring reports you can identify differences in your access rights structure. Access and changes of sensitive data, including deleting copying, moving and modifying are logged with the FS Logga.

## This is what you can achieve with the FS Logga

- Administrators get a full picture of all actions being performed on a given file server. This allows you to optimize access rights processes.
- Auditors can easily identify security incidents related to sensitive data including the involved actors.
- The executive department can be certain: The FS Logga provides all necessary data for more security and process improvement and makes security related incidents completely transparent.

## Monitor access to sensitive file server data

### Background / Value

As a first step you have hopefully limited access rights to sensitive directories. As a second step we recommend the continuous monitoring of access by individual users, including the exact actions that they performed. This ensures full process transparency for especially sensitive data and information.

## Related features

### [Grant and remove file server access rights](#)

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main navigation menu contains: Start (highlighted with a red box and a red circle with '1'), Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, and Status. The main content area is divided into several sections:

- Start - Home**: Includes navigation icons for HOME, NOTES (10), REQUESTS, TASKS, and REPORTS (1).
- Quick links**: Easy orientation, find the best tool for your productivity in ARM.
- Permission Analysis**:
  - Where does a user/group have access?
- User Provisioning**:
  - Accounts**: Create new user or group, Edit group memberships.
  - Resources**: Edit access rights.
- Security Monitoring**:
  - Alerts**: Manage alerts.
  - File server**: Who did what, except authorized users (SoD)?, **Who did what?** (highlighted with a red box and a red circle with '2'), Who made changes?
  - Active Directory**: AD Logga Report.
  - Exchange**: Exchange Logga Report.
  - OneDrive**: OneDrive Logga Report.
  - SharePoint**: SharePoint Logga Report.
- Documentation & Reporting**:
  - Reports overview (1).
  - Where has the user/group access?
  - Who has access where?
  - File server**: All 'Authenticated users' permissions, All 'Everyone' permissions, All users with direct access, Directories without administrative owners, Permission difference, Unresolved SIDs, Where have employees of a manager access (file server)?, Who has access through which permission groups?
  - Active Directory**: Account Details, Inactive accounts, Local accounts, Manager-Employees, OU Members and group memberships, Users and groups (Kerberos, Last logon).
  - Exchange**: Exchange mailbox permissions.

1. Select "Start".

2. Click on "Who did what?" in the "Security Monitoring" area.

ARM Access Rights Manager

Search

Anthony Admin

### Who did what?

**Report configuration**

1 Title

1 Comment

2 Reference period Fixed time span 9/24/2018 3:19 PM - 9/26/2018 3:19 PM

3 Resource D:\Organization (SRV-8MAN)

4 Monitored actions

Click here to select the actions you want to collect in the report or leave this field empty, to create the report for all configured actions

Authors

Please select account to filter or leave this field empty, to create the report for all existing accounts

**Settings**

The output format is PDF

Report execution mode started manually

Custom storage path is not configured

Send email is Deactivated

**Who did what?**

Monitored actions

Filter 6

- Directory / file created
- Directory / file deleted
- Directory / file moved or renamed
- File read
- File written
- Permission (ACL) changed

Cancel Start

1. Enter a title for the report and add a comment.
2. Specify the period of time for logging events in the report.
3. Add resources. You can only add resources that are included in the [FS Logga configuration](#).
4. Add recorded actions. Leave the entry blank if you want the report to contain all actions.

The screenshot shows the 'Who did what?' configuration window in the Access Rights Manager. It is split into two main sections. The left section, 'Report configuration', includes fields for Title, Comment, Reference period (Fixed time span 9/24/2018 3:19 PM - 9/26/2018 3:19 PM), Resource (D:\Organization (SRV-8MAN)), Monitored actions, Authors (Emily Employee (8man-demo\Emily Employee)), and Settings (output format: PDF, execution mode: started manually, custom storage path: not configured, send email: deactivated). The right section, 'Who did what?', has a search and filter area with 'emily' entered, showing a list of users including 'Emily Employee (8man-demo\Emily Employee)' and 'Emily Laursen (8man-demo\Emily Laursen)'. Red callouts 1, 2, and 3 point to the Authors field, the Settings section, and the Start button, respectively.

1. Add authors. Use filter and search to find the desired users. Leave the entry blank if you want the report to contain all actions.
2. Define the desired output settings:
  - Format: PDF or XLS
  - Scheduling of regular reports
  - Saving location
  - send via email
3. Start the report.

## Enable alerts for file server directories

### Background / Value

Monitor targeted safety-critical directories by defining directory-specific alerts. Should an access be made to a security-relevant directory, ARM sends an alert to the data controller.

### Related features

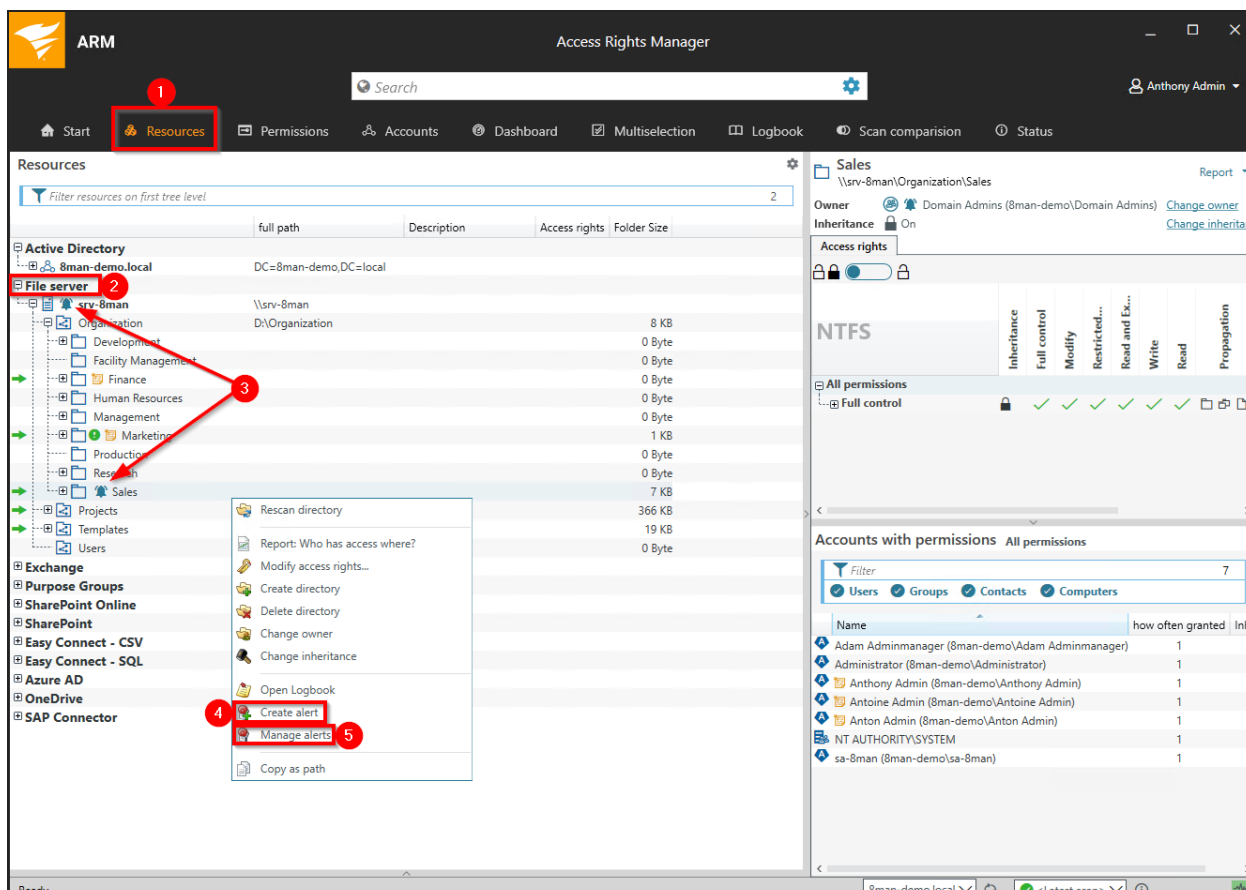
[Enable alerts for suspected data theft \(file server\)](#)

[Enable alerts for data deletion \(file server\)](#)

[Enable alerts for suspected cases on ransomware \(file server\)](#)

[Manage alerts](#)

### Step-by-step process



1. Choose Resources.
2. Expand the "file server".
3. Already configured alerts are displayed with a bell symbol.

4. Right-click on a resource and select "Create alert" in the context menu to create a new alert.
5. Right-click a resource and select [Manage alerts](#) in the context menu to customize or delete existing alerts.

### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Mark <span style="float: right;">✓</span>				Information <span style="float: right;">▼</span>

**EVENT SETTING FOR 'CHANGES IN DIRECTORY'**

DIRECTORIES	FILES
Directory created <input type="checkbox"/>	File created <input type="checkbox"/>
Directory deleted <input type="checkbox"/>	File deleted <input type="checkbox"/>
Directory moved or renamed <input type="checkbox"/>	File moved or renamed <input type="checkbox"/>
Directory permission (ACL) changed <input checked="" type="checkbox"/>	File read <input type="checkbox"/>
Directory depth 0 <input type="text"/> -- +∞	File written <input type="checkbox"/>
	File permission (ACL) changed <input checked="" type="checkbox"/>

0 [Blacklist Users](#)

0 [Blacklist Directories](#)

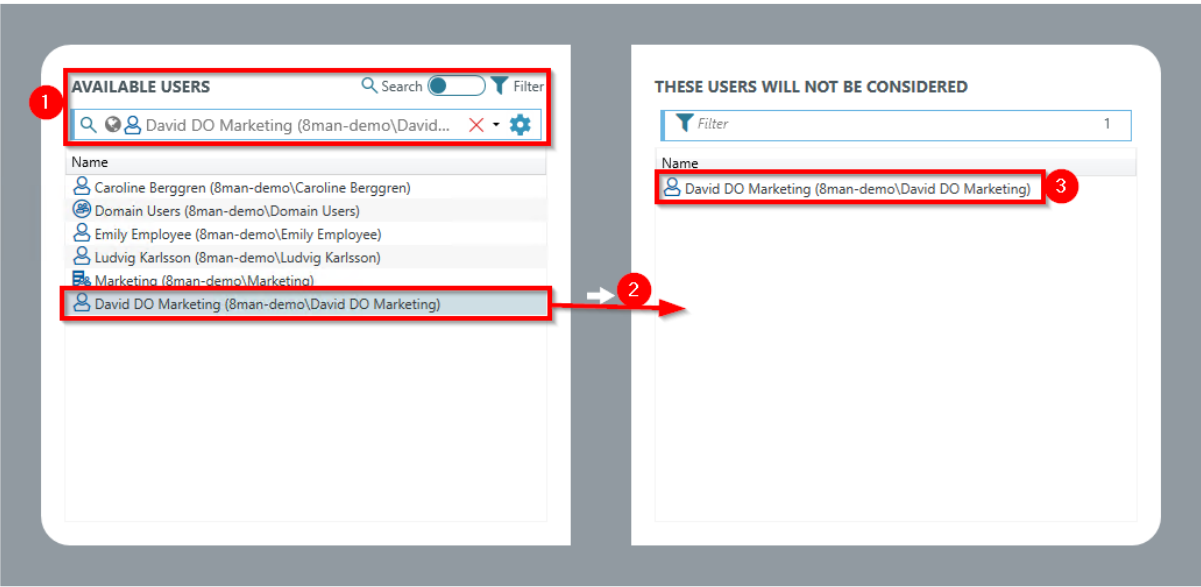
Please add a comment

[Close](#)
[Create](#)

1. Give the alert configuration a name.
2. Define which events trigger an alert.
3. Optional: Click on "Blacklist user".

**Blacklist Users** ⊗

Please choose one or more users below which are not considered for the alert



**AVAILABLE USERS** Search Filter

David DO Marketing (8man-demo\David... X ⚙️)

Name

- Caroline Berggren (8man-demo\Caroline Berggren)
- Domain Users (8man-demo\Domain Users)
- Emily Employee (8man-demo\Emily Employee)
- Ludvig Karlsson (8man-demo\Ludvig Karlsson)
- Marketing (8man-demo\Marketing)
- David DO Marketing (8man-demo\David DO Marketing)

**THESE USERS WILL NOT BE CONSIDERED** Filter 1

Name

- David DO Marketing (8man-demo\David DO Marketing)

Close Apply

Optional:

Use the blacklist to define which users do not trigger an alert.

**i** Each alert configuration has its own blacklist configuration.

**i** You can only add users, not groups.

1. Use the search function to find the users you want.
2. Use double-click or drag-and-drop to add users to the blacklist.
3. Use the "Del" key to remove users from the blacklist.
4. Click "Apply" to save the changes.

**Create alert**
✕

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME  
Changes in directory for Marki ✓

EVENT

THRESHOLD

ACTIONS !

CATEGORY  
Information ▾

EVENT SETTING FOR 'CHANGES IN DIRECTORY'

DIRECTORIES	FILES
Directory created <input type="checkbox"/>	<input type="checkbox"/> File created
Directory deleted <input type="checkbox"/>	<input type="checkbox"/> File deleted
Directory moved or renamed <input type="checkbox"/>	<input type="checkbox"/> File moved or renamed
Directory permission (ACL) changed <input checked="" type="checkbox"/>	<input type="checkbox"/> File read
Directory depth 0 <span style="font-size: 0.8em;">- + ∞</span>	<input type="checkbox"/> File written
	<input checked="" type="checkbox"/> File permission (ACL) changed

0 [Blacklist Users](#)

0 [Blacklist Directories](#)

Please add a comment

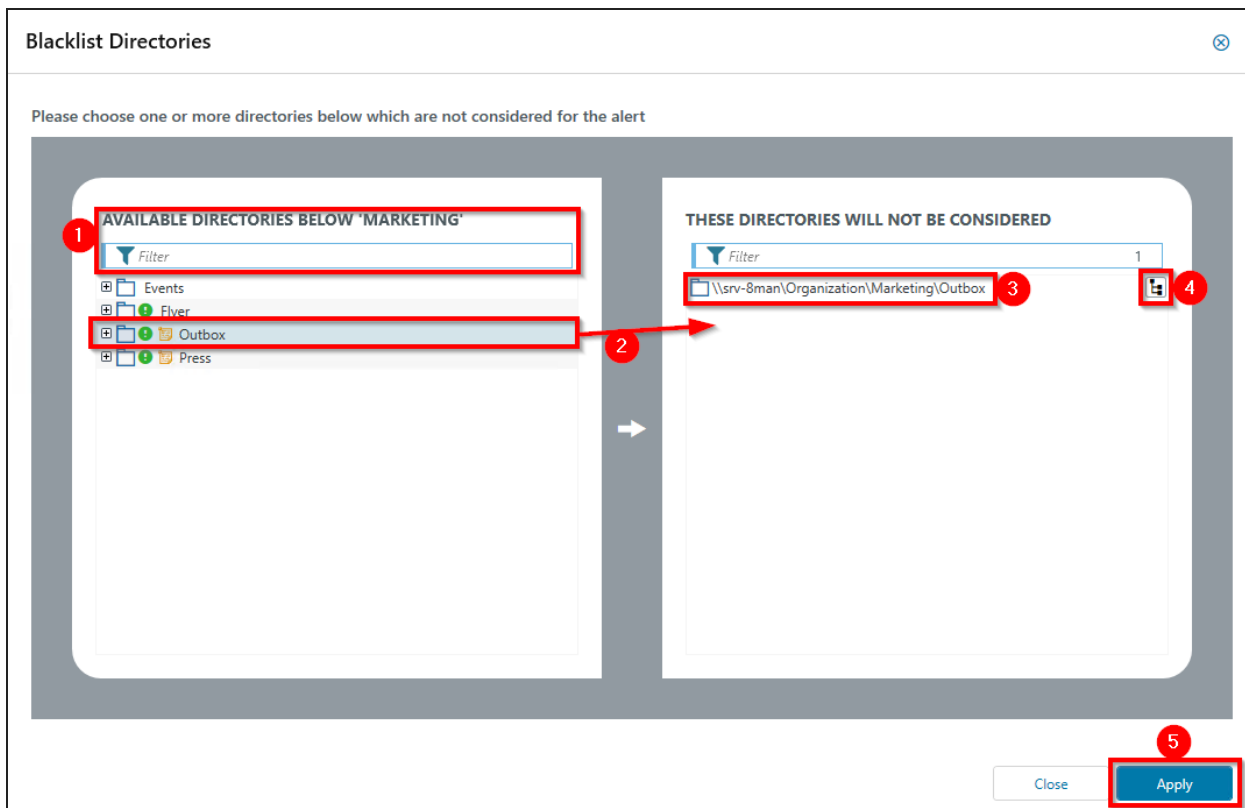
Close

Create

Optional:

Select "Blacklist Directories".








Optional:


Use the blacklist to define which directories are not monitored.


1. Use the filter function to find the desired directories. When you filter, the tree view changes to a result list of the directory paths.
2. Use double-click or drag-and-drop to add directories to the blacklist.
3. Use the "Delete" key to remove directories from the blacklist.
4. Enable or disable monitoring of subdirectories.
5. Click "Apply" to save the changes.

**Create alert** ✕

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/> <span>1</span>	Information <input type="text"/>


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 


Send email  


To:


Language:

Time zone:

Write to Windows event log  


Execute script  

Please add a comment 



1. Choose Actions. Here you specify which actions are executed when an alert is triggered. You must activate at least one action.

2. Activate the option if an email should be sent in case of an alert.




 The content of the emails can be customized. This is analogous to the [recertification emails](#).


3. The alert is written to the Windows Event Log. The categorization is used.




4. Enable the execution of a script. To activate this option, a [script configuration](#) for alerts must be stored.


**Edit alert** ✕


Edit an automatically executed alert for 'C-Level (8man-demo\C-Level)'.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Group memberships changed <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>		Information <input type="checkbox"/>

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 

- Write to Windows event log 
- Execute script   
UndoGroupMemberShipChange
- Write to SysLog 

Please add a comment 



Activate this option to write the event to a Syslog server. Syslog servers need to be [configured in the ARM configuration application](#) under Server > Syslog.

### Create alert ✕

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Mark <span style="float: right;">✔</span>				<div style="border: 1px solid #ccc; padding: 2px;"> <span style="float: right;">▼</span>                     Information                      Information                      Warning                      Critical                 </div>

**DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT**

**Send email**

To:  ▼

Language:  ▼

Time zone:  ▼

---

**Write to Windows event log**

---

**Execute script**

▼

*Please add a comment*

Choose a category. This is used when writing to the Windows Event Log and for the email subject.

Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Mark				Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To: anthony.admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Write to Windows event log

Execute script

start malware scan

Please add a comment

Close Create

1. You must specify a reason for the alert configuration in order to save it.
2. Click on "Create".

## Enable alerts for suspected data theft (file server)

### Background / Value

To efficiently capture security incidents, ARM focuses on user-initiated file server events. If these occur in unusually high numbers and additionally in a short period of time, ARM proactively informs all those responsible.

Data theft: A user account reads an unusually large number of files in a short period of time.

### Related features

[Enable alerts for file server directories](#)

[Enable alerts for data deletion \(file server\)](#)

[Enable alerts for suspected cases on ransomware \(file server\)](#)

[Manage alerts](#)

## Step-by-step process

The screenshot displays the ARM interface with the following elements:

- 1**: The "Resources" tab is selected in the top navigation bar.
- 2**: The "File server" resource is expanded in the left-hand tree view.
- 3**: A red arrow points to a bell icon next to the "Sales" folder, indicating an existing alert.
- 4**: A context menu is open over a resource, with "Create alert" highlighted.
- 5**: The "Manage alerts" option is highlighted in the context menu.

The right-hand pane shows the "Sales" resource details, including the owner (Domain Admins), inheritance status (On), and a table of permissions. The "Accounts with permissions" section lists several accounts with their respective permission levels.

Name	how often granted	Inhe
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	
Administrator (8man-demo\Administrator)	1	
Anthony Admin (8man-demo\Anthony Admin)	1	
Antoine Admin (8man-demo\Antoine Admin)	1	
Anton Admin (8man-demo\Anton Admin)	1	
NT AUTHORITY\SYSTEM	1	
sa-8man (8man-demo\sa-8man)	1	

1. Choose Resources.
2. Expand the "file server".
3. Already configured alerts are displayed with a bell symbol.
4. Right-click on a resource and select "Create alert" in the context menu to create a new alert.
5. Right-click a resource and select [Manage alerts](#) in the context menu to customize or delete existing alerts.

Create alert

Create an alert for 'Sales' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
1 Suspected data theft	2			Information

EVENT SETTING FOR 'CHANGES IN DIRECTORY'

DIRECTORIES	FILES
Directory created <input type="checkbox"/>	File created <input type="checkbox"/>
Directory deleted <input type="checkbox"/>	File deleted <input type="checkbox"/>
Directory moved or renamed <input type="checkbox"/>	File moved or renamed <input type="checkbox"/>
Directory permission (ACL) changed <input type="checkbox"/>	3 <input checked="" type="checkbox"/> File read
Directory depth 0 --+∞	File written <input type="checkbox"/>
	File permission (ACL) changed <input type="checkbox"/>

4 0 Blacklist Users

Please add a comment

1. Give the alert configuration a name.
2. Choose "Event".
3. Define which events trigger an alert. In case of suspected data theft typical: "File read".
4. Optional: Click on "Blacklist user".

**Blacklist Users** ✕

Please choose one or more users below which are not considered for the alert

**AVAILABLE USERS** Search  Filter

✕ ⚙

Name

- Caroline Berggren (8man-demo\Caroline Berggren)
- Domain Users (8man-demo\Domain Users)
- Emily Employee (8man-demo\Emily Employee)
- Ludvig Karlsson (8man-demo\Ludvig Karlsson)
- Marketing (8man-demo\Marketing)
- David DO Marketing (8man-demo\David DO Marketing)

**THESE USERS WILL NOT BE CONSIDERED**

Filter 1

Name

- David DO Marketing (8man-demo\David DO Marketing)

Close Apply

Optional: Use the blacklist to define which users do not trigger an alert.

i Each alert configuration has its own blacklist configuration.




i You can only add users, not groups.


1. Use the search function to find the users you want.
2. Use double-click or drag-and-drop to add users to the blacklist.
3. Use the "Delete" key to remove users from the blacklist.
4. Click "Apply" to save the changes.





### Create alert ✕

Create an alert for 'Marketing' that will execute the selected actions when occurred.


ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marketing <span style="float: right;">✓</span>				Information <span style="float: right;">▼</span>


**EVENT SETTING FOR 'CHANGES IN DIRECTORY'** 

DIRECTORIES 	FILES 
Directory created <input type="checkbox"/>	File created <input type="checkbox"/>
Directory deleted <input type="checkbox"/>	File deleted <input type="checkbox"/>
Directory moved or renamed <input type="checkbox"/>	File moved or renamed <input type="checkbox"/>
Directory permission (ACL) changed <input checked="" type="checkbox"/>	File read <input type="checkbox"/>
Directory depth 0 <span style="font-size: small;">-- +∞</span>	File written <input type="checkbox"/>
	File permission (ACL) changed <input checked="" type="checkbox"/>

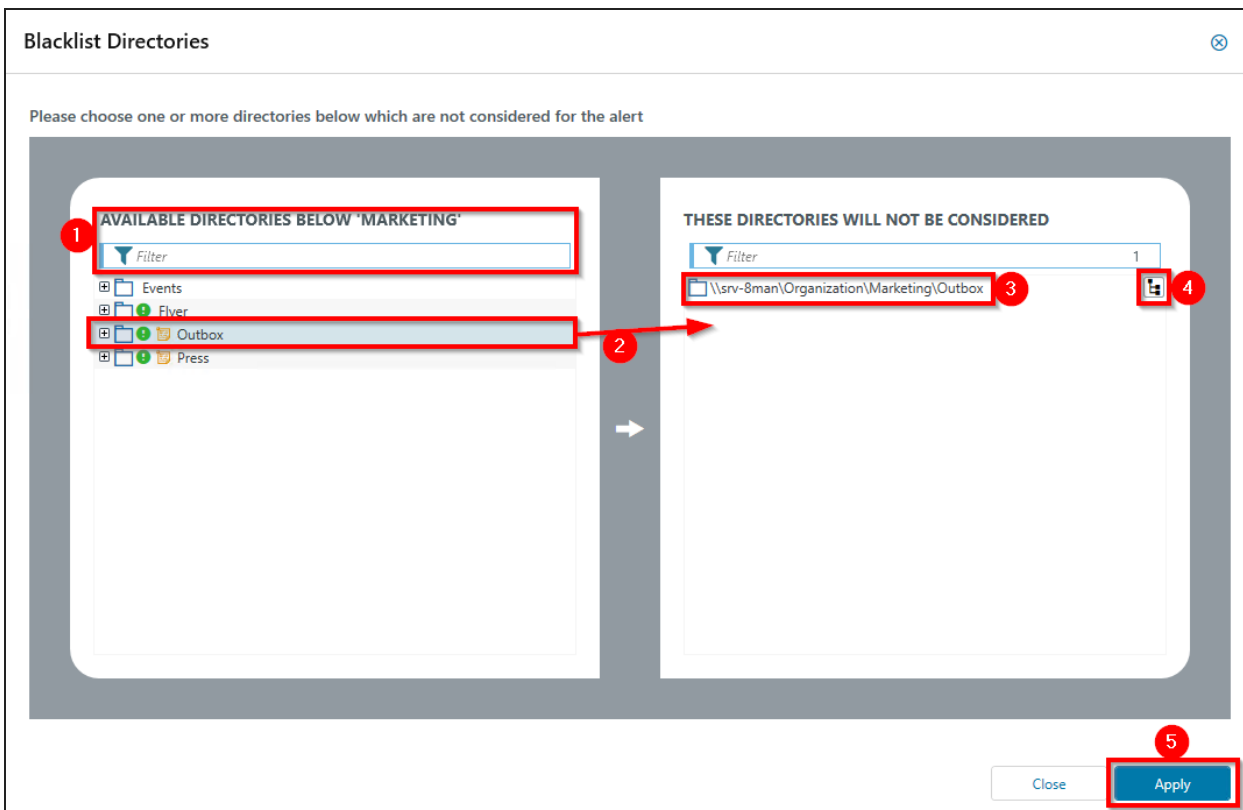
0 [Blacklist Users](#)

0 Blacklist Directories

Please add a comment 


Close Create

Optional: Select "Blacklist directories".



Optional: Use the blacklist to define which directories are not monitored.

1. Use the filter function to find the desired directories. When you filter, the tree view changes to a result list of the directory paths.
2. Use double-click or drag-and-drop to add directories to the blacklist.
3. Use the "Delete" key to remove directories from the blacklist.
4. Enable or disable monitoring of subdirectories.
5. Click "Apply" to save the changes.

**Edit alert**

Edit an automatically executed alert for '\\srv-8man'.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
suspicion of ransom ware				Information

WHEN YOU NEED AN ALERTING FOR A SET NUMBER OF EVENTS WITHIN A SET PERIOD OF TIME, THEN MAKE A THRESHOLD SETTING

	Off <input type="checkbox"/> On <input checked="" type="checkbox"/>	Turn threshold on
	No <input type="checkbox"/> Yes <input checked="" type="checkbox"/>	caused by the same initiator
	500 --+	Required number of events to trigger alert
	3 --+ Seconds	Limit monitoring to a period of time

Alert when **500 events** are initiated by **the same initiator** within a **duration of 3 Seconds** be initiated

Your threshold is set

Please add a comment

[Close](#) [Apply](#)

1. Select "Threshold".
2. Enable threshold.
3. Activate the option. If data theft is suspected, typically all events are triggered by a single user.
4. Define how many events within a period trigger the alert.

**Create alert**

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki ✓			1	Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To: anthony.admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Write to Windows event log

Execute script

start malware scan

Please add a comment

Close Create

1. Choose Actions. Here you specify which actions are executed when an alert is triggered. You must activate at least one action (arrows).

2. Activate the option if an email should be sent in case of an alert.




The content of the emails can be customized. This is analogous to the [recertification emails](#).


3. The alert is written to the Windows Event Log. The categorization is used.


4. Enable the execution of a script. To activate this option, a [script configuration](#) for alerts must be stored.

**Create alert** ✕

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Mark <span>✓</span>	 <span>✓</span>	 <span>✓</span>		<div style="border: 1px solid red; padding: 2px;"><span>Information</span> <span>▼</span> Information Warning Critical</div>


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 


Send email 

To:  ▼ ▶


Language:  ▼ ⌂

Time zone:  ▼ ⌂


Write to Windows event log 

Execute script 

▼

⚠ 

Choose a category. This is used when writing to the Windows Event Log and for the email subject.

 This option is especially useful if you are using a SIEM system.

### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki ✓				Information Information Warning Critical

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To: anthony.admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Write to Windows event log

Execute script

start malware scan

Please add a comment

Close Create

1. You must specify a reason for the alert configuration in order to save it.
2. Click "Apply".

## Enable alerts for data deletion (file server)

### Background / Value

To efficiently capture security incidents, ARM focuses on user-initiated file server events. If these occur in unusually high numbers and additionally in a short period of time, ARM proactively informs all those responsible.

Data deletions: A user account deletes very many files in a short period of time.

### Related features

[Enable alerts for file server directories](#)

[Enable alerts for suspected data theft \(file server\)](#)

[Enable alerts for suspected cases on ransomware \(file server\)](#)

[Manage alerts](#)

### Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The left pane displays a tree view of resources under the 'File server' section. The middle pane shows the details for the selected resource, including the path, owner, and inheritance settings. The right pane shows the 'All permissions' section, which is currently set to 'Full control'. Below this, the 'Accounts with permissions' section lists various accounts and their access levels.

The steps are numbered as follows:

1. Click the 'Resources' tab in the top navigation bar.
2. Expand the 'File server' section in the left pane.
3. Right-click on the 'Sales' folder in the left pane.
4. Select 'Create alert' from the context menu.
5. Select 'Manage alerts' from the context menu.

1. Choose Resources.

2. Expand the "file server".
3. Already configured alerts are displayed with a bell symbol.
4. Right-click on a resource and select "Create alert" in the context menu to create a new alert.
5. Right-click a resource and select [Manage alerts](#) in the context menu to customize or delete existing alerts.

### Create alert ✕

Create an alert for 'Sales' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS !	CATEGORY
Data deletion <span style="float: right;">✔</span>				Information <span style="float: right;">▼</span>

**EVENT SETTING FOR 'CHANGES IN DIRECTORY'**

DIRECTORIES	FILES
Directory created <input type="checkbox"/>	File created <input type="checkbox"/>
Directory deleted <input checked="" type="checkbox"/>	File deleted <input checked="" type="checkbox"/>
Directory moved or renamed <input type="checkbox"/>	File moved or renamed <input type="checkbox"/>
Directory permission (ACL) changed <input type="checkbox"/>	File read <input type="checkbox"/>
Directory depth 0 <input type="text"/> --+∞	File written <input type="checkbox"/>
	File permission (ACL) changed <input type="checkbox"/>

0 [Blacklist Users](#)

Please add a comment ⚠

Close Create

1. Give the alert configuration a name.
2. Choose "Event".
3. Define which events trigger an alert. For data deletions typically: "directory deleted" and "file deleted".
4. Optional: Click on "Blacklist user".



**Blacklist Users** ✕

Please choose one or more users below which are not considered for the alert

**AVAILABLE USERS** Search  Filter

✕ ⚙

Name

- Caroline Berggren (8man-demo\Caroline Berggren)
- Domain Users (8man-demo\Domain Users)
- Emily Employee (8man-demo\Emily Employee)
- Ludvig Karlsson (8man-demo\Ludvig Karlsson)
- Marketing (8man-demo\Marketing)
- David DO Marketing (8man-demo\David DO Marketing)

**THESE USERS WILL NOT BE CONSIDERED**

Filter 1

Name

- David DO Marketing (8man-demo\David DO Marketing)

Close Apply

Optional: Use the blacklist to define which users do not trigger an alert.

i Each alert configuration has its own blacklist configuration.

i You can only add users, not groups.

1. Use the search function to find the users you want.
2. Use double-click or drag-and-drop to add users to the blacklist.
3. Use the "Delete" key to remove users from the blacklist.
4. Click "Apply" to save the changes.

### Create alert ✕

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marketing <span style="color: green;">✔</span>				Information <span style="font-size: small;">▼</span>

**EVENT SETTING FOR 'CHANGES IN DIRECTORY'**

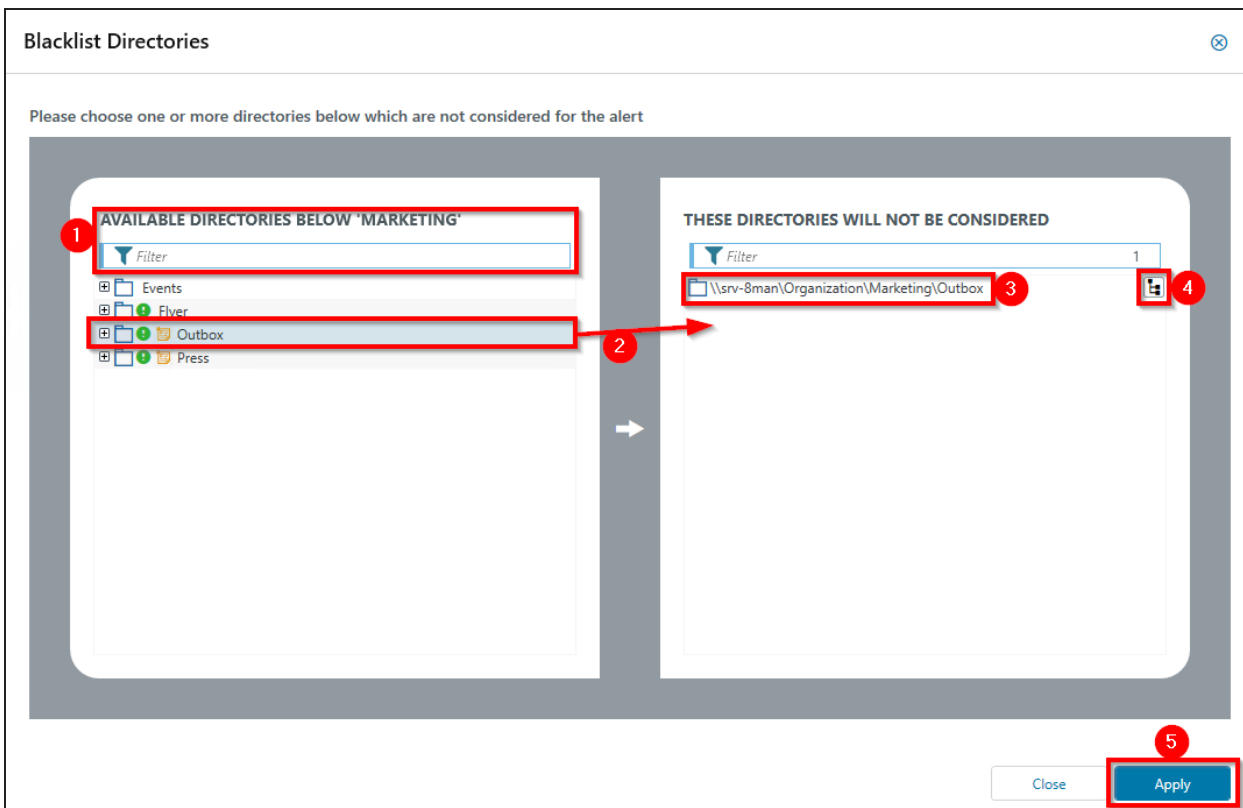
DIRECTORIES	FILES
Directory created <input type="checkbox"/>	File created <input type="checkbox"/>
Directory deleted <input type="checkbox"/>	File deleted <input type="checkbox"/>
Directory moved or renamed <input type="checkbox"/>	File moved or renamed <input type="checkbox"/>
Directory permission (ACL) changed <input checked="" type="checkbox"/>	File read <input type="checkbox"/>
Directory depth 0 <span style="font-size: small;">- + ∞</span>	File written <input type="checkbox"/>
	File permission (ACL) changed <input checked="" type="checkbox"/>

0 [Blacklist Users](#)

0 Blacklist Directories

Please add a comment

Optional: Select "Blacklist directories".



Optional: Use the blacklist to define which directories are not monitored.

1. Use the filter function to find the desired directories. When you filter, the tree view changes to a result list of the directory paths.
2. Use double-click or drag-and-drop to add directories to the blacklist.
3. Use the "Delete" key to remove directories from the blacklist.
4. Enable or disable monitoring of subdirectories.
5. Click "Apply" to save the changes.

**Edit alert**

Edit an automatically executed alert for '\\srv-8man'.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
suspicion of ransom ware ✓				Information ▾

WHEN YOU NEED AN ALERTING FOR A SET NUMBER OF EVENTS WITHIN A SET PERIOD OF TIME, THEN MAKE A THRESHOLD SETTING

	Off <input type="checkbox"/> On <input checked="" type="checkbox"/>	Turn threshold on
	No <input type="checkbox"/> Yes <input checked="" type="checkbox"/>	caused by the same initiator
	500 - +	Required number of events to trigger alert
	3 - + Seconds ▾	Limit monitoring to a period of time

Alert when 500 events are initiated by the same initiator within a duration of 3 Seconds be initiated

Your threshold is set




Please add a comment

[Close](#) [Apply](#)

1. Select "Threshold".
2. Enable threshold.
3. Activate the option.
4. Define how many events within a period trigger the alert.

Create alert


Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki ✓				Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

- Send email  
To: anthony.admin@8man-demo.local  
Language: English  
Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
- Write to Windows event log
- Execute script  
start malware scan

Please add a comment



1. Choose Actions. Here you specify which actions are executed when an alert is triggered. You must activate at least one action (arrows).

2. Activate the option if an email should be sent in case of an alert.

**i** The content of the emails can be customized. This is analogous to the [recertification emails](#).

3. The alert is written to the Windows Event Log. The categorization is used.

4. Enable the execution of a script. To activate this option, a [script configuration](#) for alerts must be stored.

### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Mark				Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To: anthony.admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Write to Windows event log

Execute script

start malware scan

Please add a comment




[Close](#) [Create](#)


Choose a category. This is used when writing to the Windows Event Log and for the email subject.


This option is especially useful if you are using a SIEM system.

### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>		Information <input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input type="checkbox"/> Critical <input type="checkbox"/>


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 


Send email 



To:

Language:

Time zone:

Write to Windows event log 

Execute script 

Please add a comment  

1. You must specify a reason for the alert configuration in order to save it.
2. Click "Create".

## Enable alerts for suspected cases on ransomware on file servers

### Background / Value

To efficiently capture security incidents, ARM focuses on user-initiated file server events. If these occur in unusually high numbers and additionally in a short period of time, ARM proactively informs all those responsible.

Ransomware Attack: The combination of file creation and deletion by one user account.

### Related features

[Enable alerts for file server directories](#)

[Enable alerts for suspected data theft \(file server\)](#)

[Enable alerts for data deletion \(file server\)](#)

[Manage alerts](#)

### Step-by-step process

The screenshot shows the ARM interface with the following elements:

- Navigation Menu:** Start, Resources (1), Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, Status.
- Resources Table:**

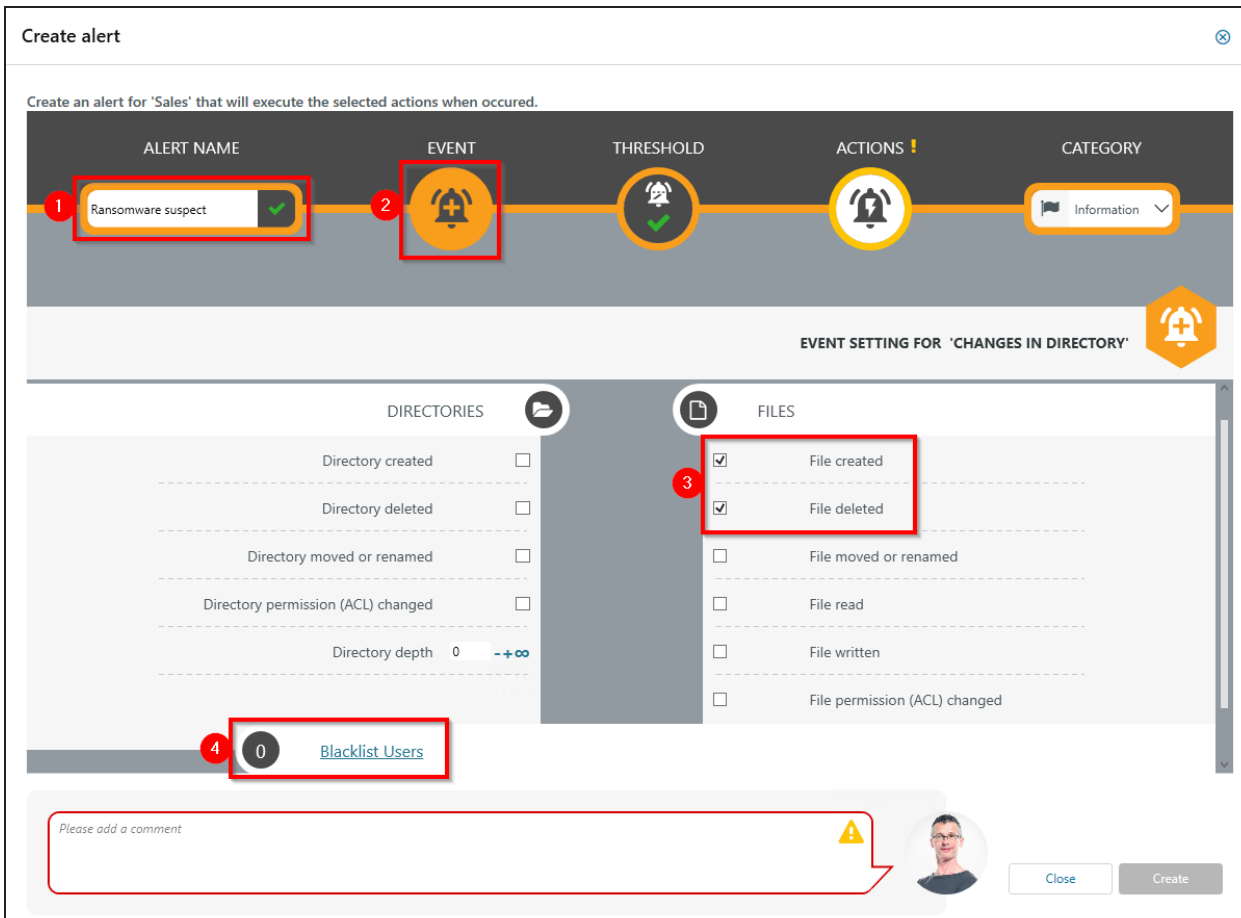
Resources	full path	Description	Access rights	Folder Size
Active Directory				
8man-demo.local		DC=8man-demo,DC=local		
File server				
srv-8man	\\srv-8man	D:\Organization		8 KB
Organization				0 Byte
Development				0 Byte
Facility Management				0 Byte
Finance				0 Byte
Human Resources				0 Byte
Management				0 Byte
Marketing				1 KB
Production				0 Byte
Research				0 Byte
Sales				7 KB
Projects				366 KB
Templates				19 KB
Users				0 Byte
- Permissions Pane (Right):** Shows NTFS permissions for the selected directory, including 'Full control' for 'Domain Admins'.
- Accounts with permissions:** A table listing accounts and their permission counts.
 

Name	how often granted	Inhe
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	
Administrator (8man-demo\Administrator)	1	
Anthony Admin (8man-demo\Anthony Admin)	1	
Antoine Admin (8man-demo\Antoine Admin)	1	
Anton Admin (8man-demo\Anton Admin)	1	
NT AUTHORITY\SYSTEM	1	
sa-8man (8man-demo\sa-8man)	1	

1. Choose Resources.






2. Expand the "file server".
3. Already configured alerts are displayed with a bell symbol.
4. Right-click on a resource and select "Create alert" in the context menu to create a new alert.
5. Right-click a resource and select [Manage alerts](#) in the context menu to customize or delete existing alerts.



Create alert


Create an alert for 'Sales' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS !	CATEGORY
Ransomware suspect				Information

EVENT SETTING FOR 'CHANGES IN DIRECTORY'

DIRECTORIES	FILES
Directory created <input type="checkbox"/>	<input checked="" type="checkbox"/> File created
Directory deleted <input type="checkbox"/>	<input checked="" type="checkbox"/> File deleted
Directory moved or renamed <input type="checkbox"/>	<input type="checkbox"/> File moved or renamed
Directory permission (ACL) changed <input type="checkbox"/>	<input type="checkbox"/> File read
Directory depth 0 <input type="text"/> <input type="button" value="-"/> <input type="button" value="+"/> <input type="button" value="∞"/>	<input type="checkbox"/> File written
	<input type="checkbox"/> File permission (ACL) changed

0 [Blacklist Users](#)

Please add a comment 

1. Give the alert configuration a name.
2. Choose "Event".
3. Define which events trigger an alert. Typical for ransomware: a combination of "file created" and "file deleted".
4. Optional: Click on "Blacklist users".

**Blacklist Users**

Please choose one or more users below which are not considered for the alert

**AVAILABLE USERS**

Search Filter

David DO Marketing (8man-demo\David...)

Name

- Caroline Berggren (8man-demo\Caroline Berggren)
- Domain Users (8man-demo\Domain Users)
- Emily Employee (8man-demo\Emily Employee)
- Ludvig Karlsson (8man-demo\Ludvig Karlsson)
- Marketing (8man-demo\Marketing)
- David DO Marketing (8man-demo\David DO Marketing)

**THESE USERS WILL NOT BE CONSIDERED**

Filter 1

Name

- David DO Marketing (8man-demo\David DO Marketing)

Close Apply

Optional: Use the blacklist to define which users do not trigger an alert.




**i** Each alert configuration has its own blacklist configuration.

**i** You can only add users, not groups.

1. Use the search function to find the users you want.
2. Use double-click or drag-and-drop to add users to the blacklist.
3. Use the "Delete" key to remove users from the blacklist.
4. Click "Apply" to save the changes.

### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.


ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marketing ✓				Information


EVENT SETTING FOR 'CHANGES IN DIRECTORY'

DIRECTORIES	FILES
Directory created <input type="checkbox"/>	File created <input type="checkbox"/>
Directory deleted <input type="checkbox"/>	File deleted <input type="checkbox"/>
Directory moved or renamed <input type="checkbox"/>	File moved or renamed <input type="checkbox"/>
Directory permission (ACL) changed <input checked="" type="checkbox"/>	File read <input type="checkbox"/>
Directory depth 0 <input type="text"/> -- +∞	File written <input type="checkbox"/>
	File permission (ACL) changed <input checked="" type="checkbox"/>

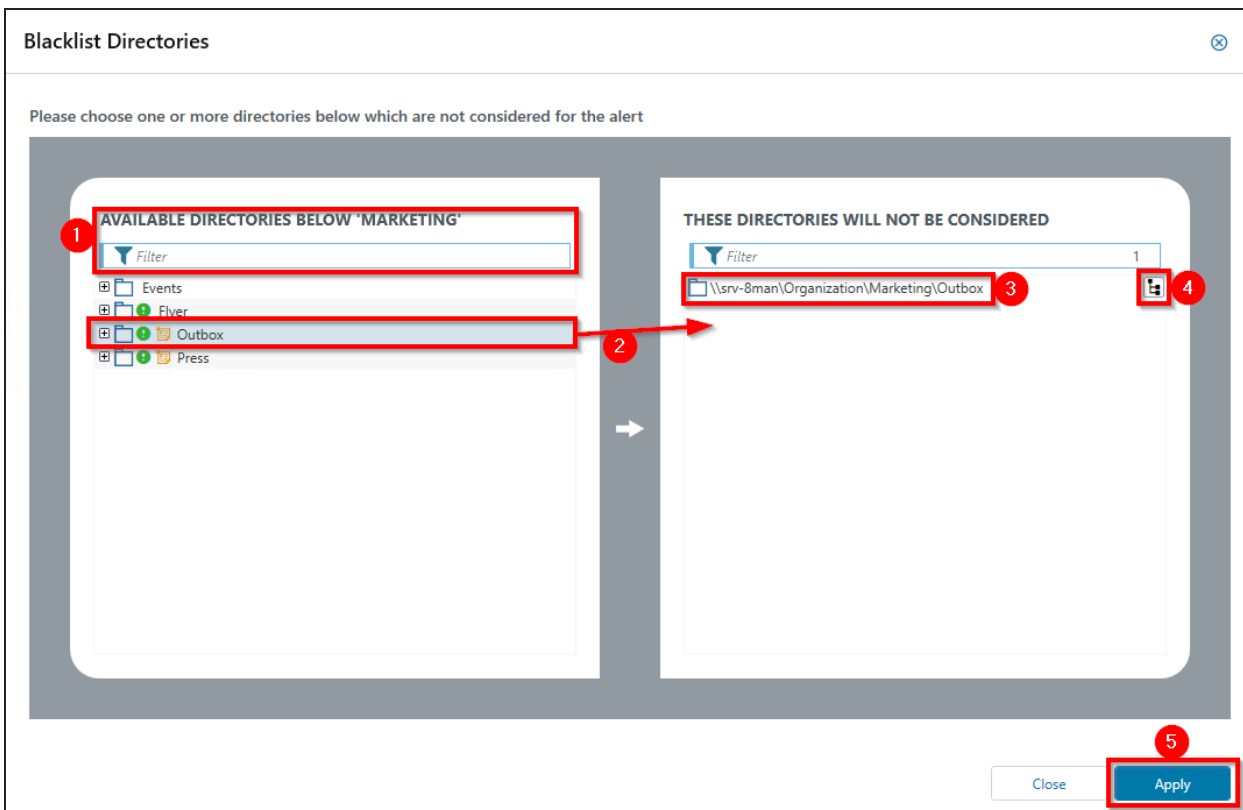
0 [Blacklist Users](#)

0 [Blacklist Directories](#)

Please add a comment 



Optional: Select "Blacklist directories".



Optional: Use the blacklist to define which directories are not monitored.

1. Use the filter function to find the desired directories. When you filter, the tree view changes to a result list of the directory paths.
2. Use double-click or drag-and-drop to add directories to the blacklist.
3. Use the "Delete" key to remove directories from the blacklist.
4. Enable or disable monitoring of subdirectories.
5. Click "Apply" to save the changes.

**Edit alert** ✕

Edit an automatically executed alert for '\\srv-8man'.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
suspicion of ransom ware <input checked="" type="checkbox"/>				Information <input type="checkbox"/>

WHEN YOU NEED AN ALERTING FOR A SET NUMBER OF EVENTS WITHIN A SET PERIOD OF TIME, THEN MAKE A THRESHOLD SETTING

	Off <input type="checkbox"/> On <input checked="" type="checkbox"/>	Turn threshold on
	No <input type="checkbox"/> Yes <input checked="" type="checkbox"/>	caused by the same initiator
	500 <input type="text"/>	Required number of events to trigger alert
	3 <input type="text"/> Seconds <input type="text"/>	Limit monitoring to a period of time

Alert when **500 events** are initiated by **the same initiator** within a **duration of 3 Seconds** be initiated Your threshold is set

Please add a comment




Close Apply


1. Select "Threshold".
2. Enable threshold.
3. Activate the option. When ransomware is suspected, typically all events are triggered by the same user.
4. Define how many events within a period trigger the alert.


Defining a threshold with a large number of events over a long period of time will consume a lot of memory (RAM). We recommend that you configure time intervals as small as possible.

**Create alert** ✕

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	Information <input type="checkbox"/>


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT 


Send email  

To: anthony.admin@8man-demo.local


Language: English


Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Write to Windows event log  

Execute script  


start malware scan

Please add a comment 



1. Choose Actions. Here you specify which actions are executed when an alert is triggered. You must activate at least one action (arrows).

2. Activate the option if an email should be sent in case of an alert.

 The content of the emails can be customized. This is analogous to the [recertification emails](#).

3. The alert is written to the Windows Event Log. The categorization is used.

4. Enable the execution of a script. To activate this option, a [script configuration](#) for alerts must be stored.

Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki ✓				Information Information Warning Critical

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To: anthony.admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Write to Windows event log

Execute script

start malware scan

Please add a comment

[Close](#) [Create](#)

Choose a category. This is used when writing to the Windows Event Log and for the email subject.

This option is especially useful if you are using a SIEM system.

### Create alert

Create an alert for 'Marketing' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Marki ✓				Information Information Warning Critical

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To: anthony.admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Write to Windows event log

Execute script

start malware scan

Please add a comment

Close Create

1. You must specify a reason for the alert configuration in order to save it.
2. Click "Create".



## Exchange Logga

Microsoft Exchange is used to centrally store and manage emails, appointments, contacts, and tasks. As a central solution for enterprise-wide collaboration, not only the question of access rights is relevant, but also a monitoring of the actual activities carried out.

The Exchange Logga logs activities of mailbox owners, their deputies, and administrators.

The following actions are particularly critical to safety:

- Hard Delete: Who deleted emails, contacts, or calendar entries from the Exchange server?
- MessageBind: Has an employee from the IT looked into my emails?
- SendAs: Who sent emails when in the name of my person?
- SendOnBehalf: Who sent emails when in my behalf?
- SoftDelete: Who (except me) has deleted emails in my mailbox?

### View activities in mailboxes, calendars, and contacts in logbook

#### **Background / Value**

Events recorded with the Exchange Logga can be analyzed in detail and recurrently using the report functions. Specific questions about Exchange changes can be answered faster with the logbook view.

#### **Related features**

Report: [Activities on mailboxes, calendars, and contacts](#)

#### **Step-by-step process**

1. Select "Logbook".
2. Set the time period for log analysis.
3. You use the filters to focus on the events that you want to check.
4. Select all events of a day (one row).

The screenshot displays the SolarWinds Access Rights Manager (ARM) Logbook. The main view is a calendar grid showing events from 8/27/2018 to Today. A red box labeled '1' highlights a cell on Wednesday, September 26, 2018. A second red box labeled '2' highlights a list of events for that date, showing two entries at 11:48 AM and 11:44 AM by IntegrationTestUser. A third red box labeled '3' highlights the details for the selected event, 'Mailbox - MoveToDeletedItems', which includes the operation name, description, folder path, and item subject.

1. Select a cell (an event type) to further narrow your query.
2. ARM displays a list of all selected events. The "Footprint icon with envelope" identifies events recorded by the Exchange Logga. Select an event.
3. ARM shows all details about the event.

## Report activities on mailboxes, calendars, and contacts

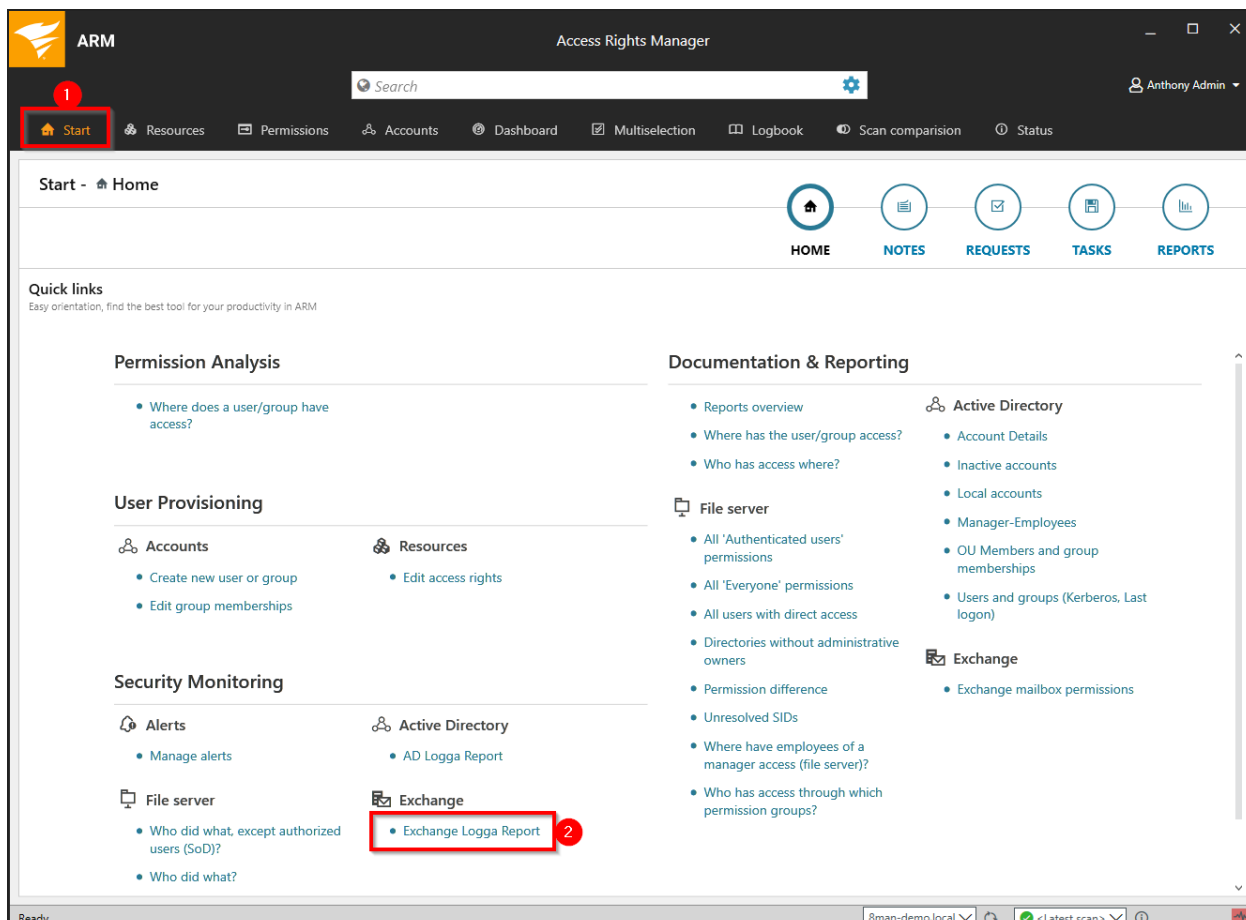
### Background / Value

Events recorded with the Exchange Logga can be analyzed in detail and recurrently using the report functions. Specific questions about Exchange changes can be answered faster with the logbook view.

Related features

[View activities in mailboxes, calendars, and contacts \(logbook\)](#)

### Step-by-step process



The screenshot shows the Access Rights Manager (ARM) interface. The top navigation bar includes a search bar, a settings gear, and the user name 'Anthony Admin'. The main navigation menu is located below the search bar, with the 'Start' button highlighted by a red box and a red circle with the number '1'. The main content area is divided into several sections: 'Permission Analysis', 'User Provisioning', 'Security Monitoring', 'Documentation & Reporting', 'Active Directory', and 'Exchange'. The 'Exchange' section is highlighted by a red box and a red circle with the number '2', and it contains the 'Exchange Logga Report' option.

1. Select "Start".
2. Click "Exchange Logga Report".

### Exchange Logga Report

#### Report configuration

1 Title

2 Comment

3 Time Period **Fixed time span** 3/10/2019 11:26 AM - 3/12/2019 11:26 AM

Show raw data only (affects only CSV)

#### Exchange Resources

8man-demo.com

#### Logon Type

All  
Administrator, delegate and mailbox owner

#### User accounts

Please select one or more accounts  
To search for all accounts leave this field empty.

#### Actions

Please select one or more actions  
To search for all actions leave this field empty.

#### Settings

The output format is [XLSX](#) ✓  
Report execution mode [started manually](#)  
Custom storage path is [not configured](#)  
Send email is [Deactivated](#)

#### Exchange Logga Report

##### Selection of monitored mailboxes

Filter 3

- 8man-demo.com
- IntegrationIestUser
- Gerd.ExLoggaTest

Cancel Start

1. Optional: Give the report a title and a description.
2. Set the period.
3. Add the required resources via drag & drop.

**Exchange Logga Report**

**Report configuration**

Title

Comment

Time Period [Fixed time span 3/10/2019 11:26 AM - 3/12/2019 11:26 AM](#)

Show raw data only (affects only CSV)

**Exchange Resources**

8man-demo.com

**Logon Type**

All  
Administrator, delegate and mailbox owner

**User accounts**

Please select one or more accounts  
To search for all accounts leave this field empty.

**Actions**

Please select one or more actions  
To search for all actions leave this field empty.

**Settings**

The output format is [CSV](#)

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

**Exchange Logga Report**

**Selection of monitored mailboxes**

Filter 3

8man-demo.com

IntegrationTestUser

Gerd.ExLoggaTest

Cancel Start

1. Select the login type.
2. If you have special users in focus, add them via drag & drop. For all users, leave the selection blank.
3. Optional: Select Actions.
4. Define output options for the report.
5. Start the execution.

# OneDrive Logga: Report activities on OneDrive

## Background / Value

OneDrive offers the possibility to store files and folders in the cloud. The advantages of the cloud service are obvious: employees can work together on documents easily and conveniently. Employees can also share documents with external partners as part of these collaborations. The interdependencies grow until it is no longer recognizable who shared which files with whom.

Events recorded with the OneDrive Logga can be analyzed in detail and recurrently using the report functions.

## Related topics

[Prepare the Office 365 integration](#)

[Add a OneDrive Logga configuration](#)

## Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The 'Start' button is highlighted with a red box and a red circle containing the number 1. Below the navigation bar, there are five main sections: HOME, NOTES (10), REQUESTS (1), TASKS, and REPORTS. The 'REPORTS' section is active. Under 'REPORTS', there are three sub-sections: 'Permission Analysis', 'User Provisioning', and 'Security Monitoring'. The 'Security Monitoring' section is expanded, showing 'Alerts', 'File server', 'Active Directory', 'Exchange', and 'OneDrive'. The 'OneDrive' section is highlighted with a red box and a red circle containing the number 2, and it contains the 'OneDrive Logga Report' option.

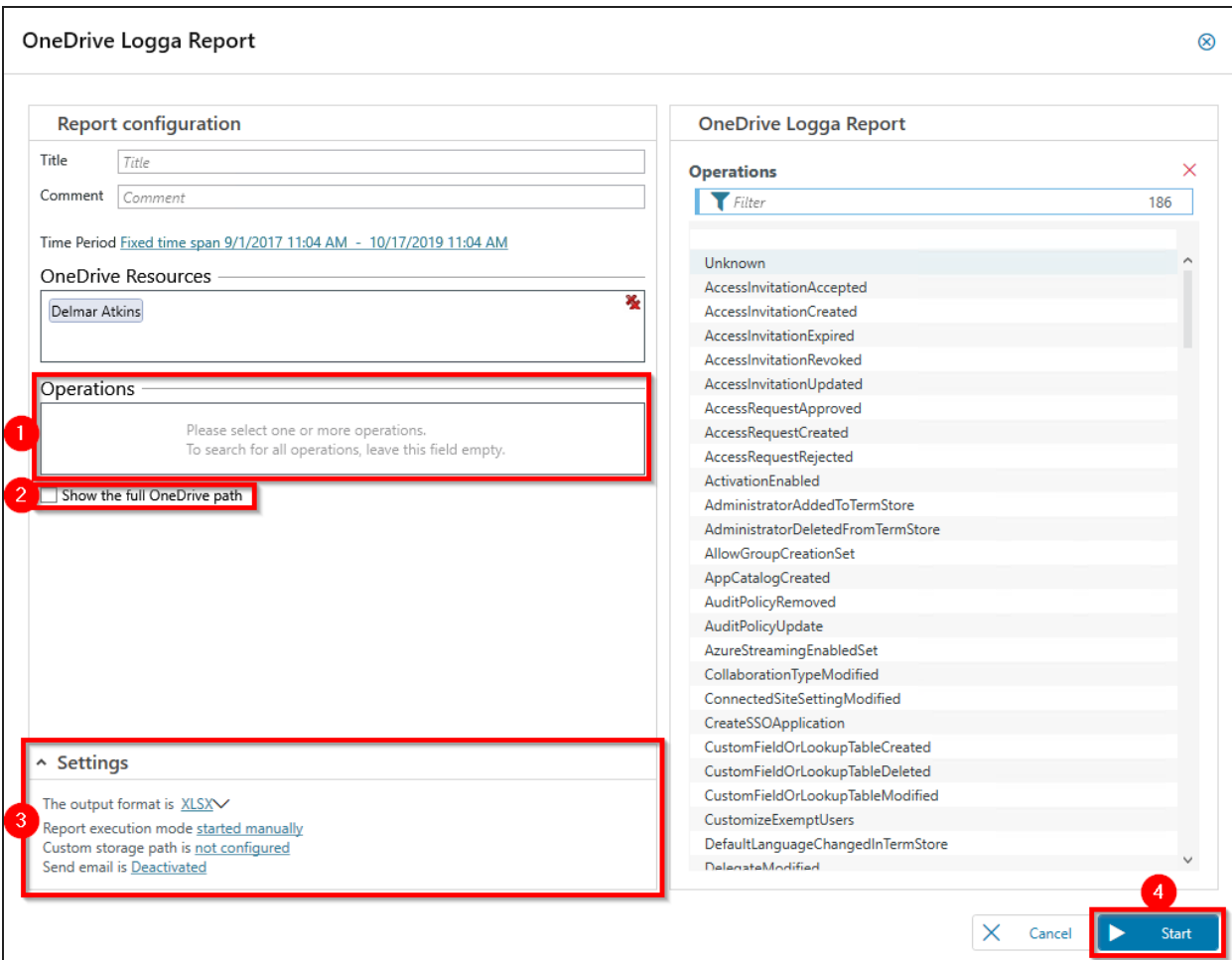
1. Select "Start".

## 2. Click "OneDrive Logga Report".

The screenshot shows the "OneDrive Logga Report" configuration window. It is divided into two main panels. The left panel, titled "Report configuration", contains fields for "Title" and "Comment", a "Time Period" dropdown set to "Fixed time span 10/15/2019 11:04 AM - 10/17/2019 11:04 AM", a "OneDrive Resources" list with "Delmar Atkins" selected, an "Operations" section with instructions to select operations, and a "Settings" section at the bottom showing output format as XLSX, execution mode as started manually, storage path as not configured, and email as deactivated. The right panel, titled "OneDrive Logga Report", shows a "Selection of monitored OneDrive entry points" list with a filter set to 3 items: "8man-demo.com", "IntegrationTestUser", and "Delmar Atkins". Red callouts with numbers 1, 2, and 3 point to the "Report configuration" header, the "Time Period" dropdown, and the "Delmar Atkins" resource in the right panel, respectively. A red arrow also points from the "Delmar Atkins" resource in the right panel to the "Delmar Atkins" resource in the left panel. At the bottom right, there are "Cancel" and "Start" buttons.

1. Optional: Give the report a title and a description.
2. Set the period.
3. Add the desired resources via drag & drop.





**Report configuration**

Title

Comment

Time Period [Fixed time span 9/1/2017 11:04 AM - 10/17/2019 11:04 AM](#)

**OneDrive Resources**

**Operations**

Please select one or more operations.  
To search for all operations, leave this field empty.

Show the full OneDrive path

**Settings**

The output format is [XLSX](#) ✓

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

**OneDrive Logga Report**

**Operations**

186

- Unknown
- AccessInvitationAccepted
- AccessInvitationCreated
- AccessInvitationExpired
- AccessInvitationRevoked
- AccessInvitationUpdated
- AccessRequestApproved
- AccessRequestCreated
- AccessRequestRejected
- ActivationEnabled
- AdministratorAddedToTermStore
- AdministratorDeletedFromTermStore
- AllowGroupCreationSet
- AppCatalogCreated
- AuditPolicyRemoved
- AuditPolicyUpdate
- AzureStreamingEnabledSet
- CollaborationTypeModified
- ConnectedSiteSettingModified
- CreateSSOApplication
- CustomFieldOrLookupTableCreated
- CustomFieldOrLookupTableDeleted
- CustomFieldOrLookupTableModified
- CustomizeExemptUsers
- DefaultLanguageChangedInTermStore
- DeactivateModified

1. Optional: Specify the operations to be included in the report. Leave the field blank to create the report including all operations.
2. Activate this option to create a report with the full OneDrive path starting with https:\\...
3. Define the desired output options for the report.
4. Start the execution.

# SharePoint Online Logga: Report activities on SharePoint Online

## Background / Value

SharePoint Online offers the possibility to store files and folders in the cloud. The advantages of the cloud service are obvious: employees can work together on documents easily and conveniently. Employees can also share documents with external partners as part of these collaborations. The interdependencies grow until it is no longer recognizable who shared which files with whom.

Events recorded with the SharePoint Online Logga can be analyzed in detail and recurrently using the report functions.

## Related topics

[Prepare the Office 365 integration](#)

[Add a SharePoint Online Logga configuration](#)

## Step-by-step process

The screenshot displays the Access Rights Manager (ARM) web application interface. The top navigation bar includes the ARM logo, a search bar, and the user name 'Anthony Admin'. The main content area is divided into several sections:

- Start - Home**: A navigation bar with icons for HOME, NOTES (10), REQUESTS (1), TASKS, and REPORTS (1).
- Quick links**: A section for easy orientation.
- Permission Analysis**: A section with a link: 'Where does a user/group have access?'.
- User Provisioning**: A section with links for 'Accounts' (Create new user or group, Edit group memberships) and 'Resources' (Edit access rights).
- Security Monitoring**: A section with links for 'Alerts' (Manage alerts), 'File server', 'Active Directory' (AD Logga Report), 'Exchange' (Exchange Logga Report), 'OneDrive' (OneDrive Logga Report), and 'SharePoint' (Sharepoint Logga Report).
- Documentation & Reporting**: A section with links for 'Reports overview' (1), 'Where has the user/group access?', 'Who has access where?', 'File server' (All 'Authenticated users' permissions, All 'Everyone' permissions, All users with direct access, Directories without administrative owners, Permission difference, Unresolved SIDs, Where have employees of a manager access (file server)?, Who has access through which permission groups?), 'Active Directory' (Account Details, Inactive accounts, Local accounts, Manager-Employees, OU Members and group memberships, Users and groups (Kerberos, Last logon)), and 'Exchange' (Exchange mailbox permissions).

The 'Start' button in the top navigation bar is highlighted with a red box and a red circle with the number '1'. The 'Sharepoint Logga Report' link in the Security Monitoring section is also highlighted with a red box and a red circle with the number '2'.

1. Select "Start".
2. Click "SharePoint Logga Report".

Sharepoint Logga Report

**Report configuration**

Title

Comment

Time Period **Fixed time span** 10/15/2019 11:34 AM - 10/17/2019 11:34 AM

**Sharepoint Resources**

8man-demo.com

**Operations**

Please select one or more operations.  
To search for all operations, leave this field empty.

**Settings**

The output format is [XLSX](#) ✓  
Report execution mode [started manually](#)  
Custom storage path is [not configured](#)  
Send email is [Deactivated](#)

**Sharepoint Logga Report**

Selection of monitored Sharepoint entry points

Filter 3

- 8man-demo.com
- 8mandemo-my.sharepoint.com
- 8mandemo.sharepoint.com

Cancel Start

1. Optional: Give the report a title and a description.
2. Set the period.
3. Add the desired resources via drag & drop.

**Report configuration**

Title

Comment

Time Period [Fixed time span 10/15/2019 11:34 AM - 10/17/2019 11:34 AM](#)

**Sharepoint Resources**

**Operations**

Please select one or more operations.  
To search for all operations, leave this field empty.

**Settings**

The output format is [XLSX](#) ✓  
Report execution mode [started manually](#)  
Custom storage path is [not configured](#)  
Send email is [Deactivated](#)

**Sharepoint Logga Report**

**Operations**

186

- Unknown
- AccessInvitationAccepted
- AccessInvitationCreated
- AccessInvitationExpired
- AccessInvitationRevoked
- AccessInvitationUpdated
- AccessRequestApproved
- AccessRequestCreated
- AccessRequestRejected
- ActivationEnabled
- AdministratorAddedToTermStore
- AdministratorDeletedFromTermStore
- AllowGroupCreationSet
- AppCatalogCreated
- AuditPolicyRemoved
- AuditPolicyUpdate
- AzureStreamingEnabledSet
- CollaborationTypeModified
- ConnectedSiteSettingModified
- CreateSSOApplication
- CustomFieldOrLookupTableCreated
- CustomFieldOrLookupTableDeleted
- CustomFieldOrLookupTableModified
- CustomizeExemptUsers
- DefaultLanguageChangedInTermStore
- DefaultLanguageModified

1. Optional: Specify the operations to be included in the report.
2. Define output options for the report.
3. Start the execution.

## Role & Process Optimization

The person with the best idea of who should have access and what they should be able to access is the data owner or the supervisor, not the IT-administrator. By introducing a role concept for analyzing and granting access rights, you are introducing the data awareness concept and corresponding action into the company.

You can map the organizational chart of your company with the data owner concept and cover all departments. Then you assign employees to the individual data owners. The data owners analyze or assign access rights to their staff.

An employee can use the ARM GrantMA to request access rights via a Web portal. The data owner then decides on the access rights in the department with a simple workflow.

## Delegation of tasks

ARM includes a variety of functionality that can benefit users who are not Administrators. ARM includes functionality that can benefit users that are not Administrators, depending on the size of your organization, sensitivity of your data as well as existing processes. Please note the following example:

COMPANY SIZE	IT MANAGER / AUDITOR / DATA SECURITY OFFICER	ADMINISTRATOR	DATA OWNER (MANAGER/TEAM LEAD)	HELP DESK
50+	Sees all reports	All ARM functionality	—	—
500+	Sees all reports	Analyzing all access rights, Creating users, Managing user and group accounts	Analyzing and administrating access rights of their employees to file servers.	—
>5,000	Sees all reports	Analyzing all access rights and administration of AD groups	Analyzing and administrating access rights of their employees to file servers.	Standardized user creation and continuous account management

## Apply an ARM account to a specific security role or data owner

There are two possibilities of involving data security officers and auditors in security related processes.

- Grant the user read only access to ARM.
- Define which reports are relevant and ARM will send them to the user automatically in the desired frequency.

Create a simple read-only account in ARM

### Background / Value

Involve security officers in the process of access rights management by granting them read-only access. This allows them to generate their own reports.

These settings can be found in the ARM configuration application. You can find more detailed information in the chapter ["Manage ARM Users"](#).

### Step-by-step process

The screenshot shows the 'Configuration' window of the Access Rights Manager (ARM) application. The main area is titled 'Users and Role Management' and is divided into two main sections: 'User Management' and 'List of accounts which can use ARM'. The 'User Management' section includes a search bar with the text 'audi' and a dropdown menu for selecting a role for the user 'Lucinda Baudinet'. The 'List of accounts which can use ARM' section displays a table of users and their roles.


Name	Role
Antoine Admin (8man-demo\Ant...	Administrator
Sebastian SAP (8man-demo\Seb...	Administrator
Anthony Admin (8man-demo\An...	Administrator
Anton Admin (8man-demo\Anto...	Administrator
Administrator (8MAN-DEMO\Ad...	Administrator
David DO Finance (8man-demo\...	Data Owner
David DO Manager (8man-demo...	Data Owner
David DO Marketing (8man-dem...	Data Owner
David DO HR (8man-demo\Dav...	Data Owner
David DO Sales (8man-demo\Da...	Data Owner
Helena Helpdesk (8man-demo\H...	IT Helpdesk
Lucinda Baudinet (8man-demo\L...	Auditor
Emily Employee (8man-demo\Em...	Requester (employee)
Henry HR (8man-demo\Henry HR)	No access

The dropdown menu for the 'Auditor' role is expanded, showing the following options:

- Administrators: Full access to ARM
- Data Owner: Read, change and create reports
- Auditor: Read and create reports** (selected)
- Requester (employee): Request access to resources in web client
- No access: No access to ARM

1. Start the ARM configuration application.

2. Select "User Management".
3. Use the search field to find the desired account.
4. Use drag&drop to move the account to the right column.
5. In the role column, select "Auditor".

 The settings are active immediately.

Schedule reports

## Background / Value

You can involve security personnel in the access rights management process by assigning reports to the appropriate security officers. ARM sends the reports in the desired frequency. The process is identical for all reports.

We recommend sending a selection of management reports to the role responsible for security. The reports are easy to read and only contain the necessary information.

## ARM Management Reports:

*Active Directory*

[Employees of a Manager](#)

[Display group memberships and user account details](#)

*File server*

[Who has access where?](#)

[Where do employees of a manager have access to?](#)

[Where do users and groups have access?](#)

*Exchange*

[Who has access to what?](#)

[Identifying mailbox permissions](#)

*SharePoint*

[Who has access where?](#)

[Where do users and groups have access?](#)

## Step-by-step process

### Who has access where? ✕

#### Report configuration

Title

Comment

Objects

Paths  Organizational categories

Organization (\srv-8man\Organization) ✕

◀ ∞ ▶ ∞ Levels to resolve under the selected resource

Translate names of groups to purpose group name

▼ Details

▼ Filter

▼ Group settings

▼ Options

---

^ Settings

The output format is [PDF](#) ✓

Report execution mode is started manually

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

#### Who has access where? ✕

Please select resource(s) ✕

Resources

- [-] File server
  - [-] srv-8man
    - [-] Organization
    - [-] Projects
    - [-] Templates
    - [-] Users
- [-] Exchange
- [-] SharePoint Online
- [-] SharePoint
- [-] Easy Connect - CSV
- [-] Easy Connect - SQL
- [-] Azure AD
- [-] OneDrive
- [-] SAP Connector

✕ Cancel
▶ Start


Select the desired report. Click on "started manually" in the "Settings" area.





Configuration ⊗


**1**


**Time schedule**


 **On demand**  
Do not schedule, the task will only be started on demand.

 **Daily**

 **Weekly**

 **Monthly**

 **Quarterly**

 **Yearly**

**Settings**


**Day**   **Hour**   **Minute**


**Time zone**  
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

**monthly, every 12. day of the month, 12:02 PM**  
*Corresponds to 11:02 AM UTC*

**2**

**Repeat mode**

 **Generate reports periodically**

 **Generate report only once**

**3**

1. Determine the frequency.
2. Activate the mode "Generate reports periodically".
3. Click on "Apply".

### Who has access where? ✕

#### Report configuration

Title

Comment

Objects

Paths  Organizational categories

Please click here to select resources

◀ ∞ ▶ ∞ Levels to resolve under the selected resource

Translate names of groups to purpose group name

▼ Details

▼ Filter

▼ Group settings

▼ Options

^ Settings

The output format is [PDF](#) ✓

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email to: Deactivated

#### Who has access where?

Access right report on resources with detailed permissions.

✕ Cancel
▶ Start

Click on "Deactivated".

### Configuration ✕

#### Email

Send email, when report is created 1

Add report as email attachment 2

Notification emails sent to: anthony.admin@8man-demo.local 3

Close
Apply 4

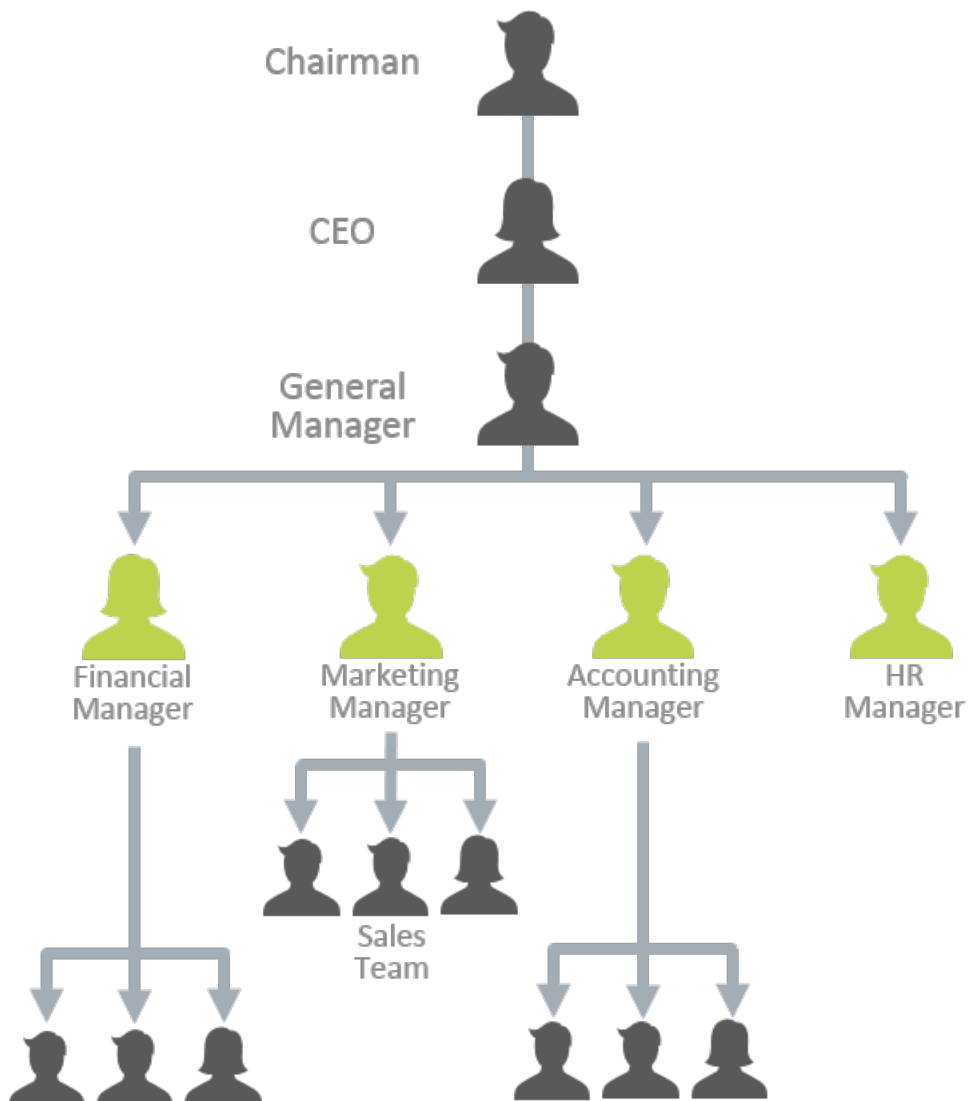
1. Activate emails.
2. Activate the option "Add report as email attachment".
3. Determine who should receive the email. You can enter more than one recipient.
4. Click on "Apply".

## Assign the administration of access rights to a Data Owner

### Background / Value

One of the most important processes in improving the security situation in your organization is the delegation of access rights to managers and team leads. As an Administrator you can, in close coordination with management, nominate Data Owners and assign resources. This has the distinct advantage that management decides who should have access to what information and is involved in the process of access rights assignment.

**Decentralize security expertise and transfer the responsibility for directory management to data owners.**



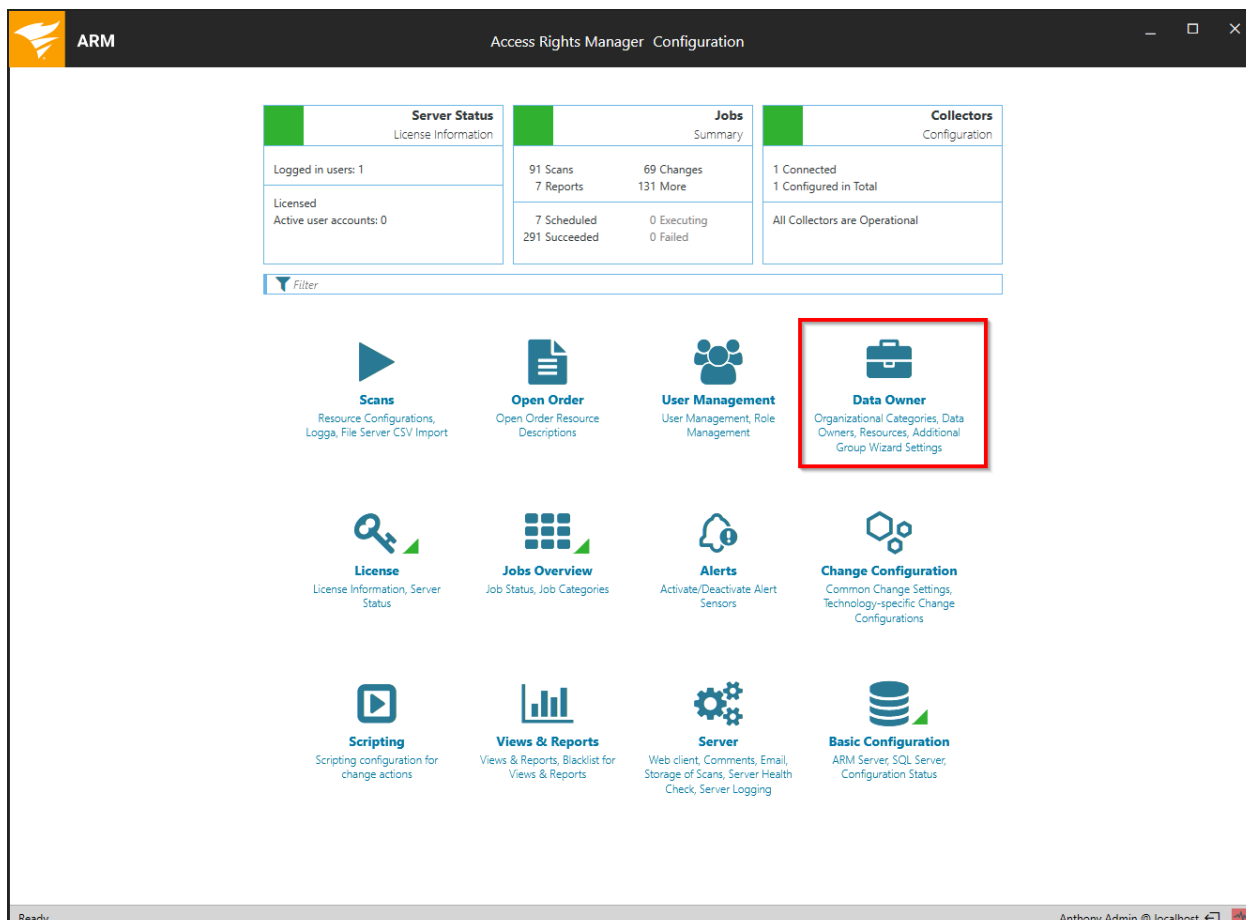
Define data owners and assign resources

## Background / Value

Data Owners and Managers have the responsibility to protect digital resources in their departments. ARM allows you to delegate this individual responsibility effectively. The following example shows a typical configuration.

These settings can be found in the ARM configuration application. You can find more detailed information in the chapters [Manage ARM users](#) and [Data Owner](#).

## Step-by-step process



The screenshot displays the ARM Configuration application interface. At the top, the title bar reads "ARM Access Rights Manager Configuration". The main content area is divided into three summary cards:

- Server Status** (License Information): Logged in users: 1, Licensed Active user accounts: 0.
- Jobs** (Summary): 91 Scans, 7 Reports, 69 Changes, 131 More, 7 Scheduled, 291 Succeeded, 0 Executing, 0 Failed.
- Collectors** (Configuration): 1 Connected, 1 Configured in Total, All Collectors are Operational.

Below the summary cards is a "Filter" button. The main dashboard features a grid of menu items, with "Data Owner" highlighted by a red box:

- Scans**: Resource Configurations, Logga, File Server CSV Import
- Open Order**: Open Order Resource Descriptions
- User Management**: User Management, Role Management
- Data Owner**: Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**: License Information, Server Status
- Jobs Overview**: Job Status, Job Categories
- Alerts**: Activate/Deactivate Alert Sensors
- Change Configuration**: Common Change Settings, Technology-specific Change Configurations
- Scripting**: Scripting configuration for change actions
- Views & Reports**: Views & Reports, Blacklist for Views & Reports
- Server**: Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**: ARM Server, SQL Server, Configuration Status

The system tray at the bottom shows "Ready" on the left and "Anthony Admin @ localhost" on the right.

Start the ARM configuration application and select "Data Owner".

The screenshot displays the 'Data Owner configuration' for the 'Marketing' category. The interface is divided into several sections:

- Organizational Categories:** A sidebar on the left with a 'Create' button (1) and a list of categories including 'Marketing' (2).
- Marketing Configuration:** The main workspace shows 'Data Owners' and 'Requesters' tables. A 'Data Owner' role is selected (5) with a dropdown menu showing options like 'Data Owner', 'Auditor', and 'No access'.
- User & Group selection:** A search field (3) and a list of users, with 'Caroline Berggren' (4) selected.
- Resources:** A table at the bottom showing file servers and templates.

1. Create an organizational category, for example "Marketing".
2. Select the newly created category.
3. Use the search field to find the desired account.
4. Use drag & drop to move the account to the column "Data Owner".
5. Select the desired role in the column "User role".

The screenshot displays the 'Data Owner configuration' for the 'Marketing' category. It includes sections for 'Data Owners', 'Requesters', 'Resources', 'User & Group selection', and 'Resource selection'. The 'Resources' section shows a table with columns for Name, Alias, and Access. The 'Resource selection' section shows a tree view of resources under 'Active Directory' and 'File server'. A red arrow points from the 'Marketing' resource in the tree to the 'Resources' table, which has four icons (2, 3, 4) above it. A red box highlights the 'Marketing' resource in the tree.

1. Use drag & drop to move resources out of the "Resource selection" into the "Resources" section. You are also able to search for resources.
2. Mark the resources as "requestable" in GrantMA.
3. Mark the resources as "visible".
4. Mark the resources as "changeable".

Enable data owners to manage permissions

## Background / Value

ARM allows you to delegate different roles and responsibilities relating to user management. We recommend starting with a simple definition of a Data Owner. This Data Owner is able to see and change access rights to file servers for their employees and areas of responsibility.

These settings can be found in the ARM configuration application. You can find detailed information in the chapter [Manage ARM users](#) and [Data Owner](#).

## Delegate user provisioning processes to help desk

User provisioning processes are easy to delegate. With ARM you can delegate all of these responsibilities to your help desk. We recommend starting with the delegation of simple account management. Depending on the qualifications of your employees it is possible to expand the responsibilities gradually.

### Processes that you can delegate to help desk with ARM

#### *Active Directory*

[Unlock user accounts](#)

[Reset passwords](#)

[Modify group and user attributes](#)

[Deactivate a user account](#)

[Delete a user account by using the "soft delete" feature](#)

[Remove a user and their permissions](#)

#### *Exchange*

[Create a mailbox \(email enable users\)](#)

[Manage mailbox and email size](#)

[Manage out of office notices](#)

[Change mailbox permissions](#)

Define your help desk and assign resources with ARM

### **Background / Value**

ARM relieves Administrators and allows the delegation of standard processes to your help desk. To do this, you must define help desk responsibilities and assign resources.

These settings can be found in the ARM configuration application. You can find detailed information in the chapter [Manage ARM users](#) and [Data Owner](#).

Assign responsibilities to help desk employees

### **Background / Value**

ARM allows you to define very specific responsibilities to individual help desk employees. The following example shows a typical assignment of responsibilities.

These settings can be found in the ARM configuration application. You can find more detailed information in the chapter [Managing ARM users](#).

## Step-by-step process

The screenshot shows the 'Users and Role Management' interface in the ARM configuration application. The interface is divided into two main sections: 'User Management' and 'List of accounts which can use ARM'. The 'User Management' section has a search bar with 'helen' entered and a 'Switch to Role Management' button. The 'List of accounts which can use ARM' section shows a table of accounts with roles. A red arrow points from the search results to the 'IT Helpdesk' role in the table. A 'Quick info' sidebar on the right provides additional context.

Name	Role
Antoine Admin (8man-demo\Ant...	Administrator
Sebastian SAP (8man-demo\Seb...	Administrator
Anthony Admin (8man-demo\An...	Administrator
Anton Admin (8man-demo\Anto...	Administrator
Administrator (8MAN-DEMO\Ad...	Administrator
David DO Finance (8man-demo\...	Data Owner
David DO Manager (8man-demo...	Data Owner
David DO Marketing (8man-dem...	Data Owner
David DO HR (8man-demo\Davi...	Data Owner
David DO Sales (8man-demo\Da...	Data Owner
Helena Helpdesk (8man-demo\H...	IT Helpdesk
Lucinda Baudinet (8man-demo\L...	Auditor
Emily Employee (8man-demo\Em...	Requester (employee)
Henry HR (8man-demo\Henry HR)	Requester (employee)

Start the ARM configuration module and select "User Management".

1. Set the view to "User Management".
2. Use the search to find the desired account.
3. Use drag & drop to add the account.
4. Assign the role "Help Desk" to the account.

**i** How to customize the "Help Desk" role is described in the chapter [Define ARM user roles](#).



# Create approval processes

Approvals in ARM can be used in two different ways:

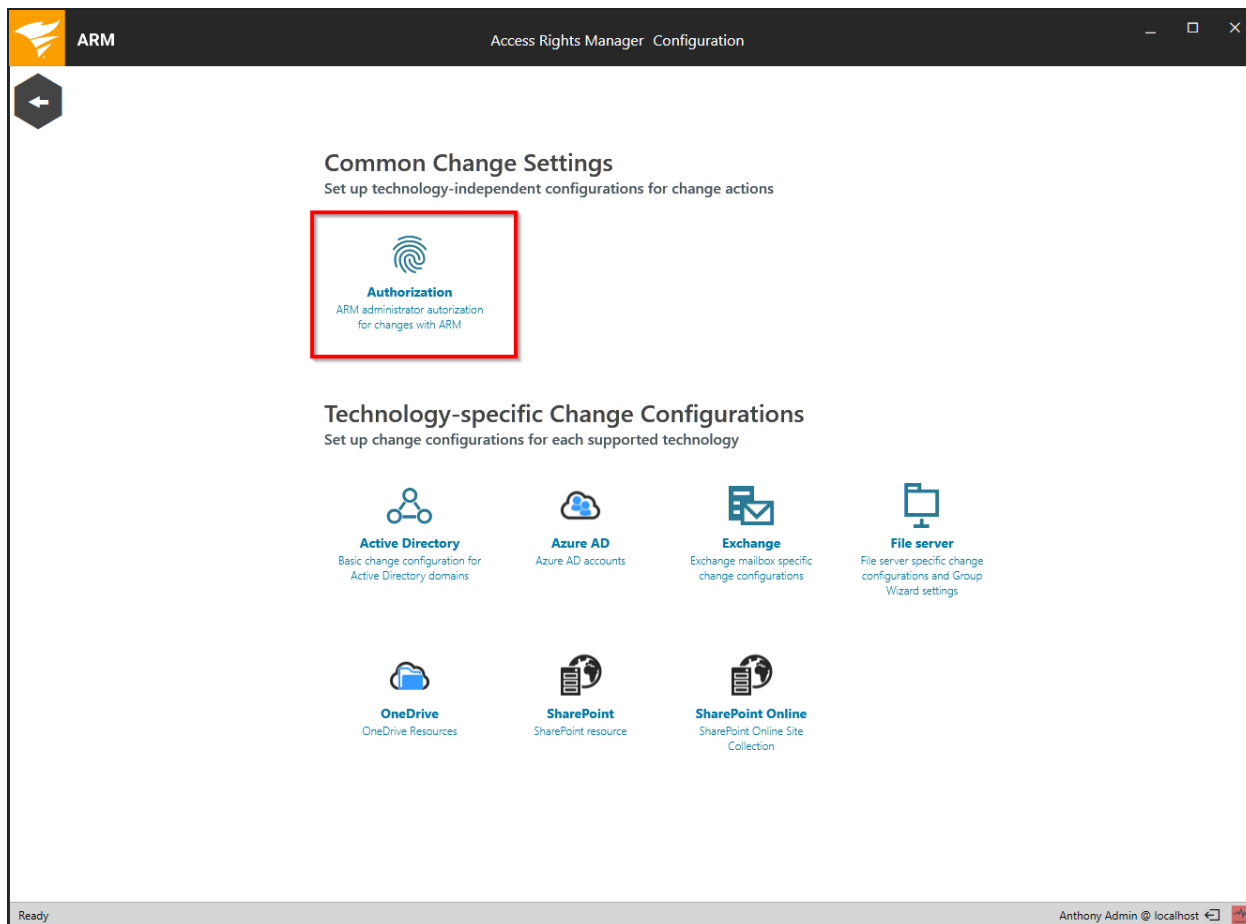
- Data owners manage permissions. Every change has to be approved by IT administrators.
- Use ARM GrantMA self service portal for employees and managers with individual approval flows and automatic execution.

## The simple authorization process - approving and rejecting actions as an administrator

### Background / Value

ARM allows you to fully empower your data owners and help desk, or to keep them on a tight leash. Initially, especially for help desk we recommend enabling the "request mode" to require approval of certain access rights changes. Once you have established processes you can gradually remove the requirement for approvals.

### Step-by-step process



In the ARM configuration application select "Change Configuration">"Authorization".

The screenshot shows the 'Authorization' configuration page in the ARM application. The page title is 'Authorization' and the breadcrumb is 'Access Rights Manager Configuration'. There are two configuration items:

- Deactivated:** Authorization is deactivated. Only Administrators or Data Owner are able to execute changes directly with ARM. It has an 'Approve/Reject' button.
- Activated:** Any changes performed by a Data Owner within ARM must be authorized by an ARM Administrator. It has a 'Request' button and an 'Approve/Reject' button. This option is highlighted with a red border.

The bottom of the window shows the status 'Ready' and the user 'Anthony Admin @ localhost'.

Activate the administrator approval mode.

ARM Access Rights Manager

Search

Anthony Admin

Start - Home

HOME NOTES **REQUESTS** TASKS REPORTS

Quick links  
Easy orientation, find the best tool for your productivity in ARM

**Permission Analysis**

- Where does a user/group have access?

**User Provisioning**

- Accounts**
  - Create new user or group
  - Edit group memberships
- Resources**
  - Edit access rights

**Security Monitoring**

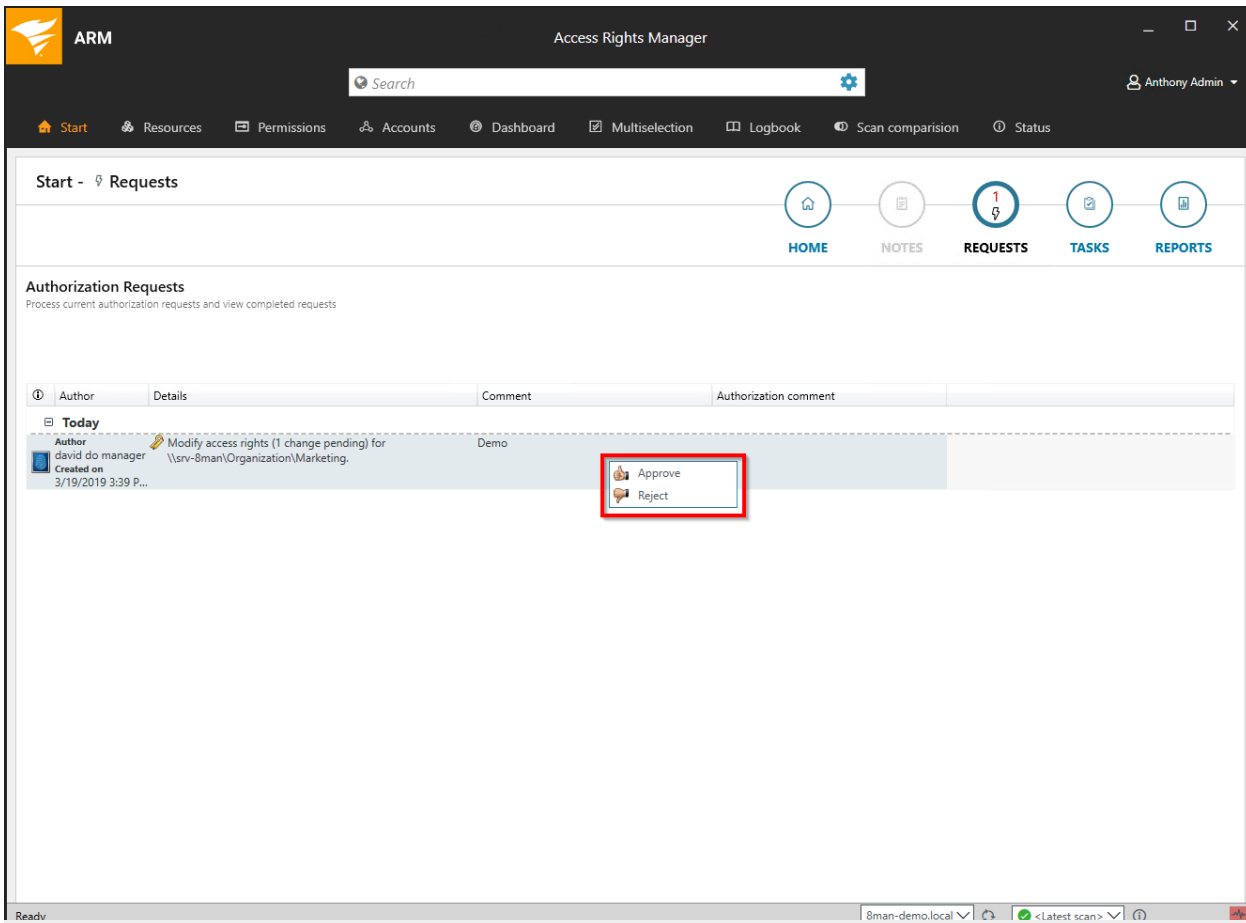
- Alerts**
  - Manage alerts
- File server**
  - Who did what, except authorized users (SoD)?
  - Who did what?
  - Who made changes?
- Active Directory**
  - AD Logga Report
- Exchange**
  - Exchange Logga Report
- OneDrive**
  - OneDrive Logga Report

**Documentation & Reporting**

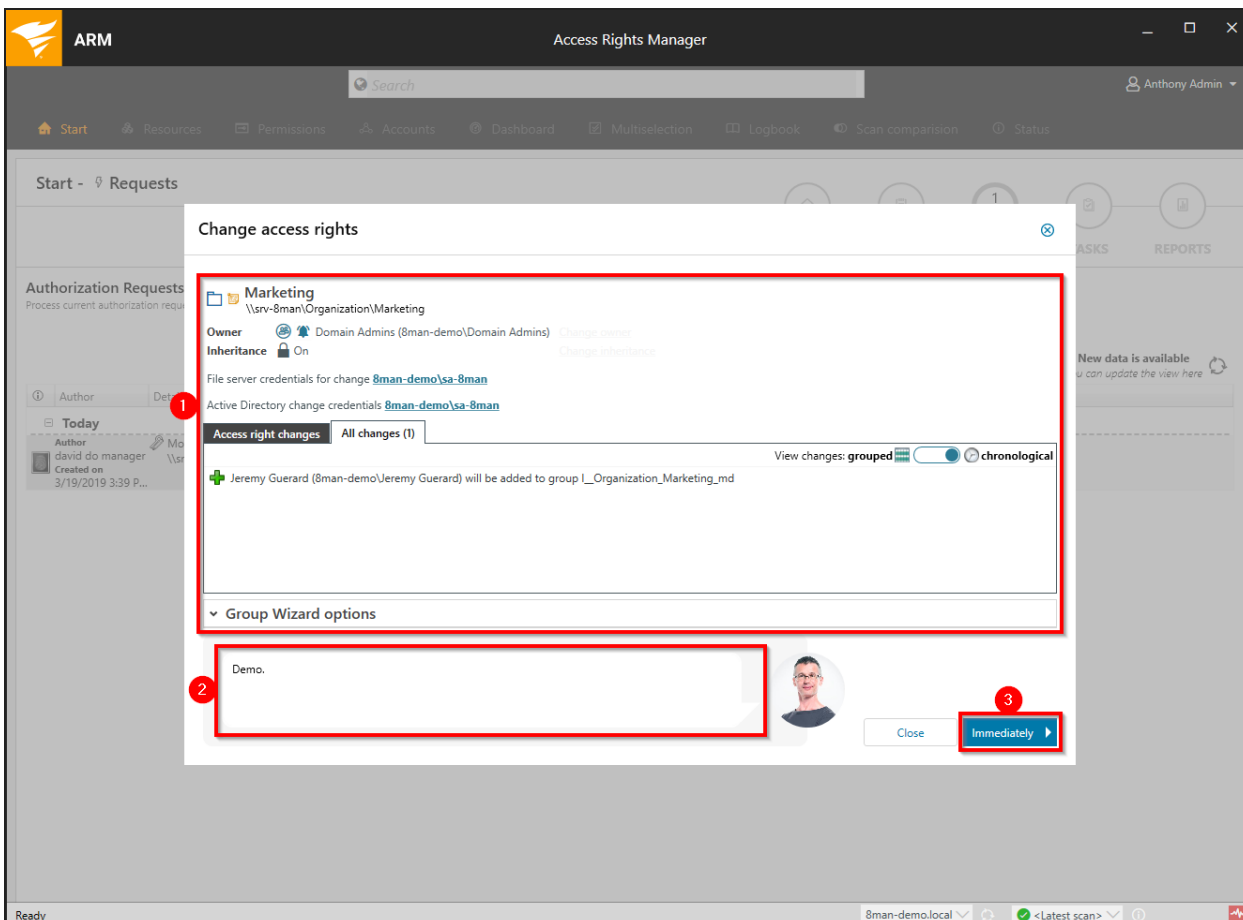
- Reports overview
- Where has the user/group access?
- Who has access where?
- File server**
  - All 'Authenticated users' permissions
  - All 'Everyone' permissions
  - All users with direct access
  - Directories without administrative owners
  - Permission difference
  - Unresolved SIDs
  - Where have employees of a manager access (file server)?
  - Who has access through which permission groups?
- Active Directory**
  - Account Details
  - Inactive accounts
  - Local accounts
  - Manager-Employees
  - OU Members and group memberships
  - Users and groups (Kerberos, Last logon)
- Exchange**
  - Exchange mailbox permissions

Ready | 8man-demo.local | <Latest scan>

Administrators are able to see open requests on the home page. Click on "Requests".



Right-click on a request and make your decision.



1. ARM shows you details about the requested changes
2. You must enter a comment.
3. Click "Apply".

## GrantMA: Design approval processes

### The problem

Administrators spend a lot of time on the assignment of access rights. In the classical process the decision (Manager) over access rights is separated from the technical implementation (Administrator).

The administrator does not know who should have which rights and becomes a mere exporter of orders.

### The Solution

It is much more efficient to combine the responsibility and technical implementation of access rights into one smooth process. This way only the actors necessary for the process to work are involved. ARM GrantMA uses a workflow that only involves an employee and their supervisor (Data Owner).

- The employee requests access rights to needed resources via a web portal.
- The data owner decides which requests are approved for his area of responsibility.

The GrantMA workflow has the following advantages:

- The Administrator is no longer part of the process and can focus on his core responsibilities.
- The Data Owner decides who can access which information since he is the one that knows which employees need access to which resources in order to do their job.
- All changes are saved in the ARM logbook.

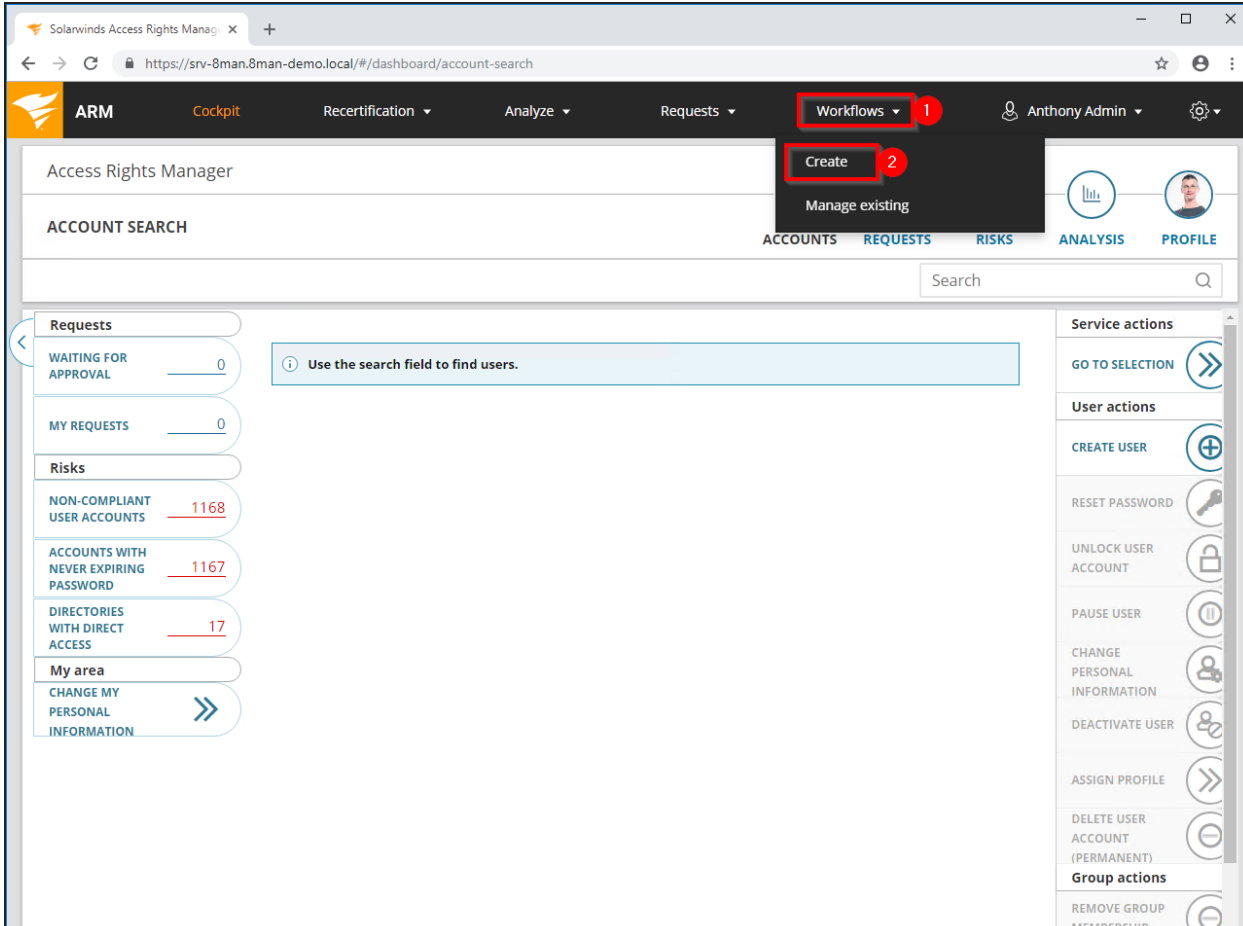
If more complex workflows with several decision-makers are required to grant access rights, you can also quickly map them.

Define individual approval flows

### **Background / Value**

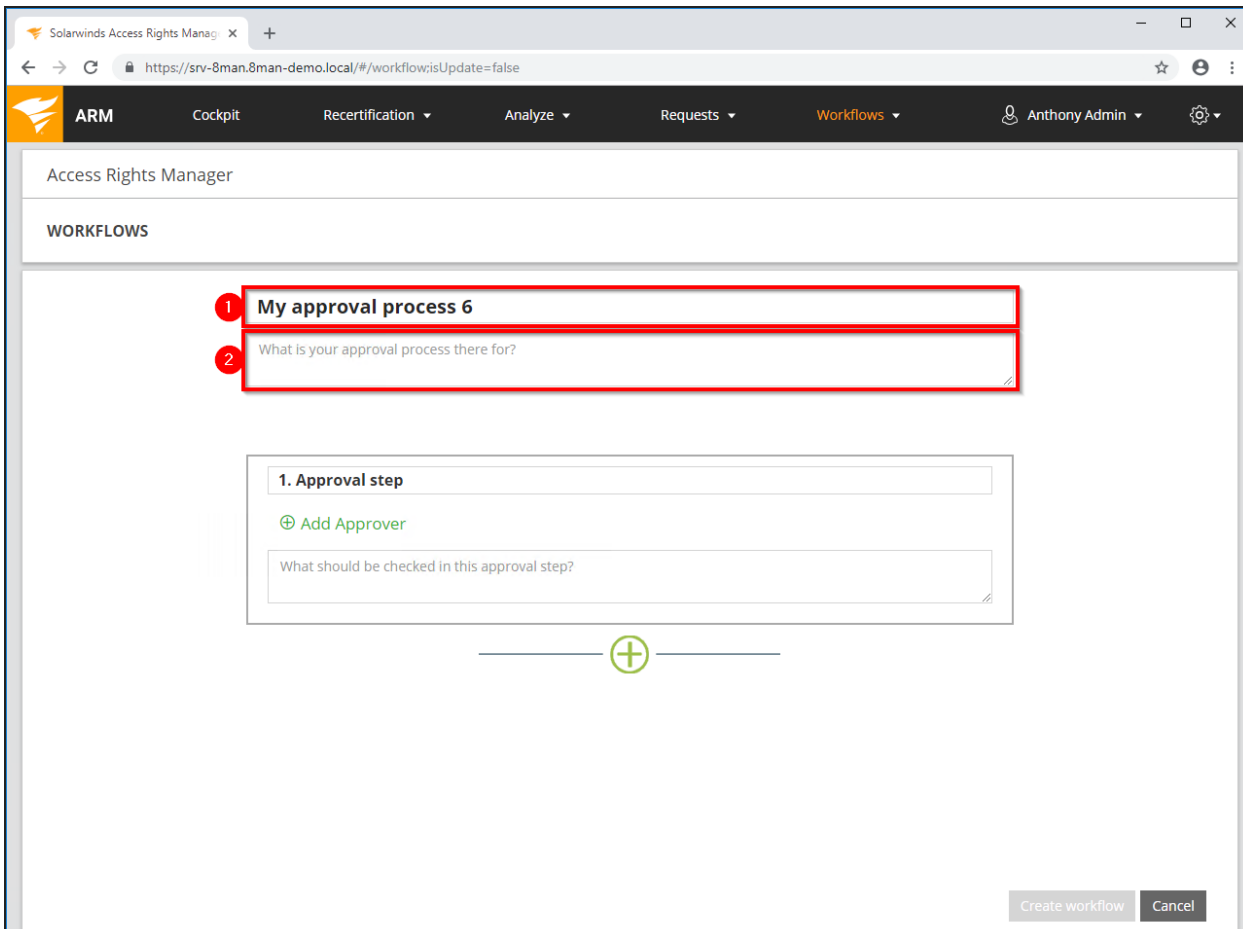
ARM GrantMA allows you to design individual approval workflows for each organizational category. You can design as many steps in the process as required. The last approver in the process is also the one making the formal change request.

## Step-by-step process



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'ARM', 'Cockpit', 'Recertification', 'Analyze', 'Requests', 'Workflows', and 'Anthony Admin'. The 'Workflows' menu is open, showing 'Create' and 'Manage existing' options. The 'Create' option is highlighted with a red box and a red circle containing the number '2'. A red circle containing the number '1' is positioned above the 'Workflows' menu. The main content area displays 'ACCOUNT SEARCH' with a search field and a message: 'Use the search field to find users.' The left sidebar shows 'Requests' (0) and 'Risks' (1168, 1167, 17). The right sidebar shows 'Service actions' and 'User actions'.

1. Select "Workflows".
2. Click on "Create".



Solarwinds Access Rights Manager

ARM Cockpit Recertification Analyze Requests Workflows Anthony Admin

Access Rights Manager

WORKFLOWS

1 My approval process 6

2 What is your approval process there for?

1. Approval step

+ Add Approver

What should be checked in this approval step?

+

Create workflow Cancel

1. Give the workflow a title.
2. Give a short, concise description of the workflow's purpose.



Solarwinds Access Rights Manager

WORKFLOWS

**My approval process 6**

What is your approval process there for?

1. Approval step

+ Add Approver

What should be checked in this approval step?

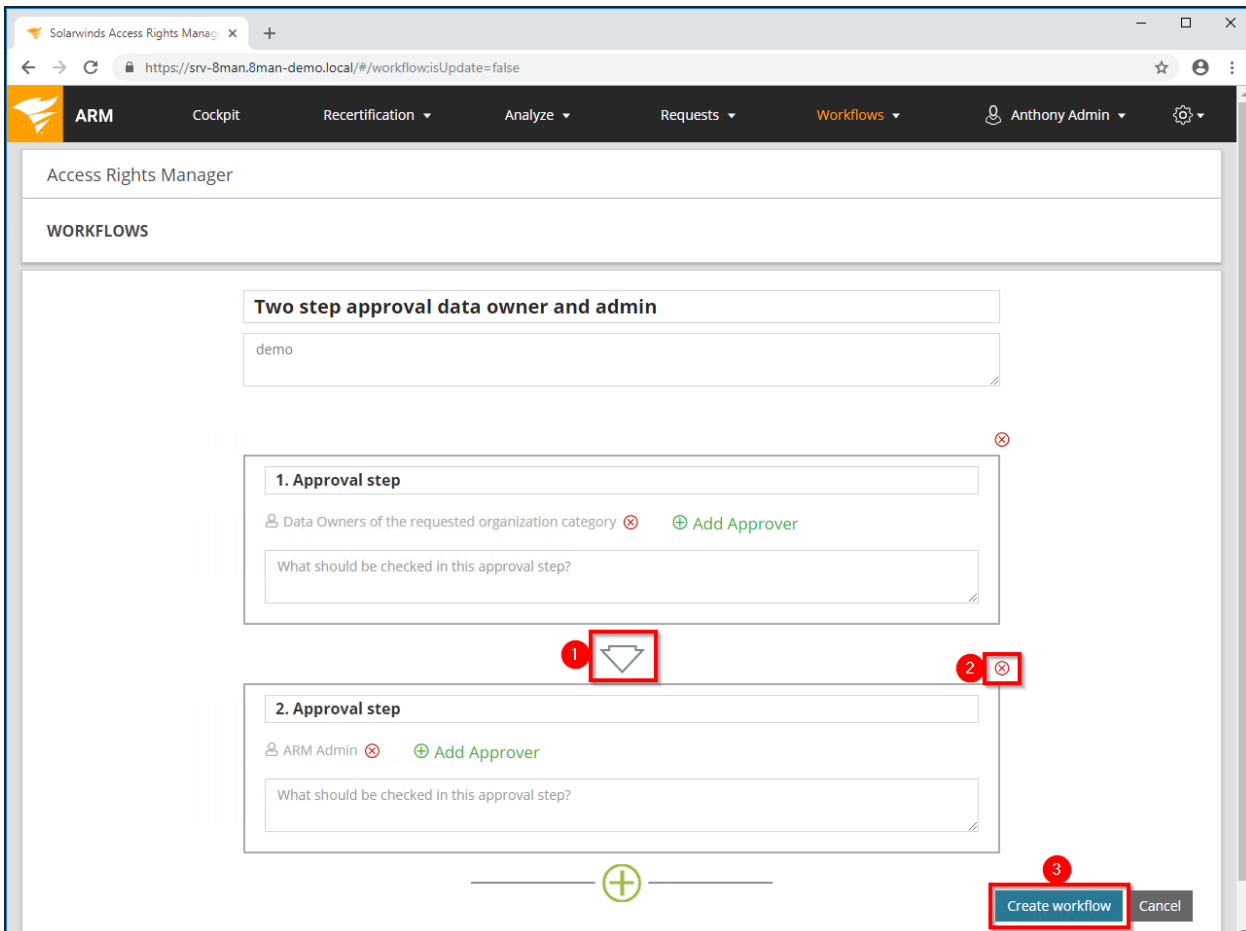
+

Create workflow Cancel

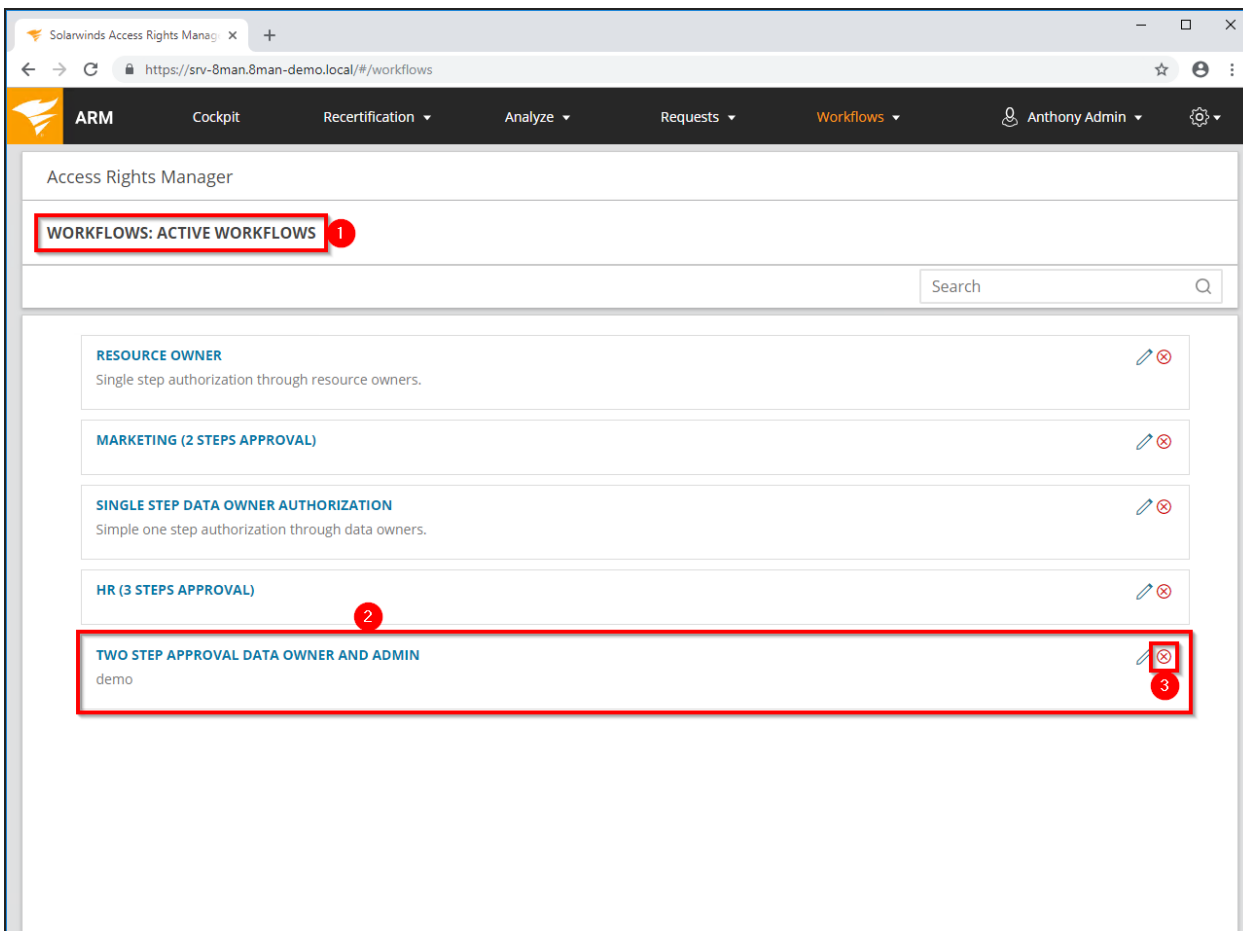
1. Name the approval step.
2. Add one or more approvers.

**i** You can also add multiple approvers for any step, which can be useful in case of vacation or illness.

3. Describe the approval step.
4. Add any additional steps in the approval process.



1. Add an additional step.
2. Delete an approval step.
3. Generate the workflow.



1. You have created a new workflow. ARM switches to the "Manage workflows" view.
2. Click on a workflow to make changes.
3. Delete the workflow.

Assign approval flows to resources

### Background / Value

Different resources need different approval flows. With the ARM data owner configuration you can connect available resources with individual approval flows.

### Step-by-step process

The screenshot shows the 'Data Owner configuration' page in the ARM application. The 'Europe' organizational category is selected in the sidebar (marked with a red box and '1'). The main area displays the configuration for this category, including a list of 'Data Owners' and 'Resources'. A workflow 'Single Step Data Owner Authorization' is assigned to the category (marked with a red box and '2'). The right-hand panel shows the 'User & Group selection' and 'Resource selection' options.

Start the ARM configuration application and select "Data Owner".

1. Select an organizational category.
2. Assign the desired workflow.

# Data Owner: Recertification of existing access rights

## Background / Value

Safety regulations demand for the implementation of the principle of least privilege. This is why data owners must check periodically the access rights situation of their resources.

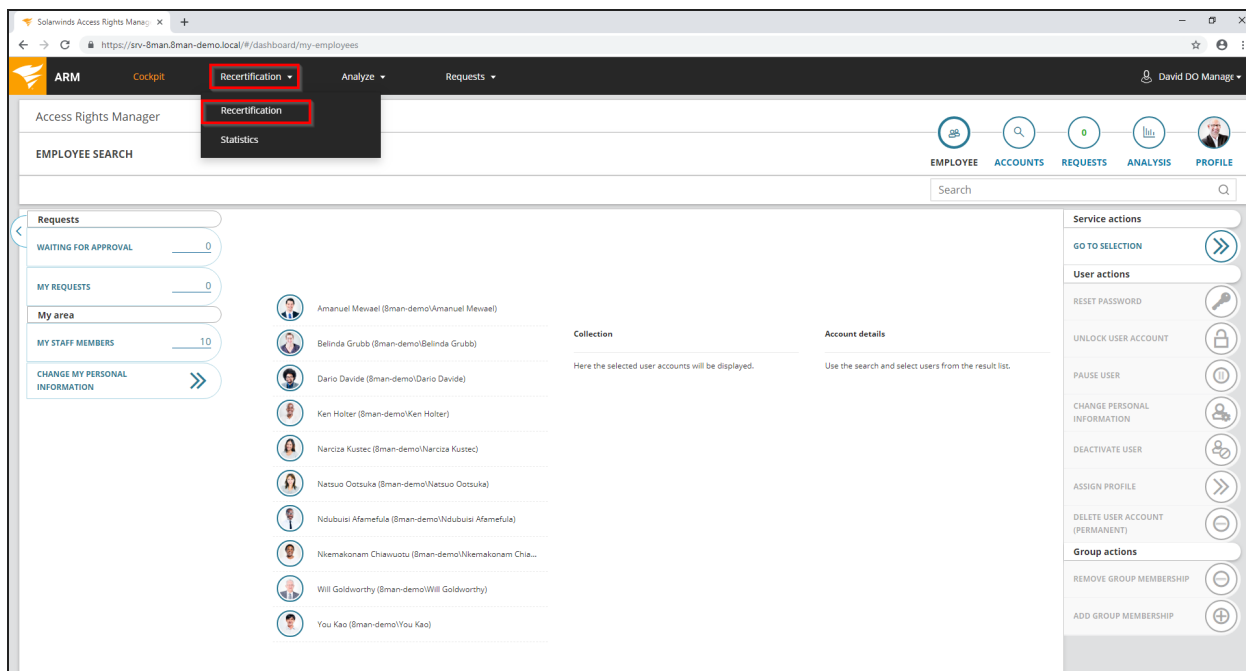
With the re-certification process you obtain the possibility to check and change the access rights situation to your resources.

You receive an email with the instructions to the re-certification process. Then you decide for each user and resource if the access right should stay or be removed. Your desired changes will be transferred automatically to the administrator.

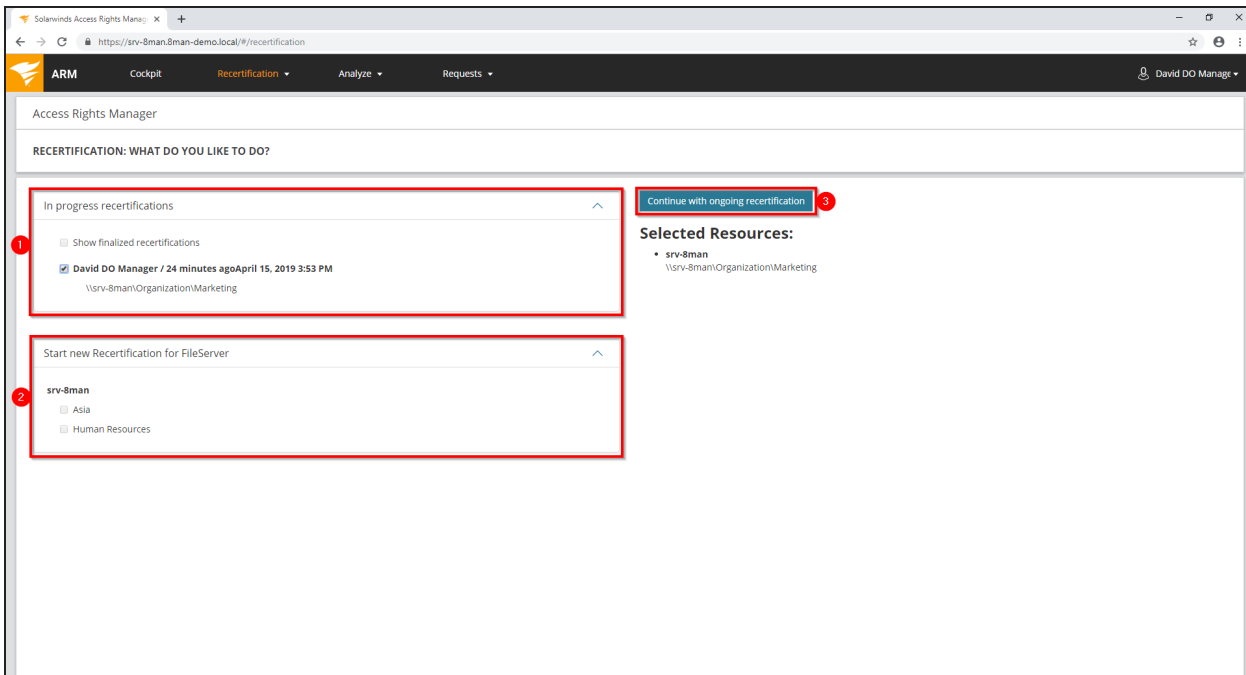
## Complementary Services

[Grant and remove file server access rights](#)

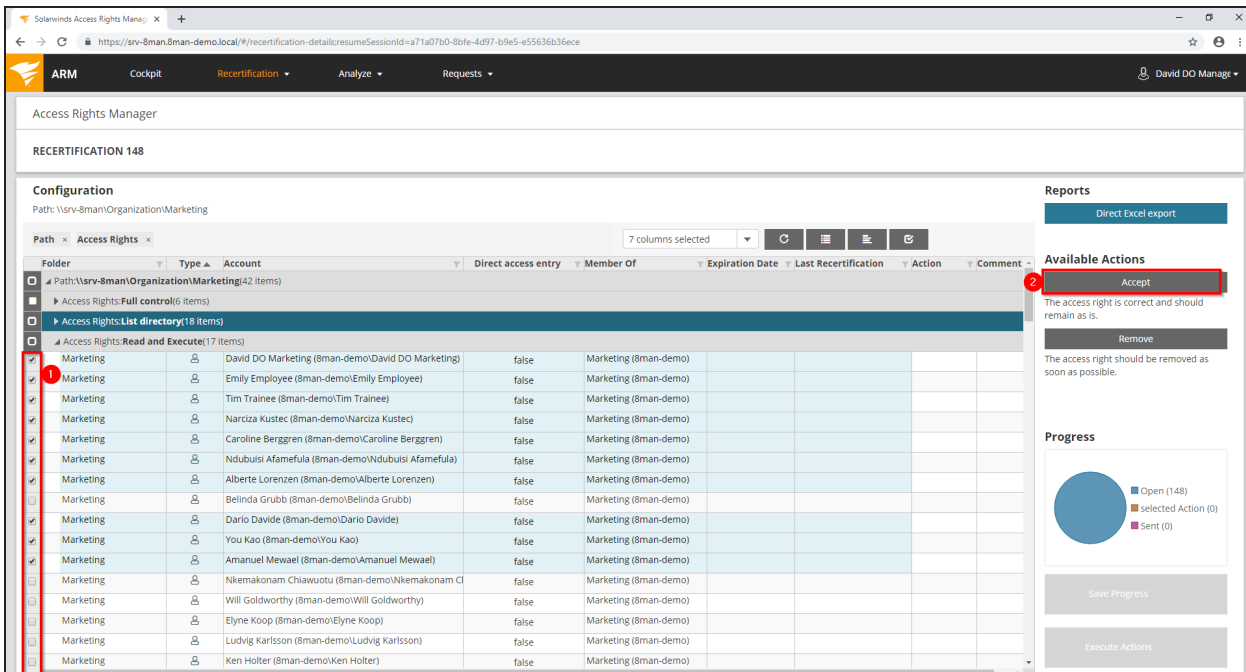
## Step-by-step process



Click "Recertification".




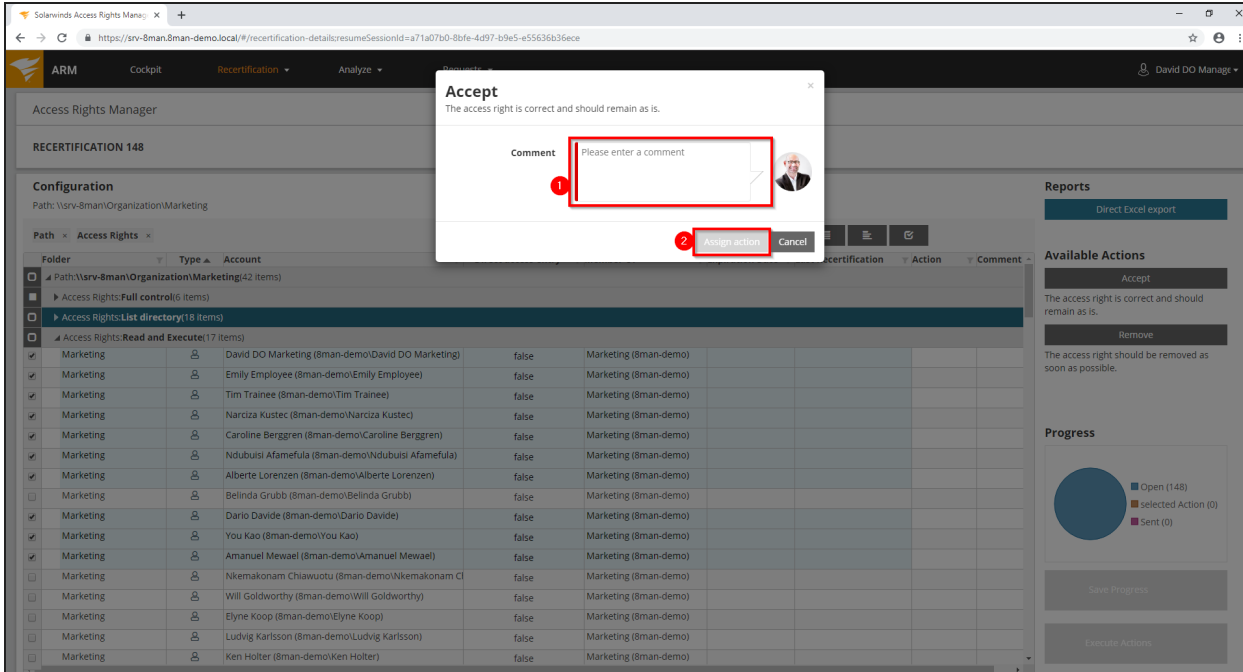
1. Continue a recertification already started.
2. Select resources for a new recertification.
3. Start the process.



You can either accept or remove the permissions.

1. Activate all Users which should keep their permissions first.
2. Click on "Accept".

 Subdirectories are only displayed, if they contain deviating permissions.



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. A modal dialog box titled "Accept" is open, displaying the message "The access right is correct and should remain as is." Below the message is a "Comment" field with a red box around it and a red "1" next to it, indicating where to enter a comment. To the right of the comment field is a user profile picture. Below the comment field is a red "2" next to the "Assign action" button, indicating where to click. The background shows a table of access rights for "RECERTIFICATION 148" under the path "Path: \\srv-8man\Organization\Marketing". The table has columns for Folder, Type, Account, and Action. The "Action" column contains "Marketing (8man-demo)".

Folder	Type	Account	Action	Comment
Path: \\srv-8man\Organization\Marketing (42 items)				
Access Rights: Full control (6 items)				
Access Rights: List directory (18 items)				
Access Rights: Read and Execute (17 items)				
Marketing		David DO Marketing (8man-demo\David DO Marketing)	Marketing (8man-demo)	
Marketing		Emily Employee (8man-demo\Emily Employee)	Marketing (8man-demo)	
Marketing		Tim Trainee (8man-demo\Tim Trainee)	Marketing (8man-demo)	
Marketing		Narciza Kustec (8man-demo\Narciza Kustec)	Marketing (8man-demo)	
Marketing		Caroline Berggren (8man-demo\Caroline Berggren)	Marketing (8man-demo)	
Marketing		Ndubusi Afamefula (8man-demo\Ndubusi Afamefula)	Marketing (8man-demo)	
Marketing		Alberte Lorenzen (8man-demo\Alberte Lorenzen)	Marketing (8man-demo)	
Marketing		Belinda Grubb (8man-demo\Belinda Grubb)	Marketing (8man-demo)	
Marketing		Dario Davide (8man-demo\Dario Davide)	Marketing (8man-demo)	
Marketing		You Kao (8man-demo\You Kao)	Marketing (8man-demo)	
Marketing		Amanuel Mewael (8man-demo\Amanuel Mewael)	Marketing (8man-demo)	
Marketing		Nkemakonam Chiawuotu (8man-demo\Nkemakonam C)	Marketing (8man-demo)	
Marketing		Will Goldworthy (8man-demo\Will Goldworthy)	Marketing (8man-demo)	
Marketing		Elyne Koop (8man-demo\Elyne Koop)	Marketing (8man-demo)	
Marketing		Ludvig Karlsson (8man-demo\Ludvig Karlsson)	Marketing (8man-demo)	
Marketing		Ken Holter (8man-demo\Ken Holter)	Marketing (8man-demo)	

1. You must enter a comment. Your notes will be saved in the system for documentation.
2. Click "Assign action".

Repeat the process for the permissions you want to remove.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface during a recertification process. The main table shows a list of access rights for various users, with the 'Action' column highlighted in red. The 'Progress' widget on the right shows a pie chart with 132 Open items, 16 Selected Actions, and 0 Sent items. The 'Available Actions' panel shows 'Accept' and 'Remove' options. The 'Save Progress' and 'Execute Actions' buttons are also highlighted in red.

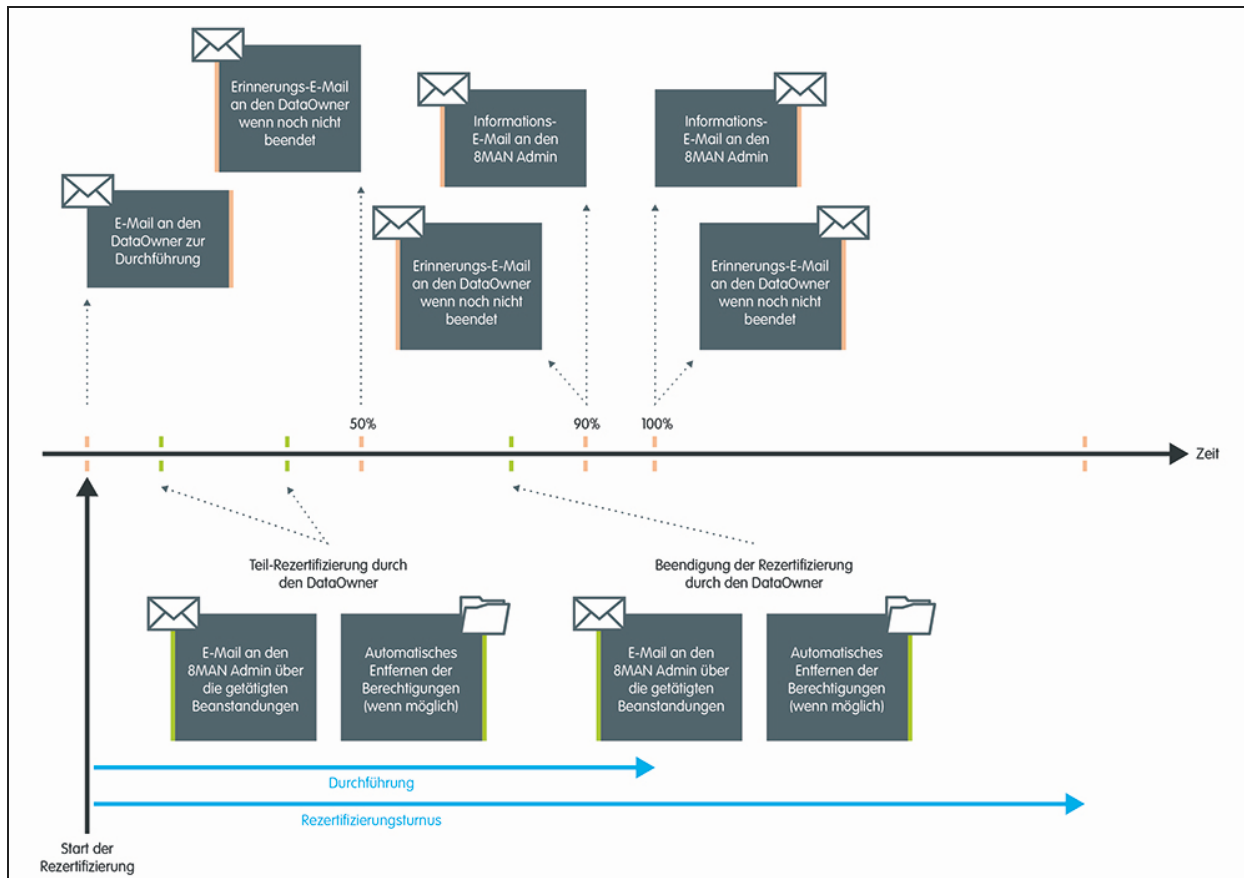
Folder	Type	Account	Direct access entry	Member Of	Expiration Date	Last Recertification	Action	Comment
Marketing	Account	David DO Marketing (8man-demo\David DO Marketing)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	Emily Employee (8man-demo\Emily Employee)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	Tim Trainee (8man-demo\Tim Trainee)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	Narciza Kustec (8man-demo\Narciza Kustec)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	Caroline Berggren (8man-demo\Caroline Berggren)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	Ndubuisi Afamefula (8man-demo\Ndubuisi Afamefula)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	Alberte Lorenzen (8man-demo\Alberte Lorenzen)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	Belinda Grubb (8man-demo\Belinda Grubb)	false	Marketing (8man-demo)			Remove	demo
Marketing	Account	Dario Davide (8man-demo\Dario Davide)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	You Kao (8man-demo\You Kao)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	Amanuel Mewael (8man-demo\Amanuel Mewael)	false	Marketing (8man-demo)			Accept	demo
Marketing	Account	Nkemakonam Chiawuotu (8man-demo\Nkemakonam Chiawuotu)	false	Marketing (8man-demo)			Remove	demo
Marketing	Account	Will Goldworthy (8man-demo\Will Goldworthy)	false	Marketing (8man-demo)				
Marketing	Account	Elyne Koop (8man-demo\Elyne Koop)	false	Marketing (8man-demo)				
Marketing	Account	Ludvig Karlsson (8man-demo\Ludvig Karlsson)	false	Marketing (8man-demo)				
Marketing	Account	Ken Holter (8man-demo\Ken Holter)	false	Marketing (8man-demo)				

1. Your decision is marked in the column "action".
2. ARM displays your current progress.
3. Click "Save Progress" to continue your review later. You will be able to modify your decisions.
4. Click "Execute Actions" to finalize your decisions. The Administrator gets a list of your decisions for implementation.

**⚠️** If you click on "Execute Actions" your administrator receives almost every time an email with your desired changes. This is why we recommend to do the recertification in one go.



## Email notifications for recertification



ARM sends automatic reminders during the recertification period.

**i** If the recertification is not completed within the deadline, ARM stops the process and the data owner and the administrator receive an email about the missing execution.

**i** [Notification emails can be customized](#) by an administrator.

## ARM GrantMA: workflows for employees

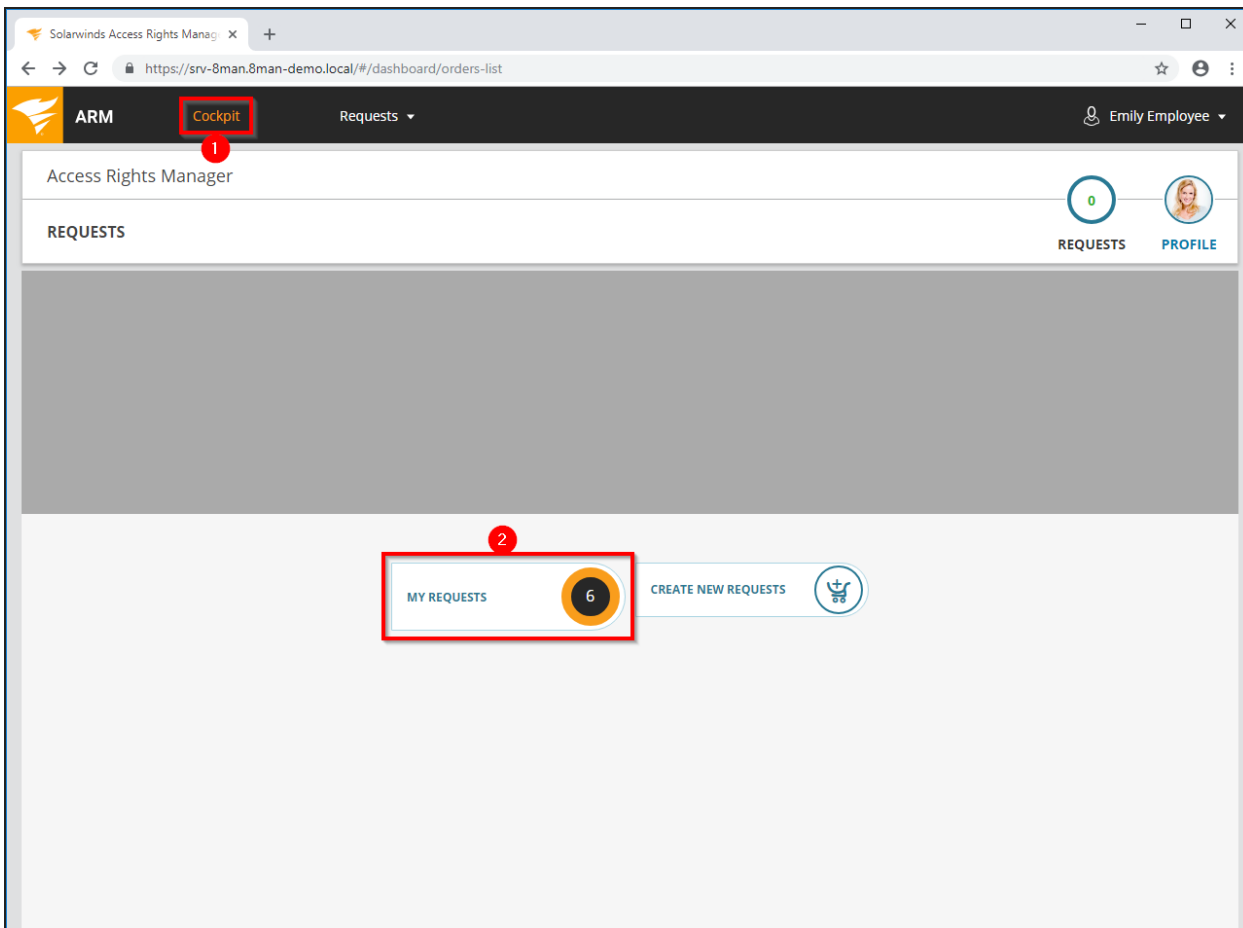
By using the ARM GrantMA self-service portal, employees are able to request access to individual resources in your organization. The next few pages contain examples of some common workflows.

### Manage my requests (cockpit)

#### Background / Value

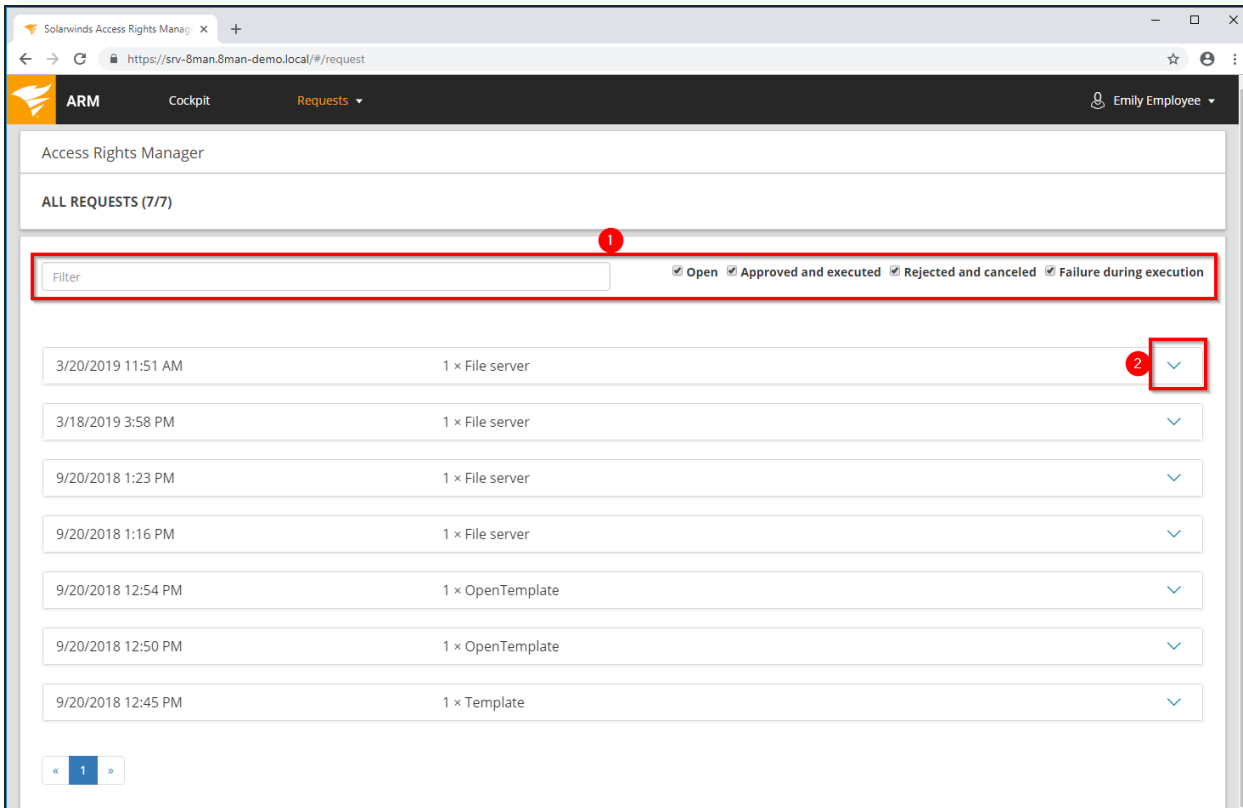
Keep track of your orders. Cancel orders or resend notifications to the approver.

#### Step-by-step process



1. Select Cockpit.
2. Click "My Requests".

**i** The range of available services (buttons) varies according to role (login), risk assessment and configuration.



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes the ARM logo, 'Cockpit', and 'Requests'. The user is logged in as 'Emily Employee'. The main content area is titled 'Access Rights Manager' and 'ALL REQUESTS (7/7)'. A red box labeled '1' highlights the filter and status options: a 'Filter' input field and checkboxes for 'Open', 'Approved and executed', 'Rejected and canceled', and 'Failure during execution'. Below this is a table of requests with columns for date/time, description, and an expand button. A red box labeled '2' highlights the expand button for the first request. The table contains the following data:

Date/Time	Description	Action
3/20/2019 11:51 AM	1 × File server	Expand
3/18/2019 3:58 PM	1 × File server	Expand
9/20/2018 1:23 PM	1 × File server	Expand
9/20/2018 1:16 PM	1 × File server	Expand
9/20/2018 12:54 PM	1 × OpenTemplate	Expand
9/20/2018 12:50 PM	1 × OpenTemplate	Expand
9/20/2018 12:45 PM	1 × Template	Expand

At the bottom left, there is a pagination control showing '1'.

1. Filter your requests to quickly find the right one in case of many entries.
2. Expand the desired request.

Solarwinds Access Rights Manager

ARM Cockpit Requests Emily Employee

Access Rights Manager

ALL REQUESTS (7/7)

Filter  Open  Approved and executed  Rejected and canceled  Failure during execution

State	Resource	Type	Next approver
Open	Finance \\srv-8man\Organization\Finance	File server	8MAN Demo Company

1. ARM shows you details about the request.
2. See more details about the request.
3. Resend a notification email to the approver.
4. Cancel your request.

## Request file server access rights

### Background / Value

Employees can request access rights to file server directories from Data Owners by using the GrantMA self-service portal.

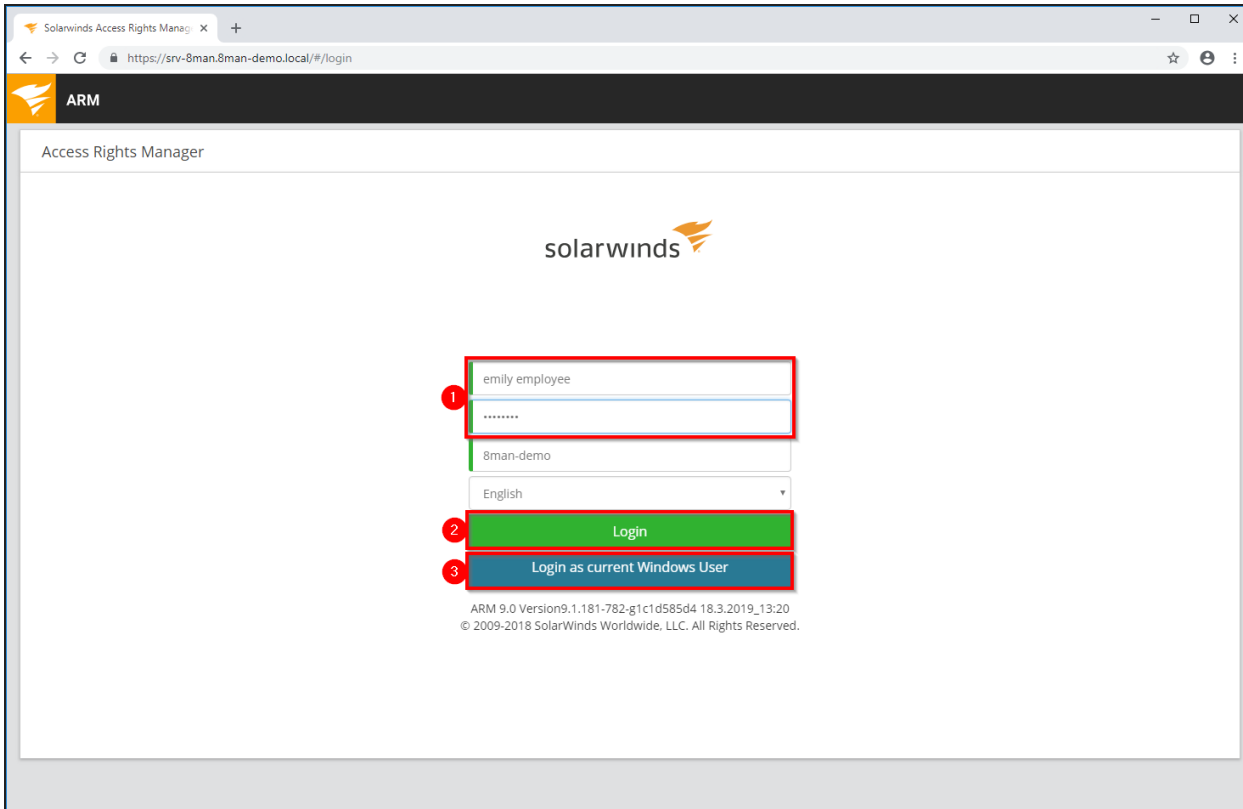
You can configure a variety of different processes and involve the relevant decision makers, depending on your security requirements.

### Related features

[Manage my requests](#)

[GrantMA: Design approval processes](#) (administrator)

## Step-by-step process

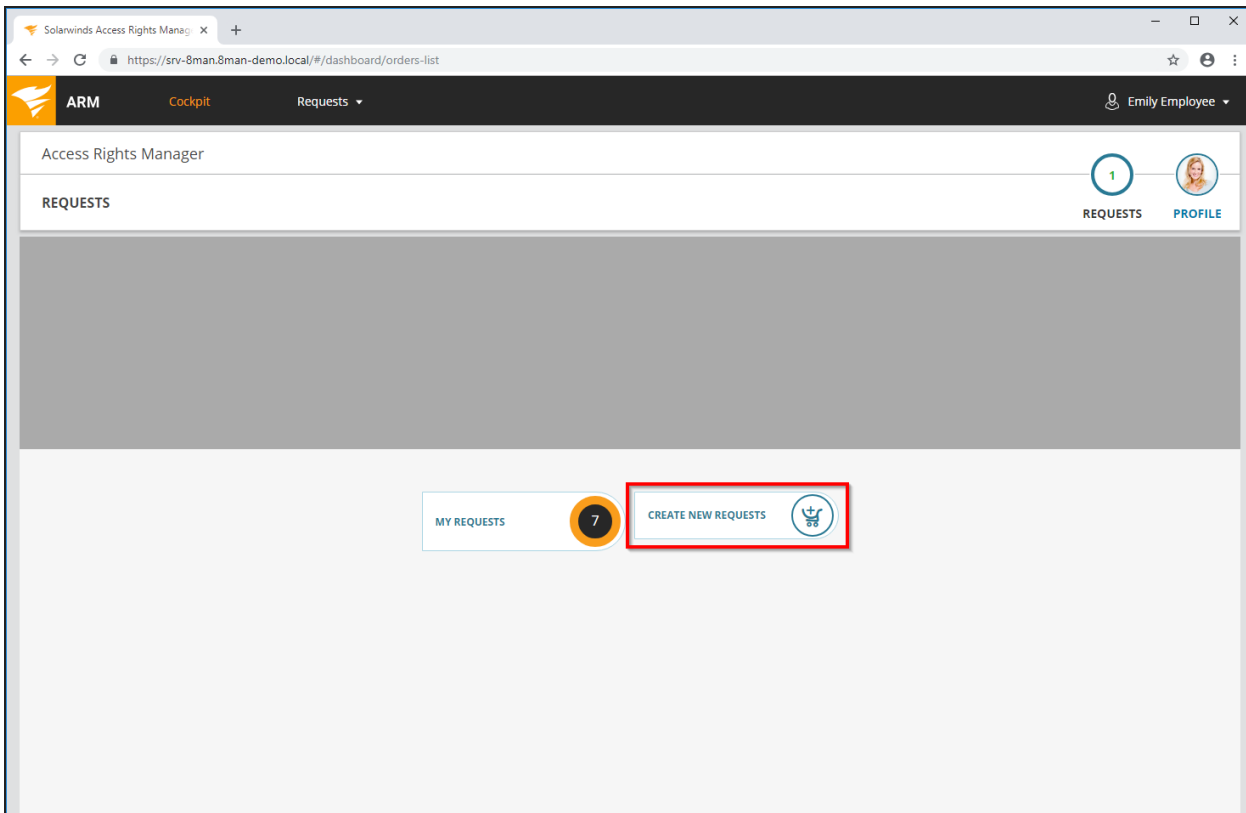


The screenshot shows the Solarwinds Access Rights Manager (ARM) login page. The page title is "Access Rights Manager" and the Solarwinds logo is displayed. The login form consists of the following elements:

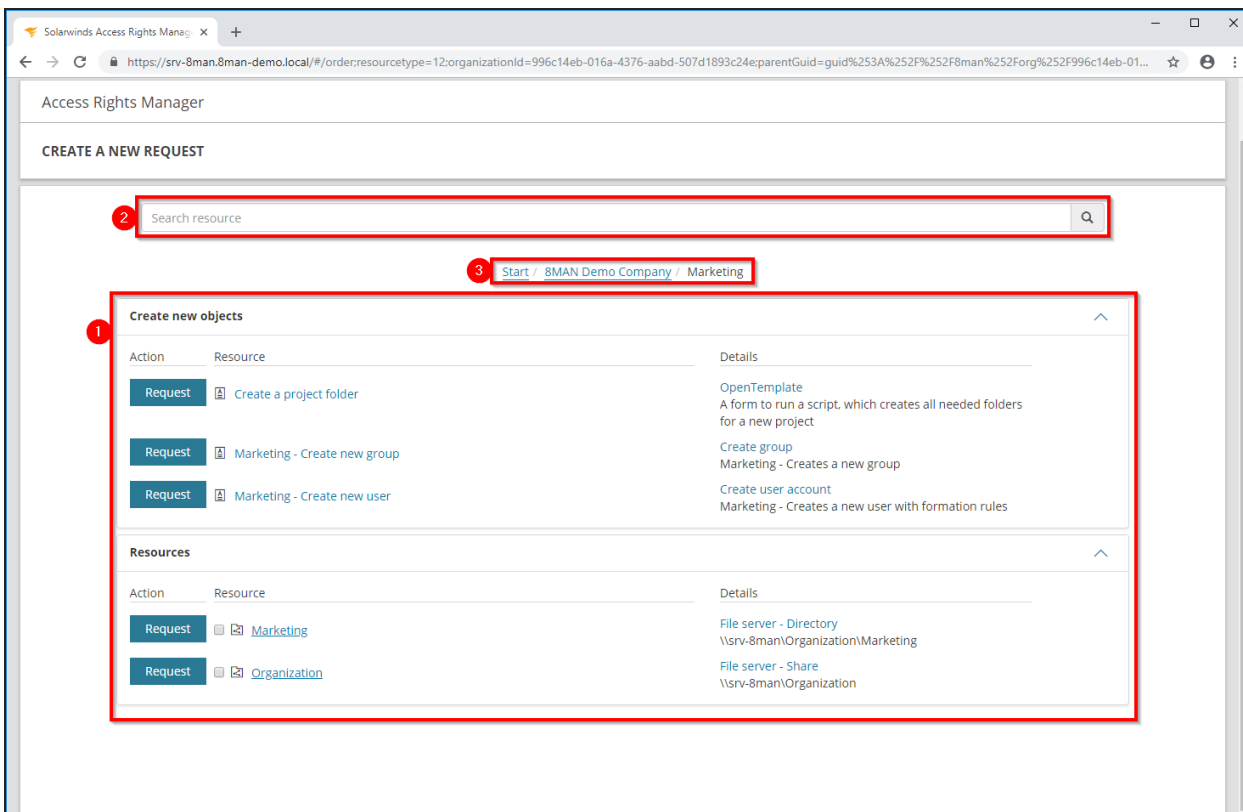
- Step 1:** A text input field containing "emily employee" and a password field with masked characters "\*\*\*\*\*".
- Step 2:** A green button labeled "Login".
- Step 3:** A blue button labeled "Login as current Windows User".

Below the buttons, the version information is displayed: "ARM 9.0 Version 9.1.181-782-g1c1d585d4 18.3.2019\_13:20 © 2009-2018 SolarWinds Worldwide, LLC. All Rights Reserved."

1. Enter your user name and password.
2. Click "Login".
3. You can alternatively login as the current windows user (no user name and password required).



Click "Create new request".



Access Rights Manager

CREATE A NEW REQUEST

2 Search resource

3 Start / 8MAN Demo Company / Marketing

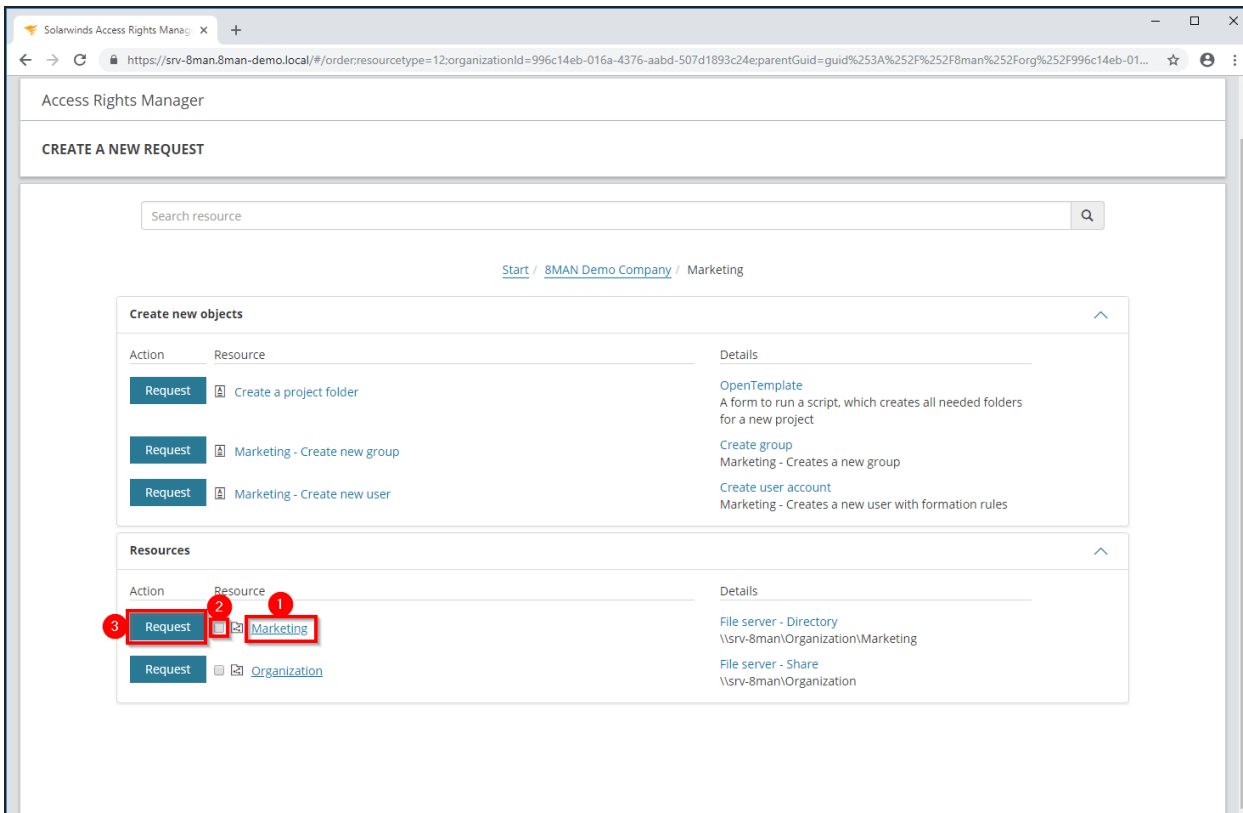
1 Create new objects

Action	Resource	Details
Request	Create a project folder	OpenTemplate A form to run a script, which creates all needed folders for a new project
Request	Marketing - Create new group	Create group Marketing - Creates a new group
Request	Marketing - Create new user	Create user account Marketing - Creates a new user with formation rules

Resources

Action	Resource	Details
Request	Marketing	File server - Directory \\srv-8man\Organization\Marketing
Request	Organization	File server - Share \\srv-8man\Organization

1. ARM shows you as the applicant only the resources that can be ordered.
2. Use the search to find the desired resource quickly.
3. Navigate through available resources.



Access Rights Manager

CREATE A NEW REQUEST

Search resource

Start / [8MAN Demo Company](#) / Marketing

**Create new objects**

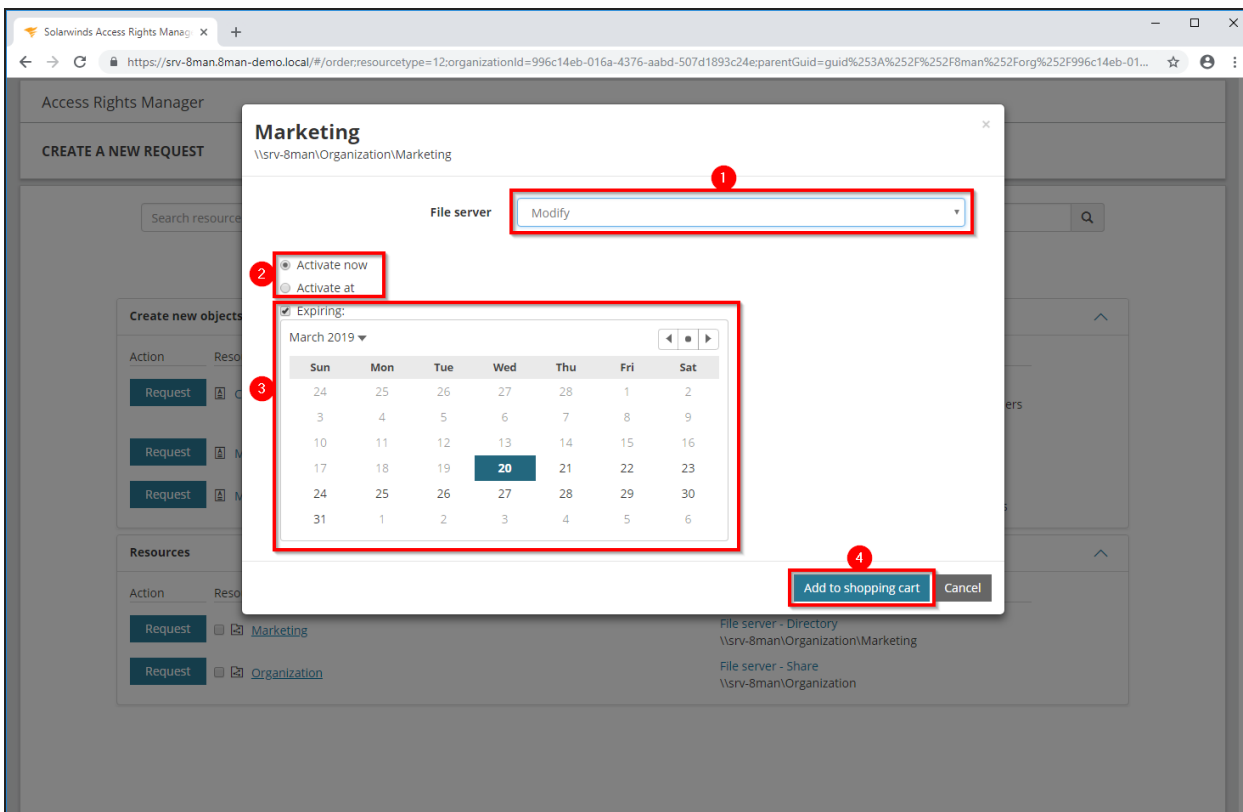
Action	Resource	Details
<a href="#">Request</a>	Create a project folder	<a href="#">OpenTemplate</a> A form to run a script, which creates all needed folders for a new project
<a href="#">Request</a>	Marketing - Create new group	<a href="#">Create group</a> Marketing - Creates a new group
<a href="#">Request</a>	Marketing - Create new user	<a href="#">Create user account</a> Marketing - Creates a new user with formation rules

**Resources**

Action	Resource	Details
<a href="#">Request</a>	<input checked="" type="checkbox"/> <a href="#">Marketing</a>	<a href="#">File server - Directory</a> \\srv-8man\Organization\Marketing
<a href="#">Request</a>	<input type="checkbox"/> <a href="#">Organization</a>	<a href="#">File server - Share</a> \\srv-8man\Organization

1. Click on a link to drill down further.
2. Check the box if you want to request access to more than one folder.
3. Click "Request".

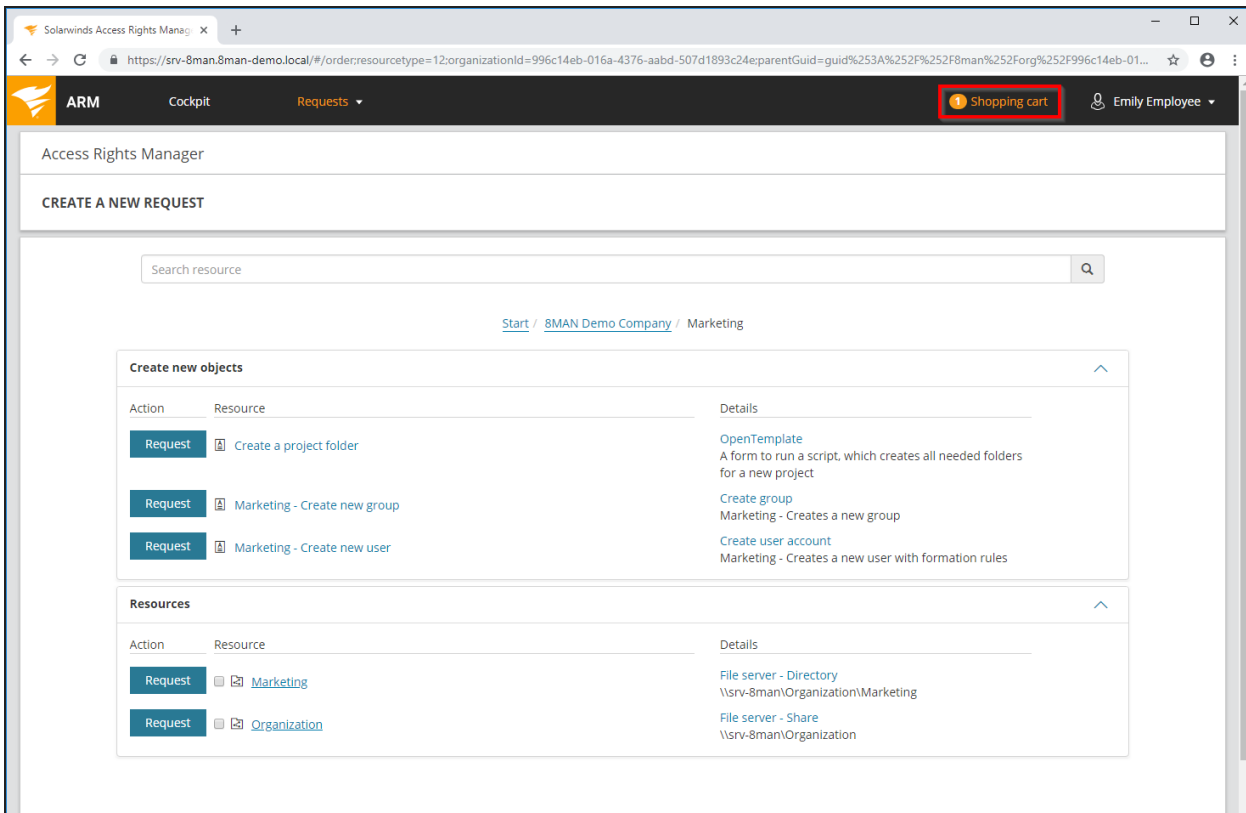




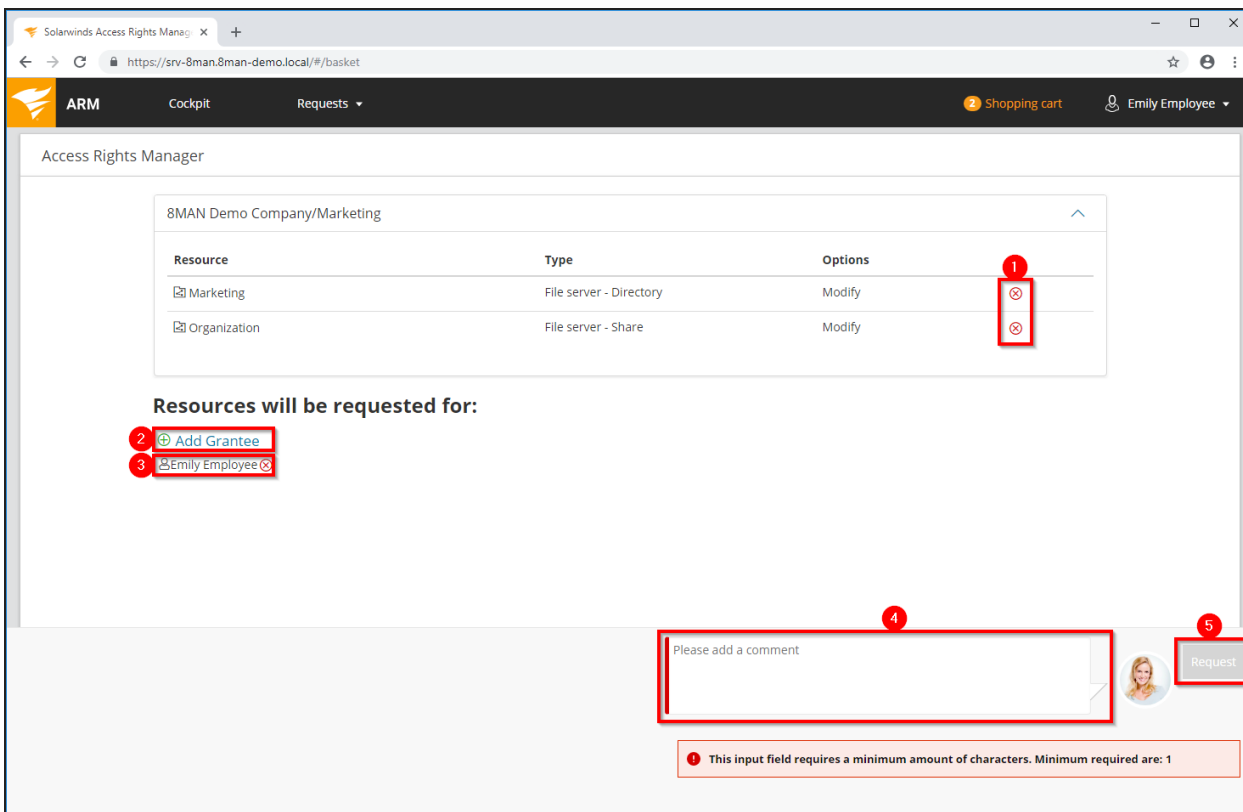
1. Select the desired kind of access.
2. Set an activation date.
3. Optional: Set an expiration date.

**i** Depending on your ARM configuration the approver may be able to modify the request.

4. Click "Add to shopping cart".



Click "Shopping cart".



The screenshot shows the Solarwinds Access Rights Manager (ARM) interface. At the top, there is a navigation bar with 'ARM', 'Cockpit', and 'Requests'. A shopping cart icon and the user 'Emily Employee' are also visible. The main content area is titled 'Access Rights Manager' and displays a table for '8MAN Demo Company/Marketing'. The table has three columns: 'Resource', 'Type', and 'Options'. Two rows are shown: 'Marketing' (File server - Directory) and 'Organization' (File server - Share), both with 'Modify' options. Red circles with numbers 1, 2, and 3 highlight the delete icons in the 'Options' column, the 'Add Grantee' button, and the 'Emily Employee' button respectively. Below the table, a section titled 'Resources will be requested for:' contains the 'Add Grantee' and 'Emily Employee' buttons. At the bottom, a text input field with the placeholder 'Please add a comment' is highlighted with a red circle 4, and a 'Request' button is highlighted with a red circle 5. A red error message at the bottom states: 'This input field requires a minimum amount of characters. Minimum required are: 1'.

Resource	Type	Options
Marketing	File server - Directory	Modify
Organization	File server - Share	Modify

Resources will be requested for:

- Add Grantee
- Emily Employee

Please add a comment

Request

This input field requires a minimum amount of characters. Minimum required are: 1

1. You can delete order items.
2. Add a recipient to your order. You are able to request access for other users.
3. Remove the recipient. You can also remove yourself and only request access for other users.
4. You must enter a comment. Give a good reason so that the approver can make a wise decision.
5. Start the request.

## Request group memberships

### Background / Value

Employees can request group memberships by using the GrantMA self-service portal.

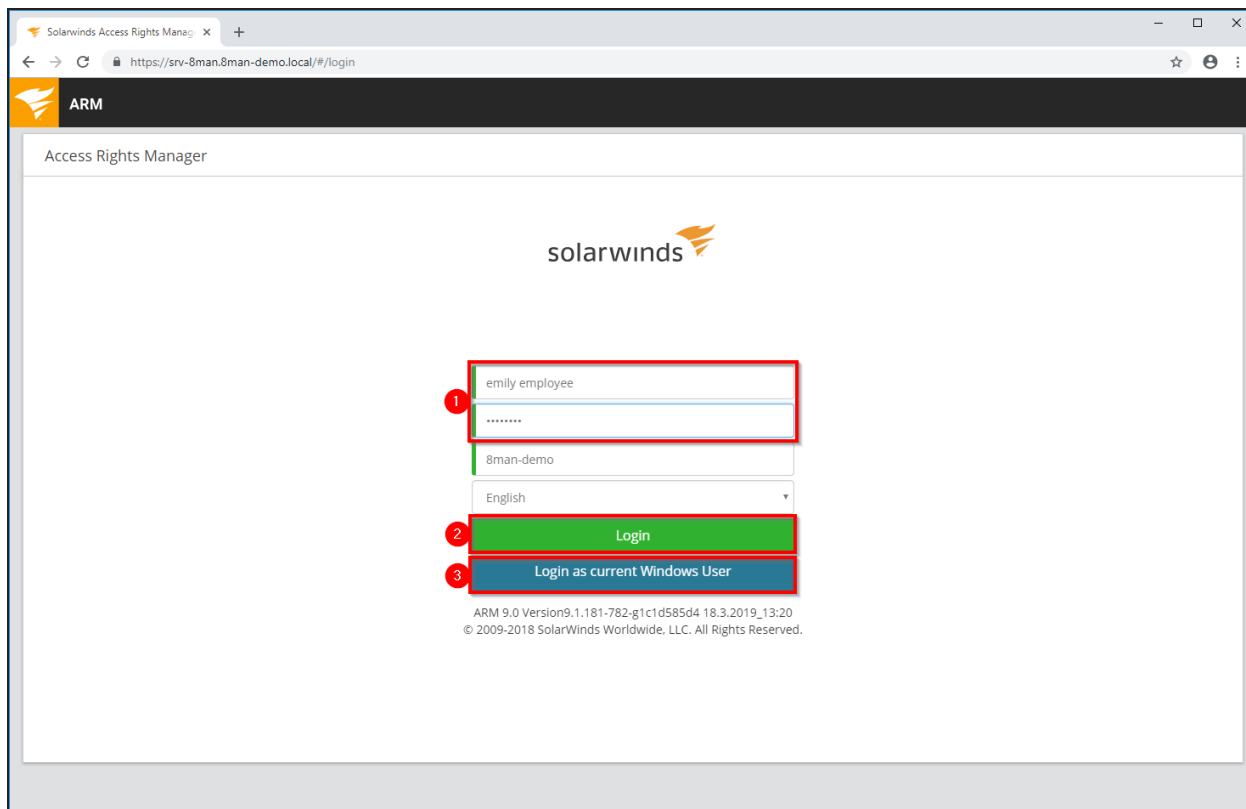
You can configure a variety of approval flows and involve the relevant decision makers, depending on your security requirements.

### Related features

[Manage my requests](#)

[GrantMA: Design approval processes](#) (administrator)

### Step-by-step process

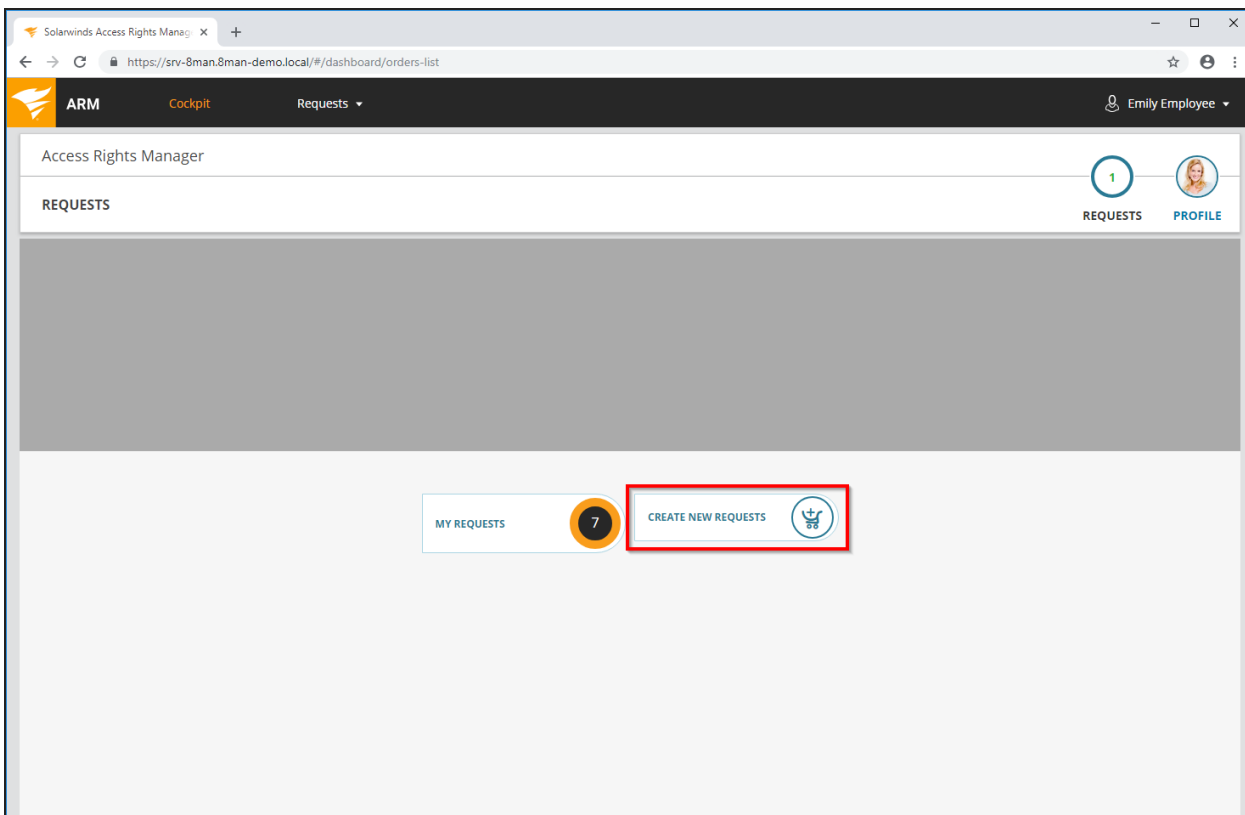


The screenshot shows the SolarWinds Access Rights Manager (ARM) login page. The page title is "Access Rights Manager" and the URL is "https://srv-8man.8man-demo.local/#/login". The page features the SolarWinds logo and a login form with the following elements:

- 1. A text input field for the user name, containing "emily employee".
- 1. A password input field with masked characters ".....".
- A dropdown menu for the domain, currently set to "8man-demo".
- A dropdown menu for the language, currently set to "English".
- 2. A green "Login" button.
- 3. A blue "Login as current Windows User" button.

At the bottom of the page, the version information is displayed: "ARM 9.0 Version 9.1.181-782-g1c1d585d4 18.3.2019\_13:20 © 2009-2018 SolarWinds Worldwide, LLC. All Rights Reserved."

1. Enter your user name and password.
2. Click "Login".
3. You can alternatively login as the current windows user (no user name and password required).



Click "Create new request".

Solarwinds Access Rights Manager

ARM Cockpit Requests Emily Employee

Access Rights Manager

CREATE A NEW REQUEST

1 Search resource

2 Start / 8MAN Demo Company / Marketing

Action	Resource	Details
Request	Create a project folder	OpenTemplate A form to run a script, which creates all needed folders for a new project
Request	Marketing - Create new group	Create group Marketing - Creates a new group
Request	Marketing - Create new user	Create user account Marketing - Creates a new user with formation rules

Action	Resource	Details
Request	Marketing (8man-demo\Marketing)	Active Directory
Request	Marketing	File server - Directory \srvr-8man\Organization\Marketing

1. Search for the group or
2. navigate to the desired level.

Solarwinds Access Rights Manager

ARM Cockpit Requests Emily Employee

Access Rights Manager

CREATE A NEW REQUEST

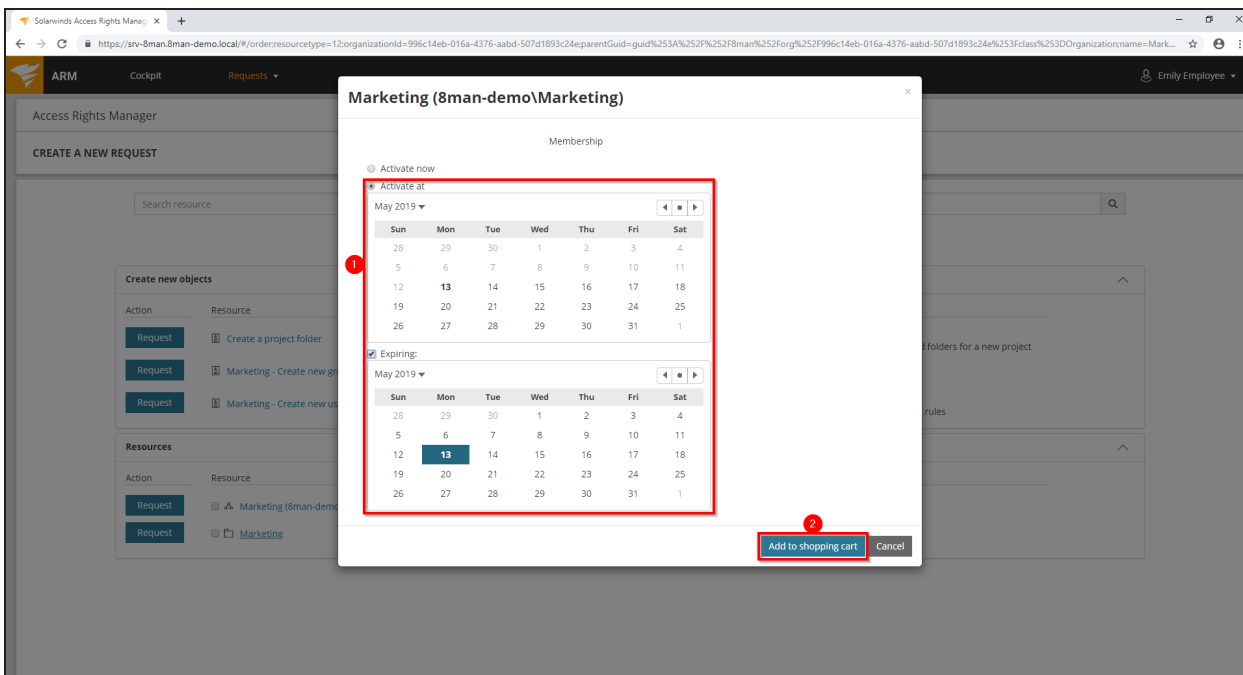
Search resource

Start / 8MAN Demo Company / Marketing

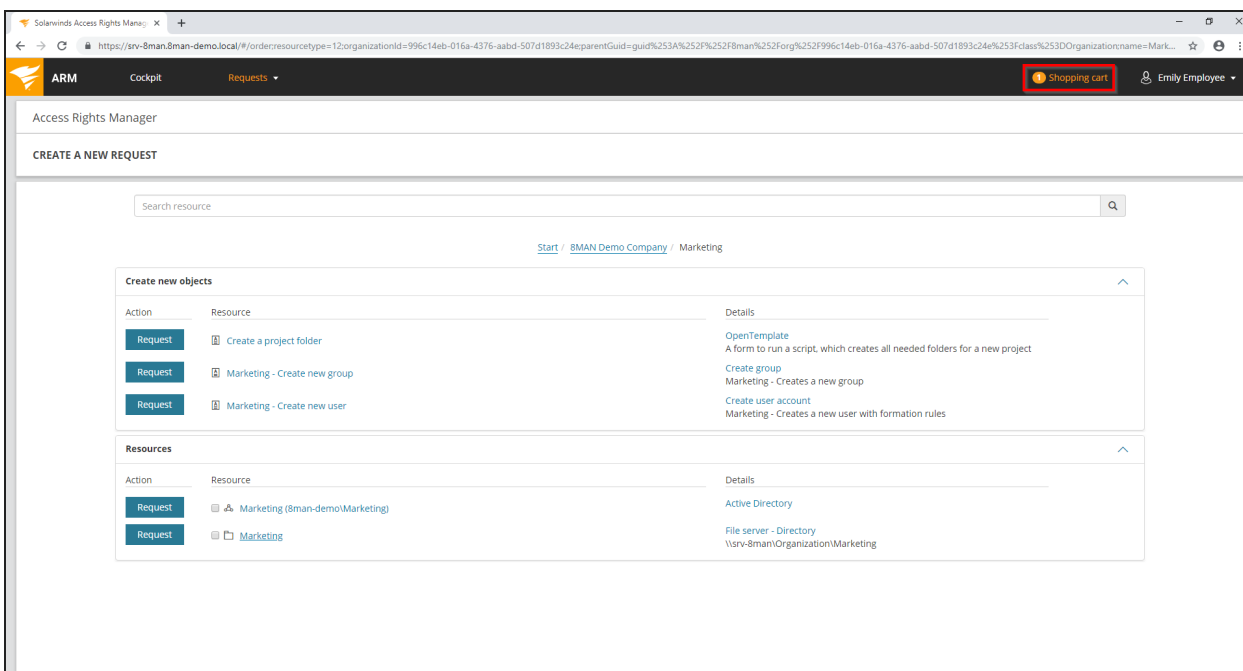
Action	Resource	Details
Request	Create a project folder	OpenTemplate A form to run a script, which creates all needed folders for a new project
Request	Marketing - Create new group	Create group Marketing - Creates a new group
Request	Marketing - Create new user	Create user account Marketing - Creates a new user with formation rules

Action	Resource	Details
Request	Marketing (8man-demo\Marketing)	Active Directory
Request	Marketing	File server - Directory \srvr-8man\Organization\Marketing

Once you have found the desired group, click "Request".



1. Optional:  
You can set an activation and an expiration date.
2. Click "Add to shopping cart".



If desired, add additional resources to your request. When ready, click "Shopping cart".

Screenshot of the SolarWinds Access Rights Manager (ARM) interface. The page title is "Access Rights Manager". The breadcrumb trail shows "8MAN Demo Company/Marketing". A table displays the resource details:

Resource	Type	Options
Marketing (8man-demo/Marketing)	Active Directory	Membership

Below the table, the section "Resources will be requested for:" lists the grantees:

- Add Grantee
- Emily Employee

The interface includes a "Please add a comment" text area, a "Request" button, and a validation message: "This input field requires a minimum amount of characters. Minimum required are: 1".

1. You can delete items from your request.
2. Add recipients to your request. You can request access for other users.
3. Remove receiver. You can also remove yourself and order only for other users.
4. You must enter a comment. Enter a valid reason. The comment will be displayed to the approver in the next step.
5. Start the request.



SolarWinds Access Rights Manager

ARM Cockpit Requests Emily Employee

Access Rights Manager

ALL REQUESTS (7/7)

Filter

Open  Approved and executed  Rejected and canceled  Failure during execution

5/13/2019 4:34 PM 1 × Active Directory

**Requested by:** Emily Employee

**Resources requested for:** Emily Employee

**Comment:** Demo

State	Resource	Type	Next approver
Open	Marketing (8man-demo\Marketing) CN=Marketing,OU=Demo Groups,DC=8man-demo,DC=local	Active Directory	8MAN Demo Company

5/10/2019 11:34 AM 1 × OpenTemplate

9/20/2018 1:23 PM 1 × File server

9/20/2018 1:16 PM 1 × File server

9/20/2018 12:54 PM 1 × OpenTemplate

9/20/2018 12:50 PM 1 × OpenTemplate

9/20/2018 12:45 PM 1 × Template

After confirmation, ARM will give you an overview of your orders.

1. Expand the detailed view of an order.
2. See more details.
3. Resend a notification email to the approver.
4. Cancel your order.

## Request directories

### Background / Value

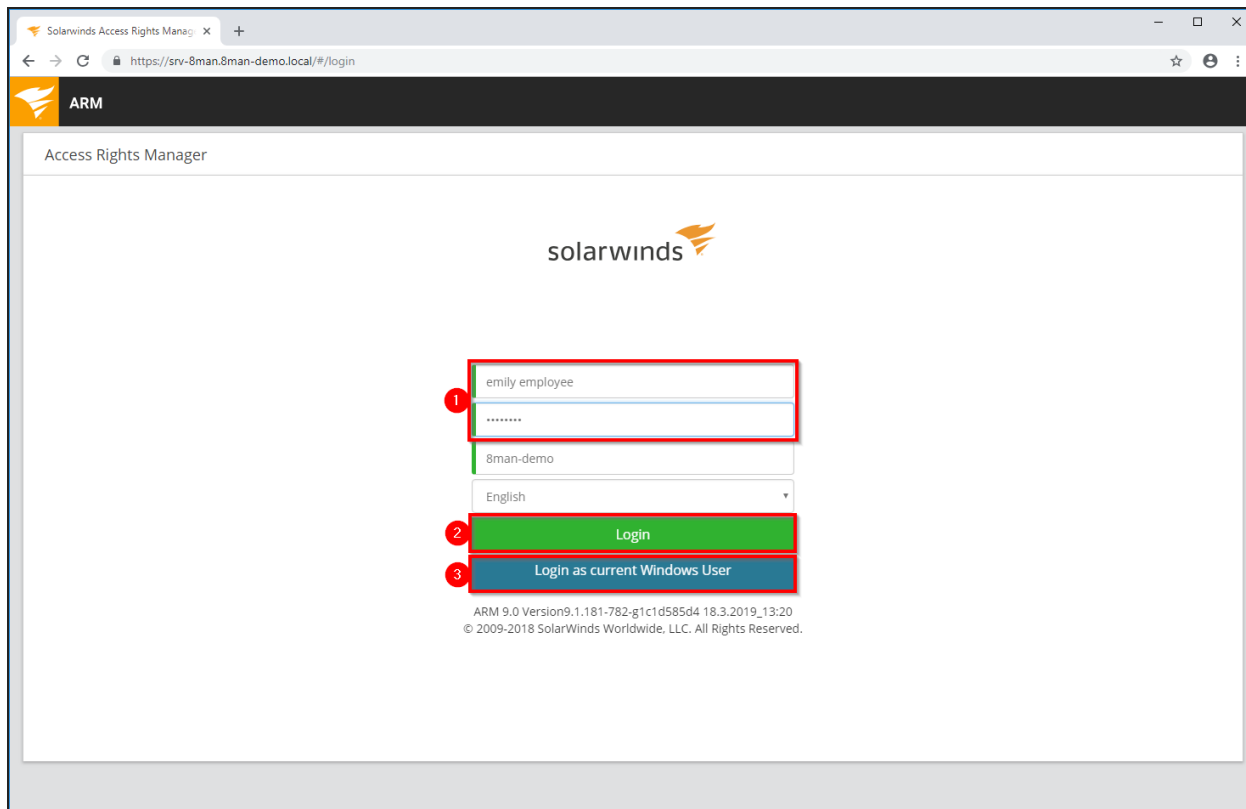
Order new directories using the GrantMA self service portal. This feature is useful for companies that follow restrictive policies for directory creation. We recommend that you allow the creation of directories up to the level three or four below the share only after requesting and approving.

### Related features

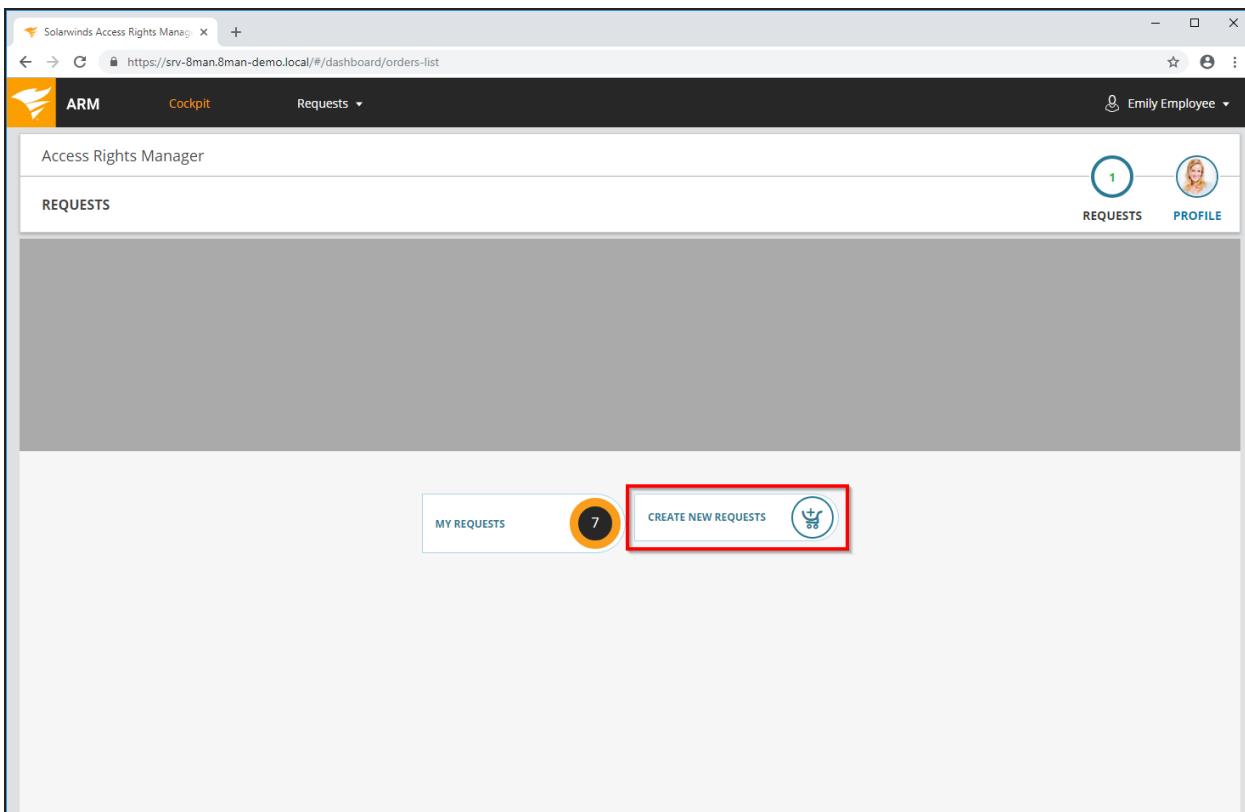
[Request file server permissions](#)

[Configure GrantMA](#)

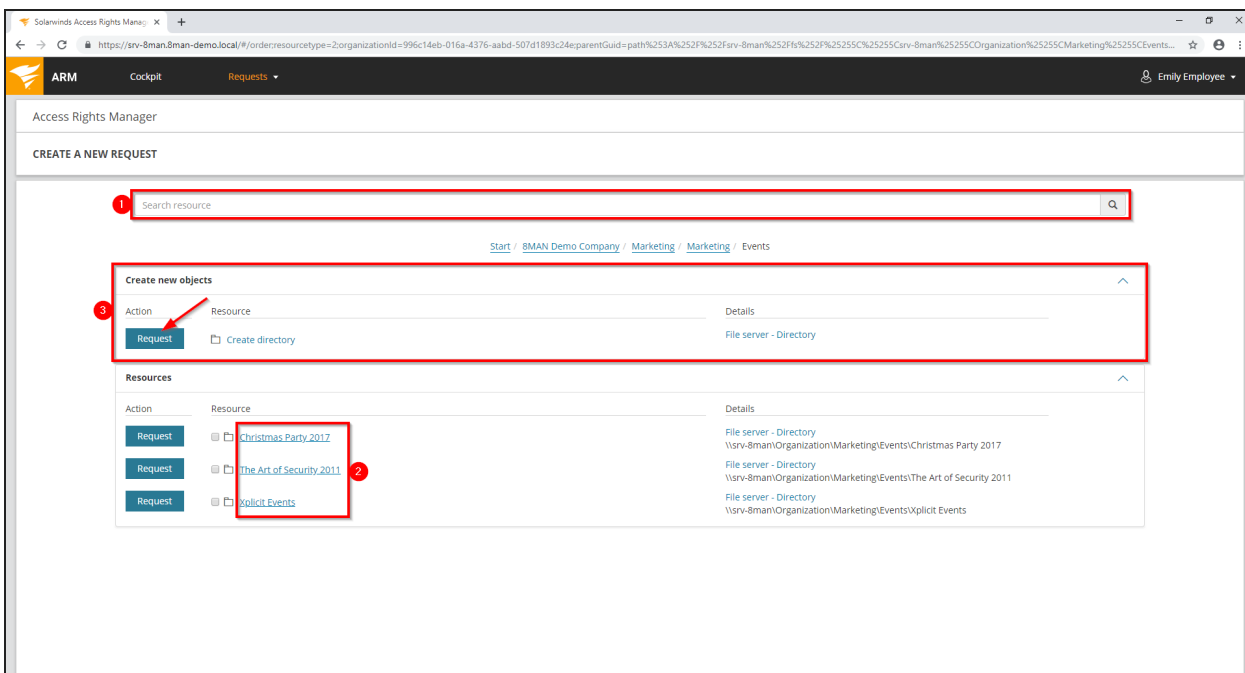
### Step-by-step process



1. Enter your user name and password.
2. Click "Login".
3. You can alternatively login as the current windows user (no user name and password required).

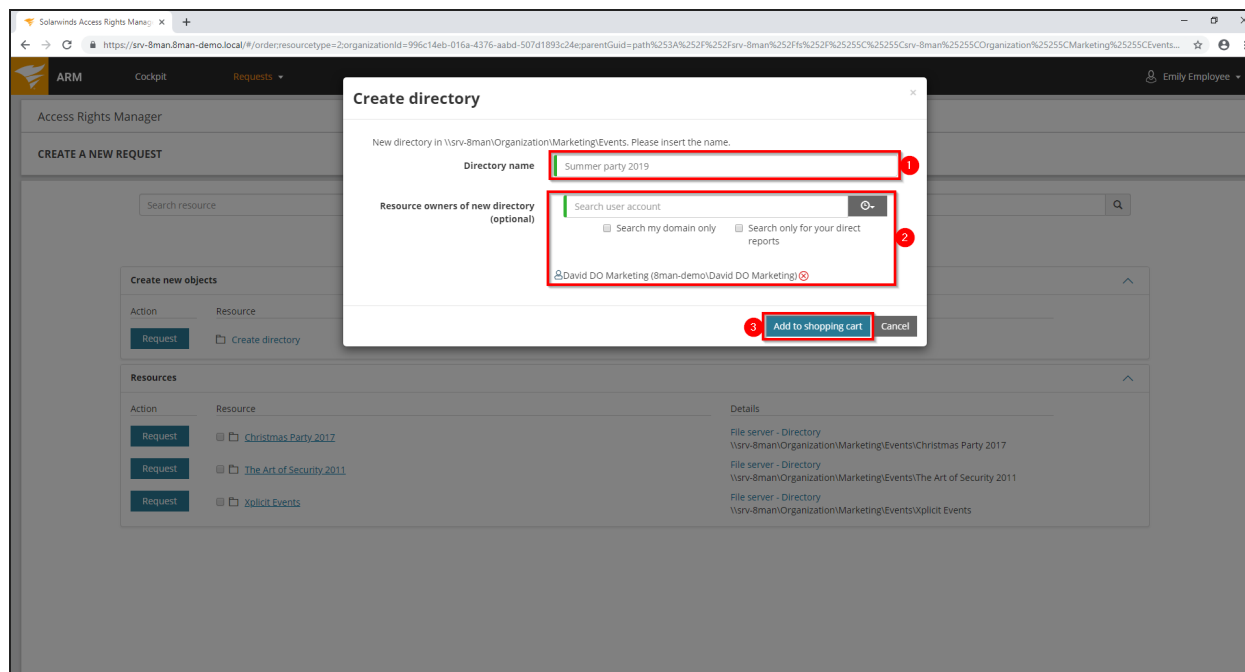


Click "Create new request".

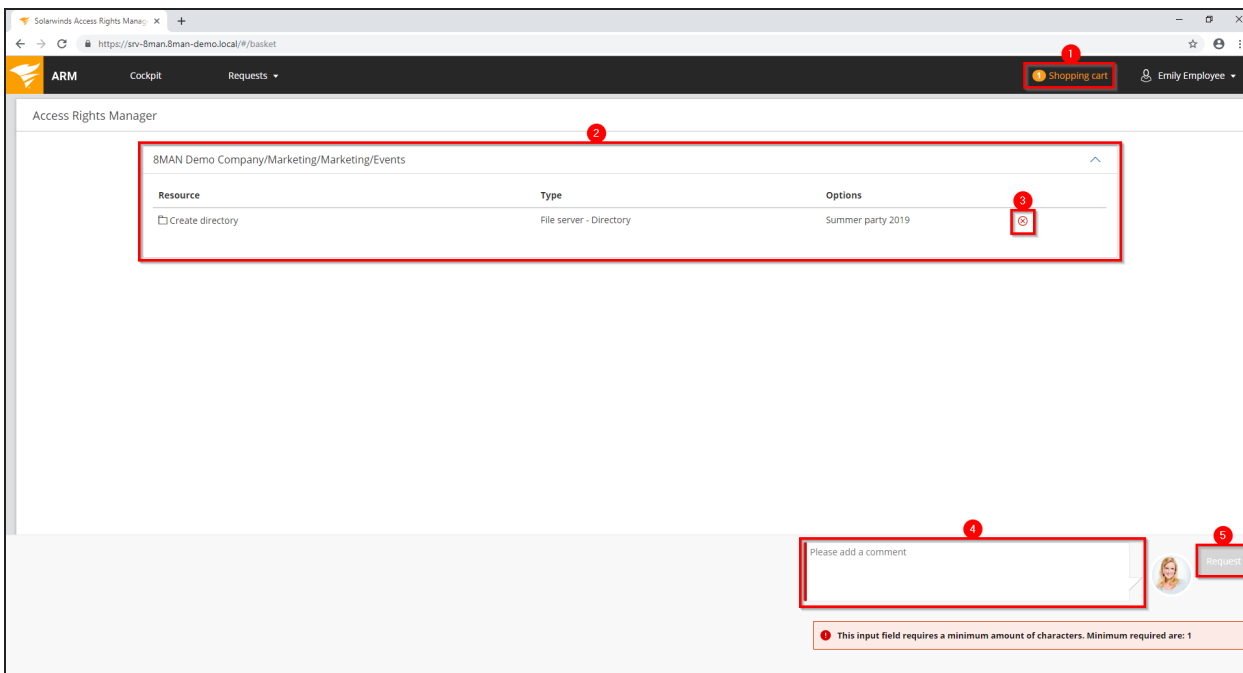


1. Use the search to find the desired resource.

2. Alternatively: Navigate to the desired resource.
3. Click "Request" in the "Create new objects" area.



1. Give the new directory a name.
2. Optional:  
If the [resource owner configuration](#) is activated, you can specify a resource owner.
3. Place the order in the shopping cart.



1. Click the shopping cart.
2. ARM will show you the order basket with your requests.
3. You can cancel your request.
4. You must enter a comment, e.g. a ticket number.
5. Start your request.

## Create a user account as an HR employee

### Background / Value

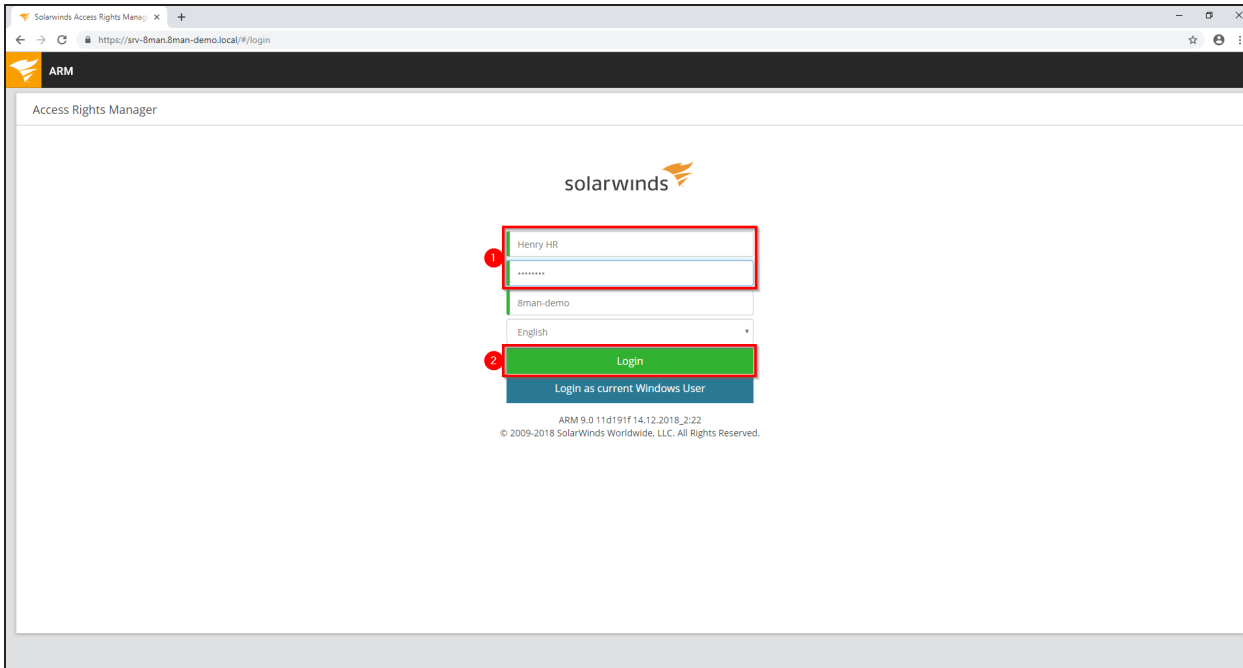
The ARM GrantMA self-service portal allows HR employees to create user accounts for new employees. Instead of sending user information to IT, the entry and creation of a new user account are combined into one simple step. IT simply has to approve the request.

This process is especially useful for departments with high employee turnover and/or a project oriented approach.

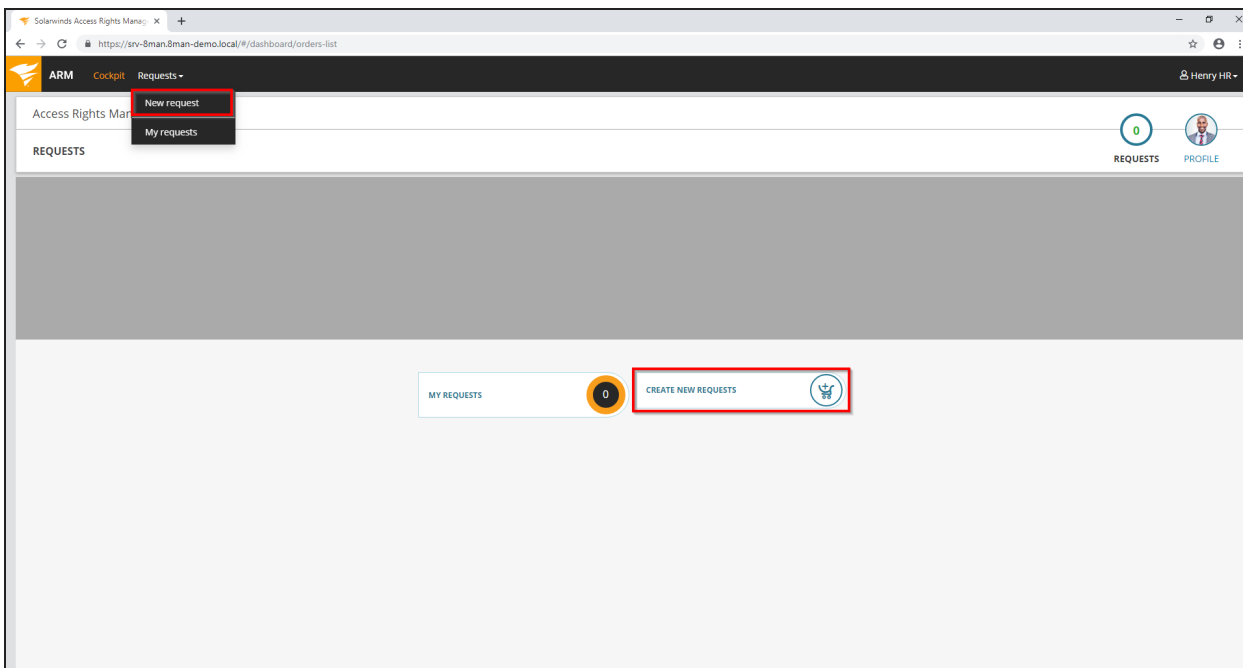
### Related features

[Approve or reject requests \(cockpit\)](#)

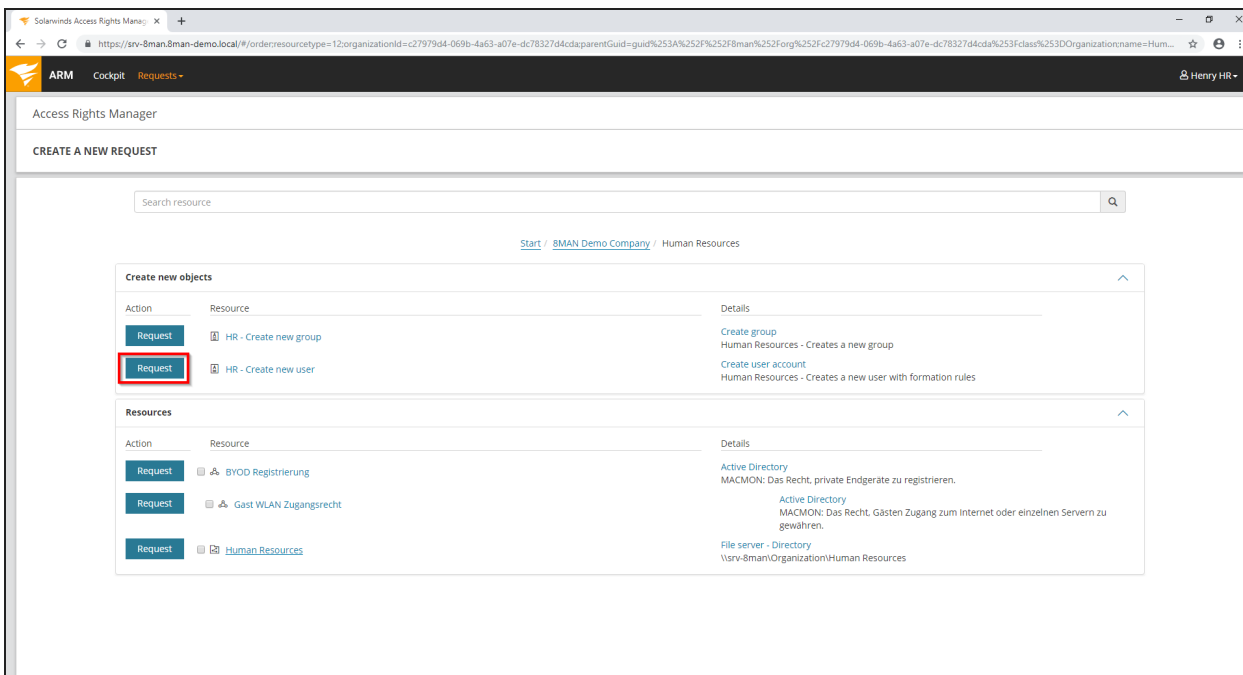
## Step-by-step process



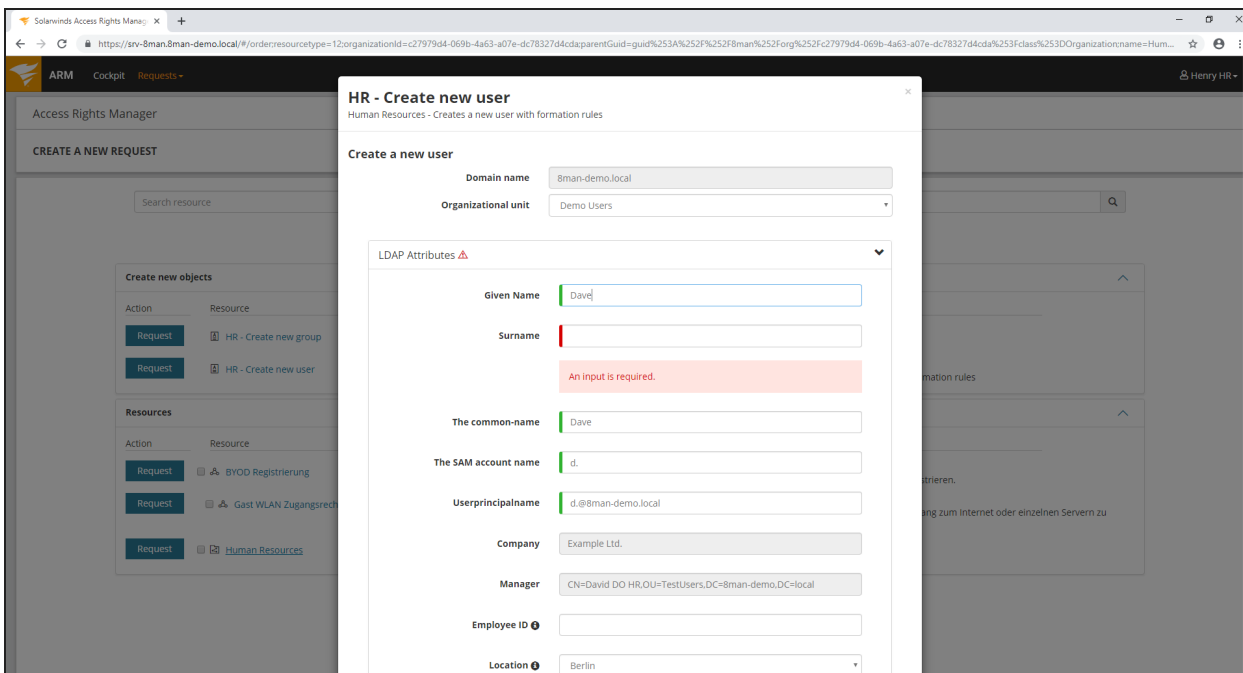
1. Enter your user name and password.
2. Click on "Login".




Click "New Request".

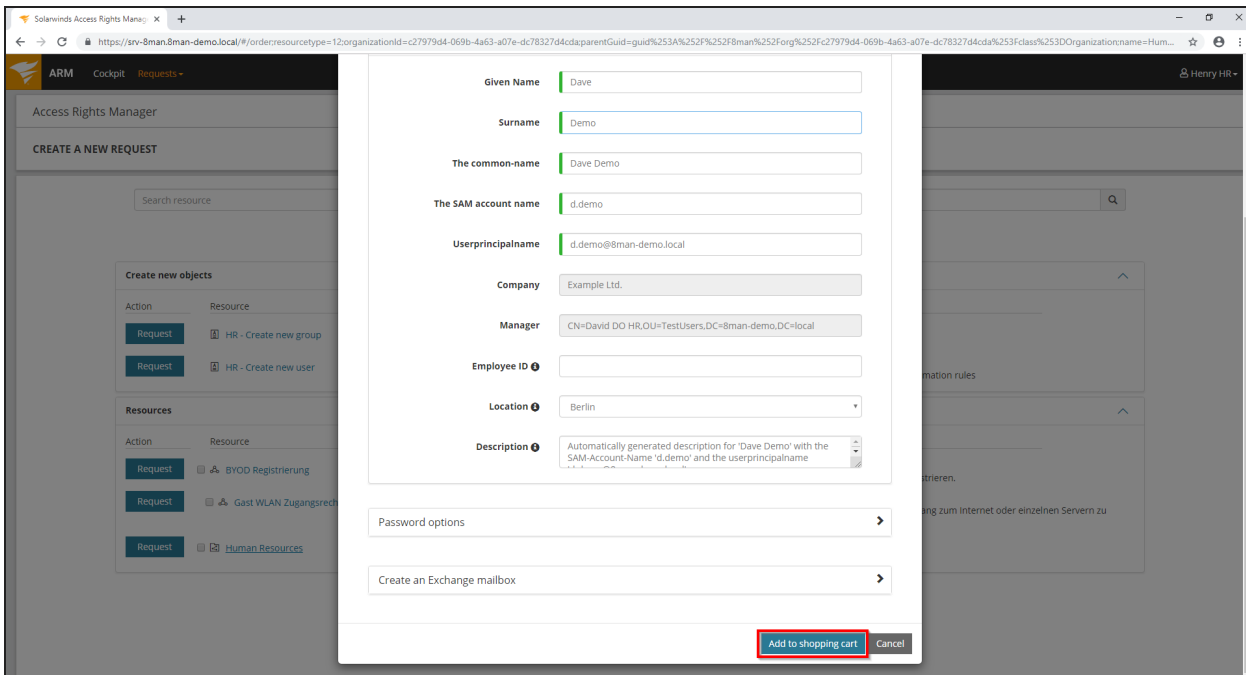


Select "new user" and click on "Request".

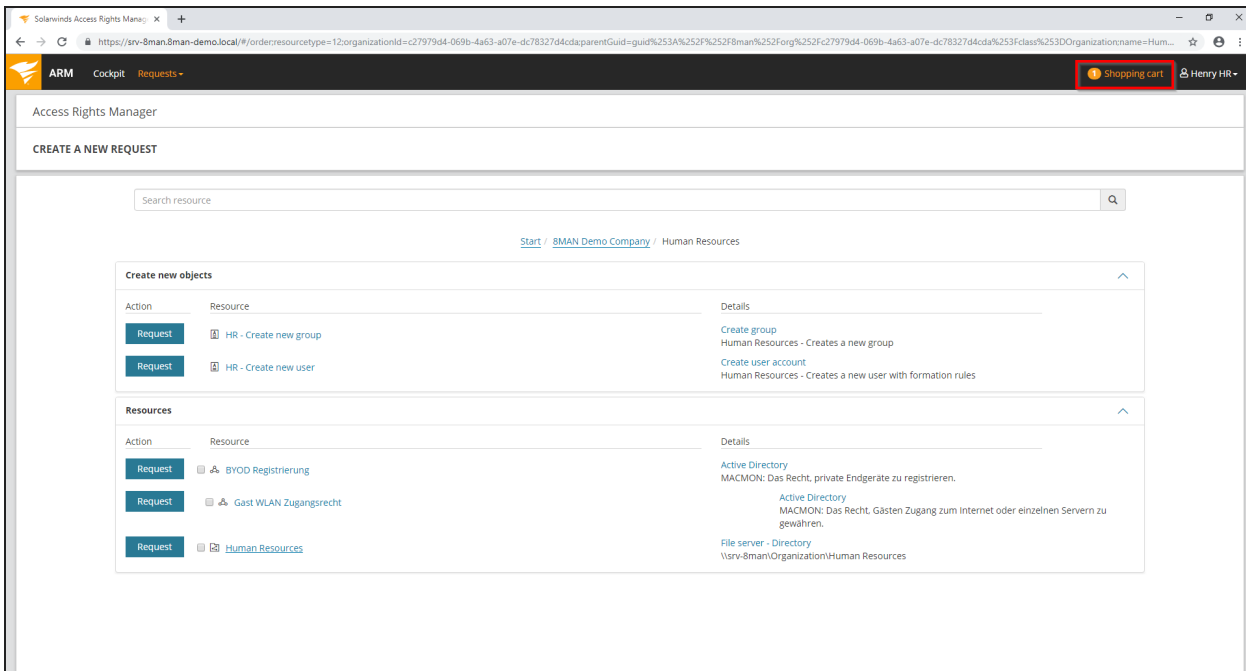


Enter the relevant information for the new user. Fields indicated in red are mandatory or contain invalid entries.

 ARM administrators can customize the input template.

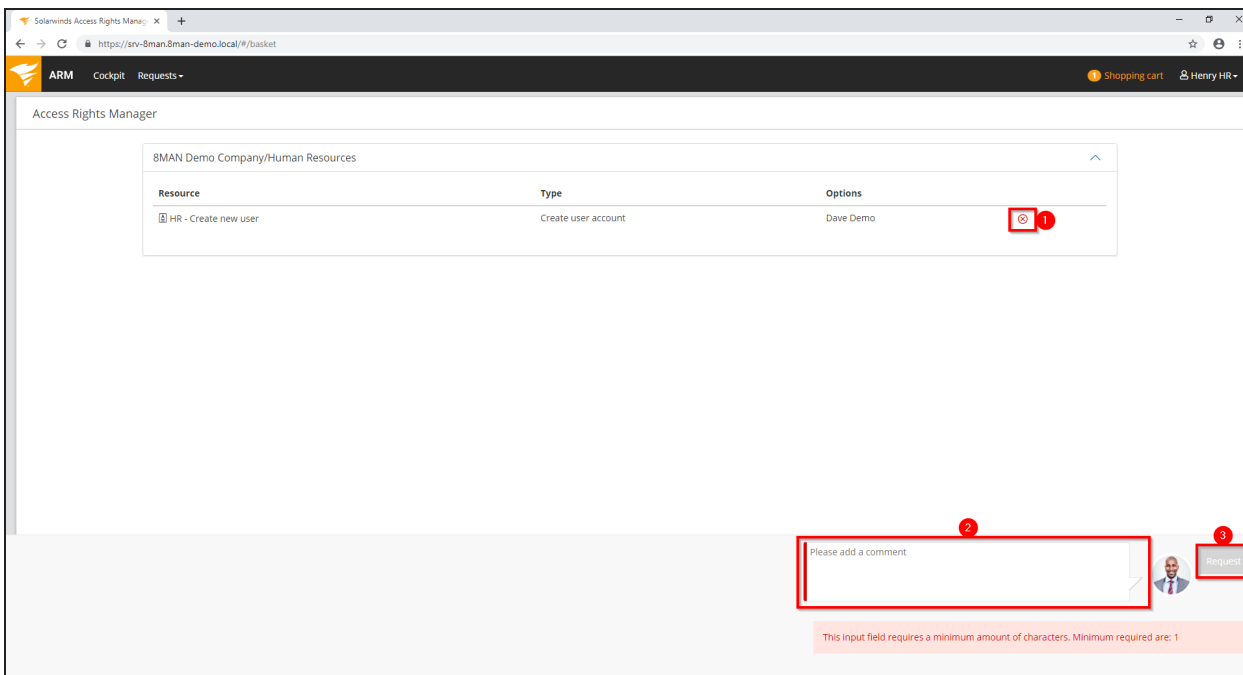


After entering all required information click on "Add to shopping cart".

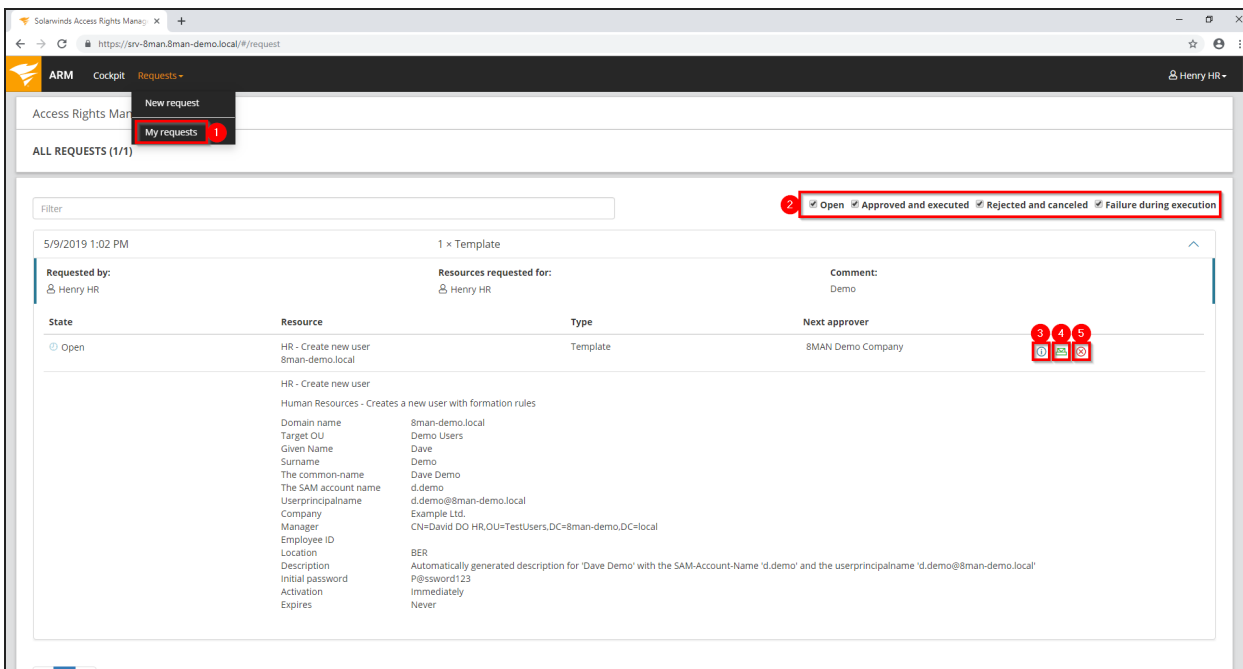


Add additional resources if desired. Click on "Order Basket".





1. You can delete an order item.
2. You must enter a comment.
3. Start the request.



1. ARM shows you an overview of your requests. You can always view your requests by selecting "My Requests" from the menu.

2. You can filter your requests to shorten a long list.
3. View additional details.
4. Resend a notification email to the approver.
5. Cancel your order.

## Order script-based services

### Background / Value

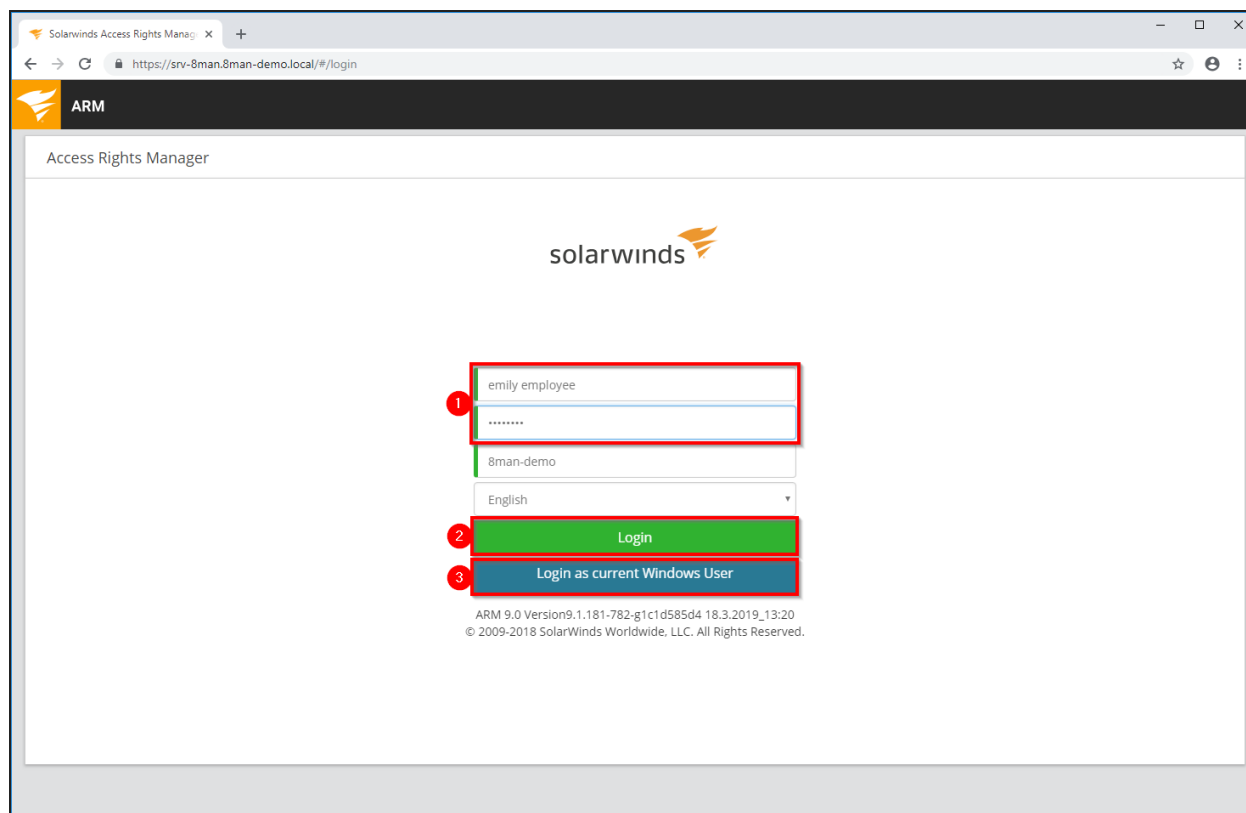
In addition to ordering user accounts, authorizations, directories or freely definable objects (OpenOrder), other script-based services can be ordered via the web client.

The IT defines a service that can be executed via a script. The service gets a meaningful name (for example, "order a project structure on the fileserver"). The employee orders the service in the GrantMA and enters the basic data via a template. After the individually configurable approval flow, the script is started automatically.

### Related features

[Configure scripts \(Administrator\)](#)

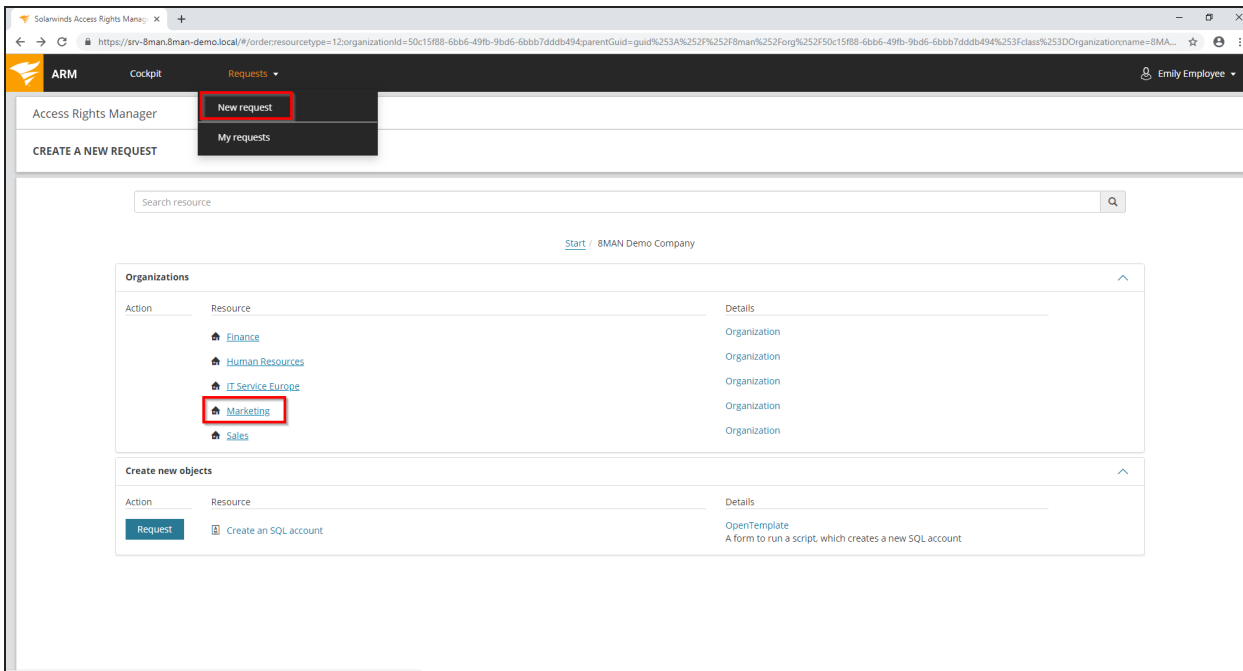
### Step-by-step process



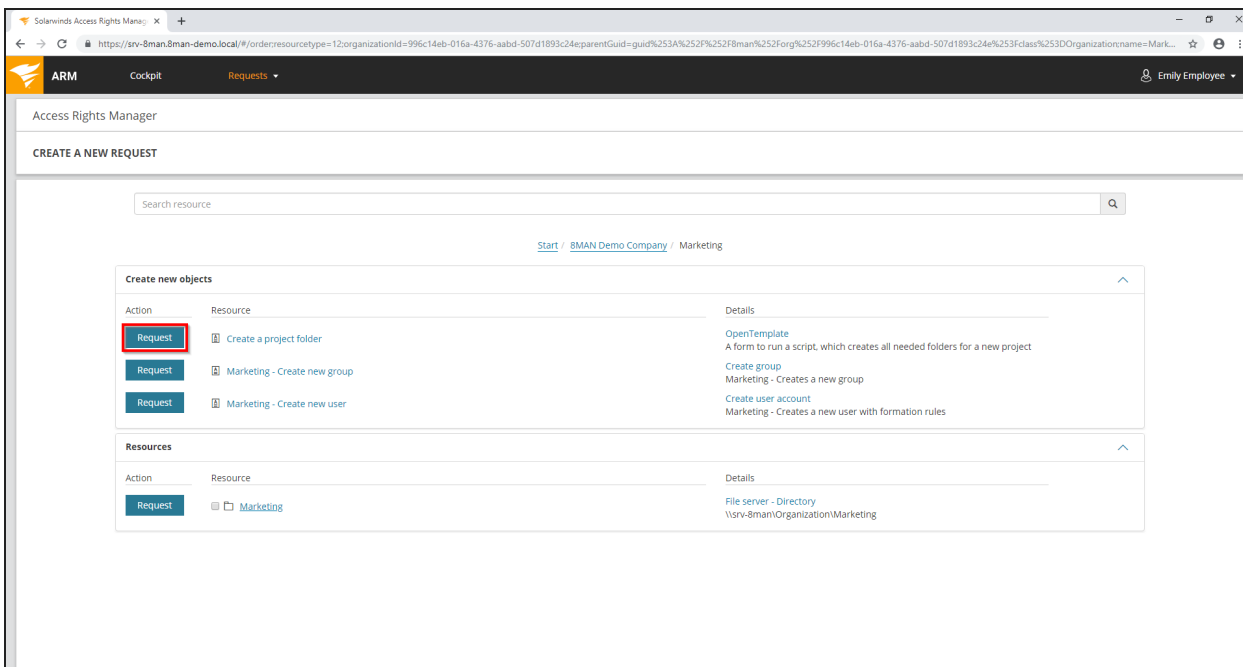
The following example, a user requests a project folder structure.

1. Enter your user name and password.
2. Click "Login".

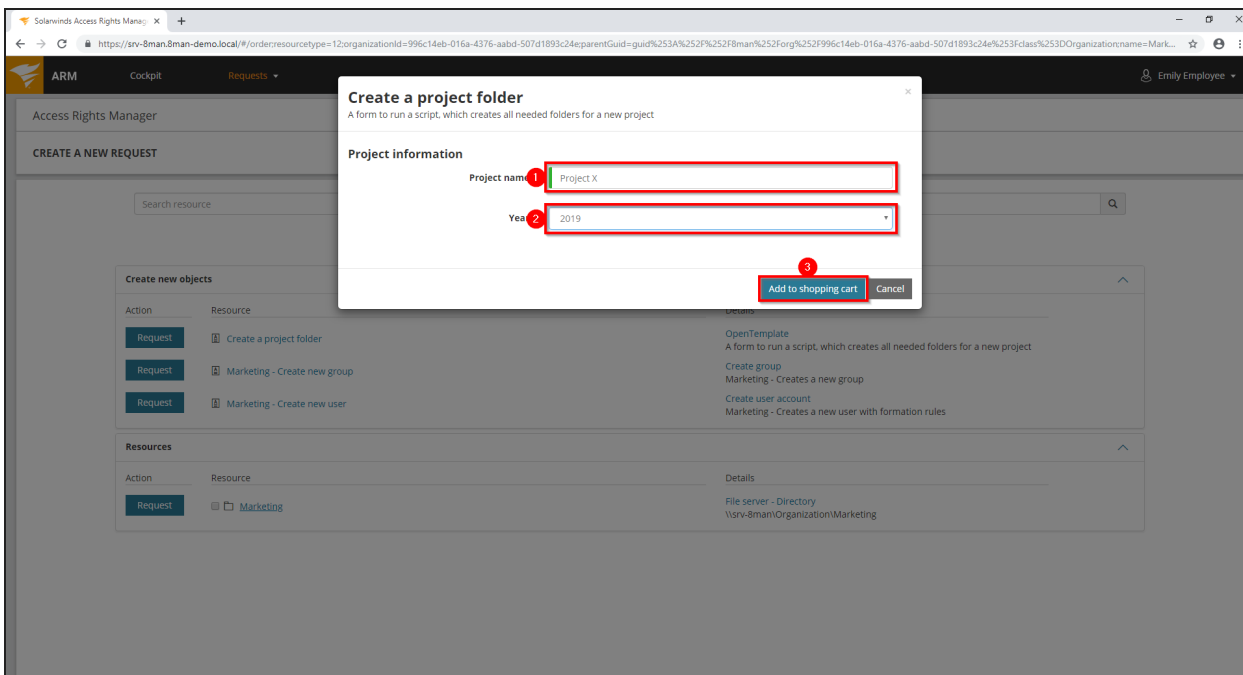
3. You can alternatively login as the current windows user (no user name and password required).



Select the organizational category that contains the service. In the example here "Marketing".

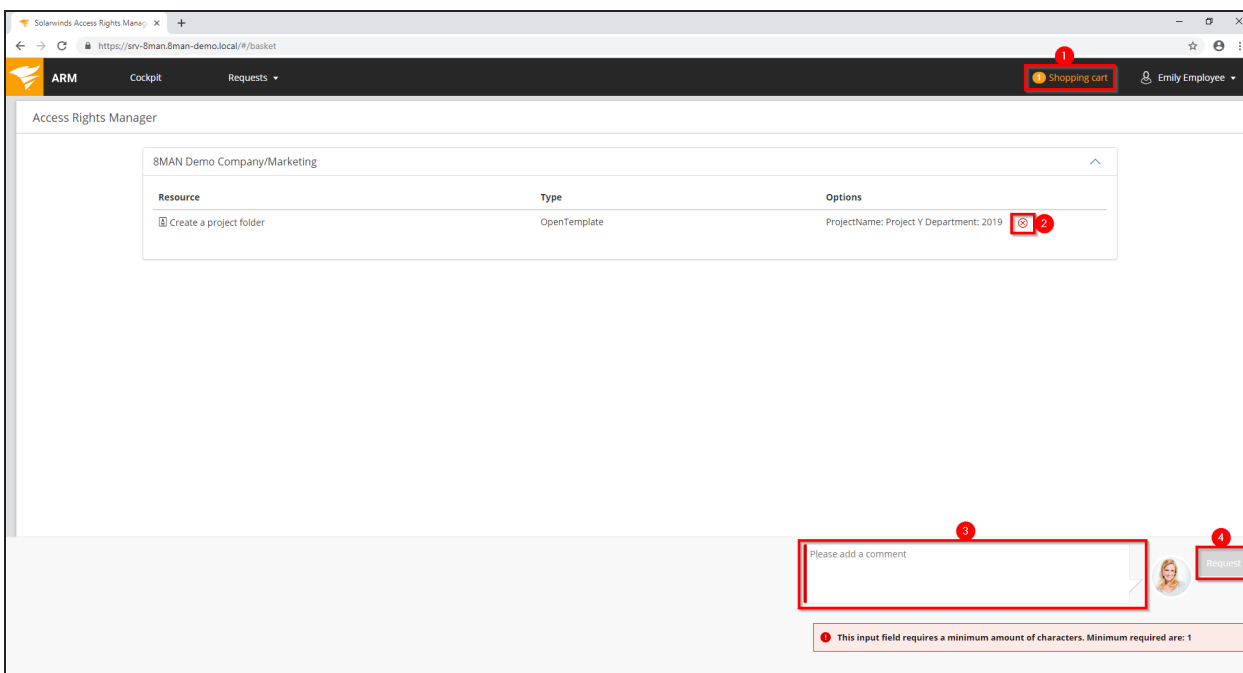


Select the service "Create project folder" and click on "Request".



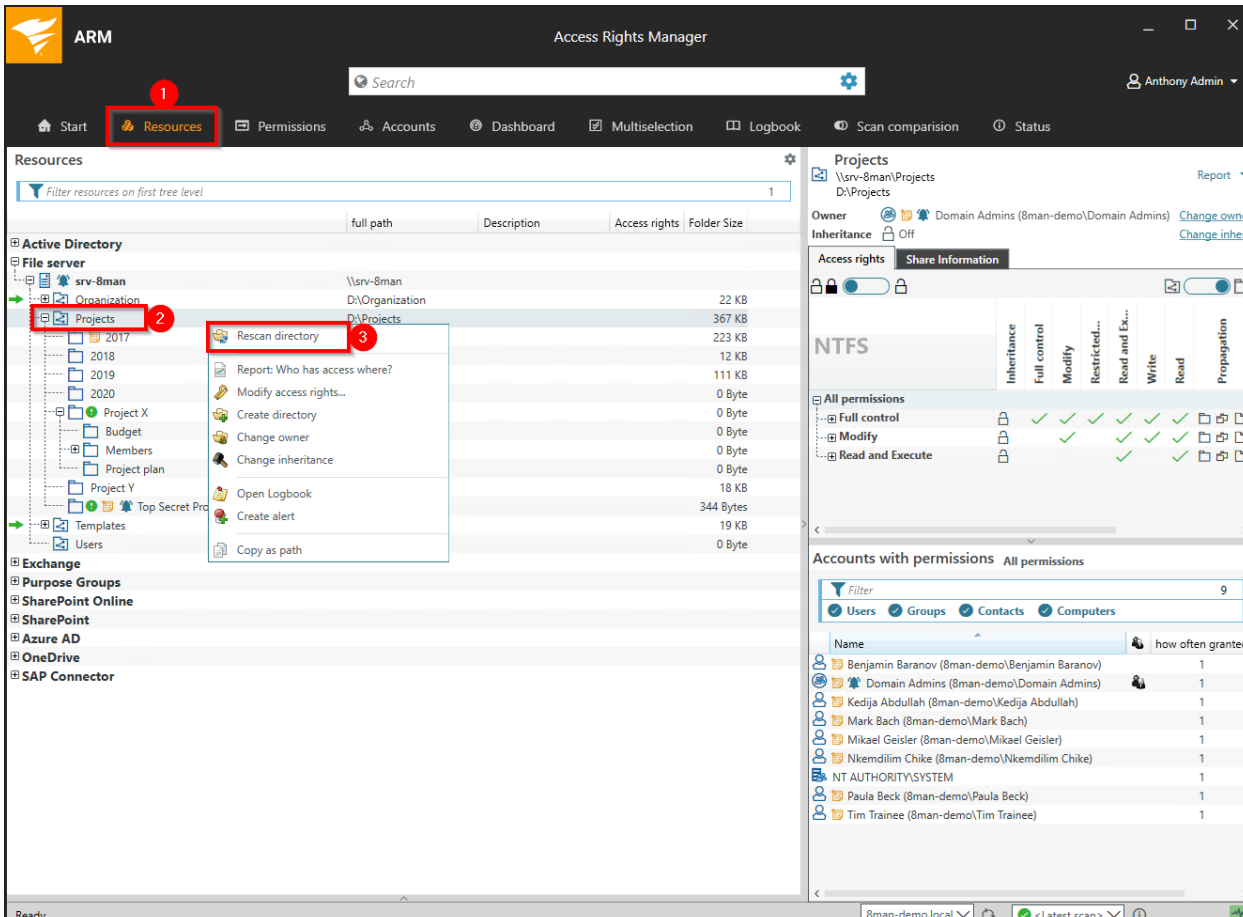
Enter the parameters for the script. In the example:

1. Assign a name to the project folder.
2. Choose a year. In the example, the "parent folder" under which the project structure is created.
3. Click on "Add to cart".



Complete the order:

1. Click on "Shopping cart".
2. You can cancel your request.
3. Enter a comment.
4. Click on "Apply".



After the approval the folder structure is generated by script "outside" of ARM. In order for the new folders to be visible within ARM, the corresponding directory must be rescanned.

1. Select "Resources".
2. Navigate to the desired folder.
3. Right-click on the folder and select "Rescan directory" from the context menu.

# ARM GrantMA: workflows for data owner/administrators

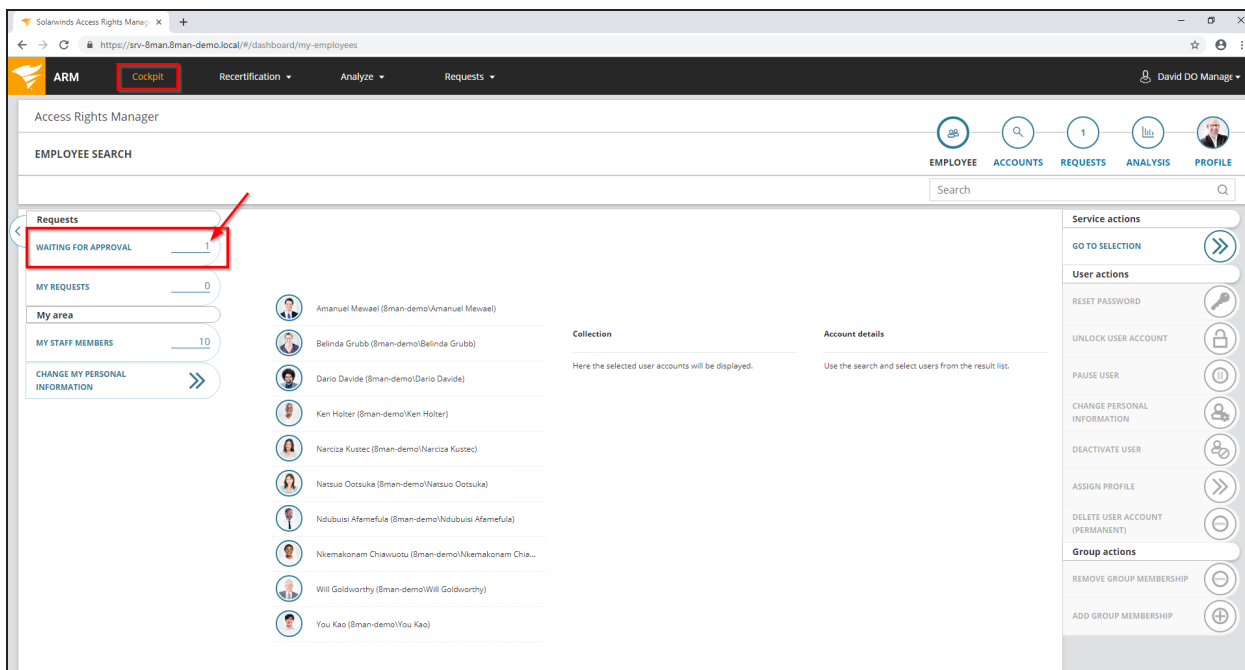
By using the ARM GrantMA self-service portal, managers and data owners are able to approve and modify or reject requests.

## Approve or reject requests (cockpit)


### Background / Value

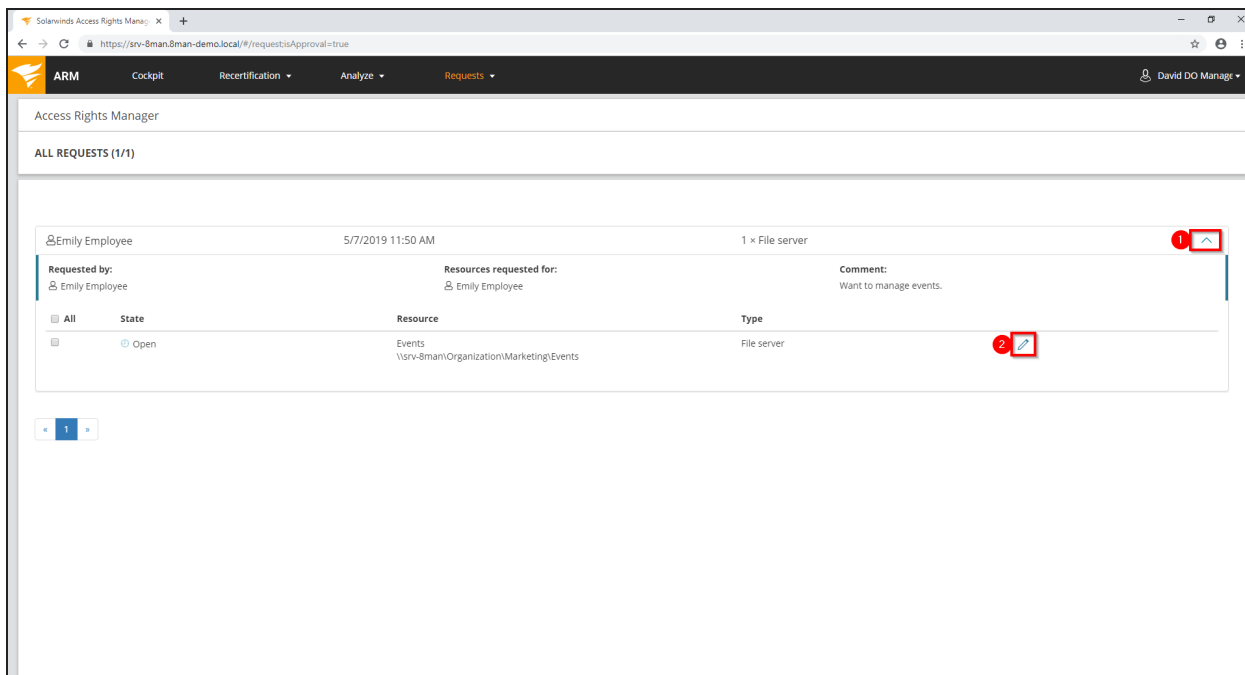
Depending on how you have set the approval process, you will receive approval requests for the individual order processes. As an administrator or data owner you keep an eye on the processes.

### Step-by-step process



Click "Waiting for Approval." In the example shown, 1 request is waiting for approval.

 The range of available services (buttons) varies according to role (login), risk assessment and configuration.



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The browser address bar indicates the URL: `https://srv-8man.8man-demo.local/#/requests?approval=true`. The page title is "Access Rights Manager". Below the title, it says "ALL REQUESTS (1/1)".

The main content area displays a request for access to a file server. The request details are as follows:

Requested by:	Resources requested for:	Comment:
Emily Employee	Emily Employee	Want to manage events.

Below the request details, there is a table with the following columns: All, State, Resource, and Type. The table contains one row:

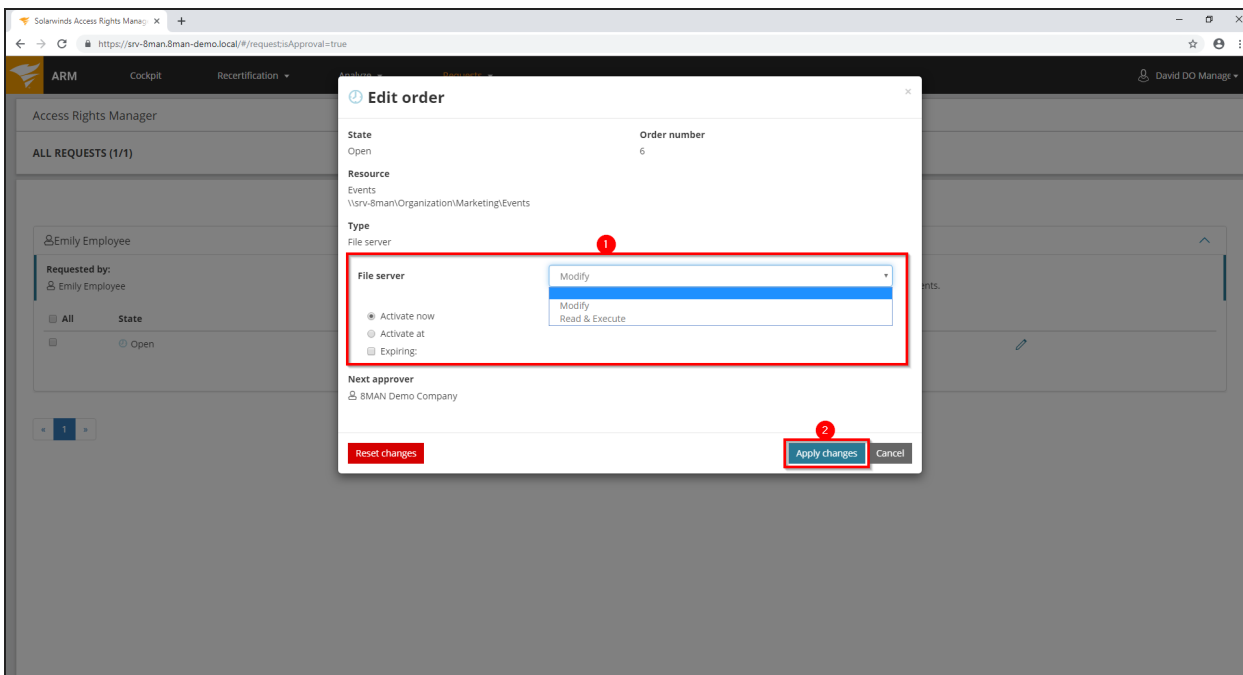
All	State	Resource	Type
<input type="checkbox"/>	Open	Events \\srv-8man\Organization\Marketing\Events	File Server

There are two red boxes with numbers 1 and 2 highlighting specific icons. Box 1 highlights an information icon (i) in the top right corner of the request card. Box 2 highlights a pencil icon (edit) in the bottom right corner of the resource row in the table.

1. Expand an order to see the items.
2. Depending on the ARM configuration set by your ARM administrator, you will see a pencil or information symbol:
  - Pencil: You can modify the order.
  - Info: You see the details and you are not allowed to modify the order.

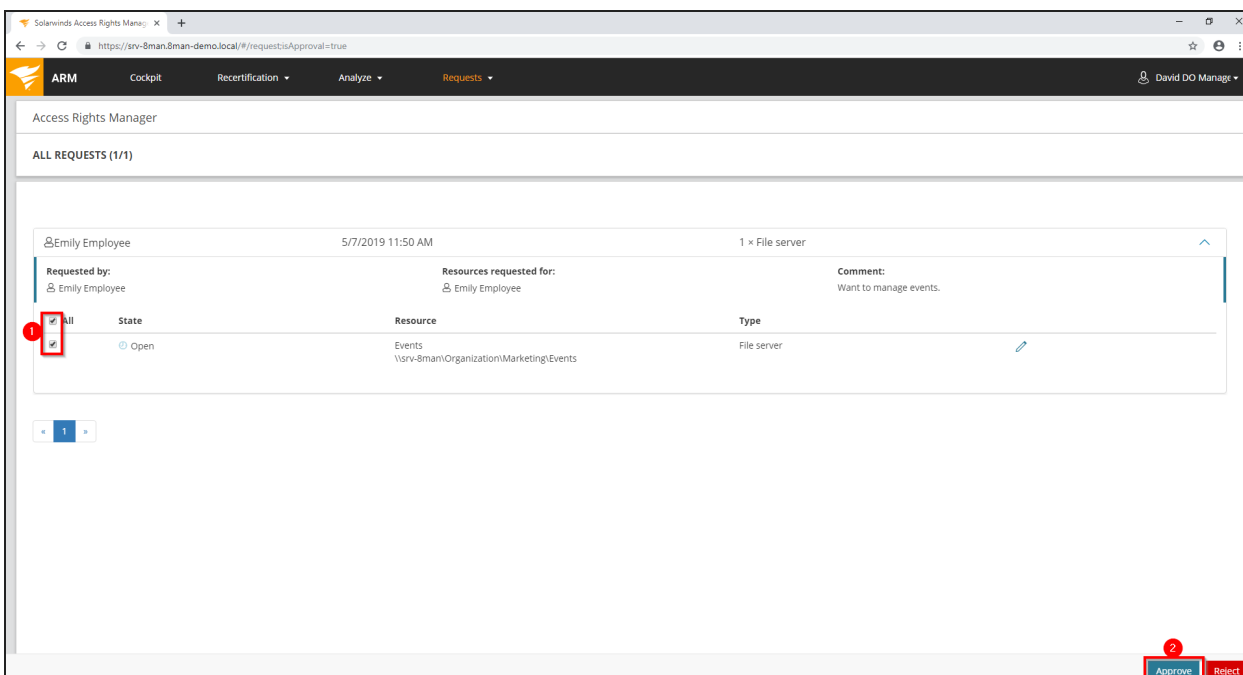
Click on the pencil icon.





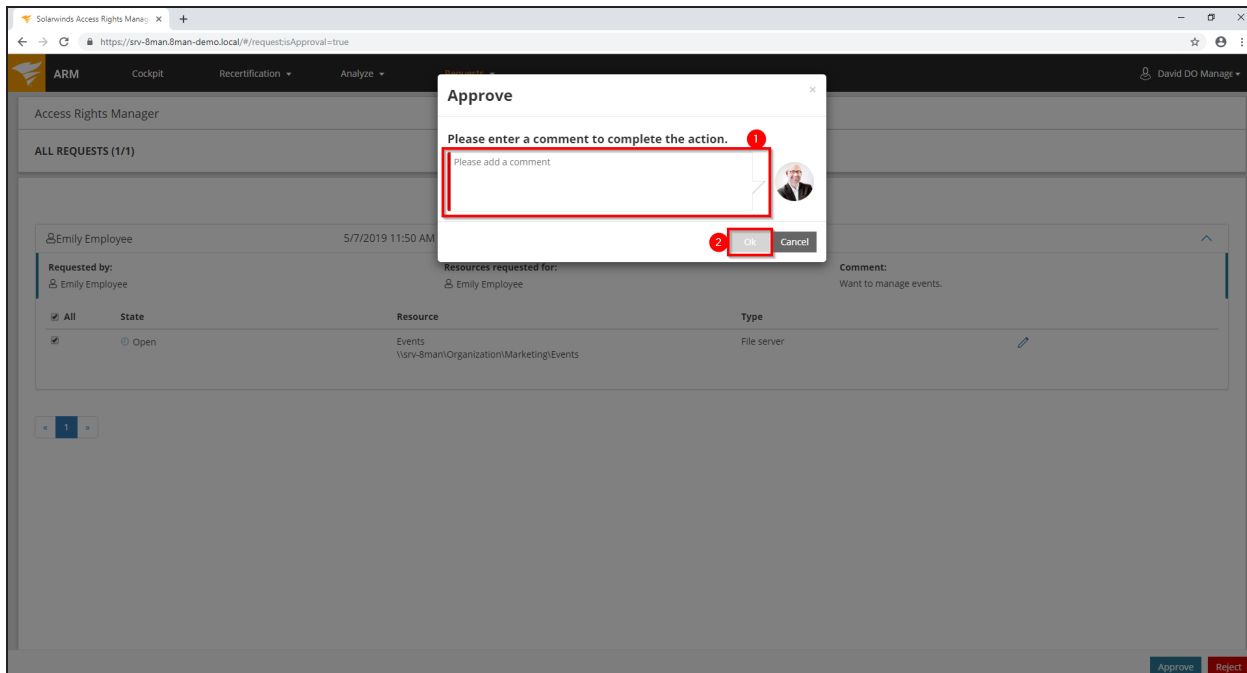
You can edit the order request.

1. For example, you can downgrade the requested "modify" right to "read" and set the permission to a start and end date.
2. Click on "Apply changes".



1. Select the desired order or item.

## 2. Click "Approve".



1. You must enter a comment.
2. Click "OK".

**i** The comment appears in the logbook and is therefore documented auditable.

## Inform approvers of new requests via email

### Background / Value

To prevent approvers from having to proactively check for open approval requests on the ARM home page, we recommend activating approval emails.

### Related features

[GrantMA: Design approval processes](#)

[Customize notification emails](#)

### Step-by-step process

The screenshot shows the Solarwinds Access Rights Manager (ARM) settings page for GrantMA. The page is titled "Access Rights Manager" and "SETTINGS: GRANTMA". The "General Settings" section is visible, showing the administrator email address for GrantMA as "Anton.Admin@man-demo.local". The "Maximum number of items to show on order overviews" is set to 1000, and "Open requests will expire after" is set to 14 days. The "Send emails to the requester on status updates" section is highlighted with a red box, containing three checked options: "Send emails to the requester on status updates (On order, reject, executed or failed)", "Send additional emails to the requester on each approval step", and "Send email on each new approvable request to the Approver". Other options include "Allow requesters to browse hierarchical resources (e.g. file system folders)", "Allow approvers to modify order details", and "Legacy mode for resolving workflows and data owner approvers". A "Save" button is visible at the bottom right of the settings area. Red numbers 1, 2, 3, and 4 are overlaid on the screenshot to indicate the steps: 1 points to the user profile menu, 2 points to the "GrantMA" menu item, 3 points to the email notification options, and 4 points to the "Save" button.

Log into the web client as an ARM administrator.

1. Click the gear.
2. Click "GrantMA".
3. Enable the email options. In order to keep the applicant as well as the approver informed, we recommend activating all options.
4. Save the settings.

**Approval required**

Dear David DO Manager (8man-demo\David DO Manager),

**Emily Employee** has placed a ARM GrantMA order that awaits your approval. The order was placed on **5/13/2019 at 4:34 PM**.

Please visit the [ARM GrantMA](#) page to approve (or reject) the items in this order.

**Order summary**

Emily Employee wrote the following comment:  
"Demo"

The following items were ordered for:

- **Emily Employee**

Order Number	Name	Type	Options	Approver history
<a href="#">7</a>	Marketing (8man-demo\Marketing)	Active Directory	Membership	

Best regards  
ARM GrantMA

Example of an email notification.

## User Provisioning

### User creation

User Provisioning allows you to set up new users within seconds. Users are generated in a standardized manner and in conformity with the roles in your company. The access rights to file servers, SharePoint sites, Exchange and further resource systems are issued at the same time. You can schedule the activation to prepare for the event in the future or to limit the access period for project work. Whether help desk or data owner: The participants work with a reduced, simple interface in both cases. All accesses are set up in a few steps.

### Access Rights Management

Modify the authorizations of existing accounts by dragging and dropping in a simple interface.

### Account Management

Account management includes modifying Active Directory attributes, password resetting, activating and deactivating accounts and setting up out-of-office notifications centrally in Exchange, among many other tasks.

## Active Directory

ARM provides many features for managing access rights via Active Directory.

We have grouped the features by complexity: for administrators (more complex), helpdesk agents and data owners/managers (less complex).

### Administrator

Create a user account

#### **Background / Value**

With ARM you can quickly create standardized user accounts. You can delegate the process to the Helpdesk and further simplify and standardize it using specifically customized templates for different company roles.

#### **Related features**

Customize templates for account creation (please refer: [Customize ARM templates](#))

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes a search bar and a user profile for Anthony Admin. The main content area is divided into several sections:

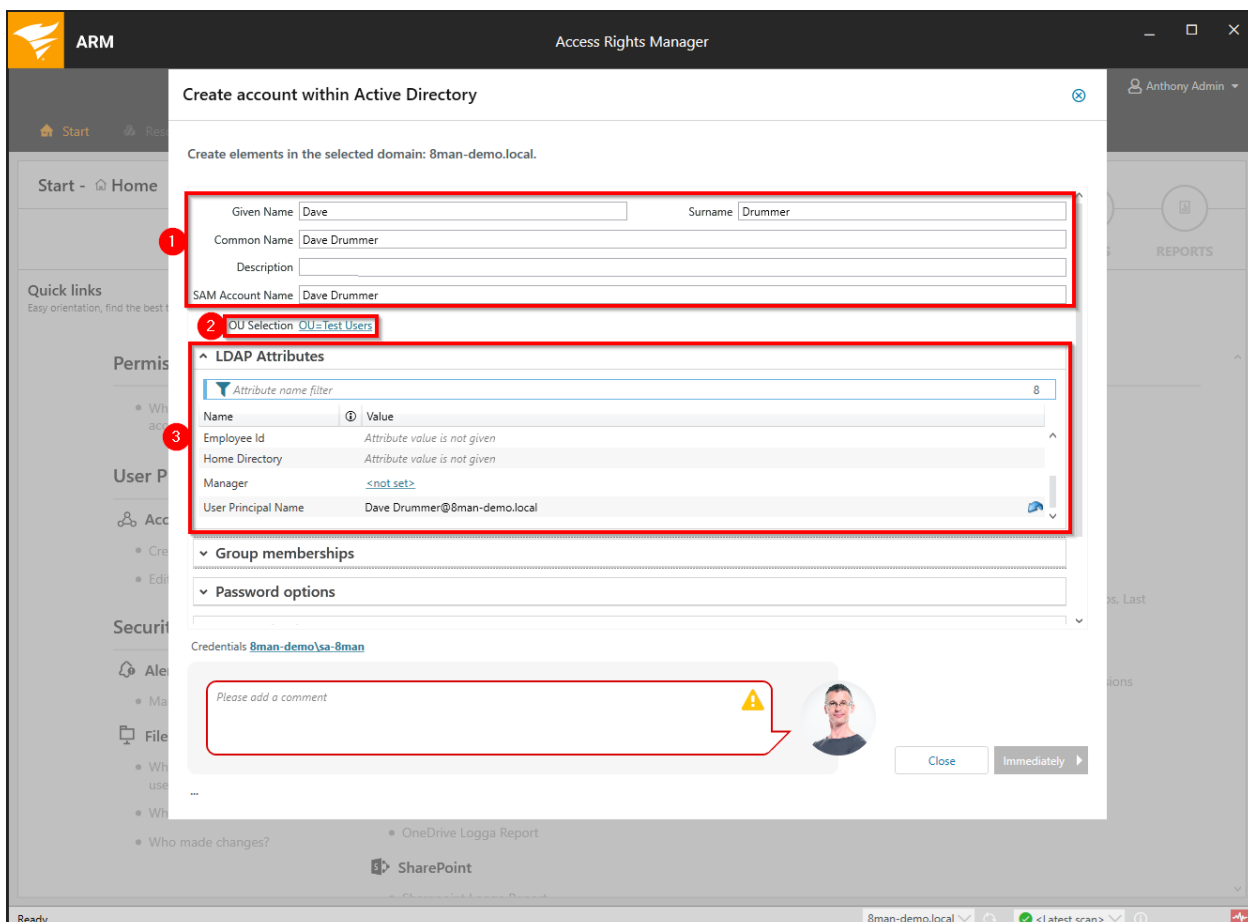
- Start - Home**: Navigation tabs for HOME, NOTES, REQUESTS, TASKS, and REPORTS.
- Quick links**: Easy orientation, find the best tool for your productivity in ARM.
- Permission Analysis**:
  - Where does a user/group have access?
- User Provisioning**:
  - Accounts
    - Create new user or group (highlighted with a red box and a red circle containing the number '2')
    - Edit group memberships
  - Resources
    - Edit access rights
- Security Monitoring**:
  - Alerts
    - Manage alerts
  - File server
    - Who did what, except authorized users (SoD)?
    - Who did what?
    - Who made changes?
  - Active Directory
    - AD Logga Report
  - Exchange
    - Exchange Logga Report
  - OneDrive
    - OneDrive Logga Report
  - SharePoint
- Documentation & Reporting**:
  - Reports overview (highlighted with a red circle containing the number '1')
  - Where has the user/group access?
  - Who has access where?
  - File server
    - All 'Authenticated users' permissions
    - All 'Everyone' permissions
    - All users with direct access
    - Directories without administrative owners
    - Permission difference
    - Unresolved SIDs
    - Where have employees of a manager access (file server)?
    - Who has access through which permission groups?
  - Active Directory
    - Account Details
    - Inactive accounts
    - Local accounts
    - Manager-Employees
    - OU Members and group memberships
    - Users and groups (Kerberos, Last logon)
  - Exchange
    - Exchange mailbox permissions

1. Click "Start".
2. Click "Create new user or group".

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. A 'Create Accounts' dialog box is open, displaying a list of account templates. The 'User' template is highlighted with a red box and a red circle labeled '1'. The 'Select' button at the bottom right of the dialog is also highlighted with a red box and a red circle labeled '2'. The background interface includes a search bar, navigation tabs (Start, Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, Status), and a sidebar with sections like Permission Analysis, User Provisioning, and Security Monitoring.

ARM offers 4 standard templates. You can generate as many of your own templates as you wish. We recommend using customized templates as a foundation as this simplifies and speeds up the process.

1. Select a User template.
2. Click on "select".



1. Enter the required information.
2. Modify the OU if desired.
3. Set further LDAP attributes.



ARM Access Rights Manager

Create account within Active Directory

Create elements in the selected domain: 8man-demo.local.

**1** **Group memberships**

Accounts [Templates](#) [Paste](#) [Clear](#)

Name

The user will automatically become a member of the groups specified here.

You can either search for a group or select a group template.

**2** **Password options**

Initial password: 1n17141P455w0rd  Hide password

[Generate a new password](#) with a length of  characters

The user must change the password at next logon

The user cannot change his password

The password never expires

**3** **User activation**

Activate immediately  Activate on 4/4/2019 12:00 AM  Do not activate

Account expires on 6/2/2019 12:00 AM

Credentials: 8man-demo\sa-8man

Please add a comment

1. You can already define group memberships when creating the user.
2. Set password options.
3. With ARM, you can schedule the activation of the account and set an expiration date during the creation of a new account.

**Create account within Active Directory**

Create elements in the selected domain: 8man-demo.local.

^ Create mailbox (Exchange)

1 Enable mailbox

2

Mailbox type	Mailbox	▼
Mailbox Database	Mailbox Database 0349104094	▼
Archive Database	<input type="checkbox"/>	
Archive Database	Mailbox Database 0349104094	▼
ActiveSync	<input checked="" type="checkbox"/>	
ActiveSync Policy	Default	▼
Outlook Web App (OWA)	<input checked="" type="checkbox"/>	
Outlook Web App (OWA) Policy	Default	▼
IMAP	<input checked="" type="checkbox"/>	
POP3	<input checked="" type="checkbox"/>	
MAPI	<input checked="" type="checkbox"/>	

3 Credentials 8man-demo\sa-8man

4 Demo.

5 Close Immediately

**Immediately**  
Execute this task immediately and wait until the changes have been made.

**In background**  
Execute this task in the background (this overlay will close).

**Overnight**  
Execute this task at the end of this day (this overlay will close).

**Schedule...**  
Execute this task at a point in time of your choice.

**Save**  
Save this task. You can resume your work immediately and execute saved tasks at any given time.

1. Activate this option to create a mailbox for the new user. You can also perform this step later with ARM.
2. Determine the email settings.
3. Determine which credentials are used in order to create the new account in AD.
4. You must enter a comment.

**i** Security relevant events such as the creation of a user account should always be justified by the creator. This also serves for your own security. We recommend that you provide a ticket number and the person who instructed you to do so.


5. Complete the action immediately or later, or save the job and complete it later.

Create a user account in Azure Active Directory

## Background / Value

With ARM you can quickly create standardized user accounts. You can delegate the process to the Helpdesk and further simplify and standardize it using specifically customized templates for different company roles.

You can assign an Office 365 license and if Exchange Online is covered by this license, a mailbox for the new user is created automatically.

 Use this feature on managed Azure Active Directory domains only. For federated domains that are synced with an on-premise AD, you must create the user in the leading on-premise AD.

## Related features

Customize templates for account creation (please refer: [Customize ARM templates](#))

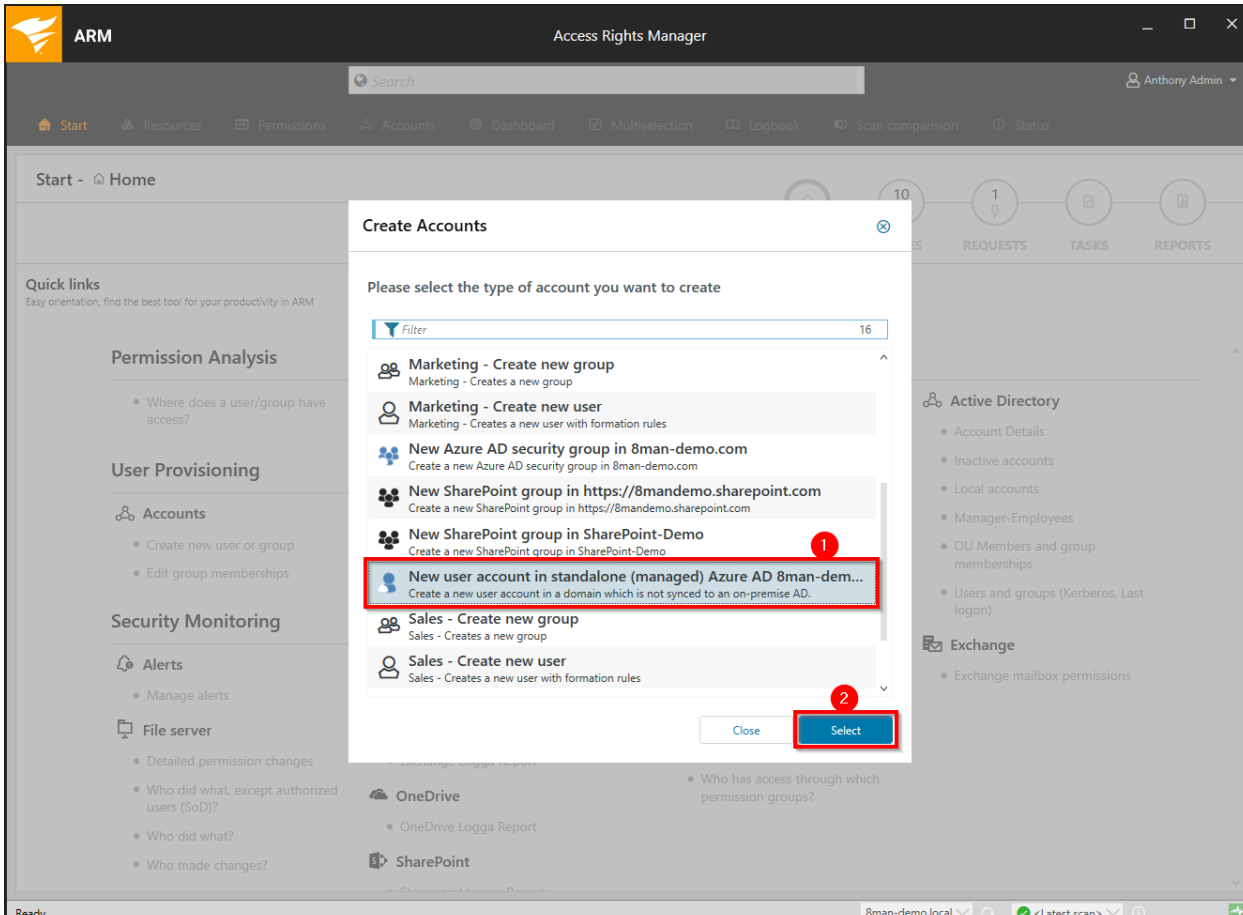
[Create a mailbox in Exchange Online](#)

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes a search bar, a user profile for 'Anthony Admin', and several tabs: Start, Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, and Status. The 'Start' tab is highlighted with a red box and a red circle containing the number '1'. Below the navigation bar, there are icons for HOME, NOTES, REQUESTS, TASKS, and REPORTS. The main content area is divided into several sections:

- Permission Analysis**
  - Where does a user/group have access?
- User Provisioning**
  - Accounts**
    - Create new user or group (highlighted with a red box and a red circle containing the number '2')
    - Edit group memberships
  - Resources**
    - Edit access rights
- Security Monitoring**
  - Alerts**
    - Manage alerts
  - File server**
    - Who did what, except authorized users (SoD)?
    - Who did what?
    - Who made changes?
  - Active Directory**
    - AD Logga Report
  - Exchange**
    - Exchange Logga Report
  - OneDrive**
    - OneDrive Logga Report
  - SharePoint**
- Documentation & Reporting**
  - Reports overview (highlighted with a red circle containing the number '1')
  - Where has the user/group access?
  - Who has access where?
  - File server**
    - All 'Authenticated users' permissions
    - All 'Everyone' permissions
    - All users with direct access
    - Directories without administrative owners
    - Permission difference
    - Unresolved SIDs
    - Where have employees of a manager access (file server)?
    - Who has access through which permission groups?
  - Active Directory**
    - Account Details
    - Inactive accounts
    - Local accounts
    - Manager-Employees
    - OU Members and group memberships
    - Users and groups (Kerberos, Last logon)
  - Exchange**
    - Exchange mailbox permissions

1. Click "Start".
2. Click "Create new user or group".



ARM offers 4 standard templates. If you add an Azure Active Directory (AAD) as a resource to ARM then you will find two templates for creating new users and groups in AAD.

**i** You can customize the Azure templates in the same way as for other resources. We recommend using customized templates as this simplifies and speeds up the process.

1. Select a New Azure AD User template.
2. Click Select.

### Create Accounts ⊗

New user account in standalone (managed) Azure AD 8man-demo.com (Create a new user account in a domain which is not synced to an on-premise AD.)  
Accounts will be created in 8man-demo.com.

**1**

Create a new user account in a managed domain which is not synced with an on-premise AD.

Given Name

Surname

DisplayName

UserPrincipalName

MailNickname  **2**

Usage Location  **2**


Exchange Online License  **2**


Account Enabled

Password  **3**

Force change password

Credentials [51ee871b-f9ca-47c2-b0b1-c898b9bd1be2](#)

Please add a comment 



1. Enter the required information. Please keep in mind, that you can customize the template, for example hide input fields, create or validate inputs. For more information please see the [customizing templates](#) section.
2. Select the location of the new user. This is mandatory and will be used for Office 365 billing purposes.
3. Select a license. If Exchange Online is included in the license, a new mailbox will be created.

### Create Accounts ✕

New user account in standalone (managed) Azure AD 8man-demo.com (Create a new user account in a domain which is not synced to an on-premise AD.)  
Accounts will be created in 8man-demo.com.

Create a new user account in a managed domain which is not synced with an on-premise AD.

Given Name	<input type="text" value="new"/>
Surname	<input type="text" value="user"/>
DisplayName	<input type="text" value="new user"/>
UserPrincipalName	<input type="text" value="new.user@8man-demo.com"/>
MailNickname	<input type="text" value="new.user"/>
Usage Location	<input type="text" value="GERMANY"/>
Exchange Online License	<input type="text" value="Office 365 Business Essentials"/>
Account Enabled	<input checked="" type="checkbox"/>
Password	<input type="text" value="P@ssw0rd"/>
Force change password	<input checked="" type="checkbox"/>

**1** Credentials `51ee871b-f9ca-47c2-b0b1-c898b9bd1be2`

**2** Demo

**3** Close Immediately ▶

1. Enter the credentials that will be used to create the new user account. Credentials can be stored in the [Azure AD change configuration](#).
2. You must enter a comment.
3. Start or schedule the process.

**⚠** If you see an error message that includes a request for an immutable ID then you are trying to add a new user to a federated domain. You can not use this feature to create a new user in a federated domain. In such cases create the new user in the leading on-premise AD.

Create groups and add users

## Background / Value

ARM allows you to create standardized groups quickly and easily. Each process is automatically documented.

## Related features

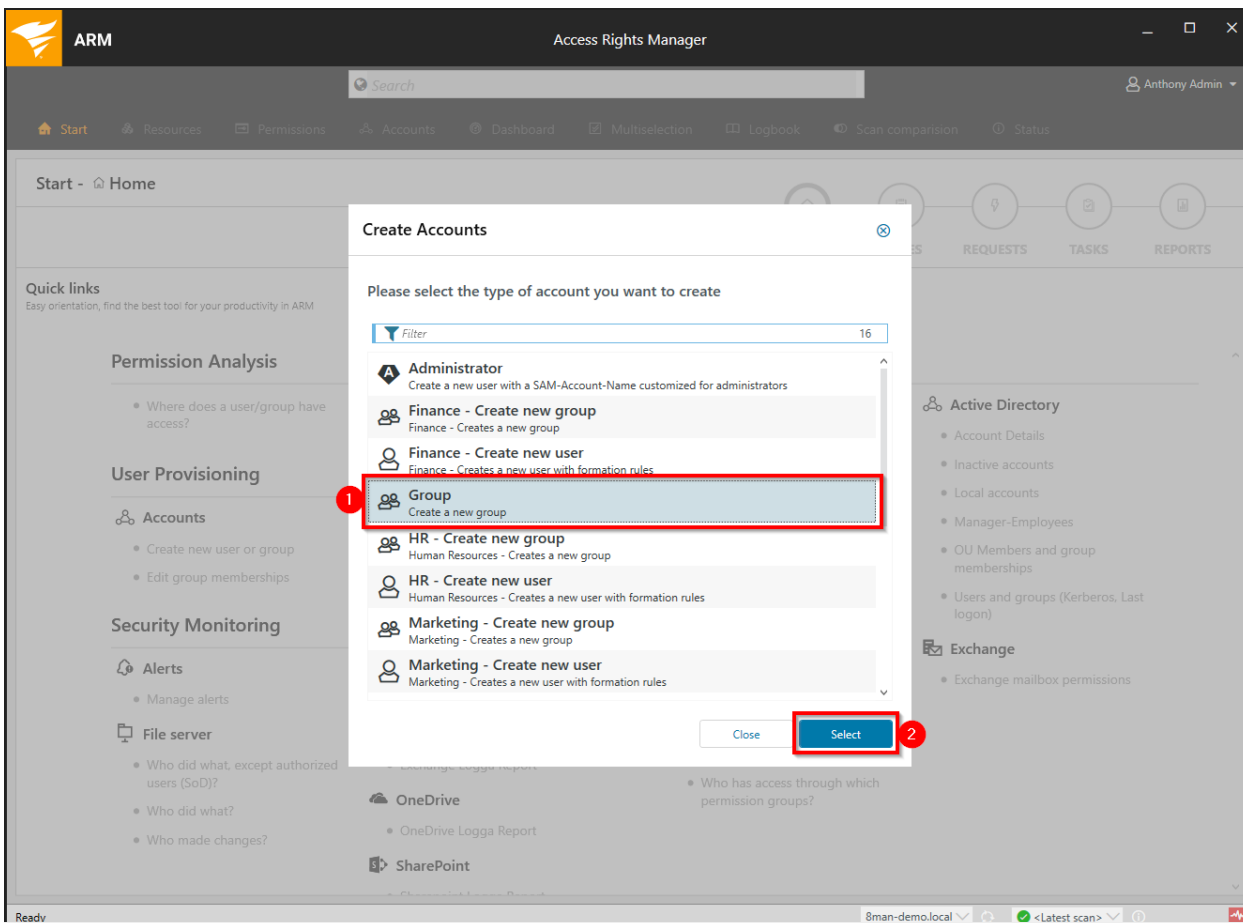
[Manage group memberships](#)

## Step-by-step process

The screenshot shows the Access Rights Manager (ARM) web interface. The top navigation bar includes a search bar, a settings gear, and the user name 'Anthony Admin'. Below the navigation bar, the 'Start' button is highlighted with a red box and a red circle containing the number '1'. The main content area is divided into several sections: 'Permission Analysis', 'User Provisioning', 'Security Monitoring', and 'Documentation & Reporting'. In the 'User Provisioning' section, the 'Accounts' sub-section is expanded, and the 'Create new user or group' option is highlighted with a red box and a red circle containing the number '2'. The 'Documentation & Reporting' section includes a 'Reports overview' link with a red circle containing the number '1'.

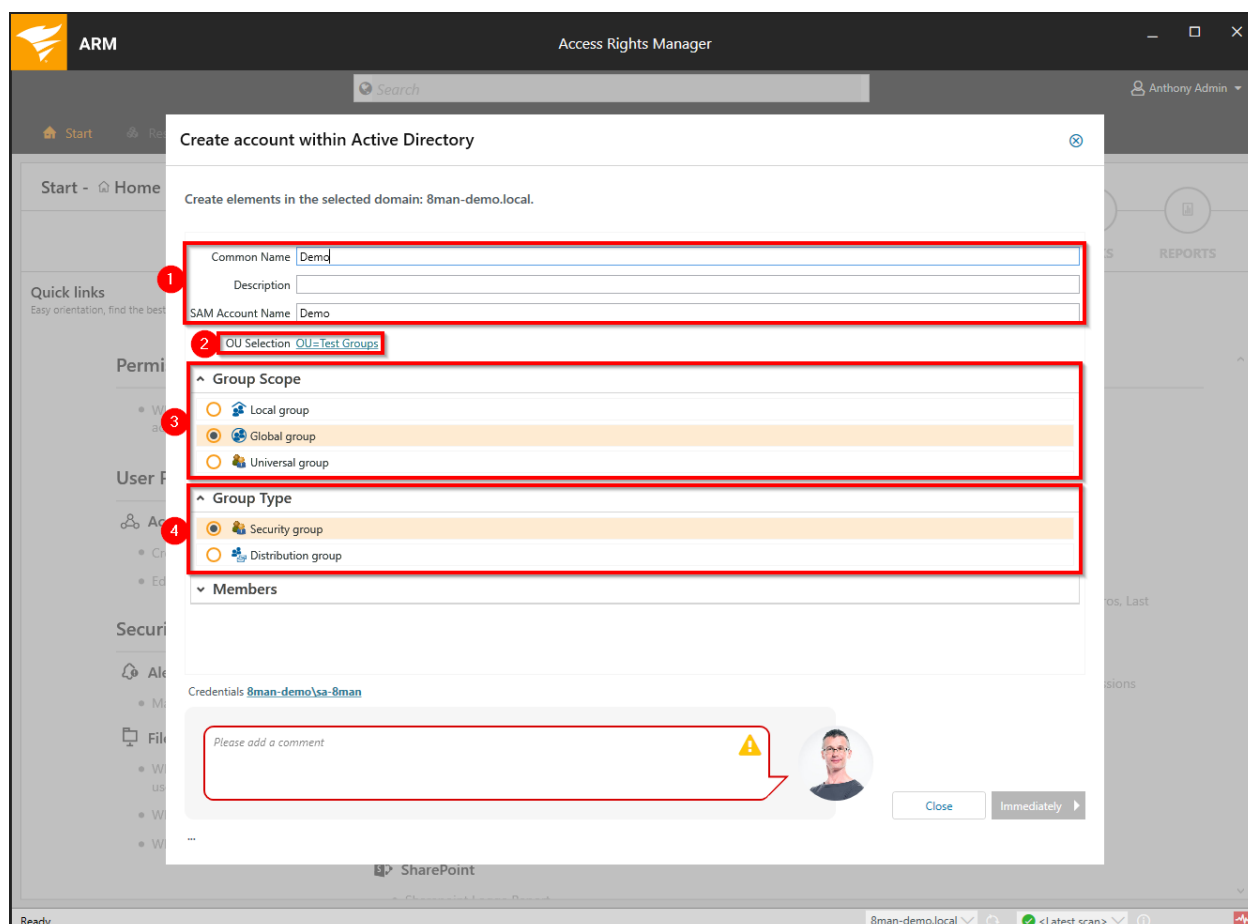
1. Select "Start".
2. Click on "Add a new user account or group".





ARM offers 4 standard templates. You can generate as many of your own templates as you wish. We recommend using customized templates as a foundation as this simplifies, standardizes and speeds up the process.

1. Select a group template.
2. Click on "Select".



1. Set the group names and description.
2. Change the OU if desired.
3. Determine the group scope.
4. Determine the group type.

ARM Access Rights Manager

Search Anthony Admin

### Create account within Active Directory

Create elements in the selected domain: 8man-demo.local.

Common Name: Demo

Description:

SAM Account Name: Demo

OU Selection: [OU=Test Groups](#)

Group Scope:

Group Type:

Members

Accounts:  [Paste](#) [Clear](#)

Name: Emily Employee (8man-demo\Emily Employee)

The accounts specified here will automatically become members of the new group.

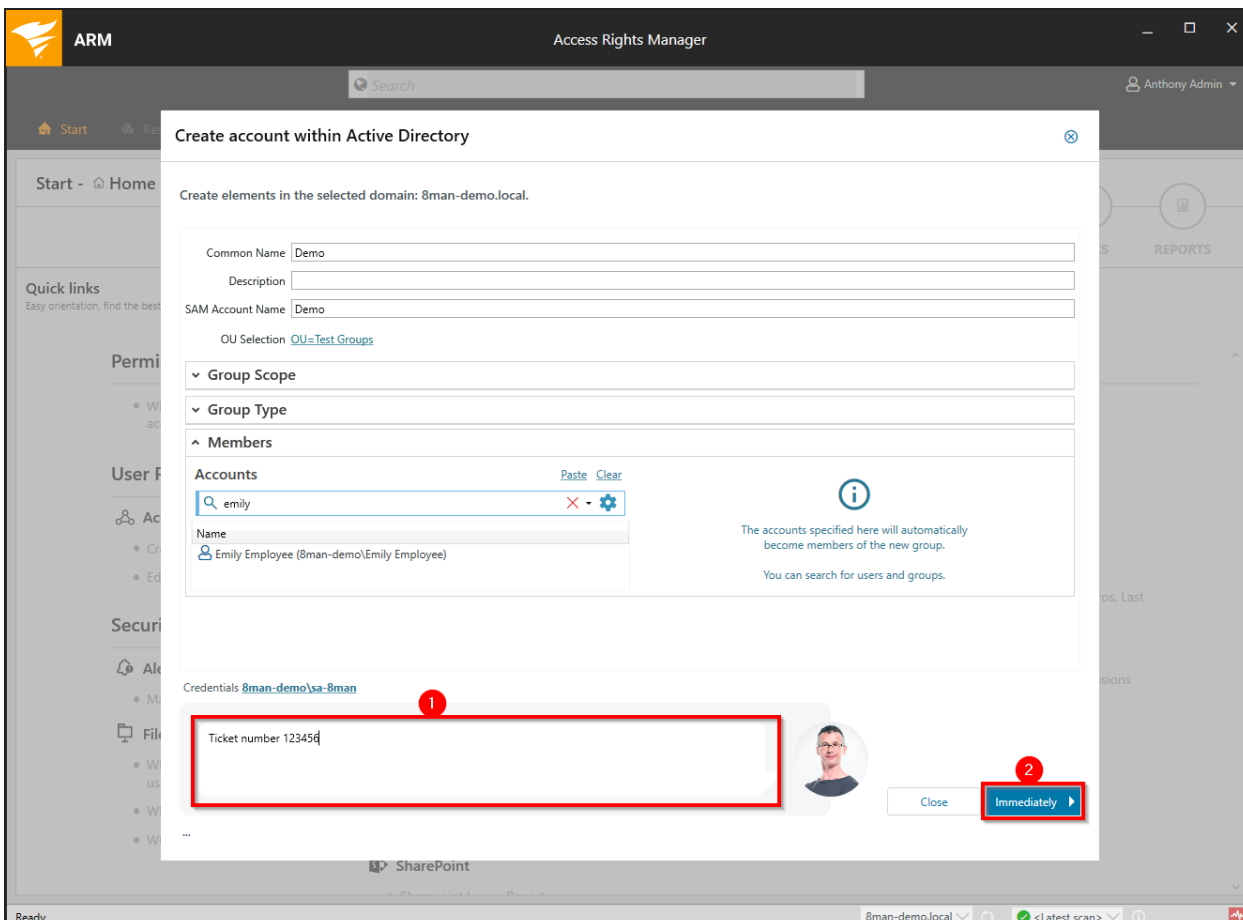
You can search for users and groups.

Credentials: **8man-demo\sa-8man**

Please add a comment

Close Immediately

1. You can add users while creating the group.
2. Determine the credentials for creating the new group in AD.



1. You must enter a comment.

**i** Sensitive administrative actions should always contain an explanation why the account is being created and/or what it is for. We recommend adding a ticket number and information who requested the account creation.

2. Complete the action immediately or later, or save it as a job.

## Manage group memberships

### Background / Value

ARM allows you to manage group memberships quickly and easily. You can also easily analyze group nesting.

### Related features

[Remove group memberships in bulk](#) (web client)

### Step-by-step process

The screenshot shows the ARM web client interface. The search bar at the top is highlighted with a red box and the number 2. The 'Accounts' tab in the navigation menu is highlighted with a red box and the number 1. The 'C-Level (8man-demo\C-Level)' account is highlighted with a red box and the number 3. The context menu is open over this account, and the 'Change group memberships...' option is highlighted with a red box and the number 4. The graph view shows a hierarchy of accounts, with '8man-demo complete (8man-demo\8man-demo complete)' at the top and three sub-accounts below it: 'David DO Finance (8man-demo\David DO Finance)', 'David DO HR (8man-demo\David DO HR)', and 'David DO Manager (8man-demo\David DO Manager)'. The right-hand pane shows a list of children for the selected account, including 'David DO Finance (8man-demo\David D...', 'David DO HR (8man-demo\David DO HR)', 'David DO Manager (8man-demo\David D...', 'David DO Marketing (8man-demo\Da...', 'David DO Sales (8man-demo\David DO S...', 'Henry HR (8man-demo\Henry HR)', and 'Sam Sales (8man-demo\Sam Sales)'. The status bar at the bottom shows 'Ready' and '8man-demo.local'.

1. Select "Accounts".
2. Use the search field to find the desired account.
3. Right-click on the account.
4. Select "Change group memberships..." in the context menu.

Alternatively you can also use "Edit group memberships" on the ARM home page.

The screenshot shows the 'Add / remove group memberships' dialog in the SolarWinds Access Rights Manager. The dialog is titled 'Add / remove group memberships' and is open over the 'C-Level (8man-demo\C-Level)' group. The dialog is divided into three main sections: 'Accounts', 'Is direct member of', and 'Has the following direct members'. The 'Accounts' section has a search bar containing 'ludvig'. The 'Is direct member of' section shows a list of groups, including 'Marketing (8man-demo\Marketing)'. The 'Has the following direct members' section shows a list of users, including 'Ludvig Karlsson (8man-demo\Ludvig Karlsson)'. A red box highlights the search bar (1). A red arrow points from the search bar to the 'Marketing (8man-demo\Marketing)' group in the 'Is direct member of' column (2). Another red arrow points from the 'Marketing' group to the 'Ludvig Karlsson (8man-demo\Ludvig Karlsson)' user in the 'Has the following direct members' column (3). At the bottom of the dialog, there is a comment field with the text 'Please add a comment' and a warning icon. There are also 'Close' and 'Immediately' buttons.

1. Use the search field to find the desired user or group.
2. Use drag & drop to move a group to the middle column. This creates a new group membership (parent).
3. Use drag & drop to move users and groups into the right column to add new group members (children).

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. A dialog box titled "Add / remove group memberships" is open, showing the configuration for the "C-Level (8man-demo\C-Level)" group. The dialog is divided into several sections:

- Accounts:** A search bar and a list of accounts. The list includes "Marketing (8man-demo\Marketing)" and "Ludvig Karlsson (8man-demo\Ludvig Karlsson)".
- Is direct member of:** A list of groups that are direct members of the selected group. It includes "8man-demo complete (8man-demo\8man...)" and "Marketing (8man-demo\Marketing)".
- Has the following direct members:** A list of users who are direct members of the selected group. It includes "David DO Finance (8man-demo\David DO...)", "David DO HR (8man-demo\David DO HR)", "David DO Manager (8man-demo\David D...)", "David DO Marketing (8man-demo\David D...)", "David DO Sales (8man-demo\David DO Sal...)", "Henry HR (8man-demo\Henry HR)", "Sam Sales (8man-demo\Sam Sales)", and "Ludvig Karlsson (8man-de...)".

A context menu is open over the "Ludvig Karlsson (8man-de..." entry in the "Has the following direct members" list. The menu options are:

- Select all (Ctrl+A)
- Copy (Ctrl+C)
- Remove (Del)
- Set expiration date

At the bottom of the dialog, there is a "Please add a comment" text box, a warning icon, a user profile picture, and "Close" and "Immediately" buttons.

Right-click and use the context menu to remove memberships (parents and children) immediately or on a designated date.

1. You must enter a comment.
2. Make changes immediately or save and schedule them for later.



## Delete empty groups

### Background / Value

Over time, empty groups accumulate in your Active Directory. These reduce performance and diminish transparency. We recommend deleting these groups.

**!** Groups without members could be system groups. These should not be deleted.

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The 'Dashboard' tab is selected in the top navigation bar. On the left, the 'Reporting' section is expanded to show 'Active Directory' and 'File server' categories. The main content area displays a list of groups and accounts. The 'Empty groups' entry is highlighted with a red box and a red '2' next to it, indicating it is the target for deletion. The 'Depth of nested groups' chart shows a bar for depth 1 with a value of 1536.

Category	Item	Count
Users and other accounts	Users	1165
	Users (disabled)	3
	Administrators	6
	Administrators (disabled)	0
Groups	All Groups	1648
	Groups with members (w/o recursions)	1549
	Empty groups	67
	Groups in recursions	32
	The largest group (Domain Users (Bman-demo\Domain Users))	1164
	Built-in security groups	29
	Global security groups	548
	Universal security groups	505
	Local security groups	553
	Global distribution groups	0
OU / Contacts / More	Computers	5
	Computers (disabled)	0
	Contacts	3
	Foreign users	0
	Organizational Units	43
Top 5 Kerberos Tokens [Bytes]	User96 (Bman-demo\User96)	3064
	User70 (Bman-demo\User70)	2944
	User2 (Bman-demo\User2)	2912
	User39 (Bman-demo\User39)	2904
	User38 (Bman-demo\User38)	2880
Top 5 Oldest logons		

1. Select "Dashboard".
2. Double-click on "Empty groups".



The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection' (highlighted with a red box and '1'), 'Logbook', 'Scan comparison', and 'Status'. The 'Multiselection' view shows a list of groups under the 'Empty groups' scenario (highlighted with a red box and '2'). The 'Production' group is selected (highlighted with a red box and '3'). A context menu is open over the 'Production' group, with 'Delete accounts' highlighted (highlighted with a red box and '4'). The right-hand pane shows 'Multiple elements' with a tree view containing 'Testing QA (8man-demo\Testing QA)' and 'Production (8man-demo\Production)'. The status bar at the bottom indicates 'Ready' and '8man-demo.local'.


1. ARM automatically switches to "Multiselection".
2. The scenario "Empty groups" is active. All listed groups are empty.
3. (Multi-) Select the groups that you know are safe to delete.
4. Right-click and select "Delete accounts" from the context menu.

### Delete accounts ⊗


...


Accounts to delete	Required credentials							
<table border="1"><thead><tr><th>Name</th></tr></thead><tbody><tr><td>Production (8man-demo\Production)</td></tr><tr><td>Testing QA (8man-demo\Testing QA)</td></tr></tbody></table>	Name	Production (8man-demo\Production)	Testing QA (8man-demo\Testing QA)	<table border="1"><thead><tr><th>Resource</th><th>Credentials</th></tr></thead><tbody><tr><td>8MAN-DEMO.LOCAL</td><td>8man-demo\sa-8man</td></tr></tbody></table>	Resource	Credentials	8MAN-DEMO.LOCAL	8man-demo\sa-8man
Name								
Production (8man-demo\Production)								
Testing QA (8man-demo\Testing QA)								
Resource	Credentials							
8MAN-DEMO.LOCAL	8man-demo\sa-8man							

 Remove groups which still have members  
 Deleting groups which are not empty may cause users to lose access rights where those groups are used. Please make sure that you really want to delete those groups.

 Remove access rights  
Remove all direct references to the selected accounts on resources which are known to ARM.  
The execution will be immediately

▼ Scripting

Please add a comment 




Close Immediately ▶


1. Optional: Change the login used to delete the groups in the AD.
2. Recommended: Activate the option "Remove access rights" and prevent the occurrence of unresolved SIDs.


### Delete accounts ⊗

...

Accounts to delete	Required credentials	
Name	Resource	Credentials

 Remove groups which still have members

 Deleting groups which are not empty may cause users to lose access rights where those groups are used. Please make sure that you really want to delete those groups.


 Remove access rights


Remove all direct references to the selected accounts on resources which are known to ARM.  
The execution will be [immediately](#) **1**

^ Scripting

Execute script before change action

None ▾

Please add a comment  **2**



Close **3** Immediately ▶

1. Choose whether to run a script before deleting. See also: [Configure scripts](#)
2. You must enter a comment.
3. Start the deletion process.

## Move objects in Active Directory

### Background / Value

ARM is able to move objects, meaning user accounts, group accounts and computers from one OU into another. This may be required if one of your users moves location or new group policies are applicable. ARM fully documents all movement among OUs.

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The search field at the top is highlighted with a red box and a '1'. The 'Emily Employee' object is highlighted with a red box and a '2'. The context menu is open, and the 'Move object' option is highlighted with a red box and a '3'.

The interface displays a graph view of Active Directory objects. The search field at the top is labeled 'Search' and has a red box around it with the number '1'. The 'Emily Employee' object is highlighted with a red box and the number '2'. The context menu is open, and the 'Move object' option is highlighted with a red box and the number '3'.

The graph shows two parent objects: 'All employees (8man-demo)\All employees' (31) and 'Domain Users (8man-demo)\Domain Users' (1168). The 'Emily Employee' object is connected to both parents. The context menu for 'Emily Employee' includes options like 'Select account', 'Show in Resources View...', 'Show access rights to resources...', 'Report: Where has the user/group access?', 'Report: Account Details', 'Change group memberships...', 'Create new user or group', 'Unlock user', 'Deactivate account', 'Change password options', 'Reset user password', 'Soft delete user account', 'Delete account', 'Edit attributes', 'Move object', 'Enable mailbox', 'Add note', 'Open Logbook', 'Create alert', and 'Copy as path'.

The 'Attributes' tab for 'Emily Employee' shows the following details:

Name	Value
Account Expires	Account never expires
Common Name	Emily Employee
Distinguished Name	CN=Emily Employee,OU=Demo...
Display Name	Emily Employee
Given Name	Emily
Last Logon	Never logged on
User Manager	CN=David DO Marketing,OU=D...
Email Address	E.Employee@8man-demo.local
Home Phone (RDN)	Emily Employee
Object GUID	6dc74776-ead9-421c-b9ae-1bc2...
Object SID	S-1-5-21-608986840-321788923...
Primary Group Id	513
Account Name	Emily Employee
Account Type	(805306368) User Object
Account Name	Employee
Phone Number	0049 302 364 1834
Account Co...	66048 / 0x10200
Account Co...	This is a default account type th...
Account Co...	The password for this account wi...
Principal Na...	Emily.Employee@8man-demo.lo...
Organizational U...	OU=Demo Users,DC=8man-de...
Organizational U...	Demo Users

The 'Properties' tab for 'Emily Employee' shows the following details:

Ort (l)	Berlin-Tiergarten
ZIP	10555
Street	Alt-Moabit 85

1. Use the search field to find the desired object.
2. Right-click on the object. You can do this in the "Accounts" view as well as in the "Resources" view.
3. Select "Move object".

### Move objects ⊗


...

Credentials **8man-demo\sa-8man** **1**



**Objects to move**

Name	Current path
Emily Employee (8man-demo\Emily Employee)	CN=Emily Employee,OU=Demo Users,DC=8man-demo,DC=local

**Please choose the target path**

 Please select **target path** **2**

▼ Scripting

Please add a comment  **3** 

**4** Close Immediately ▶

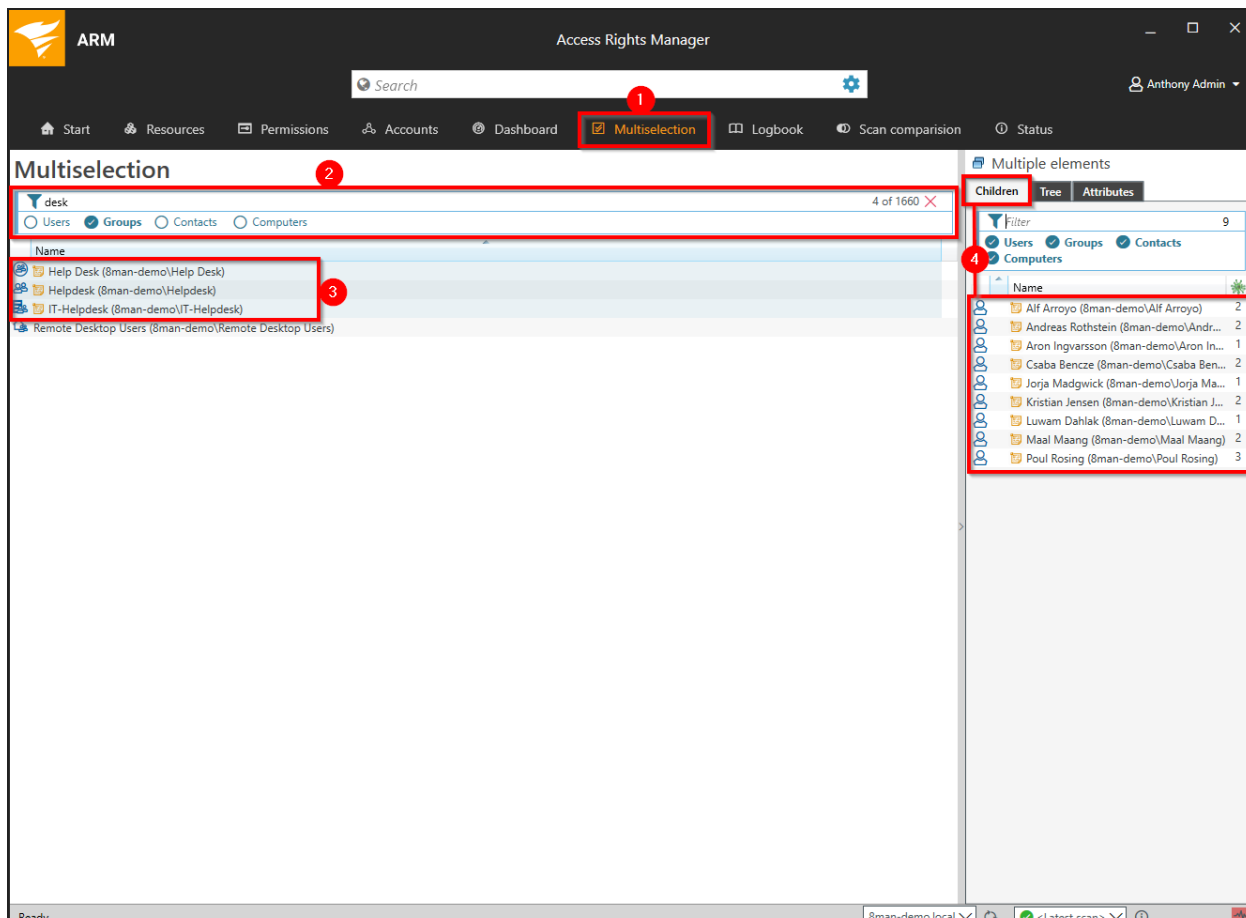
1. If required change the credentials which will be used to move the object.
2. Select a destination.
3. You must enter a comment.
4. Start the process.

Reduce multiple groups to one group

## Background / Value

On organized AD should have a limited number of groups. ARM allows you to easily combine historically accumulated and unnecessary groups. The following example shows the creation of a central help desk group. ARM allows you to simply copy all of the desired members and then combine them into one group.

## Step-by-step process



1. Select "Multiselection".
2. Apply filters to find the desired groups.
3. Select the groups.
4. Select all desired users and copy them into the clipboard. (For example CTRL+A and CTRL+C).

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The main window is titled "Multiselection" and displays a search bar with "desk" and "4 of 1660" results. Below the search bar, there are radio buttons for "Users", "Groups", "Contacts", and "Computers", with "Groups" selected. A list of resources is shown, including "Help Desk (8man-demo\Help Desk)", "Helpdesk (8man-demo\Helpdesk)", "IT-Helpdesk (8man-demo\IT-Helpdesk)", and "Remote Desktop Users (8man-demo\Remote Desktop Users)". A context menu is open over the list, with the option "Create new user or group" highlighted in a red box. Other options in the menu include "Select all", "Copy", "Show in accounts view...", "Show access rights to resources...", "Report: Where has the user/group access?", "Report: Account Details", "Change group memberships...", "Delete accounts", "Edit attributes", "Move objects", "Create Purpose Group", "Open Logbook", "Create alert", and "Copy as path". On the right side, the "Multiple elements" panel is visible, showing a list of users and groups with their names and counts.

Name	Count
Alf Arroyo (8man-demo\Alf Arroyo)	2
Andreas Rothstein (8man-demo\Andr...	2
Aron Ingvarsson (8man-demo\Aron In...	1
Csaba Benczce (8man-demo\Csaba Ben...	2
Jorja Madgwick (8man-demo\Jorja Ma...	1
Kristian Jensen (8man-demo\Kristian J...	2
Luwam Dahlak (8man-demo\Luwam D...	1
Maal Maang (8man-demo\Maal Maang)	2
Poul Rosing (8man-demo\Poul Rosing)	3

Right-click and select "Create new user or group".



ARM Access Rights Manager

Search Anthony Admin

### Create account within Active Directory

Create elements in the selected domain: 8man-demo.local.

Common Name: Central Help Desk

Description:

SAM Account Name: Central Help Desk

OU Selection: OU=Test Groups

Group Scope:

Group Type:

Members:

Accounts:

Paste Clear

Name:

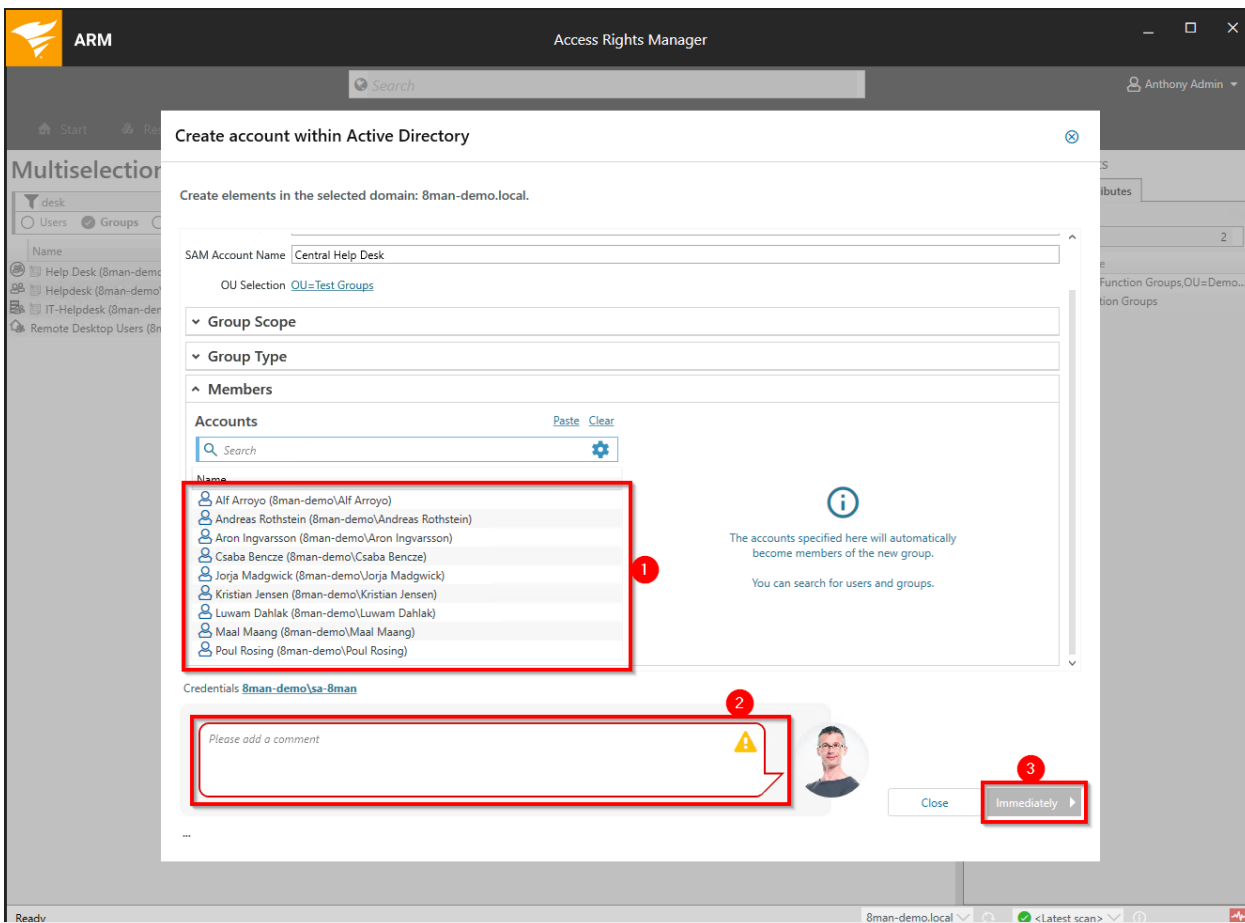
The accounts specified here will automatically become members of the new group. You can search for users and groups.

Credentials: 8man-demo\sa-8man

Please add a comment

Close Immediately

1. Name the new group.
2. In the "Members" section click on "Paste".



1. All members of the previously selected groups are now in the new group "Central Help Desk".
2. You must enter a comment.
3. Start the execution.

## Change password options

### Background/Value

Passwords should be changed regularly. Set the required password options.

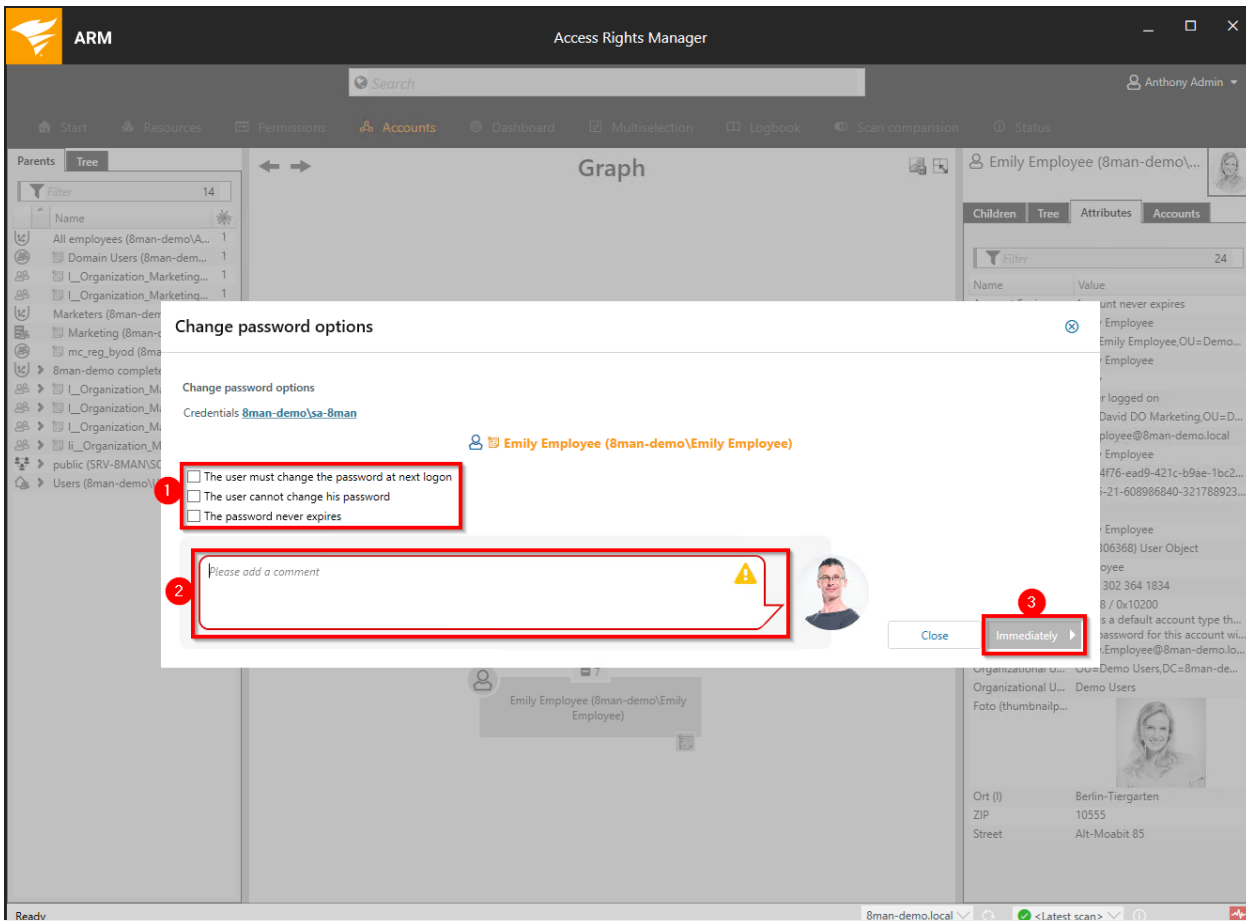
### Related features

[Change password options in bulk](#) (web client)

### Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) web client interface. The search bar at the top is highlighted with a red box and the number '1'. The 'Accounts' tab is selected in the navigation menu. The main area displays a 'Graph' view with two nodes: 'All employees (8man-demo)\All employees' and 'Domain Users (8man-demo)\Domain Users'. A red box with the number '2' highlights the 'Emily Employee (8man-demo)\Emily Employee' node. A context menu is open over this node, with a red box and the number '3' highlighting the 'Change password options' option. The right sidebar shows the user's profile information, including name, email, and address.

1. Find the desired user with the search.
2. Right-click on the user, e.g. in the Accounts view.
3. Select "Change password options" from the context menu.



1. Set password options.
2. You must enter a comment.
3. Start the execution.

Deactivate user accounts in bulk (web client)

## Background / Value

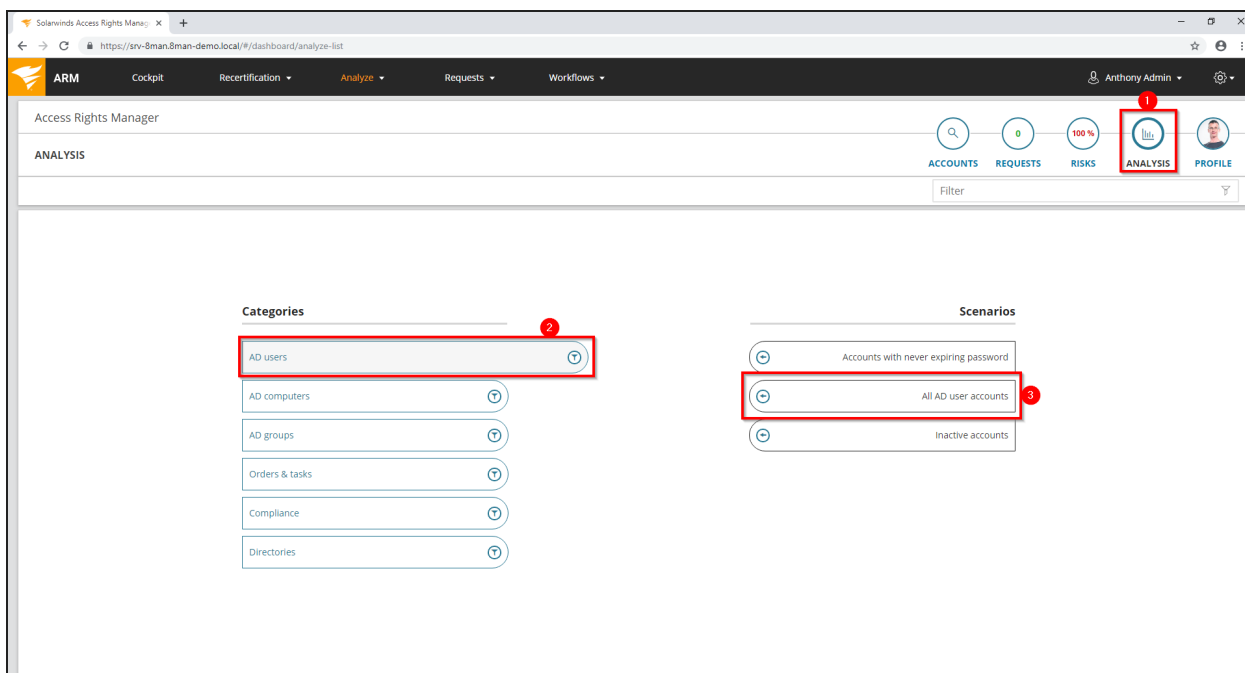
After a security breach it often makes sense to deactivate accounts in bulk. You can do this quickly and easily in the web interface.

## Additional Information

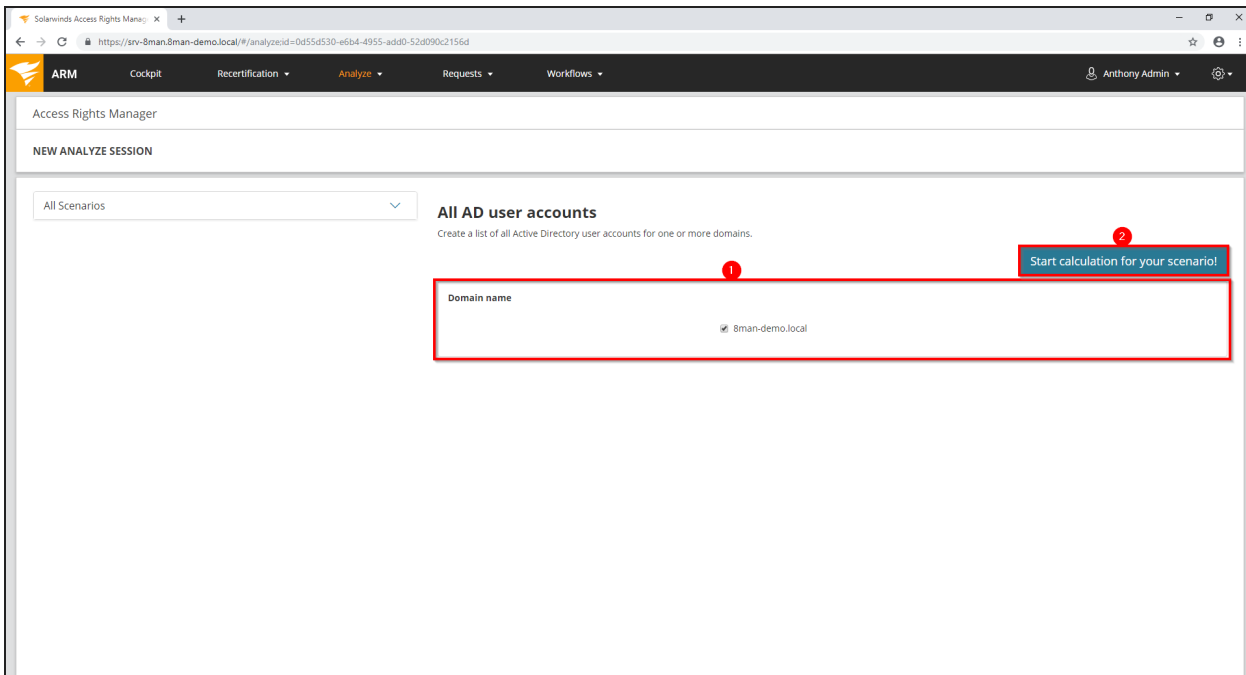
[Change password options in bulk](#) (web client)

[Delete accounts in bulk \(soft delete\)](#) (web client)

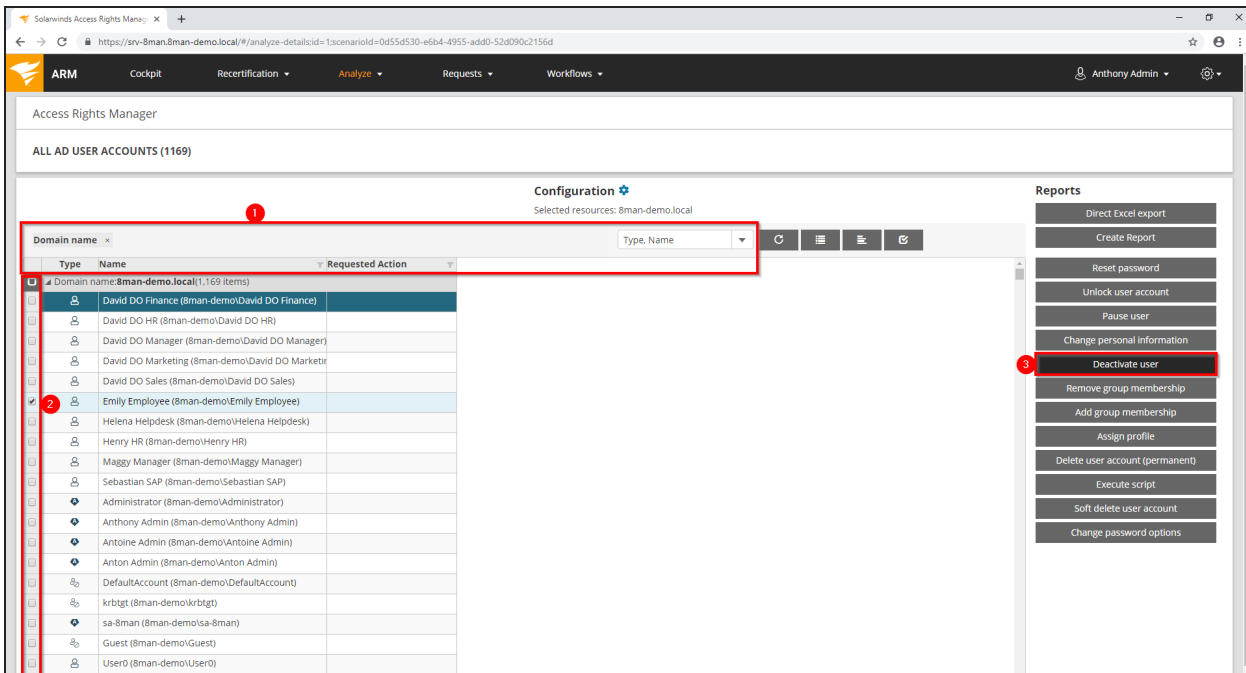
## Step-by-step process



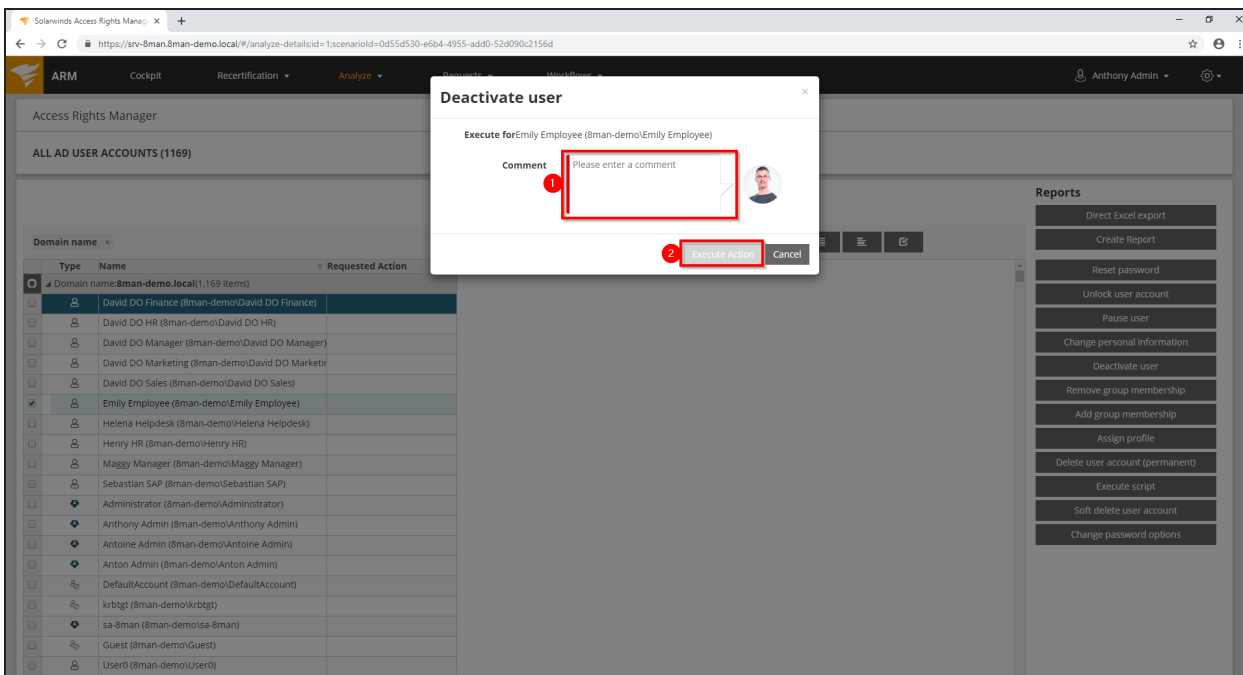
1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".



1. Set options for the scenario.
2. Click on "Start calculation".



1. Use sorting, filtering, grouping and column selection to narrow down your selection.
2. Select the desired entries.
3. Click "Deactivate user".



1. You must enter a comment.
2. Click on "Execute action".

The job will be transferred to the ARM server and executed there. ARM administrators can see the status in the task overview scenario.

Delete accounts in bulk (soft delete) (web client)

## Background / Value

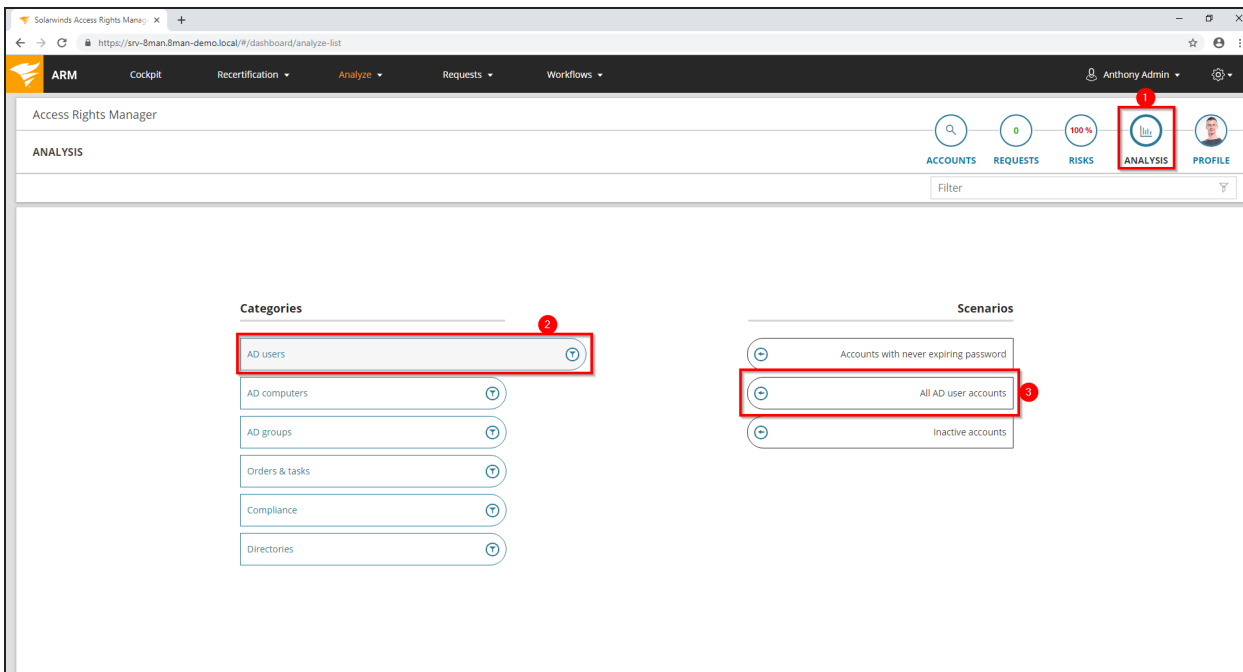
After a security breach or the dissolution of a department, it makes sense to delete several accounts at the same time. Do this conveniently in the web client.

## Related features

[Change password options in bulk](#) (web client)

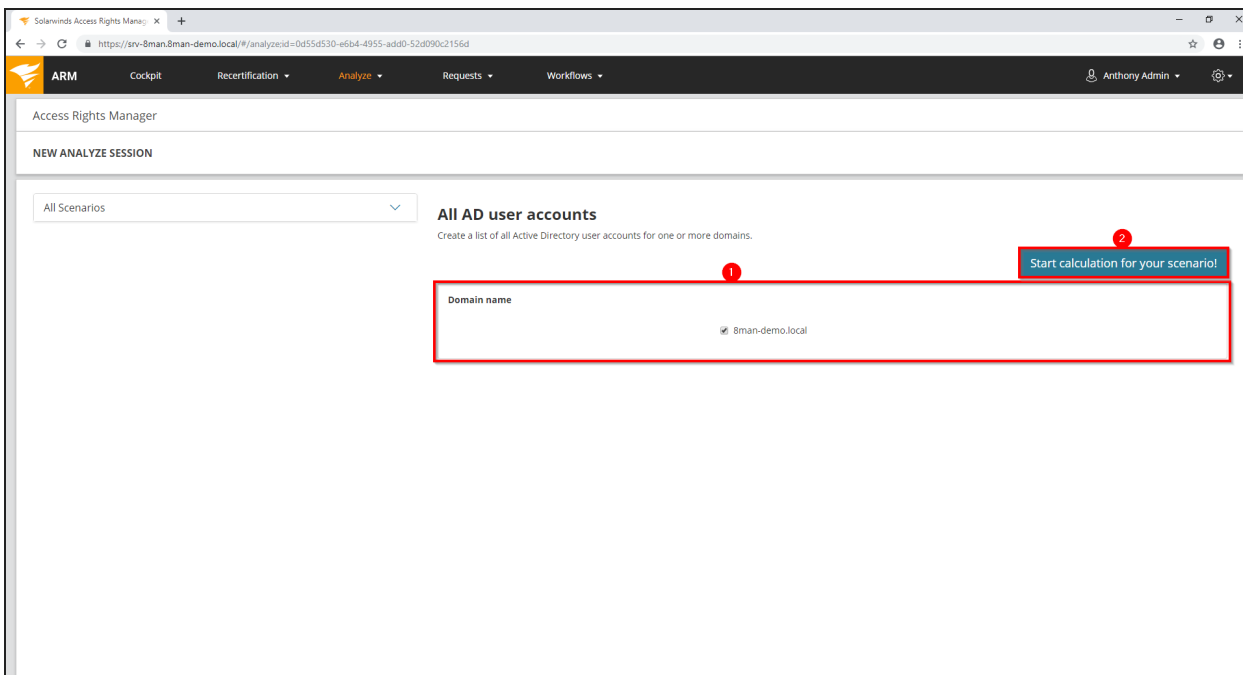
[Delete accounts in bulk \(soft delete\)](#) (web client)

## Step-by-step process

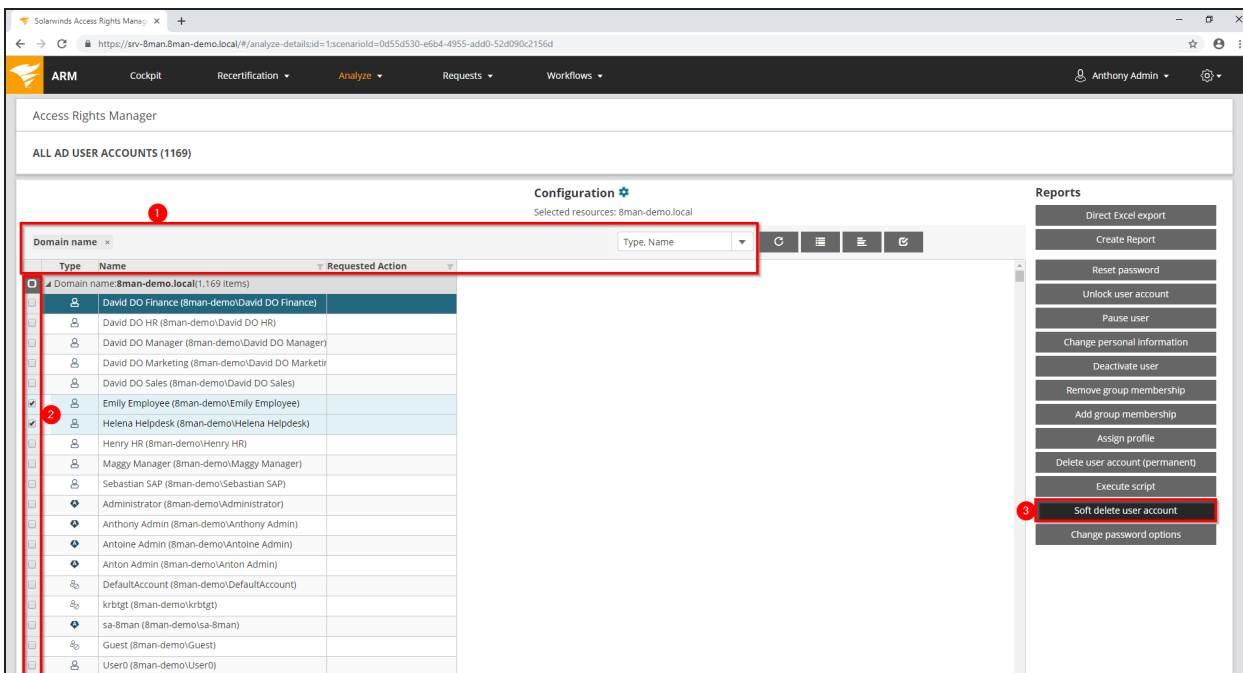


1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".

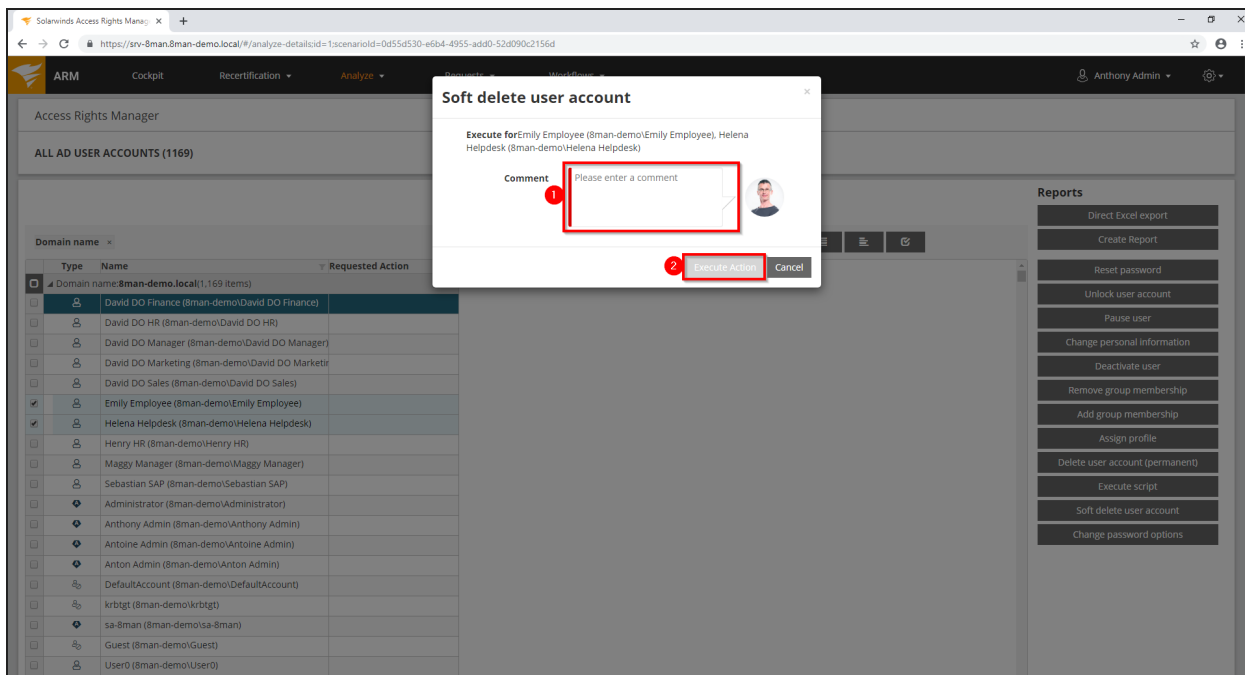




1. Set options for the scenario.
2. Click on "Start calculation".



1. Use sorting, filtering, grouping and column selection to narrow down your selection.
2. Select the desired entries.
3. Click "Soft delete user account".



1. You must enter a comment.
2. Click "Execute Action".

The job will be transferred to the ARM server and executed there. ARM administrators can see the status in the task overview scenario.

## Change password options in bulk (web client)

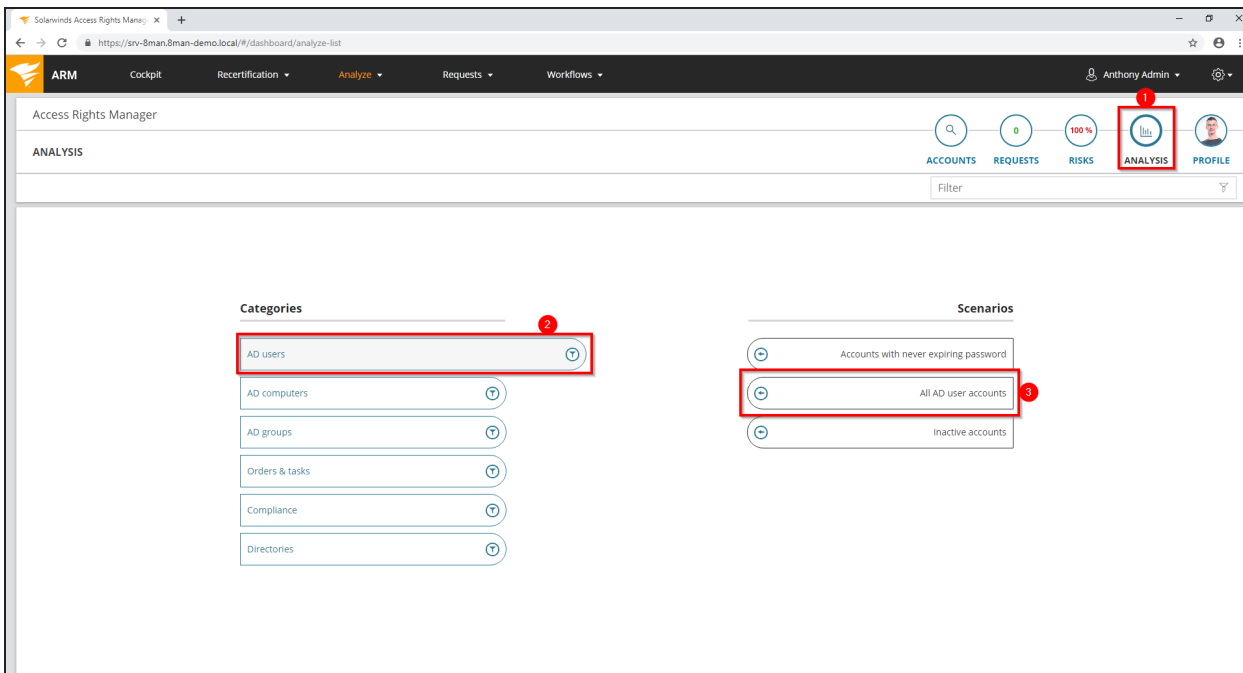
### Background / Value

Passwords must be changed regularly. You can manage password options across your entire organization, quickly and easily in the ARM web interface.

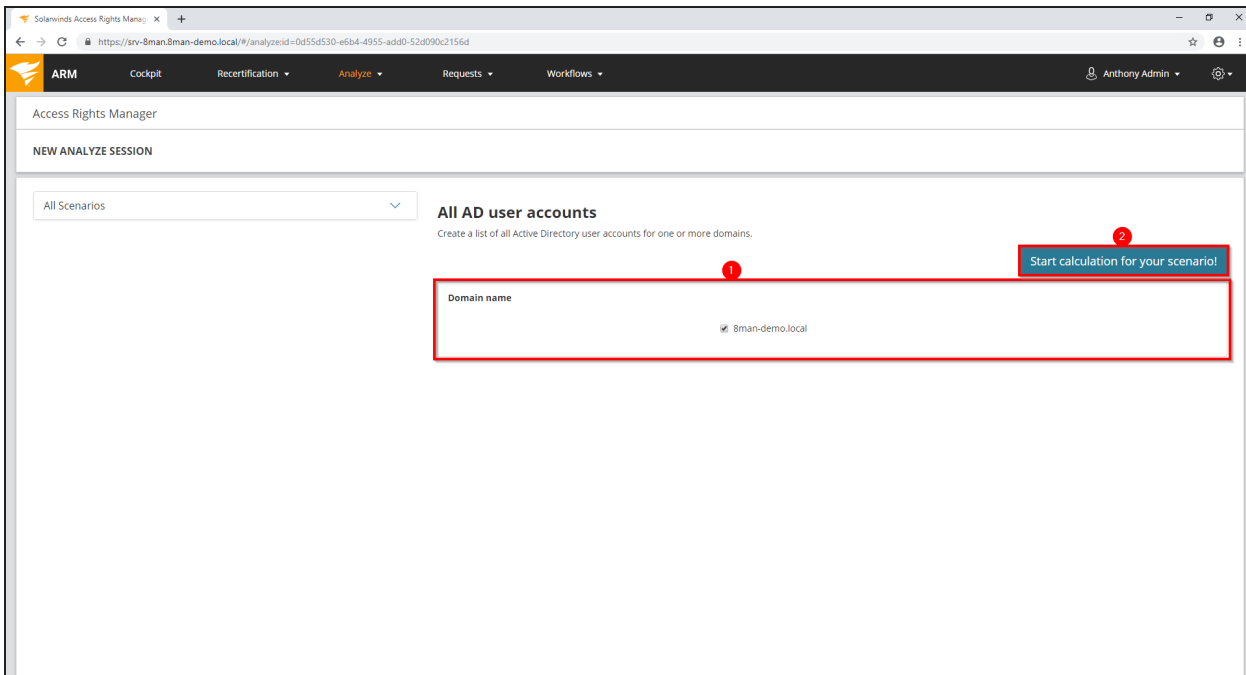
### Related features

[Reset passwords in bulk](#) (web client)

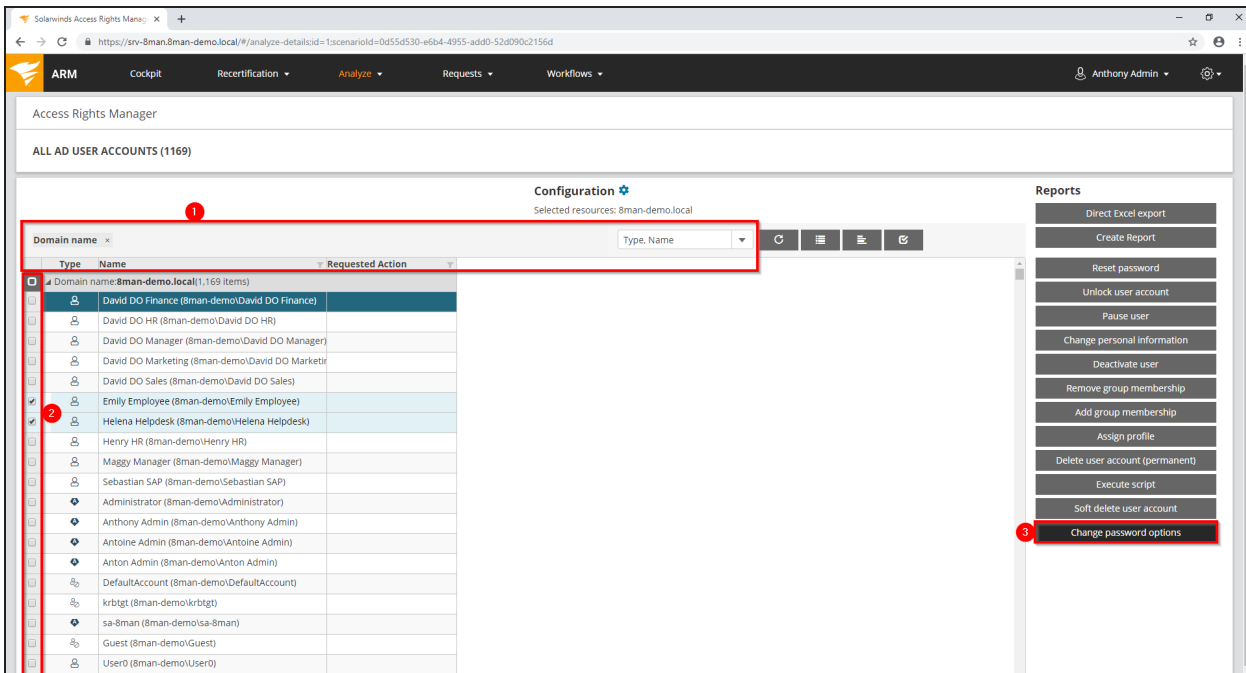
### Step-by-step process



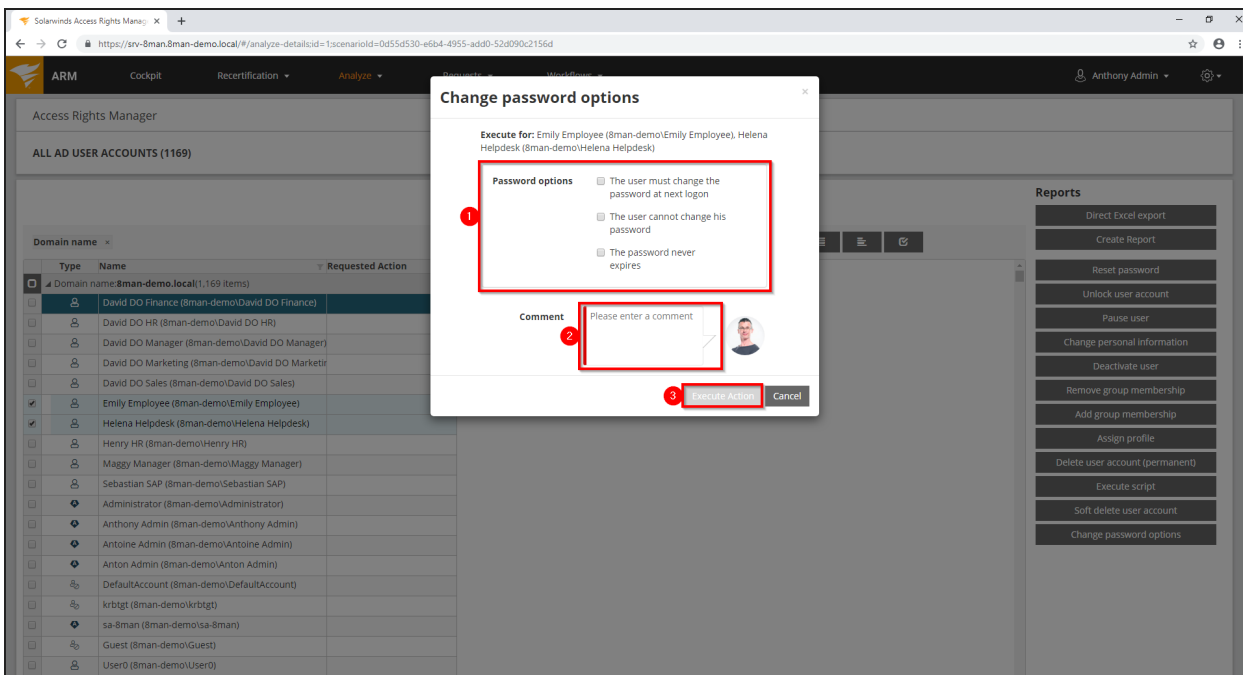
1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".



1. Set options for the scenario.
2. Click on "Start calculation".



1. Use sorting, filtering, grouping and column selection to narrow down your selection.
2. Select the desired entries.
3. Click "Change password options".



1. Set the password options.
2. You must enter a comment.
3. Click "Execute Action".

The job will be transferred to the ARM server and executed there. ARM administrators can see the status in the task overview scenario.

Modify attributes in bulk (web client)

## Background / Value

With ARM you can change AD attributes in bulk. This is can be relevant during reorganizations such as a merger and / or address change.

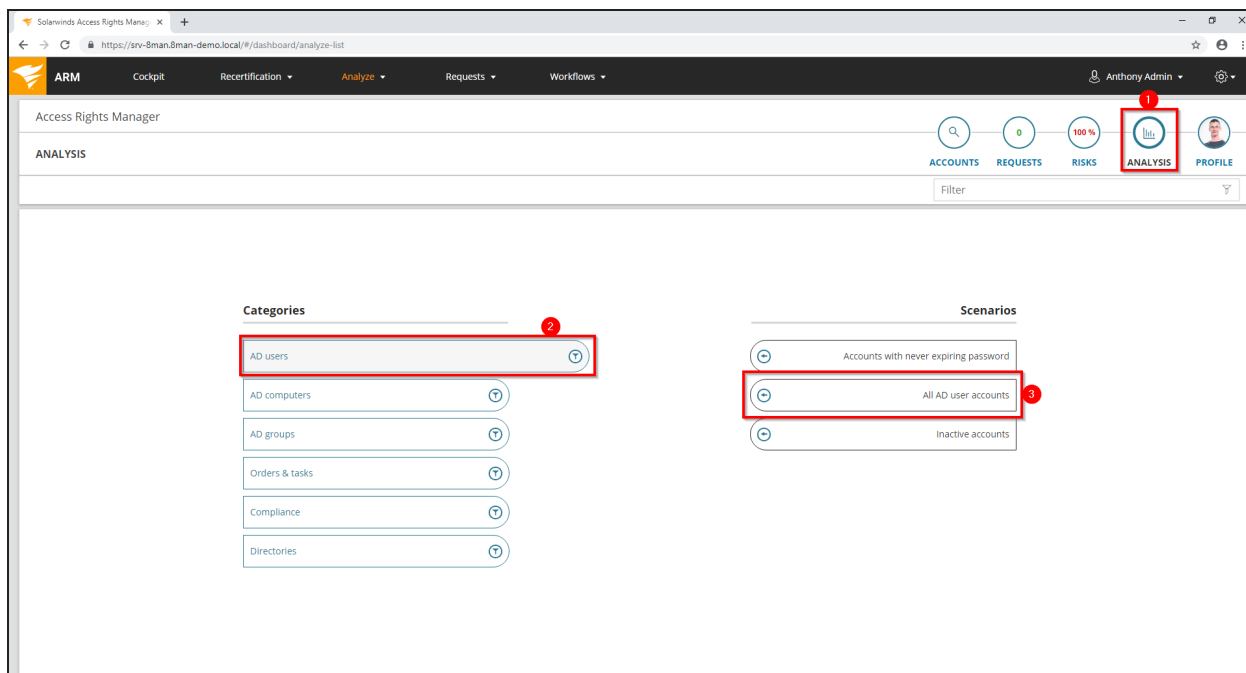
ARM provides a standard set of modifiable attributes. For each ARM role, you can specify which attributes are displayed and can therefore be changed. Please refer to the chapter: [Set attributes available to web client scenarios](#).

## Related features

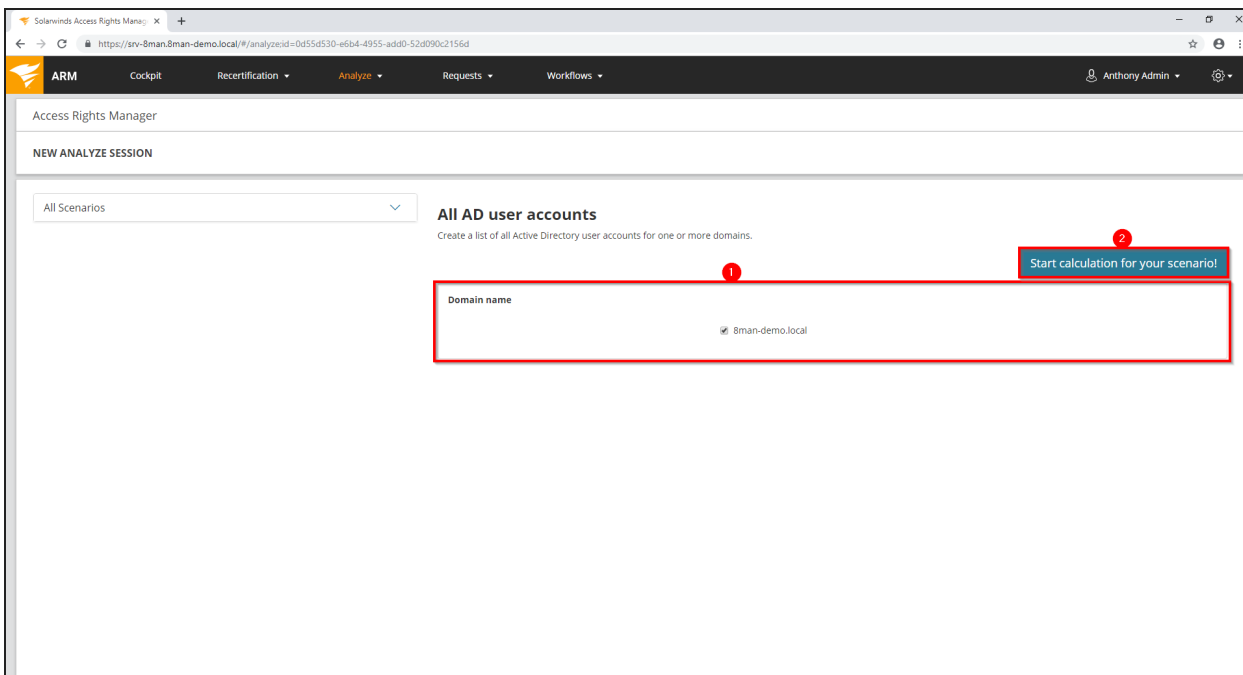
[Change password options in bulk](#) (web client)

[Reset passwords in bulk](#) (web client)

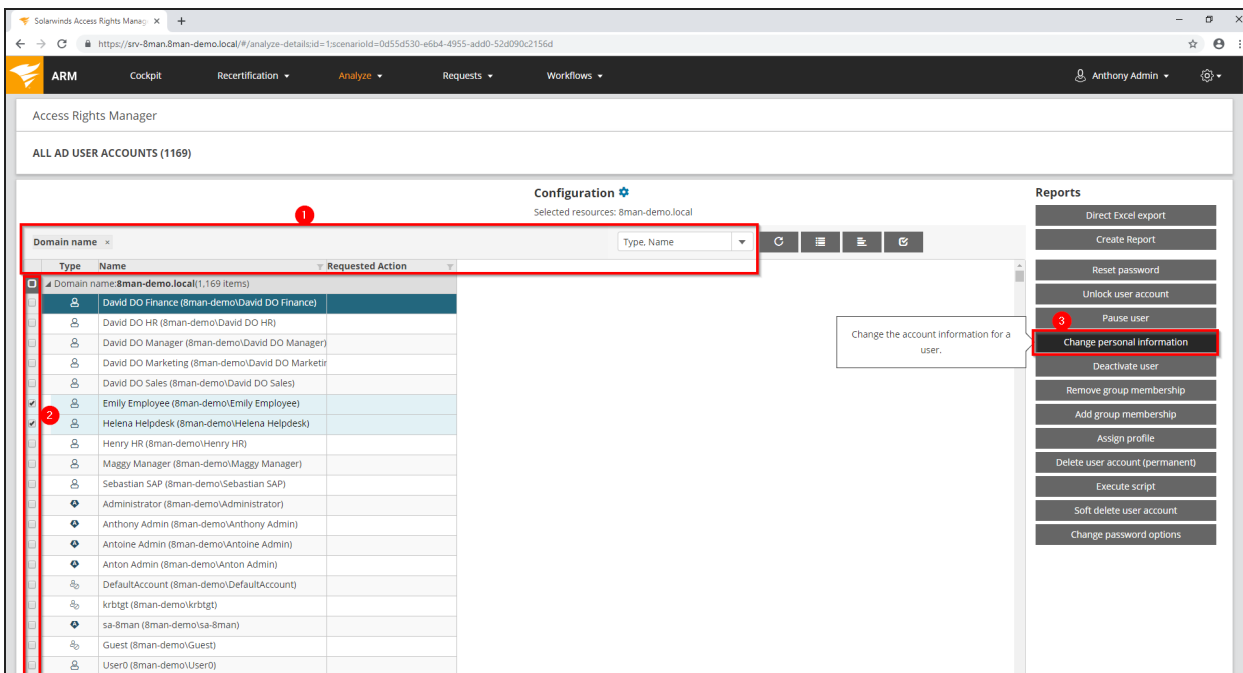
## Step-by-step process



1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".



1. Set options for the scenario.
2. Click on "Start calculation".



1. Use sorting, filtering, grouping and column selection to narrow down your selection.
2. Select the desired entries.
3. Click "Change personal information".

1. Activate the attributes that are to be changed and enter the values.

**i** If you activate an input field and do not specify a value, the content of the attribute is deleted.

2. You must enter a comment.

3. Click "Execute Action".

The job is transferred to the ARM server and executed there. ARM administrators can see the status in the task overview scenario.

**i** To set the available attributes in the dialog please refer to: [Set attributes available to web client scenarios](#)



## Remove group memberships in bulk (web client)

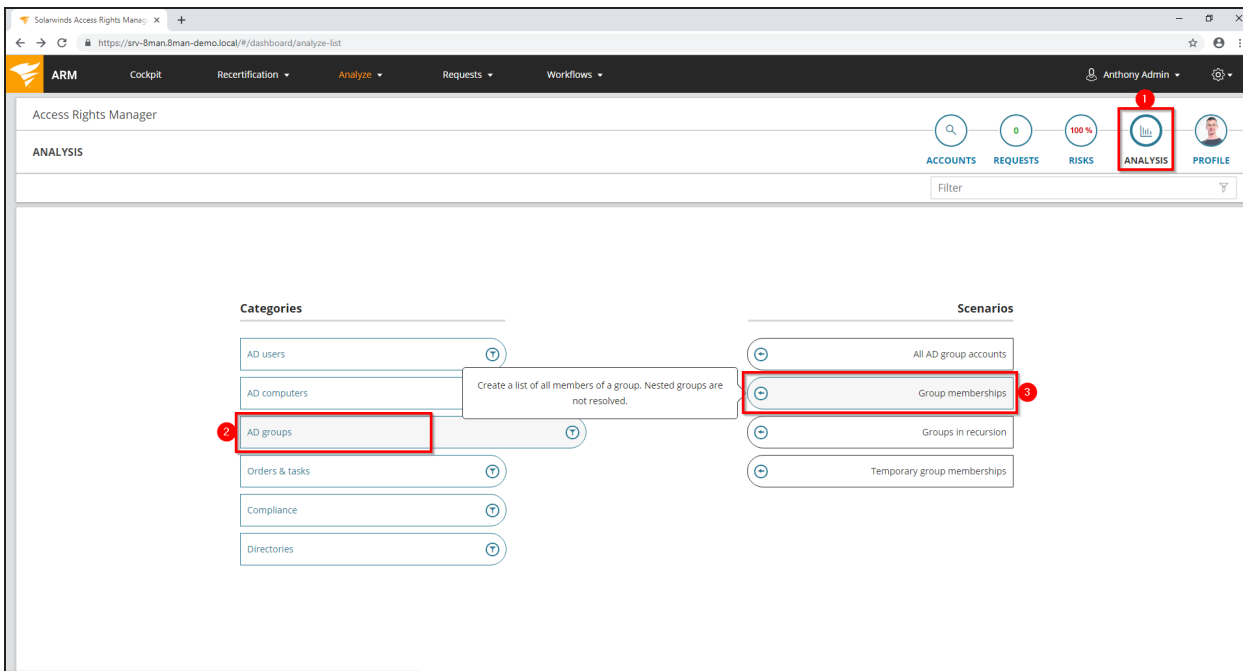
### Background / Value

Remove lots of group memberships fast using the web client.

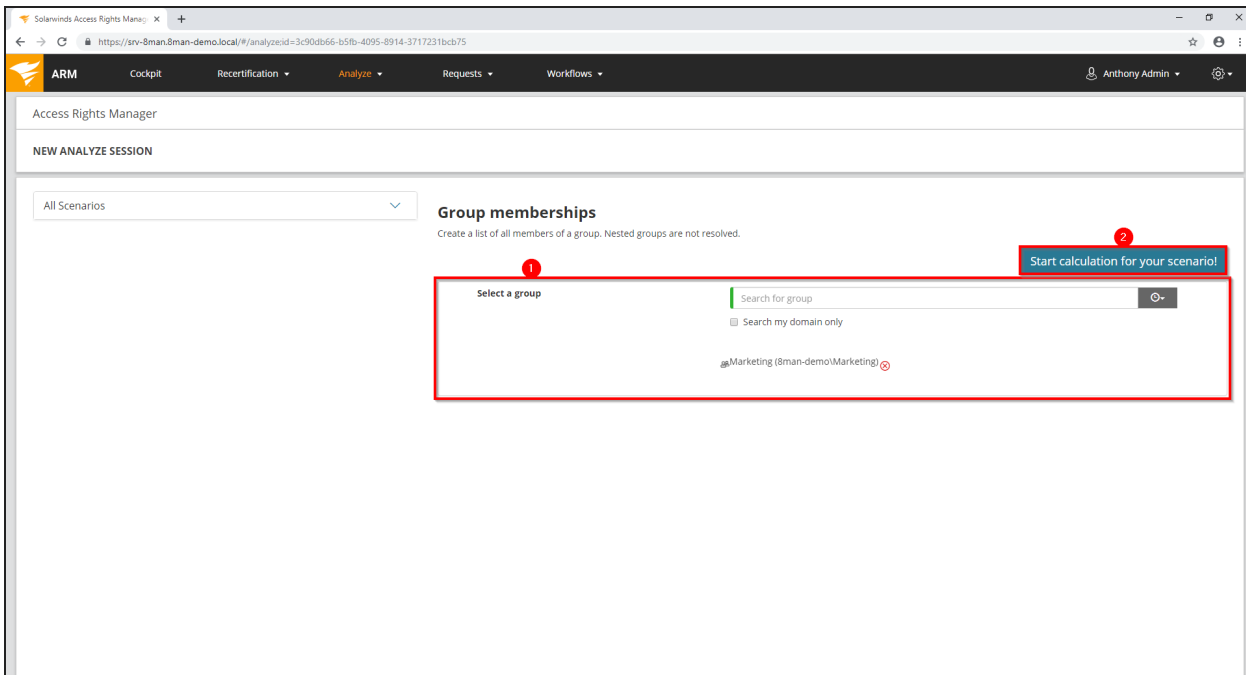
### Related features

[Manage group memberships](#) (rich client)

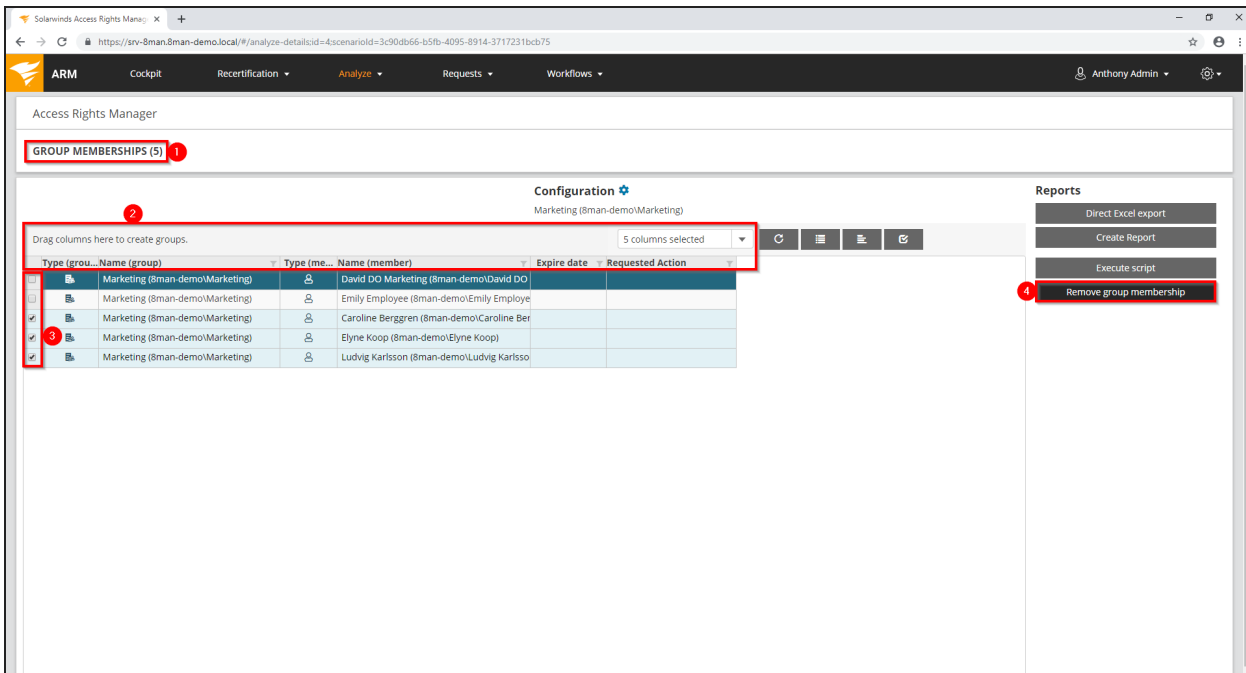
### Step-by-step process



1. Click "Analysis".
2. Select the category "AD groups".
3. Click on "Group memberships".

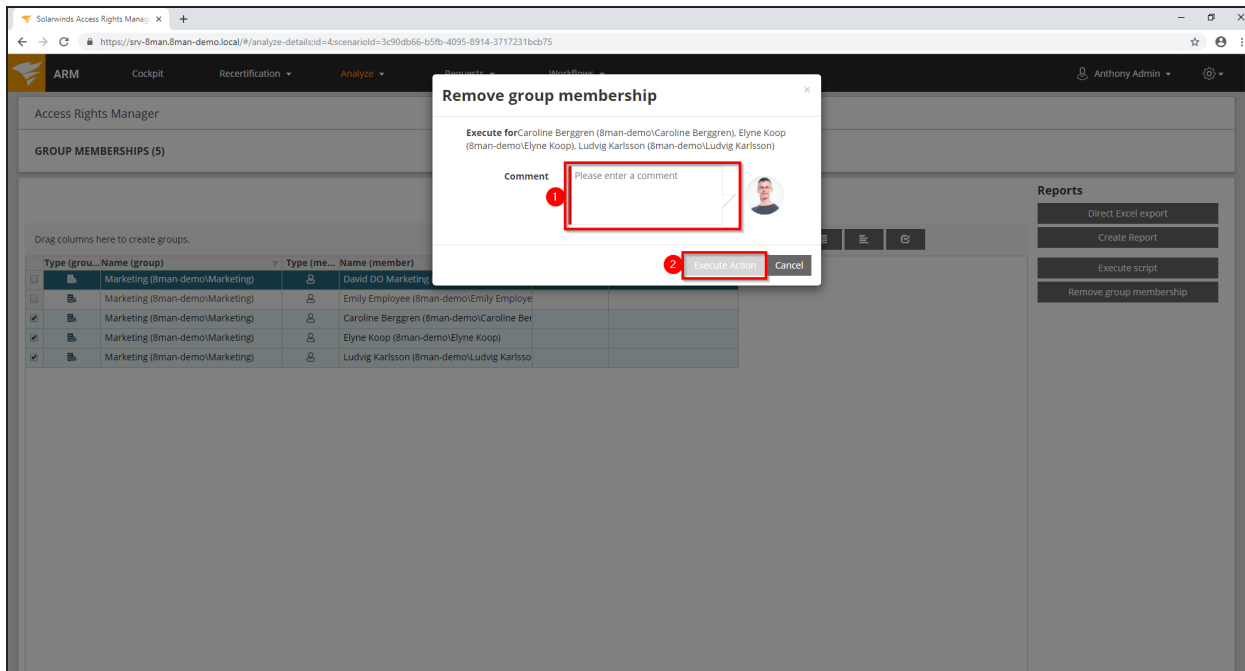


1. Find a group.
2. Start the calculation.



1. ARM lists all members of the previously selected group.
2. Use sorting, filtering, grouping and column selection to locate the desired rows.
3. Select the desired entries.

#### 4. Click "Remove membership".



1. Leave a comment.
2. Click "Execute Action".

The job will be transferred to the ARM server and executed there. ARM administrators can see the status in the task overview scenario.

Create a new department profile

## Background / Value

ARM sets new standards in the field of user provisioning: With the introduction of departmental profiles, department heads, together with the management and the compliance officer, define the scope of action of employees in the company.

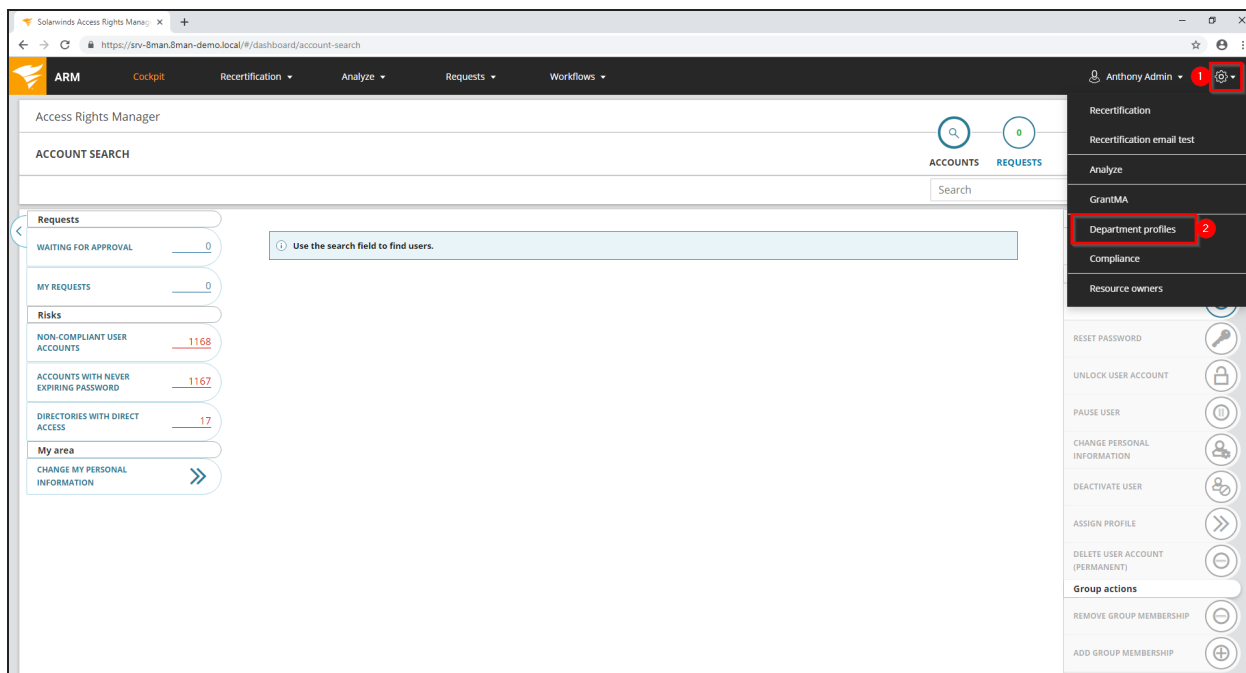
Department profiles can contain attributes and group memberships.

## Related features


[Assign a department profile to users \(Cockpit\)](#)

[Determine permissions deviating from the department profile \(compliance check\)](#)

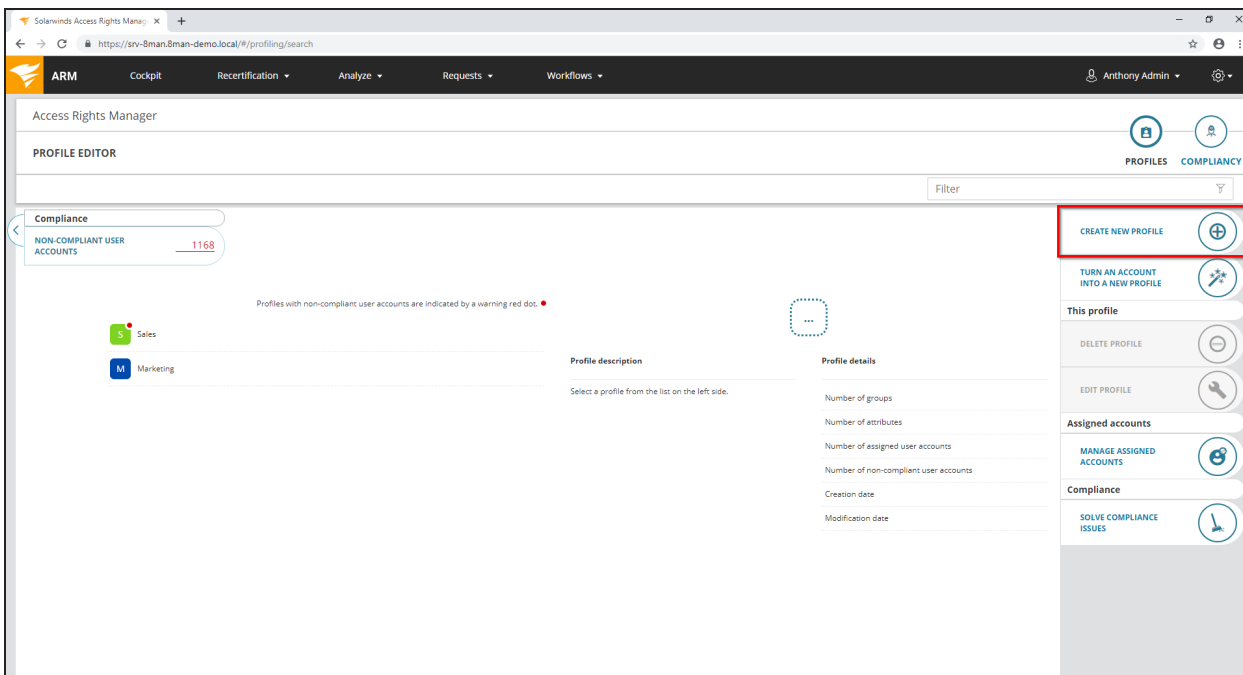
## Step-by-step process



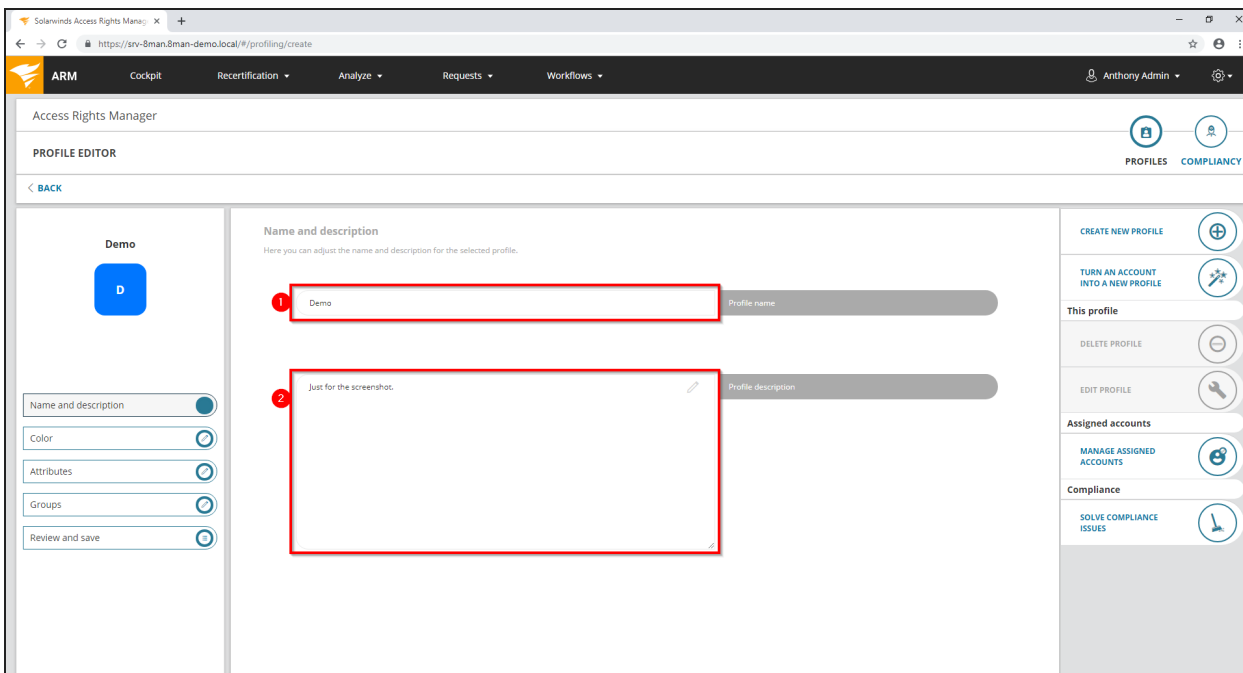
1. Click the gear.

 You must be logged in as an ARM Administrator to see the gear icon.

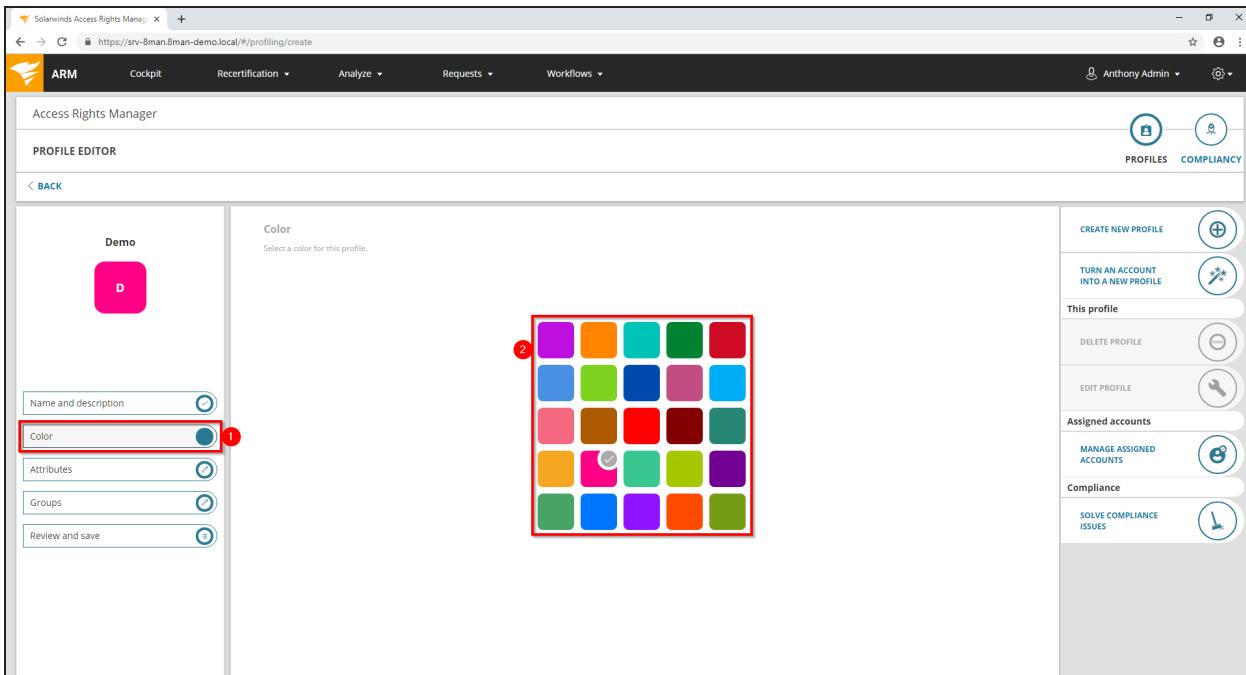
2. Click "Department profiles".



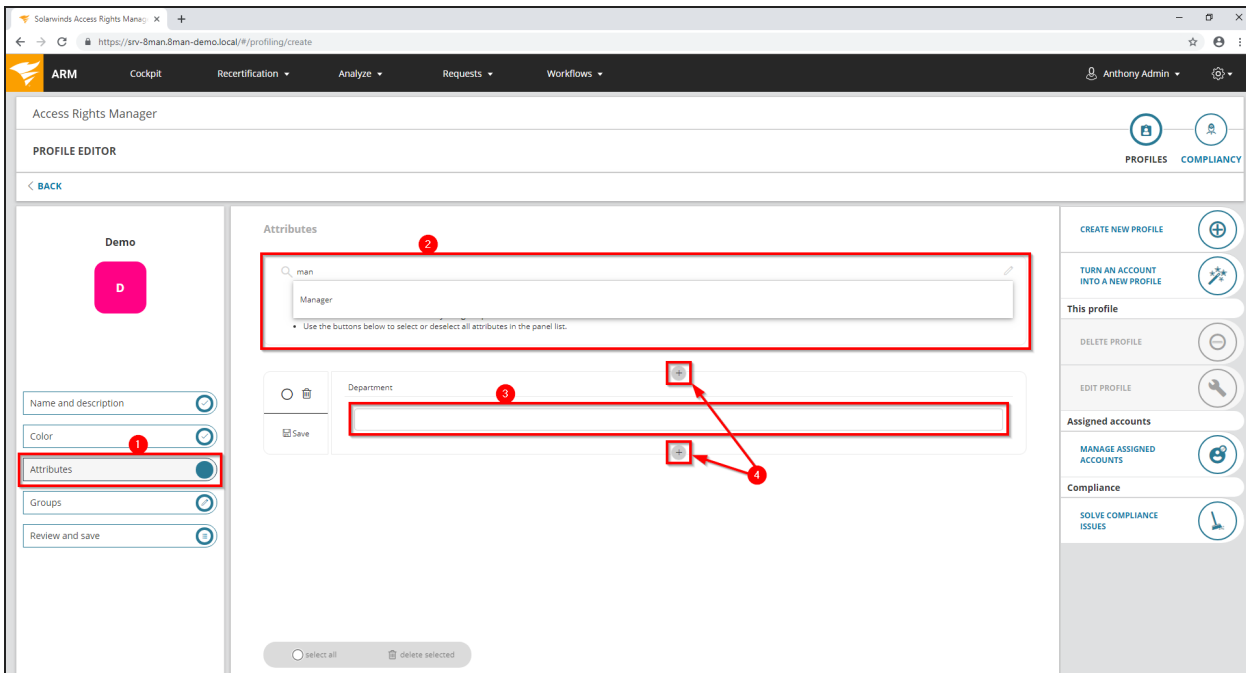
Click "Create new profile".



1. Give the department profile a name, at least 2 letters.
2. Optional: Describe the profile.

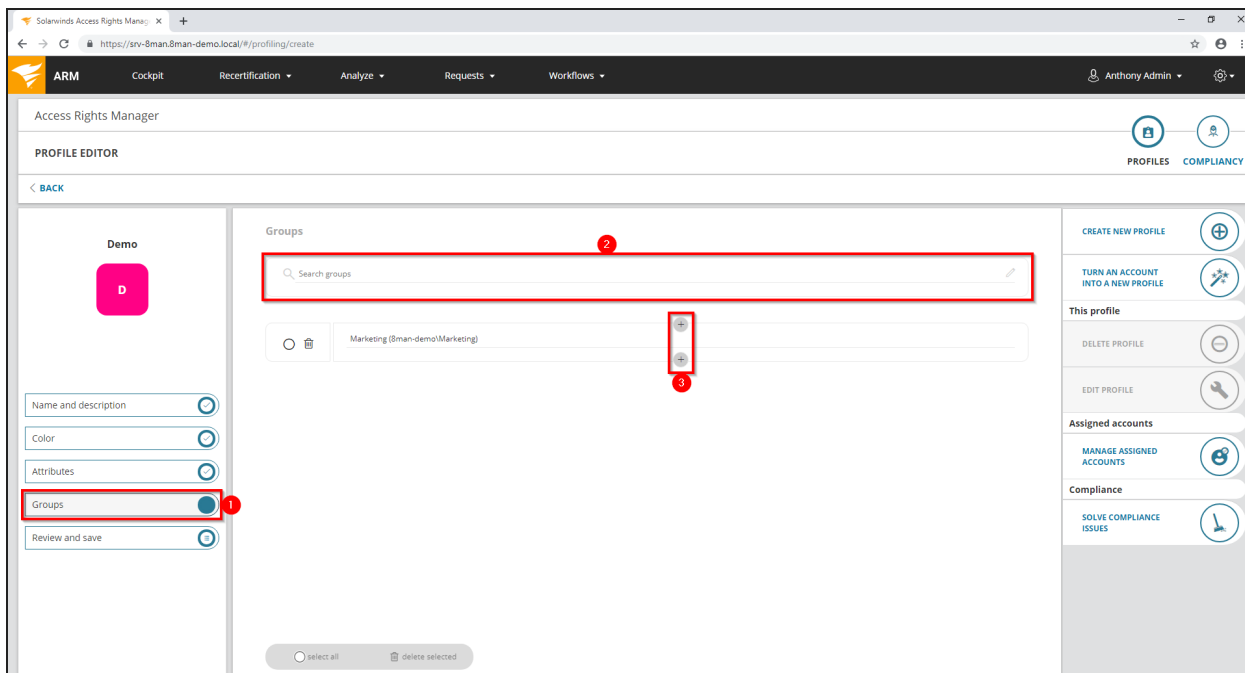


1. Click on "color".
2. Choose a color for the department profile. The color is for recognition purposes only.

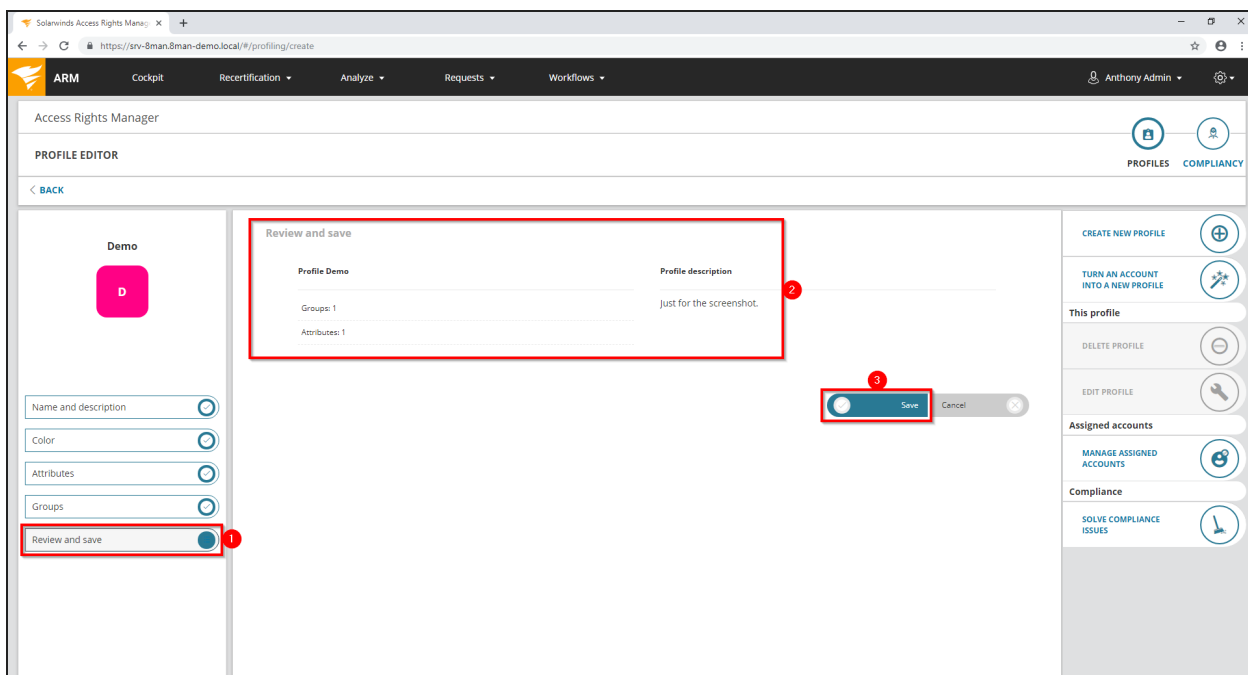


1. Click on "Attributes".
2. Use the search to find the desired attribute.
3. Enter the value of the attribute.

#### 4. Use the plus symbols to add more attributes.



1. Click on "Groups".
2. Find the desired group.
3. Use the plus symbols to add more groups.



1. Select "Review and save".
2. Review your input.
3. Click "Save" to create the department profile.



Execute scripts for directories in bulk (web client)

## Background / Value

Use self-created scripts on directories. ARM opens up space for very individual requirements. Put your scripts in the following directory to use with ARM:

```
%ProgramData%\protected-networks.com\8MAN\scripts\analyze
```

Further necessary steps and more details can be found in the chapter: [Configuring scripts](#)

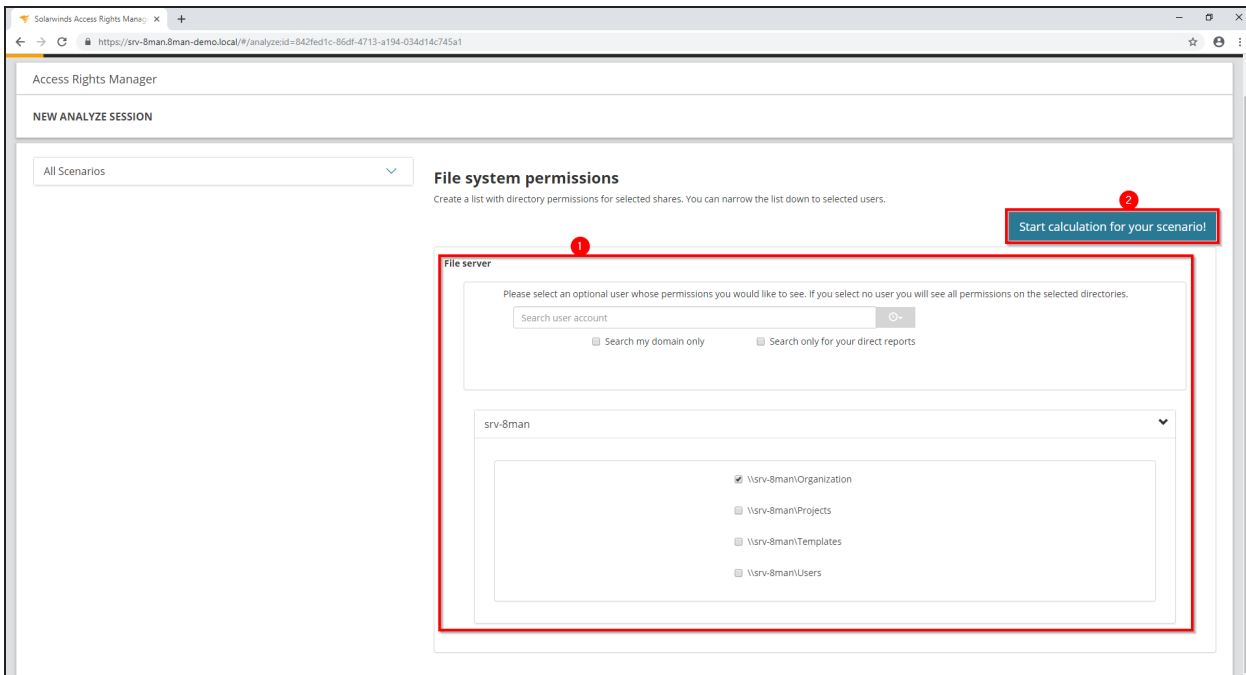
## Related features

[Execute scripts on user accounts in bulk](#) (web client)

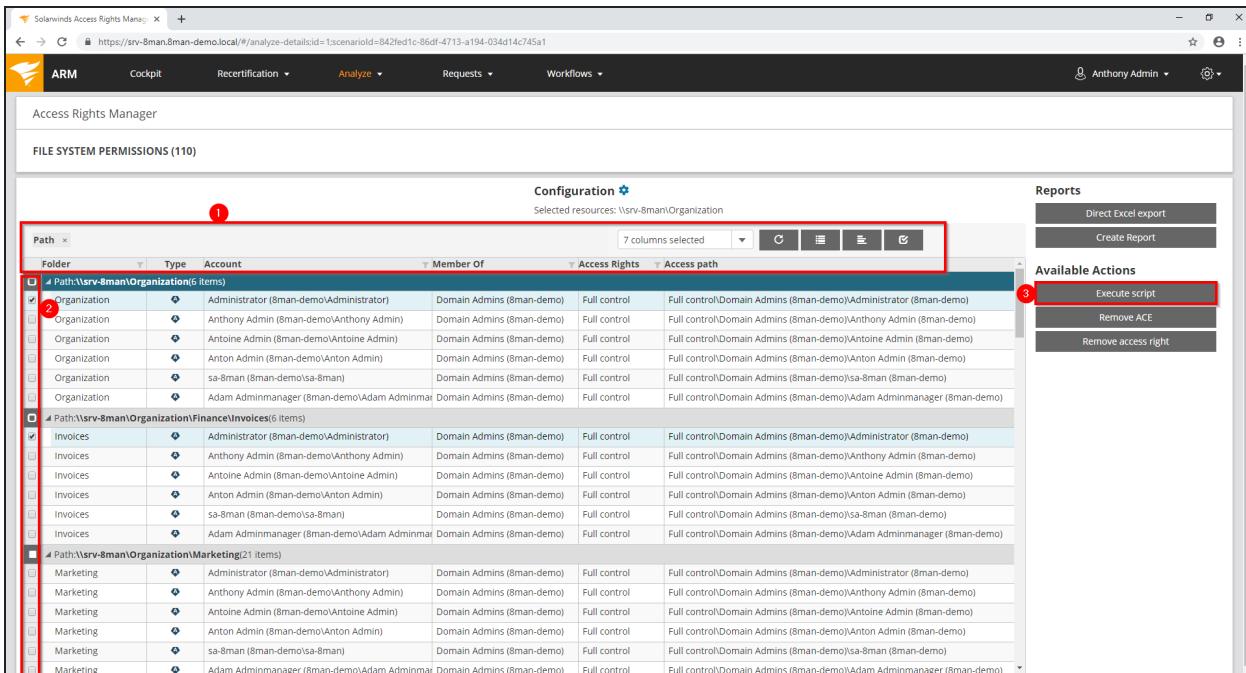
## Step-by-step process

The screenshot shows the Solarwinds Access Rights Manager (ARM) web interface. The top navigation bar includes 'ARM', 'Cockpit', 'Recertification', 'Analyze', 'Requests', and 'Workflows'. The user is logged in as 'Anthony Admin'. The main content area is titled 'Access Rights Manager' and 'ANALYSIS'. The 'ANALYSIS' tab is selected in the top navigation bar. The 'Categories' section on the left lists 'AD users', 'AD computers', 'AD groups', 'Orders & tasks', 'Compliance', and 'Directories'. The 'Directories' category is selected. The 'Scenarios' section on the right lists 'Directories with changed access rights', 'Directories with corrupted inheritance', 'Directories with direct access', 'File system permissions', 'Globally accessible directories', and 'Unresolved SIDs in directories'. The 'Directories with changed access rights' scenario is selected. A tooltip explains that the selected scenario creates a list of directory permissions for selected shares, which can be narrowed to selected users. Red boxes and numbers 1, 2, and 3 highlight the 'ANALYSIS' tab, the 'Directories' category, and the 'Directories with changed access rights' scenario respectively.

1. Select "Analysis".
2. Select the category "Directories".
3. Choose a scenario with directories in focus.



1. Set the scenario options.
2. Start the calculation.



1. Use the grouping, the sorting, filtering and column selection to narrow down your result.
2. Select the desired directories.
3. Click "Execute Script".

Execute script

Execute for 2 items

Select a script to be applied to the selected items.

Choose script to execute: createProjectFolders.ps1

Comment: Please enter a comment

Execute Action Cancel

Path: \\srv-8man\Organization\5 items

Folder	Type	Account	Member Of	Full control	Full control
Organization	Administrator (8man-demo\Administrator)	Domain Admins (8man-demo)	Administrator (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Administrator (8man-demo)
Organization	Anthony Admin (8man-demo\Anthony Admin)	Domain Admins (8man-demo)	Anthony Admin (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Anthony Admin (8man-demo)
Organization	Antoine Admin (8man-demo\Antoine Admin)	Domain Admins (8man-demo)	Antoine Admin (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Antoine Admin (8man-demo)
Organization	Anton Admin (8man-demo\Anton Admin)	Domain Admins (8man-demo)	Anton Admin (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Anton Admin (8man-demo)
Organization	sa-8man (8man-demo\sa-8man)	Domain Admins (8man-demo)	sa-8man (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\sa-8man (8man-demo)
Organization	Adam Adminmanager (8man-demo\Adam Adminmanager)	Domain Admins (8man-demo)	Adam Adminmanager (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Adam Adminmanager (8man-demo)

Path: \\srv-8man\Organization\Finance\Invoices\6 items

Invoice	Administrator (8man-demo\Administrator)	Domain Admins (8man-demo)	Administrator (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Administrator (8man-demo)
Invoice	Anthony Admin (8man-demo\Anthony Admin)	Domain Admins (8man-demo)	Anthony Admin (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Anthony Admin (8man-demo)
Invoice	Antoine Admin (8man-demo\Antoine Admin)	Domain Admins (8man-demo)	Antoine Admin (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Antoine Admin (8man-demo)
Invoice	Anton Admin (8man-demo\Anton Admin)	Domain Admins (8man-demo)	Anton Admin (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Anton Admin (8man-demo)
Invoice	sa-8man (8man-demo\sa-8man)	Domain Admins (8man-demo)	sa-8man (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\sa-8man (8man-demo)
Invoice	Adam Adminmanager (8man-demo\Adam Adminmanager)	Domain Admins (8man-demo)	Adam Adminmanager (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Adam Adminmanager (8man-demo)

Path: \\srv-8man\Organization\Marketing\25 items

Market	Administrator (8man-demo\Administrator)	Domain Admins (8man-demo)	Administrator (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Administrator (8man-demo)
Market	Anthony Admin (8man-demo\Anthony Admin)	Domain Admins (8man-demo)	Anthony Admin (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Anthony Admin (8man-demo)
Market	Antoine Admin (8man-demo\Antoine Admin)	Domain Admins (8man-demo)	Antoine Admin (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Antoine Admin (8man-demo)
Market	Anton Admin (8man-demo\Anton Admin)	Domain Admins (8man-demo)	Anton Admin (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Anton Admin (8man-demo)
Market	sa-8man (8man-demo\sa-8man)	Domain Admins (8man-demo)	sa-8man (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\sa-8man (8man-demo)
Market	Adam Adminmanager (8man-demo\Adam Adminmanager)	Domain Admins (8man-demo)	Adam Adminmanager (8man-demo)	Full control	Full control\Domain Admins (8man-demo)\Adam Adminmanager (8man-demo)

## 1. Select a script.

**i** Further necessary steps and more details can be found in the chapter: [Configuring scripts](#).

## 2. You must enter a comment.

## 3. Click on "Execute action".

Execute scripts on user accounts in bulk (web client)

## Background / Value

Use self-created scripts on directories. ARM opens up space for very individual requirements. Put your scripts in the following directory to use with ARM:

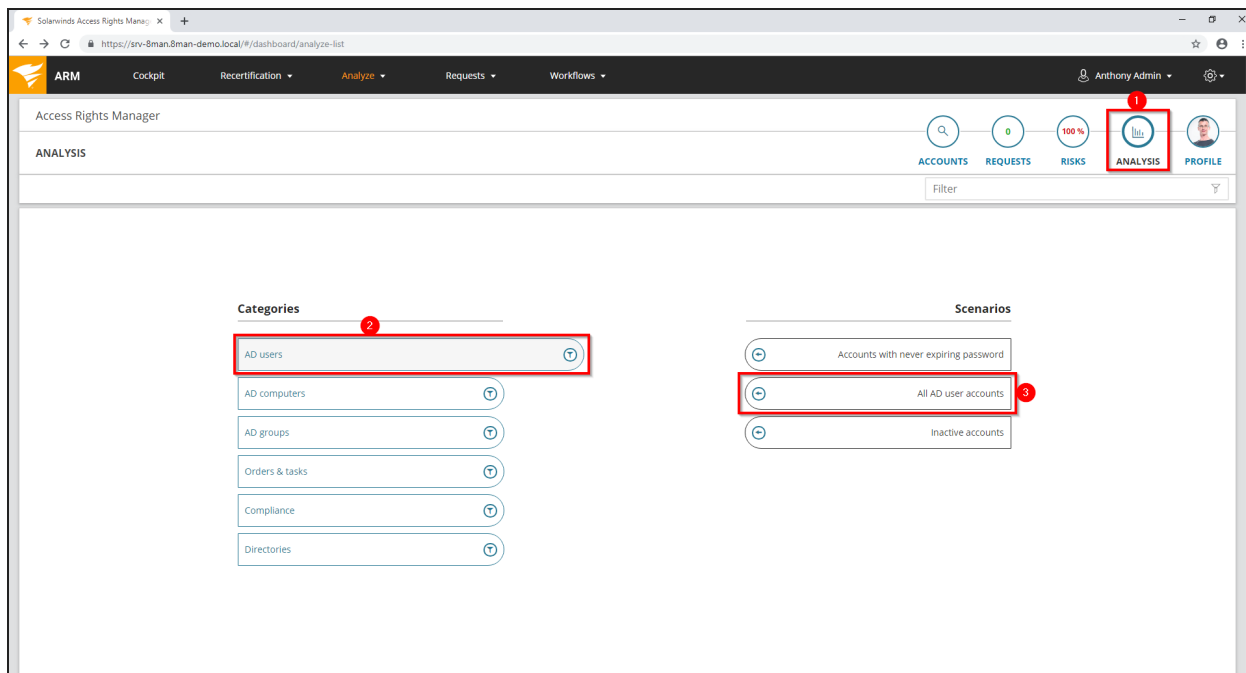
```
%ProgramData%\protected-networks.com\8MAN\scripts\analyze
```

Further necessary steps and more details can be found in the chapter: [Configuring scripts](#).

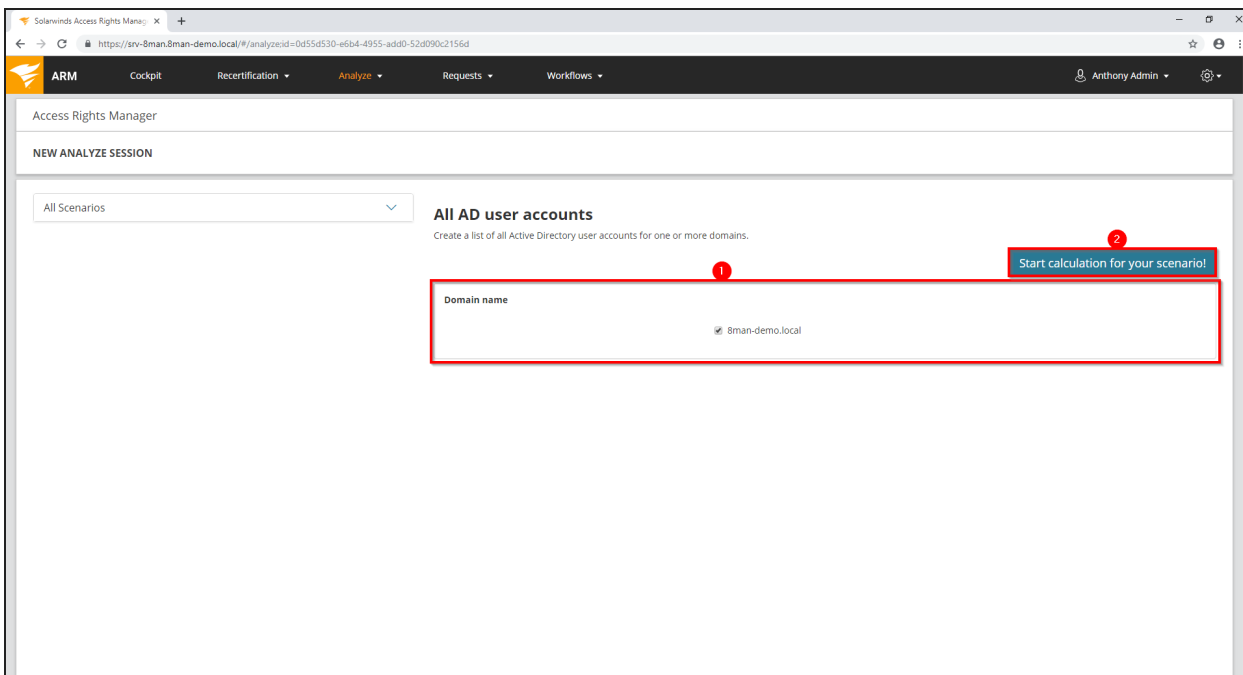
## Related features

[Execute scripts on directories in bulk](#) (web client)

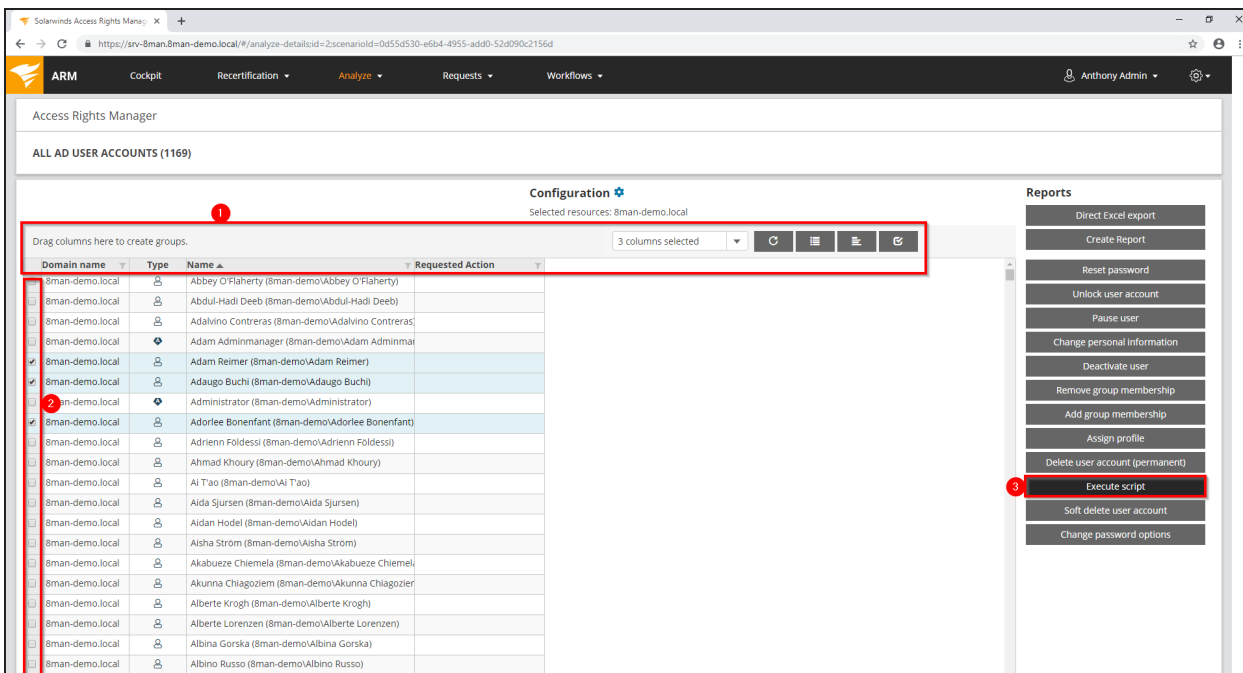
## Step-by-step process



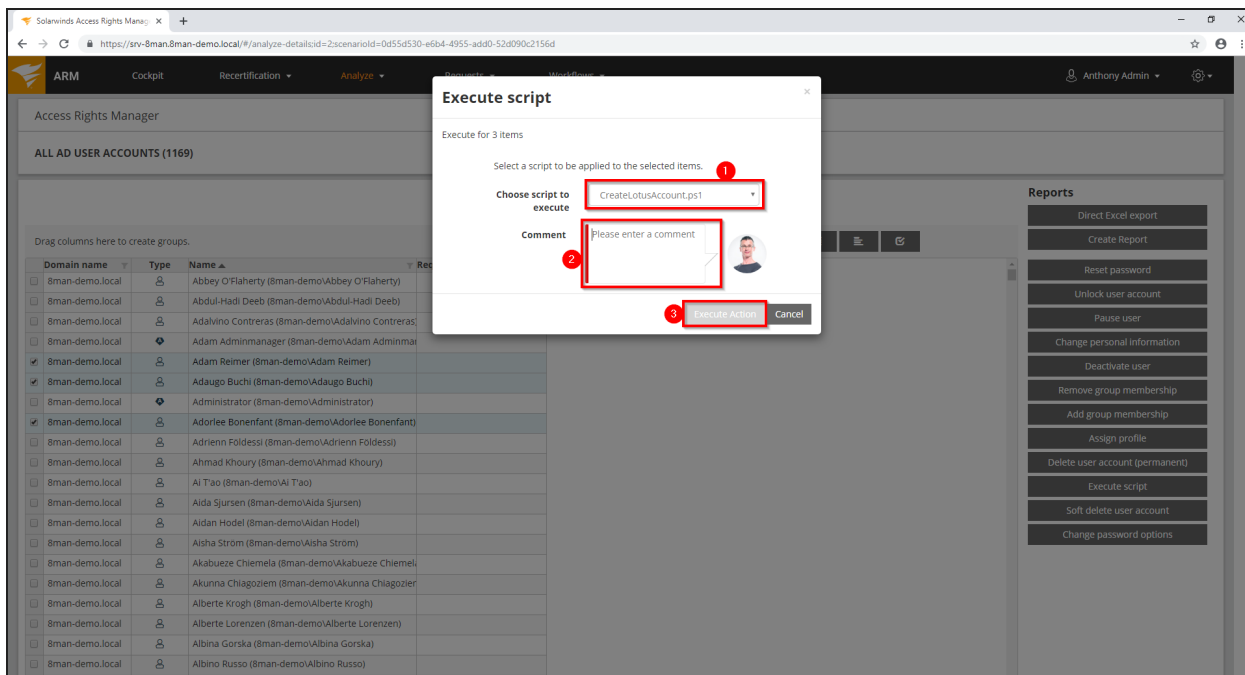
1. Select "Analysis".
2. Select the category "AD users".
3. Choose a scenario with users in focus.



1. Set the scenario options.
2. Start the calculation.



1. Use the grouping, sorting and filtering functions to narrow down your result.
2. Select the desired accounts.
3. Click "Execute Script".



### 1. Select a script.

**i** Further necessary steps and more details can be found in the chapter: [Configuring scripts](#).

### 2. You must enter a comment.

### 3. Click on "Execute action".

Edit temporary group memberships (web client)

## Background / Value

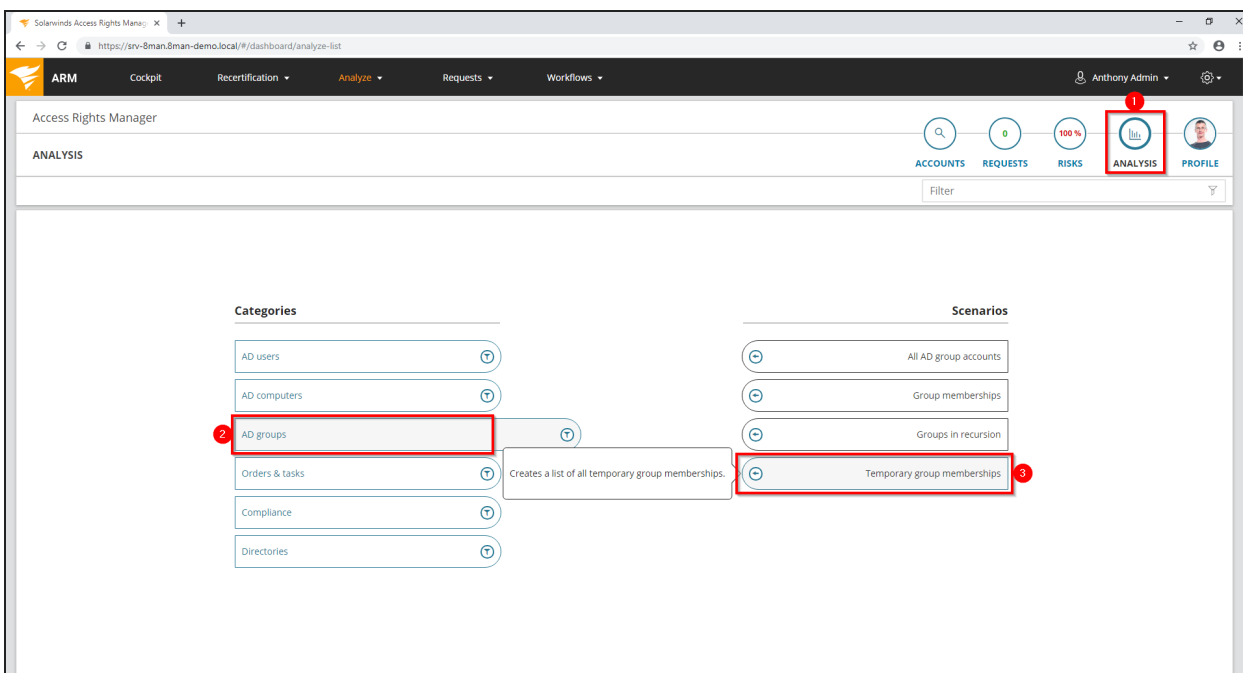
Simply change the expiration date of temporary group memberships or convert them to a permanent membership. You can also easily remove temporary memberships.

## Related features

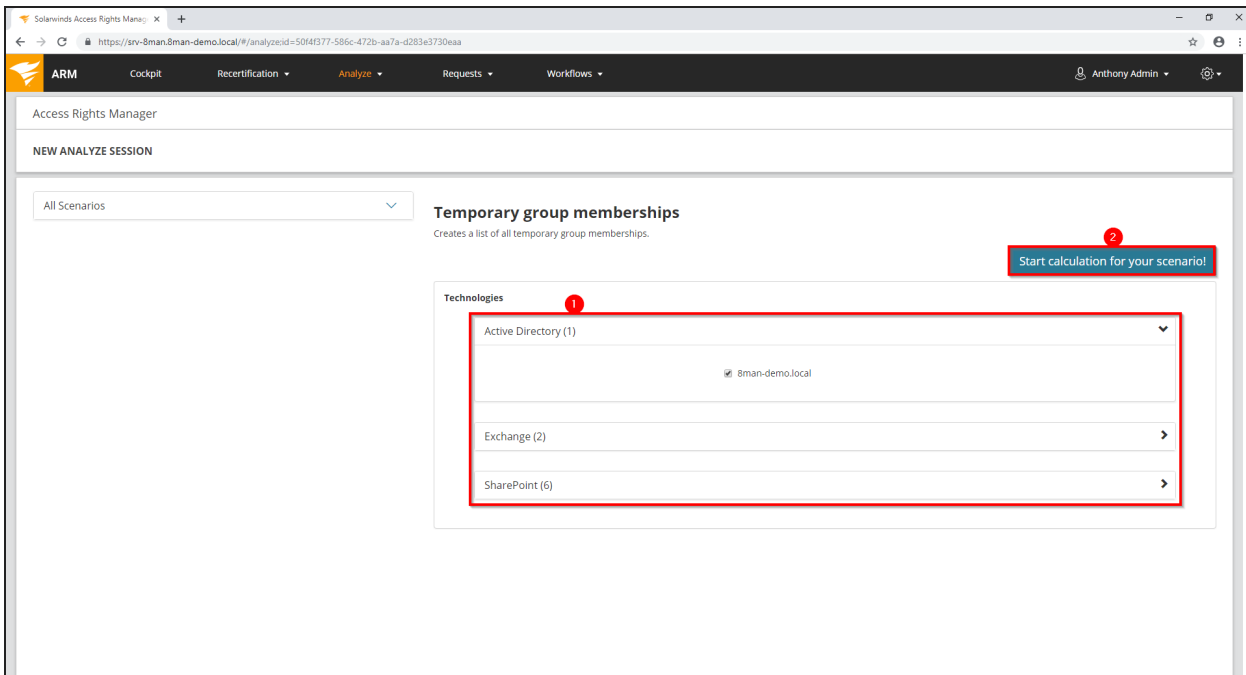
[Remove group memberships \(cockpit\)](#)

[Add group memberships \(cockpit\)](#)

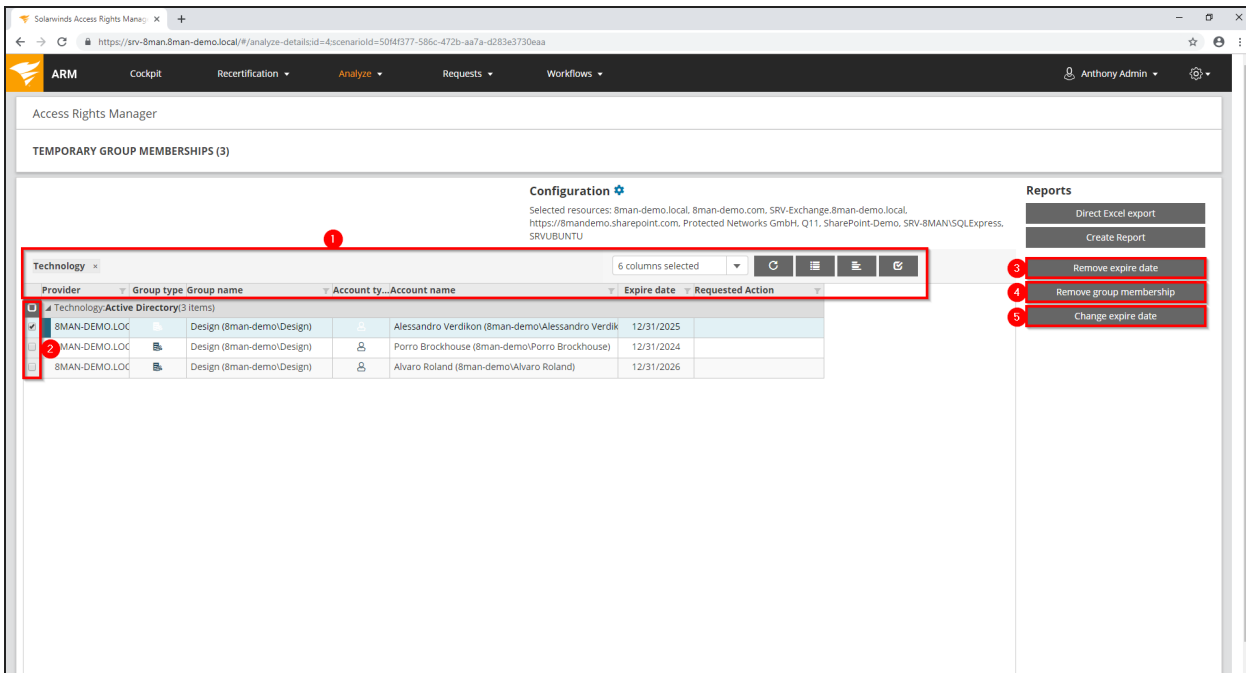
## Step-by-step process



1. Select "Analysis".
2. Select the category "AD Groups".
3. Click on "Temporary group memberships".



1. Select the resources you want to include in your analysis.
2. Start the analysis.



1. Use sorting, grouping, filtering and column selection to narrow down your selection.
2. Select the required group memberships.



3. Remove the expiration date. This is how you convert the temporary membership into a permanent group membership.
4. End the group membership immediately (before the expiration date).
5. Change the expiration date.

Edit computer accounts

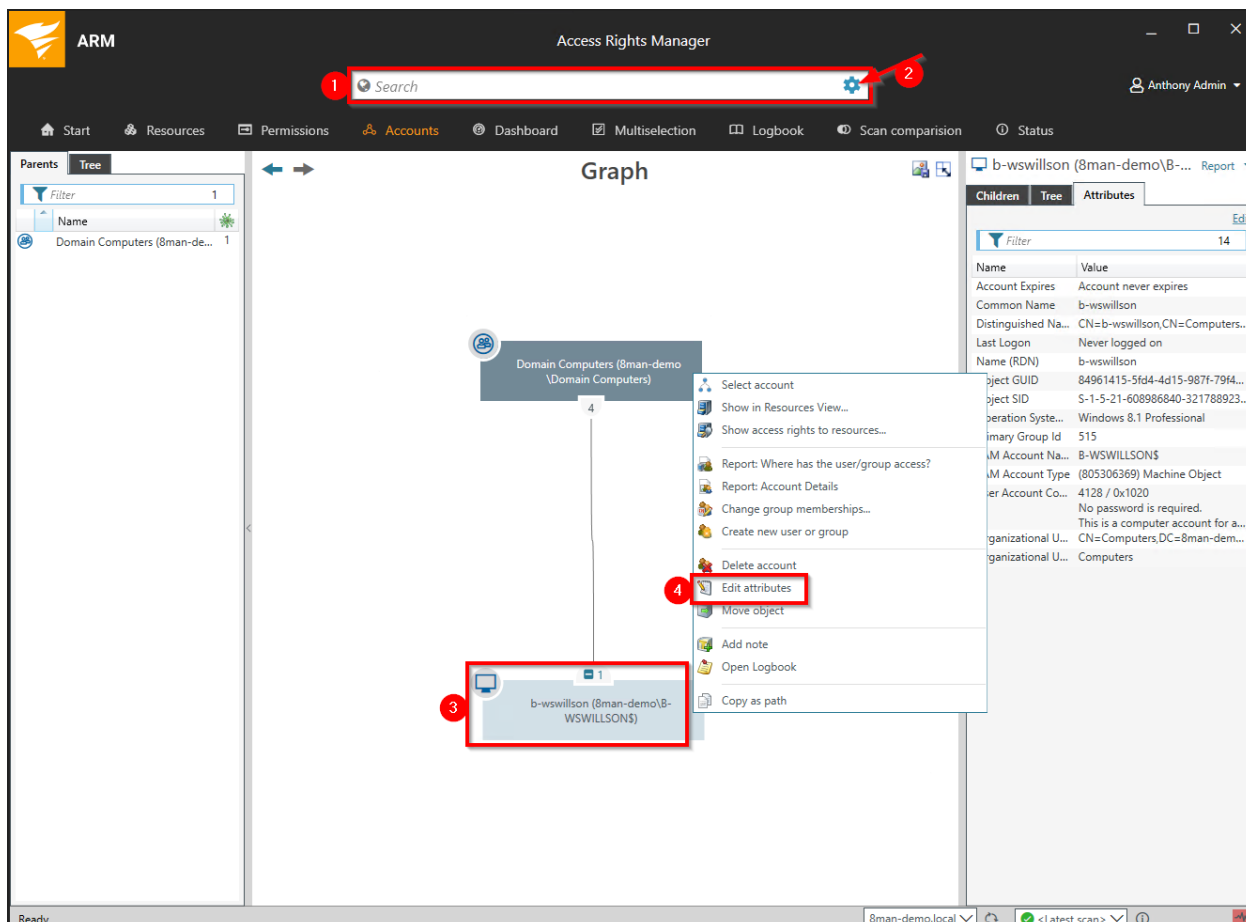
## Background / Value

Maintain computer accounts comfortably and documented within ARM.

## Related features

[Delete computer accounts](#)

## Step-by-step process



1. Find a computer account.
2. Computer accounts must be enabled in the search options (arrow).
3. Right-click the found computer account.
4. Select "Edit attributes".

The screenshot shows the 'Edit attributes' dialog in the SolarWinds Access Rights Manager. The dialog is titled 'Edit attributes' and shows a list of attributes for the computer account 'b-wswillson (8man-demo\B-WSWILLSONS)'. The attributes are listed in a table with columns for 'Name' and 'Value'. The 'Common Name' attribute is highlighted with a red box and a red circle '1'. Below the list, there is a text input field for a comment, a warning icon, and an 'Immediately' button. A red box highlights the 'Immediately' button with a red circle '3'. A red box highlights the comment input field with a red circle '2'. A red box highlights the 'Immediately' button with a red circle '3'. A red box highlights the comment input field with a red circle '2'.

Name	Value
Common Name	b-wswillson
Comment	Attribute value is not given
Company	Attribute value is not given
Department	Attribute value is not given
Description	Demo description
Display Name	Attribute value is not given
Information	Attribute value is not given
managedby	<not set>
Operation System (OS)	Windows 8.1 Professional
OS Servicepack	Attribute value is not given
OS Version	Attribute value is not given
SAM Account Name	B-WSWILLSONS
Script-Path	Attribute value is not given

1. Change the attributes.  
ARM loads a standard set of attributes. If additional attributes of computer accounts are to be loaded in ARM, please reference [Load additional LDAP attributes](#).
2. You must enter a comment.
3. Start the execution.

Delete computer accounts

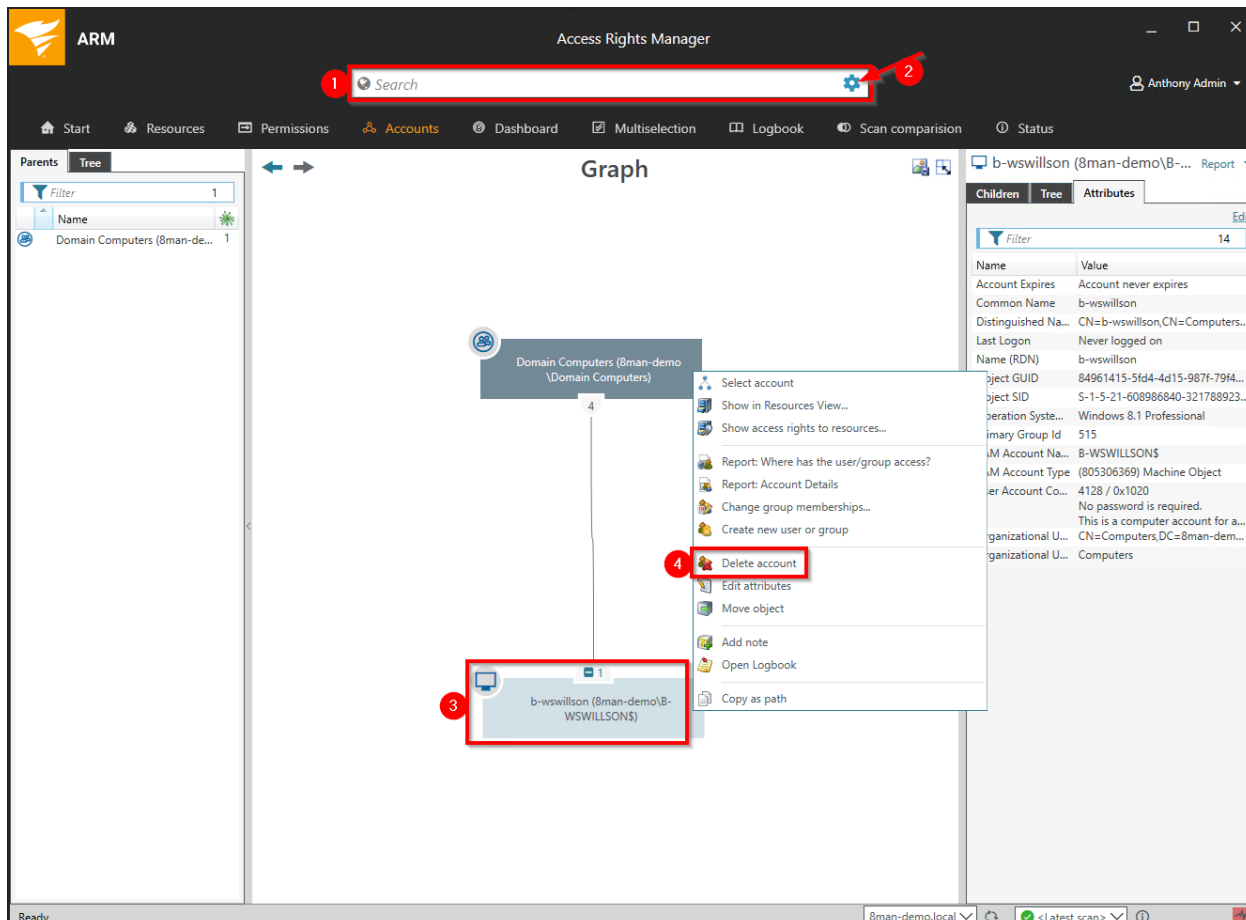
## Background / Value

Delete computer accounts comfortably and documented within ARM.

## Related features

[Edit computer accounts](#)

## Step-by-step process




1. Find a computer account.
2. Computer accounts must be enabled in the search options (arrow).
3. Right-click the found computer account.
4. Select "Delete account".


**Delete account** ⊗


...

Accounts to delete		Required credentials	
Name		Resource	Credentials
<input type="checkbox"/>	b-wswillson (8man-demo\B-WSWILLSON\$)	8MAN-DEMO.LOCAL	8man-demo\sa-8man <span>1</span>

 Remove access rights 2  
Remove all direct references to the selected accounts on resources which are known to ARM.  
The execution will be immediately

▼ Scripting

3  

 4

1. Optional: Change the login to delete the account.
2. Recommended: Enable the option to remove any existing (direct) permission entries.
3. You must enter a comment.
4. Start the execution.

## Helpdesk

Reset passwords

### **Background / Value**

Resetting passwords is one of the most common tasks performed by help desks. ARM allows an easy and secure way of resetting passwords. All sensitive actions are documented in the log book. If an employee uses native tools to reset a password and illegally tries to access that user account, the incident is captured with AD Logga. Especially sensitive user accounts can be monitored with AD Logga alerts.

### **Related features**

[AD Logga: Identify locked accounts](#)

[AD Logga: Set alerts for user accounts](#)

### **Step-by-step process**

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The 'Accounts' tab is active, showing a 'Graph' view of the user hierarchy. A search bar at the top is highlighted with a red box and labeled '1'. The graph shows a hierarchy of accounts, with 'Emily Employee (8man-demo\Emily Employee)' selected and highlighted with a red box and labeled '2'. A context menu is open over this user, with the 'Reset user password' option highlighted and labeled '3'. The right-hand pane shows the user's details, including name, email address, and organizational information.

1. Use the search field to find the desired user.
2. Right-click the user, e.g. in the Accounts view.
3. Select "Reset User Password" from the context menu.

ARM Access Rights Manager

Search Anthony Admin

Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparison Status

Parents Tree Filter 14

Name

- All employees (8man-demo\A... 1
- Domain Users (8man-dem... 1
- L\_Organization\_M...
- L\_Organization\_M...
- Marketers (8man-dem...
- Marketing (8man-s...
- mc\_reg\_byod (8ma...
- 8man-demo complet...
- L\_Organization\_M...
- L\_Organization\_M...
- L\_Organization\_M...
- public (SRV-8MAN)...
- Users (8man-demo...

Graph

Emily Employee (8man-demo\...)

Children Tree Attributes Accounts Filter 24

Reset user password

Reset user password

Credentials 8man-demo\sa-8man

Emily Employee (8man-demo\Emily Employee)

New password

1n17141P455w0rd

Hide password

Generate a new password with a length of 8 characters

The user must change the password at next logon

Unlock user account automatically

Please add a comment

Close Immediately

Ready 8man-demo.local <Latest scan>

1. Determine your password options.
2. You must enter a comment.
3. Start the reset process.



Unlock user accounts (web client)

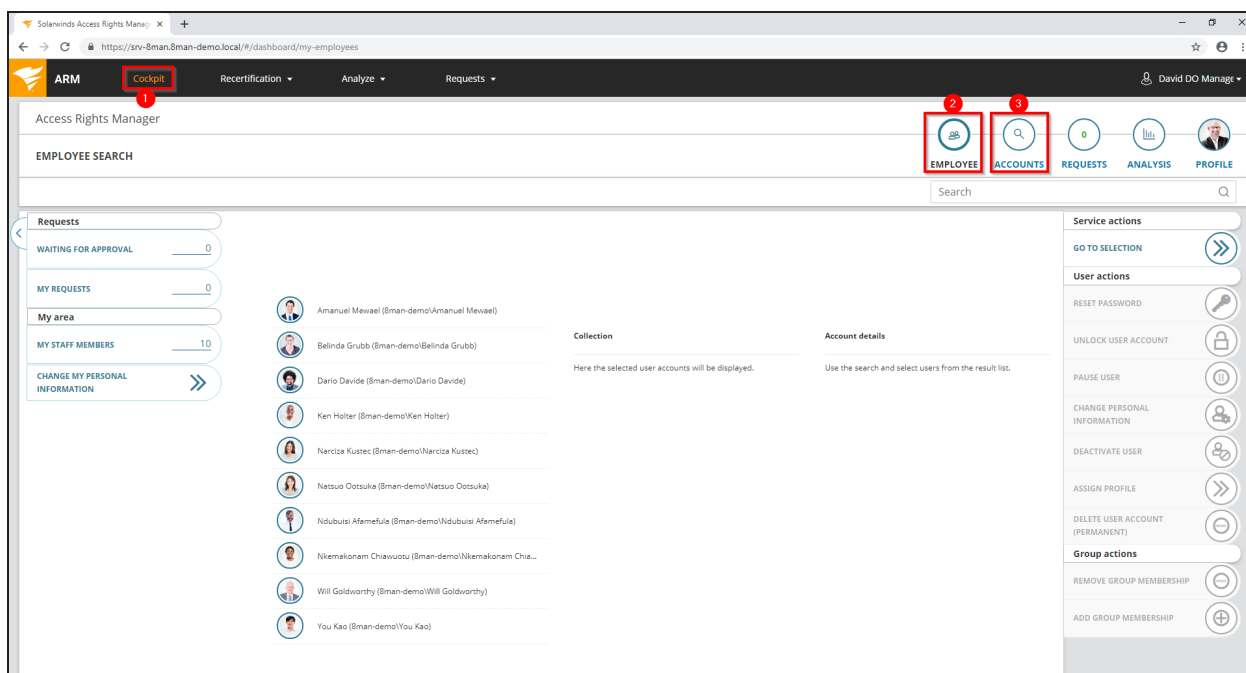
## Background / Value

The most common activity of the HelpDesk is to unlock accounts. Typically because the password was entered wrong too often. If the user remembers the password, the account can be unlocked without resetting the password.


## Additional features

### [Reset users' passwords \(Cockpit\)](#)

## Step-by-step process



1. Choose Cockpit.
2. Choose "Employee". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See [Changing Attributes](#) (Web Client).
3. Choose "Accounts". Accounts for data owners are assigned by an ARM administrator in the [data owner configuration](#).

 The range of available features (buttons) varies according to role (login), risk assessment and configuration.

The screenshot displays the Solarwinds Access Rights Manager (ARM) interface. At the top, there is a navigation bar with 'ARM' and 'Cockpit' tabs, and a search bar containing 'emily'. Below the search bar, there are several tabs: 'EMPLOYEE', 'ACCOUNTS', 'REQUESTS', 'ANALYSIS', and 'PROFILE'. The main content area shows a list of users, a 'Collection' of selected users, and 'Account details' for the selected user. The 'UNLOCK USER ACCOUNT' button is highlighted in the right-hand sidebar.

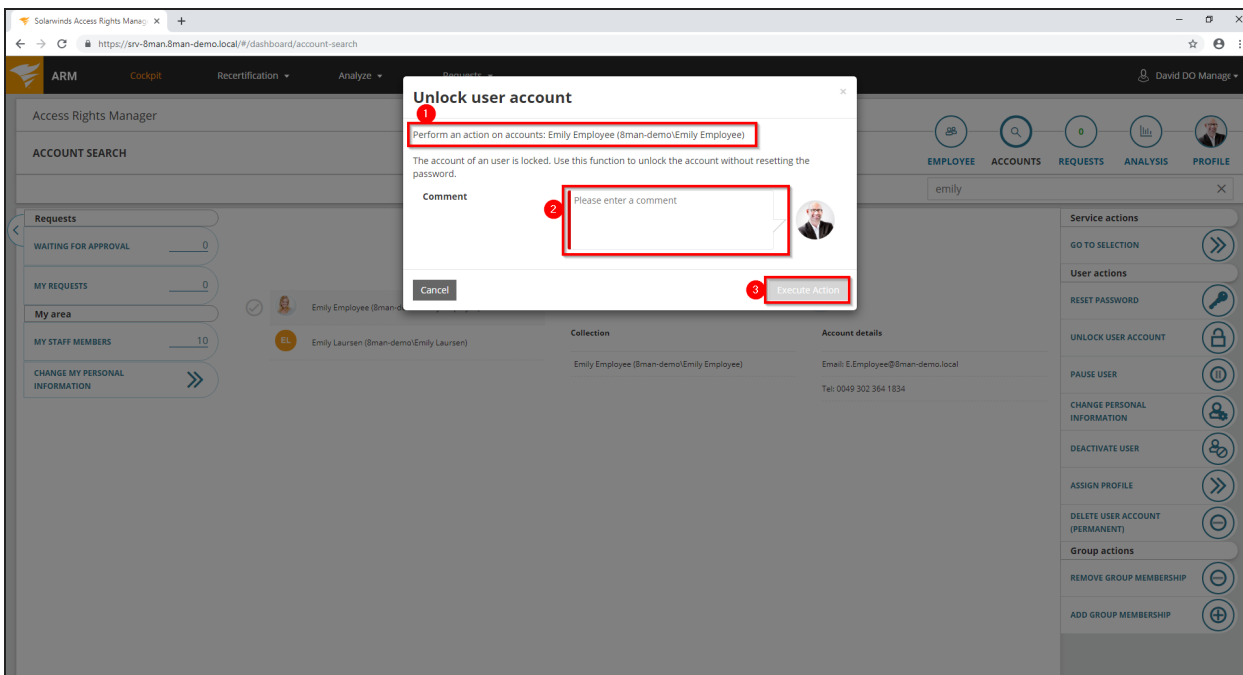
1. Use the search to filter a long list of employees or search for users.

2. Select one or more users.

3. ARM shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.

4. In the collection you can see already selected users.

5. Click "Unlock Account".



1. ARM shows you on which accounts the action should be performed.
2. You must enter a comment.
3. Click "Execute action".

Reset passwords in bulk (web client)

## Background / Value

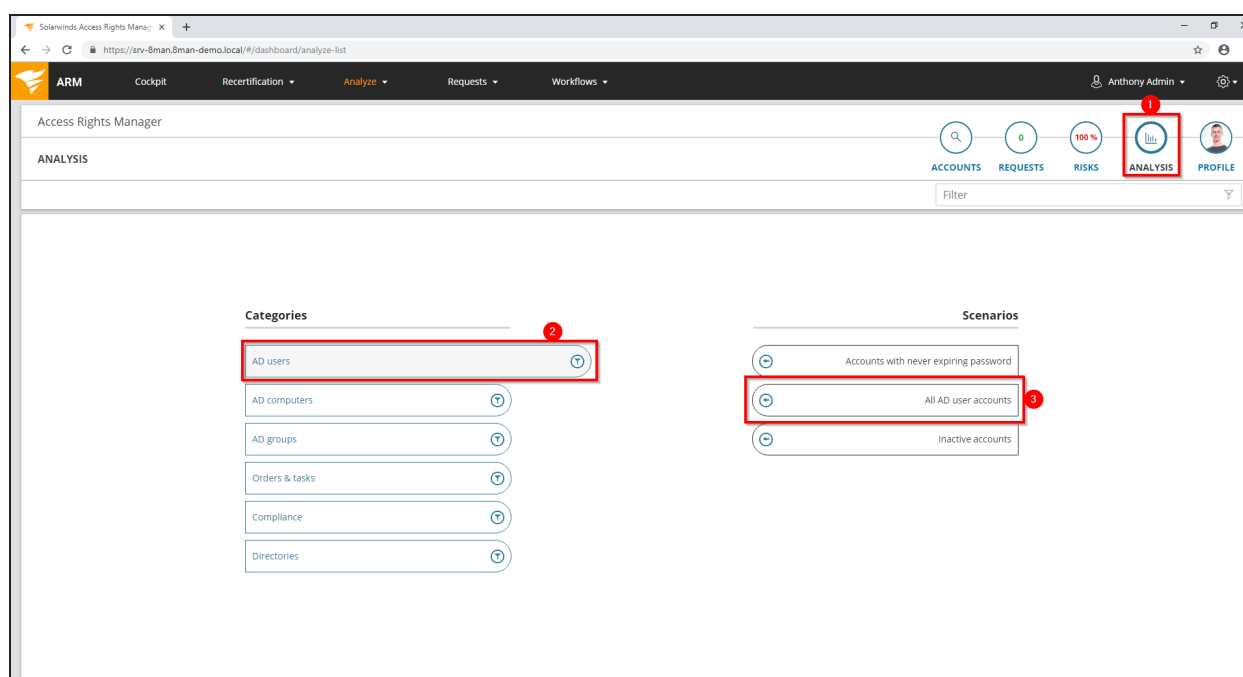
There are many use cases in which the passwords of several users must be reset simultaneously. You can reset passwords in bulk in the web interface.

## Related features

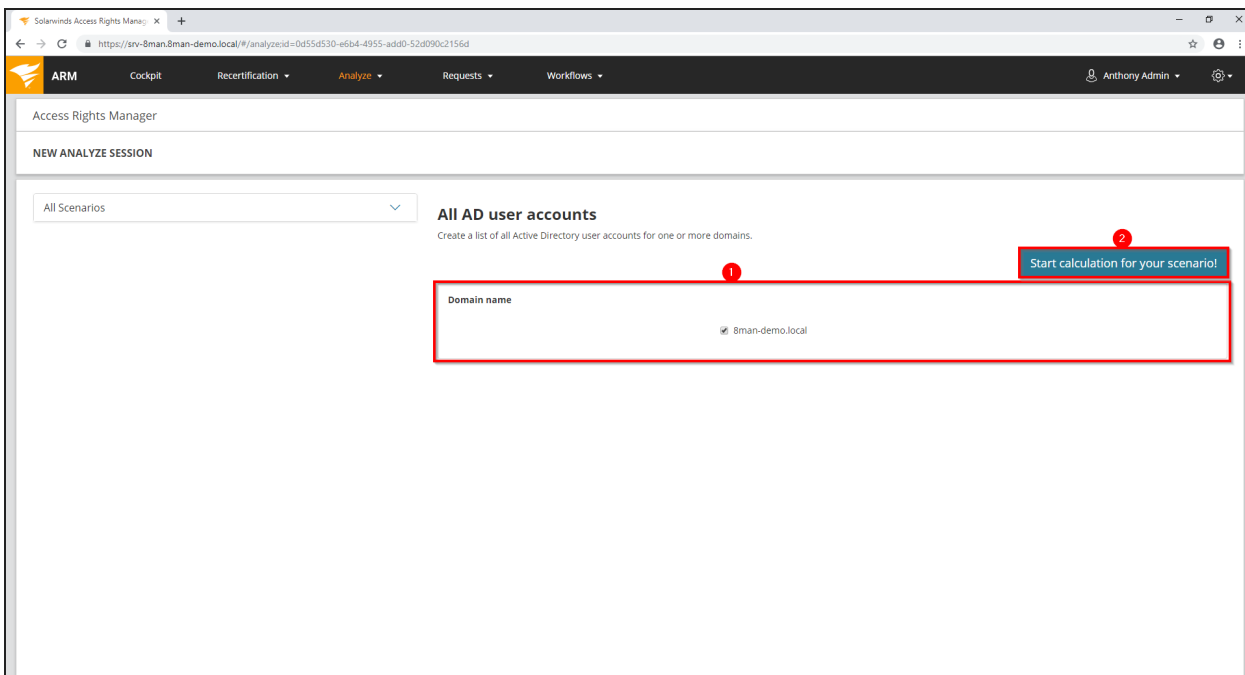
[Deactivate user accounts in bulk](#) (web client)

[Change password options in bulk](#) (web client)

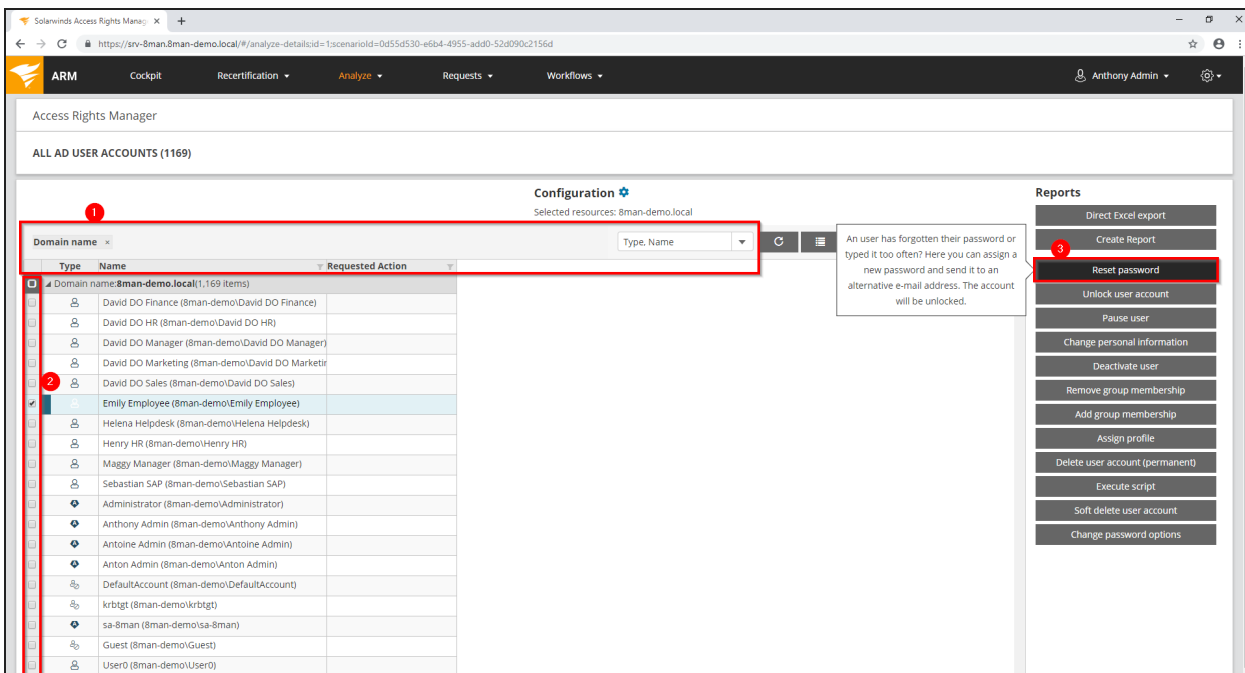
## Step-by-step process



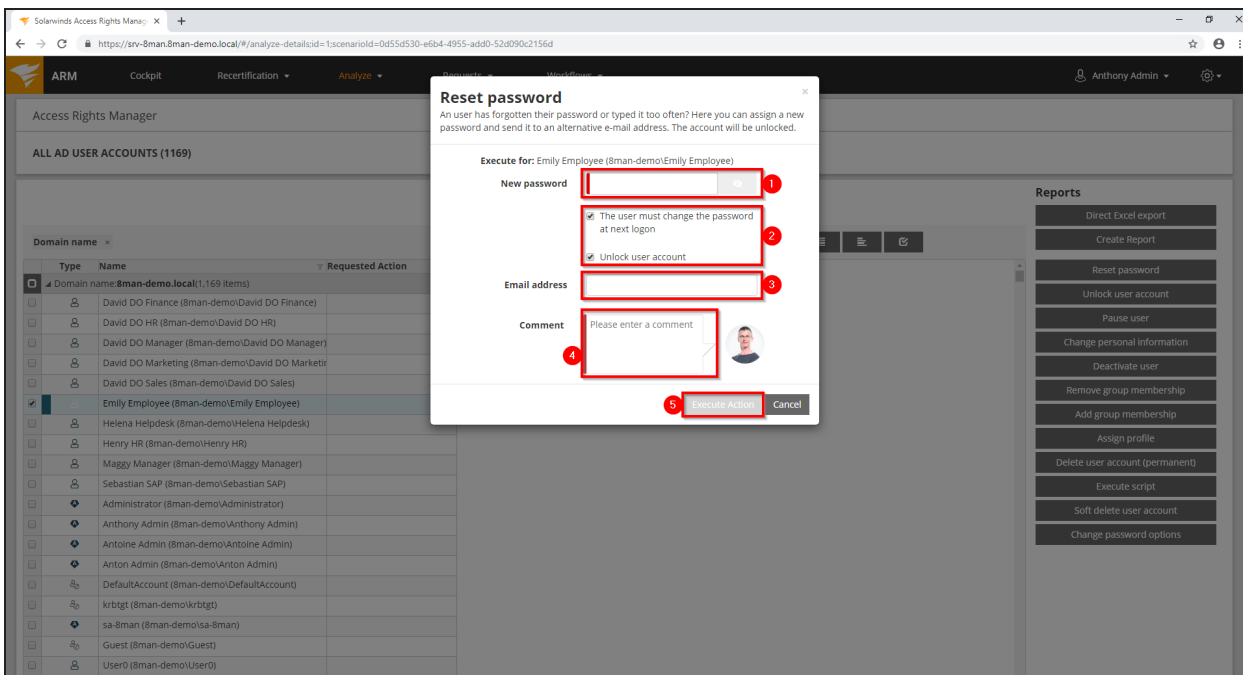
1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".



1. Set options for the scenario.
2. Click on "Start calculation".



1. Use sorting, filtering, grouping and column selection to locate the desired rows.
2. Select the desired entries.
3. Click "Reset password".



1. Assign a new password.
2. Activate the desired options.  
These options are only available to ARM administrators. For all other ARM roles, these options are not visible and always enabled.
3. Optional: Specify an email account that users can still access.
4. You must enter a comment.
5. Click "Execute action".

The job is transferred to the ARM server and executed there. ARM administrators can see the status in the task overview scenario.

Unlock a user account

## Background / Value

Unlocking user accounts is one of the most frequently performed action of most help desks. All actions are documented in the logbook.

## Related features

If employees use native tools to unlock a sensitive account, AD Logga will capture all activity. Especially sensitive accounts can be monitored with AD Logga alerts.

[AD Logga: Identify locked user accounts](#)

[AD Logga: Set alerts for user accounts](#)

## Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The search bar at the top is highlighted with a red box and a '1'. The 'Accounts' view is selected, and the 'Emily Employee' user is highlighted with a red box and a '2'. The context menu is open, and the 'Unlock user' option is highlighted with a red box and a '3'.

1. Use the search field to find the desired user.
2. Right-click the user, e.g. in the Accounts view.

## 3. Select Unlock user from the context menu.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. A dialog box titled "Unlock user" is open, displaying the user "Emily Employee (8man-demo\Emily Employee)". The dialog box contains a text input field with a red "1" next to it, a "Close" button, and a dropdown menu with "Immediately" selected and a red "2" next to it. The background shows the ARM interface with a search bar, navigation tabs, and a user list.

1. You must enter a comment.
2. Start the unlocking process.



Deactivate a user account

## Background / Value

If you deactivate an account with ARM, this is equivalent to a normal deactivation with on-board resources. The user account remains in the OU. The process is documented in the logbook.

## Related features

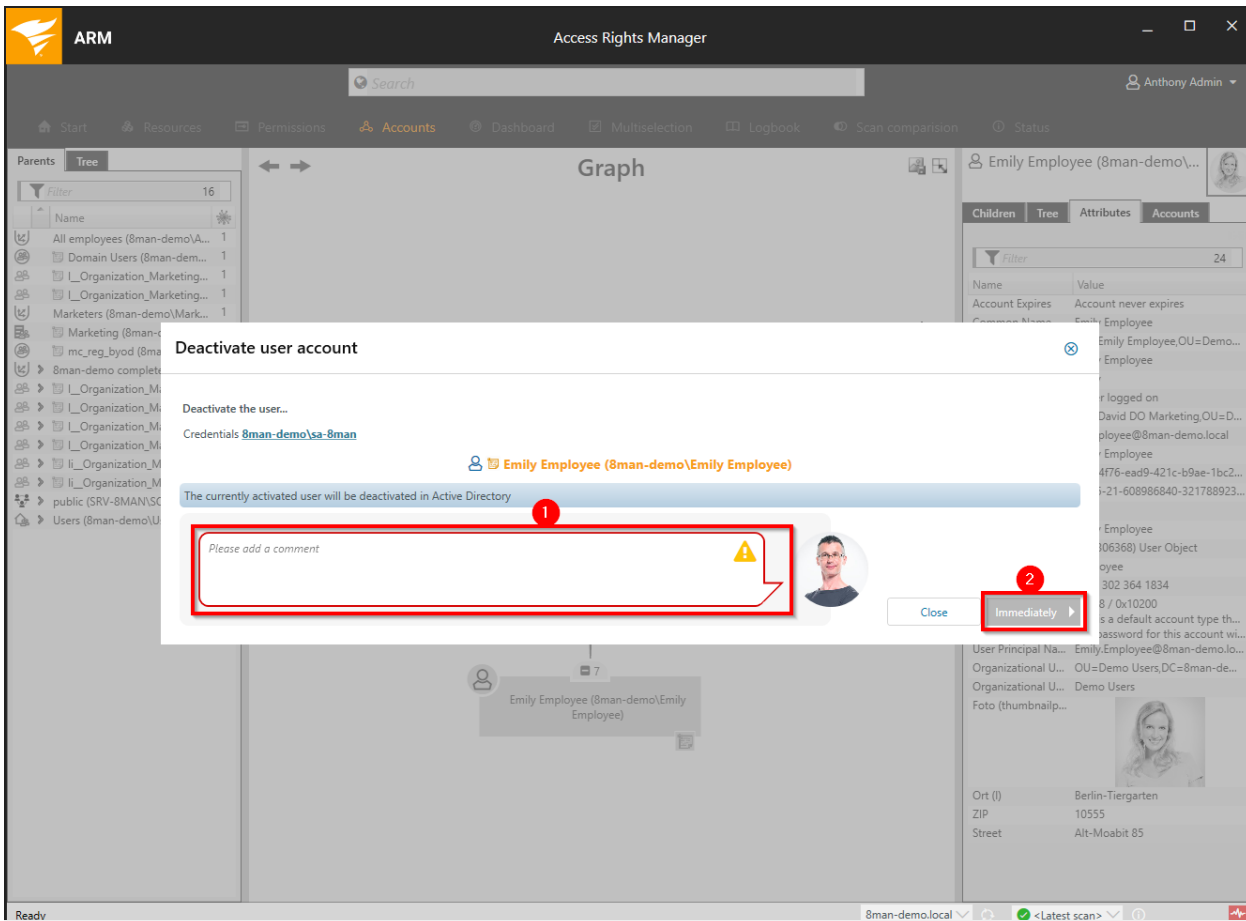
[Delete a user with soft delete](#)

[Deactivate accounts in bulk](#) (web client)

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) web interface. The search bar at the top is highlighted with a red box and a red circle with the number 1. The navigation menu includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The 'Accounts' tab is selected, and the 'Tree' view is active. The tree view shows a hierarchy of resources, with 'Emily Employee (8man-demo\Emily Employee)' selected and highlighted with a red box and a red circle with the number 2. A context menu is open over the selected user, with the 'Deactivate account' option highlighted with a red box and a red circle with the number 3. The context menu includes options such as 'Select account', 'Show in Resources View...', 'Show access rights to resources...', 'Report: Where has the user/group access?', 'Report: Account Details', 'Change group memberships...', 'Create new user or group', 'Unlock user', 'Deactivate account', 'Change password options', 'Reset user password', 'Soft delete user account', 'Delete account', 'Edit attributes', 'Move object', 'Enable mailbox', 'Add note', 'Open Logbook', 'Create alert', and 'Copy as path'. The right-hand pane shows the details of the selected user, including their name, email address, and other attributes.

1. Use the search field to find the desired user.
2. Right-click the user or group, e.g. in the Accounts view.
3. Select "Deactivate account" from the context menu.



1. You must enter a comment.
2. Start the execution.

Modify attributes of users, groups, and computers

## Background / Value

With ARM you can easily manage attributes for users, groups or computers. All actions are automatically documented.

## Related features

[Modify attributes in bulk](#) (web client)

## Step-by-step process

The screenshot displays the SolarWinds Access Rights Manager (ARM) web interface. The search bar at the top is highlighted with a red box and labeled '1'. The main area shows a 'Graph' view with a tree on the left and a central graph. The 'Emily Employee (8man-demo\Emily Employee)' account is highlighted with a red box and labeled '2'. A context menu is open over this account, with 'Edit attributes' selected and labeled '3'. The right-hand pane shows the account's details, including a table of attributes and a photo.

Attribute	Value
Account Expires	Account never expires
Common Name	Emily Employee
Distinguished Name	CN=Emily Employee,OU=Demo...
Display Name	Emily Employee
Given Name	Emily
Logon	Never logged on
Manager	CN=David DO Marketing,OU=D...
Mail Address	E.Employee@8man-demo.local
Name (RDN)	Emily Employee
Object GUID	6dc747f6-ead9-421c-b9ae-1bc2...
Object SID	S-1-5-21-608986840-321788923...
Primary Group Id	513
User Account Name	Emily Employee
User Account Type	(803306368) User Object
DisplayName	Employee
Phone Number	0049 302 364 1834
User Account Control	66048 / 0x10200
User Account Control	This is a default account type th...
User Account Control	This password for this account wi...
User Principal Name	Emily.Employee@8man-demo.lo...
User Organizational Unit	OU=Demo Users,DC=8man-de...
User Organizational Unit	Demo Users

1. Use the search field to find the desired account.
2. Right-click the account, e.g. in the Accounts view.
3. Select "Edit attributes" from the context menu.

The screenshot shows the 'Edit attributes' dialog in the SolarWinds Access Rights Manager. The dialog is for the user 'Emily Employee (8man-demo\Emily Employee)'. It contains the following elements:

- Given Name:** Emily
- Surname:** Employee
- Creation rule for SAM Account Name:** User
- Buttons:** 'Reapply creation rules for all attributes' and 'Update values for attributes affected by the name'.
- Attribute List:** A table with columns 'Name' and 'Value'.
 

Name	Value
Account Expires	Account never expires
Common Name	Emily Employee
Comment	Attribute value is not given
Company	Attribute value is not given
Department	Attribute value is not given
Description	Attribute value is not given
Display Name	Emily Employee
Employee Id	Attribute value is not given
Job Category	Attribute value is not given
Home Directory	Attribute value is not given
Home Drive	Attribute value is not given
Home Phone	Attribute value is not given
Information	Attribute value is not given
Initials	Attribute value is not given
Manager	David DO Marketing
Mobile	Attribute value is not given
Personal Title	Attribute value is not given
- Comment Field:** A text area with the placeholder 'Please add a comment' and a warning icon.
- Buttons:** 'Immediately' (with a dropdown arrow) and 'Close'.

1. Change the desired attributes.

**i** Which attributes are available depends on the account type and on your [configuration of additional attributes](#).

2. You must enter a comment.

3. Start the execution.

"Soft" delete a user

## Background / Value

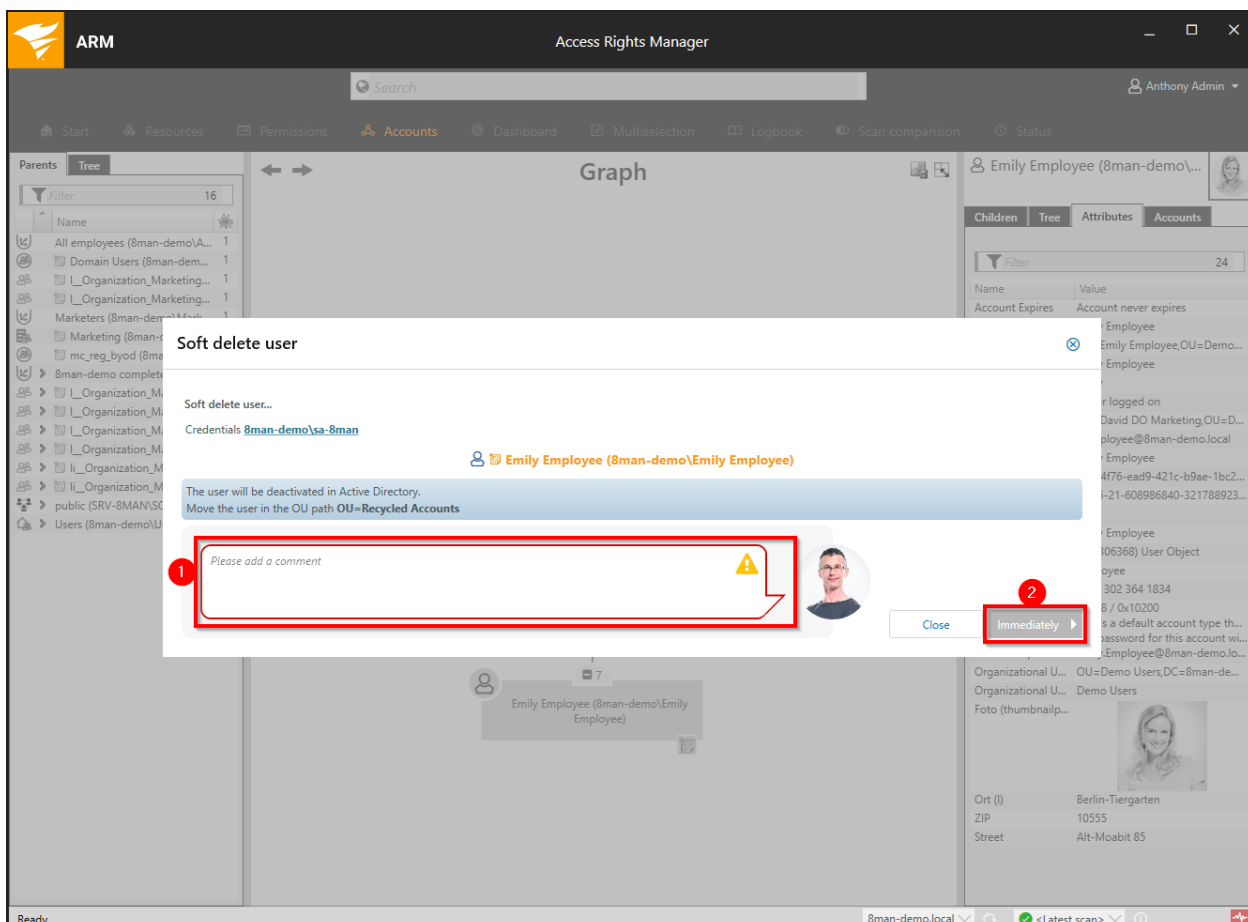
If a user is deleted with "Soft Delete", all his access rights are retained. The account is moved to a "Recycling OU" and deactivated. This account can no longer be used for a login. Set a strictly limited Group Policy for the "Recycling OU".

How to set the "Recycling OU" is described in the chapter "[AD change configuration](#)".

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The search bar at the top is highlighted with a red box and a red circle with the number 1. The main area displays a graph with nodes for "All employees (8man-demo\All employees)" and "Domain Users (8man-demo\Domain Users)". A context menu is open over the "Emily Employee (8man-demo\Emily Employee)" node, which is also highlighted with a red box and a red circle with the number 2. The "Soft delete user account" option in the context menu is highlighted with a red box and a red circle with the number 3. The right-hand pane shows the user's details, including name, email, and address.

1. Use the search field to find the desired user.
2. Right-click on the user, e.g. in the Accounts view.
3. Select "Soft delete account" from the context menu.



1. You must enter a comment, for example "ticket number" or "authorized by".
2. Start the process.

Remove a user and their permissions

## Background / Value

With ARM you can delete the user from AD and remove all of their access rights on the file server in one easy action.

## Related features

[Remove direct permissions in bulk](#) (web client)

## Step-by-step process

The screenshot displays the SolarWinds Access Rights Manager (ARM) web interface. The interface is divided into several sections:

- Search:** A search bar at the top left is highlighted with a red box and a red circle containing the number 1.
- Graph:** A central graph view shows a hierarchy of accounts. A node for "Emily Employee (8man-demo\Emily Employee)" is highlighted with a red box and a red circle containing the number 2.
- Context Menu:** A right-click context menu is open over the highlighted account. The "Delete account" option is highlighted with a red box and a red circle containing the number 3.
- Attributes Panel:** On the right side, a panel displays the attributes of the selected user, including name, email address, and organizational unit.

1. Use the search field to find the desired user.
2. Right-click the account, e.g. in the Accounts view.
3. Select "Delete account" from the context menu.

The screenshot shows the 'Delete account' dialog in the Access Rights Manager. The dialog is titled 'Delete account' and contains the following elements:

- Accounts to delete:** A table with one entry: 'Emily Employee (8man-demo\Emily Employee)'.
- Required credentials:** A table with two columns: 'Resource' and 'Credentials'. The entries are:
 

Resource	Credentials
8MAN-DEMO.LOCAL	8man-demo\sa-8man
srv-8man	8man-demo\sa-8man
- Remove access rights:** A checkbox that is checked. Below it, the text reads: 'Remove all direct references to the selected accounts on resources which are known to ARM. The execution will be *immediately*'.
- Scripting:** A text area with a dropdown arrow.
- Comment:** A text area with the placeholder text 'Please add a comment' and a warning icon.
- Buttons:** 'Close' and 'Immediately' (with a right-pointing arrow).

1. If necessary, change the credentials to delete the account and remove permissions.
2. Strongly recommended: Activate the option "Remove access rights" to avoid unresolved SIDs on file servers.
3. You must enter a comment, for example "ticket number" or "authorized by".
4. Start the process.



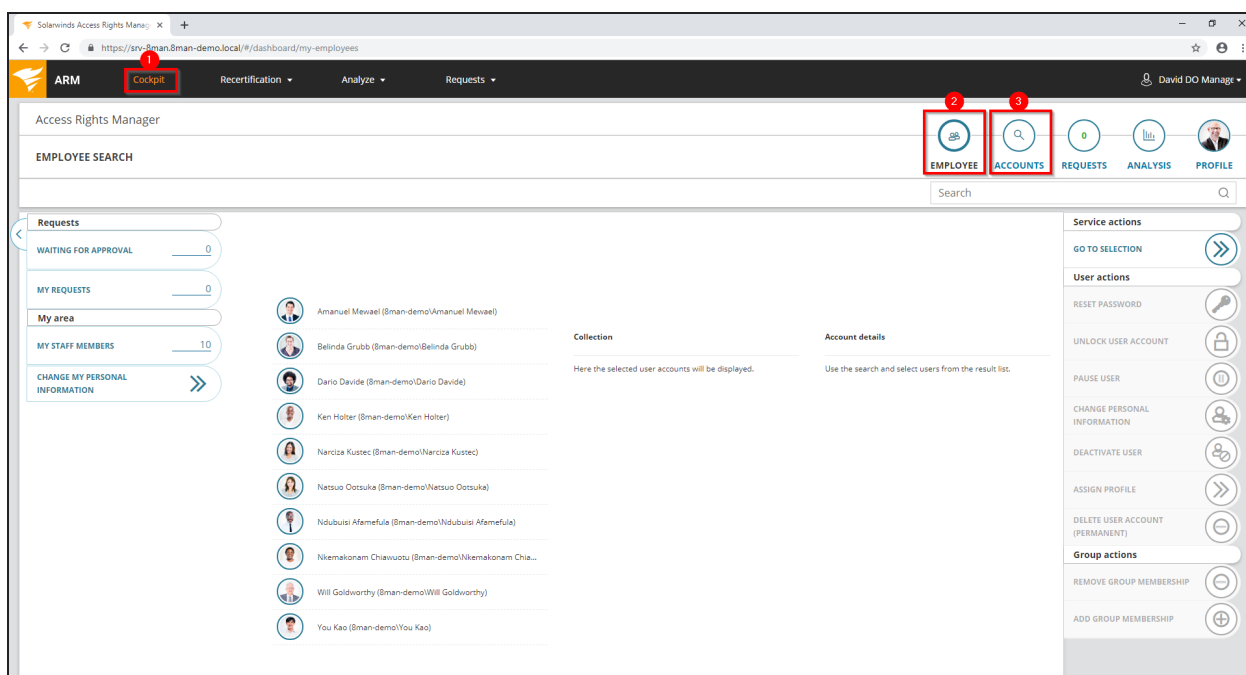
## Data Owner/Manager

Reset users' passwords (cockpit)


### Background / Value

Resetting passwords is one of the most common Helpdesk operations. ARM also allows you to delegate password resets to data owners or managers. The security-critical action is recorded in the logbook.

### Step-by-step process

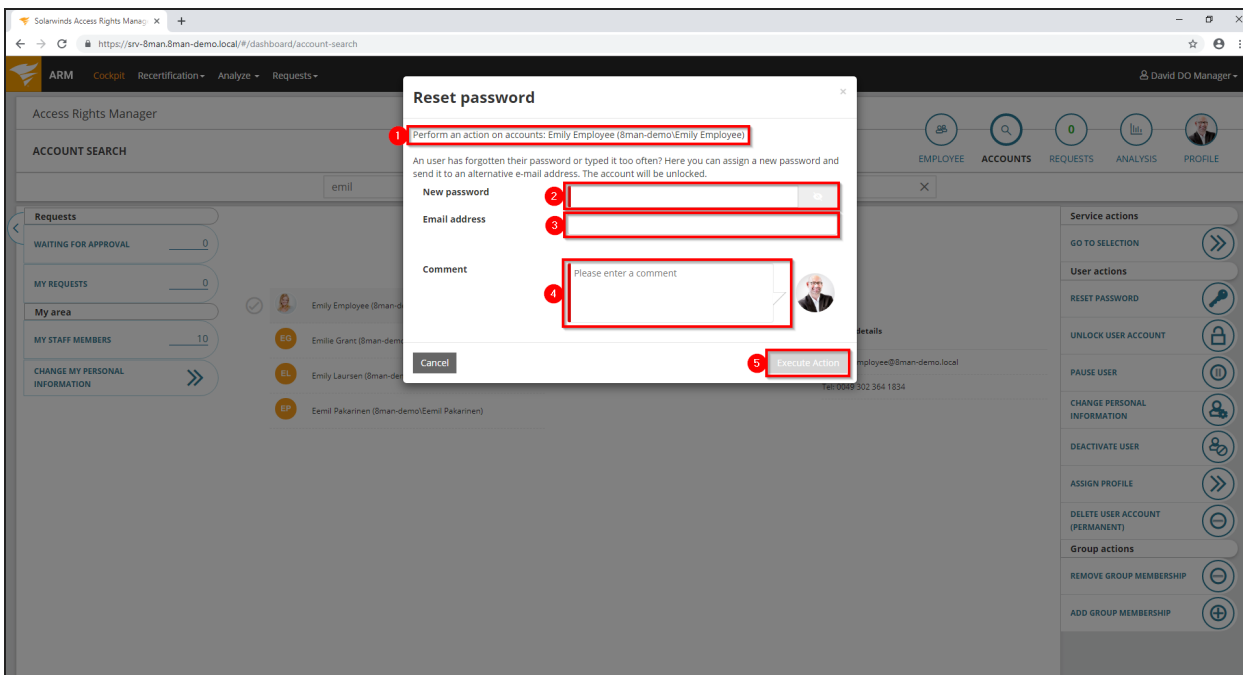


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the [Data Owner Configuration](#).

 The range of available services (buttons) varies according to role (login), risk assessment and configuration.

The screenshot shows the Solarwinds Access Rights Manager (ARM) interface. At the top, there's a navigation bar with 'ARM', 'Cockpit', 'Recertification', 'Analyze', and 'Requests'. Below that, the 'Access Rights Manager' title is visible. A search bar at the top right contains the text 'emil'. The main area displays a list of employees under the 'ACCOUNT SEARCH' section. The first employee, 'Emily Employee (Bman-demo/Emily Employee)', is selected, indicated by a checkmark and a red box (2). Below the list, a 'Collection' box shows the selected user (3). To the right, the 'Account details' for the selected user are displayed (4), including email and phone number. On the far right, a sidebar contains various actions, with 'RESET PASSWORD' highlighted (5).

1. Use the search to filter a long list of employees or search for users.
2. Select one or more users.
3. In the collection you can see already selected users.
4. ARM shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
5. Click "Reset Password".



1. ARM shows you which users you have selected and whose passwords you are resetting.
2. Assign a password. This password must be changed by the user when logging in for the next time.
3. Optional: Specify an email address to which the password will be sent.

**⚠ Choose an email address that the user can still receive.**

4. You must provide a reason for the password reset.
5. Click on "execute action".

If you are logged in as an administrator you will see two more options:

- The user must change the password at next logon
- unlock user account

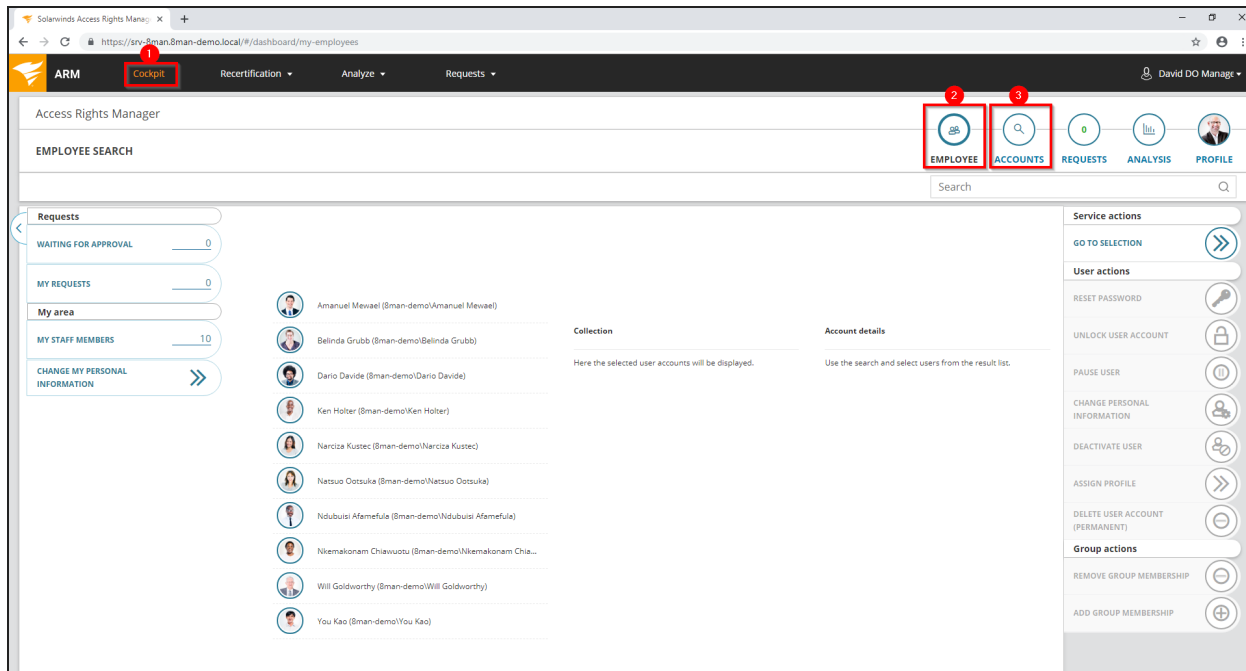
These options are always activated if logged in as a non-administrative user.

Change account data of users (cockpit)

## Background / Value

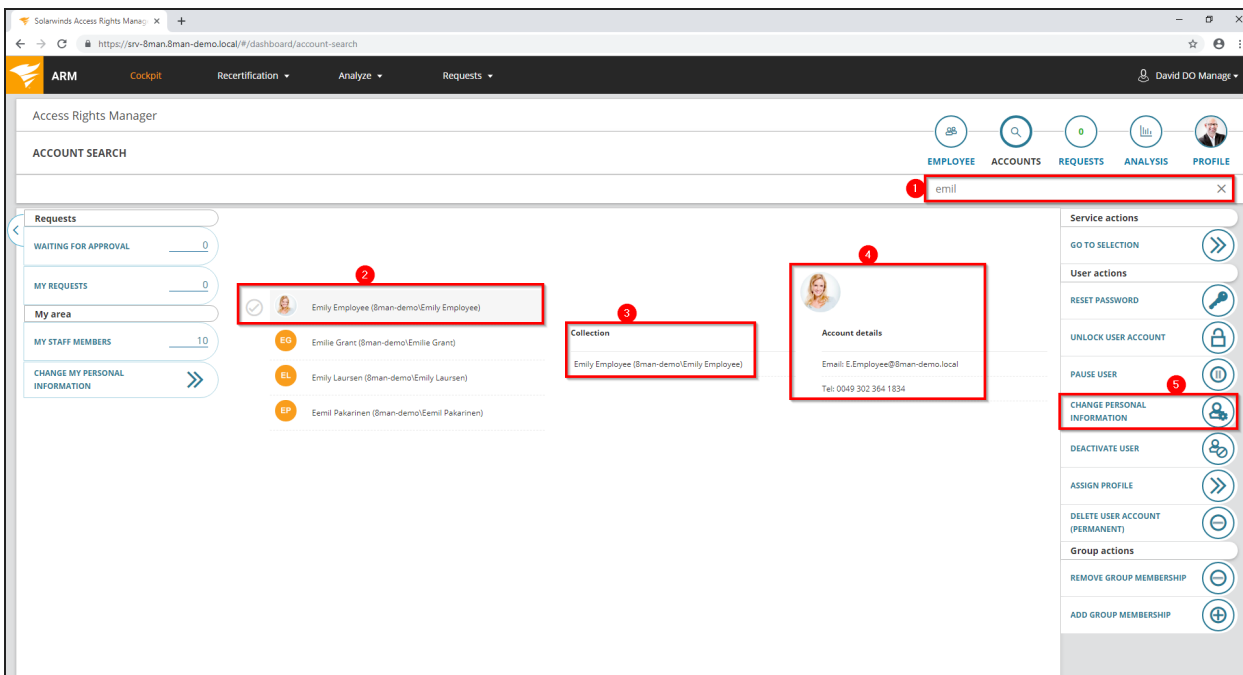
With ARM, you can quickly and easily change user account information, even from multiple users in one go. The actions are documented auditable.

## Step-by-step process

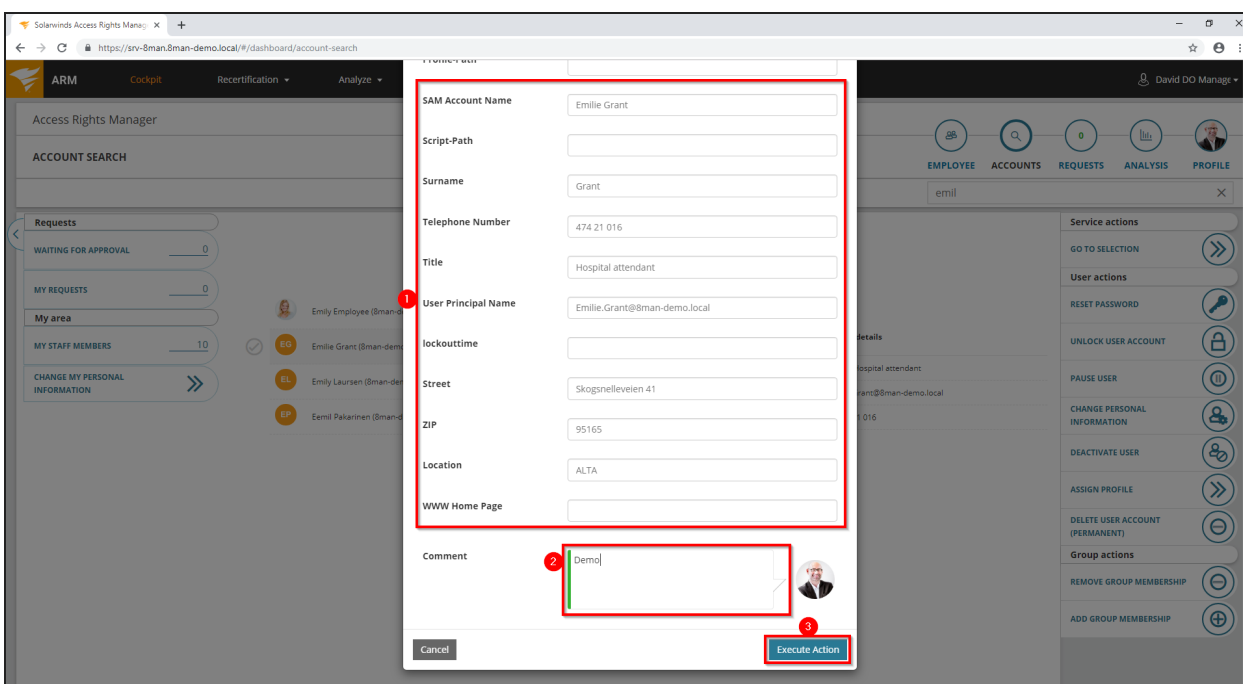


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.


**i** The range of available services (buttons) varies according to role (login), risk assessment and configuration.



1. Use the search to filter a long list of employees or search for users.
2. Select one or more users.
3. ARM shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
4. In the collection you can see already selected users.
5. Click "Change personal information".



1. Enter the desired changes.
2. You must enter a comment.
3. Click on "Execute Action".

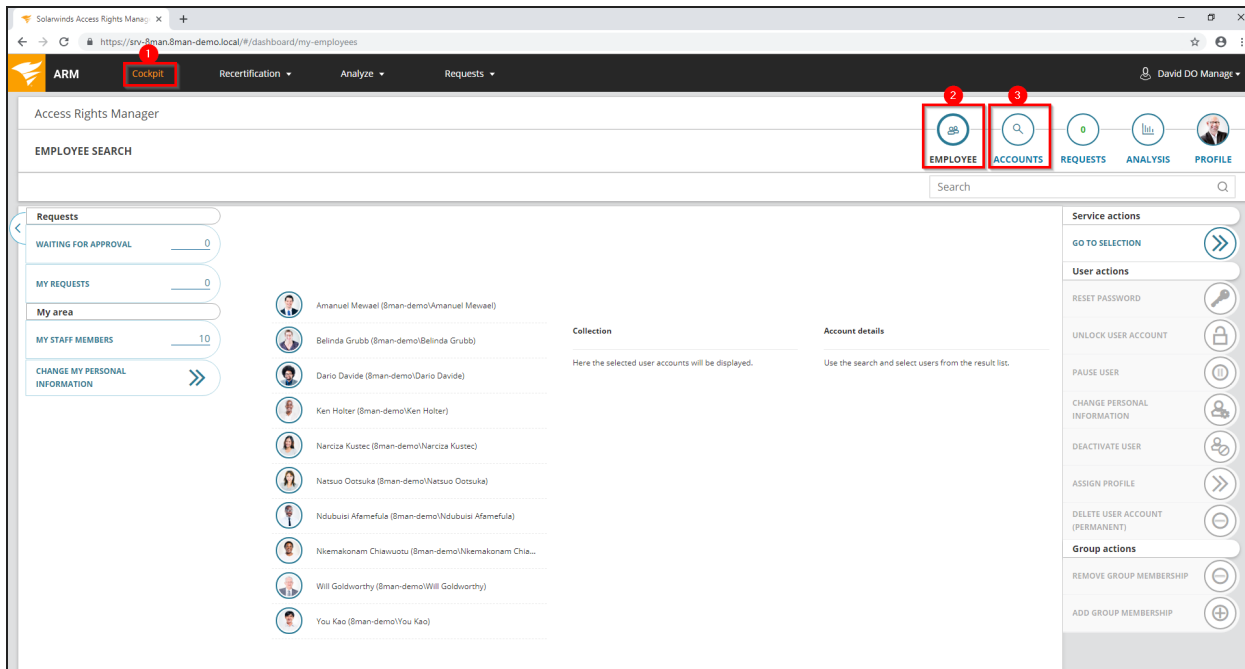
 The attributes displayed in the dialog can be adjusted by an administrator for each role. For this purpose, an adjustment of the configuration file must be made. Instructions can be found in the chapter [Set attributes available to web client scenarios](#).

## Deactivate users (cockpit)


### Background / Value

Disable a user in a few steps with ARM. Disable a user account early on discharge.

### Step-by-step process



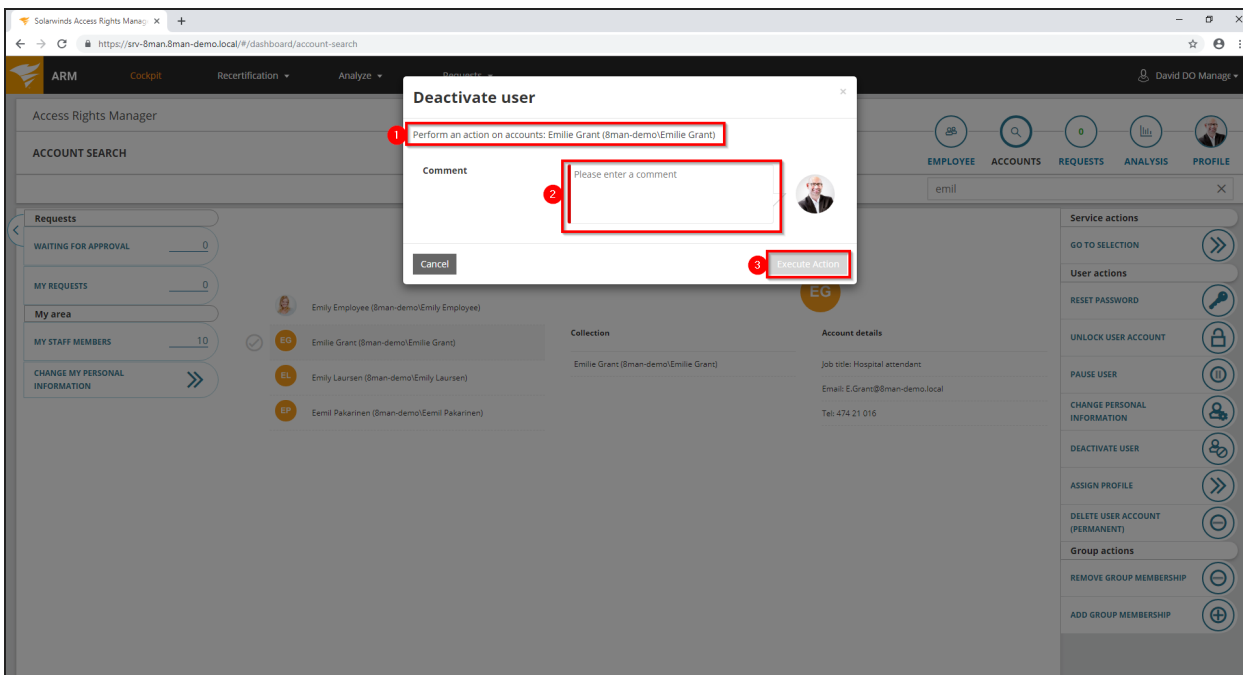
1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

 The range of available services (buttons) varies according to role (login), risk assessment and configuration.

The screenshot shows the Solarwinds Access Rights Manager (ARM) interface. The search bar at the top right contains the text "emil" (1). Below the search bar, a list of employees is displayed. The first employee, "Emily Employee (Bman-demo/Emily Employee)", is selected (2). A "Collection" box (3) shows the selected user. The "Account details" for the selected user are displayed (4), including the email "E.Employee@Bman-demo.local" and the telephone number "Tel: 0049 302 364 1834". The "Deactivate User" button is highlighted (5) in the right-hand sidebar.

1. Use the search to filter a long list of employees or search for users.
2. Select one or more users.
3. ARM shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
4. In the collection you can see already selected users.
5. Click "Deactivate user".





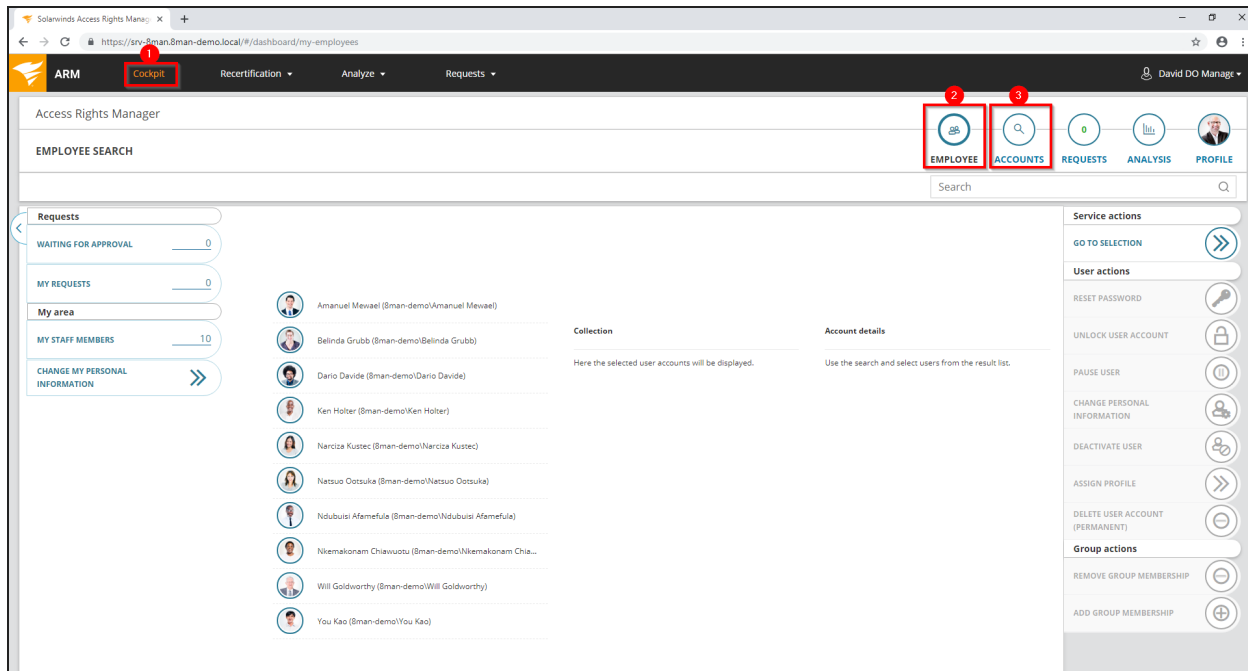
1. ARM shows you which accounts you have selected and want to deactivate.
2. You must enter a comment.
3. Click on "Execute Action".

Pause user (cockpit)


## Background / Value

Pause an employee in a few simple and quick steps, e.g. at parental leave.

## Step-by-step process



1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the [Data Owner Configuration](#).

 The range of available services (buttons) varies according to role (login), risk assessment and configuration.

The screenshot shows the Solarwinds Access Rights Manager (ARM) interface. The search bar at the top right contains the text "emil" (1). Below the search bar, a list of employees is displayed. The first employee, "Emily Employee (Bman-demo\Emily Employee)", is selected (2). A "Collection" box (3) shows the selected user. The "Account details" for the selected user are displayed (4), including the email "E.Employee@Bman-demo.local" and the telephone number "Tel: 0049 302 364 1834". The "PAUSE USER" button (5) is highlighted in the right-hand sidebar.

1. Use the search to filter a long list of employees or search for users.
2. Select one or more users.
3. ARM shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
4. In the collection you can see already selected users.
5. Click "Pause user".

Perform an action on accounts: Emilie Grant (8man-demo-Emilie Grant)

When you pause an employee, you revoke all permissions for a period of time, including the ability to log on to the domain.

**Timeframe**

Start date: April 10, 2019  
End date: April 10, 2019

April 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4

End date

April 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4

Comment

Please enter a comment

Cancel Execute Action

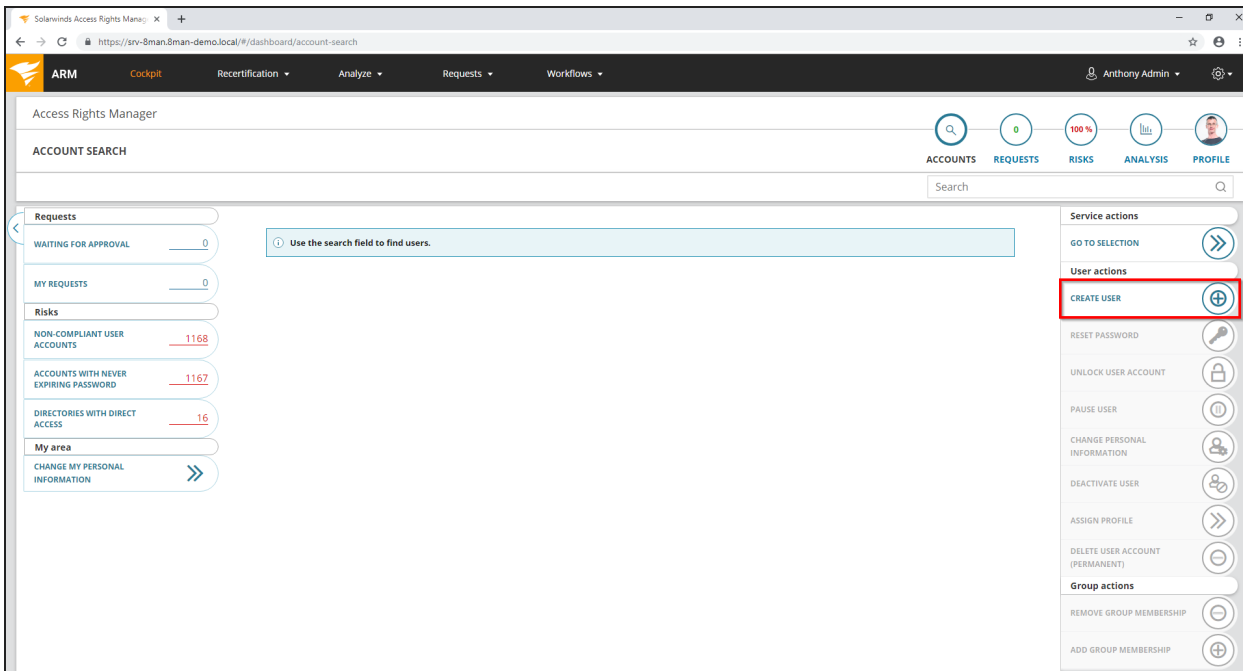
1. ARM shows you which accounts you have selected and want to pause.
2. ARM shows the start and end dates.
3. Set the beginning and the end.
4. If the break is perpetual, deactivate the option "End date".
5. You must enter a comment.
6. Click on "Execute Action".

Create a new user (cockpit)


## Background / Value

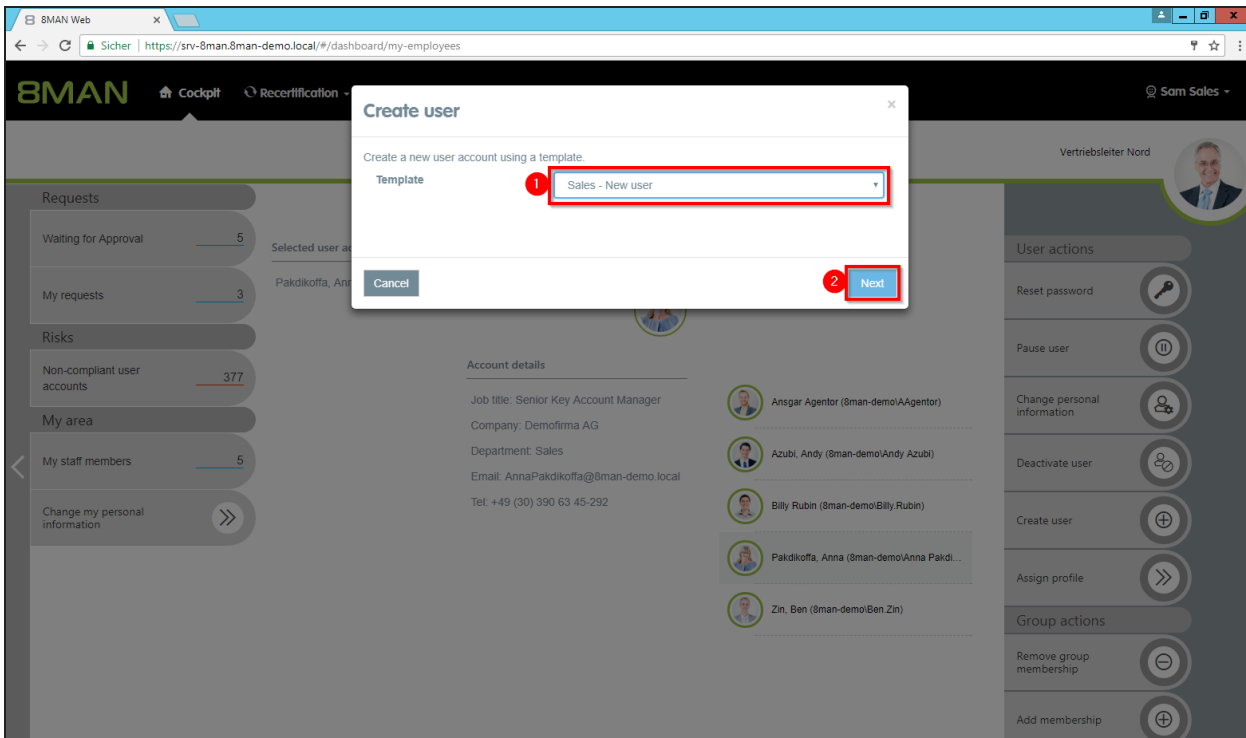
Create a new user in the web client. The creation is based on templates predefined by an administrator and is therefore efficient and standardized.

## Step-by-step process

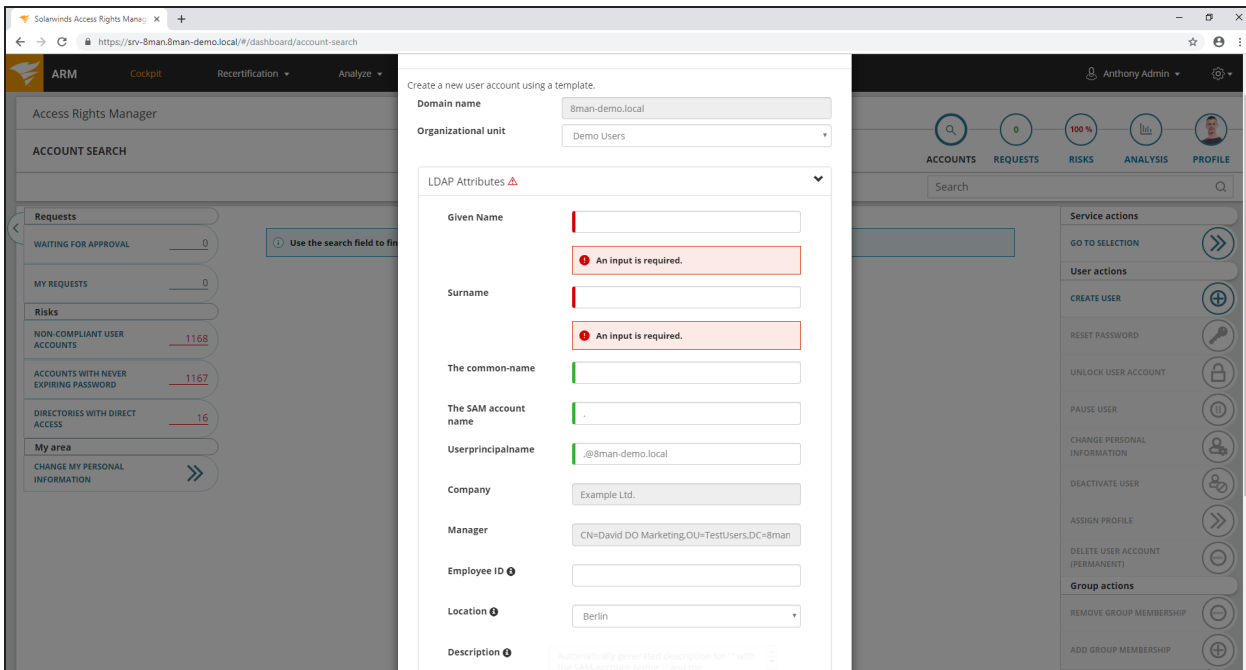


Click on "Create user" in the cockpit.

 The range of available services (buttons) varies according to role (login), risk assessment and configuration.



1. Select a template.
2. Click "Next".



Enter the required information.

**i** The amount of information required here can vary widely. User templates must be created by an administrator.

The screenshot displays the Solarwinds Access Rights Manager (ARM) interface. The main content area shows a form for creating or editing an account. The form includes the following fields:

- The SAM account name: [ ]
- Userprincipalname: [ @sman-demo.local ]
- Company: [ Example Ltd. ]
- Manager: [ CN=David DO Marketing,OU=TestUsers,DC=sman ]
- Employee ID: [ ]
- Location: [ Berlin ]
- Description: [ Automatically generated description for ' ' with the SAM Account Name ' ' and the ' ' ]

Below these fields are sections for "Password options" and "Create an Exchange mailbox". At the bottom of the form, there is a "Comment" field with a red box around it and a red "1" next to it, indicating that a comment must be entered. The "Execute Action" button is also highlighted with a red box and a red "2" next to it, indicating that it must be clicked.

1. You must enter a comment.
2. Click on "Execute Action".

Assign a department profile to users (cockpit)

## Background / Value

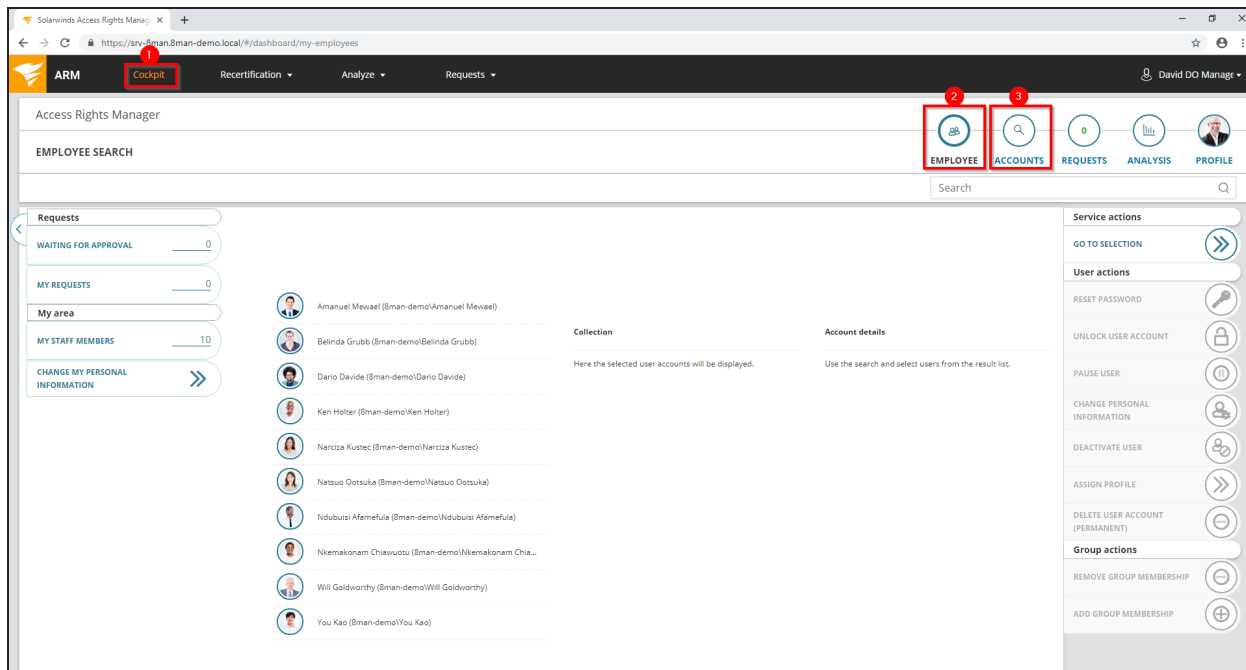
With a department profile, you can assign a basic set of permissions to a user in just a few clicks. If the employee changes department, the supervisor can easily apply his department profile to the corresponding user account.

## Related features

[Create a new department profile](#)

[Determine permissions deviating from the department profile \(Compliance Check\)](#)

## Step-by-step process



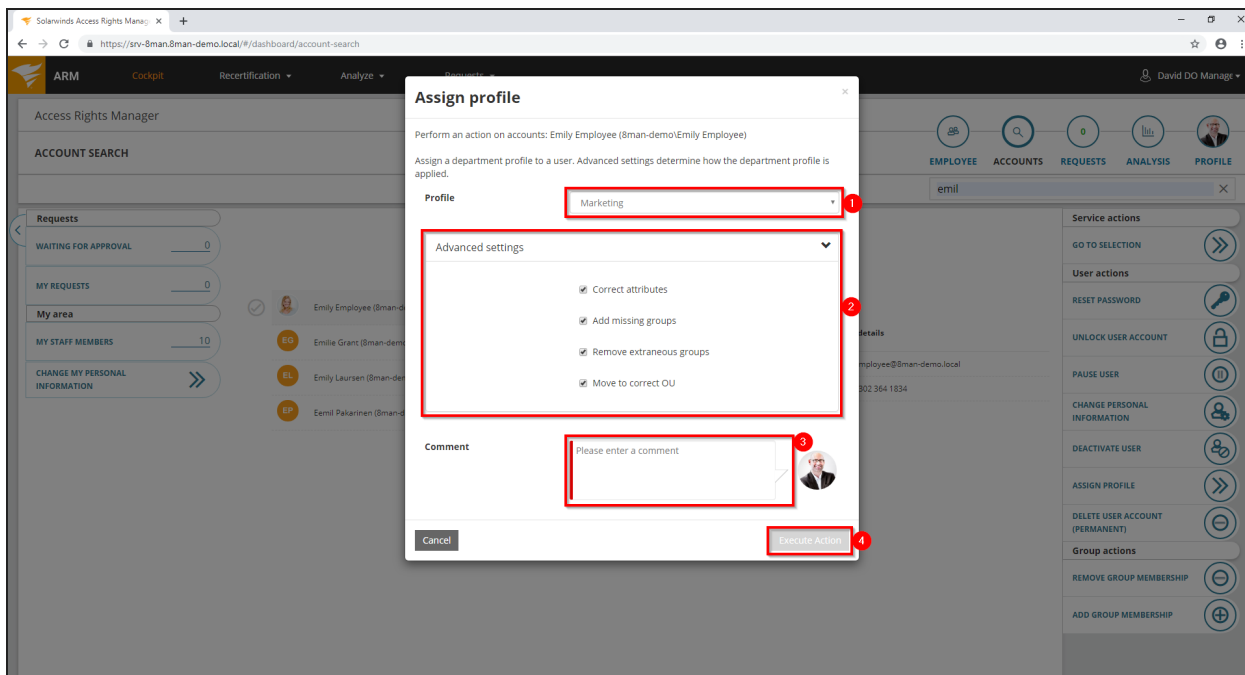
1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

**i** The range of available services (buttons) varies according to role (login), risk assessment and configuration.



The screenshot shows the Solarwinds Access Rights Manager (ARM) interface. At the top, there's a navigation bar with 'ARM', 'Cockpit', 'Recertification', 'Analyze', and 'Requests'. The main area is titled 'Access Rights Manager' and 'ACCOUNT SEARCH'. A search bar at the top right contains the text 'emil'. Below the search bar, there are several tabs: 'EMPLOYEE', 'ACCOUNTS', 'REQUESTS', 'ANALYSIS', and 'PROFILE'. The 'EMPLOYEE' tab is active. On the left, there are several filters: 'Requests' (0), 'WAITING FOR APPROVAL' (0), 'MY REQUESTS' (0), 'My area', 'MY STAFF MEMBERS' (10), and 'CHANGE MY PERSONAL INFORMATION'. The main content area shows a list of users. The first user, 'Emily Employee (Bman-demo\Emily Employee)', is selected and highlighted with a red box (2). Below this, there are three other users: 'Emilie Grant (Bman-demo\Emilie Grant)', 'Emily Laursen (Bman-demo\Emily Laursen)', and 'Eemil Pakarinen (Bman-demo\Eemil Pakarinen)'. A 'Collection' box (3) shows the selected user. To the right, an 'Account details' box (4) displays the user's email and phone number. On the right-hand side, there is a 'Service actions' menu with various options. The 'ASSIGN PROFILE' button is highlighted with a red box (5).

1. Use the search to filter a long list of employees or search for users.
2. Select one or more users.
3. In the collection you can see already selected users.
4. ARM shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
5. Click "Assign profile".



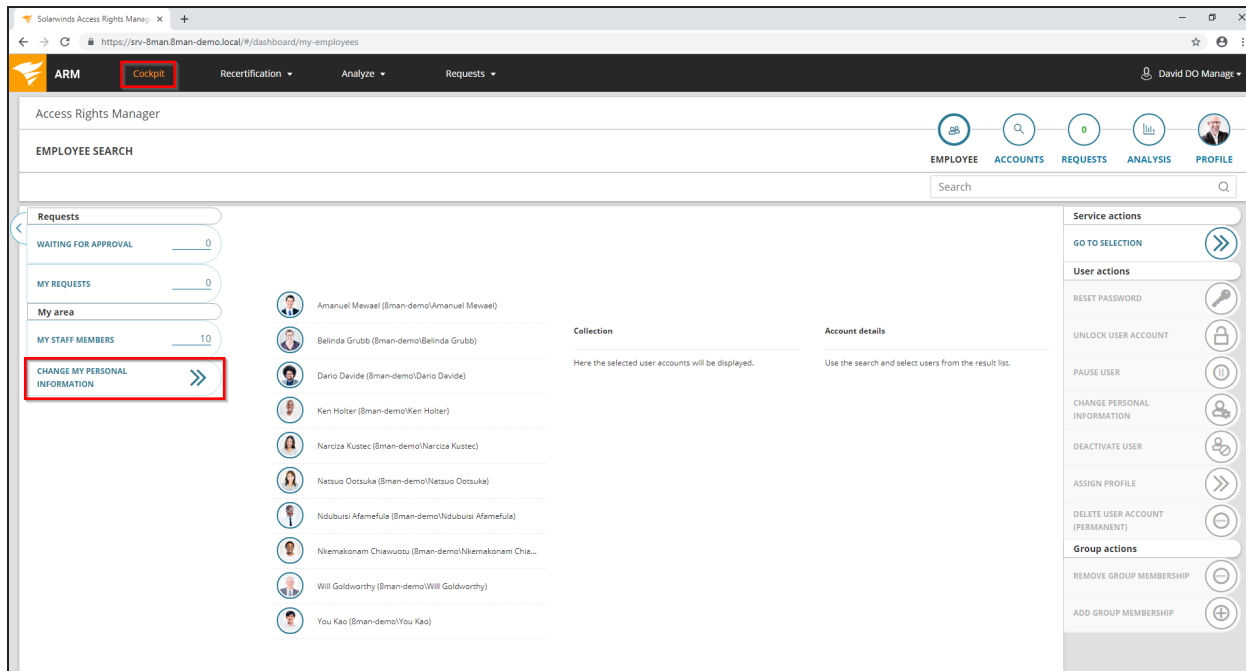
1. Choose a department profile.
2. In the advanced settings, specify how the department profile is applied.
3. You must enter a comment.
4. Click on "Execute Action".

Change your own account information (cockpit)


## Background / Value

With ARM you can quickly and easily change your own account information. The actions are documented in the logbook.

## Step-by-step process



Click on "Change my personal information" in the cockpit.

 The range of available services (buttons) varies according to role (login), risk assessment and configuration.

The screenshot shows the 'Edit User' dialog box in the SolarWinds Access Rights Manager. The dialog box is titled 'Edit User' and contains the following fields:

- SAM Account Name: David DO Manager
- Script-Path: (empty)
- Surname: DO Manager
- Telephone Number: 0049 301 689 9874
- Title: (empty)
- User Principal Name: David.DO.Manager@8man-demo.local
- lockouttime: (empty)
- Street: Saatwinkler Damm 27
- ZIP: 13627
- Location: Berlin-Charlottenburg
- WWW Home Page: (empty)
- Comment: Please enter a comment

Red boxes and numbers 1, 2, and 3 highlight the 'SAM Account Name' field, the 'Comment' field, and the 'Execute Action' button respectively.

1. Change your account information.
2. You must enter a comment.
3. Click on "Execute Action".

**i** The attributes displayed in the dialog can be adjusted by an administrator. Please refer to the chapter [Set attributes available to web client scenarios](#).

## Manage my employees (cockpit)

### Background / Value

With ARM you can quickly and easily manage your assigned employees. Actions are documented in the logbook.

**i** Employees are users which attribute "Manager" in Active Directory is assigned to you. Ask your administrator.

### Step-by-step process

The screenshot shows the Solarwinds Access Rights Manager (ARM) interface. The top navigation bar includes 'ARM', 'Cockpit' (highlighted with a red box and a '1'), 'Recertification', 'Analyze', and 'Requests'. The main content area is titled 'Access Rights Manager' and 'EMPLOYEE SEARCH'. On the left, there are several buttons: 'Requests', 'WAITING FOR APPROVAL', 'MY REQUESTS', 'My area' (highlighted with a red box and a '3'), 'MY STAFF MEMBERS' (highlighted with a red box and a '2'), and 'CHANGE MY PERSONAL INFORMATION'. The 'MY STAFF MEMBERS' button shows a count of '10'. Below this, a list of employees is displayed, including Amanuel Mewael, Belinda Grubb, Dario Davide, Ken Holter, Narciza Kustec, Natsuo Ootsuka, Ndubusi Afamefula, Nkemakonam Chiauustu, Will Goldwarthy, and You Kao. On the right, there are sections for 'Collection' and 'Account details', and a 'Service actions' sidebar with various user management options like 'GO TO SELECTION', 'User actions', 'RESET PASSWORD', 'UNLOCK USER ACCOUNT', 'PAUSE USER', 'CHANGE PERSONAL INFORMATION', 'DEACTIVATE USER', 'ASSIGN PROFILE', 'DELETE USER ACCOUNT (PERMANENT)', and 'Group actions'.

1. Select "Cockpit".
2. The number on the button indicates how many employees are assigned to you.
3. Click "My staff members".

**i** The range of available services (buttons) varies according to role (login), risk assessment and configuration.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The main area displays a table of staff members under the heading "MY STAFF MEMBERS (10)". The table has columns for "Type", "Name", "Image", and "Requested Action". A red box labeled "1" highlights the selection checkboxes in the "Type" column. A red box labeled "2" highlights the "3 columns selected" dropdown menu above the table. A red box labeled "3" highlights the "Reports" sidebar on the right, which includes options like "Direct Excel export", "Create Report", "Reset password", "Unlock user account", "Pause user", "Change personal information", "Deactivate user", "Remove group membership", "Add group membership", "Assign profile", "Delete user account (permanent)", and "Execute script". A red box labeled "4" highlights the action buttons for the selected user "Dario Davide".

Type	Name	Image	Requested Action
<input type="checkbox"/>	Amanuel Mewael (8man-demo\Amanuel Mewael)		
<input type="checkbox"/>	Belinda Grubb (8man-demo\Belinda Grubb)		
<input checked="" type="checkbox"/>	Dario Davide (8man-demo\Dario Davide)		
<input type="checkbox"/>	Ken Holter (8man-demo\Ken Holter)		
<input type="checkbox"/>	Narciza Kustec (8man-demo\Narciza Kustec)		
<input type="checkbox"/>	Natsuo Ootsuka (8man-demo\Natsuo Ootsuka)		
<input type="checkbox"/>	Ndubuisi Afamefua (8man-demo\Ndubuisi Afamefua)		
<input type="checkbox"/>	Nkemakonam Chlawuotu (8man-demo\Nkemakonam C)		
<input type="checkbox"/>	Will Goldworthy (8man-demo\Will Goldworthy)		
<input type="checkbox"/>	You Kao (8man-demo\You Kao)		

1. Select employees.
2. Adjust which columns are displayed.
3. Export the list to Excel or PDF.
4. Perform actions on the selected employee accounts.

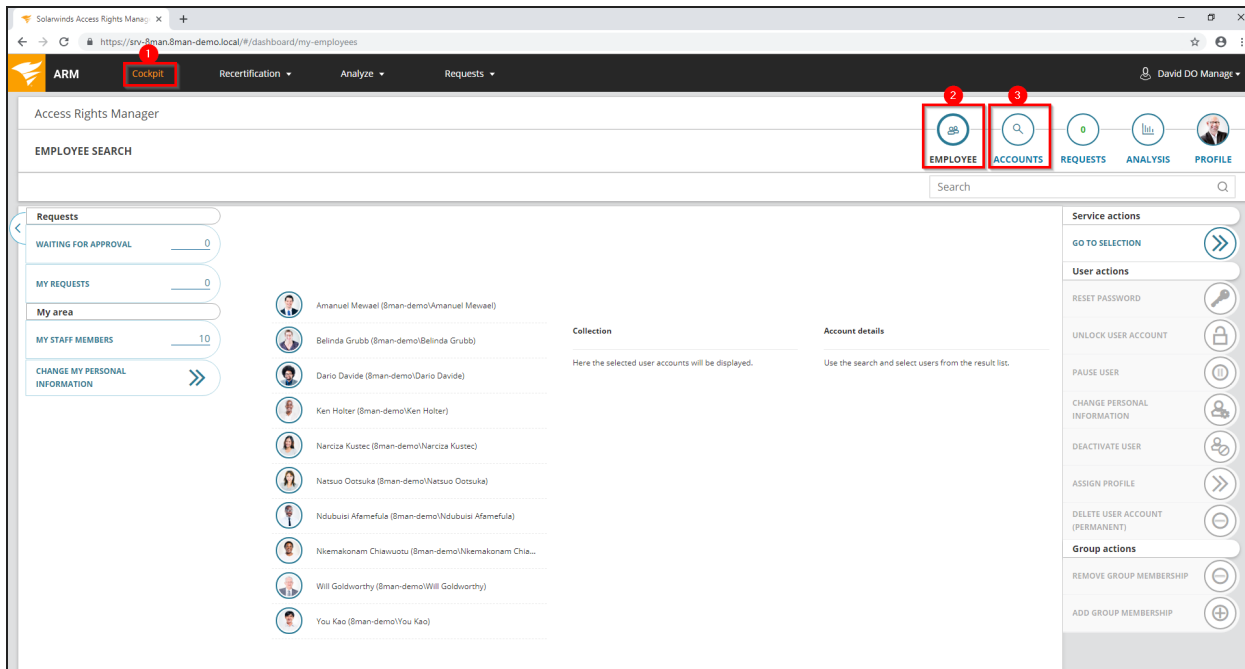
The range of available services (buttons) varies according to configuration.

Add group memberships (cockpit)


## Background / Value

If a manager finds that his employee lacks group membership, he can add it in a few simple steps.

## Step-by-step process



1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the [Data Owner Configuration](#).

 The range of available services (buttons) varies according to role (login), risk assessment and configuration.

1. Use the search to filter a long list of employees or search for users.
2. Select one or more users.
3. In the collection you can see already selected users.
4. ARM shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
5. Click "Add group memberships".



The screenshot shows the 'Add group membership' dialog box in the SolarWinds Access Rights Manager. The dialog is titled 'Add group membership' and contains the following elements:

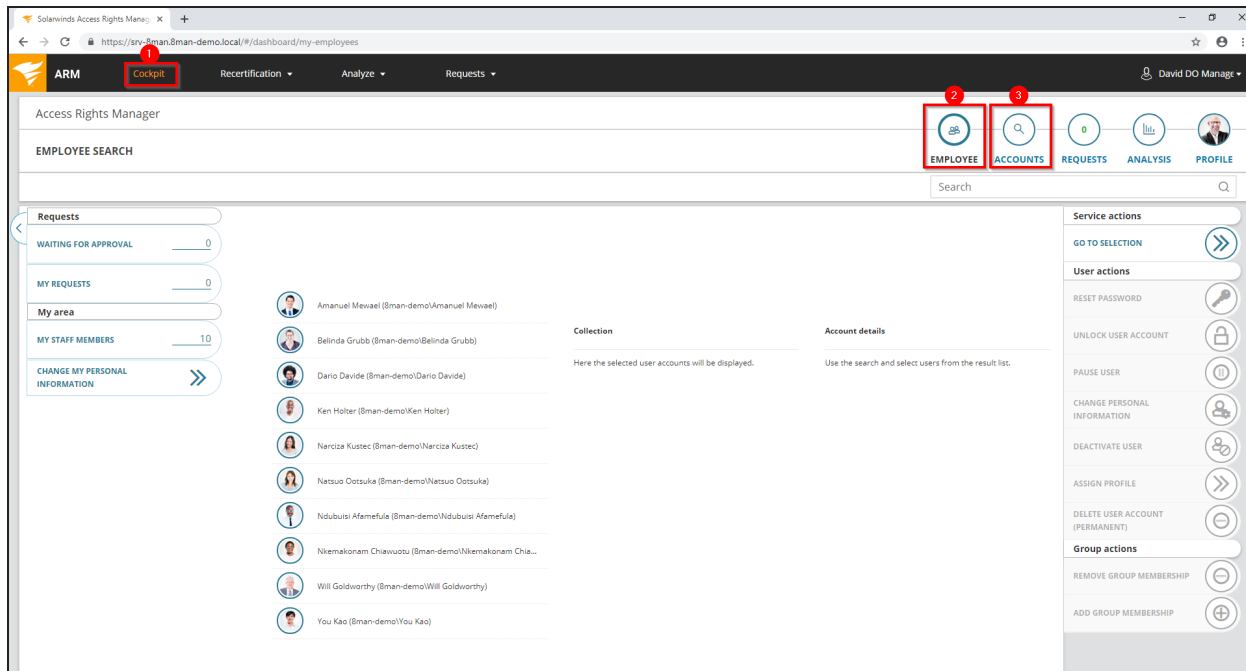
- 1:** A red box highlights the text 'Perform an action on accounts: Belinda Grubb (sman-demo\Belinda Grubb)'.
- 2:** A red box highlights the search bar with the text 'Search for group' and a dropdown arrow.
- 3:** A red box highlights the 'Marketing (sman-demo\Marketing)' group name.
- 4:** A red box highlights the 'Timeframe' section, which includes a calendar for April 2019 with the start date set to 'April 12, 2019'.
- 5:** A red box highlights the 'Comment' field with the placeholder text 'Please enter a comment'.
- 6:** A red box highlights the 'Execute Action' button.

1. ARM shows you which accounts you have selected.
2. Search for and add groups.
3. Optional: Remove already selected groups.
4. You can set a start and end date for the group memberships.
5. You must enter a comment.
6. Click on "Execute Action".

## Remove group memberships (cockpit)

**Background / Value**

Excessive access rights are often caused by group memberships. In the cockpit, you can quickly remove group memberships.

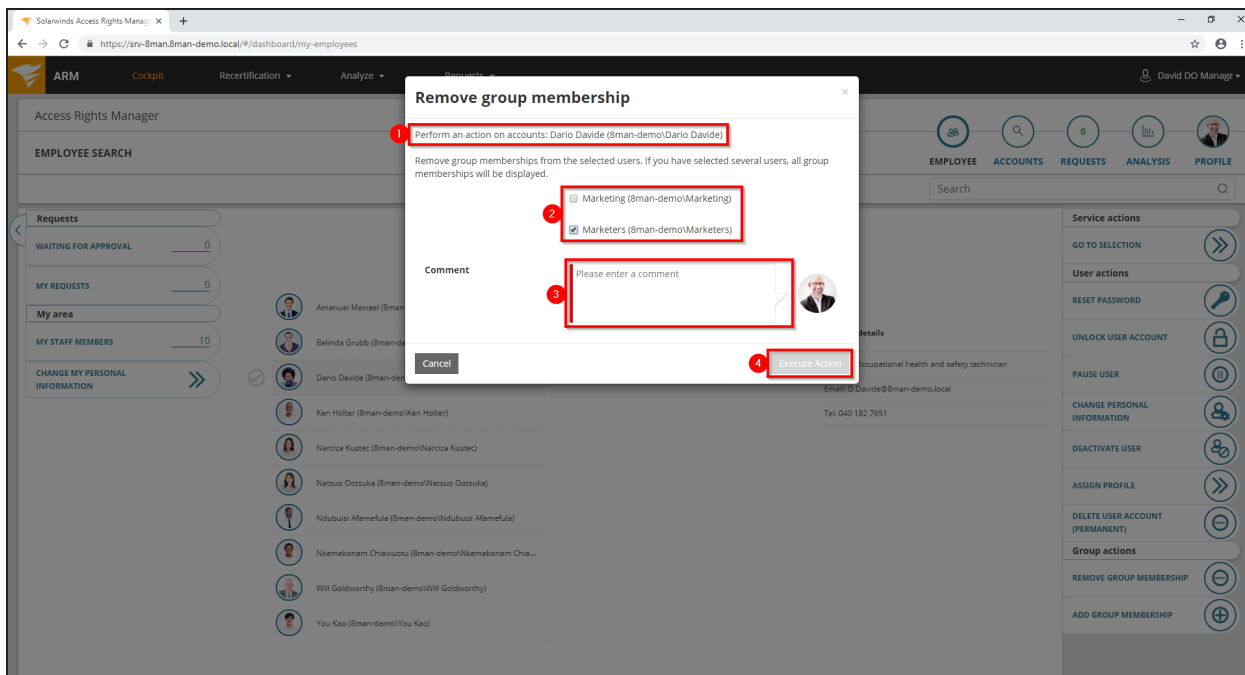
**Step-by-step process**

1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the [Data Owner Configuration](#).

**i** The range of available services (buttons) varies according to role (login), risk assessment and configuration.

The screenshot displays the Solarwinds Access Rights Manager (ARM) interface. At the top, there is a navigation bar with 'ARM', 'Cockpit', 'Recertification', 'Analyze', and 'Requests' tabs. The main header shows 'Access Rights Manager' and 'ACCOUNT SEARCH'. A search bar at the top right contains the text 'emil'. Below the search bar, there are several tabs: 'EMPLOYEE', 'ACCOUNTS', 'REQUESTS', 'ANALYSIS', and 'PROFILE'. The main content area shows a list of users with a search filter applied. The first user, 'Emily Employee (Bman-demo/Emily Employee)', is selected and highlighted with a red box labeled '2'. To the right of this user, there is a 'Collection' box labeled '3' containing the same user name. Further right, an 'Account details' box labeled '4' shows the user's email and telephone number. On the right side of the interface, there is a sidebar with various actions. The 'Group actions' section is highlighted with a red box labeled '5', and the 'REMOVE GROUP MEMBERSHIP' button is specifically highlighted.

1. Use the search to filter a long list of employees or search for users.
2. Select one or more users.
3. ARM shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
4. In the collection you can see already selected users.
5. Click "Remove group memberships".



1. ARM shows you which accounts you have selected.
2. Select at least one group.
3. You must enter a comment.
4. Click "Execute Action".

## File server


ARM provides many features to manage file server permissions and security risks.

### Grant and remove file server access rights

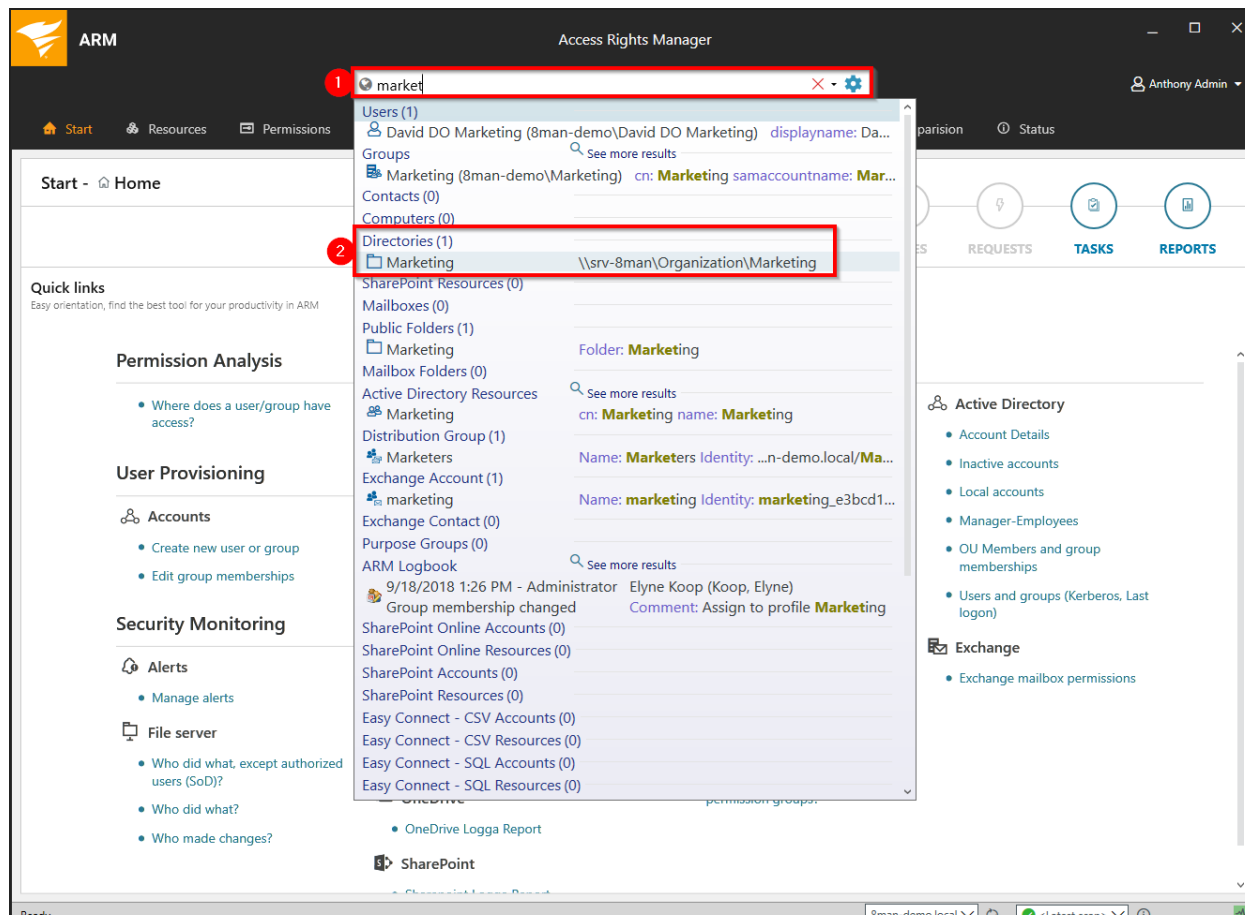
#### **Background / Value**

Access rights should be easy to assign and revoke. So Data Owners and Managers can also do this quickly and easily for the employees in their department. No special knowledge of Active Directory and / or file servers is needed.

Simply decide what type of access rights you would like to assign: modify or read.

 In order to maintain data integrity we recommend assigning modify permissions only to carefully selected employees.

## Step-by-step process



1. Use the search field to find the desired directory.
2. Click on the search result in the directories section.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The main window is titled 'ARM Access Rights Manager' and has a search bar and a user profile 'David DO Manager'. The interface is divided into several sections:

- Resources:** A tree view on the left shows a file server structure. The 'Events' directory under 'Marketing' is selected, and a context menu is open over it. The menu options include 'Rescan directory', 'Report: Who has access where?', 'Modify access rights...', 'Create directory', 'Delete directory', 'Open Logbook', and 'Copy as path'. The 'Modify access rights...' option is highlighted with a red box.
- Events:** A panel on the right shows the selected directory's details, including the owner 'Domain Admins', inheritance status 'On', and a table of NTFS permissions.
- NTFS:** A table showing permissions for 'Full control', 'Modify', and 'Read and Execute' with columns for Inheritance, Full control, Modify, Restricted..., Read and Ex..., Write, Read, and Propagation.
- Accounts with permissions:** A list of 14 accounts with their names and the number of times permissions were granted.

Name	how often granted
Adam Adminmanager (8man-demo\Adam Adminmanager)	1
Administrator (8man-demo\Administrator)	1
Alberte Lorenzen (8man-demo\Alberte Lorenzen)	1
Anthony Admin (8man-demo\Anthony Admin)	1
Antoine Admin (8man-demo\Antoine Admin)	1
Anton Admin (8man-demo\Anton Admin)	1
Caroline Berggren (8man-demo\Caroline Berggren)	1
David DO Marketing (8man-demo\David DO Marketing)	1
Elyne Koop (8man-demo\Elyne Koop)	1
Emily Employee (8man-demo\Emily Employee)	2

1. ARM switches to the "Resources" view with the desired directory in focus.
2. Select a sub-directory if desired by right-clicking on it.
3. Select "Modify access rights..."

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes the ARM logo, a search bar, and the user name "David DO Manager". The main interface is divided into several sections:

- Permissions View:** A red box labeled "1" highlights the "Permissions" tab in the top navigation bar.
- Resource Path:** A red box labeled "2" highlights the breadcrumb navigation path: "File server > srv-8man > Organization > Marketing > Events".
- Resource Details:** The main area shows details for the "Events" directory, including its path, owner, and inheritance status. A red box labeled "3" highlights the "Modify" and "Read & execute" permission tables.
- Permission Tables:**

Modify		Read & execute	
Name		Name	
		Emily Employee (8man-demo\Emily Employee)	
- Children Panel:** A panel on the right side shows a filter for "Children" with options for "Users", "Groups", "Contacts", and "Computers".

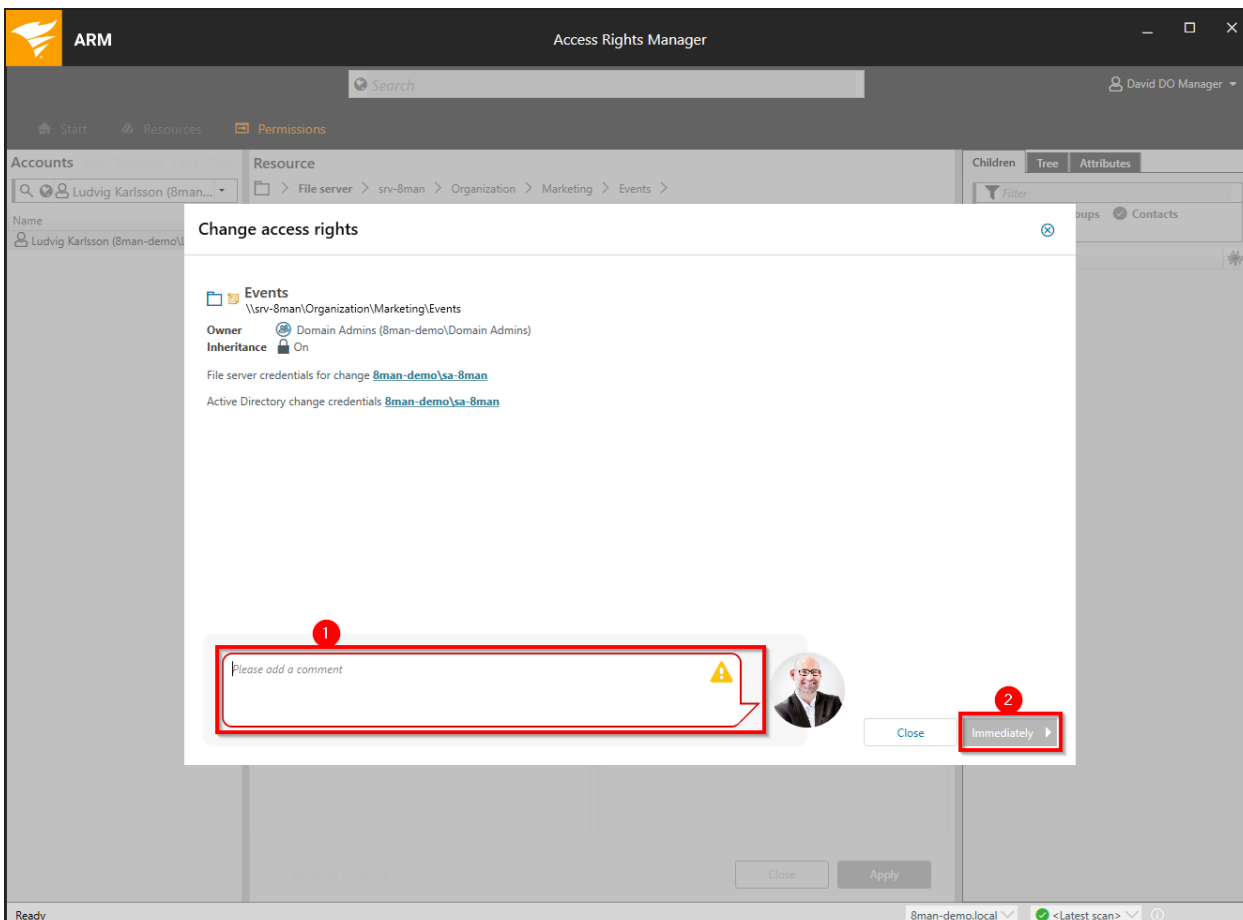
At the bottom of the interface, there are "Close" and "Apply" buttons, and a status bar showing "Ready" and system information.

1. ARM switches to the "Permissions" view.
2. ARM shows you the directory that you are working on. You can change this directory.
3. ARM shows you all existing access rights in the categories "Modify" and "Read & execute".



The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', and 'Permissions'. The main area is divided into 'Accounts' and 'Resource' sections. In the 'Accounts' section, a search bar contains 'Ludvig Karlsson...' and a red box highlights the search field with a red circle '1'. Below the search bar, a list of accounts shows 'Ludvig Karlsson (8man-demo\Ludvig Ka...)' with a red box around it and a red arrow pointing to the 'Modify' column, labeled with a red circle '2'. The 'Modify' column contains a table with columns for 'Name' and 'Read & execute'. The 'Read & execute' column shows 'Emily Employee (8man-demo\Emily Employeee)' with a red box around it and a red circle '3'. A context menu is open over this entry, with the 'Remove' option highlighted by a red box and a red circle '3'. At the bottom right, the 'Apply' button is highlighted with a red box and a red circle '4'. The right-hand pane shows details for the selected user, including 'Name', 'Account Expires', 'Common Name', 'Distinguished Name', 'Display Name', 'Telephone Number', 'User Account Control', 'User Principal Name', 'Organizational Unit', and 'Foto (thumbnail...)'.

1. Use the search field to find the desired user or group.
2. Use drag & drop to move the users into a column and assign corresponding access rights.
3. Right-click on a user and select "Remove" from the context menu to revoke access.
4. Click "Apply".



1. You must enter a comment.
2. Start the execution.

## Remove multiple access paths to file server directories

### Background / Value

Multiple access rights often occur through nested AD group memberships. They are often a symptom of a confusing group and AD structure. Access rights to a particular resource should only be achieved through one group membership. ARM allows you to remove multiple access paths quickly and easily.

## Step-by-step process

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The left pane shows a tree view of resources under 'Active Directory' and 'File server'. The right pane shows the 'Events' resource selected, with a context menu open over the 'Accounts with permission' section. The context menu includes options like 'Show in accounts view...' and 'Show access rights to resources...'. The 'Accounts with permission' section lists three access paths for the account 'Emily Employee (8man-demo)'. Red boxes and numbers 1 and 2 highlight the account and the 'Show in accounts view...' option, respectively.

Resources

Filter resources on first tree level

Active Directory

File server

Organization

Events

Owner: Domain Admins (8man-demo\Domain Admins)

Inheritance: On

Access rights: Full control, Modify

Accounts with permission

emil

Users Groups

Emily Employee (8man-demo)

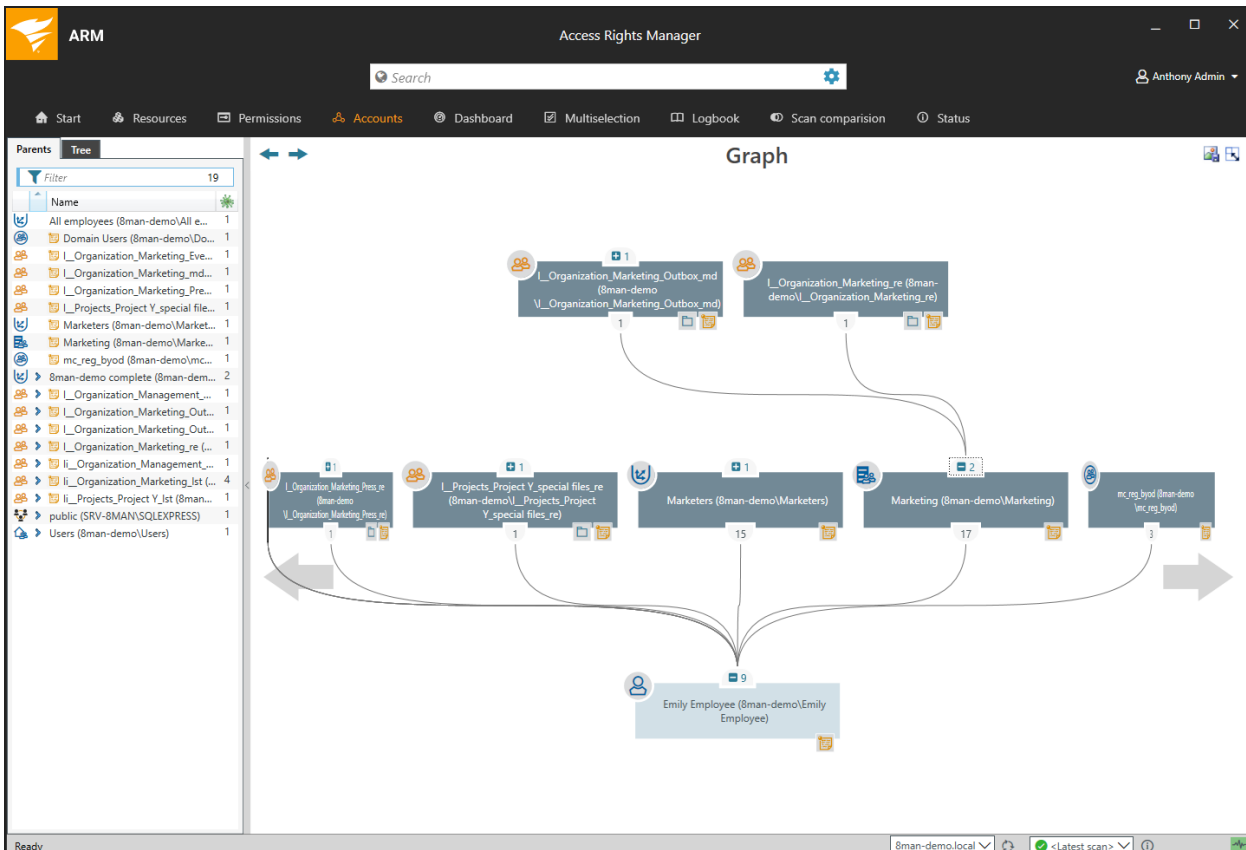
3 Access paths

Modify\\_\_Organization\_Marketing\_md (8man-demo)\Marketing (8man-demo)\Emily Employee

Modify\\_\_Organization\_Marketing\_md (8man-demo)\Emily Employee (8man-demo)

Modify\Emily Employee (8man-demo)

1. You have identified "Emily Employee" as having [multiple access paths](#).
2. Right-click on the account and select "Show in account view" from the context menu.



Use the AD graph to analyze multiple access paths.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The user is logged in as 'Anthony Admin'. The main area is titled 'Graph' and shows a network of accounts and their relationships. A context menu is open over the 'Emily Employee (8man-demo\Emily Employee)' account, with the option 'Change group memberships...' highlighted in red. The context menu includes various actions such as 'Select account', 'Show in Resources View...', 'Report: Where has the user/group access?', 'Report: Account Details', 'Create new user or group', 'Unlock user', 'Deactivate account', 'Change password options', 'Reset user password', 'Soft delete user account', 'Delete account', 'Edit attributes', 'Move object', 'Enable mailbox', 'Add note', 'Open Logbook', 'Create alert', and 'Copy as path'. The left sidebar shows a 'Tree' view of the account hierarchy, and the bottom status bar indicates the system is 'Ready' and shows the local IP '8man-demo.local'.

Right-click on the account and select "Change group memberships" from the context menu.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The main window is titled "Add / remove group memberships" and is open for the user "Emily Employee (8man-demo\Emily Employee)". The interface displays a list of groups under the heading "Is direct member of". The group "L\_Projects\_Project\_Y\_special files\_re" is selected, and a context menu is open over it, with the "Remove" option highlighted. Below the list, there is a text input field for a comment, a "Close" button, and an "Immediately" dropdown menu. Red circles and boxes highlight these key elements: 1. The "Remove" option in the context menu, 2. the comment input field, and 3. the "Immediately" dropdown.

1. Remove the unnecessary group membership.
2. You must enter a comment.
3. Start the process.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The left pane displays a tree view of resources under 'Active Directory' and 'File server'. The 'Events' folder is selected, and a context menu is open over it. The 'Modify access rights...' option is highlighted. The right pane shows the 'Events' folder details, including the owner 'Domain Admins', inheritance status 'On', and a table of NTFS permissions. The 'Accounts with permissions' section shows a list of accounts, with 'Modify\Emily Employee (8man-demo)' highlighted.

Resources

Filter resources on first tree level 1

Active Directory

File server

srv-8man \\srv-8man

Organization 8 KB

Development 0 Byte

Facility Management 0 Byte

Finance 0 Byte

Human Resources 0 Byte

Management 0 Byte

Marketing 1 KB

Events 0 Byte

Flyer 0 Byte

Outbox 408 Bytes

Press 728 Bytes

Production 0 Byte

Research 0 Byte

Sales 7 KB

Projects D:\Projects 366 KB

Templates D:\Templates 19 KB

Users D:\Users 0 Byte

Exchange

Purpose Groups

SharePoint Online

SharePoint

Easy Connect - CSV

Easy Connect - SQL

Azure AD

OneDrive

SAP Connector

Events \\srv-8man\Organization\Marketing\Events

Owner Domain Admins (8man-demo\Domain Admins) Change owner

Inheritance On Change inheritance

Access rights

NTFS

All permissions

Full control

Modify

Accounts with permissions All permissions

1 of 12 X

Users Groups Contacts Computers

Name how often granted Inheritance

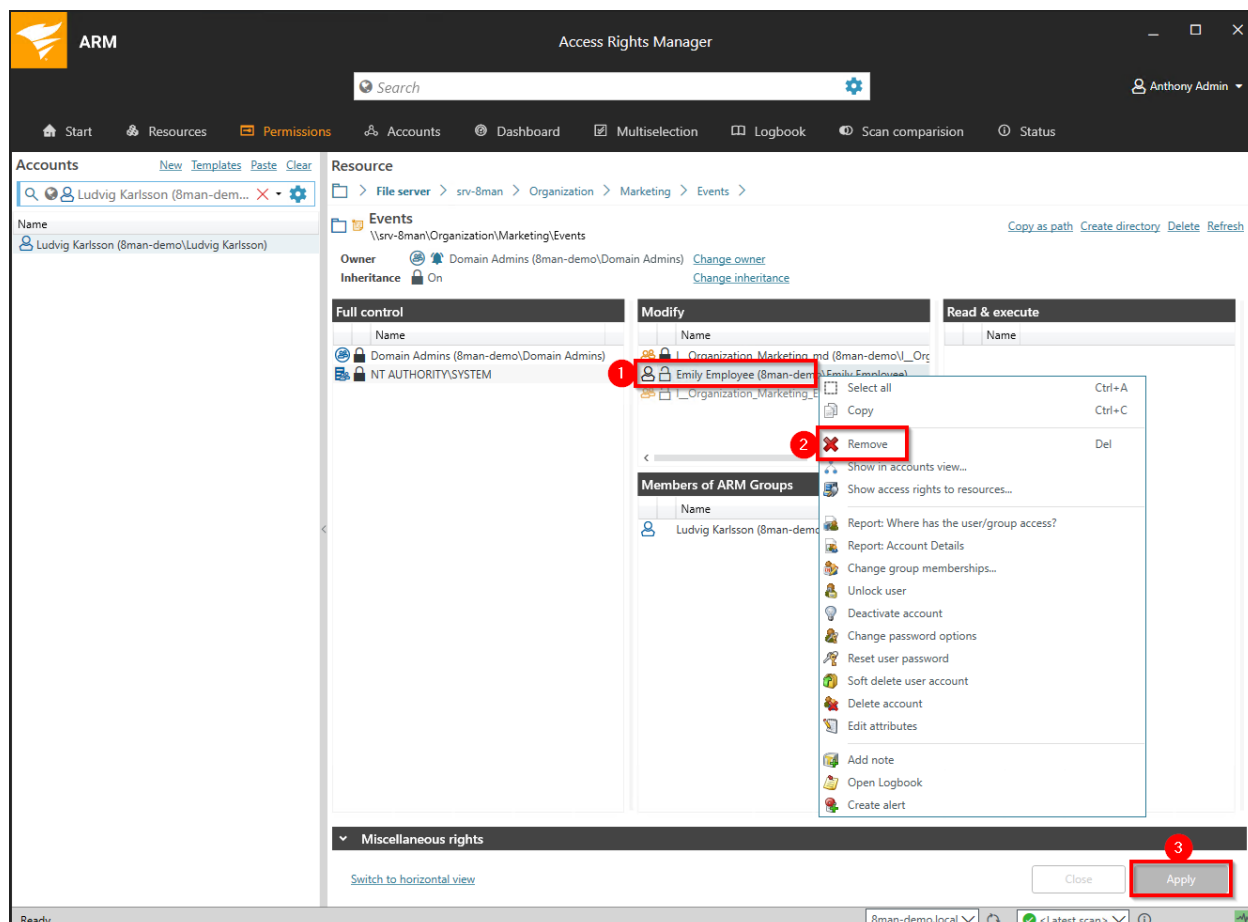
Emily Employee (8man-demo\Emily Employee) 2 1x 1x

2 Access paths

Modify\Organization\Marketing\_md (8man-demo)\Marketing (8man-demo)\Emily Employee

Modify\Emily Employee (8man-demo)

1. After removing all unnecessary group memberships you still need to remove the direct permissions.
2. Right-click on the desired directory.
3. Select "Modify access rights" from the context menu.



1. Right-click on the desired user.
2. Select "Remove" from the context menu.
3. Start the removal process.



The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The 'Resources' tab is active, showing a tree view of file servers. Under 'File server', the 'Marketing' folder is selected, and its sub-folder 'Events' is highlighted with a red box. The right pane shows the details for the selected resource: \\srv-8man\Organization\Marketing\Events. It lists the owner as Domain Admins, inheritance as 'On', and a table of NTFS permissions. The 'Accounts with permissions' section shows a search for 'emil' and a list of accounts, with 'Emily Employee (8man-demo\Emily Employee)' having '1' permission, highlighted with a red box.

Verify the result in the resource view.

## Create a protected file server directory

### Background / Value

Managers and team leads can use ARM to quickly and easily create protected file server directories. This is done by creating a directory, removing all inherited rights and then adding new access rights. The result is a protected directory that only selected users have access to.

## Step-by-step process

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The 'Resources' tab is active, showing a tree view of the file system. The 'Project Y' folder is selected, and a context menu is open over it. The 'Create directory' option is highlighted. The right-hand pane shows the 'Access rights' and 'Accounts with permissions' for the selected folder.

**Resources**

Filter resources on first tree level	1		
full path	Description	Access rights	Folder Size
<b>Active Directory</b>			
<b>File server</b>			
srv-8man			
Organization	D:\Organization		9 KB
Projects	D:\Projects		366 KB
2017			223 KB
2018			12 KB
2019			111 KB
2020			0 Byte
Project X			0 Byte
Project Y			18 KB
Top Secret Project Z			0 Byte
Templates			19 KB
Users			0 Byte
<b>Exchange</b>			
<b>Purpose Groups</b>			
<b>SharePoint Online</b>			
<b>SharePoint</b>			
<b>Easy Connect - CSV</b>			
<b>Easy Connect - SQL</b>			
<b>Azure AD</b>			
<b>OneDrive</b>			
<b>SAP Connector</b>			

**Project Y**

Owner: Domain Admins (8man-demo\Domain Admins) [Change owner](#)

Inheritance: On [Change inheritance](#)

Access rights: On

**NTFS**

Inheritance	Full control	Modify	Restricted...	Read and Ex...	Write	Read	Propagation
On	On	On	On	On	On	On	On

**All permissions**

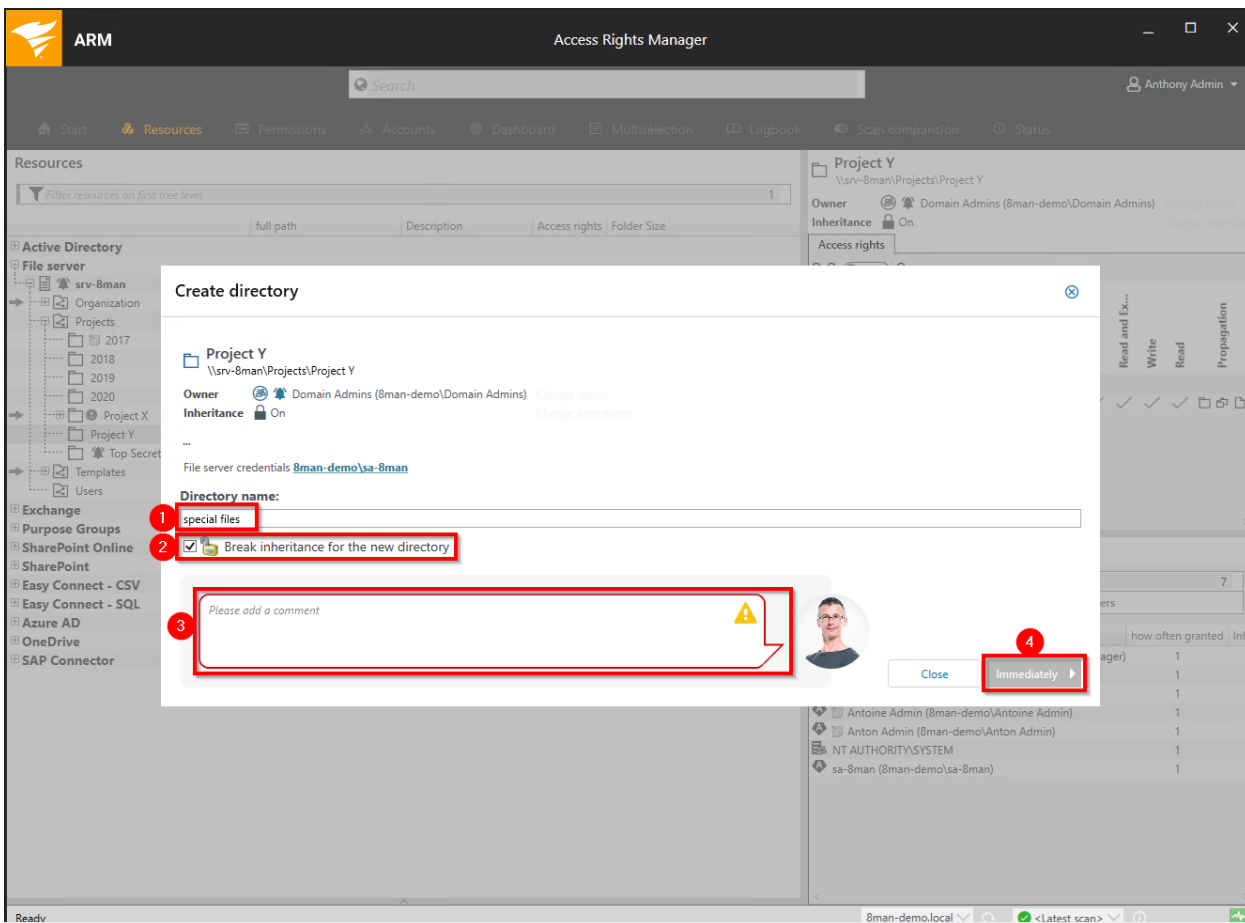
Full control	On	On	On	On	On	On	On
--------------	----	----	----	----	----	----	----

**Accounts with permissions** All permissions

Filter: 7

Name	how often granted	Inhe
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	
Administrator (8man-demo\Administrator)	1	
Anthony Admin (8man-demo\Anthony Admin)	1	
Antoine Admin (8man-demo\Antoine Admin)	1	
Anton Admin (8man-demo\Anton Admin)	1	
NT AUTHORITY\SYSTEM	1	
sa-8man (8man-demo\sa-8man)	1	

1. Select "Resources".
2. Navigate to the desired folder.
3. Right-click on the desired object and select "Create directory" from the context menu.



1. Name the directory.
2. Activate the option.
3. You must enter a comment.
4. Start the creation of a new directory.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main window is titled "Access Rights Manager" and shows a navigation pane on the left with a search bar and a list of resources. The "Resources" pane is filtered to show "special files" under the "File server" section. A context menu is open over the "special files" directory, with the "Modify access rights..." option highlighted. The right-hand pane shows the "special files" directory details, including the owner (Administrators), inheritance (Off), and a table of permissions. The "Accounts with permissions" section lists 7 accounts with their respective permissions.

Name	how often granted	Inhe
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	
Administrator (8man-demo\Administrator)	1	
Anthony Admin (8man-demo\Anthony Admin)	1	
Antoine Admin (8man-demo\Antoine Admin)	1	
Anton Admin (8man-demo\Anton Admin)	1	
NT AUTHORITY\SYSTEM	1	
sa-8man (8man-demo\sa-8man)	1	

1. Navigate to the newly created directory.
2. Right-click on the directory and select "Modify access rights..." from the context menu.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main window is titled "Access Rights Manager" and shows a navigation pane on the left with "Accounts" and "Resources". The "Accounts" pane lists "Domain Users (8man-demo\Domain Users)", "Ludvig Karlsson (8man-demo\Ludvig Karlsson)", and "Marketing (8man-demo\Marketing)". The "Resources" pane shows a path: "File server > srv-8man > Projects > Project Y > special files". Below this, the "special files" resource is selected, showing its "Owner" as "Administrators (8man-demo\Administrators)" and "Inheritance" as "Off". The "Full control" and "Modify" sections are visible, with "Full control" listing "NT AUTHORITY\SYSTEM" and "Domain Admins (8man-demo\Domain Admins)". The "Members of ARM Groups" section is highlighted, showing "Ludvig Karlsson (8man-demo\Ludvig Karlsson)" selected. A context menu is open over the "Members of ARM Groups" section, with the "Remove" option highlighted in red. The context menu includes options like "Select all", "Copy", "Set expiration date", "Show in accounts view...", "Show access rights to resources...", "Report: Where has the user/group access?", "Report: Account Details", "Change group memberships...", "Unlock user", "Deactivate account", "Change password options", "Reset user password", "Soft delete user account", "Delete account", "Edit attributes", "Add note", "Open Logbook", and "Create alert". The "Remove" option is also associated with the "Del" keyboard shortcut. The interface includes a search bar at the top, a navigation bar with "Start", "Resources", "Permissions", "Accounts", "Dashboard", "Multiselection", "Logbook", and "Scan" buttons, and a status bar at the bottom showing "Ready" and "8man-demo.local".

Remove all unnecessary access rights.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The user 'Anthony Admin' is logged in. The main area is divided into 'Accounts' and 'Resource' sections. In the 'Accounts' section, a search field is used to find 'Emily Employee (8man-dem...)'. In the 'Resource' section, the path is 'File server > srv-8man > Projects > Project Y > special files'. The 'special files' resource is selected, and its permissions are being configured. The 'Full control' column contains 'NT AUTHORITY\SYSTEM' and 'Domain Admins'. The 'Modify' column contains 'I\_Projects\_Project Y\_special files\_md (8man-dem)'. The 'Read & execute' column contains 'Emily Employee (8man-demo\Emily Employee)'. A red arrow points from the search field to the 'Emily Employee' user in the 'Read & execute' column. At the bottom right, the 'Apply' button is highlighted with a red box.

1. Use the search field to find the desired users and groups.
2. Use drag & drop to move the desired accounts into the access rights columns.
3. Start the process.

ARM

Access Rights Manager

Search

Anthony Admin

Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparison Status

Accounts Resource

Emily Employee (8man-demo\Emil...)

File server > srv-8man > Projects > Project Y > special files

### Change access rights

special files  
\\srv-8man\Projects\Project Y\special files

Owner Administrators (8man-demo\Administrators) [Change owner](#)

Inheritance Off [Change inheritance](#)

File server credentials for change 8man-demo\sa-8man

Active Directory change credentials 8man-demo\sa-8man

**Access right changes** All changes (7)

- Remove access rights for Ludvig Karlsson (8man-demo\Ludvig Karlsson) with Modify
- Set access rights for Emily Employee (8man-demo\Emily Employee) Read & execute

Group Wizard options

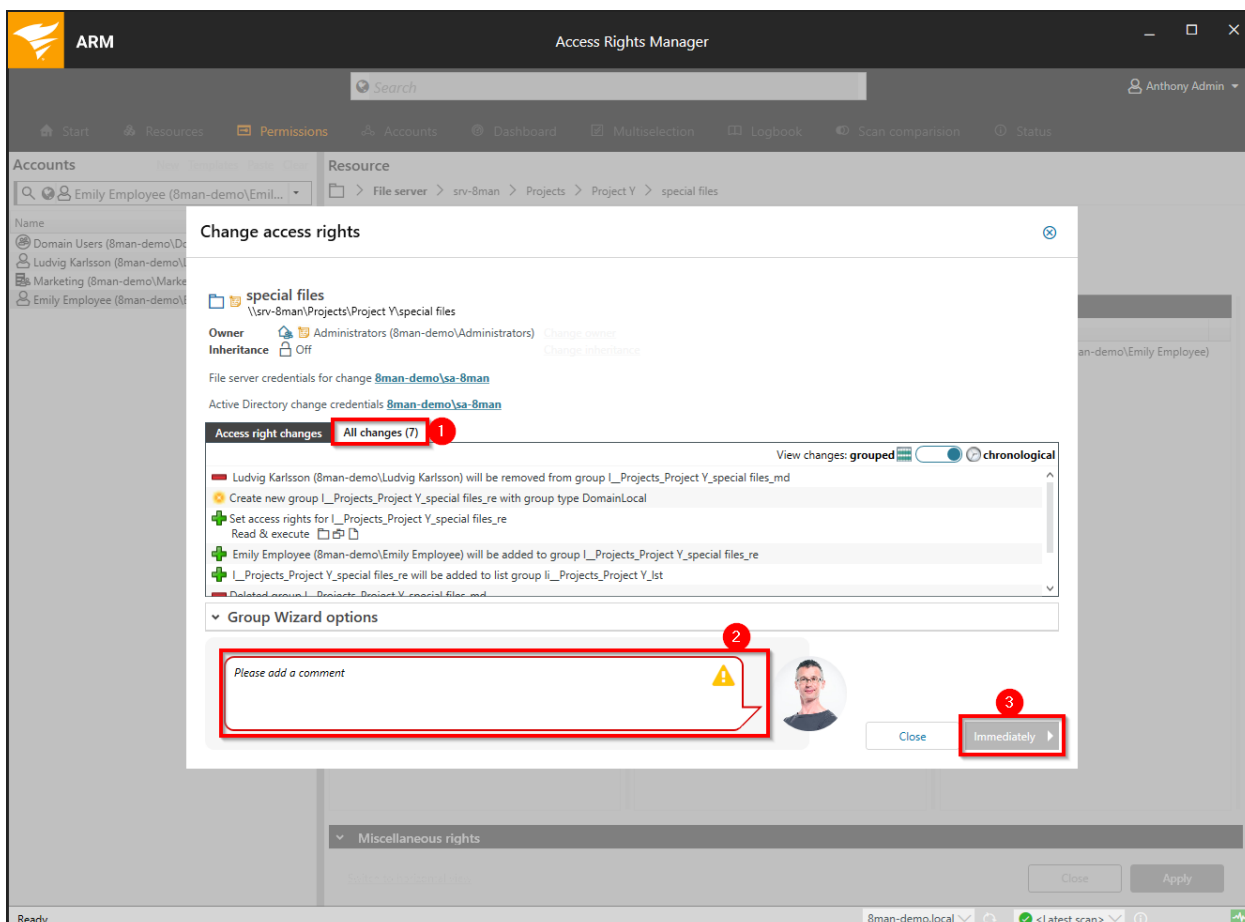
Please add a comment

Close Immediately

Miscellaneous rights

Ready 8man-demo.local <Latest scan>

ARM lists all planned access right changes.



1. Click on the tab "All changes". You see a detailed list of all individual steps that the Group Wizard is performing for you.
2. You must enter a comment.
3. Start the process.



## Remove direct permissions

### Background / Value

Direct access rights should be avoided and replaced by group access rights. Firstly, direct access rights are inefficient because every user is managed independently. Secondly, each directory needs to be examined individually to ensure the removal of all direct access rights. ARM shows you all direct access rights on your file server(s). You can then use drag & drop to turn direct access rights into group access rights.

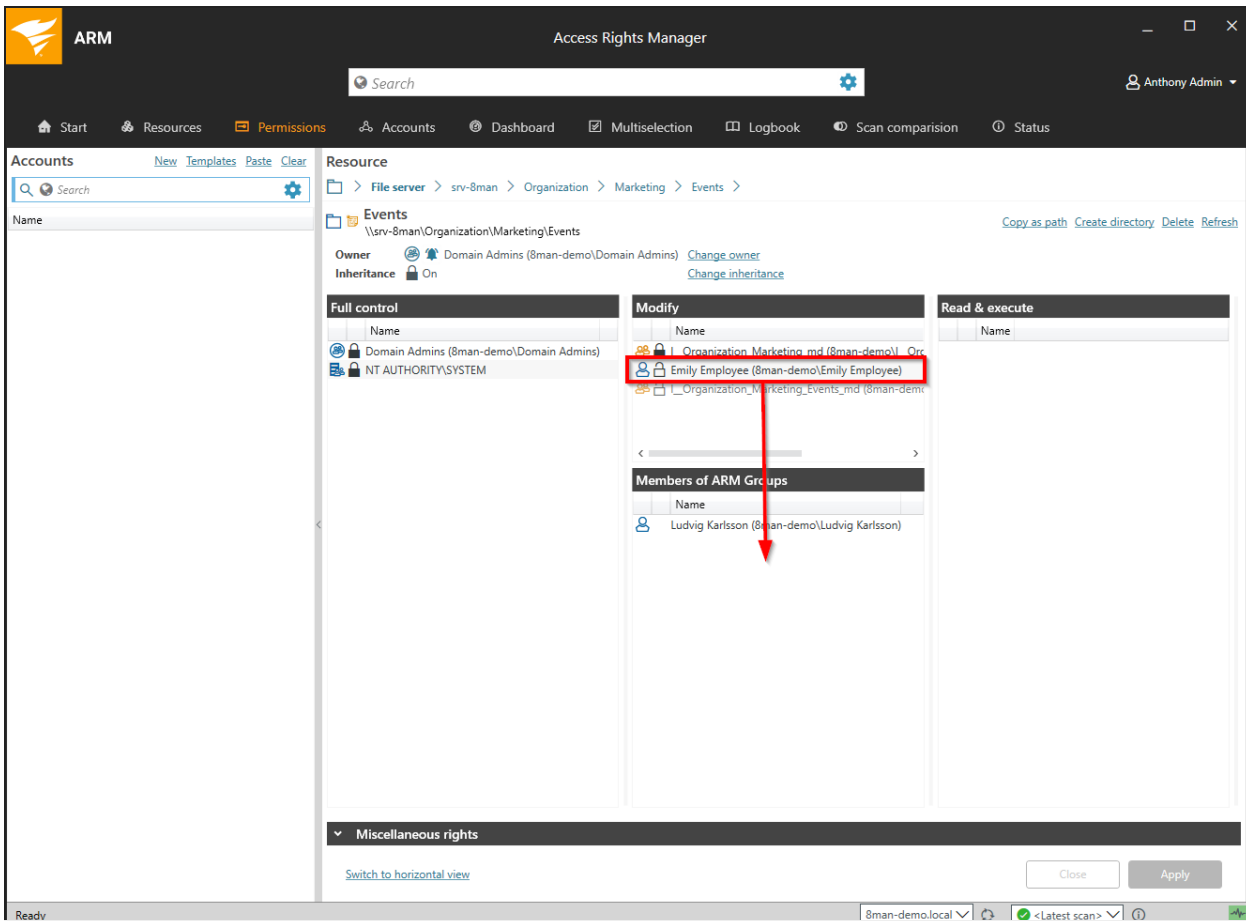
### Related features

[Remove direct permissions in bulk](#) (web client)

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The left pane shows a tree view of resources under 'Active Directory' and 'File server'. The 'Events' directory is selected, and a context menu is open with 'Modify access rights...' highlighted. The right pane shows the 'NTFS' permissions table with 'Full control' and 'Modify' permissions listed. The 'Accounts with permissions' section shows a list of users and groups with their access paths. Red boxes and numbers 1, 2, and 3 indicate the steps: 1. Selecting the 'Modify' permission in the 'Accounts with permissions' table; 2. Right-clicking the 'Events' directory in the 'Resources' tree; 3. Selecting 'Modify access rights...' from the context menu.

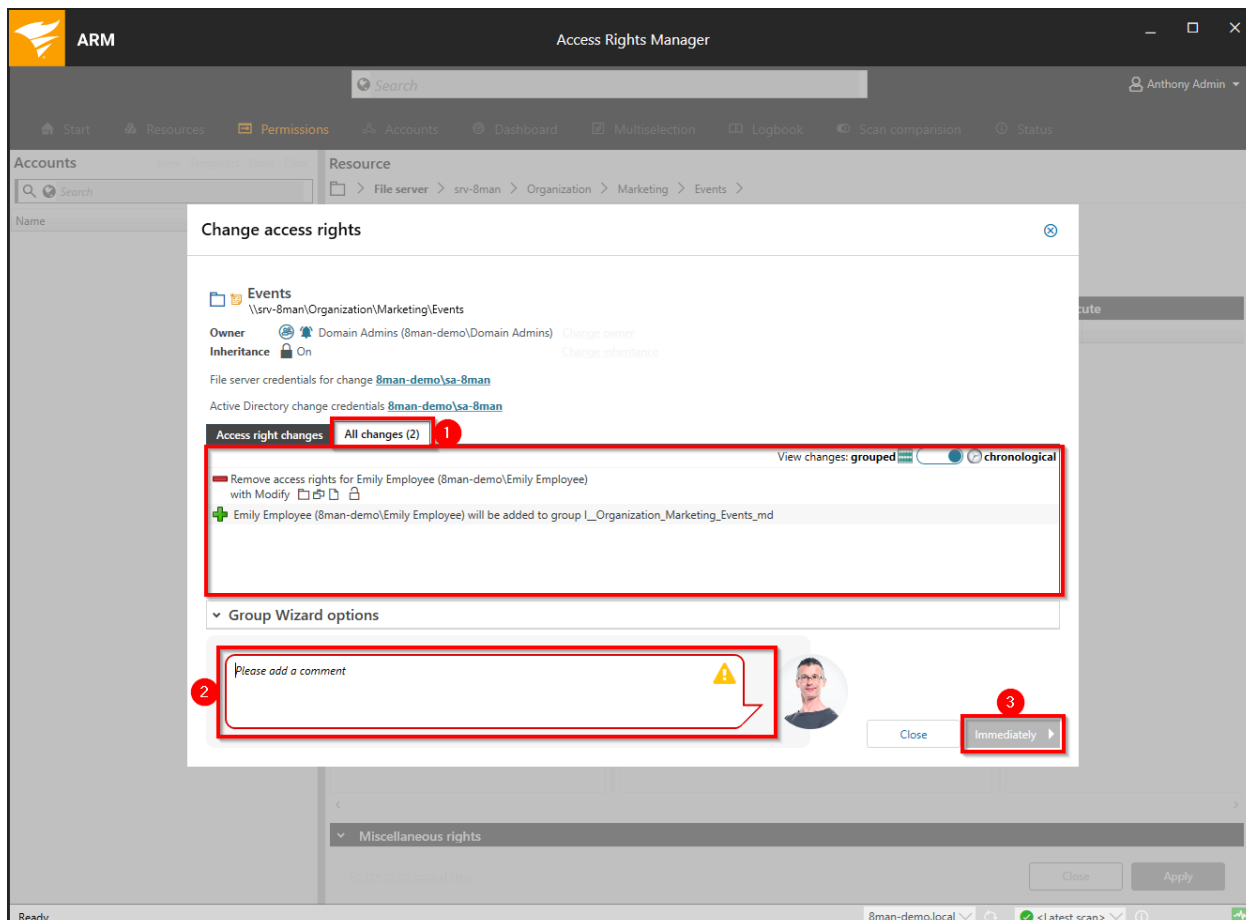
1. You have identified direct access rights.
2. Right-click on the affected directory.
3. Select "Modify access rights..." from the context menu.



Drag the user into the ARM group.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The main window displays the 'Events' resource path: \\srv-8man\Organization\Marketing\Events. The 'Full control' tab is active, showing a list of permissions. A red box labeled '1' highlights the 'Organization\_Marketing\_md (8man-demo\Organization\_Marketing\_md)' entry, which is being removed. A 'Members of ARM Groups' dialog box is open, showing a list of groups. A red box labeled '2' highlights the 'Emily Employee (8man-demo\Emily Employee)' group, which is being assigned. At the bottom right, a red box labeled '3' highlights the 'Apply' button. The interface also shows the 'Accounts' pane on the left and the 'Miscellaneous rights' section at the bottom.

1. The direct access right will be removed.
2. The group membership will be assigned.
3. Click on "Apply".



1. You can see the individual steps in the detail view.
2. You must enter a comment.
3. Start the process.

## Remove direct permissions in bulk (web client)

### Background / Value

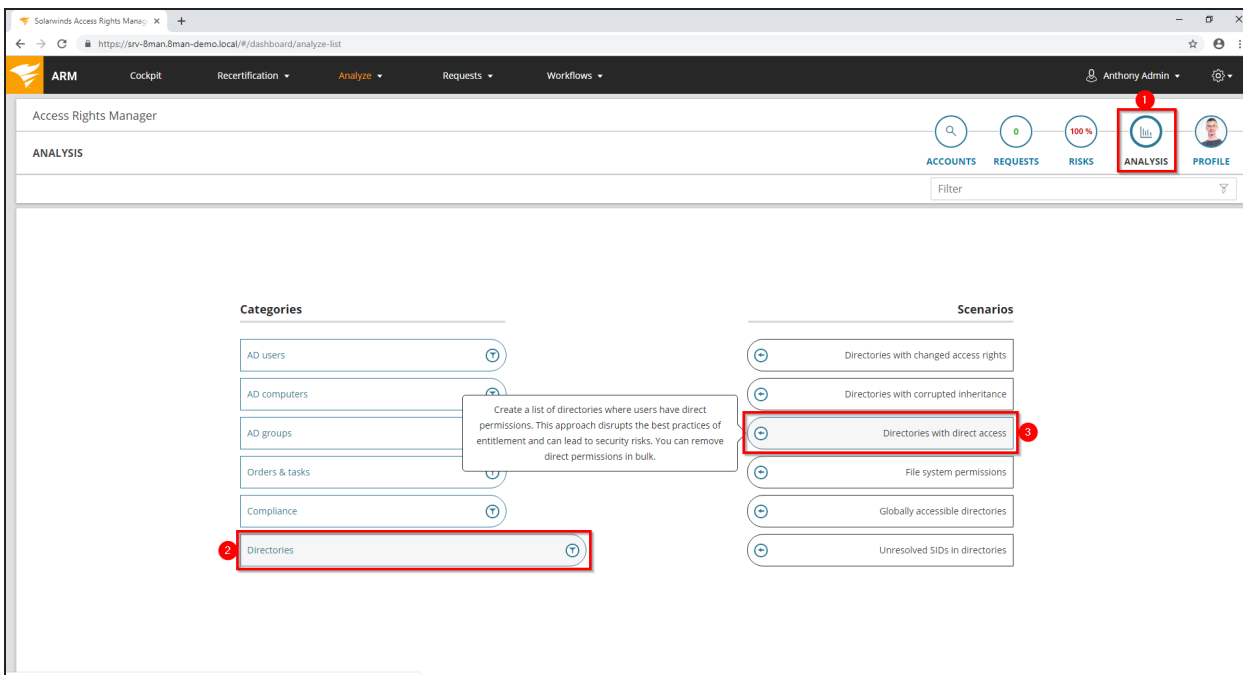
Direct permissions should be avoided and replaced by group permissions. Firstly, direct access rights are inefficient because every user is managed independently. Secondly, with native tools every directory needs to be examined individually to ensure the removal of all direct permissions. ARM shows you all direct access rights on your file server(s). You can remove them in bulk using the web client.

### Related features

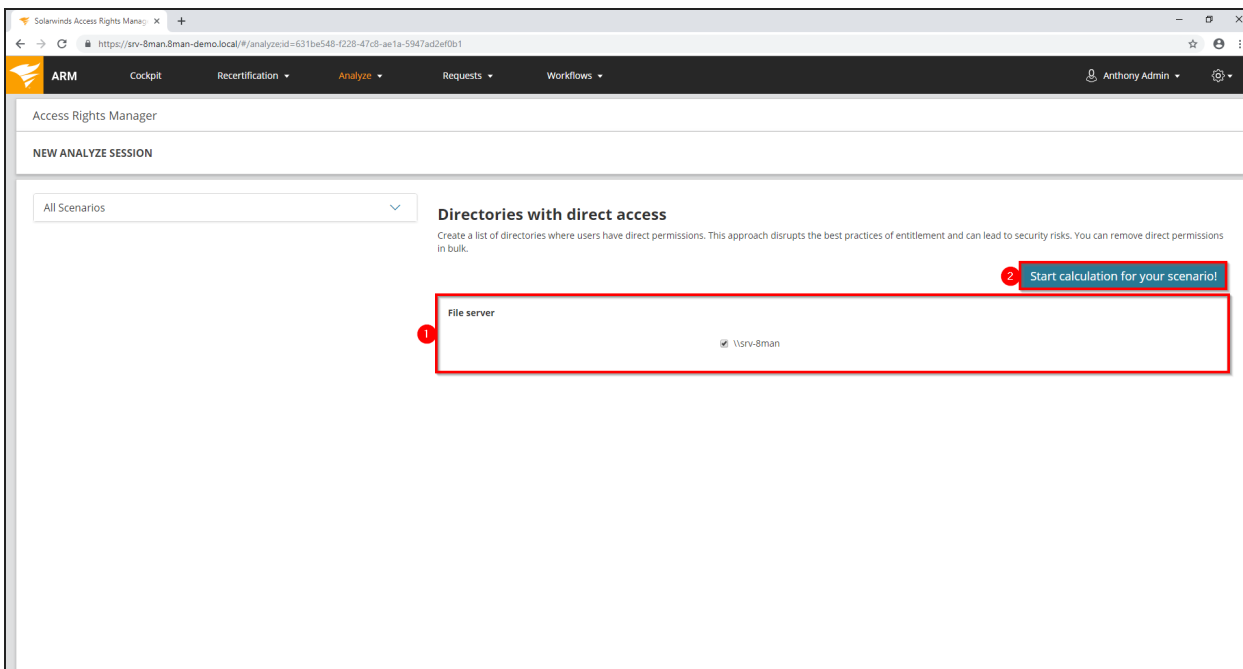
[Change password options in bulk](#) (web client)

[Remove unresolved SIDs in bulk](#) (web client)

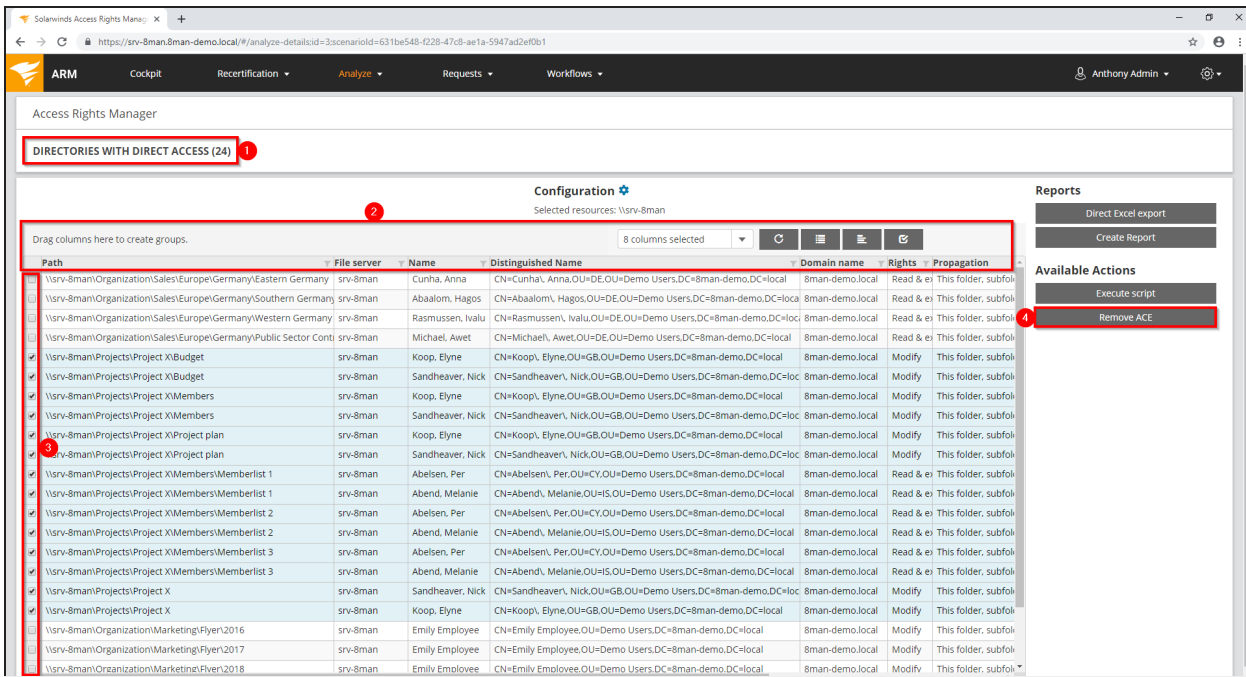
### Step-by-step process



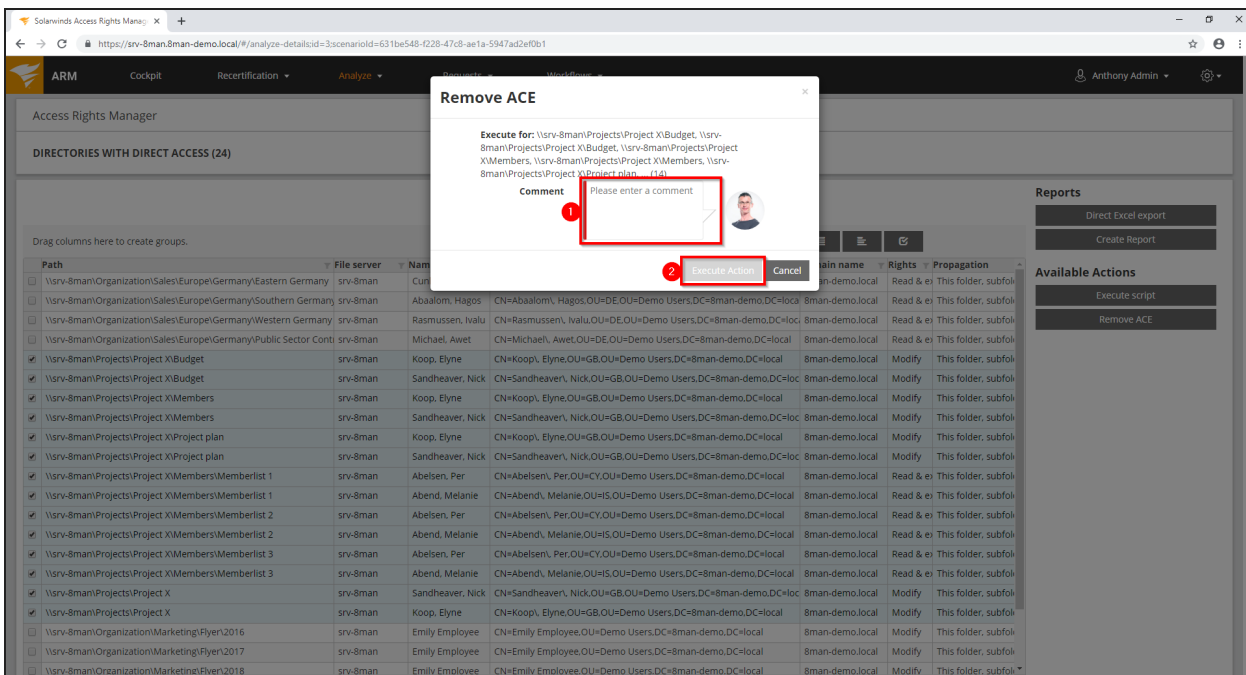
1. Select "Analysis".
2. Select the category "Directories".
3. Click "Directories with direct access".



1. Select the file servers.
2. Start the calculation.



1. ARM lists all directories with direct access.
2. Use sorting, filtering, grouping and column selection to locate the desired rows.
3. Select the desired entries.
4. Click "Remove ACE".



1. Leave a comment.

2. Click "Execute Action".

The job will be transferred to the ARM server and executed there. You can find the status in [Jobs overview](#).

## Remove corrupted inheritance

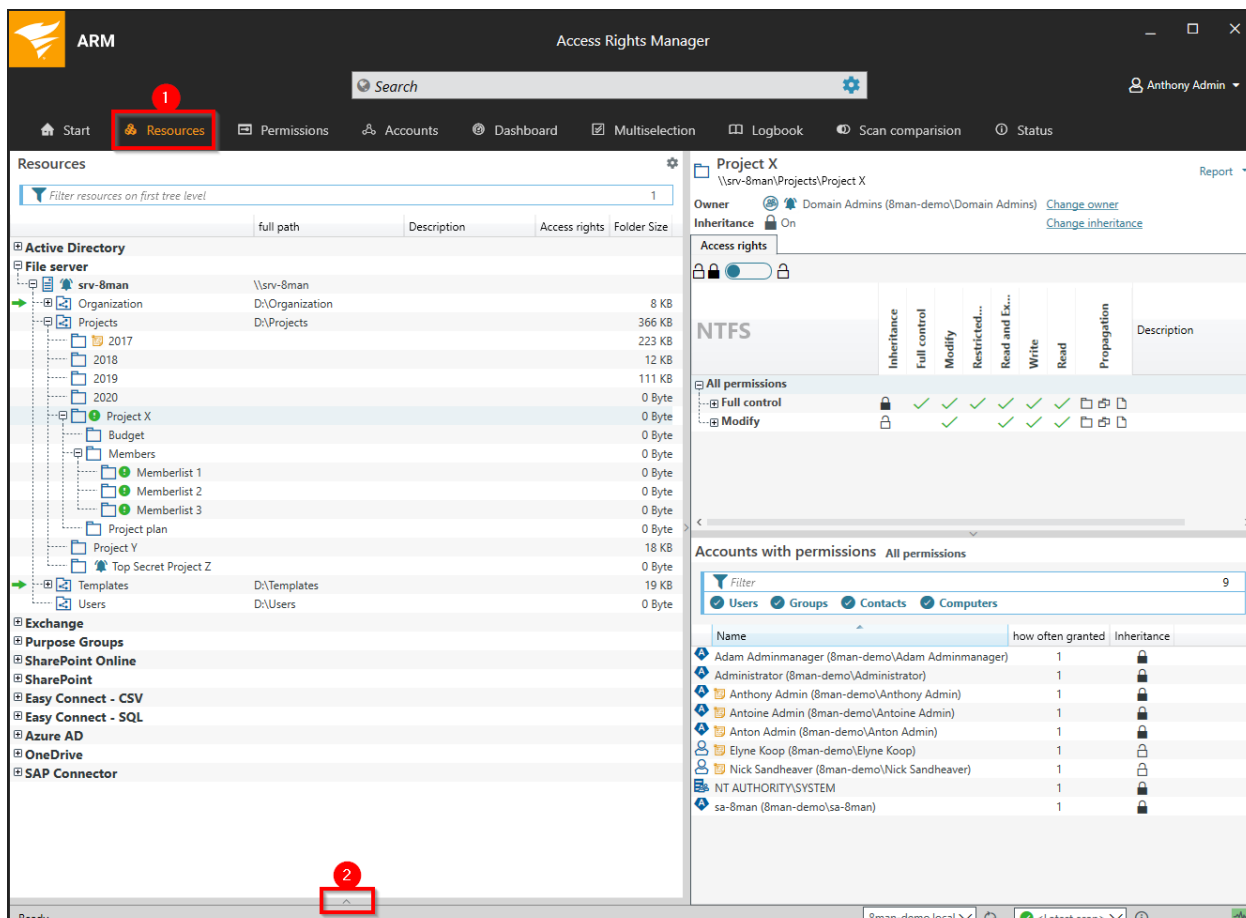
### Background / Value

Broken ACLs (Access Control Lists) interfere with permission inheritances on file servers. As a consequence the sub-directory will not inherit the correct permissions, despite this feature being activated. ARM displays "Broken ACLs" and removes them by reapplying the inheritance.

### Related features

[Identify errors in inheritance in the webclient and fix them in bulk](#)

### Step-by-step process



The screenshot shows the Access Rights Manager (ARM) web interface. The 'Resources' tab is selected and highlighted with a red box and a red circle containing the number '1'. The left sidebar shows a tree view of resources under 'Active Directory' and 'File server'. The main area displays details for 'Project X', including its owner, inheritance status, and a table of permissions. A table titled 'Accounts with permissions' is also visible, listing various users and their permission counts. A red box and a red circle containing the number '2' are positioned at the bottom of the interface, near the 'Ready' status bar.

1. Select "Resources".
2. Expand the frame.



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. On the left, a file tree under 'Active Directory' shows a file server 'srv-8man' with a 'Projects' folder containing 'Project X'. A red box highlights the 'Rights differ from parent' section for 'Project X', which contains a table with columns for Path, Size/items, Deny, and Inheritance. The 'Inheritance' column shows yellow lock icons for three memberlists. A red circle '1' points to the 'Project X' folder in the tree, and a red circle '2' points to the 'Inheritance' column header.

Path	Size/items	Deny	Inheritance
Memberlist 1 (\srv-8man\Projects\Project X\Members\Memberlist 1)	0 Byte		2 2
Memberlist 2 (\srv-8man\Projects\Project X\Members\Memberlist 2)	0 Byte		2 2
Memberlist 3 (\srv-8man\Projects\Project X\Members\Memberlist 3)	0 Byte		2 2

1. ARM lists all subdirectories with deviating permissions.
2. The yellow lock indicates a corrupted inheritance.

Use the sort function in the "Inheritance" column for long lists.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. On the left, a tree view shows the file server structure under 'Active Directory' and 'File server'. The 'Project X' folder is selected. Below the tree, a table shows 'Rights differ from parent' for 'Project X'.

Path	Size/items	Deny	Inheritance
Memberlist 1 (\\srv-8man\Projects\Project X\Members\Memberlist 1)	0 Byte	2	2
Memberlist 2 (\\srv-8man\Projects\Project X\Members\Memberlist 2)	0 Byte	2	2
Memberlist 3 (\\srv-8man\Projects\Project X\Members\Memberlist 3)	0 Byte	2	2

On the right, the 'Access right changes' pane shows a comparison between 'Members' and 'Memberlist 1'. It lists 'Unchanged' entries (Domain Admins, NT AUTHORITY\SYSTEM) and 'Added or removed entries' (Elyne Koop, Melanie Abend, Nick Sandheaver, Per Abelsen).

1. Select an entry.
2. ARM shows you in all details which permissions are different compared to the parent directory.

The screenshot shows the SolarWinds ARM interface. The 'Resources' pane on the left shows a tree view of the file system. The 'Members' folder is selected, and a context menu is open over it. The 'Change inheritance' option is highlighted with a red box and the number 2. The 'Members' pane on the right shows the 'Change inheritance' button highlighted with a red box and the number 3. The 'Accounts with permissions' pane at the bottom right shows a list of accounts with their permissions.

Name	how often granted	Inheritance
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	🔒
Administrator (8man-demo\Administrator)	1	🔒
Anthony Admin (8man-demo\Anthony Admin)	1	🔒
Antoine Admin (8man-demo\Antoine Admin)	1	🔒
Anton Admin (8man-demo\Anton Admin)	1	🔒
Elyne Koop (8man-demo\Elyne Koop)	1	🔒
Nick Sandheaver (8man-demo\Nick Sandheaver)	1	🔒
NT AUTHORITY\SYSTEM	1	🔒
sa-8man (8man-demo\sa-8man)	1	🔒

1. Select the subdirectory where you want to correct the corrupted inheritance.
2. or 3. Click "Change Inheritance".

Change inheritance

Members  
\\srv-8man\Projects\Project X\Members

Owner Administrators (8man-demo\Administrators) Change owner  
Inheritance On Change inheritance

File server credentials for change 8man-demo\sa-8man  
Active Directory change credentials 8man-demo\sa-8man

Change inheritance from parent folder  
Activate Deactivate  
Restores the inheritance for this object. It will inherit all access rights from its parent.

Enforce inheritance  
Restores the inheritance for all objects below this one. They will all have the same access rights as this object.

You have chosen to remove all custom access rights from the selected object and all children and replace them with inheritable permissions of the selected objects parent. This process may affect a lot of items and will take some time to complete.

Please add a comment

Immediately

Close

1. Enable inheritance.
2. Enforce inheritance for all subdirectories.
3. You must enter a comment.
4. Start the execution.

## Identify errors in inheritance and fix them in bulk (web client)

### Background / Value

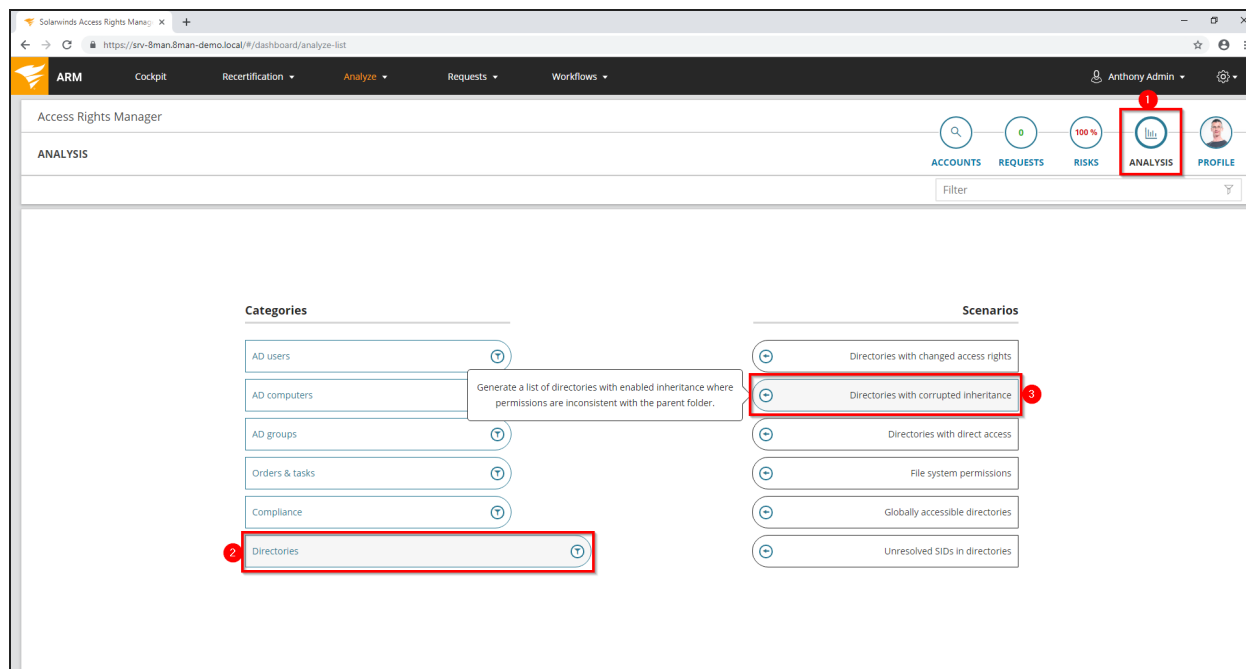
Errors in the inheritance of file server permissions often occur when employees copy or move directories. This can lead to unwanted access.

With the "Directories with corrupted inheritance" scenario, you can identify corrupted inheritance in a few clicks and eliminate them in one go.

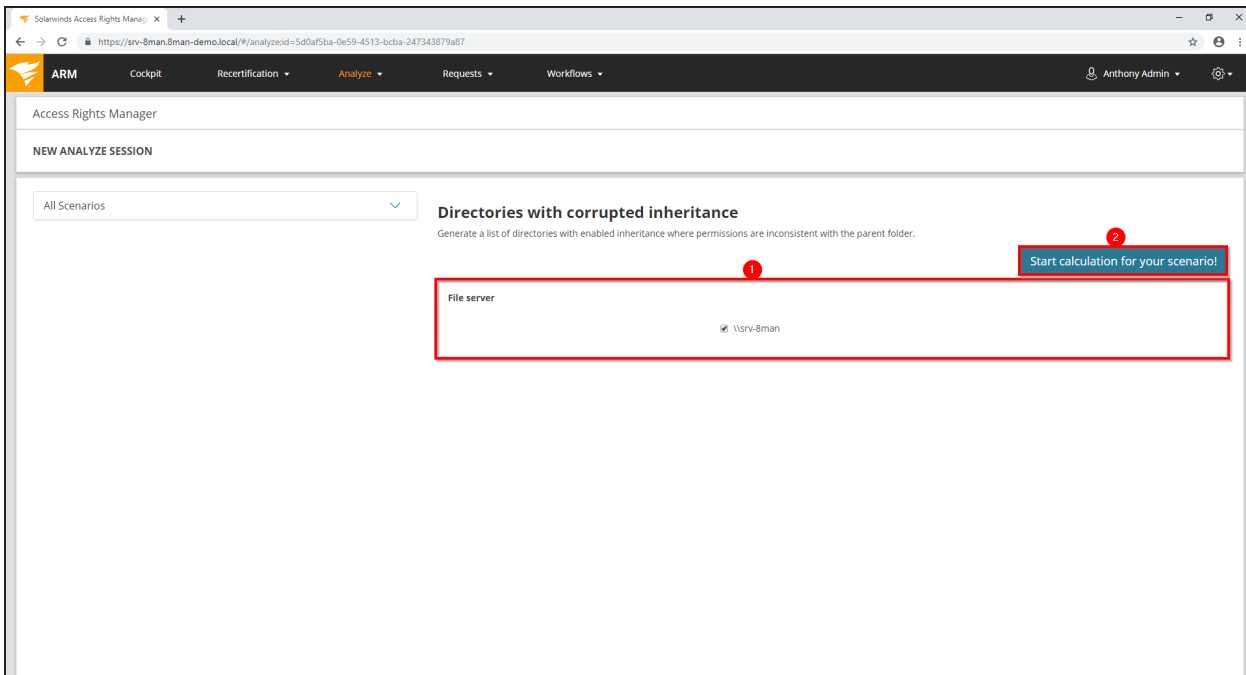
### Related features

[Identify corrupted inheritance](#)

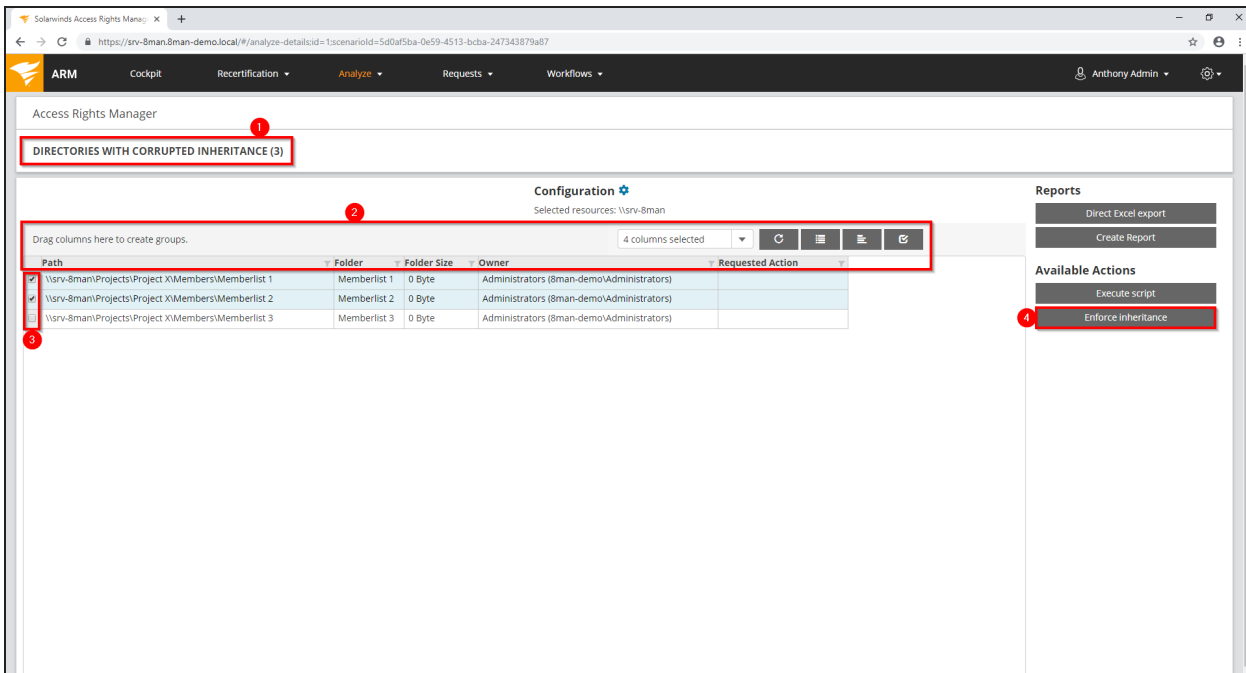
### Step-by-step process



1. In the cockpit, choose "Analysis".
2. Select the category "Directories".
3. Click "Directories with corrupted inheritance".

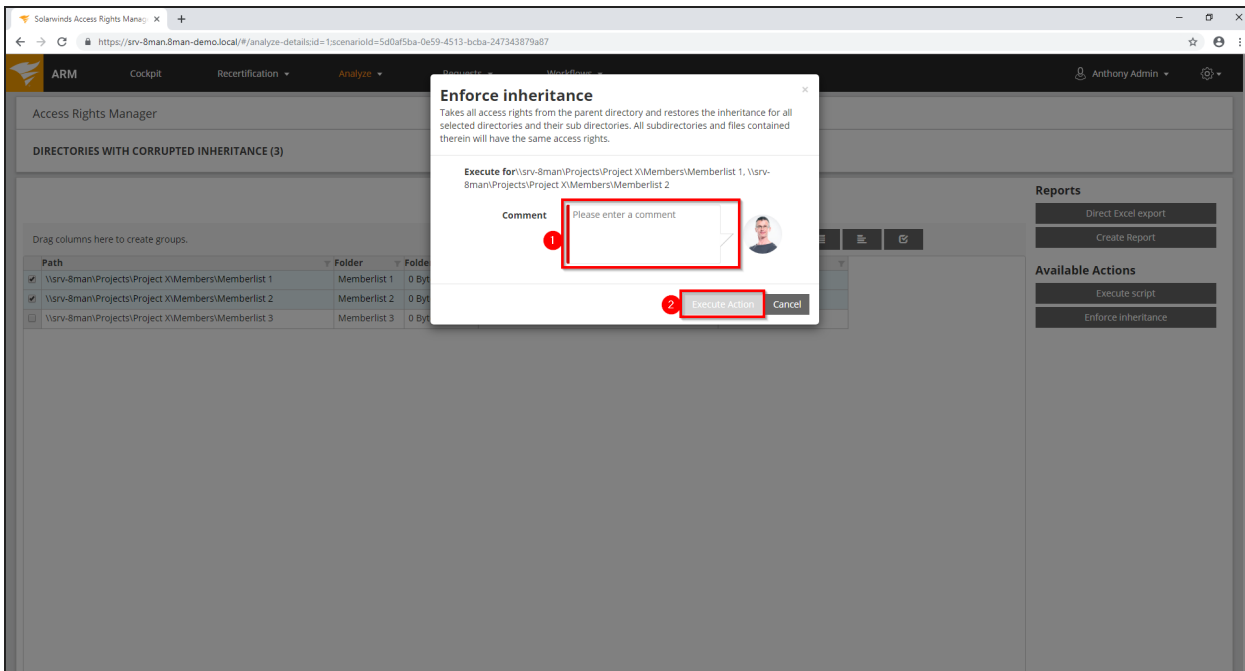


1. Determine which file servers are included in your analysis.
2. Start the calculation.



1. ARM lists all directories with corrupted inheritance.
2. Use sorting, filtering, grouping and column selection to locate the desired rows.
3. Select the desired entries.

#### 4. Click "Enforce Inheritance".



1. Leave a comment.
2. Click "Execute Action".

The job will be transferred to the ARM server and executed there. You can find the status in [Jobs overview](#).

## Identify and delete unresolved SIDs

### Background / Value

SIDs (Security Identifiers) are character strings that are used to identify user and group accounts in Active Directory. SIDs become unresolved when users or groups with direct access rights on file servers are deleted in AD.

By using unresolved SIDs insider threats can gain access to sensitive resources. ARM clearly identifies unresolved SIDs in your system allowing you to delete them.

### Related features

[Remove unresolved SIDs in bulk](#) (web client)

### Step-by-step process

The screenshot shows the ARM web client interface. The 'Dashboard' menu item is highlighted with a red box and a red circle containing the number 1. In the left-hand 'Reporting' sidebar, the 'Unresolved SIDs' item is highlighted with a red box and a red circle containing the number 2. The main content area displays a list of system components and their counts, including Users (1169), Groups (1660), and OU / Contacts / More (45). A 'Depth of nested groups' bar chart is visible at the bottom left of the main content area.

1. Select "Dashboard".
2. Click on "Unresolved SIDs".



ARM Access Rights Manager

Search

Anthony Admin

### Unresolved SIDs

**Report configuration**

Title

Comment

**Objects**

- srv-8man

**Unresolved SIDs**

Please select resource(s)

Resources

- File server
  - srv-8man

**Settings**

The output format is [XLSX](#)

Report execution mode [started manually](#)

Custom storage path is [not configured](#)

Send email is [Deactivated](#)

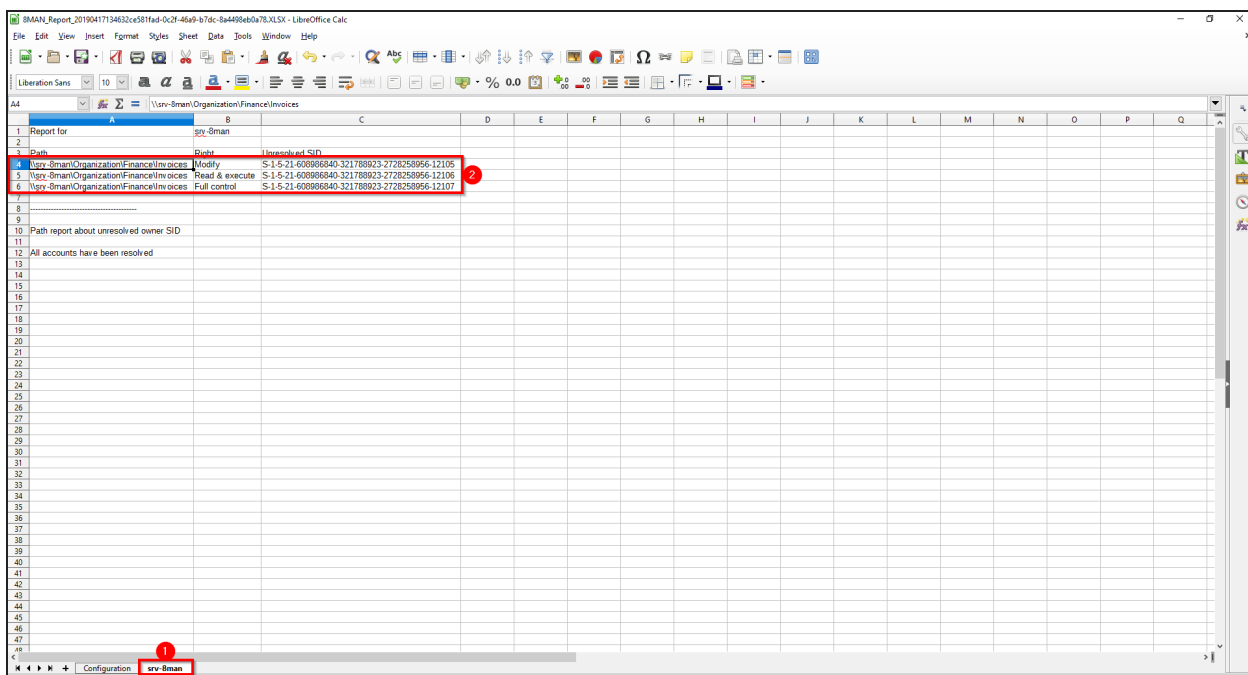
Cancel Start

Depth of 1564

Depth	User39 (8man-demo\User39)	2984
1	User38 (8man-demo\User38)	2960

Ready 8man-demo.local <Latest scan>

1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired report settings.
4. Start the report.



Open the report in your spreadsheet application.

1. Switch to the file server tab.
2. All unresolved SIDs are listed in the report.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The 'Resources' tab is active, showing a tree view of the file system. The 'Invoices' directory is selected, and its context menu is open, with 'Modify access rights...' highlighted. The right pane shows the 'NTFS' permissions for the selected directory, including 'Full control', 'Modify', and 'Read and Execute'. The 'Accounts with permissions' section is also visible, showing a list of accounts with a red arrow pointing to a specific account ID.

1. Select "Resources".

2. Select an affected directory.

3. Right-click on the directory and select "Modify access rights..." from the context menu.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The main window shows the 'Invoices' resource under the path 'File server > srv-8man > Organization > Finance > Invoices'. The permissions are listed in three columns: Full control, Modify, and Read & execute. In the 'Modify' column, the SID 'S-1-5-21-608986840-31788923-2728258956-12105 (8ma)' is highlighted with a red box and a red circle labeled '1'. A context menu is open over this SID, with the 'Remove' option selected and highlighted with a red box and a red circle labeled '2'. At the bottom of the window, the 'Apply' button is highlighted with a red box and a red circle labeled '3'. The interface also shows a search bar, navigation tabs (Start, Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, Status), and a user profile for 'Anthony Admin'.

1. Right-click the unresolved SID.
2. Select "Remove" from the context menu.
3. Click "Apply".

1. ARM lists all planned changes.
2. You must enter a comment.
3. Start the process.

## Remove unresolved SIDs in bulk (web client)

### Background / Value

SIDs (Security Identifiers) are strings that are used to identify user and group accounts in Active Directory. SIDs become unresolved when users or groups with direct permissions are deleted in AD. By using unresolved SIDs insider threats can gain access to sensitive resources.

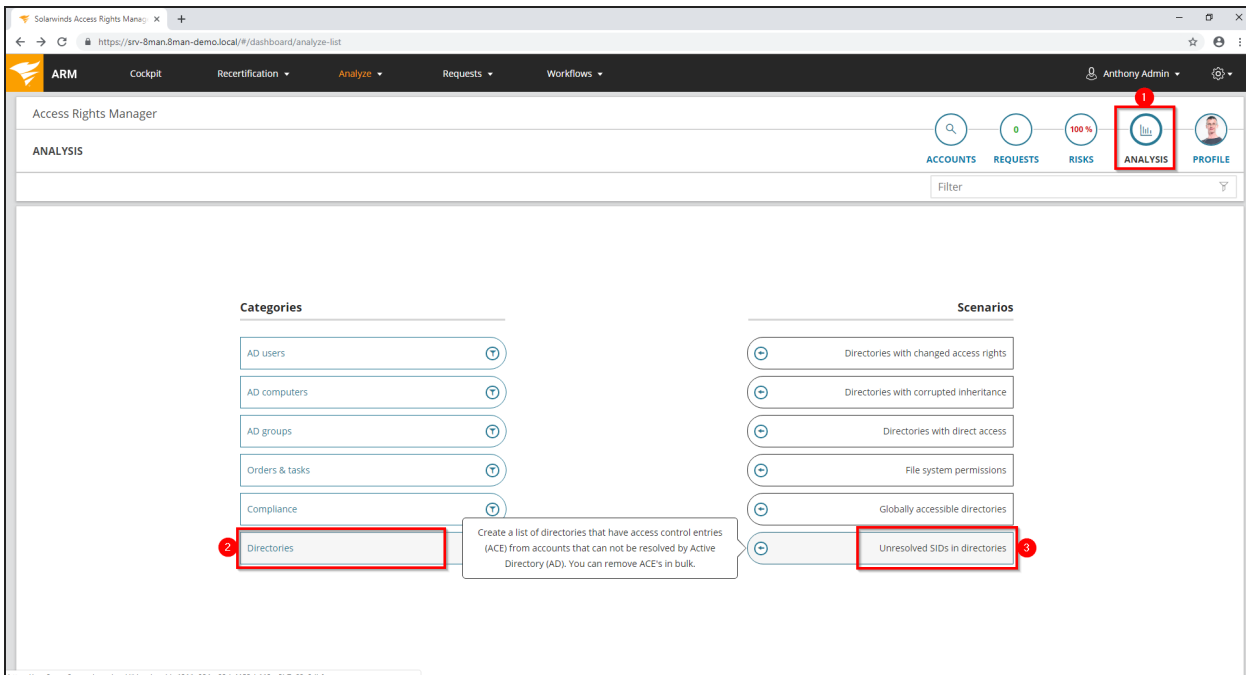
ARM clearly identifies unresolved SIDs in your system. Delete unresolved SIDs in bulk using the web client.

### Related features

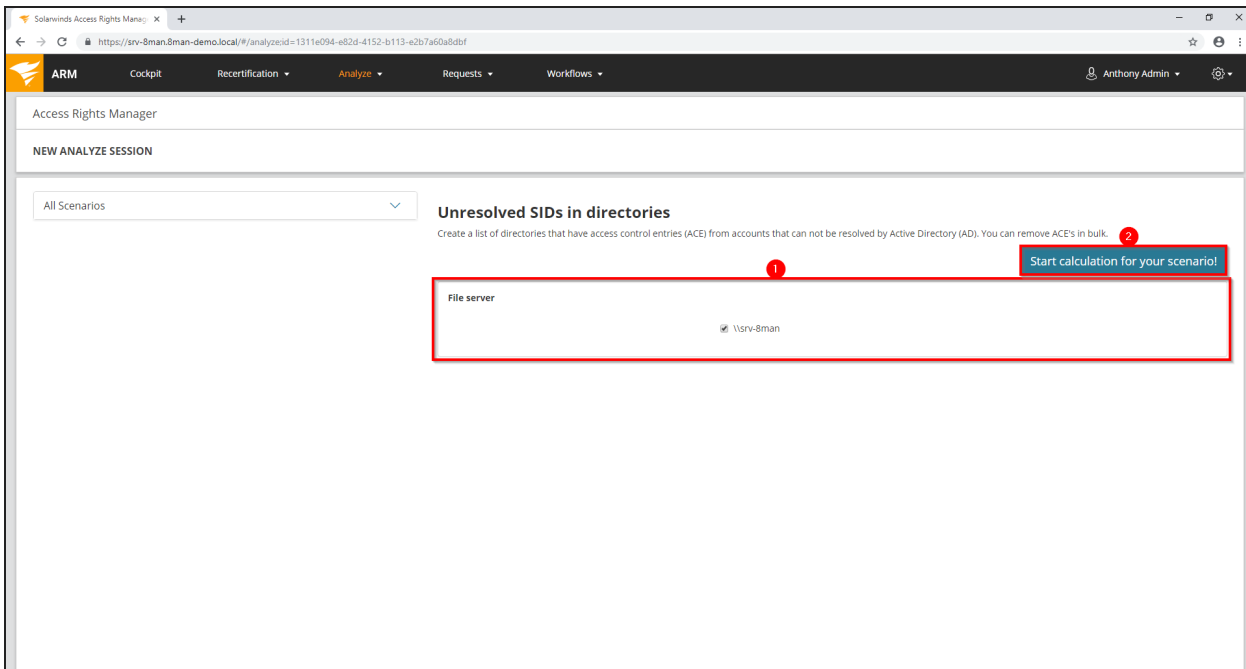
[Identify and delete unresolved SIDs](#) (rich client)

[Report: Identify unresolved SIDs](#) (rich client)

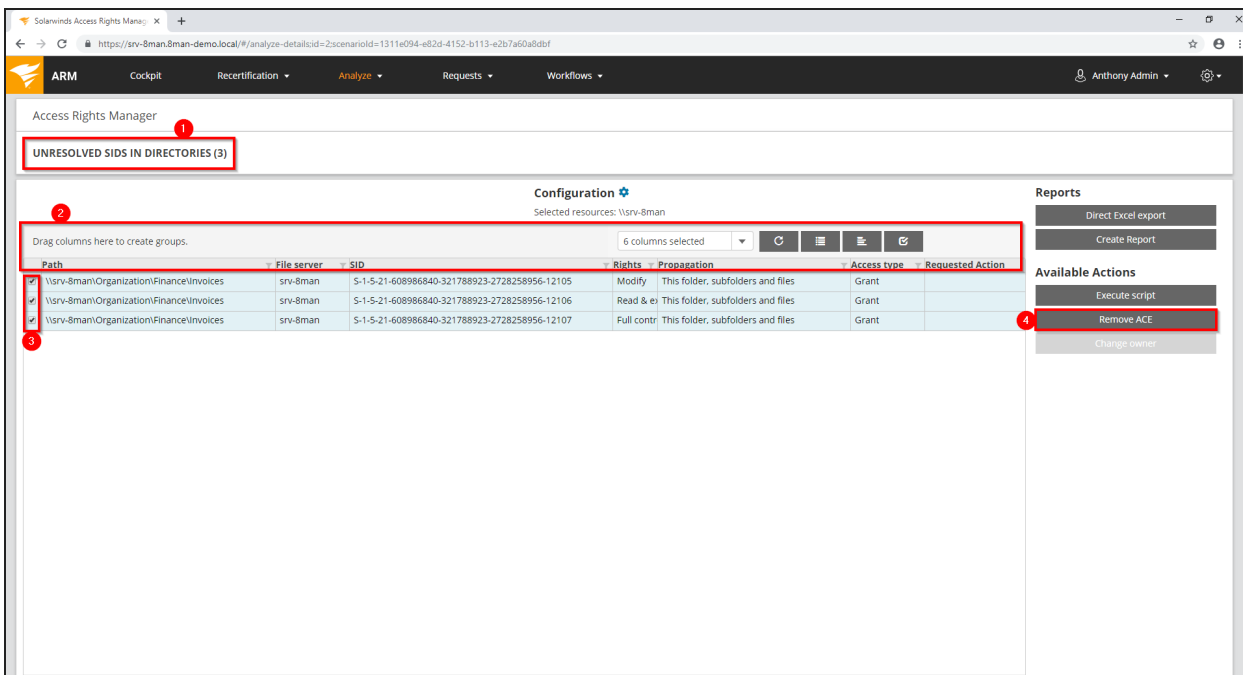
### Step-by-step process



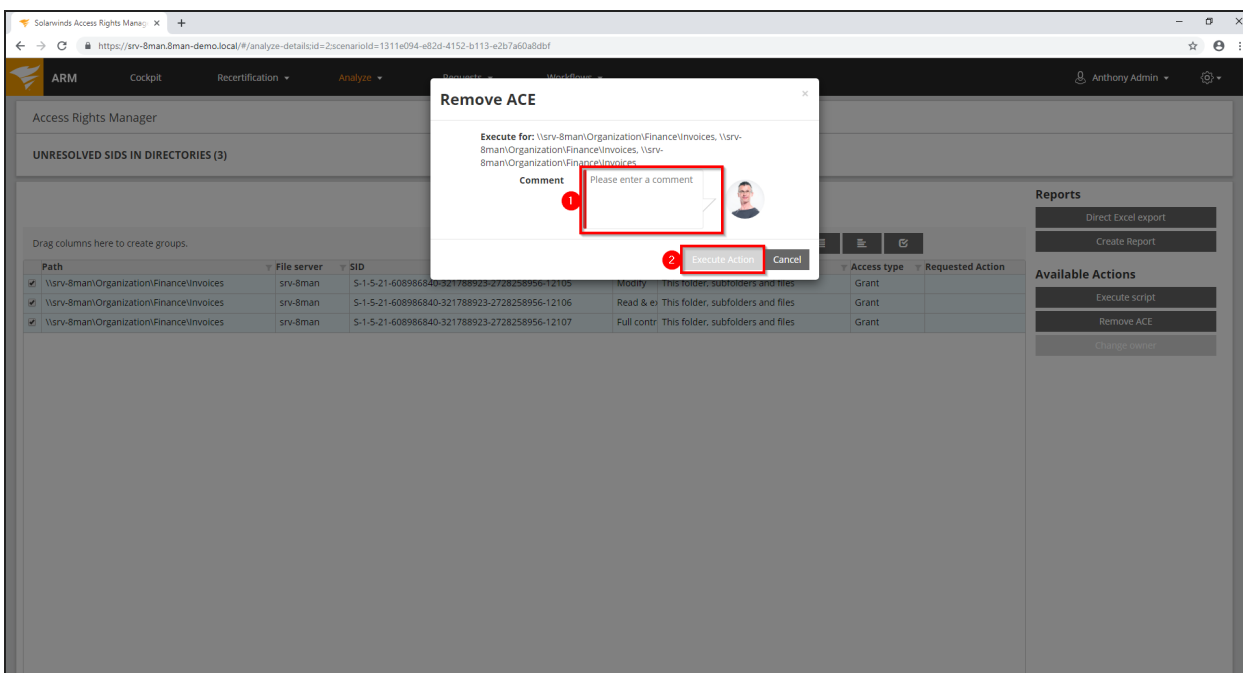
1. Select "Analysis".
2. Select the category "Directories".
3. Click "Unresolved SIDs in directories".



1. Select the file servers.
2. Start the calculation.



1. ARM lists all directories with unresolved SIDs.
2. Use sorting, filtering, grouping and column selection to locate the desired rows.
3. Select the desired entries.
4. Click "Remove ACE".



1. You must enter a comment.

2. Click "Execute Action".

The job will be transferred to the ARM server and executed there. You can find the status in [Jobs overview](#).

## Remove "everyone" permissions in bulk (web client)

### Background / Value

If "Everyone accounts" are used for the assignment of access rights, (almost) everyone has access to the connected resources. The consequence is an excessive assignment of access rights and a high probability for unauthorized access. These go against the principle of least privilege and should therefore not be used. Before deleting permissions you should assign specific groups to the appropriate resources.

"Everyone accounts" are:

- Everyone
- Authenticated Users
- Domain-Users

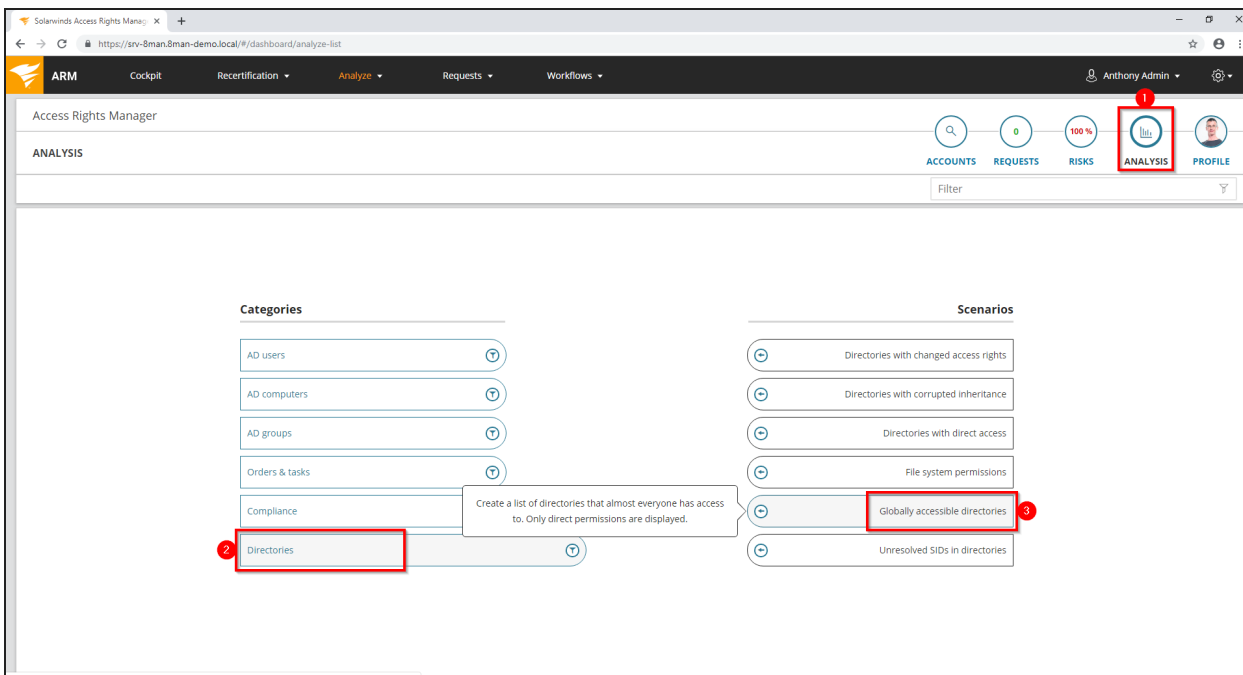
### Related features

[Report: Identify usage of "Everyone"](#) (rich client)

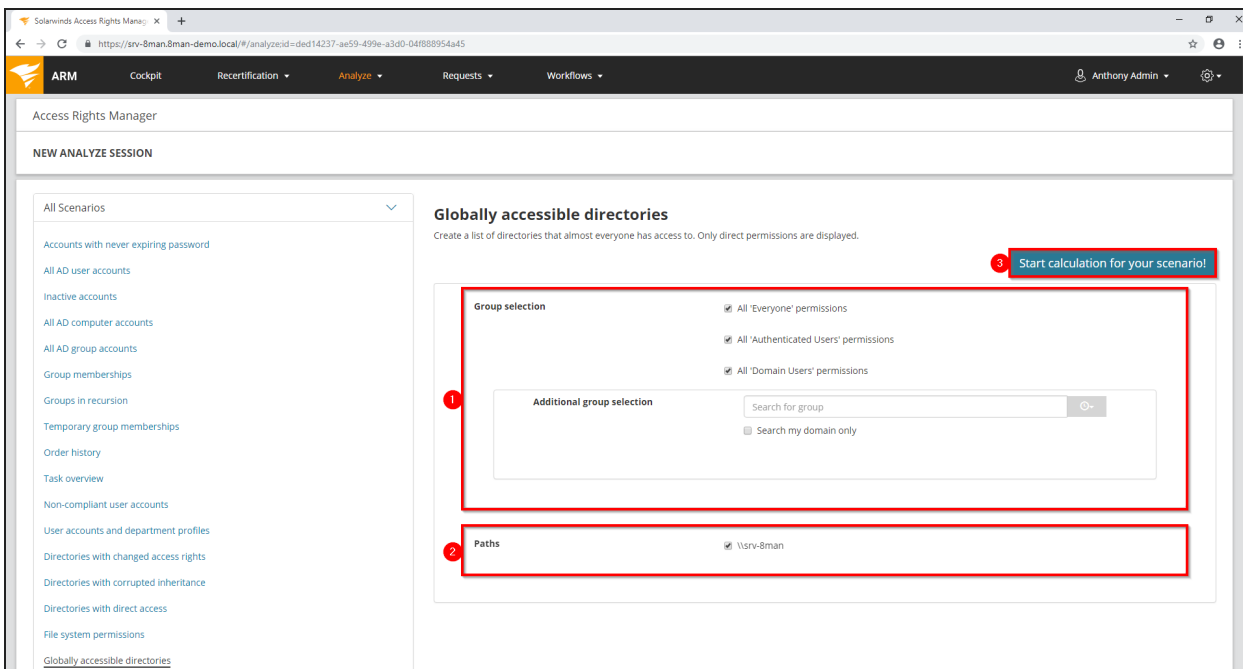
[Report: Identify usage of "Authenticated Users"](#) (rich client)

### Step-by-step process





1. Select "Analysis".
2. Select the category "Directories".
3. Click "Globally accessible directories".



1. Select security principals.  
You can add one additional group. This is very useful for "catch-all" groups, e.g. "mycompany-

complete".

**i** The scenario only considers direct access control entries (ACEs). Group nesting is not resolved.

2. Select the file servers.
3. Start the calculation.

Access Rights Manager

**GLOBALLY ACCESSIBLE DIRECTORIES (5)**

Configuration **+**  
All 'Everyone' permissions, All 'Authenticated Users' permissions, All 'Domain Users' permissions

Drag columns here to create groups. 3 columns selected

Path	Account	Rights	Requested Action
\\srv-8man\Templates\Power Point Templates	Everyone	Full control	
\\srv-8man\Templates\Instructions	Authenticated Users	Full control	
\\srv-8man\Templates\Signatures	Authenticated Users	Full control	
\\srv-8man\Templates\Word Templates	Authenticated Users	Full control	
\\srv-8man\Templates	Domain Users	Full control	

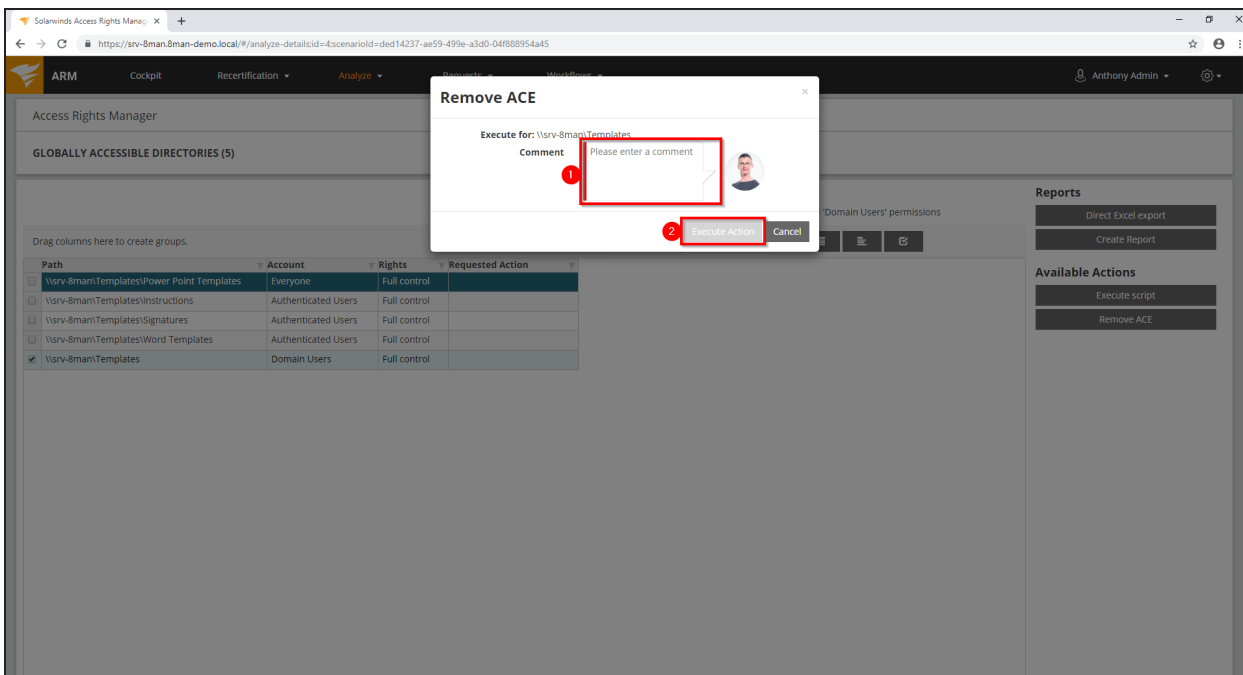
Reports

- Direct Excel export
- Create Report

Available Actions

- Execute script
- Remove ACE**

1. ARM lists all globally accessible directories.
2. Use sorting, filtering, grouping and column selection to locate the desired rows.
3. Select the desired entries.
4. Click "Remove ACE".



1. Leave a comment.
2. Click "Execute Action".

The job will be transferred to the ARM server and executed there. You can find the status in [Jobs overview](#).

## Change directory ownership

### Background / Value

With ARM, you simply change the owner of file server directories. If you exclude users from ownership of directories, you can prevent unwanted permission changes.

### Related features

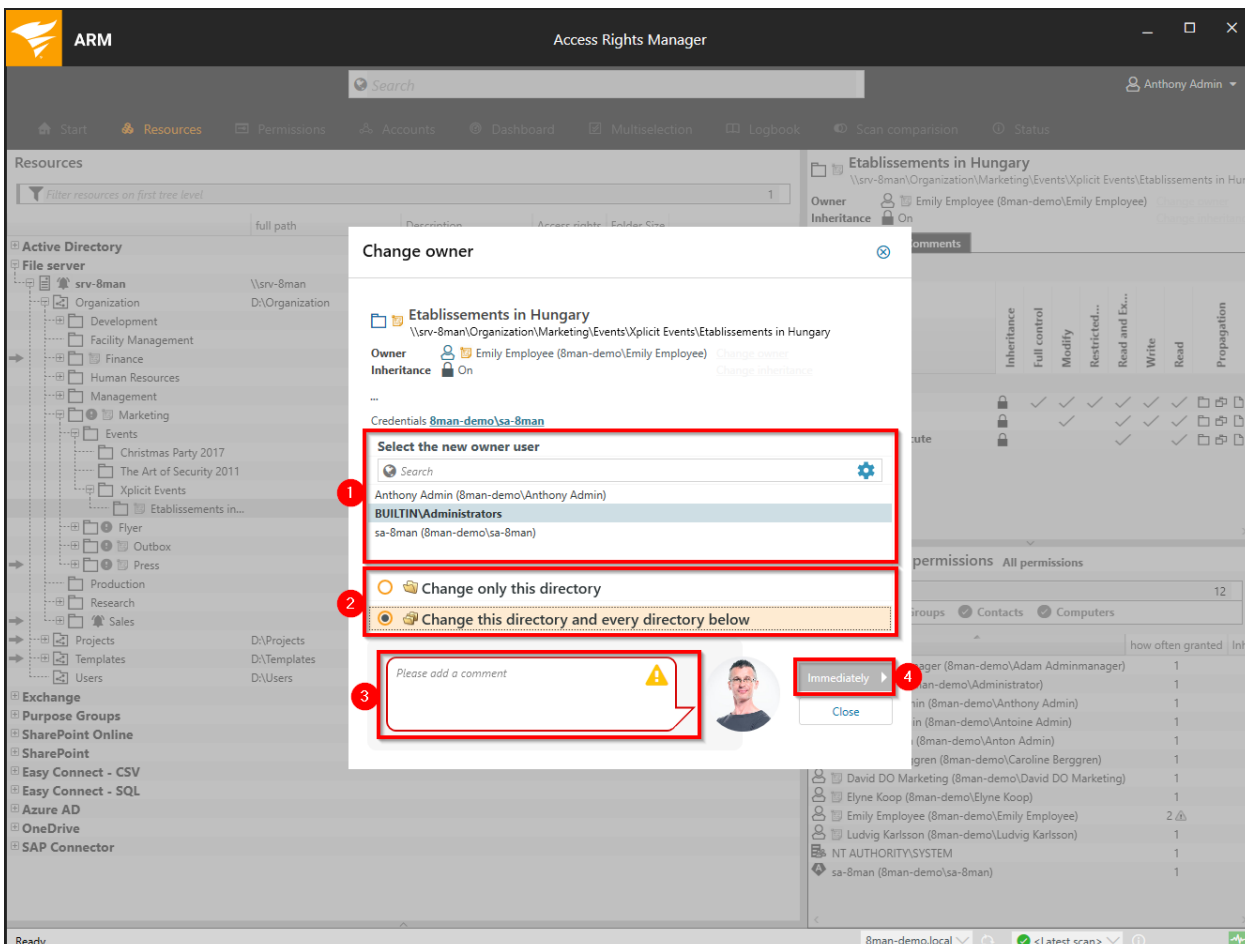
[Identify directories whose owners are not administrators](#) (report)

### Step-by-step process

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The 'Resources' tab is active, showing a tree view of the file system. The path is: \\srv-8man\Organization\Marketing\Events\Xplicit Events\Etablissements in Hungary. The current owner is 'Emily Employee (8man-demo\Emily Employee)'. A 'Change owner' button is visible. The 'All permissions' section shows 'Full control' and 'Modify' permissions. The 'Accounts with permissions' section lists 12 accounts, including 'Adam Adminmanager', 'Administrator', 'Anthony Admin', 'Antoine Admin', 'Anton Admin', 'Caroline Berggren', 'David DO Marketing', 'Elyne Koop', 'Emily Employee', 'Ludvig Karlsson', 'NT AUTHORITY\SYSTEM', and 'sa-8man'.

Name	how often granted	Inhe
Adam Adminmanager (8man-demo\Adam Adminmanager)	1	
Administrator (8man-demo\Administrator)	1	
Anthony Admin (8man-demo\Anthony Admin)	1	
Antoine Admin (8man-demo\Antoine Admin)	1	
Anton Admin (8man-demo\Anton Admin)	1	
Caroline Berggren (8man-demo\Caroline Berggren)	1	
David DO Marketing (8man-demo\David DO Marketing)	1	
Elyne Koop (8man-demo\Elyne Koop)	1	
Emily Employee (8man-demo\Emily Employee)	2	
Ludvig Karlsson (8man-demo\Ludvig Karlsson)	1	
NT AUTHORITY\SYSTEM	1	
sa-8man (8man-demo\sa-8man)	1	

1. Select "Resources".
2. Navigate to the desired directory. Alternatively, use the search.
3. ARM will show you the current owner.
4. Click "Change owner".



1. Determine a new owner.
2. Specify whether the change will only be applied to the current or all subdirectories.
3. You must enter a comment.
4. Start the execution.

## Exchange

ARM provides many features to manage Exchange permissions effectively and documented.

Create a mailbox (email enable accounts)

### Background / Value

With ARM you can create mailboxes (email enable accounts) in Exchange (on-premise).

### Related features

[Create a mailbox in Exchange Online](#)

## Step-by-step process

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. At the top, there is a search bar with a red box around it and a '1' next to it. Below the search bar, there are navigation tabs: Start, Resources, Permissions, Accounts, Dashboard, Multiselection, Logbook, Scan comparison, and Status. The main area is titled 'Graph' and shows a hierarchy of accounts. On the left, there is a 'Parents' tree with a filter set to 'Name' and 14 items. In the center, there are two main nodes: 'All employees (8man-demo)All employees' with 31 members and 'Domain Users (8man-demo)Users' with 1168 members. Below these, there is a node for 'Emily Employee (8man-demo)Emily Employee' with 7 members, highlighted with a red box and a '2'. A context menu is open over this node, with the 'Enable mailbox' option highlighted with a red box and a '3'. On the right, there is a detailed view of the 'Emily Employee' account, showing various attributes like Name, Account Expires, Common Name, Distinguished Name, Display Name, Given Name, Surname, Last Logon, Manager, Mail Address, Name (RDN), Object GUID, Object SID, Primary Group Id, M Account Name, M Account Type, Name, Telephone Number, User Account Control, User Principal Name, Organizational Unit, and Organizational Unit. A profile picture and address information are also visible.

1. Use the search to find the desired user or distribution group of type universal.
2. Right-click on the user, e.g. in the Accounts view.
3. Click on "Enable mailbox" from the context menu.

**i** This option is only available if no mailbox has yet been created. This option is only available for Exchange on-premise. Please see also: [Create a mailbox in Exchange Online](#).

The screenshot shows the 'Enable mailbox' dialog in the SolarWinds Access Rights Manager (ARM) interface. The dialog is for the user 'Emily Employee (8man-demo\Emily Employee)'. It displays the following configuration options:

- Storage:**
  - Mailbox Database: <Select automatically>
  - Archive Database:  Mailbox Database 0349104094 (Default)
- Connectivity:**
  - ActiveSync:  Policy: Default (Default)
  - Outlook Web App (OWA):  Policy: <None>
  - IMAP:
  - POP3:

At the bottom of the dialog, there is a comment field with the placeholder text 'Please add a comment' and a warning icon. A red box highlights this field, with a red circle '2' next to it. To the right of the comment field is an 'Immediately' button with a right-pointing arrow, also highlighted with a red box and a red circle '3'. A 'Close' button is located below the 'Immediately' button. A red box also highlights the 'Storage' and 'Connectivity' sections, with a red circle '1' next to it.

1. Determine the Exchange options.
2. You must enter a comment, for example a ticket number.
3. Start the process.

## Create a mailbox in Exchange Online (assign an Office 365 license)

### Background / Value

With ARM you can create mailboxes in Exchange Online by assigning an Office 365 license that includes Exchange Online.

### Related features

[Create a new user account in Azure Active Directory](#)

[Create a mailbox in Exchange on-premise](#)

### Step-by-step process

The screenshot shows the Access Rights Manager (ARM) interface. The search bar at the top contains the text "new user". The search results are displayed in a list view, with the "Azure AD Accounts (1)" section highlighted. The search results for "new user" are shown in a table format on the right side of the interface.

Name	Value
AccountEnabled	True
AssignedLicenses	Office 365 Business Essentials
DisplayName	new user
GivenName	new
Id	7108567d-4c6c-4d5f-9c5a-5602...
Mail	new.user@8man-demo.com
MailNickname	new.user
SignInSessionsVa...	10/15/2019 3:21:27 PM
Surname	user
UsageLocation	DE
UserPrincipalName	new.user@8man-demo.com
UserType	Member

1. Use the search in Accounts view to find the desired user.
2. Find the desired user in the section "Azure AD Accounts".
3. If needed, configure the search options to include Azure AD Accounts in the search results.



**i** You need a configured and scanned Azure AD resource to perform this action. Please see [Azure AD scans](#).

The screenshot shows the Access Rights Manager (ARM) interface. The main area displays a 'Graph' view of user accounts. A user tile for 'new user (e6d421c0-debd-411f-be4d-67072347a870)' is highlighted with a red box and a red circle labeled '1'. A context menu is open over this tile, with the 'Change license' option highlighted by a red box and a red circle labeled '2'. The right-hand pane shows the 'Attributes' tab for the selected user, displaying a table of user properties.

Name	Value
AccountEnabled	True
AssignedLicenses	Office 365 Business Essentials
DisplayName	new user
GivenName	new
Id	7108567d-4c6c-4d5f-9c5a-5602...
Mail	new.user@8man-demo.com
MailNickname	new.user
SignInSessionsVa...	10/15/2019 3:21:27 PM
Surname	user
UsageLocation	DE
UserPrincipalName	new.user@8man-demo.com
UserType	Member

1. Right-click on the desired user tile.
2. Select Change license.

Change license ⊗

**Change O365 licenses**

**Account**

Displayname

Principal name

**Flow Free**

Enabled

**Included Service Plans**

Common Data Service

Flow Free

**Office 365 Business Essentials**

Enabled

**Included Service Plans**


To Do Plan 1

Exchange Online

Flow For Office 365

Credentials [51ee871b-f9ca-47c2-b0b1-c898b9bd1be2](#)

Please add a comment ⚠



Close **Immediately** ▶

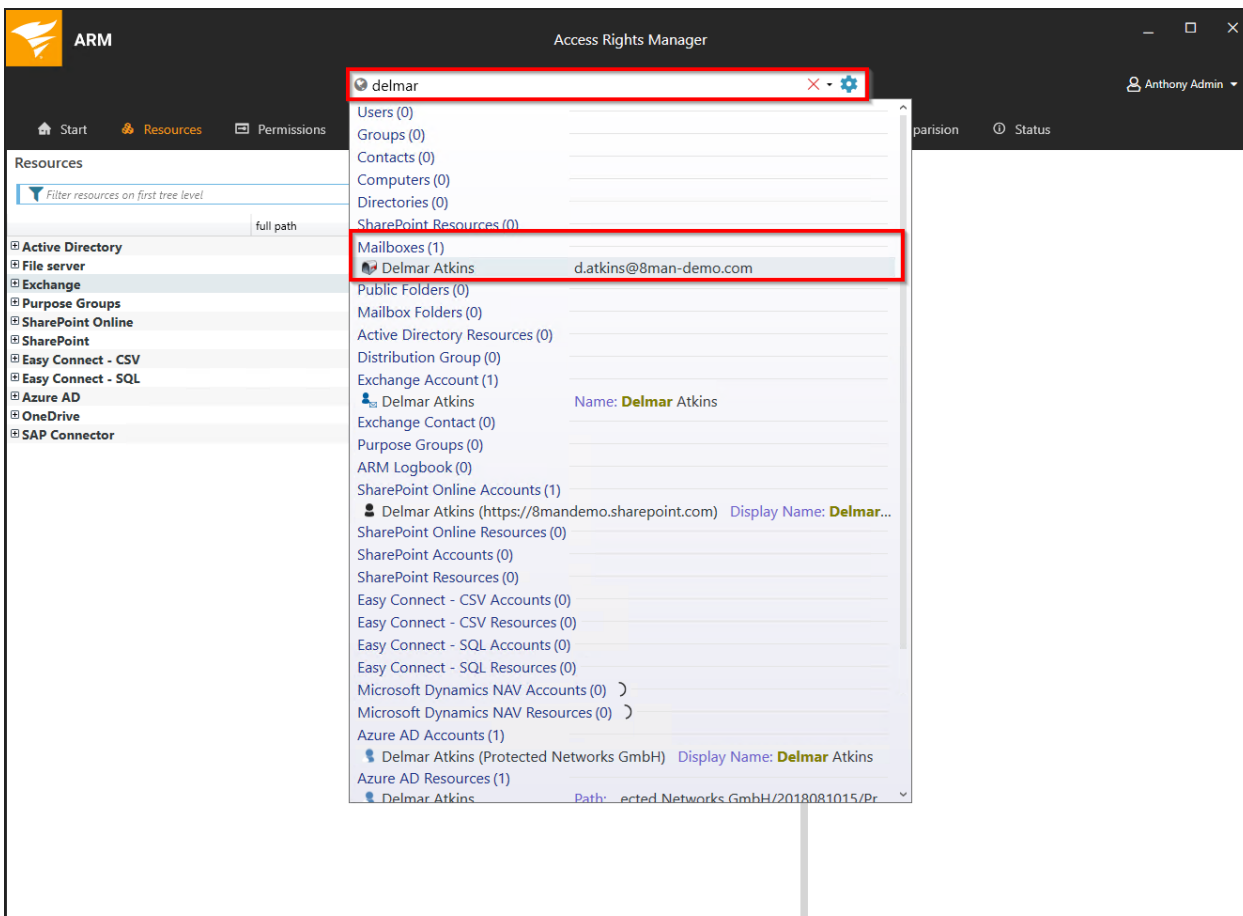
1. Activate a license that includes Exchange Online.
2. You must enter a comment.
3. Start the process.

## Change mailbox permissions

### Background / Value

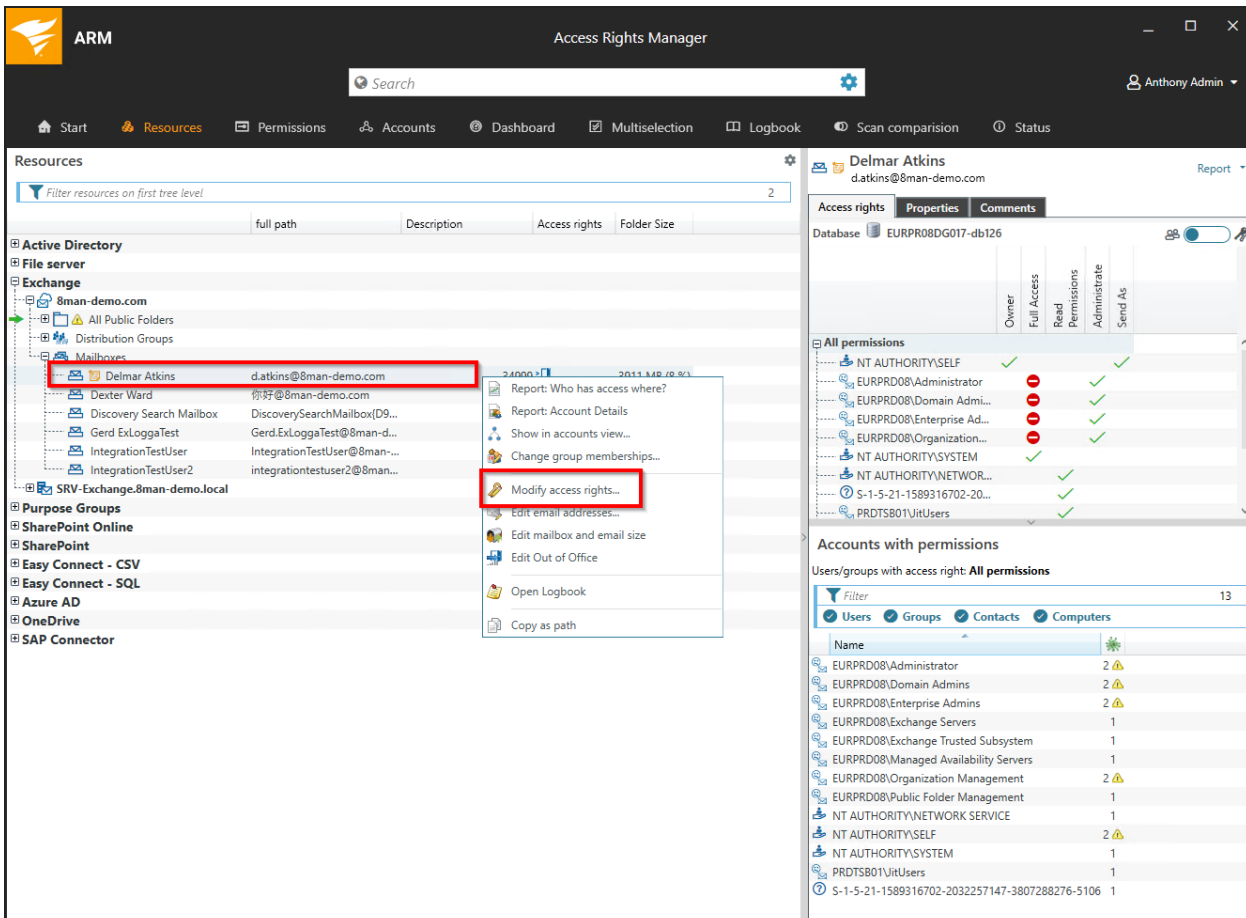
ARM displays the access rights to Mailboxes in the resource view. Mailbox access rights are shown as follows: "Owner", "Full access", "Read permissions", "Administrate" and "Send As". You can manage the following mailbox permissions "Full access", "Send as" and "Receive as".

### Step-by-step process



The screenshot shows the Access Rights Manager (ARM) interface. A search bar at the top contains the text 'delmar'. Below the search bar, a list of resources is displayed. The 'Mailboxes (1)' section is highlighted, showing a single mailbox entry: 'Delmar Atkins' with the email address 'd.atkins@8man-demo.com'. The interface also shows a navigation pane on the left with various resource categories like Active Directory, File server, Exchange, etc.

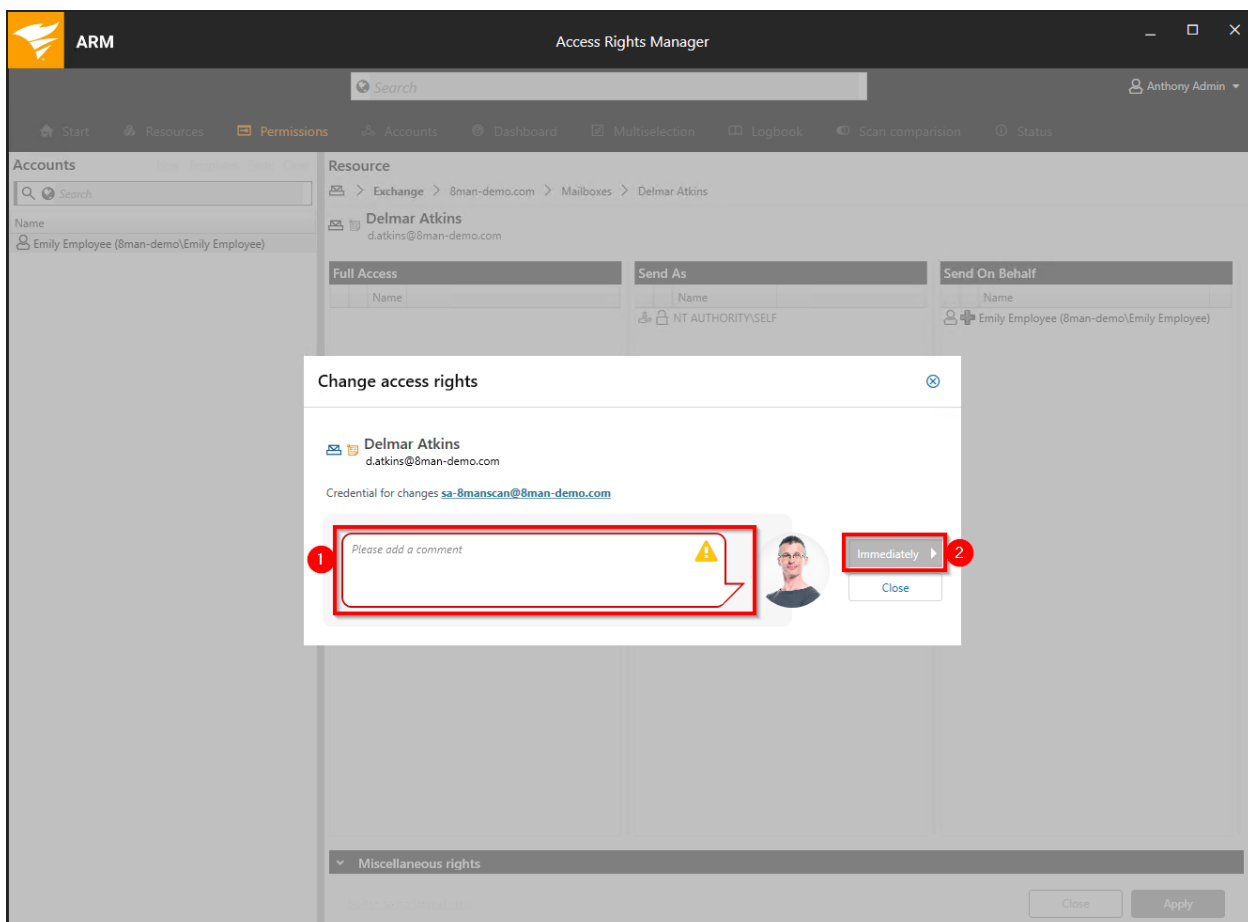
Use the search field to find the desired mailbox.



Right-click on the mailbox and select "Modify access rights" from the context menu.

The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The user is logged in as 'Anthony Admin'. The main area is divided into 'Accounts' and 'Resource' sections. The 'Accounts' section has a search field (1) and a list of accounts, including 'Emily Employee (8man-demo\Emily Employee)'. The 'Resource' section shows a tree view for 'Exchange > 8man-demo.com > Mailboxes > Delmar Atkins'. Below this, there are three columns for permissions: 'Full Access', 'Send As', and 'Send On Behalf'. The 'Send On Behalf' column contains a table with a header 'Name' and one entry: 'Emily Employee (8man-demo\Emily Employee)'. A red arrow (2) points from the account in the 'Accounts' list to this entry. At the bottom right, there are 'Close' and 'Apply' buttons (3).

1. Use the search field to find the desired account.
2. Use drag & drop to move the account to an access rights column.
3. Click on "Apply".



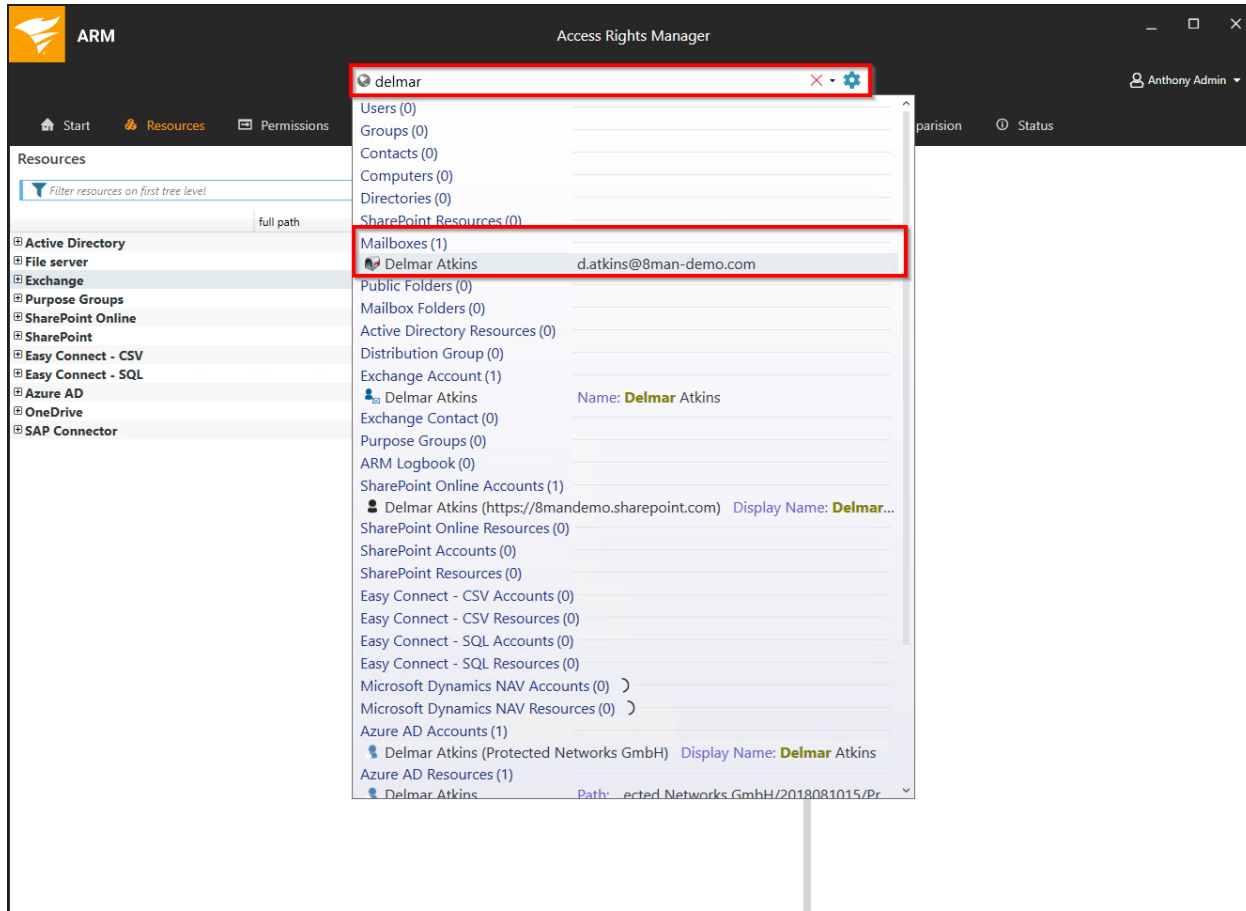
1. You must enter a comment, for example a ticket number.
2. Start the process.

## Manage out of office notices

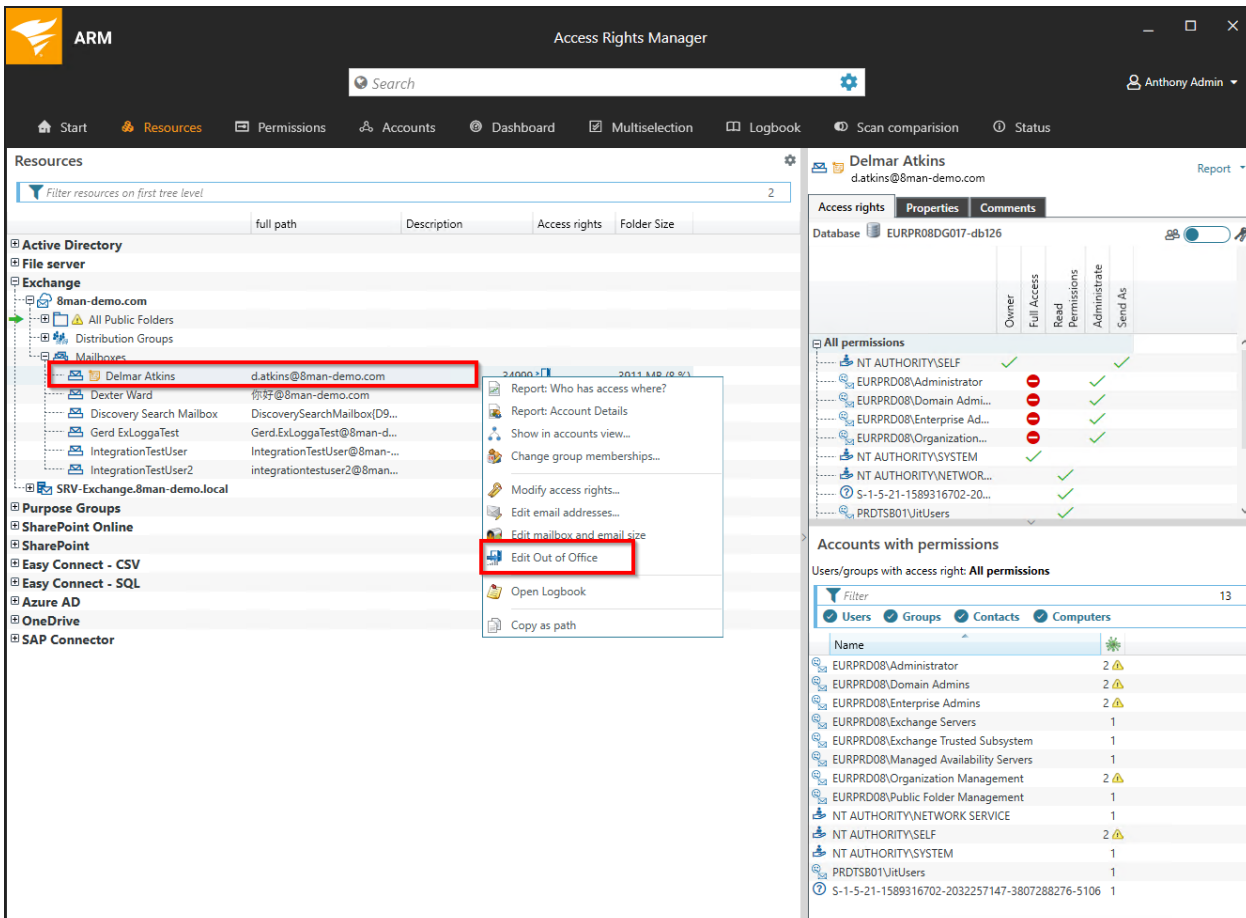
### Background / Value

ARM allows help desk to set out of office notices for employees without gaining access to email content.

### Step-by-step process



Use the search field to find the desired mailbox.



Right-click on the mailbox and select "Edit Out of Office" from the context menu.



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. A dialog box titled "Out of Office" is open for the user Delmar Atkins (d.atkins@8man-demo.com). The dialog has three main sections:

- Section 1 (Red box 1):** A checked checkbox labeled "I am Out of Office for an indefinite period of time". Below it is a text area containing "Out of office in 2019".
- Section 2 (Red box 2):** A text input field with the placeholder "Please add a comment" and a yellow warning icon.
- Section 3 (Red box 3):** A dropdown menu currently set to "Immediately" and a "Close" button.

The background shows the ARM interface with a left-hand navigation pane and a right-hand pane displaying user properties and permissions for Delmar Atkins.

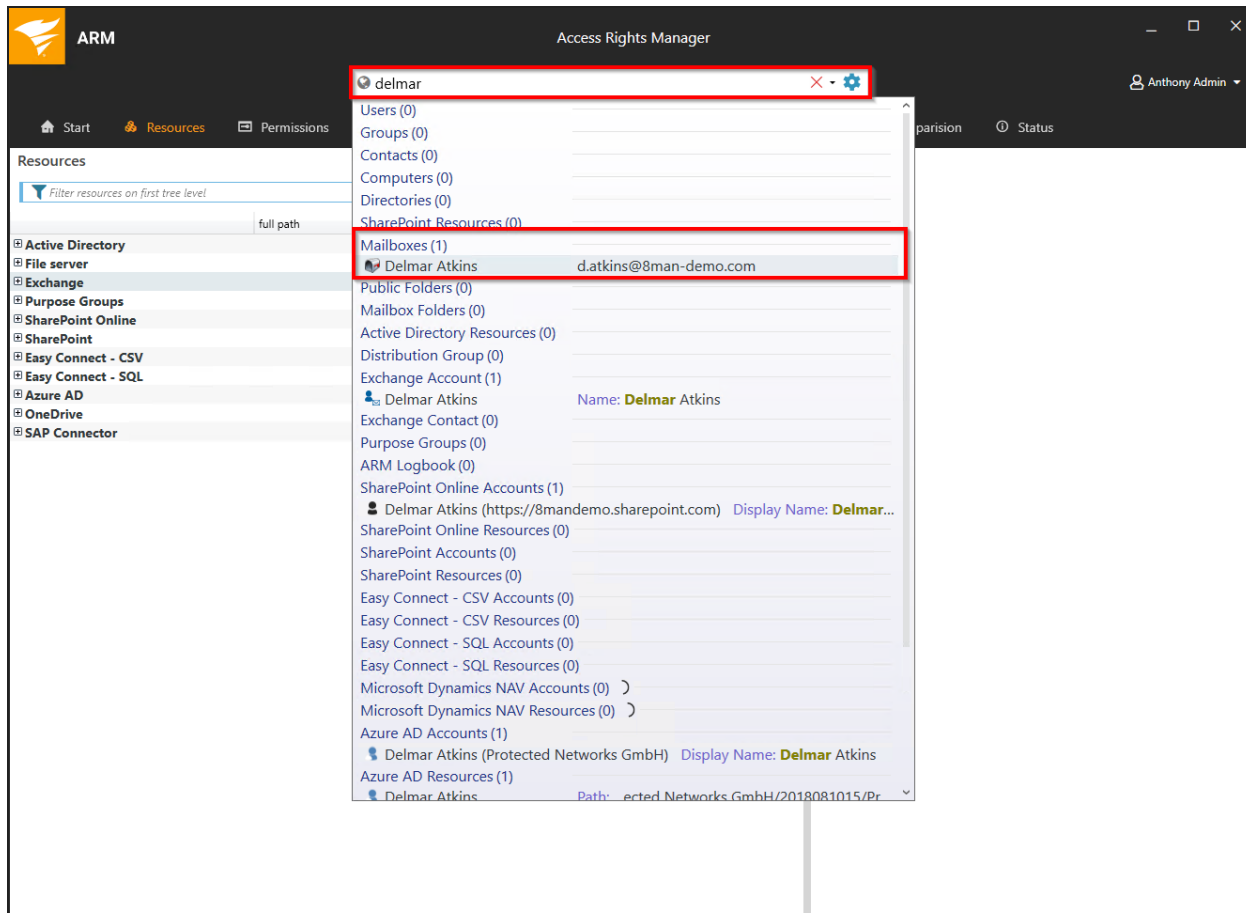
1. Determine the out of office settings.
2. You must enter a comment, for example a ticket number.
3. Start the process.

## Manage mailbox and email size

### Background / Value

Managing mailbox size is a common task for help desk. ARM allows you to make these quickly and efficiently.

### Step-by-step process



Use the search field to find the desired mailbox.

The screenshot shows the SolarWinds ARM interface. On the left, the 'Resources' pane displays a tree view of Exchange mailboxes. The 'Delmar Atkins' mailbox is selected, and a context menu is open with 'Edit mailbox and email size' highlighted. The right pane shows the 'Access rights' for the mailbox, including a table of permissions and a list of accounts with permissions.

Account	Owner	Full Access	Read Permissions	Administrative	Send As
NT AUTHORITY\SELF	✓			✓	
EURPRD08\Administrator		✗		✓	
EURPRD08\Domain Admins		✗		✓	
EURPRD08\Enterprise Ad...		✗		✓	
EURPRD08\Organization...				✓	
NT AUTHORITY\SYSTEM	✓				
NT AUTHORITY\NETWORK...			✓		
S-1-5-21-1589316702-20...			✓		
PRDTSB01\itUsers			✓		

Name	Count	Warning
EURPRD08\Administrator	2	⚠
EURPRD08\Domain Admins	2	⚠
EURPRD08\Enterprise Admins	2	⚠
EURPRD08\Exchange Servers	1	
EURPRD08\Exchange Trusted Subsystem	1	
EURPRD08\Managed Availability Servers	1	
EURPRD08\Organization Management	2	⚠
EURPRD08\Public Folder Management	1	
NT AUTHORITY\NETWORK SERVICE	1	
NT AUTHORITY\SELF	2	⚠
NT AUTHORITY\SYSTEM	1	
PRDTSB01\itUsers	1	
S-1-5-21-1589316702-2032257147-3807288276-5106	1	

Right-click on the Mailbox and select "Edit mailbox and email size" from the context menu.

1. Click on "Customize" to change the mailbox sizes and warning messages threshold.
2. Quickly add 1 GB of storage. The [increments](#) can be adjusted in the configuration application.
3. Click on the pen icon to edit the maximum email size.
4. You must enter a comment, for example a ticket number.
5. Start the process.

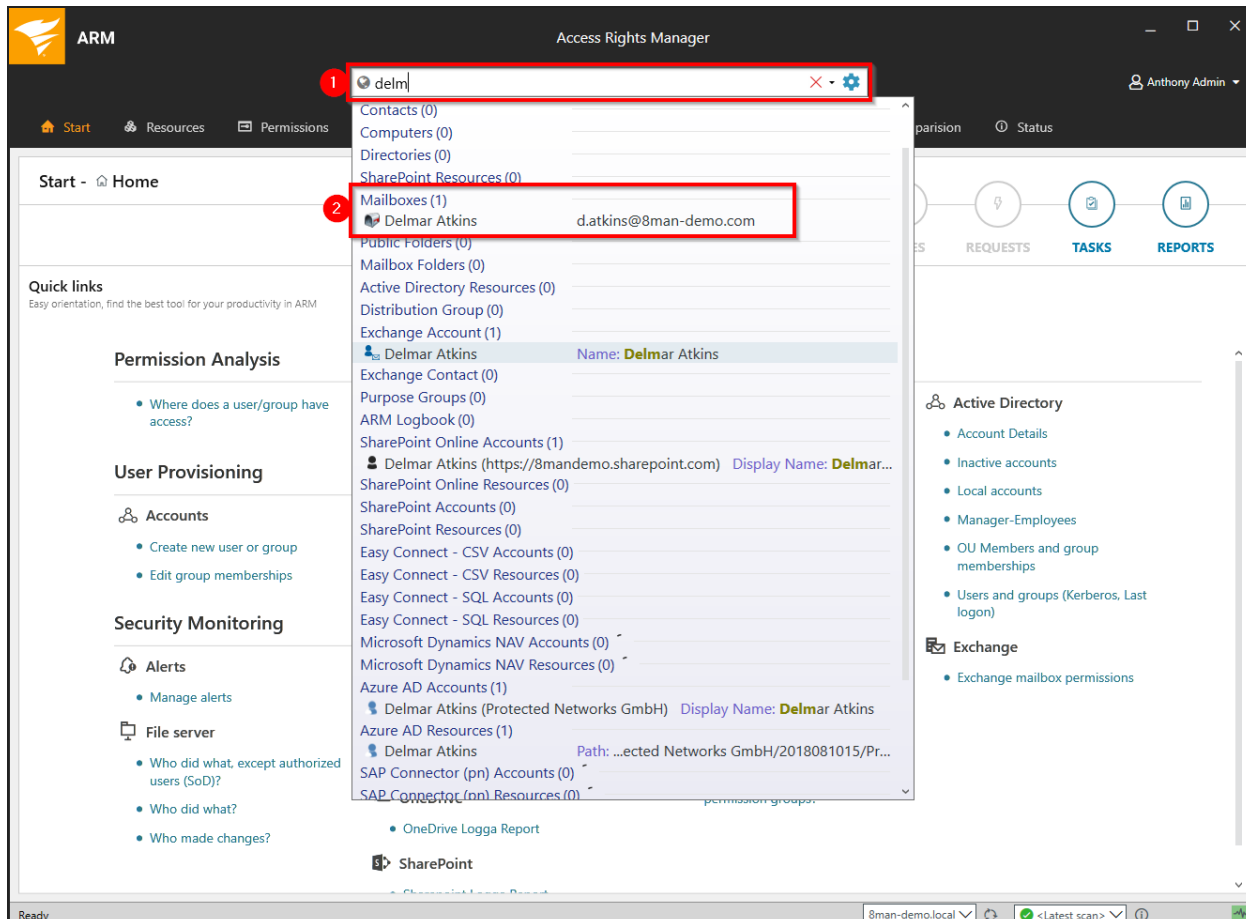
## Manage email addresses

### Background / Value

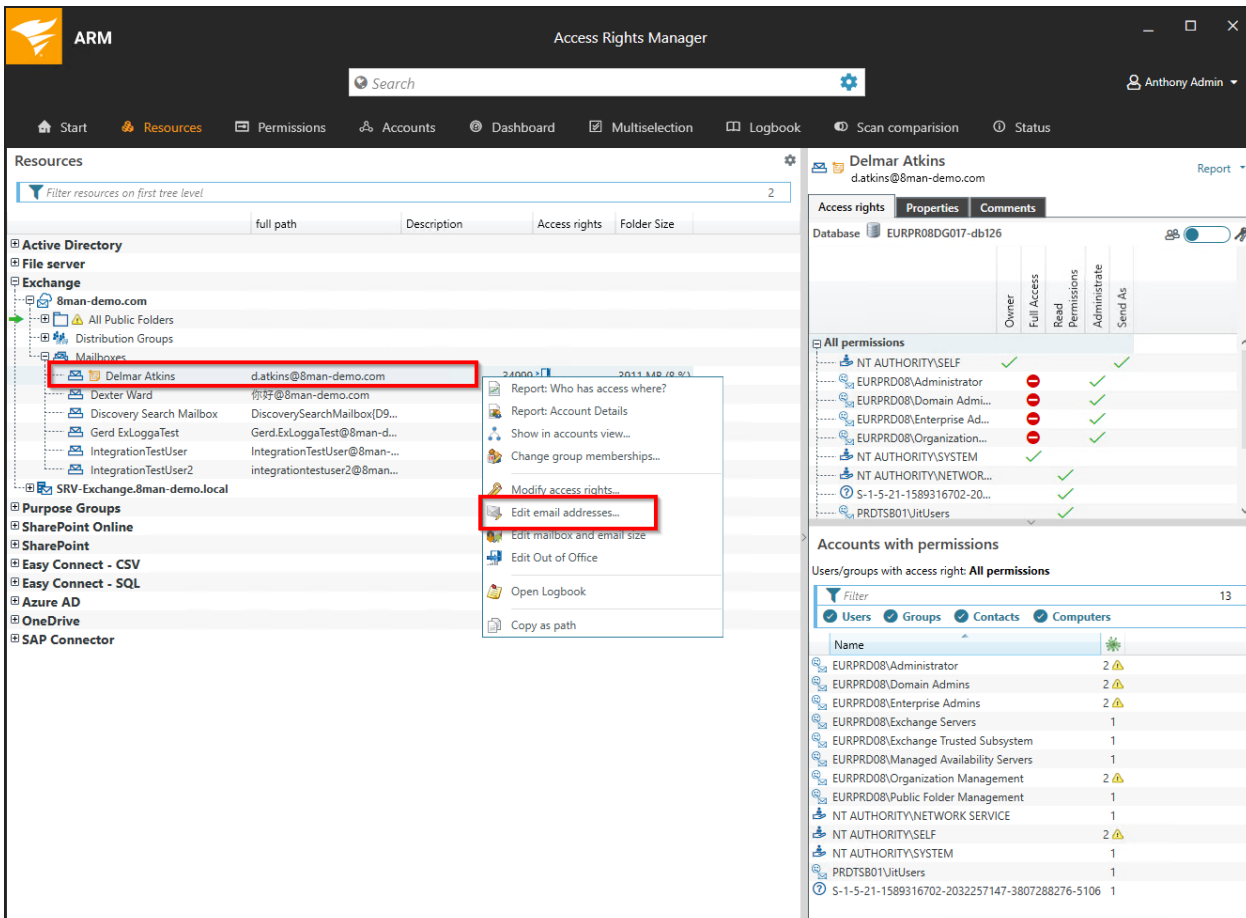
With ARM you can assign and remove multiple email addresses to mailboxes, distribution groups and contacts.

The process is documented automatically.

### Step-by-step process



Use the search field to find the desired mailbox.



Right-click on the Mailbox and select "Edit email addresses" from the context menu.

The screenshot shows the 'Edit email addresses' dialog for user Delmar Atkins. The dialog contains a table of email addresses and a comment field. Red callouts 1-5 highlight the following elements:

- 1. Add or delete button (plus and minus icons)
- 2. Primary address checkbox
- 3. Double-click on the value field
- 4. Comment field (Please add a comment)
- 5. Immediately button

Protocol	Primary address	Value
smtp	<input type="checkbox"/>	d.atkinssss@8man-demo.com
smtp	<input type="checkbox"/>	d.atkins@8mandemo.onmicrosoft.com
SMTP	<input checked="" type="checkbox"/>	d.atkins@8man-demo.com
SPO	<input checked="" type="checkbox"/>	SPO_c20a7426-2ef4-4435-8d3f-3354f5dca7d9@SPO_e6d421c0-debd-41f6-be4d-67072347a870
SIP	<input checked="" type="checkbox"/>	d.atkins@8man-demo.com

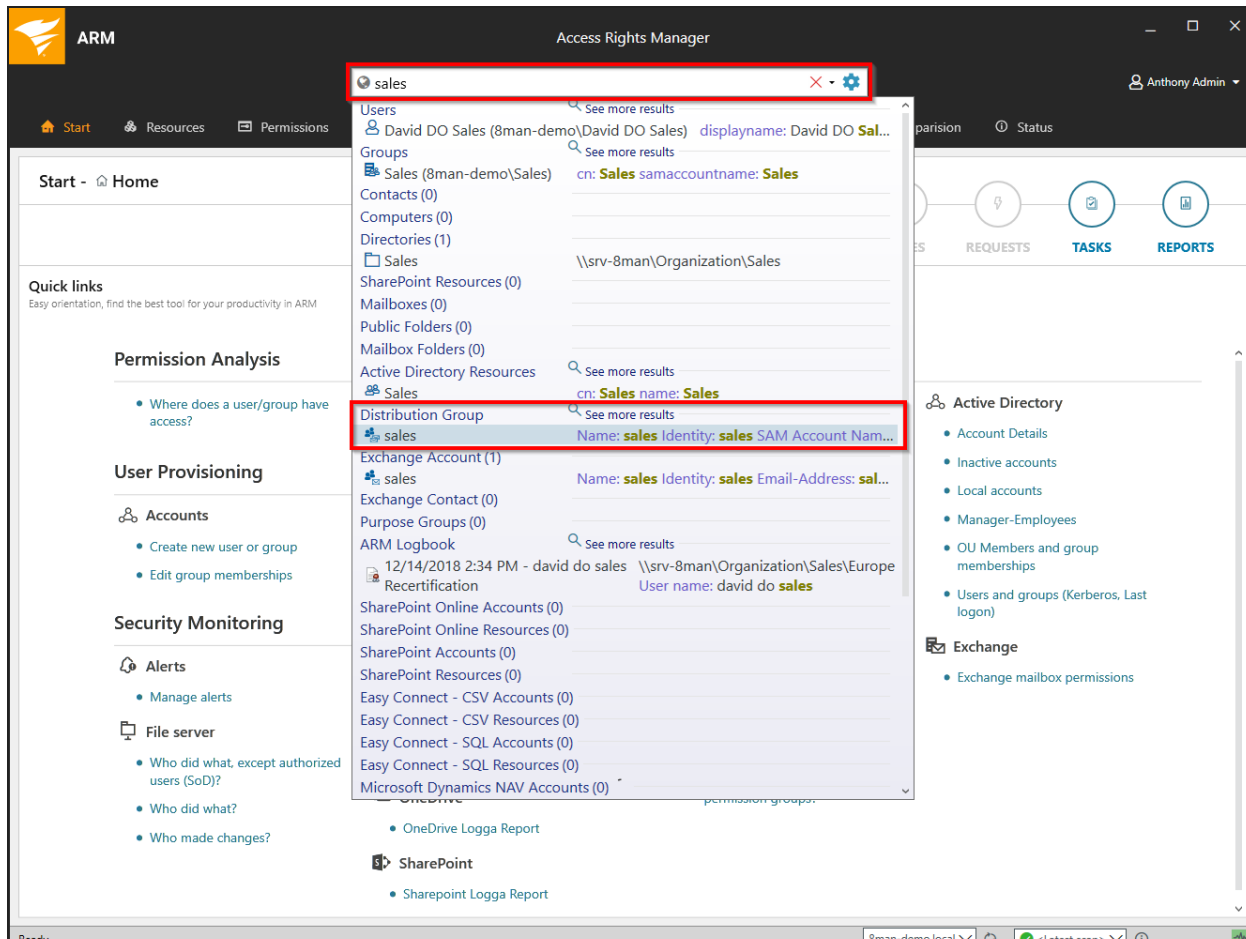
1. Add an email address or delete an existing one.
2. Set the primary address.
3. Double-click the field where you want to enter or change the address.
4. You must enter a comment, for example the ticket number.
5. Start the process.

## Manage distribution group memberships

### Background / Value

ARM allows you to manage the members of distribution groups. This includes the addition and removal of recipients as well as the nesting within other groups (parent child relationships). The process is automatically documented.

### Step-by-Step process



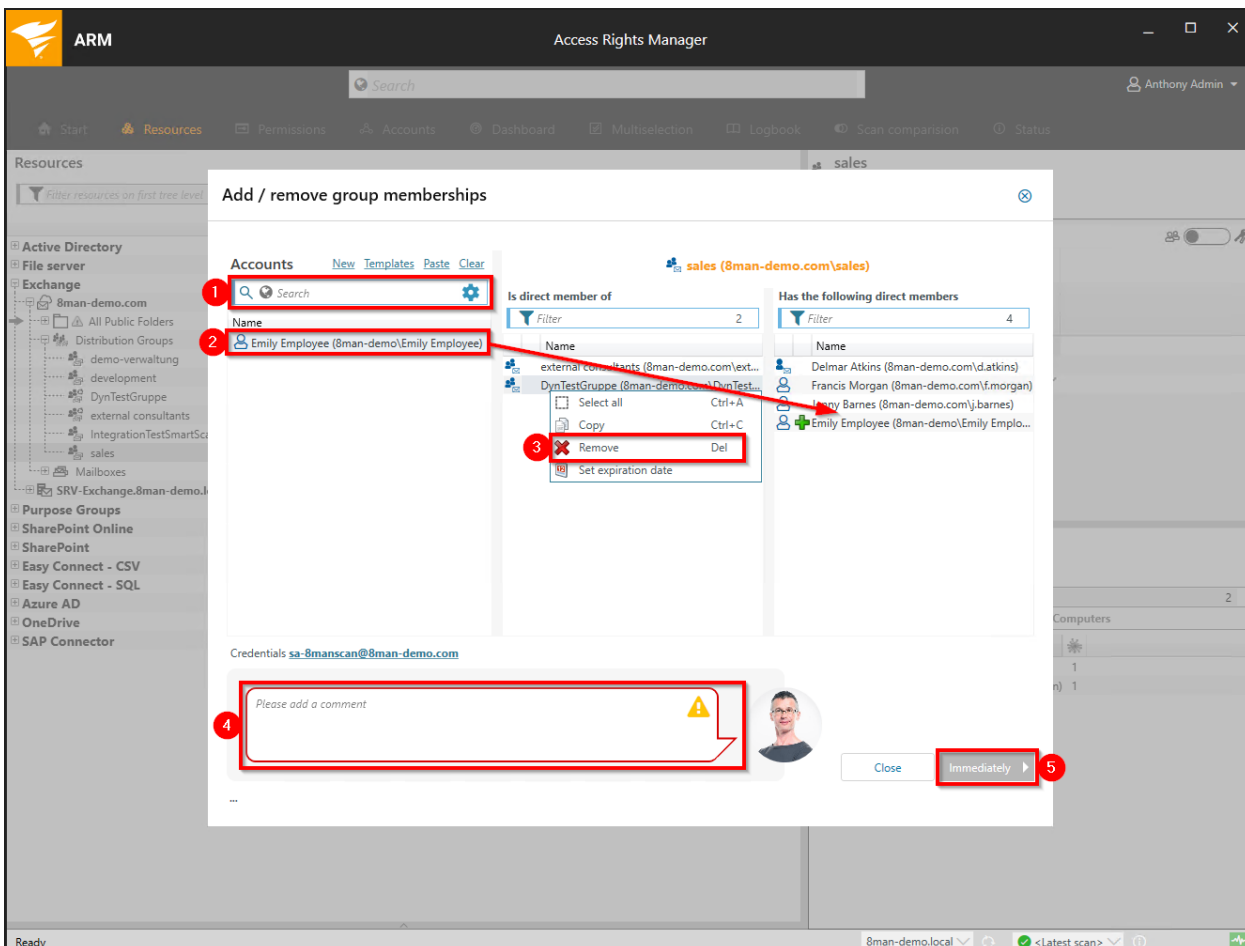
Use the search field to find the desired distribution group.



The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The main window is titled "ARM Access Rights Manager" and shows a search bar and a navigation menu. The "Resources" pane on the left displays a tree view of resources, with the "sales" group under "Exchange" selected. A context menu is open over the "sales" group, and the "Change group memberships..." option is highlighted. The right pane shows the "Access rights" tab for the "sales" group, displaying a list of permissions and a table of accounts with permissions.

Name	Count
h.armitage@8man-demo.com	1
Richard Pickman (8man-demo.com/r.pickman)	1

1. ARM focuses on the desired group.
2. Right-click on the group and select "Change group memberships".



1. Use the search to find the desired account.
2. Use drag & drop to move the account to a column, to assign a group membership.
3. To remove a membership use right-click and then select "Remove" from the context menu.
4. You must enter a comment, for example a ticket number.
5. Start the process.

## Manage distribution group permissions

### Background / Value

ARM allows you to change who can send emails from which distribution groups. As usual, this is automatically documented. The most relevant cases are "Send as" and "Send on behalf". The former is especially sensitive since it is not clearly indicated who actually sent the Email. With "Send on behalf" on the other hand the "deputy" sender is clearly visible.

### Step-by-step process

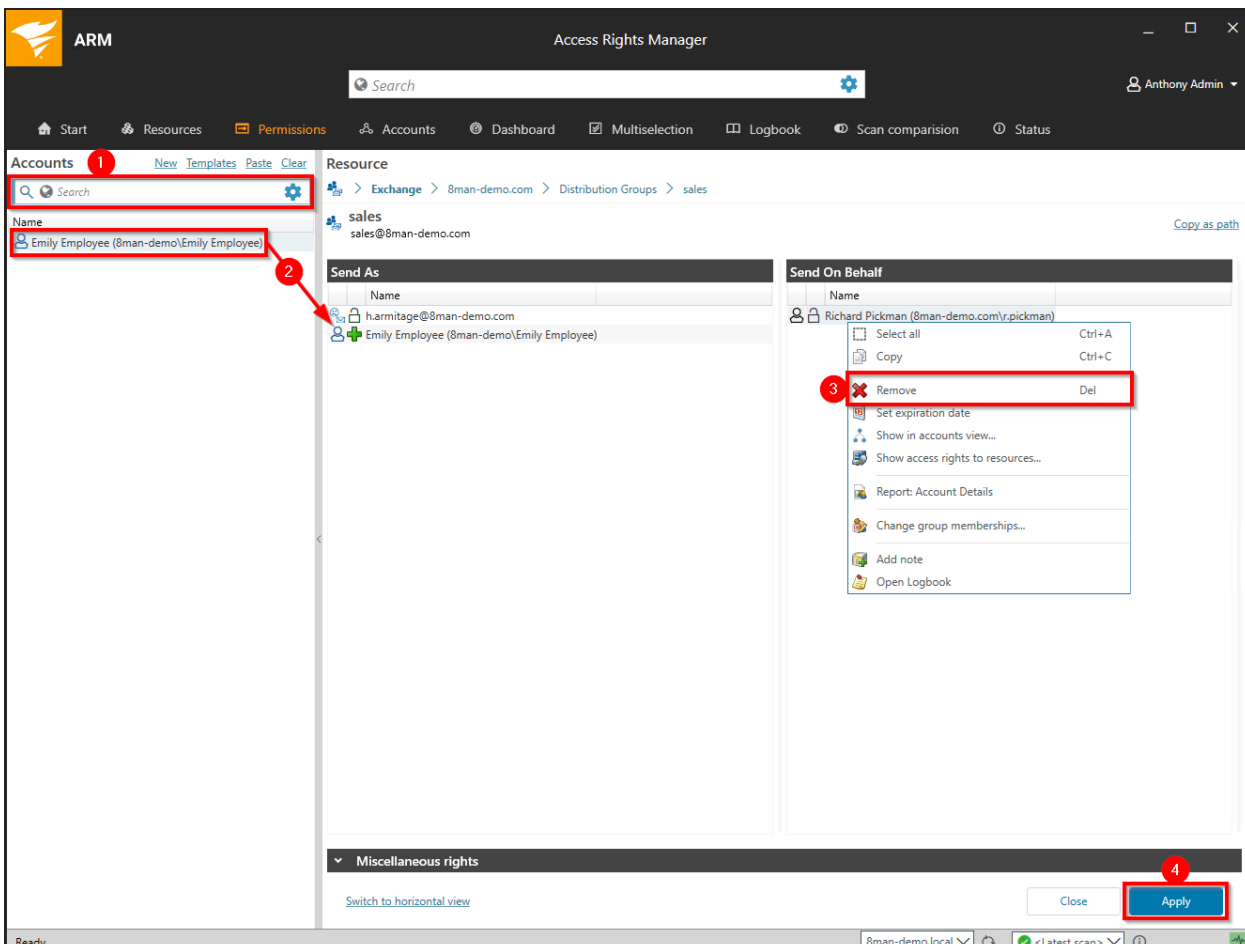
The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The search bar at the top contains the text "sales". A search results dropdown menu is open, listing various system resources. The "Distribution Group" entry is highlighted, showing details such as "Name: sales Identity: sales SAM Account Nam...". The interface includes a sidebar with navigation options like "Start", "Resources", and "Permissions", and a main content area with sections for "Permission Analysis", "User Provisioning", and "Security Monitoring".

Use the search field to find the desired mailing list.

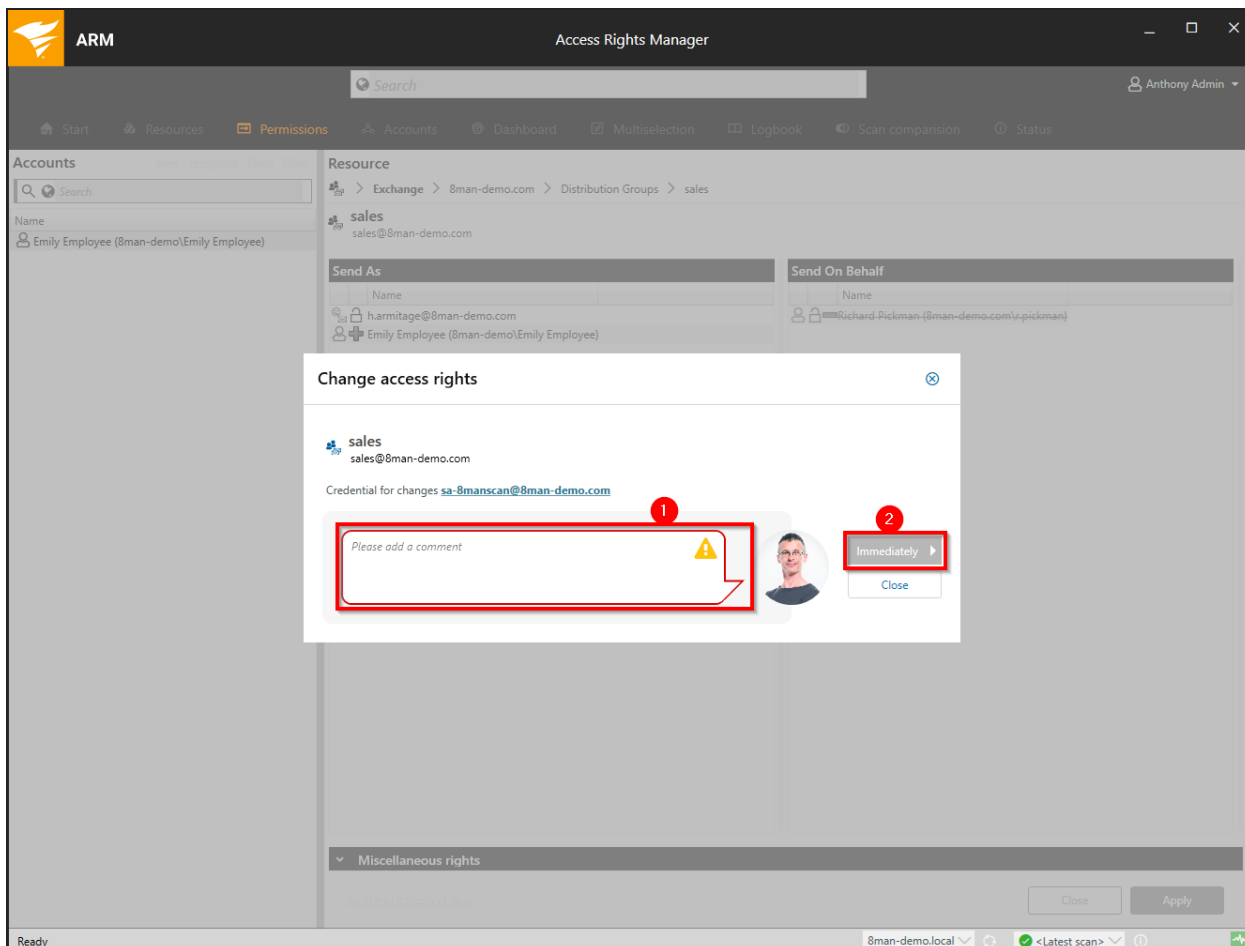
The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. The left pane shows a tree view of resources under the 'Exchange' section, with the 'sales' distribution group selected and highlighted by a red box and a red circle labeled '1'. A context menu is open over the 'sales' group, with the 'Modify access rights...' option highlighted by a red box and a red circle labeled '2'. The right pane shows the 'Access rights' tab for the 'sales' group, displaying a table of permissions. Below this, the 'Accounts with permissions' section shows a table of users/groups with access rights.

Name	Count
h.armitage@8man-demo.com	1
Richard Pickman (8man-demo.com/r.pickman)	1

1. Select the desired distribution group.
2. Right-click on the group and select "Modify access rights" from the context menu.



1. Use the search function to find the account.
2. Use drag & drop to assign the desired permission.
3. Right-click on an entry and select "Remove" from the context menu to remove a permission.
4. Click on "Apply".




1. You must enter a comment.
2. Start the process.

## Modify moderation of distribution groups

### Background / Purpose

With ARM you can quickly modify the moderation of distribution groups. The process will be documented automatically.

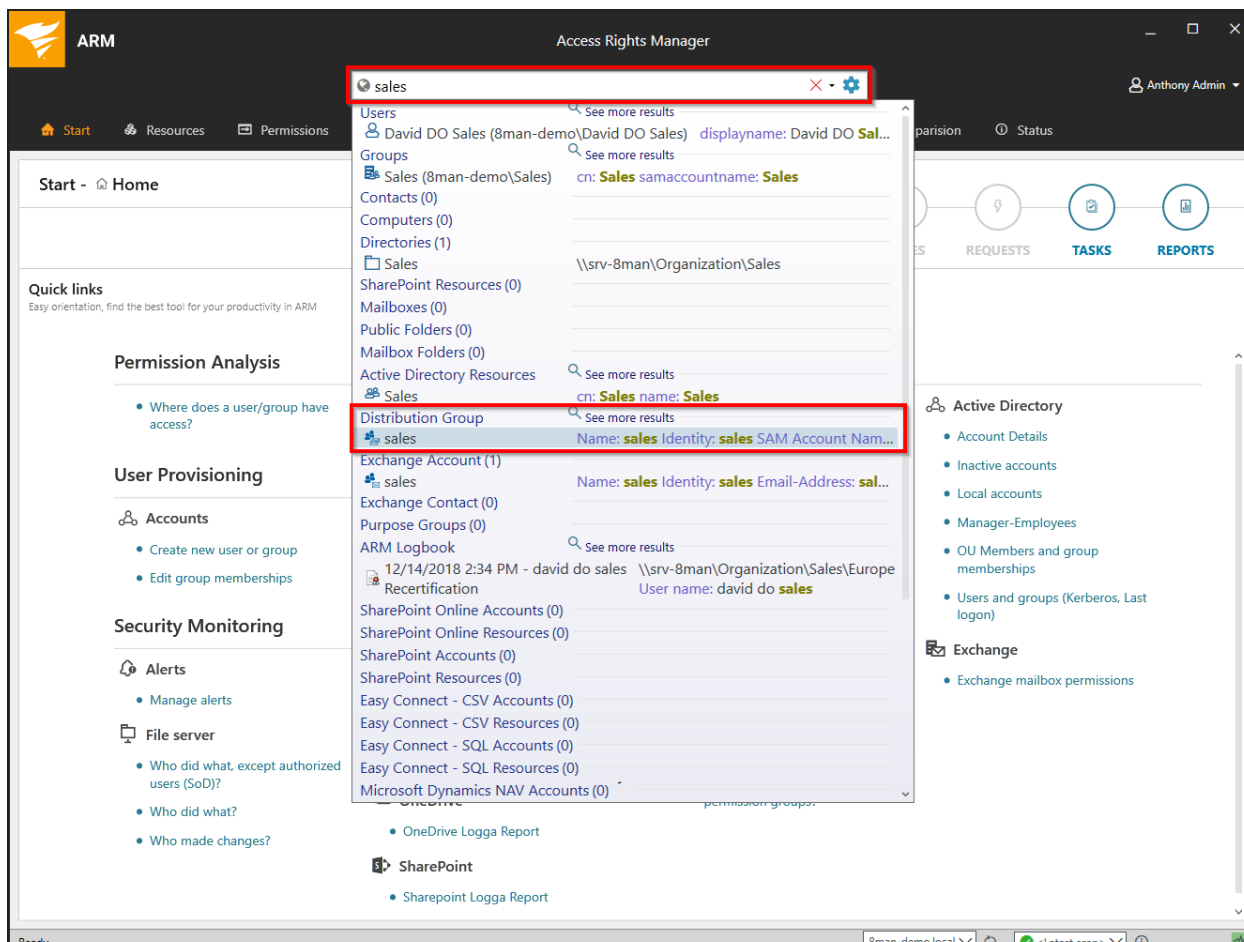
If no moderators are nominated the role is filled out by the manager of the group.

 The change also works for dynamic Exchange groups.

### Related features

[Change the manager of distribution groups](#)

### Step-by-step process



Use the search field to find the desired distribution group.

The screenshot shows the 8MAN interface with the 'sales' group selected in the Resources tree. A context menu is open over the 'sales' group, and the 'Edit moderation...' option is highlighted. The right-hand pane shows the 'Access rights' for the 'sales' group, listing 'All permissions' for Richard Pickman and Henry Armitage. The bottom pane shows 'Accounts with permissions' for 'All permissions', listing Henry Armitage and Richard Pickman.

Resources

Resources filter first level 2

Active Directory

File server

SharePoint

Exchange

8man-demo.onmicrosoft.com

All Public Folders

Distribution Groups

development development@8man-demo...

externalConsultants externalConsultants@8man...

sales sales sales@8man-demo.com

Mailboxes

srv-exchange13.8man-dem

vSphere

Purpose Groups

SAP-System

SharePoint 2010

SharePoint Online

Report: Account Details

Show in accounts view...

Change group memberships...

Modify access rights...

Edit email addresses...

Edit manager

Edit moderation...

Create Purpose Group

Open Logbook

Copy as path

Access right Properties Members

Access rights

Send On Behalf Send As

All permissions

Richard Pickman (8man-...)

Henry Armitage (8man-d...)

Accounts with permissions

Users/groups with access right: All permissions

Filter 2

Users Groups Contacts Computers

Name

Henry Armitage (8man-demo.onmicrosoft.com/h.armitage) 1

Richard Pickman (8man-demo.onmicrosoft.com/r.pickman) 1

1. You are focusing in the desired group.
2. Right-click on a group and select "Edit moderation".



The screenshot shows the 'Edit moderation' dialog in the BMAN interface. The dialog is titled 'Edit moderation' and is for the distribution group 'sales' (sales@8man-demo.com). It contains the following elements:


- 1**: A checkbox labeled 'Messages sent to this group have to be approved by a moderator. Please check if managers/owners have a mailbox when you encounter problem enabling the moderation.' which is checked.
- 2**: A search field in the 'Accounts' section.
- 3**: A red arrow pointing from the search results (showing 'Sam Sales der Boss (8man-demo\Sam.Sales)') to the 'Moderators' column.
- 4**: Three radio button options for notification preferences:
  - Notify all senders when their messages aren't approved. (Selected)
  - Notify senders in your organization when their message aren't approved.
  - Don't notify senders when their messages aren't approved.
- 5**: A text area for 'Please add a comment'.
- 6**: A button labeled 'Immediately'.

1. Enable or disable the moderation of the distribution group.
2. Use the search field to find accounts.
3. Use drag & drop to move accounts to the column "Moderators" or "Sender without moderation" (Whitelist).
4. Determine the workflow for rejected messages.
5. You must enter a comment.
6. Start the process.

## Change the manager of distribution groups

### Background / Value

ARM allows you to quickly change managers for distribution groups. The process is automatically documented. In the default settings, managers are the only ones allowed to change the configuration.

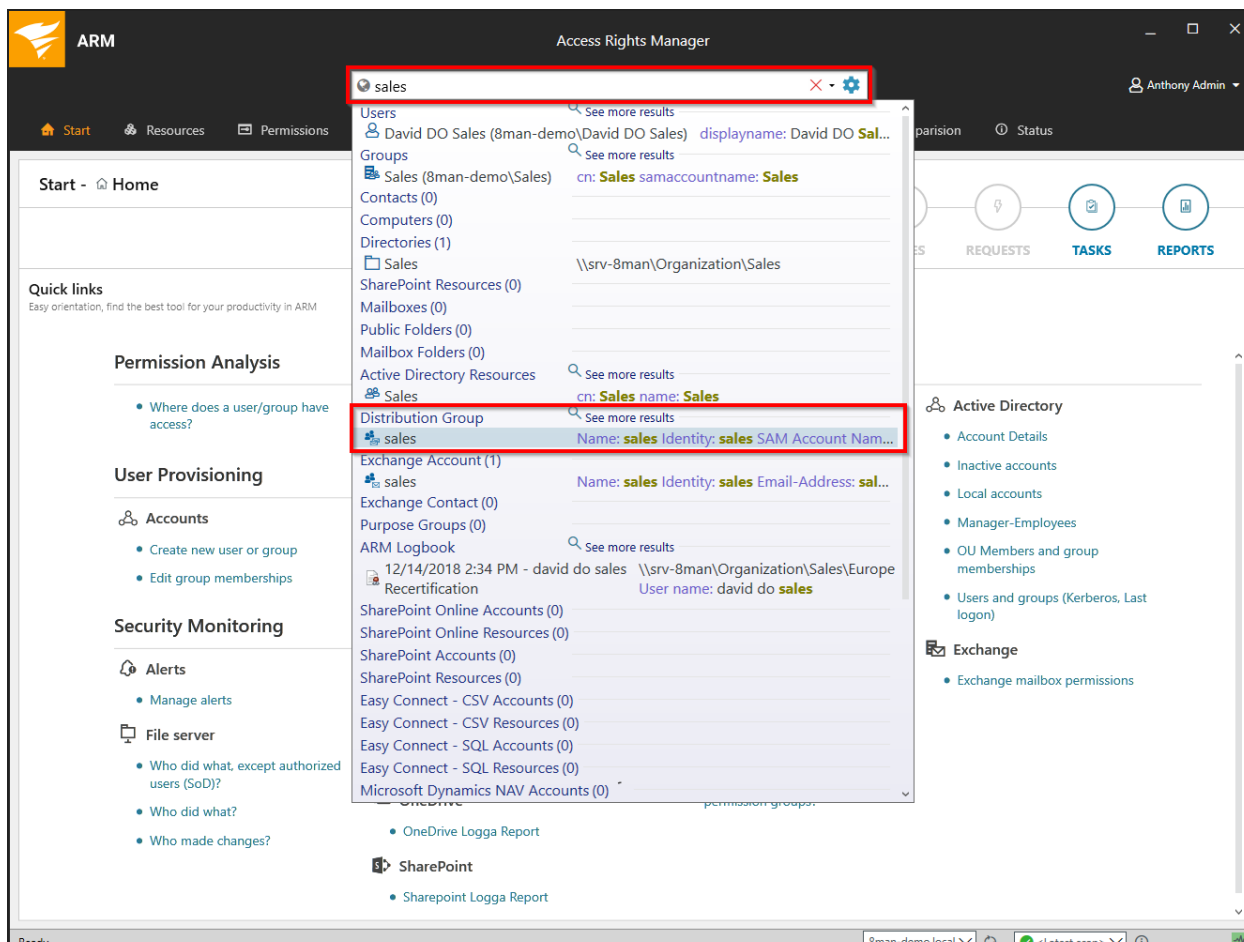
 The change also works for dynamic Exchange groups.

### Related features

[Manage distribution group memberships](#)

[Modify moderation of distribution groups](#)

### Step-by-step process



Use the search field to find the desired distribution group.

The screenshot shows the SolarWinds Access Rights Manager (ARM) interface. The left pane displays a tree view of resources under the 'Exchange' section. The 'sales@8man-demo.com' group is selected, and a context menu is open over it. The 'Edit manager...' option is highlighted. The right pane shows the 'Access rights' tab for the selected group, displaying a list of permissions and a table of accounts with permissions.

**Resources**

full path	Description	Access rights	Folder Size
8man-demo.com			
All Public Folders			
Distribution Groups			
demo-verwaltung	demo-verwaltung@8mande...		
development	development@8man-demo...		
DynTestGruppe	dyntestgruppe@8man-dem...		
external consultants	externalConsultants@8man...		
IntegrationTestSmartScan	IntegrationTestSmartScan@...		
sales	sales@8man-demo.com		
Mailboxes			
SRV-Exchange.8man-demo.local			
Purpose Groups			
SharePoint Online			
SharePoint			
Easy Connect - CSV			
Easy Connect - SQL			
Azure AD			
OneDrive			
SAP Connector			

**Context Menu**

- Report: Account Details
- Show in accounts view...
- Change group memberships...
- Modify access rights...
- Edit email addresses...
- Edit manager...**
- Edit moderation...
- Edit sender authentication...
- Create Purpose Group
- Open Logbook
- Copy as path

**Access rights**

Properties Members

**All permissions**

	Send On Behalf	Send As
Richard Pickman (8man-d...	✓	
h.armitage@8man-demo...		✓

**Accounts with permissions**

Users/groups with access right: All permissions

Filter

Users Groups Contacts Computers

Name	
h.armitage@8man-demo.com	1
Richard Pickman (8man-demo.com/r.pickman)	1

1. ARM expands the tree and focuses on the desired group.
2. Right-click on the group and select "Edit manager...".

The screenshot shows the 'Edit manager/owner' dialog in the SolarWinds Access Rights Manager. The dialog is titled 'Edit manager/owner' and is for the 'sales' manager (sales@8man-demo.com). It features a search bar (1) containing 'Dexter Ward (8man-demo.com\d.ward)'. Below the search bar is a list of accounts, with 'Dexter Ward (8man-demo.com\d.ward)' selected (2). To the right is a table with columns 'Name' and 'Action'. The table contains one entry: 'Delmar Atkins (8man-demo.com\d.ward)' with a 'Delete' button (3) next to it. Below the table is a 'Credentials' section for 'sa-8manscan@8man-demo.com' with a comment field (4) containing 'Please add a comment'. At the bottom right, there is a 'Close' button and an 'Immediately' button (5).

1. Use the search field to find the desired accounts.
2. Use drag & drop to add accounts.
3. Use right-click to remove accounts.
4. You must enter a comment, for example a ticket number.
5. Start the process.

## Create and delete contacts

### Background / Value

With ARM, you can documented create contacts and manage them quickly, e.g. to add them to distribution groups.

### Related features

[Manage distribution group memberships](#)

### Step-by-step process

1. Select "Start".
2. Click "Create new user or group".

Select a template to create a contact.

**i** ARM provides a sample template for the creation of contacts. You must customize this template before you can use it. See [Customize ARM templates](#).

**i** ARM creates contacts using the Exchange Powershell connection. Therefore, an [Exchange resource](#) configuration including the [preparation of the Exchange Powershell](#) has to be completed.

1. Specify an OU.
2. Enter names and email addresses.
3. You must enter a comment.
4. Start the process.

1. Use the search to find a contact.
2. Click on the search result.

1. ARM switches to the Accounts view.
2. Right-click the contact.
3. Select Delete account.

1. ARM shows the contact to be deleted.
2. ARM shows the login which is used to delete the contact. If necessary, specify other credentials.
3. You must enter a comment.
4. Start the execution.

# SharePoint

ARM provides many features to manage SharePoint permissions effectively and documented.

## Manage SharePoint permissions

### **Background / Value**

Integrating SharePoint into ARM all analytical and management tasks are centralized with access rights management processes for other resources. You can conveniently view all access rights across your network and make changes quickly and efficiently. Managing permissions with ARM also enables you to use the group wizard functionality which creates permission groups on SharePoint automatically.

### **Related features**

[SharePoint change configuration](#)

### **Step-by-step process**

The process is identical to [manage file server directory permissions](#).

## Create SharePoint groups

### **Background / Value**

SharePoint groups can exist separately from Active Directory on a SharePoint server. With ARM you can easily create new SharePoint groups.

### **Related features**

[Manage SharePoint permissions](#)

### **Step-by-step process**

ARM Access Rights Manager

Search

Anthony Admin

Start - Home

HOME NOTES REQUESTS TASKS REPORTS

Quick links  
Easy orientation, find the best tool for your productivity in ARM

**Permission Analysis**

- Where does a user/group have access?

**User Provisioning**

**Accounts**

- Create new user or group
- Edit group memberships

**Resources**

- Edit access rights

**Security Monitoring**

**Alerts**

- Manage alerts

**File server**

- Who did what, except authorized users (SoD)?
- Who did what?
- Who made changes?

**Active Directory**

- AD Logga Report

**Exchange**

- Exchange Logga Report

**OneDrive**

- OneDrive Logga Report

**SharePoint**

**Documentation & Reporting**

- Reports overview
- Where has the user/group access?
- Who has access where?

**File server**

- All 'Authenticated users' permissions
- All 'Everyone' permissions
- All users with direct access
- Directories without administrative owners
- Permission difference
- Unresolved SIDs
- Where have employees of a manager access (file server)?
- Who has access through which permission groups?

**Active Directory**

- Account Details
- Inactive accounts
- Local accounts
- Manager-Employees
- OU Members and group memberships
- Users and groups (Kerberos, Last logon)

**Exchange**

- Exchange mailbox permissions

Ready 8man-demo.local <Latest scan>

Select "Create a new user account or group" on the start page.



The screenshot displays the SolarWinds Access Rights Manager (ARM) interface. A 'Create Accounts' dialog box is open, prompting the user to 'Please select the type of account you want to create'. The dialog features a search filter with the value '16'. The list of options includes:

- Marketing - Create new group (Marketing - Creates a new group)
- Marketing - Create new user (Marketing - Creates a new user with formation rules)
- New Azure AD group in Protected Networks GmbH (Create a new Azure AD group in Protected Networks GmbH)
- New Azure AD user in Protected Networks GmbH (Create a new Azure AD user in Protected Networks GmbH)
- New SharePoint group in https://8mandemo.sharepoint.com** (Create a new SharePoint group in https://8mandemo.sharepoint.com)
- New SharePoint group in SharePoint-Demo (Create a new SharePoint group in SharePoint-Demo)
- Sales - Create new group (Sales - Creates a new group)
- Sales - Create new user (Sales - Creates a new user with formation rules)

The 'Select' button at the bottom right of the dialog is highlighted with a red box. The background interface shows various navigation tabs like 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard', 'Multiselection', 'Logbook', 'Scan comparison', and 'Status'. The user is logged in as 'Anthony Admin'.

Select the template for the desired SharePoint resource.

### Create Accounts ✕

New SharePoint group in https://8mandemo.sharepoint.com (Create a new SharePoint group in https://8mandemo.sharepoint.com)  
Accounts will be created in https://8mandemo.sharepoint.com.

#### Create a new SharePoint group

Name

Description

Owning web site collection

Owner

Who can see the members of this group? 

- Dexter Ward (https://8mandemo.sharepoint.com) Display Name: Dexter Ward

Who can modify the group memberships?

Membership requests

Credentials [<not set>](#) ⚠

Please add a comment

1. Specify a name for the new group.
2. Optional: Enter a description.
3. Select the site collection to which the group is assigned.
4. Use the search to specify an owner.

### Create Accounts ✕

New SharePoint group in <https://8mandemo.sharepoint.com> (Create a new SharePoint group in <https://8mandemo.sharepoint.com>)  
Accounts will be created in <https://8mandemo.sharepoint.com>.

#### Create a new SharePoint group

Name

Description

Owning web site collection https://8mandemo.sharepoint.com)"/> ▾


Owner [Dexter Ward \(<https://8mandemo.sharepoint.com>\)](https://8mandemo.sharepoint.com) ✕ ↺


Who can see the members of this group?  ▾ 1


Who can modify the group memberships?  ▾ 2

Membership requests

- 
-

Credentials [<not set>](#) 

Please add a comment 



▾

1. Select who can see the members of the group.
2. Select who can edit the group memberships.

### Create Accounts

New SharePoint group in https://8mandemo.sharepoint.com (Create a new SharePoint group in https://8mandemo.sharepoint.com)  
Accounts will be created in https://8mandemo.sharepoint.com.

#### Create a new SharePoint group

Name:

Description:

Owning web site collection:

Owner: [Dexter Ward \(https://8mandemo.sharepoint.com\)](https://8mandemo.sharepoint.com) ✕ ↺

Who can see the members of this group?:

1 Who can modify the group memberships?:

^ Membership requests

Allow requests to join/leave the group?

Auto accept?

Send requests to the following e-mail addresses:

2 Credentials

3  ⚠

4

1. Determine how membership requests are handled.
2. Specify credentials that have the permissions to create the new group on SharePoint.
3. You must enter a comment.
4. Start the execution.

# Customize ARM templates

With ARM you can use customized templates for:

- Creating users
- Creating groups
- Creating contacts (Rich Client only)
- Open Order

Customize the templates according to your needs to standardize, simplify and accelerate the creation of objects. We describe the advantages of individualized templates in the next section [Take advantage of customized templates](#).

In the section [All templates](#), we describe the blocks of the templates: The input options with their [properties](#), [constraints](#) and [CreationRules](#). These are the same for all types of templates.

We also provide information on the specific elements of the templates for [users](#), [groups](#), [contacts](#) and [Open Order](#).

## Take advantage of customized templates

ARM provides a set of standard templates, for example for the creation of new users. Based on the template, ARM generates the input masks. Use templates customized to your needs and create new objects in a standardized, simplified and accelerated way. The most important advantages are described below.

### Dropdown menus and lookups

Assign input fields with drop-down menus from which users can choose. Depending on the selection, additional fields can be filled automatically. You avoid incorrect entries, accelerate the input and have a standardized result.

#### *Example*

For the location field, choose "Berlin", "Munich", "Vienna". Based on the selection, the fields "Street", "ZIP" and "City" are filled automatically.

### Validation rules

Validate whether the value entered matches certain rules.

#### *Examples*

- Minimum length for a password
- Check the format of a telephone number

### Group memberships

When creating a user, specify in which groups the new user becomes a member.

### Required fields

Specify which entries must be made (must not remain empty).

### Set default values

Assign fields with default values - changeable or not changeable.

### Creation rules

Determine how a resulting field is filled from entries that have already been made.

#### *Example*

The login name and the email address are automatically generated from the first name and last name.

### Hide input fields

If certain inputs are not required in your company or are already filled with defaults, hide individual input fields or entire areas. This reduces the complexity of the input masks.

## Load templates in ARM

Save Templates in the directory:

**%ProgramData%\protected-networks.com\8MAN\data\templates**

This directory is constantly monitored by ARM on new templates (file watcher). ARM will load new templates automatically based on the .json file extension.

 LDAP attributes used in templates are loaded dynamically.

ARM Access Rights Manager

Search Anthony Admin

Start - Home

HOME NOTES (10) REQUESTS (1) TASKS REPORTS

Quick links

Permission Analysis

User Provisioning

Security Monitoring

Server Health Check

- ARM SQL Database: 8632.00 MB are free on the ARM SQL Express database.
- Scan Archive: 21.66 GB are free on the volume for the archive.
- Alert Message-Queue-System: The state of the Alert-Message-Queue-System is ok.
- ARM database disk space: 21.66 GB are free on the volume for the ARM SQL Server database.
- Templates for user and group creation: 16 templates have been successfully loaded. Click here for further details.

Close

Active Directory

Exchange

1

2

3

If errors occur when the templates are loaded, they are displayed in the [server health check](#). You will also find information on the conditions ([constraints](#)) applied here.

## Edit and name templates

ARM provides sample templates in the directory:

**%ProgramData%\protected-networks.com\8MAN\data\templates**

Remove the extension ".example" and assign the desired filename.

The filenames must end as follows depending on the template type:

- **.CreateNewUser.json**
- **.CreateNewGroup.json**
- **.CreateMailContact.json (rich client only)**
- **.OpenOrderTemplate.json**

### *Example*

"NewUserSales.CreateNewUser.json"

The templates use the JSON format. Customize the templates with appropriate editors.

We recommend using [Visual Studio Code](#) (with syntax check) or [notepad++](#).

You can find more information about the JSON format on [Wikipedia](#).

## All templates - the header of the template

### **"Version": 1**

Leave the value 1.

A value prepared / reserved for future versions of templates.

### **"TemplateType":**

Specify the type of the template. The following types are available:

- CreateNewUser
- CreateNewGroup
- CreateMailContact (rich client only)
- OpenOrderRequest

The entry must match the [file name](#).

### **"Id":**



Assign a unique ID. The format is freely selectable. Doubled IDs result in an error message in the [server health check](#).

We recommend using a GUID, e.g. from [guidgen.com](#).

### "Displayname":

Assign a name for the template. The name is displayed to the ARM user in the template selection (rich client and GrantMA).

### "Description":

Assign a description which is also displayed to the user when the template is selected and helps to further distinguish it.

### "FullQualifiedDomainName":

Specify the FQDN of the domain. Templates can only be mapped to one domain and are only available in this domain.

The value defined here is available as variable [fqdn] for [creation rules](#).

## Availability of input types

	USER	GROUP	CONTACT	OPEN ORDER
<a href="#">TextField</a>	Yes	Yes	Yes	Yes
<a href="#">TextArea</a>	Yes	Yes	Yes	Yes
<a href="#">DropDownList</a>	Yes	Yes	Yes	Yes
<a href="#">FixedValue</a>	Yes	Yes	Yes	Yes
<a href="#">Checkbox</a>	Yes	Yes	No	Yes
<a href="#">Radio</a>	No	No	No	Yes
<a href="#">AccountSearchTextField</a>	No	No	No	Yes
GroupAccountSearchTextField	No	No	No	Yes
DatePicker	No	No	No	Yes
DateRangePicker	No	No	No	Yes
PasswordField	No	No	No	Yes
Numeric	No	No	No	Yes

## Basic structure of an input option

With an input option, you create the prerequisite for the user to enter data into a form.

Prior to the actual input possibility, the allocation, e.g. for which LDAP attribute the input is to be made.

*Example of an assignment in templates for users / groups / contacts*

**"Name": "sn",**

**"Definition": {**

*Properties listing*

**}**

The properties define how the input option is displayed and how it behaves.

### Frequent properties

<b>"Type":</b>	Specifies the type of the input field.
Optional:	no
Characteristics:	This entry must be the first within the definition.
Possible values:	Depending on the template type. An overview of the available types can be found <a href="#">here</a> .
Default value:	
Example:	<b>"Type": TextArea</b>

<b>"Label":</b>	The label of the input field to be displayed.
Optional:	yes
Characteristics:	
Possible values:	any text
Default value:	
Example:	<b>"Label": "[ 'en-us:name', 'de-de:Name', 'fr-fr:Nom' ]"</b>

**"DefaultValue":** A value already pre-filled when the form is loaded.

Optional: yes

Characteristics: depends on Type, see [TextArea](#), [MultiValueText](#), [DropDownList](#)

Possible values: any text

Default value:

Example: **"DefaultValue": "This is a pre-filled value."**

**"IsEnabled":** Indicates whether the field is editable.

Optional: yes

Characteristics: Fields that can not be edited must not be required fields.

Possible values: **true** or **false**

Default value: true

Example: **"IsEnabled":false**

**"IsRequired":** Indicates whether the field is a mandatory field.

Optional: yes

Characteristics: Required fields must not be disabled ("IsEnabled").

Possible values: **true** or **false**

Default value: false

Example: **"IsRequired":true**

**"Description":** Description of the field for display in the tooltip.

Optional: yes

Characteristics:

Possible values: any text

Default value:

Example: **"Description": "Automatically created, non-modifiable comment."**

**"Items":** An items list for a drop down menu.

Optional: no

Characteristics: used only in [DropDownList](#)

Possible values: listing

Default value:

Example: **"Items": [**  
**{ "Value": "Berlin", "DisplayValue": "Berlin - Germany" },**  
**{ "Value": "Paris", "DisplayValue": "Paris - France" }**  
**]**

**"DisplayValue":** Value displayed in conjunction with Value.

Optional: yes

Characteristics: for [DropDownList](#) and [FixedValue](#)

Possible values: any text

Default value:

Example: **"Value": "Berlin", "DisplayValue": "Berlin - Germany"**

**"Value":** Actual value, in conjunction with "DisplayValue".

Optional: yes

Characteristics: for [DropDownList](#) and [FixedValue](#)

Possible values: any text

Default value:

Example: **"Value": "Berlin", "DisplayValue": "Berlin - Germany"**

## Constraints

Use constraints to define:

- Conditions that must be fulfilled when entering the data
- [Creation rules](#)

The specification of constraints is optional.

If you define constraints for LDAP attributes, ARM checks whether the Active Directory also uses constraints for the attribute. If so, the stricter condition is applied. ARM shows in the [server health check](#) which conditions are used.

### Available constraints (all optional)

- **"MaxLength"**: maximum length. Default: -1 (unlimited).
- **"ForbiddenChars"**: Specifies which characters can not be used. Default: [] (empty list).
- **"ValidationRule"**: Regular Expression. Conditions that the entered text must meet.
- **"ValidationInformation"**: Tooltiptext, der bei Verletzung der Constraints angezeigt wird.
- **"UniquenessConstraint"**: "properties/ldap/uniqueness" Ensures that the input for AD attributes is unique (prevents duplicates).
- **"CreationRule"**: A creation rule that automatically calculates and uses the value for the field. Only allowed if [DefaultValue](#) is not set.

Additional validity checks and visibility controls are available for Open Order Templates.

#### Example

```
"Constraints": {  
  "MaxLength": 20  
  "ForbiddenChars": ["ö", "ä", "ü", "ß"],  
  "ValidationRule": "(?=[A-Z])",  
  "ValidationInformation":  
    "Use a maximum of 20 characters, no umlauts and at least one uppercase letter."  
  "CreationRule": "<toLowerCase>(<firstLetter>({givenname}).{sn})",  
}
```

### Multilanguage templates

Templates can be designed multilingual.

The language selected at ARM login is used for the display. If there is no entry for the selected language, the first language is used.

#### Example

```
{  
  "Key": "Name",  
  "Value": {
```

```

"Type": "TextField",
"DefaultValue": "",
"IsRequired": "true",
"Label": "['en-us:name', 'de-de:Name', 'fr-fr:Nom']"
}
},

```

You can find more examples (.example) provided in the setup under:

```
%programdata%\protected-networks.com\8MAN\data\templates
```

## Creation rules

All input fields that can contain a constraints field can define a CreationRule within the constraints field, which automatically calculates the value of the field.

Creation rules are only valid if you do not define a default value.

Creation rules can be linked to one another as desired, e.g. „<firstLetter>({givenname}).{sn}@[fqdn]“. Spaces are also relevant.

The creation rule is also executed when the field:

- Is hidden ("**IsHiddenFromRequester**": true or "**IsHidden**": true)
- Is not editable ("**IsEnabled**": false)

Possibilities for creation rules

### {sn}

This text is replaced by the current value of the input field for the LDAP attribute specified in curly braces (in this example, "sn").

This also works if the referenced input field is hidden and / or not editable.

If the referenced field contains a creation rule, it is executed first. The order of execution is calculated on the basis of such field dependencies. If the creation rules of a template form a cyclic field dependency (for example, if the creation rule for "sn" contains {cn} and that for "cn" {sn}), the template is rejected as invalid. The error is displayed in the [server health check](#).

### [fqdn]

This text is replaced by the domain name defined in the template ([FullQualifiedDomainName](#)).

### Hello 123

Strings are accepted one by one, in this case "Hello 123".

The following special characters must be escaped with a backslash (\): backslash, round brackets, braces, comma.

Note: In JSON format, the double quotes and the backslash must be escaped with a backslash. Backslashes in creation rules must therefore be doubled, e.g.

- "\\(" for the round bracket
- "\\\" for a single backslash

A simple solution is provided by online tools that perform escaping for the JSON format e.g. <http://www.infobyip.com/jsonencoderdecoder.php>. So you only have to manually perform the escaping for the creation rules.

### **<firstLetter>(…)**

Returns the first character of the argument.

*Example*

<firstLetter>(Hello) is replaced by "H".

### **<toUpperCase>(…)**

Converts the argument to uppercase.

*Example*

<toUpperCase>(Hello) is replaced by "HELLO".

### **<toLowerCase>(…)**

Converts the argument to lowercase.

*Example*

<toLowerCase>(Hello) is replaced by "hello".

### **<trim>(…)**

Deletes spaces at the beginning and end of the argument.

*Example*

<trim>( Hello ) is replaced by "Hello".

### **<subst>(…)**

Deletes blanks and hyphens from the argument, replacing letters with accents by letters or combinations of letters

without accents.

*Example*

<subst>(Zoë Roßmäßler-Öker) is replaced by "ZoeRossmuesslerOeker".

**<replace>(.,.,.)****<replaceOnce>(.,.,.)>**

Replaces characters.

*Examples*

<replace>(the dog and the fox,the,a) = "a dog and a fox"

<replaceOnce>(the dog and the fox,the,a) = "a dog and the fox"

<replace>(Norbert Van Eggert, ,) = "NorbertVanEggert"

<replace>(Norbert Van Eggert, ,,) = "Norbert.Van.Eggert"

**<reverse>(..)**

Reverses the order of the characters.

*Example*

<reverse>(apfel) = "lefpa"

**<regExpr>('...',...)**

Specifies the first match of the regular expression (within the single quotation marks), applied to the second

argument (begins immediately after the comma, spaces after the comma are counted).

*Example*

<regExpr>('.{3}',Hello) Is replaced by "Hel".

All common regular expressions are supported. As a special feature, the grouping construct (? <This> ...) is also

supported. The match on this group is returned.

*Example*

<regExpr>('.{3}(?<this>.\*)',Hello) Is replaced by "lo".

There are online tools that can be used to test regular expressions, e.g. <http://regex101.com>.



All functions can be arbitrarily nested.

#### Example

```
<regExpr>('{1}',<trim>(<toLowerCase>({sn})))
```

Complex example for an email address validation

```
"Name": "emailaddresses",
```

```
"Definition": {
```

```
  "Type": "TextArea",
```

```
  "Label": "Email addresses",
```

```
  "IsRequired": true,
```

```
  "IsEnabled": true,
```

```
  "Constraints": {
```

```
    "MaxLength": 500,
```

```
    "ValidationRule": "^[([a-z][a-z0-9]+)?([A-Z][A-Z0-9]+)?(\\w+([-+.']\\w+)*@\\w+([-.]\\w+)*\\.\\w+([-.]\\w+)*(\r\n)?\n?)*$)",
```

```
    "ValidationInformation": "Does not match the email format!",
```

```
    "CreationRule" : "SMTP:<toLowerCase>({samaccountname})@<toLowerCase>([fqdn]
```

```
\\r\nsmtp:<toLowerCase>(<firstLetter>({givenname})).<toLowerCase>({sn})@<toLowerCase>([fqdn])"
```

```
  }
```

```
}
```

#### LookupTable

With **LookupTable**, you create pairs of values that you use to fill fields automatically.

A definition for a lookup table has the following format:

- **LookupTableId**: This identifier is used to refer to the lookup table for additional fields.
- **LookupTable**: Value pairs of the table. The assignment is always one-to-one.

#### Example

In the following example, the user selects a company in a drop-down. Depending on the choice, the street, zip code, city are defined.

Define value pairs

```
"LookupTables": [
```

```
{ "Name": "LookupTableStreet",
  "Definition": {
    "Type": "LookupTable",
    "LookupTableId" : "Street",
    "LookupTable" : {
      "Demo Company Holding": "Demostreet 1",
      "Demo Company Marketing Solutions": "Demostreet 2",
      "Demo Company Services": "Demostreet 3"
    }
  }
},
{ "Name": "LookupTableZIPcode",
  "Definition": {
    "Type": "LookupTable",
    "LookupTableId" : "ZIPcode",
    "LookupTable" : {
      "Demo Company Holding": "10000",
      "Demo Company Marketing Solutions": "20000",
      "Demo Company Services": "90000"
    }
  }
},
{ "Name": "LookupTableCity",
  "Definition": {
    "Type": "LookupTable",
    "LookupTableId" : "City",
    "LookupTable" : {
      "Demo Company Holding": "Berlin",
      "Demo Company Marketing Solutions": "Hamburg",
      "Demo Company Services": "Munich"
    }
  }
}
```

```
    }  
  }  
],  
Drop down menu and fill the fields  
{  
  "Name": "company",  
  "Definition": {  
    "Type": "DropDownList",  
    "Items": [  
      { "Value": "Demo Company Holding", "DisplayValue": "Demo Company Holding" },  
      { "Value": "Demo Company Marketing Solutions", "DisplayValue": "Demo Company  
Marketing Solutions" },  
      { "Value": "Demo Company Services", "DisplayValue": "Demo Company Services" }  
    ],  
    "Label": "Company"  
  }  
},  
{  
  "Name": "streetAddress",  
  "Definition": {  
    "Type": "TextField",  
    "IsEnabled": false,  
    "Constraints": {  
      "CreationRule": "<lookup>(Street,{company})"  
    },  
    "Label": "Street"  
  }  
},  
{  
  "Name": "postalCode",  
  "Definition": {  
    "Type": "TextField",
```

```

    "IsEnabled": false,
    "Constraints": {
      "CreationRule": "<lookup>(ZIPcode,{company})"
    },
    "Label": "ZIP"
  }
},
{
  "Name": "I",
  "Definition": {
    "Type": "TextField",
    "IsEnabled": false,
    "Constraints": {
      "CreationRule": "<lookup>(City,{company})"
    },
    "Label": "City"
  }
},

```

## Hide input fields

**IsHiddenFromRequester** Specifies that the affected area is not displayed to the requester.

Optional: yes

Characteristics: Effective only in the web client / GrantMA, can be overridden by "IsHidden":true

Possible values: **true** or **false**

Default value: false

Example: "IsHiddenFromRequester":true

**IsHidden** Specifies that the area is never displayed, even to the administrator in the post-processing of requests.

Optional:	yes
Characteristics:	if set to true, IsHiddenFromRequester is ineffective
Possible values:	<b>true</b> or <b>false</b>
Default value:	false
Example:	"IsHidden":true

## TextField

TextField is a single-line text input field.

### *Required*

- Type

### *Optional properties*

- Label
- DefaultValue
- Description
- IsRequired
- IsEnabled
- Constraints

### *Example*

```
{  
  "Type": "TextField",  
  "Label": "Text entry box 1",  
  "DefaultValue": "Apple",  
  "Description": "Please enter something.",  
  "IsRequired": true,  
}
```

## TextArea

TextArea is a multi-line input field for multi-line attributes. In DefaultValue, line breaks (`\r\n`) may be included.

### *Required*

- Type

### *Optional properties*

- Label
- DefaultValue
- Description
- IsRequired
- IsEnabled
- Constraints

### *Example*

```
{  
  "Type": "TextArea",  
  "Label": "Multiline text input field 1",  
  "DefaultValue": "line1\r\nline2\r\nline3",  
}
```

## MultiValue Text

MultiValueText is a text input field for multiple values (for multi-value attributes).

Special conditions for MultiValueText:

- [DefaultValue](#) is a list of text values
- The [Constraints](#) are applied to each line

### *Required*

- Type

### *Optional properties*

- Label
- DefaultValue
- Description

- IsRequired
- IsEnabled
- Constraints

*Example*

```
{  
  "Type": "MultiValueText",  
  "DefaultValue": [ "Apple", "Banana", "Orange" ],  
  "Label": "entry list",  
  "Description": "Please enter one or more values (one per line).",  
  "IsRequired": true,  
  "IsEnabled": true,  
  "Constraints": see Constraints  
}
```

## DropDownList

A **DropDownList** is a selection list with non-editable values.

*Required*

- Type
- Items

*Optional properties*

- Label
- DefaultValue
- Description
- IsRequired
- IsEnabled
- Constraints

In addition, you define:

- "[Items](#)": The list of values to select. A distinction is made here between [DisplayValue](#) (the value displayed in the selection list) and [Value](#) (the actual value that is stored for the LDAP attribute).
- "[DefaultValue](#)": (optional) Specifies the value that is preselected when the template is loaded. This value must match a value in the Items list. Default value: The value of the first entry in Items.

*Example*

```
{
  "Type": "DropDownList",
  "DefaultValue": "Berlin",
  "Label": "Location",
  "Description": "Select the location of the user."
  "Items": [
    { "Value": "Berlin", "DisplayValue": "Berlin - Germany" },
    { "Value": "Vienna", "DisplayValue": "Vienna - Austria" }
  ]
}
```

## FixedValue

**FixedValue** sets a fixed, non-editable value. The displayed value may differ from the value used.

*Required*

- Type

*Optional properties*

- Label

In addition, you define:

- **"DisplayValue"**: The value displayed in the template.
- **"Value"**: The actual value that is stored for the LDAP attribute.

*Example*

```
{
  "Type": "FixedValue",
  "Label": "Fixed value 1",
  "Description": "This is a fixed Value."
  "DisplayValue": "Displayed value",
  "Value": "Real value"
}
```



## Checkbox

A checkbox, which knows the states activated/enabled (true) and deactivated/disabled (false).

Checkboxes are only used in the Modules area for the email activation of users (create a mailbox) and groups (create a distribution group) in Exchange.

### *Required*

- Type

### *Optional properties*

- Label
- DefaultValue (valid values for checkboxes are only **true** or **false**)

### *Example*

**"Name": "createdistributiongroup",**

**"Definition": {**

**"Type": "Checkbox",**

**"DefaultValue": true,**

**"Label": "Create distribution group",**

**}**

## Customize templates for new users

Customize templates according to your needs to standardize, simplify and accelerate the creation of new users.

## Enter Name and OU

### Create account within Active Directory ⊗

Create elements in the selected domain: 8man-demo.local.

Given Name  Surname

Common Name  ⚠

Description

SAM Account Name  ⚠

OU Selection [OU=Demo Users](#)

▼ LDAP Attributes ⚠

▼ Group memberships

▼ Password options


▼ User activation

▼ Create mailbox (Exchange)

▼ Scripting

Credentials [8man-demo\sa-8man](#)

Please add a comment ⚠



[Close](#) [Immediately ▶](#)

...

In the template shown, the first name ("**givenname**") and the last name ("**sn**") are mandatory.

The common name ("**cn**"), the SAM account name ("**samaccountname**") and the description are built by a creation rule.

Create account within Active Directory ✕

Create elements in the selected domain: 8man-demo.local.

Given Name  Surname

Common Name  ⚠

Description

SAM Account Name  ⚠

OU Selection [OU=Demo Users](#)

▼ LDAP Attributes ⚠

▼ Group memberships


▼ Password options

▼ User activation

▼ Create mailbox (Exchange)

▼ Scripting

Credentials [8man-demo\sa-8man](#)

Please add a comment  ⚠ 

Close Immediately ▶

...

To select the OU in which the new user is stored. A click on the link opens up an OU-selector.

### Example

```
"OrganizationalUnit": {  
  "IsHiddenFromRequester": false,  
  "Definition": {  
    "Type": "OuSelection",  
    "Label": "Organizational Unit",  
    "DefaultValue": "OU=Demo Users,DC=DOMAIN",  
    "DisplayValue": "Demo Users"  
  }  
},
```

It creates a tree selection in the rich client and a drop down with all OUs in the web client.

## Enter additional LDAP attributes

**Create account within Active Directory** ✕

Create elements in the selected domain: 8man-demo.local.

Given name  ⚠ Surname  ⚠

Common name

Description  Automatically generated description for .

SAM account name

Organisational unit (OU) Sales ▾

**LDAP Attributes**

Attribute name filter 6


Name	Value
User principal name	.@8man-demo.local
Company	Example Holding
Street	Example Holding
Postal code	Example Marketing Solutions
	Example Services

Group memberships

Start external program

Credentials [8man-demo\sa-8man](#)

Please add a comment ⚠


[Close](#)
[Immediately ▶](#)

In the LDAP Attributes area, further entries can be made for these.

i If you use an LDAP attribute in the assignment, ARM dynamically loads the attribute from the AD when loading the template. Please see: [Load templates in ARM](#).

In this example the "**userprincipalname**" is preset via [CreationRule](#) and [editable](#). The input field "**company**" is implemented as [DropDownList](#). Depending on the choice of the company, the "**streetaddress**", "**postalcode**" and the location ("I") are set. The user cannot edit these values.

*Example*

"LdapAttributes": [

{

"Name": "sn", //Assignment, the following definition for the input of the attribute "sn"

"Definition": {

/\* [property](#) listing

.

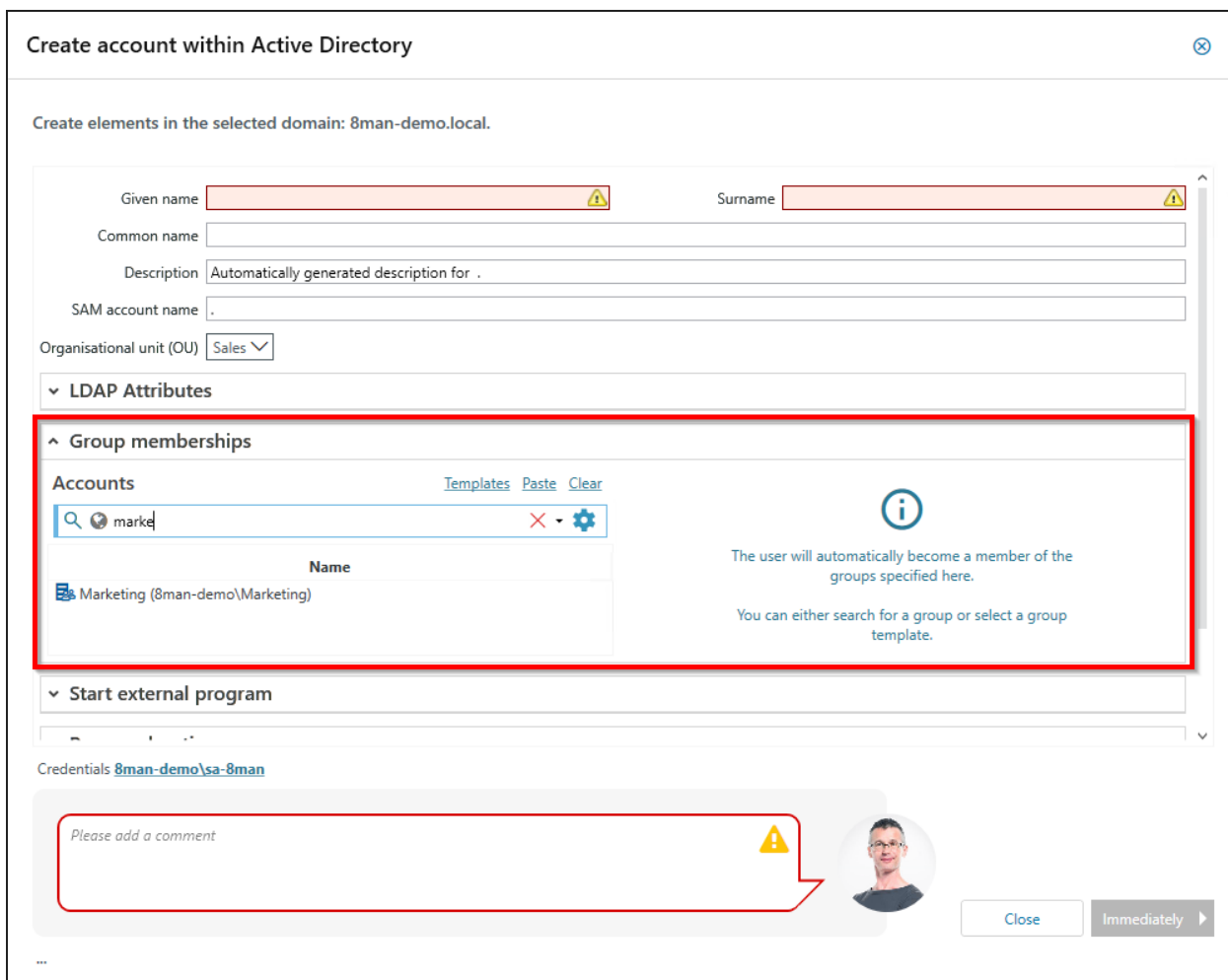
. \*/

}

}

]

## Assign group memberships



Create account within Active Directory

Create elements in the selected domain: 8man-demo.local.

Given name  Surname

Common name

Description Automatically generated description for .

SAM account name

Organisational unit (OU)

LDAP Attributes

Group memberships

Accounts  Templates Paste Clear

Name
Marketing (8man-demo\Marketing)


The user will automatically become a member of the groups specified here.

You can either search for a group or select a group template.

Start external program

Credentials 8man-demo\sa-8man

Please add a comment



Close Immediately

In the group memberships area ("**Memberof**"), you can define in which groups the new user should become a member. Add the SIDs of the desired groups to the Accounts list.

Example

```

"Memberof": {
  "IsHiddenFromRequester": false,
  "IsHidden": false,
  "Accounts": [
    "sid:///ad/S-1-5-21-1545227963-2195427628-2857504096-1440"
  ]
},

```

## Run an external program

**Create account within Active Directory** ✕

Create elements in the selected domain: 8man-demo.local.

Given name  Surname

Common name

Description  Automatically generated description for .

SAM account name

Organisational unit (OU)  Sales

▼ LDAP Attributes

▼ Group memberships

▲ Start external program

Start the program after the user creation

The external program with the name **Create a welcome package.** is located on ARM Server path `\\srv-8man\scripts\WelcomePackage.ps1`  
 Configured command line parameters are `{CommonName} {samaccountname} {DomainName}`


▼ Password options

▼ User activation

▼ Create an Exchange mailbox ⚠

Credentials [8man-demo\sa-8man](#)

Please add a comment ⚠



Close
Immediately ▶

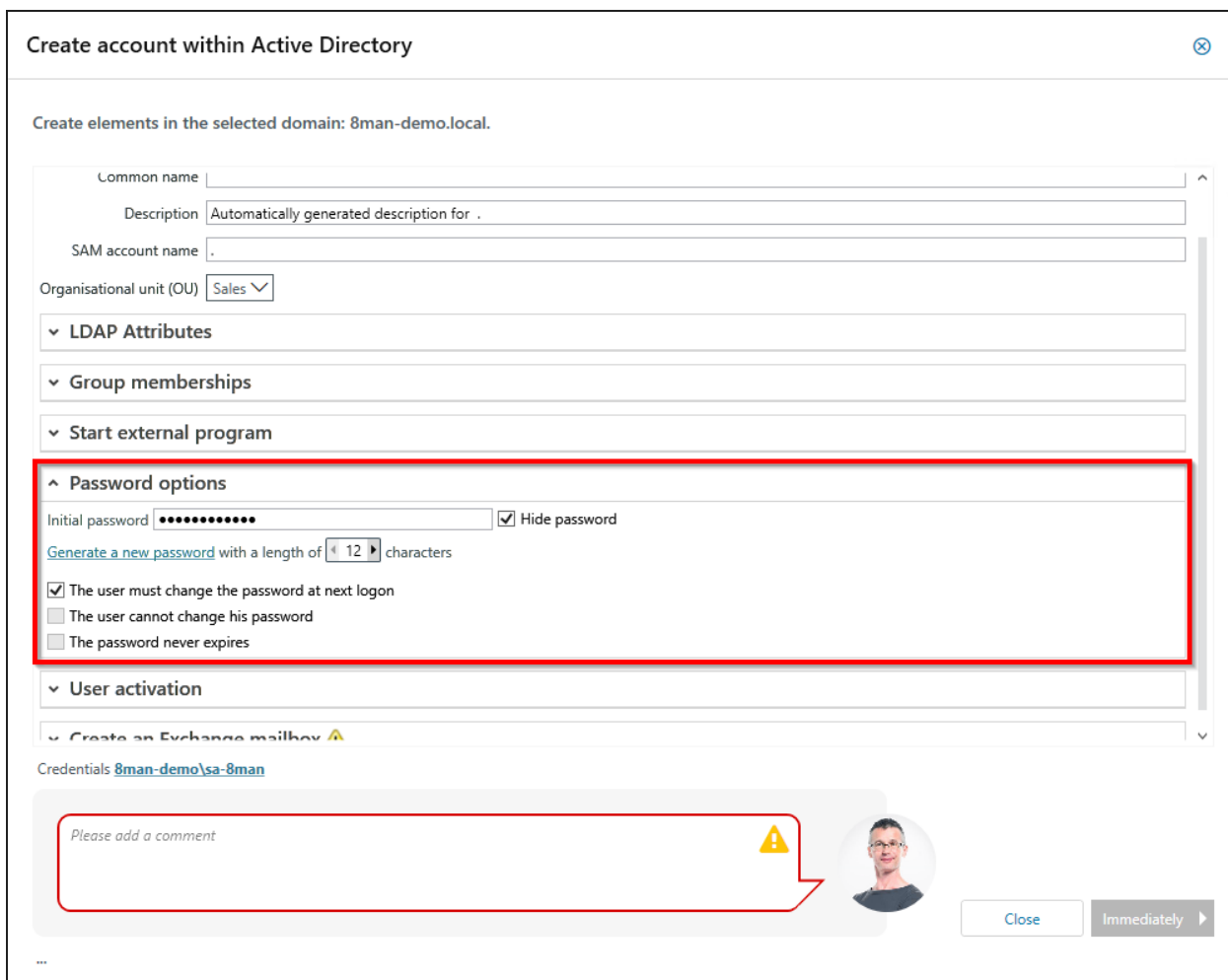
...

In the Execute external program ("**ScriptOptions**") section, you can specify that a program (script) is executed after creating the new user.

### Example

```
"ScriptOptions" : {  
  "IsHiddenFromRequester": false,  
  "IsScriptEnabledDefault": true,  
  "DisplayName": "Create a welcome package",  
  "Path": "\\srv-8man\\scripts\\WelcomePackage.ps1",  
  "CommandLineParameters": "{CommonName} {samaccountname} {DomainName}"  
},
```

## Enter password options



Create account within Active Directory

Create elements in the selected domain: 8man-demo.local.

Common name

Description Automatically generated description for .

SAM account name

Organisational unit (OU) Sales

LDAP Attributes

Group memberships

Start external program

**Password options**

Initial password   Hide password

[Generate a new password](#) with a length of 12 characters

The user must change the password at next logon

The user cannot change his password

The password never expires

User activation

Create an Exchange mailbox

Credentials 8man-demo\sa-8man

Please add a comment

In the password options section, you specify how the initial password ("InitialPassword") and the password options ("PasswordOptions") are preset.

Example

```
"InitialPassword": {  
  "MinLength": 12,  
  "IsComplex": true,  
  "IsMasked": false,  
  "DefaultValue": "P@ssword1234",  
  "Constraints": {  
    "ValidationRule": "[^\s]*",  
    "ValidationInformation":  
      "At least 12 characters, uppercase and lowercase letters, at least one digit or a special  
      character. No spaces."  
  }  
},  
"PasswordOptions": {  
  "MustBeChangedAtNextLogonDefault": true,  
  "CannotBeChangedByUserDefault": false,  
  "NeverExpiresDefault": false  
},
```



## Activation options


### Create account within Active Directory ⊗

Create elements in the selected domain: 8man-demo.local.

Given name	<input type="text"/>	Surname	<input type="text"/>
Common name	<input type="text"/>		
Description	Automatically generated description for .		
SAM account name	<input type="text"/>		
Organisational unit (OU)	Sales		
LDAP Attributes	<input type="text"/>		
Group memberships	<input type="text"/>		
Start external program	<input type="text"/>		
Password options	<input type="text"/>		
<b>User activation</b>	<input type="text"/>		
<input checked="" type="radio"/> Activate immediately	<input type="radio"/> Activate on 7/7/2019 12:00 AM	<input type="radio"/> Do not activate	
<input type="checkbox"/> Account expires on 9/5/2019 12:00 AM			
Create an Exchange mailbox	<input type="text"/>		

Credentials 8man-demo\sa-8man

Please add a comment ⚠



Close Immediately ▶

In the Activation section, you determine whether the activation options ("**ActivationOptions**") are hidden.

### Example

```
"ActivationOptions": {
```

```
  "IsHidden": false,
```

```
  "IsHiddenFromRequester": true
```

```
  "AccountActivationState": "Immediately" // possible values: Immediately, Later, Inactive
```

```
},
```

## Create an Exchange mailbox


**Create account within Active Directory** ✕

Create elements in the selected domain: 8man-demo.local.

Mailbox type	Regular	▼
E-mail addresses	SMTP:;@8man-demo.local smtp:;@8man-demo.local	⚠️ 🌐
Mailbox Database	Mailbox Database1	▼
Address book policy	display name for default policy	▼
Enable archive database	<input type="checkbox"/>	
Archive database	Mailbox archive database	▼
ActiveSync	<input checked="" type="checkbox"/>	
ActiveSync policy	Default	▼
Outlook Web App (OWA)	<input checked="" type="checkbox"/>	
Outlook Web App (OWA) policy	Default	▼
IMAP	<input checked="" type="checkbox"/>	
POP3	<input checked="" type="checkbox"/>	
MAPI	<input checked="" type="checkbox"/>	
Credentials	<a href="#">8man-demo\sa-8man</a>	↖️

Credentials [8man-demo\sa-8man](#)

Please add a comment ⚠️


Close Immediately ▶

...

In the section "Modules", you email-enable the user. You can define Exchange mailbox settings in the same step. The entire section is optional.

i The credentials (arrow) can not be influenced by the template. You make this setting in the [Exchange change configuration](#).

### Example

```

"Modules" : [
{
  "Name" : "Exchange.Create.MailBox",
  "Displaytext" : "Create an Exchange mailbox.",
  "Description" : "Description text",
  "CredentialType" : "Windows",
  "Fields" : [

```

```
{
  "Name": "createmailbox",
  "Definition": {
    "Type": "Checkbox",
    "DefaultValue": true,
    "Label": "Create mailbox"
  }
},
{
  "Name": "emailaddresses",
  "Definition": {
    "Type": "TextArea",
    "Label": "Email addresses",
    "IsRequired": true,
    "IsEnabled": true,
    "Constraints": {
      "MaxLength": 500,
      "ValidationRule": "^((([a-z][a-z0-9]+)?([A-Z][A-Z0-9]+)?(\\w+([-+.']\\w+)*@\\w+([-.]\\w+)*\\.\\w+([-.]\\w+)*(\\r\\n)?\\n?)+)*$",
      "ValidationInformation": "Does not match the Email format!",
      "CreationRule" : "SMTP:<toLowerCase>({samaccountname})@<toLowerCase>
({fqdn})r\\nsmtp:<toLowerCase>(<firstLetter>({givenname})).<toLowerCase>({sn})@<toLowerCase>
({fqdn})"
    }
  }
},
{
  "Name": "MailboxDatabase",
  "Definition": {
    "Type": "DropDownList",
    "DefaultValue": "Mailbox Database1",
    "Label": "Mailbox Database",
```

```
"IsRequired": true,
"Items": [
  {
    "Value": "Mailbox Database1",
    "DisplayValue": "Mailbox Database1"
  },
  {
    "Value": "Mailbox Database2",
    "DisplayValue": "Mailbox Database2"
  }
]
}
},
{
  "Name": "ActivateArchive",
  "Definition": {
    "Type": "Checkbox",
    "DefaultValue": "false",
    "Label": "Archive database"
  }
},
{
  "Name": "ArchiveDatabase",
  "Definition": {
    "Type": "DropDownList",
    "DefaultValue": "Mailbox Database1",
    "Label": "Archiv Datenbank",
    "IsRequired": true,
    "Items": [
      {
        "Value": "Mailbox Database1",
```

```
        "DisplayValue": "Mailbox Database1"
    },
    {
        "Value": "Mailbox Database2",
        "DisplayValue": "Mailbox Database2"
    }
]
}
},
{
    "Name": "ActivateActiveSync",
    "Definition": {
        "Type": "Checkbox",
        "DefaultValue": "true",
        "Label": "ActiveSync"
    }
},
{
    "Name": "ActivateActiveSyncPolicy",
    "Definition": {
        "Type": "DropDownList",
        "DefaultValue": "Default",
        "Label": "ActiveSync policy",
        "IsRequired": true,
        "Items": [
            {
                "Value": "Default",
                "DisplayValue": "Default"
            },
            {
                "Value": "Other",
```

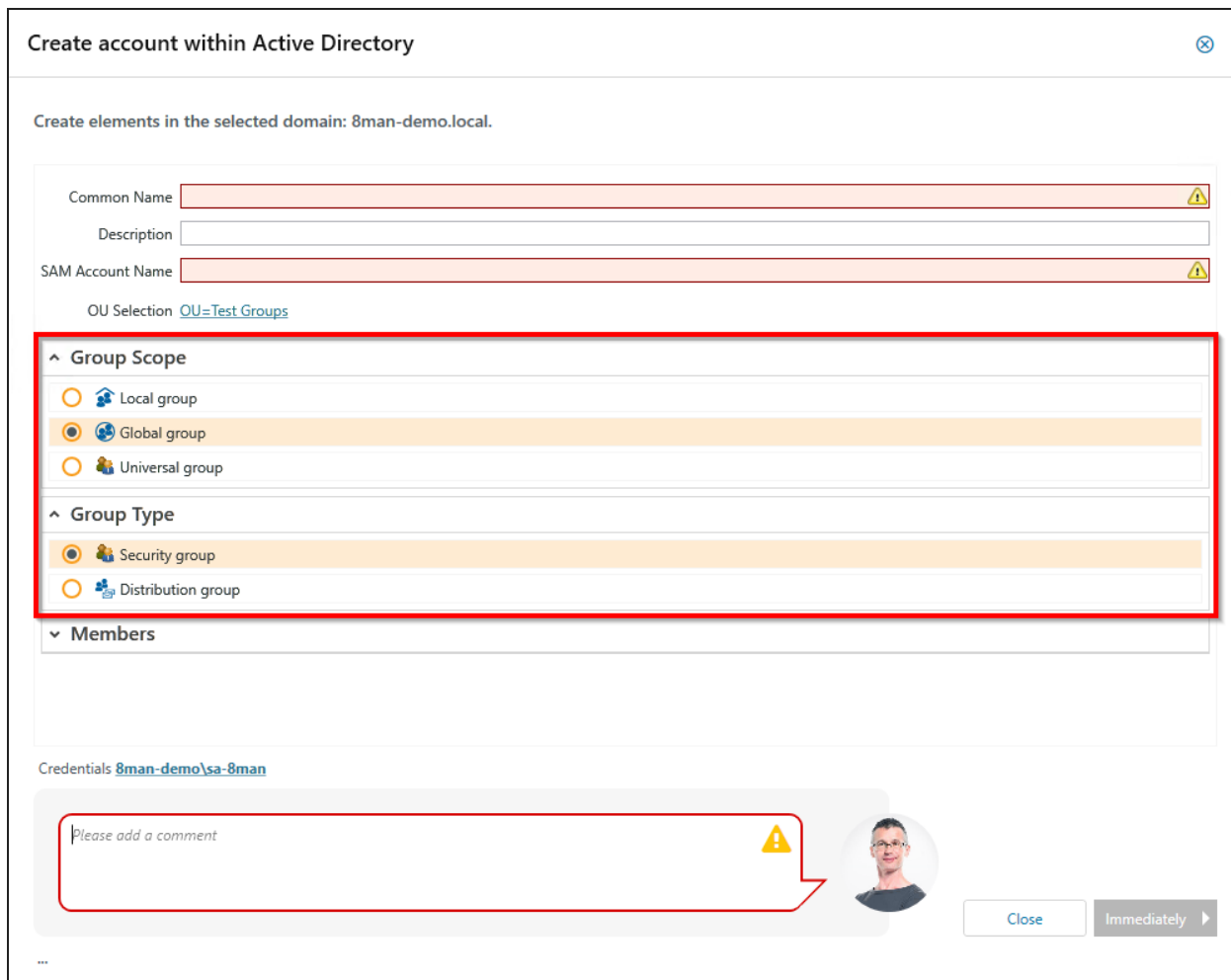
```
        "DisplayValue": "Other"
      }
    ]
  }
},
{
  "Name": "ActivateOwa",
  "Definition": {
    "Type": "Checkbox",
    "DefaultValue": "true",
    "Label": "Outlook Web App (OWA)"
  }
},
{
  "Name": "ActivateOwaPolicy",
  "Definition": {
    "Type": "DropDownList",
    "DefaultValue": "Default",
    "Label": "Outlook Web App (OWA) policy",
    "IsRequired": true,
    "Items": [
      {
        "Value": "Default",
        "DisplayValue": "Default"
      },
      {
        "Value": "Other",
        "DisplayValue": "other"
      }
    ]
  }
}
```

```
},  
{  
  "Name": "ActivateImap",  
  "Definition": {  
    "Type": "Checkbox",  
    "DefaultValue": "true",  
    "Label": "IMAP"  
  }  
},  
{  
  "Name": "ActivatePop",  
  "Definition": {  
    "Type": "Checkbox",  
    "DefaultValue": "true",  
    "Label": "POP3"  
  }  
},  
{  
  "Name": "ActivateMapi",  
  "Definition": {  
    "Type": "Checkbox",  
    "DefaultValue": "true",  
    "Label": "MAPI"  
  }  
}  
]  
}
```

## Customize templates for new groups

The template for a new group contains many items that are also contained in the template for a new user. In the following sections, you will find only the different adjustments in a template for a new group.

### Preset group options (group type/scope)



Create account within Active Directory ⊗

Create elements in the selected domain: 8man-demo.local.

Common Name  ⚠

Description

SAM Account Name  ⚠

OU Selection [OU=Test Groups](#)

^ Group Scope

- Local group
- Global group
- Universal group


^ Group Type

- Security group
- Distribution group

▼ Members

Credentials [8man-demo\sa-8man](#)

Please add a comment  ⚠



[Close](#) [Immediately ▶](#)

Specify which options are already preselected.

*Example*

**"GroupTypeOptions": {**

*/\* Determine the group scope radio button preset.*

*Possible values:*

*- Global (Default)*



- Local

- Universal (must be used for email enabling) \*/

**"GroupArea" : "Universal",**

*/\* Determine the group type radio button preset.*

*Possible values:*

- Security (Default)

- Distribution (must be used for email enabling) \*/

**"GroupType" : "Distribution",**

*// Hide the area GroupTypeOptions to prevent user changes.*

**"IsHidden": false,**

**"IsHiddenFromRequester": false**

**},**

## Preset group members

**Create account within Active Directory** ⊗

Create elements in the selected domain: 8man-demo.local.

Common Name  ⚠

Description

SAM Account Name  ⚠

OU Selection [OU=Test Groups](#)


▼ Group Scope


▼ Group Type

^ **Members**

**Accounts** [Paste](#) [Clear](#)

✕ ⚙

Name
 Emily Employee (8man-demo\Emily Employee)




The accounts specified here will automatically become members of the new group.

You can search for users and groups.

Credentials [8man-demo\sa-8man](#)

Please add a comment ⚠


[Close](#)
[Immediately](#) ▶

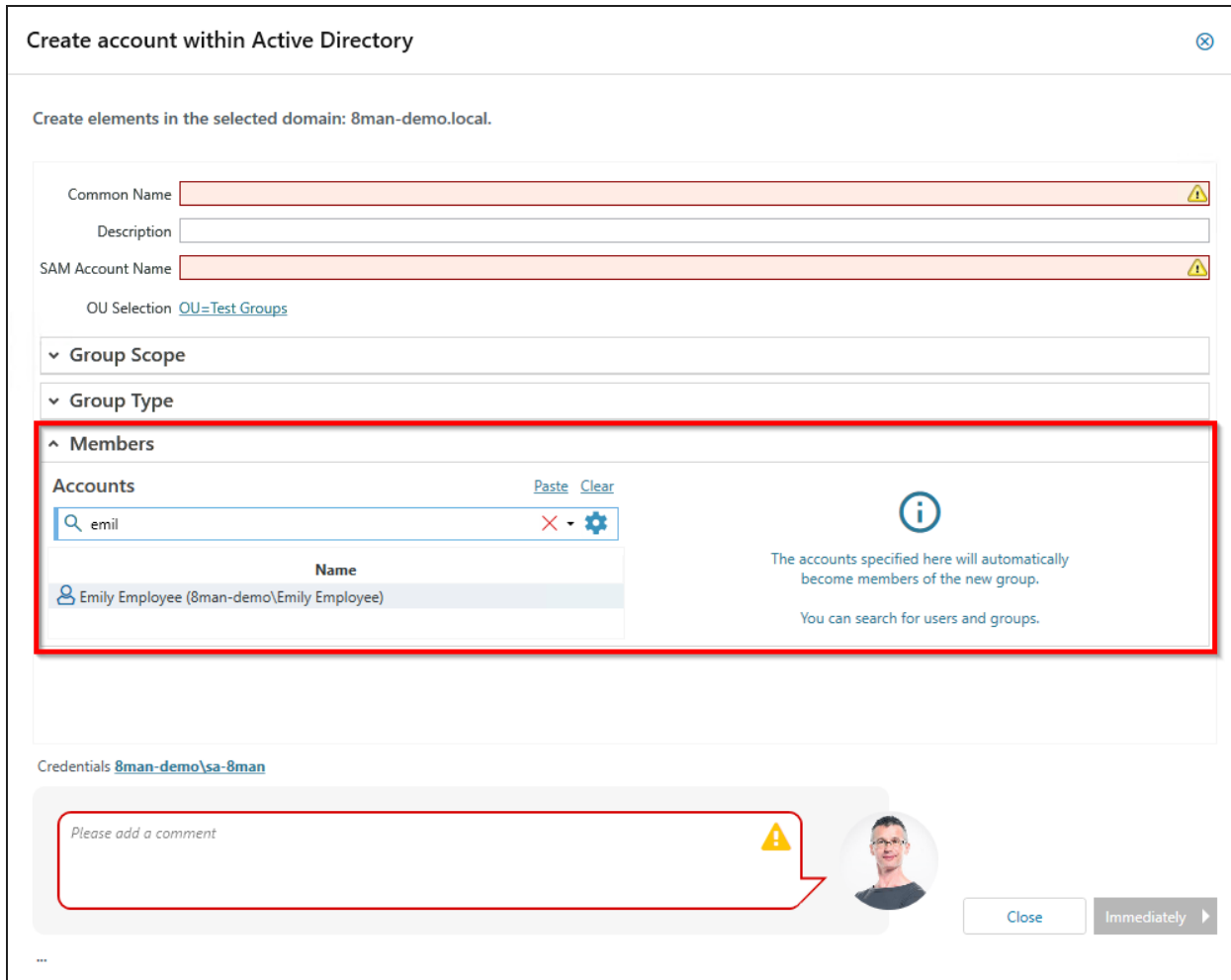
...

In the **"members"** section, define which members are already preset.

### Example


```
"Members" : {
  "Accounts" :[
    "sid:///ad/S-1-5-21-2680840348-2237289205-2993809228-13534"
  ]
}
```

## Enable email (create distribution group) in Exchange




Create account within Active Directory

Create elements in the selected domain: 8man-demo.local.

Common Name  

Description



SAM Account Name  


OU Selection [OU=Test Groups](#)

Group Scope

Group Type


Members


Accounts  [Paste](#) [Clear](#)  

Name
 Emily Employee (8man-demo\Emily Employee)

The accounts specified here will automatically become members of the new group.  
You can search for users and groups.


Credentials [8man-demo\sa-8man](#)

Please add a comment  



[Close](#) [Immediately](#)

In the optional "**Modules**" section, you provide Exchange options. With this template, the new group can be email activated and become an Exchange distribution group.

 For a successful distribution role in Exchange, the group scope must be universal.

The credentials (arrow) can not be influenced by the template. You make this setting in the [Exchange change configuration](#).

### Example

"Modules" : [

{

// (required) Name of the module as key to depending processes. Do not change.

"Name" : "Exchange.Create.DistributionGroup",

// (required) Short description of the module. Used as section headline.

"Displaytext" : "Create Distribution Group in Exchange",

// (optional) Long description of the module. Displayed within the section.

"Description" : "Long description for demo.",

/\* (optional) Determine the Credential Type.

Possible values:

- UsernamePassword (default)

- Windows \*/

"CredentialType" : "Windows",

// (required) required input values (all fields)

"Fields" : [

{

  "Name": "createdistributiongroup",

  "Definition": {

    "Type": "Checkbox",

    "DefaultValue": true,

    "Label": "Create distribution group ",

    "IsRequired": true

  }

},

{

  "Name": "emailaddresses",

  "Definition": {

    "Type": "TextArea",

    "Label": "E-Mail addresses ",

    "IsRequired": true,

    "IsEnabled": true,

    "Constraints": {

      "MaxLength": 500,

      "ValidationRule": "^((((([a-z][a-z0-9]+)?([A-Z][A-Z0-9]+)?(\\w+([-+.'\\w+)\*@\\w+([-.]\\w+)\*\\.\\w+([-.]\\w+)\*(\\r\\n)?\\n?)+)\*\$)",

      "CreationRule" : "SMTP:<toLowerCase>({samaccountname})@<toLowerCase>([fqdn])\r\nsmtp:<toLowerCase>({samaccountname})@mydomain.com"

  }

```
    }  
  },  
{  
  "Name": "RequireSenderAuthenticationEnabled",  
  "Definition": {  
    "Type": "Checkbox",  
    "Label": "Only authenticated senders ",  
    "DefaultValue": true,  
    "IsRequired": true  
  }  
}  
]  
}  
]
```

## Customize templates for new contacts

With customized templates for contacts, you can create contacts with ARM.

Templates for new contacts record the following three values:

- OU (organizational unit)
- Name
- Email address

 You can only use templates for contacts in the Rich Client (not the Web client).

To display all information from contacts in ARM, you must configure the AD scan and the Exchange-Scan accordingly.

*Example*

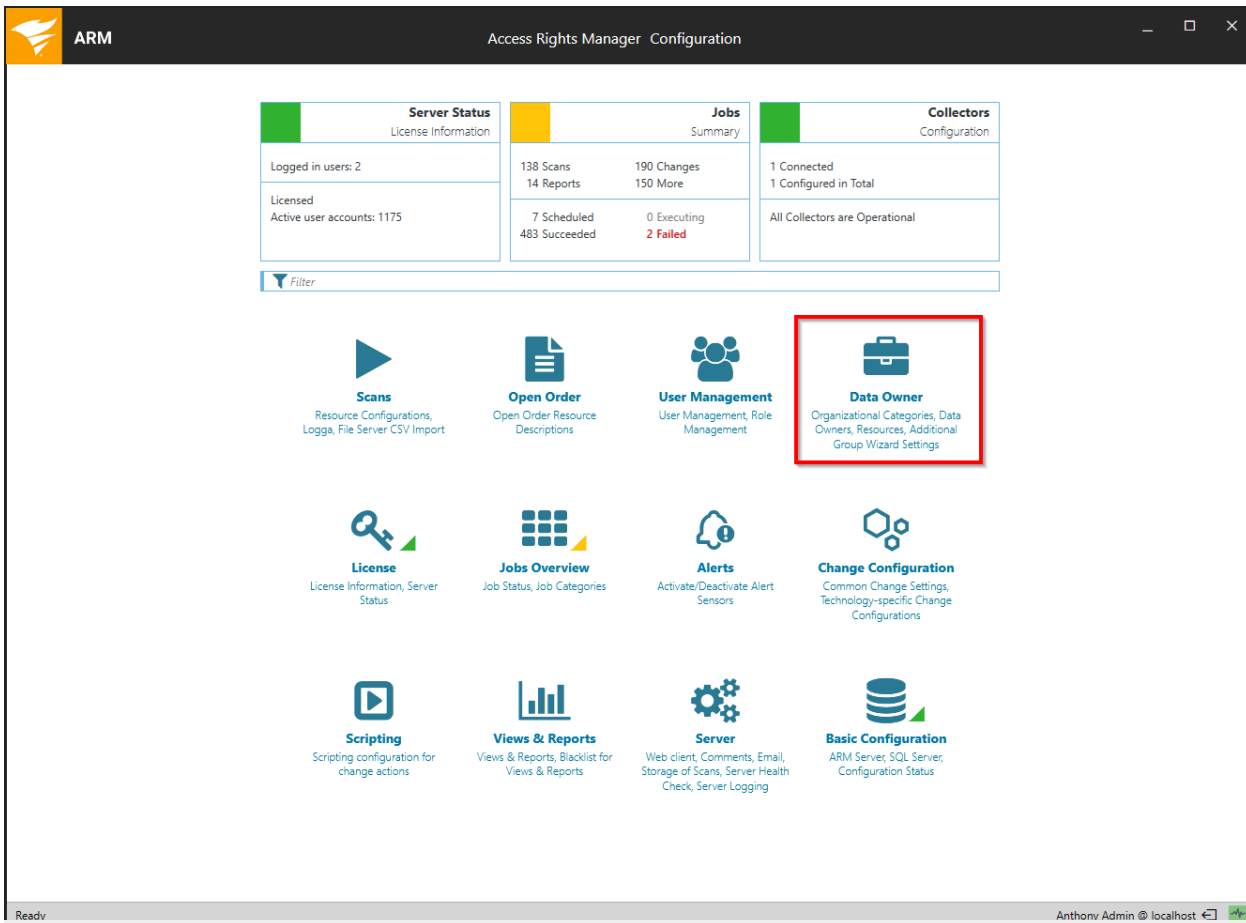
```
[[  
  "TemplateType": "CreateMailContact",  
  "Version": 1,  
  "Id": "2adee521-9423-464e-a52b-0d20a54ec4f6",  
  "DisplayName": "Create contact",
```

```
"Description": "Creates a contact with Exchange",
"FullQualifiedDomainName": "8man-demo.local",
"OrganizationalUnit": {
  "Definition": {
    "Type": "DropDownList",
    "Items": [
      {
        "Value": "OU=Sales,OU=Berlin,DC=8man-demo,DC=local",
        "DisplayValue": "Sales"
      },
      {
        "Value": "OU=Marketing,OU=Berlin,DC=8man-demo,DC=local",
        "DisplayValue": "Marketing"
      }
    ],
    "DefaultValue": "OU=Sales,OU=Berlin,DC=8man-demo,DC=local",
    "Label": "Organizational unit (OU)"
  }
},
"LdapAttributes": [
  {
    "Name": "name",
    "Definition": {
      "Type": "TextField",
      "Label": "Name",
      "IsRequired": true,
      "IsEnabled": true,
      "IsHidden": false,
      "Constraints": {
        "MaxLength": 50
      }
    }
  }
]
```

```
    }  
  },  
  {  
    "Name": "externalemailaddress",  
    "Definition": {  
      "Type": "TextField",  
      "Label": "External email address",  
      "IsRequired": true,  
      "IsEnabled": true,  
      "Constraints": {  
        "MaxLength": 200,  
        "ValidationRule": "[A-Z0-9a-z._%+~]+@[A-Za-z0-9.-]+\\.[A-Za-z]{2,6}"  
      }  
    }  
  }  
]  
}  
]
```

## Make templates for users/groups/contacts available in the Web client

Templates for users/groups/contacts are available for use in the rich client as soon as they have been successfully loaded (see [Load templates](#)). To allow a "requester" in the self service portal GrantMA to use a template, the template must be assigned to an organizational category as a resource.



In the ARM configuration application, select Data Owner.



The screenshot shows the 'Data Owner configuration' for the 'Marketing' category in the ARM Configuration tool. The interface includes a left sidebar for 'Organizational Categories' (Finance, Human Resources, IT Service Europe, Marketing, Sales), a top navigation bar, and several main sections: 'Marketing' (with 'Additional Group Wizard Settings' and 'Assigned workflow'), 'Data Owners' (table with 2 entries), 'Requesters' (table with 2 entries), and 'Resources' (table with 6 entries). A 'Resource selection' panel is open on the right, showing a search bar and a list of templates. Three red annotations highlight the process: 1. A red circle around the 'Resource selection' panel title. 2. A red arrow pointing from a template 'Marketing - Create new group' in the list to the 'Resources' table. 3. A red circle around the 'Marketing - Create new group' template in the list.

1. [Successfully loaded](#) custom templates are automatically displayed in the resource selection.
2. Drag and drop a template into the resources area.
3. The template is automatically set to "Resource can be requested".

## Open order templates

Open Order templates differ from the templates for users / groups / contacts by the following characteristics:

- OpenOrder templates can only be used in the GrantMA / web client.
- Open Order Templates can be used for a wide range of orders. Therefore, there are no specialized input options or modules, but only freely definable containers, which can be interleaved as often as required.
- Open Order templates are assigned to Open Order resources via an XML configuration file. After uploading the XML configuration, only the resources are displayed in the data owner configuration, not the corresponding templates.

## Structure of an Open Order template

The required information in the [header of the template](#) is the same as for users / groups / contacts.

The structure of the input form follows the following scheme:

```
"Form": {
  "Type": "Container",
  "Label": "Labeling",
  "Templates": [
    {
      "Key": "Value1",
      "Value": {
        "Type": input method
      }
    },
    { "Key": "^Value2",
      "Value": {
        "Type": input method
      }
    }
  ]
}
```

As an input method, you can use containers to create nesting.

With `CollapsibleContainer`, you create a container that can be collapsed and expanded. Use the `IsCollapsed` property to set the default.

*Example for nested containers:*

```
"Form": {
  "Type": "Container",
  "Label": "Root container",
  "Templates": [
    {
      "Key": "nested_container",
      "Value": {
        "Type": "CollapsibleContainer",
        "Label": "Nested container",
        "IsCollapsed": true,
      }
    }
  ]
}
```

```
"Templates": [  
  {  
    "Key": "Collapsible_grandchild_container",  
    "Value": {  
      "Type": "Container",  
      "Label": "Additional container",  
      "Templates": [  
        {  
          "Key": "Container3",  
          "Value": {  
            "Type": "CollapsibleContainer",  
            "Label": "And one more to fold",  
            "Templates": [  
              { //etc...            ]  
          }  
        }  
      ]  
    }  
  }  
]
```

## Create an input option

The same input options are available for Open Order Templates as for templates for users, groups, and contacts. You can also use the same constraints and creation rules.

There are additional possibilities for inputs, descriptions, visibility control and validity checks, which can only be used in Open Order templates in the Web client (not in the Rich Client).

An overview of available input options can be found [here](#).

## Specific Open Order input options

### AccountSearchTextField

AccountSearchTextField is an input option for searching for a user or group. A text field with an additional search button is displayed. If the button is pressed a search dialog appears. The search result can be further processed in the form.

**AccountSearchTextField can only be used in Open Order Templates.**

*Properties*

**Type**

**"Type": "AccountSearchTextField"****Label**

The annotation of the search field displayed in the form.

**LookupTableId**

Identifies the lookup table from which the LDAP attributes from the search can be used in the template.

**AttributesToLoad**

A list of LDAP attributes to load, for example ["sn", "cn"].

*Example*

```
// Define search input
```

```
{  
  "Key": "Requester",  
  "Value": {  
    "Type": "AccountSearchTextField",  
    "Label": "Request for",  
    "LookupTableId": "RequesterSearchResult",  
    "AttributesToLoad": [  
      "sn",  
      "givenname"  
    ]  
  }  
},
```

```
// Use search results
```

```
{  
  "Key": "given name",  
  "Value": {  
    "Type": "TextField",  
    "Label": "given name",
```

```
"IsEnabled": "false",
"Constraints": {
  "CreationRule": "<lookup>(RequesterSearchResult,givename)"
}
},
{
  "Key": "Surname",
  "Value": {
    "Type": "TextField",
    "Label": "Surname",
    "IsEnabled": "false",
    "Constraints": {
      "CreationRule": "<lookup>(RequesterSearchResult,sn)"
    }
  }
}
```

## Radio Buttons

Radio is a group of radio buttons. You can only use radio buttons in Open Order Templates.

### *Properties*

#### **Type**

For a group of radio buttons is the "**Type**": "**Radio**".

#### **RadioGroupId**

All radio buttons with the same id are grouped into one group. Within a group, only one radio button can be selected at a time.

#### **Label**

The value displayed in the form.

## Value

The actual value that is stored.

## IsChecked

Sets the initial selected radio button of a group.

### Example

```
"Key": "ActionRadio1",  
"Value": {  
  "Type": "Radio",  
  "RadioGroupId": "Group1",  
  "IsChecked": "true",  
  "Label": "Displayed value 1",  
  "Value": "Real value 1"  
}  
"Key": "  
ActionRadio2",  
"Value": {  
  "Type": "Radio",  
  "RadioGroupId": "Group1",  
  "Label": "Displayed value 2",  
  "Value": "Real value 2"  
}
```

## Include open order templates in the ARM GrantMA

To create Open Order Templates, follow these steps:

1. [Enter the template's call into the XML Resource Configuration.](#)
2. [Upload an XML resource configuration to the Data Owner configuration.](#)
3. [Set the Open Order resource to requestable.](#)

## Enter the template's call into the XML resource configuration

Assign the [unique ID](#) of the OpenOrderTemplate to one or more resources.

For more information on the structure of the XML resource configuration, see the Open Order manual.

### Example

```
<?xml version="1.0" encoding="utf-8"?>
<resourceImport Version="3">
  <technology Id="D54C16F2-42C1-477A-BD20-3285158F68D3" Name="Hardware" IconId="2"
  Color="#0000be">
    <definitions>
      <permissionSets>
        <permissionSet PermissionSetId="1" Description="['en-US:Buy','de-DE:Kaufen']" />
        <permissionSet PermissionSetId="2" Description="['en-US:Lease','de-DE:Leasen']" />
        <permissionSet PermissionSetId="3" Description="['en-US:Rent','de-DE:Mieten']" />
      </permissionSets>
      <types>
        <type Id="1" Description="['en-US:Hardware','de-DE:Hardware']" IconId="Container"
        PermissionSetIds="[]" />
        <type Id="3" Description="['en-US:Desktop','de-DE:Desktop']" IconId="Computer"
        PermissionSetIds="[1,2,3]" />
      </types>
    </definitions>
    <data>
      <root Id="6CE9B526-9FFD-46A5-9ED0-36FB4E1303B5" Name="Computer" Typeld="1"
      Merge="no">
        <resource Name="Desktop PCs" Typeld="3" Description="['en-US:Stationary PC','de-
        DE:Stationäre Arbeitsplatz-PCs']">
          <resource Name="Desktop-PC Simple" Typeld="3" />
          <resource Name="Desktop-PC Standard" Typeld="3" />
          <resource Name="Desktop-PC Custom" Typeld="3" TemplateID="E3865726-6FDF-489E-
          A7D5-4ABBA5B2BF83" />
        </resource>
      </root>
```

&lt;/data&gt;

&lt;/technology&gt;

&lt;/resourceImport&gt;

## Upload an XML resource configuration to the Data Owner configuration

The screenshot shows the 'Access Rights Manager Configuration' window. At the top, there are three summary cards: 'Server Status' (License Information), 'Jobs' (Summary), and 'Collectors' (Configuration). Below these is a 'Filter' dropdown. The main area contains a grid of 12 functional buttons, each with an icon and a description. The 'Open Order' button, which features a document icon and the text 'Open Order Resource Descriptions', is highlighted with a red rectangular border. Other buttons include Scans, User Management, Data Owner, License, Jobs Overview, Alerts, Change Configuration, Scripting, Views & Reports, Server, and Basic Configuration.

Server Status License Information	Jobs Summary	Collectors Configuration
Logged in users: 2	138 Scans 14 Reports	190 Changes 150 More
Licensed Active user accounts: 1175	7 Scheduled 483 Succeeded	0 Executing 2 Failed

Filter

**Open Order**  
Open Order Resource Descriptions

In the ARM configuration, click "Open Order".



The screenshot shows the 'Open Order Configuration' page in the SolarWinds Access Rights Manager (ARM) Configuration tool. The page is divided into two main sections: 'Open Order Resource Descriptions' and 'Quick info'.

**Open Order Resource Descriptions:**

- Import File:** A section with the instruction 'Select a valid XML file which contains open order resource descriptions for import.' Below this is a file selection area with an 'Upload' button highlighted by a red box. An orange arrow points down from the 'Upload' button to the 'XML schema' section.
- XML schema:** A section with the instruction 'The XML schema will be used to verify that the import file is valid. It also serves as documentation for creating an import file. You can download the schema [here](#)'. An orange arrow points down from this section to the 'Hardware' and 'Software' sections.
- Hardware:** A section with a blue icon and the text 'Hardware'.
- Software:** A section with a blue icon and the text 'Software'.

**Quick info:**

- Open Order Configuration:** A section with the text 'Here you can manage external resource descriptions of several Open Order technologies. Use the Open Order technologies in the Data Owner configuration in order to assign your requestable resources.'
- Functions:**
  - Import Open Order resource descriptions from XML file
  - Remove loaded Open Order resource descriptions

The status bar at the bottom of the window shows 'Ready' on the left and 'Anthony Admin @ localhost' on the right.

Click "Upload" to import the XML Resource Configuration. After successful import, the resources are available in the Data Owner configuration and can be assigned to organizational categories.

## Set the open order resource to requestable

ARM Access Rights Manager Configuration

Server Status License Information	Jobs Summary	Collectors Configuration
Logged in users: 2	138 Scans 14 Reports	1 Connected 1 Configured in Total
Licensed Active user accounts: 1175	190 Changes 150 More	All Collectors are Operational
	7 Scheduled 483 Succeeded	
	0 Executing 2 Failed	

Filter

- Scans**  
Resource Configurations, Logga, File Server CSV Import
- Open Order**  
Open Order Resource Descriptions
- User Management**  
User Management, Role Management
- Data Owner**  
Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**  
License Information, Server Status
- Jobs Overview**  
Job Status, Job Categories
- Alerts**  
Activate/Deactivate Alert Sensors
- Change Configuration**  
Common Change Settings, Technology-specific Change Configurations
- Scripting**  
Scripting configuration for change actions
- Views & Reports**  
Views & Reports, Blacklist for Views & Reports
- Server**  
Web client, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic Configuration**  
ARM Server, SQL Server, Configuration Status

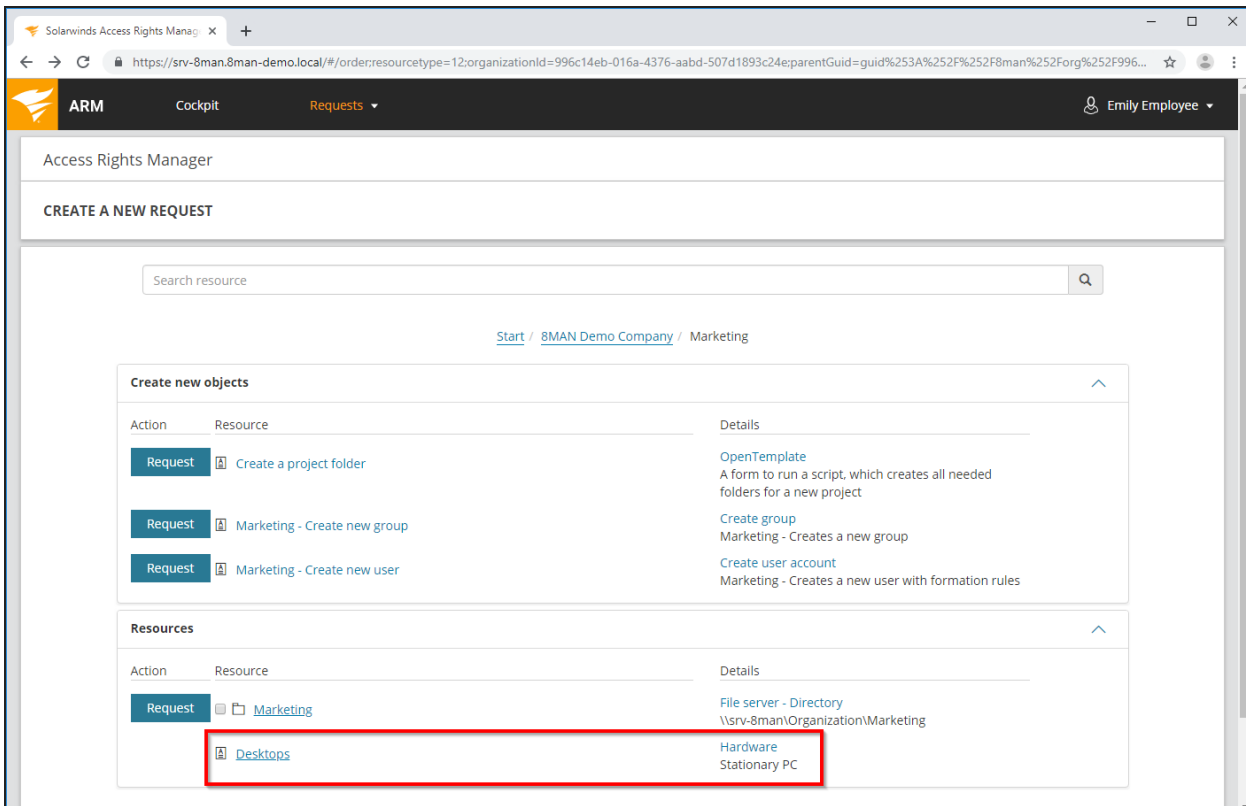
Ready Anthony Admin @ localhost

In the ARM configuration, click "Data Owner".

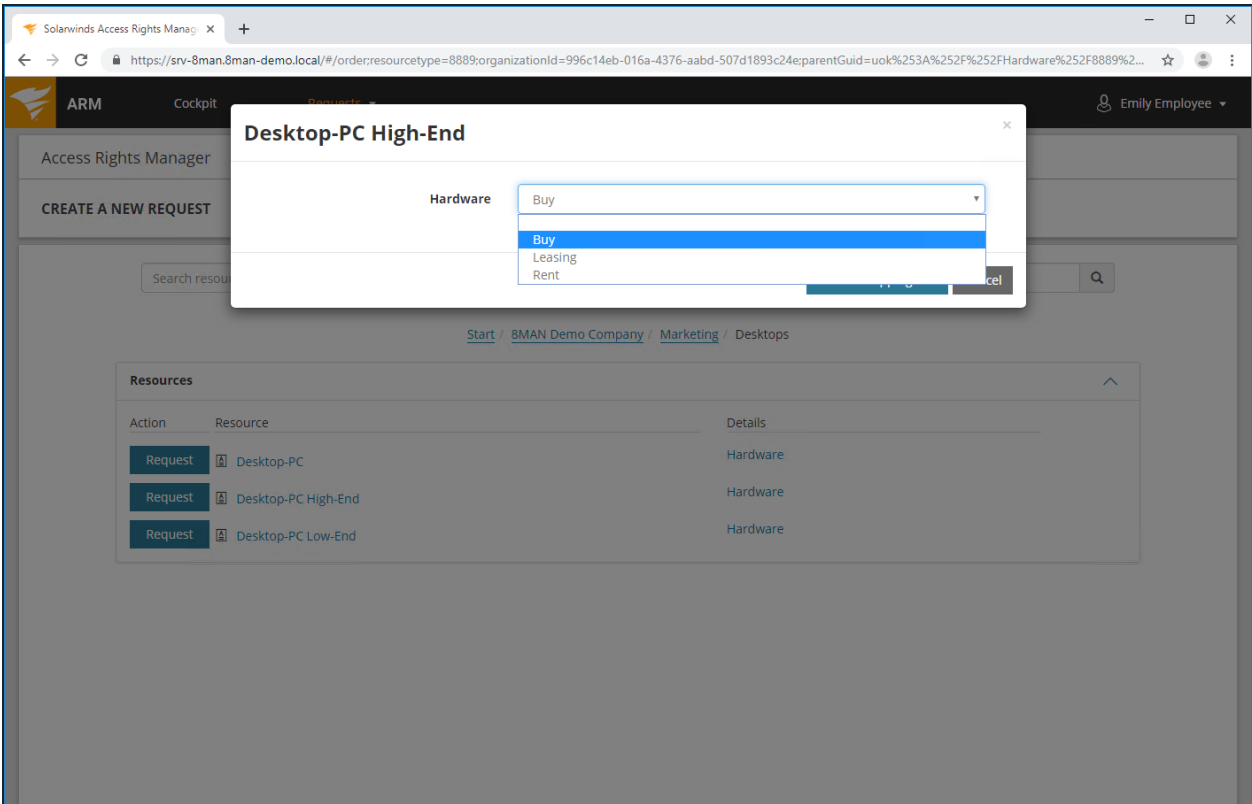
The screenshot shows the 'Data Owner configuration' for the 'Marketing' category in the SolarWinds Access Rights Manager. The interface is divided into several sections:

- Organizational Categories:** A sidebar on the left showing a tree view of categories: 8MAN Demo Company, Finance, Human Resources, IT Service Europe, Marketing (selected), and Sales.
- Data Owners:** A table listing users with roles. Two entries are visible: David DO Marketing (Data Owner) and David DO Manager (Data Owner).
- Requesters:** A table listing users with roles. Two entries are visible: Emily Employ... (Requester) and Henry HR (Requester).
- Resources:** A table listing resources. The 'Desktops' resource under the 'Hardware' category is highlighted with a red box and a shopping cart icon, indicating it is requestable. A red arrow points from the 'Desktops' resource in the 'Resource selection' pane to this icon.
- User & Group selection:** A section for selecting users and groups, currently showing Dexter Ward.
- Resource selection:** A pane on the right showing a tree view of resources: Active Directory, File server, Exchange, Template, Hardware (with 'Desktops' selected), Software, SharePoint Online, SharePoint, Azure AD, and OneDrive.

1. Add the desired resource by drag & drop.
2. The resource is automatically marked as requestable.



The requester can find the resource available via Open Order.



Example for a template based Open Order request.