ADMINISTRATOR GUIDE

Access Rights Manager

Version 2019.4

solarwinds

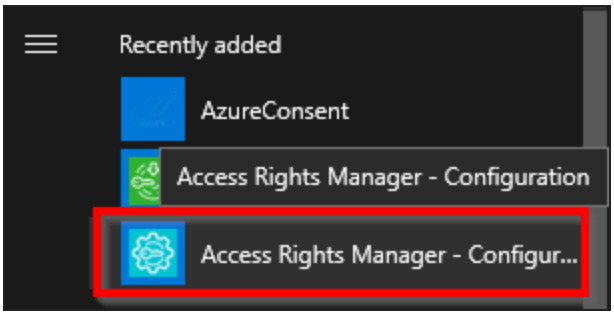
Last Updated: Friday, March 6, 2020

Table of Contents

Configuration

This section provides detailed information on configuring ARM.

Start the configuration application

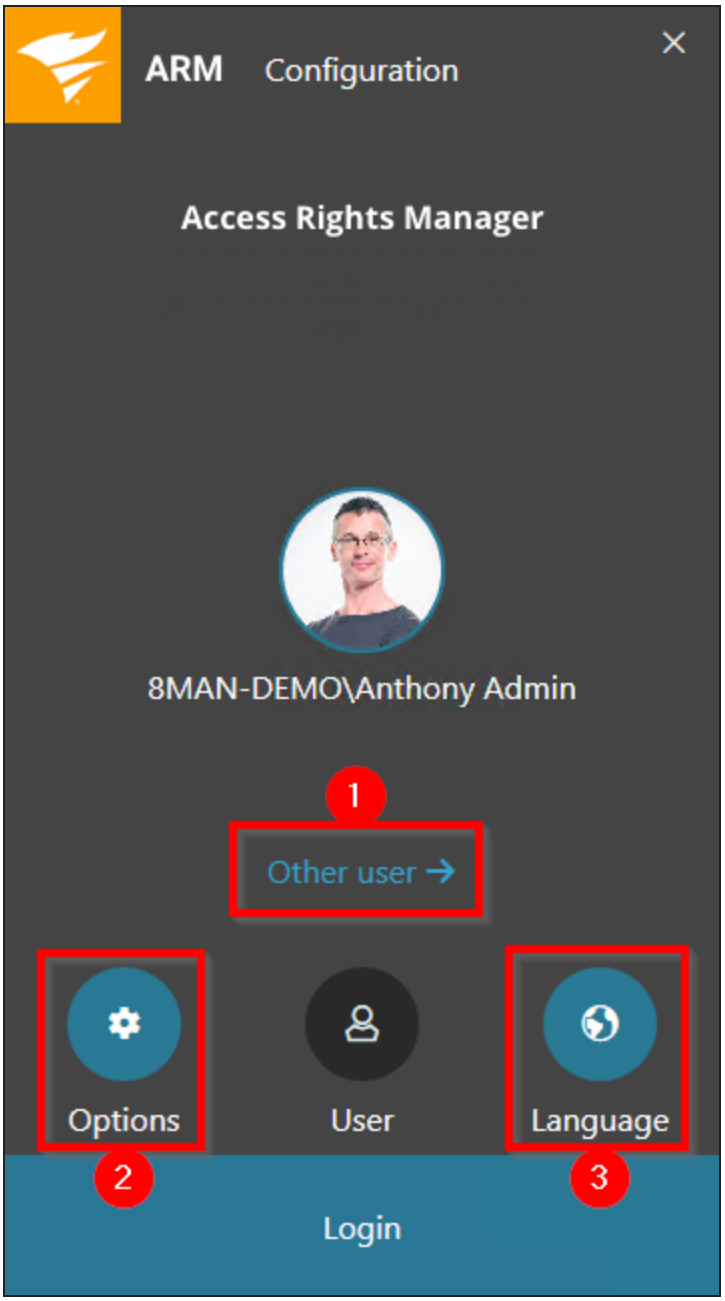


Start the configuration module.

Login

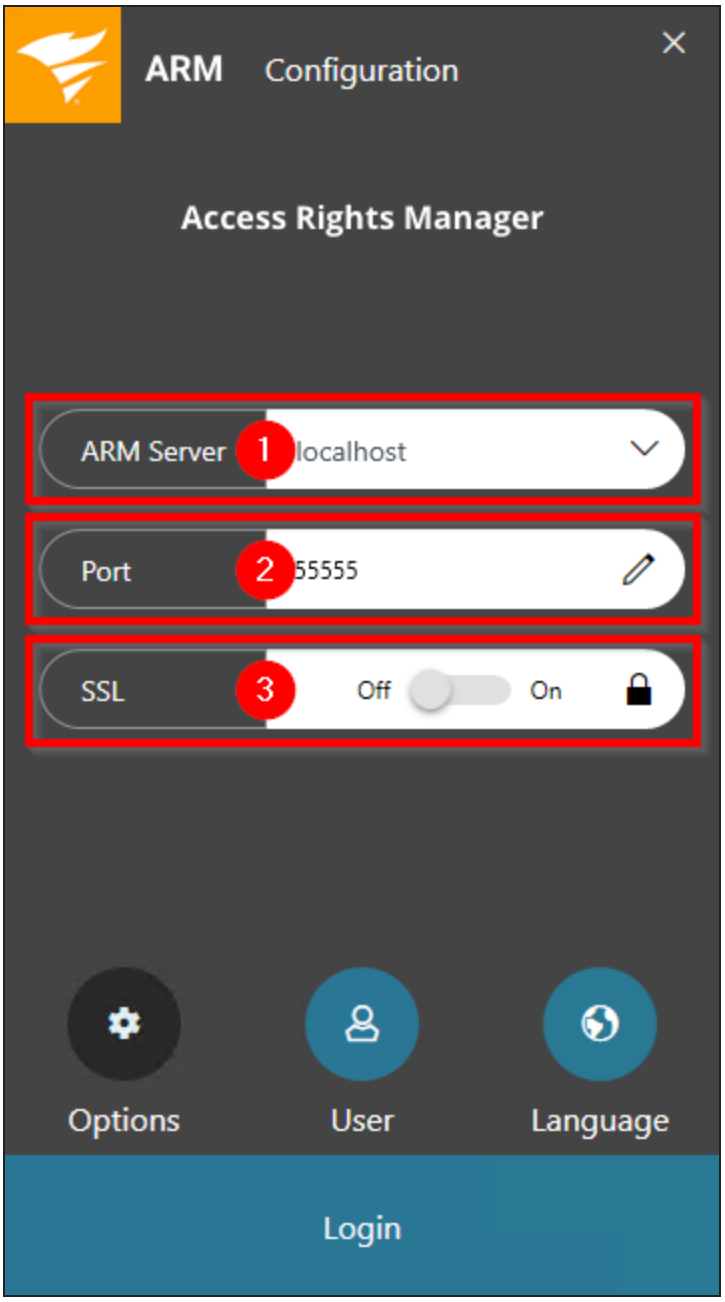
After a new installation, there is only one user who can log into ARM: the user who performed the installation.

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:

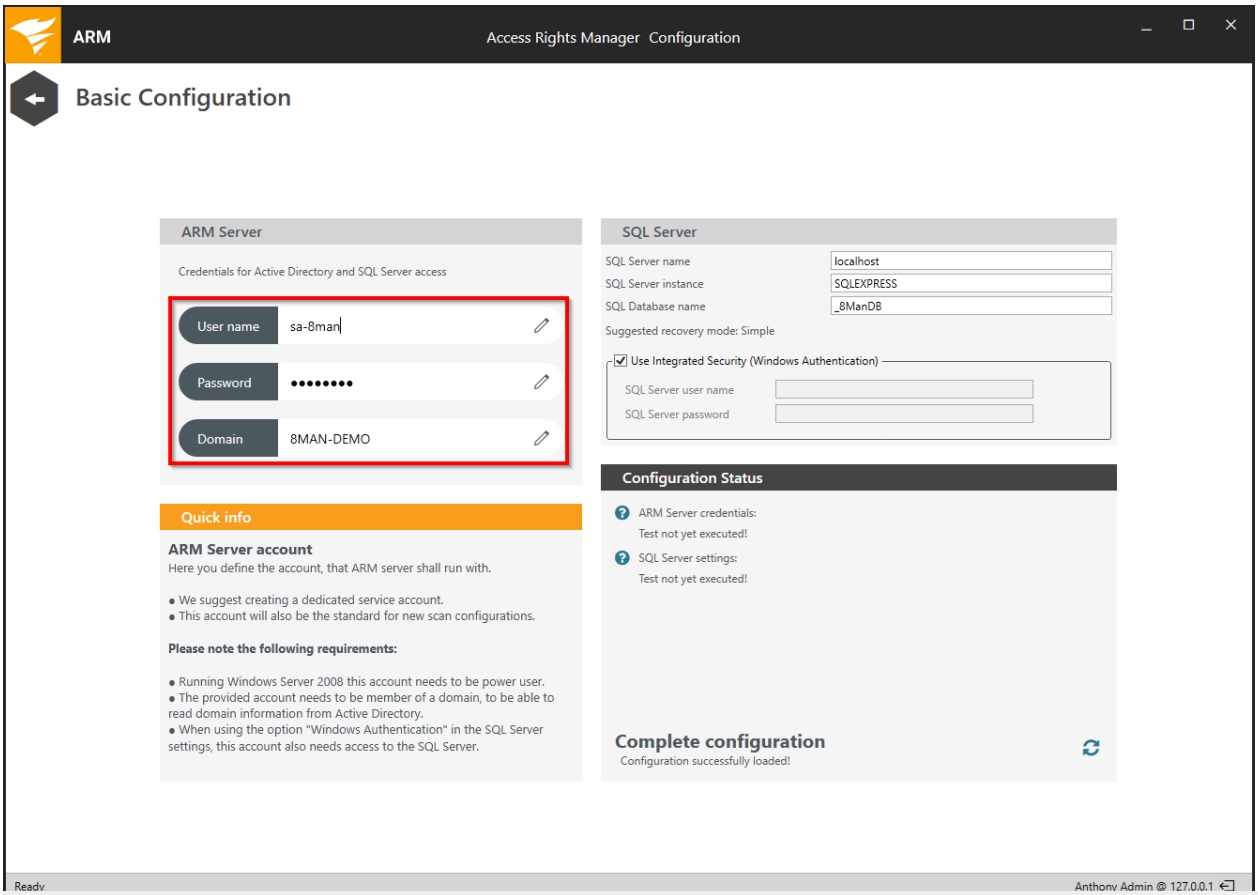
- SQL Server Name
- SQL Server Instance
- SQL Server authentication method and credentials

Select Basic Configuration on the ARM configuration application start page.

Enter ARM server credentials

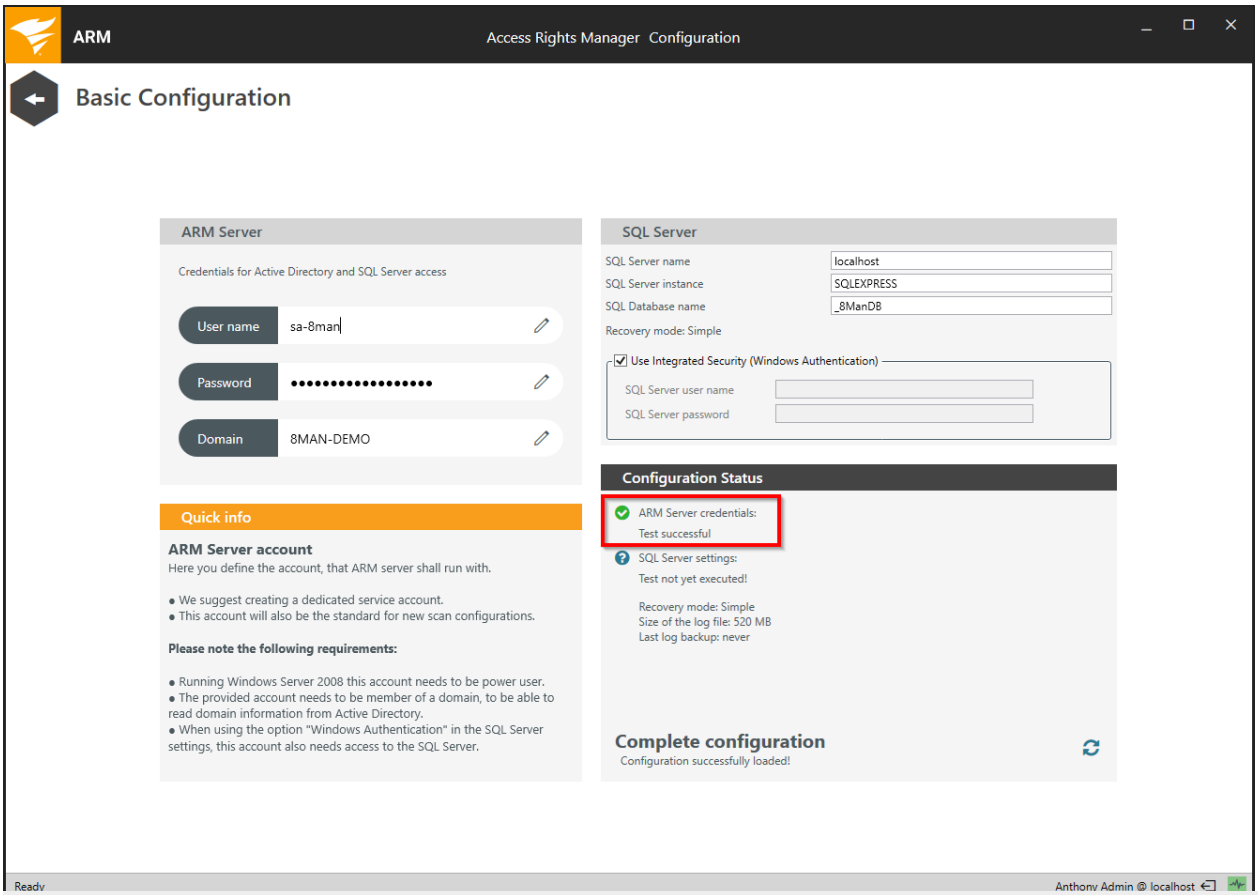
The ARM server is a service that runs with local permissions. The ARM server requires credentials to log on to Active Directory and the SQL server (if Windows authentication is used).

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



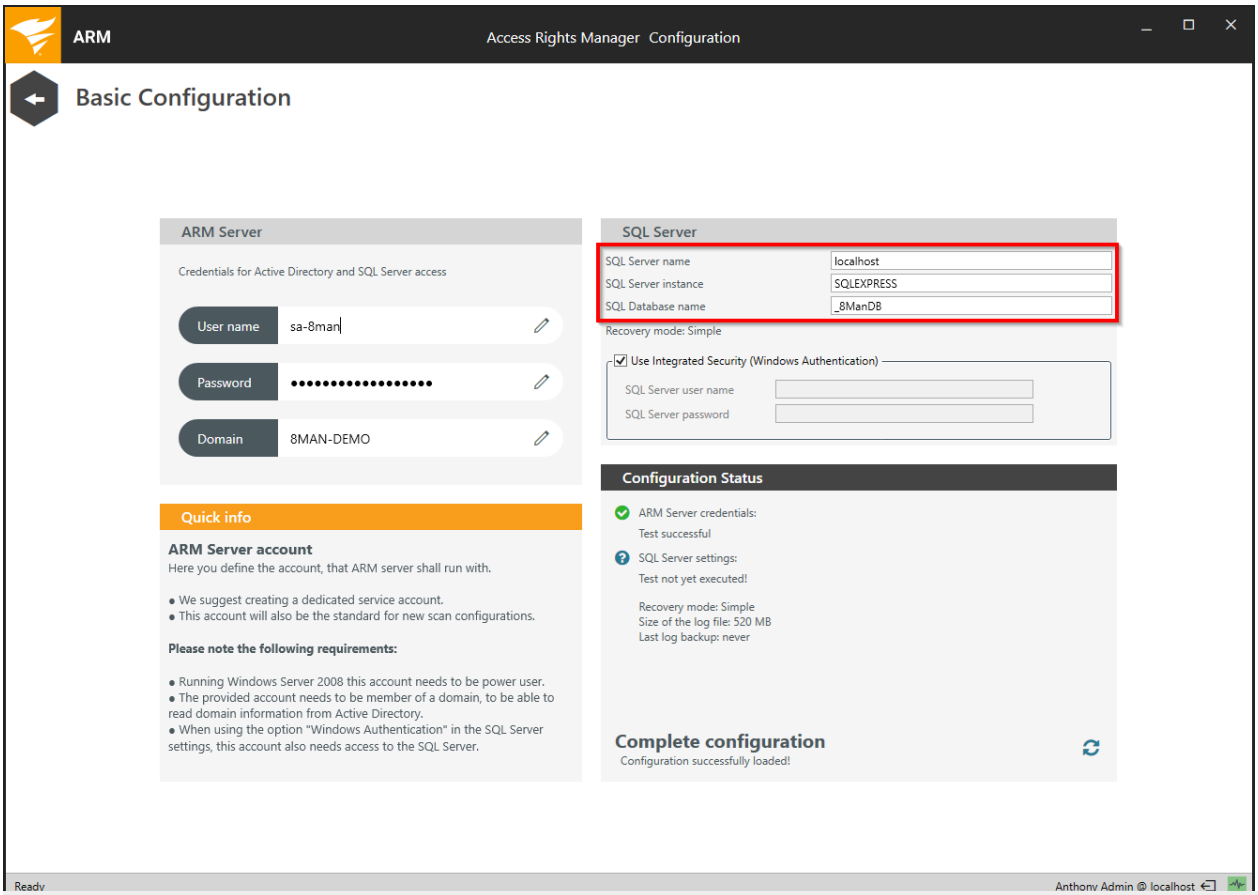
Enter the login credentials for Active Directory.

SolarWinds recommends the use of service accounts.



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

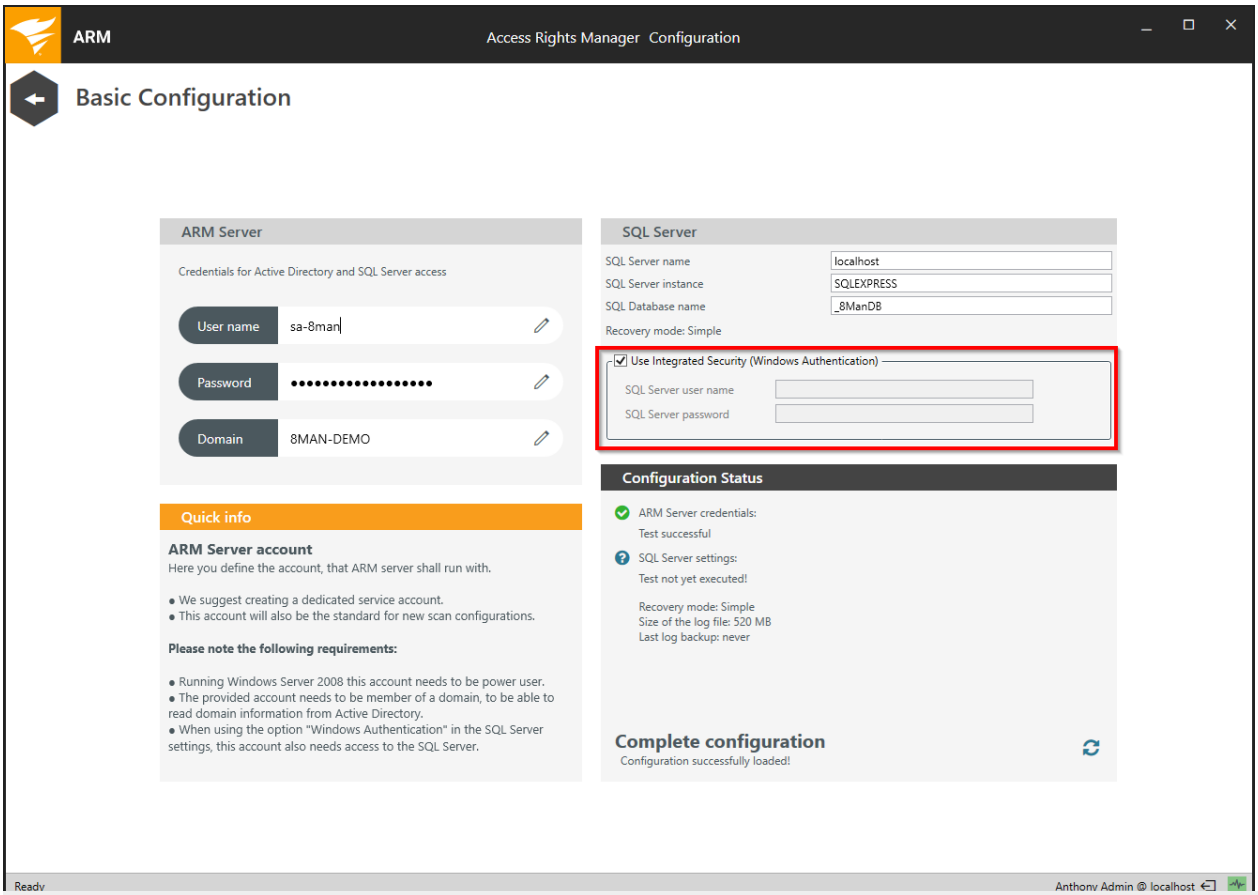
Enter SQL server credentials



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.

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).



Specify the type of logon to the SQL server.

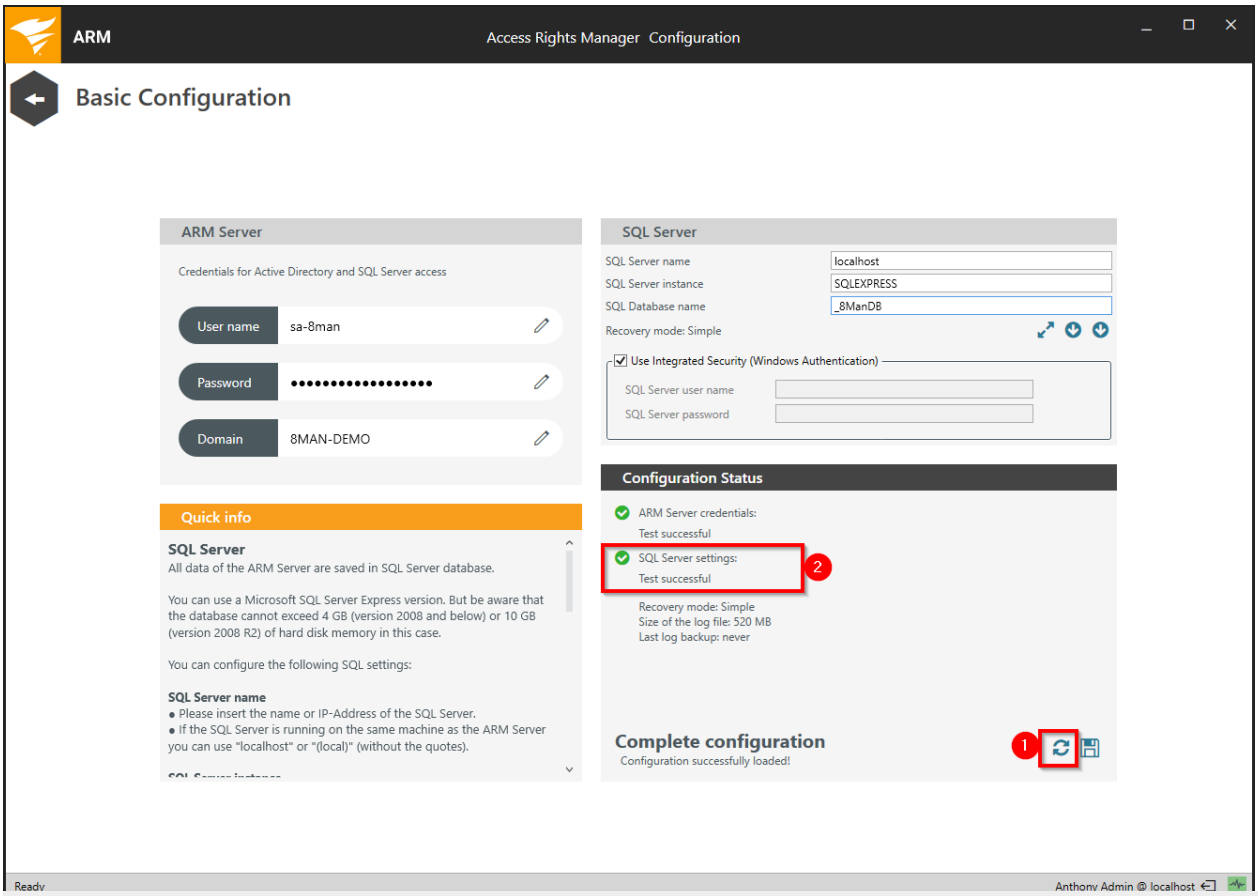
Option enabled

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

Option disabled

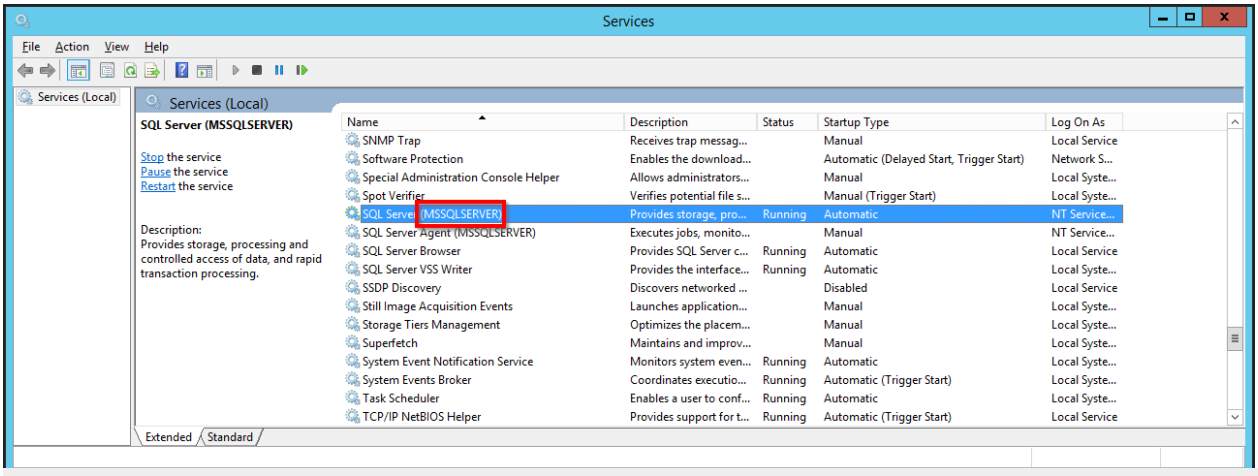
SQL server authentication is used. Enter user name and password to log into the SQL server.

Please refer to the notes on the use of service accounts.



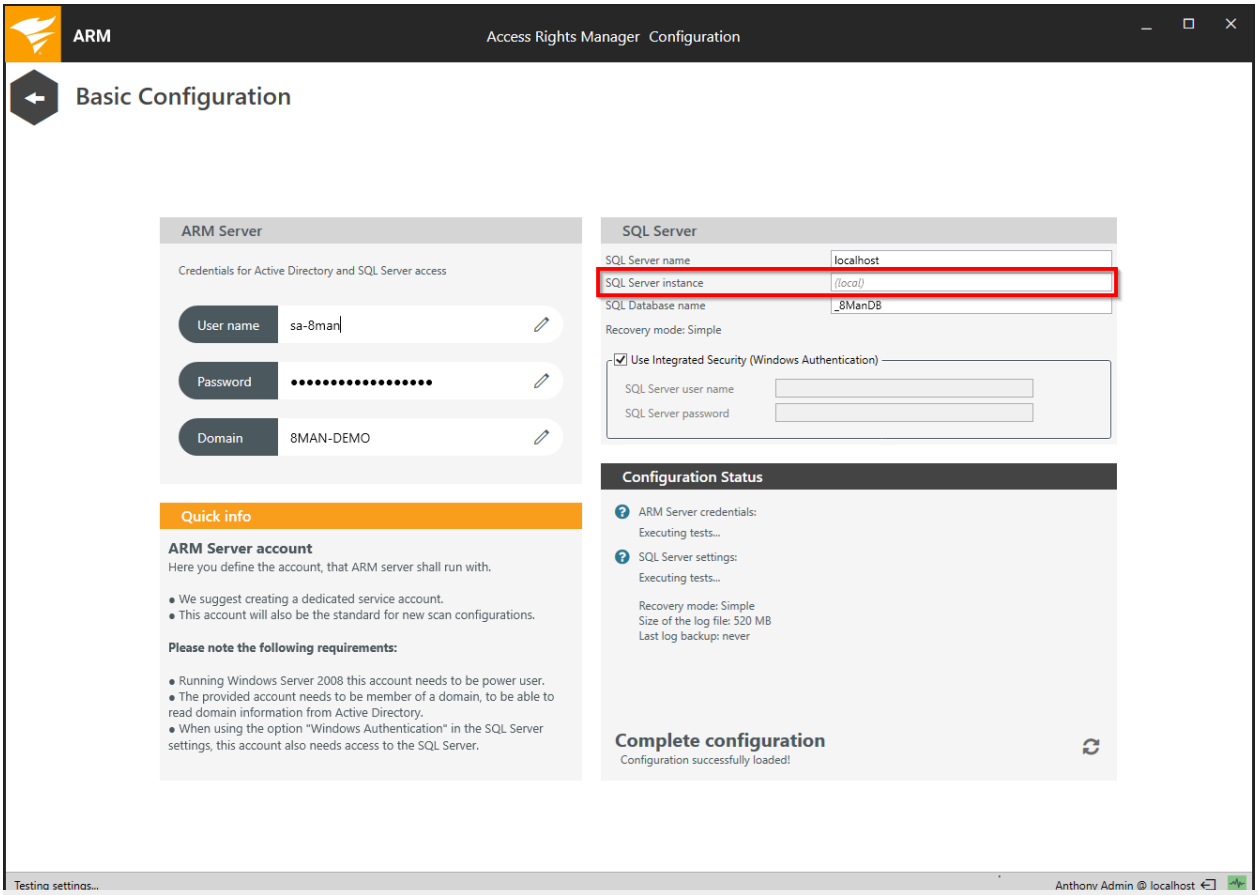
1. Click the button to verify the connection to the SQL server.
2. If valid credentials have been entered, ARM displays the message "Test successful".

Identify the SQL server instance name



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

```
services.msc
```



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:

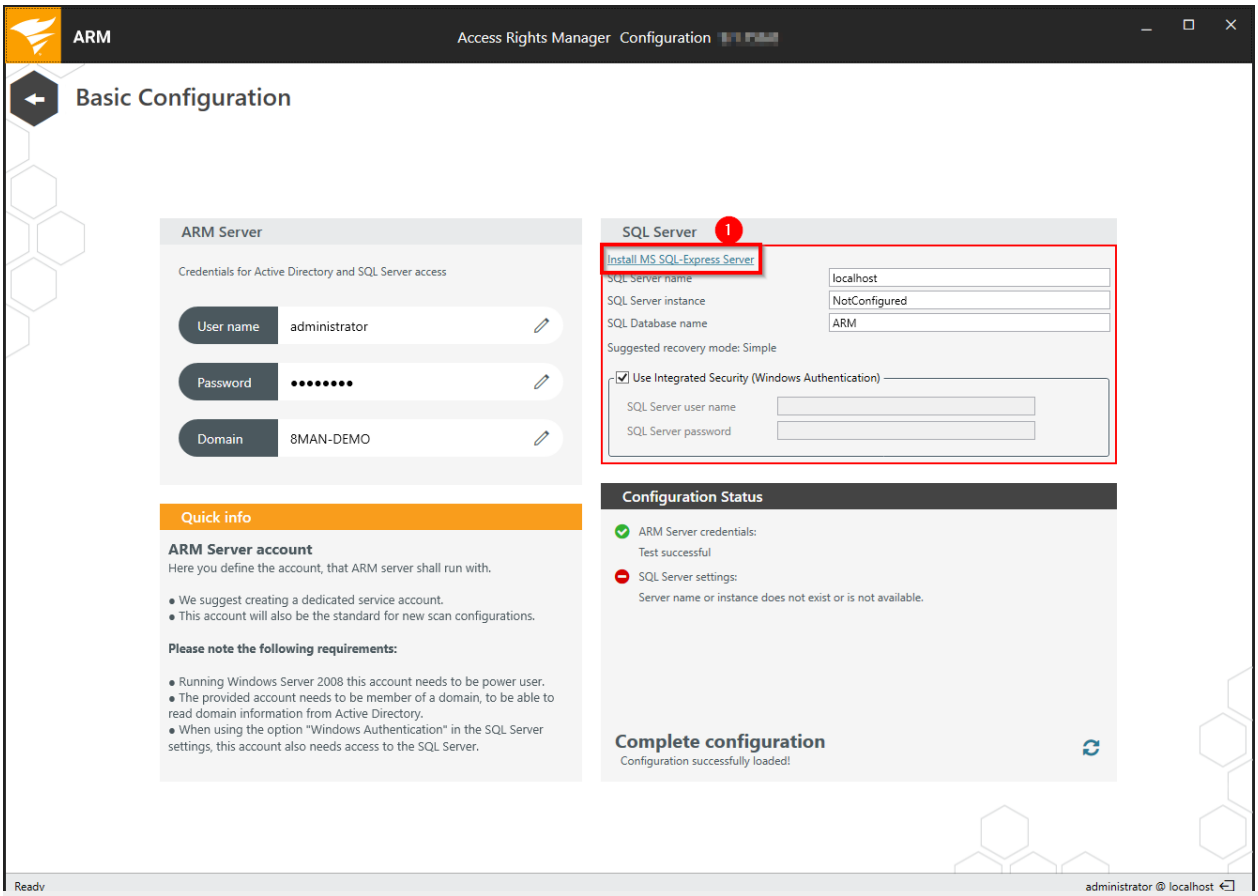
Information on actual data base size can be found in the Server health check.

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

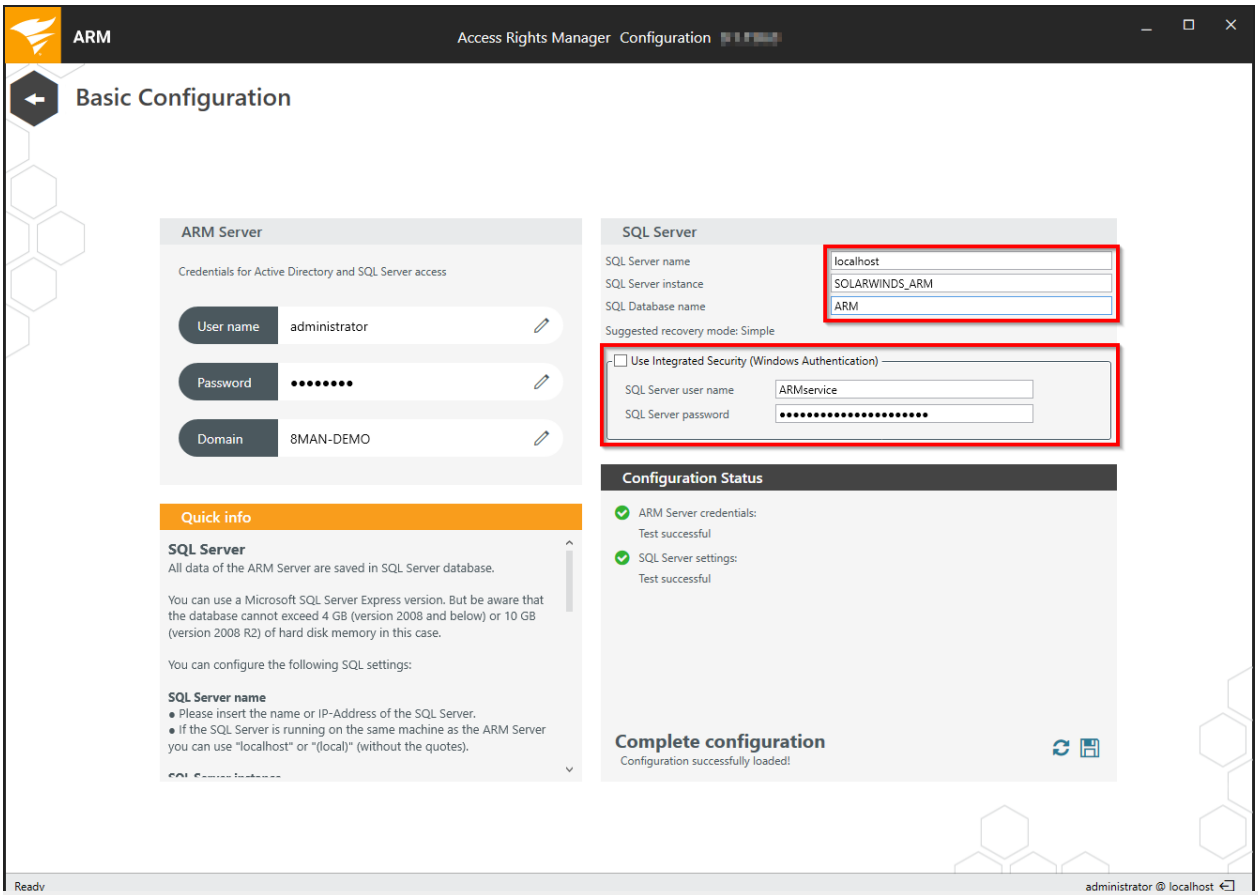
You can find additional information in the article Available SQL Server 2017 editions. (© 2020 Microsoft, https://www.microsoft.com/en-us/sql-server/sql-server-2017-editions, obtained on January 29, 2020).

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.



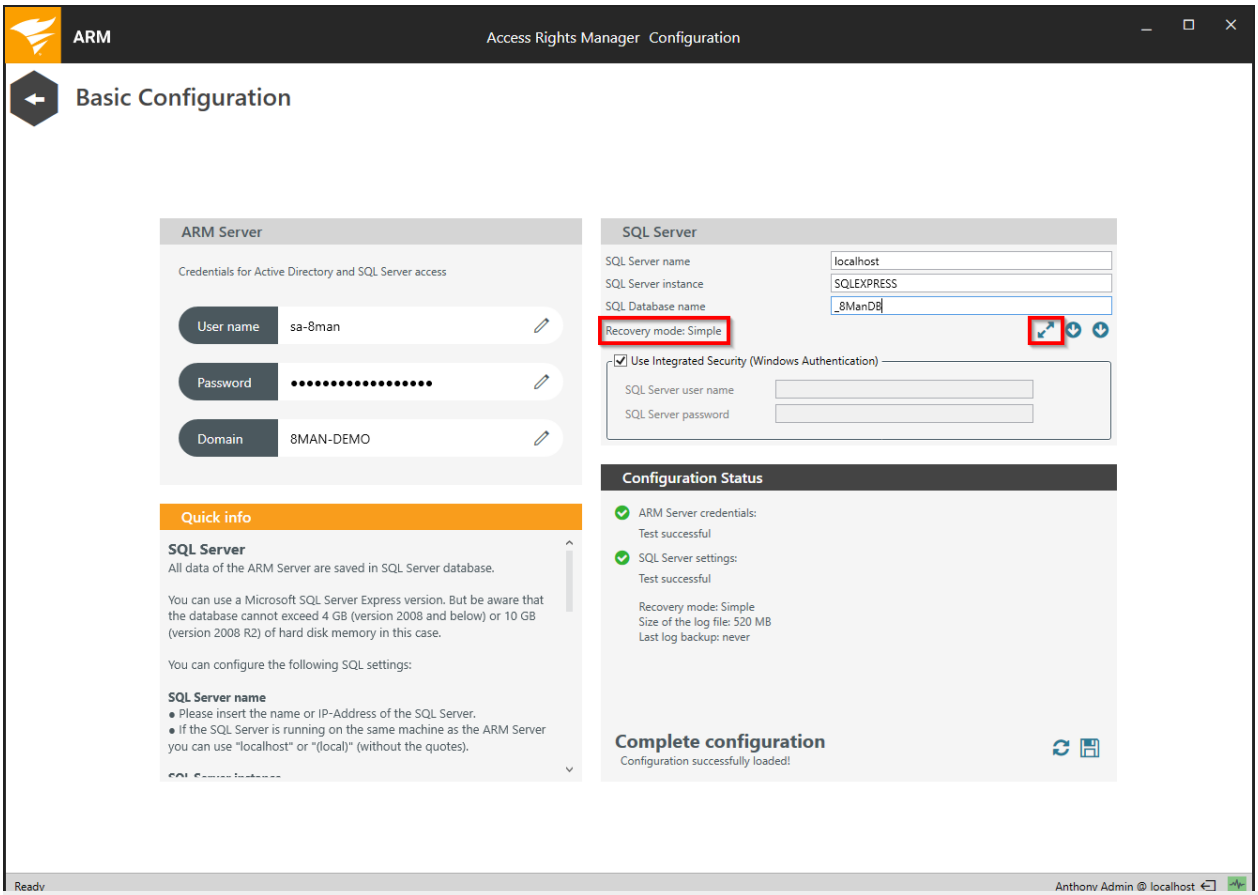
Click on the link to perform an SQL Express installation on the ARM server.



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

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 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.

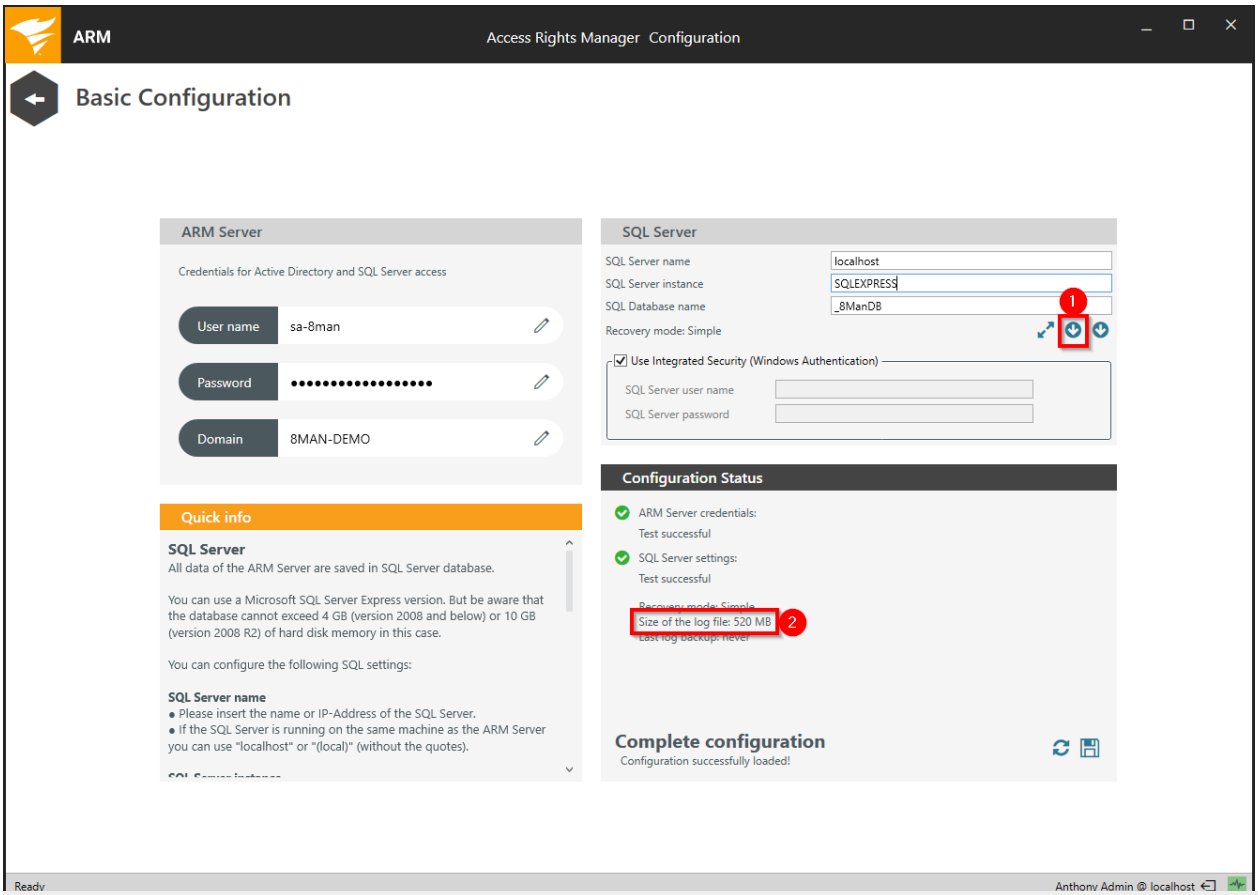
ⓘ For more information about recovery mode, see the article Recovery Models (SQL Server). (© 2020 Microsoft, https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/recovery-models-sql-server?view=sql-server-2017, obtained on January 29, 2020)

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.

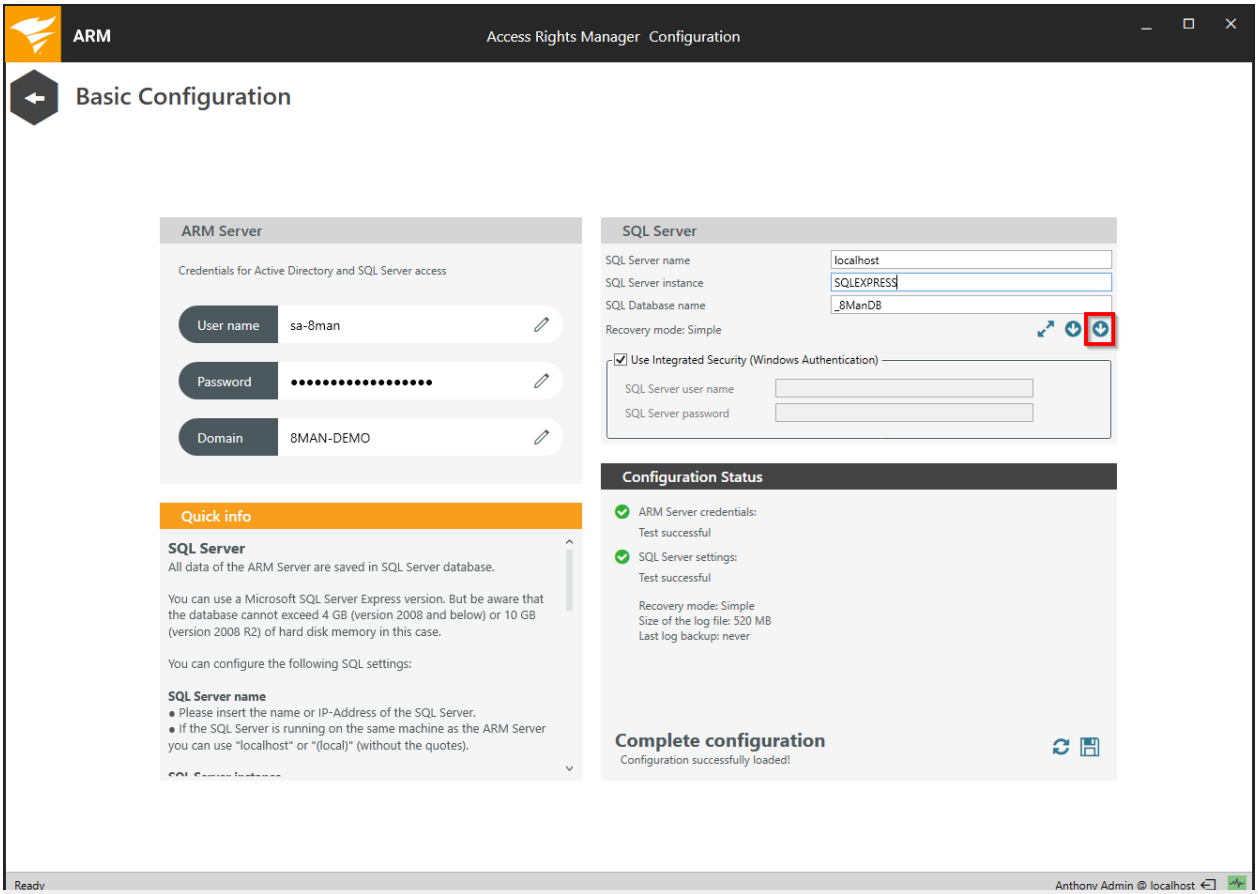
Scheduled data base maintenance is only performed if all ARM user interfaces are closed. You can identify logged in users in the menu item server status.

Shrink database logs



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

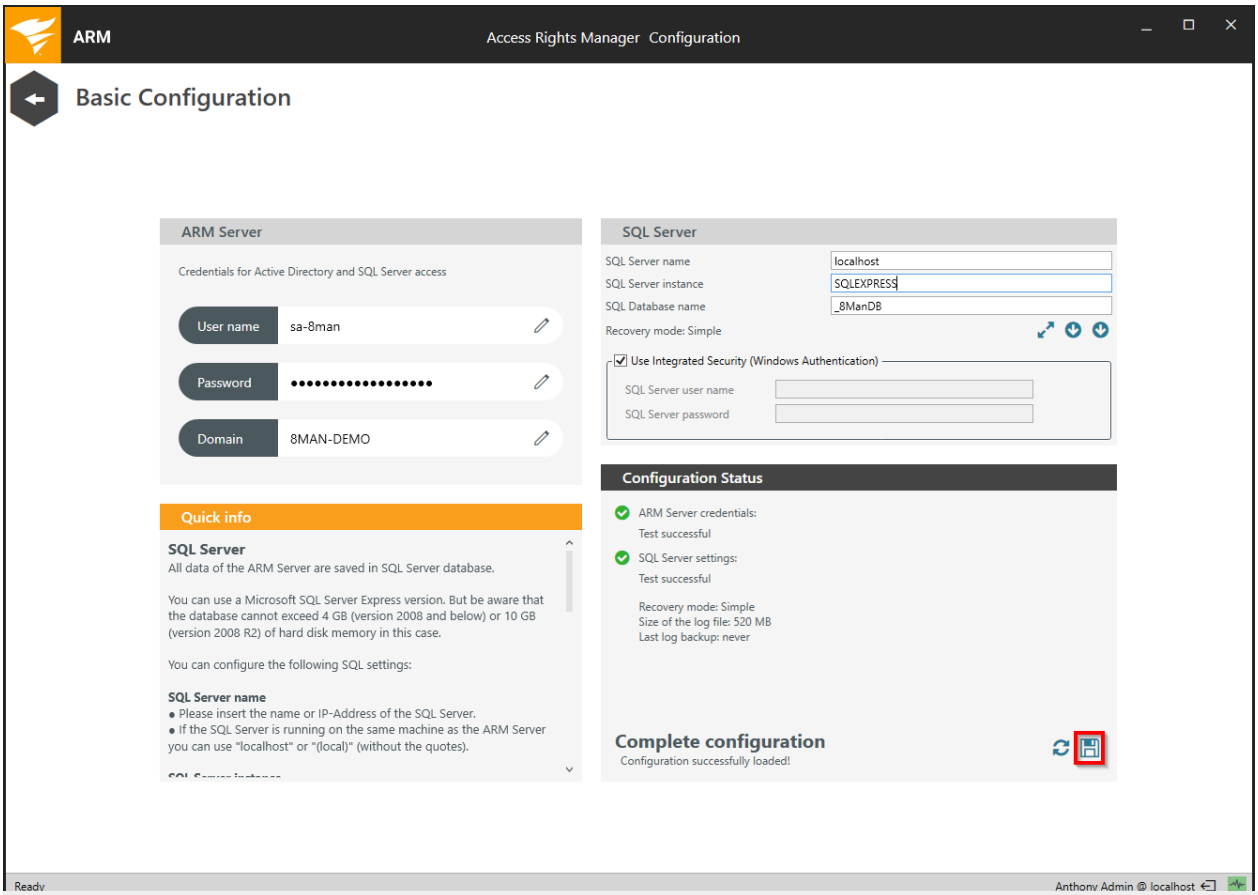


Shrinking the database frees up disk space. This action is performed immediately when clicking the button.

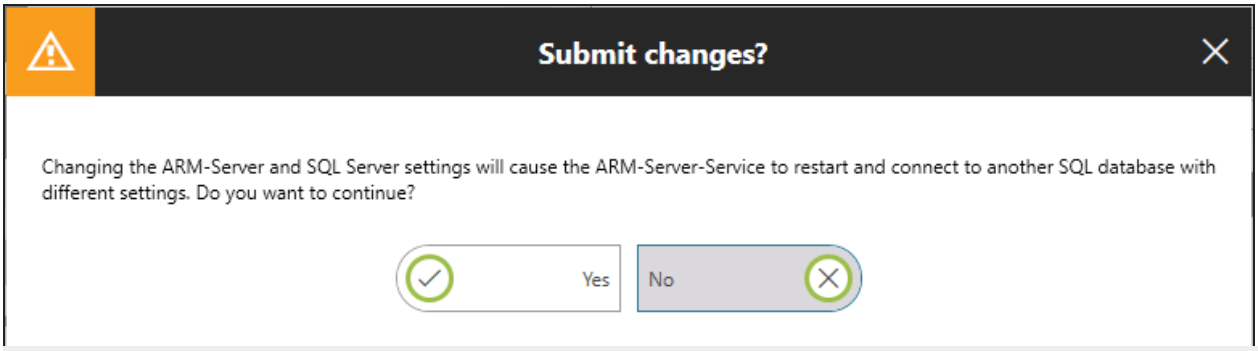
For more information on data base size or available disk space please see: Server Health-Check.

Please see additional notes on SQL Express Edition.

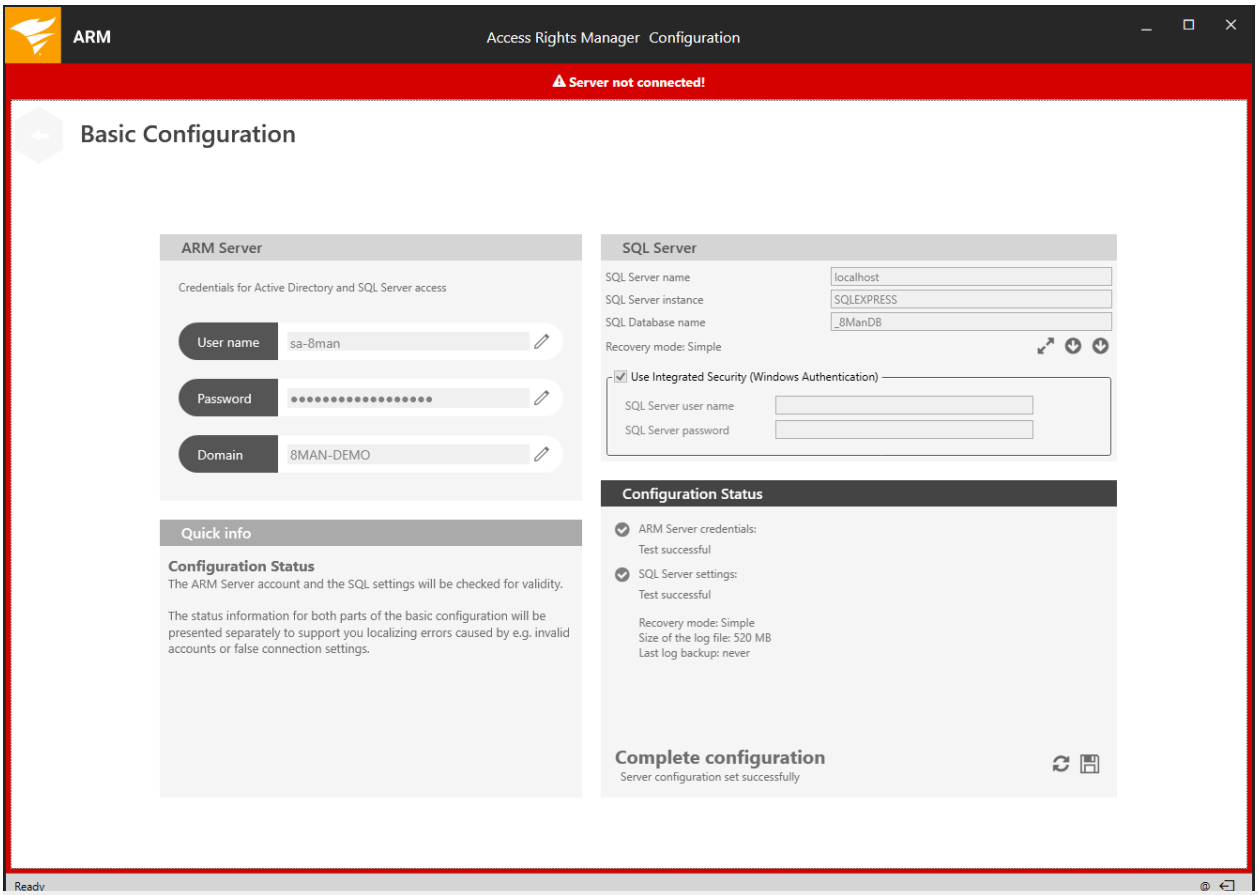
Complete and save basic configuration



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



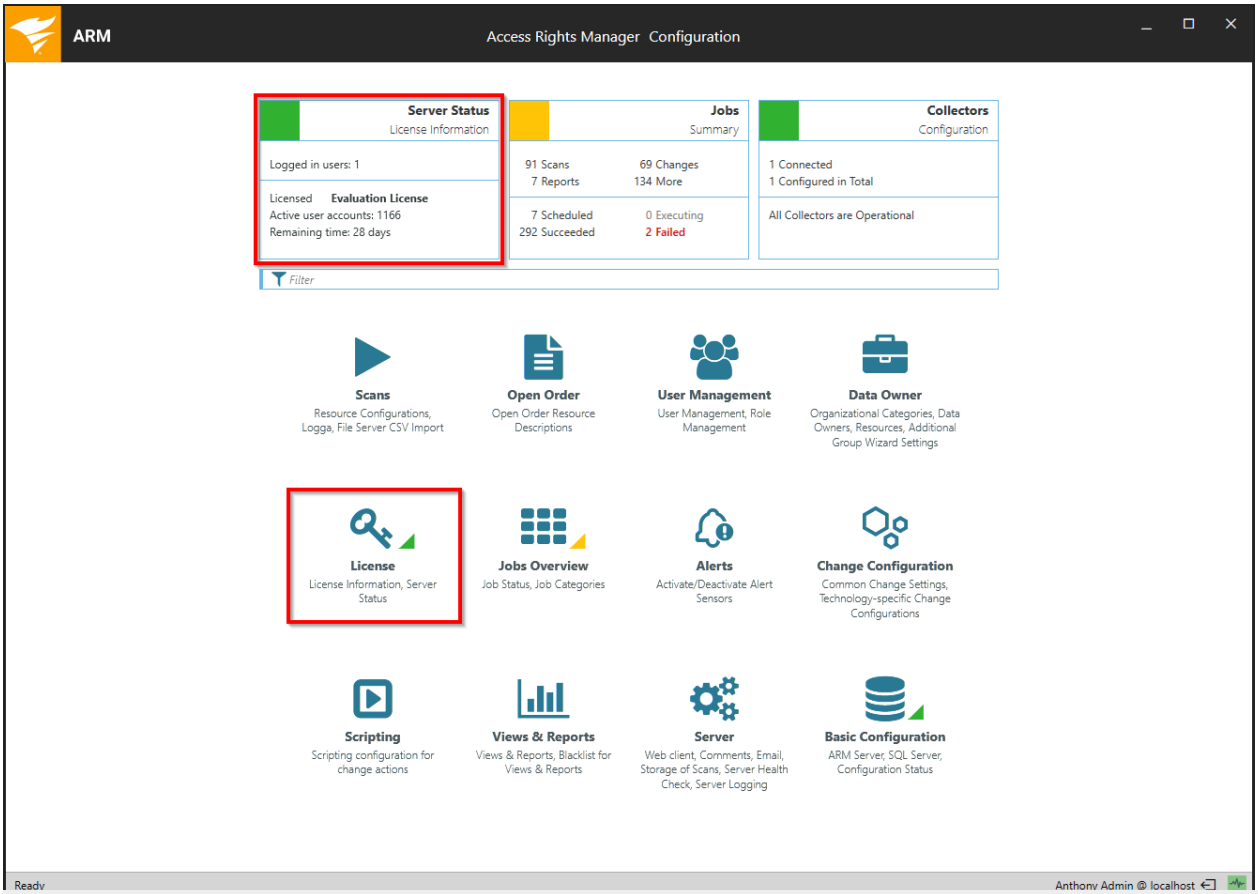
Confirm the changes.



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



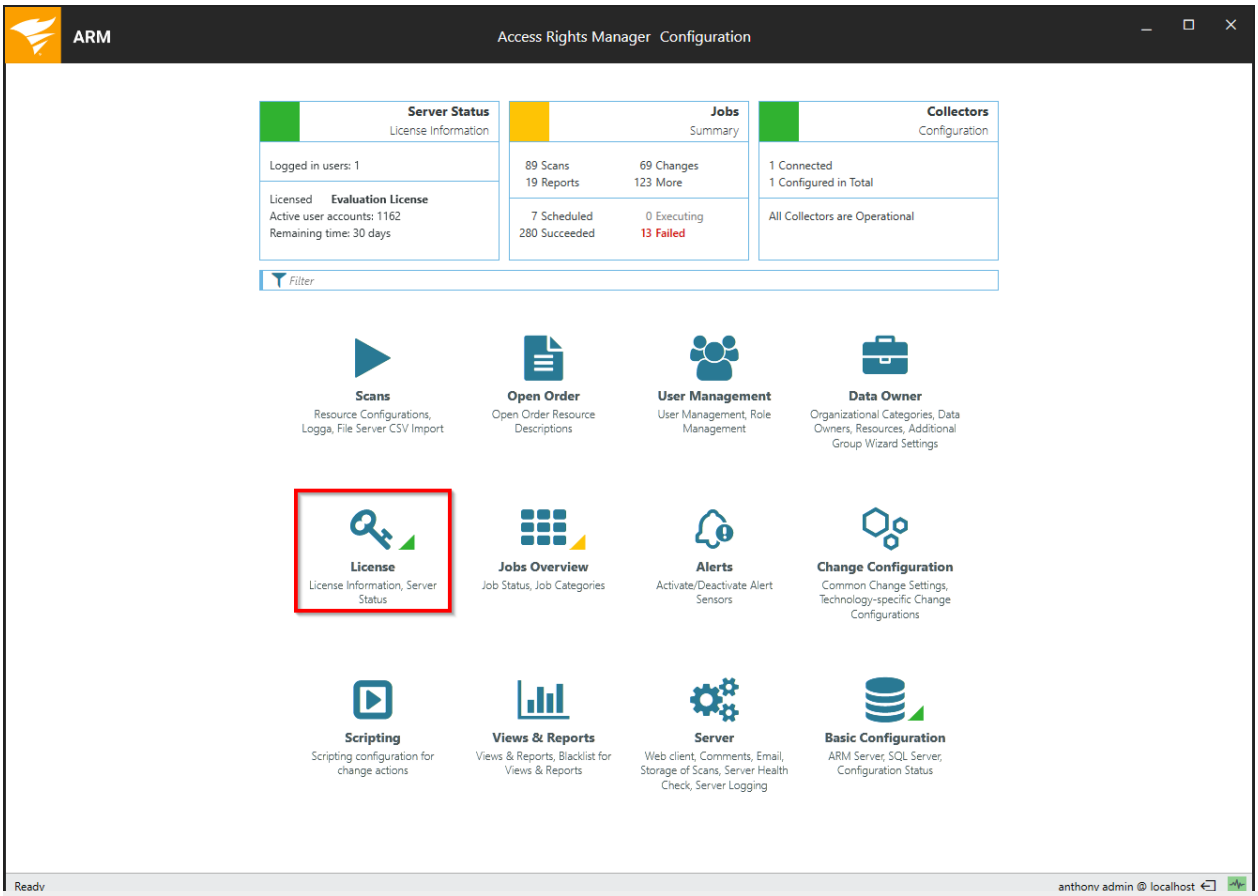
The ARM configuration home page displays information about the "Server Status" including license information.

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

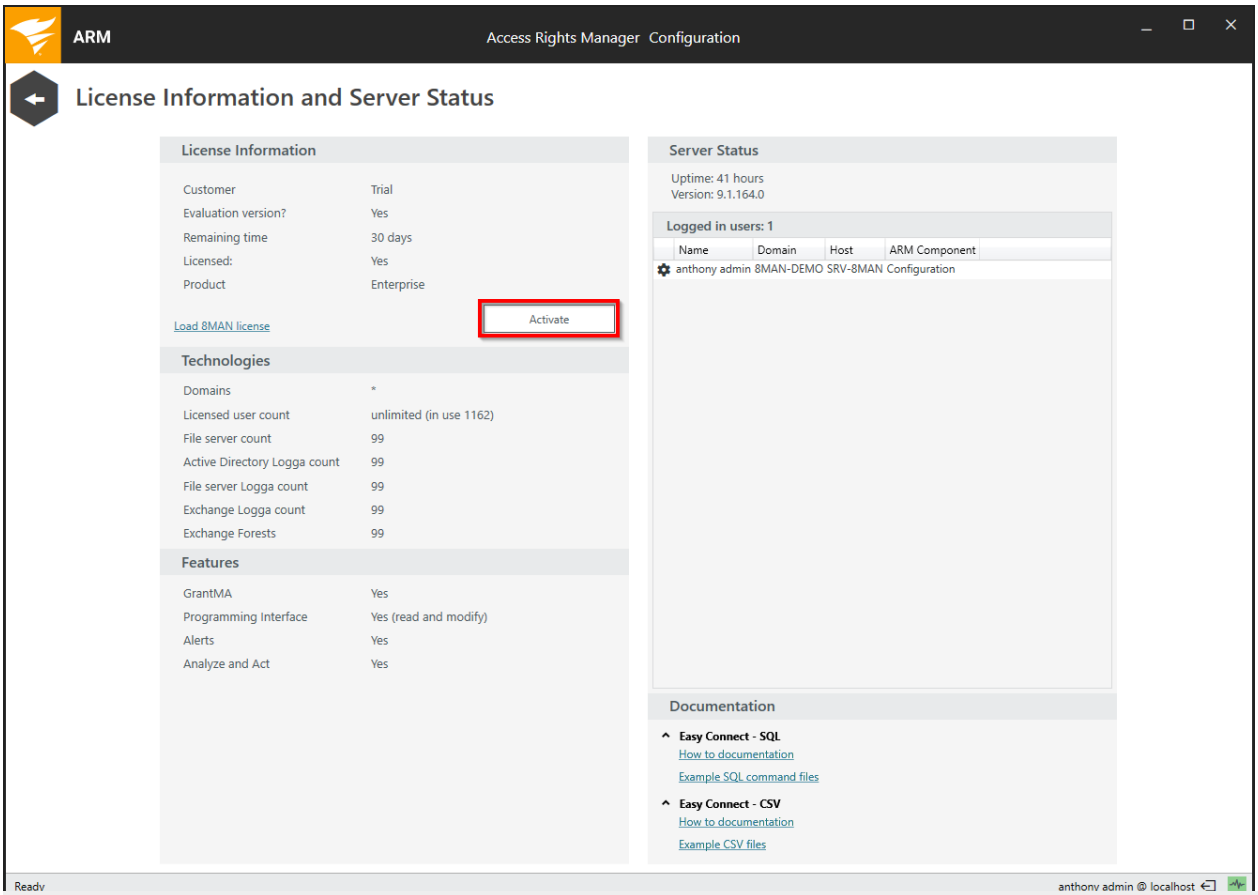
Switch from an evaluation license to a production license

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.

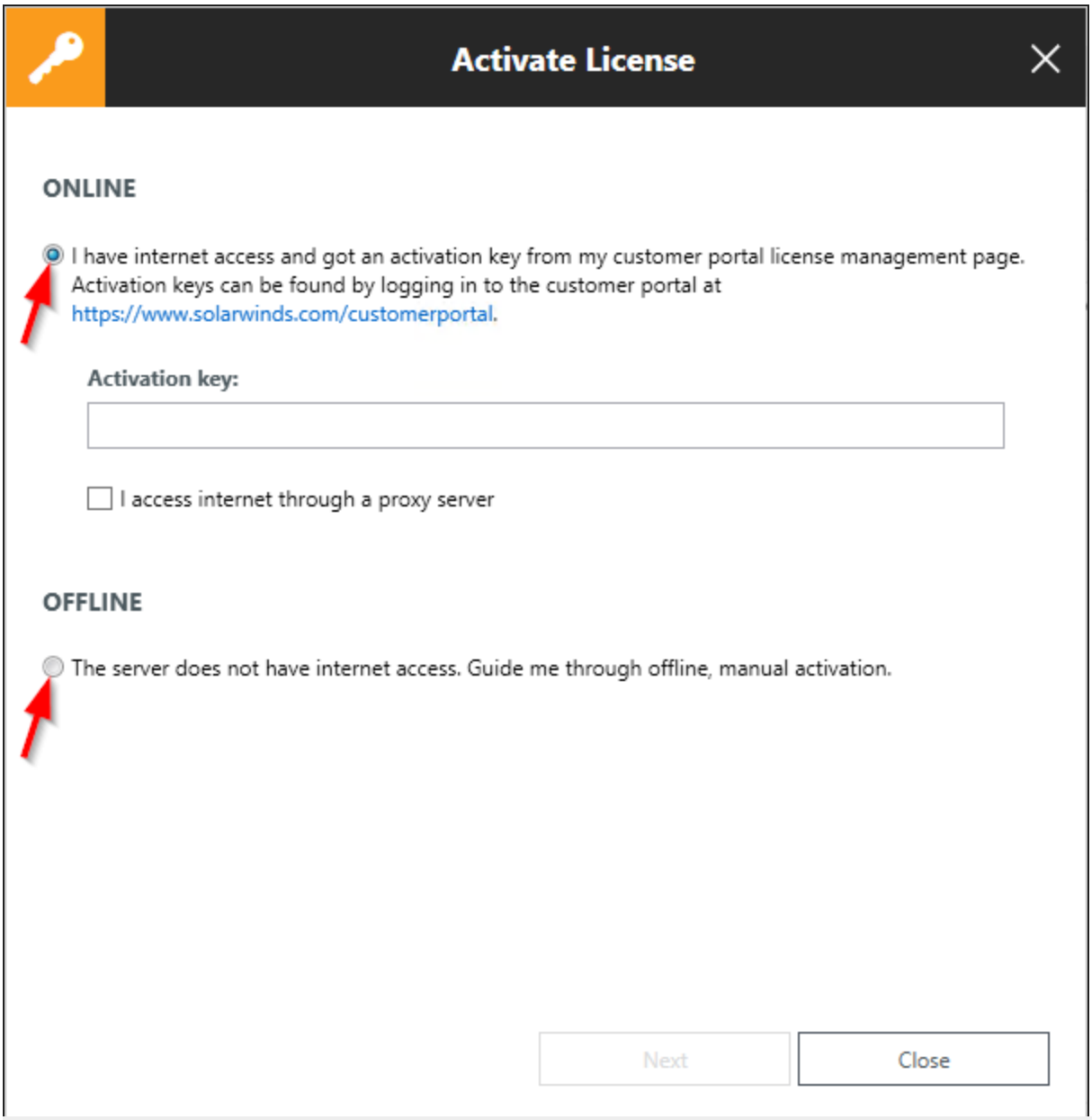
Activating a license binds your purchased license to a single installation. Please refer to the chapter transfer a license to another server if needed.



Start the ARM configuration application and click "License".



Click "Activate".

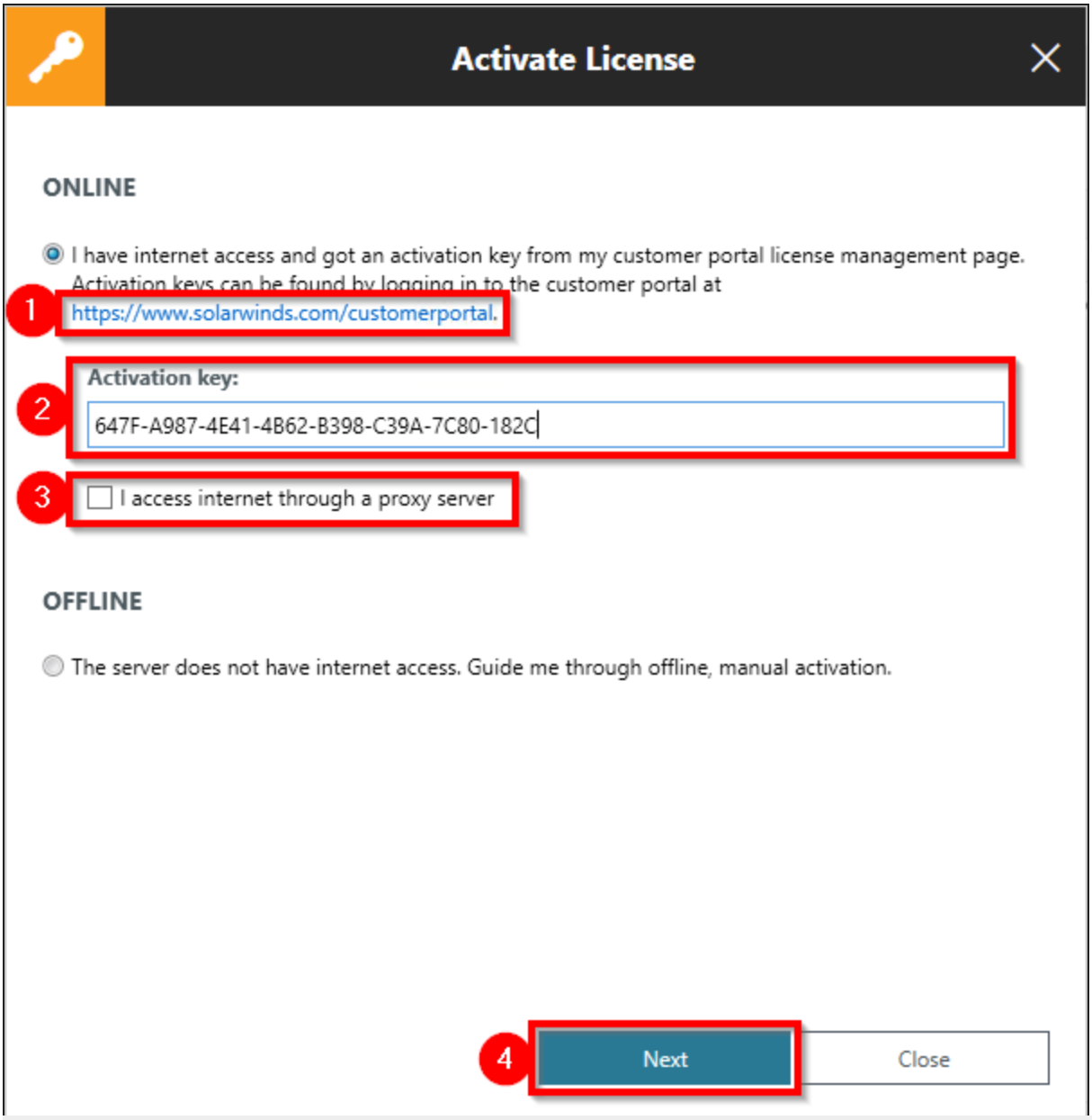


Decide how you want to perform the license activation.

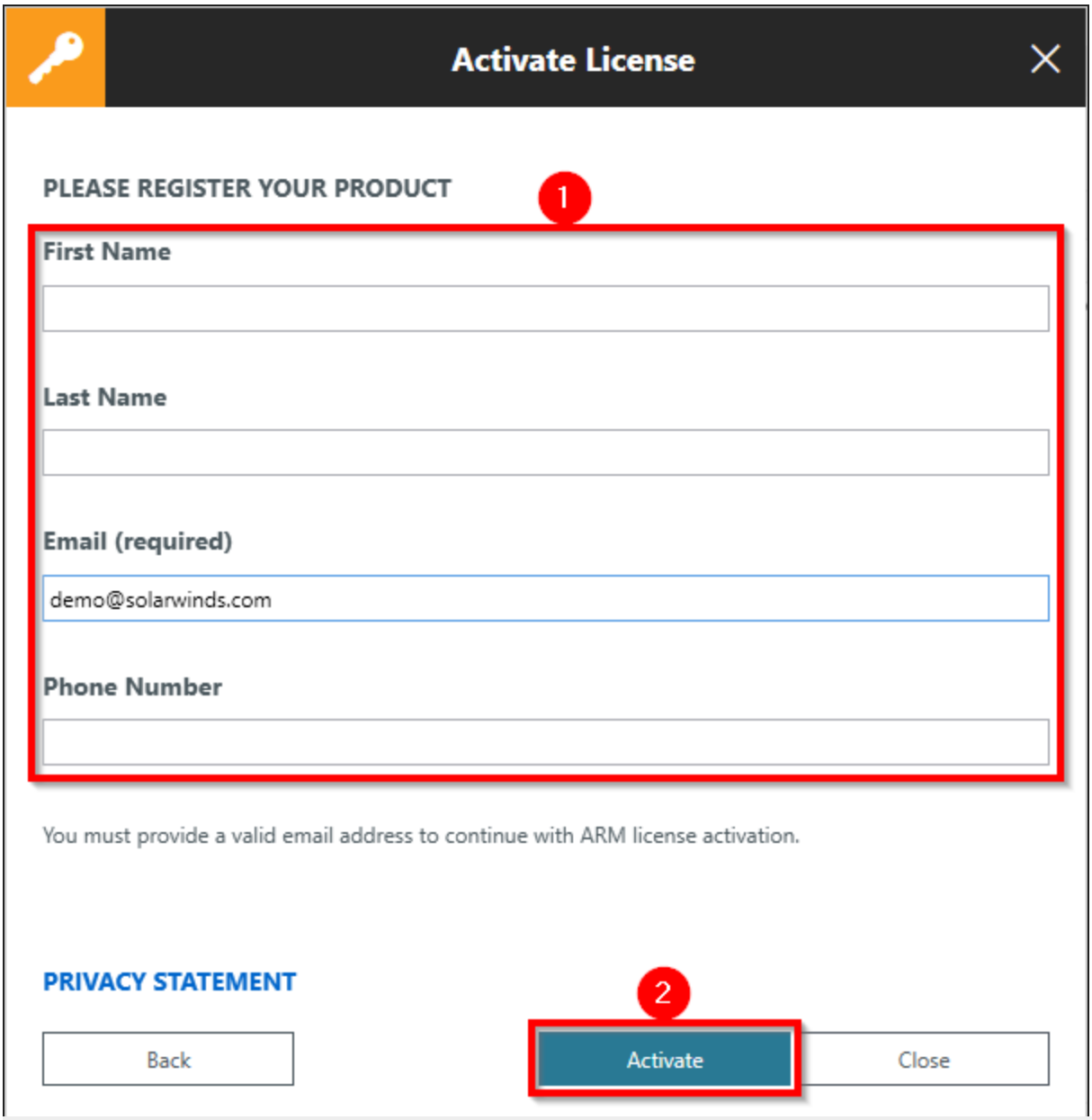
ONLINE
Recommended. The ARM server needs an internet connection.

OFFLINE
Use offline if the ARM server has no internet connection.

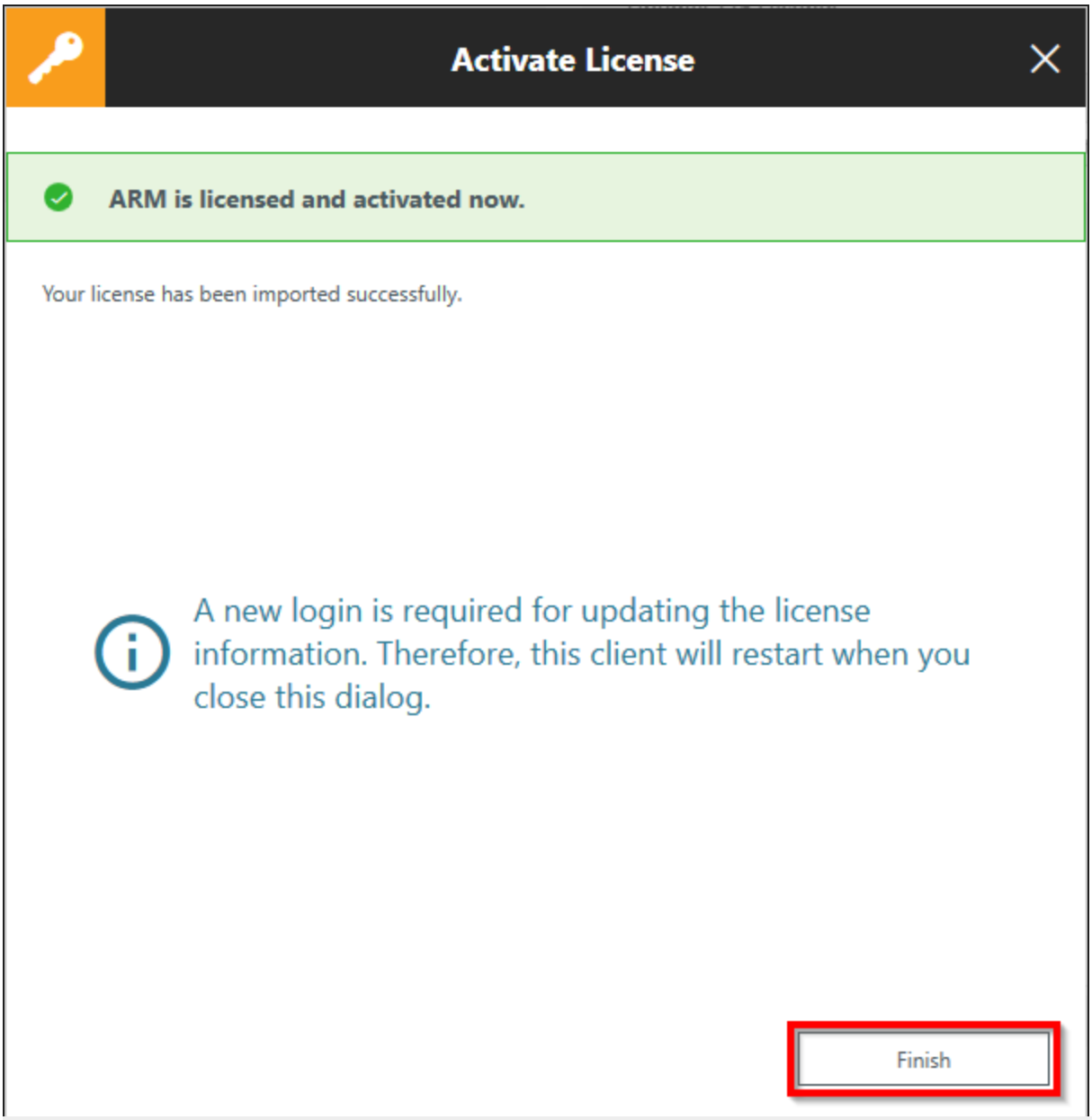
Online activation



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".

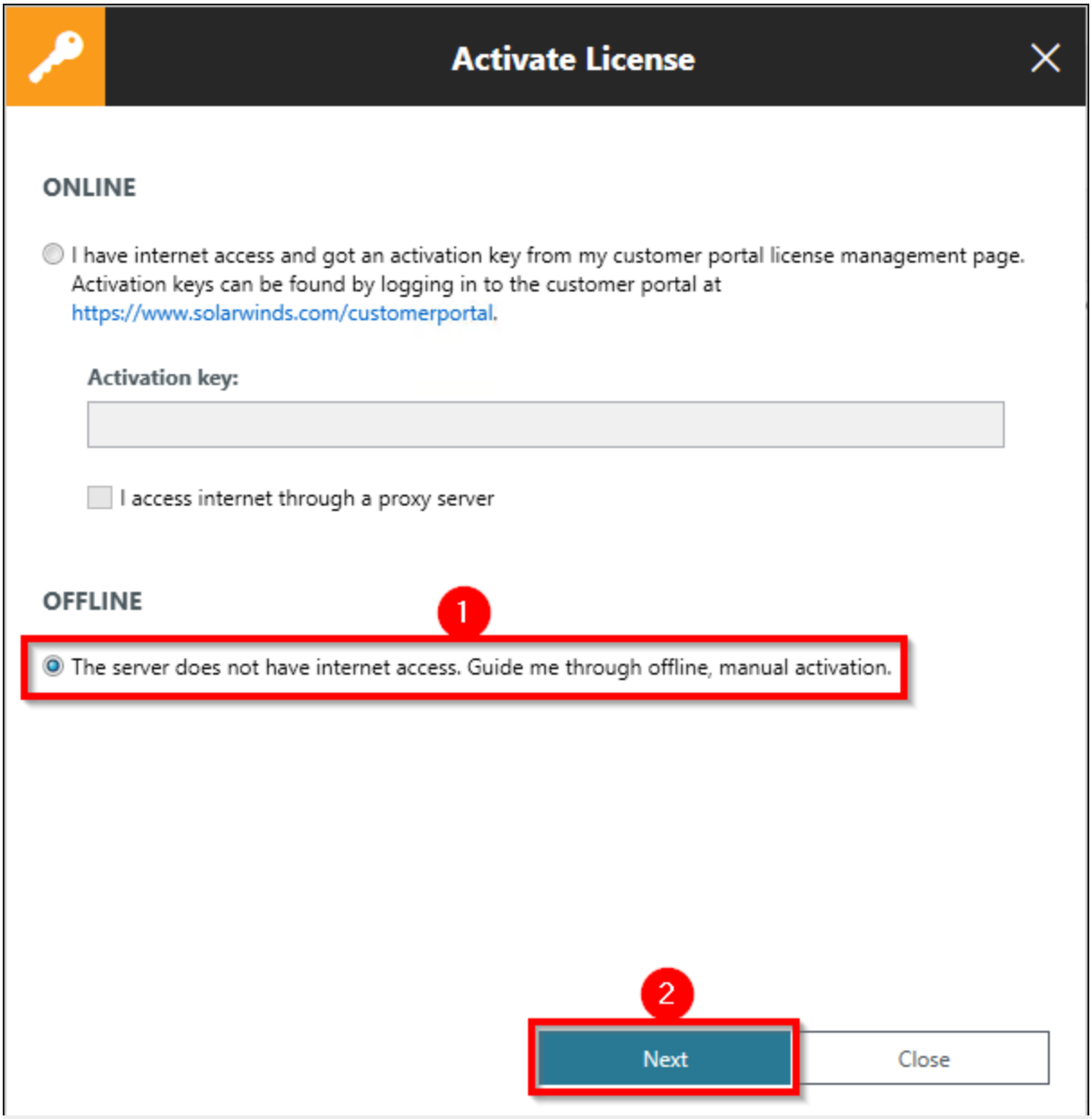


1. Specify to whom the product should be registered. You must enter at least one email address.
2. Click "Activate".



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

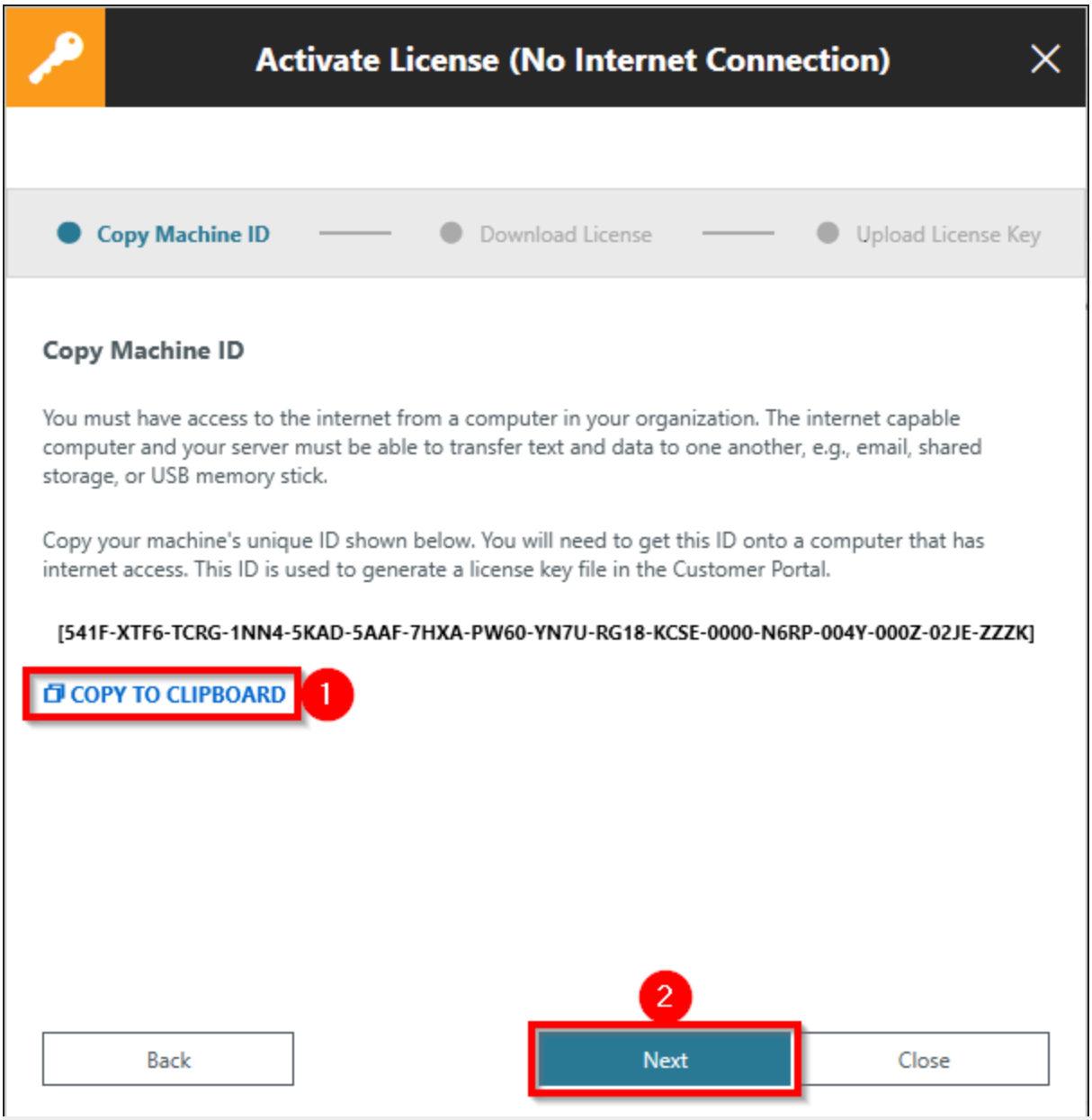
Offline activation



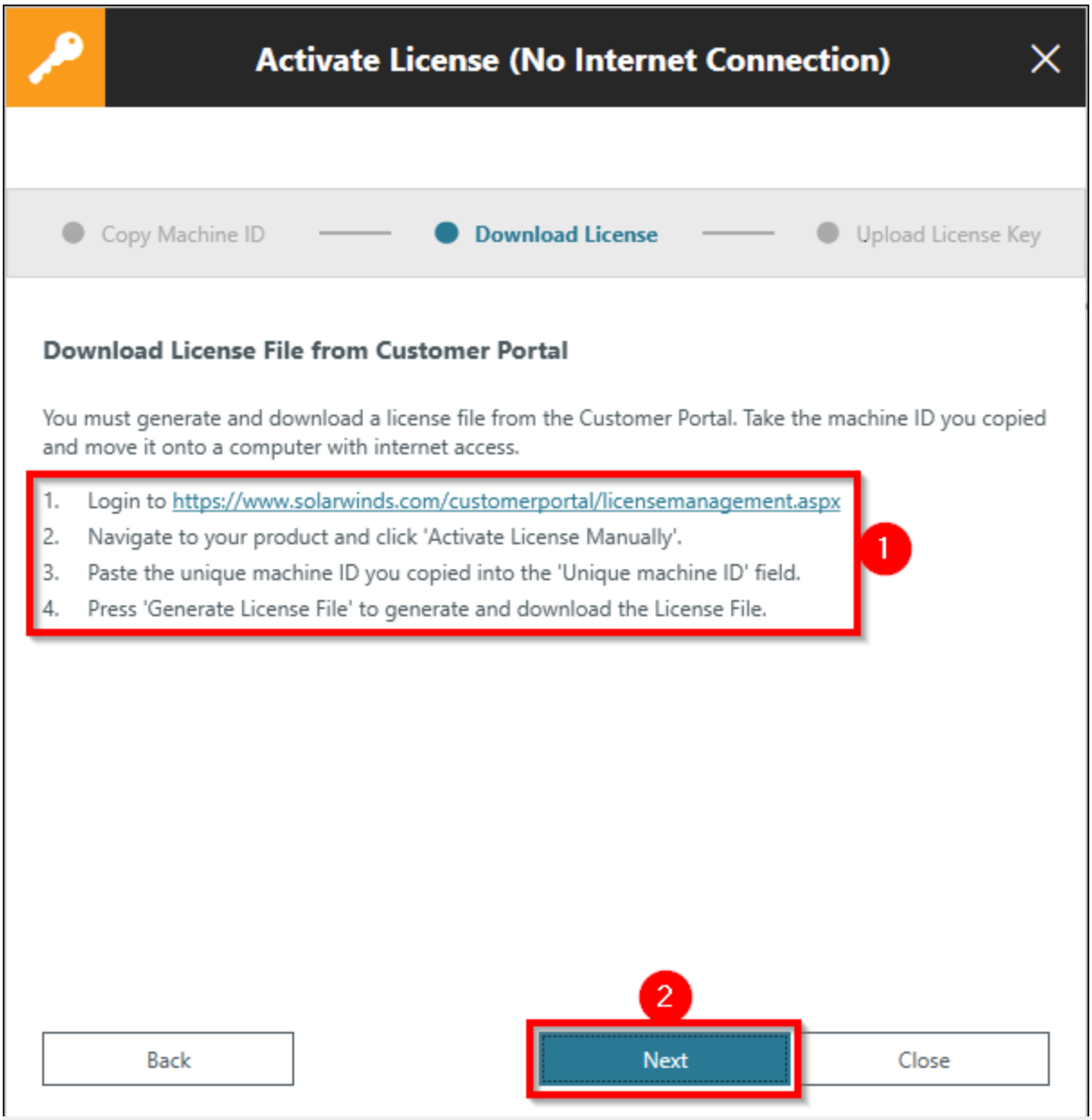
1. Select "Offline" activation.
2. Click "Next".

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

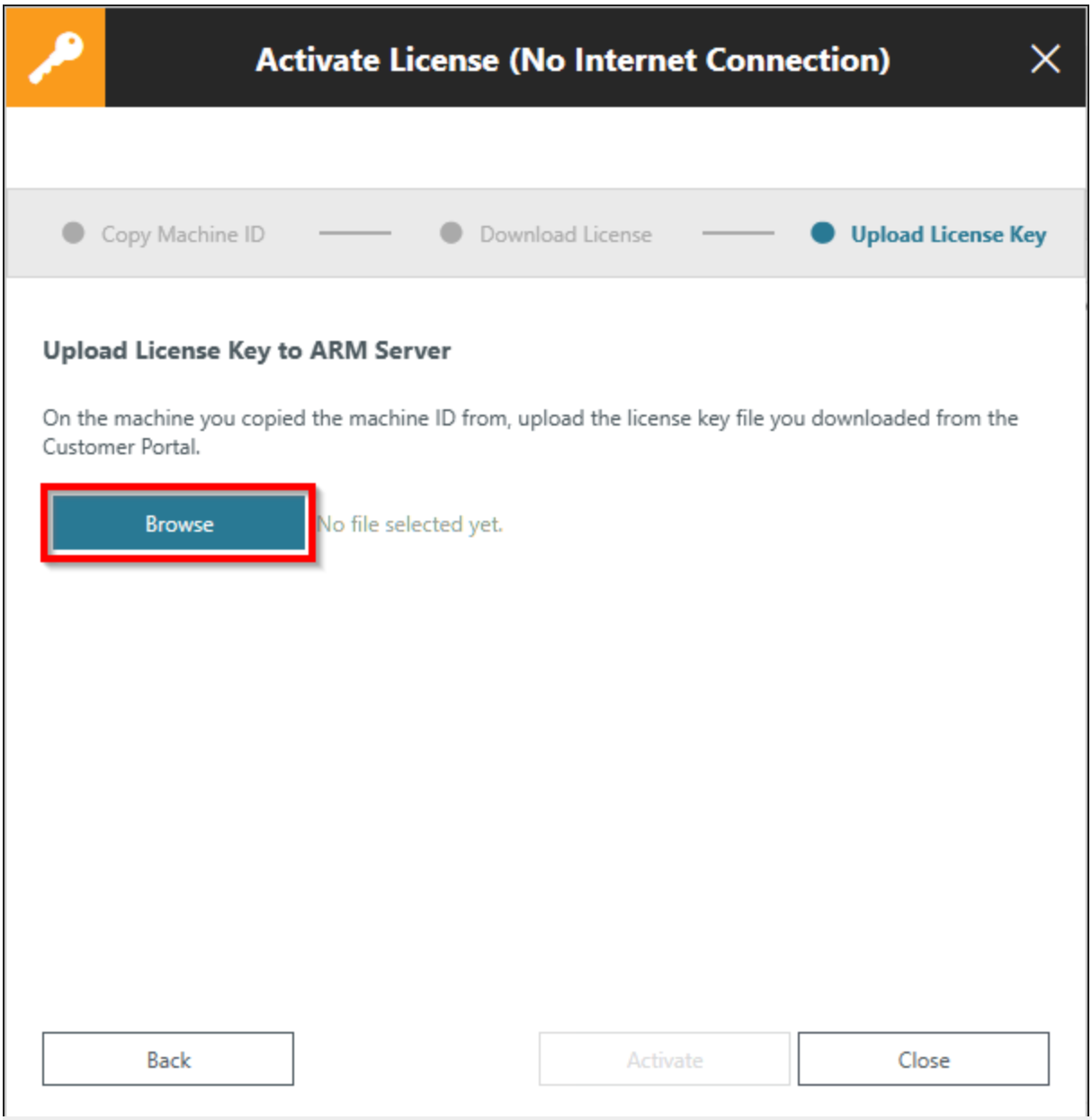
- clipboard shared with guest and host
- shared folders
- email
- USB memory stick etc.



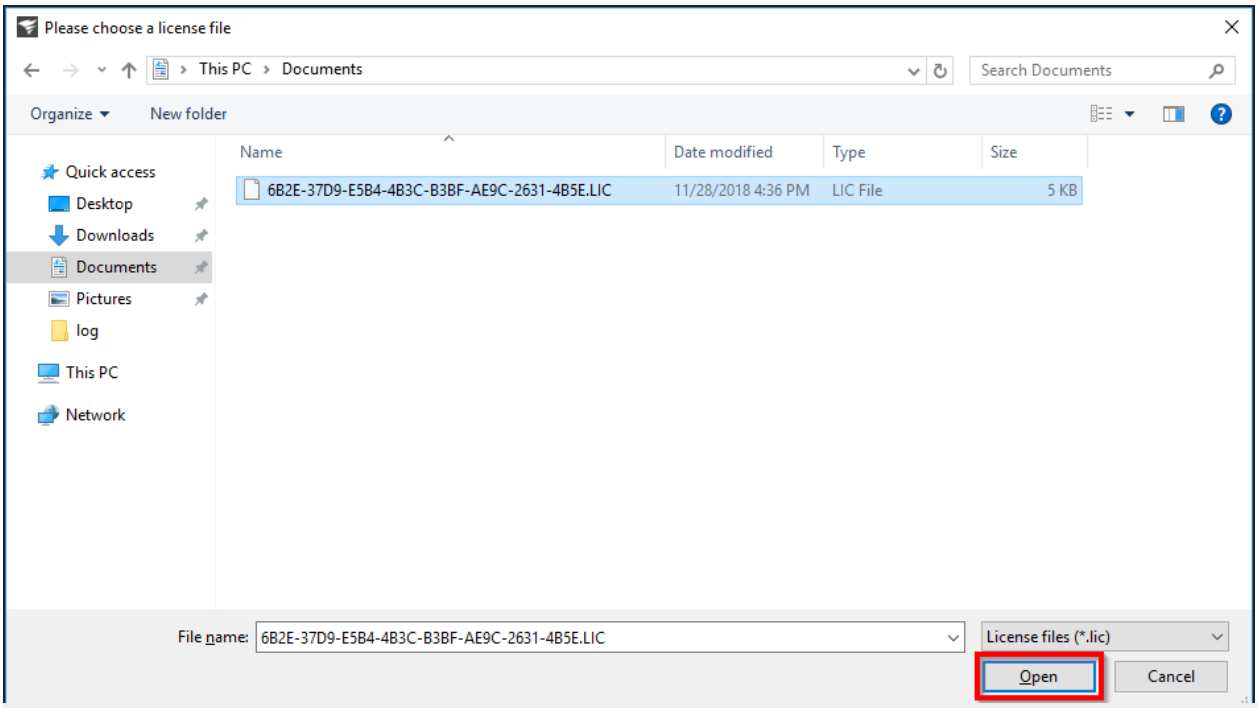
1. Click "Copy to clipboard".
2. Click "Next".



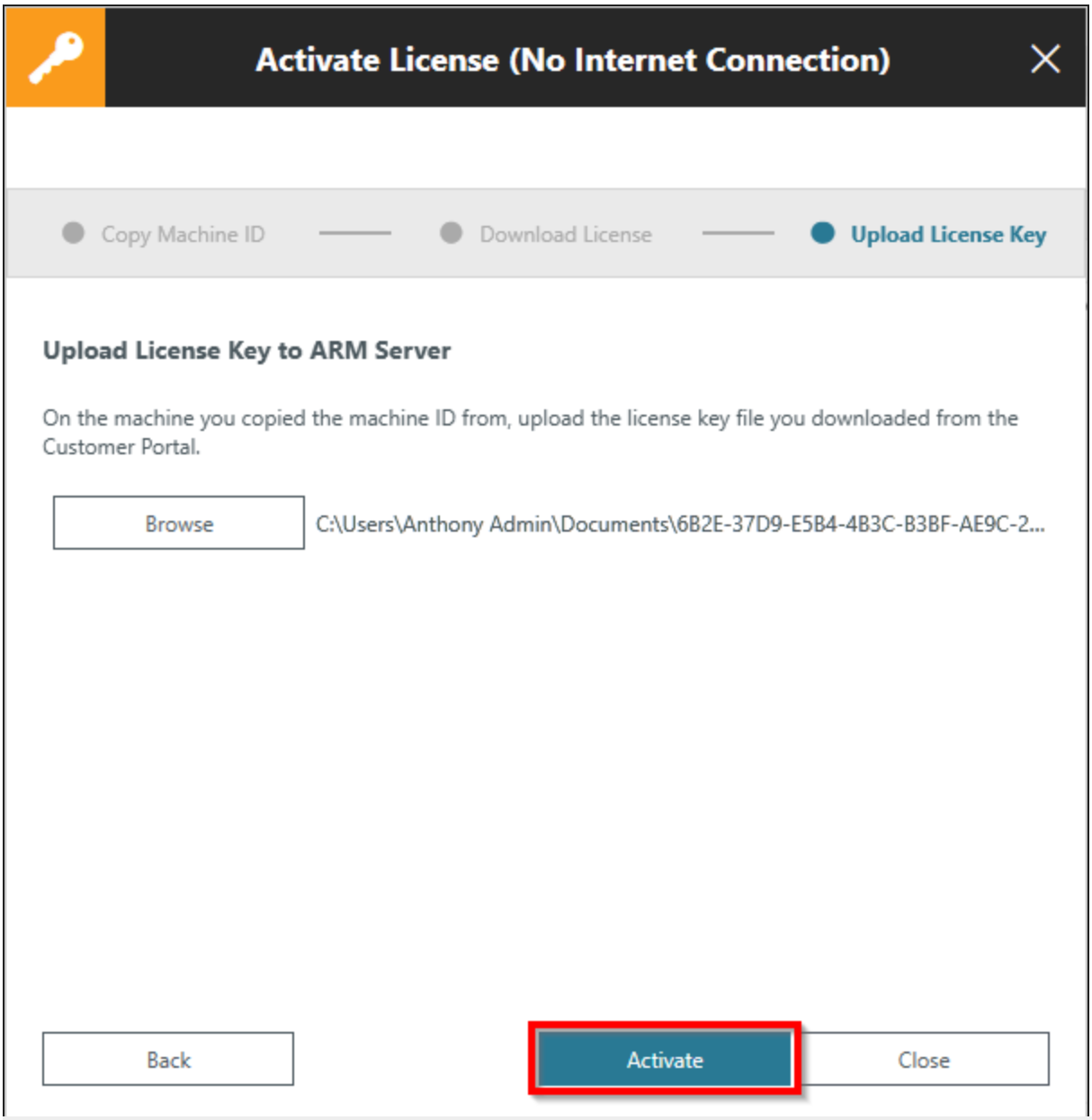
1. Follow the instructions on the screen.
2. Click "Next".



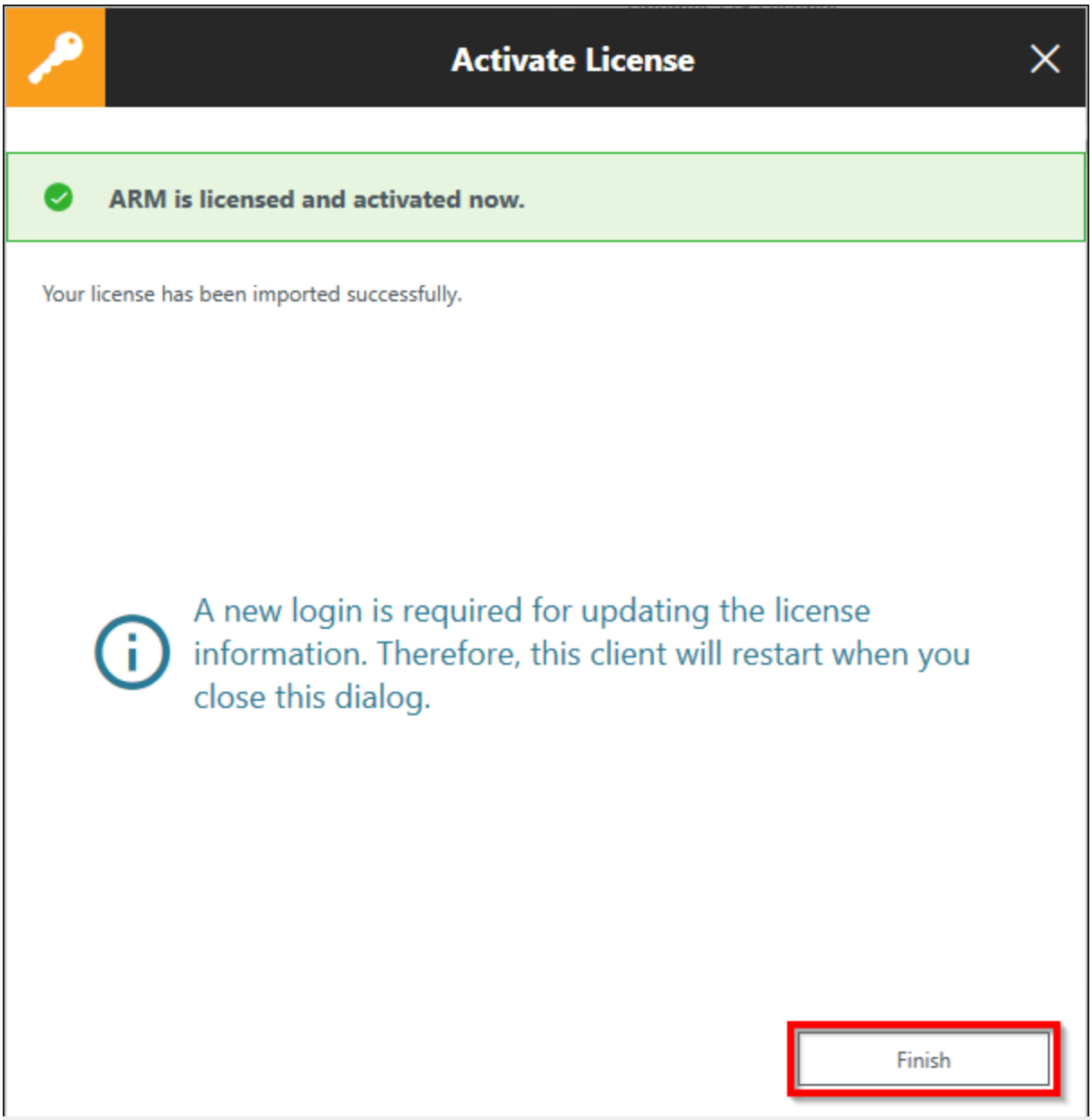
Click "Browse".



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



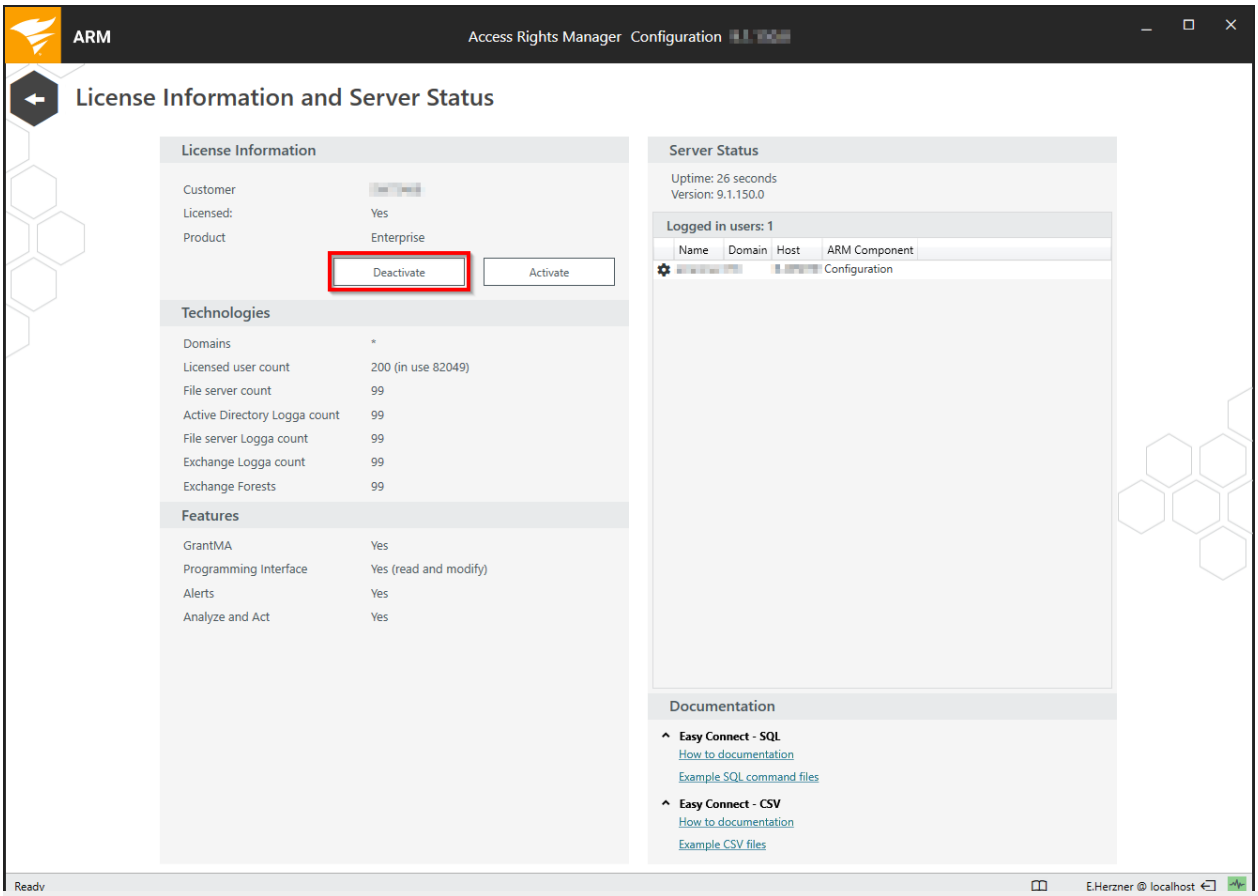
Click "Activate" to complete the license activation.



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.



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

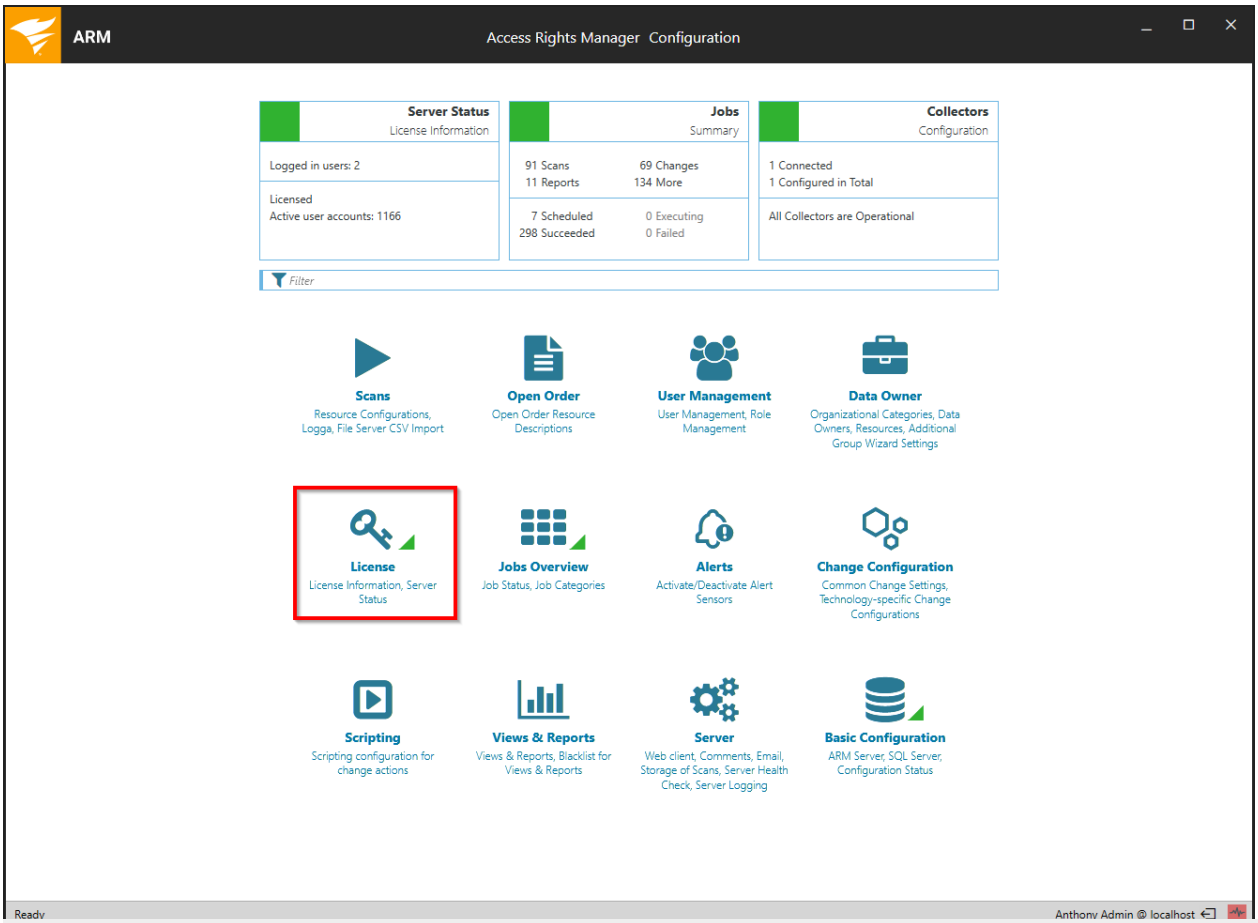
The activation is described in the topic Switch from an evaluation license to a production license.

Assign licenses to AD objects

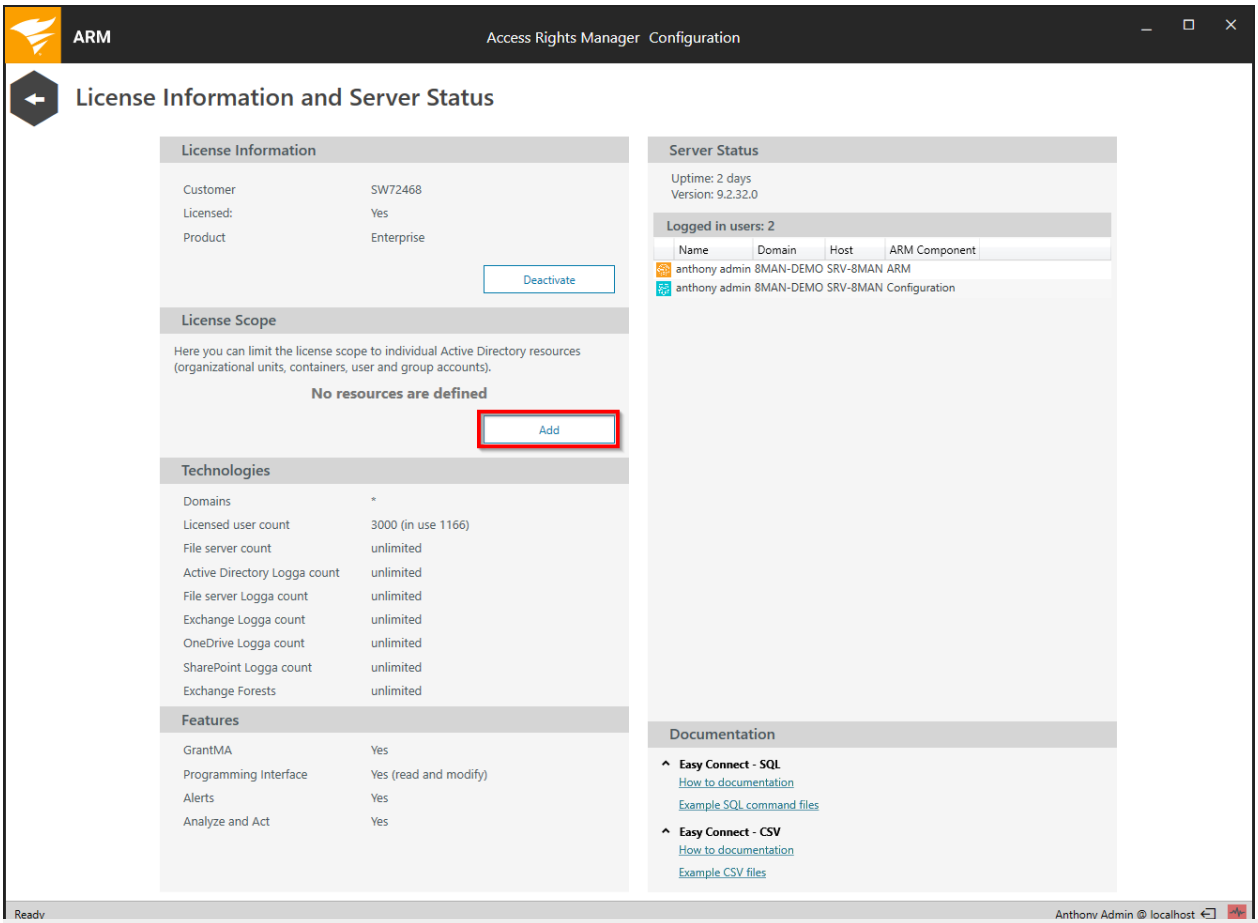
⚠ This chapter is only relevant to the SolarWinds licensing mechanism, not for the legacy 8MAN licensing.

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

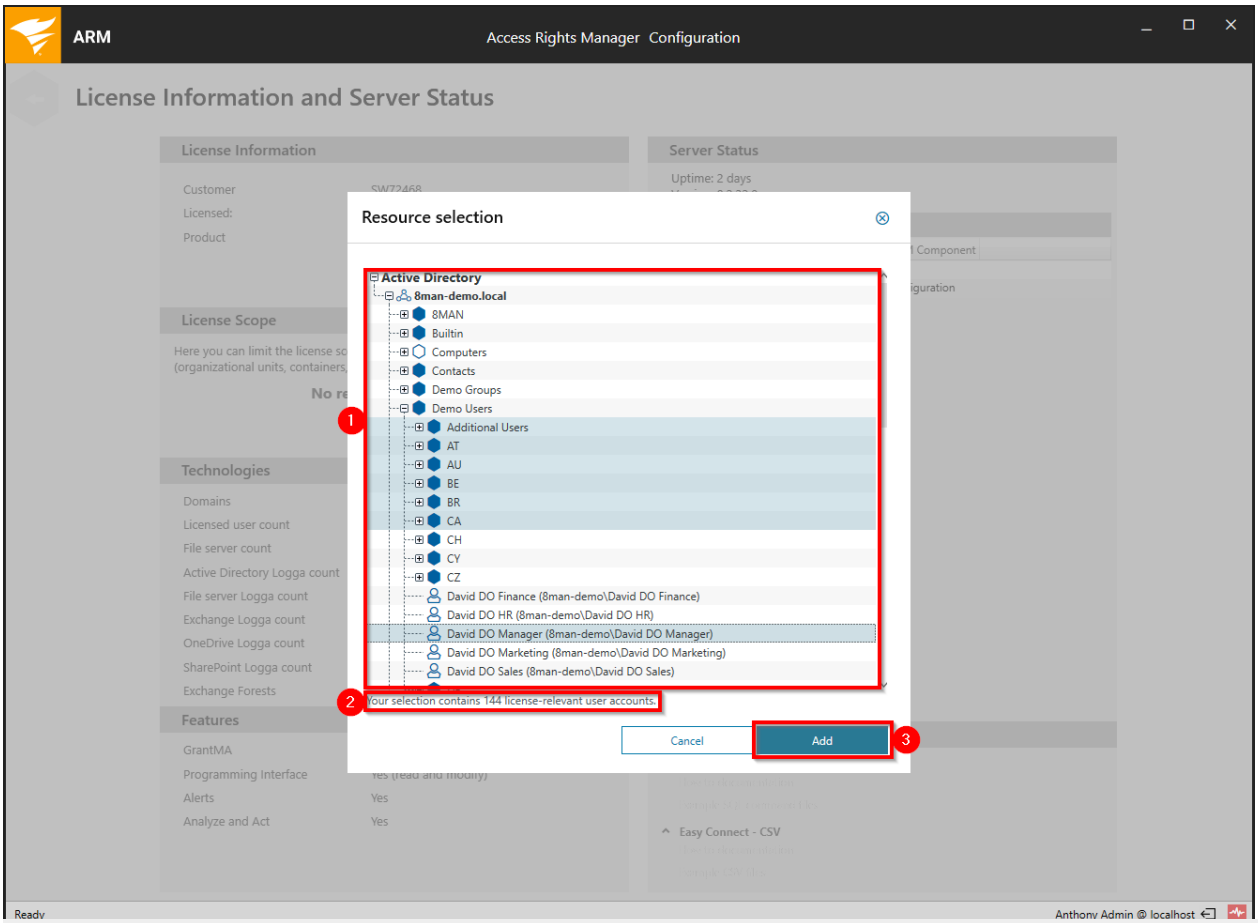
If you have a license coverage for all users in your domains, you do not need to make an assignment.



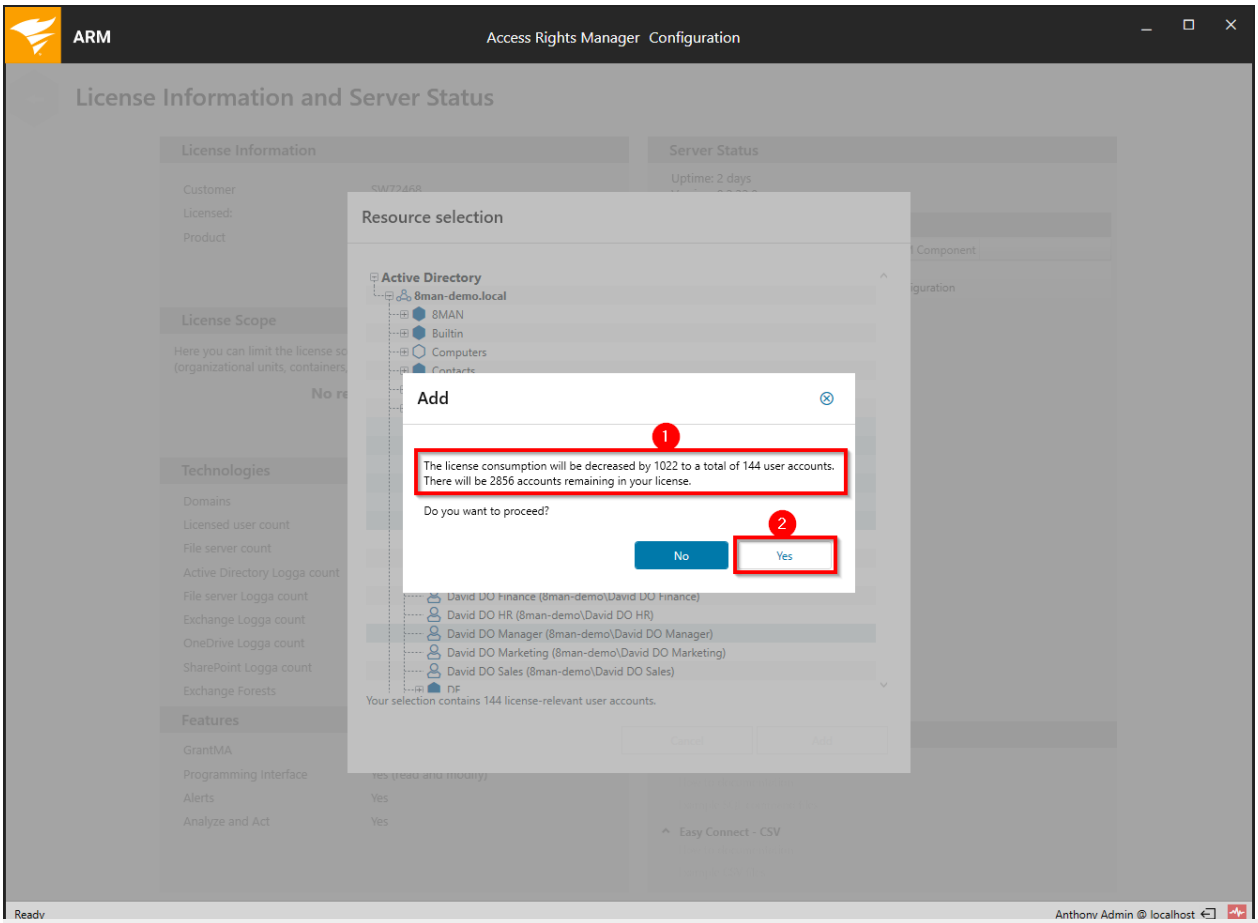
In the ARM configuration application click "License".



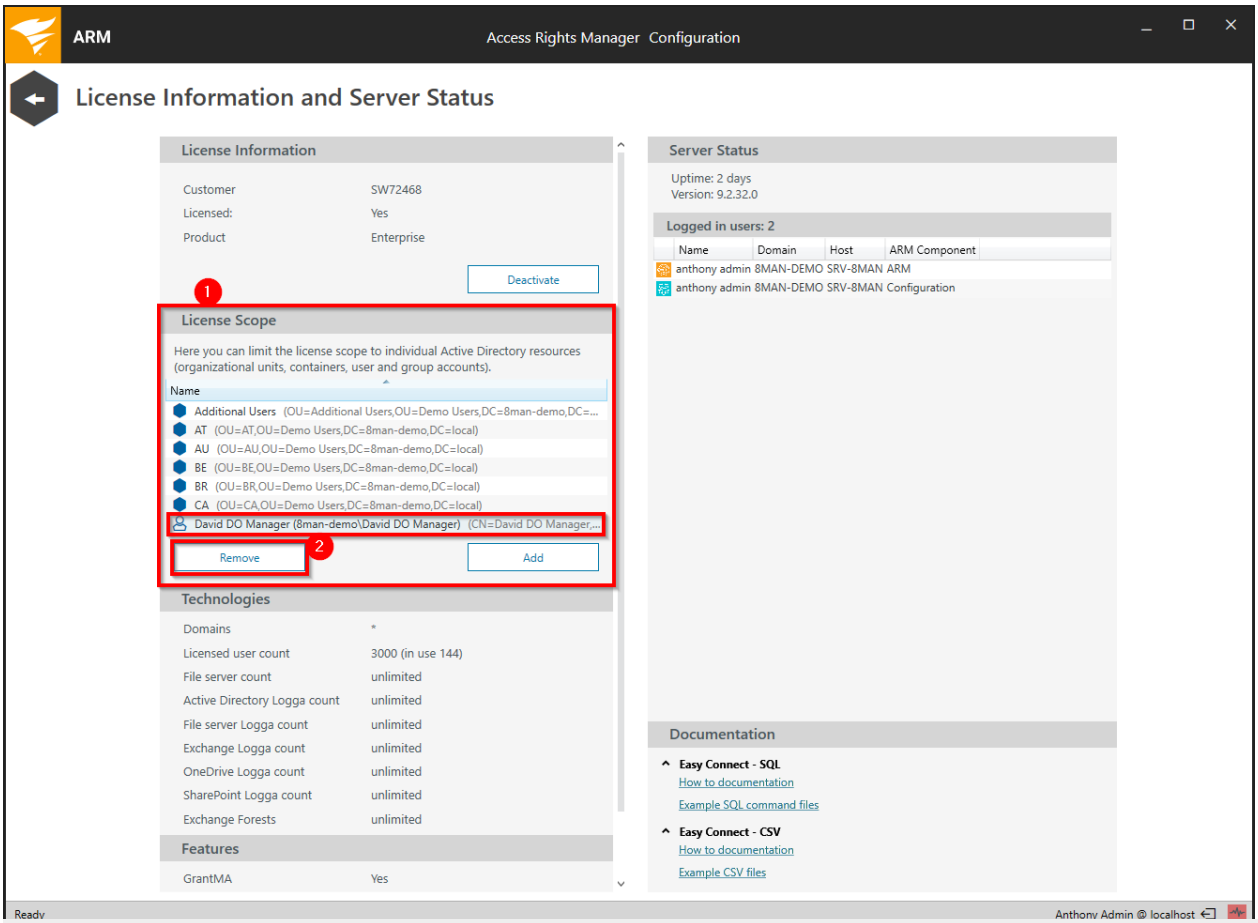
Under License Scope click "Add".



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".

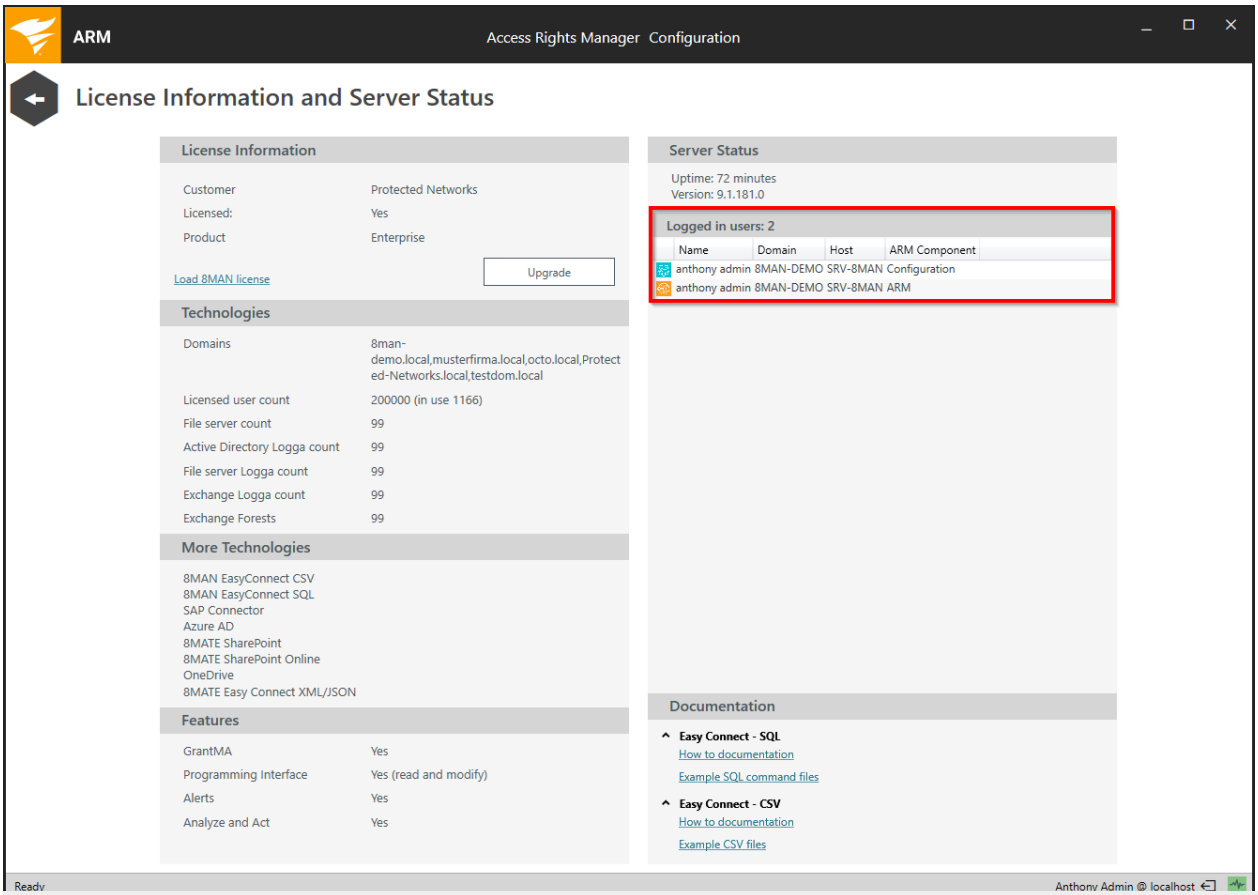


1. ARM shows you how many licenses will be assigned and how many will remain.
2. Click "Yes" to proceed.



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

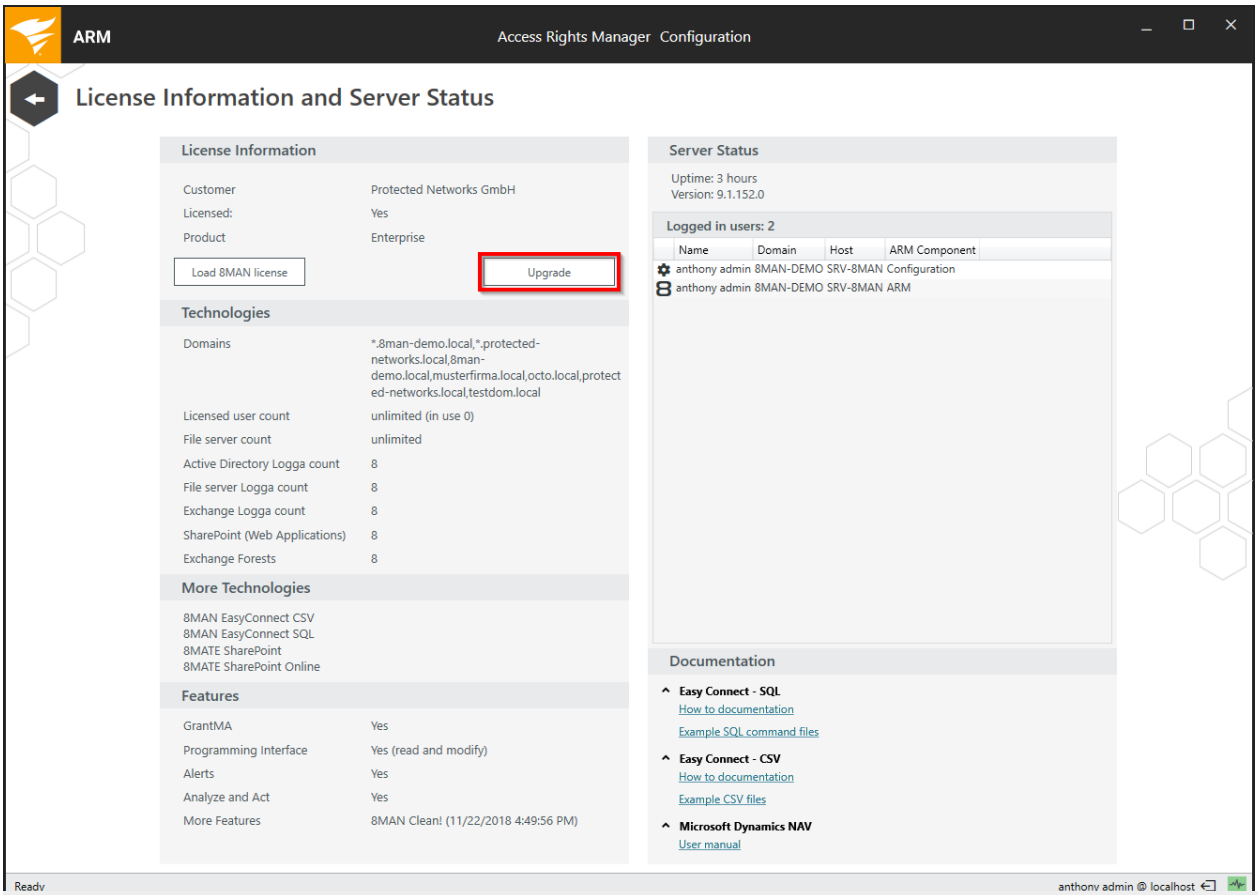
Identify logged in users



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

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

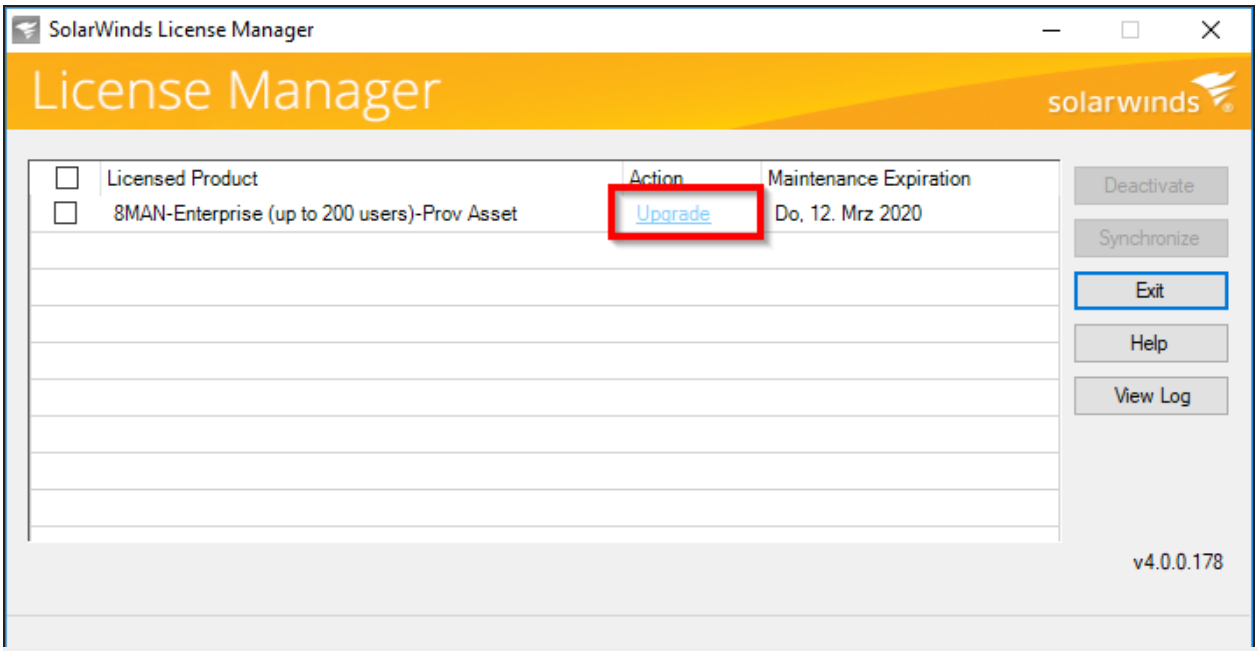


In the ARM configuration application under "License," click "Upgrade."

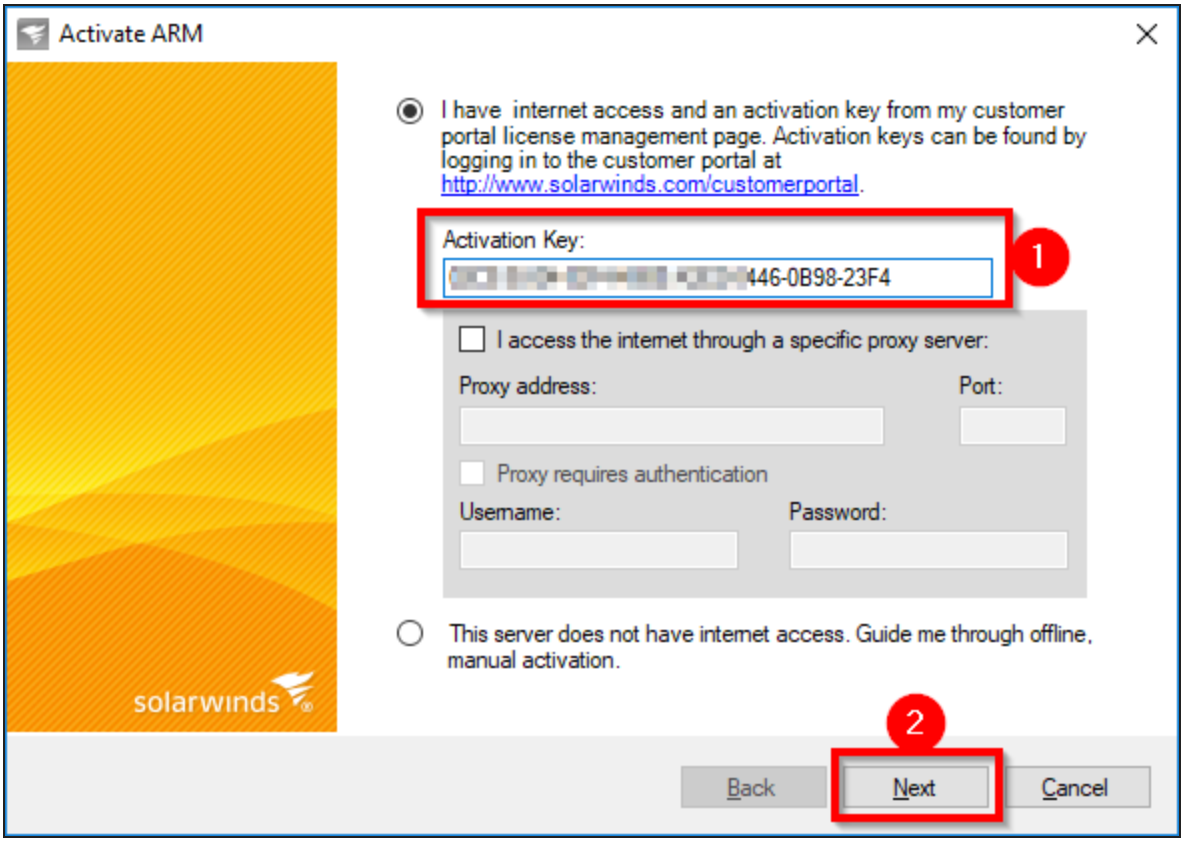
For the first license key use the same procedure as described in the chapter Switch from an evaluation license to a production license.

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.

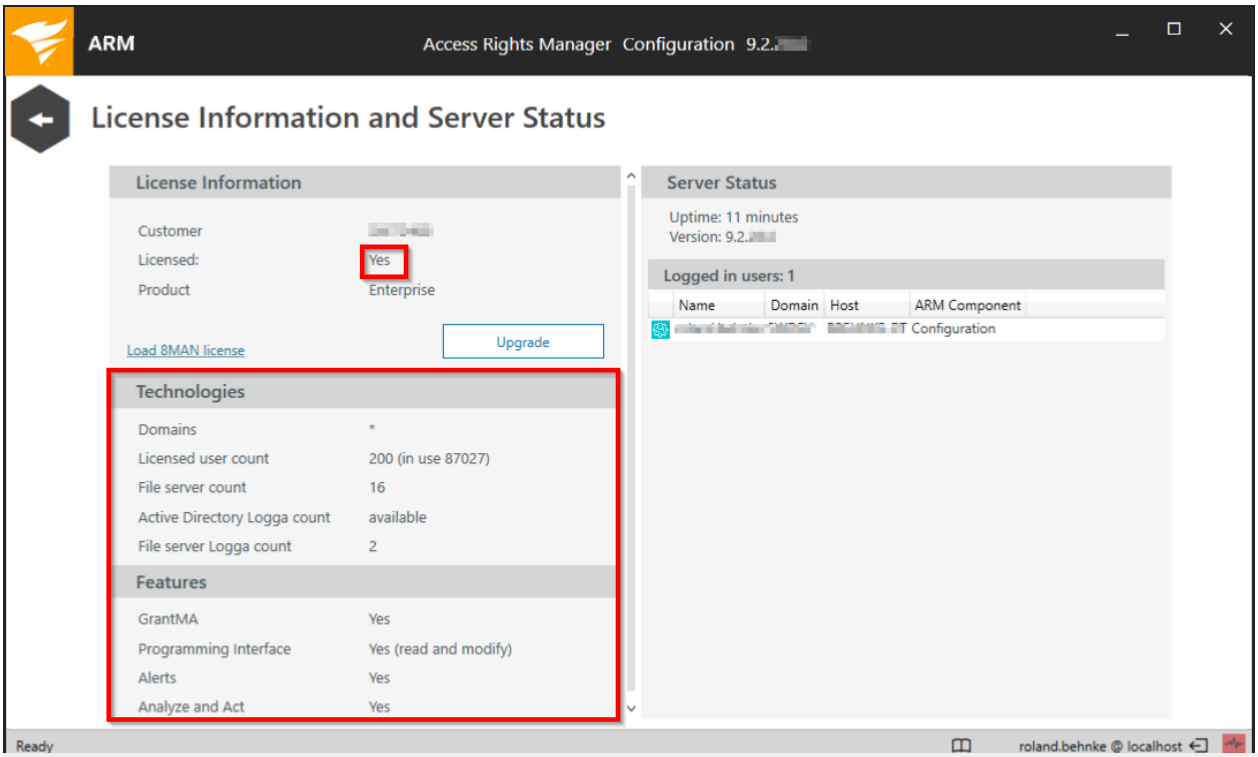


Click "Upgrade".



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

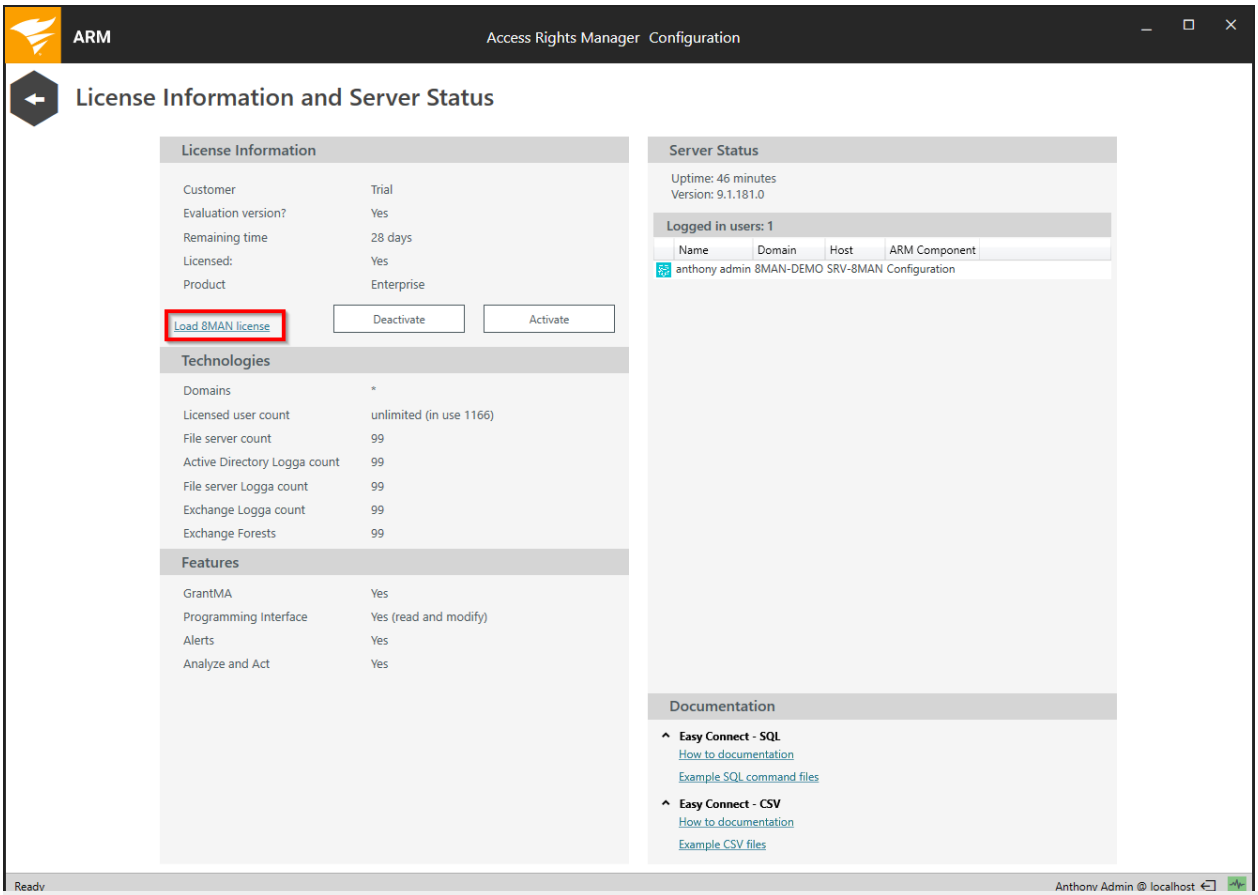
Repeat the steps until all your license keys are activated.



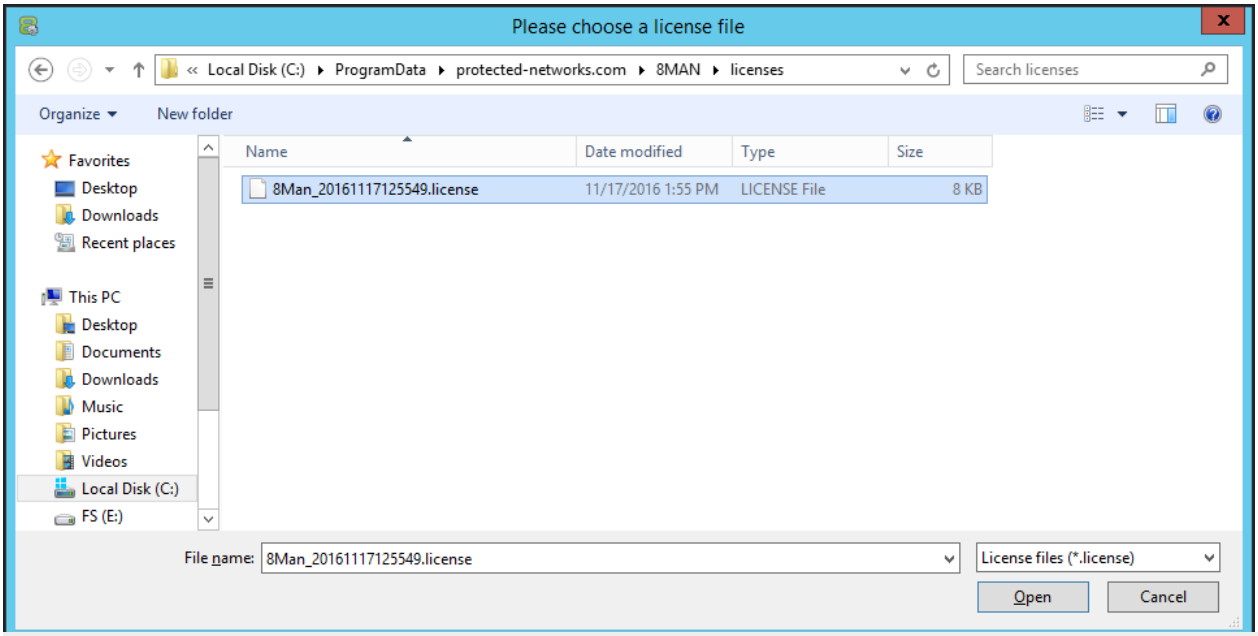
Double check under "Features" and "Technologies" all your licensed features.

Load the license file and check covered features

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



Click "Load 8MAN license".

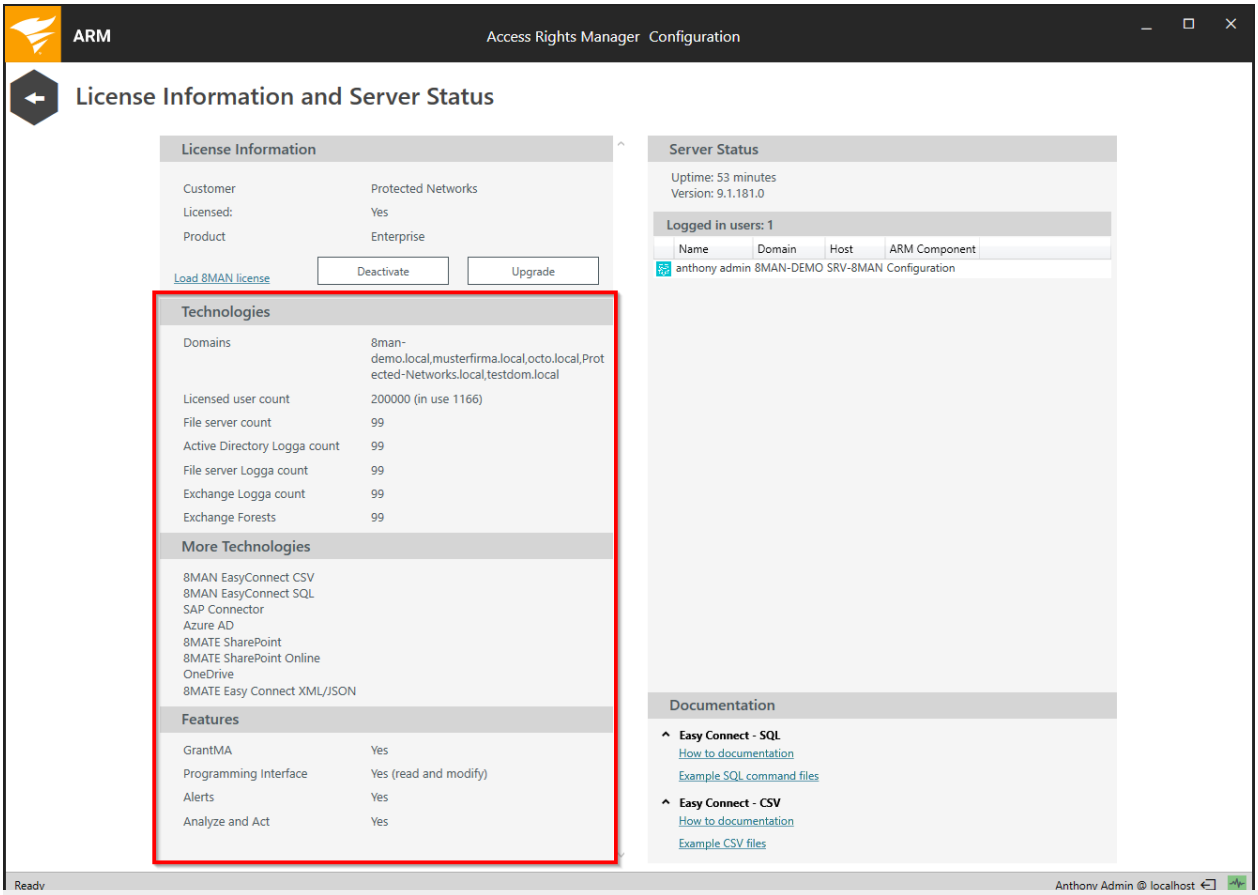


Select the path where your license key is stored. 8MAN license files have the file extension ".license".

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

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

All licensed features are activated immediately.



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

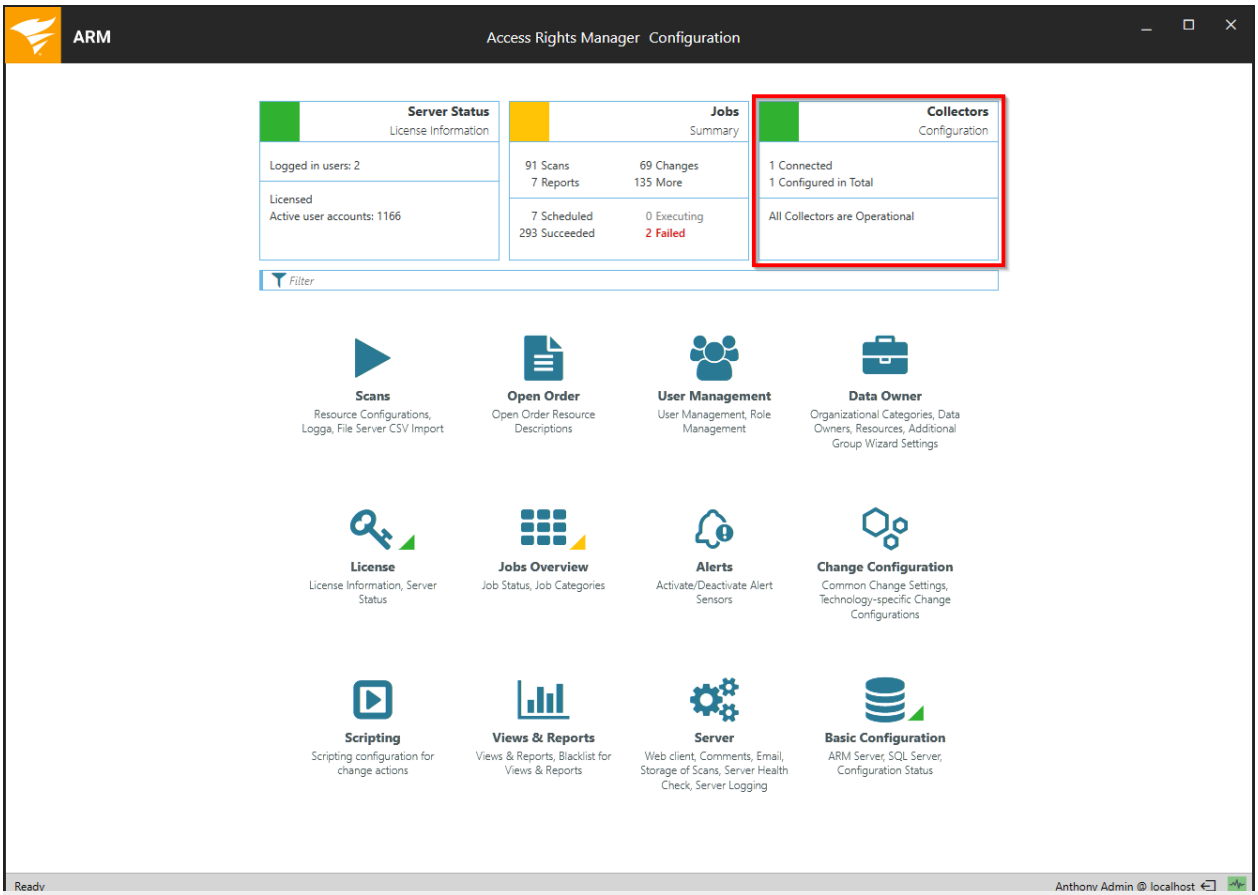
Collectors

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

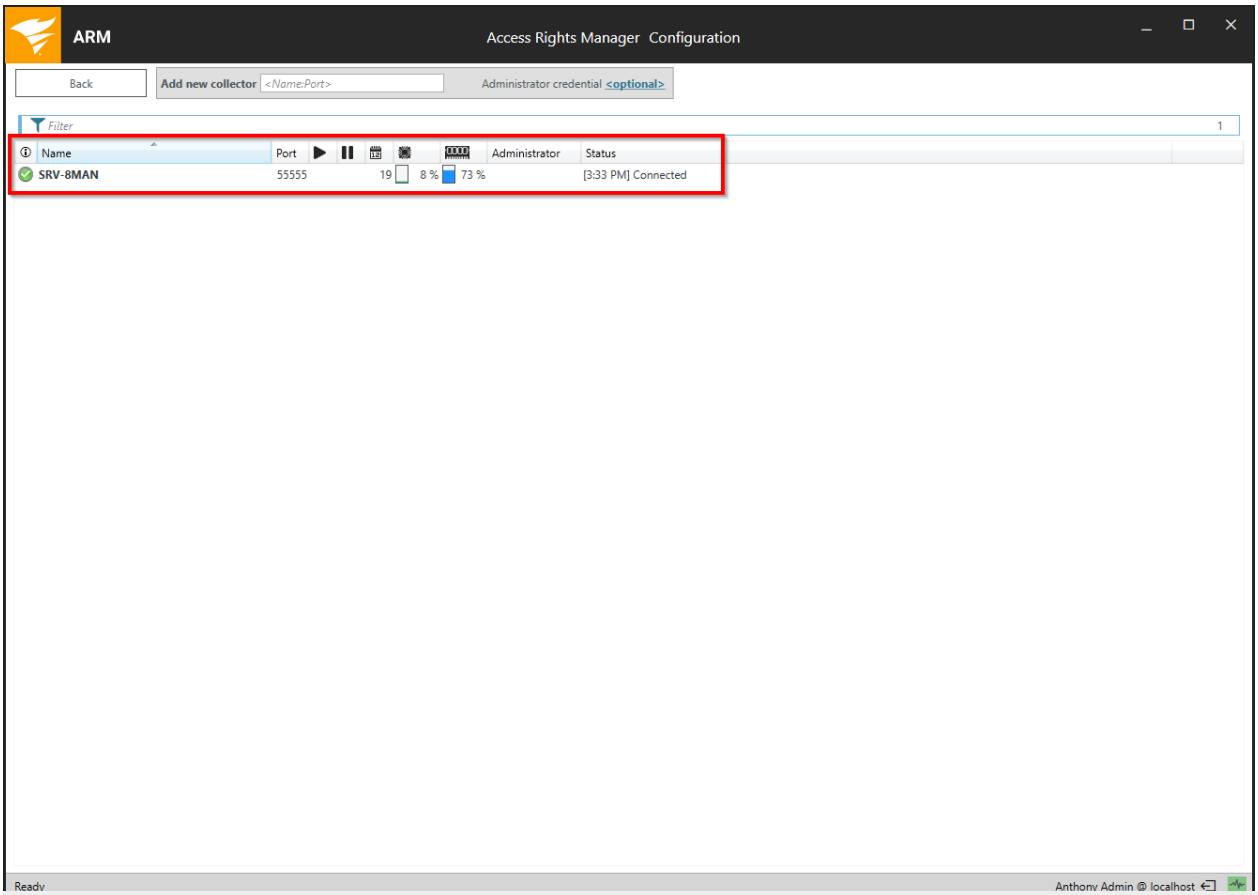
Additional collectors may be installed for the following reasons:

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.

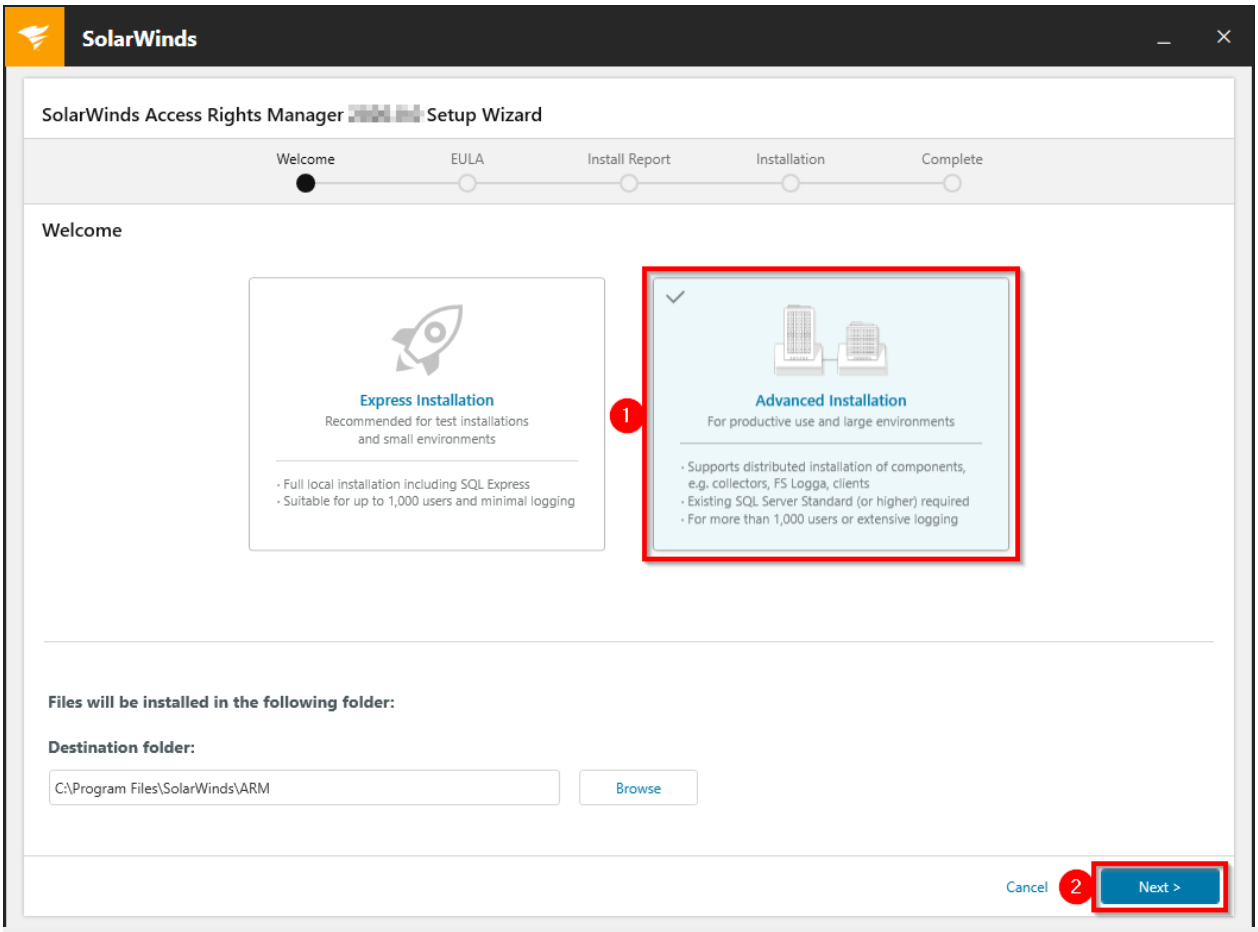
If you are having problems with the connection please see Firewall settings.

Install additional collectors

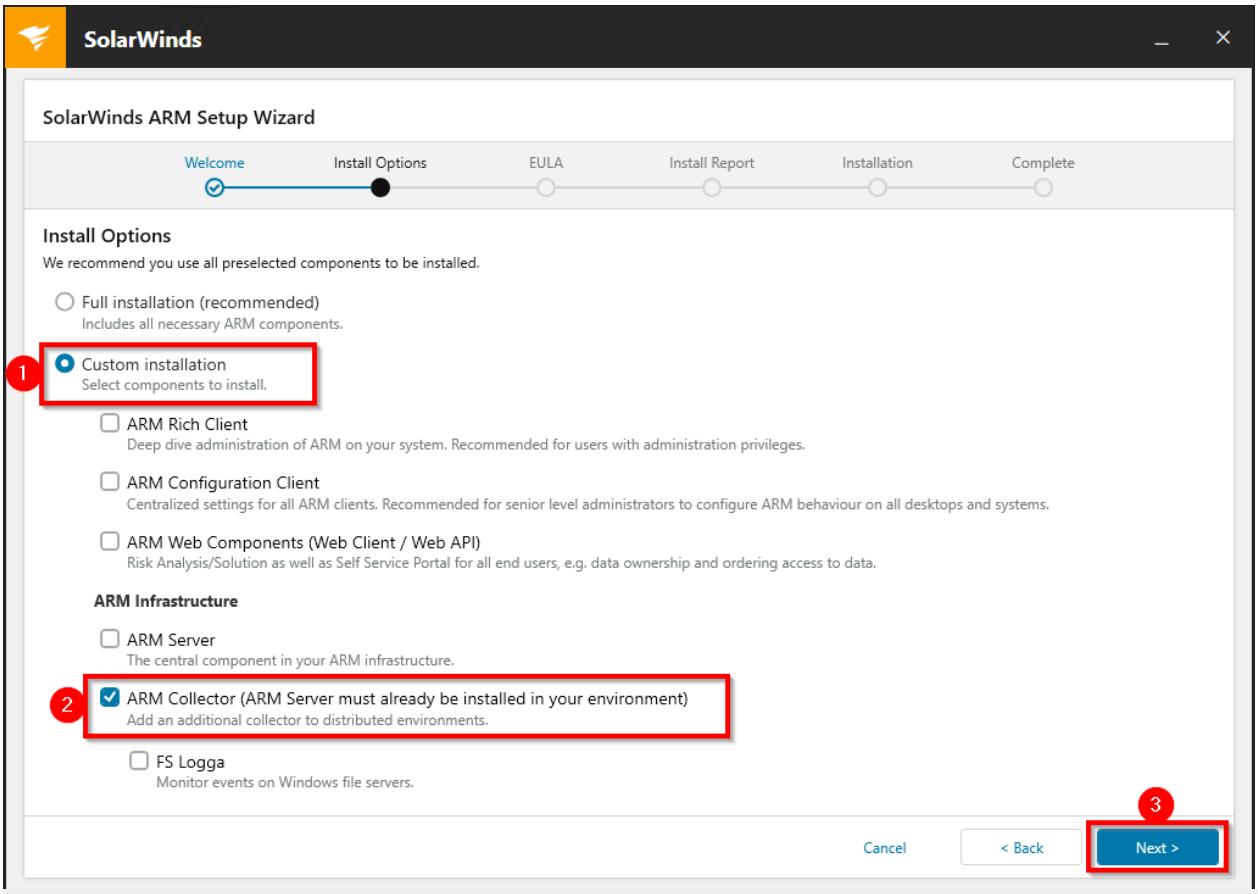
Add collectors using setup

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.



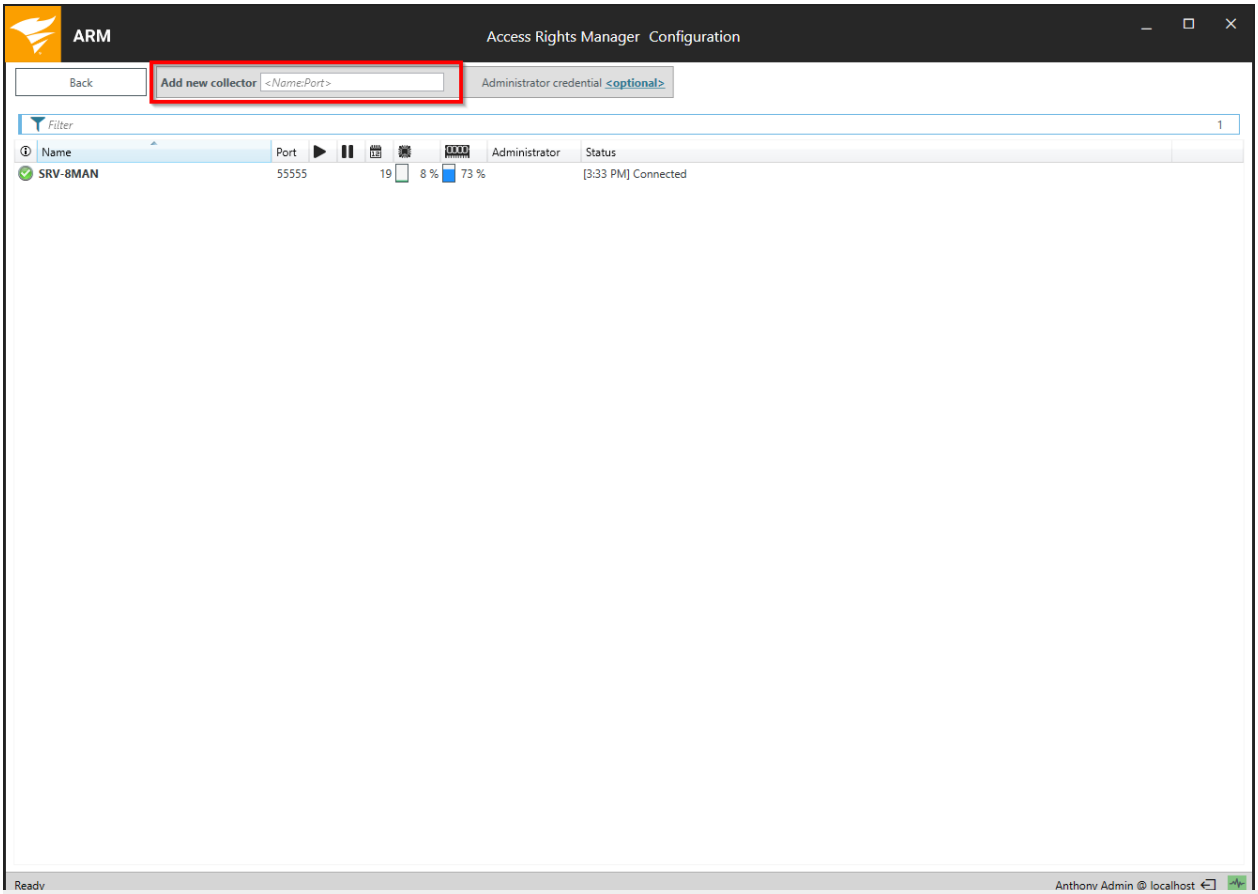
1. On the welcome page select production installation.
2. Click Next.



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

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

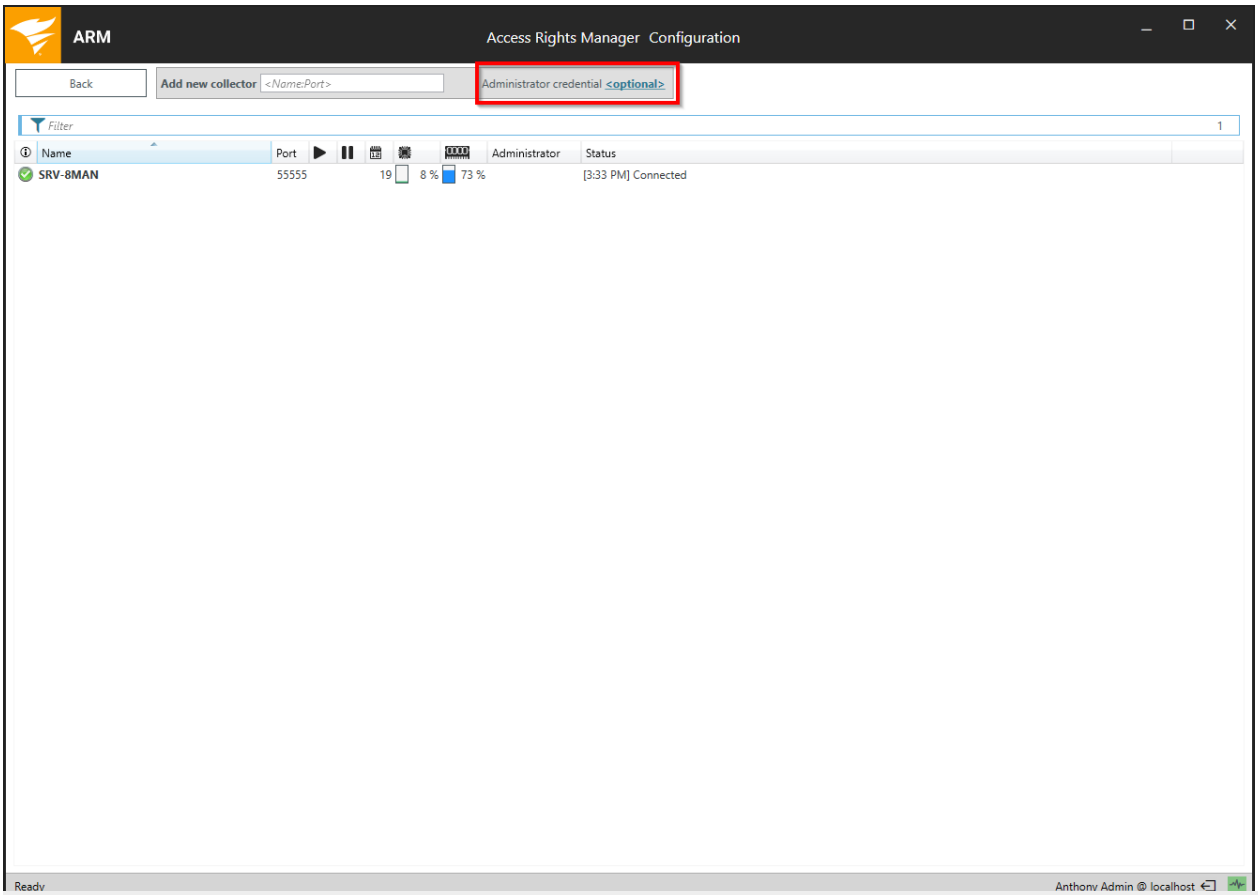


Enter the name of the desired server. Enter a port number after the name, if you don't use the default port "55555".

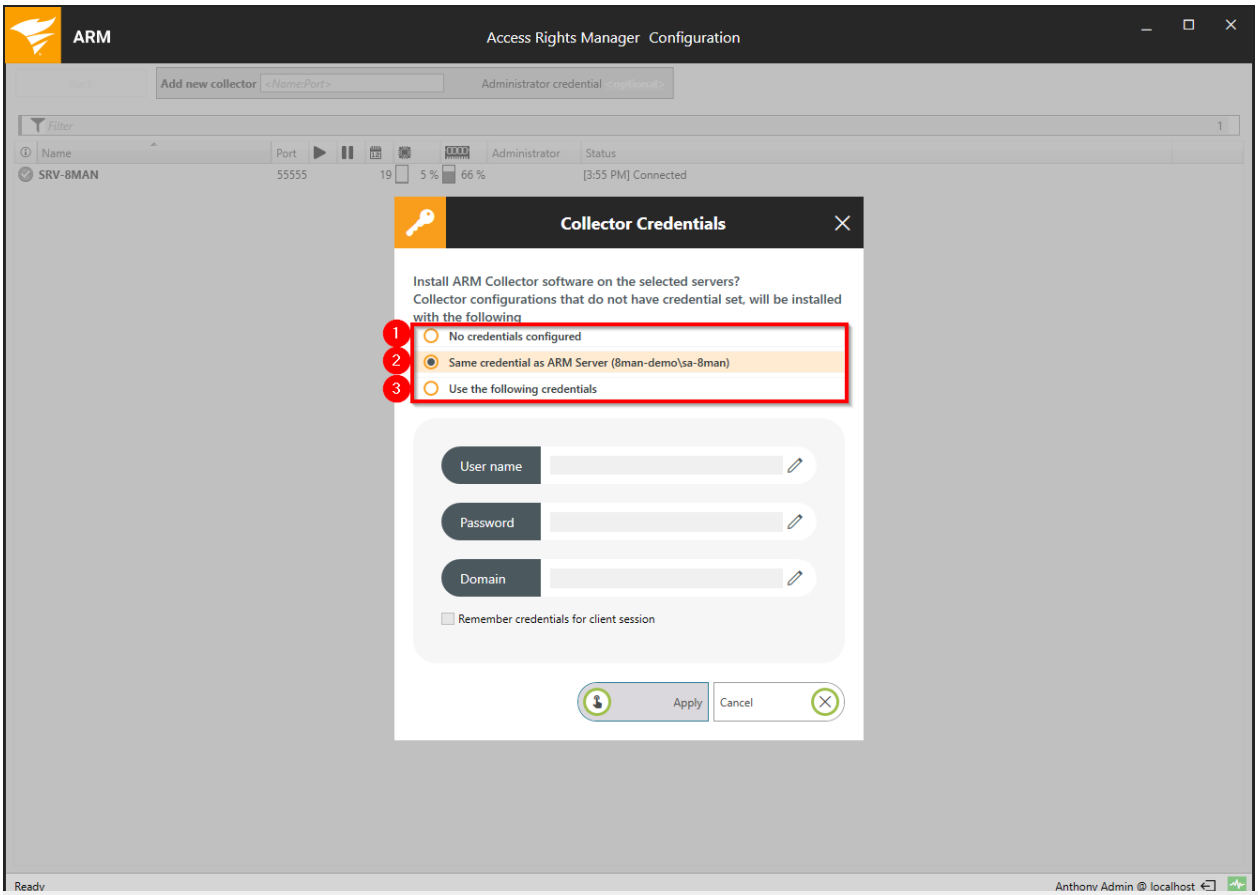
If the target system already has a collector installed, it will be added to a lists of collectors and establish a connection. You do not need to enter any login credentials.

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

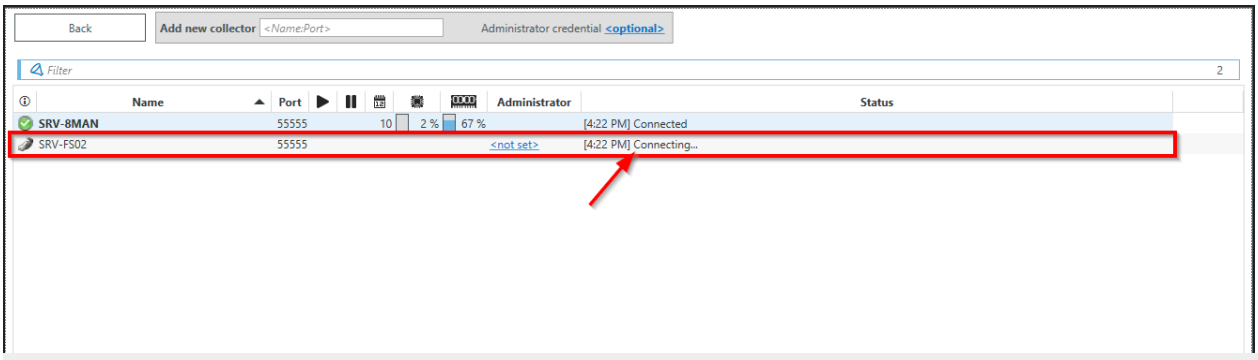
If you are having connection problems please see: Firewall settings.



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.

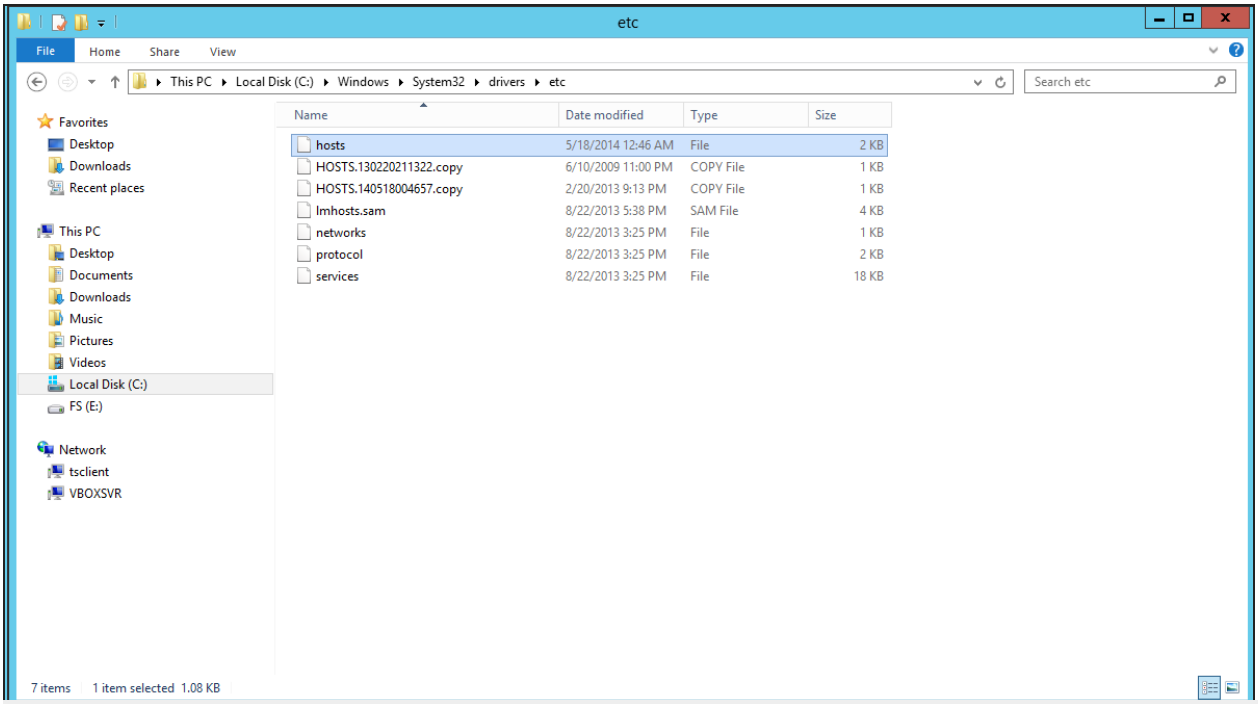
Up to 2 collectors are updated simultaneously.

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.

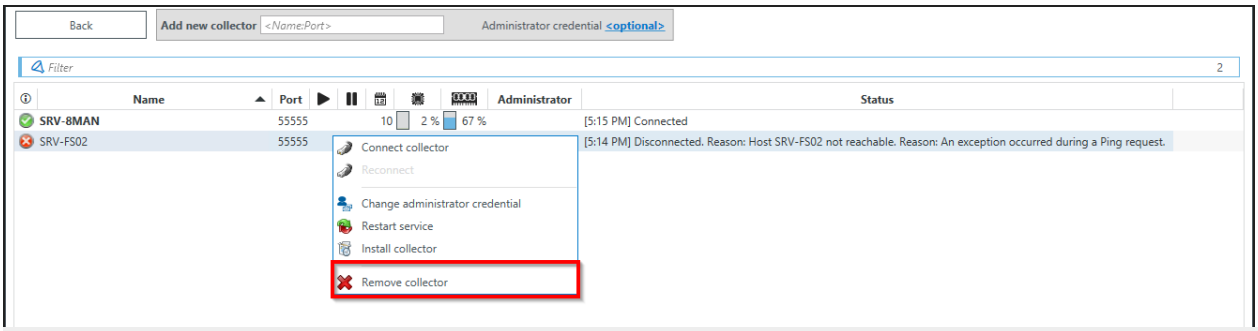
Depending on your network configuration, the automatic update mechanism for collectors may not work. In such cases the installation of this collector must be performed manually by using the setup, as described in Install additional collectors.

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

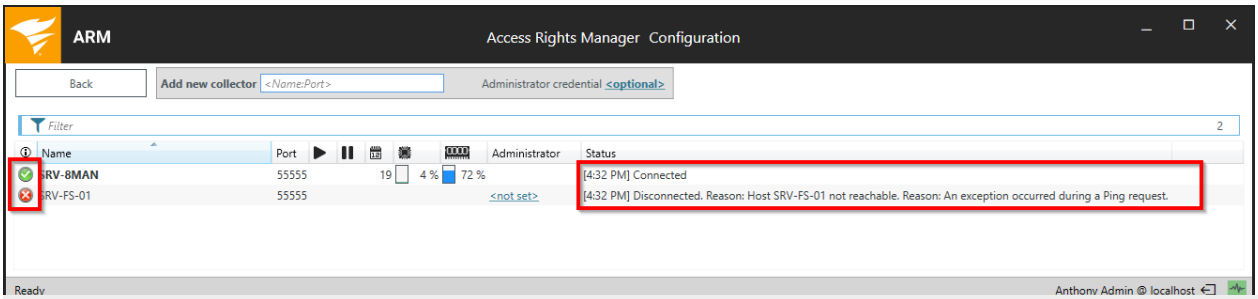


You can remove a collector by right-clicking on it and selecting "Remove collector" from the context menu.

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.

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:

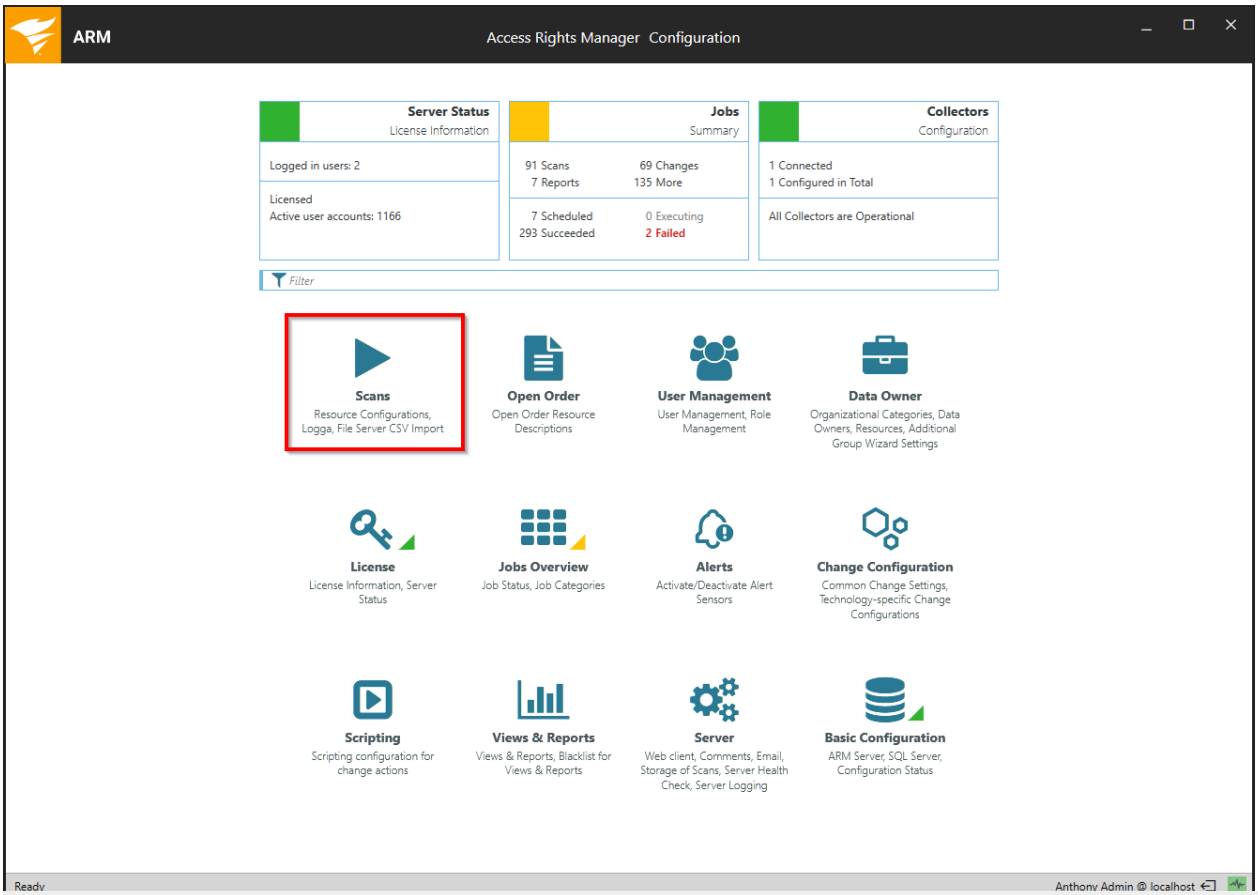
You will receive a message starting with ".Net..." and further containing "...expacting preamble...". This error message is generated by the ARM service.

⚠ 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 date base.

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

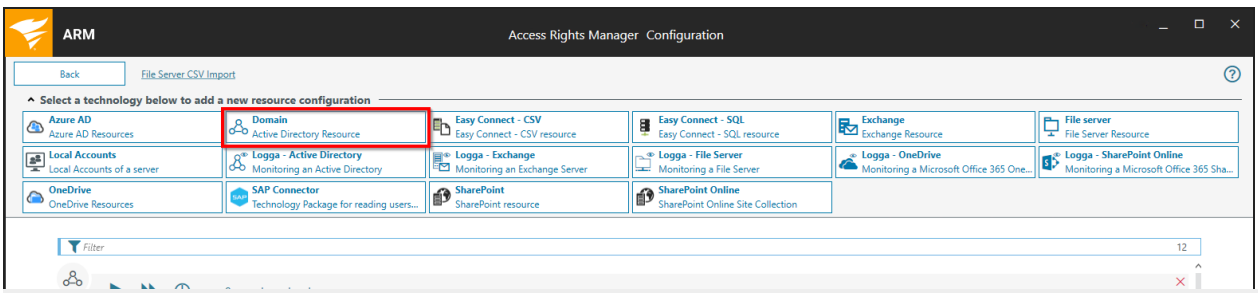


Click on "Scans" to configure resource scans and Logga settings.

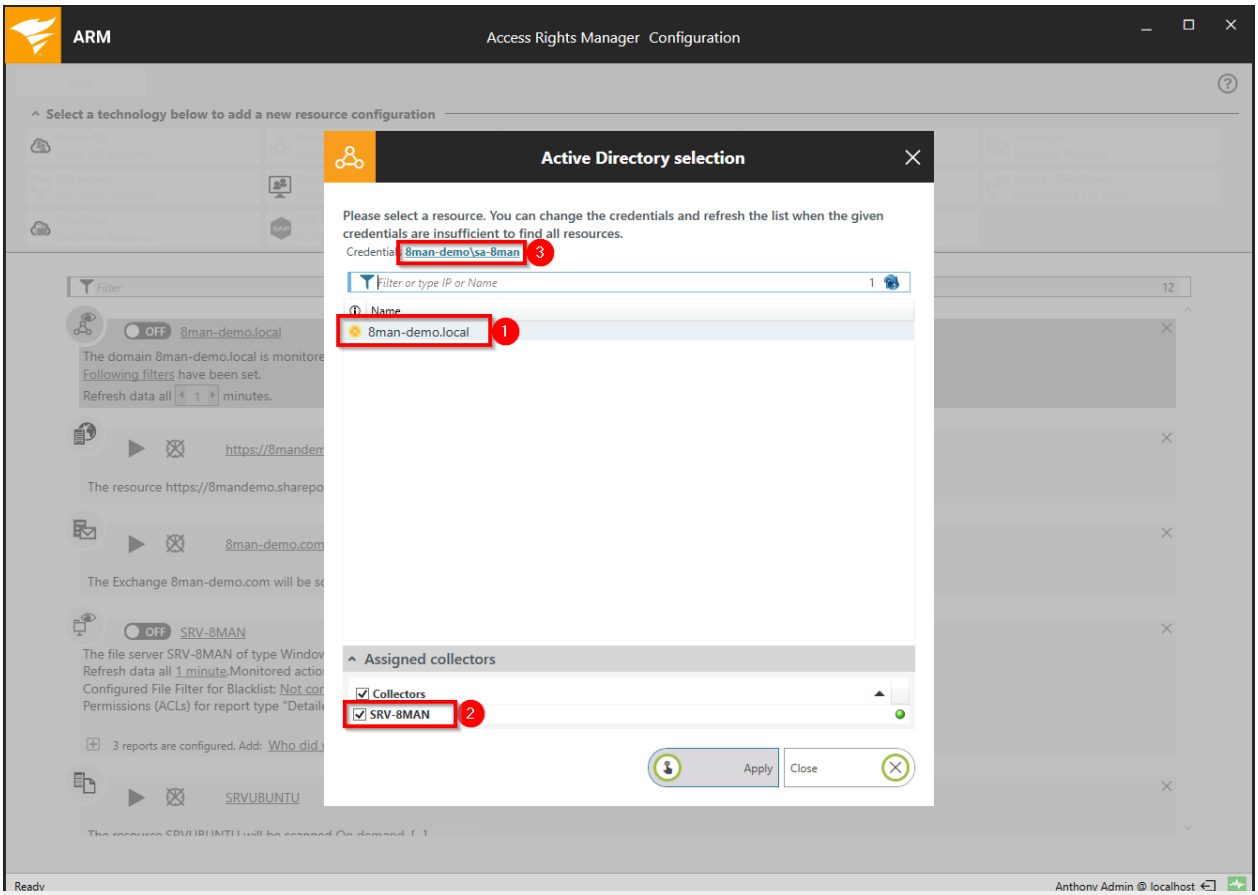
Active Directory (AD) scans

Add AD scans

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



Click on Domain to add an AD scan.

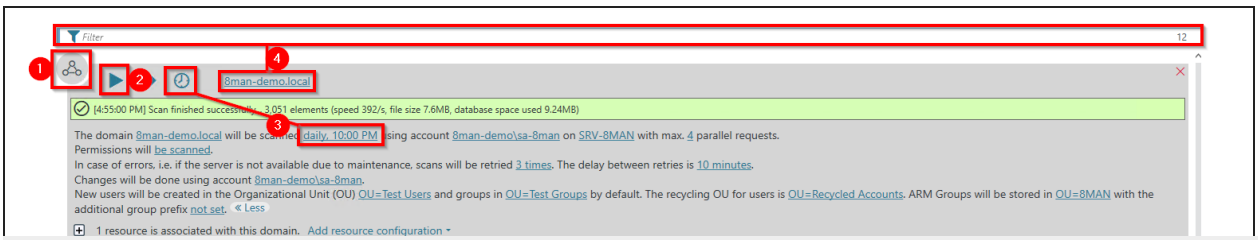


1. Select the desired domain for the AD scan.
2. Select a collector for the AD scan.
3. By default the credentials from the ARM server basic configuration will be used. You can specify different credentials.

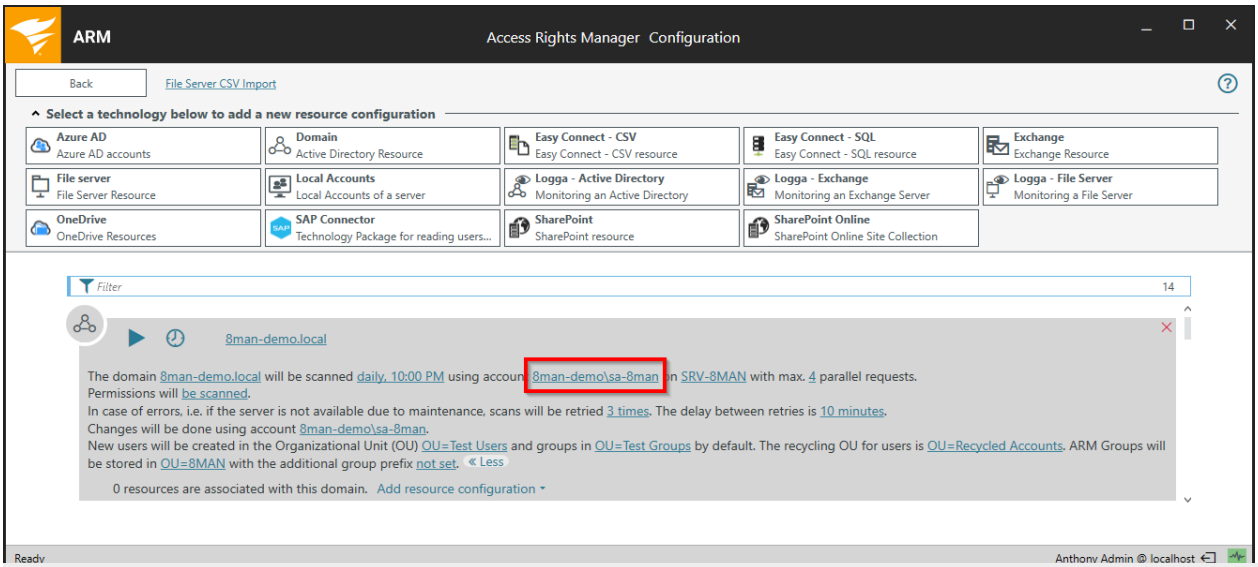
If the desired domain is not shown please check the following:

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

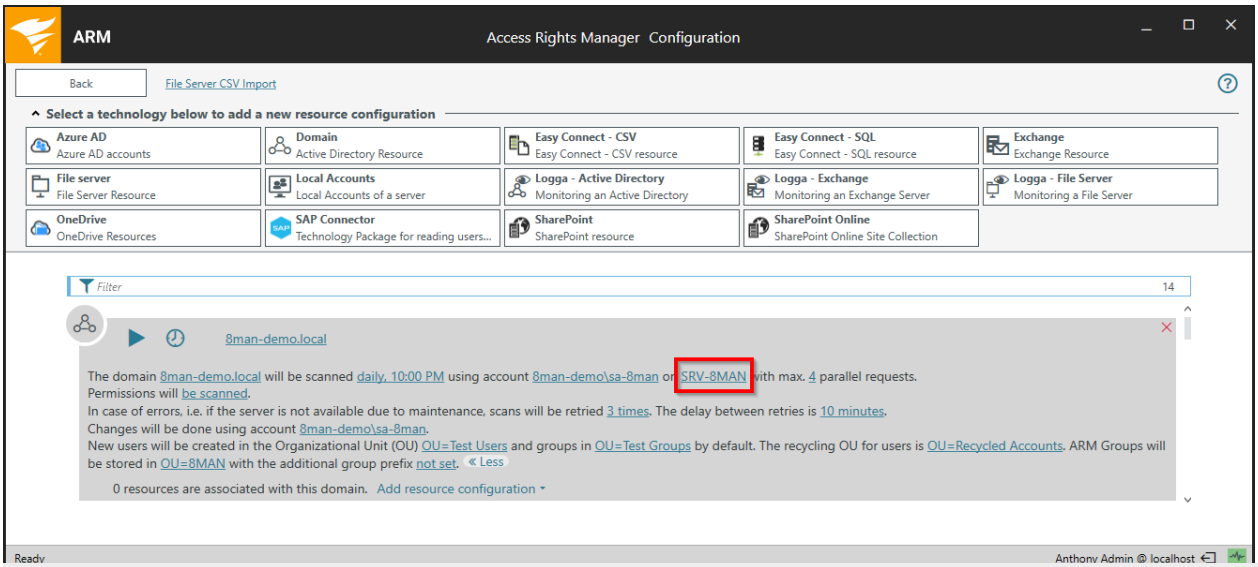


1. This icon is used for easy recognition of an AD scan configuration.
2. Sart/Stop an AD scan. During and after a scan you can find information on the progress and the success of a scan in the light green box. Saved information about the scans of the last 14 days can be found in the Job overview.
3. 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.



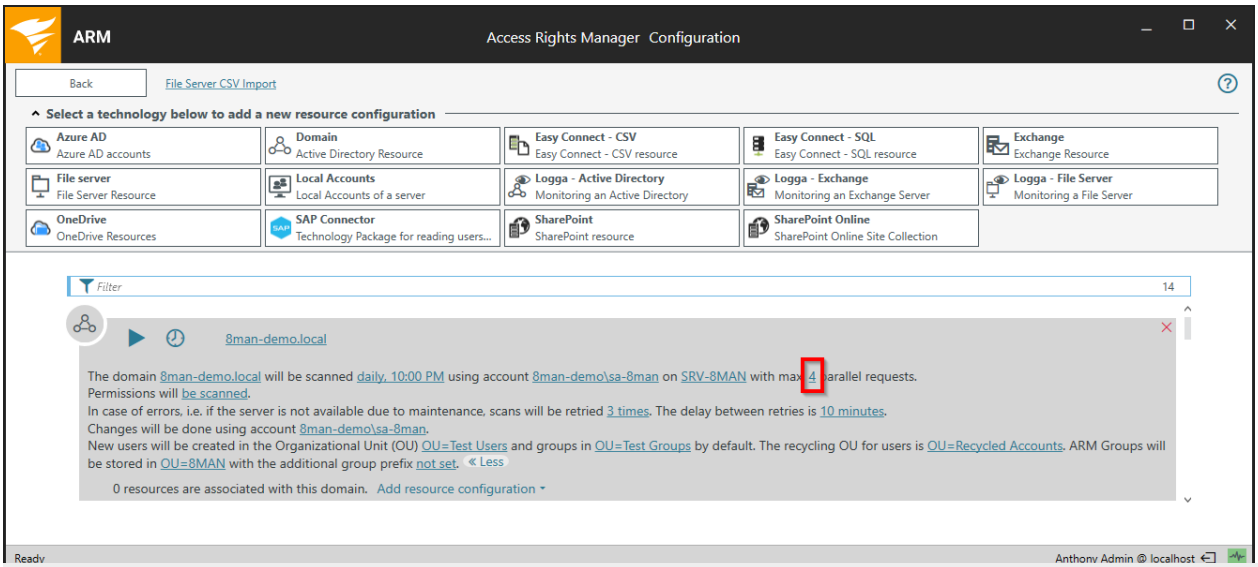
Specify the credentials that will be used to perform the AD scan.

Follow our recommendation for using service accounts.



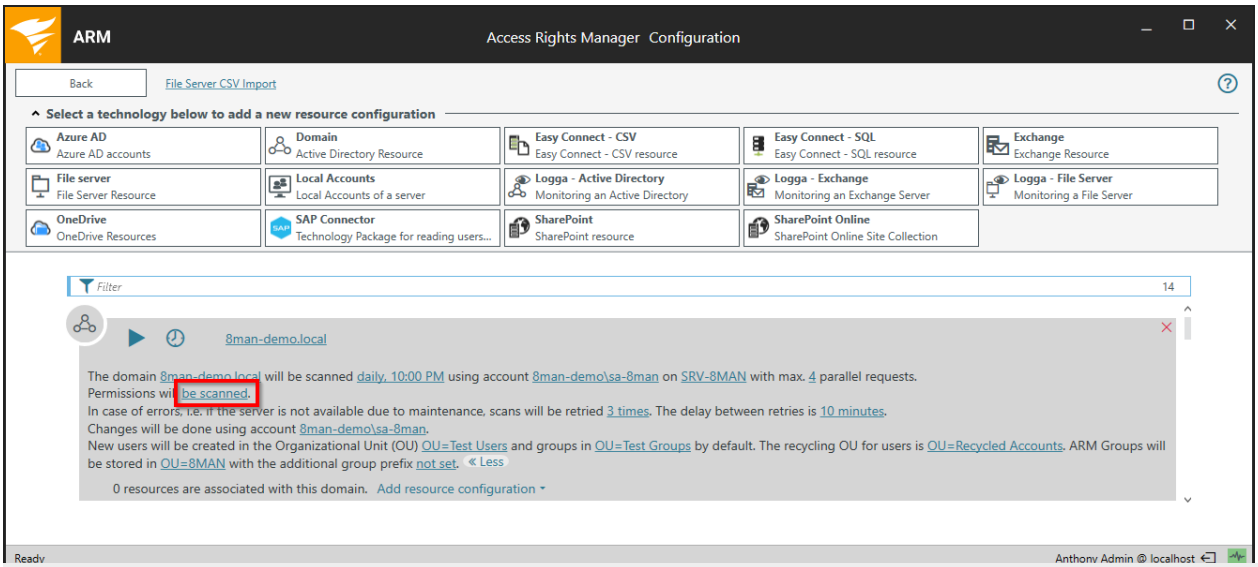
Determine which collector performs the scan.

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



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

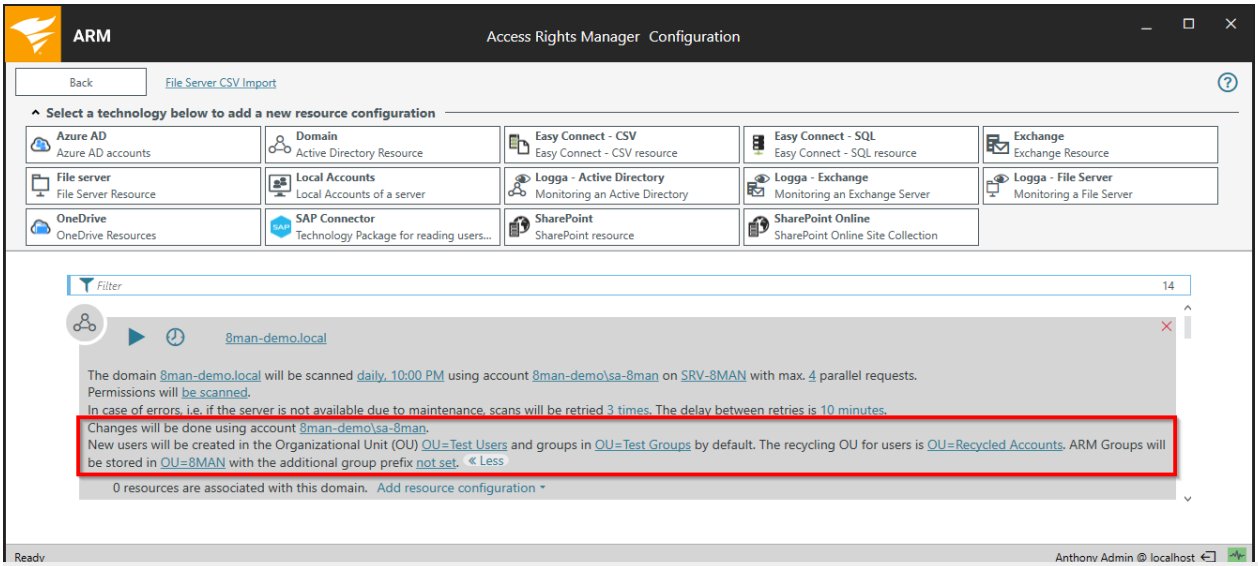
Possible values are 1 (no parallel requests) to 128.



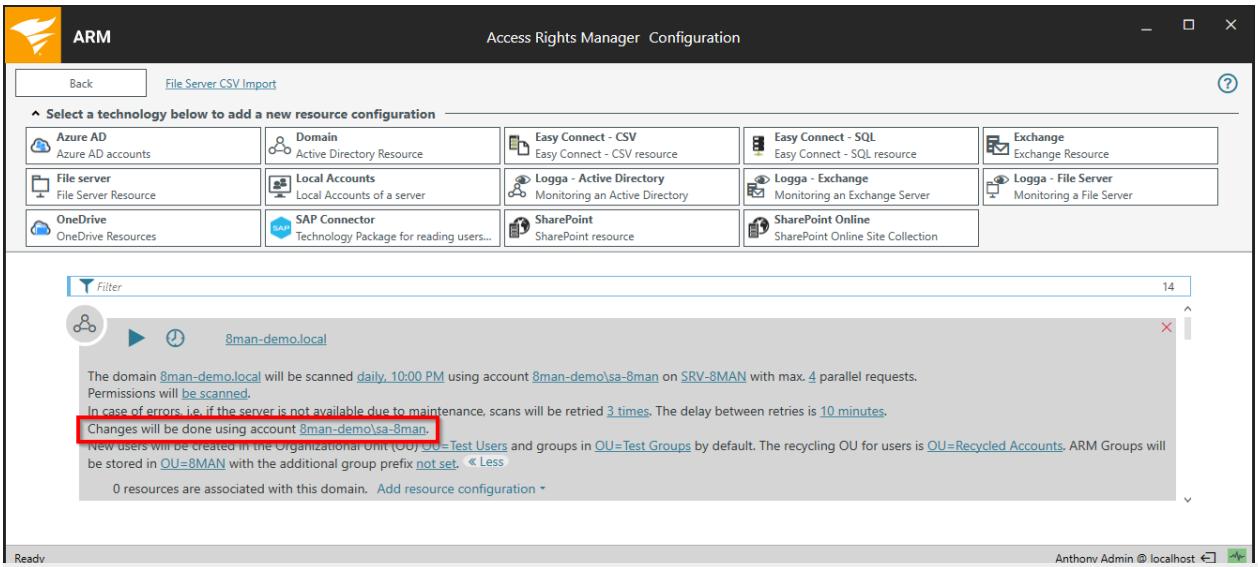
Specify for which Active Directory object classes the permissions are read.

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

AD change configuration



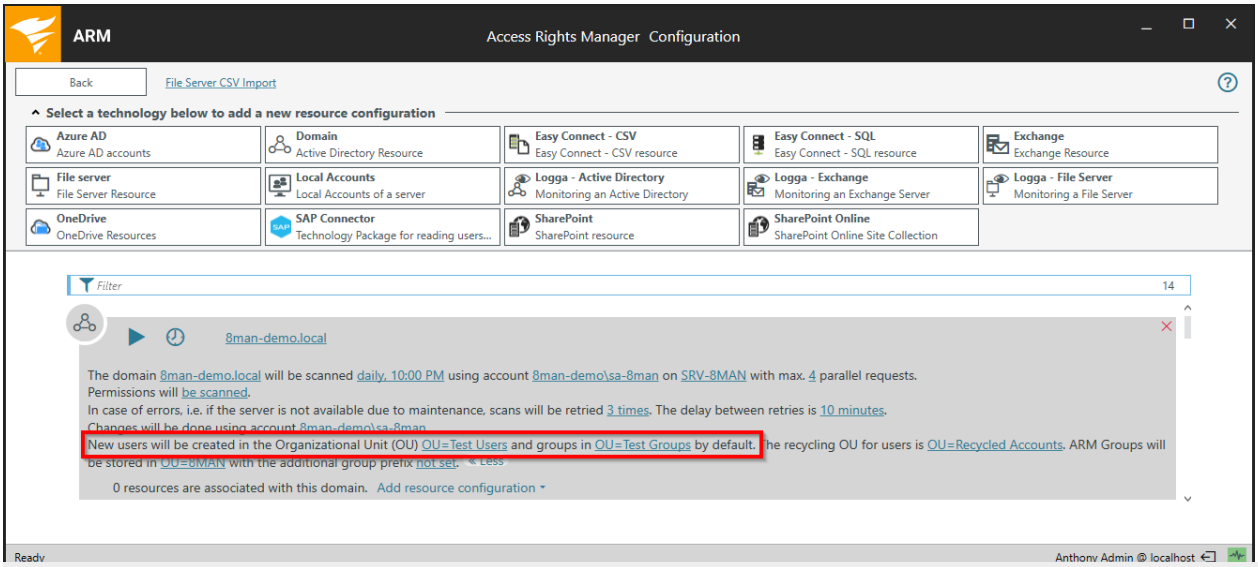
The marked area shows the AD change configuration.



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

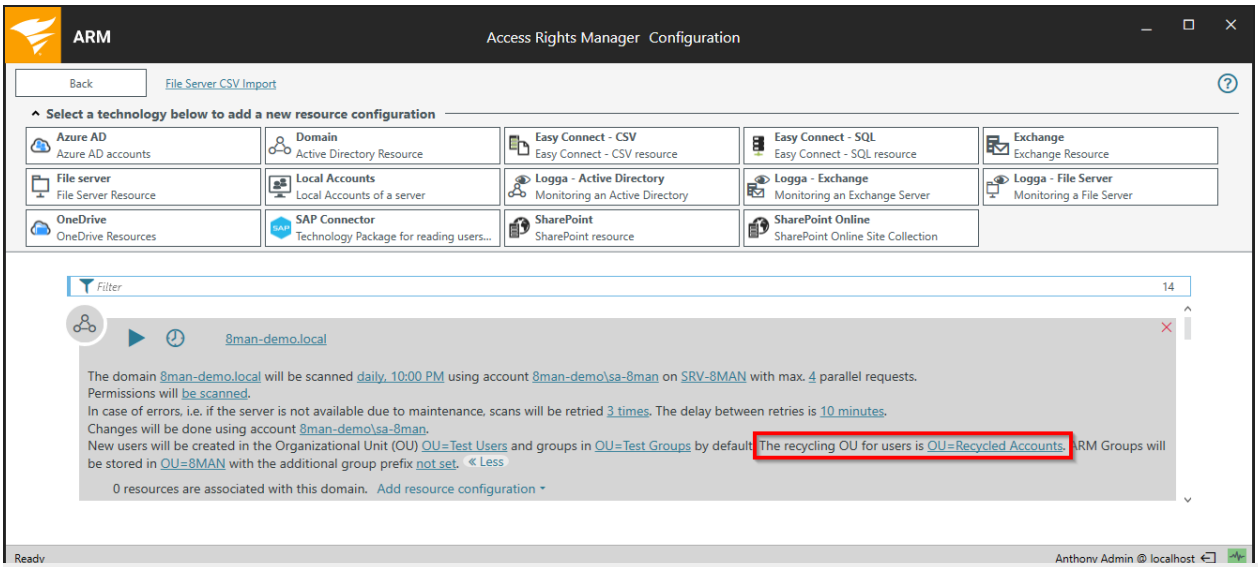
If you leave the option set to "not set", the credentials will be prompted for each change.

Follow our recommendation for using service accounts.

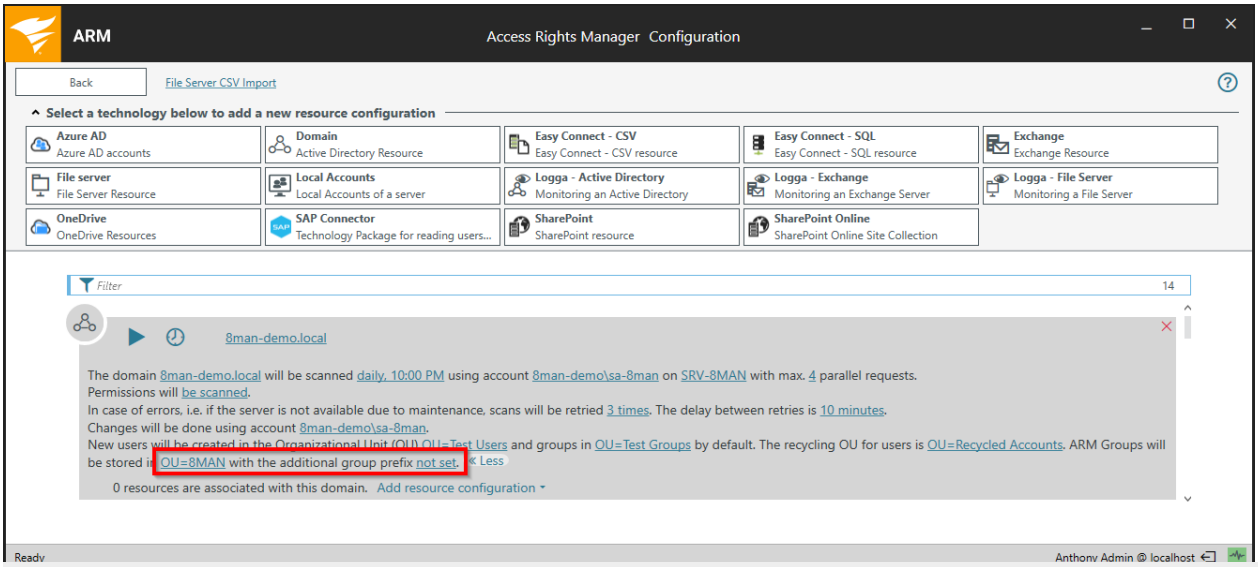


Configure in which OU you want ARM to create new users and groups.

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.



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

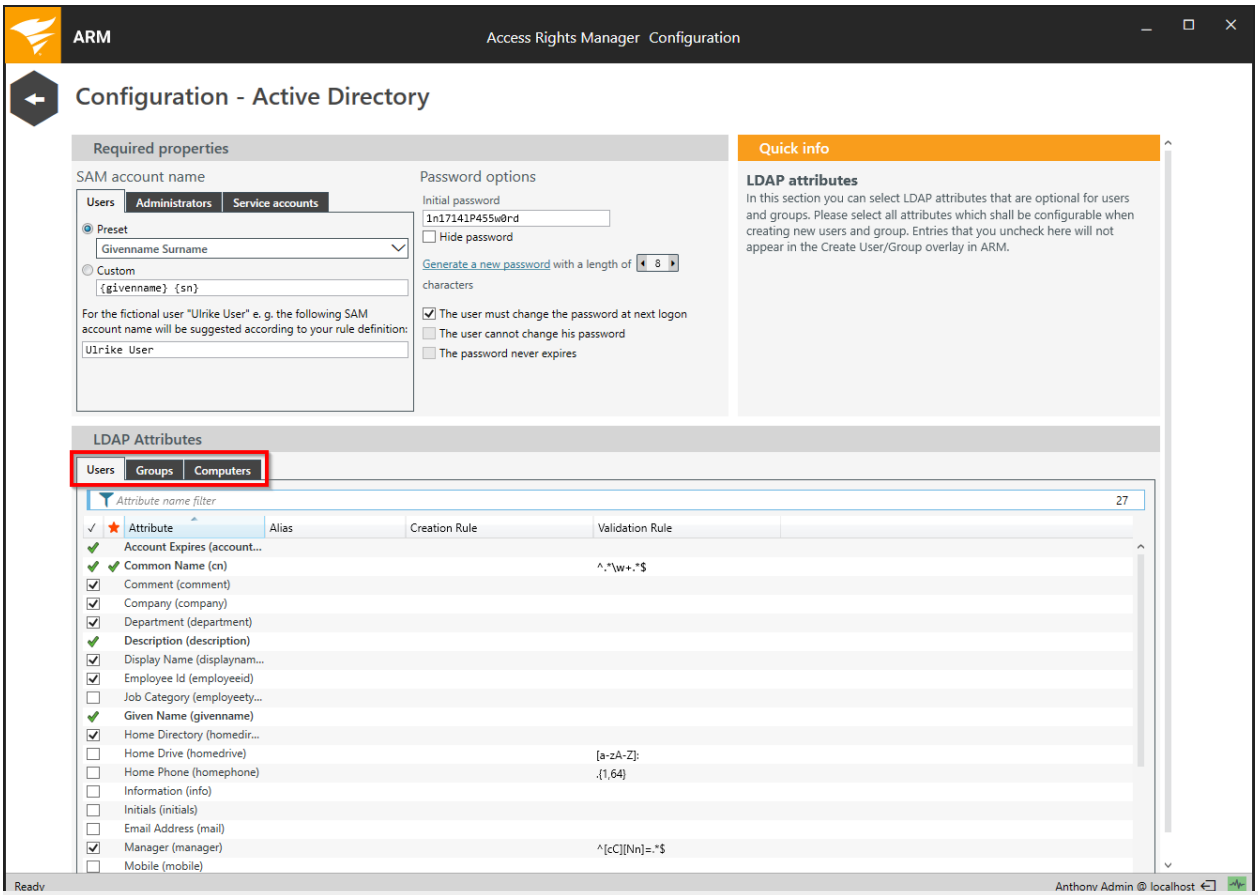


If using the group wizard, you can determine into which OU automatically created ARM groups are placed.

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.



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

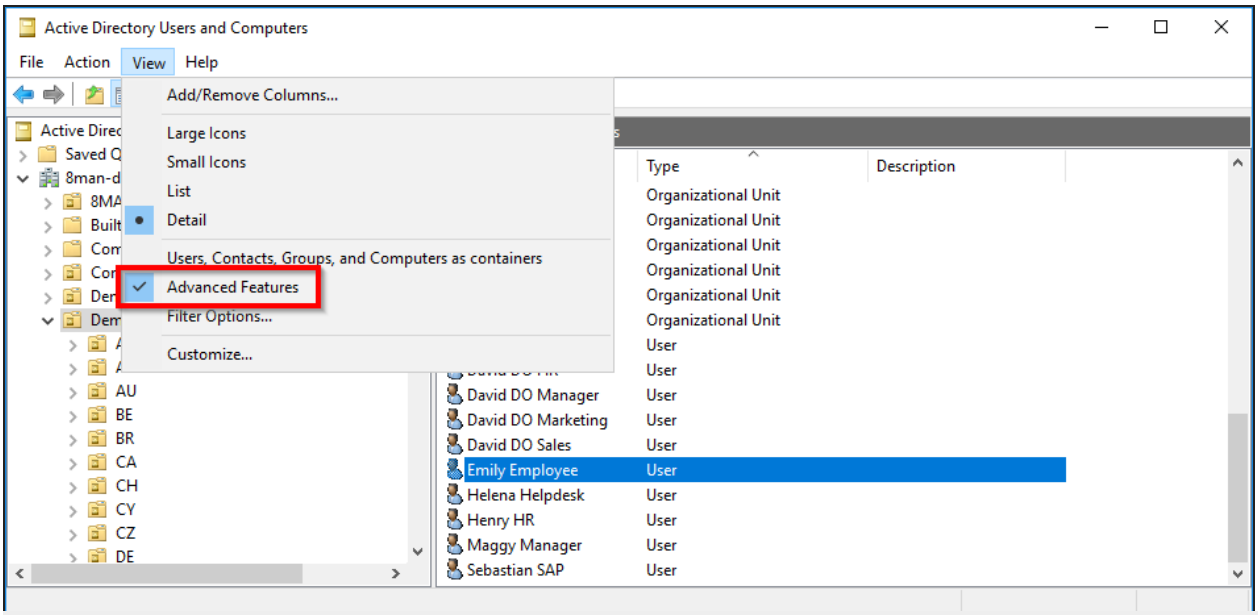
The following example loads the additional attributes `employeetype` and `wWWHomePage`:

```
<changeConfiguration>

<activeDirectory>

<PropertiesToLoad
type="System.String">employeetype;wWWHomePage</PropertiesToLoad>

<PropertiesDetails>

<employeetype>

<AliasDisplayName type="System.String">Job Category</AliasDisplayName>

</employeetype>
```

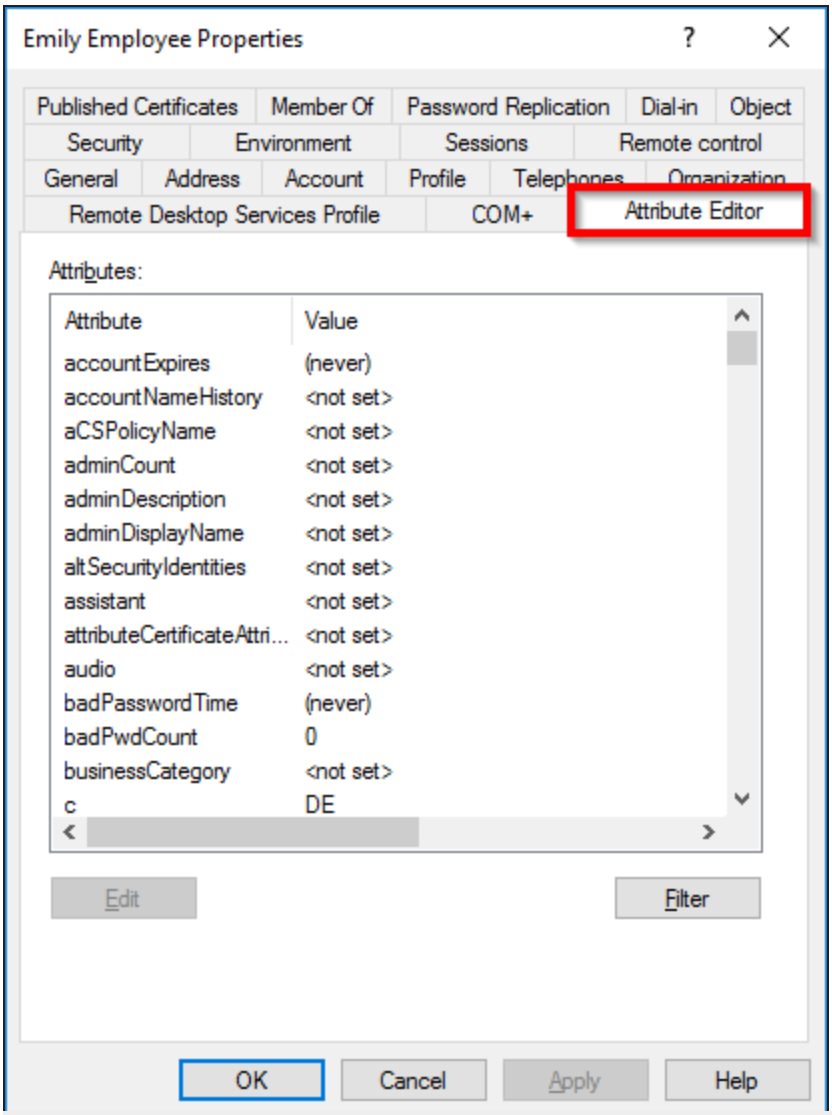
```
<wWWHomePage>
<AliasDisplayName type="System.String">Website</AliasDisplayName>
</wWWHomePage>
</PropertiesDetails>
</activeDirectory>
</changeConfiguration>
```

It is also possible to load attributes of type boolean:

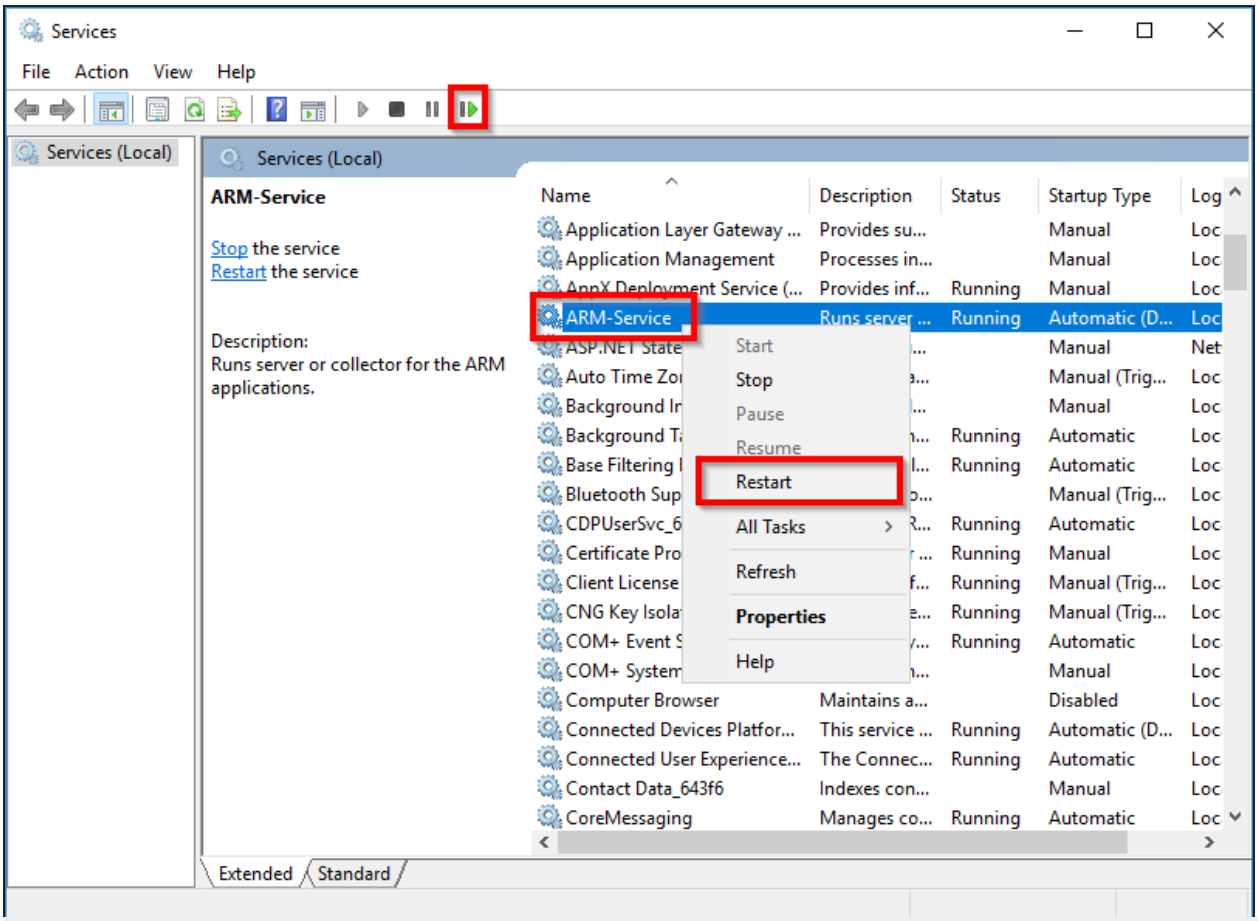
```
<changeConfiguration>
<activeDirectory>
<PropertiesToLoad
type="System.String">msExchHideFromAddressLists</PropertiesToLoad>
<PropertiesDetails>
<msExchHideFromAddressLists>
<TypeInfo>System.Boolean</TypeInfo>
<AllowOnlyDefinedValues type="System.String">true</AllowOnlyDefinedValues>
<DefinedValues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



Identify the correct attribute names with the help of the Active Directory Users and Computers console. Enable "Advanced Features".



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:

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

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
"employeetype"	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
"operatingsystemservicepack"	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 pnserver.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;l;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

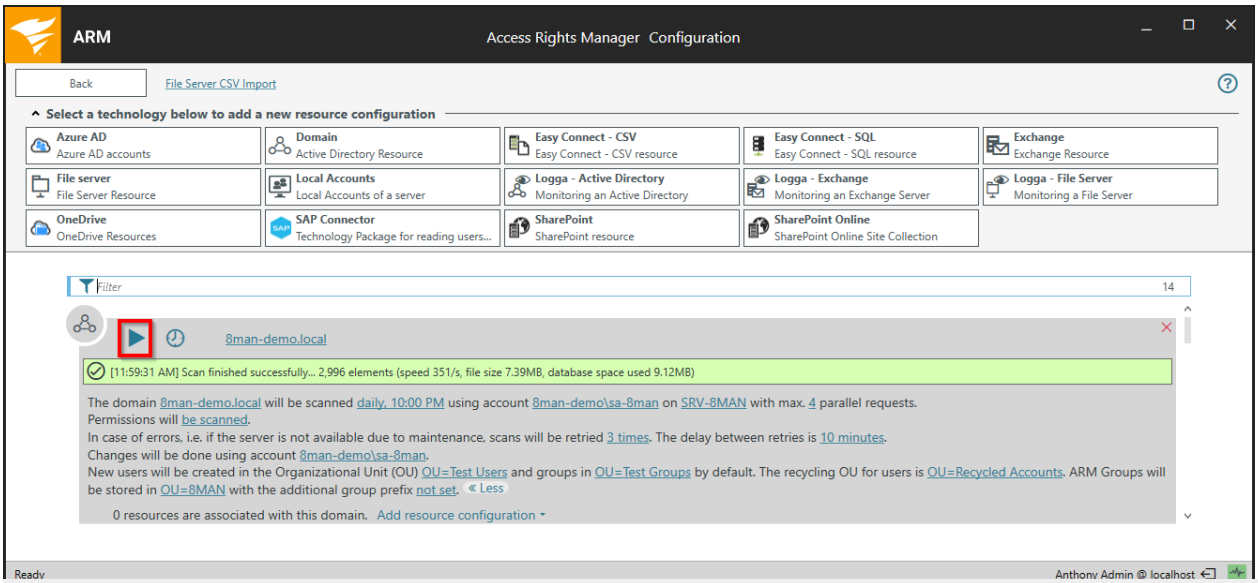
Self Service in the cockpit: "Change my personal information"

WebClient.Cockpit.ChangeAttributes.SelfService

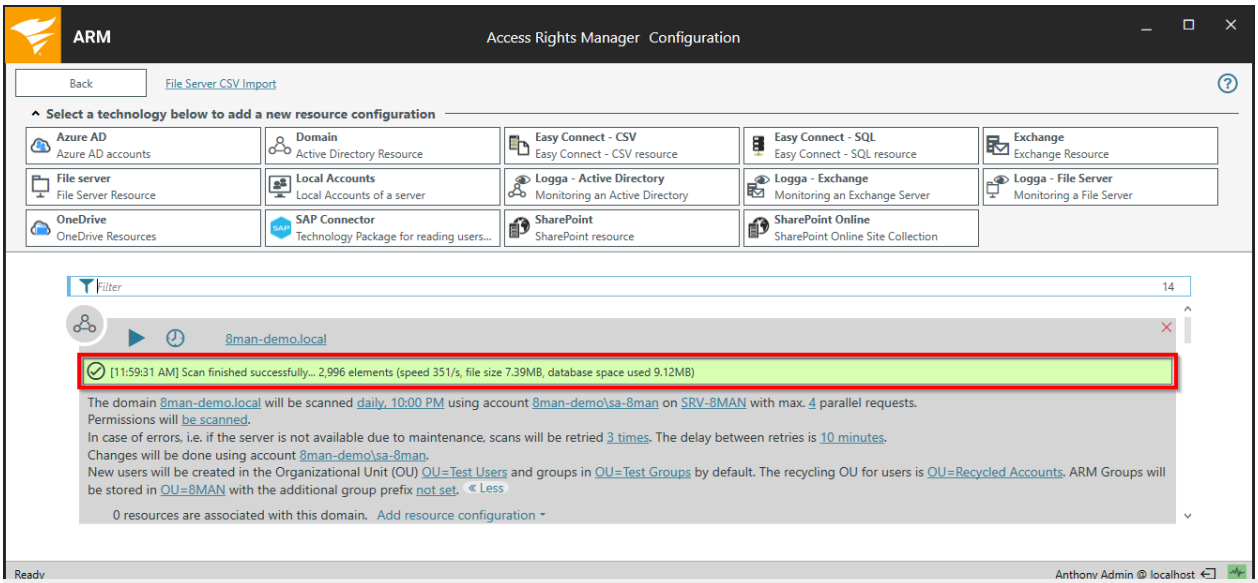
Line 02

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

Start AD scans



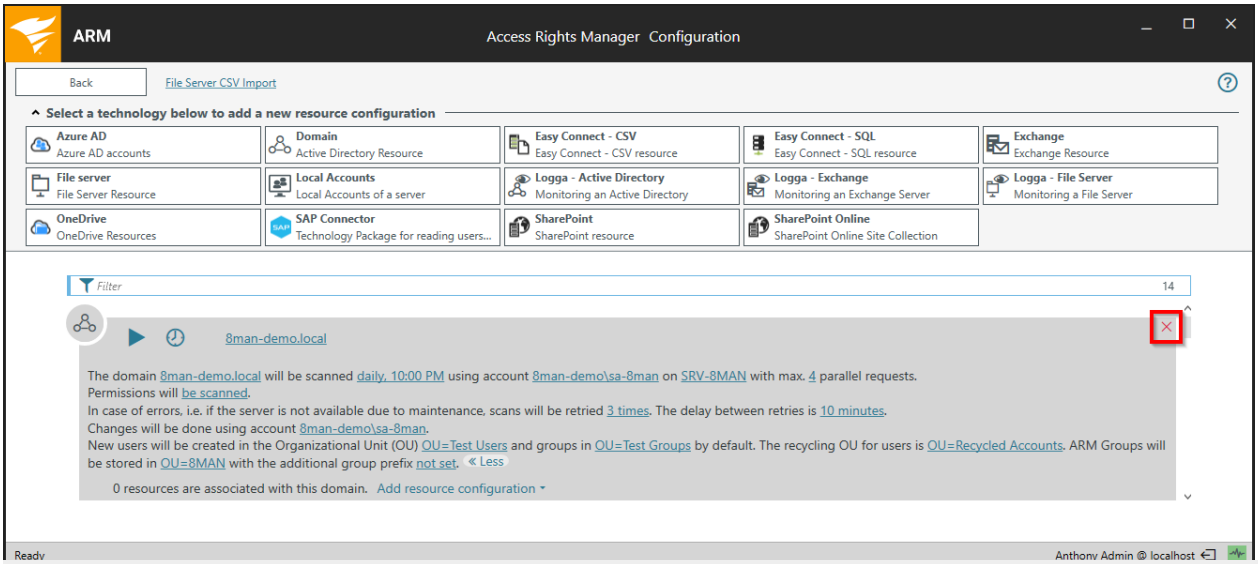
Start/cancel an AD scan. Typically AD scans only take a couple of minutes.



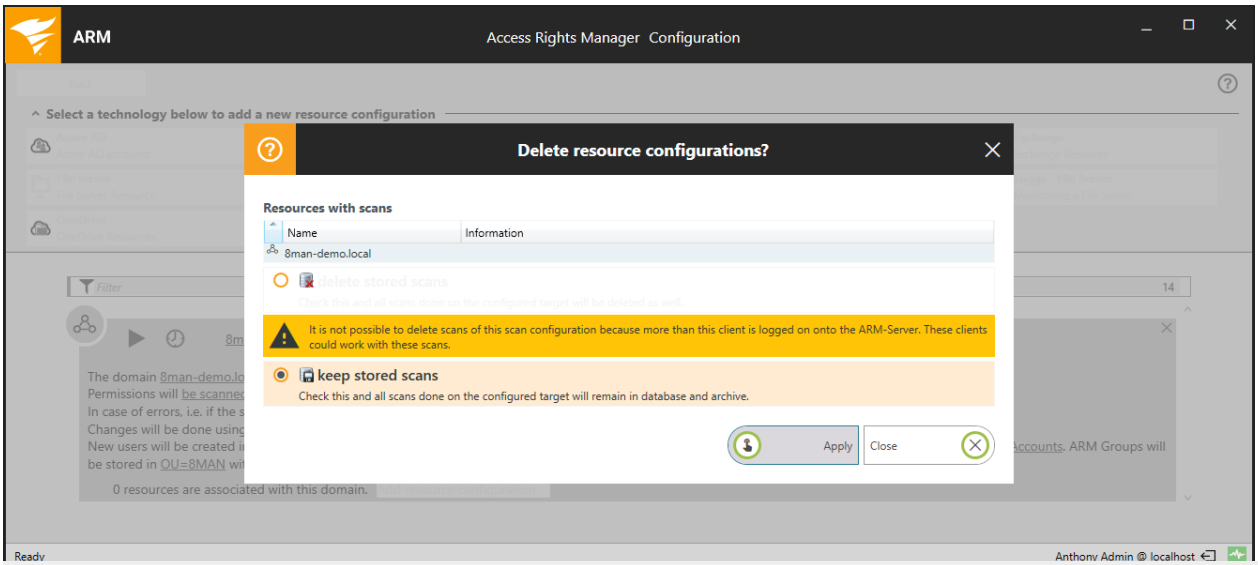
Status information is shown during and after the AD scan.

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.

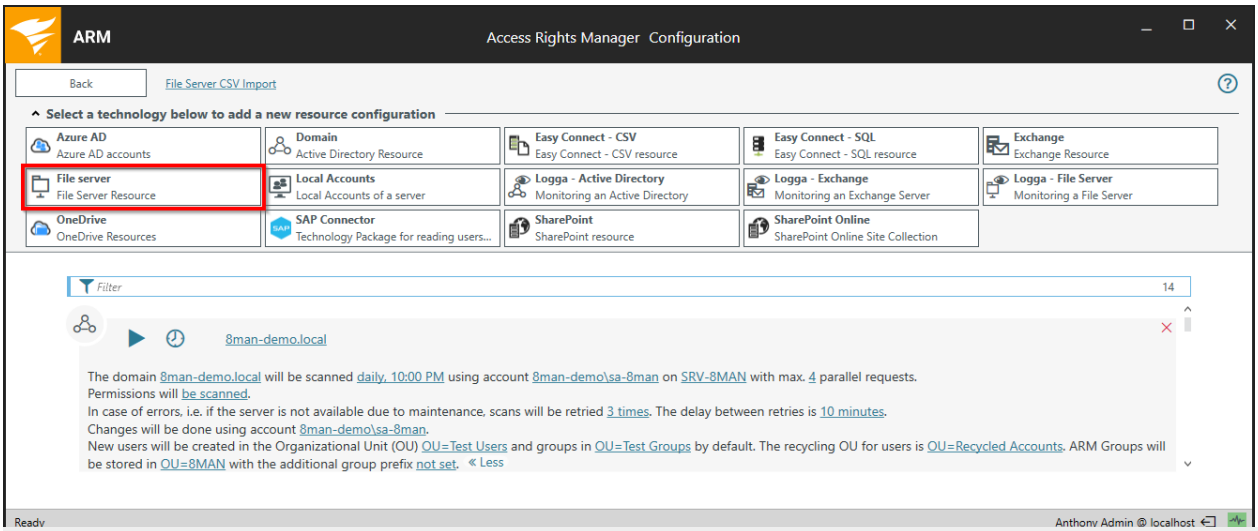


If you delete a scan configuration, you can either keep or delete the stored scan data.

Deleting is only possible if all other ARM applications are closed. You can identify logged in users in the Server status section.

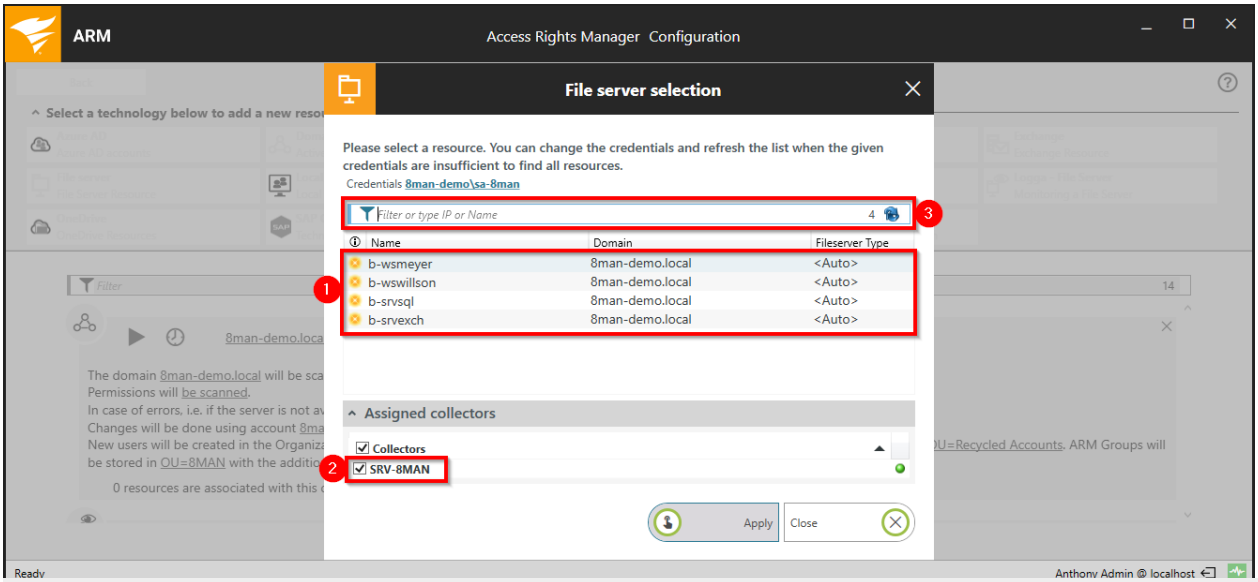
File server (FS) scans

Add FS scans

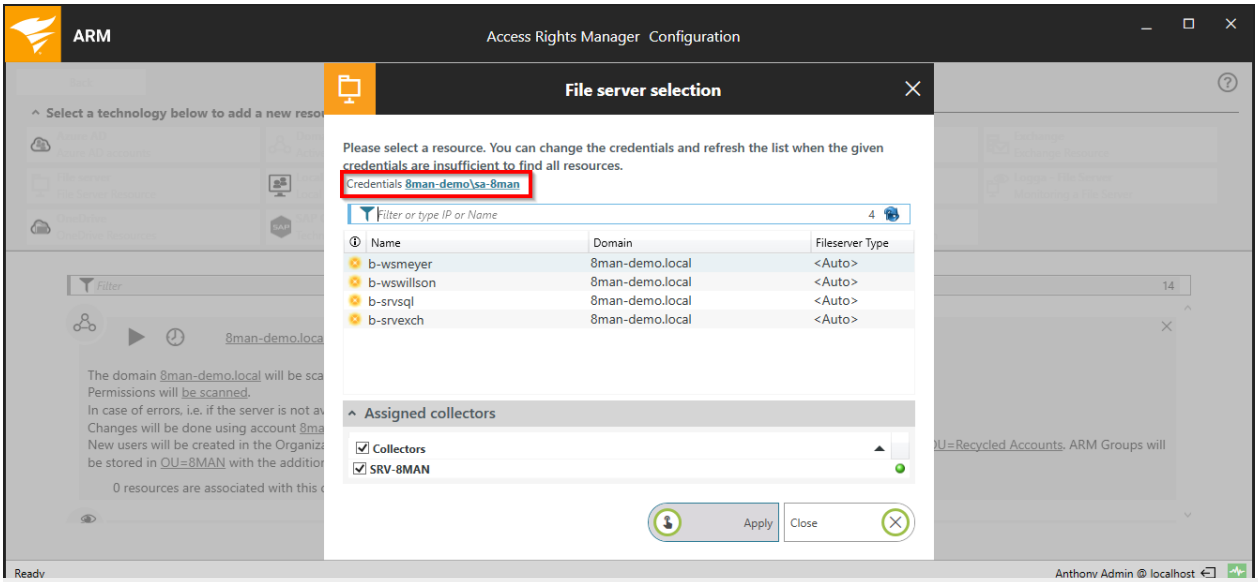


Click on "File server" to add an FS scan.

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.



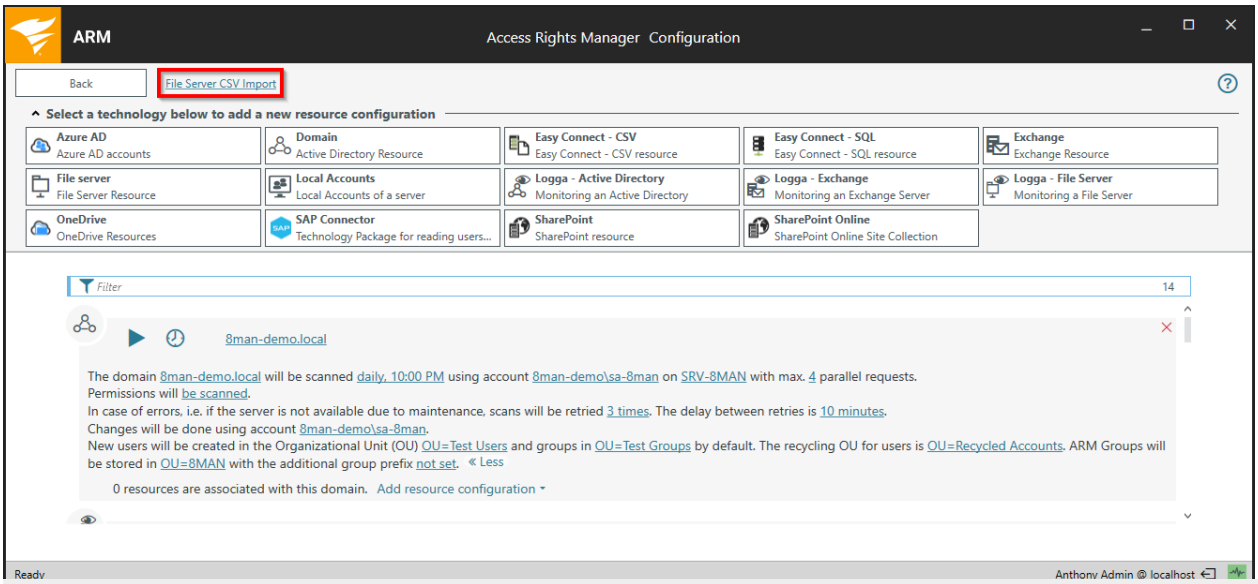
By default the ARM server basic configuration credentials will be used.

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

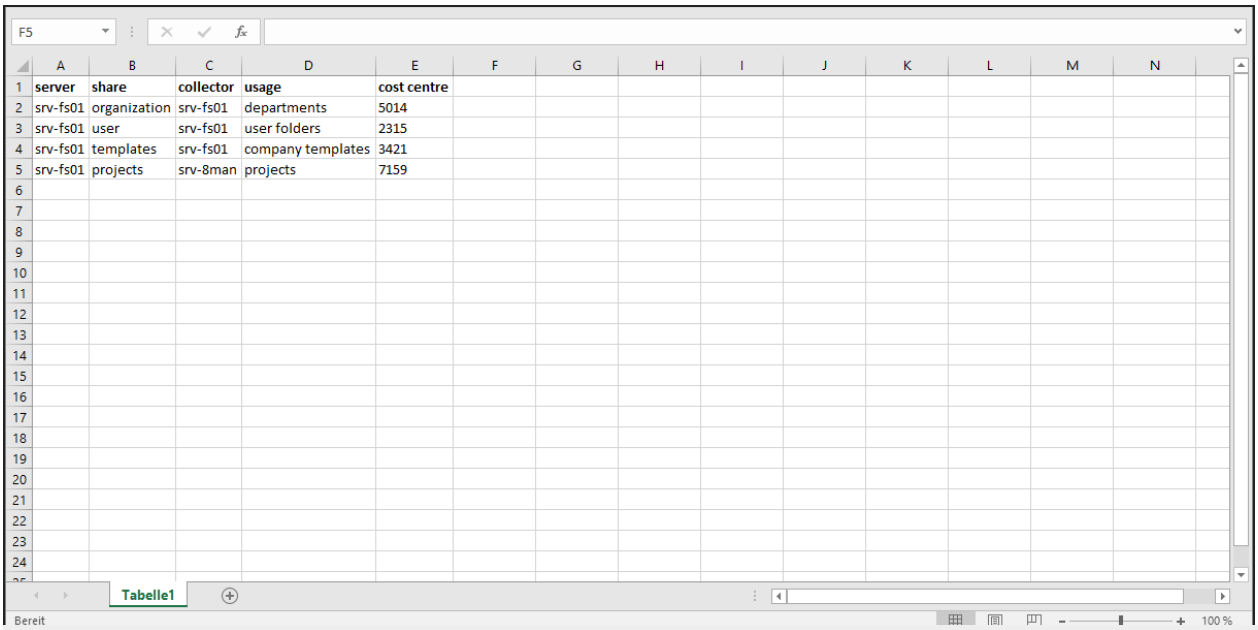
If the scan configuration is invalid you will see an error message at the start of the scan. This will also be recorded in a Logfile.

Import FS scan configurations



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.



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 templates	3421
srv-fs01	projects	srv-8man	projects	7159

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

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

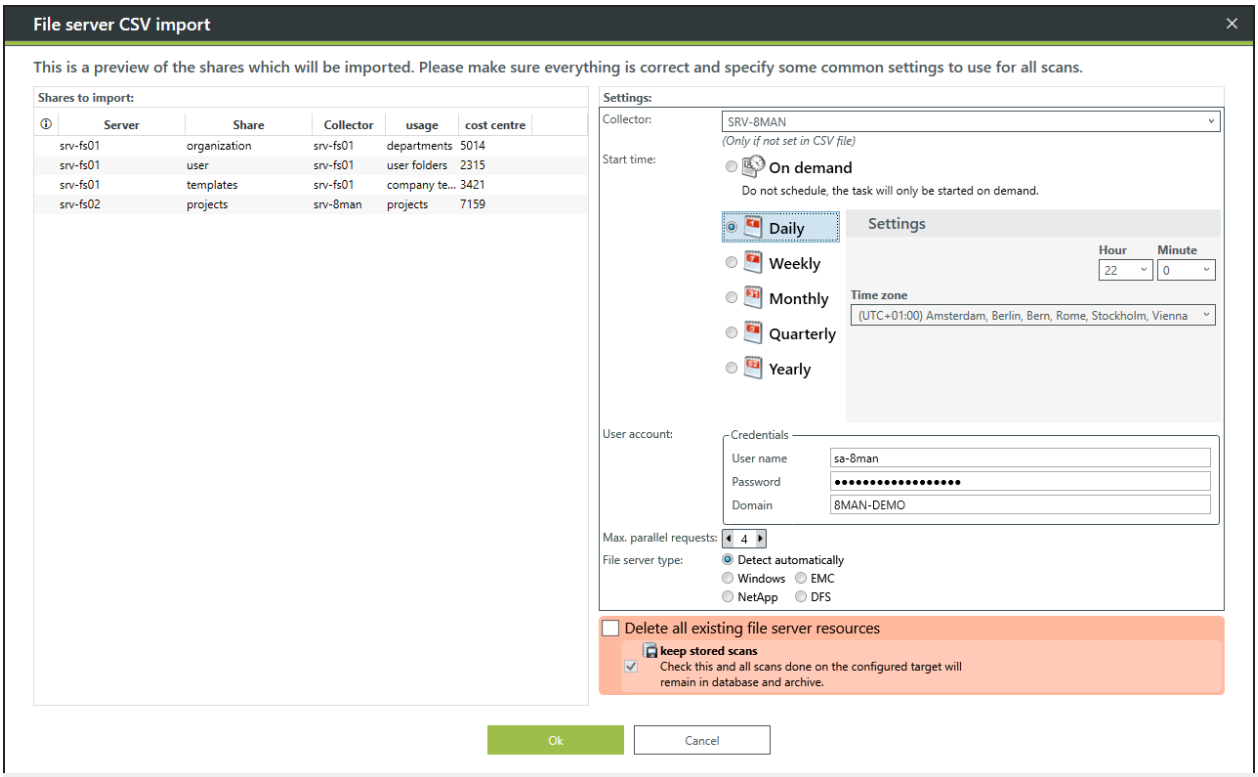
Optional columns:

- "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"

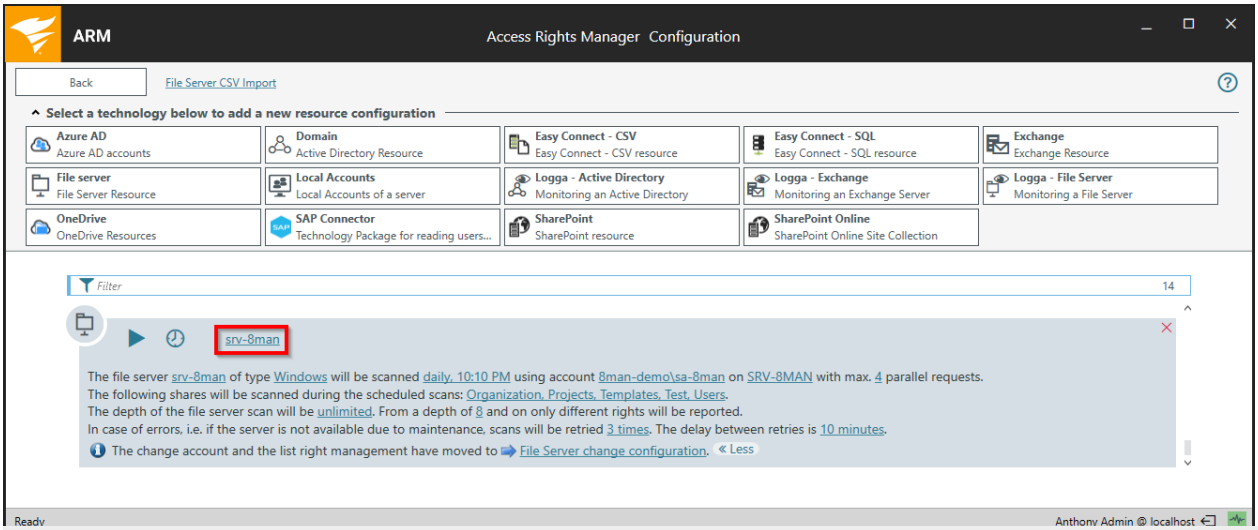


Determine the import settings:

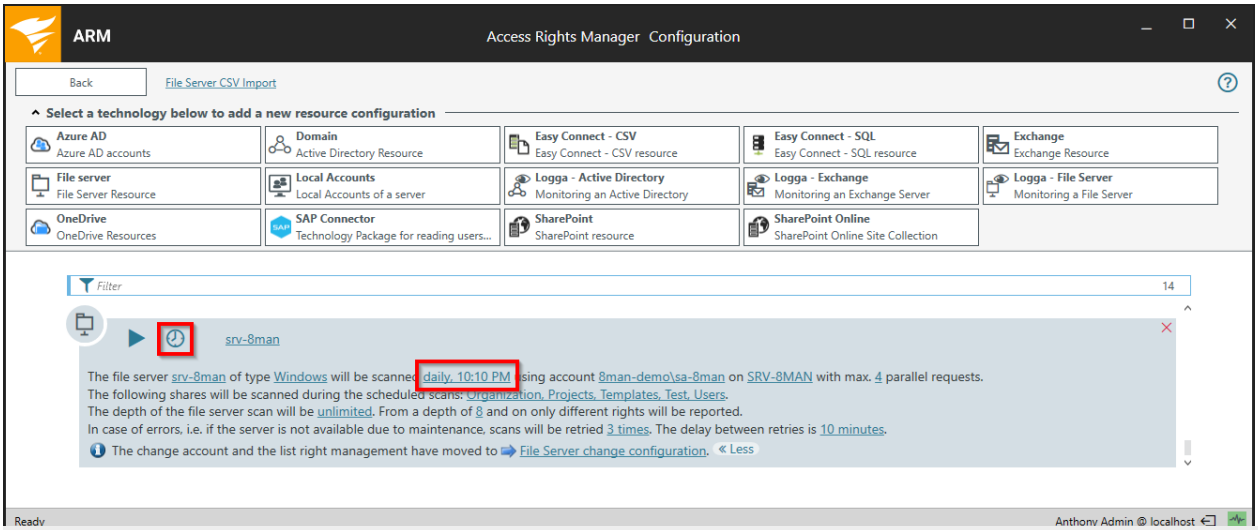
- which collector(s) perform(s) scans (only required if not included in the CSV file)
- at what time the scans are performed
- how many parallel requests are performed
- file server type
- if previously entered scan configurations should be deleted

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

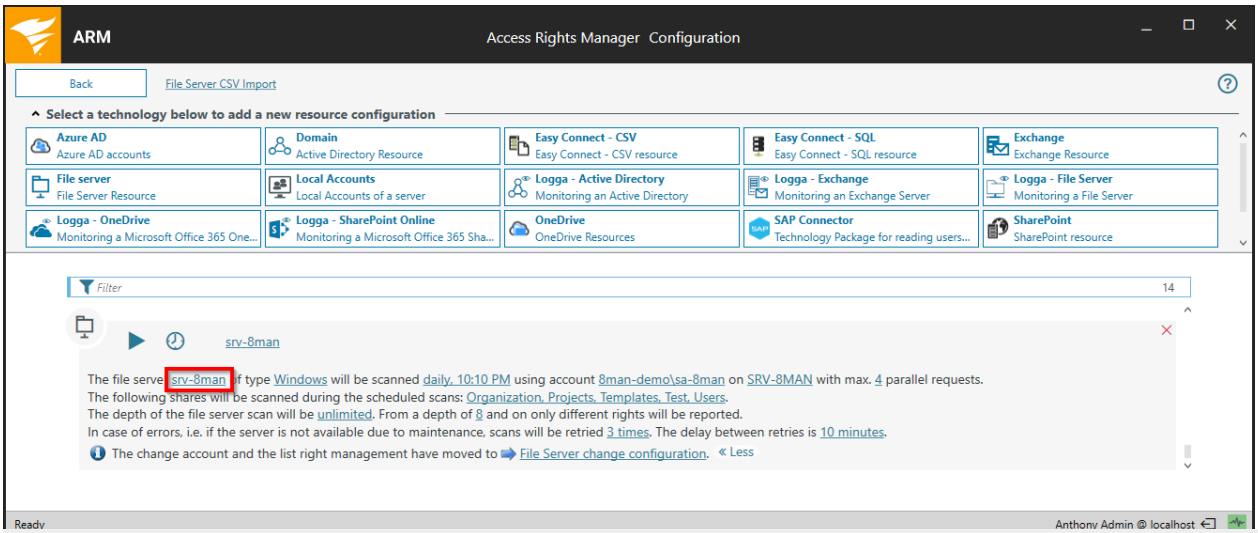
Configure FS scans



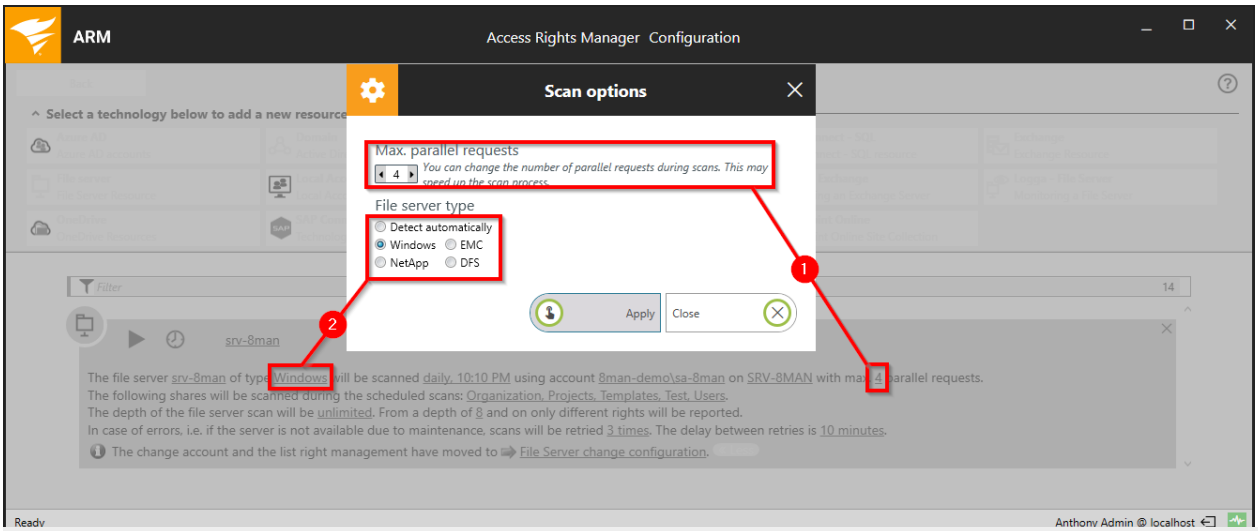
Edit the name of the FS scan configuration.



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

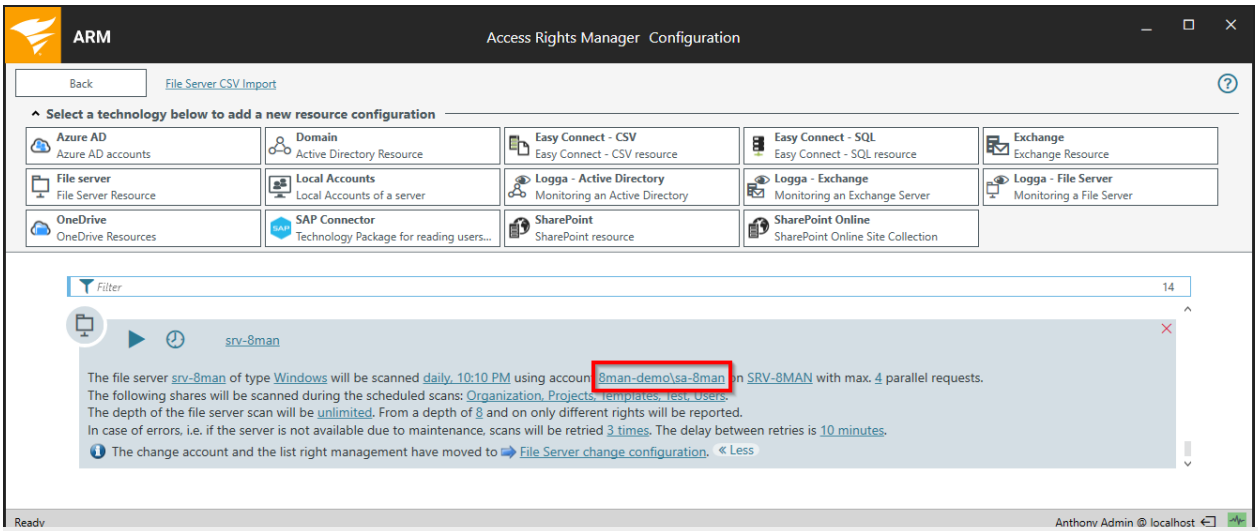


You can change the file server for which this scan configuration is valid.



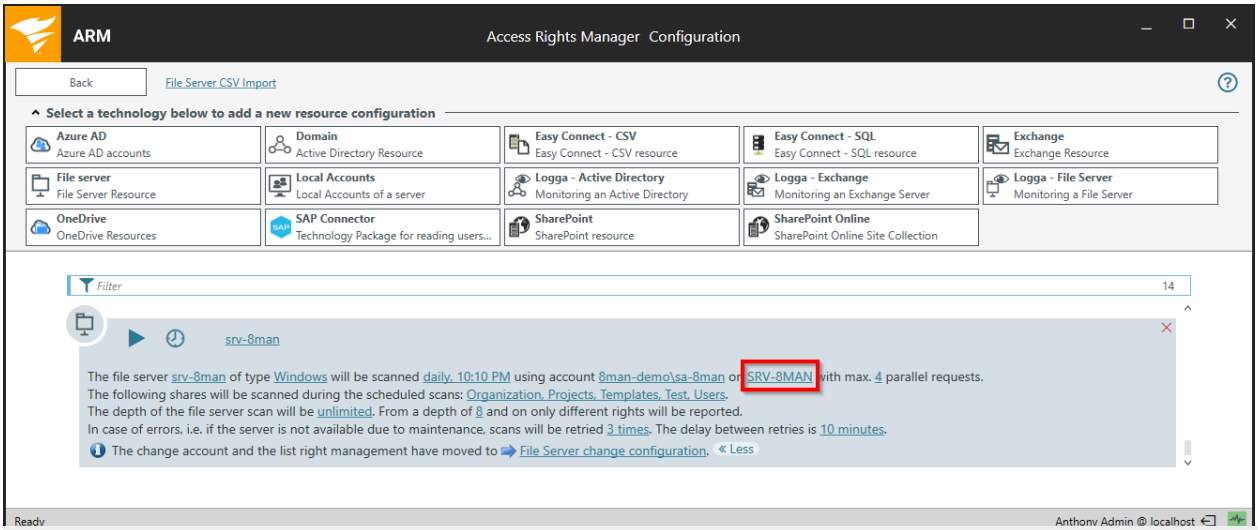
1. Configure the number of parallel requests. The more parallel requests the faster the scan and the higher the CPU load. Possible values are 1 (no parallel requests) to 128.
2. Set the file server type.

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

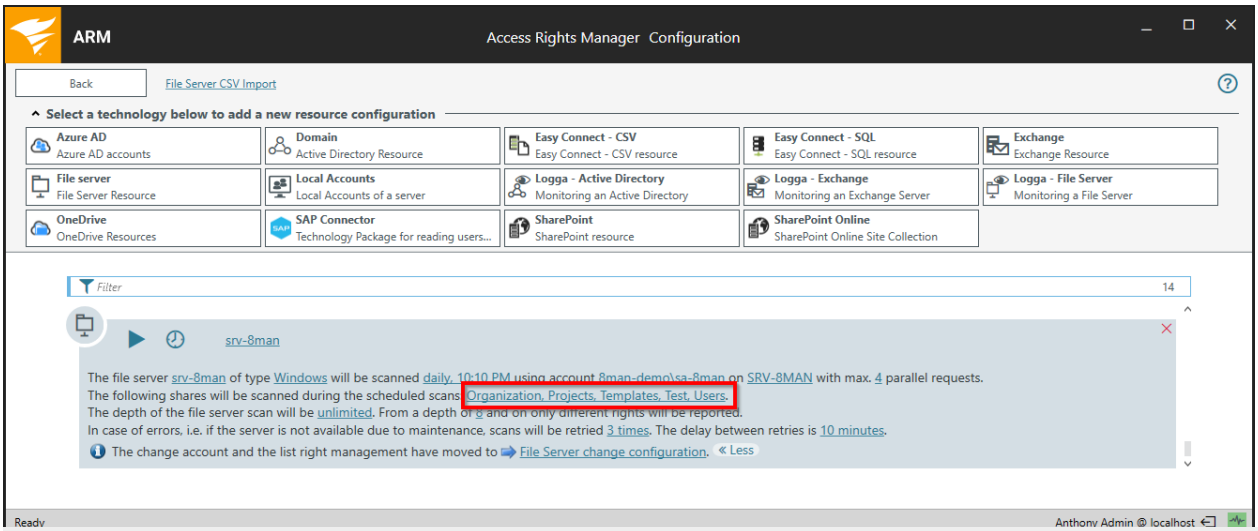


Determine which credentials are used to perform the FS scan.

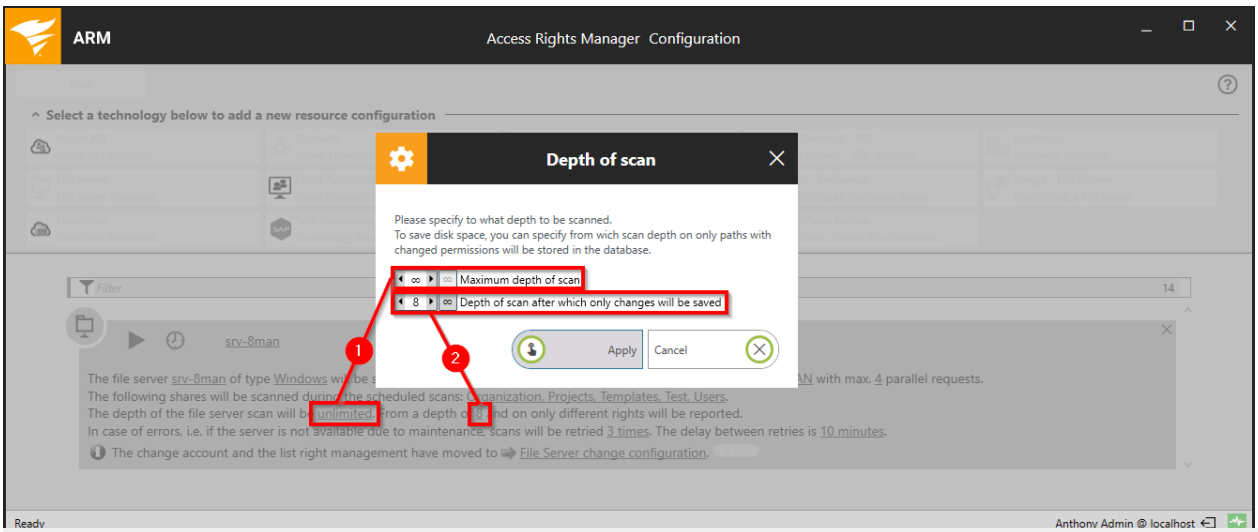
Please reference the following section: Service accounts.



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.

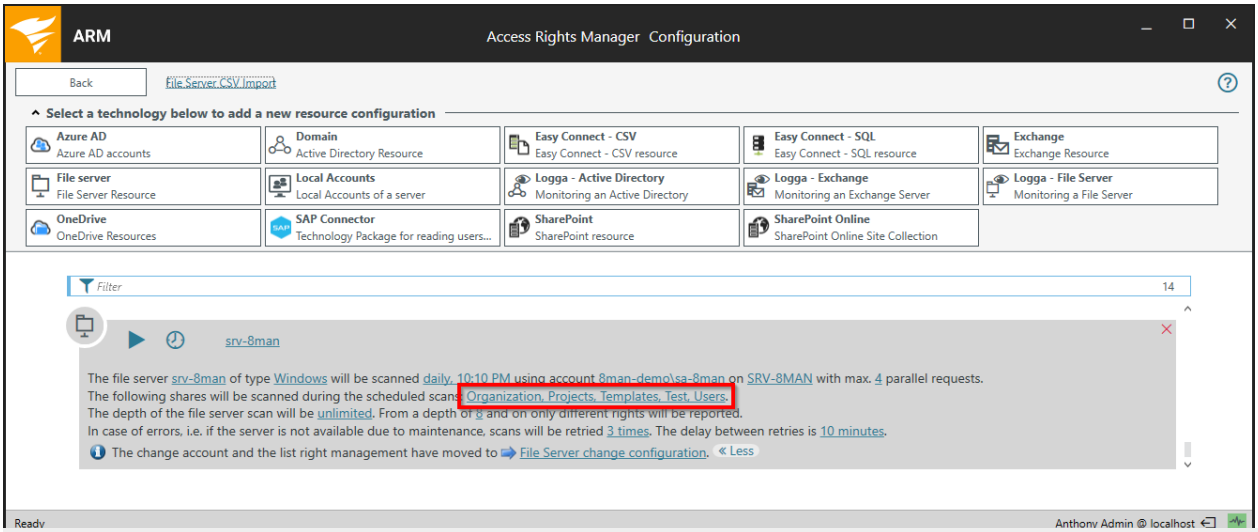


Determine the shares that will be scanned.



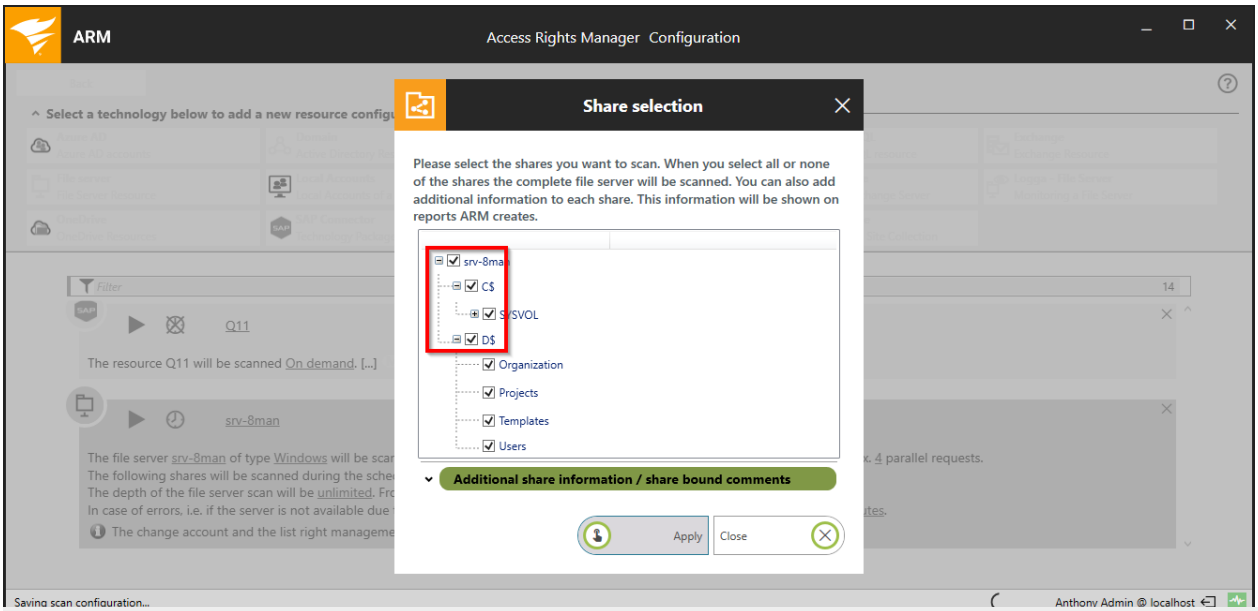
1. Determine the scan depth.
2. To save storage space, you can specify from which depth only paths with deviating permissions are stored.

Select shares

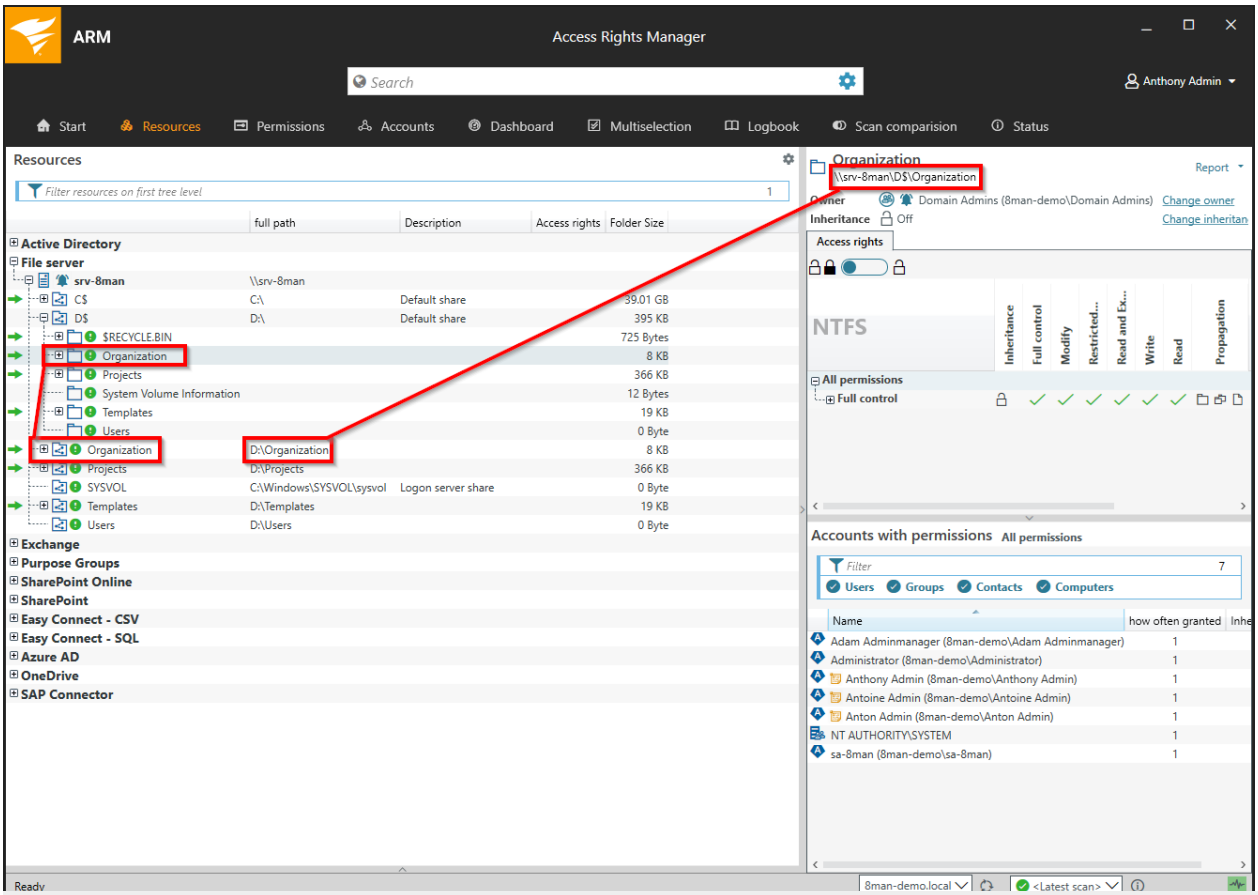


To ensure optimal results for reports and viewing information in the ARM resource view, consider the following points when selecting shares.

Unfavorable



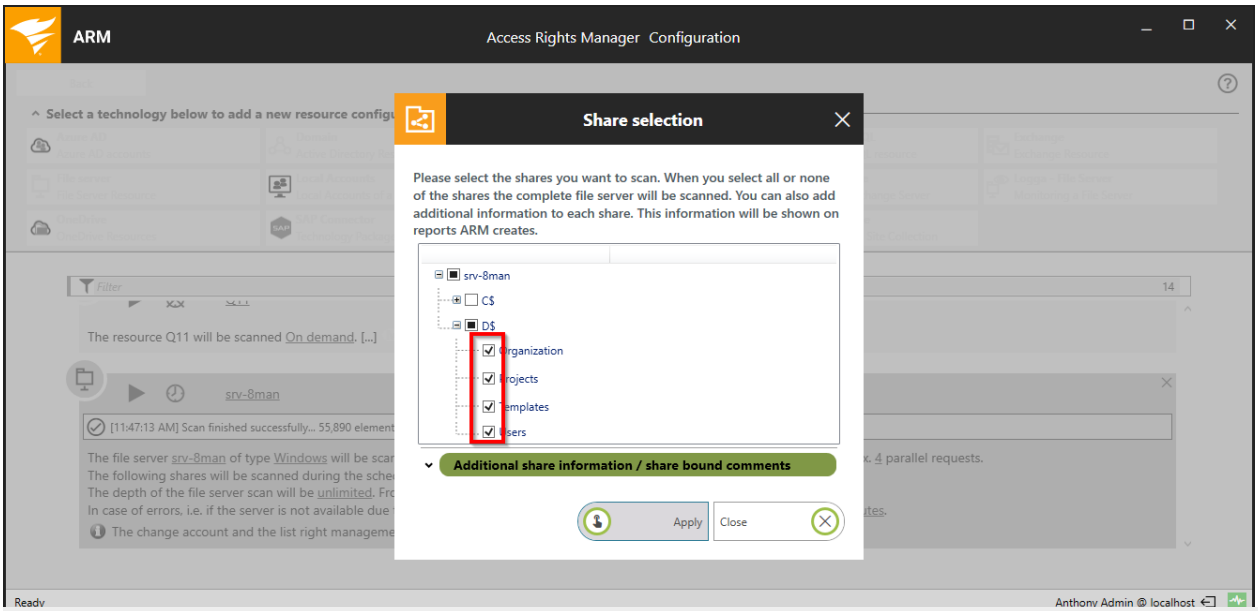
A selection of these shares will result in the following resource view:



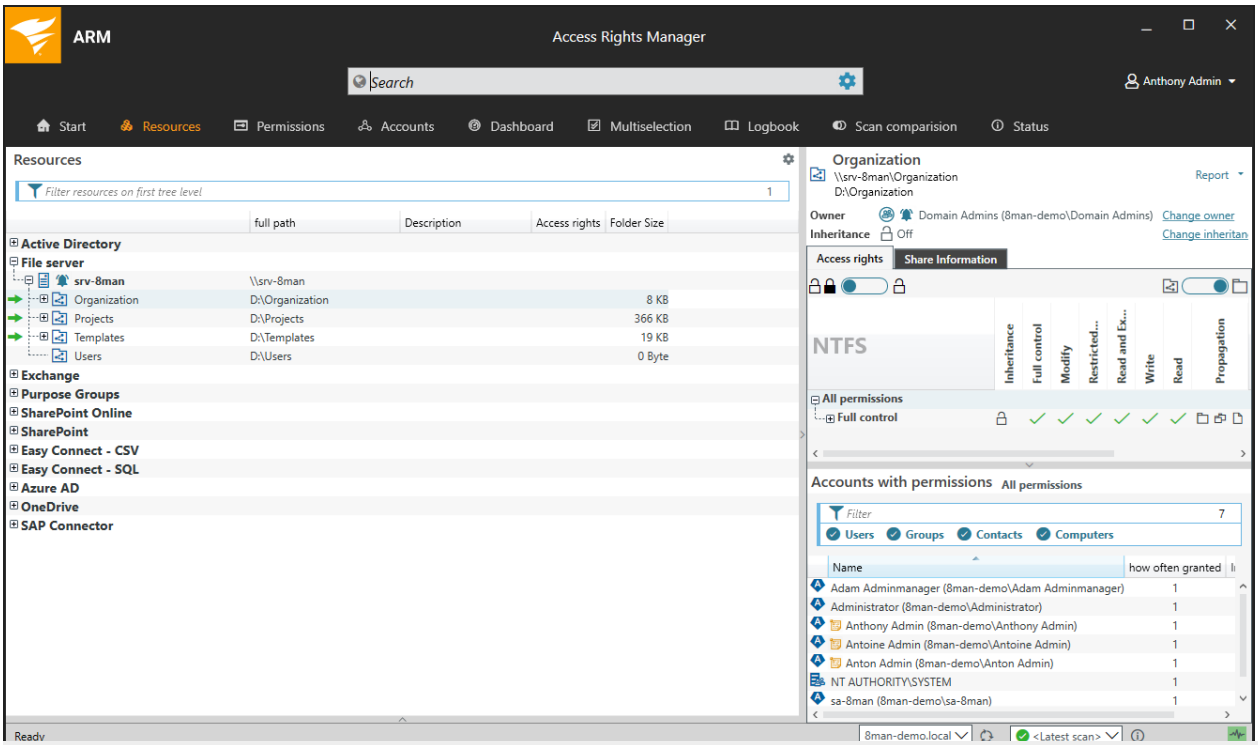
Folders are shown twice (for example "Organization").

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

Ideal

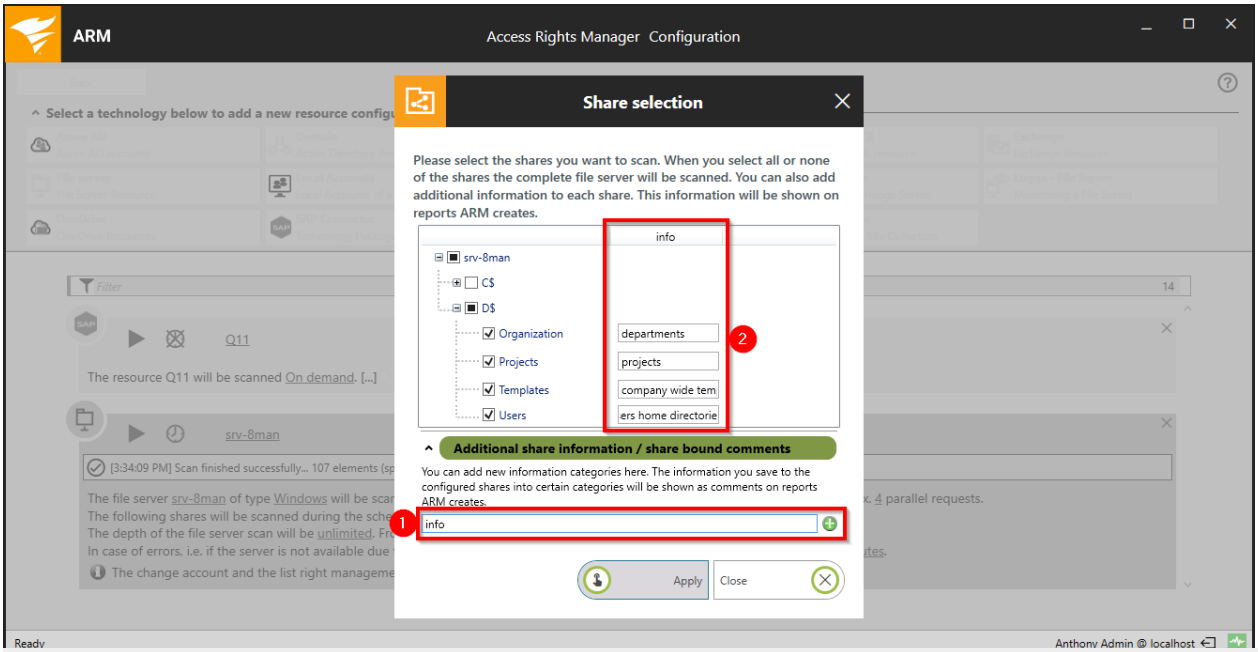


Only select shares, which are entry points and visible/relevant for users.



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

Label shares

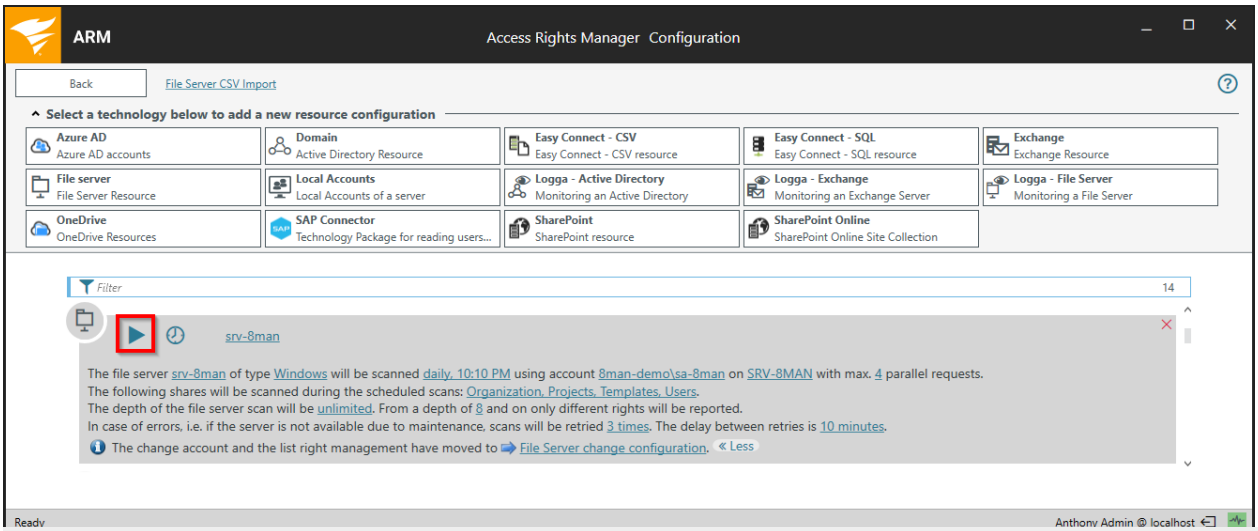


You can add descriptions and additional information to shares.

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.

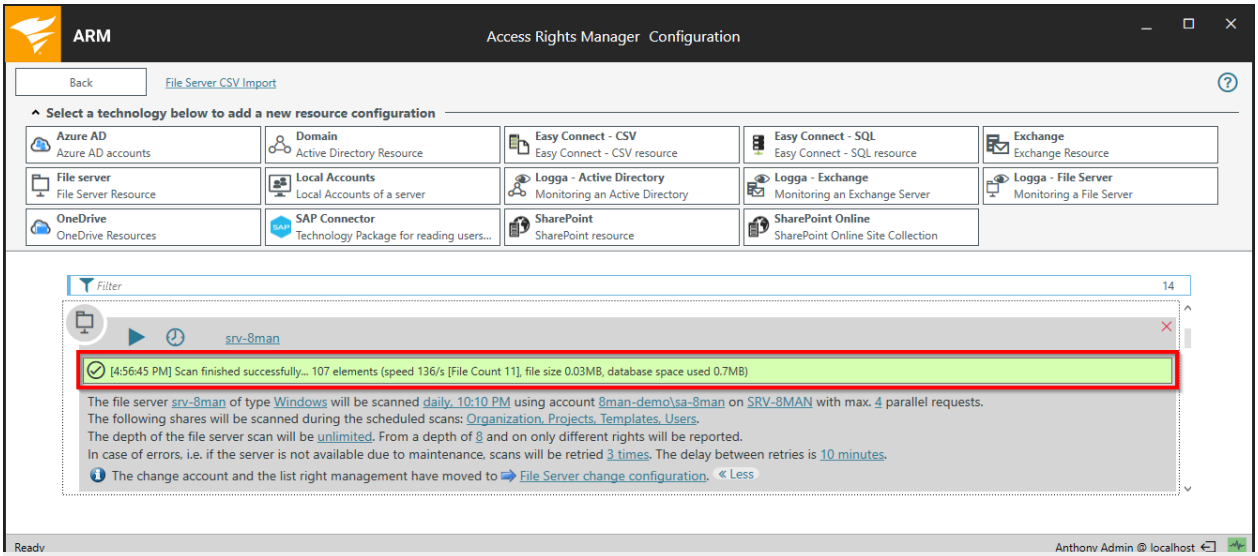
The descriptions are shown in ARM reports.

Start FS scans



Start/cancel the FS scan.

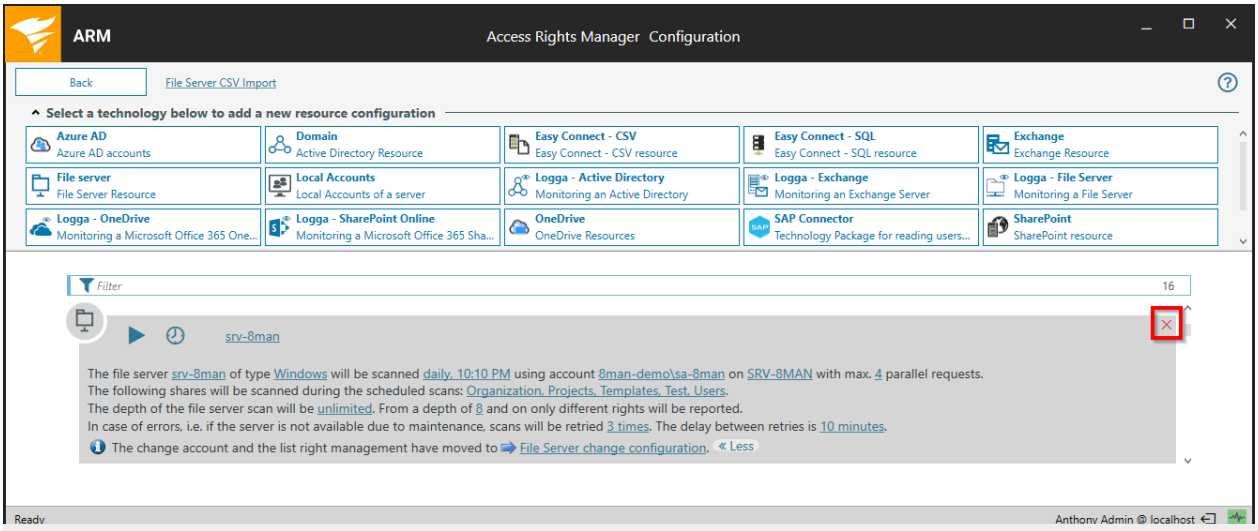
FS scans may take a long time depending on your file server performance and load, network load, and most significantly the number of file server directories that need to be scanned. Initially you can limit your scans on a few shares and lesser scan depth.



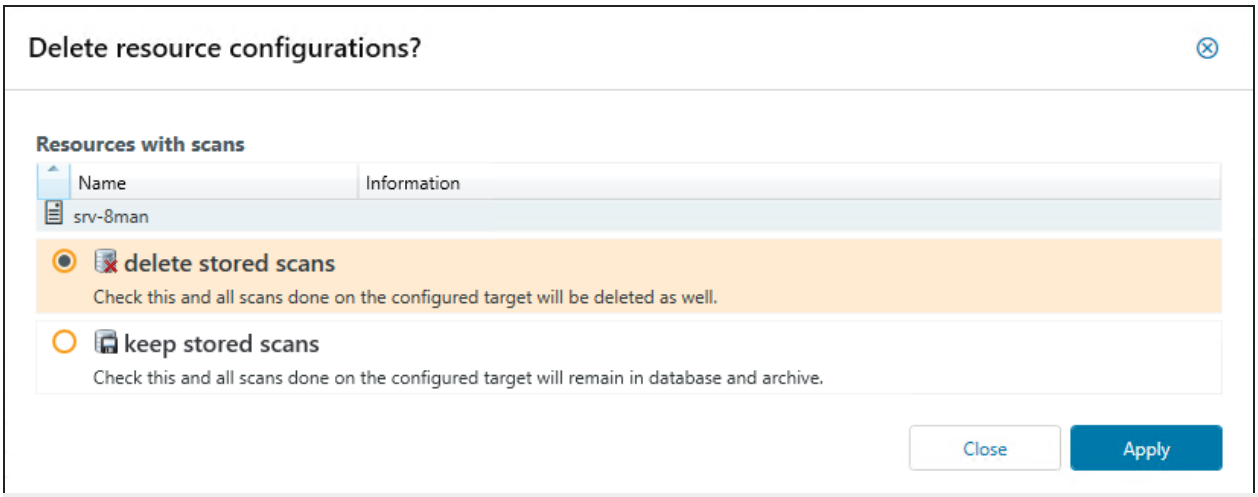
Status information is shown during and after the FS scan.

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



Delete an FS scan configuration.



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.

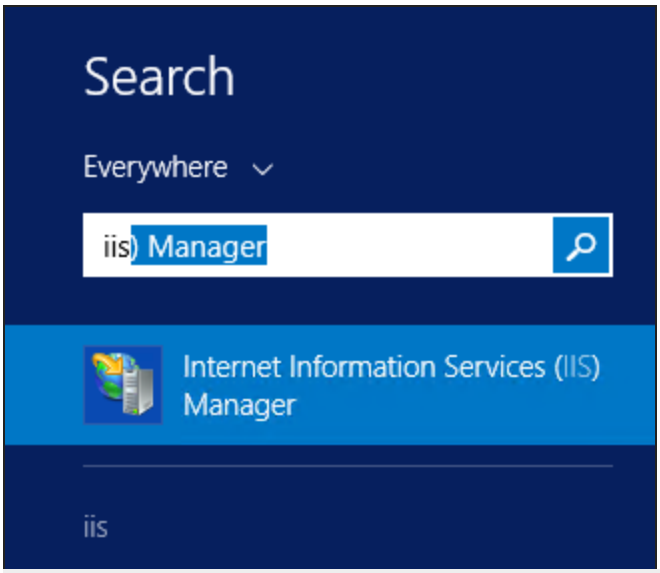
An Exchange scan can be performed by any collector.

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

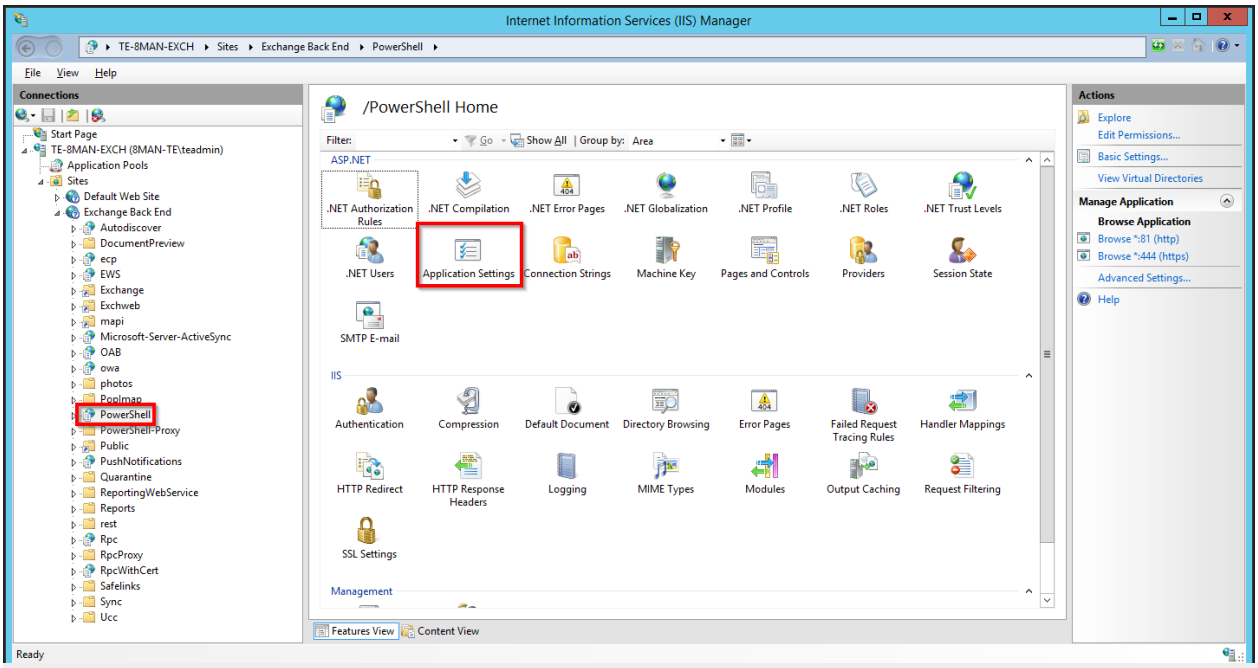
Prepare the PowerShell website

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

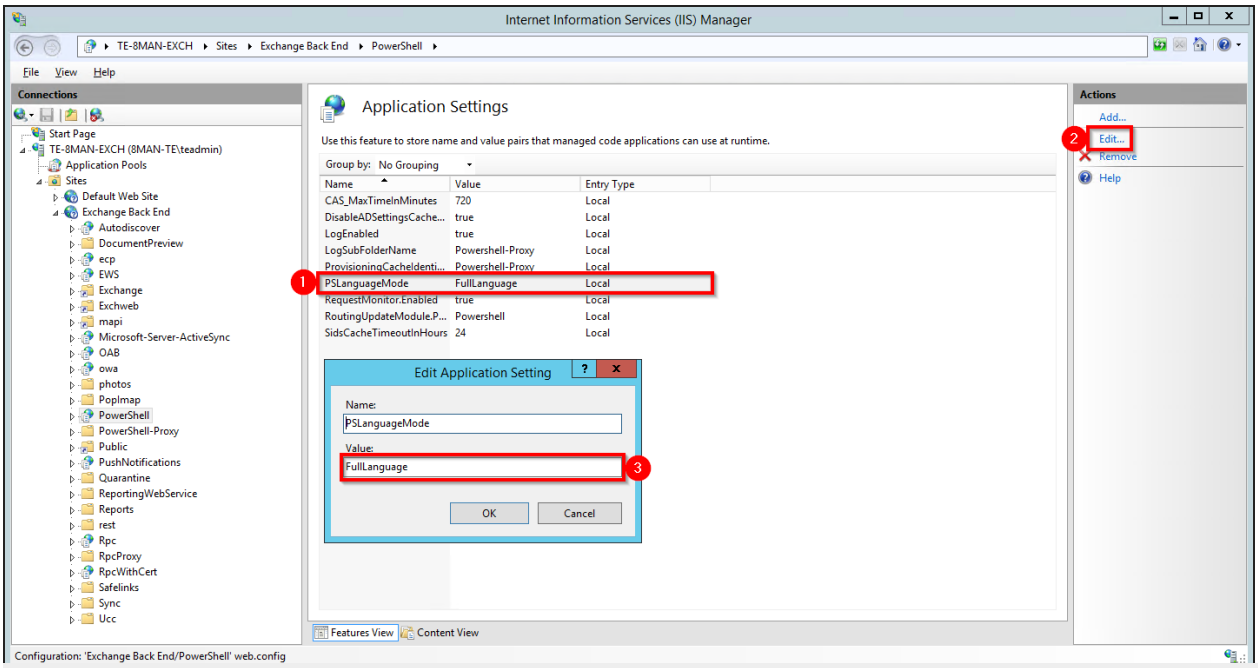
The Exchange Client Access Server (CAS) hosts a site within the IIS, that allows users to access the Exchange Server. It is called "Default Web Site" (2010) or "Exchange Back End" (2013 and higher) and includes the sub-site "PowerShell". This must be configured to allow ARM access to Exchange.



Start the IIS Manager on the CAS.

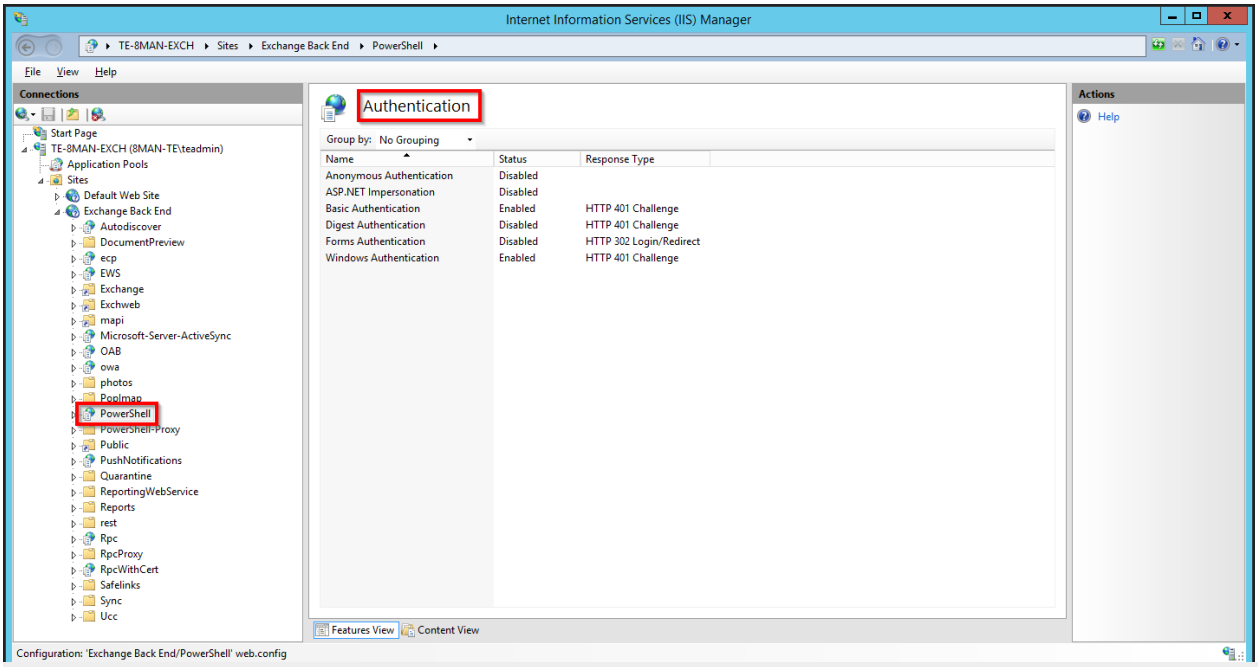


Navigate to "Powershell". In Exchange 2010 this can be found under "Default Web Site". In Exchange 2013 it is found under "Exchange Back End". Double-click "Application Settings".



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

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



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/bernhard_frank/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.

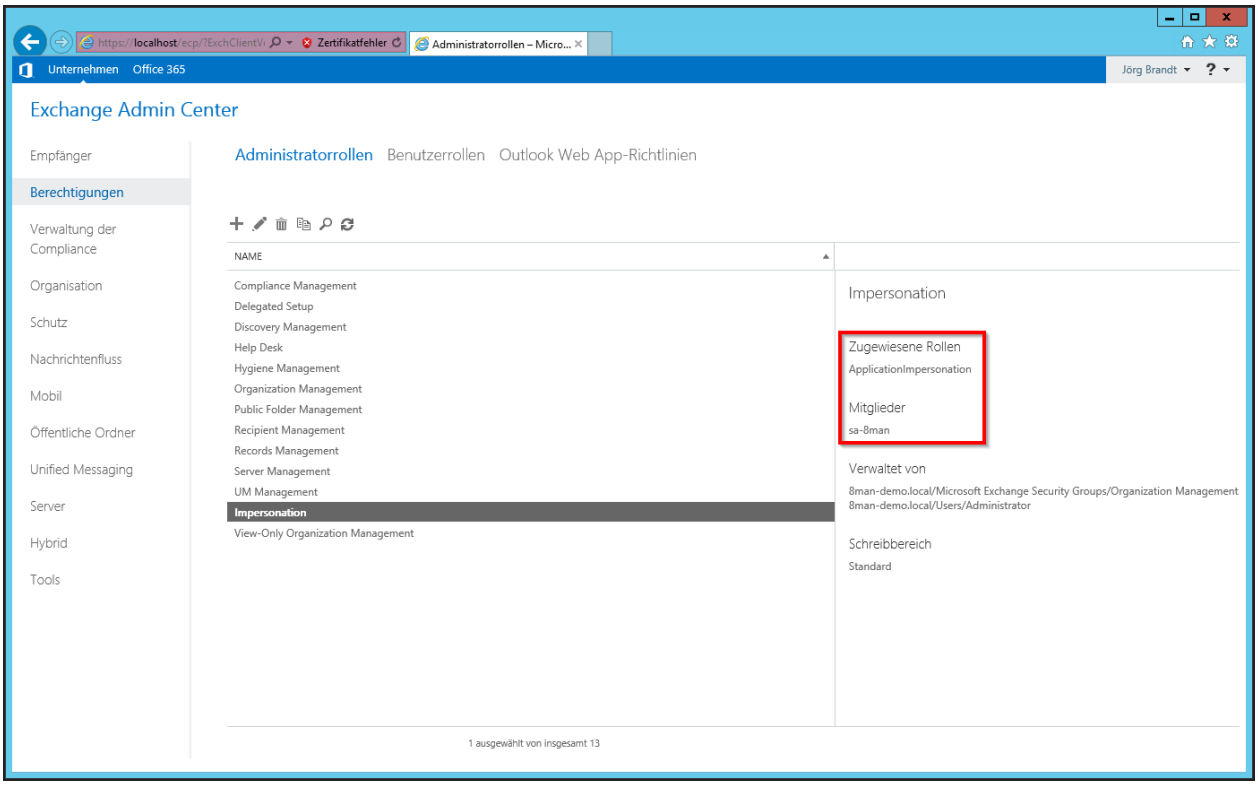
Access to the Exchange Web Service always happen in context with the mailbox user. This requires that the scan account (service account) has the right to impersonate.

> ⓘ 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 (© 2020 Microsoft, 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 (© 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:



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.

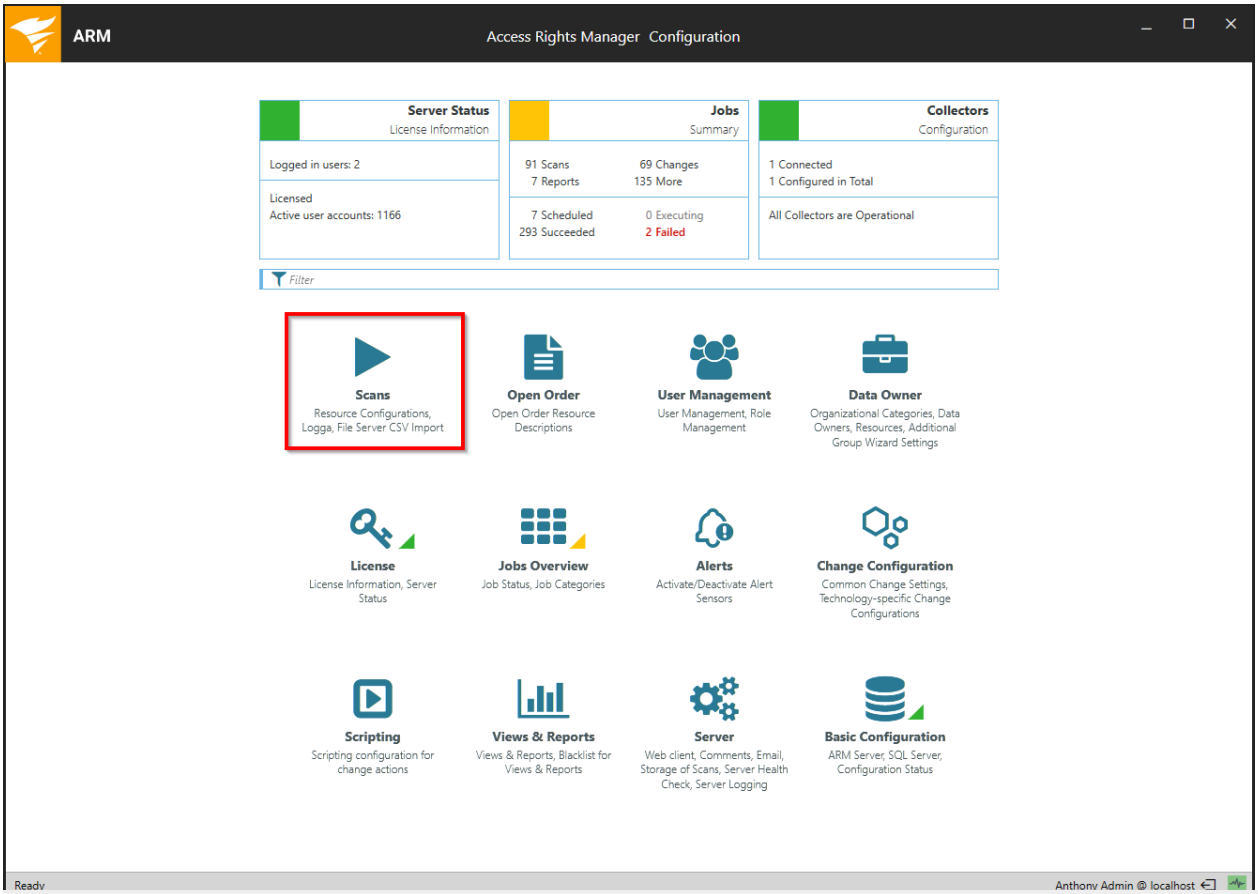
Summary: The scan account must be assigned a management role, including the explicit impersonation right.

Test the connection to Exchange PowerShell

Use the following process to test the connection to PowerShell:

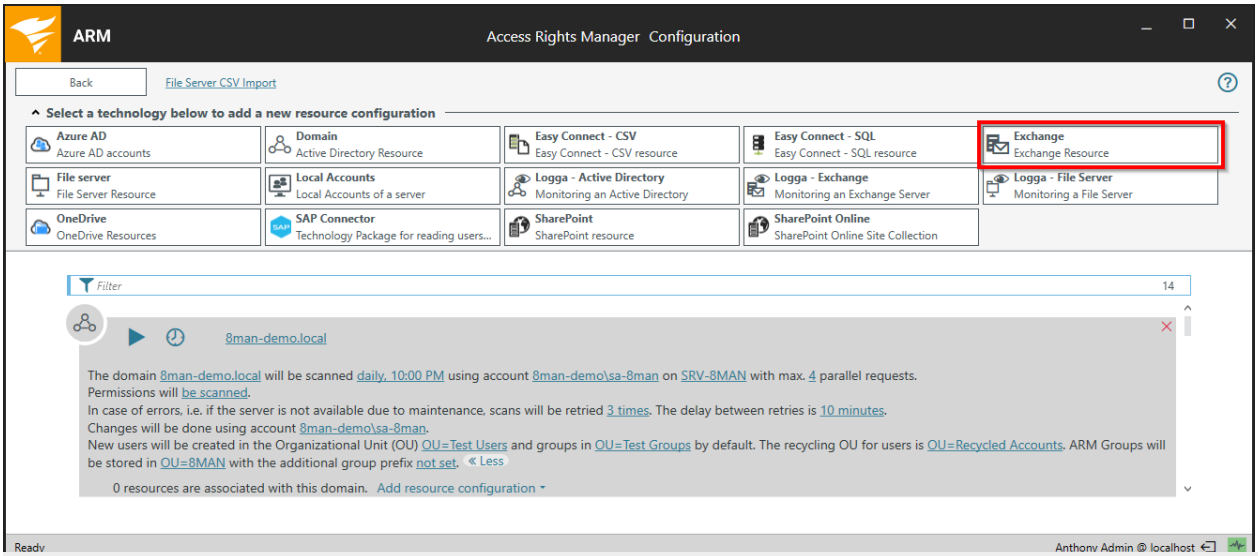
1. Start a power shell console with the credentials that are also used for the remote session. (CTRL+SHIFT+right-click on the PowerShell-Icon -> "Run as different user")
2. Create a credential object:
   ```
   $cred = get-credential
   ```
3. Create a SessionOption object (turn off all checks for the 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

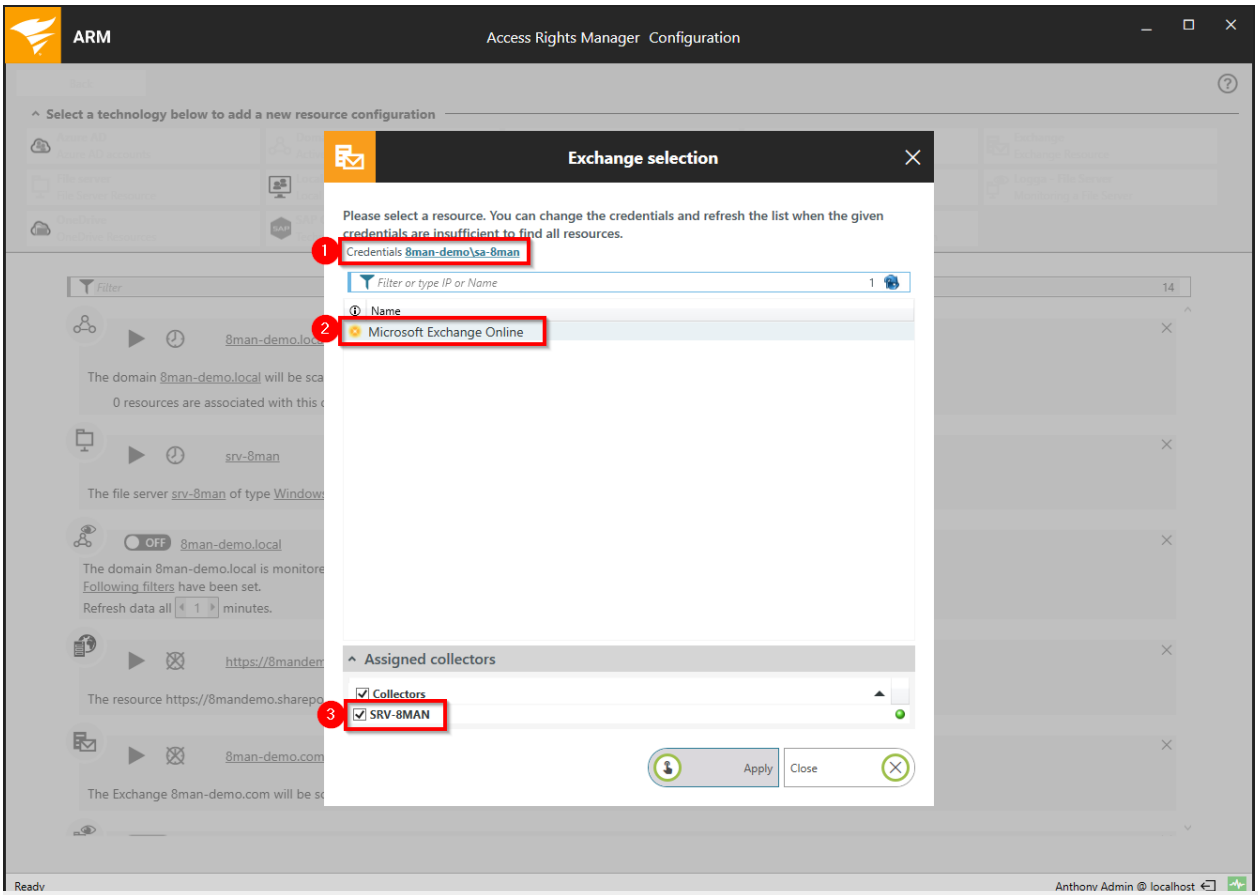


Select "Scans" from the home page of the configuration application.

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.

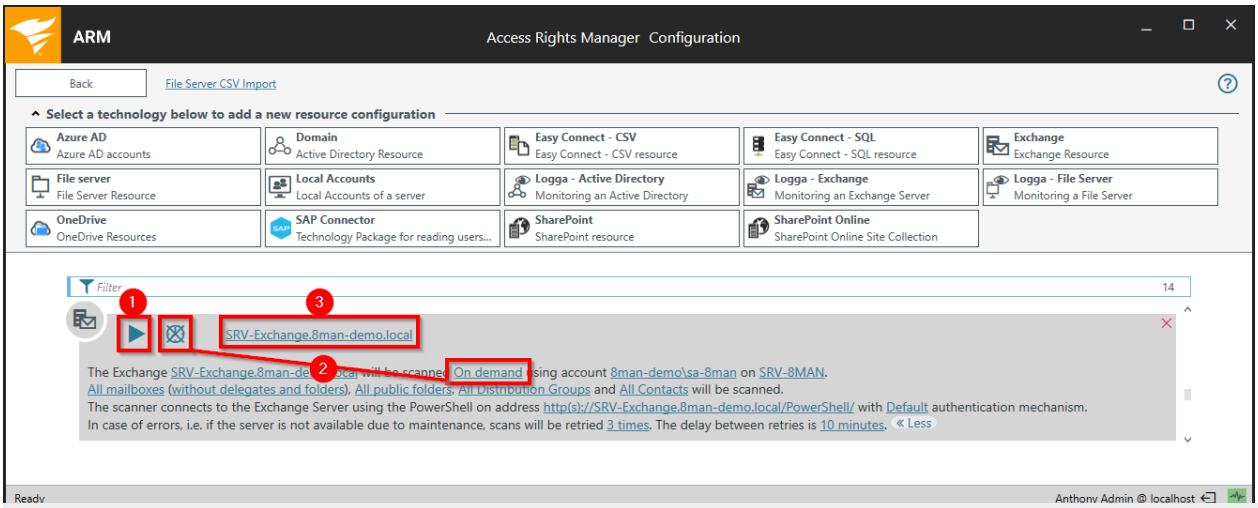
Special considerations for Exchange Online:

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.

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.

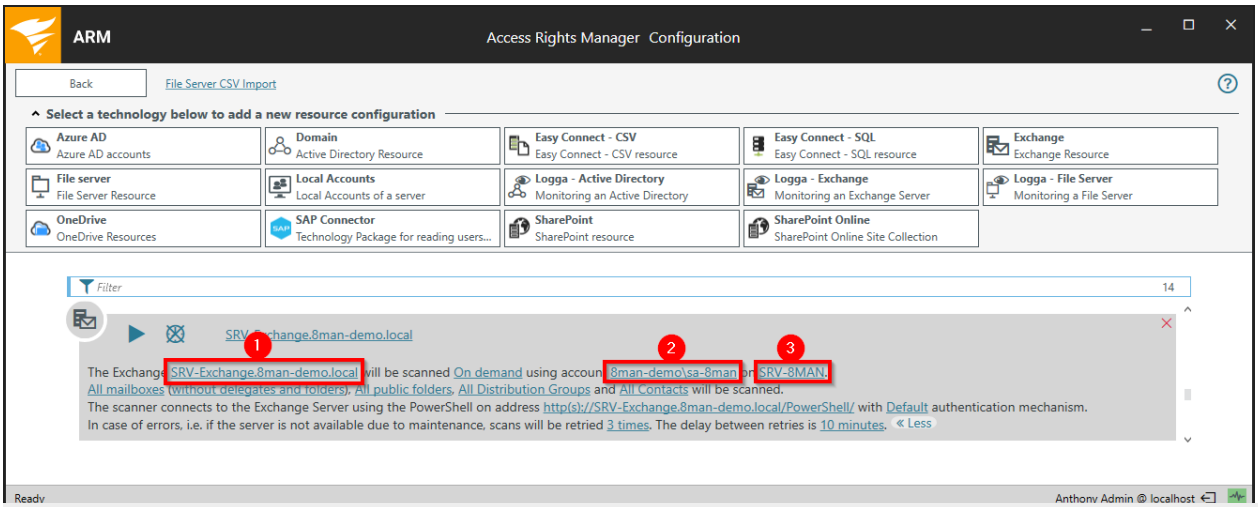
Customize an Exchange scan configuration



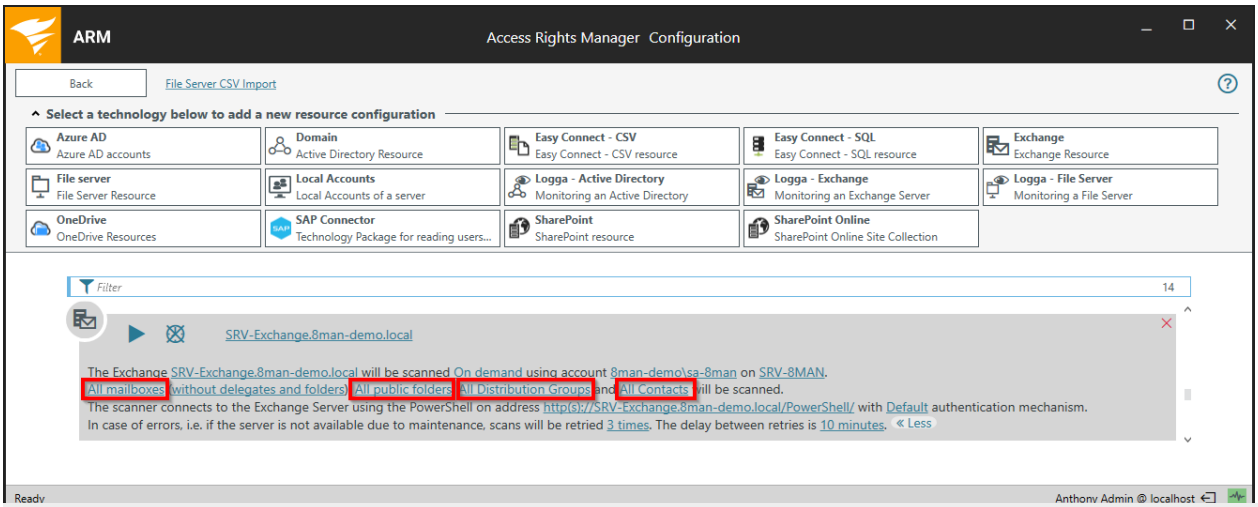
1. Start/cancel an Exchange Scan.
2. Schedule regular scans.

3. Change the name of the configuration.

The typical scan speed is around 10 elements per second.

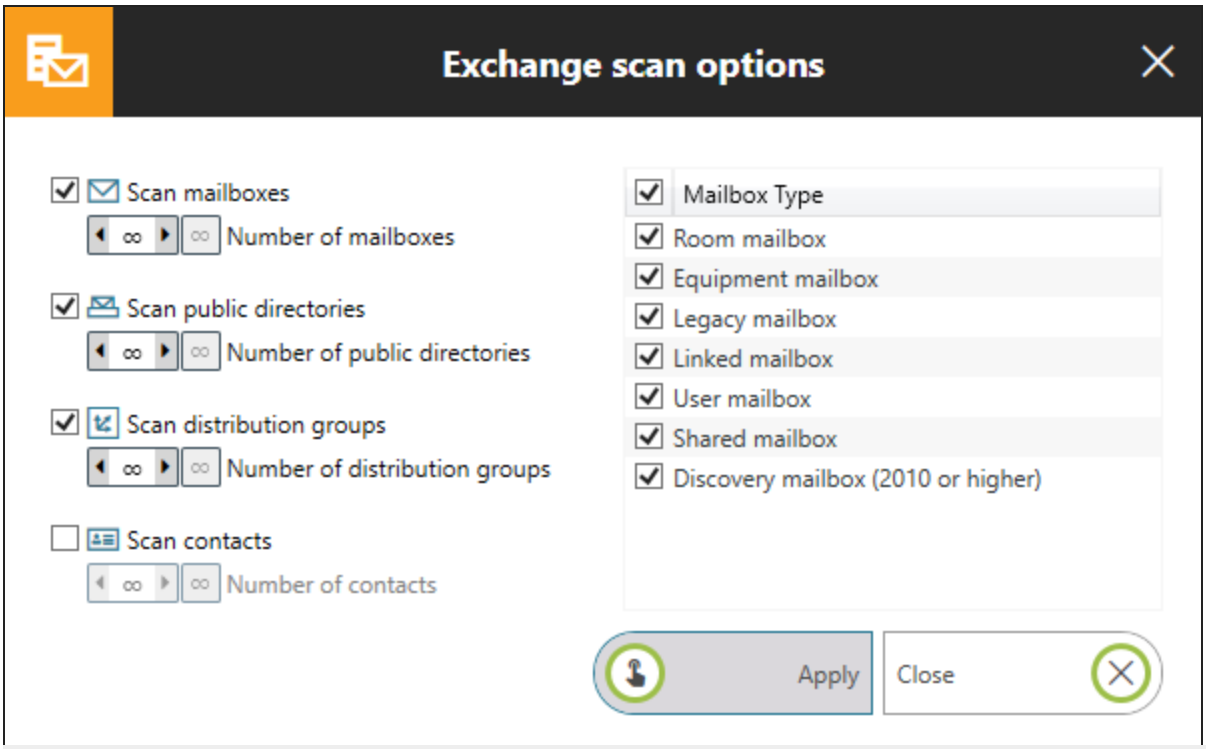


1. Change the Exchange Server that you want to scan.
2. Change the credentials that are used to execute the scan.
3. Switch the collector server. Please note that the collector server requires internet access when using Exchange Online.



Define the range of the scan.

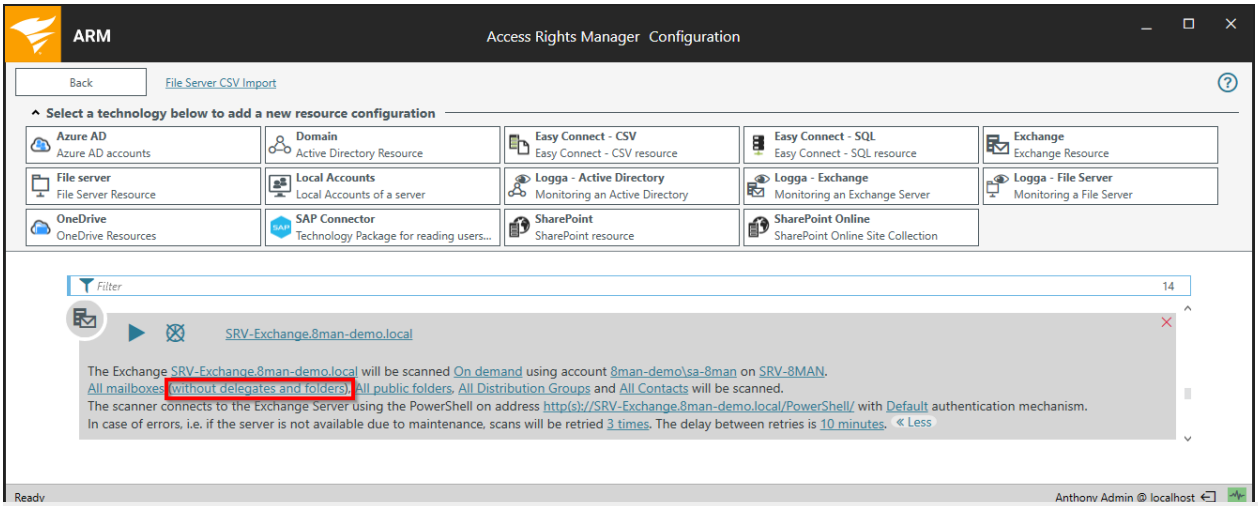
All the links lead to the following dialog:



If you select only a subset of folders for readable public folders, then no statistical data will be available.

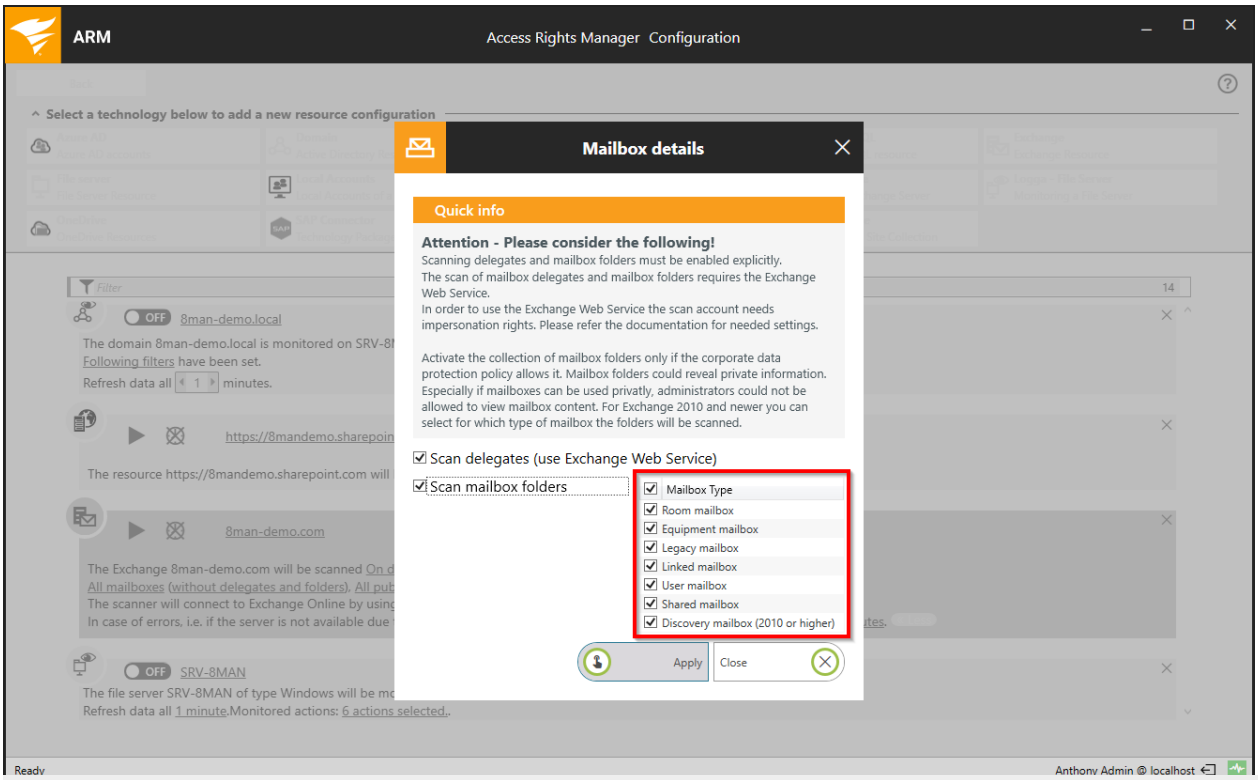
Administrative permissions to public folders are not available (since Exchange 2013).

A filter is applied to the mailbox property "RecipientTypeDetails", to select the mailbox type.



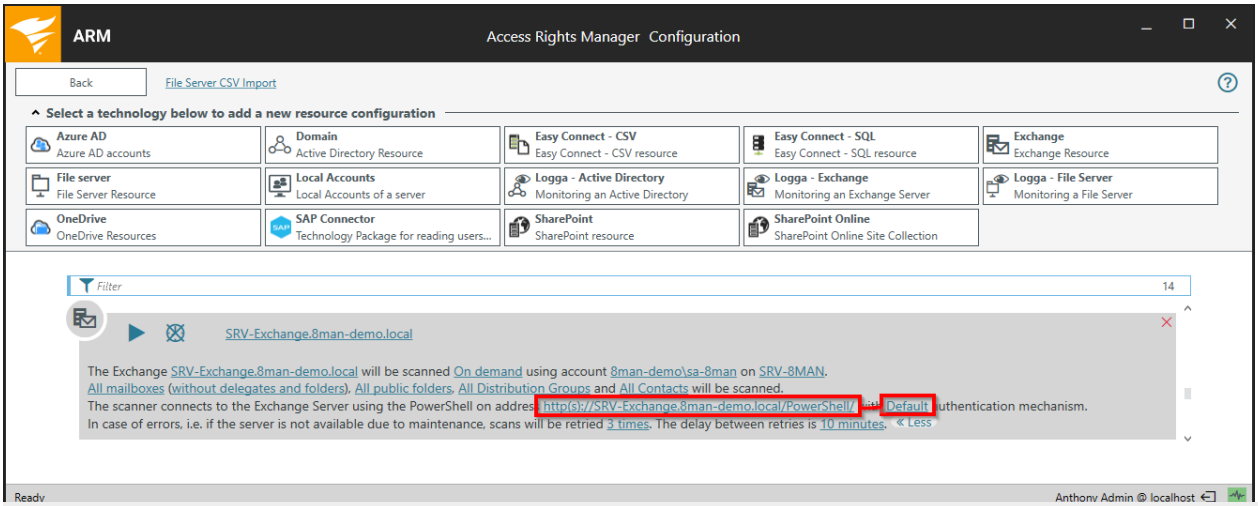
You can determine if substitution rules and mailbox folders are read.

Please note that Exchange Web Services - Impersonation is used.

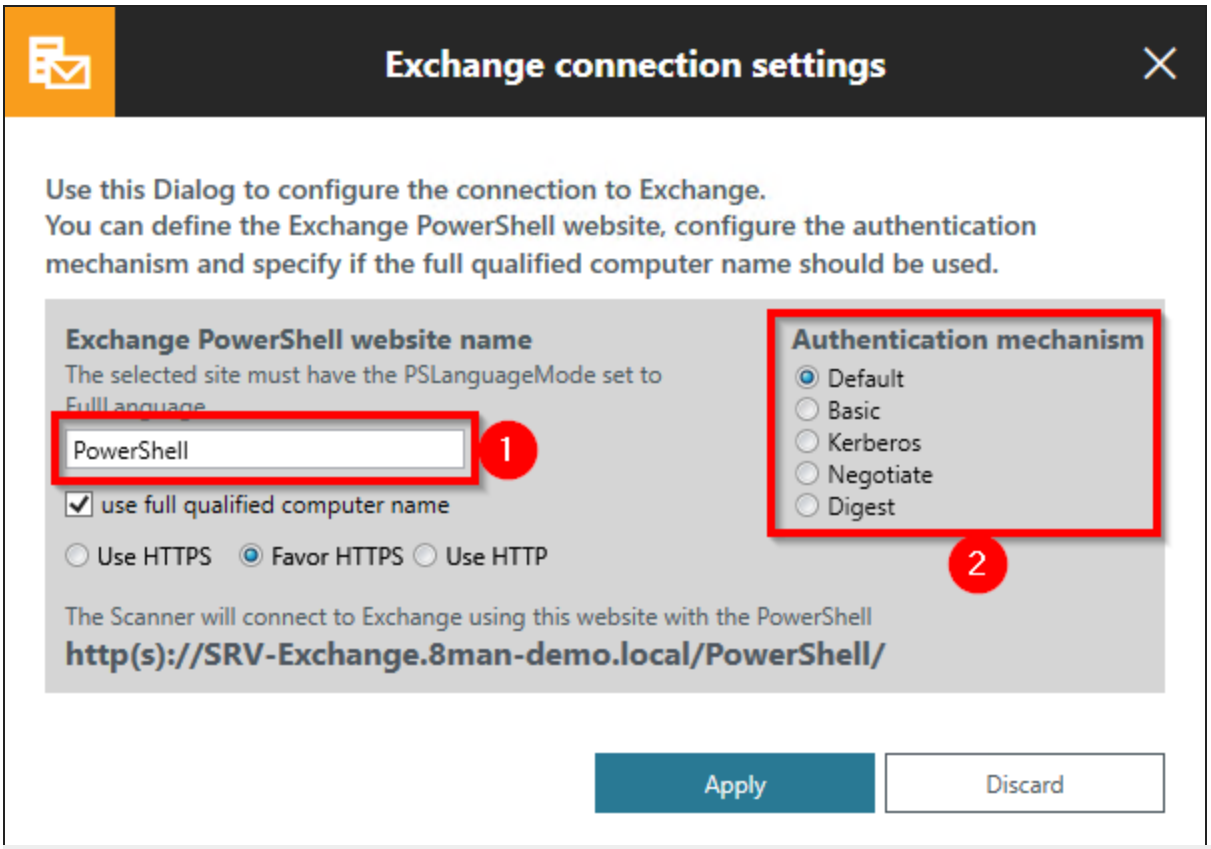


Determine the range in which mailbox details are read with Exchange Web Service (EWS).

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.

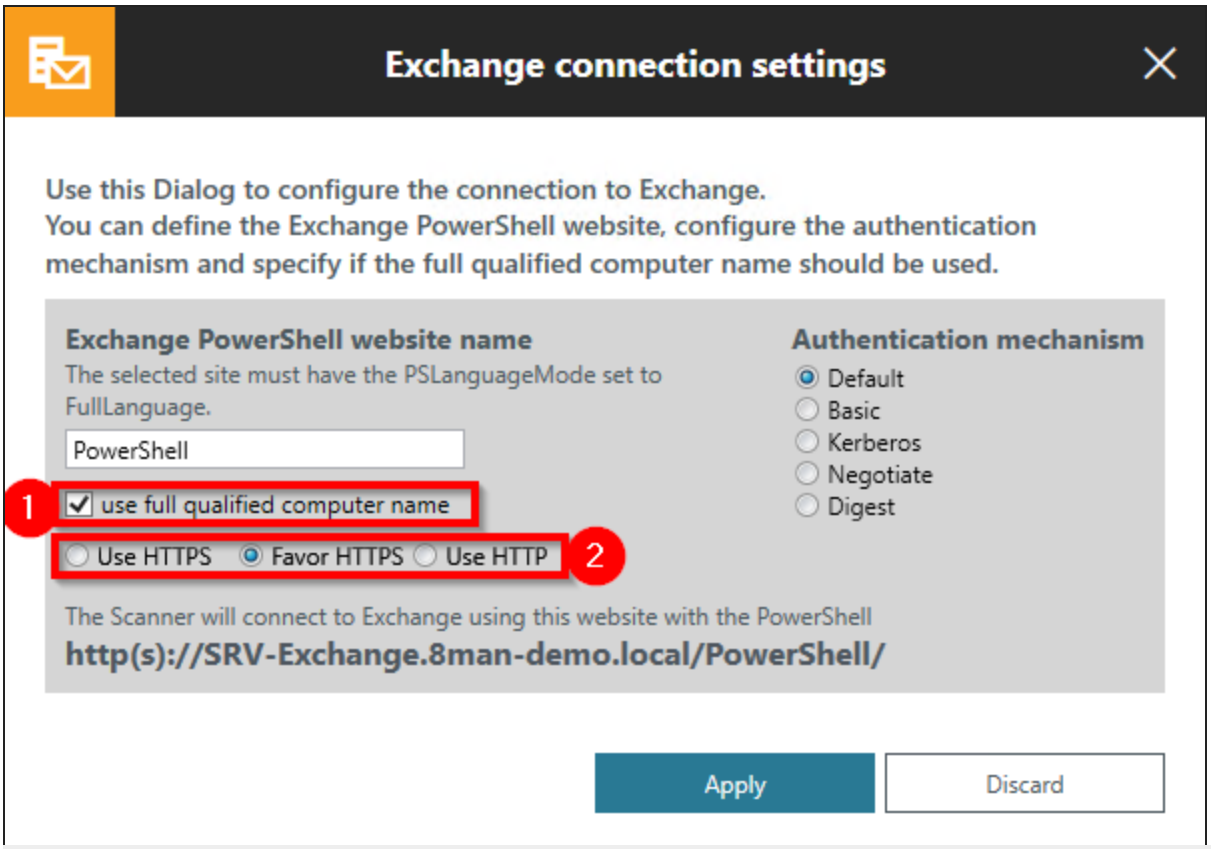


Click one of the links to configure the connections settings for the Exchange scan.



The 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".



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. (© 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.

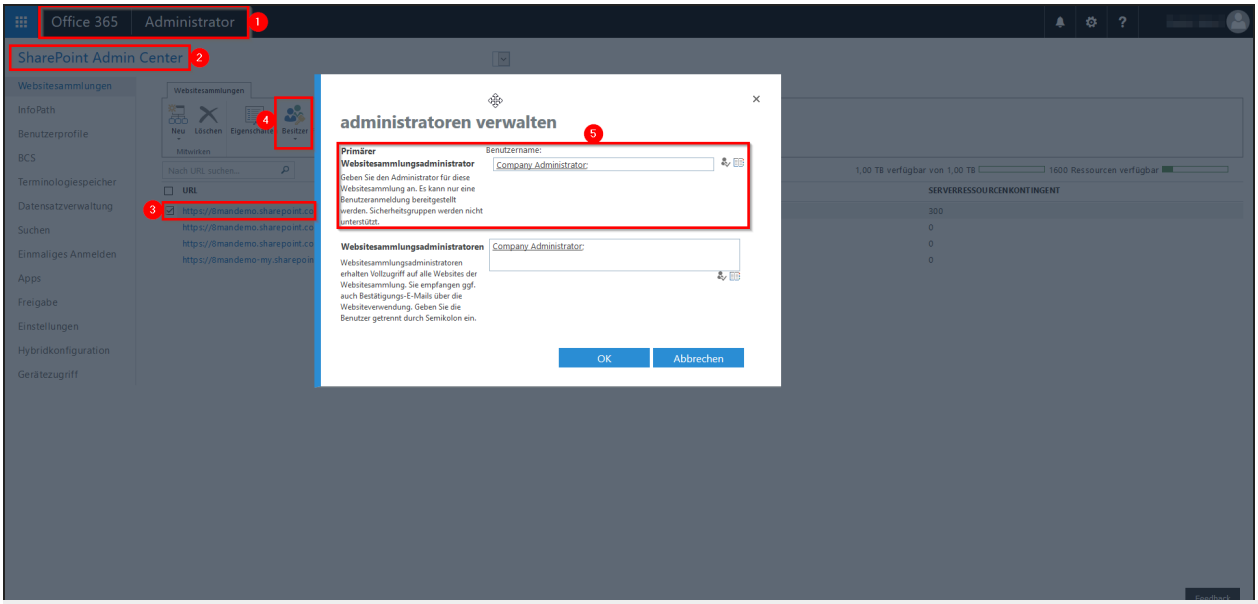
Scan Account

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

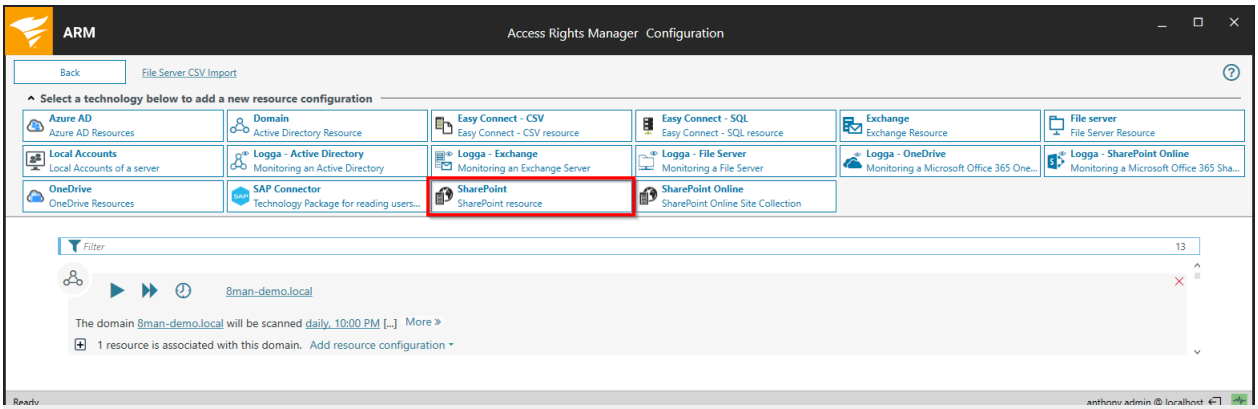
Identify the primary site collection administrator in SharePoint Online



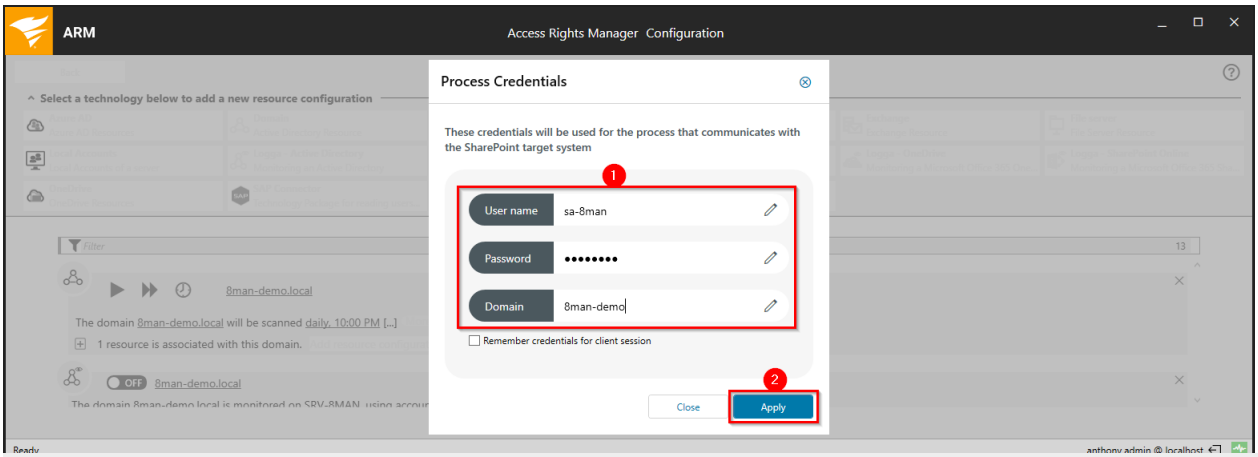
1. Log into your Office 365 environment as an administrator.
2. Go to the SharePoint Admin Center.
3. Select the collection to be scanned (set the checkmark).
4. Click Owner-> Manage Administrators.
5. You will see the primary site collection administrator.

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 ressource.

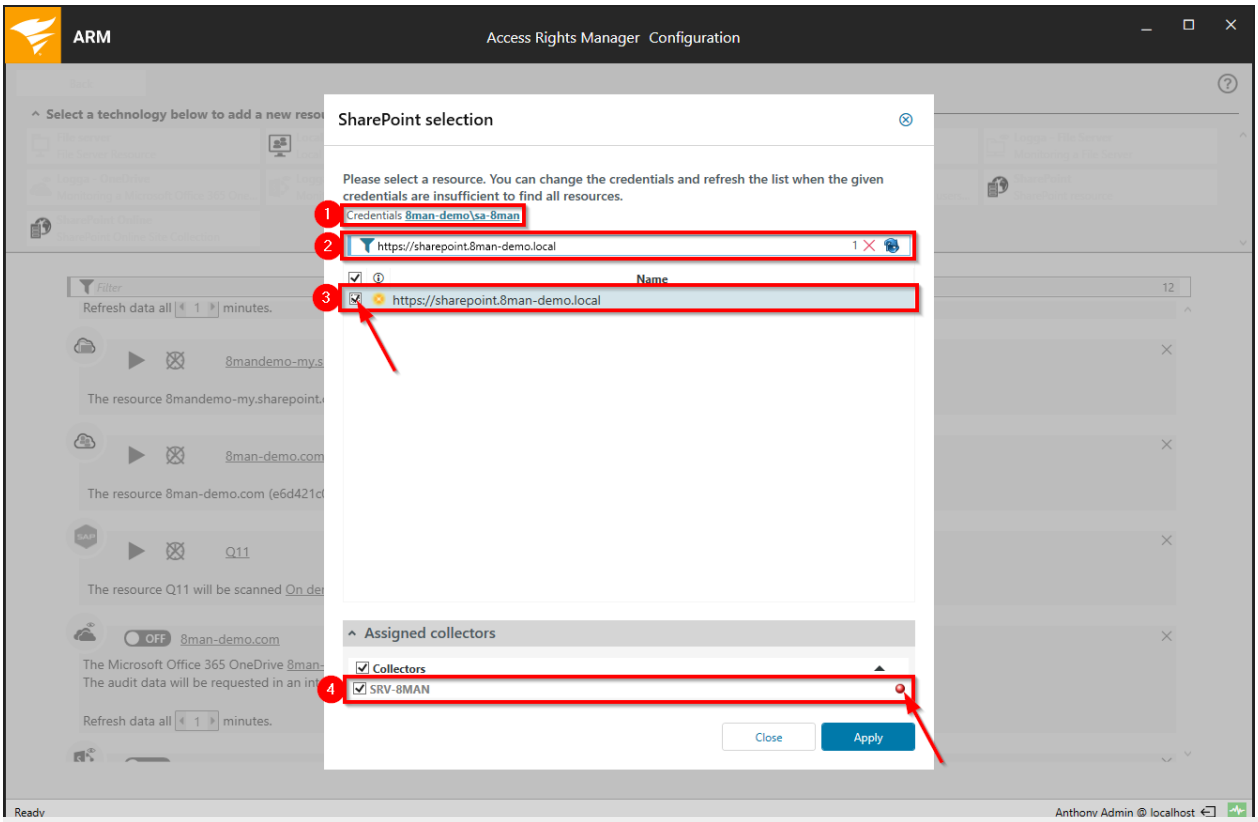


1. Specify the credentials for the "Process Account". We recommend to use the ARM service account.

> 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.



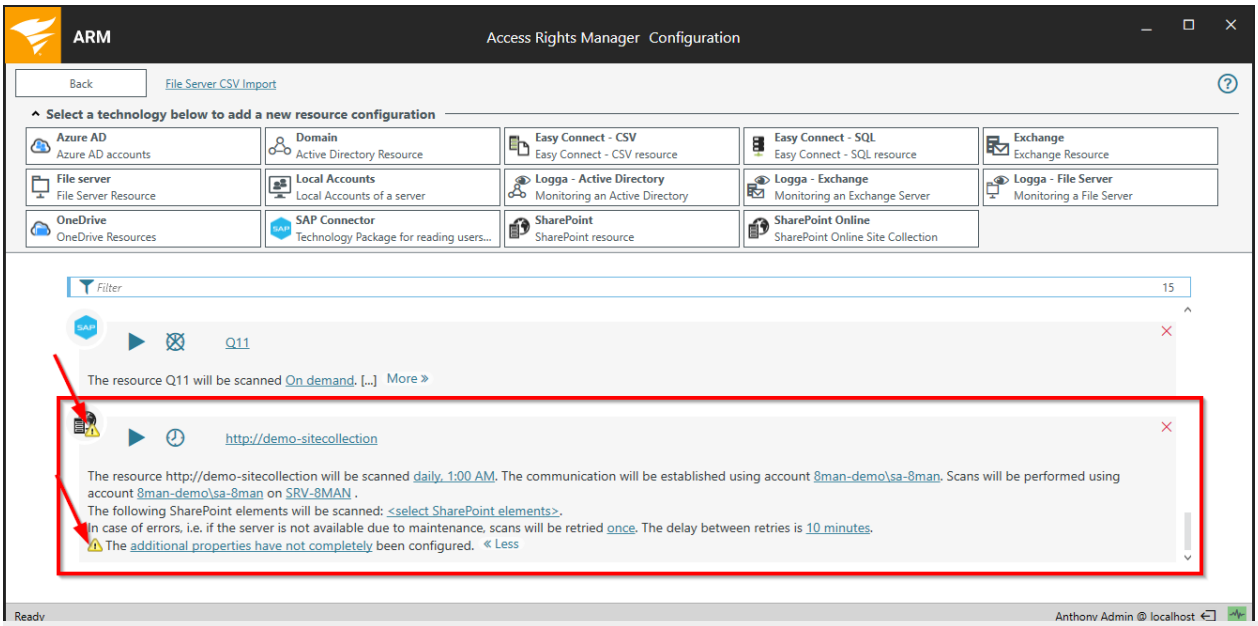
1. If necessary, change the account used to read the SharePoint resources. Preset is the "Process account".
2. Specify the SharePoint server name (recommended) or a URL of a SharePoint element. Confirm your entry with the ENTER key.

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.

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.

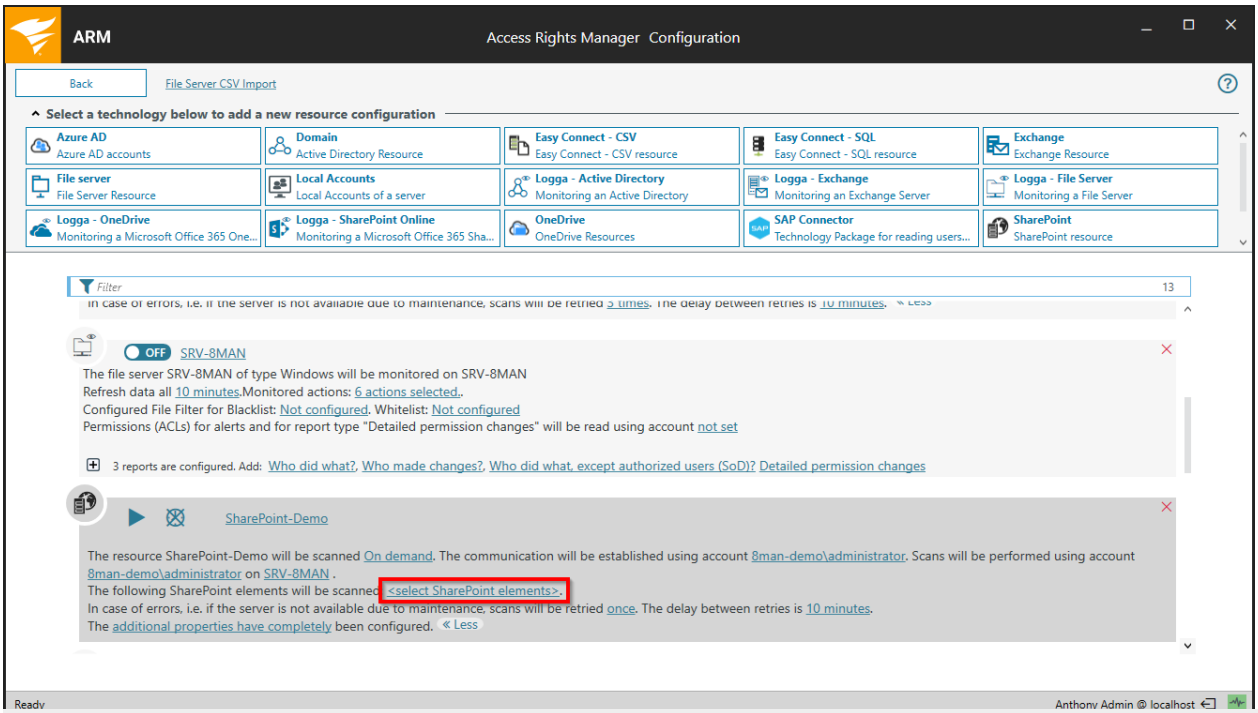


You have created a new SharePoint configuration.

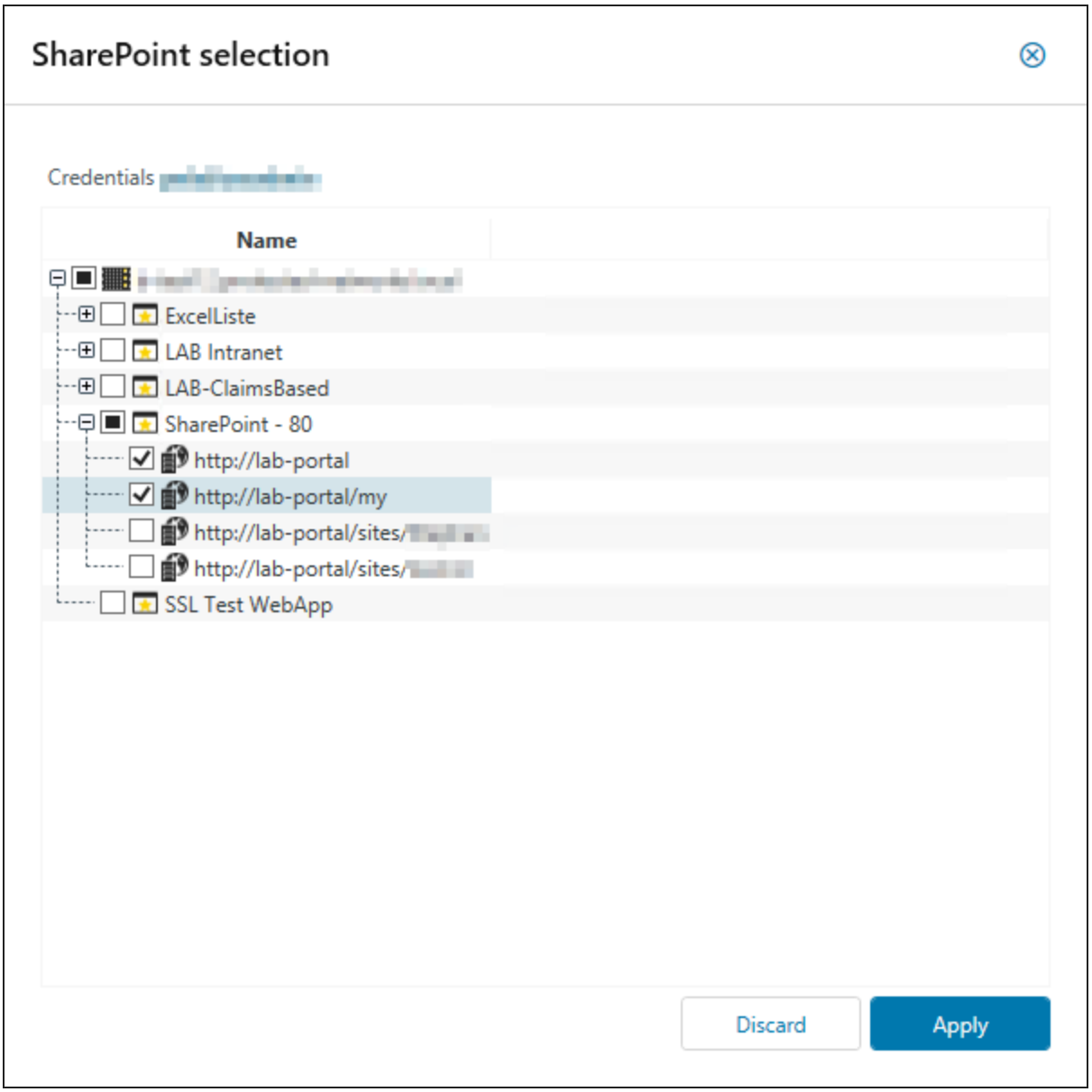
The warning indicates that you must configure additional properties before you can successfully perform a scan.

Select SharePoint on-premise elements to be integrated

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



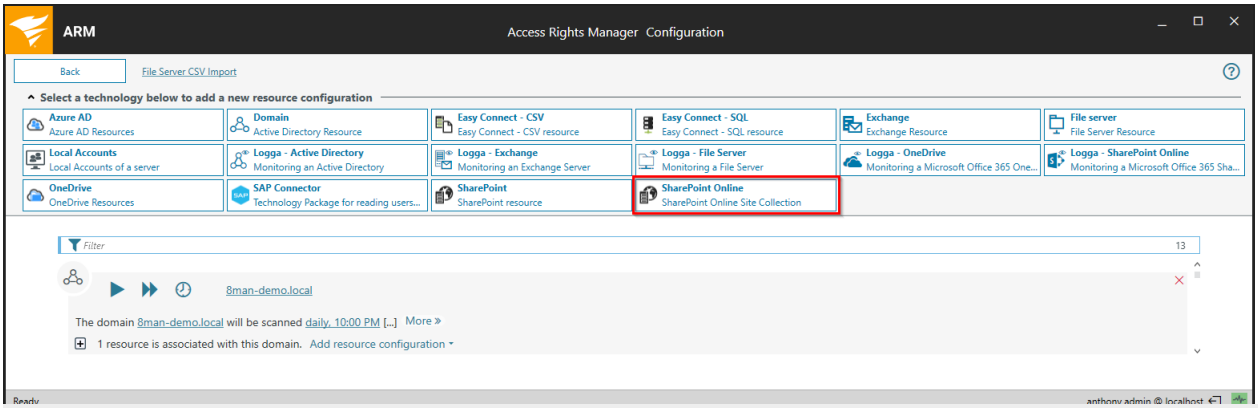
Click on "Select SharePoint elements" in the SharePoint configuration.



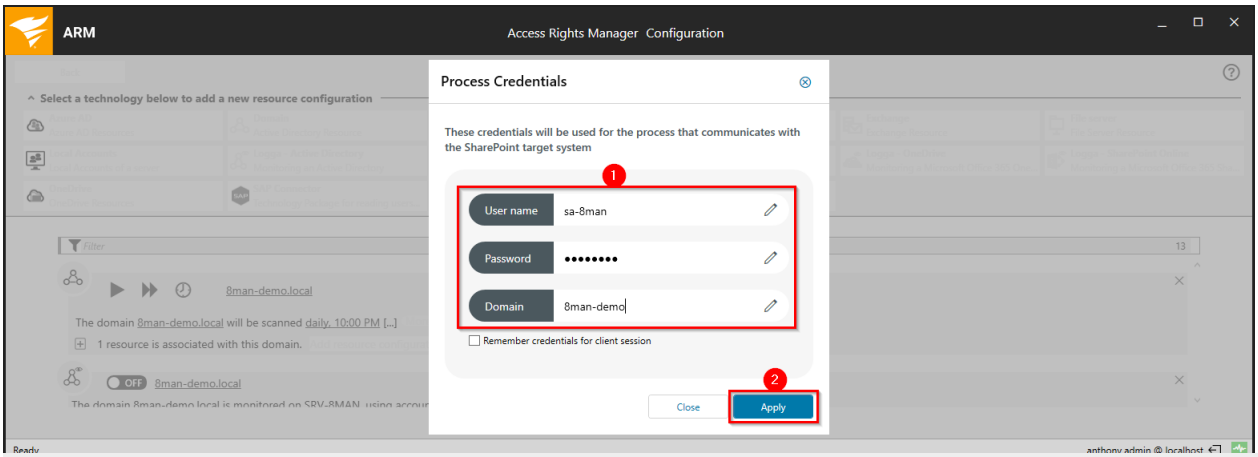
Select the elements to be integrated.

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 ressource.

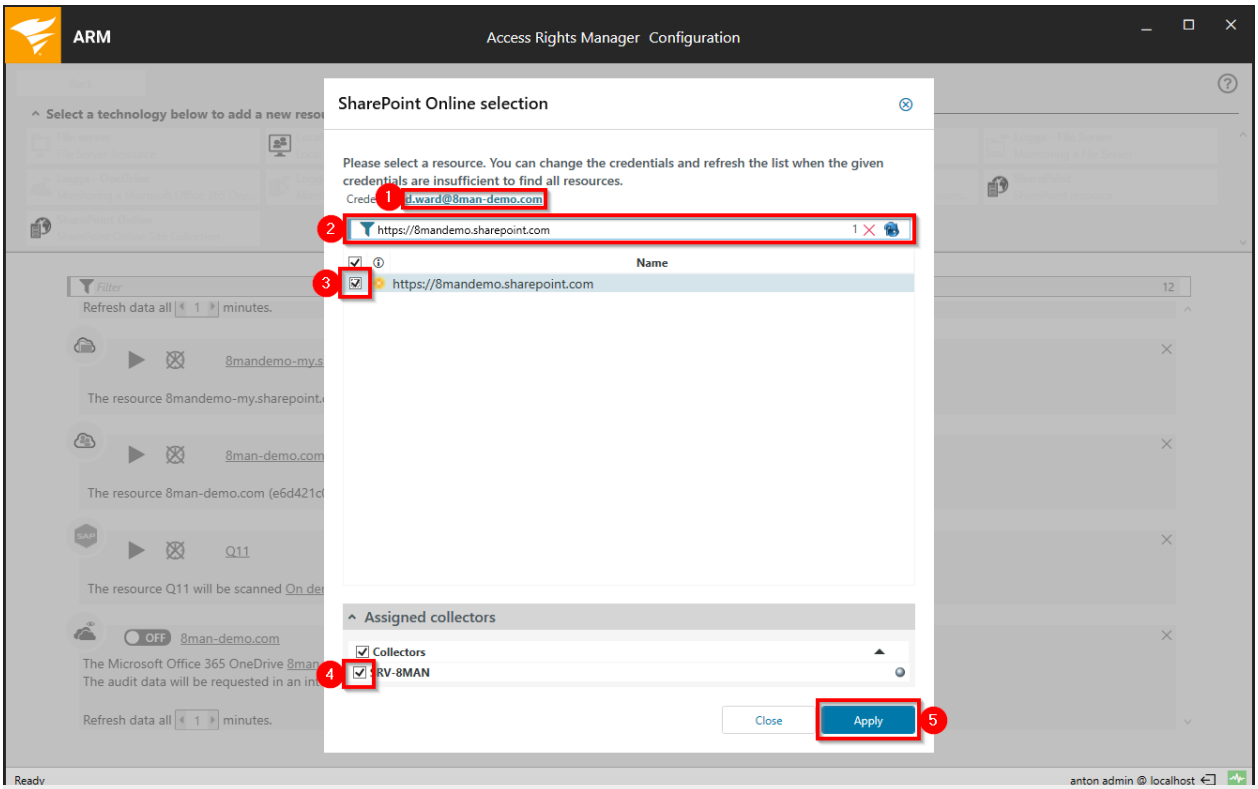


1. Specify the credentials for the "Process Account". We recommend to use the ARM service account.

> 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.

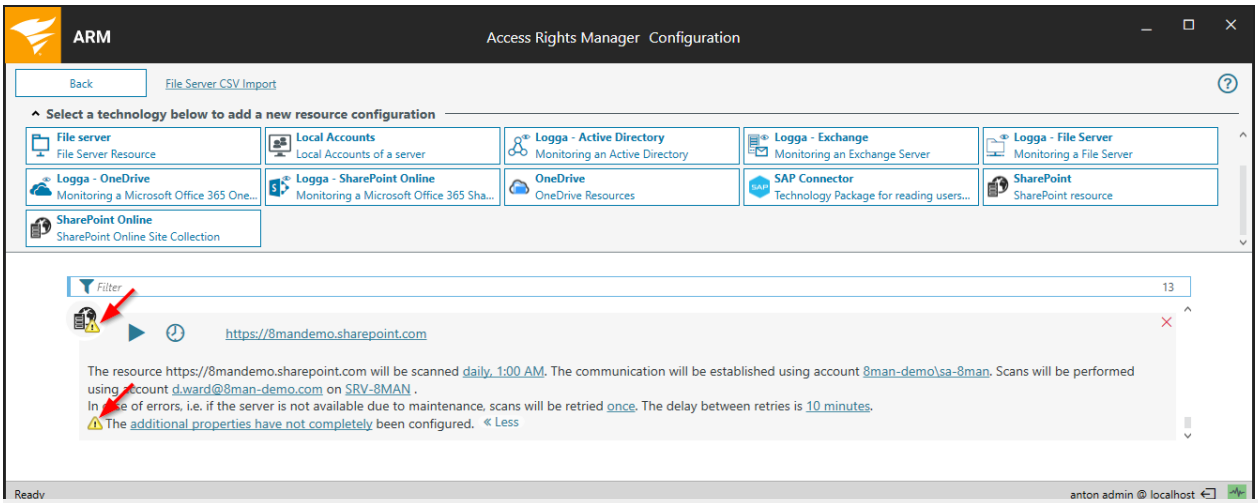
⚠ Please be careful, the entry is not checked for validity at this point.

ⓘ 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.

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

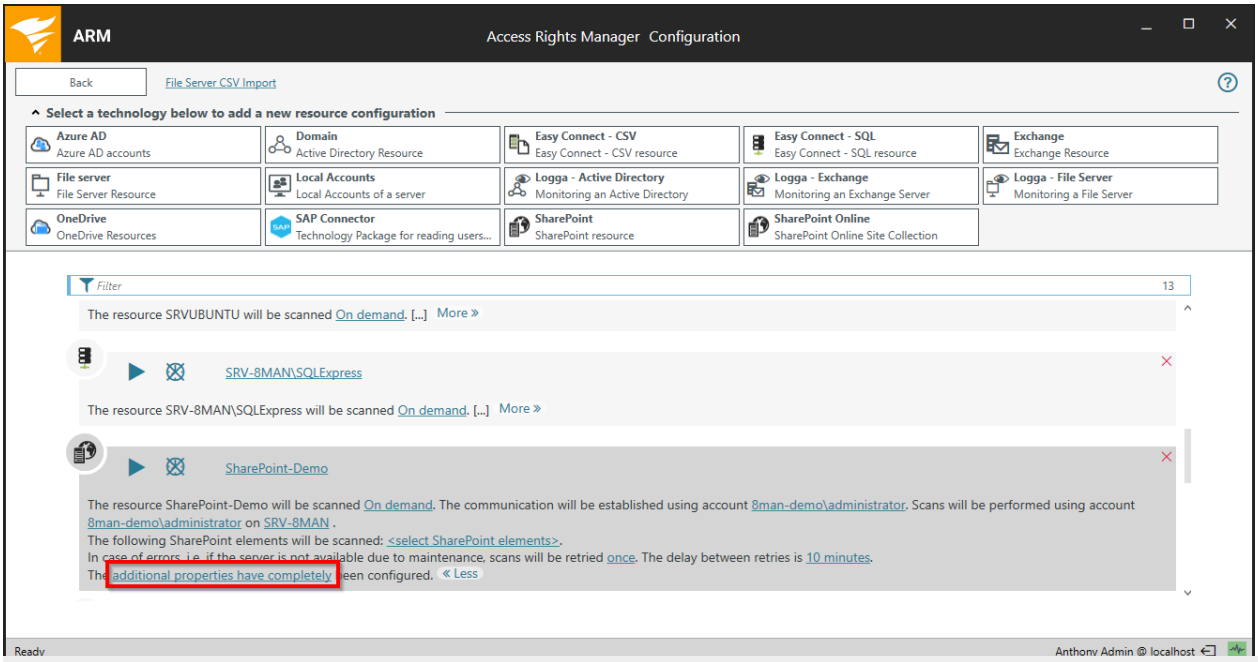
5. Click Apply.



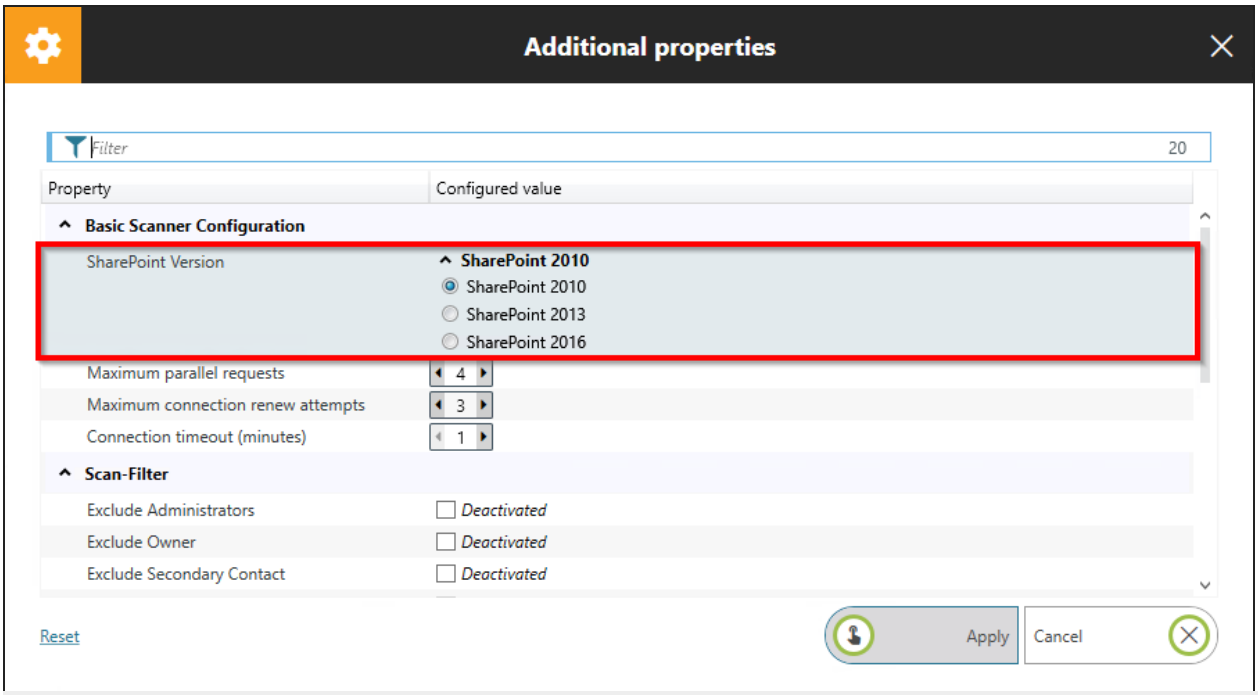
You have successfully created a SharePoint Online scan configuration. The symbols (arrows) indicate that the additional options still need to be set. This procedure is identical for SharePoint Online and SharePoint on-premise and is described in the chapter Configuring additional SharePoint properties.

How to customize a SharePoint Online scan configuration is described in the chapter Customize a SharePoint Scan Configuration.

Configure additional properties



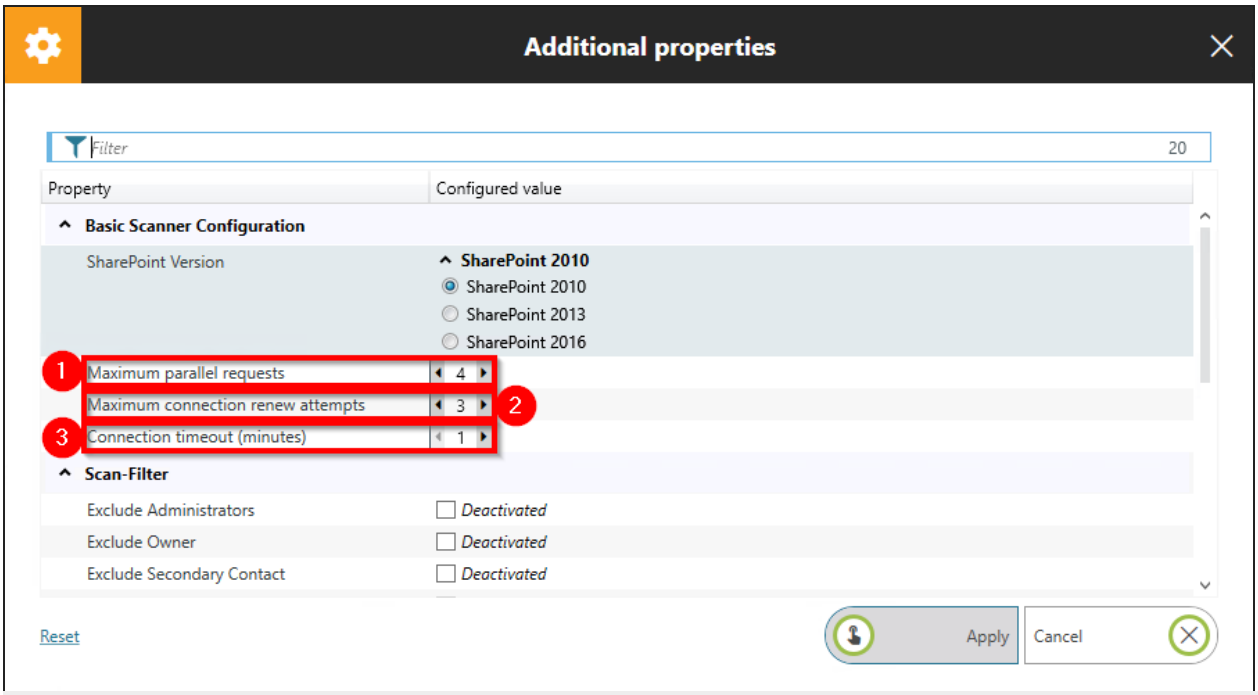
Click the link.



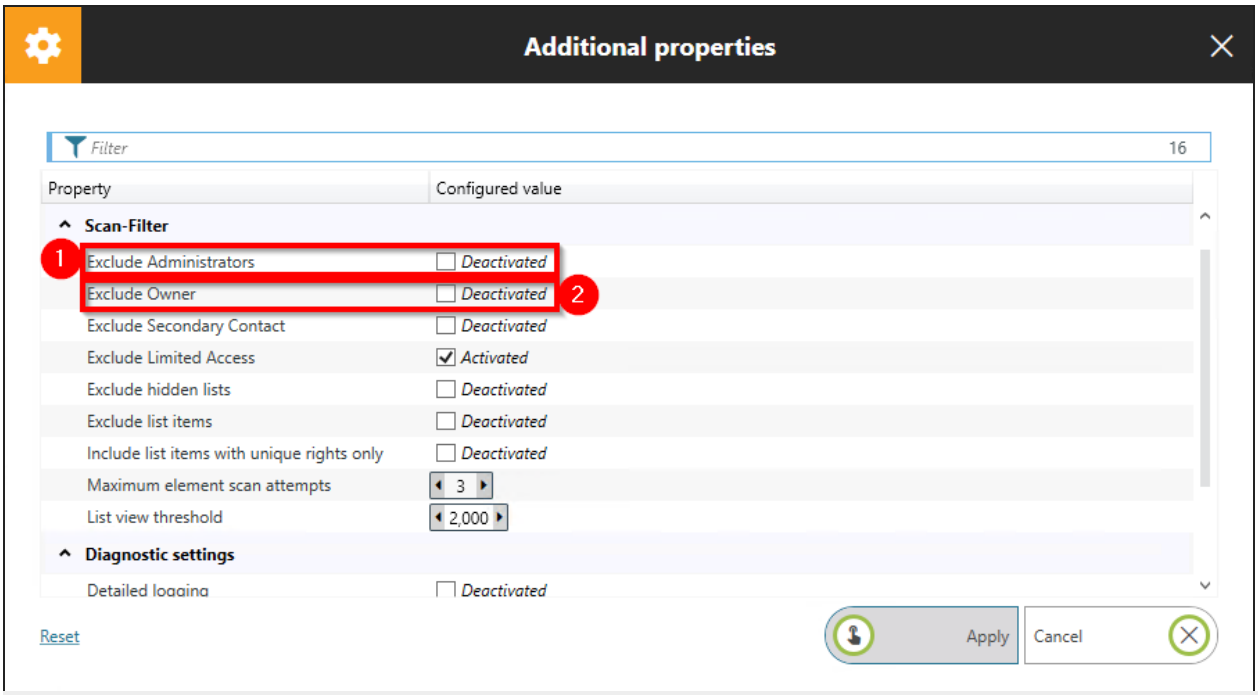
Select the SharePoint version.

For SharePoint 2019 please select SharePoint 2016.

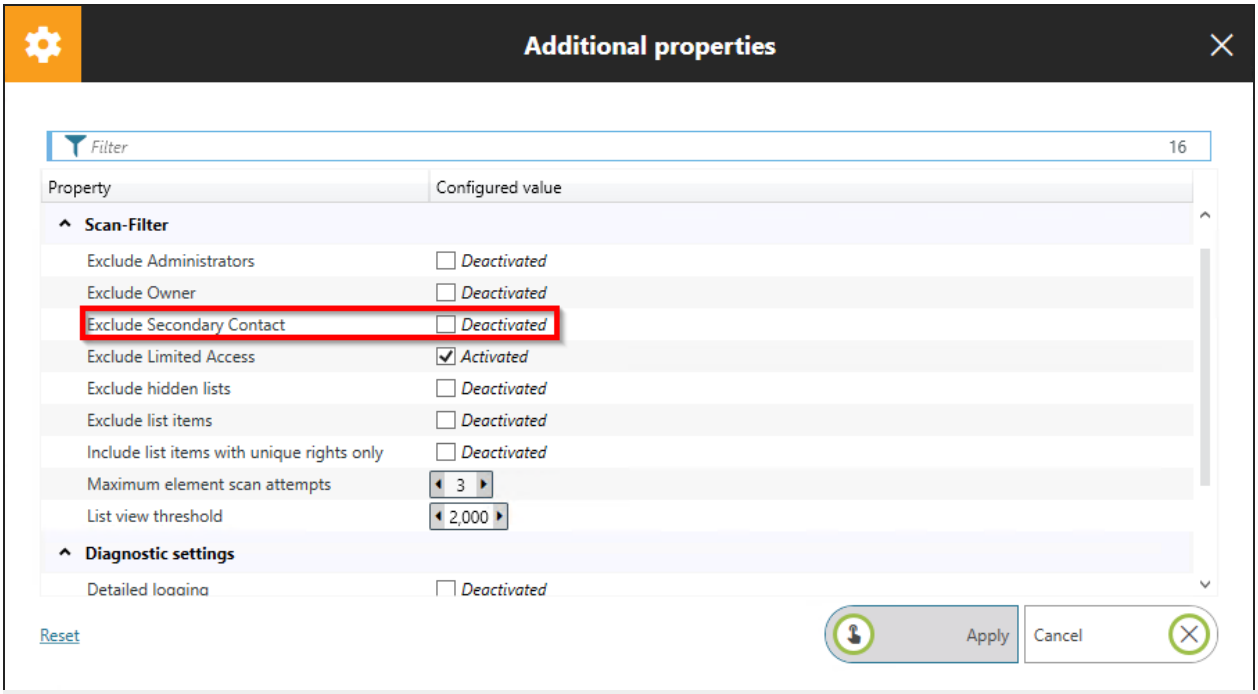
To communicate with the SharePoint system, ARM uses Microsoft components that are specific to the version of the SharePoint system that is used. Specifying the correct SharePoint version ensures that all information is shared correctly with the SharePoint system. If the configured version of SharePoint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



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



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.

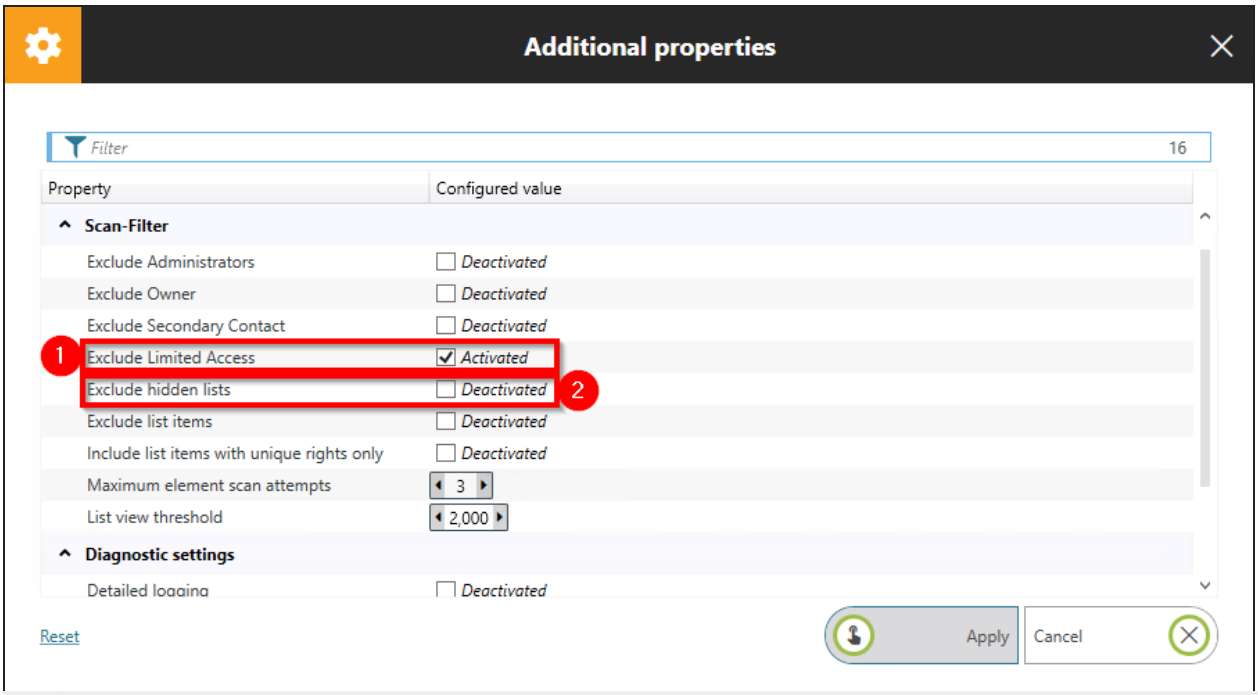


Option enabled:

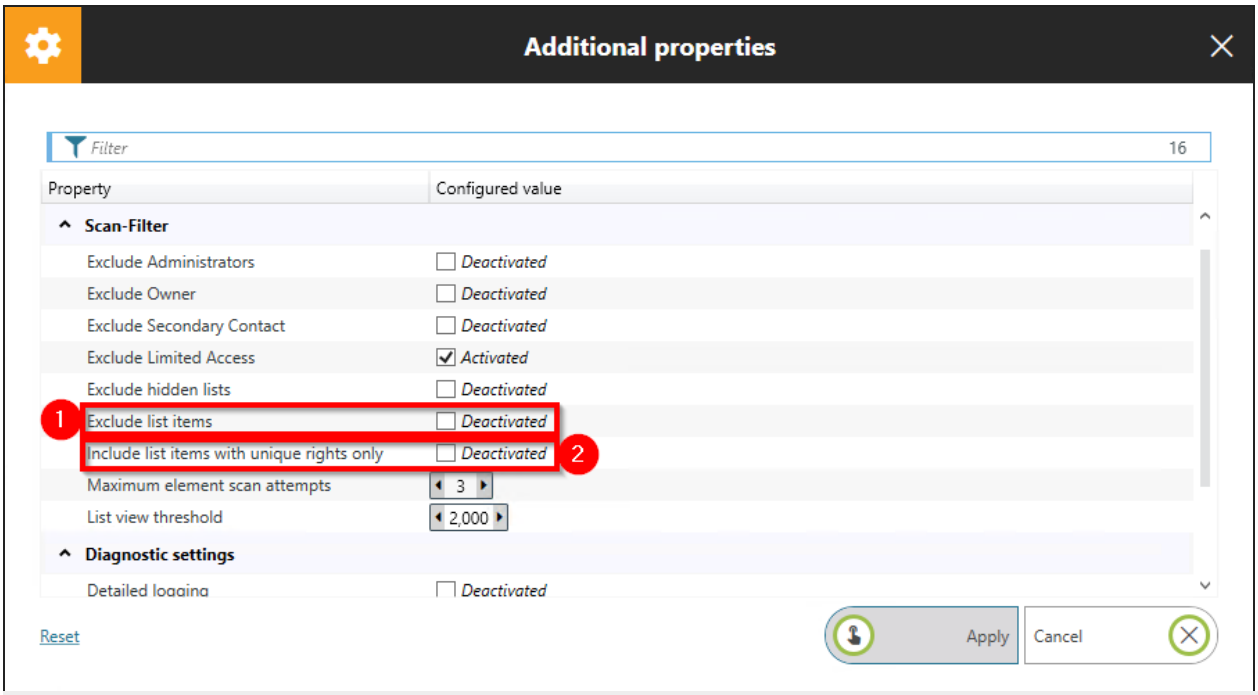
ARM excludes secondary contacts from the scan. They are not available in views and reports.

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

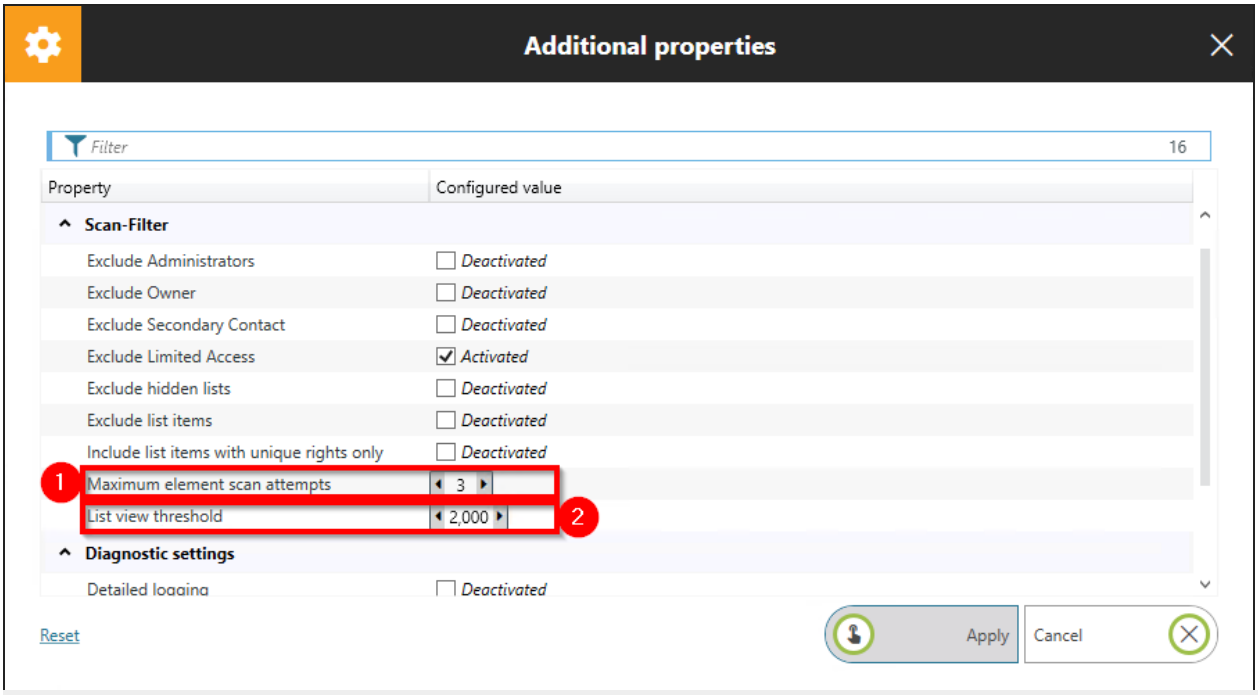
This option is not effective for SharePoint 2010. Microsoft does not provide the secondary contact information in this release.



1. **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.
2. **Option enabled**: ARM excludes hidden lists from the scan. They are not available in views and reports.



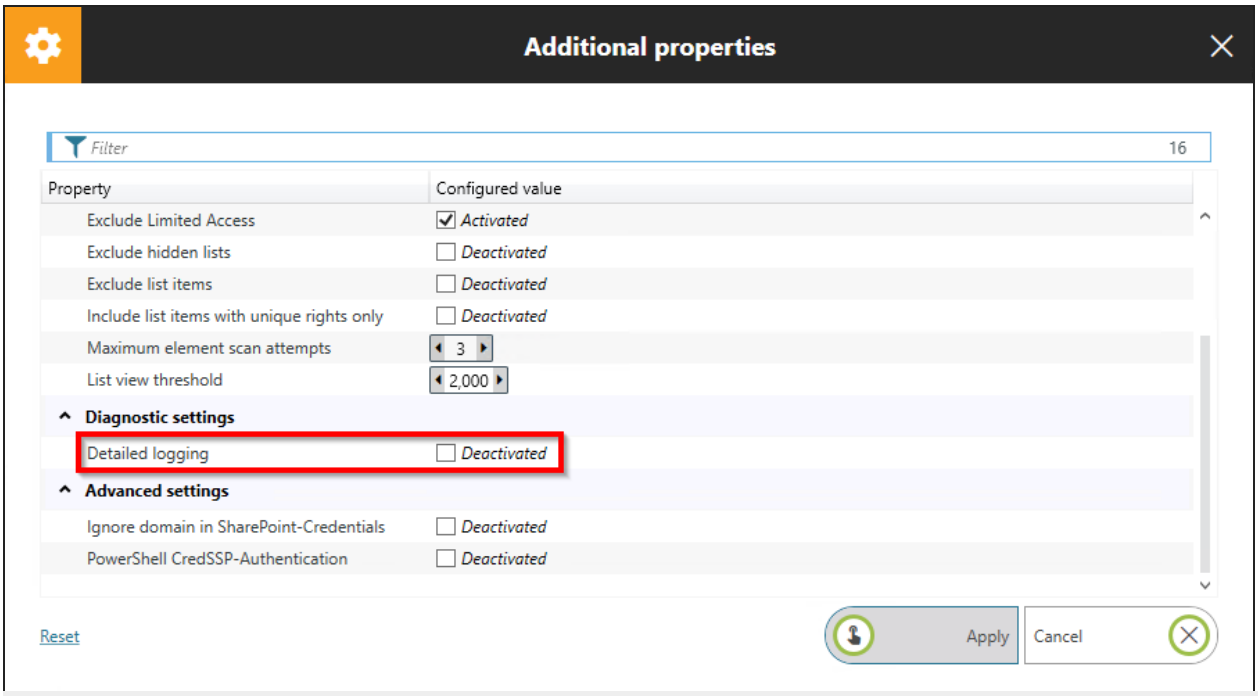
1. Option enabled: ARM excludes list items from the scan. They are not available in views and reports.
2. Determine whether only list elements or documents with specific permissions (interrupted inheritance) will be scanned.



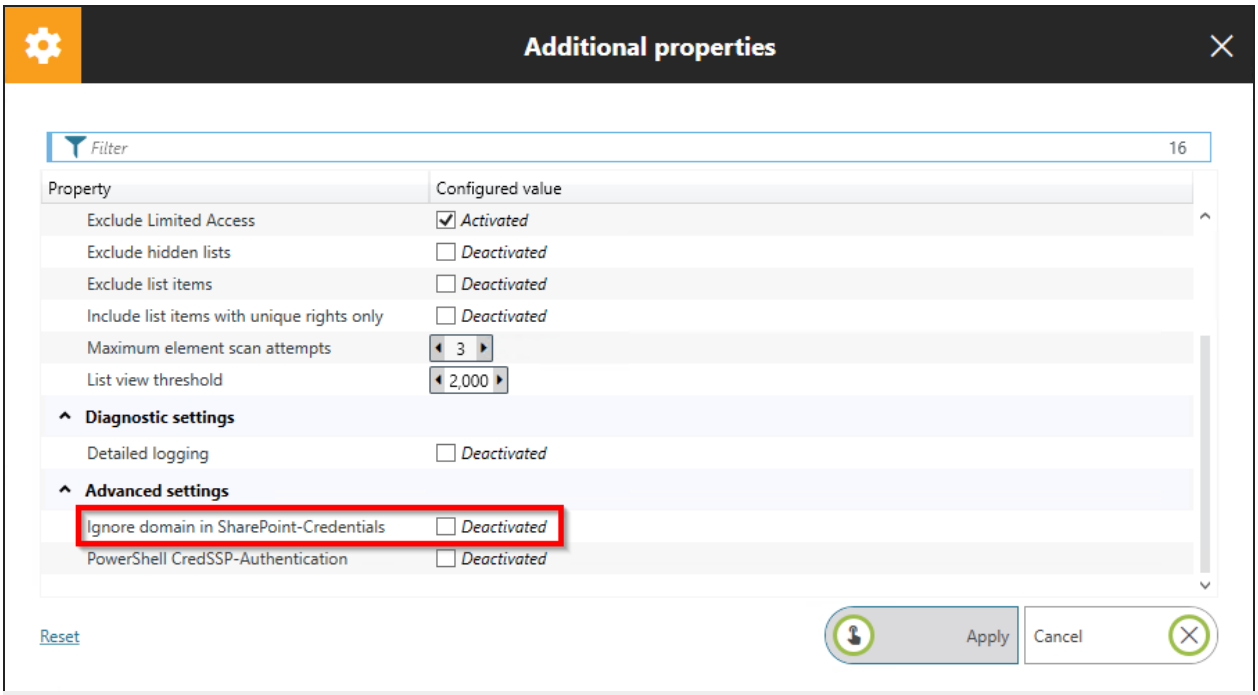
1. Determine the maximum number of attempts after which the scan of a specific SharePoint object

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.

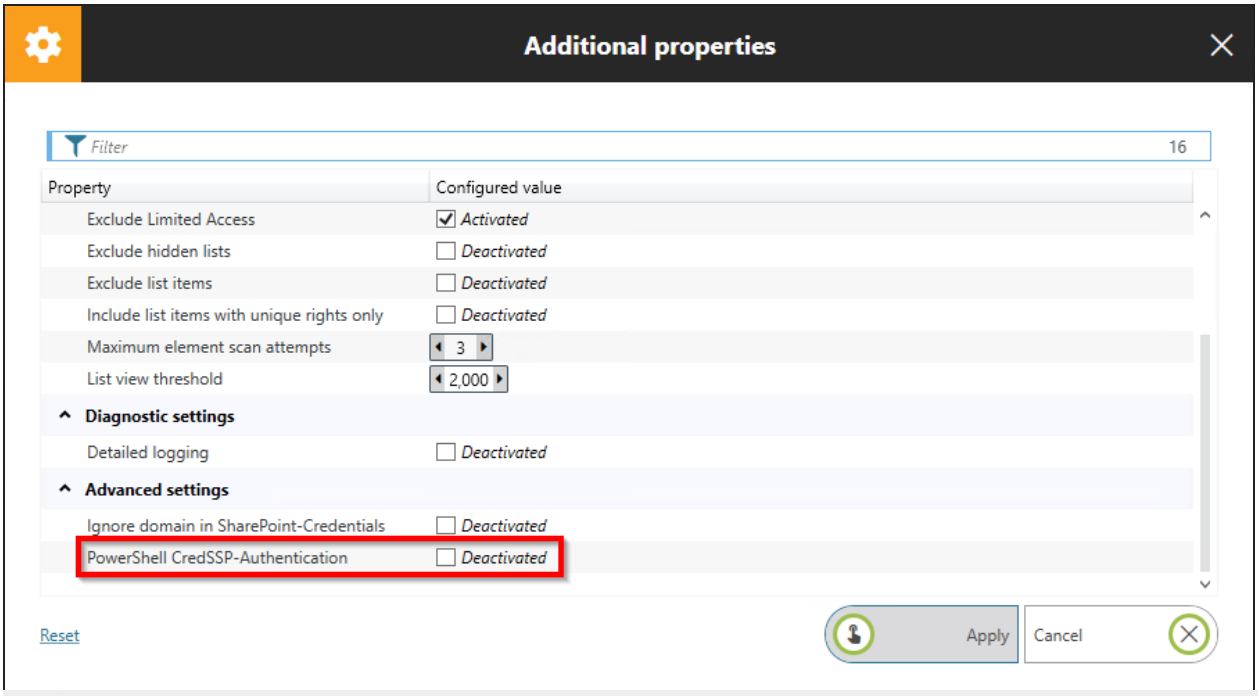


Enable the option for extended error analysis only. If this option is enabled, the scan speed will slow down and the size of the log file of the ARM server will increase faster.



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.



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

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

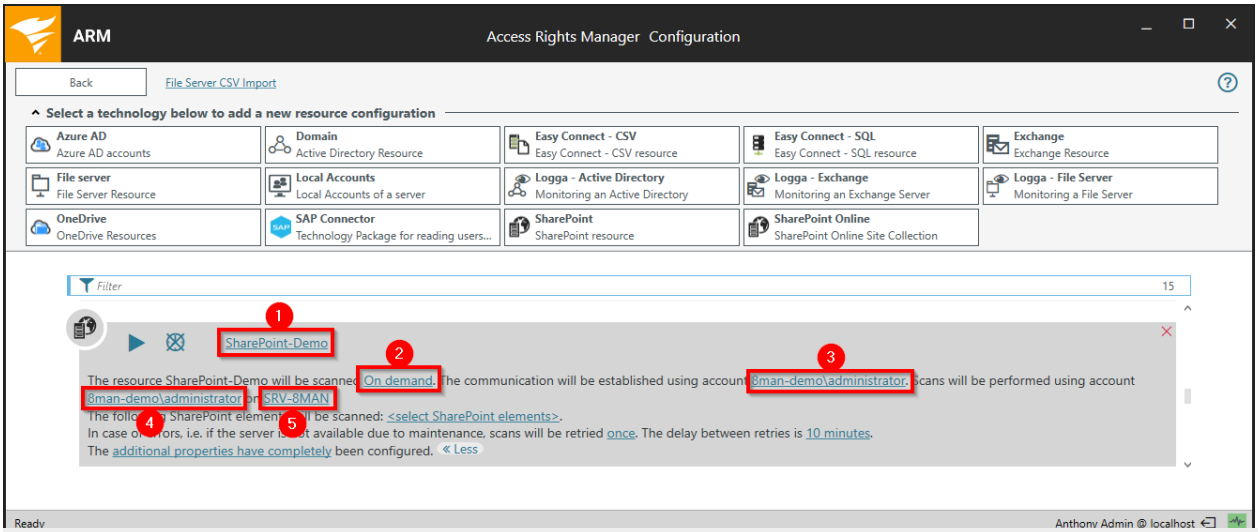
1. Start the SharePoint Management Shell with local administrator privileges.
2. Activate Remoting for PowerShell
   `Enable-PSRemoting -Force`
3. Activate MultiHop support in WinRM
   `Enable-WSManCredSSP -Role "Server" -Force`

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

> 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`

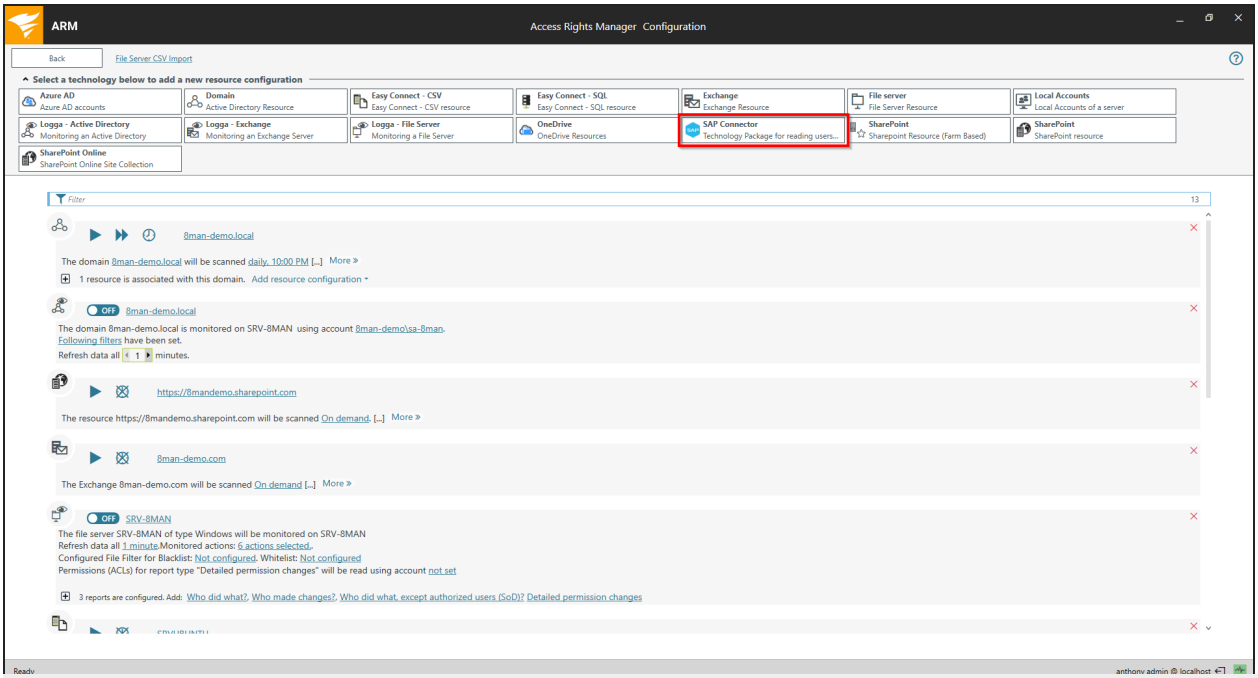
`sapnco.dll`

The components are contained in the downloaded package.

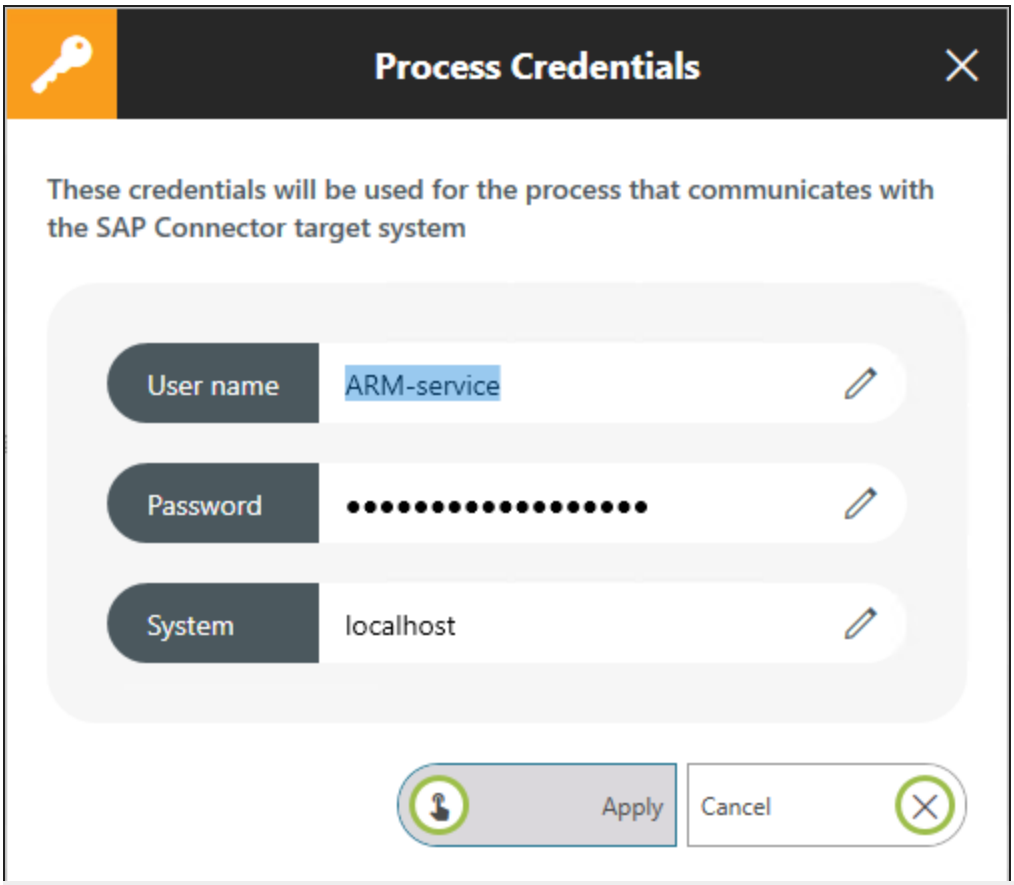
Copy the missing files to the following target directory on the ARM server:

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

Add an SAP scan



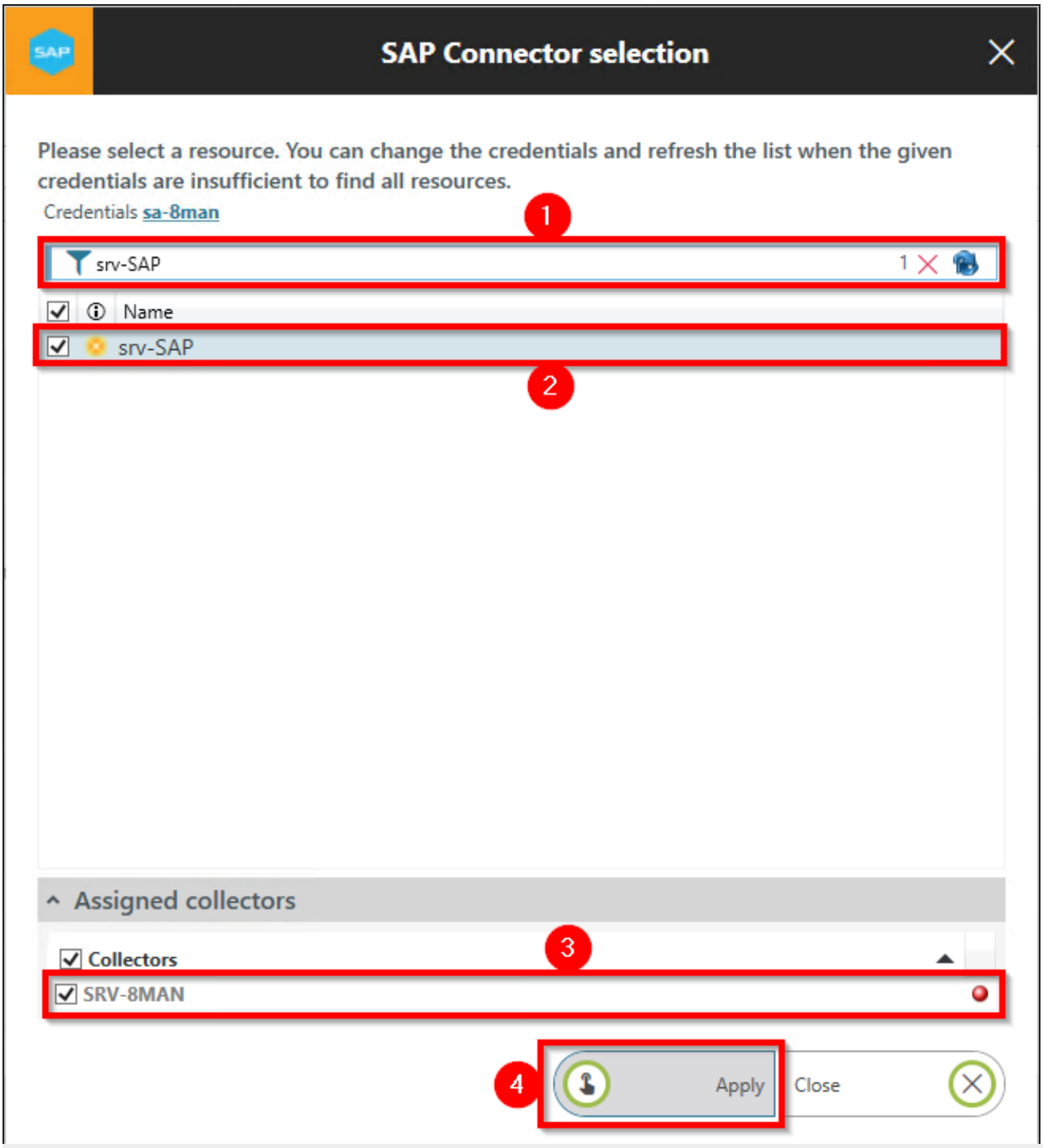
In the ARM Configuration Application click Scans > SAP Connector to add an SAP resource.



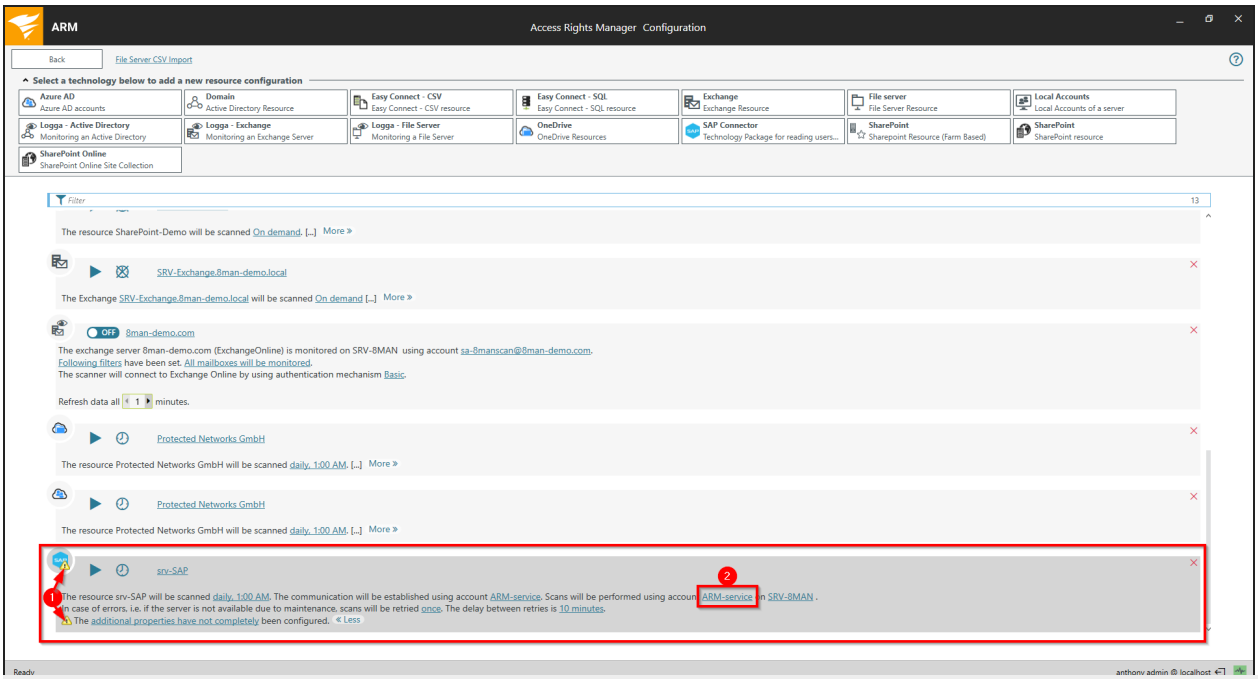
Specify the credentials for the "Process account".

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.



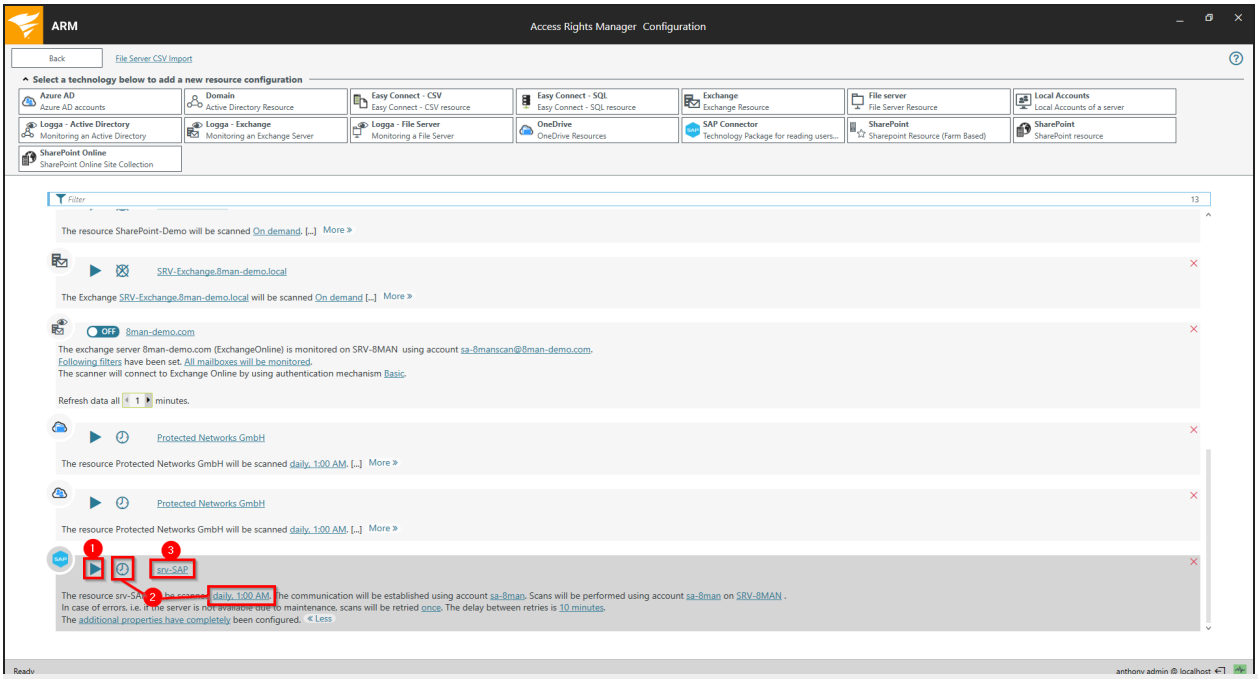
1. Enter the name or IP address of the SAP server. Confirm your input with the ENTER key.
2. Activate the added entry (check the box).
3. Select one or more collectors to scan through.
4. Click "Apply".



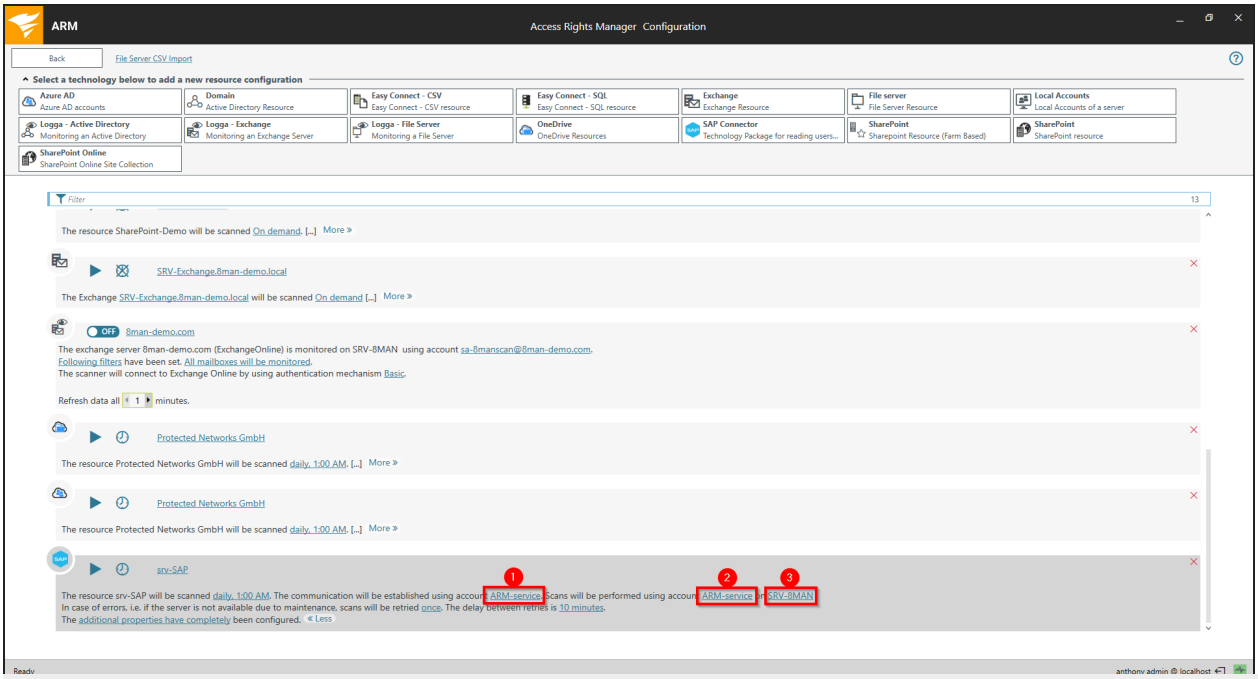
You have created a new SAP scan configuration.

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



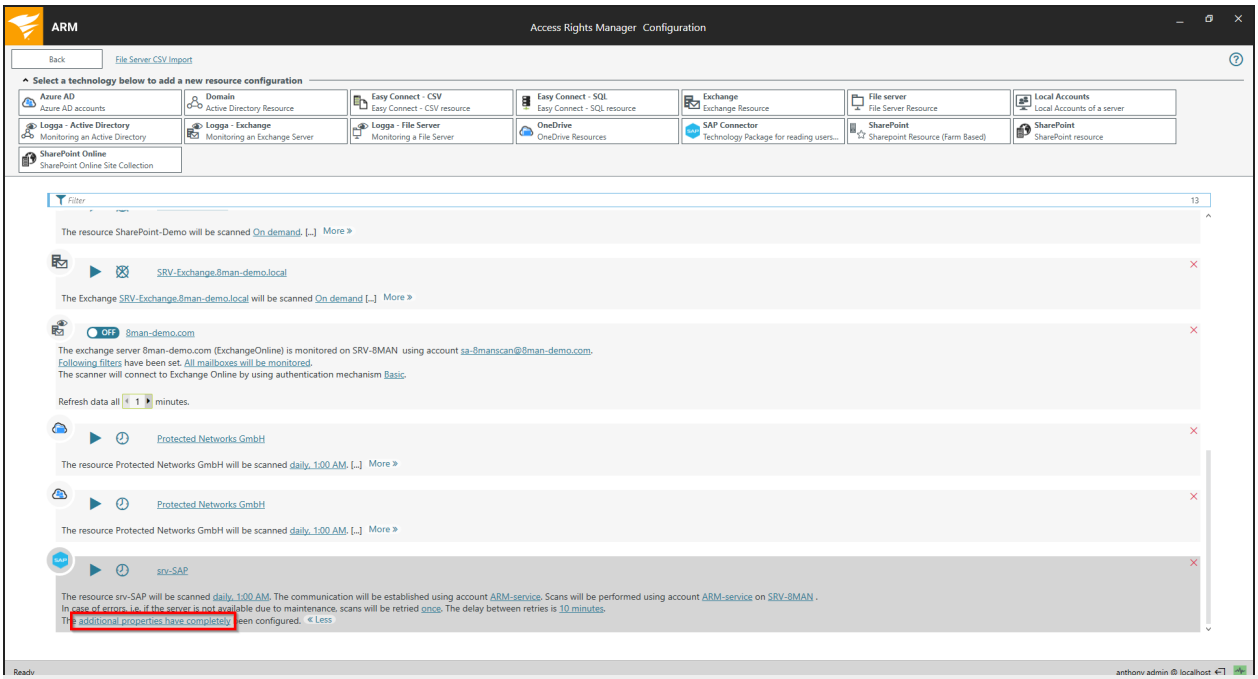
1. Start or stop a scan.
2. Change the schedule for periodic scanning.



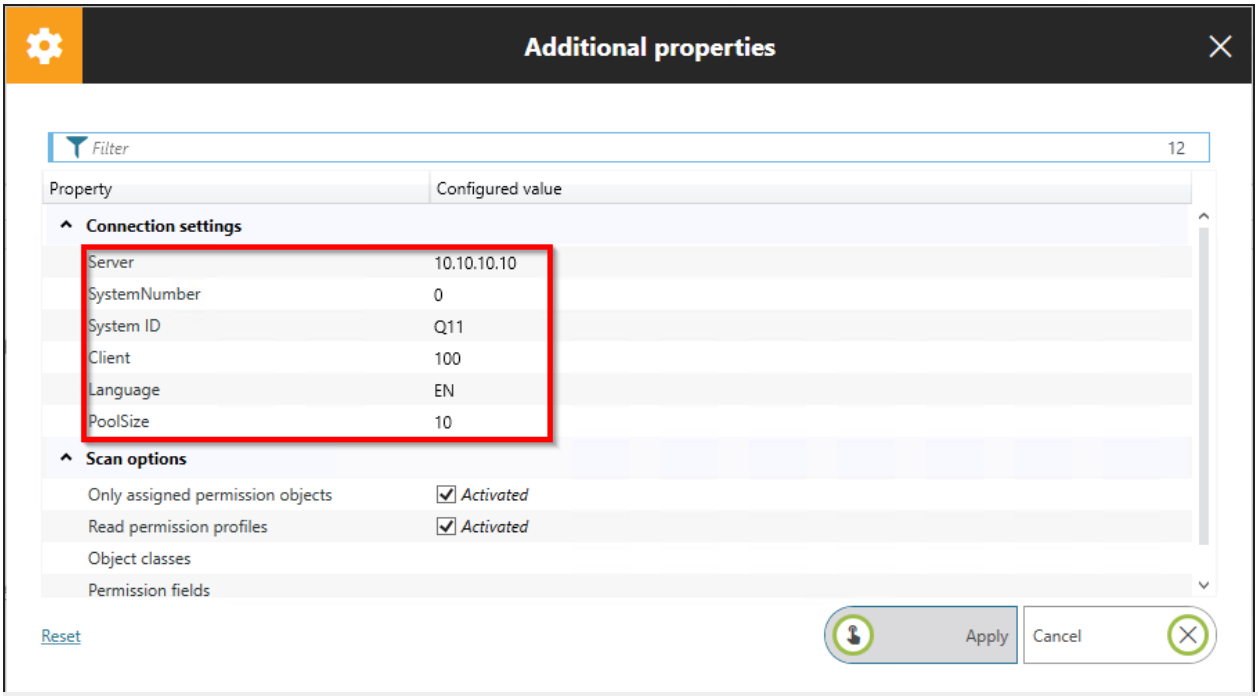
1. Change the process account.
2. Change the scan account.

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

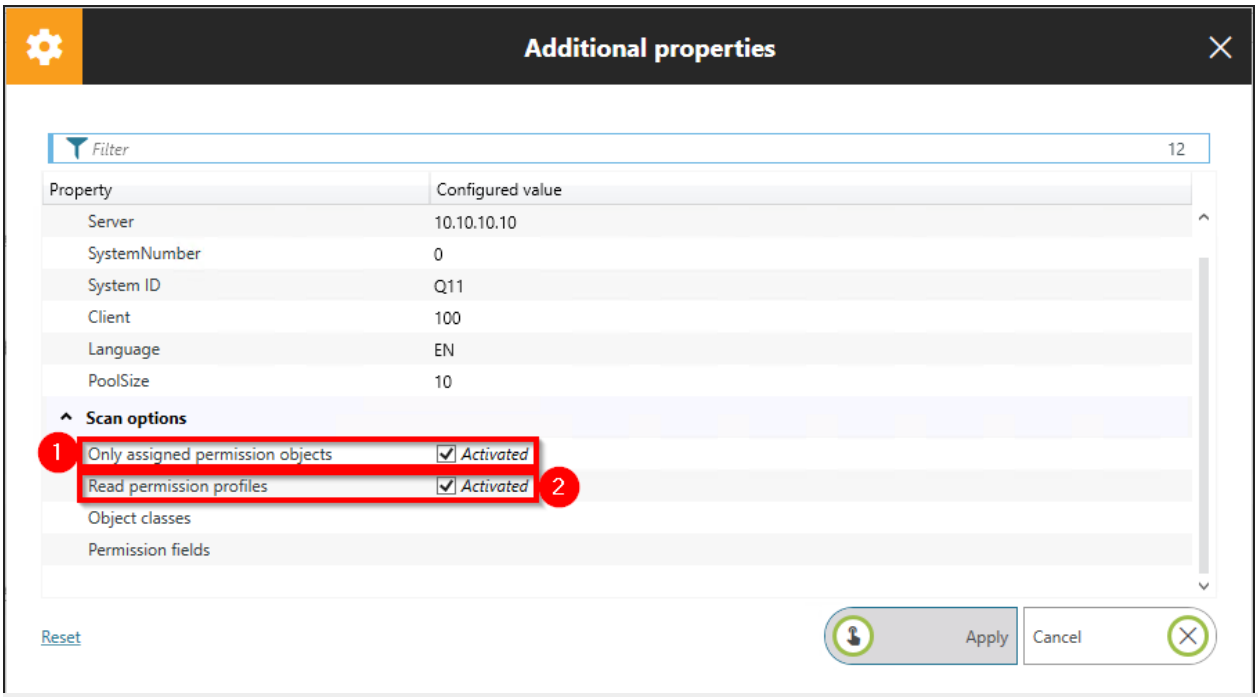
Configure additional SAP properties



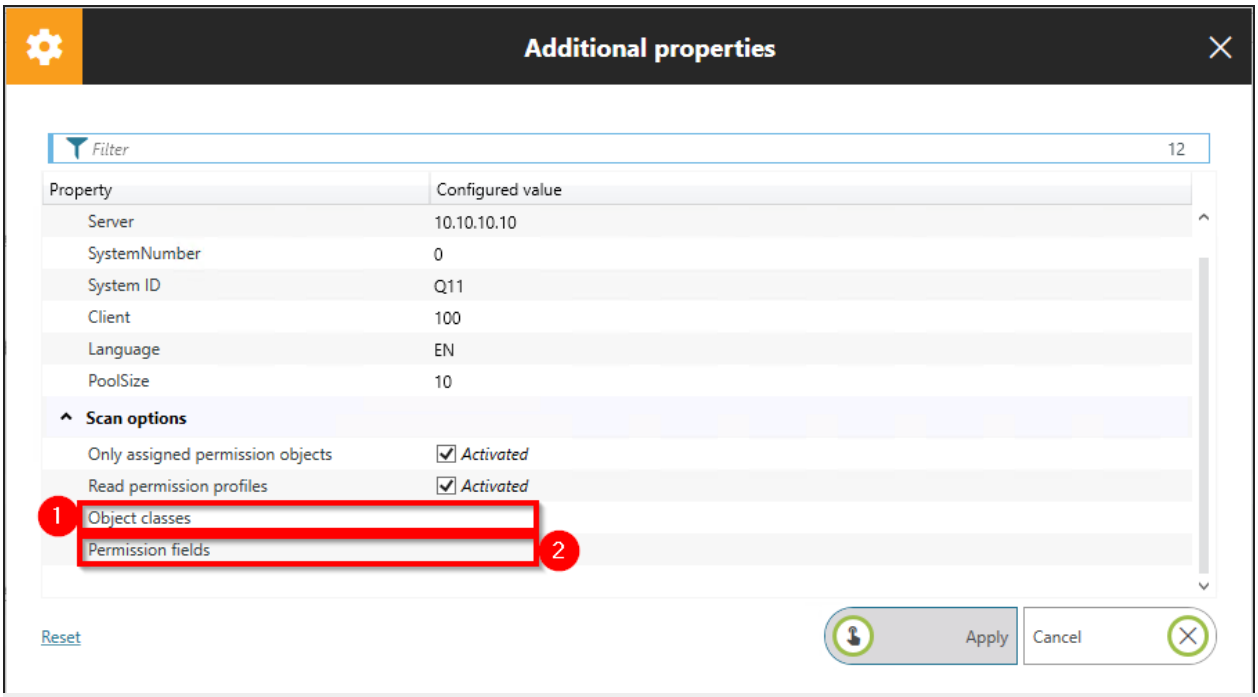
Click on the link to configure the additional properties.



Enter the access data for your SAP system.



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.



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

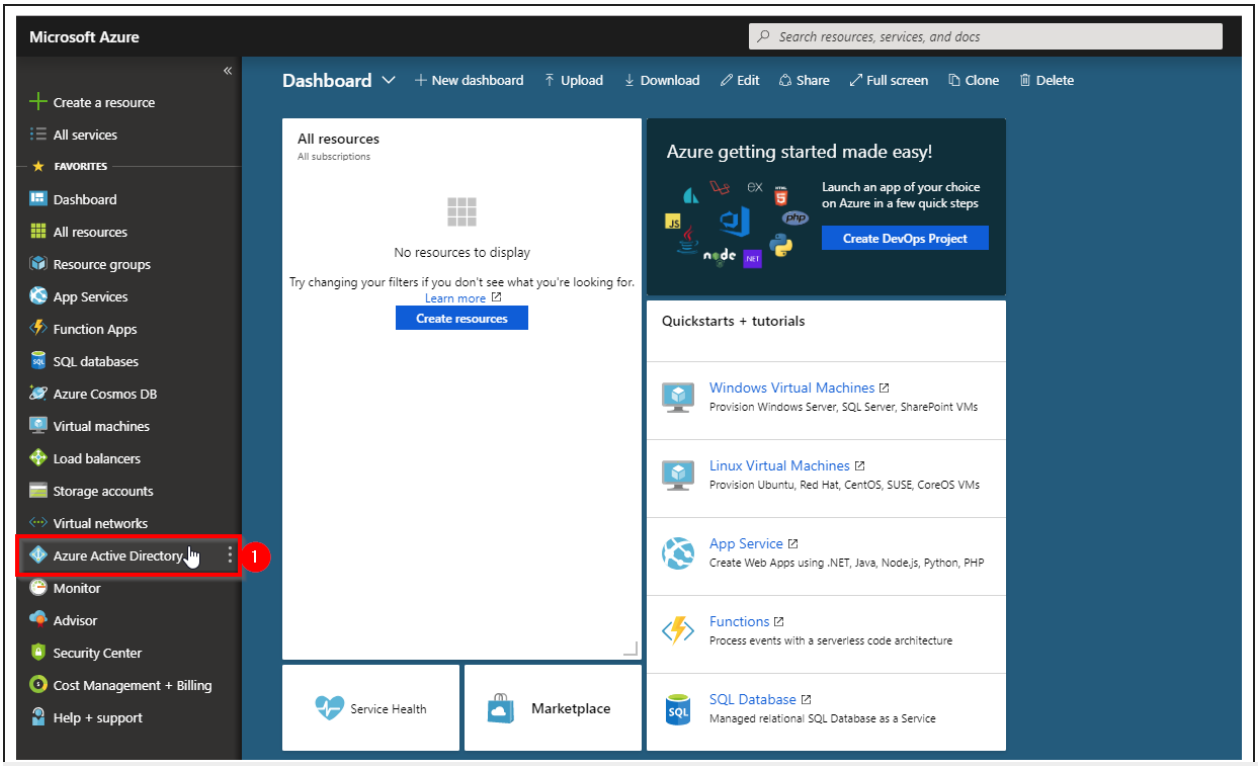
ARM uses the Office 365 Management API to access OneDrive and SharePoint Online events.

To retrieve events, Office 365 auditing must be enabled. How to enable auditing can be found at Microsoft.

The following permissions are required:

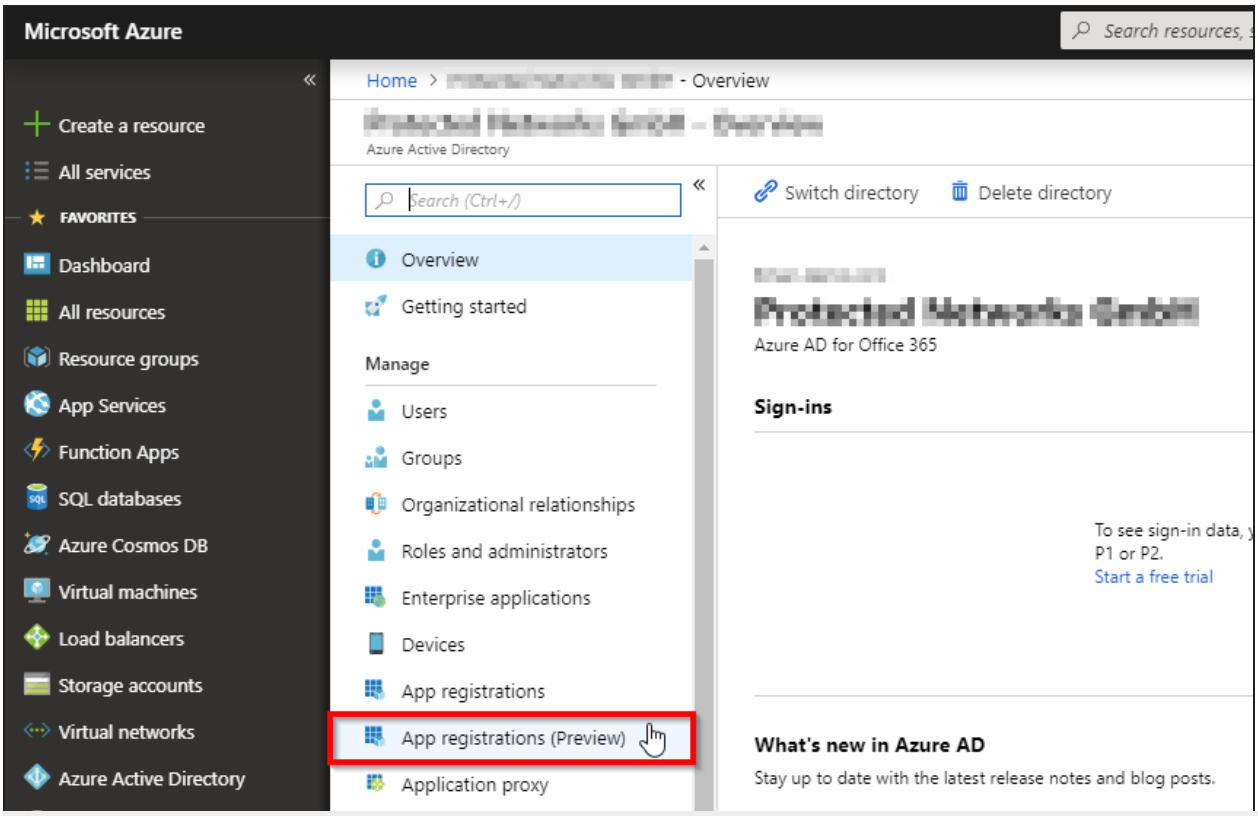
- ActivityFeed.Read
- ServiceHealth.Read

To assign the required permissions, perform the following steps.

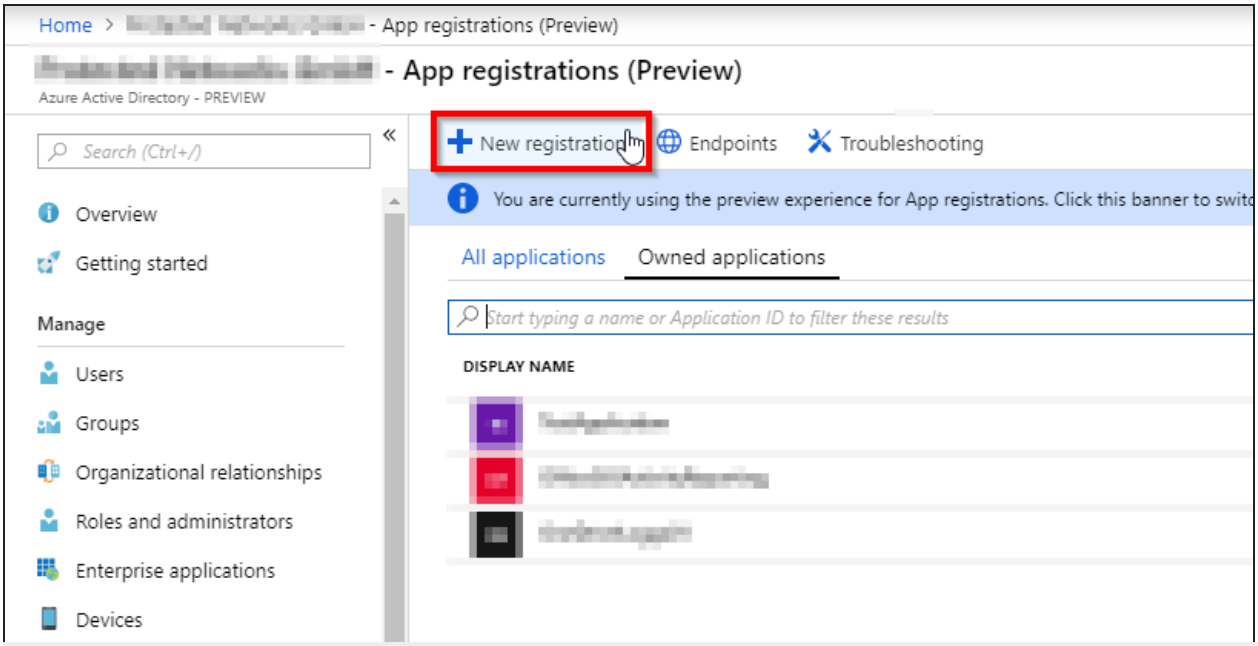


Go to the Azure Portal Website (https://ms.portal.azure.com) and log in with admin credentials.

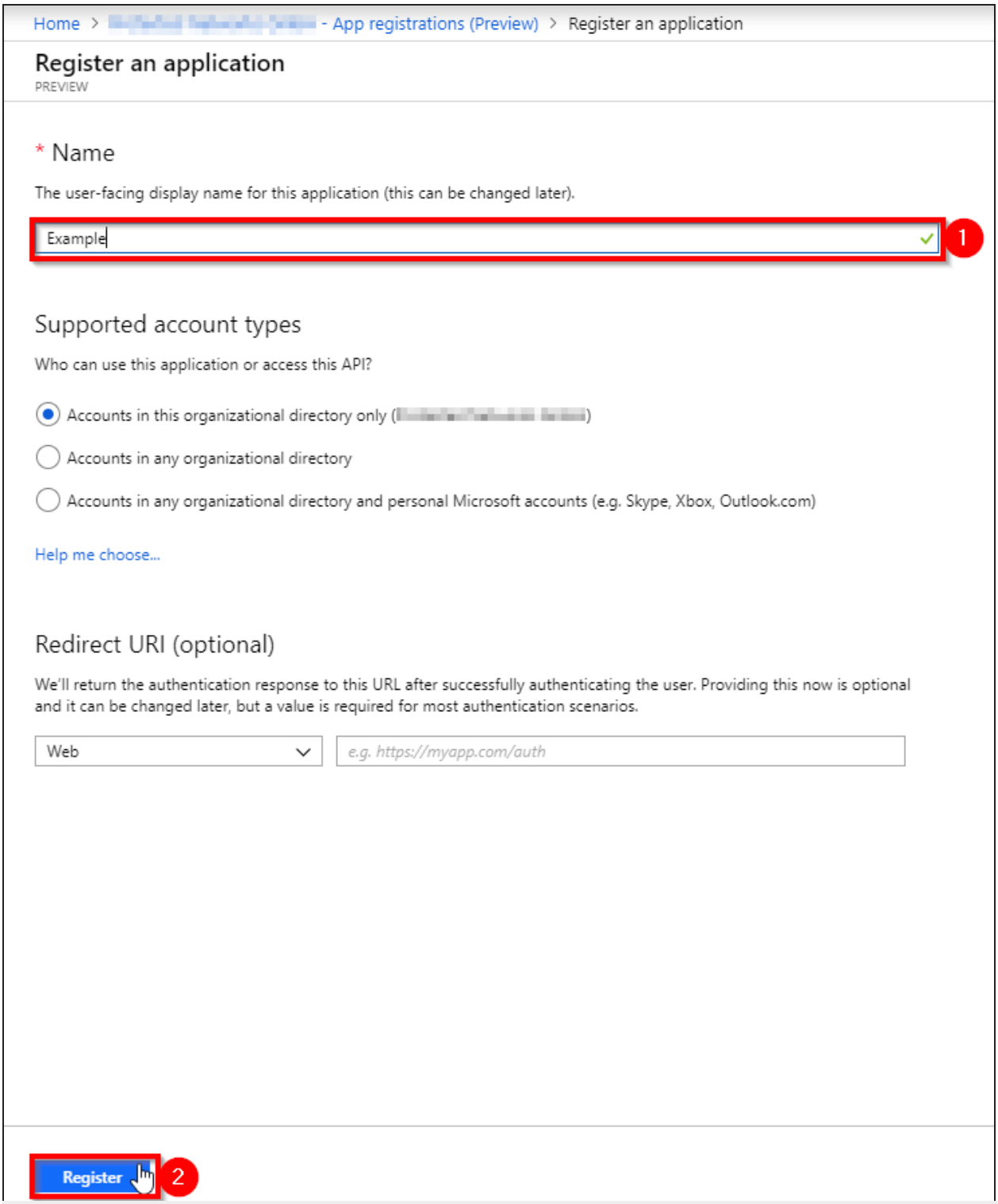
1. Click "Azure Active Directory".



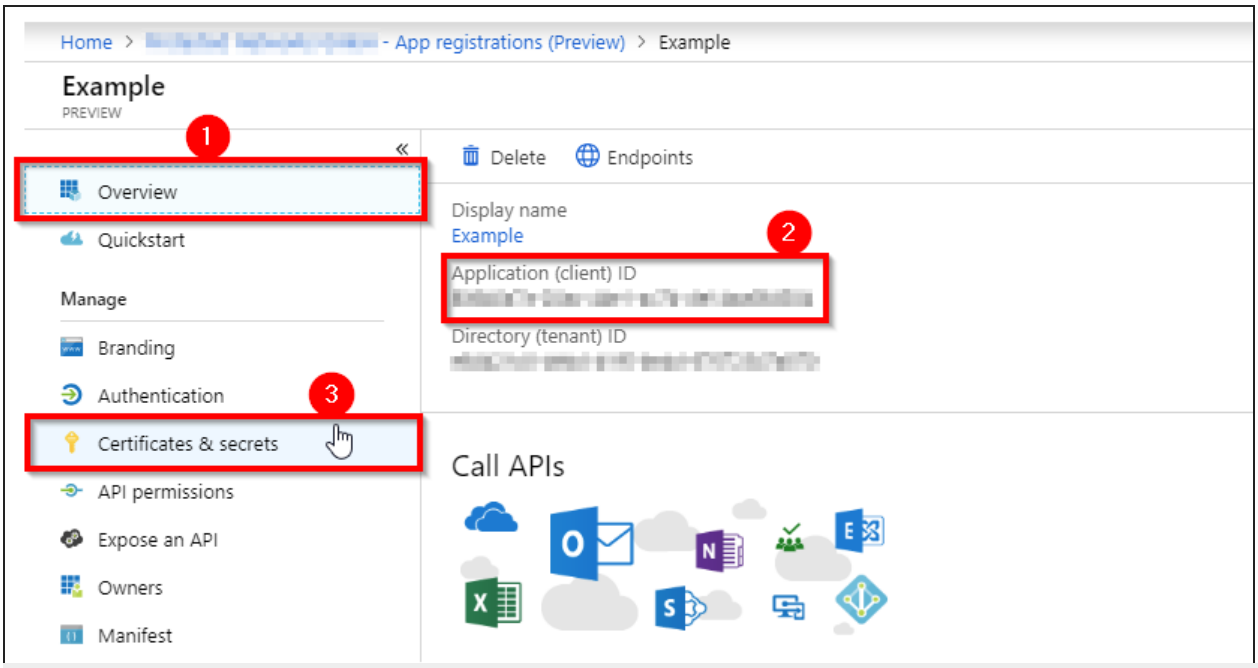
Click "App registrations (Preview)".



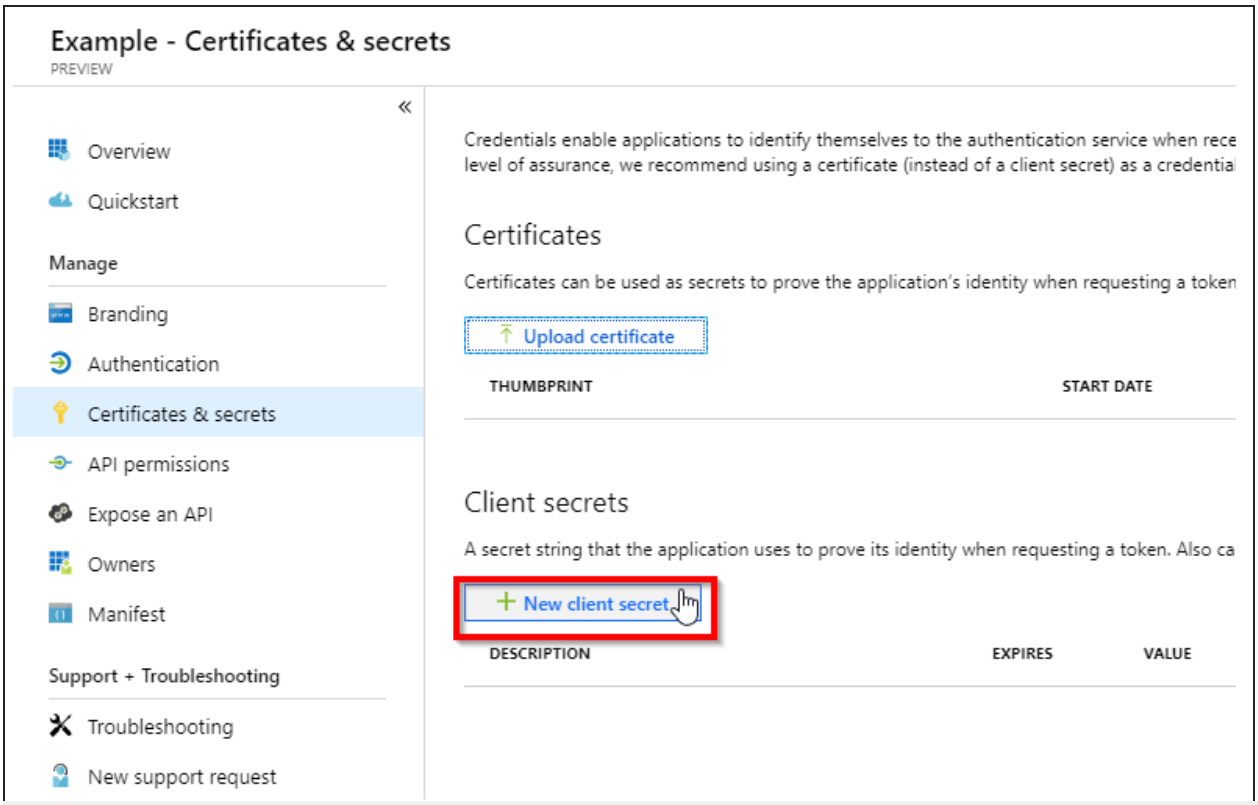
Add a new app registration.



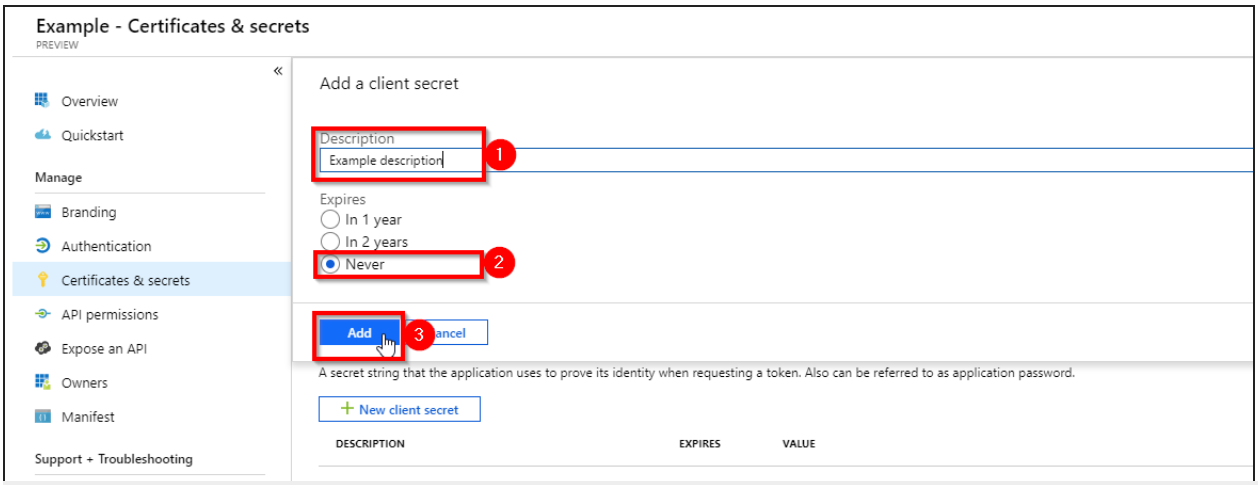
1. Assign a name to the registration.
2. Click "Register".



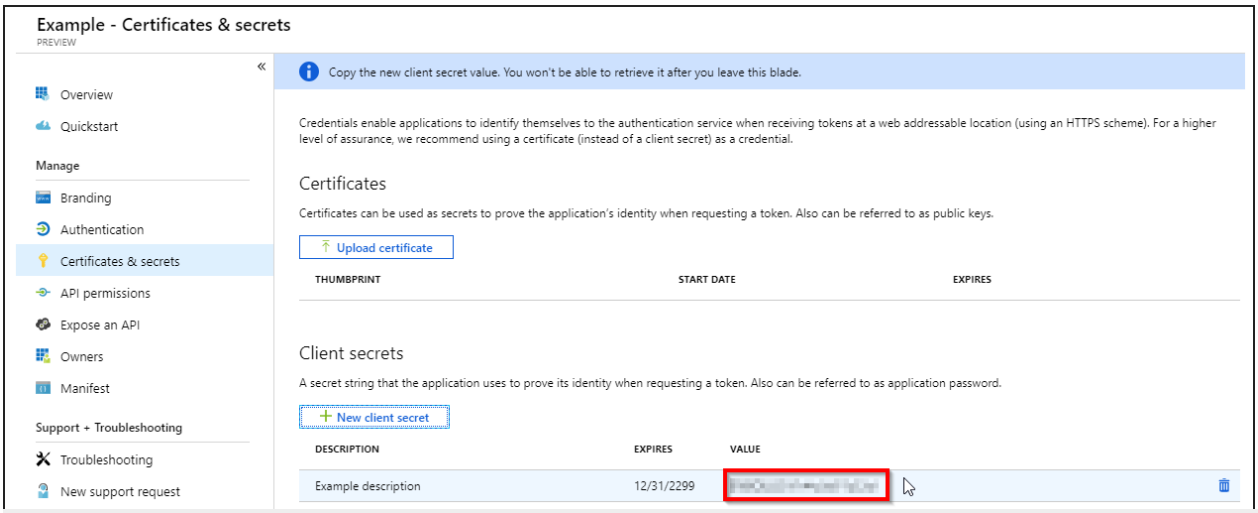
1. Click "Overview".
2. Copy the Application ID to a file. The Application ID will later be used as the user name to access Azure/O365 resources.
3. Click "Certificates & secrets".



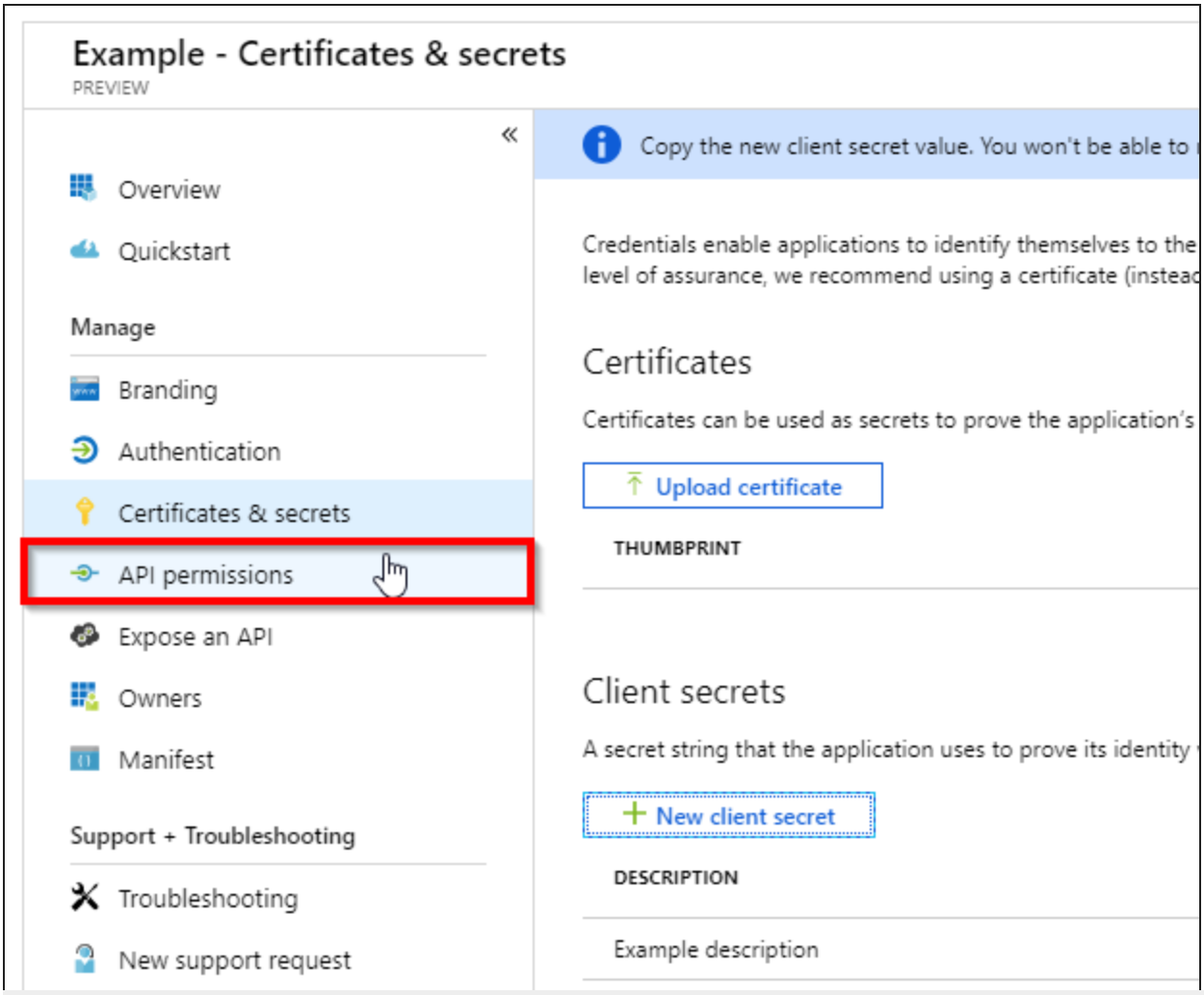
Add a new "Client secret".



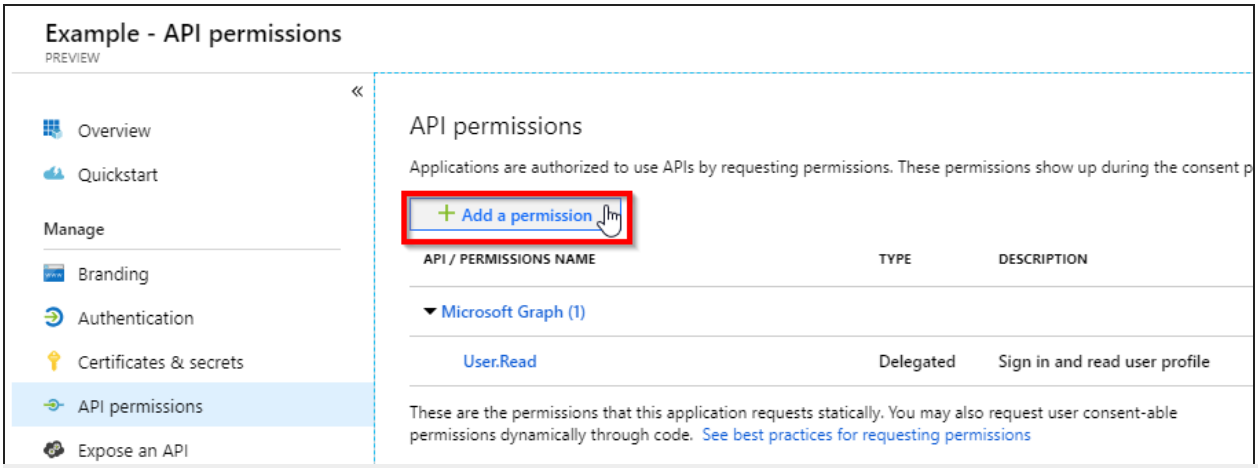
1. Enter a description.
2. Set the expiration date to "Never".
3. Click "Add".



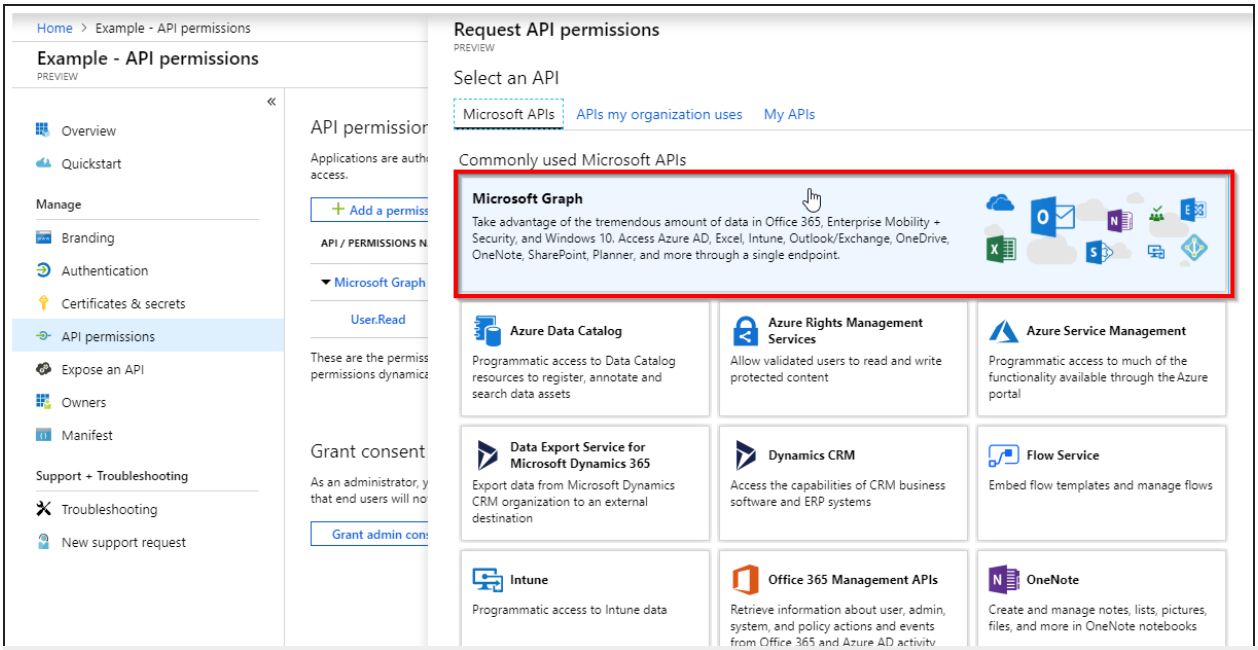
Save the value to a file. The Client secret will later be used as the password to access Azure/O365 resources.



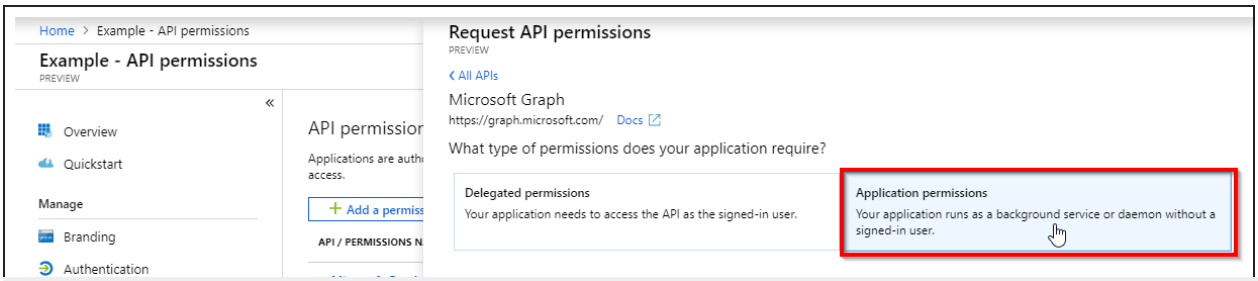
Click "API permissions".



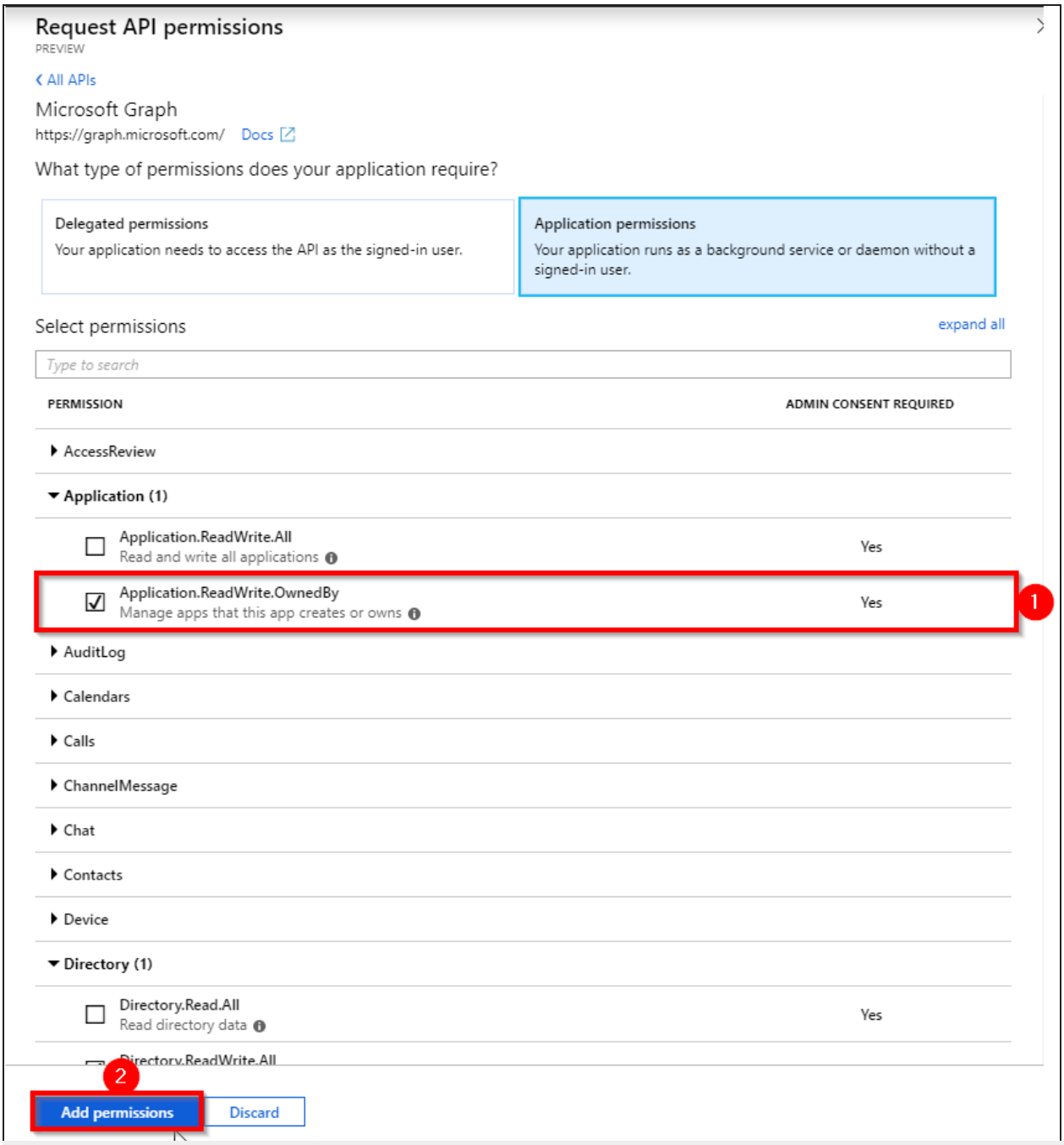
Click "Add a permission".



Click "Microsoft Graph".



Click "Application permissions".

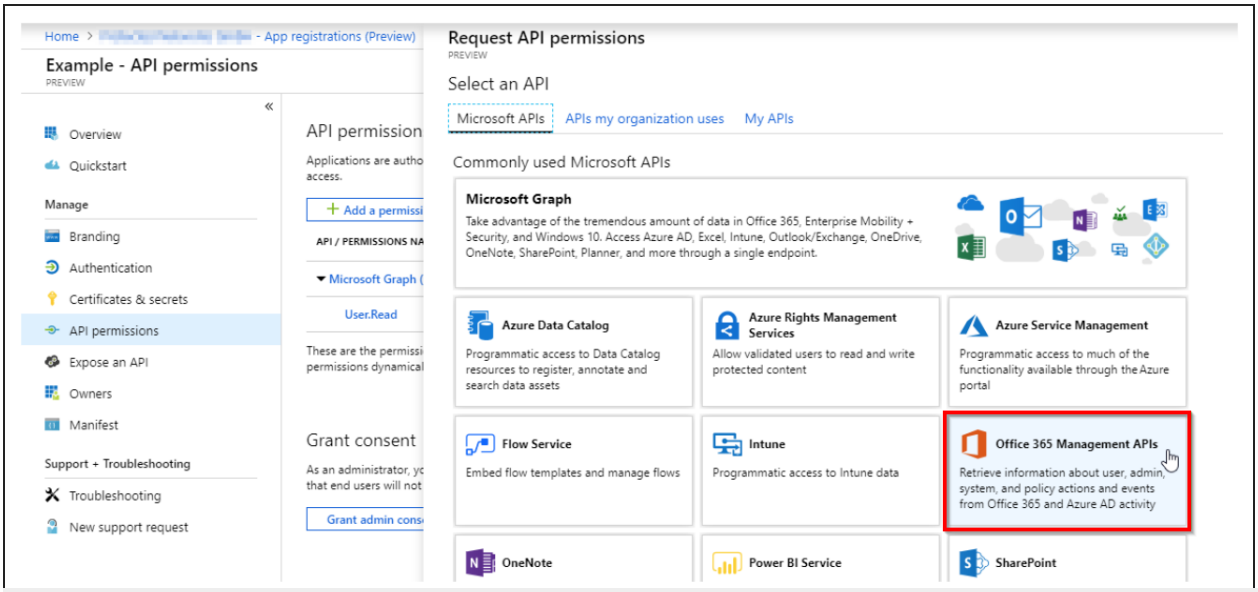


1. Enable **all** of the following permissions:

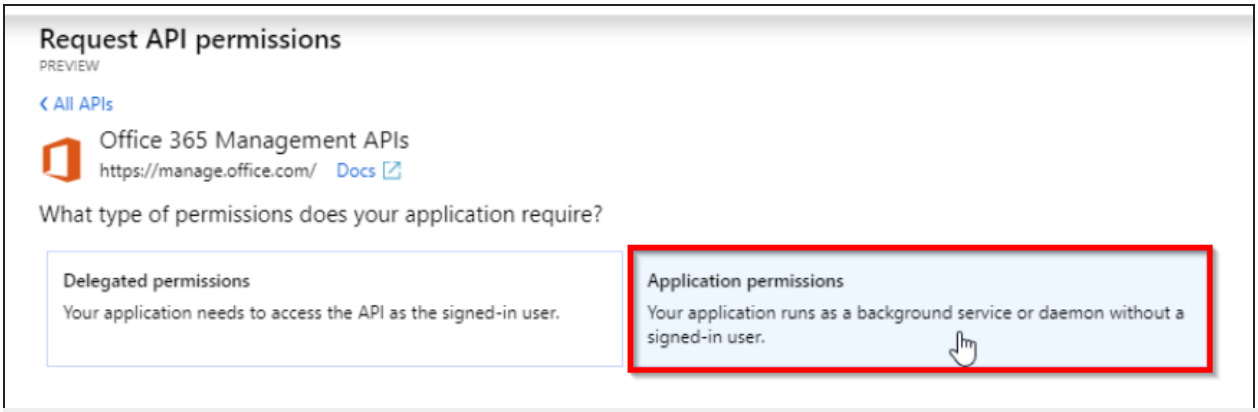
- Application.ReadWrite.OwnedBy
- Directory.ReadWrite.All
- Files.ReadWrite.All
- Group.ReadWrite.All
- Member.Read.Hidden

- User.ReadWrite.All
- Sites.FullControl.All

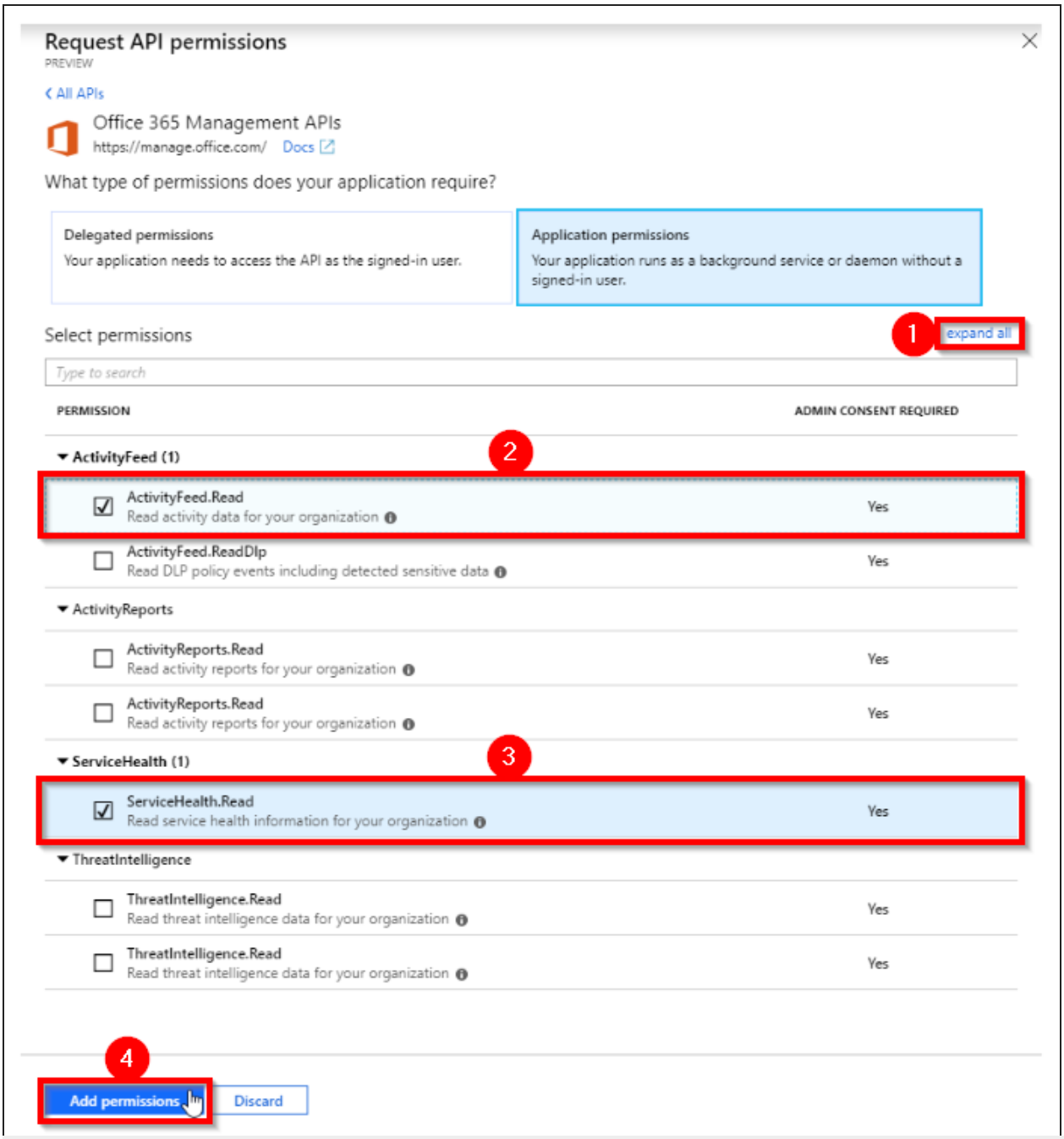
2. Save your settings.



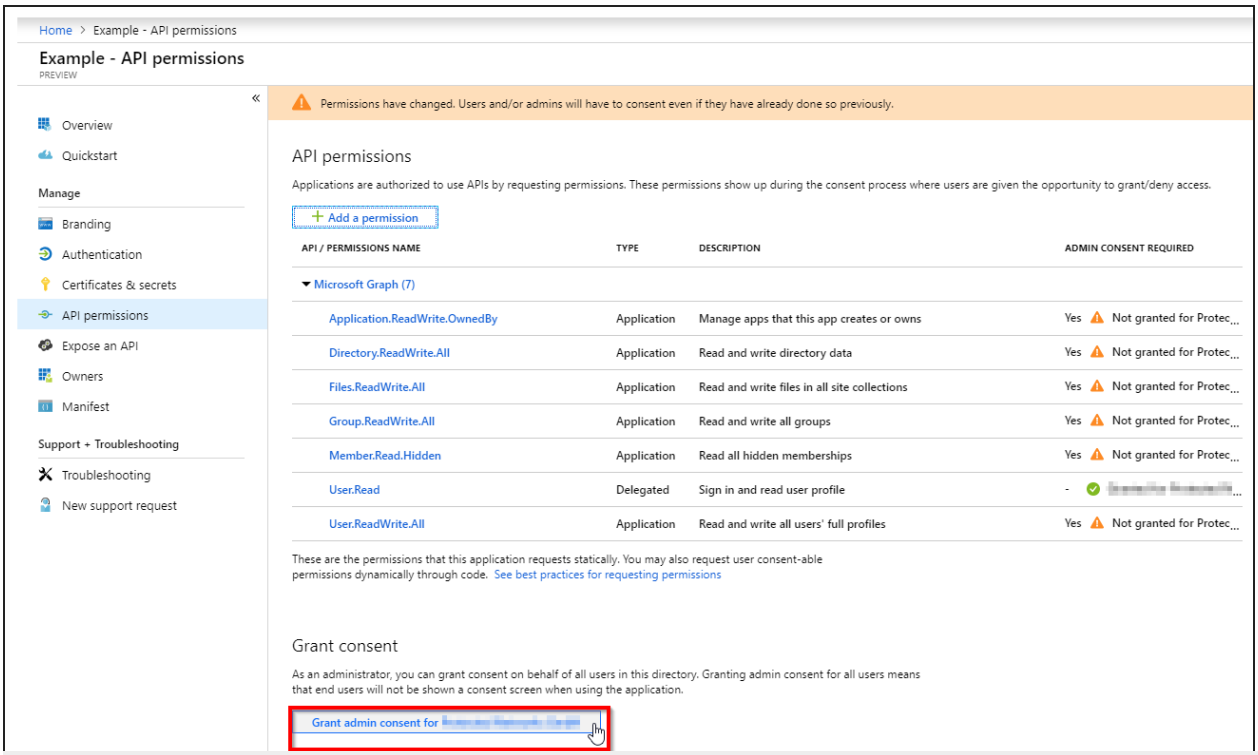
Click "Office 365 Management APIs".



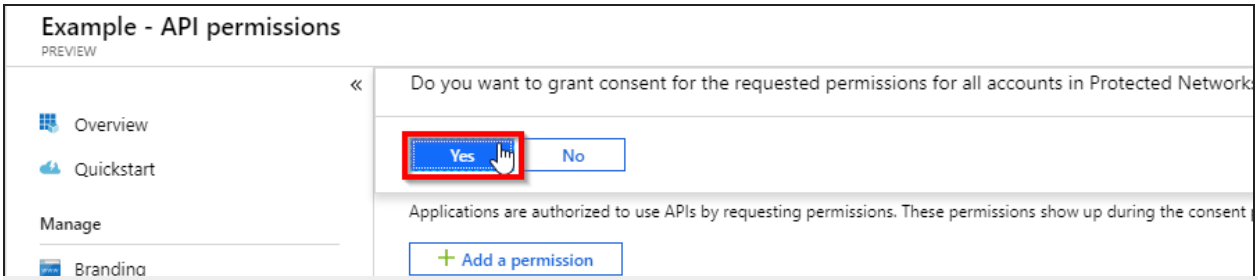
Select "Application permissions".



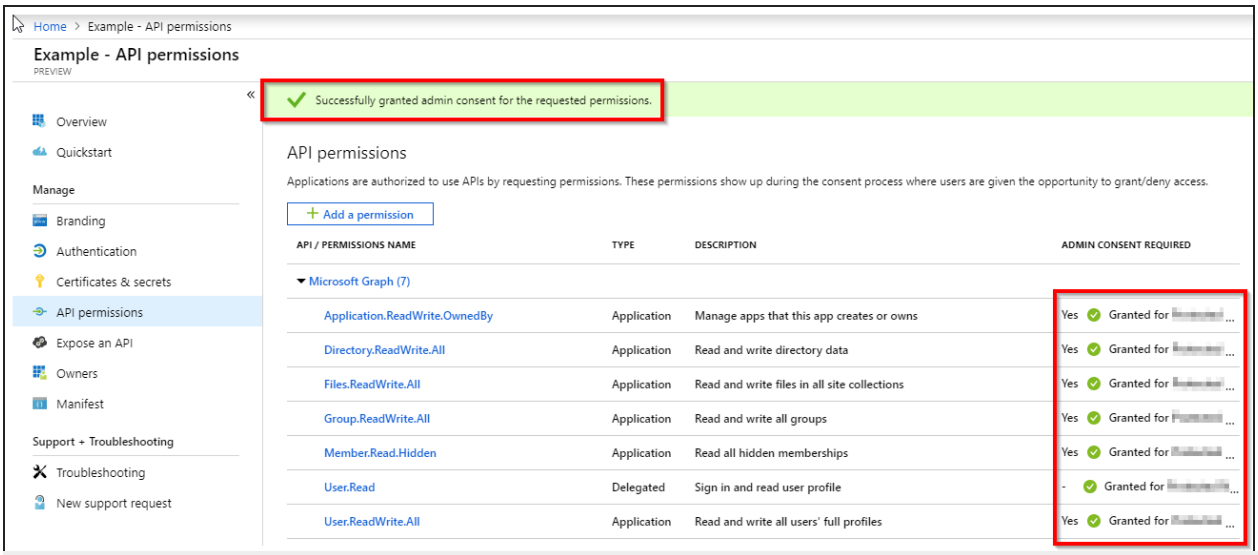
1. Click "expand all".
2. Enable "ActivityFeed.Read".
3. Enable "ServiceHealth.Read".
4. Click "Add permissions".



Click "Grant admin consent for...".



Confirm the dialog box.



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

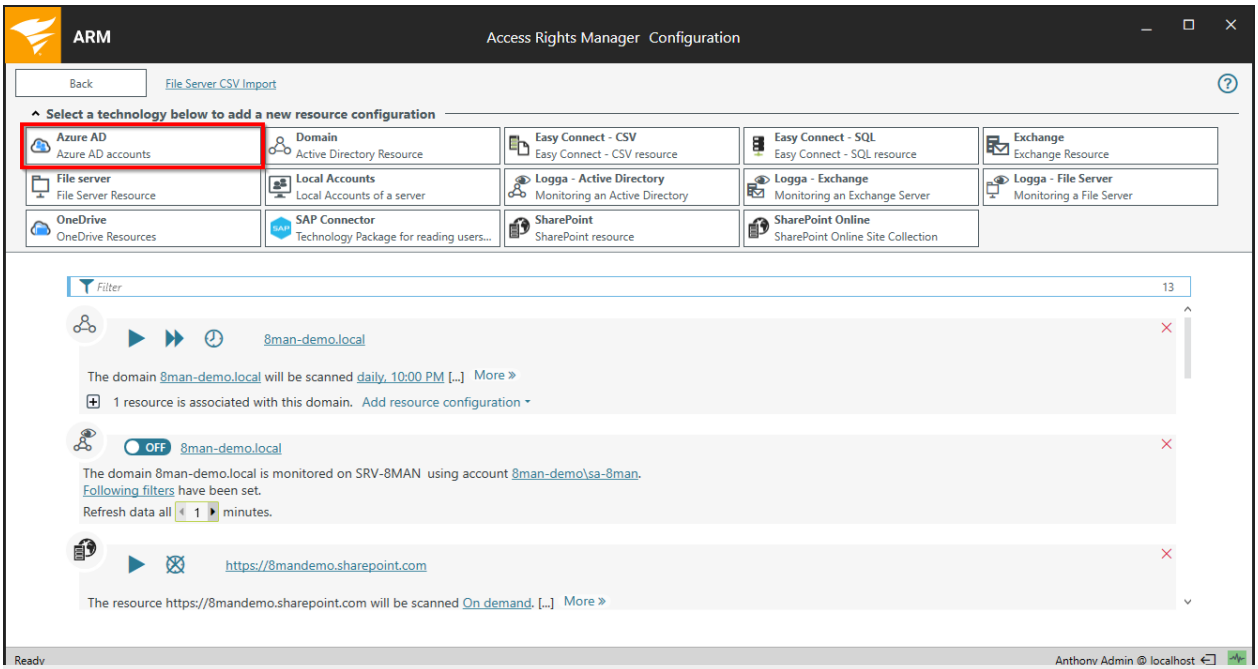
The "Process account" is used to execute the scan process on the selected collector. This account must have local administrative rights and interactive logon privileges on the collector.

Scan Account

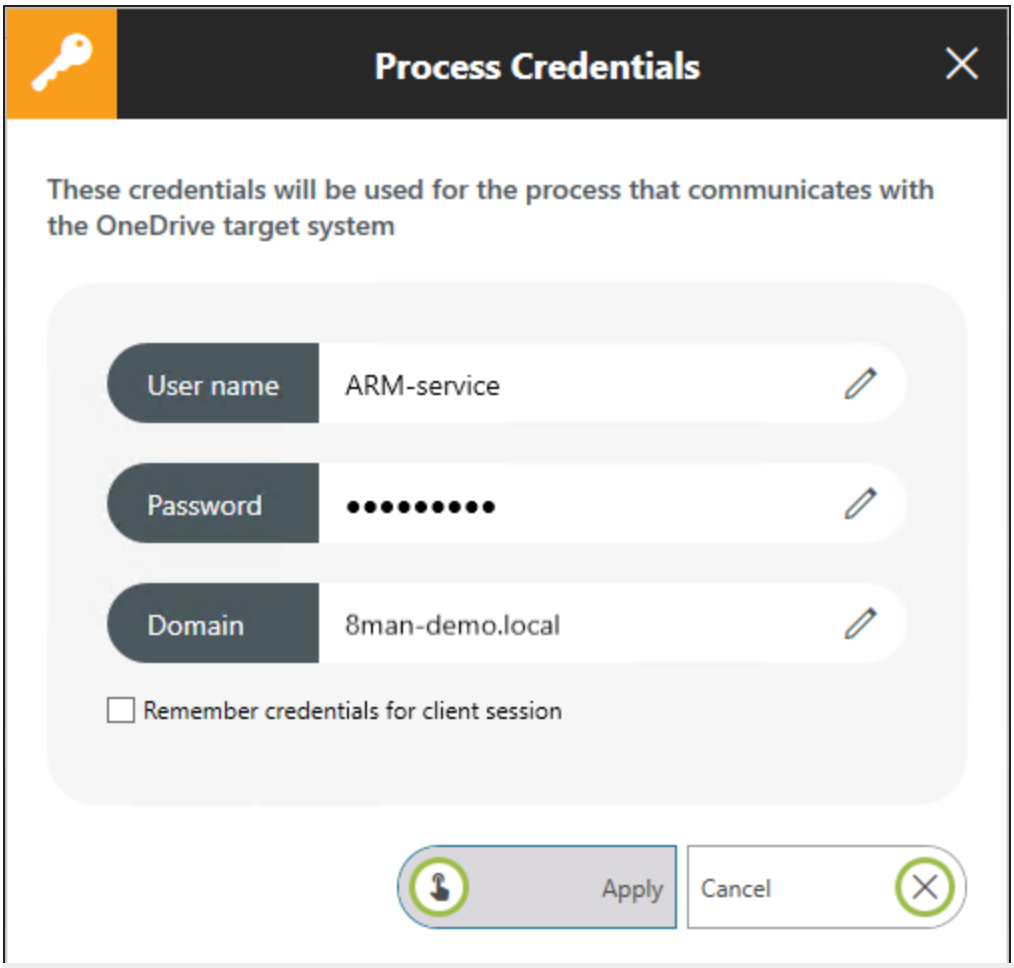
The "scan account" is used for the actual scan. This account must have the permissions described in the section "Prepare Office 365 integration".

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.



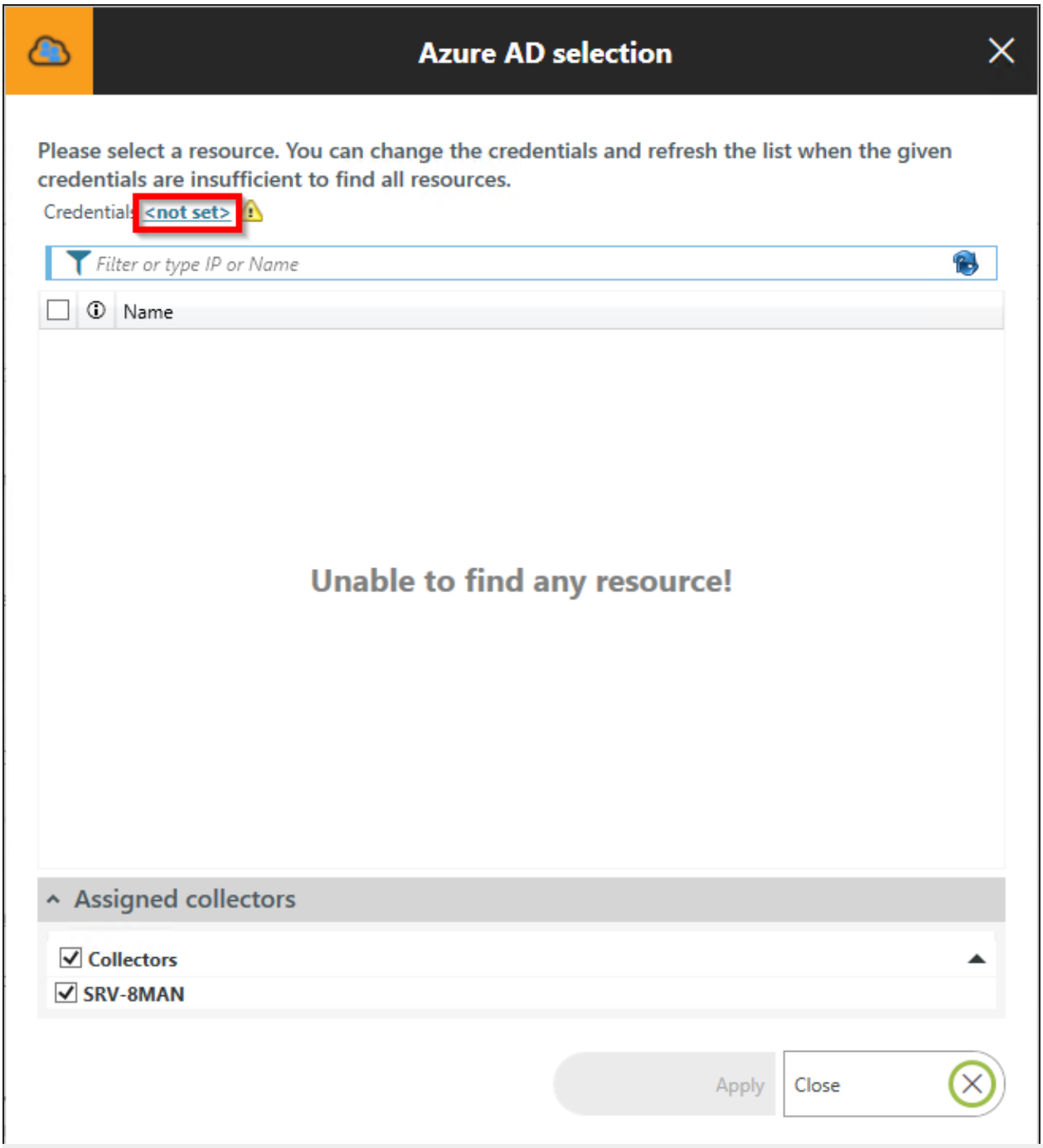
From the ARM Configuration Application > Scans, click "Azure AD".



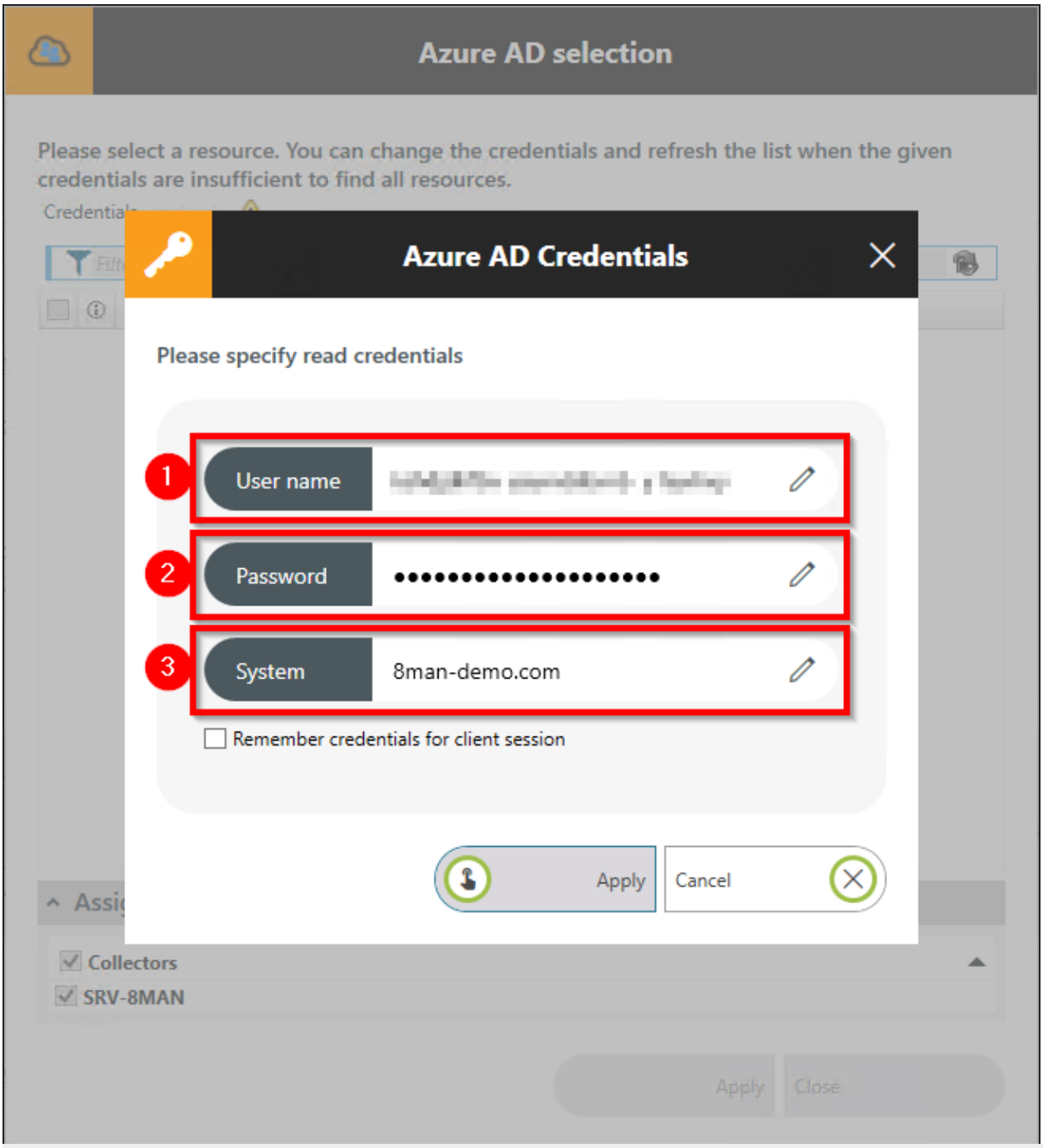
Specify the credentials for the "Process Account".

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.

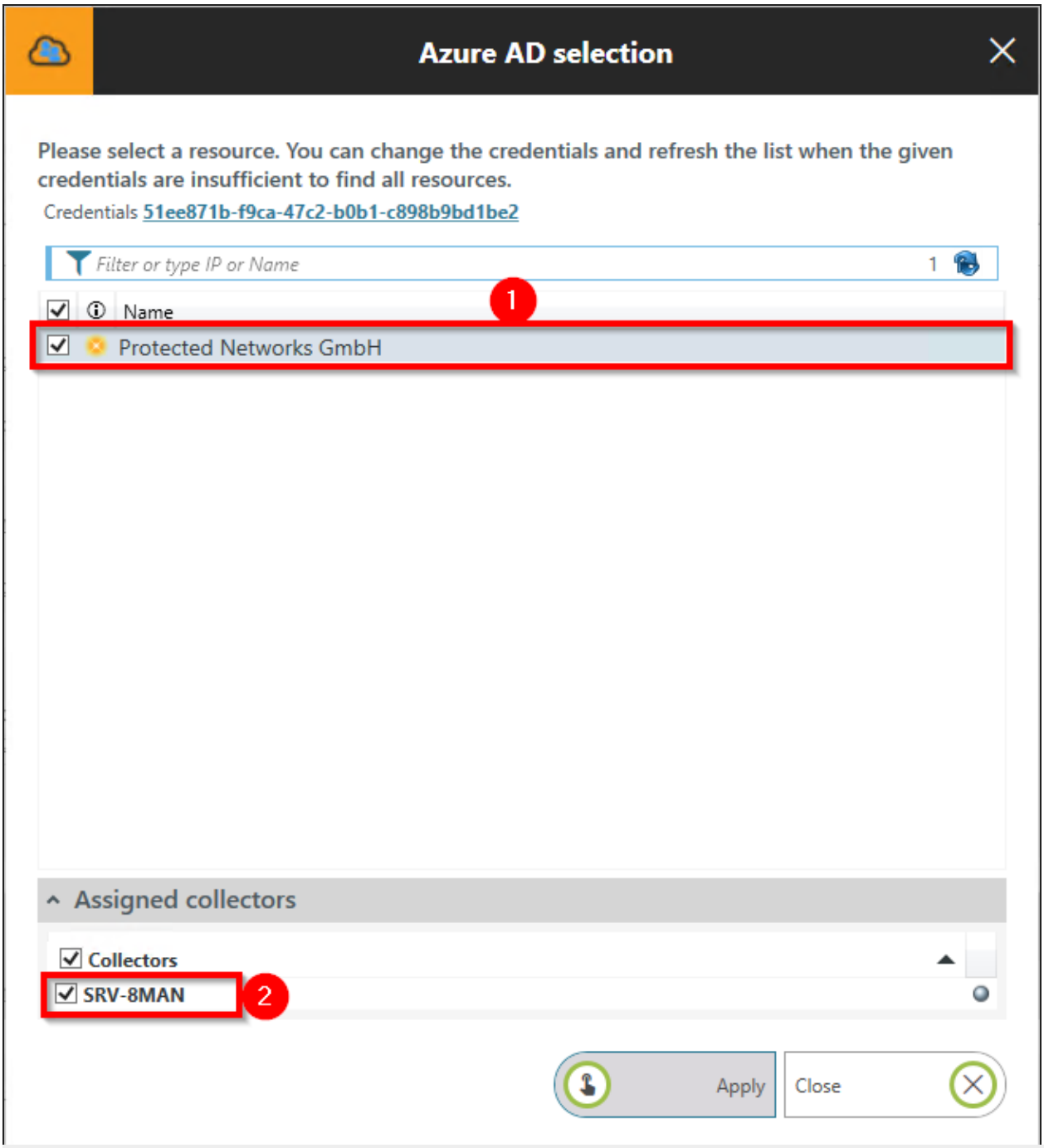


Click the link.



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.



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

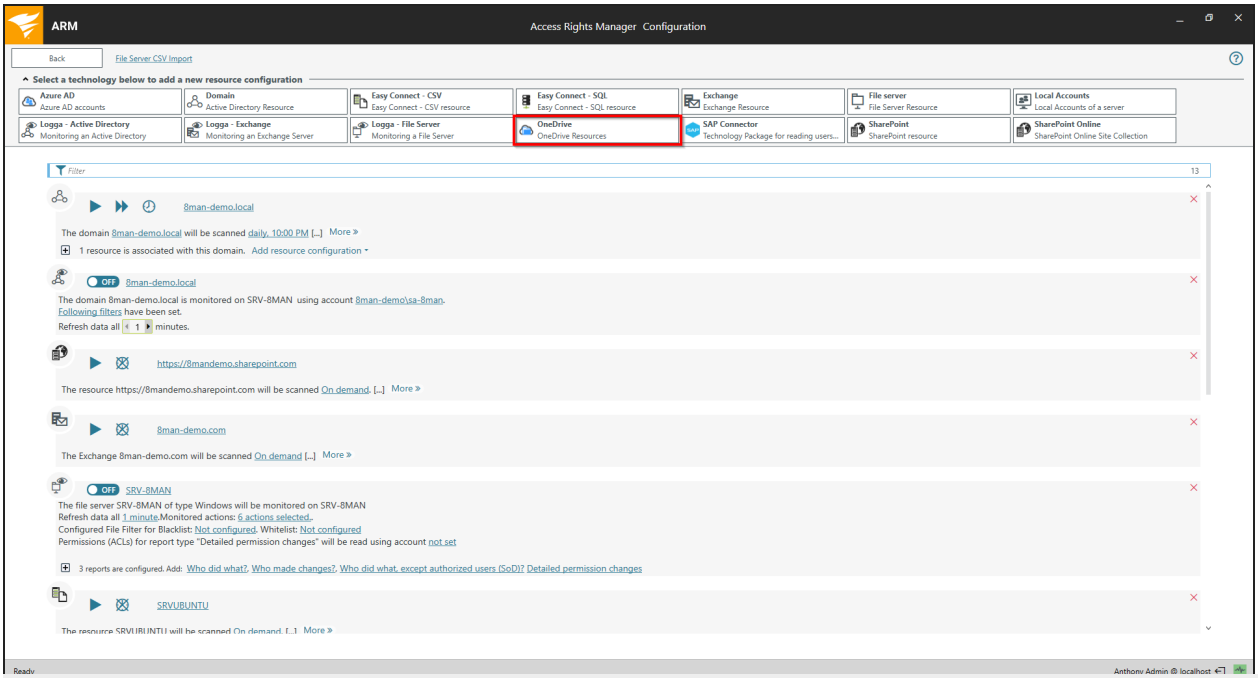
The "Process account" is used to execute the scan process on the selected collector. This account must have local administrative rights and interactive logon privileges on the collector.

Scan Account

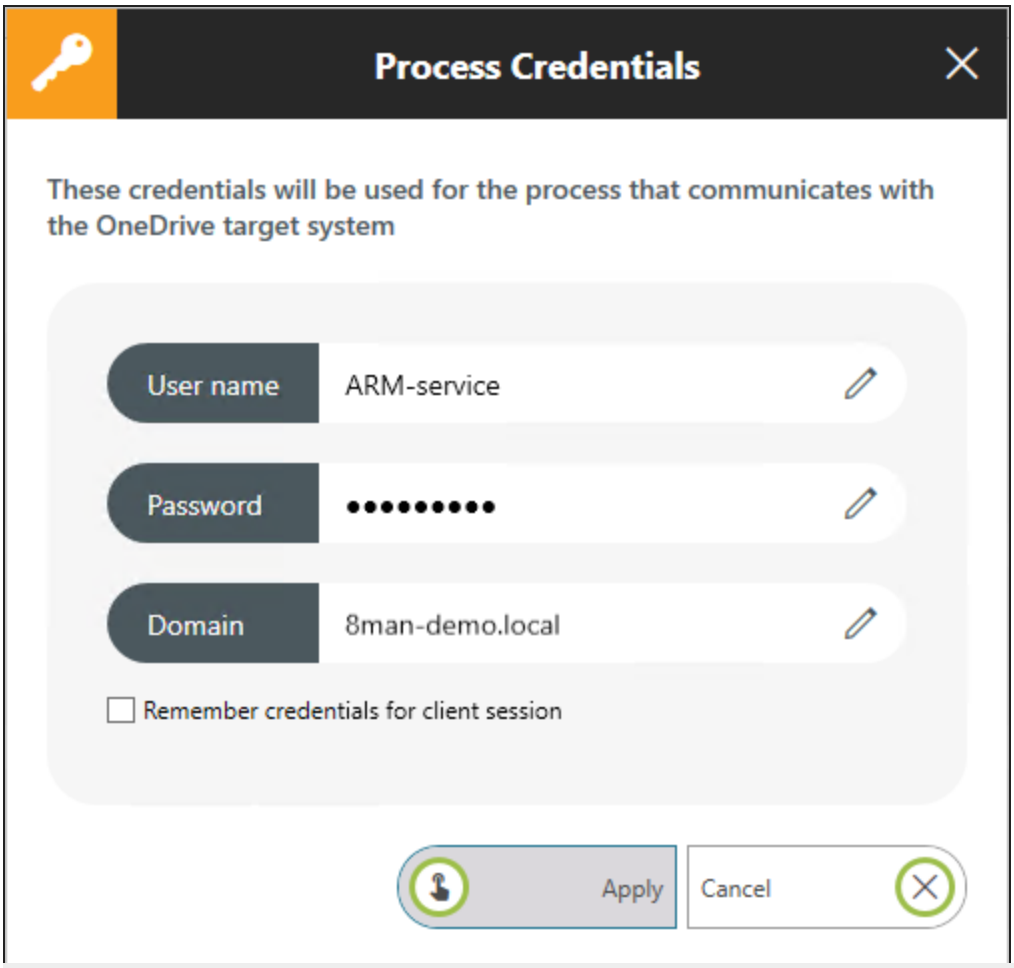
The "scan account" is used for the actual scan. This account must have the permissions described in the section "Prepare Office 365 integration".

Add OneDrive scans

> You must at first set up access in the Azure portal to be able to configure a OneDrive scan completely.



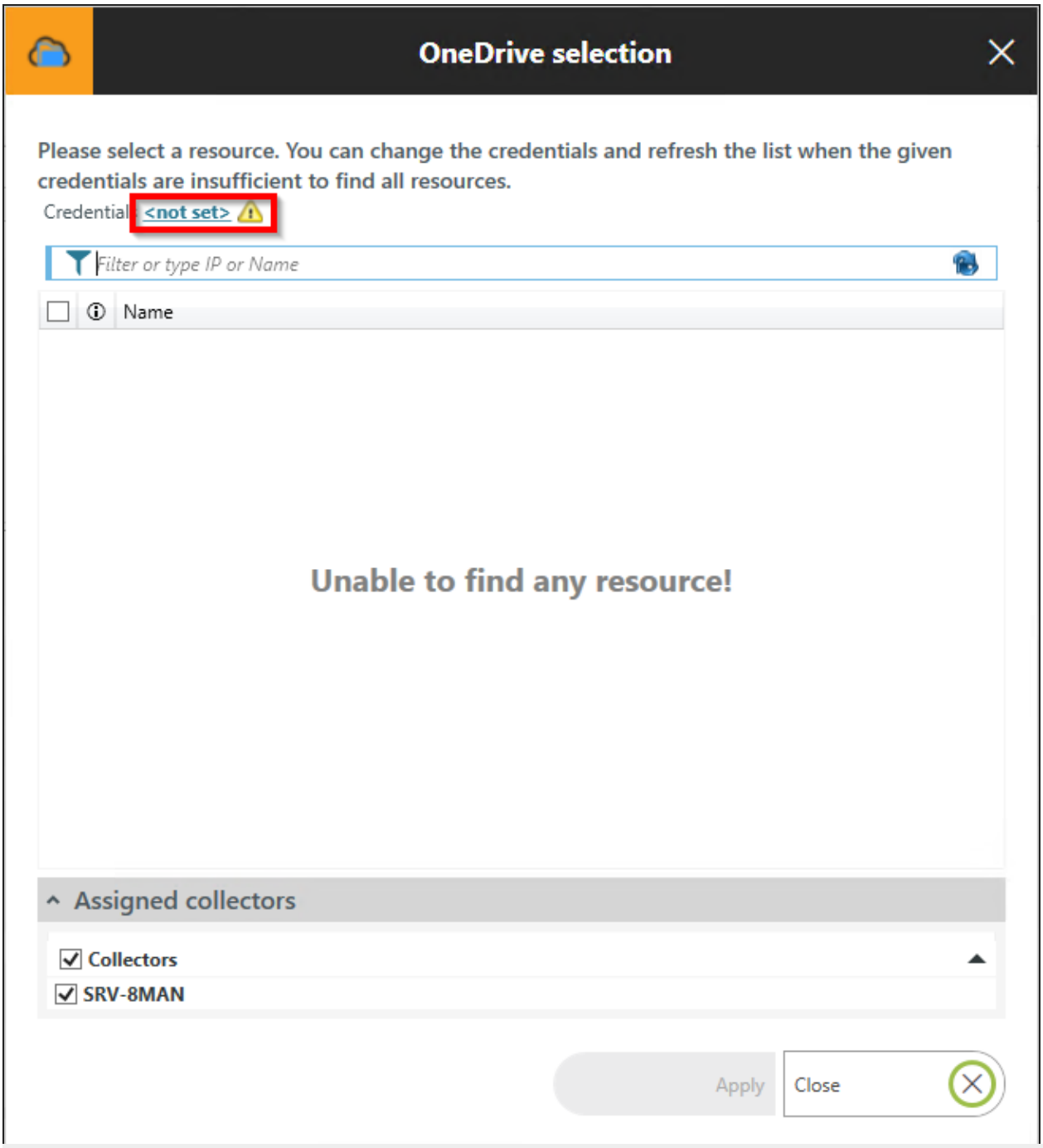
In the ARM Configuration Application > Scans, click "OneDrive" to add a OneDrive resource.



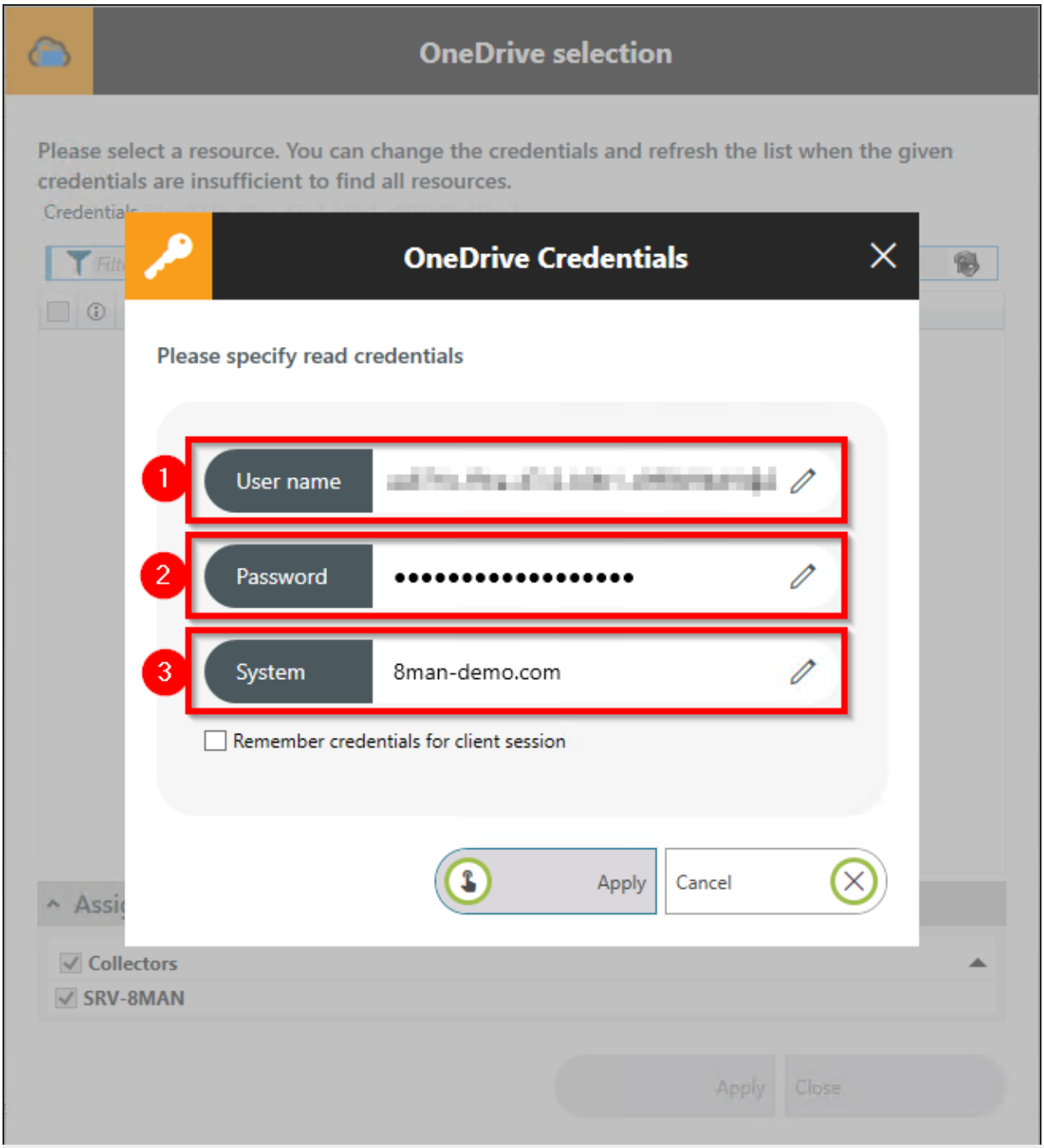
Specify the credentials for the "Process Account".

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.

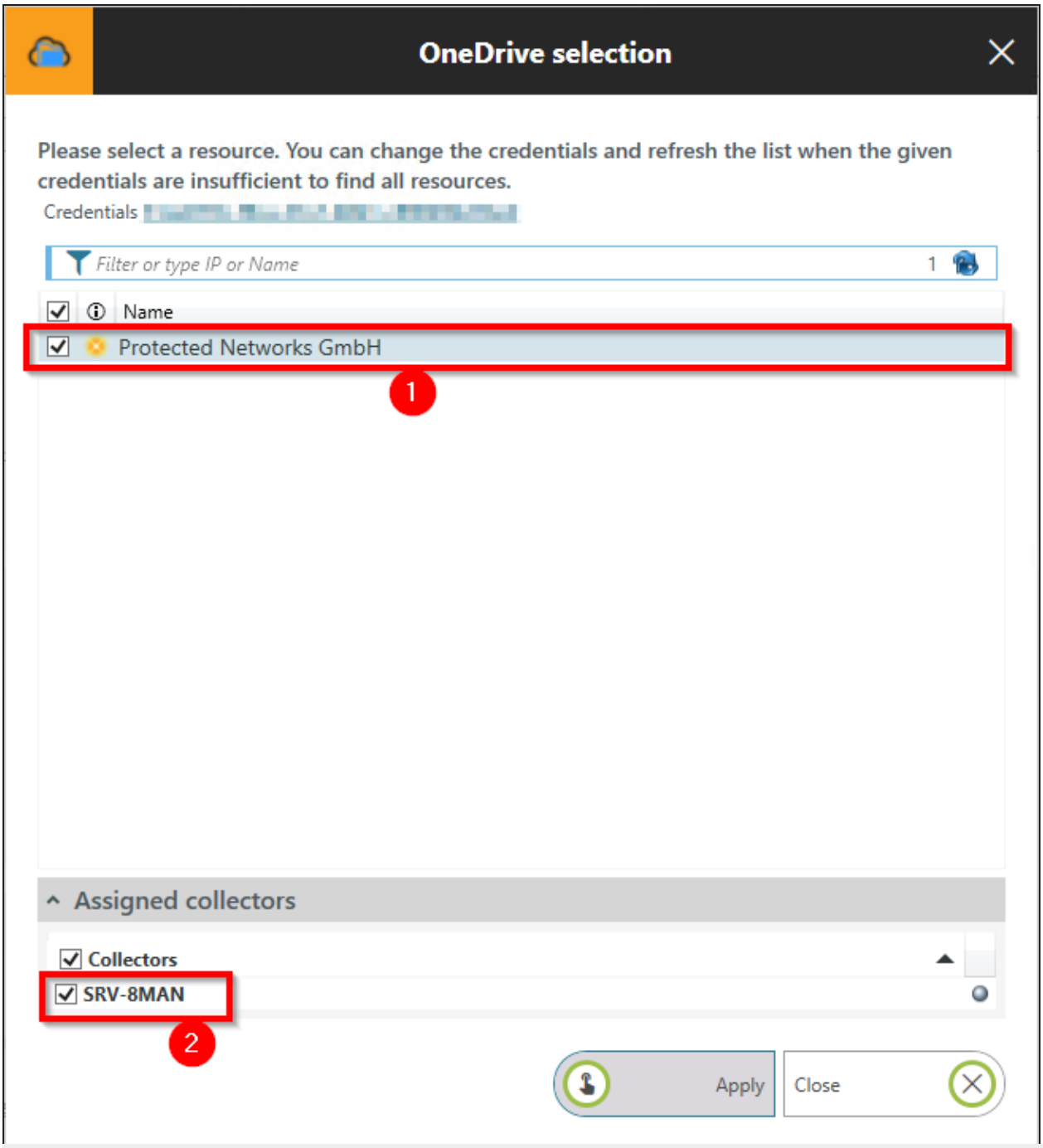


Click the link.



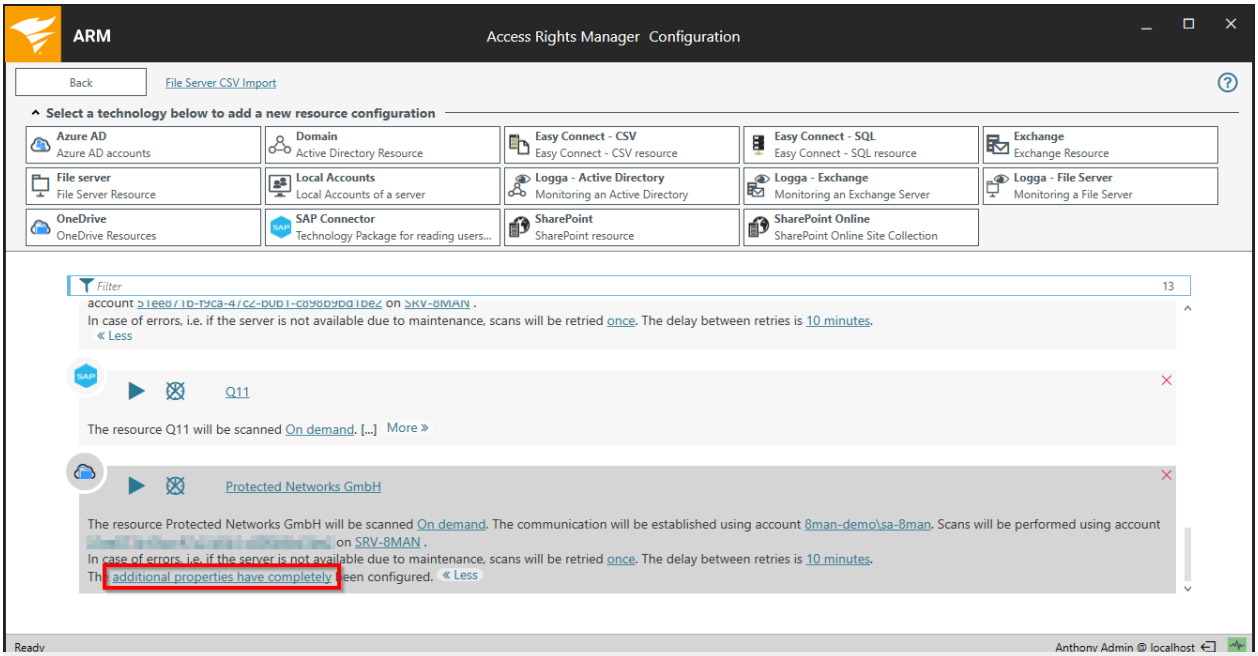
Enter the access data that you created during preparation on the Azure portal.

1. Enter the application ID as the user name.
2. Enter the client secret as the password.
3. Enter the online domain.

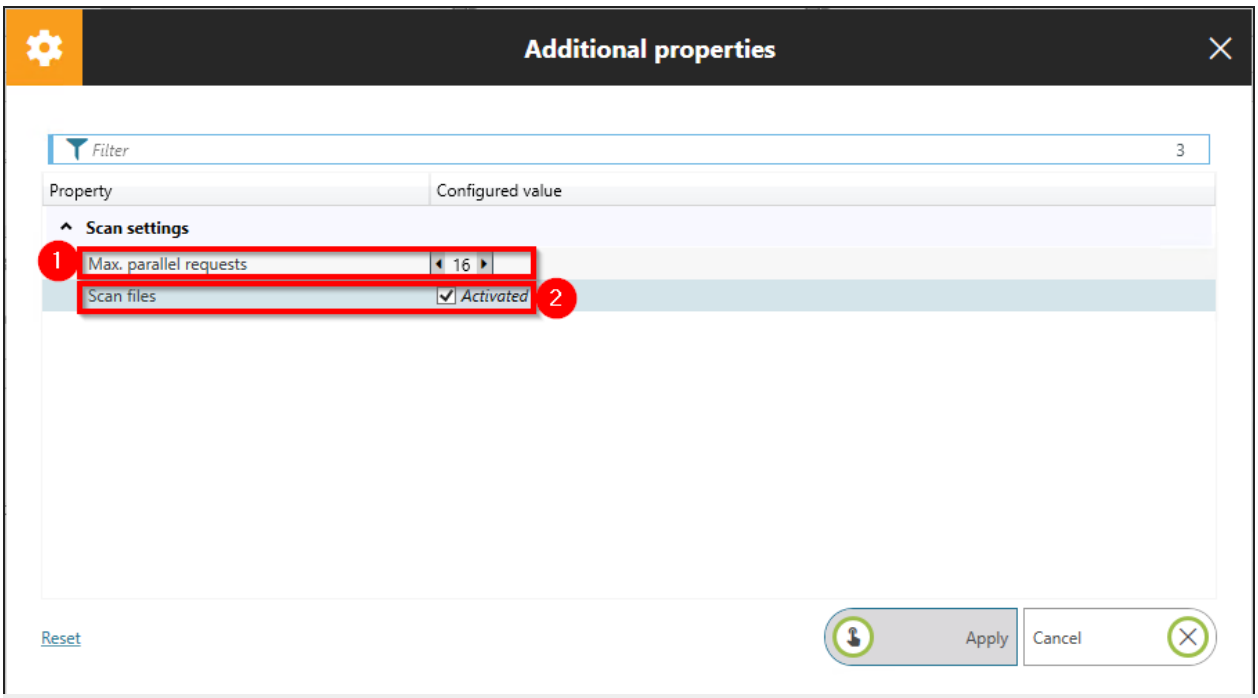


1. Activate the required resource (check the box).
2. Select one or more collectors. Note that the collector servers require an Internet connection.

Configure additional OneDrive scan properties



Click the link.



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!

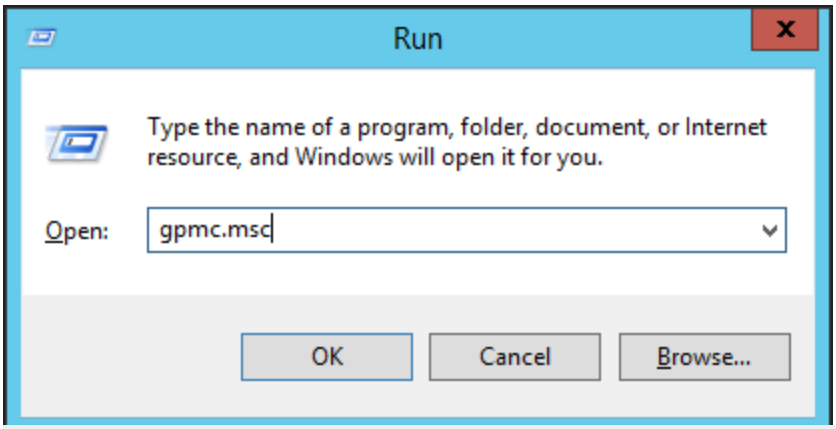
Configure audit policies for DCs on Server 2008 R2 or higher

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.

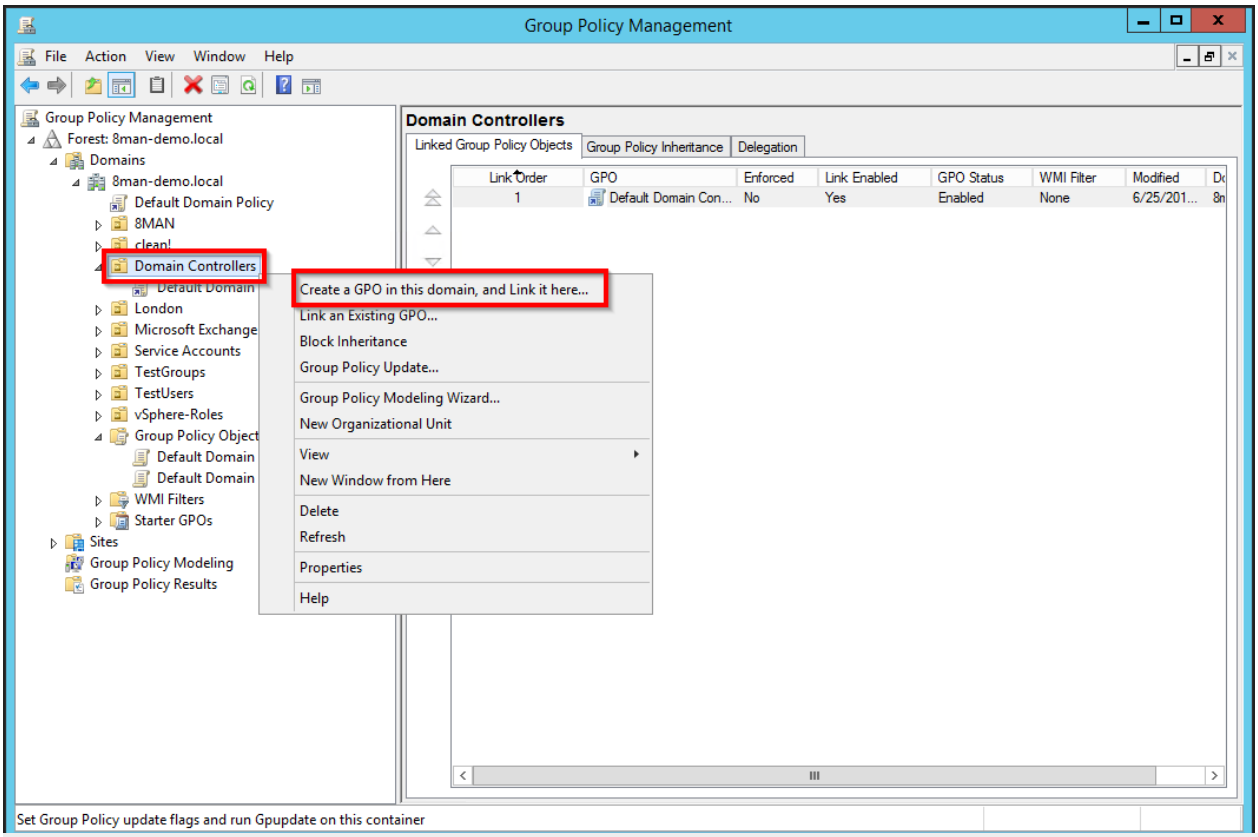
Once you have completed these settings:

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



Start managing group policies, by opening:

```
gpmc.msc
```

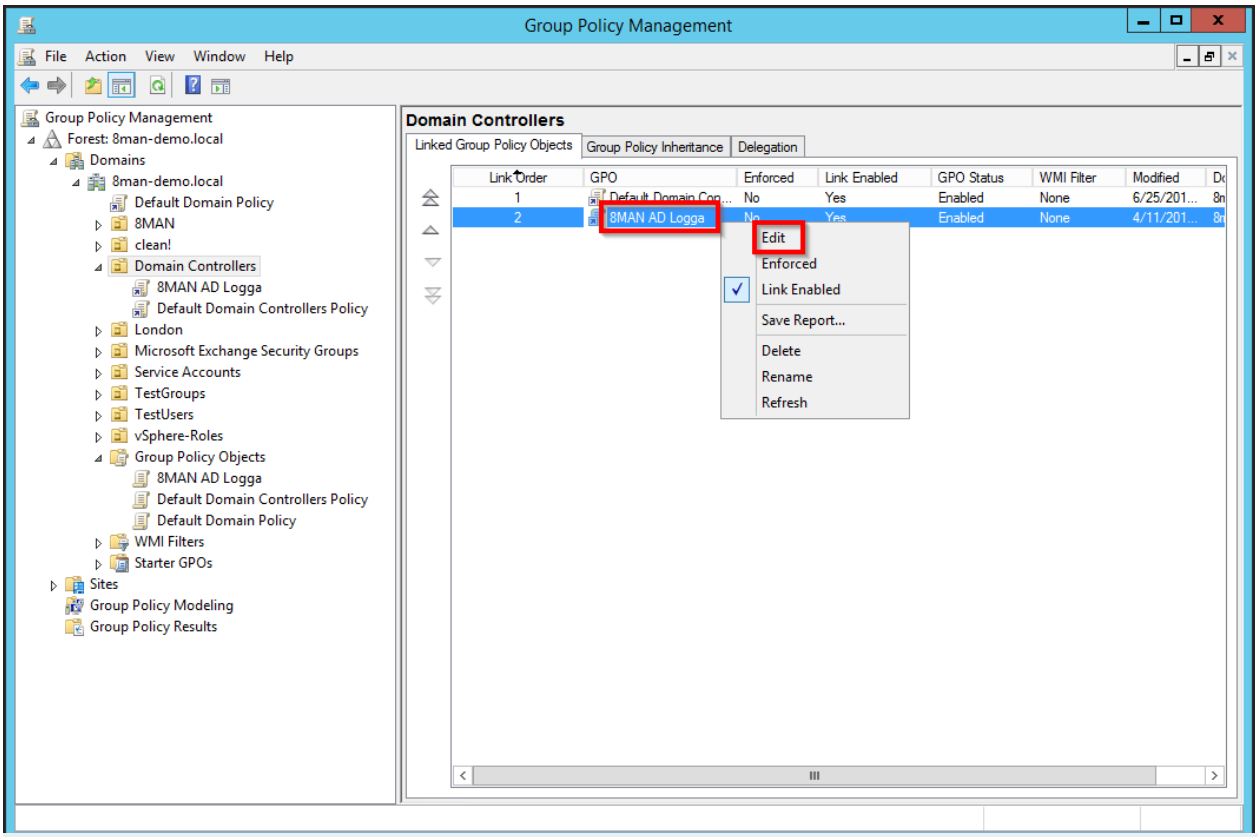


Create a new group policy.

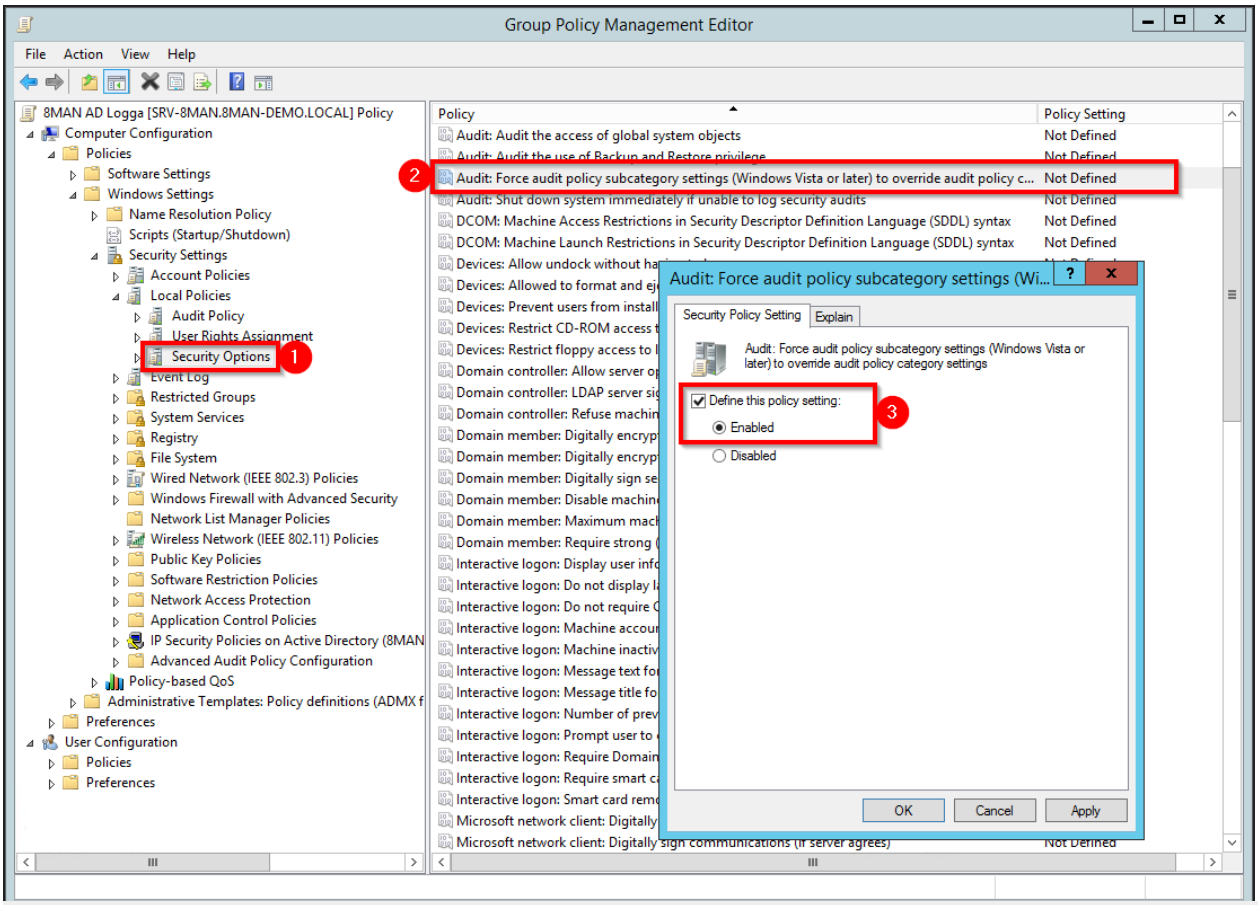
Select the OU in which the DC computer accounts are located. By default they are located in the OU "Domain Controllers".

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!

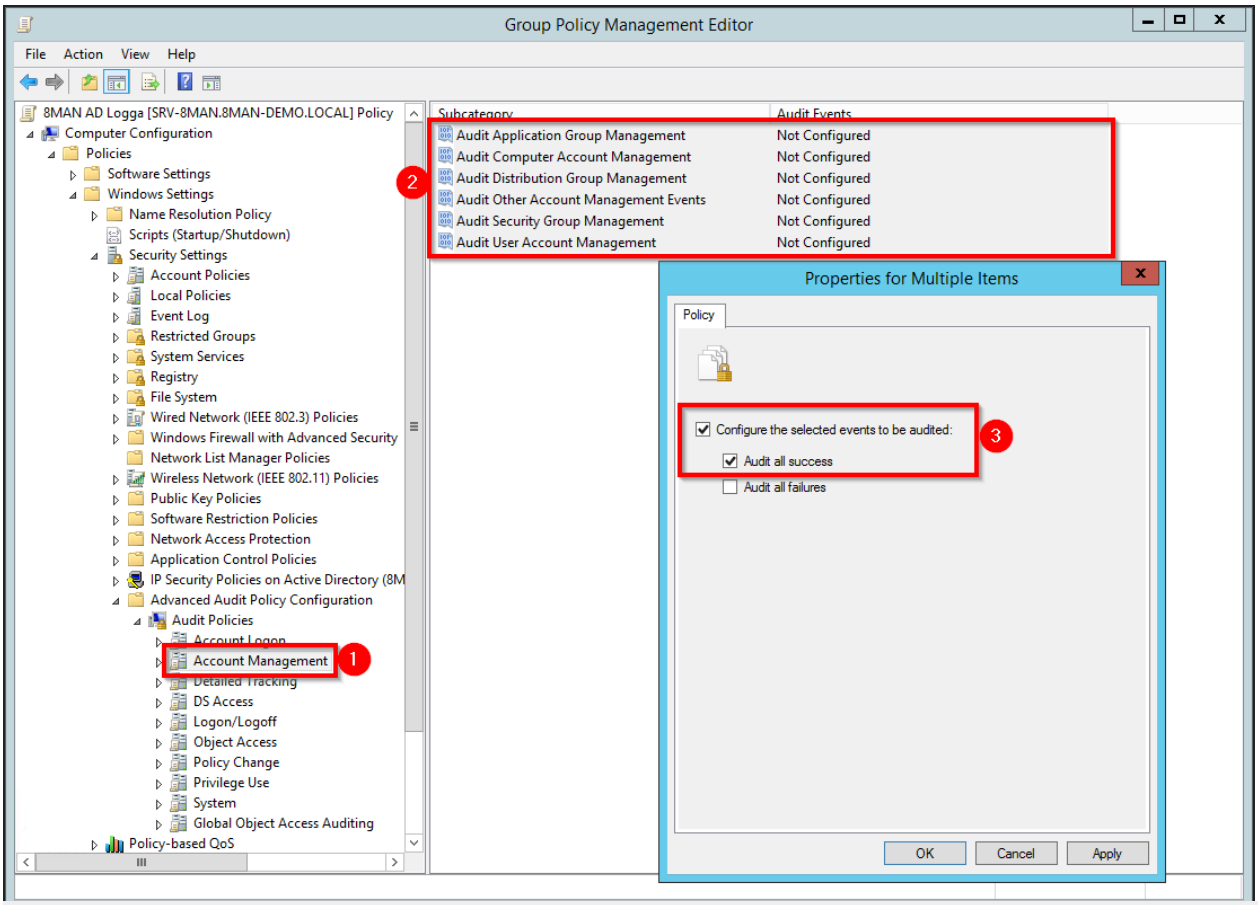


Select the newly created group policy by right clicking and selecting "edit".

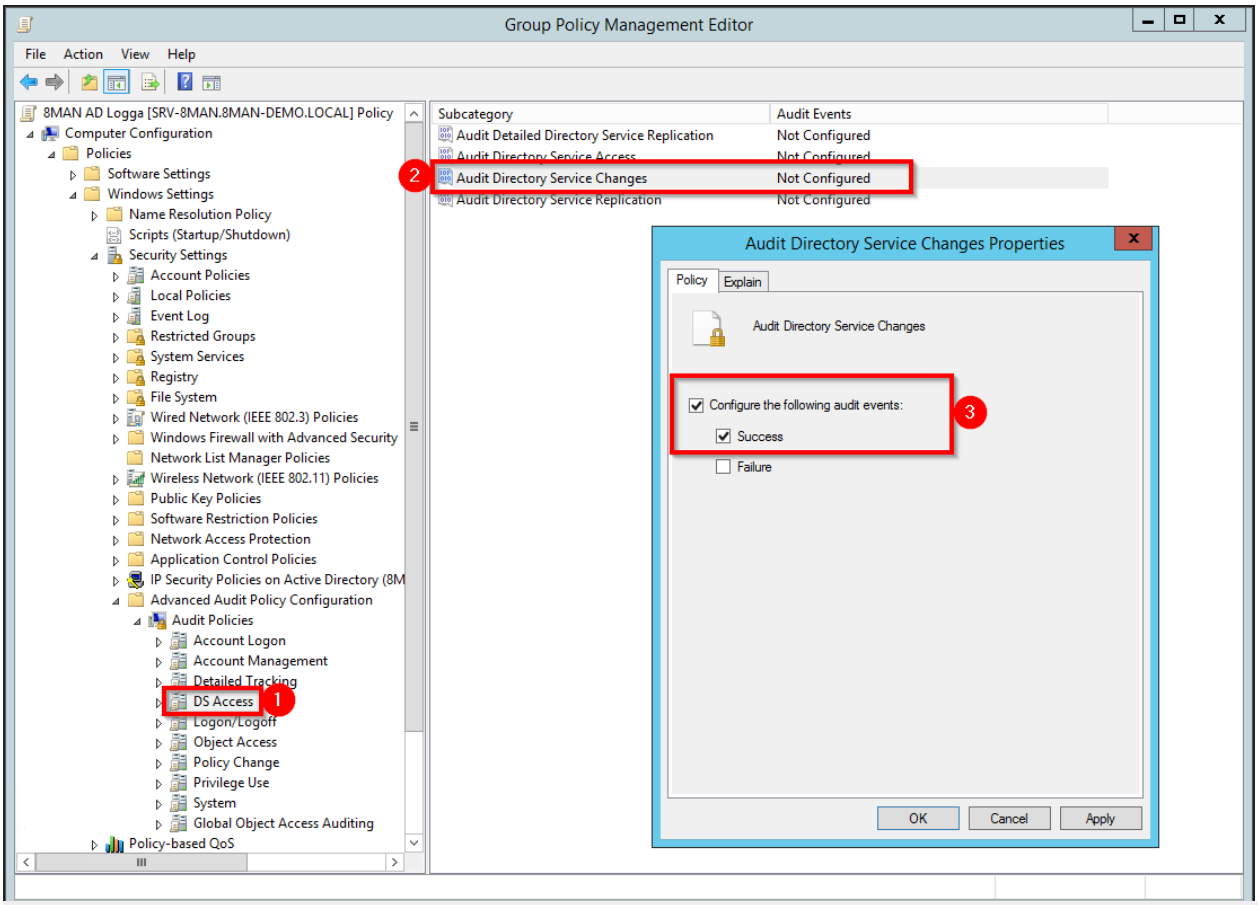


1. Navigate to "security options".
2. Double-click the policy "Audit: Force audit policy...".
3. Activate the security policy as shown in the screenshot.

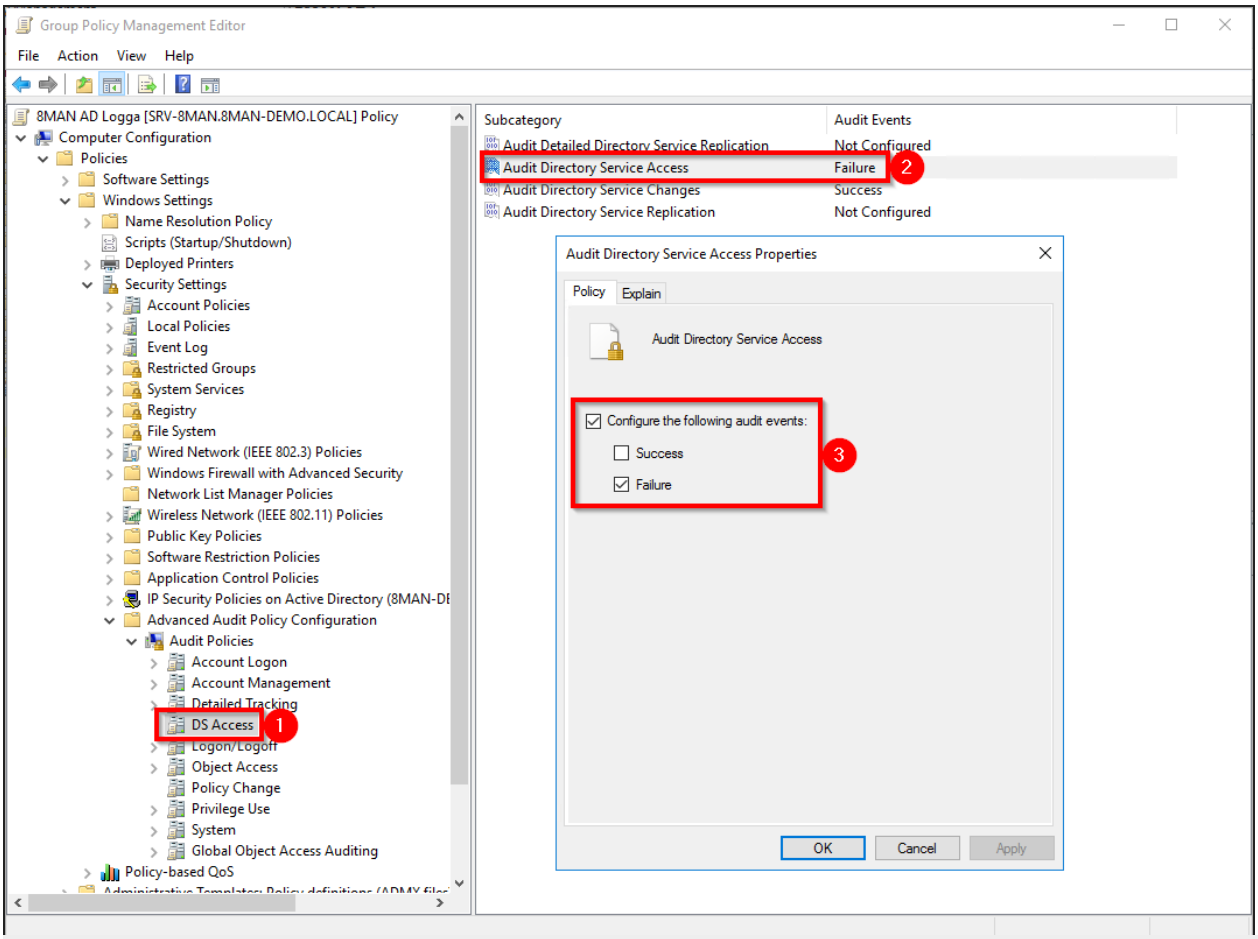
⚠ The order in which you set the options affects the effectiveness of the policy. Follow the order given here!



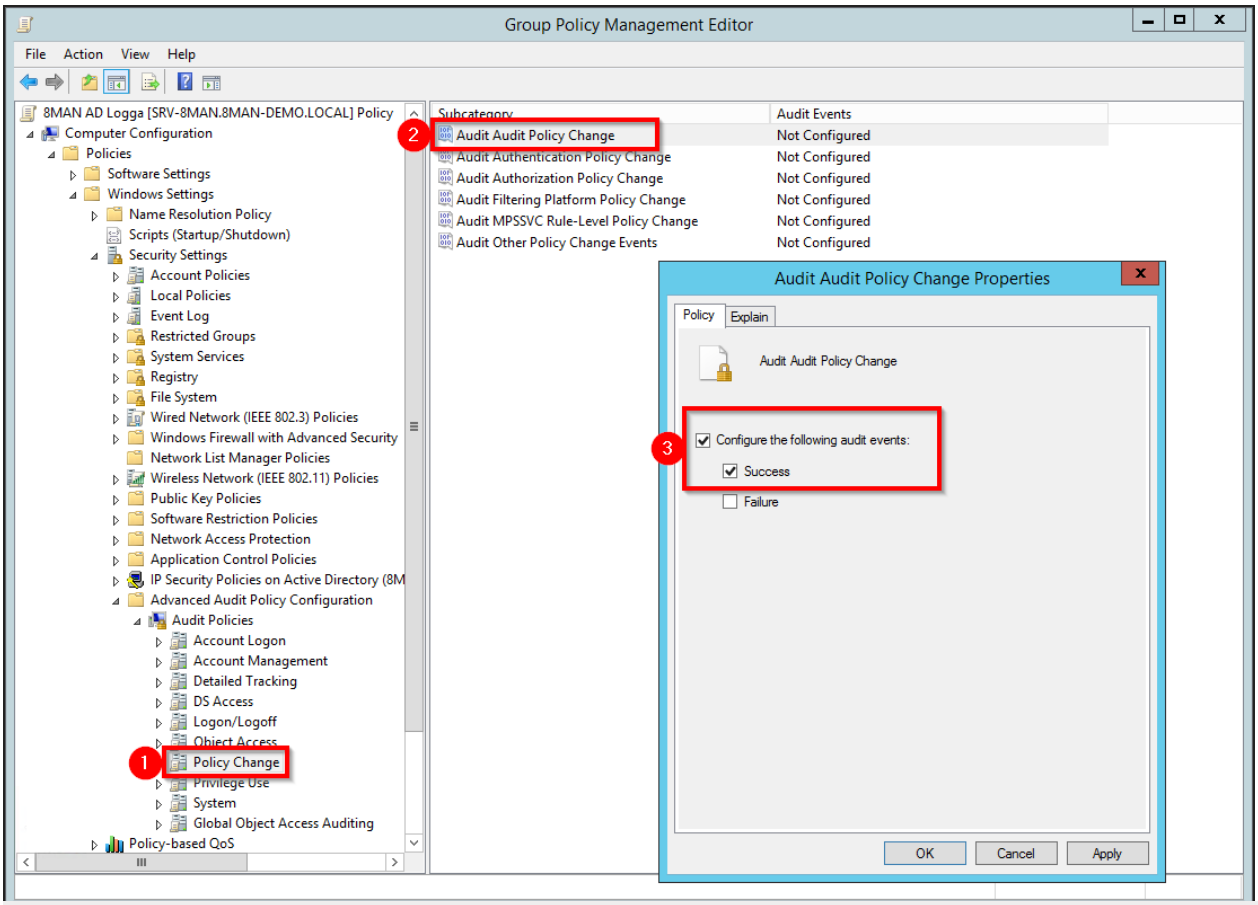
1. Navigate to account management.
2. Use multi-select and select **all** subcategories.
3. Activate the audit by right-clicking and selecting "Properties", as shown in the diagram.



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. (© 2020 Microsoft, 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

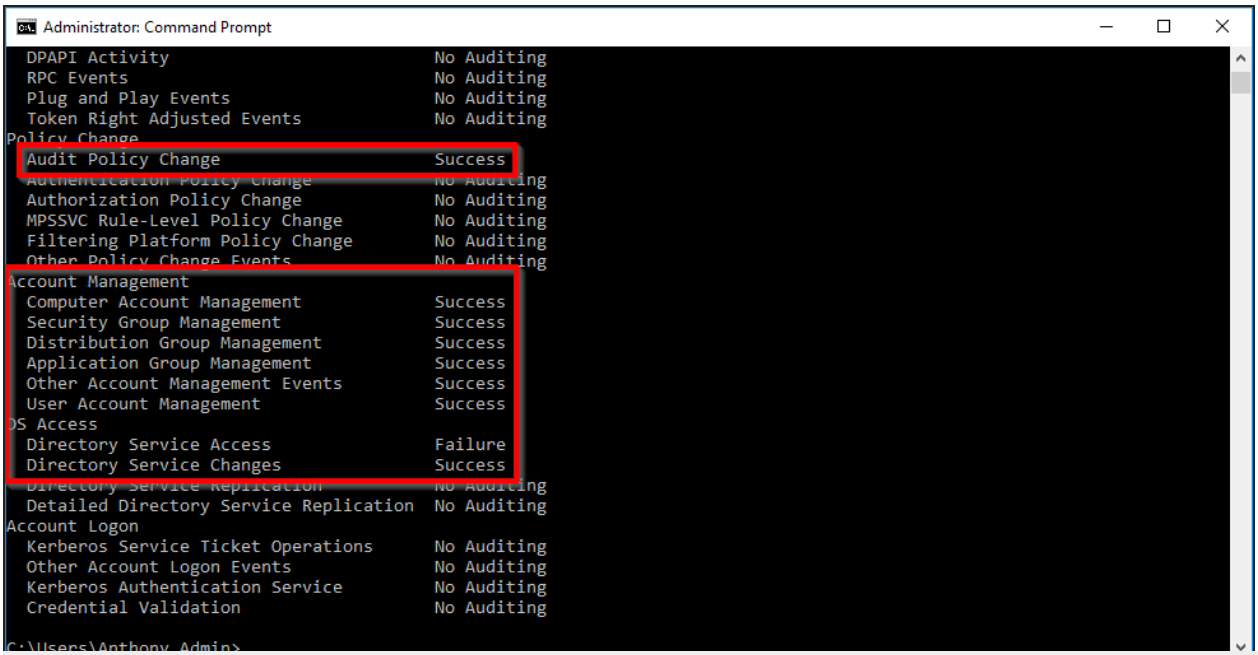
You can verify the effectiveness of audit policies by starting the command prompt with admin rights and entering the following command:

For english servers

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

For all languages

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



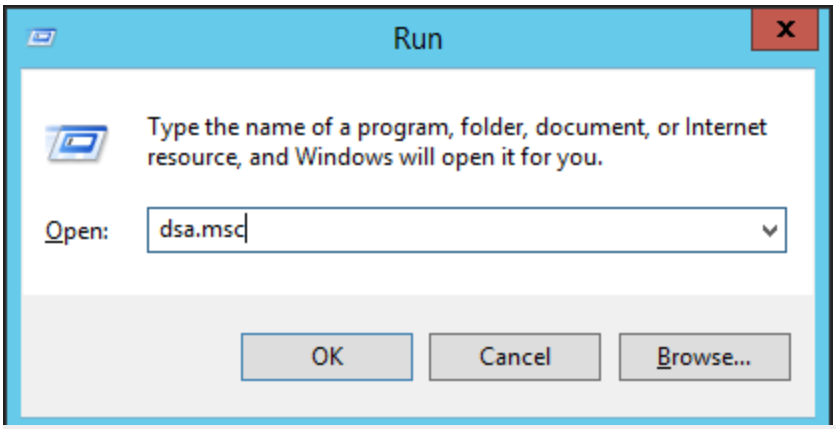
The marked subcategories must be set to "Success" or "Failure" as shown.

Set audit permissions in the AD object SACLs

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

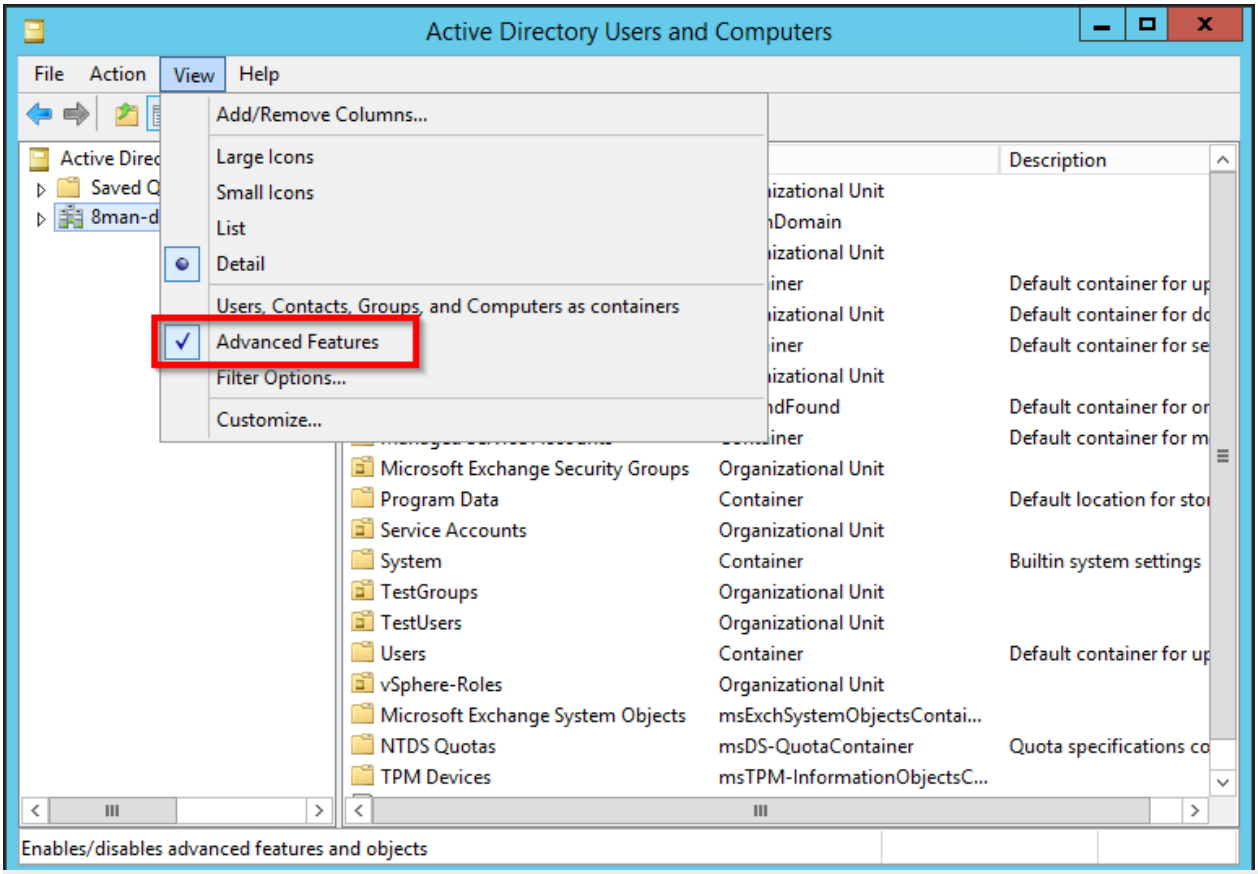
The user right "Manage auditing and security log" is required for the configuration of the SACL (this corresponds to the privilege "SeSecurityPrivilege"). You must be a member of the "event log reader" or domain admin group.

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

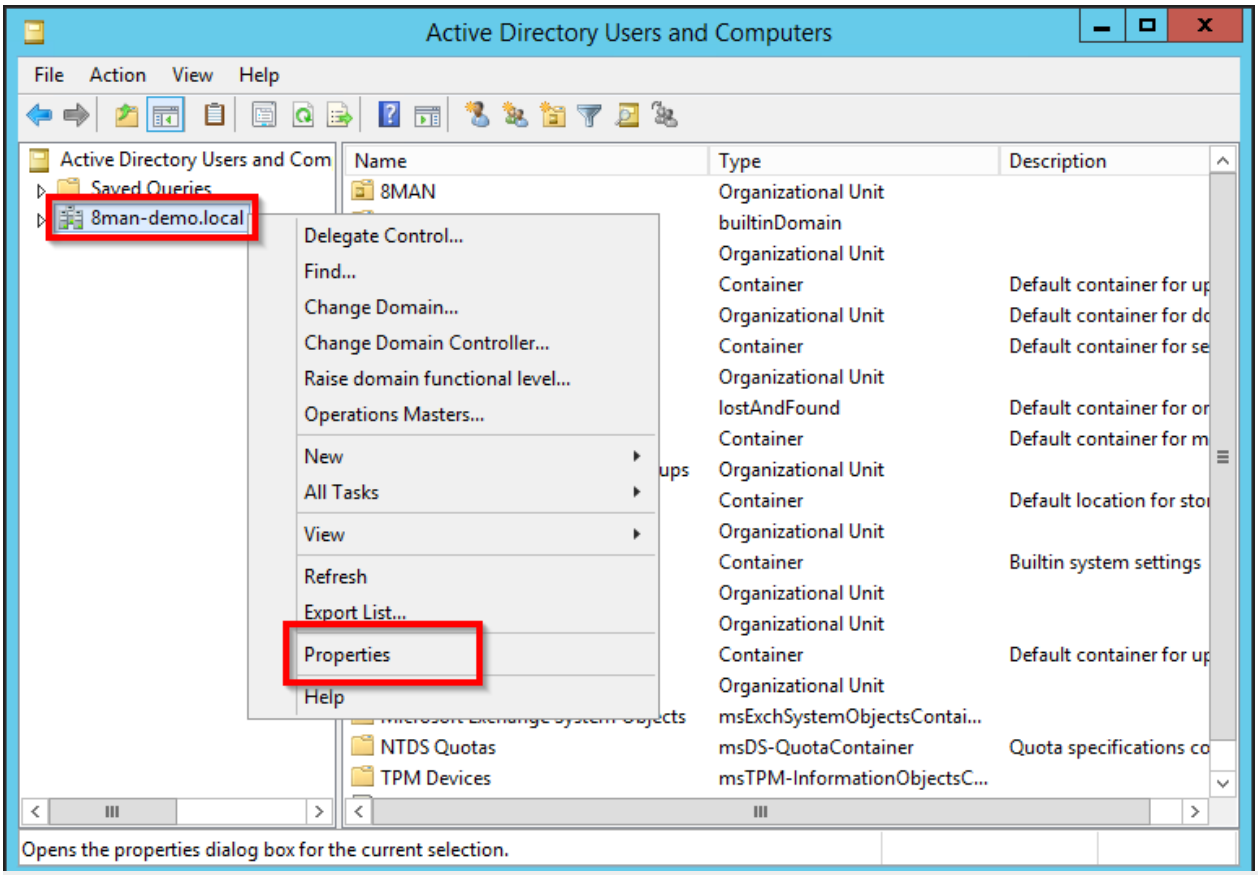


Start the management of Active Directory users and computers on a DC by opening

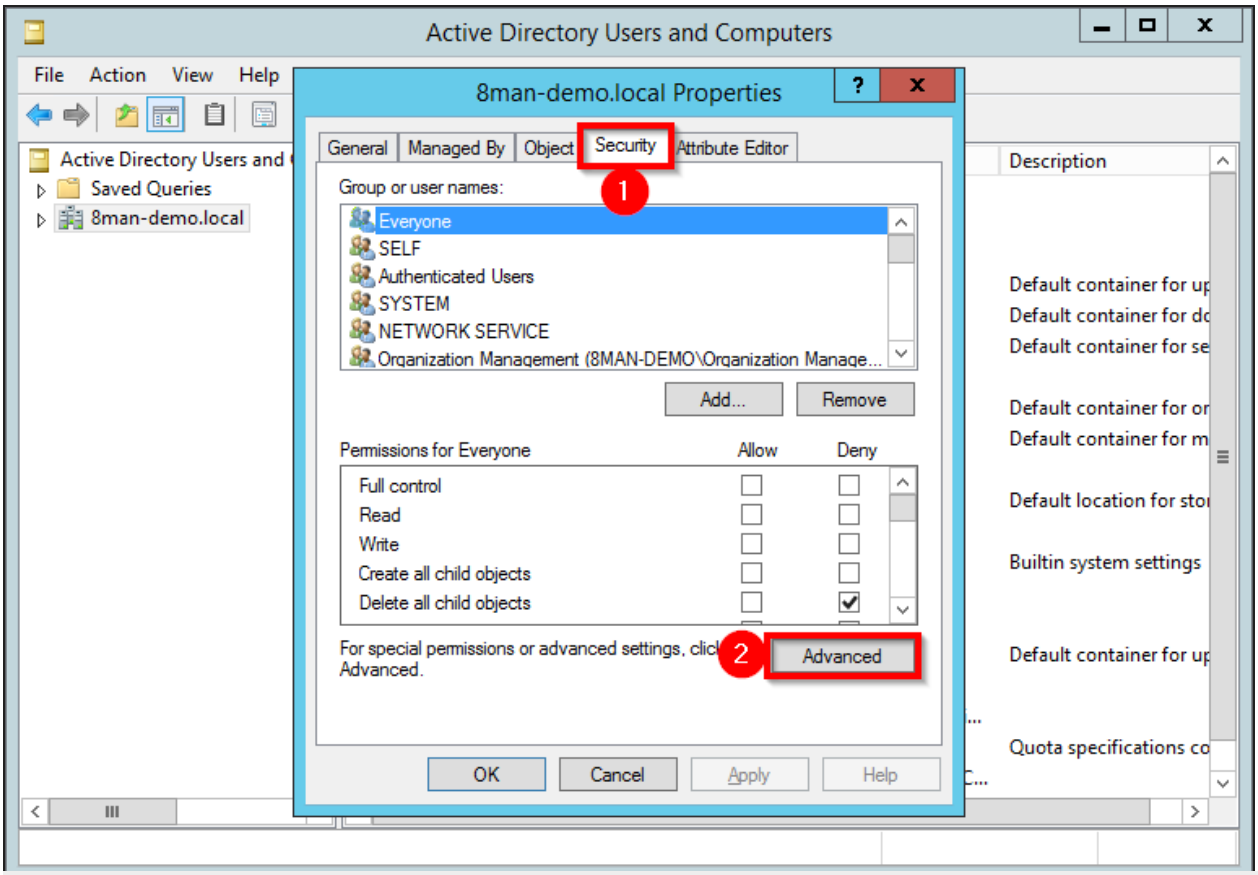
```
dsa.msc
```



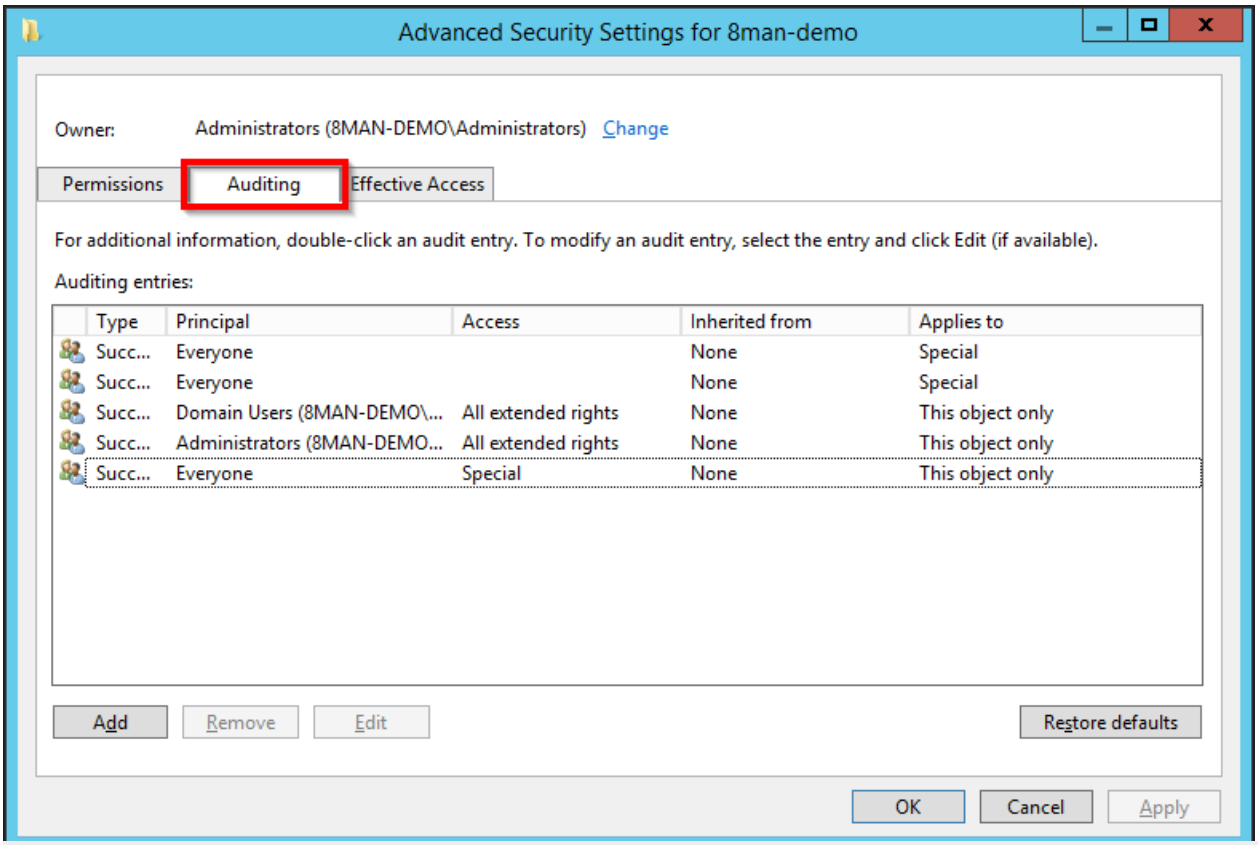
Activate the option "Advanced Features".



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



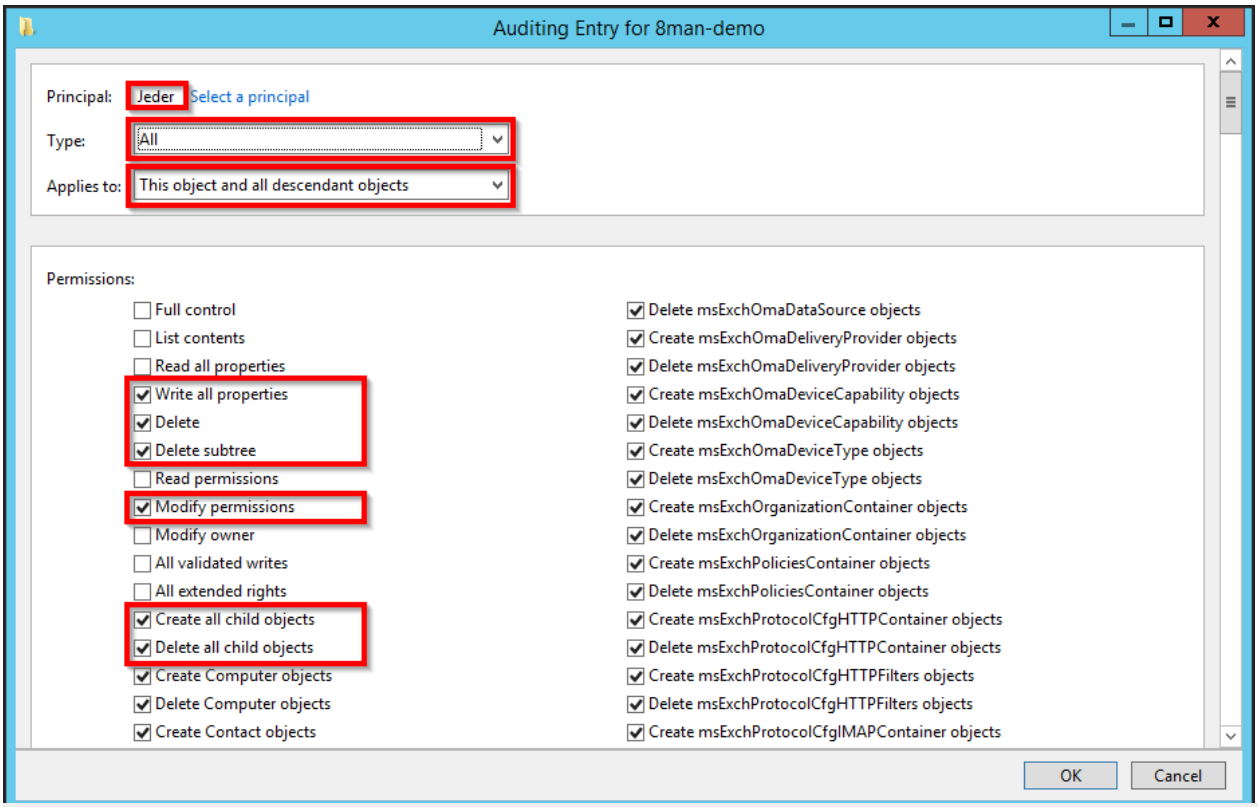
In the properties window, select the tab "Security" and then click on "Advanced".



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.



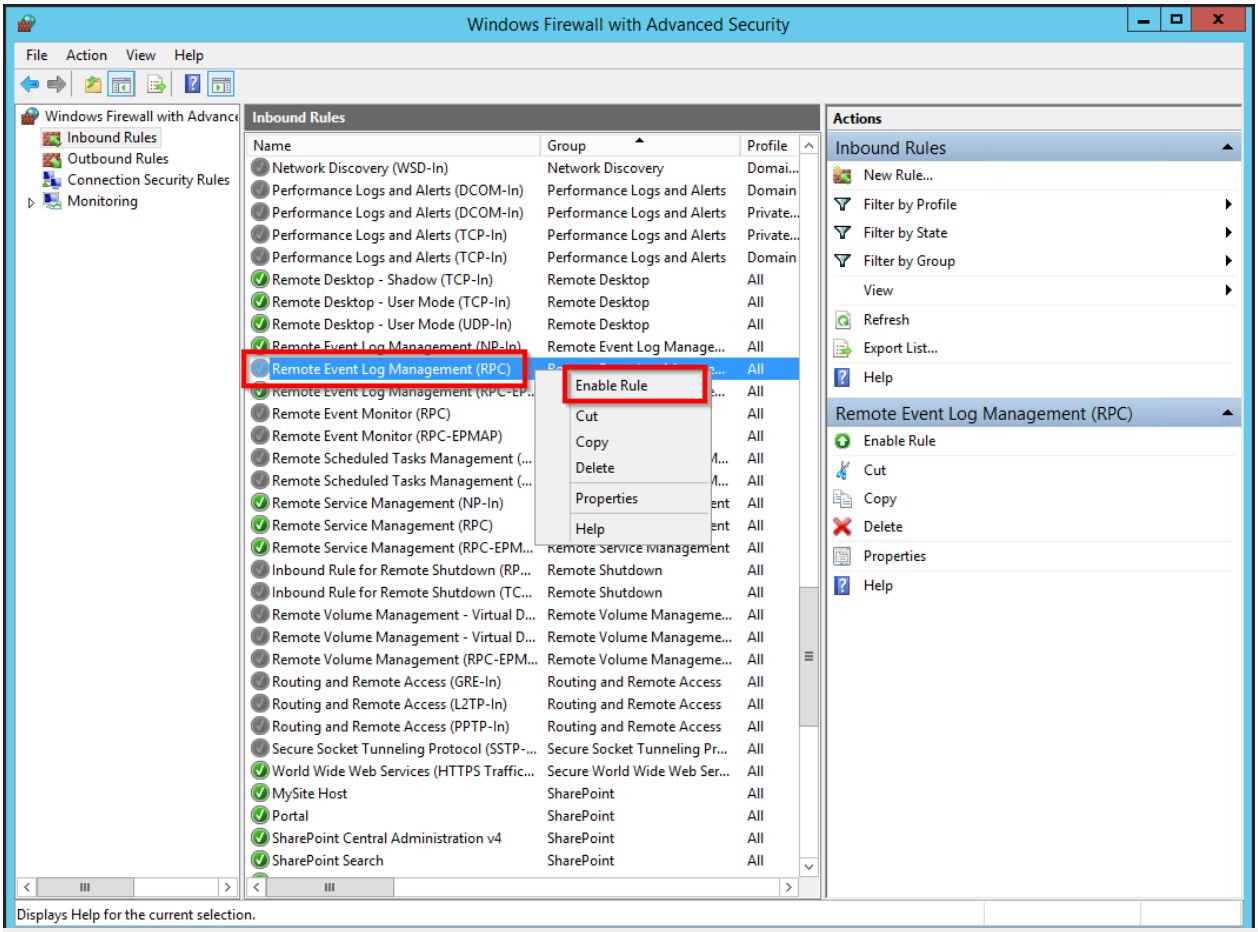
At minimum, the following is required:

- 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

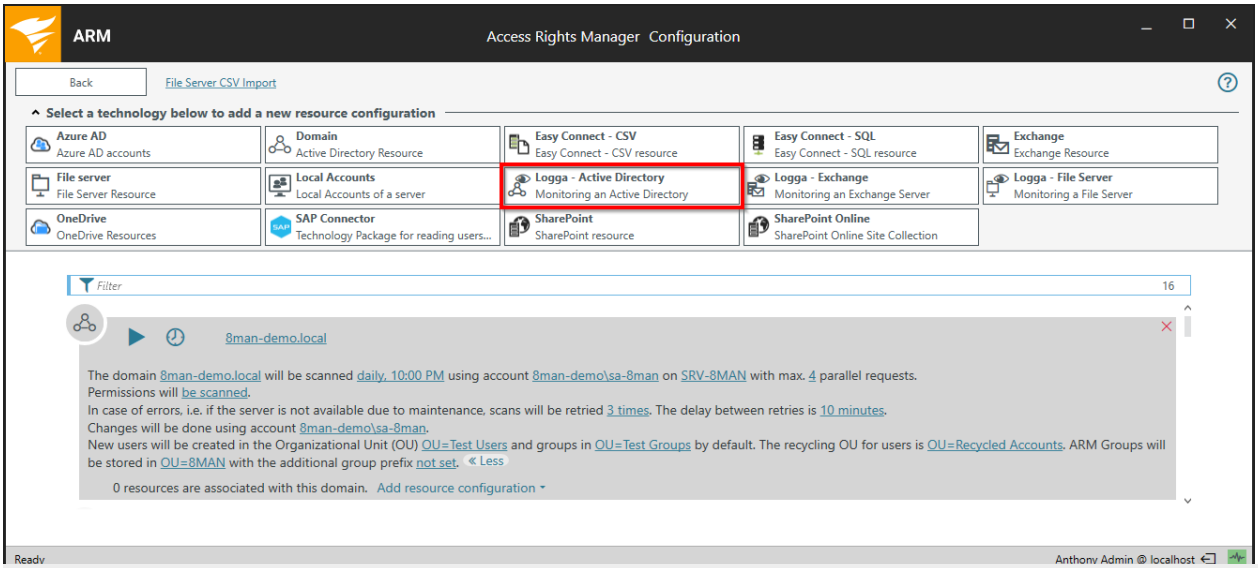
Configure the Windows firewall for AD Logga



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.

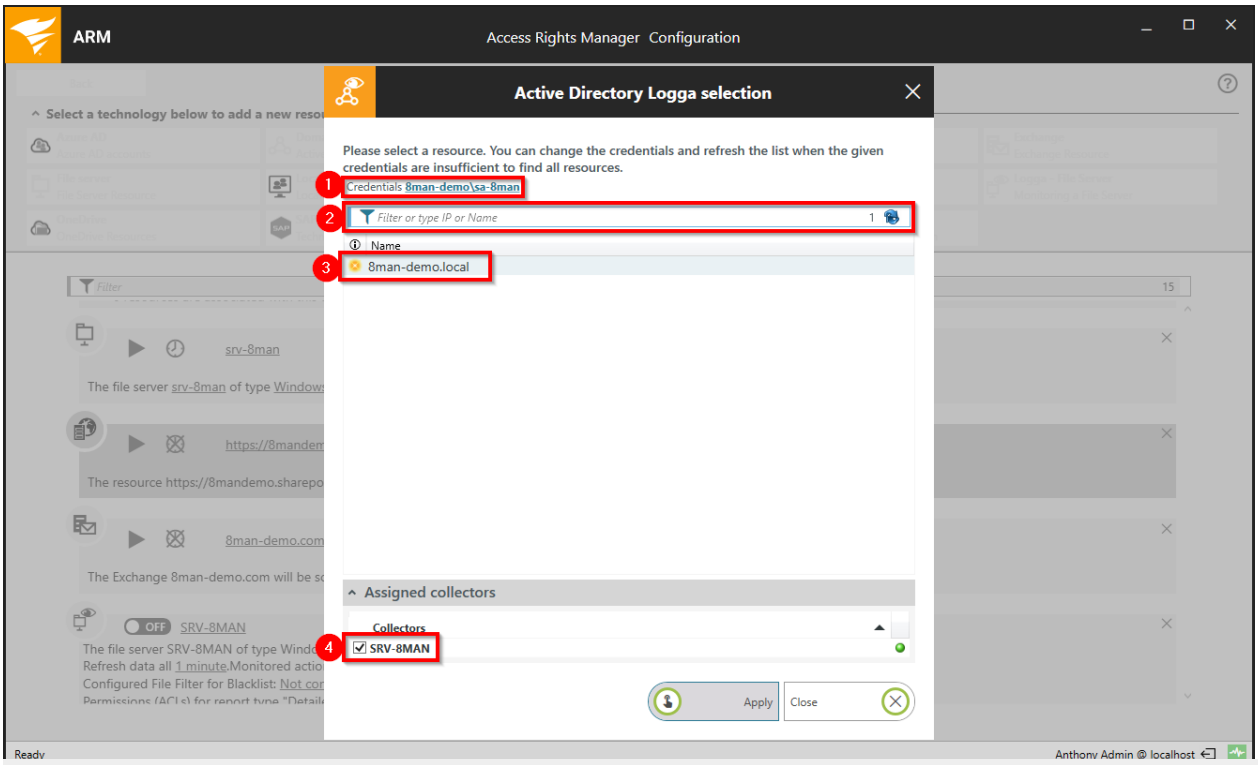
⚠ Repeat the procedure for each DC to be monitored.

Add an AD Logga configuration



On the configuration home page select "Scans".

Select "Logga - Active Directory".

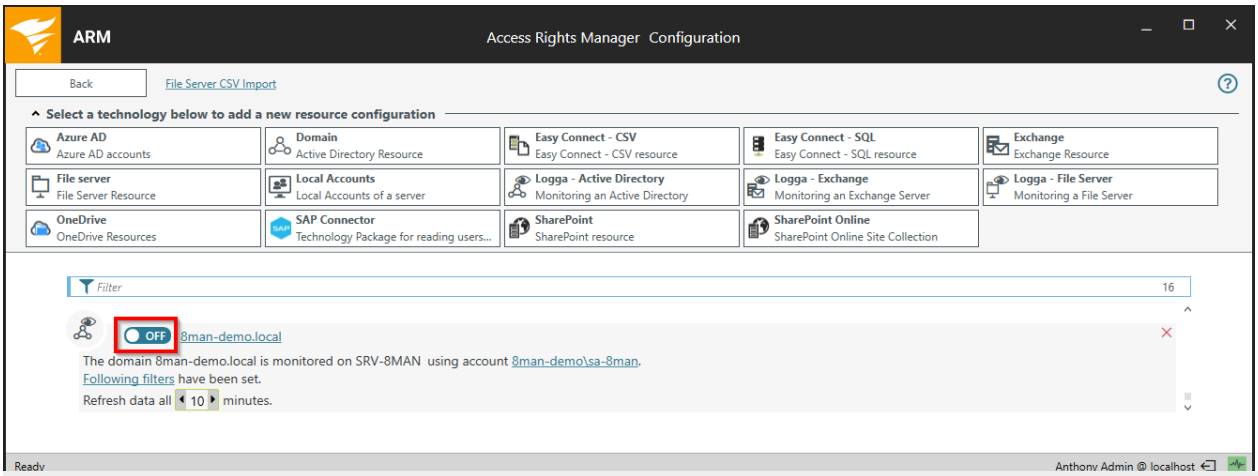


1. Enter valid credentials for the domain that you want to monitor.
2. Use the filters to find the desired domains.

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.

After adding an AD Logga configuration, it initially remains deactivated. You must activate the AD Logga to record events.

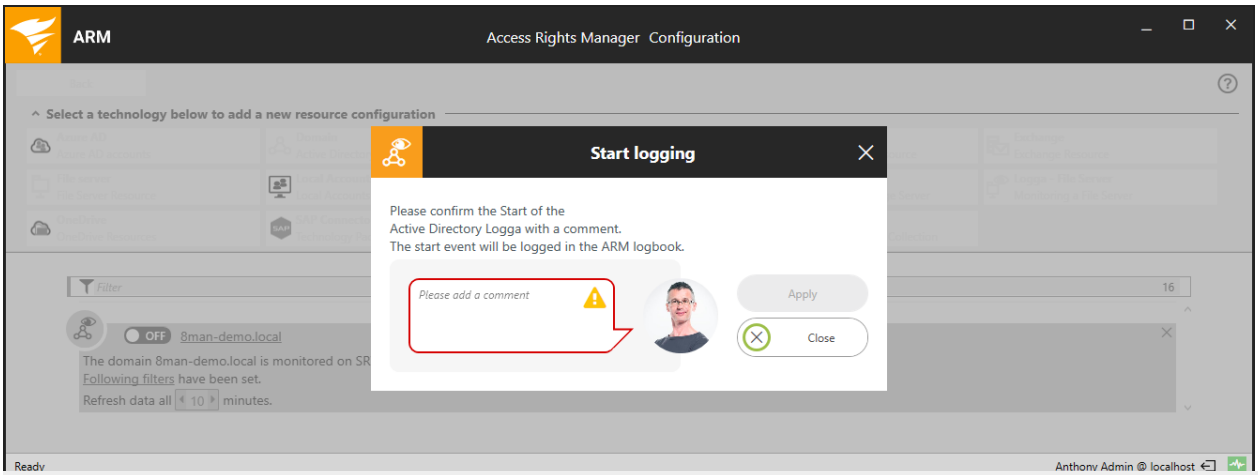
Activate or deactivate AD Logga



On the configuration home page select "Scans".

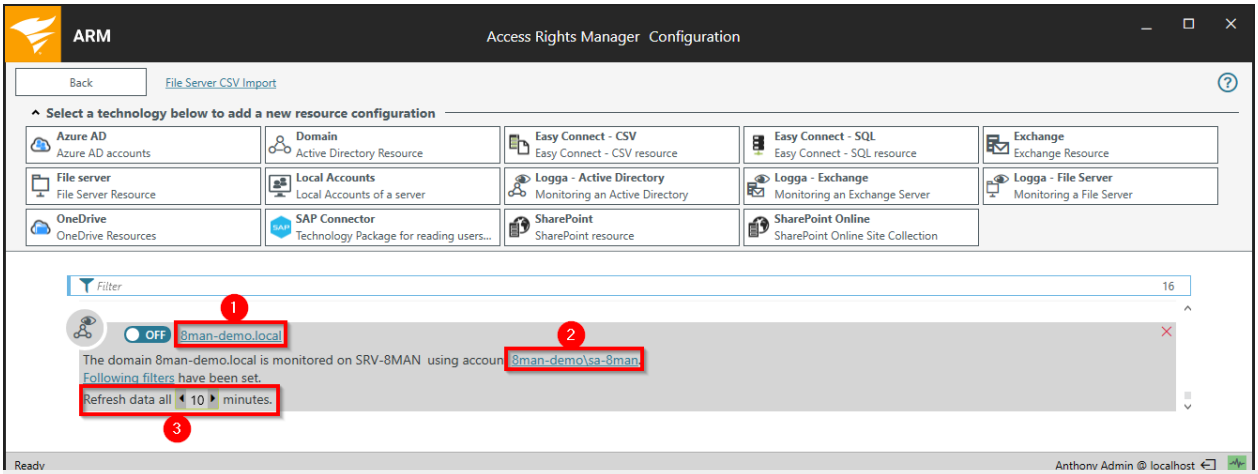
Click on the switch icon to activate or deactivate AD Logga.

AD Logga events are stored by default for 30 days. See Configure storage of scans settings.



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.

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.

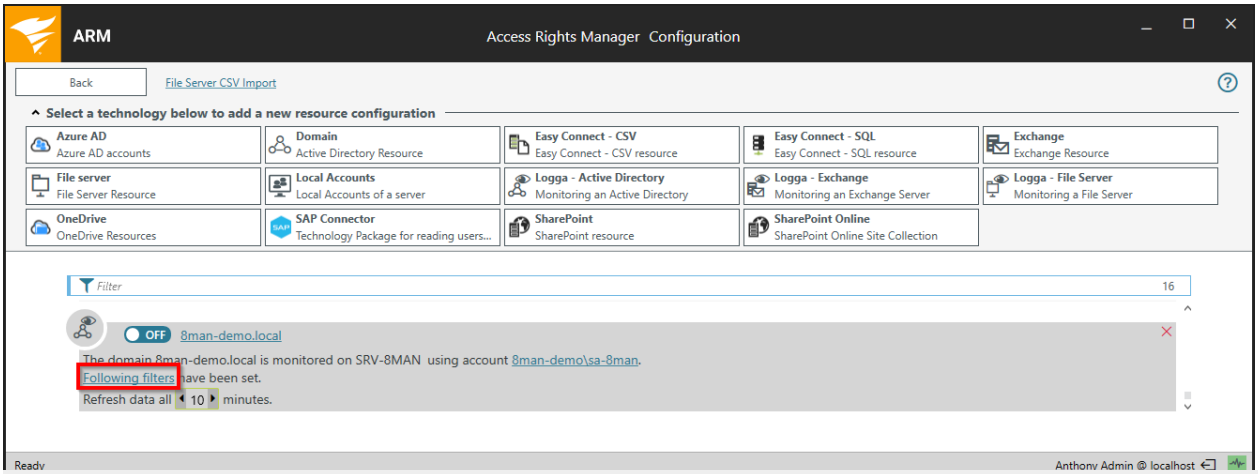
The filter criteria do not correlate to each other. The events are evaluated by the AD Logga consecutively based upon the entered criteria. If one of the criteria is fulfilled, the AD Logga immediately excludes the result independent of whether any other criteria have been evaluated.

For example:

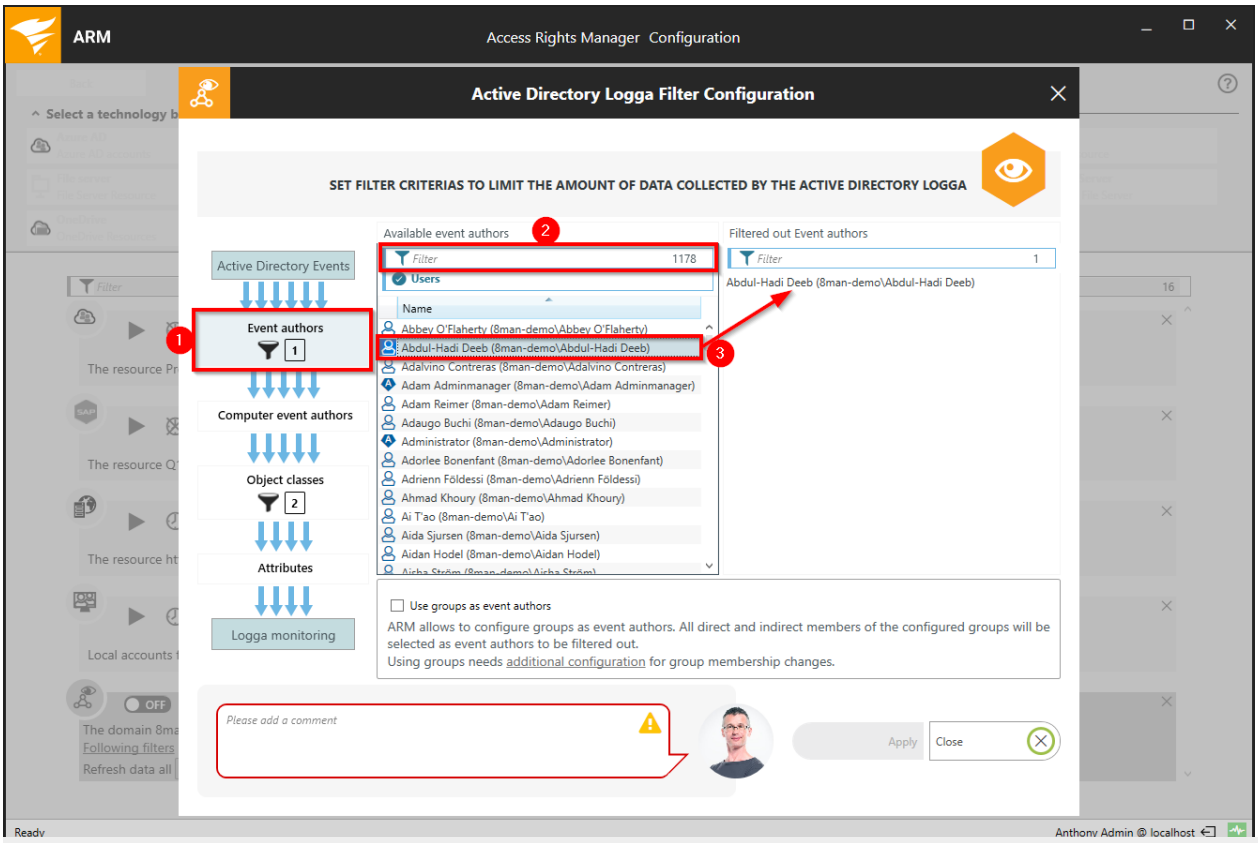
- If User A is configured as a filter, then all changes made by him will be excluded, even if the object classes or attributes that he made changes to are not configured as a filter. Changes that affect User A are still included.
- If object class X is configured as a filter, then all events, that include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

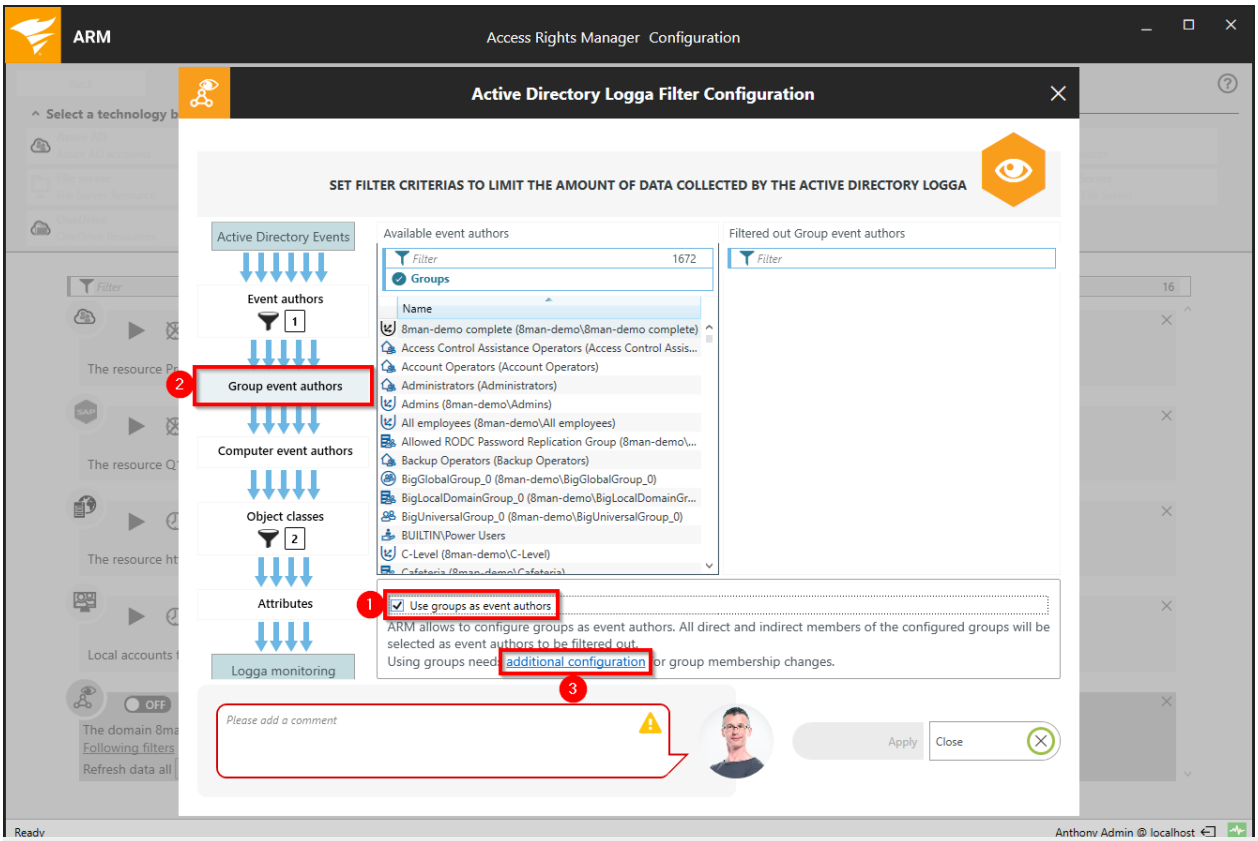
Configure the event filters



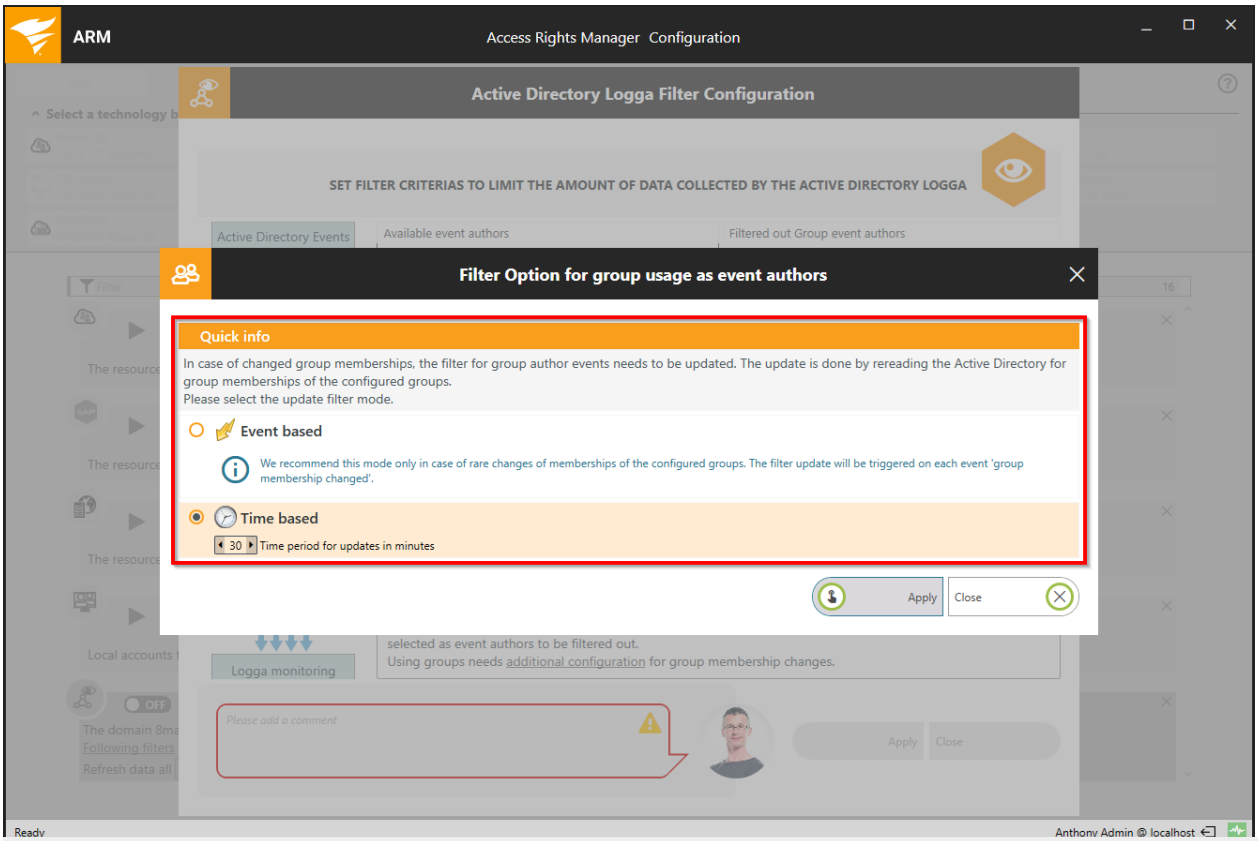
Click the link.



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.



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".

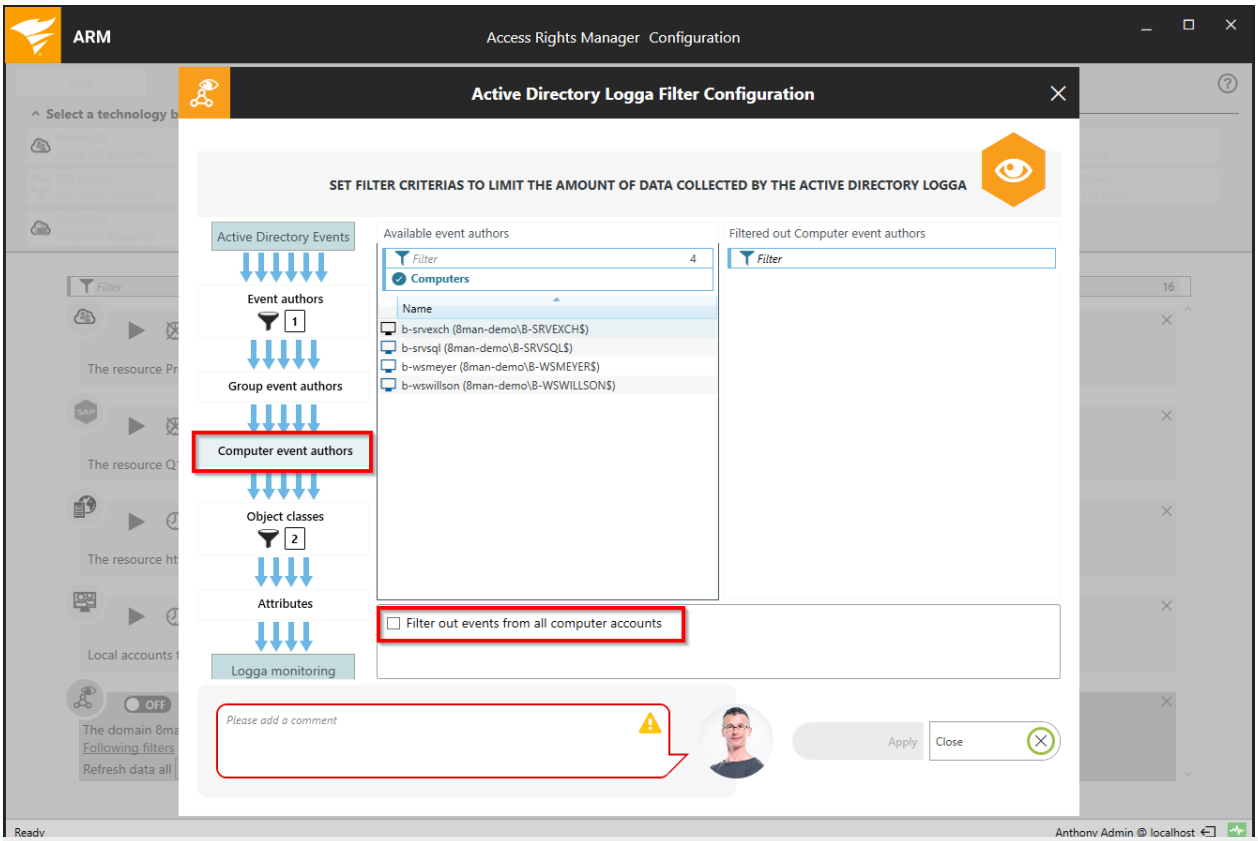


Determine which mode is used by the filter to update group memberships.

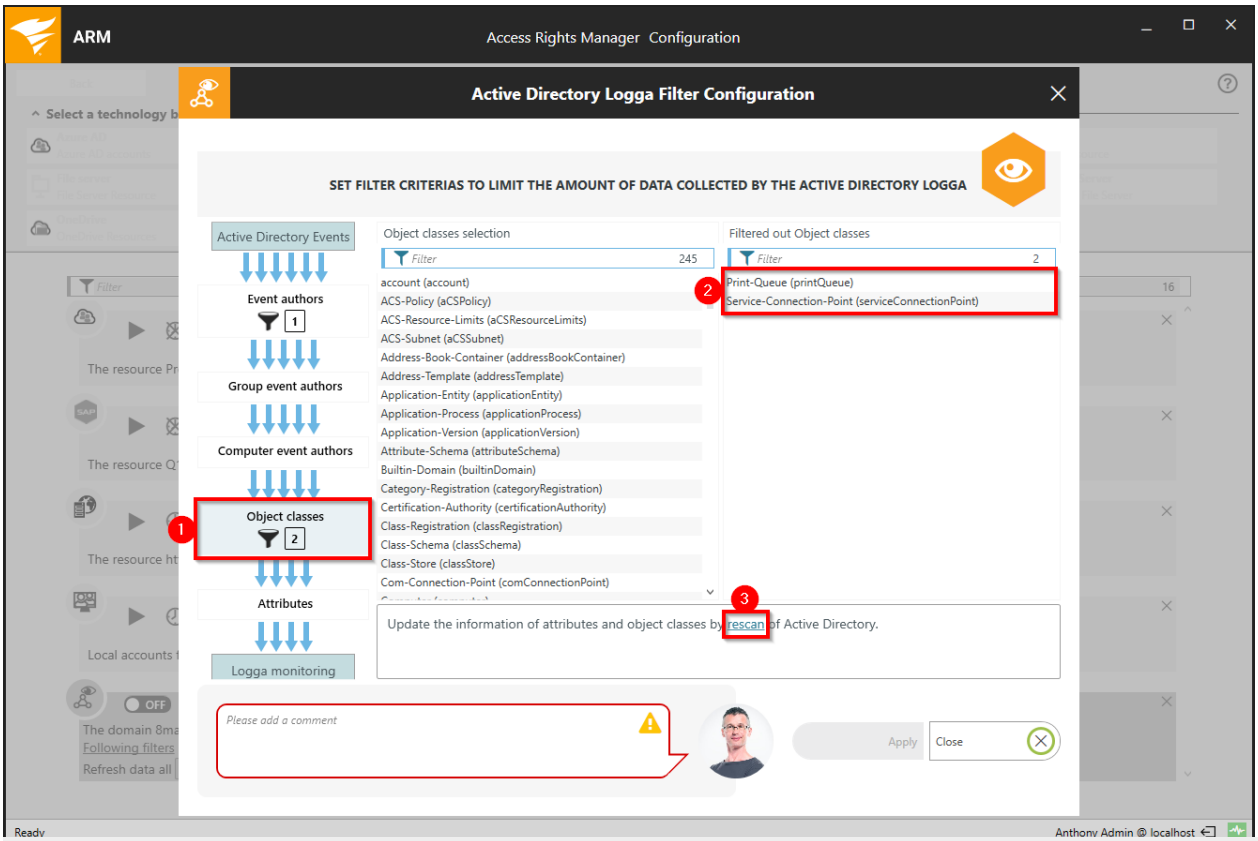
Please note the information in the displayed dialog.

Only use "event-based" if memberships in the filtered groups change rarely.

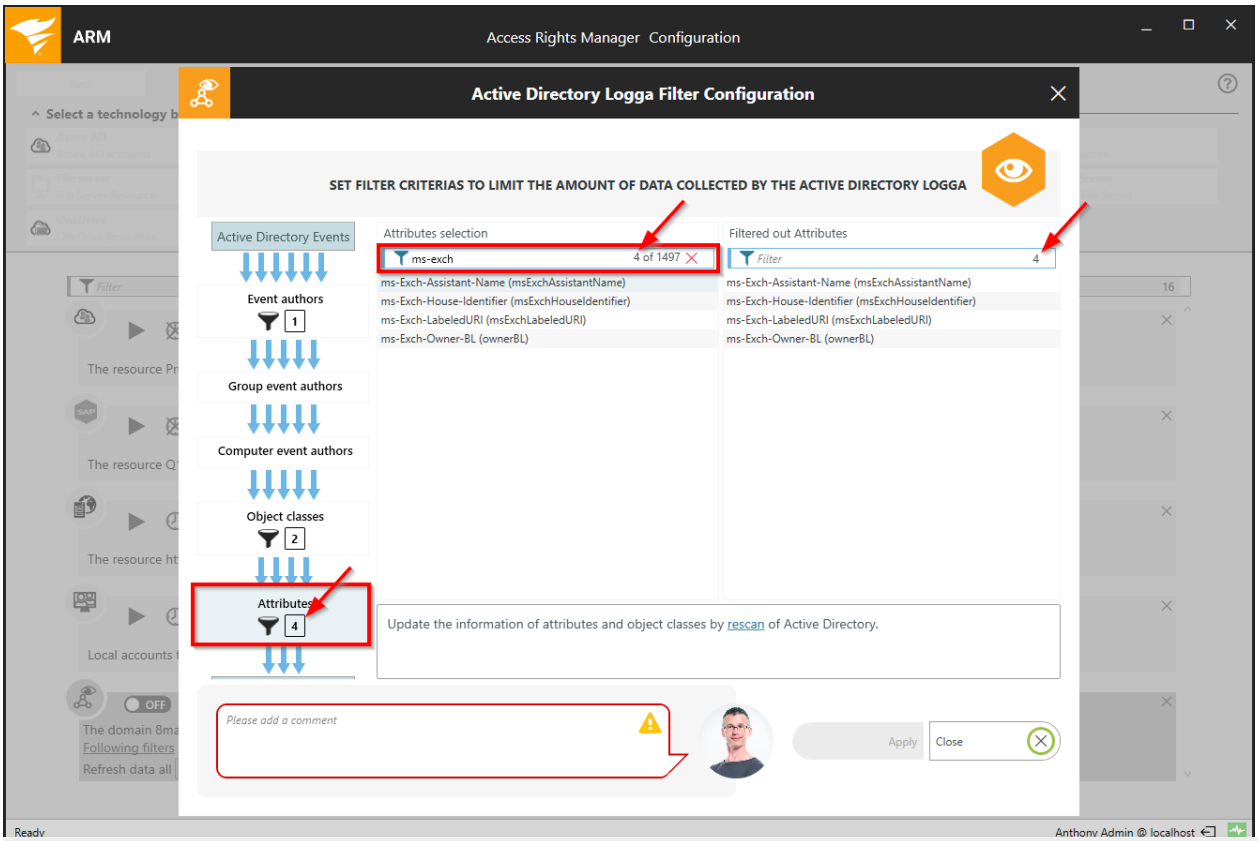
The update interval for the "time-based" option can be set between 10 and 1440 min (24h). The shorter the interval, the higher the load on your AD.



Filter events for selected or all computer accounts.



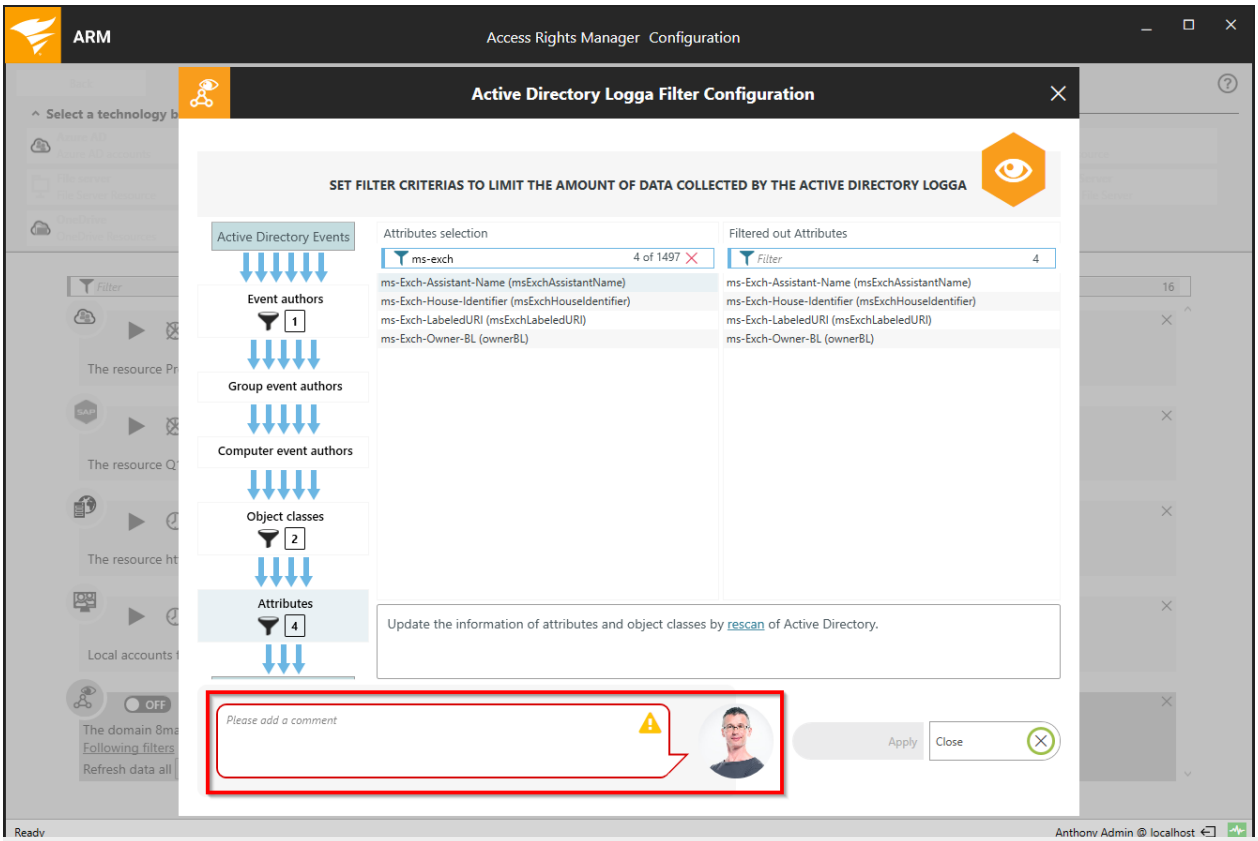
1. Filter the events of specific object classes.
2. By default events relating to the two selected object classes will be filtered.
3. The initial loading (and a rescan) of object classes from AD may take some time. After that the object classes will be loaded from the data base. Click "rescan" to update the object classes, e.g. after a schema change.



Filter events related to specific attributes.

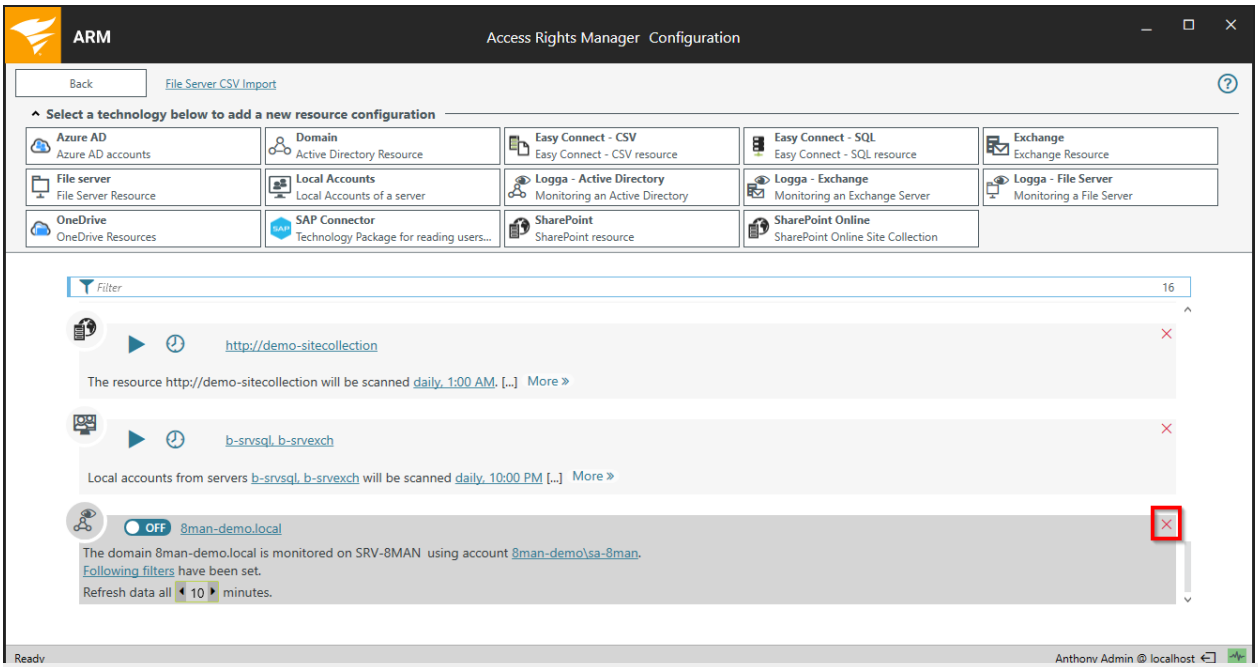
For example:

All events related to attributes that include "ms-exch" are filtered out / excluded.

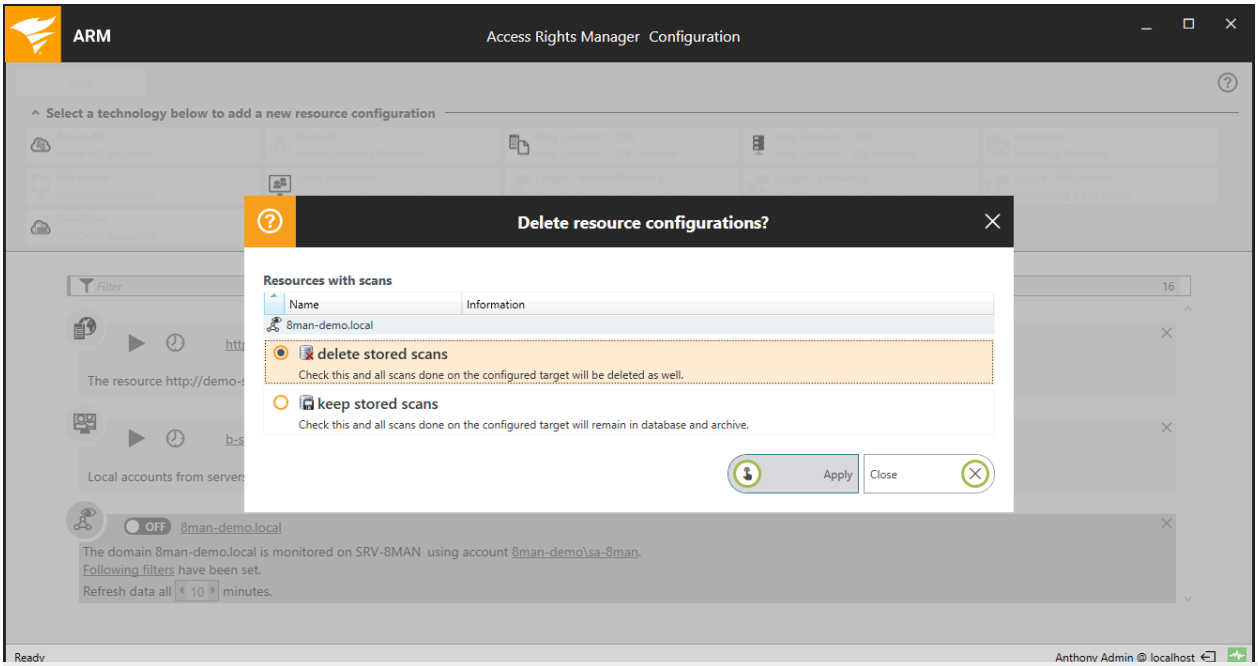


You must enter a comment to apply any changes made to filter settings.

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

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.

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).

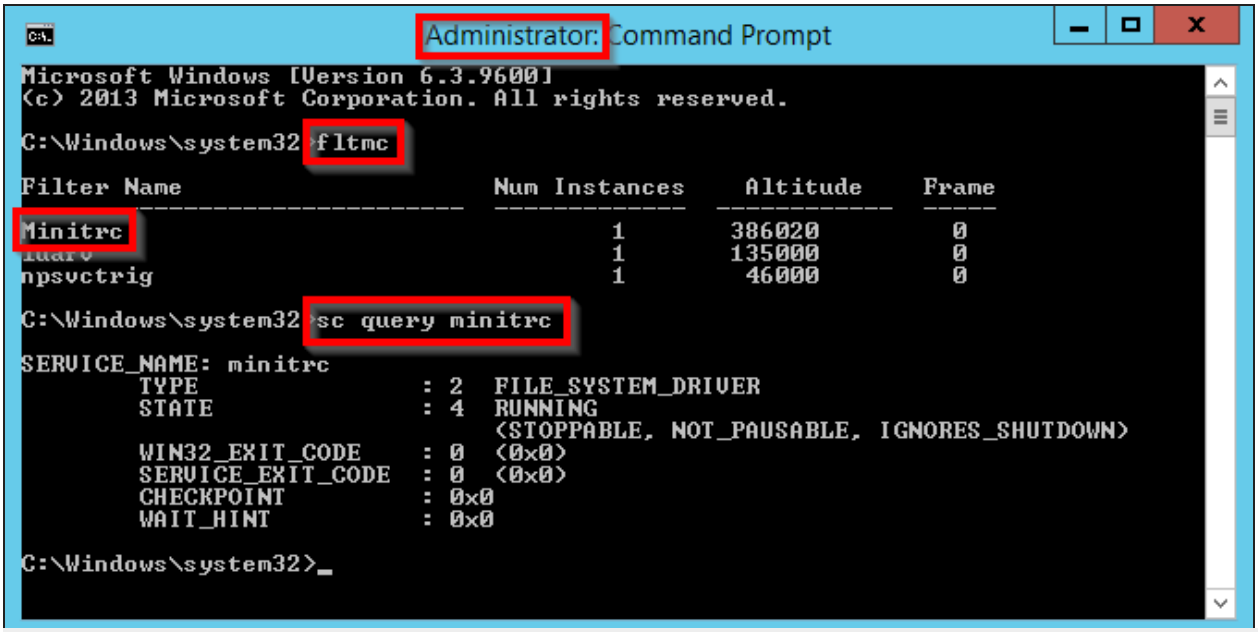
If you want to use the server name then make sure that the server name can be resolved by DNS or edit the hosts files. See also Collectors in foreign domains (non-trusted).

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.



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>
```

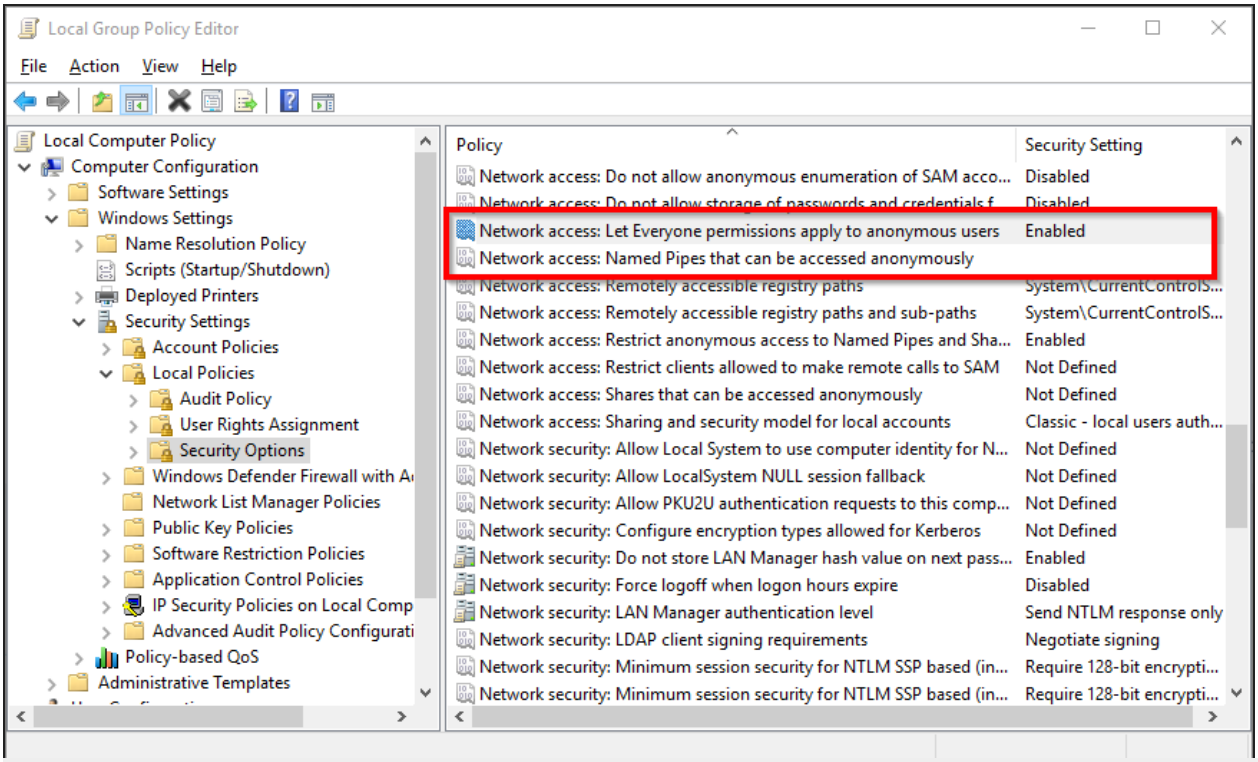
```
        </netapp>
    </tracer>
</config>
```

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.

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\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:

- wich events will be monitored
- wich events will not be monitored
- wich 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 pathes 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 EMC 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>
```

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 (© 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 youwant 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).

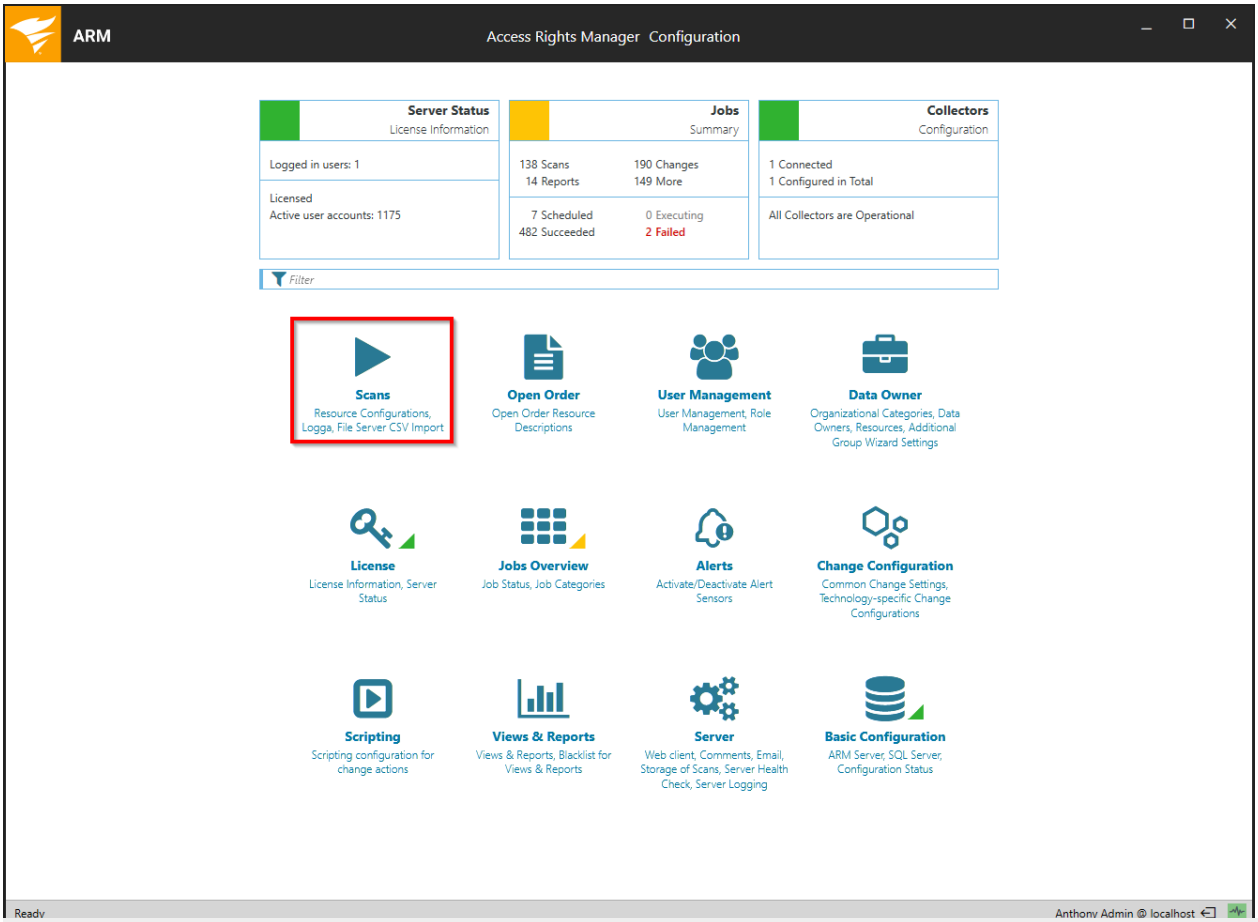
This setting is the basis for the selection of the directories to be monitored in the FS Logga Reports. If you select a directory for an FS Logga report that is not included in a monitored zone, the report will contain no events.

```
isi audit settings global modify --audited-zones <zone>
```

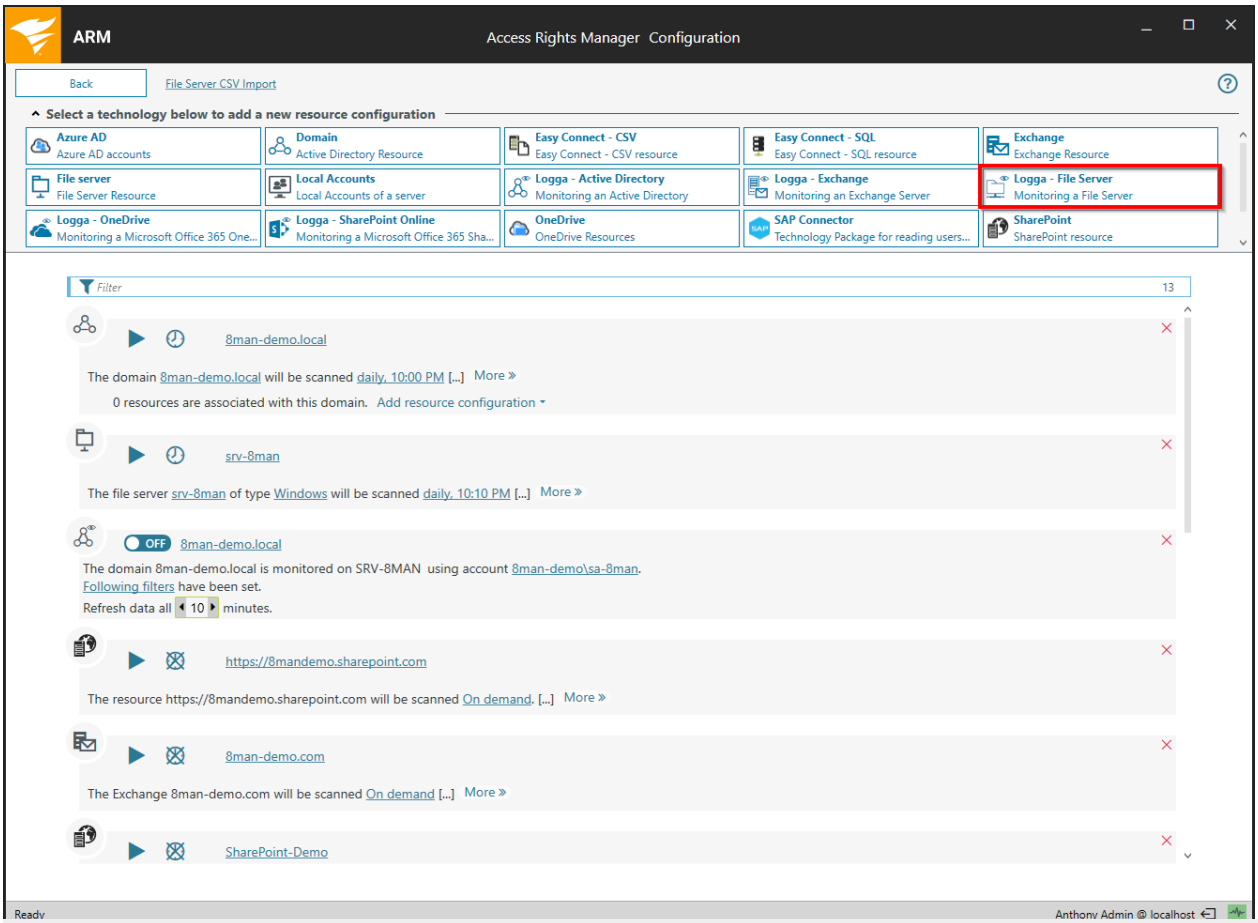
Enable auditing

```
isi audit settings global modify --protocol-auditing-enabled on
```

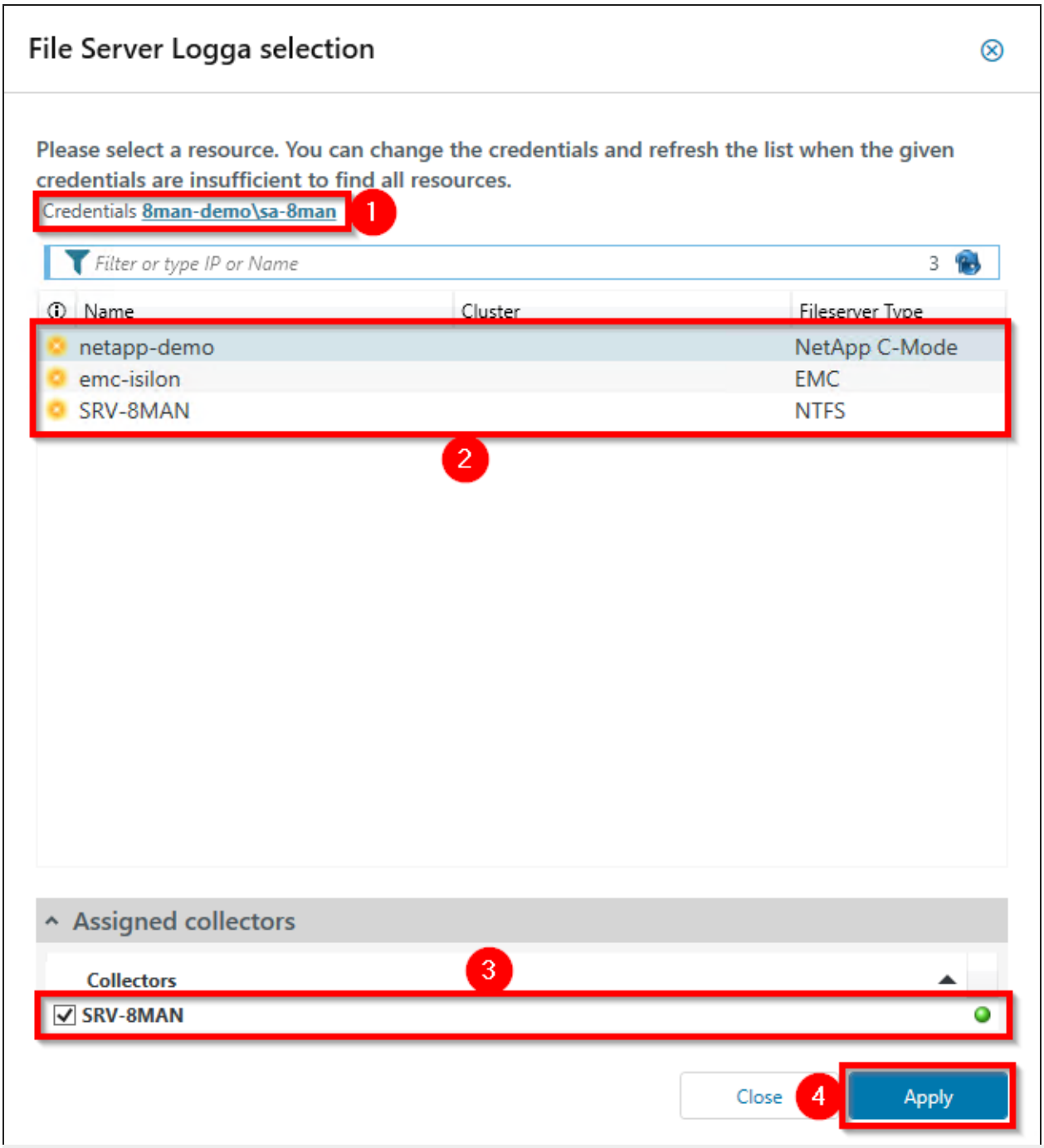
Add a FS Logga configuration



Log in to the ARM configuration application. Click Scans.



Click Logga - File Server.



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.

For Windows failover clusters, please refer to the following notes.

If you are missing NetApp file servers, please see Set NetApp file server findable.

If you are missing EMC file servers, please see Set EMC file servers findable.

3. Select a collector server.

For Windows file servers you can only select the collector that is installed on the file server.

For Windows failover clusters, please refer to the following notes.

For NetApp or EMC file servers, we strongly recommend 1:1 collector to file server mapping.

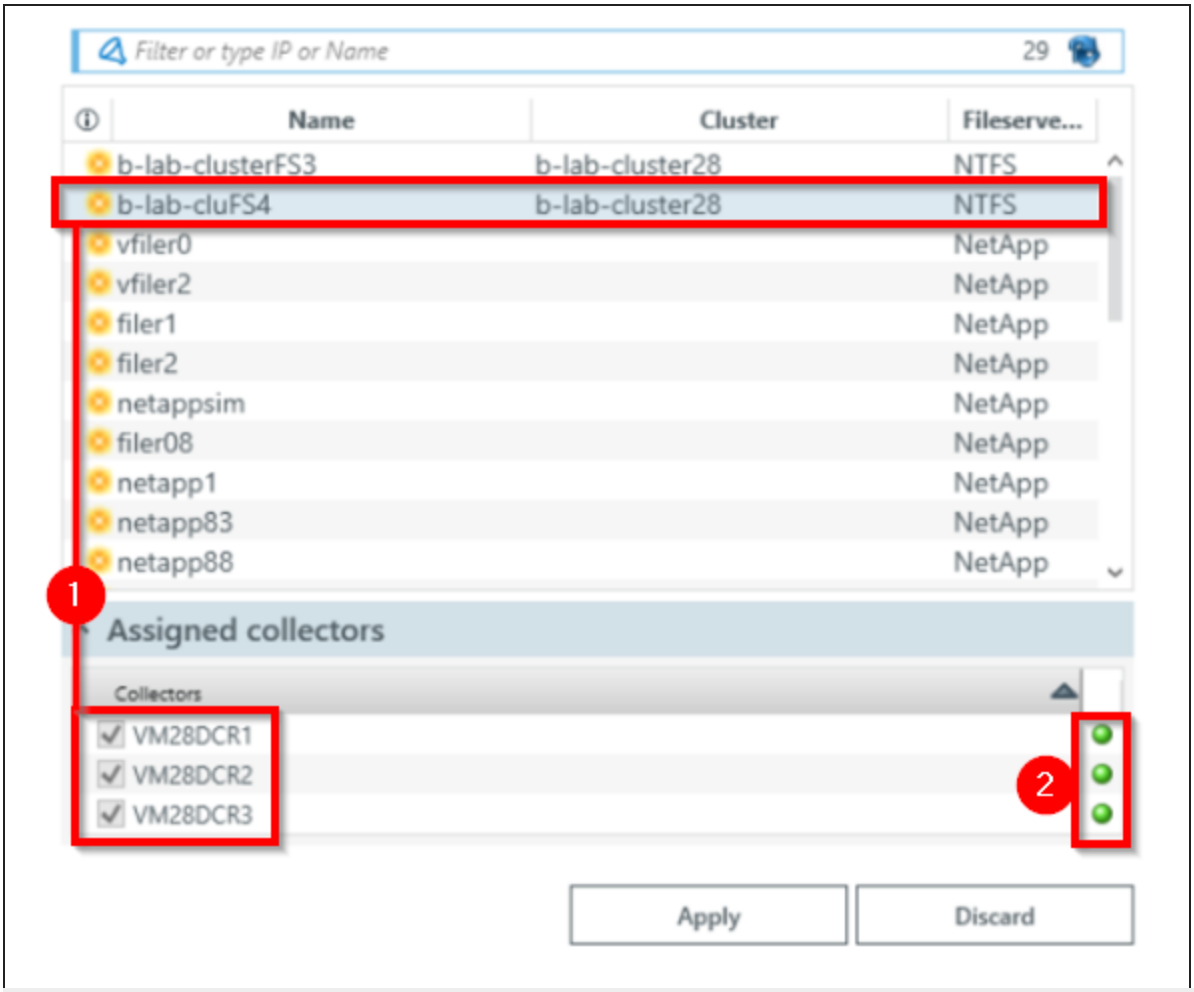
4. Click Apply.

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.

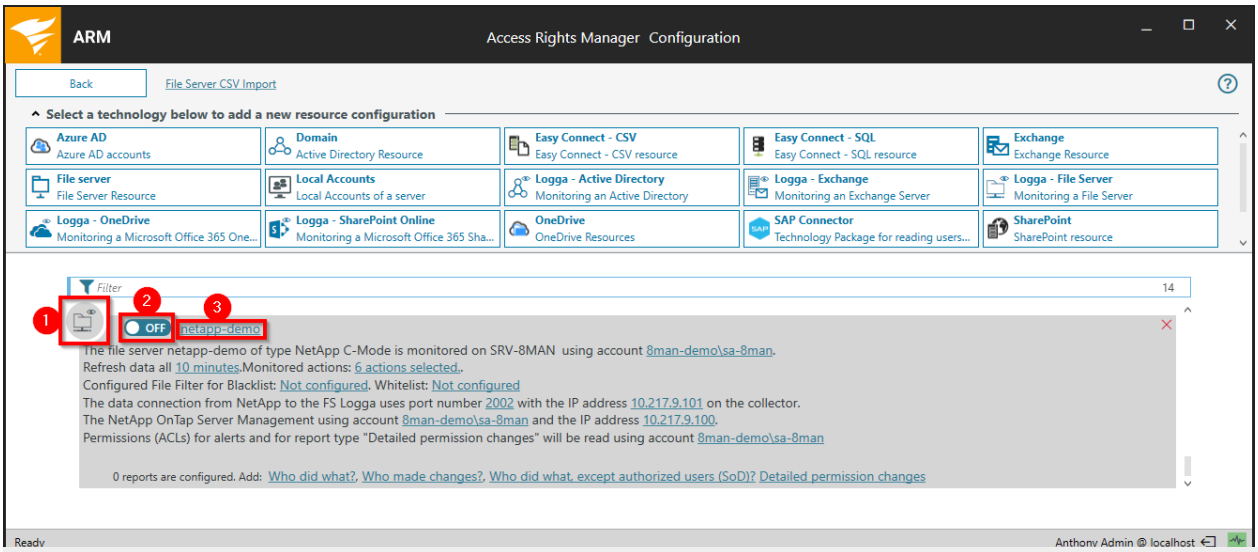
To successfully configure a FS Logga for a Windows failover cluster, the following requirements must be met:

- 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



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

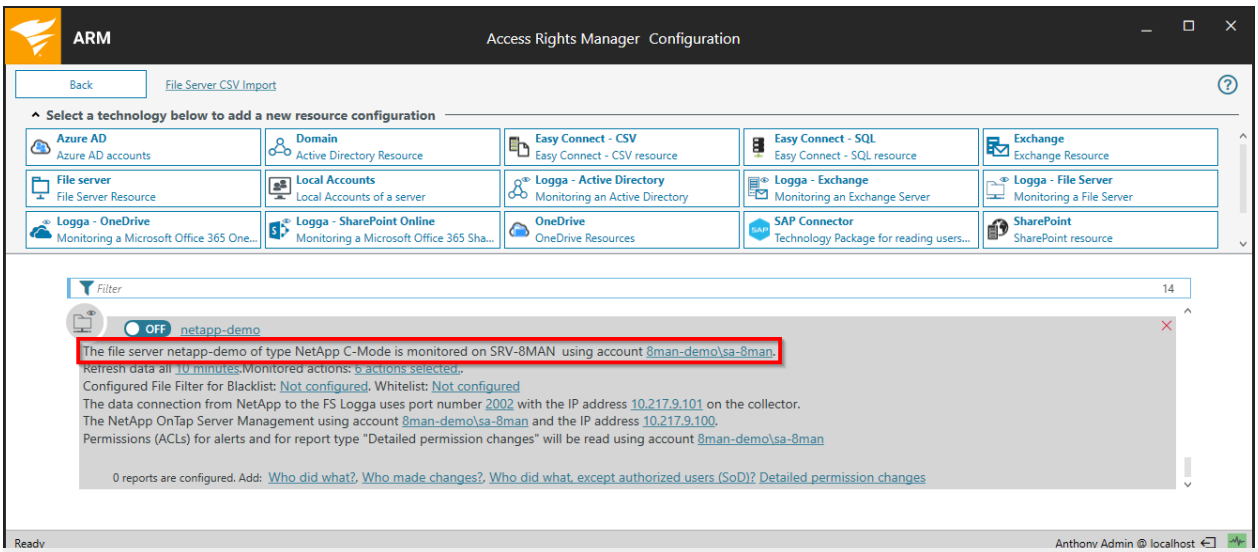


1. The folder icon with the eye indicates a FS Logga configuration.
2. Turn the FS Logga on or off. You must enter a comment to perform the action. The event and the comment is recorded in the ARM logbook.

Use the logbook to verify that the FS Logga has been turned on successfully.

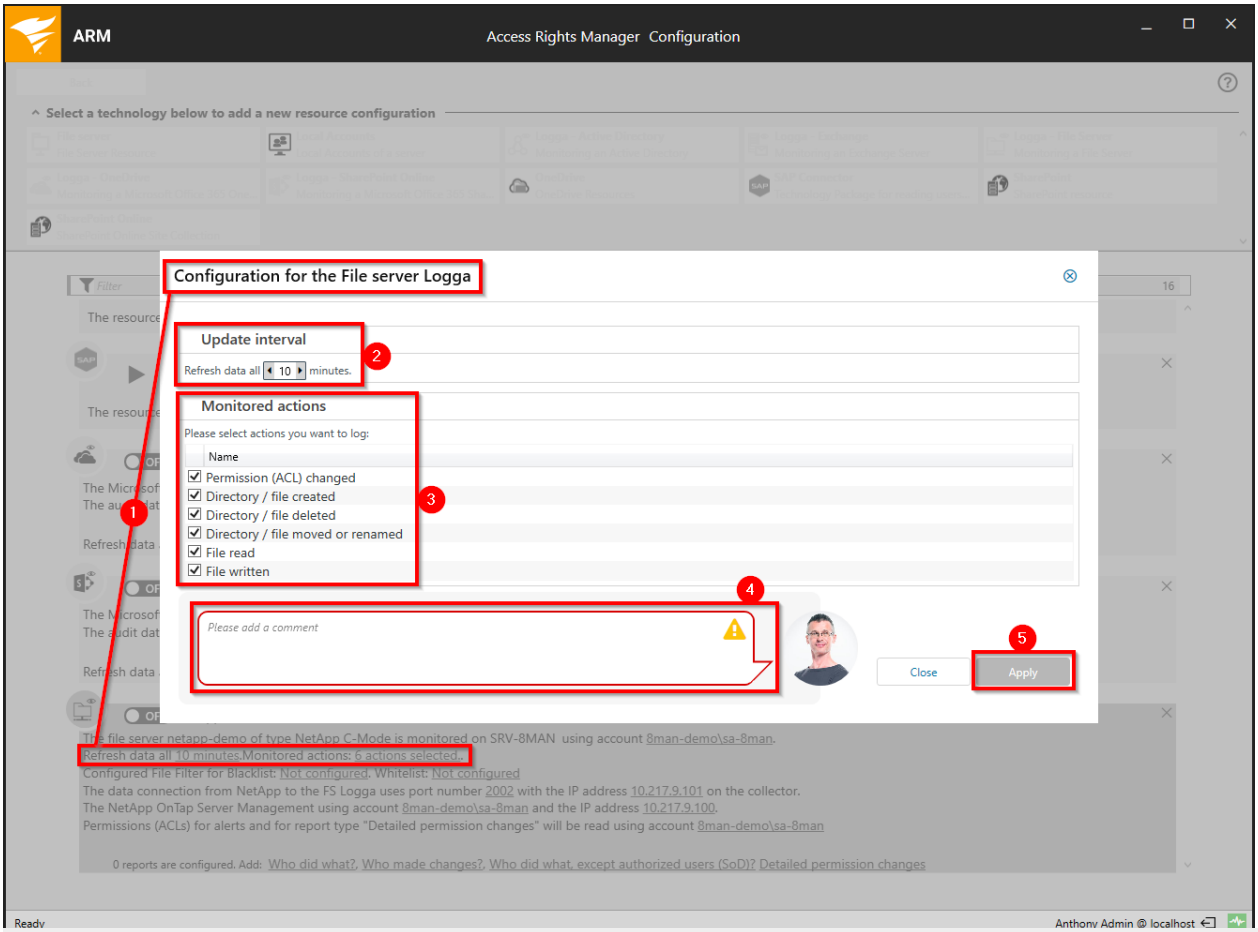
You cannot change credentials if the FS Logga is turned on.

3. You can change the name of the configuration. The name has no impact on the FS Logga function.



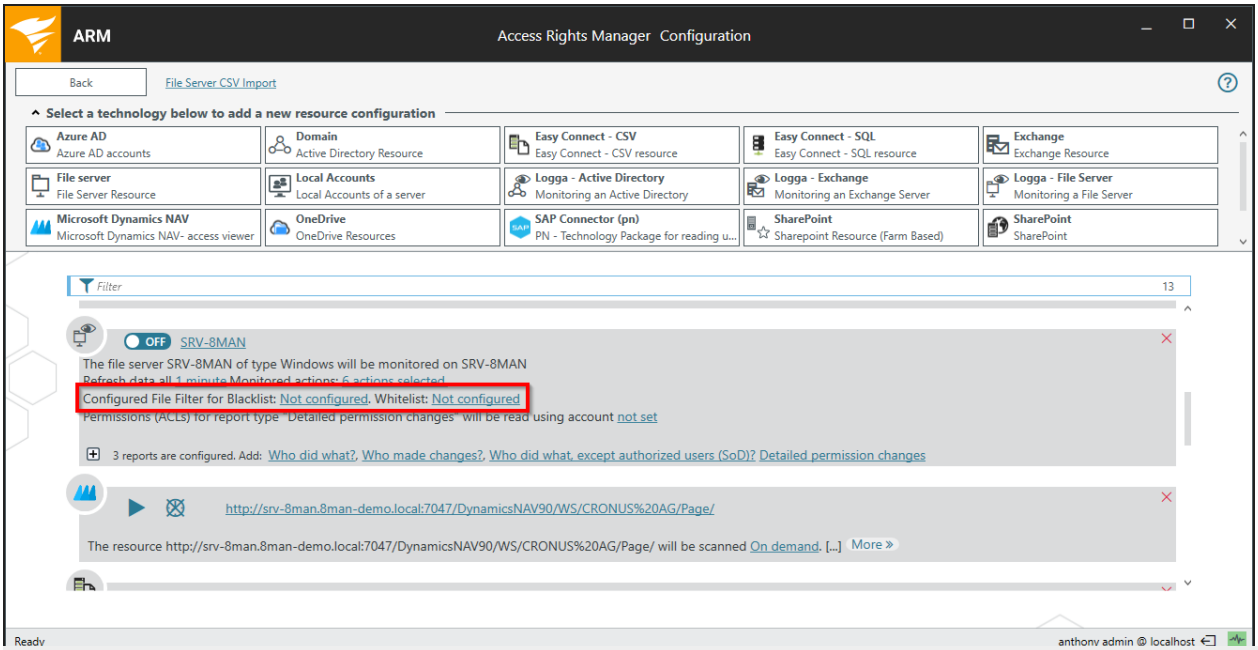
ARM shows you the file server name and type and the collector that is used. For NetApp and EMC you can change the account that is used for monitoring.

Monitored actions and data refresh interval

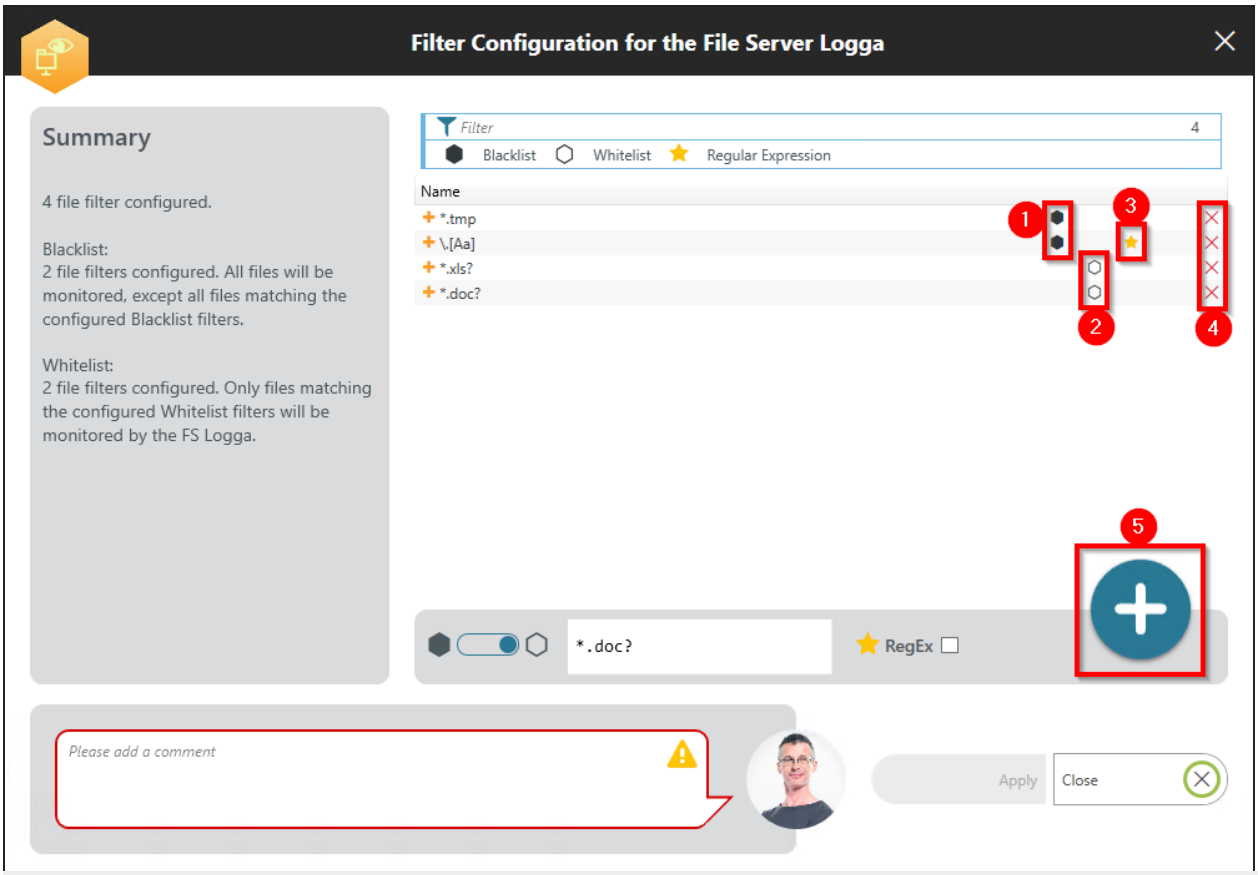


1. Click on one of the links to open up this dialog.
2. Specify the interval at which the Logga data is written from the collector to the ARM database. The default value is 10 minutes, minimum is 1 minute, maximum 60 minutes.
3. With monitored actions you can filter what type of events are recorded. 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



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.

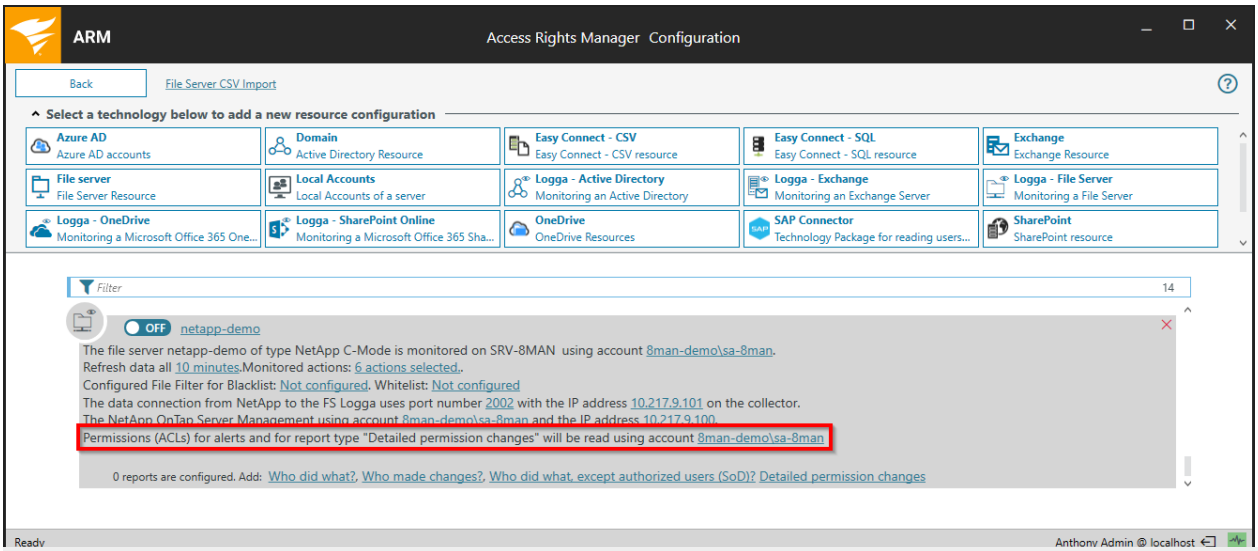
The filter configuration shown here is illogical and is for demonstration purposes only.

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.

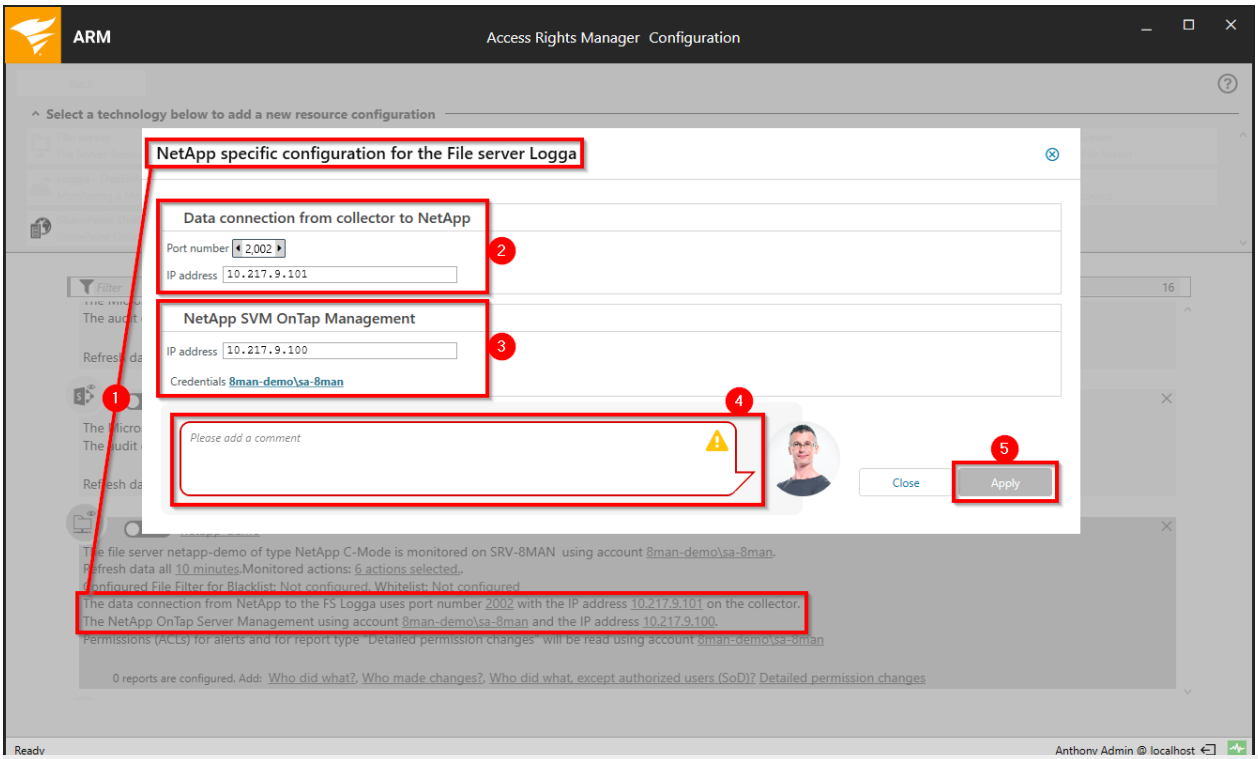
This feature is not available for Windows failover cluster resources.



Click on the link to enter the credentials of the account that is used for reading the ACLs.

NetApp Clustered Data ONTAP configuration

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.

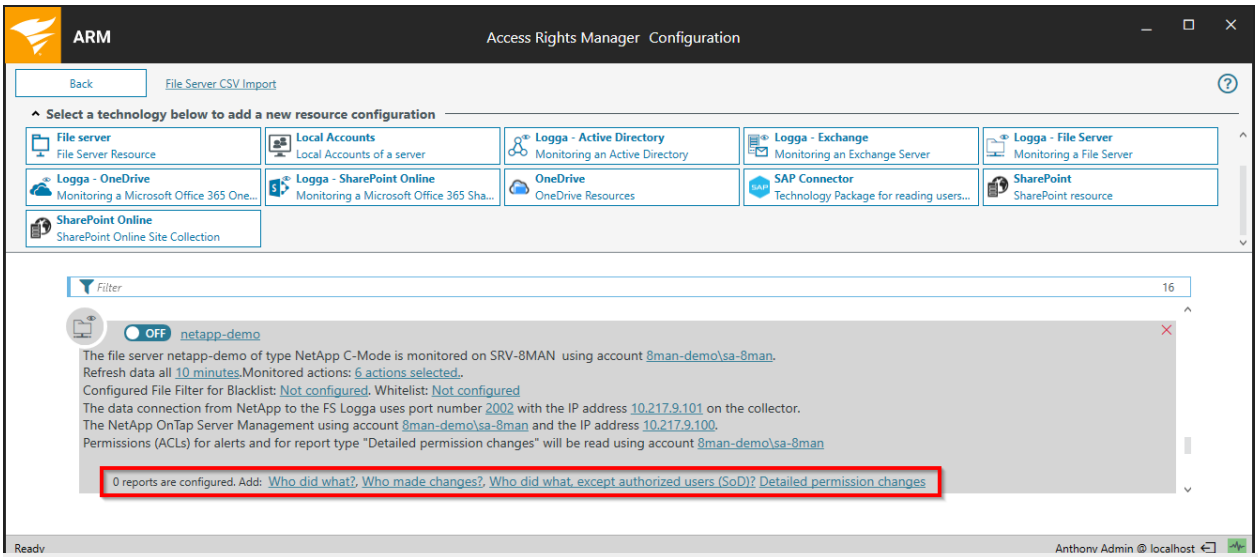
> The IP address and port is used to receive the events from the NetApp and therefore must be available.

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

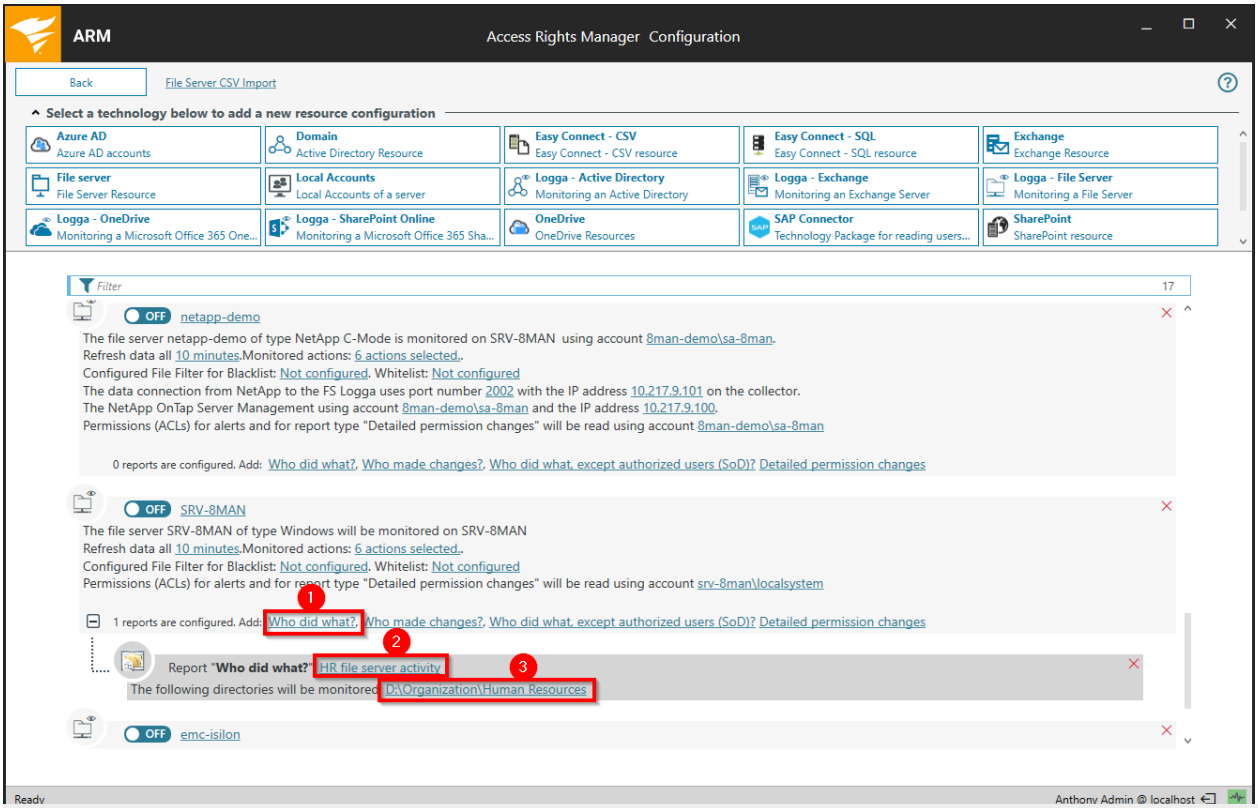
Events captured by the FS Logga are recorded in the ARM database. To view the information recorded, you must create a report.

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.



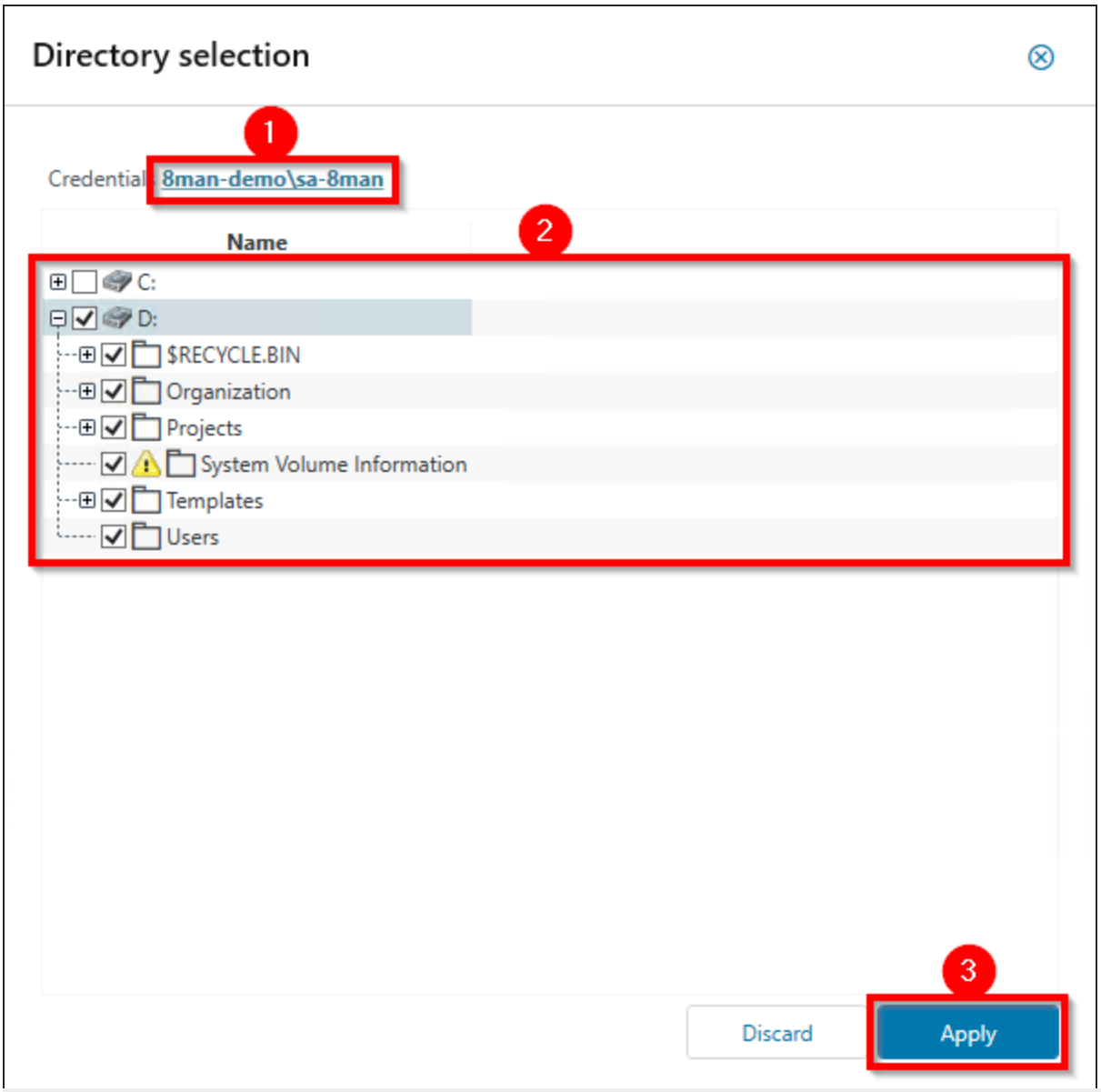
Click one of the links to create a report configuration.

Configure the "Who did what?" report



1. Click "Who did what?".
2. Name the FS Logga report configuration.

3. Select the directories to be monitored.



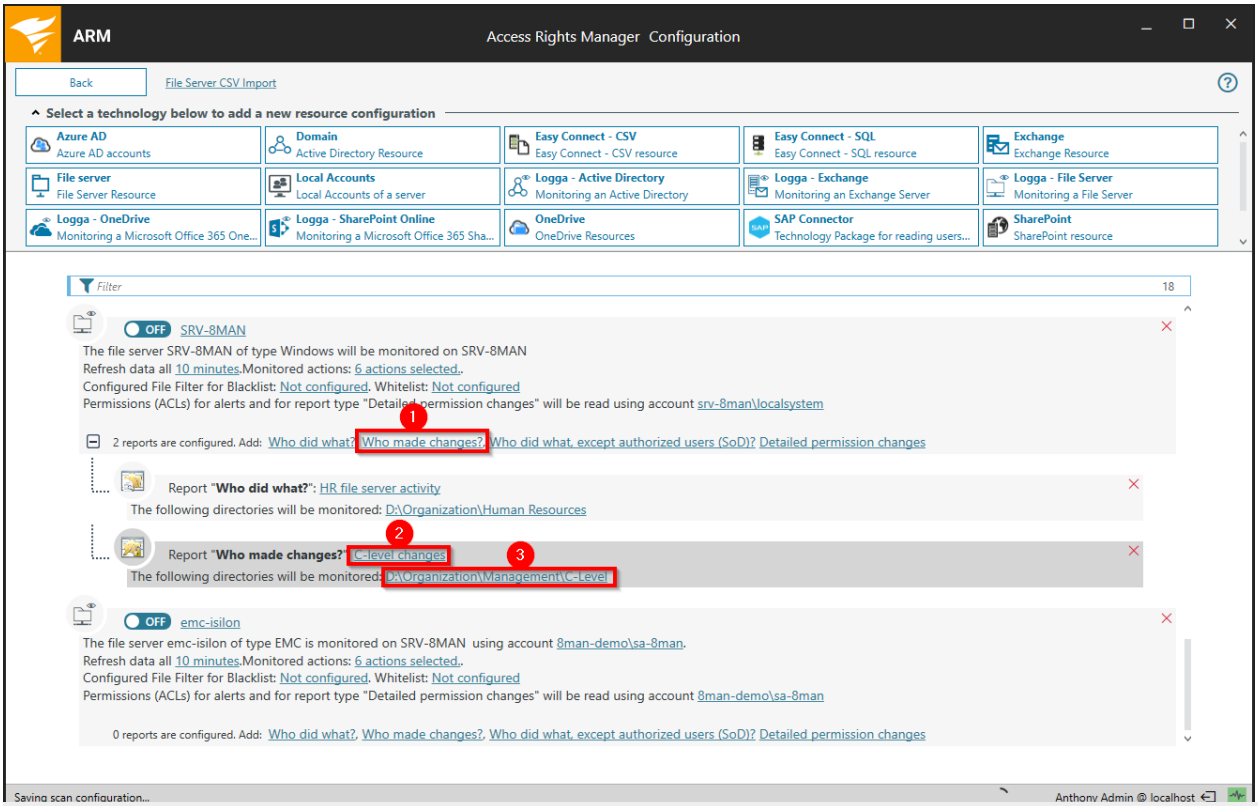
1. Use credentials of an account that is allowed to read file server paths. On NetApp the account has to be a member of the Power User group. See NetApp clustered or NetApp 7-mode.
2. Select the directories to be monitored. Subdirectories and files are included.
3. Click Apply.

For the selected directories, subdirectories and the files in there are the following operations recorded:

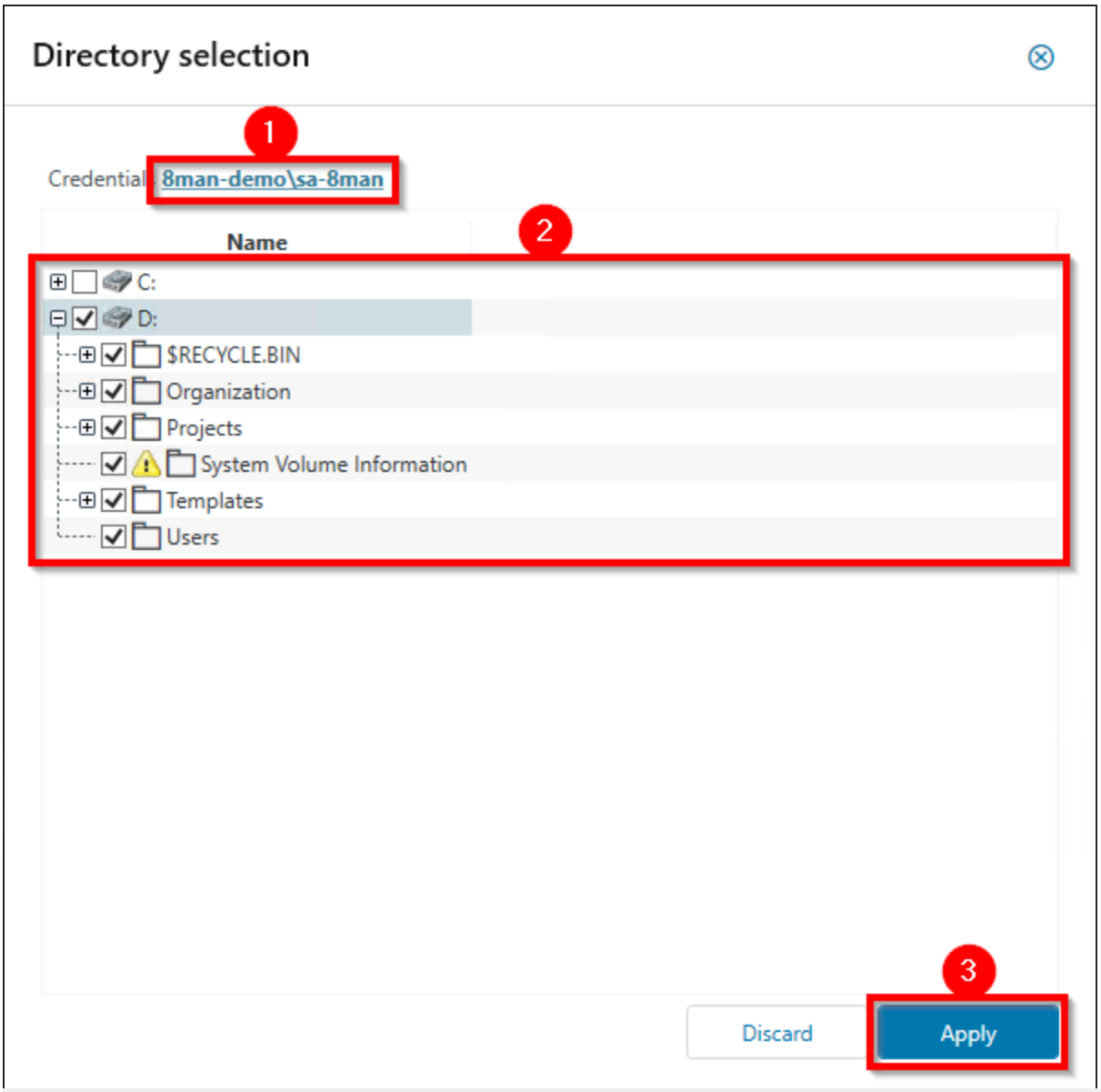
- File read
- File written
- Directory or file created

- 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



1. Click "Who made changes?".
2. Name the FS Logga report configuration.
3. Select the directories to be monitored.

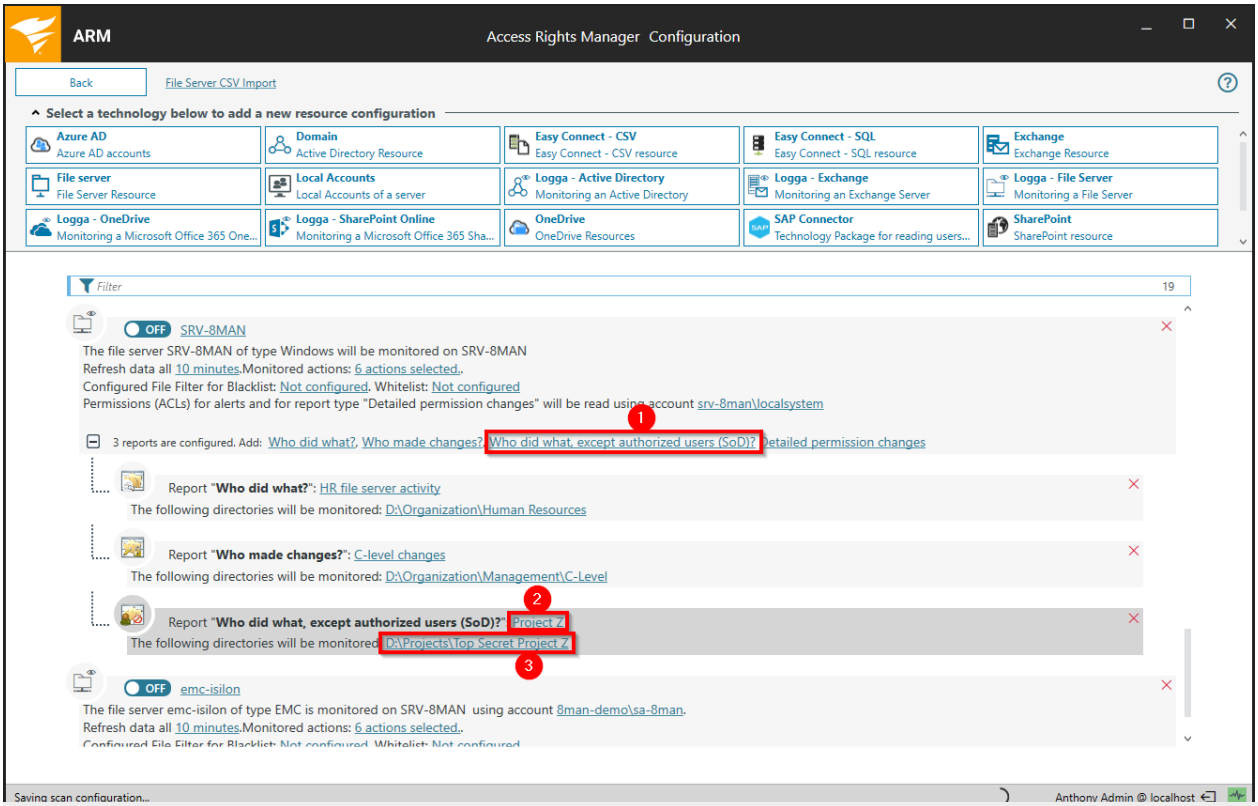


1. Use credentials of an account that is allowed to read file server paths. On NetApp the account has to be a member of the Power User group. See NetApp clustered or NetApp 7-mode.
2. Select the directories to be monitored. Subdirectories and files are included.
3. Click Apply.

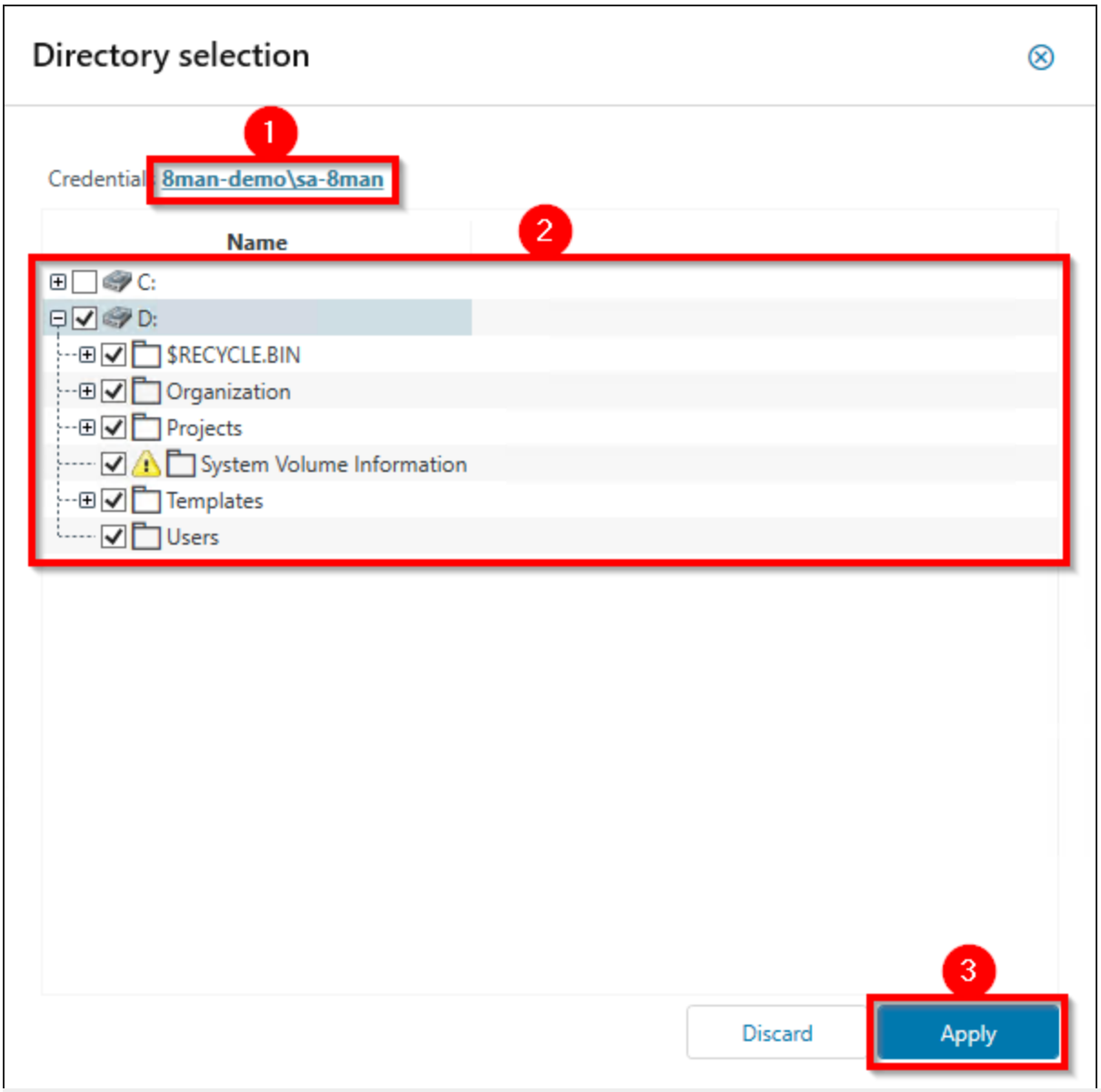
For the selected directories, subdirectories and the files in there are the following operations recorded:

- File written
- ACL changed

Configure the "Who did what, except authorized users (SoD)?" report



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.

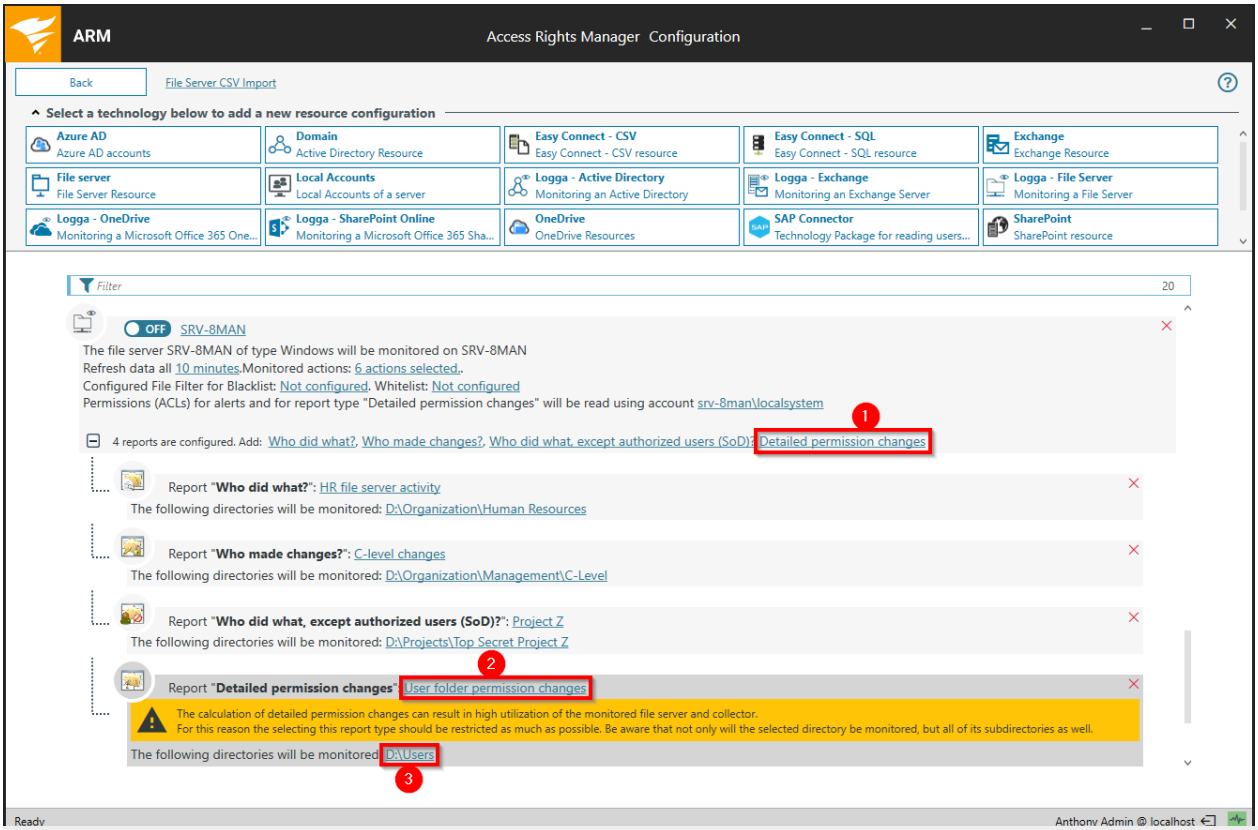
- File read
- File written
- Directory or file created
- Directory or file deleted

- 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)

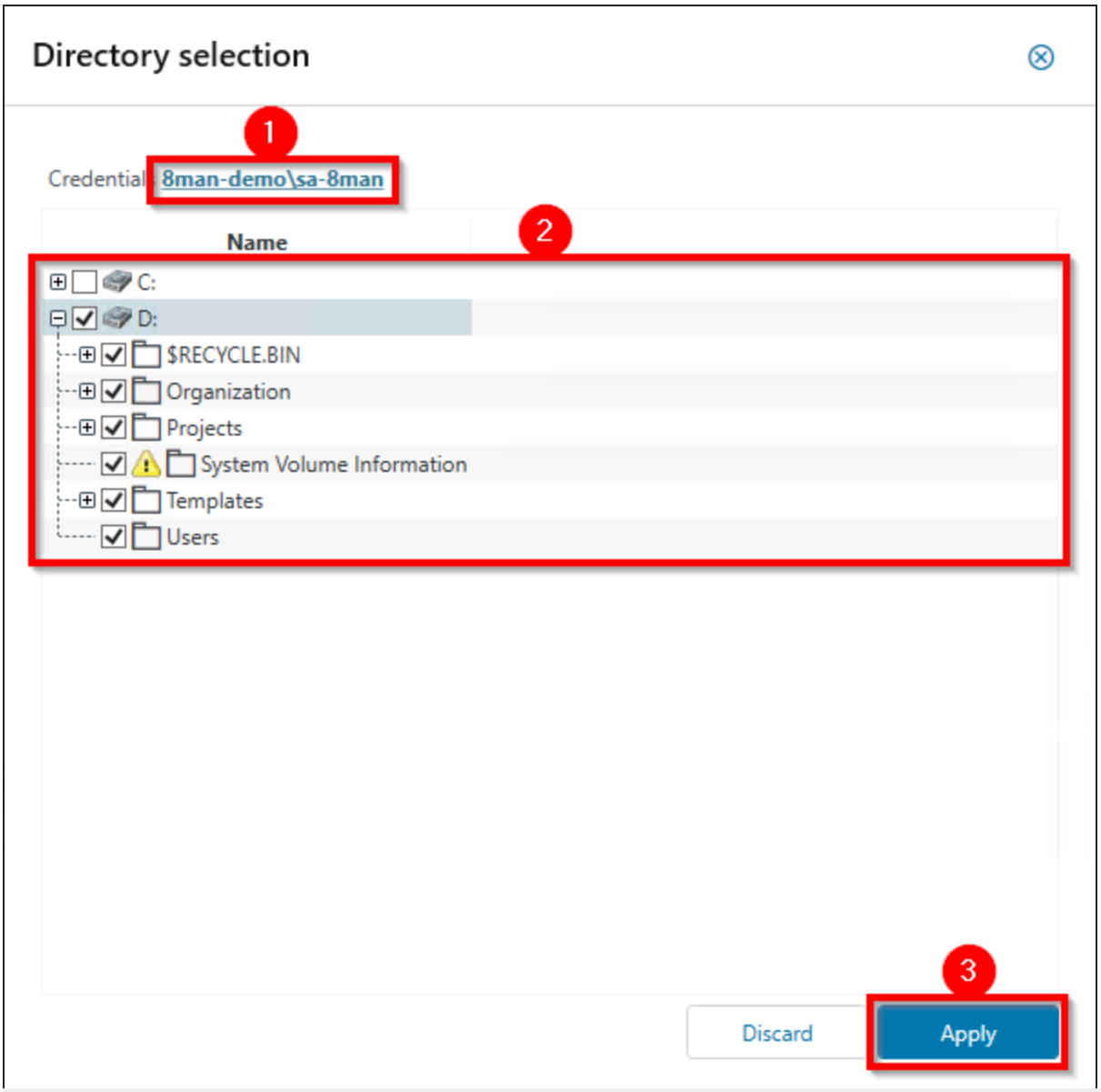
Configure the "Detailed permission changes" report

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.



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

maximium 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.

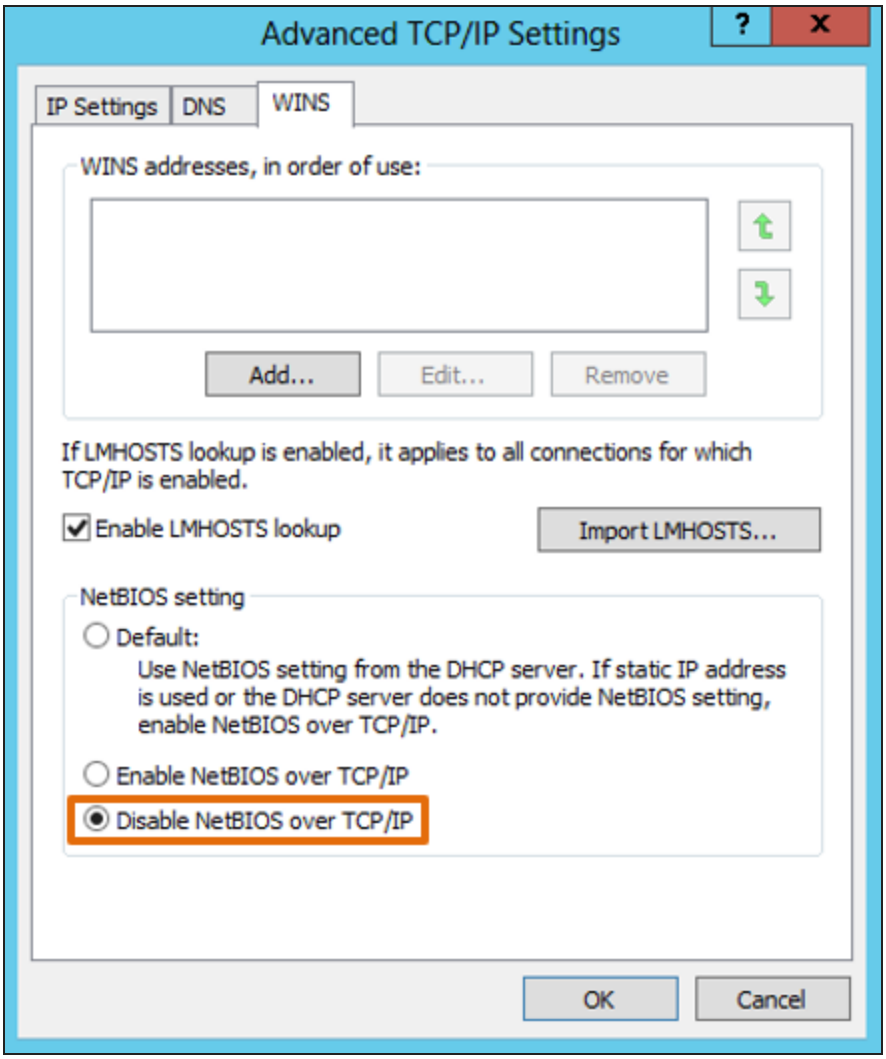
After saving the pnTracer.config.xml file you have to stop and then start the FS Logga so that the changes can take effect.

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

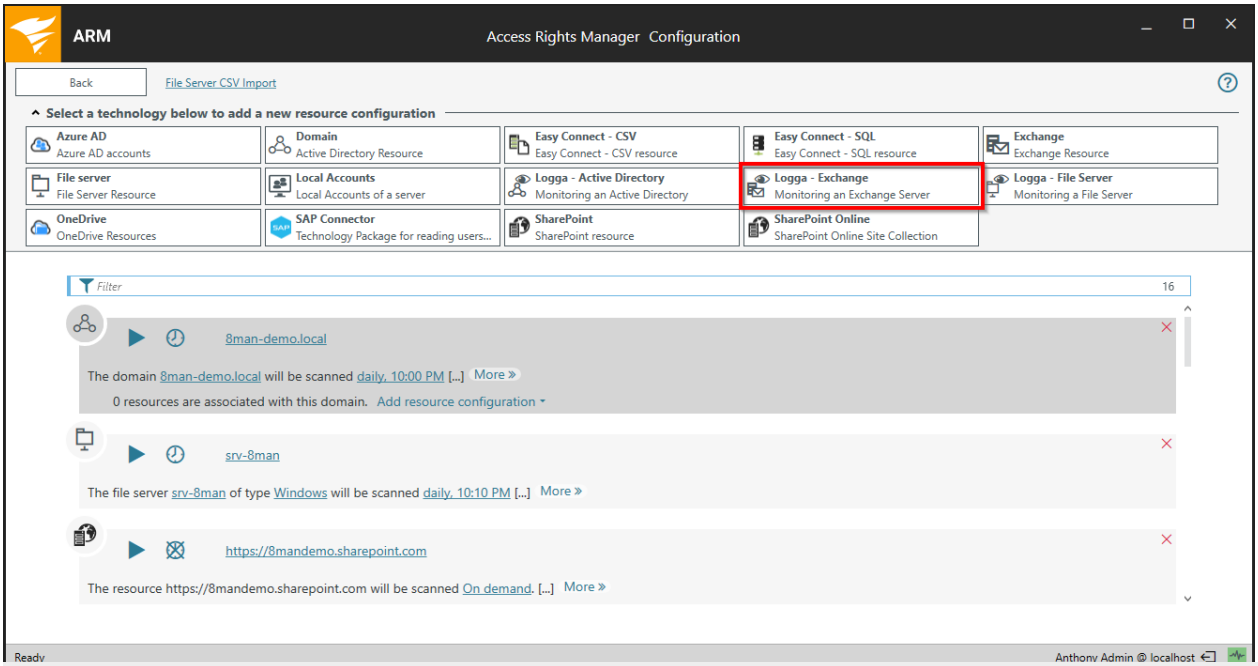
Empty report for Windows failover cluster resource

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.

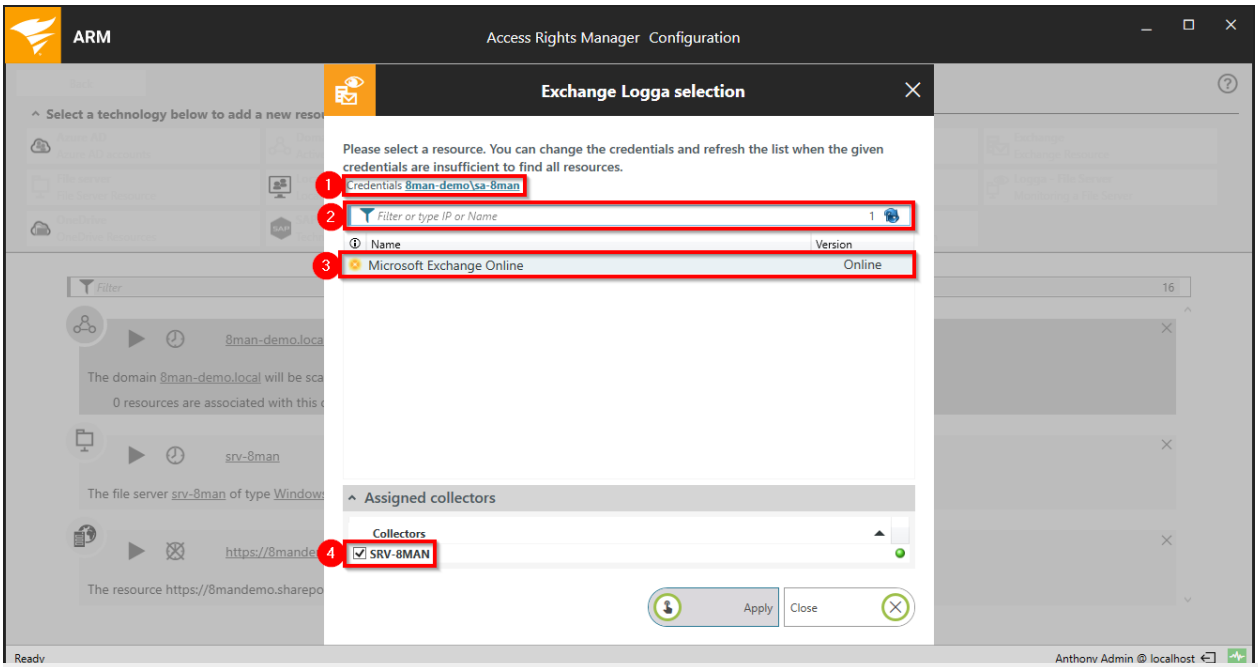
To solve this problem, turn the logga off and on again after 10 seconds.

Configure Exchange Logga

Add an Exchange Logga configuration



Select "Logga - Exchange".

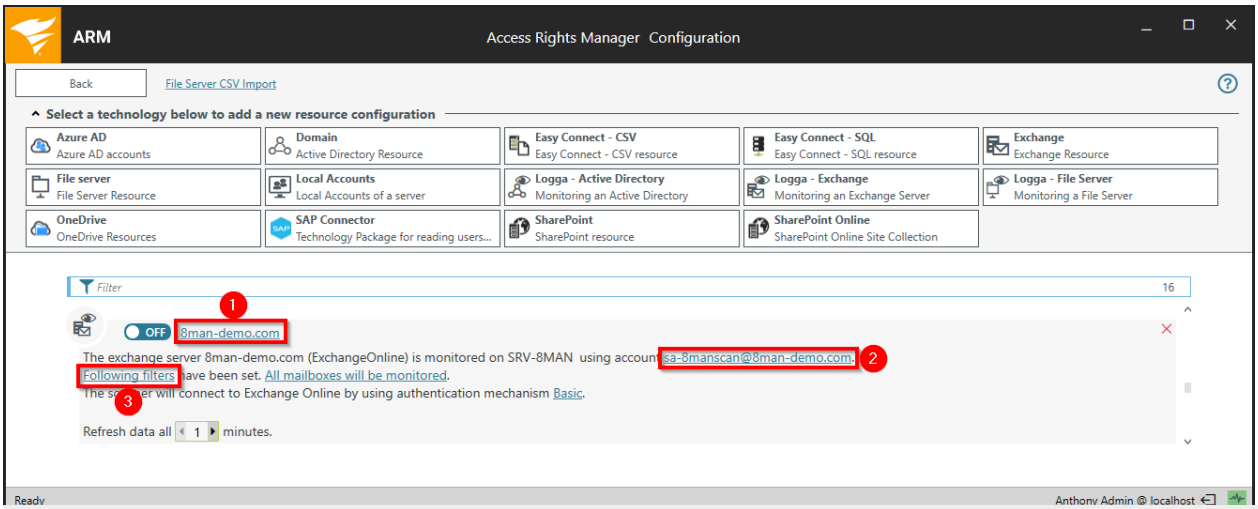


1. Specify valid credentials for the Exchange to be monitored. See also: required permissions.
2. Optional: Use the filter to find the desired server.
3. Select a server.

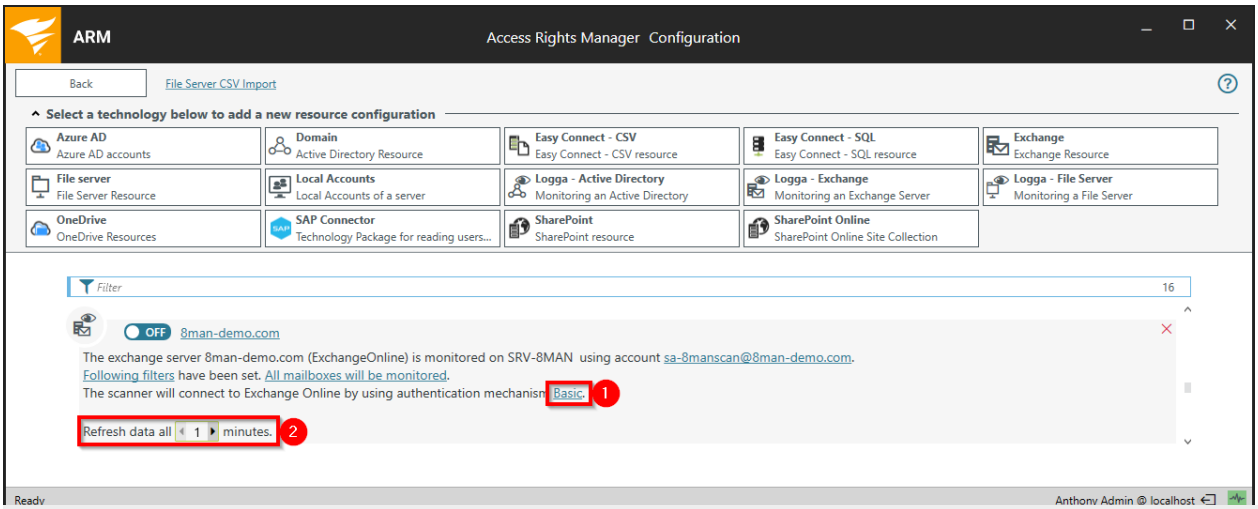
4. Choose a collector server. You can only select one collector per Exchange.

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



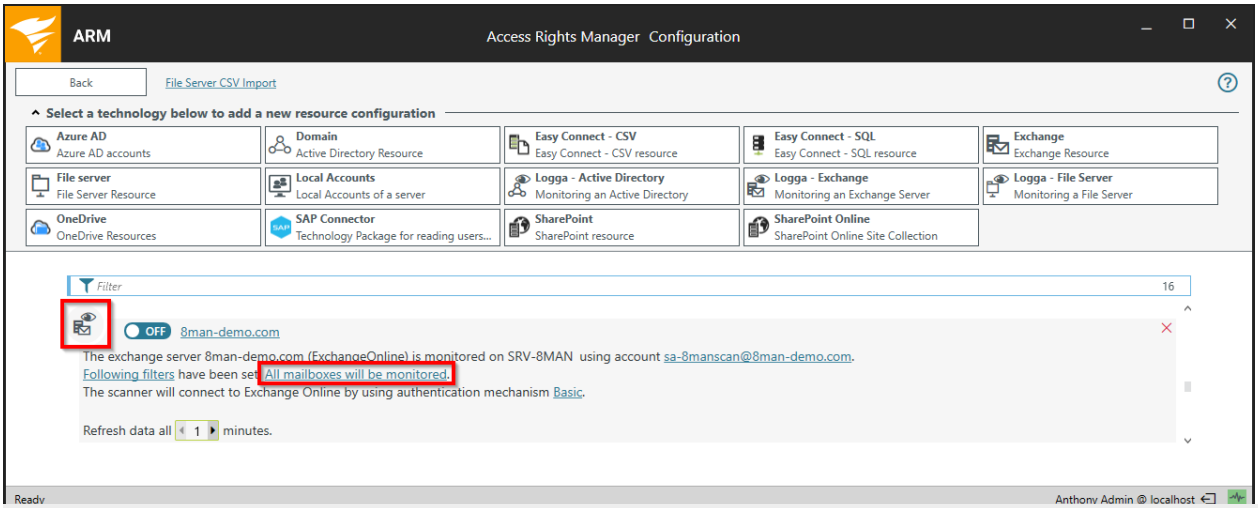
1. Rename the configuration.
2. Change the credentials used by the Exchange Logga to read the events from the Exchange Server. See also: required permissions.
3. Optional: Put filters.



1. Choose the authentication method that must match the PowerShell website configuration.

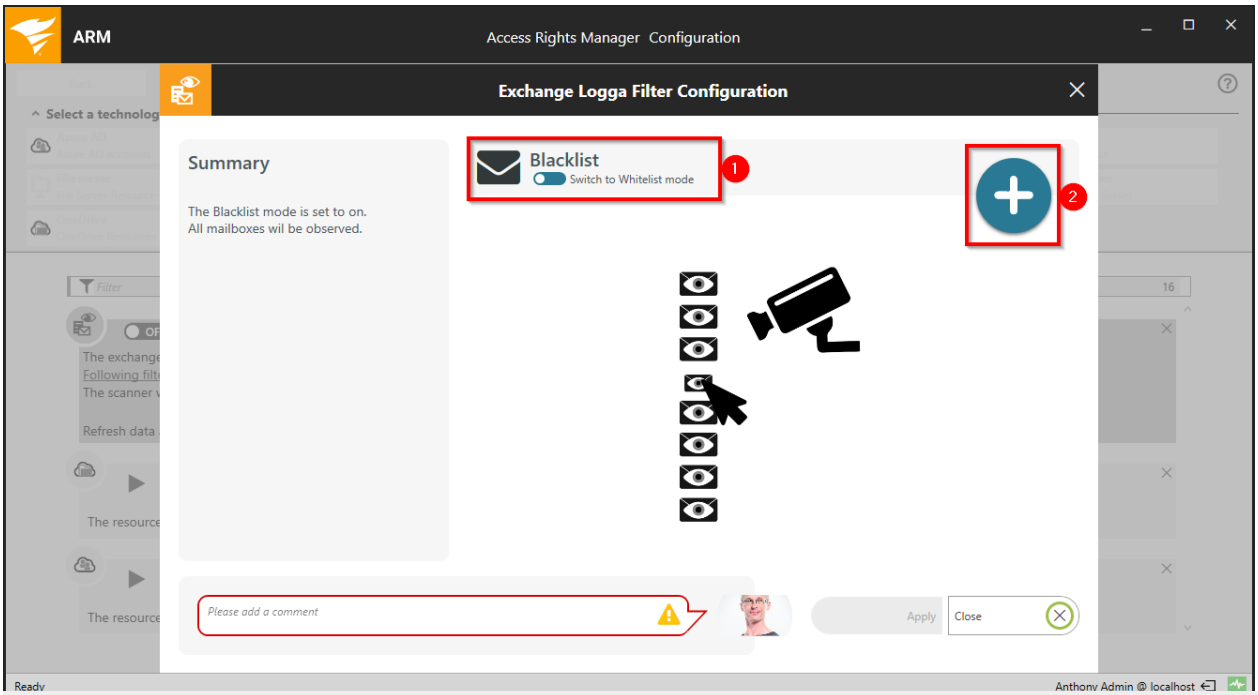
2. Set the interval for the data refresh. The events are collected by the collector and passed to the ARM server in the defined interval. Default value (recommended): 10 minutes.

Select the mailboxes to be monitored

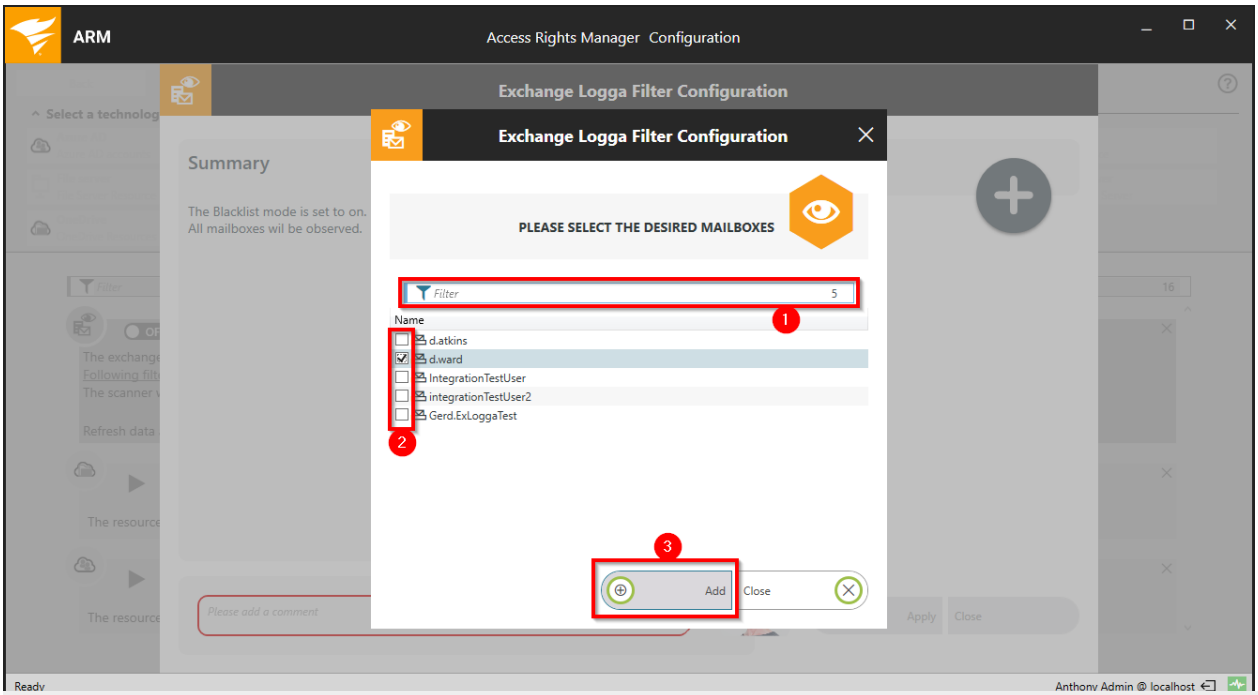


1. The symbol indicates an Exchange Logga configuration.
2. Click on the link.

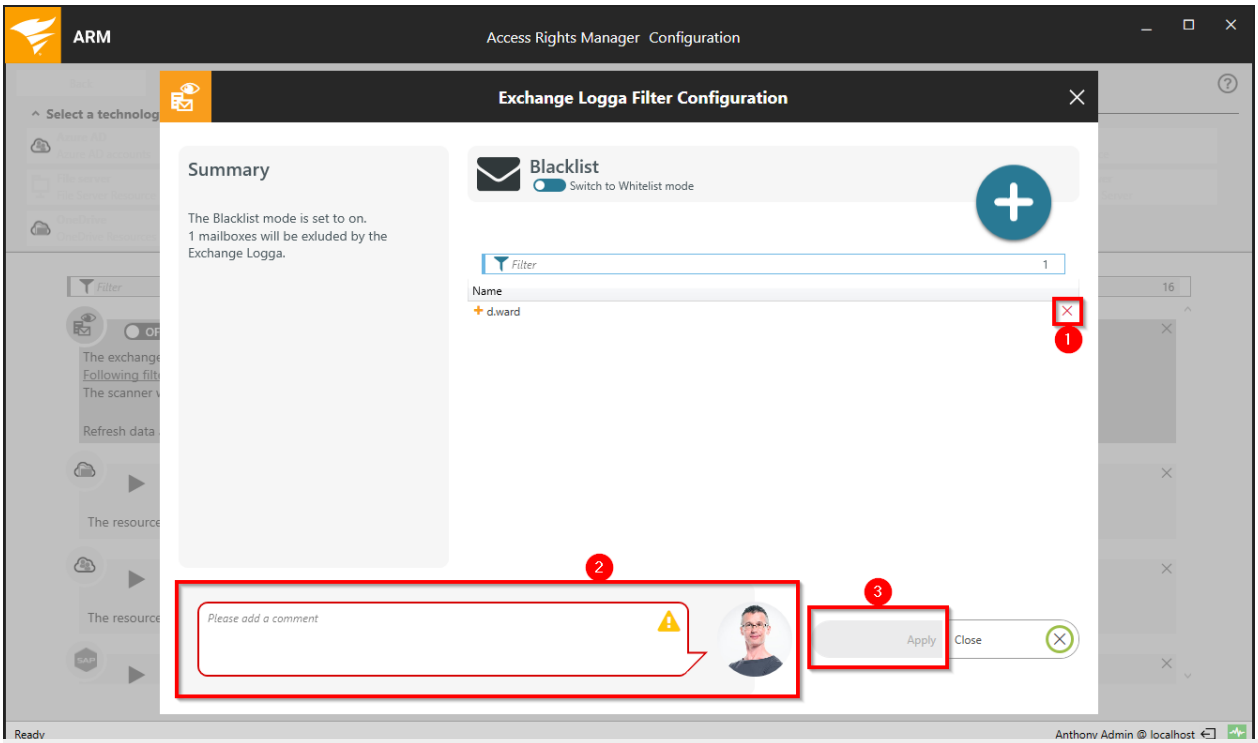
By default, all mailboxes are monitored.



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).

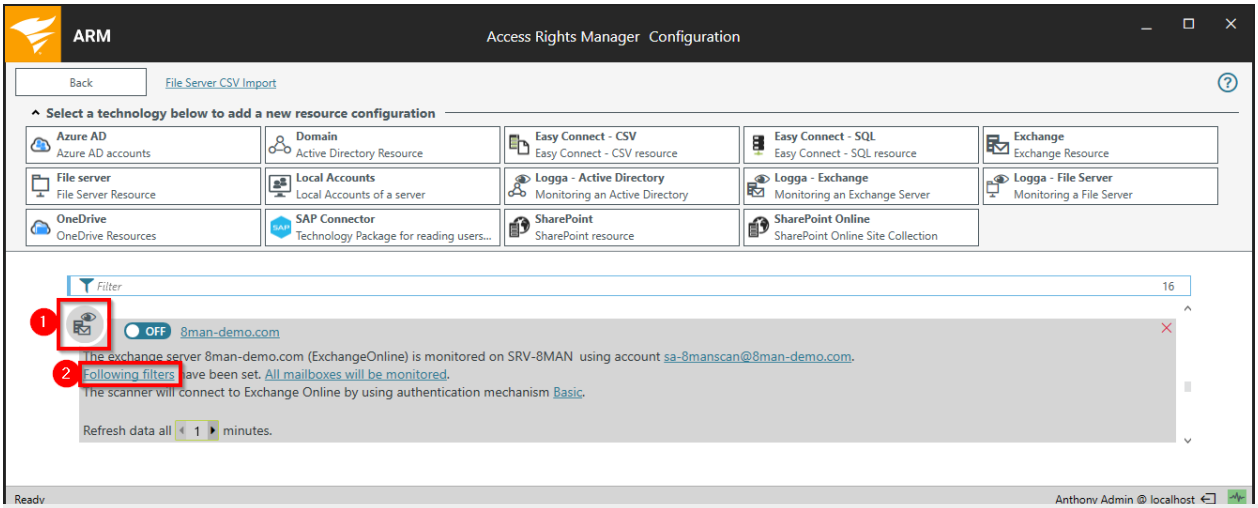
The filter criteria work additively. An event is rejected if criterion 1 or criterion 2 or criterion 3 applies, or several criteria simultaneously.

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.

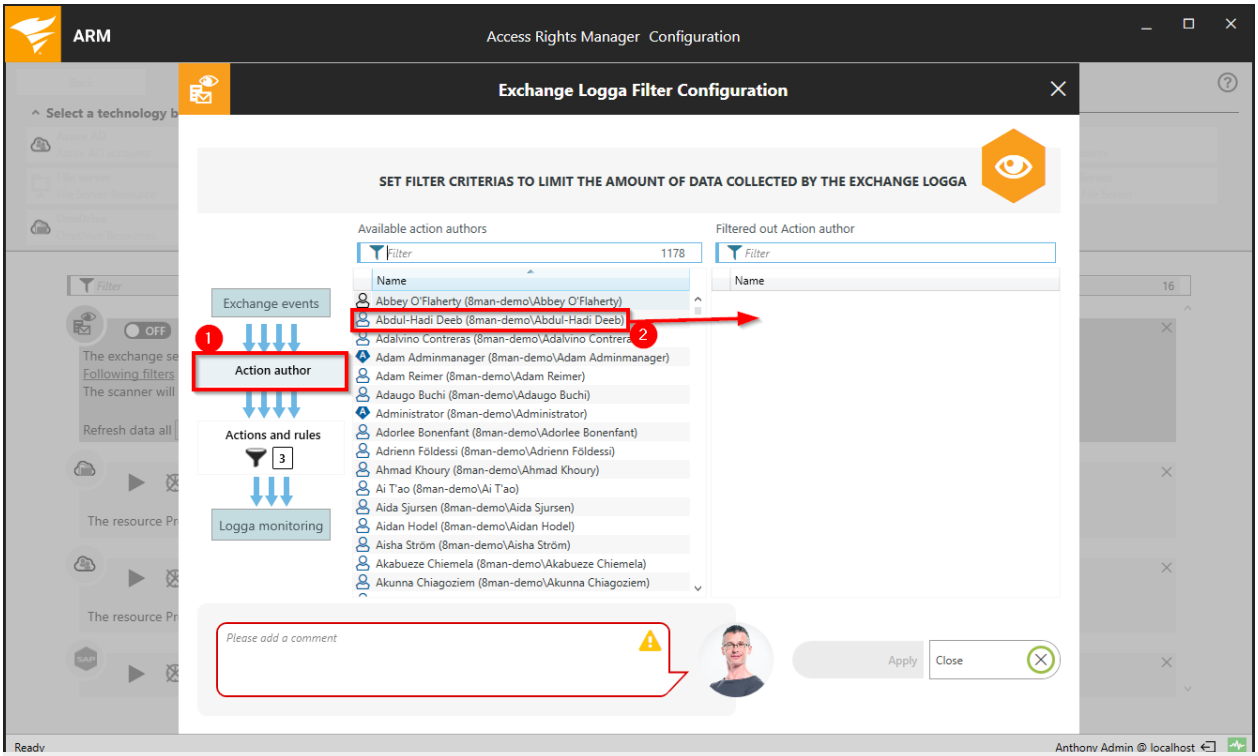
Example:

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.

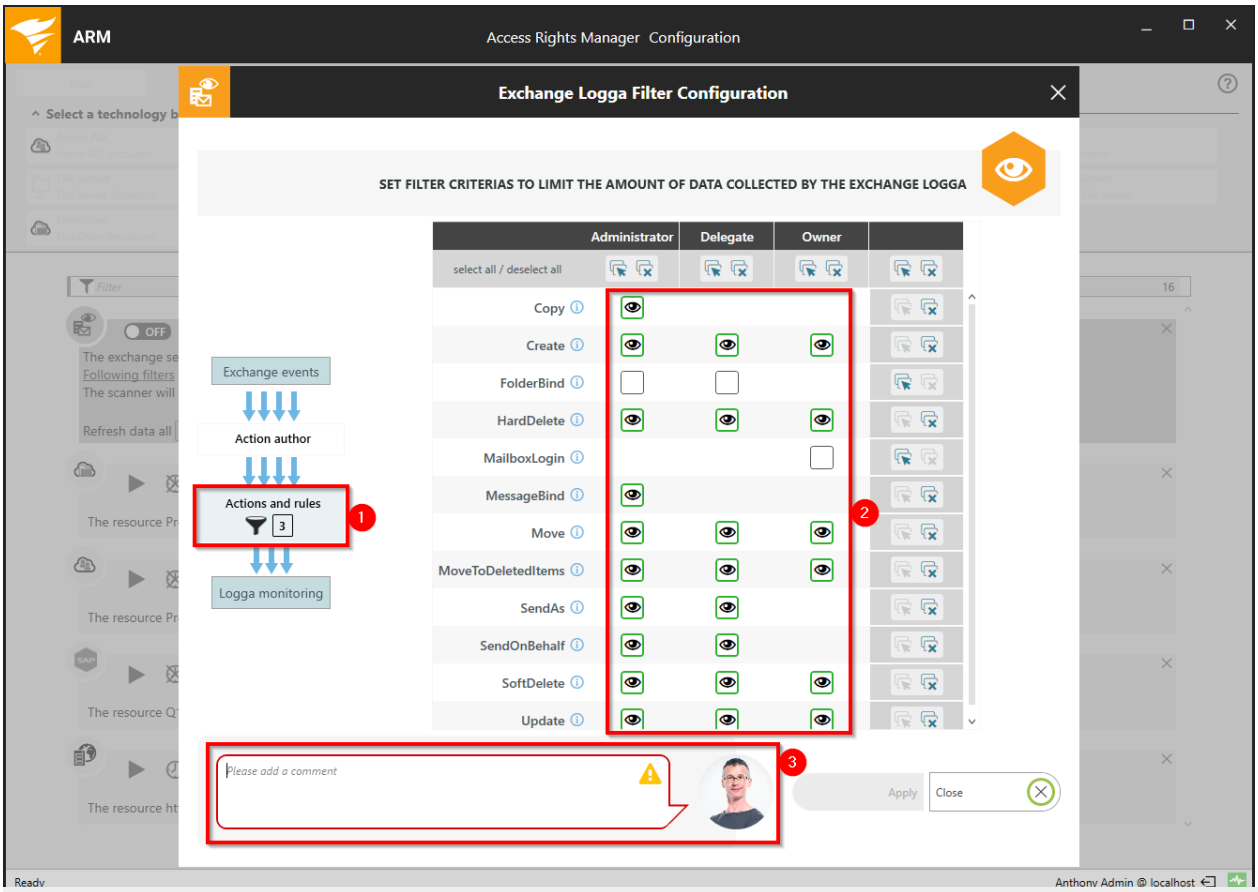
Configure the event filters for an Exchange Logga



1. The symbol indicates an Exchange Logga configuration.
2. Click on the link.



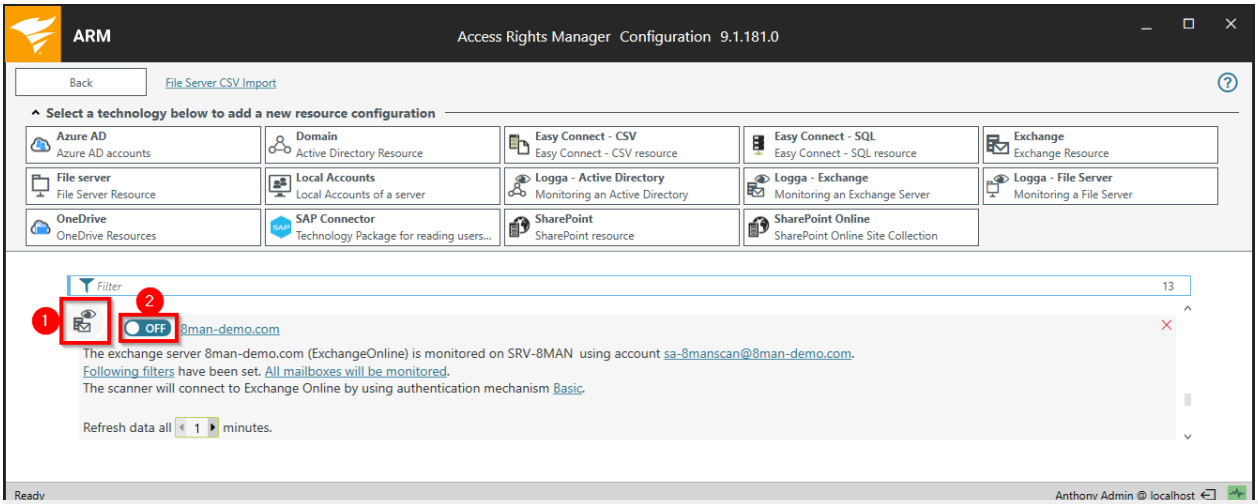
1. Filter events from users.
2. Select one or more users and drag them to the right column. Events triggered by these users are not recorded (blacklist).



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 (© 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



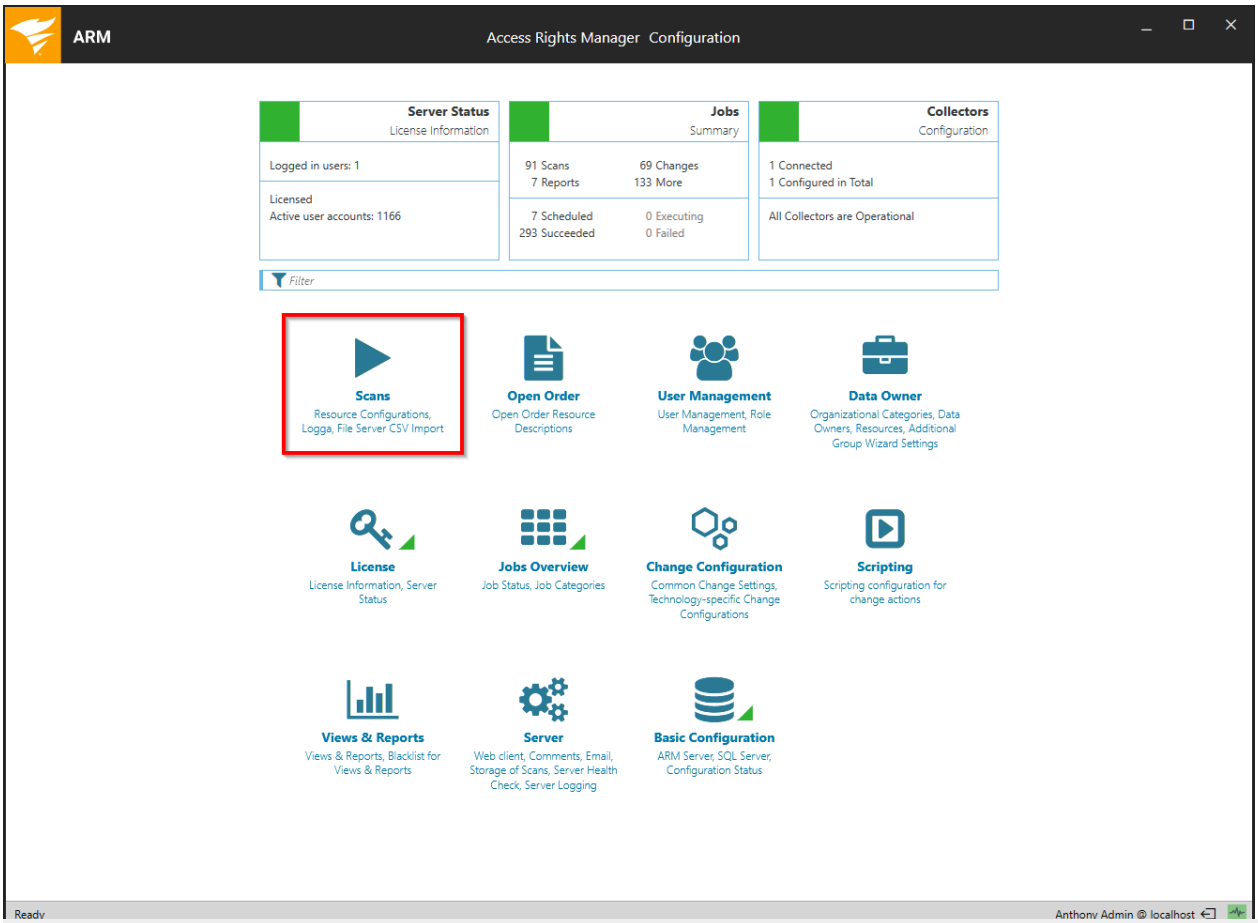
1. The symbol indicates an Exchange Logga configuration.
2. In the desired Exchange Logga configuration, click the switch to enable or disable the Exchange Logga.

You must enter a comment to enable or disable the Exchange Logga.

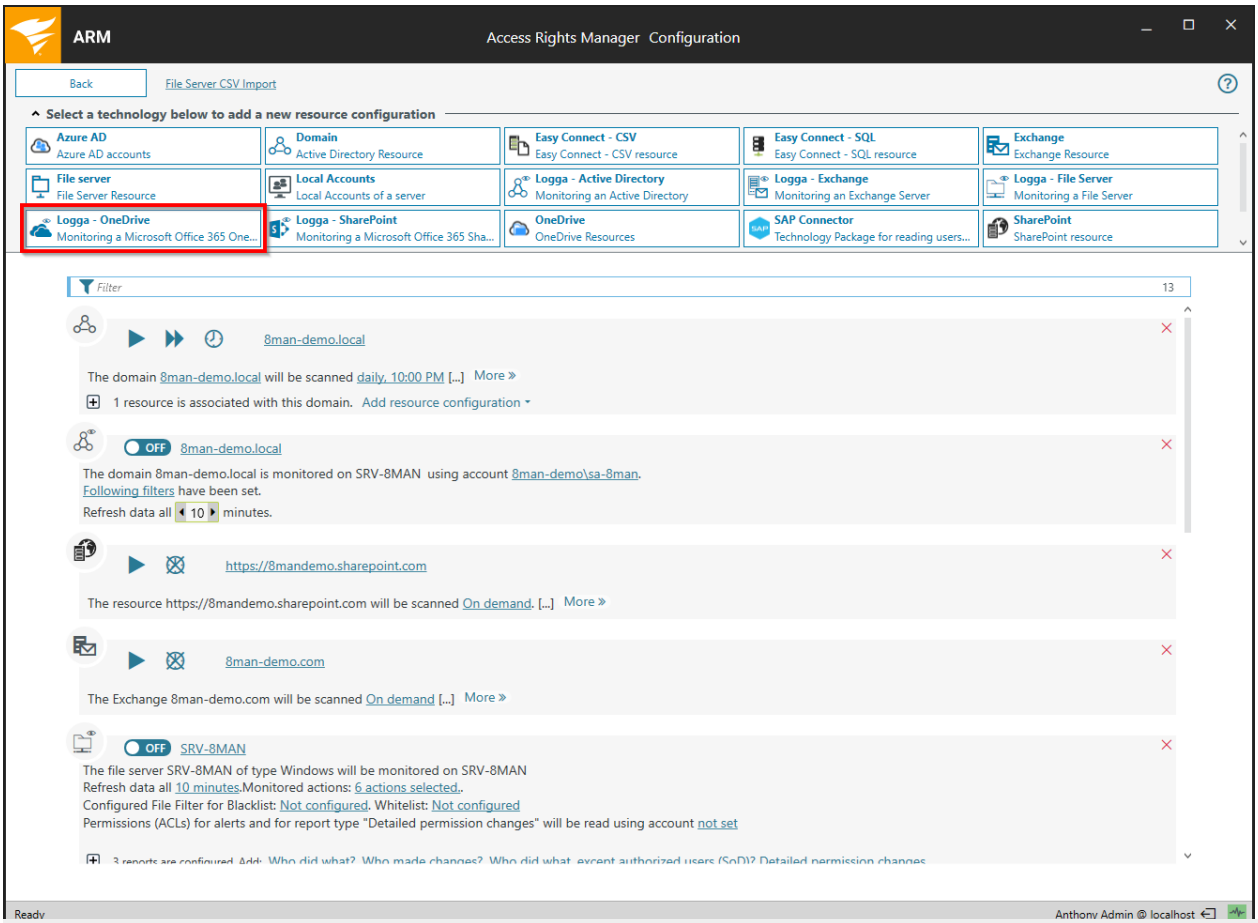
AD Logga events are stored by default for 30 days. See Configure storage of scans settings.

Configure OneDrive Logga

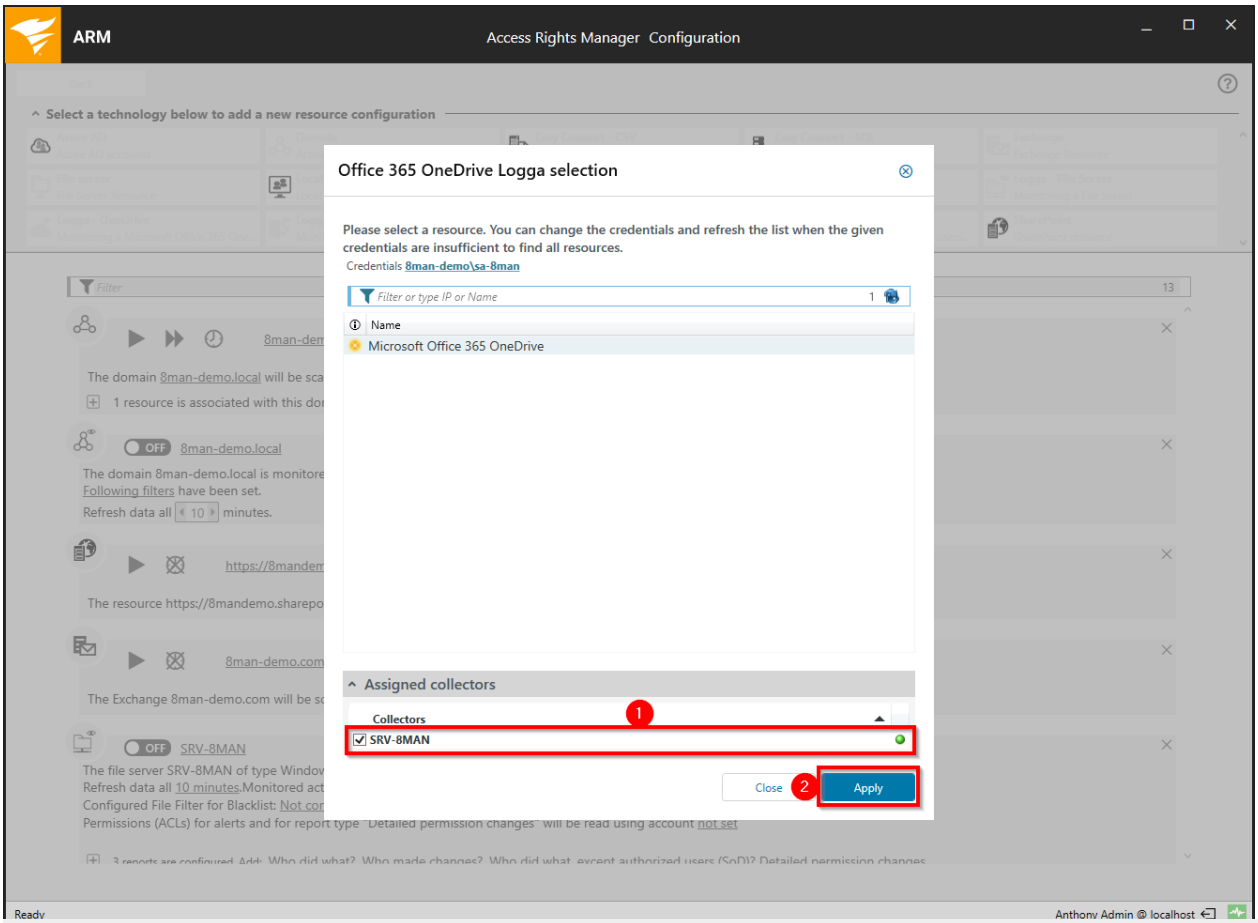
To enable the OneDrive Logga, you must have completed the preparation for Office 365 integration in the Azure Portal.



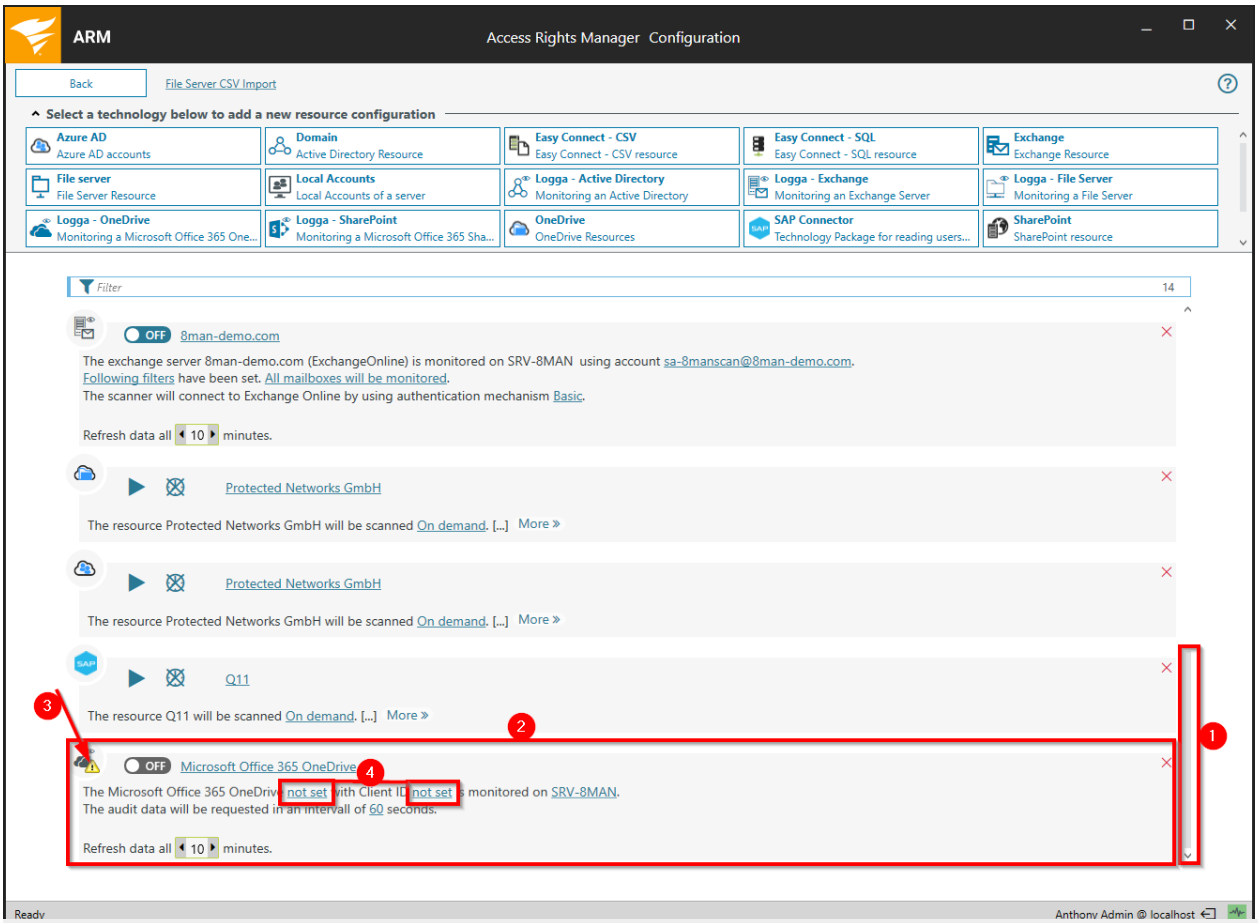
Start the ARM configuration application and click "Scans".



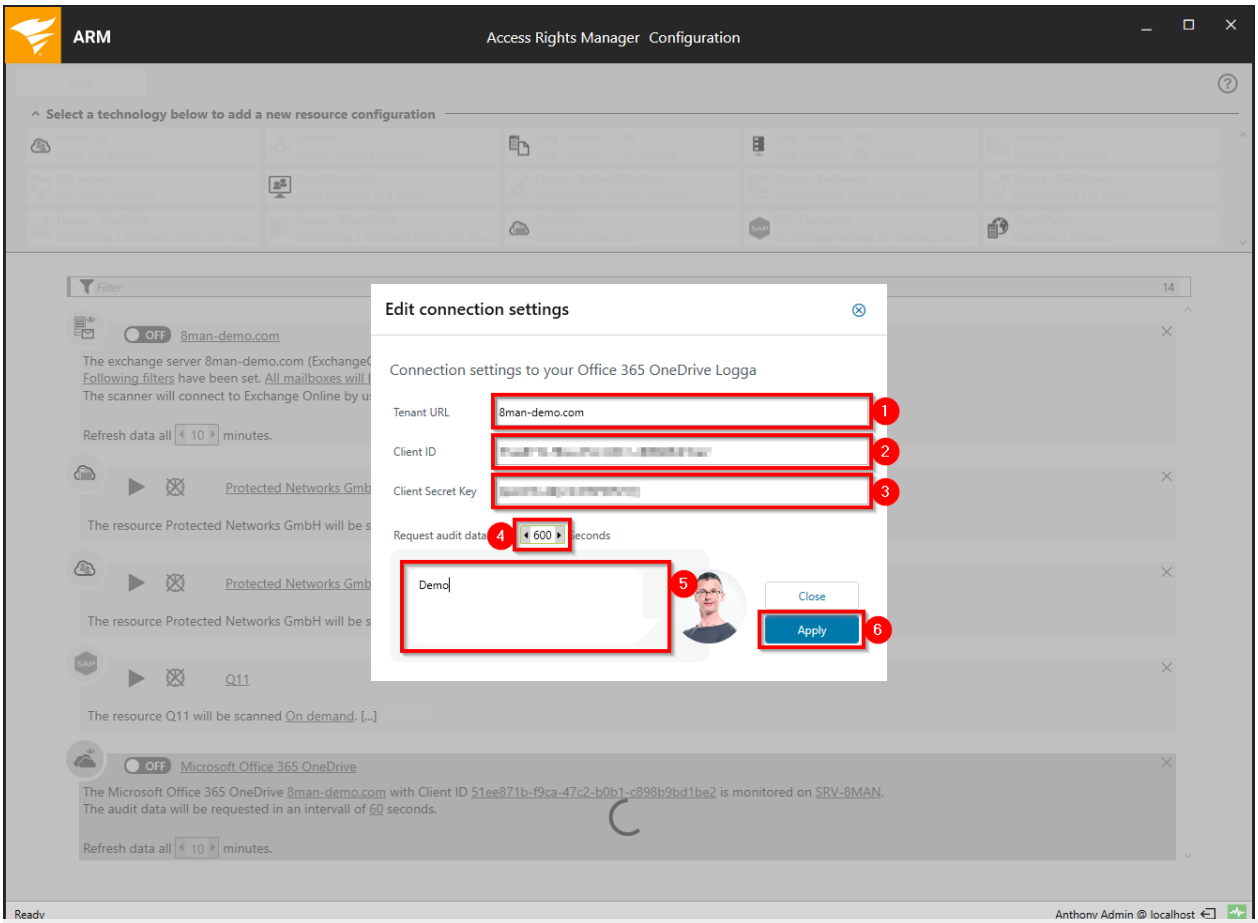
Select "Logga - OneDrive".



1. Select a collector server. Note, that the collector server needs internet access to pull OneDrive events.
2. Click "Apply".



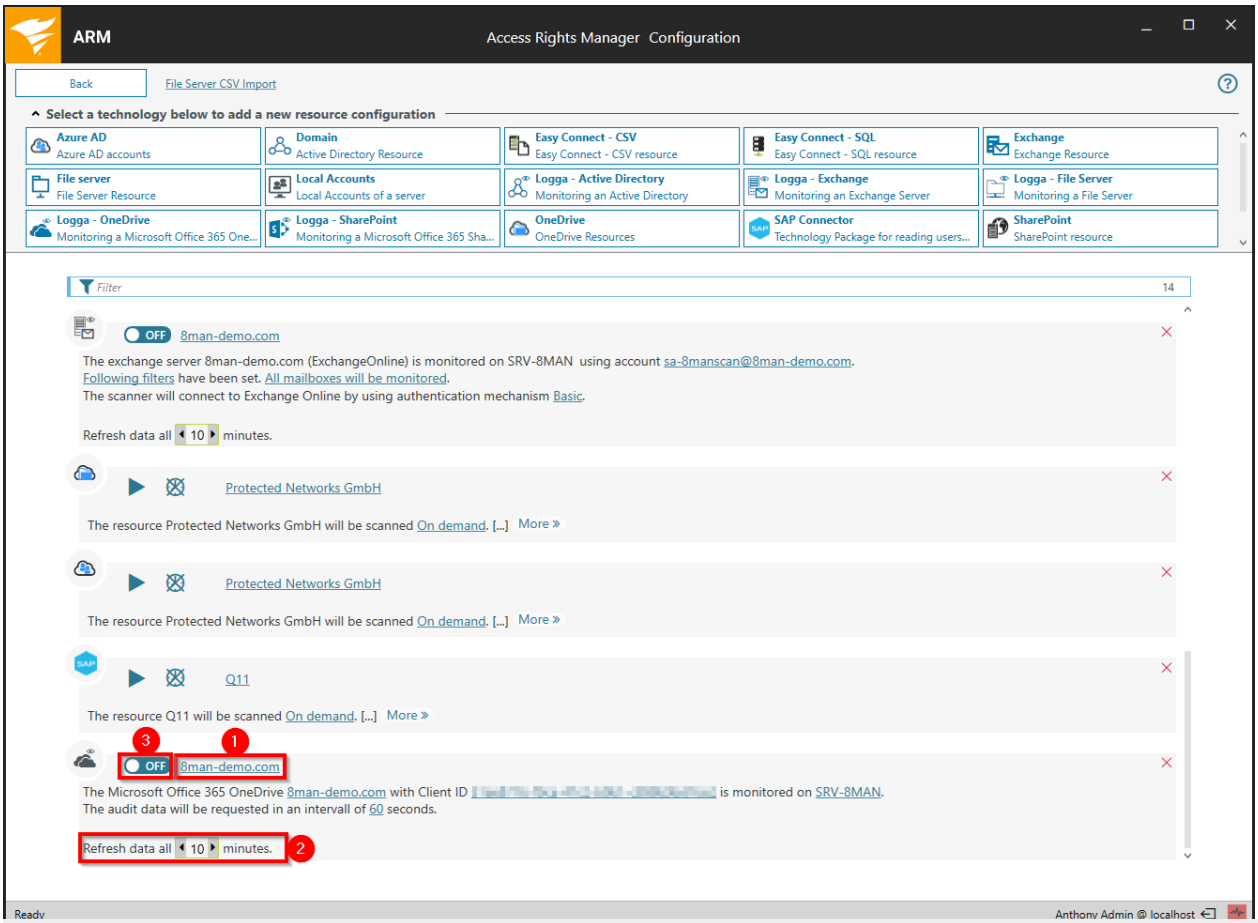
1. Newly added resources are always at the bottom.
2. You have created a OneDrive Logga configuration.
3. The warning indicates that not all required settings are made.
4. Click one of the links.



1. Enter the tenant, for example "mycompany.com".
2. Enter the application ID.
3. Enter the client secret.

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".

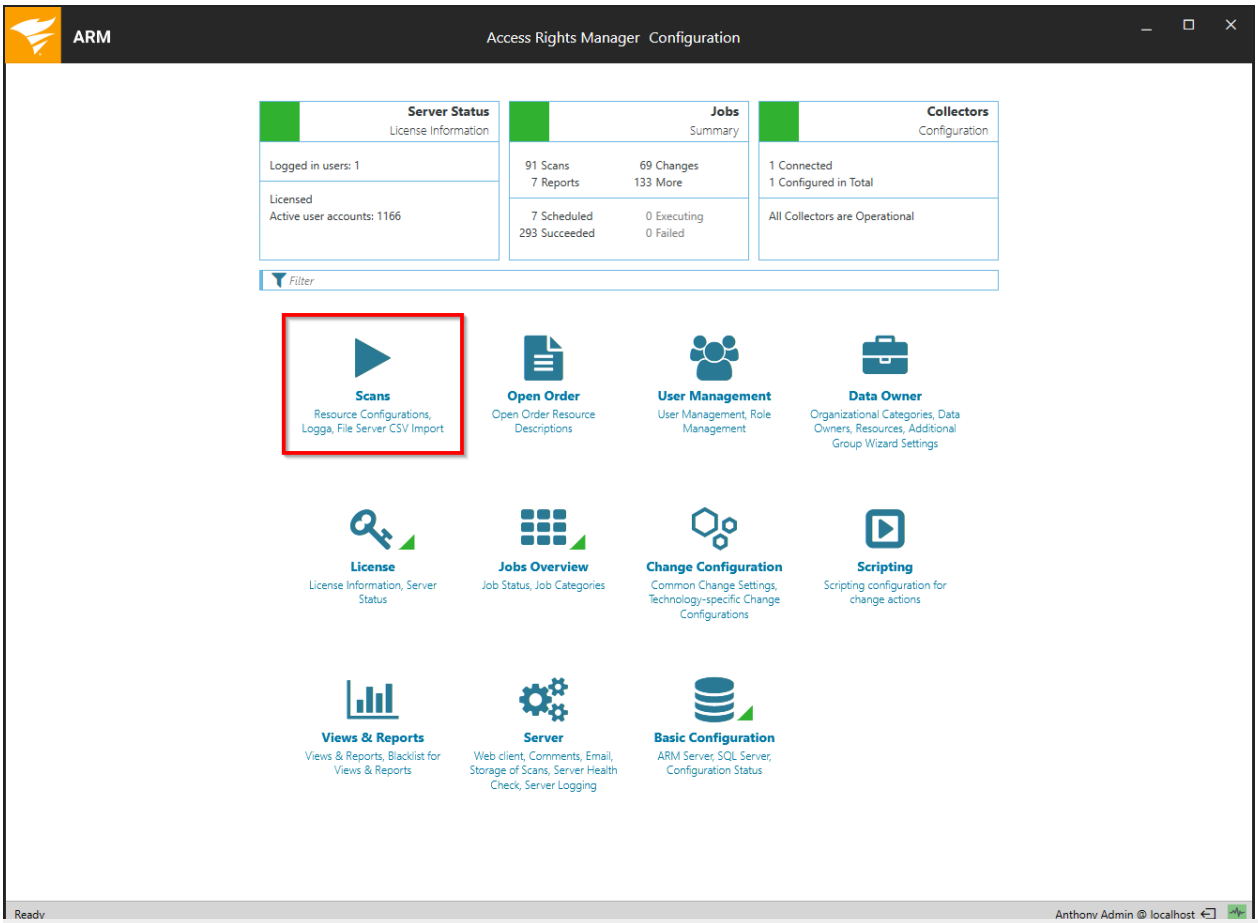


1. Give the OneDrive Logga configuration a new name.
2. Specify the interval at which the Logga data is written from the collector to the ARM database.
3. Turn on the Logga.

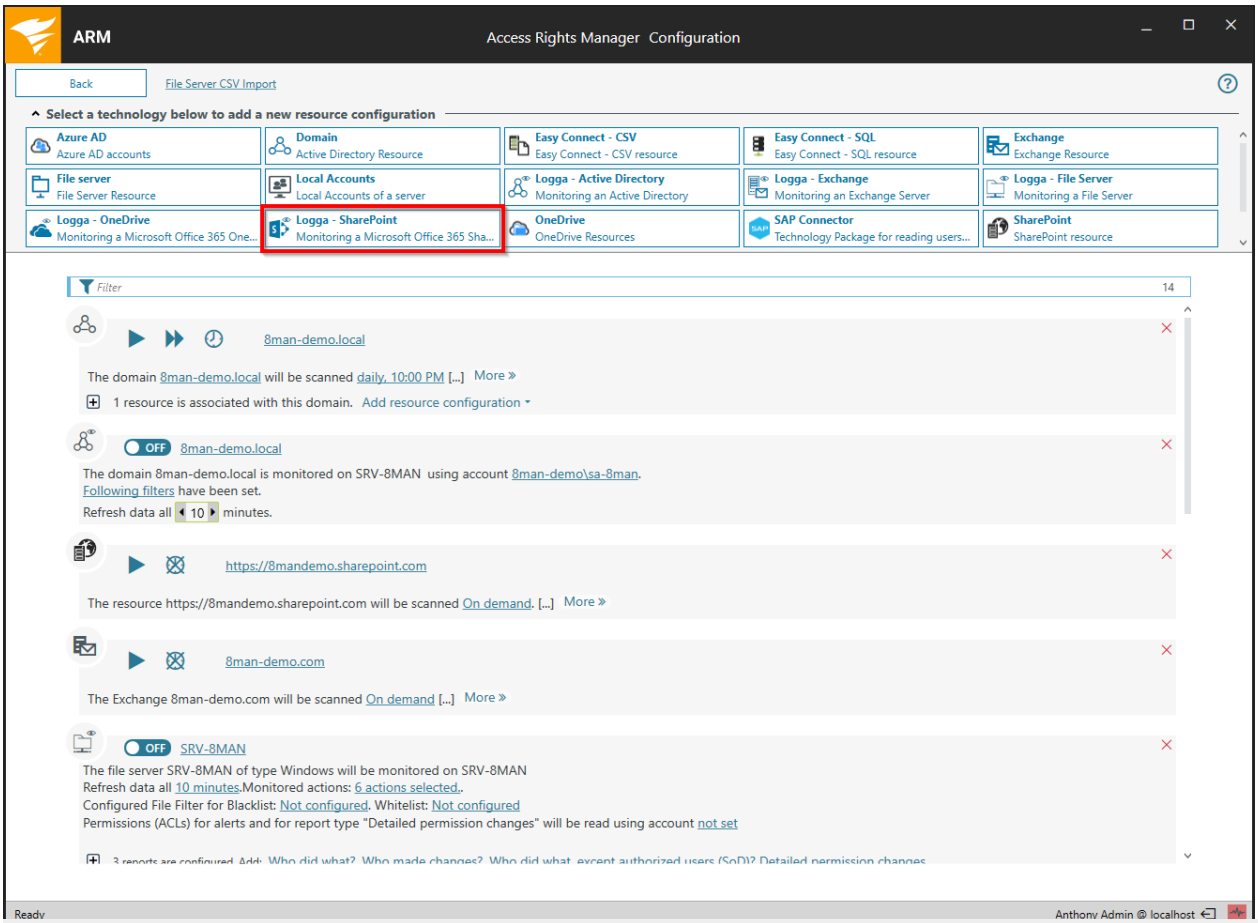
Please note that when you enable logging for the first time, Microsoft states that it can take up to 12 hours for the first events to be recorded.

Configure SharePoint Online Logga

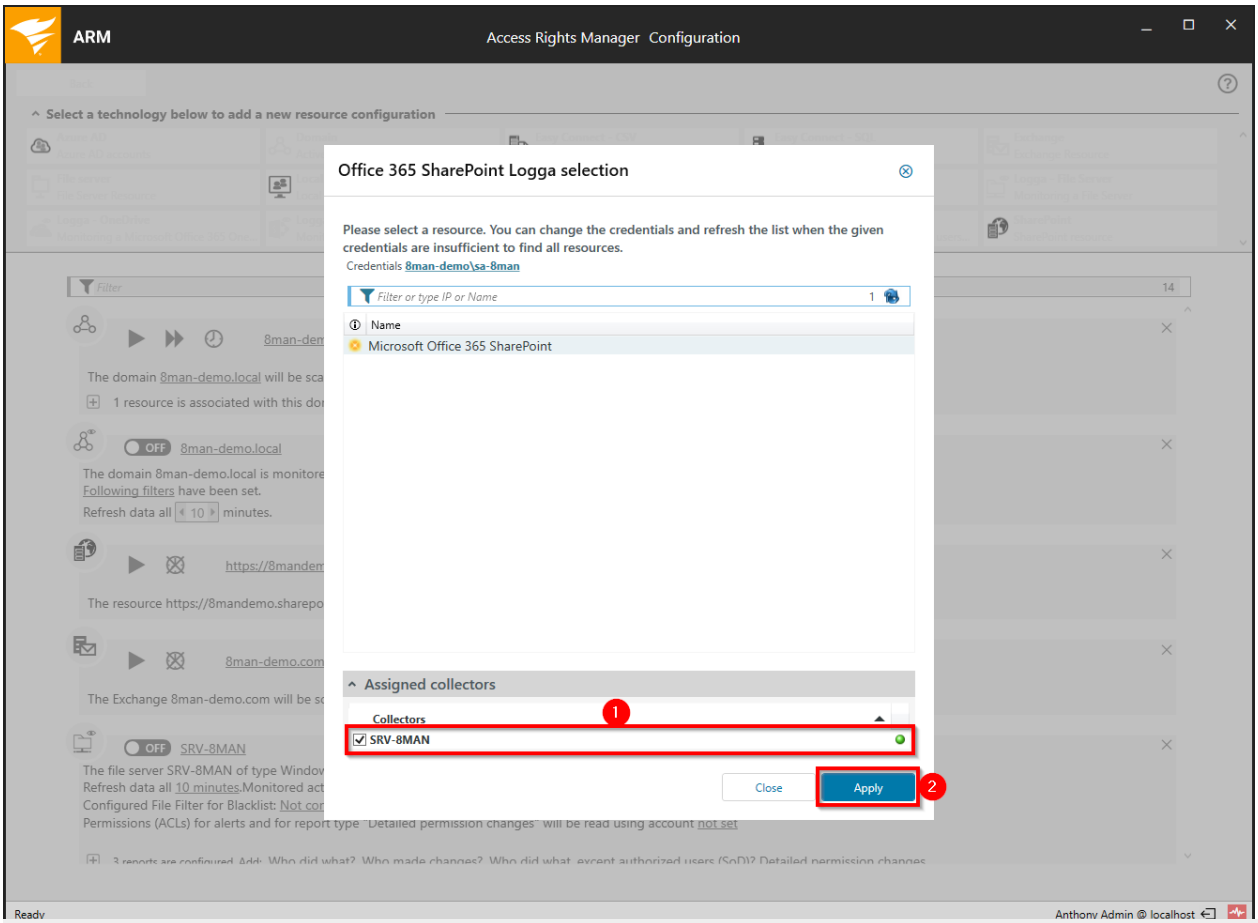
To enable the SharePoint Online Logga, you must have completed the preparation for Office 365 integration in the Azure Portal.



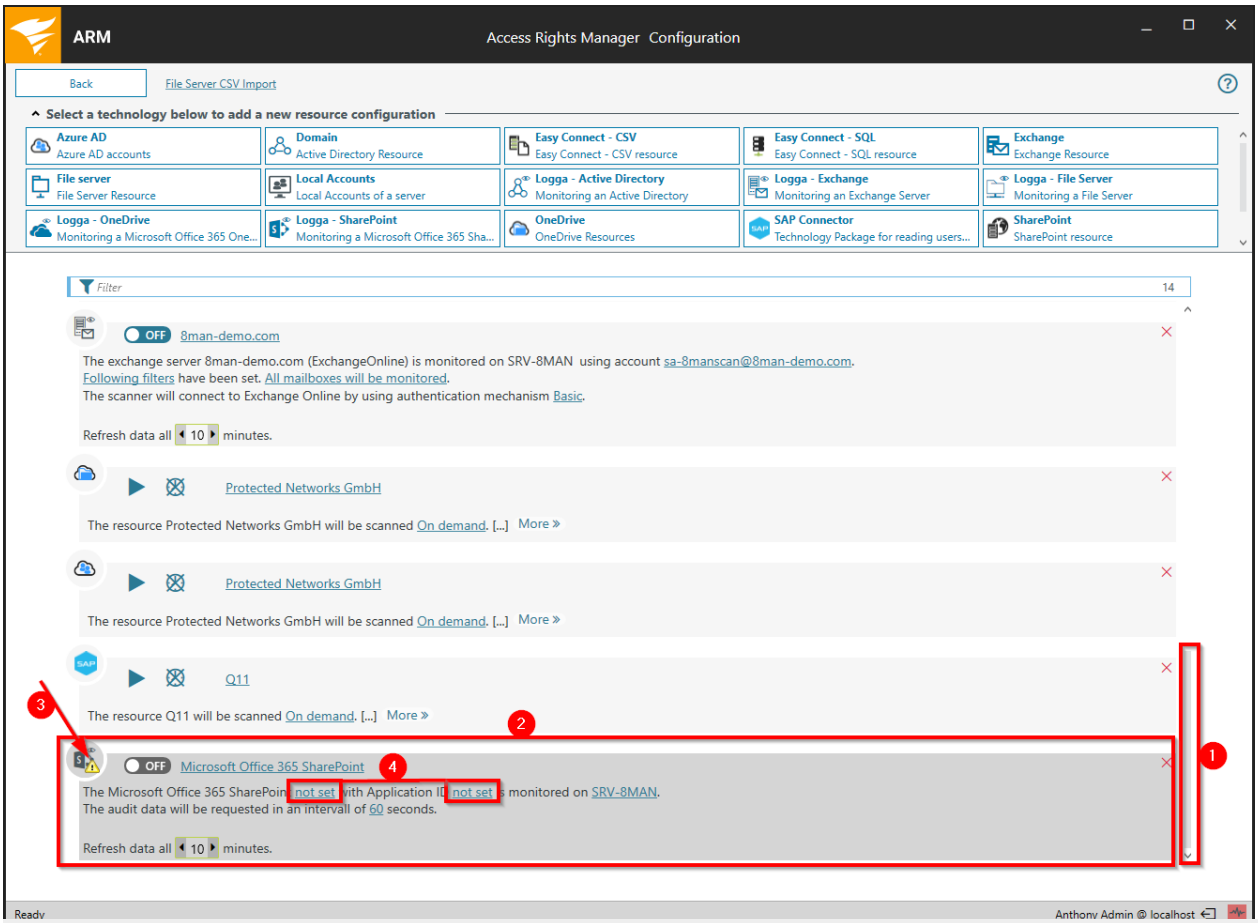
Start the ARM configuration application and click "Scans".



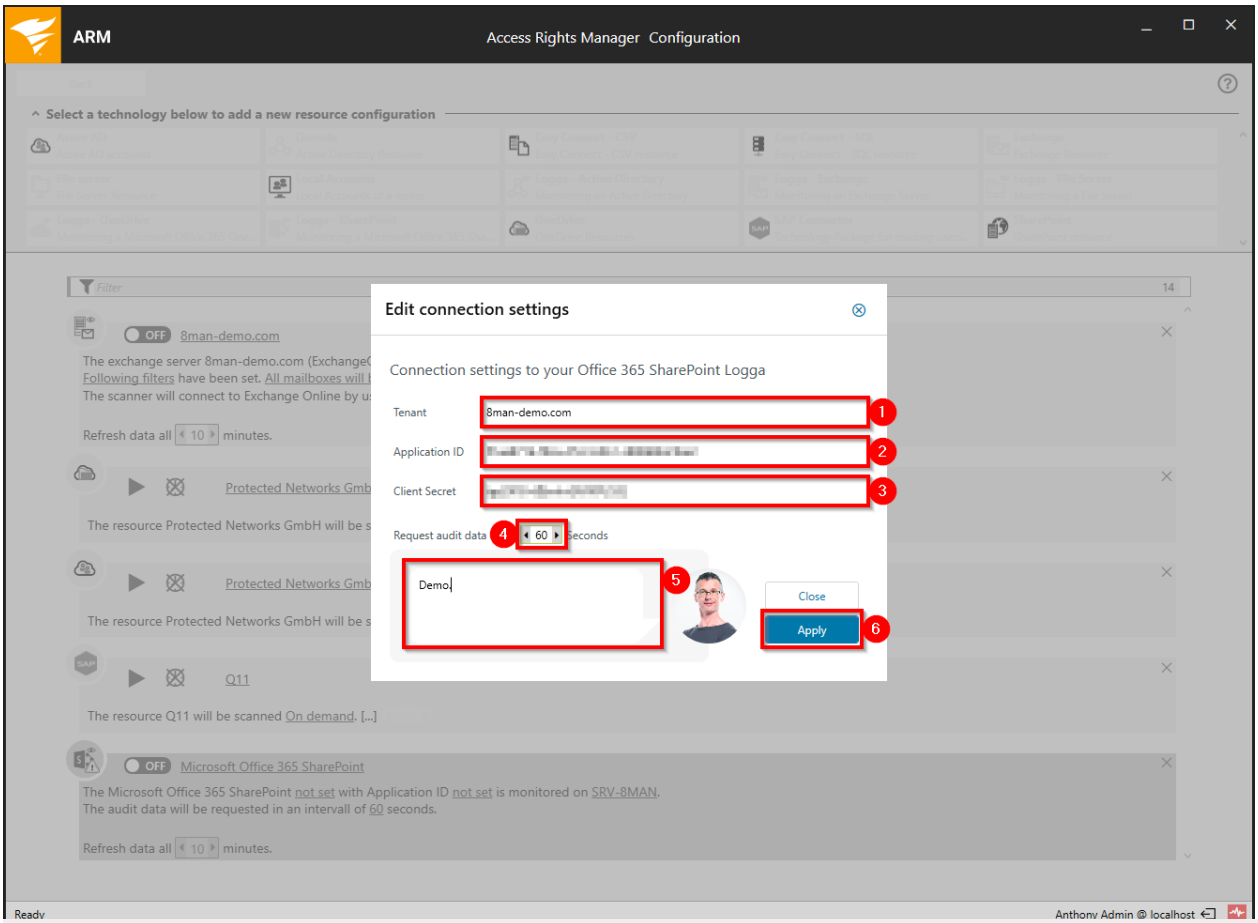
Select "Logga - SharePoint Online".



1. Select a collector server. Note, that the collector server needs internet access to pull SharePoint Online events.
2. Click "Apply".



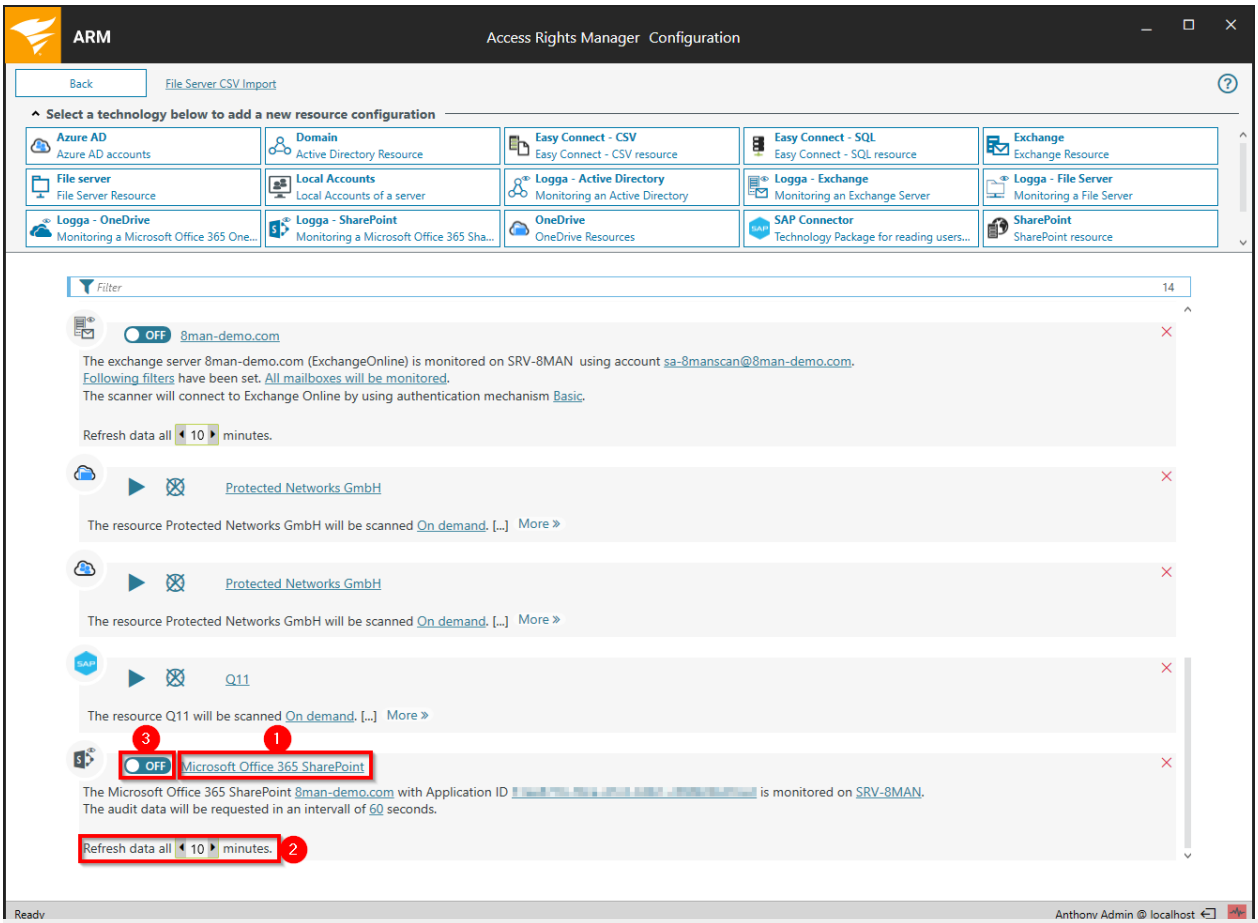
1. Newly added resources are always at the bottom.
2. You have created a SharePoint Online Logga configuration.
3. The warning indicates that not all required settings are made.
4. Click one of the links.



1. Enter the tenant, for example "mycompany.com".
2. Enter the application ID.
3. Enter the client secret.

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".



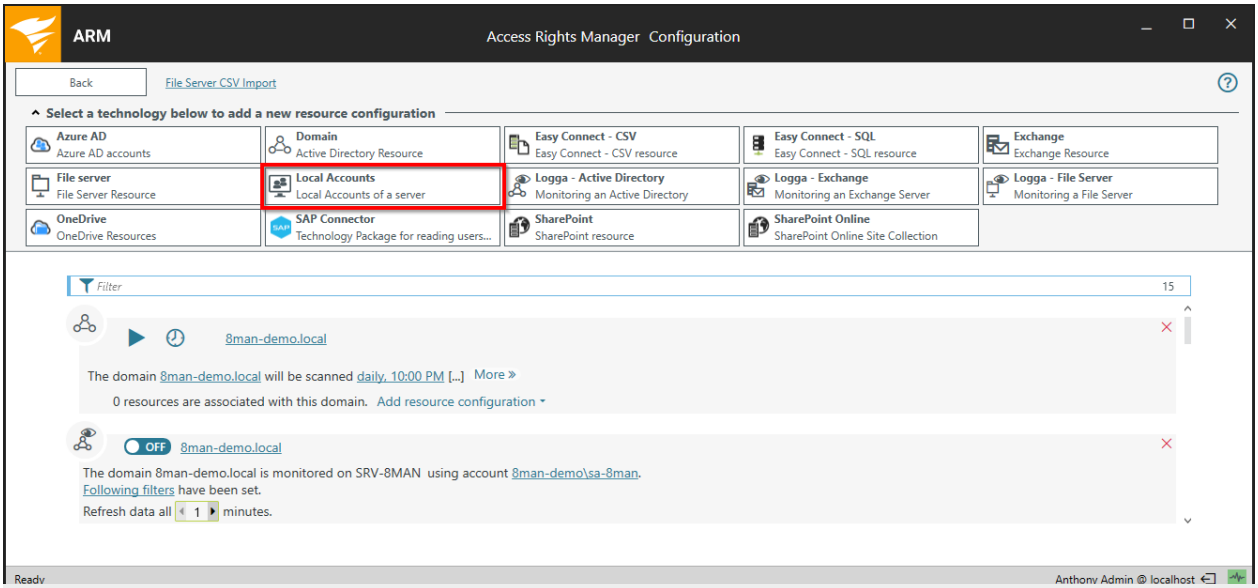
1. Give the SharePoint Online Logga configuration a new name.
2. Specify the interval at which the Logga data is written from the collector to the ARM database.
3. Turn on the Logga.

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.

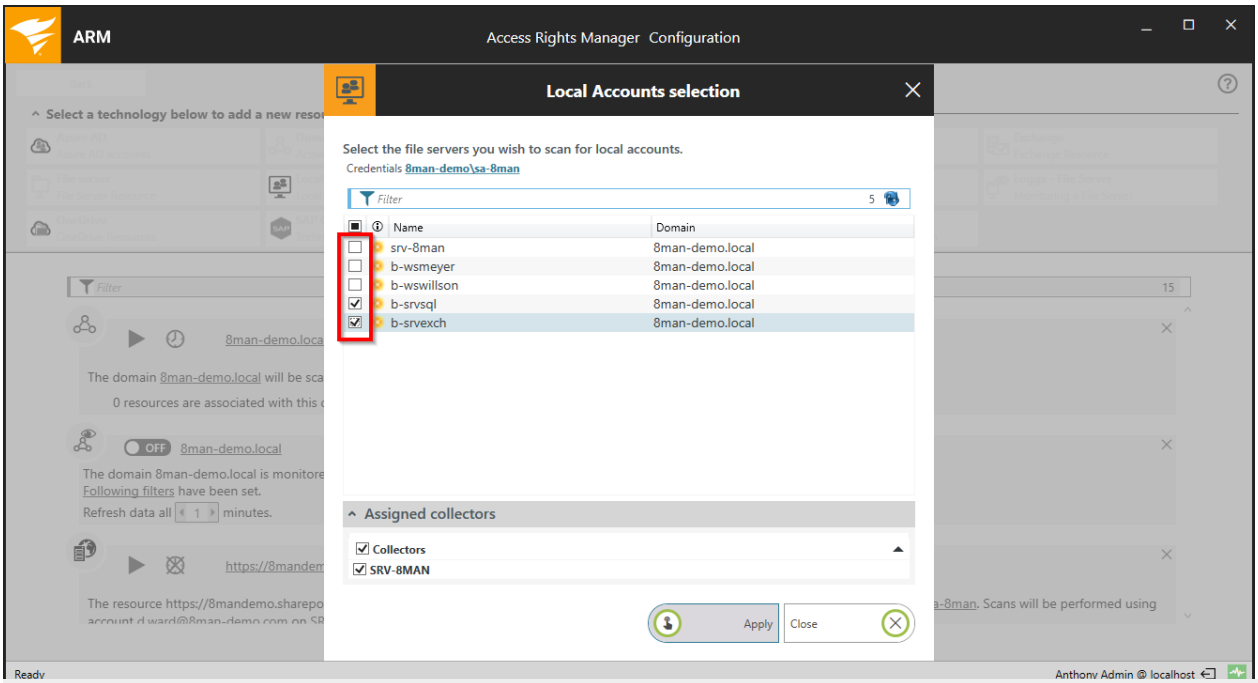
Scan local accounts

ARM is able to read local accounts of computers (and not just file servers).

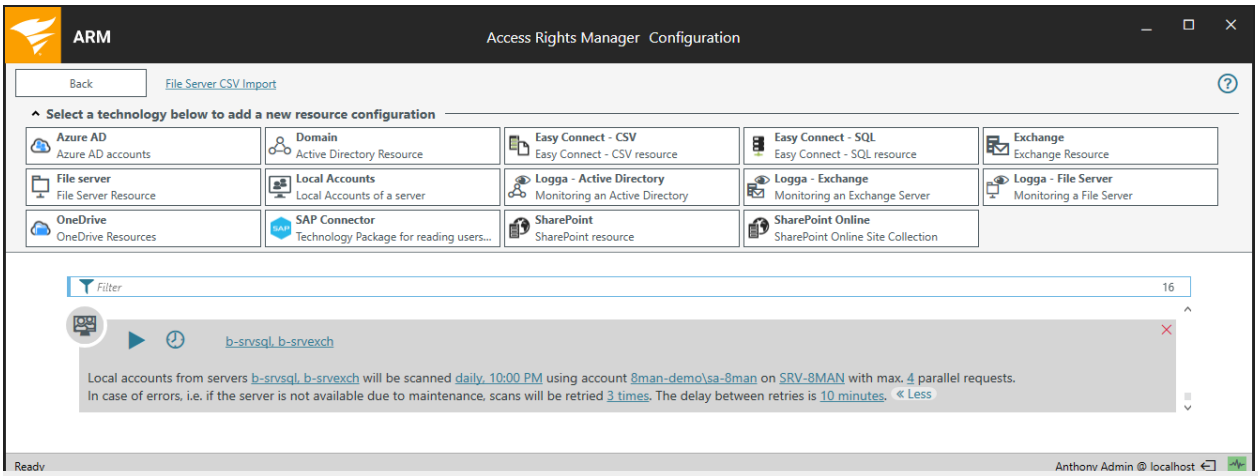
Adding local accounts scans



Select "Local Accounts".



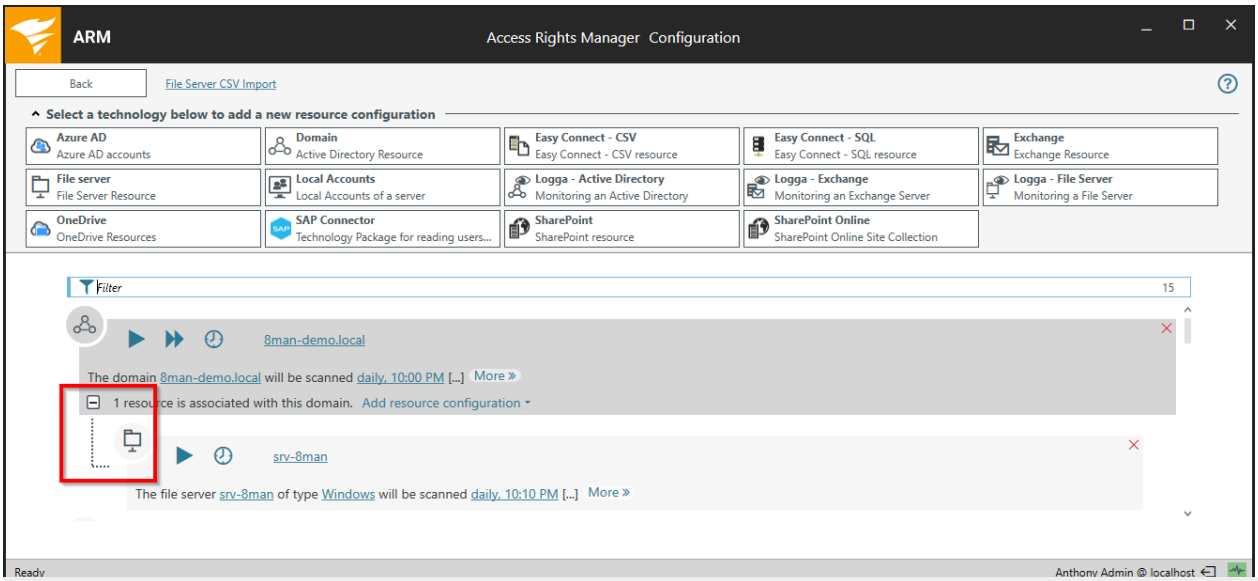
Select the computers for which you want to read local accounts.



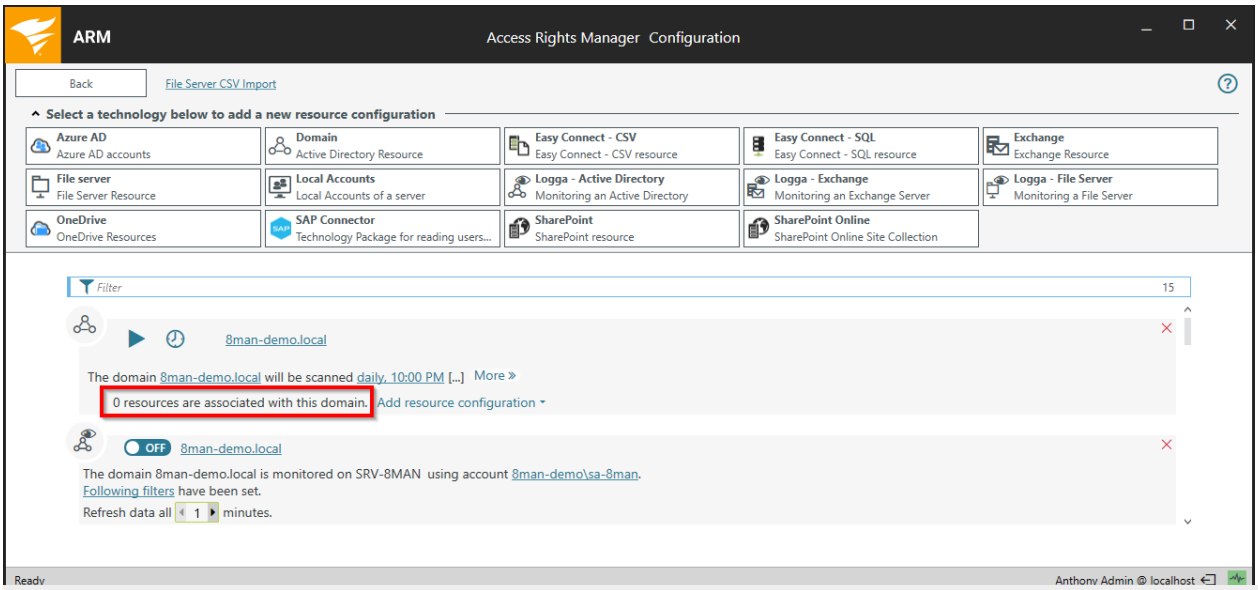
The available configuration options are the same as with an AD-scan.

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.

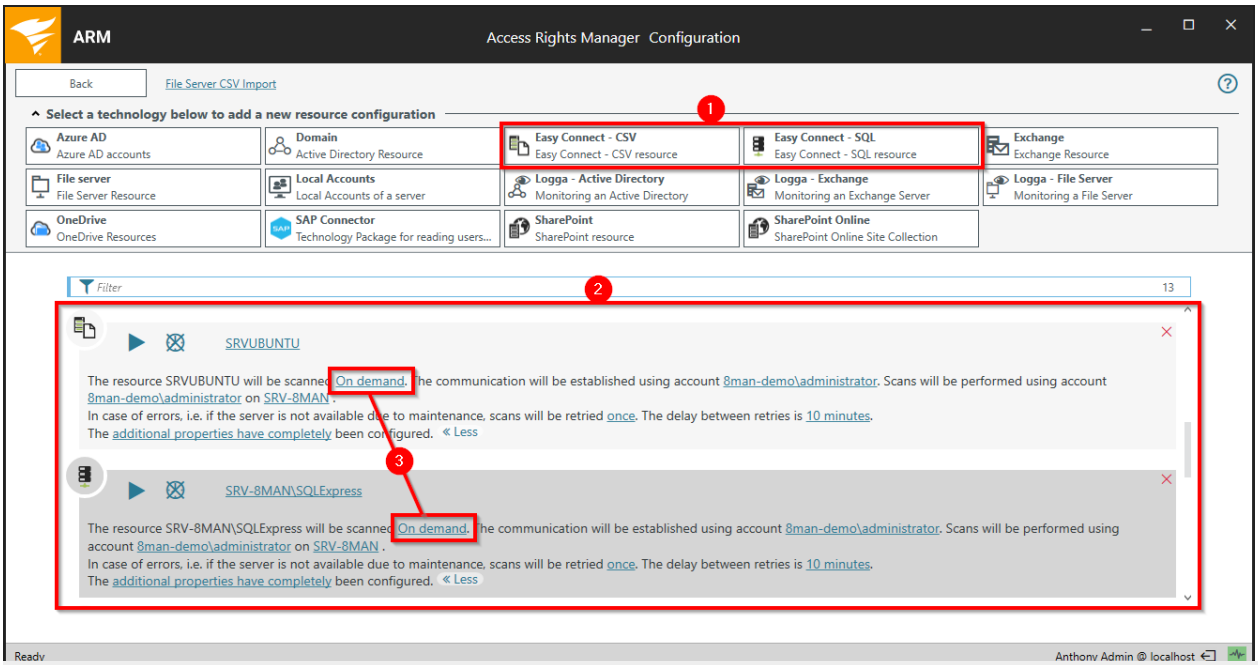


ARM displays assigned resources in the ARM application only if the appropriate domain has been selected.



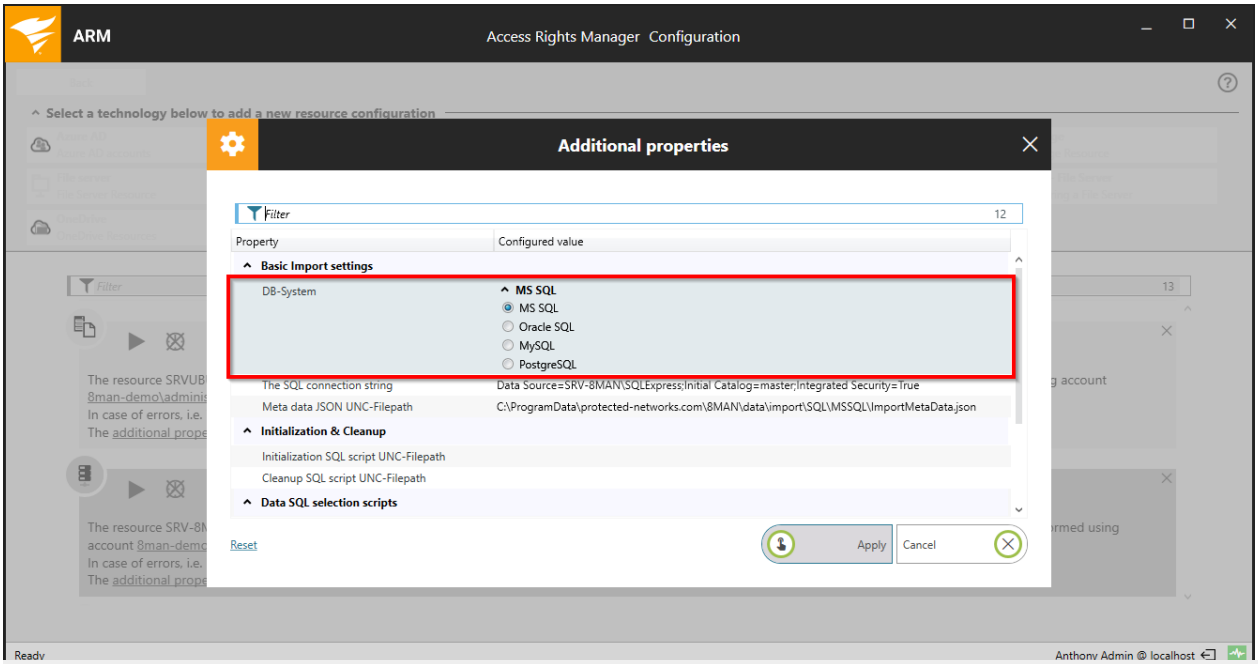
Unassigned resources are always displayed in the ARM application, regardless of the domain selected by the current user.

Integrate Easy Connect resources



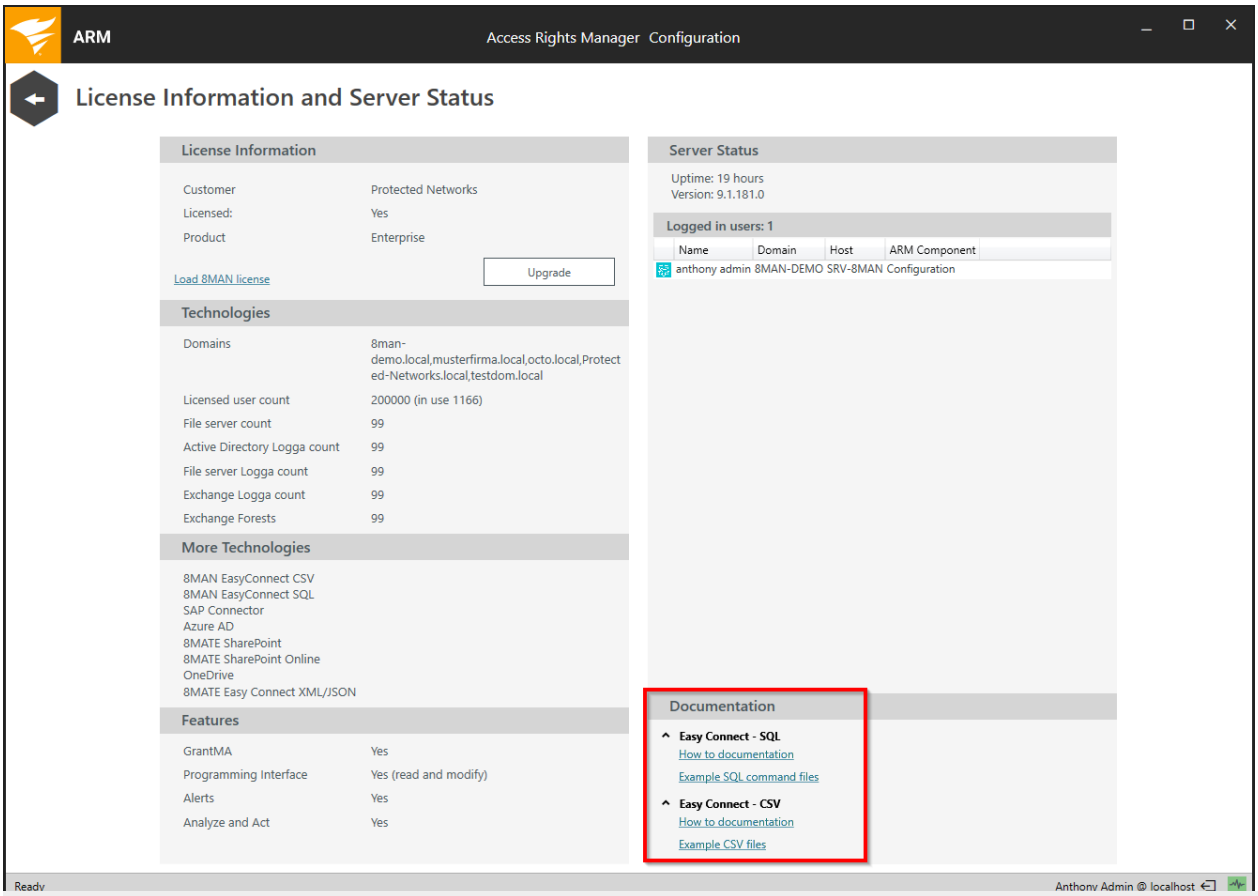
Click "Scans" on the ARM configuration application homepage.

1. Add an Easy Connect resource.
2. The configuration is seamlessly integrated.
3. Configure a regularly import.



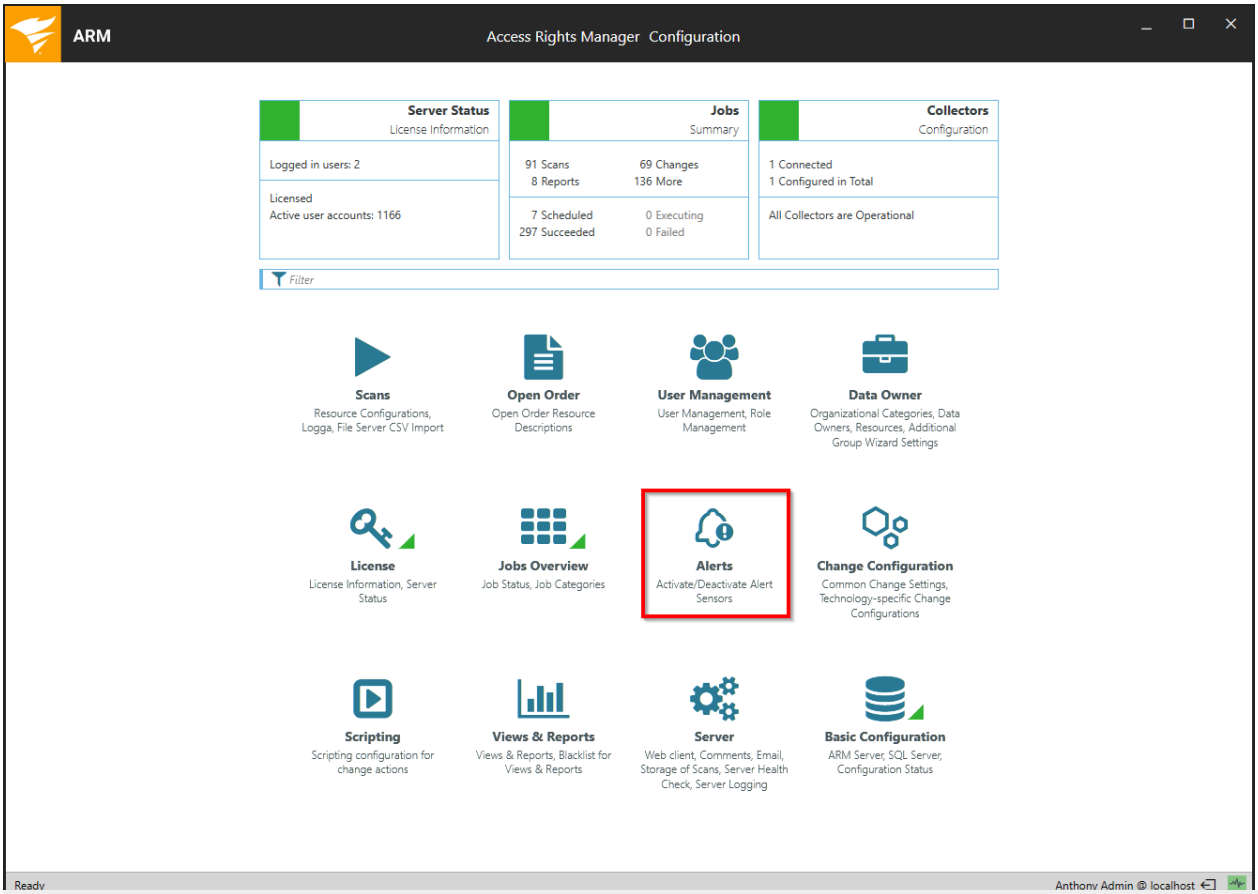
ARM supports the following SQL-server:

- Microsoft SQL
- Oracle SQL
- MySQL
- PostgreSQL



Find a detailed documentation on required CSV-file structure and example files under "License" in the configuration application.

Alerts

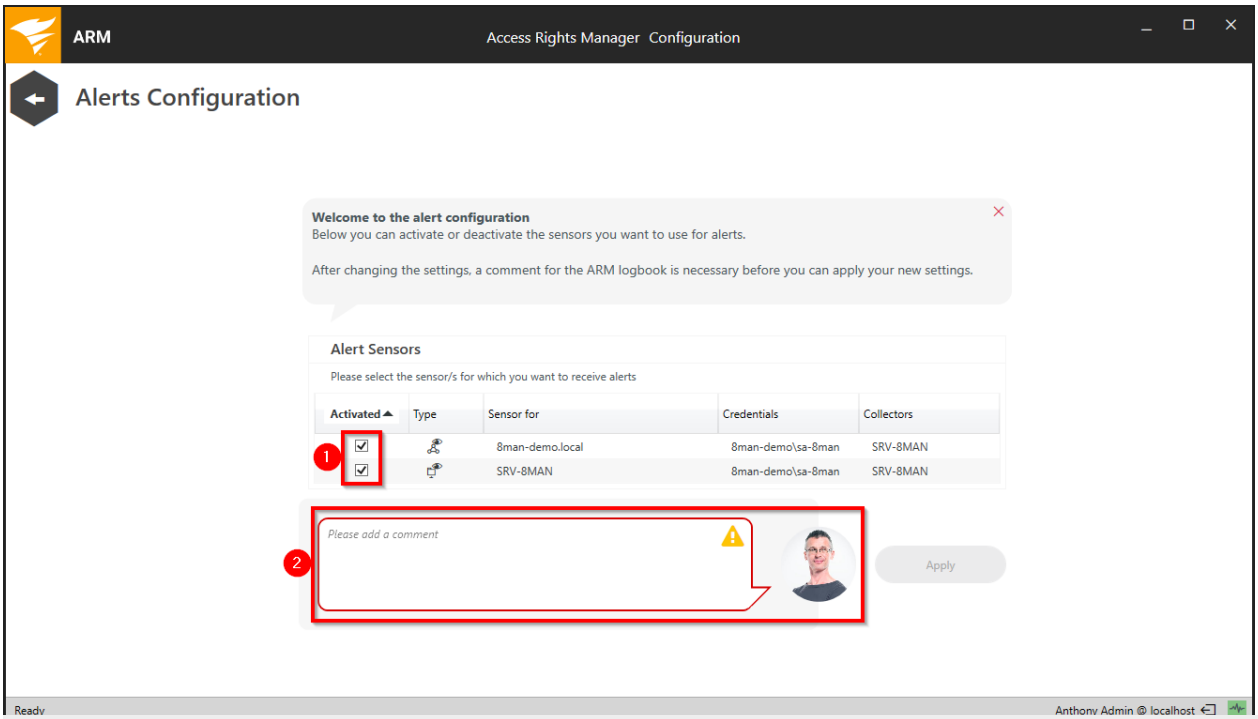


You activate and deactivate the alarm sensors in the "Alarms" category.

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



1. Enable/disable alert sensors.
2. You must enter a comment.

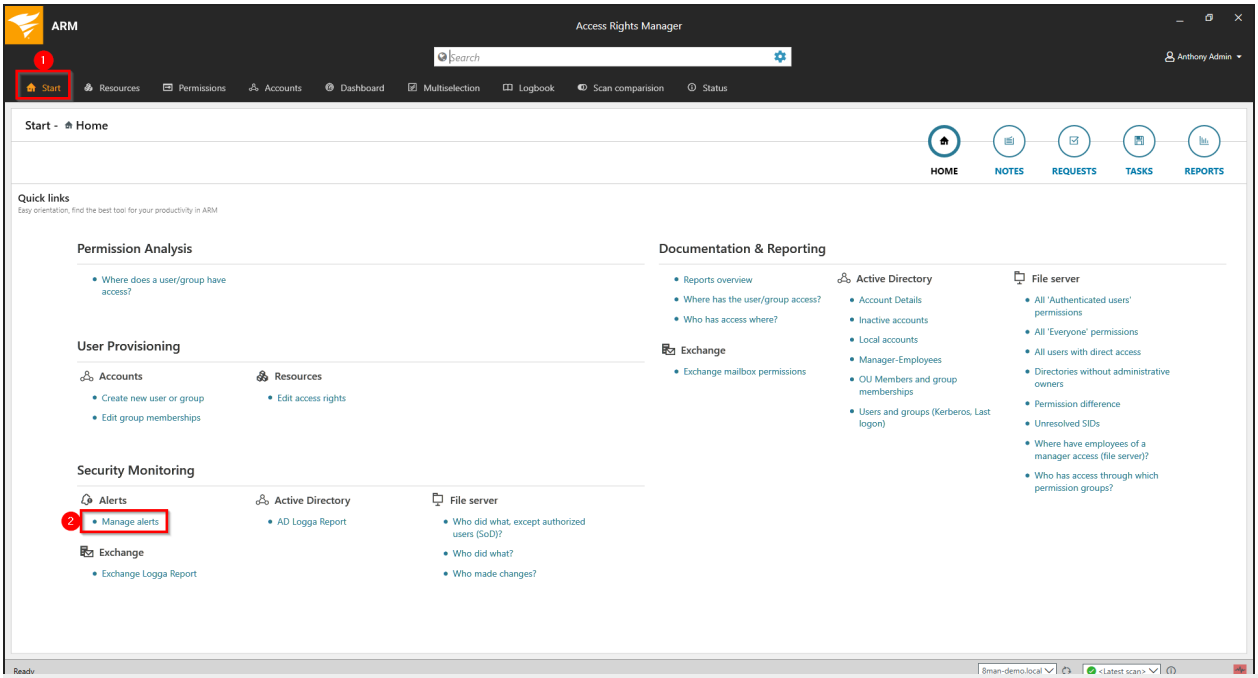
⚠ The alert configurations are only effective with active sensors.

Manage alerts

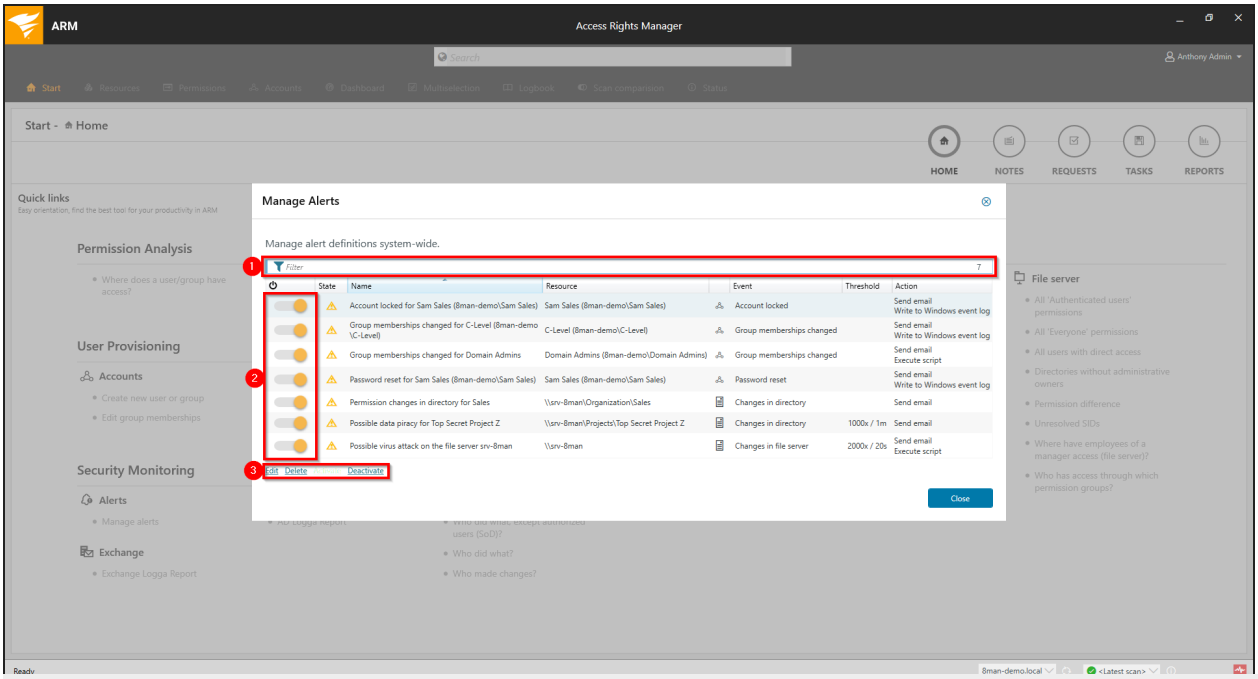
Background / Value

Saved alert configurations can be modified at any time via the ARM home page.

Step-by-step process



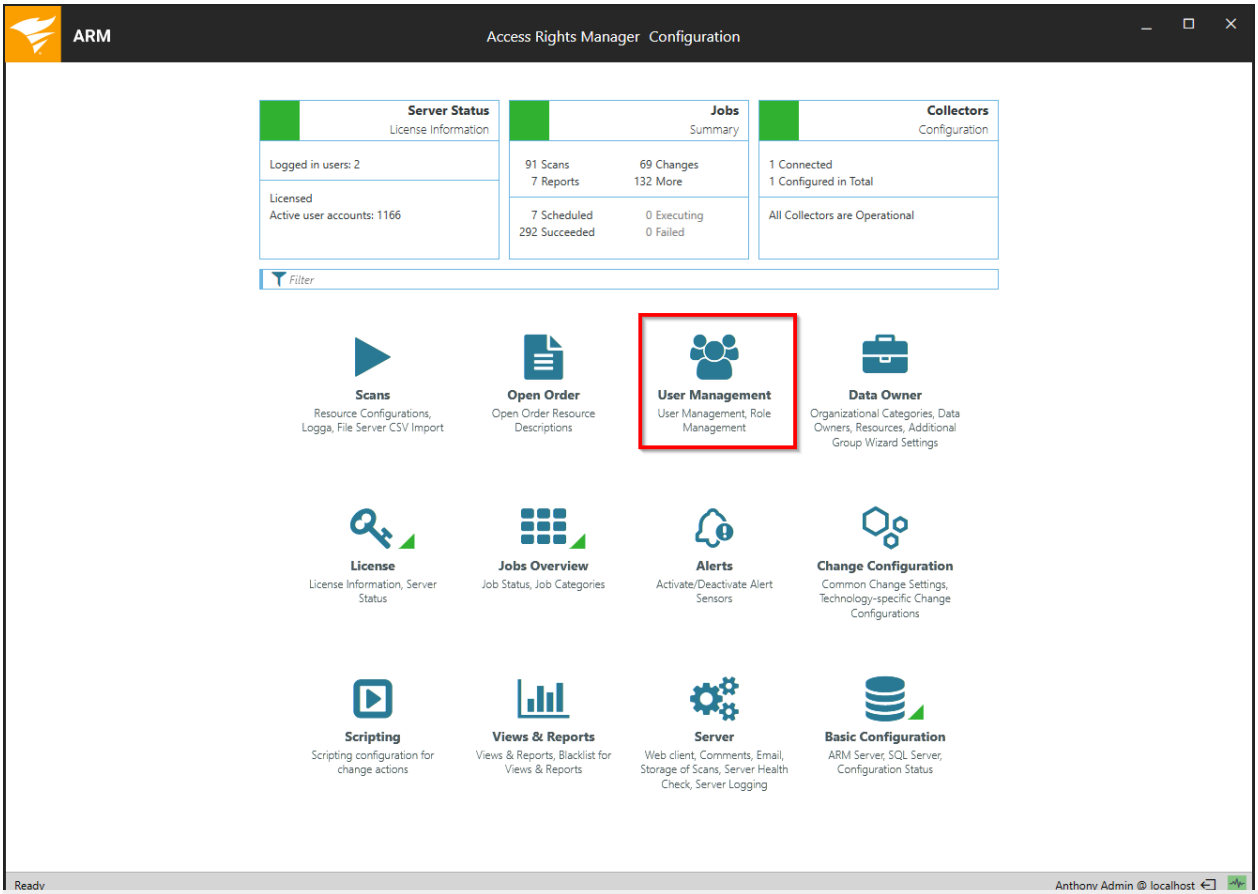
1. Select "Start".
2. Click "Manage alerts".



ARM shows you all alert configurations.

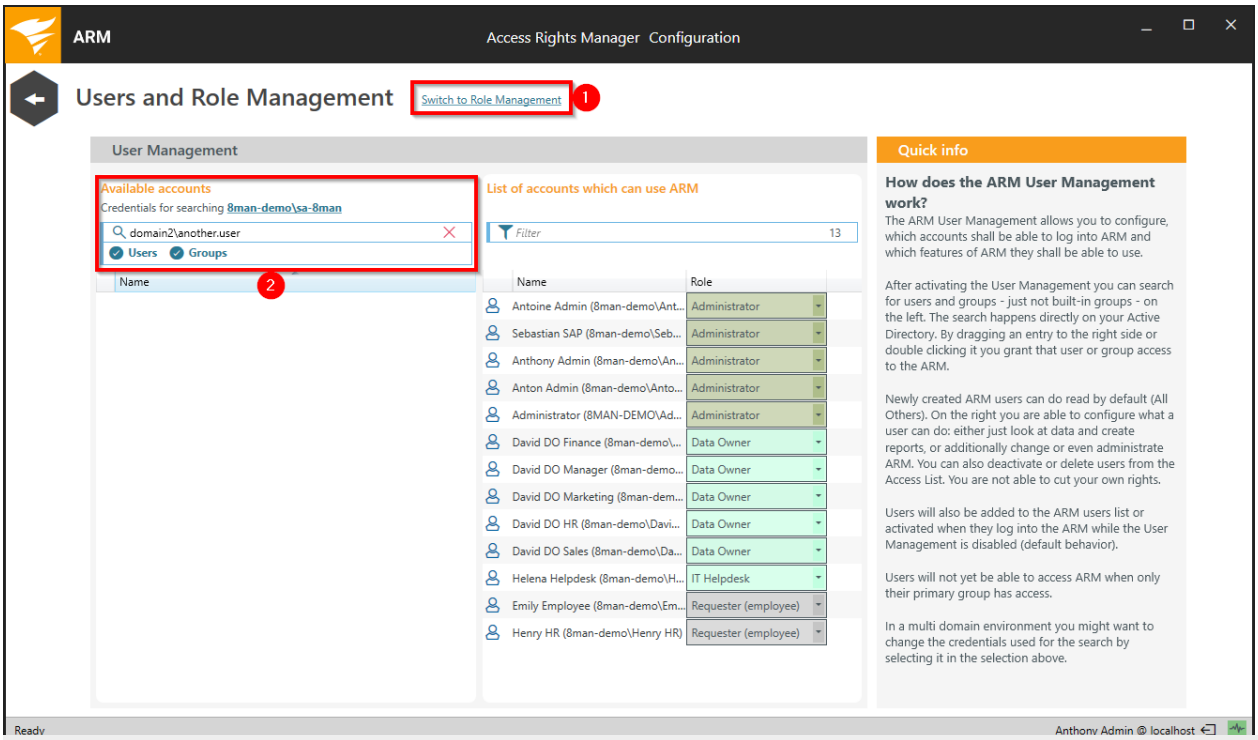
1. Search for an alert configuration.
2. Turn alerts on or off.
3. Use the links to edit, delete or enable/disable the selected alert configuration. Alternatively you can right-click an entry and use the context menu.

Manage ARM users



Click "User Management" to add ARM-Users and assign roles.

Add ARM users

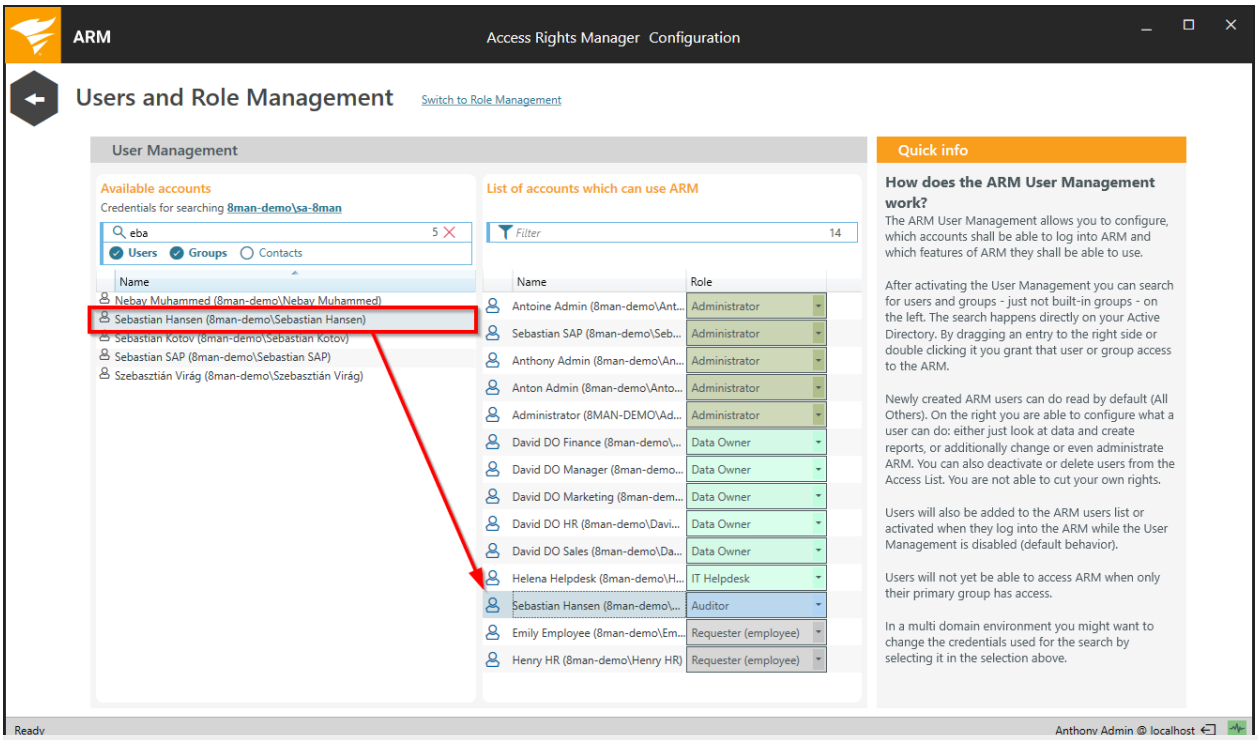


1. Use the link to switch between user and role management.
2. ARM triggers a live request to your AD when adding an ARM user. It is therefore not required to perform an AD scan prior to adding a user.

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.



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

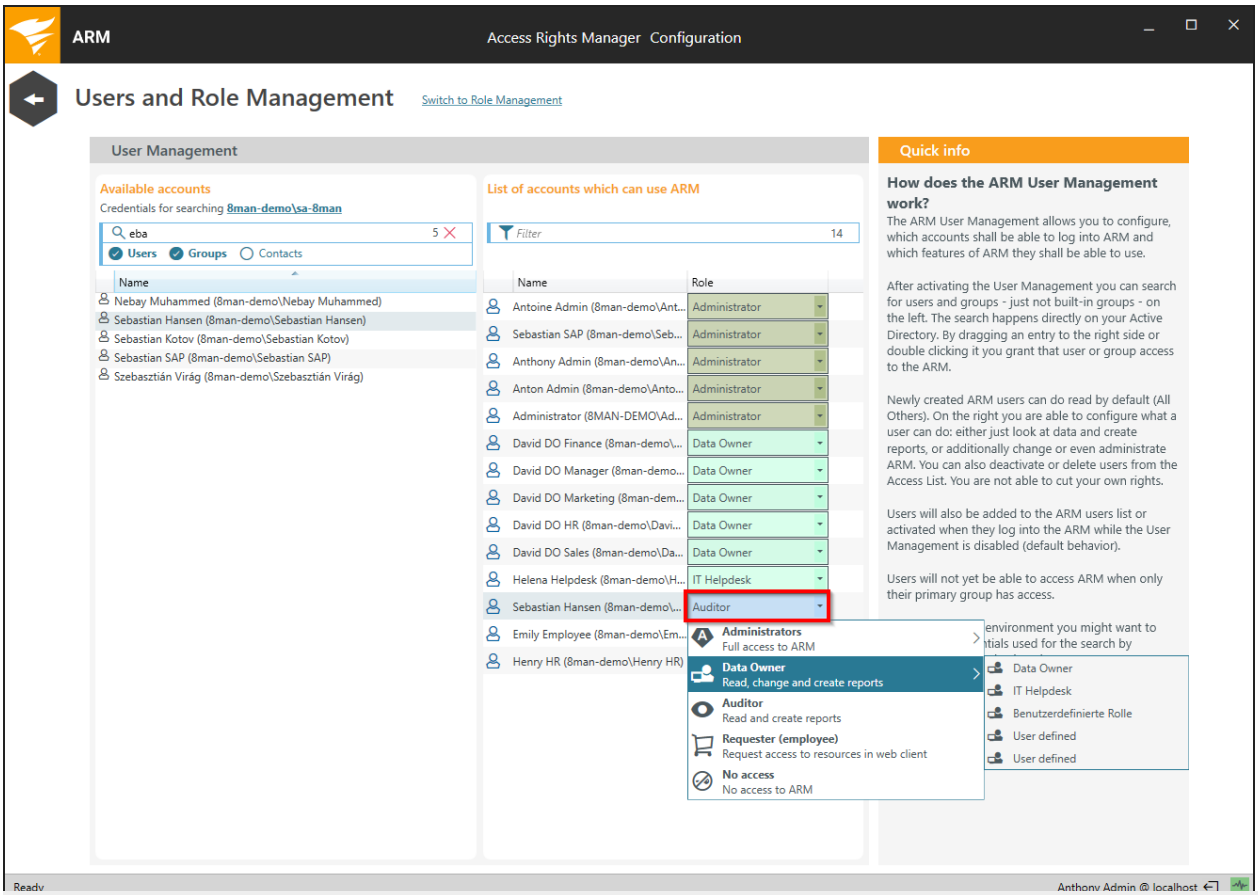
If nested group memberships should be resolved, please follow the instructions in the knowledgebase article Configure ARM for the use of nested groups in the ARM user management.

⚠ 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.

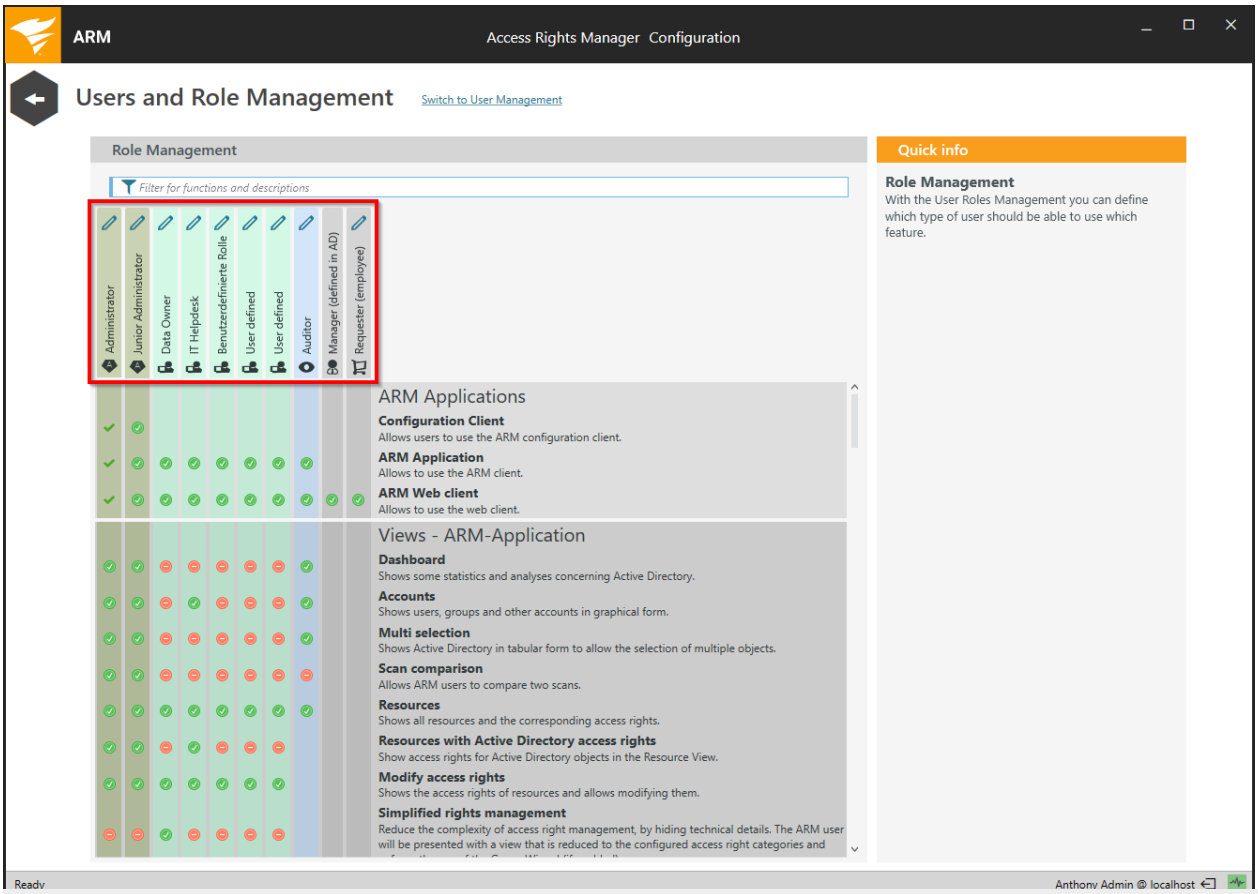
Assign a role to ARM users



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



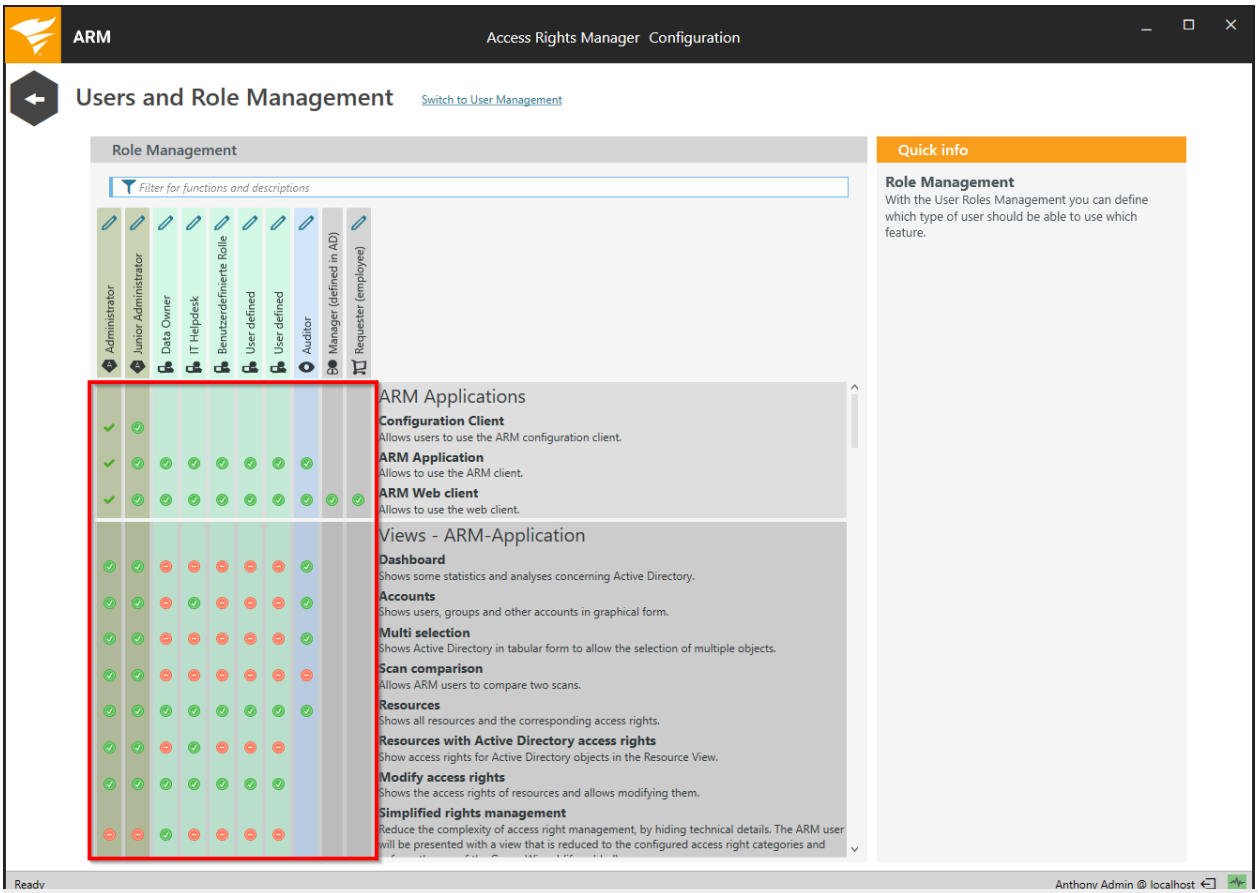
ARM provides different user role types (from left to right):

- 2 Administrator-roles
- 5 Change-roles
- 1 Read only-role
- 1 Manager Role
- 1 Requester Role

The Manager Role can not be assigned by the ARM user management. It is assigned by the AD attribute "Manager".

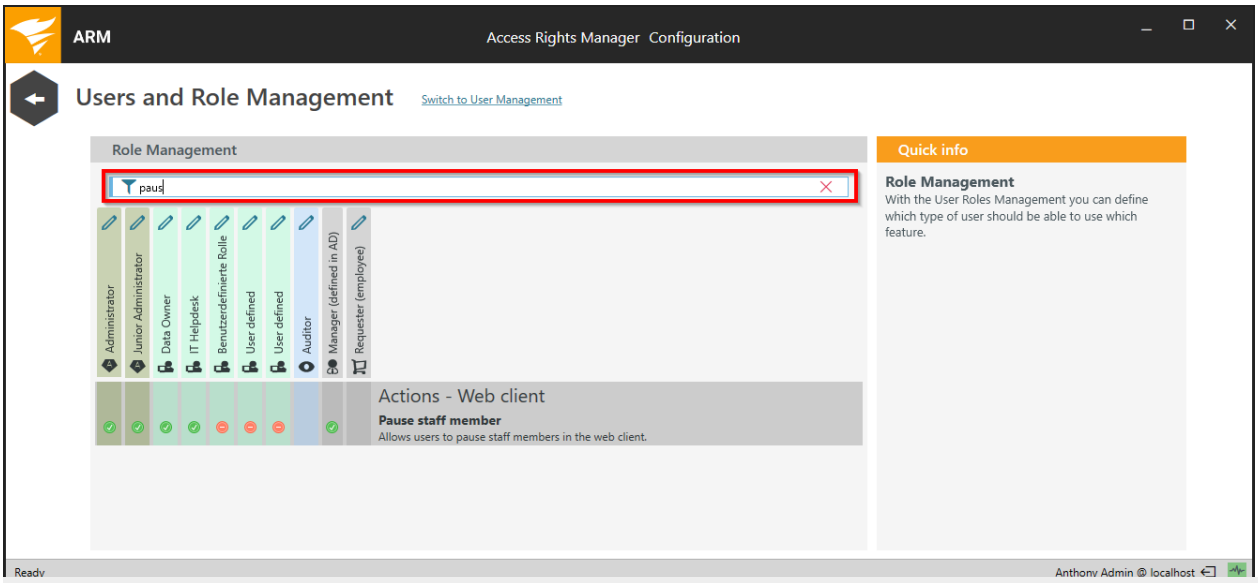
You can change the name of the role by clicking on the pen icon.

Only the first administrator role (leftmost column) can use the user 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).

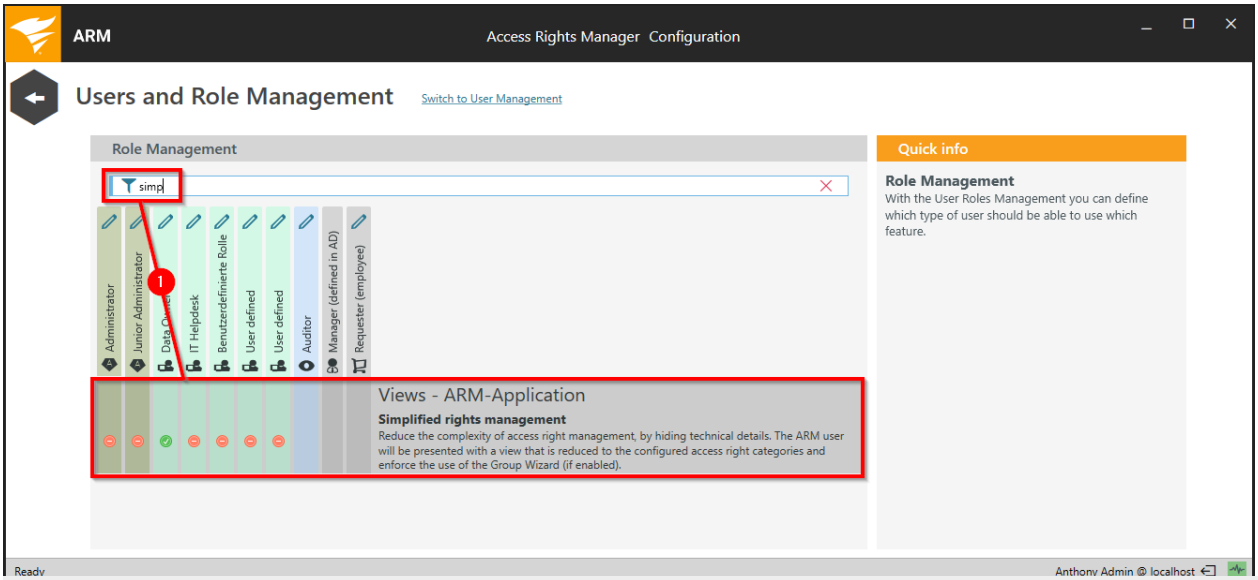


Use the filter to quickly find the desired option.

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.

The changes take effect immediately without requiring users to log in again.

Simplified rights management

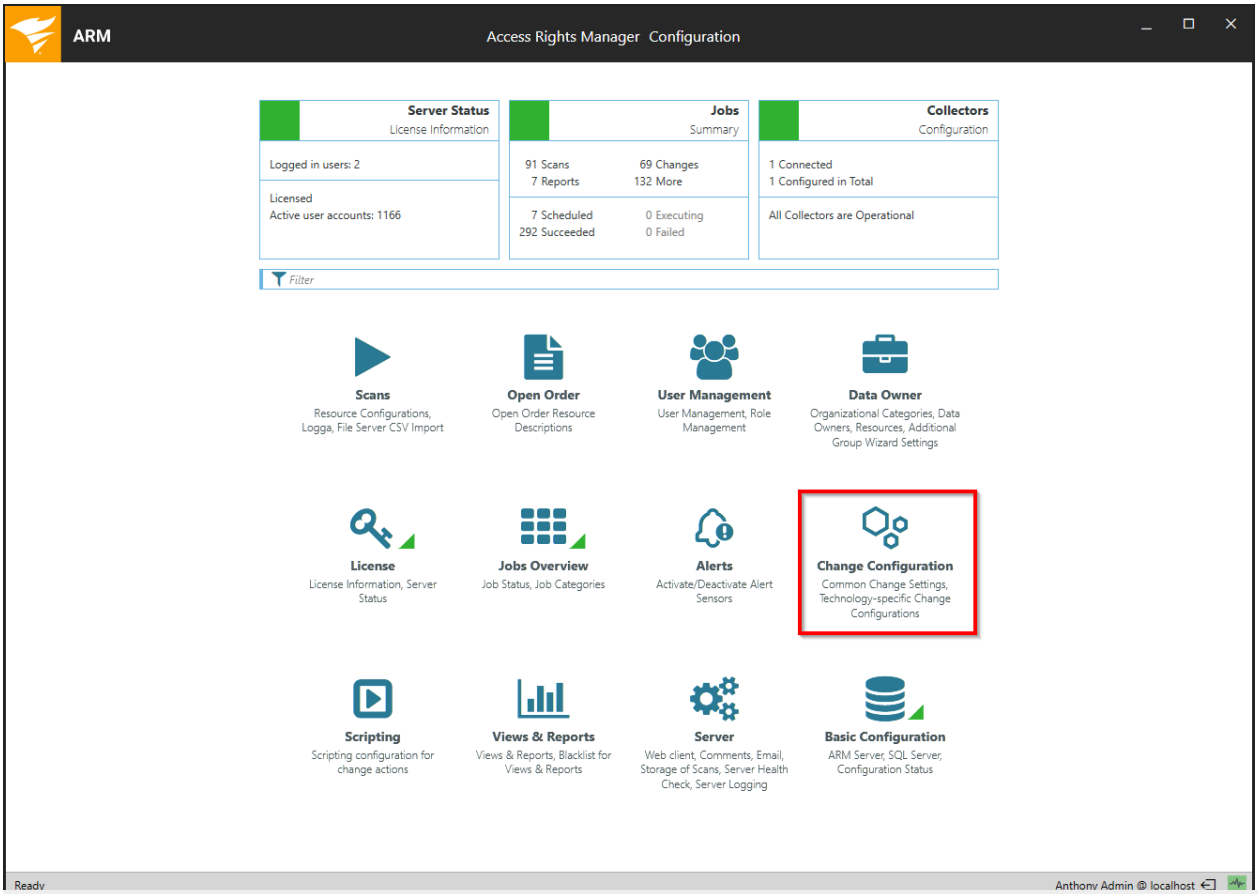


1. With the simplified rights management, certain details are hidden to simplify operation. This option is suitable for non-technical data owners.

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.

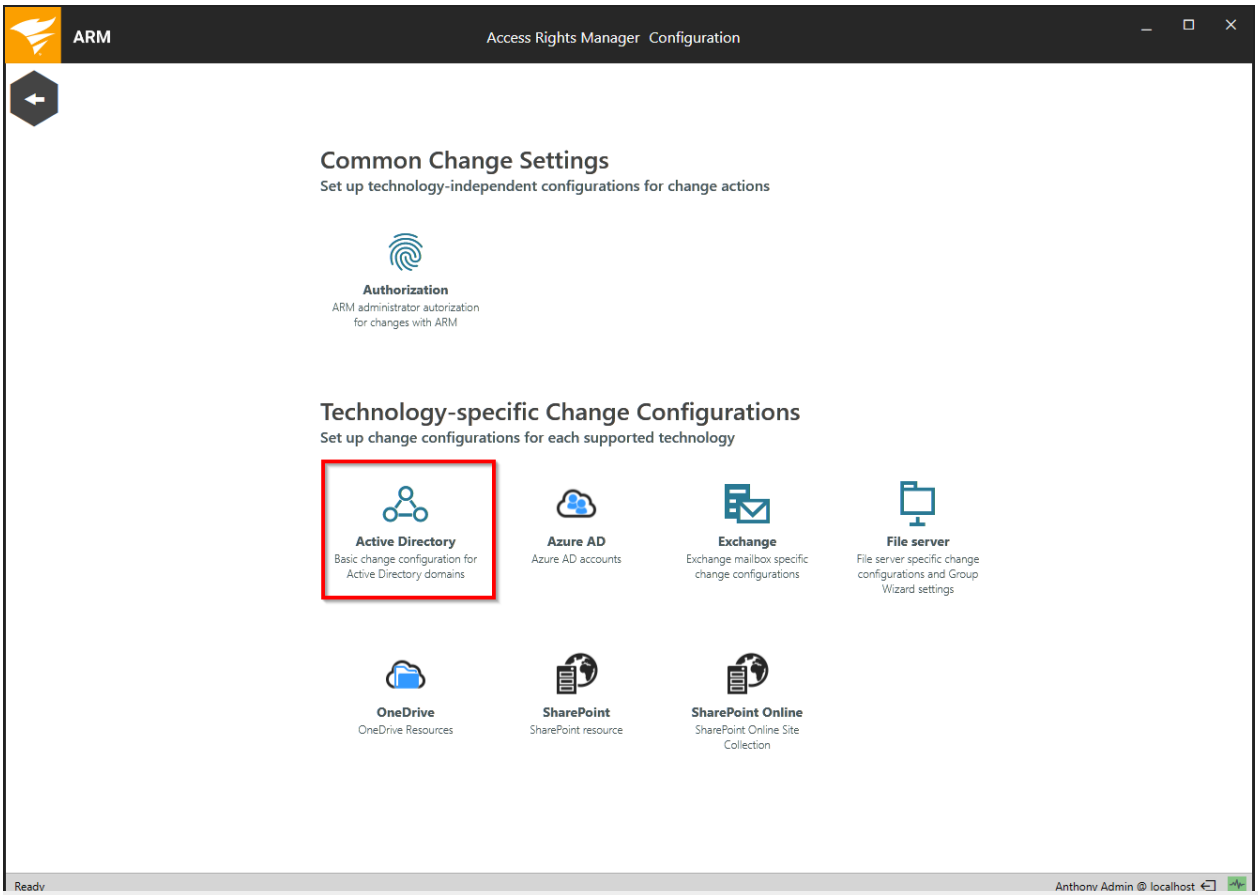
Change configuration



Click on "Change configuration".

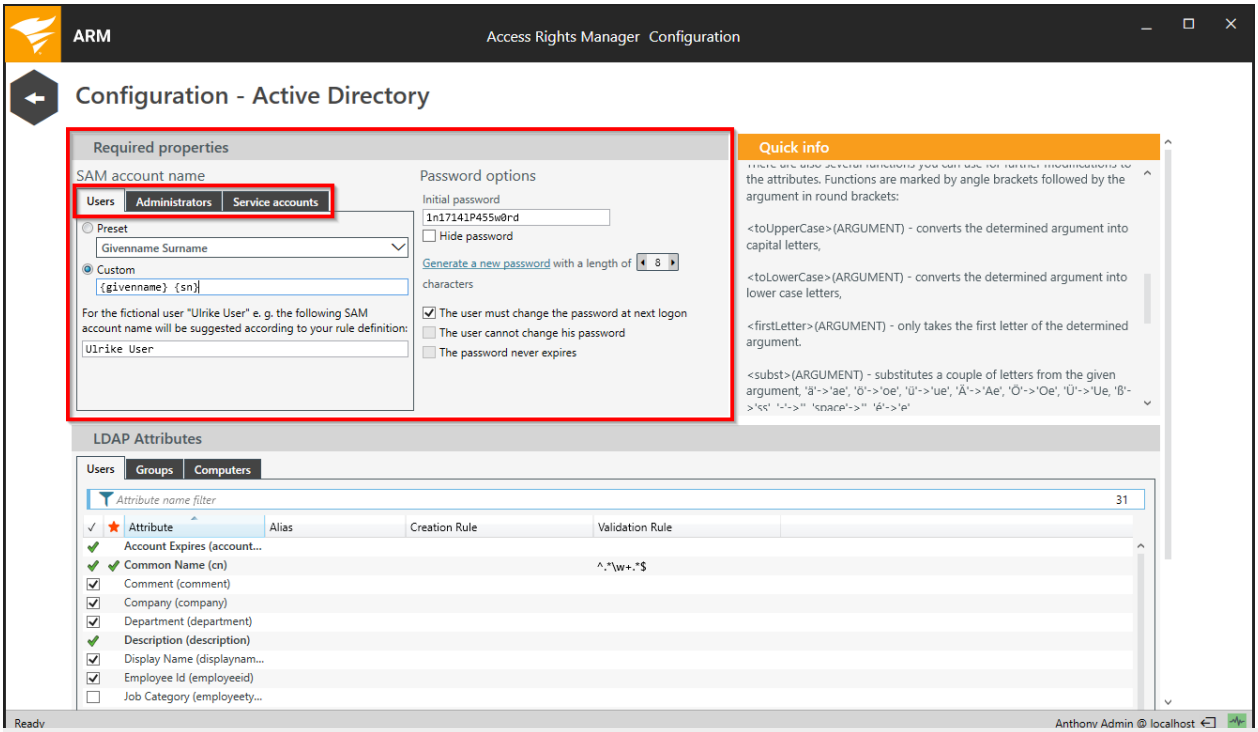
If you are using the ARM Audit Edition (or legacy 8MAN Visor) the chapter "Change configuration" is not relevant.

Customize the Active Directory (AD) change configuration



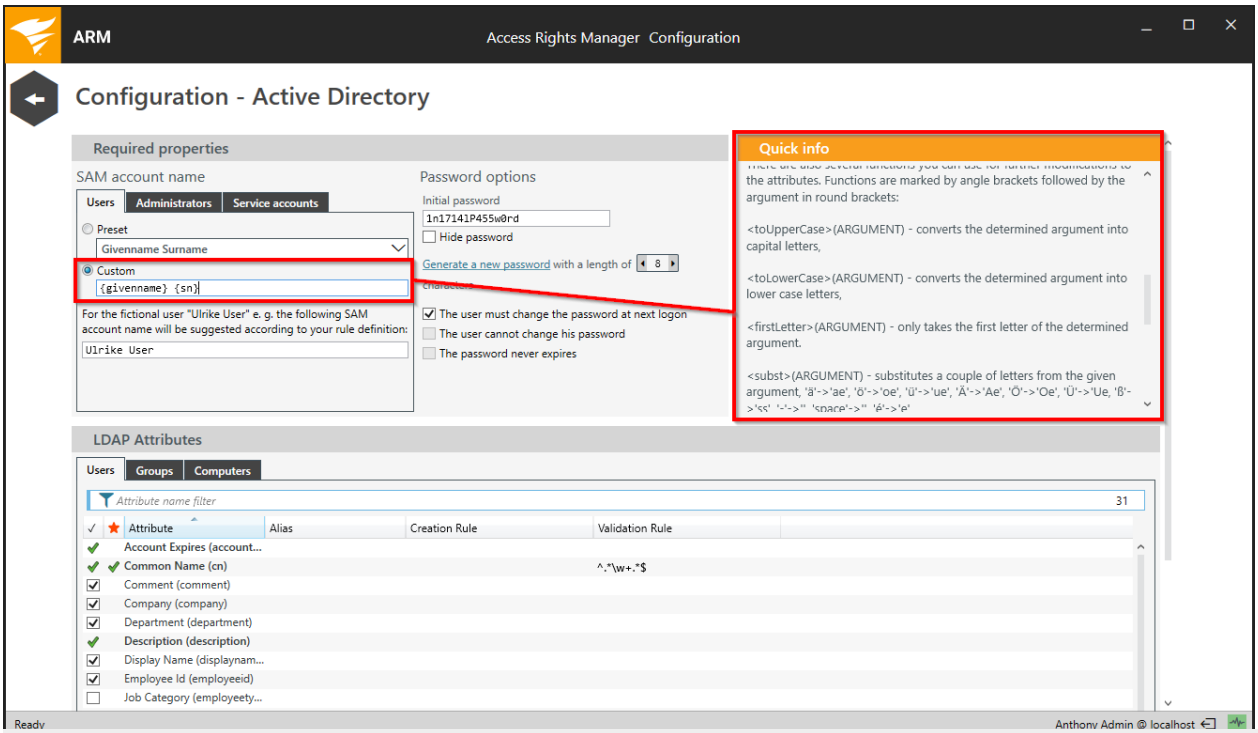
Click on "Active Directory".

Configuring new user default settings



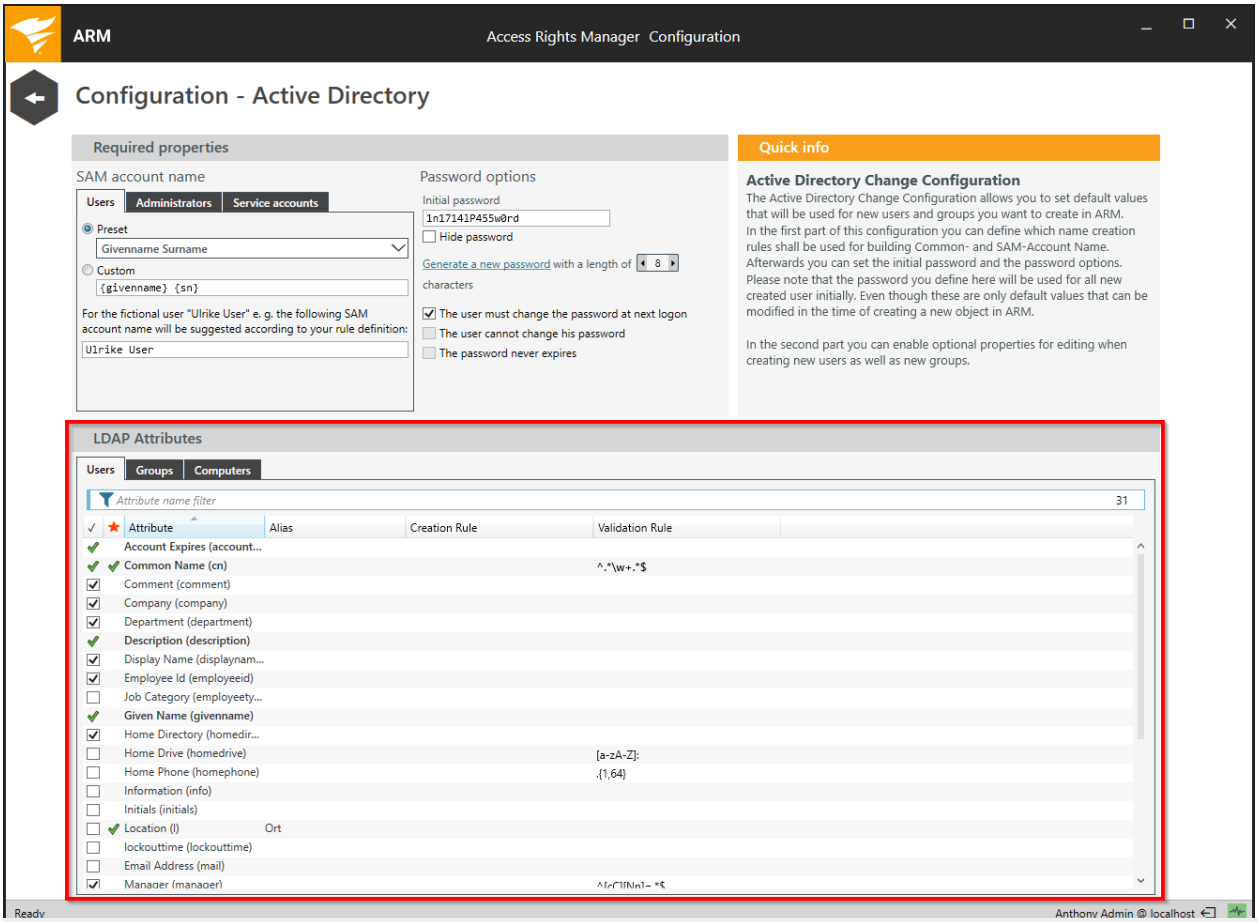
You can determine default settings that are applied to newly created users in the ARM application.

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.



Different possibilities for naming rules are described in the "Quick info" section.

Select available LDAP attributes



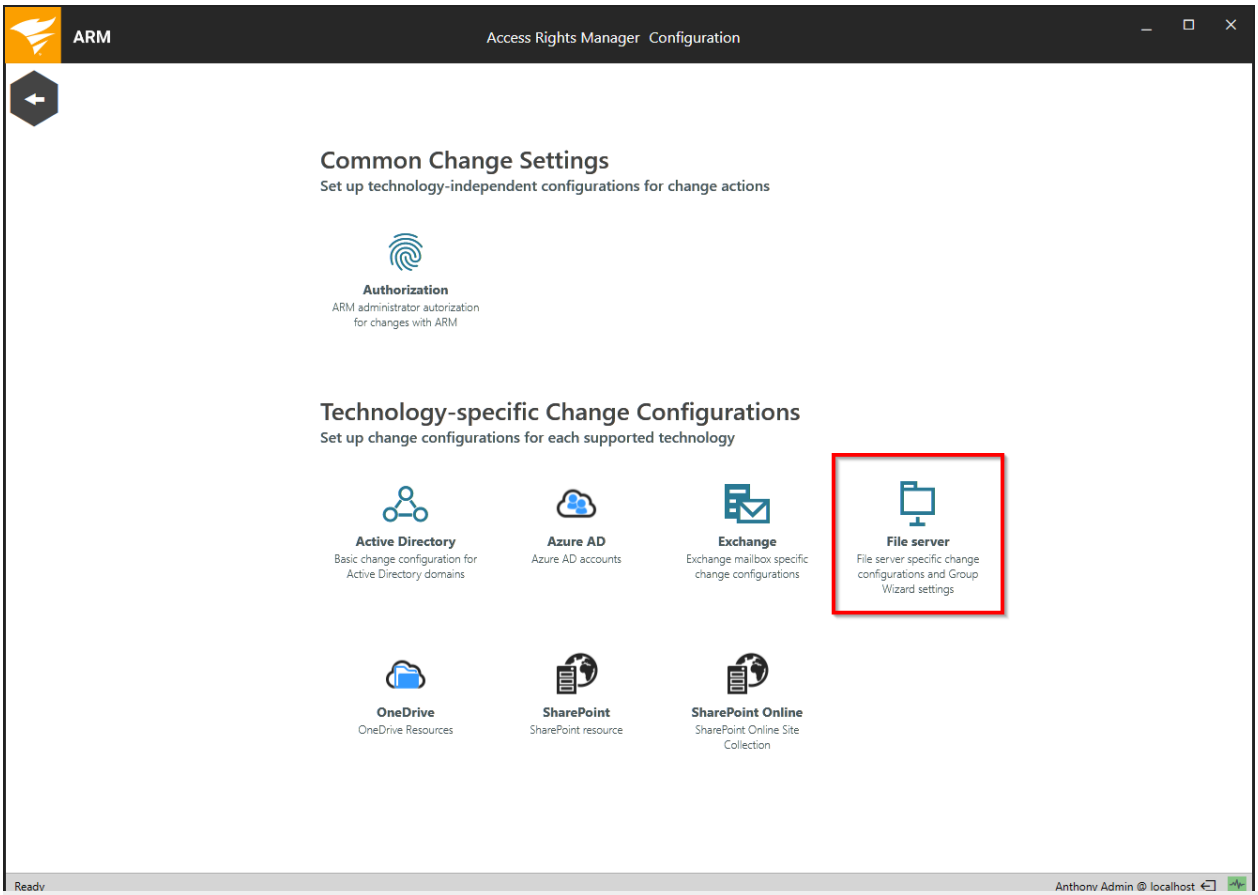
You can select which LDAP attributes are available in the ARM application for the creation of new users and groups.

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.

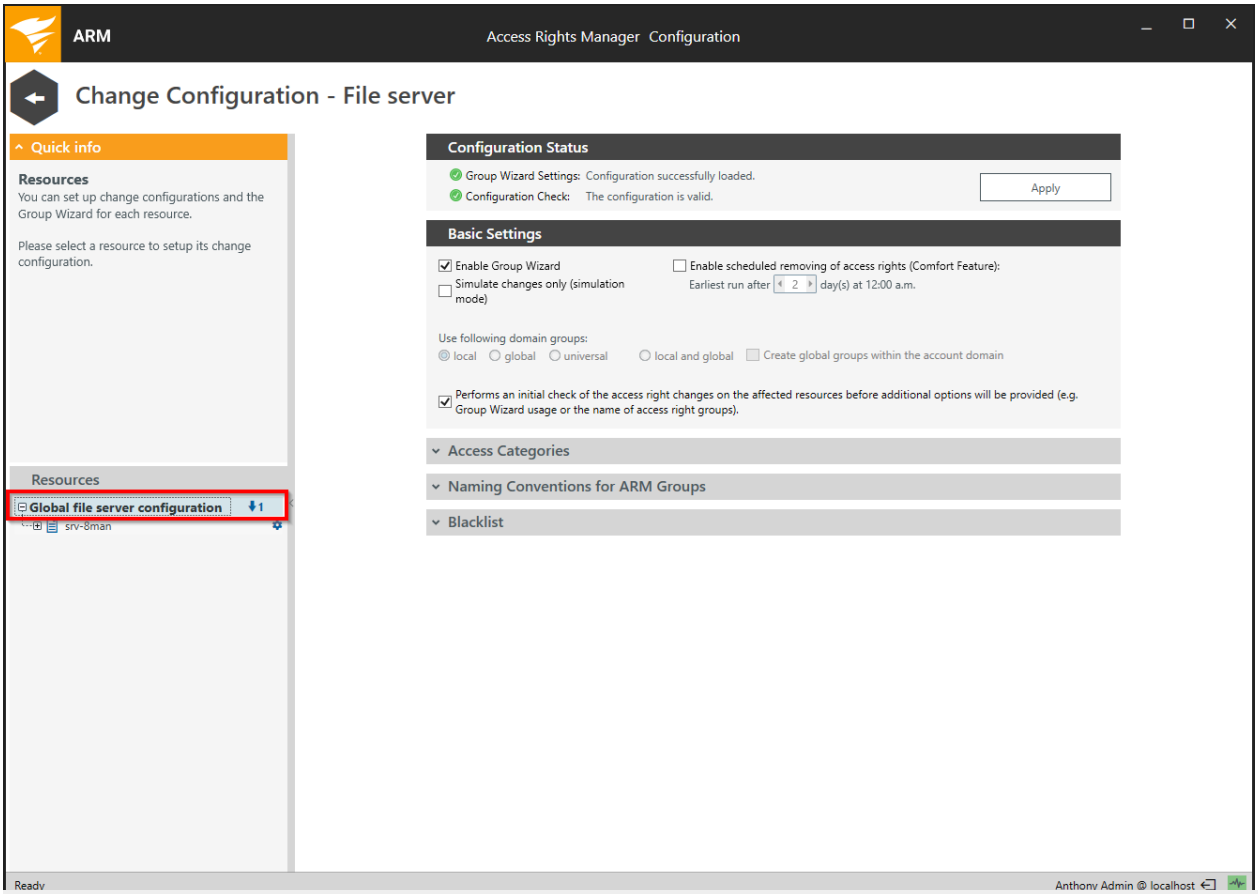
ARM reads and displays a standard set of LDAP attributes. If you would like to use additional attributes, please refer to load additional LDAP attributes and customize LDAP attributes properties.

File Server (FS) change configuration



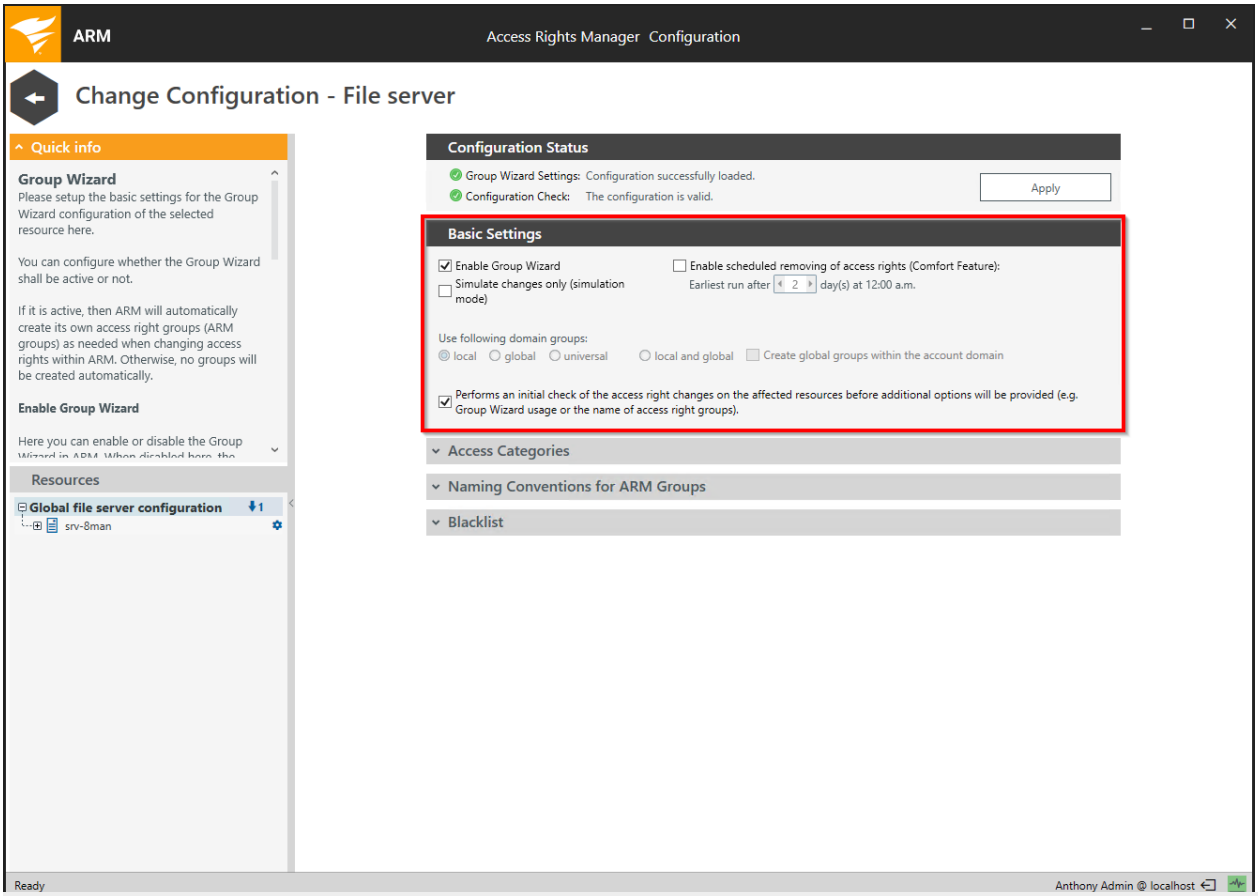
Click on "File server".

Manage global settings for FS changes



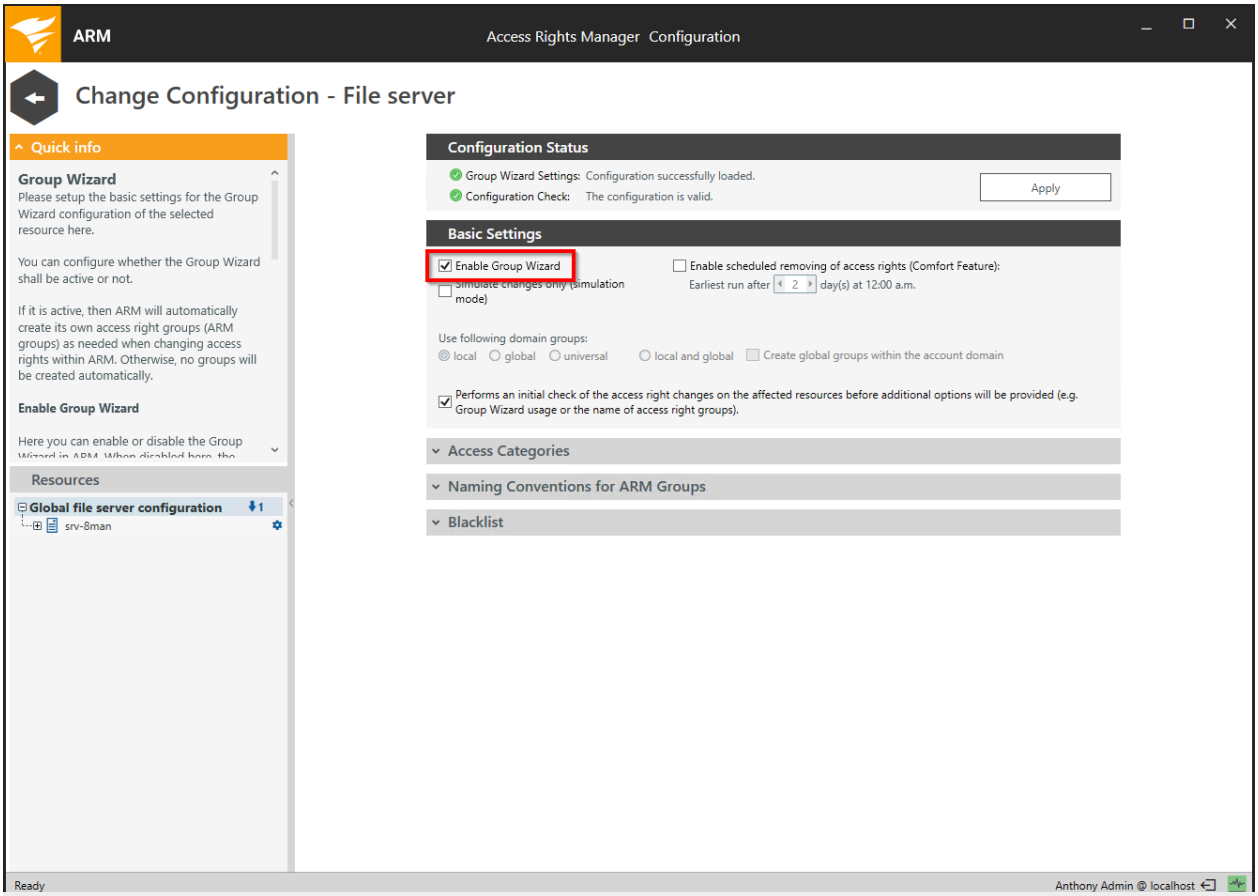
Click "Global file server configuration" in the "Resources" section.

Basic settings



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.

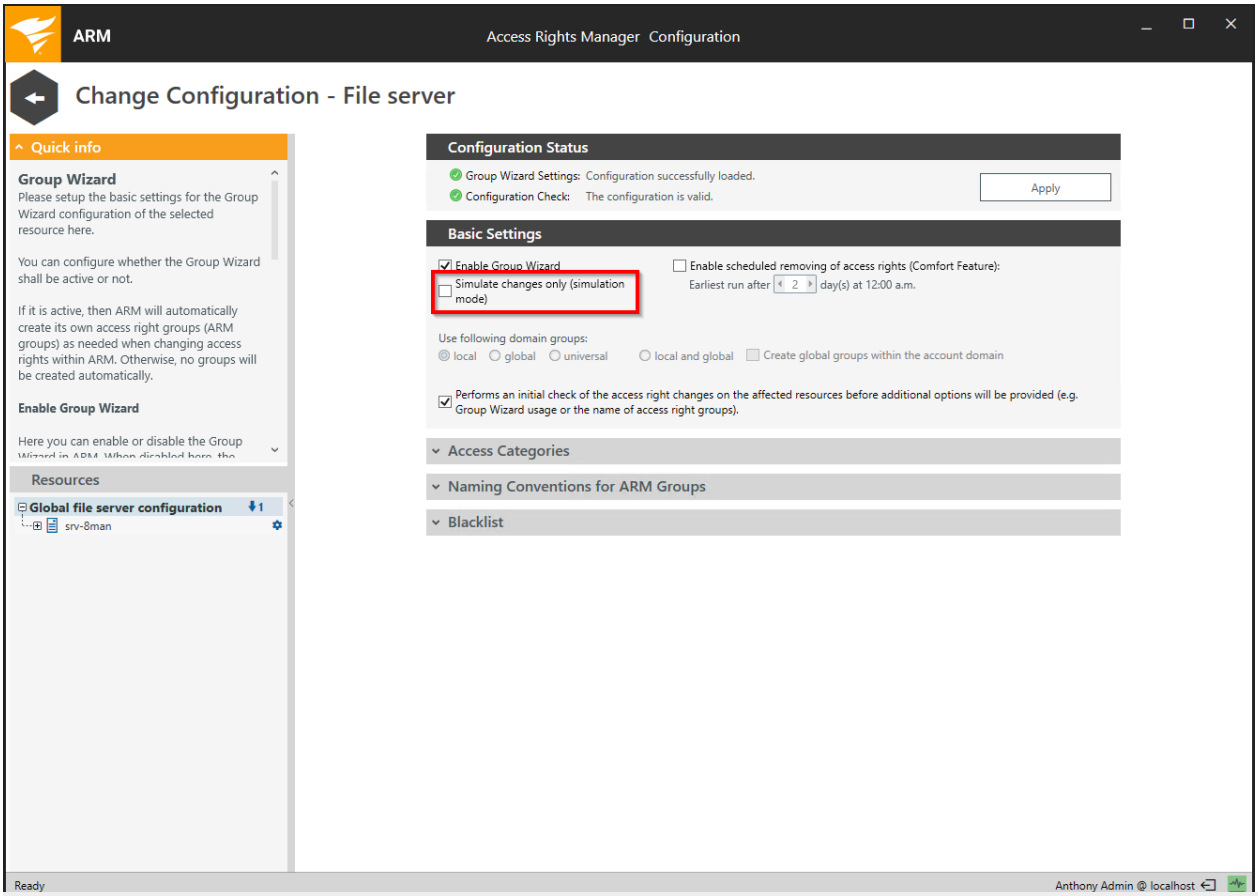
Option disabled

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.

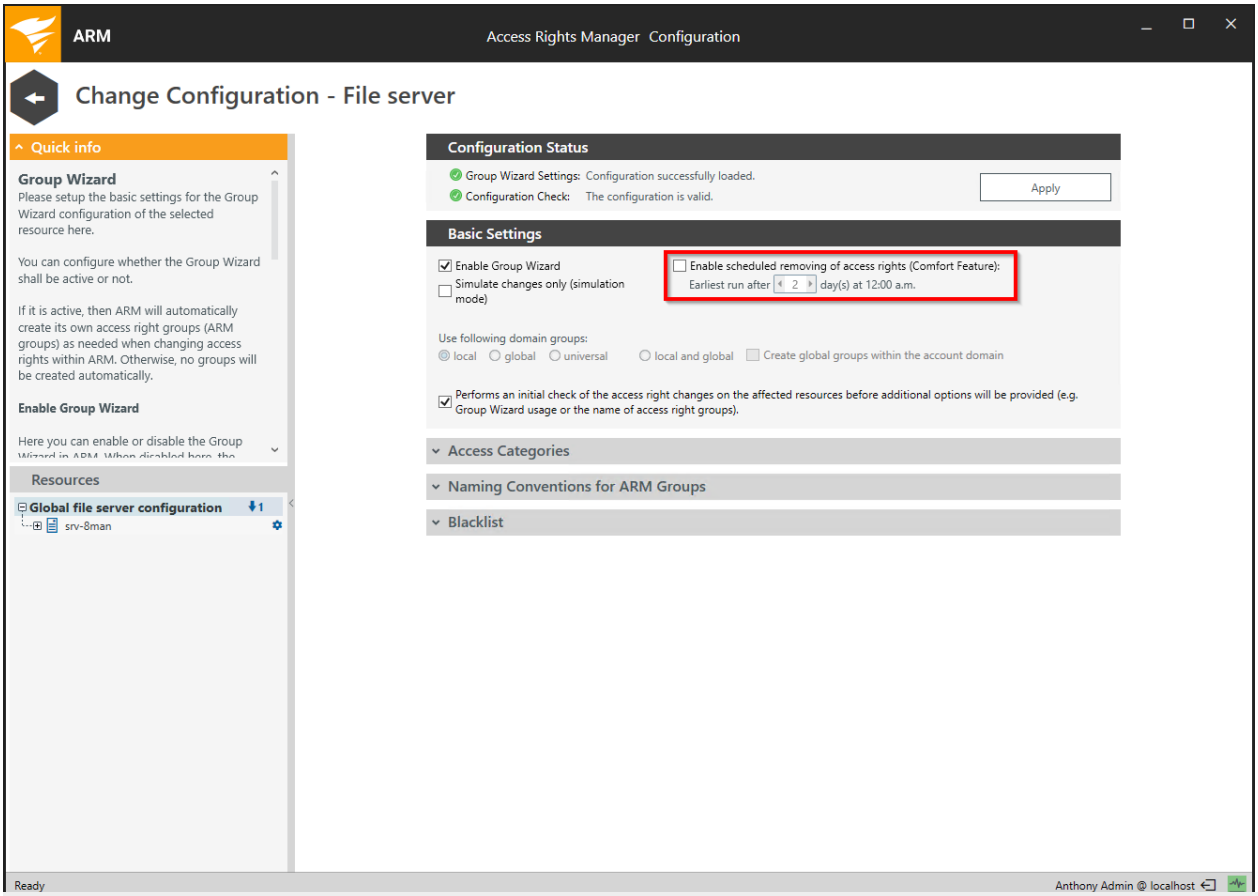
Use the simulation mode



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

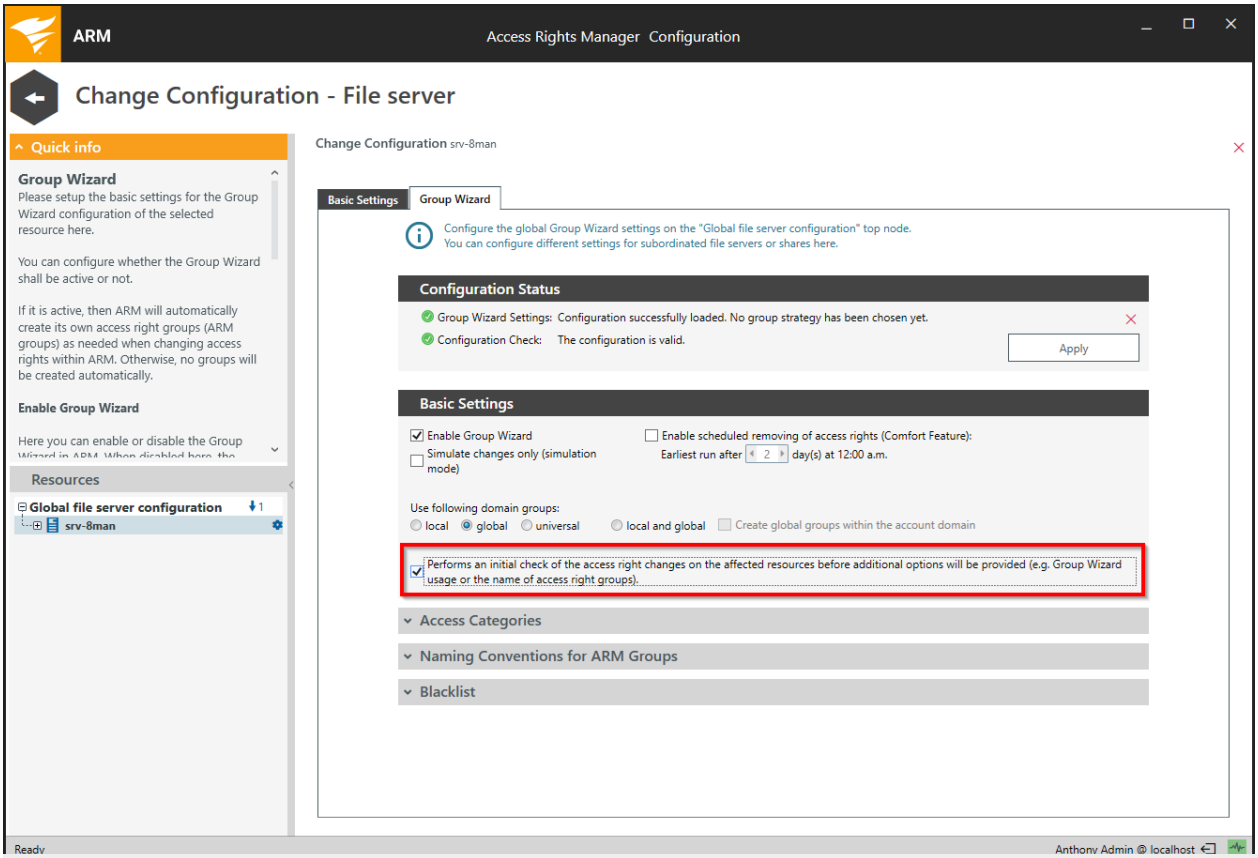


When users register on the network, their group memberships are verified and added to the Kerberos token. When assigning permissions with the Group Wizard via group memberships, they only become active after the user logs out of and into the system again.

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.

ARM does not set temporary list permissions. Users may not be able to navigate to the folders.

Activate or deactivate an initial test



Option enabled

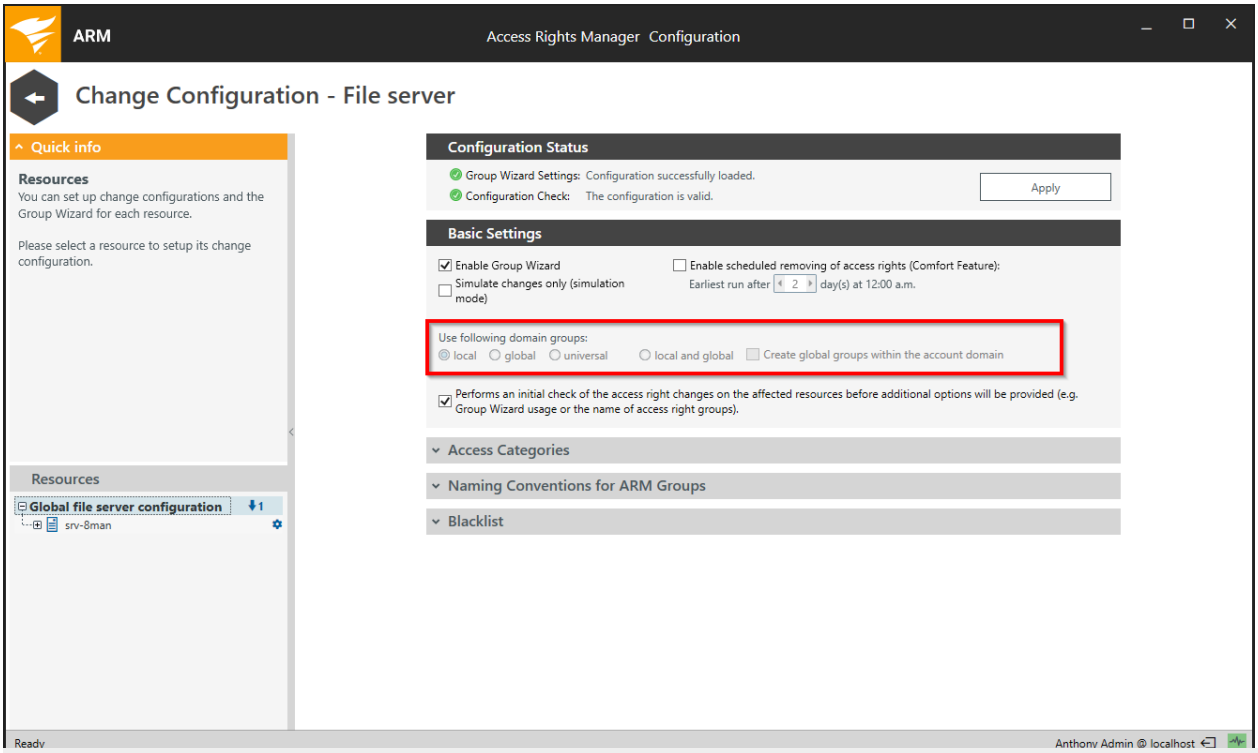
The Group Wizard will determine all required steps for access rights changes in the ARM application immediately after clicking on "Apply".

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!

More information regarding the use of AD groups can be found on the following pages and in the article Understanding Groups (© 2020 Microsoft, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd861330(v=ws.11), obtained an January 30, 2020).

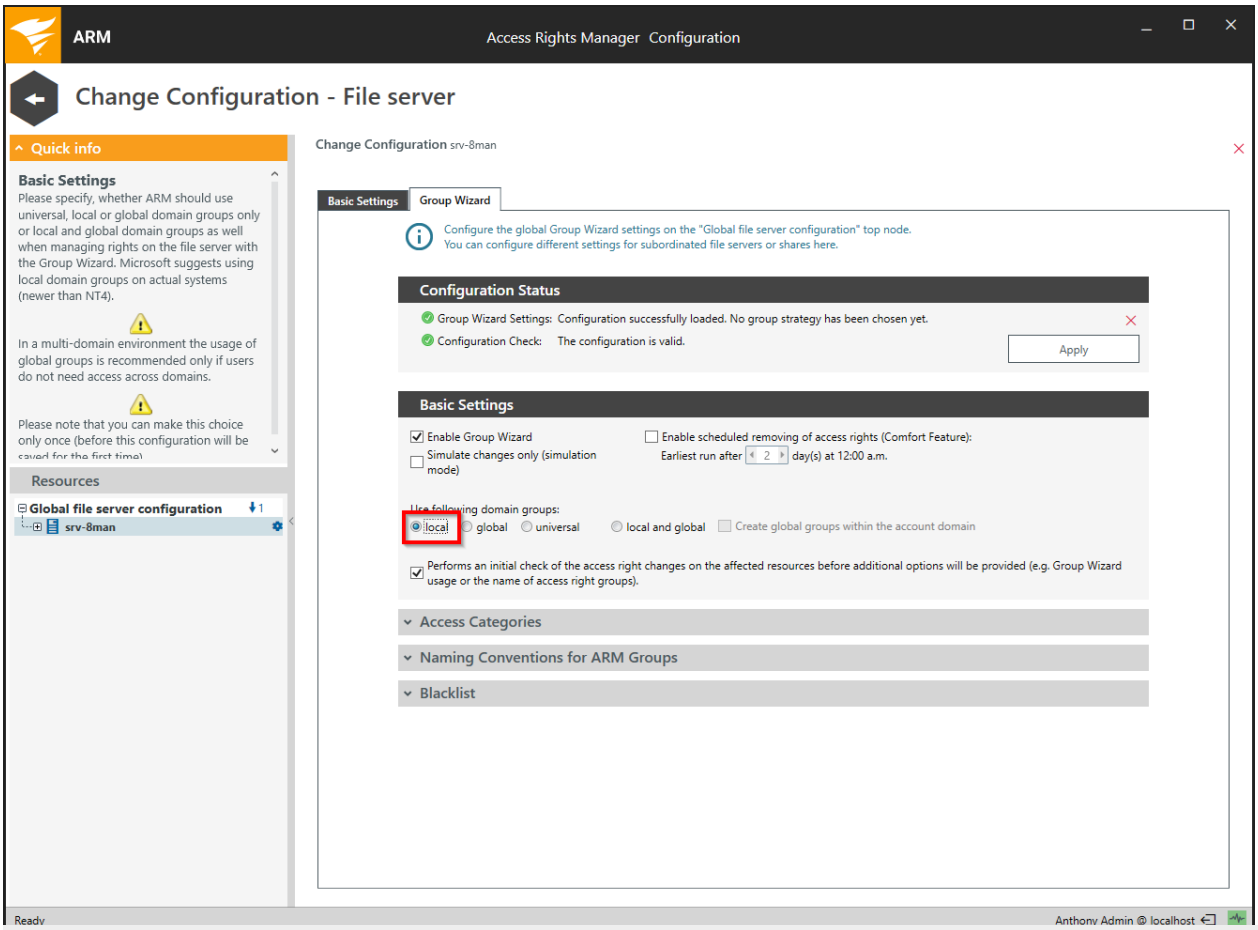
Use local AD groups

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	DISADVANTAGES
Users and groups from other domains or forests can be a member of a local AD group and thereby be assigned permissions.	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.

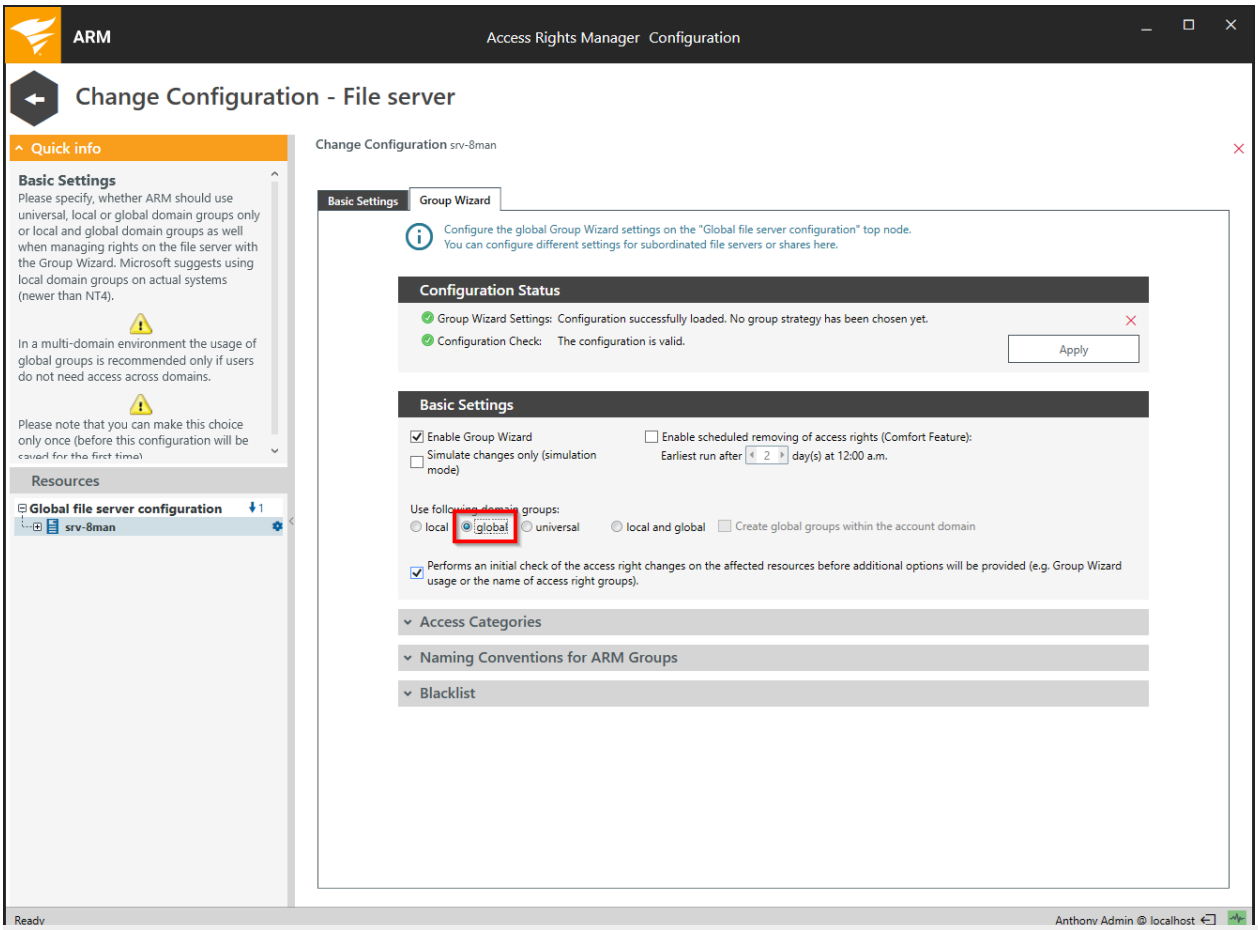
Use global AD groups

A -> G-> P

A - account (user account)

G - global group (global AD-group)

P - permission



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	DISADVANTAGES
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.	Only users and groups of the corresponding domain can be members of global AD-groups. Therefore, this approach is unsuitable for multi-domain environments.

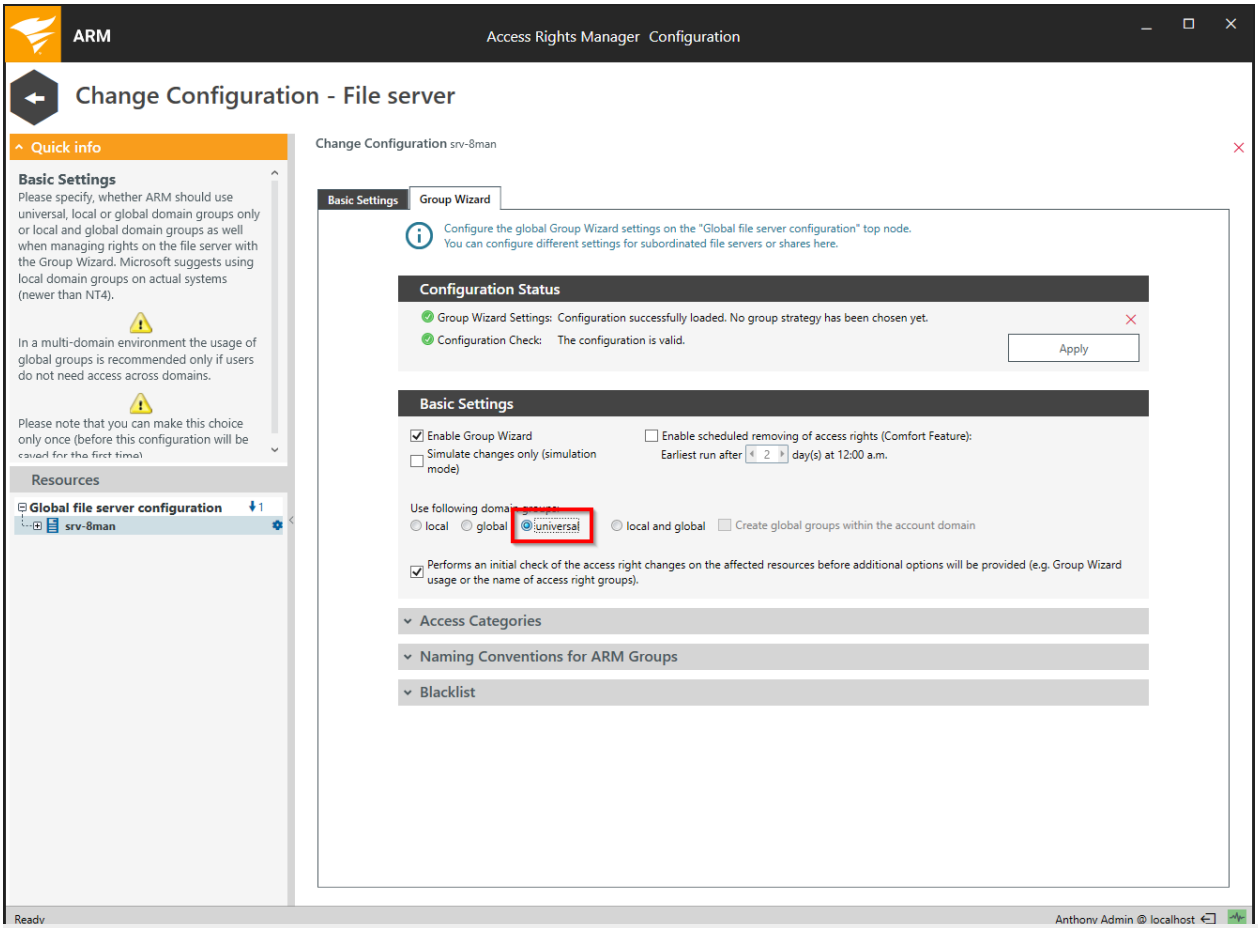
Use universal AD groups

A -> U -> P

A - account (user-account)

U - universal group (universal AD-group)

P - permission



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	DISADVANTAGES
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.	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

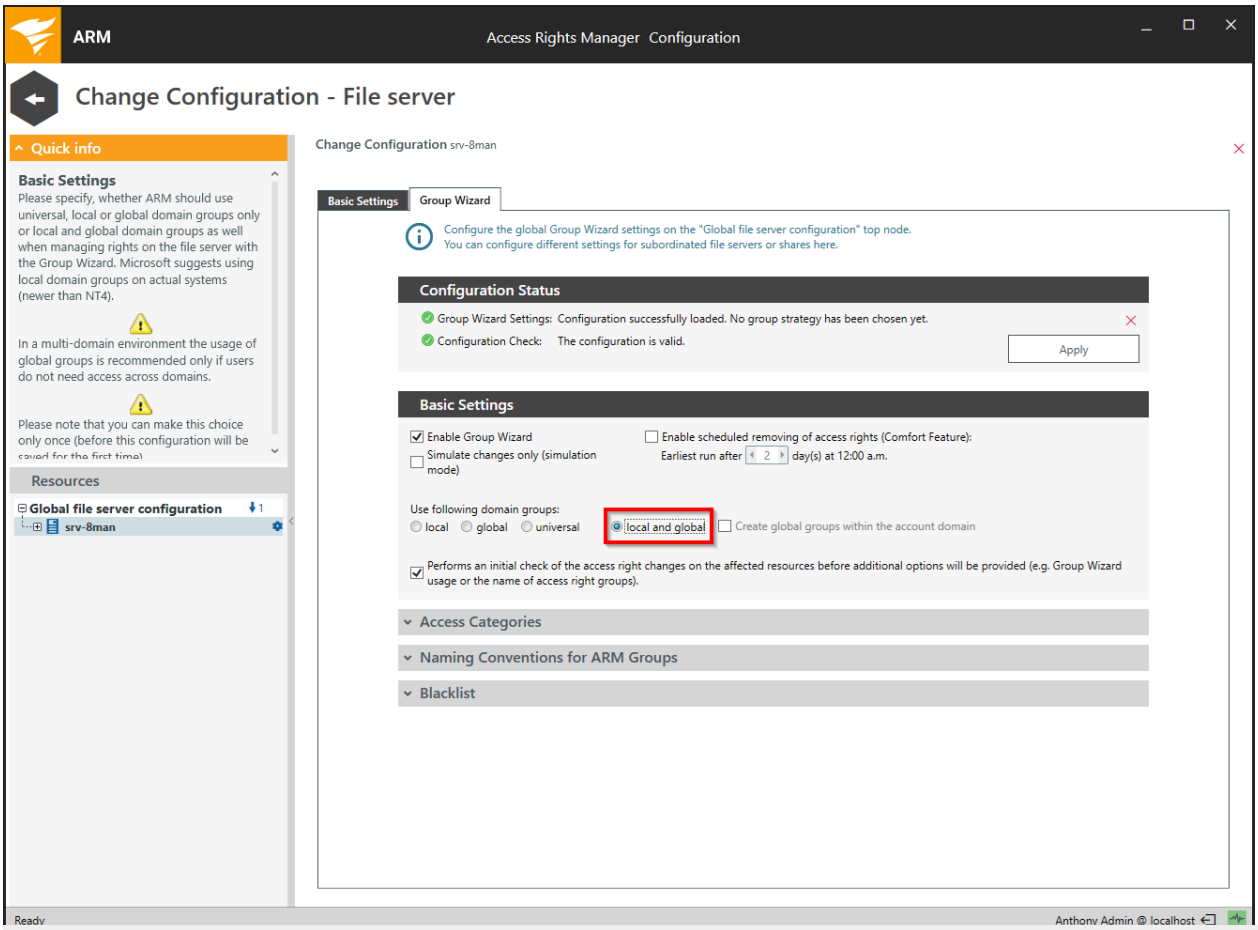
A - account (user-account)

G - global group (global AD-group)

DL - domain local group (local AD-group)

P - permission

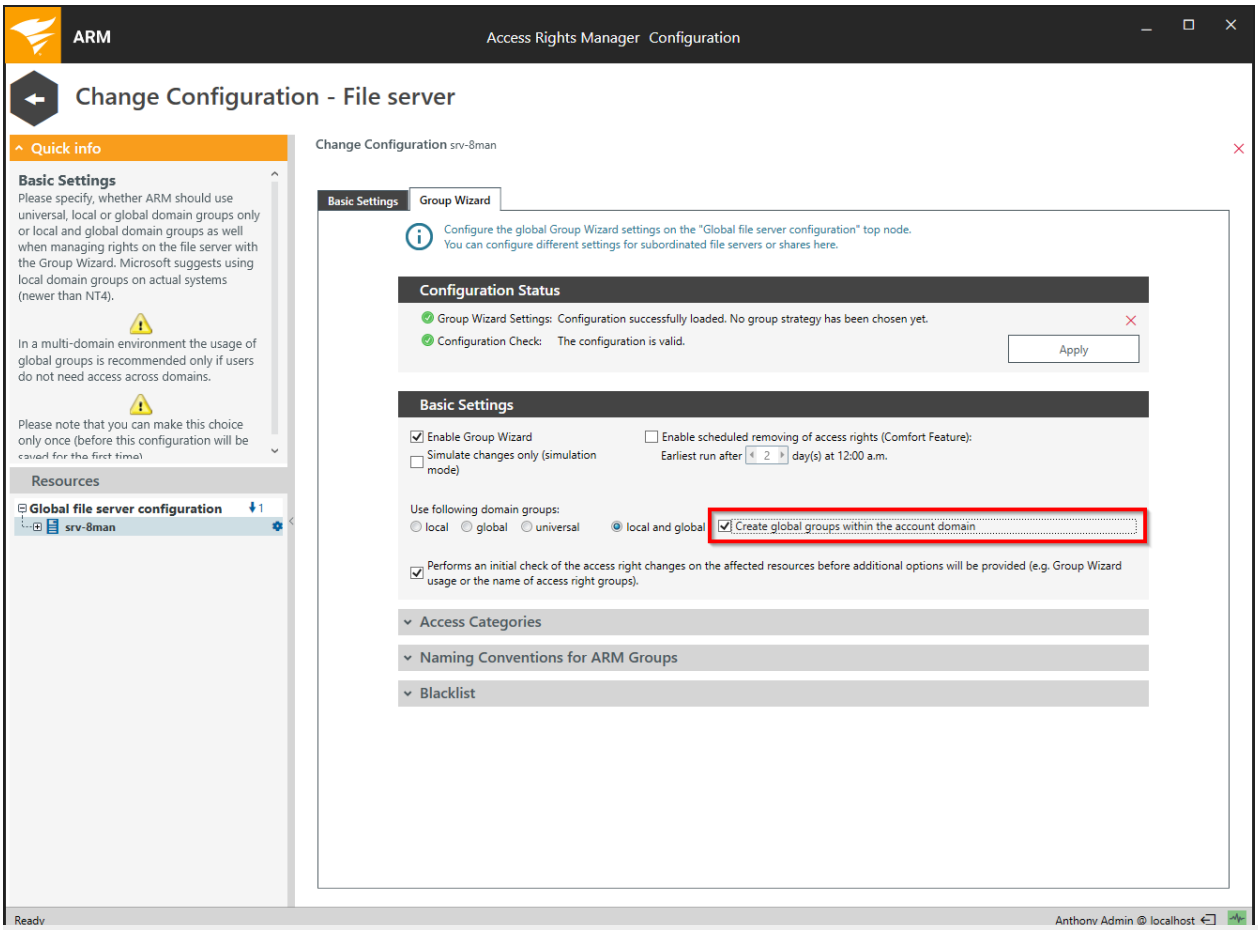
Consider all groups created by the group wizard as file server resource groups. You should not use these groups for other purposes (for example: VPN access).



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".



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.

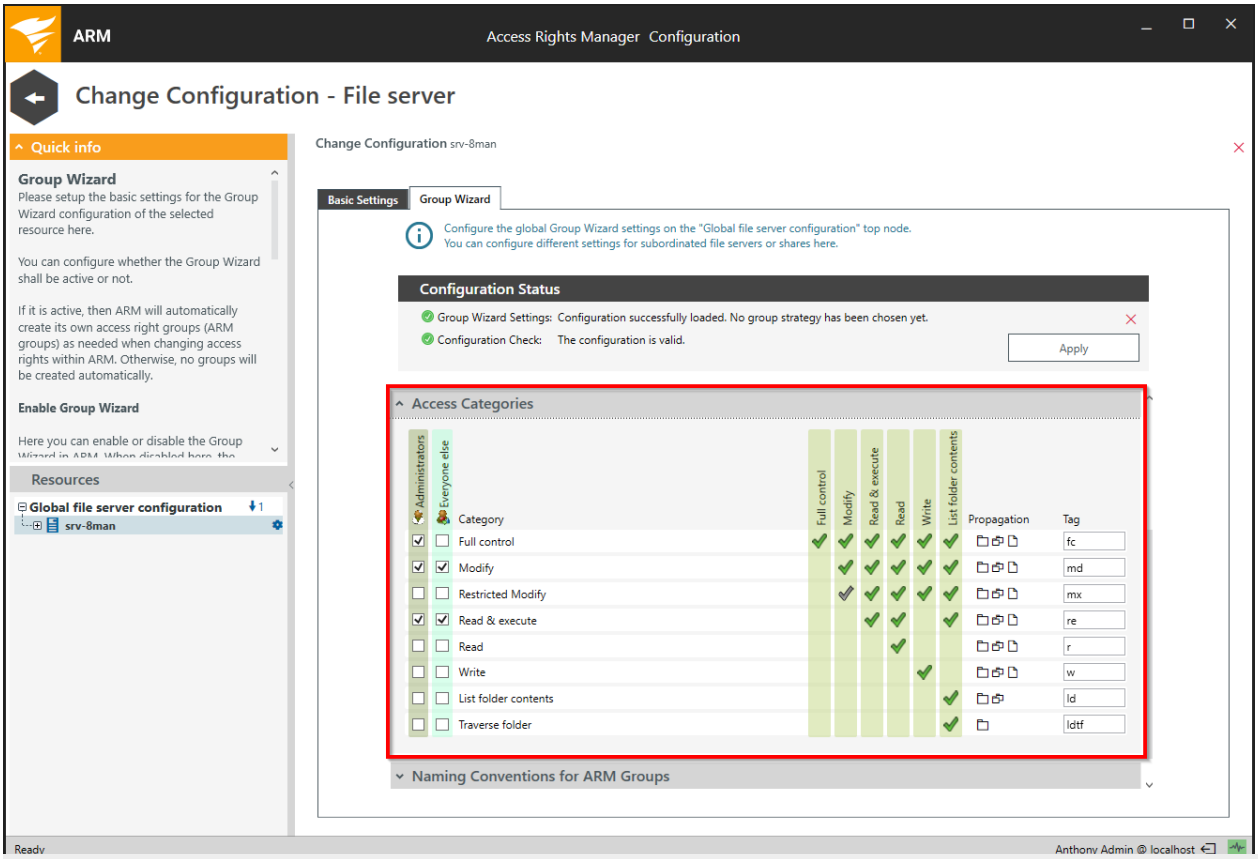
Option disabled

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	DISADVANTAGES
The A-G-DL-P-principle ensures a variety of different options and approaches in multi-domain and multi-forest environments.	Users require two or more group memberships for their permissions. Therefore this approach may lead to issues with token size.

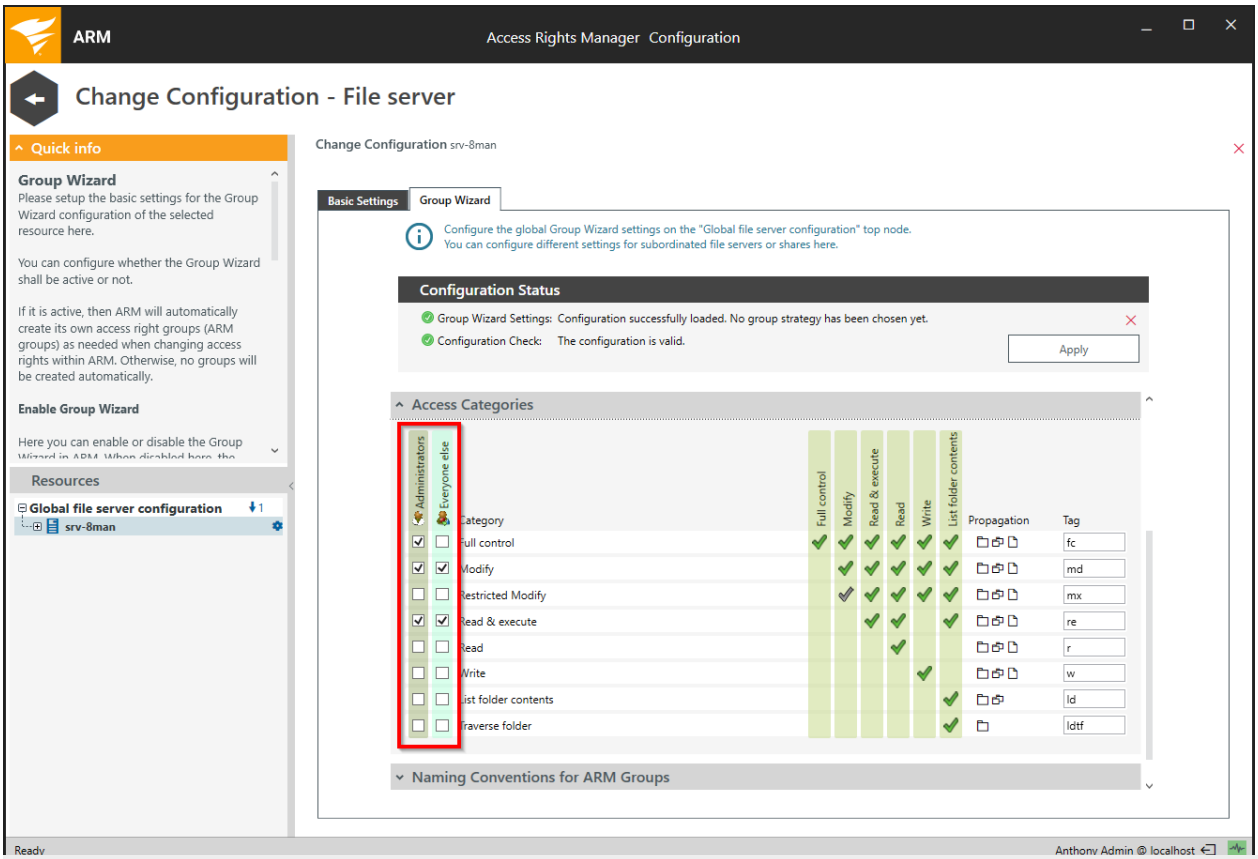
Select access categories available in ARM

ARM bundles the Microsoft permission combinations into access categories. This allows for a simplification of access rights assignment.



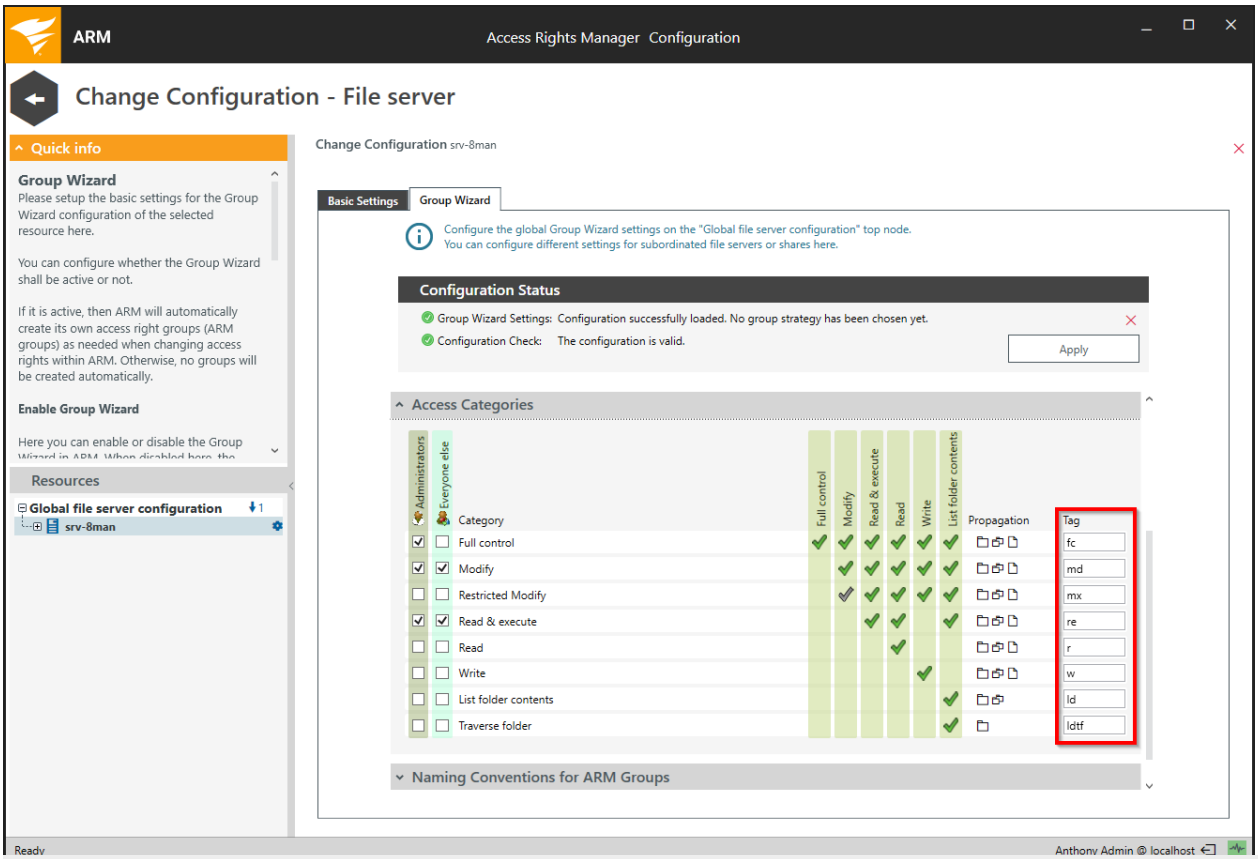
Select the access category that you would like to make available in ARM.

Selected access categories will then be visible as columns in the ARM application.



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.

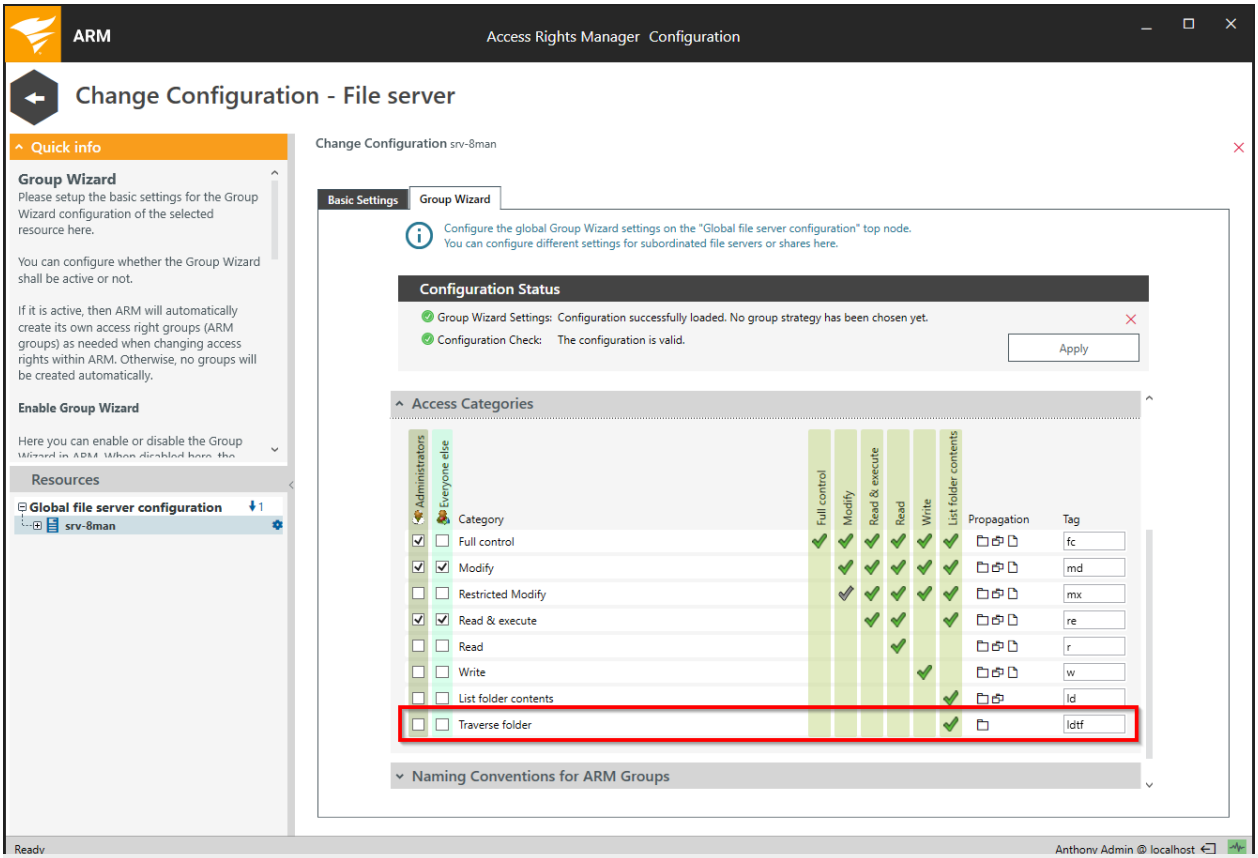


Determine the abbreviations for the individual access categories. The abbreviations can also be used for the naming convention of ARM-groups.

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)

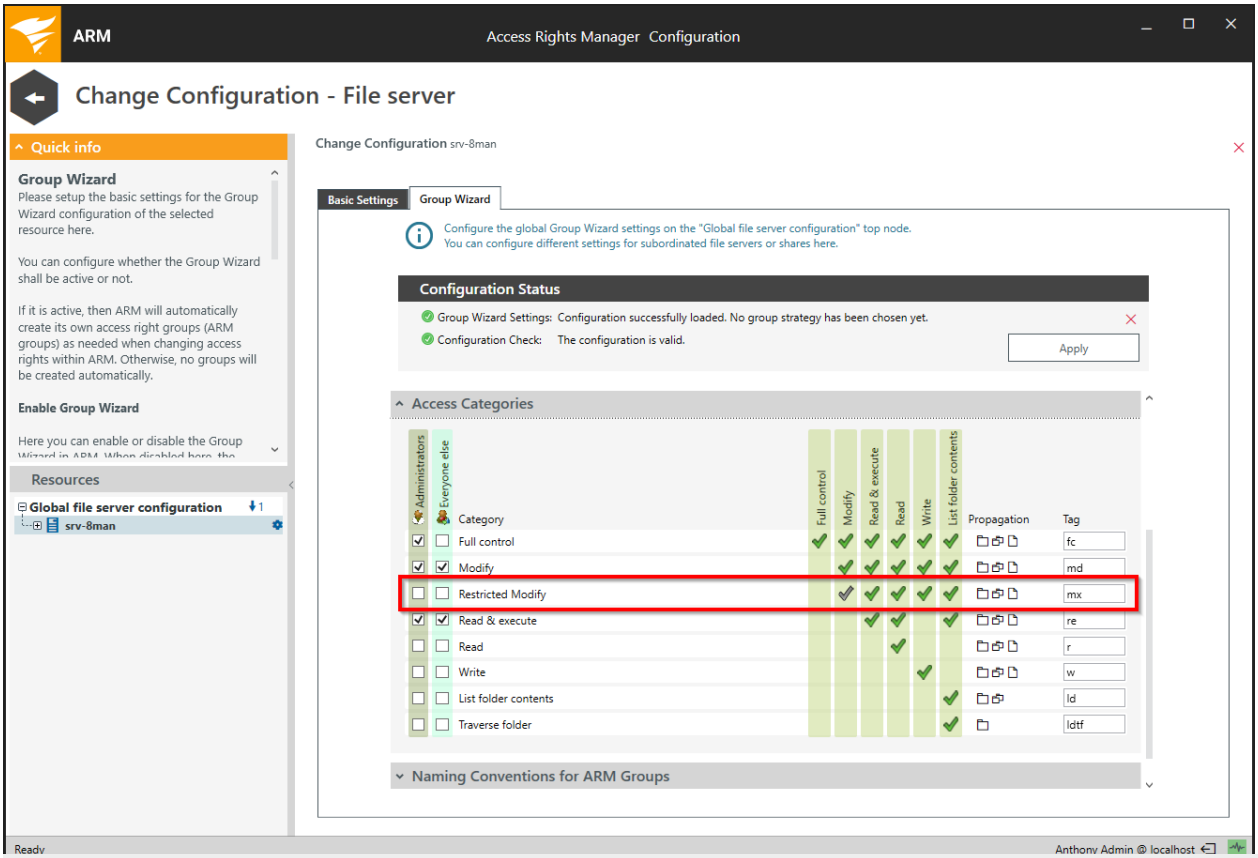
Traverse folder



"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).

This access category is not visible to users if ARM manages list rights automatically.

Restricted modify

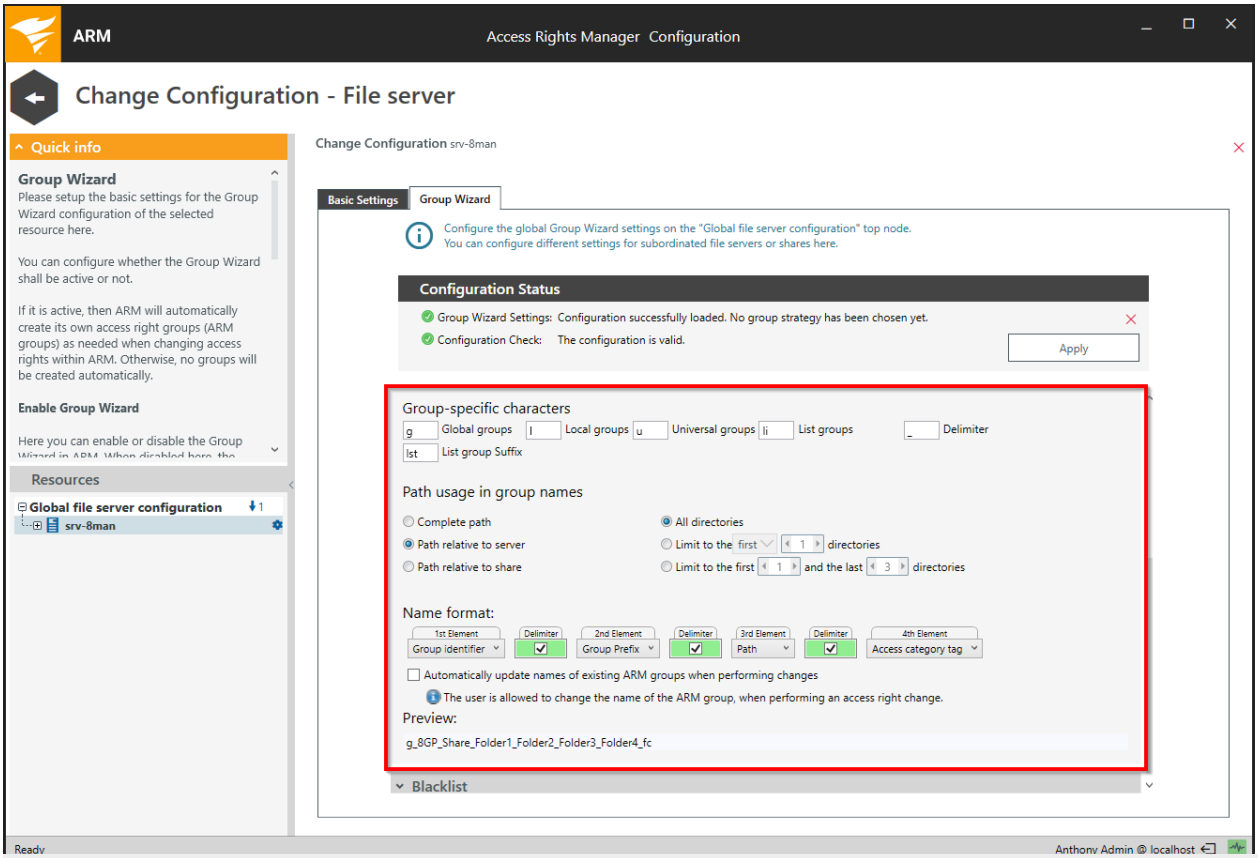


Restricted modify is a special combination of permissions where users have modify rights to folders and sub-folders but are not able to delete this folder (keep it as parent for inheritance).

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

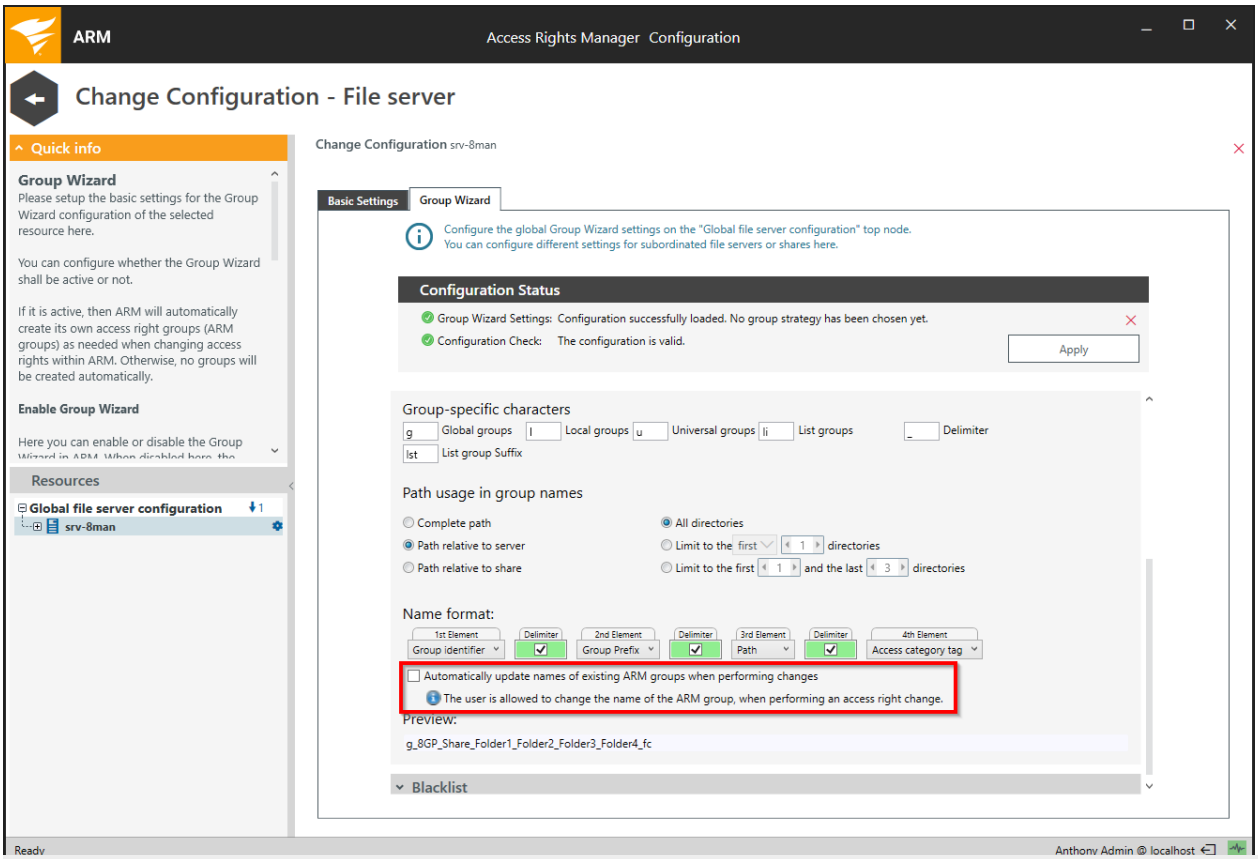


Determine how names of ARM groups are build.

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).

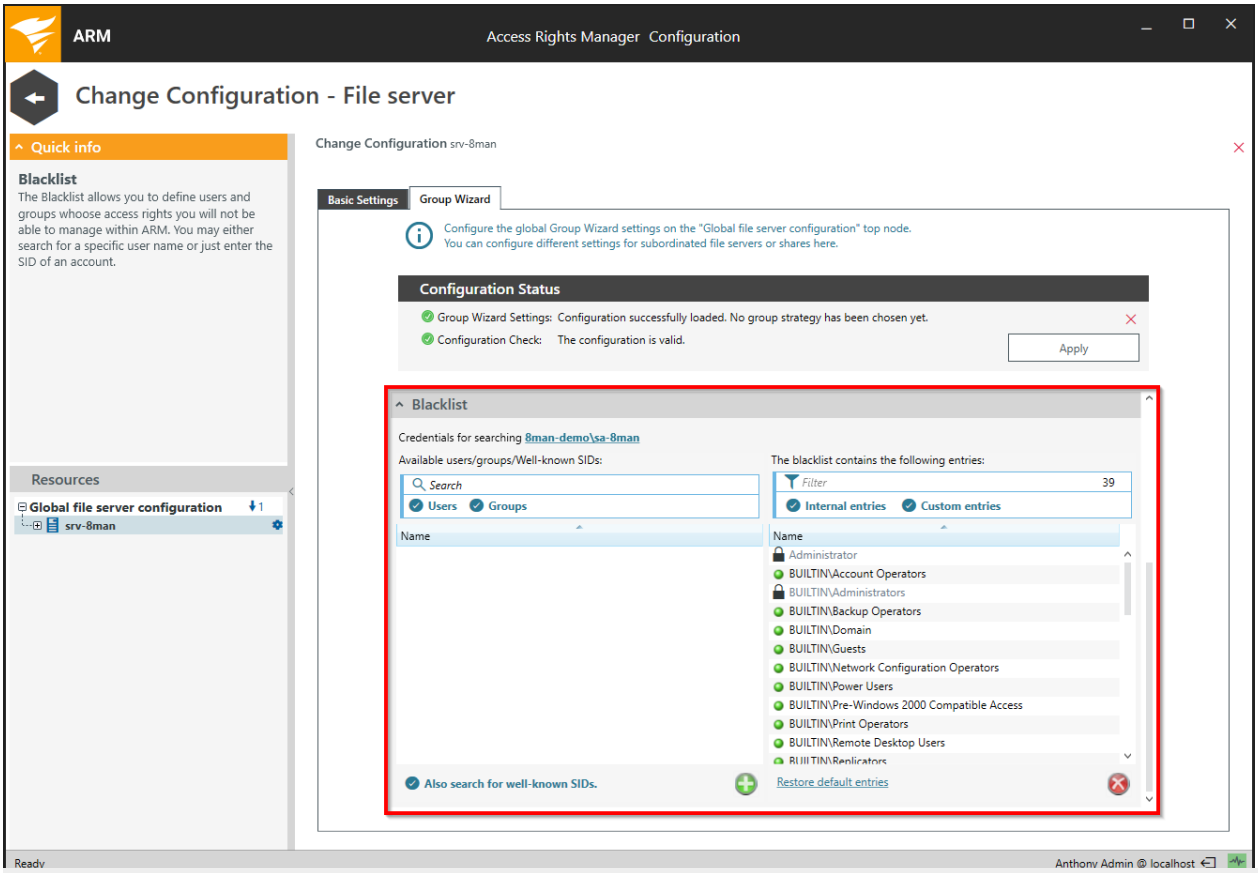
Users are not able to change the name of the ARM-group in the ARM application.

Option disabled

When changing folder names, ARM-groups are not automatically renamed.

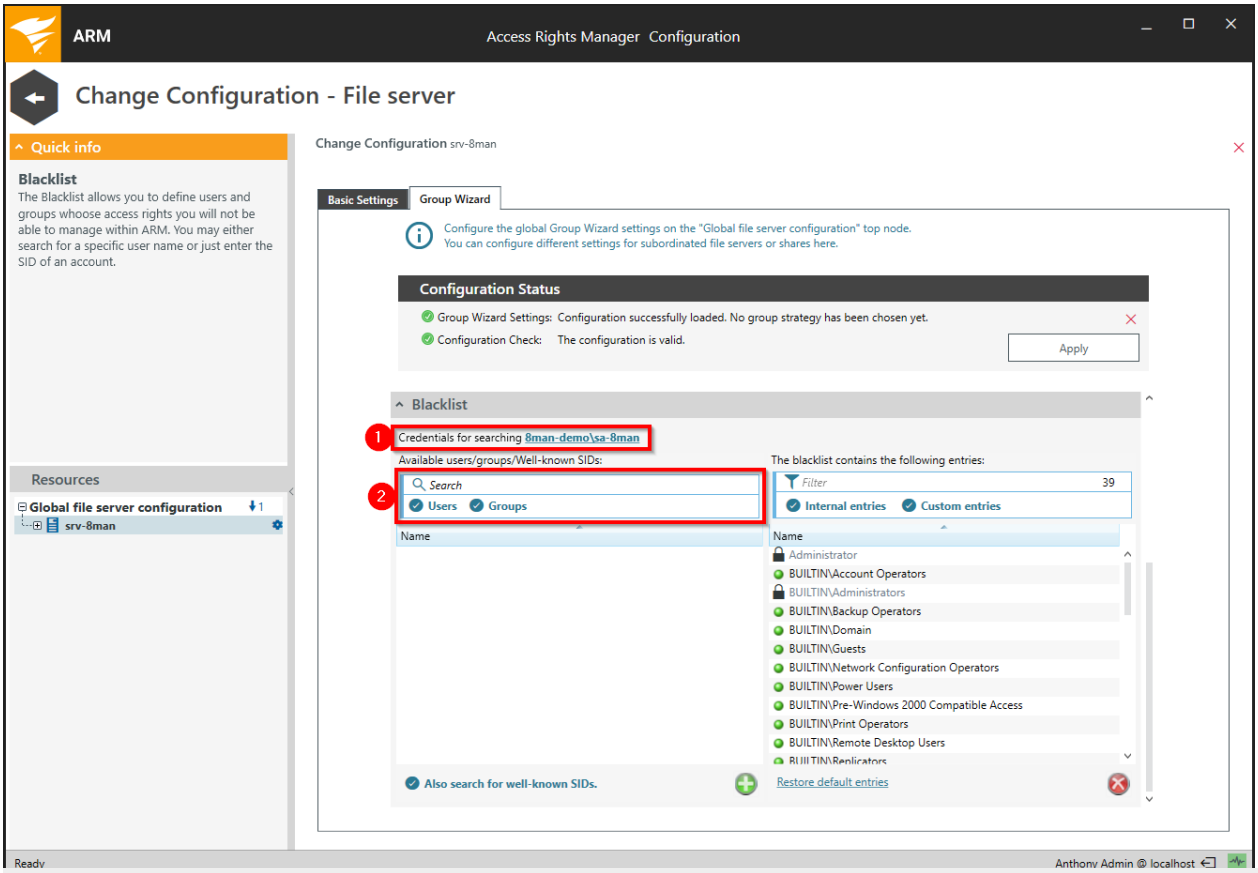
Users are able to change the name of the ARM-group in the ARM application.

Blacklist - exclude users and groups from use



Determine which users and groups are excluded from usage within ARM for granting and removing access.

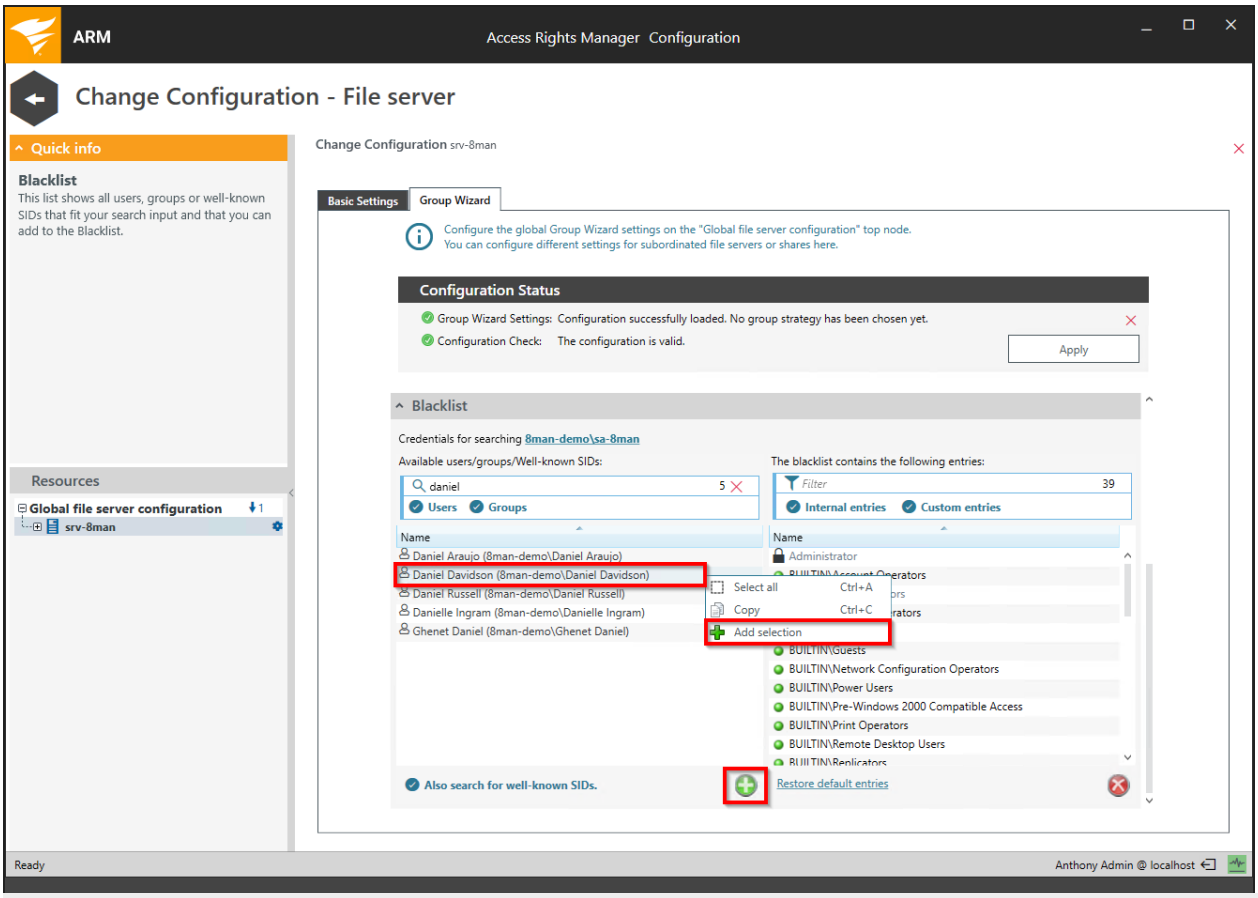
Add entries to the blacklist



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:

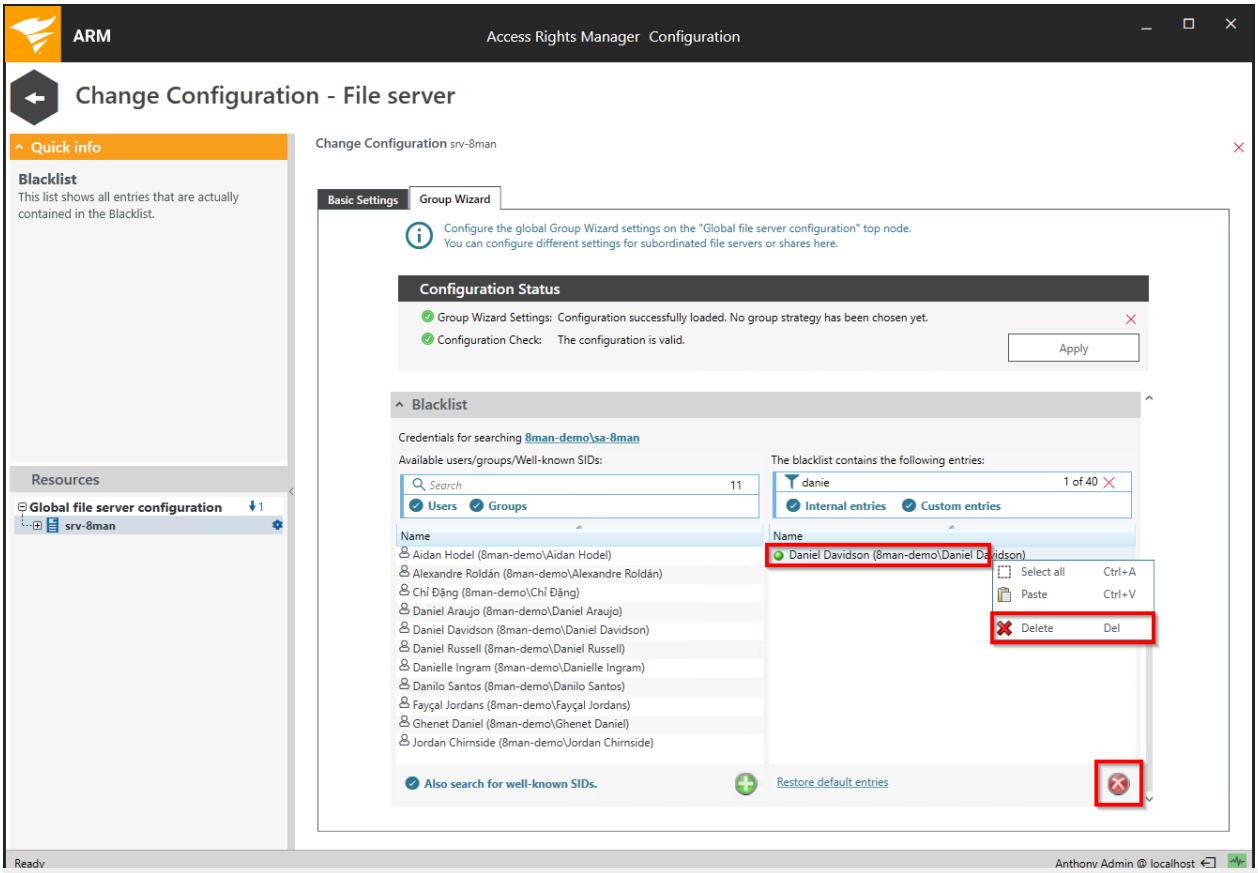
- If no domain is entered into the search field, the domain is selected based upon the credentials.
- If a domain is entered (for example: domain2\another.user"), ARM will search that domain (domain2).



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

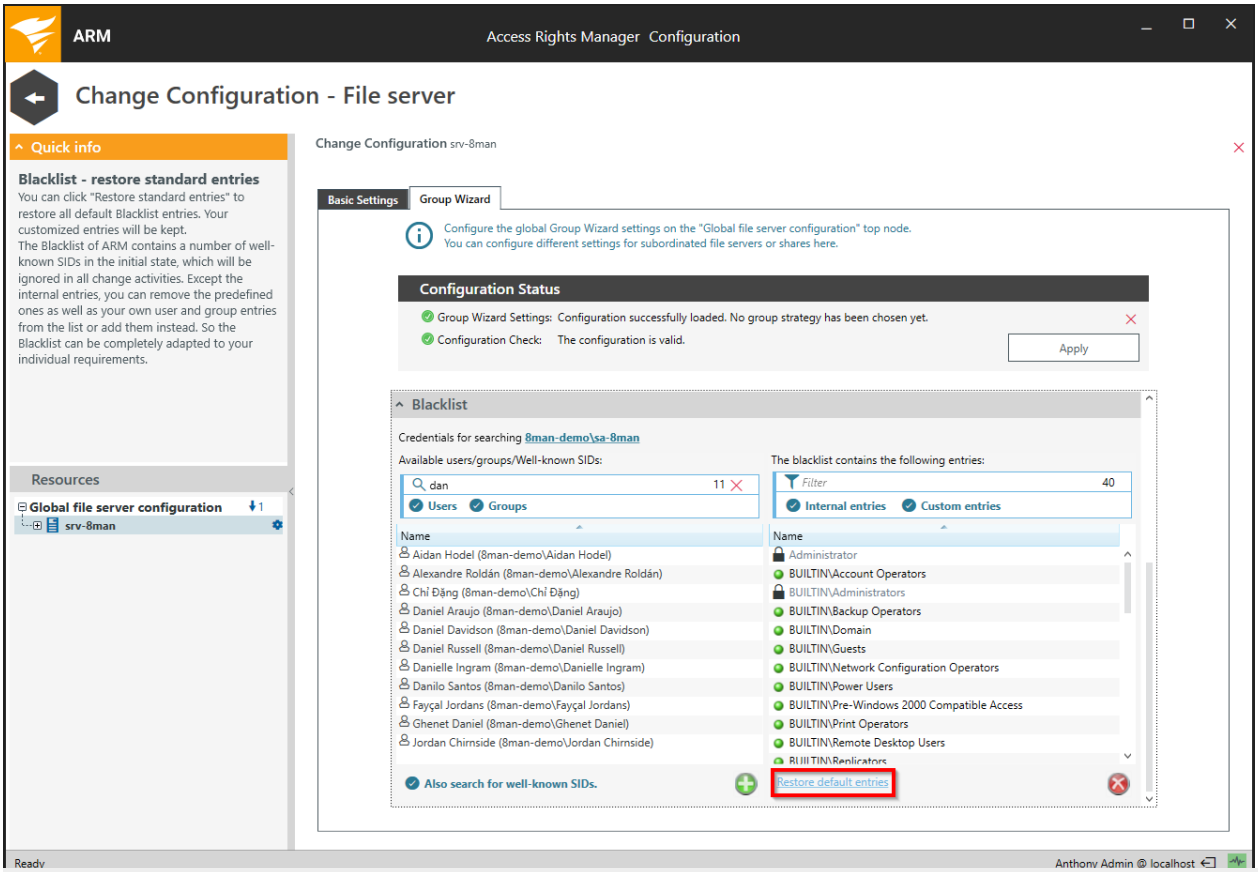


Filter the entries and remove the desired entry by

- 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.

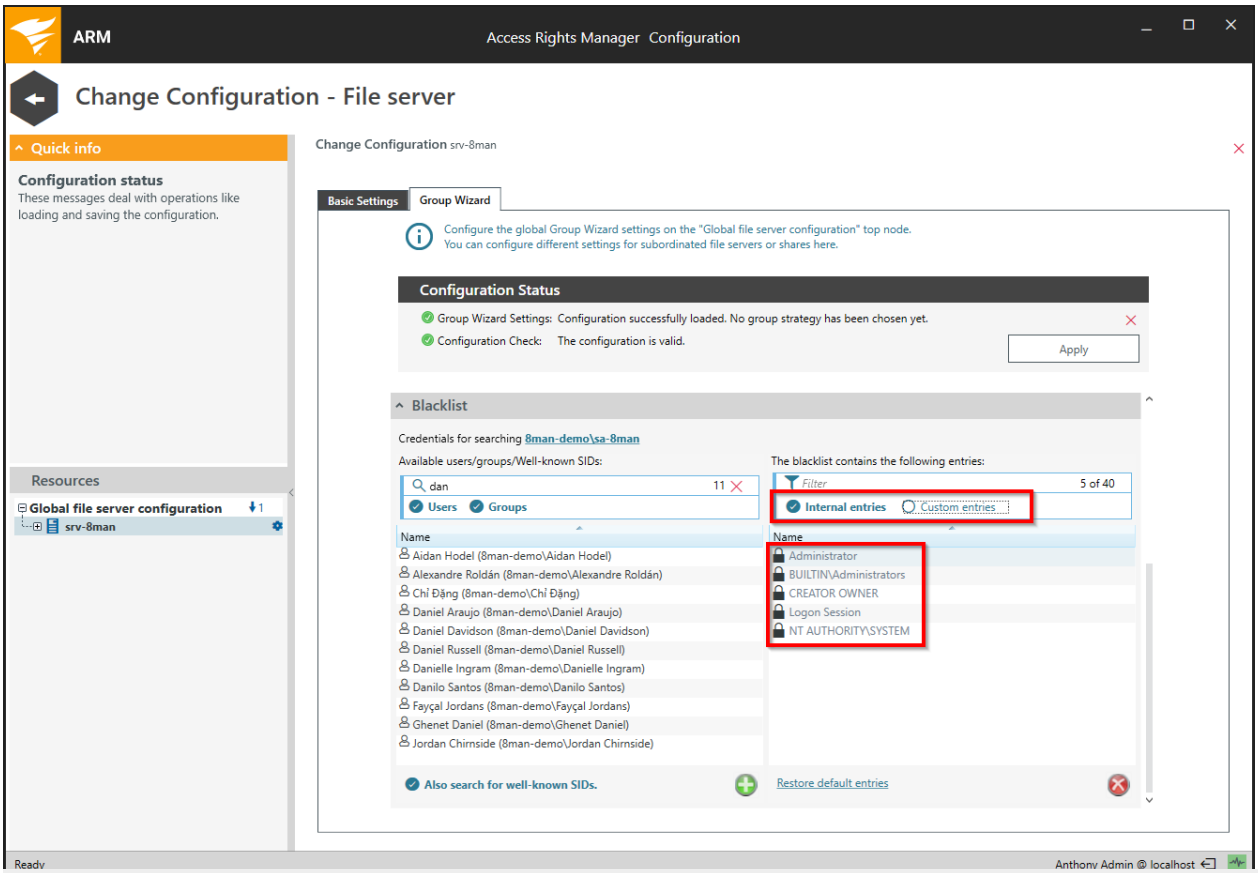
Restore default blacklist entries



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.

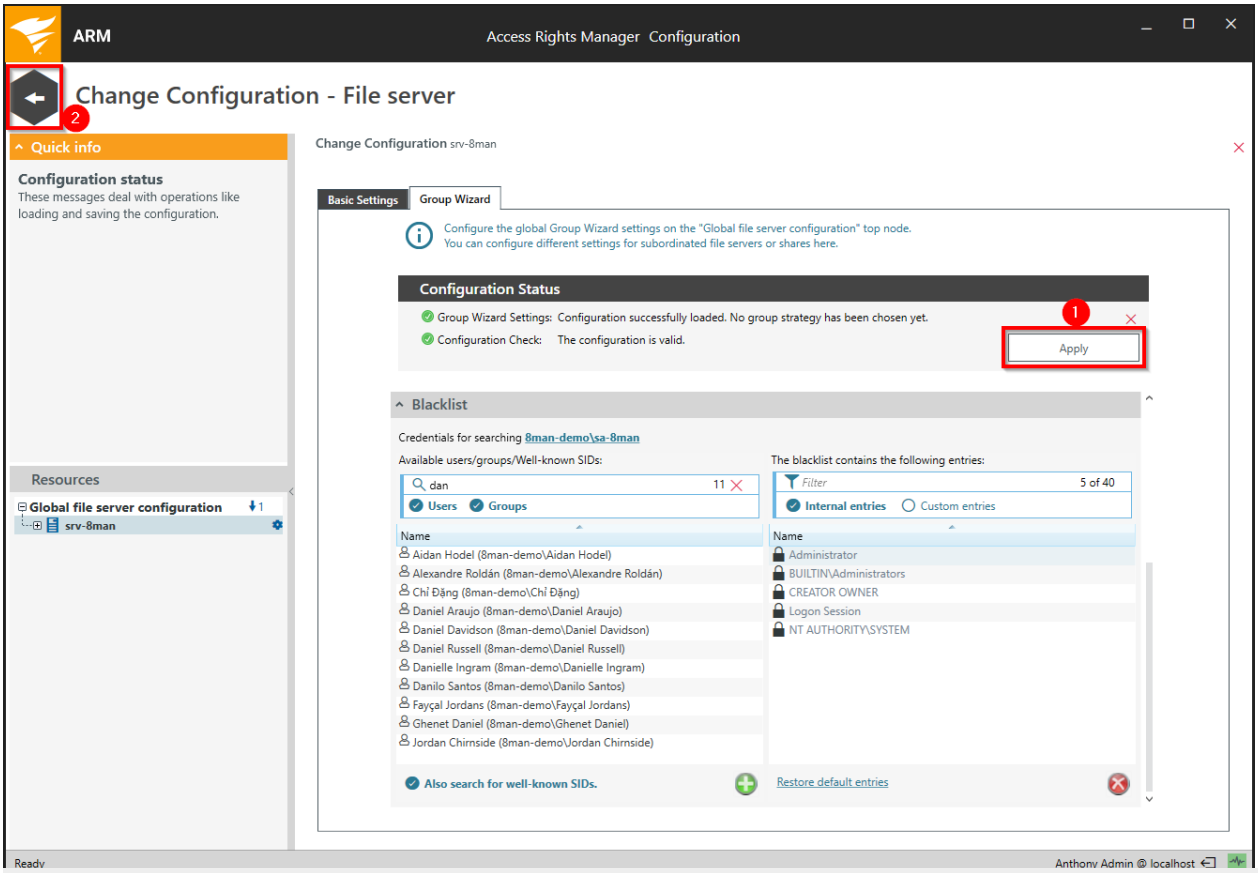
You are able to remove and restore the entries with the green dot. This may be required if you need to remove "Everyone" access rights, for example.

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



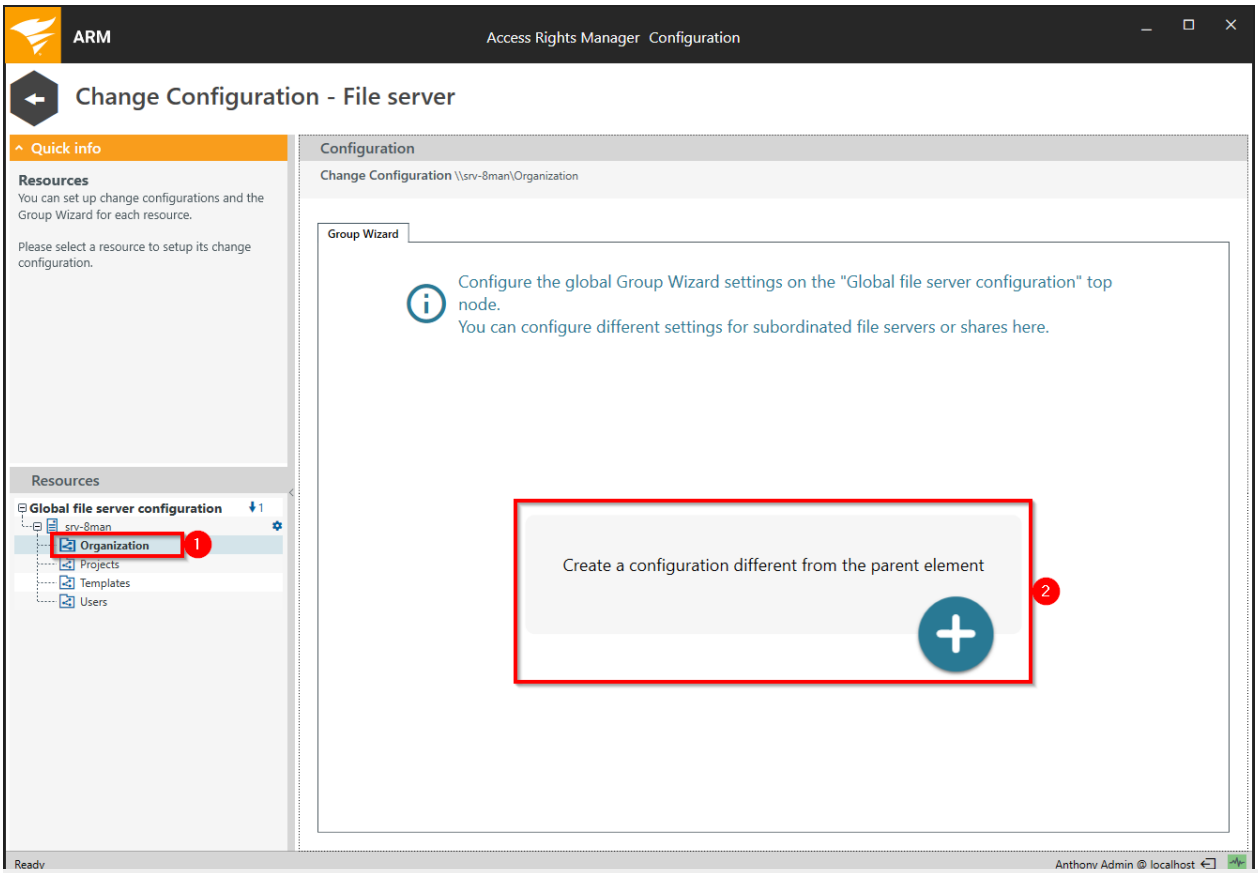
1. You must confirm changes in the file server change configuration by clicking "Apply".
2. If you click "Back" instead, a warning appears and you can discard all changes if necessary.

Define file server and share specific change settings

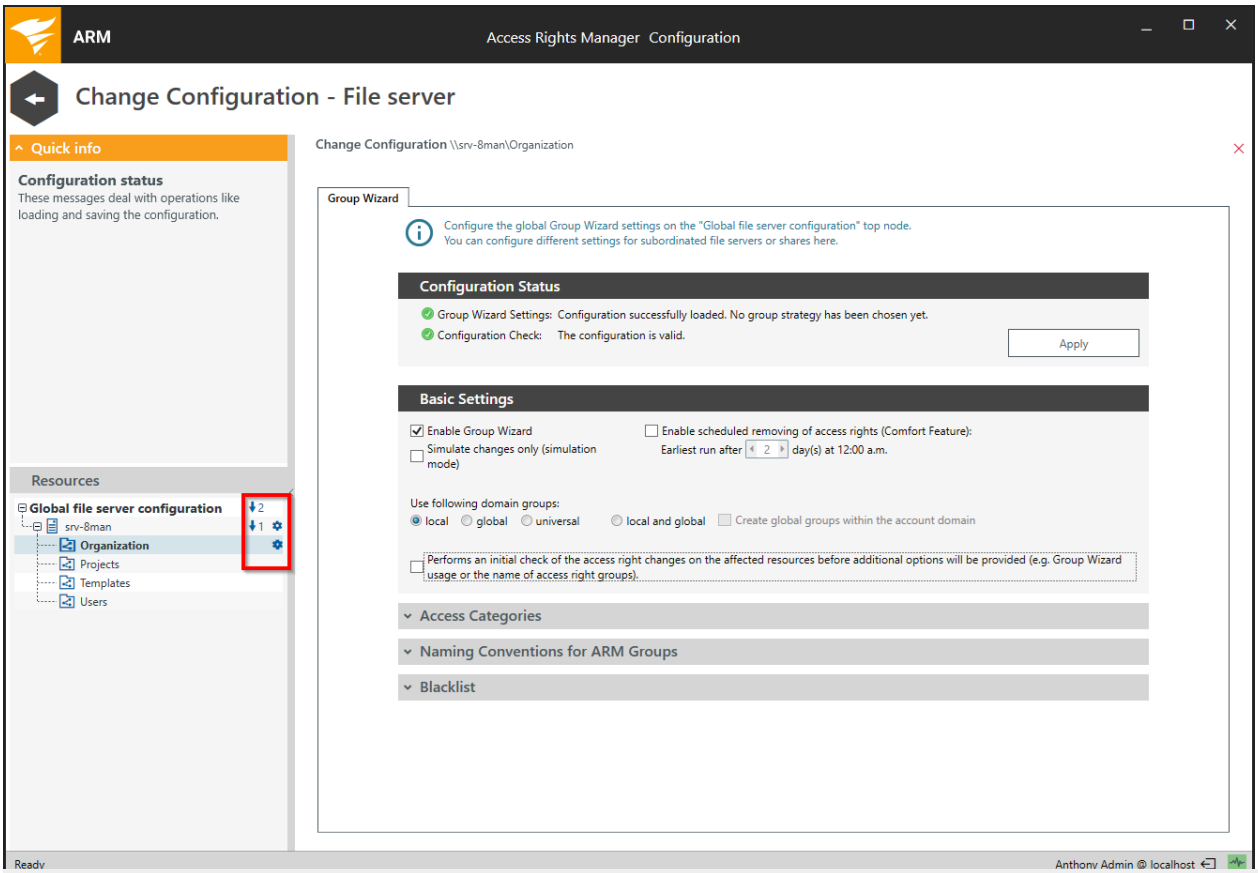
You can configure specific settings for each file server and configured shares:

- 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.

If you do not set any optional Group Wizard settings, the parent level settings will be used.

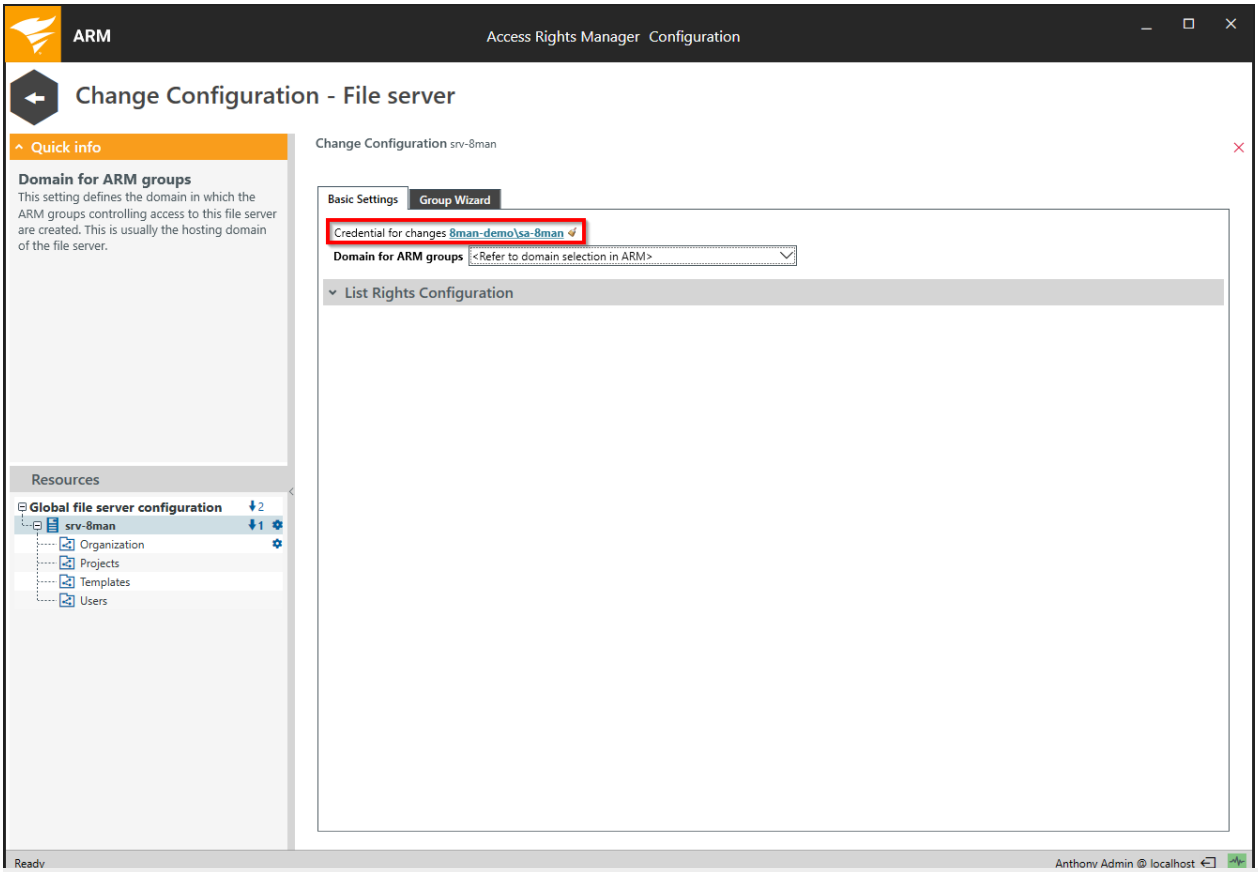


1. Select the desired file server or share in the "Resources" area. How to add a file server is described in the chapter Add FS scans. Newly added file servers and shares do not have a configuration.
2. Create a new configuration.



ARM shows you how many configurations exist below (arrow with number) and where they are (gear).

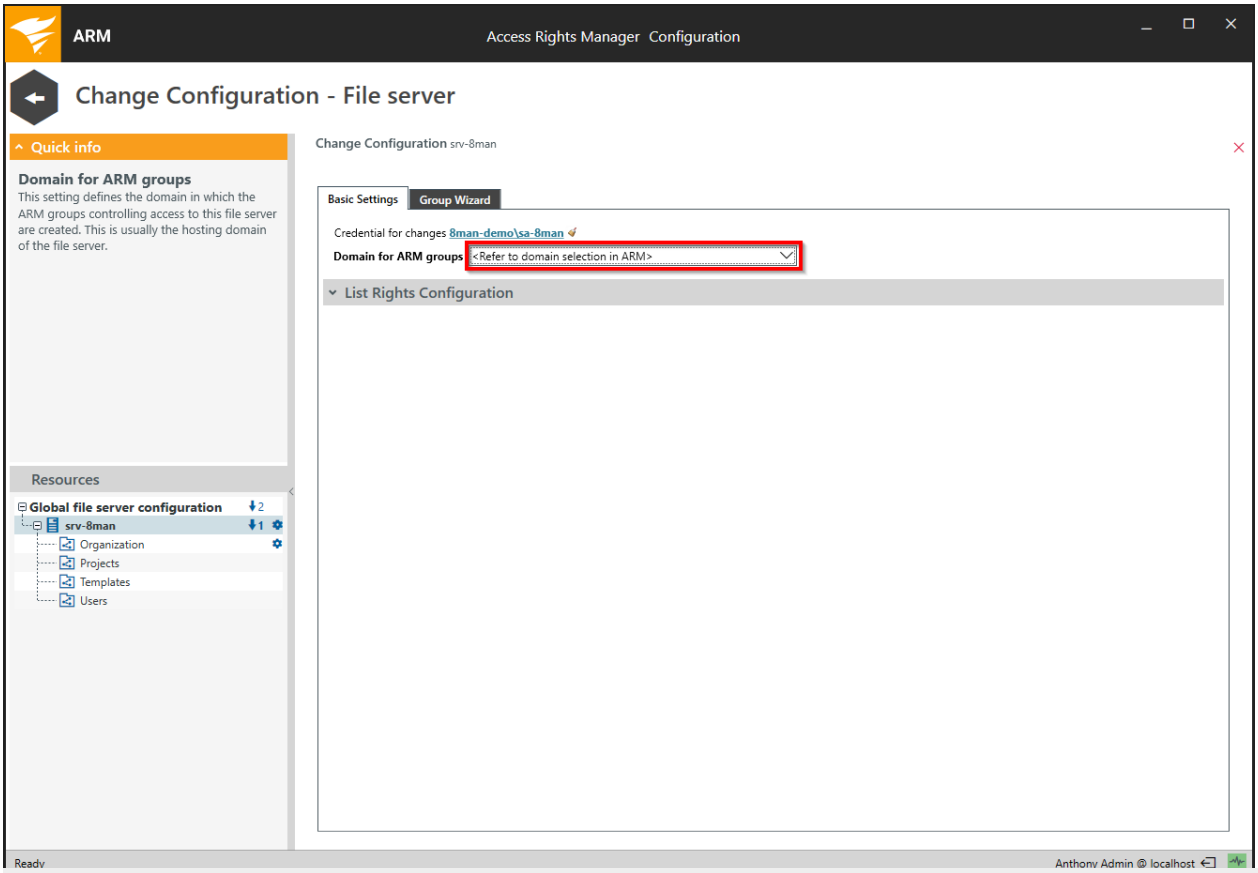
Configure the FS change account



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.

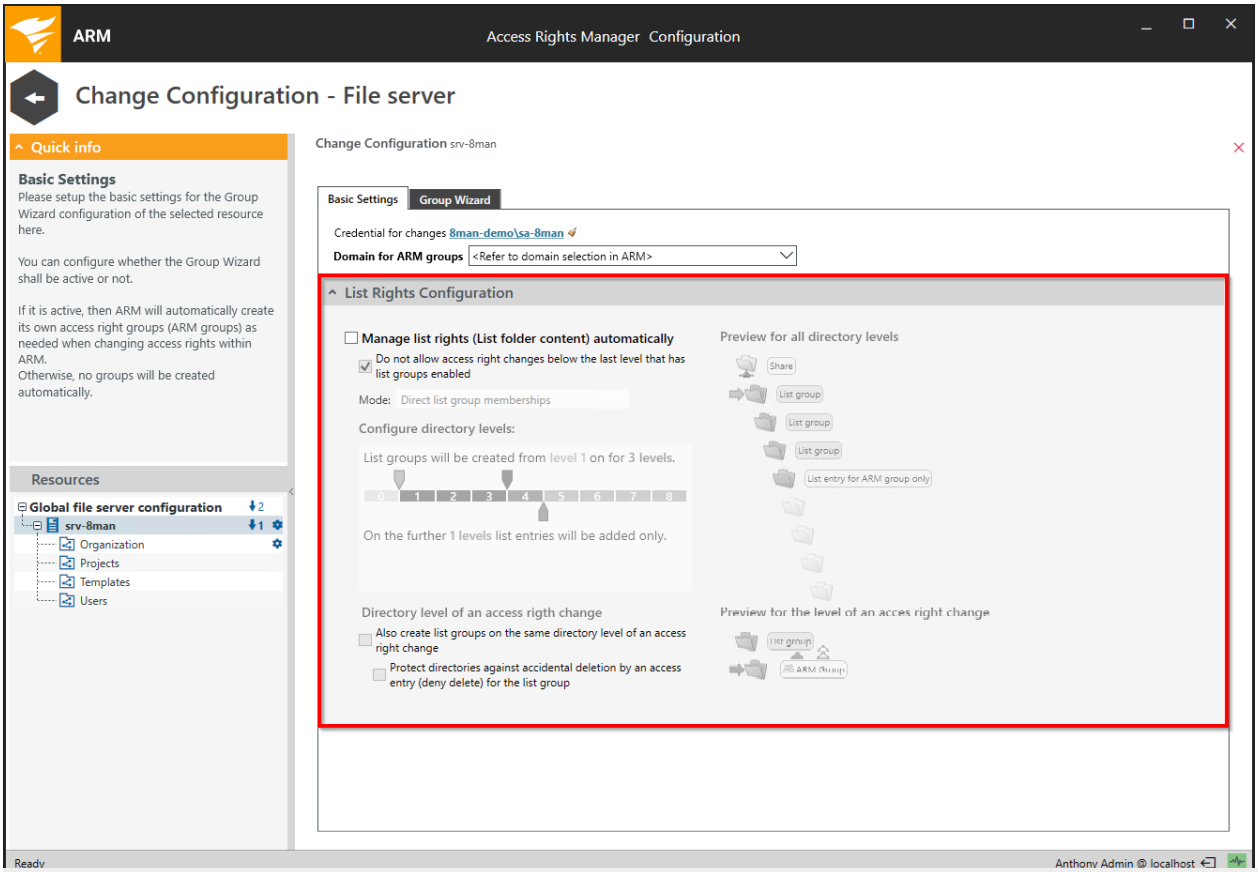
Determine the domain for ARM groups



Select the domain in which the ARM groups are stored.

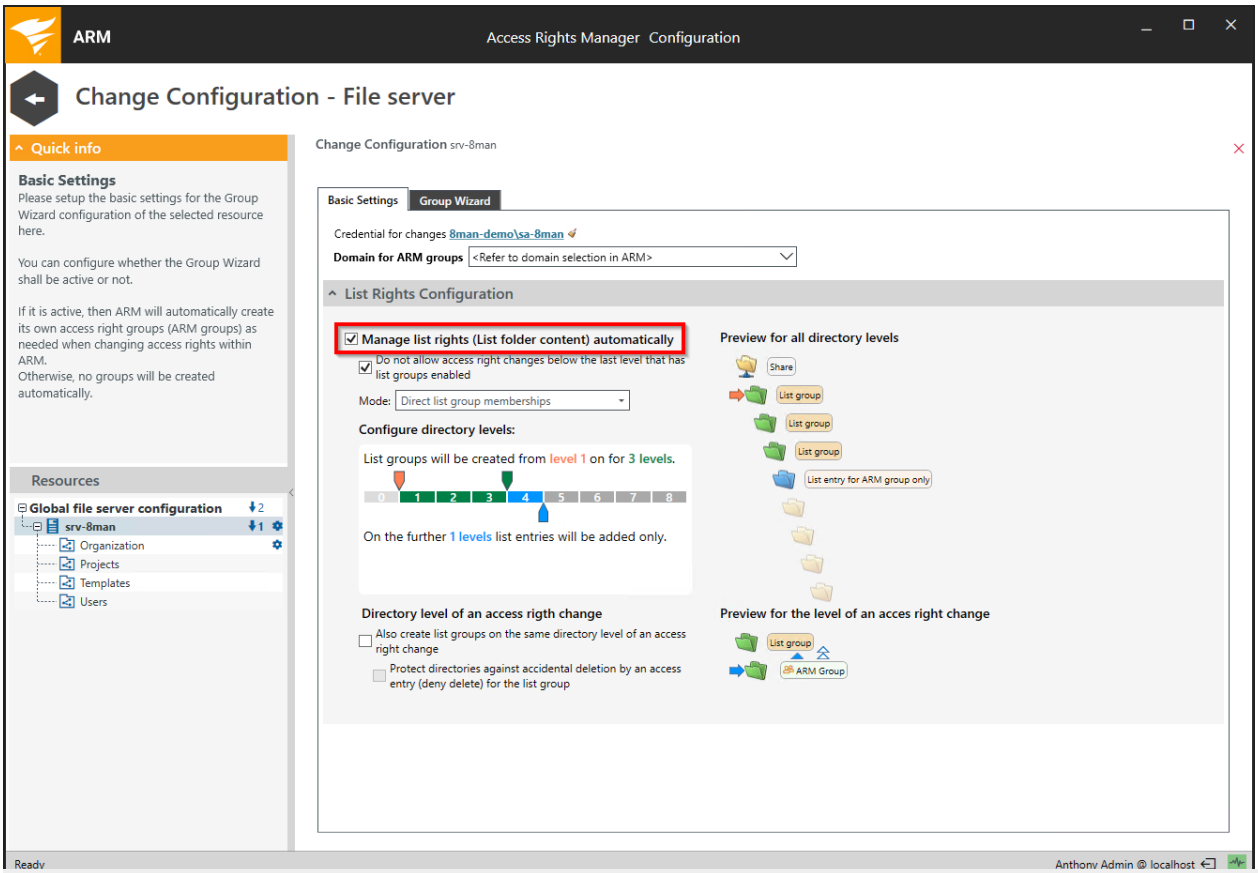
If you don't enter a domain, the ARM-groups will automatically be stored in the domain that the user has selected in the ARM application.

Configure automatic list rights management

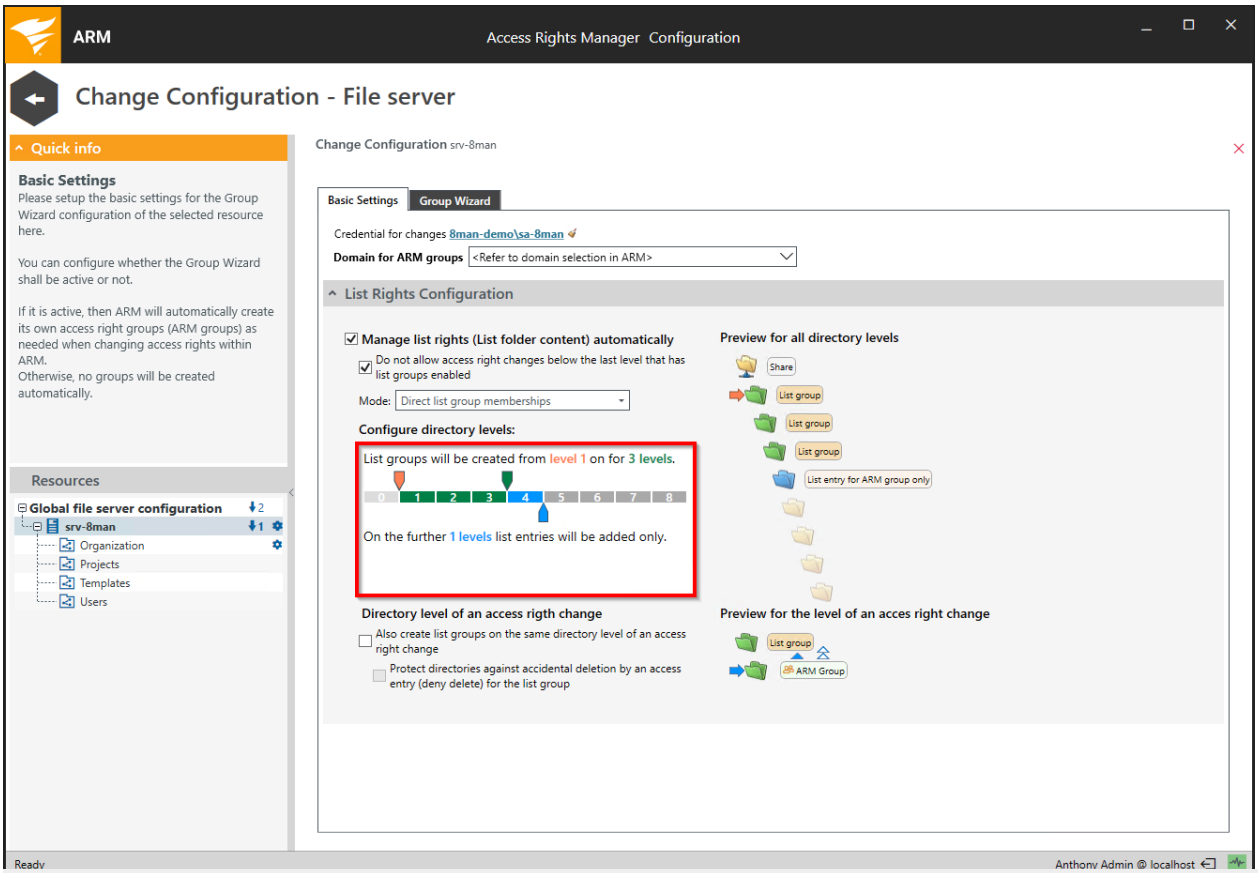


The list right configuration includes several options for determining how ARM automatically ensures that users can navigate to the folders that they have access to.

Compared to Microsoft native tools you can avoid many cumbersome and error prone administrative steps.



Activate the automatic list rights management.



Use the sliders to determine the level of folder depth that ARM manages.

Level 0

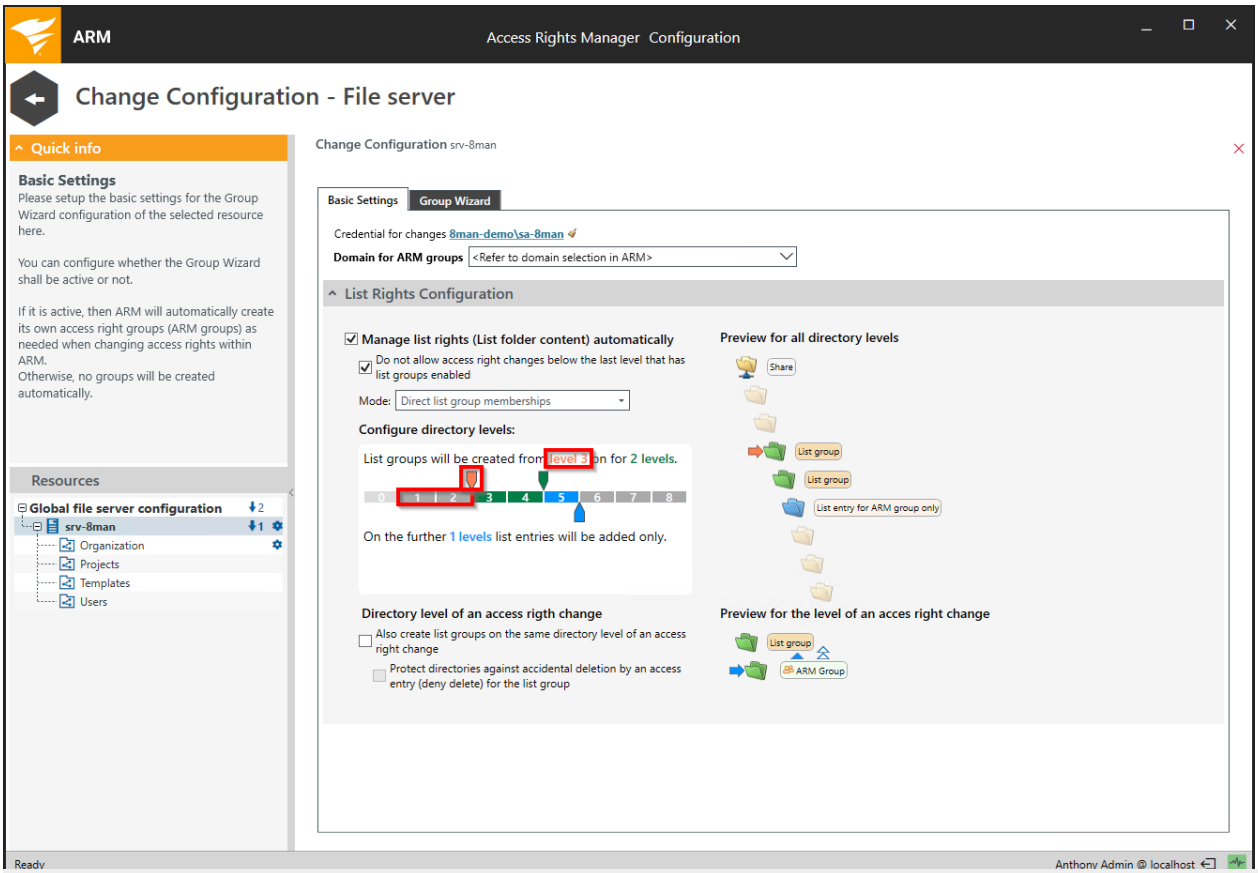
Level 0 is the shared folder (share level). This folder is visible to users based on share rights. An assignment of list rights on this level is not required.

green levels

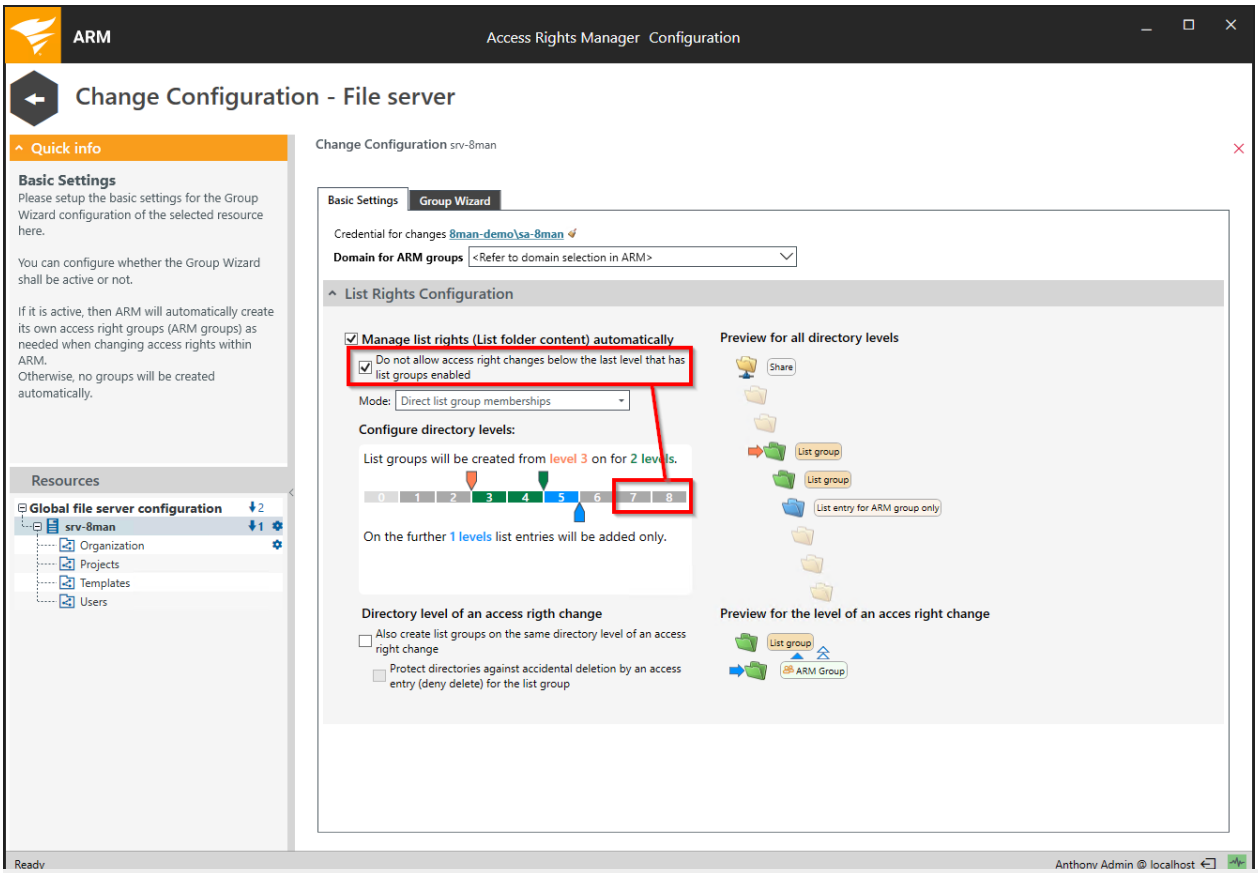
ARM creates list groups for every level. The access rights groups become members of list groups.

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.

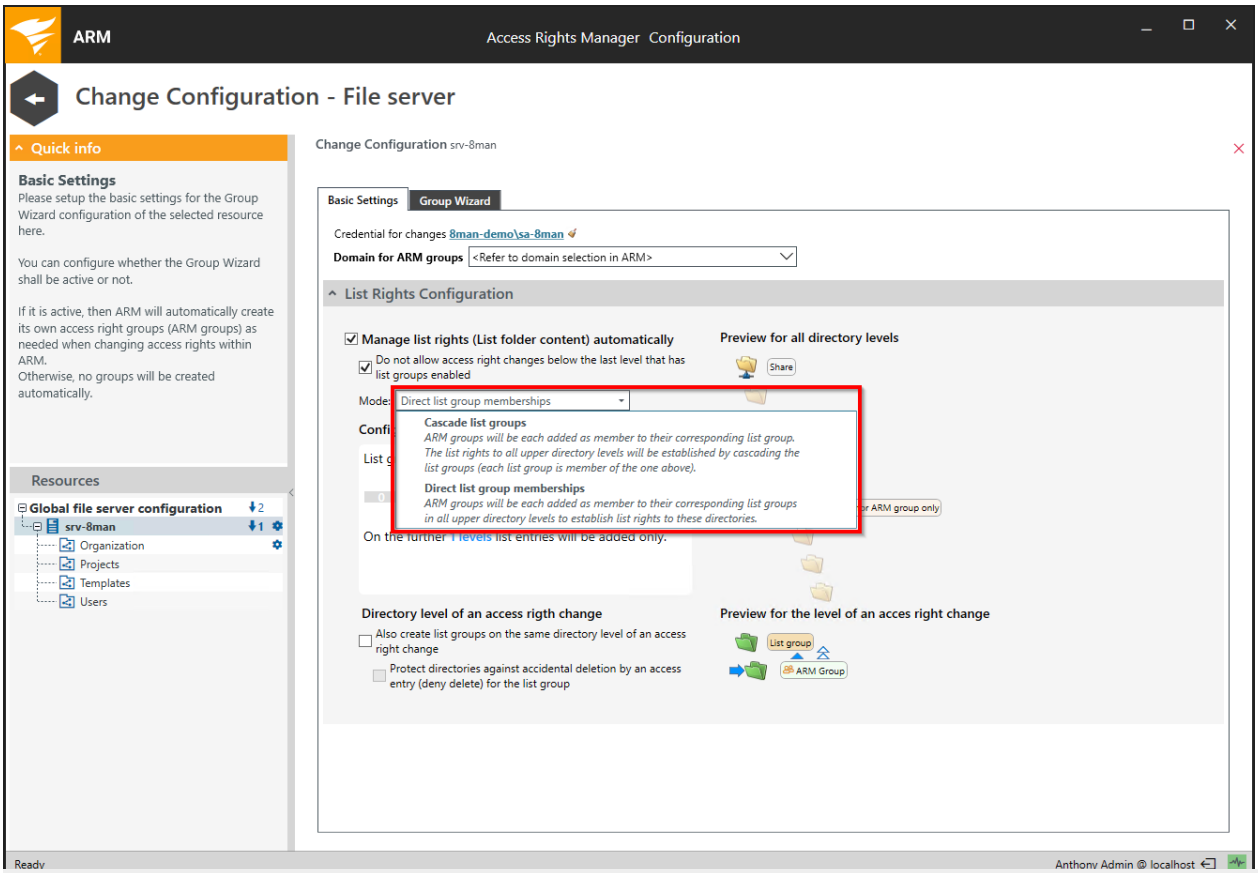


Move the orange slider to exclude folder levels from the automatic creation of list groups. This is useful if users already have list rights to these folder levels.



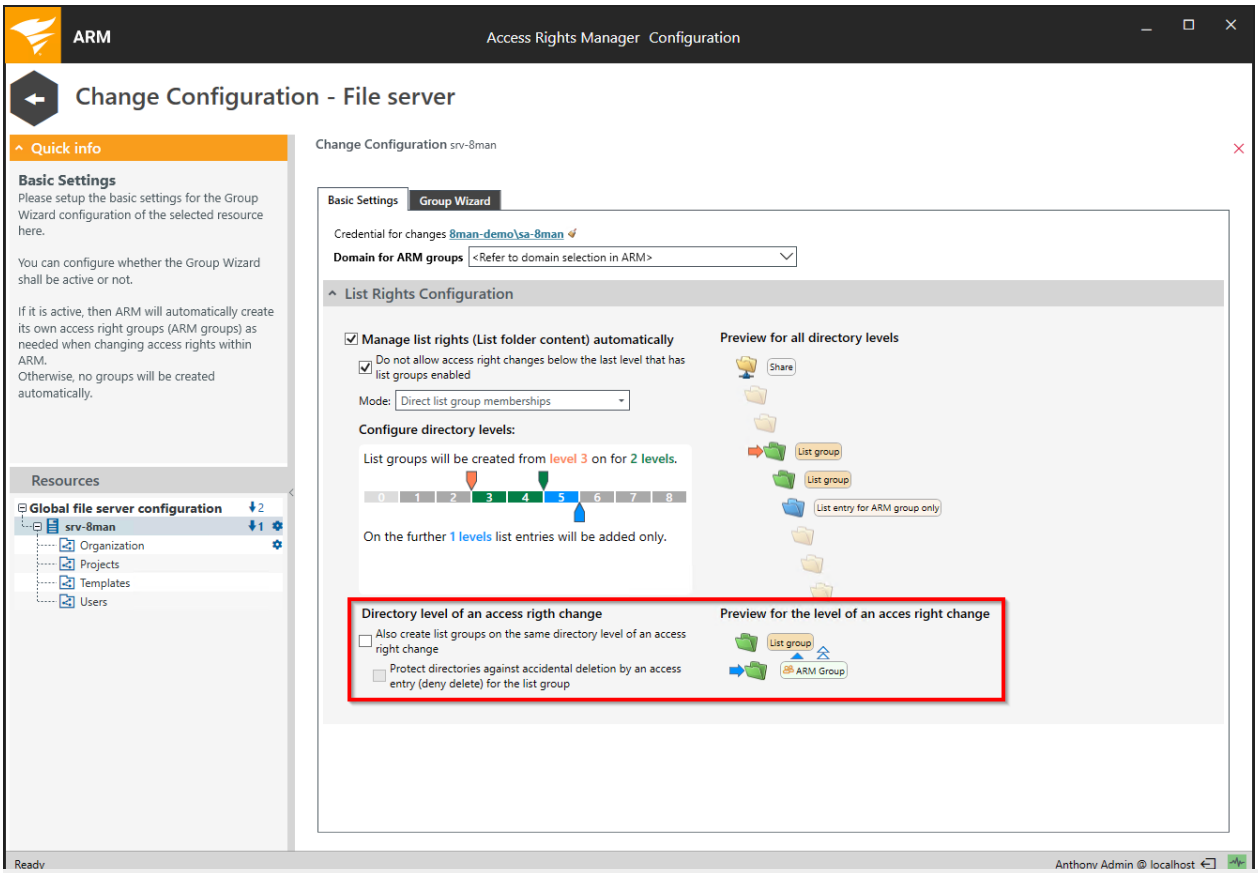
Activate this option to prevent access rights changes with ARM below the lowest "list-rights-level" plus one (for example level 7, as in the screenshot).

You should activate this option to prevent users from gaining access to levels that they are not able to navigate to.



Select a list group mode.

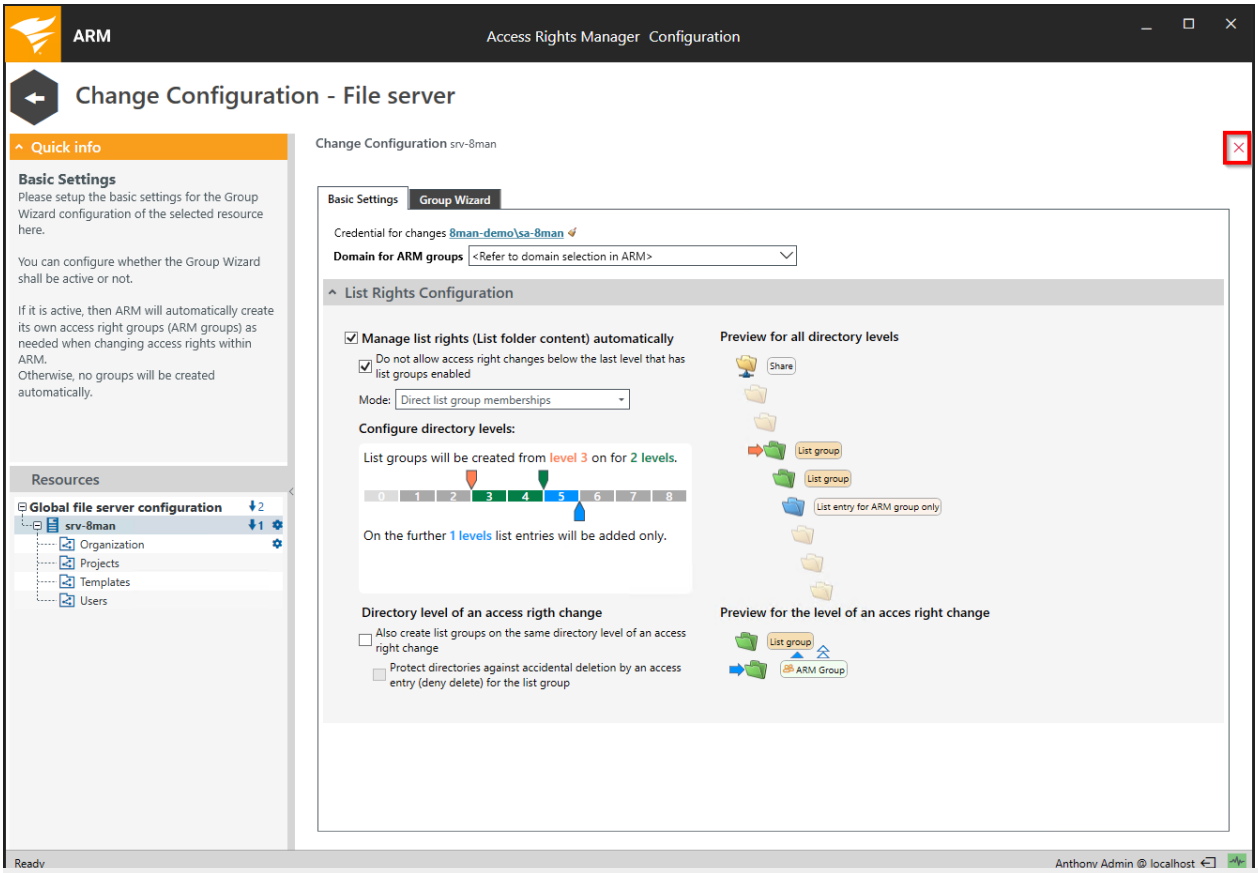
This setting has no impact on Kerberos token size.



You can use these options to prevent the deletion of folders that are to be retained as parents for inheritance.

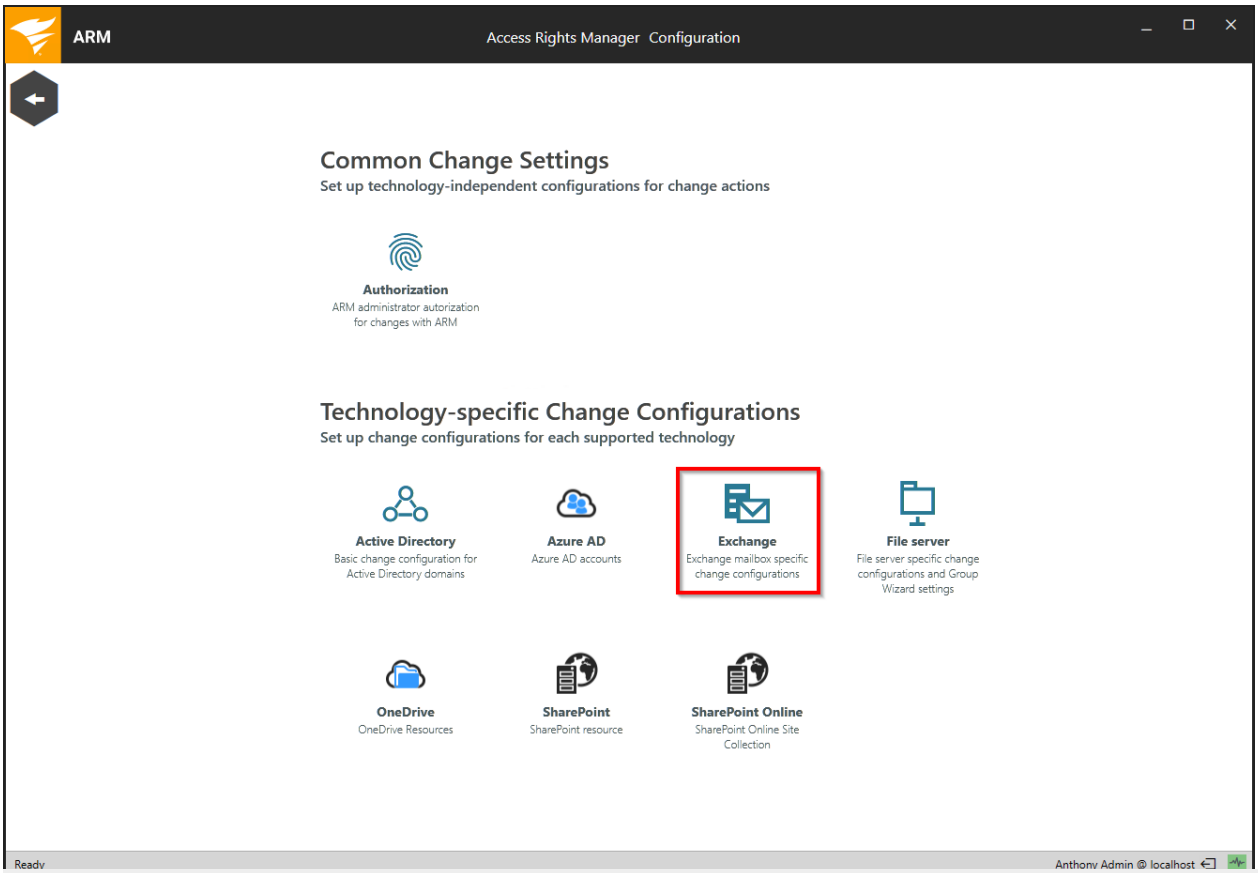
> It is more beneficial to protect folder levels by assigning "restricted modify", as these require fewer group memberships.

Delete a file server- and share-specific change configuration



Click the red X to remove a change configuration.

Exchange change configuration



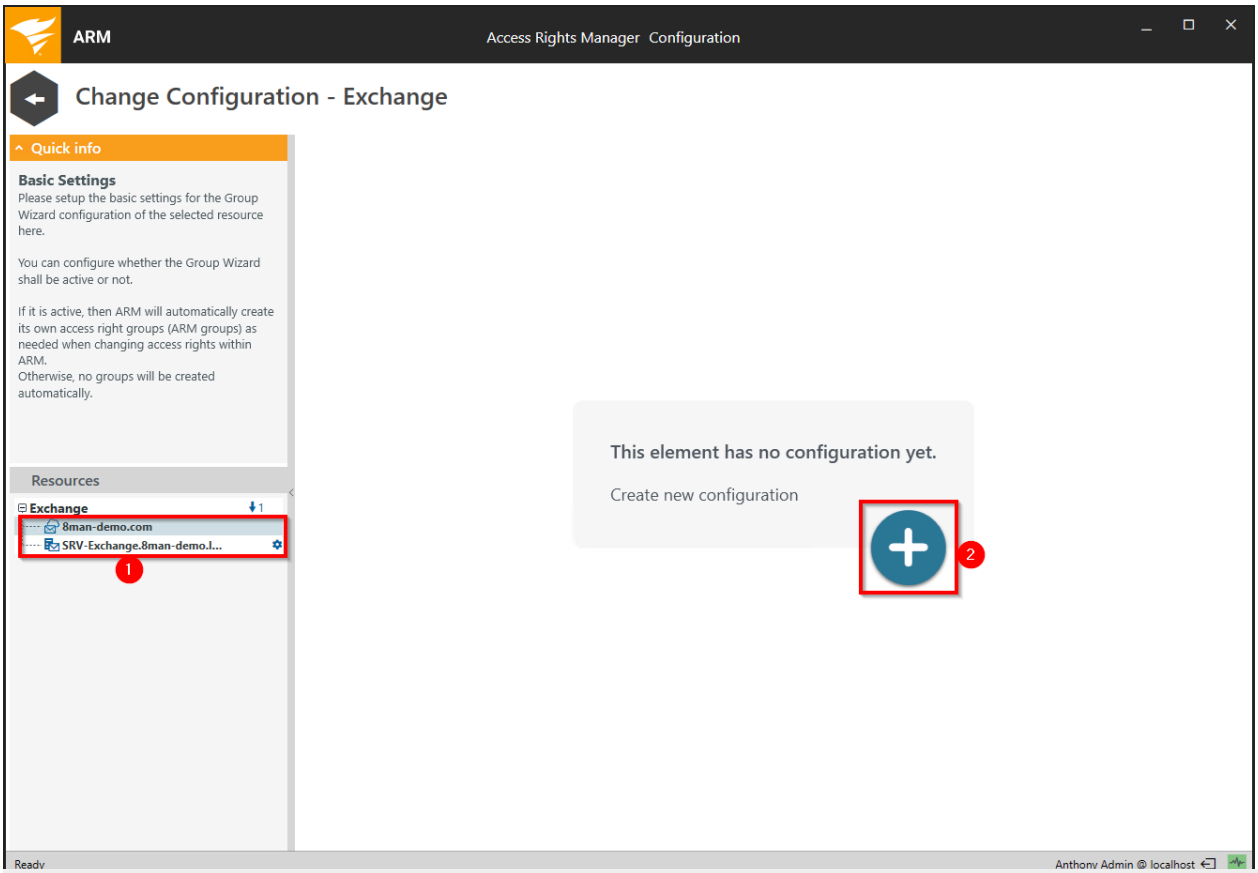
Select "Change configuration" from the ARM Configuration application home menu.

Click "Exchange".

Create an Exchange change configuration

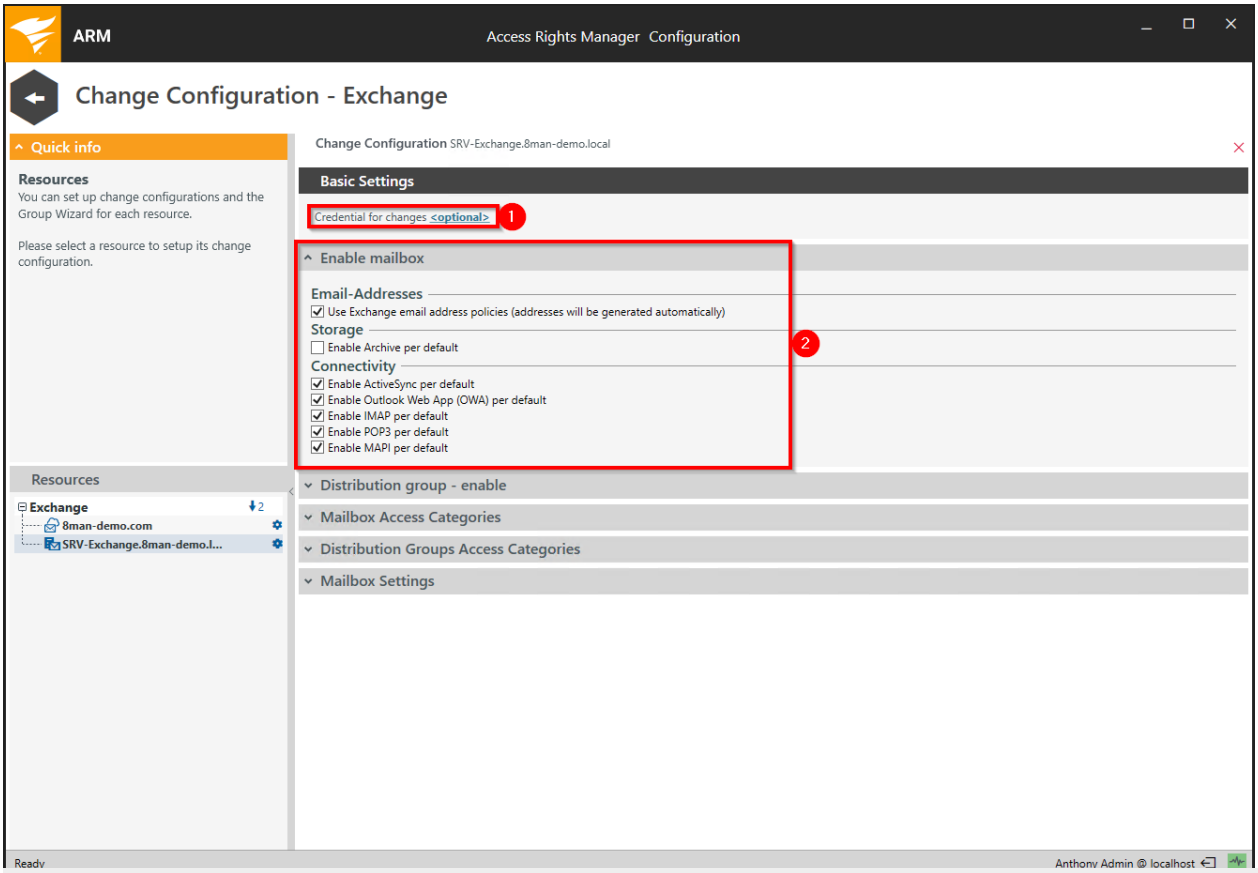
In order to create an Exchange Change configuration, complete the following steps first:

1. Create an Exchange Scan configuration.
2. Have ARM complete at least one Exchange scan.



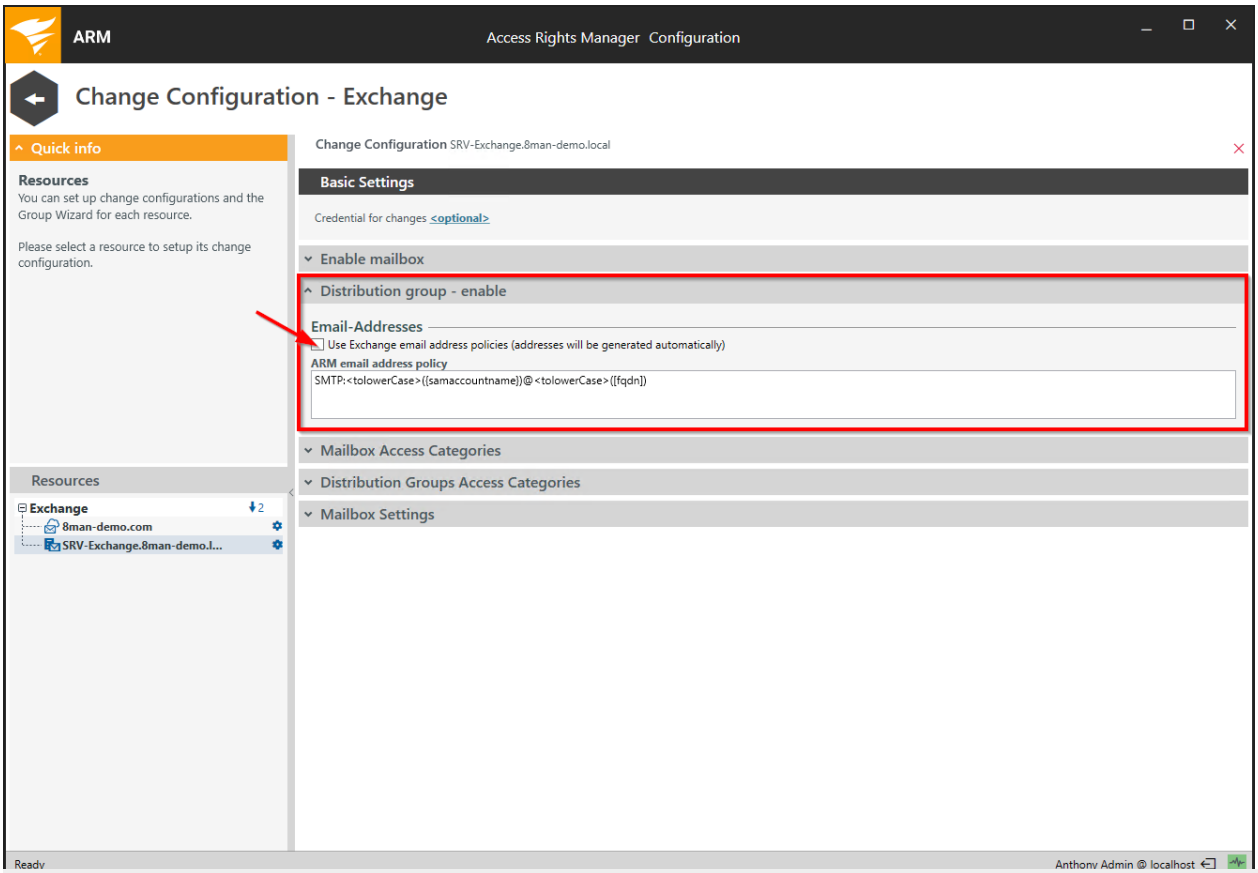
1. Select an (already scanned) Exchange server.
2. Click the plus icon.

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).

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:

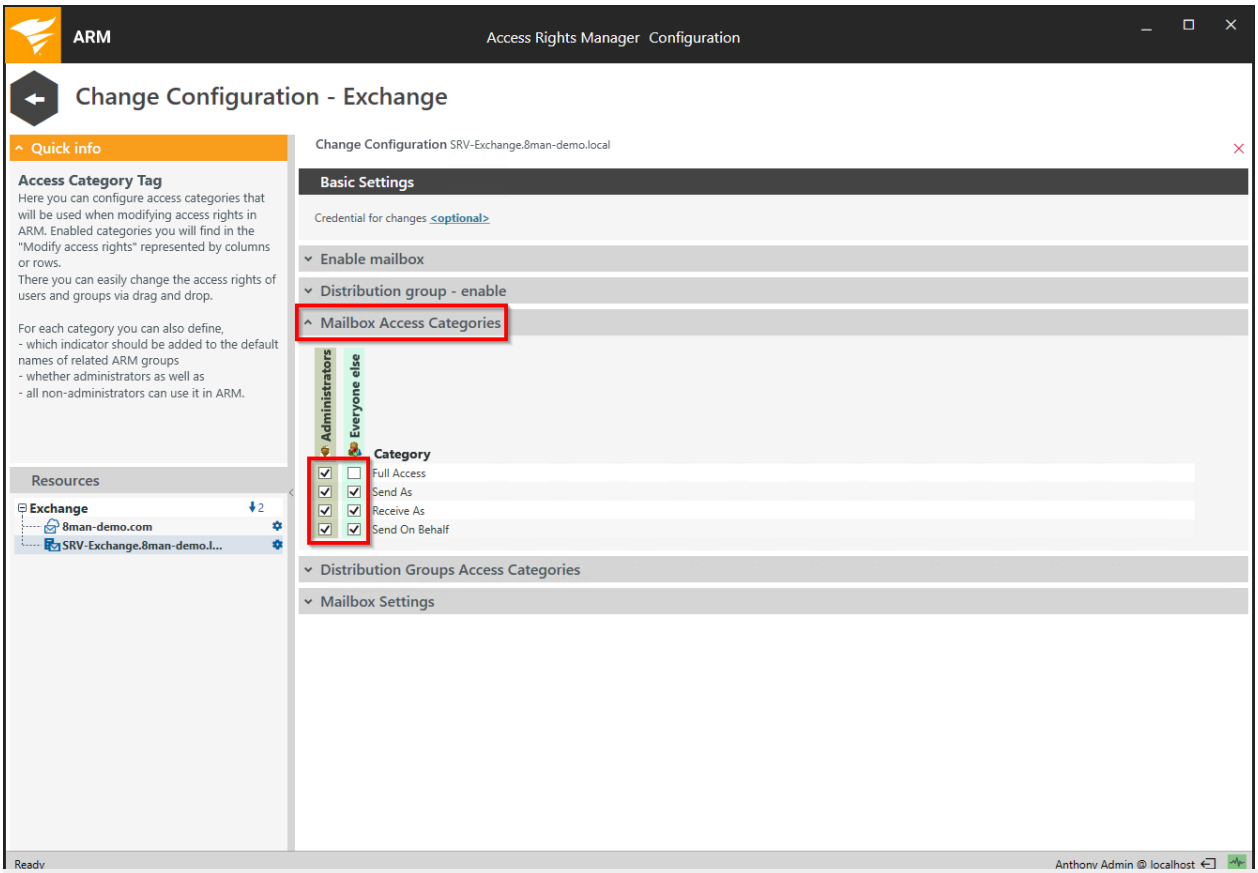
E-Mail-Addresses are automatically built based on Exchange policies. When activating emails for mailing lists the email address can not be changed.

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.

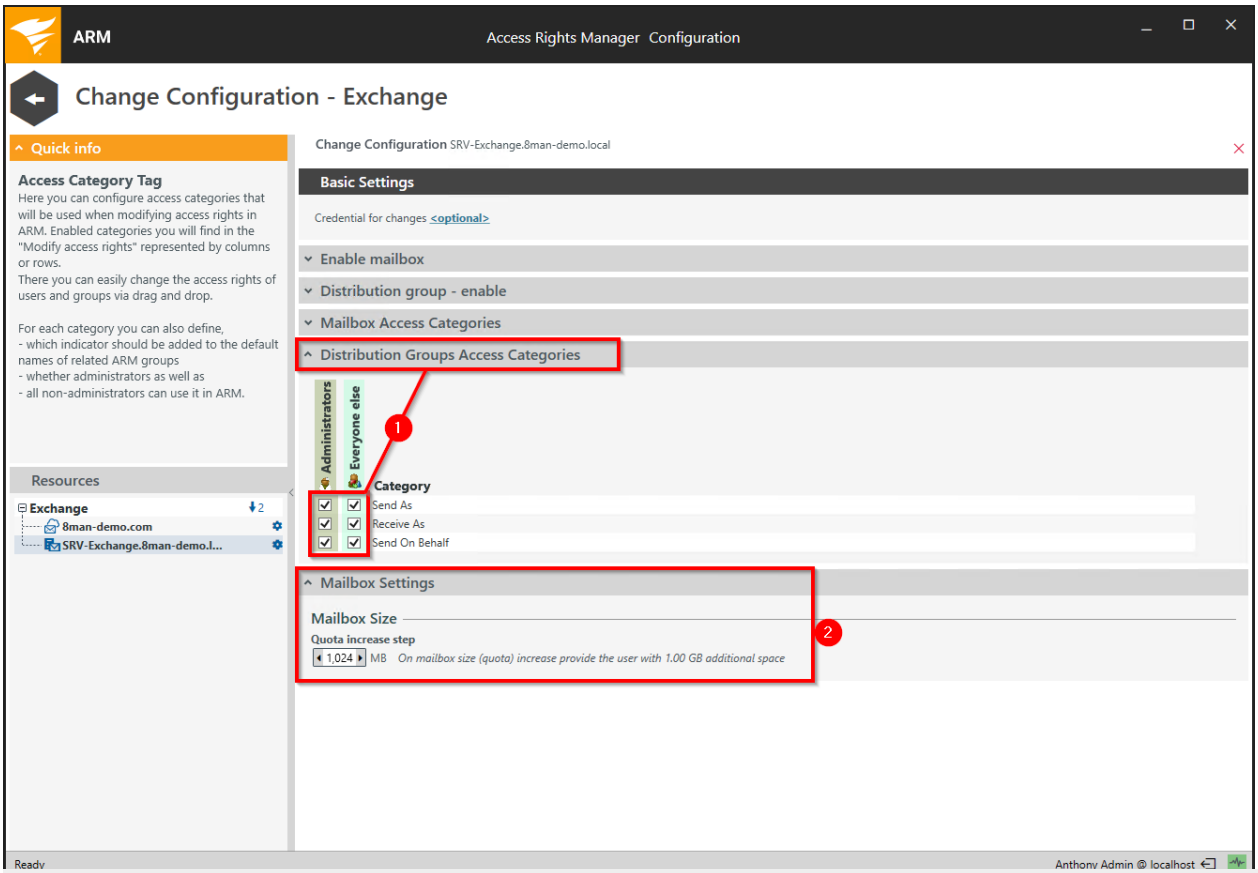
When activating email of the distribution group, the email address can be changed.

Creating distribution groups in Exchange Online is not supported.



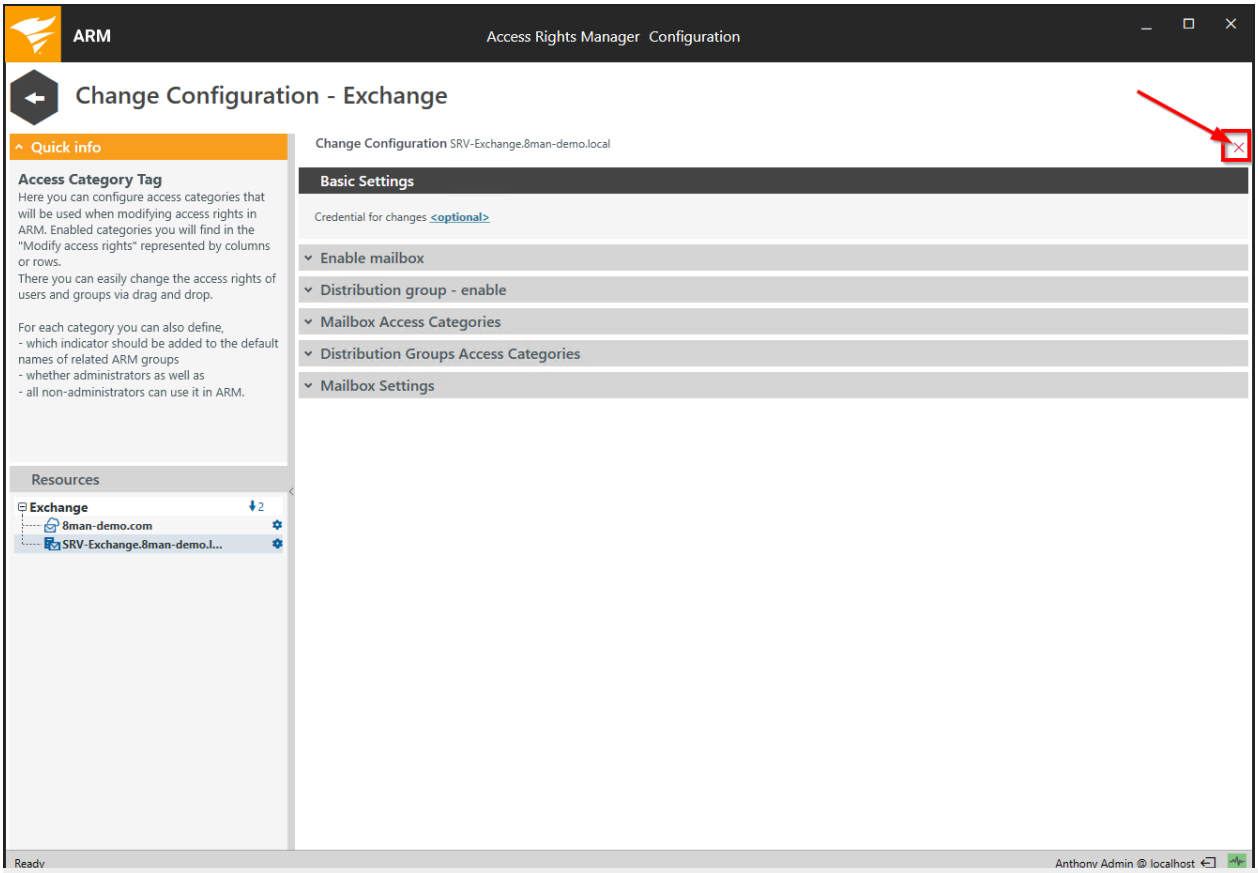
Determine which mailbox access categories are available to ARM users.

The category "Receive As" is not supported by Exchange Online.



1. Determine which distribution group access categories are available to ARM users.
2. Determine the increments that will be used to increase mailbox size.

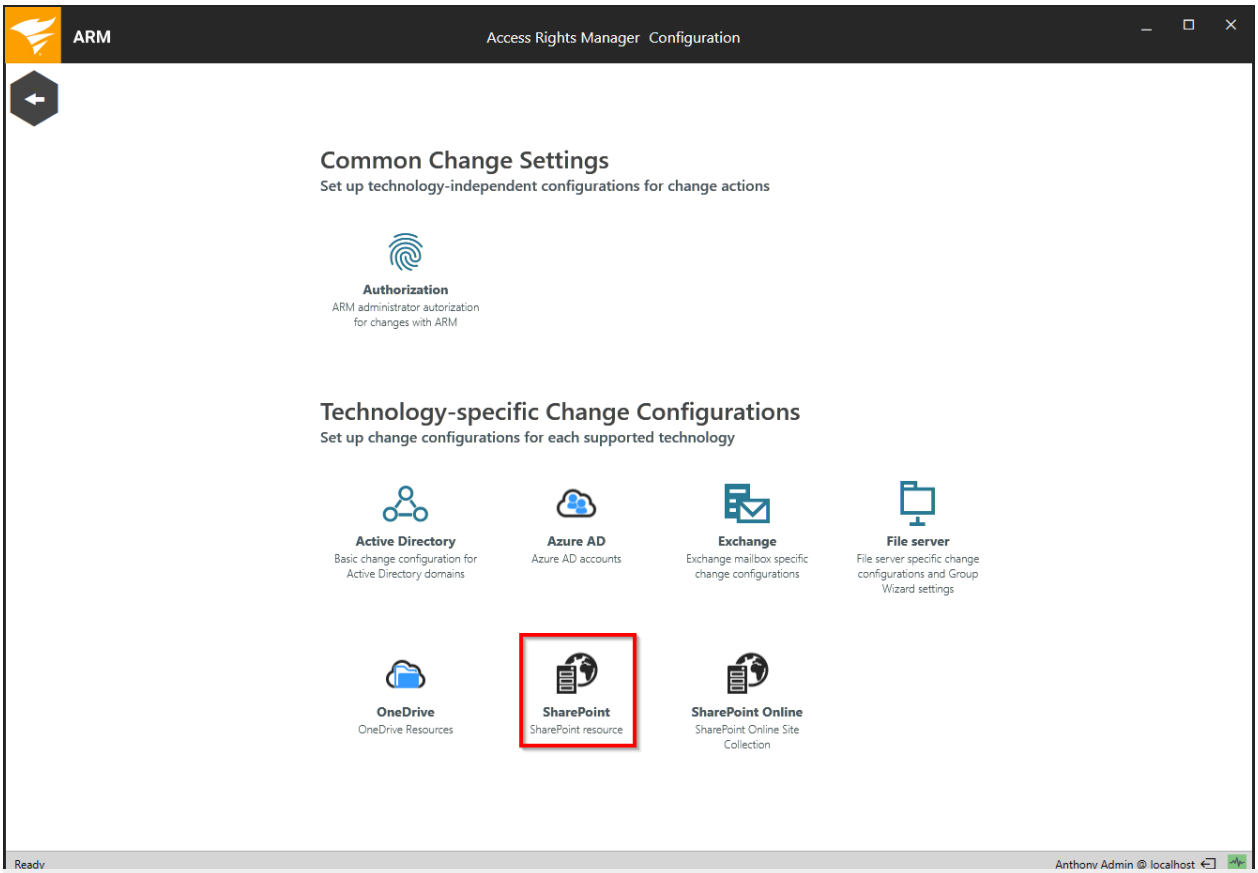
Delete an Exchange change configuration



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.

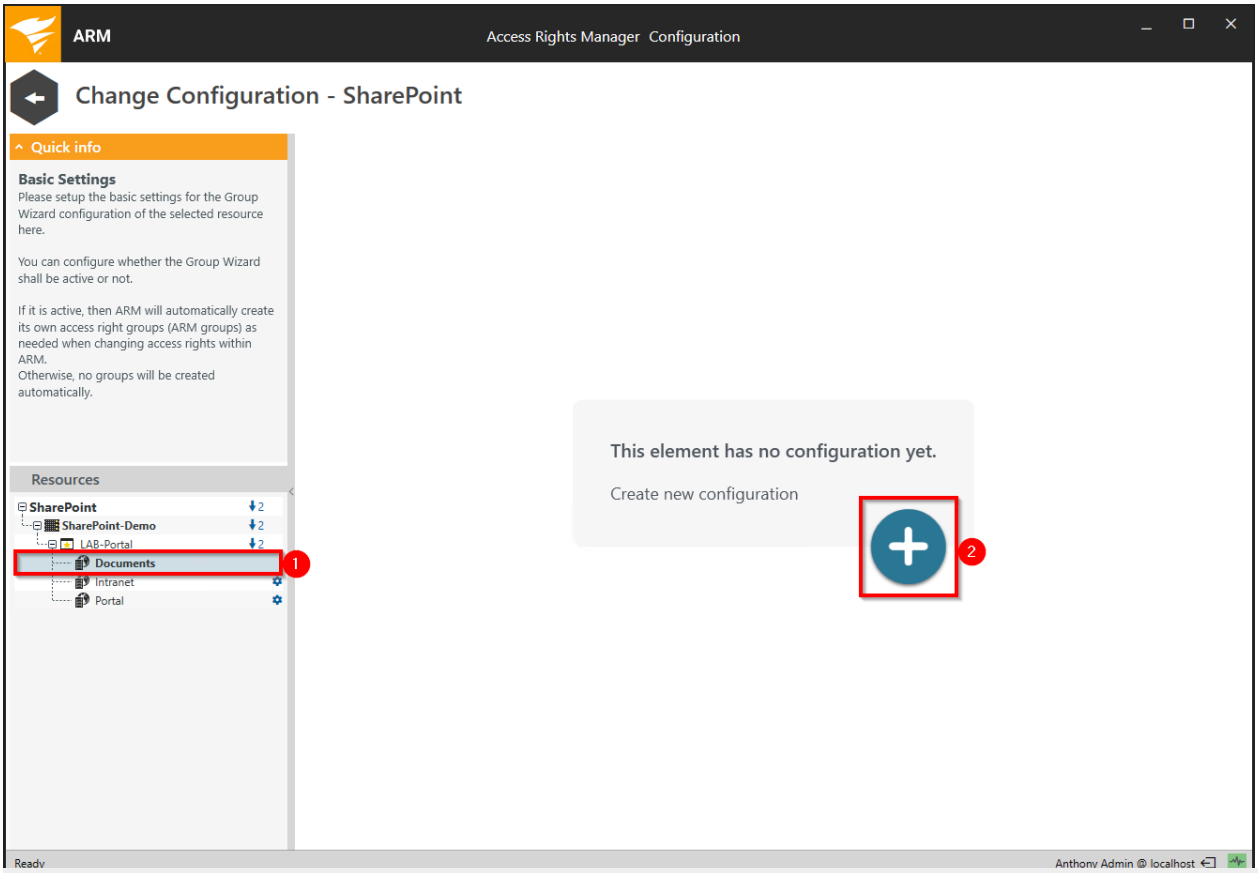
SharePoint change configuration



In the ARM Configuration application, navigate to "Change Configuration" -> "SharePoint".

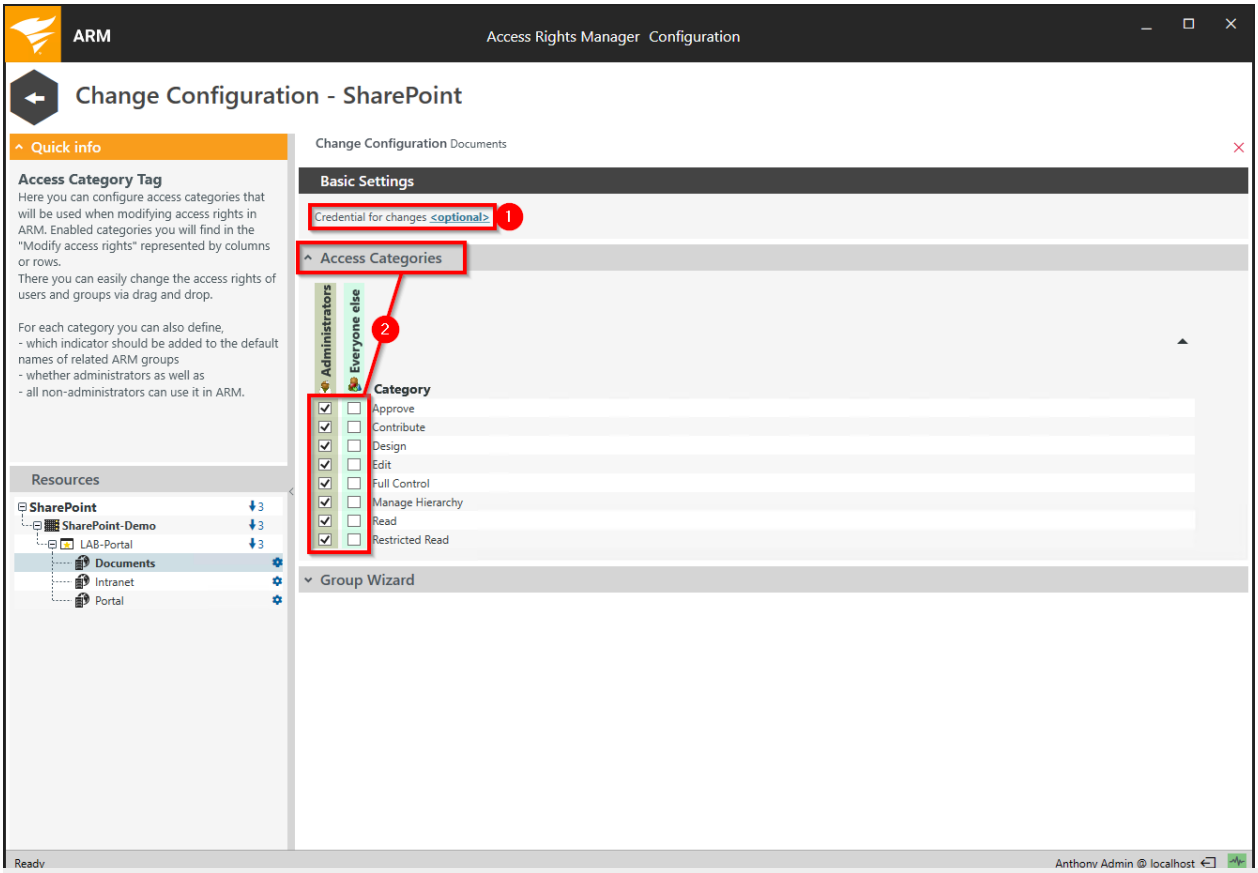
You must have run at least one SharePoint scan to create a change configuration.

Add a SharePoint change configuration

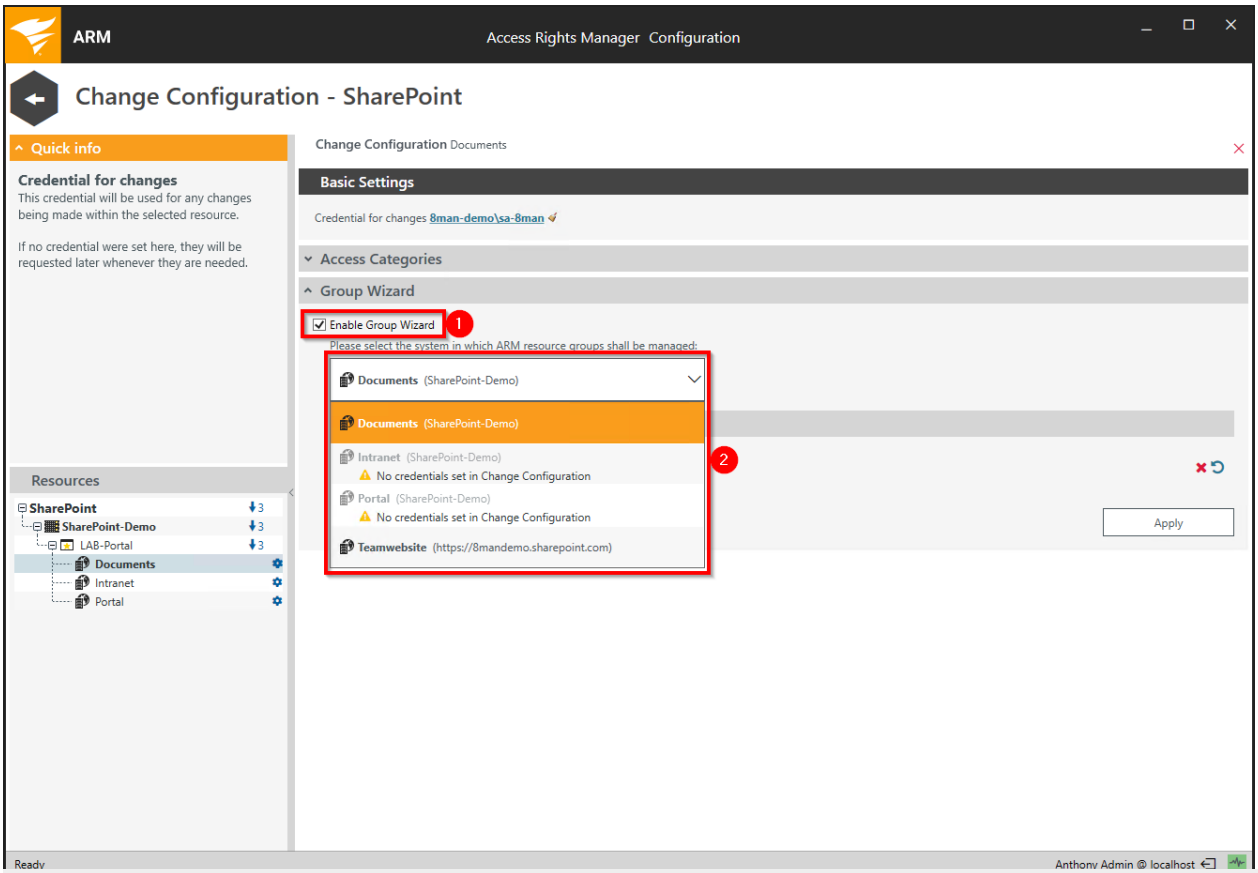


1. Select a SharePoint resource.
2. Click the plus icon.

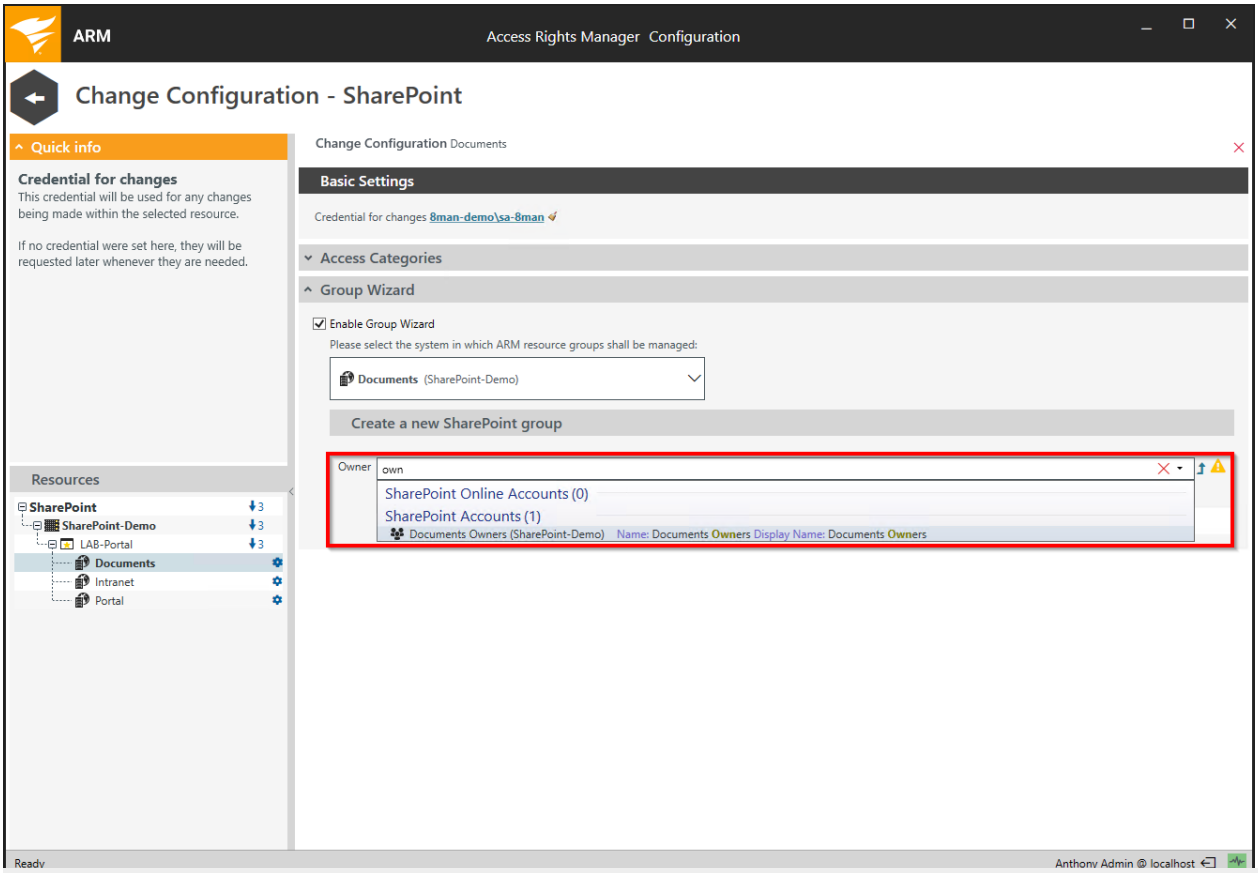
Modify a SharePoint change configuration



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).

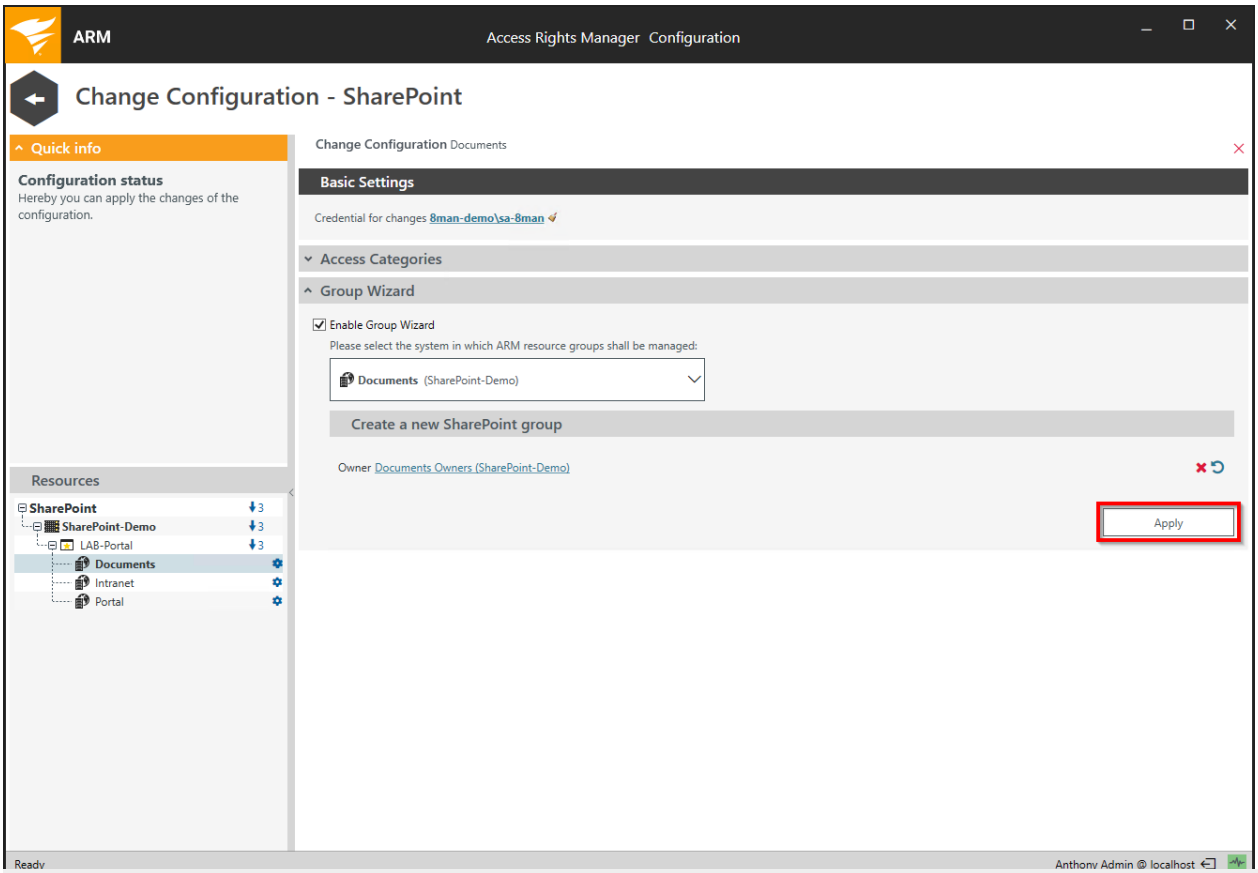


1. **Option enabled**
   ARM automatically creates permission groups when assigning permissions using drag & drop in the ARM application.
2. Determine where the permission groups are stored.



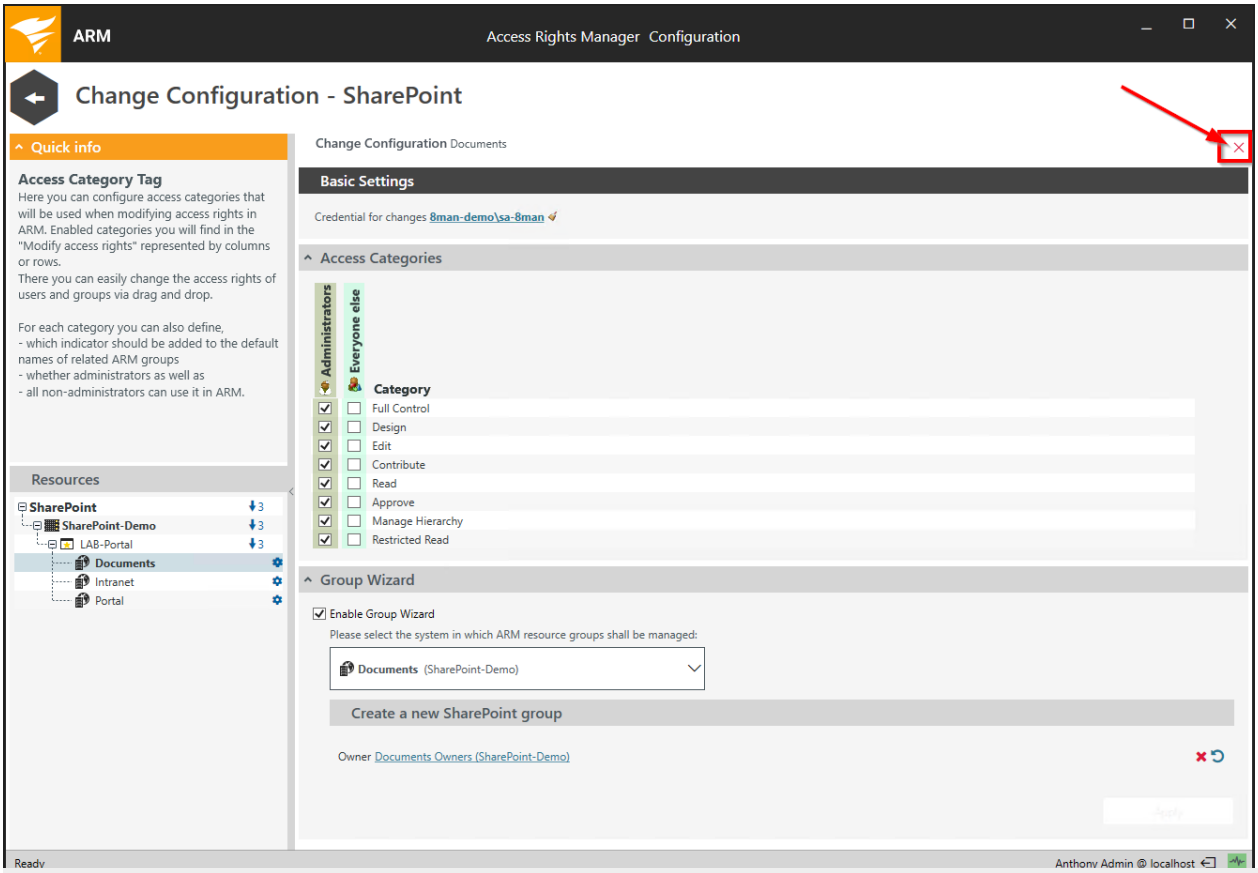
SharePoint groups must have an owner. Use the search to specify a SharePoint account which will be the owner of the automatically created permission groups.

Enter a space in the search box to get a list of all available accounts.



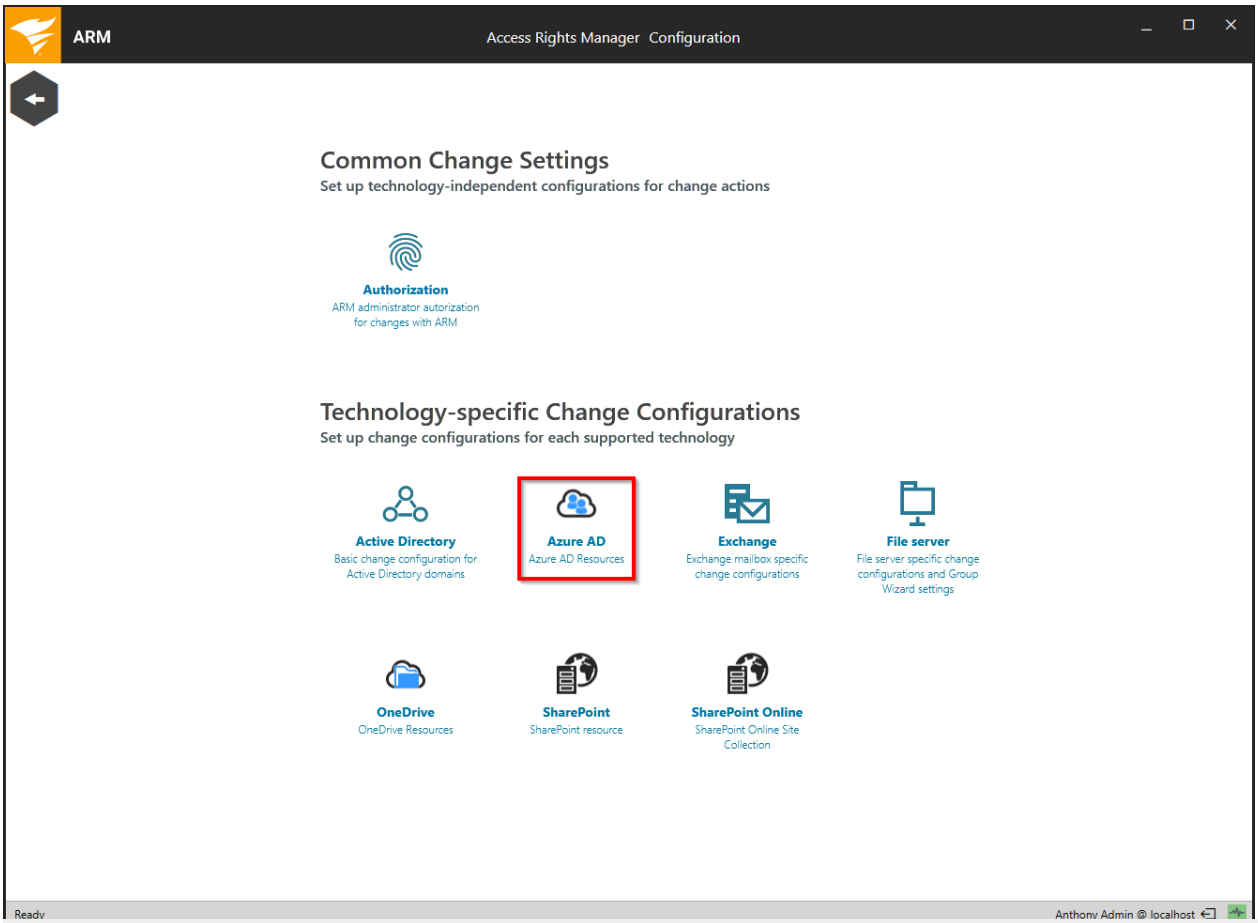
Click "Apply" to save your SharePoint Group Wizard settings.

Delete a SharePoint change configuration



Delete a SharePoint change configuration.

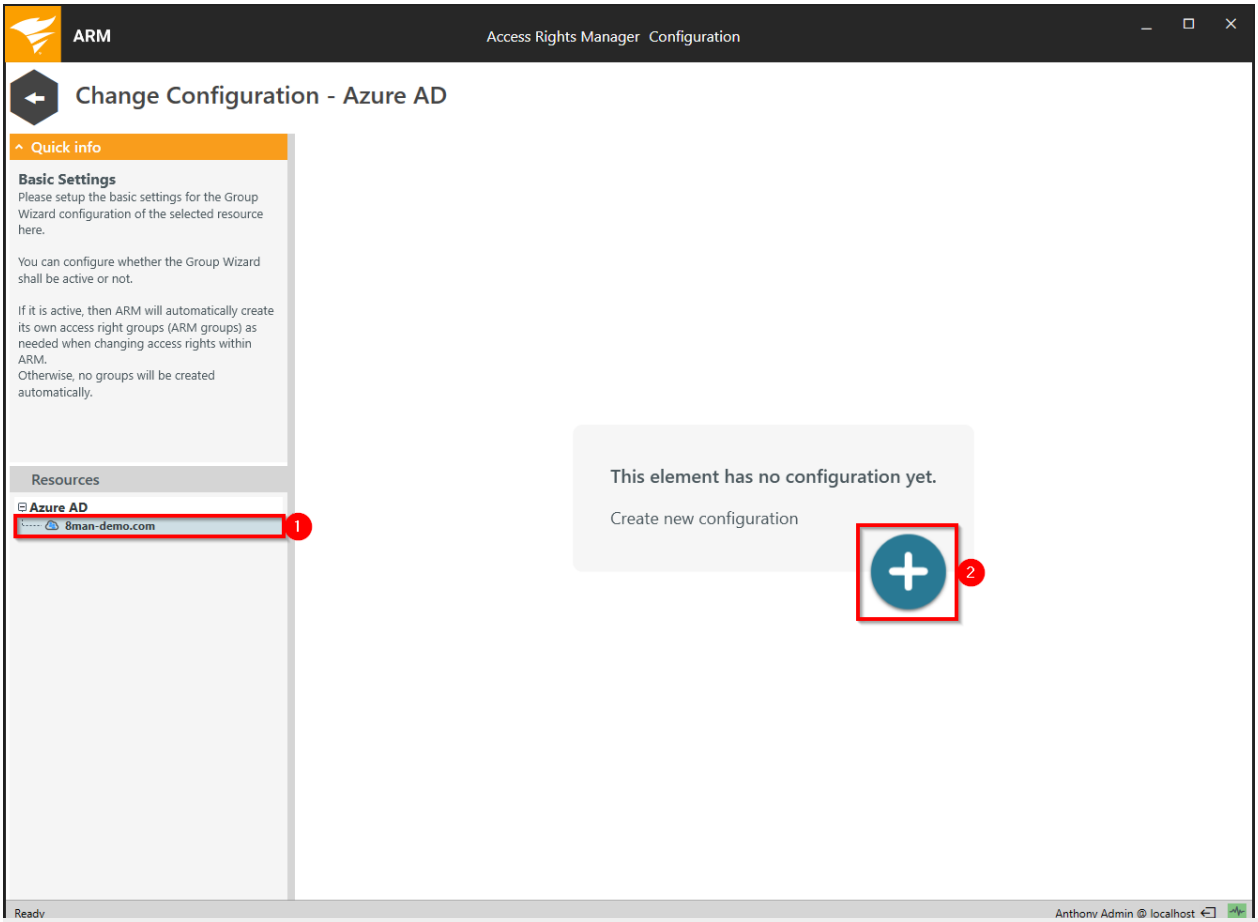
Azure Active Directory (AAD) change configuration



In the ARM configuration application, navigate to Change Configuration > Azure AD.

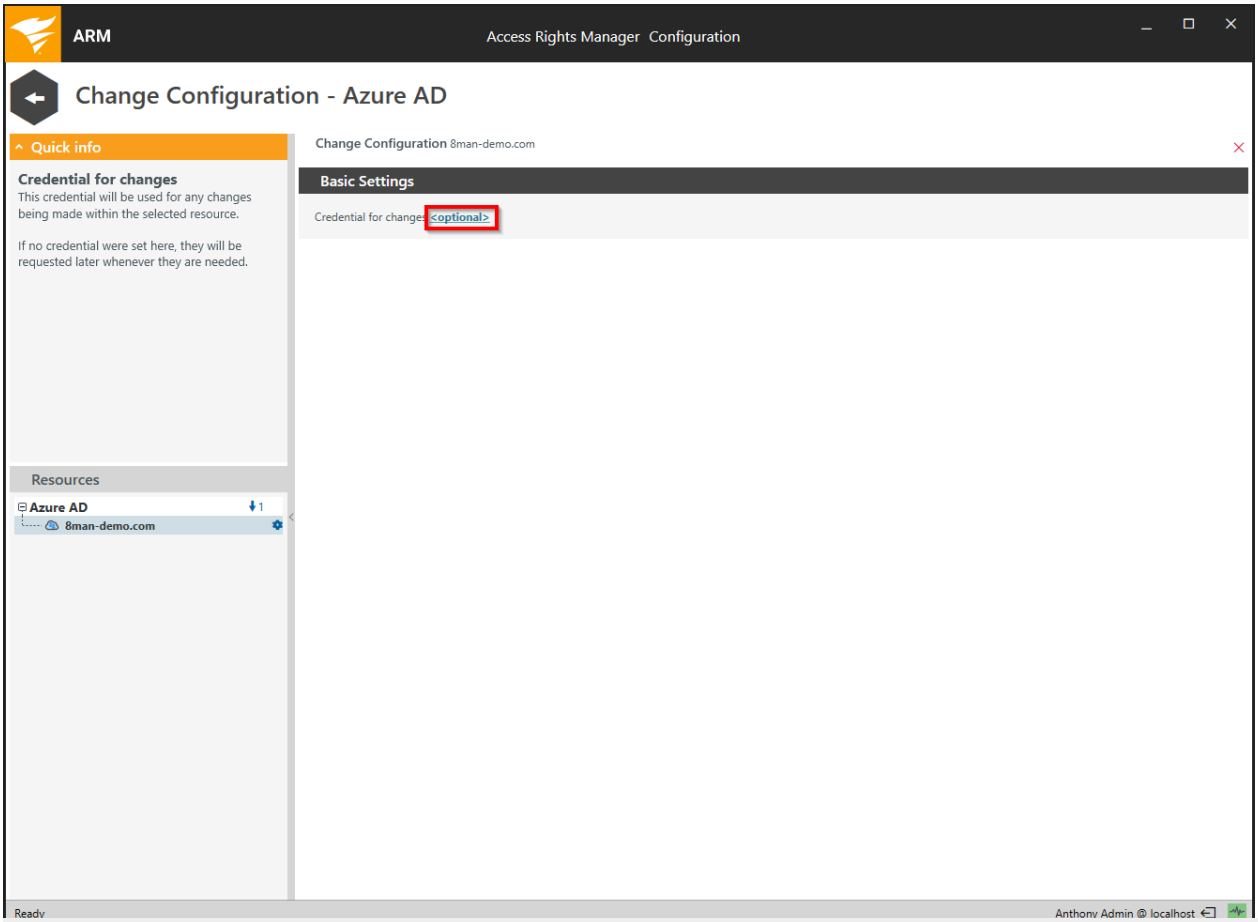
You must have run at least one AAD scan to create a change configuration.

Add an AAD change configuration



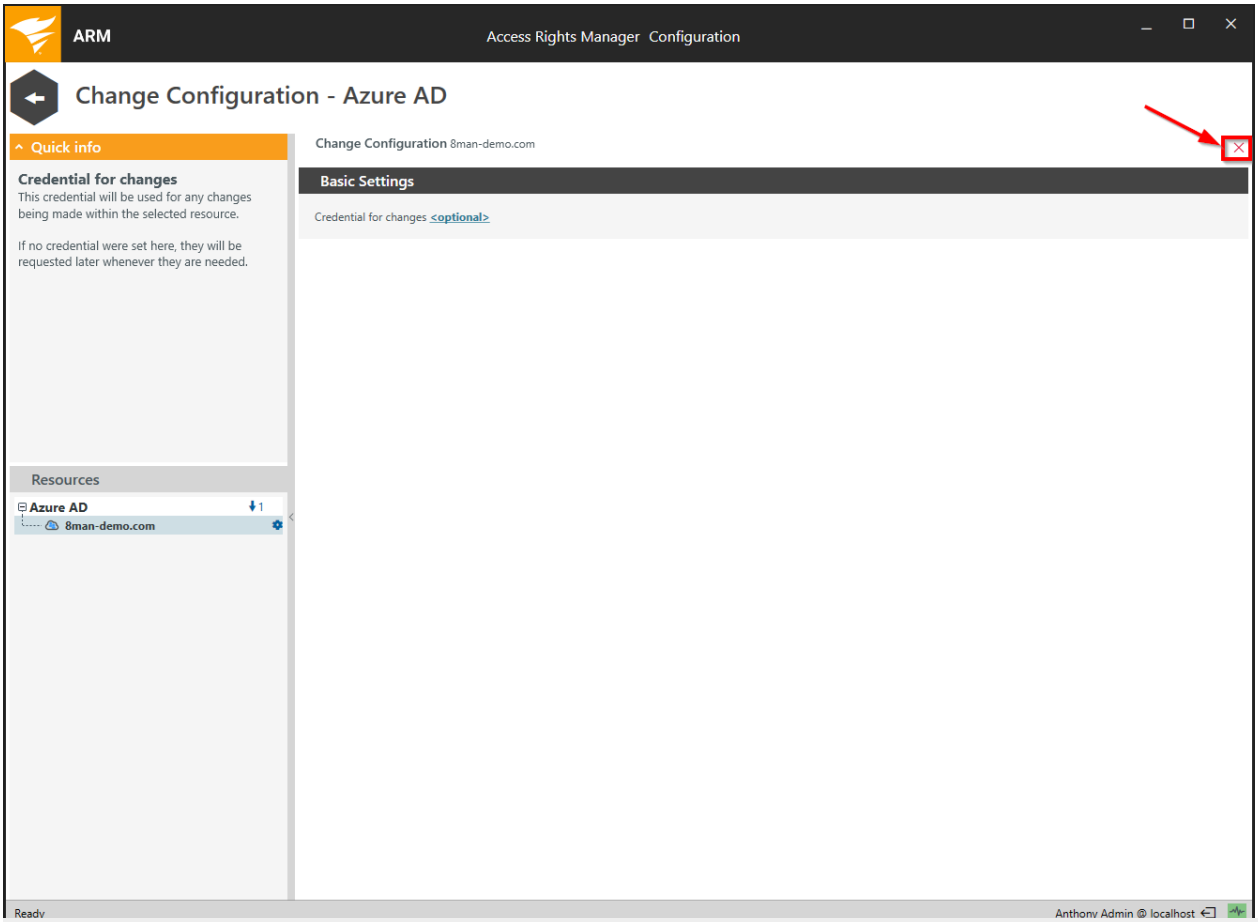
1. Select an AAD resource.
2. Click the plus icon.

Modify an AAD change configuration



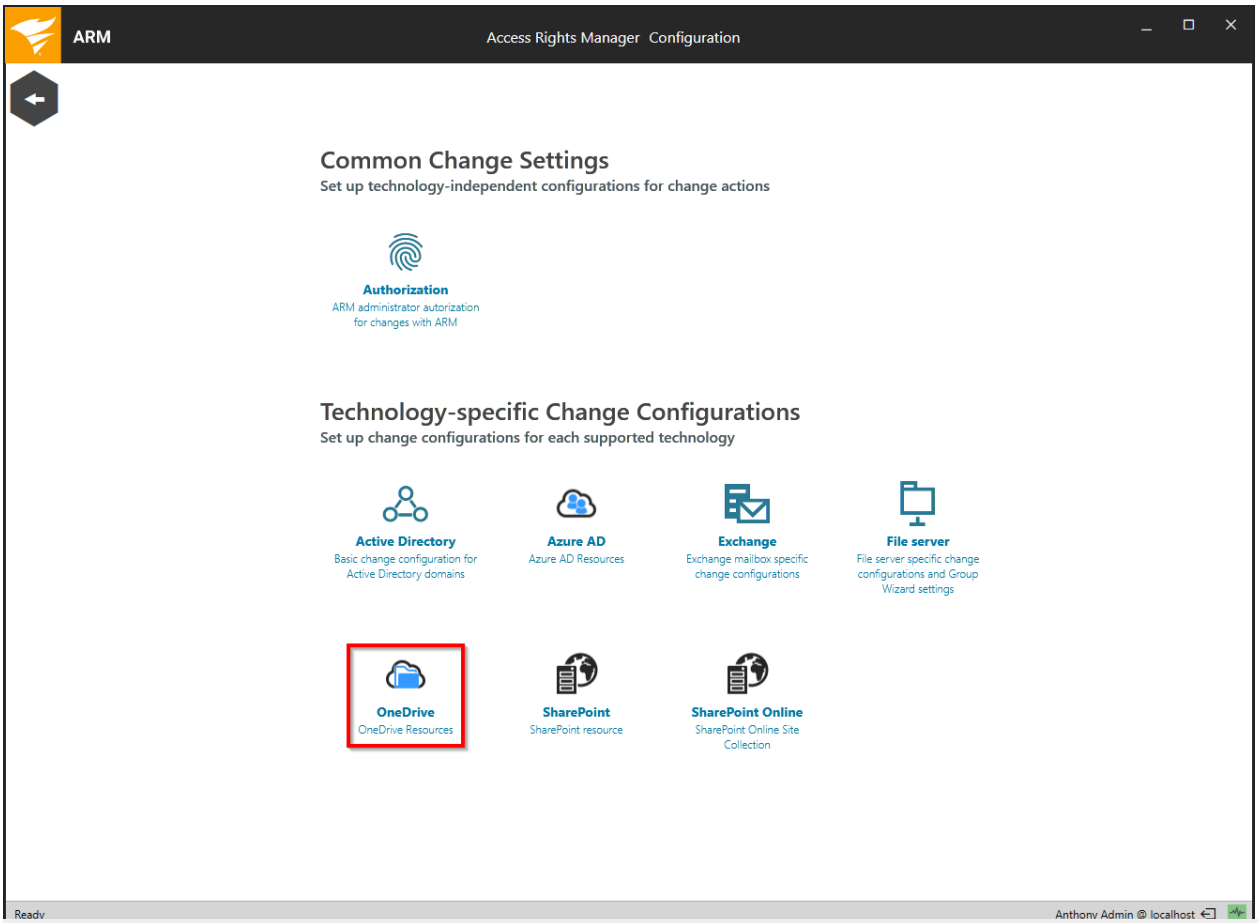
Specify which credentials are used to make changes to the AAD resource.
If you do not specify any, ARM users are prompted for each change.

Delete an AAD change configuration



Click on the red cross to delete an AAD Change configuration.

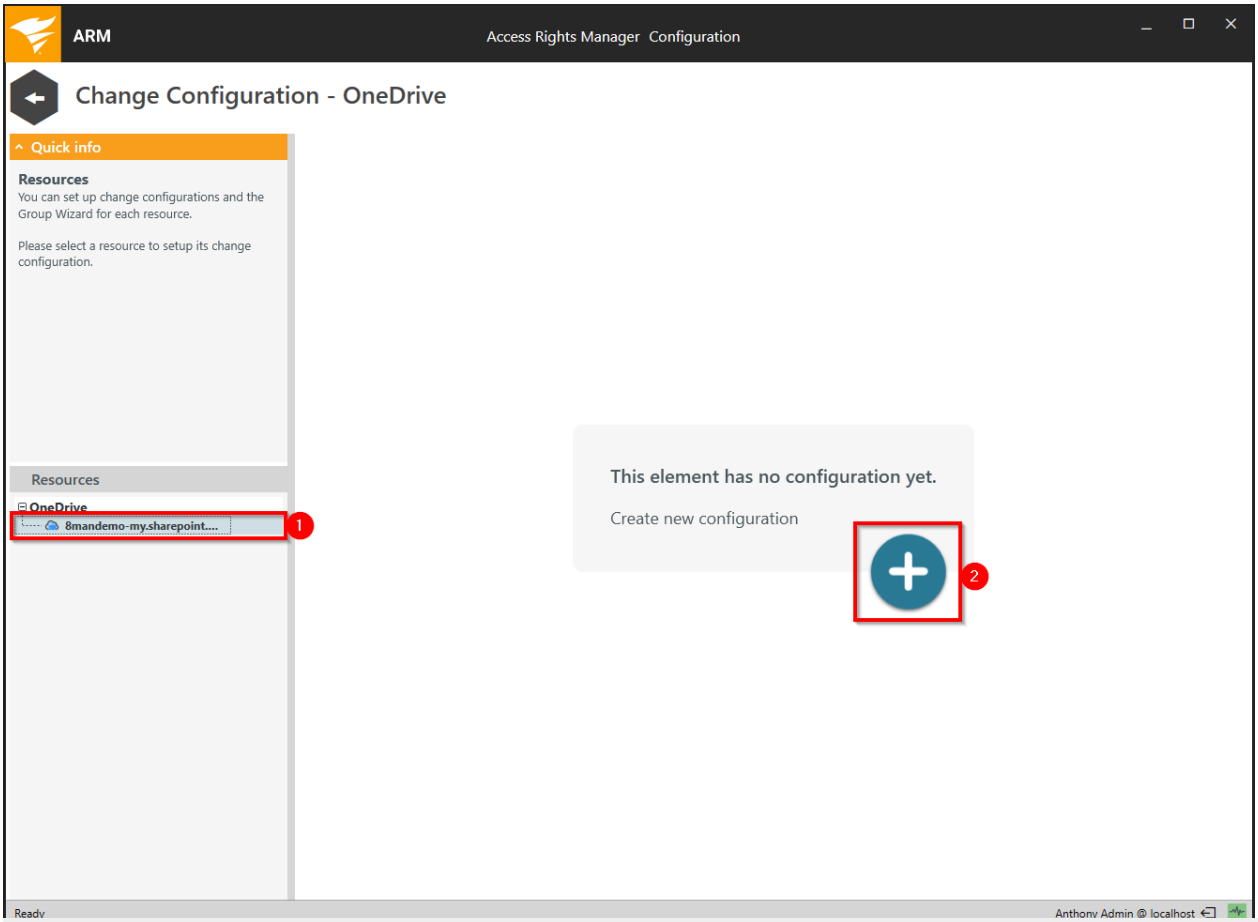
OneDrive change configuration



In the ARM configuration, navigate to Change Configuration > OneDrive.

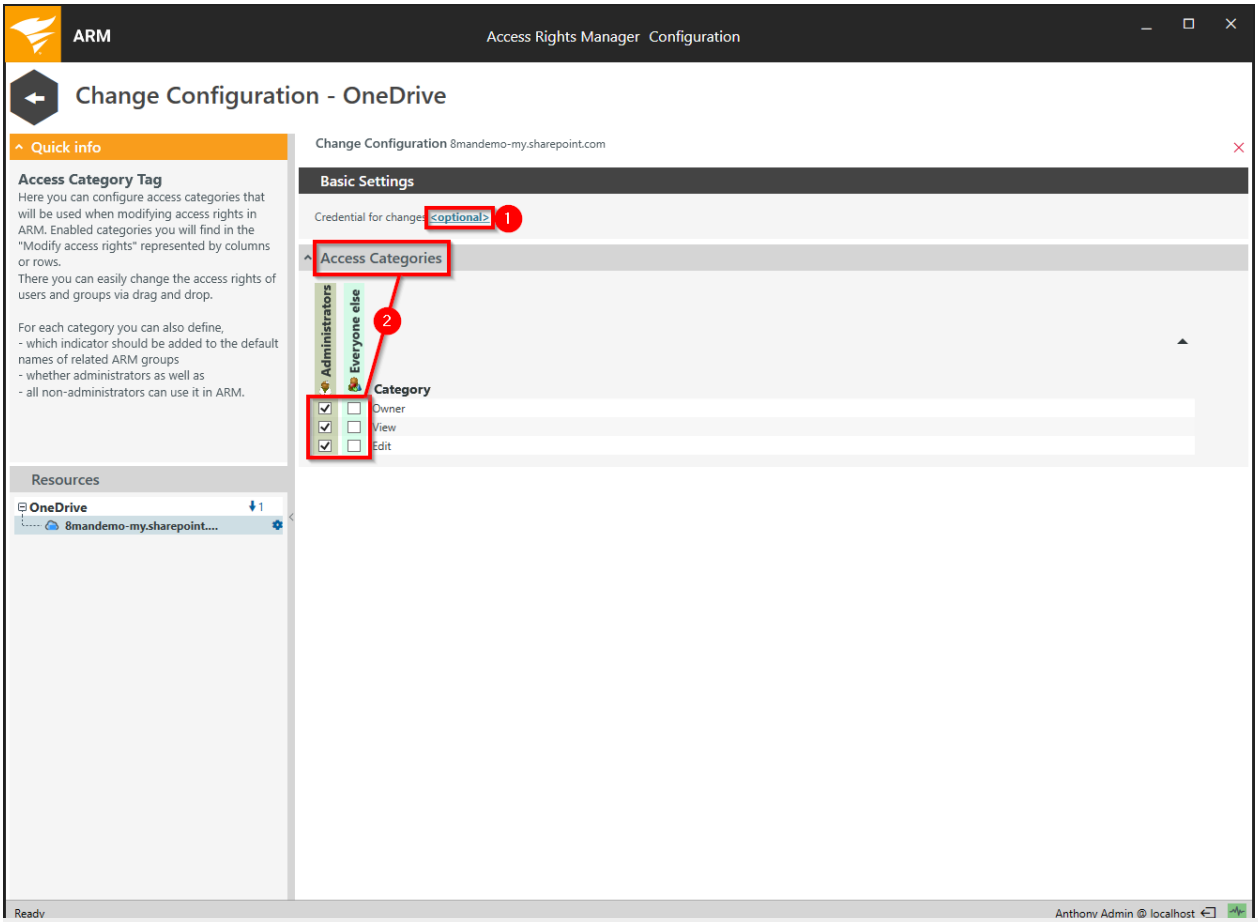
You must have run at least one OneDrive scan to create a change configuration.

Add a OneDrive change configuration



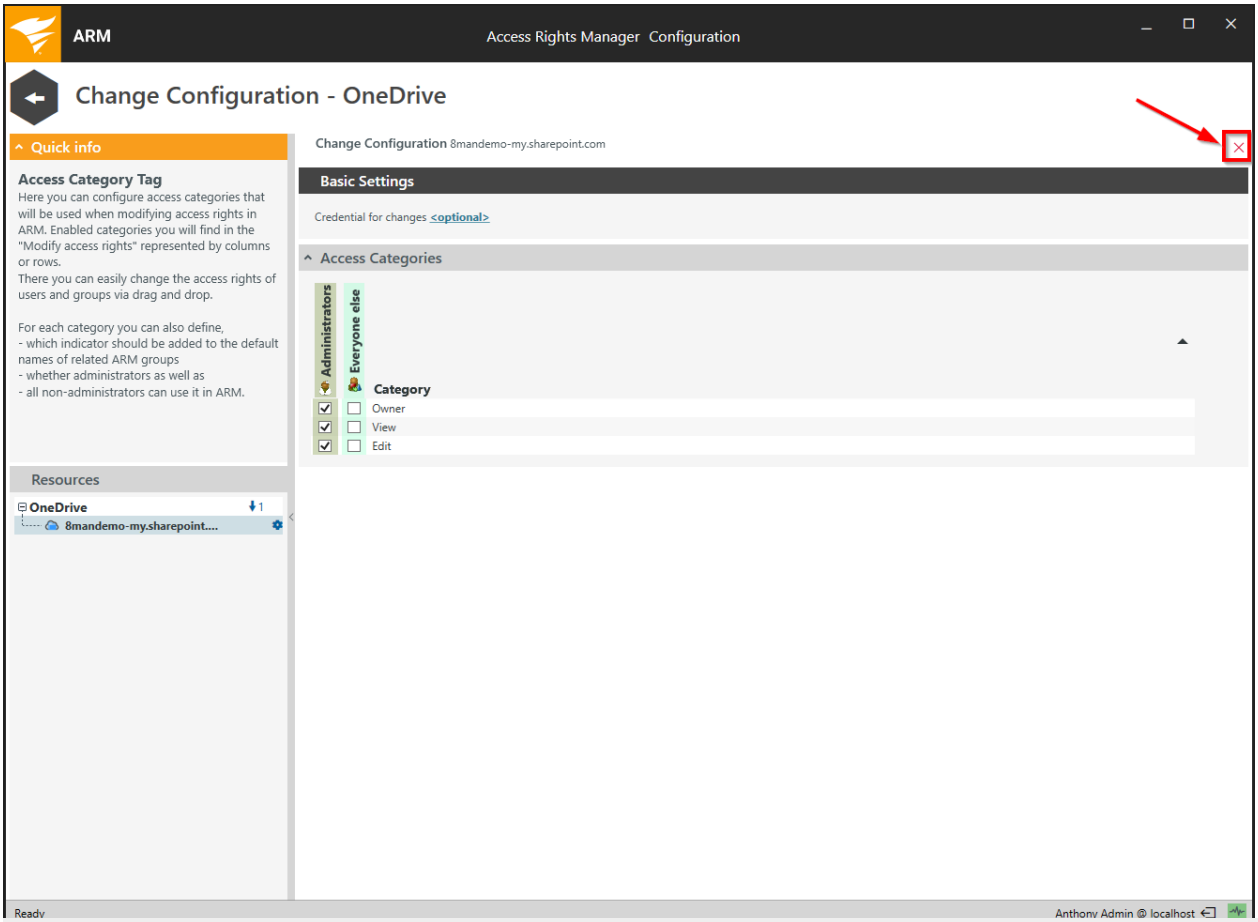
1. Select a OneDrive resource.
2. Click the plus icon.

Modify a OneDrive change configuration



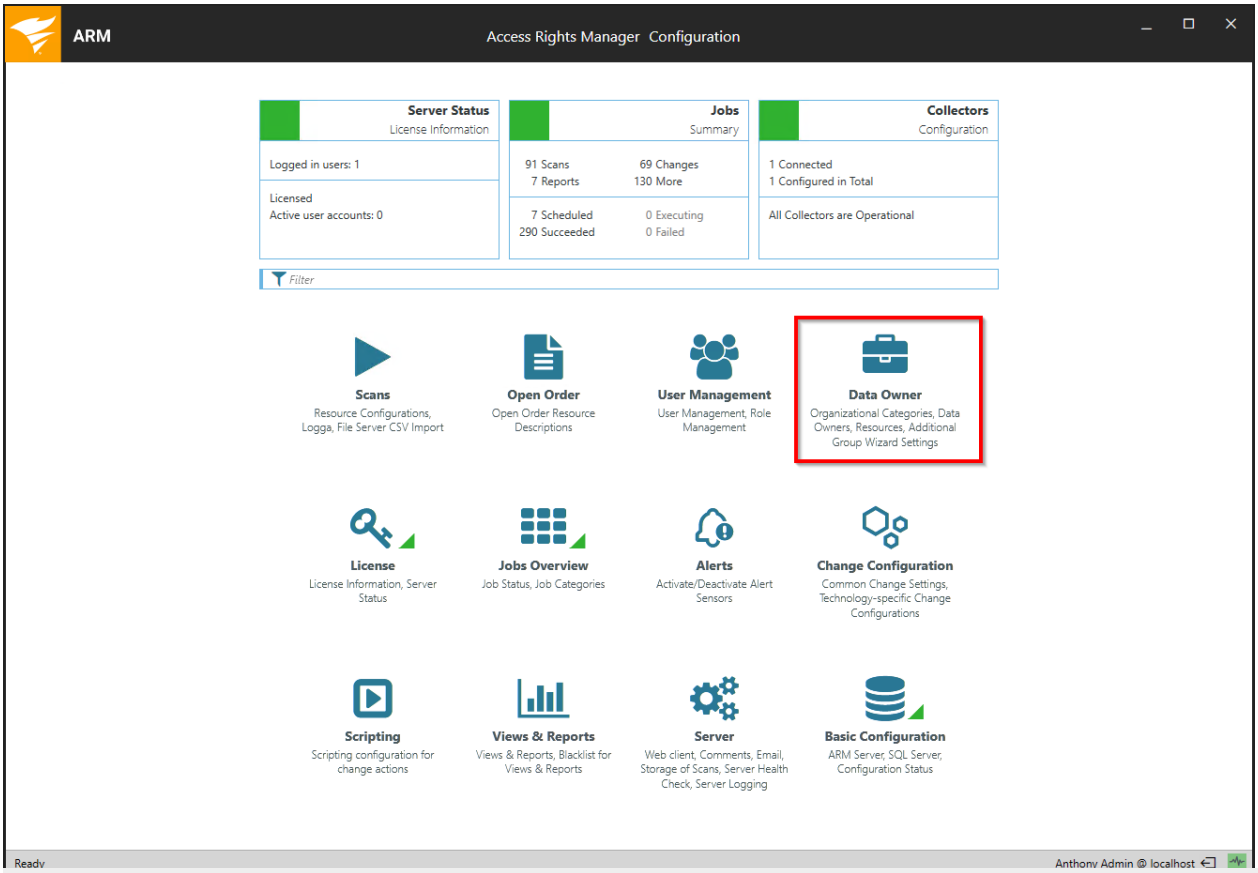
1. Specify which credentials are used to make changes to the OneDrive resource.
   If you do not specify any, the ARM users are prompted for each change.
2. Determine which access categories are available for ARM users to change access rights. Define a set for ARM administrators and another for all ARM modify user roles (See also: manage ARM users).

Delete a OneDrive change configuration



Click on the red cross to delete a OneDrive change configuration.

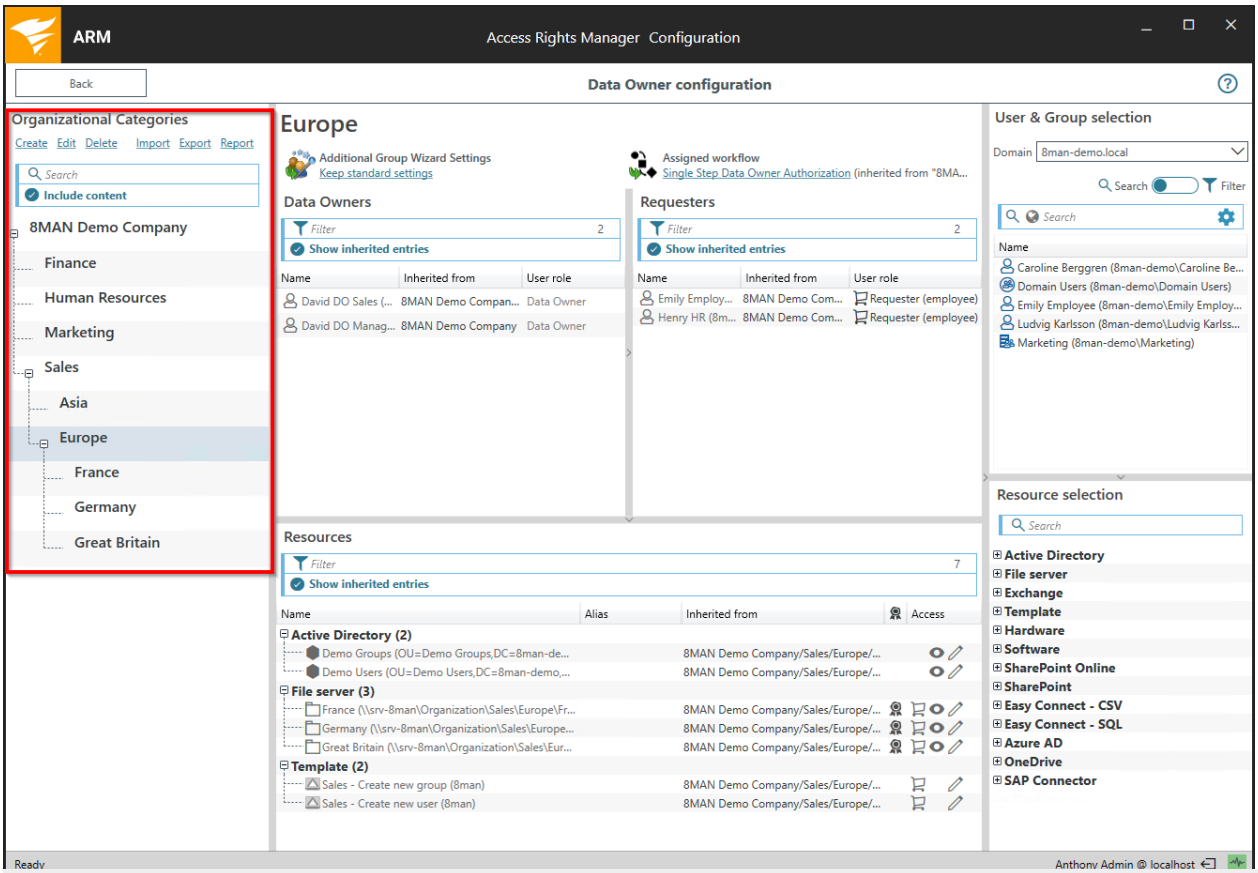
Data owner



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.

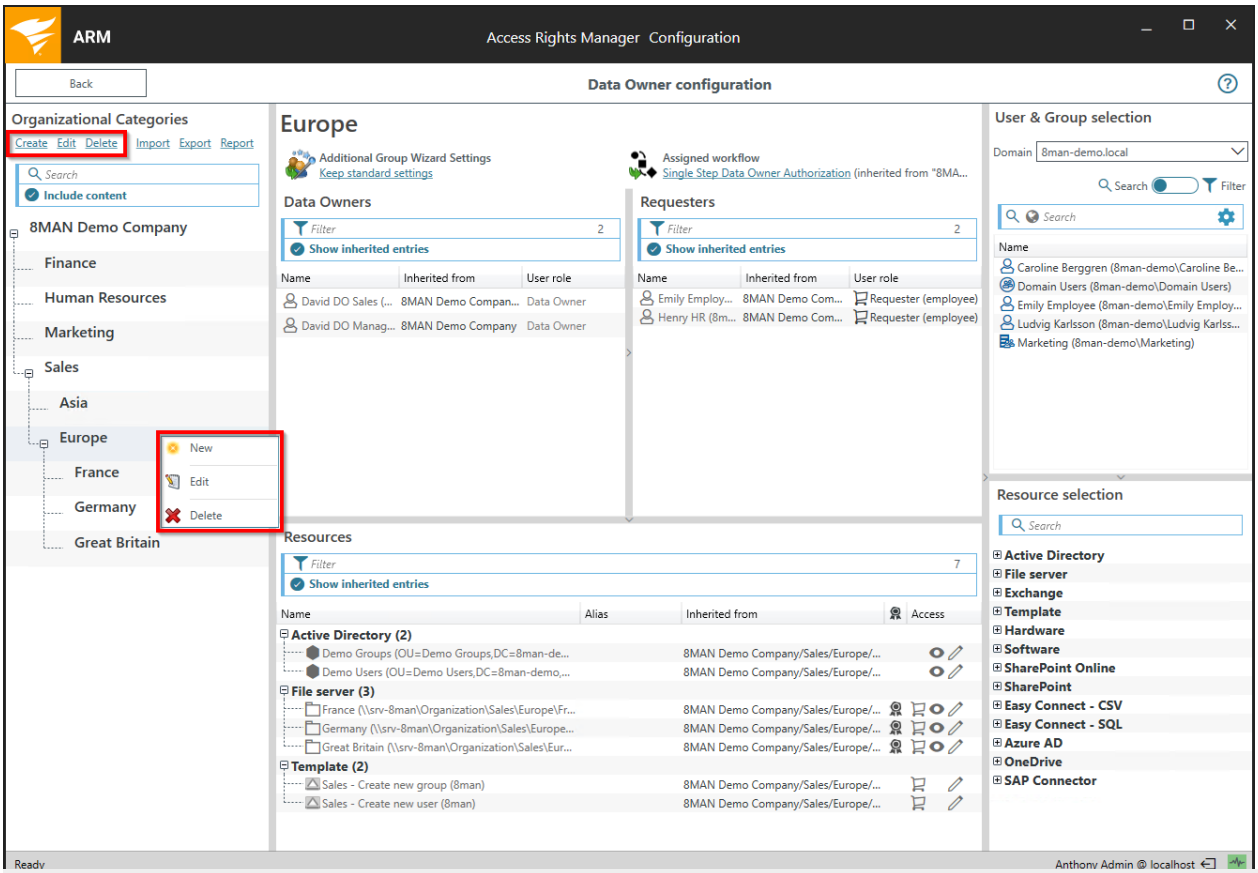
Create organizational categories



You use the organizational categories to bundle resources in containers that the data owners manage.

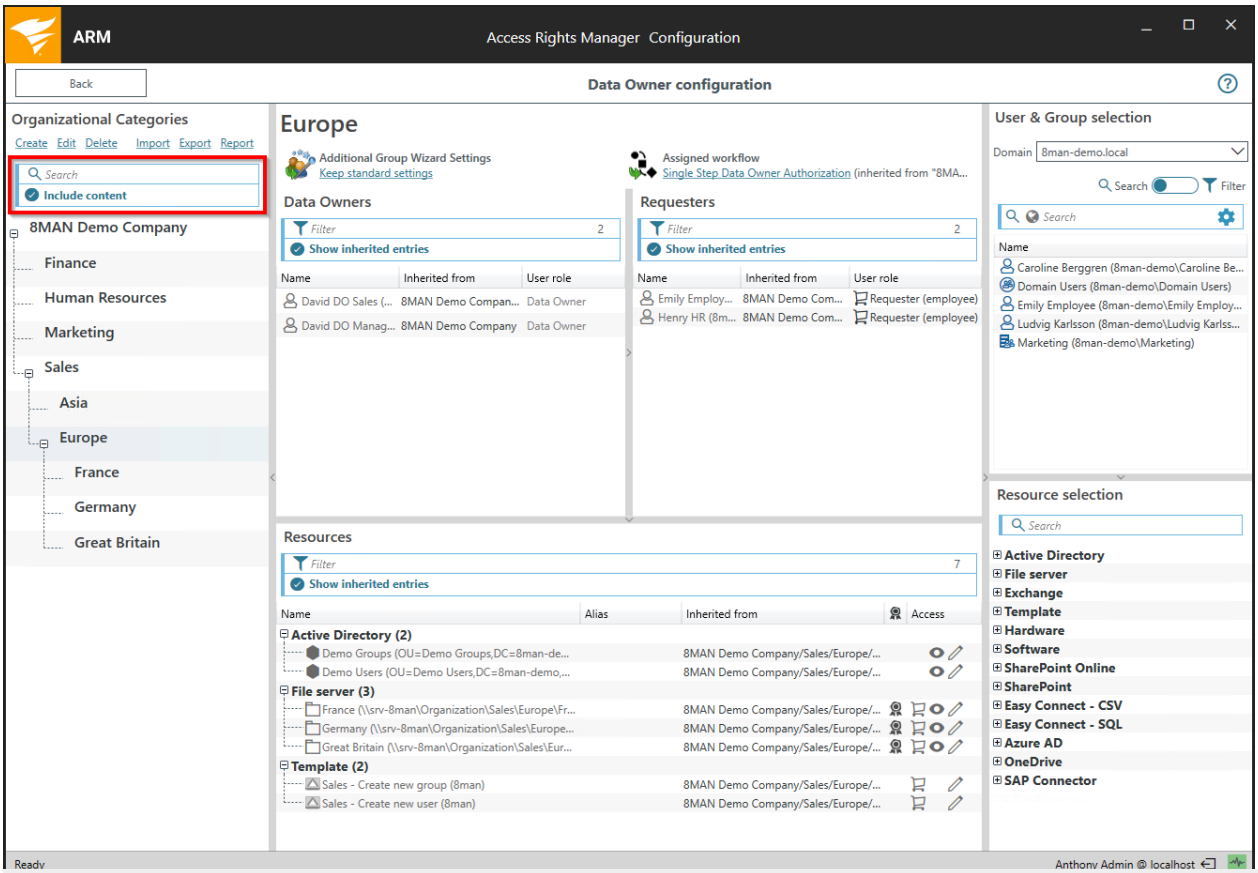
Create structures and hierarchies similar to your companies org chart.

You can add a description to all organizational categories.



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.

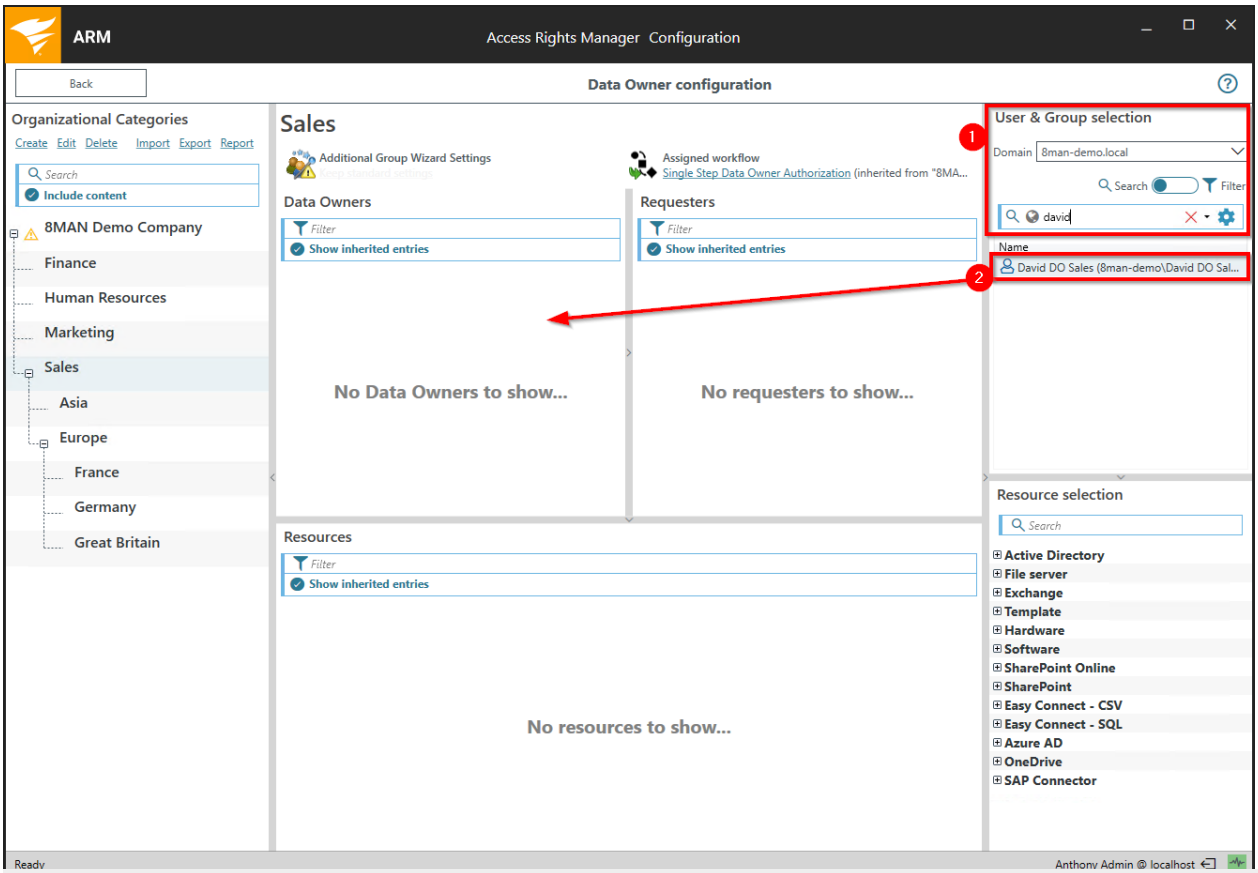


Search the organizational categories.

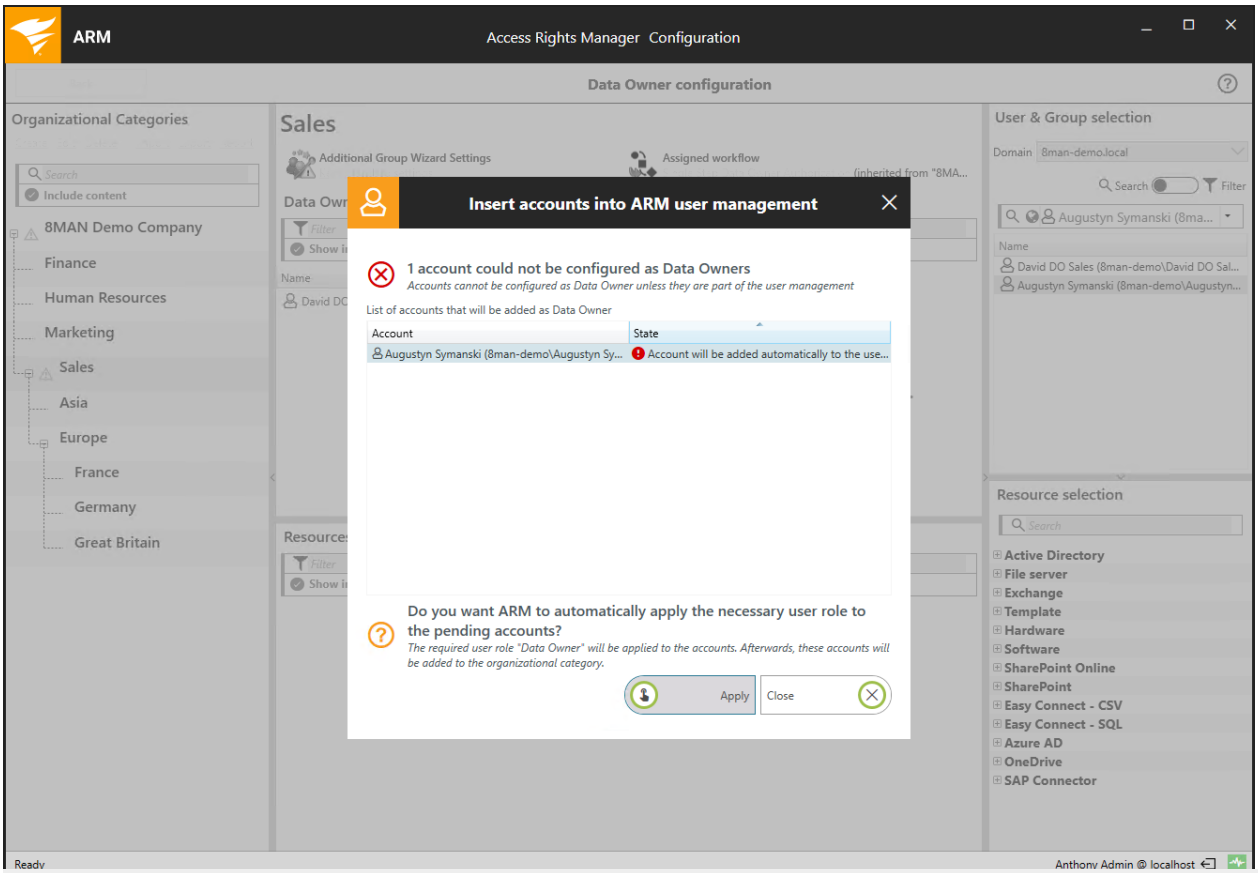
Option "Include content" deactivated:
The search is only applied to names and descriptions of the organizational category.

Option "Include content" activated:
The search also includes Data Owners and resources.

Assign a Data Owner to an organizational category



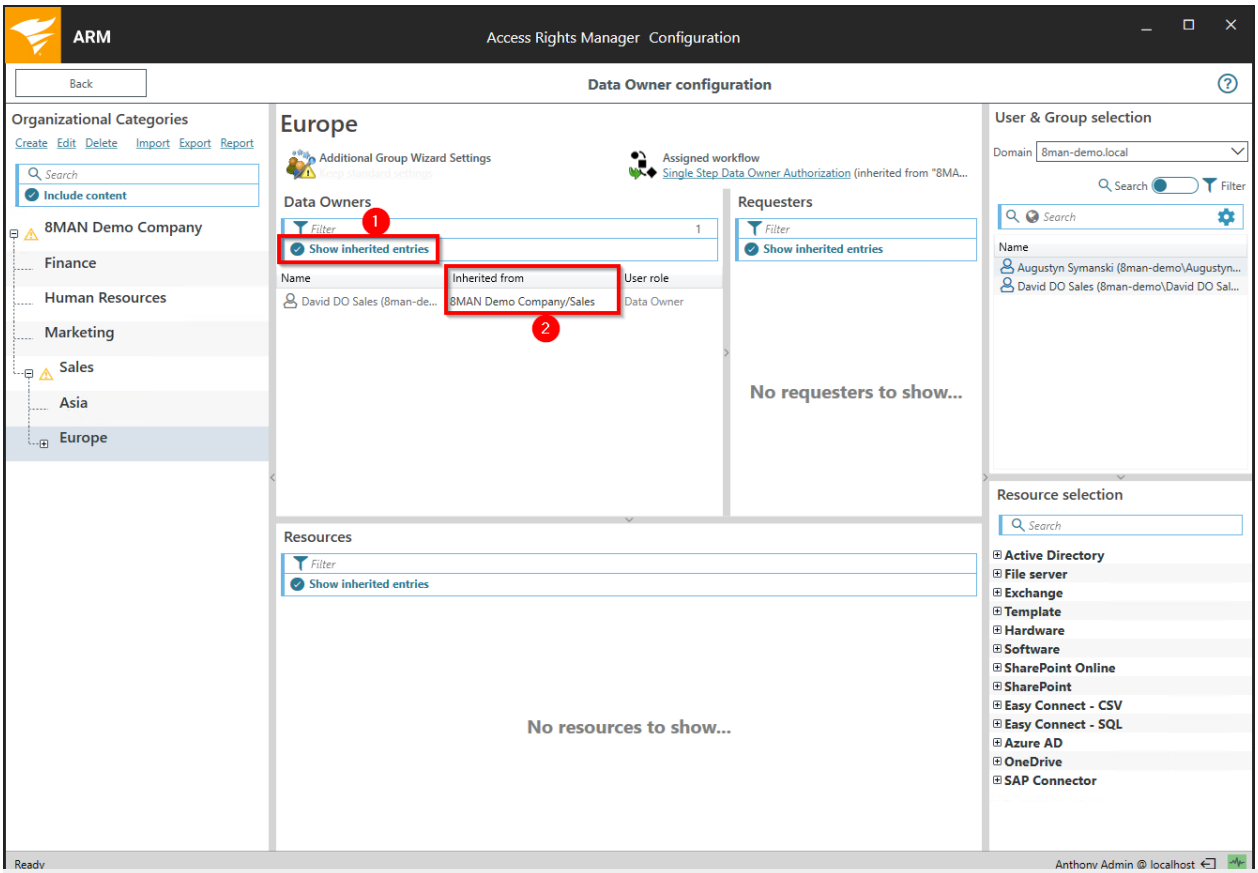
1. Use the search and filter options to find the desired users and groups.
2. Use drag & drop to add the selected entries as data owners.



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.

ARM-Admin roles can not be configured as Data Owners.

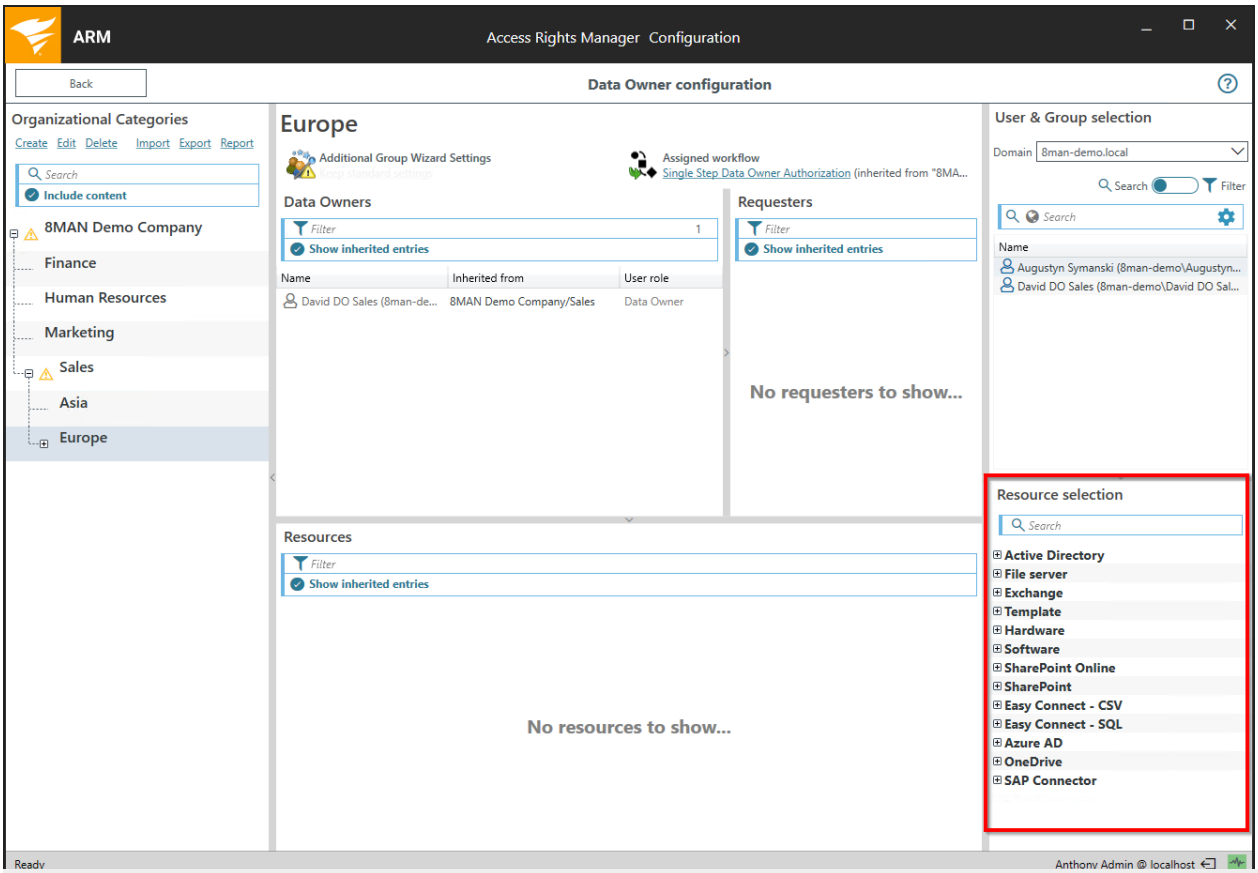


Hierarchy rule:

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

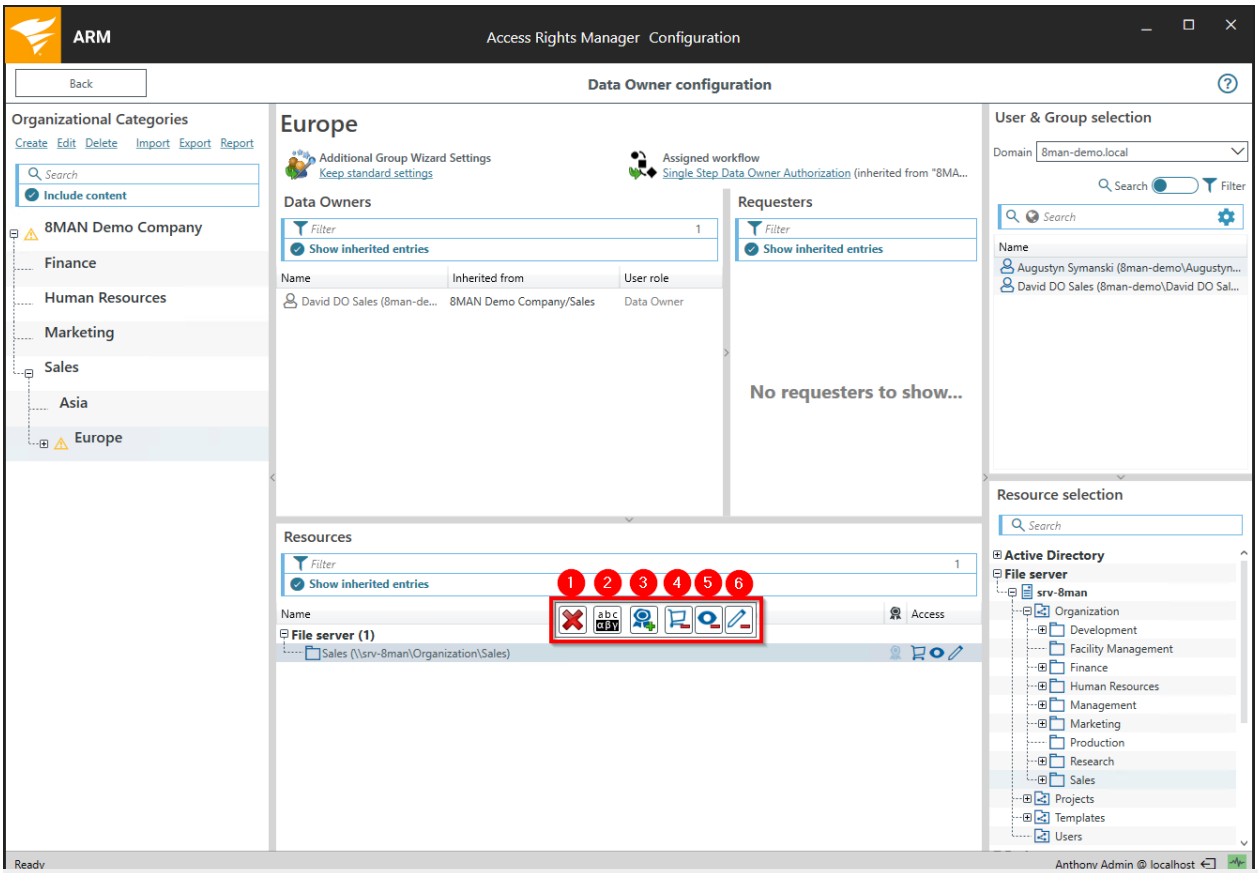


Select the desired resource and add it to the organizational category via drag & drop or by double-clicking on it.

> You can only add resources which have been scanned.

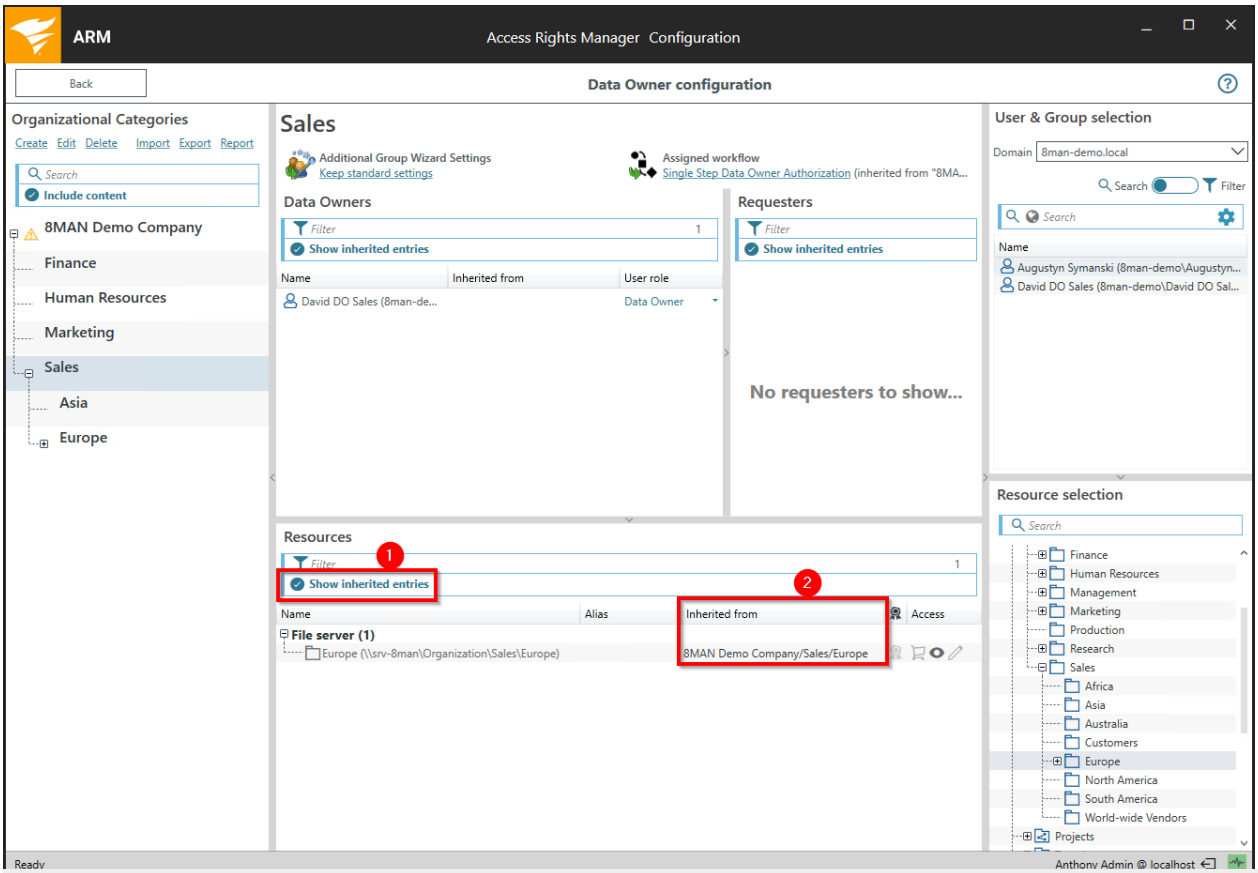
Open order resources such as "template", "hardware" or "software" can only be added if:

- you have the required license
- you have imported an open order configuration.



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.

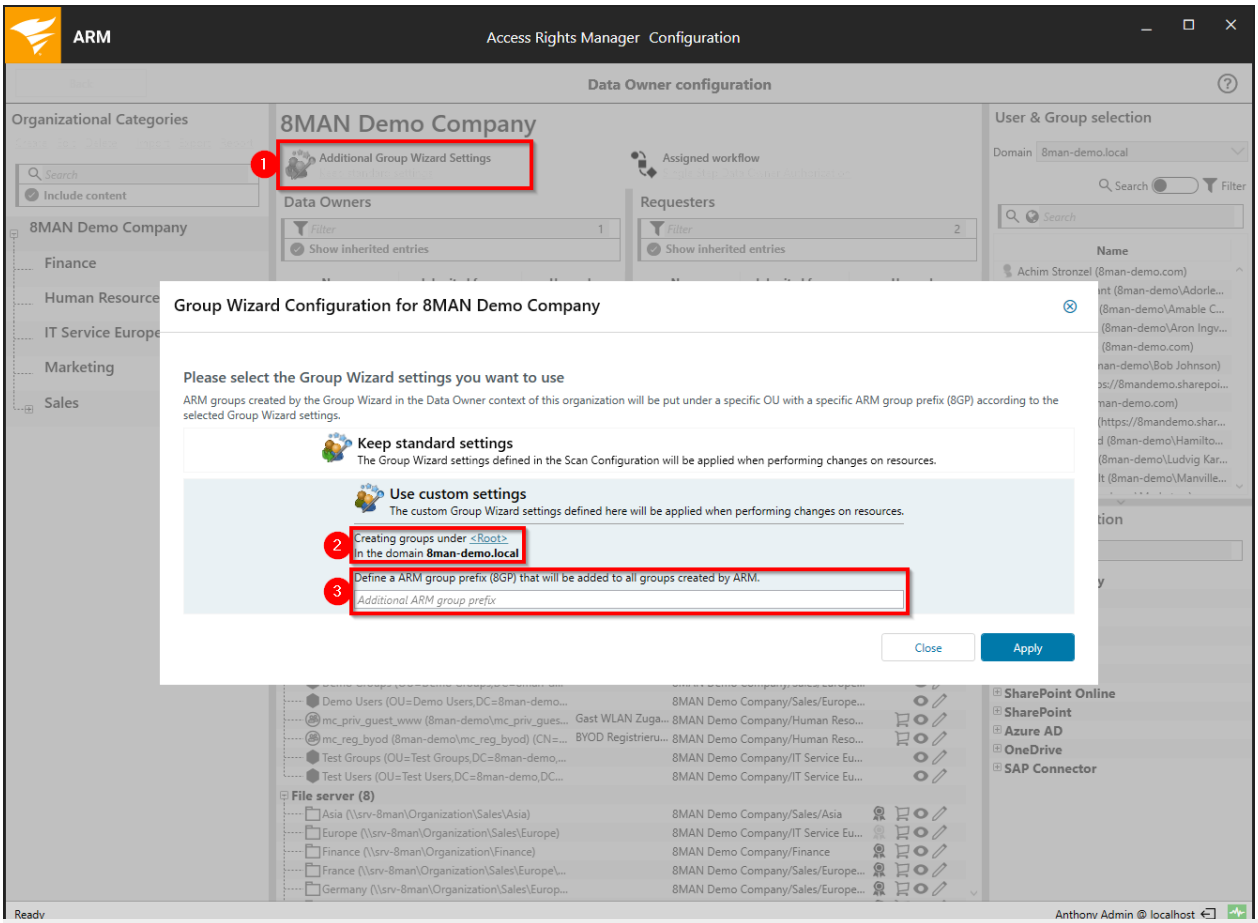


Hierarchy rule:

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



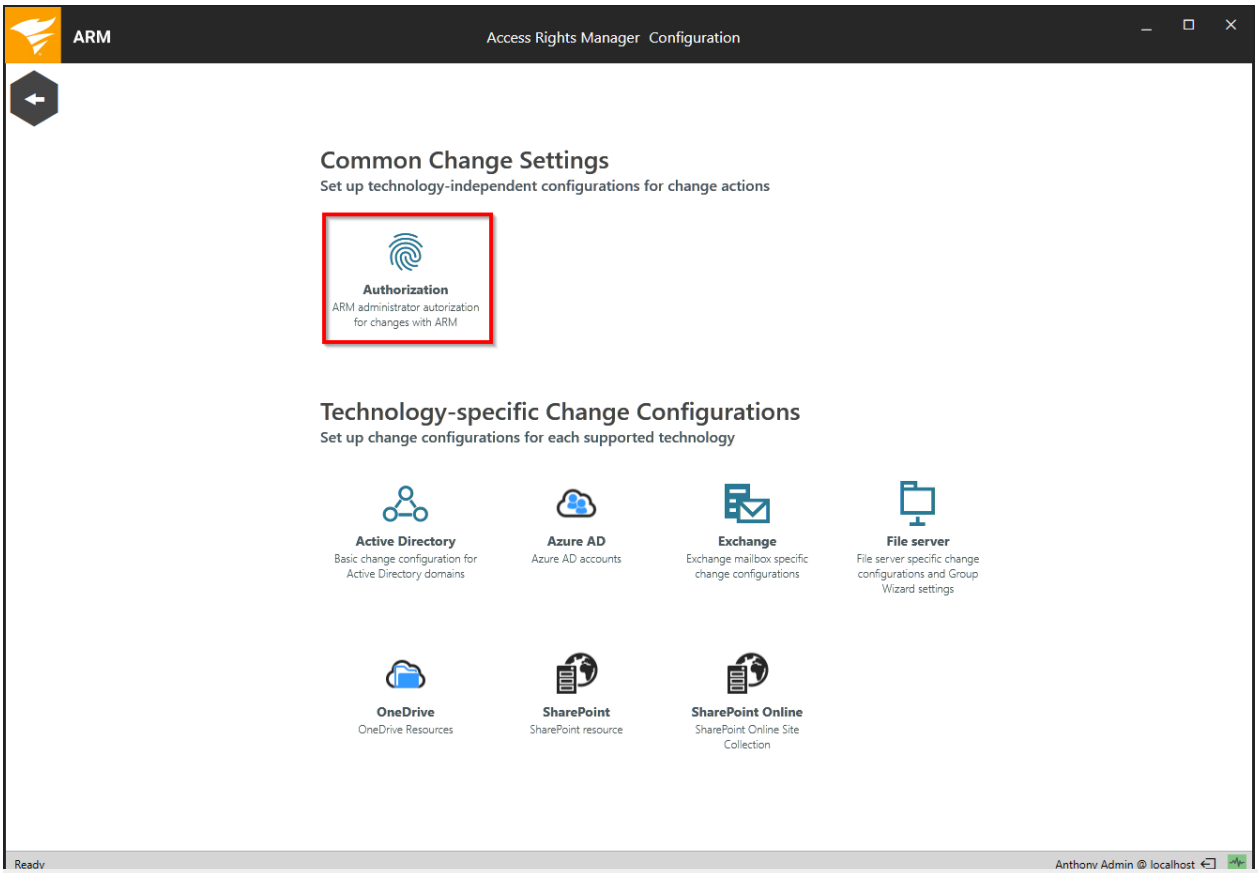
1. You can modify the group wizard configuration for every organizational category.

This allows you to use

2. separate OUs and
3. specific prefixes for group names

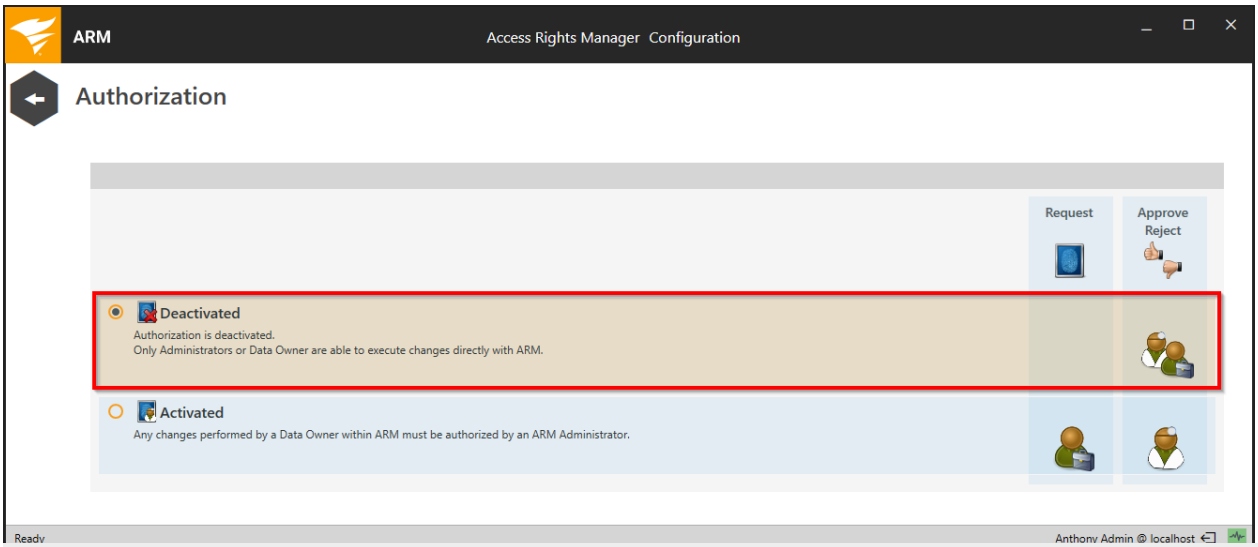
for ARM groups that are created by Data Owners.

Activate or deactivate simple approvals for Data Owners



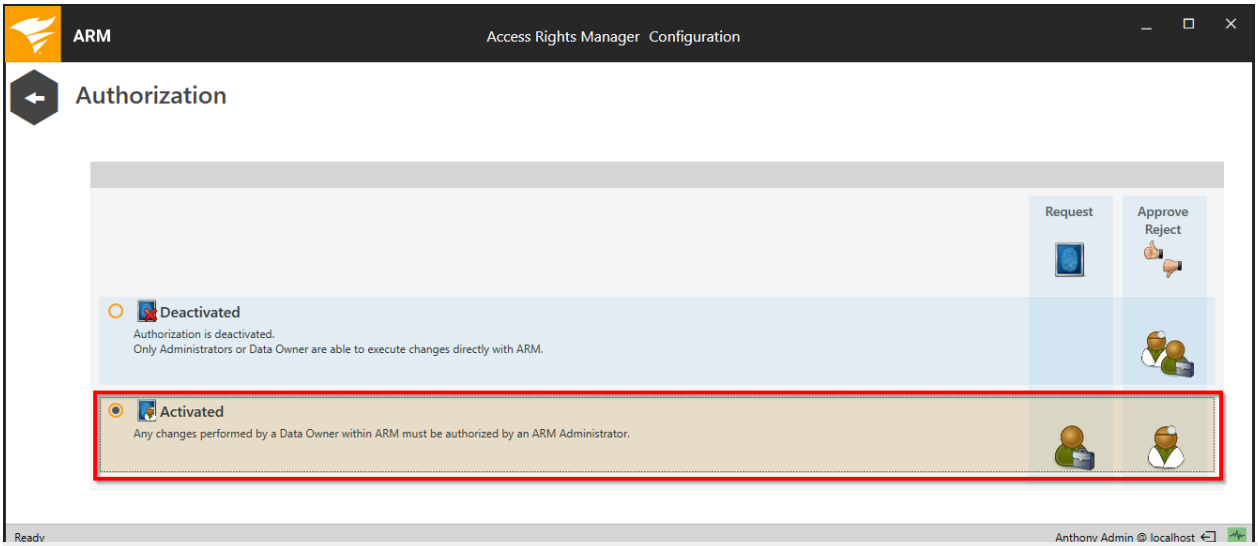
In the ARM Configuration application, click Change Configuration > Authorization.

⚠ The authorization settings do not affect GrantMA workflows.



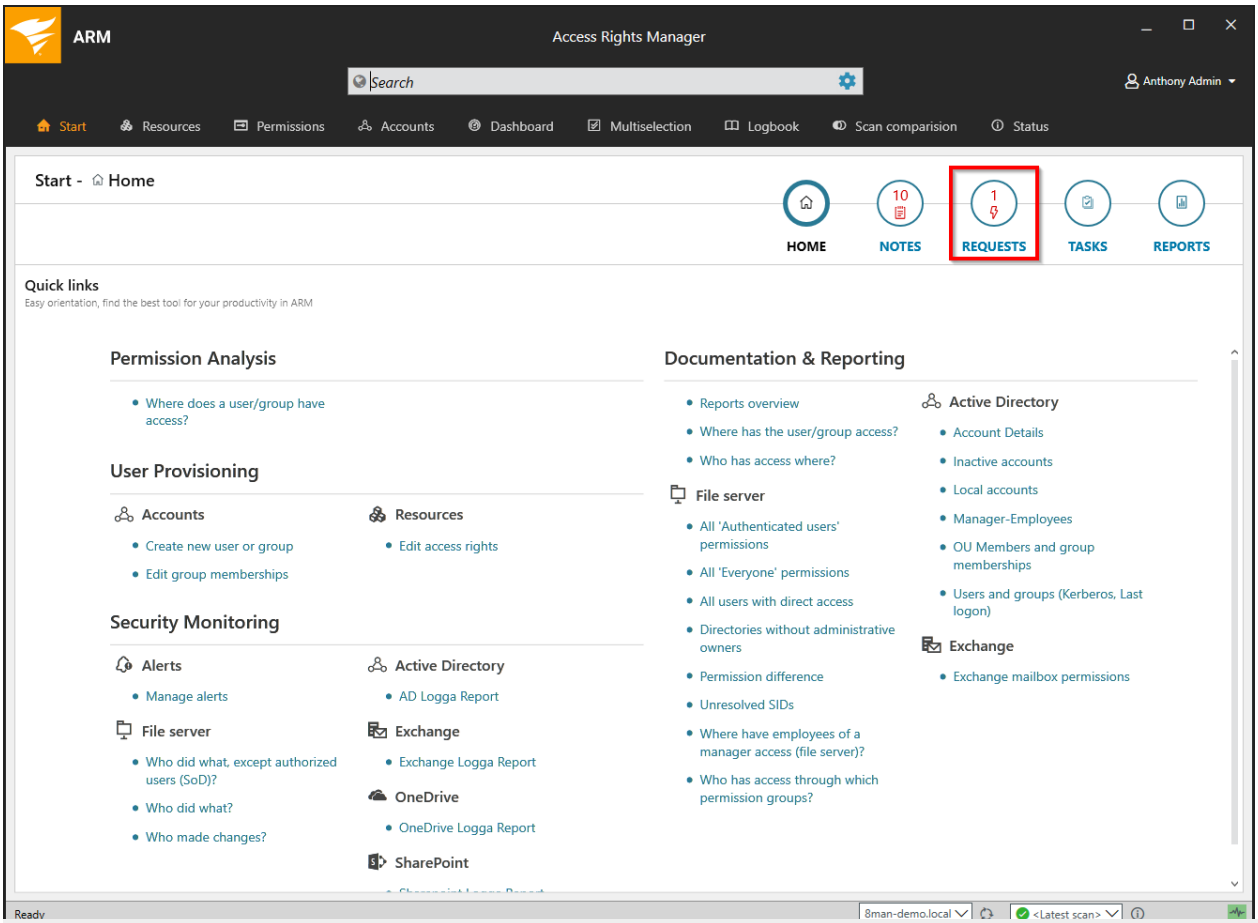
Option "Deactivated":

ARM executes changes made by data owners without further approval.



Option "Activated":

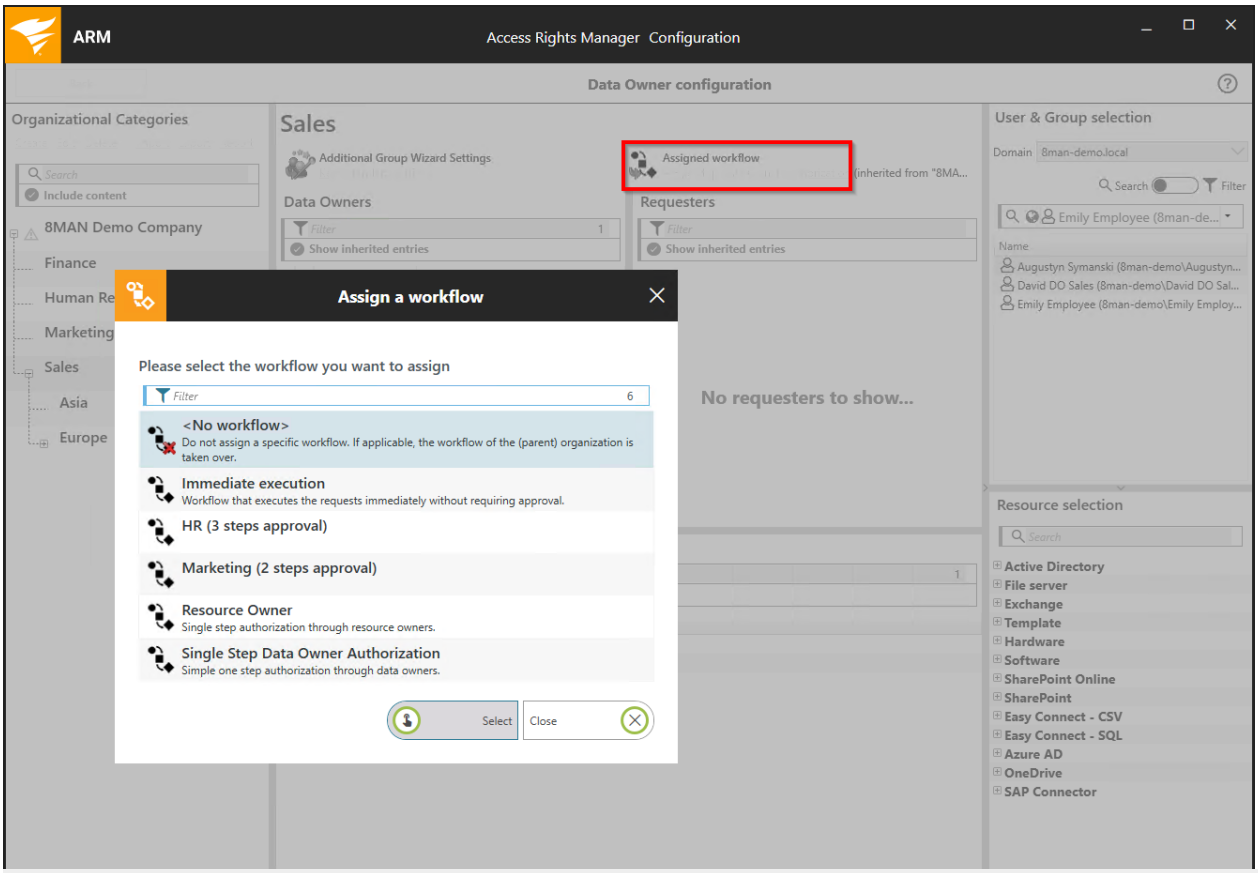
Changes made by Data Owners must be approved by an ARM Administrator.



ARM administrators must log on to the ARM application and click on "Requests" on the start page to find open approval requests.

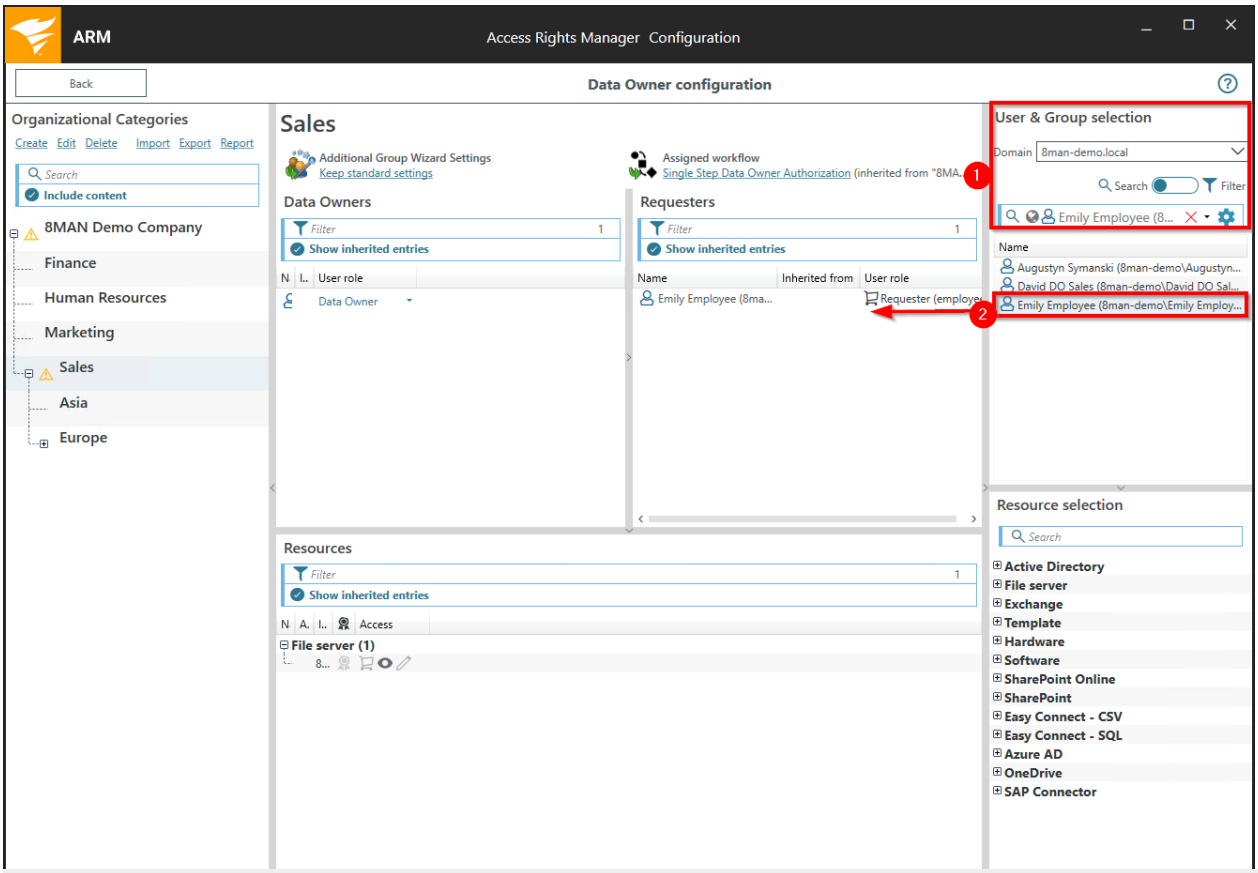
Simple approvals without GrantMA do not include any active notification functionality.

Data Owner configuration and GrantMA

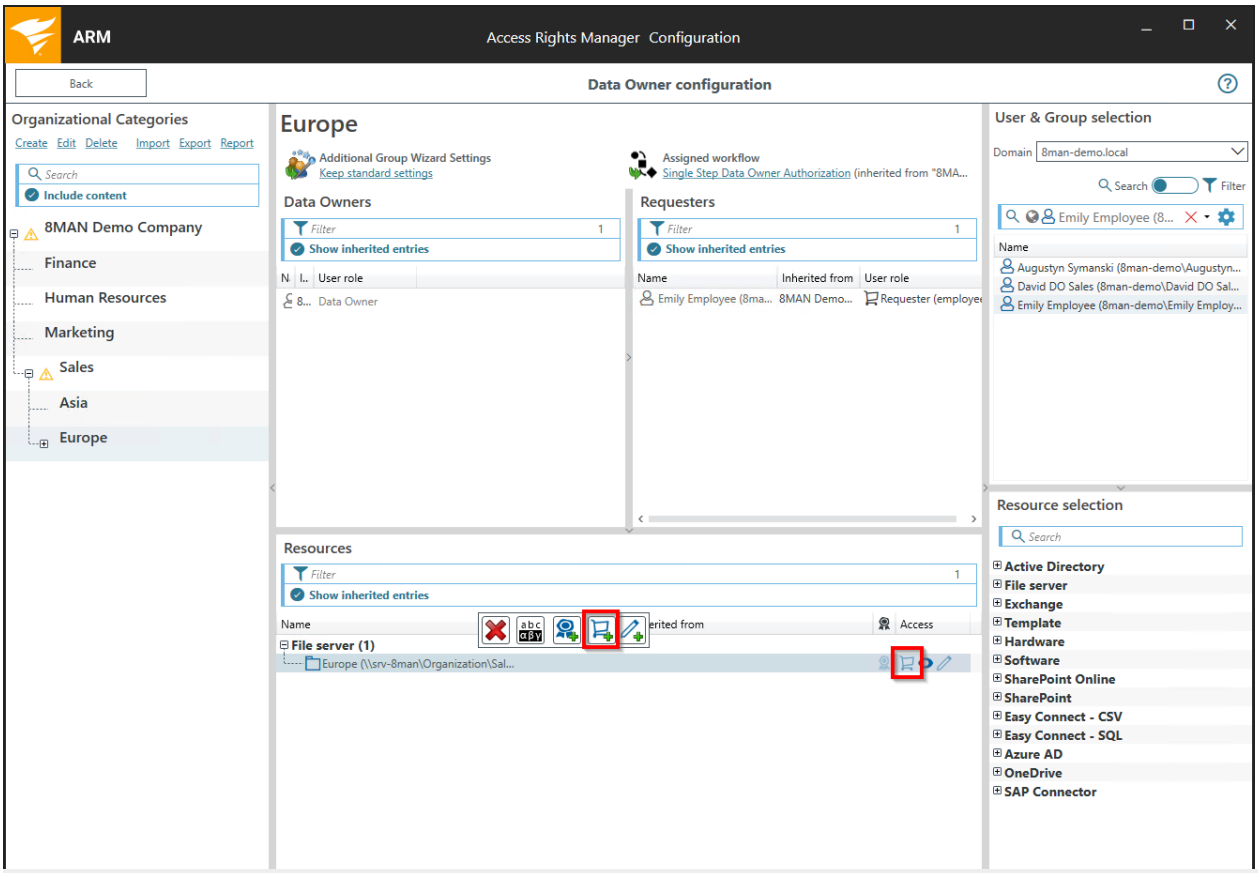


Assign a workflow for an organizational category. In this way, you can use different workflows with different approval steps for each organizational category.

Workflows are created in the GrantMA web interface. See: GrantMA: Design approval processes

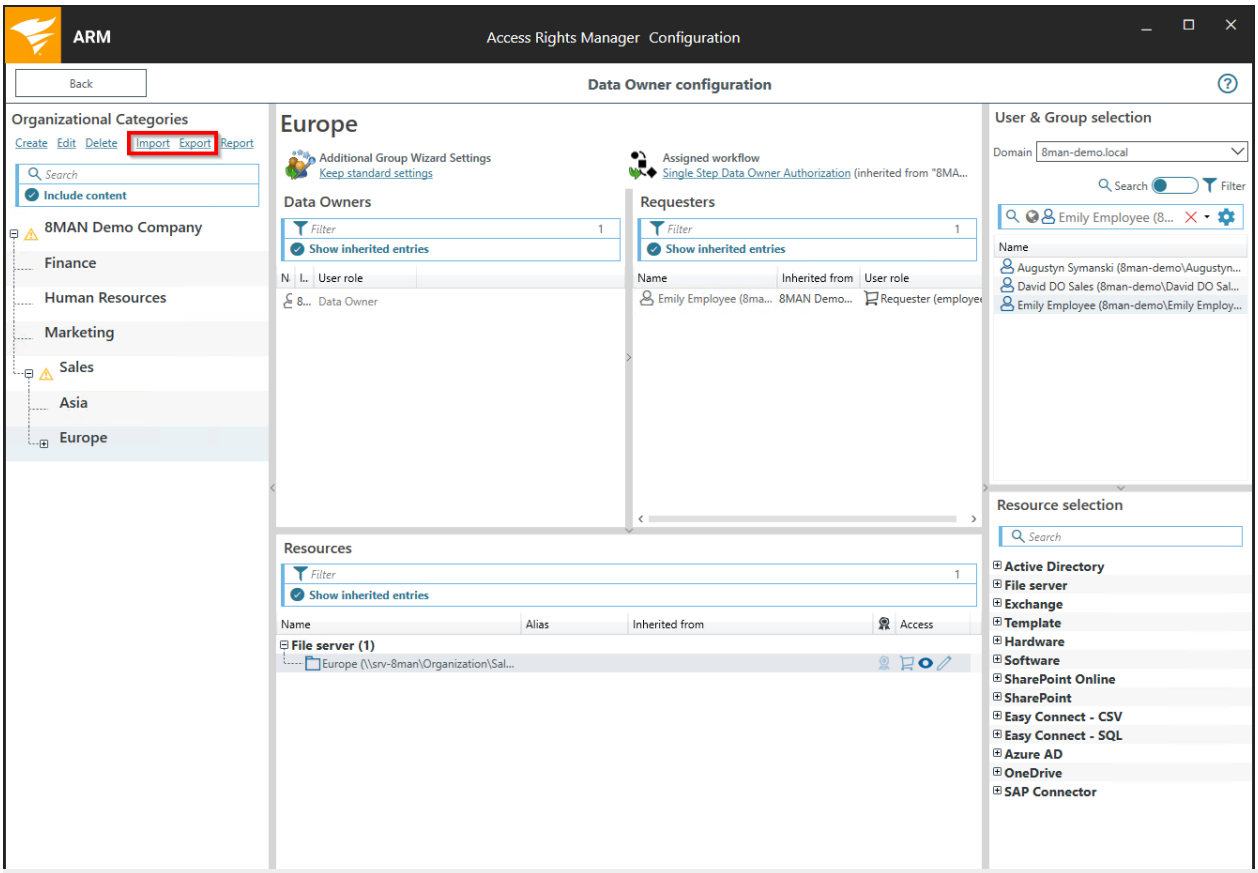


1. Select a user or group from the account selection area.
2. Add your selection to the "Requester" section via drag & drop.



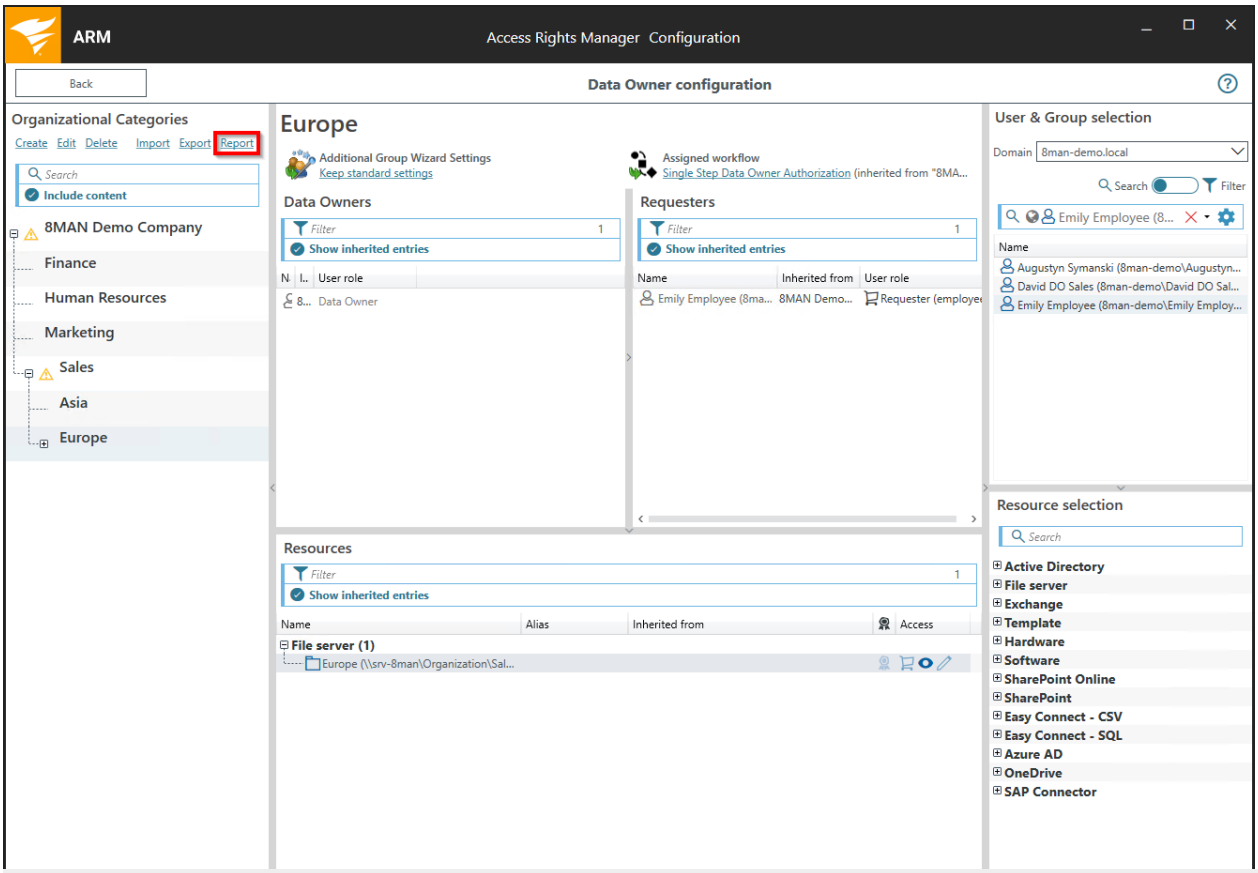
Mark the resources as requestable, so they can be ordered in the GrantMA web interface.

Import or export Data Owner configurations

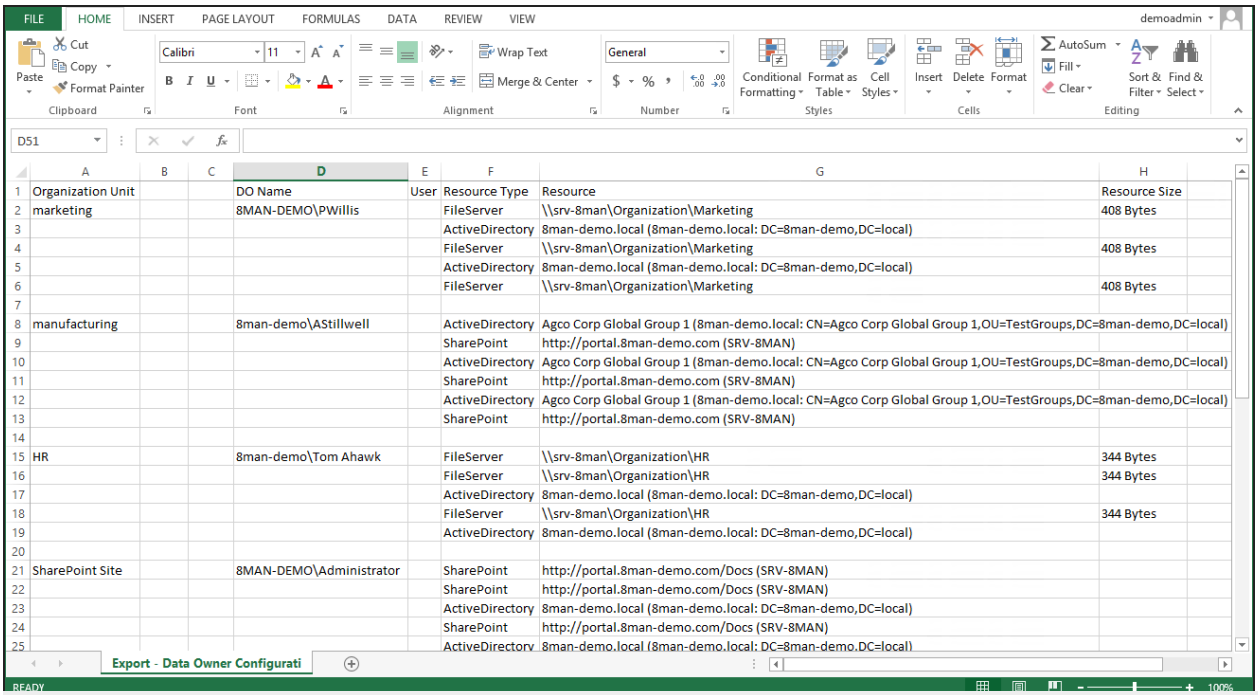


You can export an existing Data Owner configuration in order to be able to perform bulk operations or a transfer to and from other systems (for example from testing to productive).

Create a Data Owner configuration report



You can create a Data Owner configuration report in CSV format.

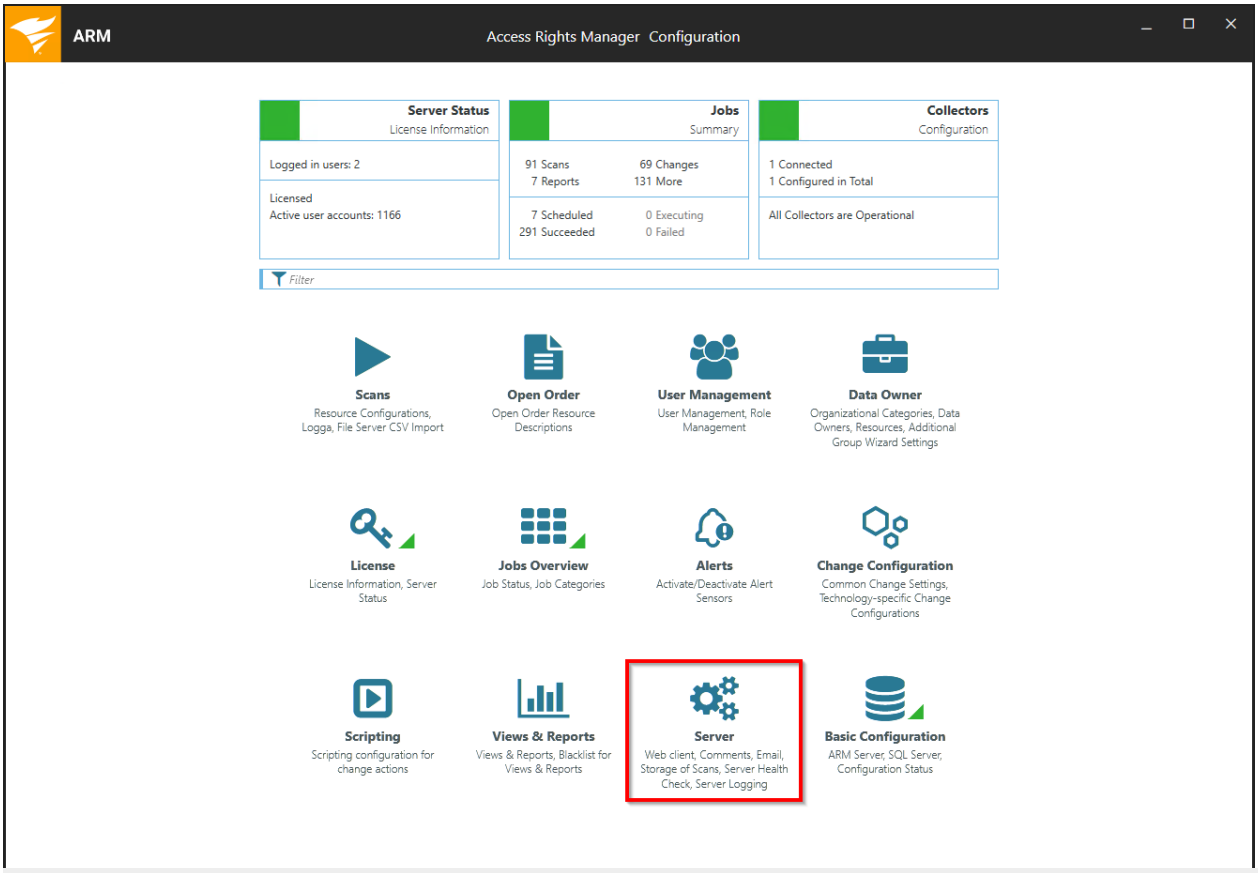


Organization Unit	DO Name	User	Resource Type	Resource	Resource Size
marketing	8MAN-DEMO\PWillis		FileServer	\\srv-8man\Organization\Marketing	408 Bytes
			ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)	
			FileServer	\\srv-8man\Organization\Marketing	408 Bytes
			ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)	
			FileServer	\\srv-8man\Organization\Marketing	408 Bytes
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)	
			SharePoint	http://portal.8man-demo.com (SRV-8MAN)	
			ActiveDirectory	Agco Corp Global Group 1 (8man-demo.local: CN=Agco Corp Global Group 1,OU=TestGroups,DC=8man-demo,DC=local)	
			SharePoint	http://portal.8man-demo.com (SRV-8MAN)	
			ActiveDirectory	Agco Corp Global Group 1 (8man-demo.local: CN=Agco Corp Global Group 1,OU=TestGroups,DC=8man-demo,DC=local)	
			SharePoint	http://portal.8man-demo.com (SRV-8MAN)	
HR	8man-demo\Tom Ahawk		FileServer	\\srv-8man\Organization\HR	344 Bytes
			FileServer	\\srv-8man\Organization\HR	344 Bytes
			ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)	
			FileServer	\\srv-8man\Organization\HR	344 Bytes
			ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)	
SharePoint Site	8MAN-DEMO\Administrator		SharePoint	http://portal.8man-demo.com/Docs (SRV-8MAN)	
			SharePoint	http://portal.8man-demo.com/Docs (SRV-8MAN)	
			ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)	
			SharePoint	http://portal.8man-demo.com/Docs (SRV-8MAN)	
			ActiveDirectory	8man-demo.local (8man-demo.local: DC=8man-demo,DC=local)	

The last column contains information on data storage of file server resources.

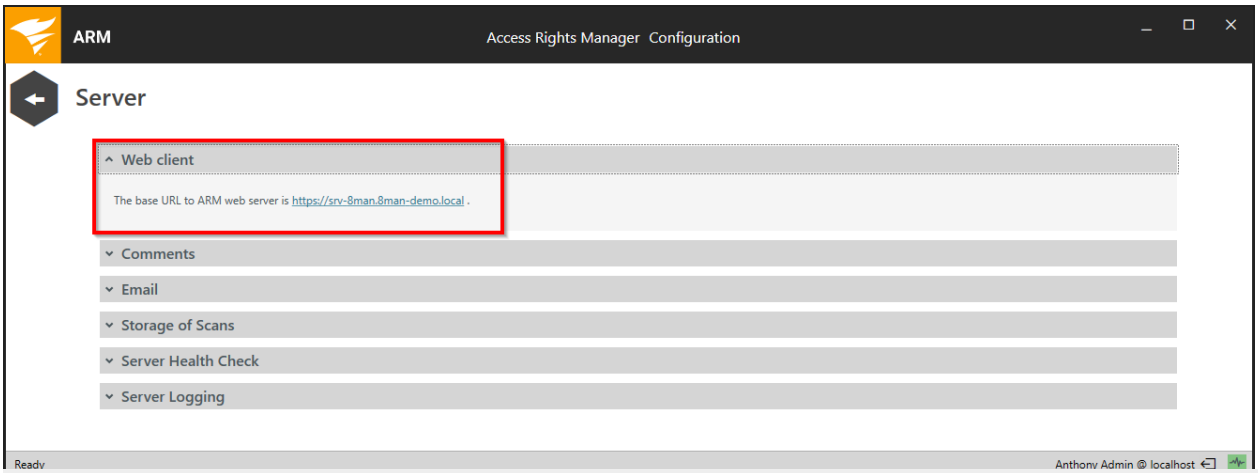
The column users will only contain values if a group has been configured as the Data Owner.

Server



Click "Server" to manage settings related to comments, email, data storage, health-check and event logs.

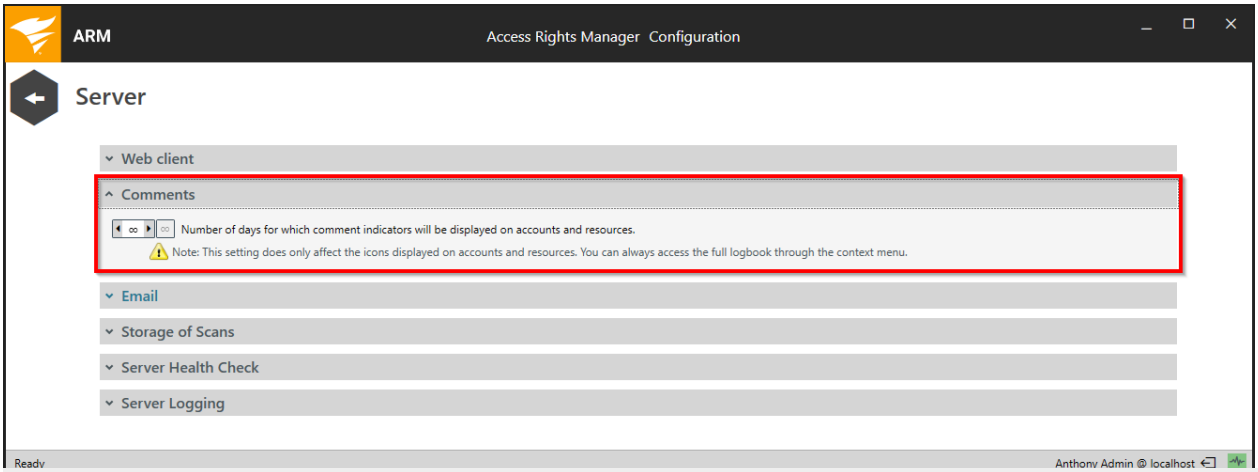
Configure the web client URL



Specify the URL of the web server running the ARM Website.

This is used for the link in the notification emails.

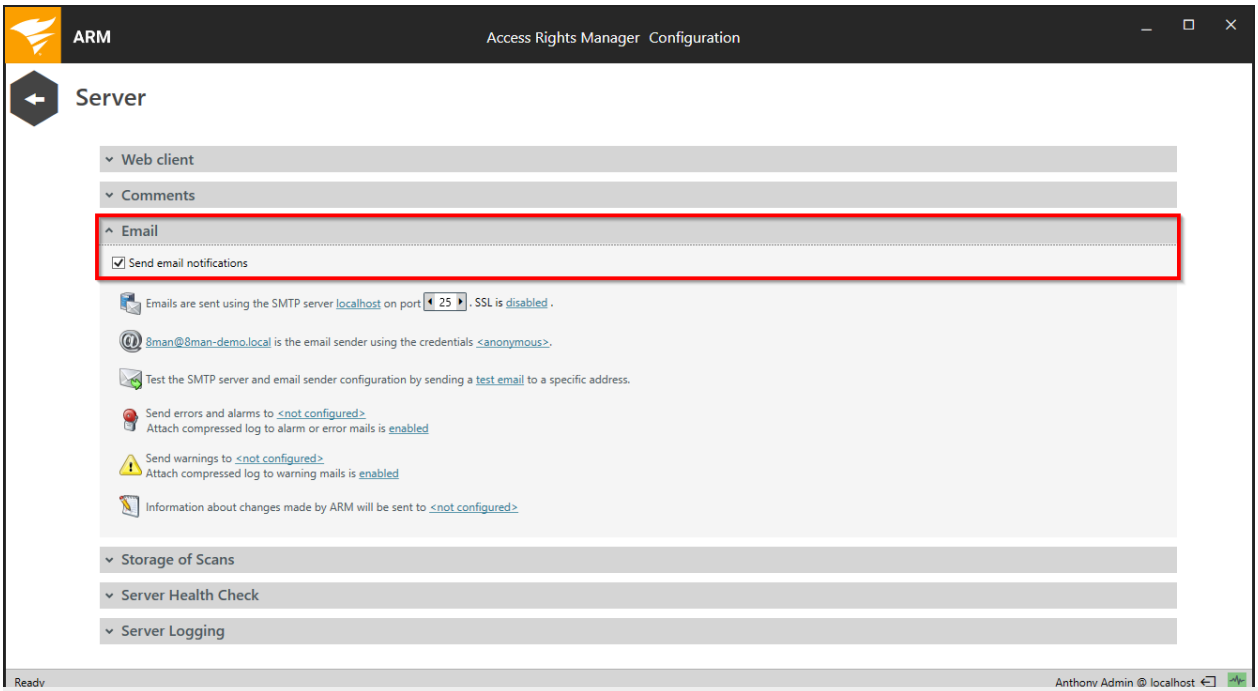
Set the display duration for comment icons



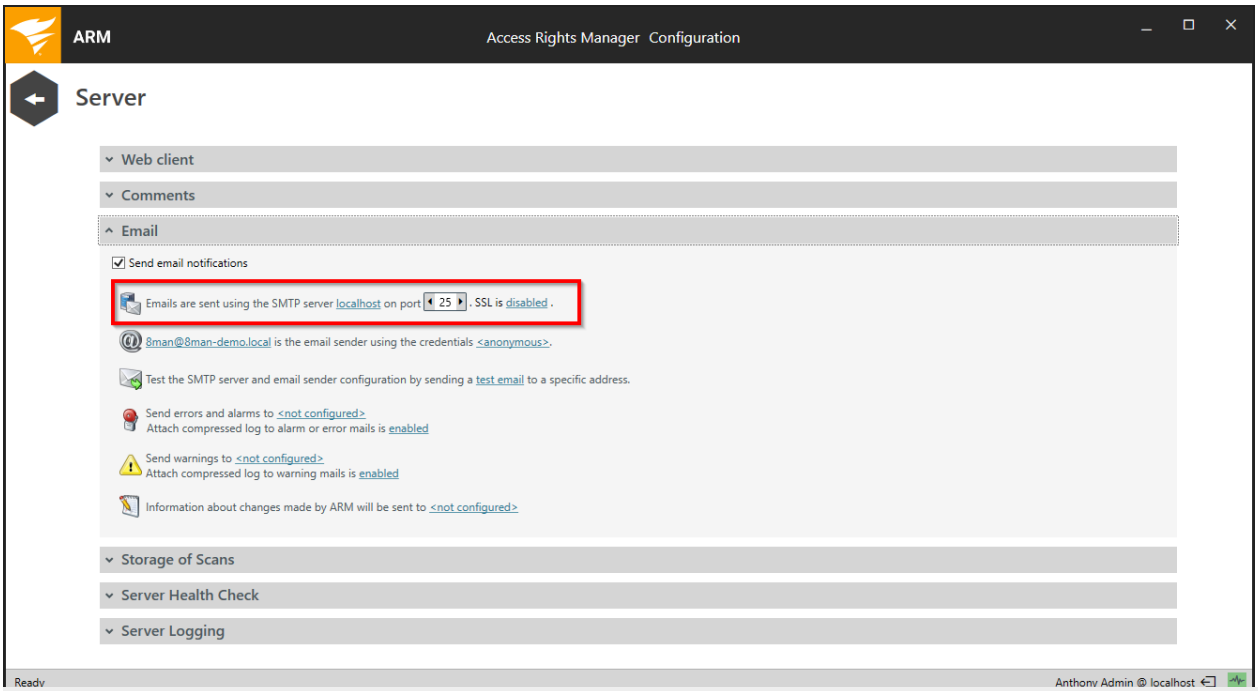
ARM displays a note icon in the resource or accounts view for stored comments or AD Logga information.

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



Activate email support in ARM.

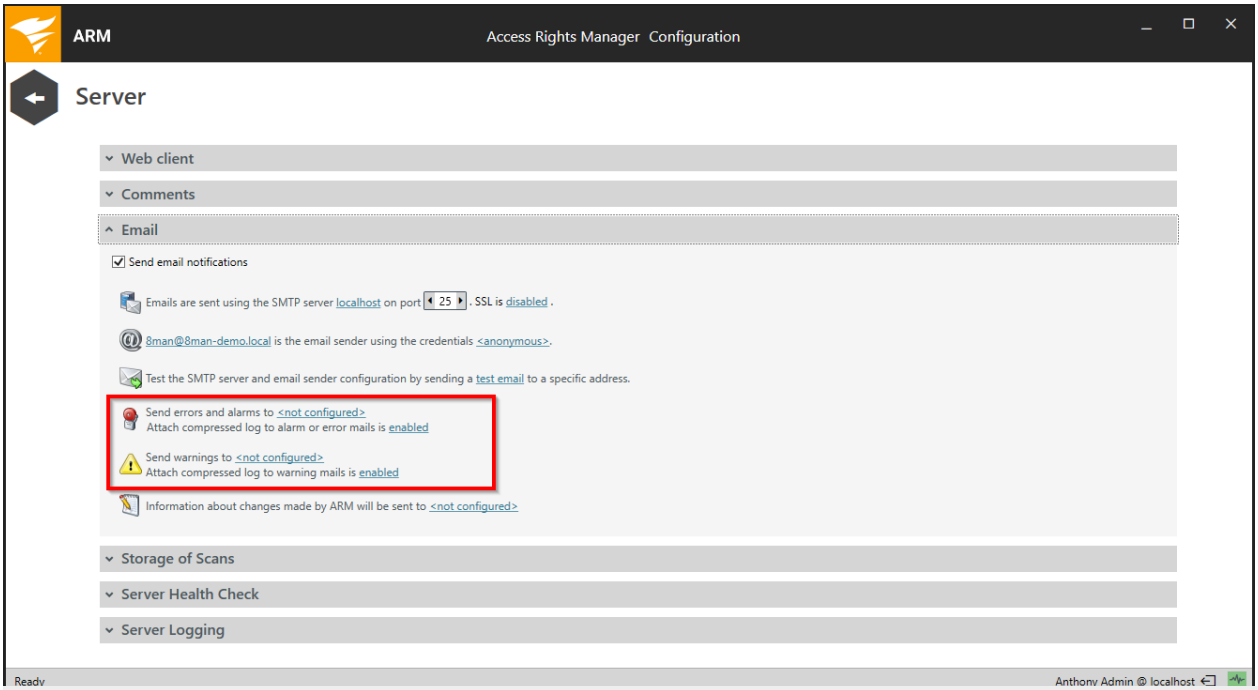


Configure an SMTP-server for sending emails.

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:

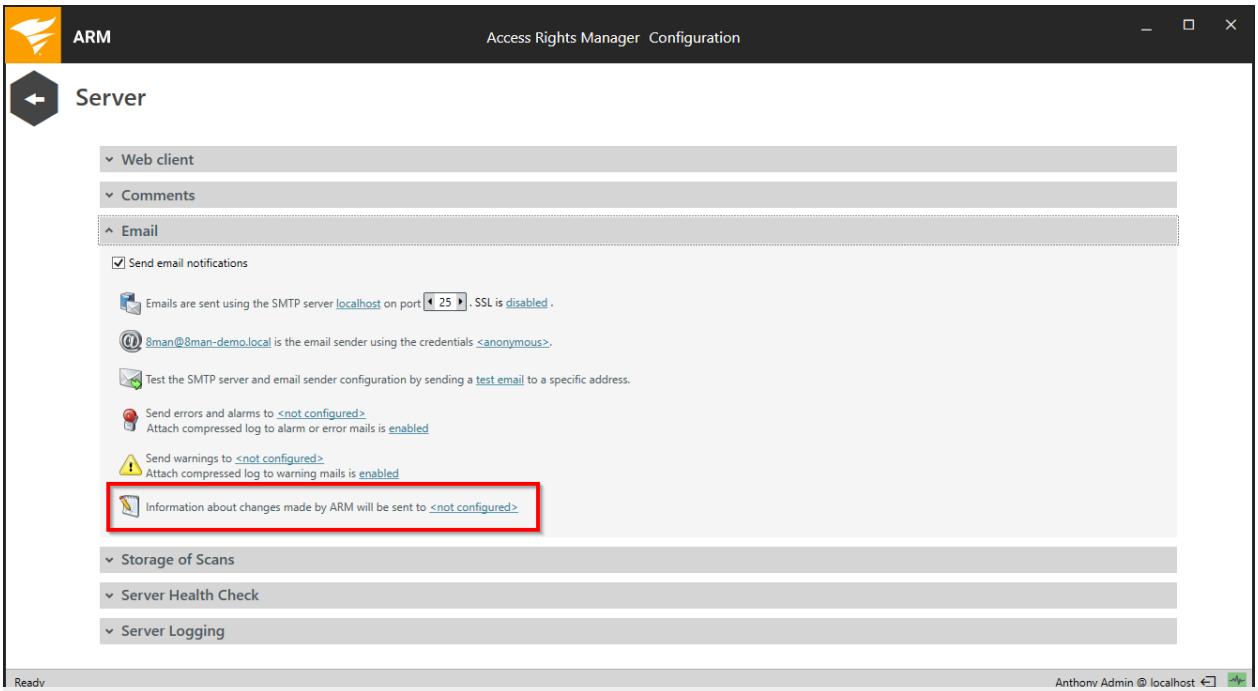
- 25 without SSL
- 465 or 587 with SSL/TLS



Sources for errors, alerts and warnings include the following:

- Thresholds from the Server Health-Check
- Errors when running ARM

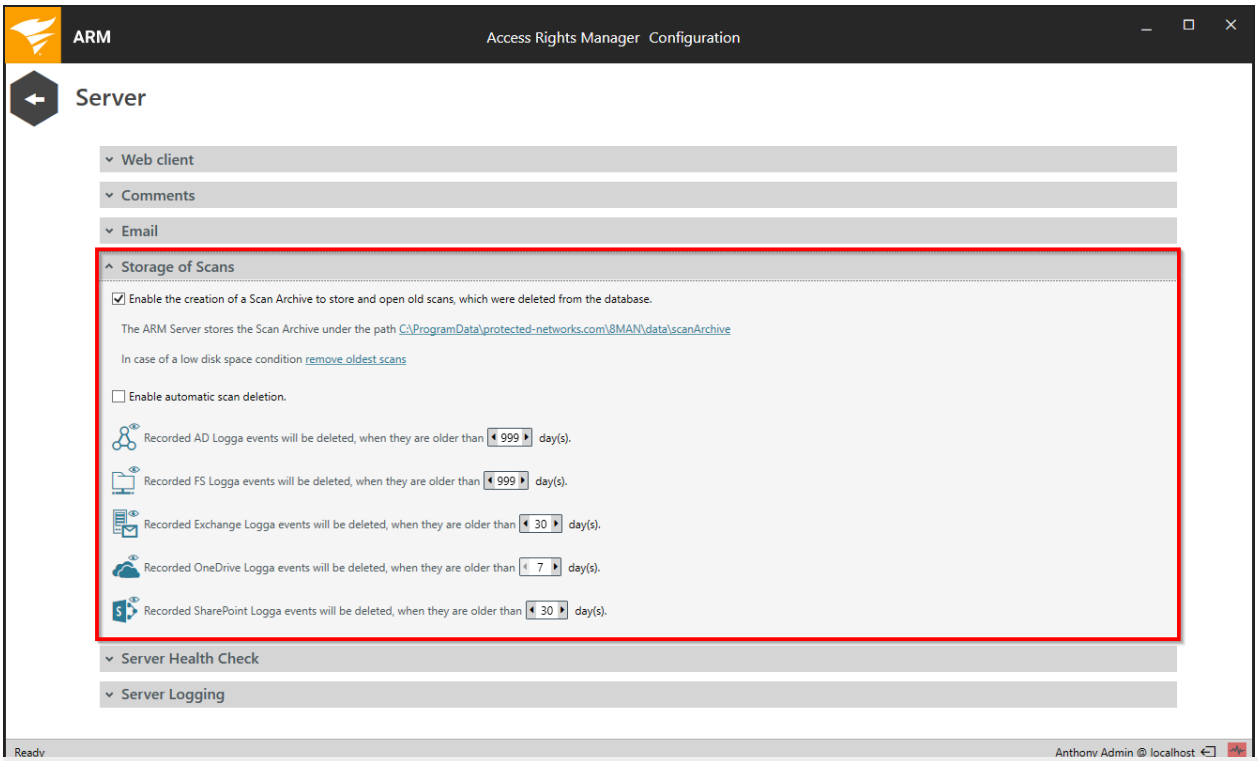
The events of the last 4 hours are summarized in an email.



Enter an email address if you want to be alerted every time a user completes a change with ARM.

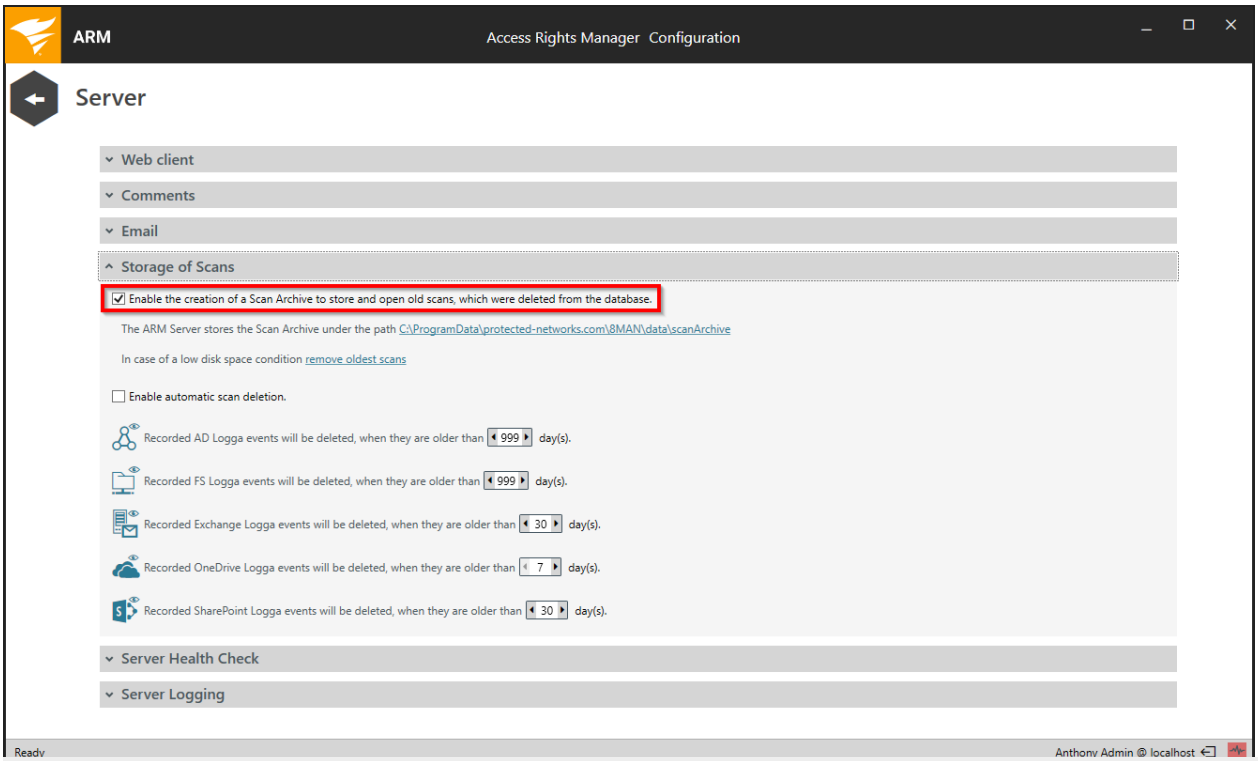
SPAM Alert! Every change generates an email.

Configure storage of scans settings



The "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.

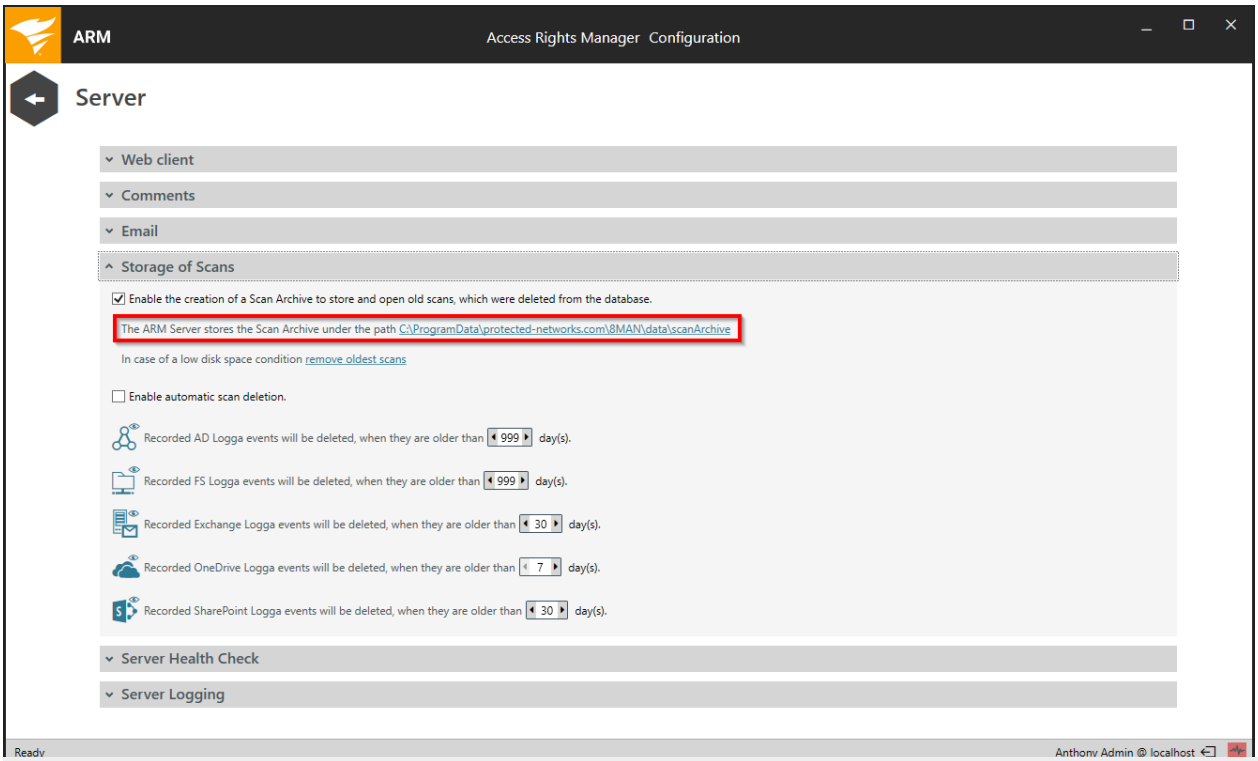


Option activated:

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:

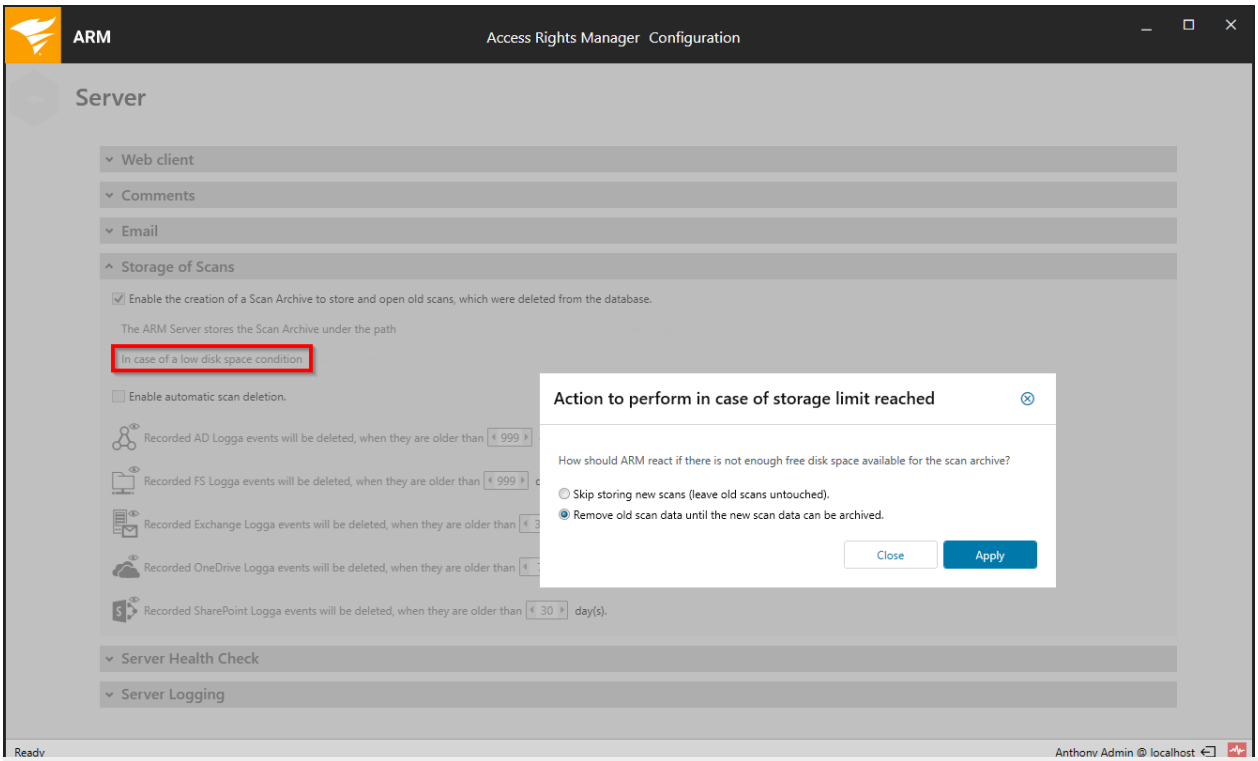
ARM does not create a scan archive. ARM users are only able to access data available in the data base.



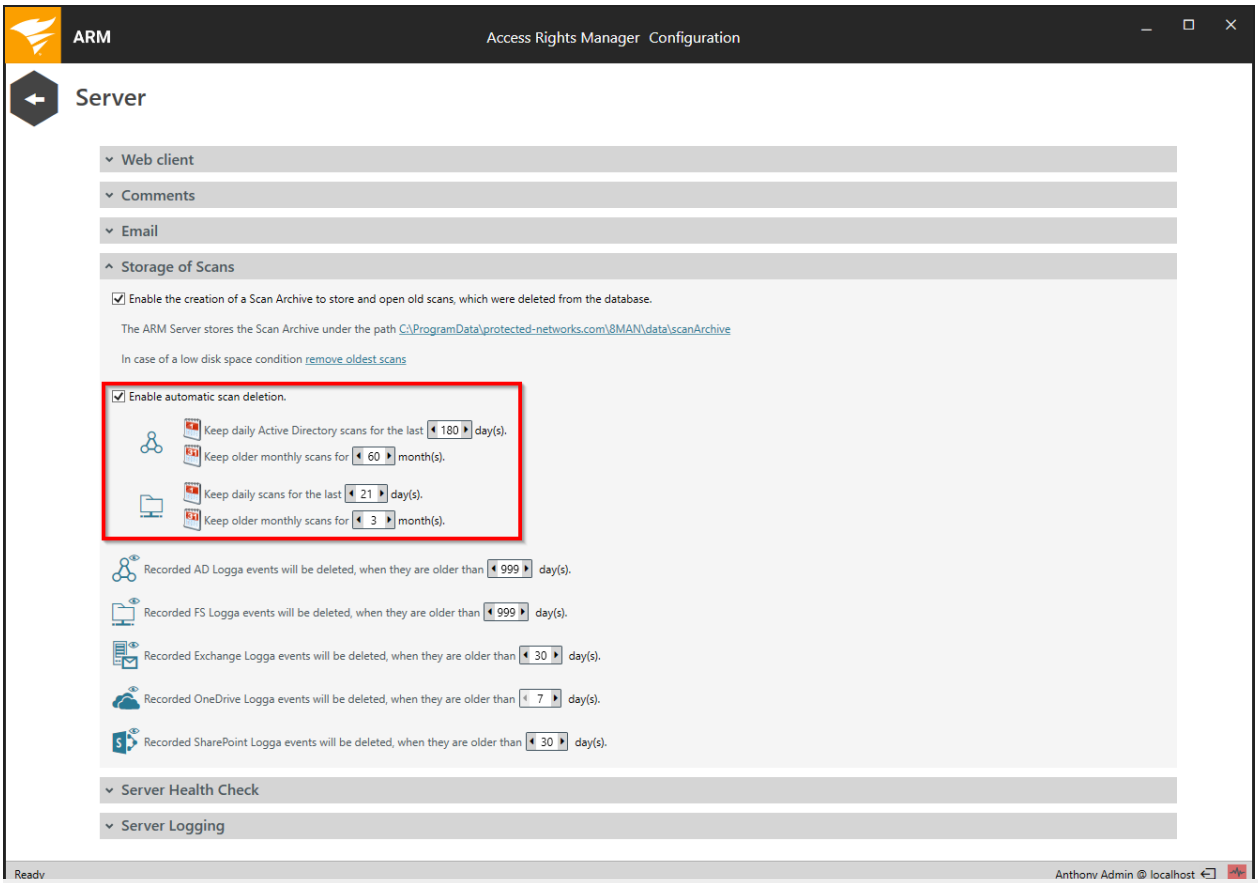
Determine where the ARM scan archives are stored. For example, you can store the scan archives on another volume.

Default path for the scan archives:

```
%ProgramData%\protected-networks.com\8MAN\data\ScanArchive
```



Determine how ARM reacts in case of low disk space (volume full).



Option deactivated:

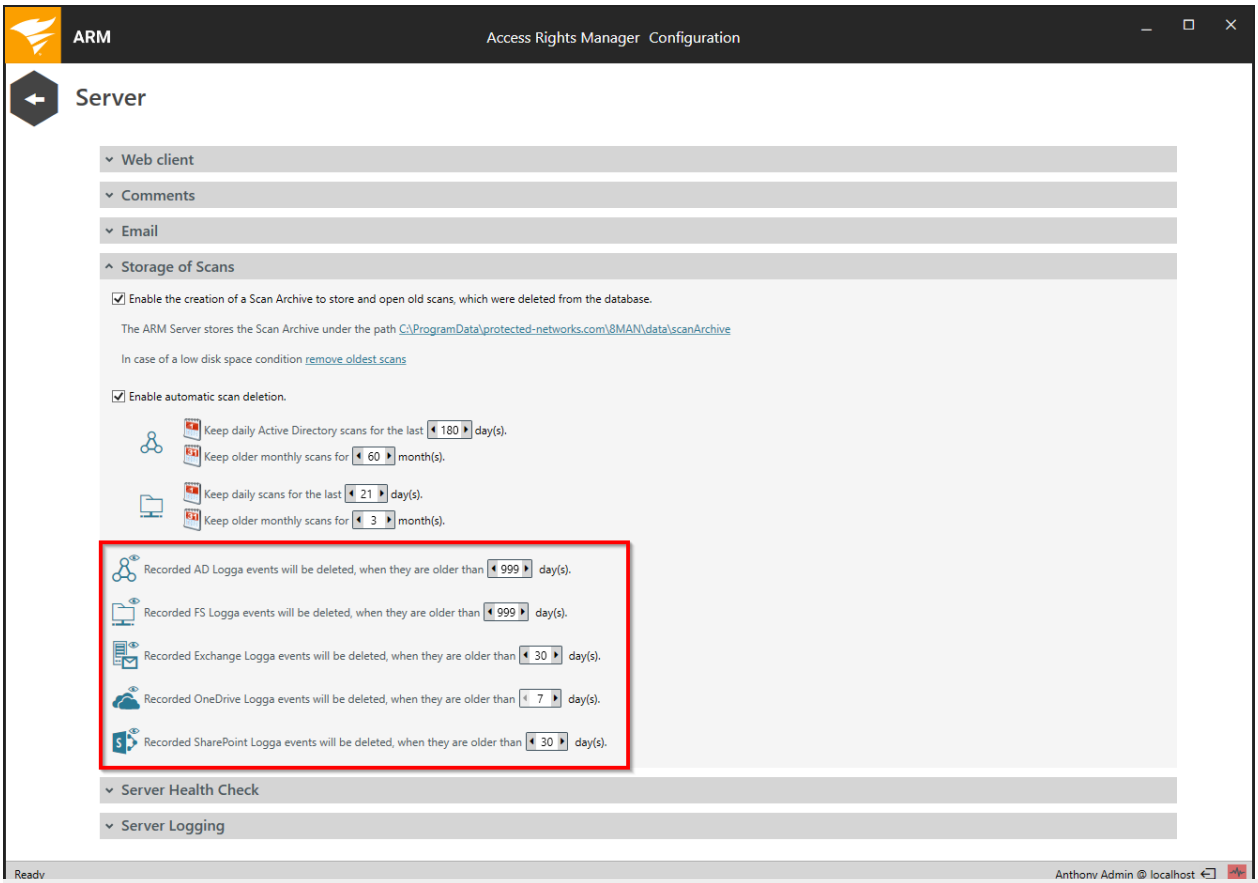
ARM does not delete any scans from the data base.

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.



Determine how long Logga data is stored.

Default: 30 days

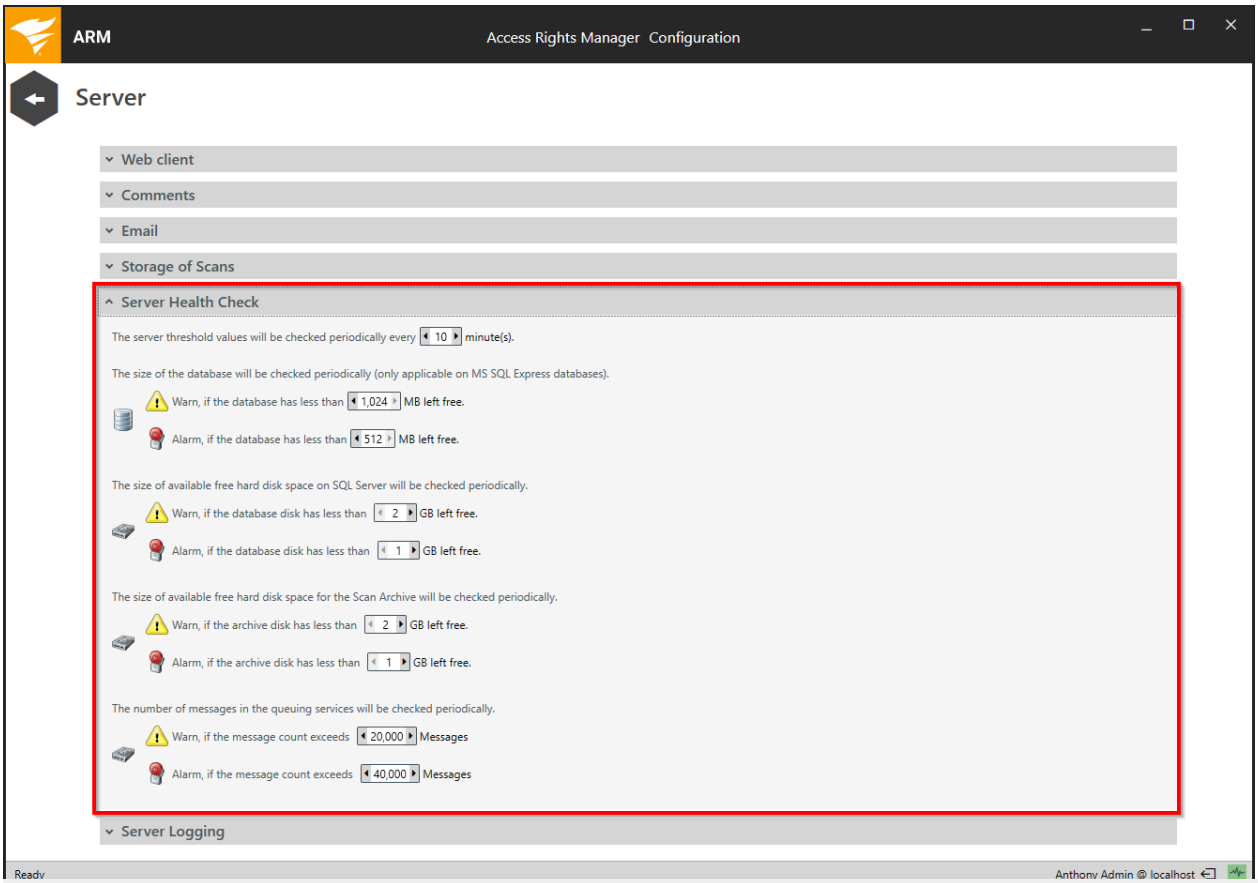
An event generates the following average amount of data:

FS Logga about 43 bytes

AD Logga about 600 bytes

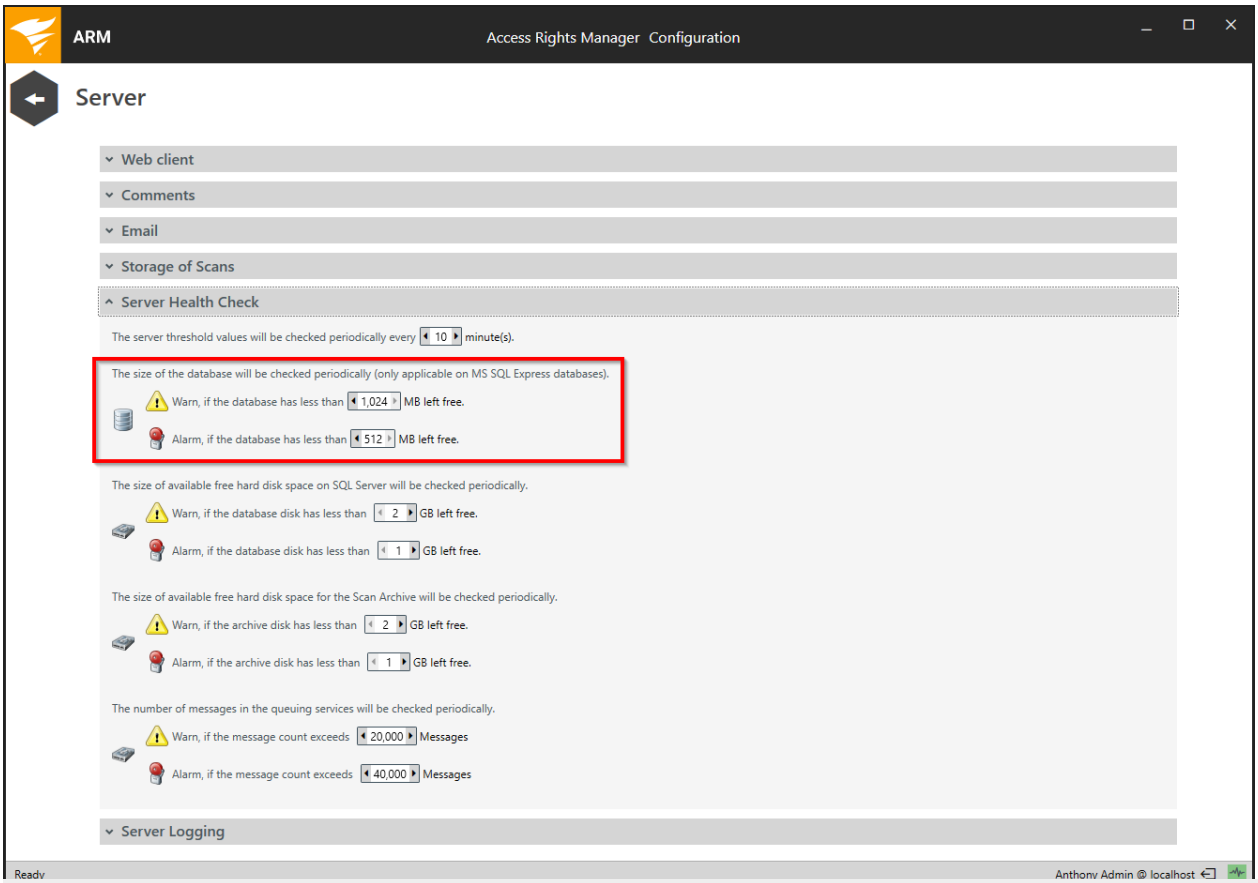
Exchange Logga about 600 bytes

Determine server thresholds



Determine server thresholds and monitoring frequency.

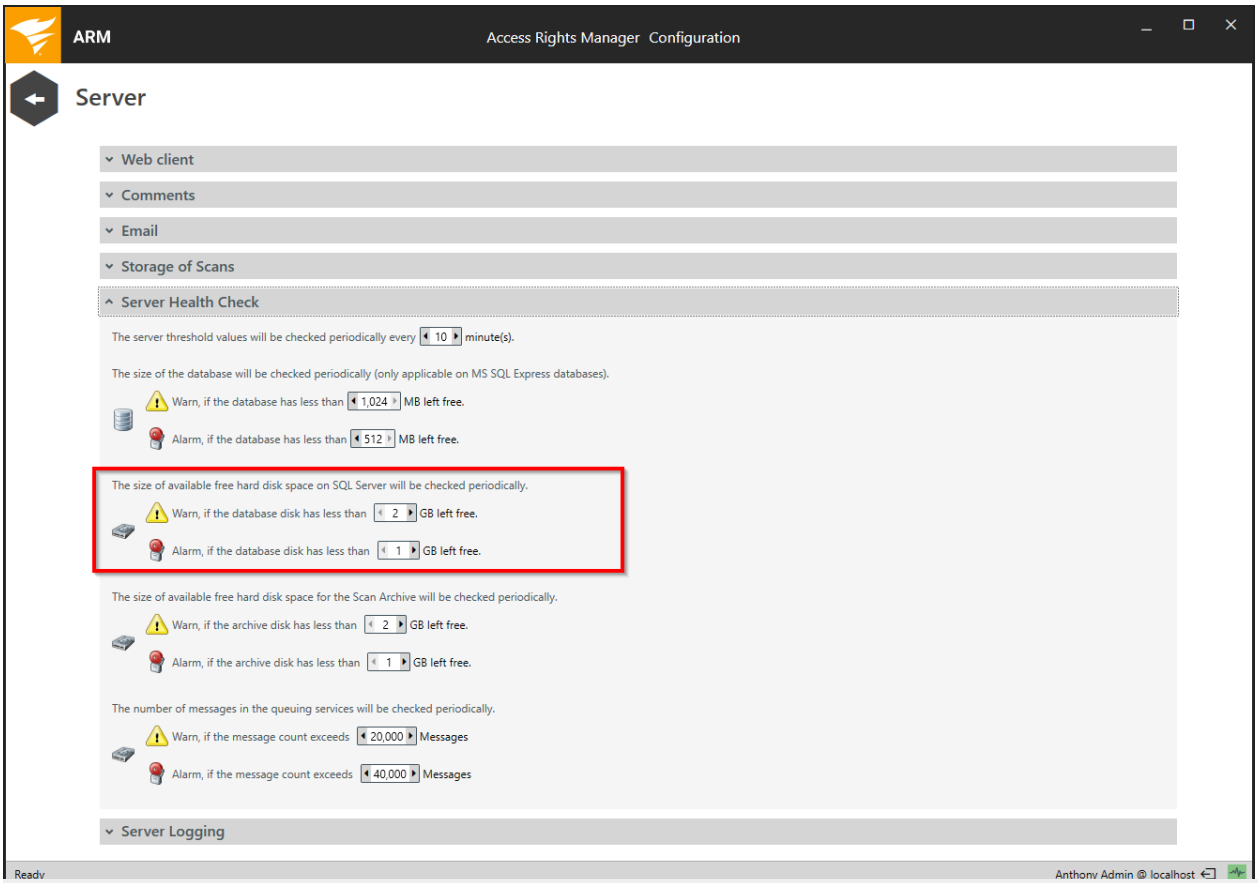
Please also reference the following chapter: Display actual server thresholds.



ARM identifies automatically whether you are using SQL Express. In this case you can determine thresholds for data base size.

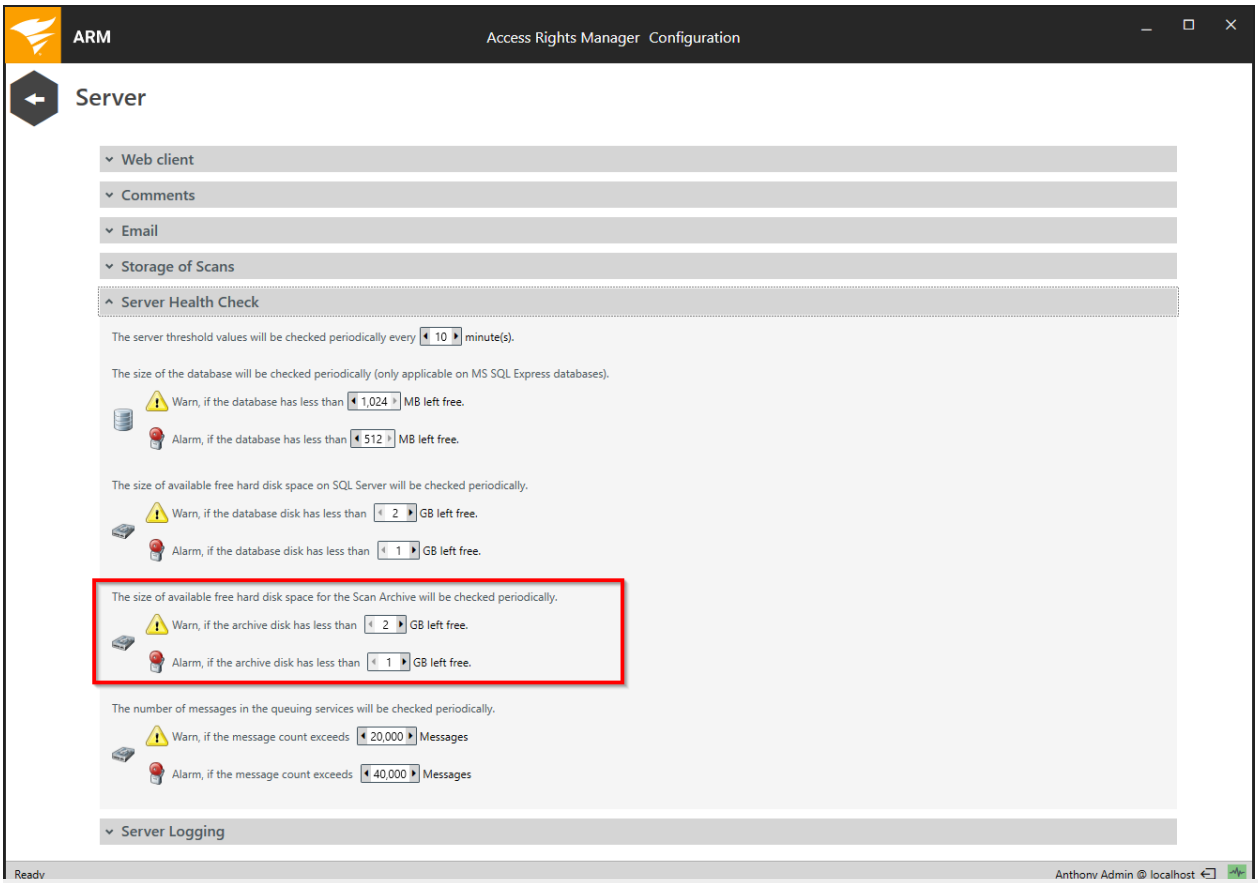
If you are using a "full" SQL server, then these settings are not relevant.

Please refer to the following section for additional information: ARM and SQL Express.



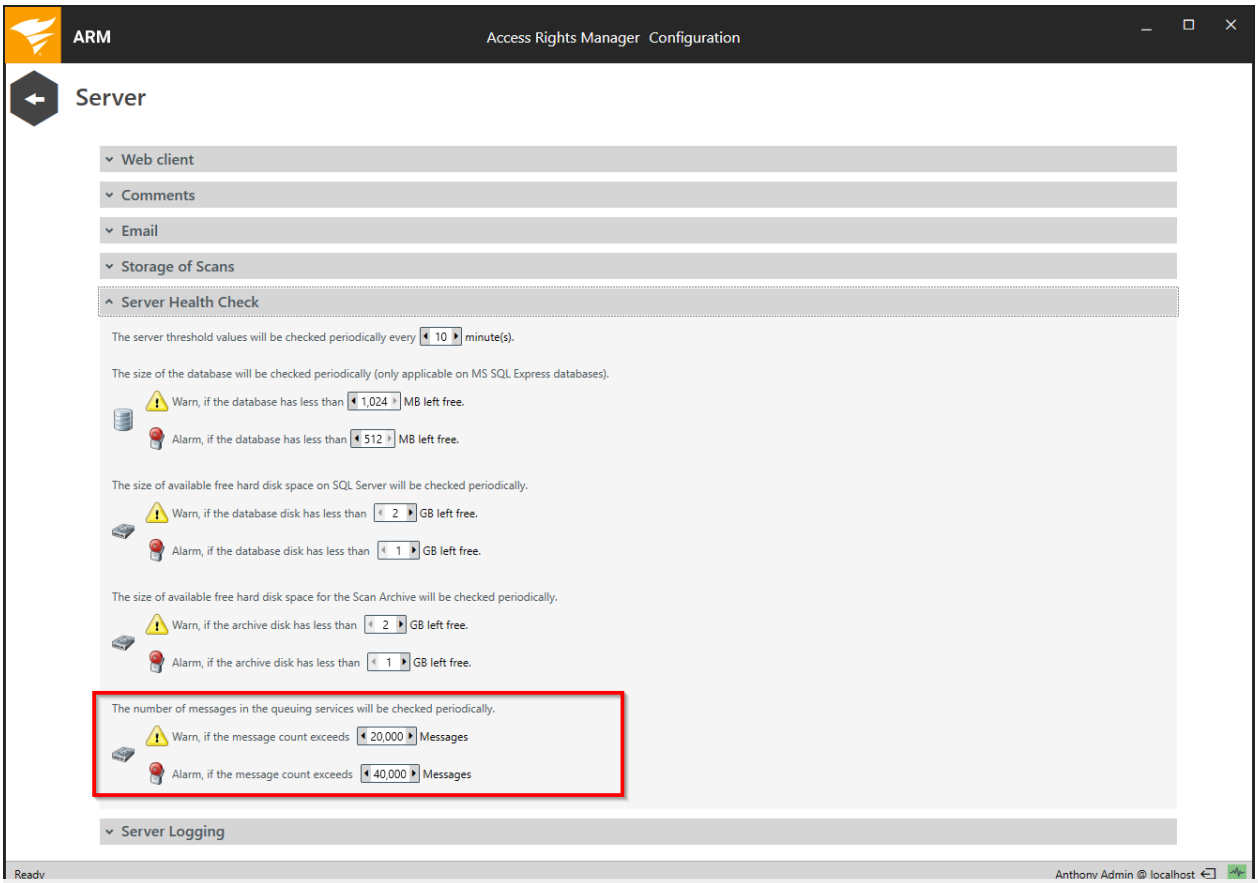
ARM automatically determines the available disk space on the volume storing SQL data base files.

Determine thresholds for available storage space.



Determine the thresholds for available disk space of the scan archive.

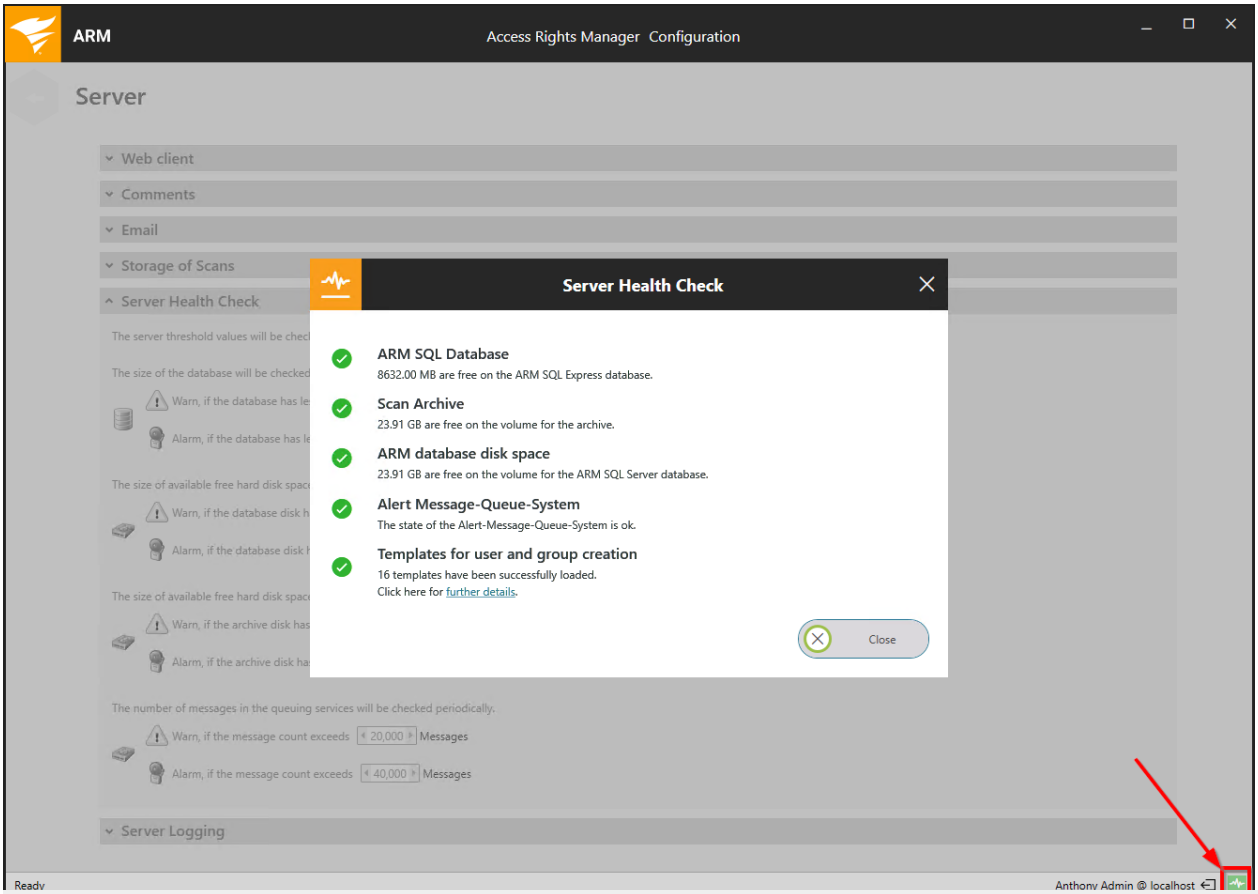
Settings for the scan archive can be found in Storage of Scans.



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

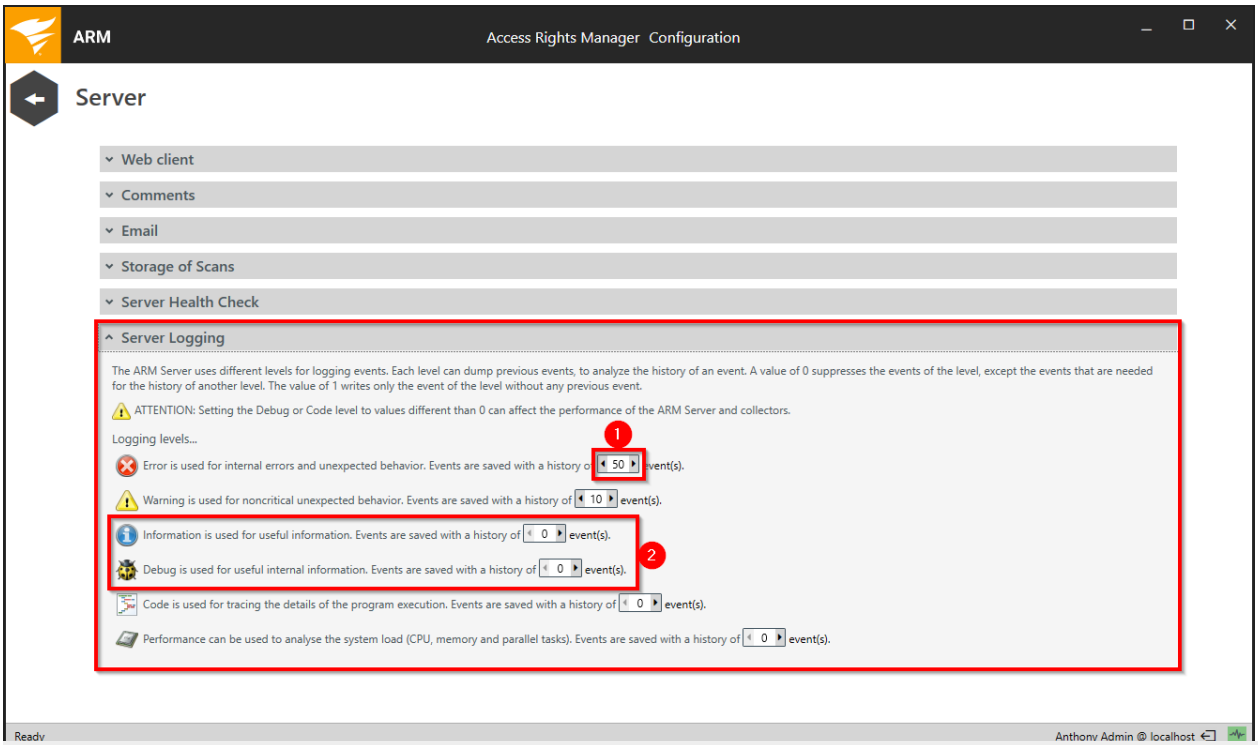


Click on the marked symbol in the status bar to see the current server values.

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.

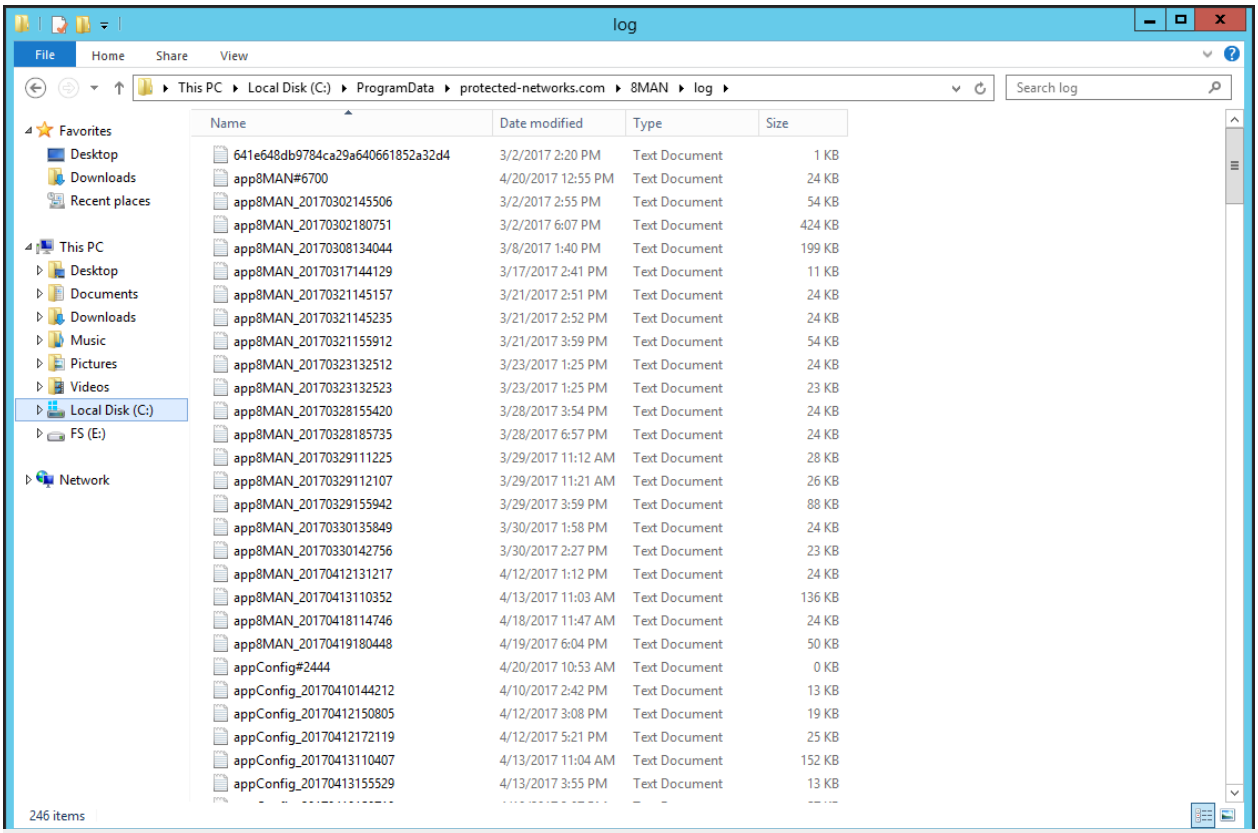
Retrieve ARM log files

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.

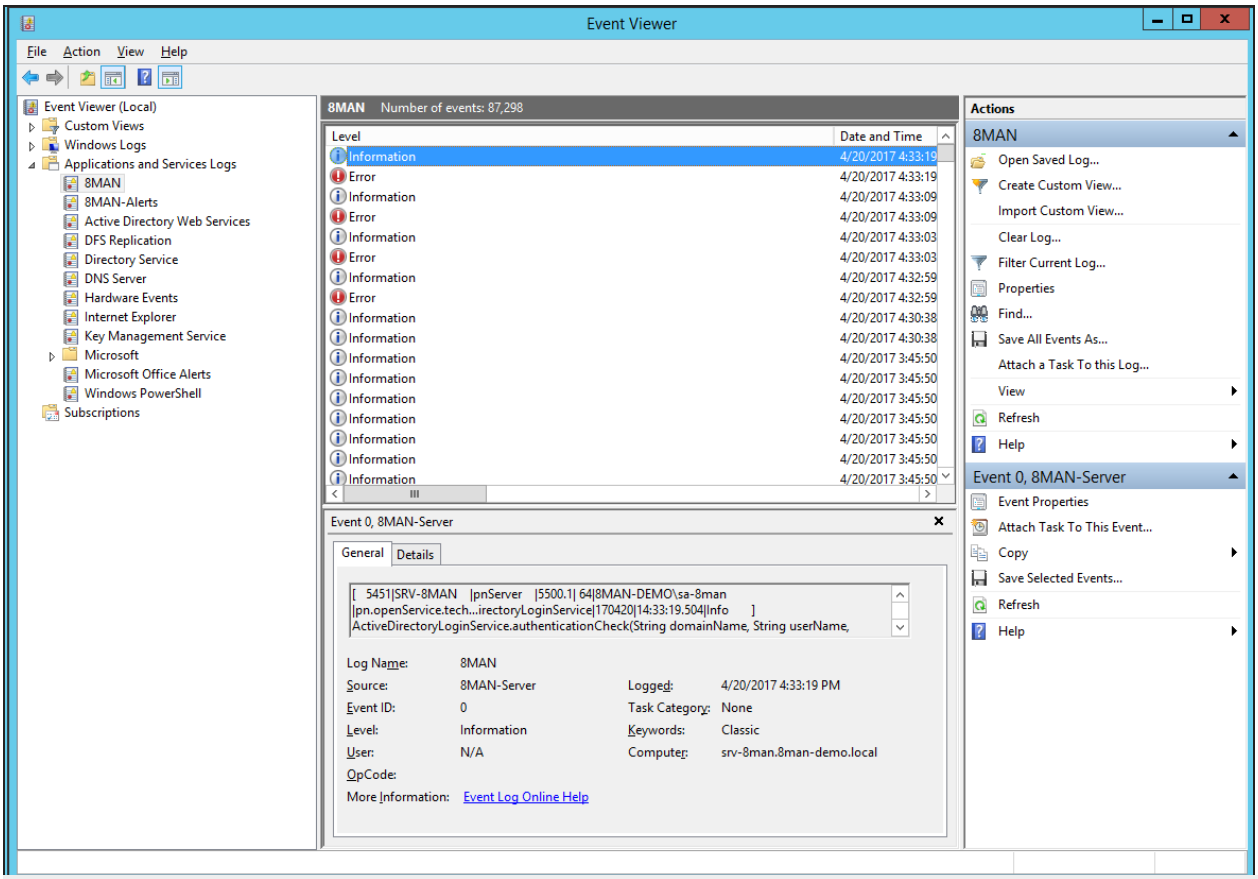
Log files either grow to a size of 50MB or 7 days. When restarting the ARM service a new log file is started. ARM saves a maximum of 20 log files per type.



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 .



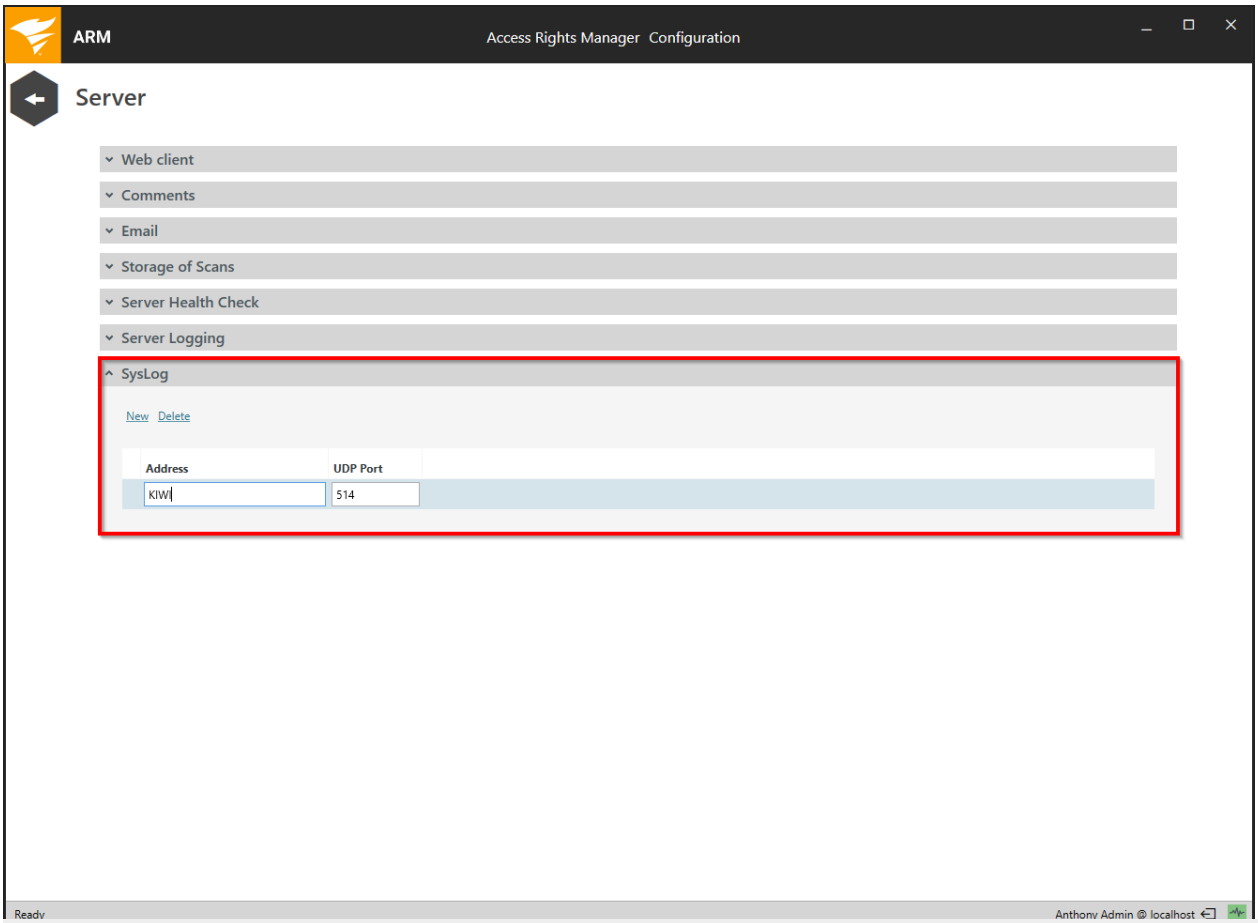
The following event types are entered into the Windows event log: "Error", "Warning" and "Information". ARM creates its own node under "Application and Service Logs".

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.

FILENAME	CONTAINES...
pnAlert	Information about alert engine (FS Logga and AD Logga).
grantMa	Information on GrantMA, webAPI.

Set Syslog servers

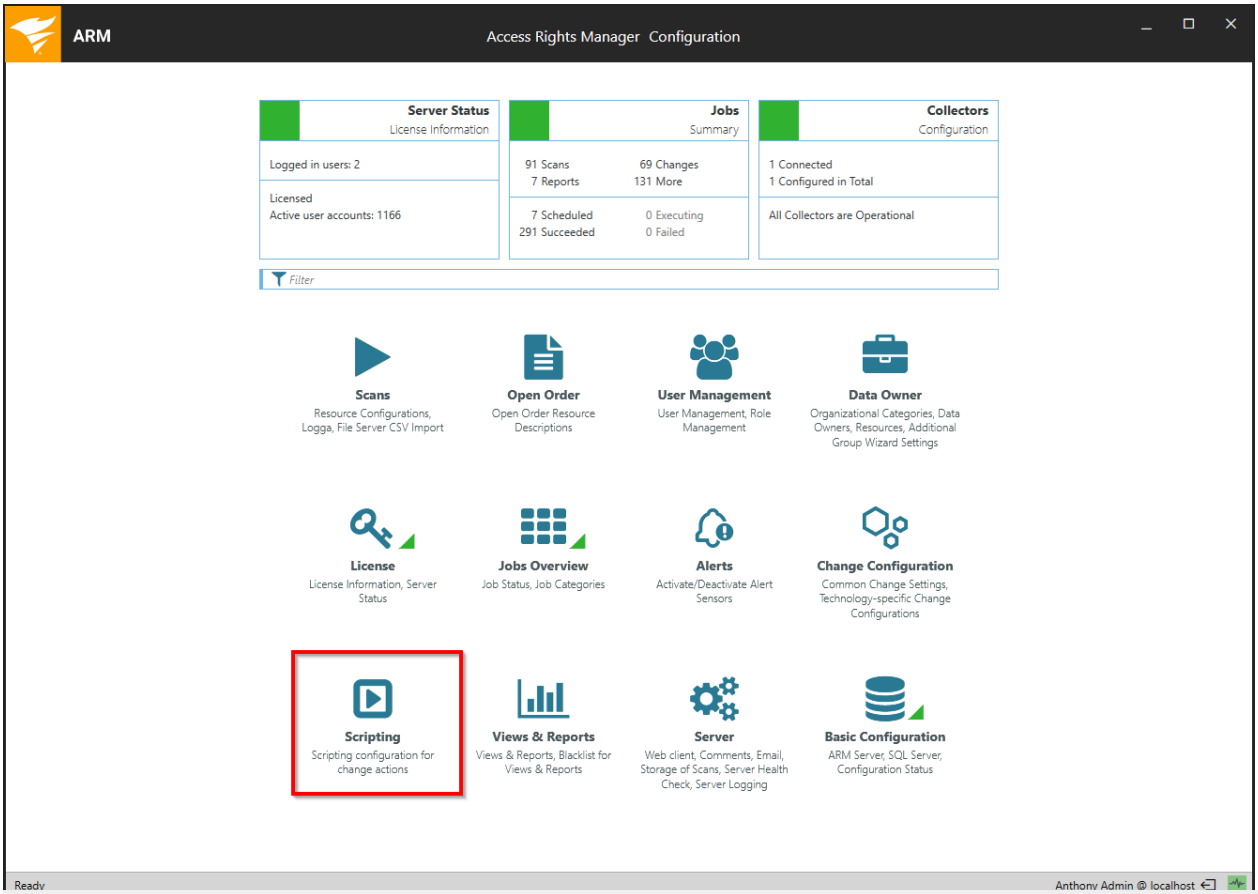


Configure Syslog servers with Name/IP address and port.

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



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:

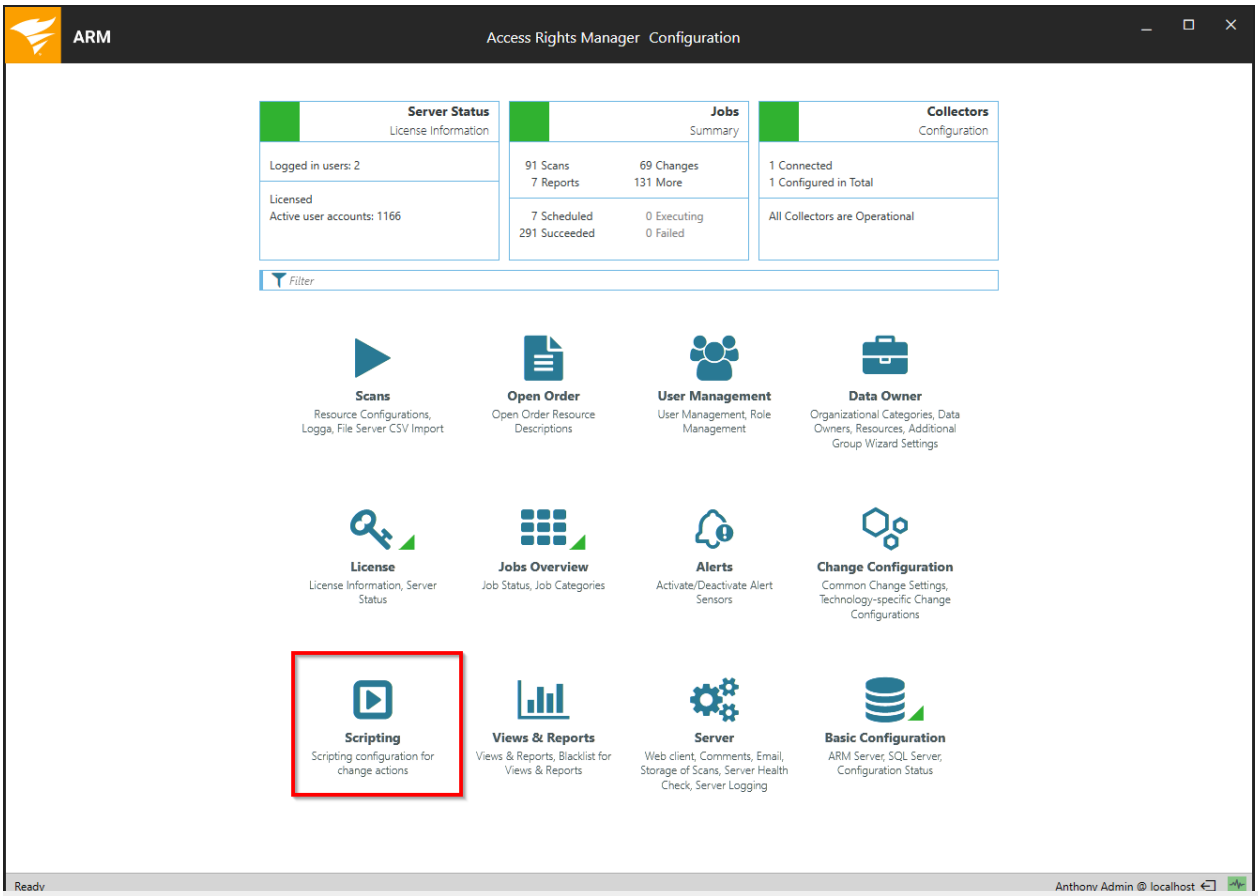
```
%ProgramData%\protected-networks.com\8MAN\scripts\analyze
```

Supported file types are:

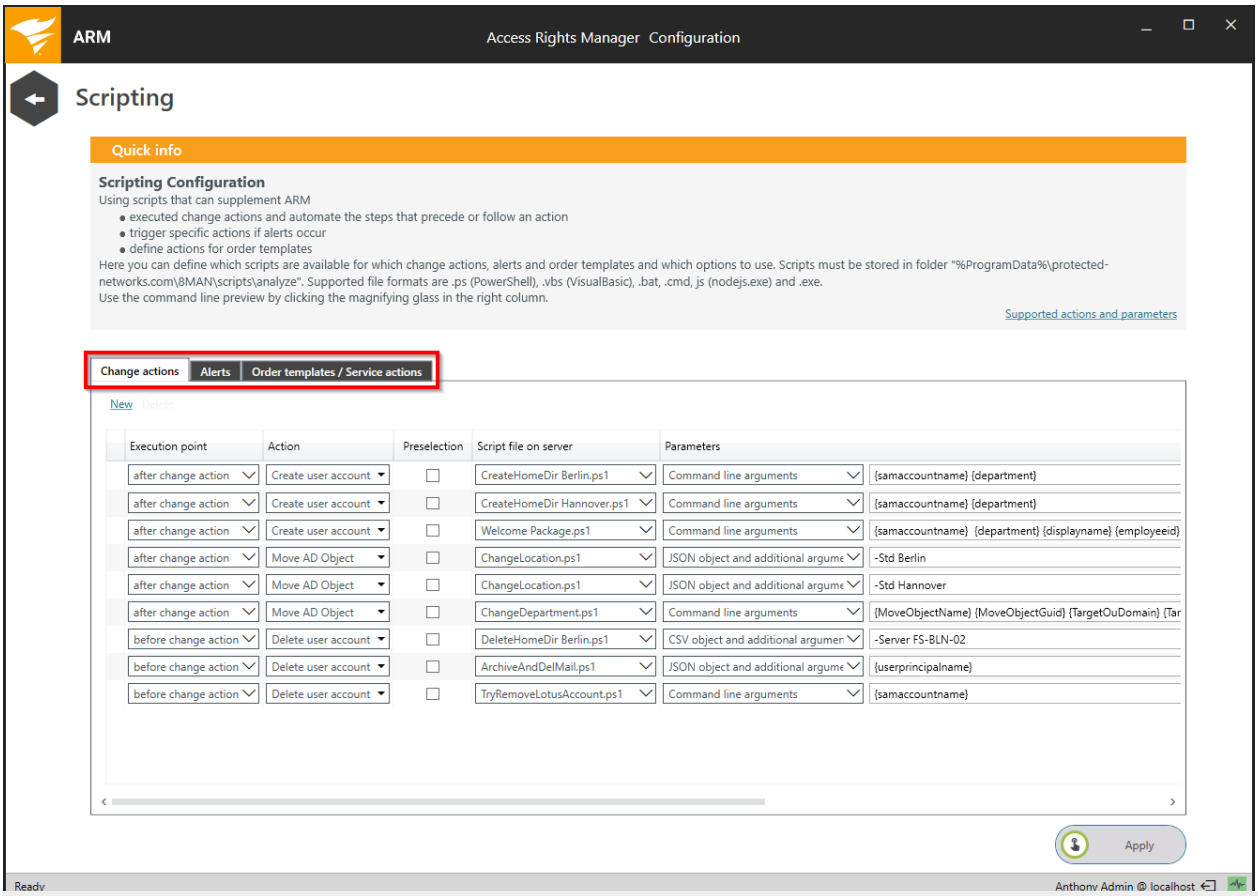
- .ps (PowerShell)
- .vbs (VisualBasic)
- .bat
- .cmd

- .js (nodejs.exe)
- .exe

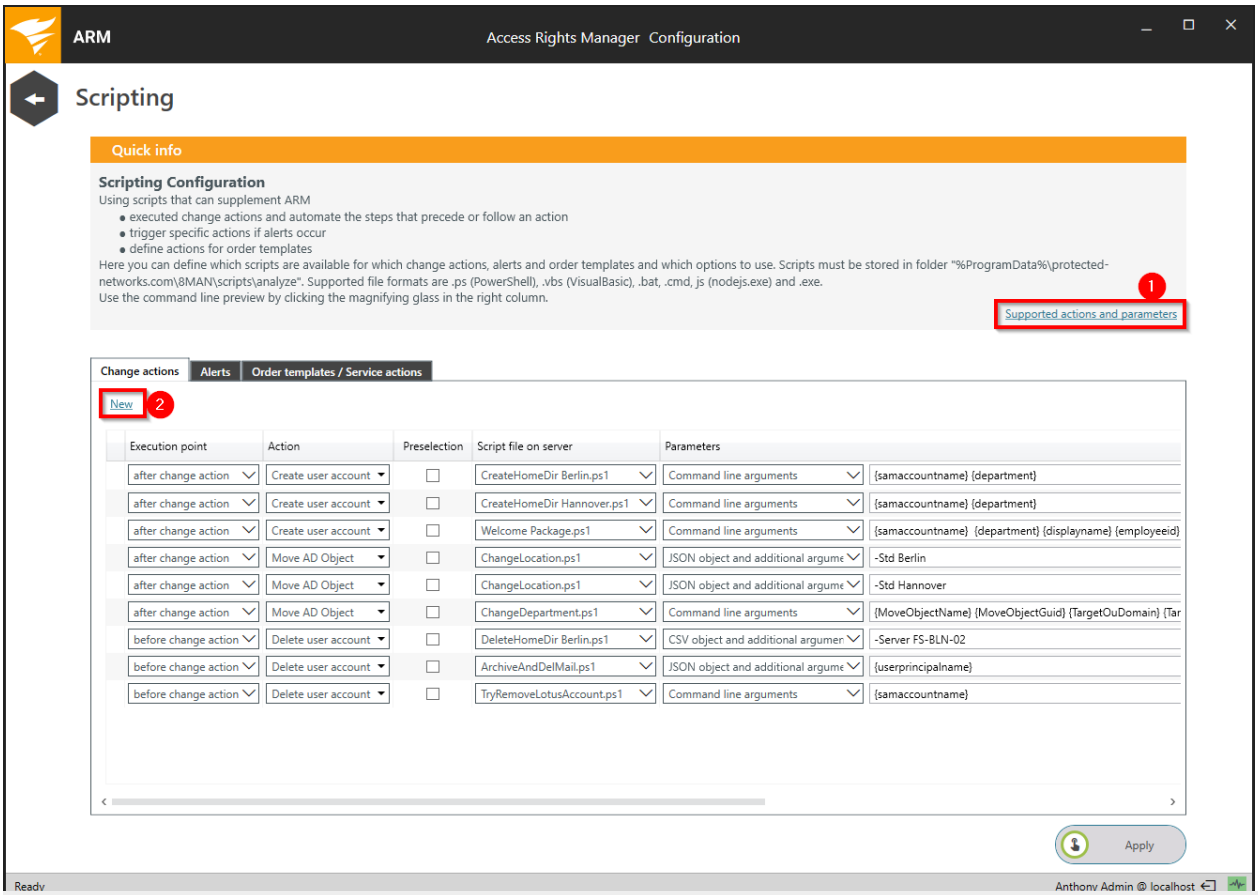
Required PowerShell modules must be installed on the ARM server.



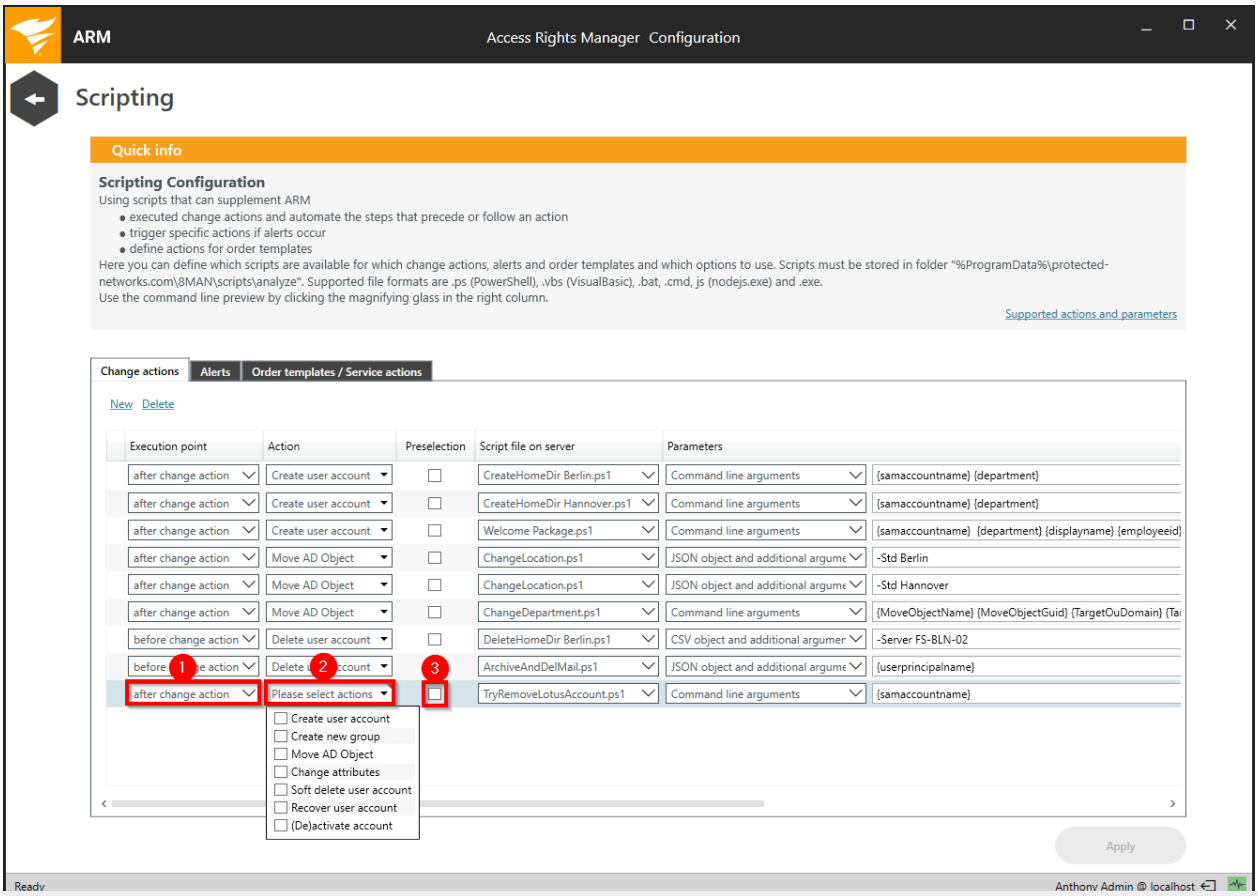
On the start page of the ARM configuration application, click "Scripting".



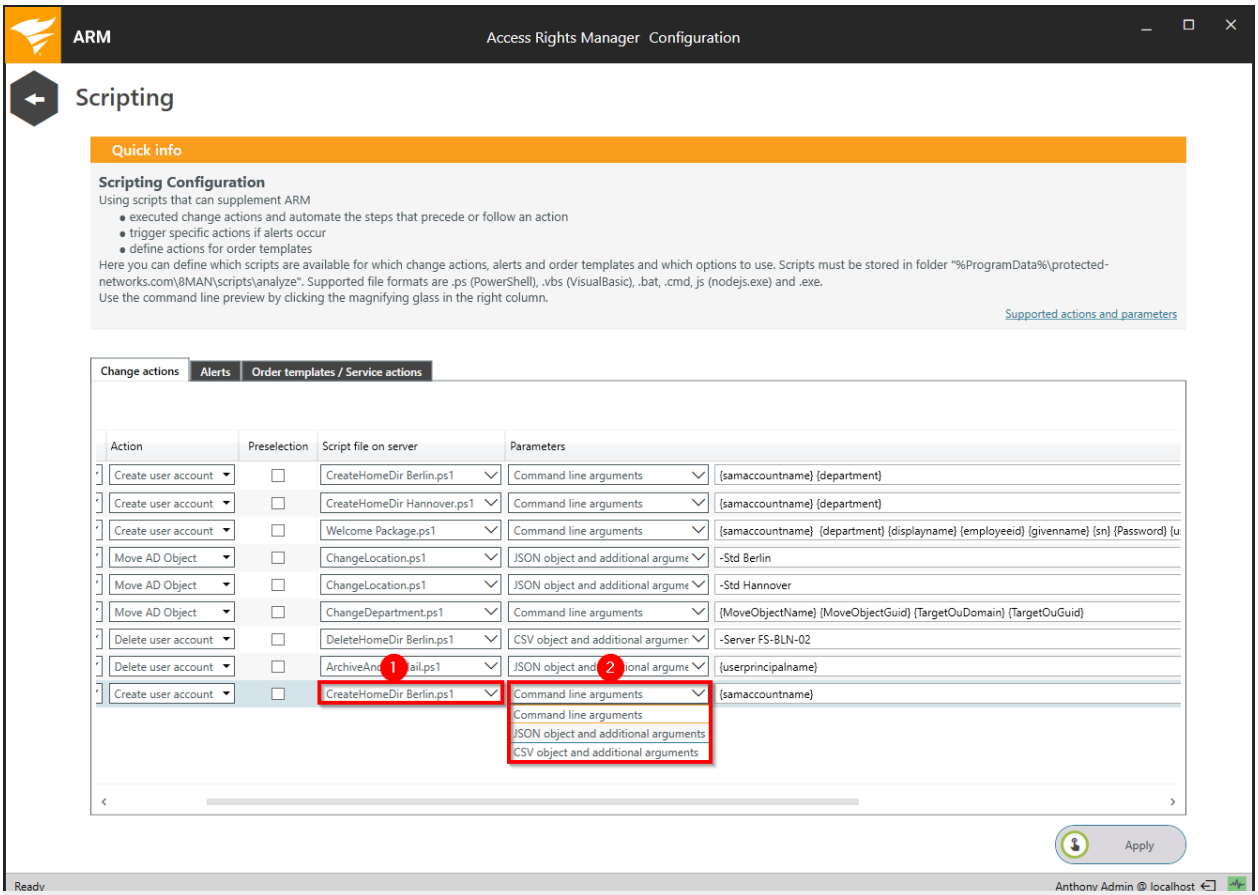
Select the area for which you are configuring scripts.



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.

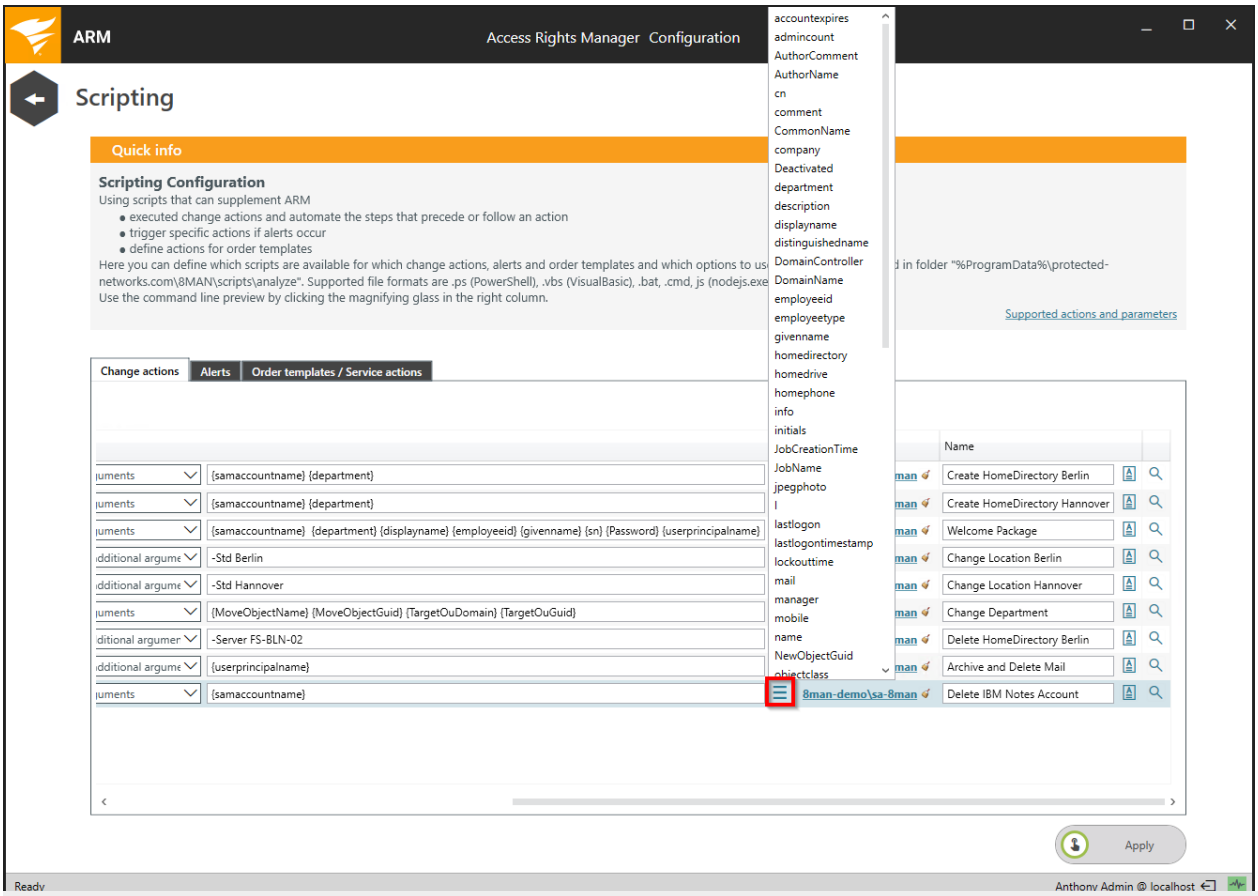


1. Select whether to run the script before or after the action. Your selection filters the available actions (column 2).
2. Select an action for which you want to make a script available.
3. If you have several scripts available for an action, specify the default settings for the ARM users in the drop-down menu.

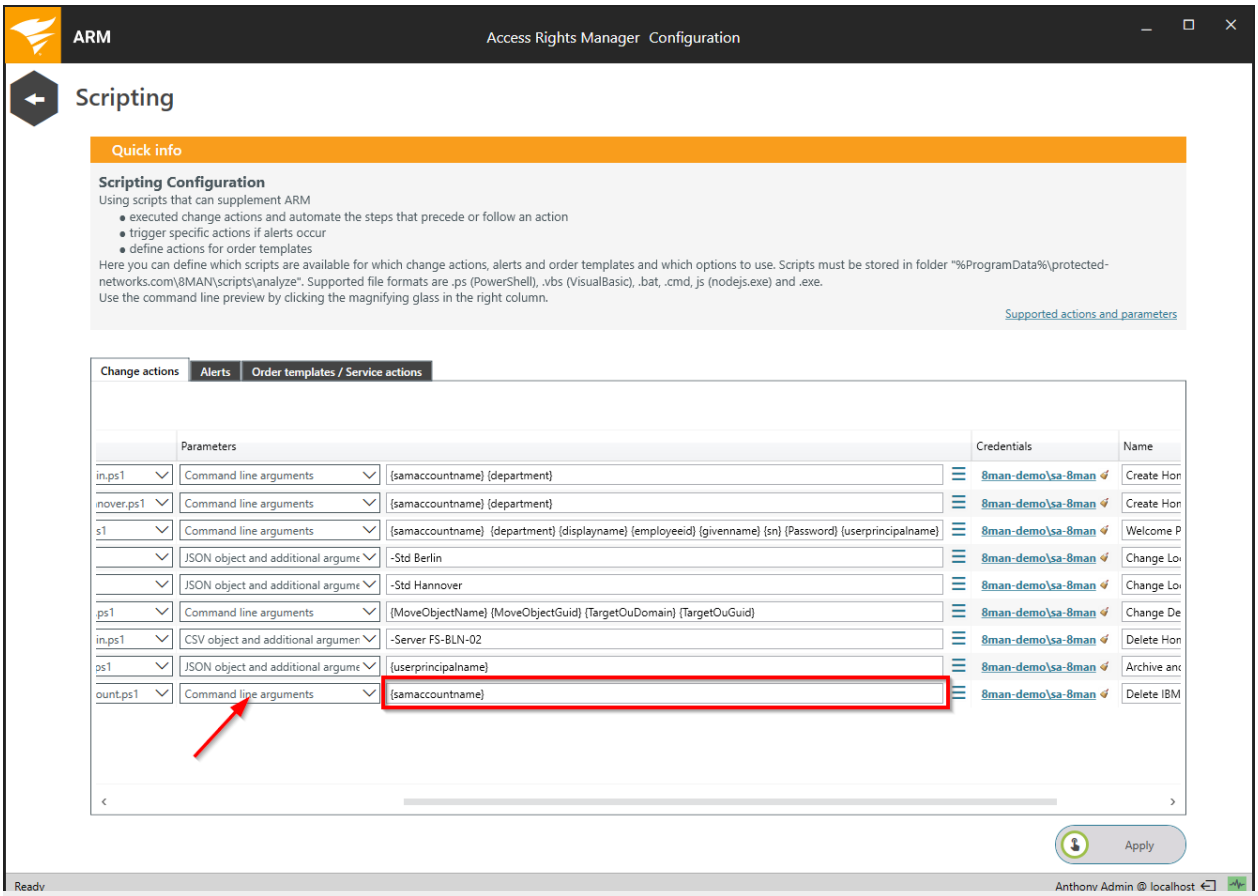


1. Select a script file.
2. Select how ARM passes the parameters to the script.

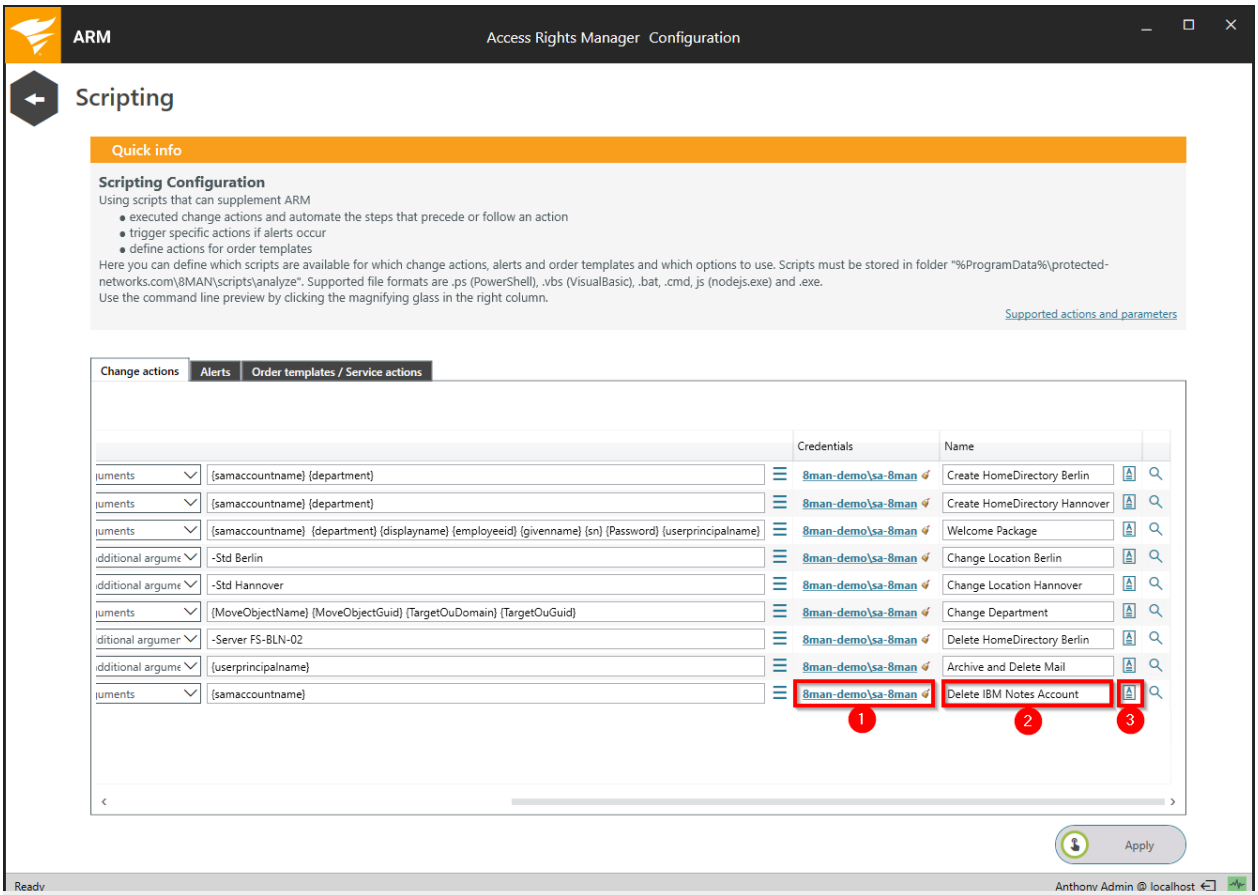
You can select the parameters directly or pass them as JSON or CSV objects.



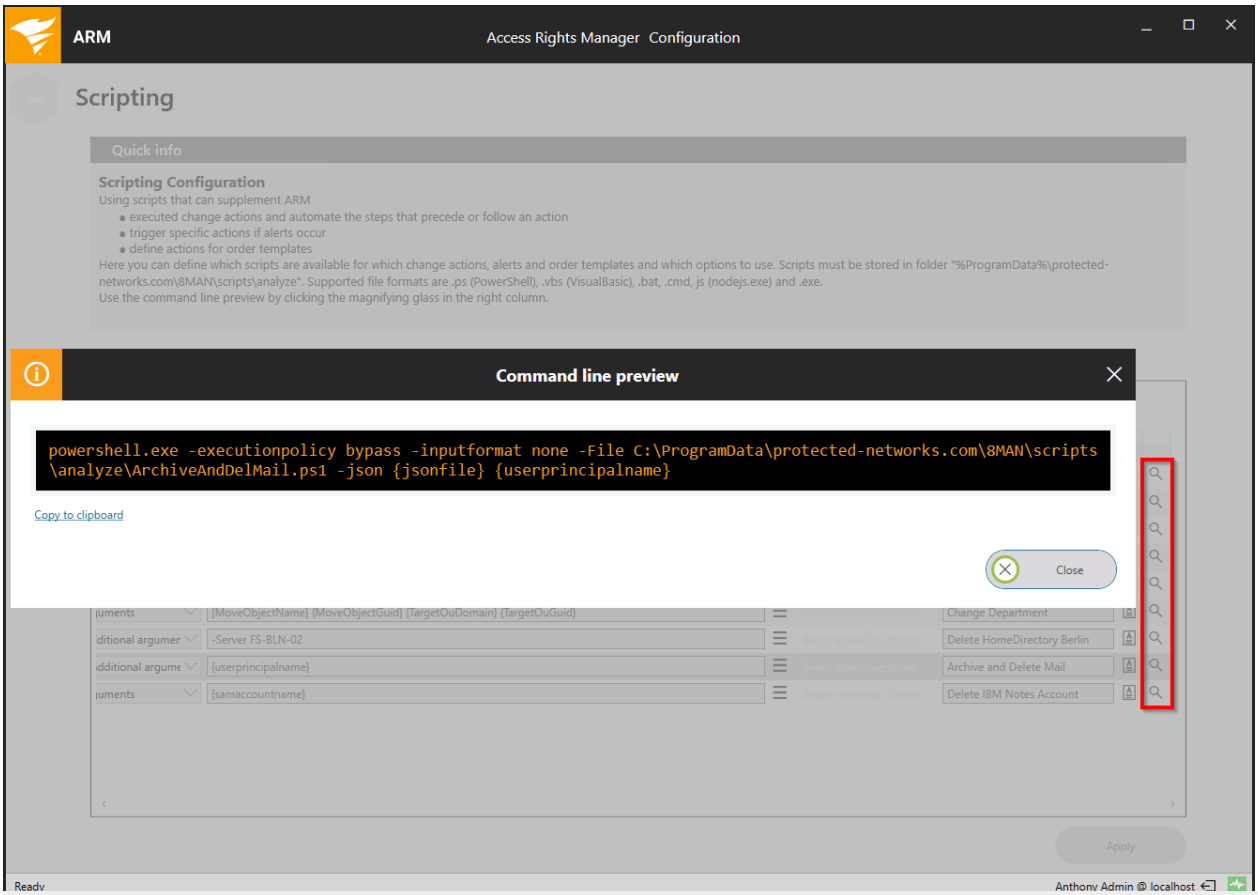
Select the command line parameters.



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.



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.



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.

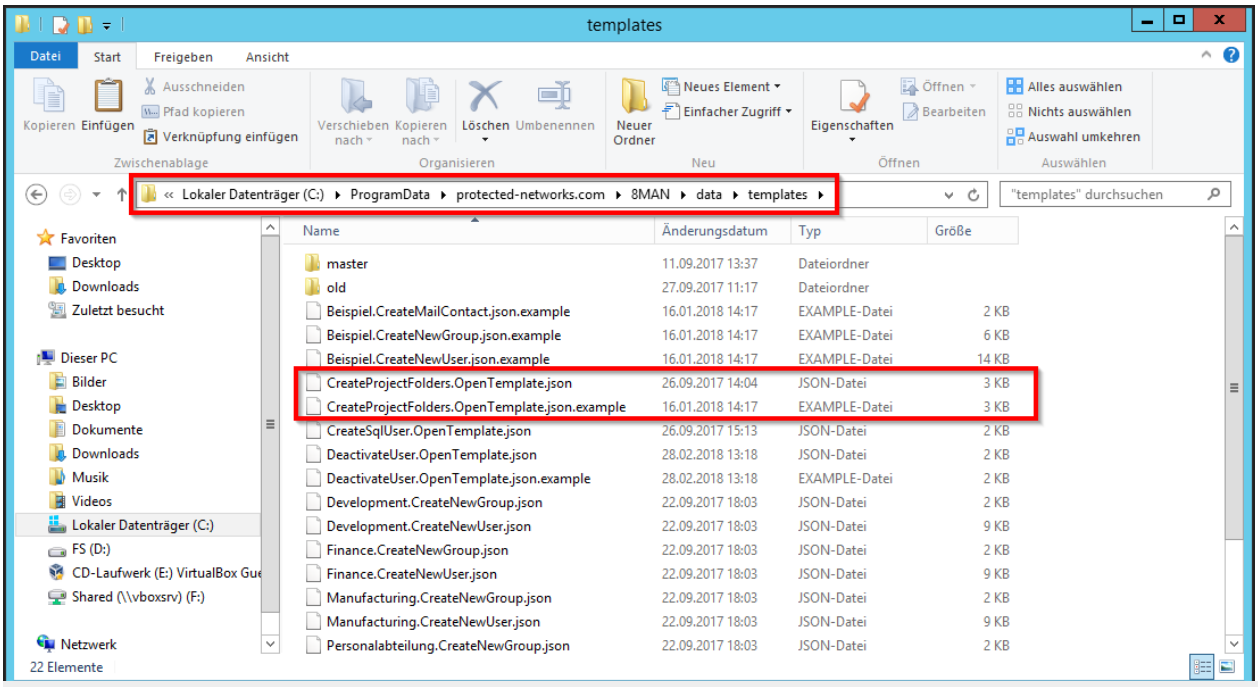
An example is the option described below of ordering the deactivation of a user:

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



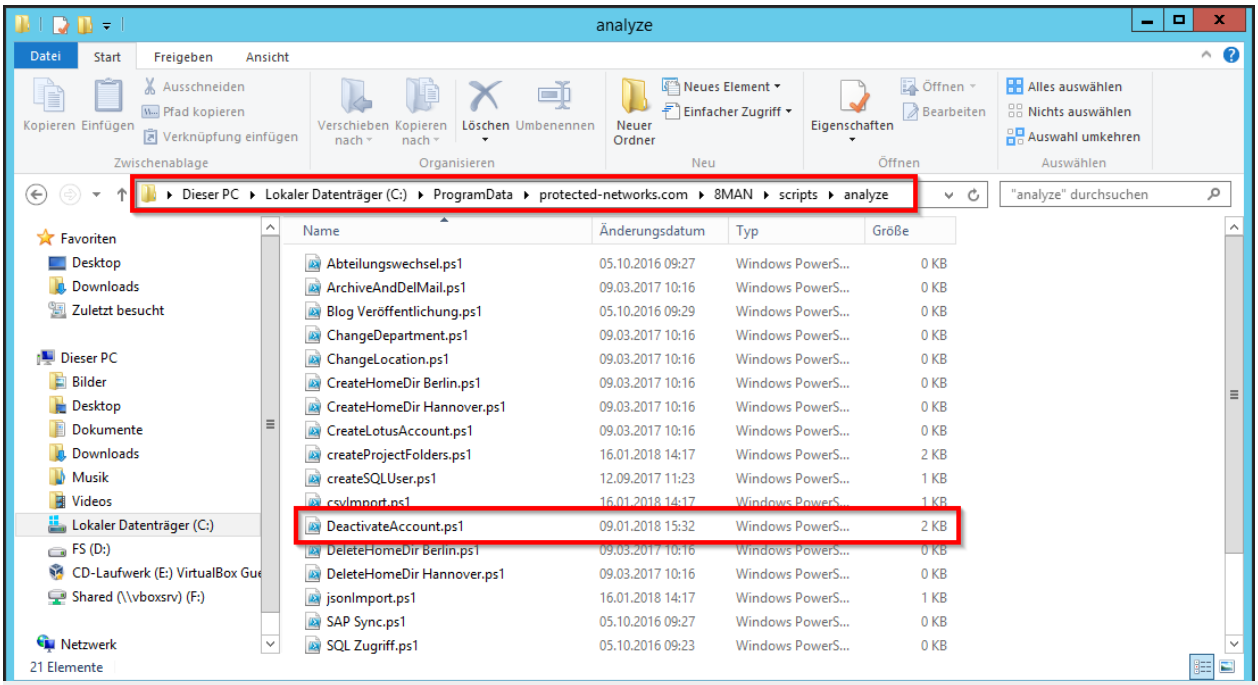
In the directory

```
%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.

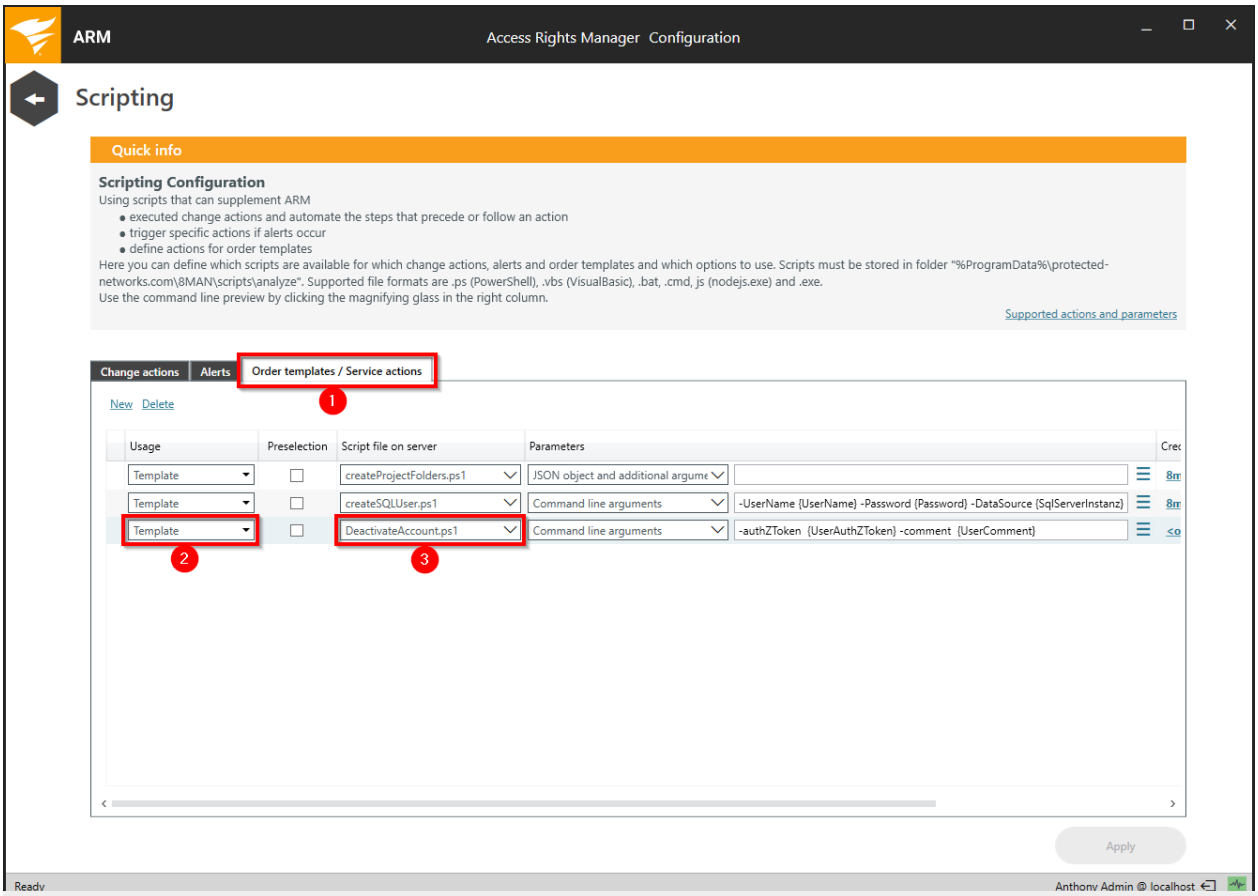
The template will be loaded automatically. Errors while loading the template are displayed in the server health check.



In the directory

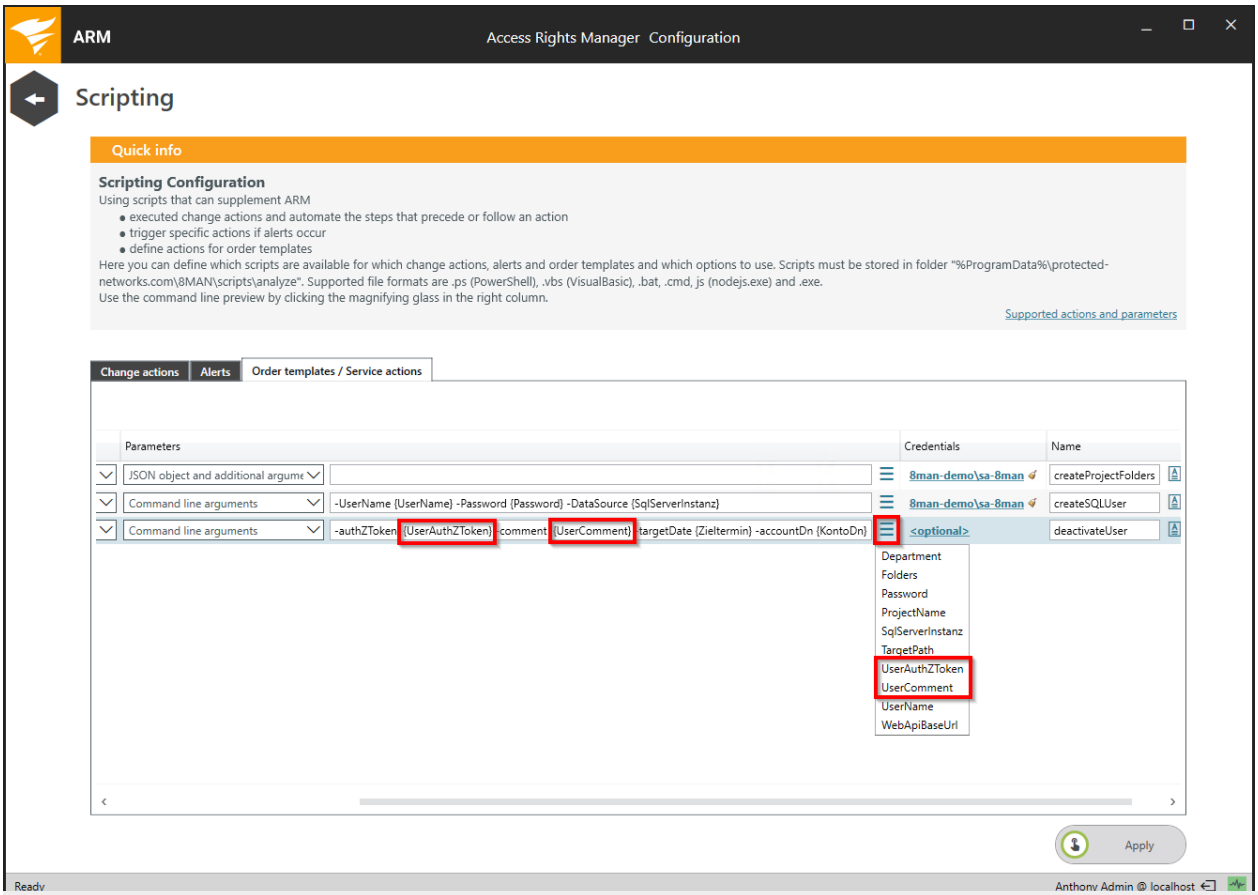
```
OLD: %programdata%\Protected Networks\8MAN\scripts\analyze
NEW: %programdata%\SolarWinds\ARM\scripts\analyze
```

ARM provides a sample script for disabling users.



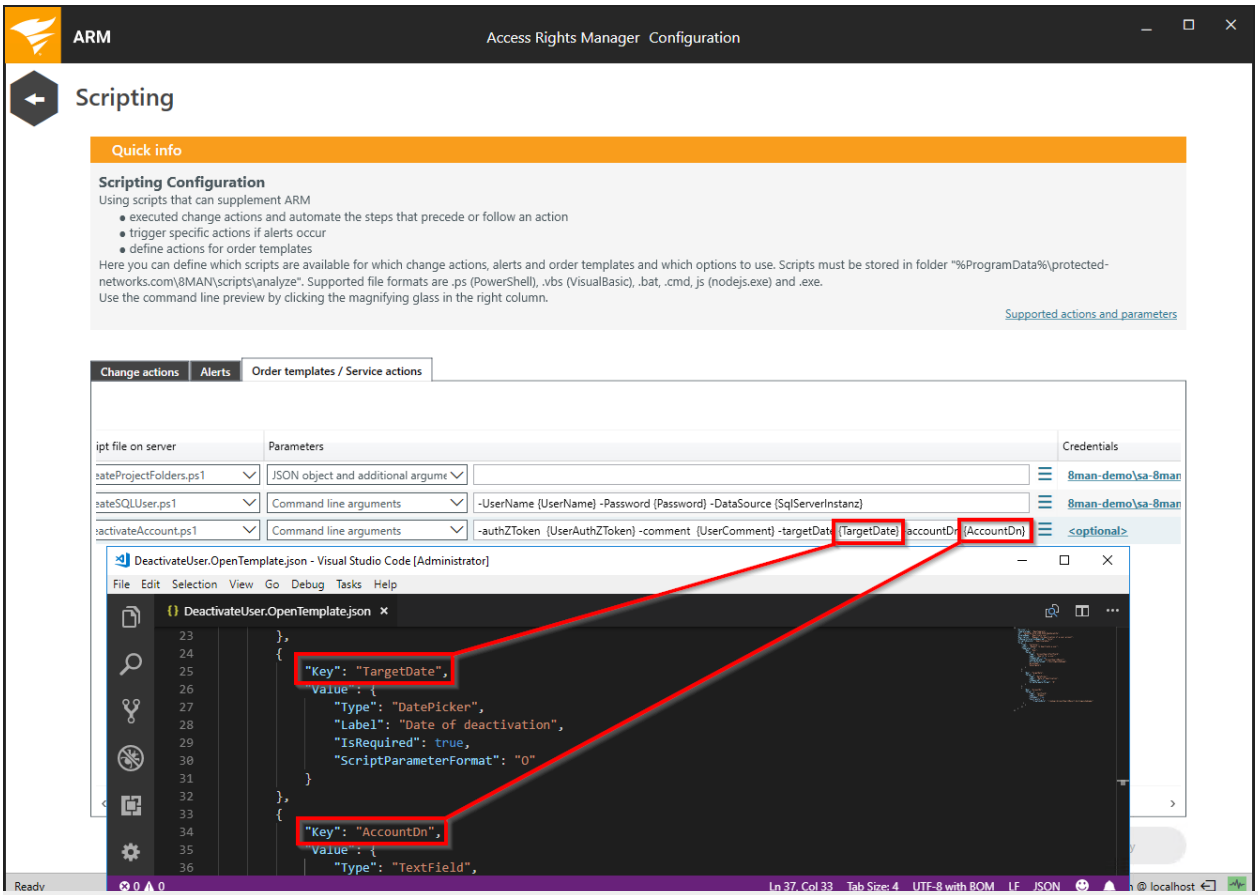
On the start page of the ARM configuration select "Scripts".

1. Click on the tab "Order templates / Service actions".
2. Choose "Template".
3. Select the script, in this example here "DeactivateAccount.ps1".



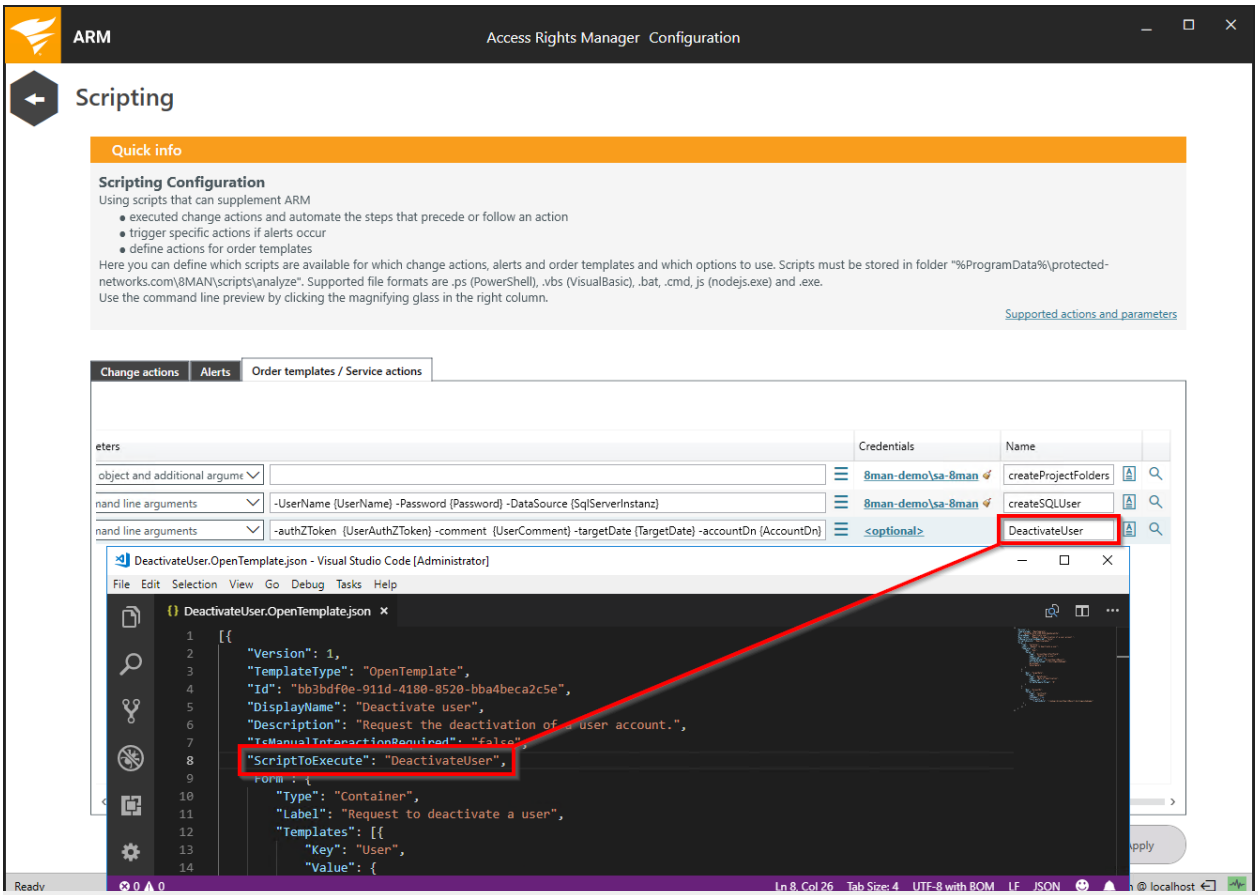
Specify which parameters are passed to the script.

In the example here, the authentication token and the comment are passed.

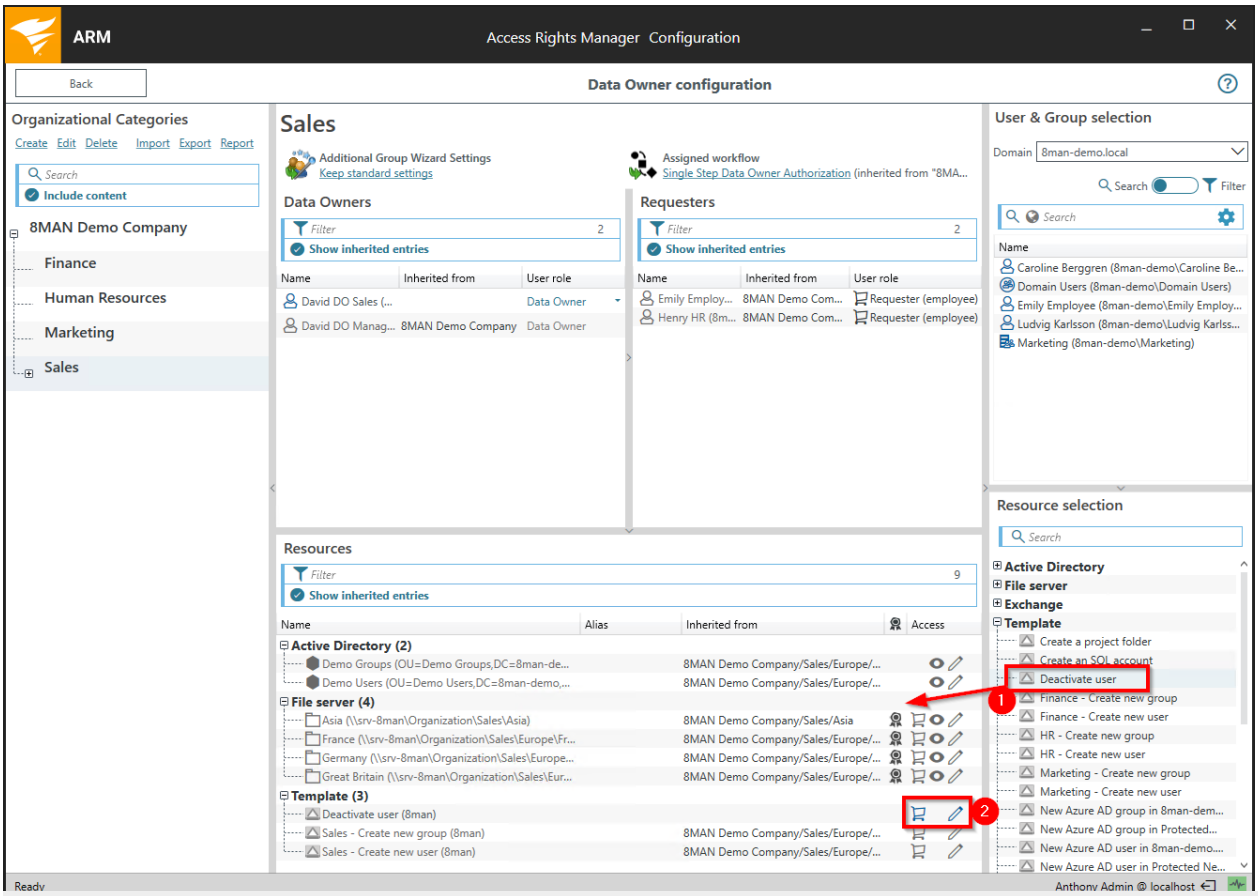


In addition, the values queried in the template are passed to the script:

- The name of the account to be deactivated
- The date on which the account should be deactivated

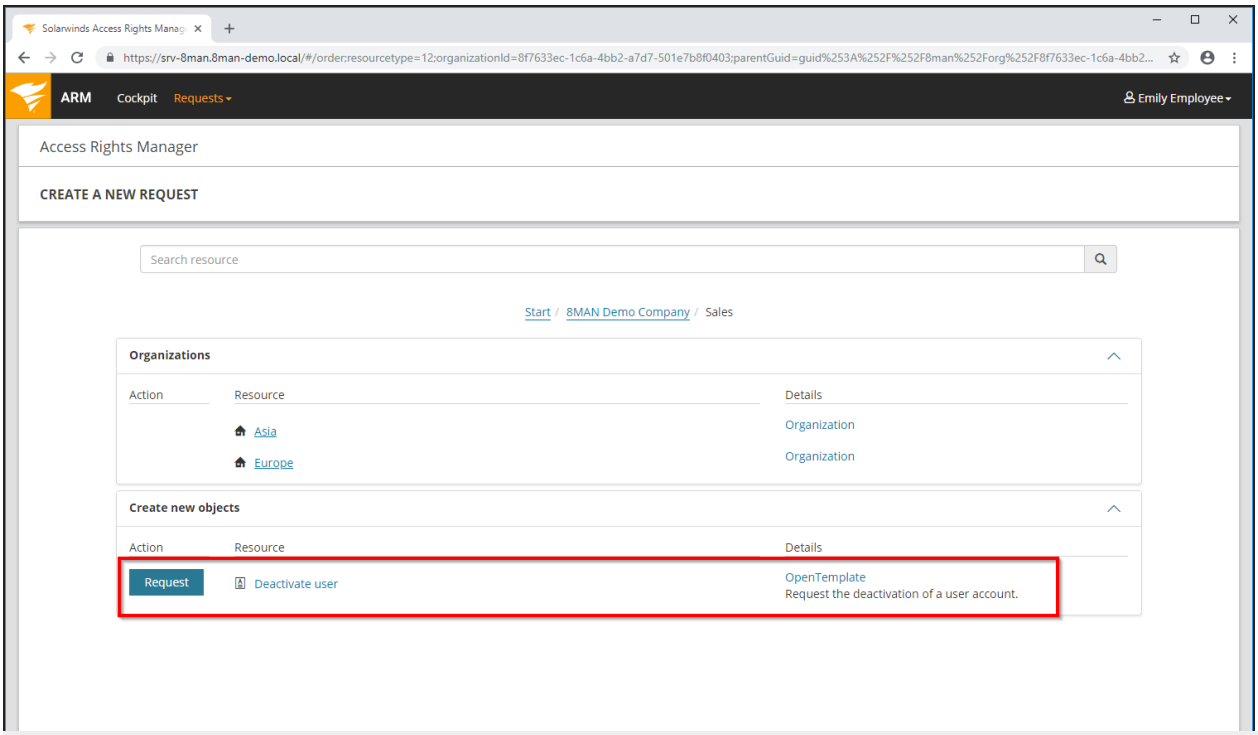


Enter the name of the script. The name must match the call in the template.

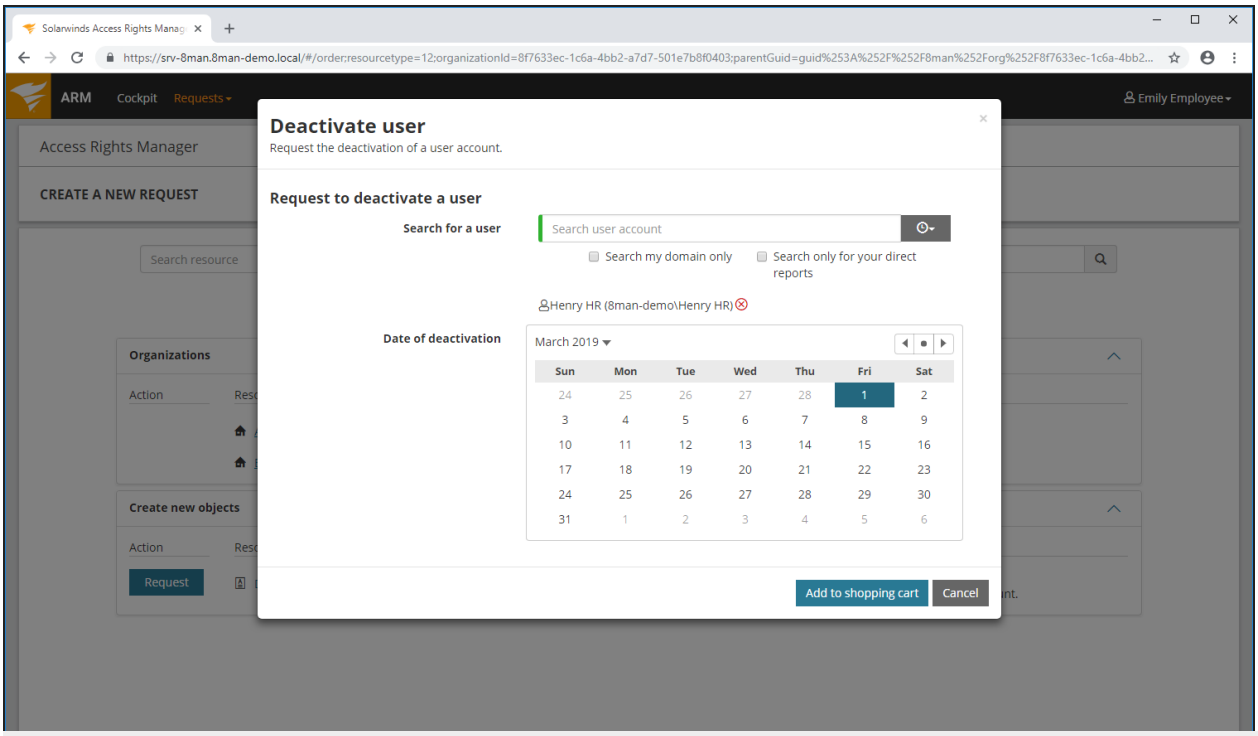


In the Data Owner configuration you set the template to requestable.

1. Use Drag & Drop to add the template to an organizational category.
2. The template must be requestable (default) and modifiable.



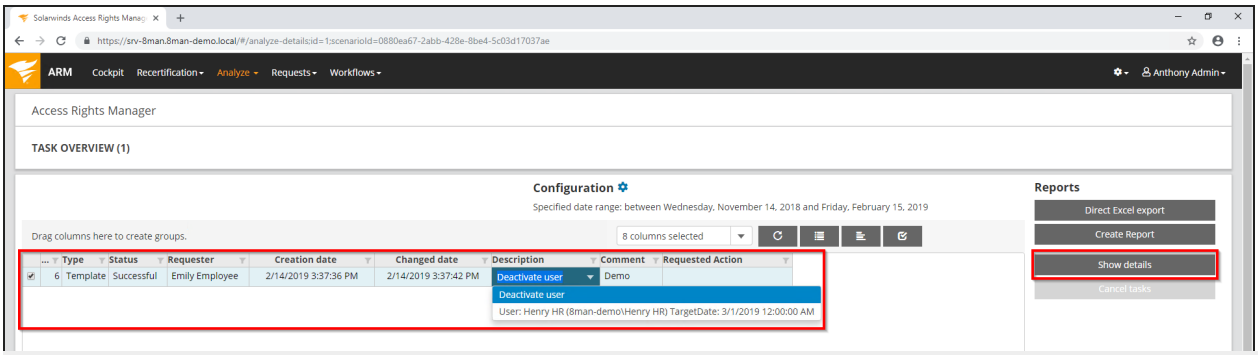
Start the request in GrantMA.



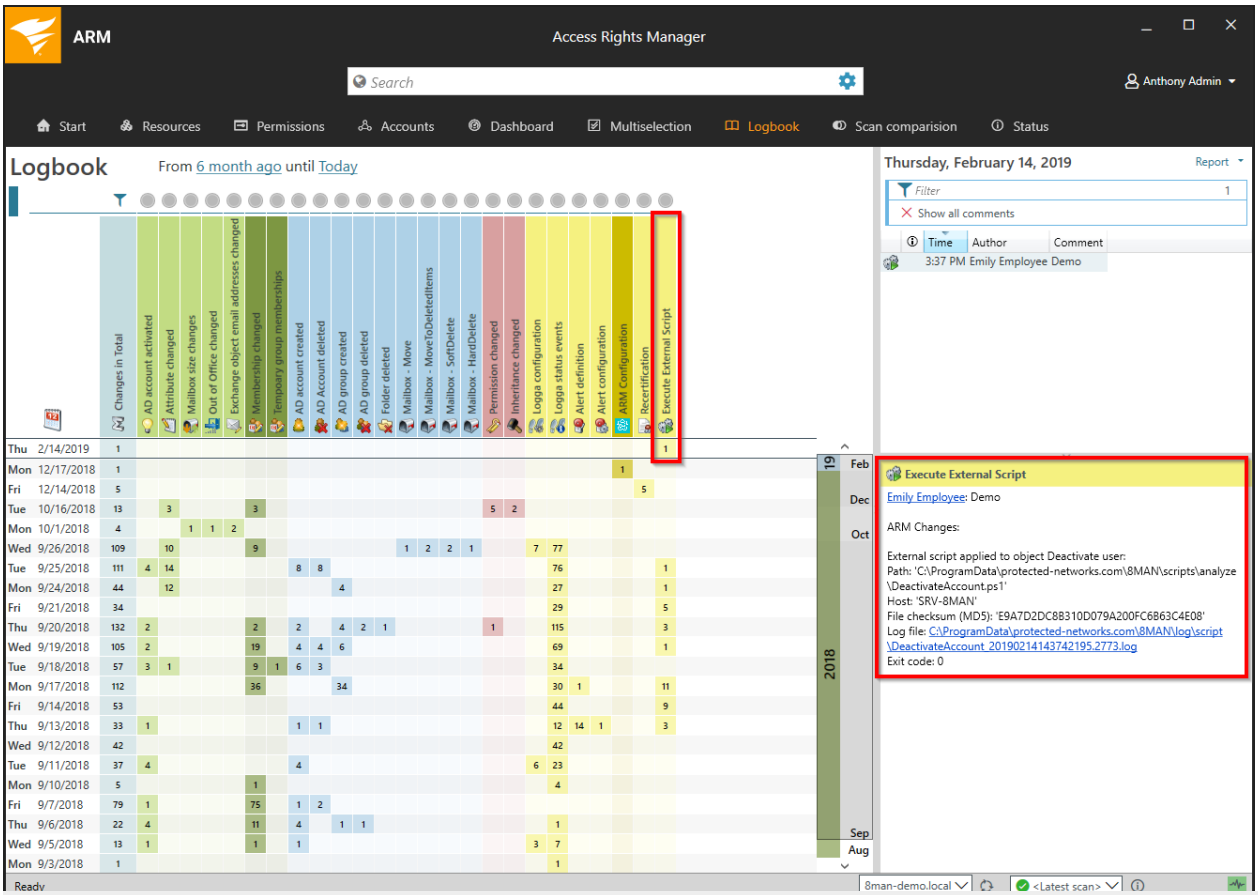
The freely configurable template queries the values that will later be passed as parameters to the script. In the example here:

- 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.

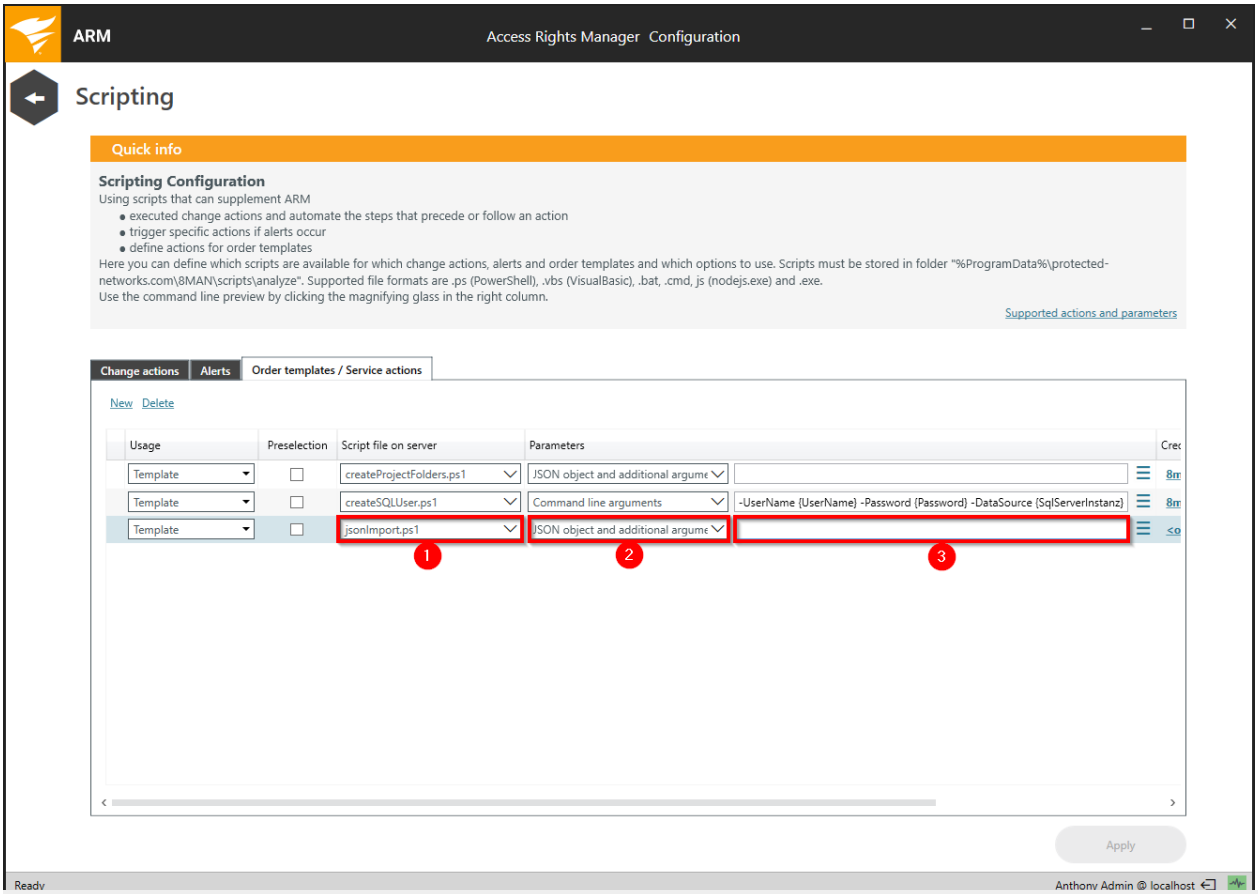
Location

```
%ProgramData%\Protected Networks\8MAN\scripts\analyze\jsonImport.ps1
```

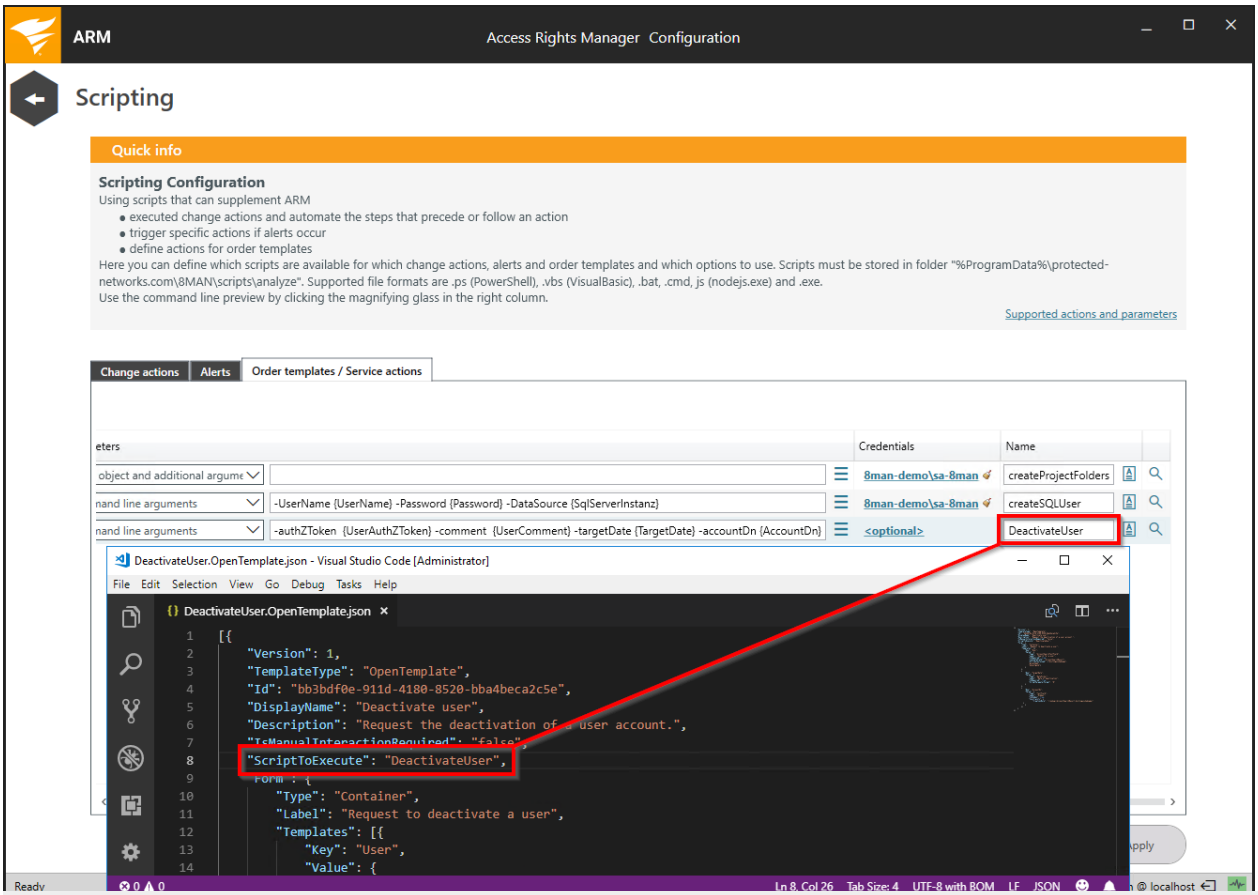
Code

```
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
```

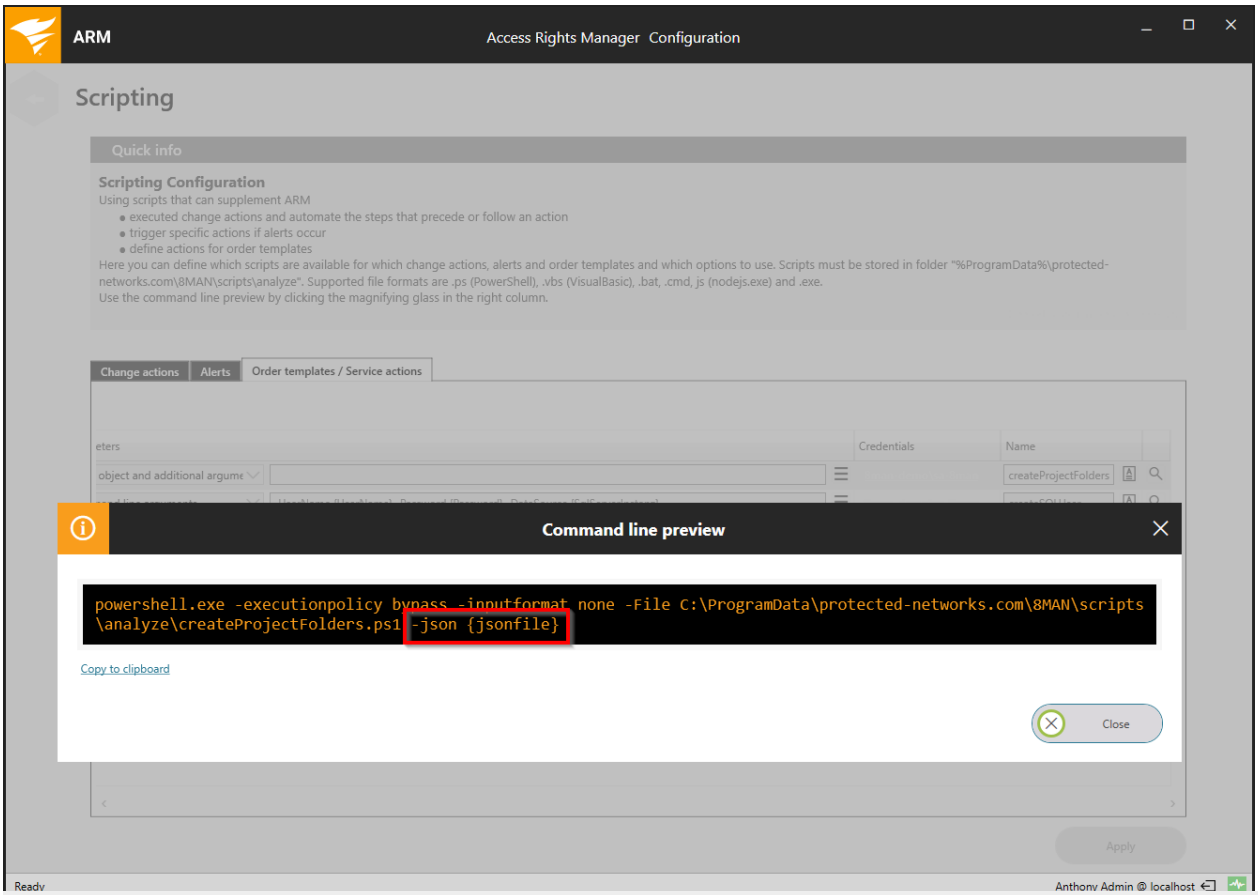
Configuration of the script



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.



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).

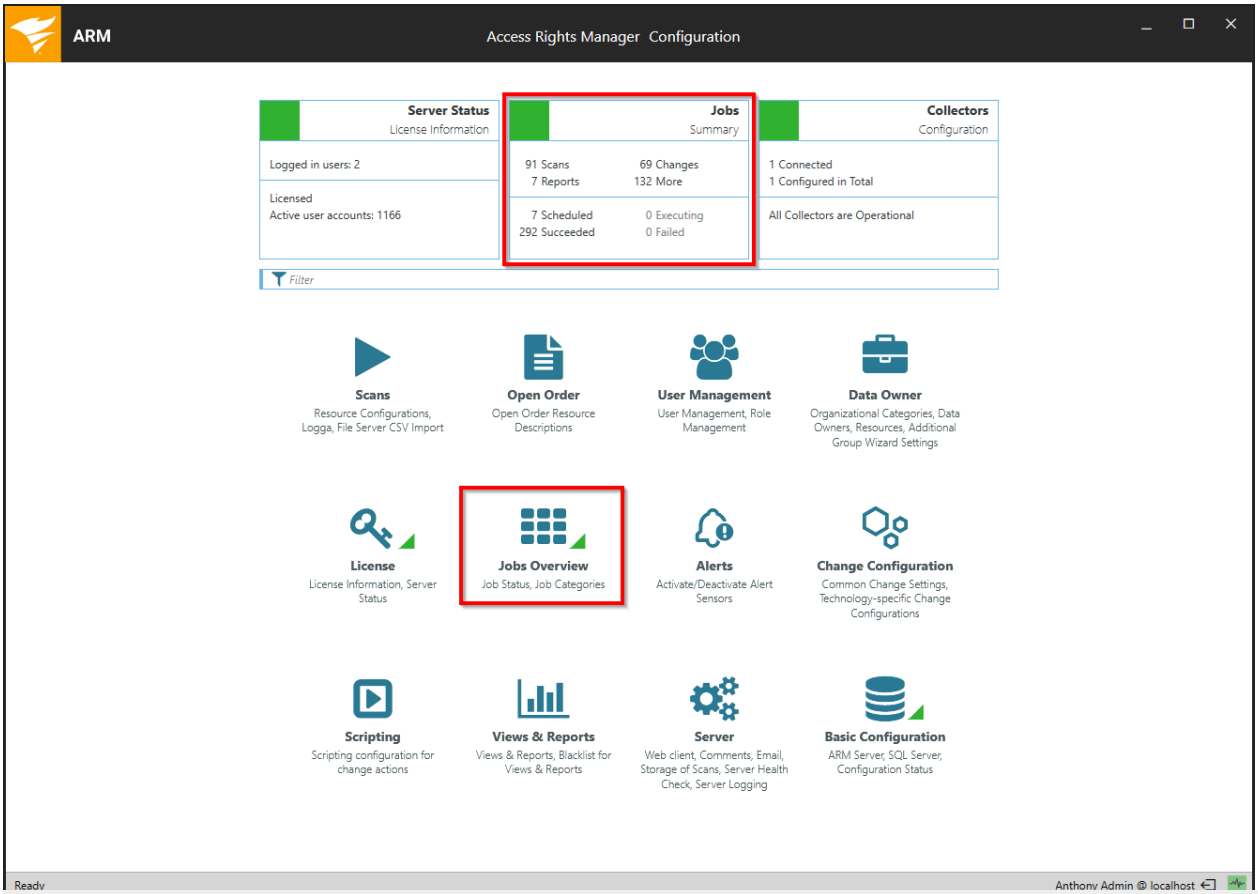
RadioButton

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"
}
```

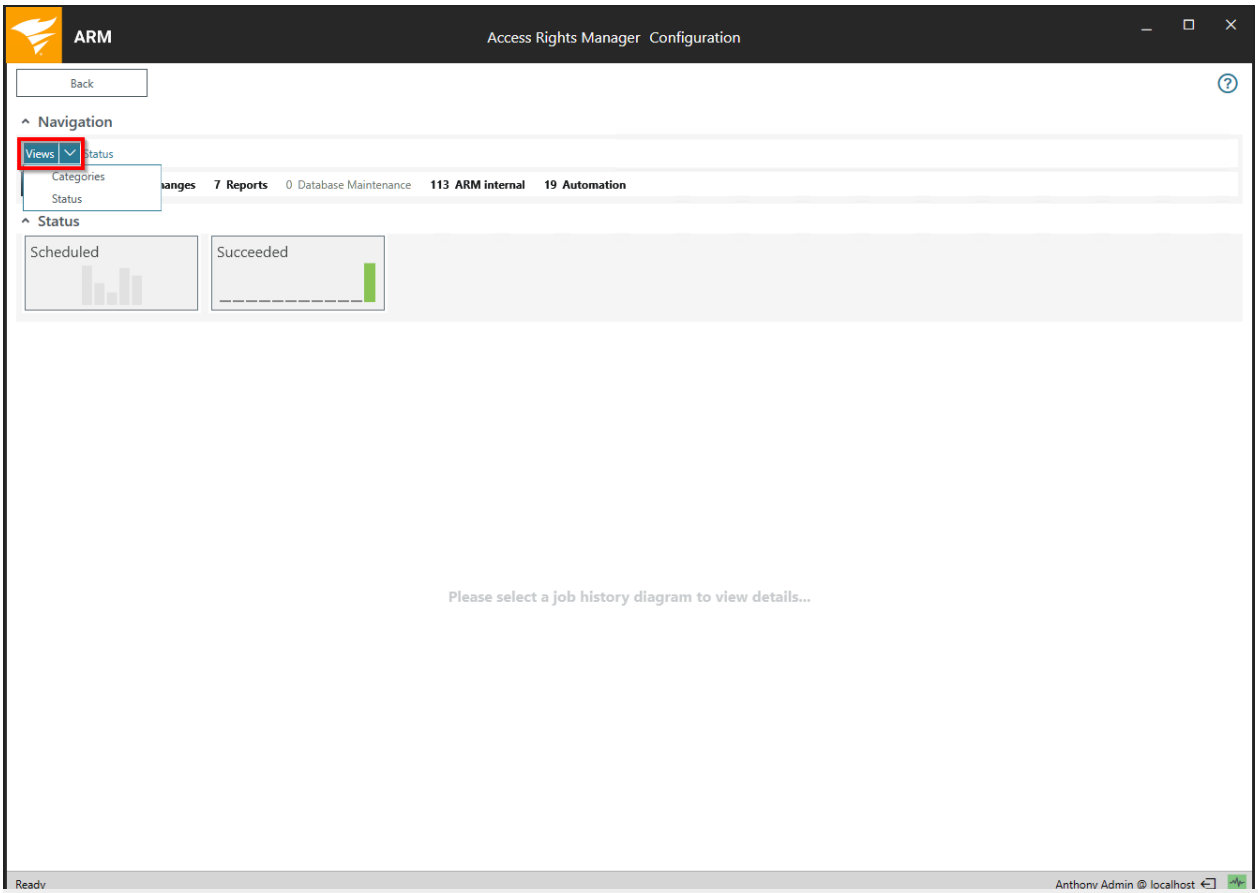
Jobs overview



The job overview contains a variety of information including scan speed and the amount of collected data.

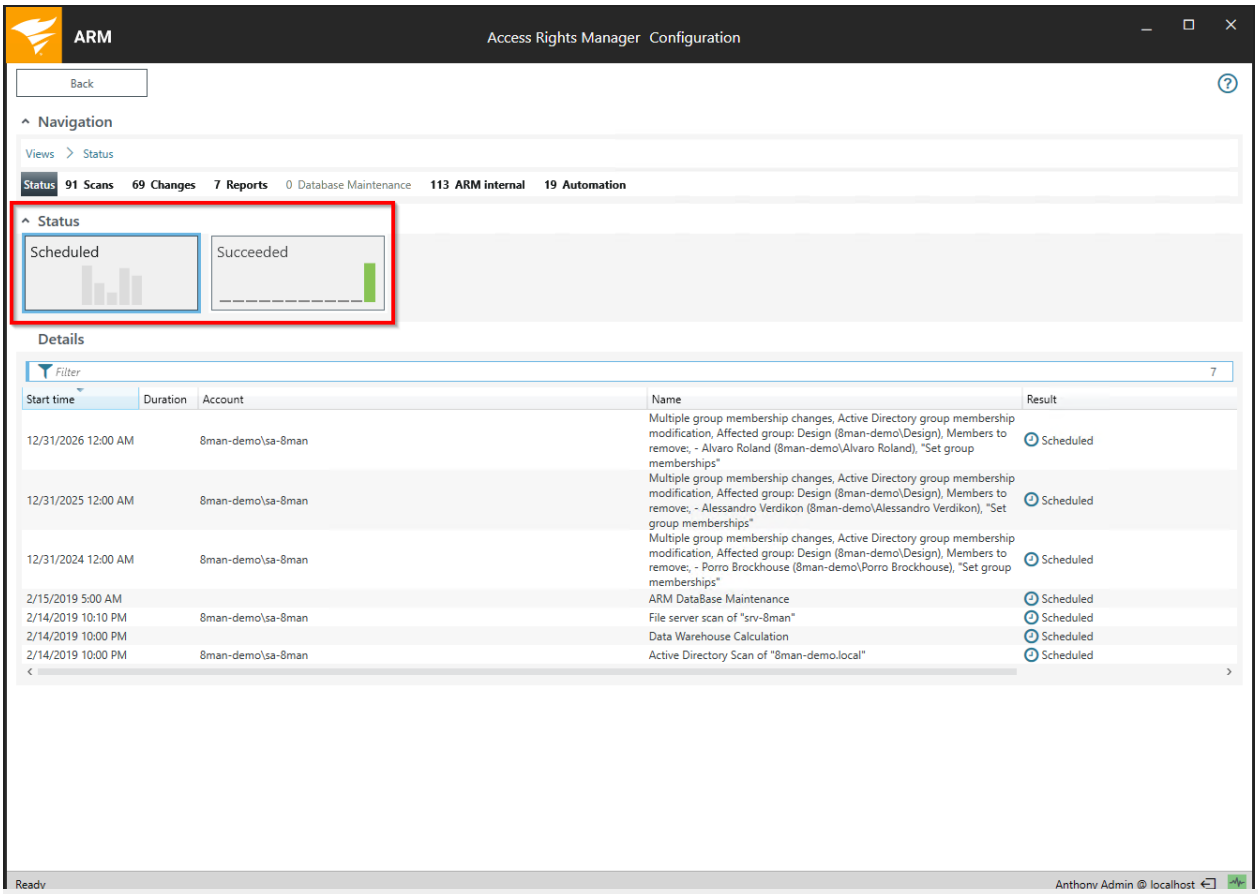
You are not able to edit or configure the displayed information in the job overview tile. Successful jobs are displayed for 2 weeks, failed jobs for 4 weeks.

Click the tile for more details.



Select between two views.

Display jobs grouped by status

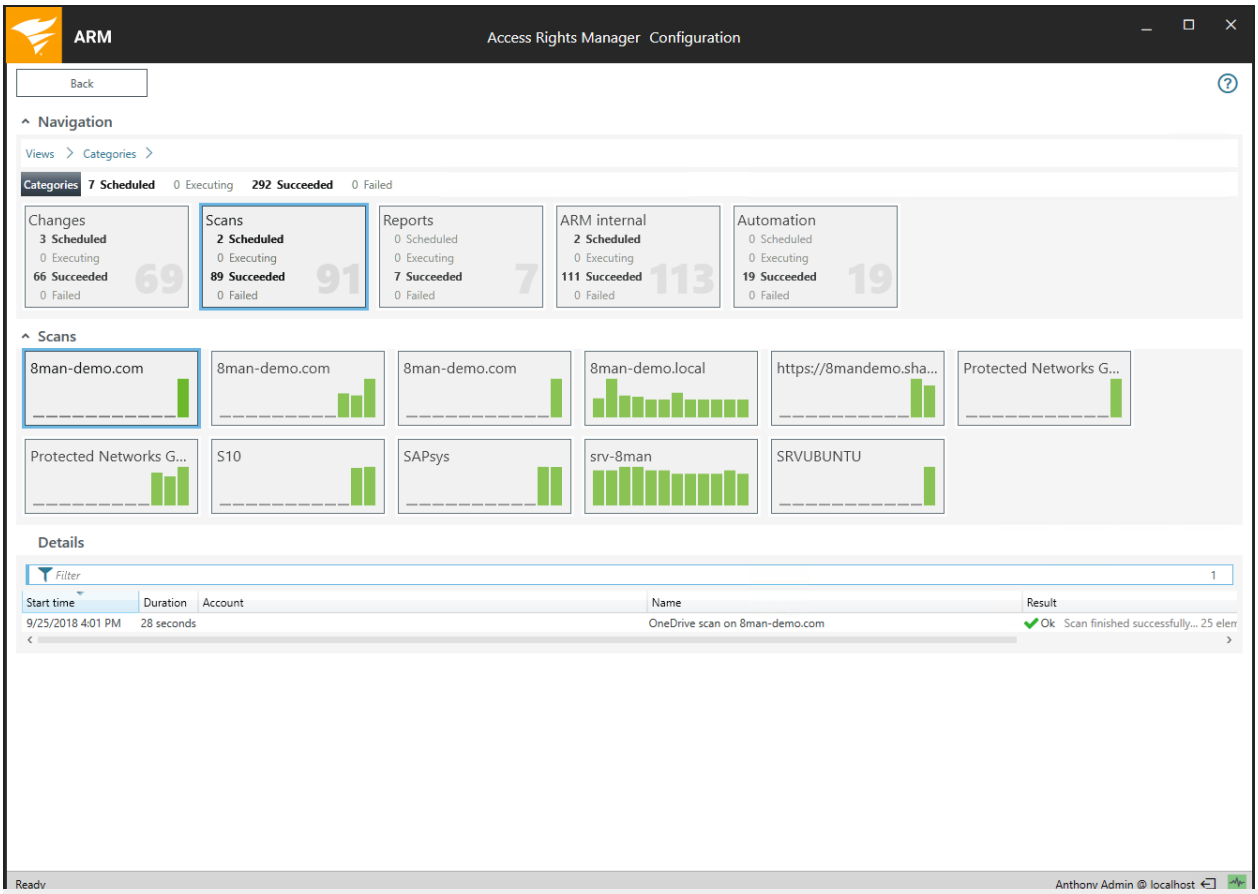


You can see a job progress diagram for every status.

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

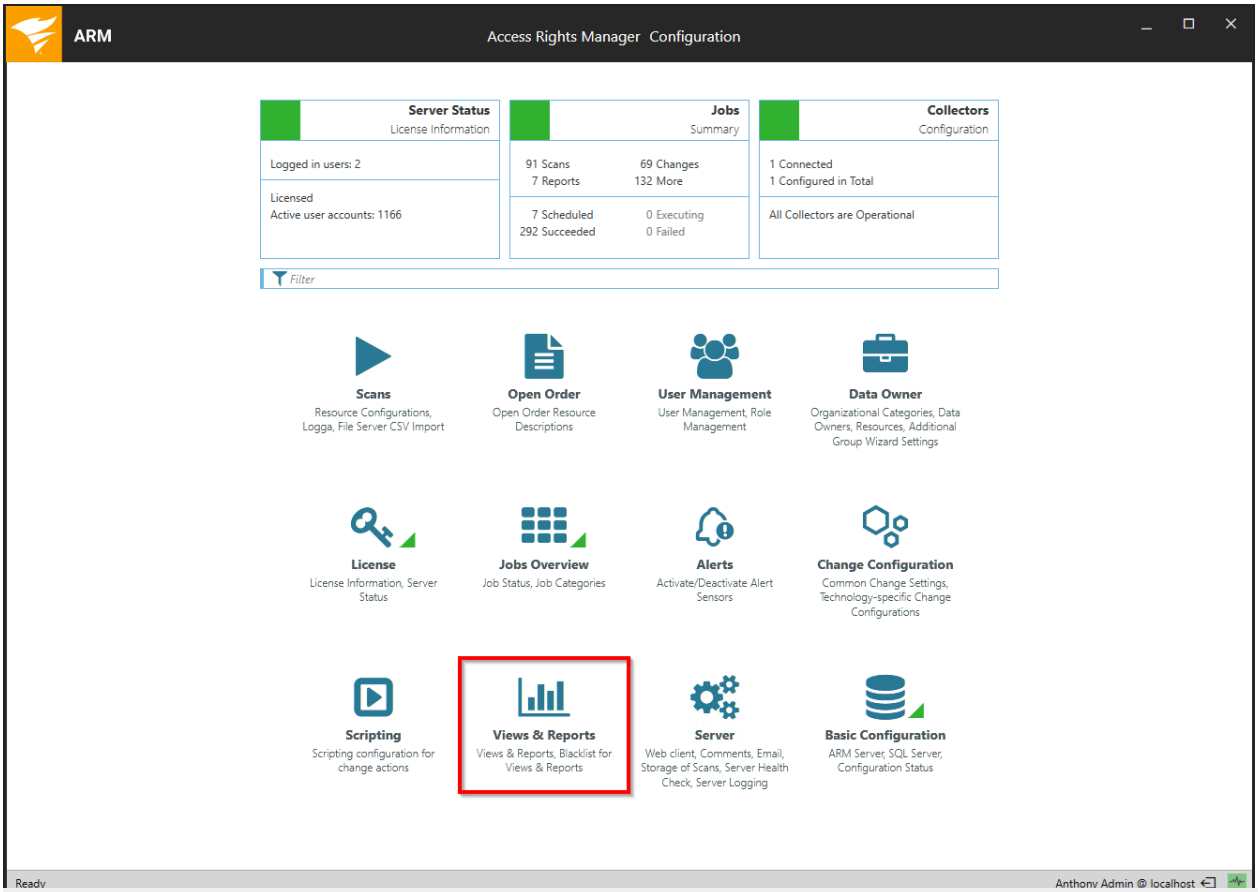


In the category view the jobs are listed in more granularity.

ARM provides job progress diagrams for each category.

Click on a diagram to list the associated jobs.

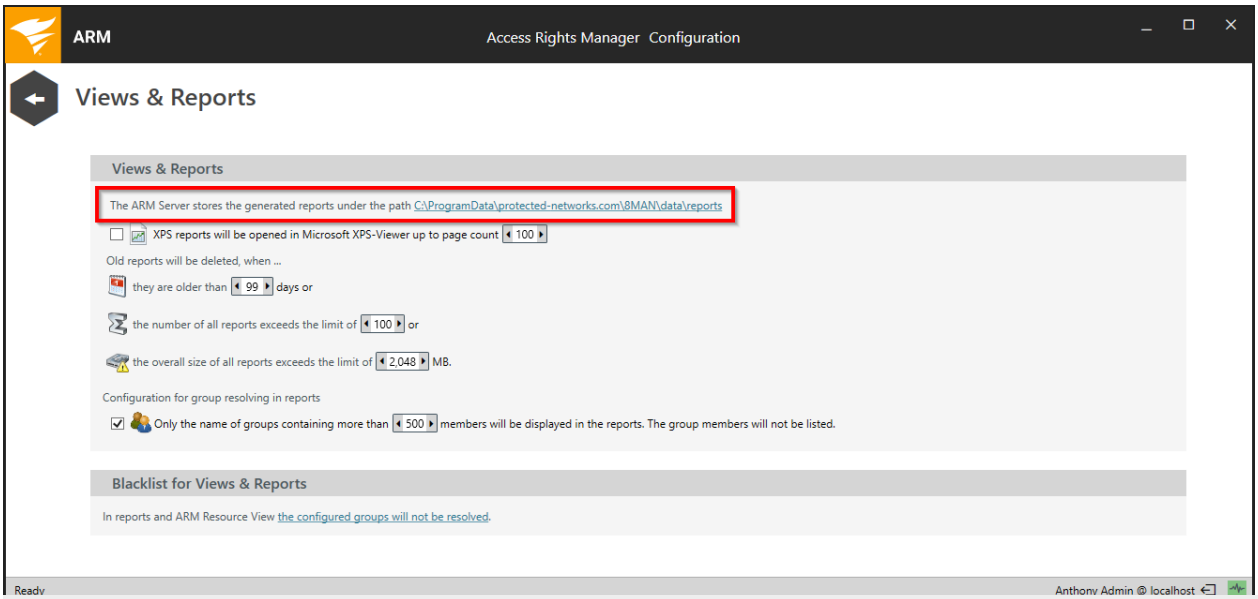
Configure and view reports



Determine the options for report creation, views and blacklists.

Click on "Views & reports".

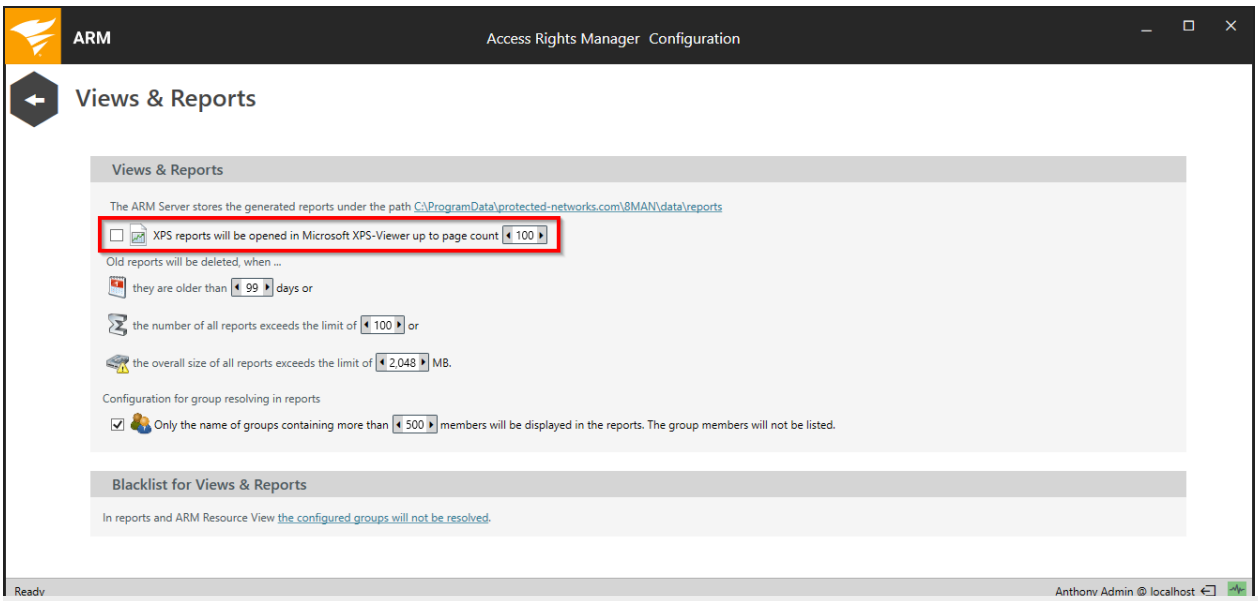
Configure report options



Click the link to determine where ARM stores reports.

The default path is:

```
%ProgramData%\protected-networks.com\8MAN\data\reports
```



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:

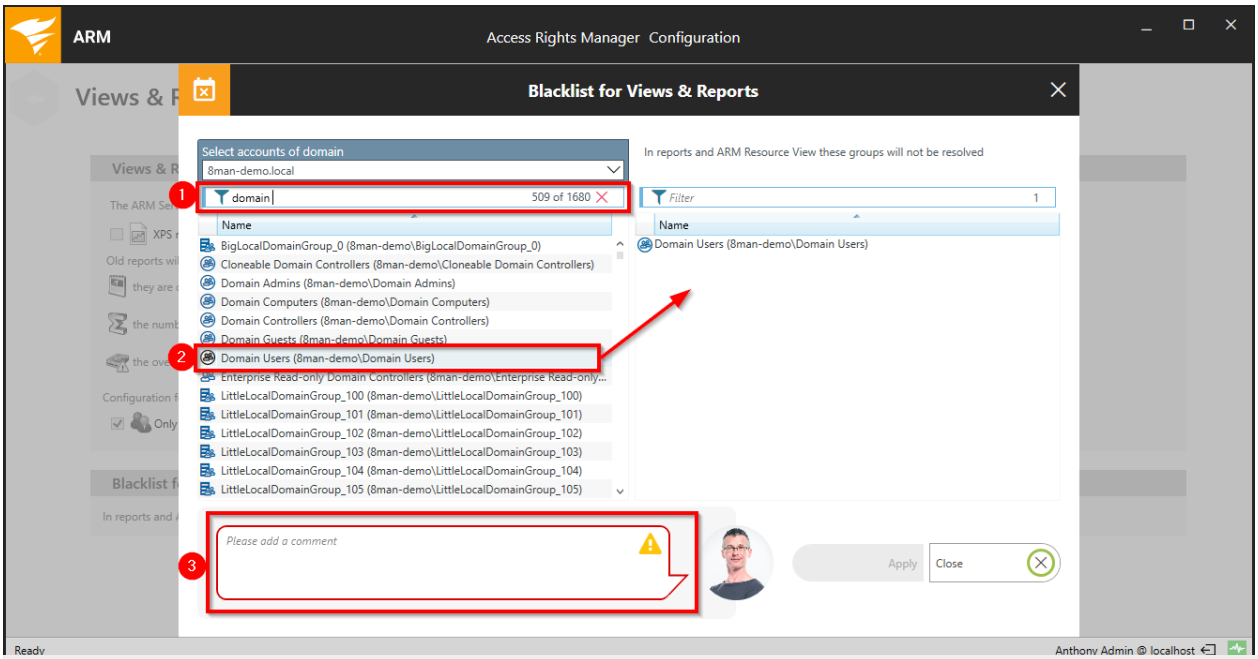
- reports
- views in ARM application
- Analyze&Act web interface

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)

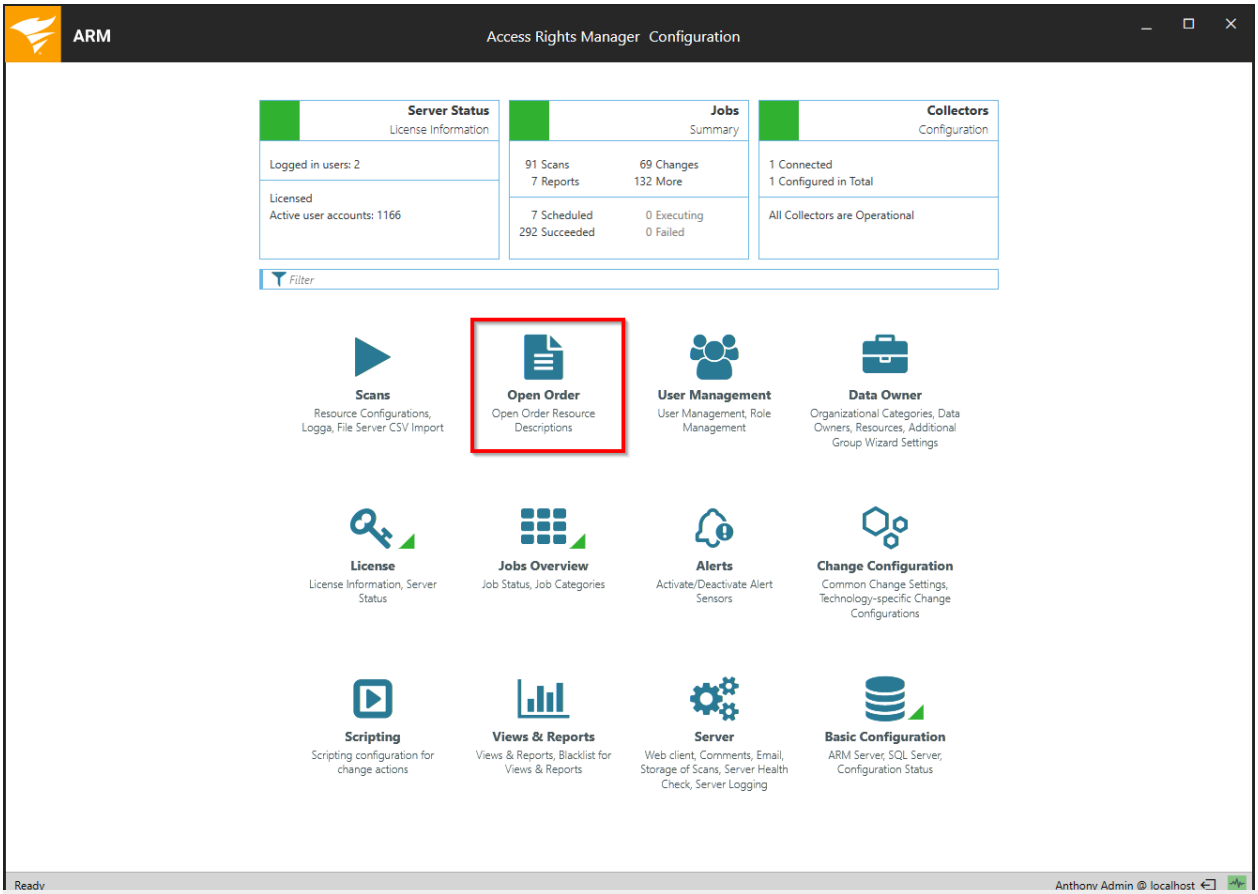
Hiding group memberships may also be required in order to ensure compliance with company regulations and guidelines.

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



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

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

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

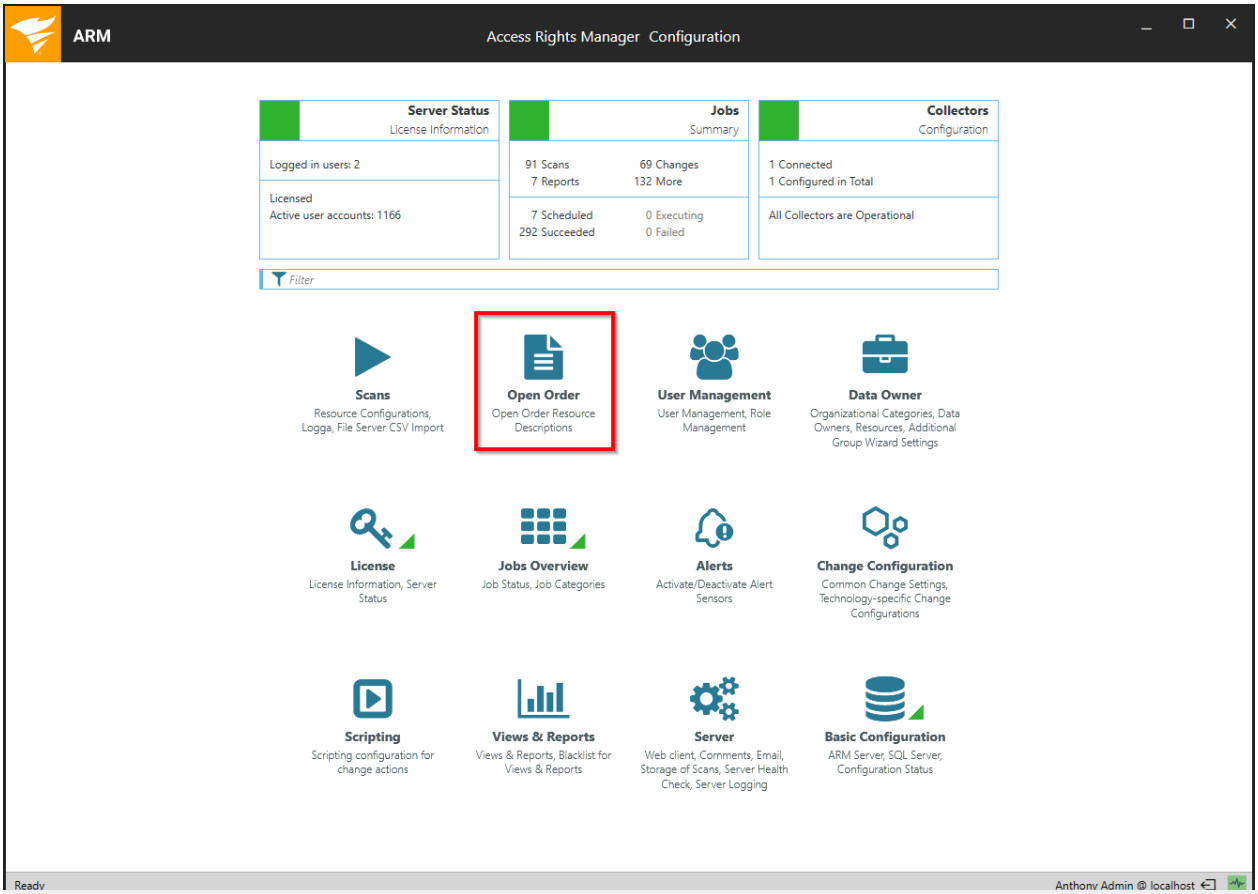
```
Description="['en-US:Buy','de-DE:Kaufen','fr-FR:Acheter']
```

You can add additional languages. Use the Windows Language Code Identifier (LCID).

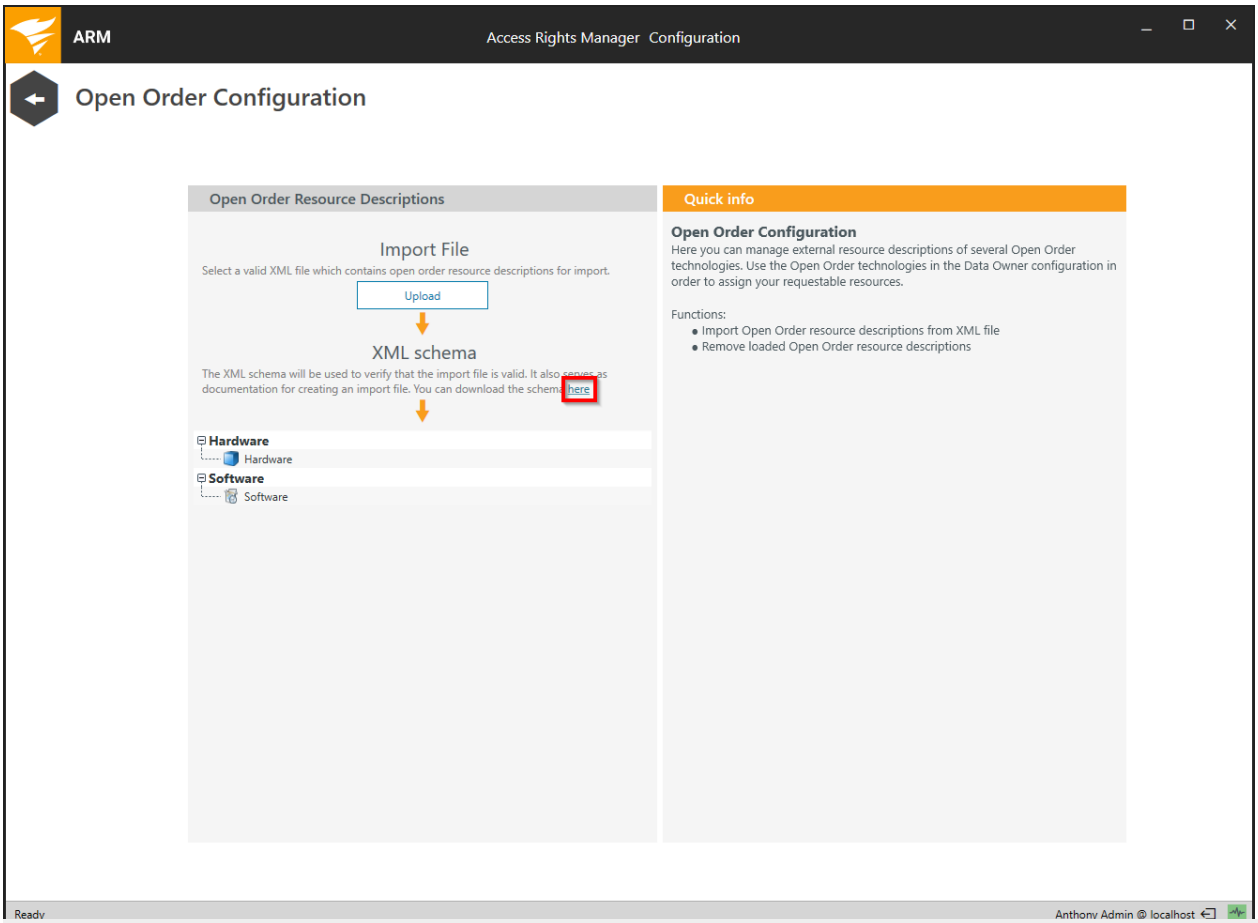
If you need to use an apostrophe (escape character) within the description text, this must be quoted:
`Description="['en-US:PC&quots']`

Validate an XML configuration file

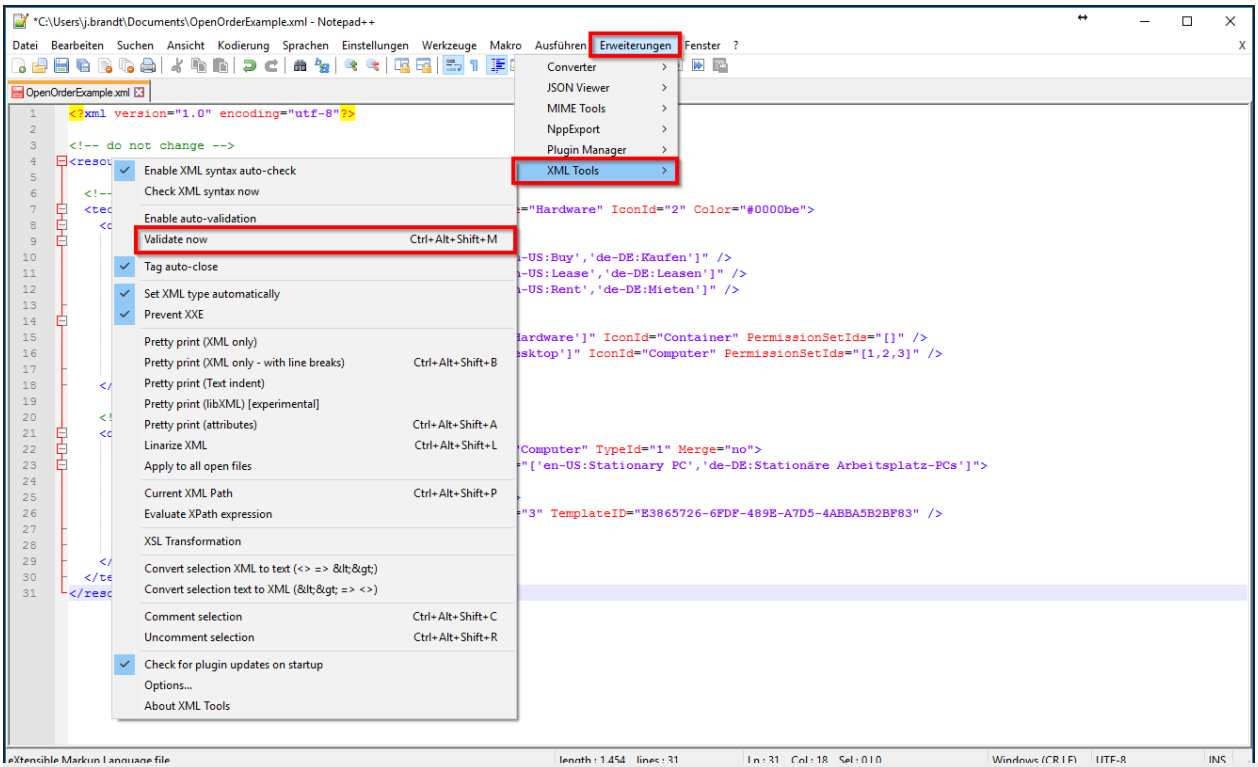
At the latest when uploading to ARM, your XML configuration is validated. You can already check the structure of your XML data in the editor for validity.



In the ARM configuration application, click "Open Order".



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

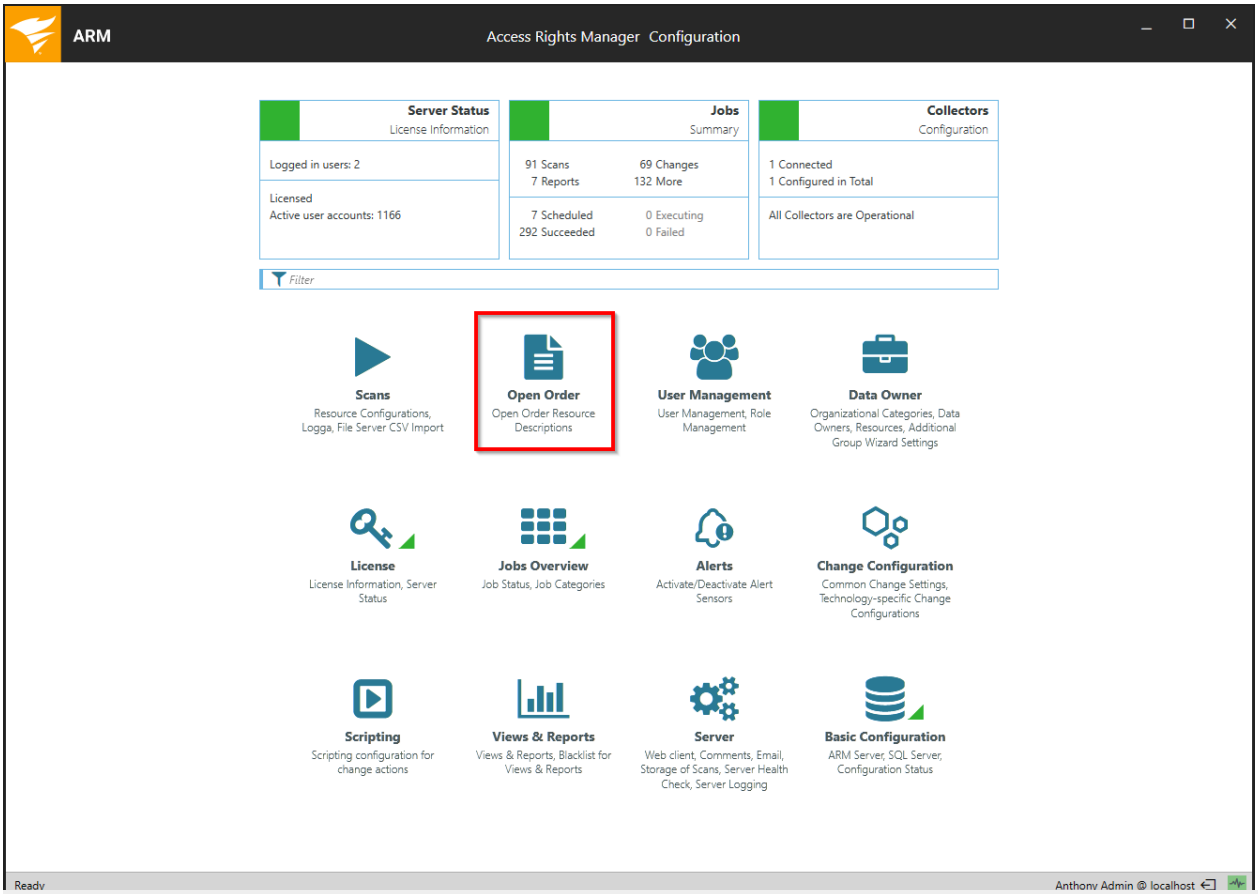
Assign the unique ID of the OpenOrderTemplate to one or more resources.

Example

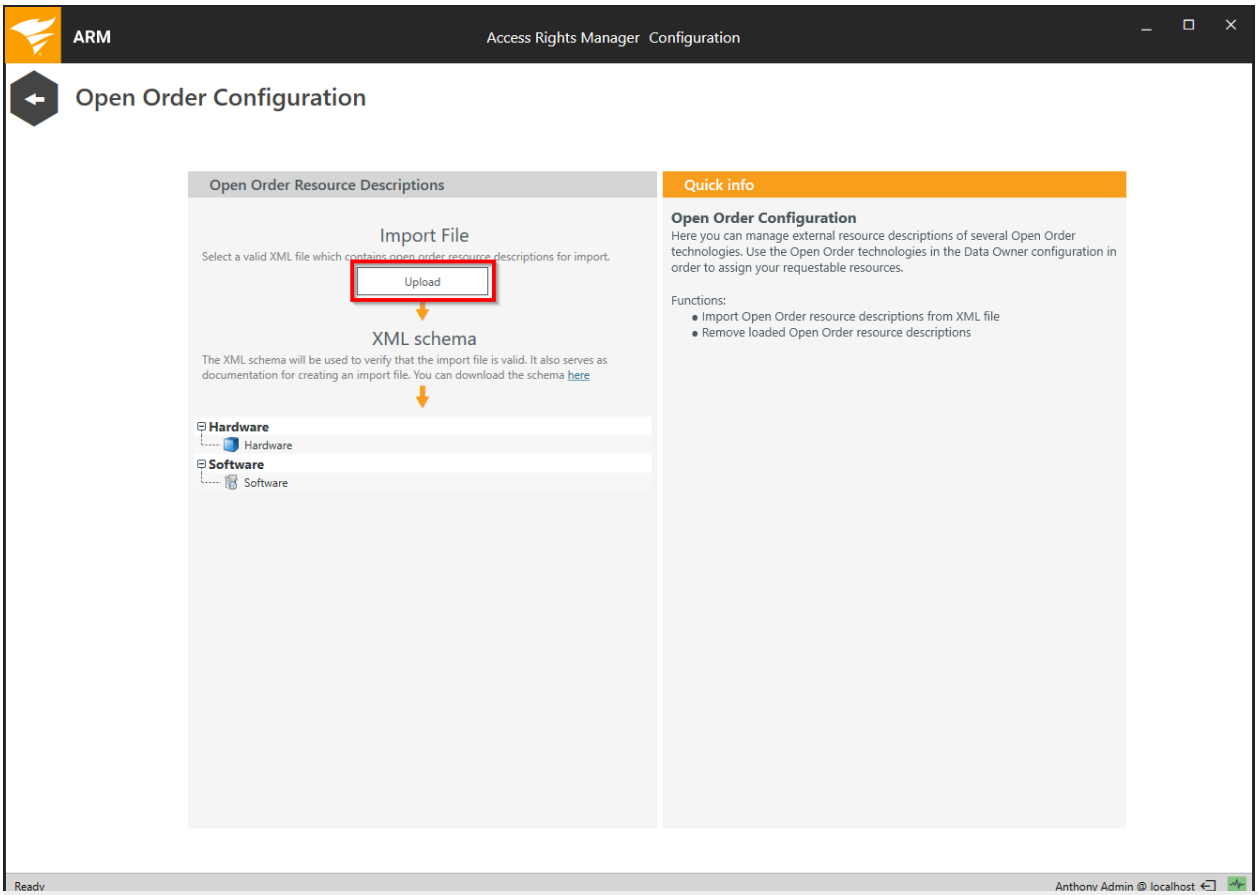
```
<?xml version="1.0" encoding="utf-8"?>

<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



In the ARM configuration application, click "Open Order".

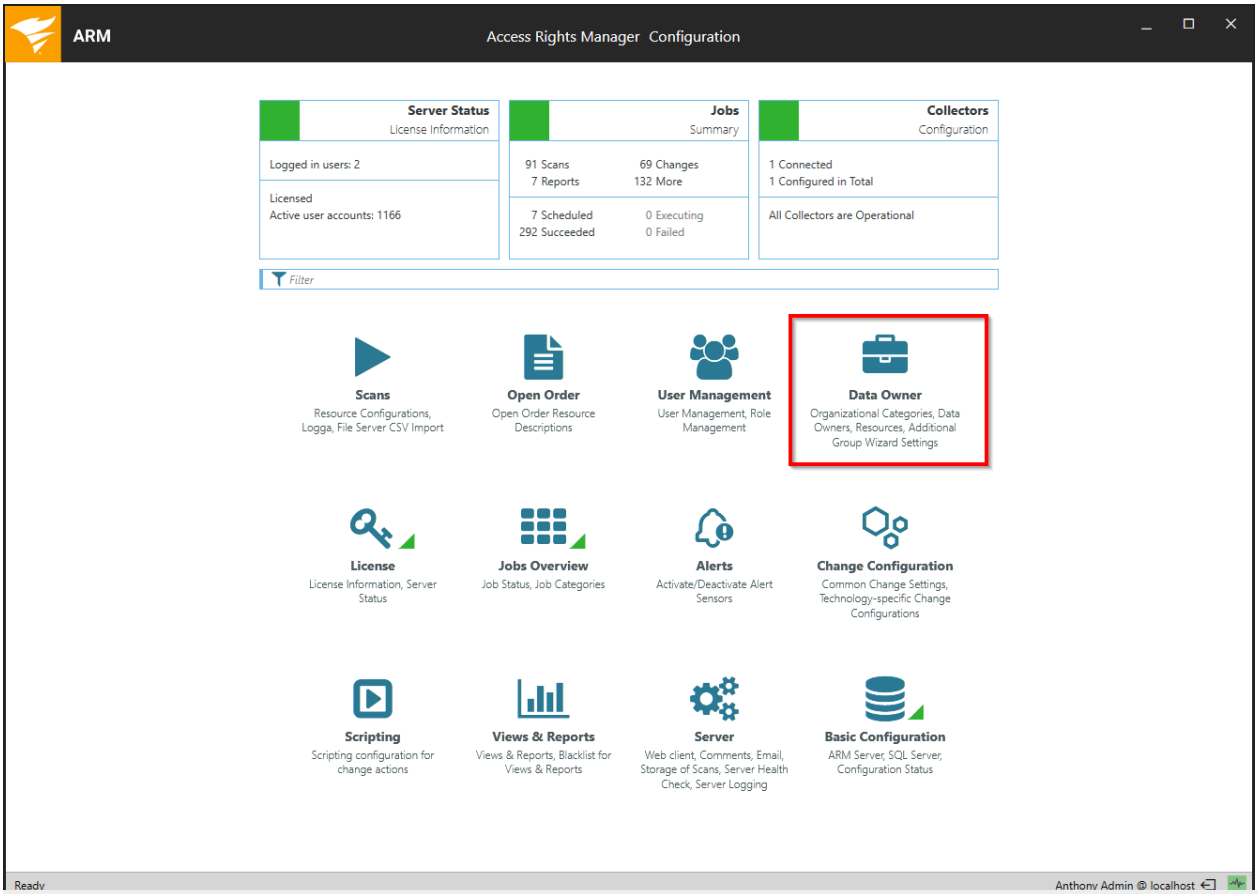


Click "Upload" to import the XML Resource Configuration.

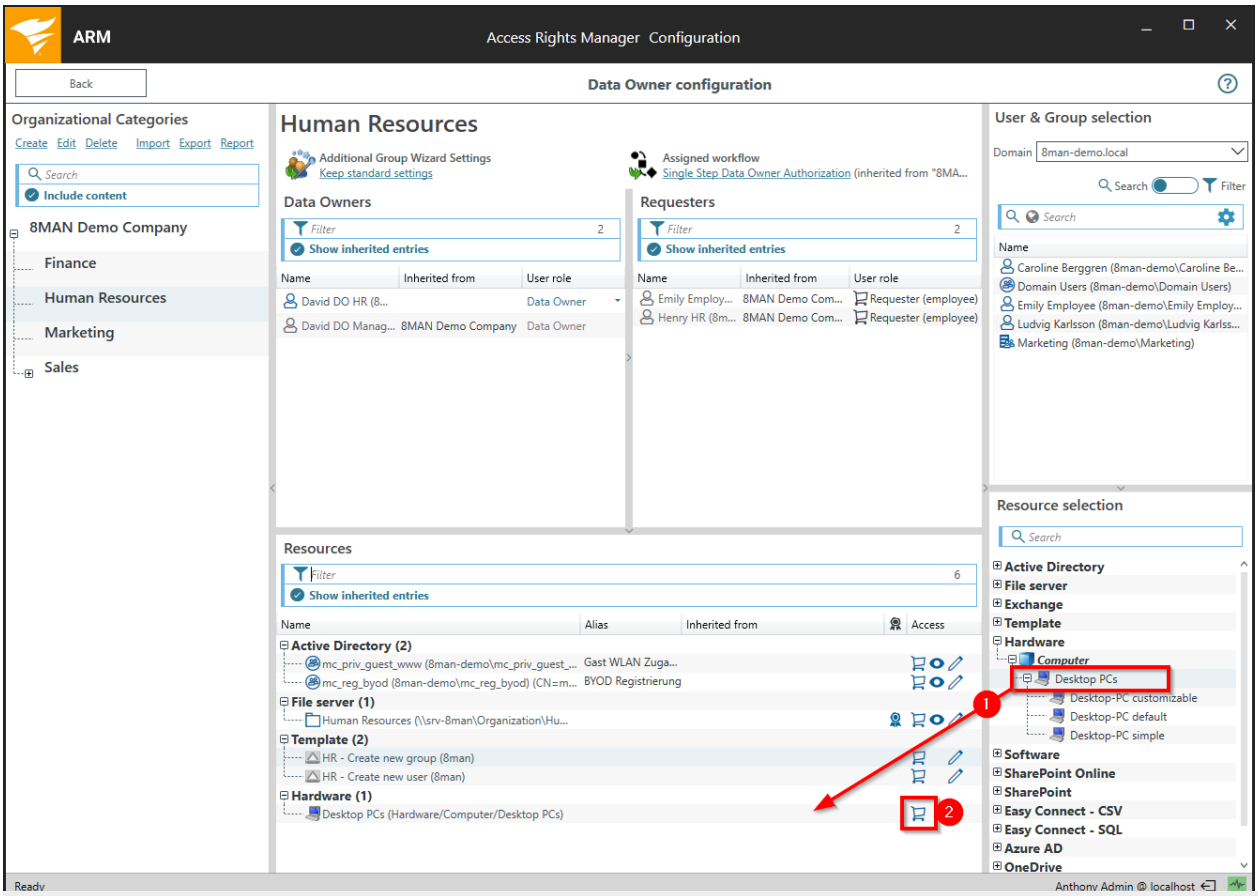
After successful import, the resources are available in the Data Owner configuration and can be assigned to organizational categories (see next chapter).

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.

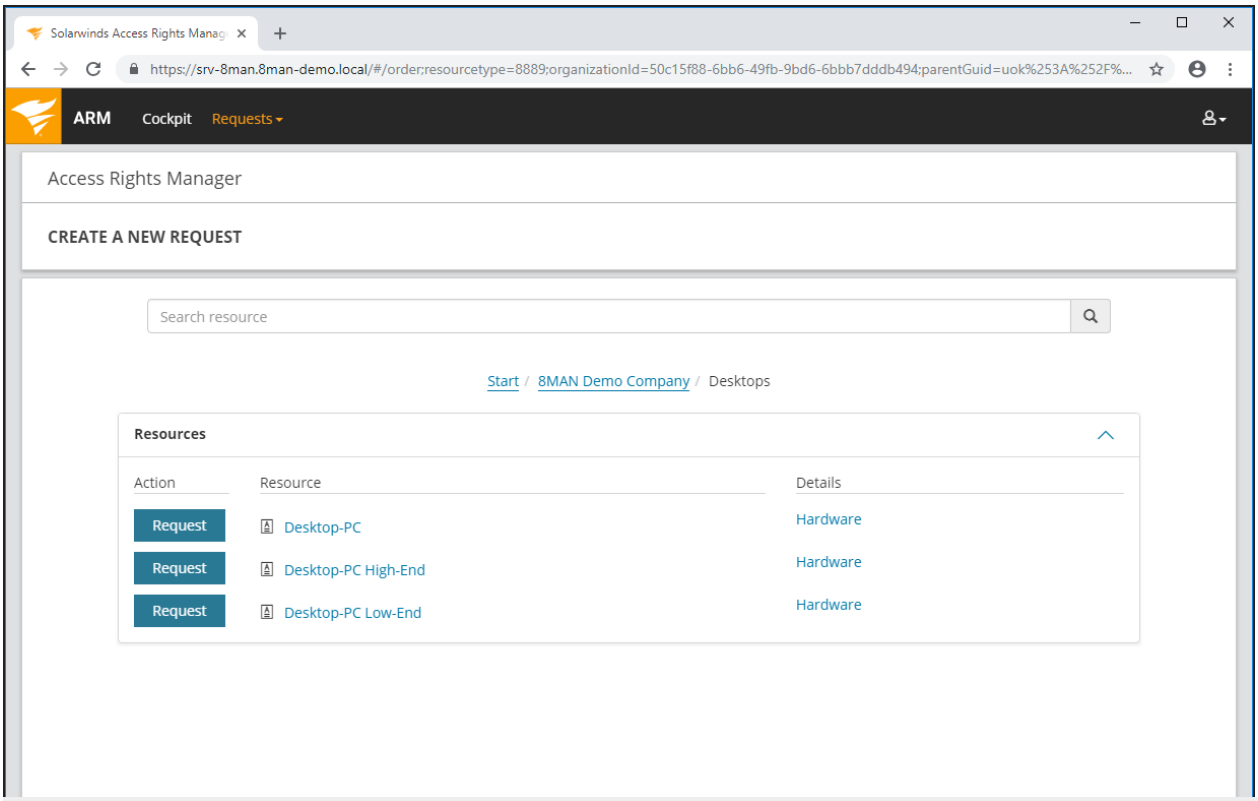
Set the Open Order resource to requestable



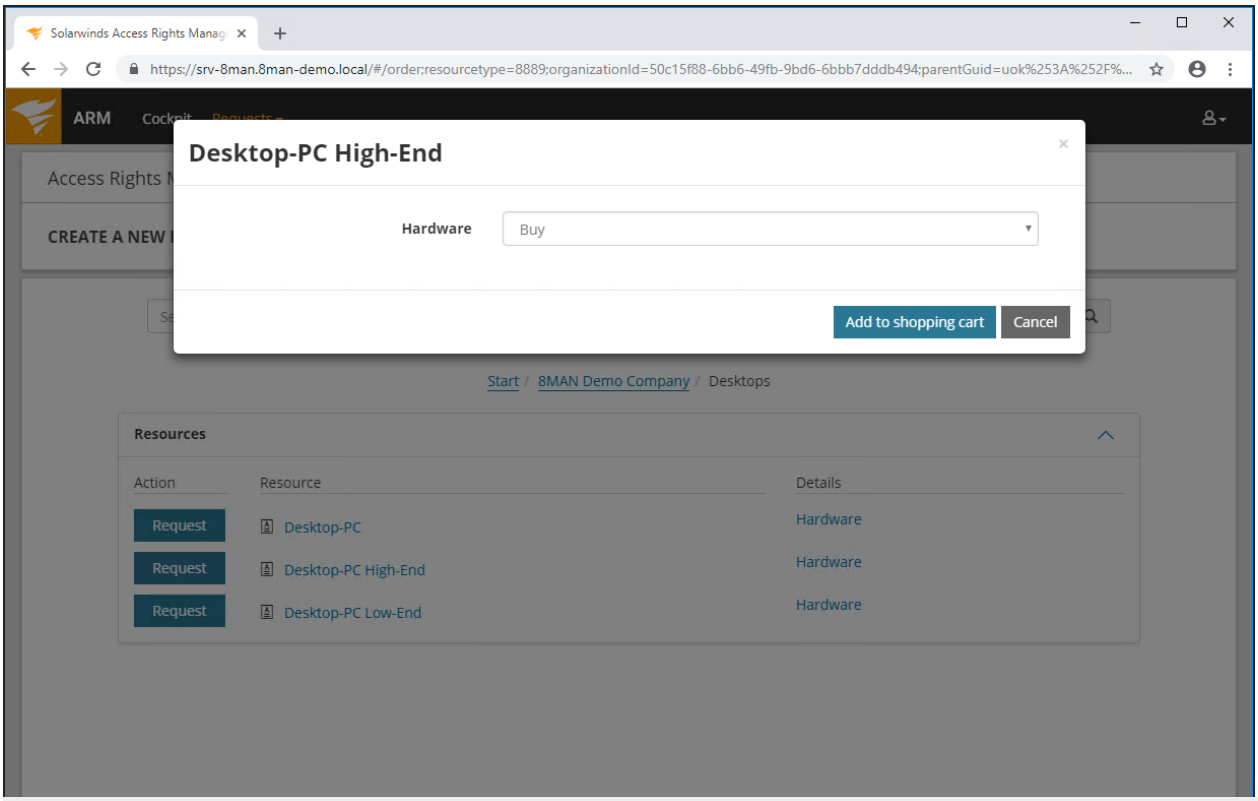
In the ARM configuration application, click "Data Owner".



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.

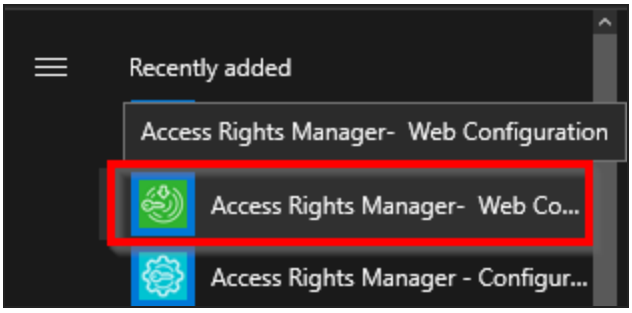


Example for an template based Open Order request.

Configure web components

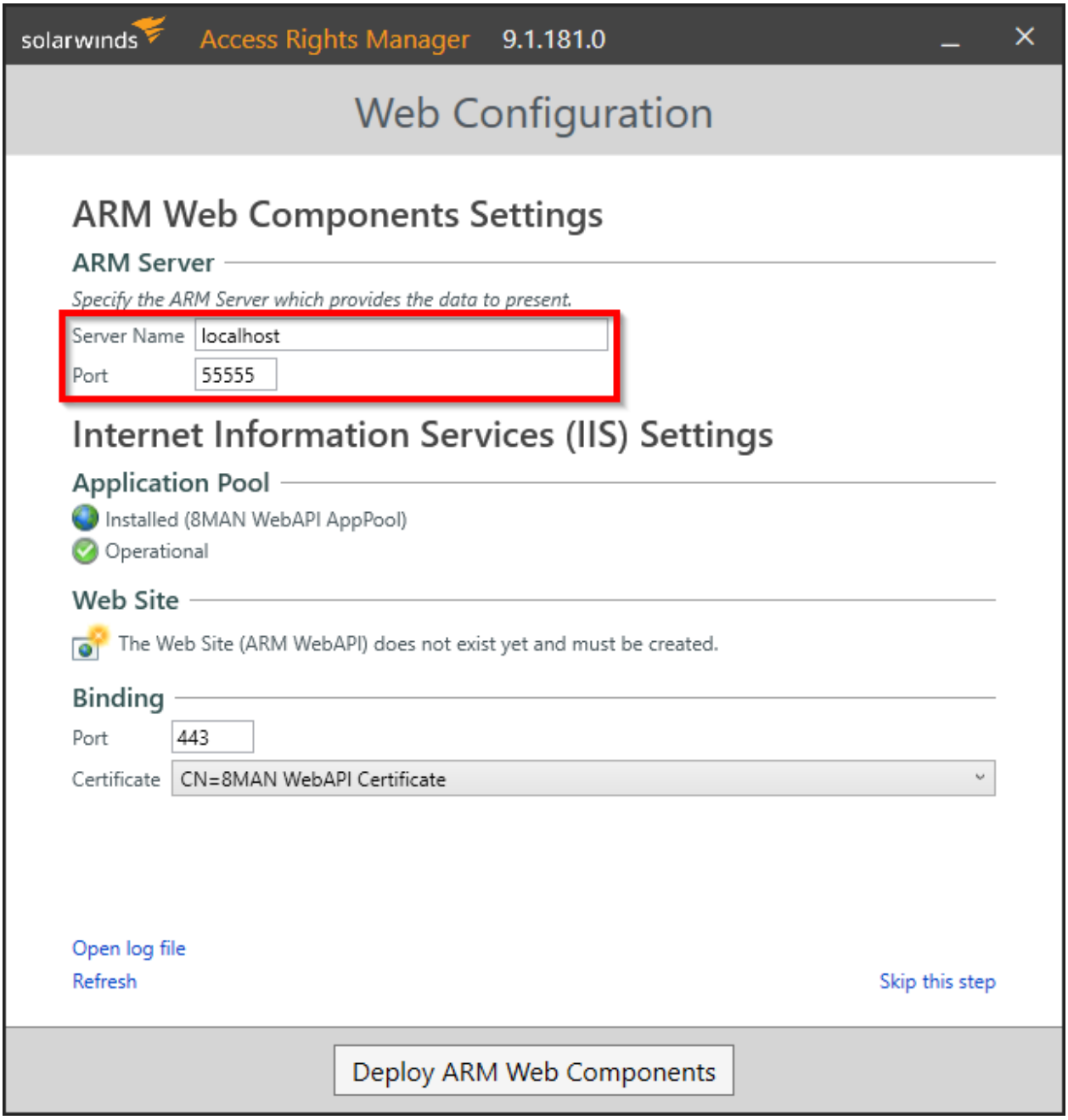
ARM web components are pre-configured during an evaluation installation with default values.

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.



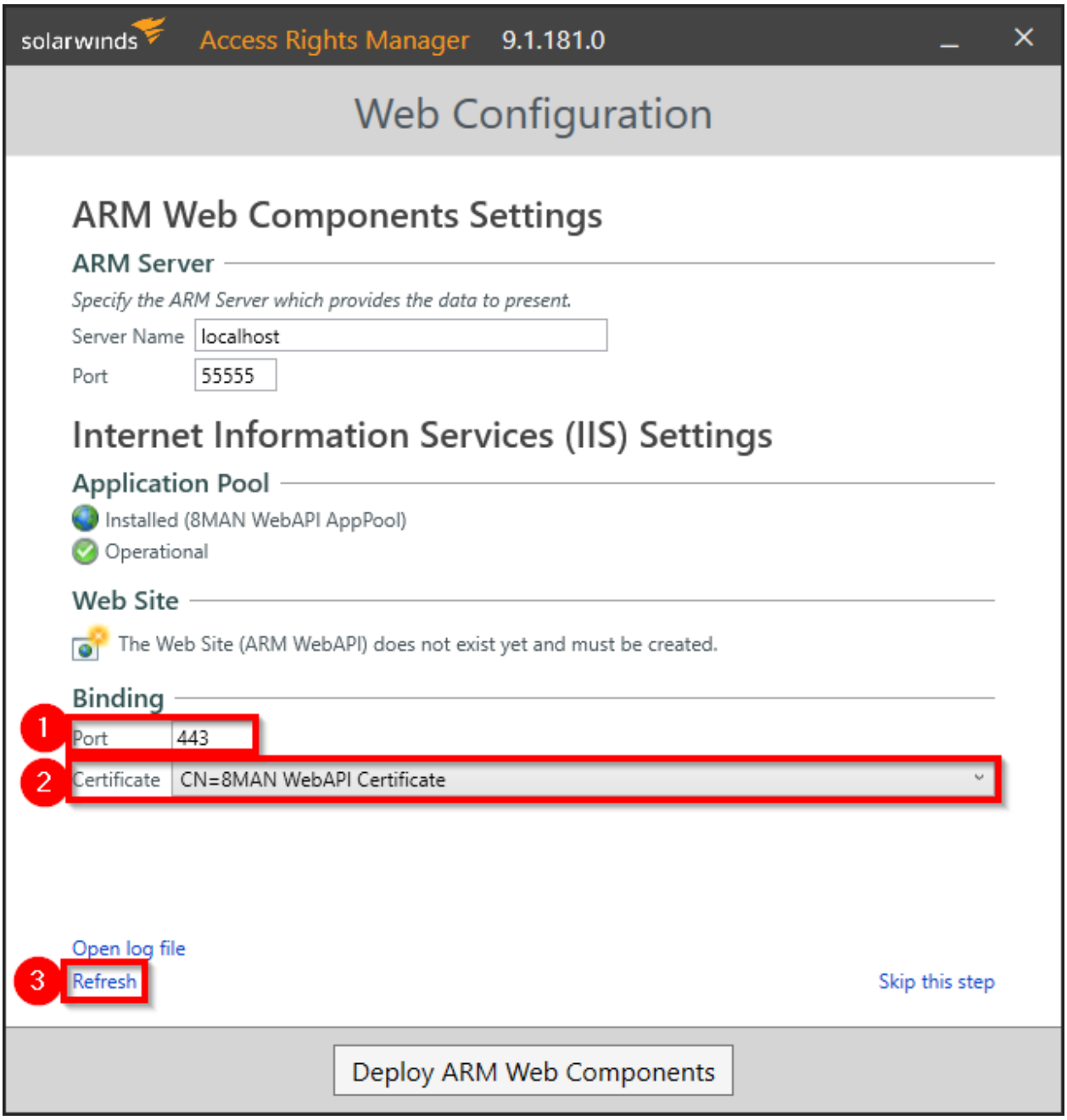
Open the ARM web configuration application.

After a Production Installation with enabled web components the web configuration application starts automatically.

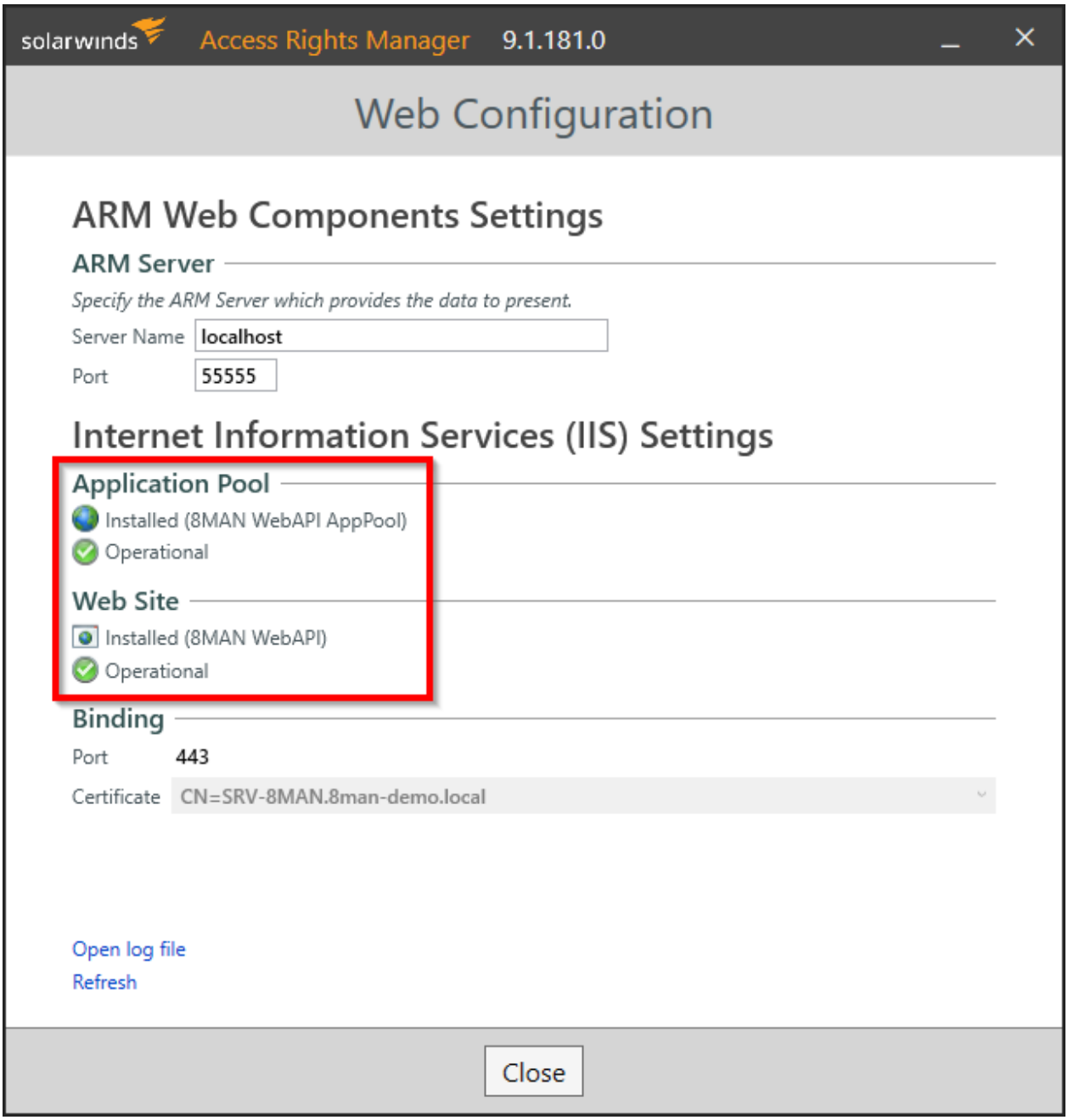


Enter the name of the ARM server. If you are running both Web Components and the ARM server on the same computer, you can use localhost.

Enter the port of the ARM server. By default the ARM server communicates through port "55555".



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".

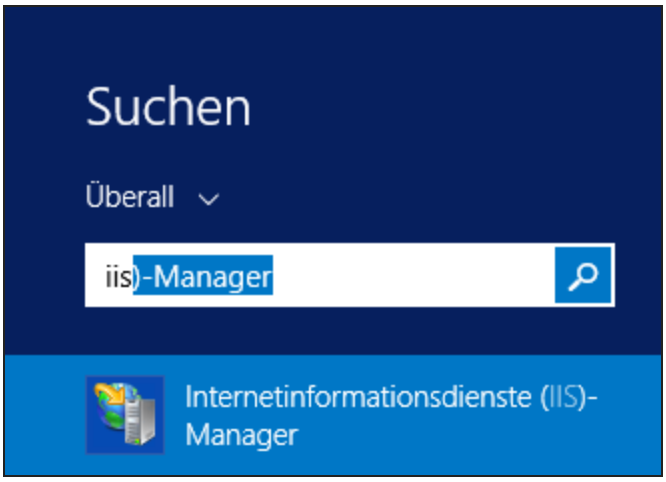


The web components will be available once all settings for "Application Pool" and "Web Site" are shown as operational.

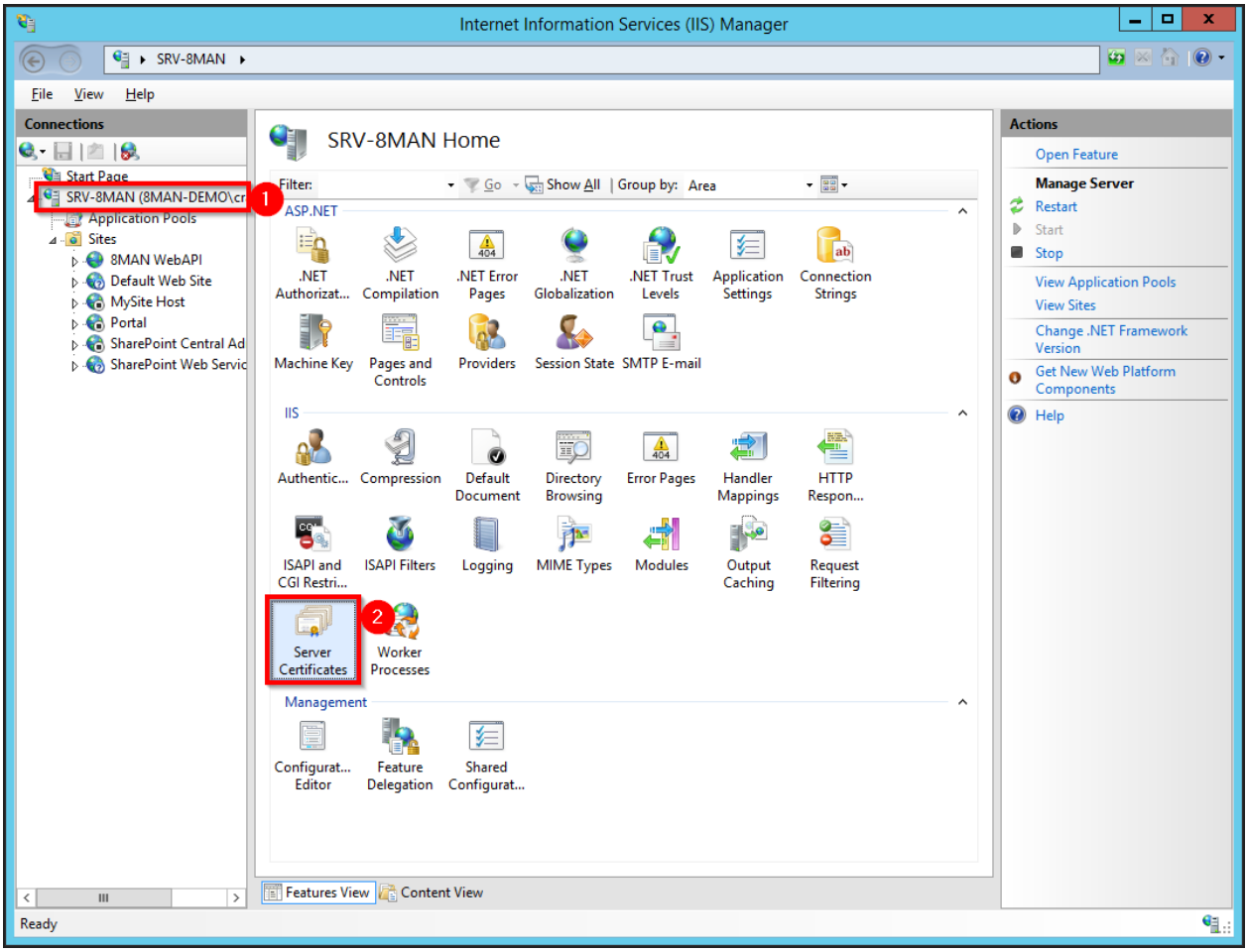
Generate a self-signed certificate

The following steps are optional.

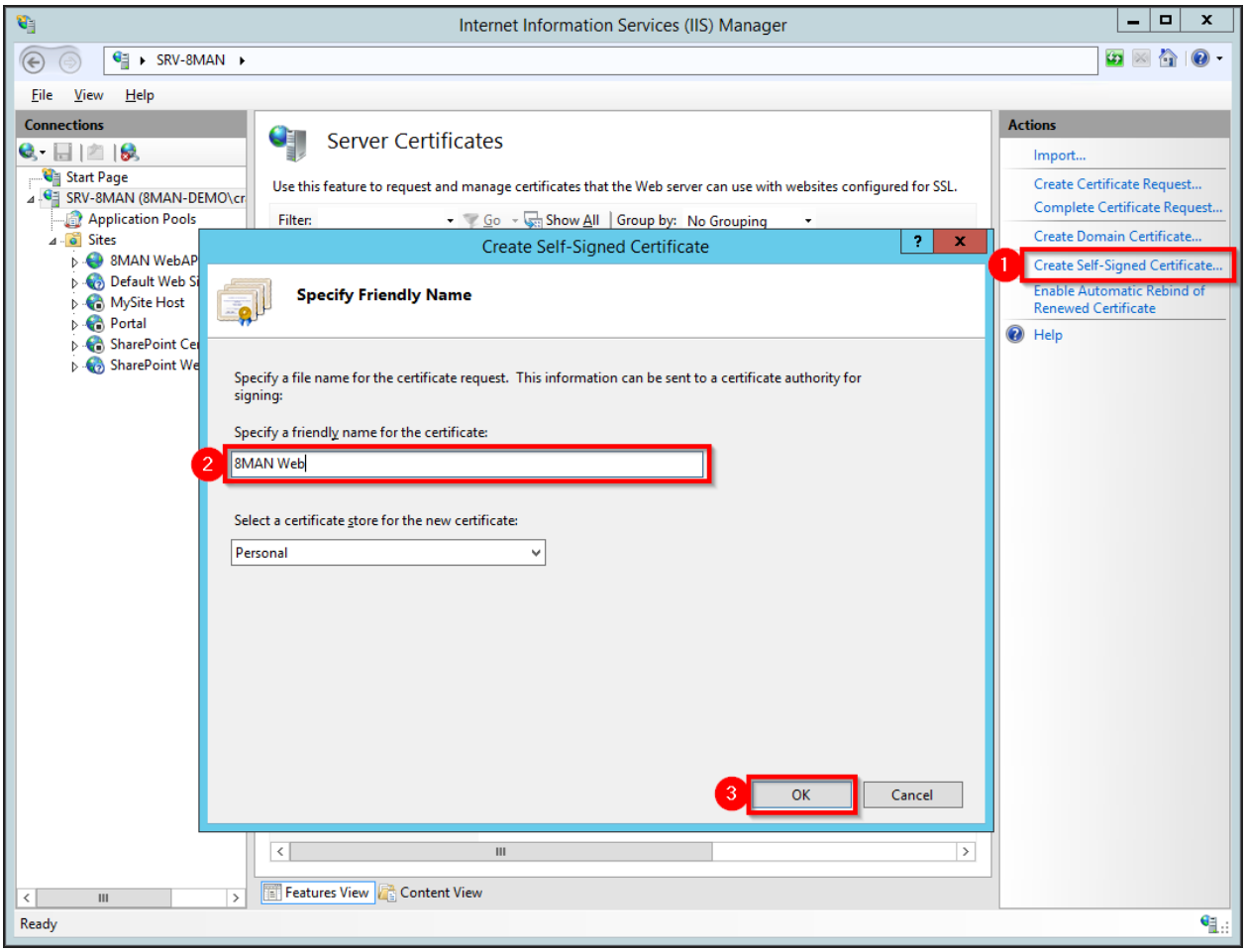
The self-signed certificates described in the following steps create security warnings in various browsers, as an out-of-date SHA-1 based encryption is used. Use certificates with SHA2 / 256 encryption for productive use.



Start the IIS-Manager.



1. Select the server.
2. Double-click "Server Certificates".

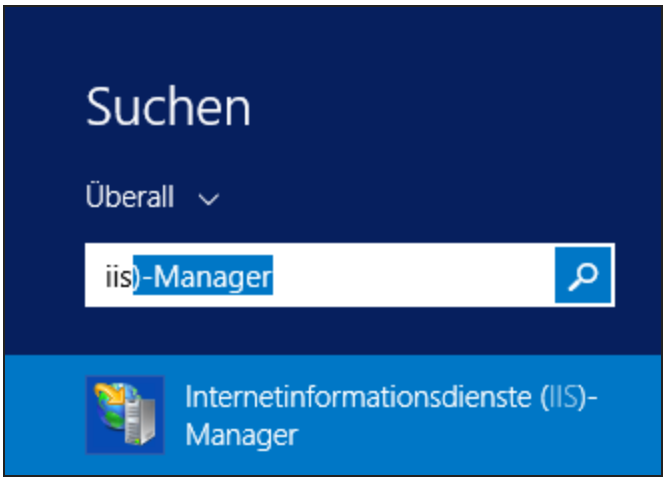


1. Click "Create Self-Signed Certificate".
2. Give the certificate a name.
3. Generate the certificate.

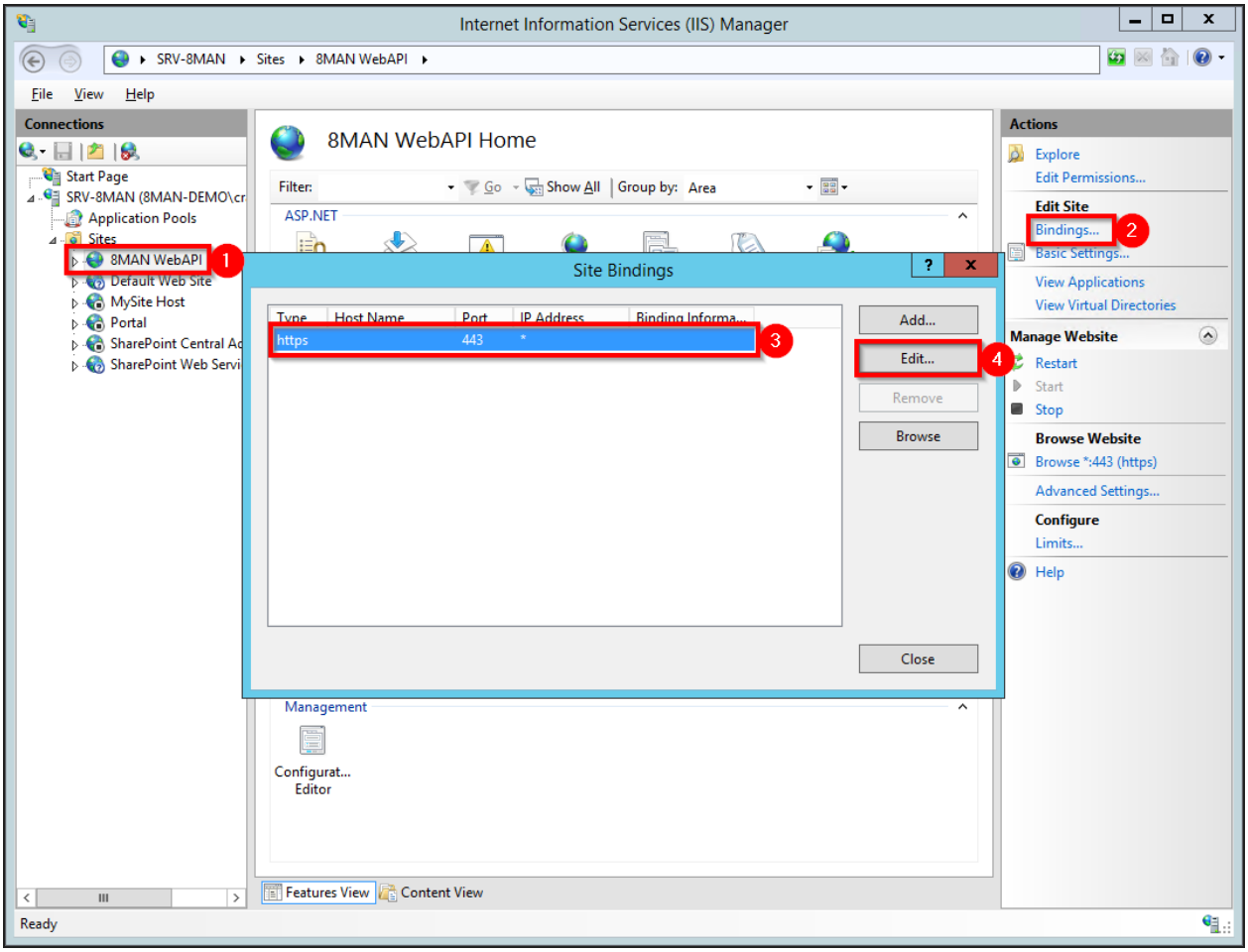
The next step is to bind the certificate to the website.

Bind a certificate to a site

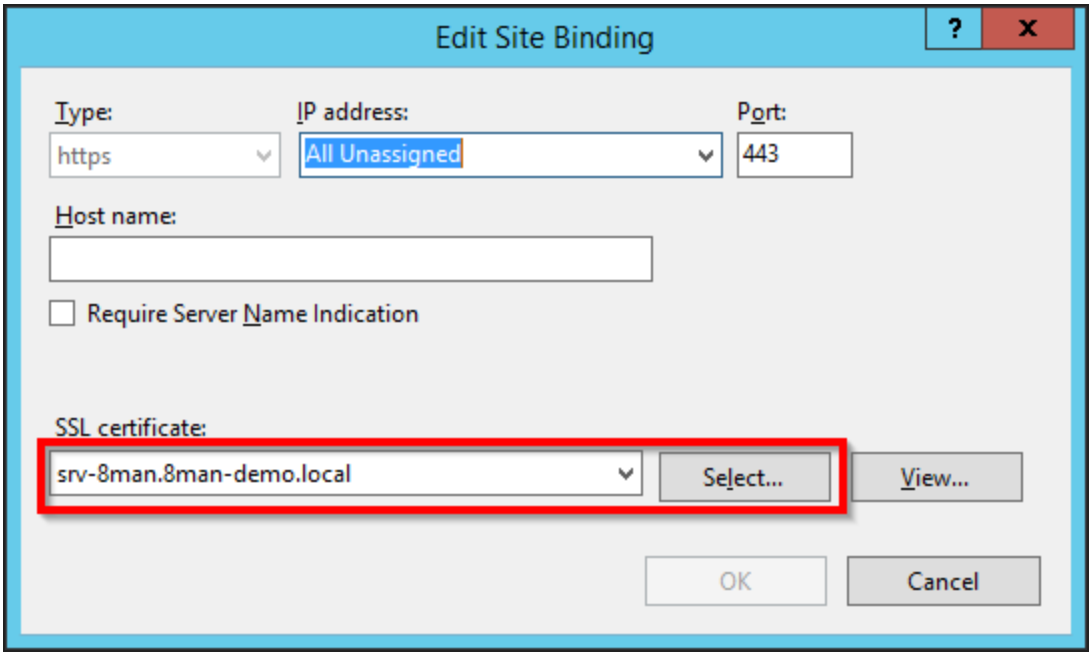
You can add a certificate to the site during the provisioning process. It may be necessary to add another certificate, for example when the old one has expired.



Start the IIS-Manager.



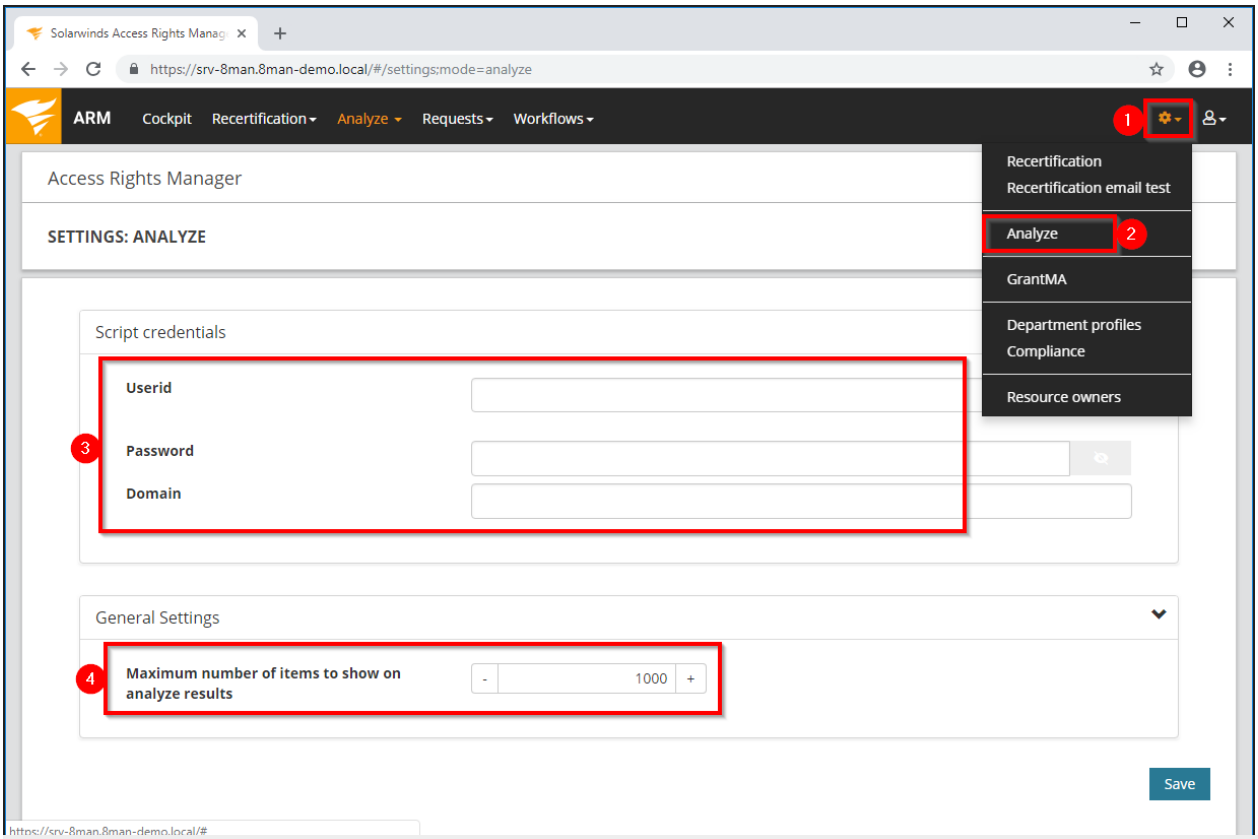
1. Navigate to the site "ARM WebAPI".
2. Click "Bindings...".
3. Select the certificate with type "https" and port "443" (standard settings).
4. Click "Edit...".



Select a certificate. Click "OK" to bind the certificate to the site.

Configuration in the web client

Set analyze options

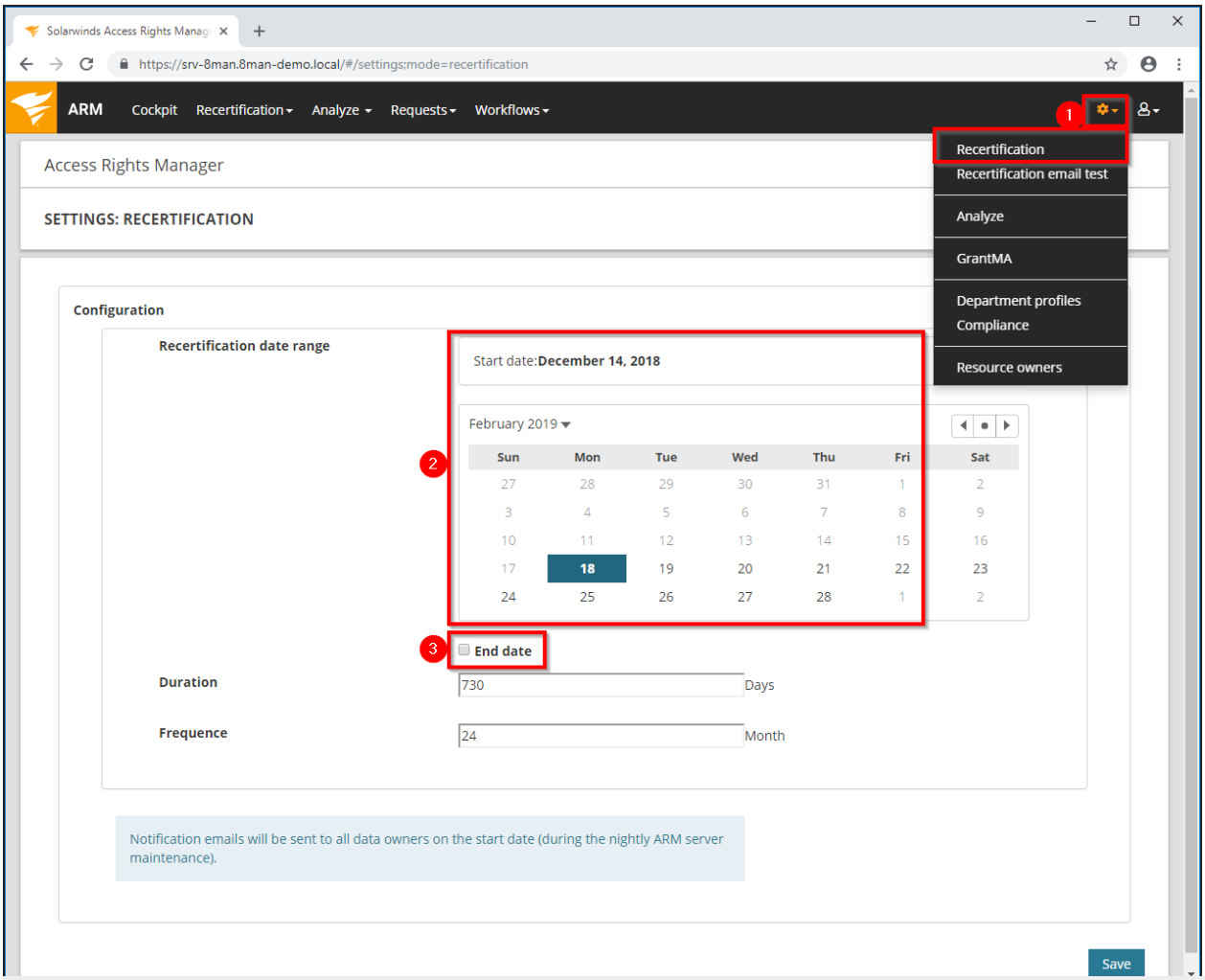


Log into the WebClient as ARM administrator.

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



1. Login with ARM administrator credentials and select "Recertification".
2. Select a start date. Recertification is active from this date on.

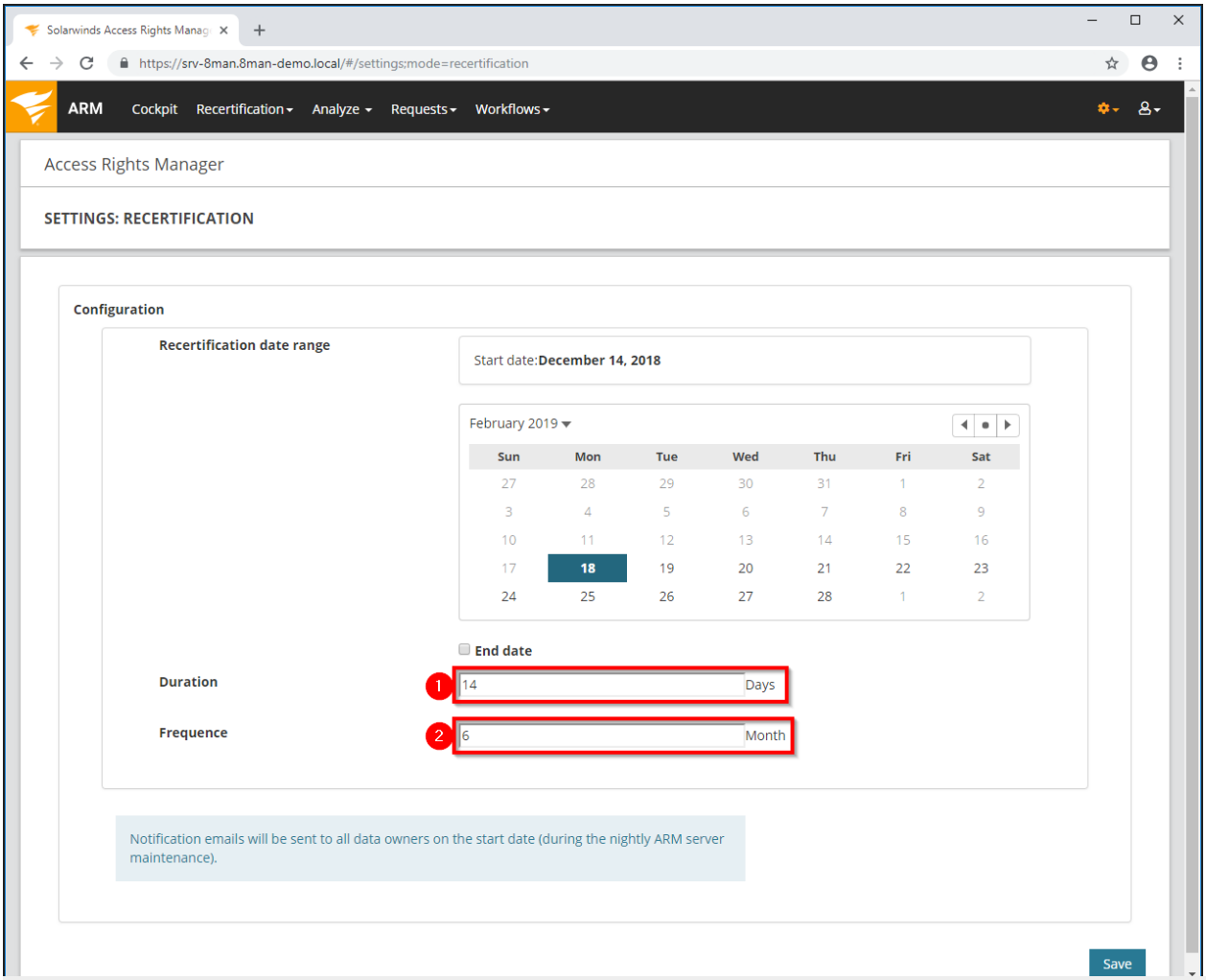
> The recertification is based on scan data of this date. Permission changes that occur after this date will not be considered by an active recertification.

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.

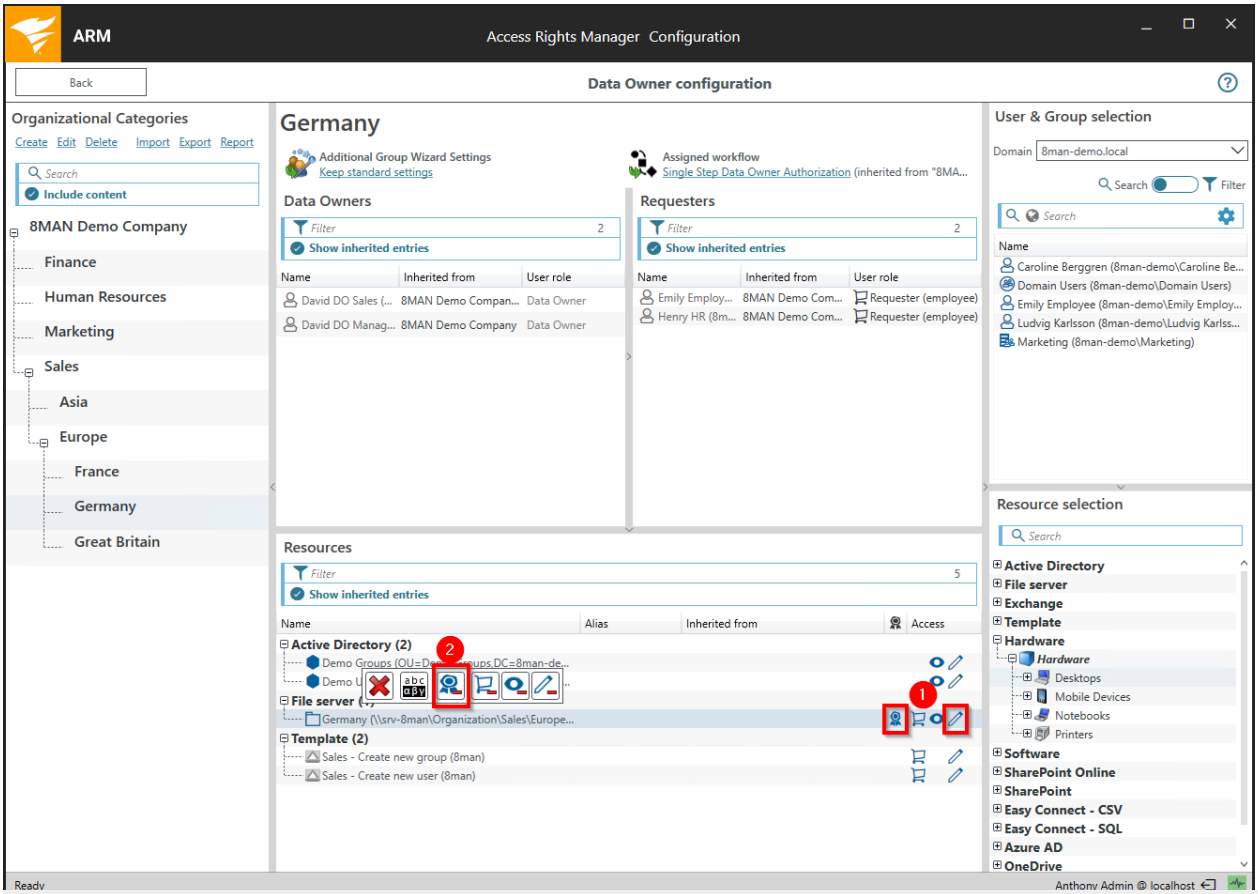
Deadlines and intervals



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.

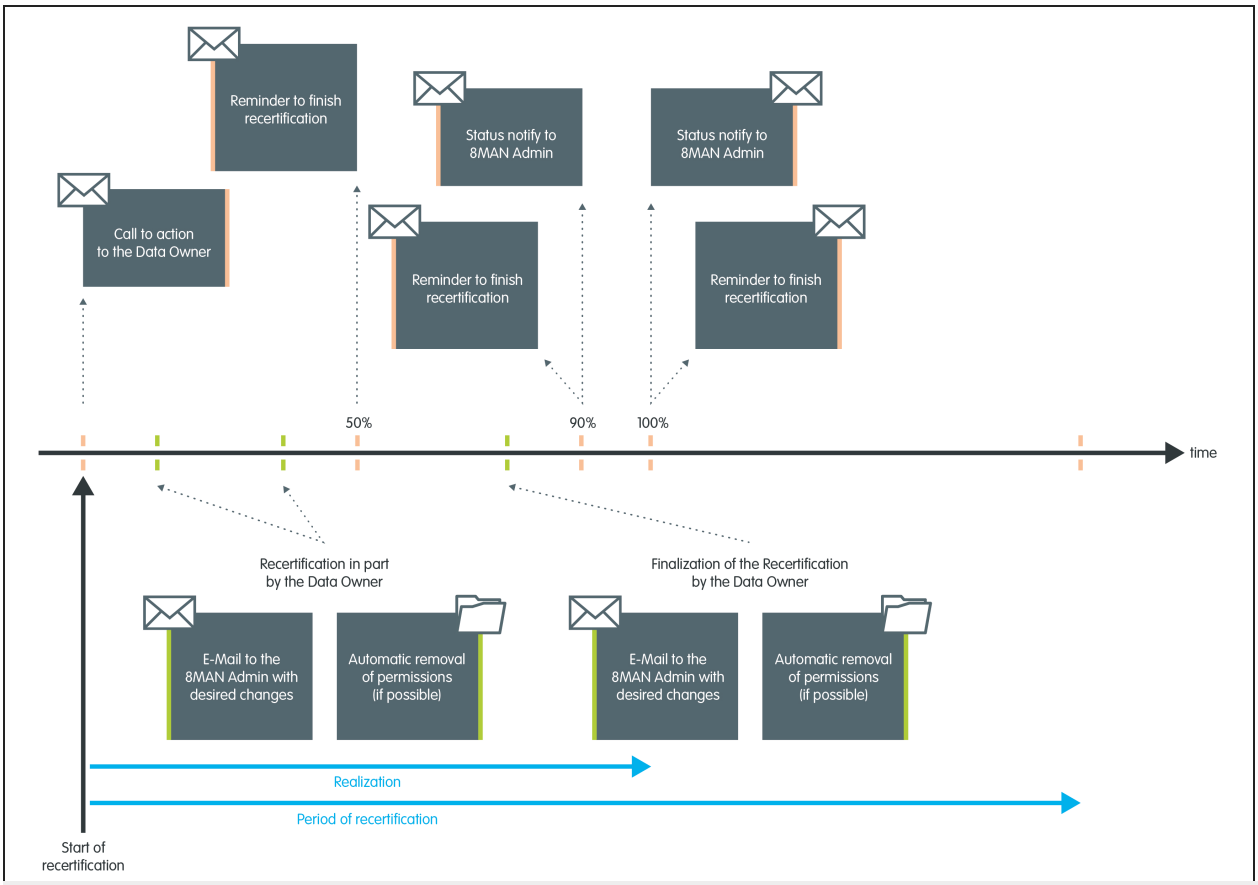
Activate recertifications in the Data Owner configuration



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

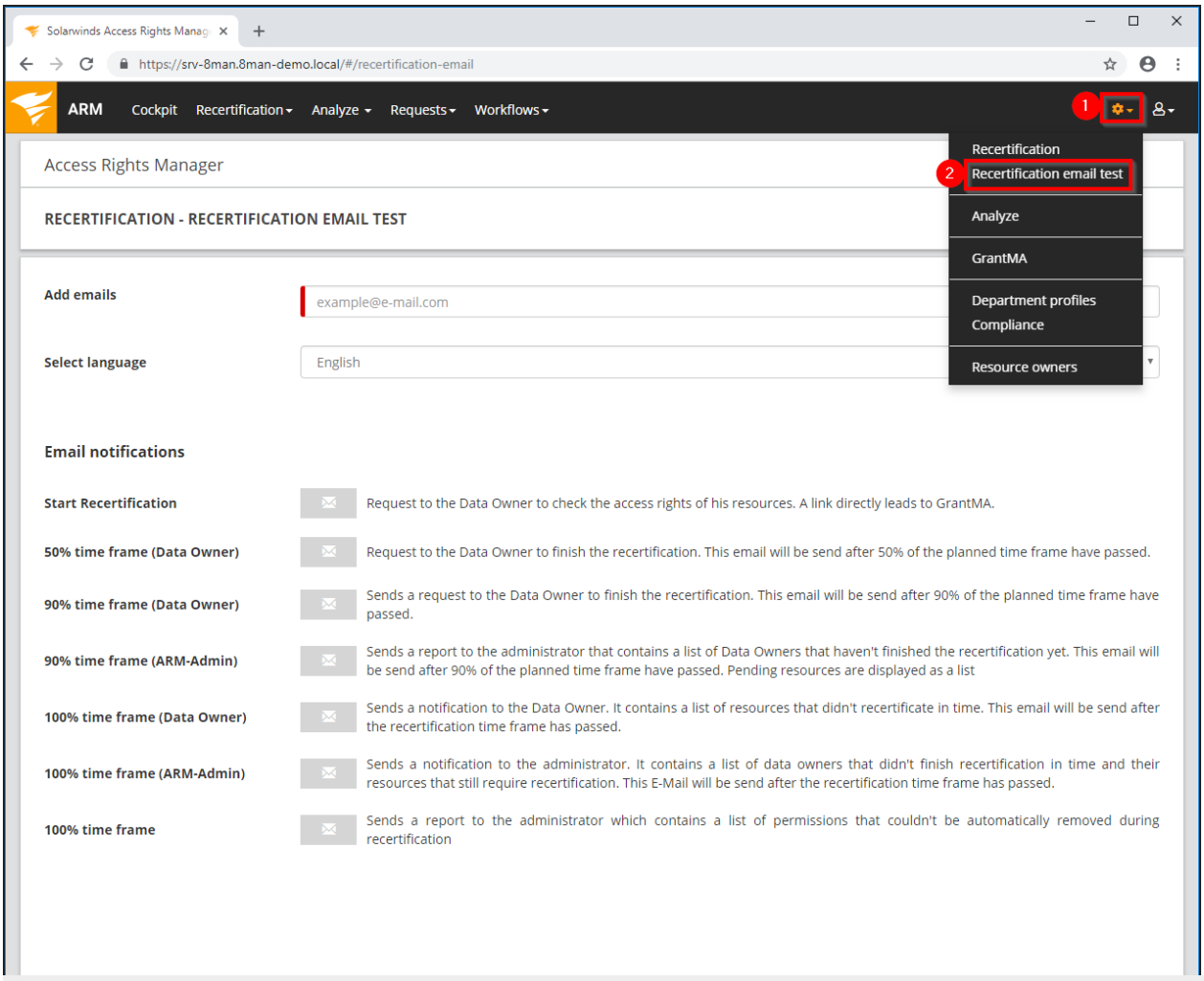
Background / Value

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

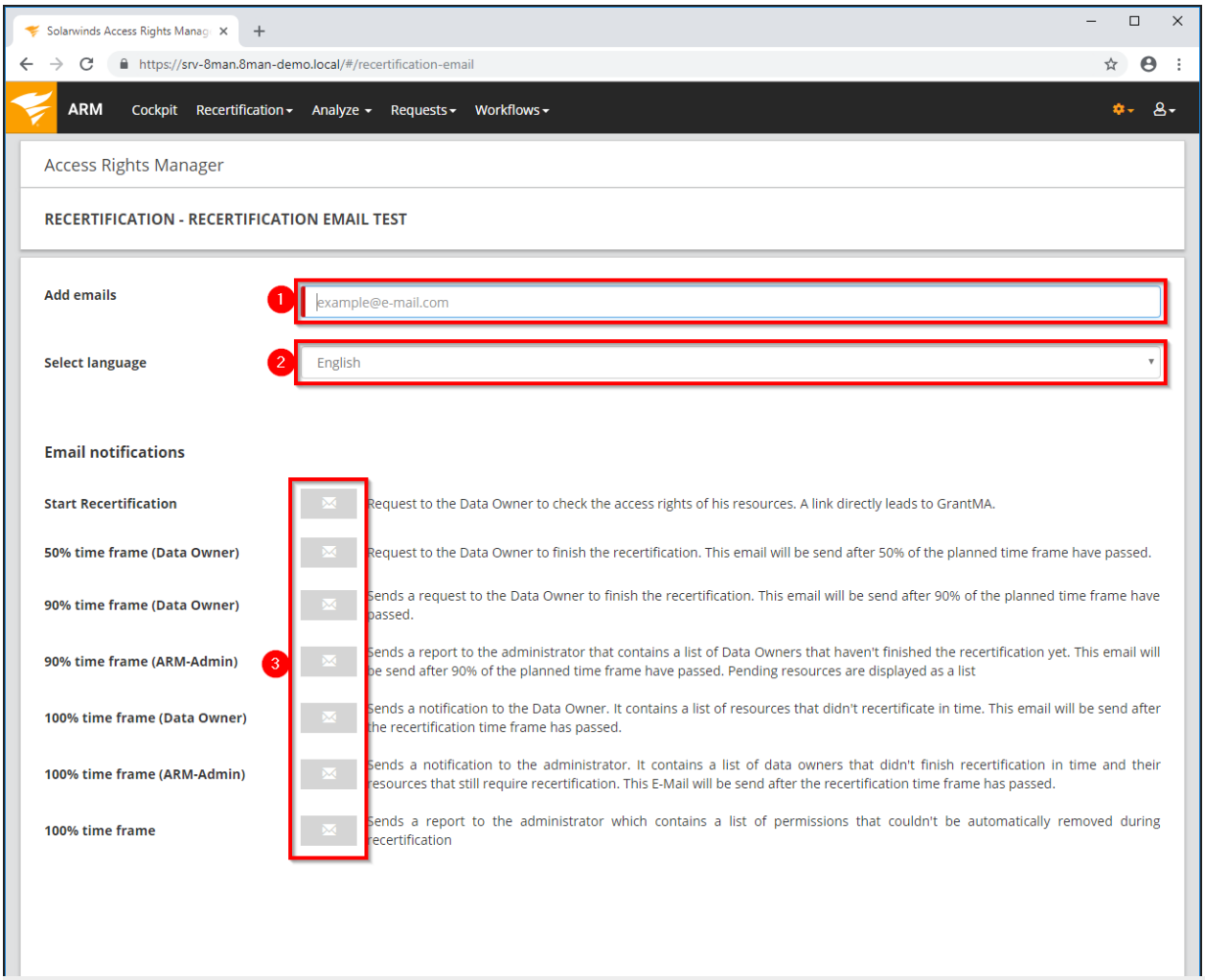
Customize notification emails for recertification (Administrator)

Step-by-step process

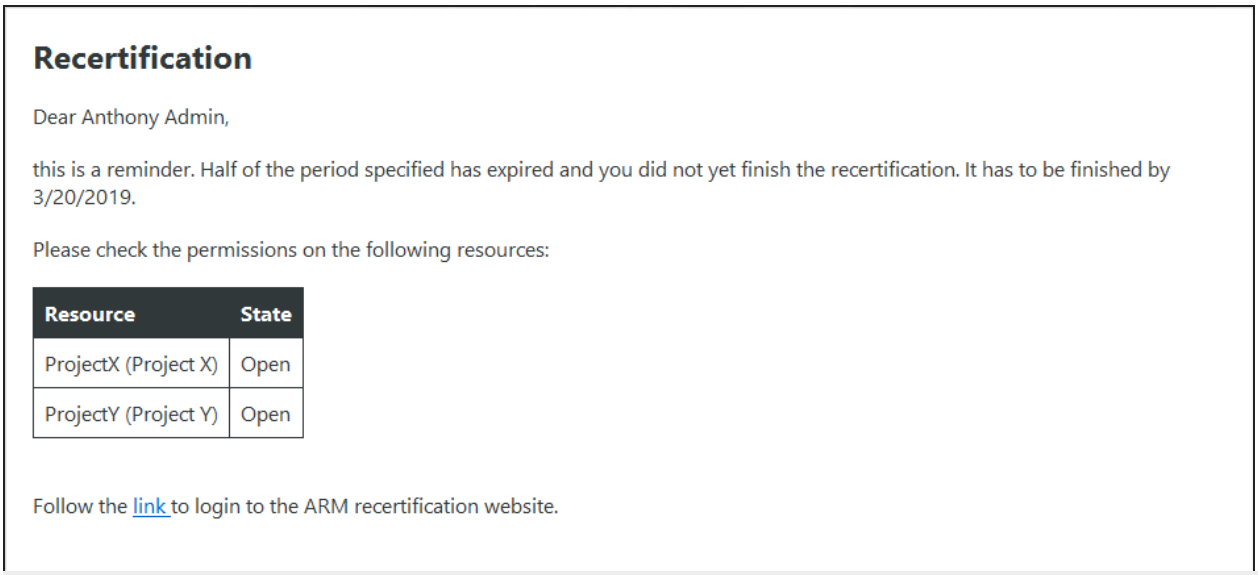


Log into the web client as an administrator.

1. Click on the gear.
2. Select "Recertification email test".



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

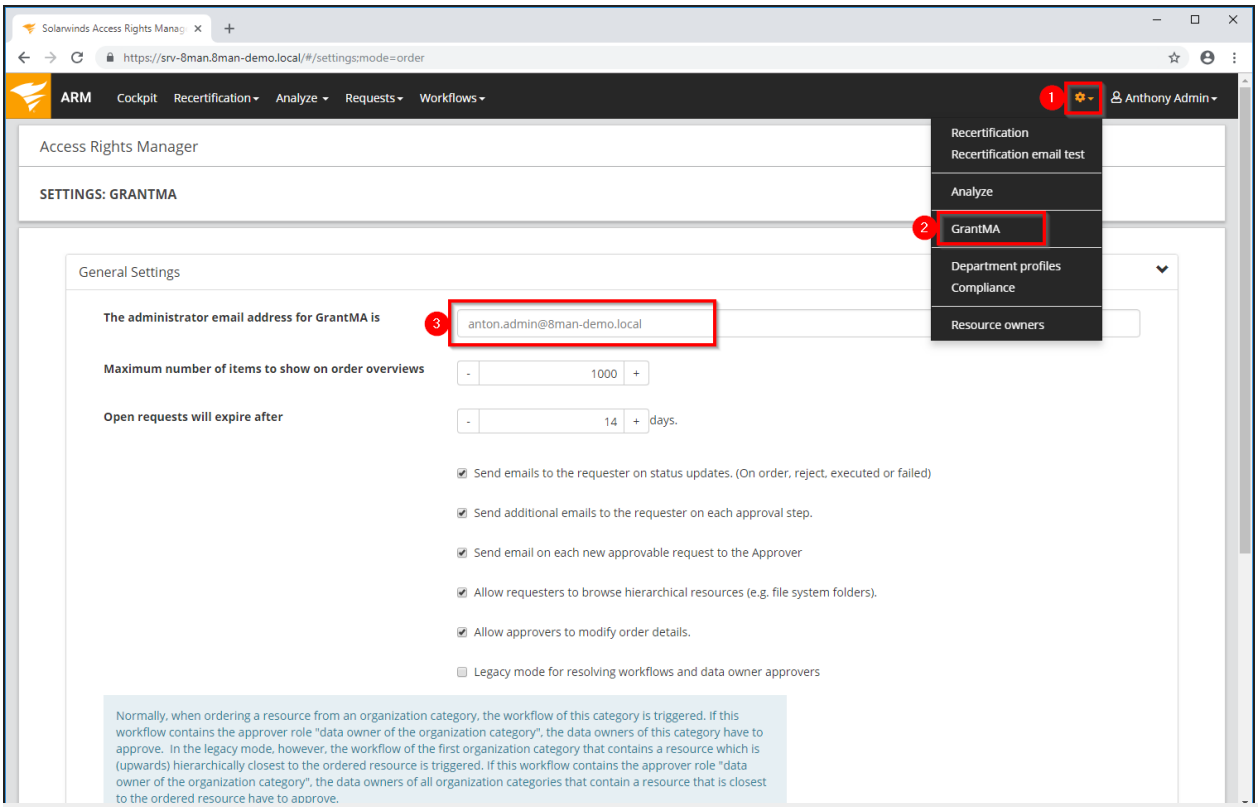
The recertification process has been designed to check the permissions of real users. Technical accounts (see the following list) are not displayed:

- 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

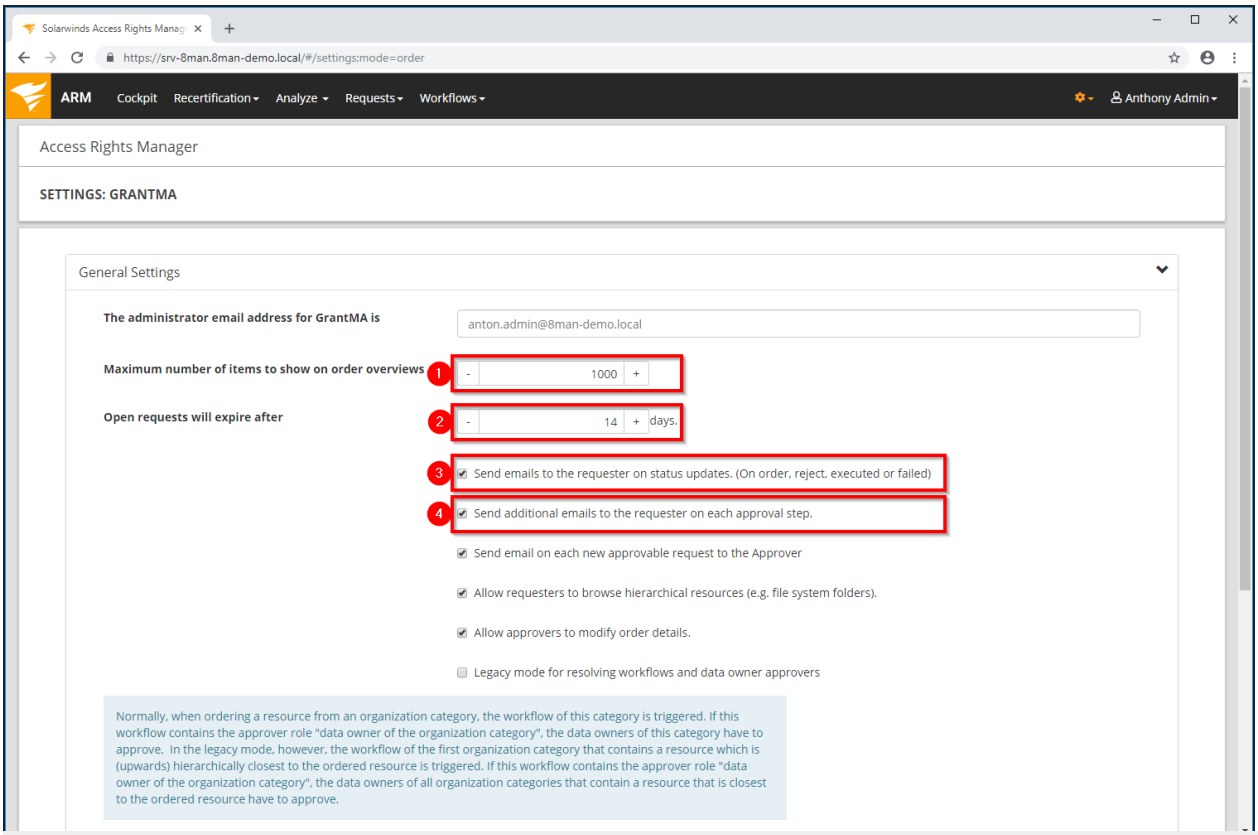
Recertifications adopt the settings of the blacklist for views and reports. Please see the section "Configure the blacklist for views & reports".

GrantMA settings

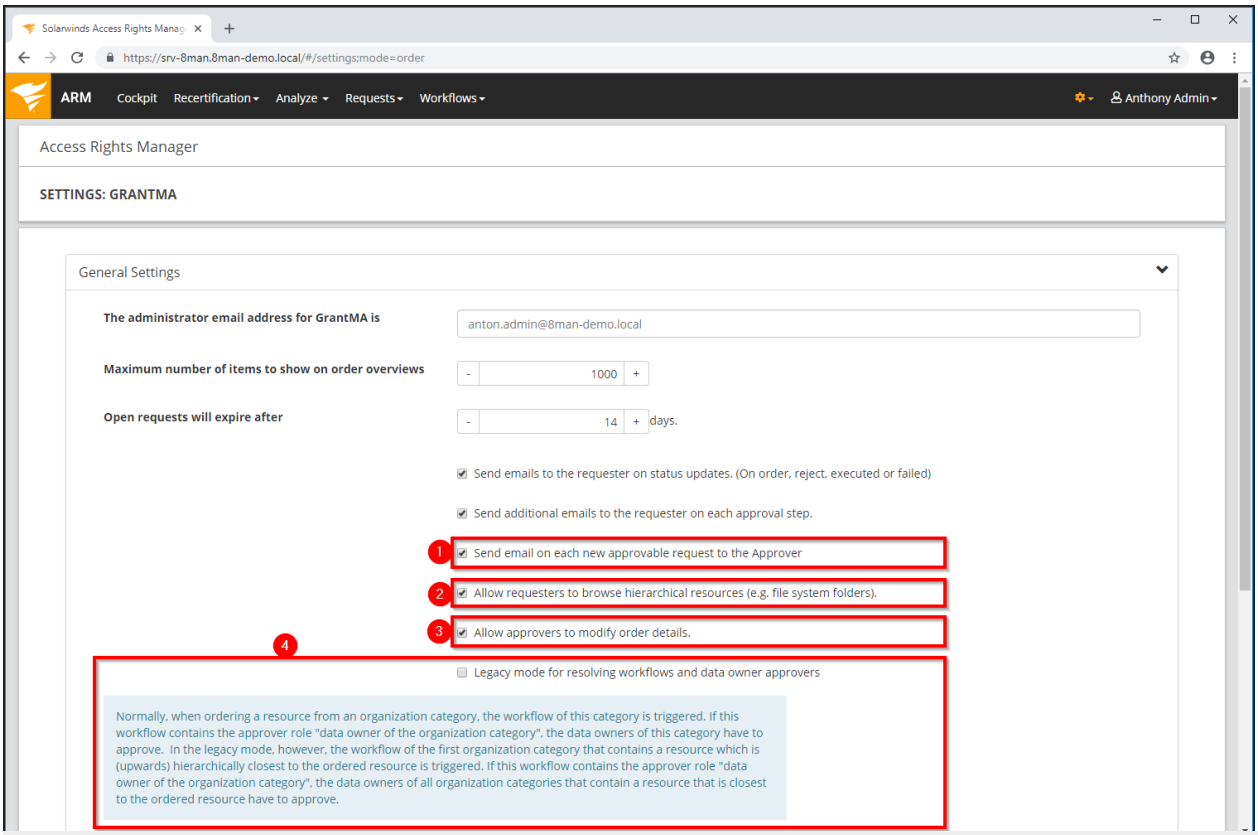


Log into the web client as an ARM administrator.

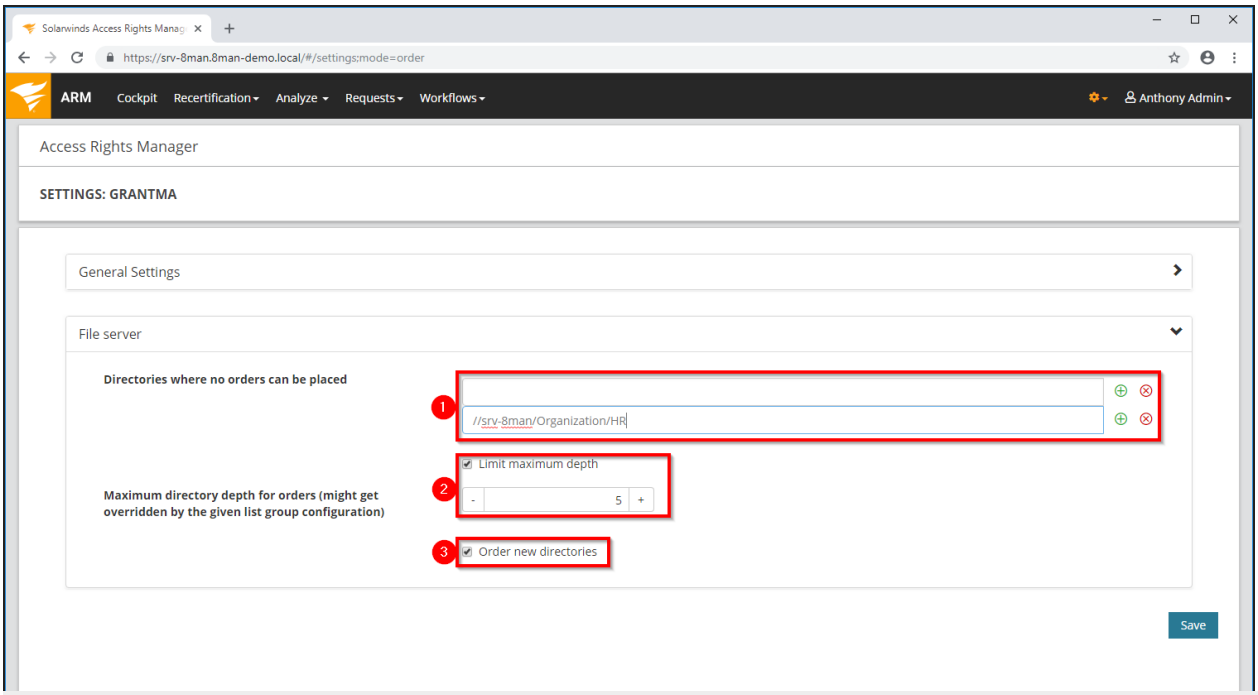
1. Click the gear.
2. Select GrantMA.
3. Specify the administrator's email address for GrantMA. ARM sends emails if errors occur in the order process (not for Recertification and Analyze & Act).



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.



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 pnserver.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

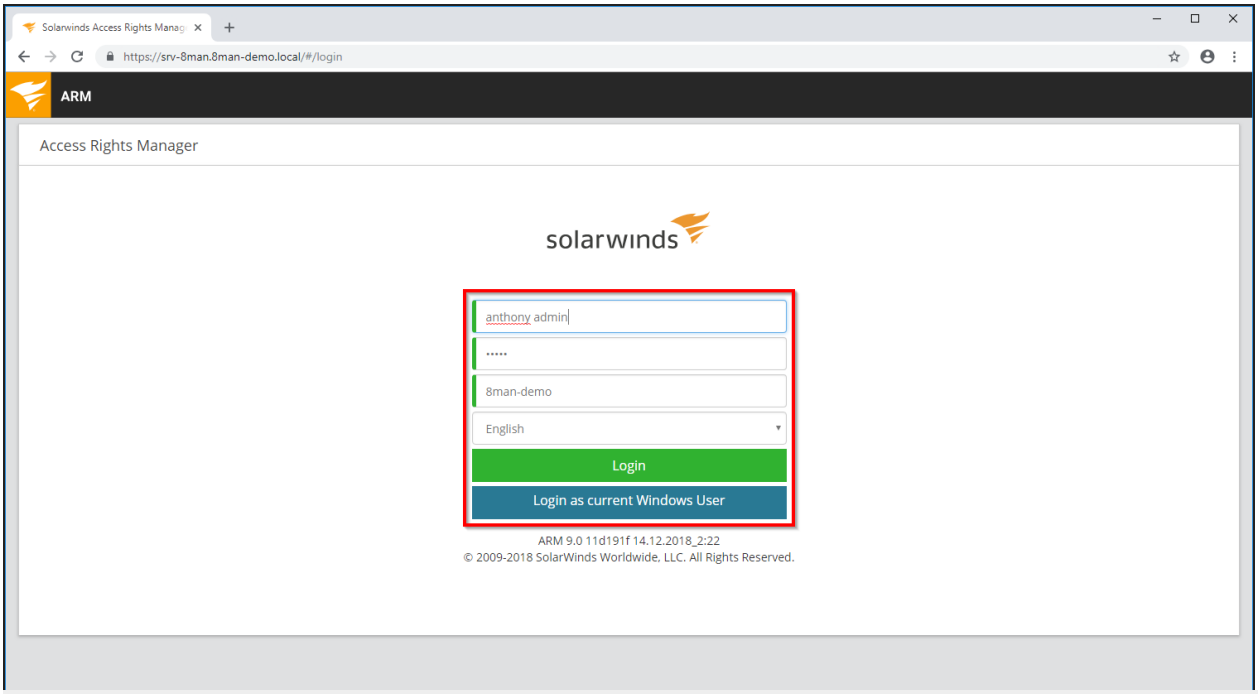
With version 8.0 ARM releases new features to move the GrantMA configuration into the web client. We inserted the new role "Resource Owner". Assign this role completely using the web client. Due to the requirements of our customers we designed a direct assignment between the Resource Owner and the resource - 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.

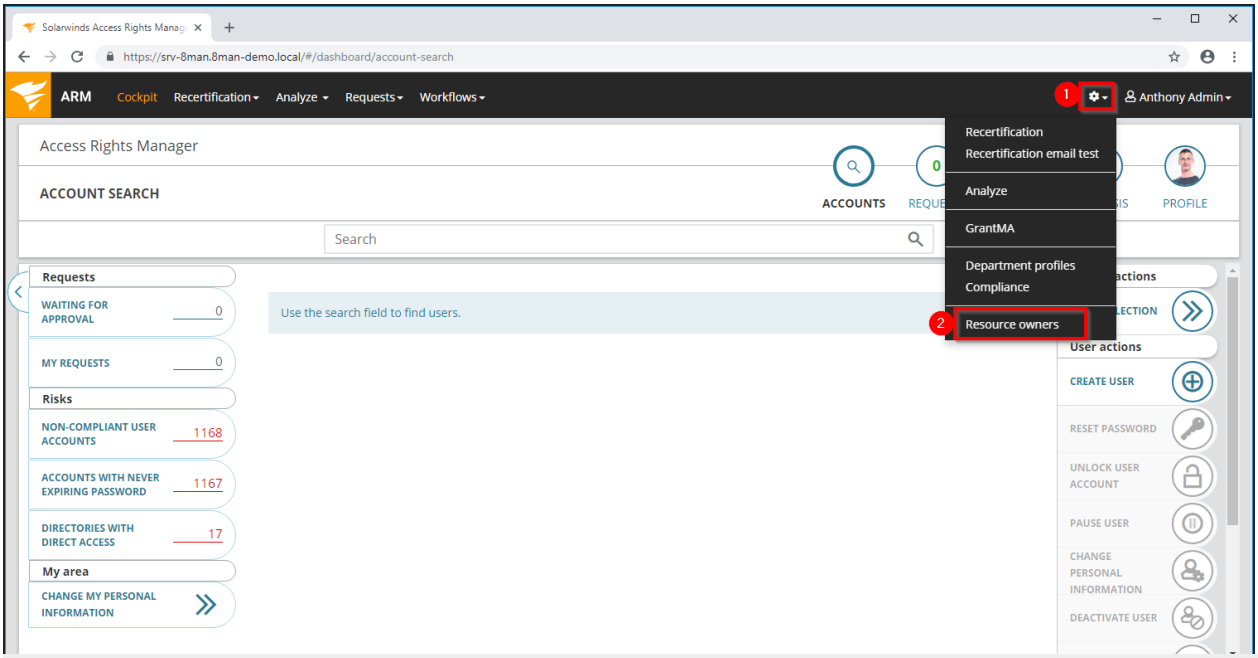
Related features

GrantMA: Design approval processes (administrator)

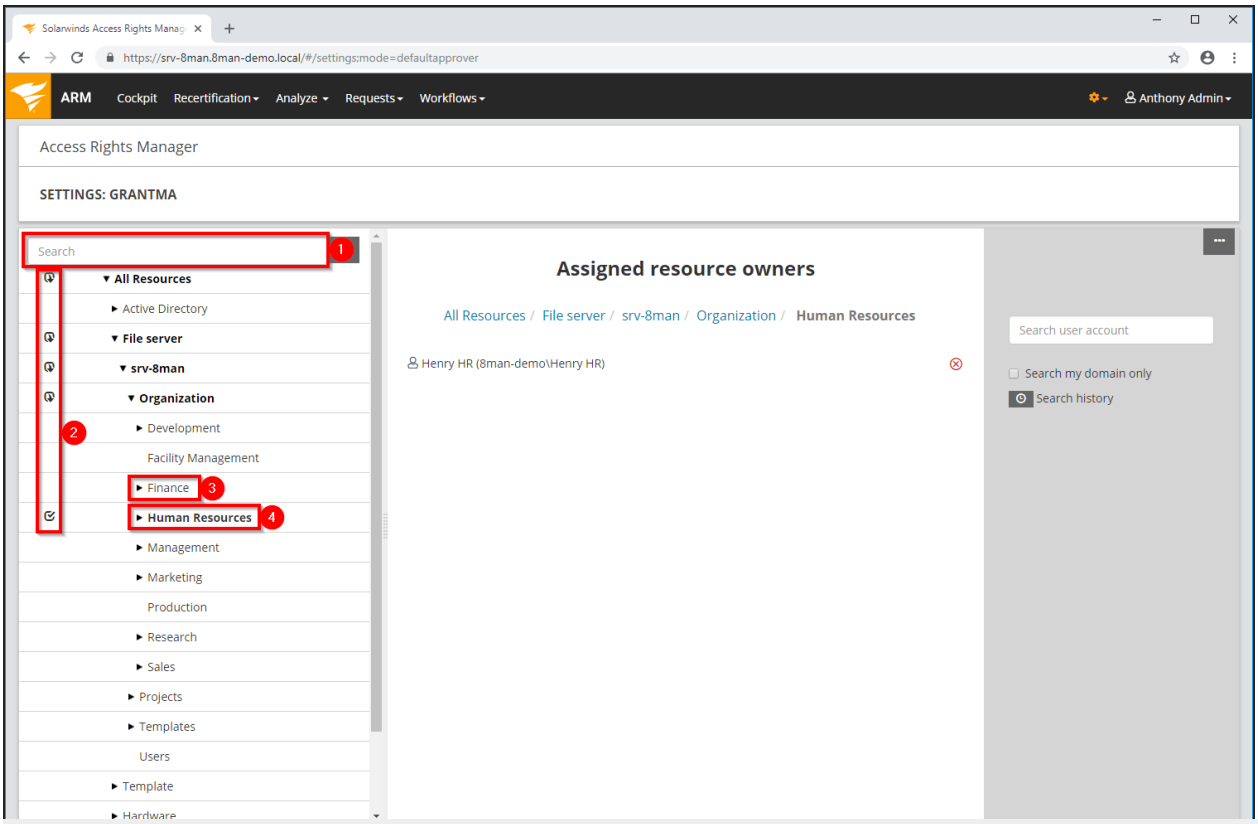
Step-by-step process



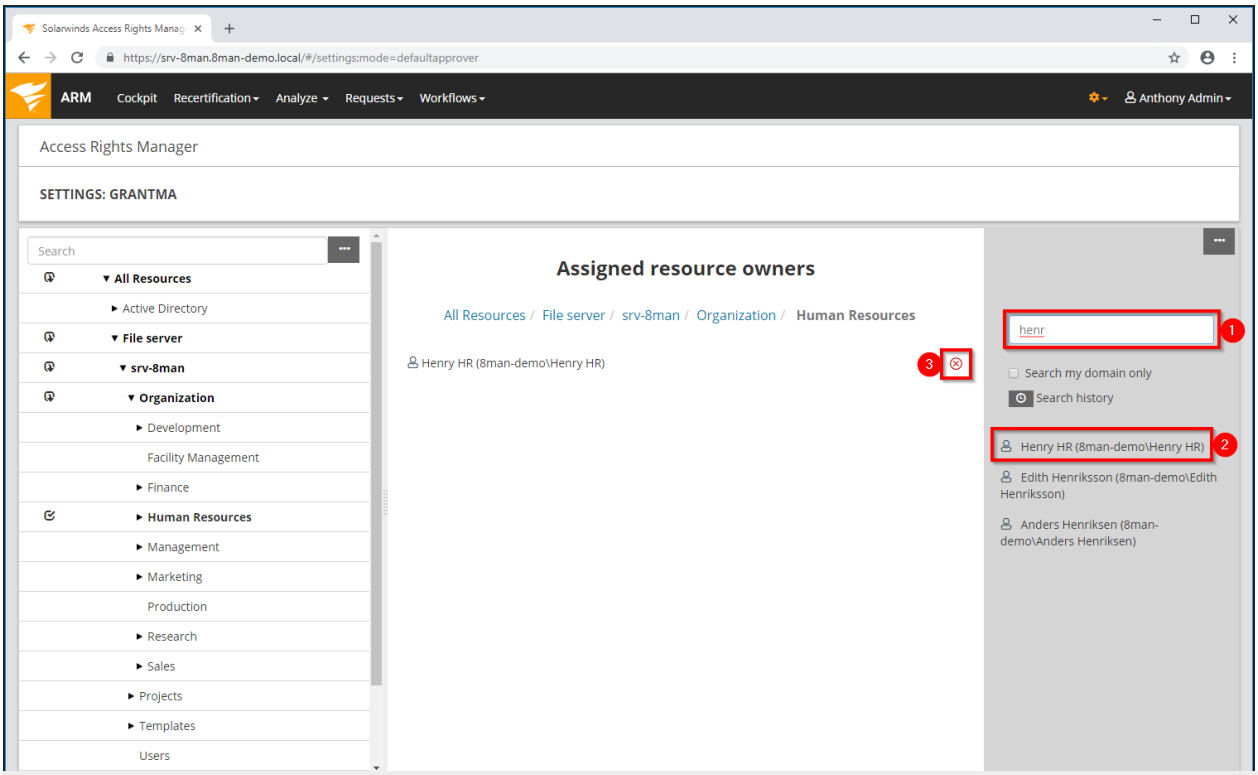
Login to the web interface with admin credentials.



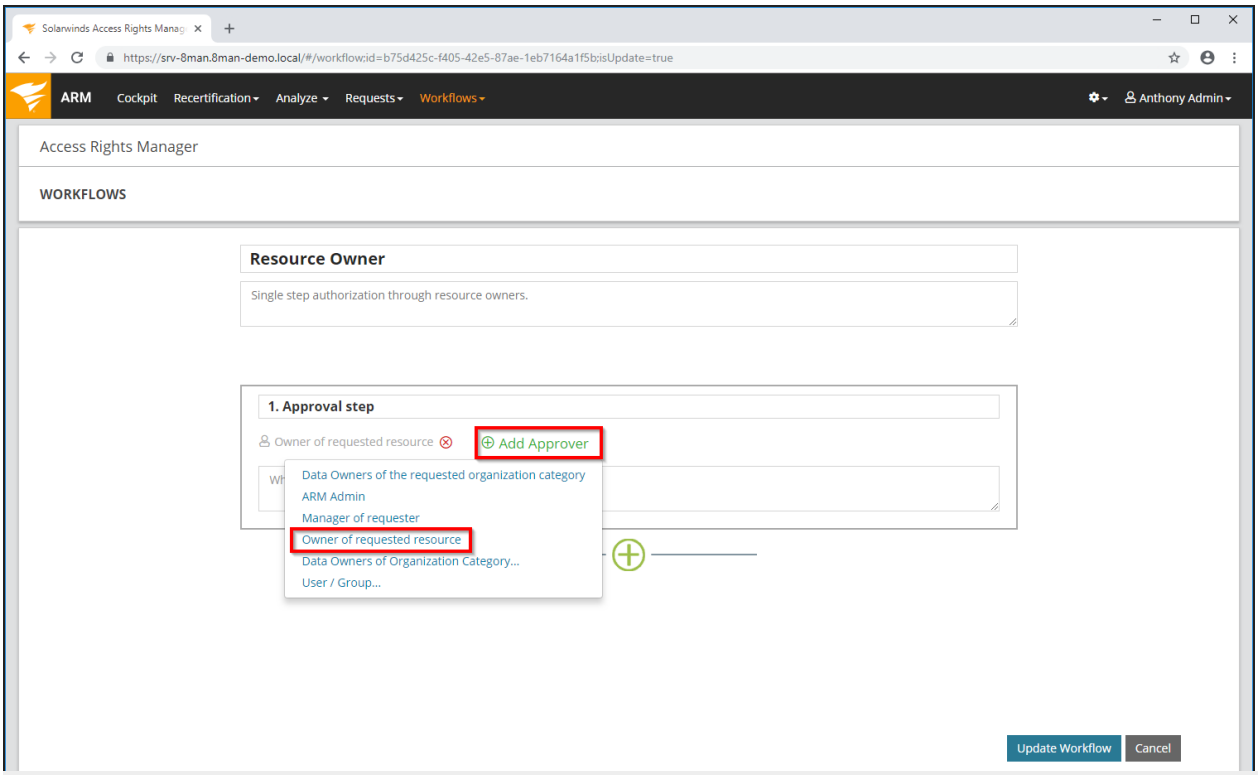
1. Click the gear-wheel.
2. Select "Resource owners".



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.



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

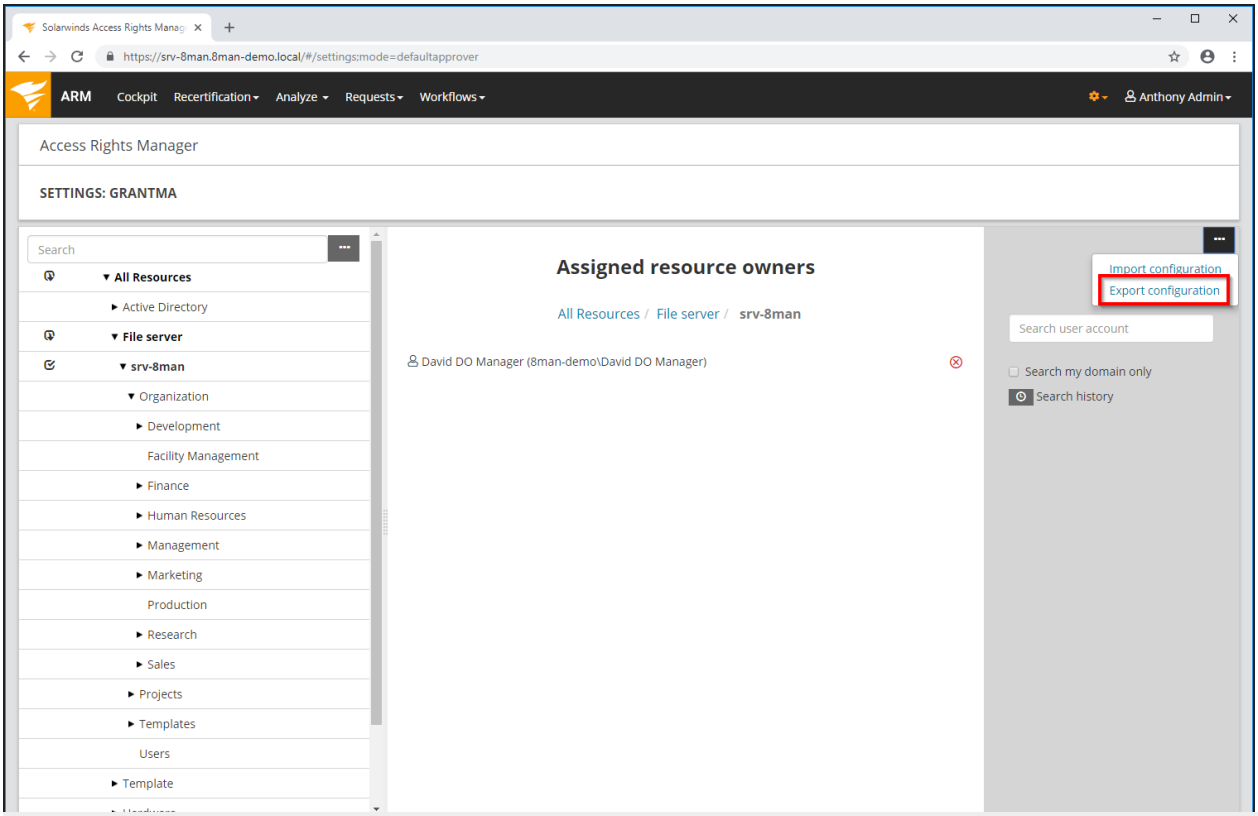
Background / Value

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.

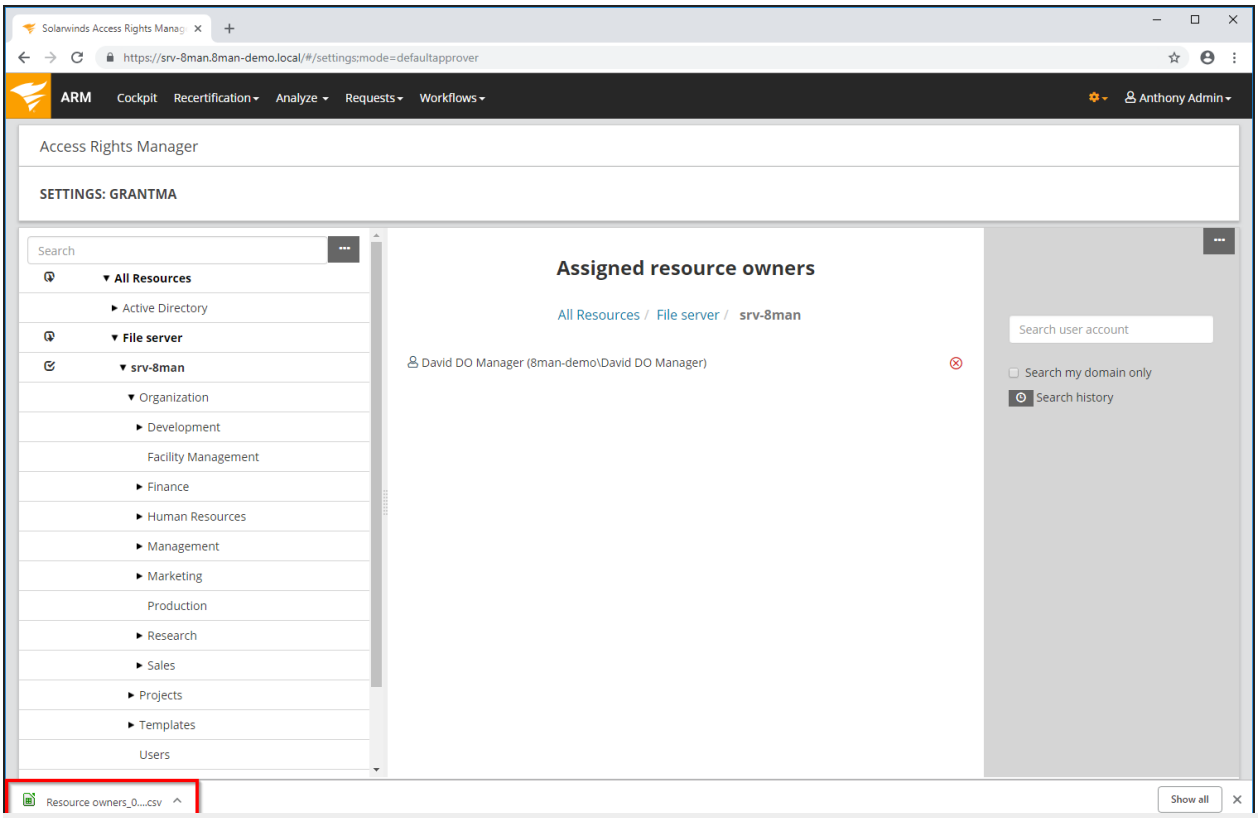
Related features

GrantMA: Design approval processes (administrator)

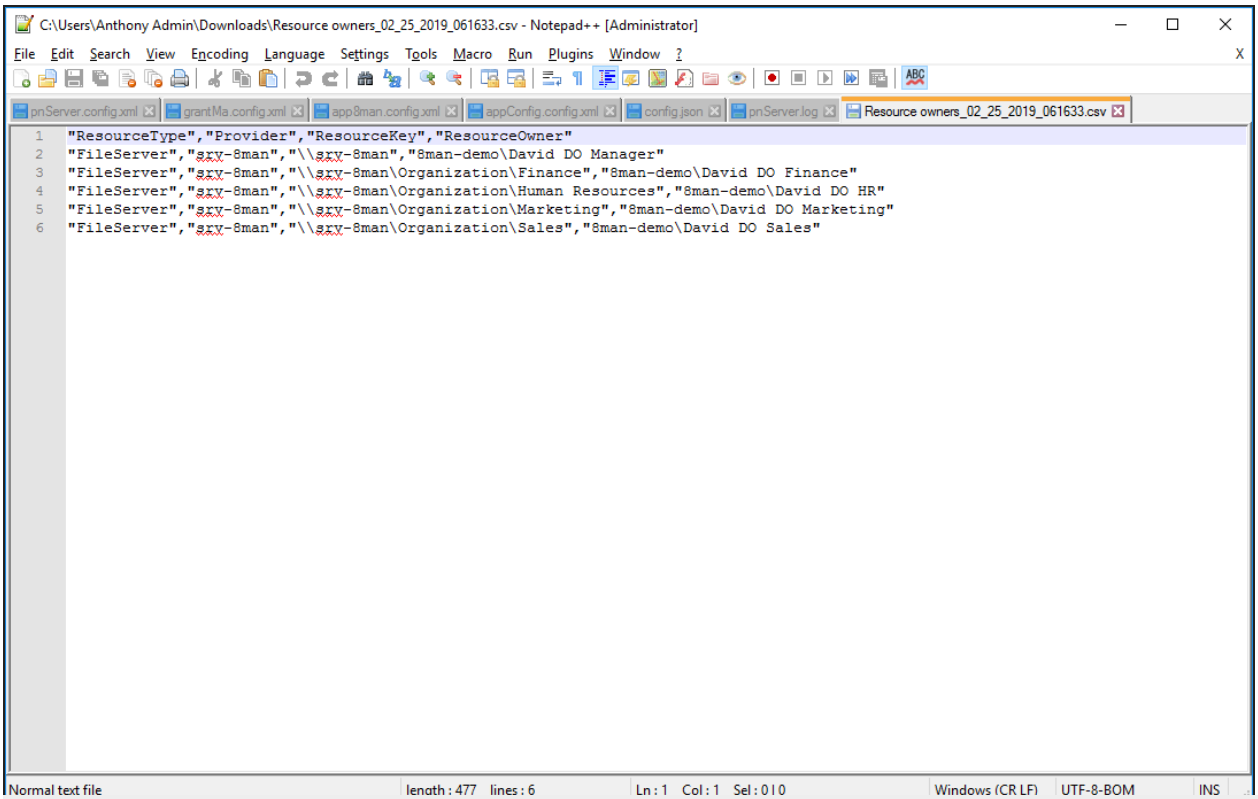
Step-by-step process



Export the configuration to a CSV-file after assigning resource owners. Click "Export configuration".

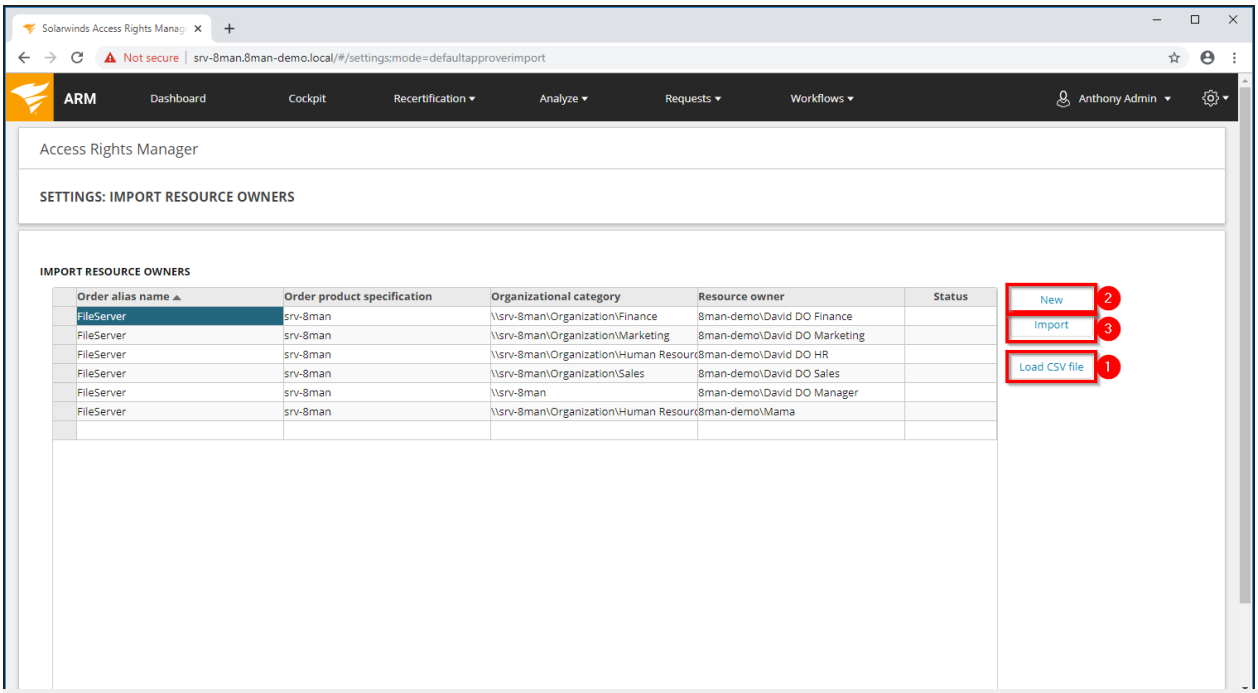


The export file is handled as a download. Displaying and saving of the file depends on the browser.

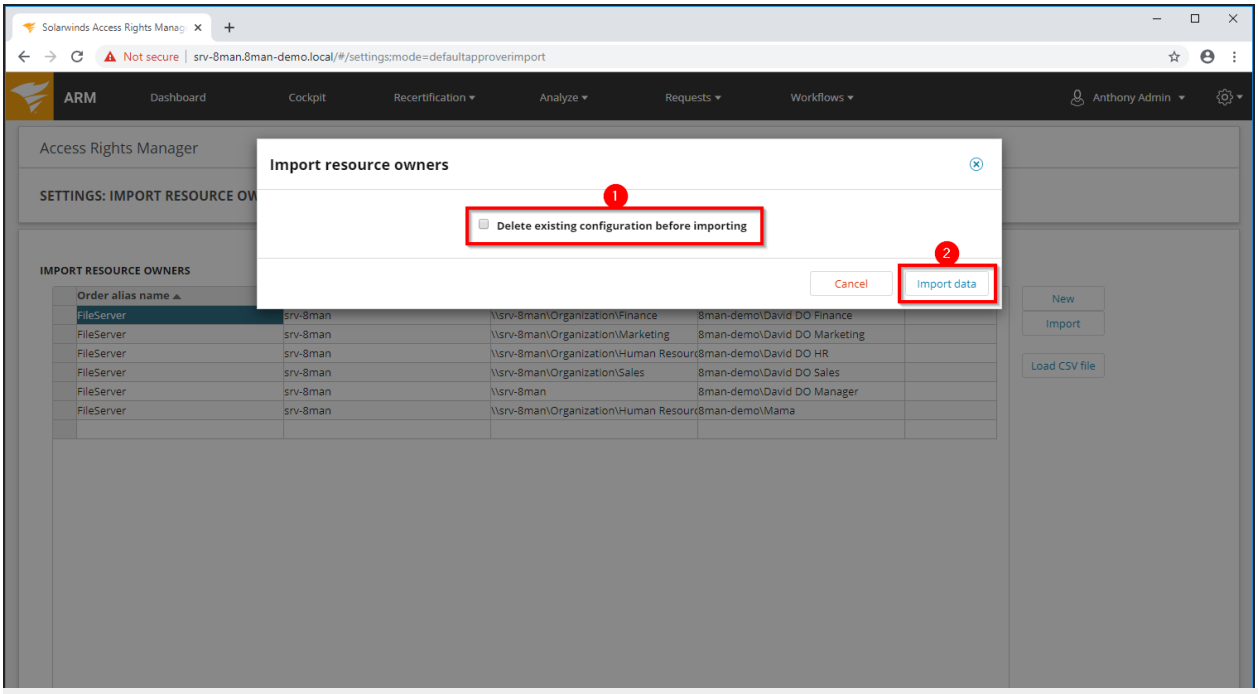


You can edit the CSV-file.

Please note that the assignment must always be one-to-one.



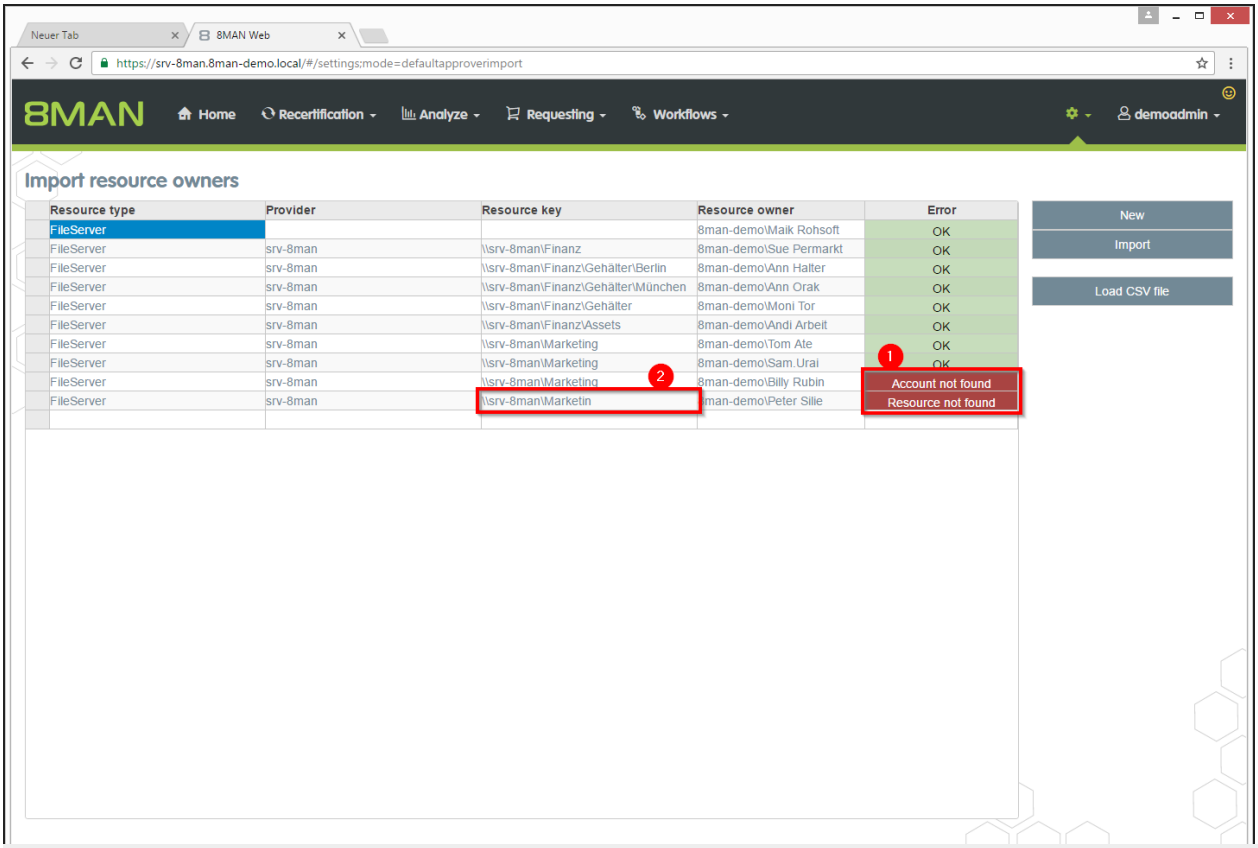
1. Load a CSV-file.
2. Clear the loaded list.
3. Click "Import".



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.



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

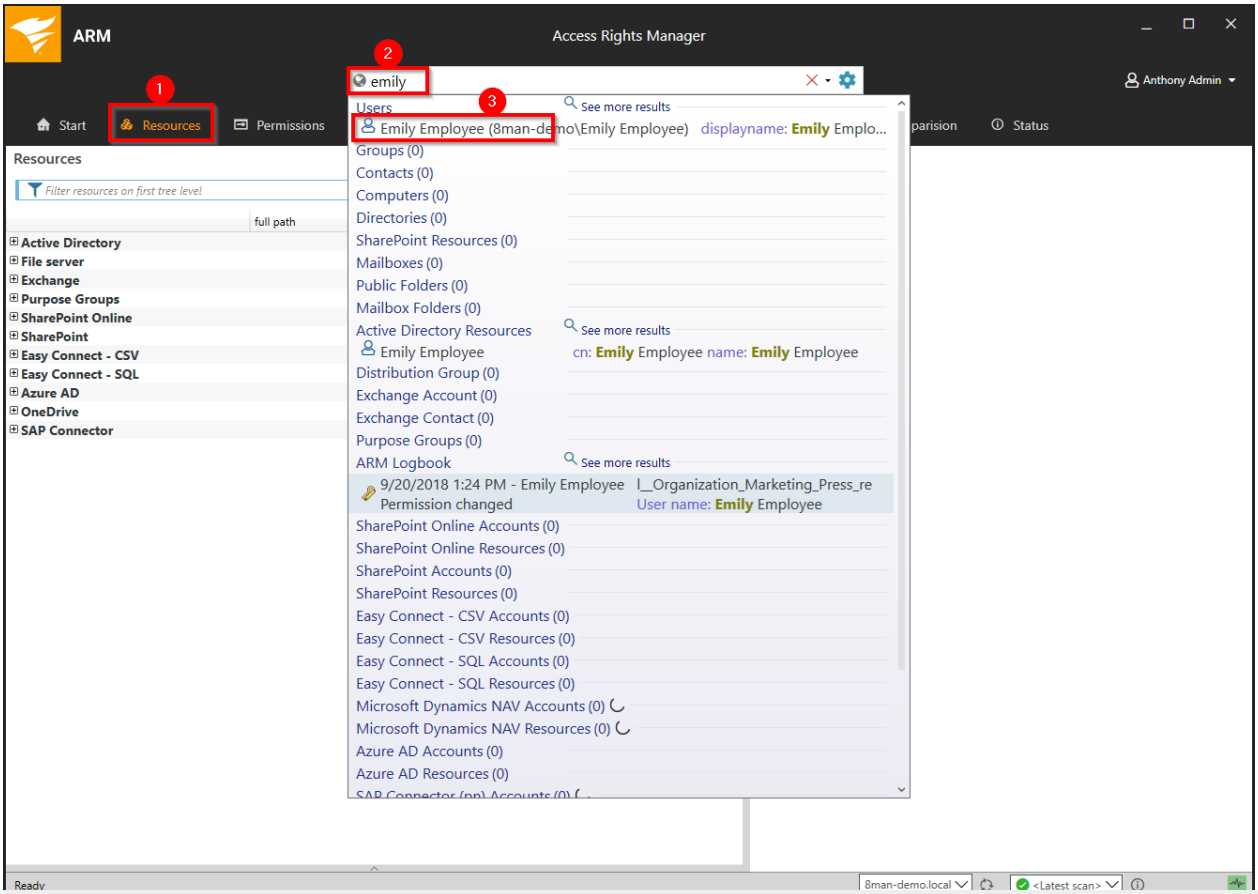
Background / Value

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.

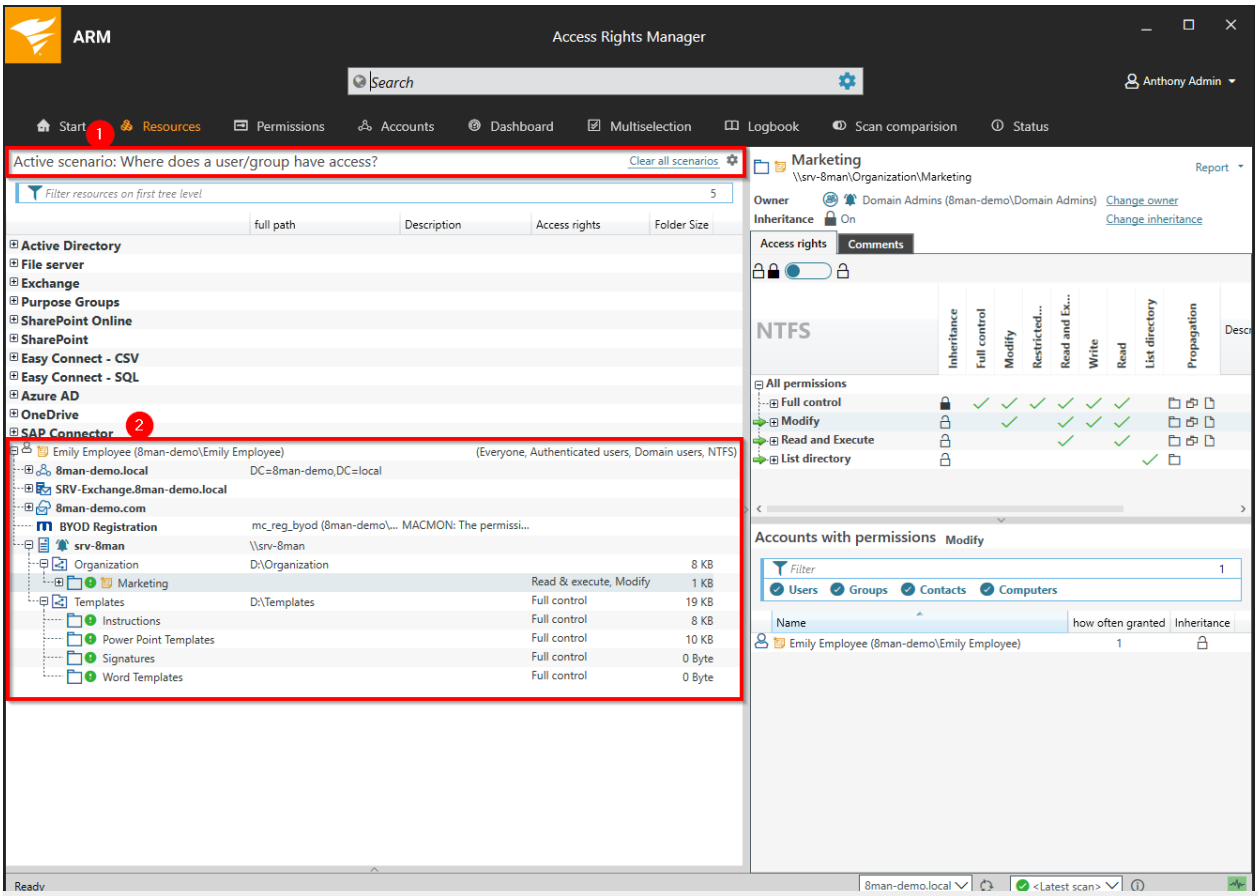
Related features

Report: Where do users and groups have access to?

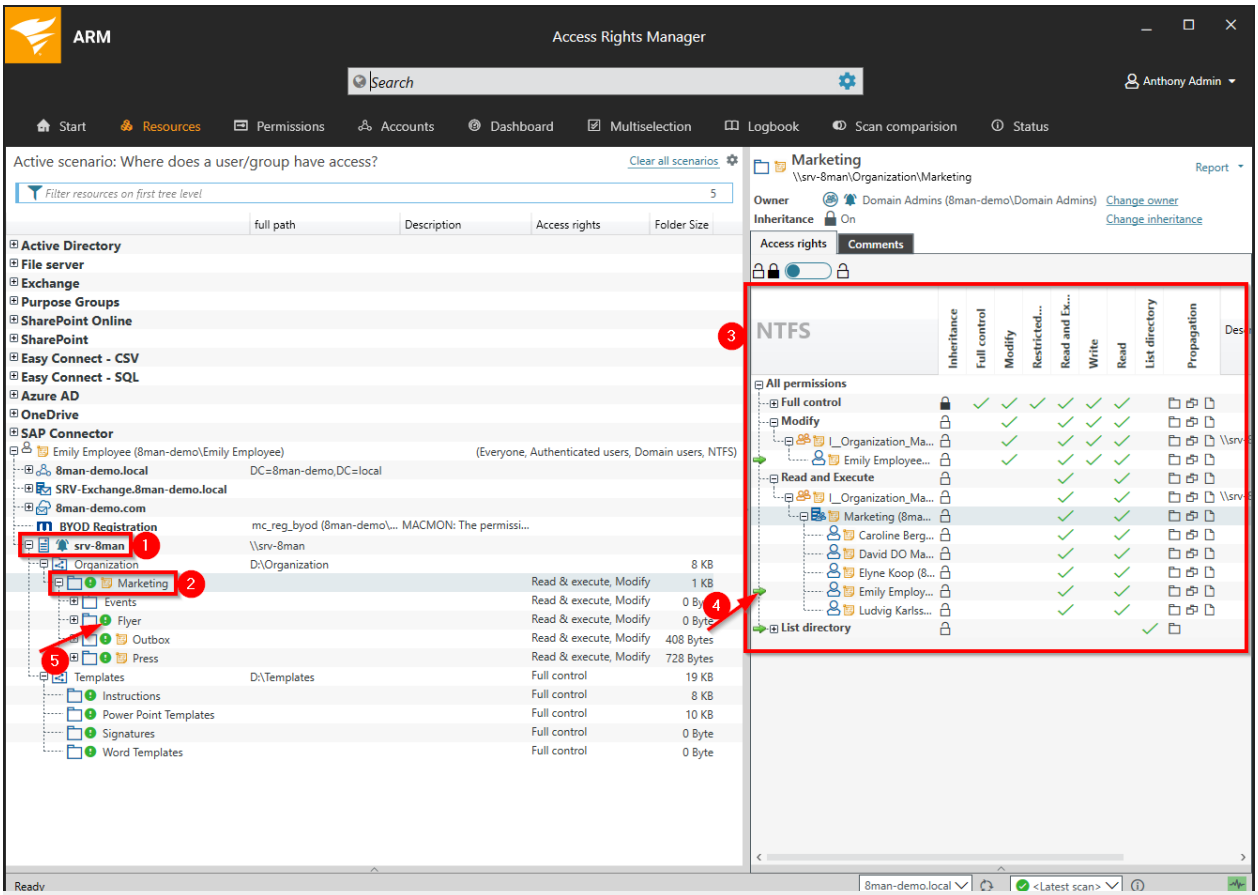
Step-by-step process



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.



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?

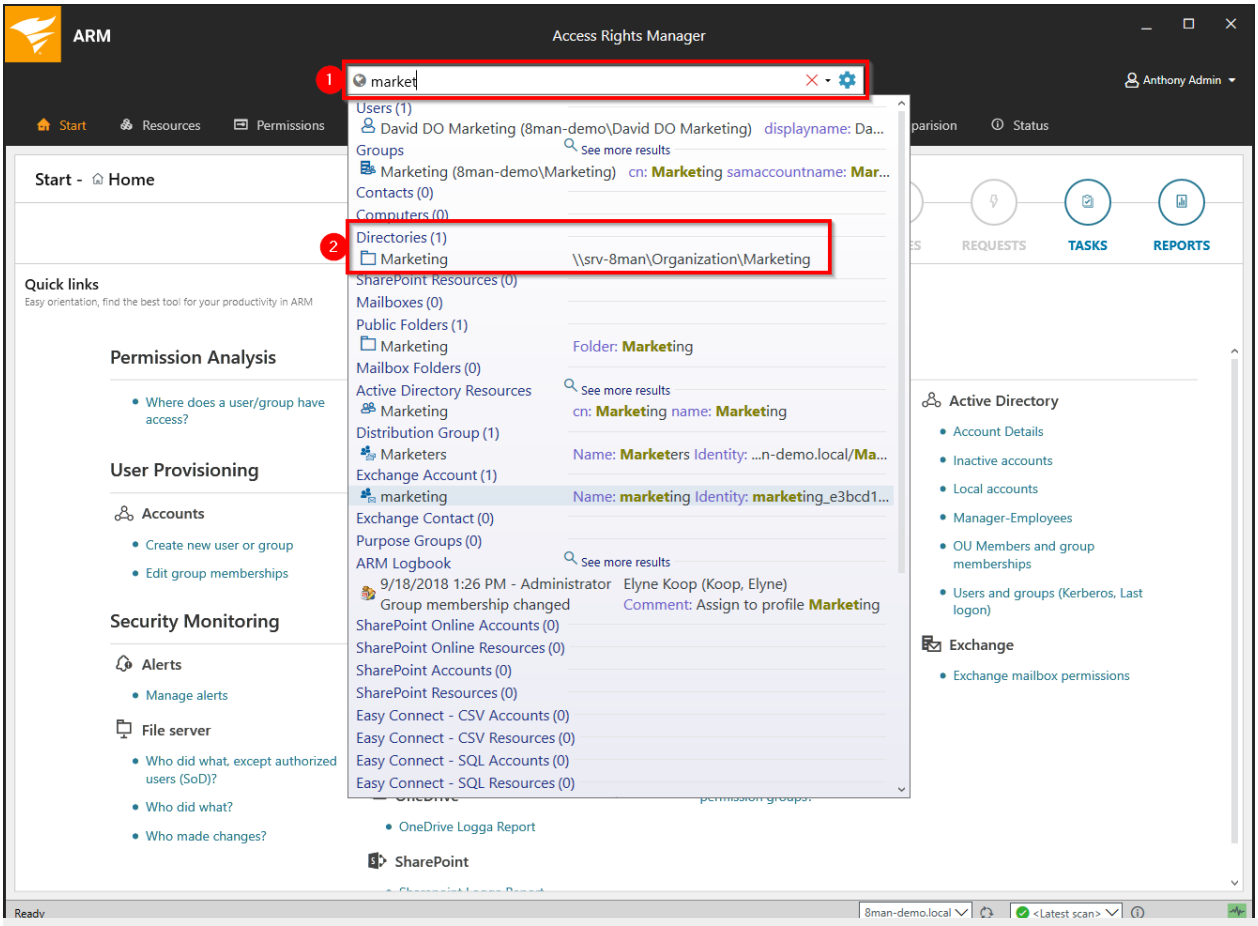
Related features

Report: Who has access where?

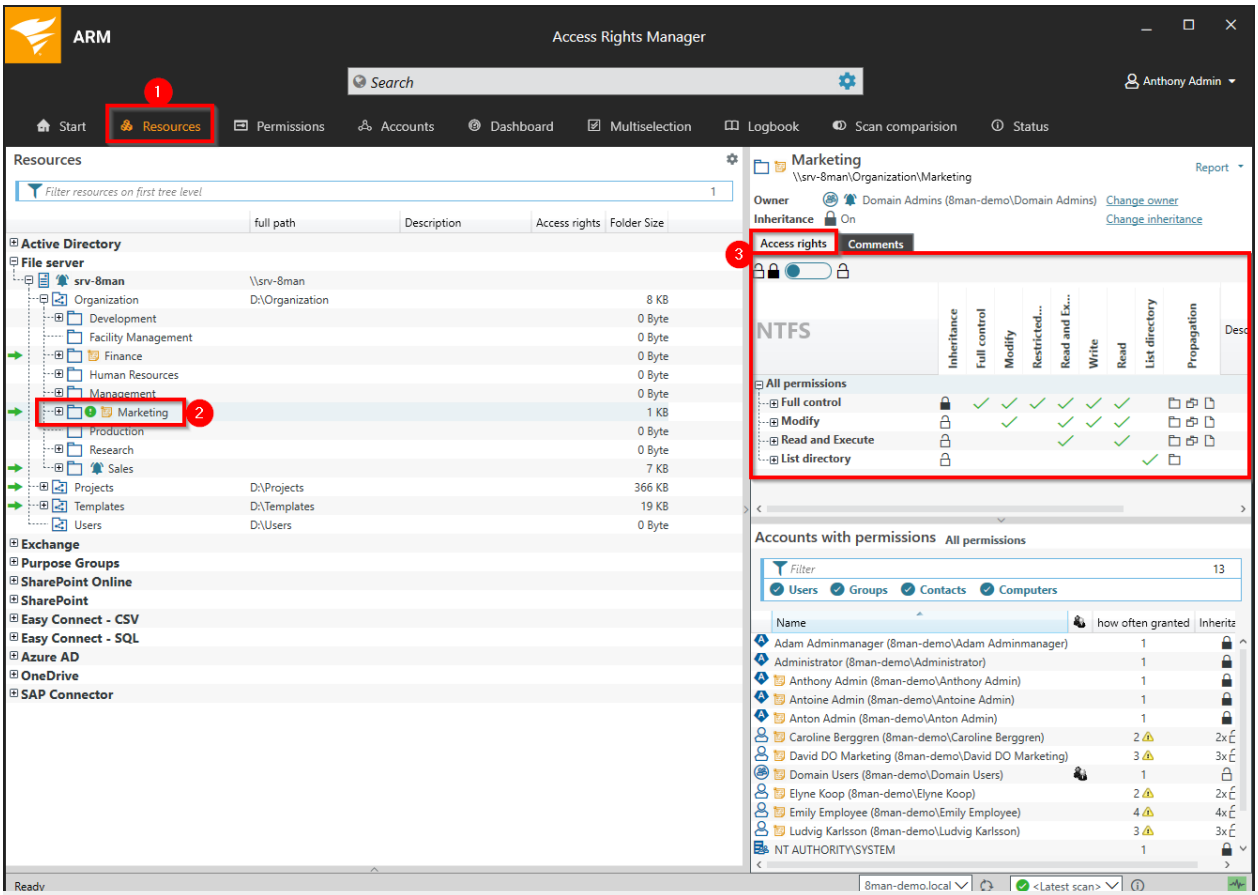
Modify directory access rights

Monitor access to sensitive data

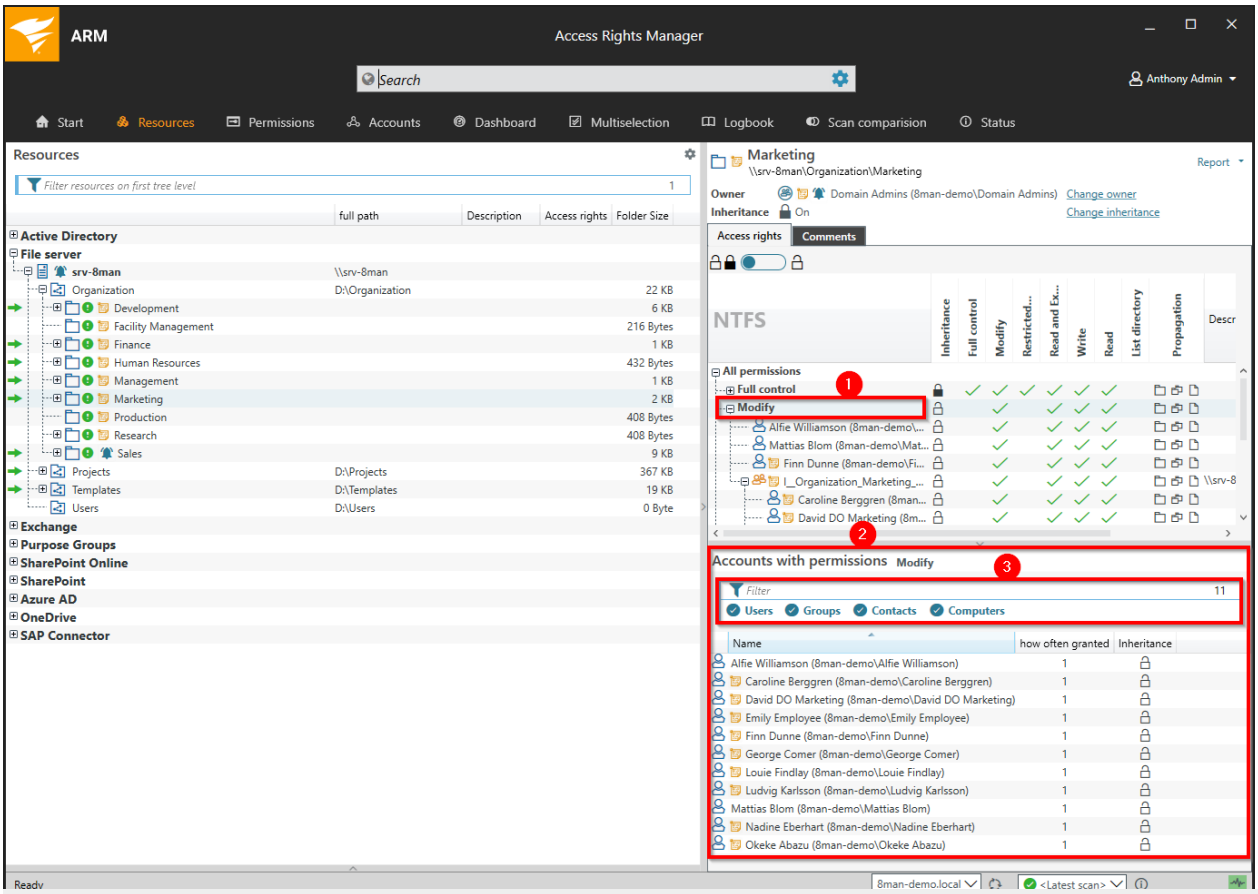
Step-by-step process



1. Search for the desired directory.
2. You can find your search result in the directory section.



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.



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.

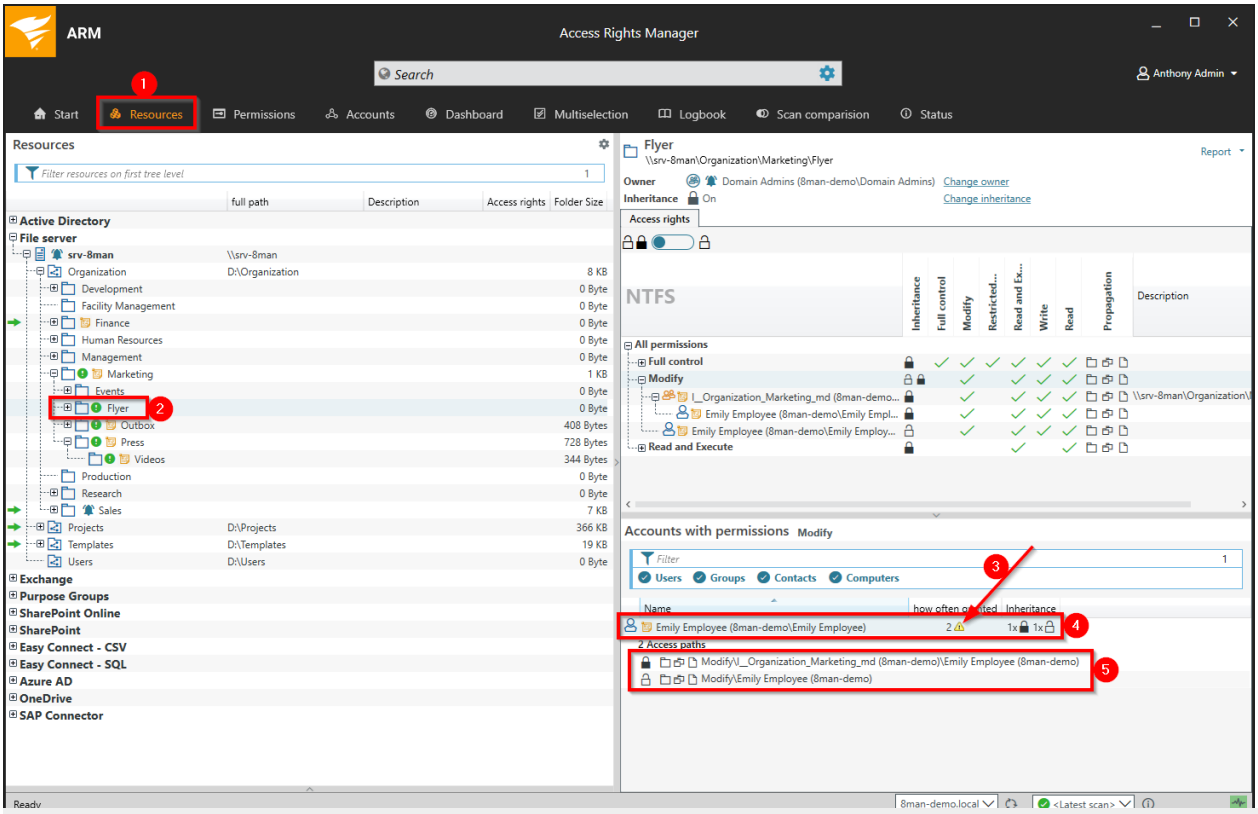
In practice, it often happens that you remove only one access path and then wonder why the user still has access. With ARM you can see all existing access paths with just a few clicks. This is the basis for completely removing all access paths.

Related features

Remove multiple access paths to file server directories

Manage group memberships

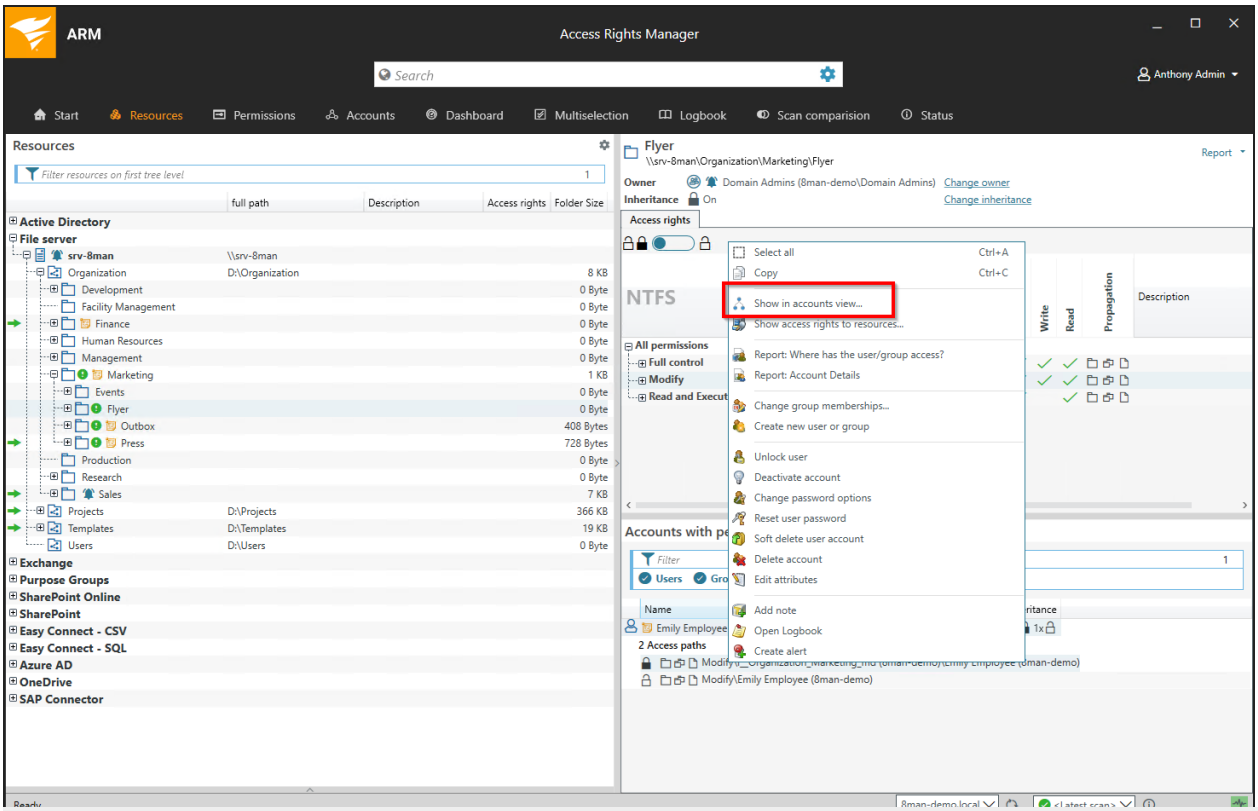
Step-by-step process



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.



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.

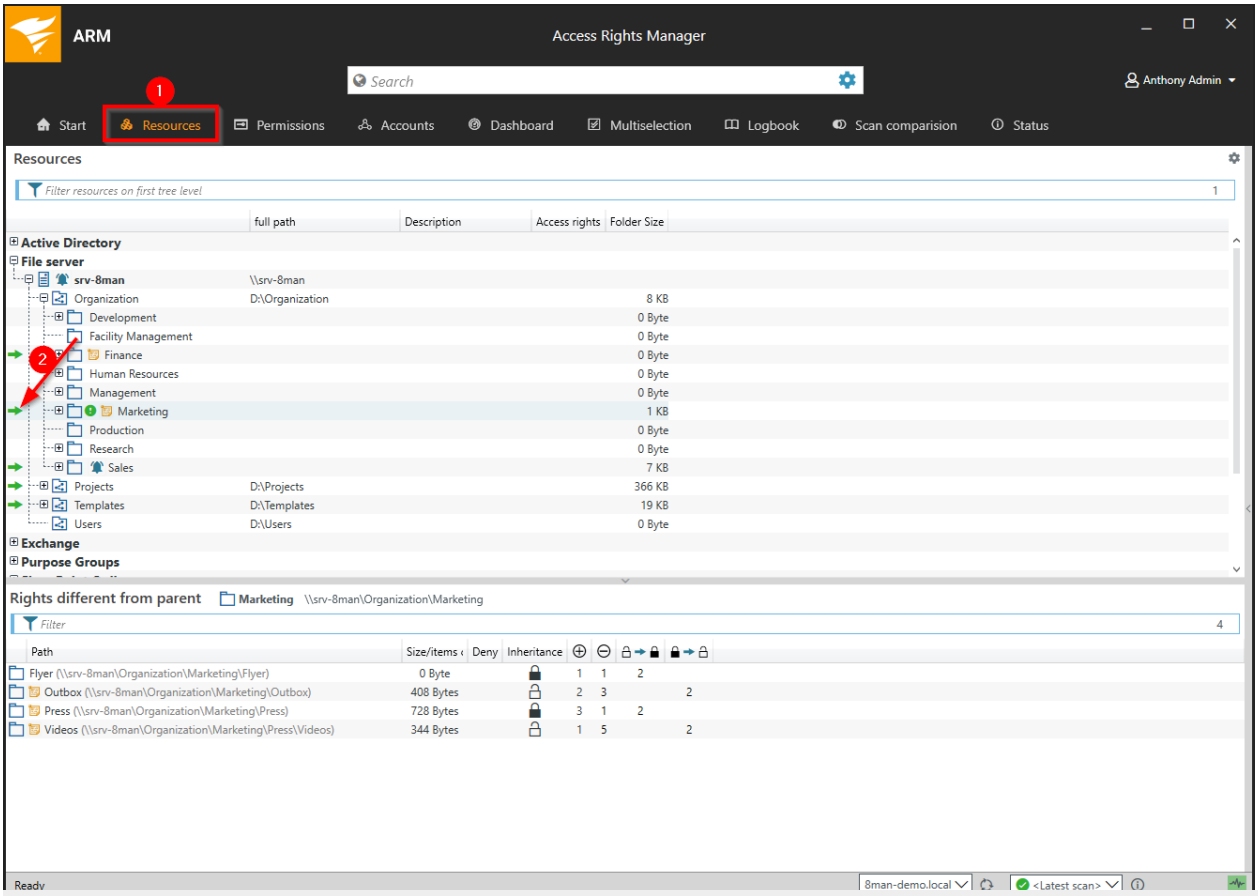
Related features

Report: Who has access where?

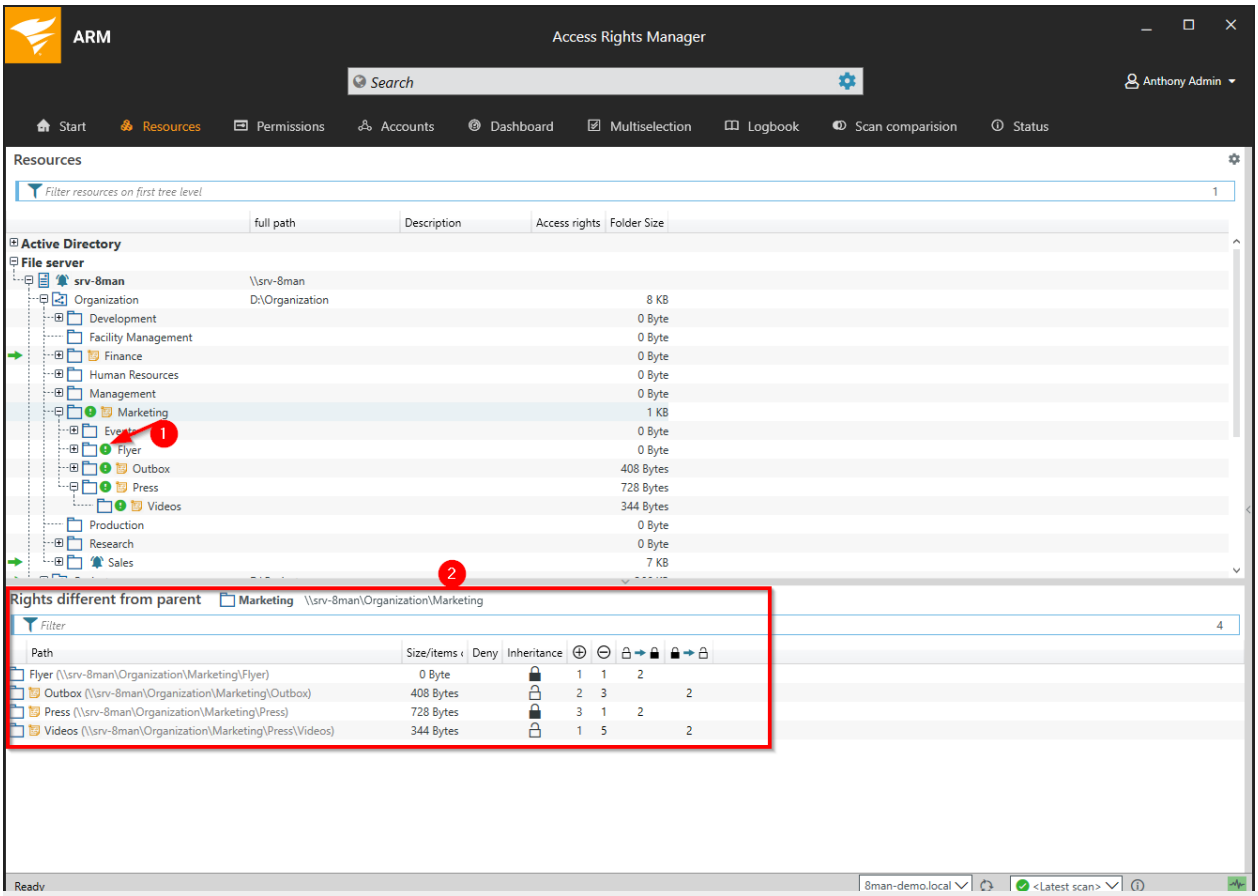
Report: Where do users/groups have access?

Identify corrupted inheritance

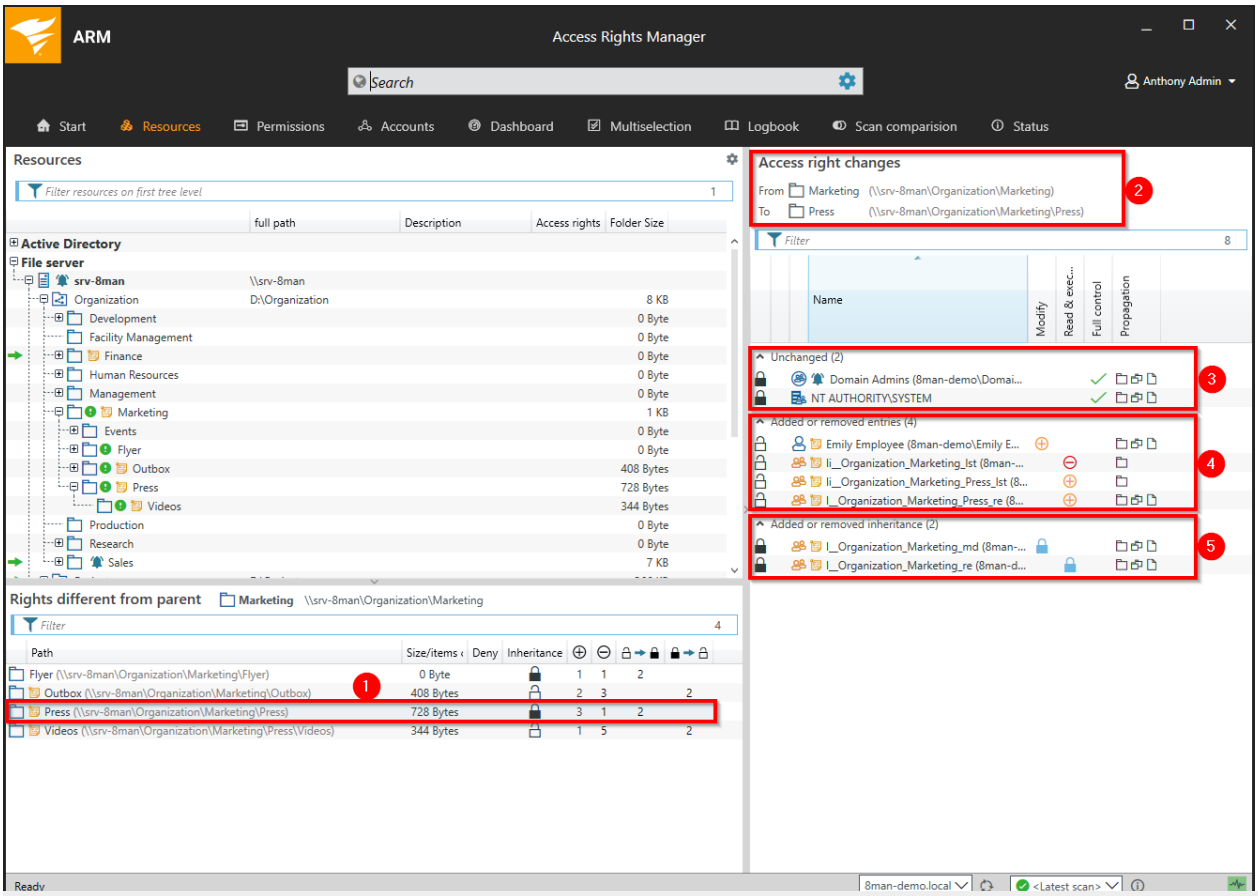
Step-by-step process



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.



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 diviating access rights. A "Plus" signifies added access rights while a "Minus" signifies removed access rights.

Analyze historical access rights situations

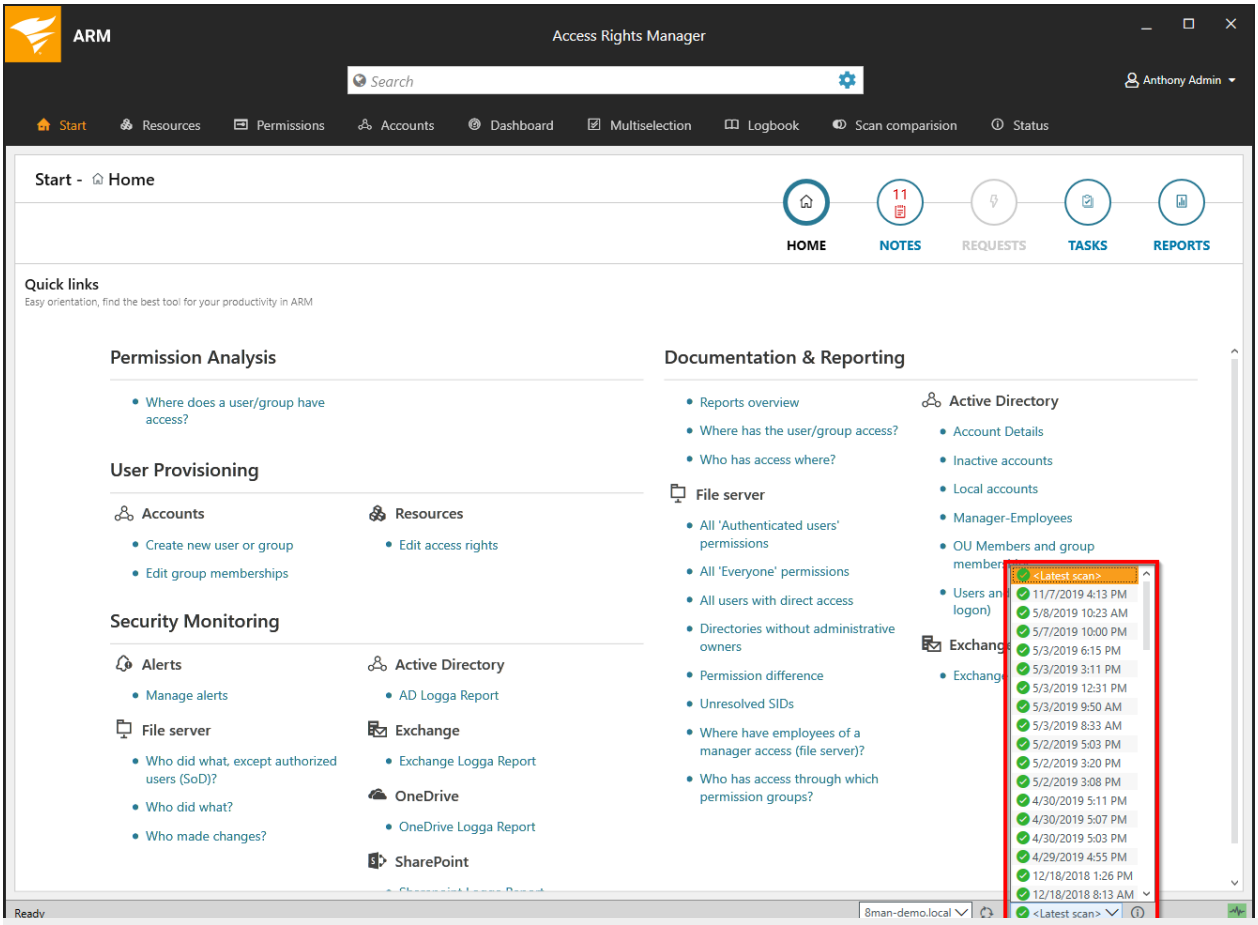
Background / Value

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.

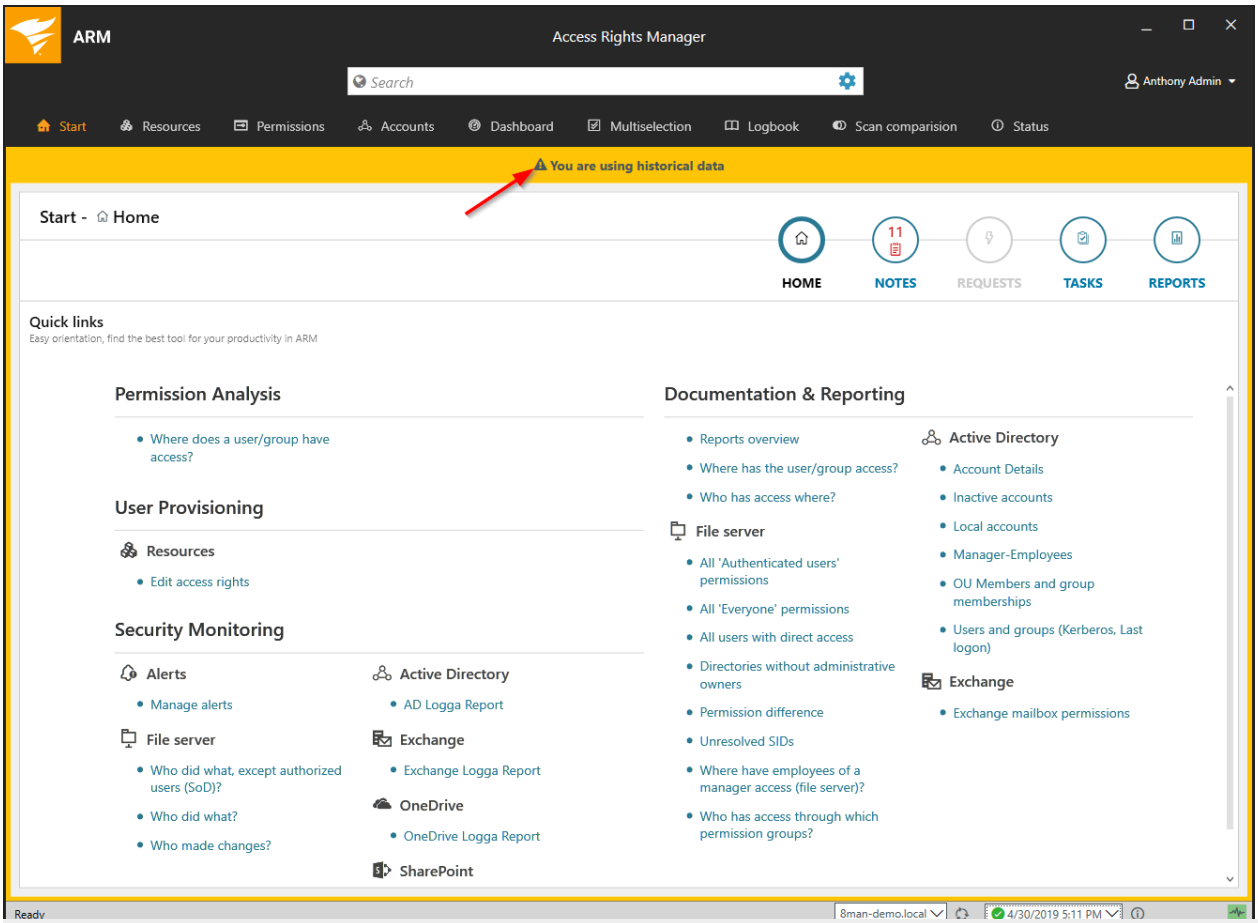
Related features

Compare two scans from different points in time

Step-by-step process



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

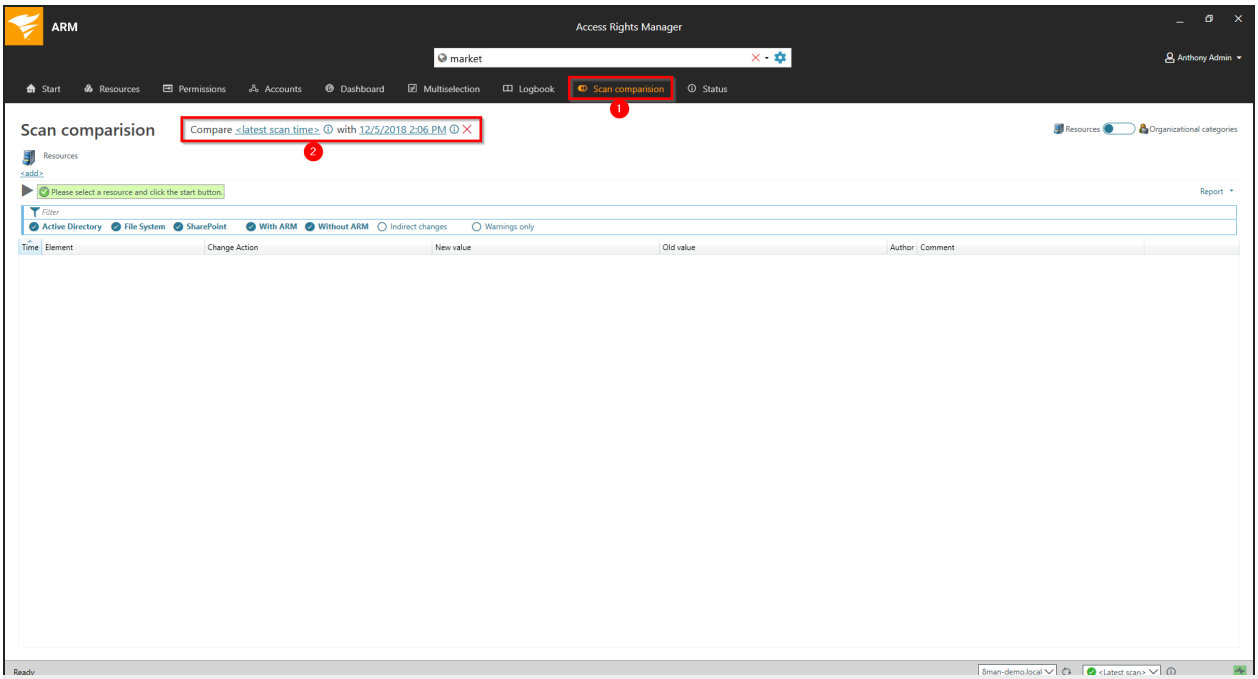
The scan comparison shows the actual states of two authorization situations in the AD and on file servers and compares them with each other. This enables you to determine how the authorization situation has changed.

Related features

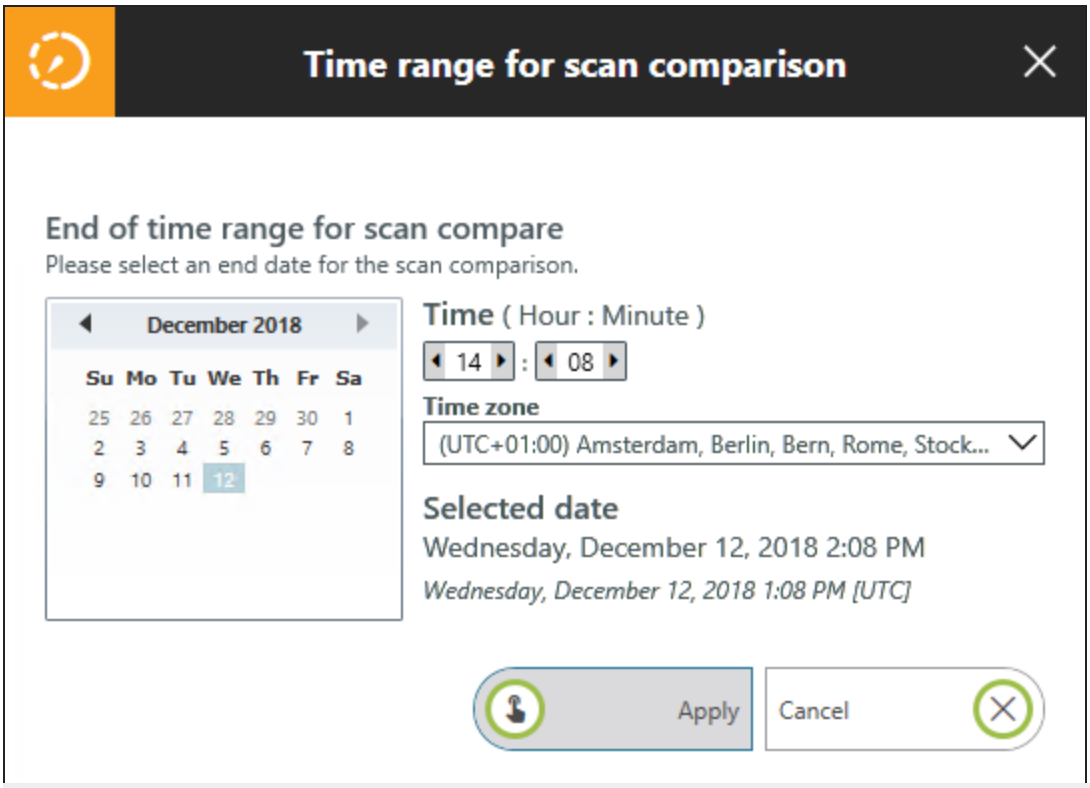
The comparison refers exclusively to two measurement points. Use the Logga reports to analyze all changes of a period.

Use the Report on permission differences to forward comparison results to other persons.

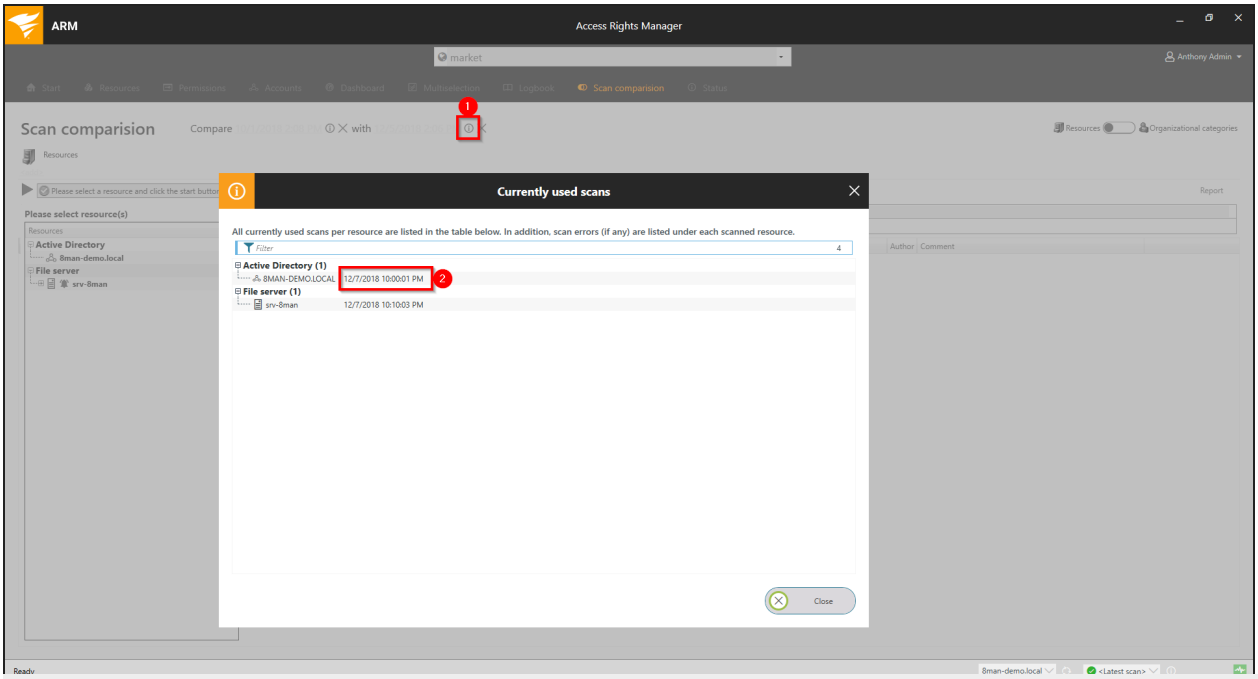
Step-by-step process



1. Click on "Scan comparison".
2. Select the two scans that you want to compare.

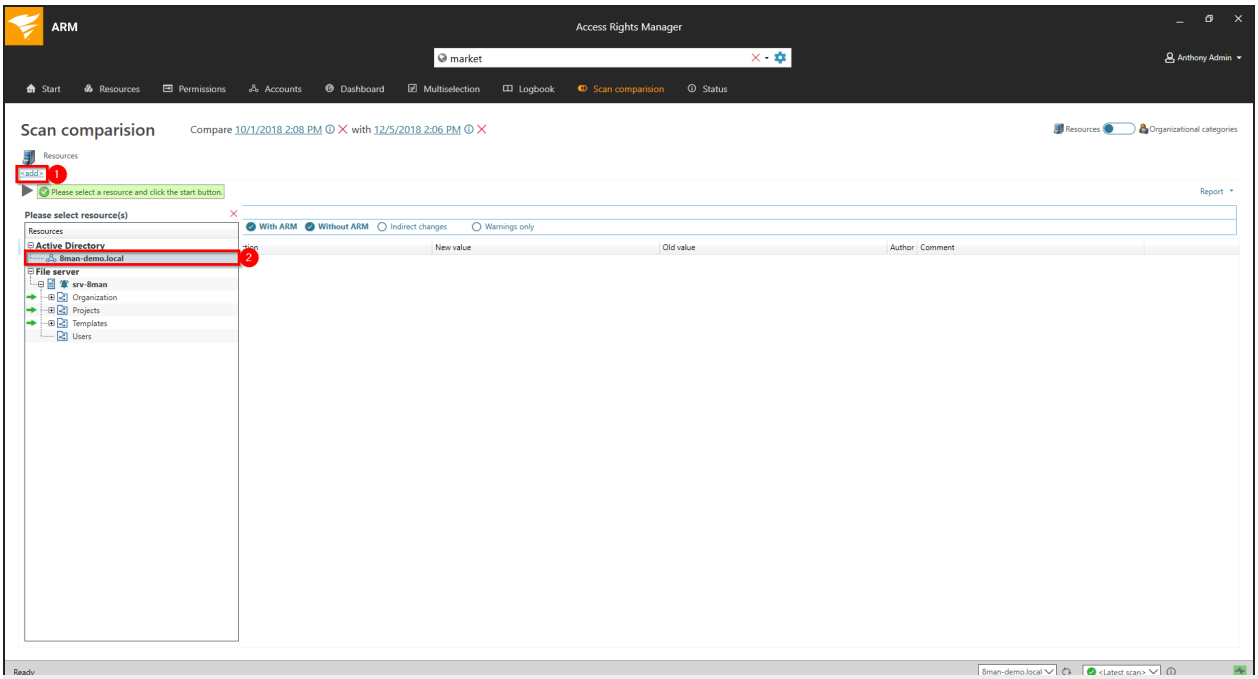


Specify the date and time for the start and end points.

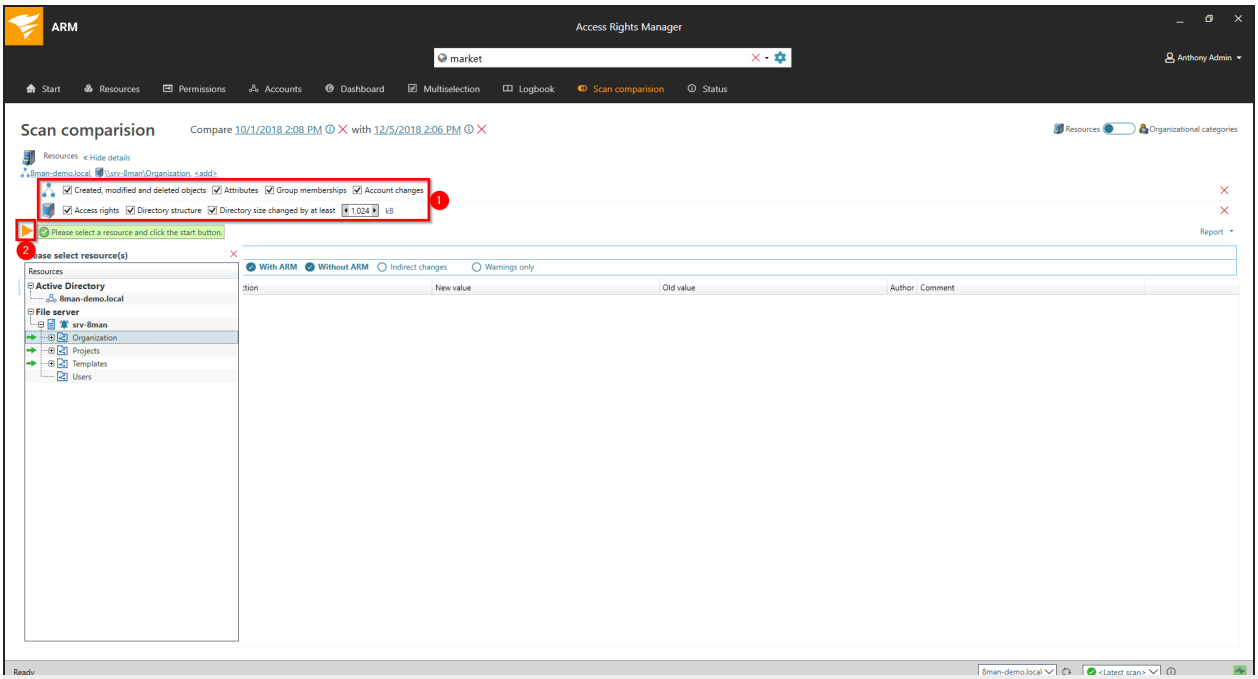


The comparison always compares existing scans.

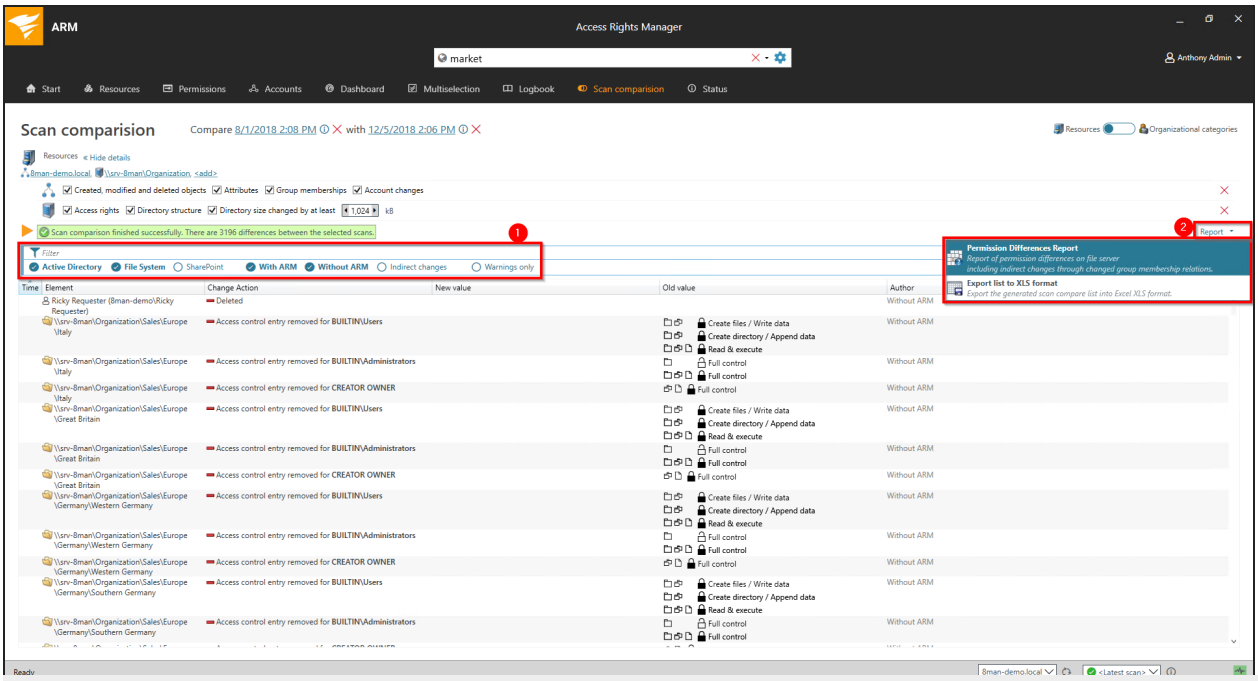
1. Click on the information symbol.
2. Date and time of the selected scan is indicated on the right-hand side.



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

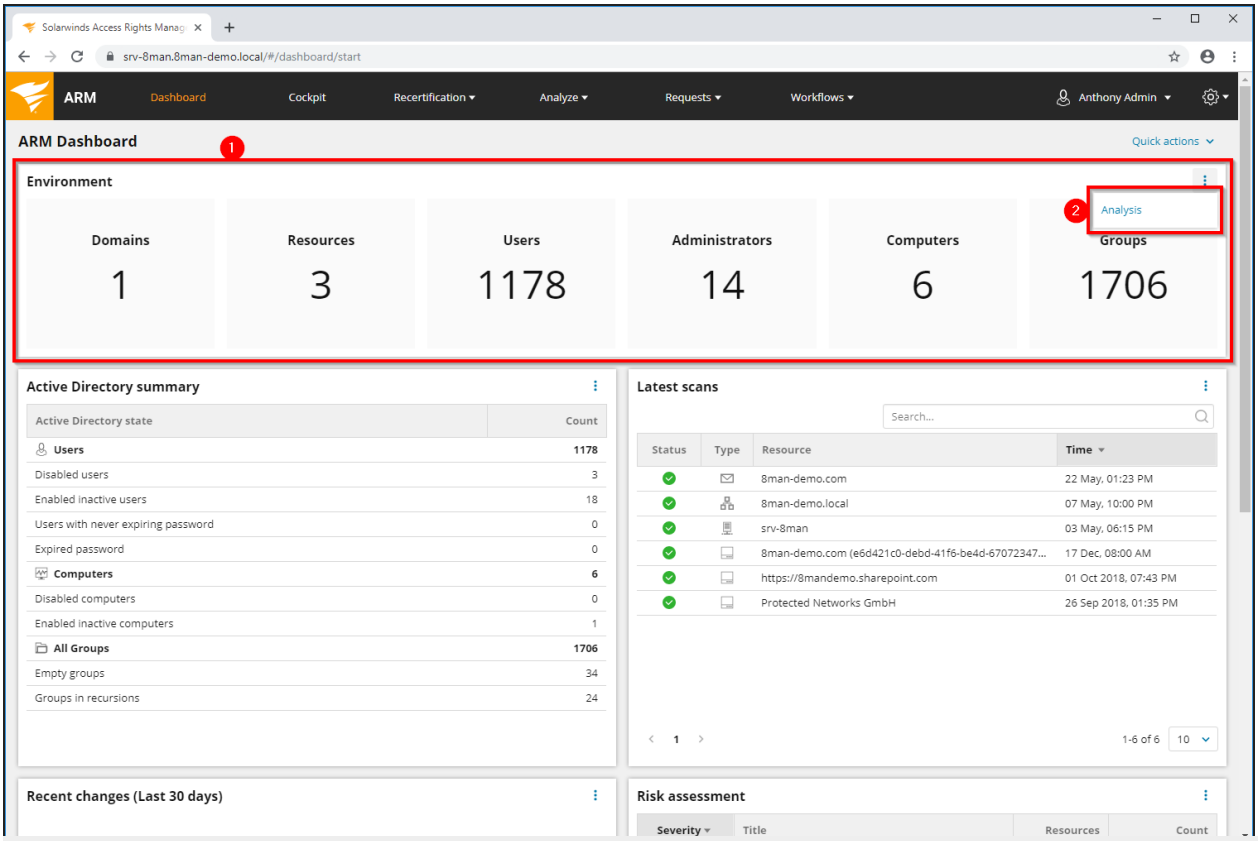
Background / Value

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.

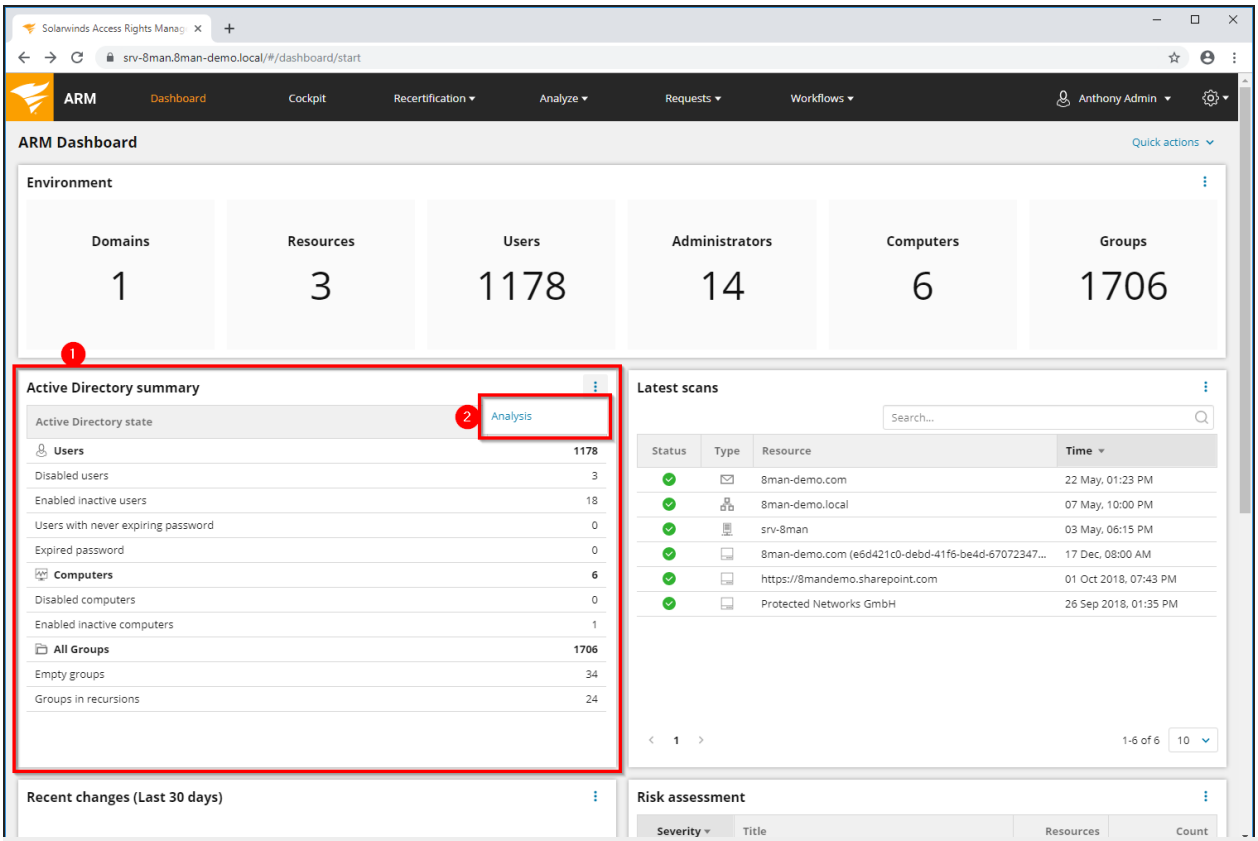
Related features

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.

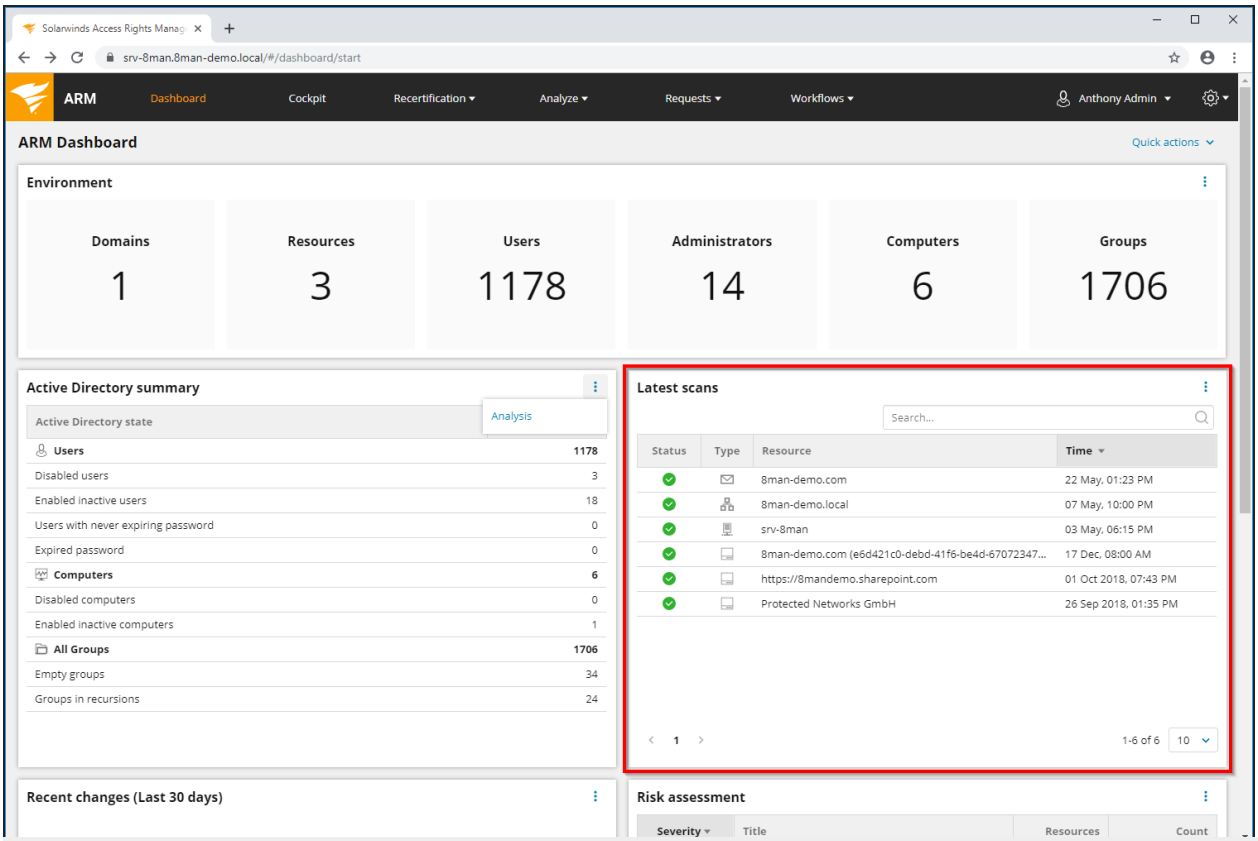
Step-by-step process



1. Summary of your environment.
2. Jump quickly to the Analyze scenarios.

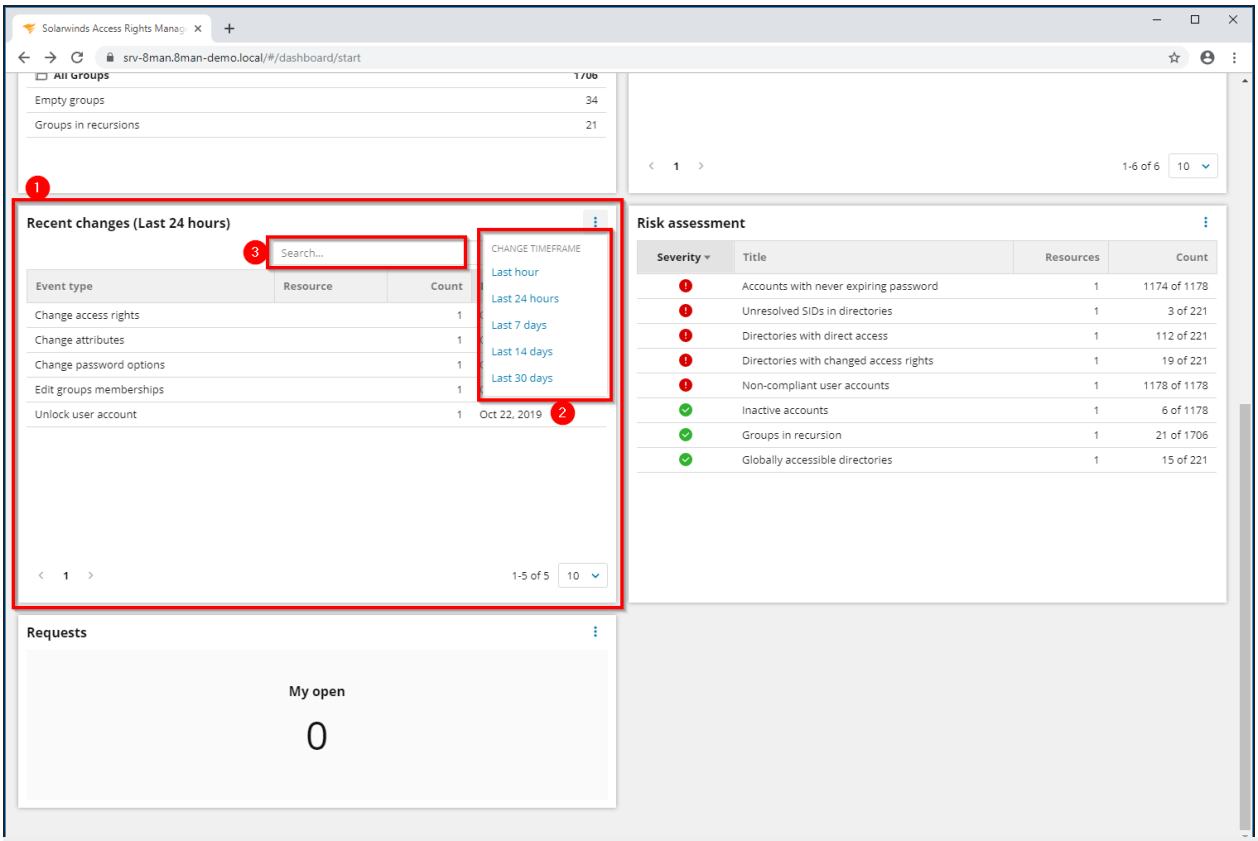


1. Summary of your Active Directory.
2. Jump quickly to the Active Directory Analyze scenarios.

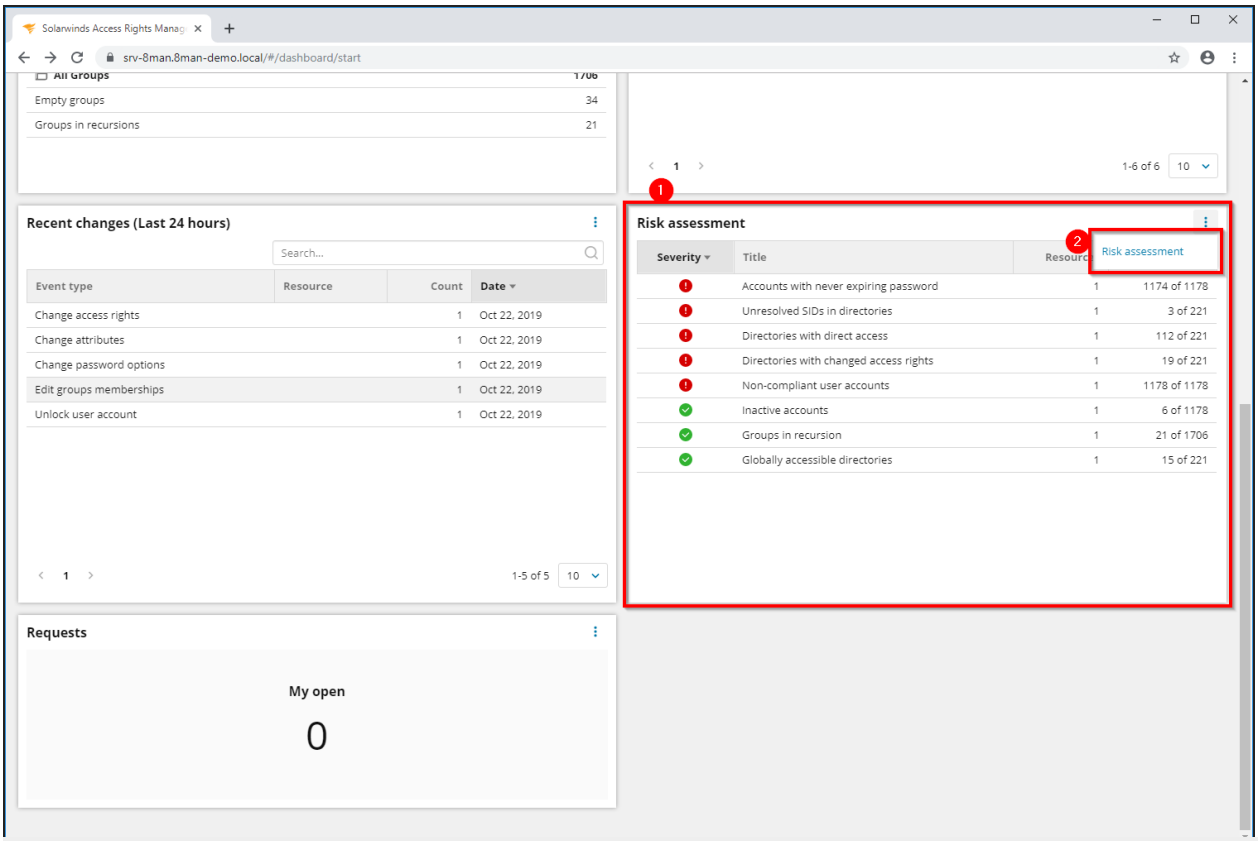


ARM shows you the status of your configured scans of resources.

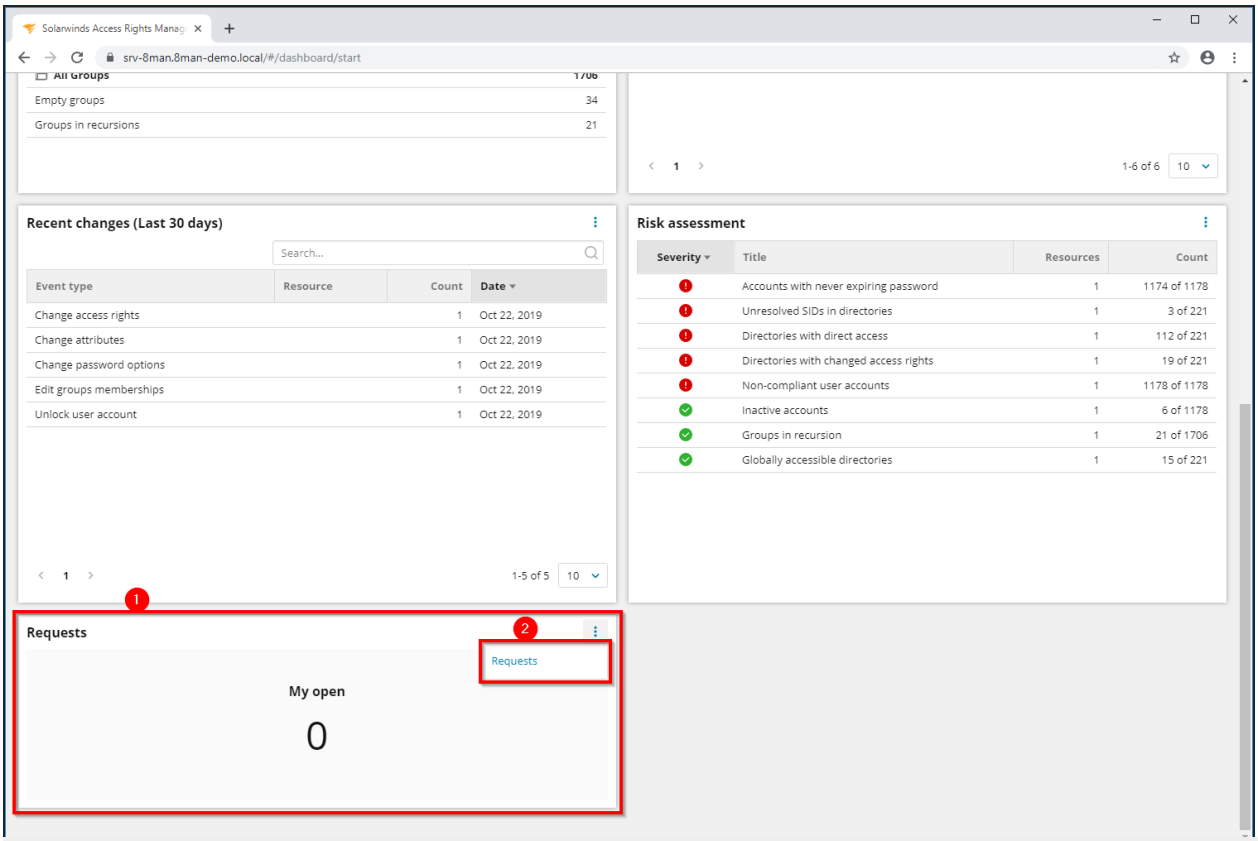
Use the ARM configuration application to find detailed status messages of your scans or to adjust the scan configuration.



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 finds 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.



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.

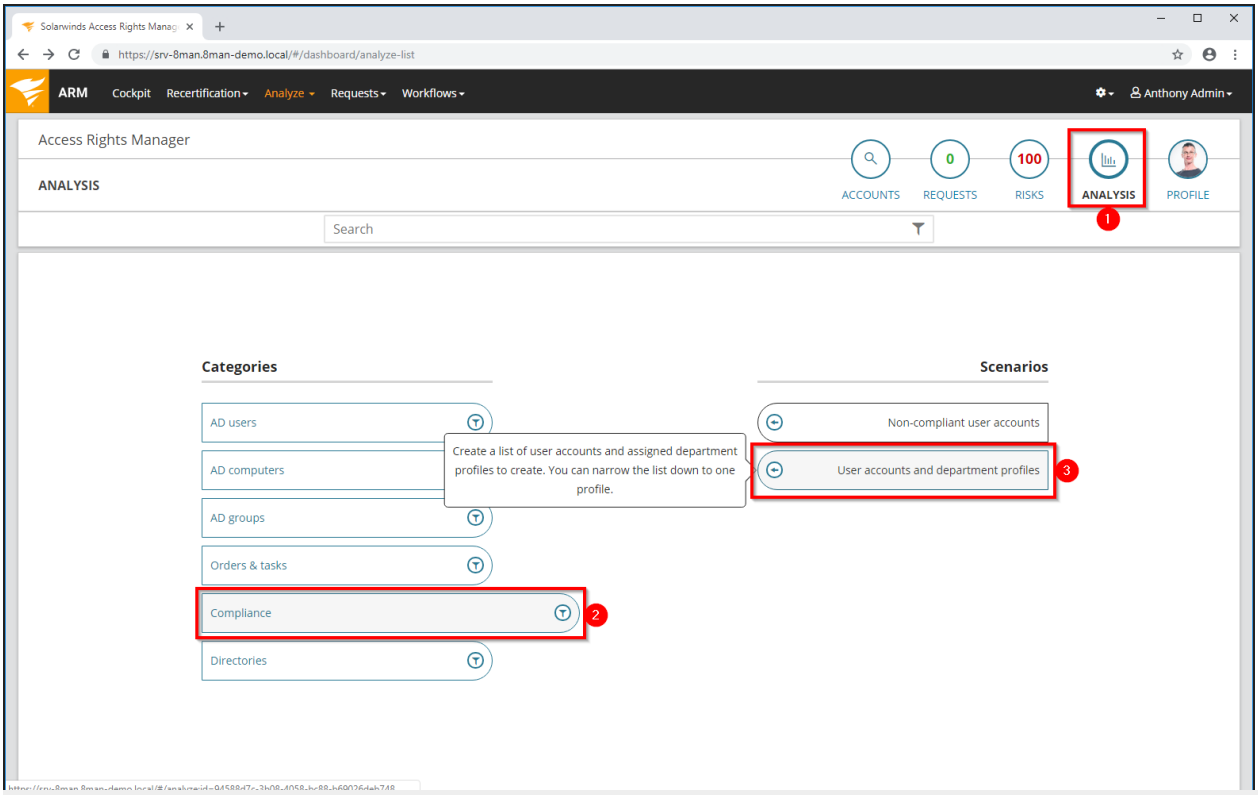
To be able to use the compliance functions, you must have created at least one department profile.

Related features

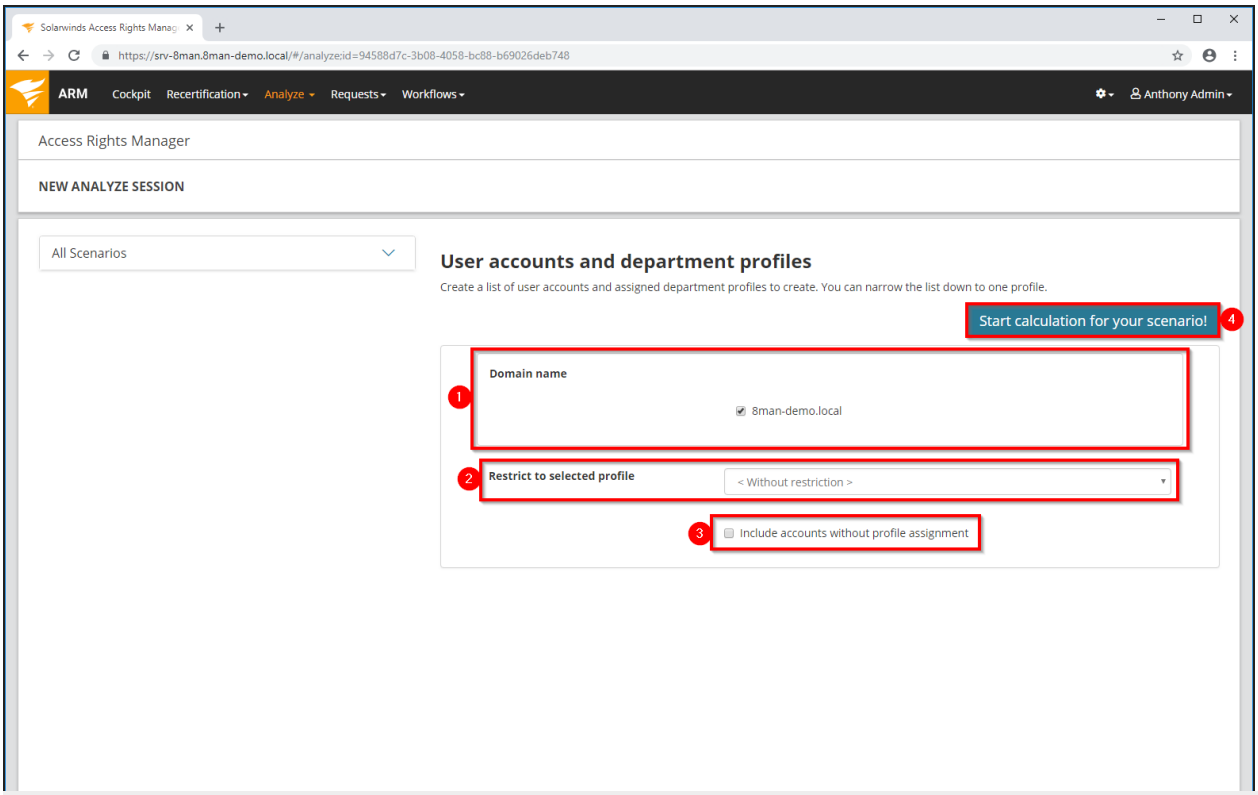
Create a new department profile (Administrator)

Assign a department profile to users

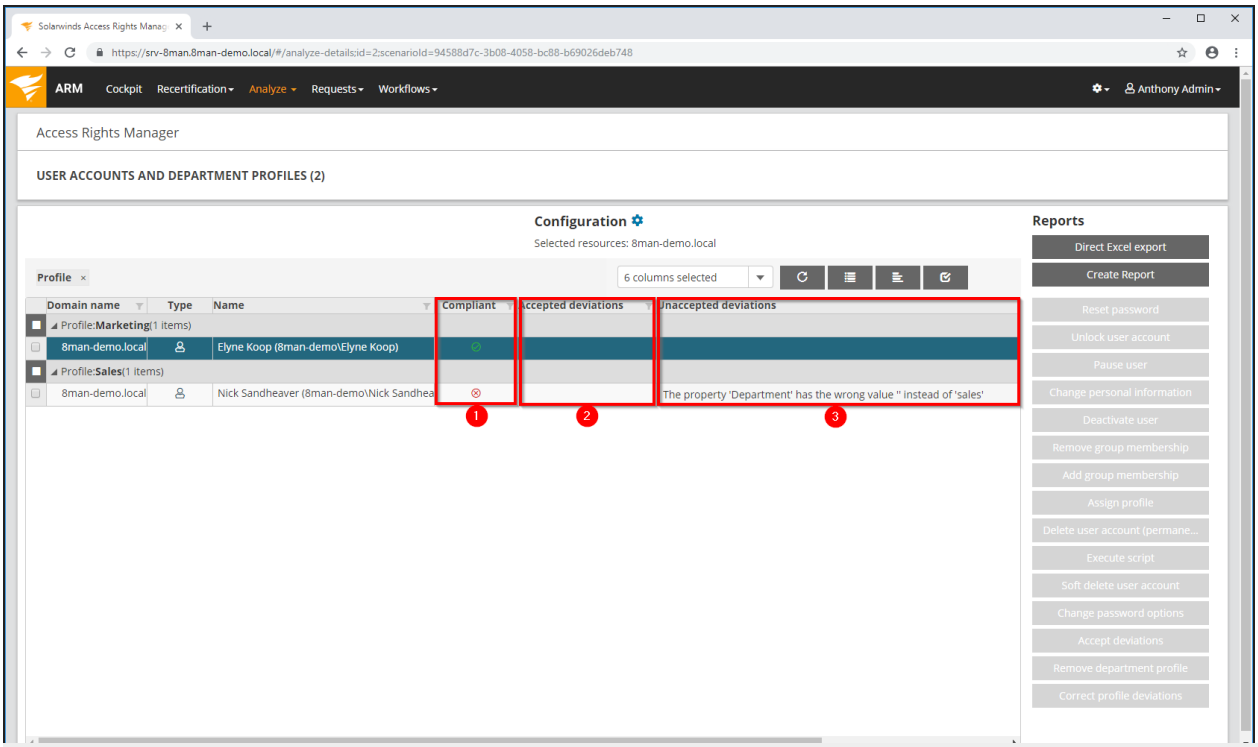
Step-by-step process



1. Select "Analysis".
2. Click "Compliance".
3. Click on "User Accounts and Department Profiles".



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.



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

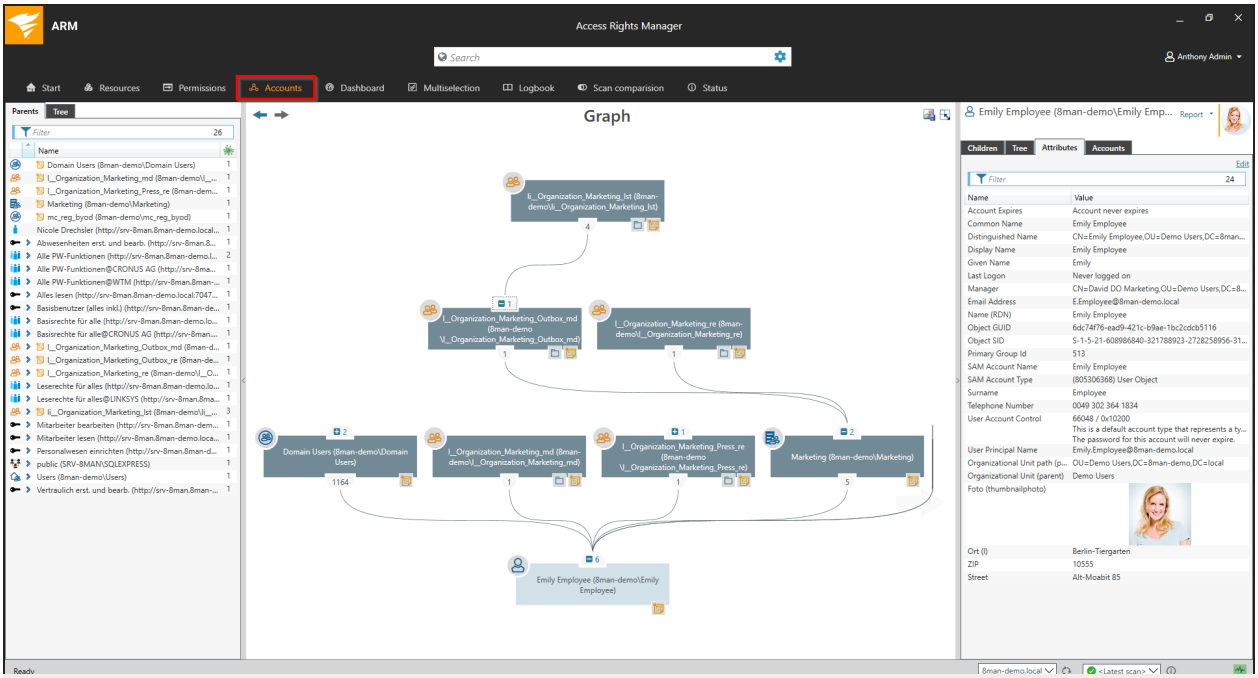
The central component of every Active Directory (AD) is the group concept. Administrators use groups to assign access rights and resources to individual users or user groups. This results in nesting: For example, the group "Marketing" gives access rights to the corresponding file server directories of 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

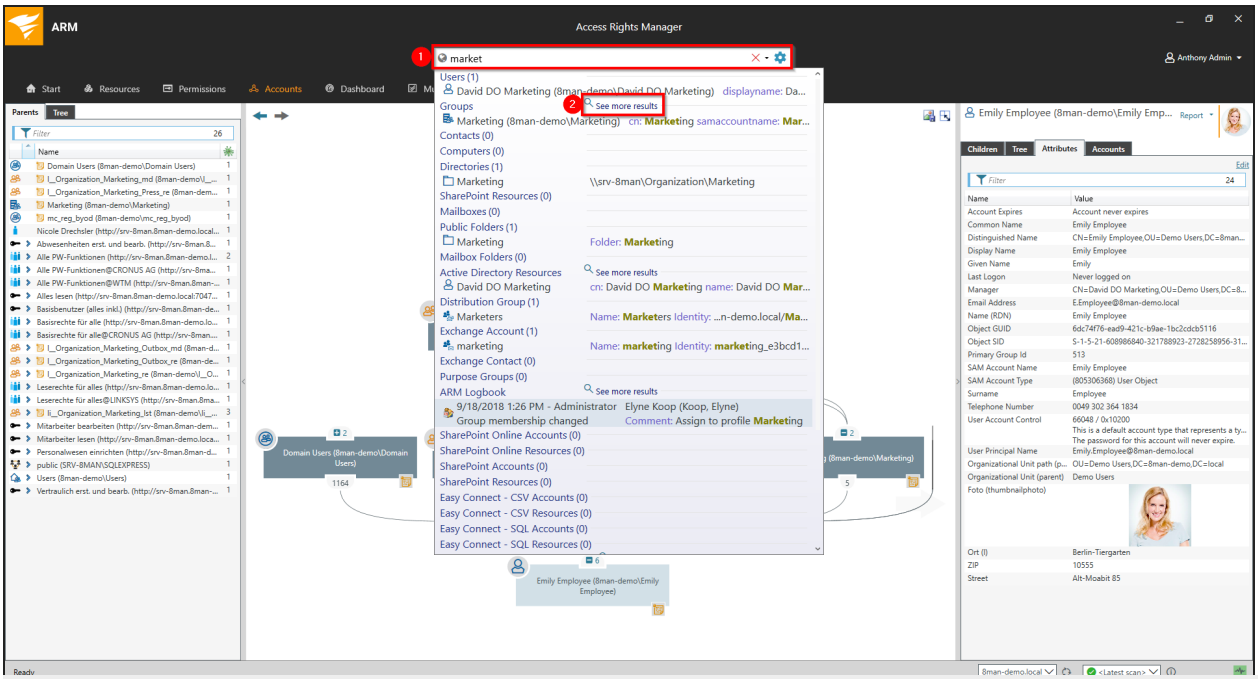
Identify the depth of nesting in your AD

Identify groups in recursion

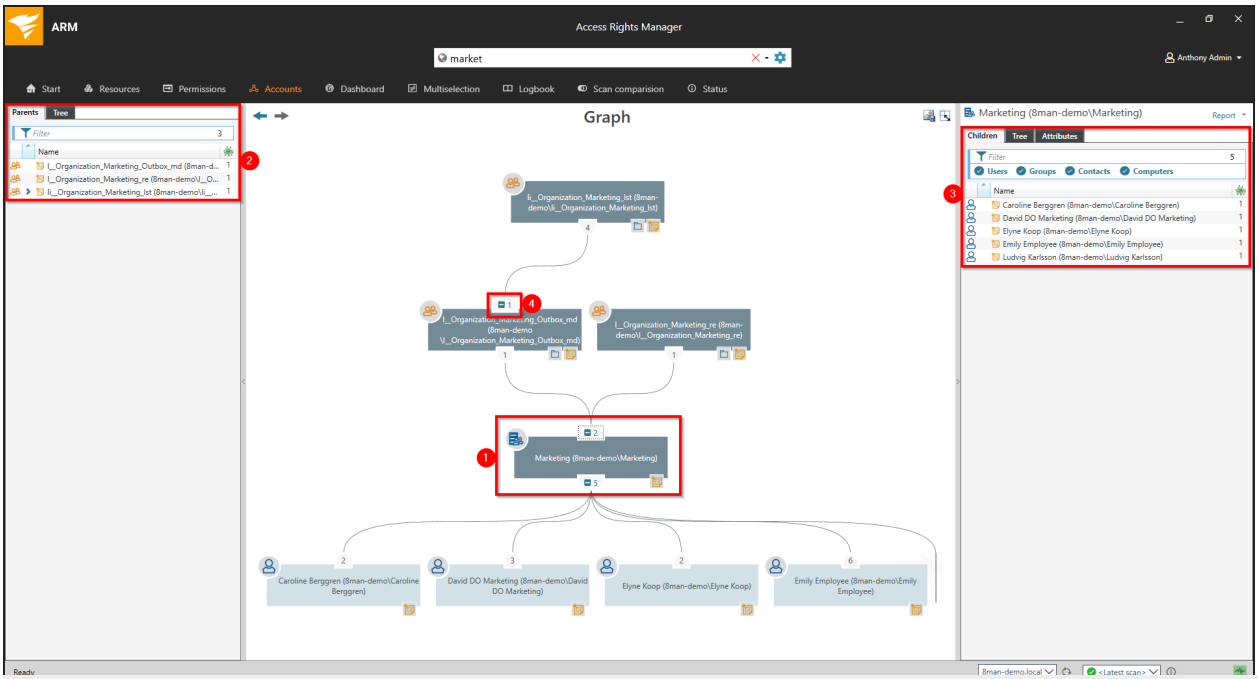
Step-by-step process



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".

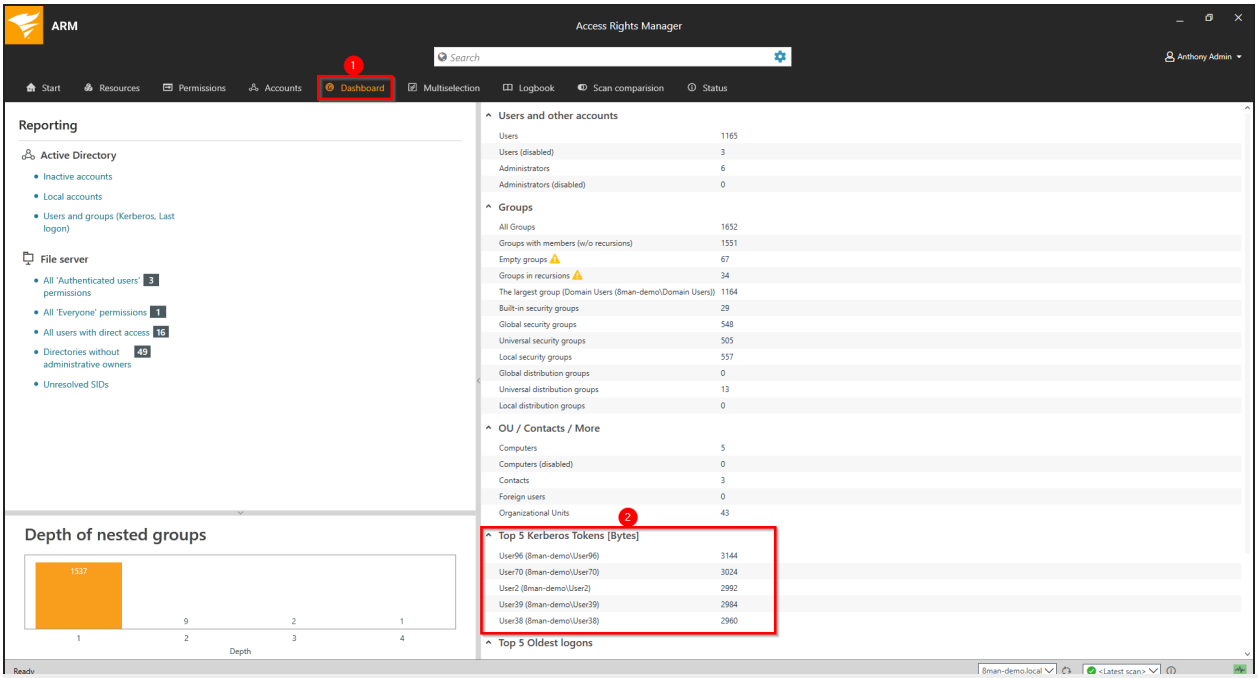
Identify overpriviledged users based on Kerberos token size

Background/Value

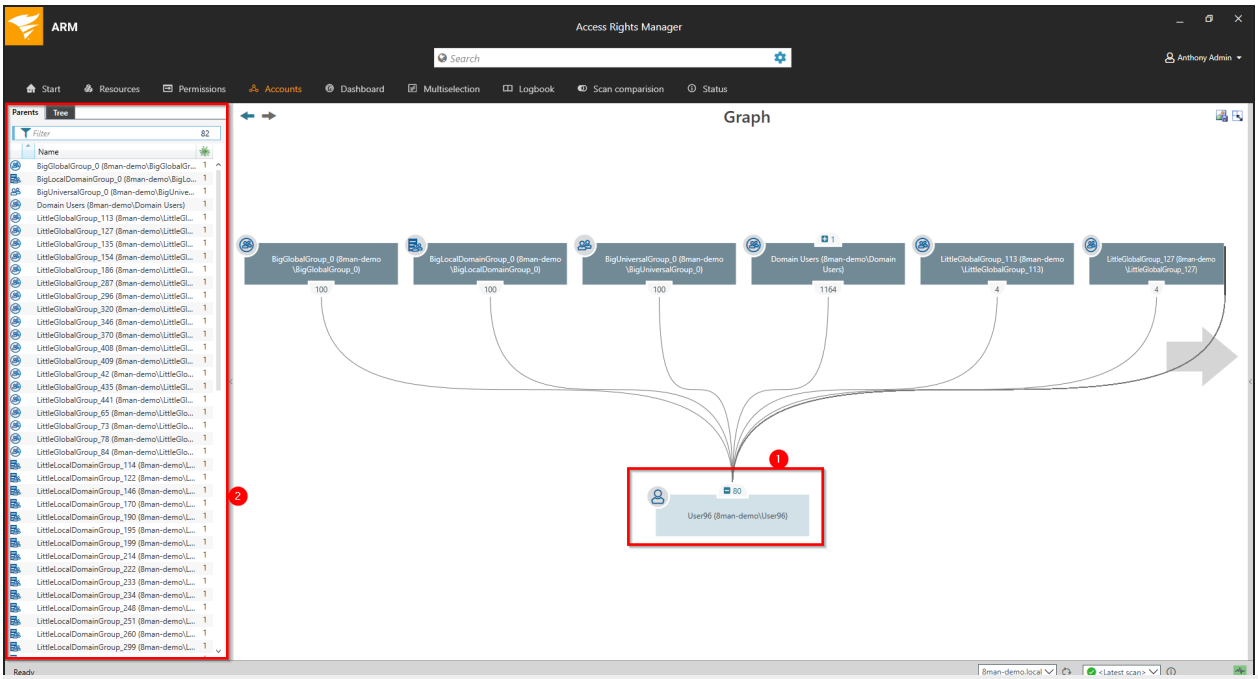
The size of a Kerberos token is a good indicator for identifying users with excessive access rights. The more group memberships a user has, the bigger their Kerberos token. Even if a group membership does not automatically grant privileges, it is worthwhile analyzing the listed users.

In addition, there is a risk that users with too many group memberships will no longer be able to login.

Step-by-step process



1. Select "Dashboard".
2. Double-click on the user in the list "Top 5 Kerberos Tokens".



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

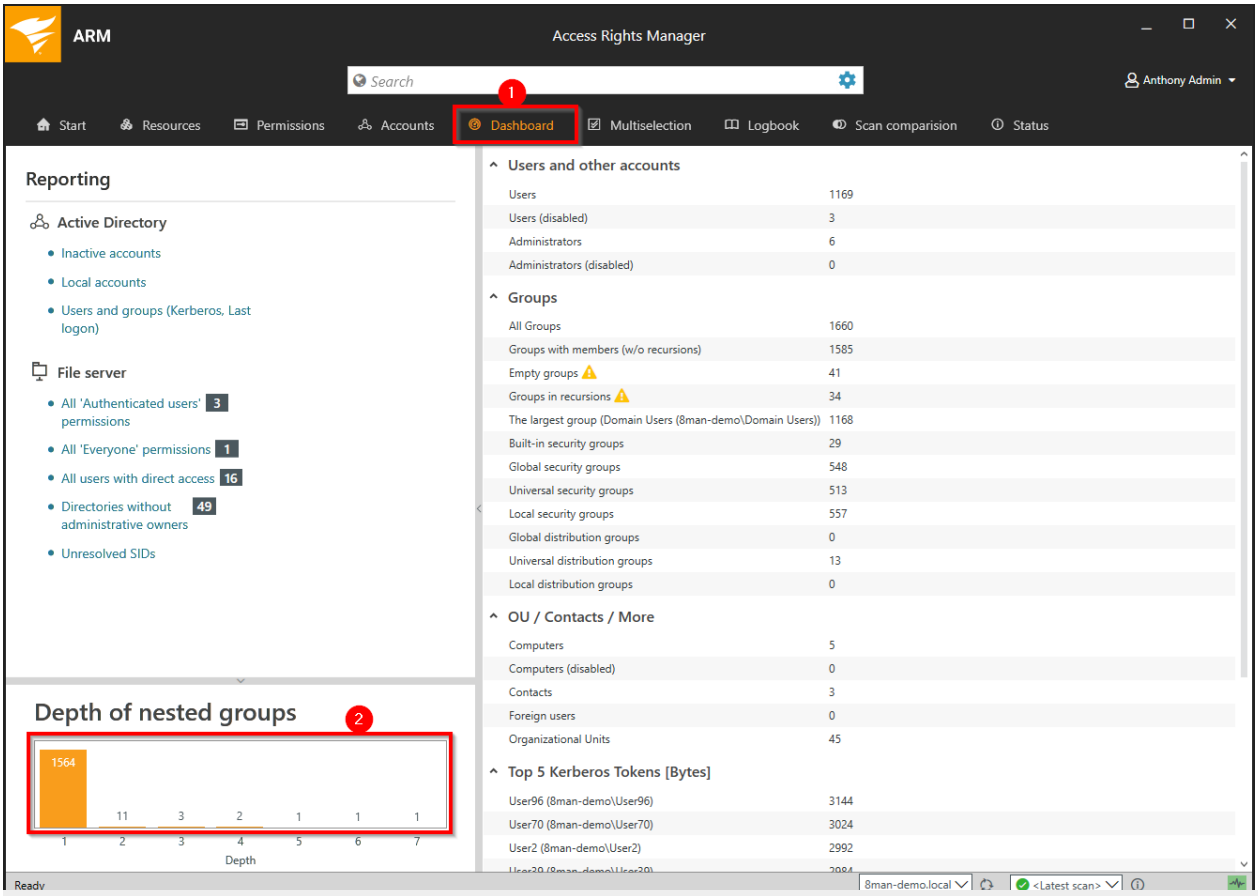
Background/Value

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.

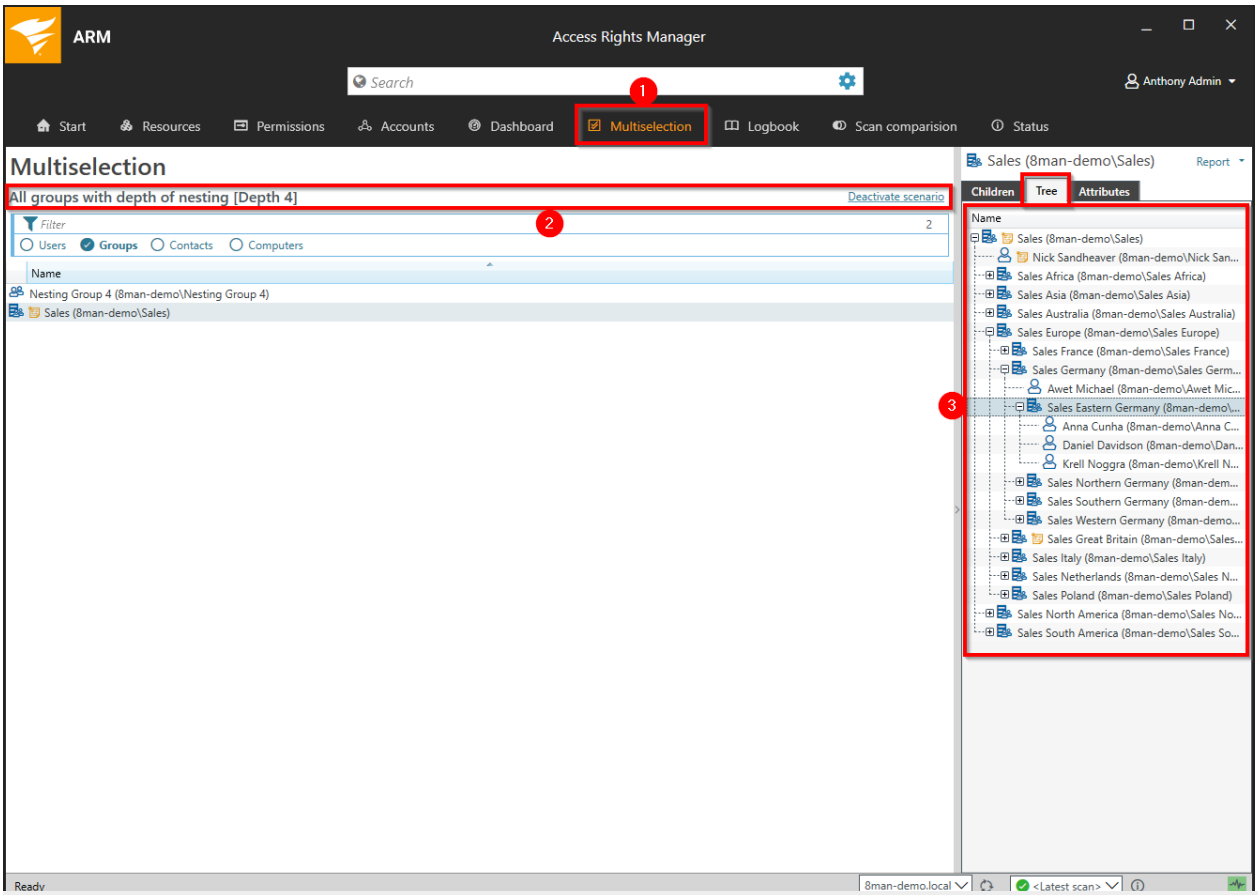
Related features

Reduce multiple groups to one group

Step-by-step process



1. Select the Dashboard.
2. Click on any of the nesting levels.



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

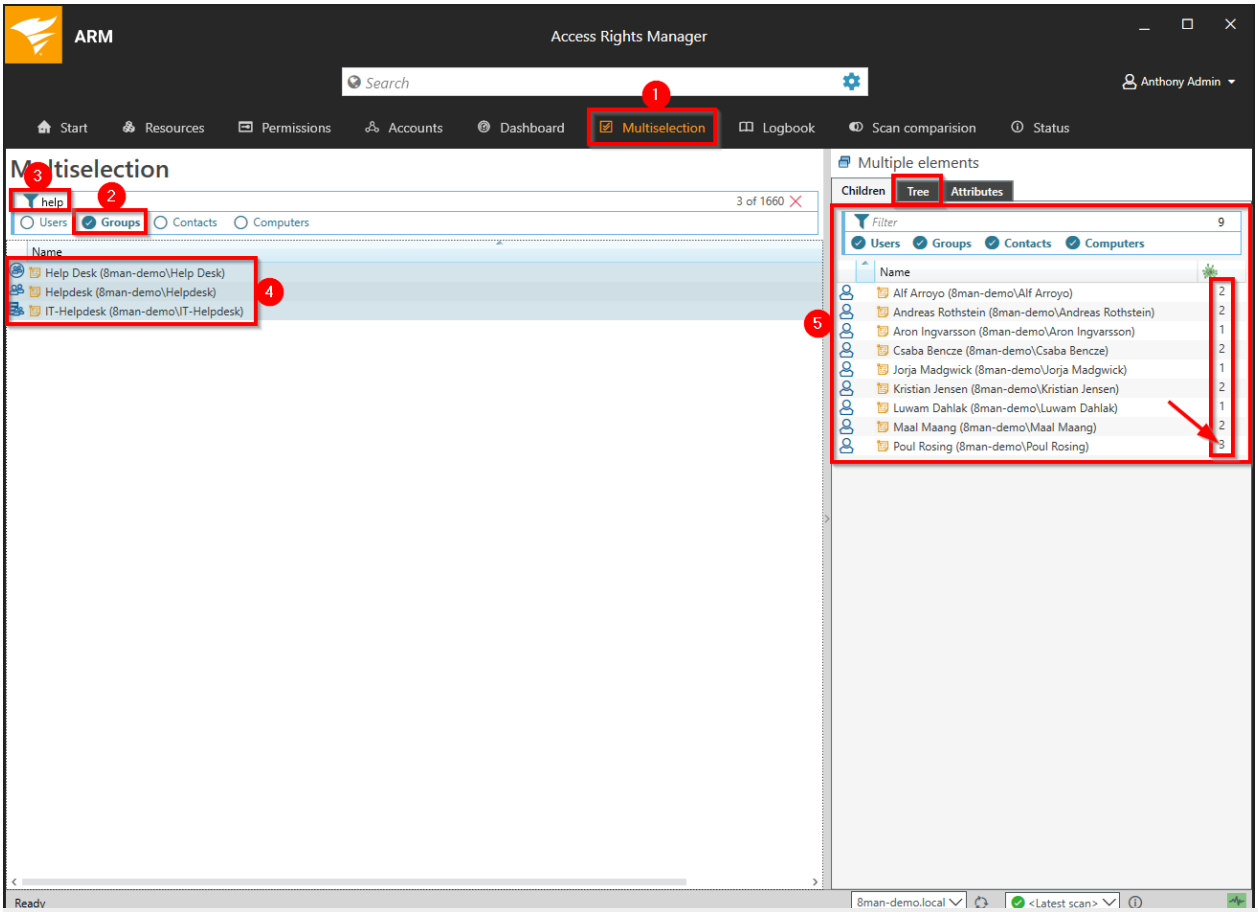
Background/Value

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).

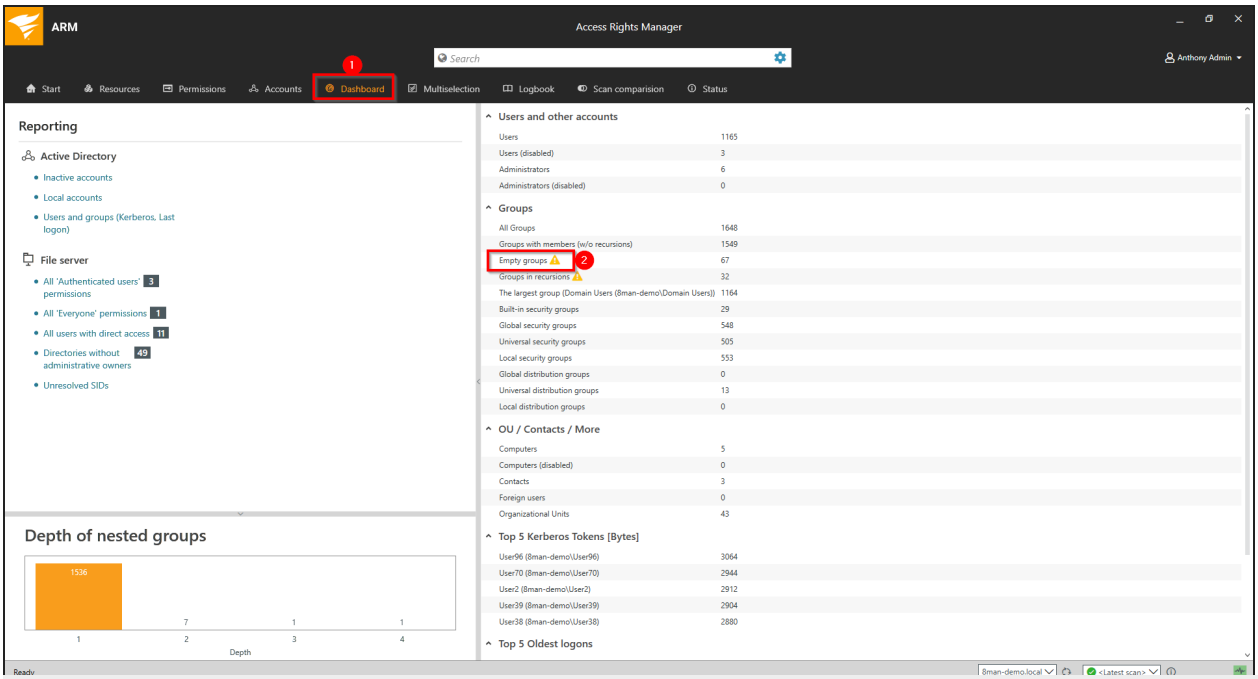
Identify empty groups

Background/Value

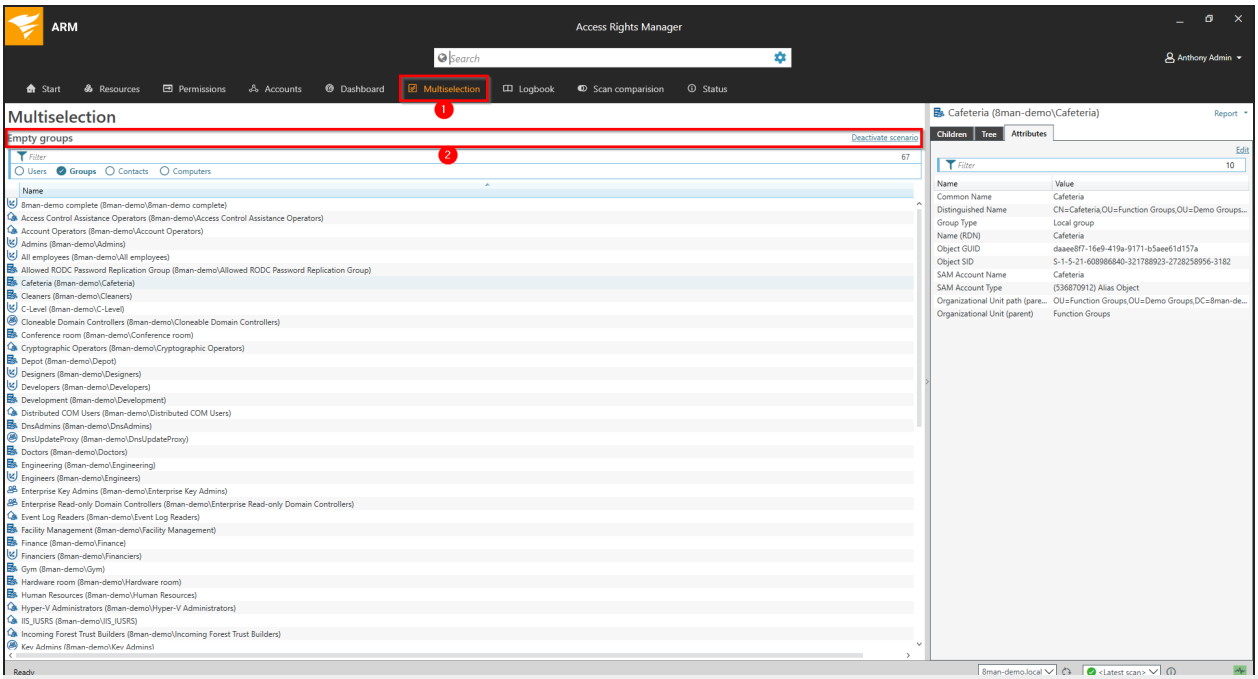
Over time empty groups often accumulate in an AD structure. These empty groups reduce performance and diminish transparency. We recommend deleting these groups.

⚠ Groups without members can be system groups. You should not delete them.

Step-by-step process



1. Select the Dashboard.
2. Double-click "Empty 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.

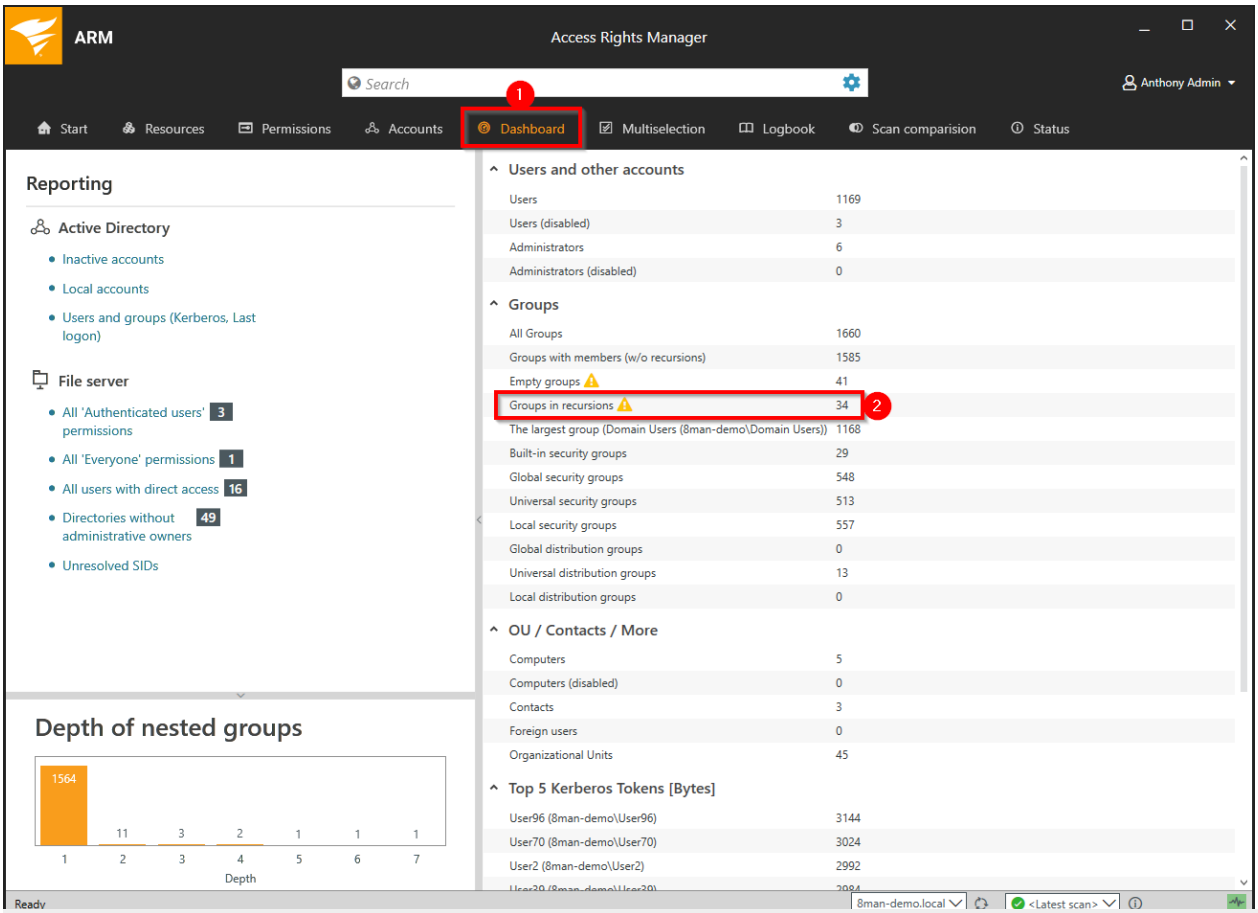
Related features

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.

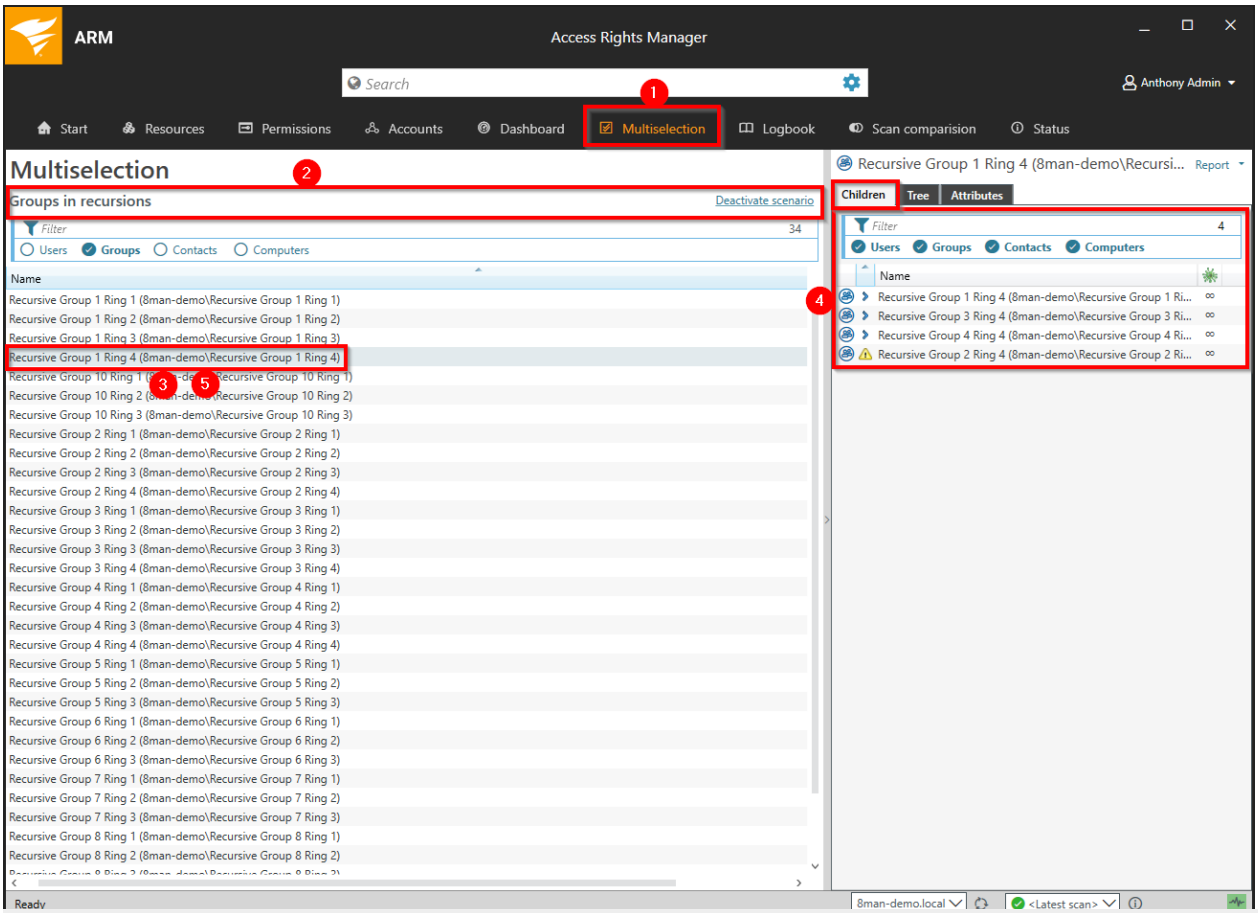
Identify groups in recursion (web client)

Break the circle by managing group memberships (rich client) or removing group memberships (web client).

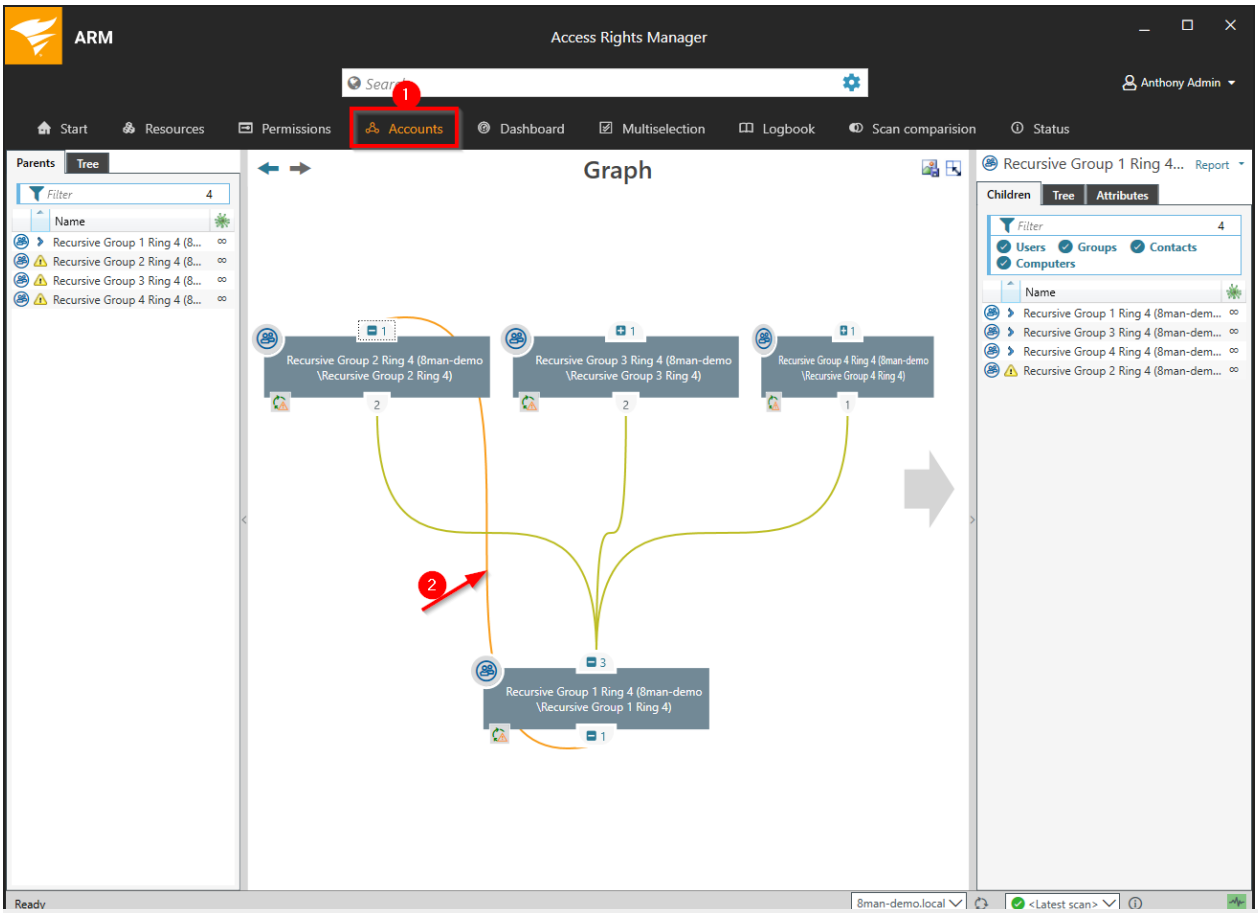
Step-by-step process



1. Select the dashboard.
2. Double-click on "groups in recursions".



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.



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.

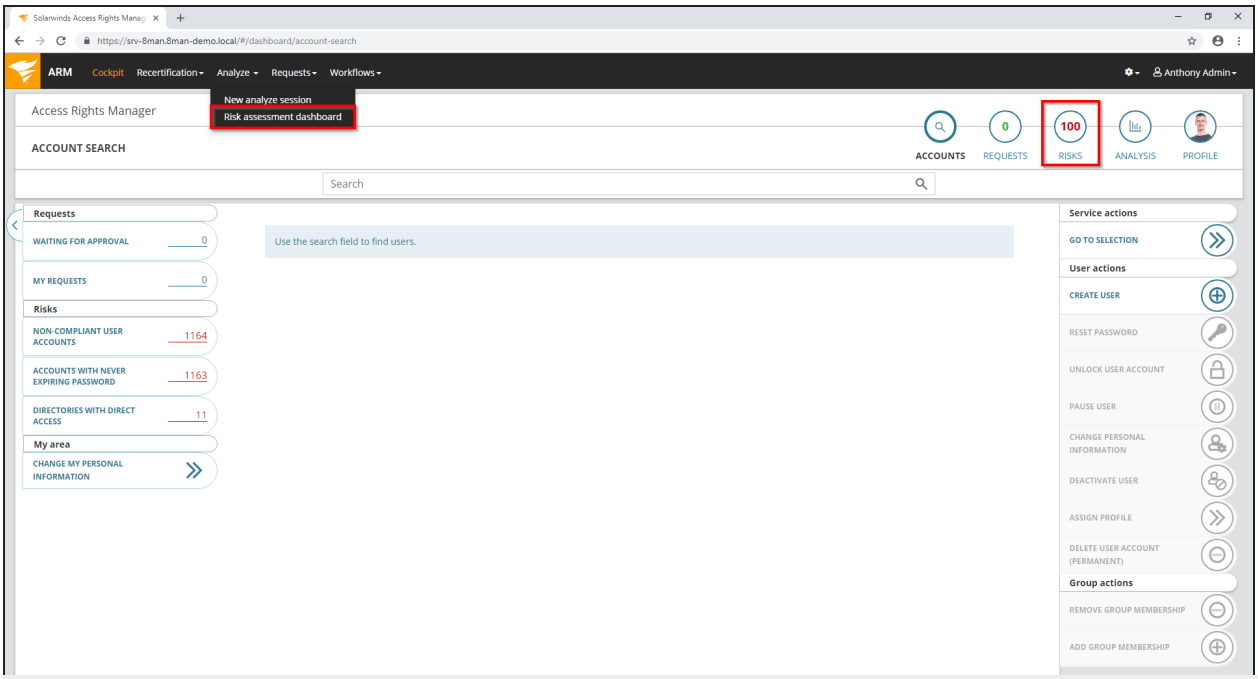
Related features

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.

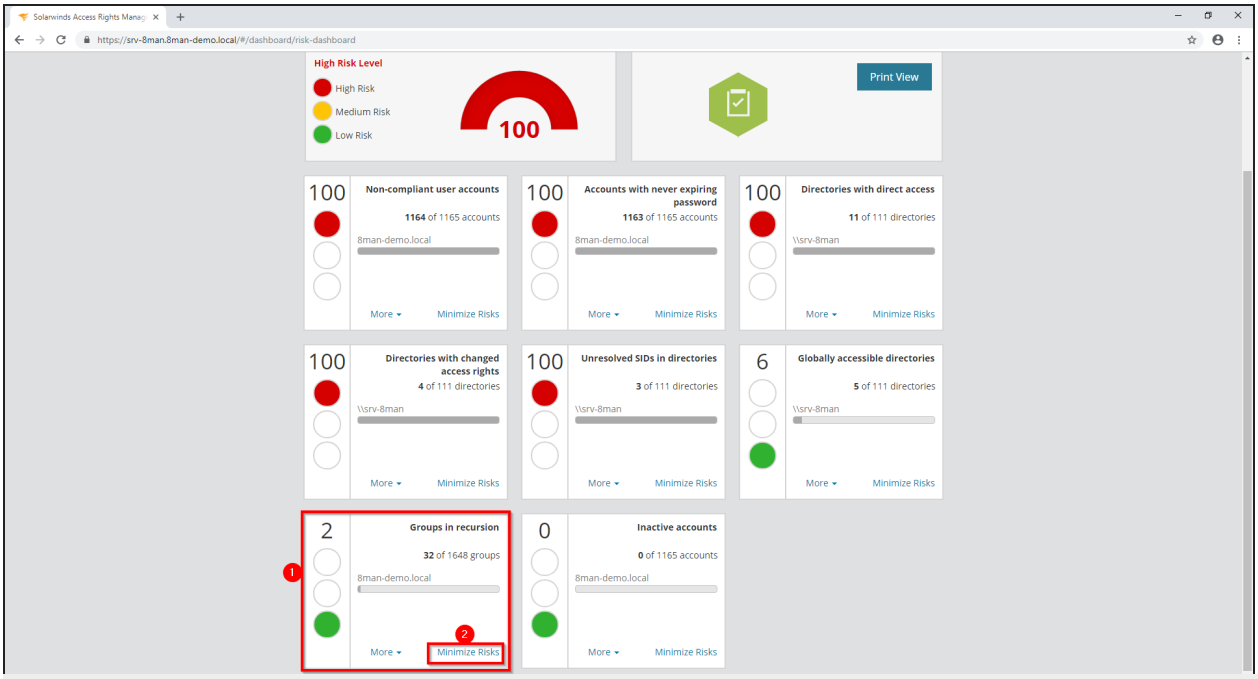
Identify recursive groups (rich client)

Break the circle by managing group memberships (rich client) or removing group memberships (web client).

Step-by-step process

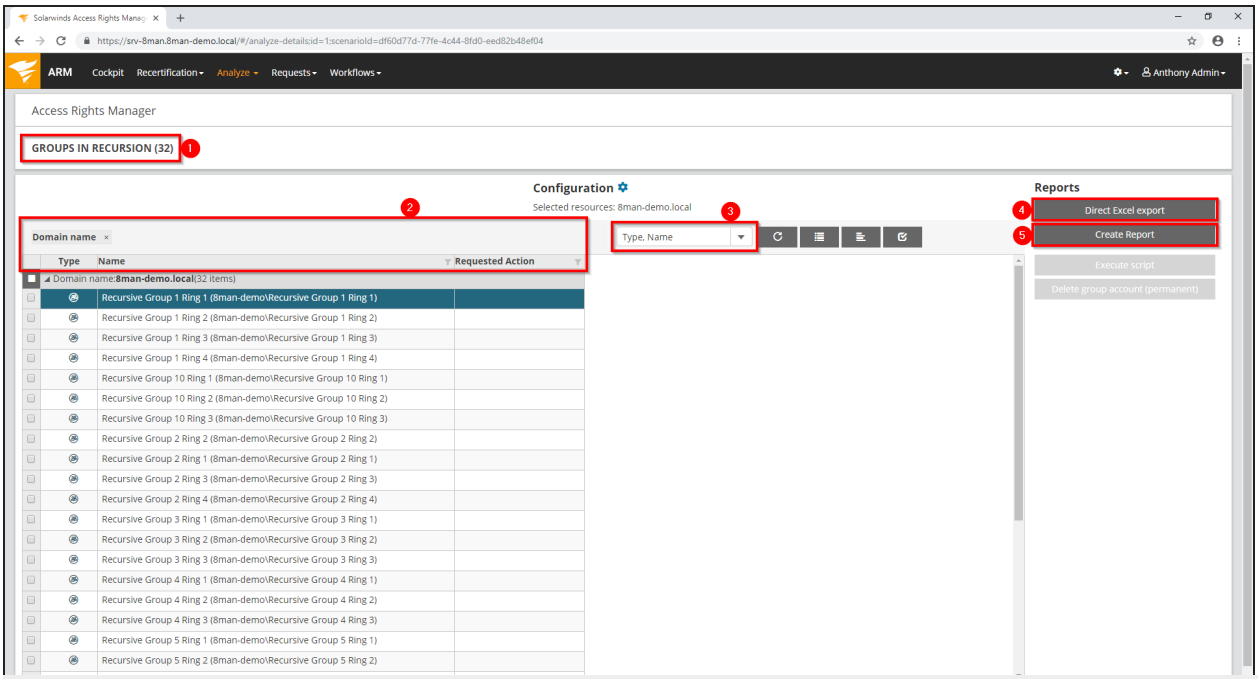


Go to the Risk Assessment Dashboard.



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.



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" an "Groups".

Related features

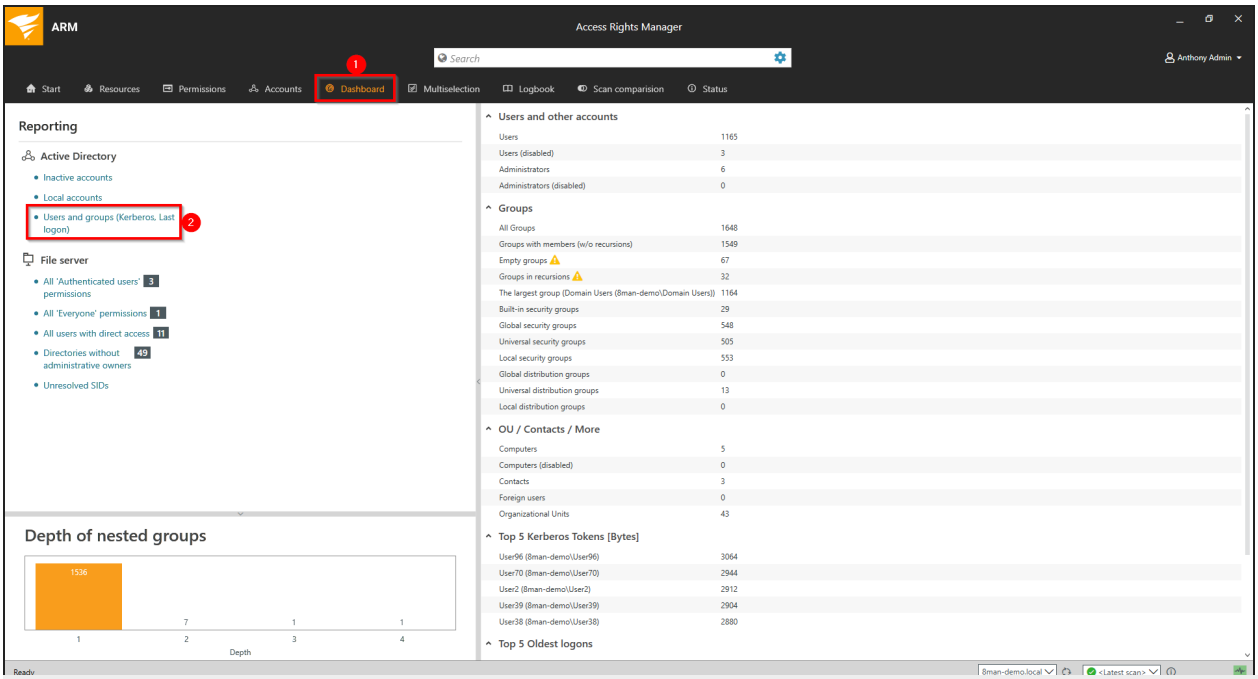
Reset passwords

Change password options

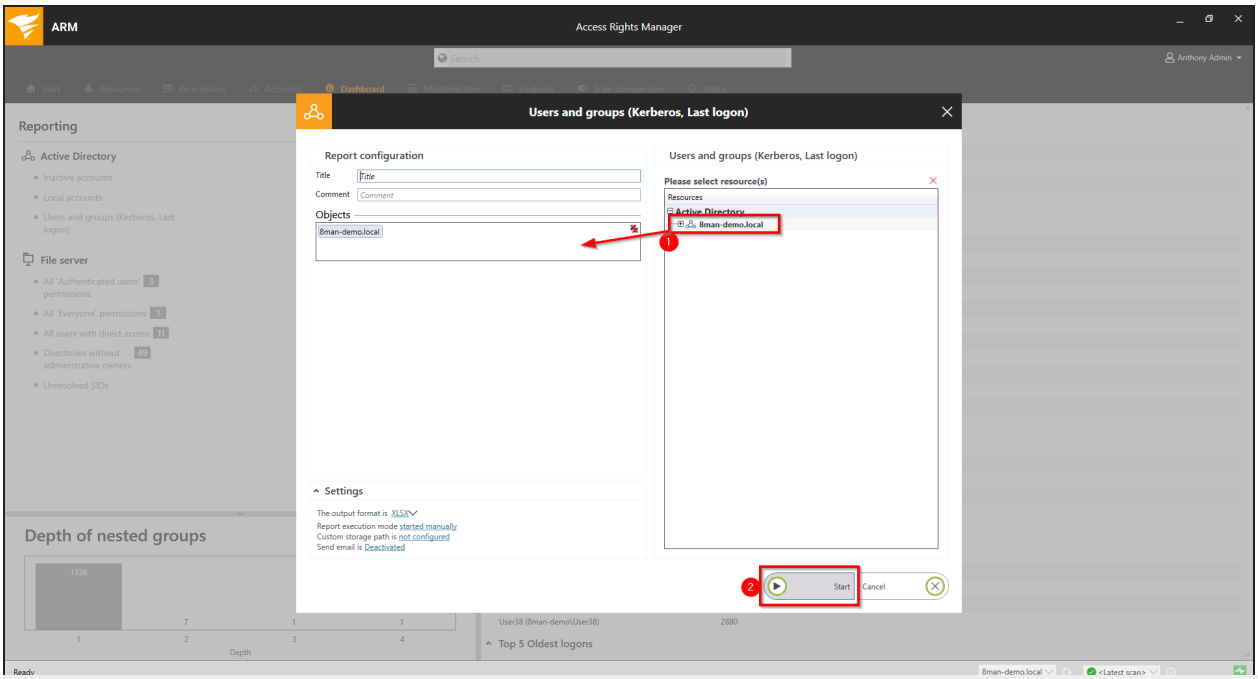
Identify users with never expiring password (web client)

Change password options in bulk (web client)

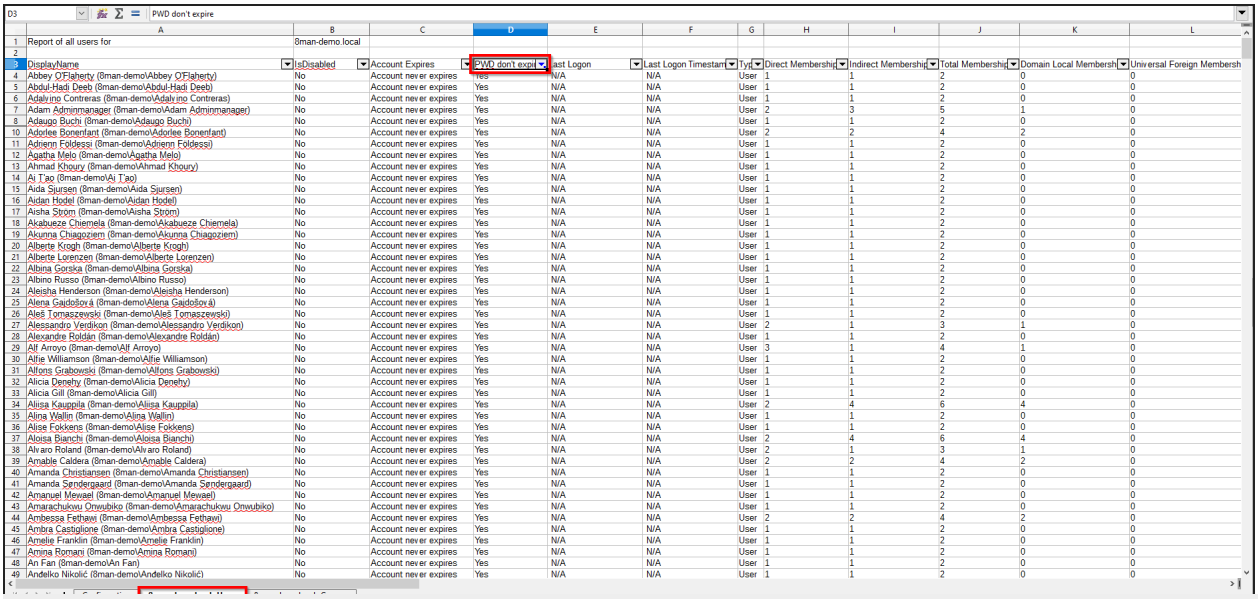
Step-by-step process



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.



	A	B	C	D	E	F	G	H	I	J	K	L
1	Report of all users for	8man-demo.local										
2												
3	DisplayName	IsDisabled	Account Expires	PWD don't expi	Last Logon	Last Logon Timestam	Typ	Direct Membershi	Indirect Membershi	Total Membershi	Domain Local Membersh	Universal Foreign Membersh
4	Abbey O'Flaherty (8man-demo\Abbey O'Flaherty)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
5	Abdul-Hadi Deeb (8man-demo\Abdul-Hadi Deeb)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
6	Adalvino Contreras (8man-demo\Adalvino Contreras)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
7	Adam Admin manager (8man-demo\Adam Admin manager)	No	Account never expires	Yes	N/A	N/A	User	2	3	5	1	0
8	Adaugo Buchi (8man-demo\Adaugo Buchi)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
9	Adorlee Bonenfant (8man-demo\Adorlee Bonenfant)	No	Account never expires	Yes	N/A	N/A	User	2	2	4	2	0
10	Adrienn Földessi (8man-demo\Adrienn Földessi)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
11	Agatha Melo (8man-demo\Agatha Melo)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
12	Ahmad Khoury (8man-demo\Ahmad Khoury)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
13	Ai Tạo (8man-demo\Ai Tạo)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
14	Aida Sjursen (8man-demo\Aida Sjursen)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
15	Aidan Hodel (8man-demo\Aidan Hodel)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
16	Aisha Ström (8man-demo\Aisha Ström)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
17	Akabueze Chiemela (8man-demo\Akabueze Chiemela)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
18	Akunna Chiagoziem (8man-demo\Akunna Chiagoziem)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
19	Alberte Krogh (8man-demo\Alberte Krogh)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
20	Alberte Lorenzen (8man-demo\Alberte Lorenzen)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
21	Albina Gorska (8man-demo\Albina Gorska)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
22	Albino Russo (8man-demo\Albino Russo)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
23	Aleisha Henderson (8man-demo\Aleisha Henderson)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
24	Alena Gajdošová (8man-demo\Alena Gajdošová)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
25	Aleš Tomaszewski (8man-demo\Aleš Tomaszewski)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
26	Alessandro Verdikon (8man-demo\Alessandro Verdikon)	No	Account never expires	Yes	N/A	N/A	User	2	1	3	1	0
27	Alexandre Roldán (8man-demo\Alexandre Roldán)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
28	Alf Arroyo (8man-demo\Alf Arroyo)	No	Account never expires	Yes	N/A	N/A	User	3	1	4	1	0
29	Alfie Williamson (8man-demo\Alfie Williamson)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
30	Alfons Grabowski (8man-demo\Alfons Grabowski)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
31	Alicia Denehy (8man-demo\Alicia Denehy)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
32	Alicia Gill (8man-demo\Alicia Gill)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
33	Alissa Kauppila (8man-demo\Alissa Kauppila)	No	Account never expires	Yes	N/A	N/A	User	2	4	6	4	0
34	Alina Wallin (8man-demo\Alina Wallin)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
35	Alise Fokkens (8man-demo\Alise Fokkens)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
36	Aloisa Bianchi (8man-demo\Aloisa Bianchi)	No	Account never expires	Yes	N/A	N/A	User	2	4	6	4	0
37	Alvaro Roland (8man-demo\Alvaro Roland)	No	Account never expires	Yes	N/A	N/A	User	2	1	3	1	0
38	Amable Caldera (8man-demo\Amable Caldera)	No	Account never expires	Yes	N/A	N/A	User	2	2	4	2	0
39	Amanda Christiansen (8man-demo\Amanda Christiansen)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
40	Amanda Søndergaard (8man-demo\Amanda Søndergaard)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
41	Amanuel Mewael (8man-demo\Amanuel Mewael)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
42	Amarachukwu Onwubiko (8man-demo\Amarachukwu Onwubiko)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
43	Ambessa Fethawi (8man-demo\Ambessa Fethawi)	No	Account never expires	Yes	N/A	N/A	User	2	2	4	2	0
44	Ambra Castiglione (8man-demo\Ambra Castiglione)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
45	Amelie Franklin (8man-demo\Amelie Franklin)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
46	Amina Romani (8man-demo\Amina Romani)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
47	An Fan (8man-demo\An Fan)	No	Account never expires	Yes	N/A	N/A	User	1	1	2	0	0
48	Anđelko Nikolić (8man-demo\Anđelko Nikolić)	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

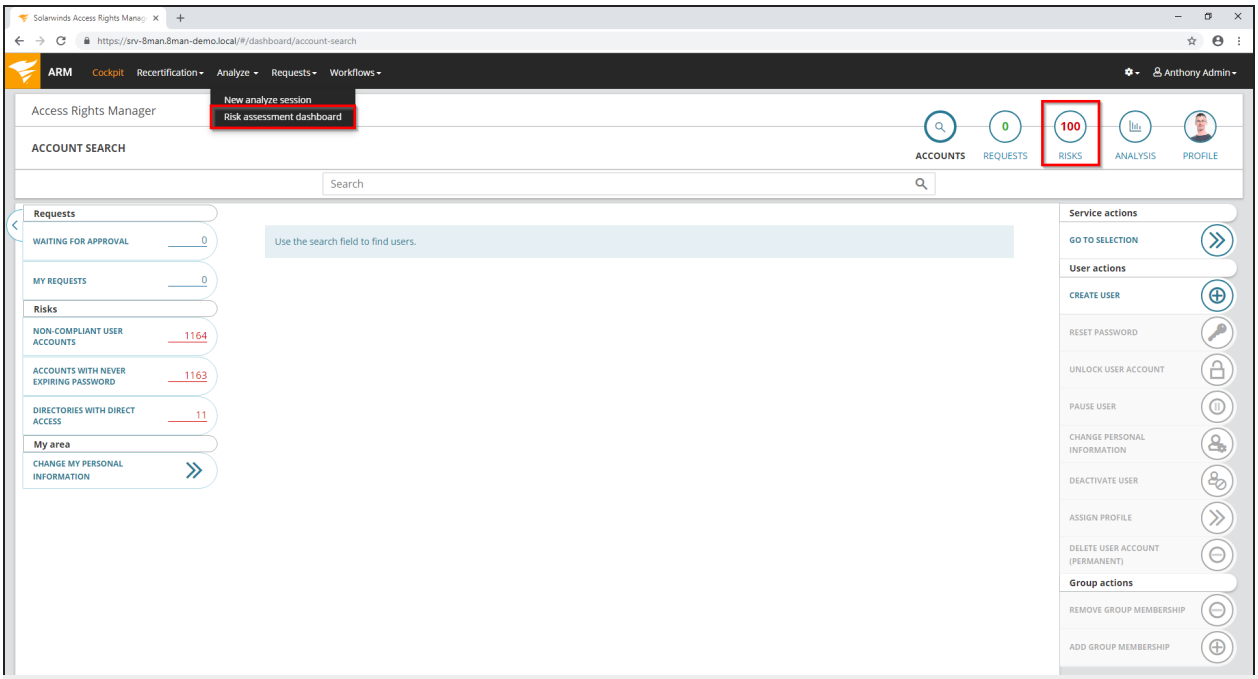
One key security requirement within any organization is that passwords are changed regularly. Use the scenario to find accounts where this requirement has not been activated. View this information in the web interface and create reports.

Related features

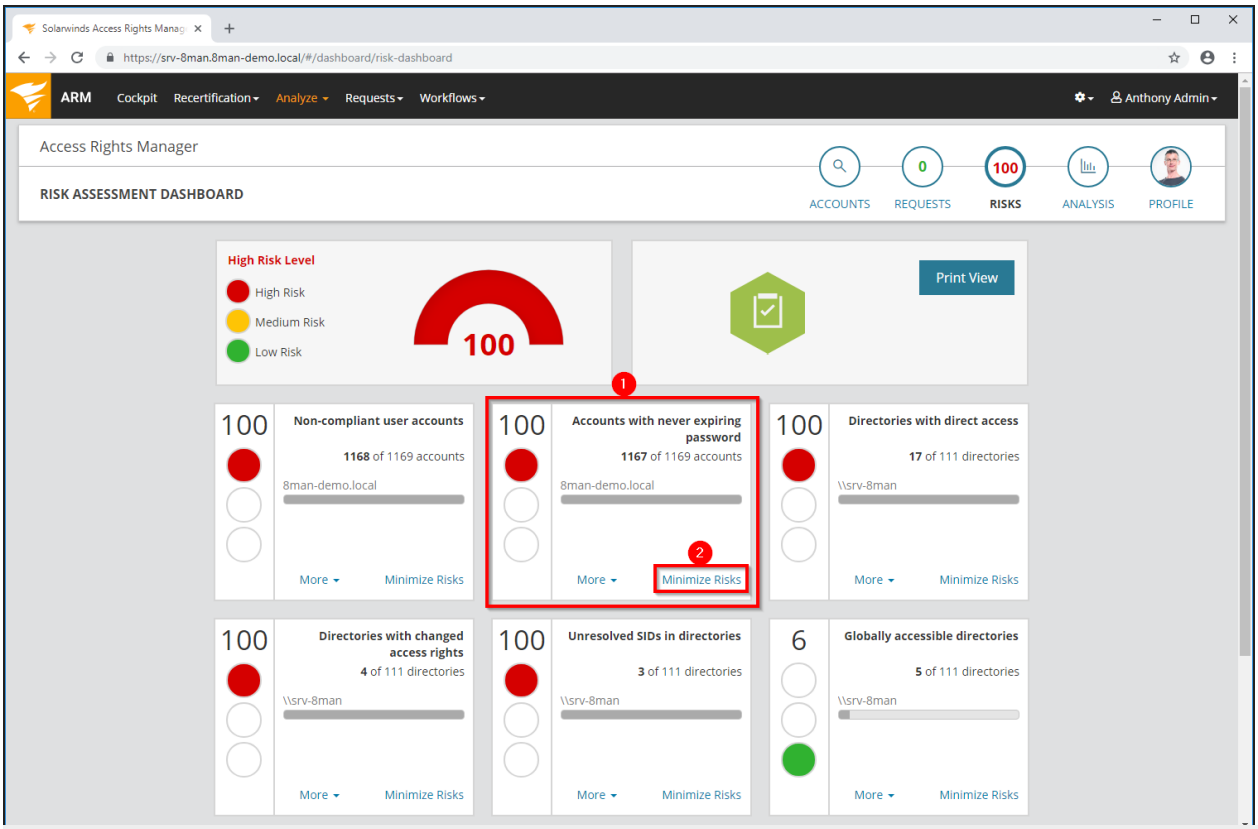
Reset passwords (rich client)

Change password options (rich client)

Step-by-step process

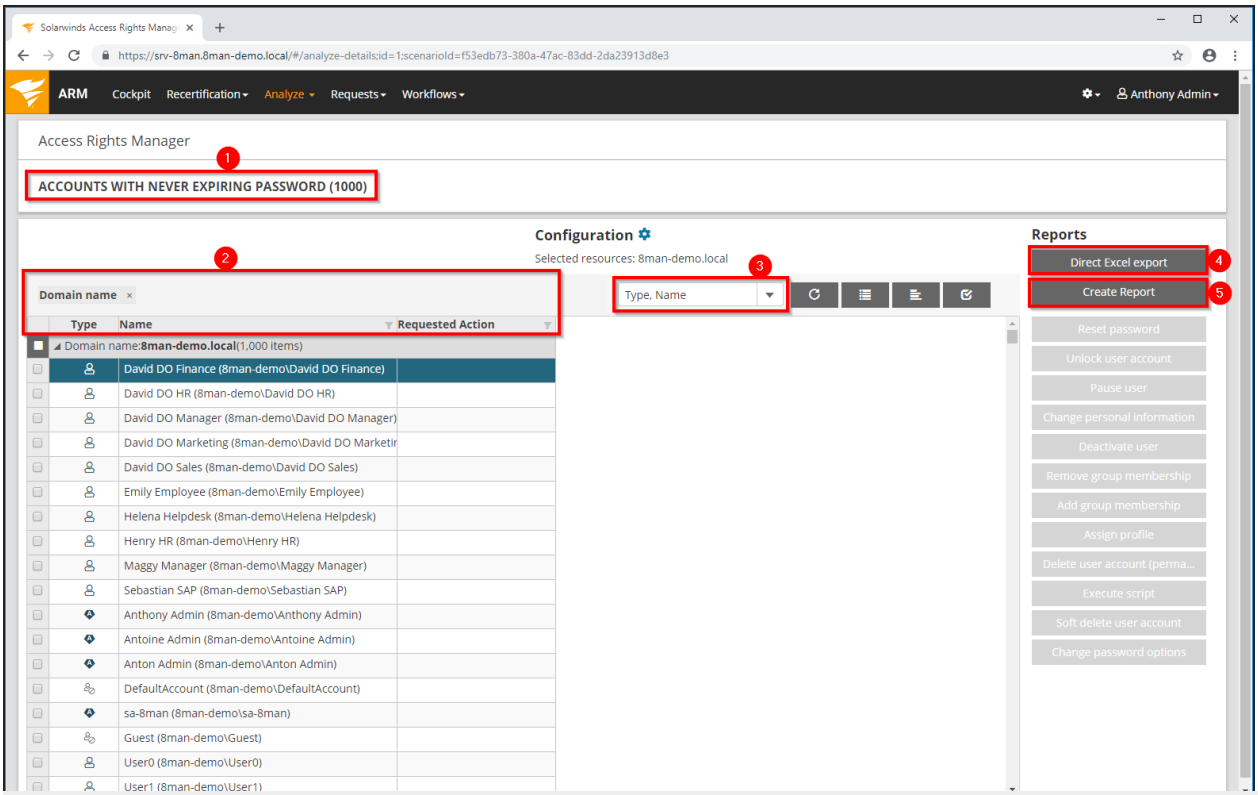


Go to the Risk Assessment Dashboard.



1. ARM shows a rating for the risk factor "Accounts with never expiring password".
2. Click on "Minimize risks".

The tiles are sorted by risk level and may therefore be located in different places.



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

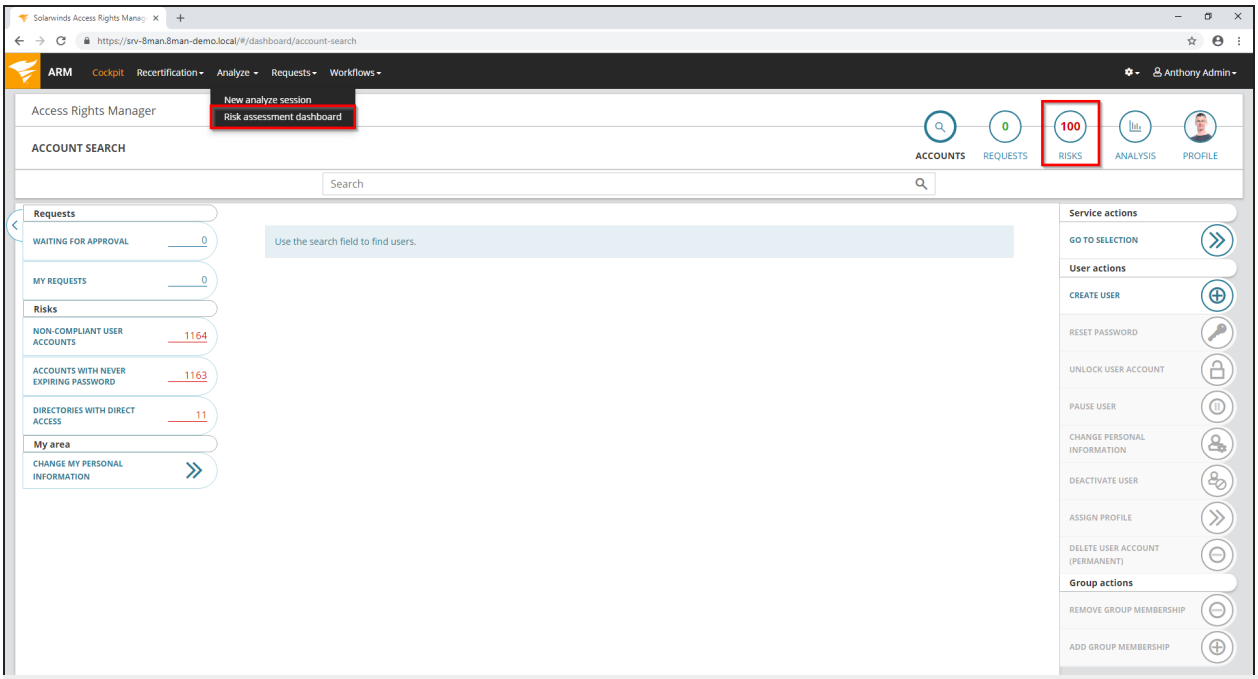
Inactive accounts can be used for data theft and manipulation without being detected. Since most inactive accounts are remnants of past employees, they are often a symptom of a communication problem between HR and IT. ARM displays all inactive accounts in Active Directory with a last logon older than 30 days. Remove or deactivate accounts that are no longer needed.

Related features

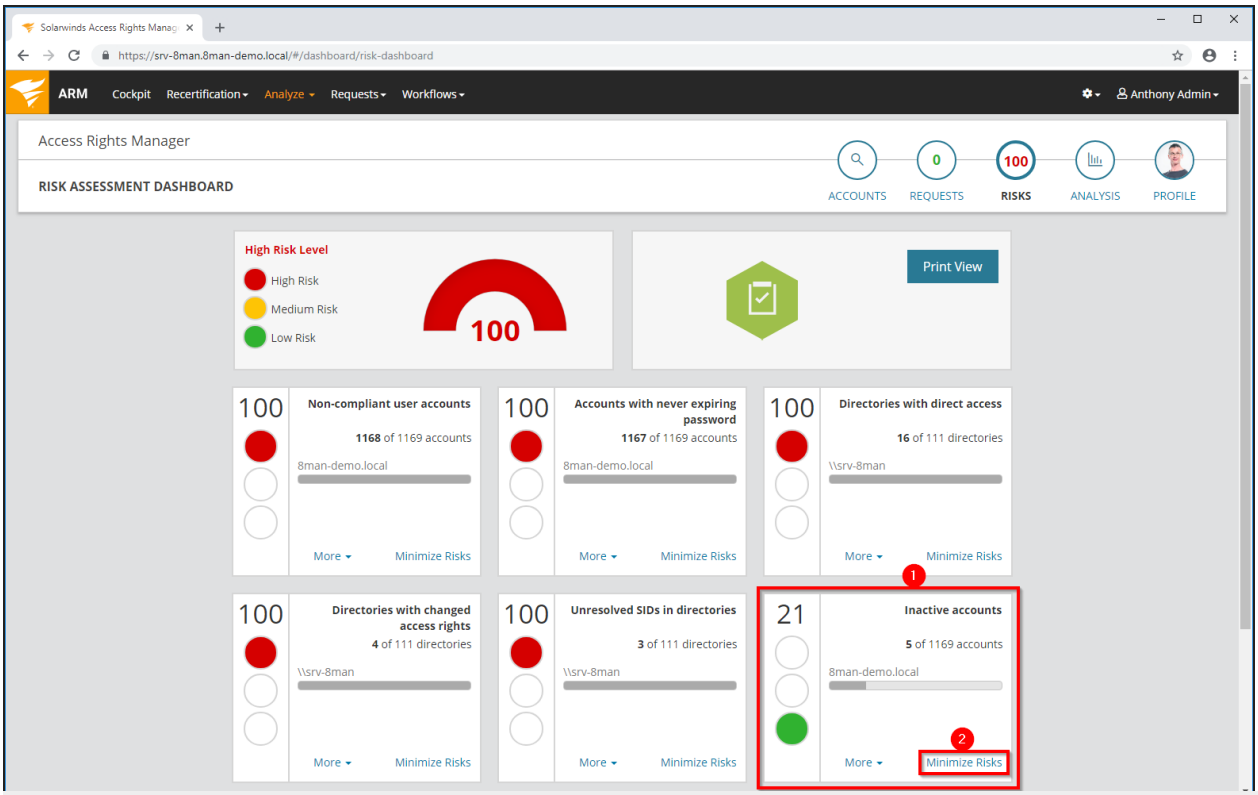
Report: Inactive accounts

Deactivate accounts in bulk (web client)

Step-by-step process

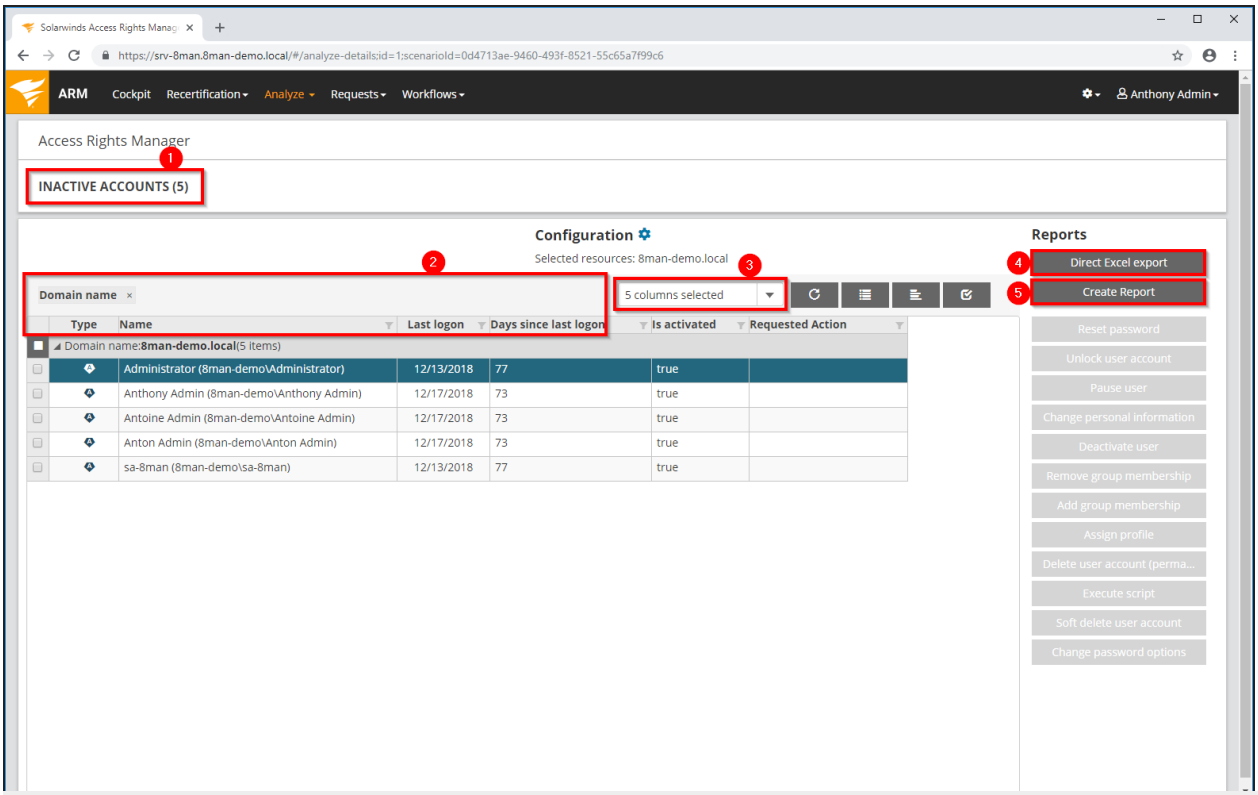


Go to the Risk Assessment Dashboard.



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.



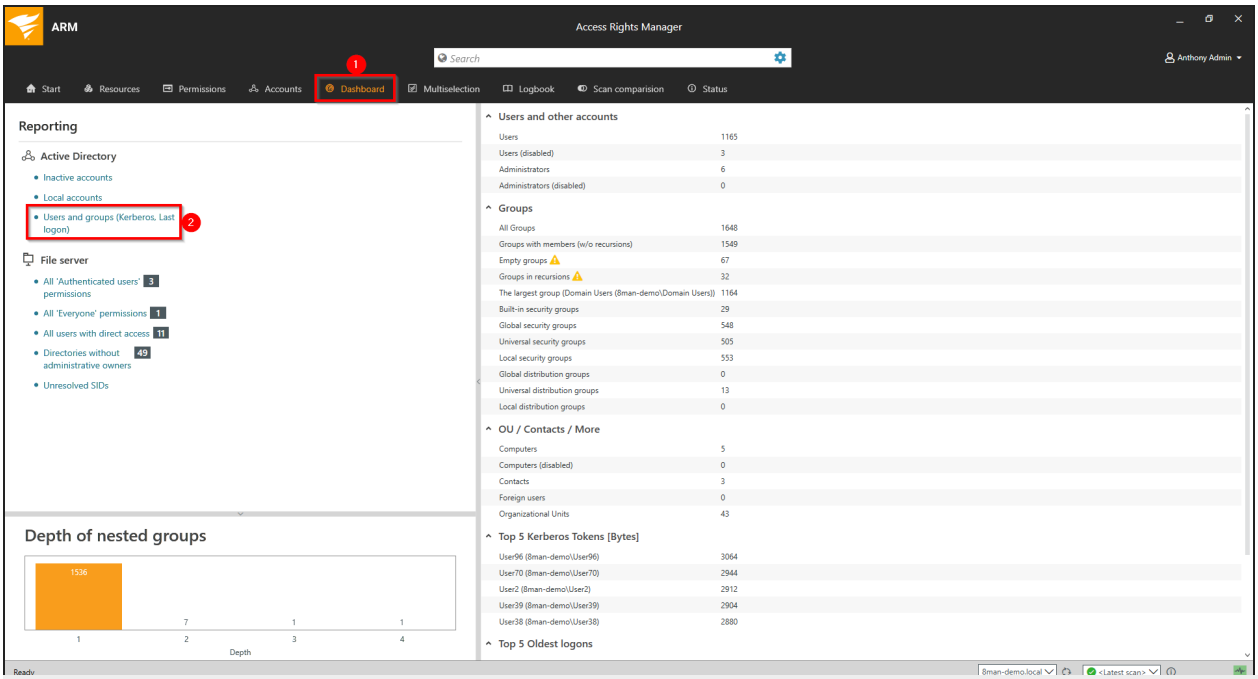
1. ARM lists all inactive accounts.
2. Use sorting, filtering and grouping to analyze the data.
3. Select the rows to display in the grid and in the reports.
4. Export the data into Excel.
5. Create a report in PDF- or CSV-format. Save the report or email it.

Identify expiring user accounts

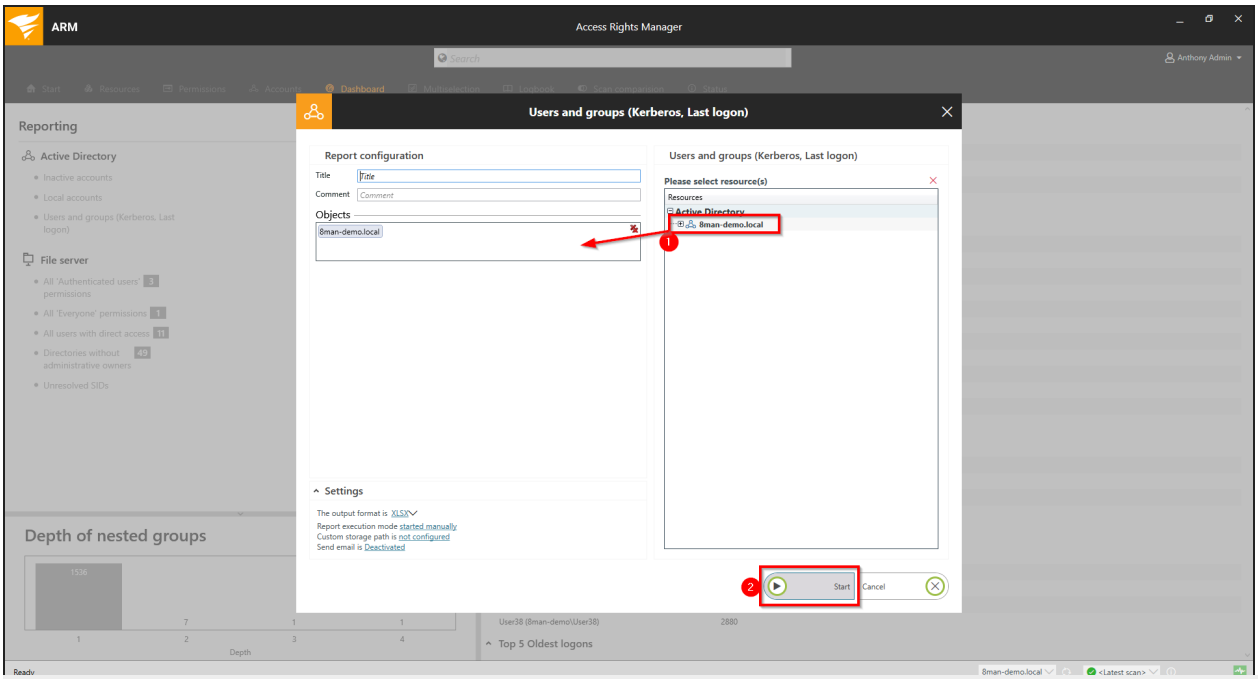
Background / Value

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".

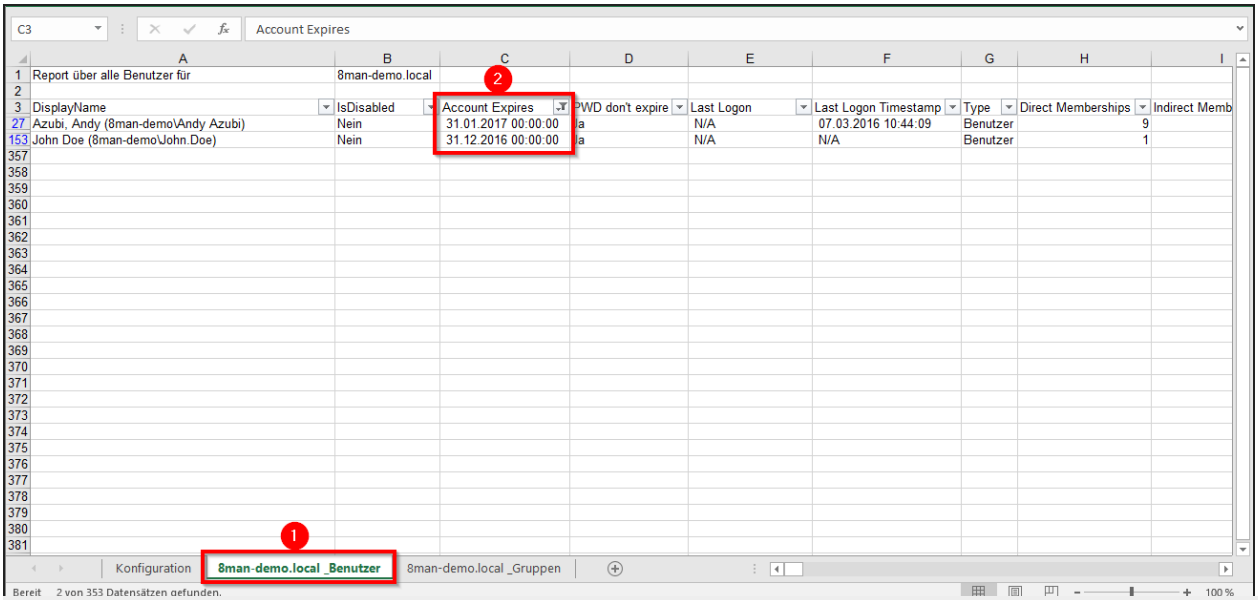
Step-by-step process



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.



Open the report in your spreadsheet application.

1. Select the tab "User".
2. Filter the column "Account expires" by positive entries.

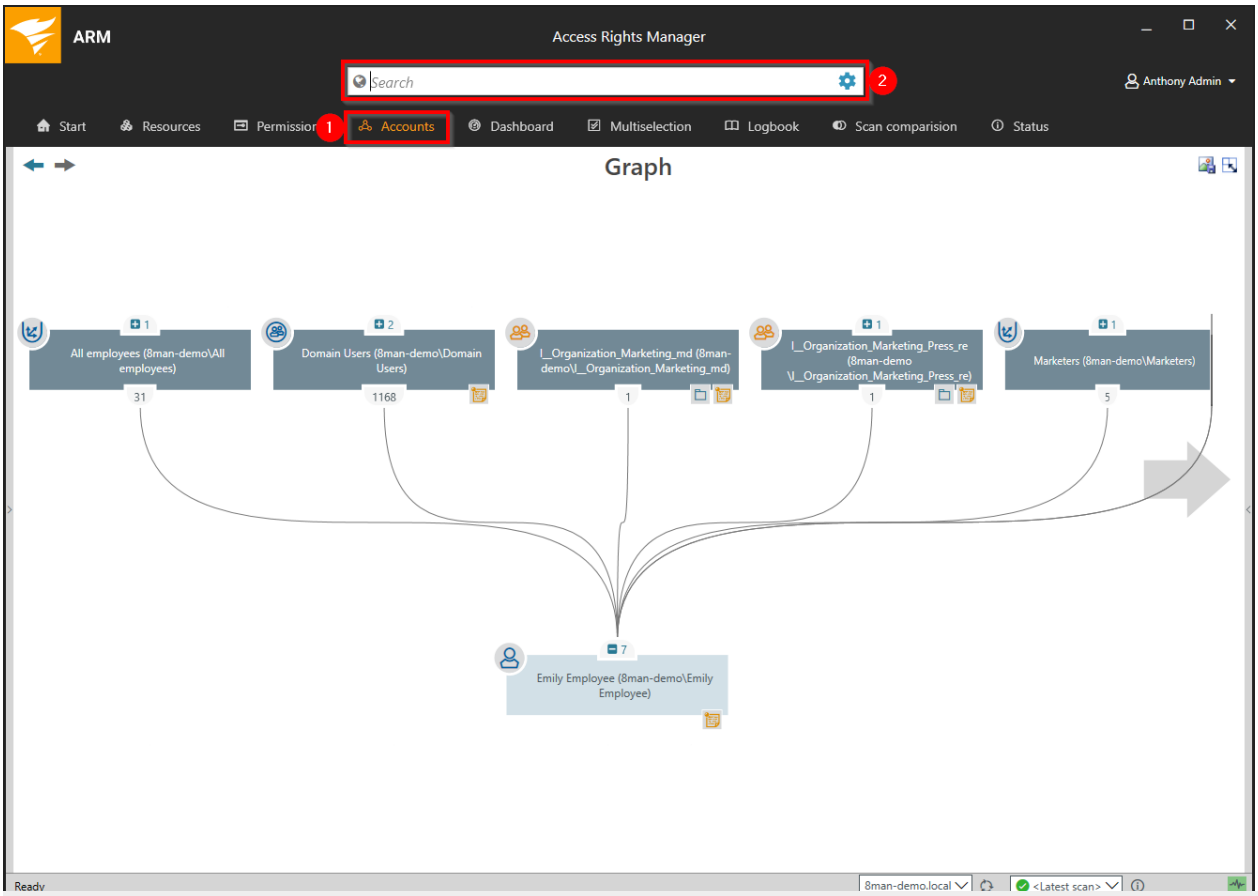
We recommend checking with your HR department if any of these accounts are still needed.

Identify the most recent actions on an account

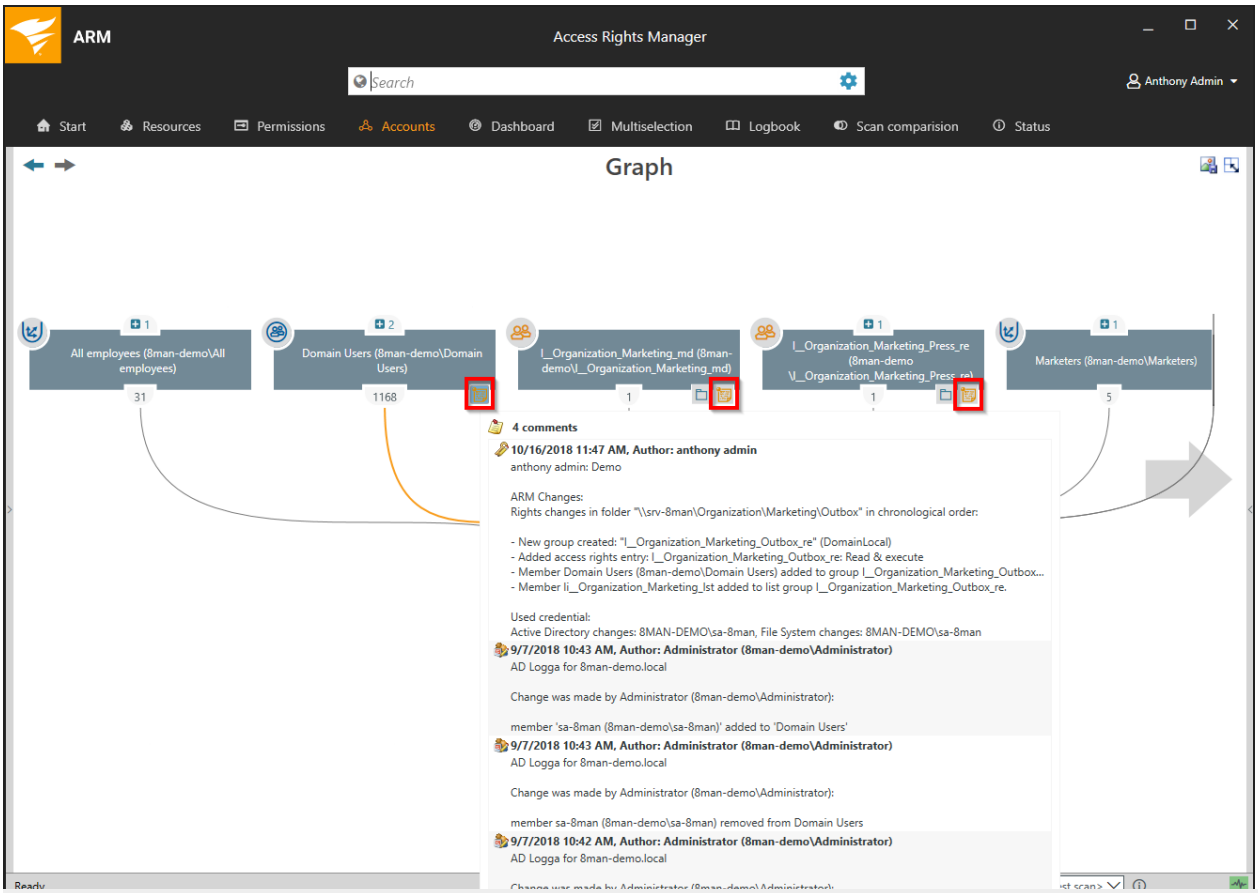
Background / Value

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.

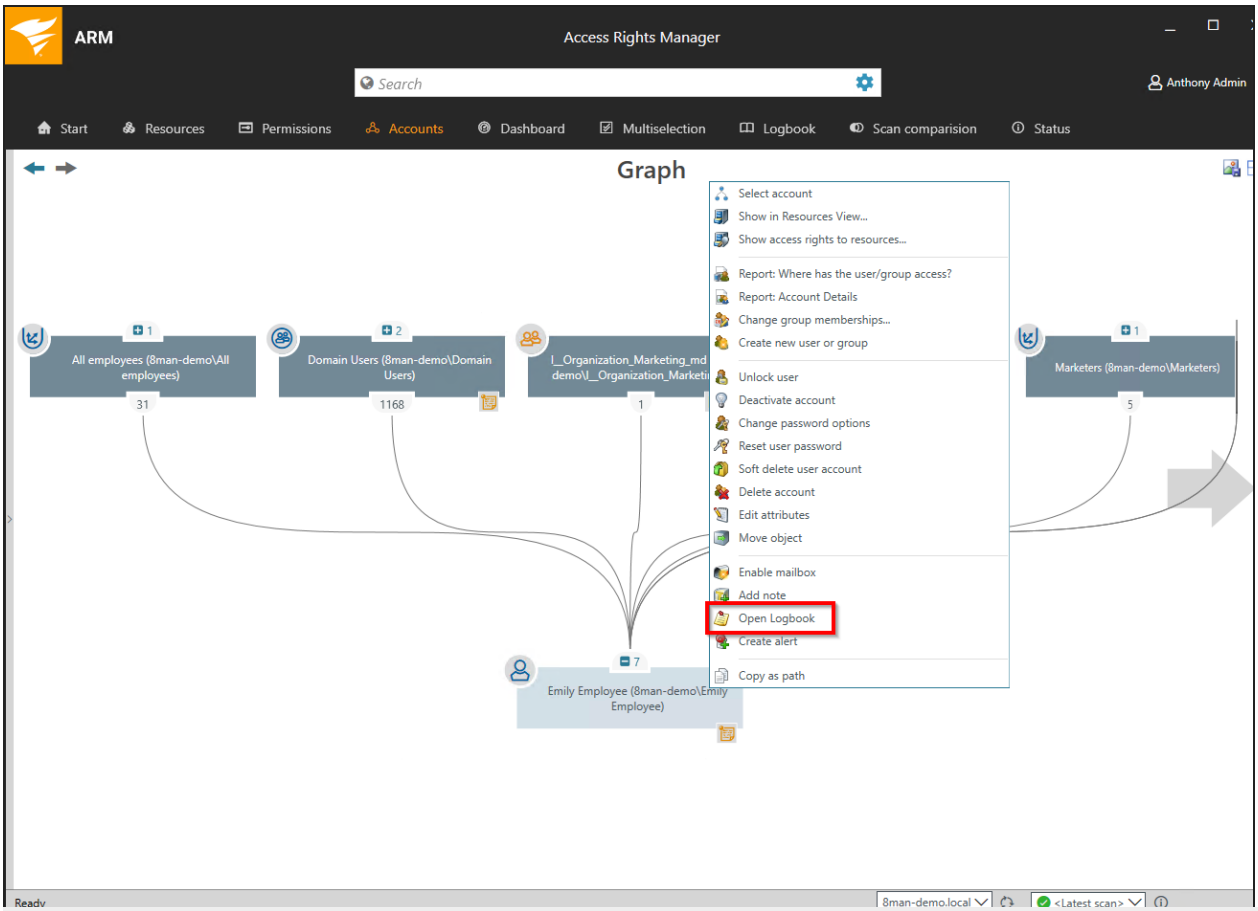
Step-by-step process



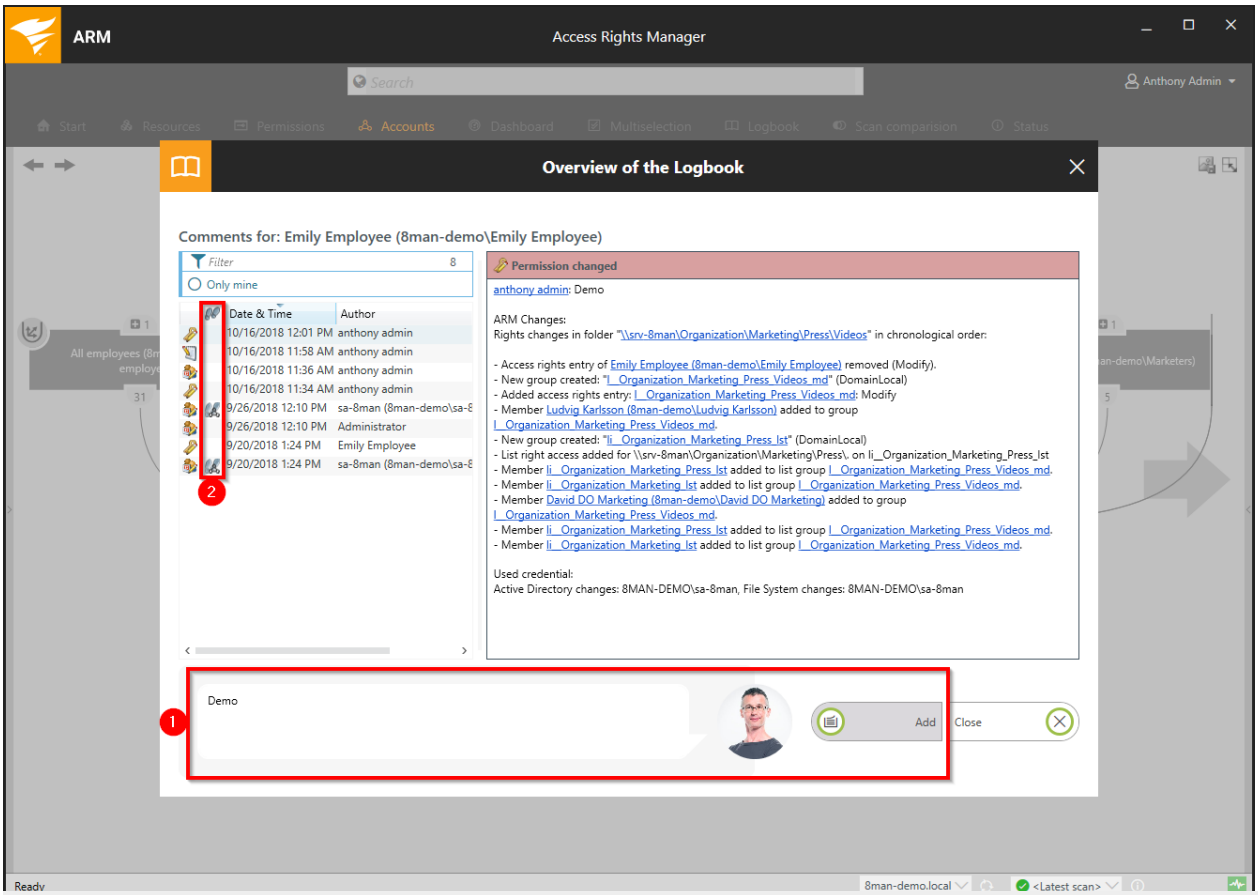
1. Select "Accounts".
2. Search for the desired user or group.



The 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.



Right-click on the desired object and select "Open Logbook" to view all recorded information.



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.

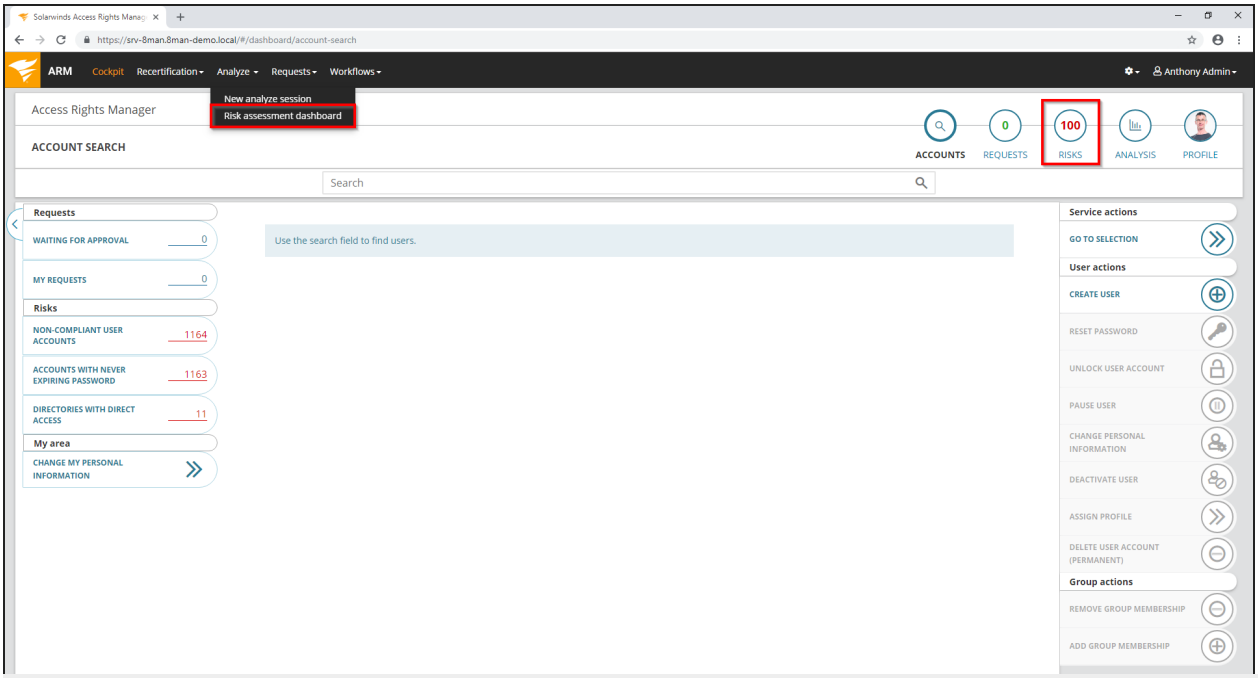
"Everyone accounts" are:

- Everyone
- Authenticated Users
- Domain-Users

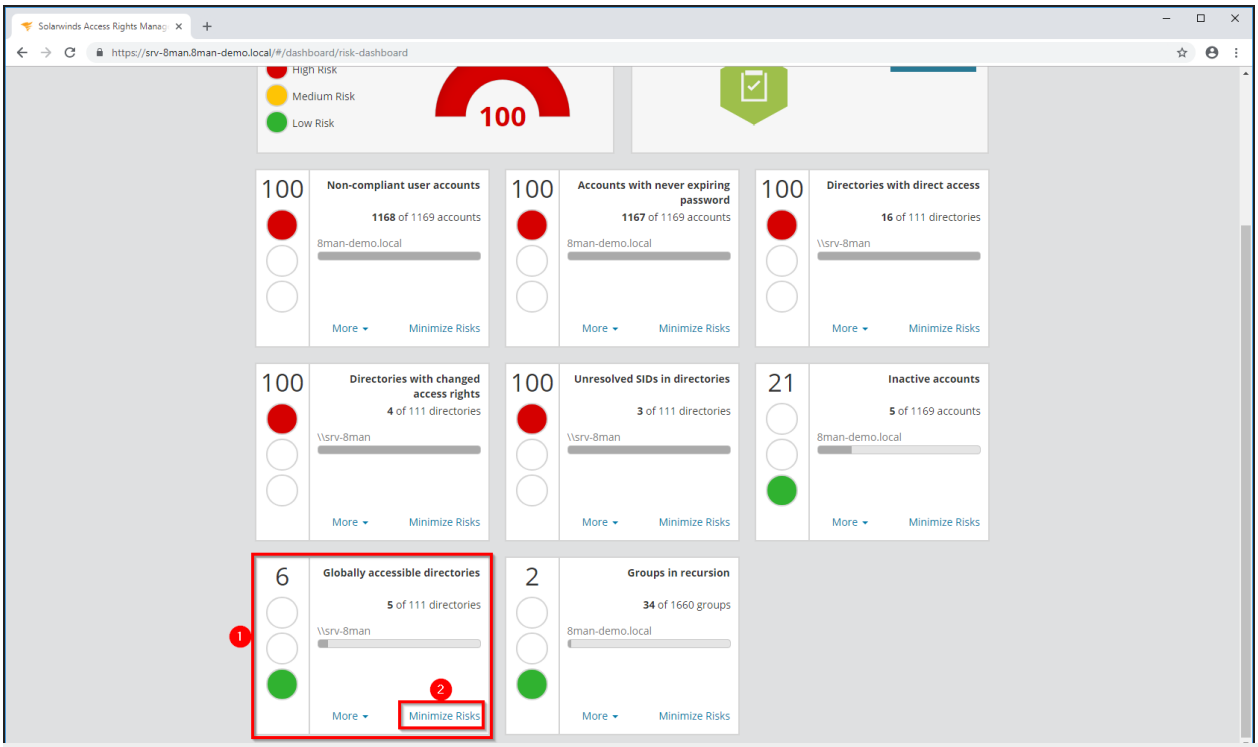
Related features

Remove permissions from globally accessible directories in bulk

Step-by-step process

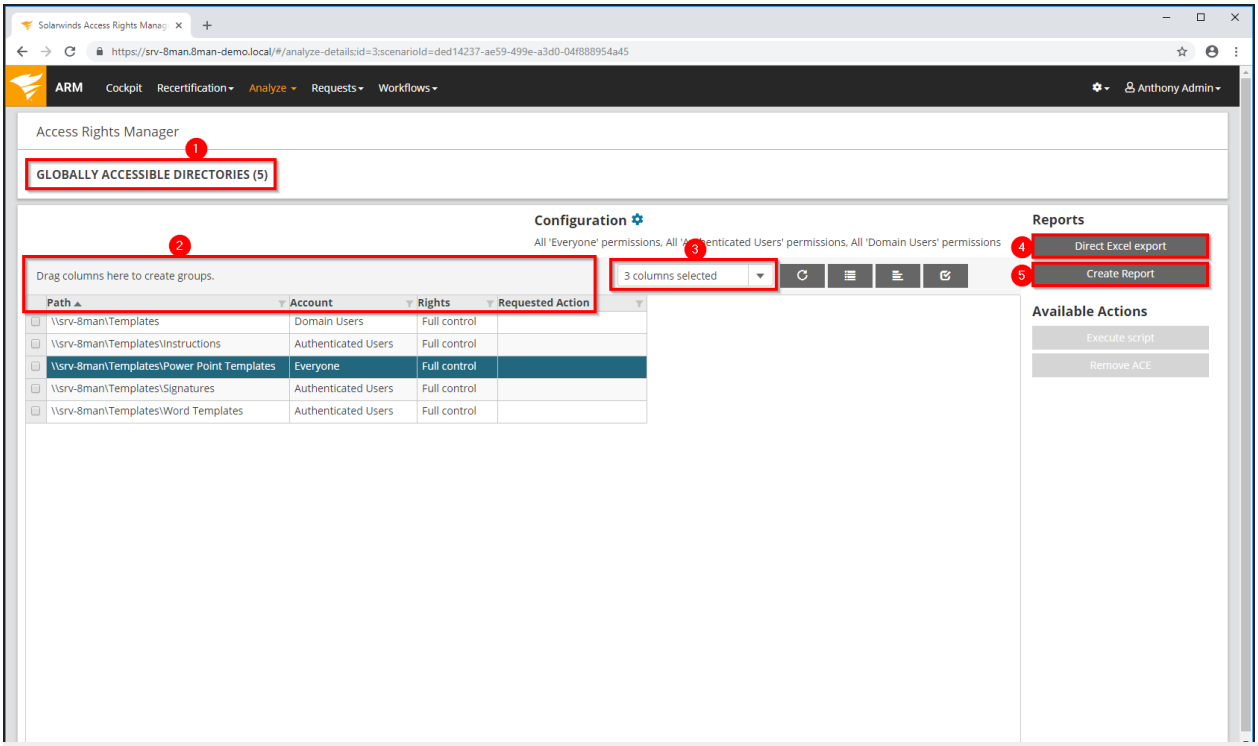


Go to the Risk Assessment Dashboard.



1. ARM shows a rating for the risk factor "Globally accessible directories".
2. Click "Minimize risks".

The tiles are sorted by risk level and may therefore be located in different places.



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

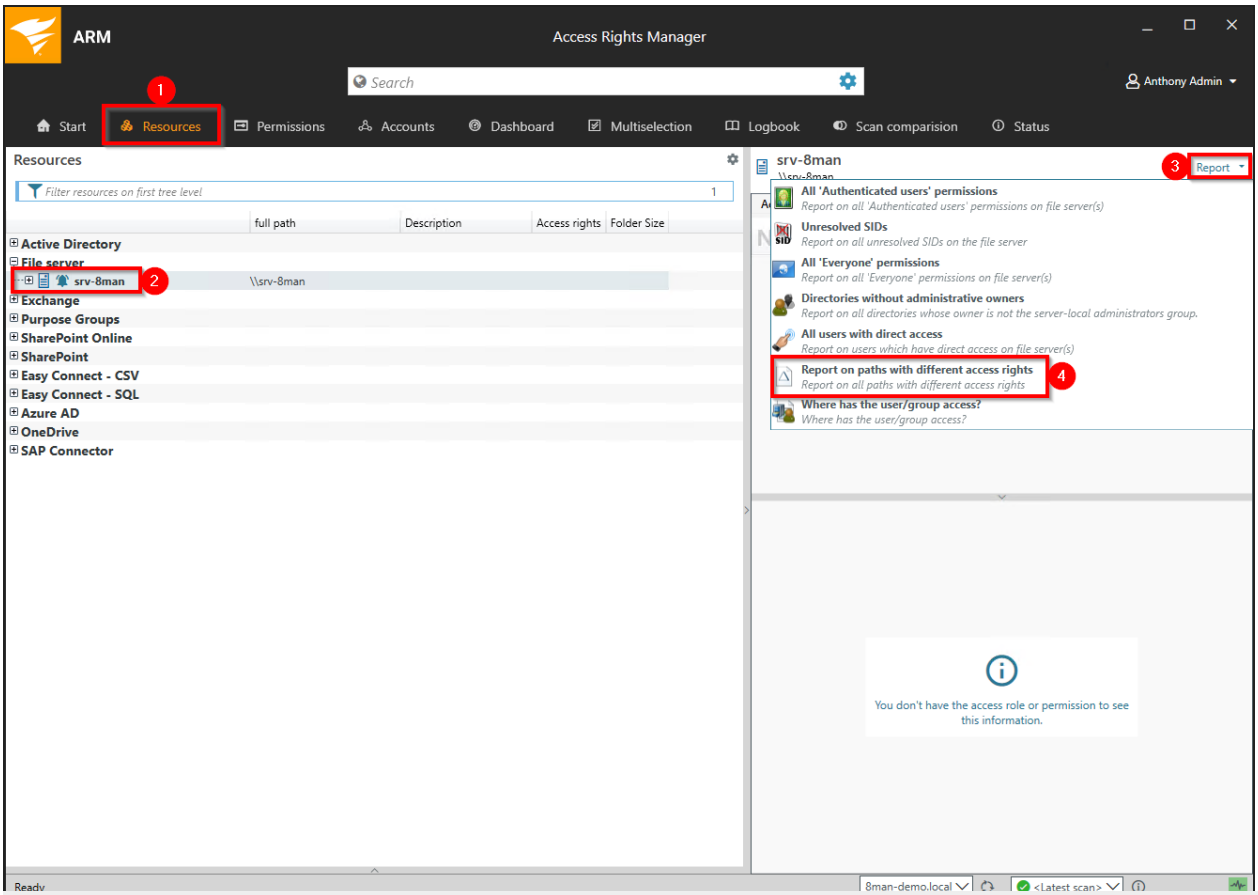
Broken ACLs (Access Control Lists) interfere with the NTFS inheritance on the fileserver. The consequences: The subdirectory does not get the correctly inherited permissions, even though the inheritance is enabled.

ARM shows you broken ACLs in a report.

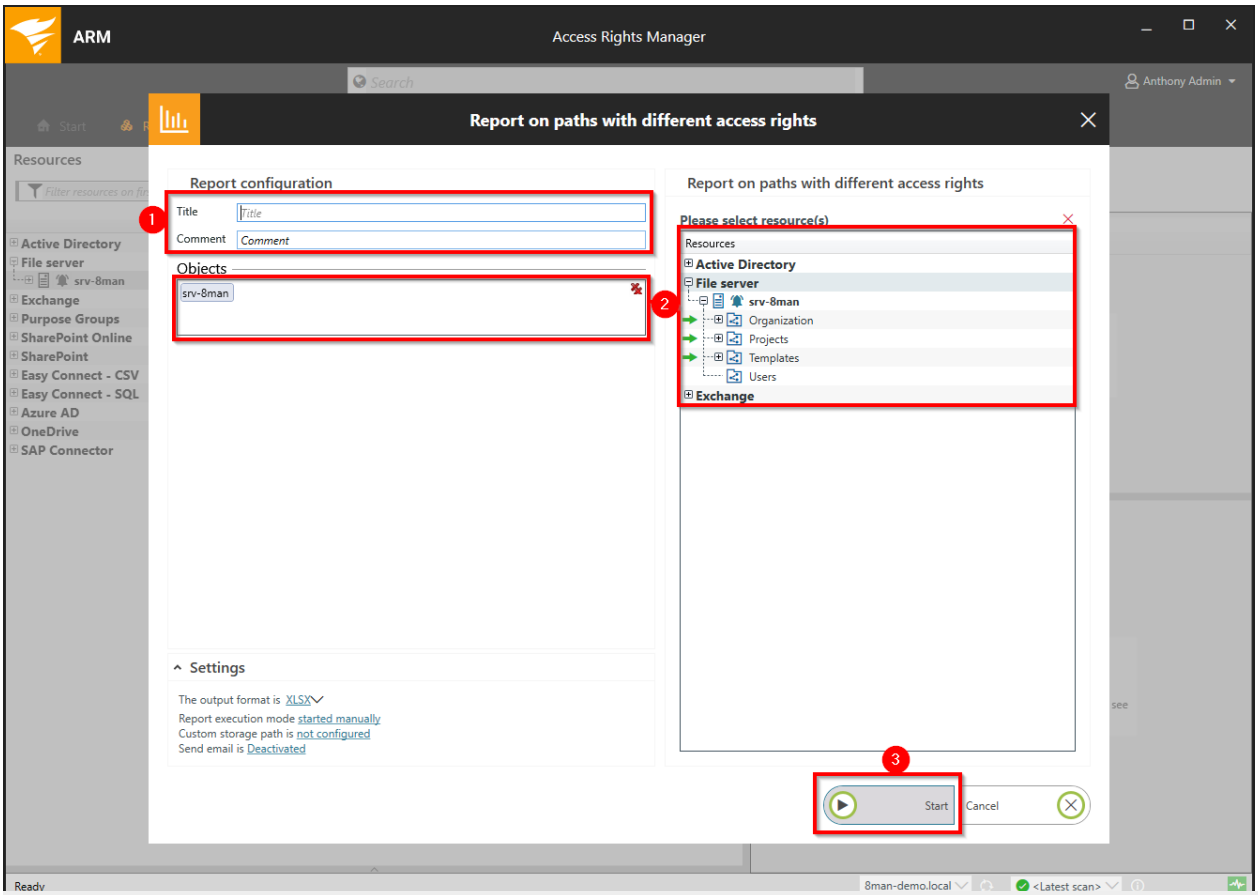
Related features

Remove corrupted inheritance

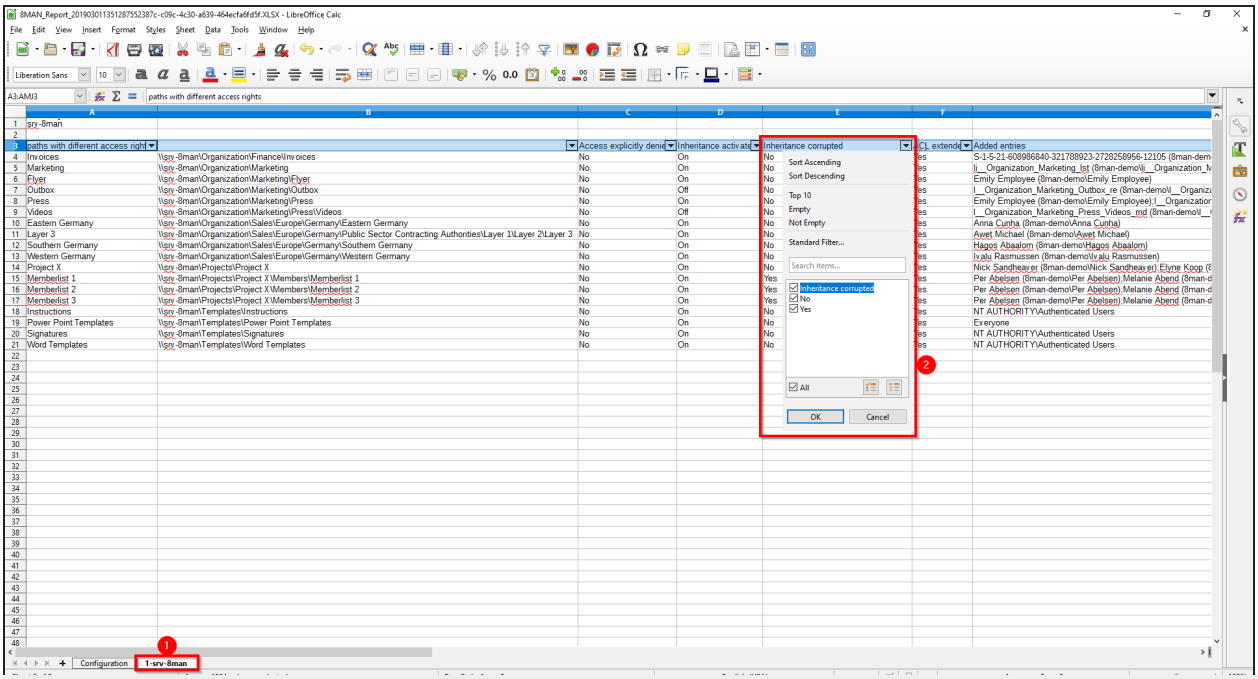
Step-by-step process



1. Select "Resources".
2. Select the desired file server.
3. Click on "Report".
4. Select "report on all sub-directories with different access rights".

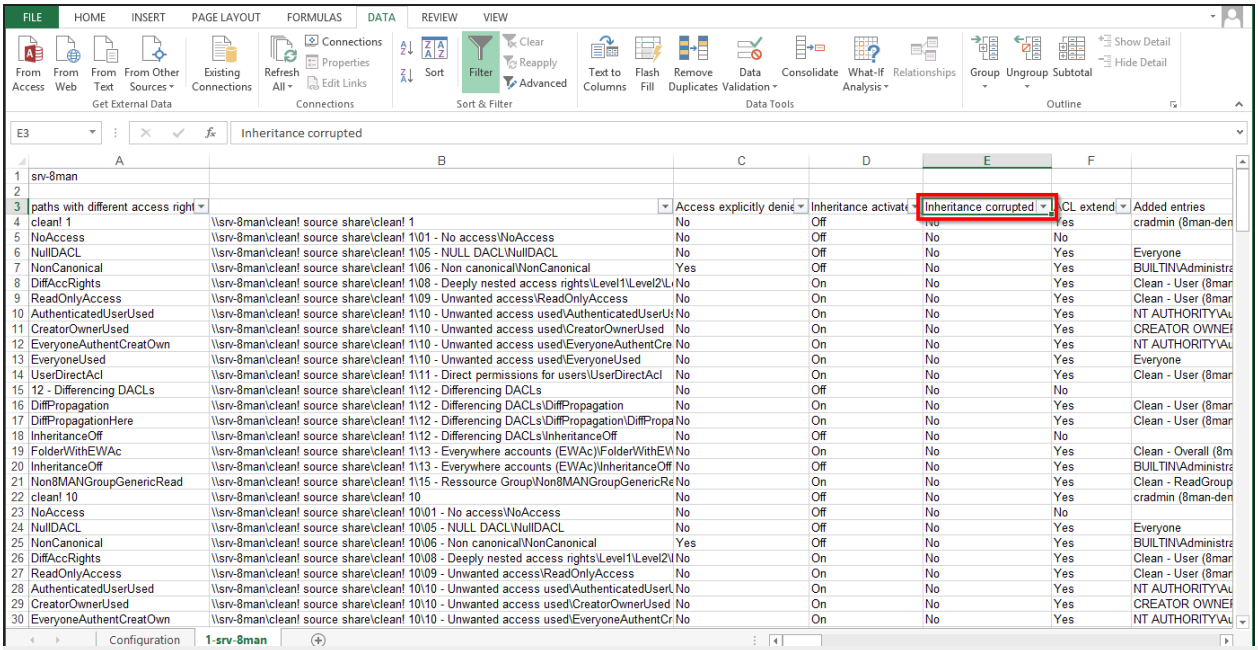


1. You can name the report and add a comment.
2. You can change the range of the report.
3. Start the report creation.



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.



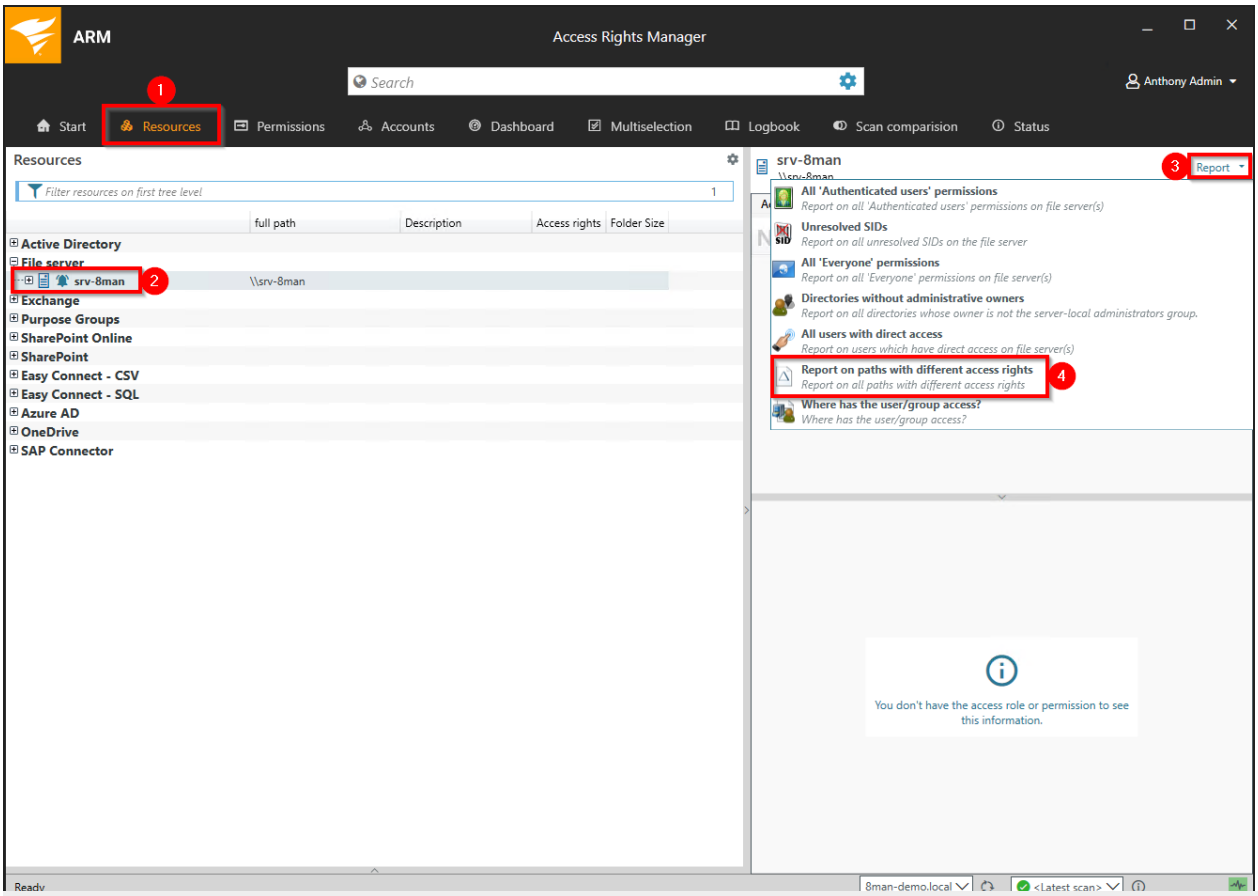
Filter the column "inheritance corrupted" by "yes".

Identify folders with special protection

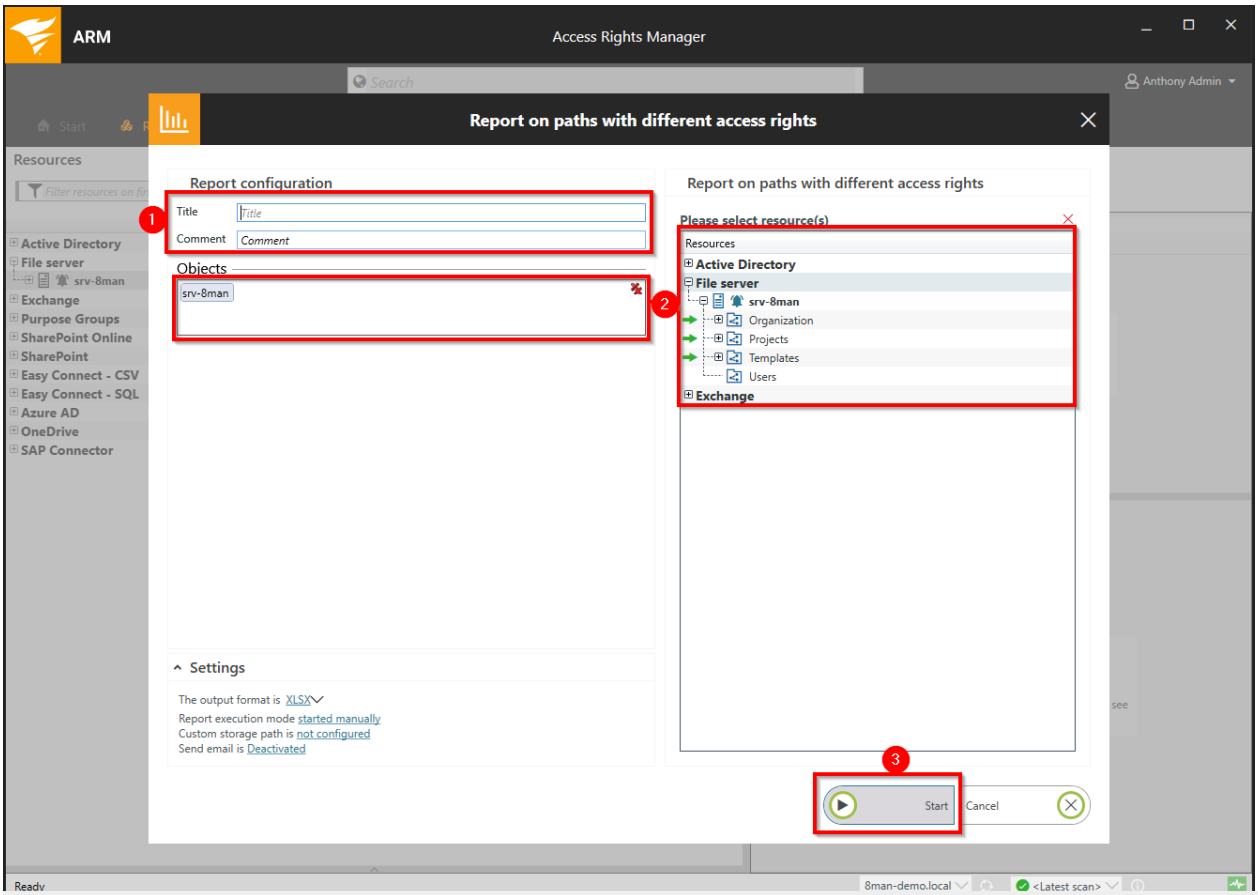
Background / Value

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.

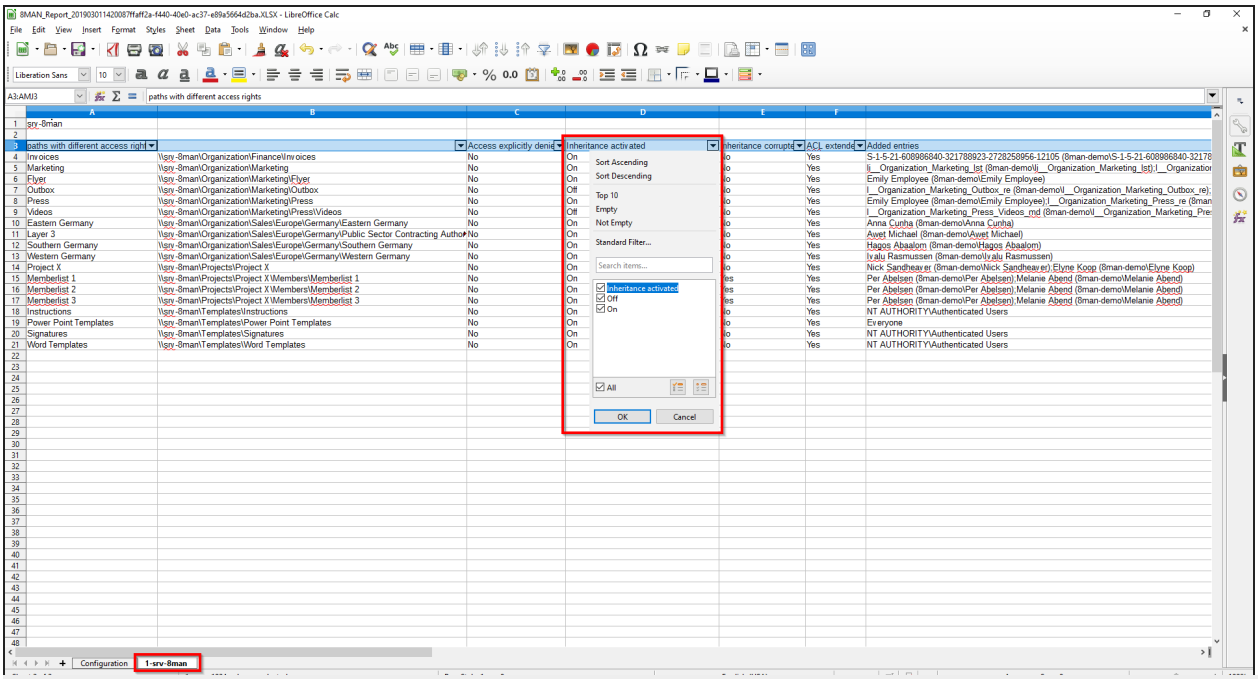
Step-by-step process



1. Select "Resources"
2. Select the desired file server.
3. Click on "Report"
4. Select the report "Report on paths with different access rights"



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.



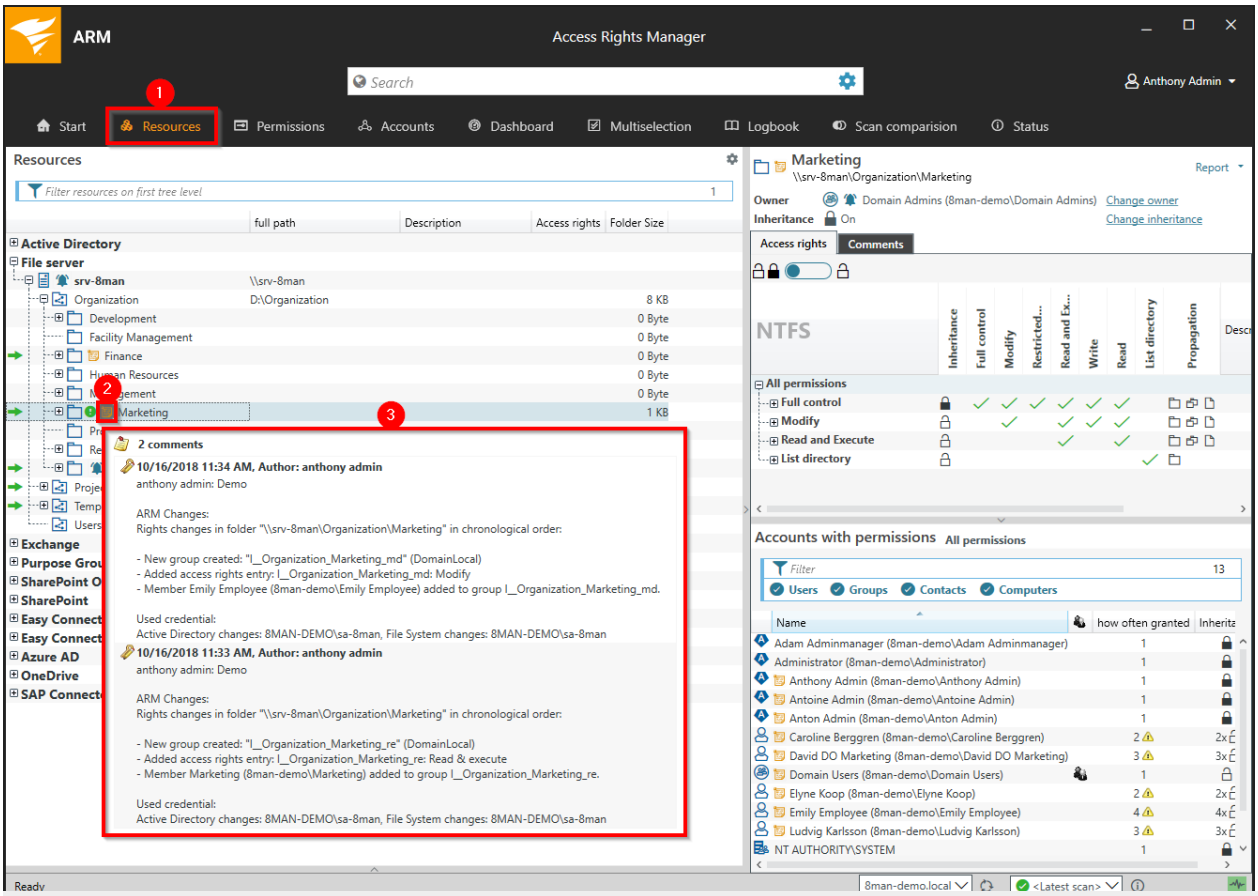
1. Open the .XLSX file with your spreadsheet application.
2. Click on the "resource tab".
3. We recommend using "auto filter" to analyze the "Inheritance activated" column. If set to "off" the report shows all directories with disabled inheritance.

Identify the latest activities on a directory

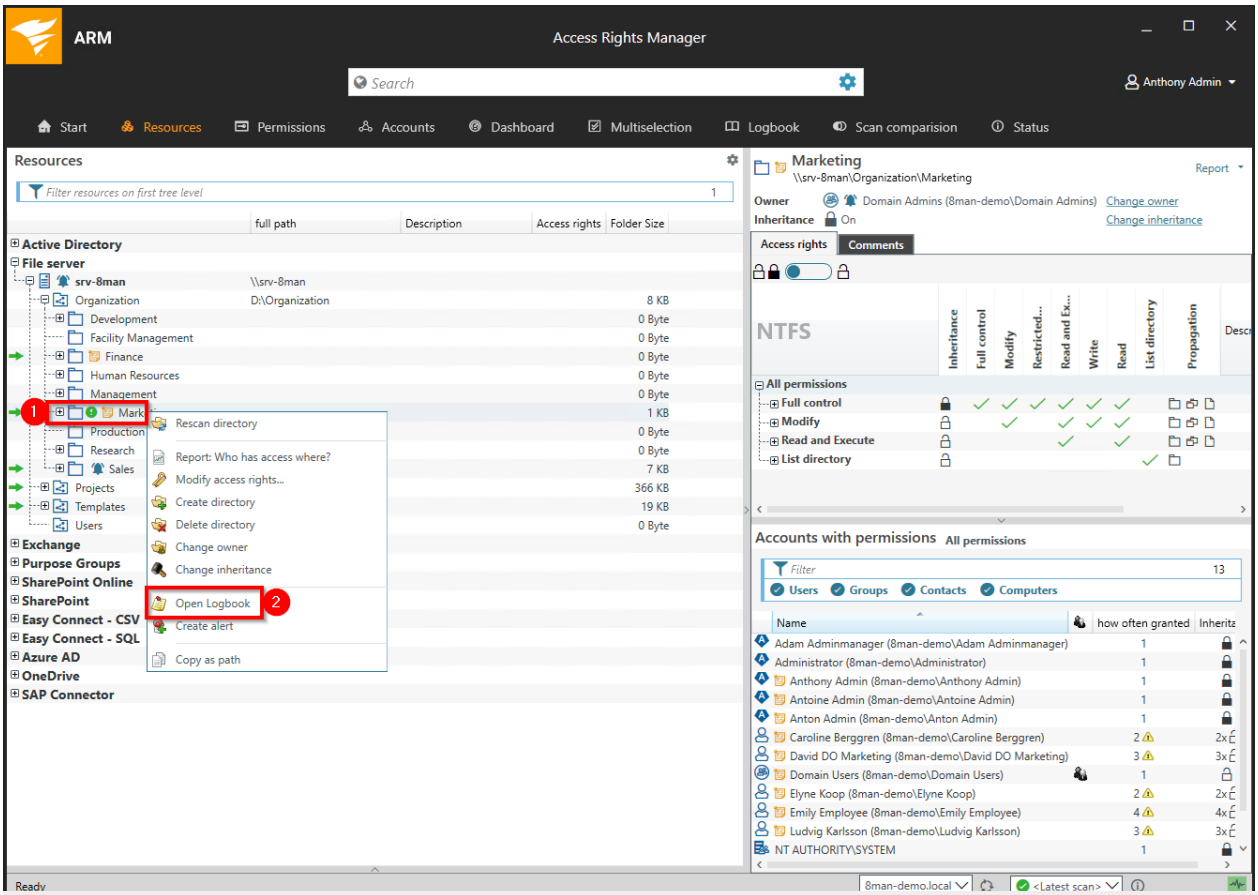
Background / Value

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.

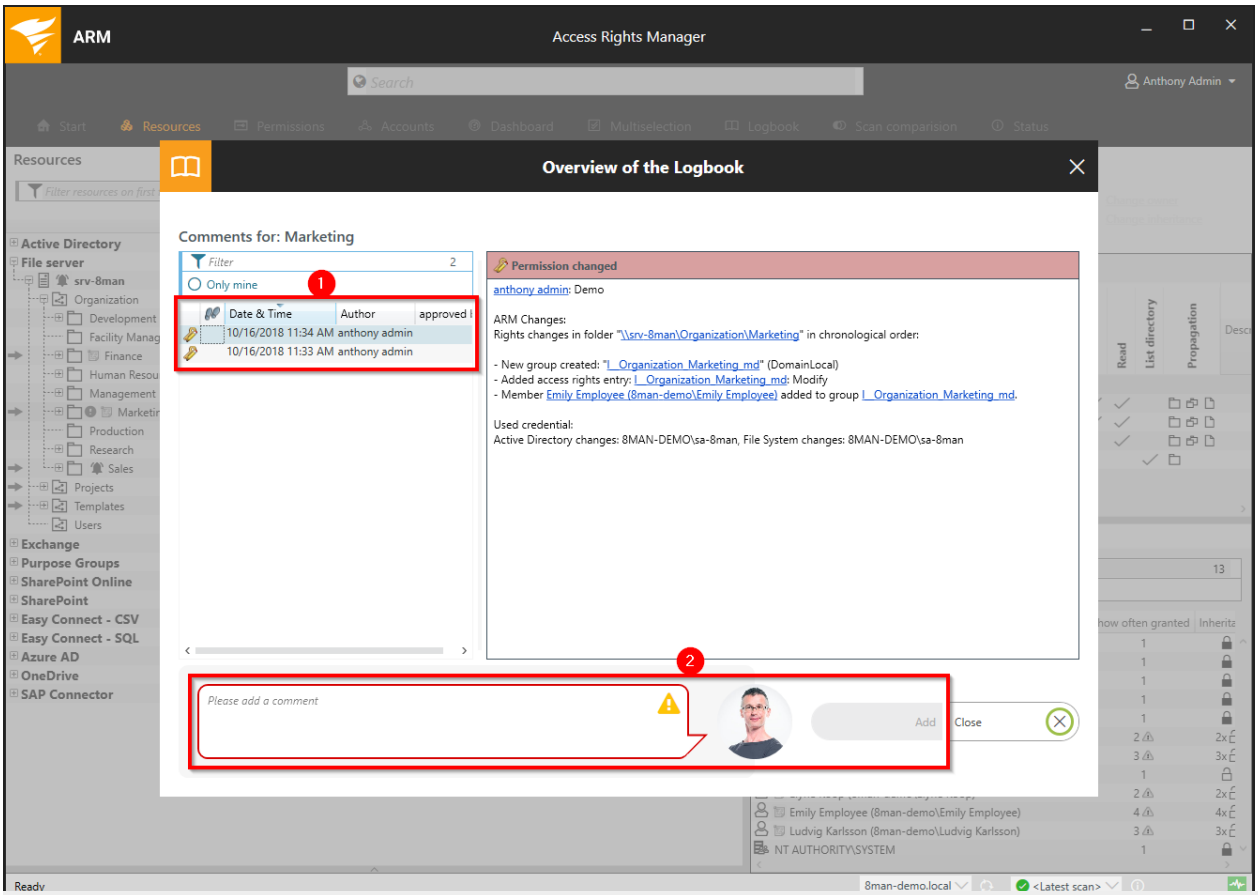
Step-by-step process



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.



1. Right-click on a directory.
2. Click on "Open Logbook".



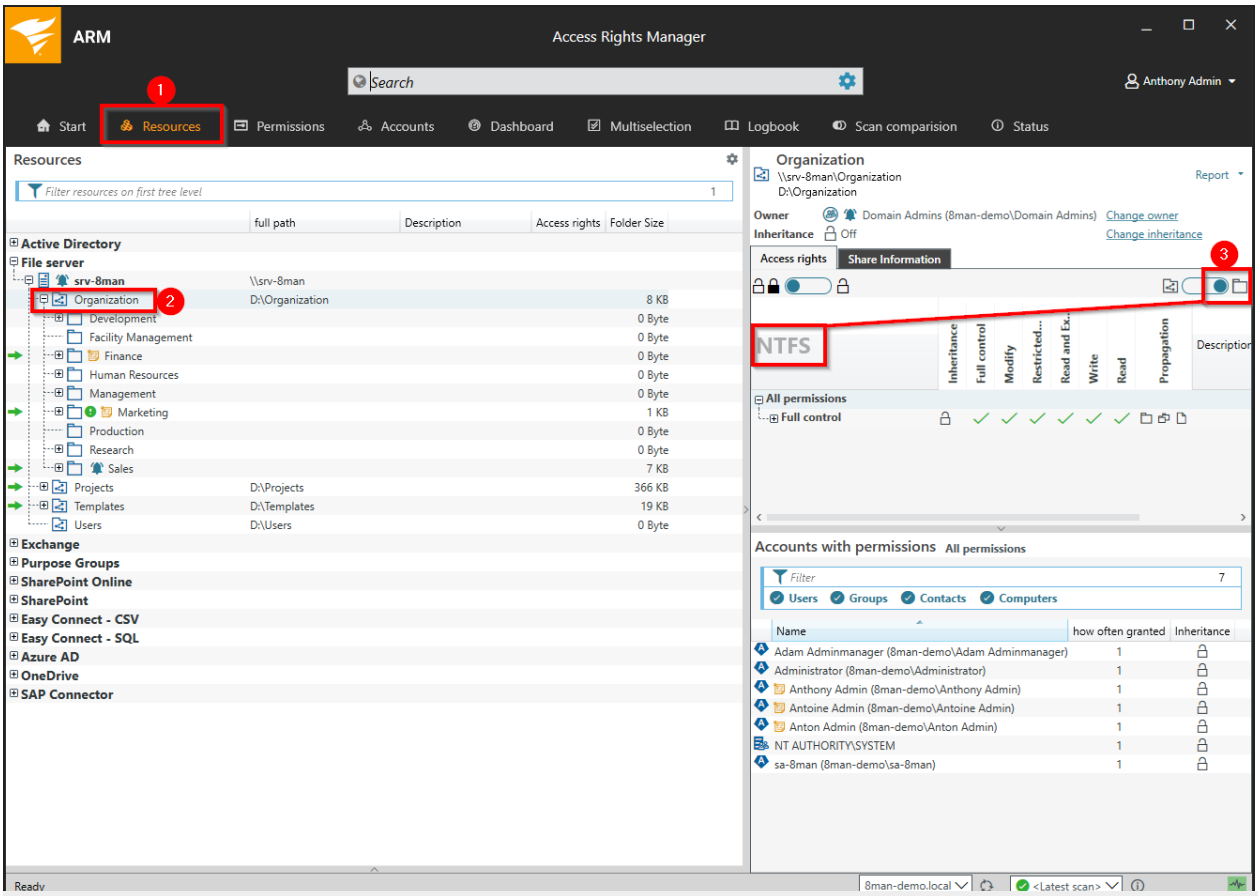
1. Check the previous actions on the object.
2. You can also add a comment at any time to the logbook.

Identify share permissions

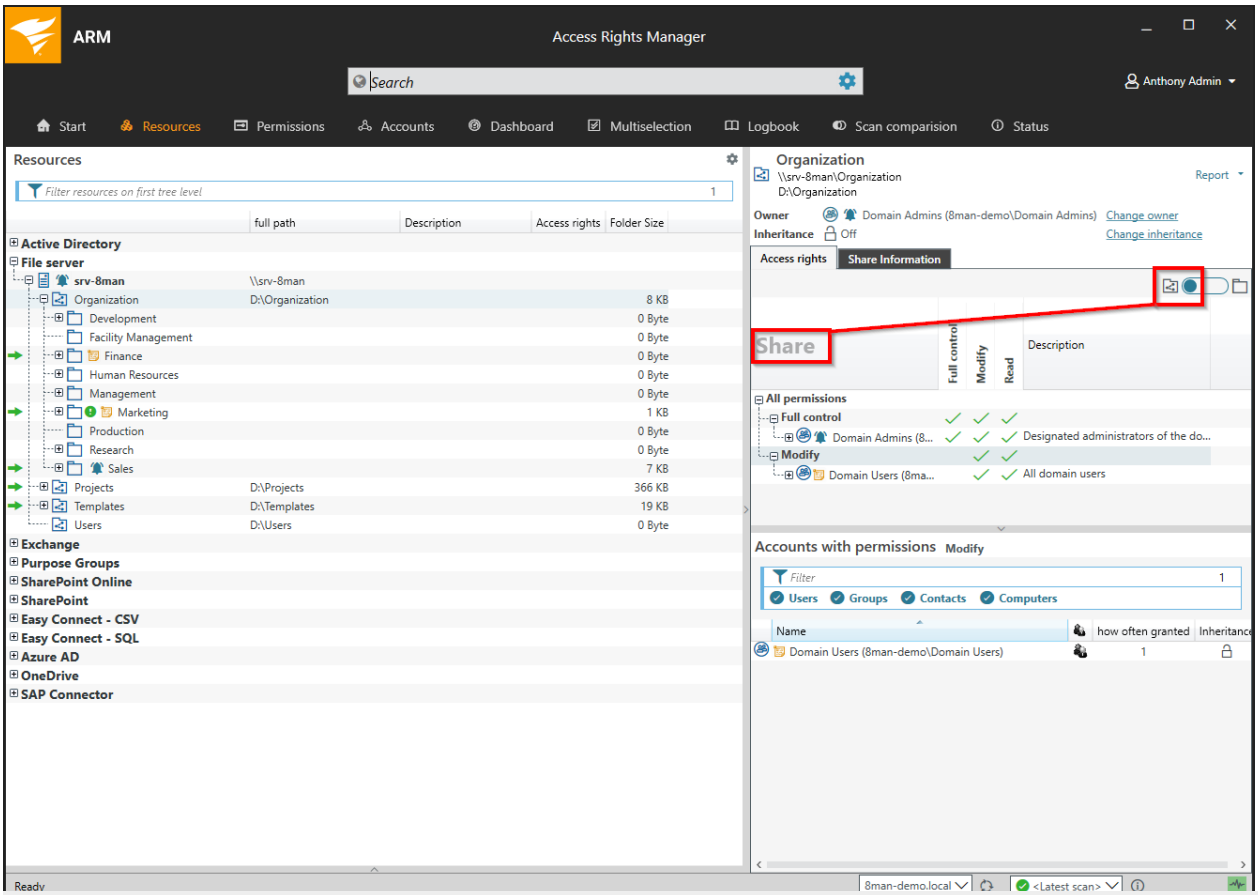
Background / Value

ARM shows both on shared directories: share permissions as well as NTFS permissions. By default NTFS permissions are listed.

Step-by-step process



1. Select "Resources".
2. Select a shared folder (recognizable by the special folder icon).
3. By default ARM shows NTFS permissions.



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

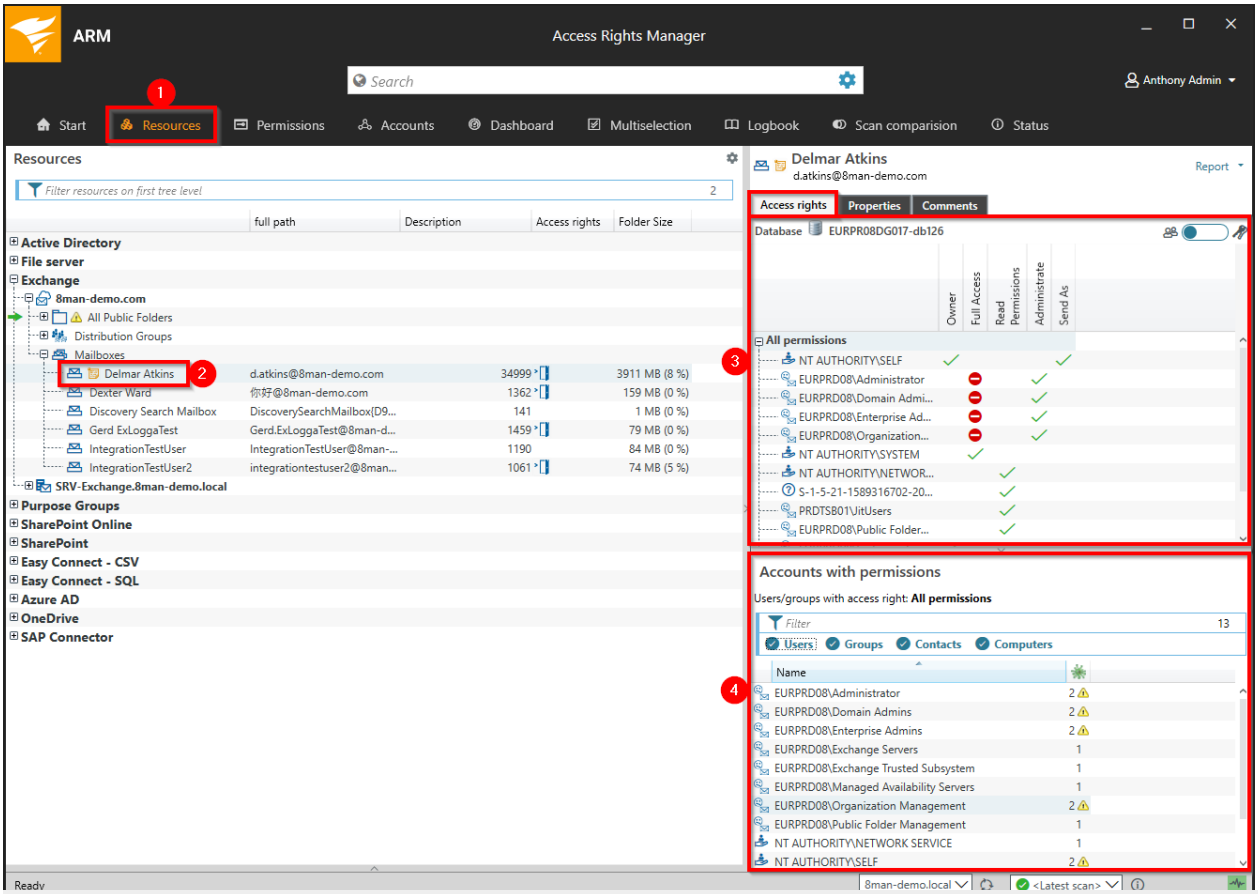
Who as access to which mailbox? ARM for Exchange shows you all access rights in the resources view.

Related features

Report: Who has access where?

Report: Identify mailbox permissions

Step-by-step process



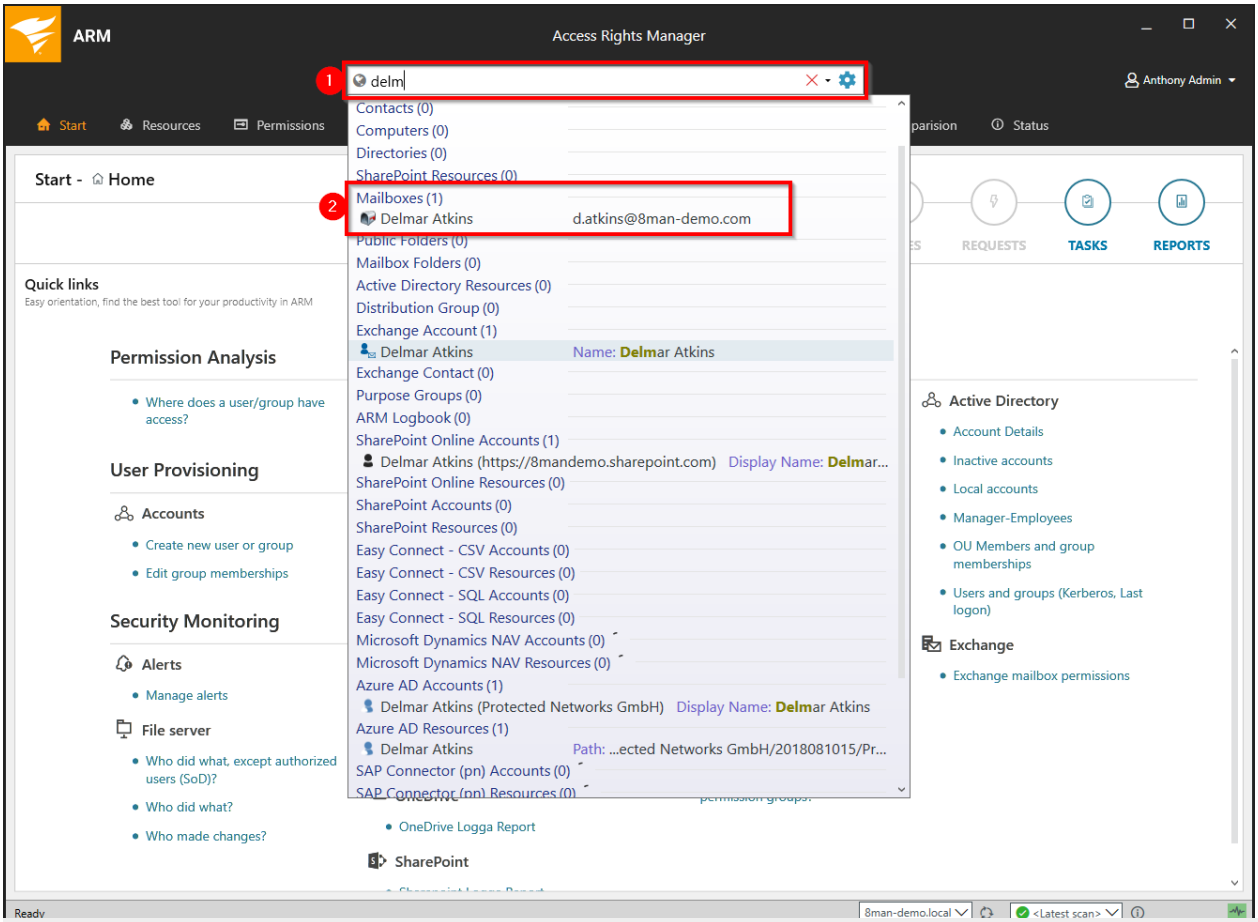
1. Select "Resources".
2. Navigate to the desired mailbox.
3. ARM shows you which users/groups have which rights.
4. ARM shows all accounts with access rights in a flat list.

Identify mailbox properties

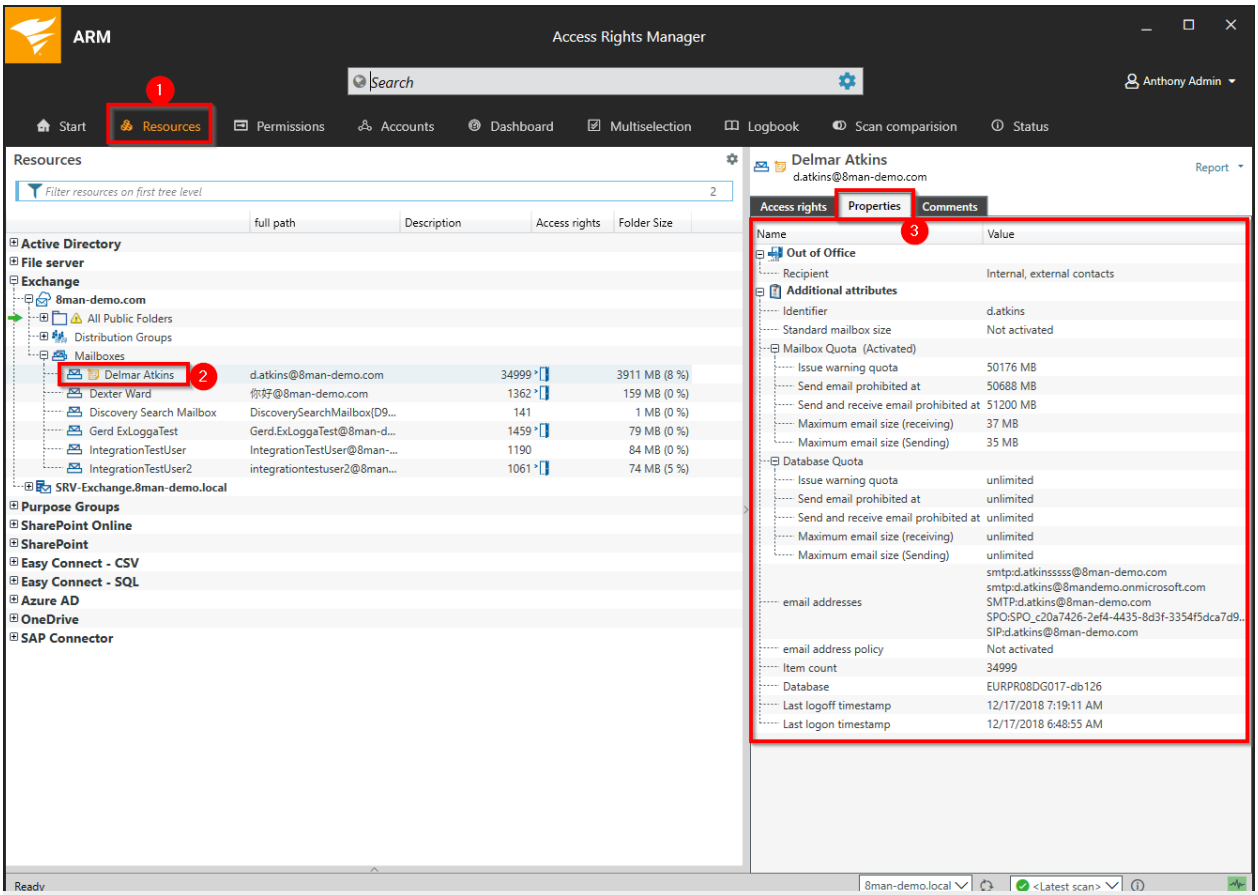
Background / Purpose

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.



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

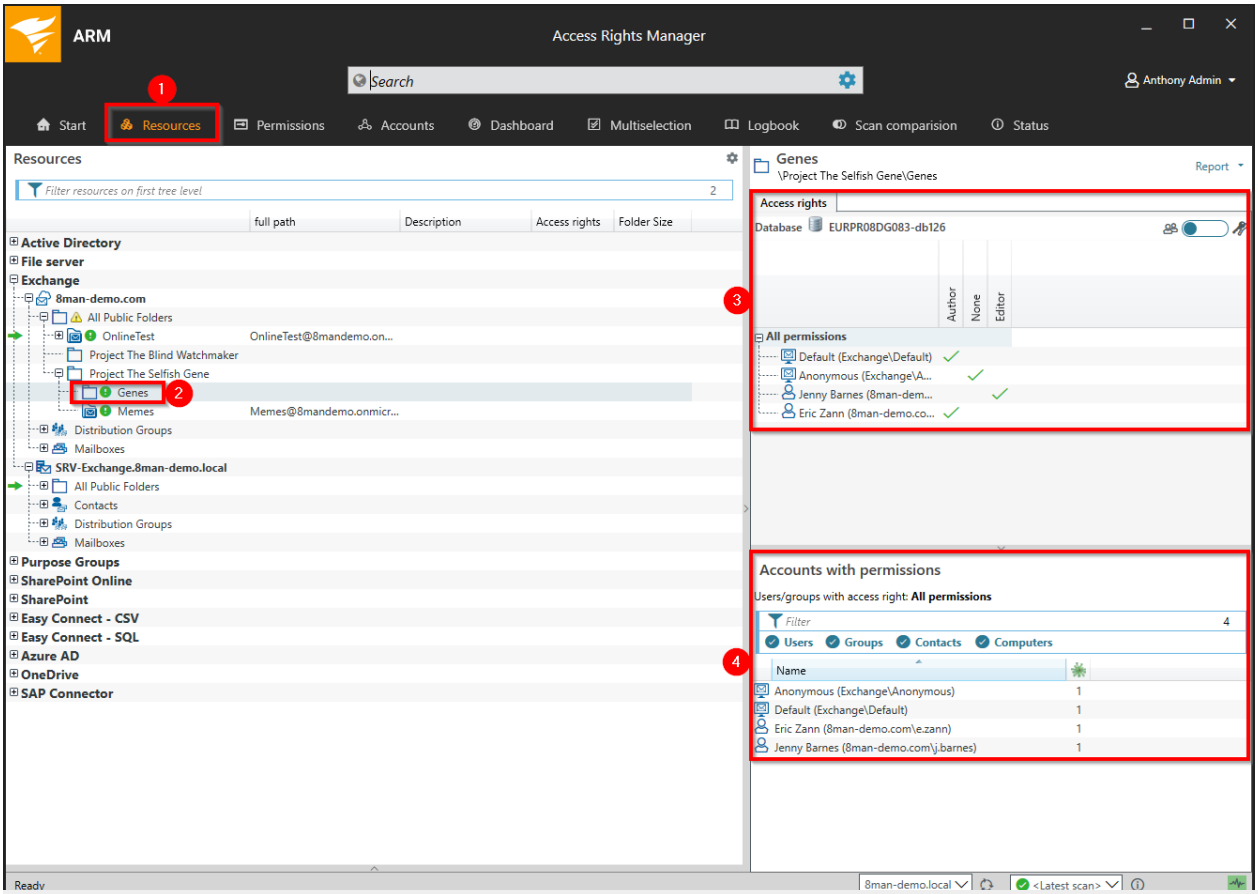
Create a mailbox

Change mailbox permissions

Manage out-of office notices

Manage mailbox and email size

Step-by-step process



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.

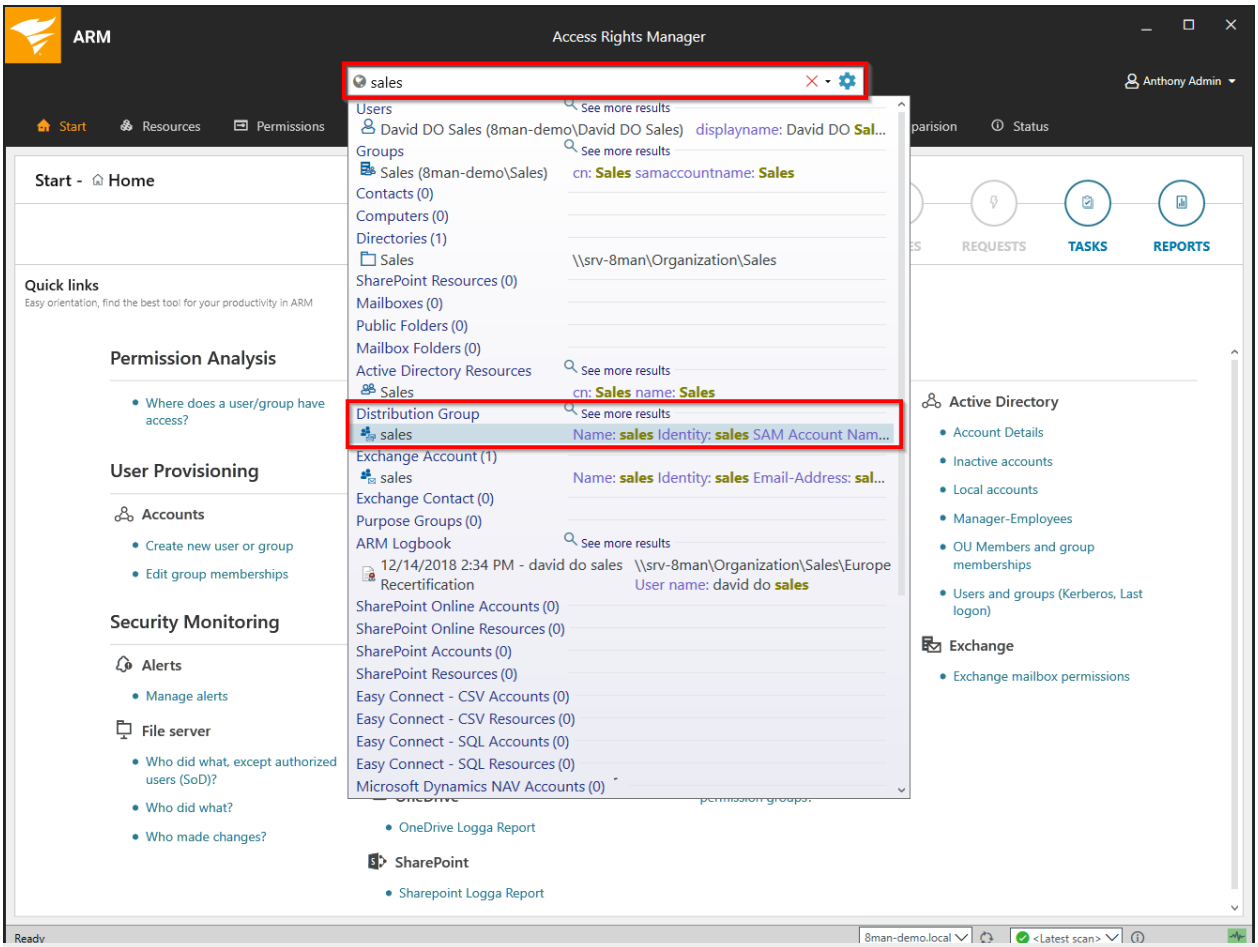
Identify permissions on distribution groups

Background / Value

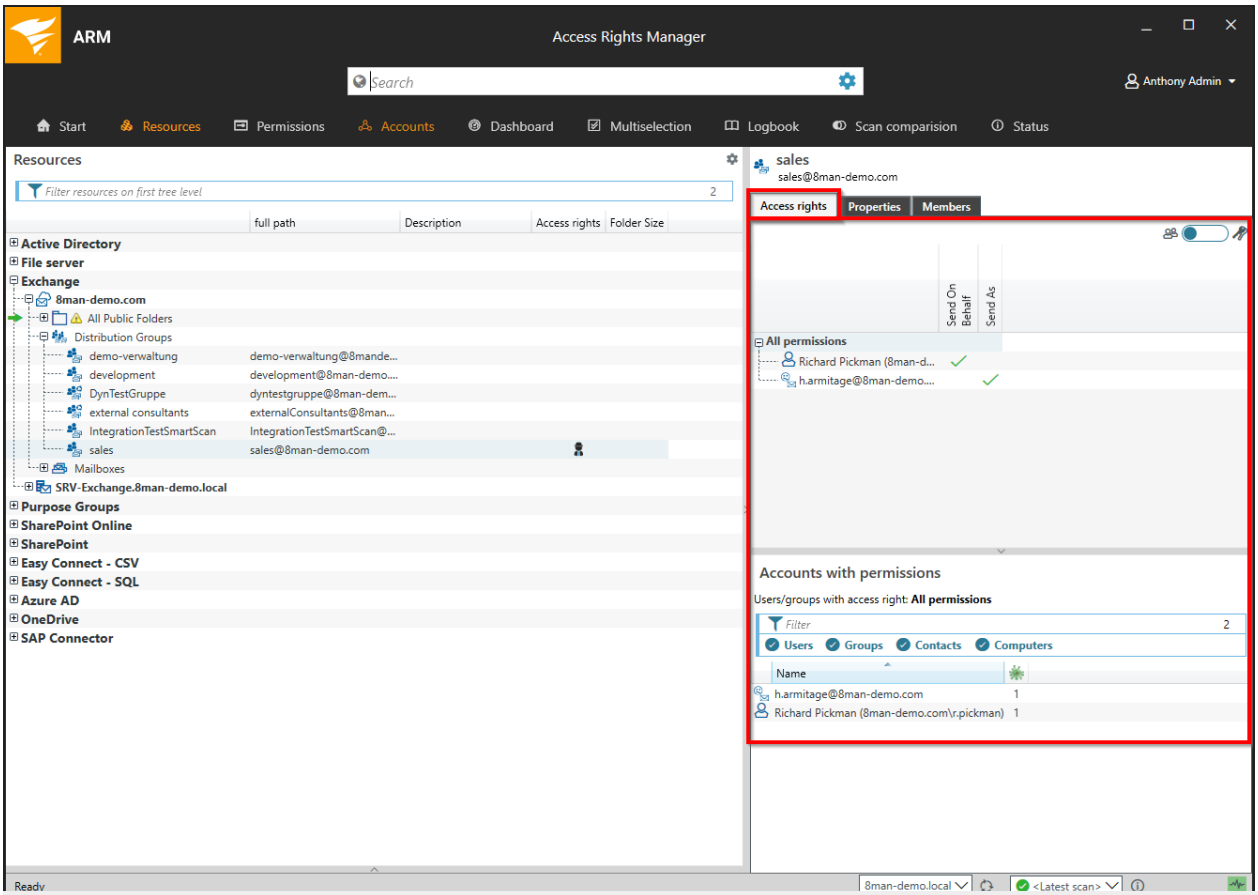
With ARM you can quickly check who is allowed to send emails from which distribution list. The relevant cases are "send as" and "send on behalf of". The former is the most critical, since it is not easy to identify who actually sent the email. In the scenario for "send on behalf" the PA or deputy sending 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.



ARM shows all access rights on the right-hand side.

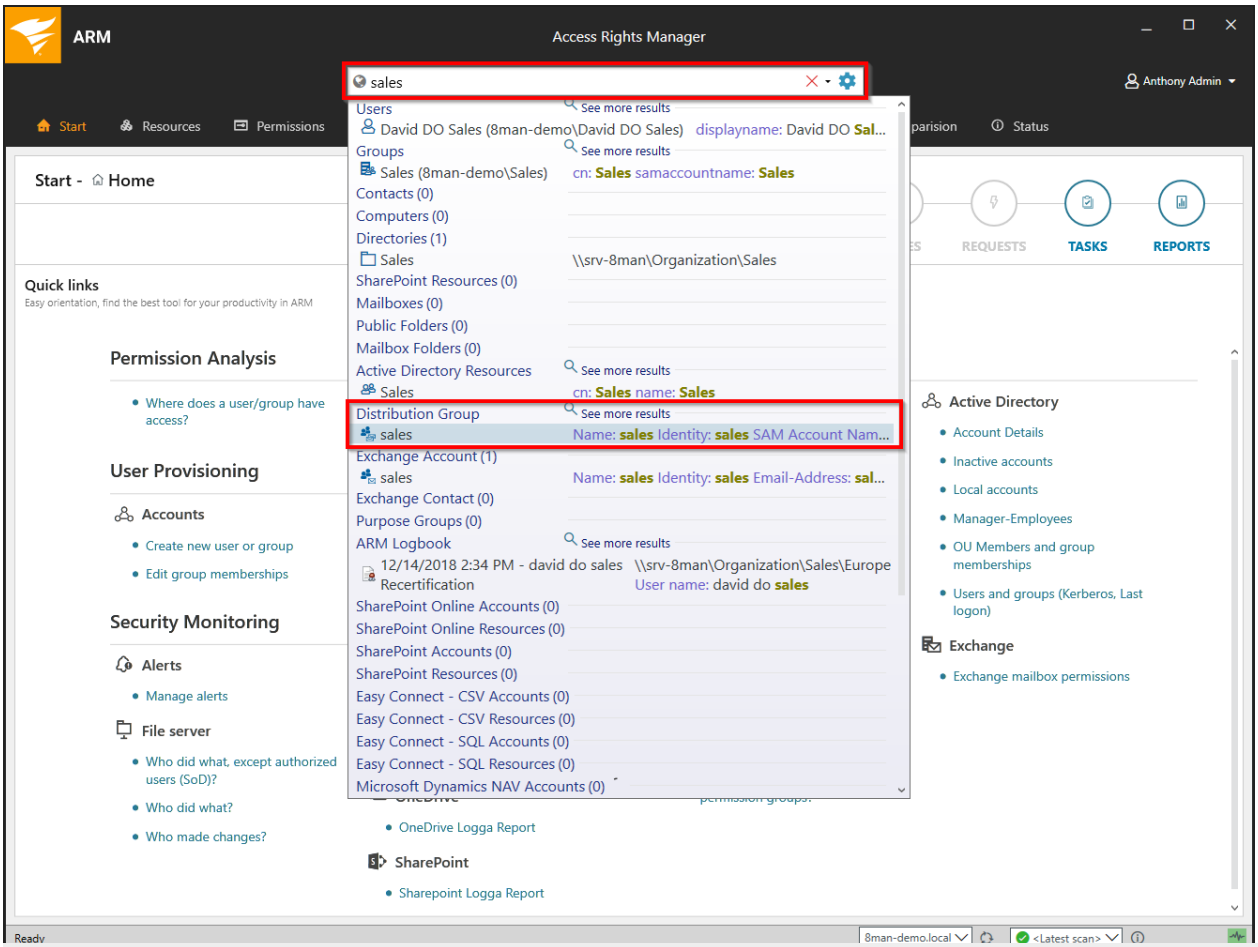
Identify members of distribution groups

Background / Purpose

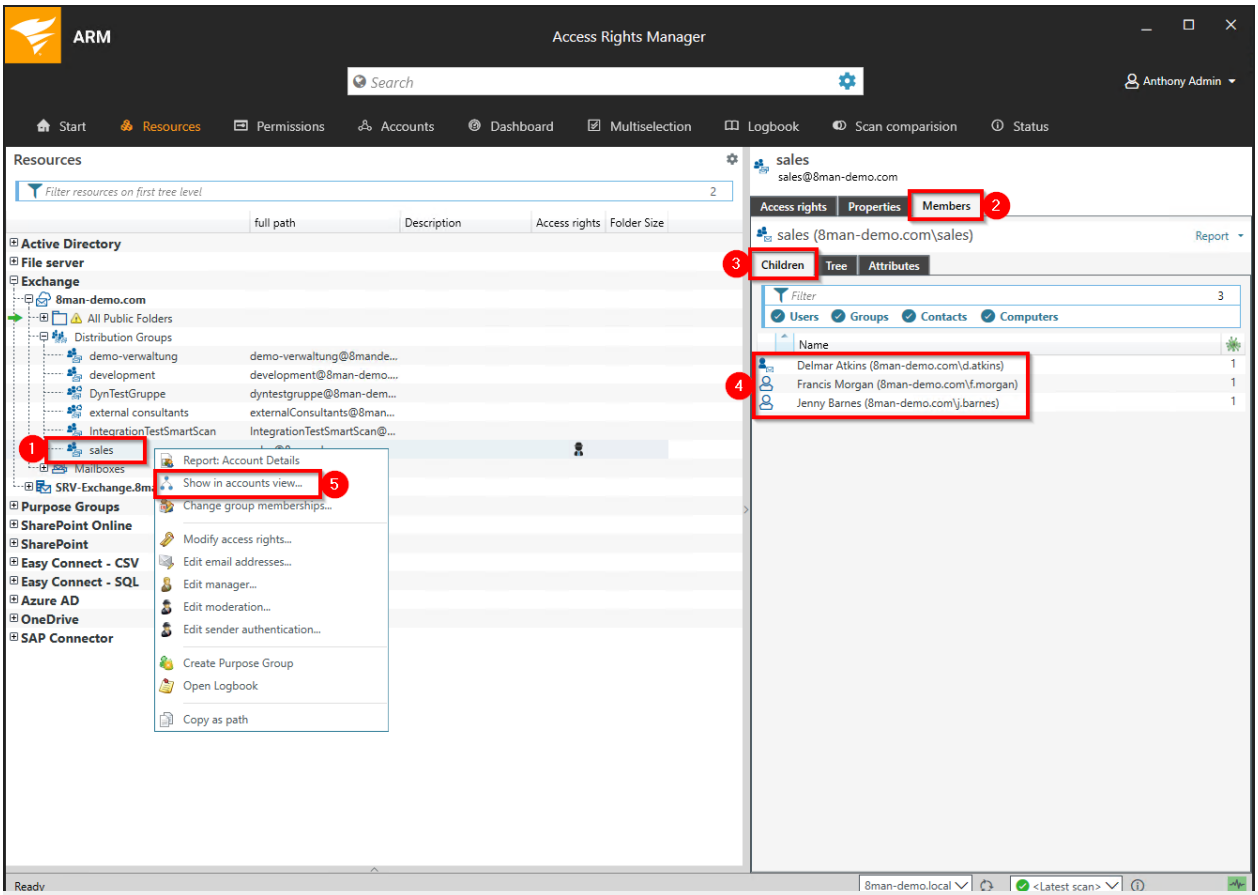
ARM allows you to display all members and / or recipients of distribution lists. In typical ARM style this also includes nested group memberships.

ARM also works with dynamic Exchange groups.

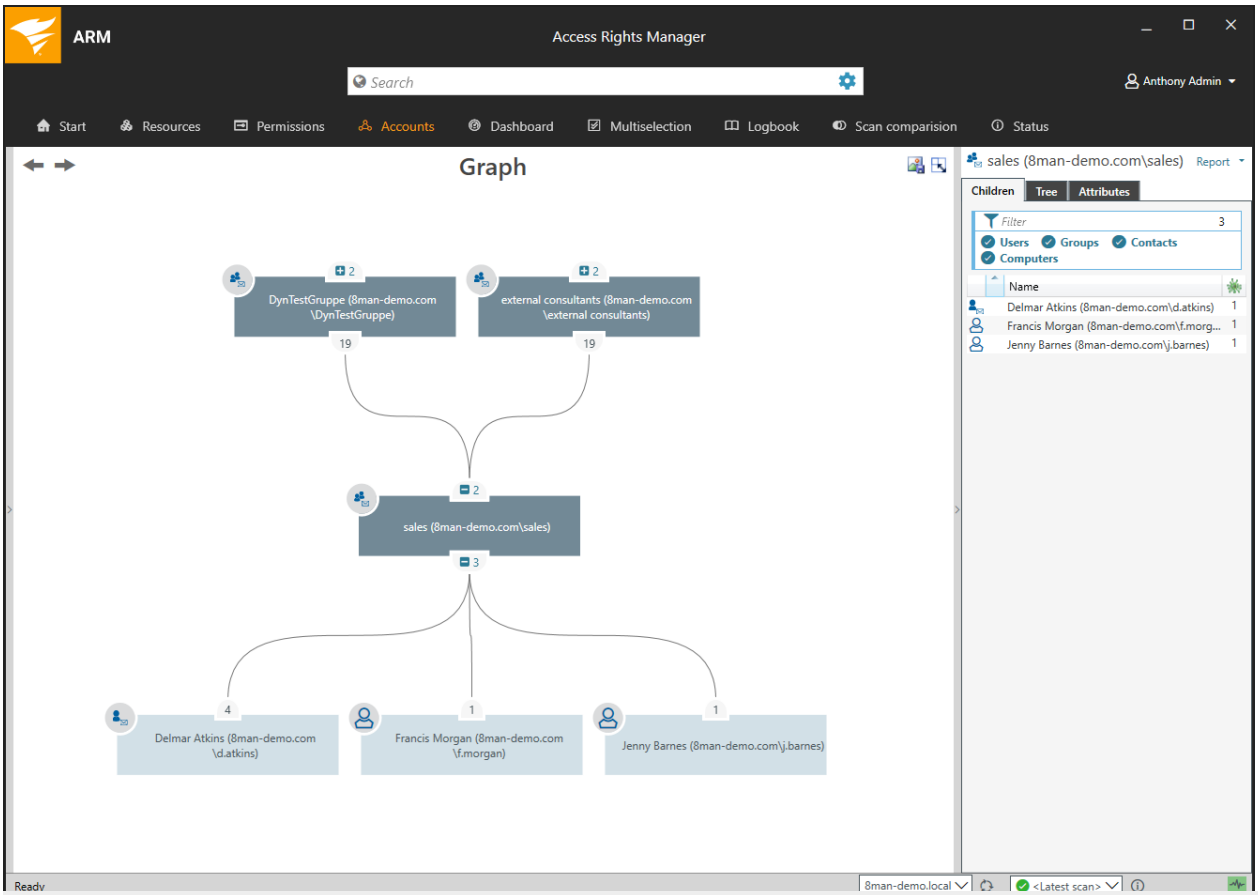
Step-by-step process



Use the search field to find the desired distribution group.



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.



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

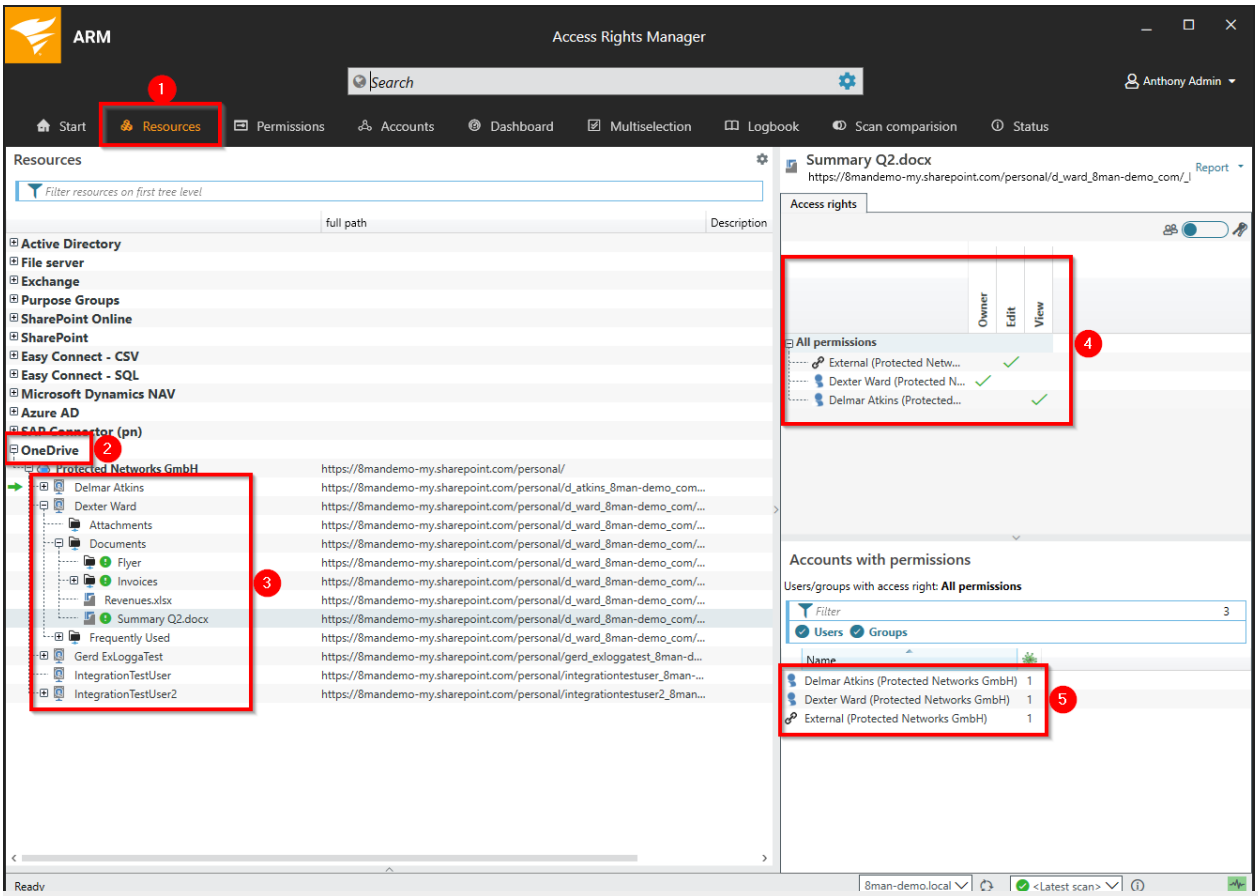
OneDrive offers the possibility to store files and folders in the cloud. The advantages of the cloud service are obvious: employees can work together on documents easily and conveniently. The external sharing of documents is particularly critical as it is possible to share documents without authorization for an unlimited period of time.

ARM shows you with its typical simplicity which users shared which files and folders how and with whom.

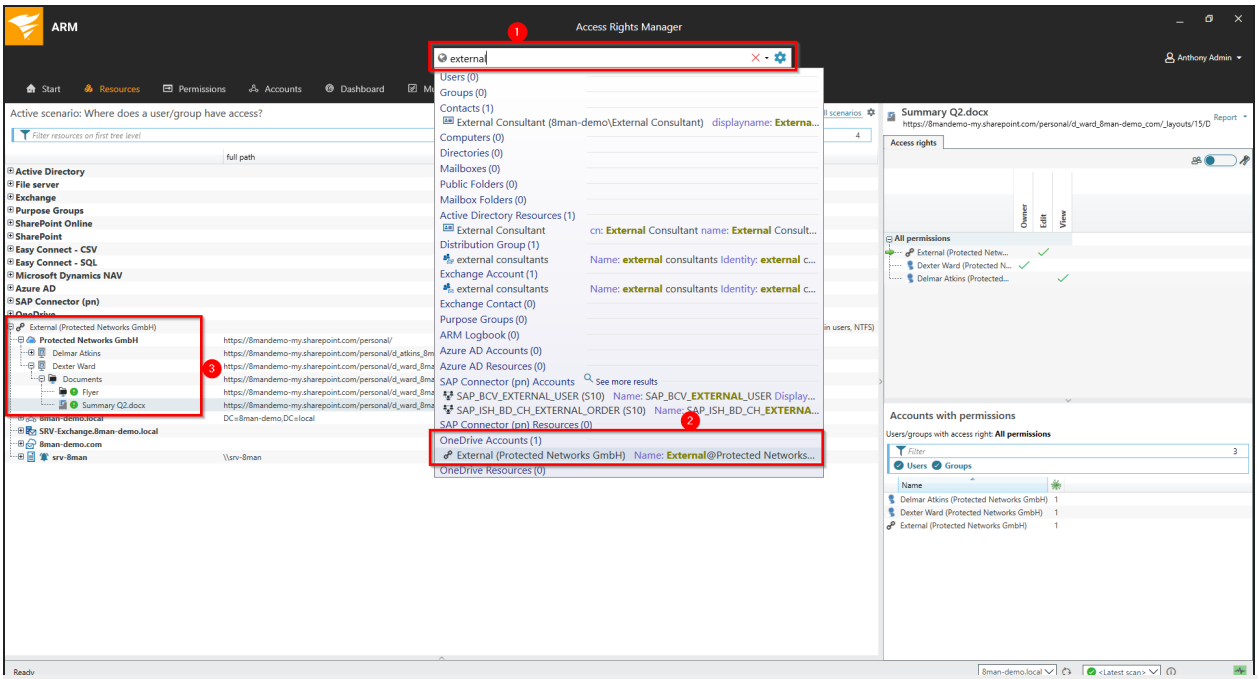
Related features

Create a report about directories and files shared on OneDrive

Step-by-step process



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:

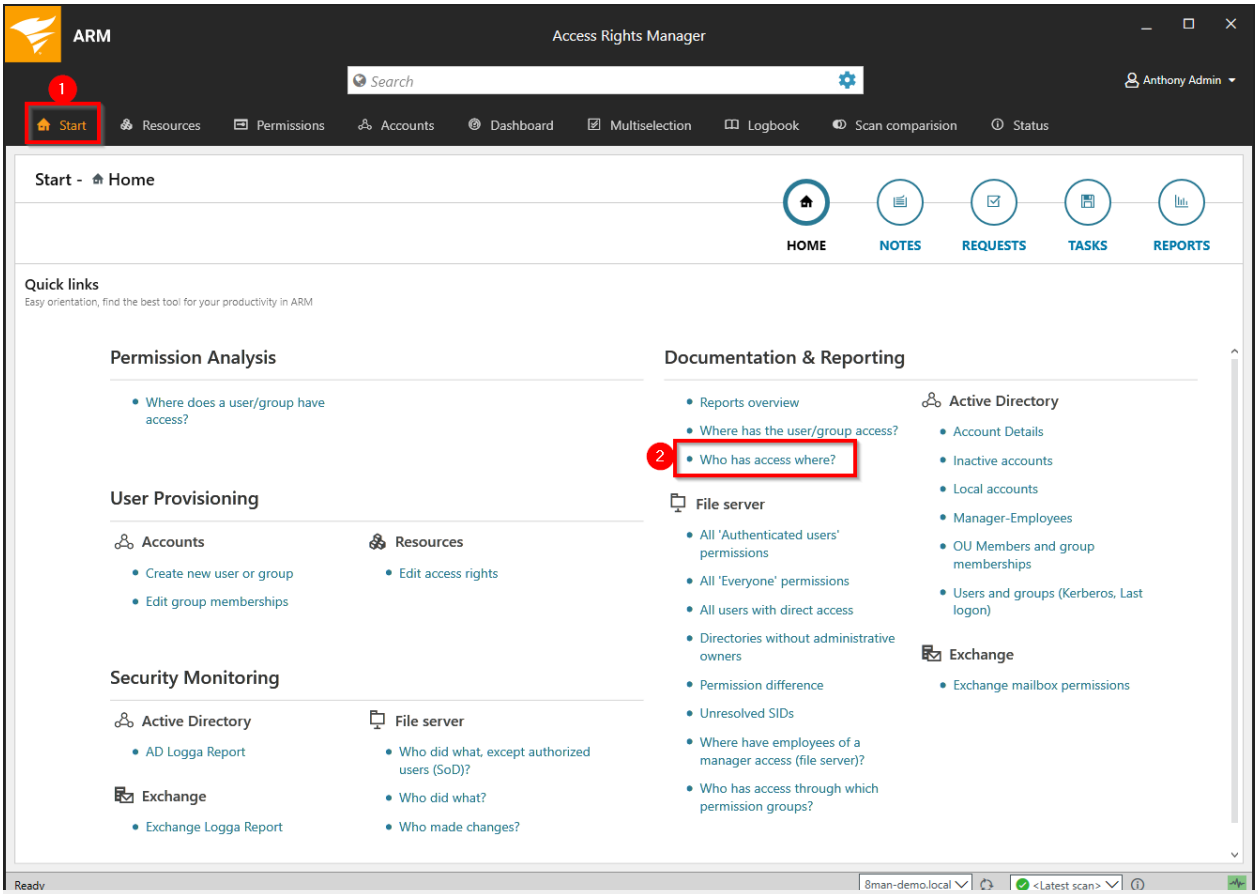
- Who should have access to what? (increase in data security)
- Which access rights should exist? (improvement of data integrity)

Related features

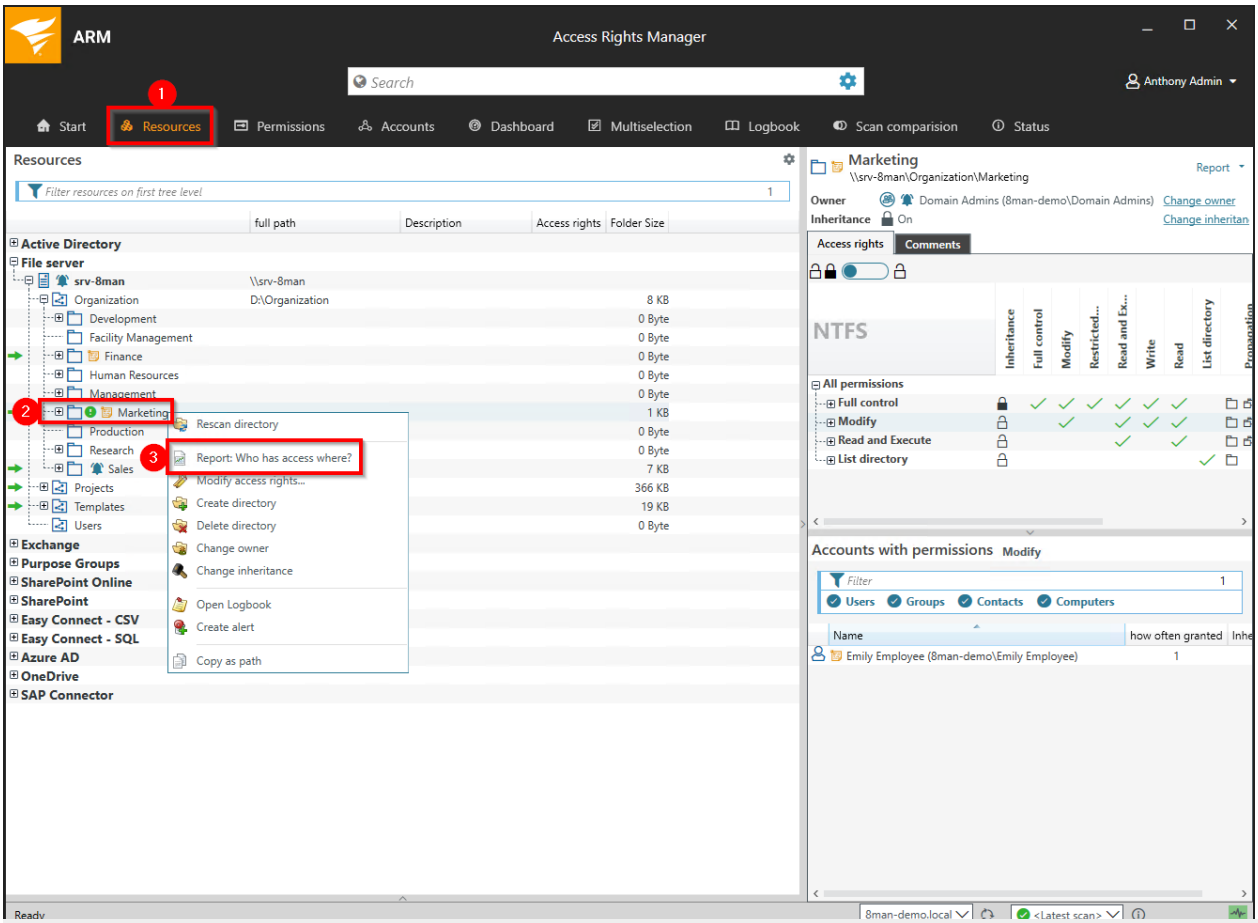
Report: Where do users and groups have access? (user in focus)

Modify directory access rights

Step by step process

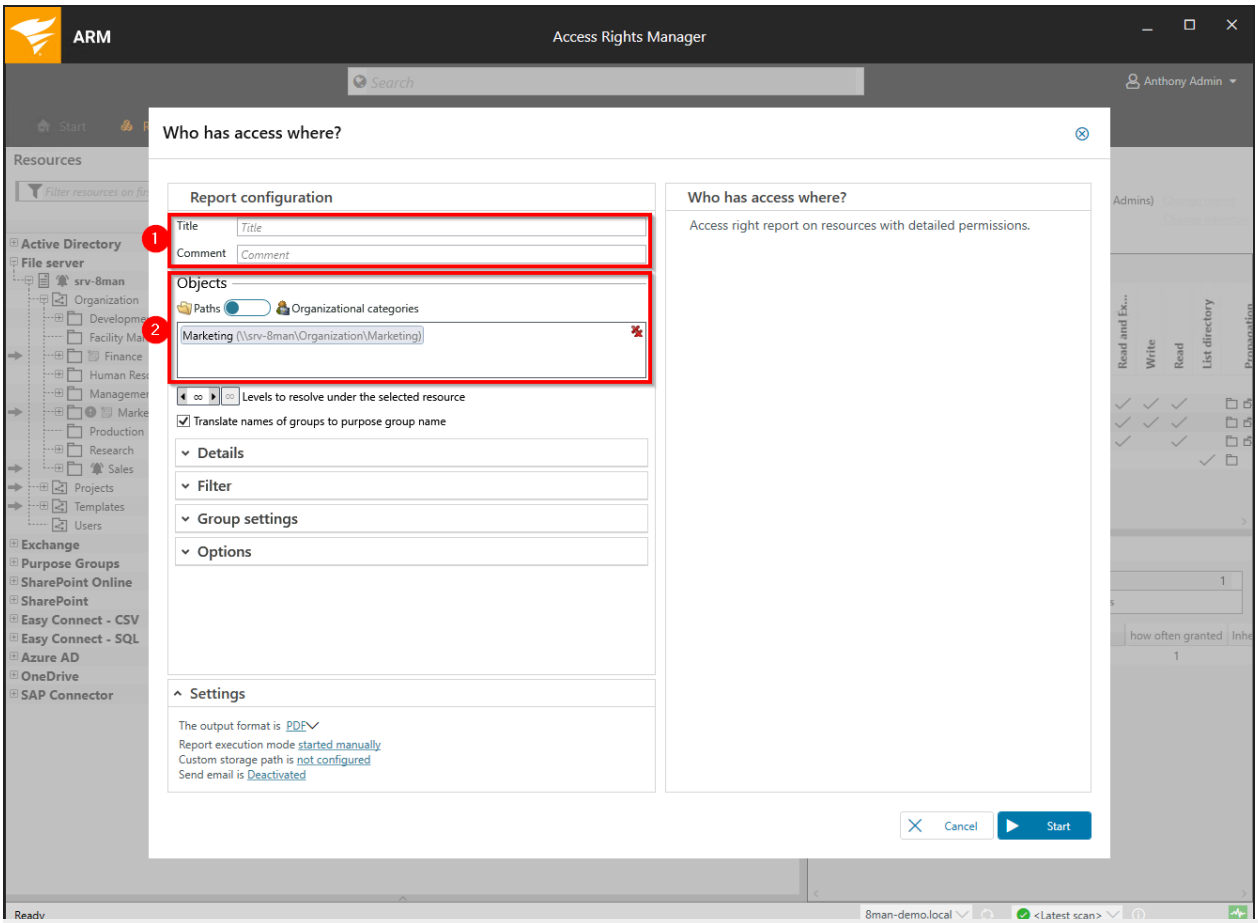


1. Select "Start".
2. Click "Who has access where?".

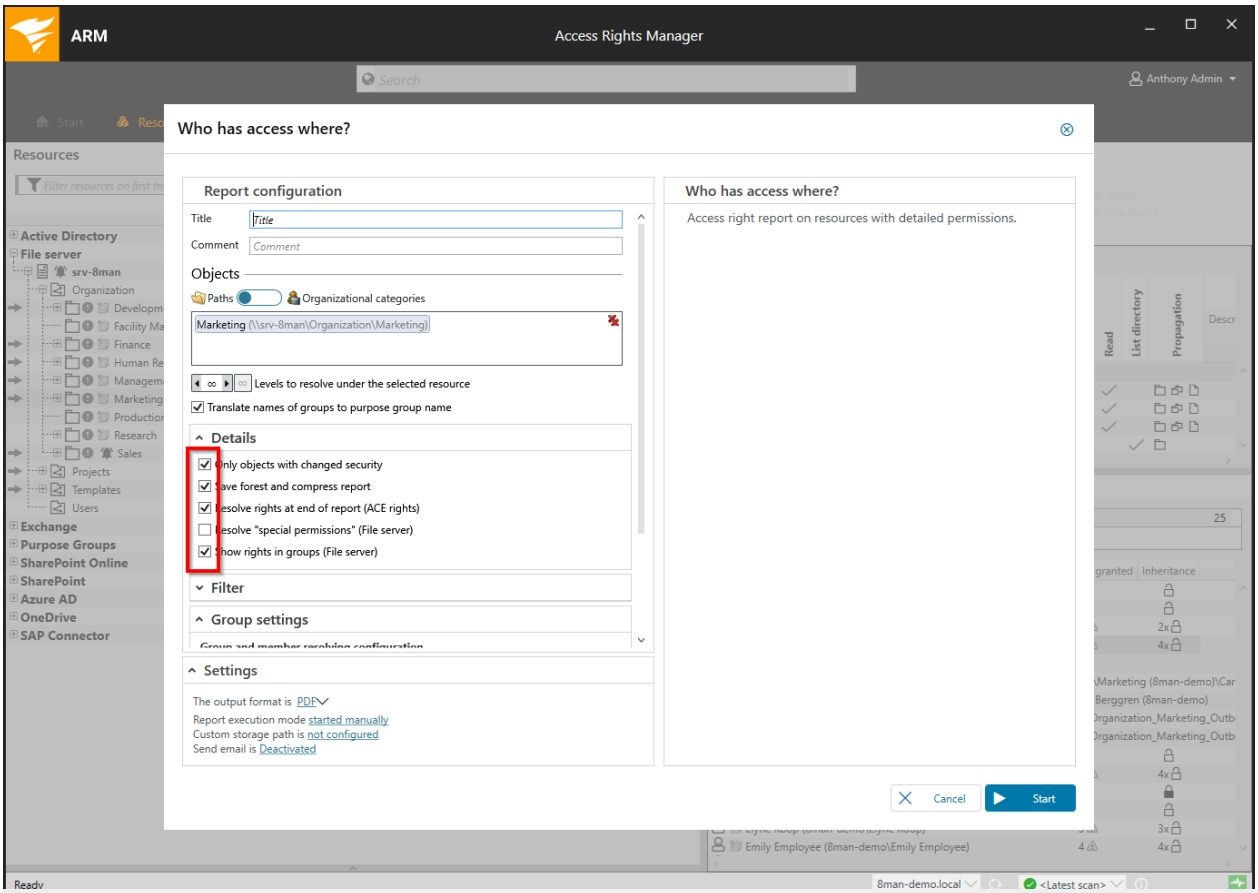


Alternative way to start the report:

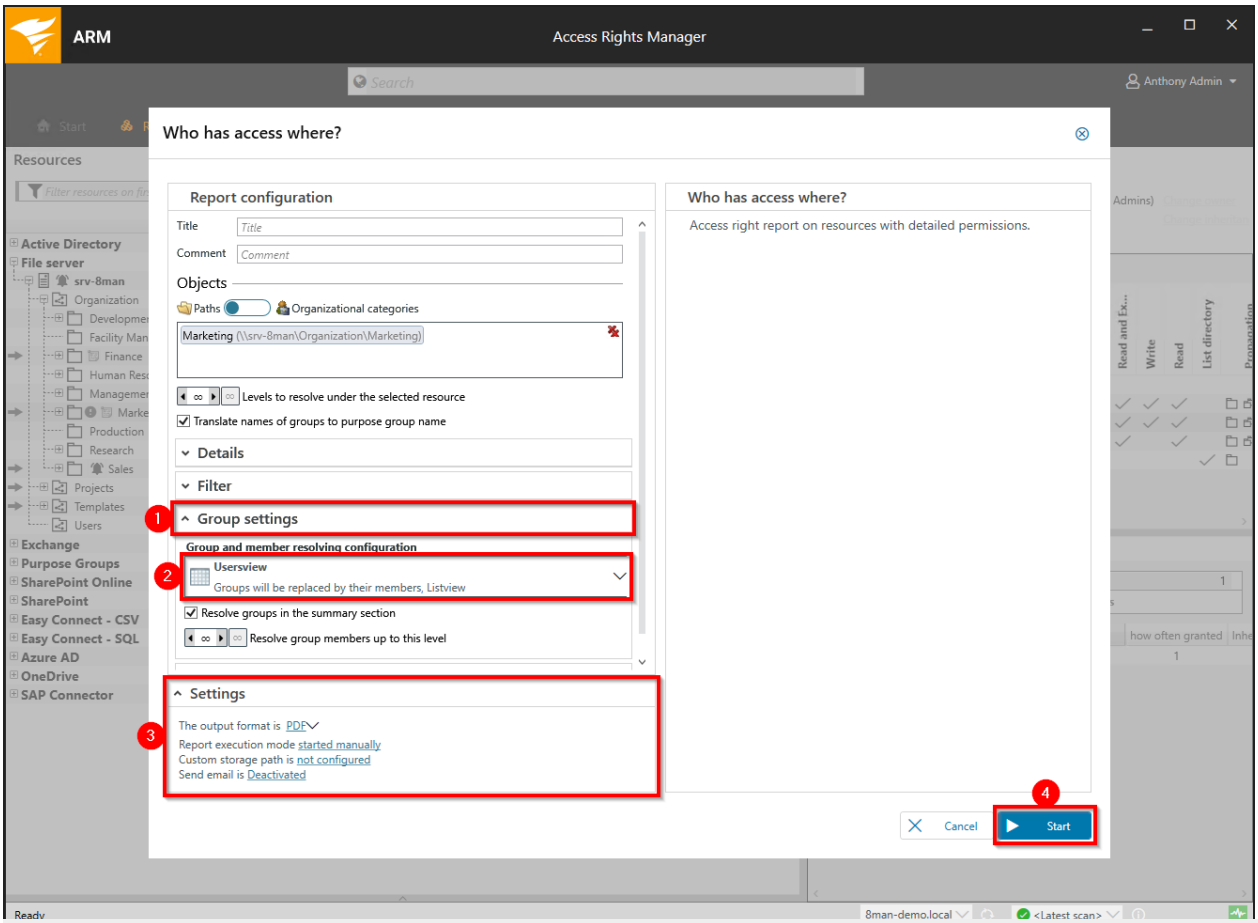
1. Select "Resources".
2. Right-click on a directory that you are responsible for.
3. Click on "Report: Who has access where?" from the context menu.



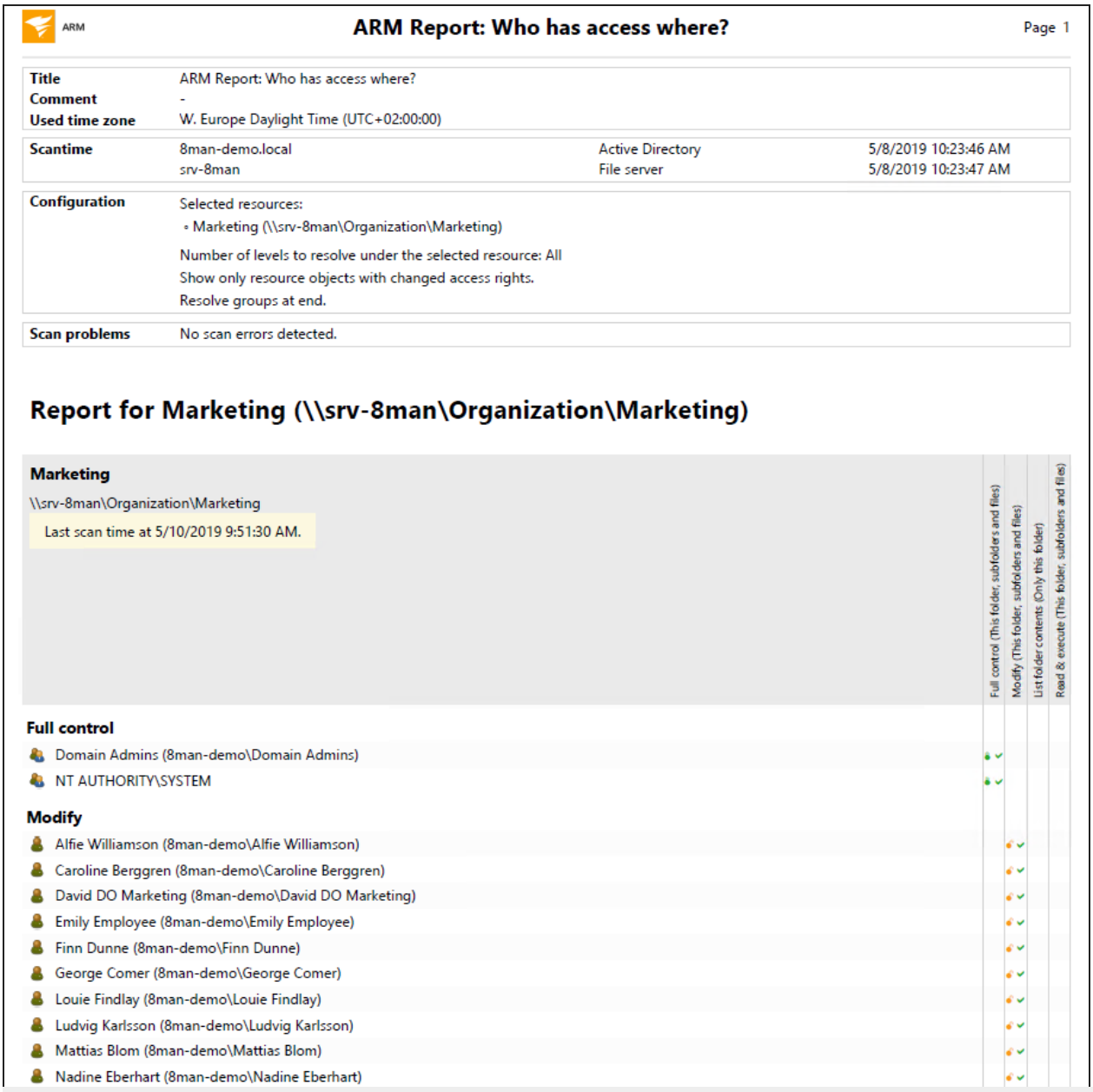
1. Name the report and add a comment.
2. The selected resource is automatically included in the list of objects to be analyzed. You can add further resources.



We recommend that you set the options in the details area for a first run as shown above.



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

ARM Report: Who has access where?

Page 1

Title	ARM Report: Who has access where?
Comment	-
Used time zone	W. Europe Daylight Time (UTC+02:00:00)

Scantime	8man-demo.local	Active Directory	5/8/2019 10:23:46 AM
	srv-8man	File server	5/8/2019 10:23:47 AM

Configuration

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.

Scan problems 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)

Full control

- Domain Admins (8man-demo\Domain Admins)
- NT AUTHORITY\SYSTEM

Modify

- 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.

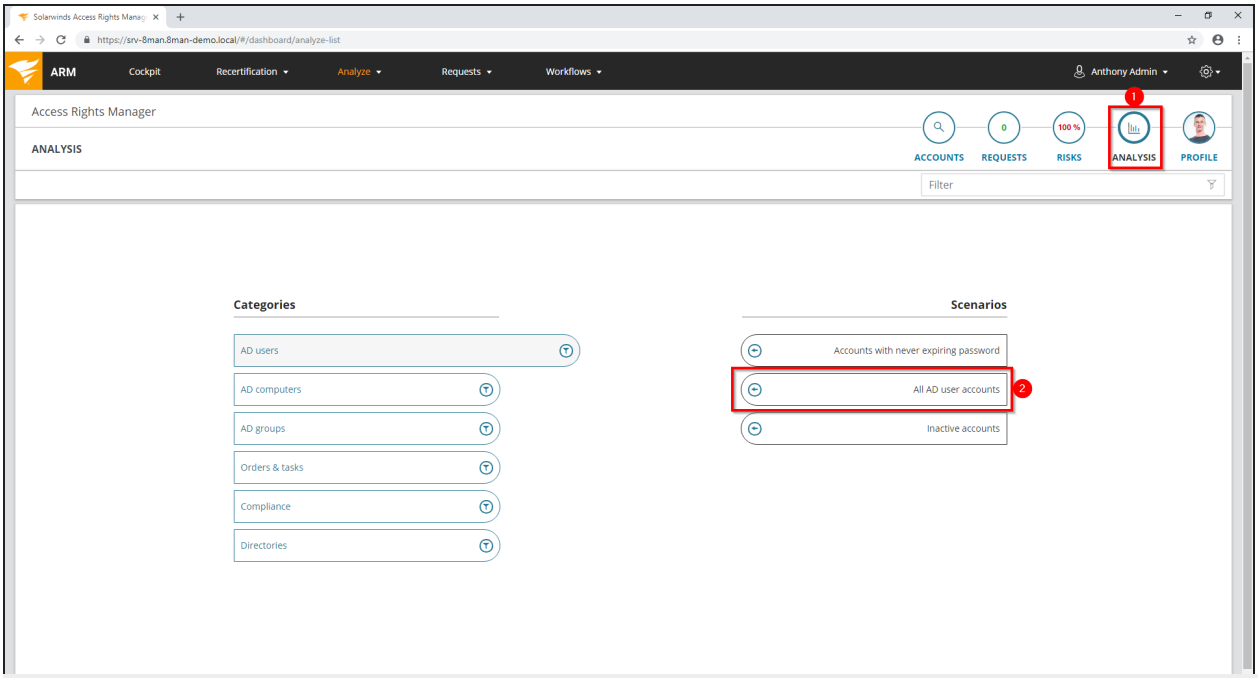
You should also check to see if the access rights of some users can not be reduced for example from "full access" to "read" or "modify". This ensures a higher level of data integrity.

Flexible reports (web client)

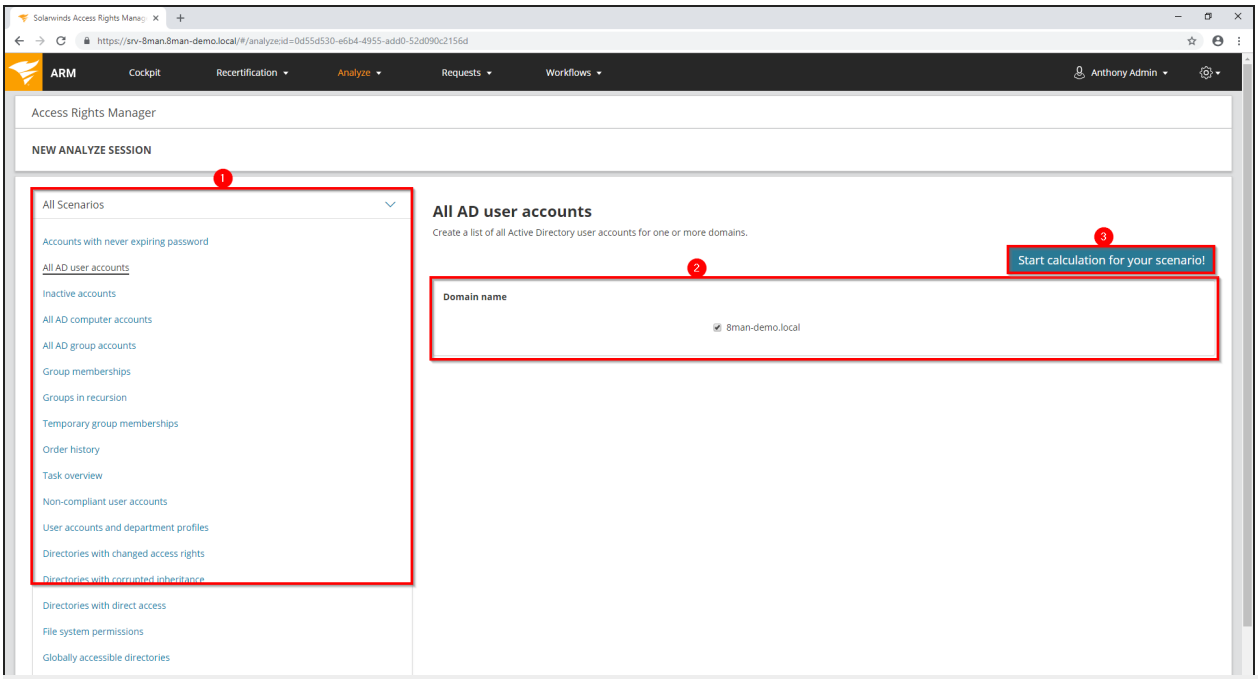
Background / Value

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.

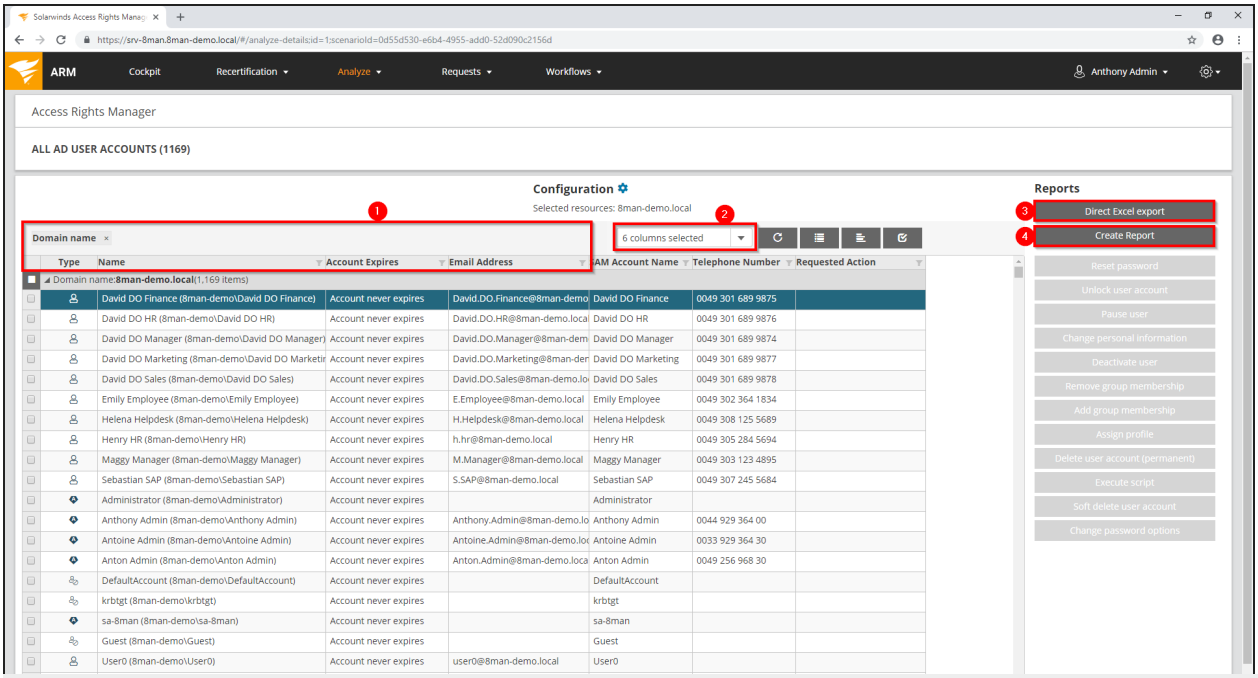
Step-by-step process



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?

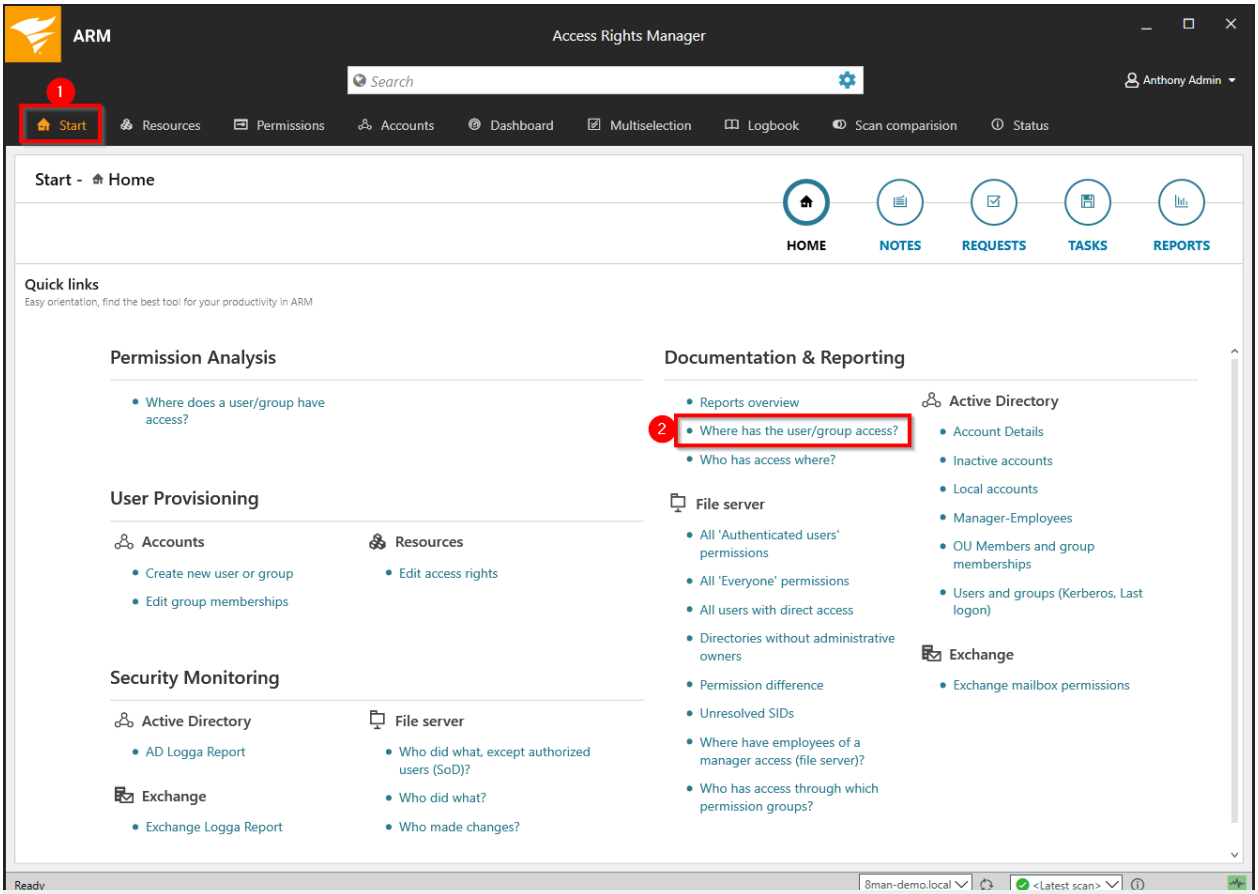
Background / Value

The report "Where has the user/group access?" lists all access rights of users and groups across **all** selected resources (user in focus).

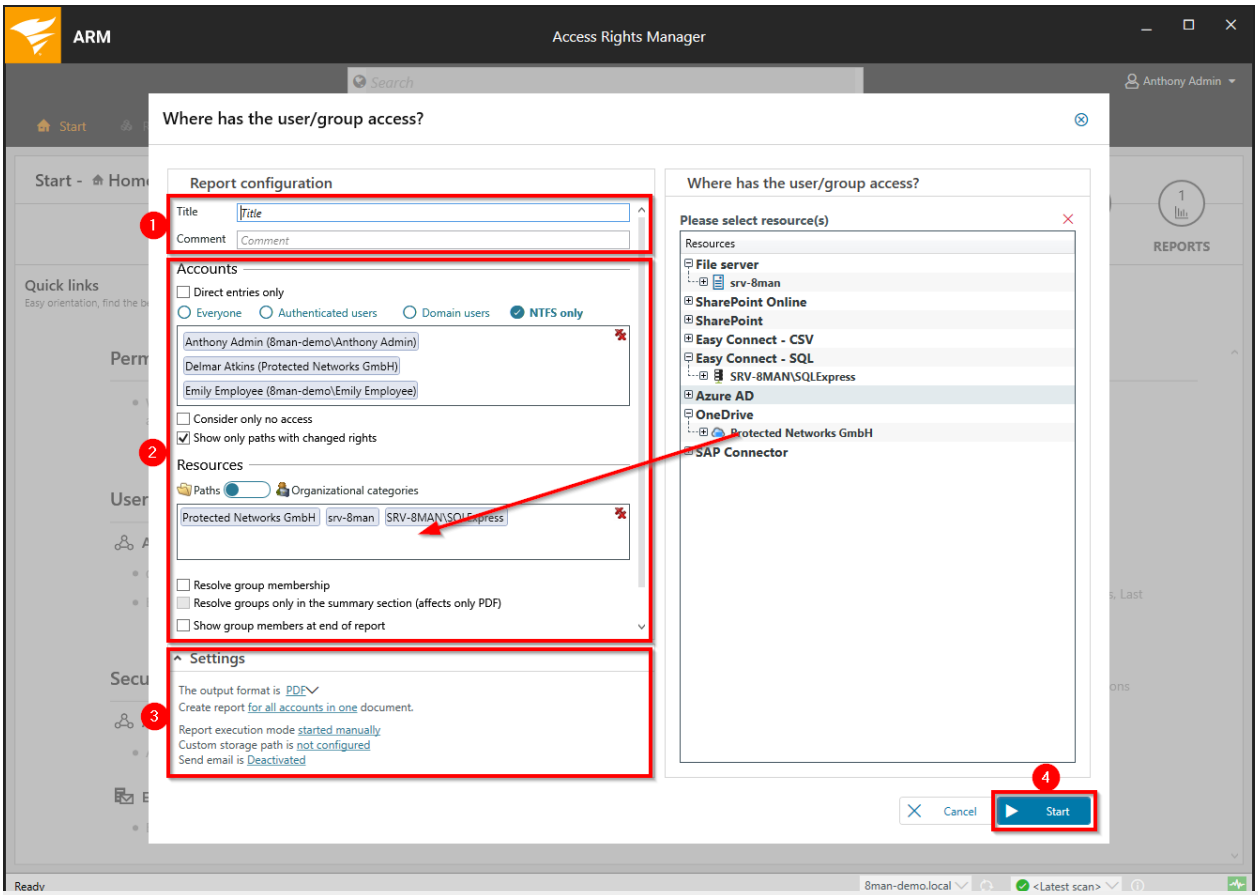
Related features

Report: Who has access where? (resource in focus)

Step-by-step process



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

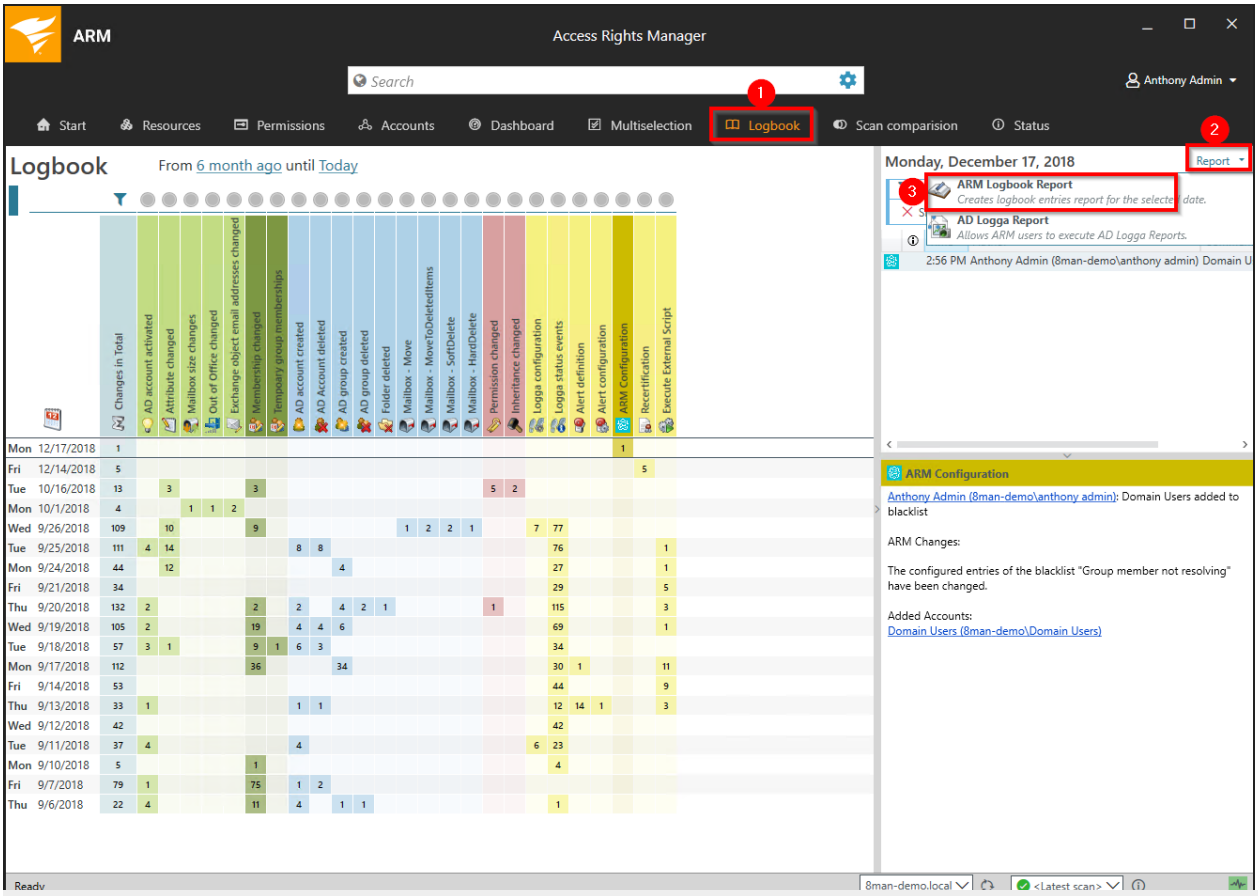
All changes made with ARM are automatically recorded in the log book. This ensures compliance with a number of legal and best-practice standards and saves the time of manual documentation. The log book report allows you to capture events by person or event type within any desired time period. This ensures fully transparent processes and documentation.

> 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

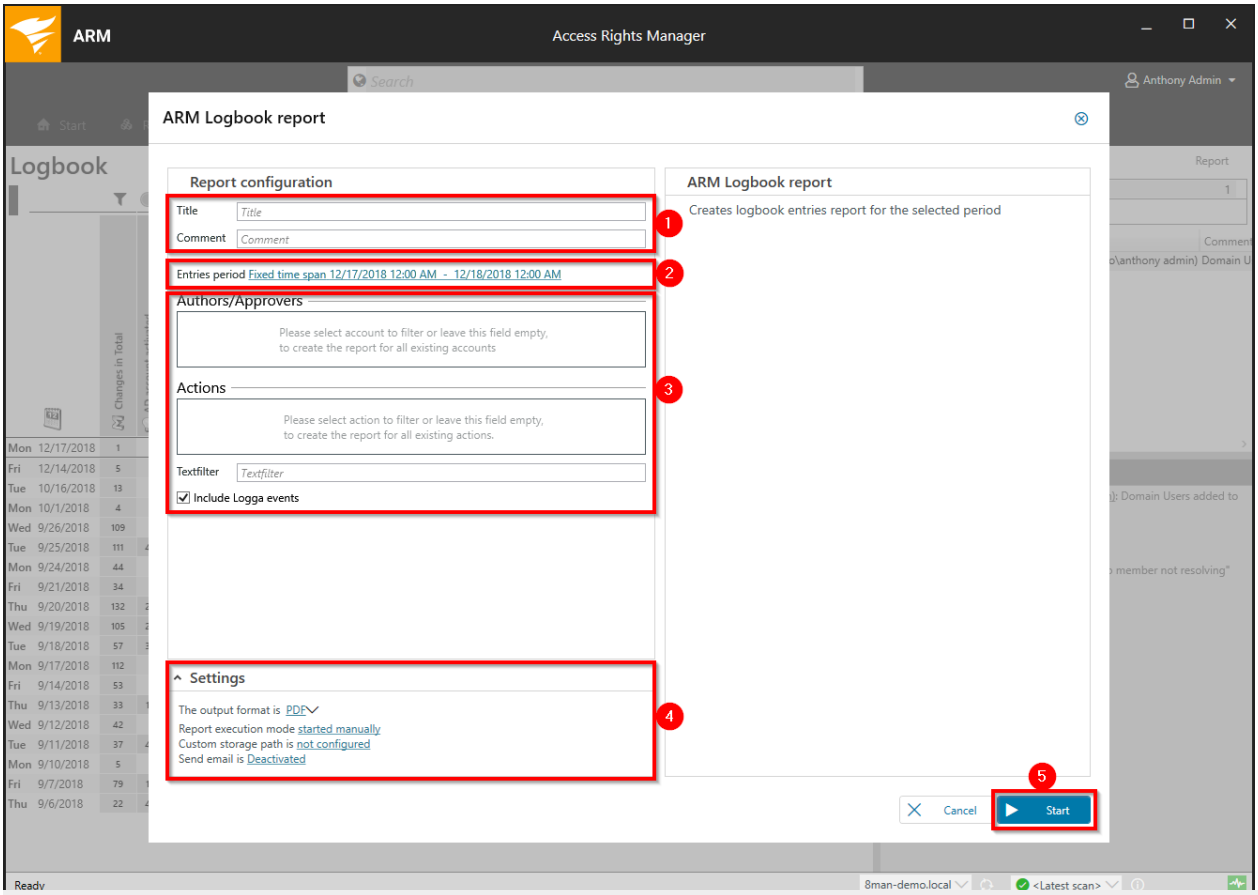
[FS Logga Report: Who did what?]

Step-by-step process



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.

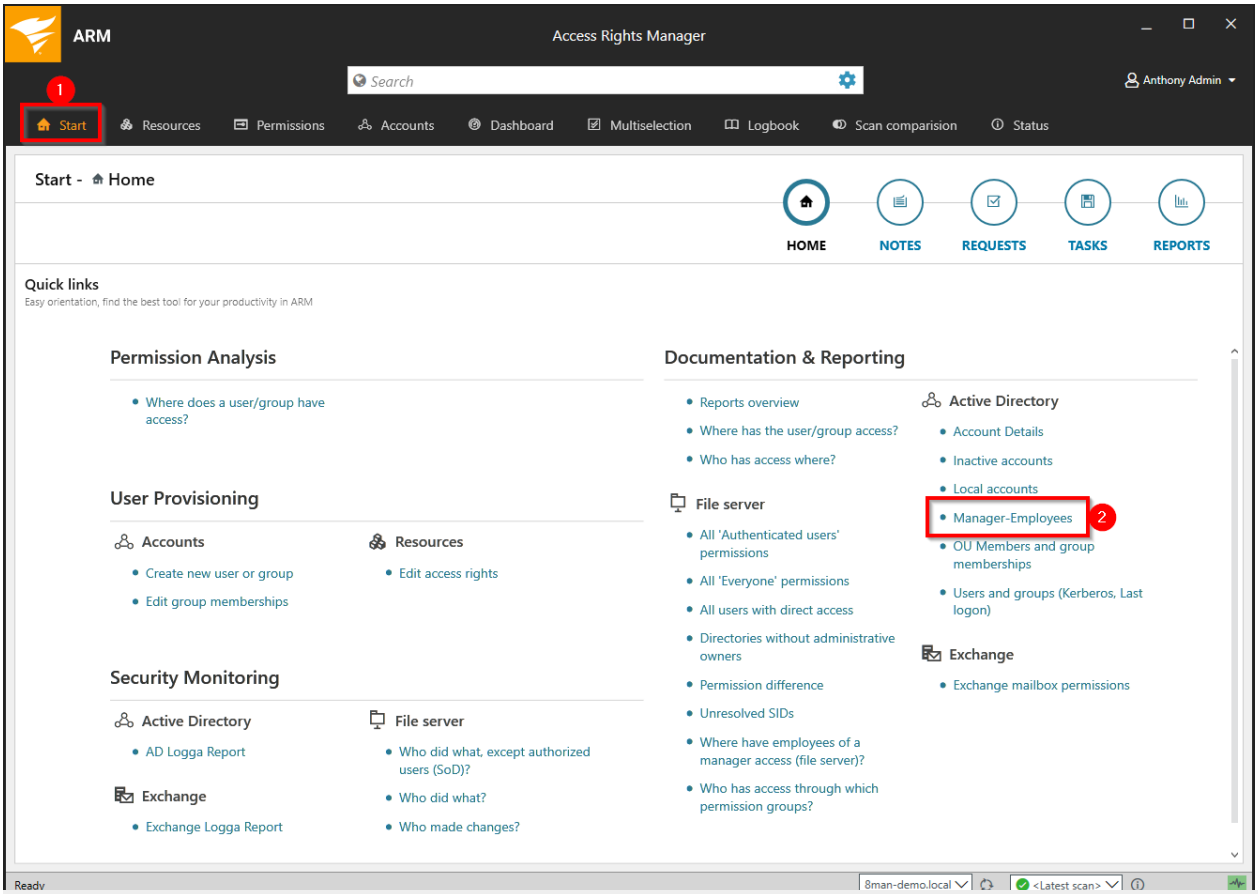
The report utilizes the attribute "manager" in Active Directory.

Related features

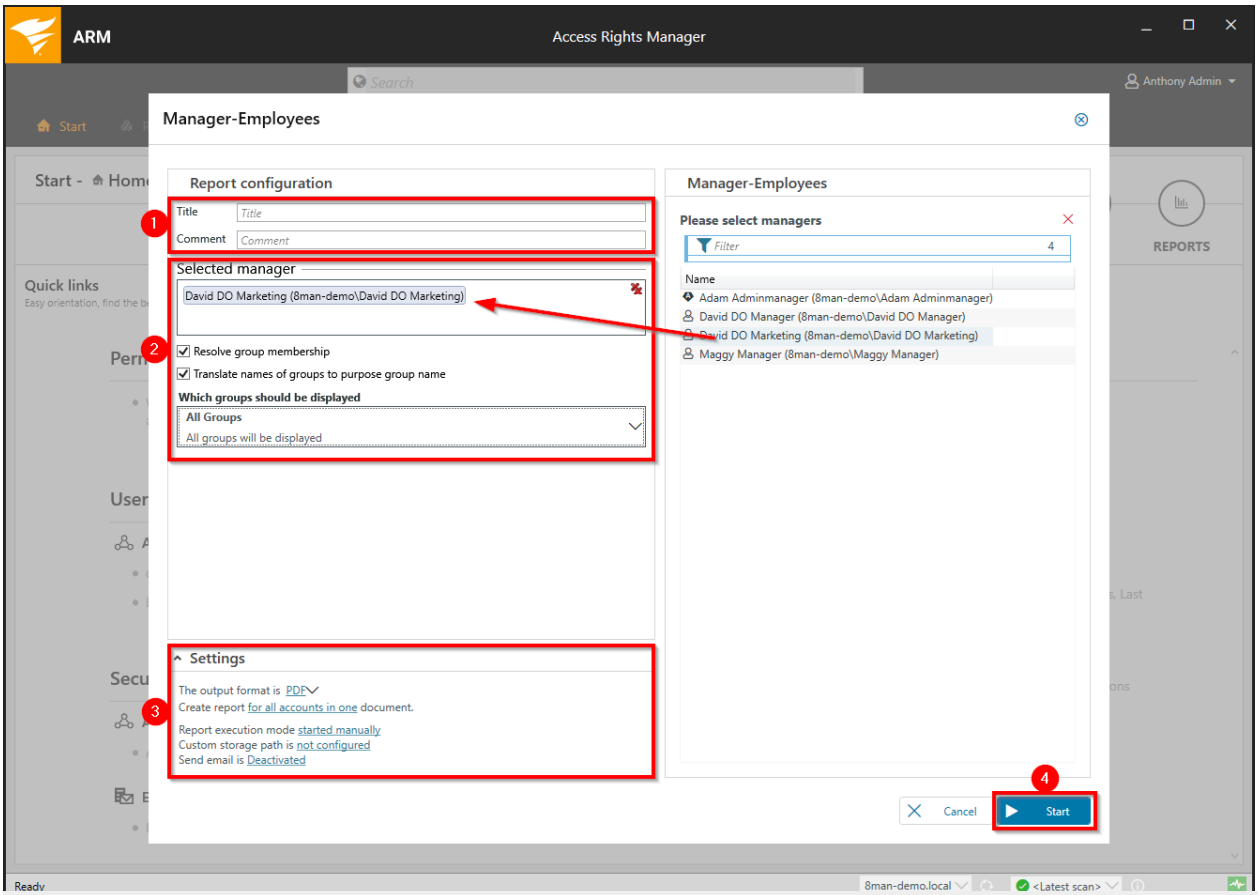
For more detailed information and the inclusion of assigned file server resources we recommend the report:

Where do employees of a manager have access (file server)?

Step-by-step process



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.

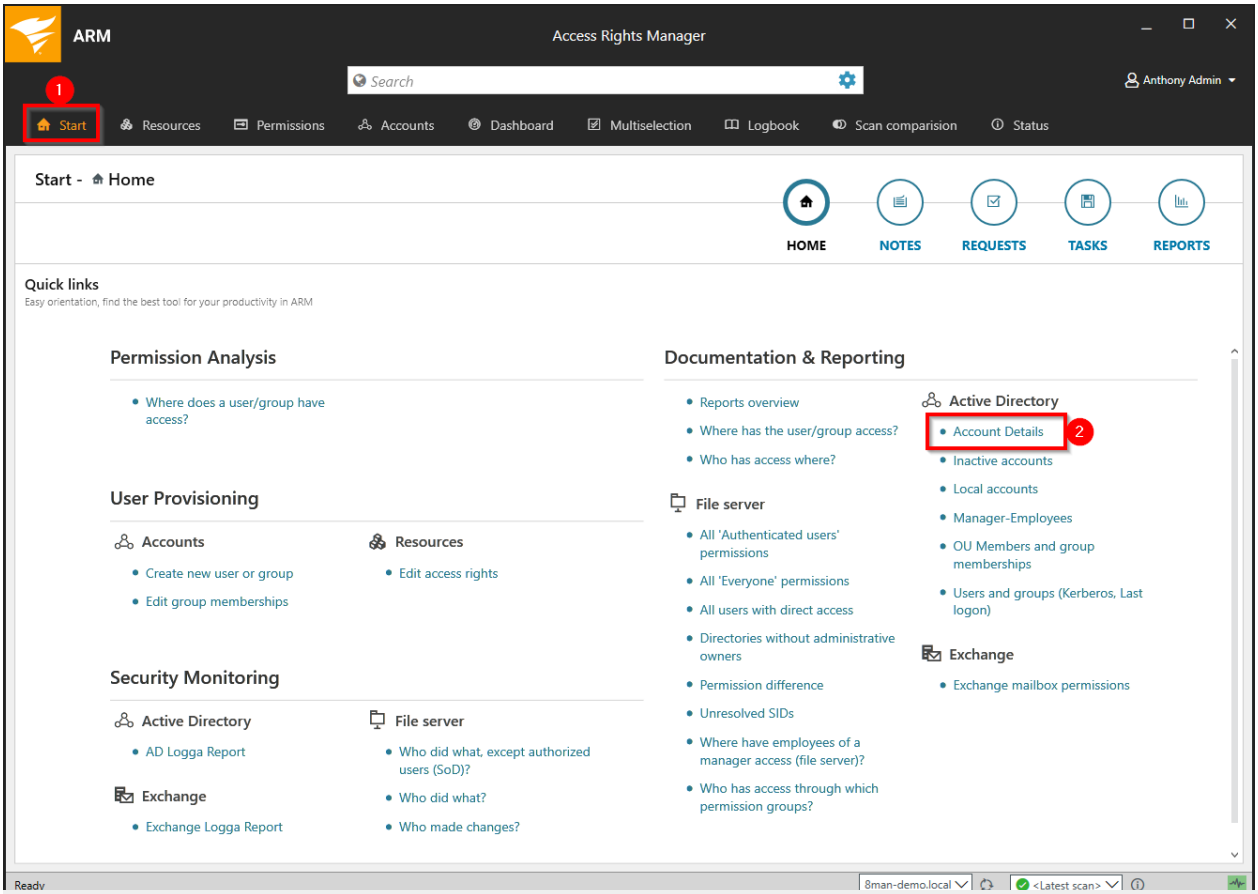
The following account details are shown in the report by default:

- 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

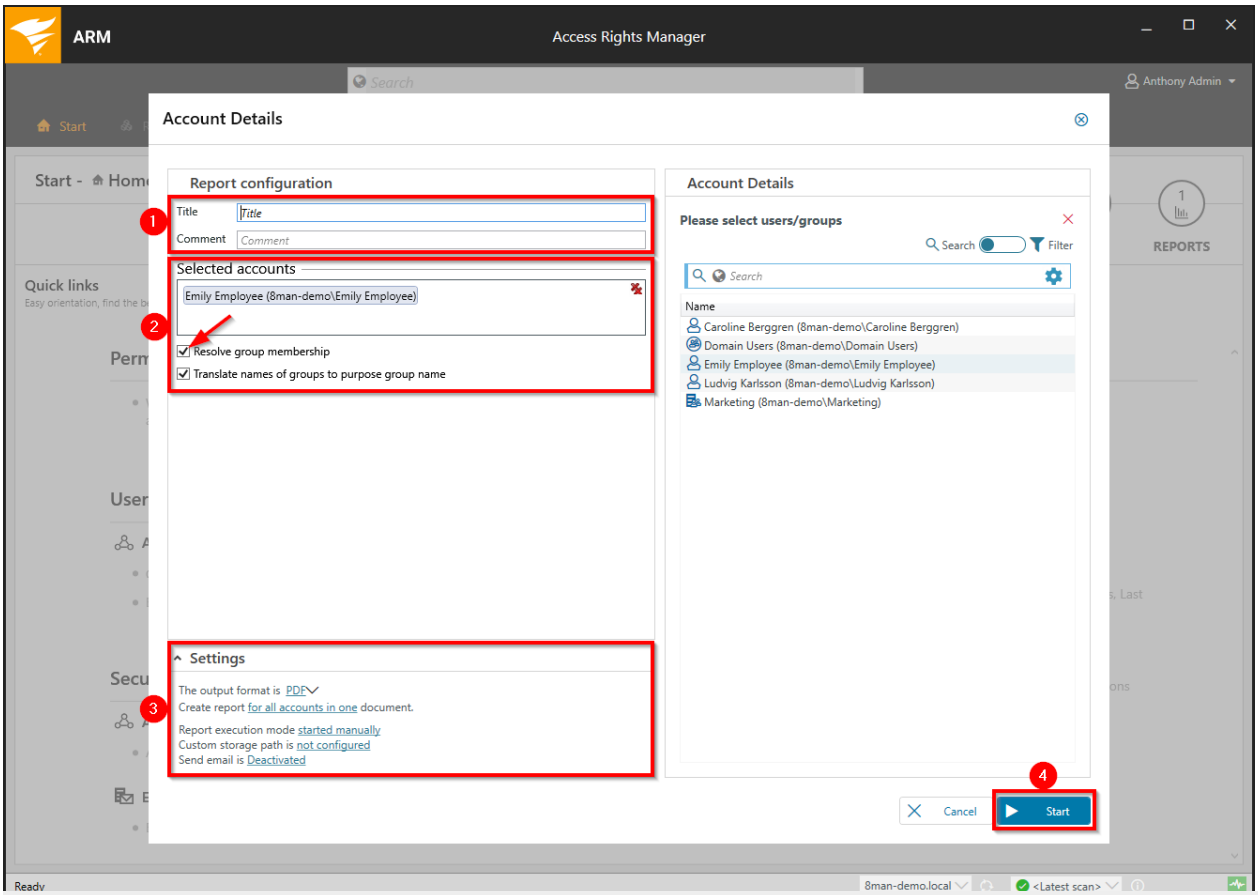
Related features

Report: OU members

Step-by-step process



1. Select "Start".
2. Click on "Account Details".



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

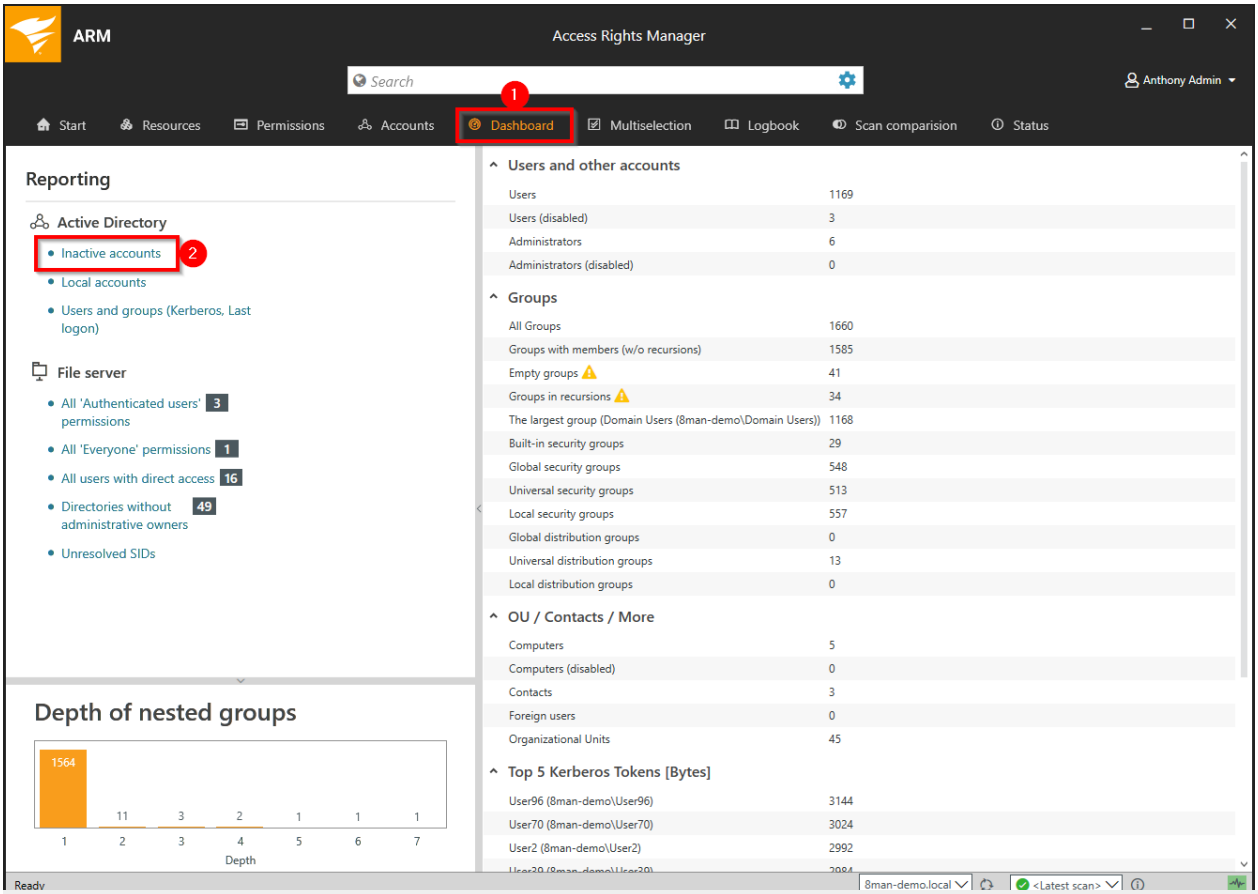
"Soft" delete a user account

Deactivate a user account

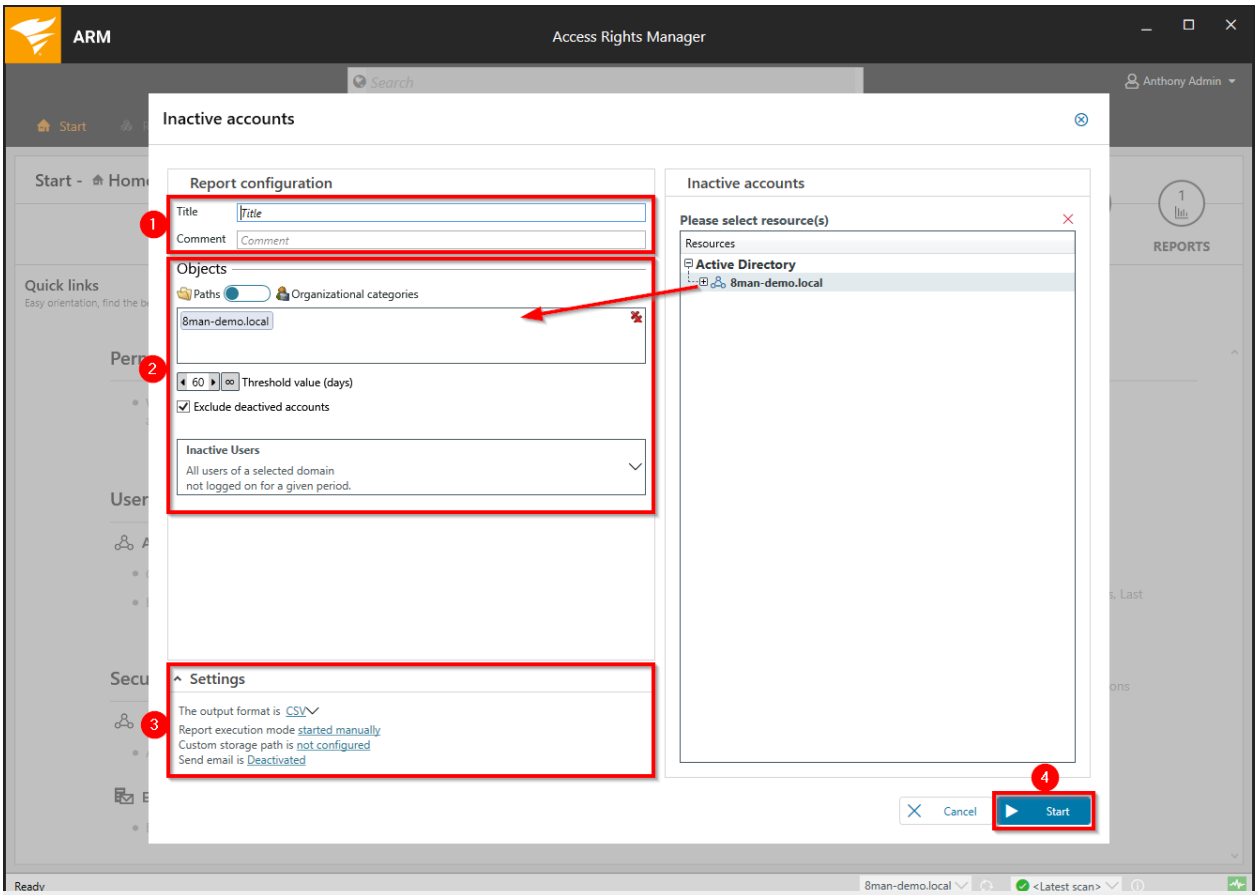
Identify inactive accounts (web client)

Deactivate user accounts in bulk (web client)

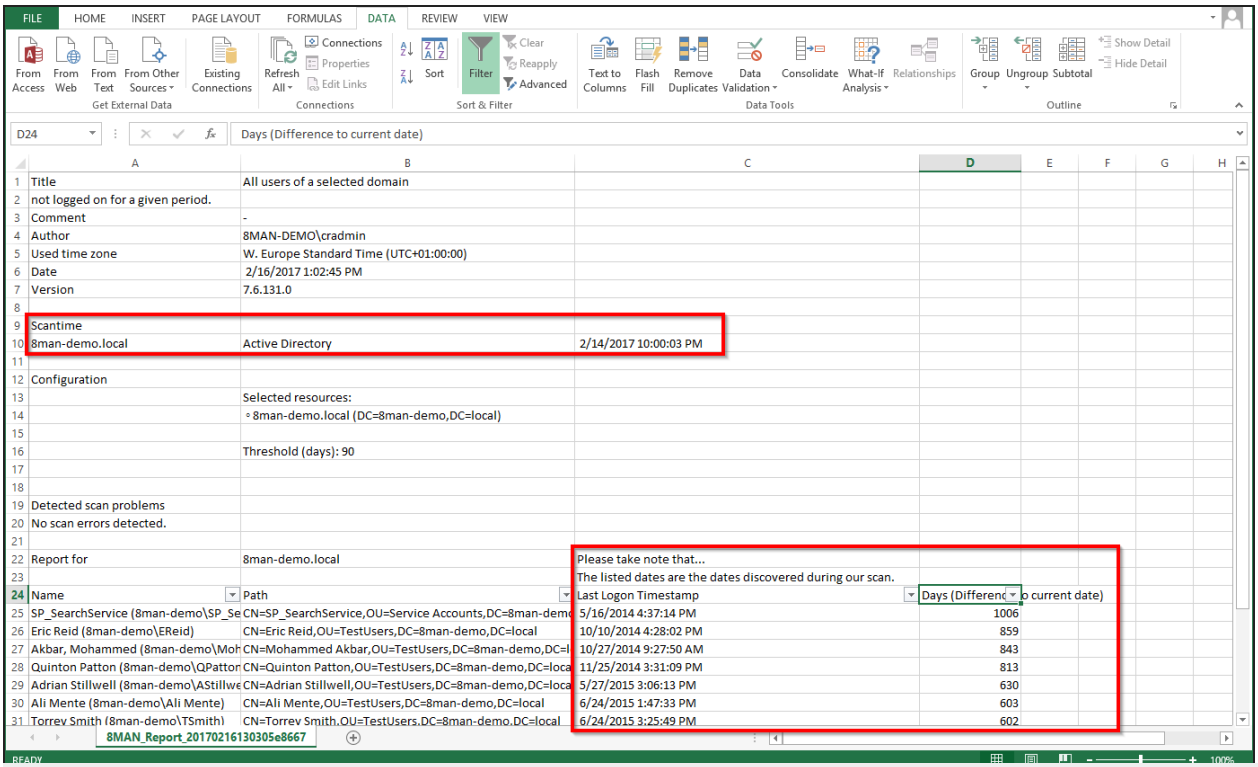
Step-by-step process



1. Select "Dashboard".
2. Click on "Inactive accounts".



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.



	A	B	C	D
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		
8				
9	Scantime			
10	8man-demo.local	Active Directory	2/14/2017 10:00:03 PM	
11				
12	Configuration			
13		Selected resources:		
14		◦ 8man-demo.local (DC=8man-demo,DC=local)		
15				
16		Threshold (days): 90		
17				
18				
19	Detected scan problems			
20	No scan errors detected.			
21				
22	Report for	8man-demo.local	Please take note that...	
23			The listed dates are the dates discovered during our scan.	
24	Name	Path	Last Logon Timestamp	Days (Difference to current date)
25	SP_SearchService (8man-demo\SP_Se	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\Moh	CN=Mohammed Akbar,OU=TestUsers,DC=8man-demo,DC=l	10/27/2014 9:27:50 AM	843
28	Quinton Patton (8man-demo\QPattor	CN=Quinton Patton,OU=TestUsers,DC=8man-demo,DC=loca	11/25/2014 3:31:09 PM	813
29	Adrian Stillwell (8man-demo\AStillwe	CN=Adrian Stillwell,OU=TestUsers,DC=8man-demo,DC=loca	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	Torrey Smith (8man-demo\TSmith)	CN=Torrey 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

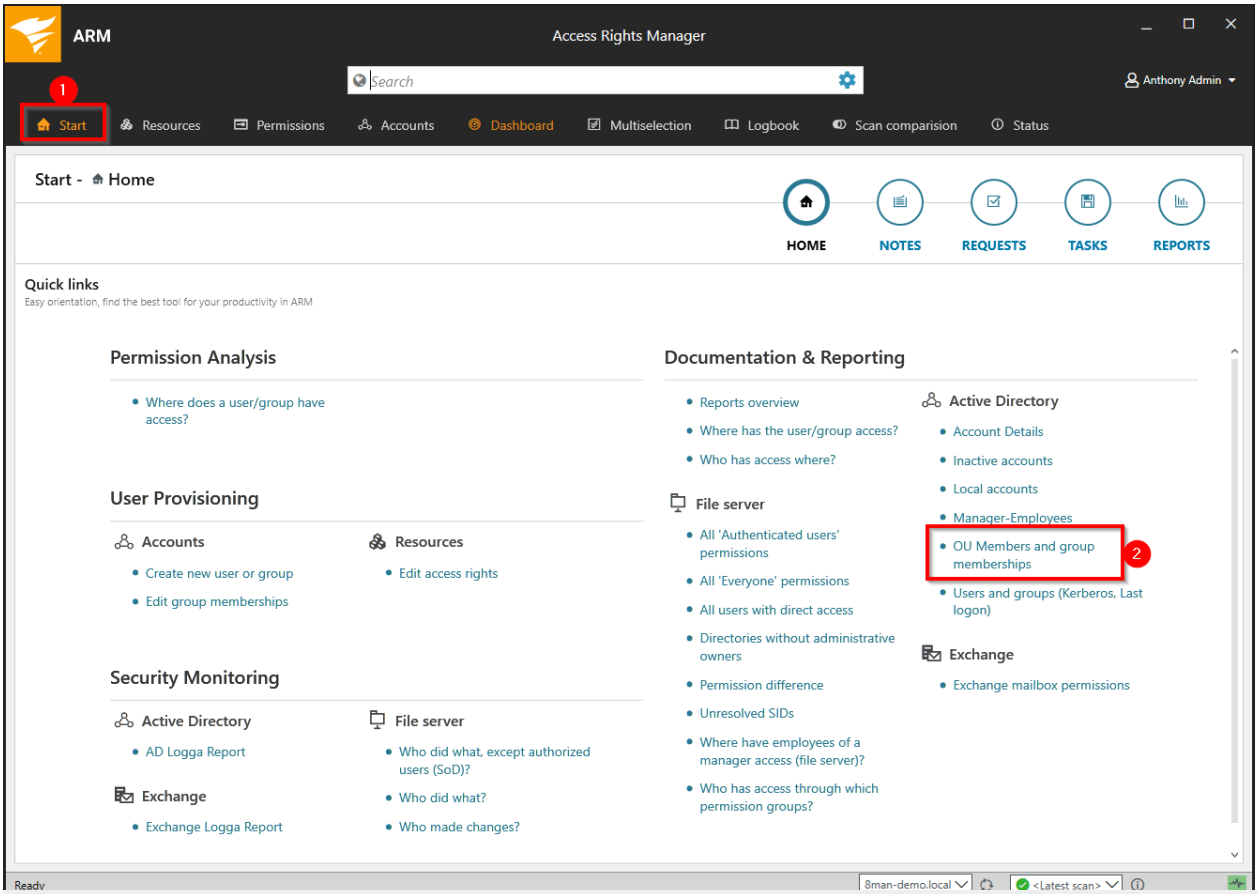
Background / Value

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.

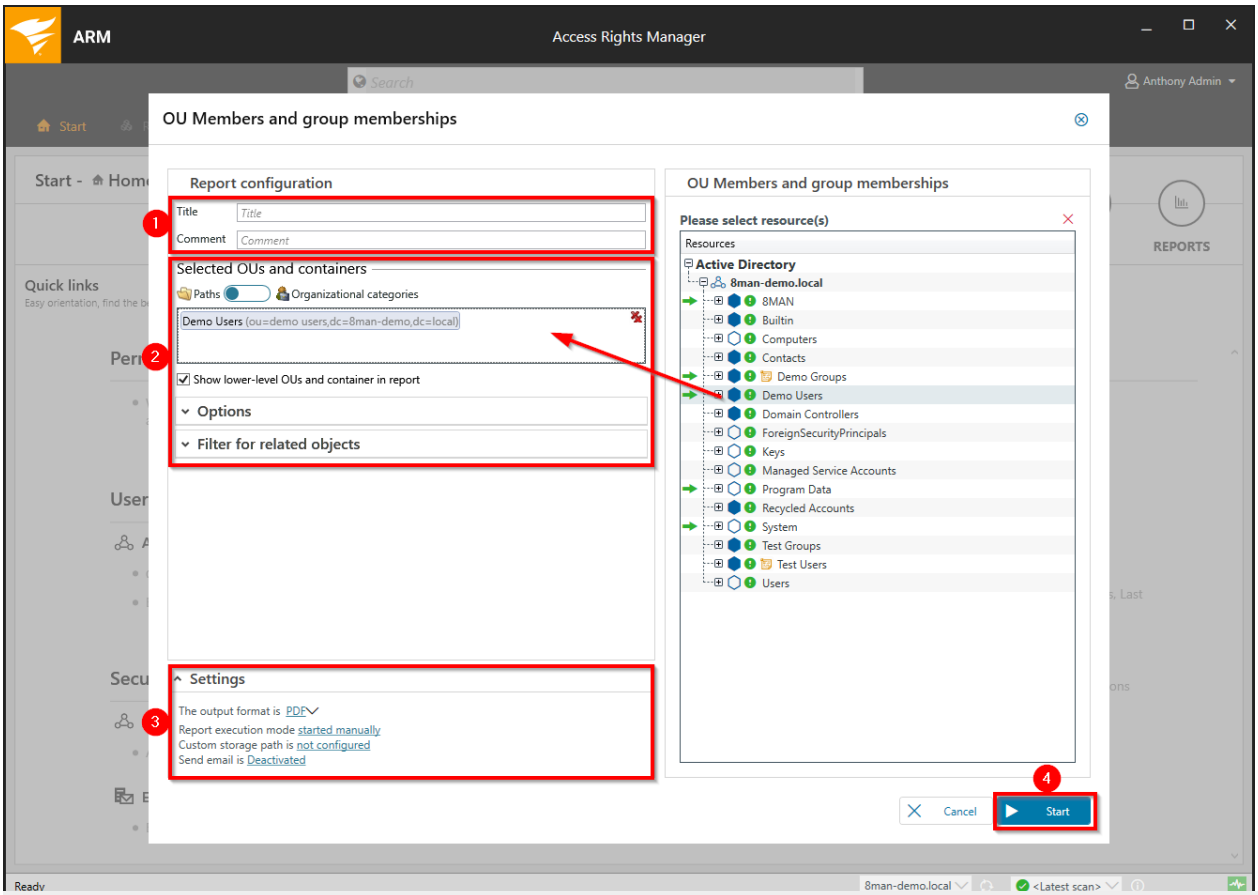
Related features

Group memberships and account details

Step-by-step process



1. Select "Start".
2. Click on "OU members and group memberships".



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.

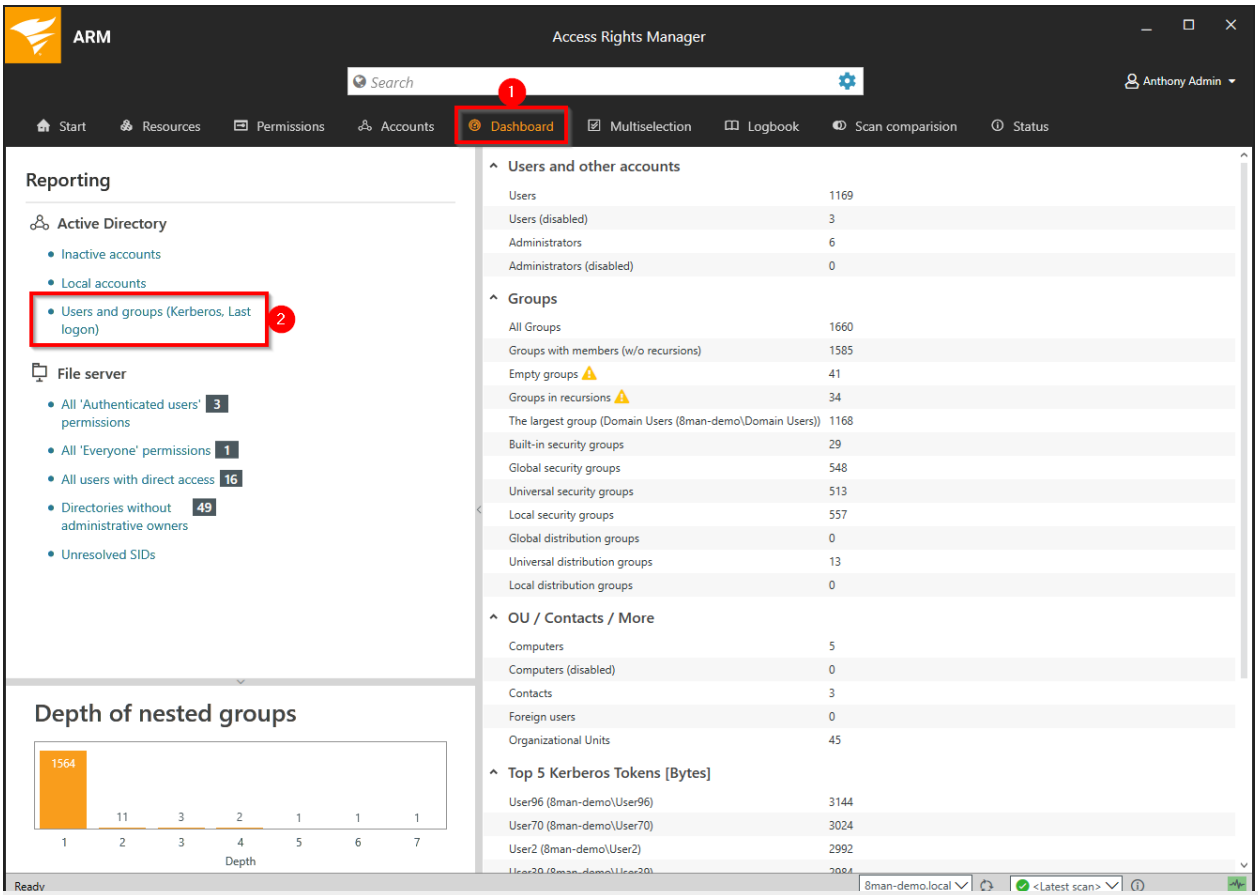
In addition the following information is also displayed:

- Account expiry date
- Password expires yes/no
- Admin account yes/no

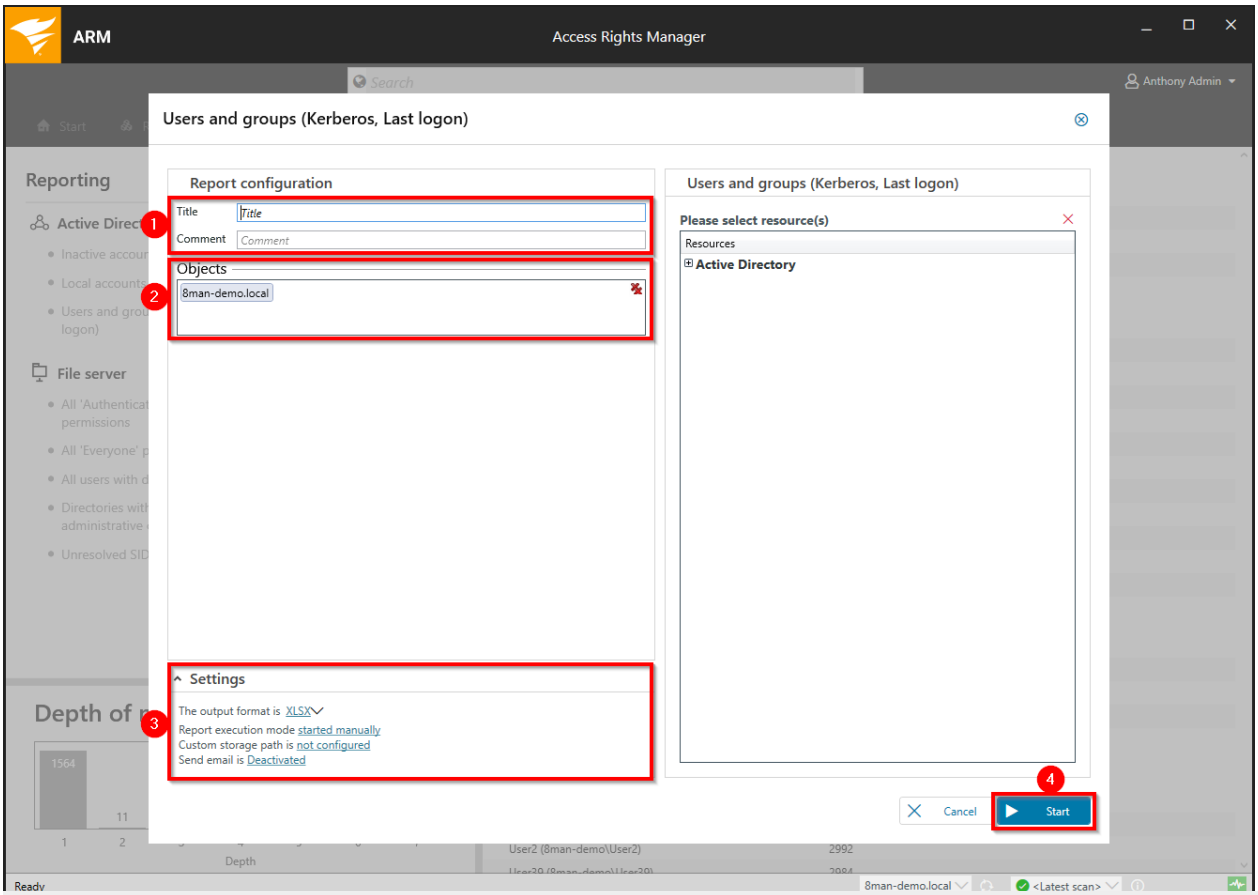
Groups

Displays direct and indirect group membership count as well as group scope (local, global, universal)

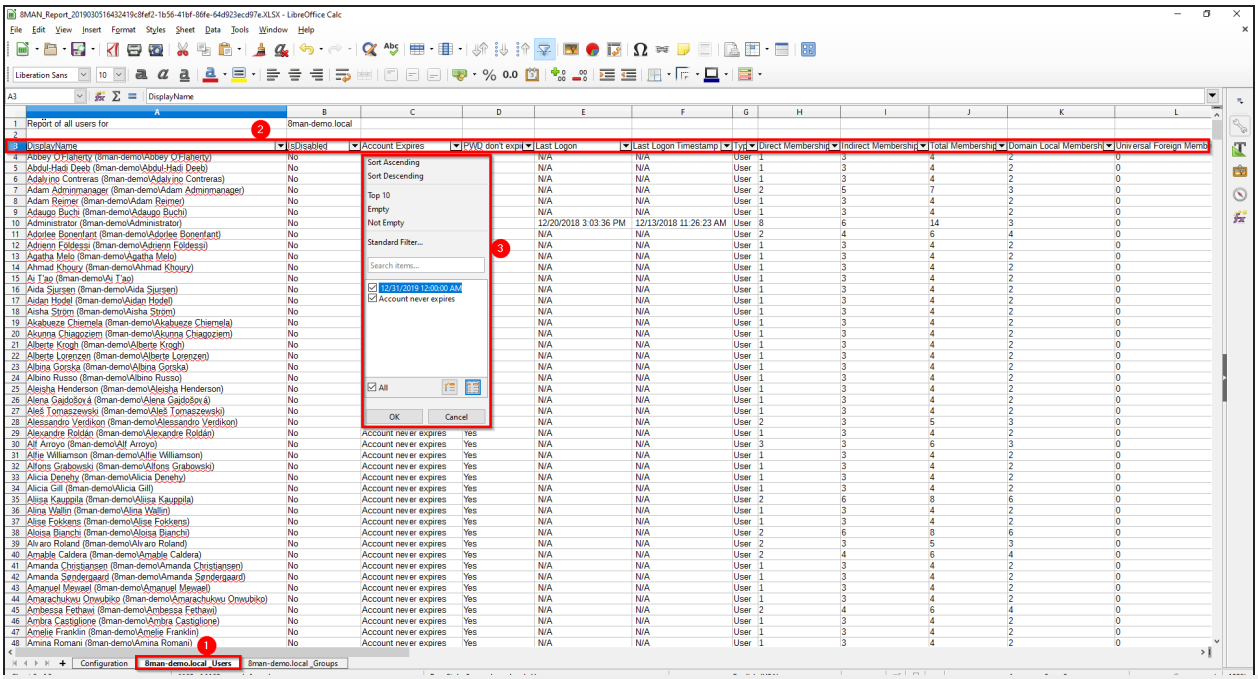
Step-by-step process



1. Select "Dashboard".
2. Click on "Users and groups".

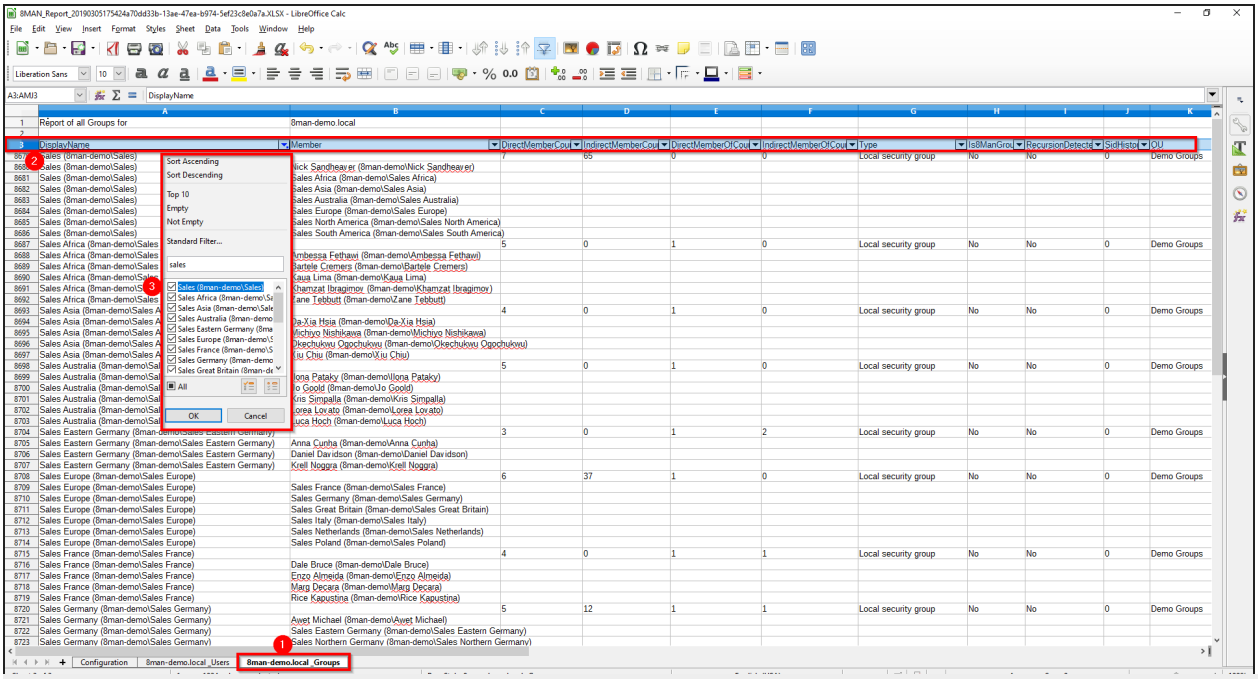


1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired output settings.
4. Start the report.



Open the report in your spread sheet 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

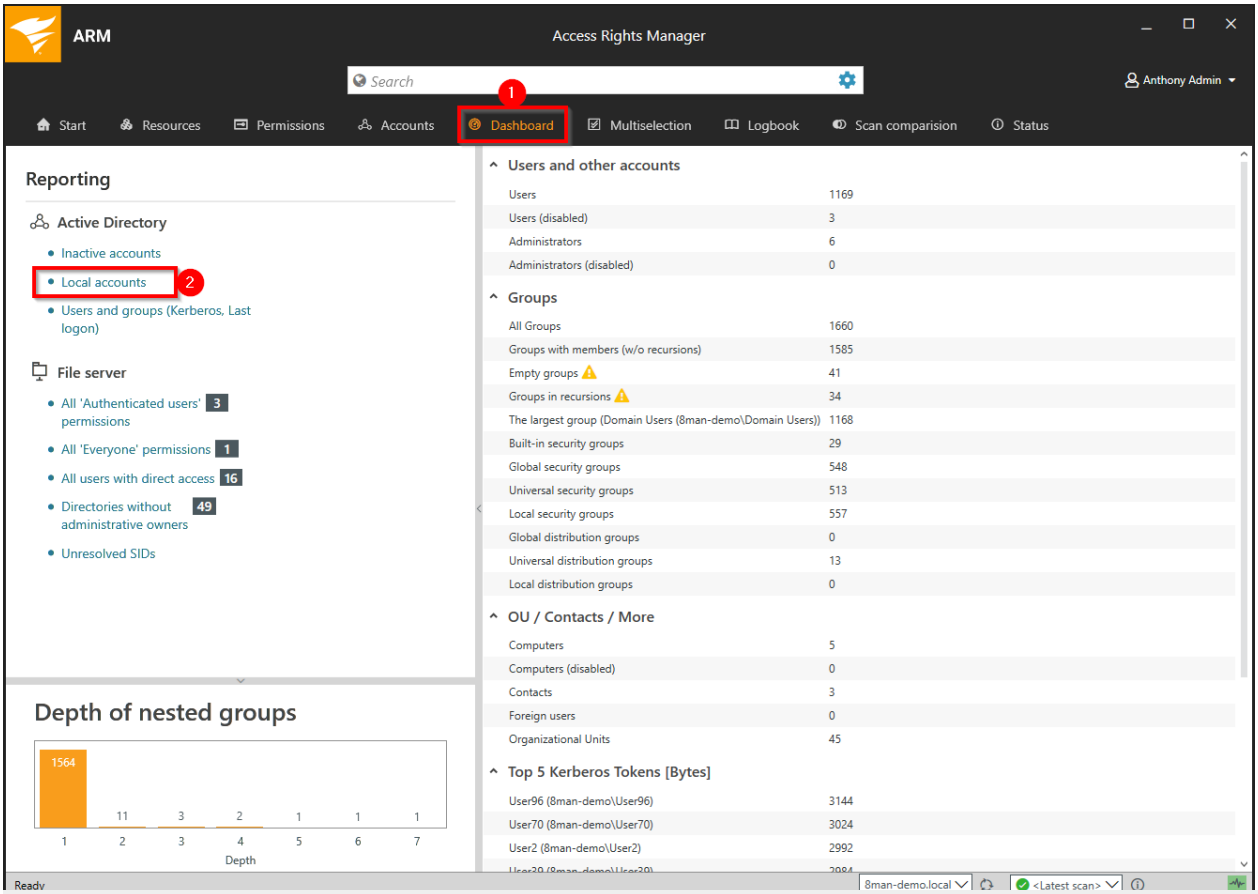
The local account report displays local administrative rights on end points. This way you can see which administrators and users have access to which end point. In this scenario the principle of "least privilege" applies. The report thereby gives you a complete picture regarding access rights in your organization as local accounts are not visible through AD group memberships.

This report can only show results if you have configured local accounts scans.

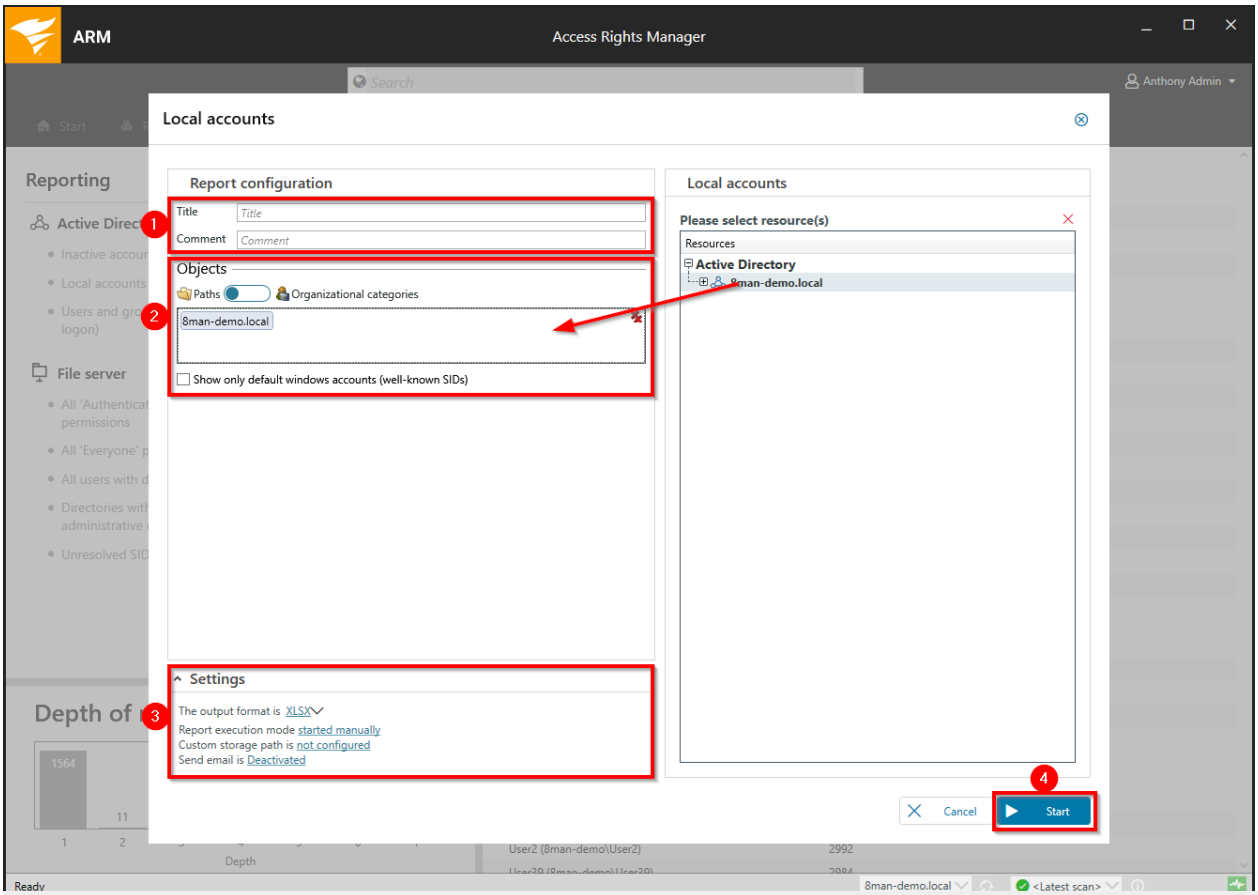
Related features

Scan local accounts (configuration)

Step-by-step process



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.

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

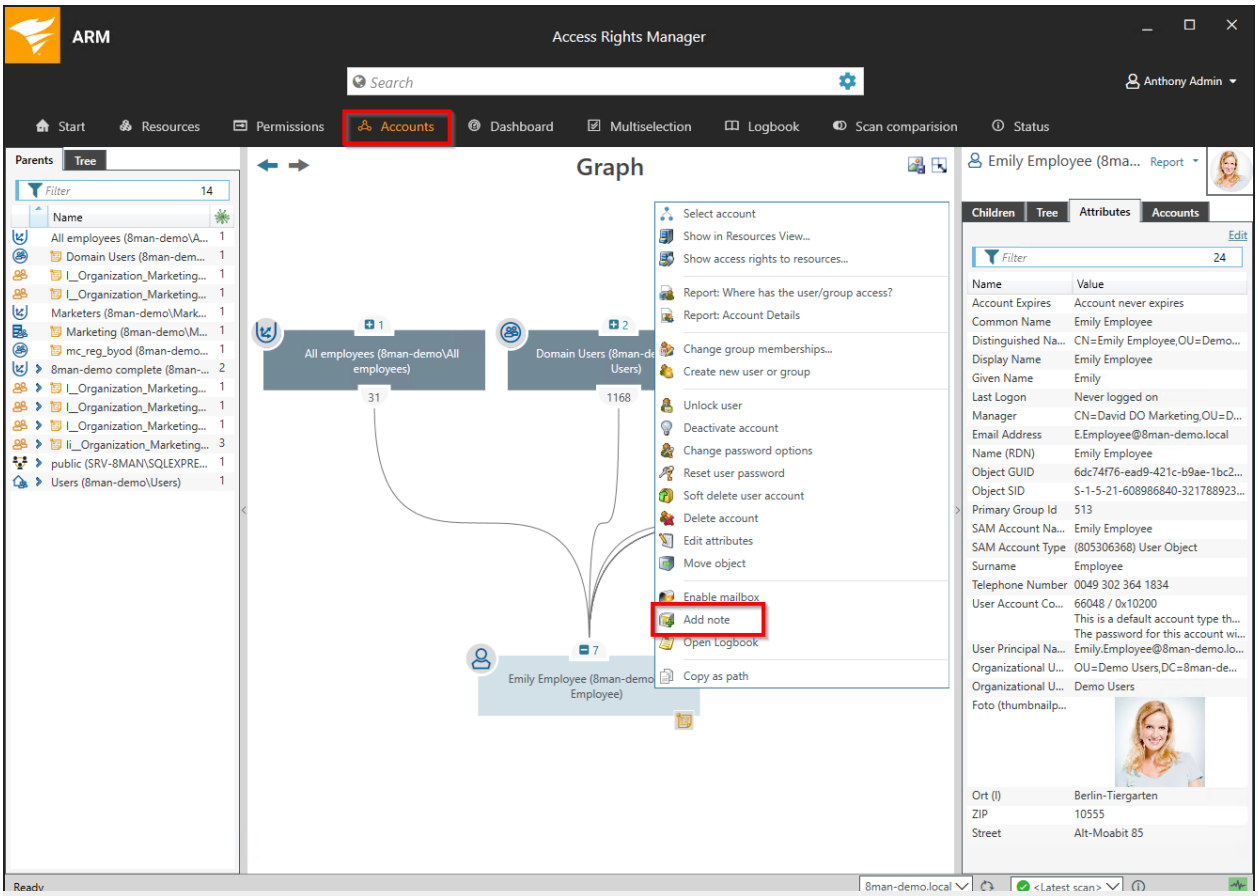
Besides automated documentation and reports ARM also includes a number of additional documentation features. These allow you to add post-its to objects manually or give AD groups aliases with the "purpose groups" feature.

Add notes to user accounts and groups

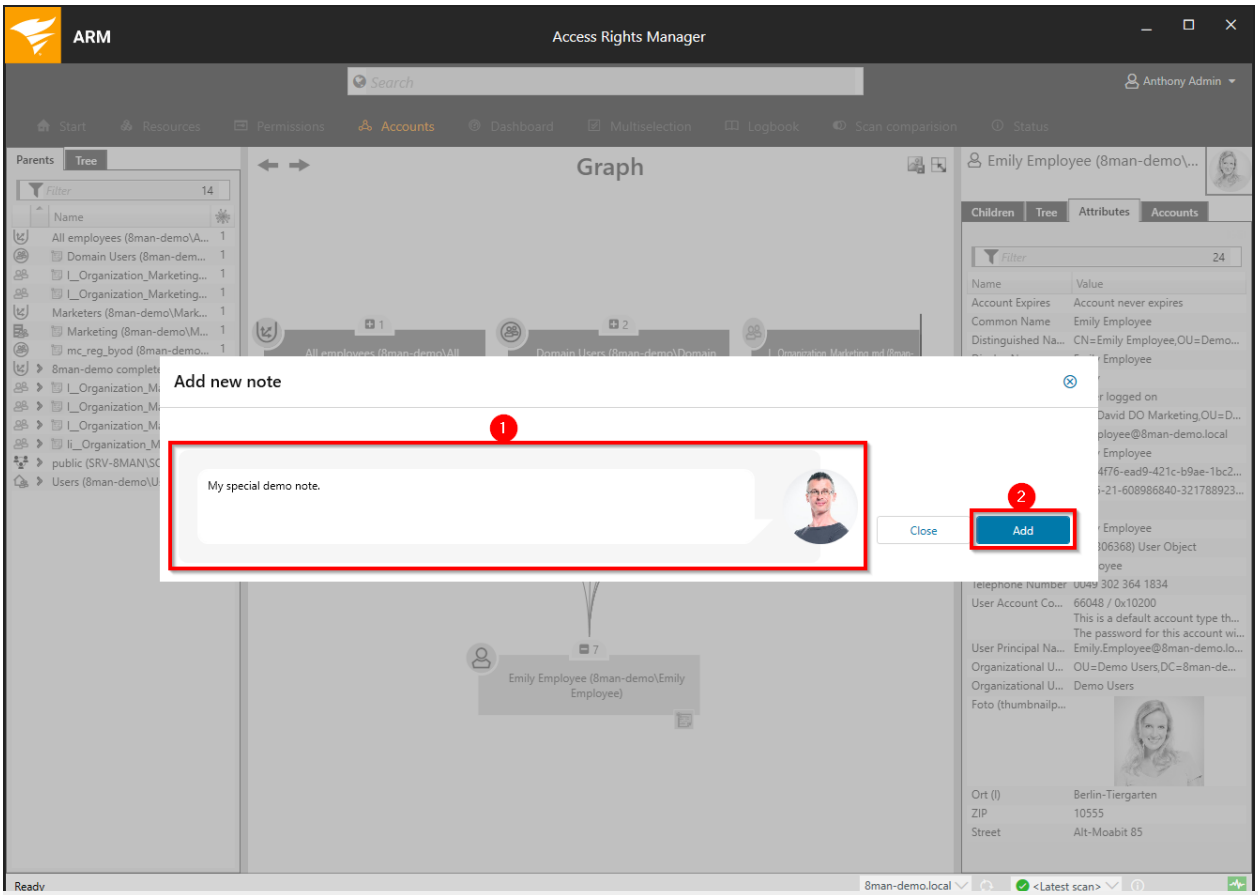
Background / Value

Flag user and group accounts with post-its. This allows you to add tasks directly to individual objects.

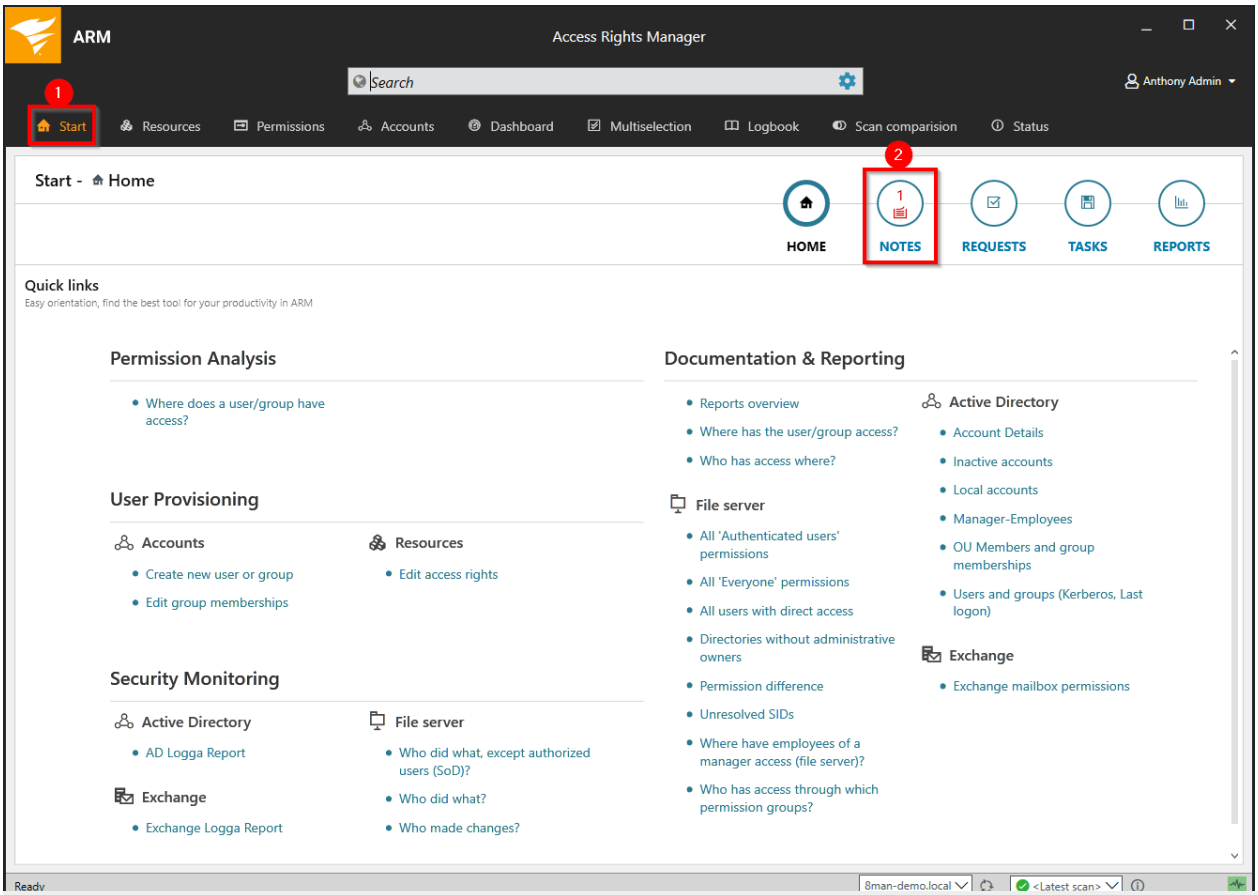
Step-by-step process



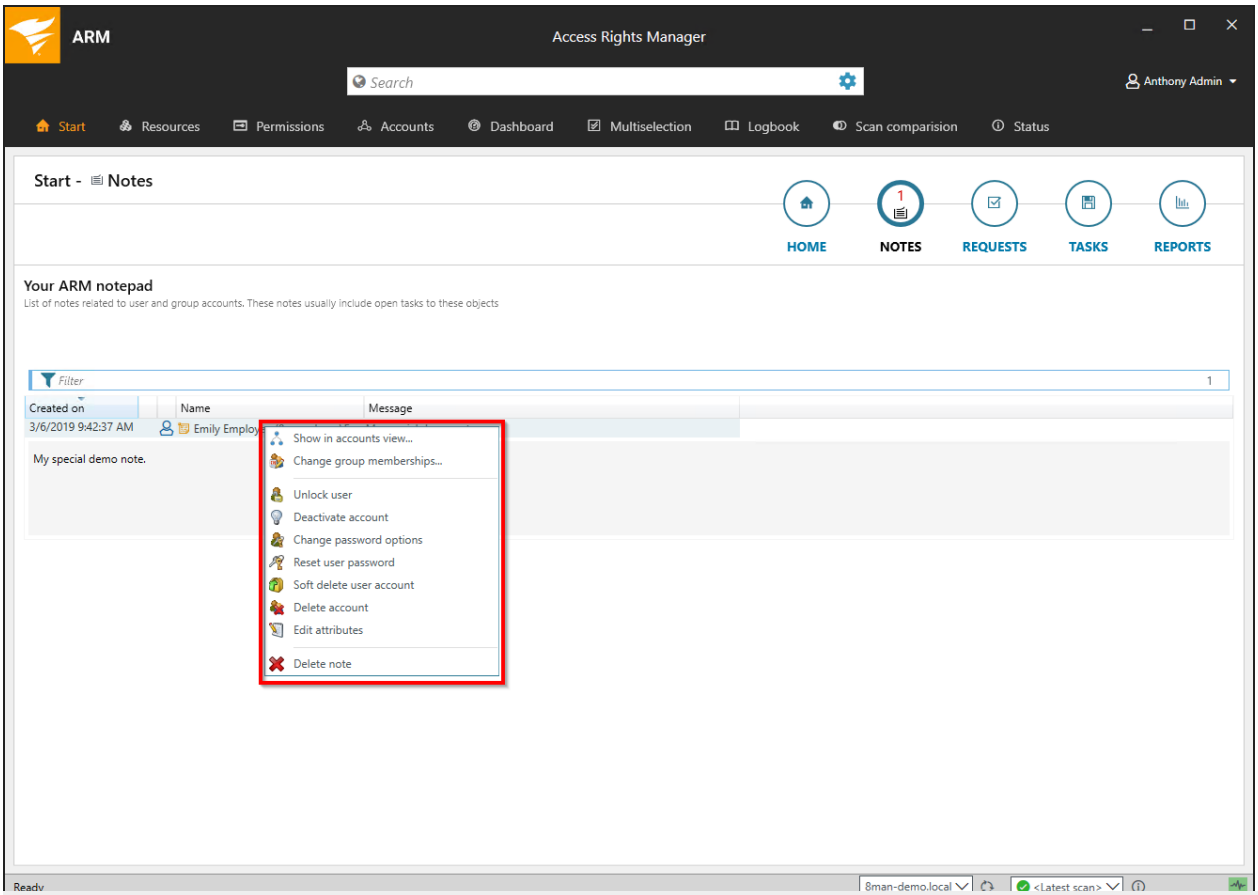
Right-click on an account and select "Add note" from the context menu.



1. Add a note.
2. Click "Add".



1. Select "Start".
2. Click "Notes".



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

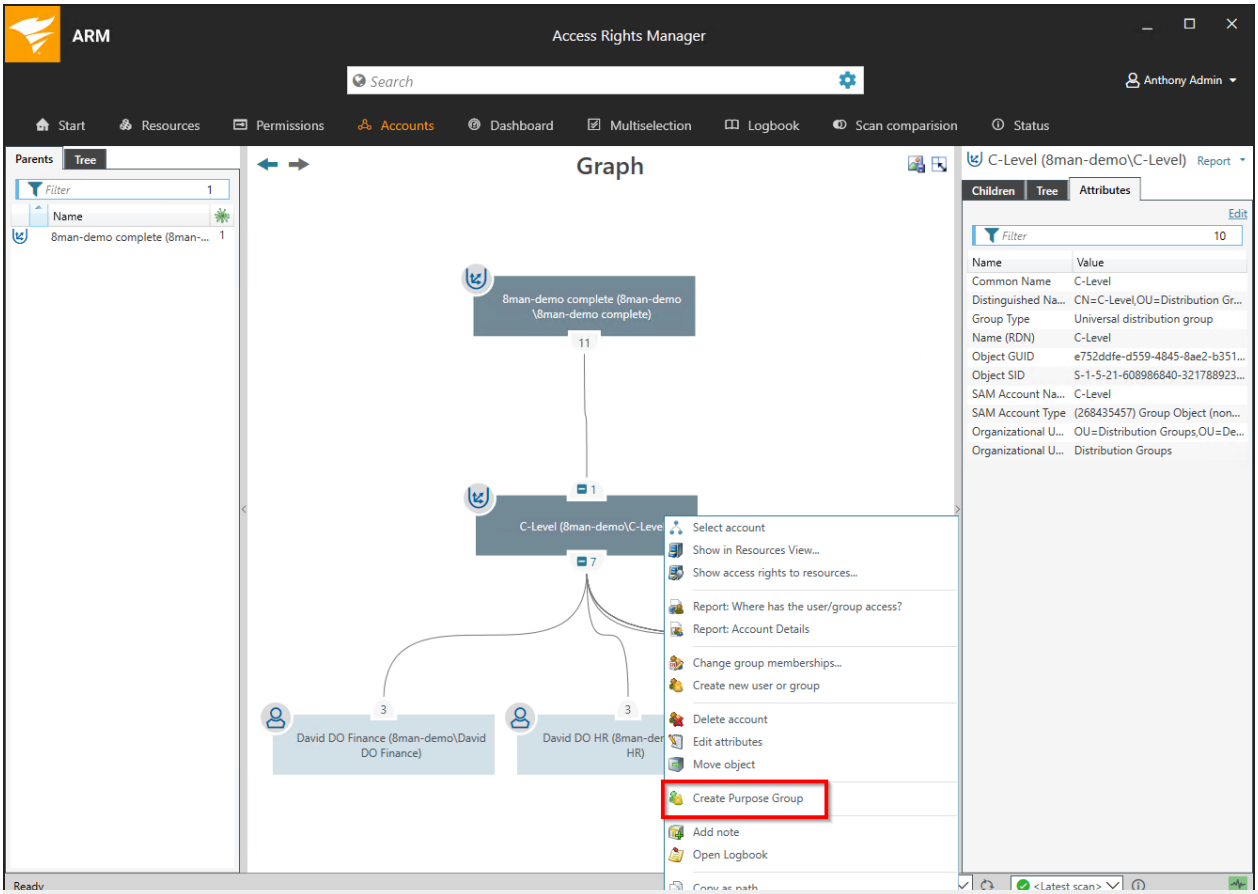
Background / Value

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.

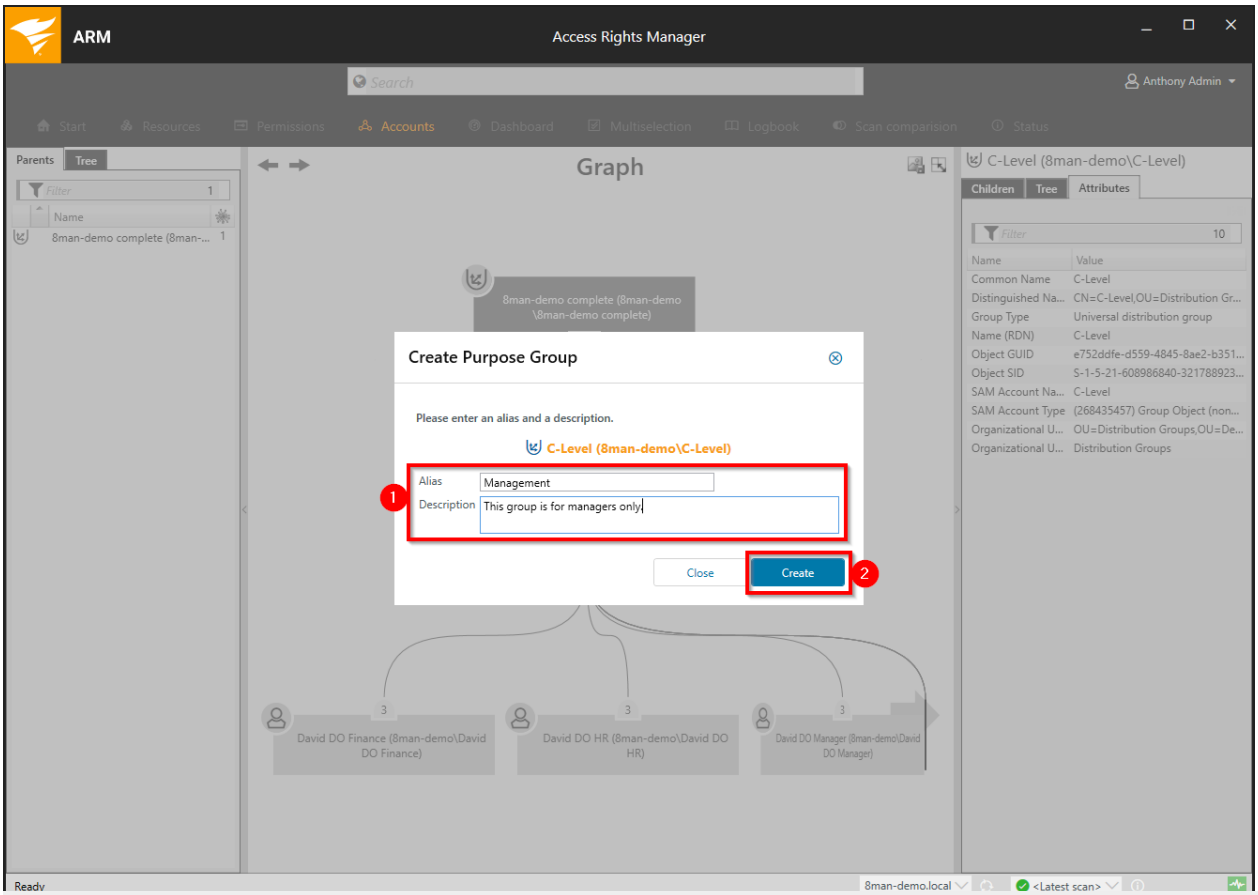
The alias descriptions are only visible in the ARM views and reports. There are no changes to Active Directory attributes.

Create a purpose group

Step-by-step process



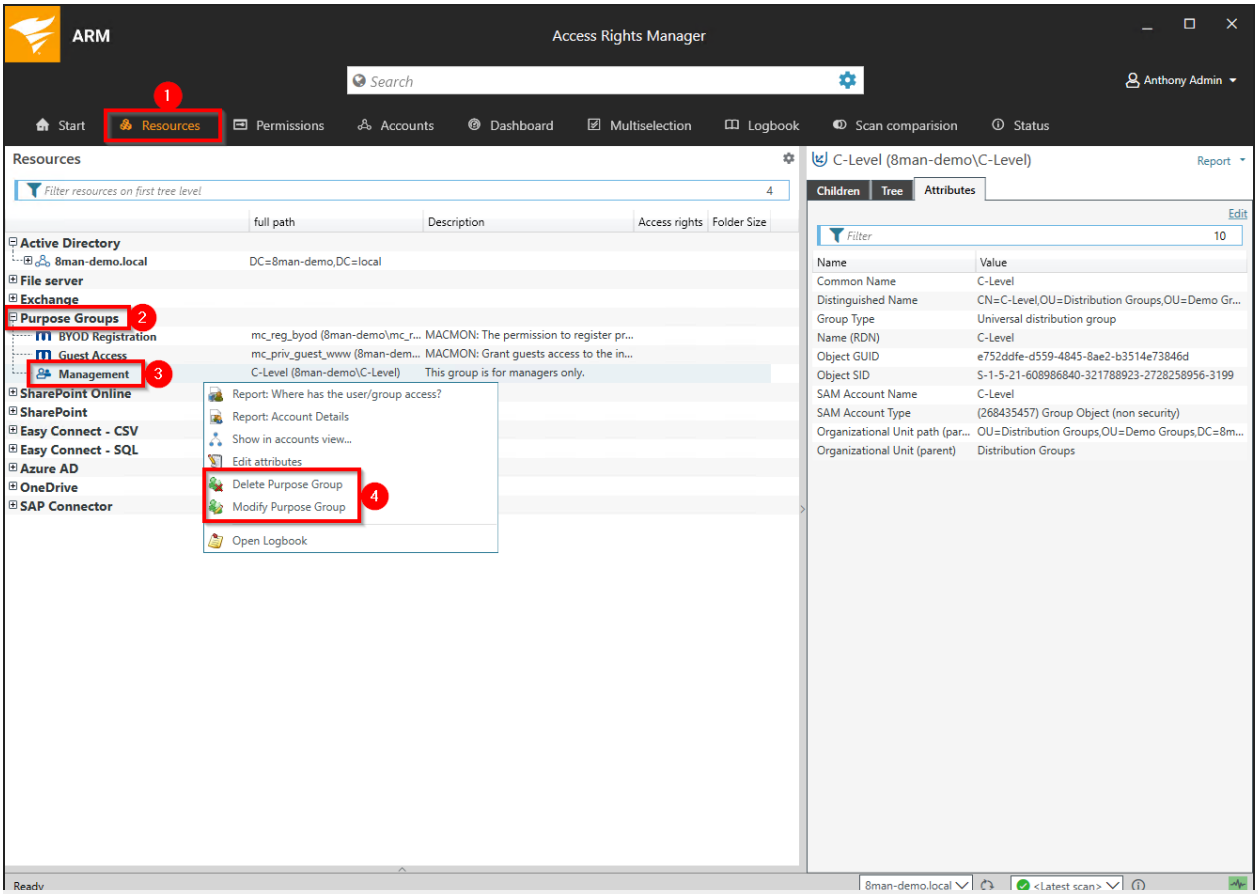
Right-click on an AD group. Select "Create Purpose Group" from the context menu.



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



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.

The removal process only affects the purpose group, the added alias in ARM. No changes are made to Active Directory.

File server

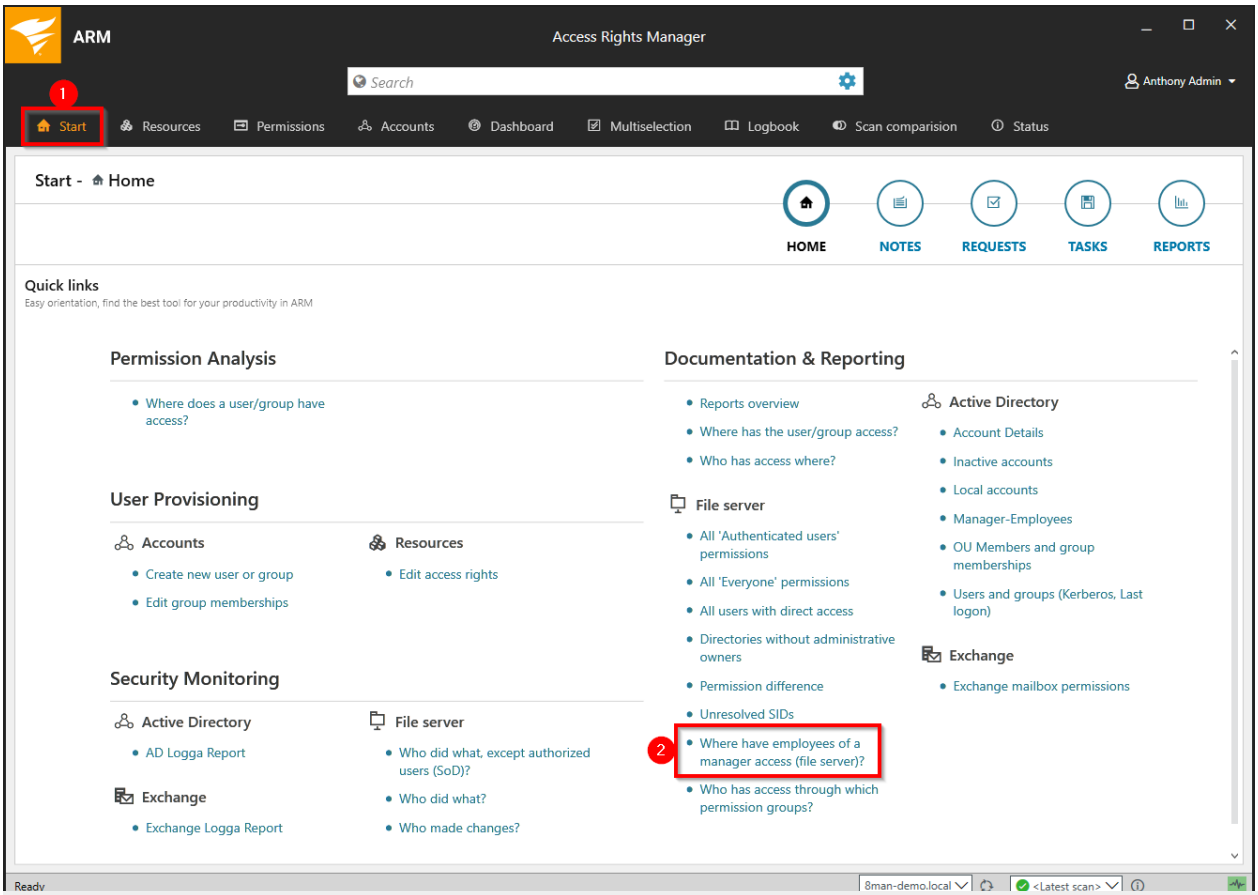
ARM lets you create easy to read reports on file server permissions and security risks.

Where do employees of a manager have access?

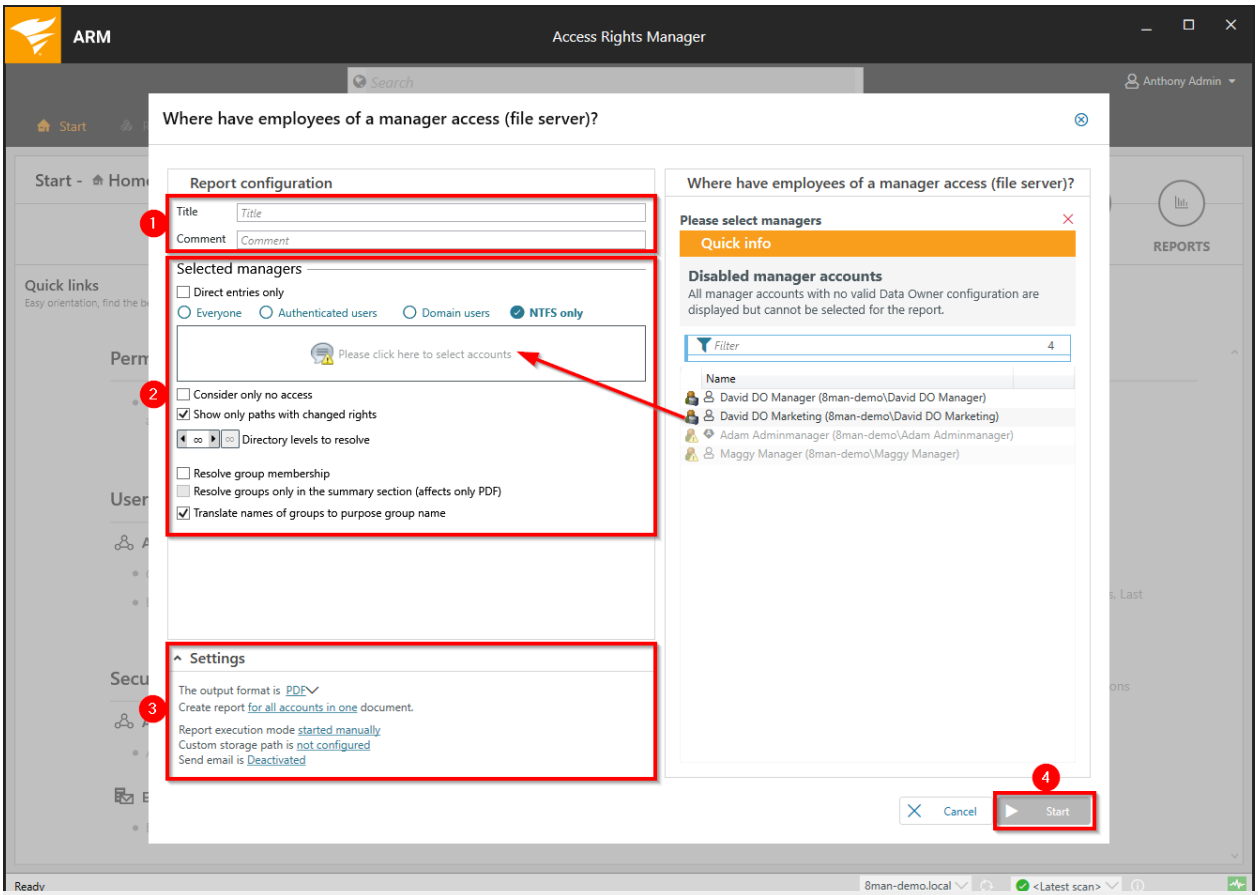
Background / Value

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



1. Select "Start".
2. Click on "Where have employees of a manager access (file server)" .



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.

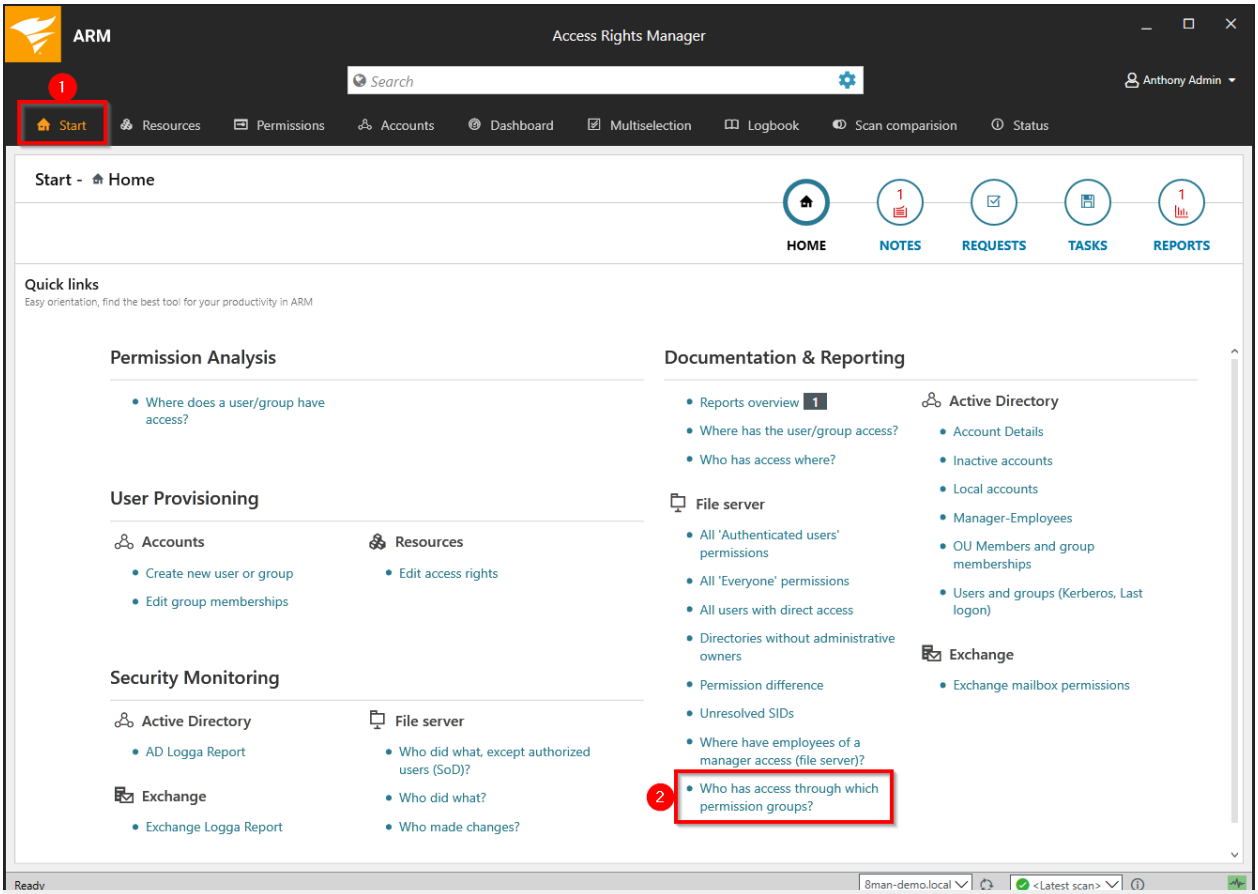
Who has access through which permission groups?

Background / Value

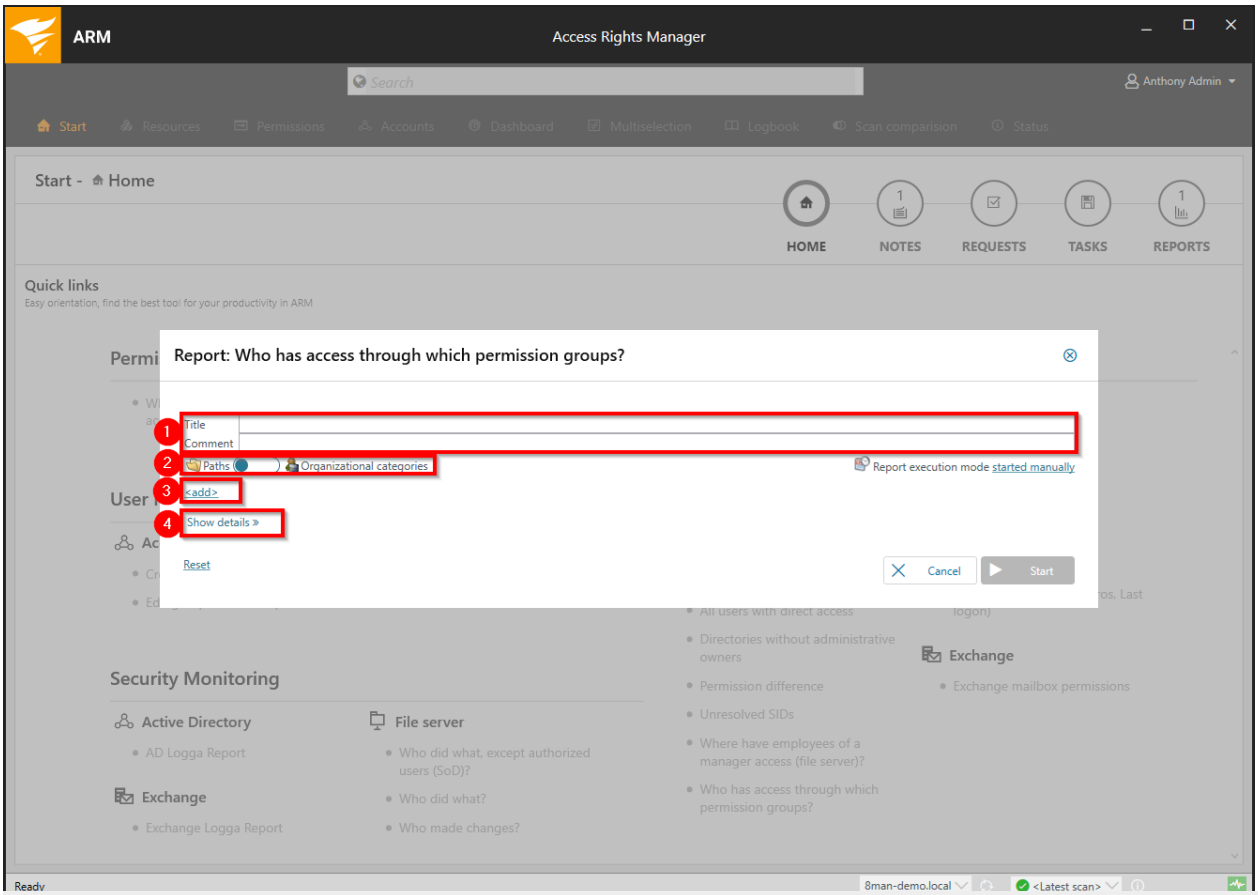
The report "Who has access through which permission groups?" shows the groups that give access to the selected resource and the users that are members of said groups.

Instead of analyzing individual directories you could also use Organizational Categories of the Data Owner configuration.

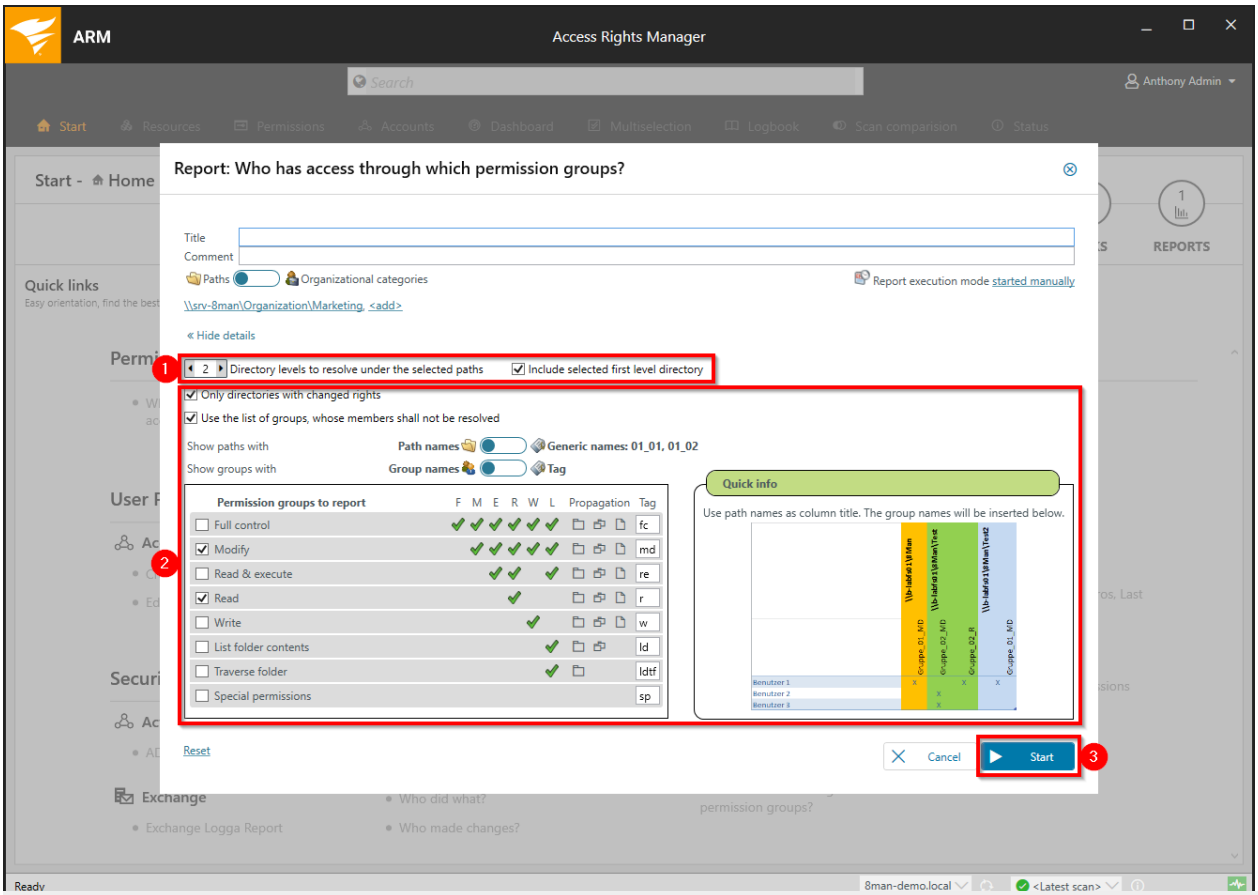
Step-by-step process



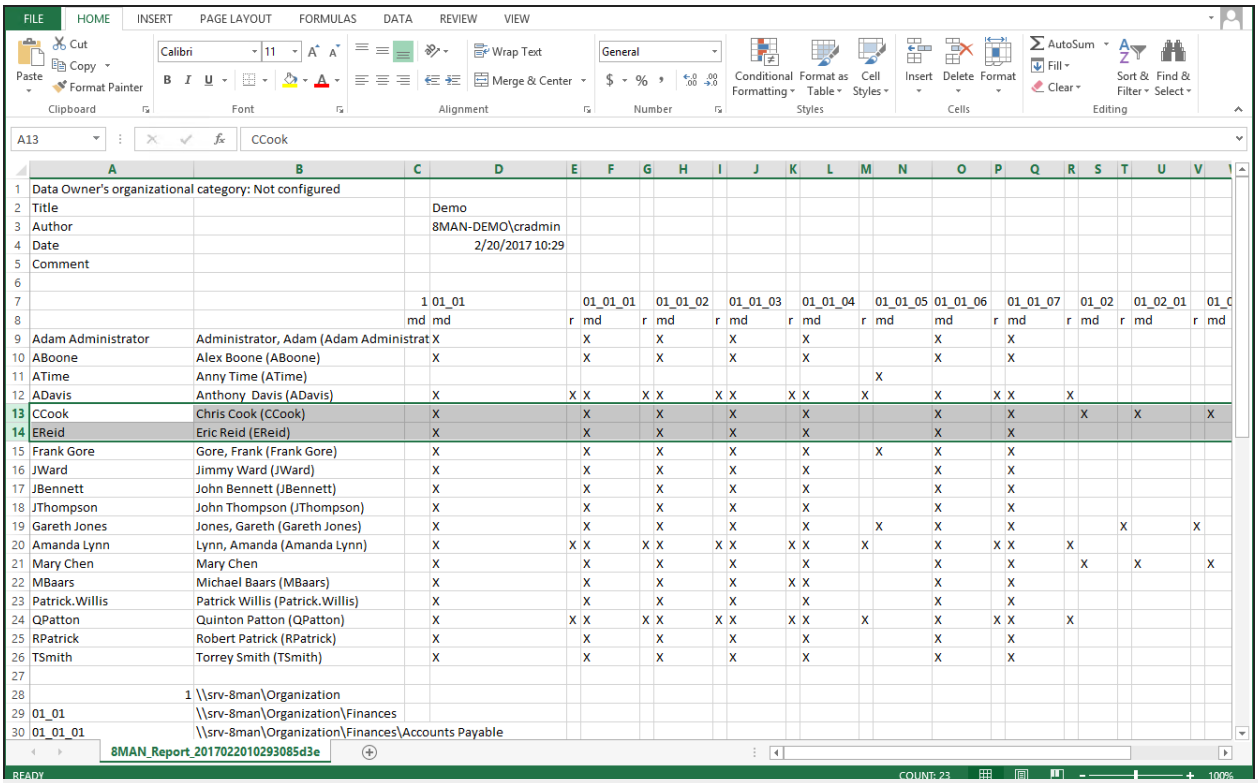
1. Select "Start".
2. Click on "Access Rights Groups".



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".



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		01_01_01		01_01_02		01_01_03		01_01_04		01_01_05	01_01_06		01_01_07		01_02		01_02_01	01_0
8			md	md	r	md	r	md	r	md	r	md	r	md	md	r	md	r	md	r	md	r	md
9	Adam Administrator	Administrator, Adam (Adam Administrat		X		X		X		X		X			X		X					
10	ABoone	Alex Boone (ABoone)		X		X		X		X		X			X		X					
11	ATime	Anny Time (ATime)												X								
12	ADavis	Anthony Davis (ADavis)		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
14	EReid	Eric Reid (EReid)		X		X		X		X		X			X		X					
15	Frank Gore	Gore, Frank (Frank Gore)		X		X		X		X		X		X	X		X					
16	JWard	Jimmy Ward (JWard)		X		X		X		X		X			X		X					
17	JBennett	John Bennett (JBennett)		X		X		X		X		X			X		X					
18	JThompson	John Thompson (JThompson)		X		X		X		X		X			X		X					
19	Gareth Jones	Jones, Gareth (Gareth Jones)		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					
21	Mary Chen	Mary Chen		X		X		X		X		X			X		X		X		X	X
22	MBaars	Michael Baars (MBaars)		X		X		X		X	X	X			X		X					
23	Patrick.Willis	Patrick Willis (Patrick.Willis)		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					
25	RPatrick	Robert Patrick (RPatrick)		X		X		X		X		X			X		X					
26	TSmith	Torrey Smith (TSmith)		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

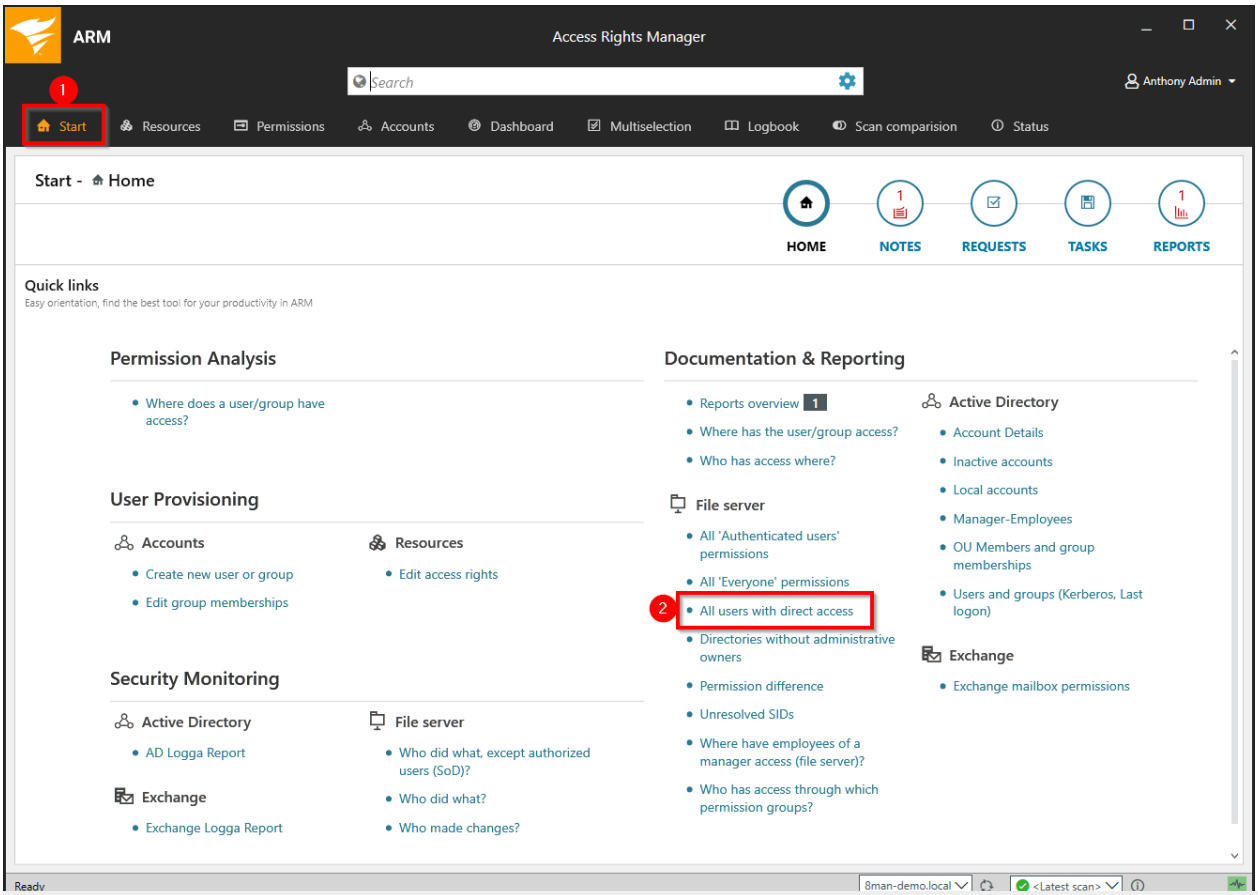
Direct access rights should be avoided at all costs and be replaced by group access rights. Firstly, direct access rights are inefficient because every user has to be managed independently. Secondly, each directory needs to be examined individually to ensure the removal of all direct permissions. ARM shows you all direct permissions on your file server(s) in one simple report.

Related features

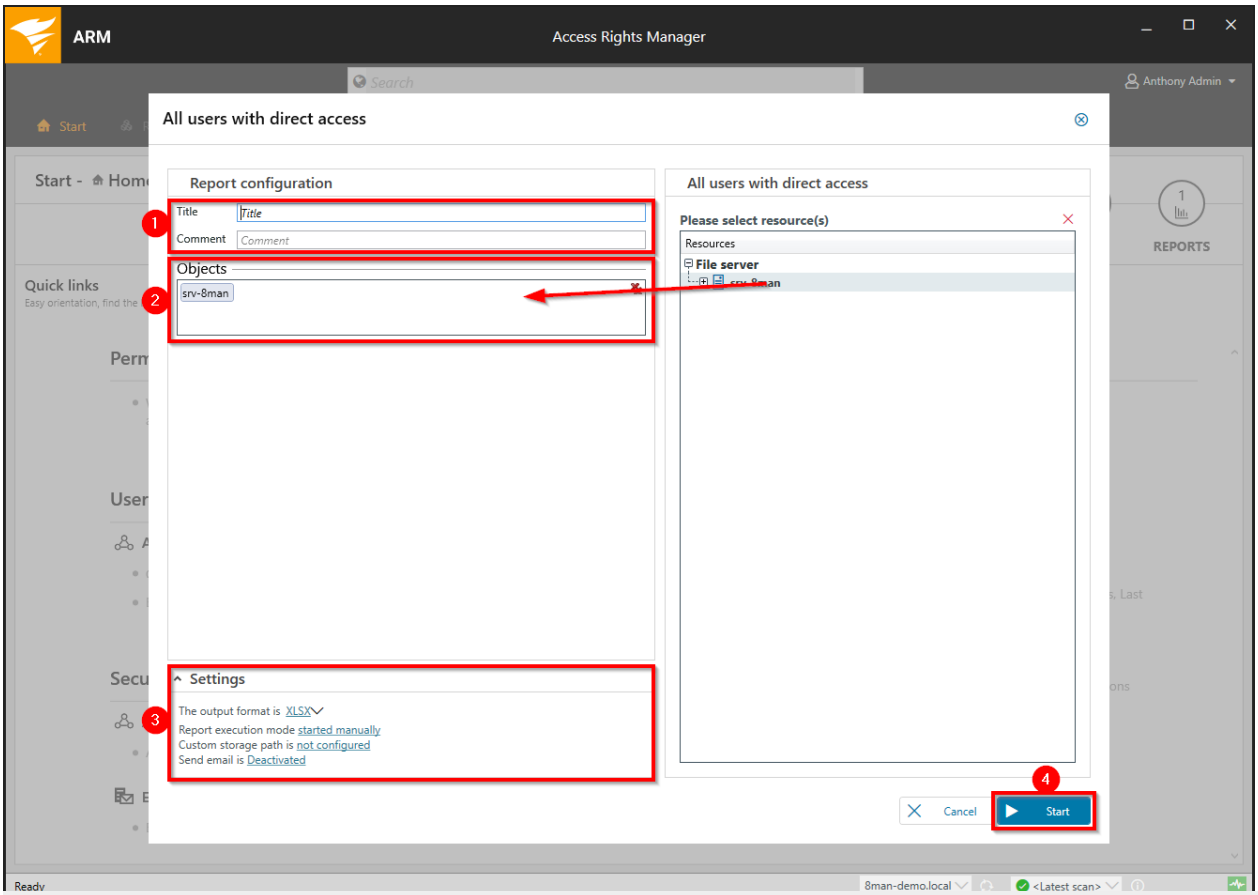
Remove direct permissions (rich client)

Remove direct permissions in bulk (web client)

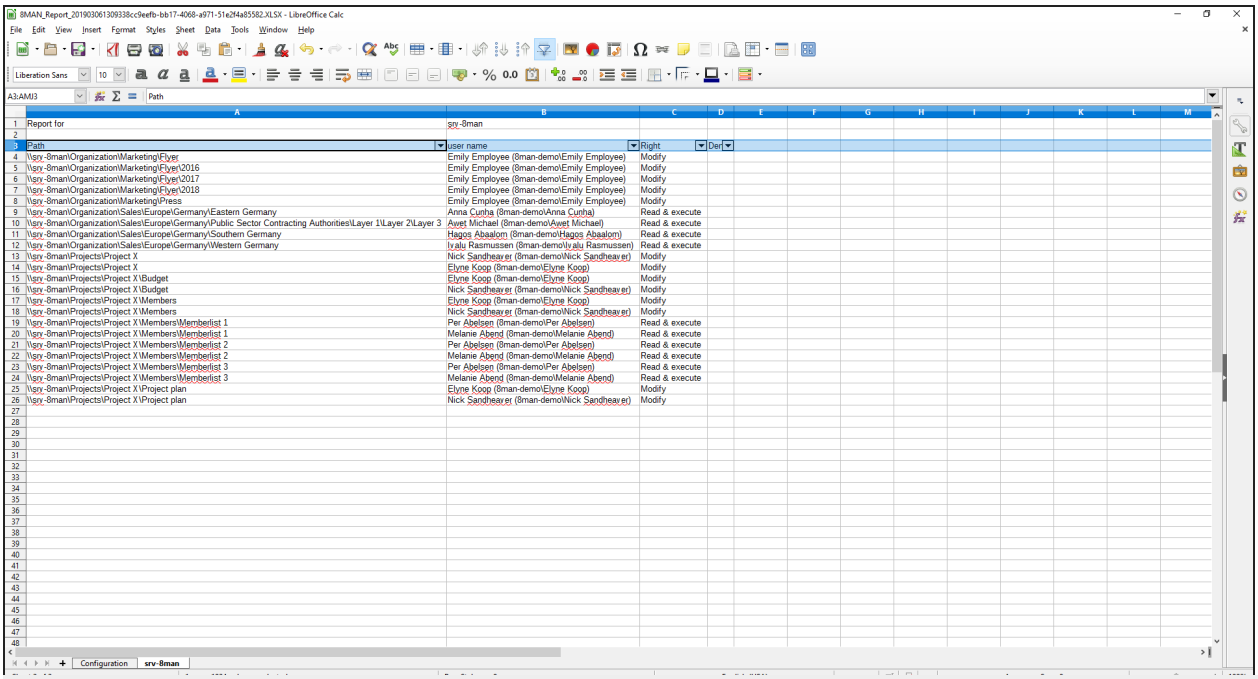
Step-by-step process



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.



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.

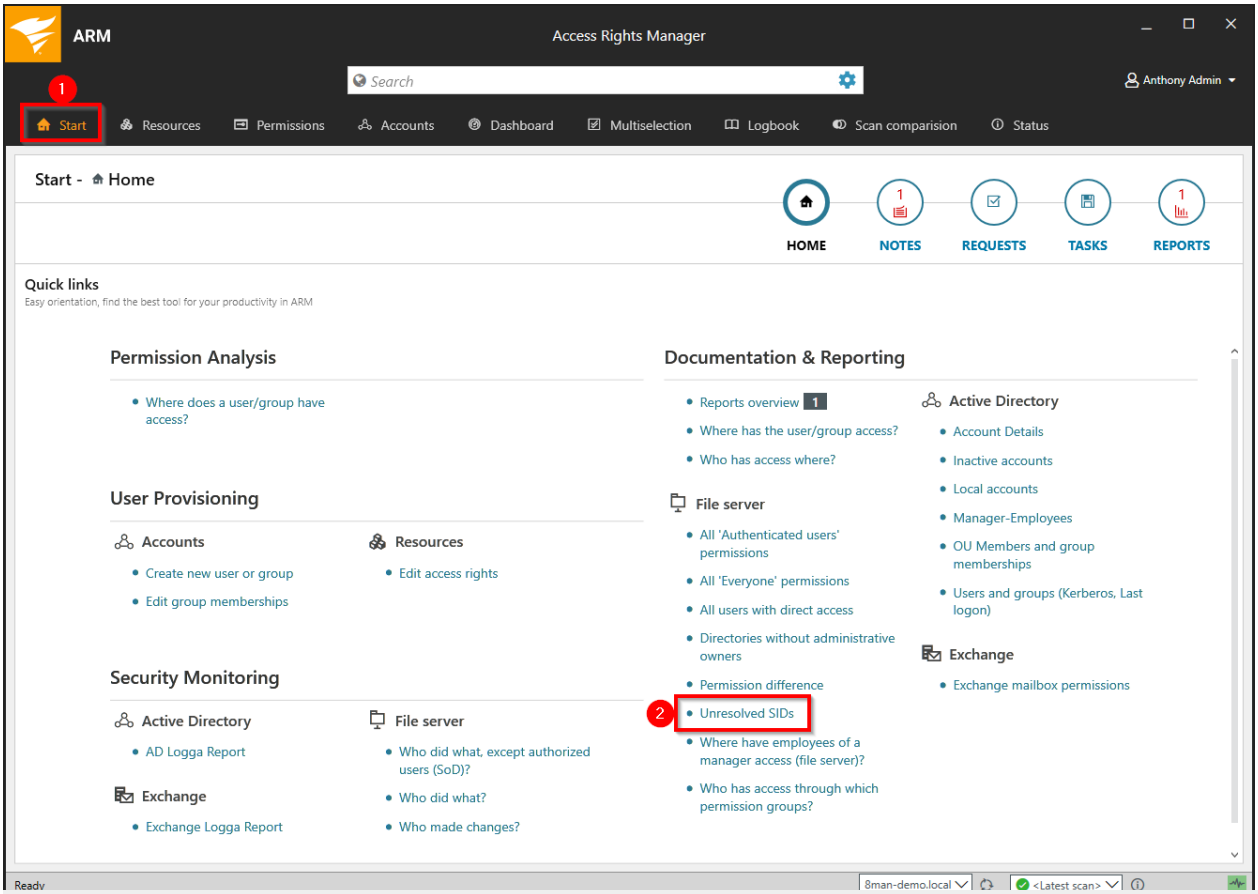
ARM clearly identifies unresolved SIDs in your system.

Related features

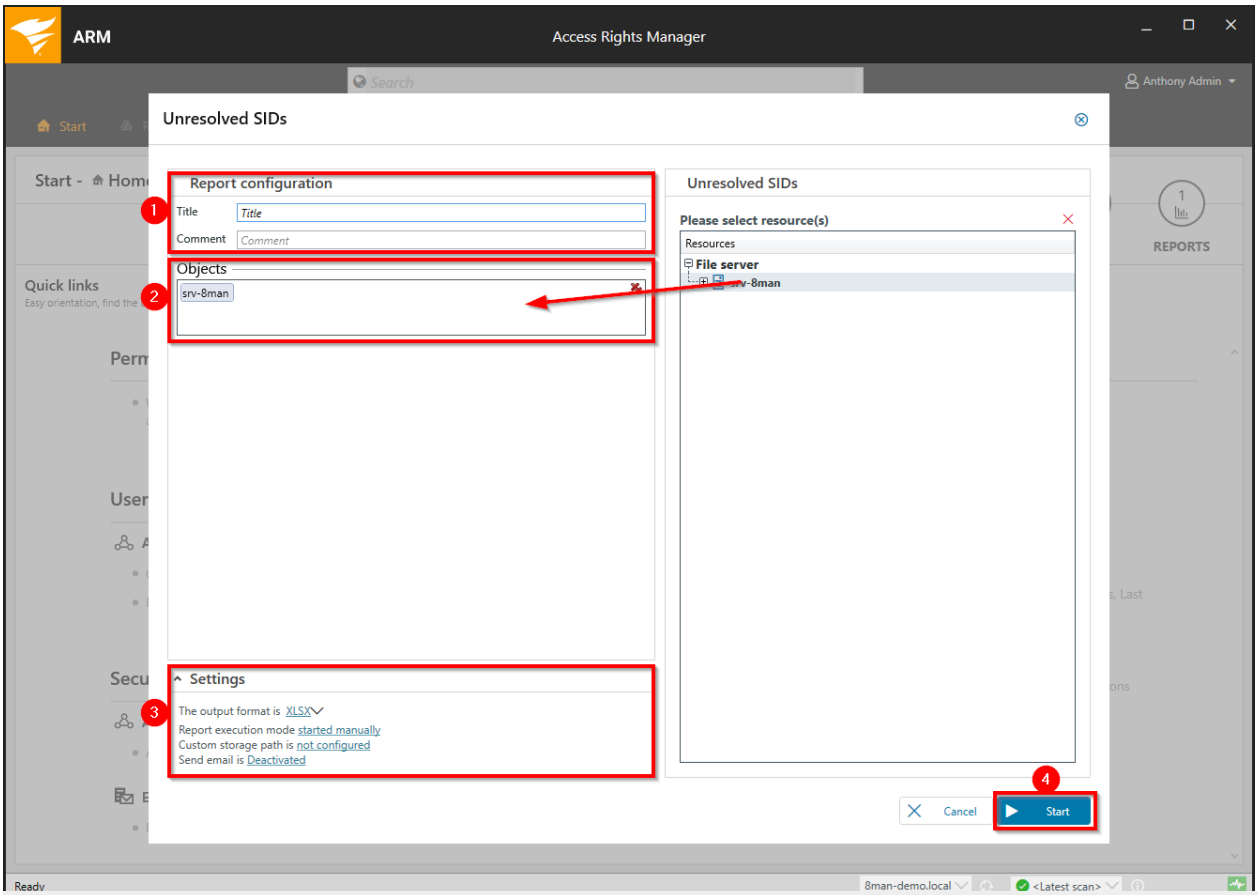
Identify and delete unresolved SIDs (rich client)

Remove unresolved SIDs in bulk (web client)

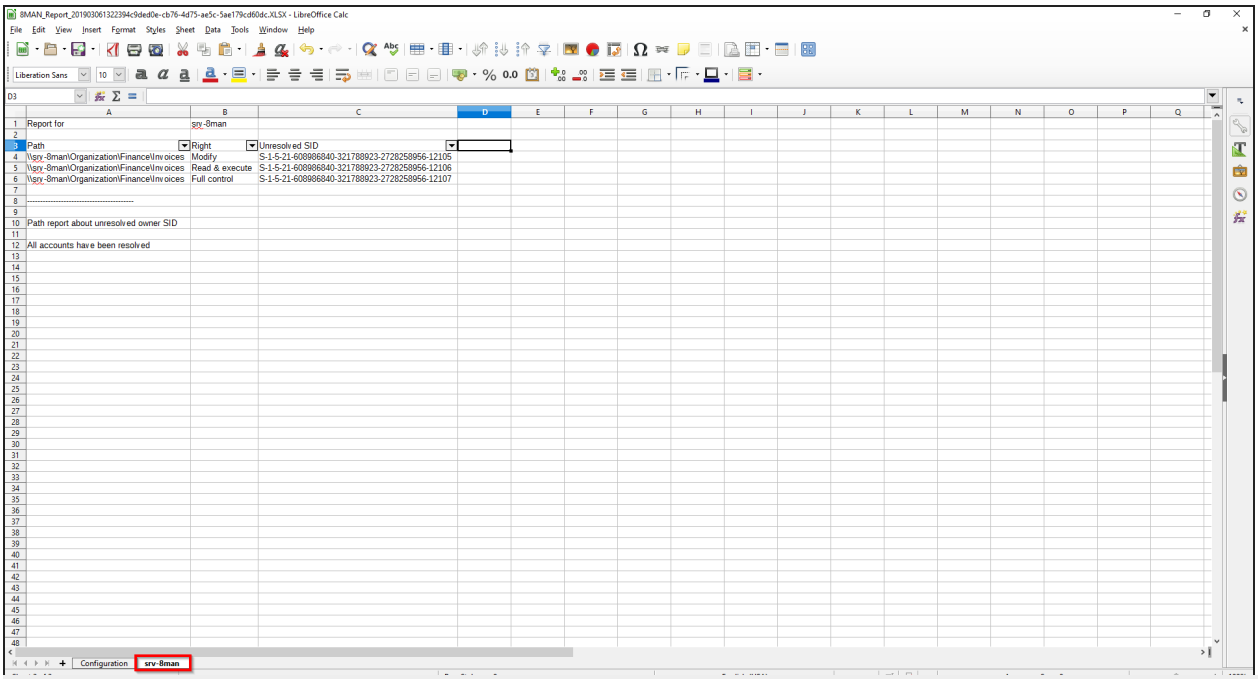
Step-by-step process



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.



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.

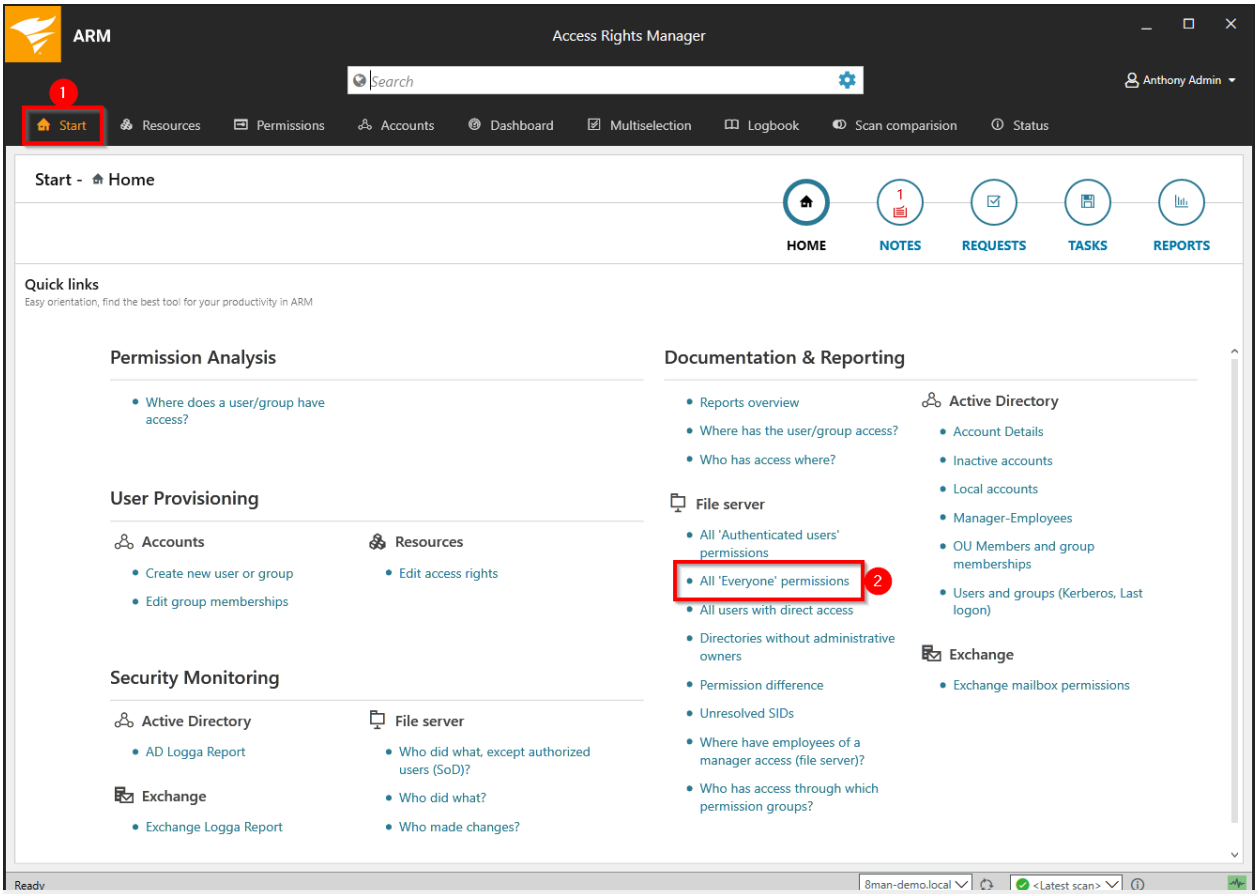
Related features

Also keep an eye on the critical Authenticated Users.

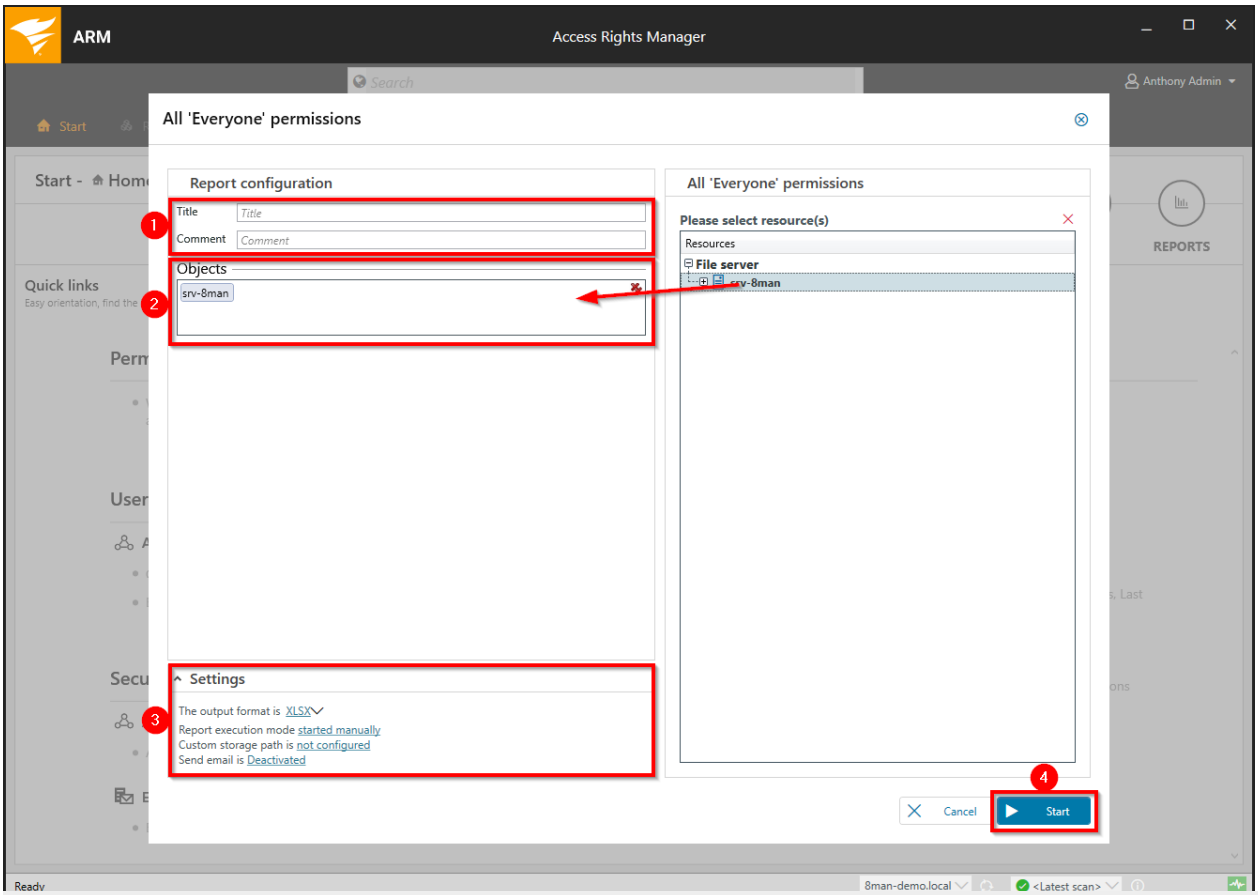
Identify globally accessible directories (web client)

Remove "everyone" permissions in bulk (web client)

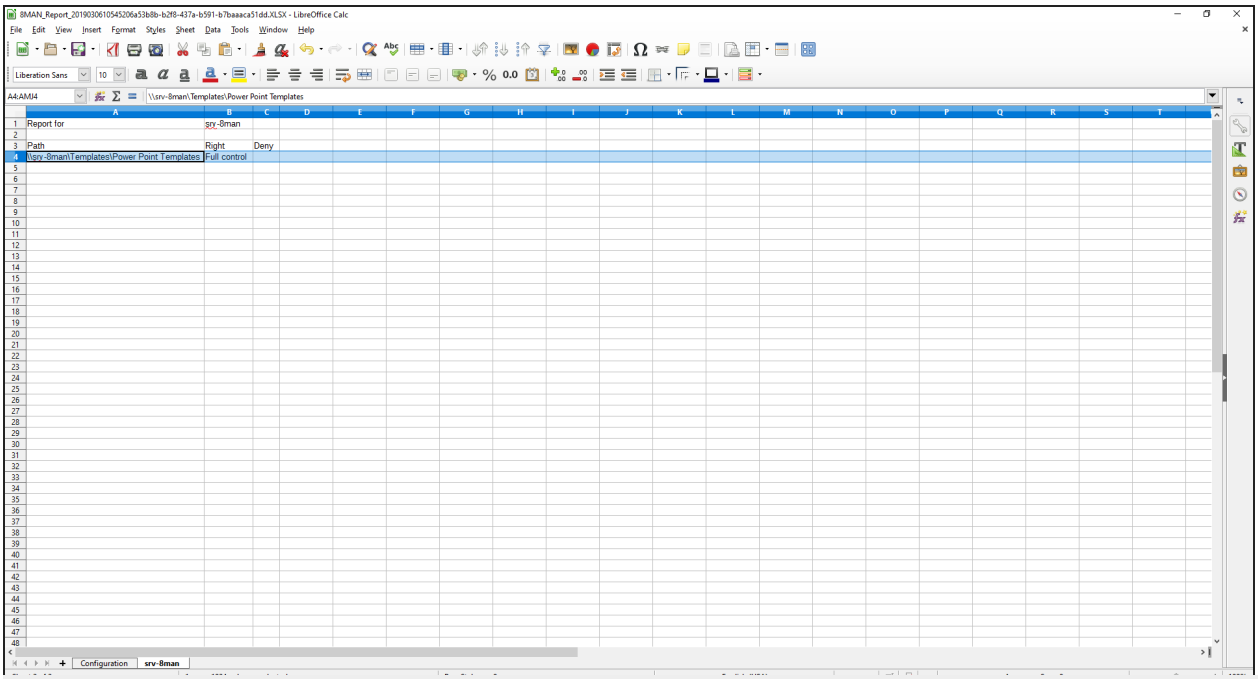
Step-by-step process



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.



In the example you see directories that everyone has access to.

Report on the usage of "Authenticated Users"

Background / Value

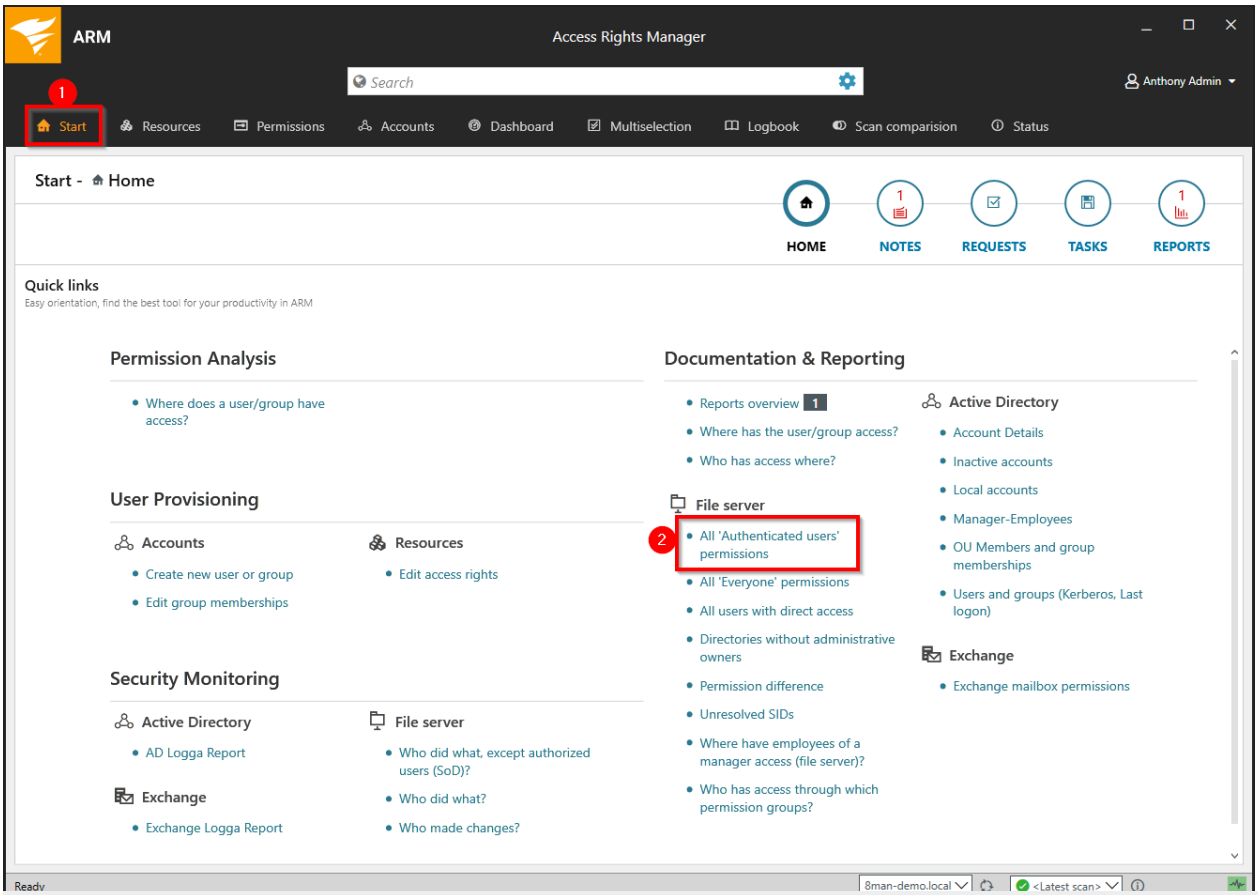
The report shows all directories where the account "Authenticated Users" has access. Just like the "Everyone" account, his technical user account should never be used to grant access to sensitive resources. Scan the report for sensitive directories and remove the access rights for "Authenticated Users".

Related features

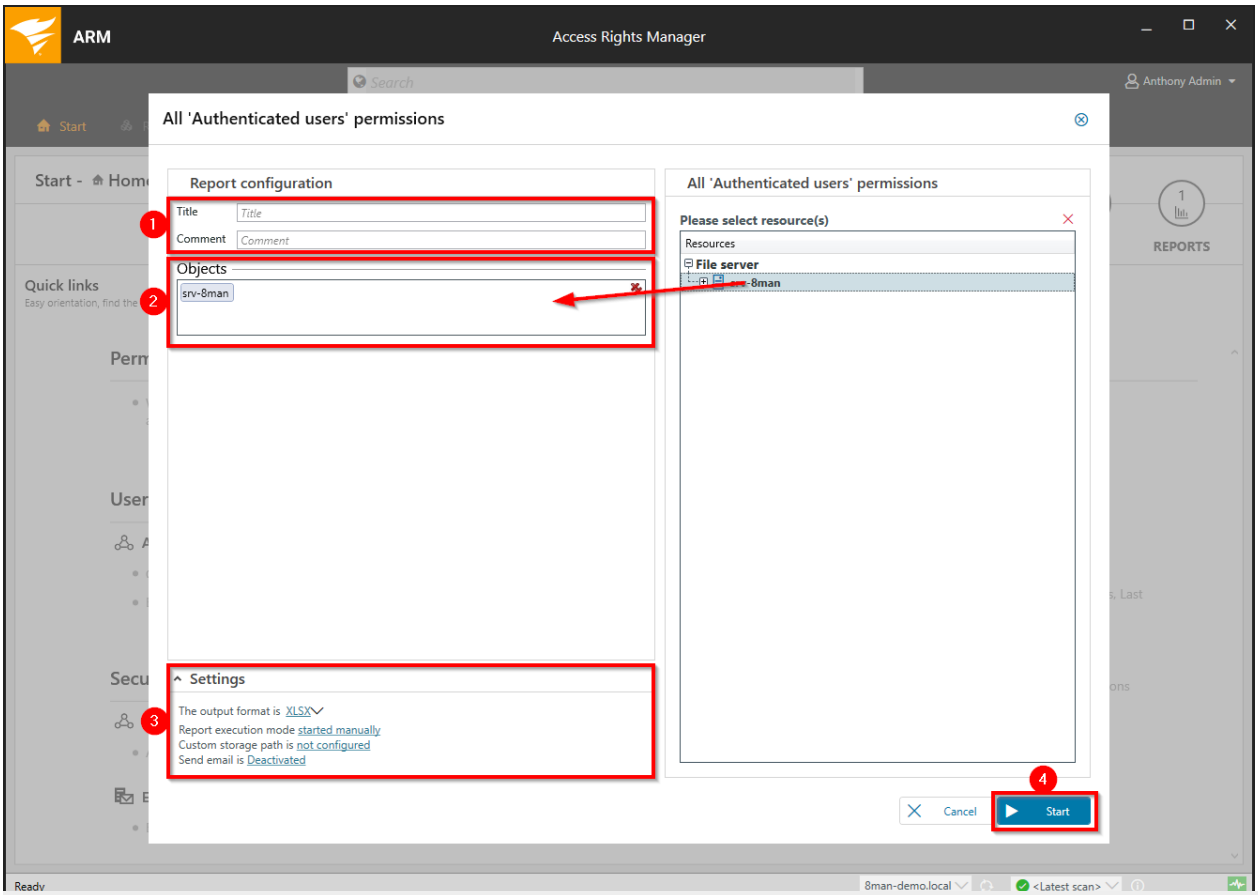
Report on the usage of "everyone"

Identify globally accessible directories (web client)

Step-by-step process



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

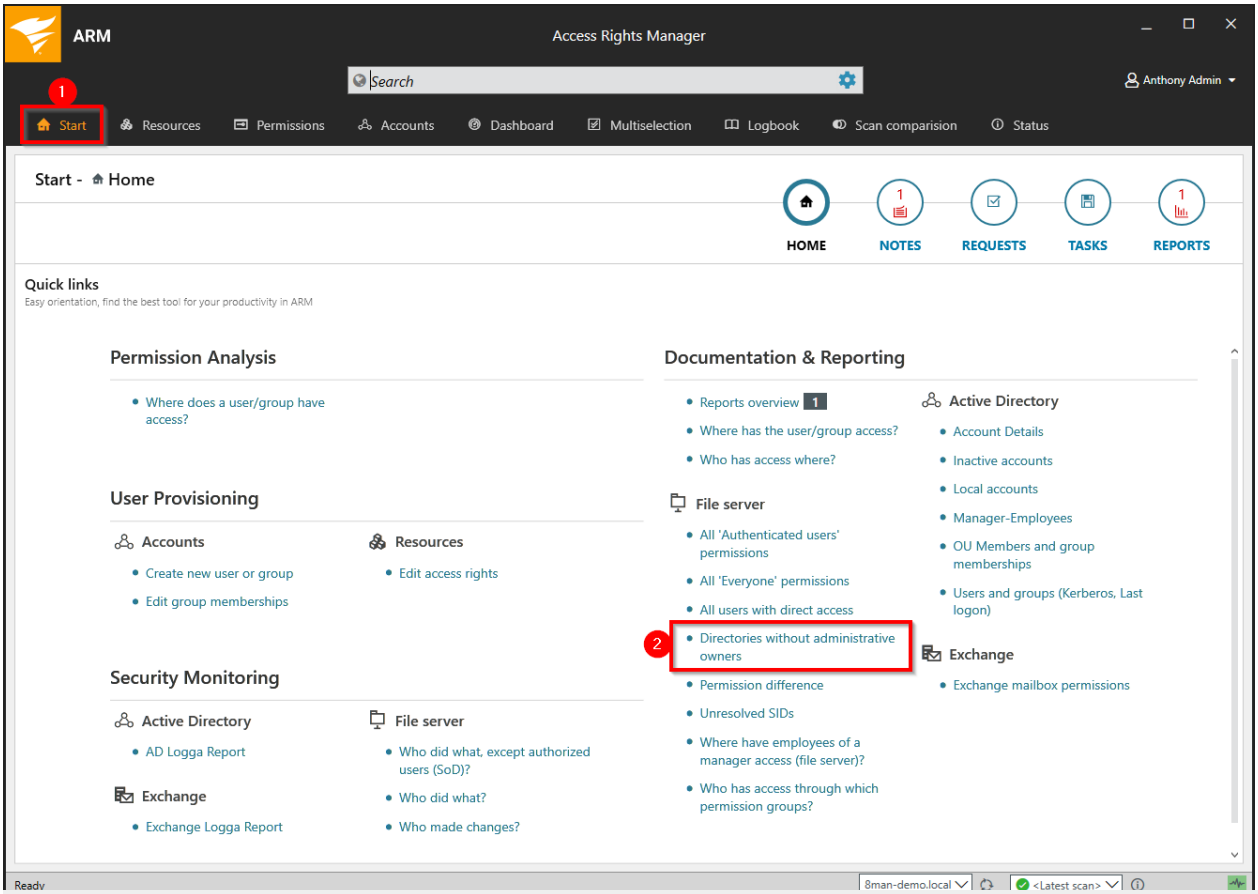
Background / Value

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.

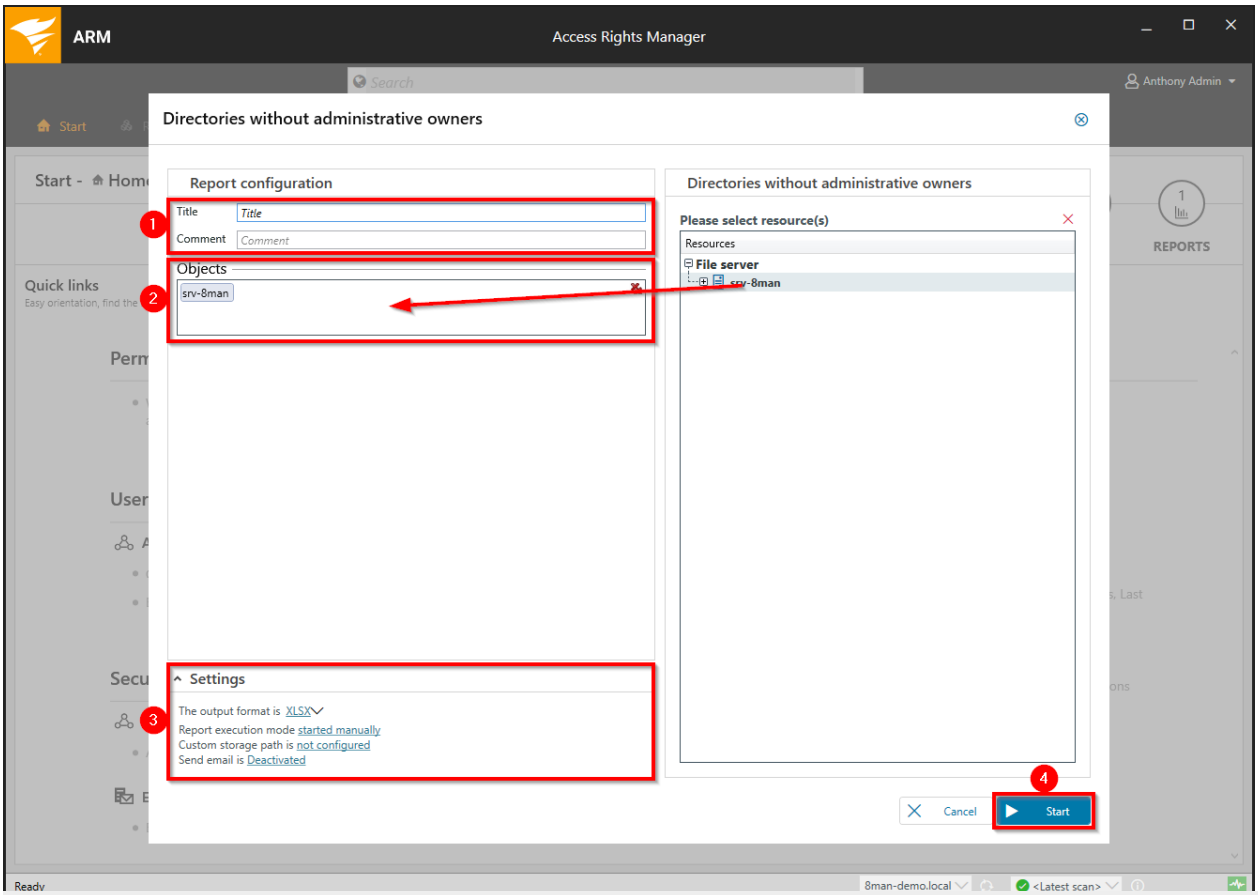
Related features

Change directory ownership

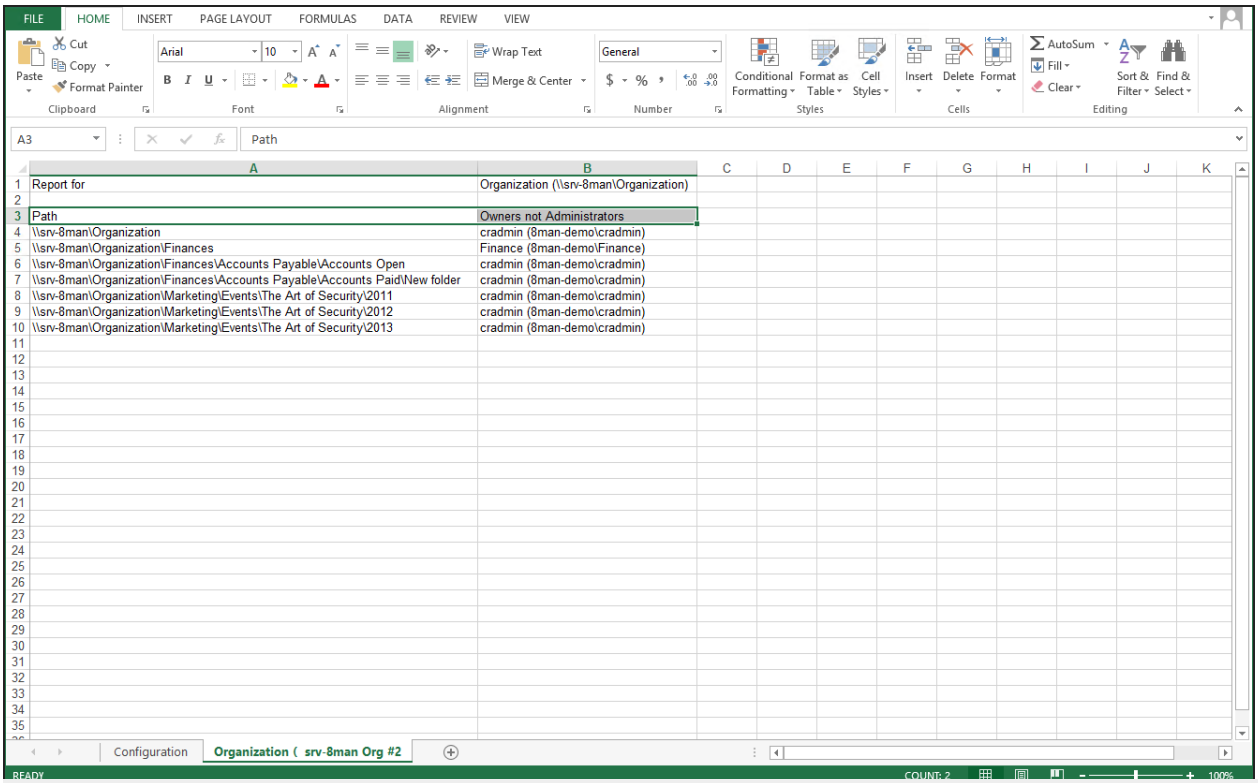
Step-by-step process



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.



Open the report in your spreadsheet application. ARM lists all directories that are not owned by administrators.

Permission differences

Background / Value

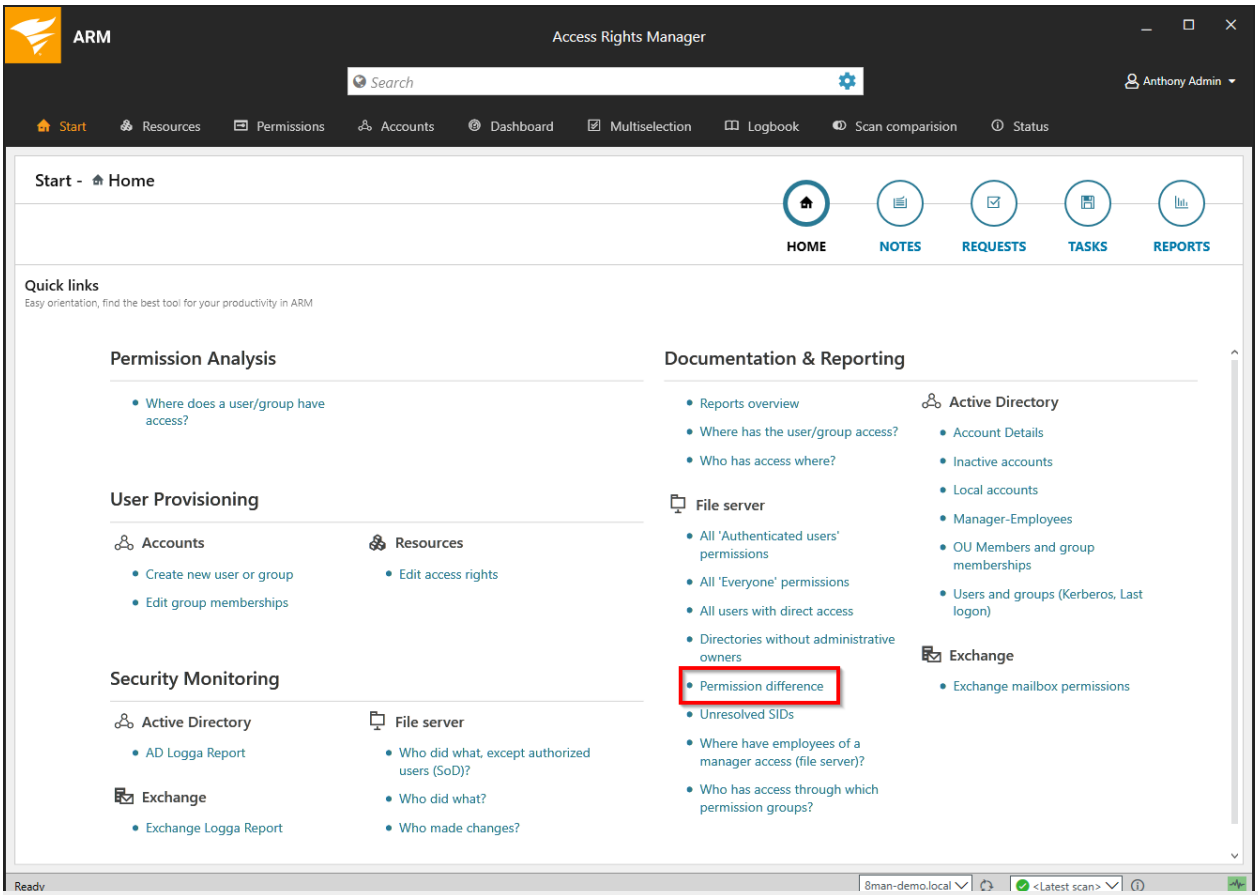
The "Permission differences" report compares the access rights on your file server at two different points in time and shows you how your access rights situation has changed.

Related features

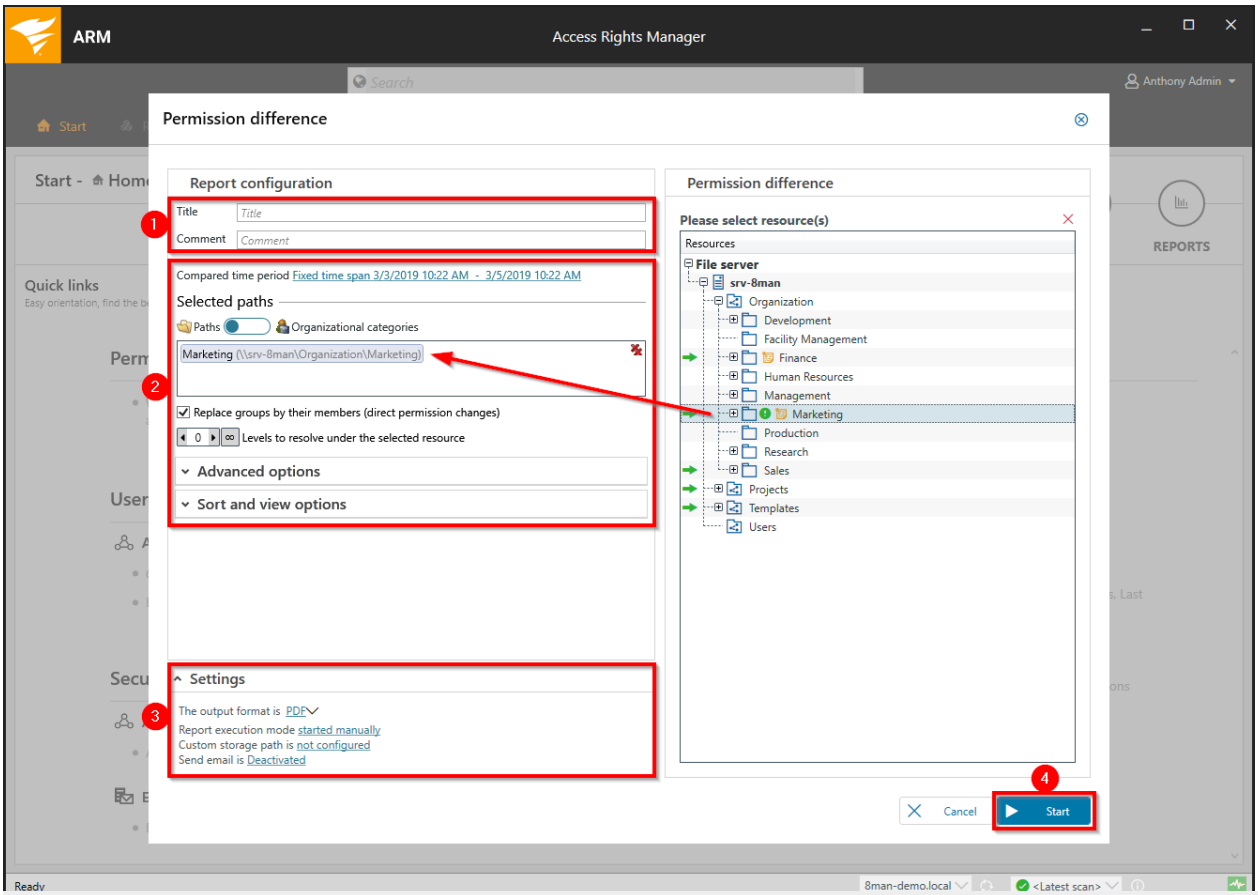
Compare two different access rights situations (scan comparison)

Analyze historical access rights situations

Step-by-step process



1. Select "Start".
2. Click on "Permission difference".



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:

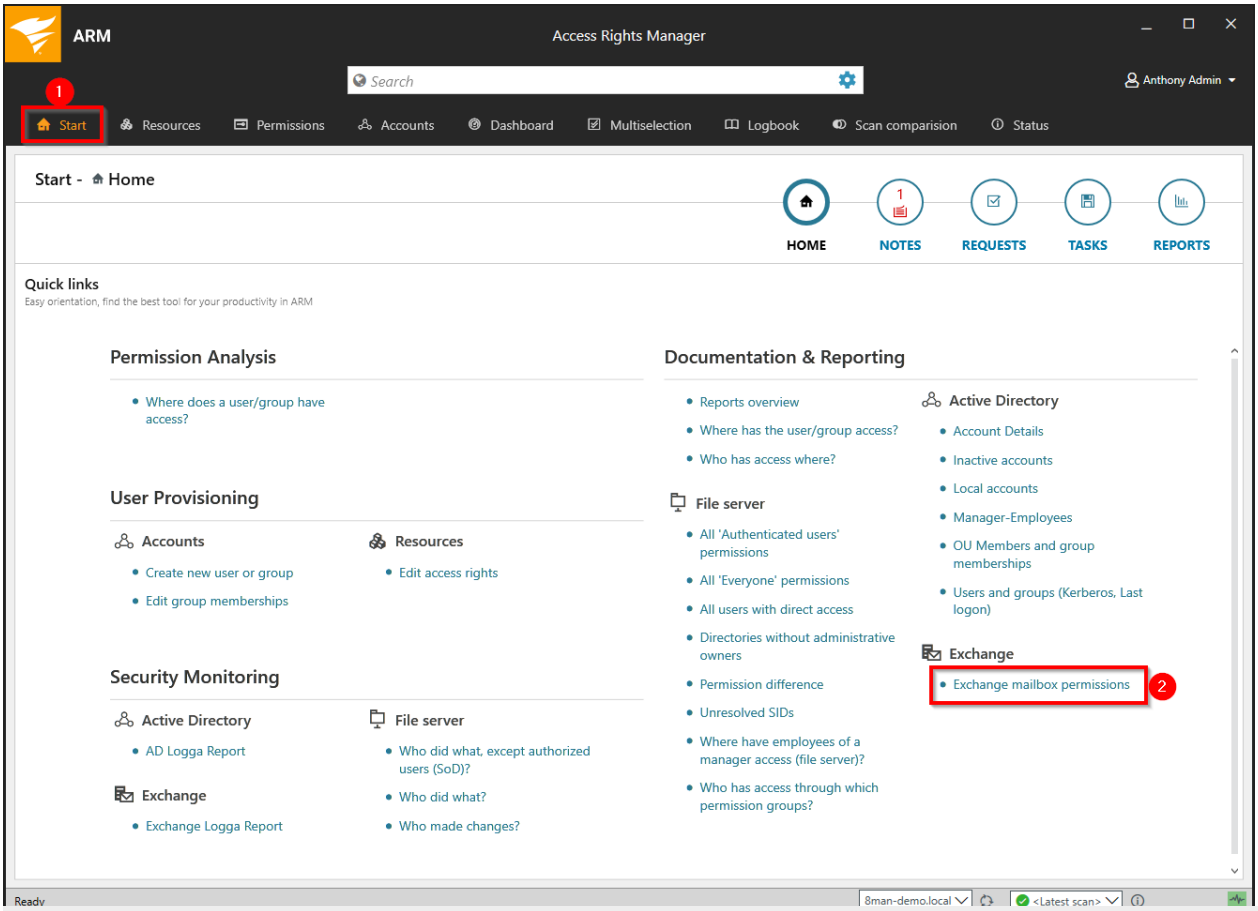
- Mailbox permissions
- Mailbox folder permissions
- Mailbox properties
- Delegates for mailboxes
- Out of office notices

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.

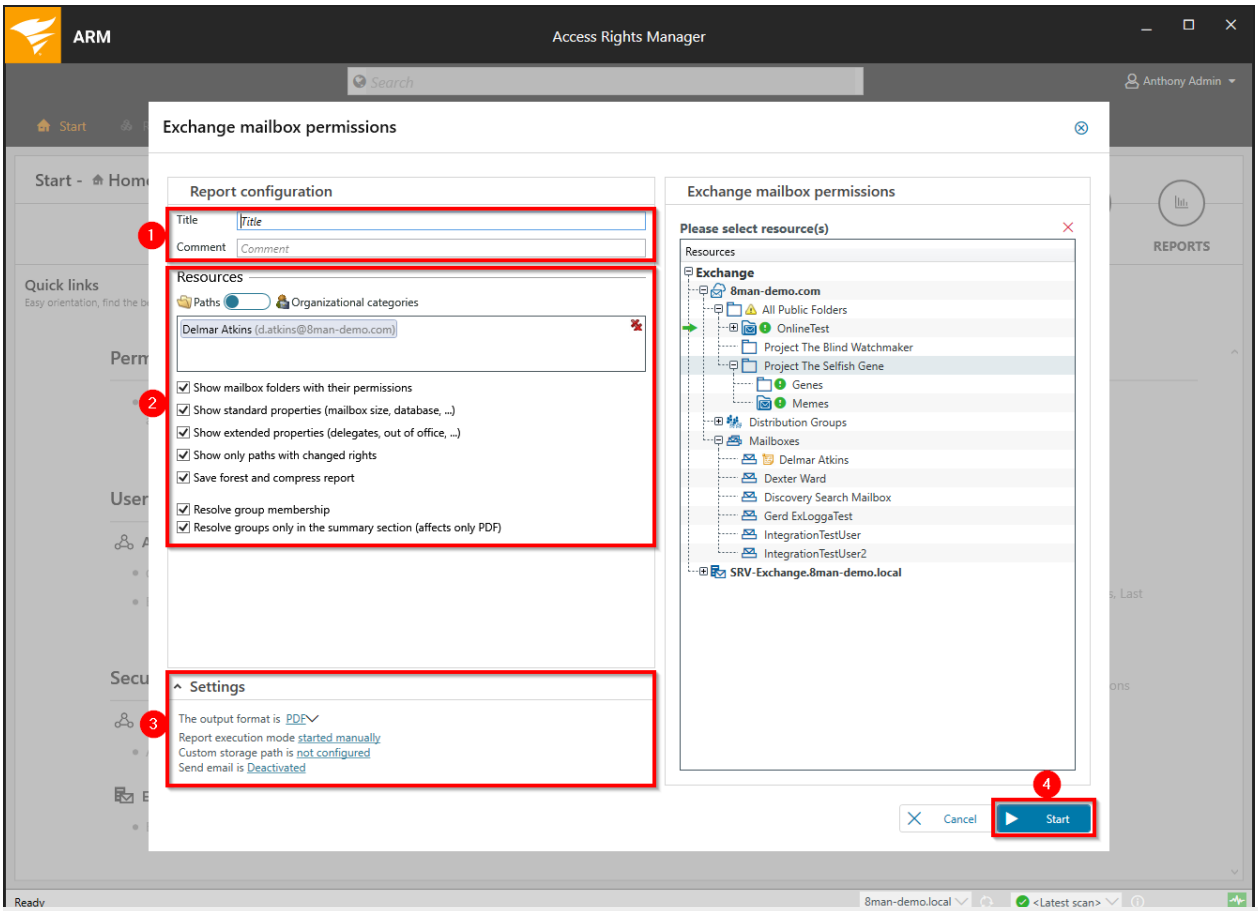
Related features

"Send As" access rights are shown in the report "Who has access where?".

Step-by-step process



1. Select "Start".
2. Click on "Exchange Mailbox permissions" in the "Documentation and Reporting" area.



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?

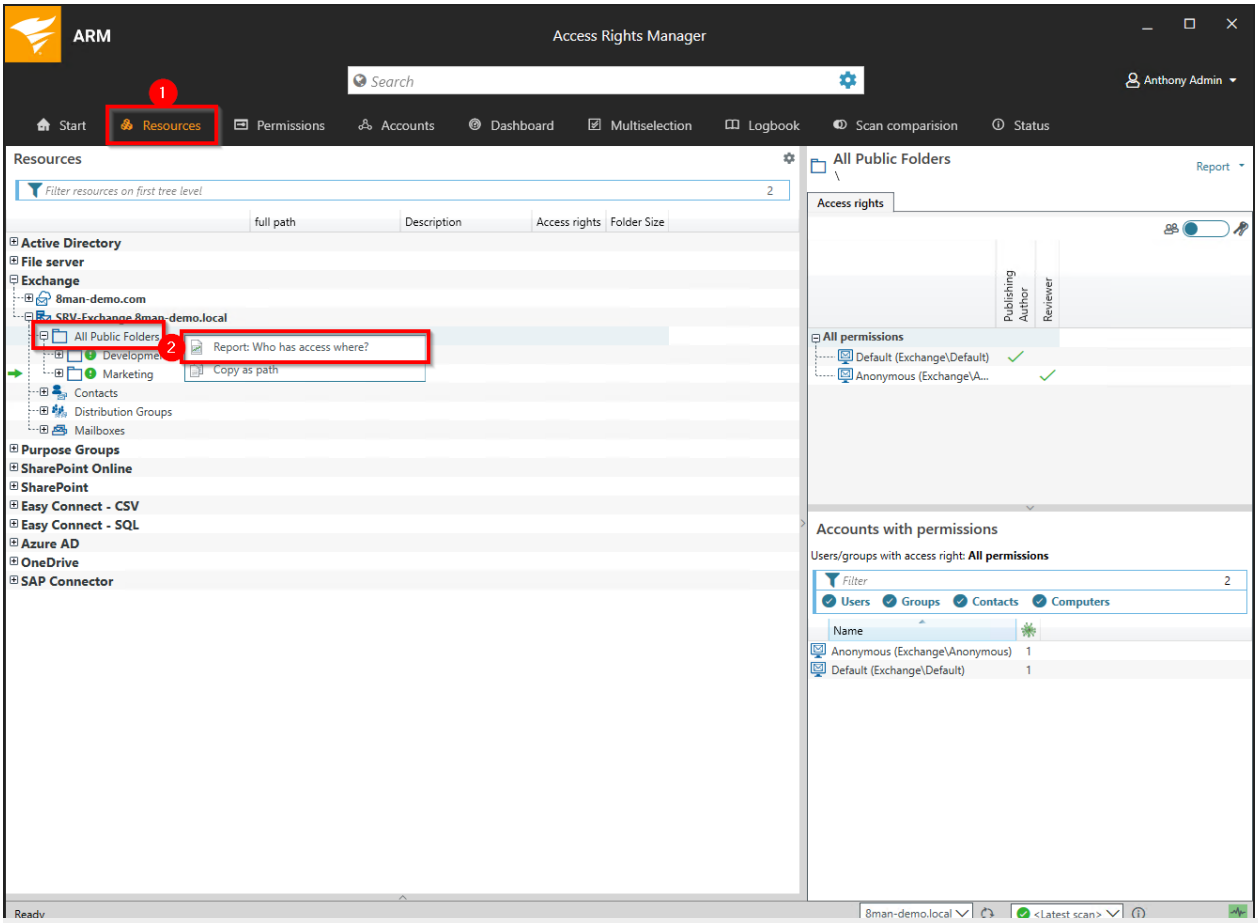
Background / Value

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.

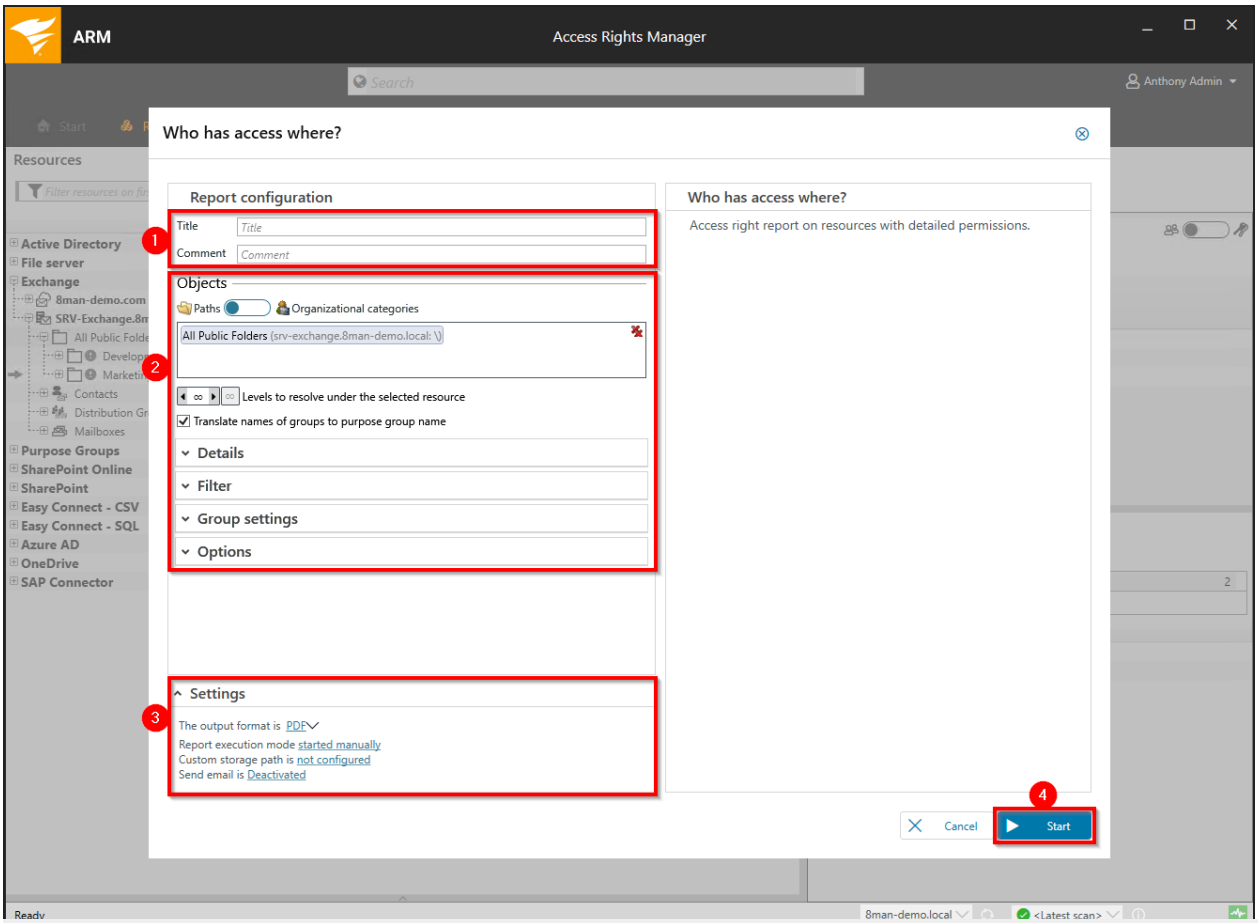
Related features

Report on mailbox permission

Step-by-step process



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

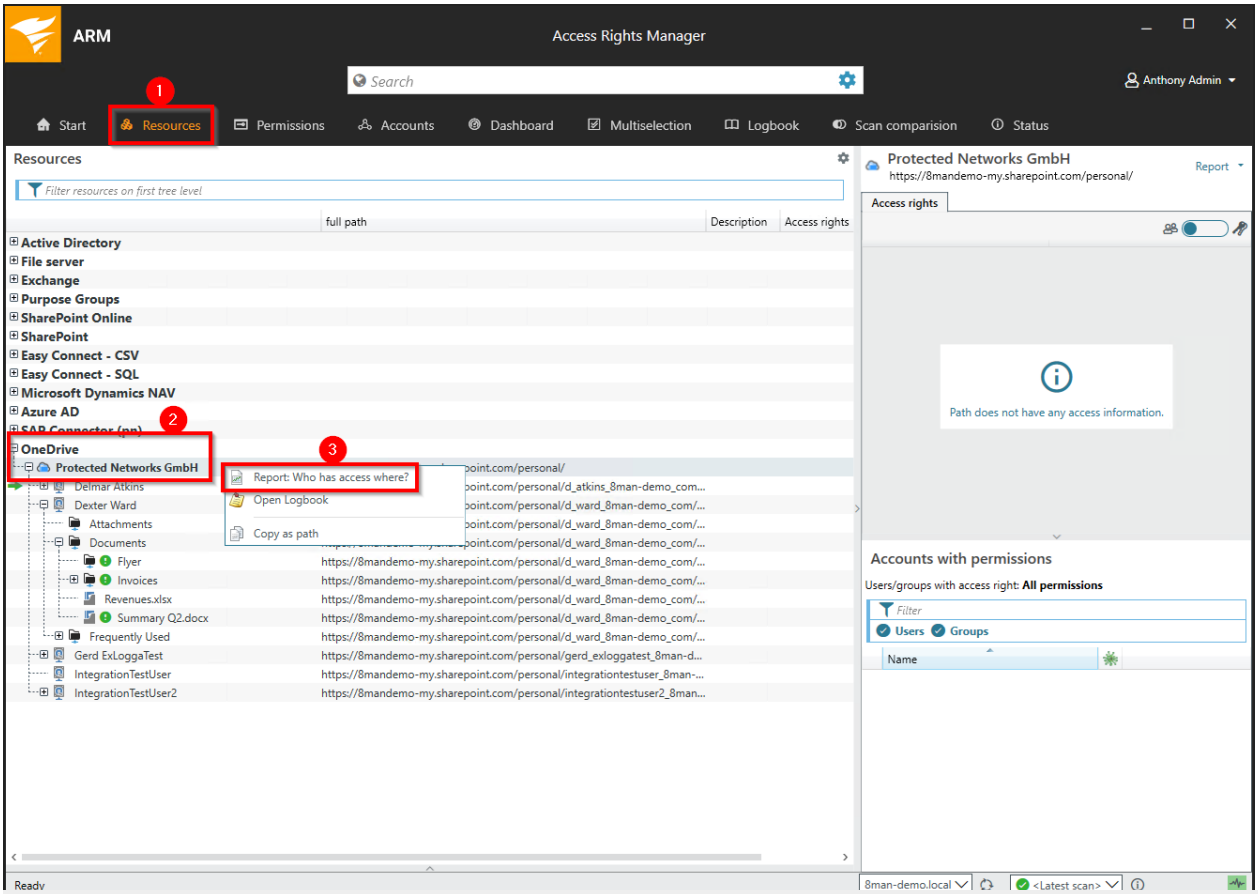
Background/Value

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.

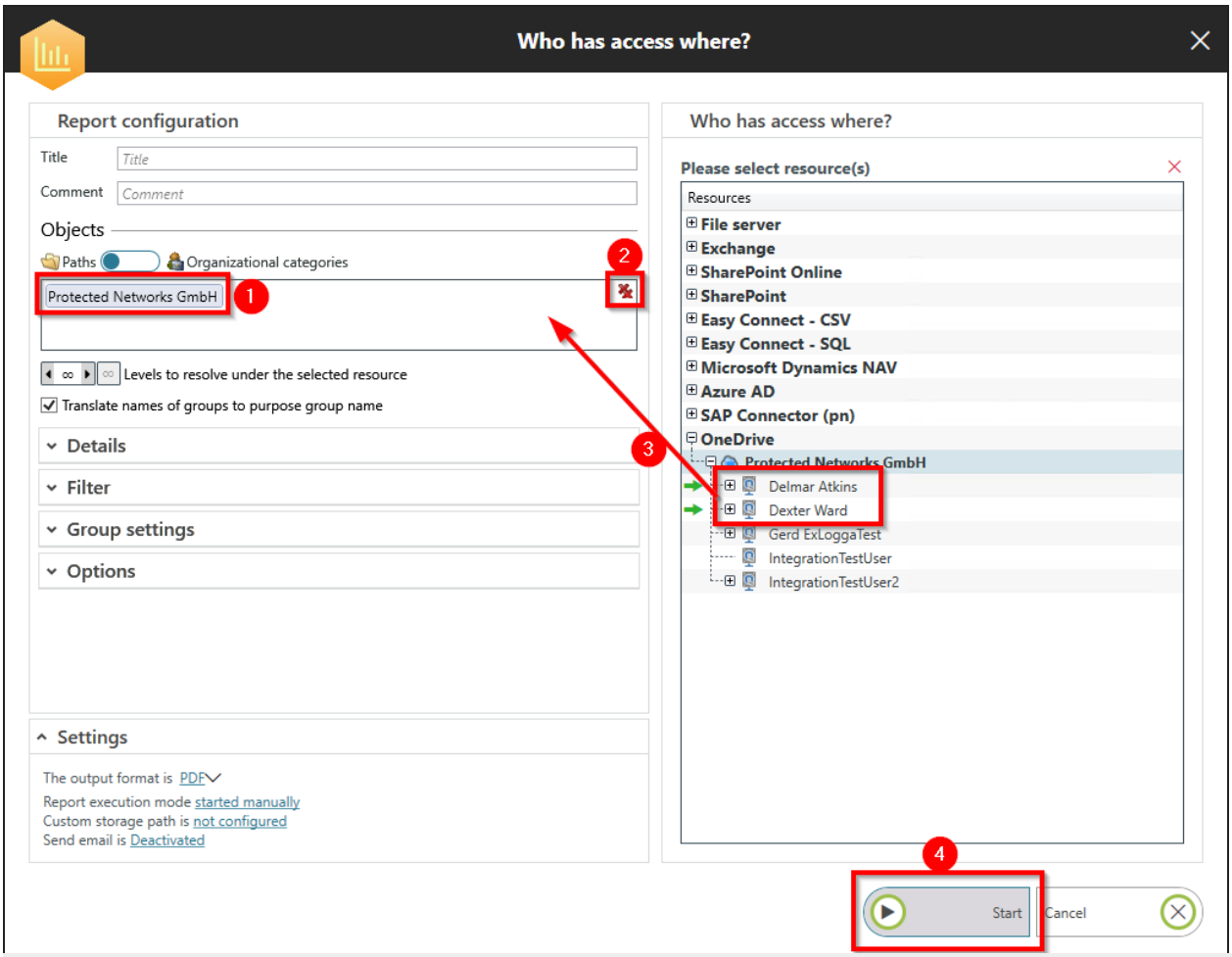
Related features

Identify shared directories and files on OneDrive

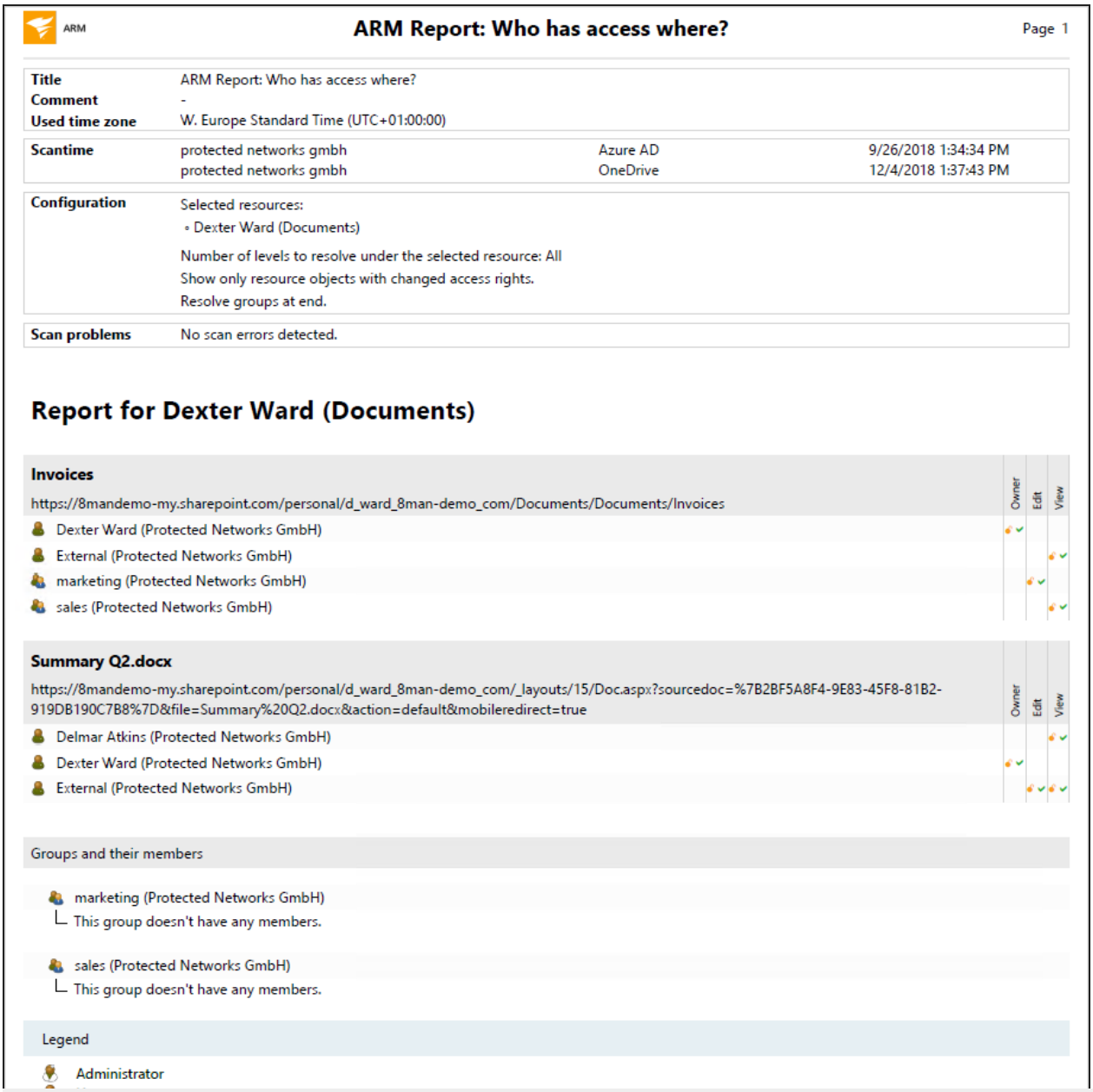
Step-by-step-process



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.



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

ARM Report: Who has access where?

Page 1

Title	ARM Report: Who has access where?
Comment	-
Used time zone	W. Europe Standard Time (UTC+01:00:00)

Scantime	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

	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

	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.

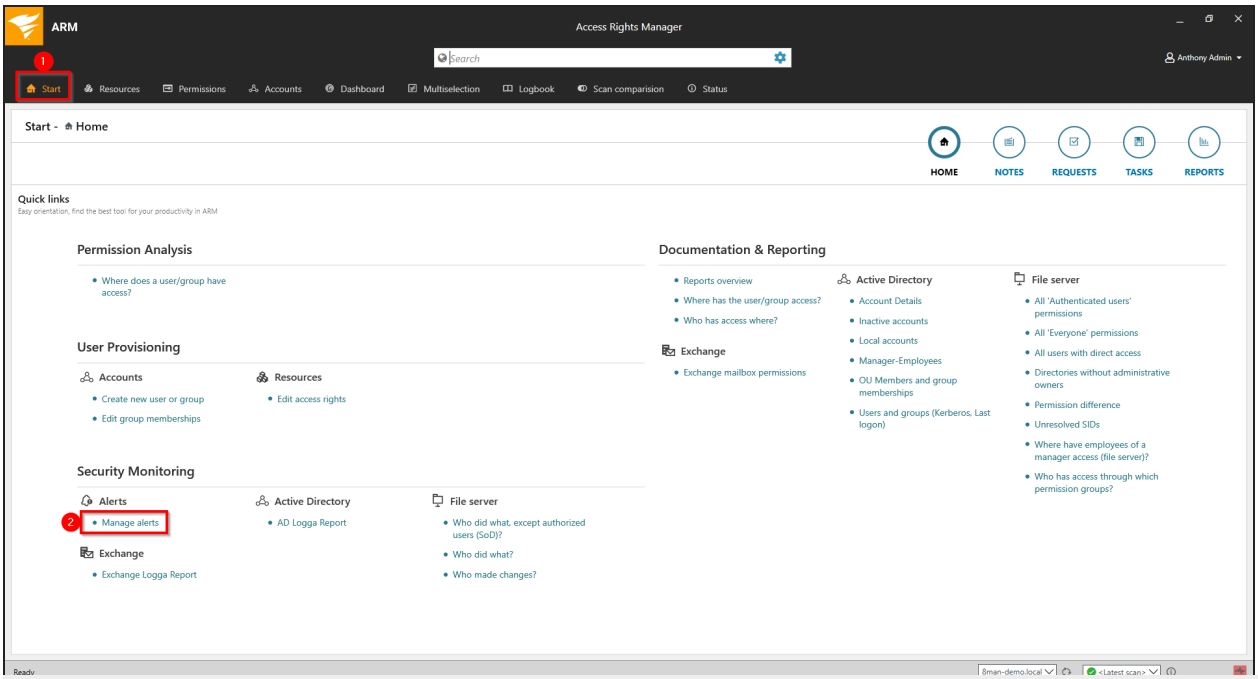
Cross-resource

Manage alerts

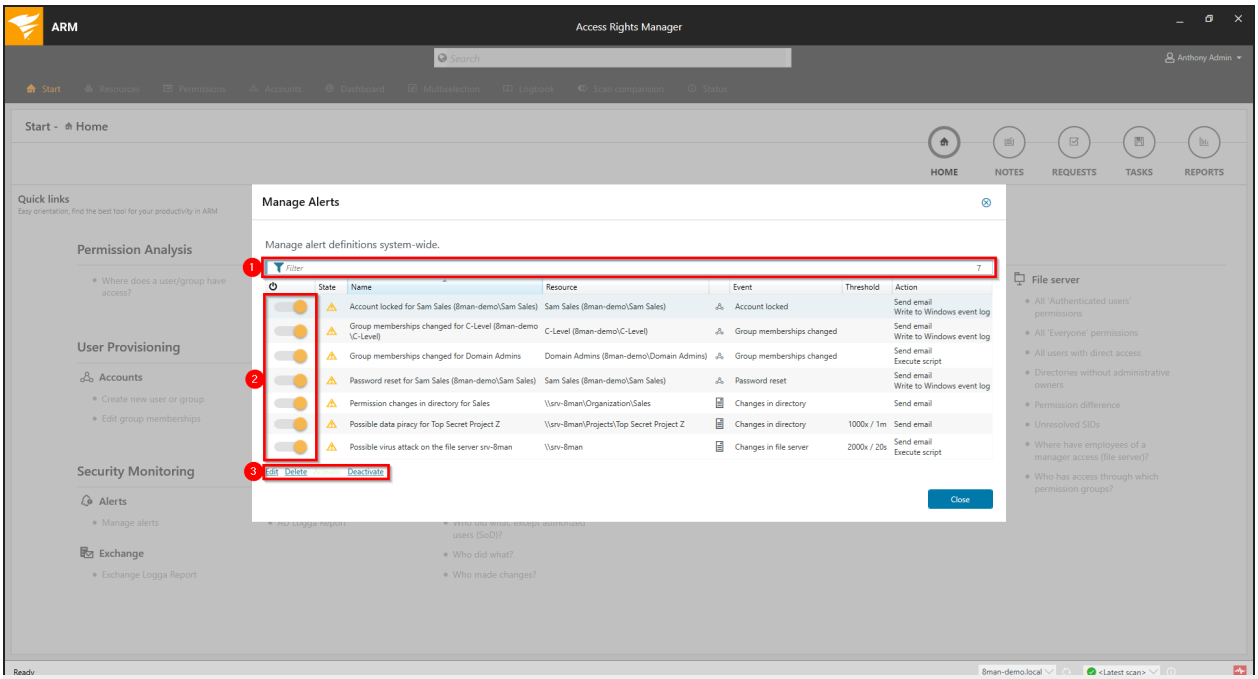
Background / Value

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 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

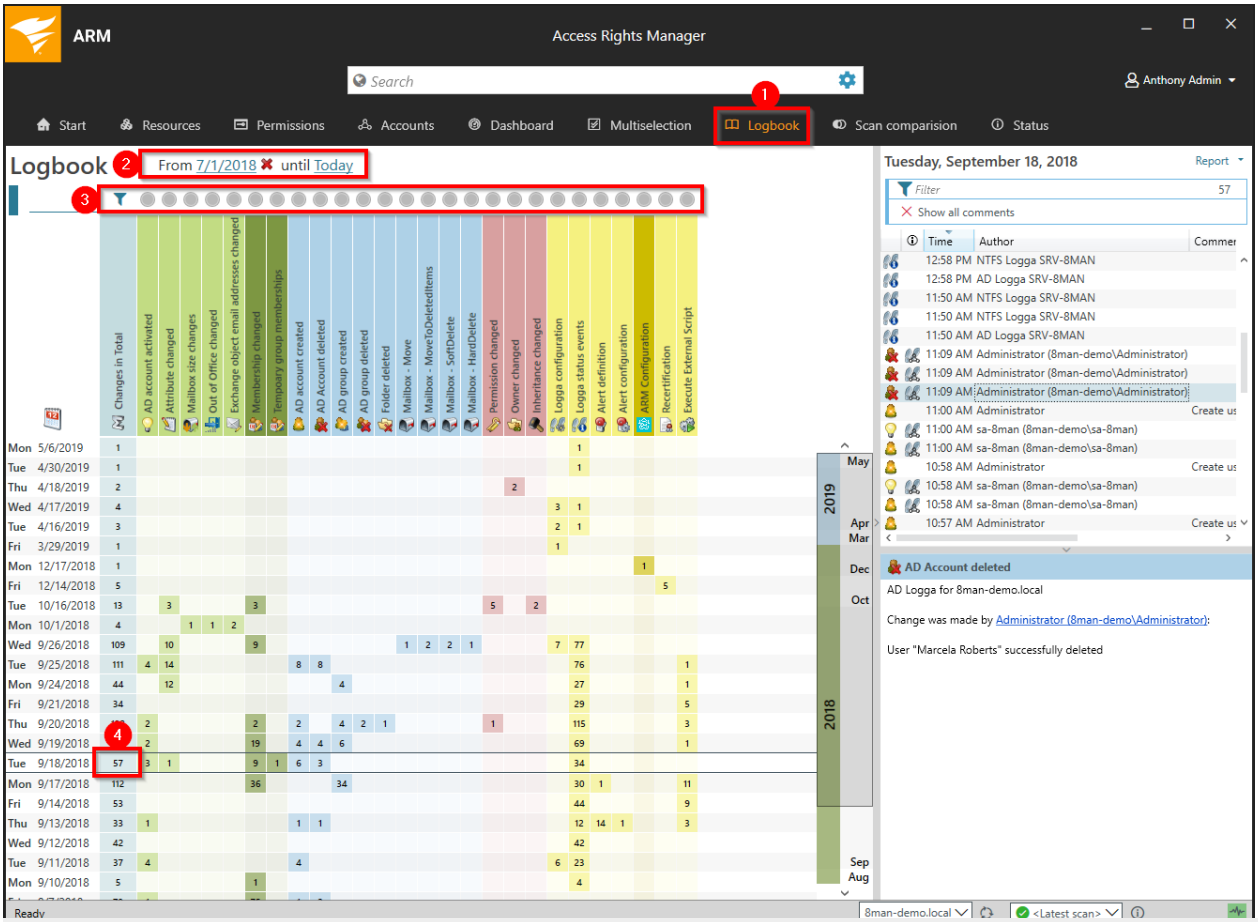
Identify locked user accounts

Monitor password resets

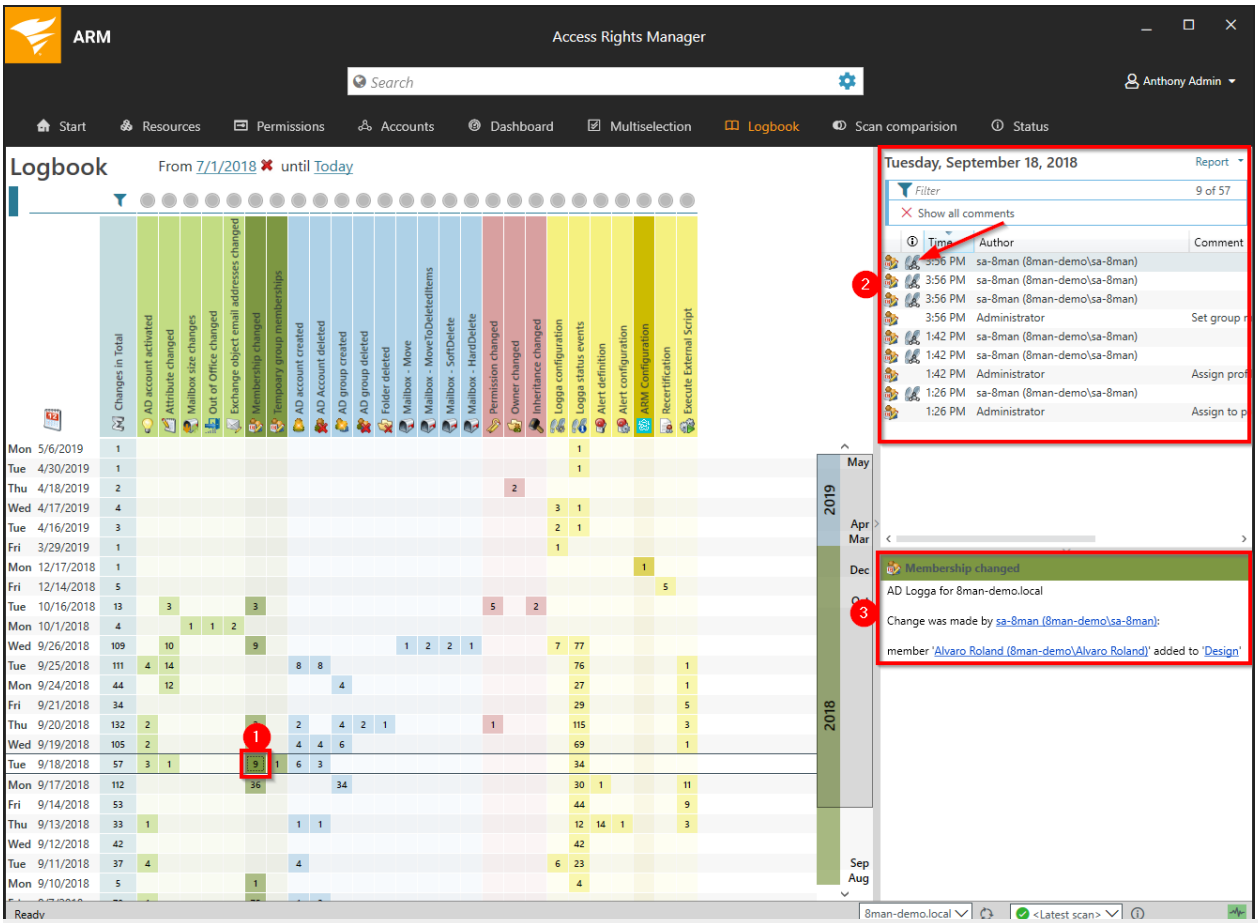
Set alerts for groups

Set alerts for user accounts

Step-by-step process



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).



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.

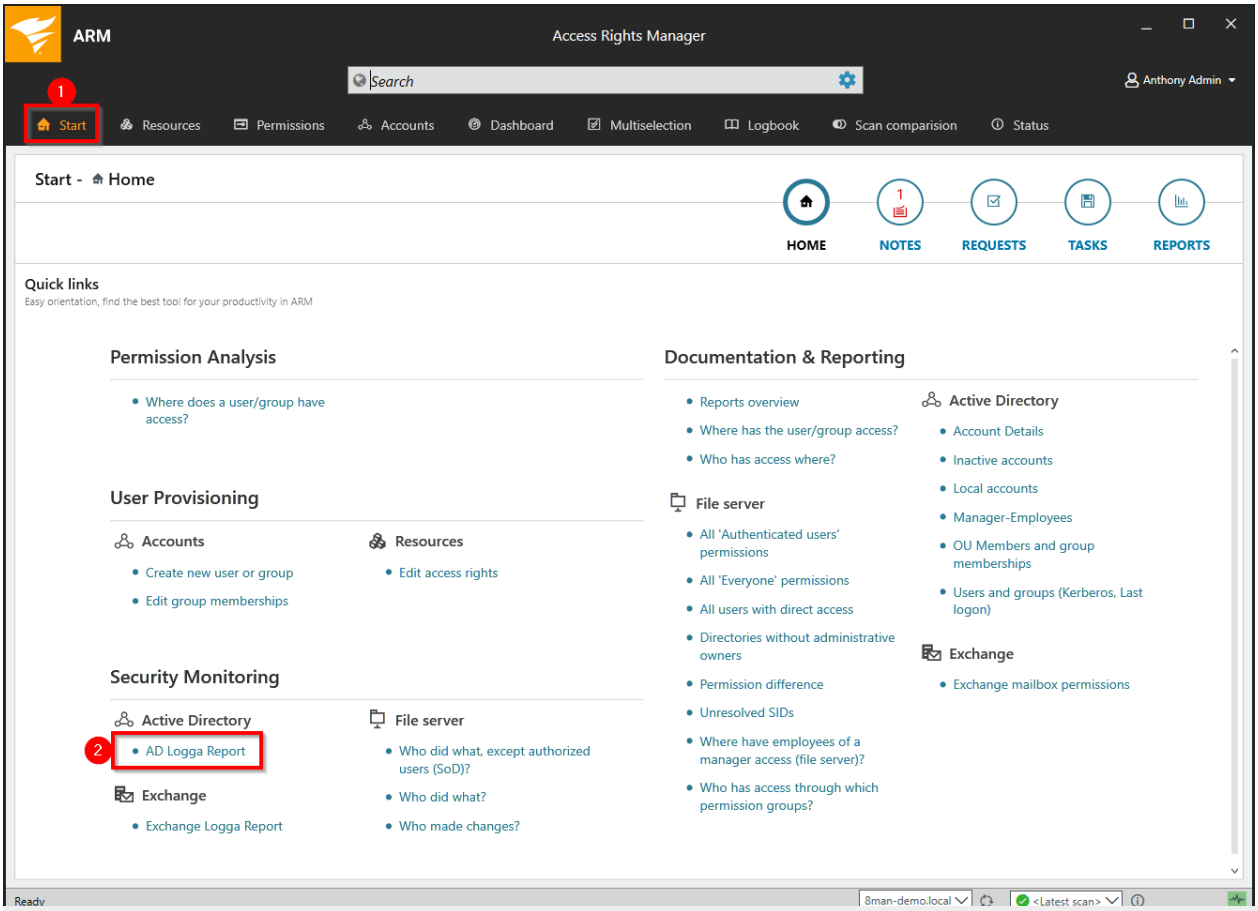
Related features

Analyze AD Logga events with the logbook

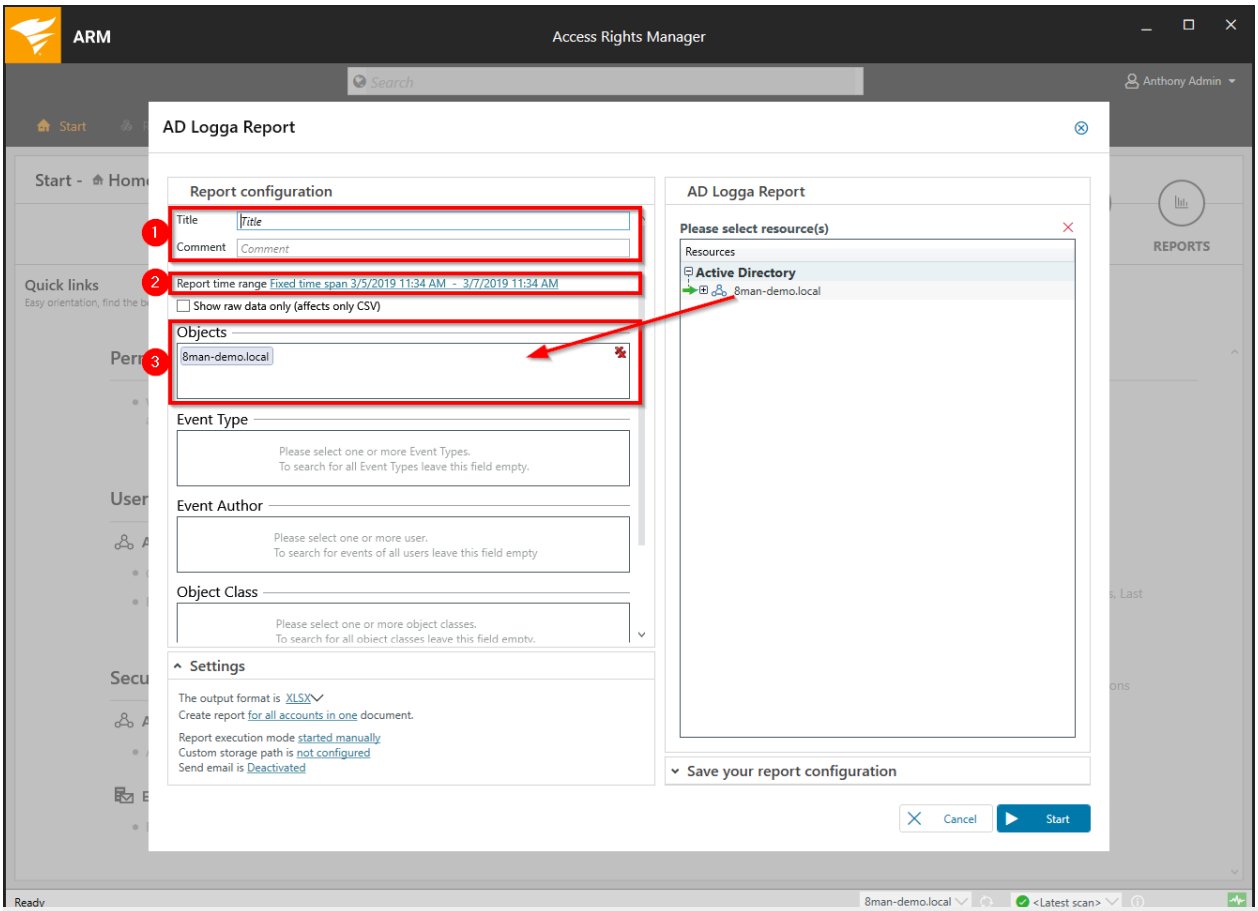
Set alerts for groups

Set alerts for user accounts

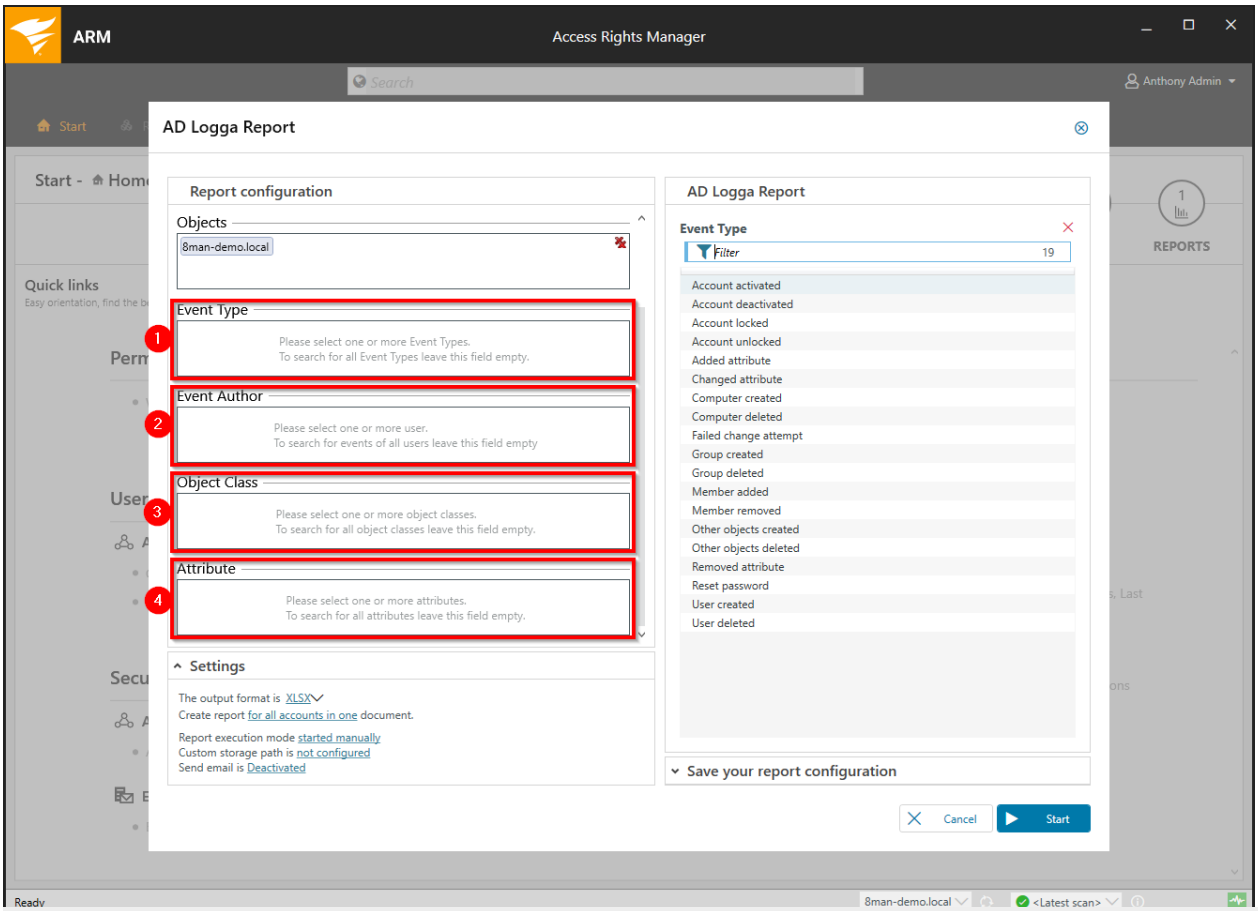
Step-by-step process



1. Select "Start".
2. Click on "AD Logga Report".

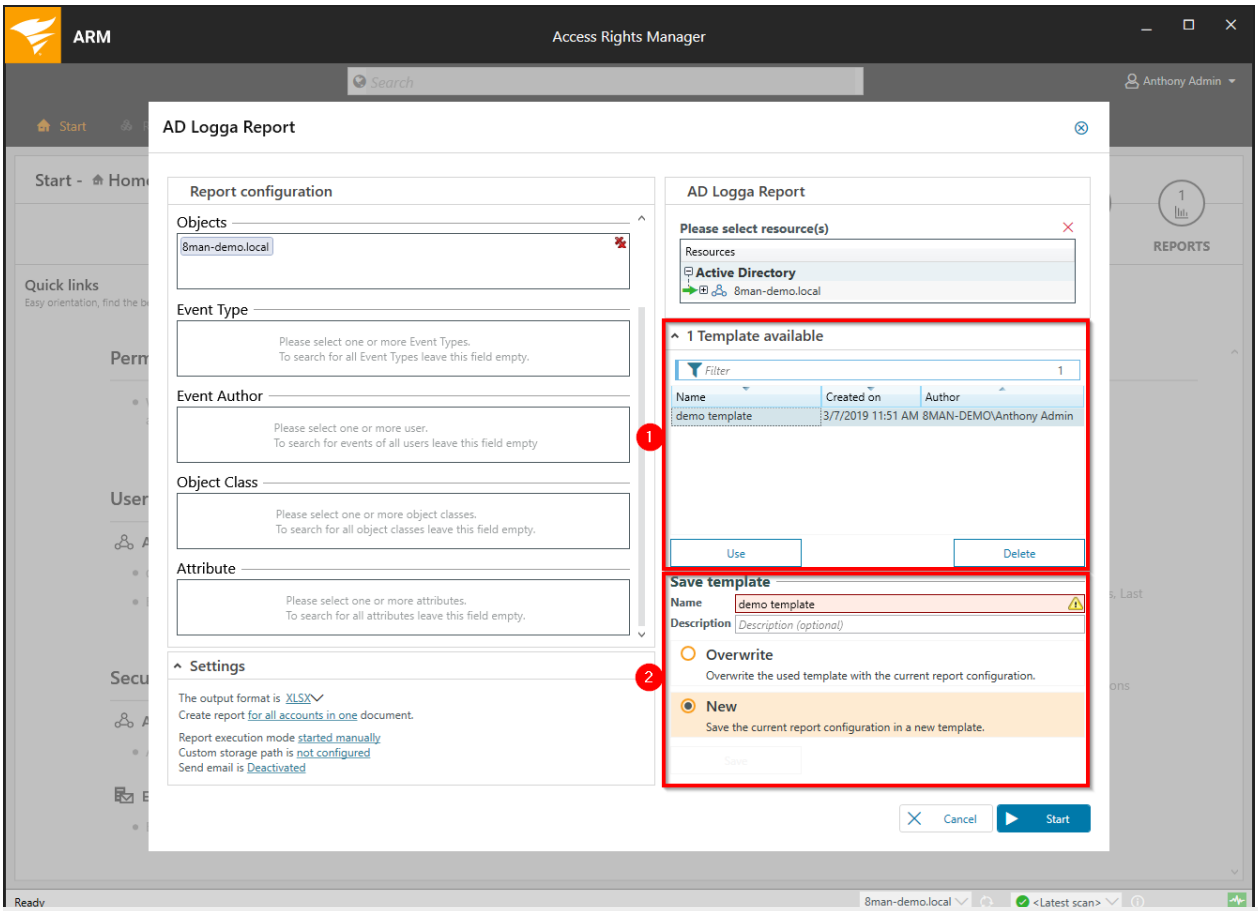


1. Enter a title for the report and add a comment.
2. Define the date range of the report.
3. Select domain objects whose events should be captured in the report.



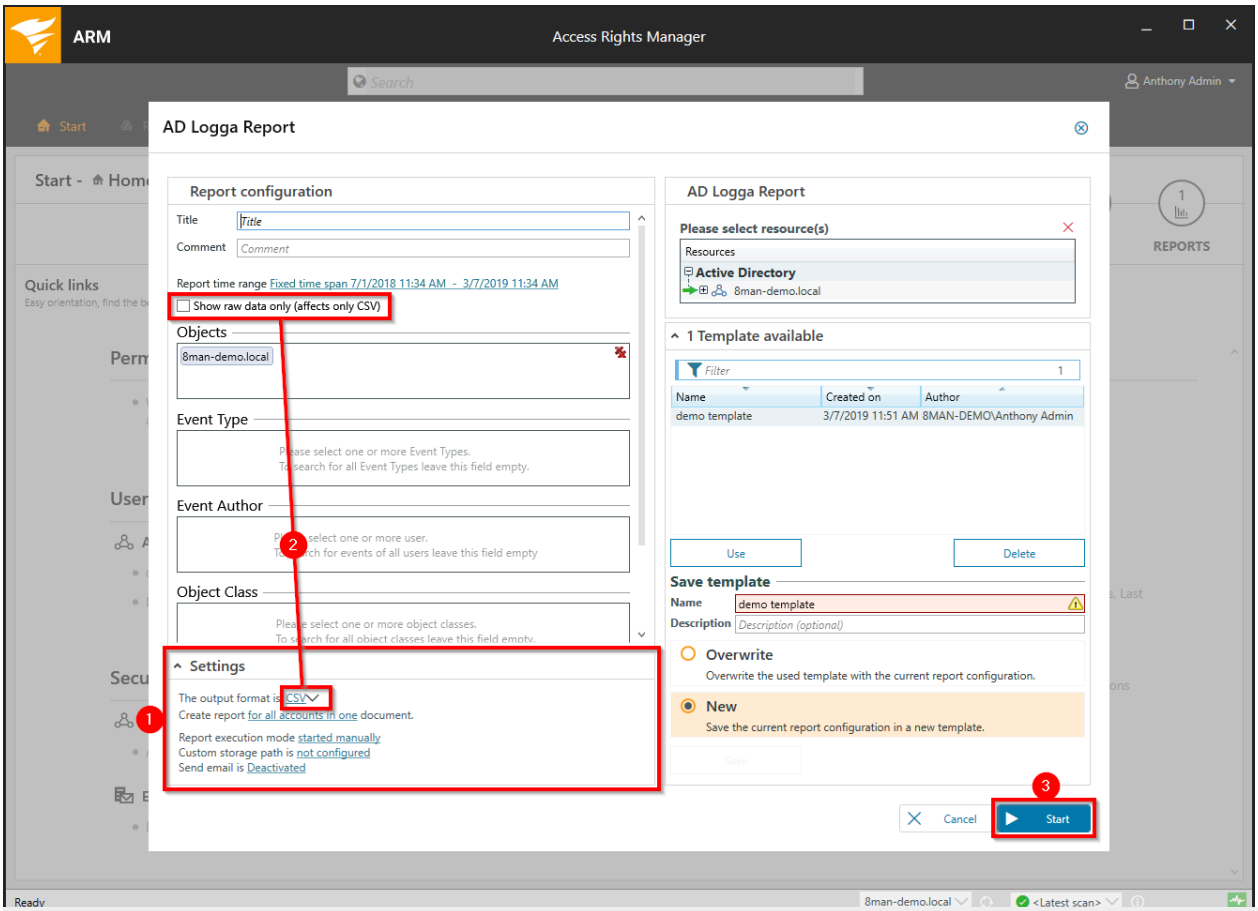
Define the range of the report by setting filters. By definition filters exclude the selected data.

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.



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.



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.

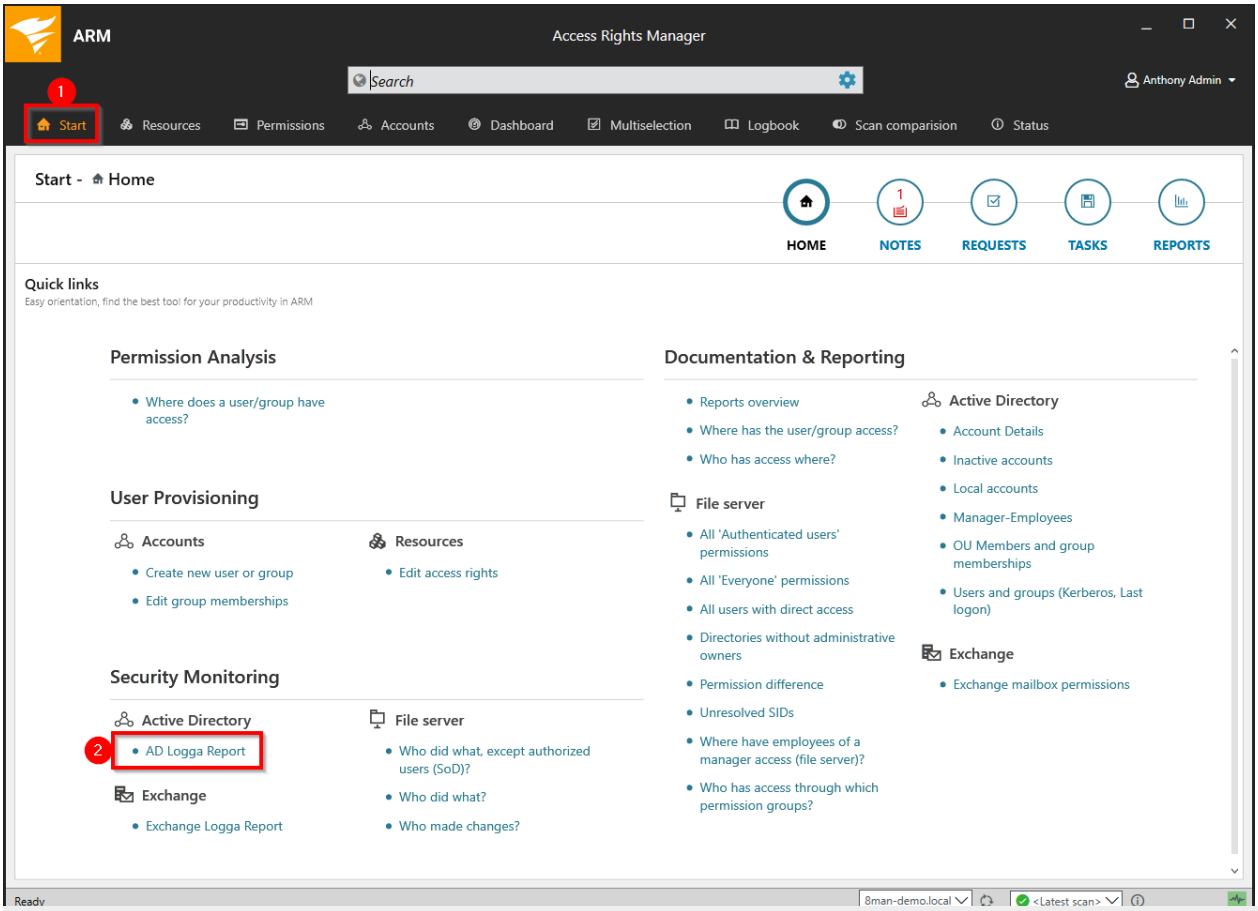
Related features

Analyze AD Logga events with the logbook

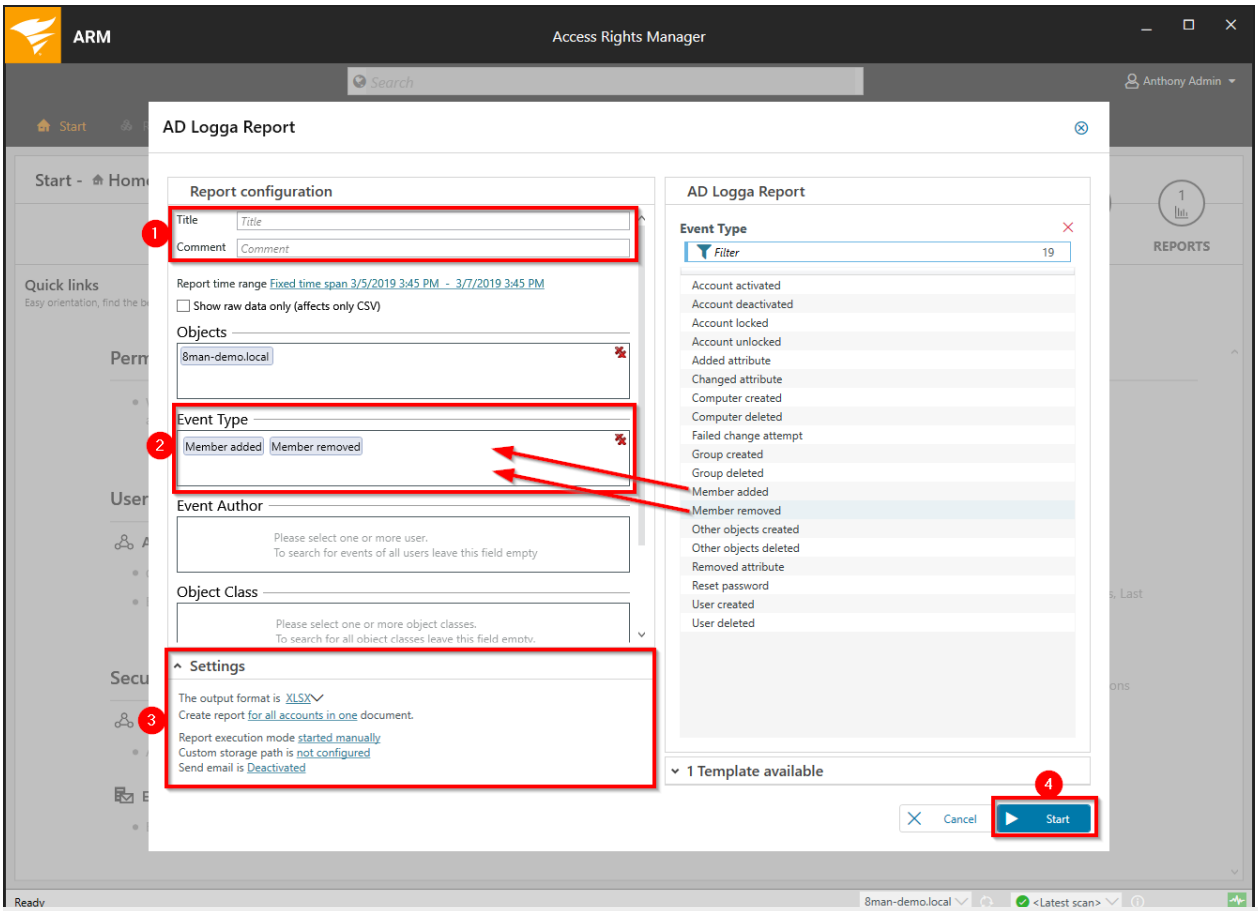
Set alerts for groups

Set alerts for user accounts

Step-by-step process



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 elses account ends with a locked user account. The AD Logga shows you from which computer the attack occurred.

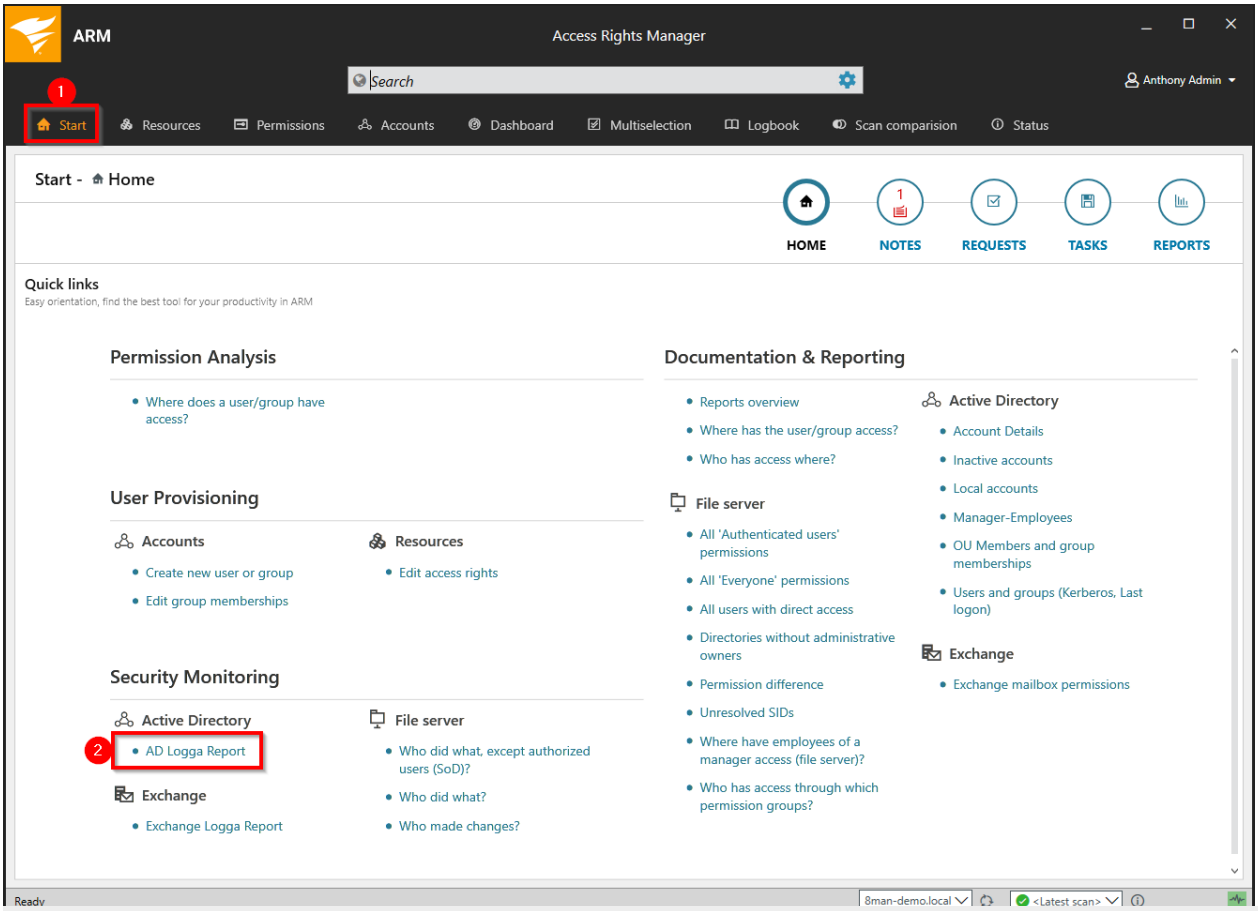
Related features

Analyze AD Logga events with the logbook

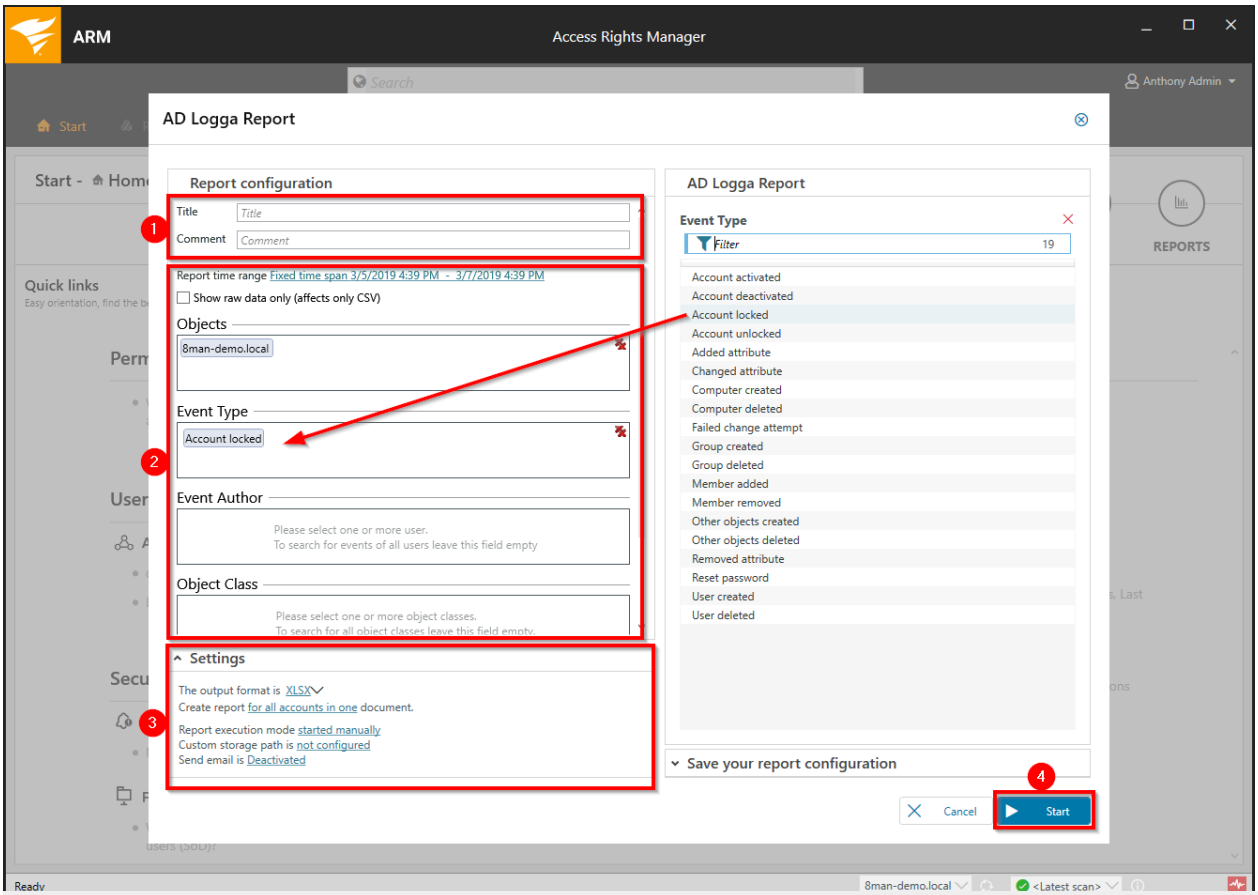
Set alerts for groups

Set alerts for user accounts

Step-by-step process



1. Select "Start".
2. Click on "AD Logga Report".



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.

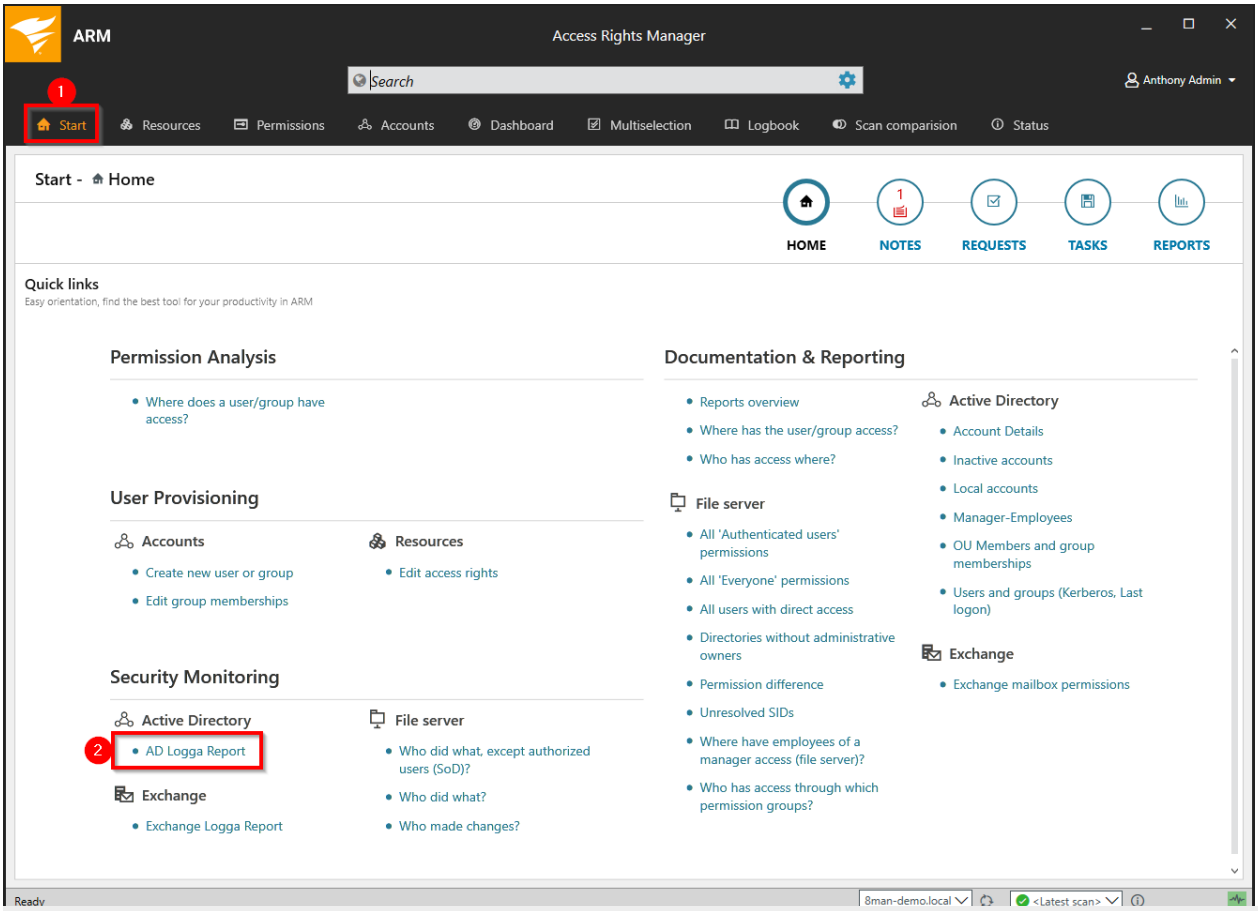
Related features

Analyze AD Logga events with the logbook

Set alerts for groups

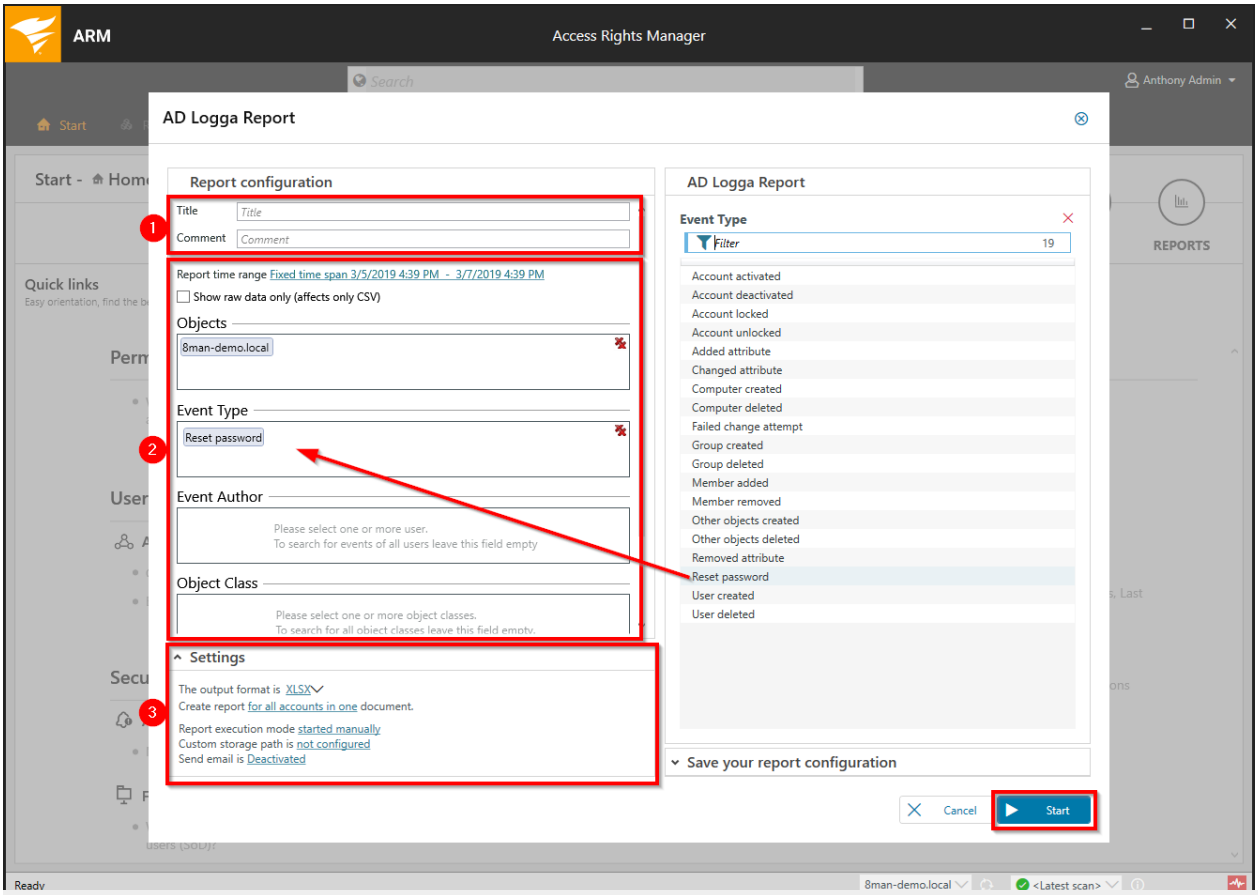
Set alerts for user accounts

Step-by-step process



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 "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.

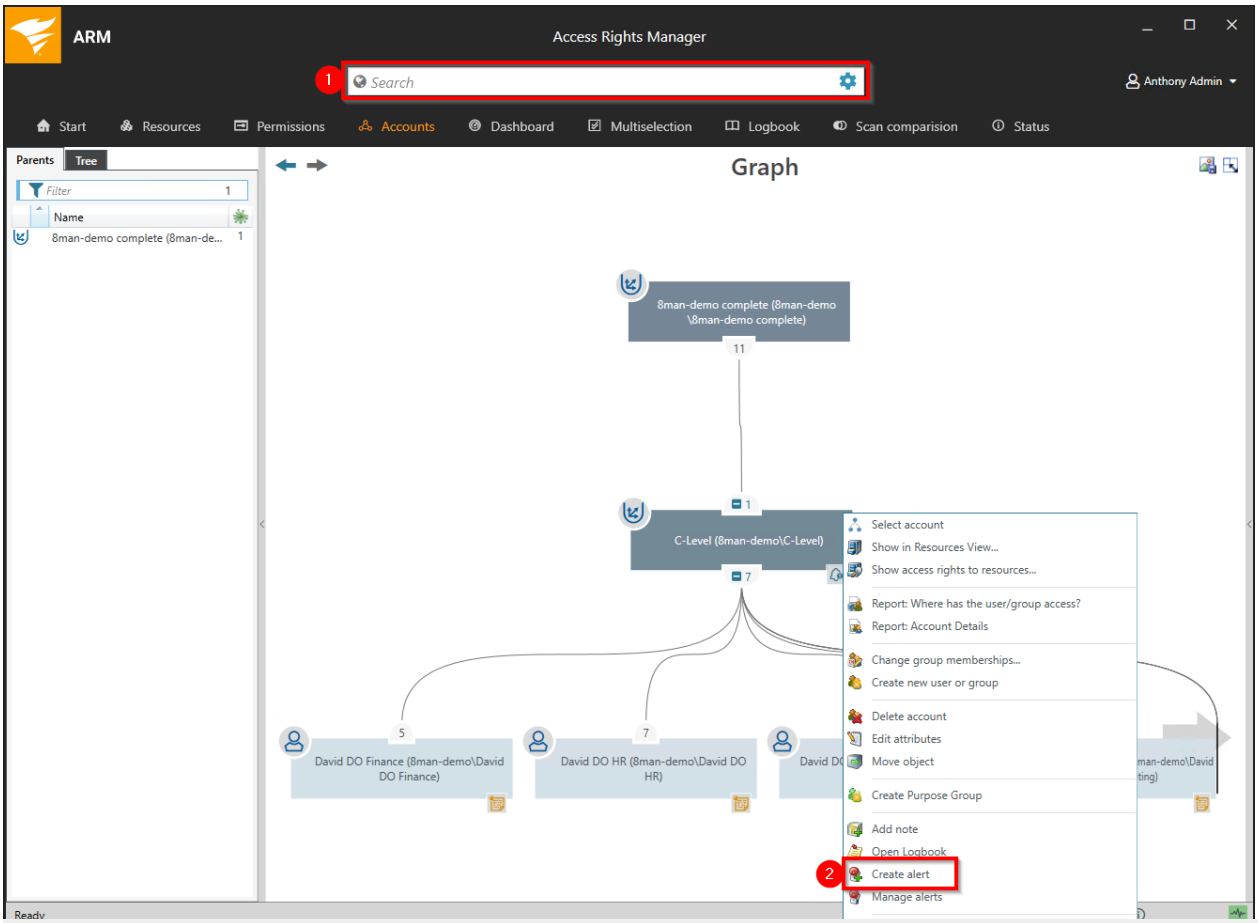
Related features

Set alerts for user accounts

Set alerts for OUs/domains

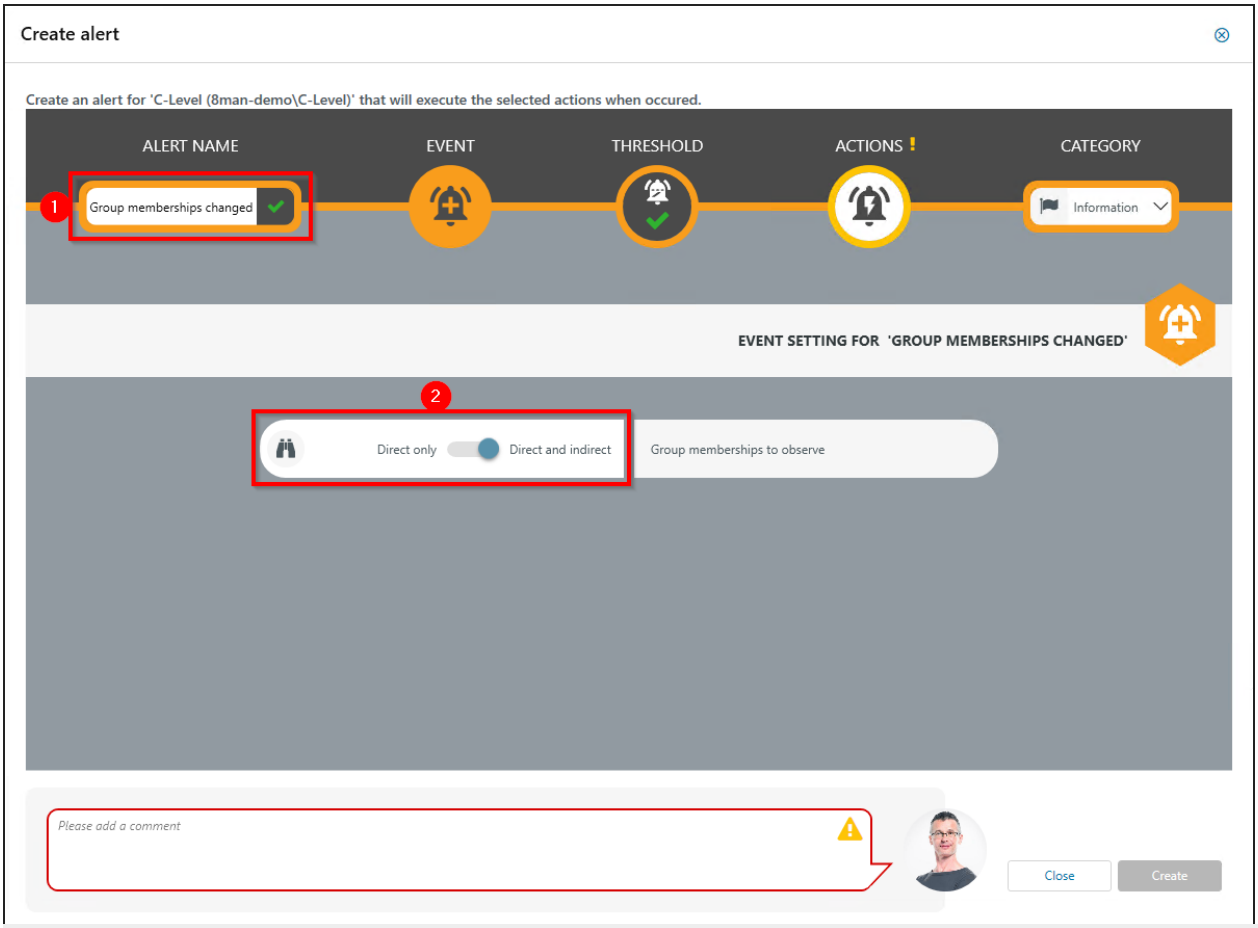
Manage alerts

Step-by-step process

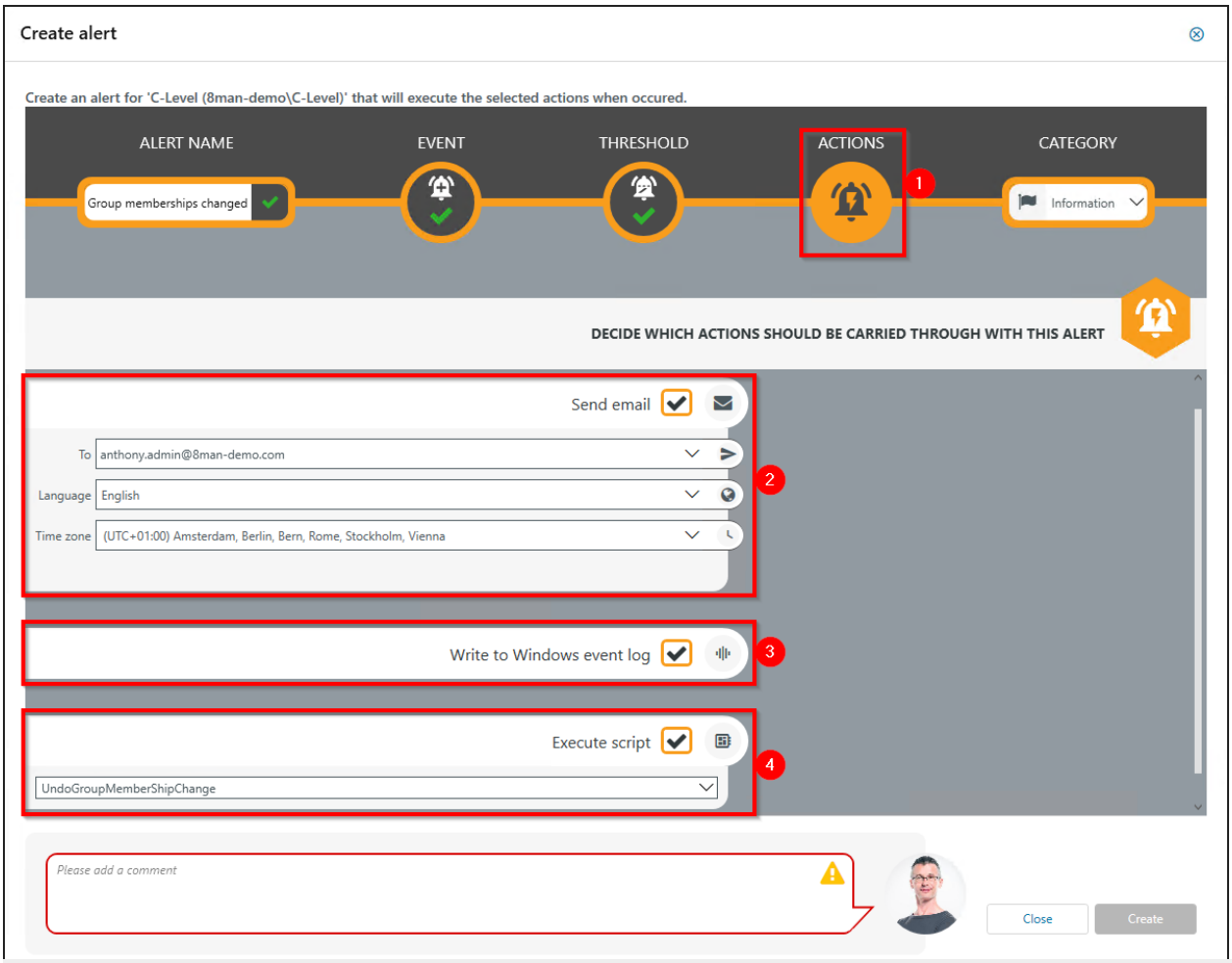


1. Use the search to find the desired group.

2. Right-click on the group and select "Create alert" from the context menu.



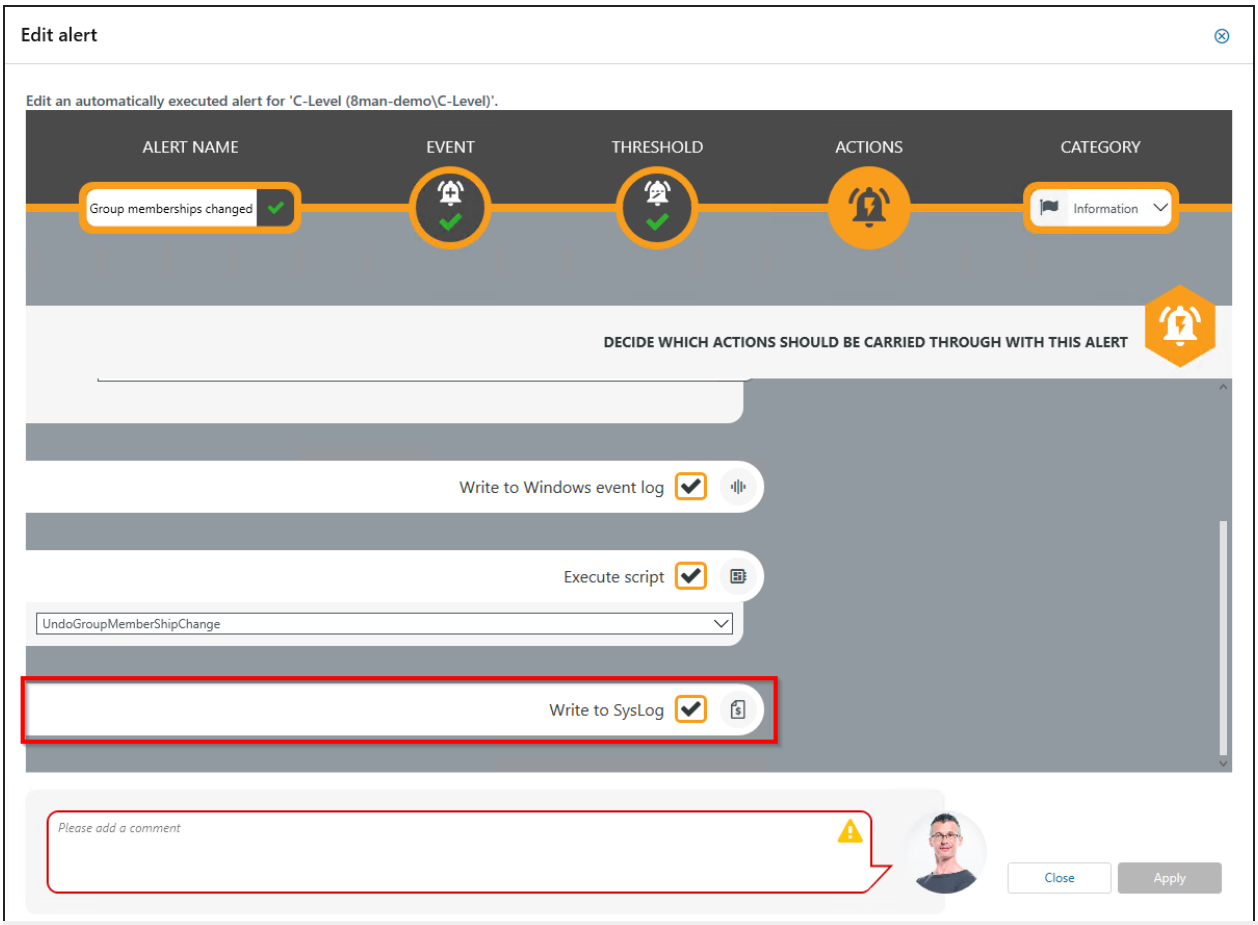
1. Enter a title for the alert.
2. Select whether only direct or direct and indirect group membership changes (recommended) trigger an alert.



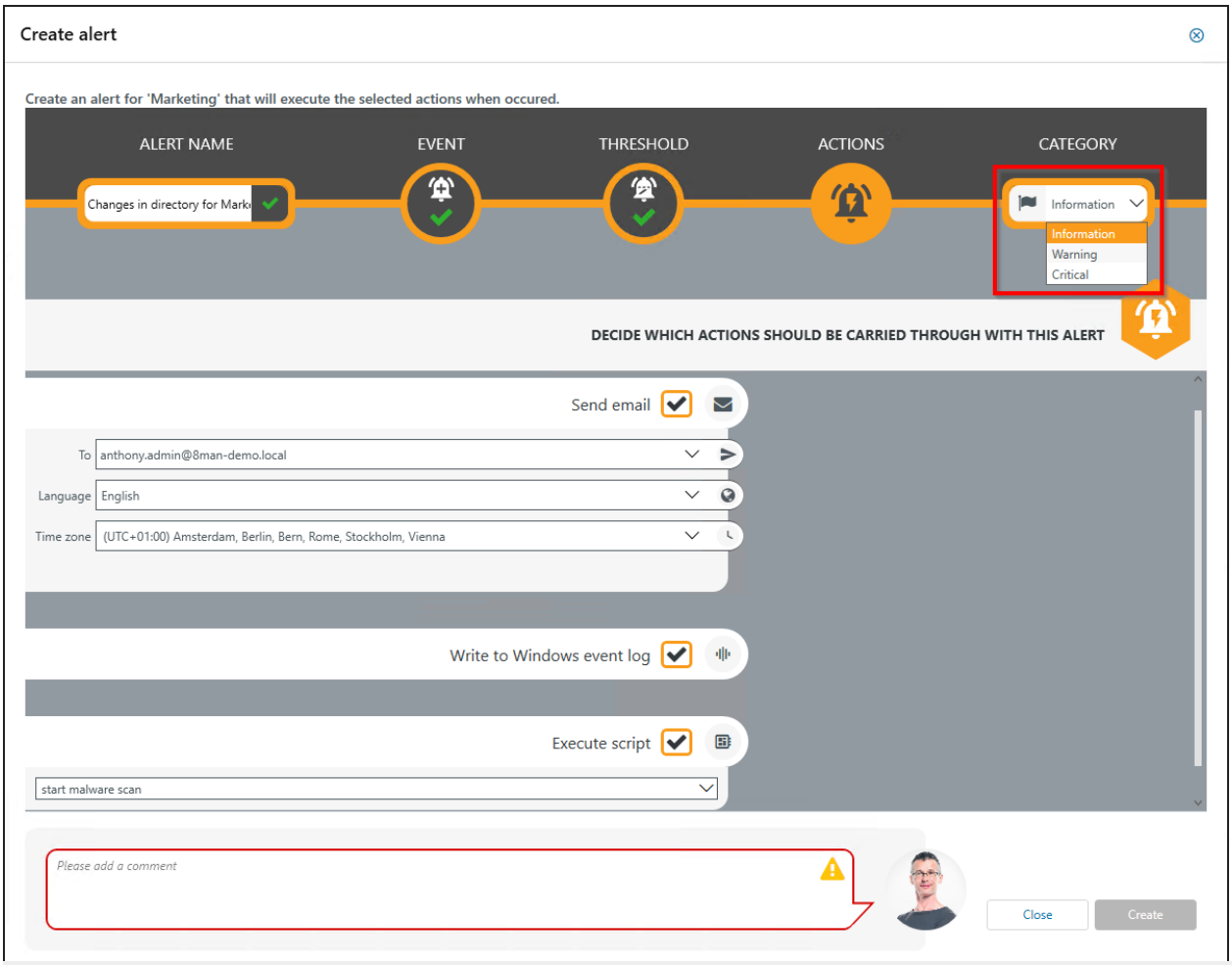
1. Choose Actions.
   Here you specify which actions are executed when an alert is triggered. You must activate at least one action.
2. Activate the option if an email should be sent in case of an alert.

The content of the emails can be customized. This is analogous to the recertification emails.

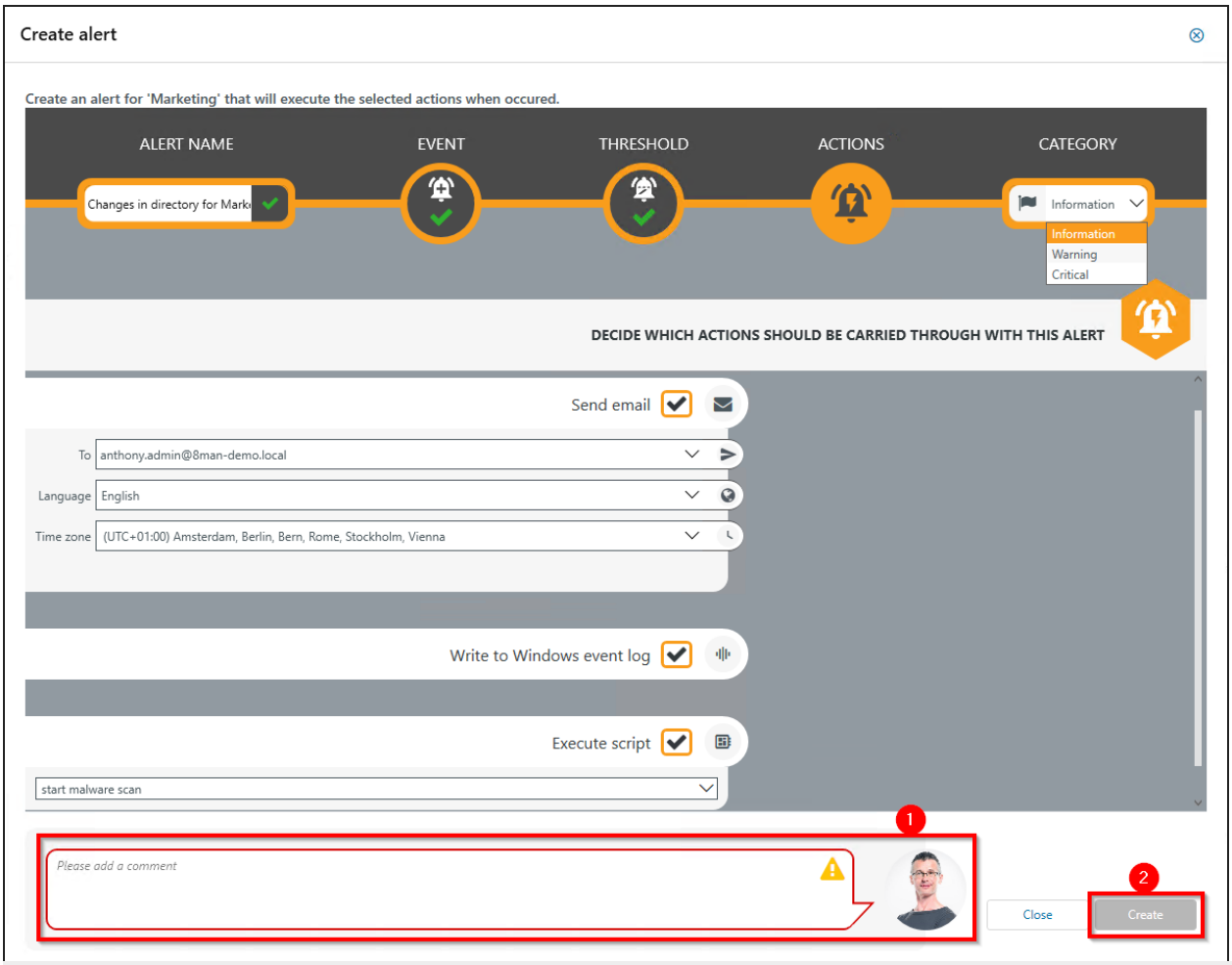
3. The alarm is written to the Windows event log using the categorization. This option is especially useful if you are using a SIEM system that monitors the Windows Event Log.
4. Enable the execution of a script. To be able to activate this option, a script configuration for alerts must exist.



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.



Choose a category. This is used when writing to the Windows Event Log and for the email subject.



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.

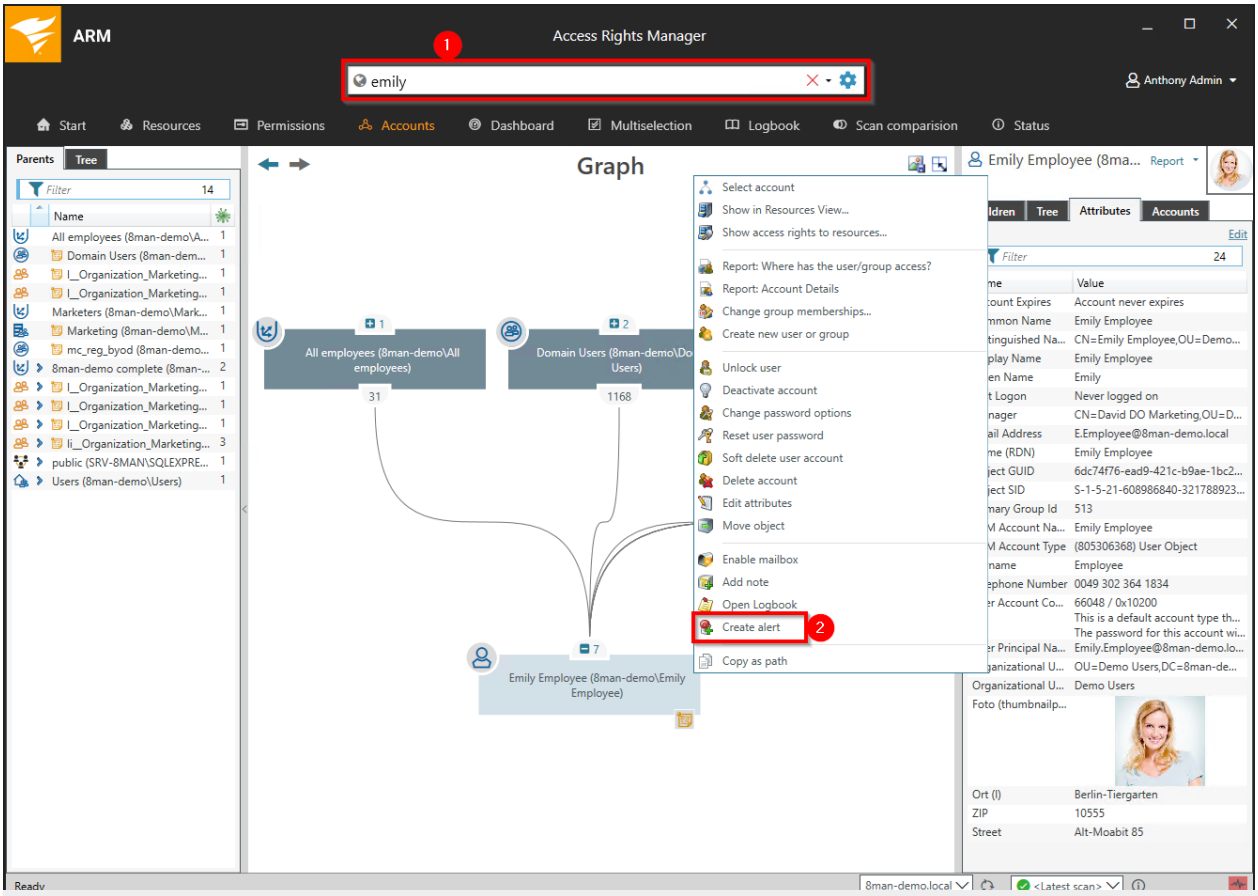
Related features

Set alerts for groups

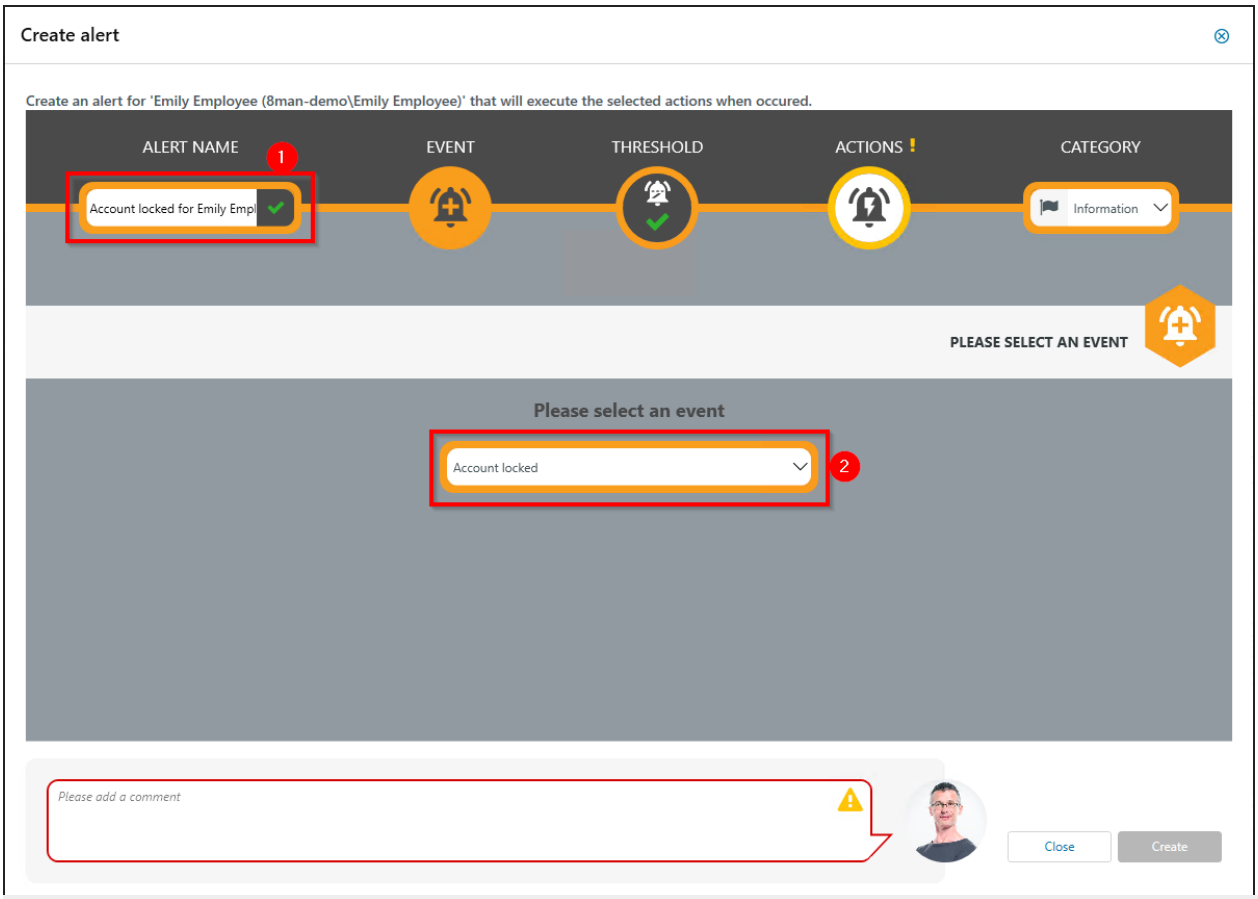
Set alerts for OUs/domains

Manage alerts

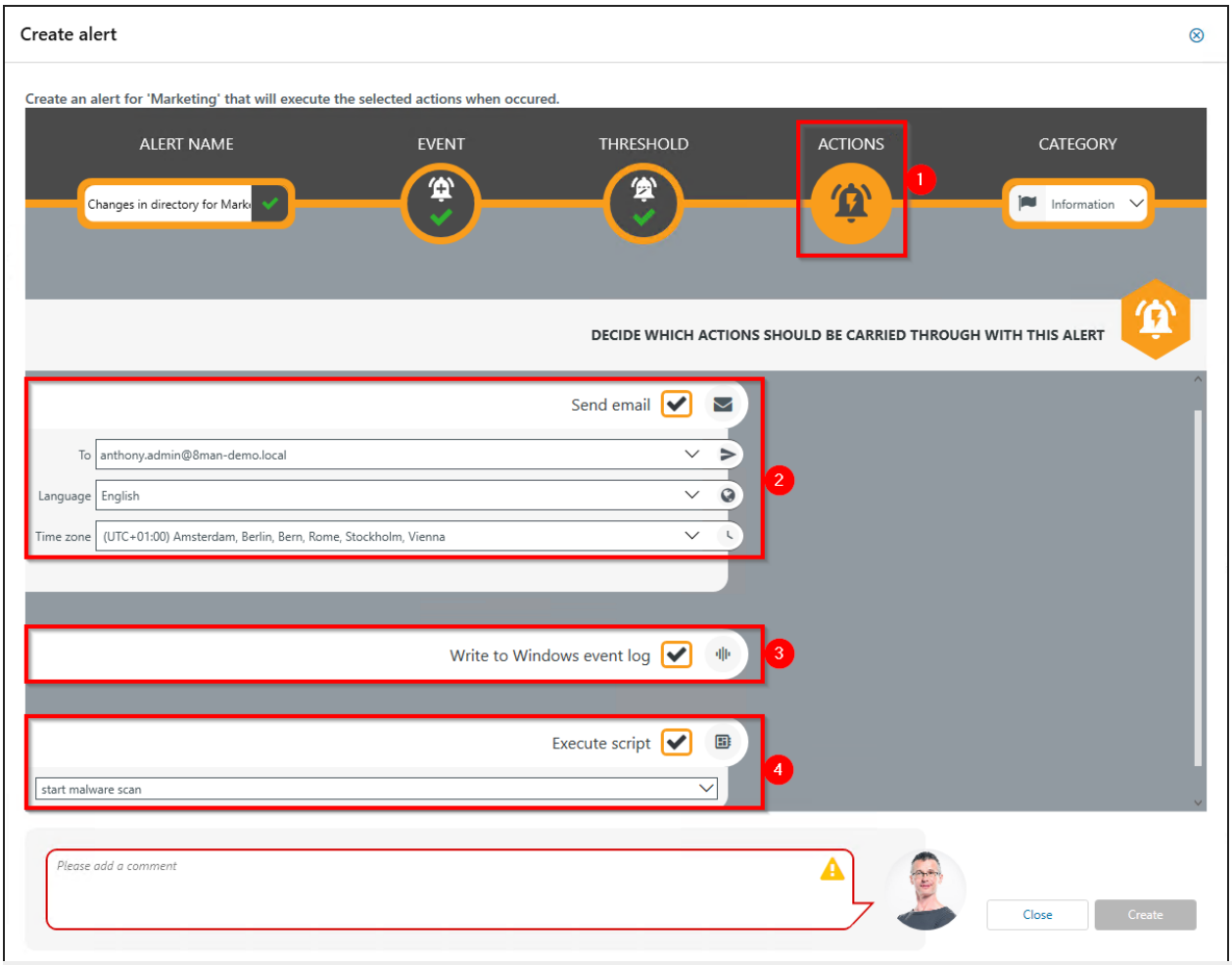
Step-by-step process



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.



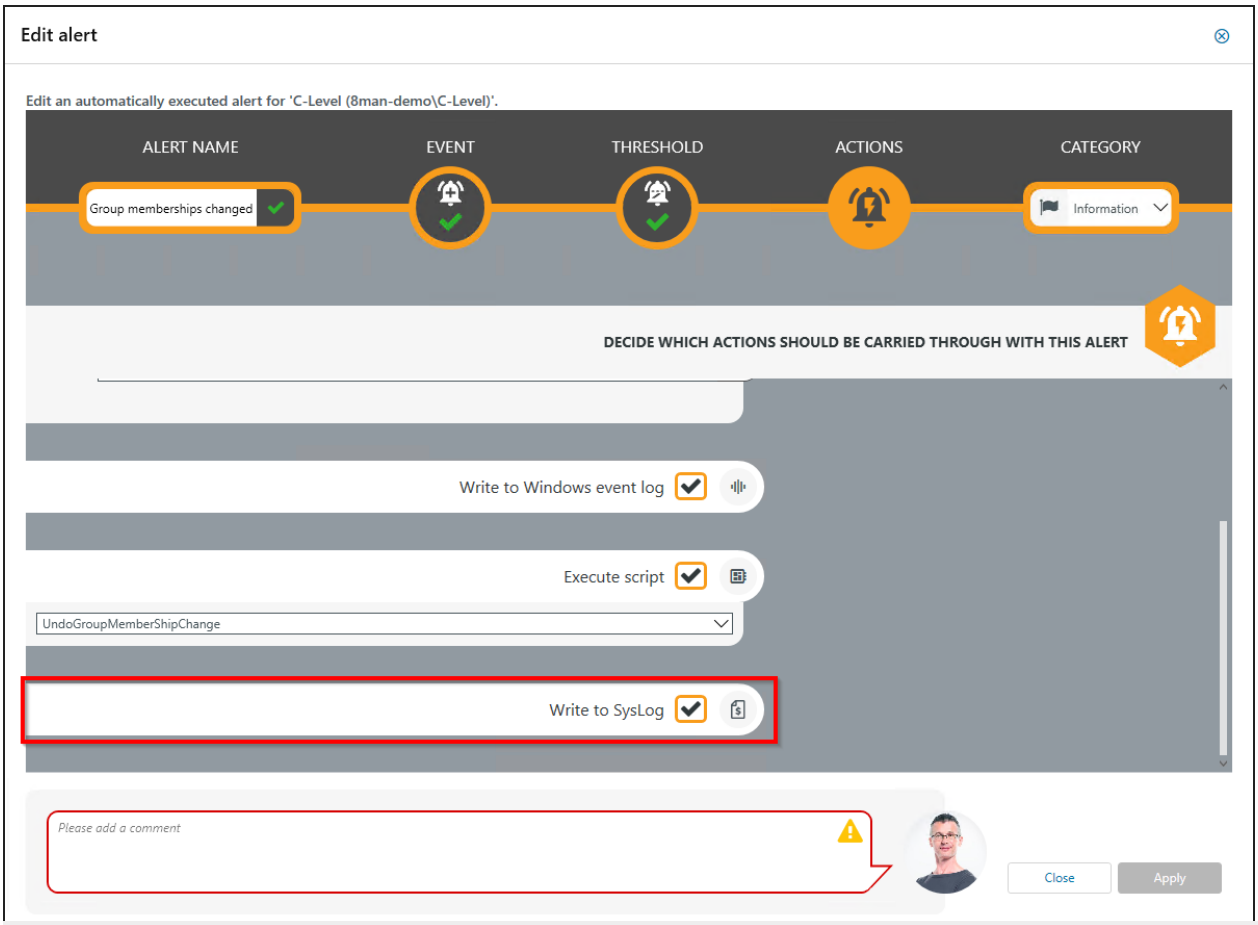
1. Enter a title for the alert.
2. Select an event type that triggers the alert.



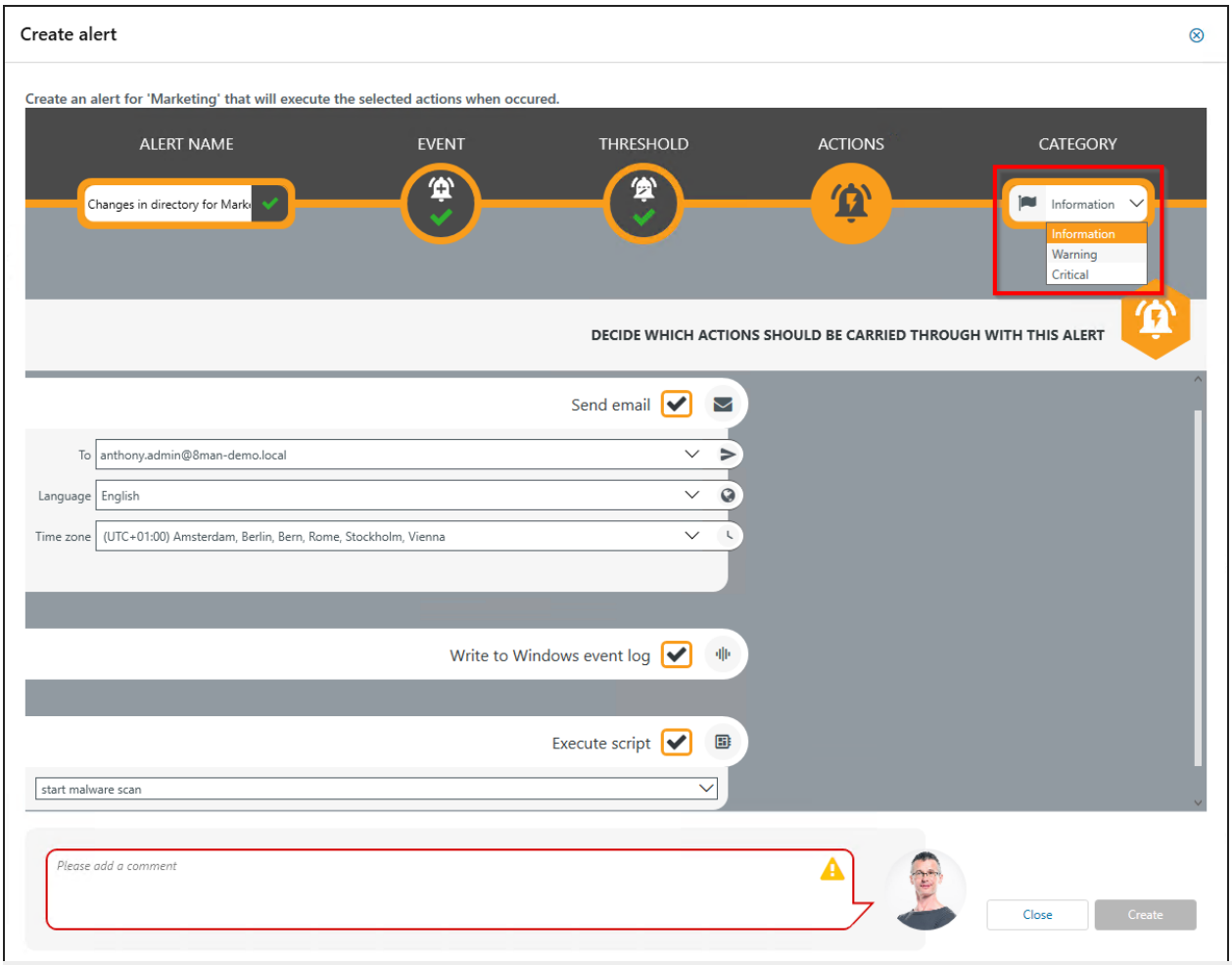
1. Choose Actions.
   Here you specify which actions are executed when an alert is triggered. You must activate at least one action.
2. Activate the option if an email should be sent in case of an alert.

The content of the emails can be customized. This is analogous to the recertification emails.

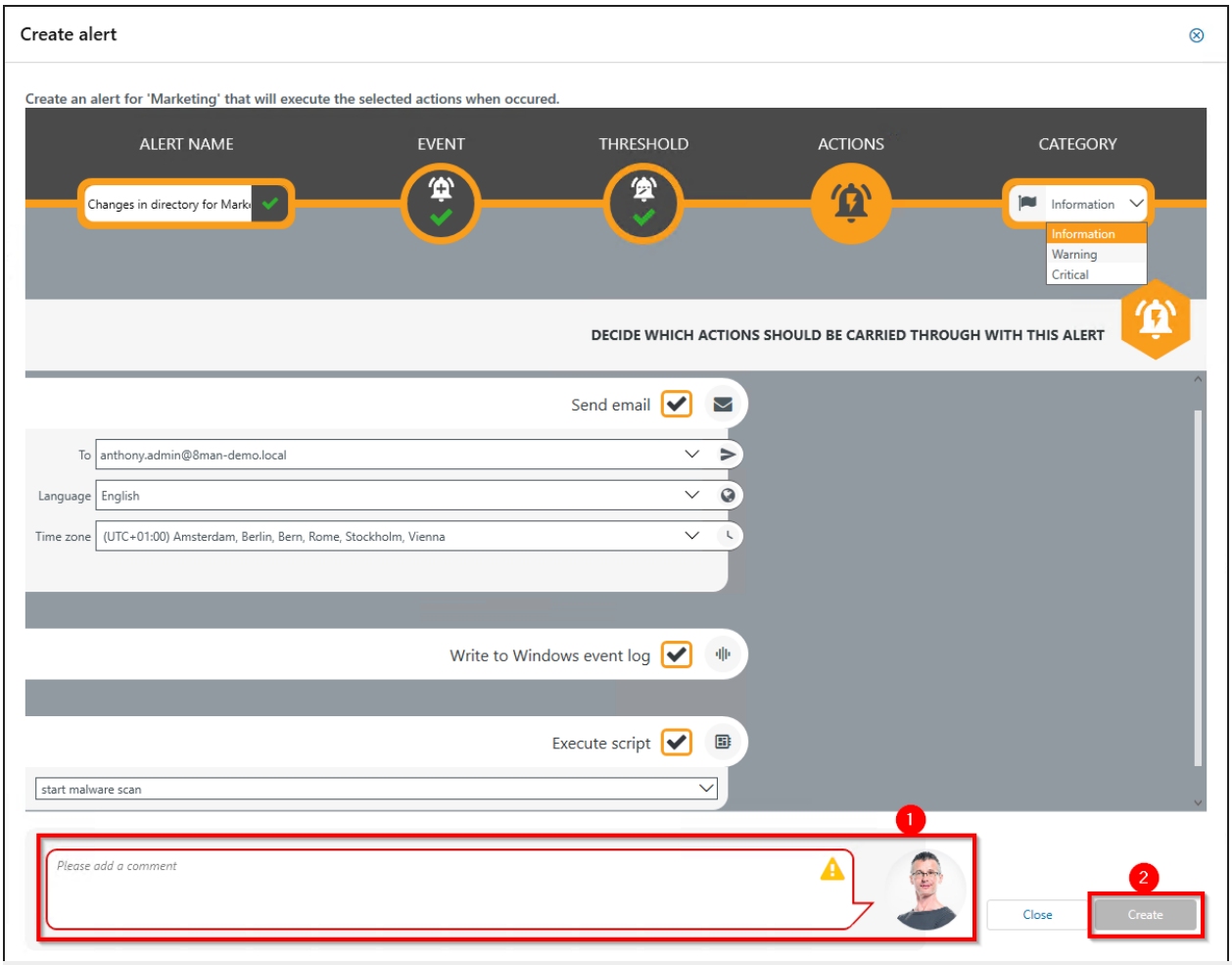
3. The alarm is written to the Windows event log using the categorization. This option is especially useful if you are using a SIEM system that monitors the Windows Event Log.
4. Enable the execution of a script. To be able to activate this option, a script configuration for alerts must exist.



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.



Choose a category. This is used when writing to the Windows Event Log and for the email subject.



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.

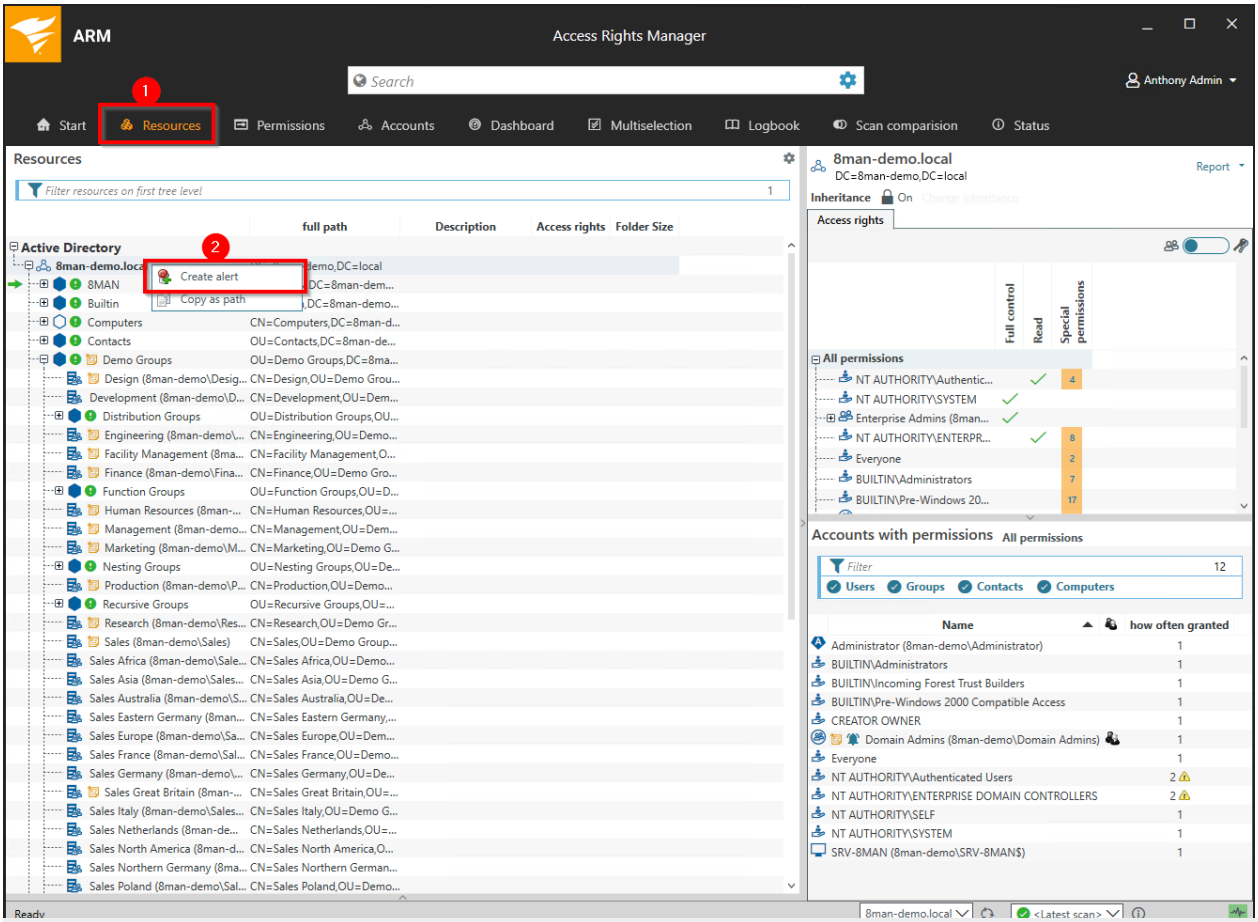
Related features

Set alerts for user accounts

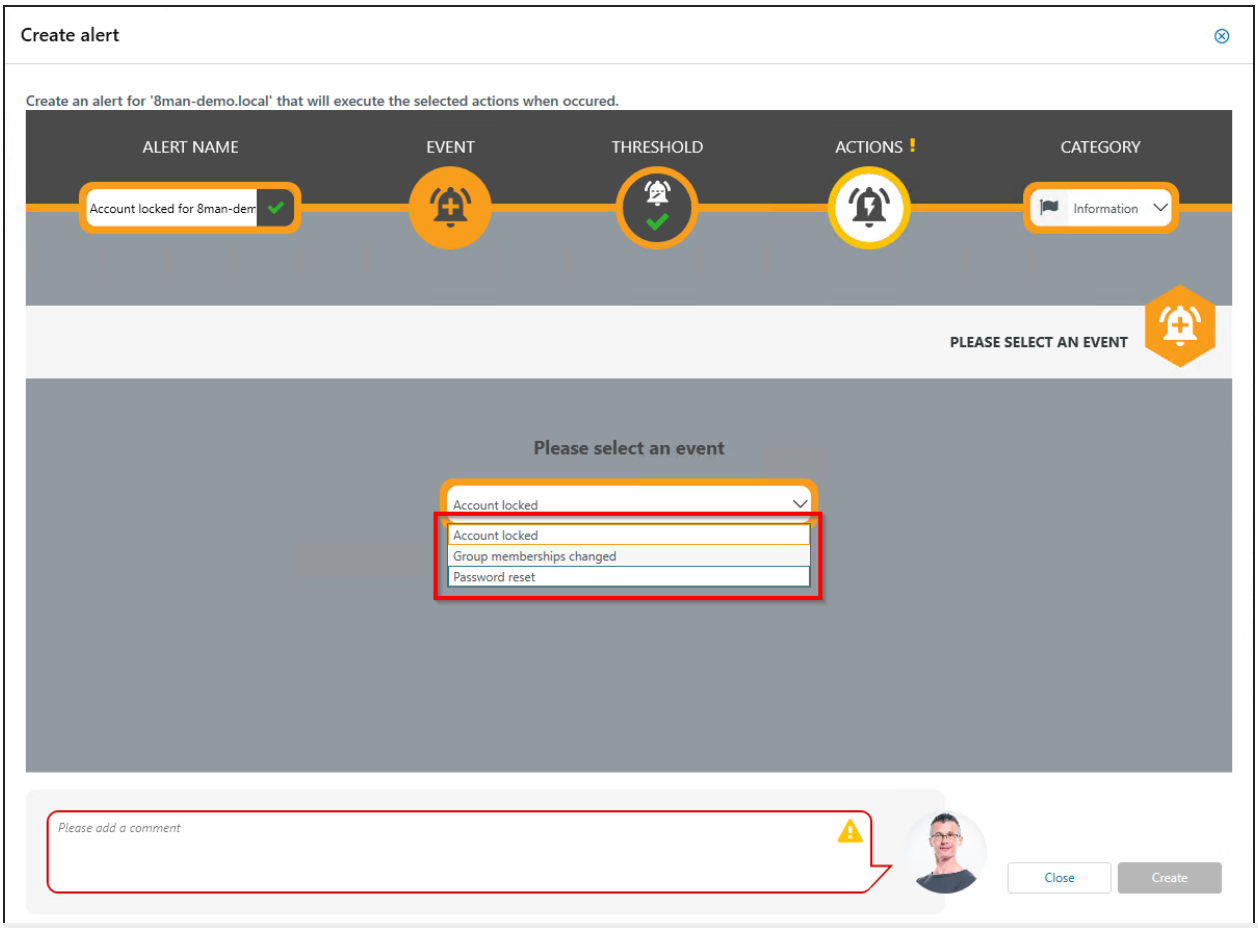
Set alerts for groups

Manage alerts

Step-by-step process

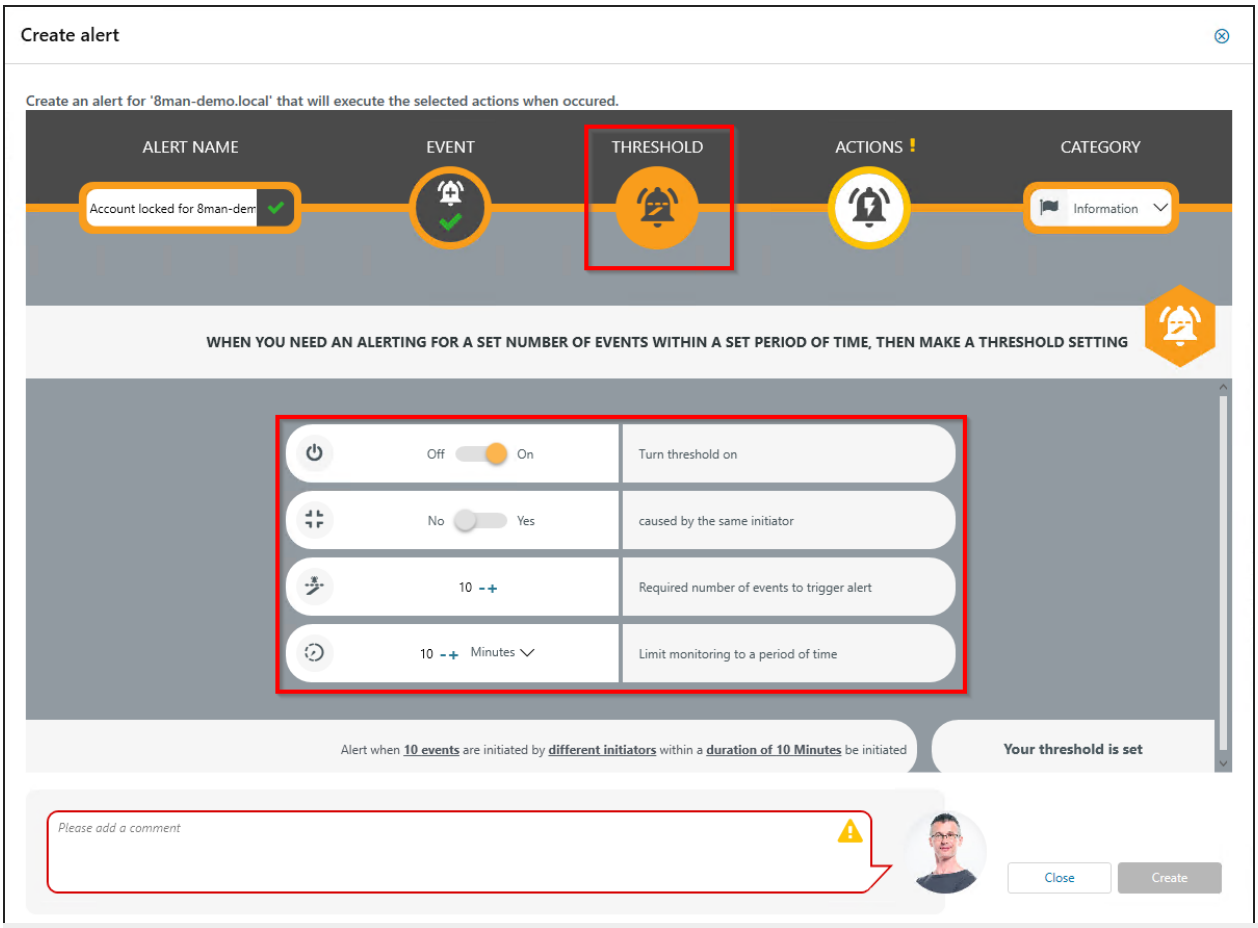


1. Select Resources.
2. Navigate to the desired domain, OU or container. You can alternatively use the search to find the desired AD object. Right-click on it and select "Create alert" from the context menu.

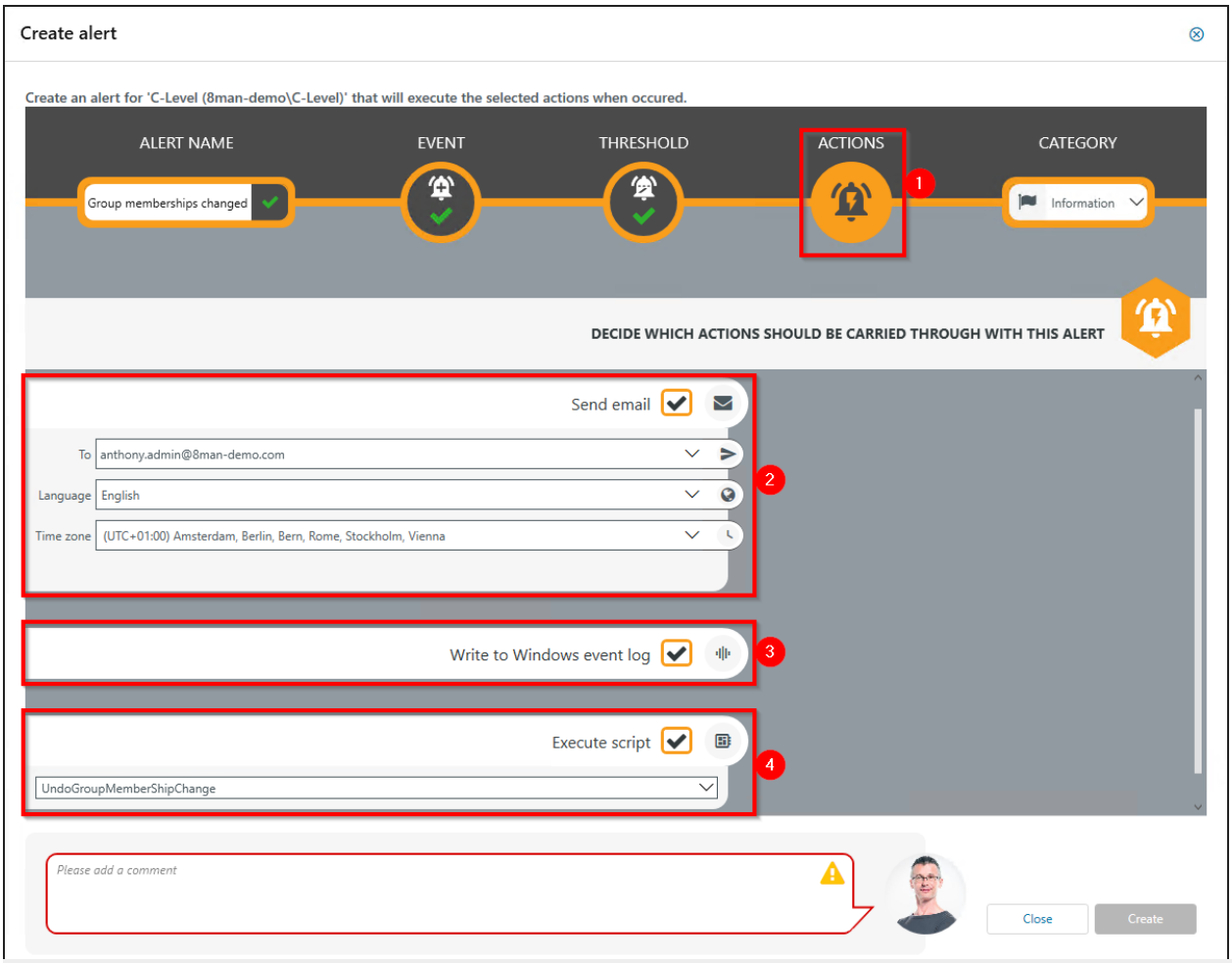


Select one of the following event types that can trigger the alert:

- Account locked
- Group membership changed
- Password reset



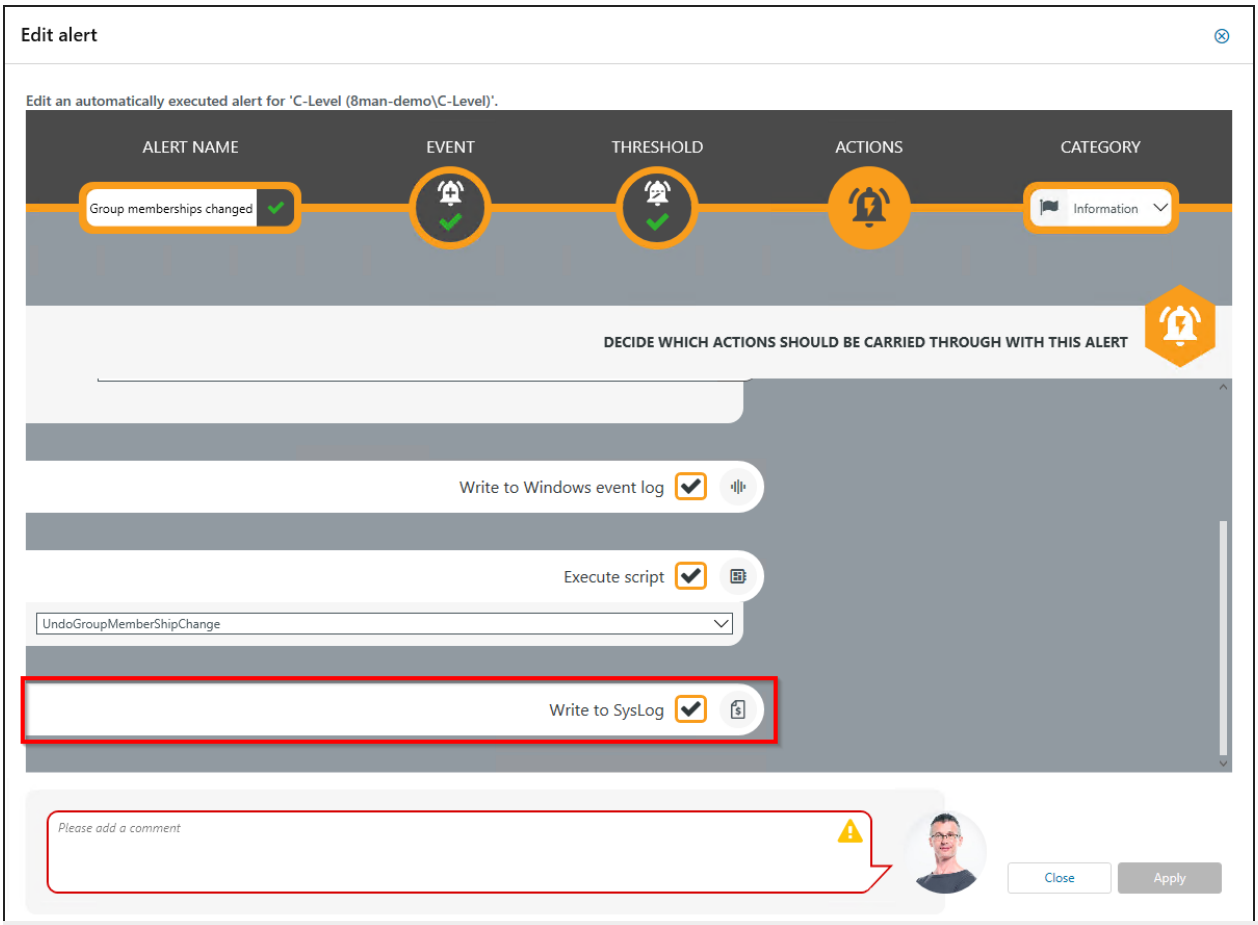
You can set a threshold if needed.



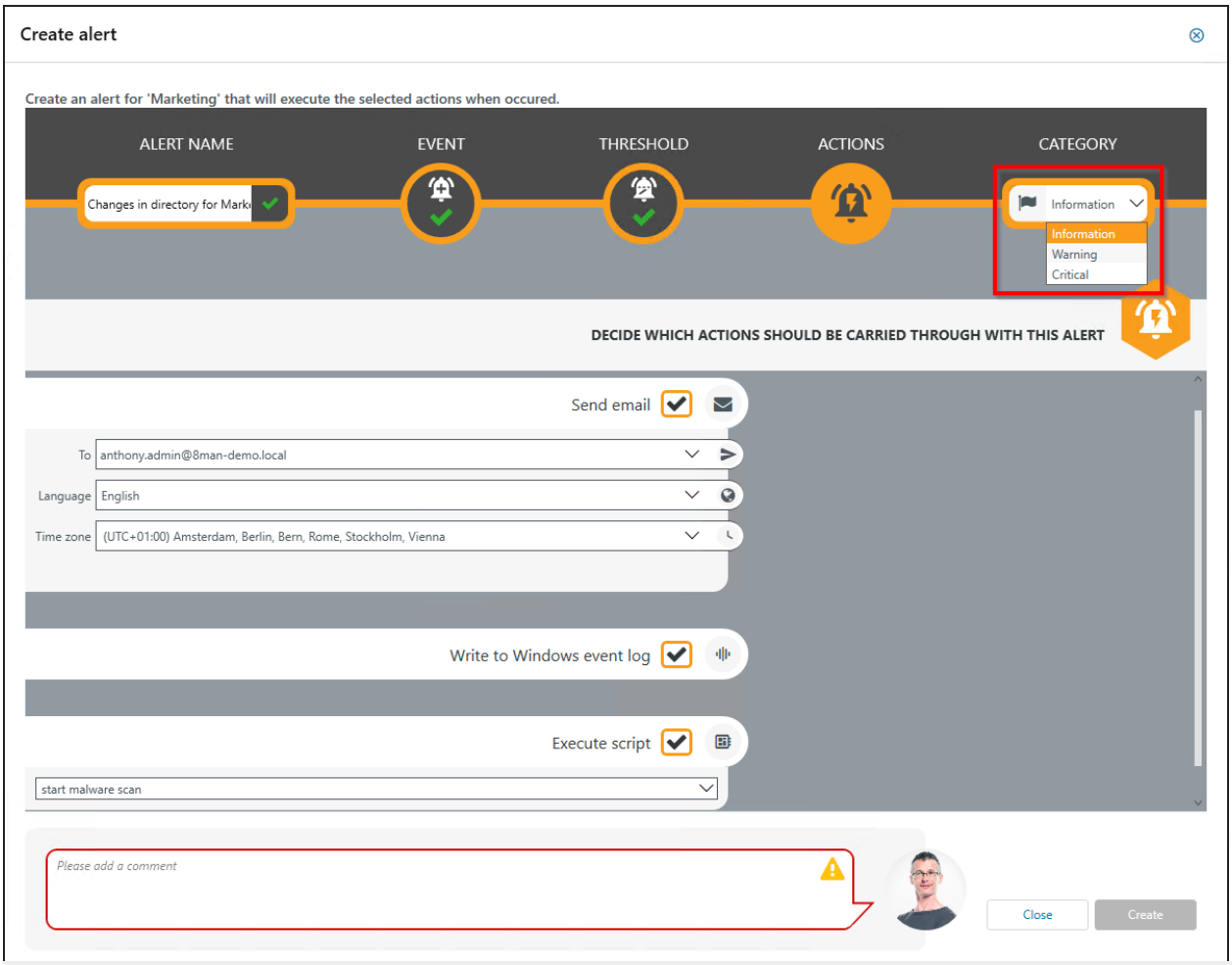
1. Choose Actions.
   Here you specify which actions are executed when an alert is triggered. You must activate at least one action.
2. Activate the option if an email should be sent in case of an alert.

The content of the emails can be customized. This is analogous to the recertification emails.

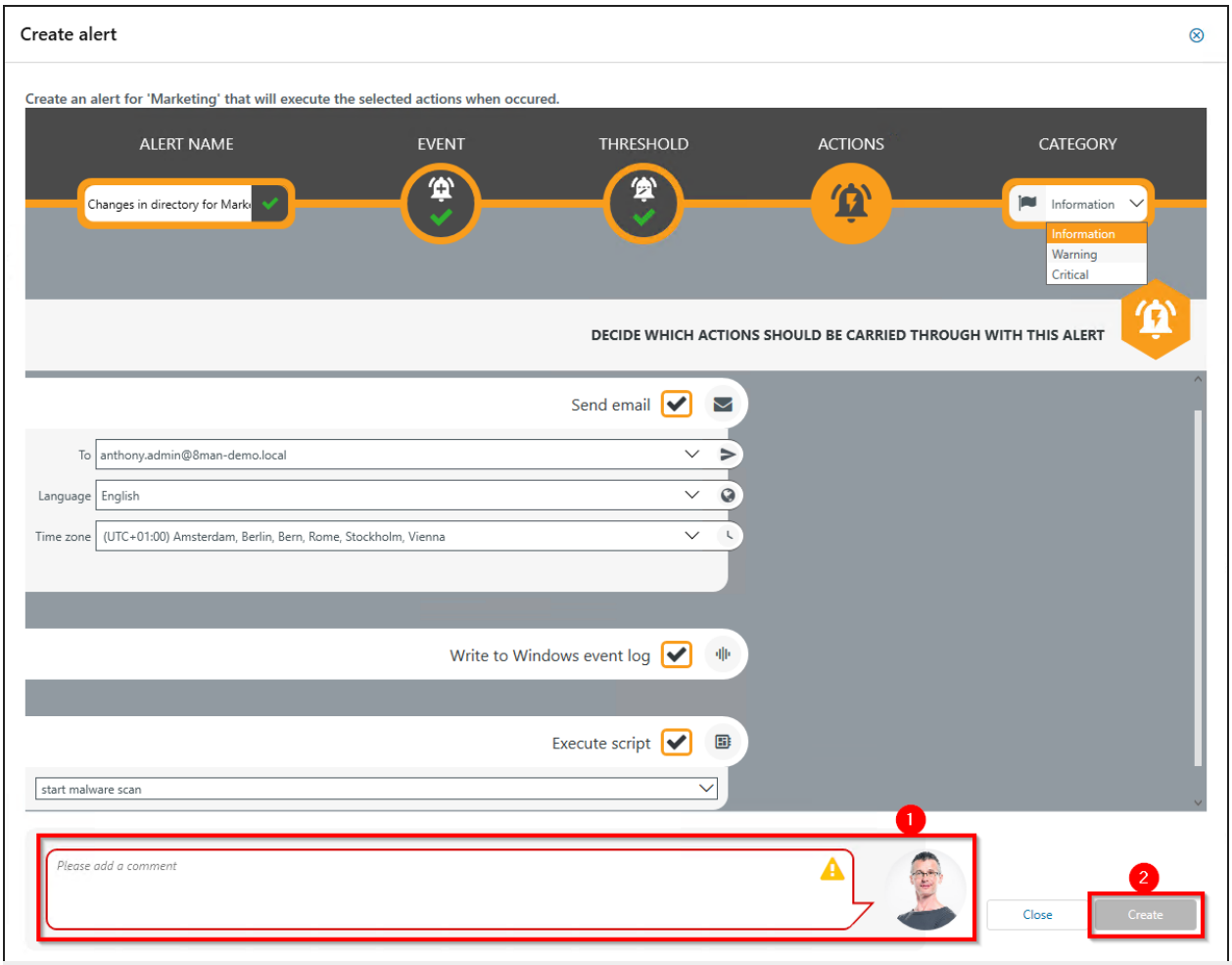
3. The alert is written to the Windows Event Log. The categorization is used. This option is especially useful if you are using a SIEM system.
4. Enable the execution of a script. To activate this option, a script configuration for alerts must be stored.



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.



Choose a category. This is used when writing to the Windows Event Log and for the email subject.



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 date 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

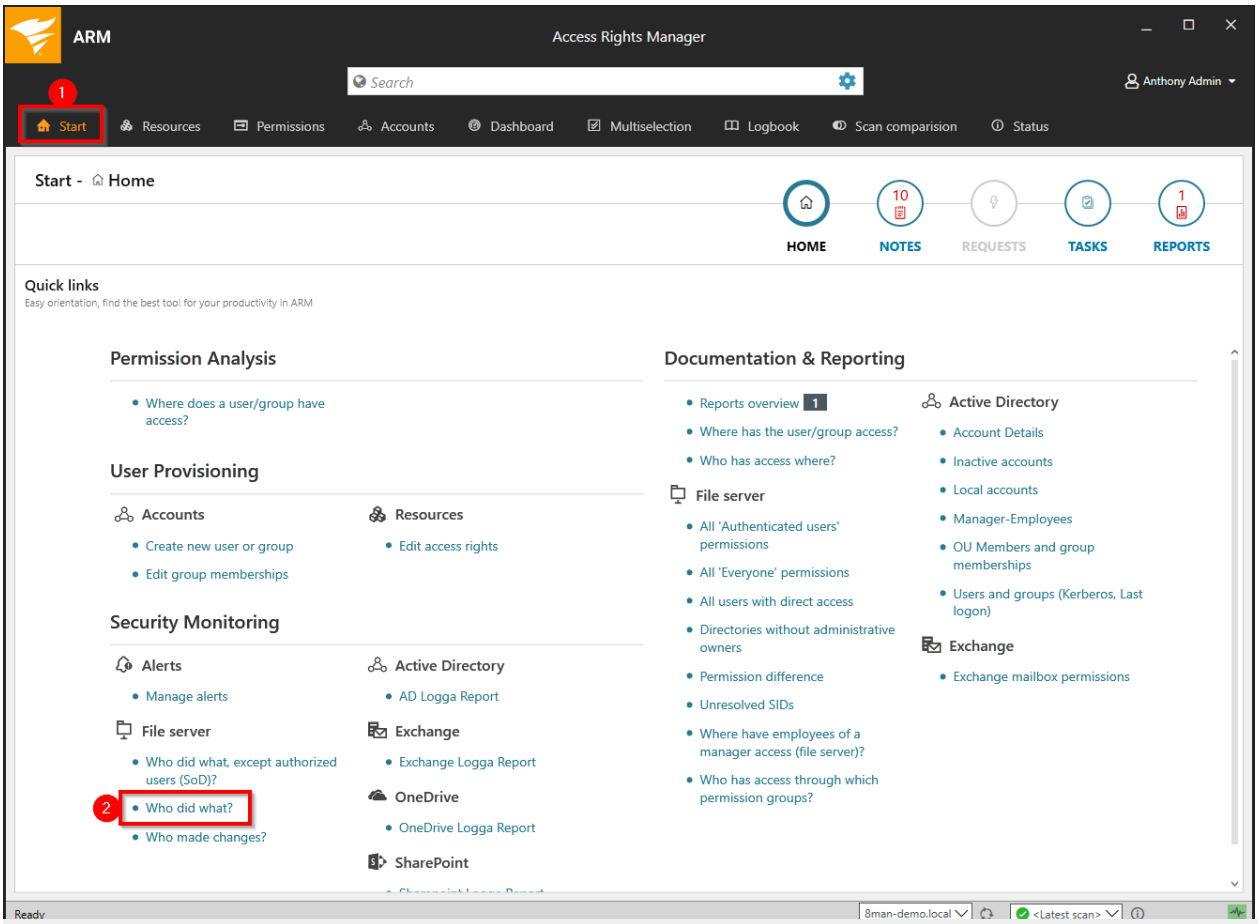
Background / Value

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.

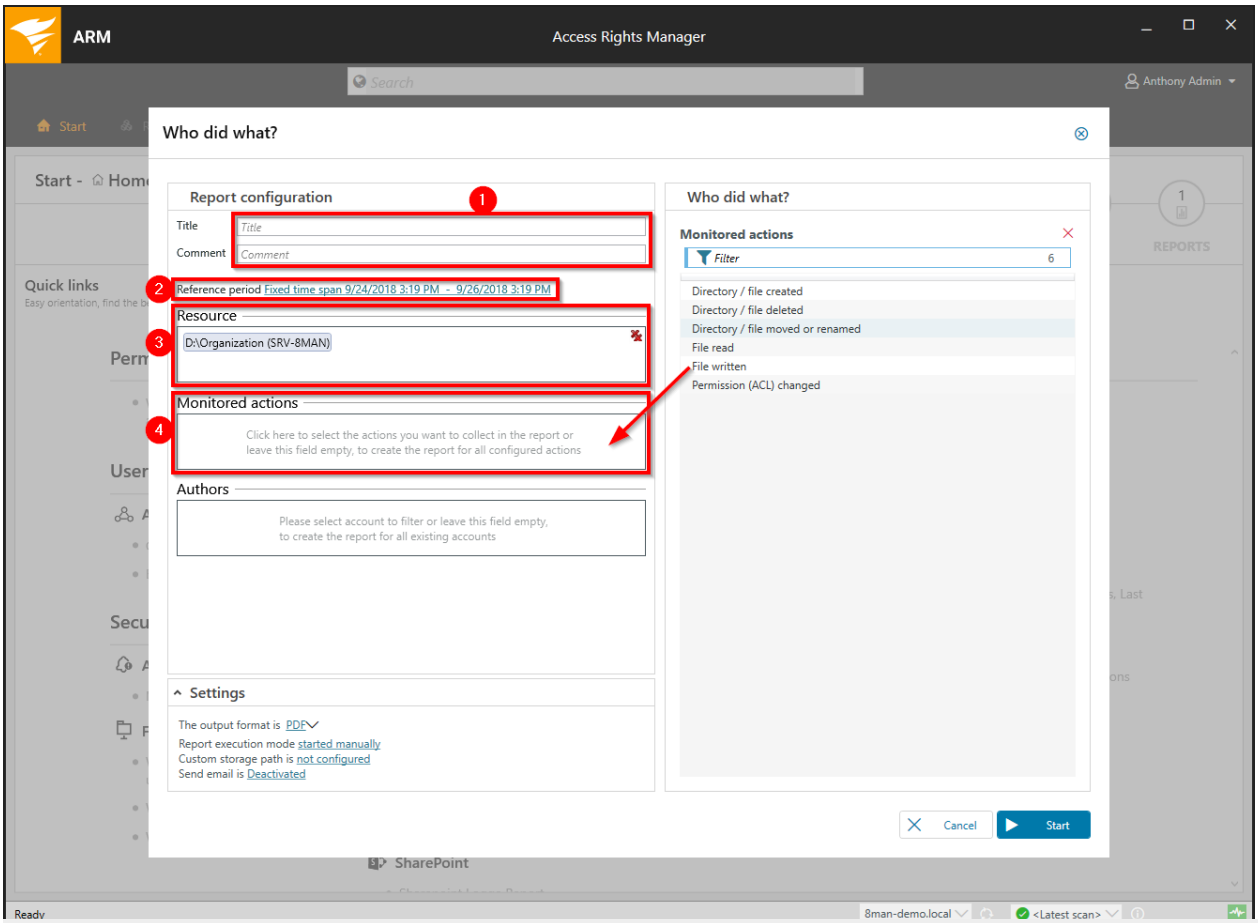
Related features

[Grant and remove file server access rights]

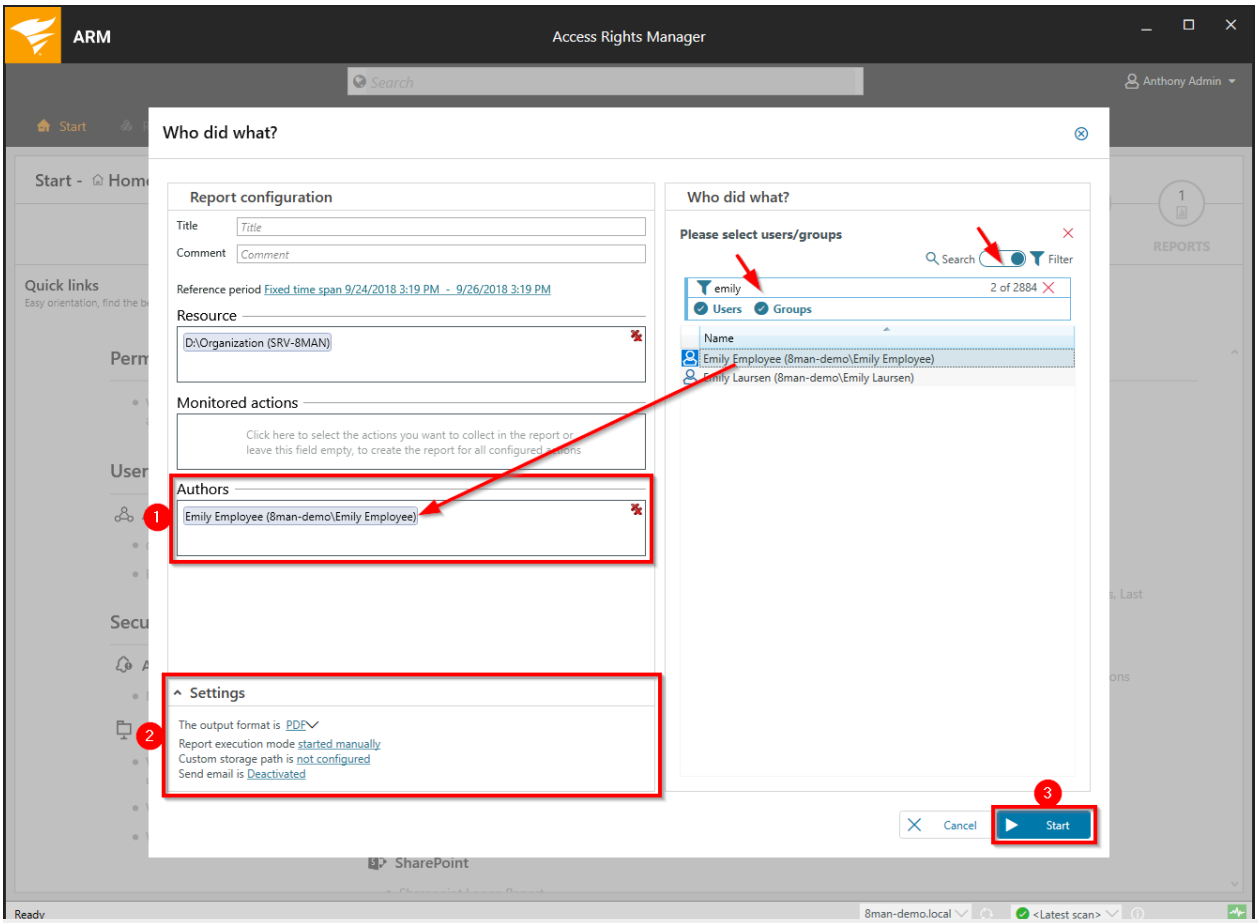
Step-by-step process



1. Select "Start".
2. Click on "Who did what?" in the "Security Monitoring" area.



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.



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

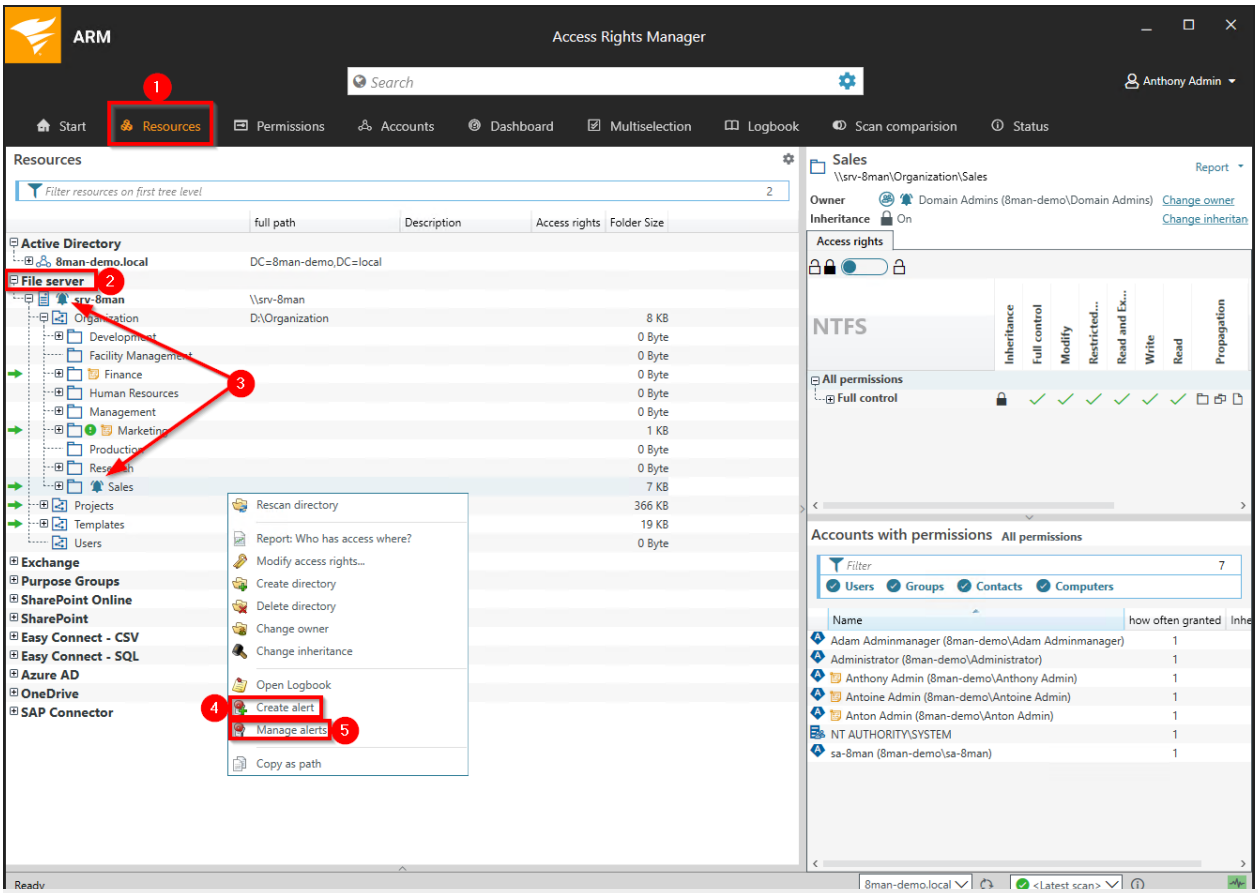
Enable alerts for suspected data theft (file server)

Enable alerts for data deletion (file server)

Enable alerts for suspected cases on ransomware (file server)

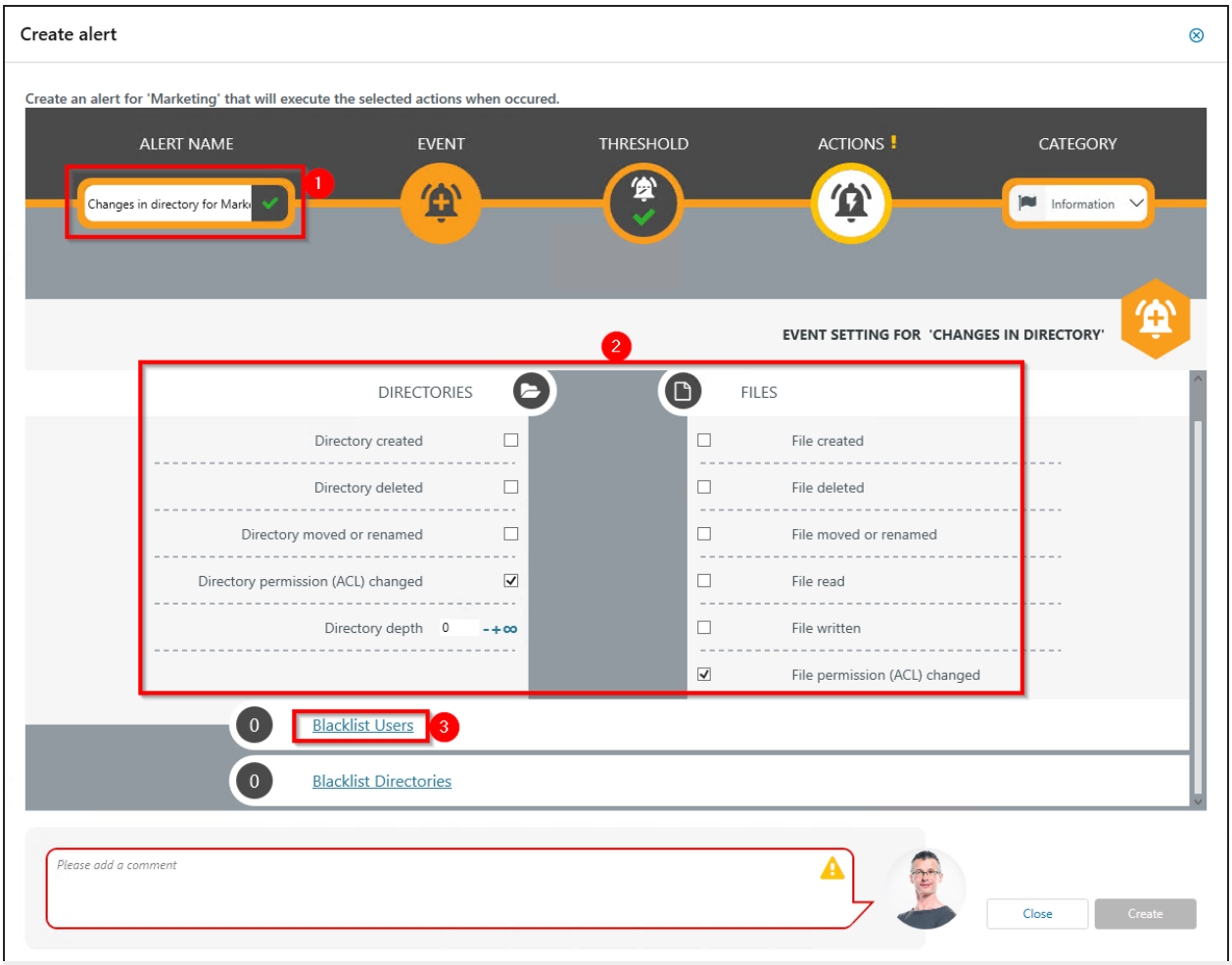
Manage alerts

Step-by-step process

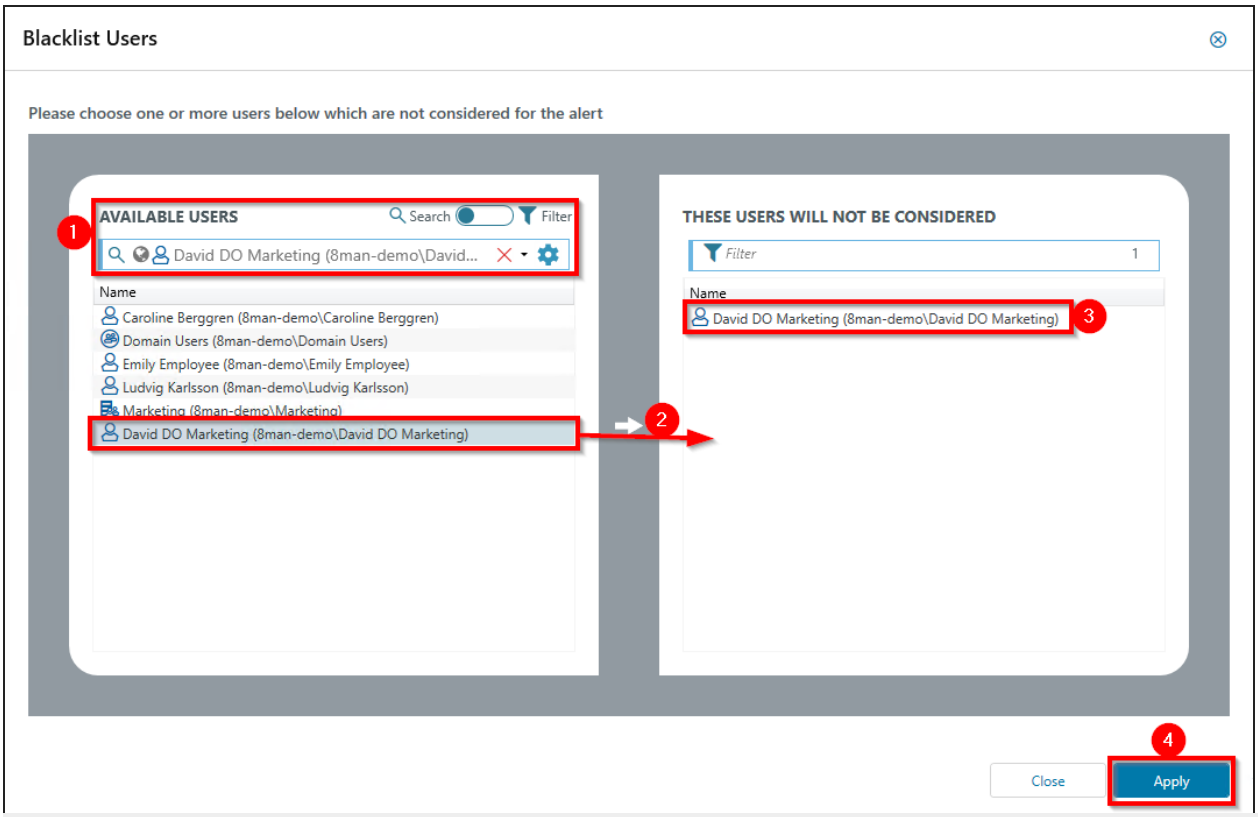


1. Choose Resources.
2. Expand the "file server".
3. Already configured alerts are displayed with a bell symbol.

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.



1. Give the alert configuration a name.
2. Define which events trigger an alert.
3. Optional: Click on "Blacklist user".



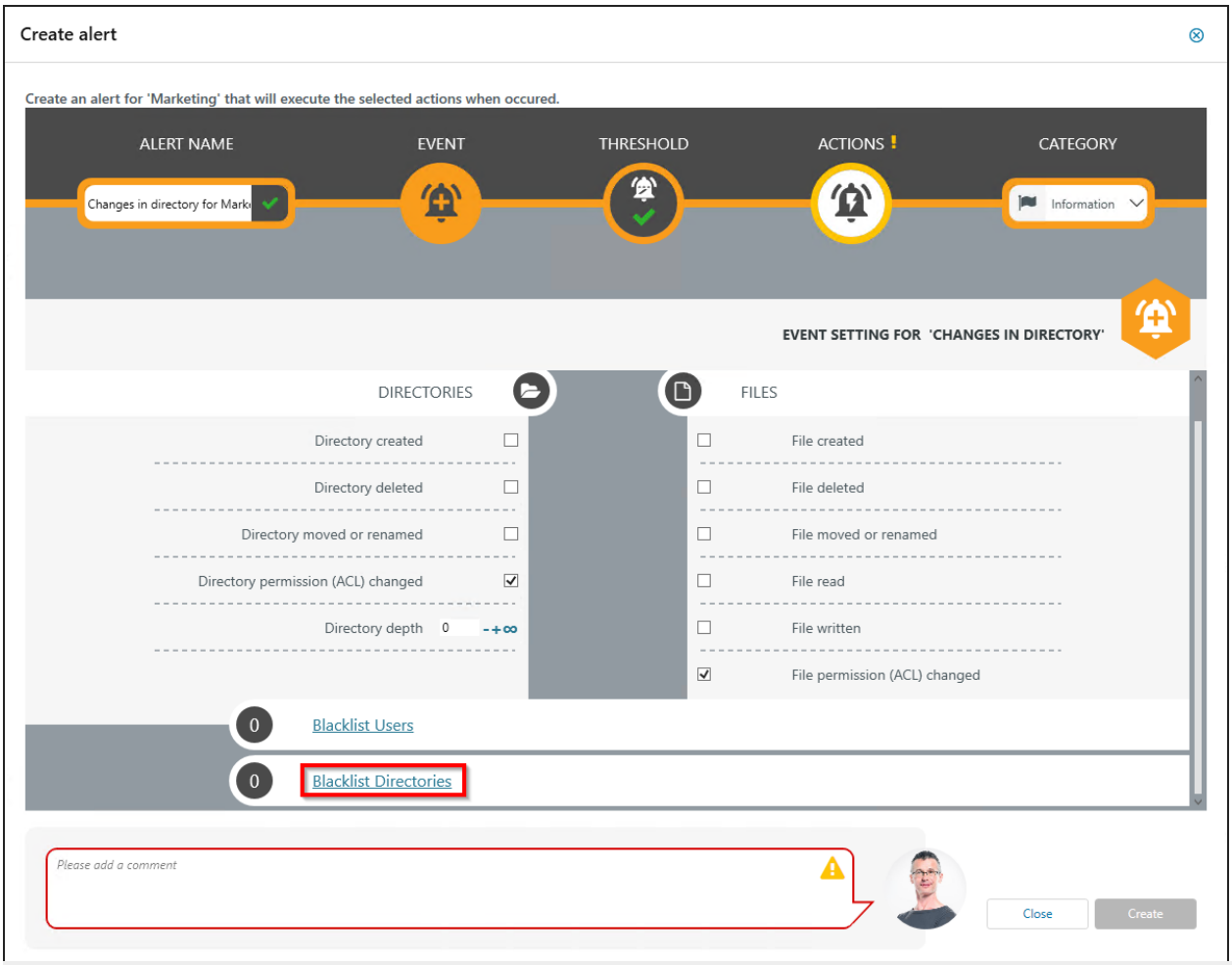
Optional:

Use the blacklist to define which users do not trigger an alert.

Each alert configuration has its own blacklist configuration.

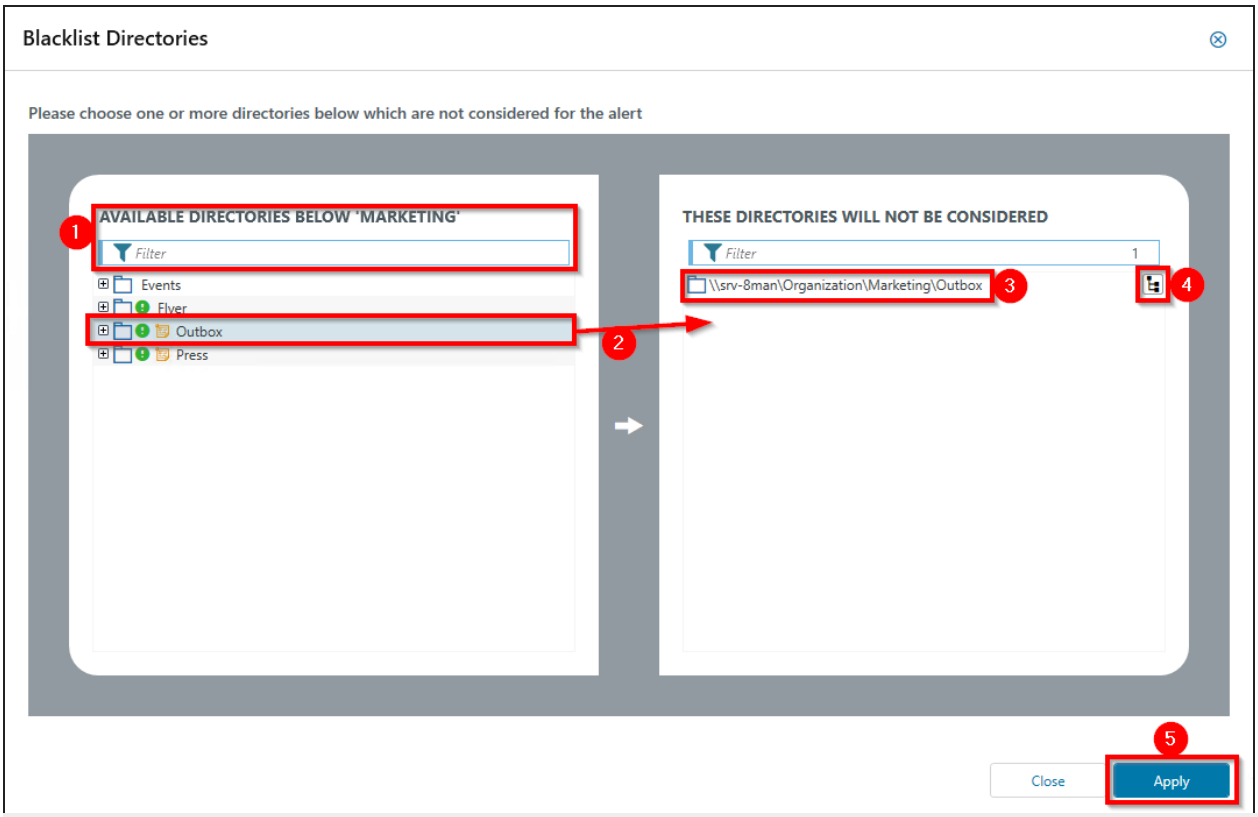
You can only add users, not groups.

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.



Optional:

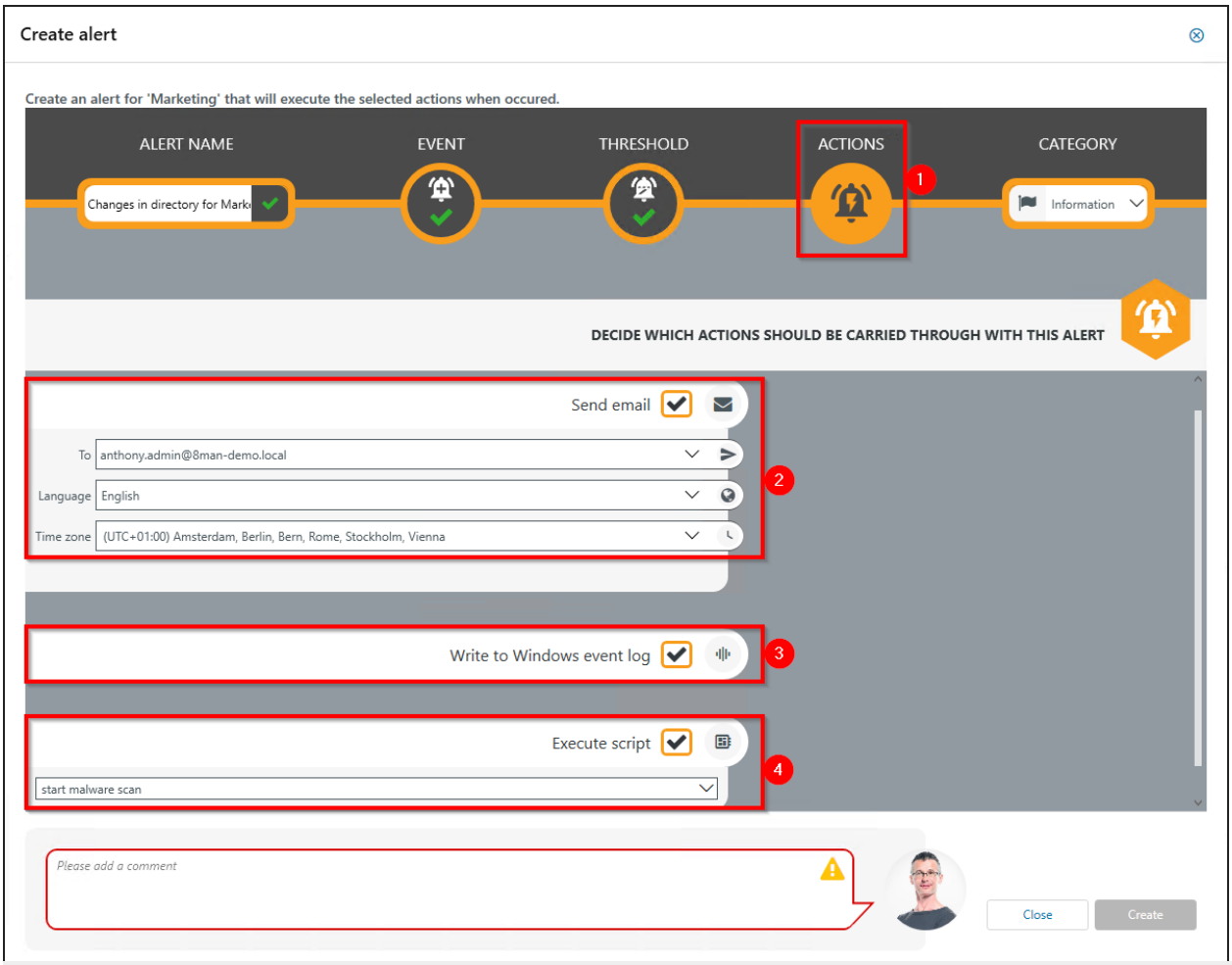
Select "Blacklist Directories".



Optional:

Use the blacklist to define which directories are not monitored.

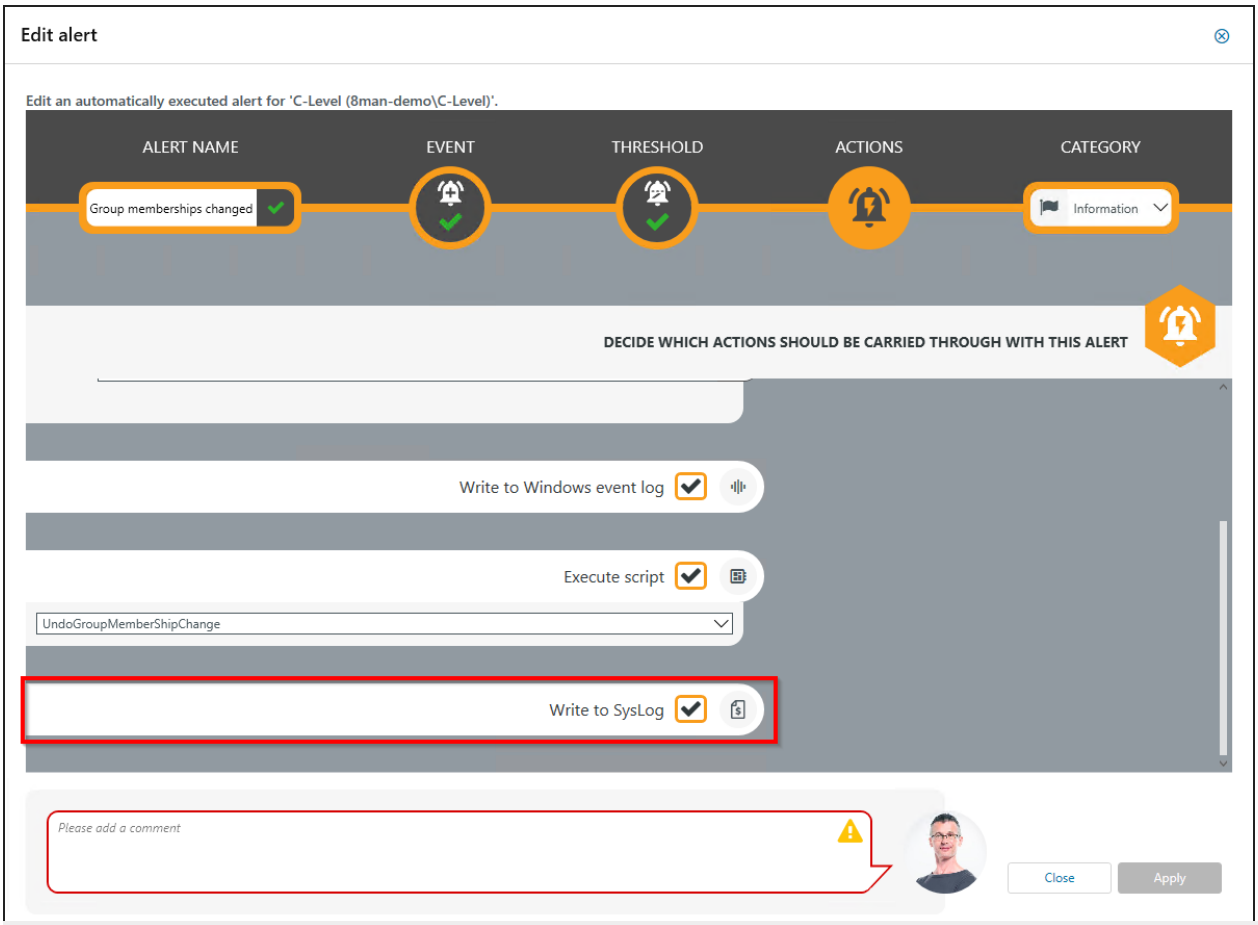
1. Use the filter function to find the desired directories. When you filter, the tree view changes to a result list of the directory paths.
2. Use double-click or drag-and-drop to add directories to the blacklist.
3. Use the "Delete" key to remove directories from the blacklist.
4. Enable or disable monitoring of subdirectories.
5. Click "Apply" to save the changes.



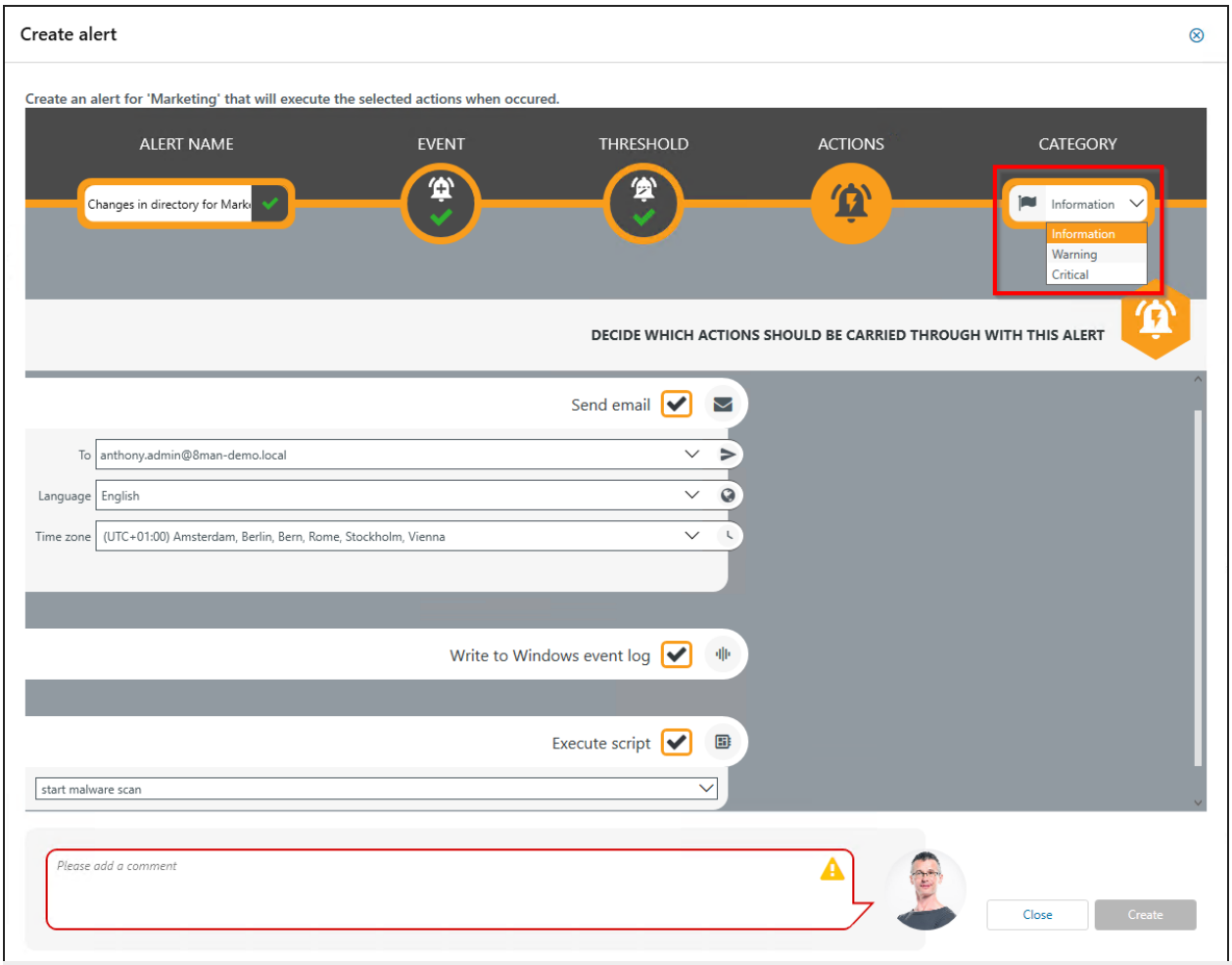
1. Choose Actions. Here you specify which actions are executed when an alert is triggered. You must activate at least one action.
2. Activate the option if an email should be sent in case of an alert.

The content of the emails can be customized. This is analogous to the recertification emails.

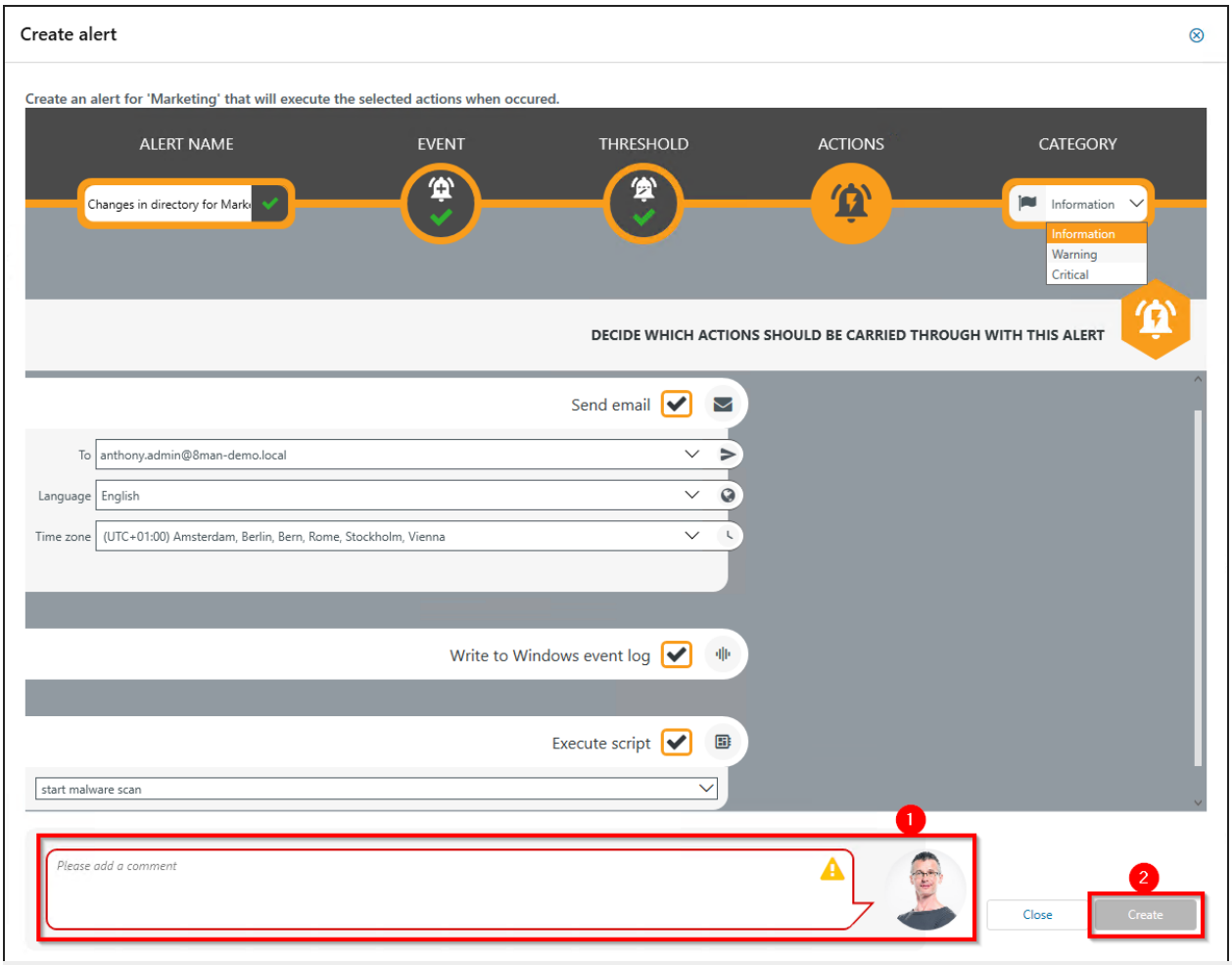
3. The alert is written to the Windows Event Log. The categorization is used.
4. Enable the execution of a script. To activate this option, a script configuration for alerts must be stored.



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.



Choose a category. This is used when writing to the Windows Event Log and for the email subject.



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

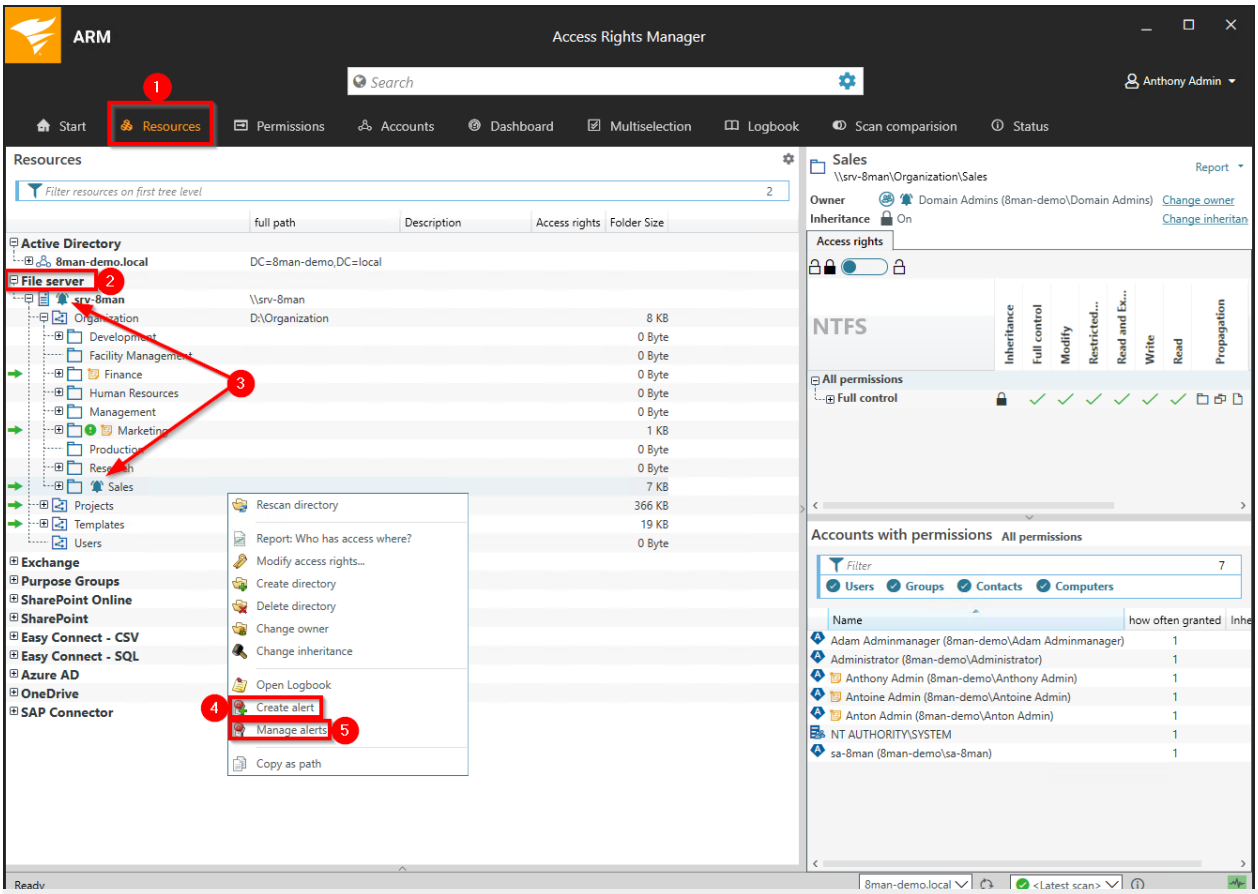
Enable alerts for file server directories

Enable alerts for data deletion (file server)

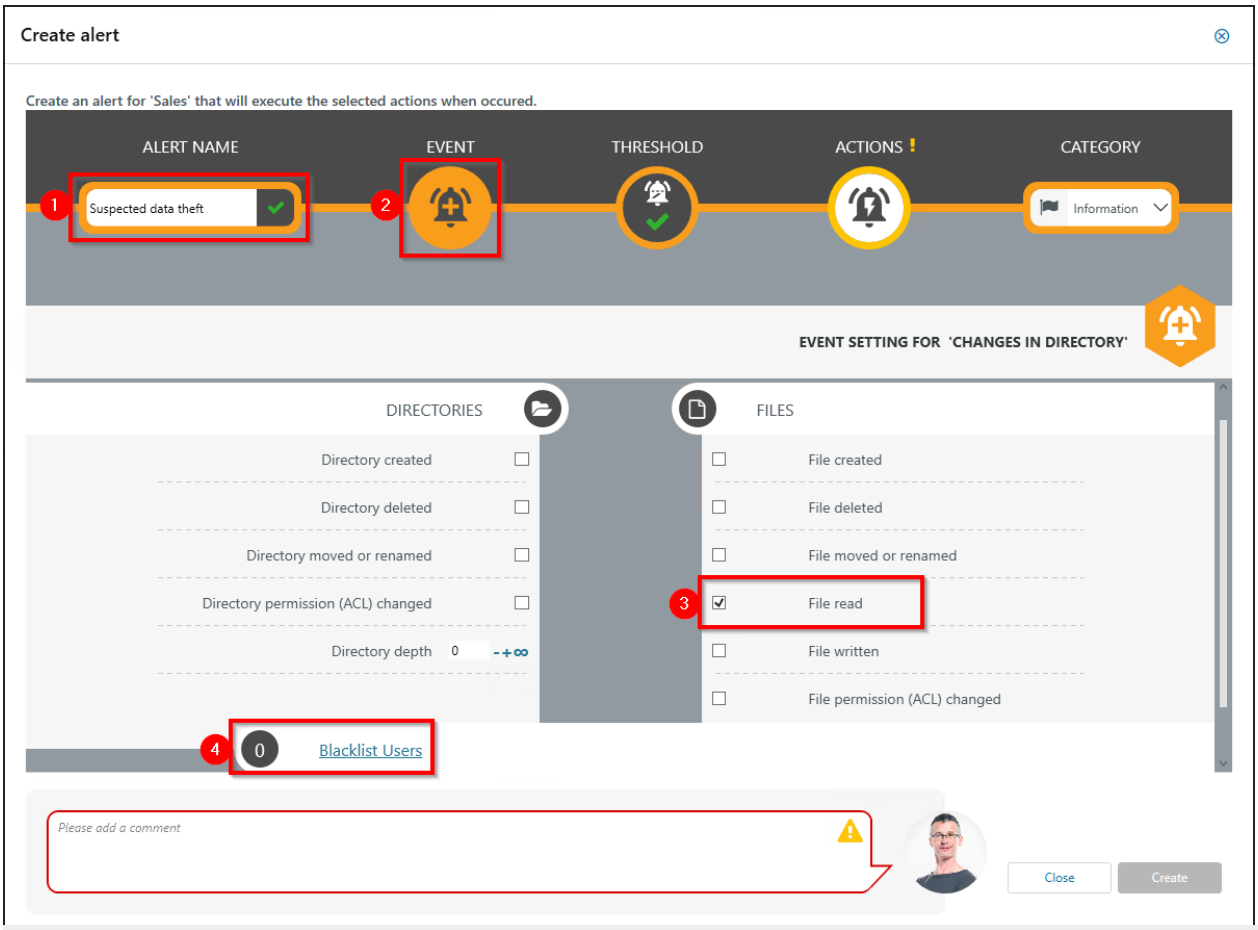
Enable alerts for suspected cases on ransomware (file server)

Manage alerts

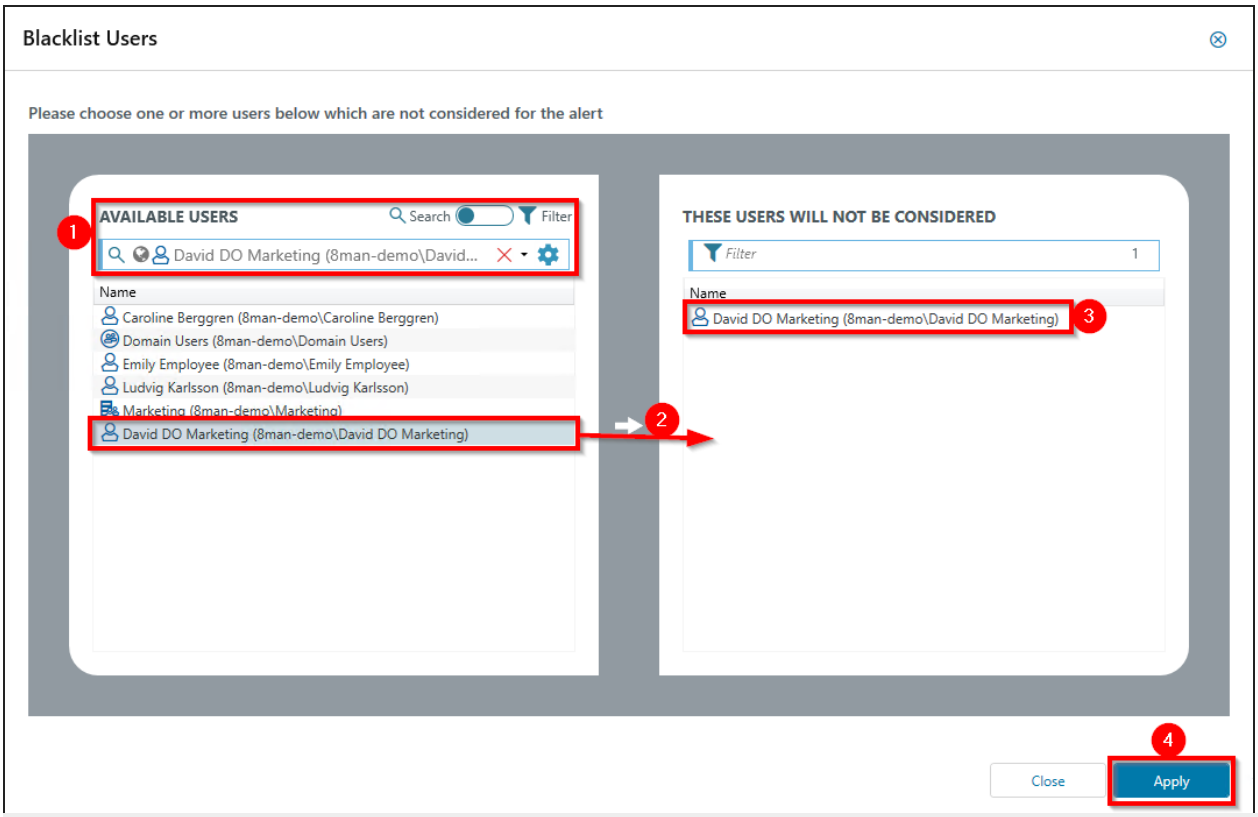
Step-by-step process



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.



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".

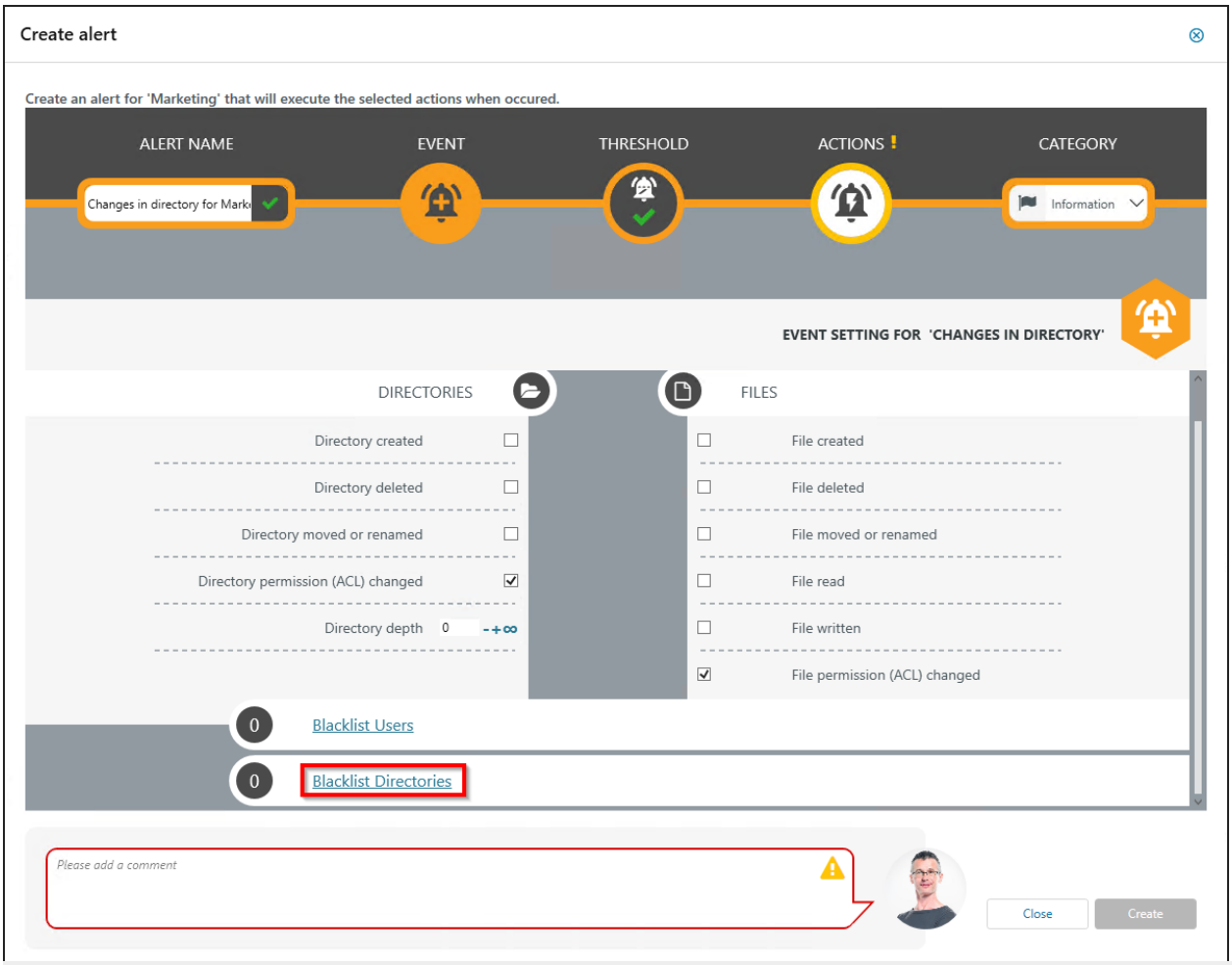


Optional: Use the blacklist to define which users do not trigger an alert.

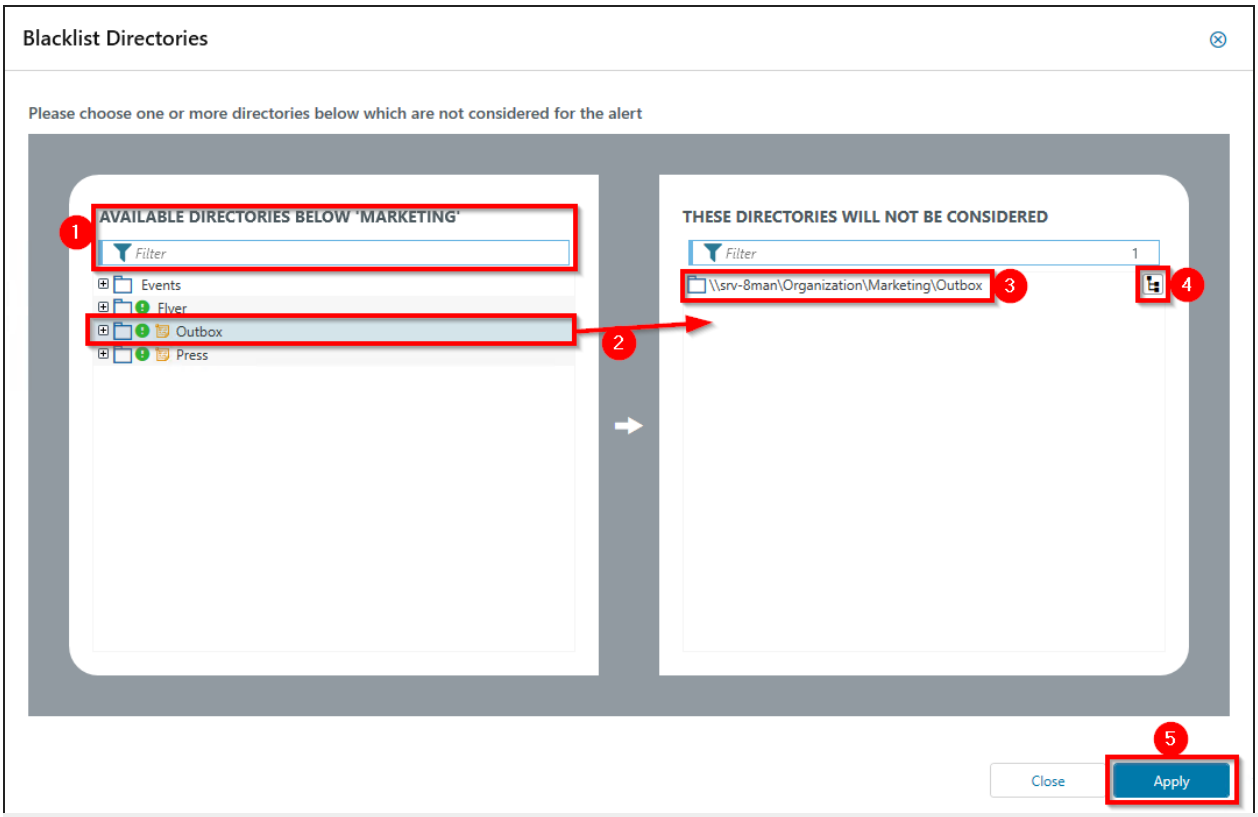
Each alert configuration has its own blacklist configuration.

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.

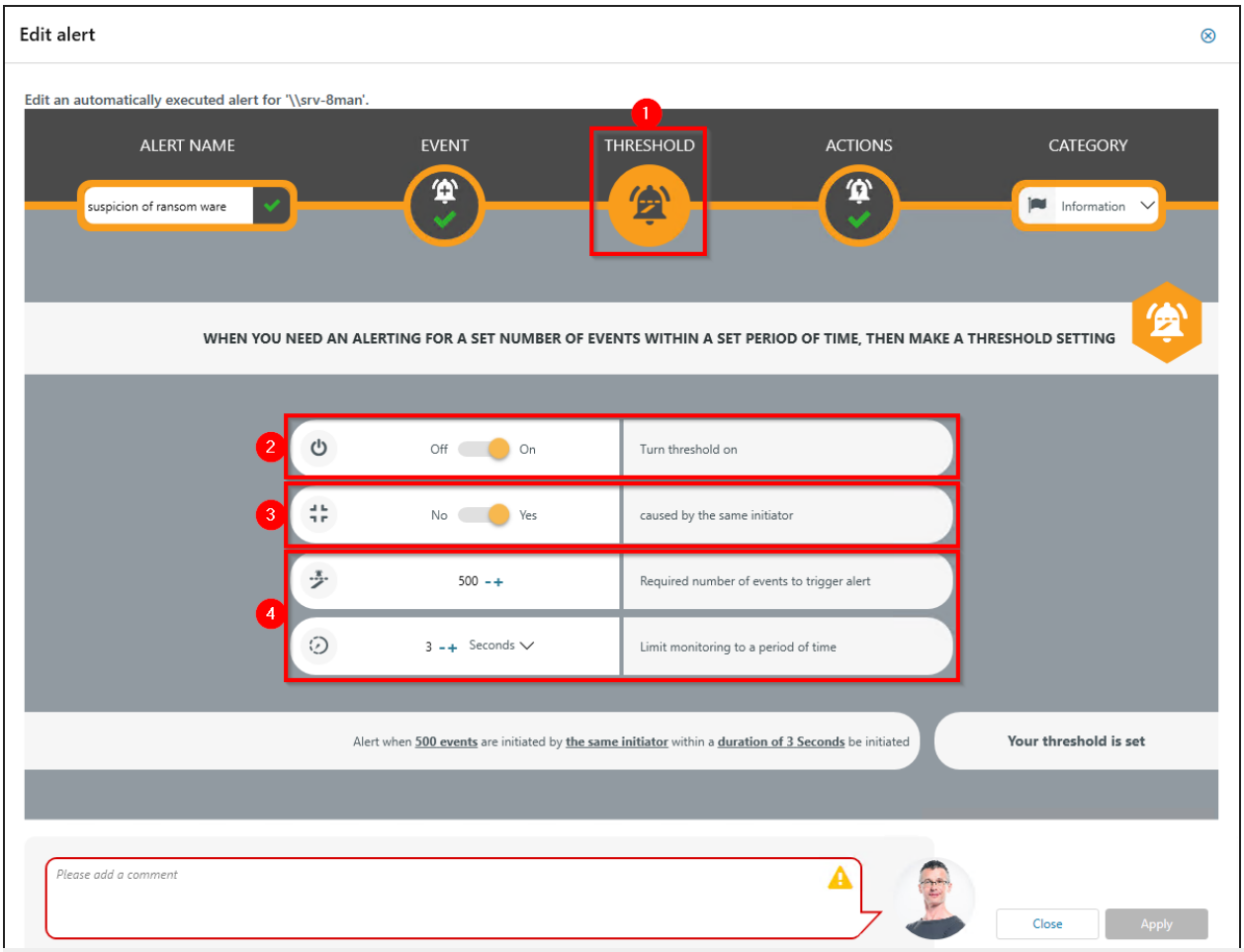


Optional: Select "Blacklist directories".

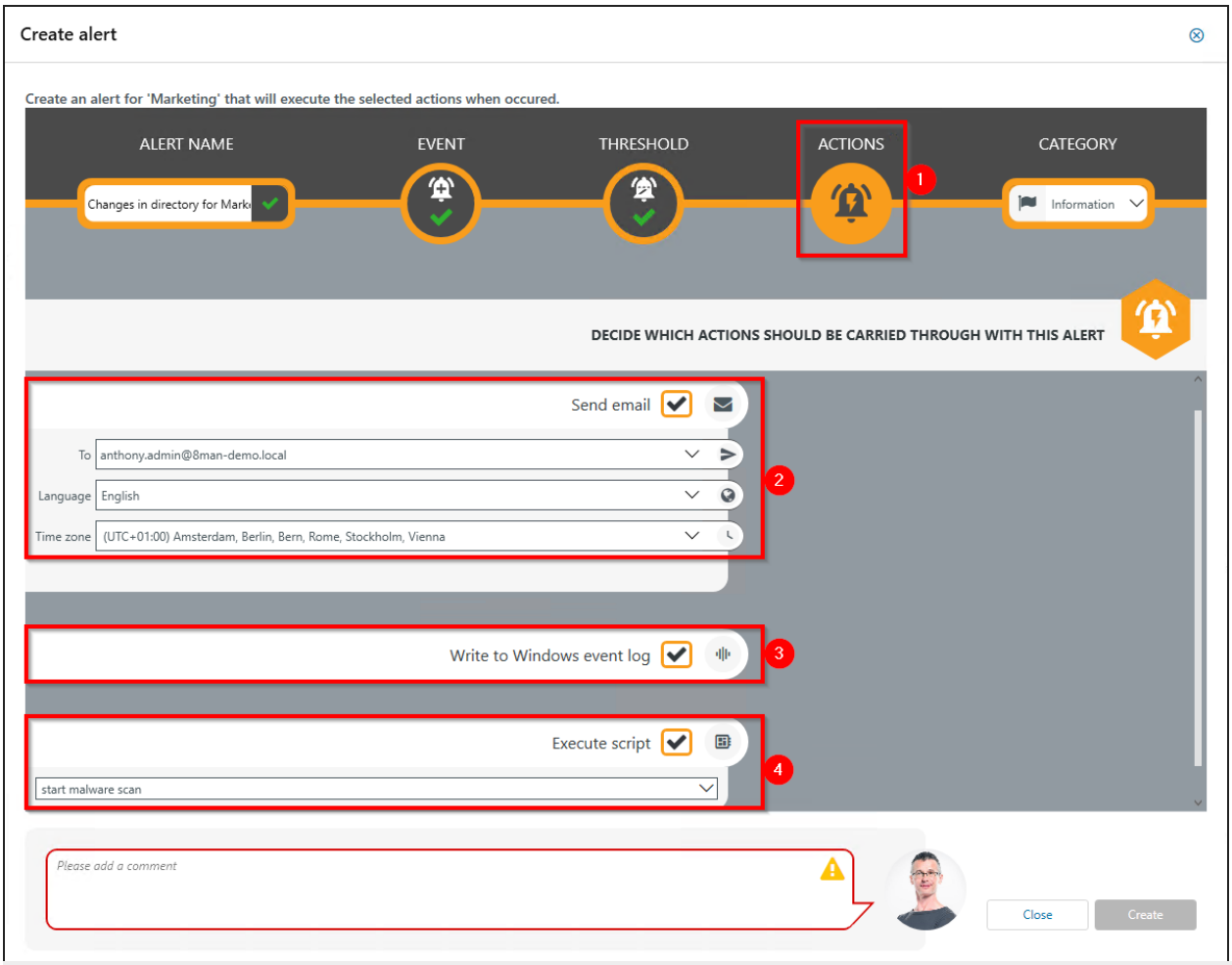


Optional: Use the blacklist to define which directories are not monitored.

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.



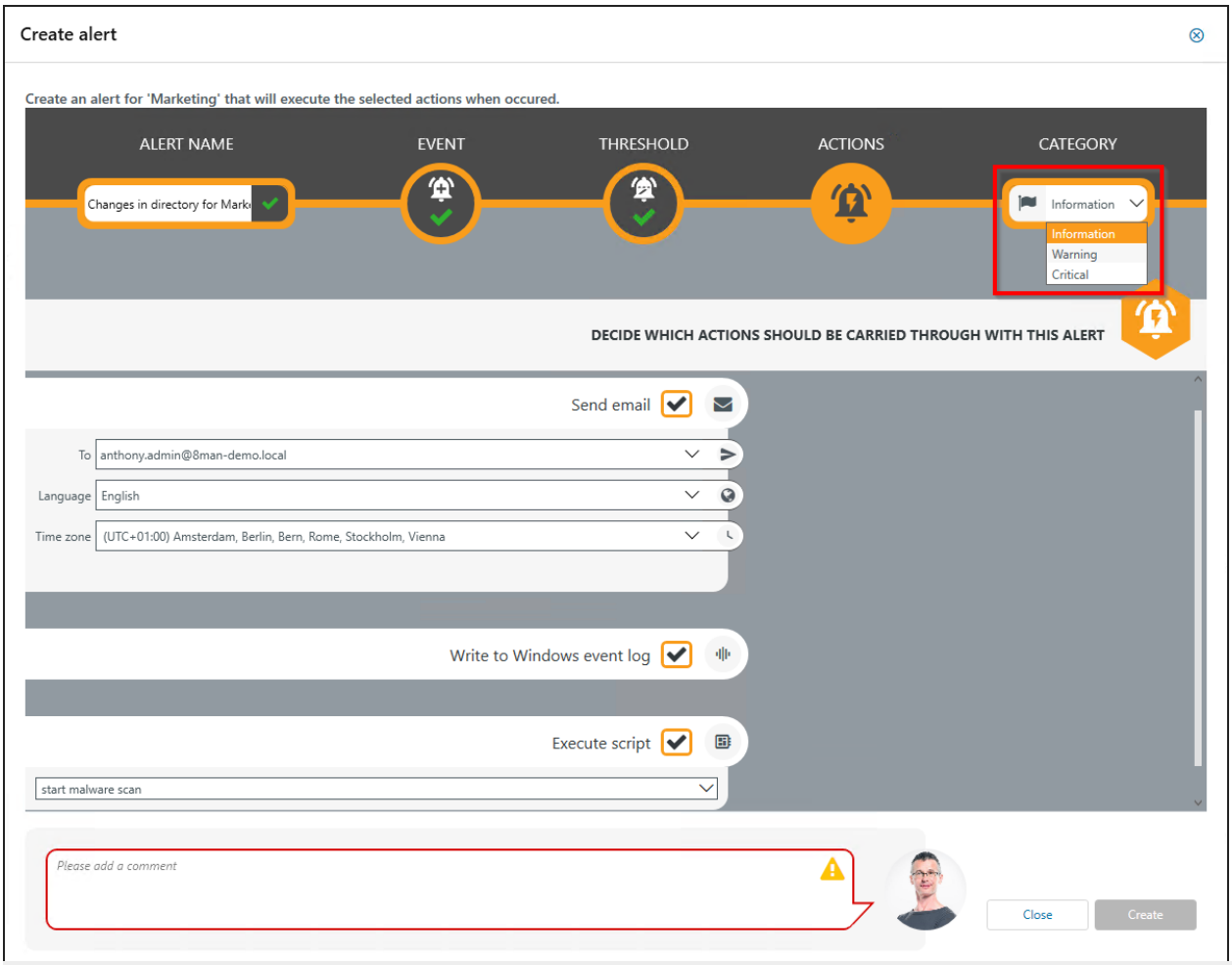
1. Select "Threshold".
2. Enable threshold.
3. Activate the option. If data theft is suspected, typically all events are triggered by a single user.
4. Define how many events within a period trigger the alert.



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.

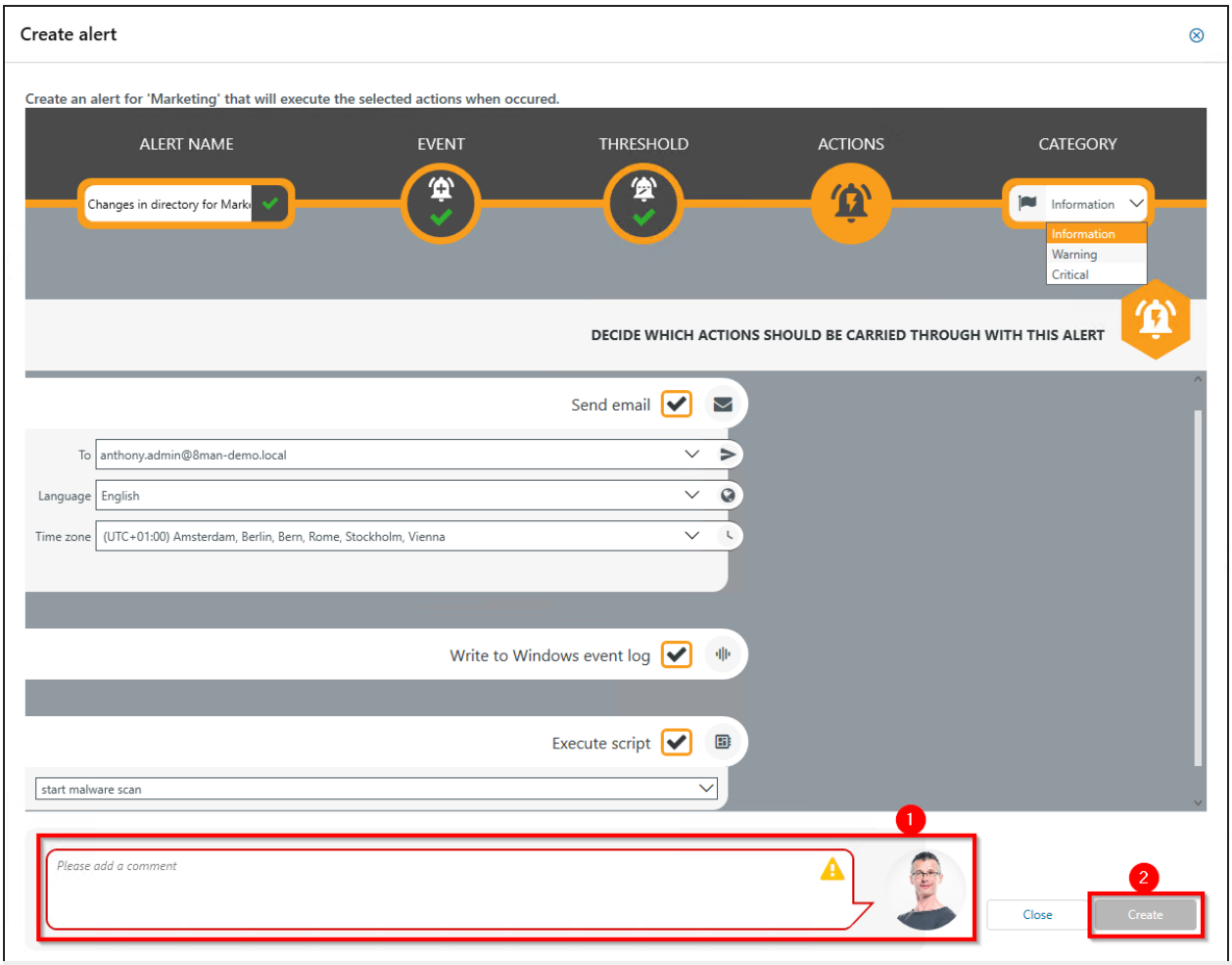
The content of the emails can be customized. This is analogous to the recertification emails.

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.



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.



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

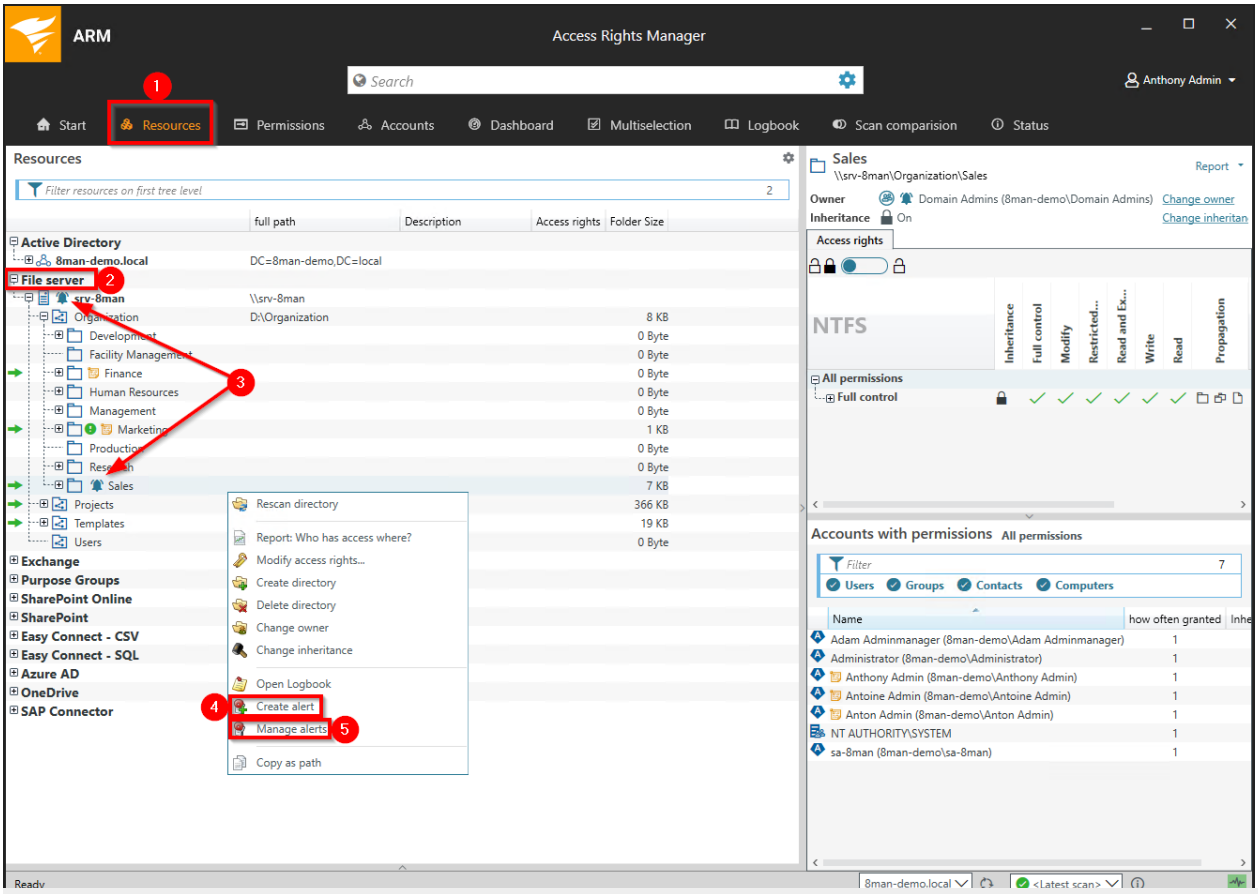
Enable alerts for file server directories

Enable alerts for suspected data theft (file server)

Enable alerts for suspected cases on ransomware (file server)

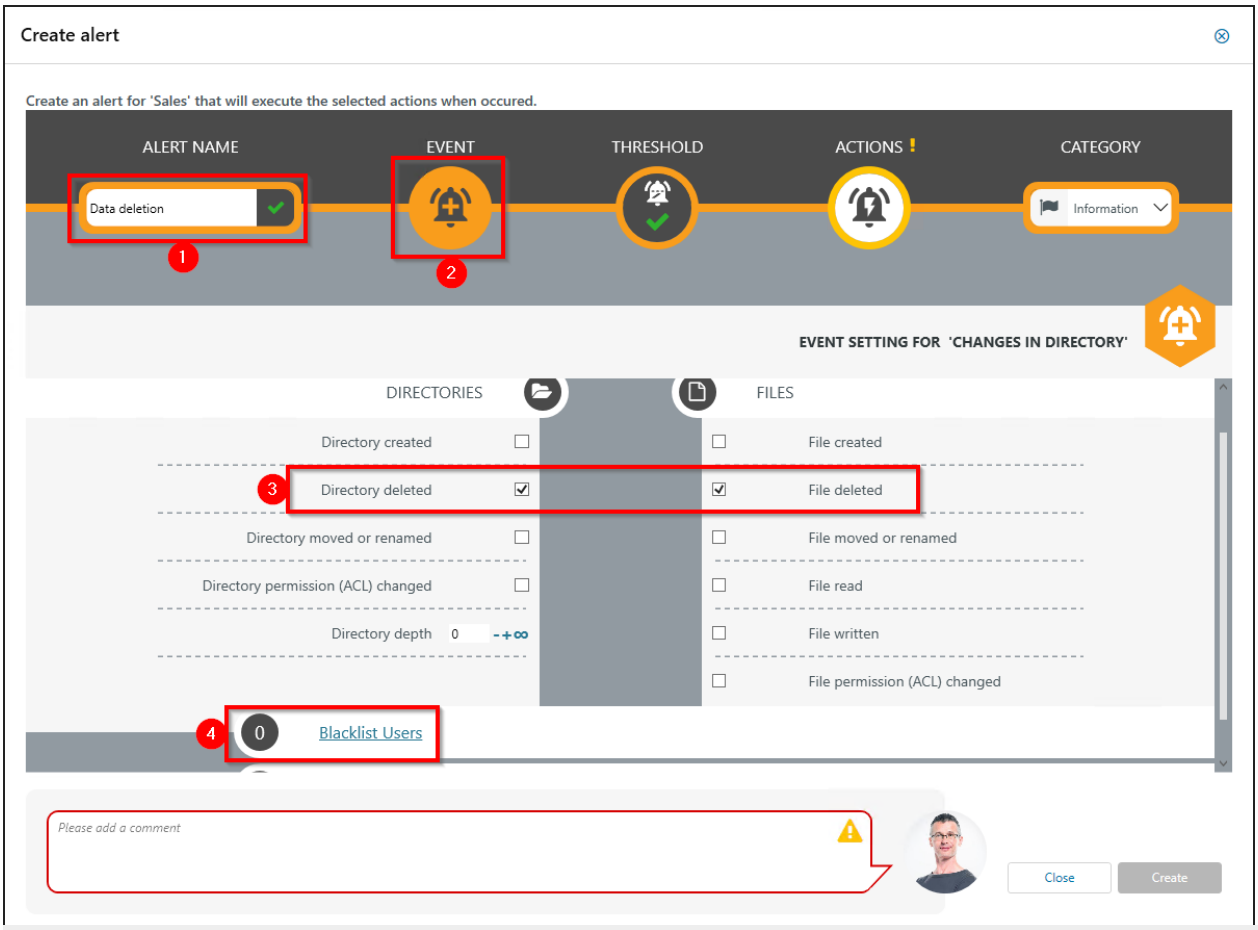
Manage alerts

Step-by-step process

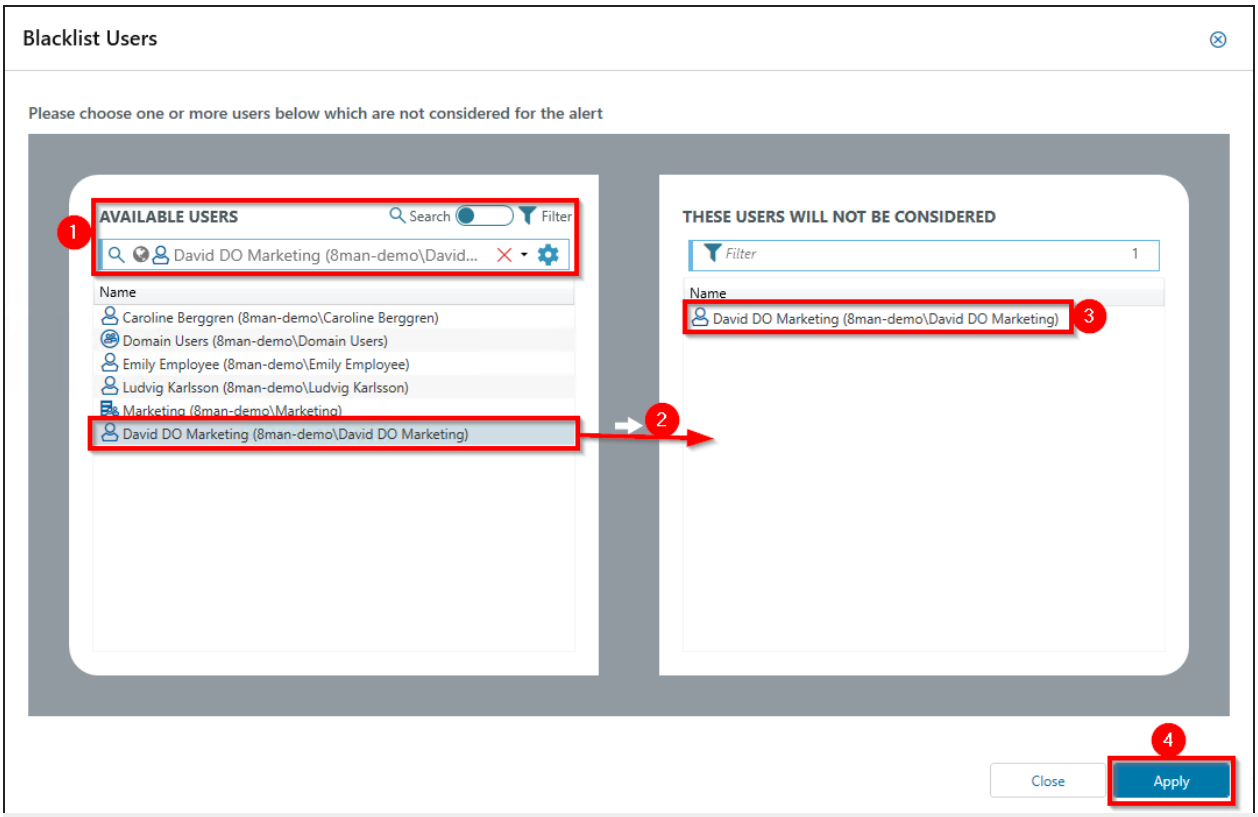


1. Choose Resources.

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.



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".

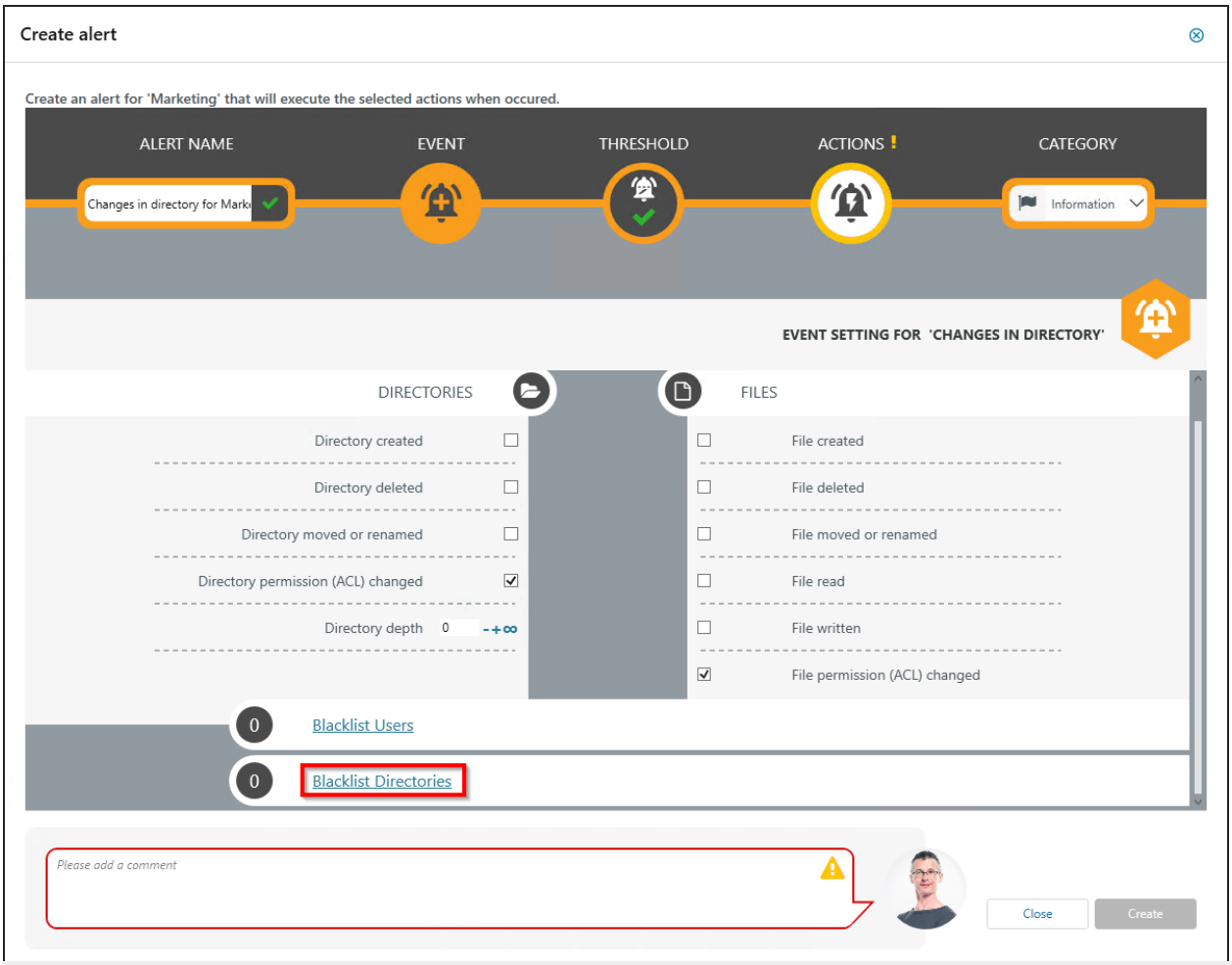


Optional: Use the blacklist to define which users do not trigger an alert.

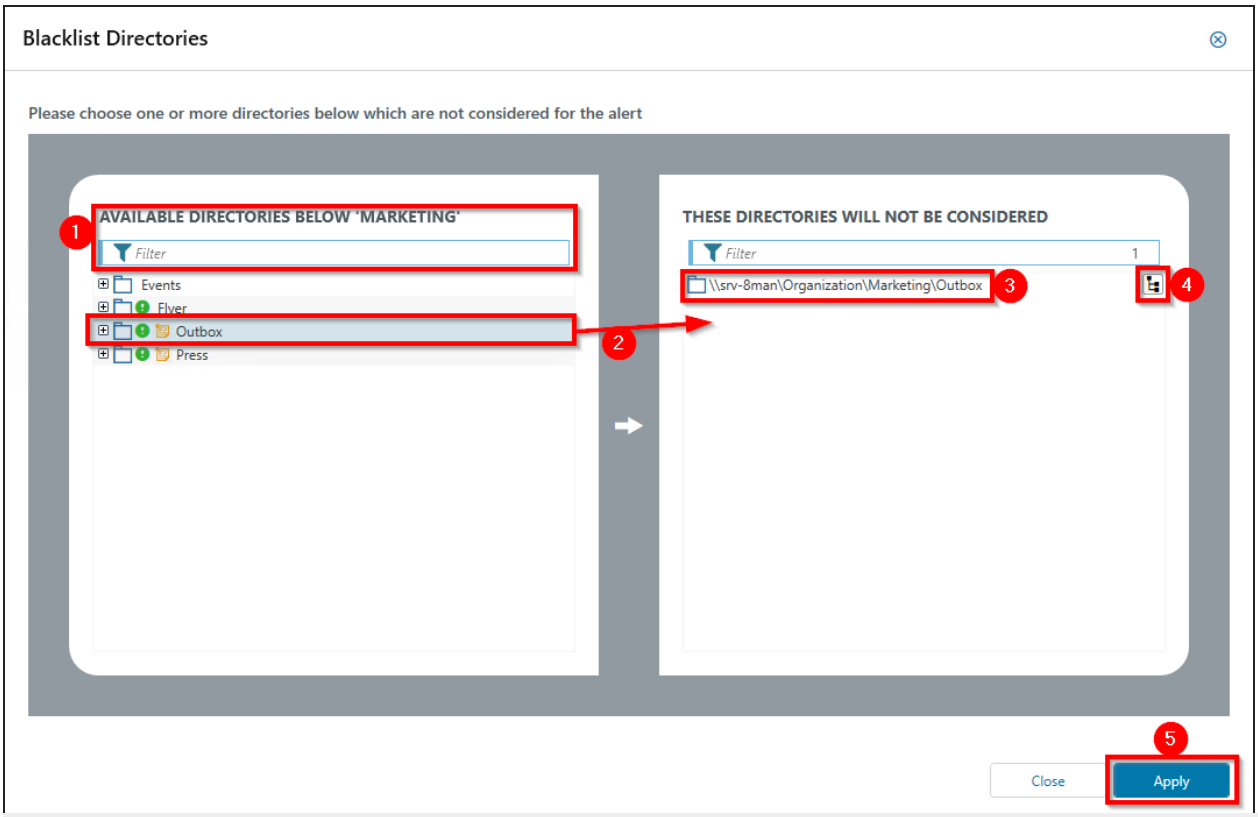
ⓘ Each alert configuration has its own blacklist configuration.

ⓘ 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.

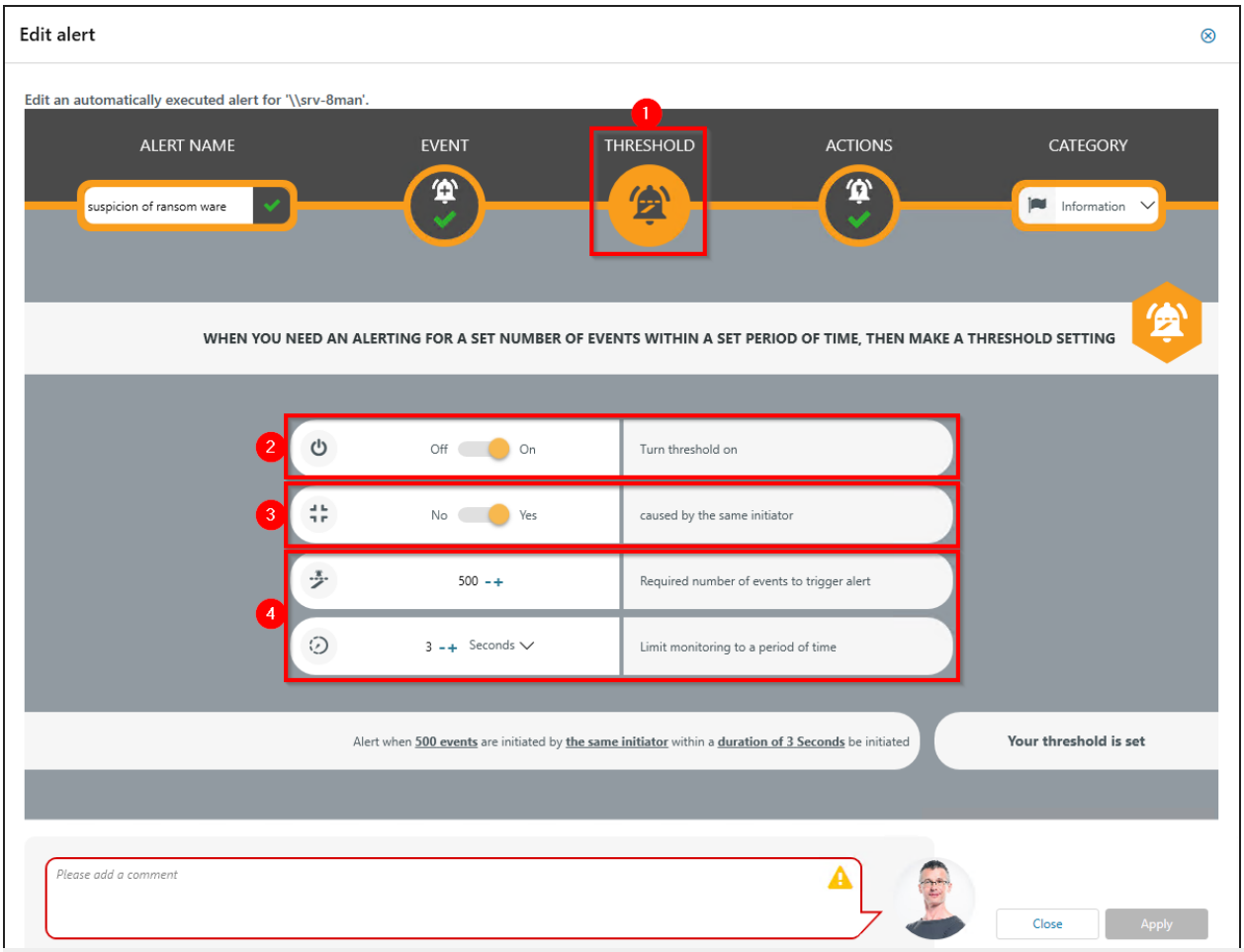


Optional: Select "Blacklist directories".

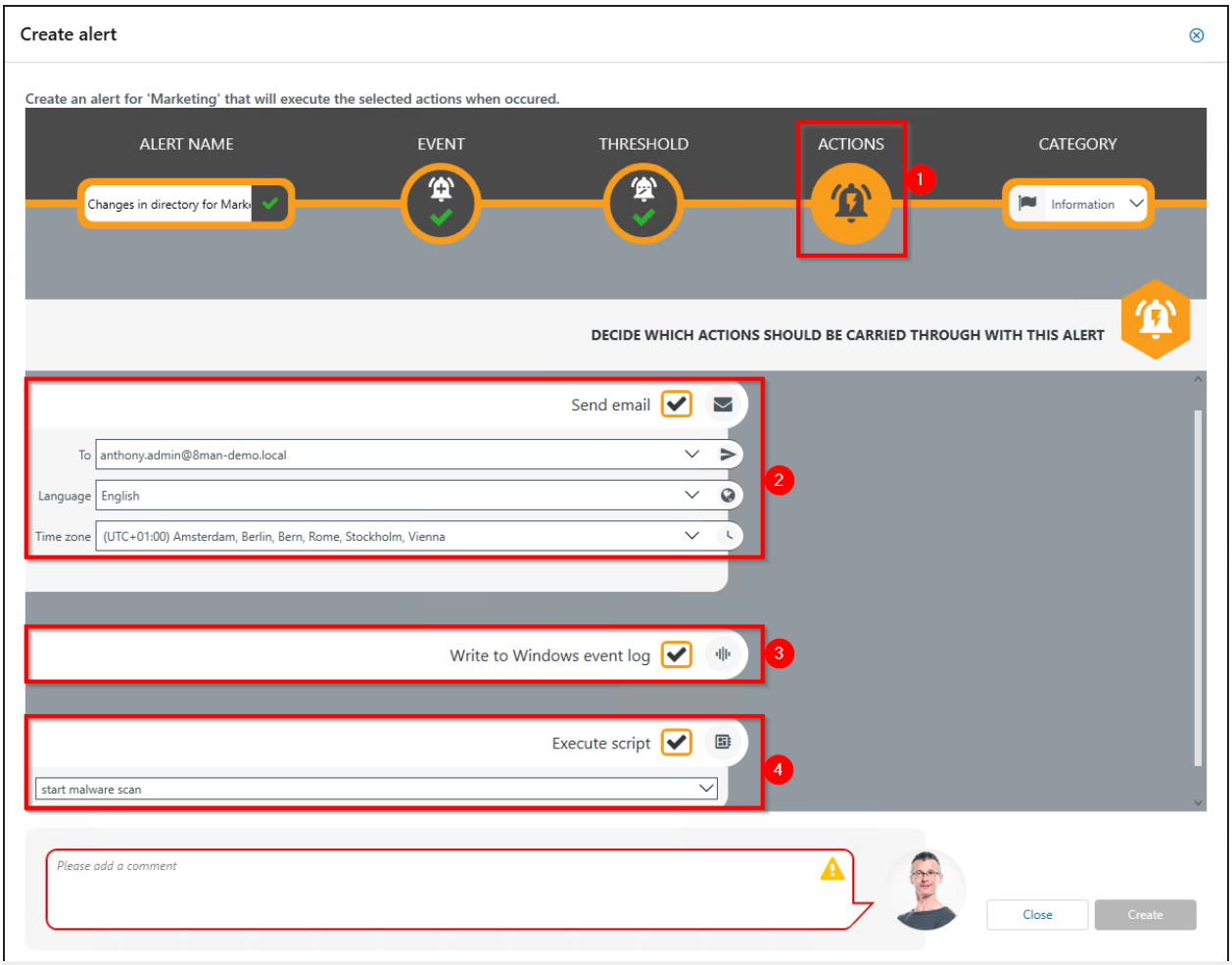


Optional: Use the blacklist to define which directories are not monitored.

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.



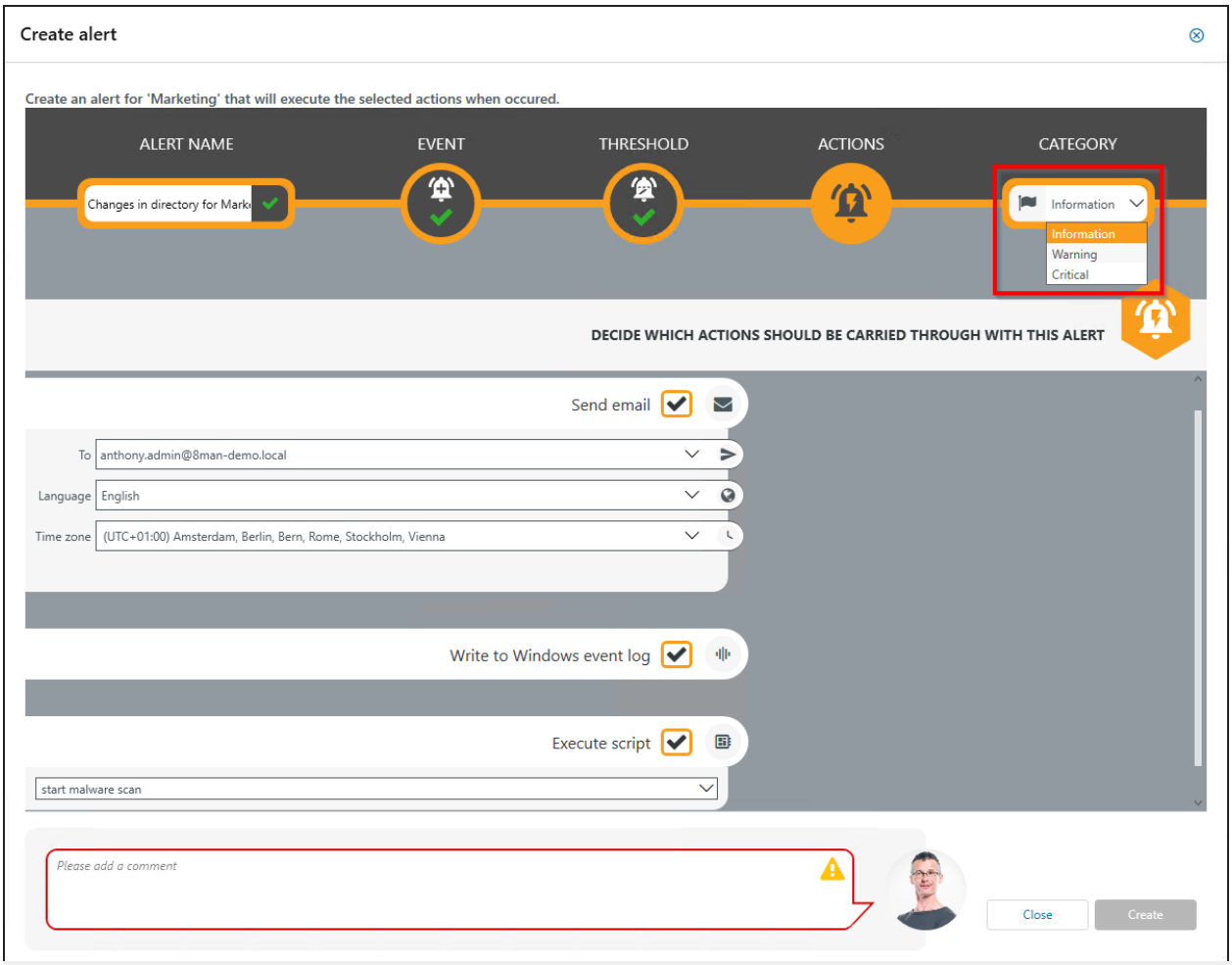
1. Select "Threshold".
2. Enable threshold.
3. Activate the option.
4. Define how many events within a period trigger the alert.



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.

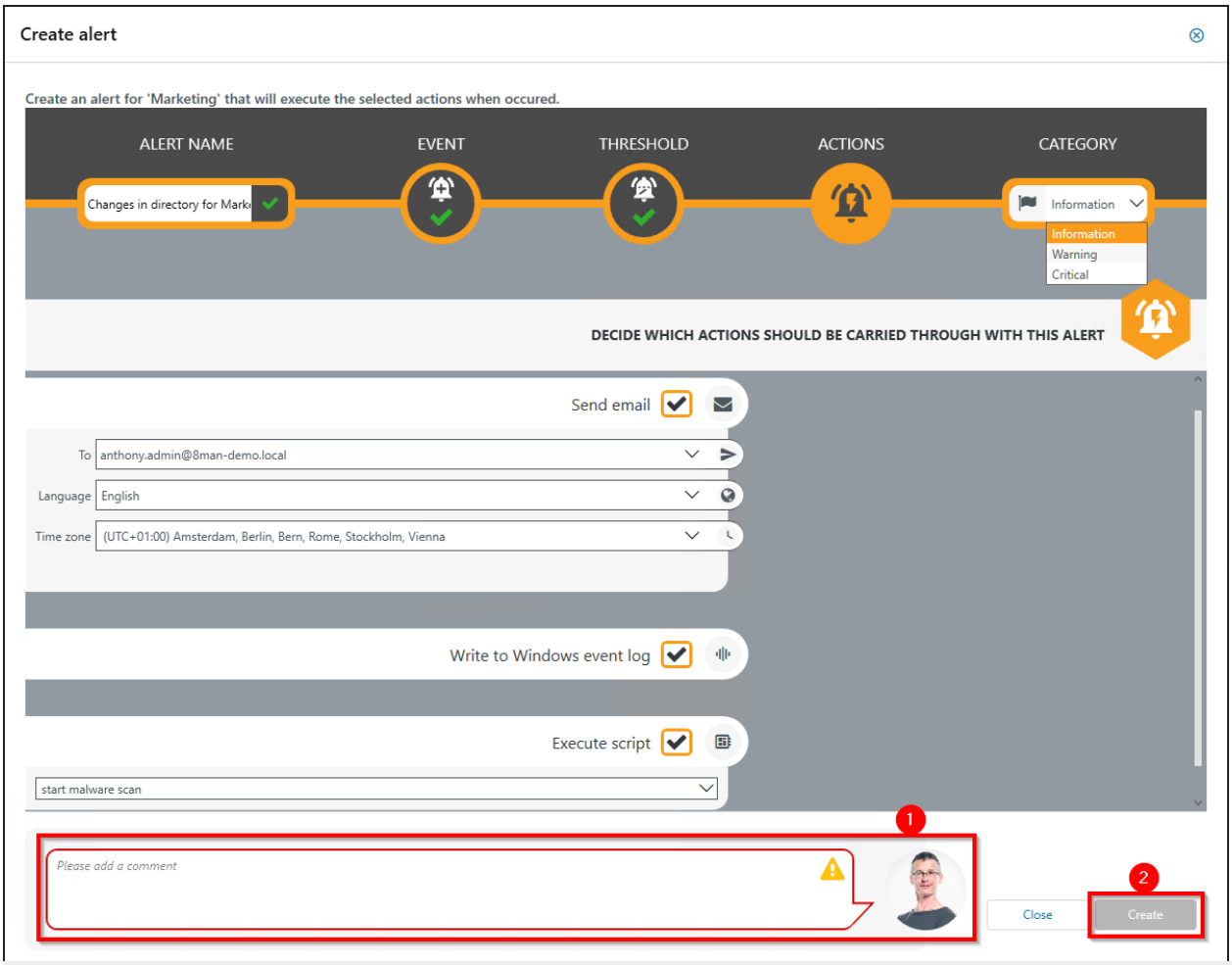
The content of the emails can be customized. This is analogous to the recertification emails.

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.



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.



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

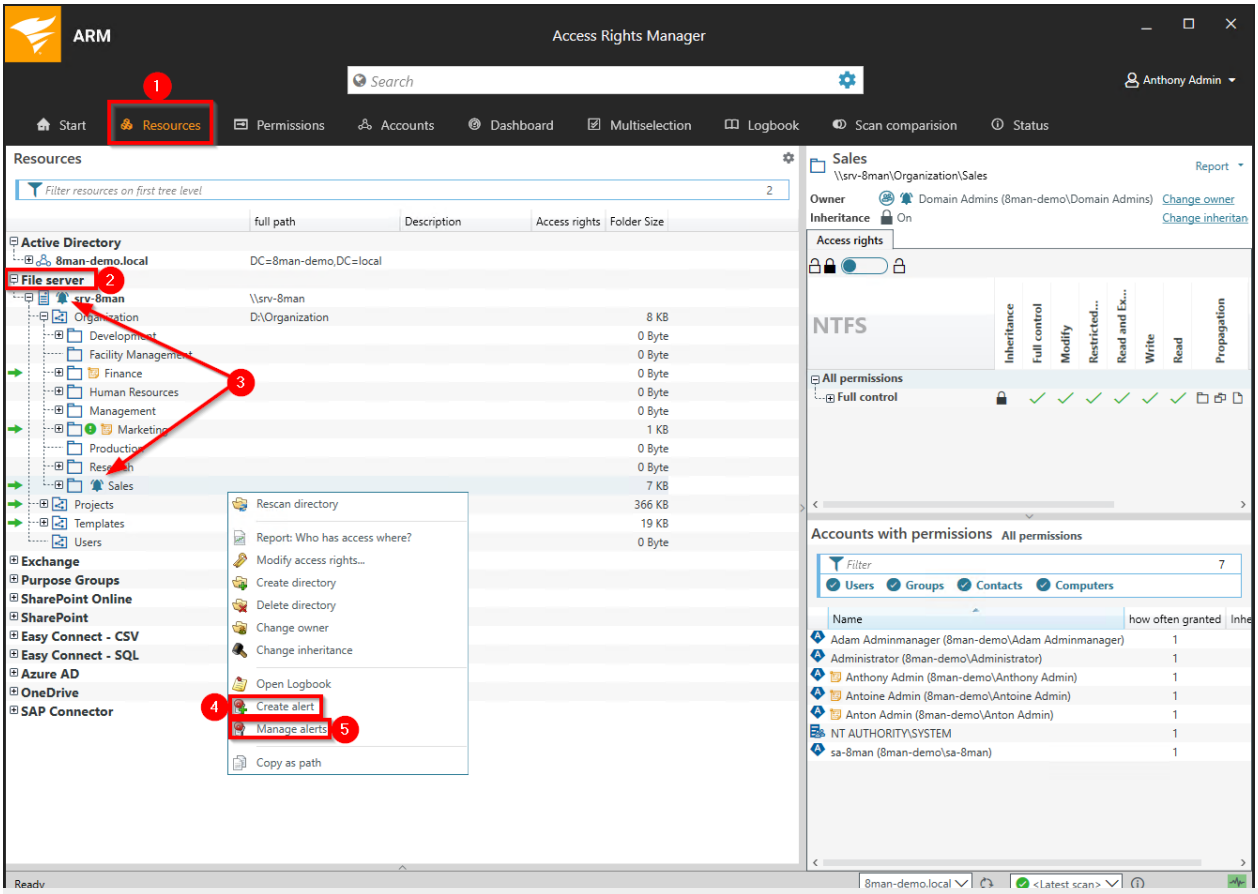
Enable alerts for file server directories

Enable alerts for suspected data theft (file server)

Enable alerts for data deletion (file server)

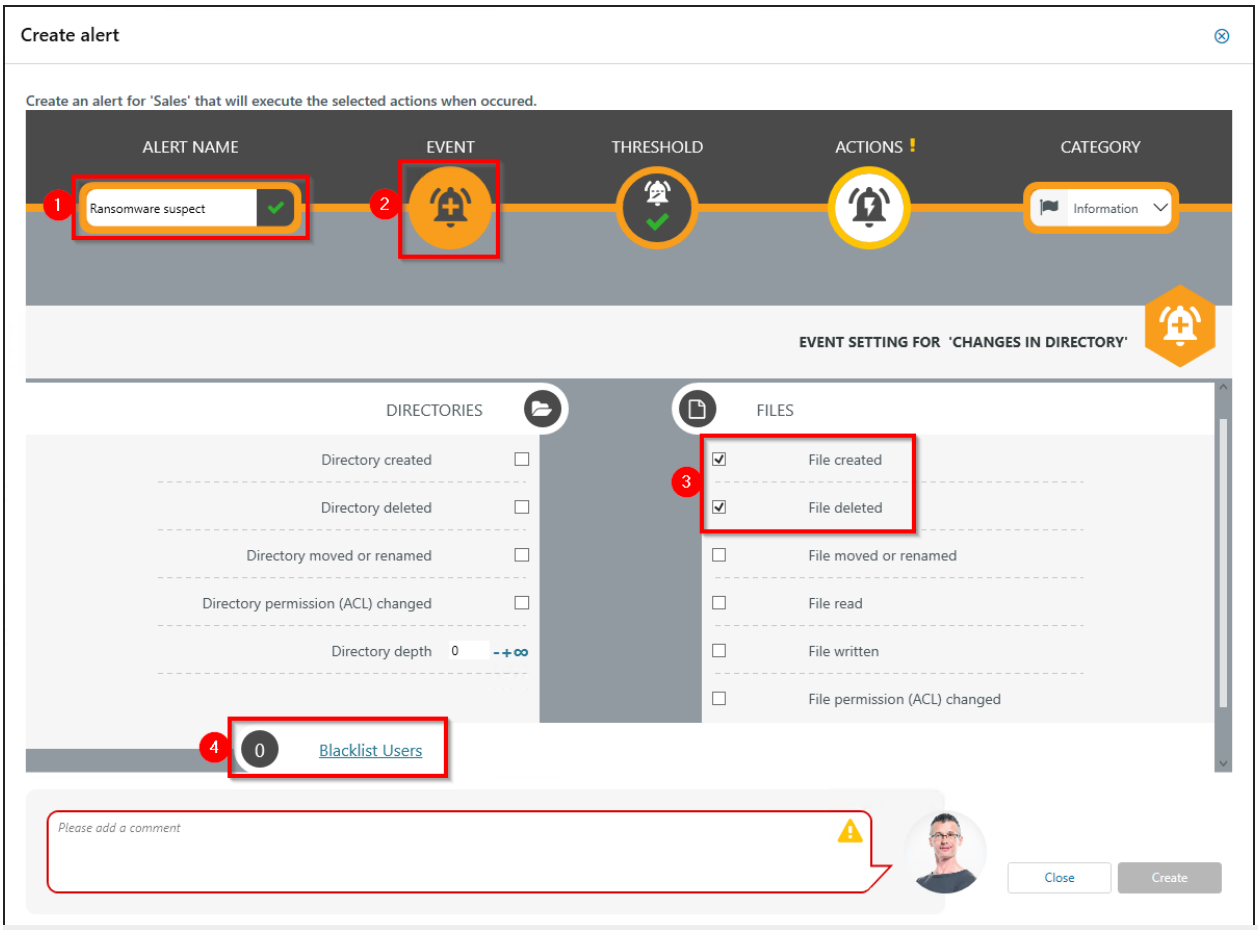
Manage alerts

Step-by-step process

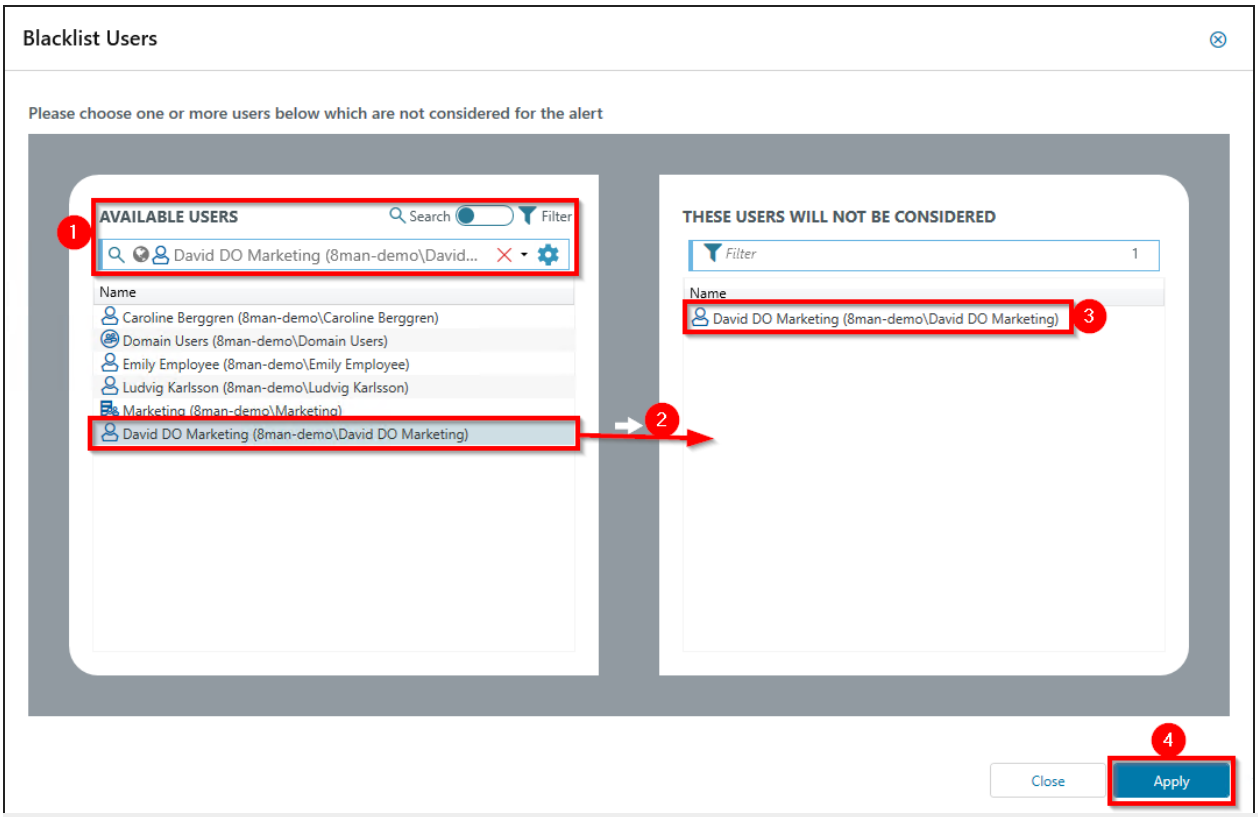


1. Choose Resources.

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.



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".

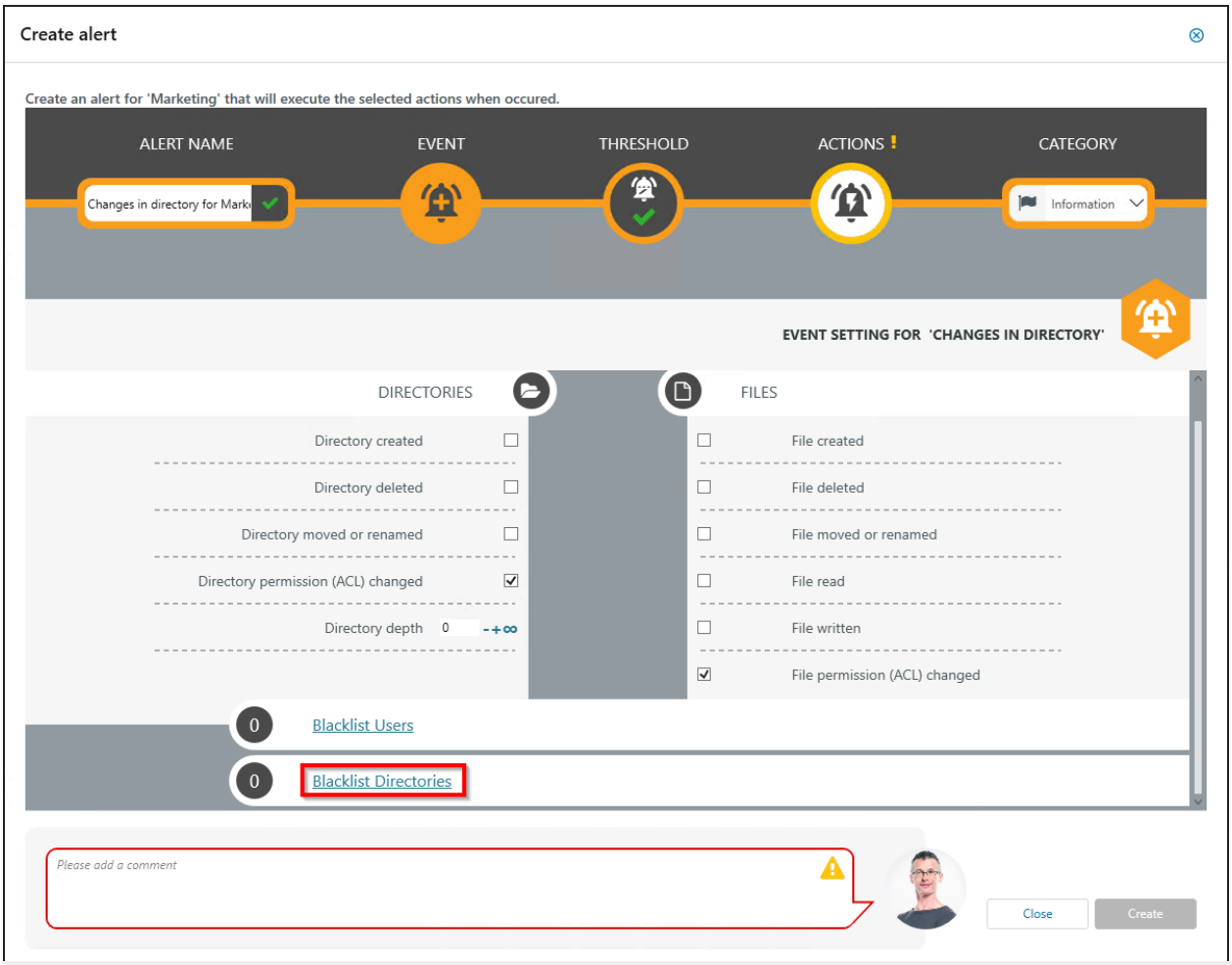


Optional: Use the blacklist to define which users do not trigger an alert.

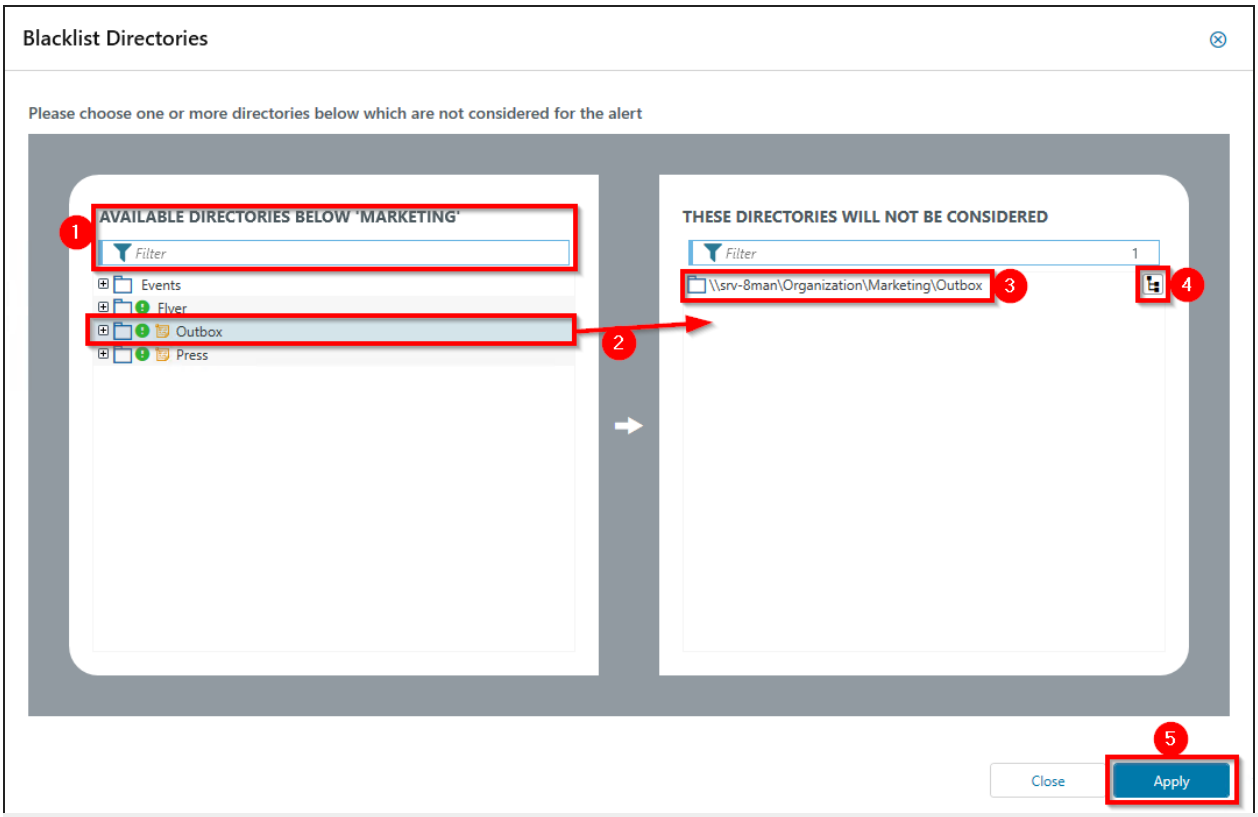
Each alert configuration has its own blacklist configuration.

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.

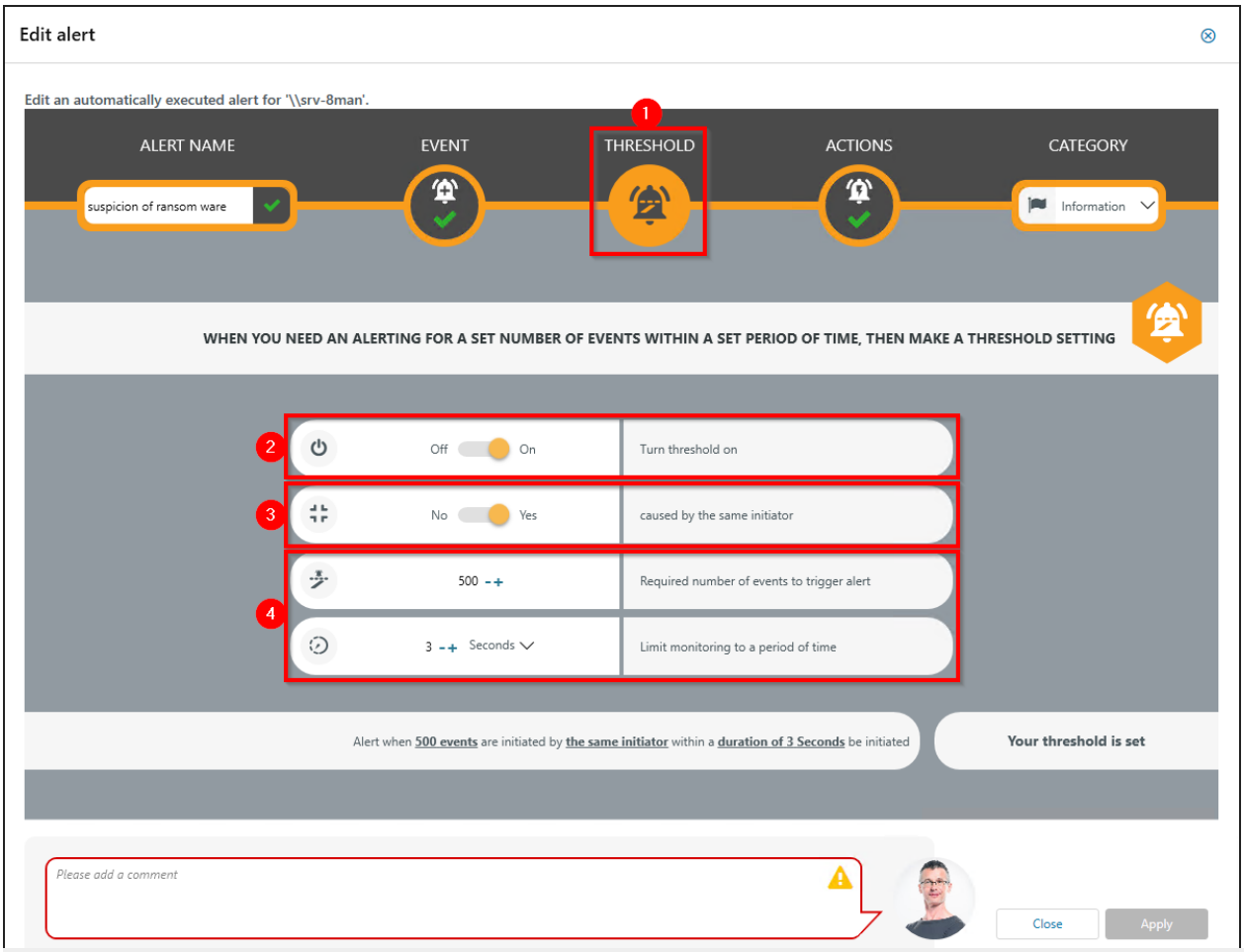


Optional: Select "Blacklist directories".



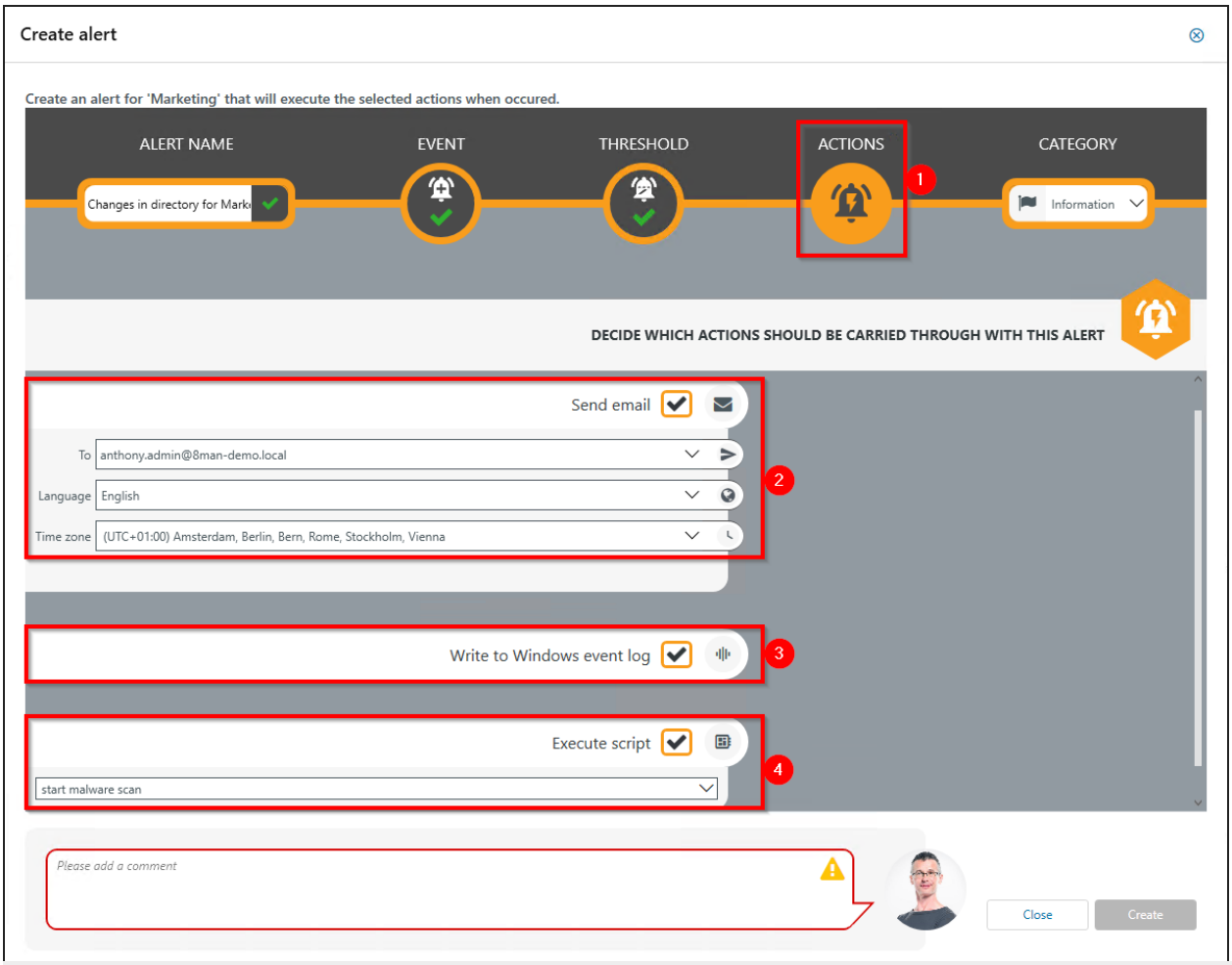
Optional: Use the blacklist to define which directories are not monitored.

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.



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.

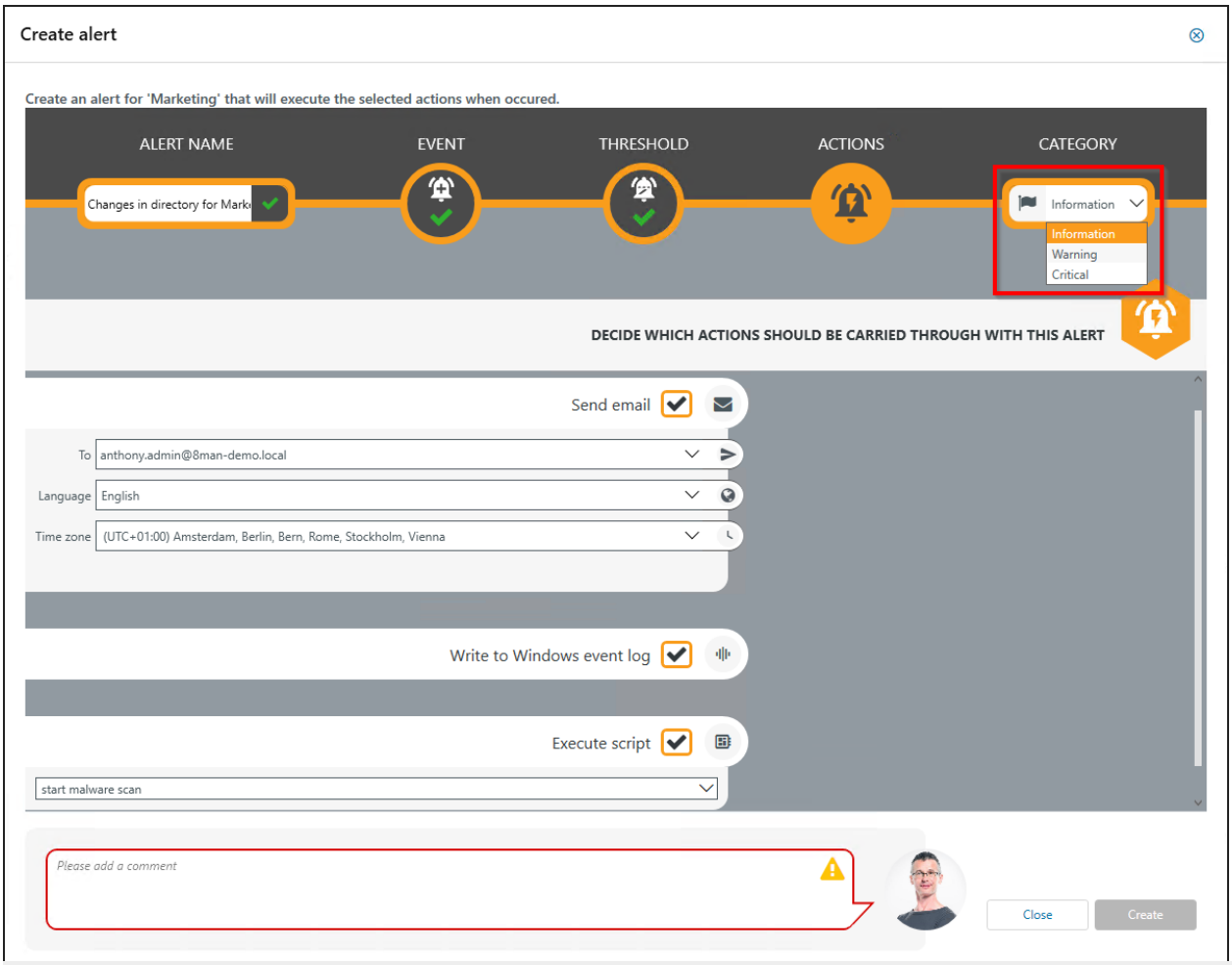
⚠ Defining a threshold with a large number of events over a long period of time will consume a lot of memory (RAM). We recommend that you configure time intervals as small as possible.



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.

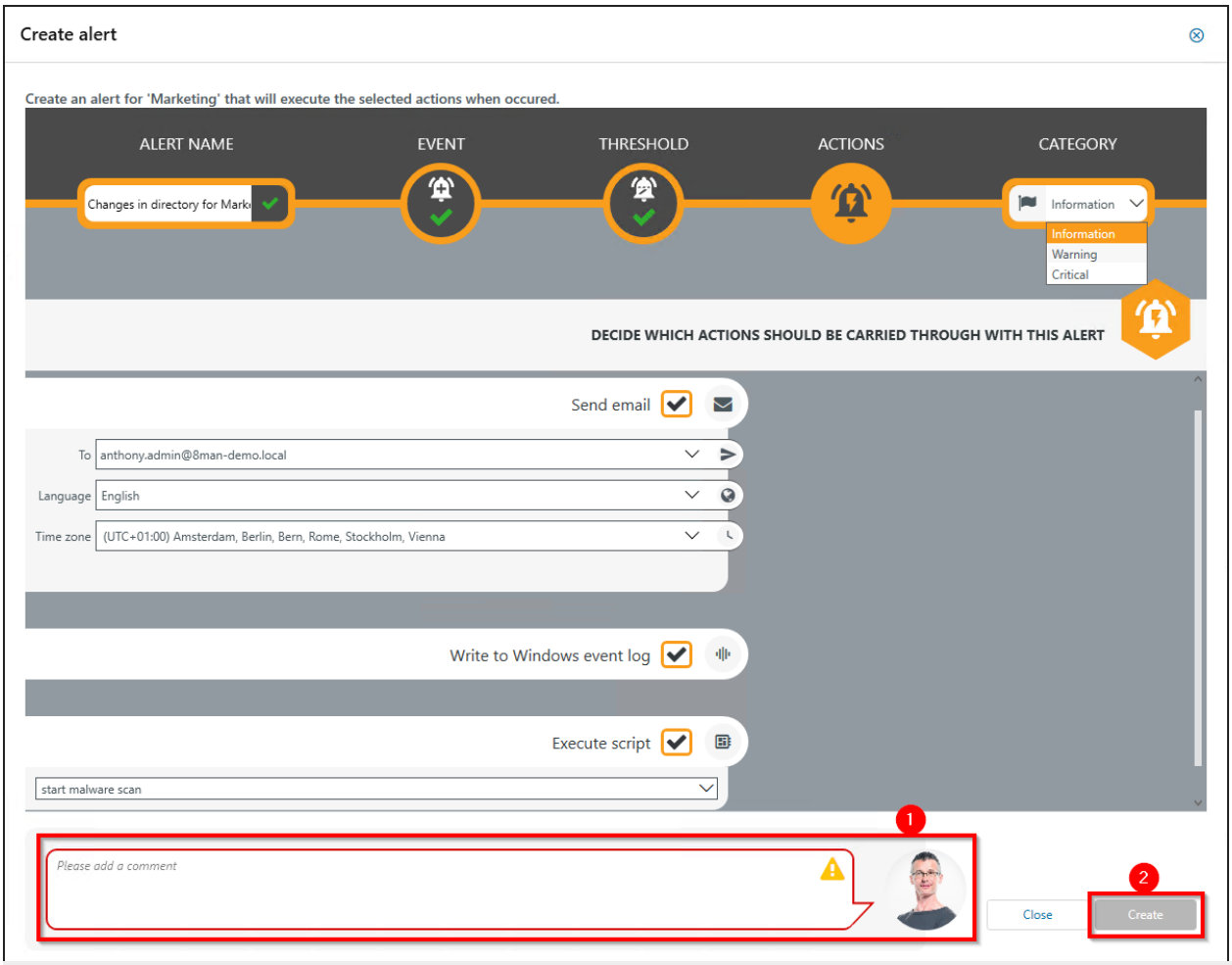
The content of the emails can be customized. This is analogous to the recertification emails.

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.



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.



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

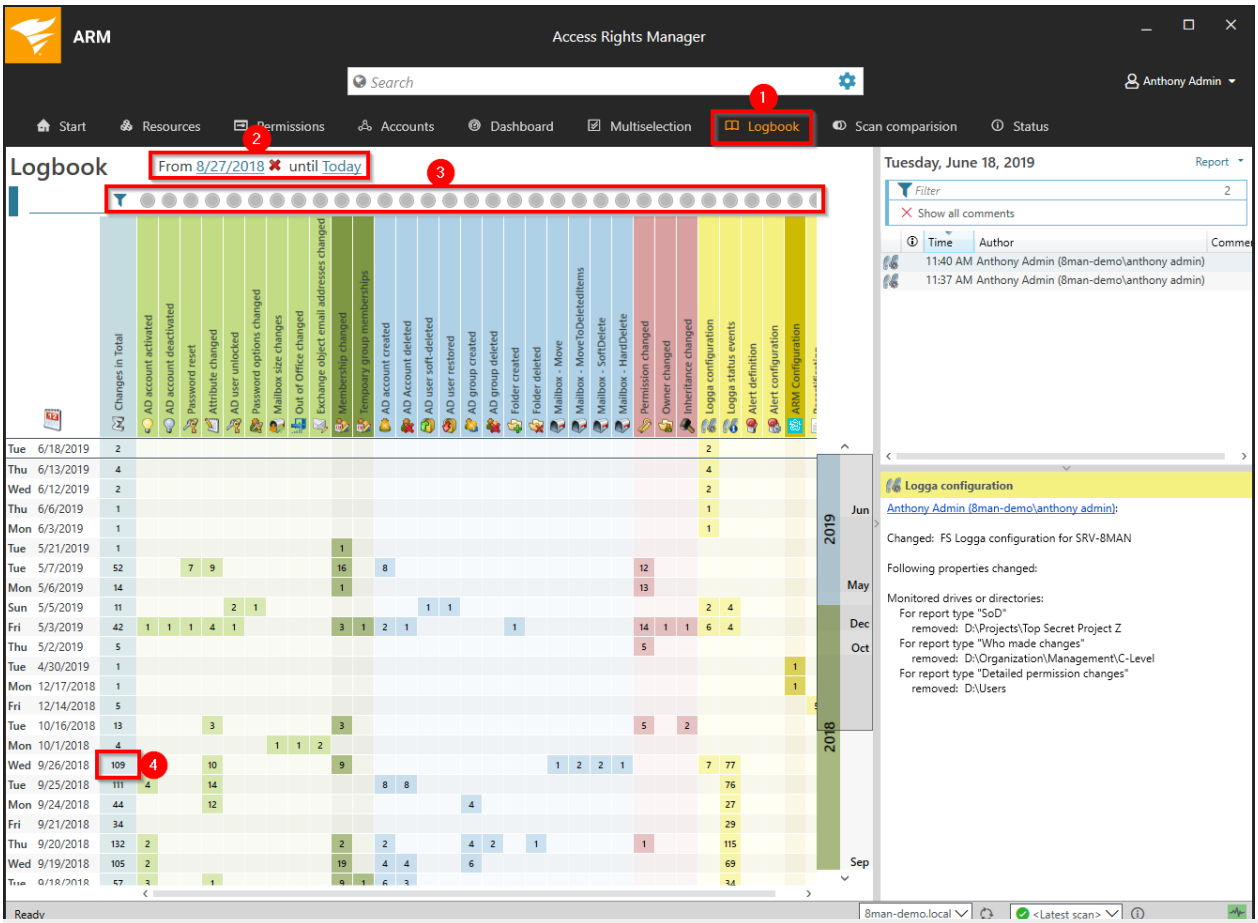
Background / Value

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.

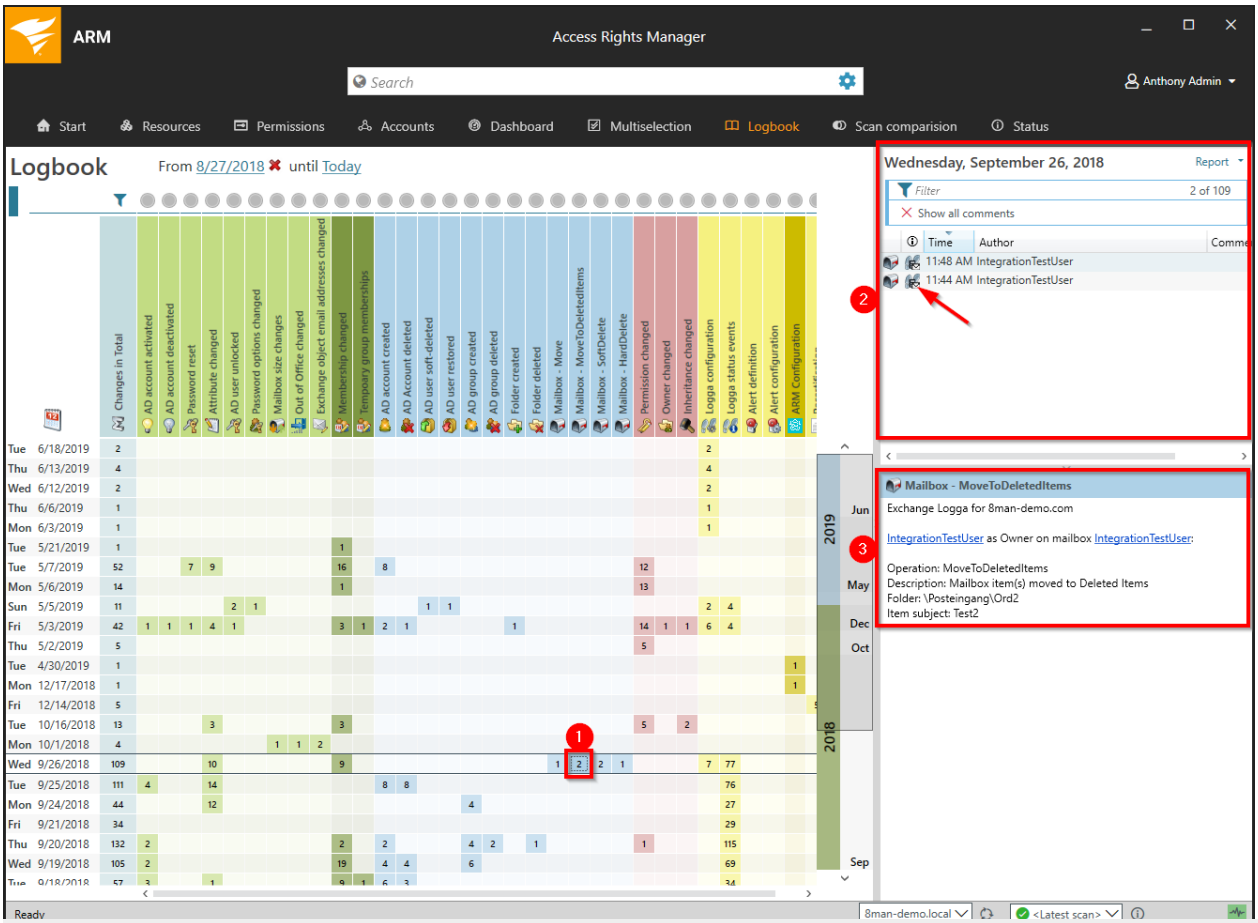
Related features

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).



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

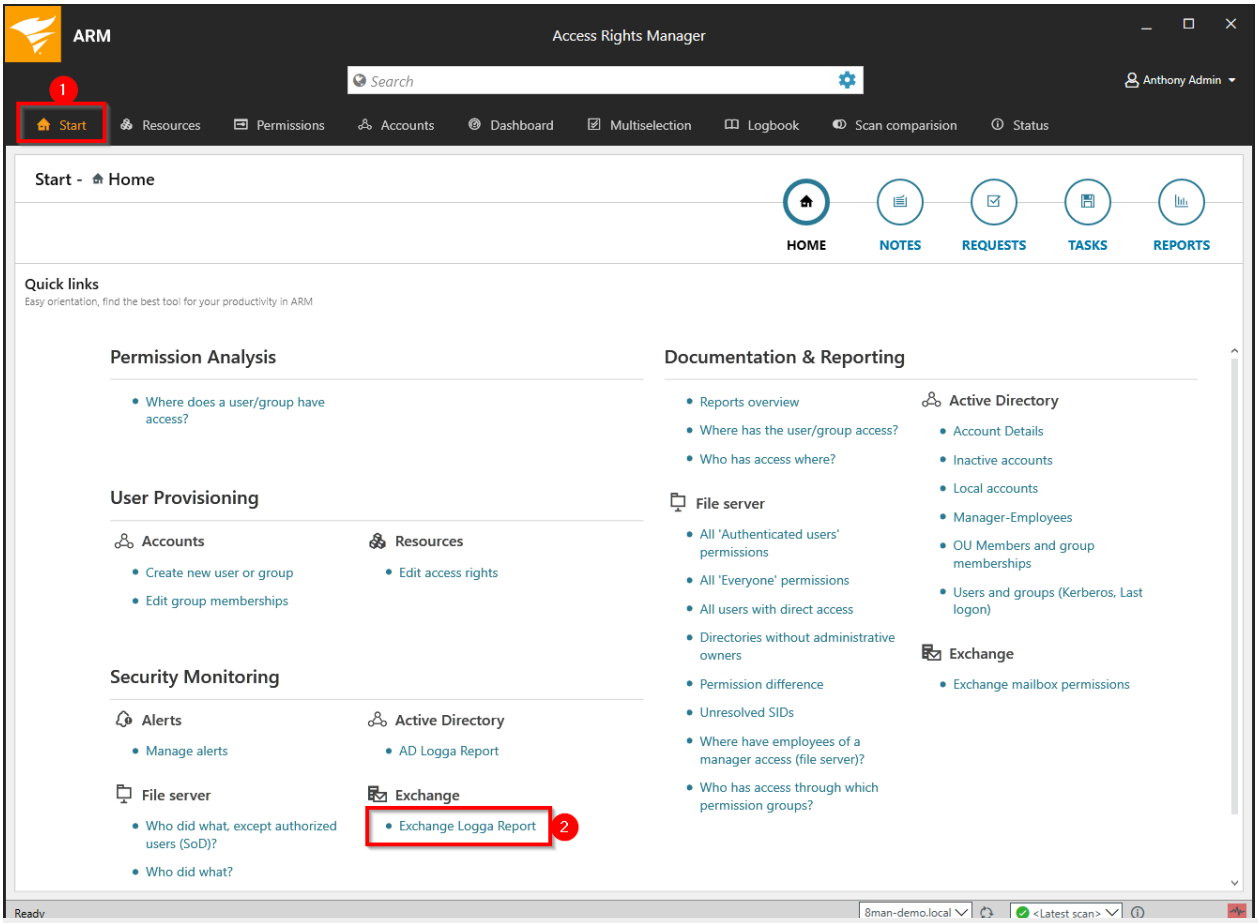
Background / Value

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.

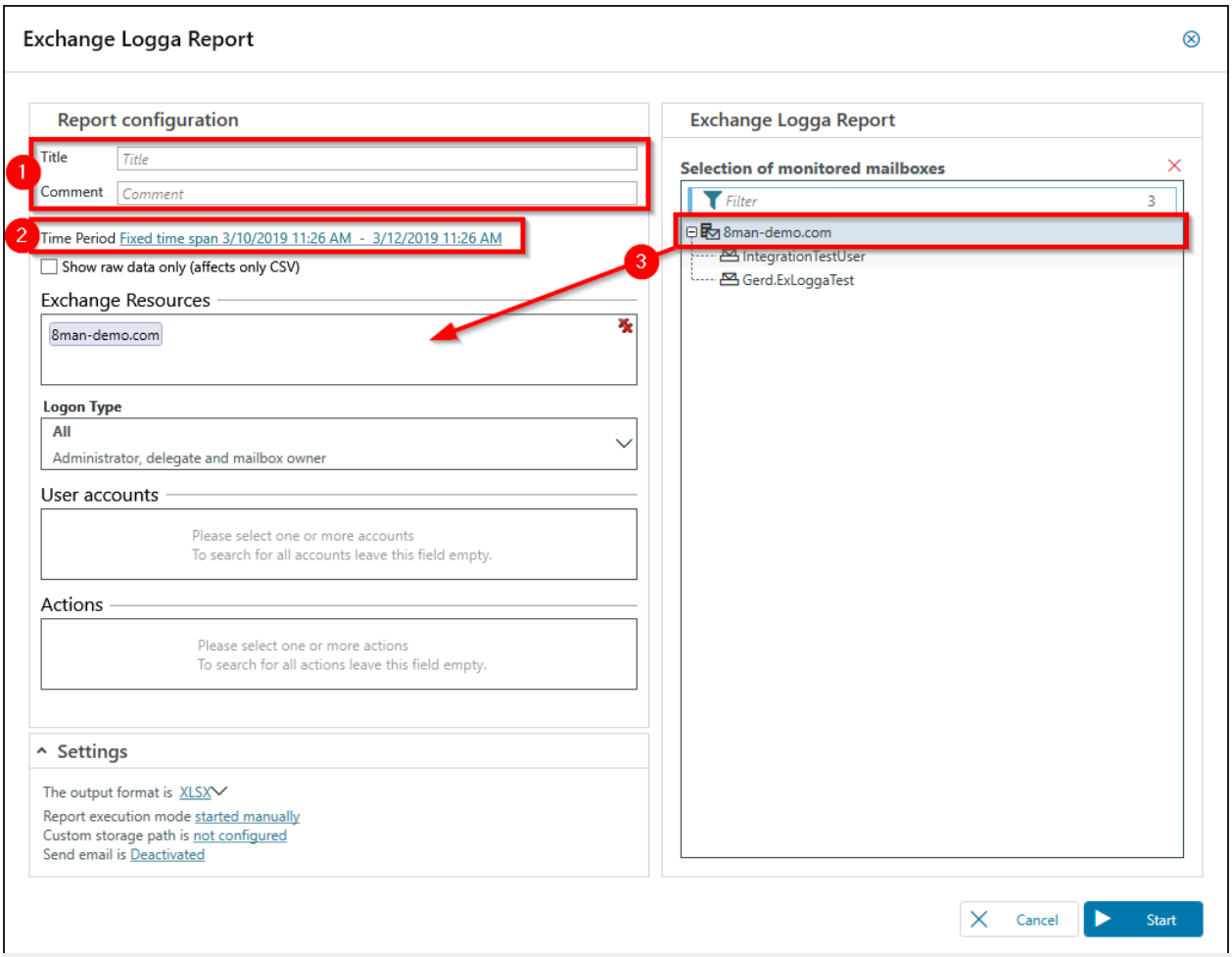
Related features

View activities in mailboxes, calendars, and contacts (logbook)

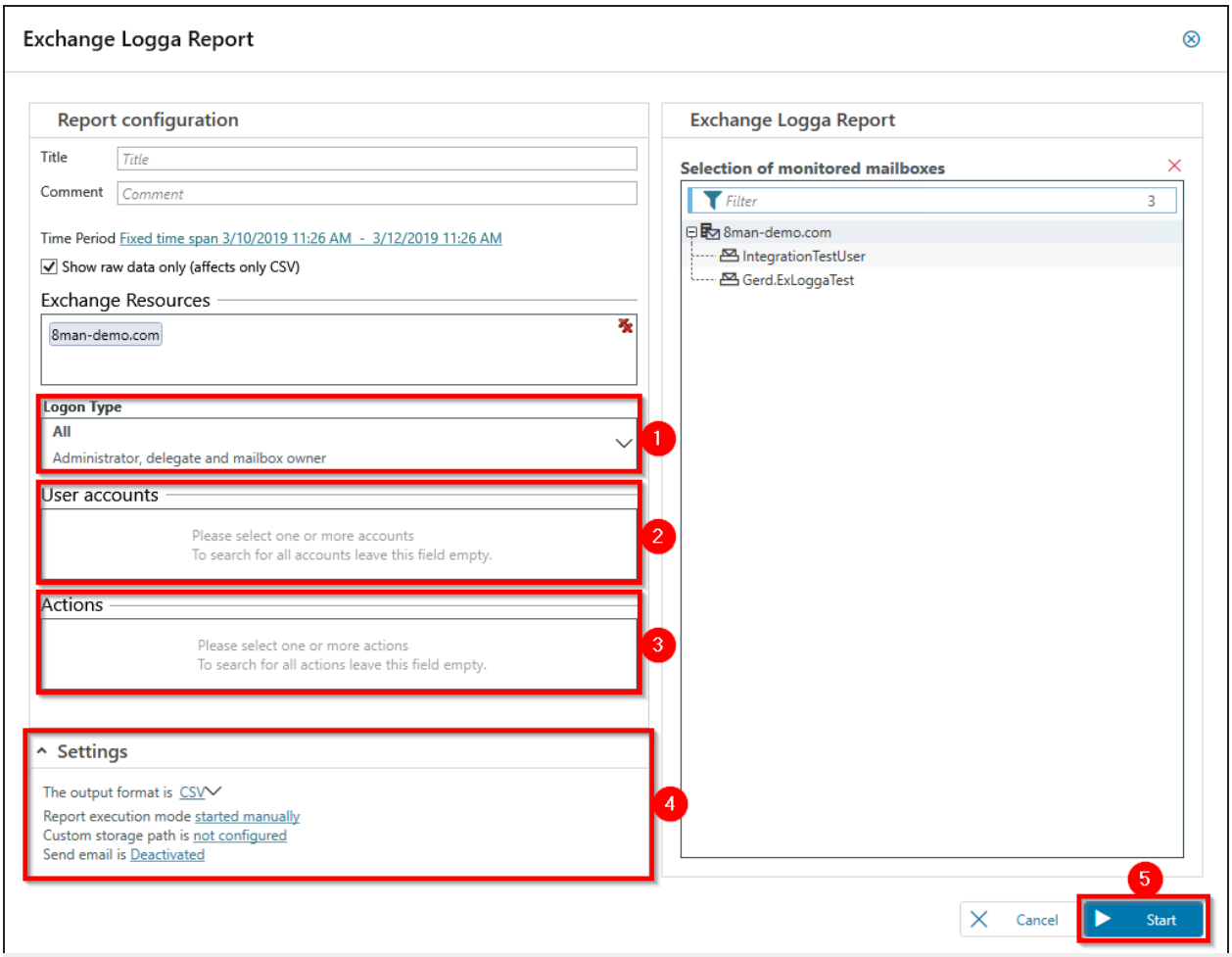
Step-by-step process



1. Select "Start".
2. Click "Exchange Logga Report".



1. Optional: Give the report a title and a description.
2. Set the period.
3. Add the required resources via drag & drop.



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.

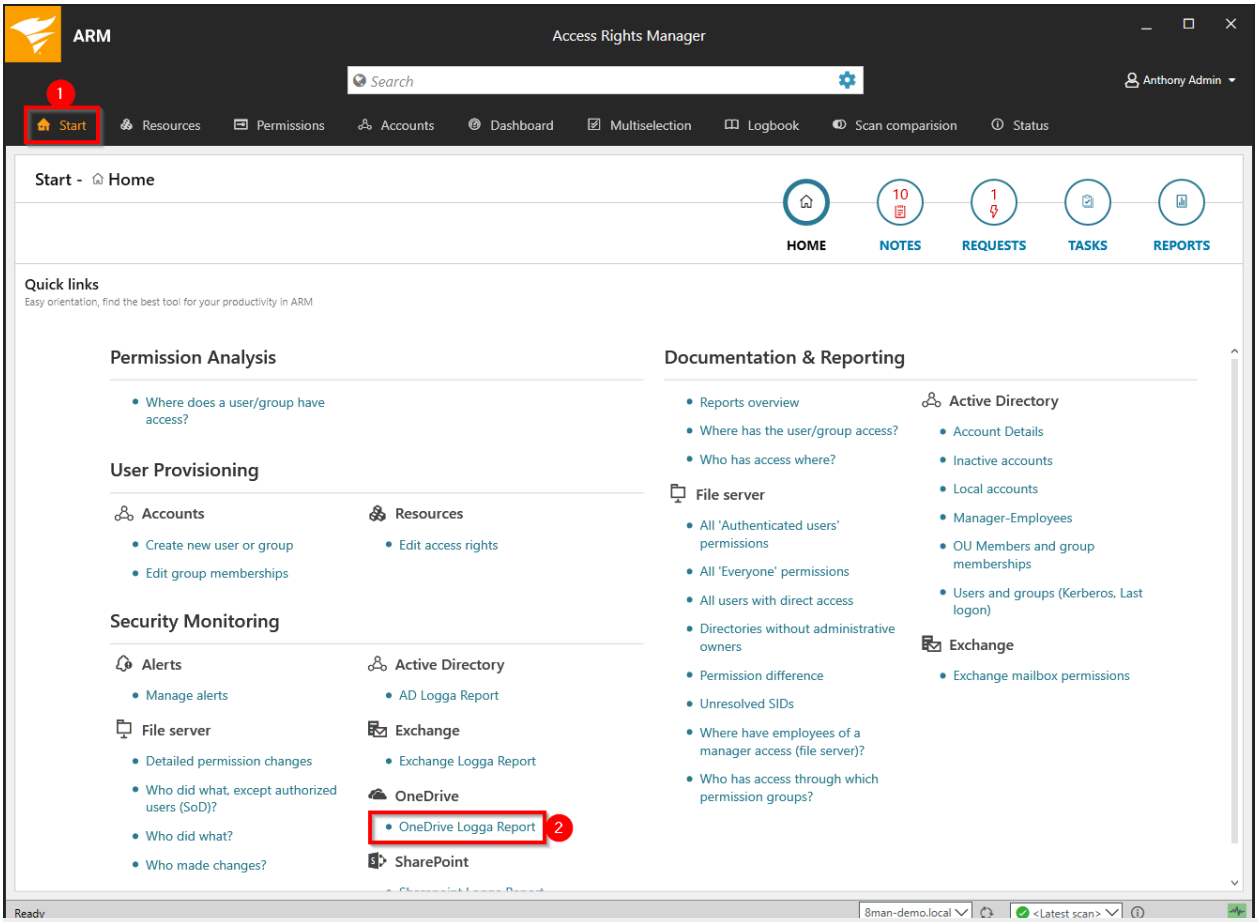
Events recorded with the OneDrive Logga can be analyzed in detail and recurrently using the report functions.

Related topics

Prepare the Office 365 integration

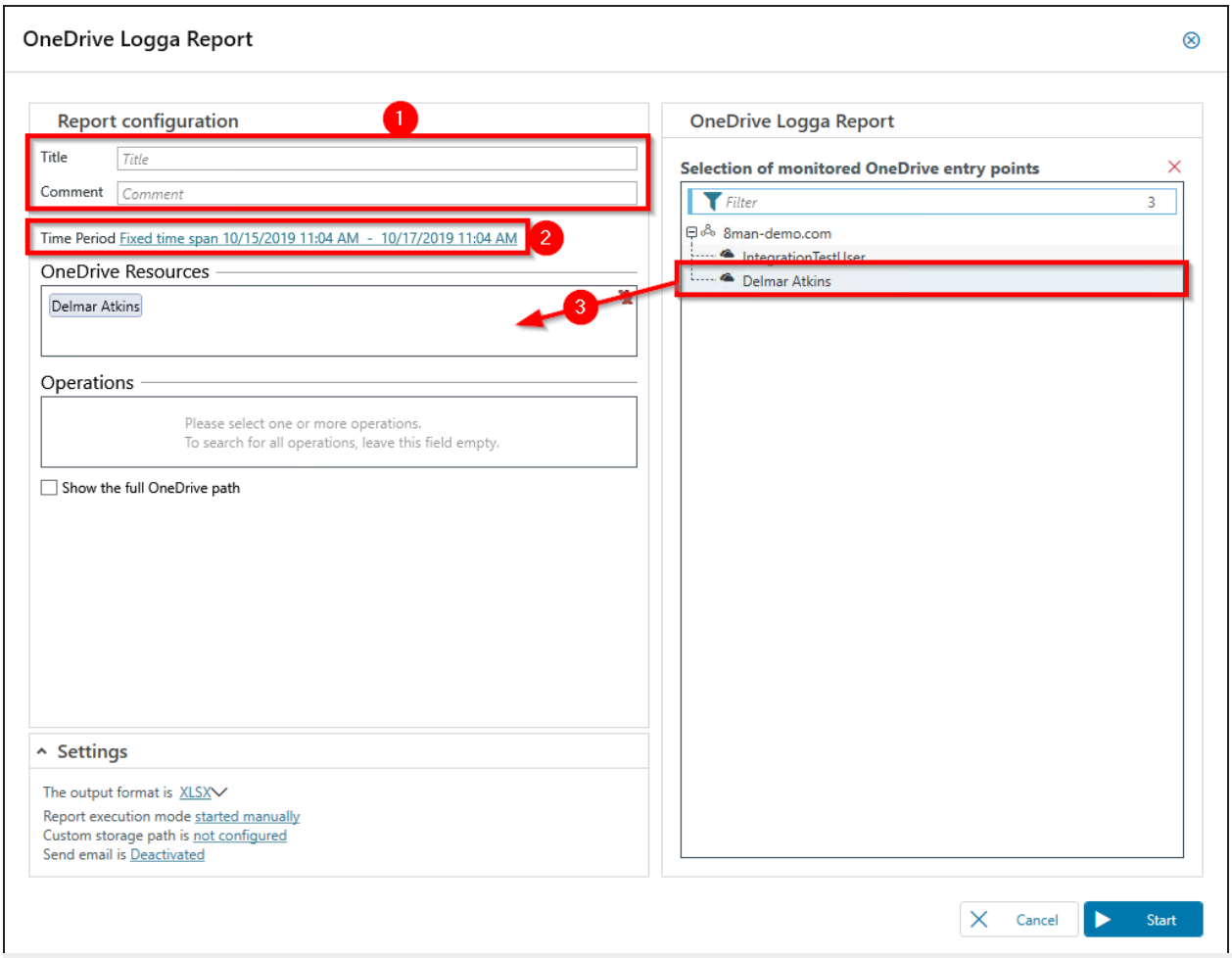
Add a OneDrive Logga configuration

Step-by-step process

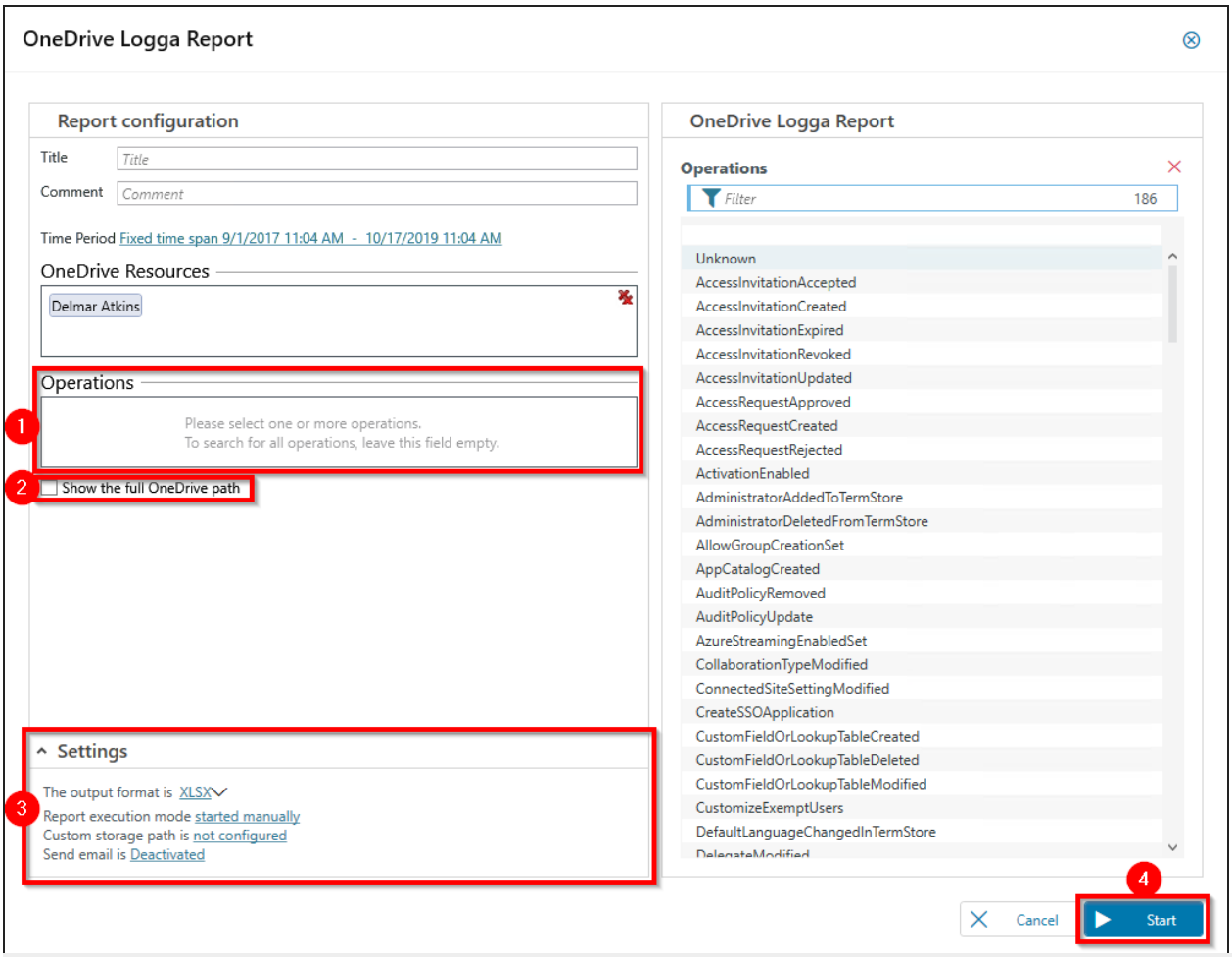


1. Select "Start".

2. Click "OneDrive Logga Report".



1. Optional: Give the report a title and a description.
2. Set the period.
3. Add the desired resources via drag & drop.



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.

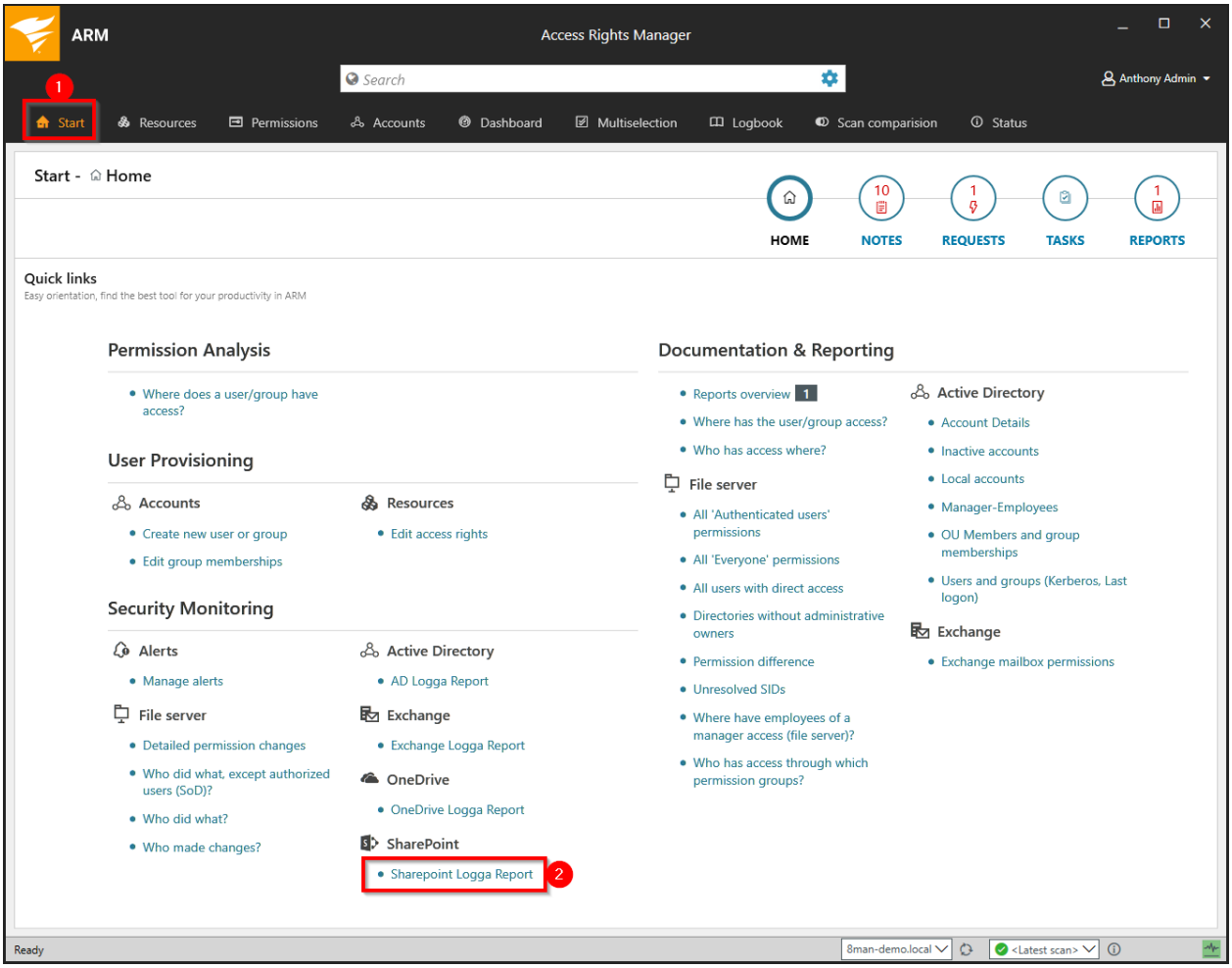
Events recorded with the SharePoint Online Logga can be analyzed in detail and recurrently using the report functions.

Related topics

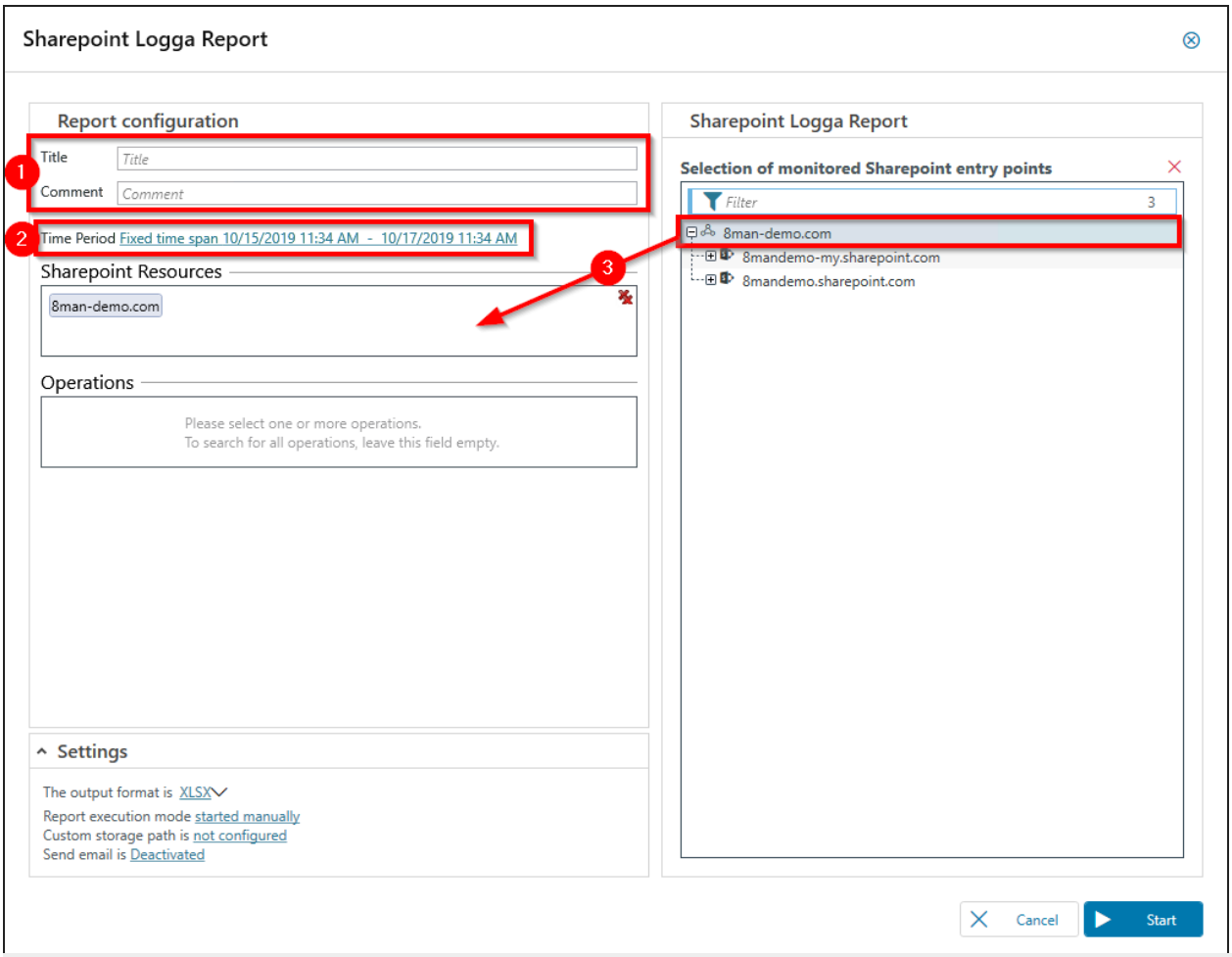
Prepare the Office 365 integration

Add a SharePoint Online Logga configuration

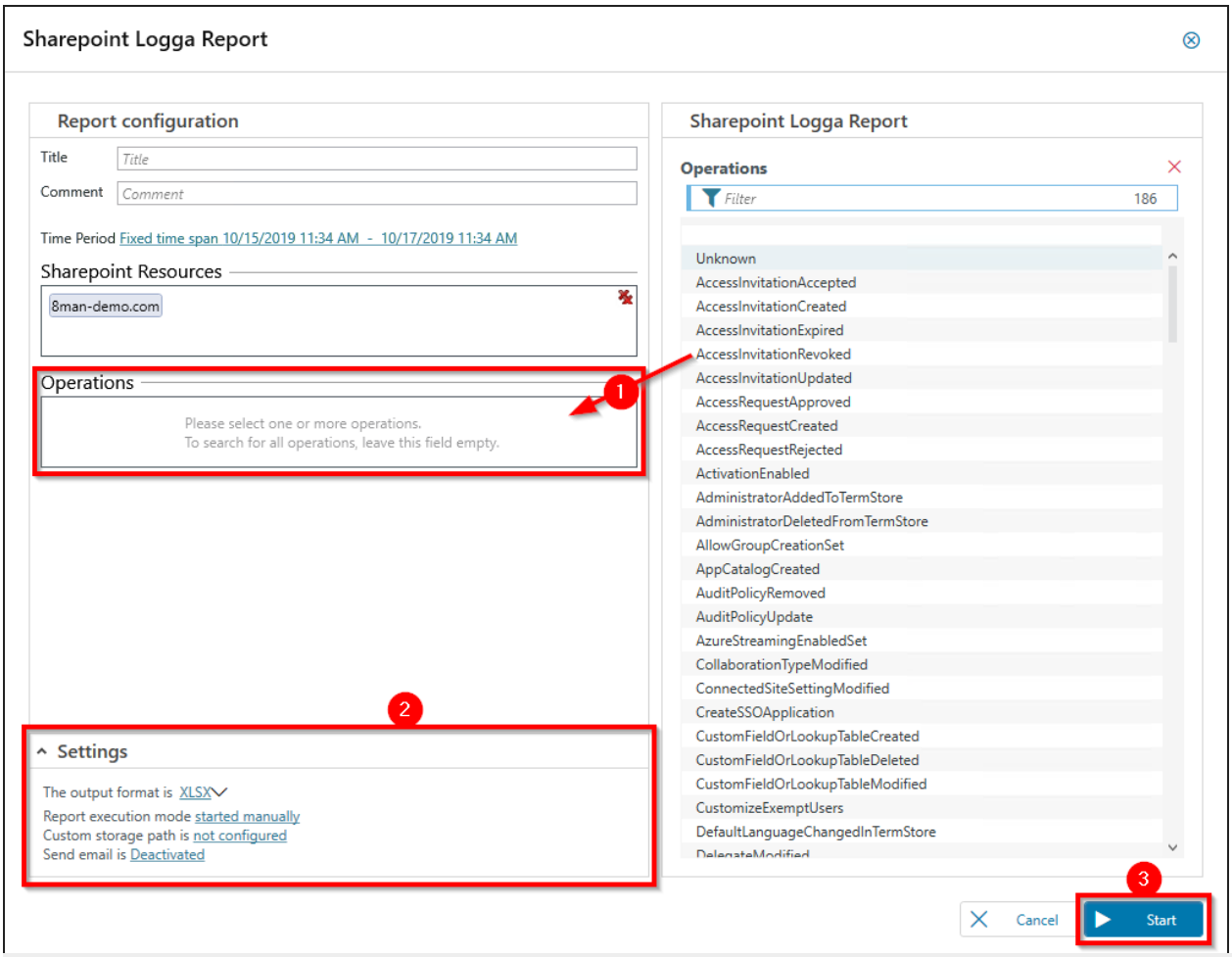
Step-by-step process



1. Select "Start".
2. Click "SharePoint Logga Report".



1. Optional: Give the report a title and a description.
2. Set the period.
3. Add the desired resources via drag & drop.



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.

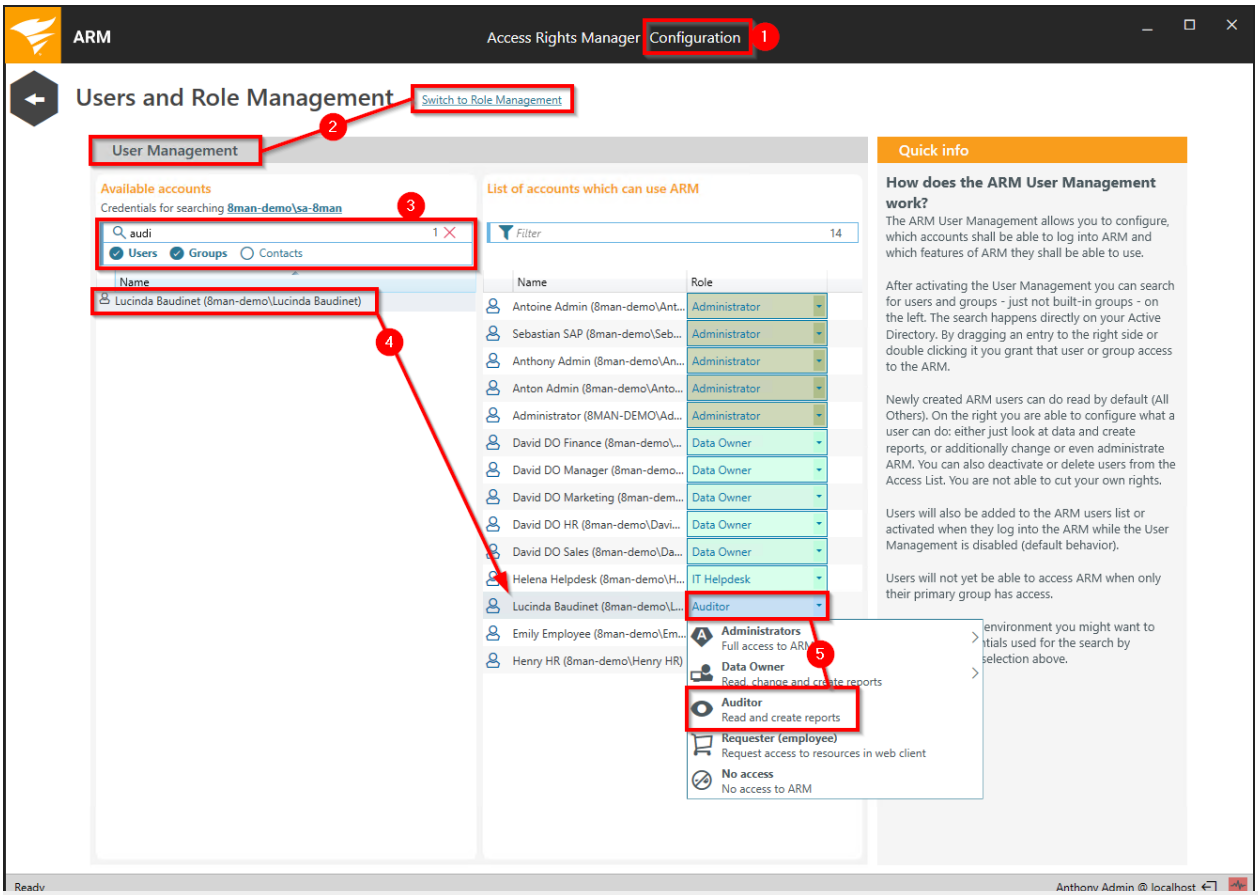
Create a simple read-only account in ARM

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



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?

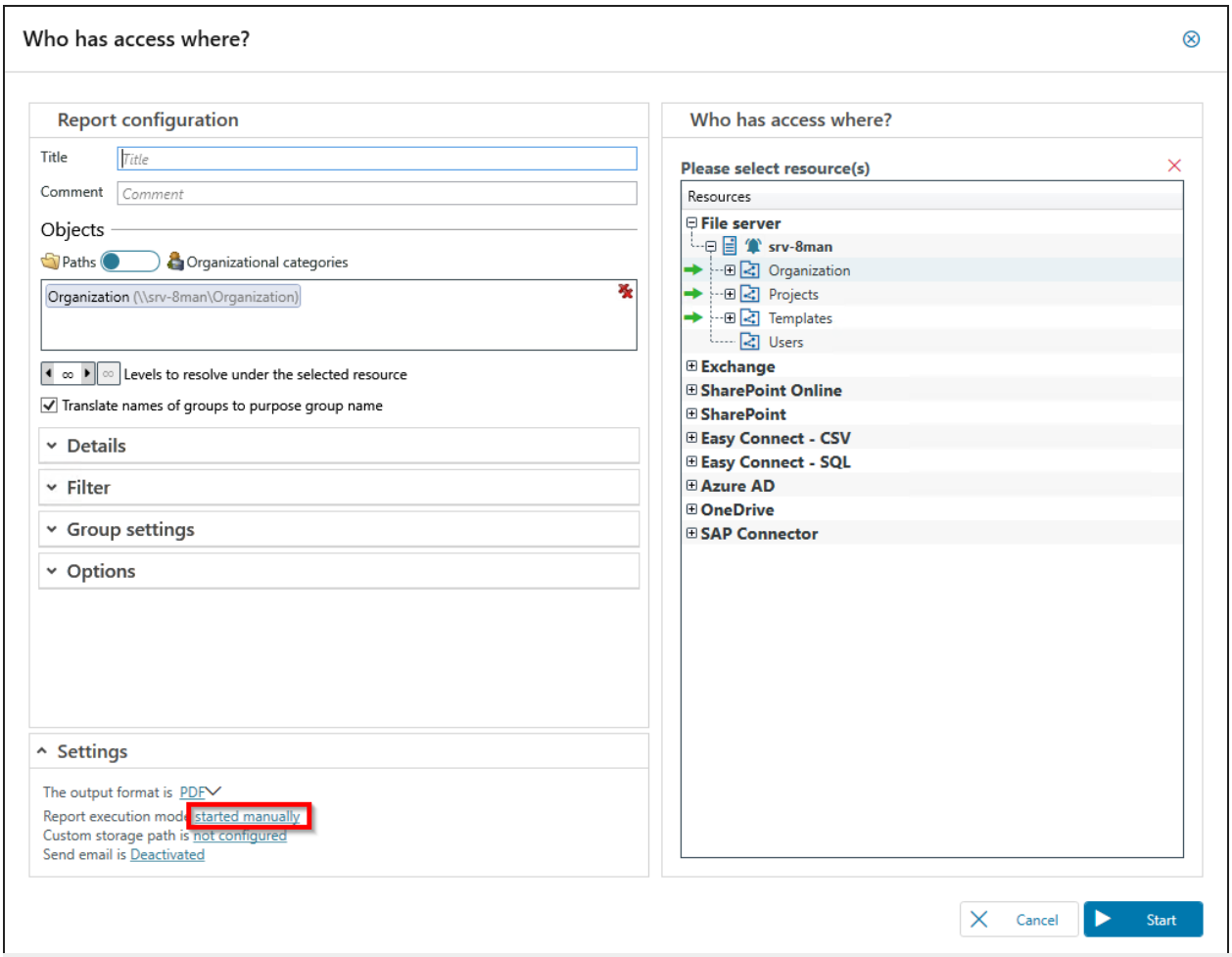
Exchange

Who has access to what?
Identifying mailbox permissions

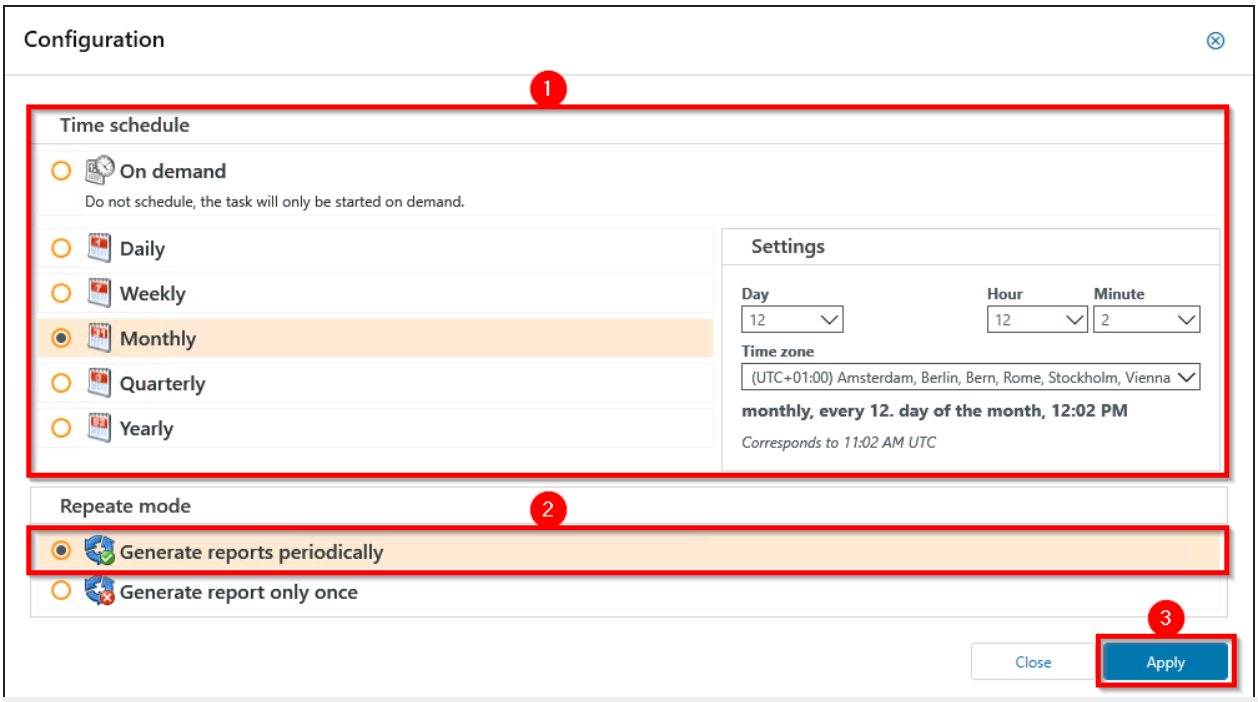
SharePoint

Who has access where?
Where do users and groups have access?

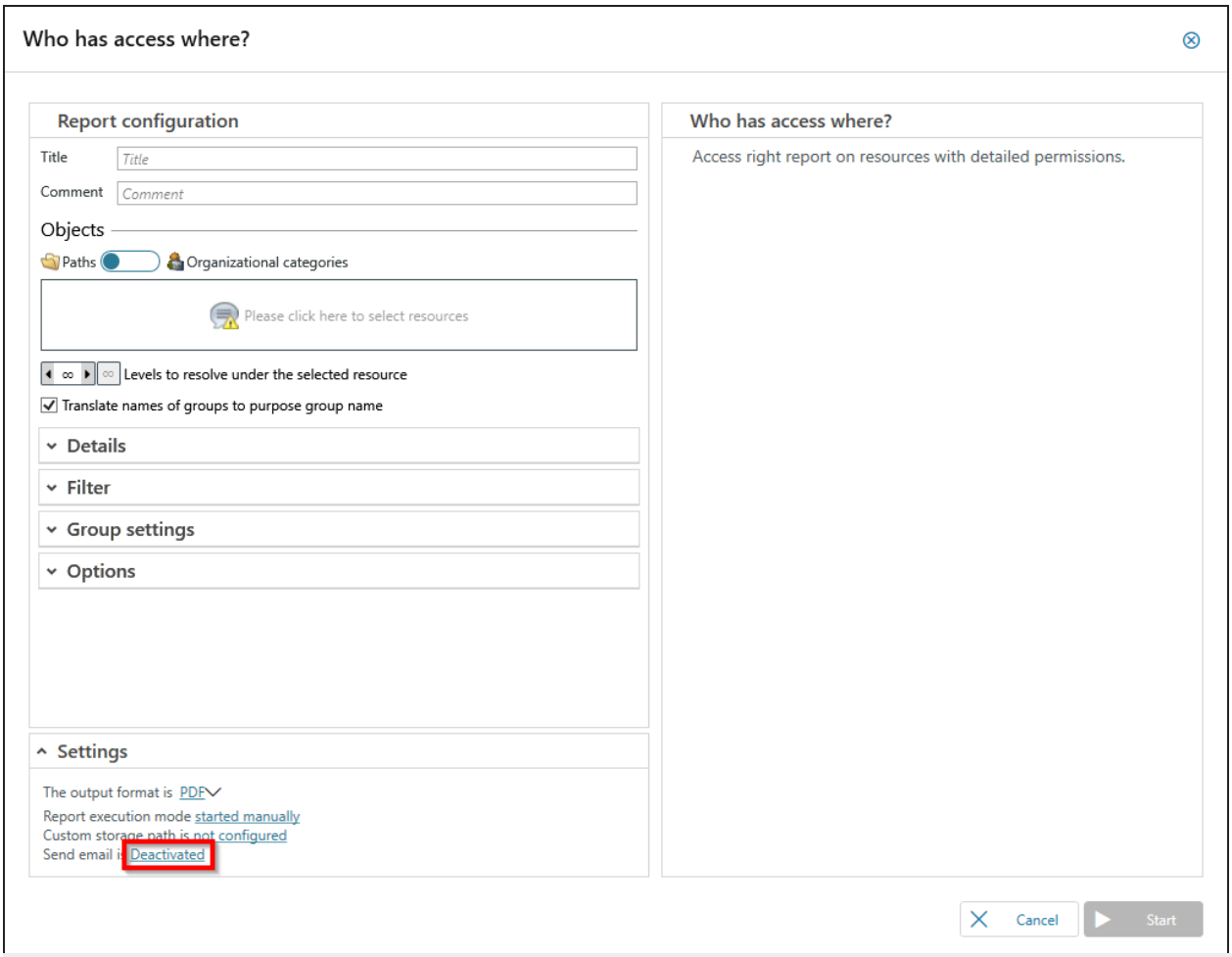
Step-by-step process



Select the desired report. Click on "started manually" in the "Settings" area.



1. Determine the frequency.
2. Activate the mode "Generate reports periodically".
3. Click on "Apply".



Click on "Deactivated".

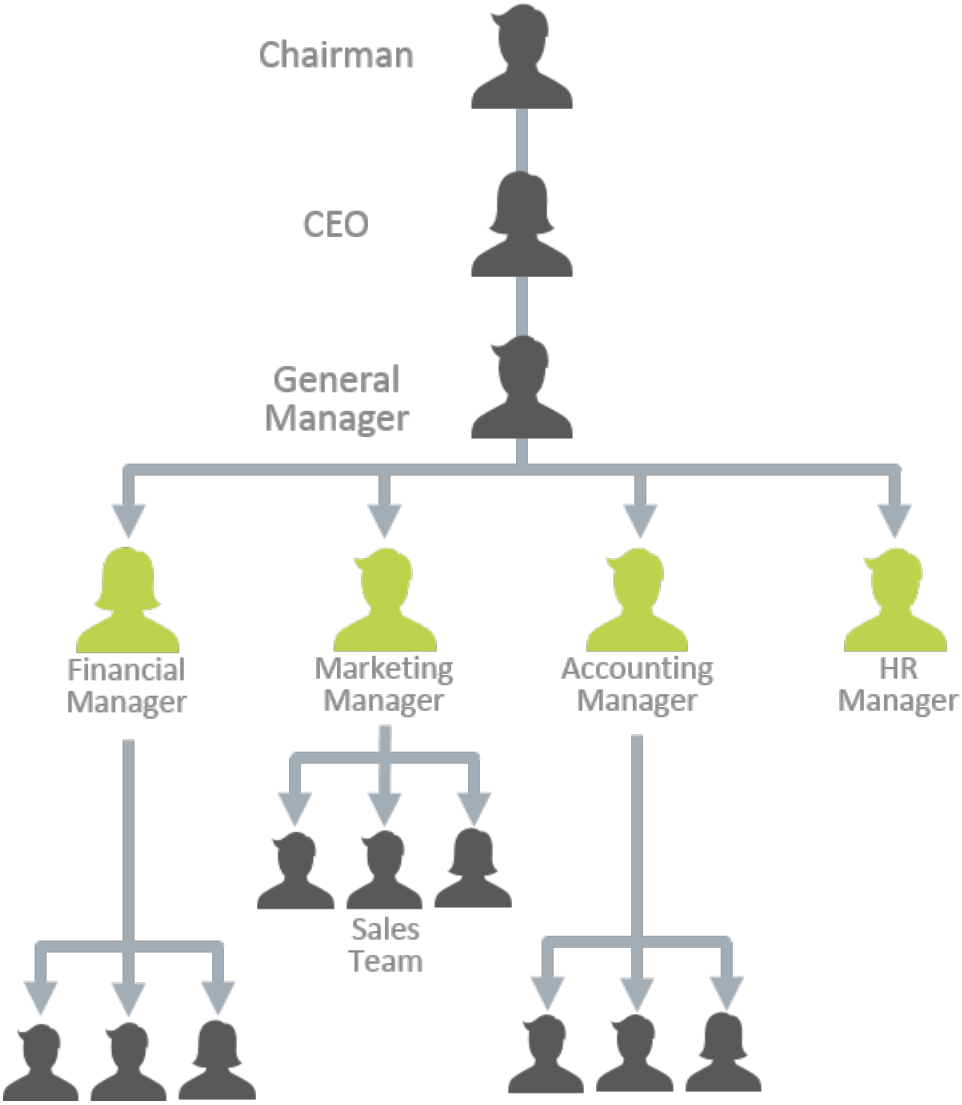
1. Activate emails.
2. Activate the option "Add report as email attachment".
3. Determine who should receive the email. You can enter more than one recipient.
4. Click on "Apply".

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.



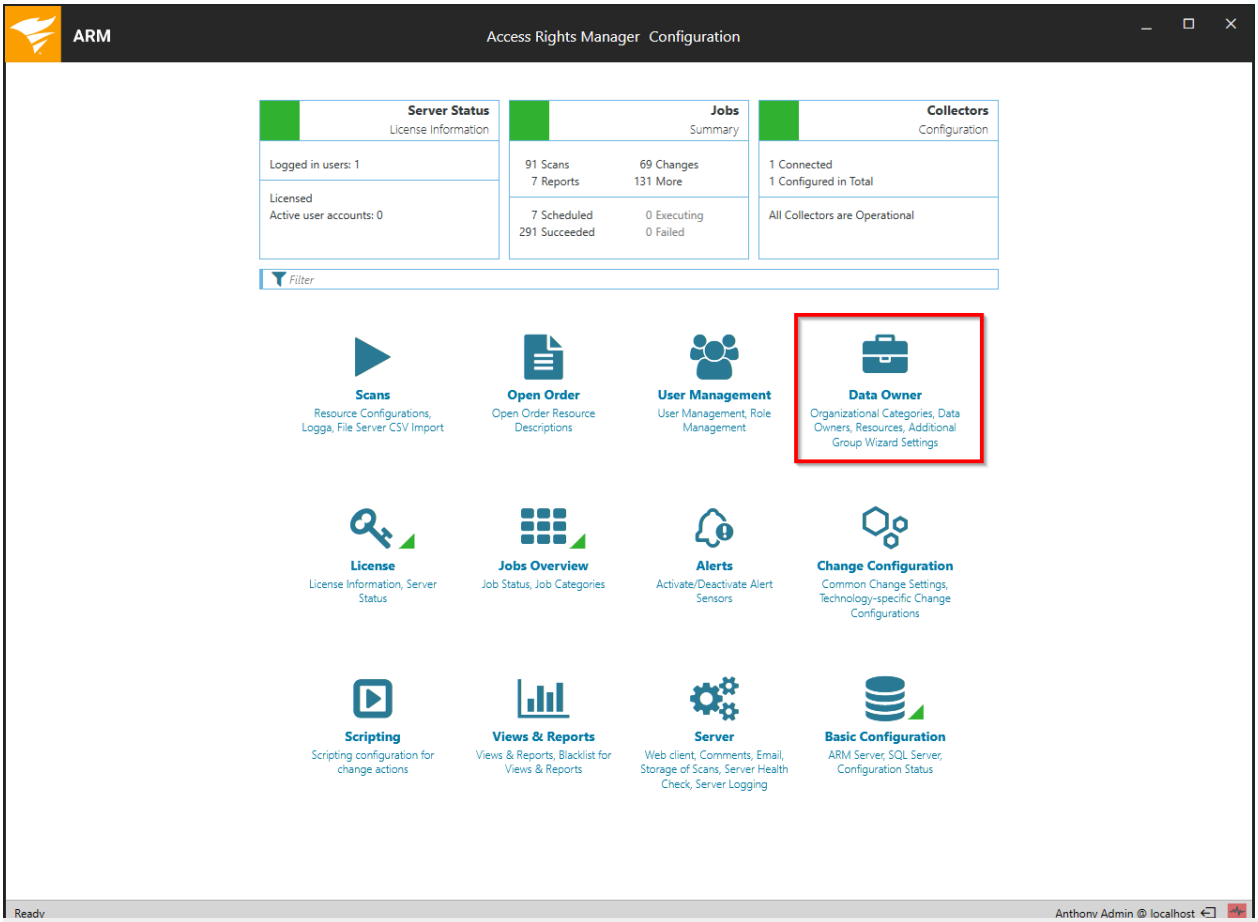
Define data owners and assign resources

Background / Value

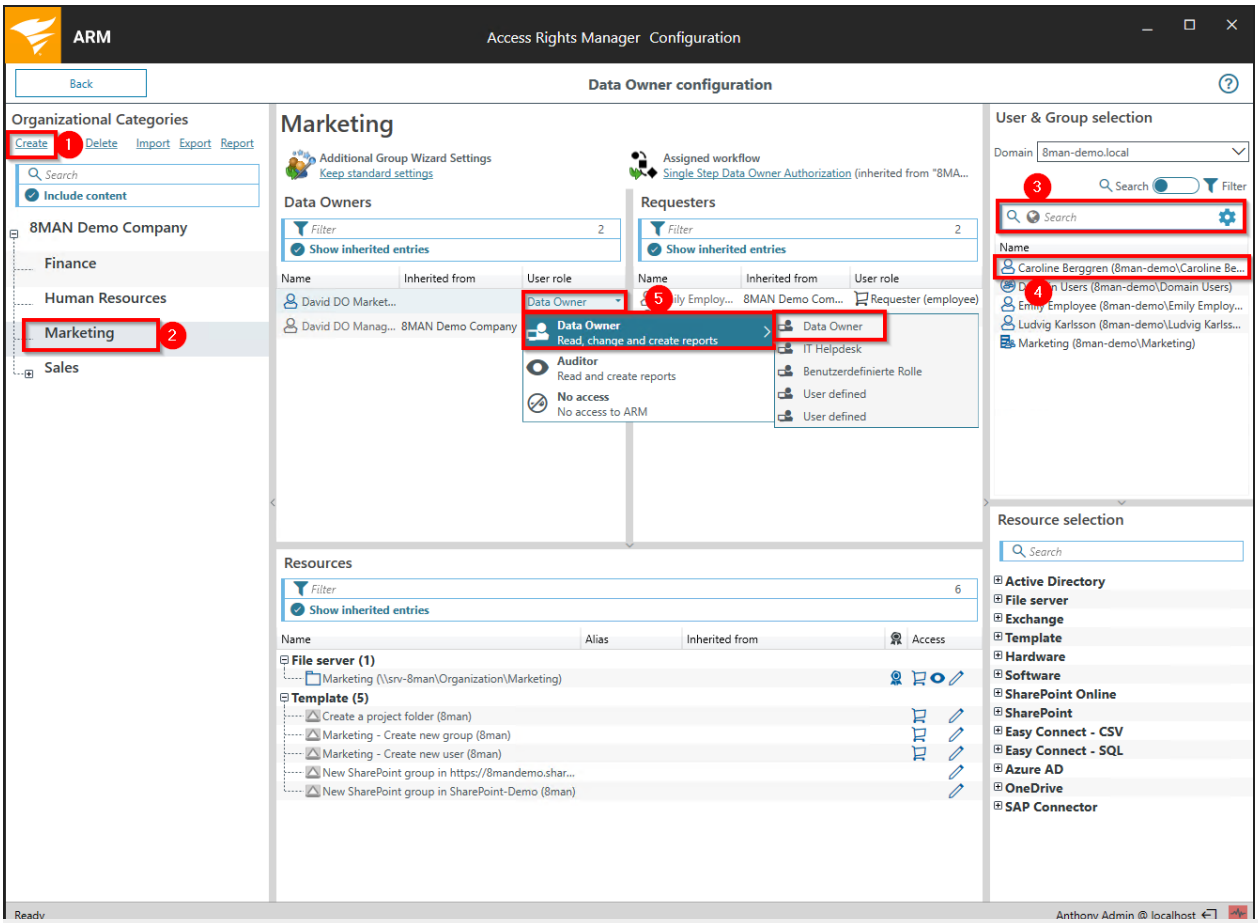
Data Owners and Managers have the responsibility to protect digital resources in their departments. ARM allows you to delegate this individual responsibility effectively. The following example shows a typical configuration.

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.

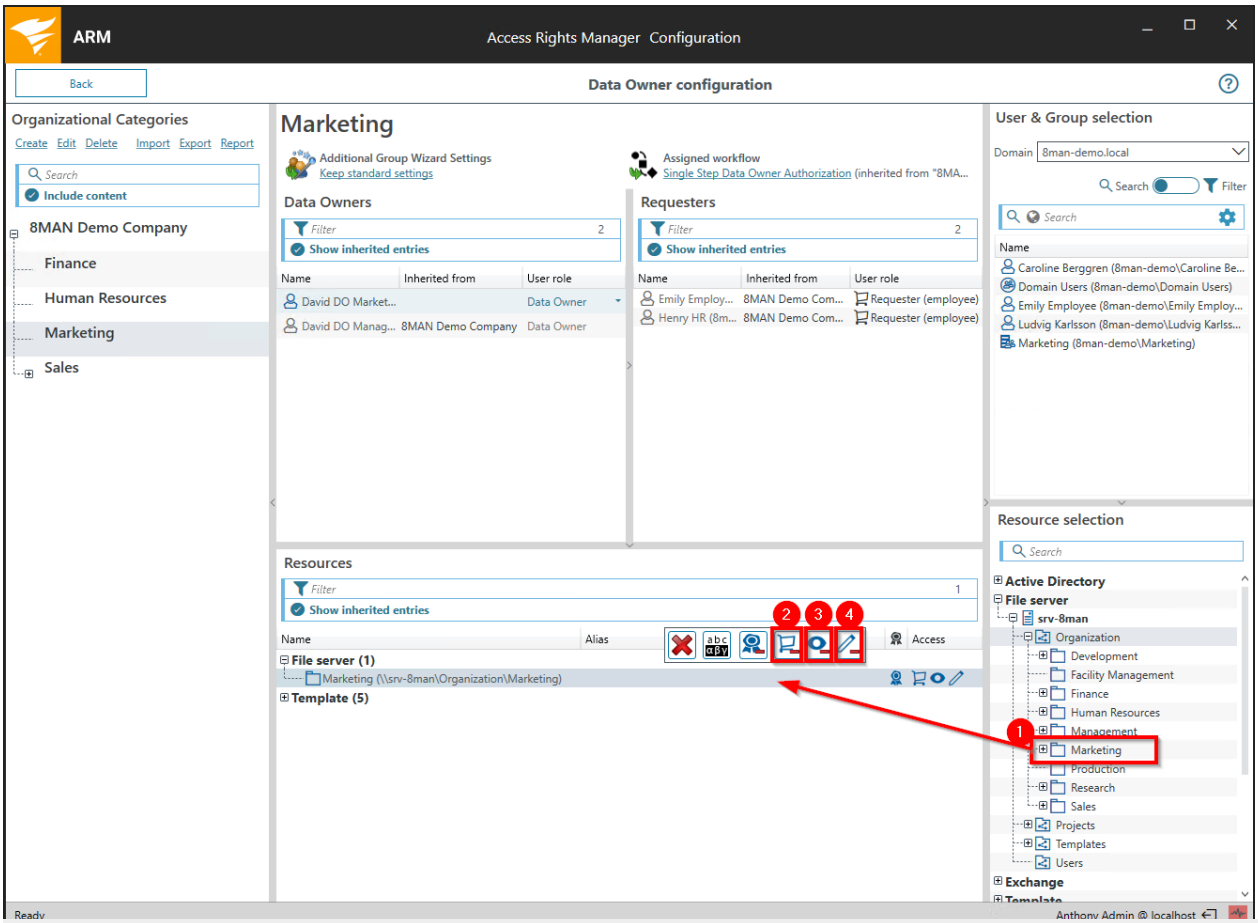
Step-by-step process



Start the ARM configuration application and select "Data Owner".



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".



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.

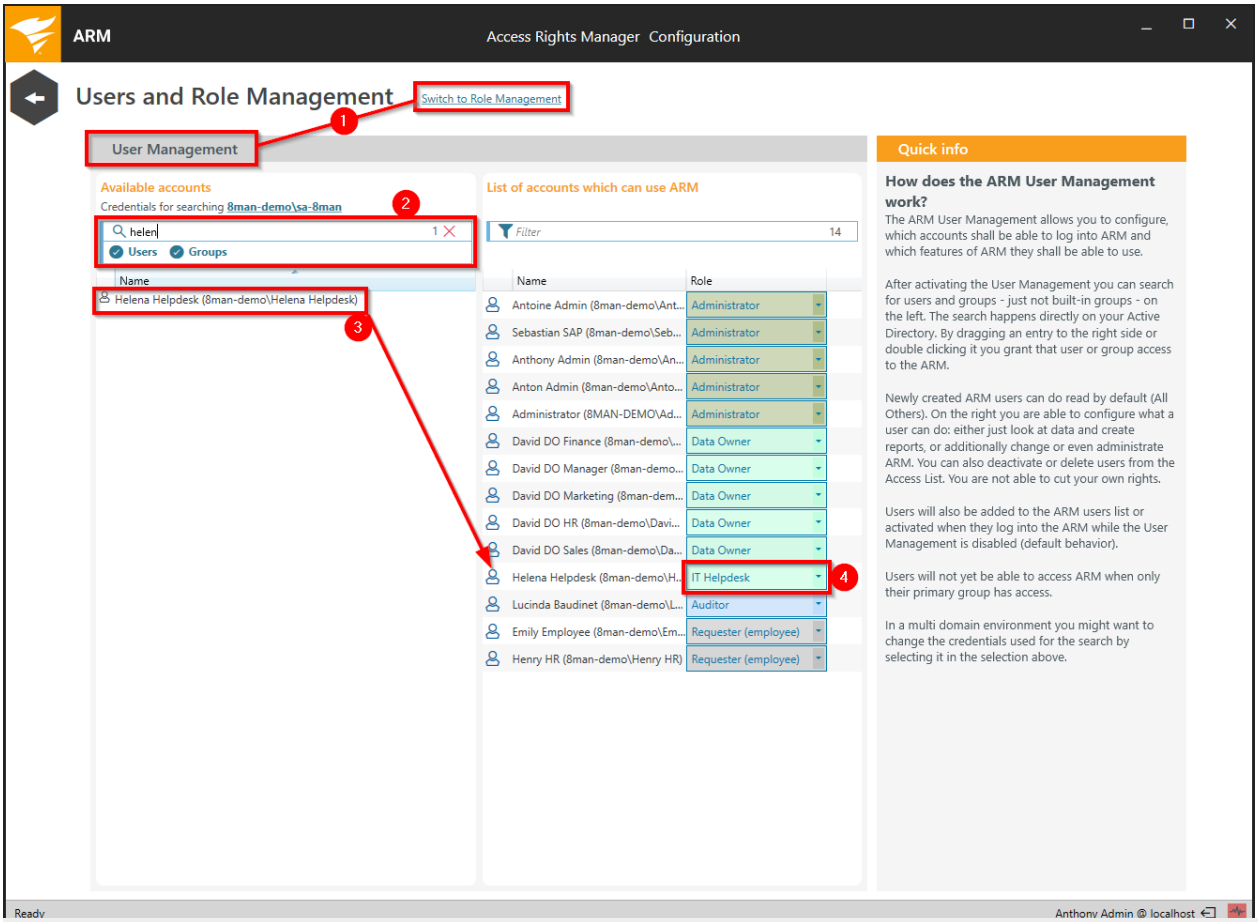
Assign responsibilities to help desk employees

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



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.

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:

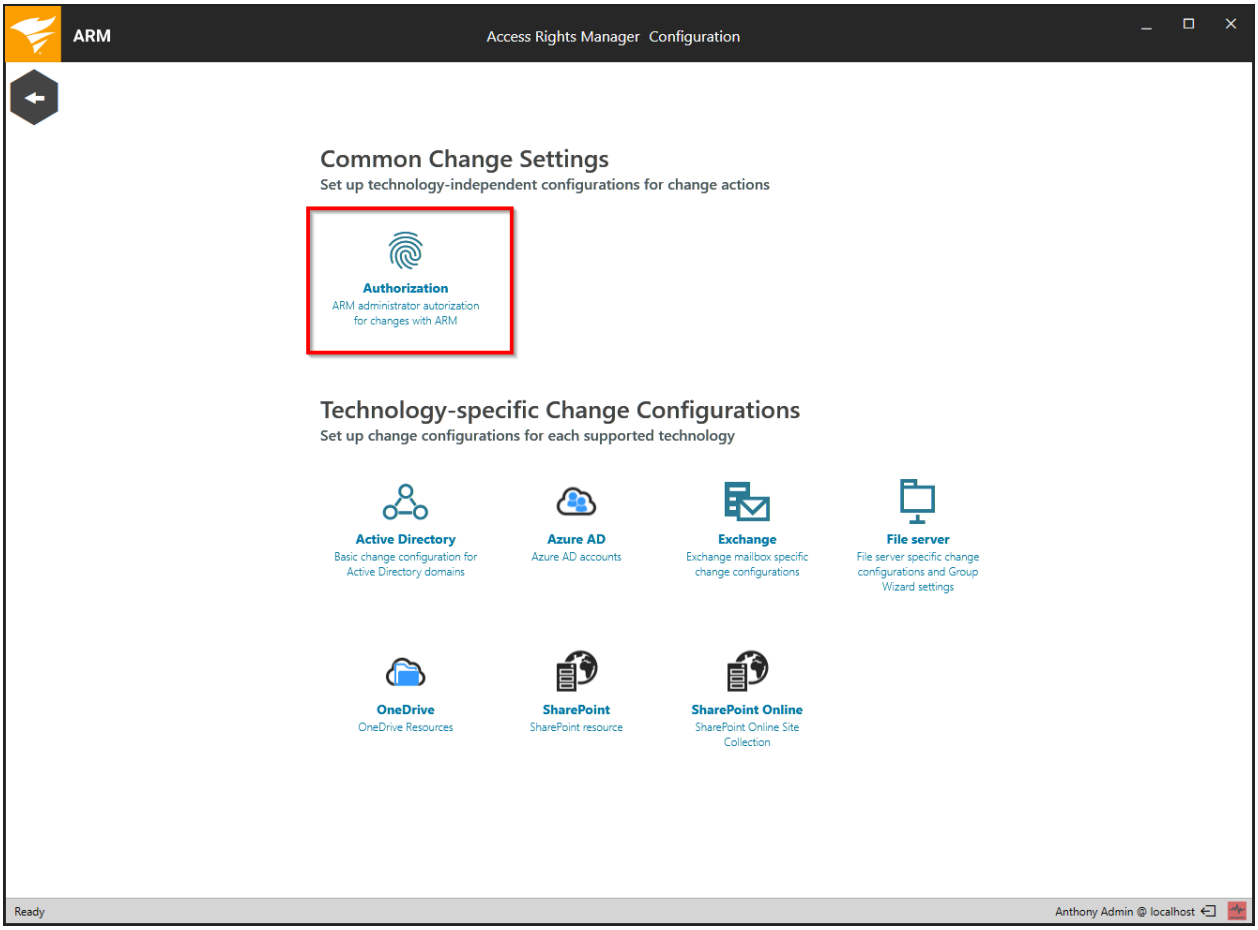
- Data owners manage permissions. Every change has to be approved by IT administrators.
- Use ARM GrantMA self service portal for employees and managers with individual approval flows and automatic execution.

The simple authorization process - approving and rejecting actions as an administrator

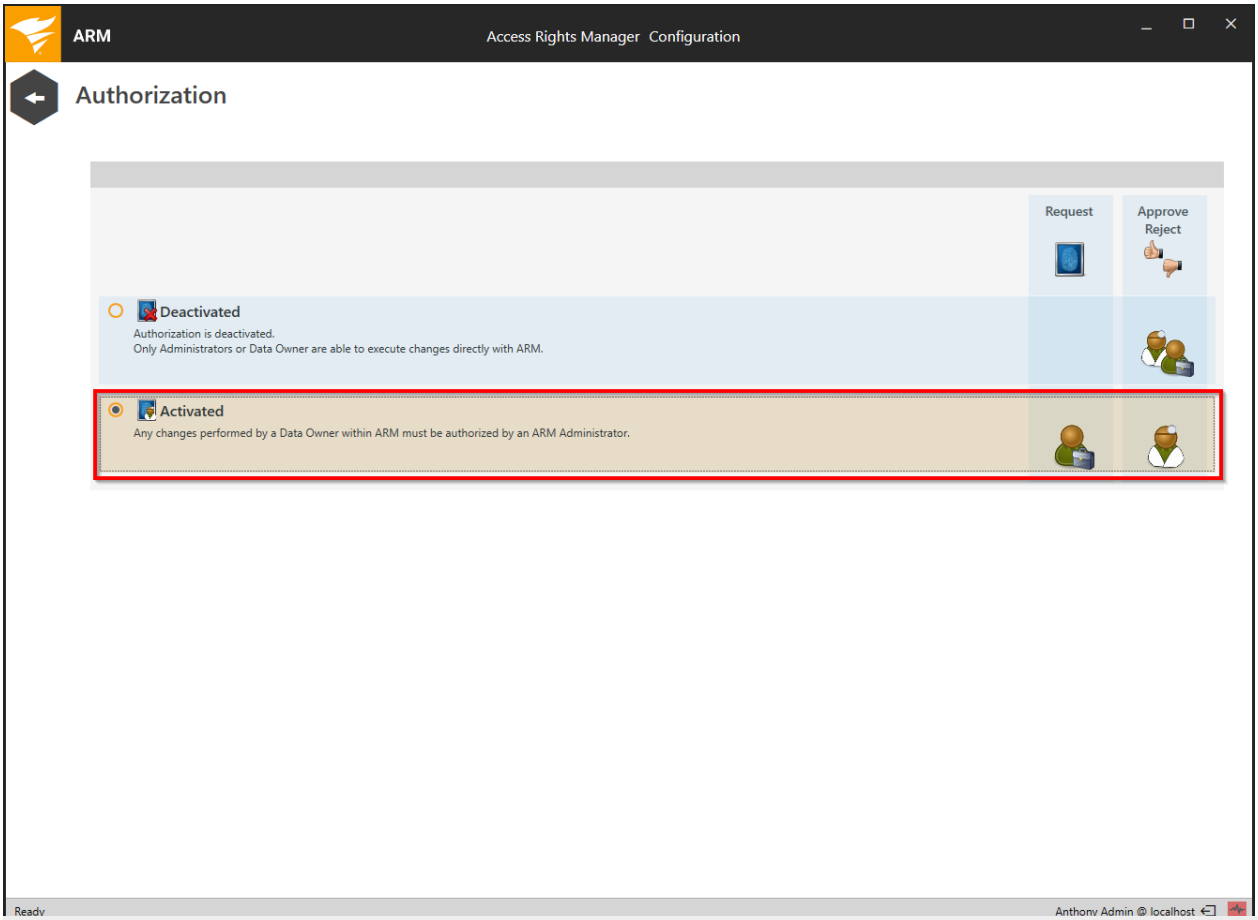
Background / Value

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.

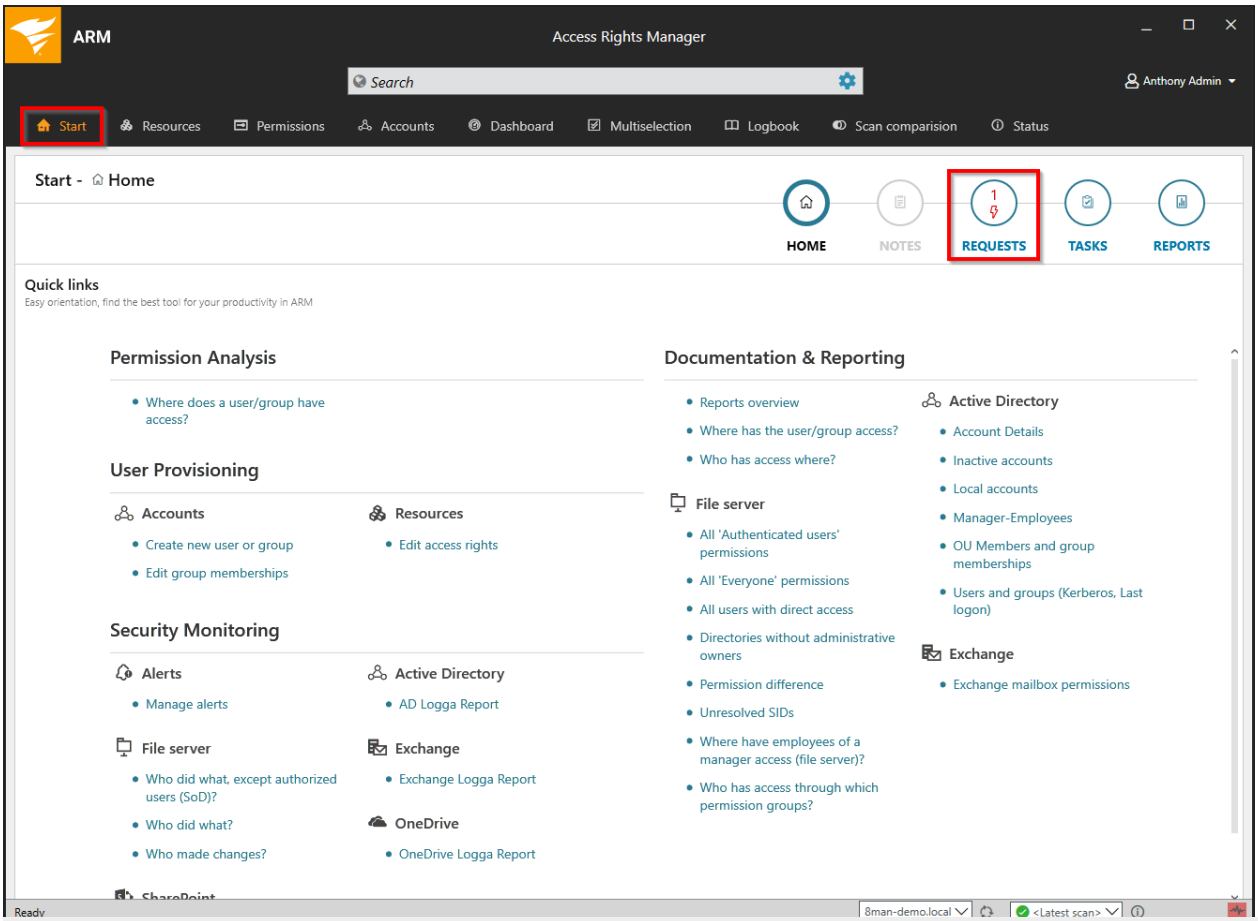
Step-by-step process



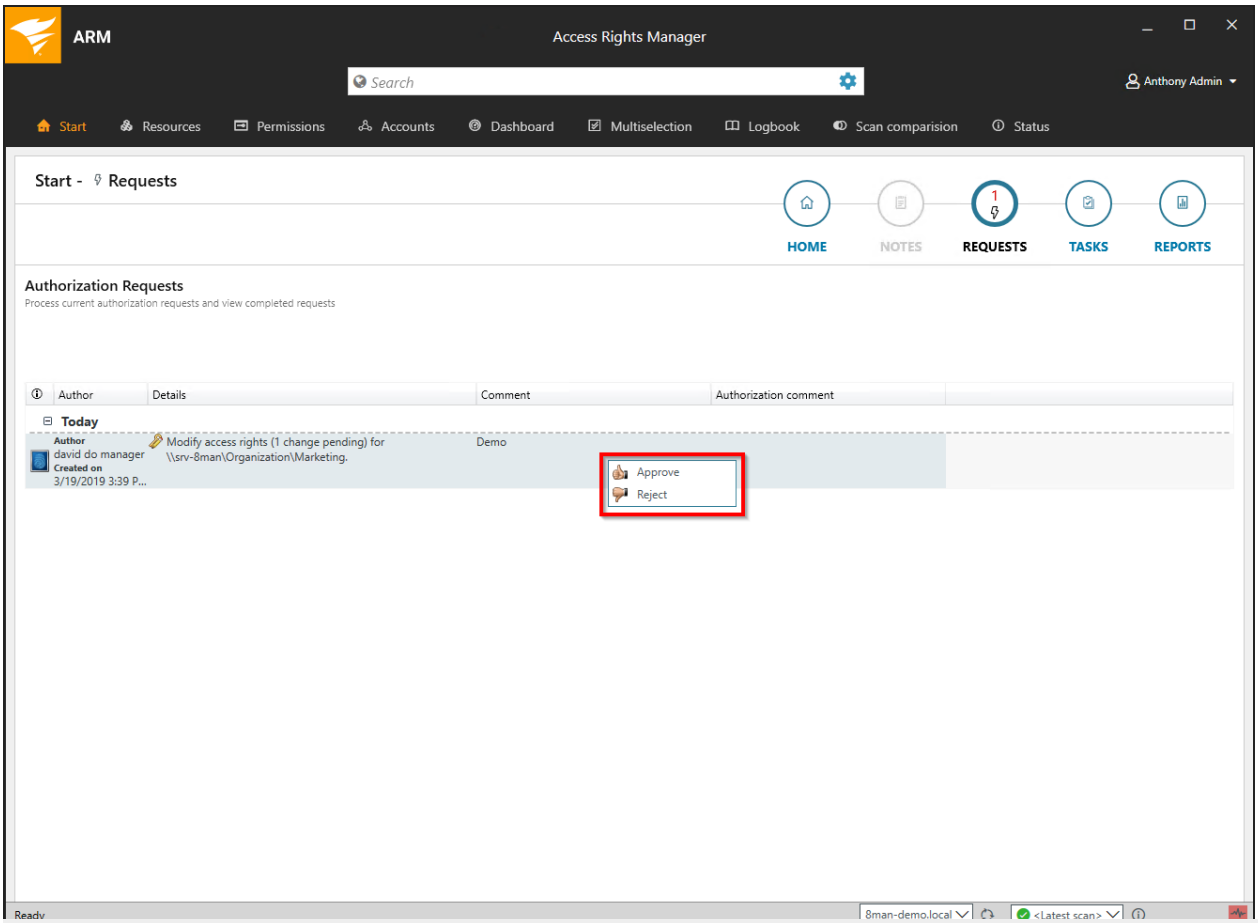
In the ARM configuration application select "Change Configuration">"Authorization".



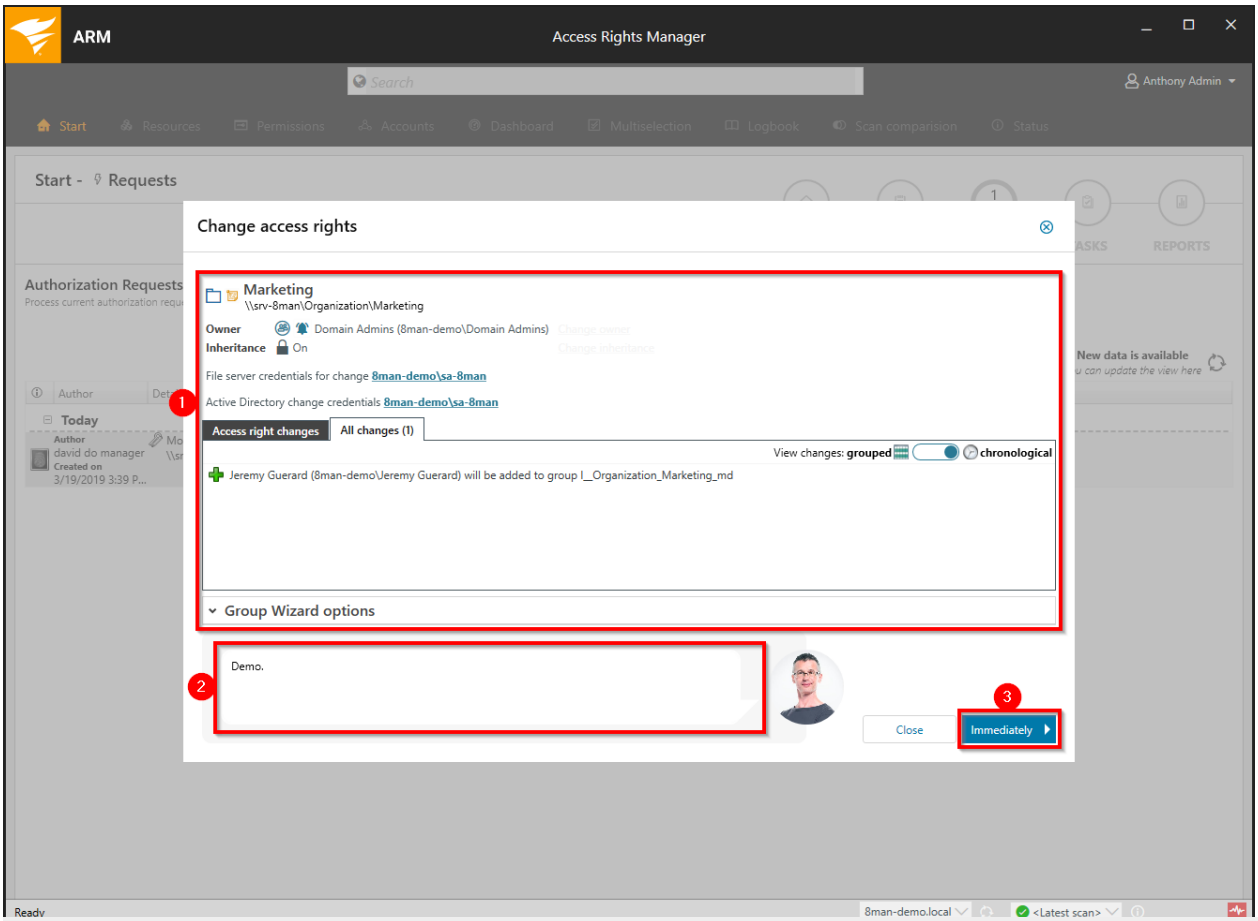
Activate the administrator approval mode.



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.

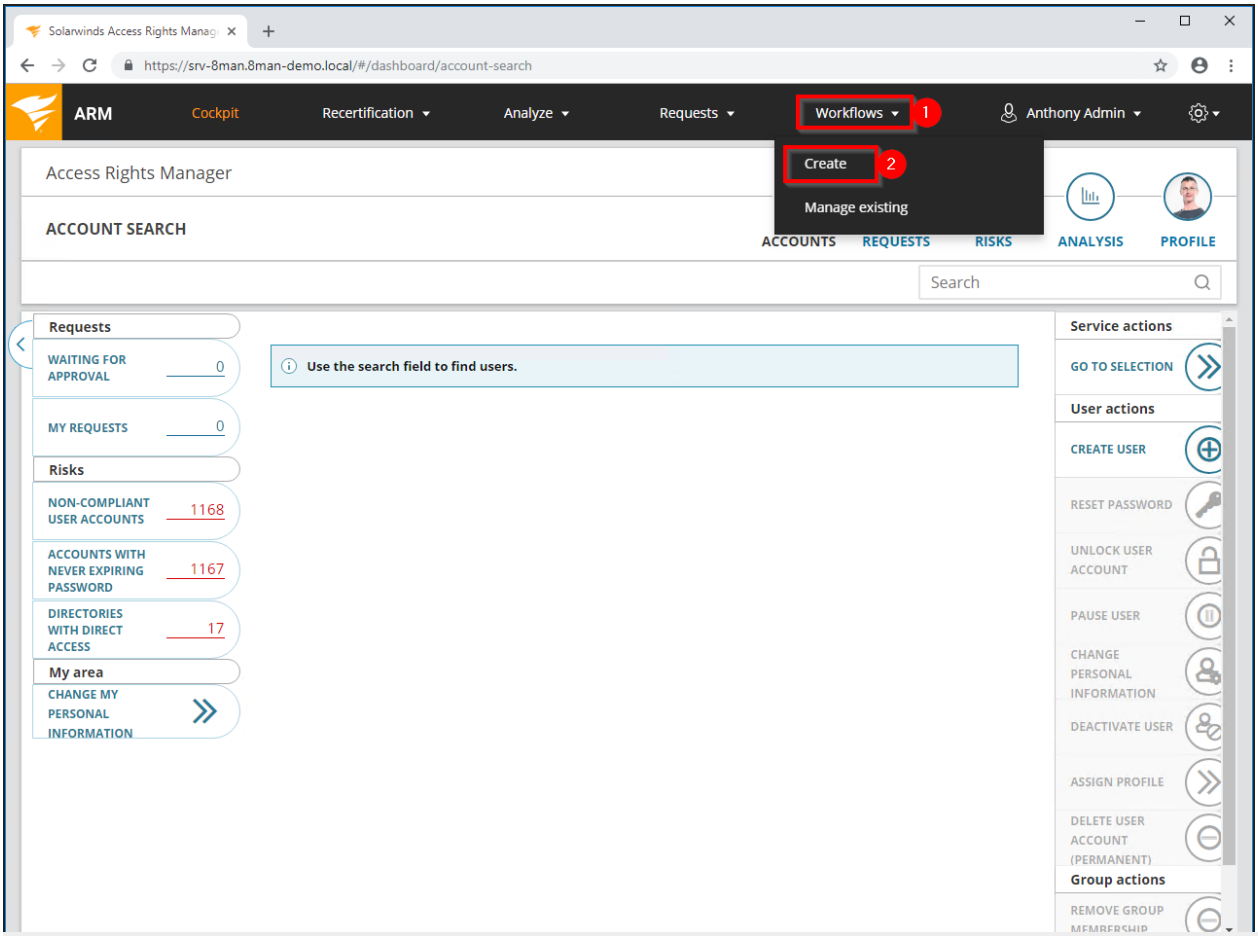
If more complex workflows with several decision-makers are required to grant access rights, you can also quickly map them.

Define individual approval flows

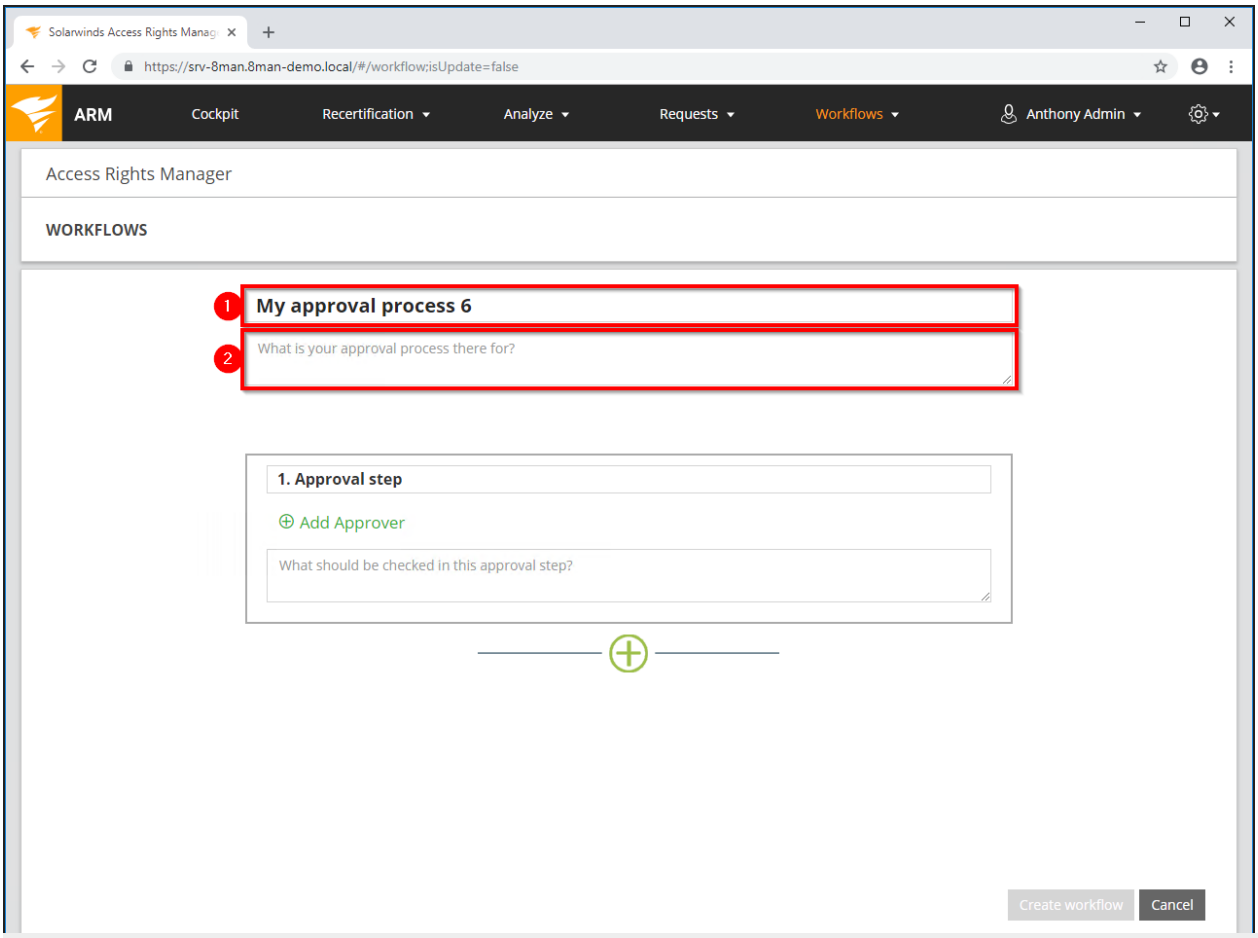
Background / Value

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.

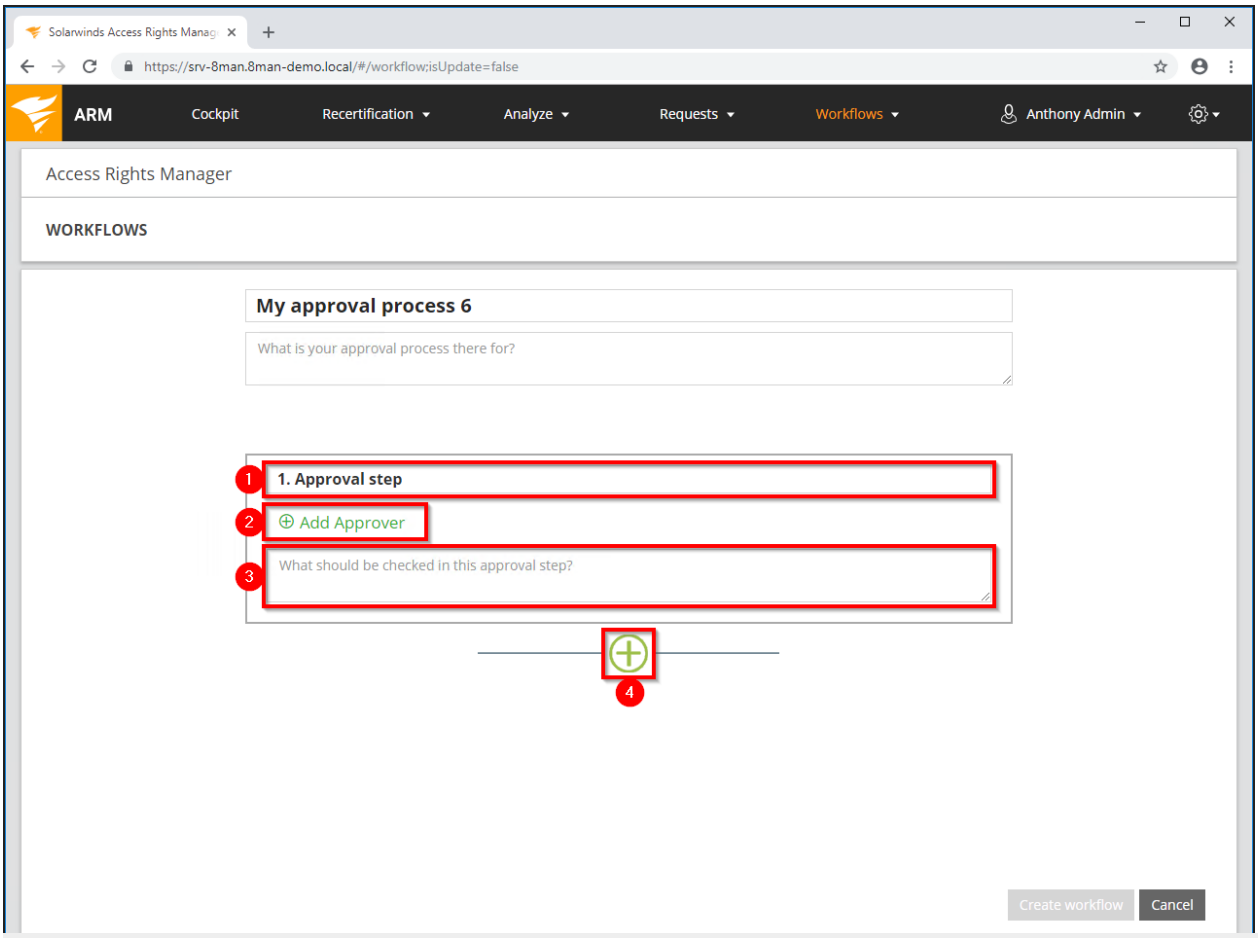
Step-by-step process



1. Select "Workflows".
2. Click on "Create".



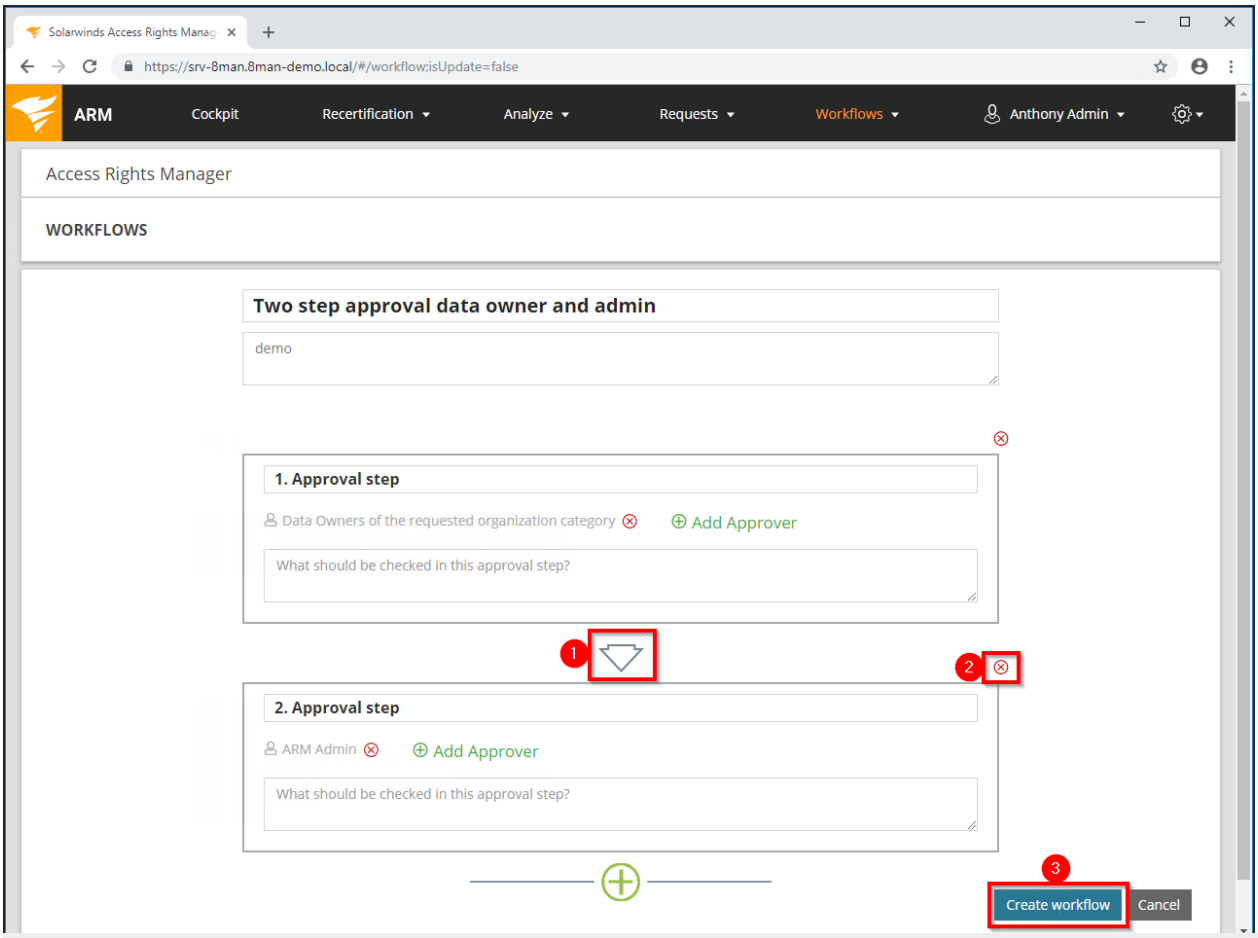
1. Give the workflow a title.
2. Give a short, concise description of the workflow s purpose.



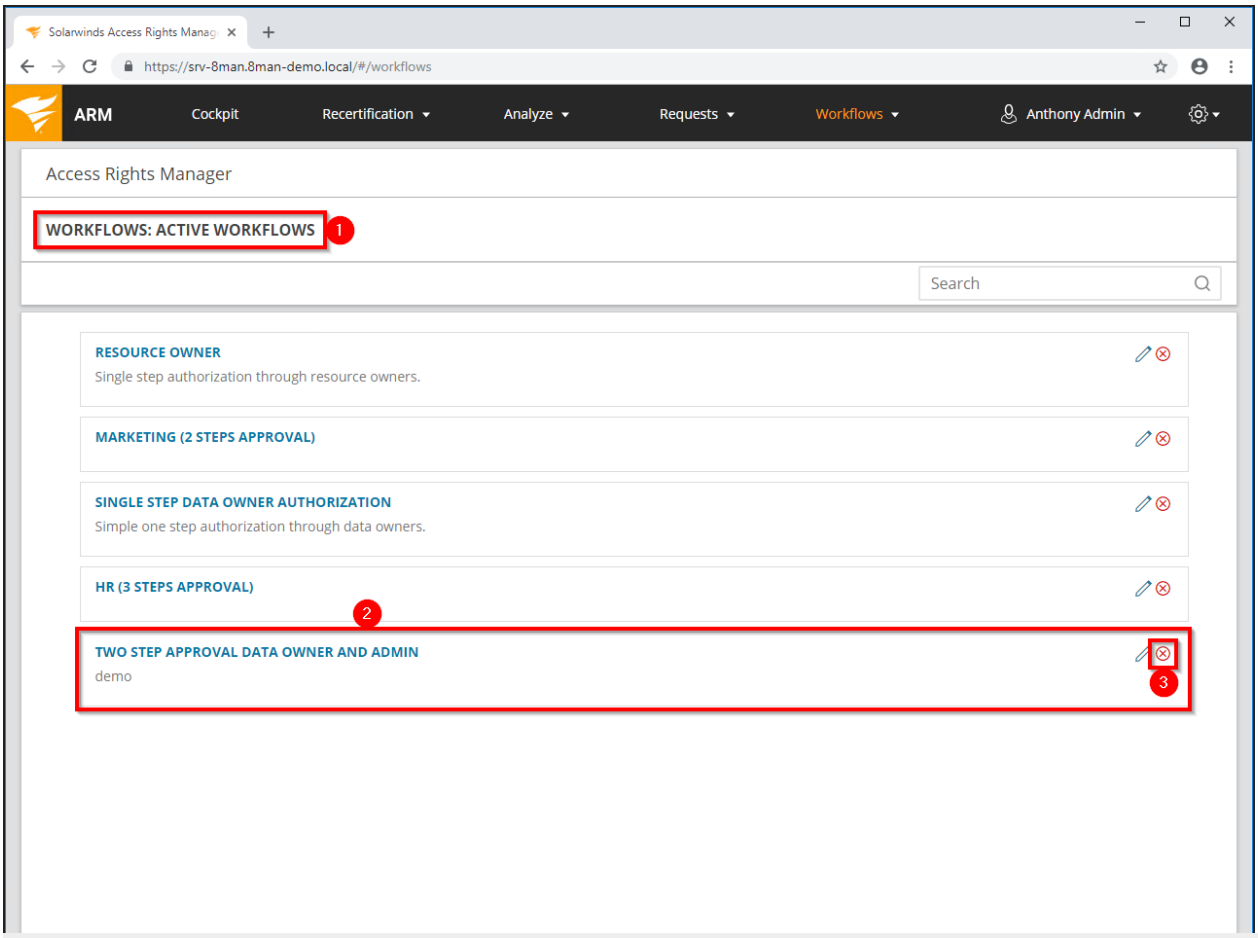
1. Name the approval step.
2. Add one or more approvers.

> 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.



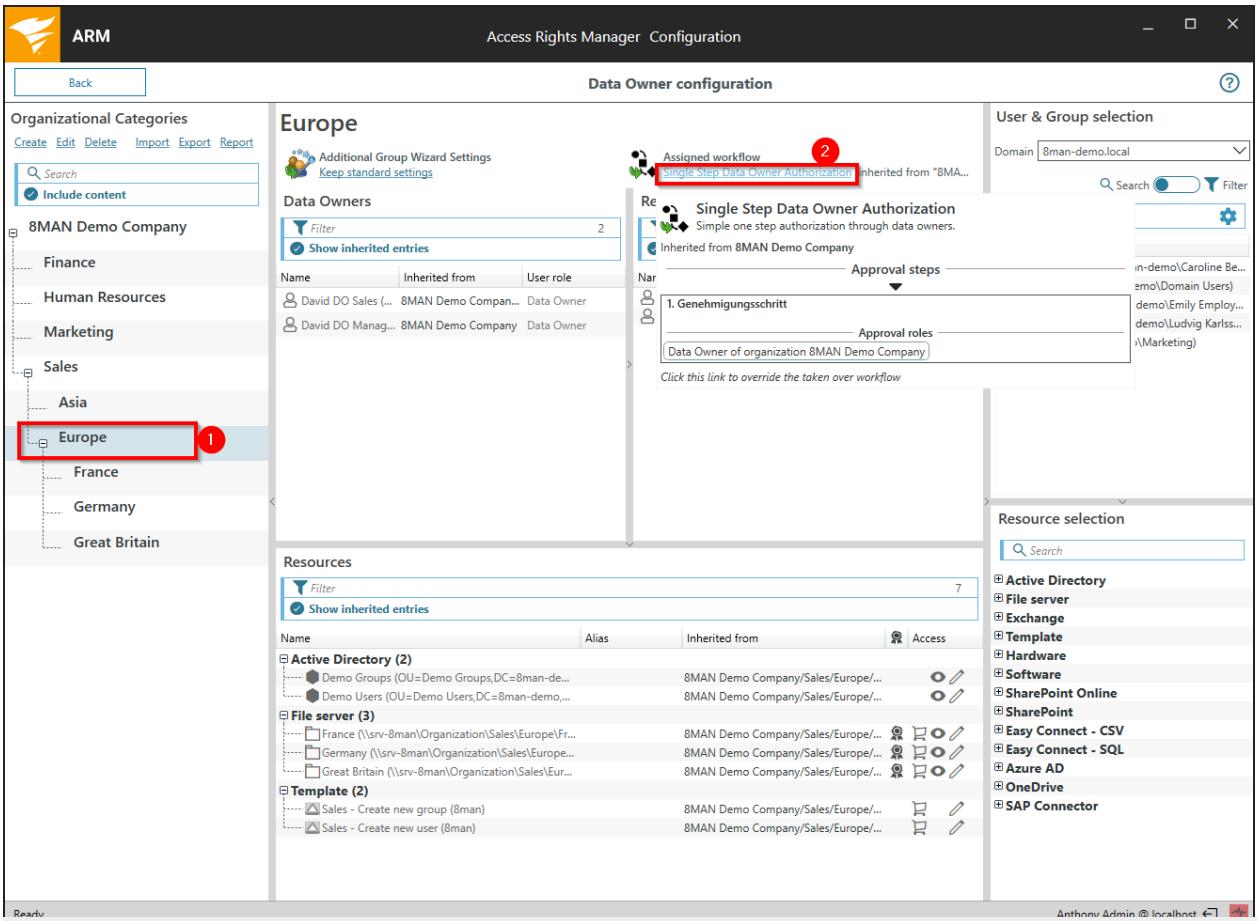
1. You have created a new workflow. ARM switches to the "Manage workflows" view.
2. Click on a workflow to make changes.
3. Delete the workflow.

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



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.

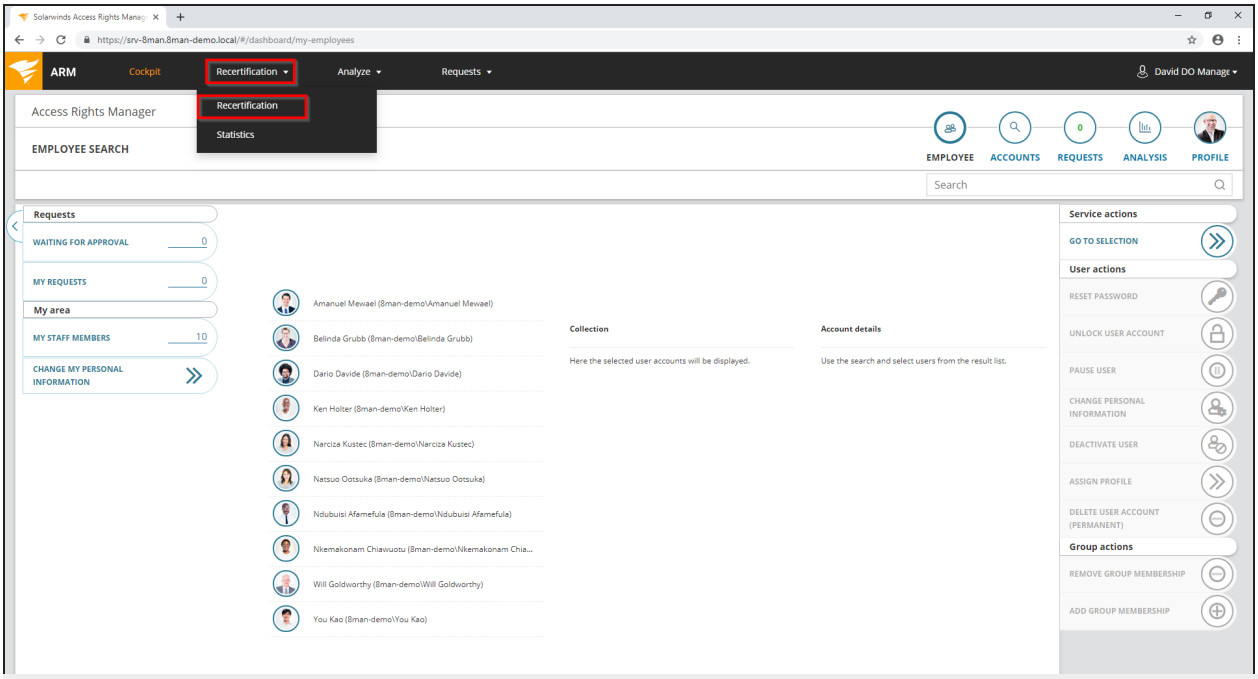
With the re-certification process you obtain the possibility to check and change the access rights situation to your resources.

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.

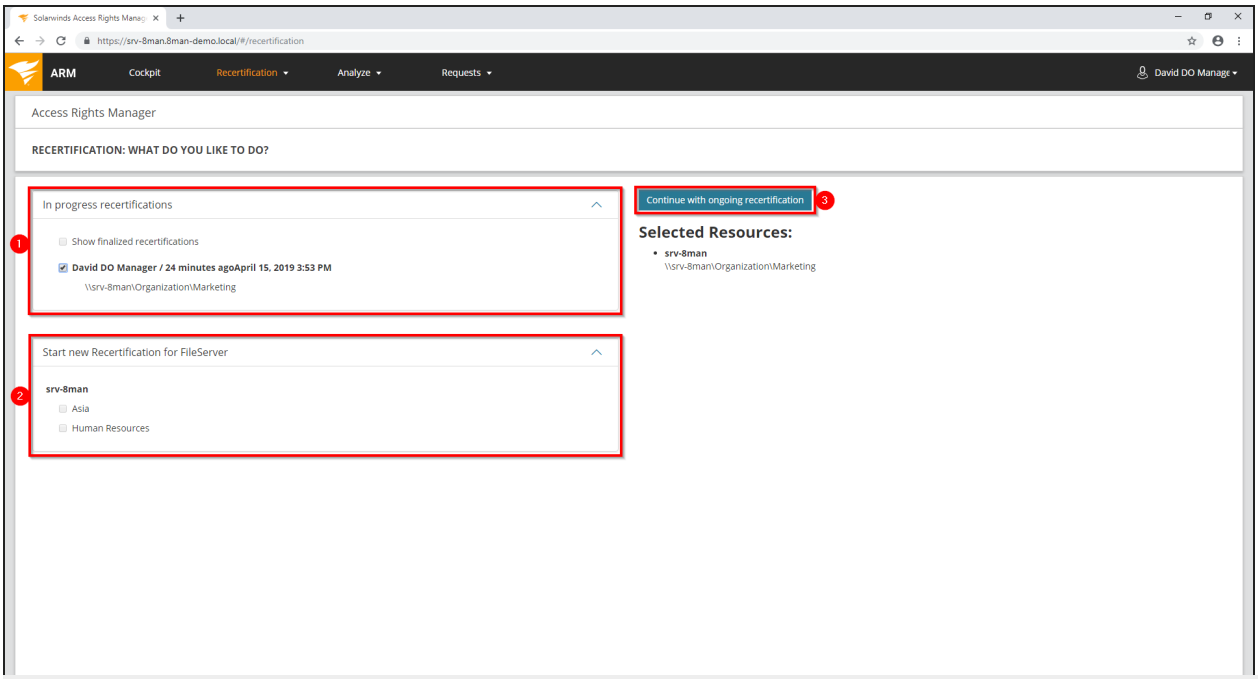
Complementary Services

Grant and remove file server access rights

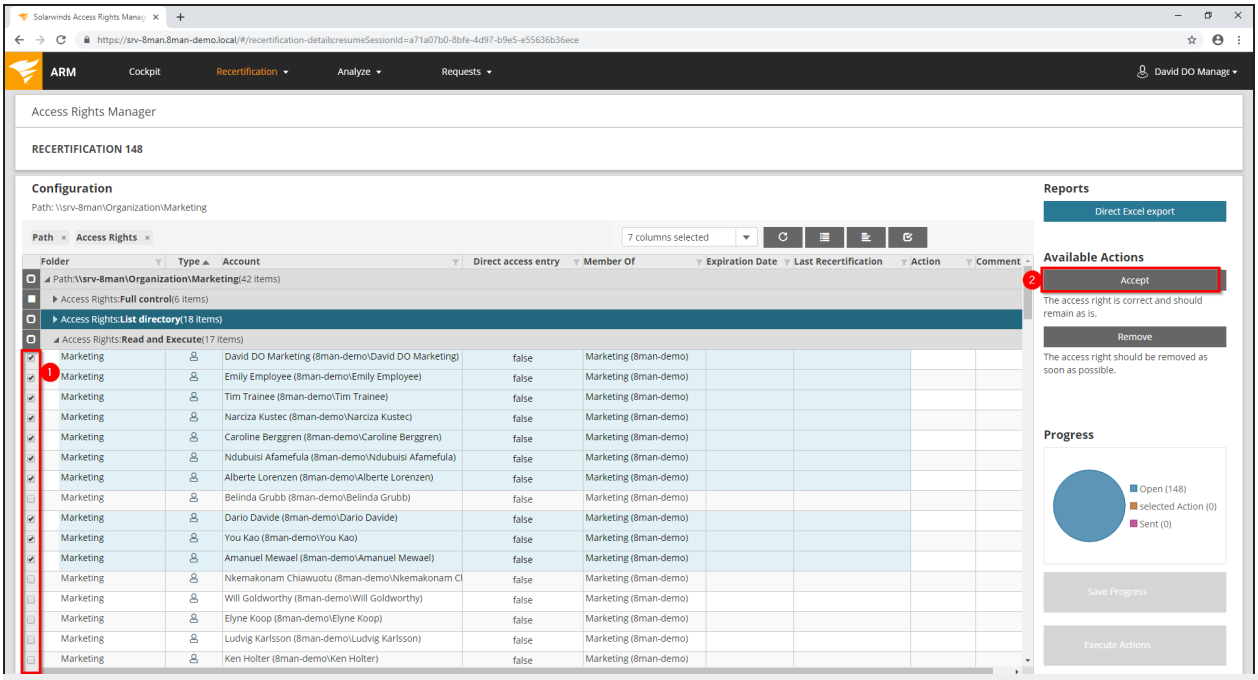
Step-by-step process



Click "Recertification".



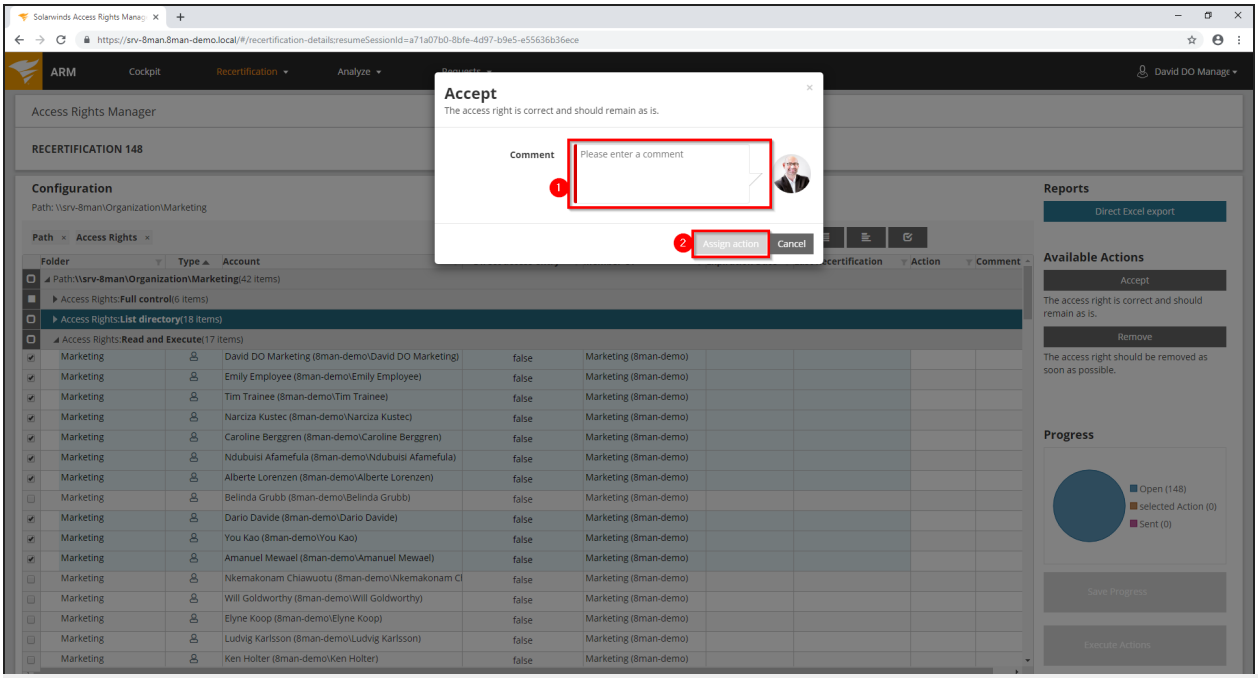
1. Continue a recertification already started.
2. Select resources for a new recertification.
3. Start the process.



You can either accept or remove the permissions.

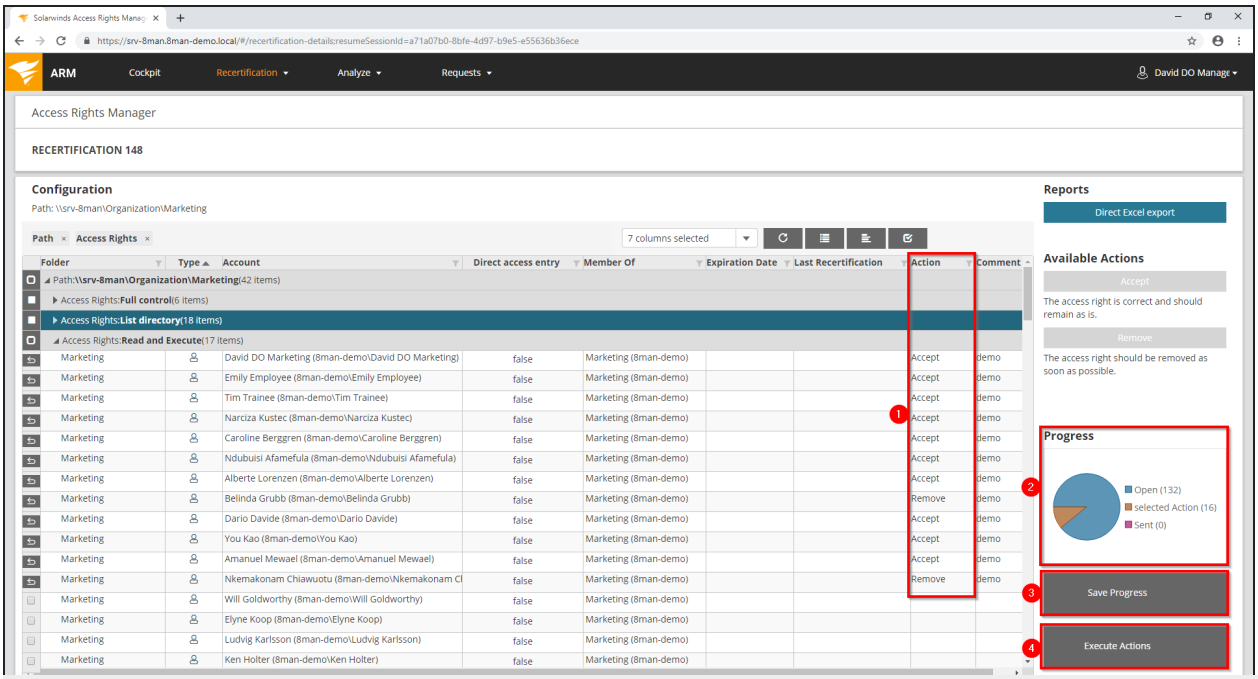
1. Activate all Users which should keep their permissions first.
2. Click on "Accept".

Subdirectories are only displayed, if they contain deviating permissions.



1. You must enter a comment. Your notes will be saved in the system for documentation.
2. Click "Assign action".

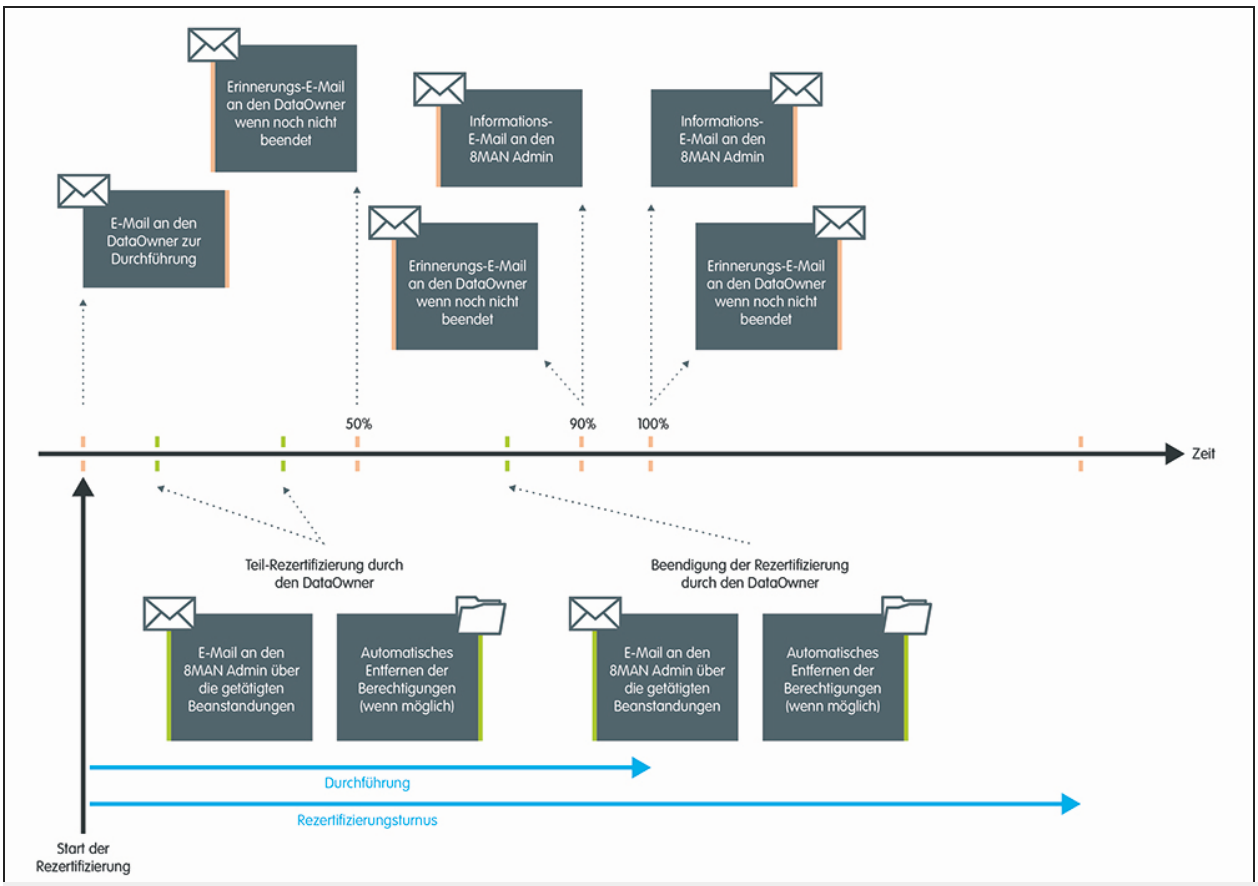
Repeat the process for the permissions you want to remove.



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.

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.

Notification emails can be customized by an administrator.

ARM GrantMA: workflows for employees

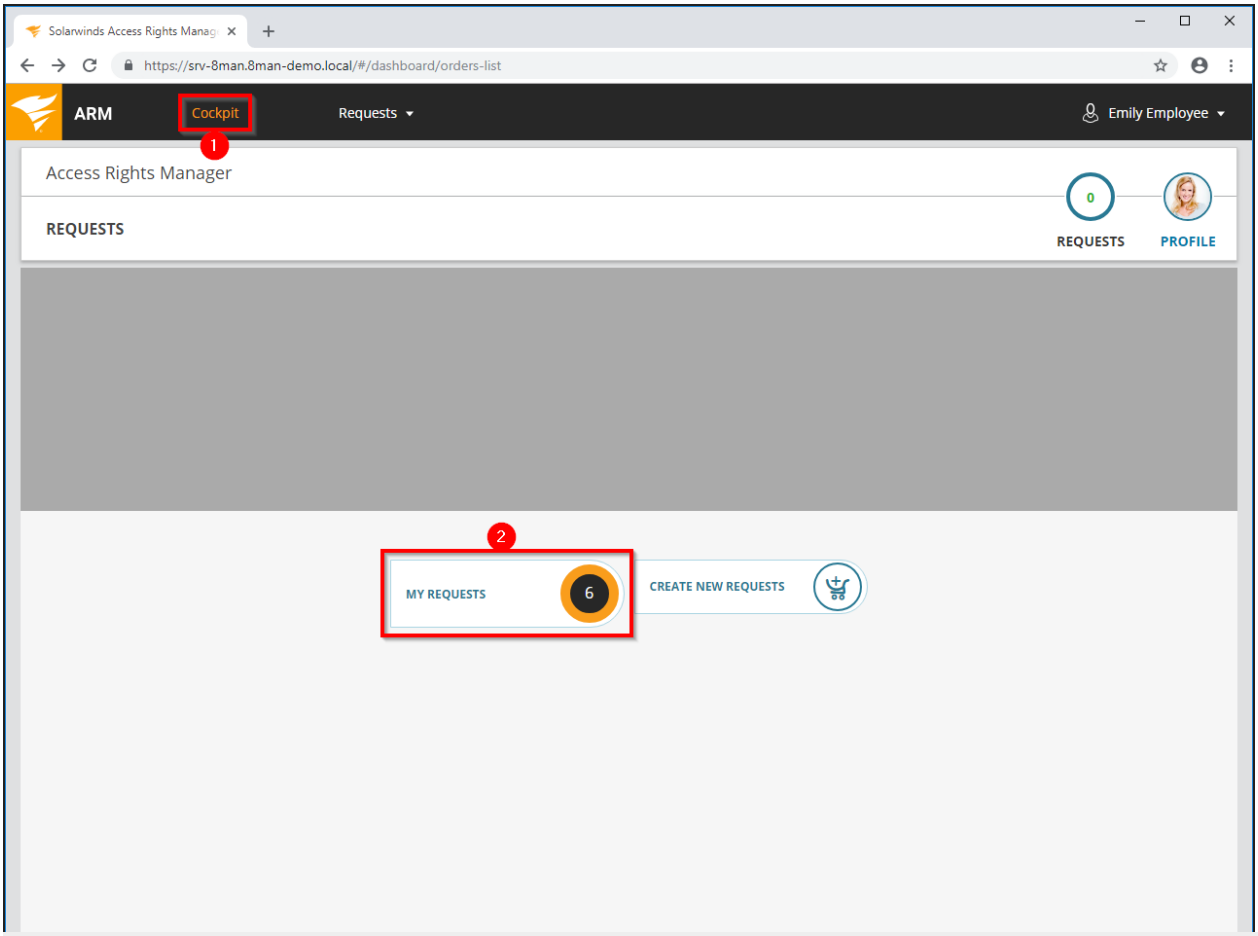
By using the ARM GrantMA self-service portal, employees are able to request access to individual resources in your organization. The next few pages contain examples of some common workflows.

Manage my requests (cockpit)

Background / Value

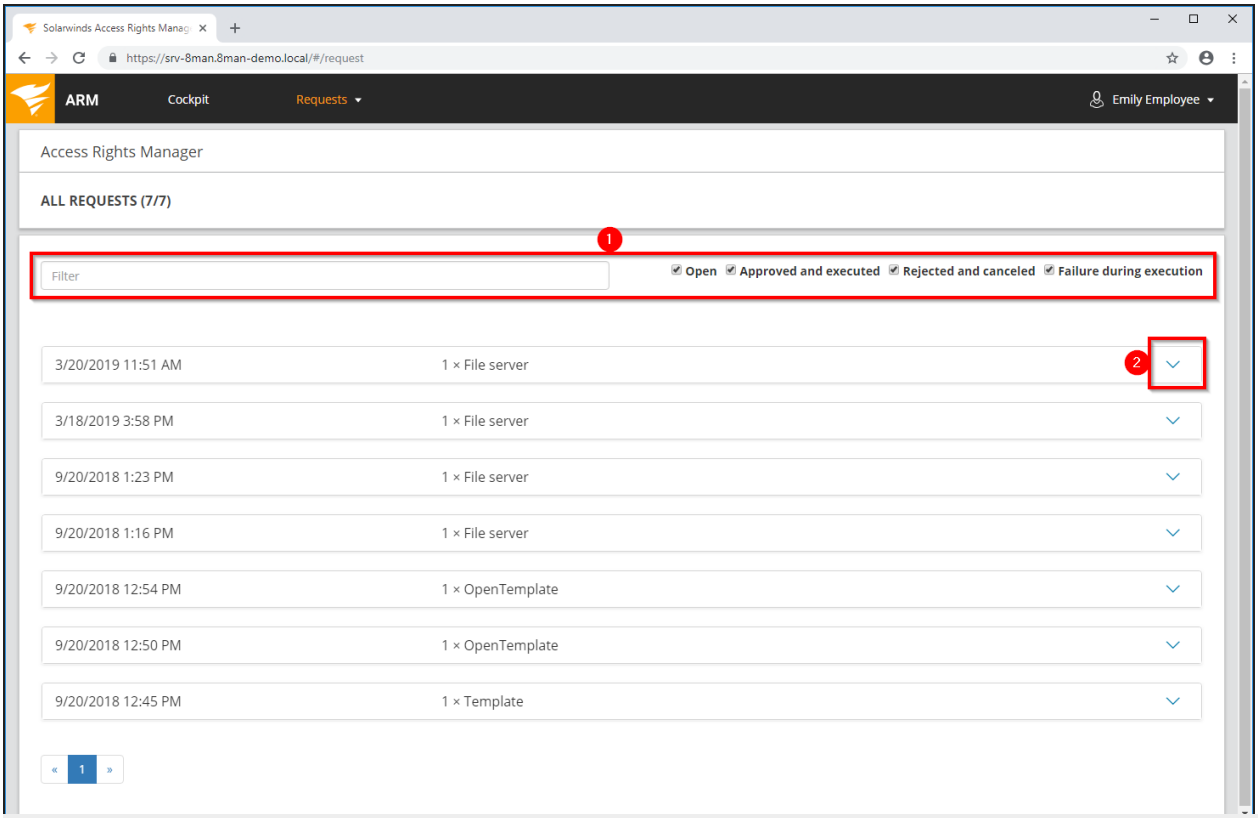
Keep track of your orders. Cancel orders or resend notifications to the approver.

Step-by-step process

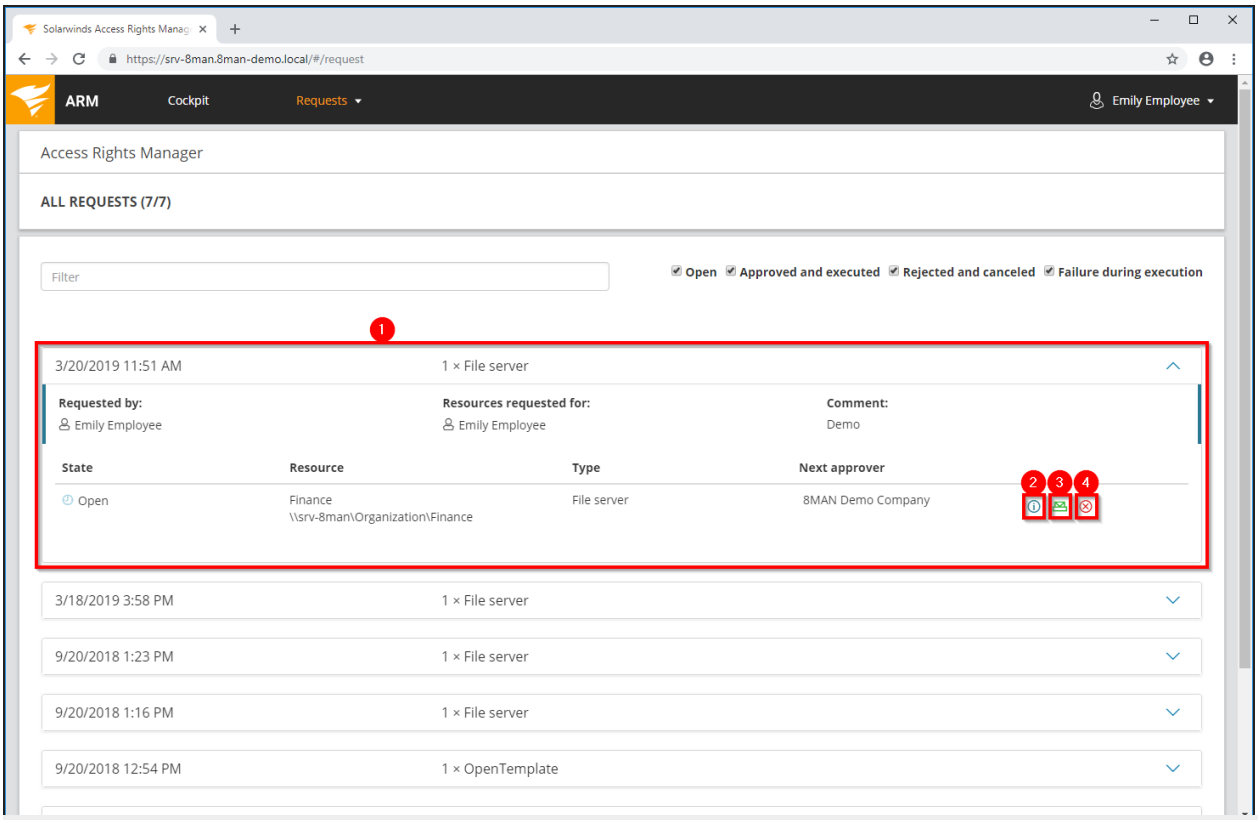


1. Select Cockpit.
2. Click "My Requests".

The range of available services (buttons) varies according to role (login), risk assessment and configuration.



1. Filter your requests to quickly find the right one in case of many entries.
2. Expand the desired request.



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.

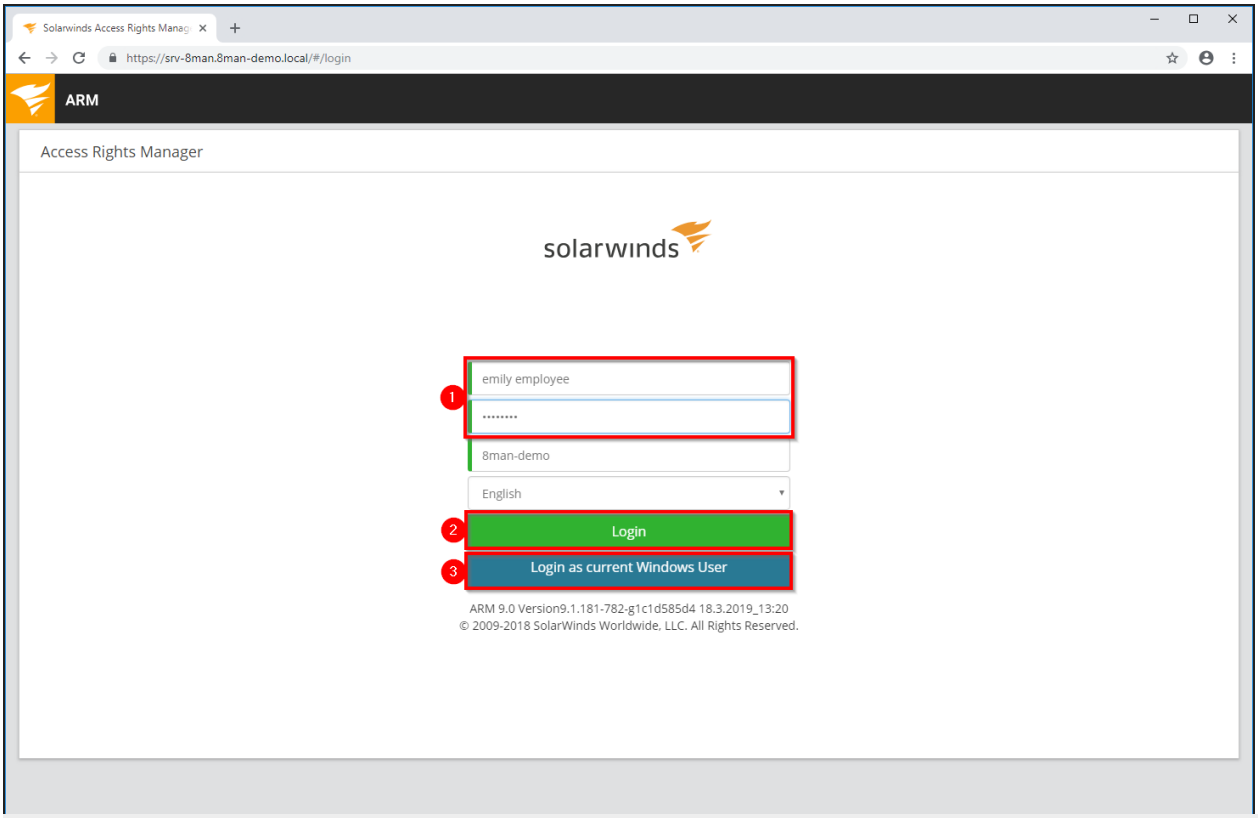
You can configure a variety of different processes and involve the relevant decision makers, depending on your security requirements.

Related features

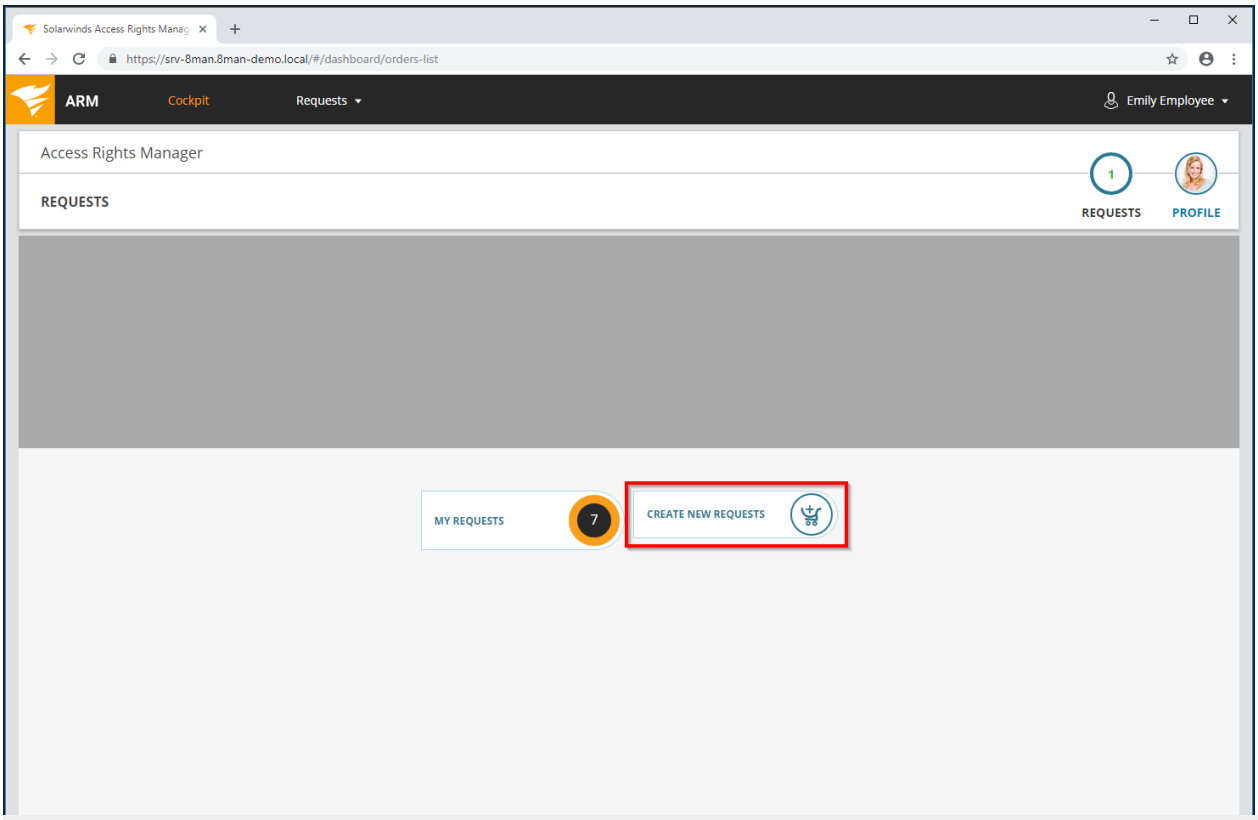
Manage my requests

GrantMA: Design approval processes (administrator)

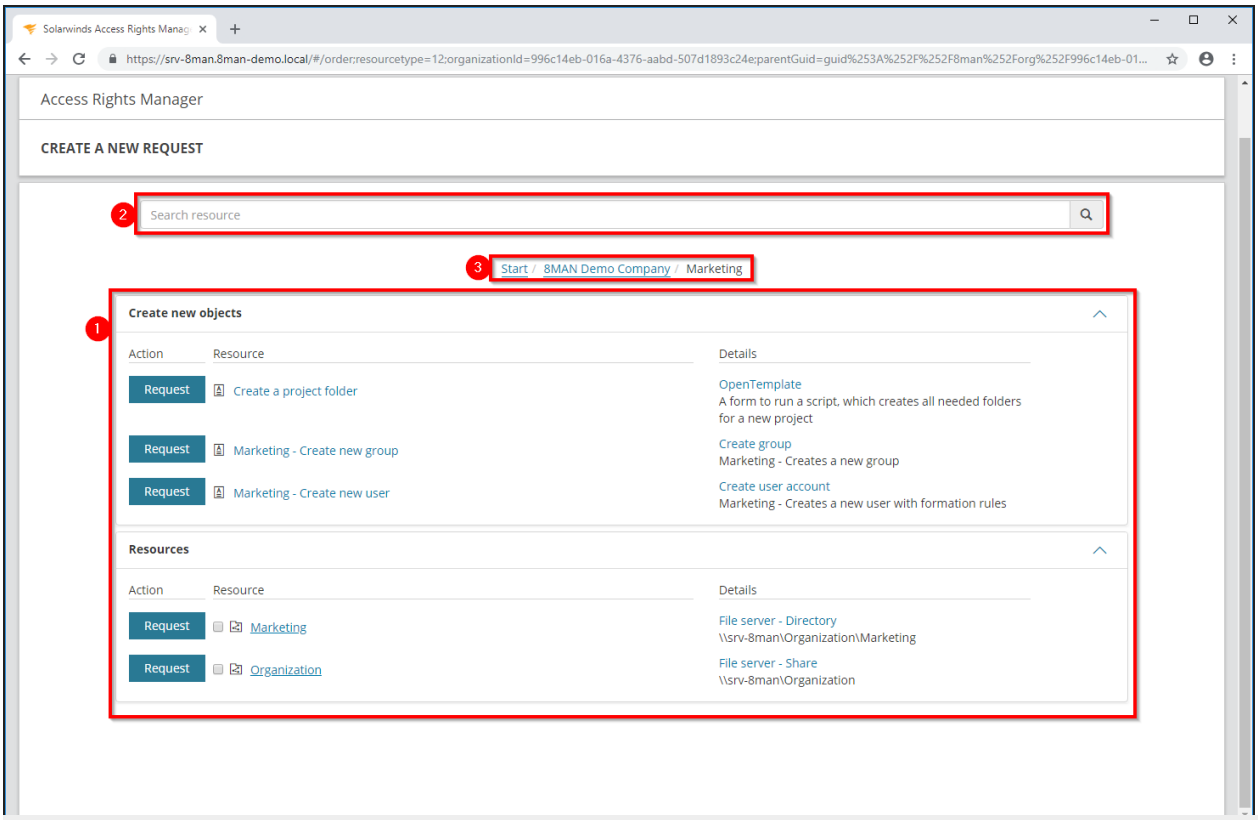
Step-by-step process



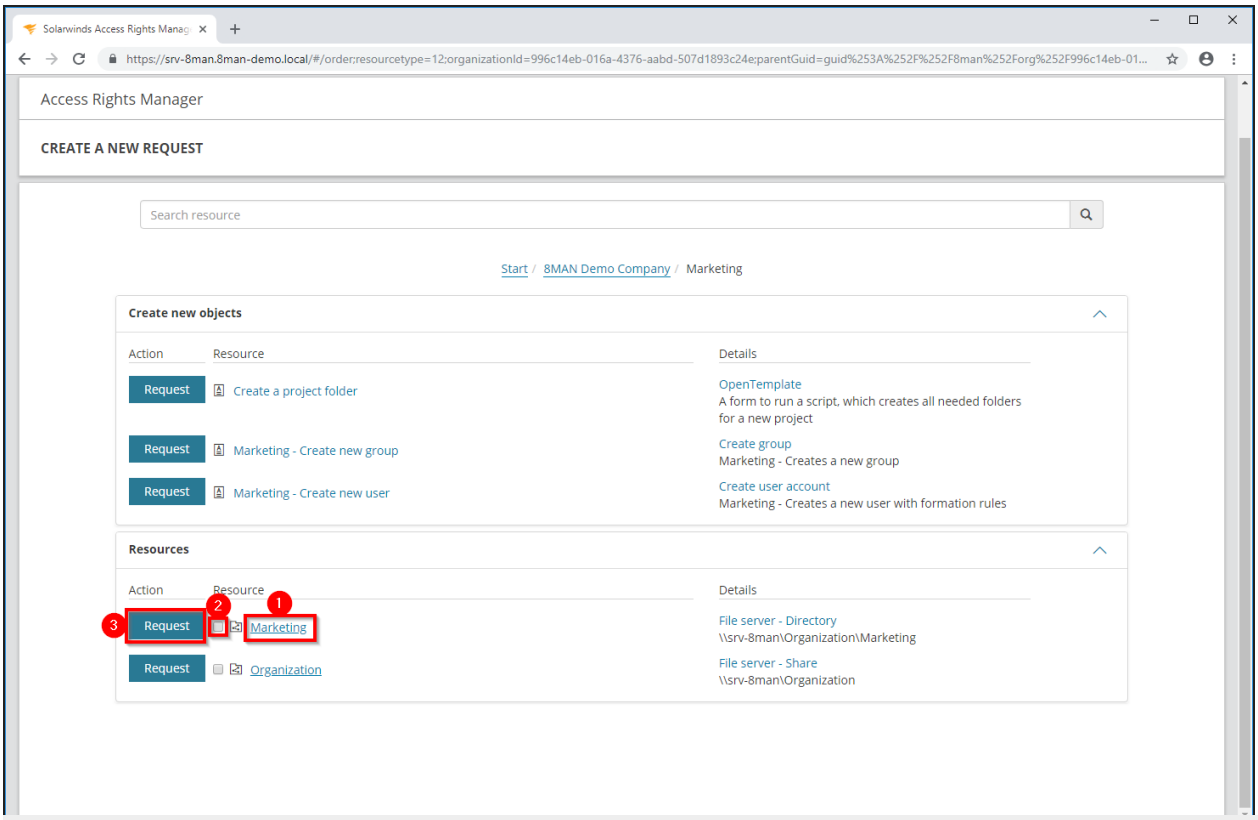
1. Enter your user name and password.
2. Click "Login".
3. You can alternatively login as the current windows user (no user name and password required).



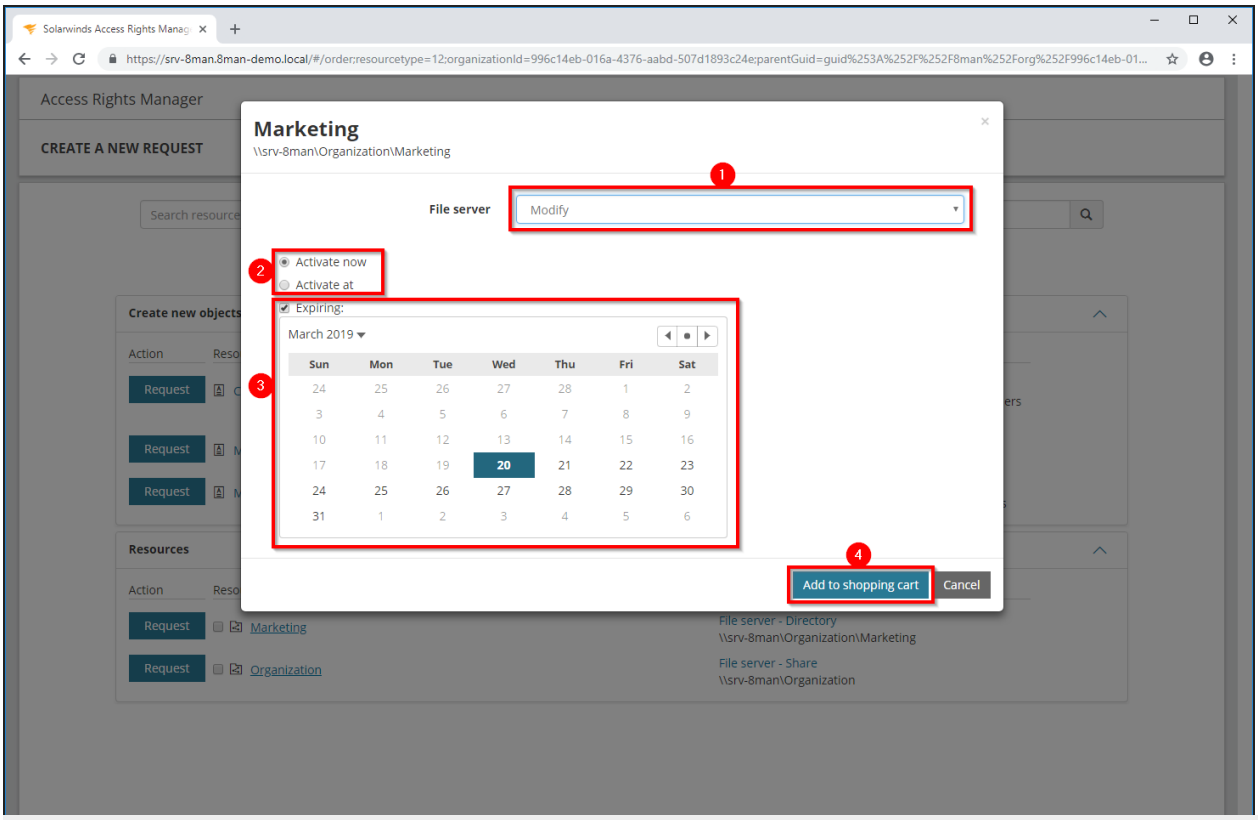
Click "Create new request".



1. 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.



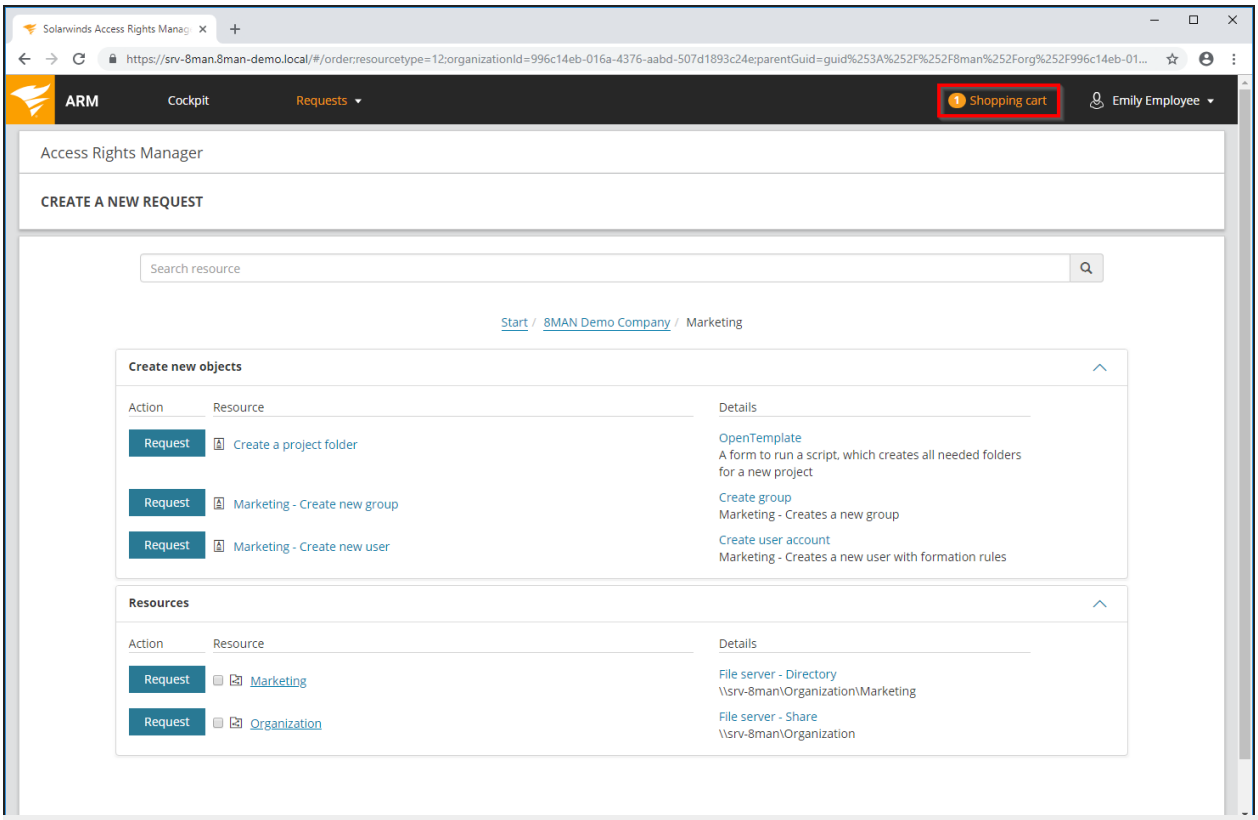
1. Click on a link to drill down further.
2. Check the box if you want to request access to more than one folder.
3. Click "Request".



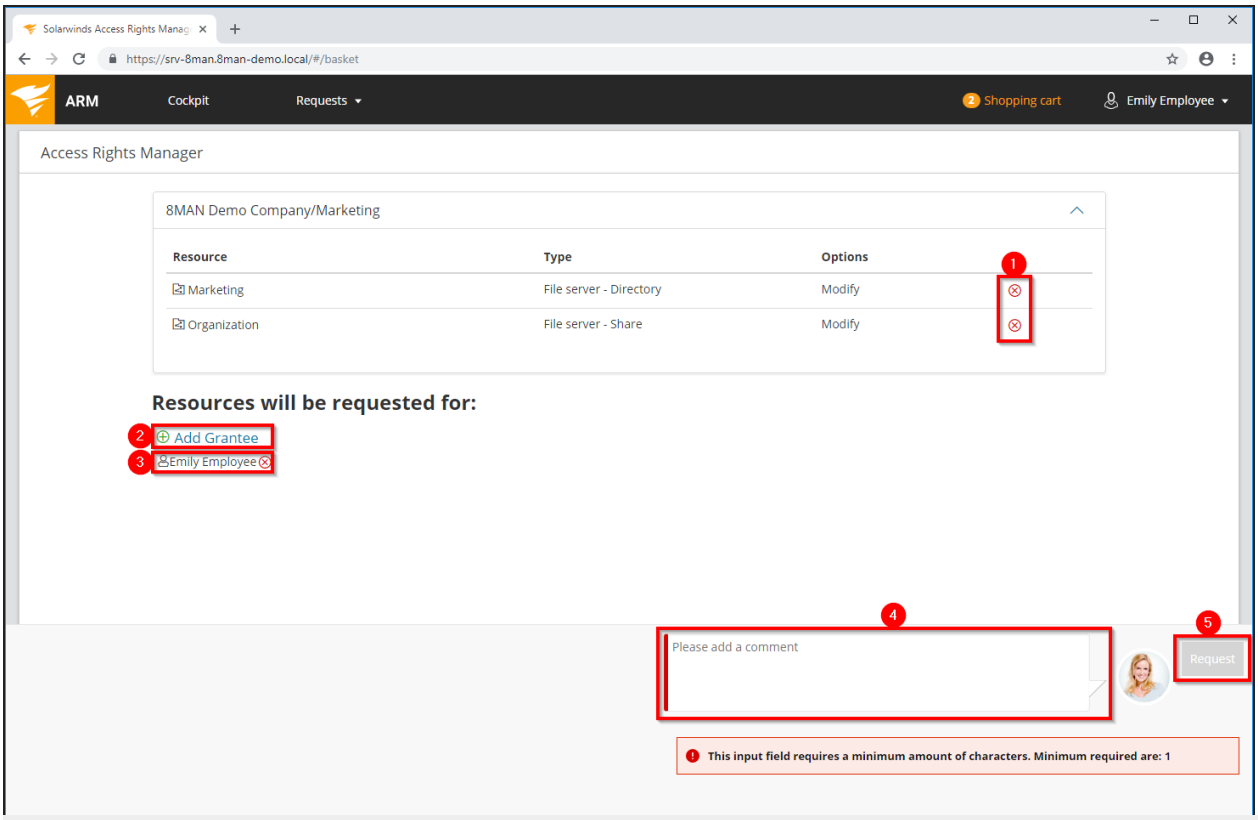
1. Select the desired kind of access.
2. Set an activation date.
3. Optional: Set an expiration date.

Depending on your ARM configuration the approver may be able to modify the request.

4. Click "Add to shopping cart".



Click "Shopping cart".



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.

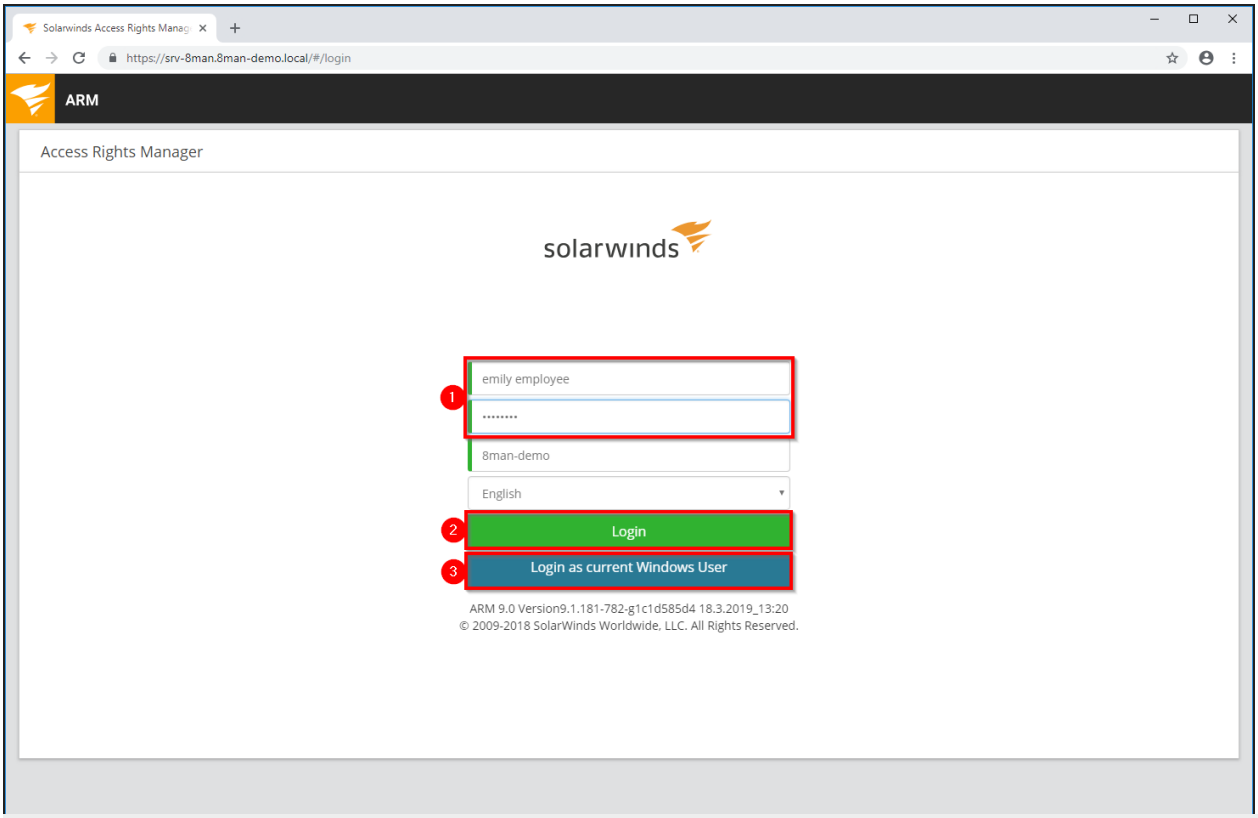
You can configure a variety of approval flows and involve the relevant decision makers, depending on your security requirements.

Related features

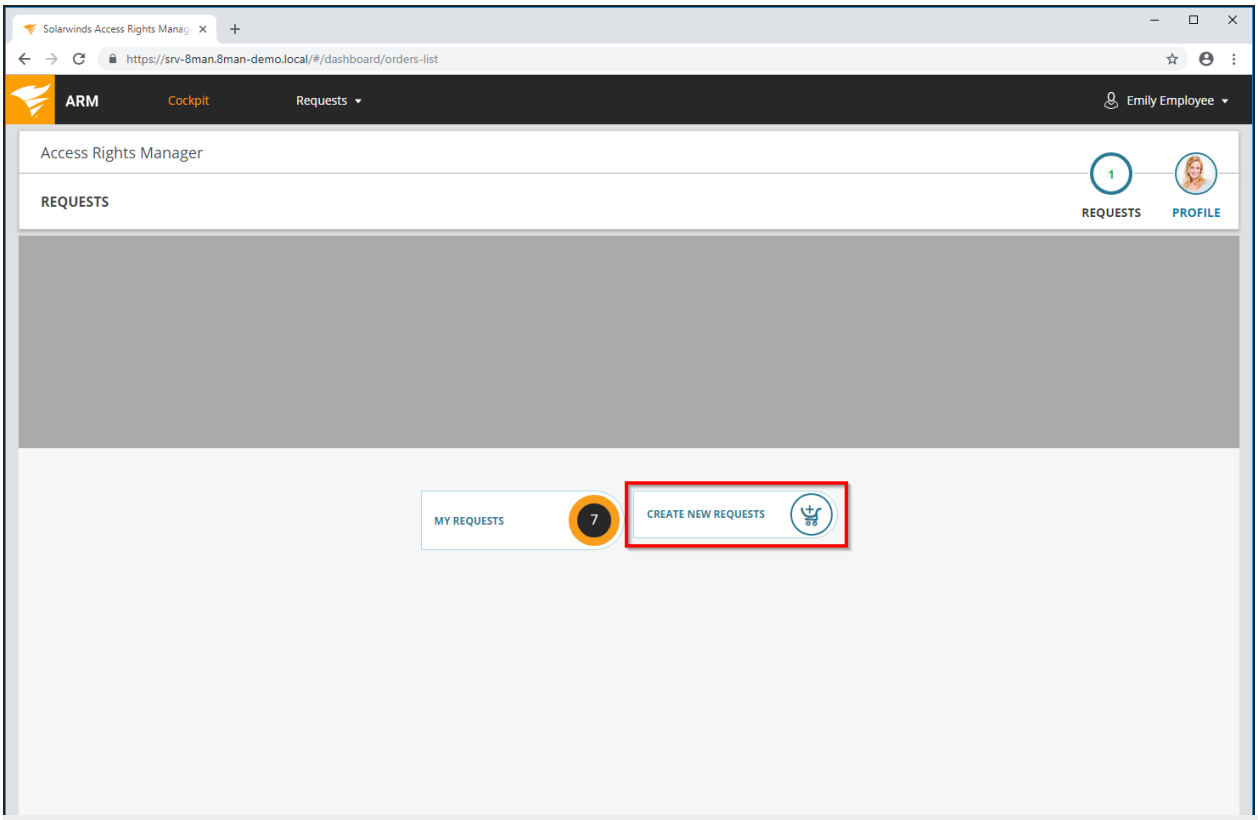
Manage my requests

GrantMA: Design approval processes (administrator)

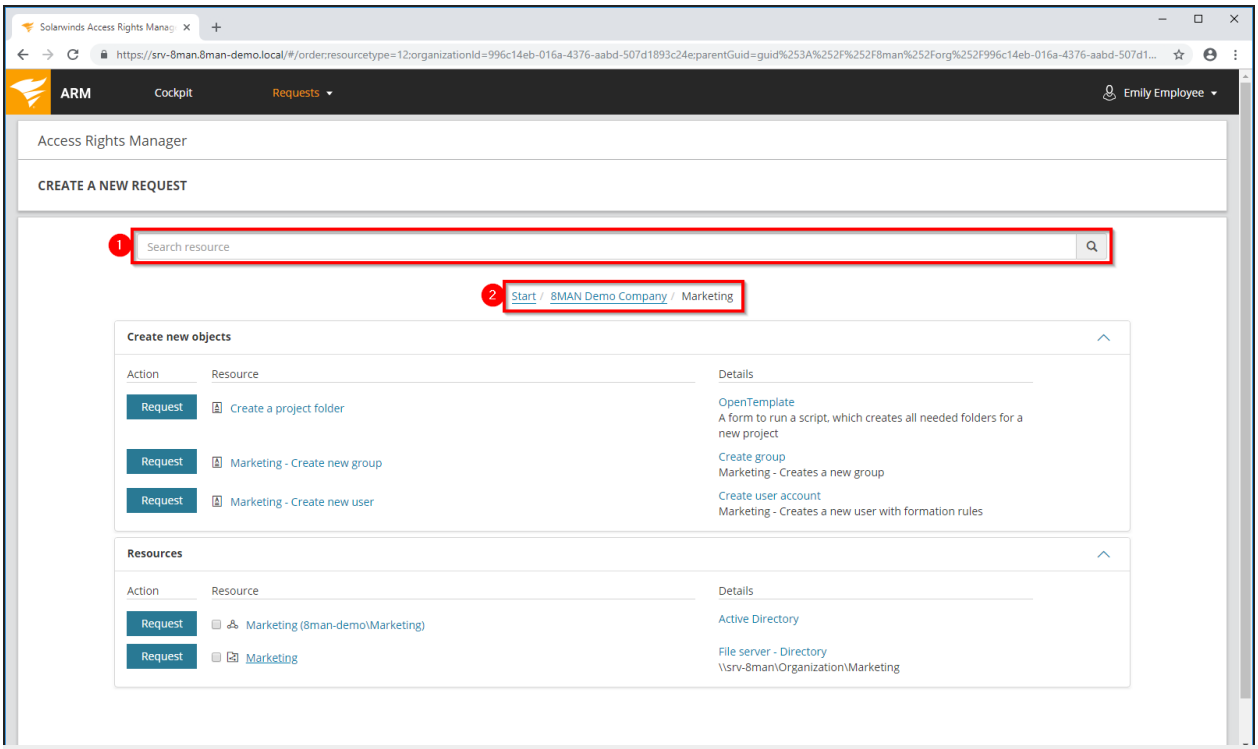
Step-by-step process



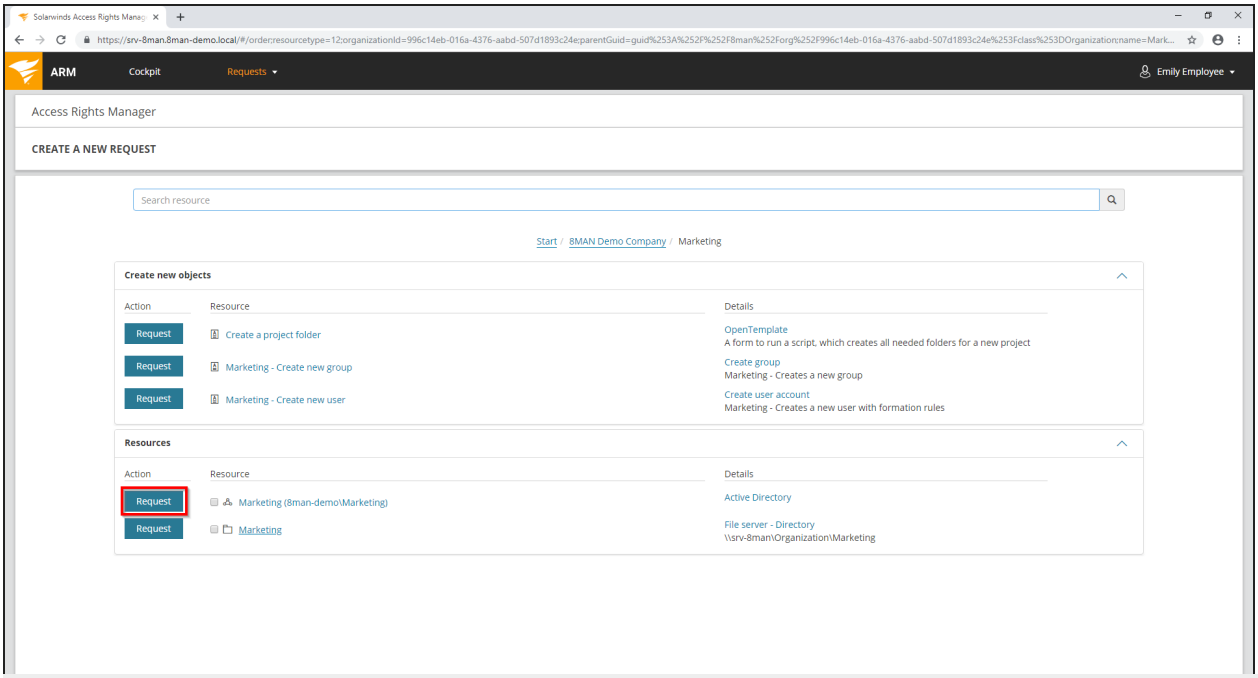
1. Enter your user name and password.
2. Click "Login".
3. You can alternatively login as the current windows user (no user name and password required).



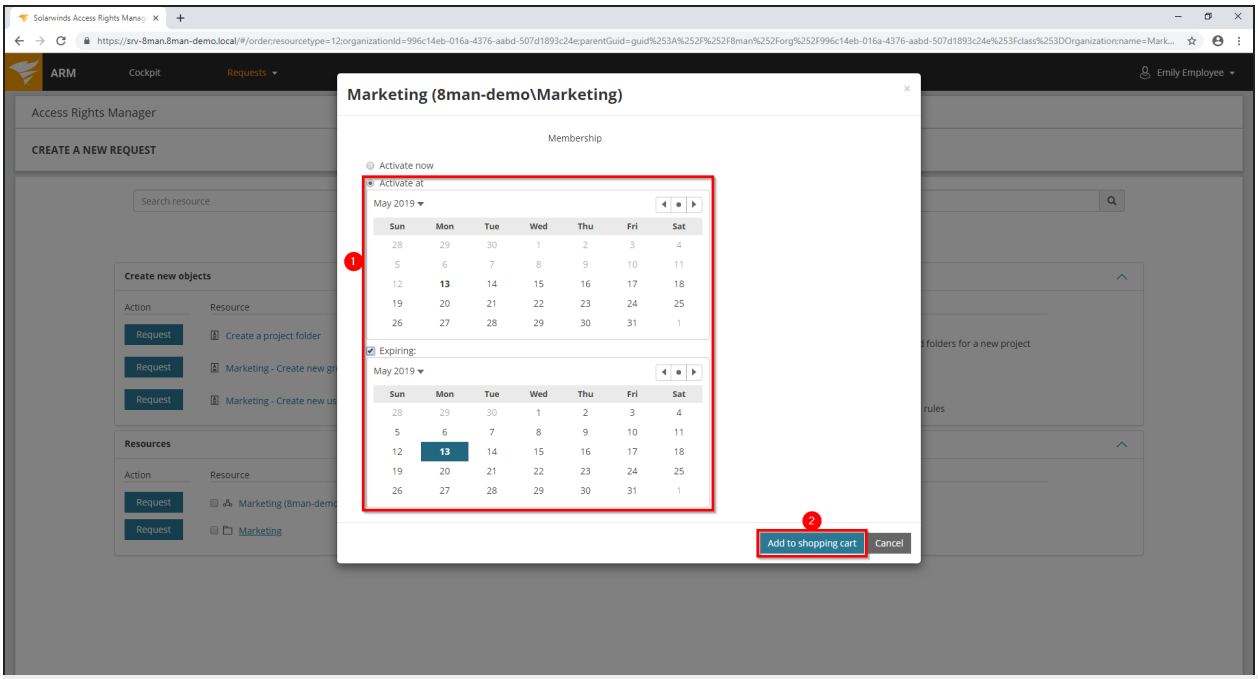
Click "Create new request".



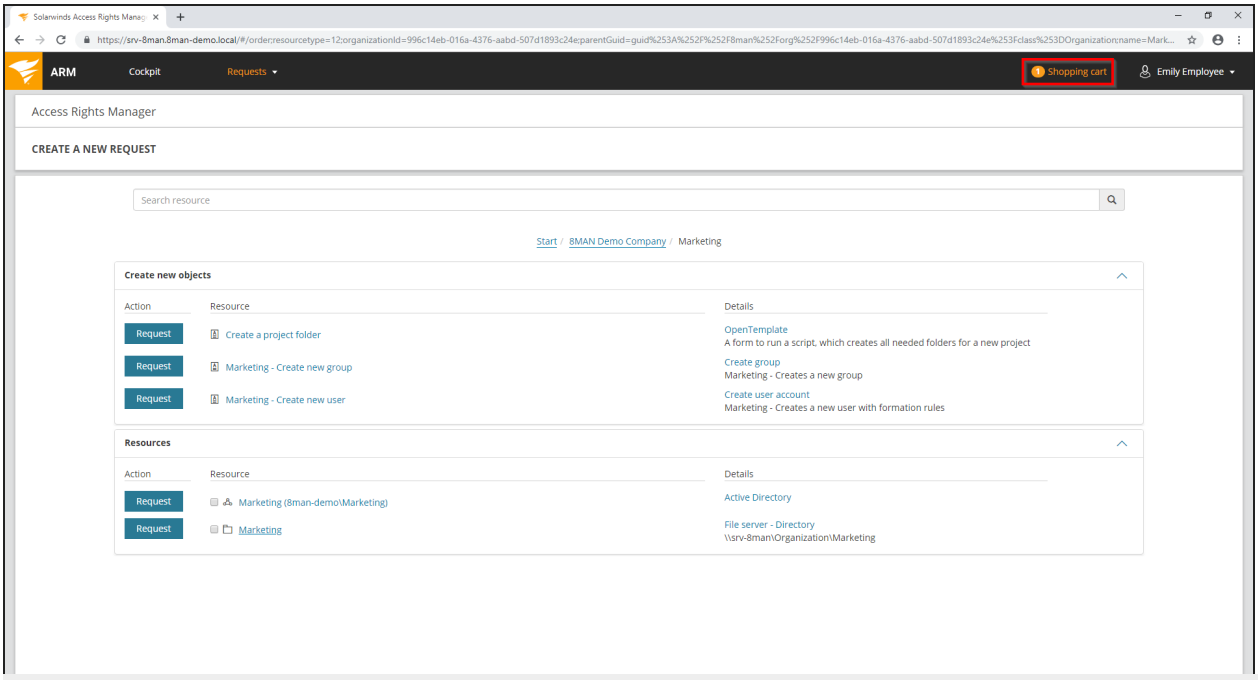
1. Search for the group or
2. navigate to the desired level.



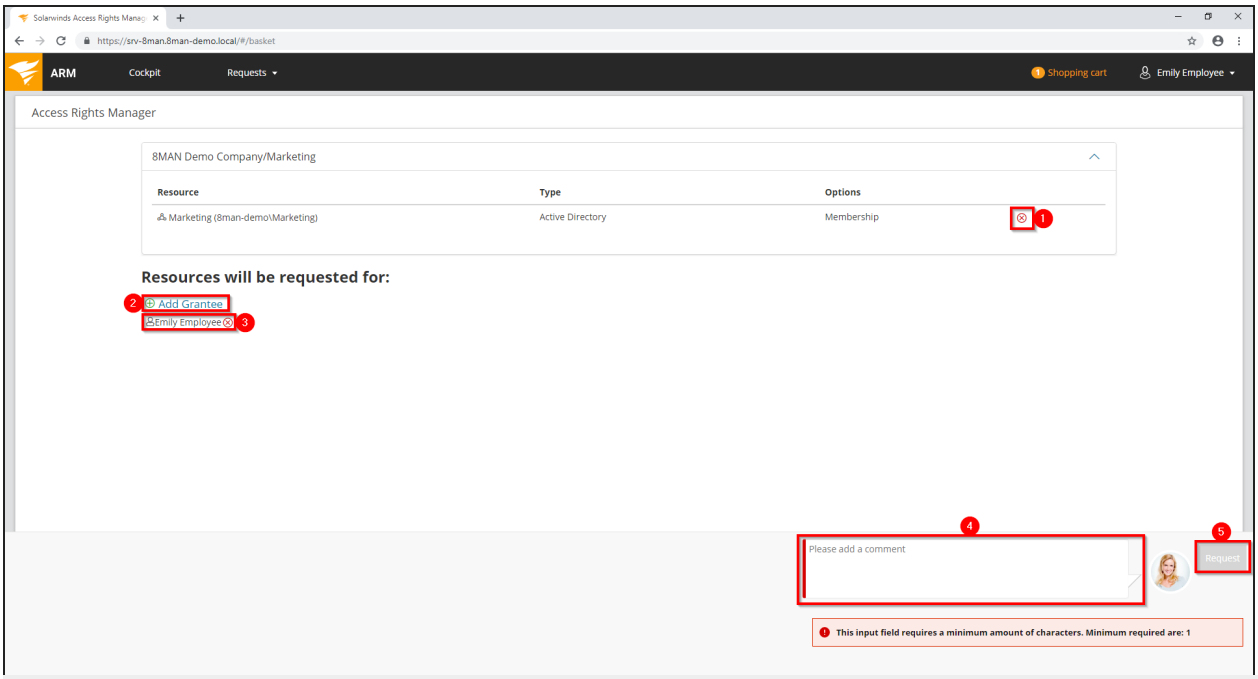
Once you have found the desired group, click "Request".



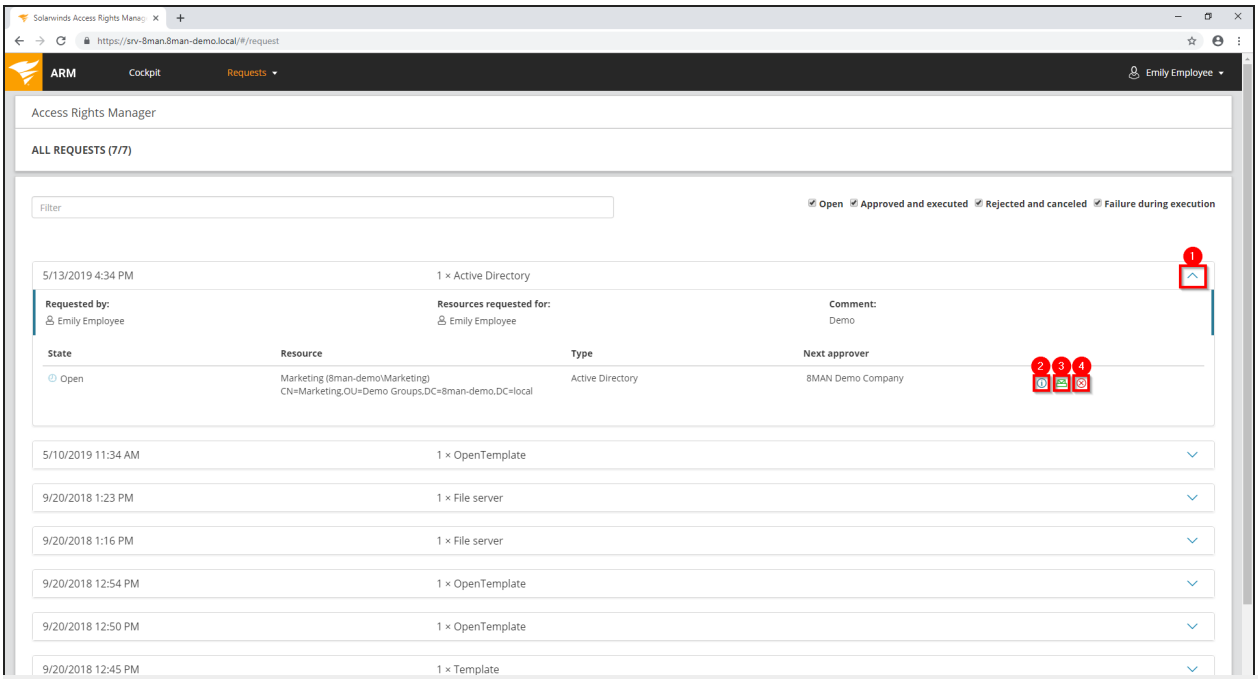
1. Optional:
   You can set an activation and an expiration date.
2. Click "Add to shopping cart".



If desired, add additional resources to your request. When ready, click "Shopping cart".



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.



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

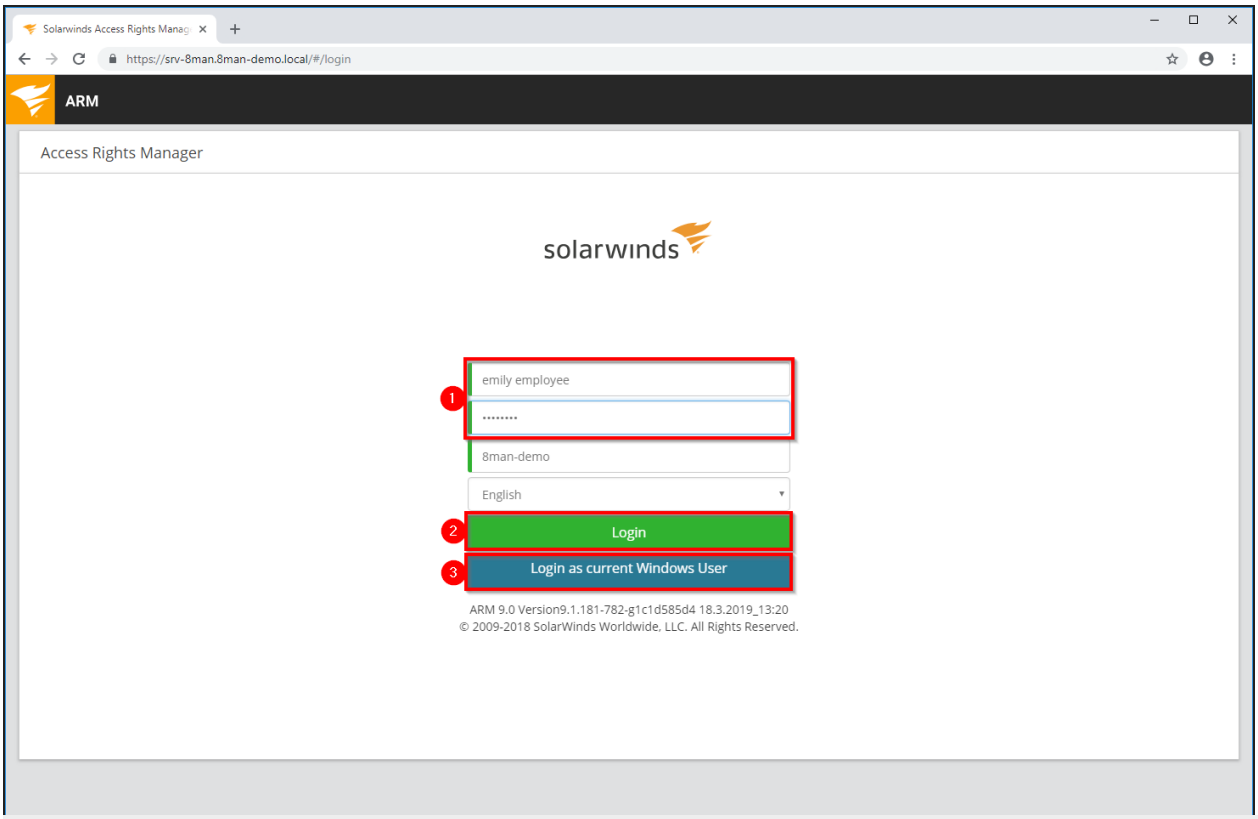
Order new directories using the GrantMA self service portal. This feature is useful for companies that follow restrictive policies for directory creation. We recommend that you allow the creation of directories up to the level three or four below the share only after requesting and approving.

Related features

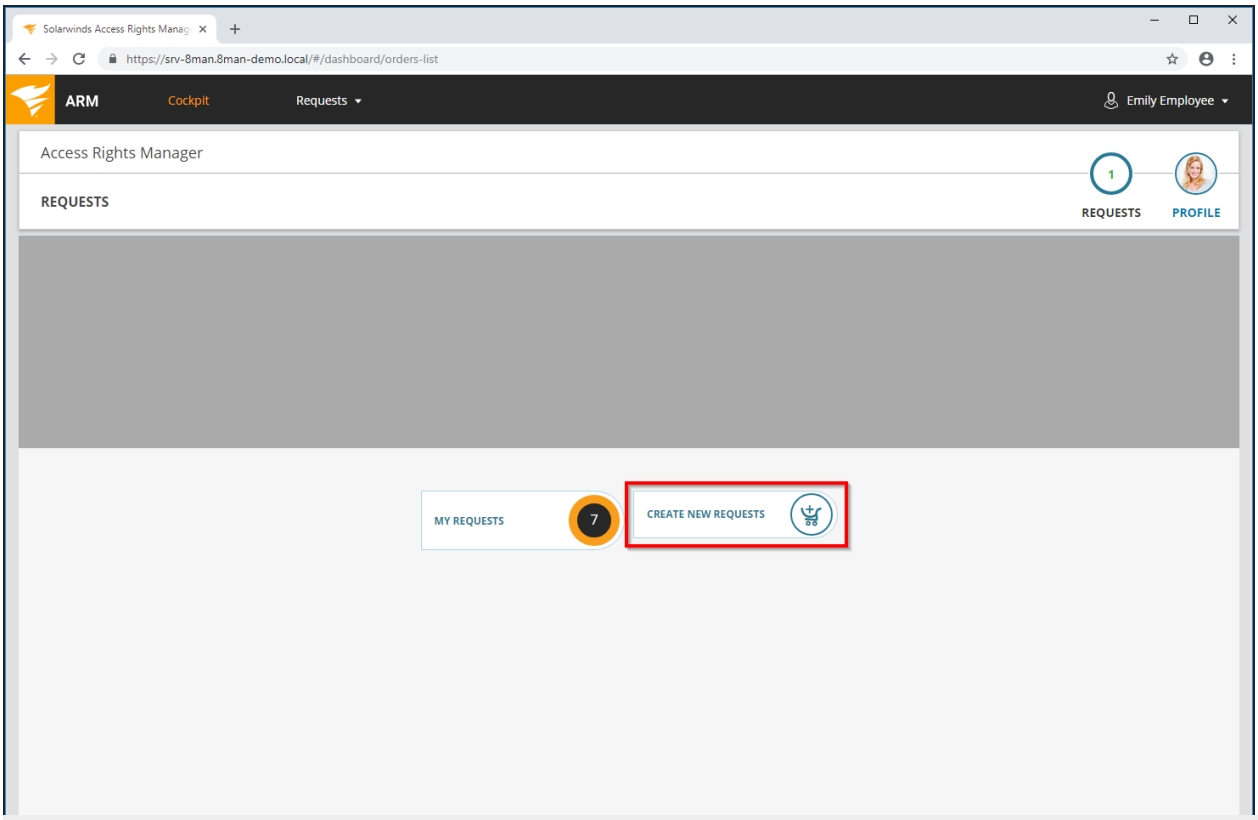
Request file server permissions

Configure GrantMA

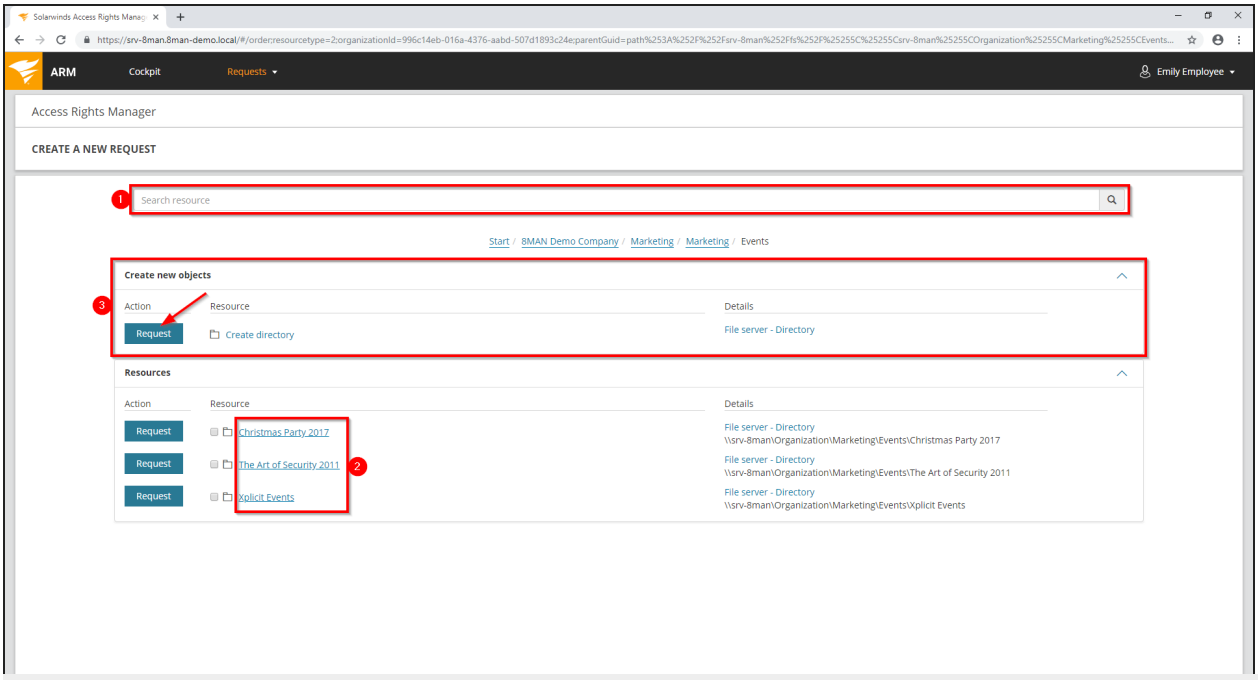
Step-by-step process



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).

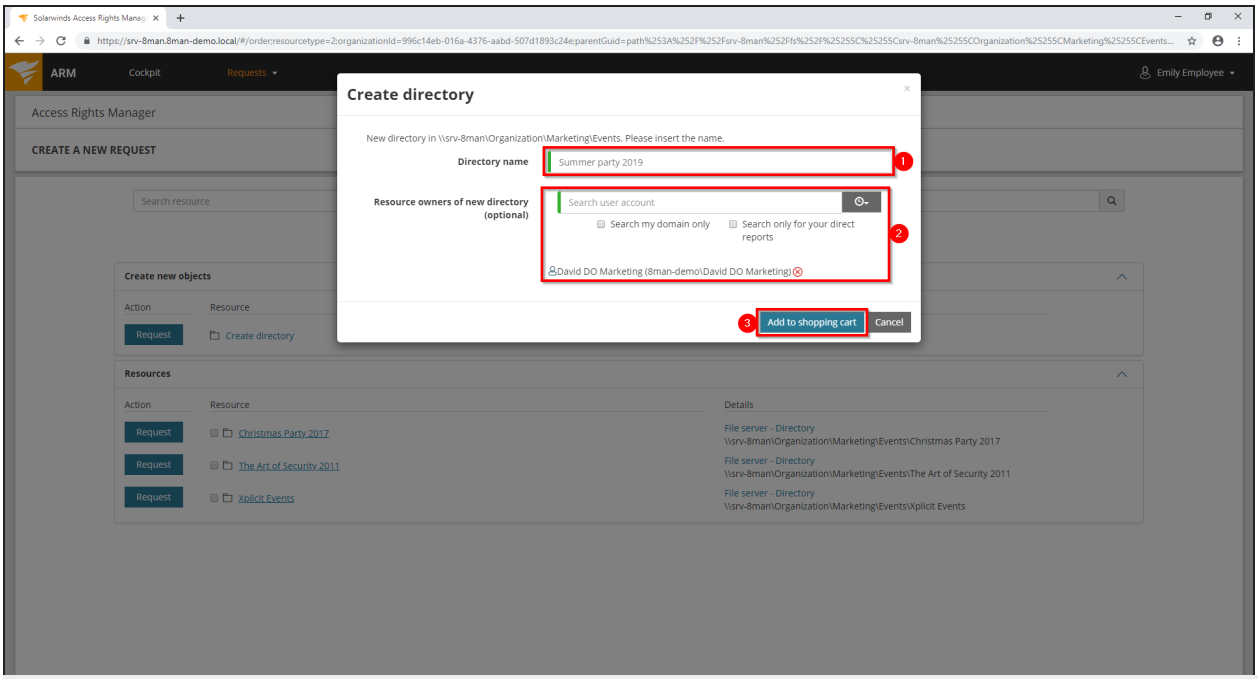


Click "Create new request".

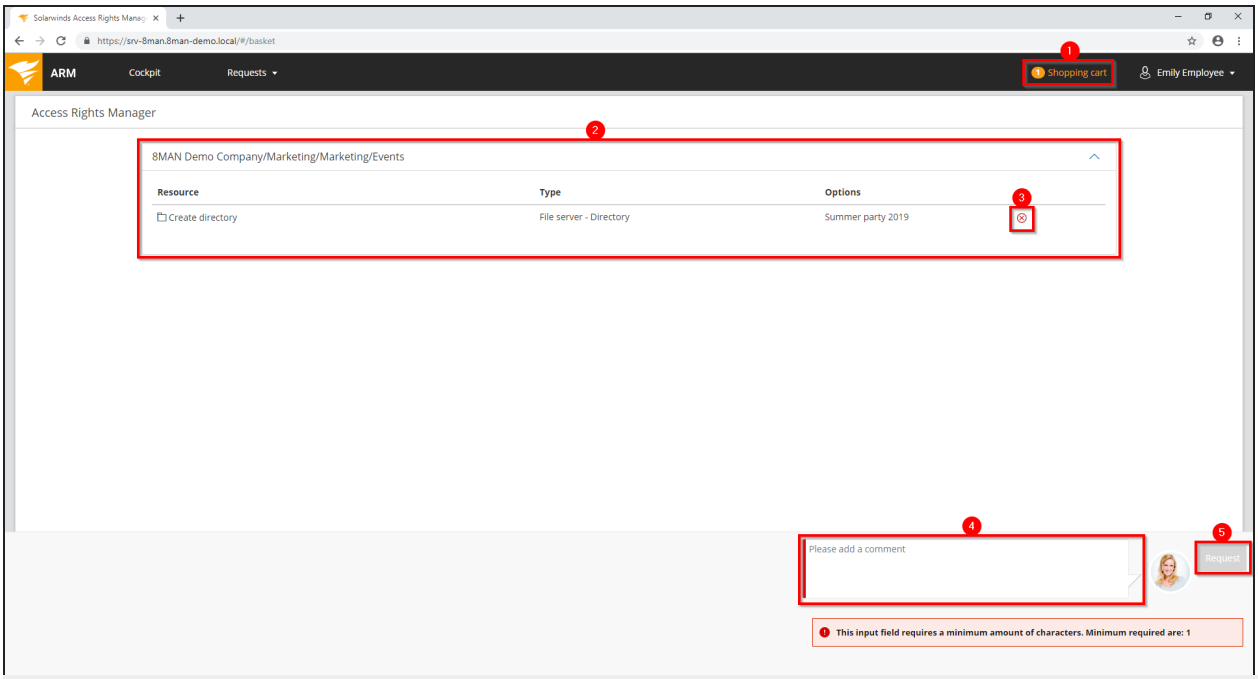


1. Use the search to find the desired resource.

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

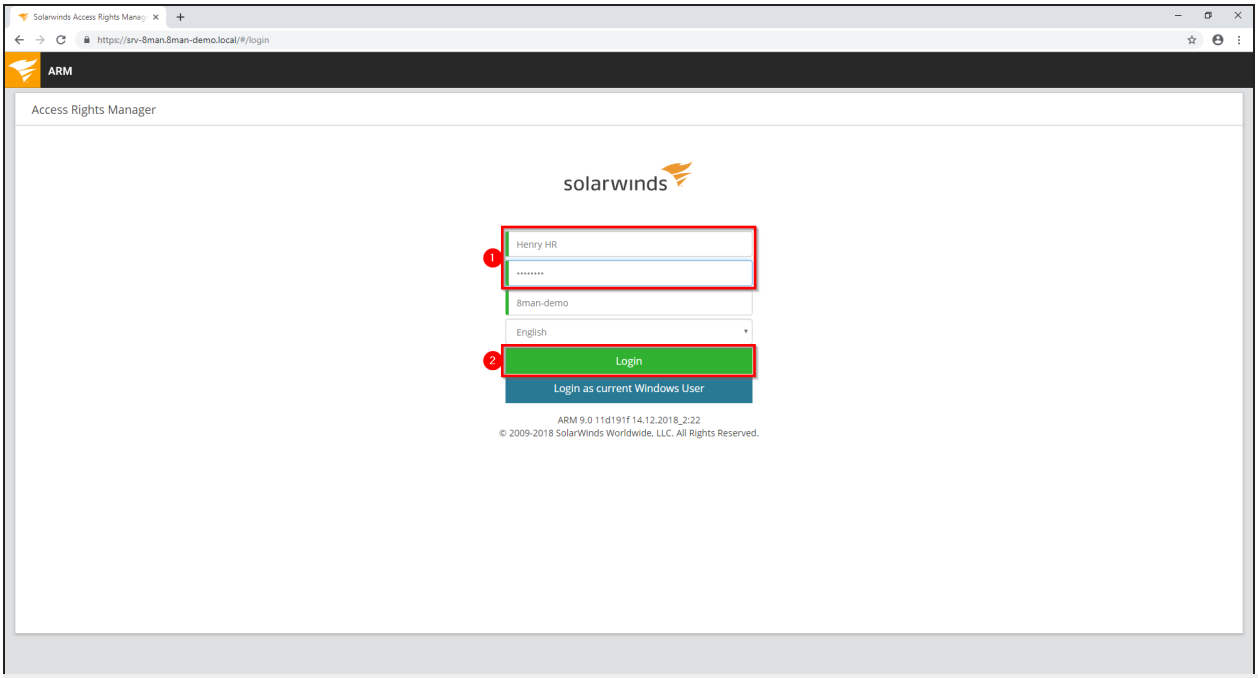
The ARM GrantMA self-service portal allows HR employees to create user accounts for new employees. Instead of sending user information to IT, the entry and creation of a new user account are combined into one simple step. IT simply has to approve the request.

This process is especially useful for departments with high employee turnover and/or a project oriented approach.

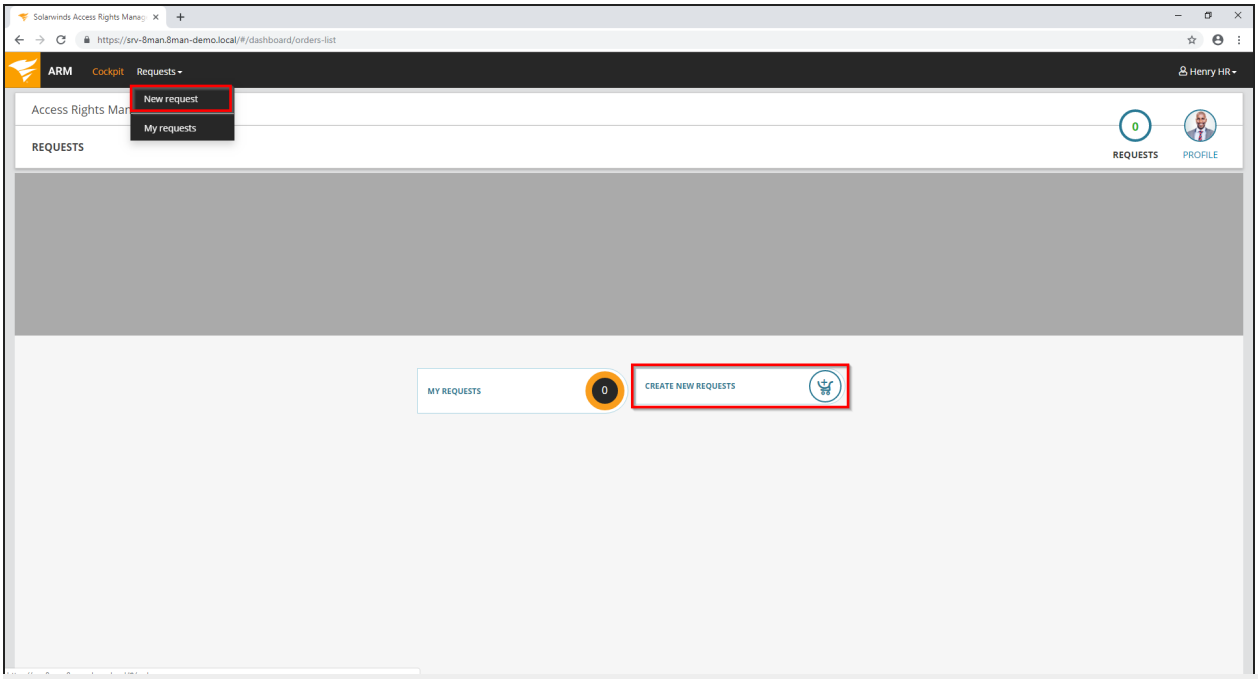
Related features

Approve or reject requests (cockpit)

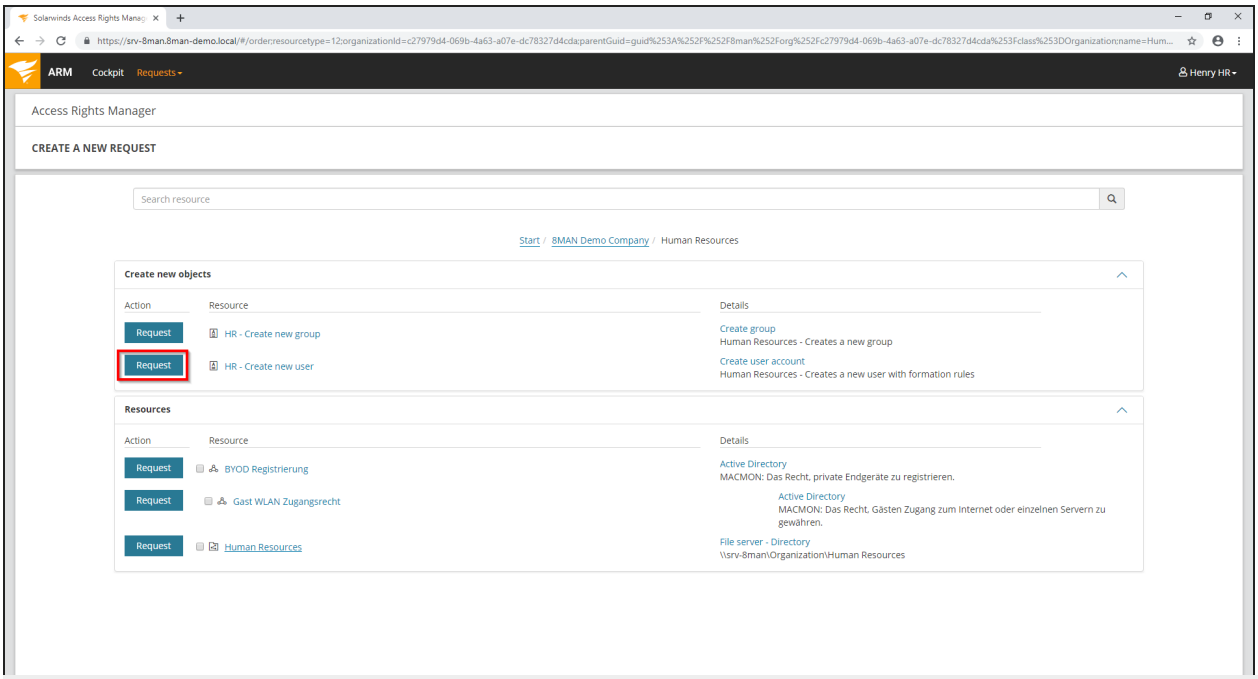
Step-by-step process



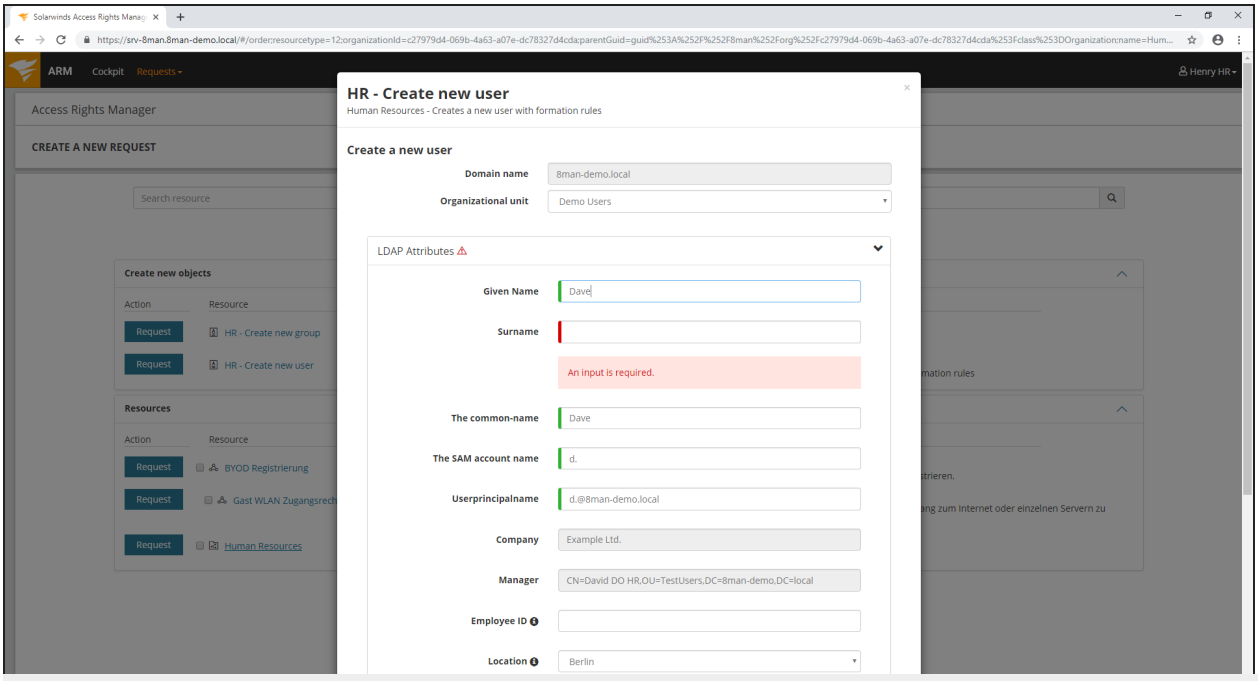
1. Enter your user name and password.
2. Click on "Login".



Click "New Request".

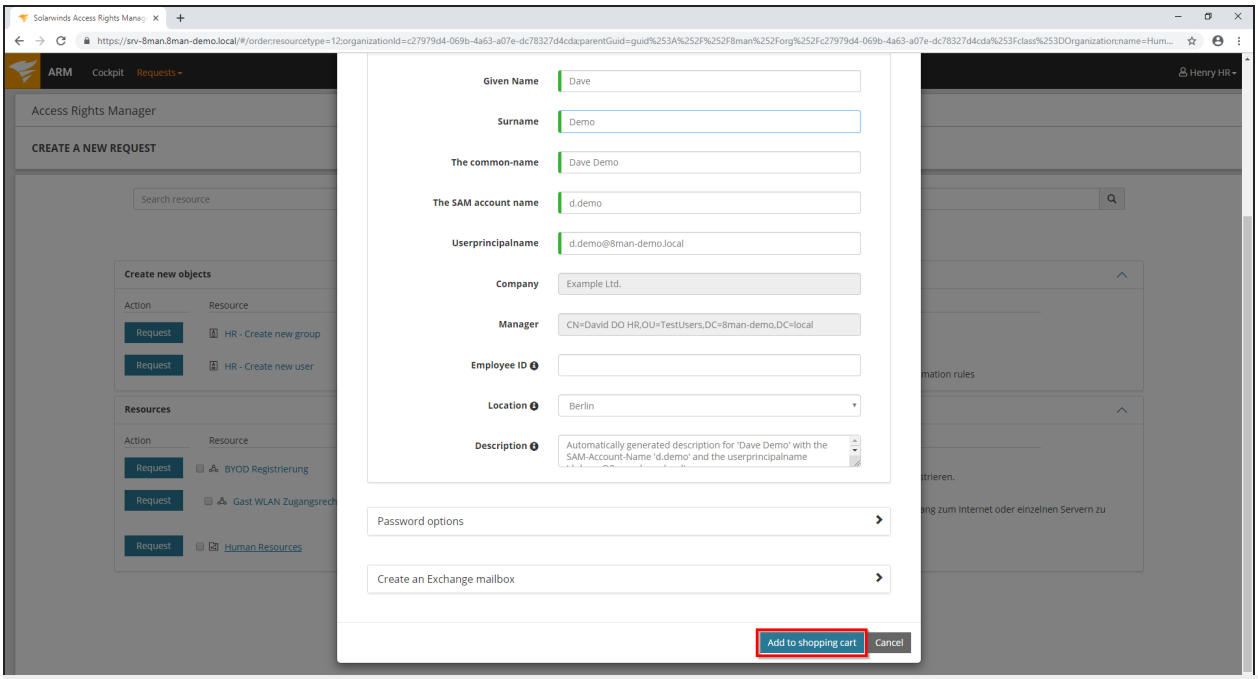


Select "new user" and click on "Request".

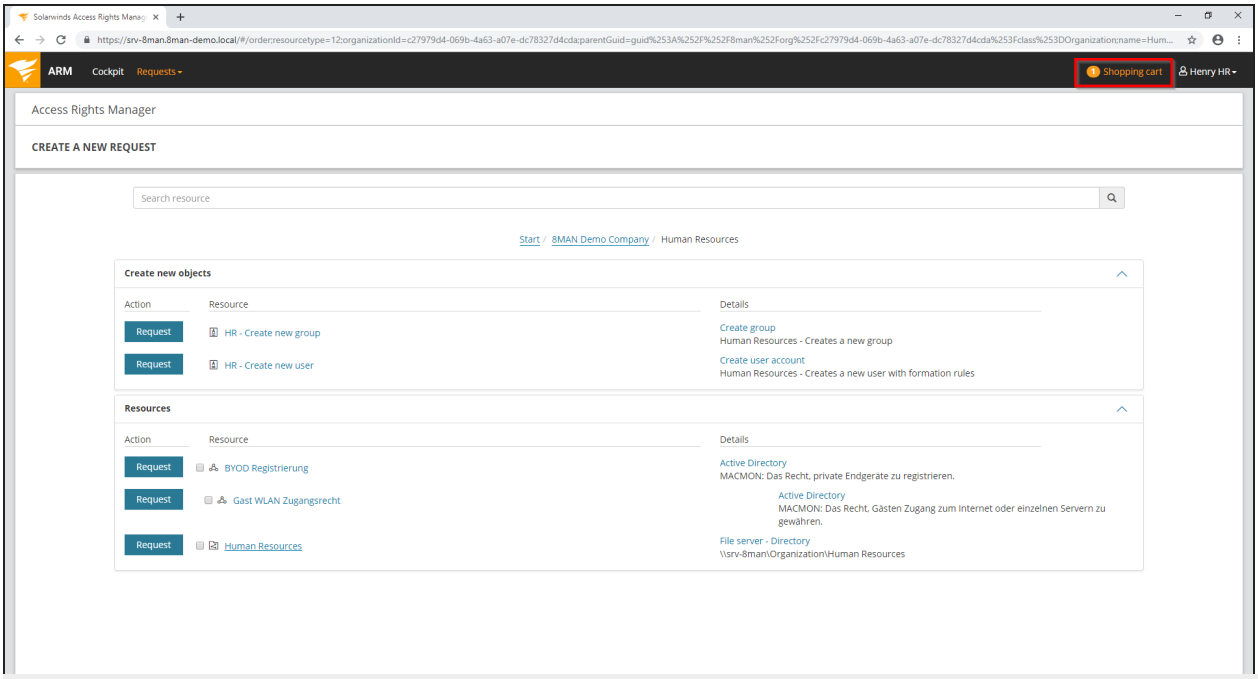


Enter the relevant information for the new user. Fields indicated in red are mandatory or contain invalid entries.

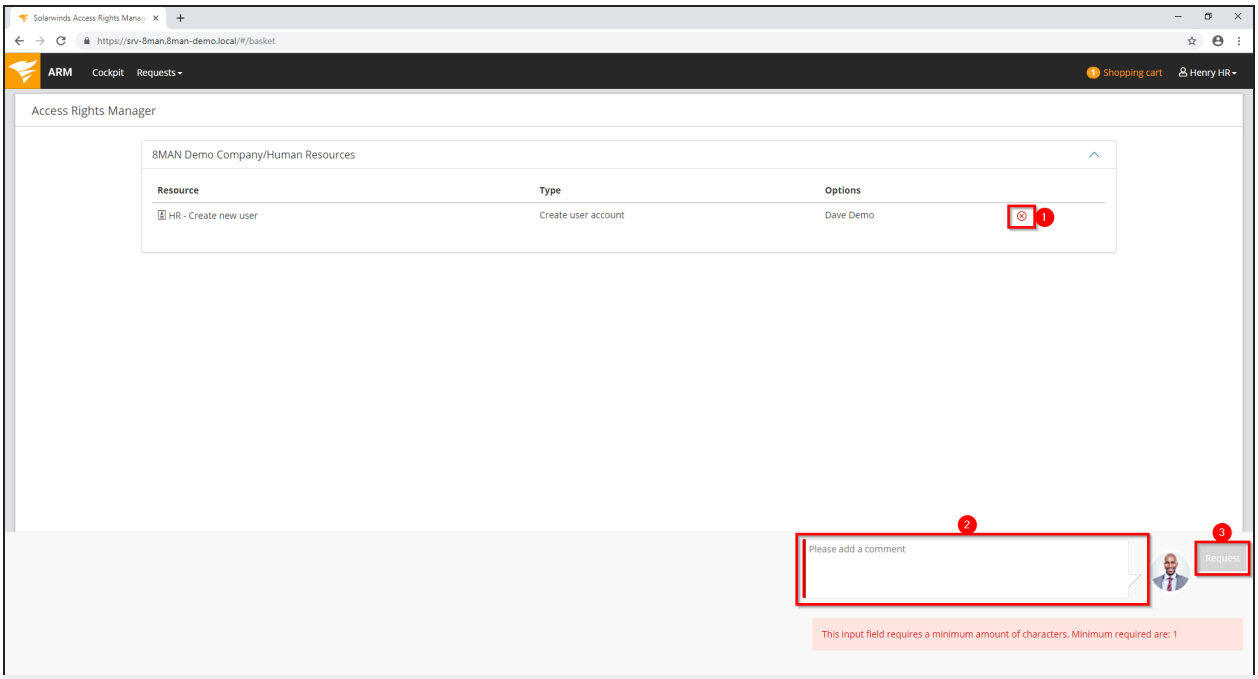
ARM administrators can customize the input template.



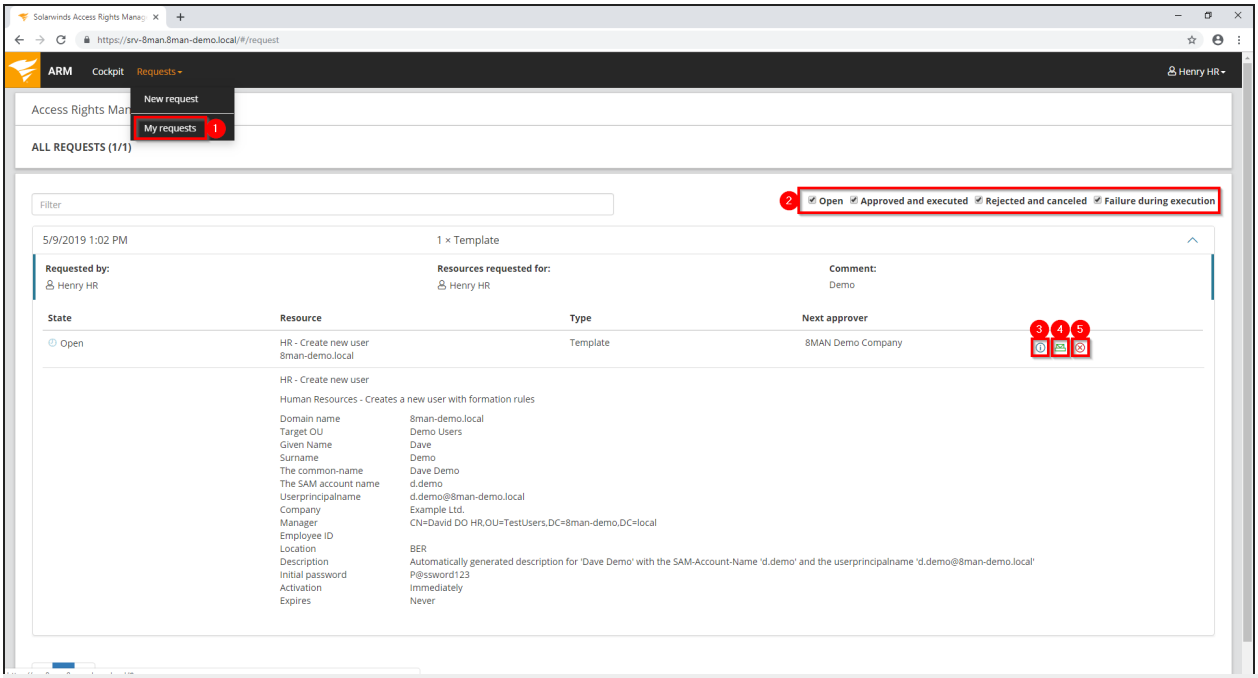
After entering all required information click on "Add to shopping cart".



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

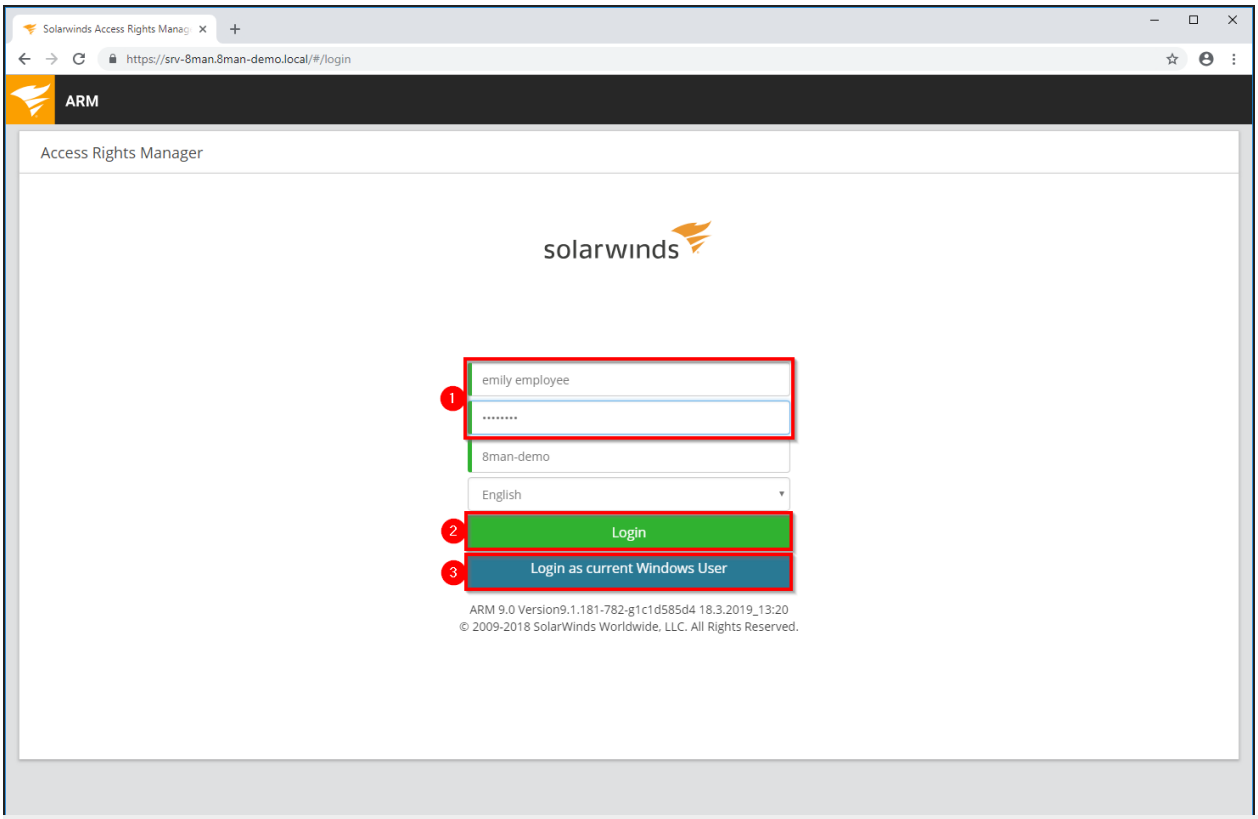
In addition to ordering user accounts, authorizations, directories or freely definable objects (OpenOrder), other script-based services can be ordered via the web client.

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)

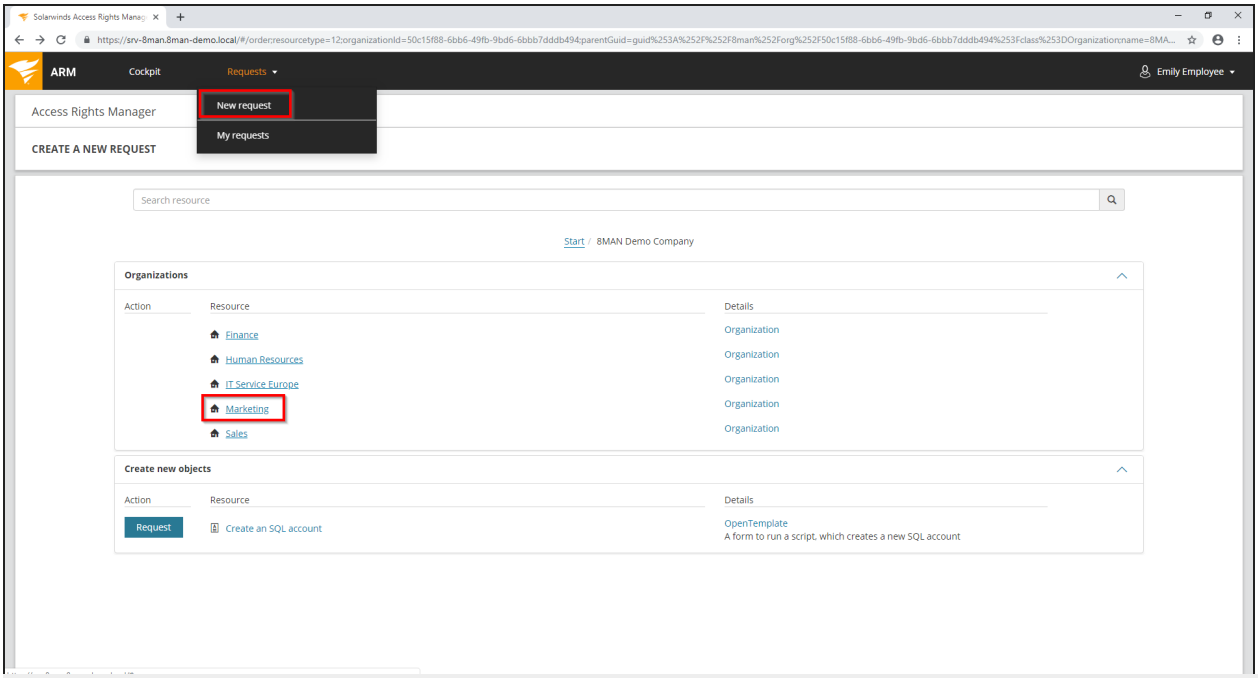
Step-by-step process



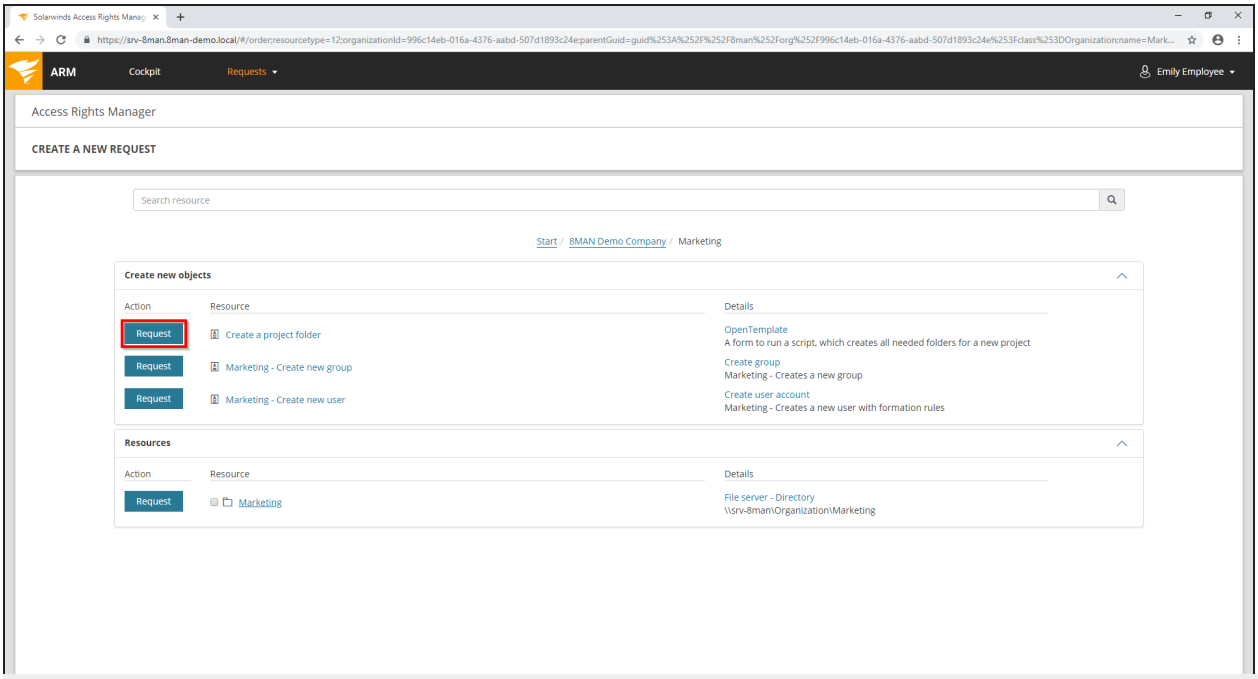
The following example, a user requests a project folder structure.

1. Enter your user name and password.
2. Click "Login".

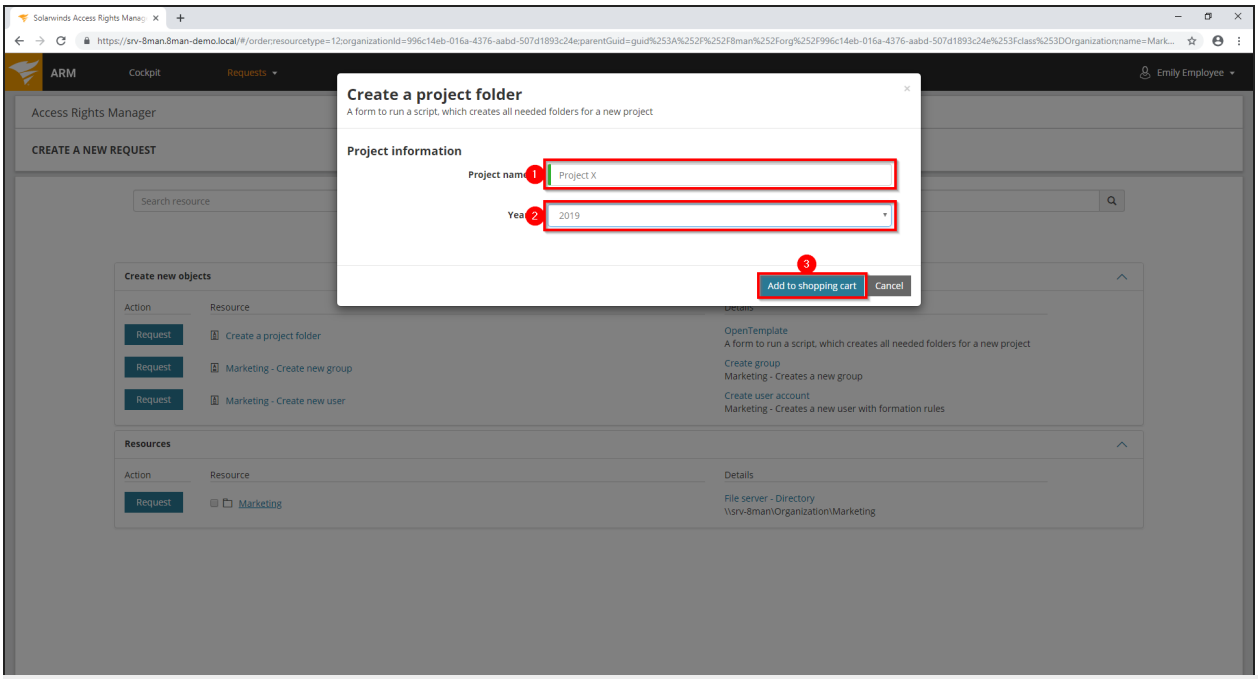
3. You can alternatively login as the current windows user (no user name and password required).



Select the organizational category that contains the service. In the example here "Marketing".

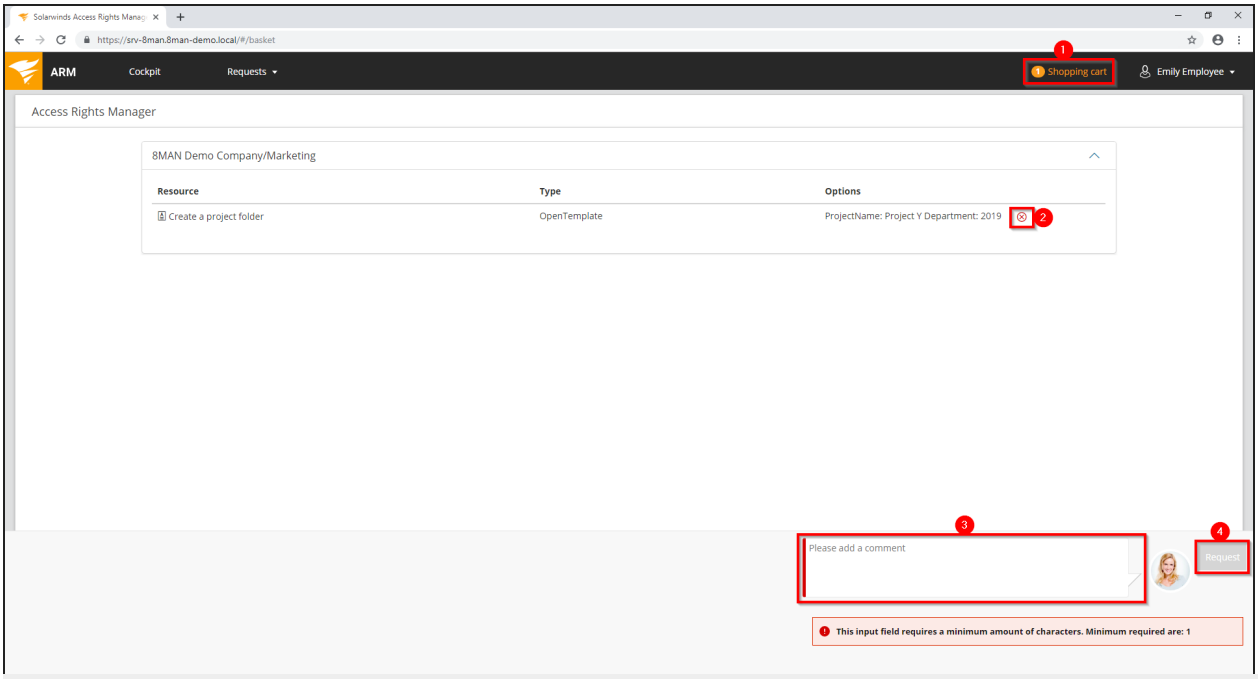


Select the service "Create project folder" and click on "Request".



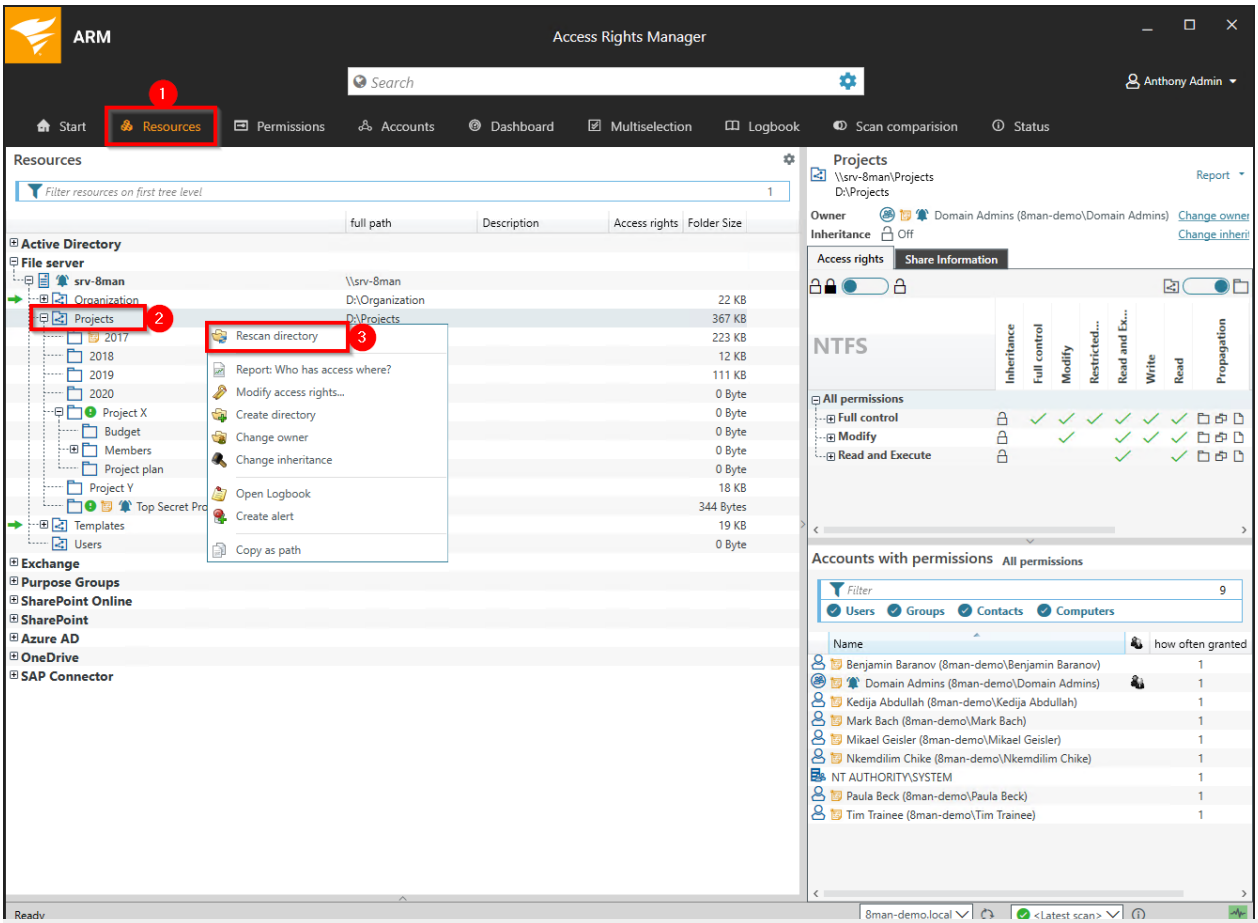
Enter the parameters for the script. In the example:

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

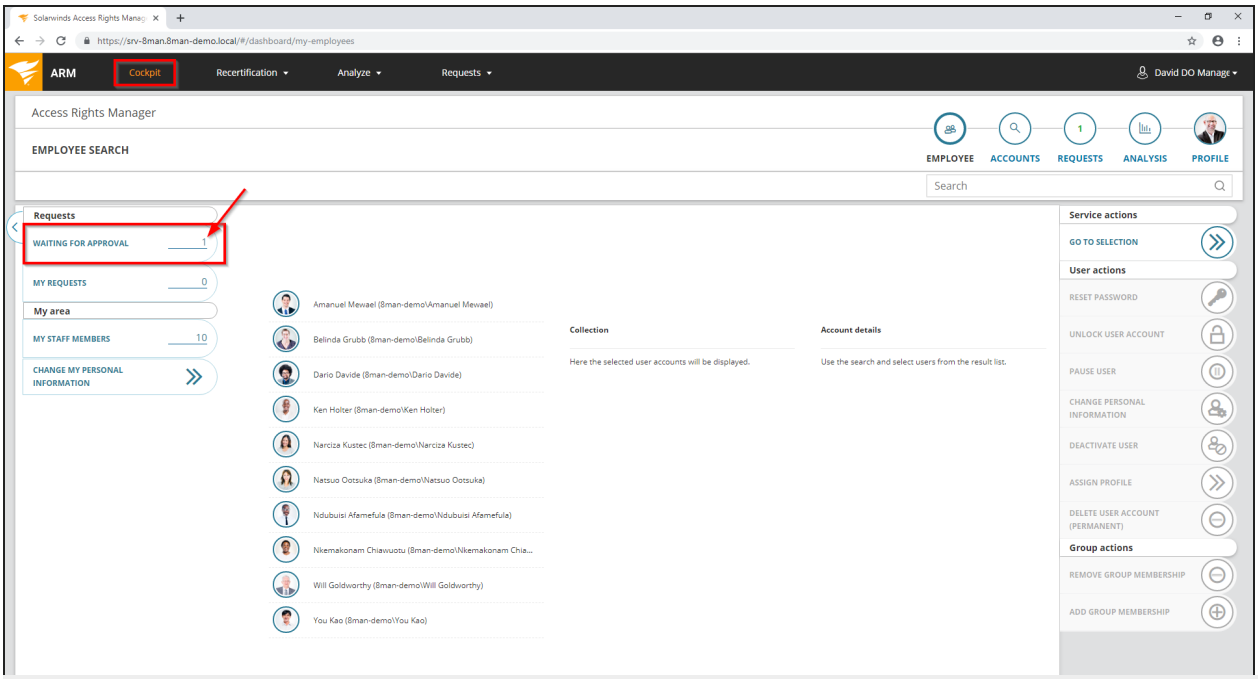
By using the ARM GrantMA self-service portal, managers and data owners are able to approve and modify or reject requests.

Approve or reject requests (cockpit)

Background / Value

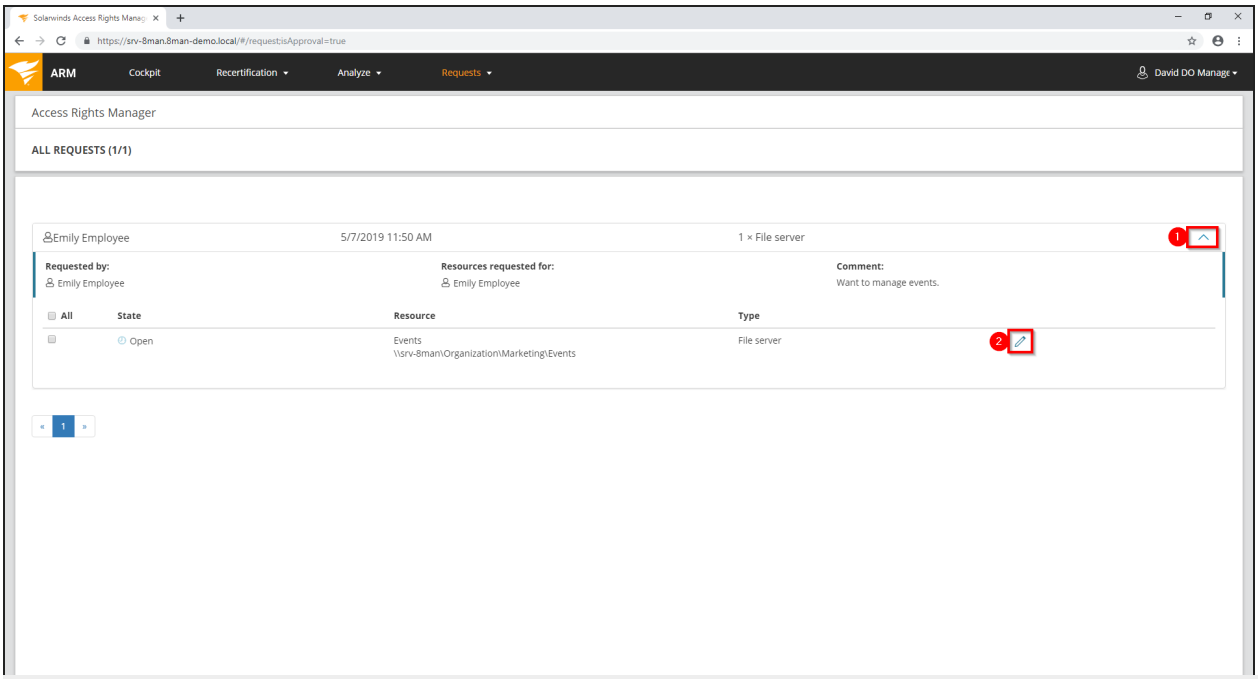
Depending on how you have set the approval process, you will receive approval requests for the individual order processes. As an administrator or data owner you keep an eye on the processes.

Step-by-step process



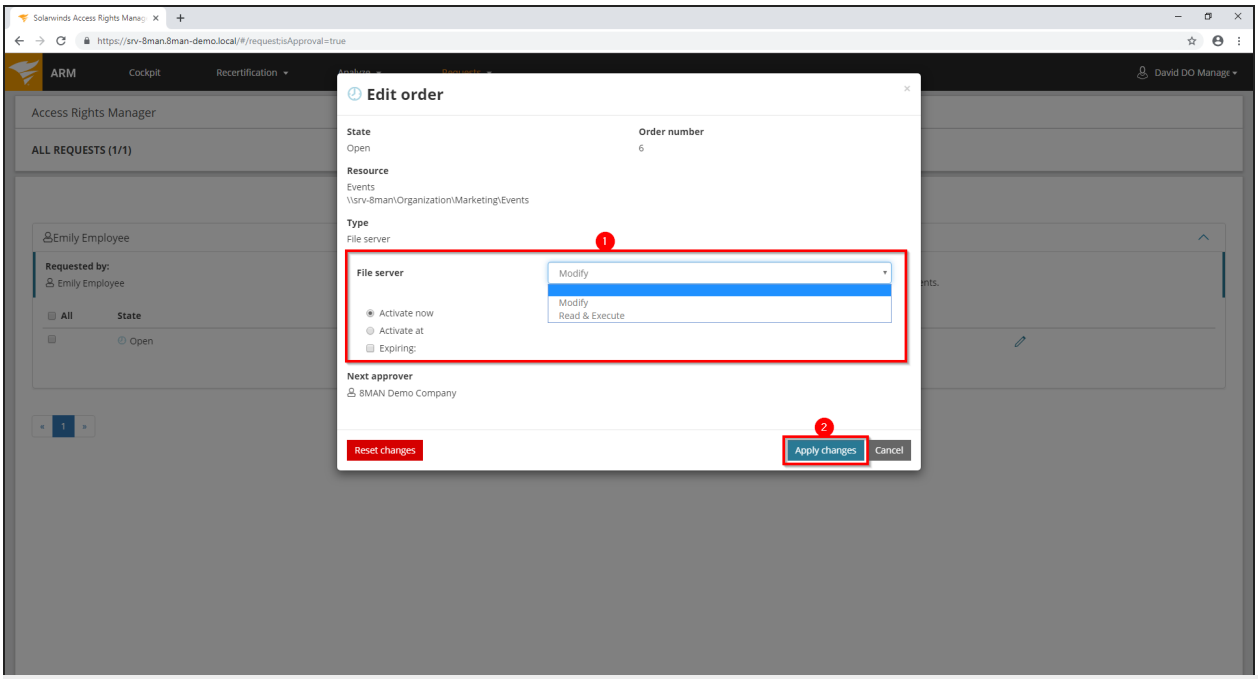
Click "Waiting for Approval." In the example shown, 1 request is waiting for approval.

> The range of available services (buttons) varies according to role (login), risk assessment and configuration.



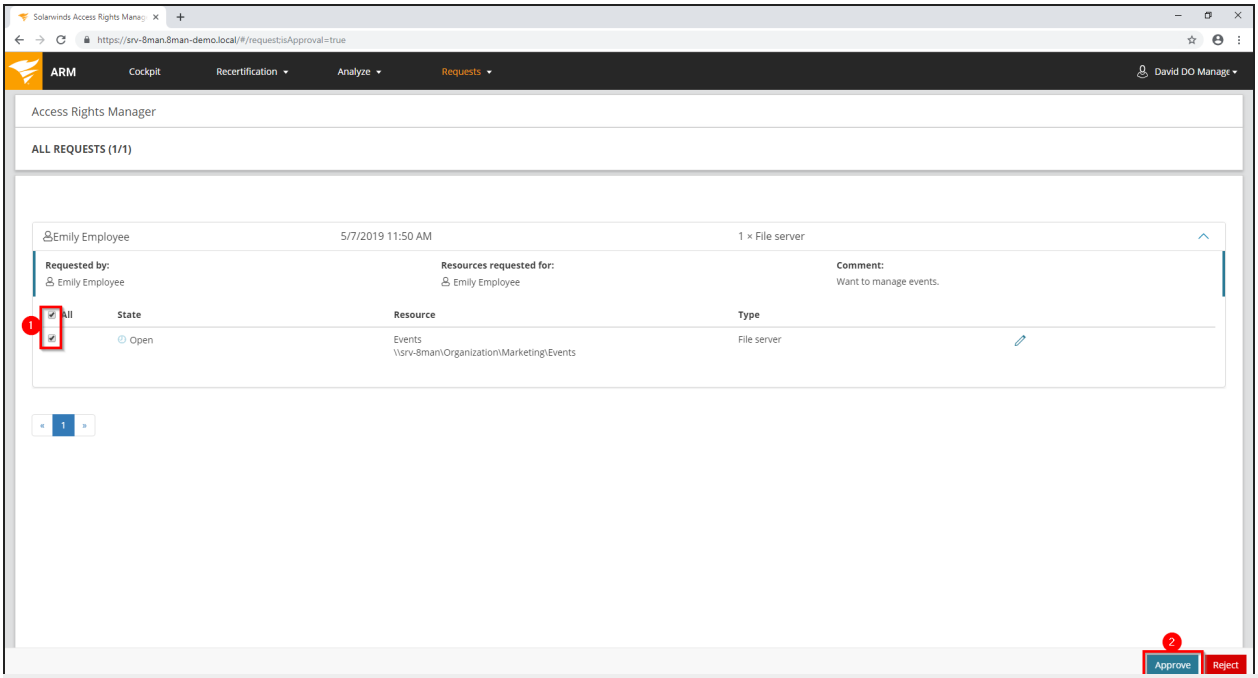
1. Expand an order to see the items.
2. Depending on the ARM configuration set by your ARM administrator, you will see a pencil or information symbol:
   - Pencil: You can modify the order.
   - Info: You see the details and you are not allowed to modify the order.

Click on the pencil icon.



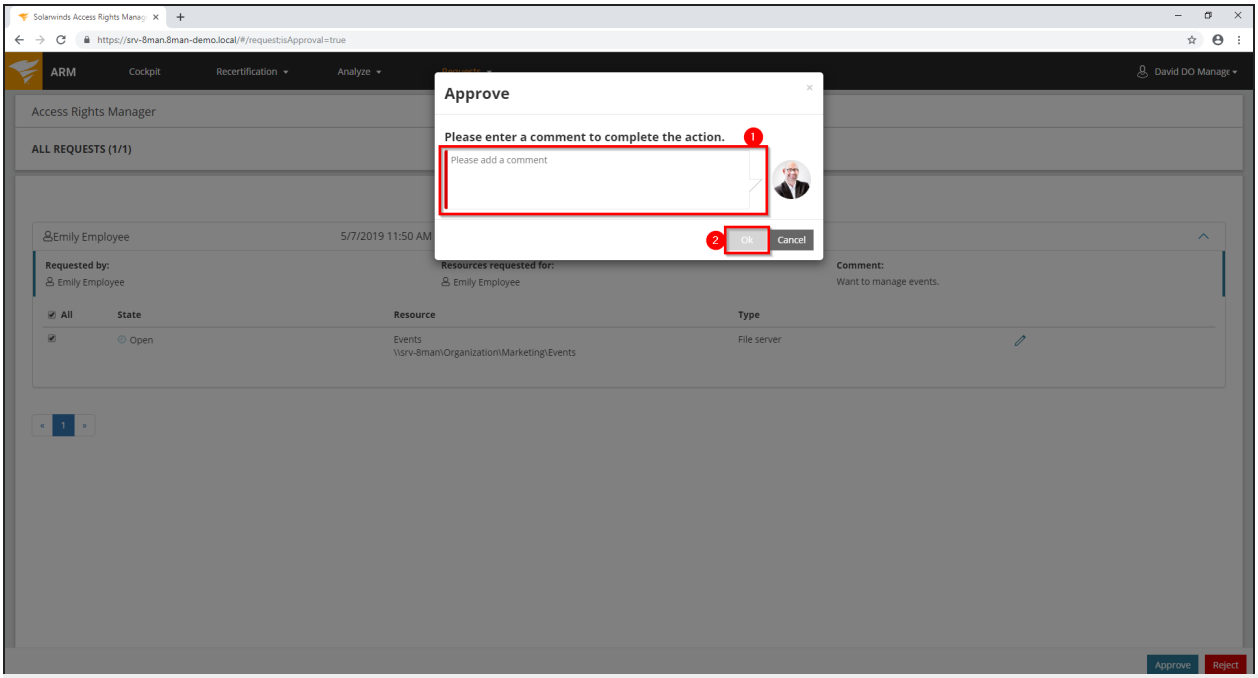
You can edit the order request.

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".

The comment appears in the logbook and is therefore documented auditable.

Inform approvers of new requests via email

Background / Value

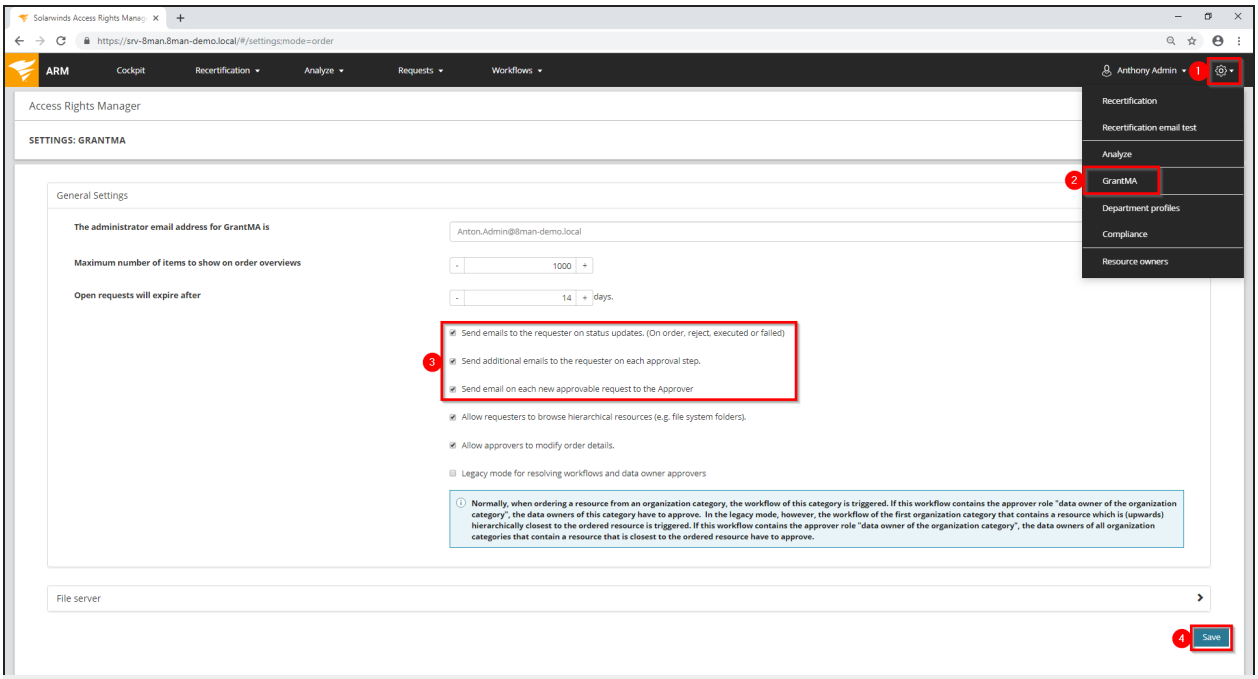
To prevent approvers from having to proactively check for open approval requests on the ARM home page, we recommend activating approval emails.

Related features

GrantMA: Design approval processes

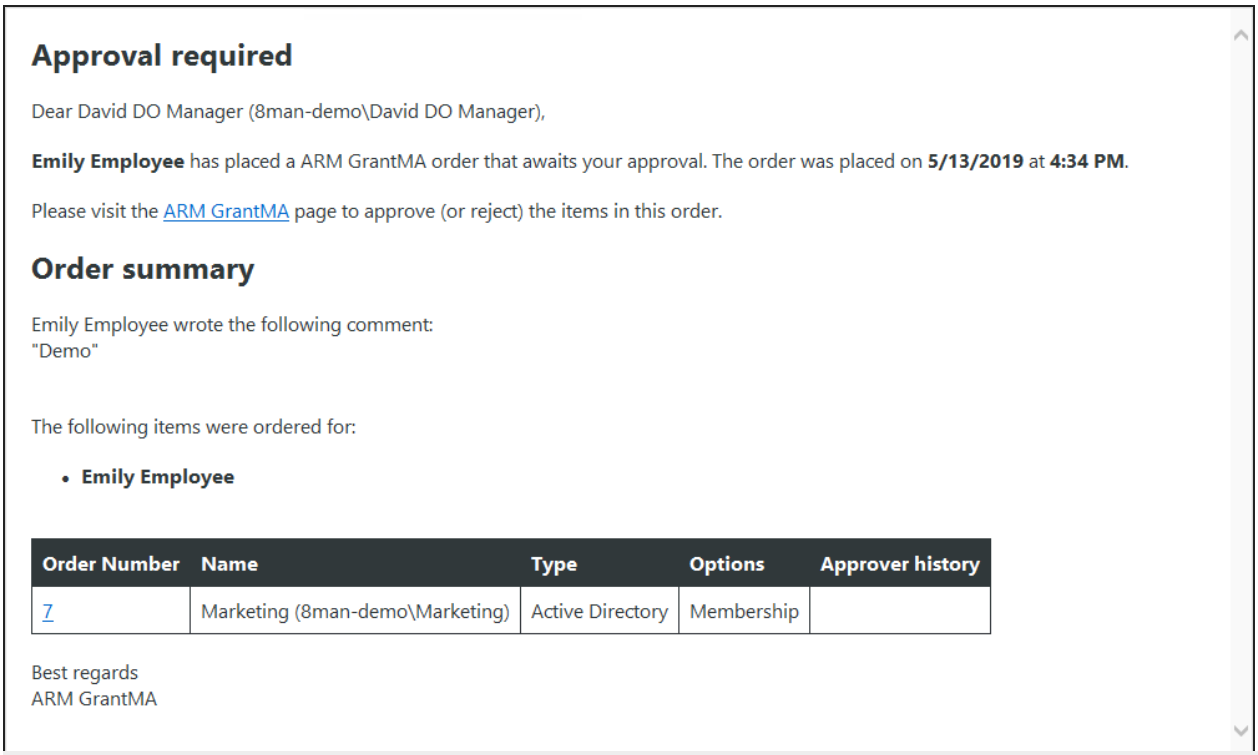
Customize notification emails

Step-by-step process



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
7	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

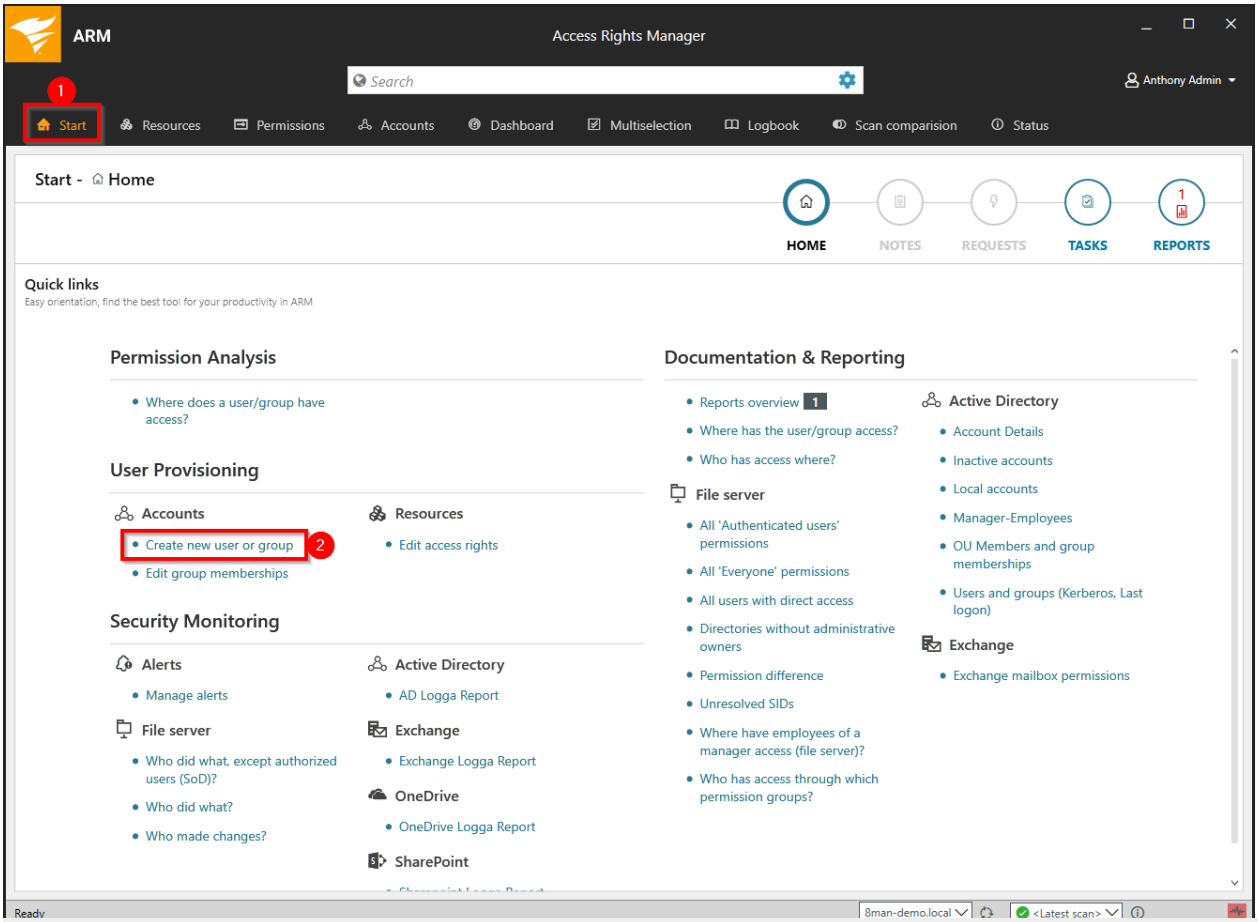
Background / Value

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.

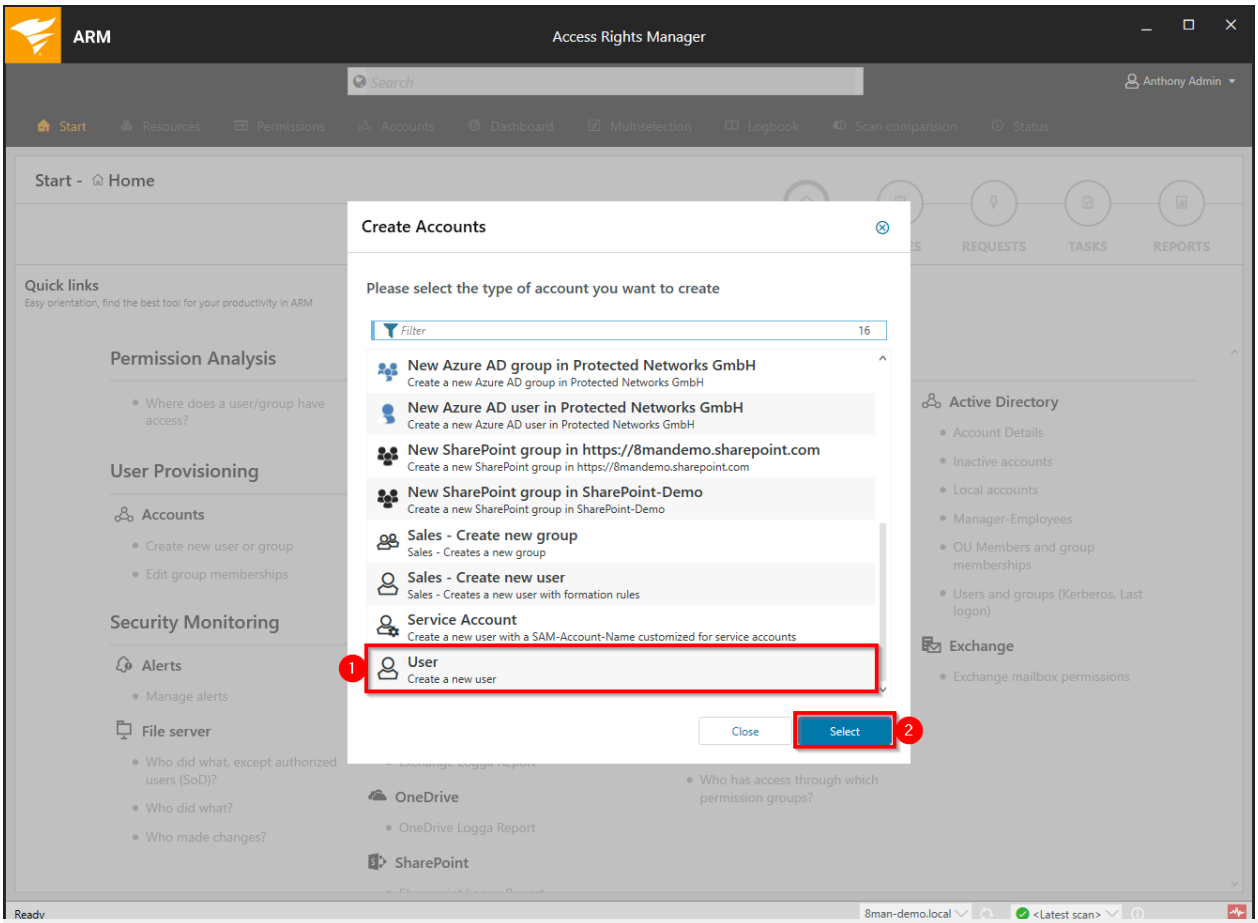
Related features

Customize templates for account creation (please refer: Customize ARM templates)

Step-by-step process

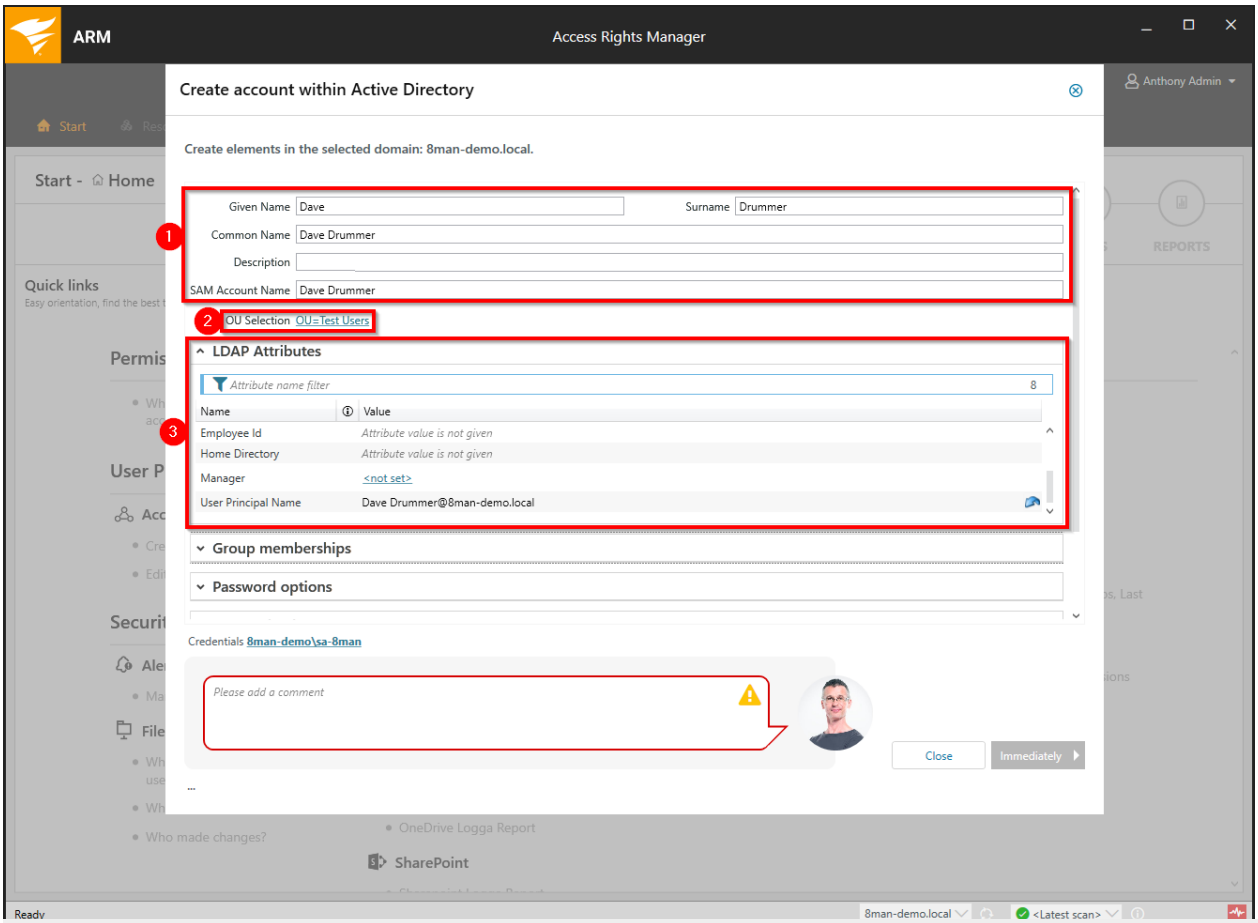


1. Click "Start".
2. Click "Create new user or group".

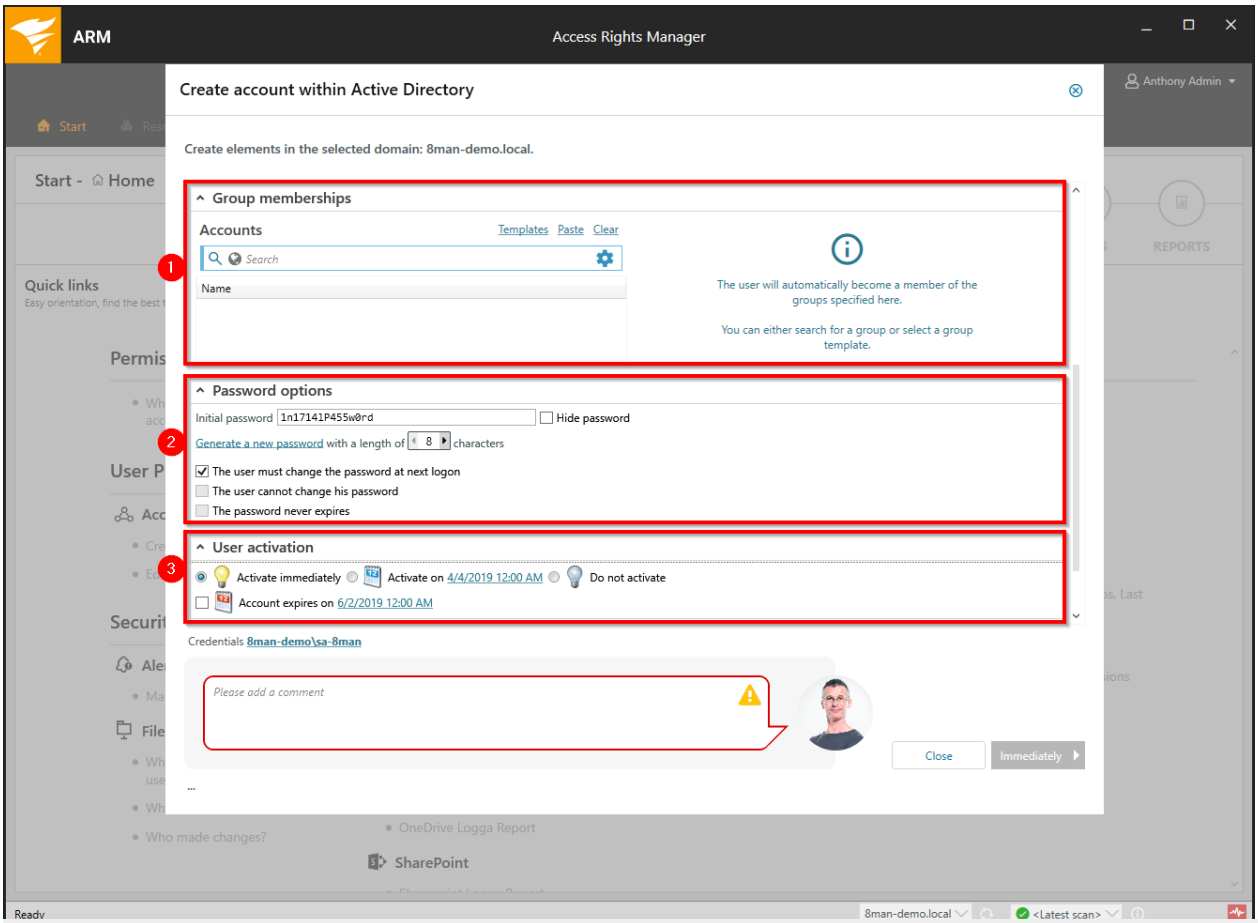


ARM offers 4 standard templates. You can generate as many of your own templates as you wish. We recommend using customized templates as a foundation as this simplifies and speeds up the process.

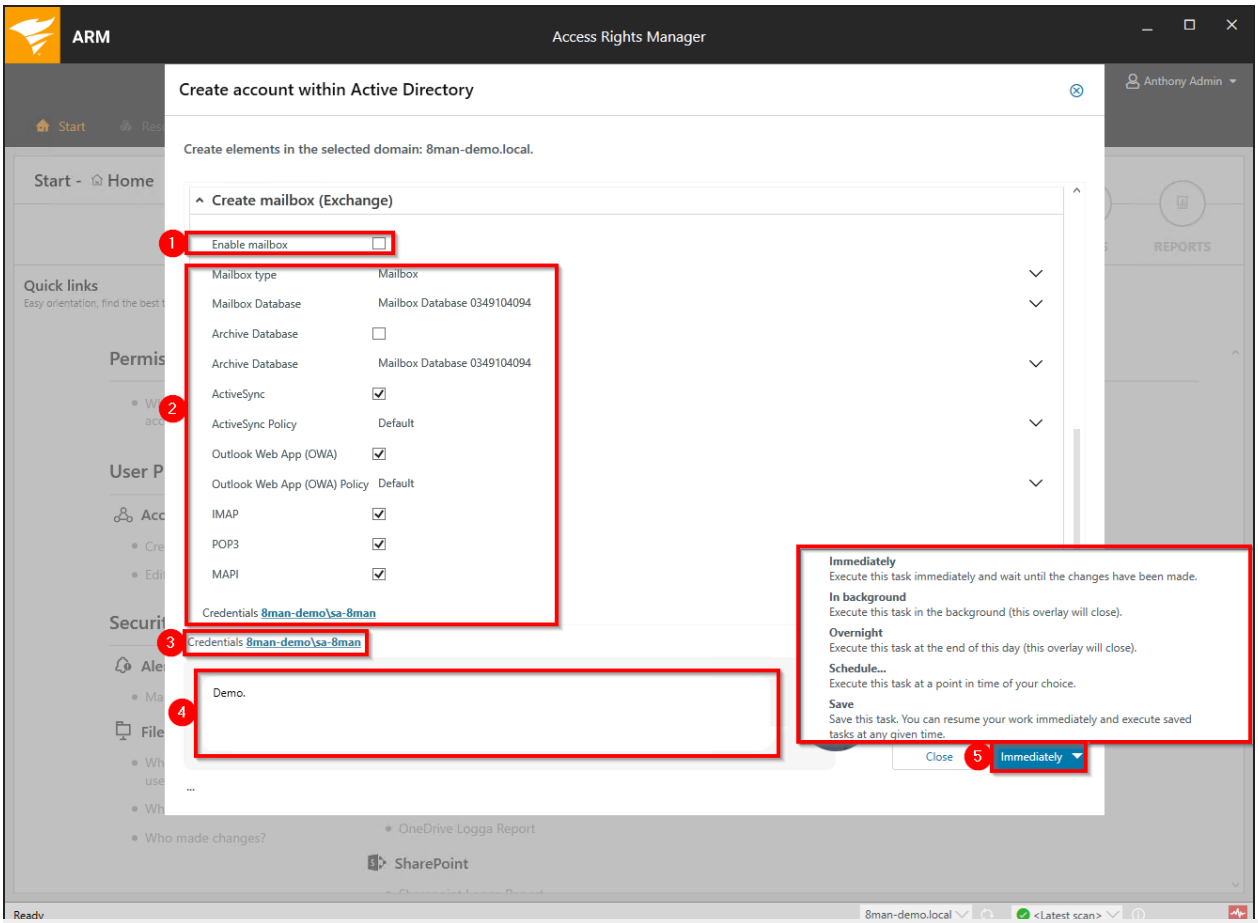
1. Select a User template.
2. Click on "select".



1. Enter the required information.
2. Modify the OU if desired.
3. Set further LDAP attributes.



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.



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.

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.

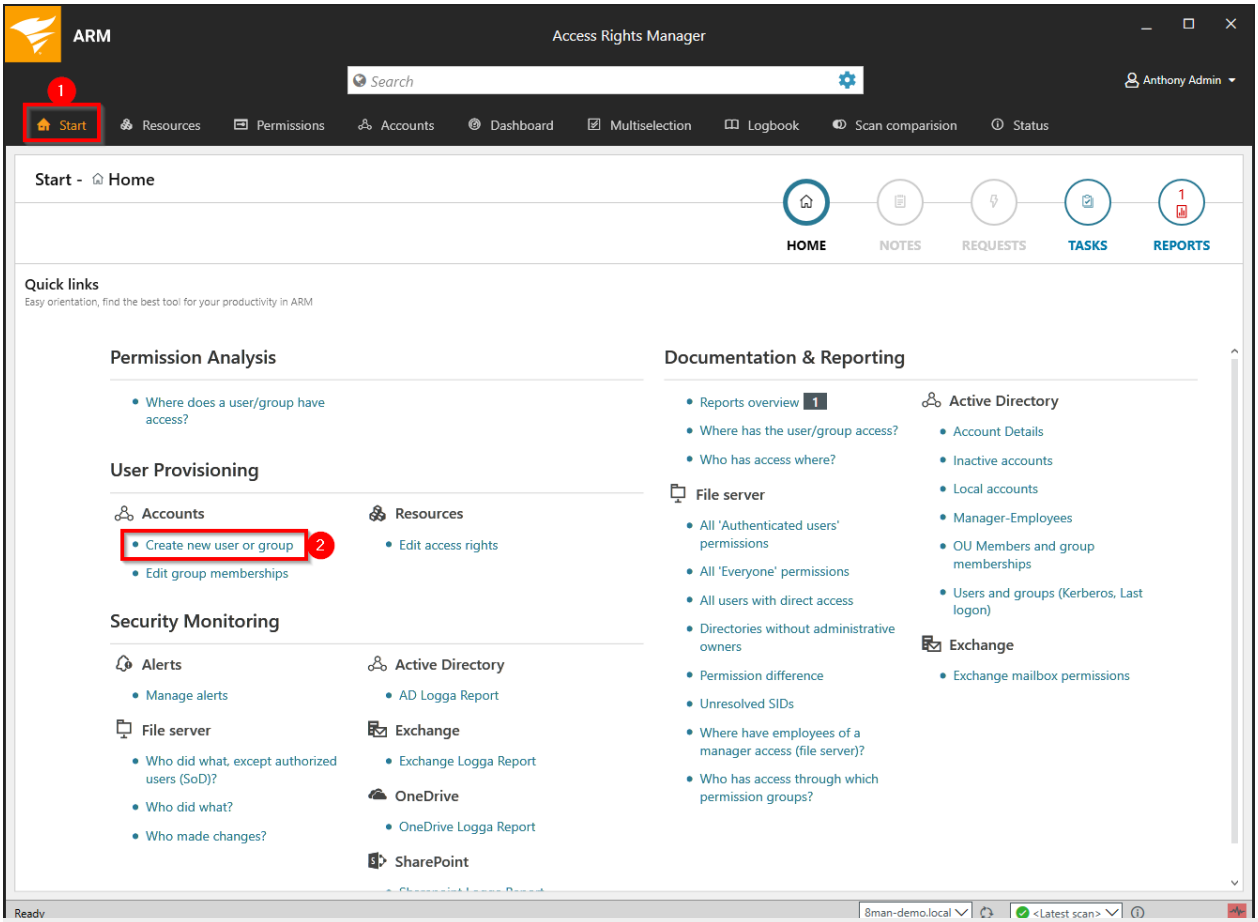
⚠ Use this feature on managed Azure Active Directory domains only. For federated domains that are synced with an on-premise AD, you must create the user in the leading on-premise AD.

Related features

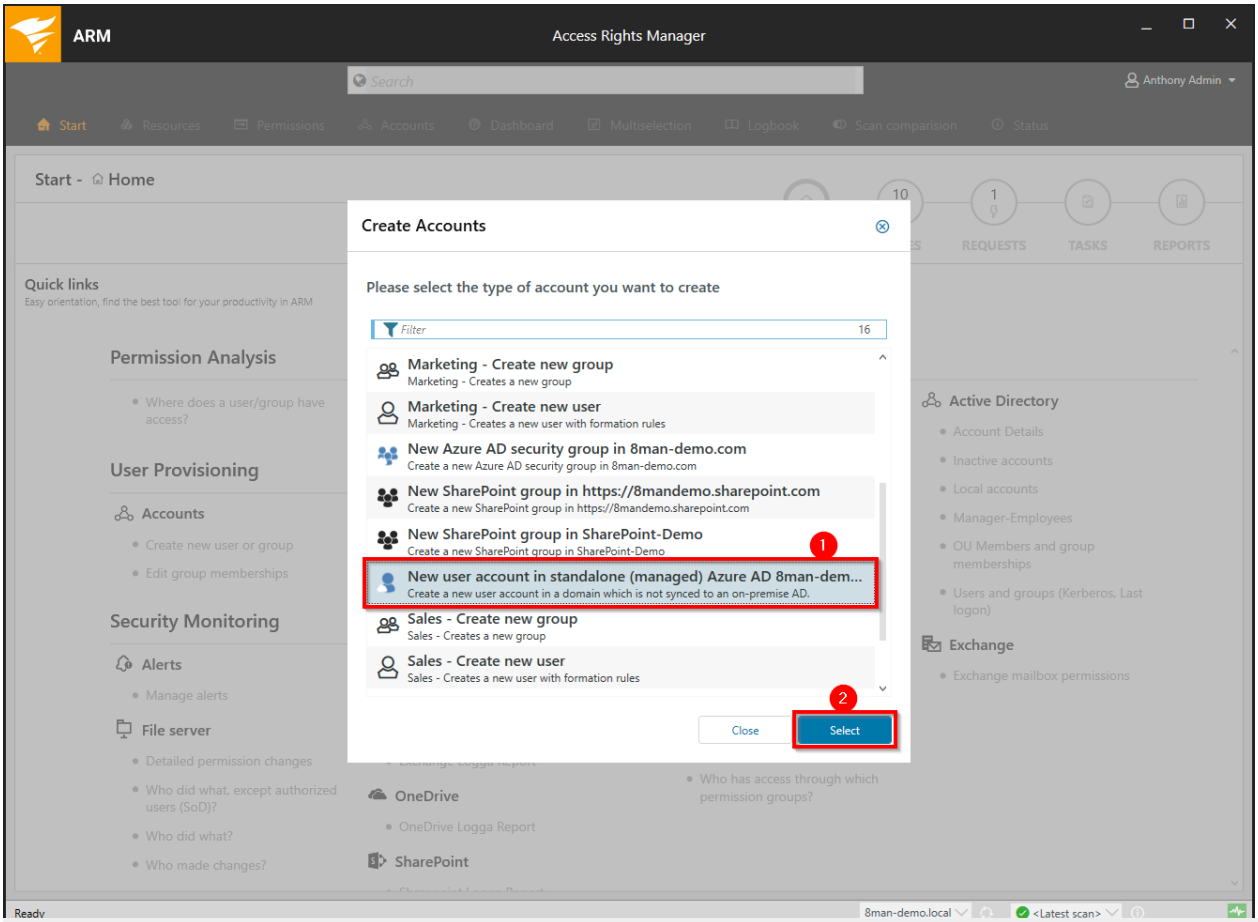
Customize templates for account creation (please refer: Customize ARM templates)

Create a mailbox in Exchange Online

Step-by-step process



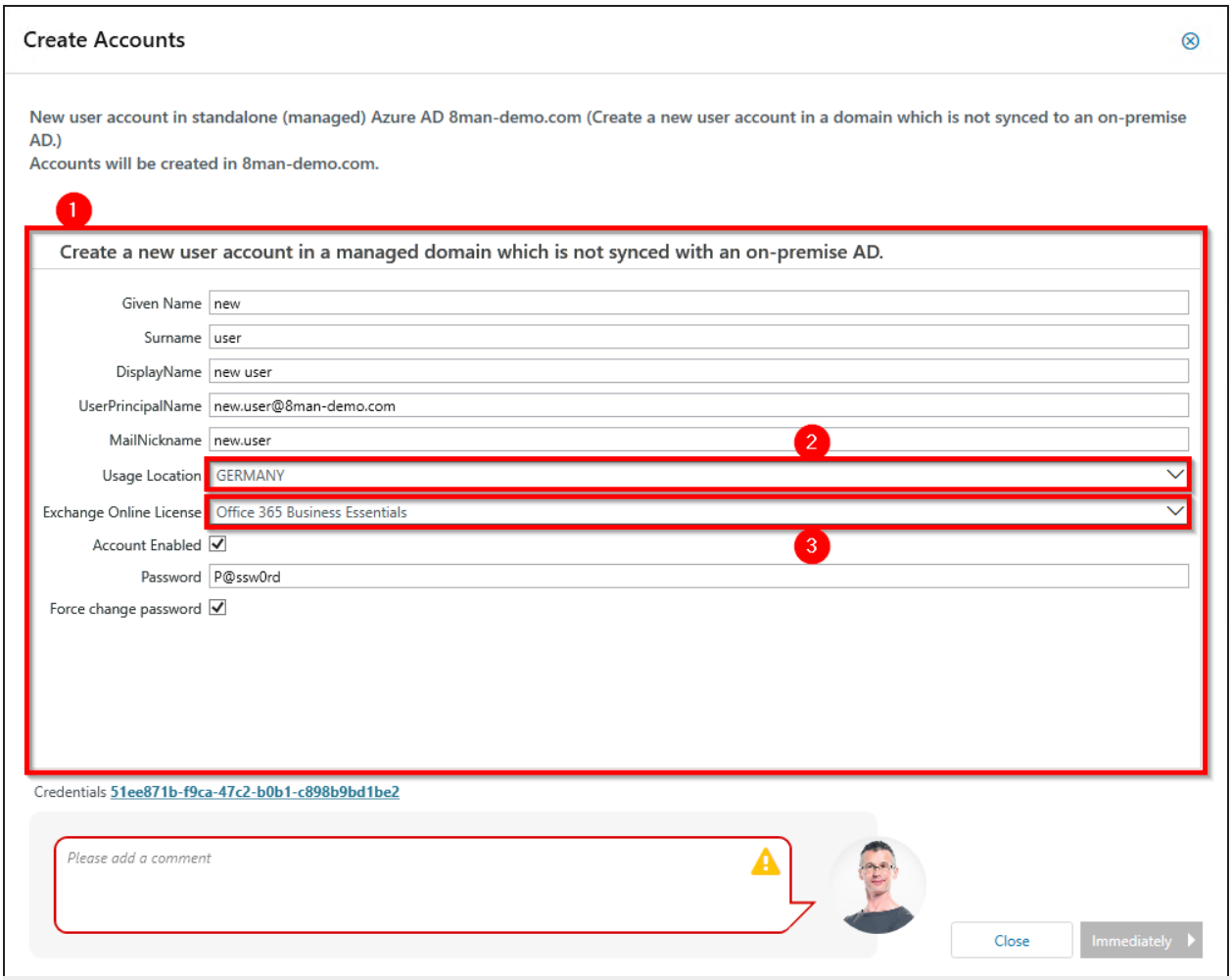
1. Click "Start".
2. Click "Create new user or group".



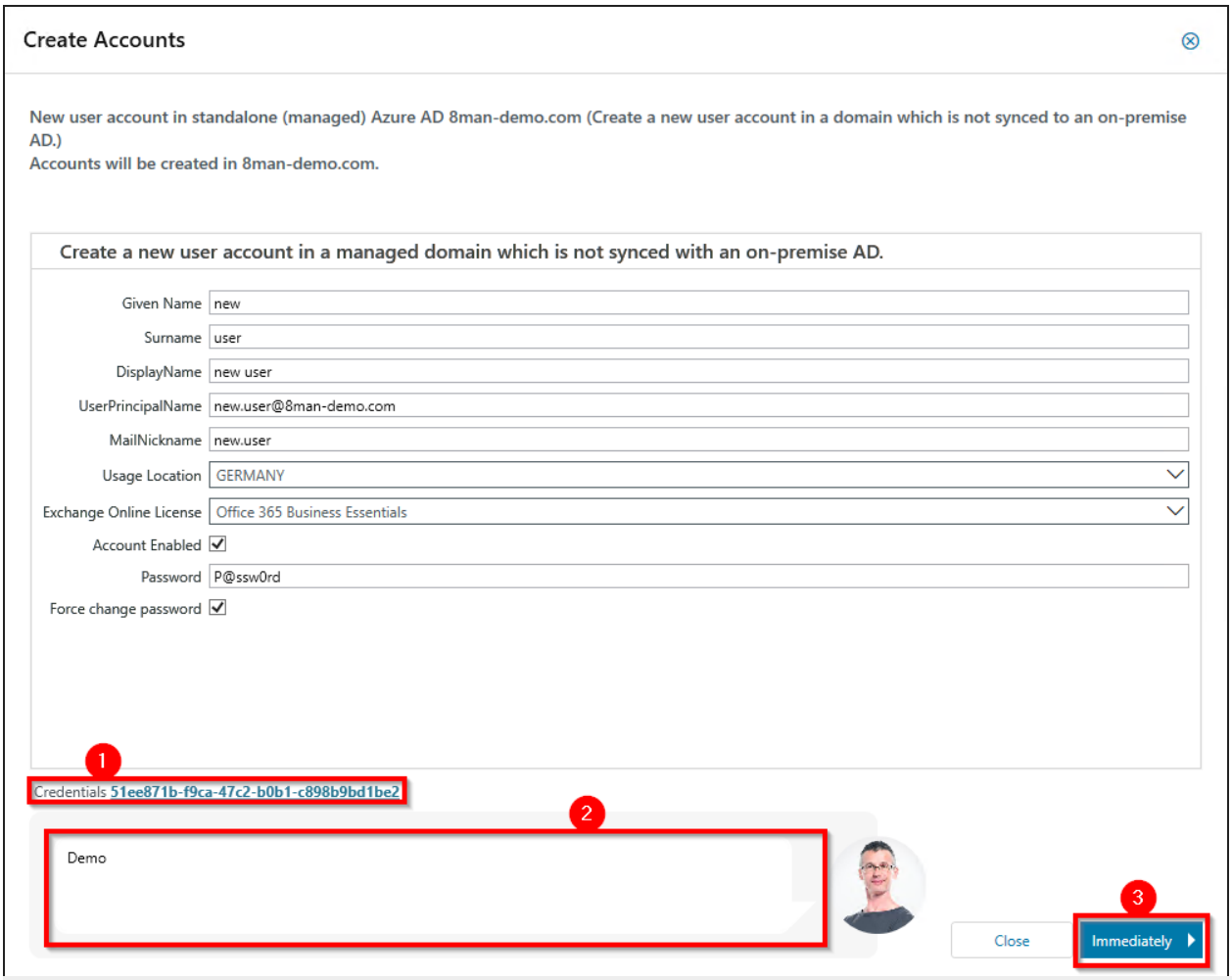
ARM offers 4 standard templates. If you add an Azure Active Directory (AAD) as a resource to ARM then you will find two templates for creating new users and groups in AAD.

> 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.



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.



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

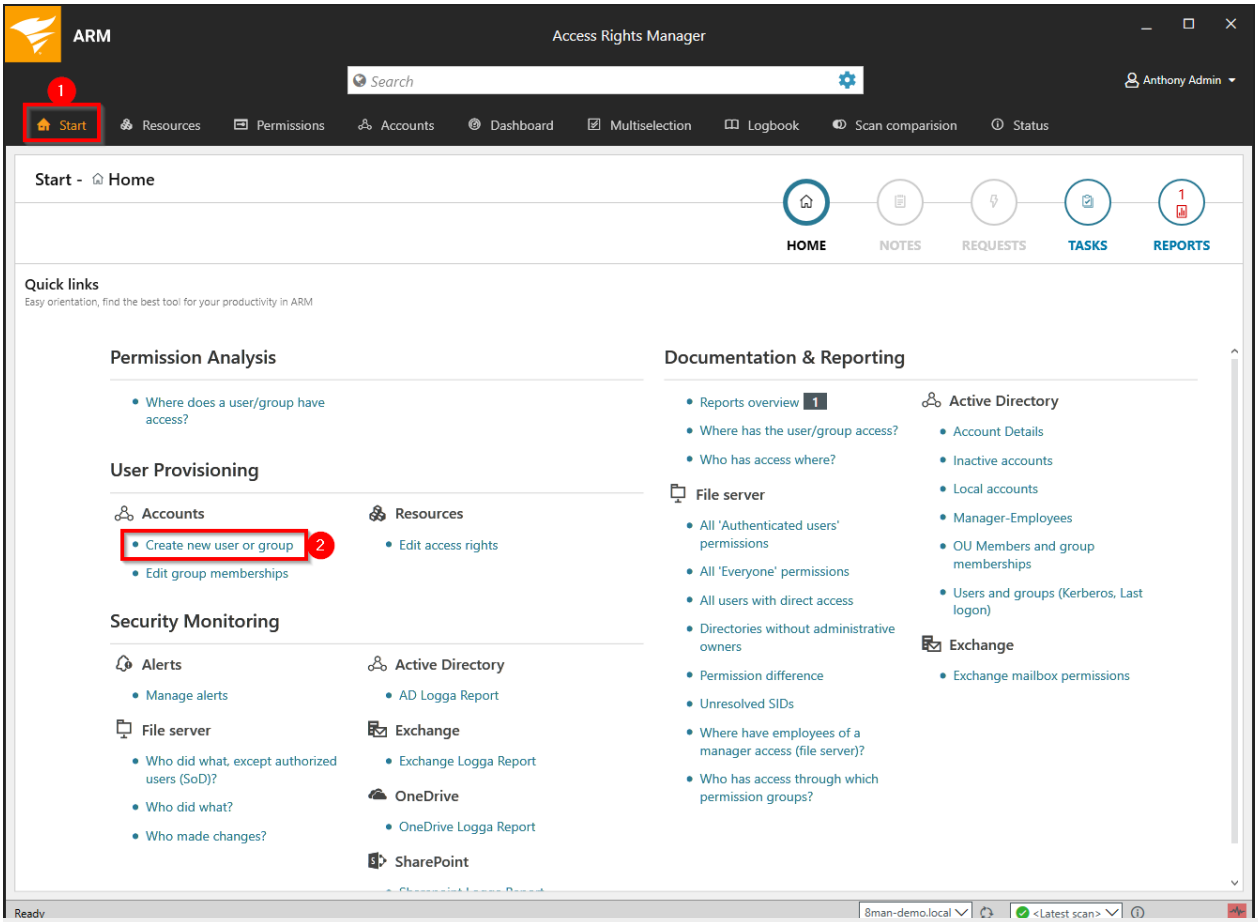
Background / Value

ARM allows you to create standardized groups quickly and easily. Each process is automatically documented.

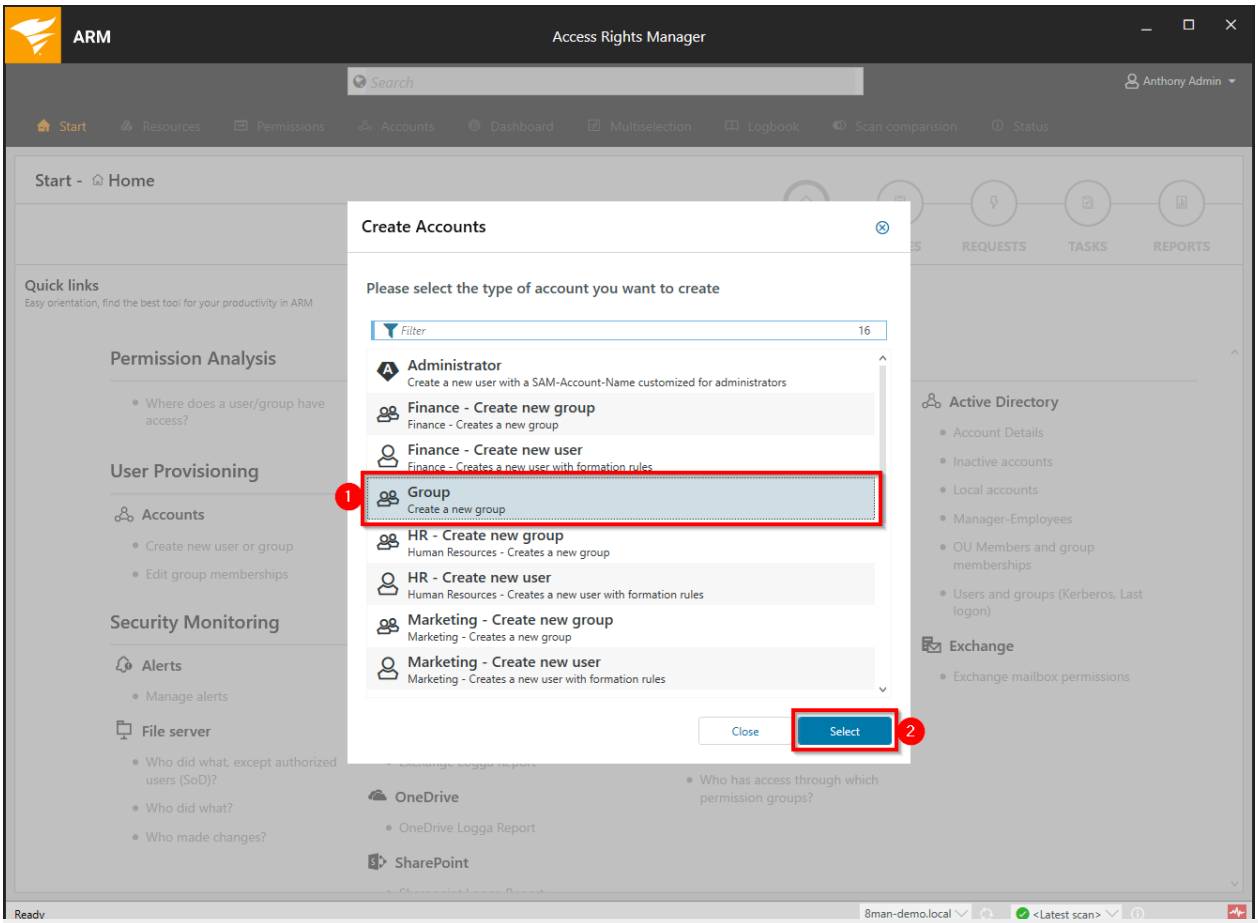
Related features

Manage group memberships

Step-by-step process

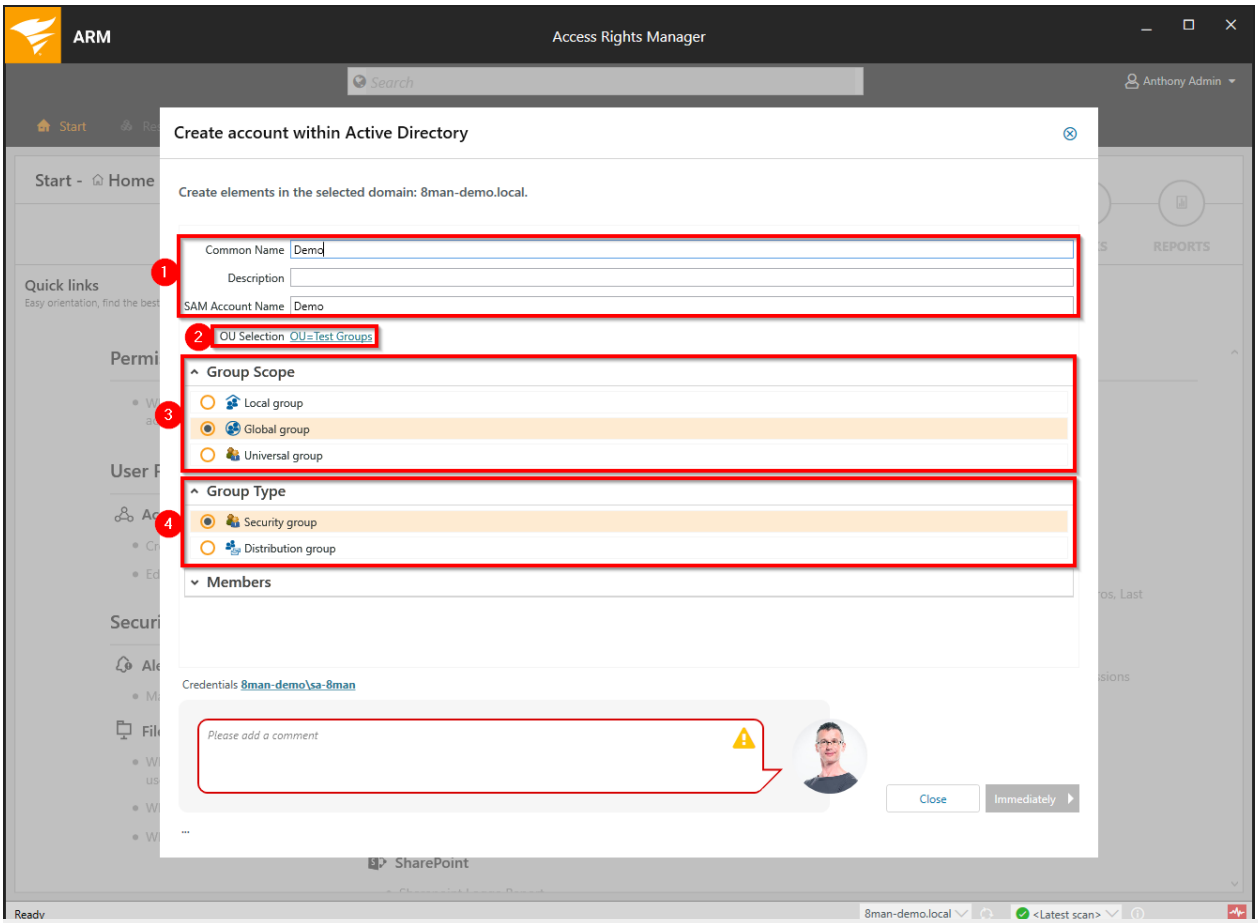


1. Select "Start".
2. Click on "Add a new user account or group".

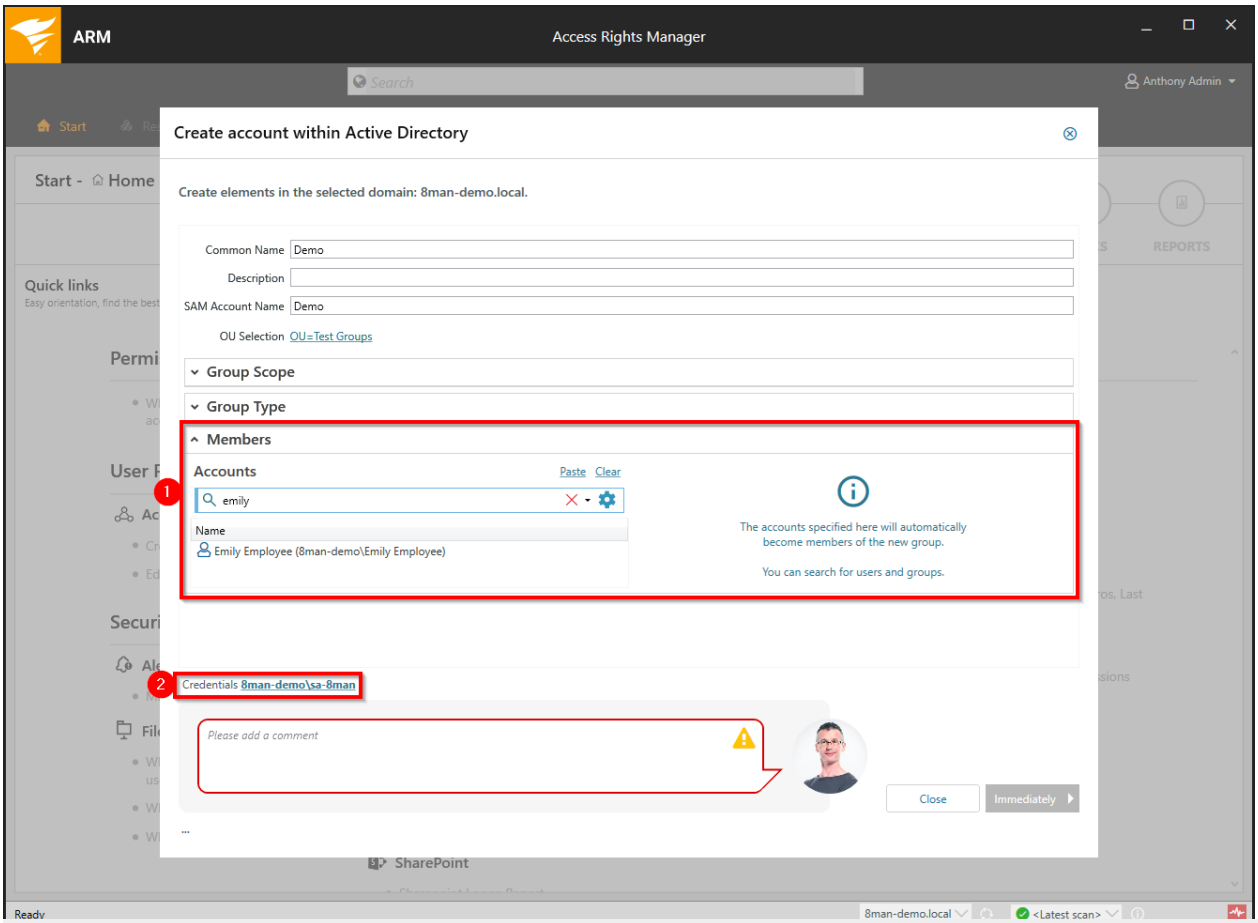


ARM offers 4 standard templates. You can generate as many of your own templates as you wish. We recommend using customized templates as a foundation as this simplifies, standardizes and speeds up the process.

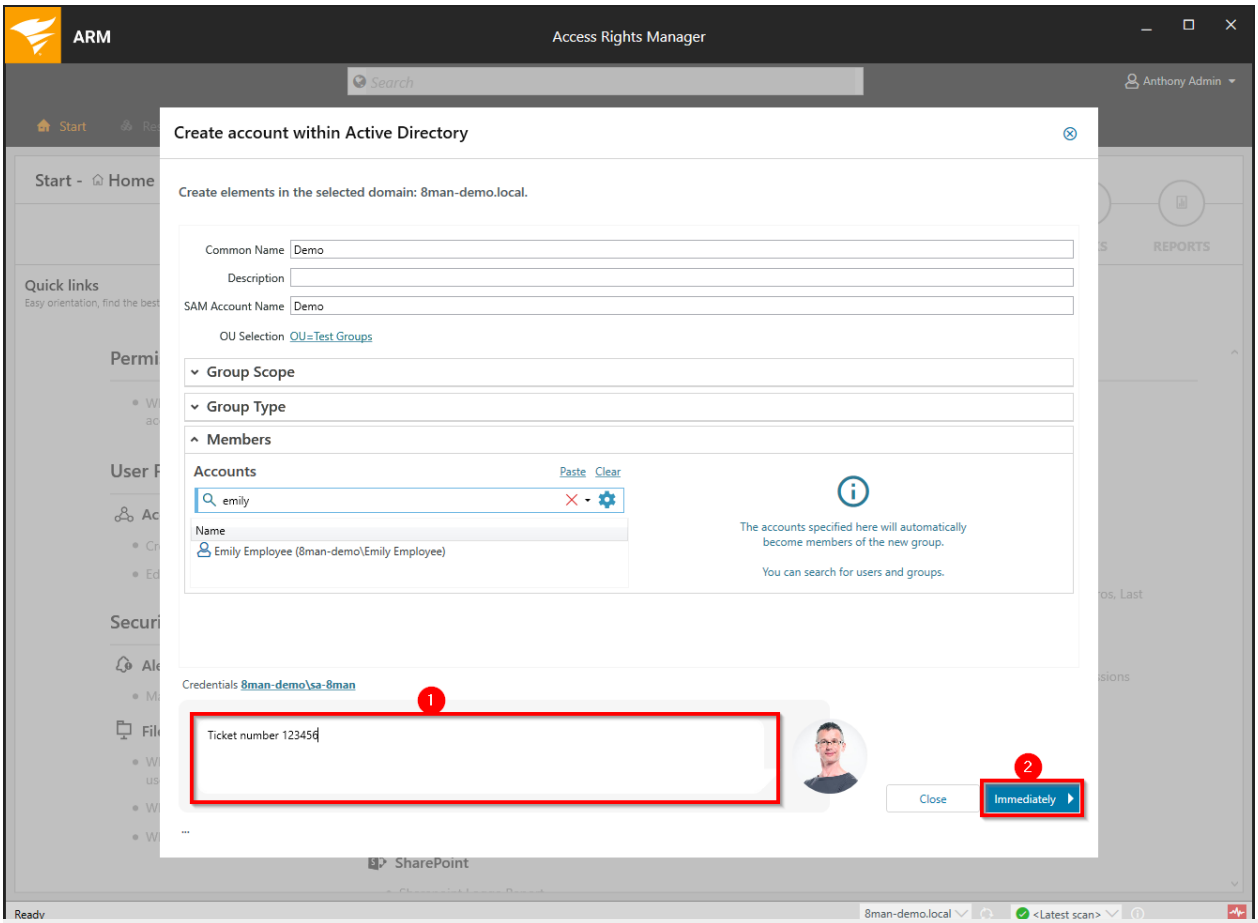
1. Select a group template.
2. Click on "Select".



1. Set the group names and description.
2. Change the OU if desired.
3. Determine the group scope.
4. Determine the group type.



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.

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

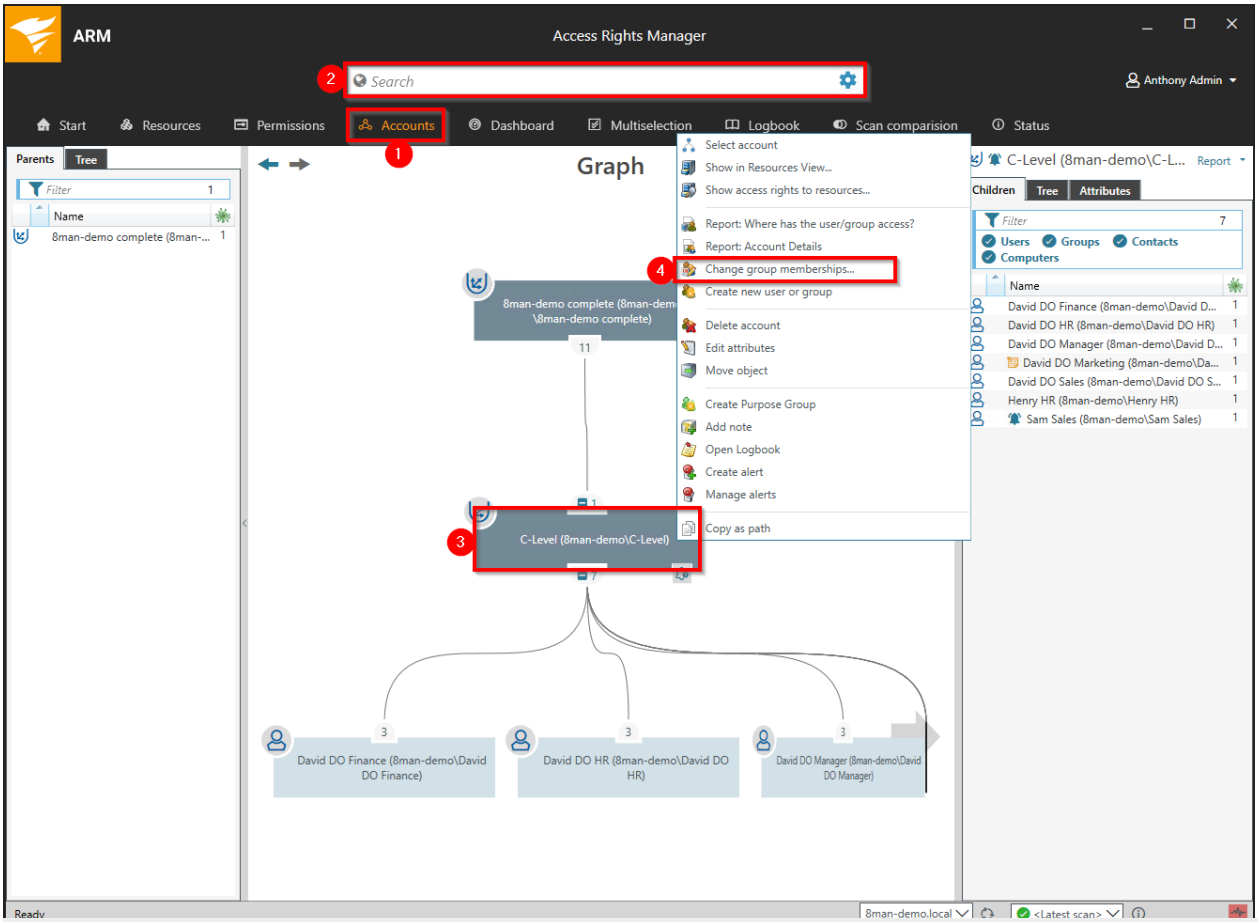
Background / Value

ARM allows you to manage group memberships quickly and easily. You can also easily analyze group nesting.

Related features

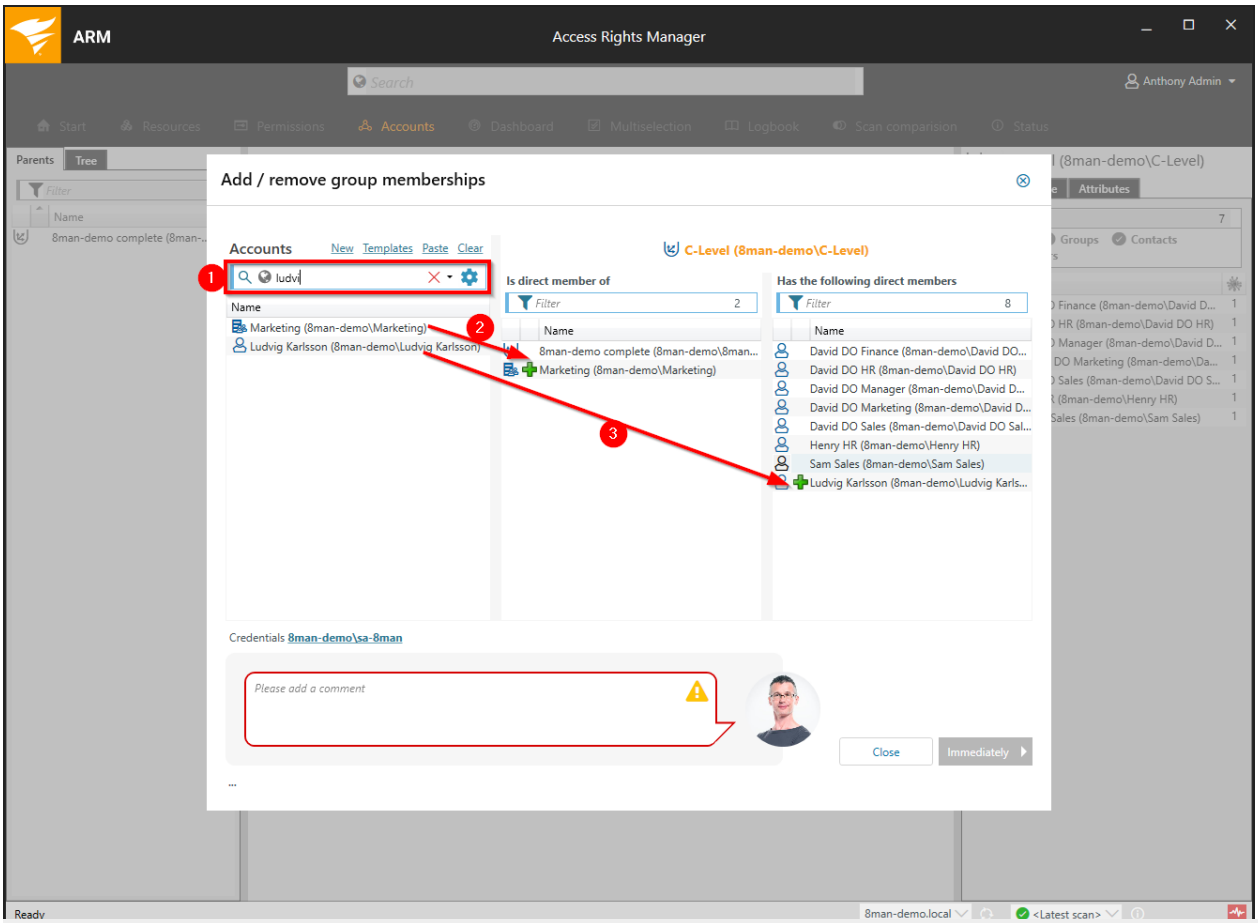
Remove group memberships in bulk (web client)

Step-by-step process

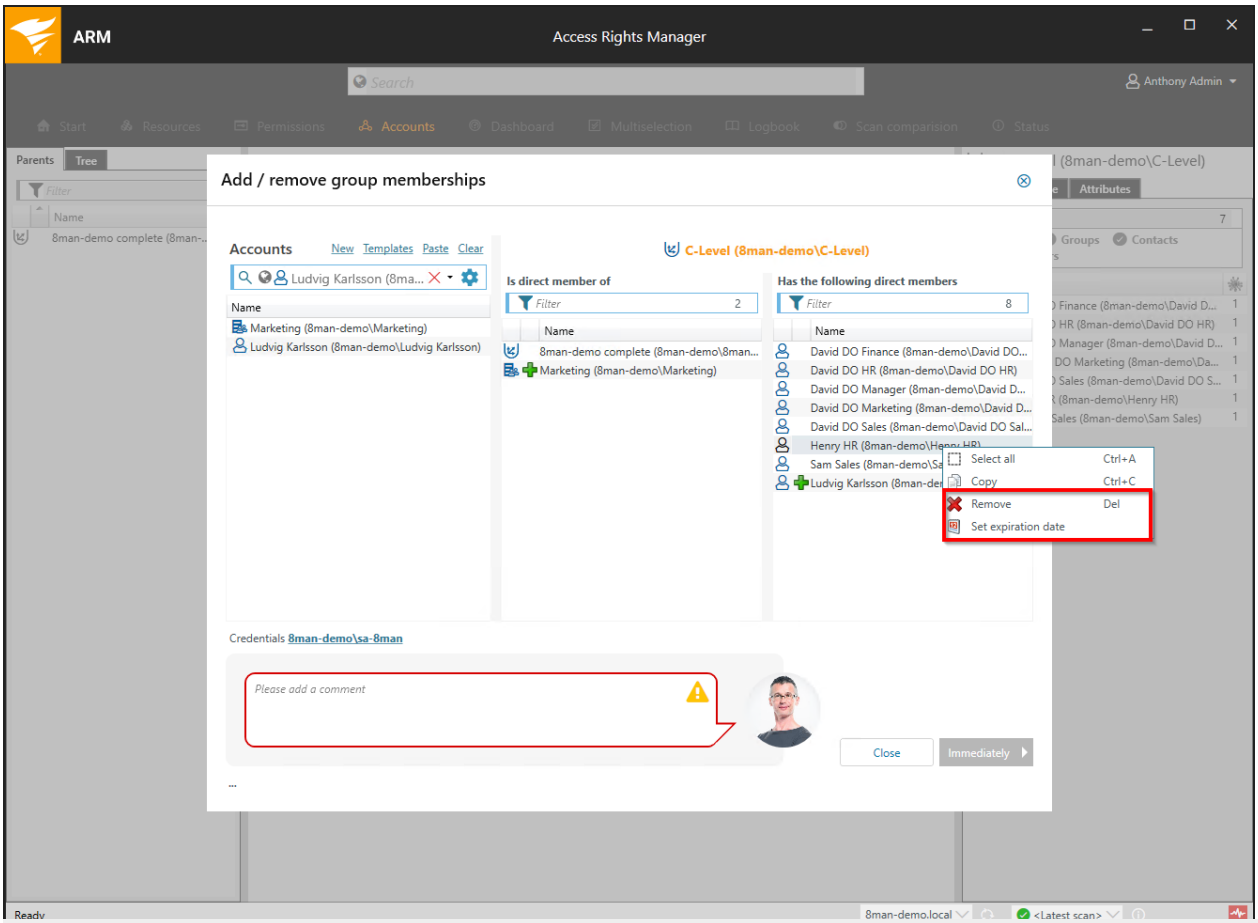


1. Select "Accounts".
2. Use the search field to find the desired account.
3. Right-click on the account.
4. Select "Change group memberships..." in the context menu.

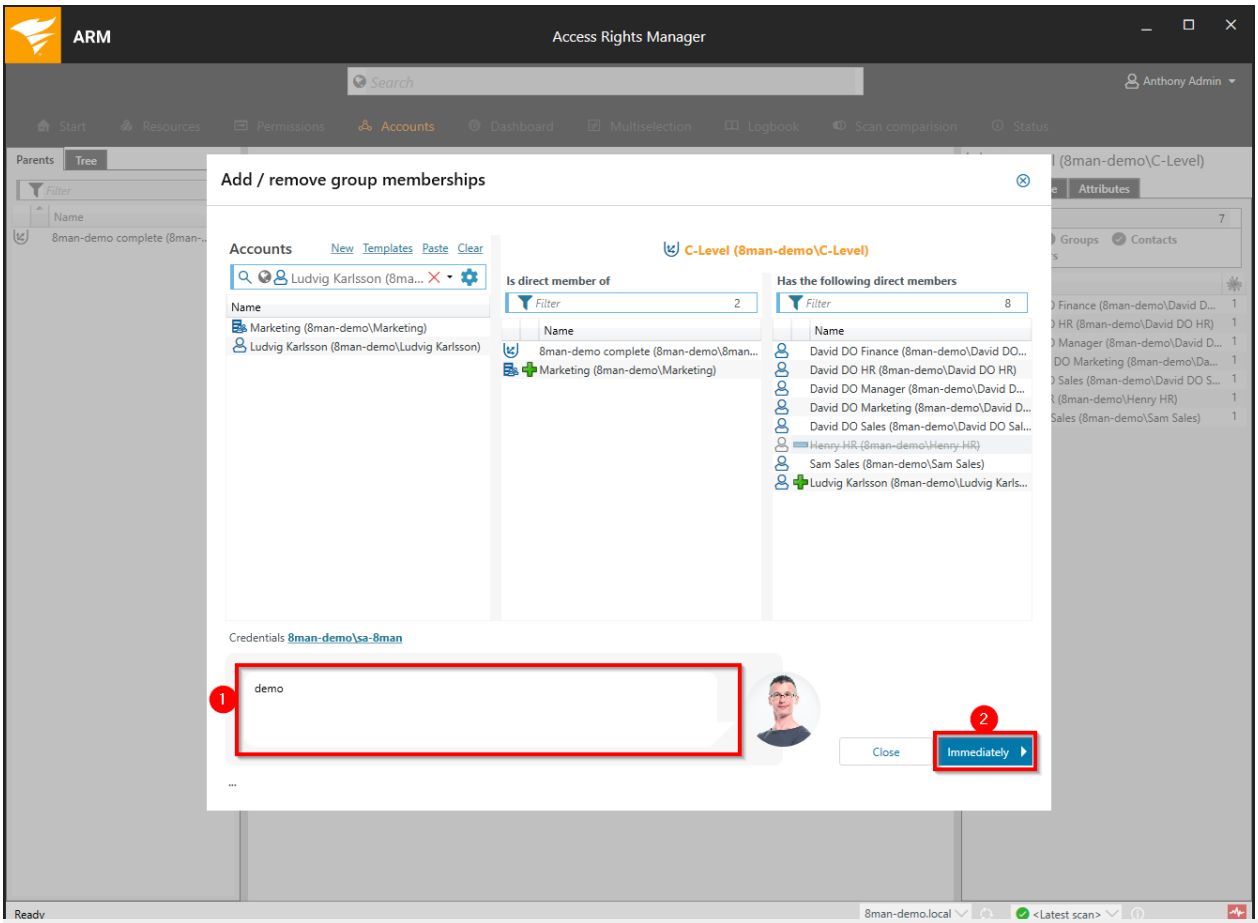
Alternatively you can also use "Edit group memberships" on the ARM home page.



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).



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.

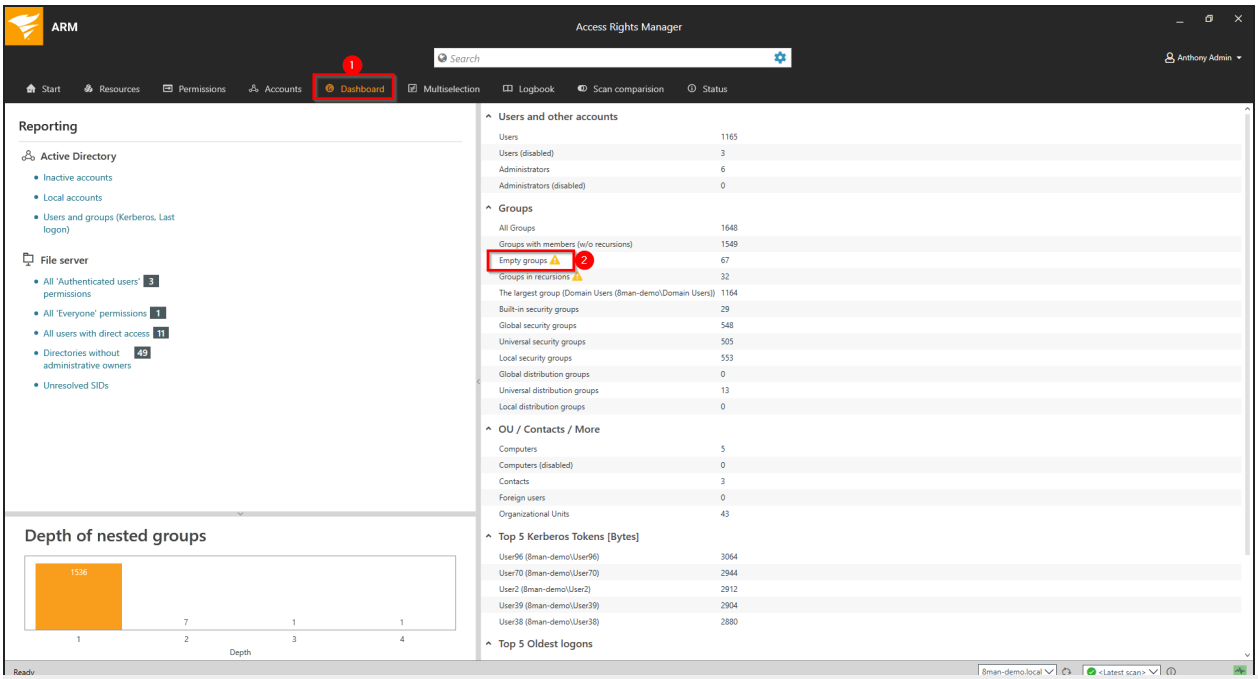
Delete empty groups

Background / Value

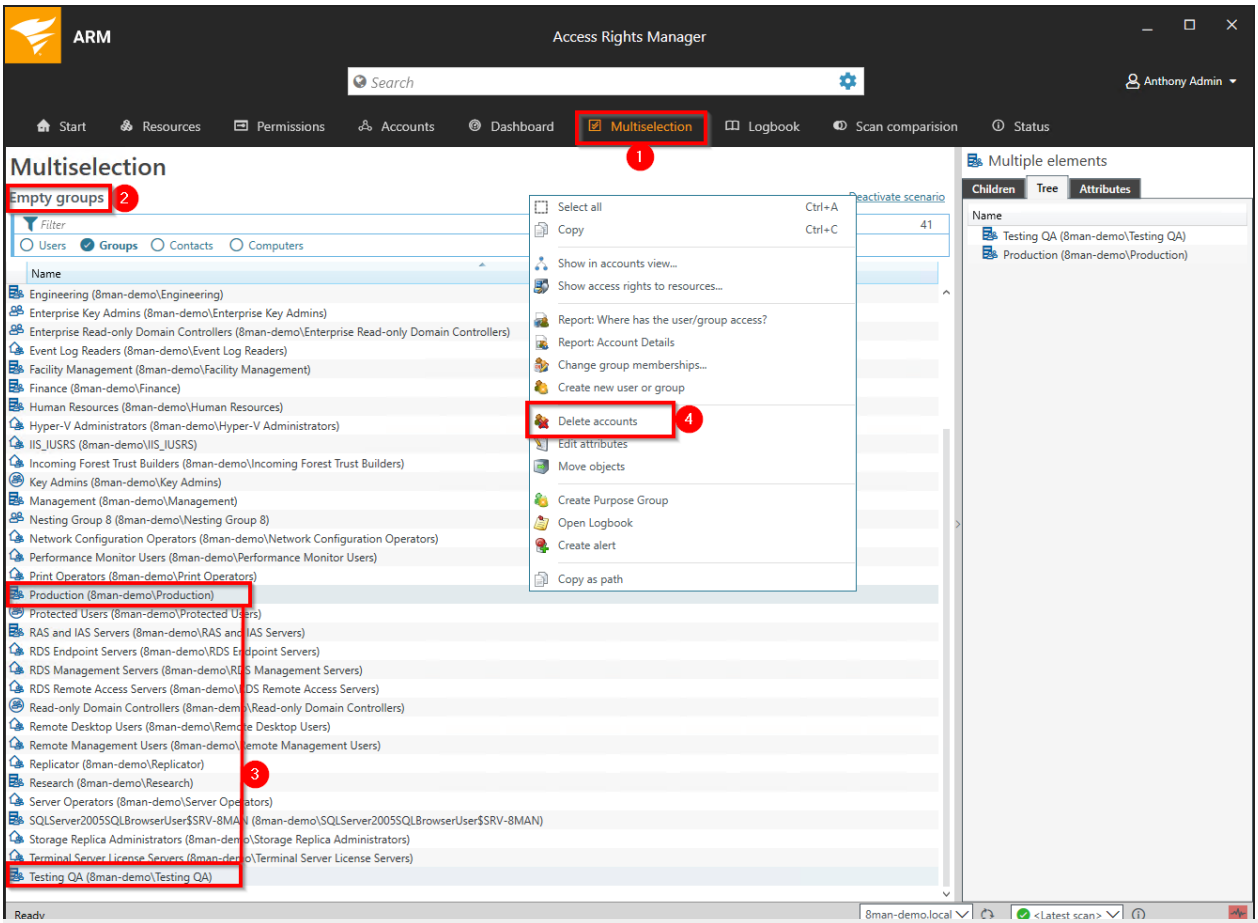
Over time, empty groups accumulate in your Active Directory. These reduce performance and diminish transparency. We recommend deleting these groups.

⚠ Groups without members could be system groups. These should not be deleted.

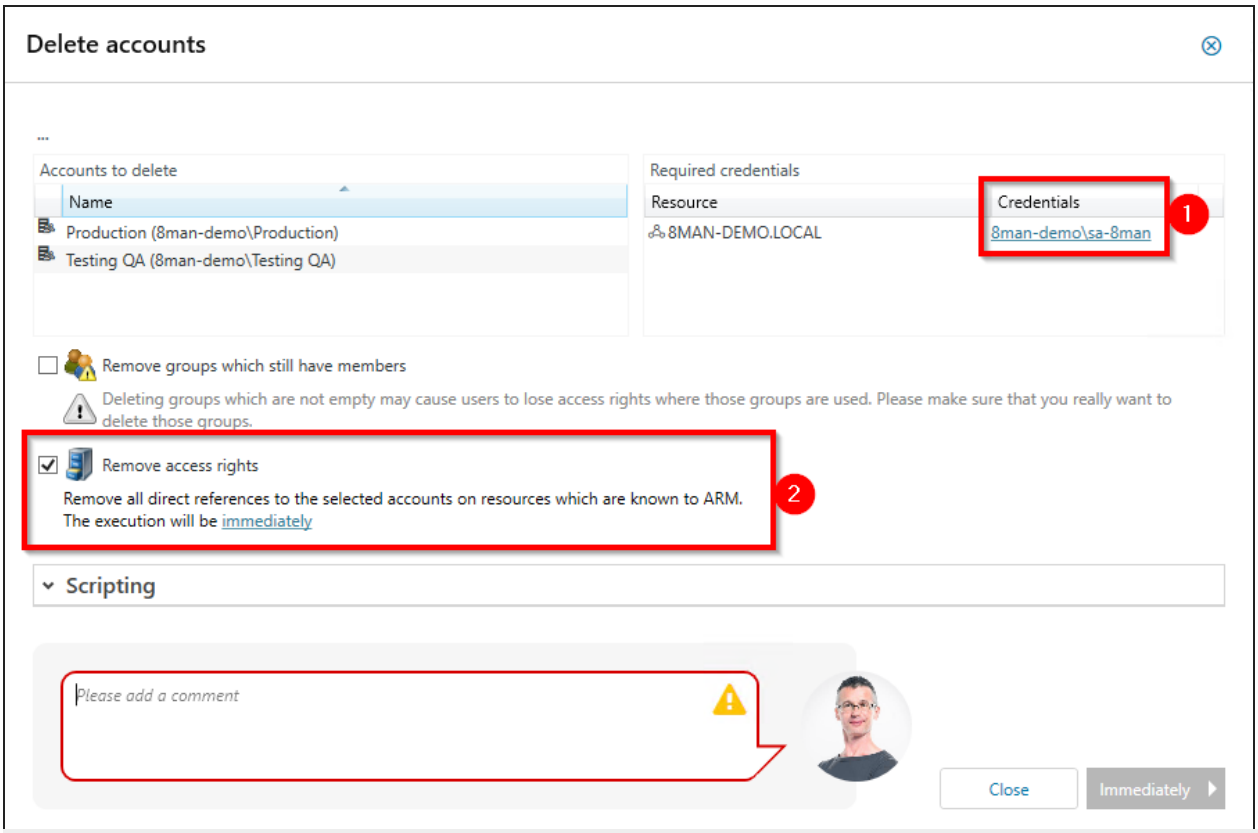
Step-by-step process



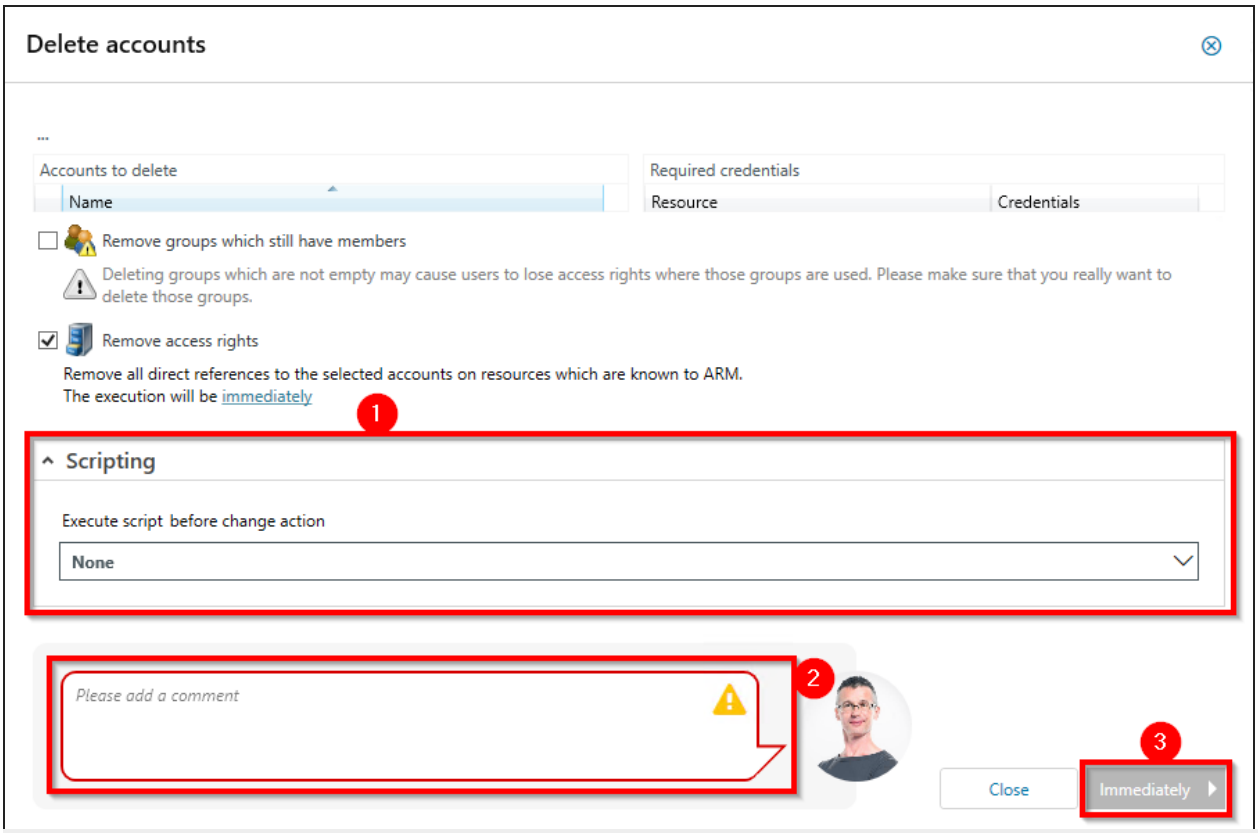
1. Select "Dashboard".
2. Double-click on "Empty groups".



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.



1. Optional: Change the login used to delete the groups in the AD.
2. Recommended: Activate the option "Remove access rights" and prevent the occurance of unresolved SIDs.

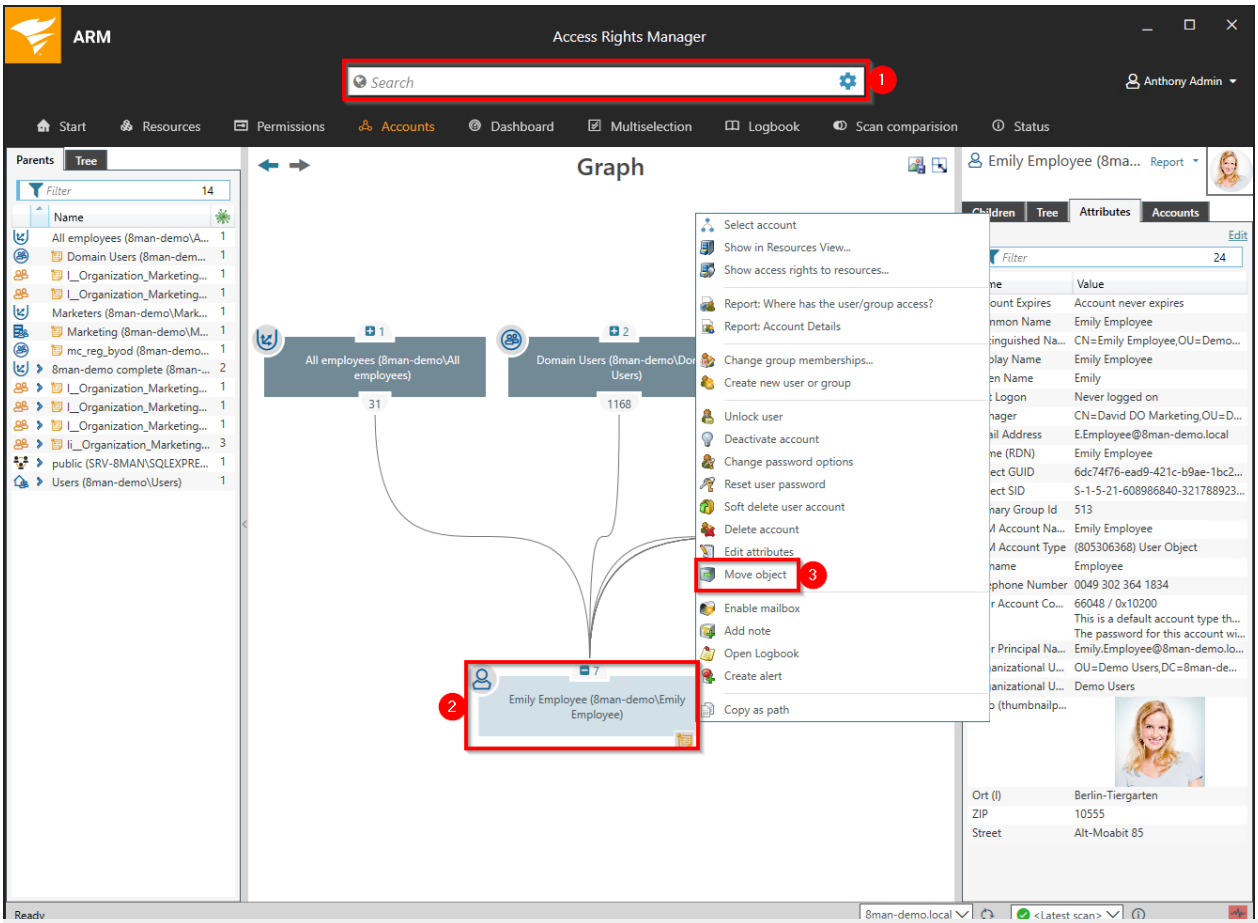


1. Choose whether to run a script before deleting. See also: Configure scripts
2. You must enter a comment.
3. Start the deletion process.

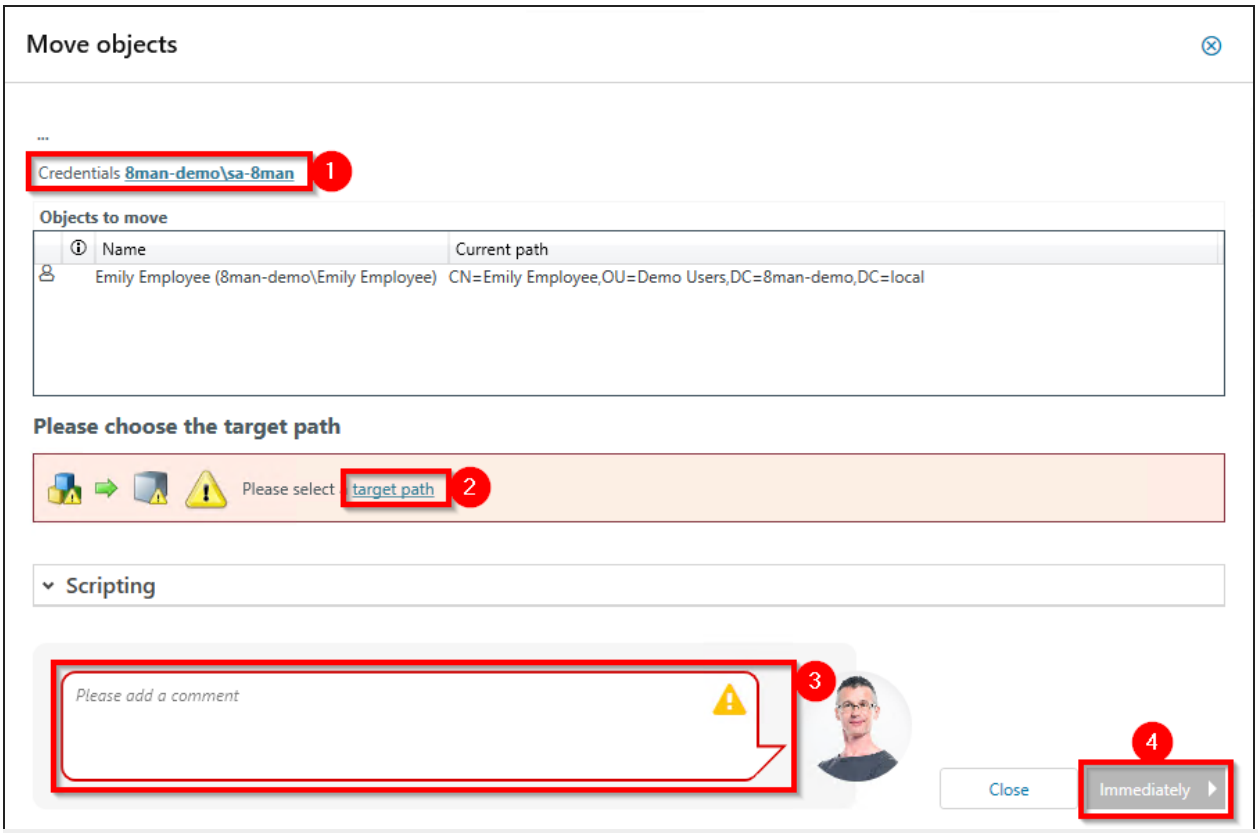
Background / Value

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



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".



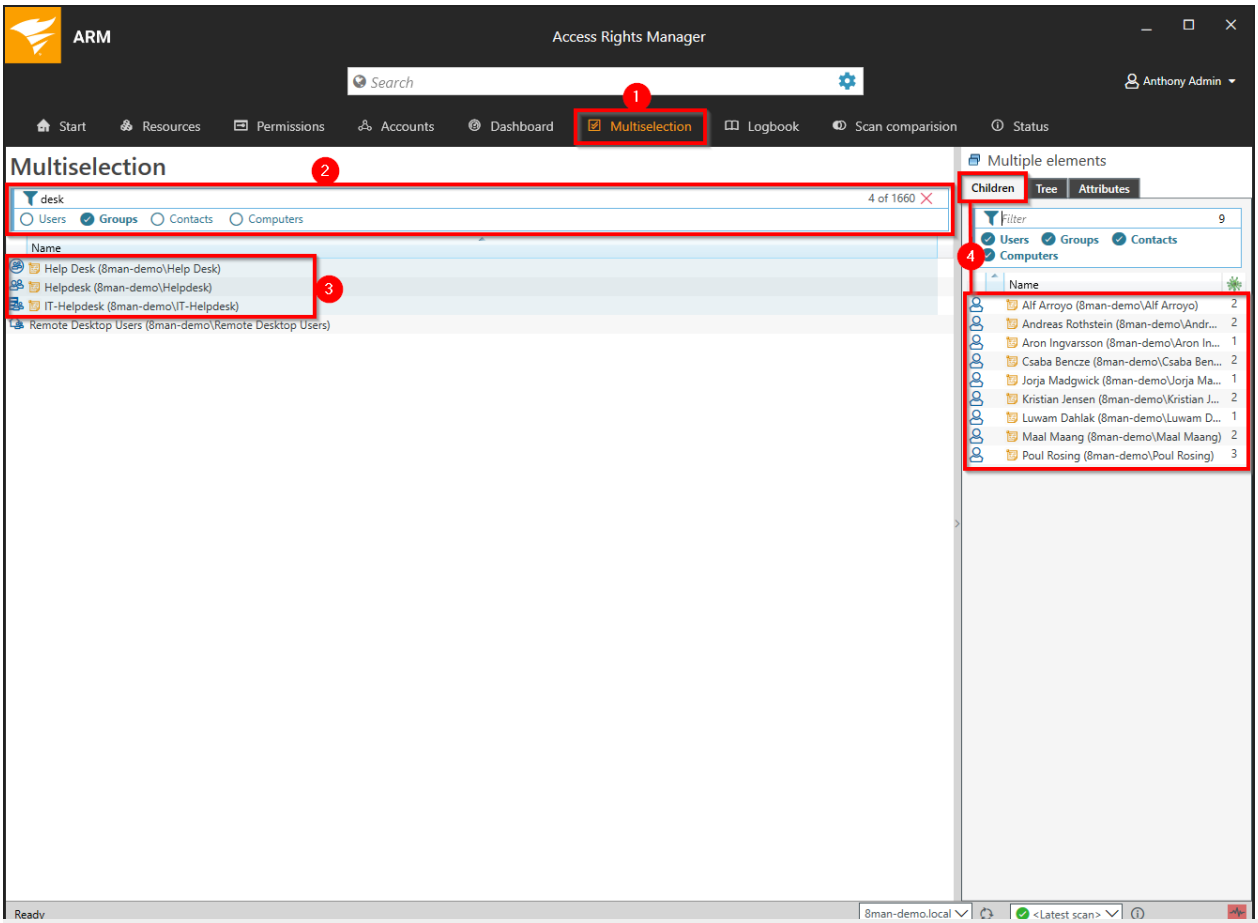
1. If required change the credentials which will be used to move the object.
2. Select a destination.
3. You must enter a comment.
4. Start the process.

Reduce multiple groups to one group

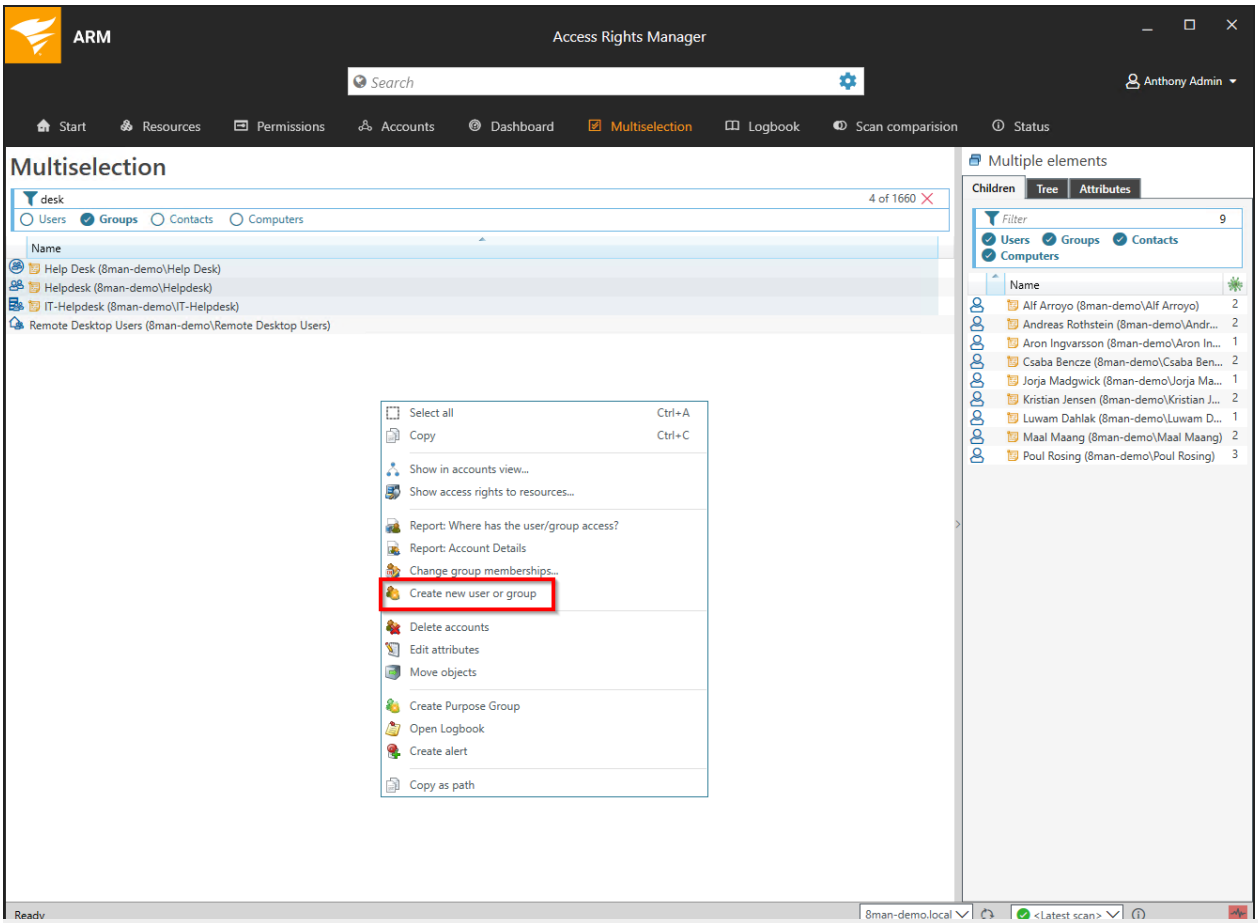
Background / Value

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.

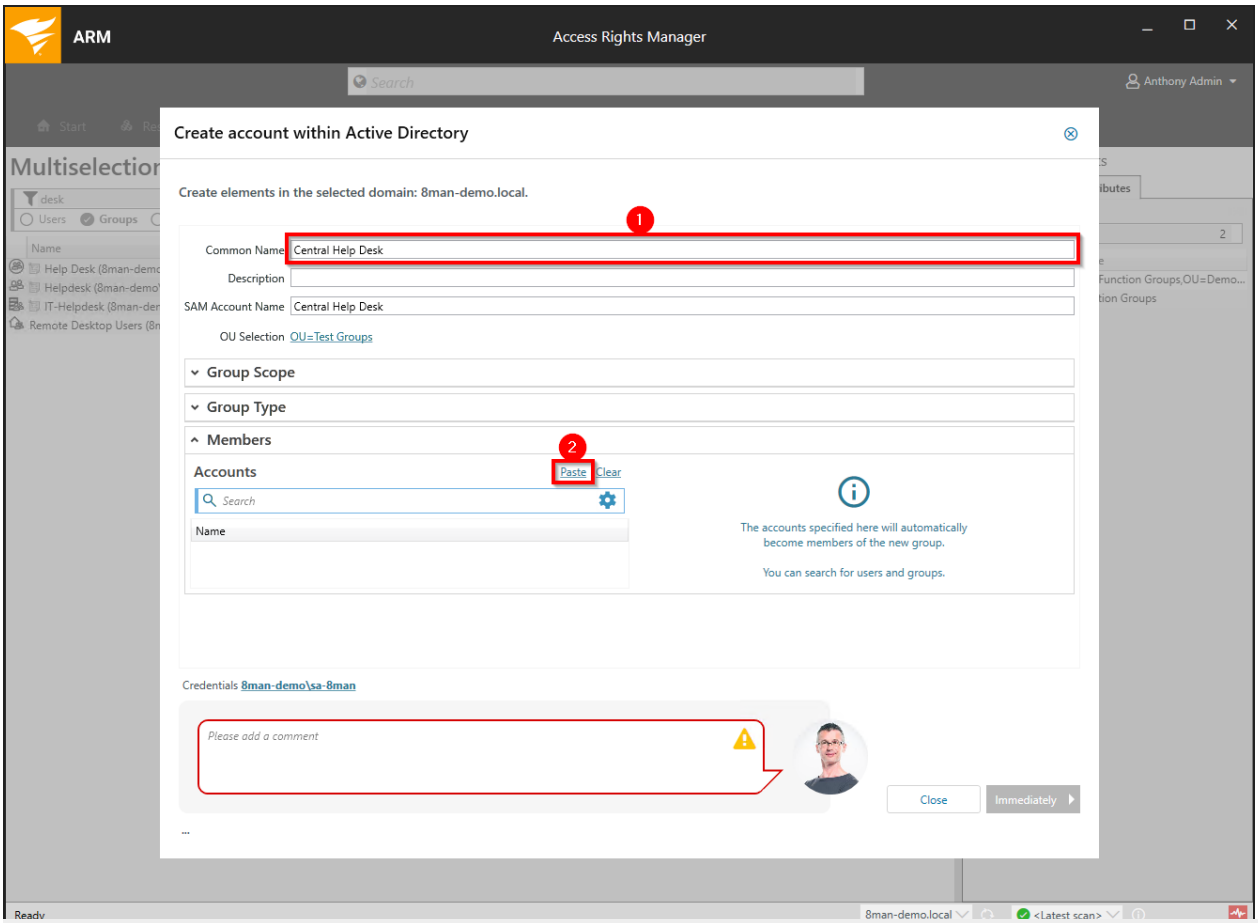
Step-by-step process



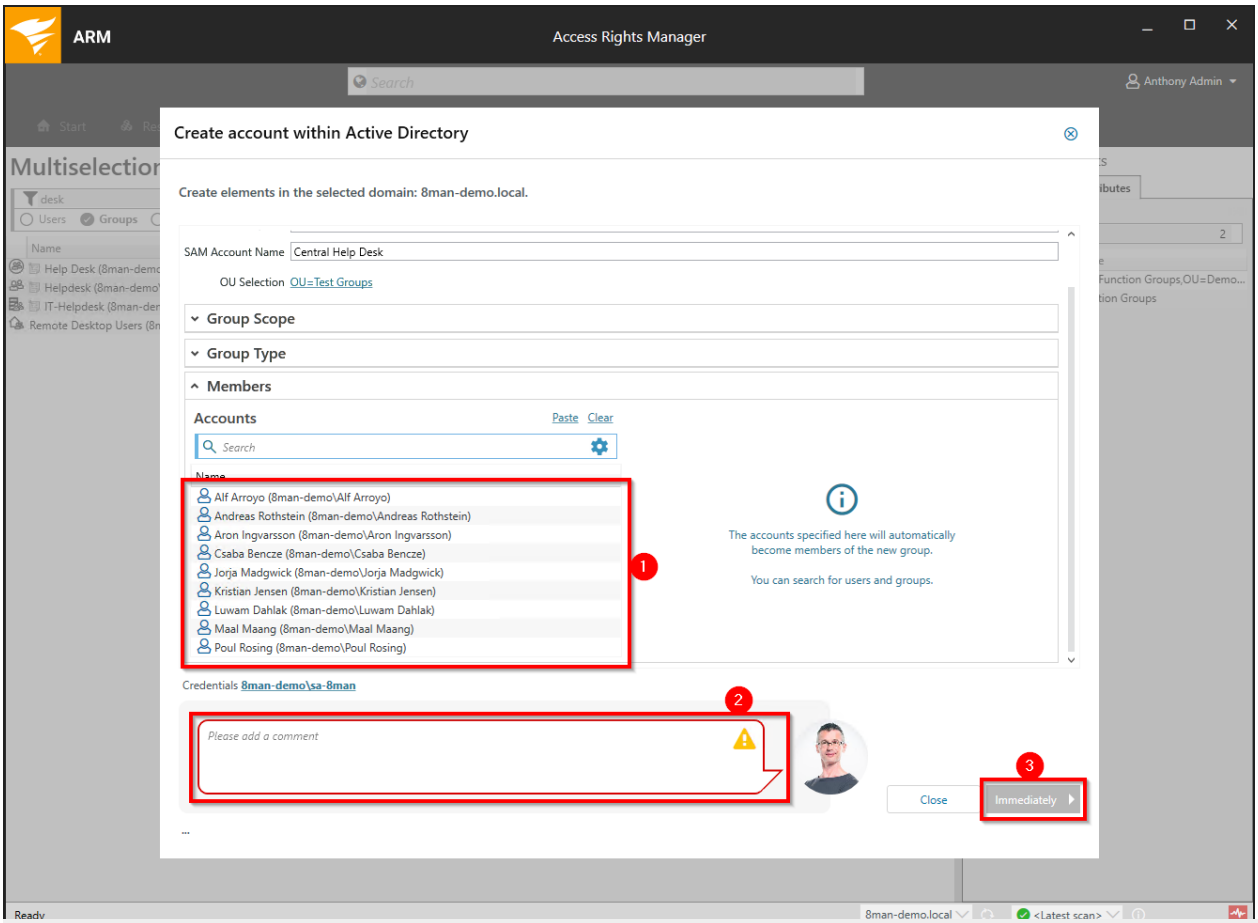
1. Select "Multiselection".
2. Apply filters to find the desired groups.
3. Select the groups.
4. Select all desired users and copy them into the clipboard. (For example CTRL+A and CTRL+C).



Right-click and select "Create new user or group".



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.

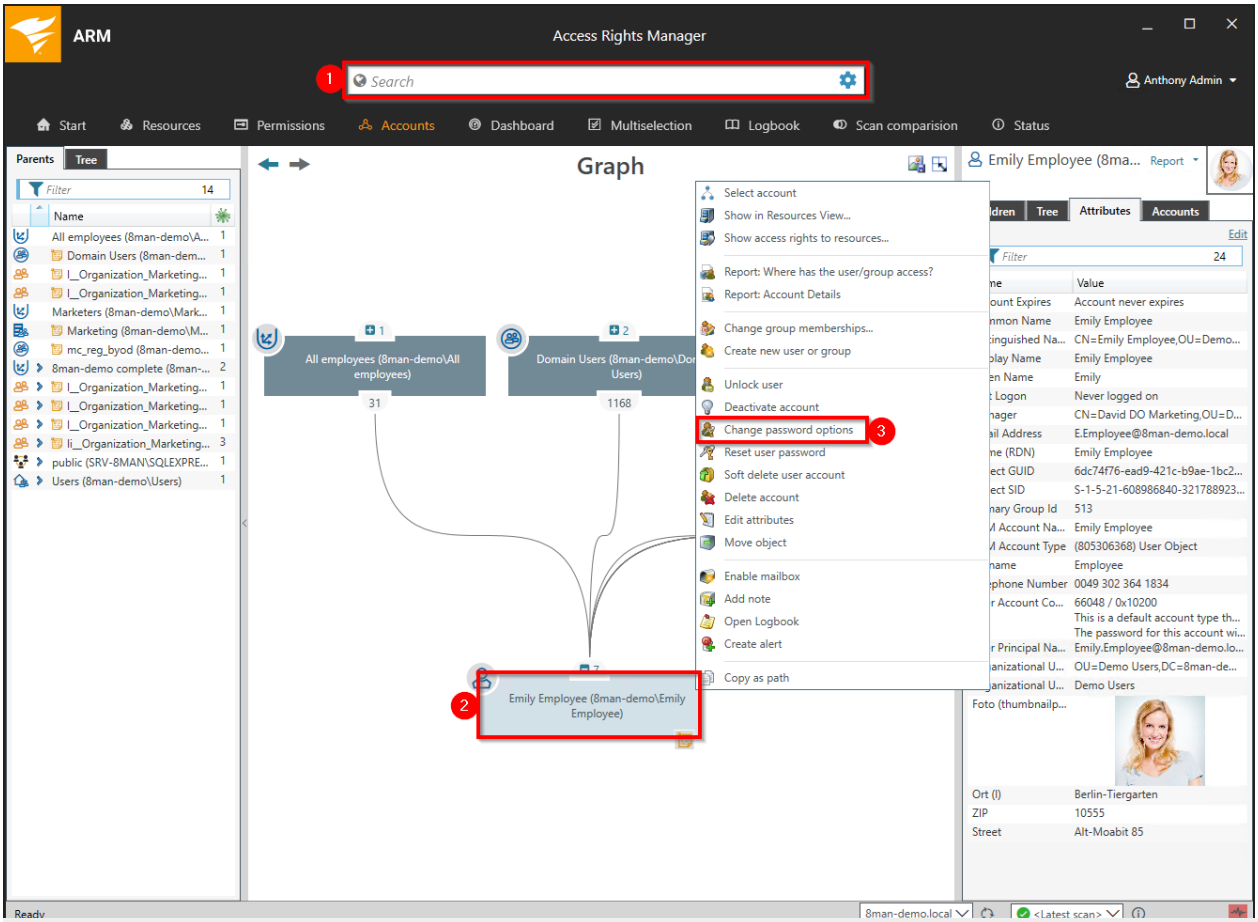
Background/Value

Passwords should be changed regularly. Set the required password options.

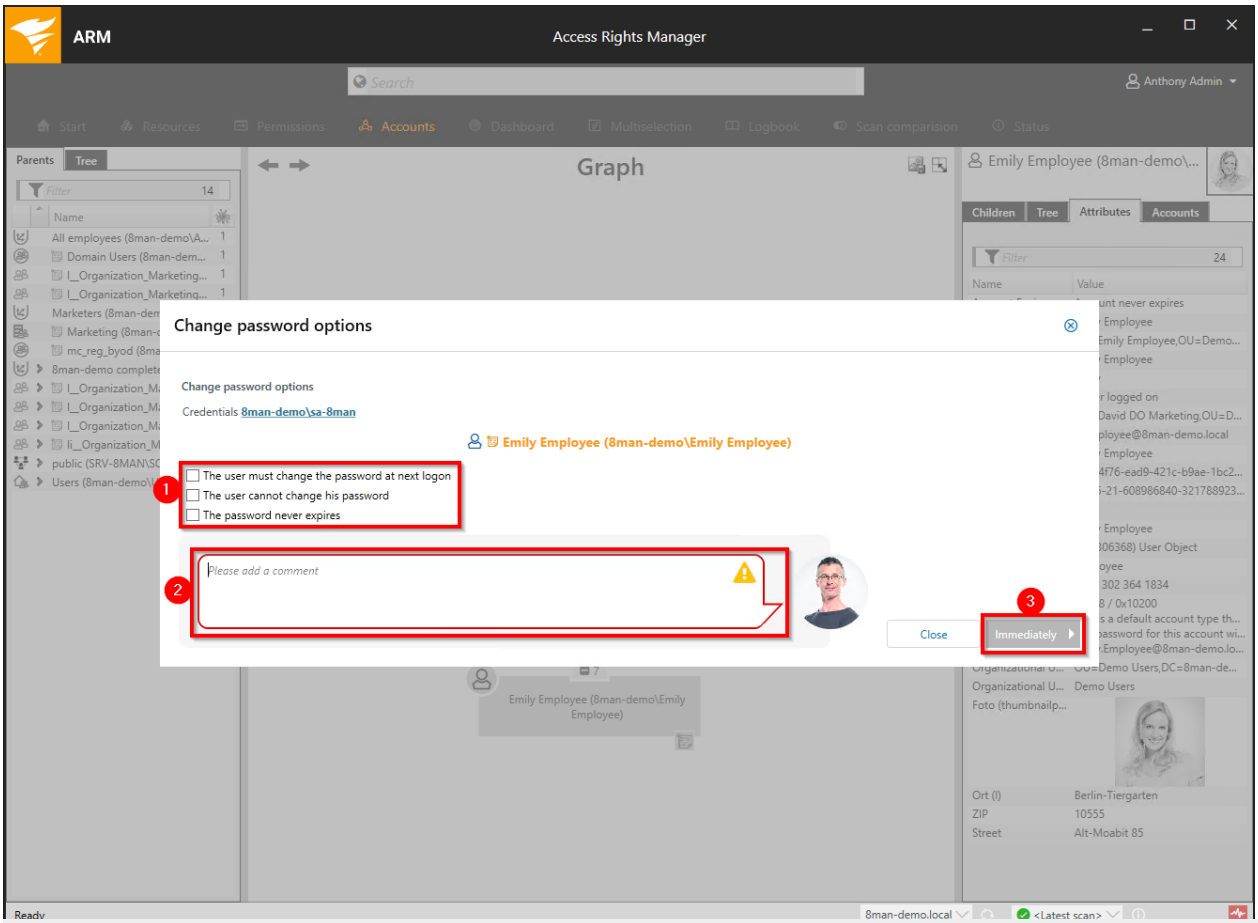
Related features

Change password options in bulk (web client)

Step-by-step process



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

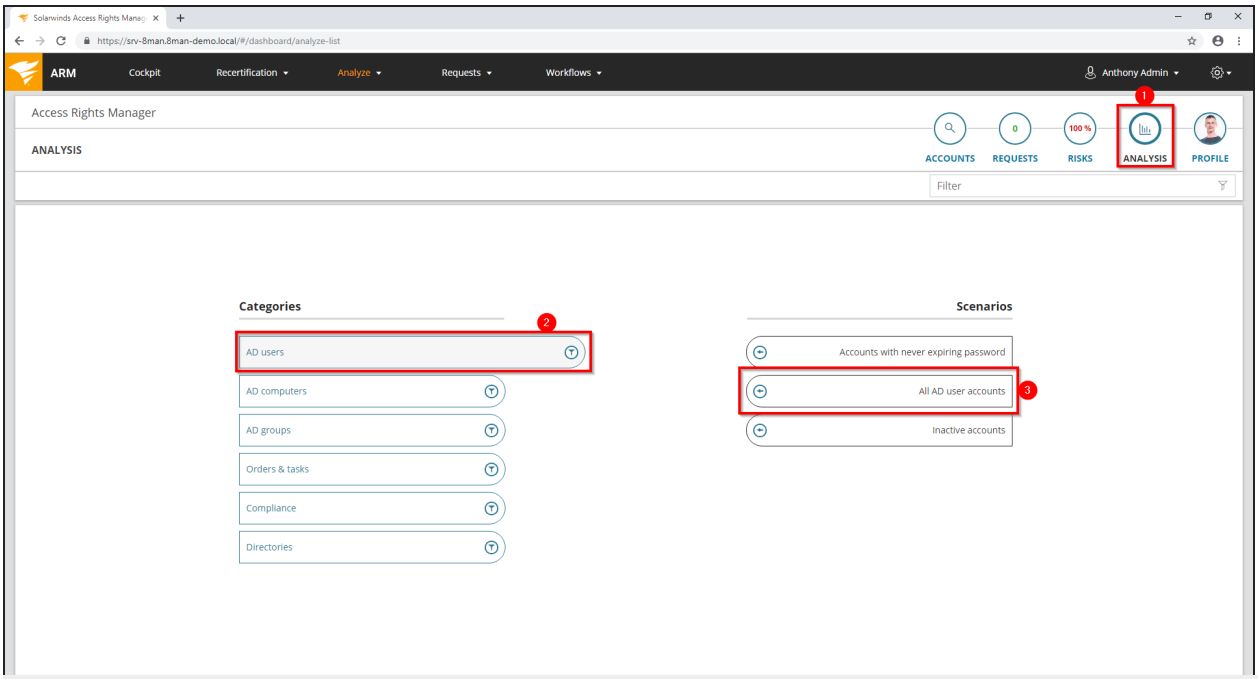
After a security breach it often makes sense to deactivate accounts in bulk. You can do this quickly and easily in the web interface.

Additional Information

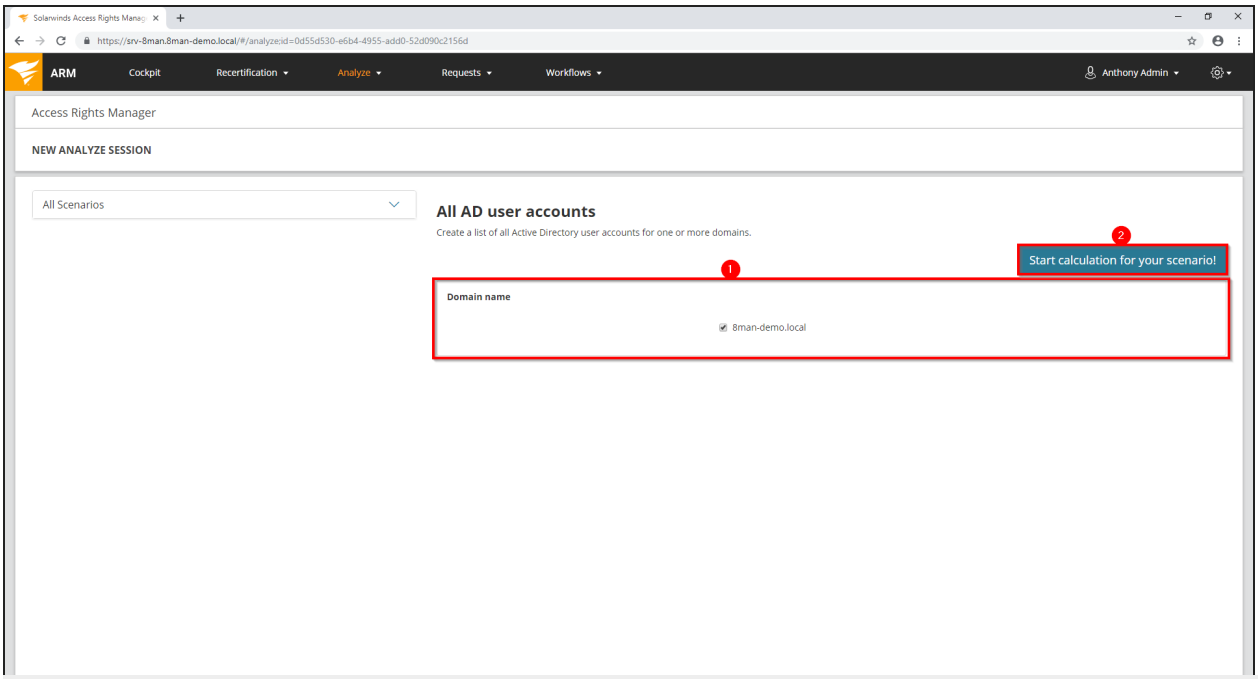
Change password options in bulk (web client)

Delete accounts in bulk (soft delete) (web client)

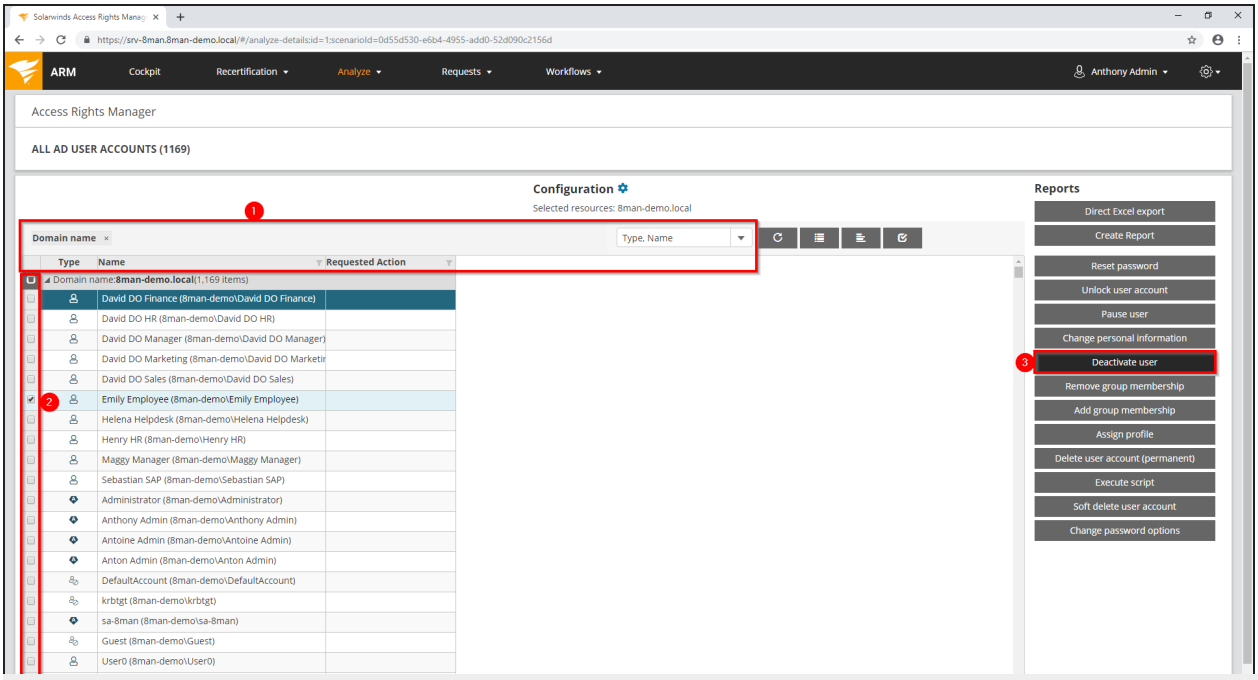
Step-by-step process



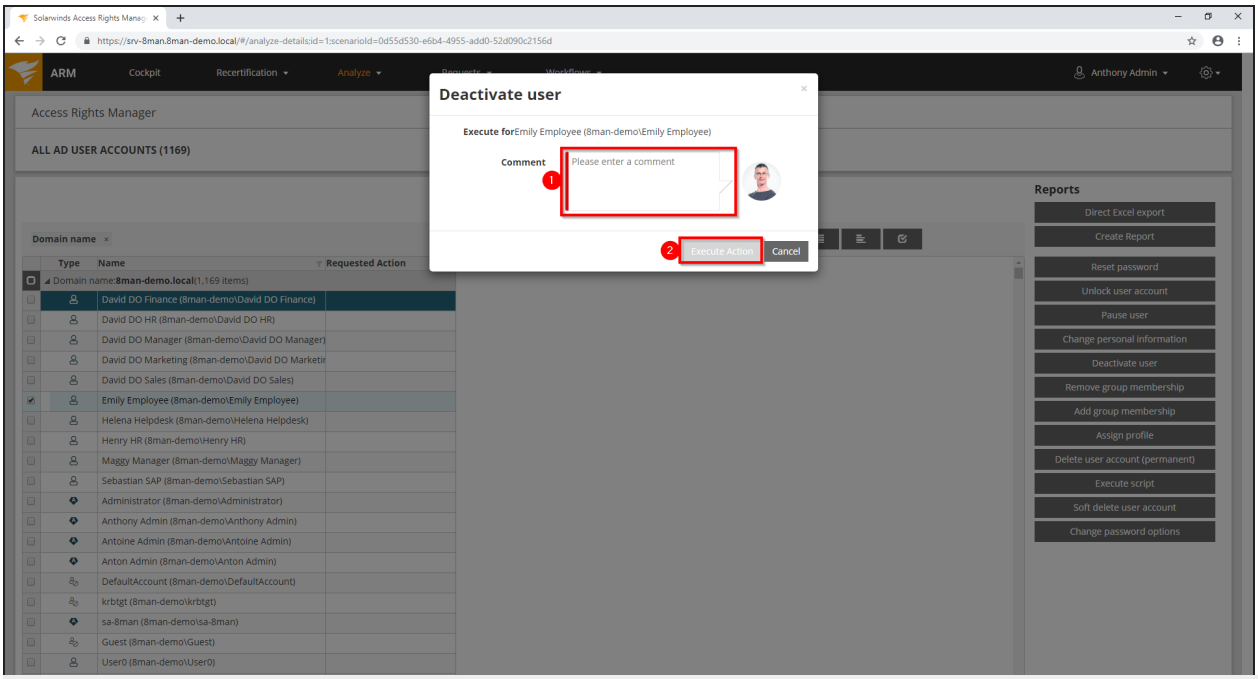
1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".



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 betransferred 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

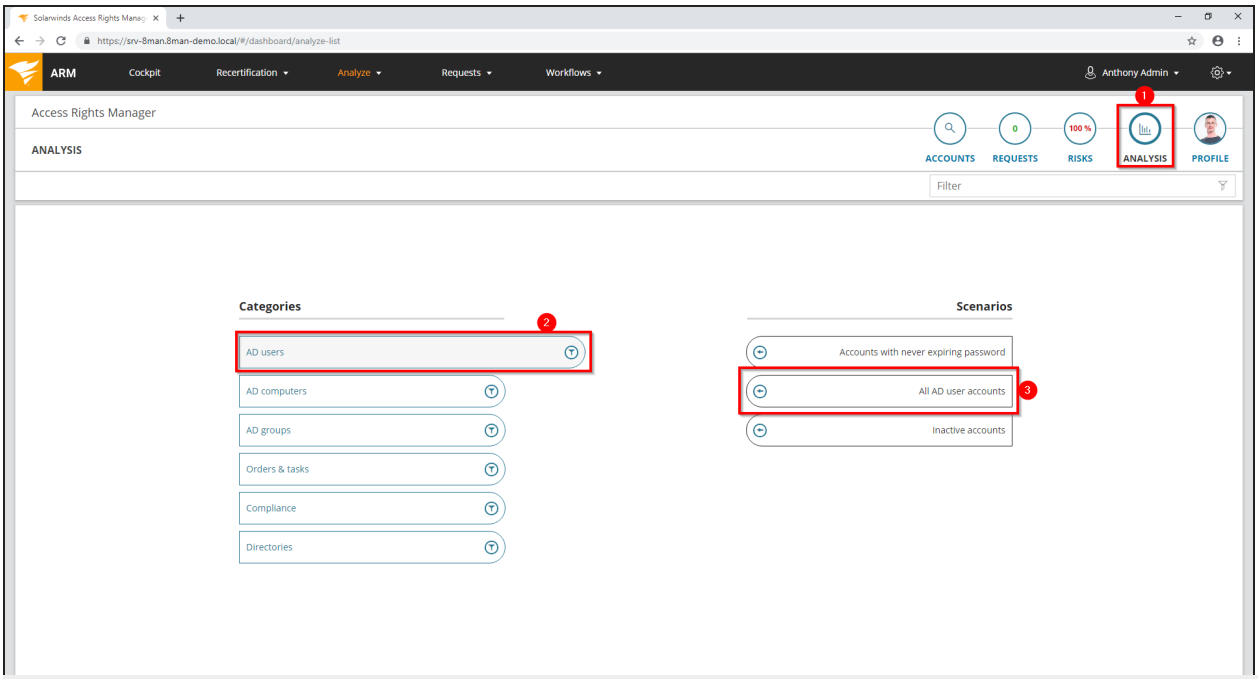
After a security breach or the dissolution of a department, it makes sense to delete several accounts at the same time. Do this conveniently in the web client.

Related features

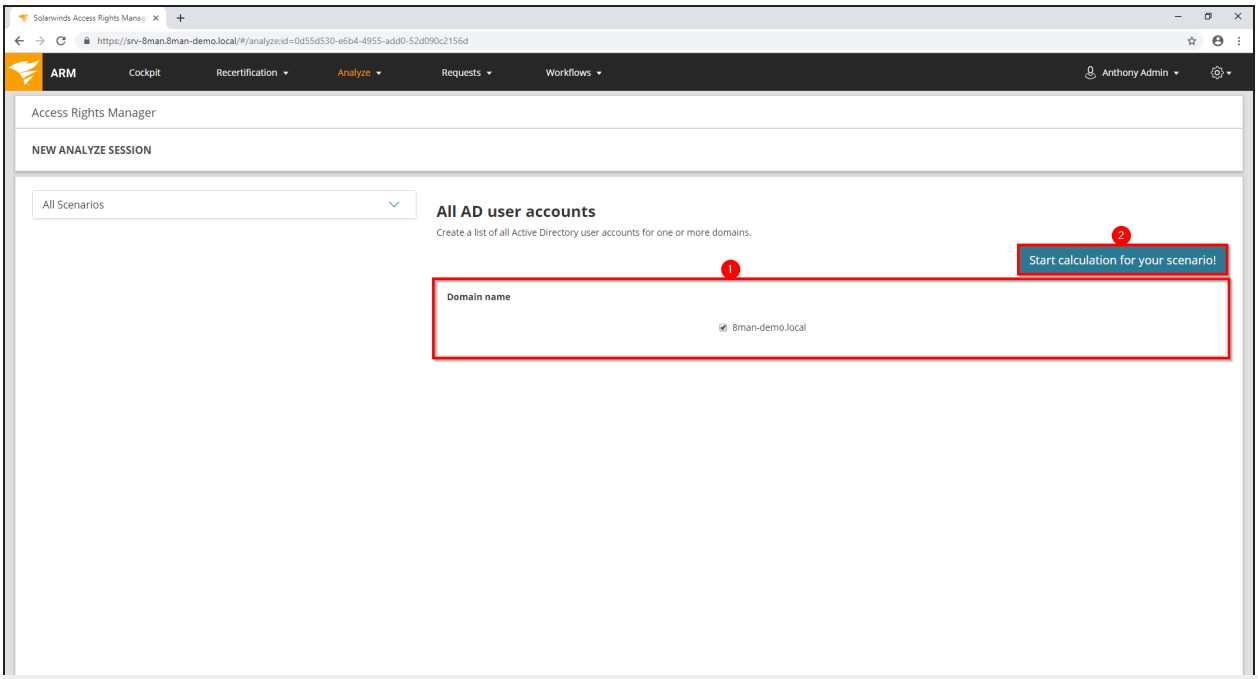
Change password options in bulk (web client)

Delete accounts in bulk (soft delete) (web client)

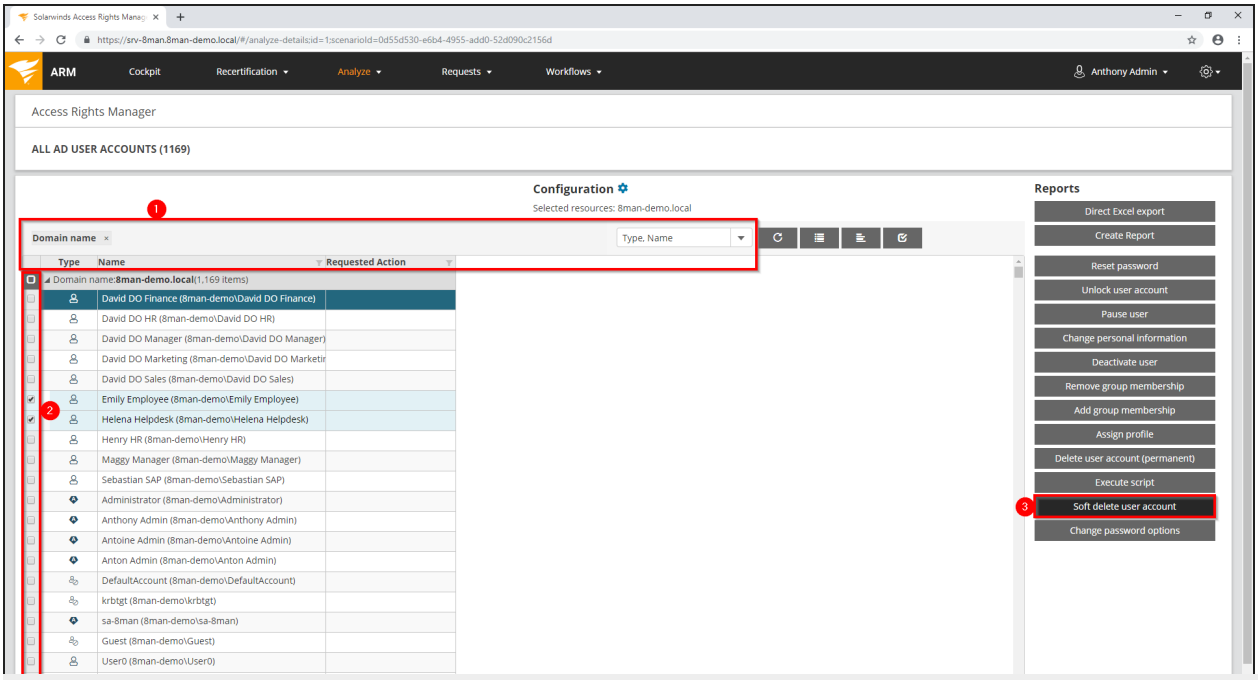
Step-by-step process



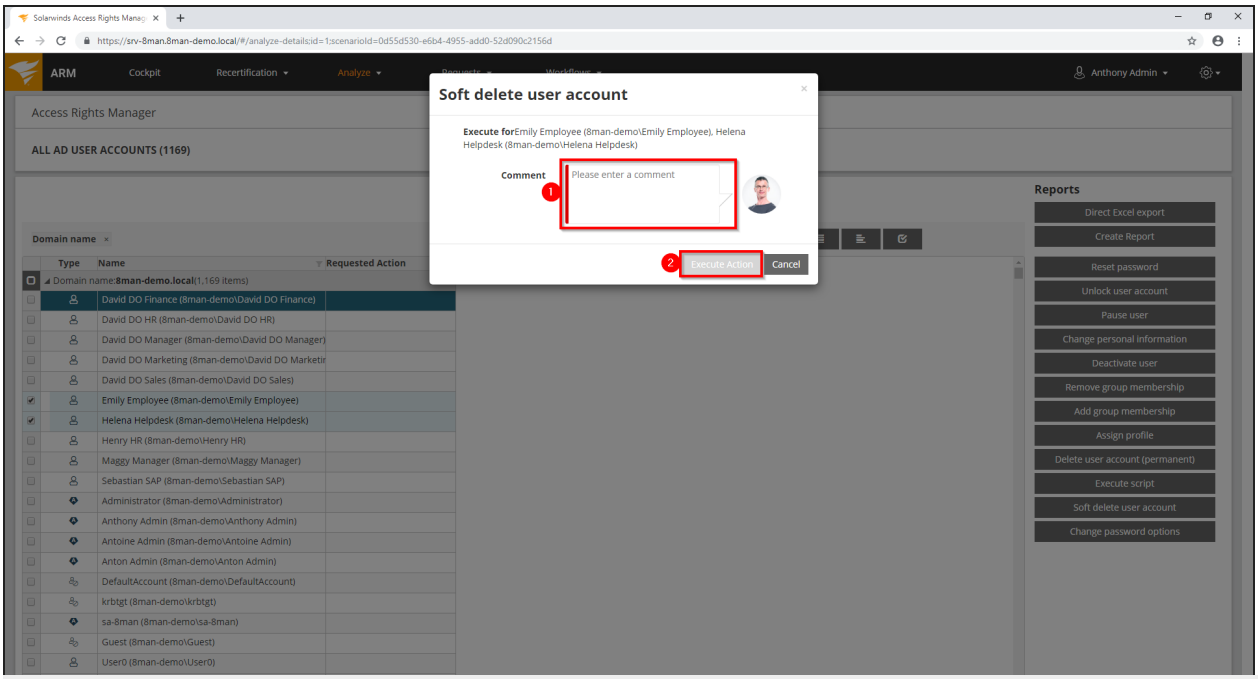
1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".



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)

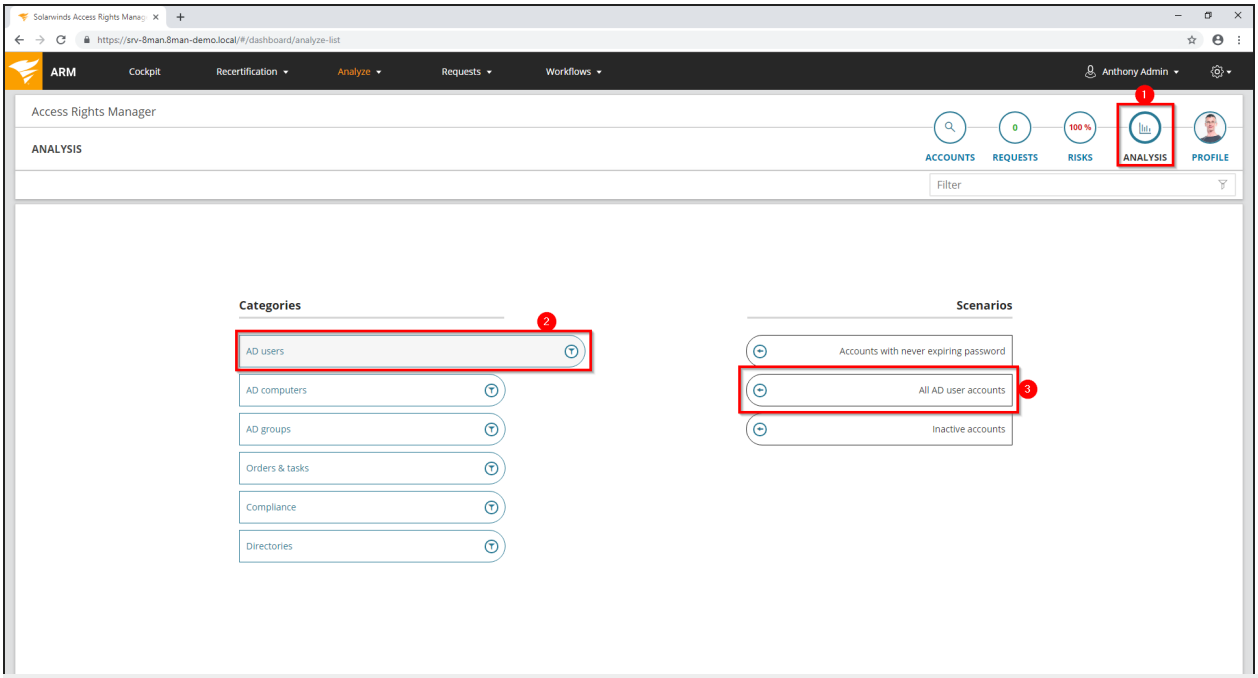
Background / Value

Passwords must be changed regularly. You can manage password options across your entire organization, quickly and easily in the ARM web interface.

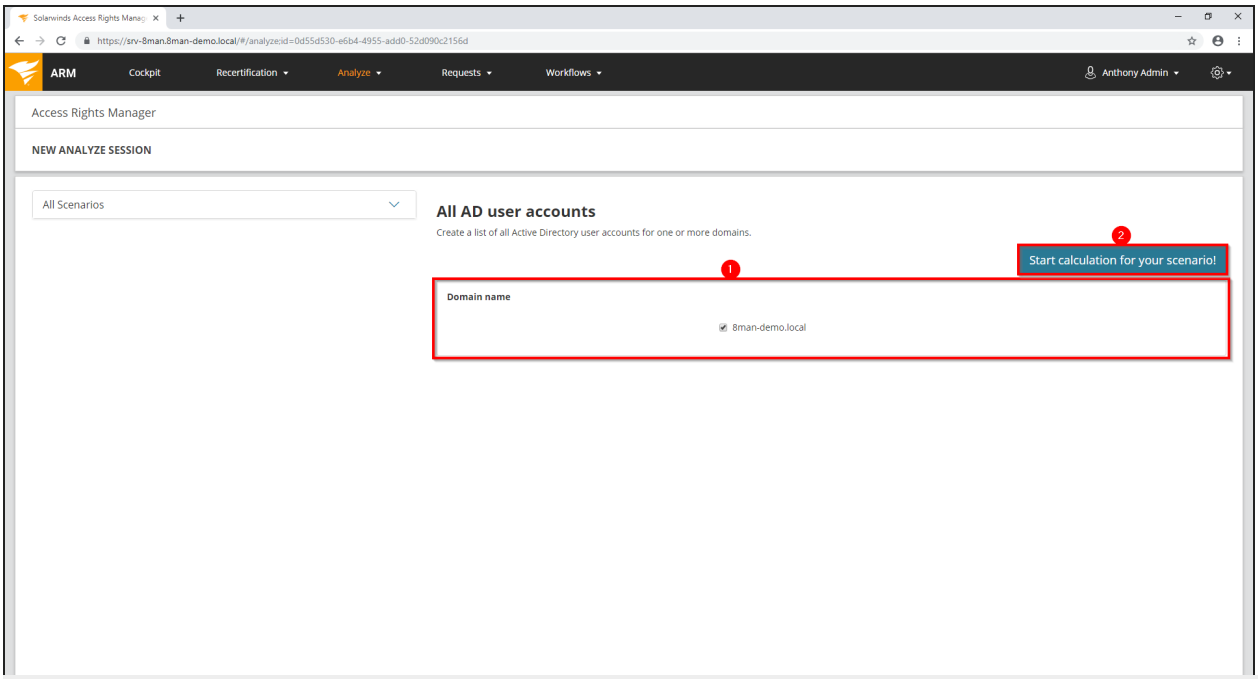
Related features

Reset passwords in bulk (web client)

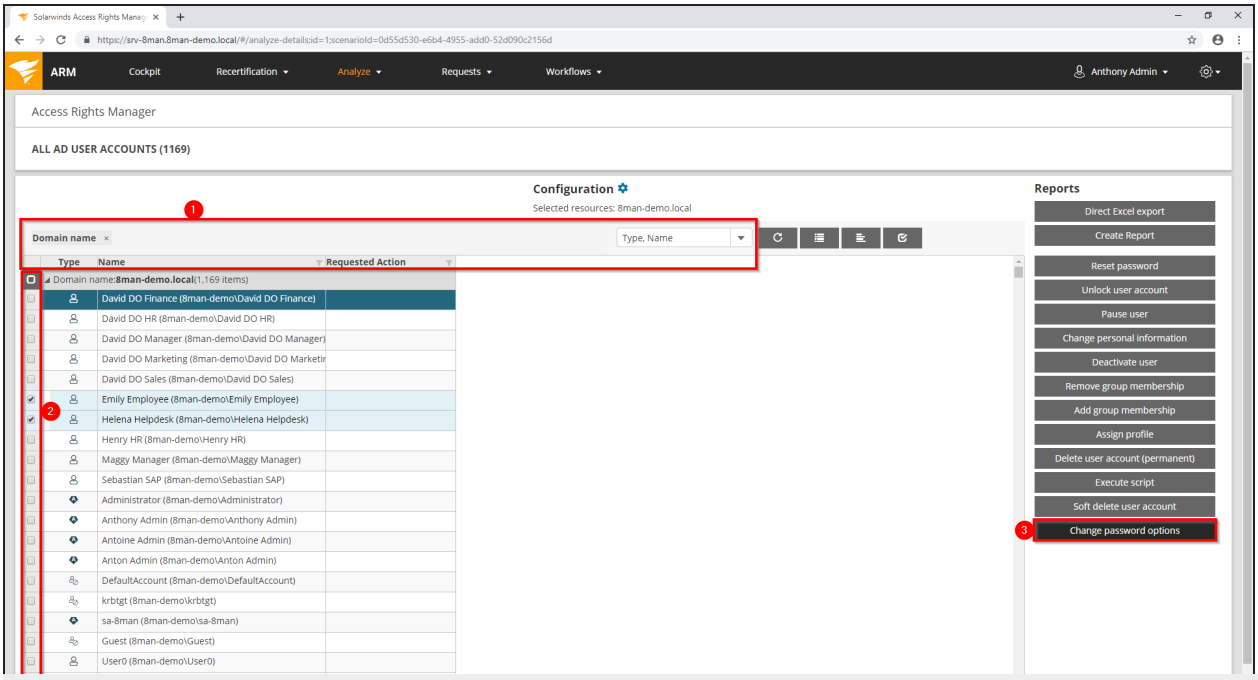
Step-by-step process



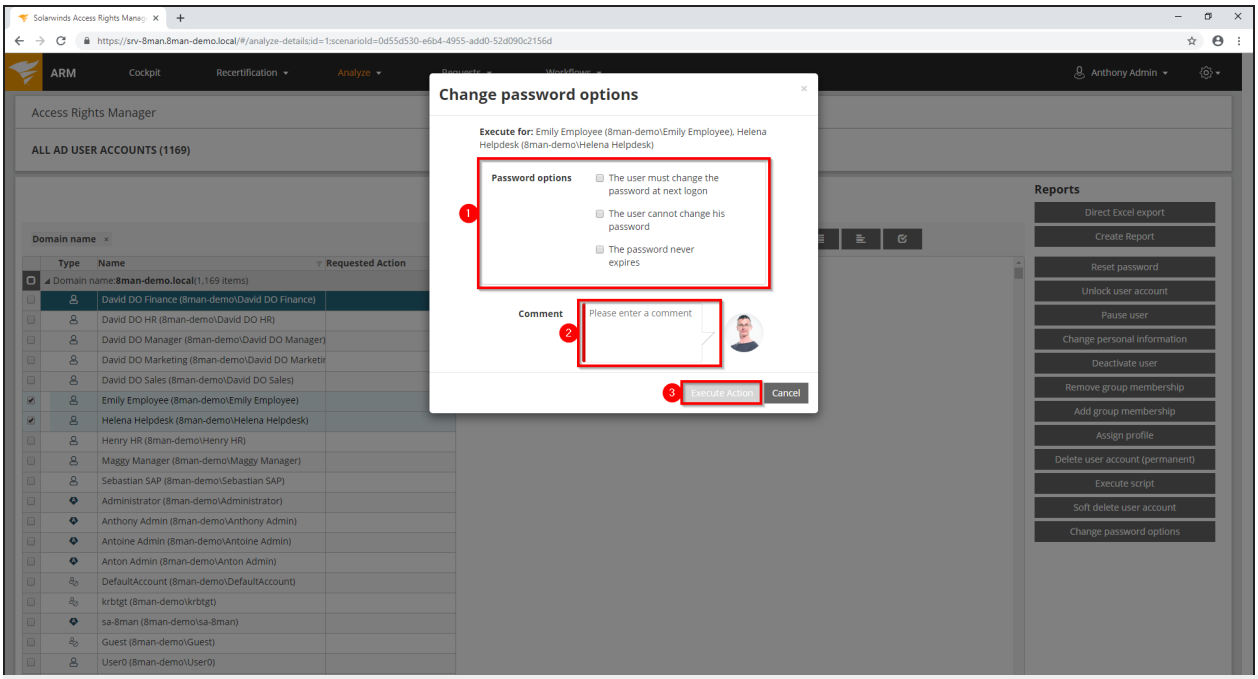
1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".



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.

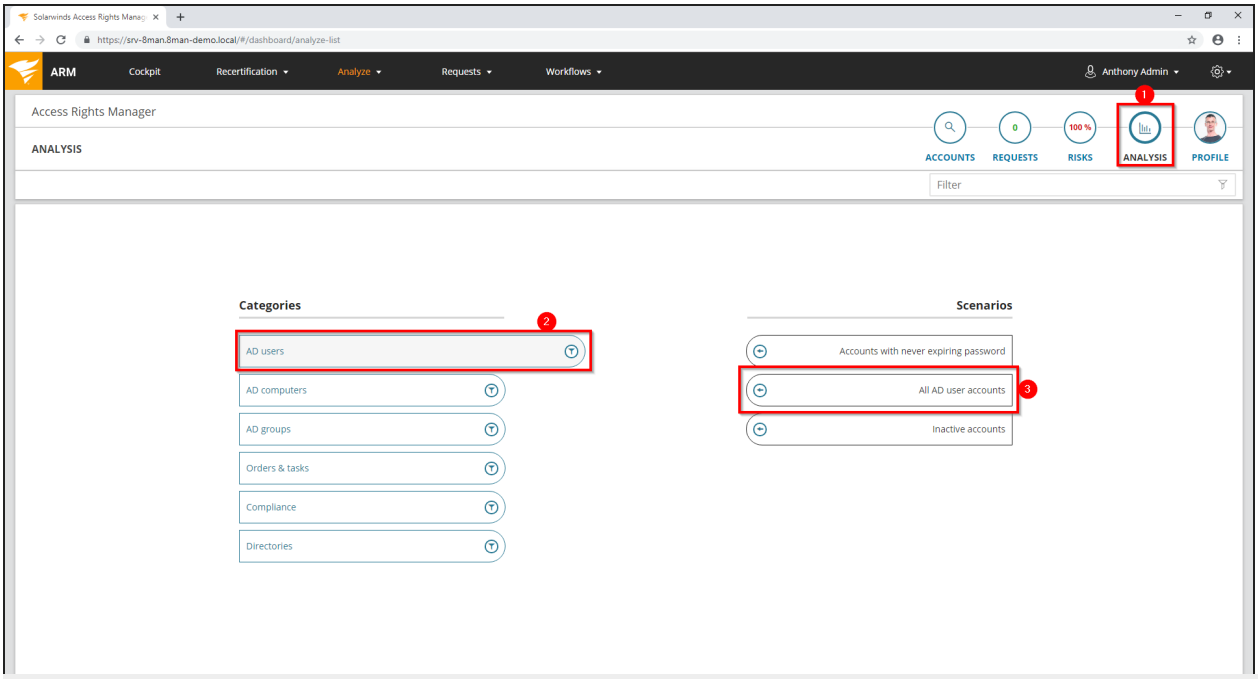
ARM provides a standard set of modifiable attributes. For each ARM role, you can specify which attributes are displayed and can therefore be changed. Please refer to the chapter: Set attributes available to web client scenarios.

Related features

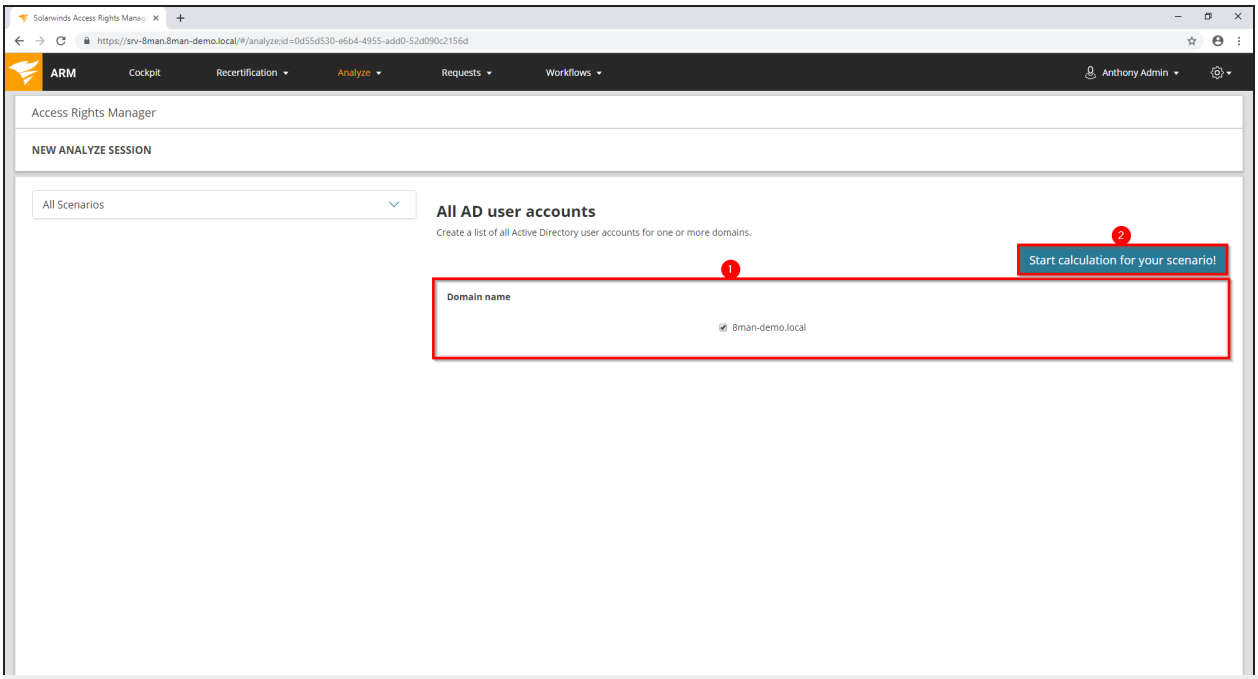
Change password options in bulk (web client)

Reset passwords in bulk (web client)

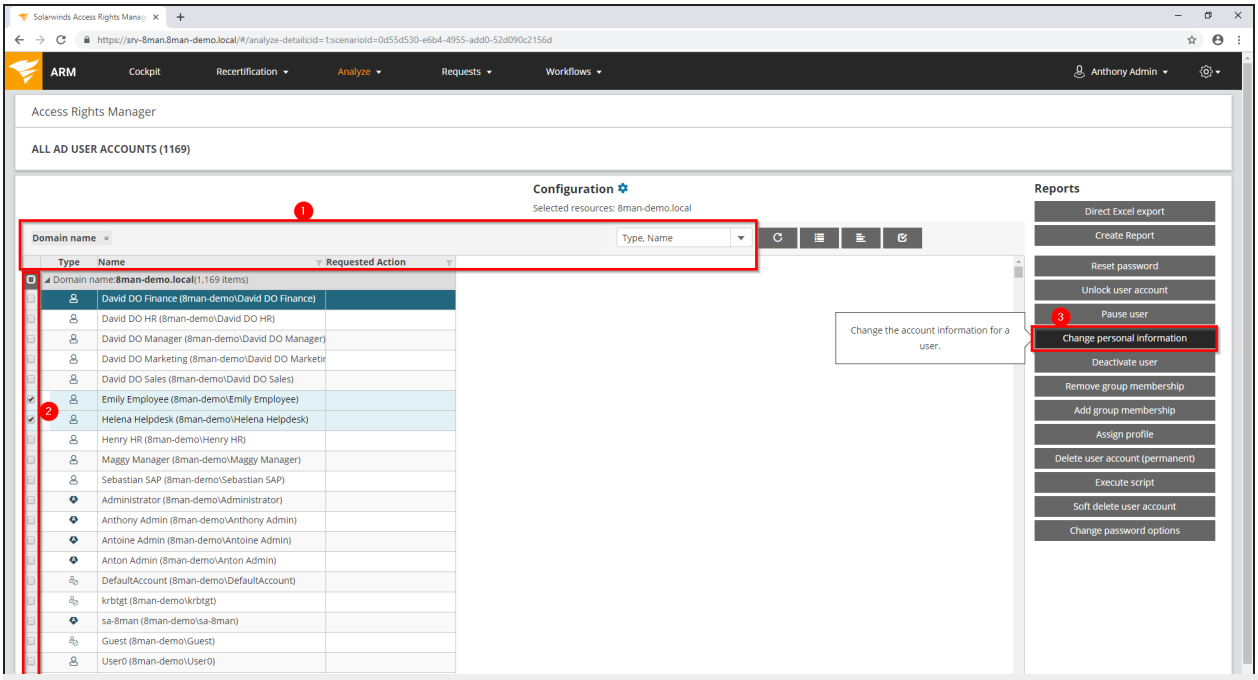
Step-by-step process



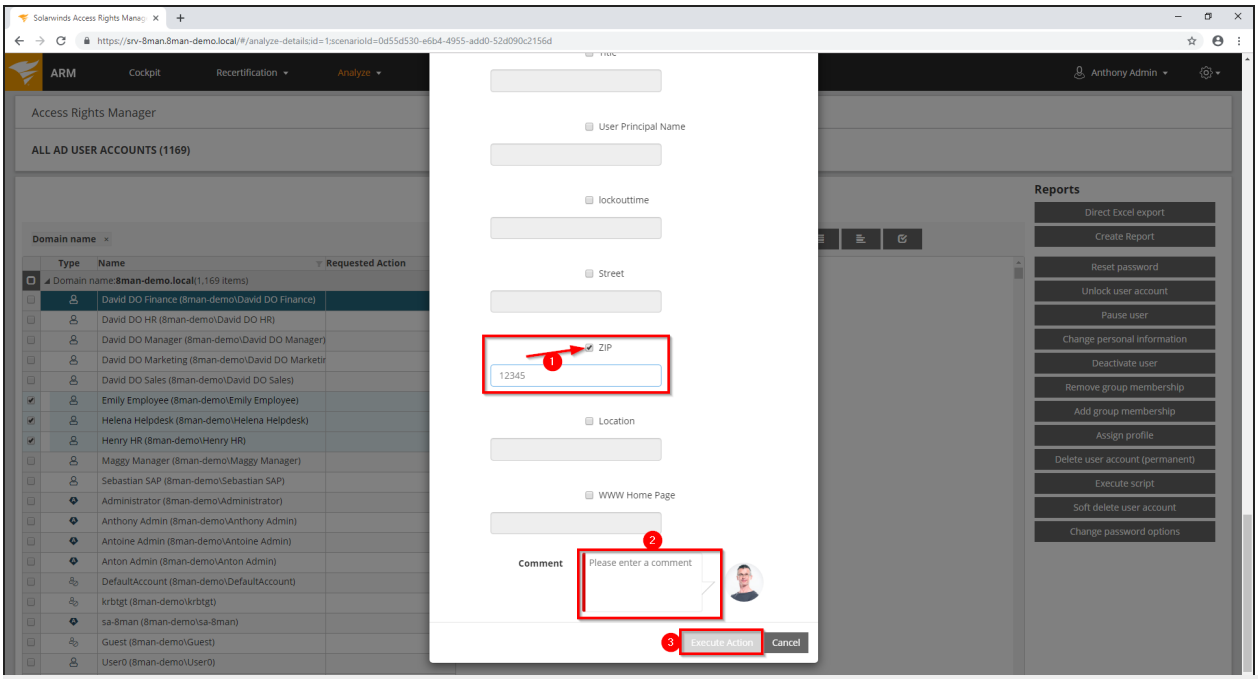
1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".



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.

> 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.

> 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)

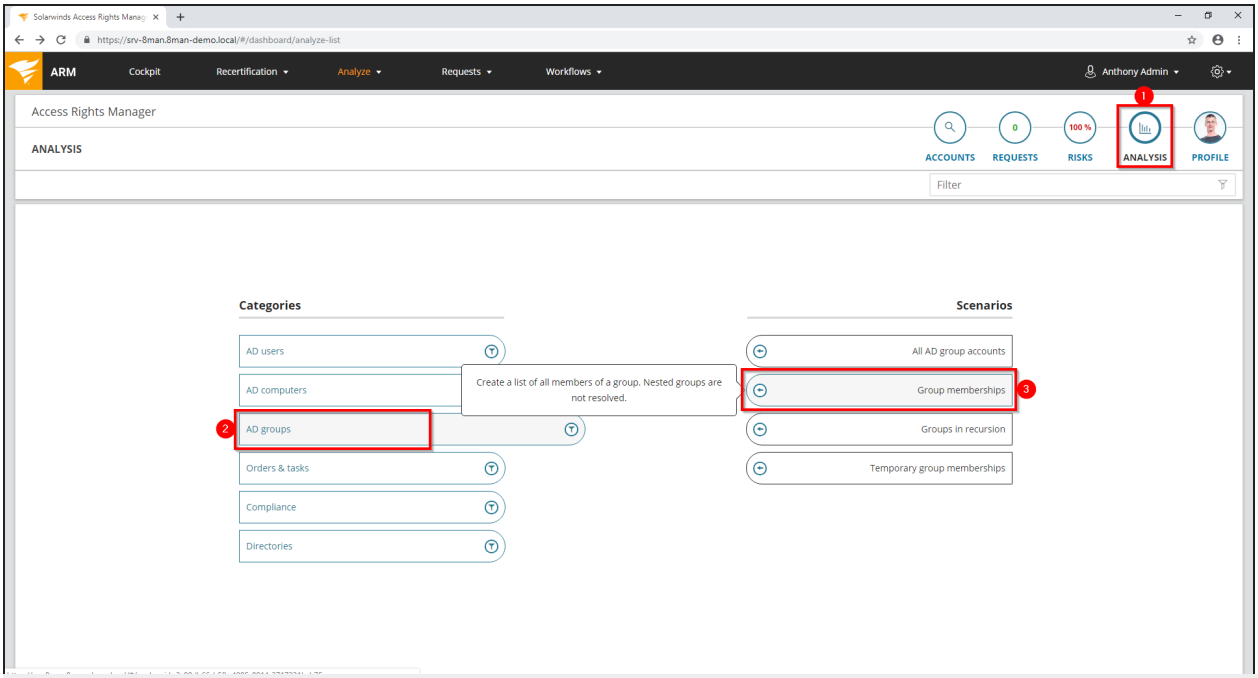
Background / Value

Remove lots of group memberships fast using the web client.

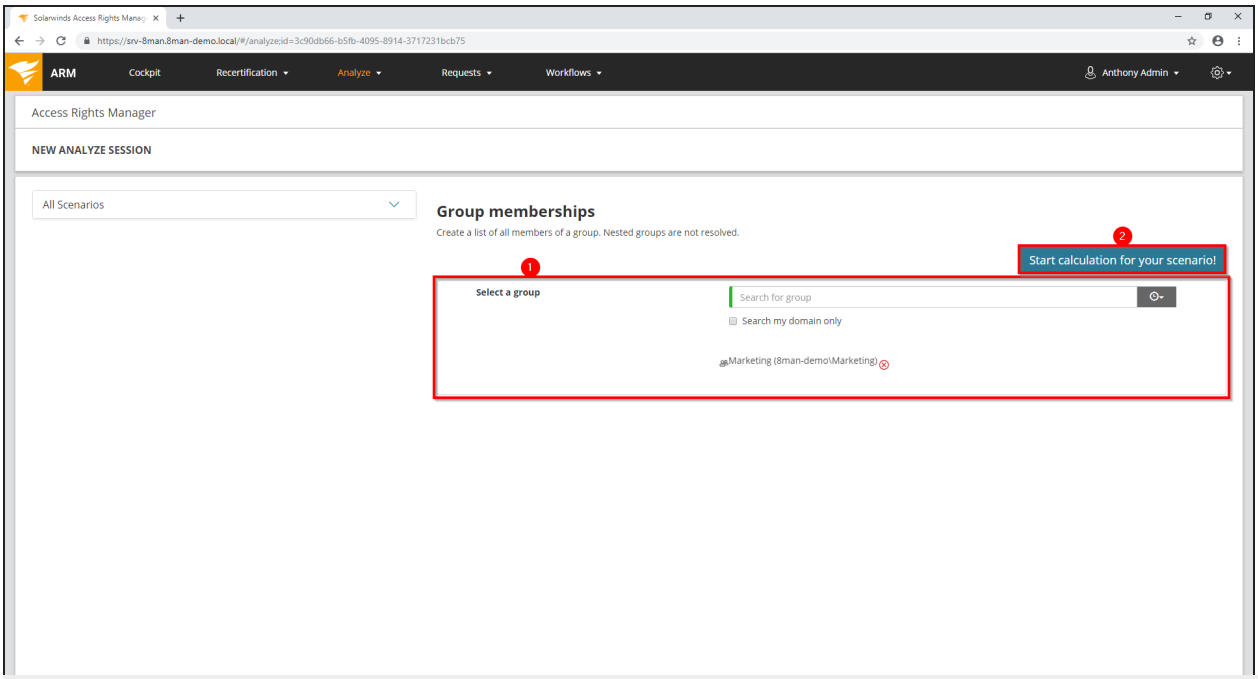
Related features

Manage group memberships (rich client)

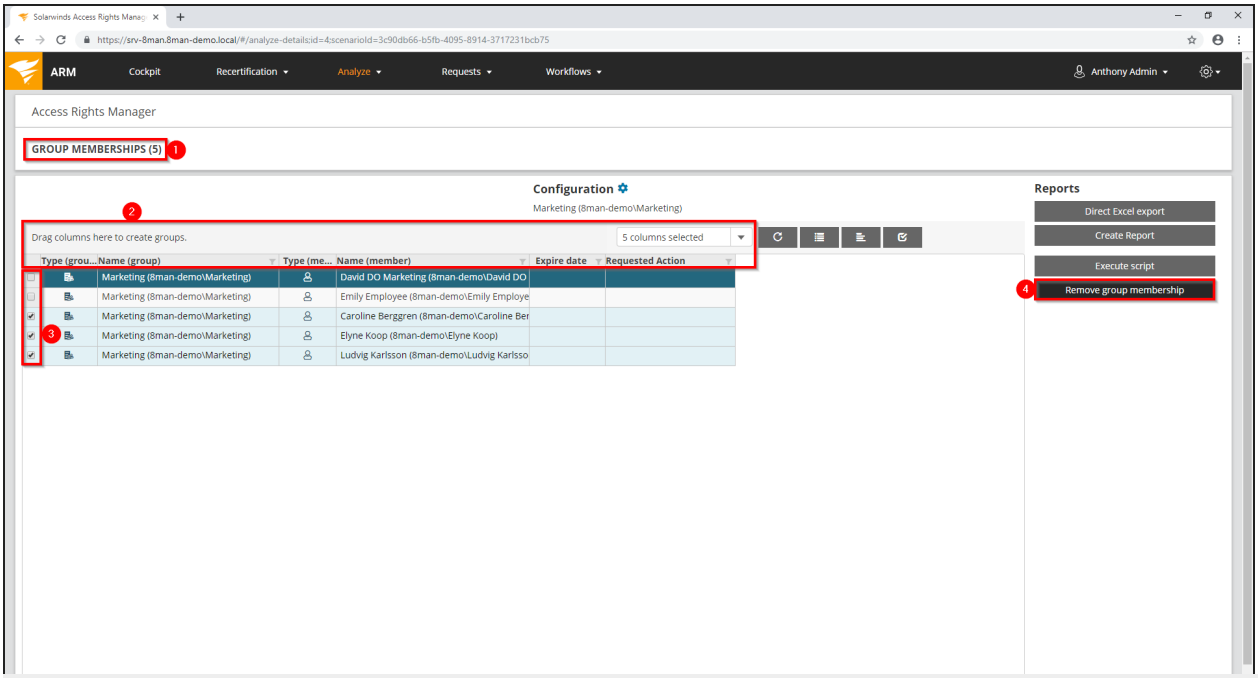
Step-by-step process



1. Click "Analysis".
2. Select the category "AD groups".
3. Click on "Group memberships".

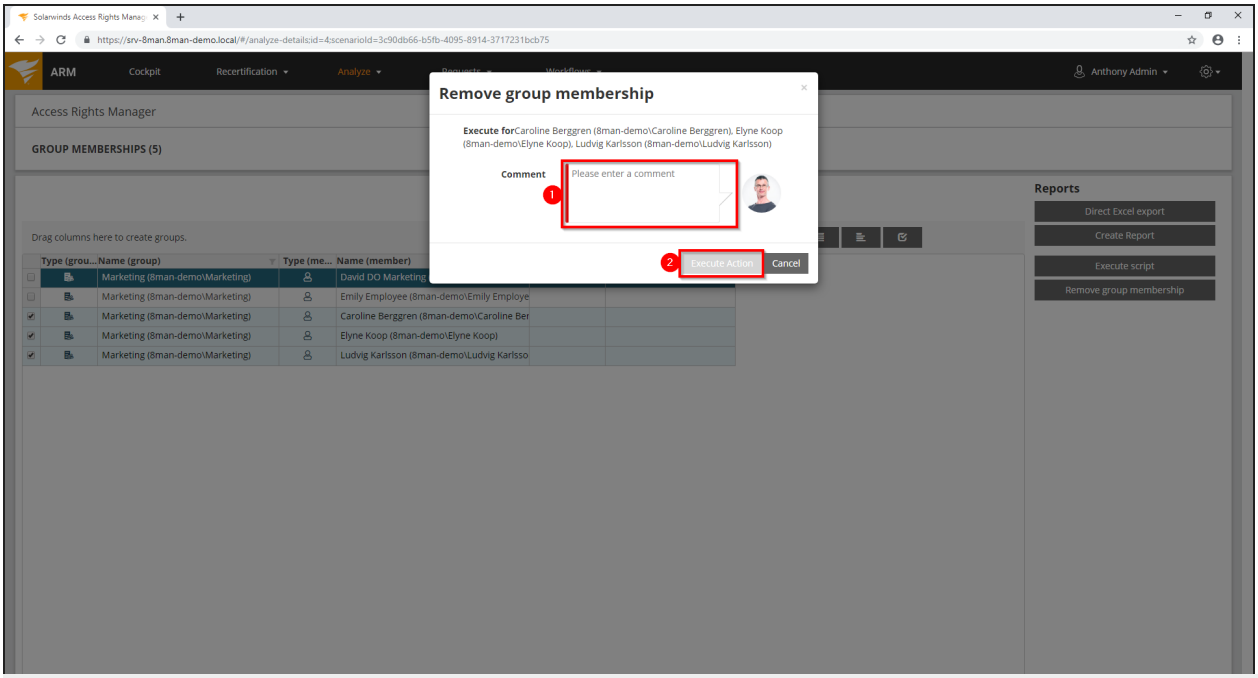


1. Find a group.
2. Start the calculation.



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.

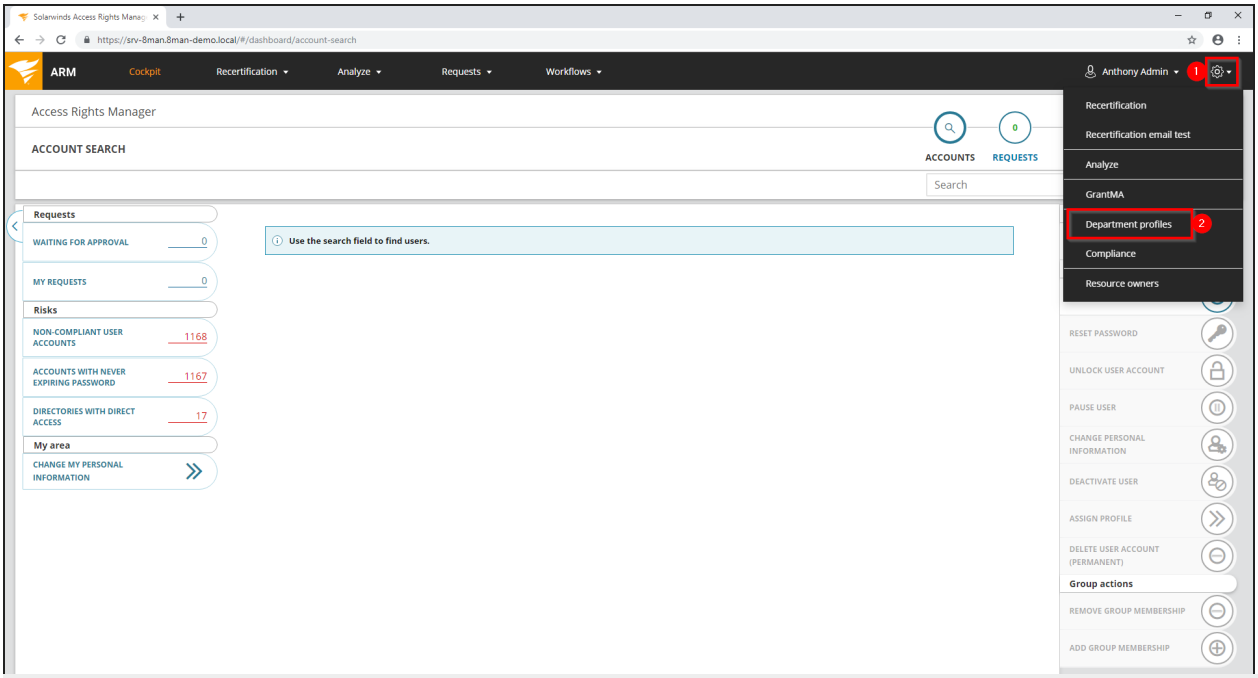
Department profiles can contain attributes and group memberships.

Related features

Assign a department profile to users (Cockpit)

Determine permissions deviating from the department profile (compliance check)

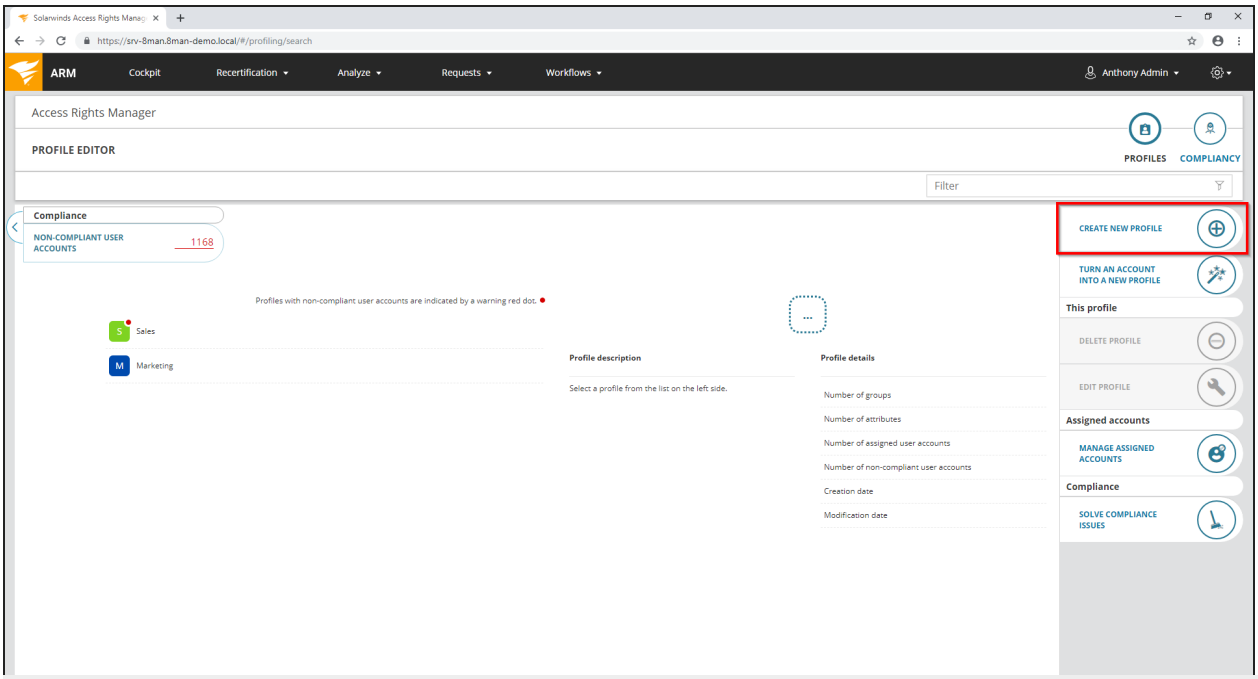
Step-by-step process



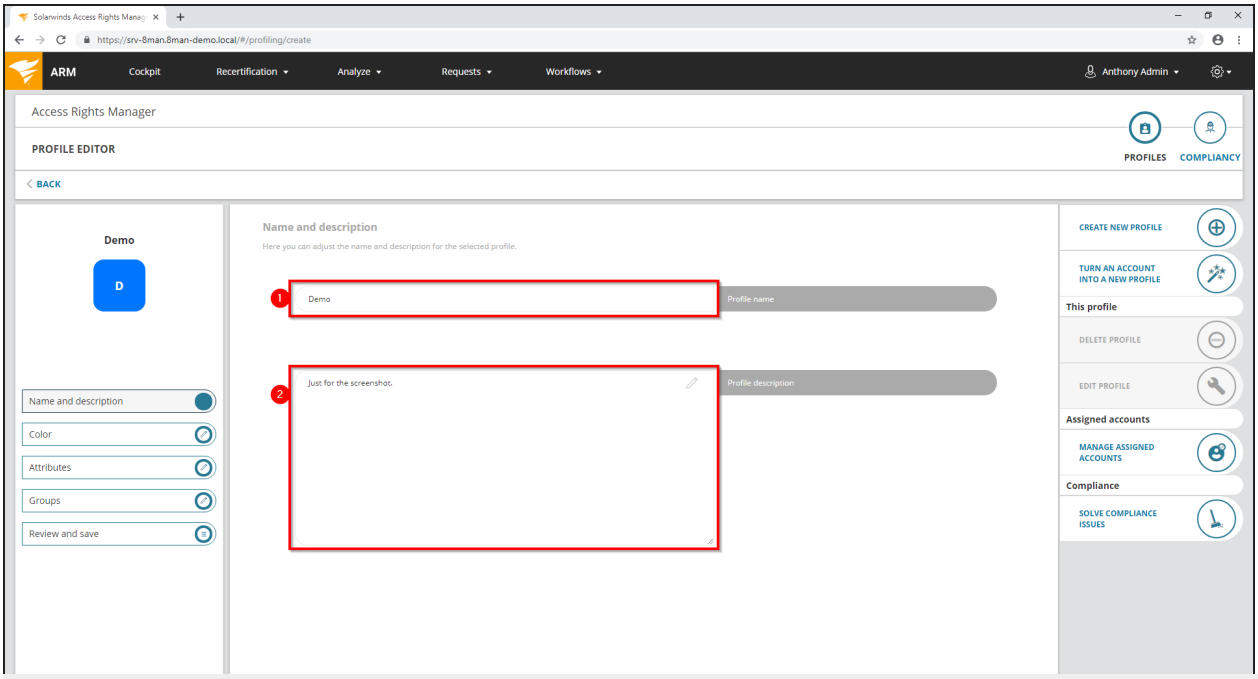
1. Click the gear.

You must be logged in as an ARM Administrator to see the gear icon.

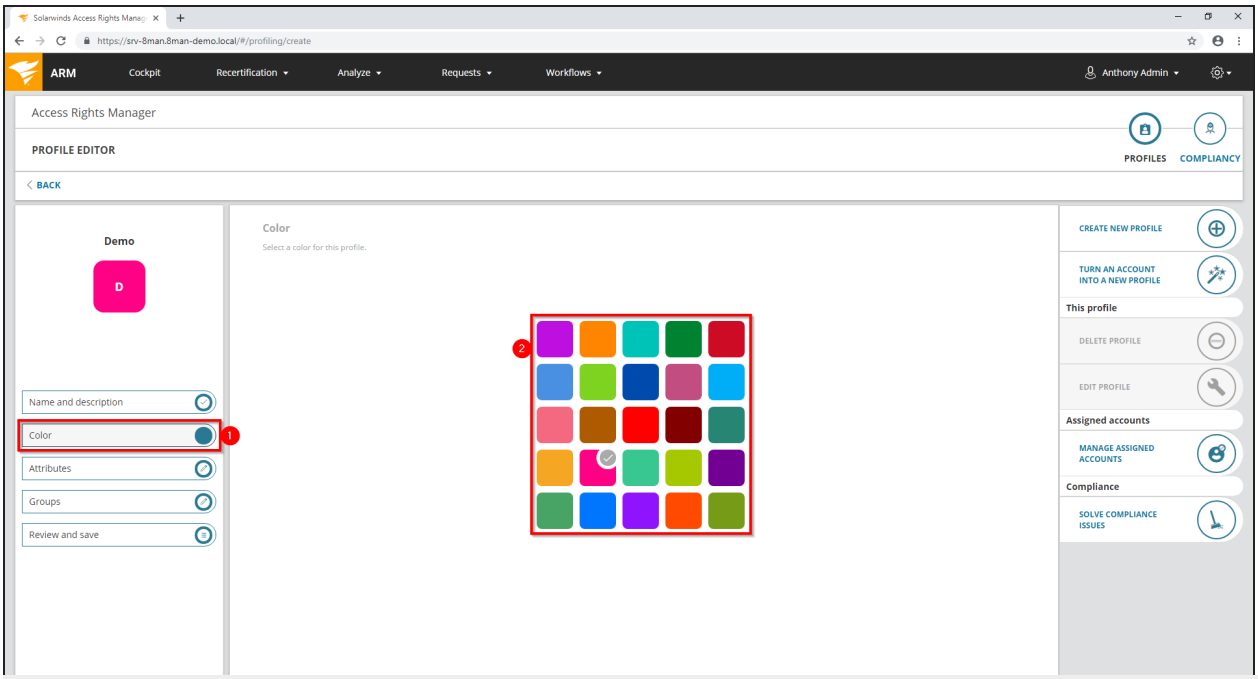
2. Click "Department profiles".



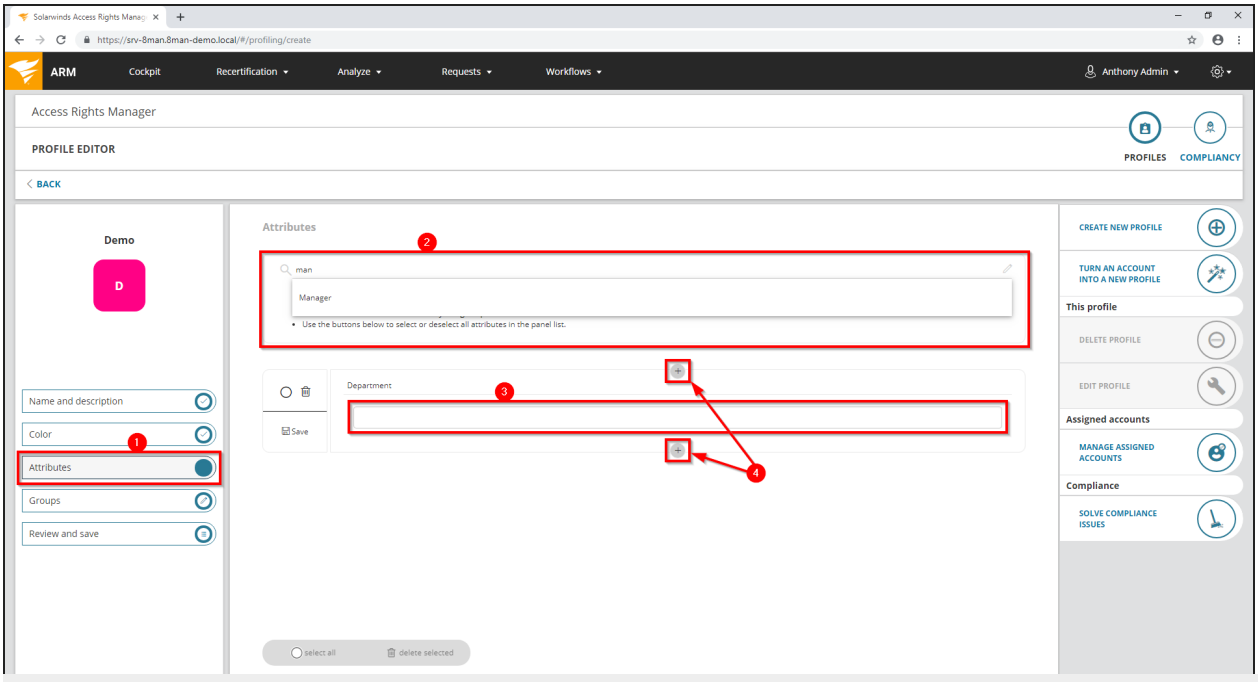
Click "Create new profile".



1. Give the department profile a name, at least 2 letters.
2. Optional: Describe the profile.

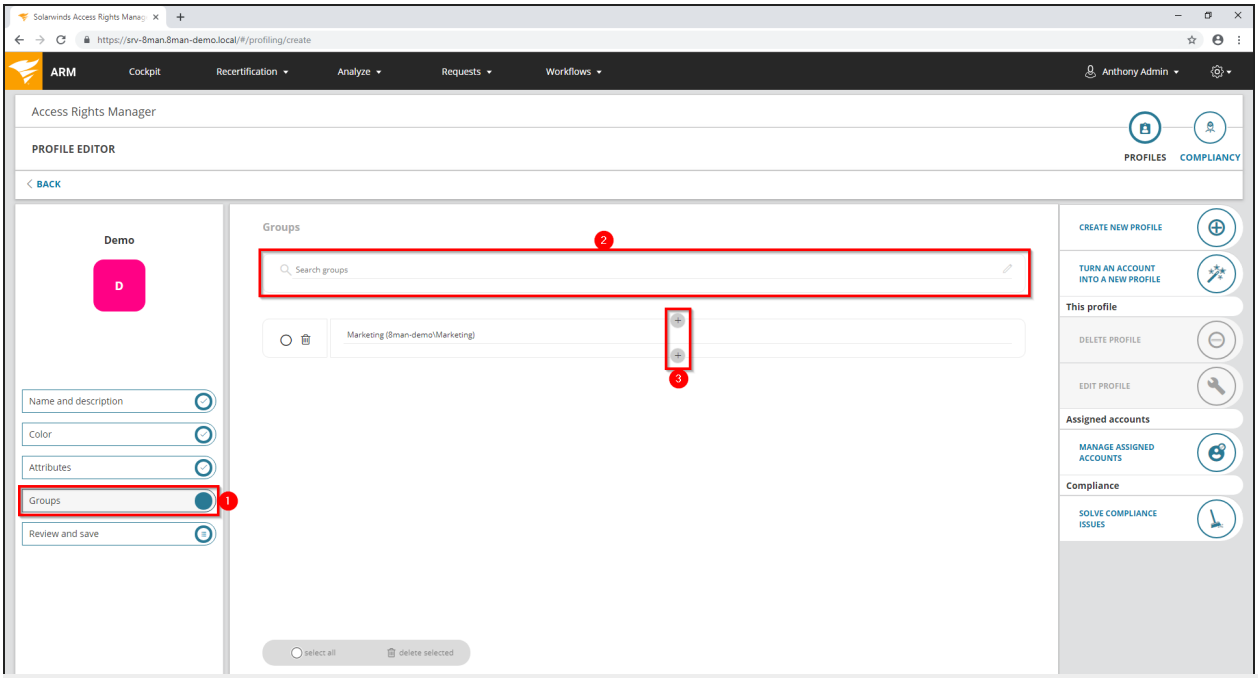


1. Click on "color".
2. Choose a color for the department profile. The color is for recognition purposes only.

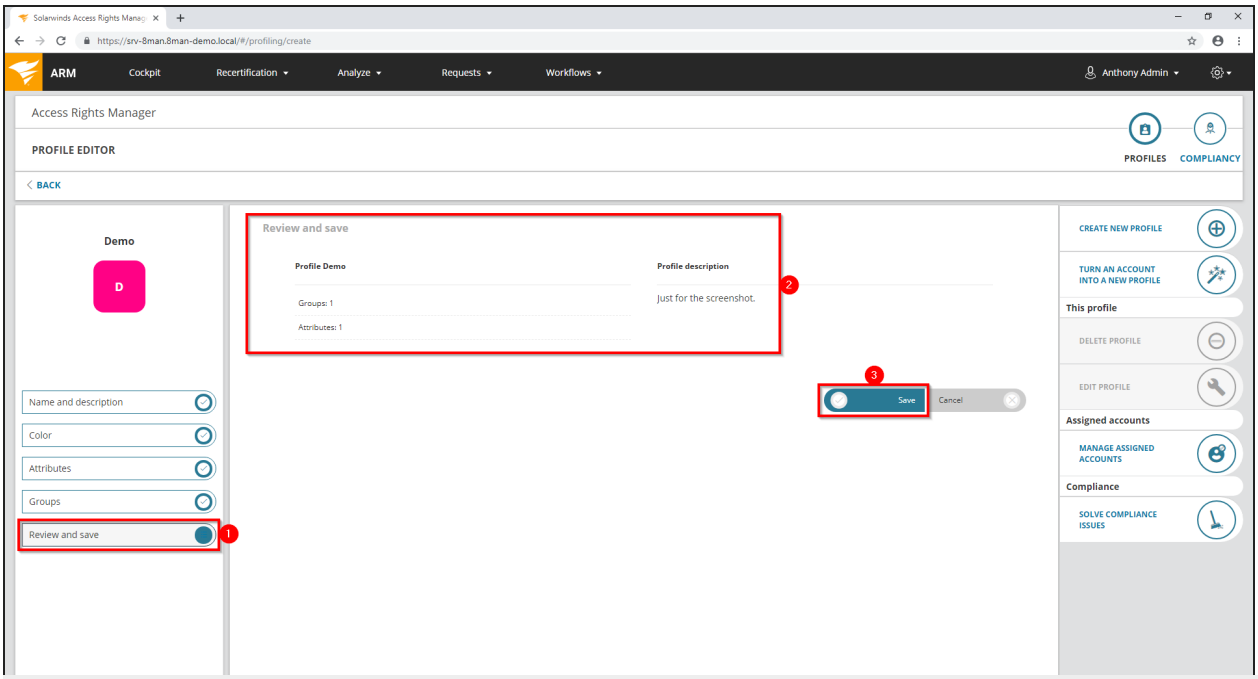


1. Click on "Attributes".
2. Use the search to find the desired attribute.
3. Enter the value of the attribute.

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:

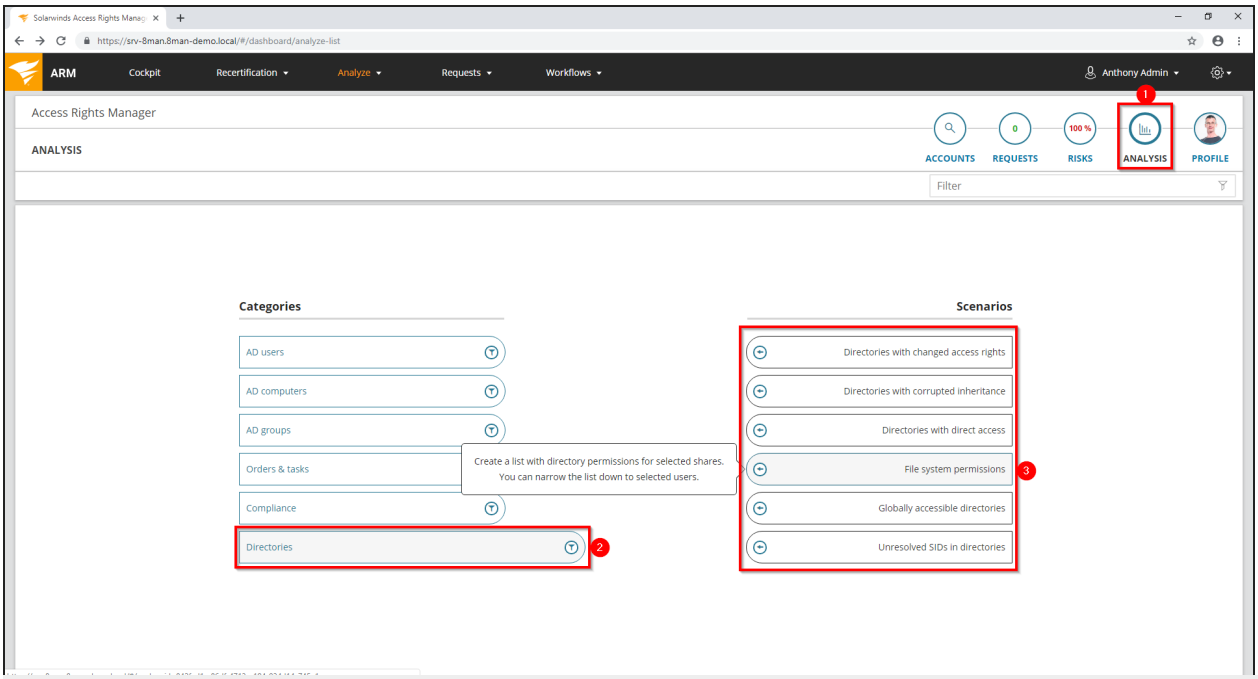
```
%ProgramData%\protected-networks.com\8MAN\scripts\analyze
```

Further necessary steps and more details can be found in the chapter: Configuring scripts

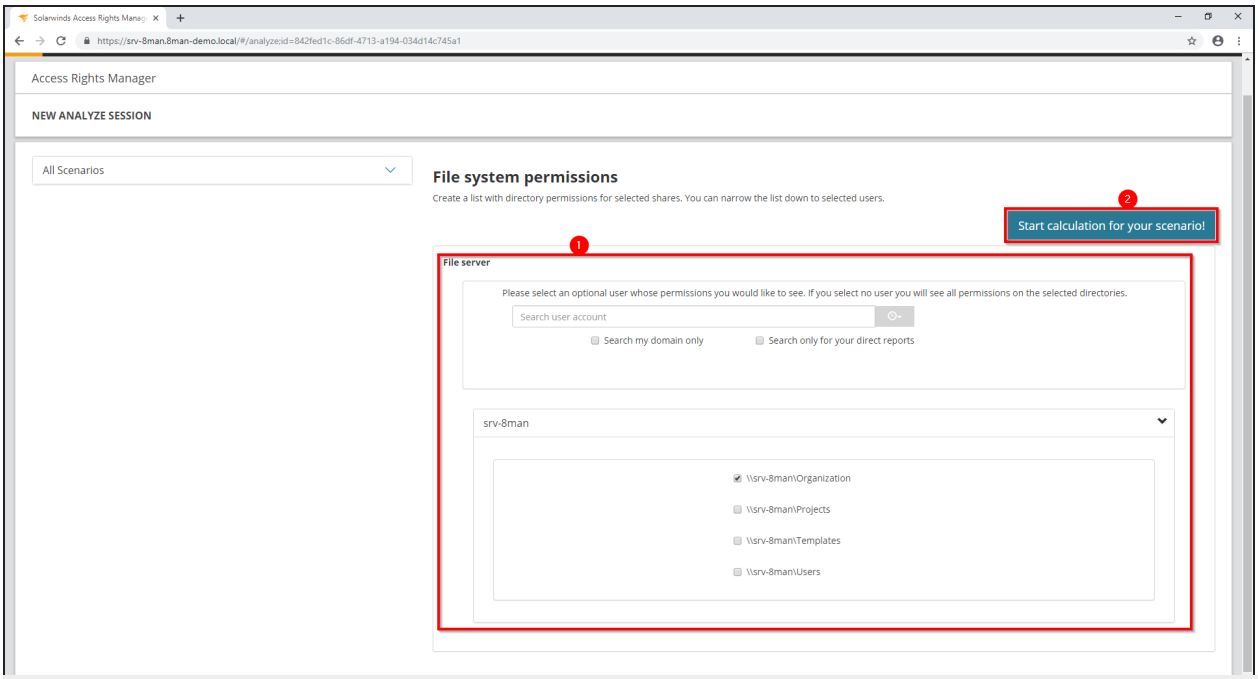
Related features

Execute scripts on user accounts in bulk (web client)

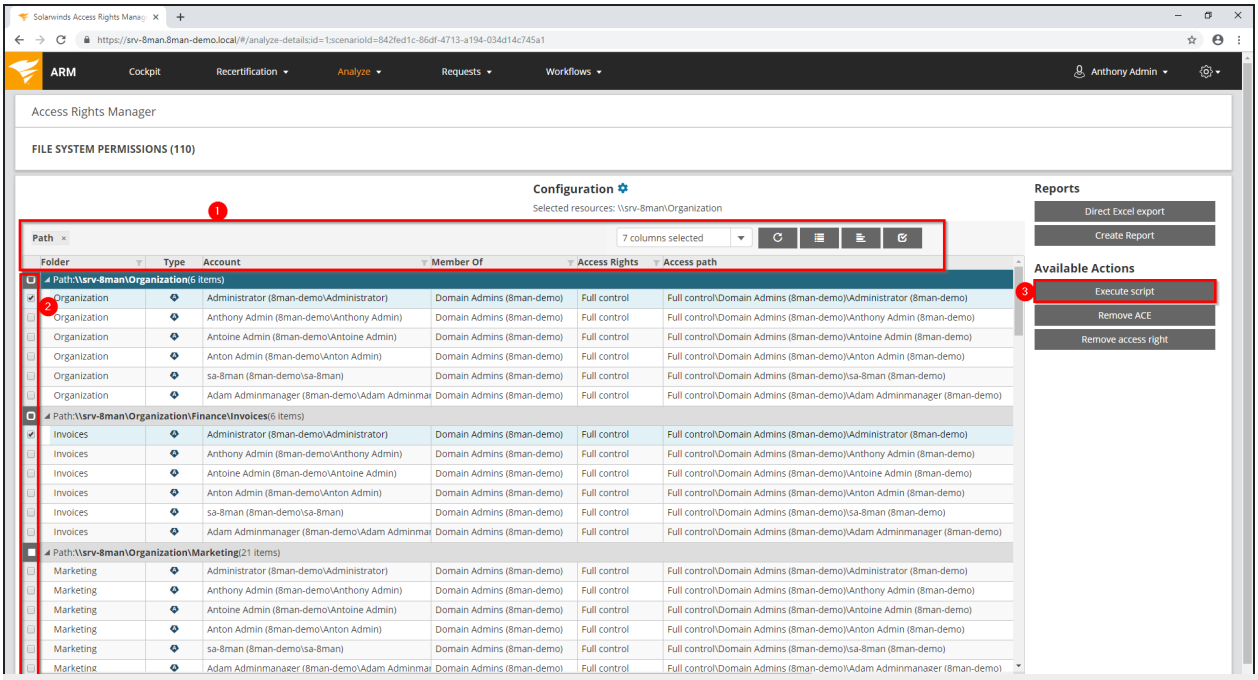
Step-by-step process



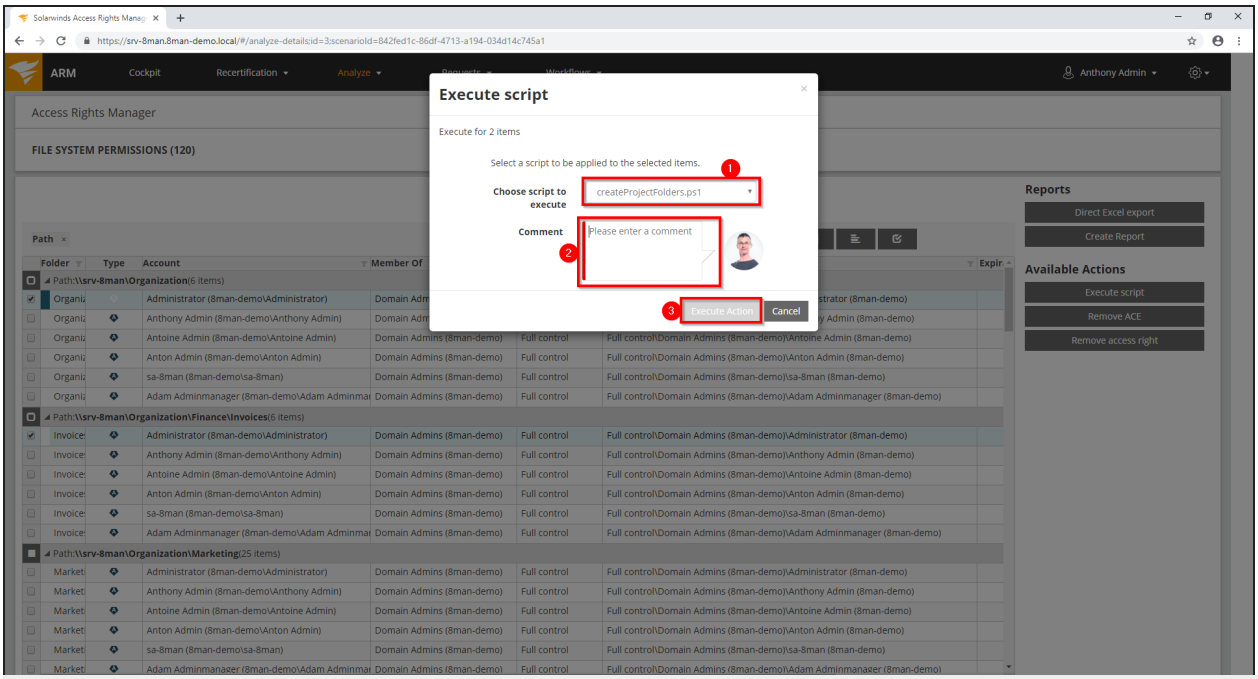
1. Select "Analysis".
2. Select the category "Directories".
3. Choose a scenario with directories in focus.



1. Set the scenario options.
2. Start the calculation.



1. Use the grouping, sorting, filtering and column selection to narrow down your result.
2. Select the desired directories.
3. Click "Execute Script".



1. Select a script.

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:

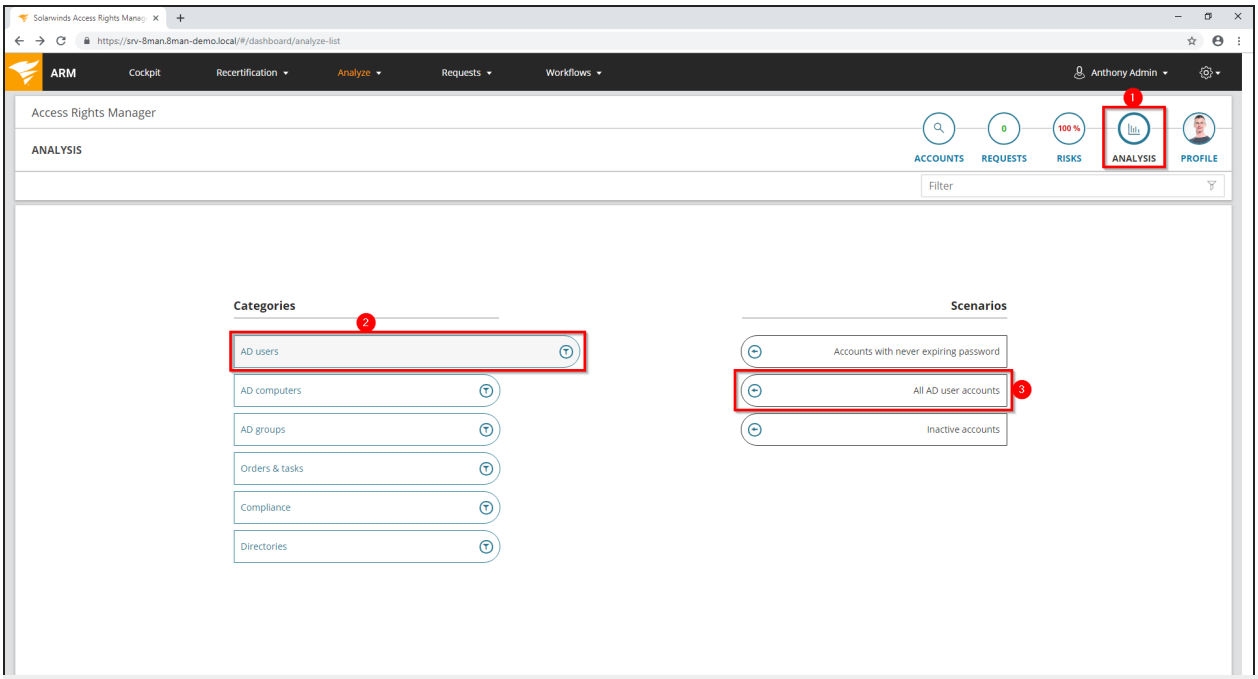
```
%ProgramData%\protected-networks.com\8MAN\scripts\analyze
```

Further necessary steps and more details can be found in the chapter: Configuring scripts.

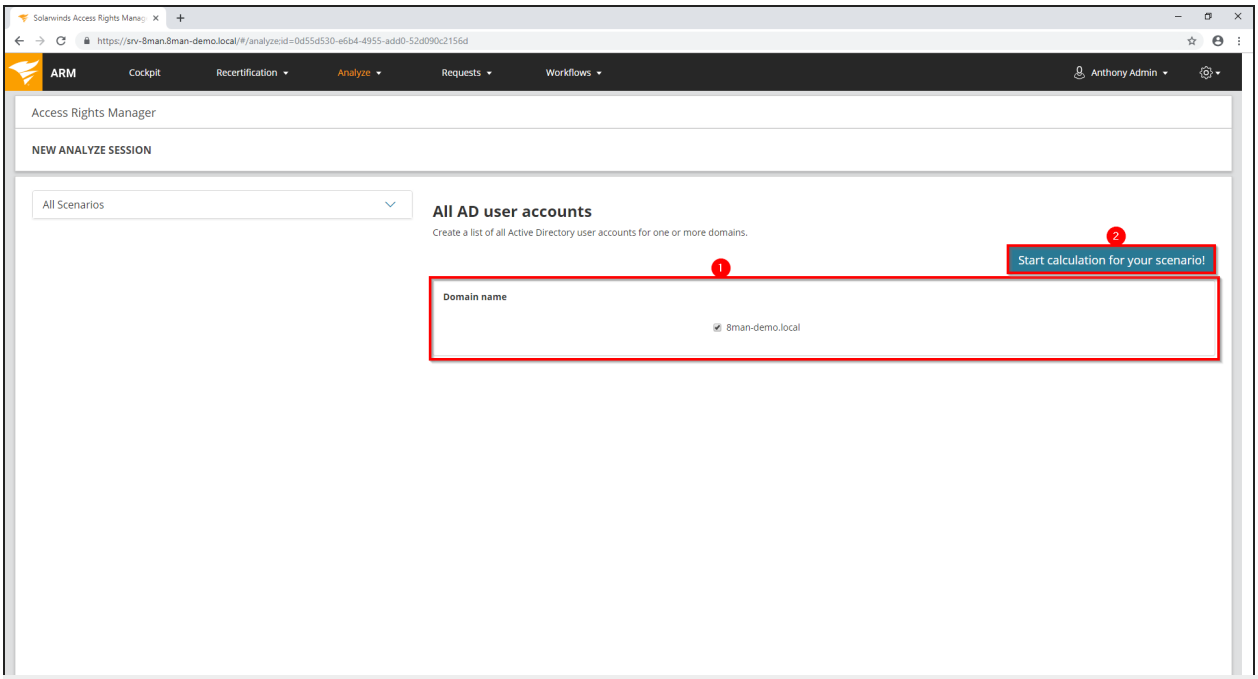
Related features

Execute scripts on directories in bulk (web client)

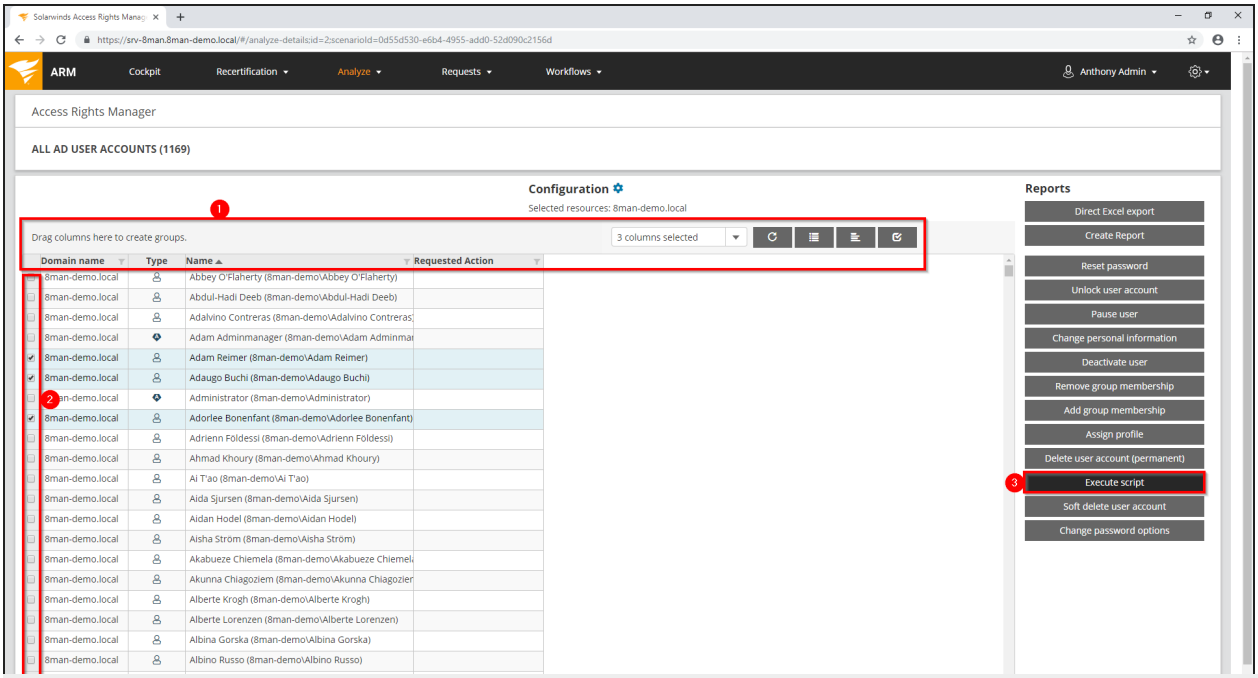
Step-by-step process



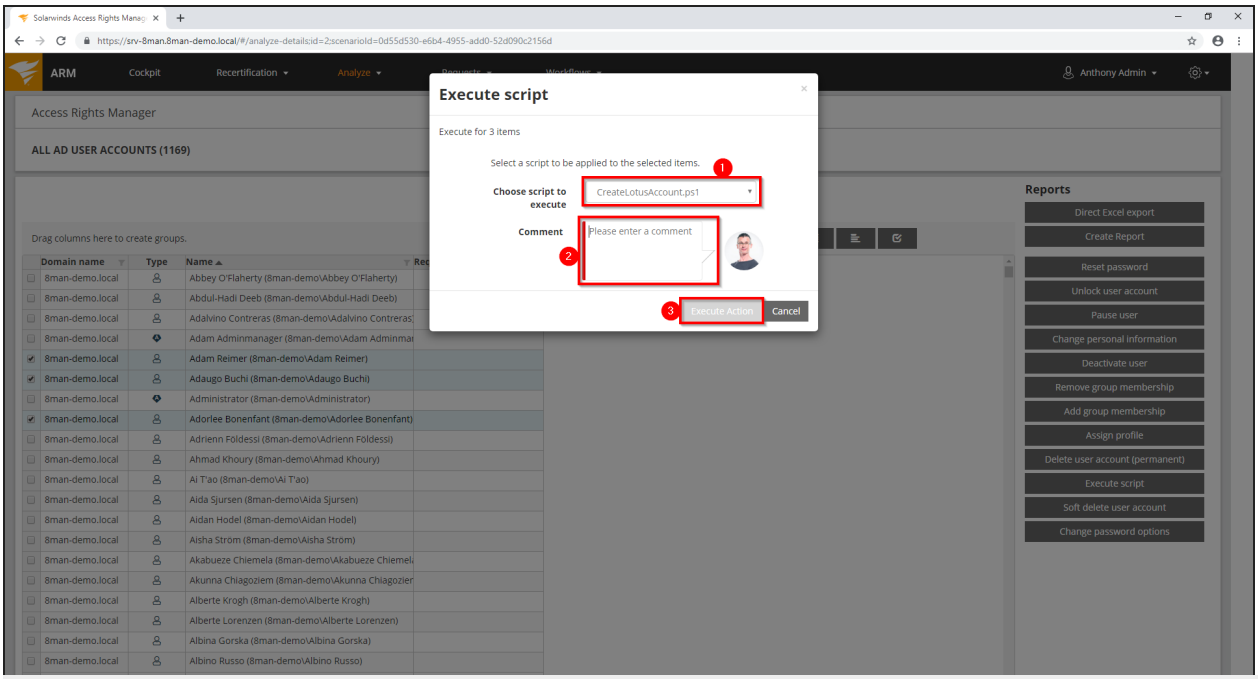
1. Select "Analysis".
2. Select the category "AD users".
3. Choose a scenario with users in focus.



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.

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

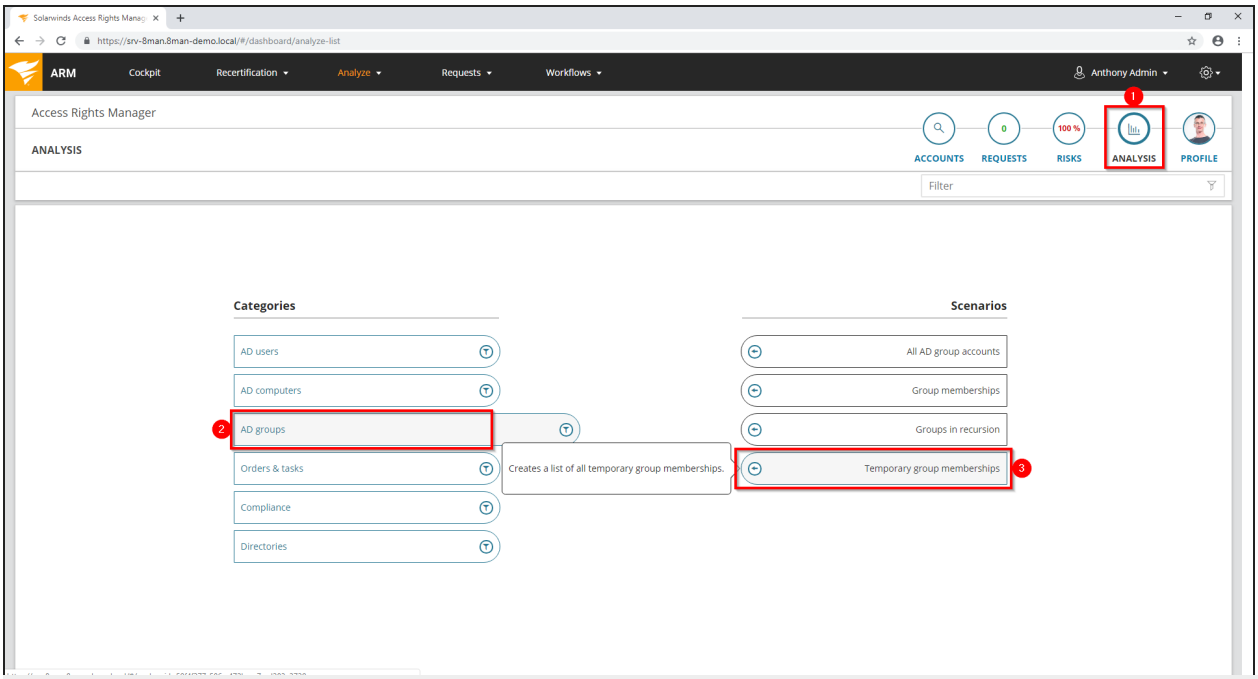
Simply change the expiration date of temporary group memberships or convert them to a permanent membership. You can also easily remove temporary memberships.

Related features

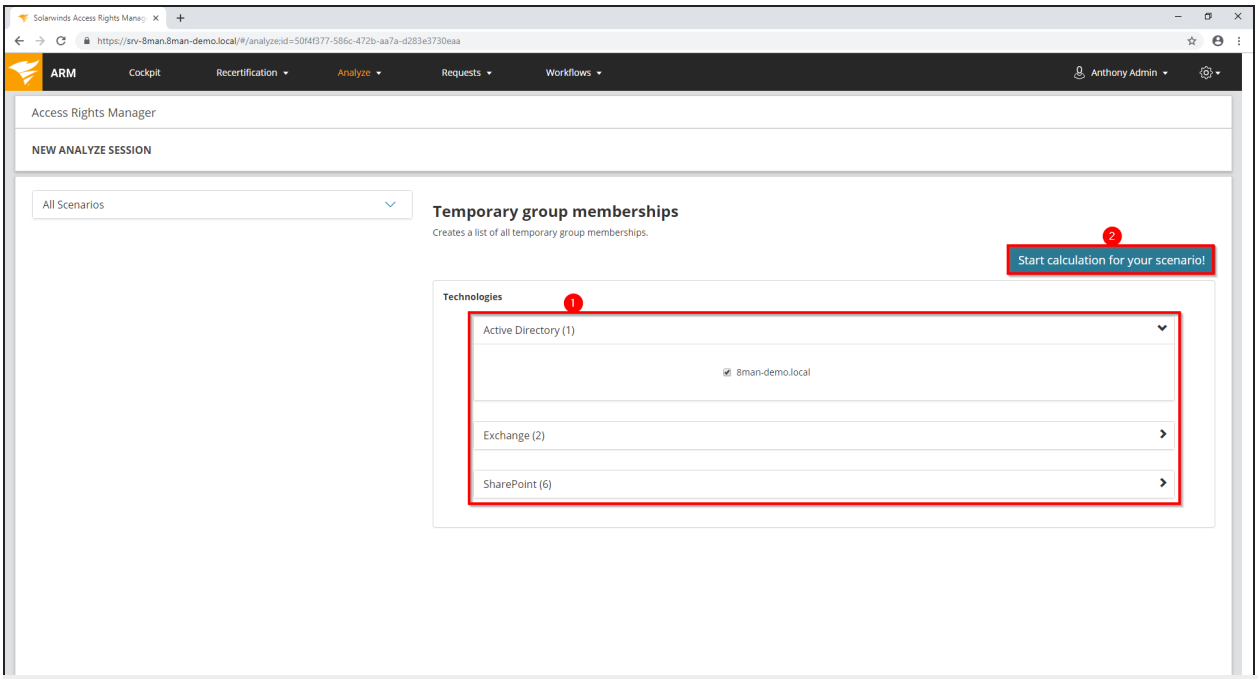
Remove group memberships (cockpit)

Add group memberships (cockpit)

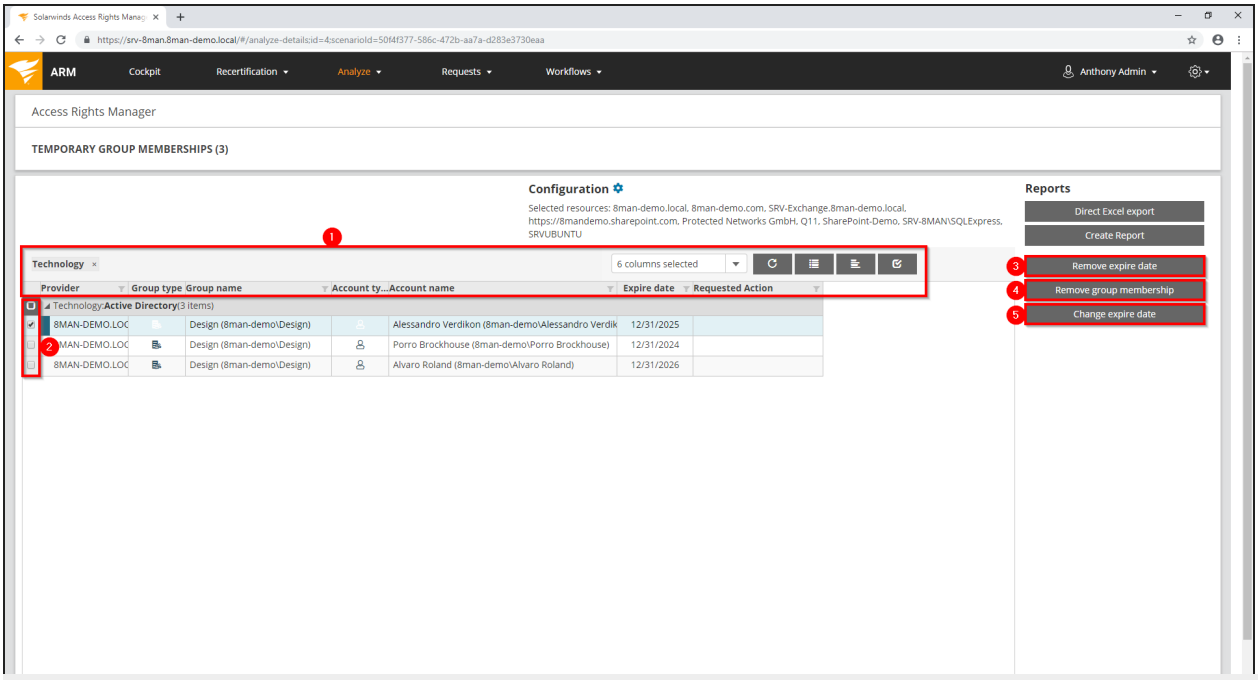
Step-by-step process



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

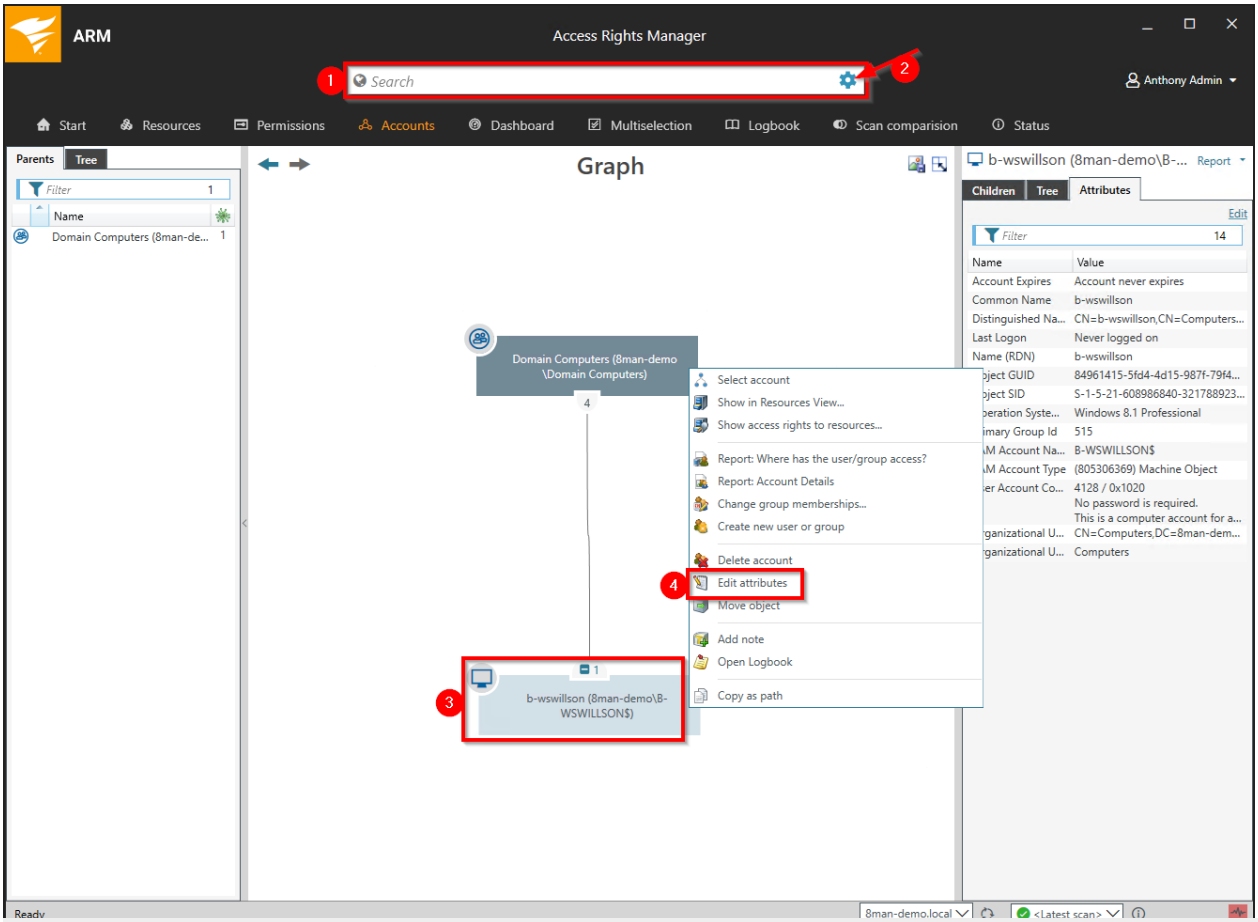
Background / Value

Maintain computer accounts comfortably and documented within ARM.

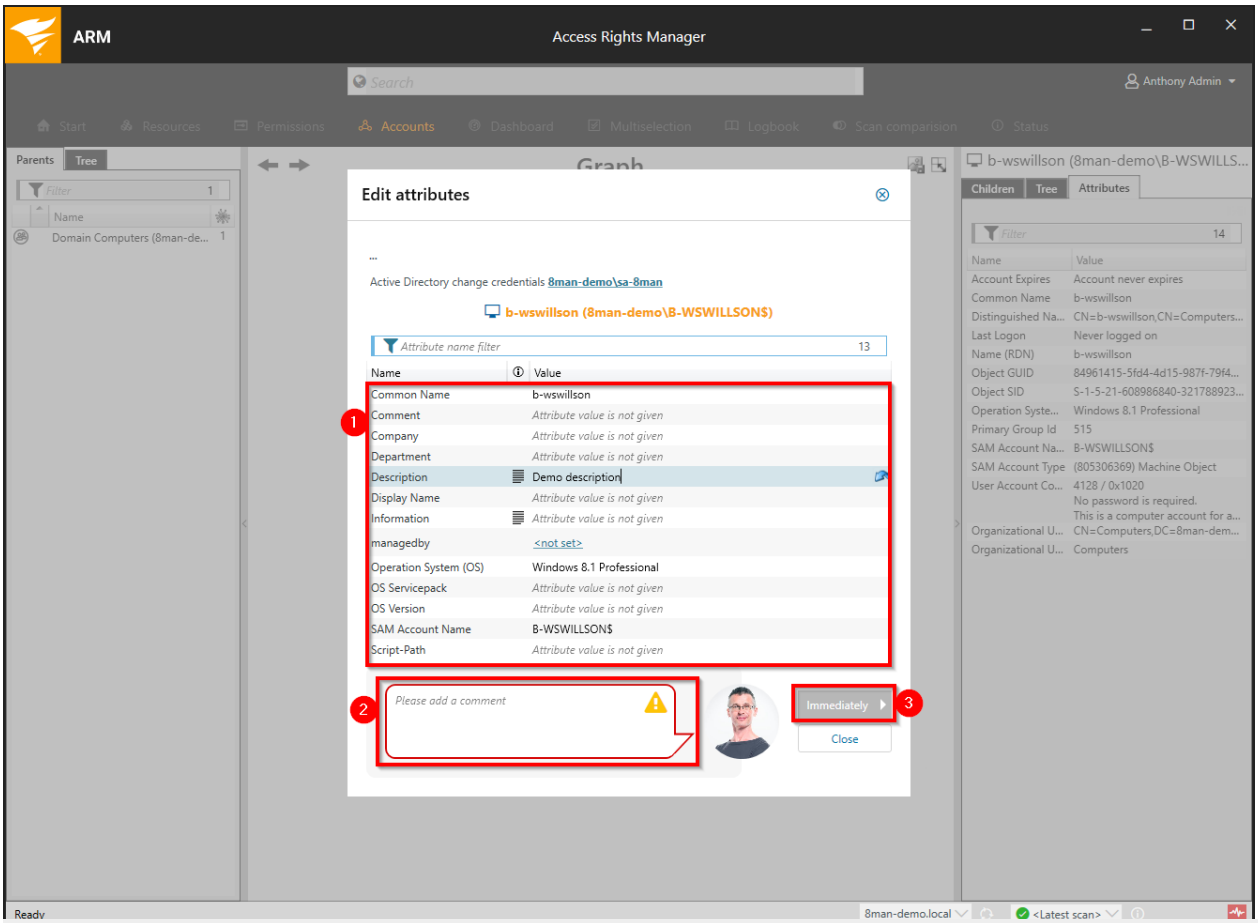
Related features

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".



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

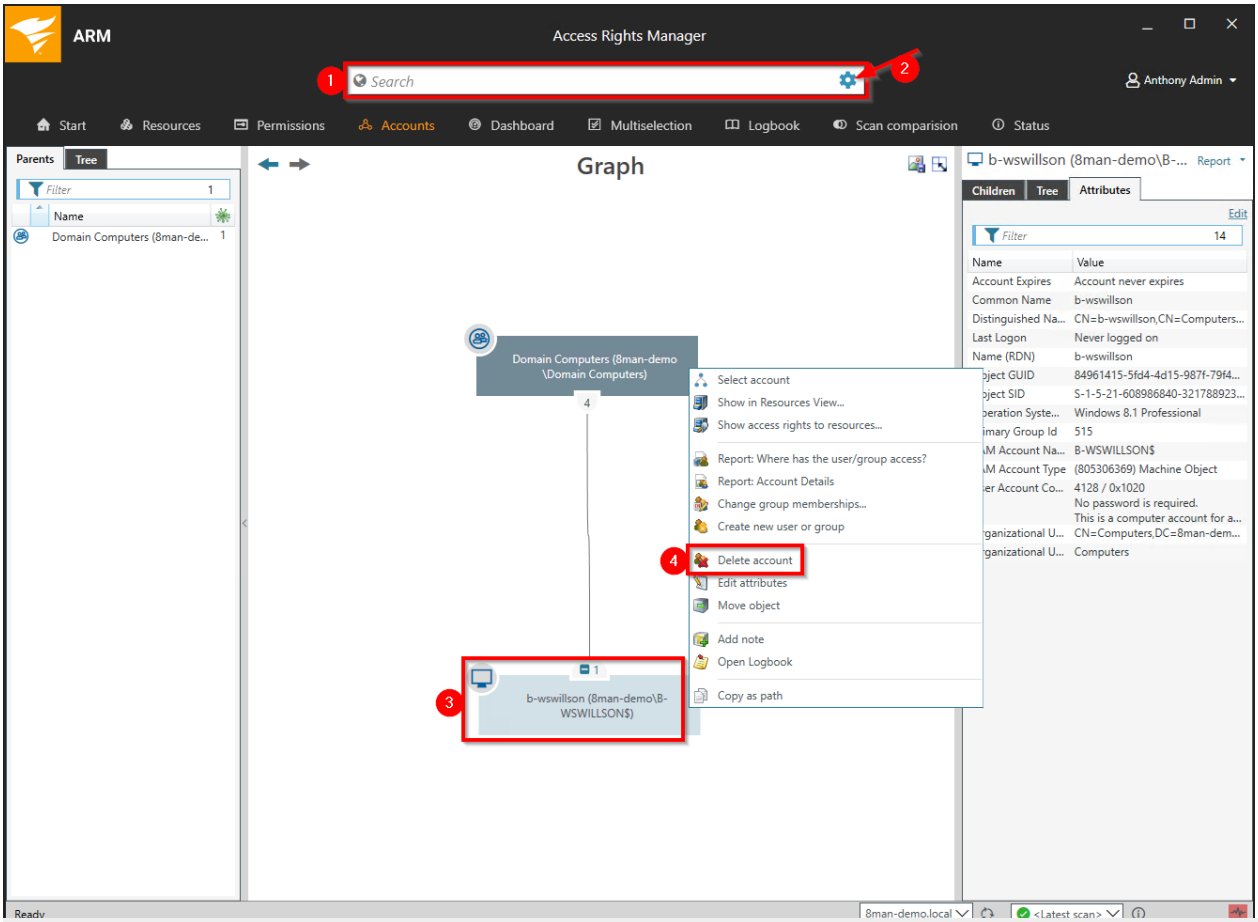
Background / Value

Delete computer accounts comfortably and documented within ARM.

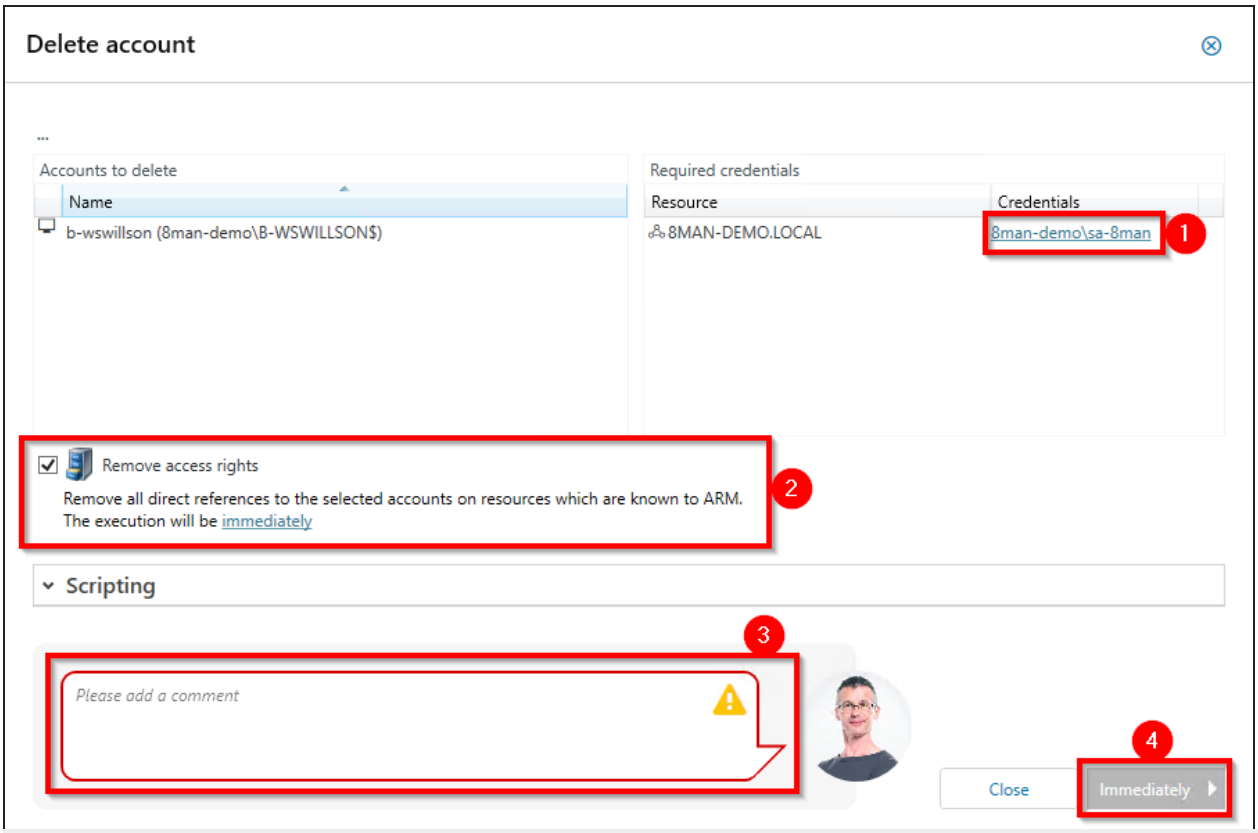
Related features

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".



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

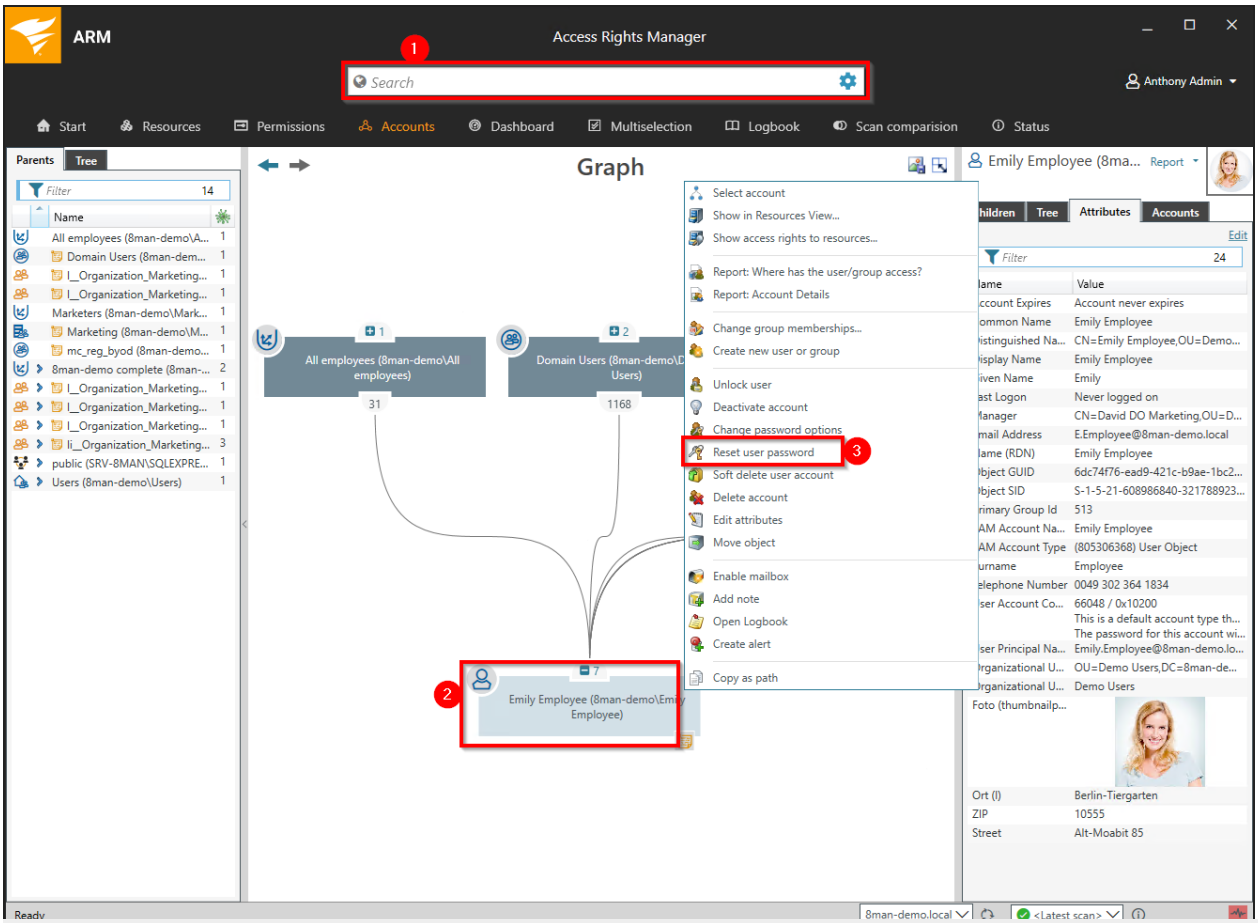
Resetting passwords is one of the most common tasks performed by help desks. ARM allows an easy and secure way of resetting passwords. All sensitive actions are documented in the log book. If an employee uses native tools to reset a password and illegally tries to access that user account, the incident is captured with AD Logga. Especially sensitive user accounts can be monitored with AD Logga alerts.

Related features

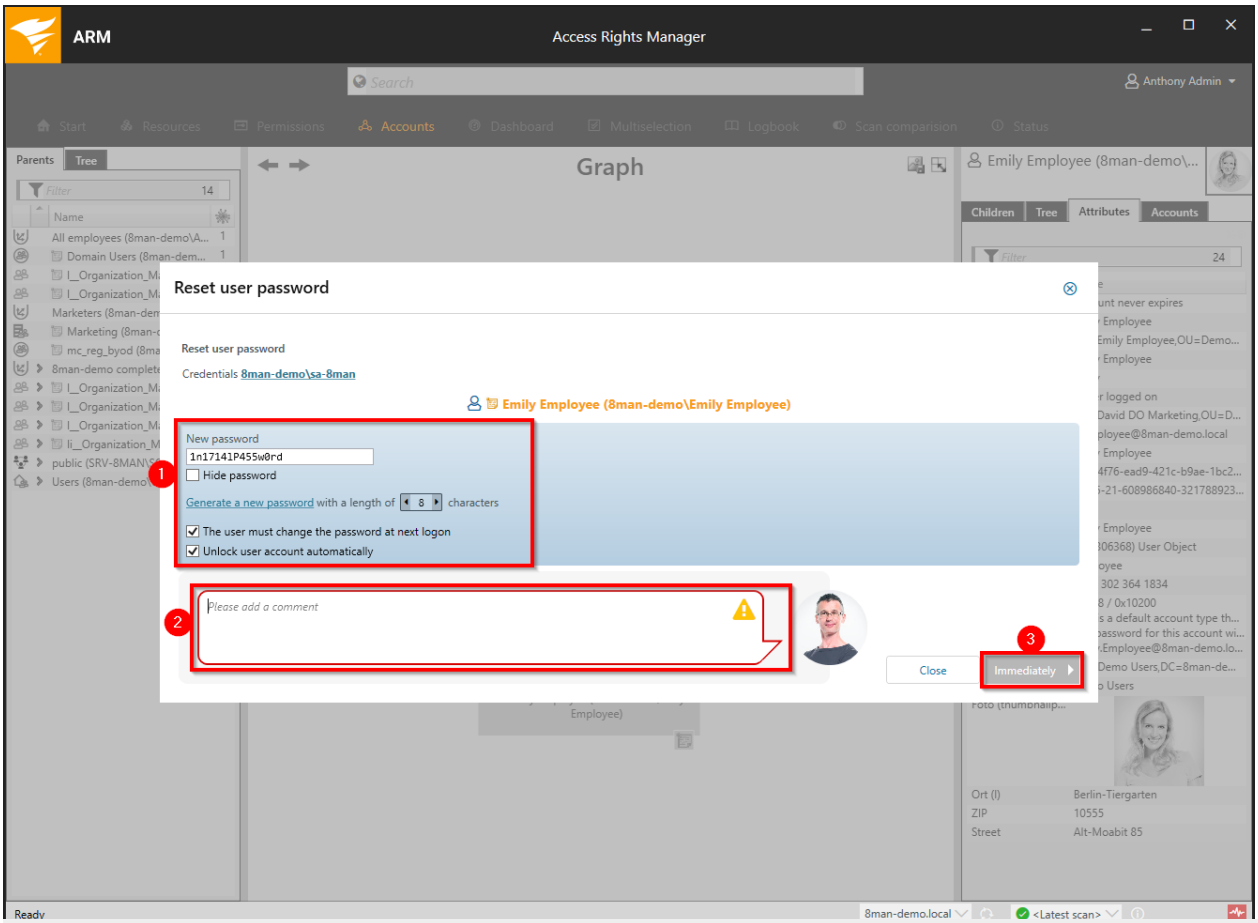
AD Logga: Identify locked accounts

AD Logga: Set alerts for user accounts

Step-by-step process



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.



1. Determine your password options.
2. You must enter a comment.
3. Start the reset process.

Unlock user accounts (web client)

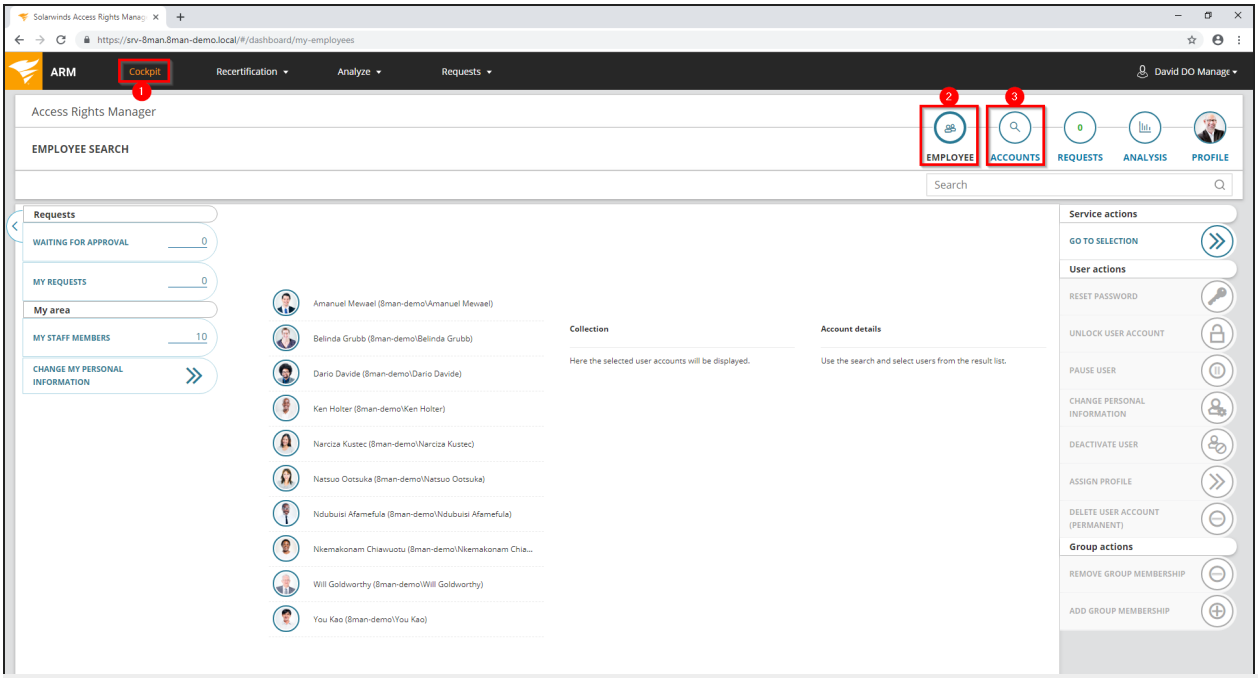
Background / Value

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

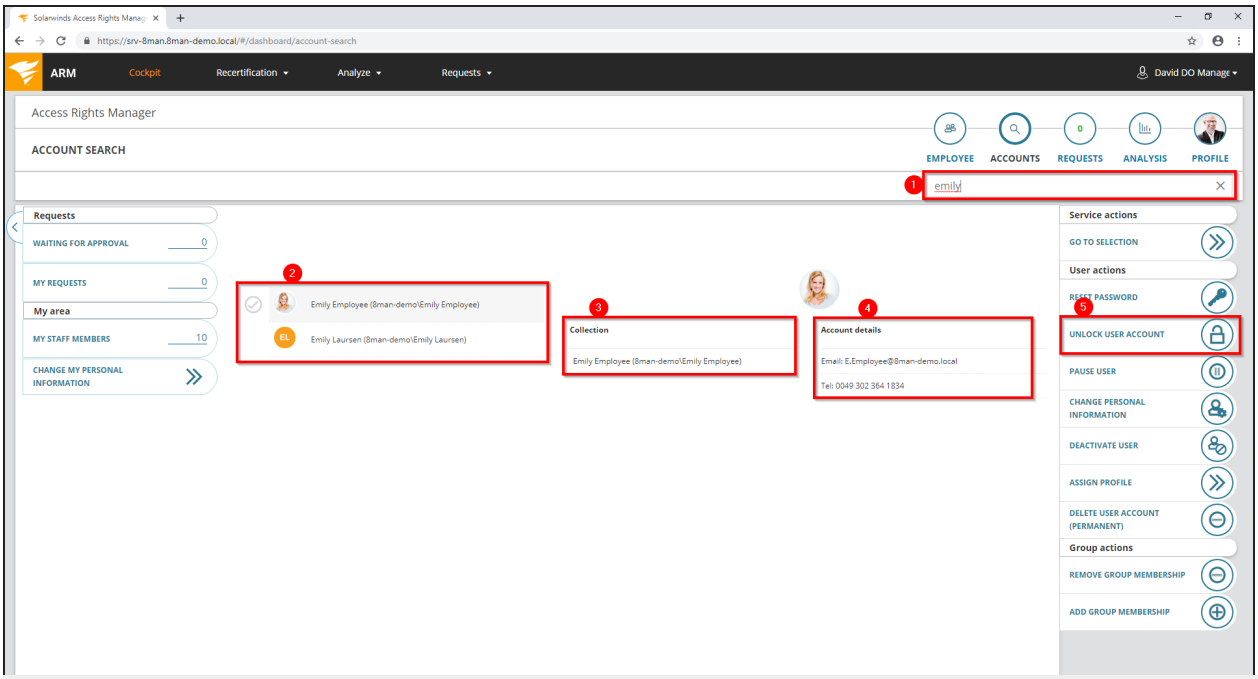
Reset users' passwords (Cockpit)

Step-by-step process

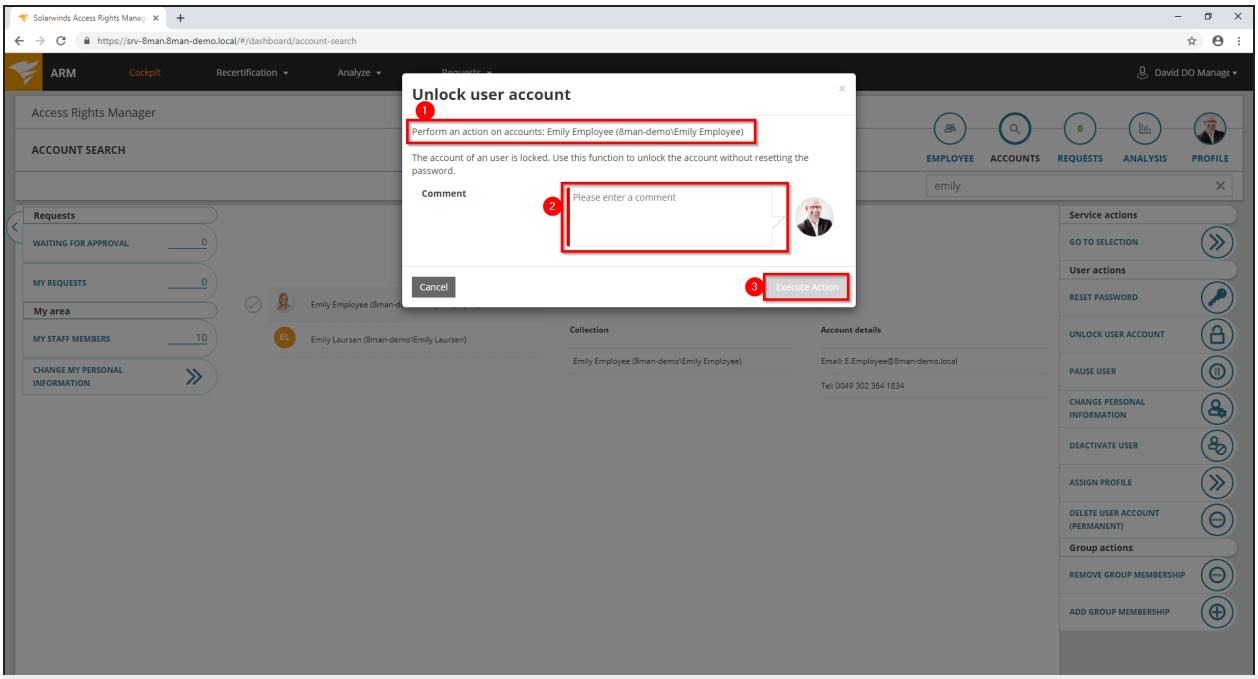


1. Choose Cockpit.
2. Choose "Employee". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See Changing Attributes (Web Client).
3. Choose "Accounts". Accounts for data owners are assigned by an ARM administrator in the data owner configuration.

The range of available features (buttons) varies according to role (login), risk assessment and configuration.



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

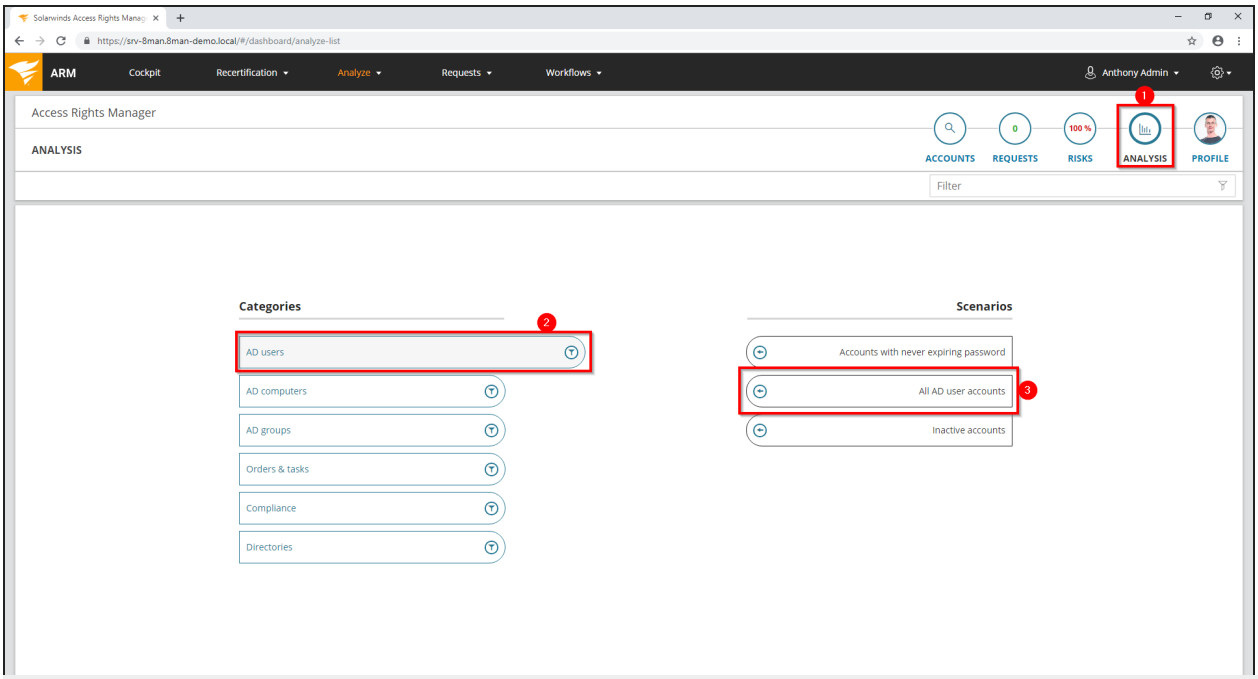
There are many use cases in which the passwords of several users must be reset simultaneously. You can reset passwords in bulk in the web interface.

Related features

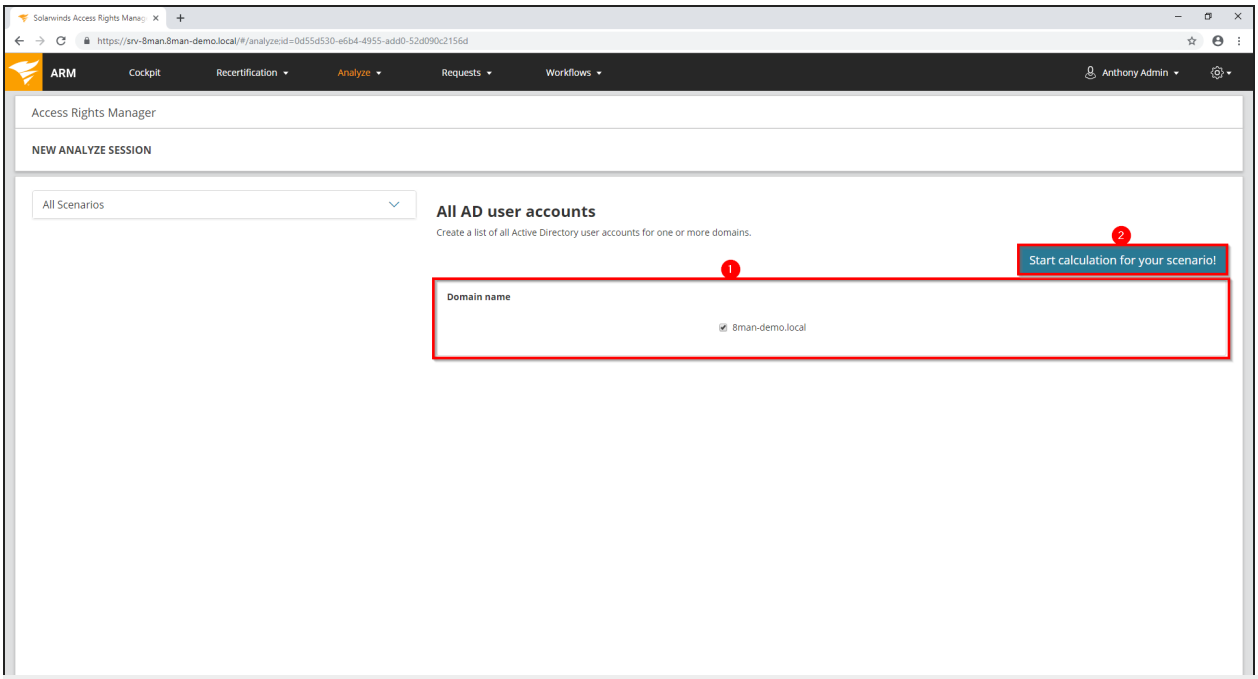
Deactivate user accounts in bulk (web client)

Change password options in bulk (web client)

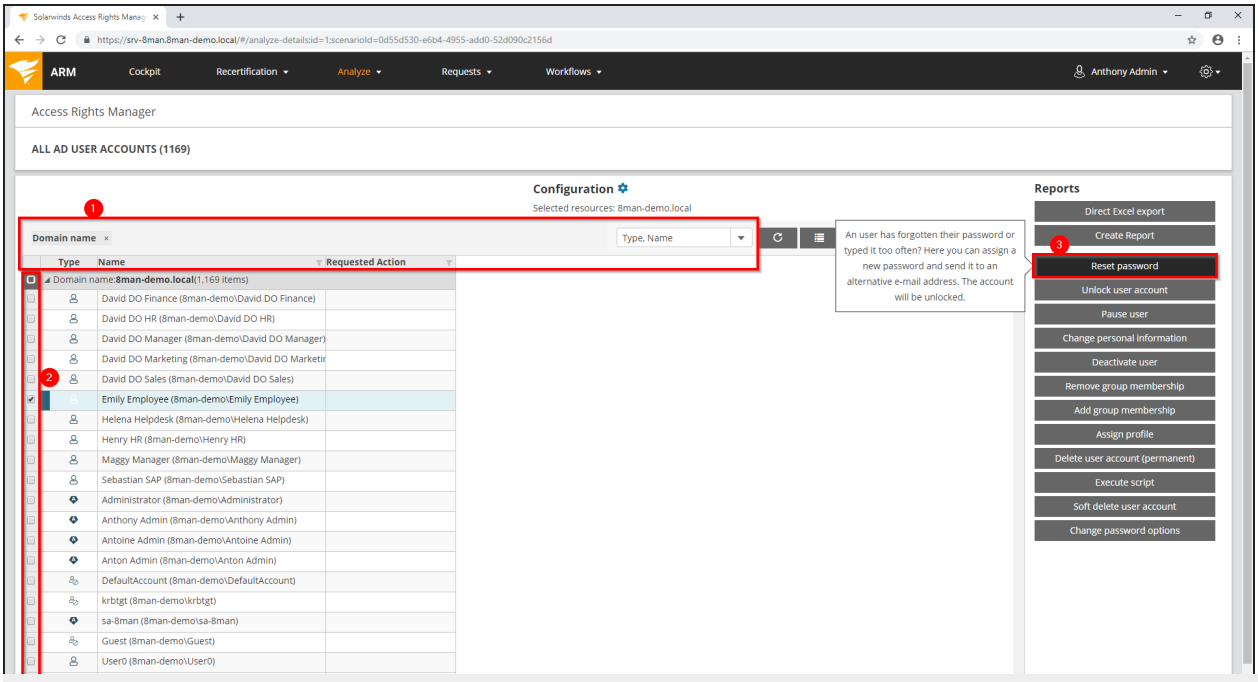
Step-by-step process



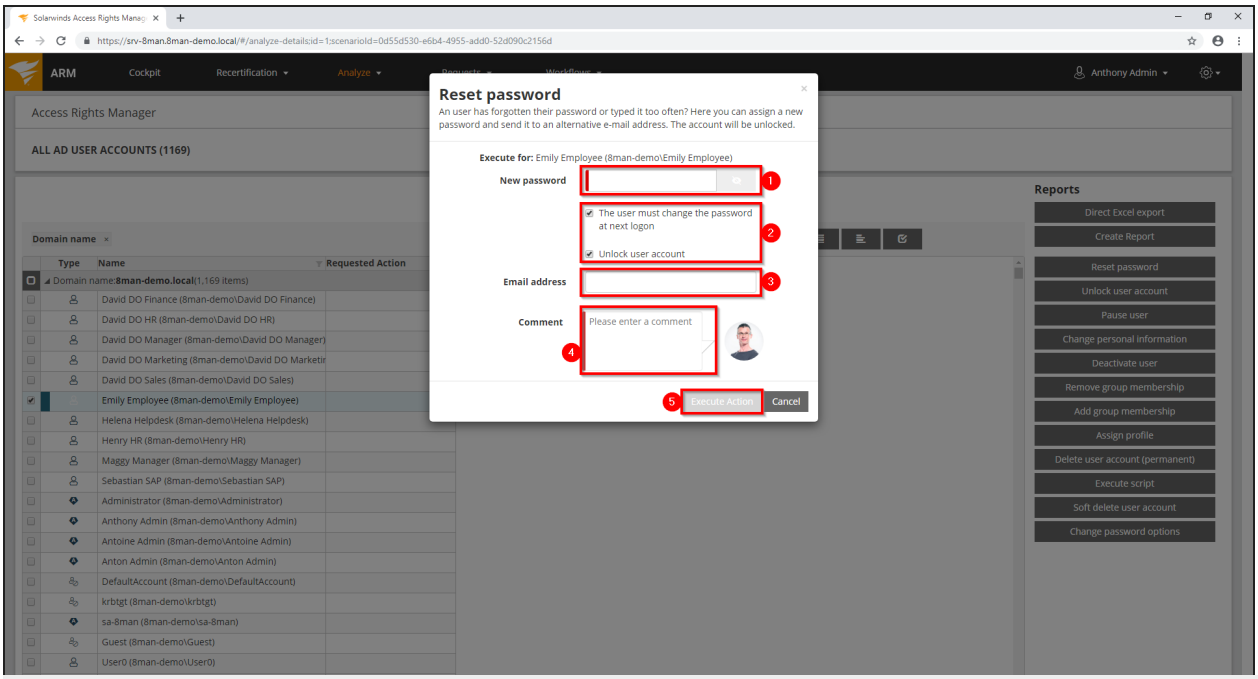
1. Click "Analysis".
2. Select the category "AD users".
3. Click on "All AD user accounts".



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.

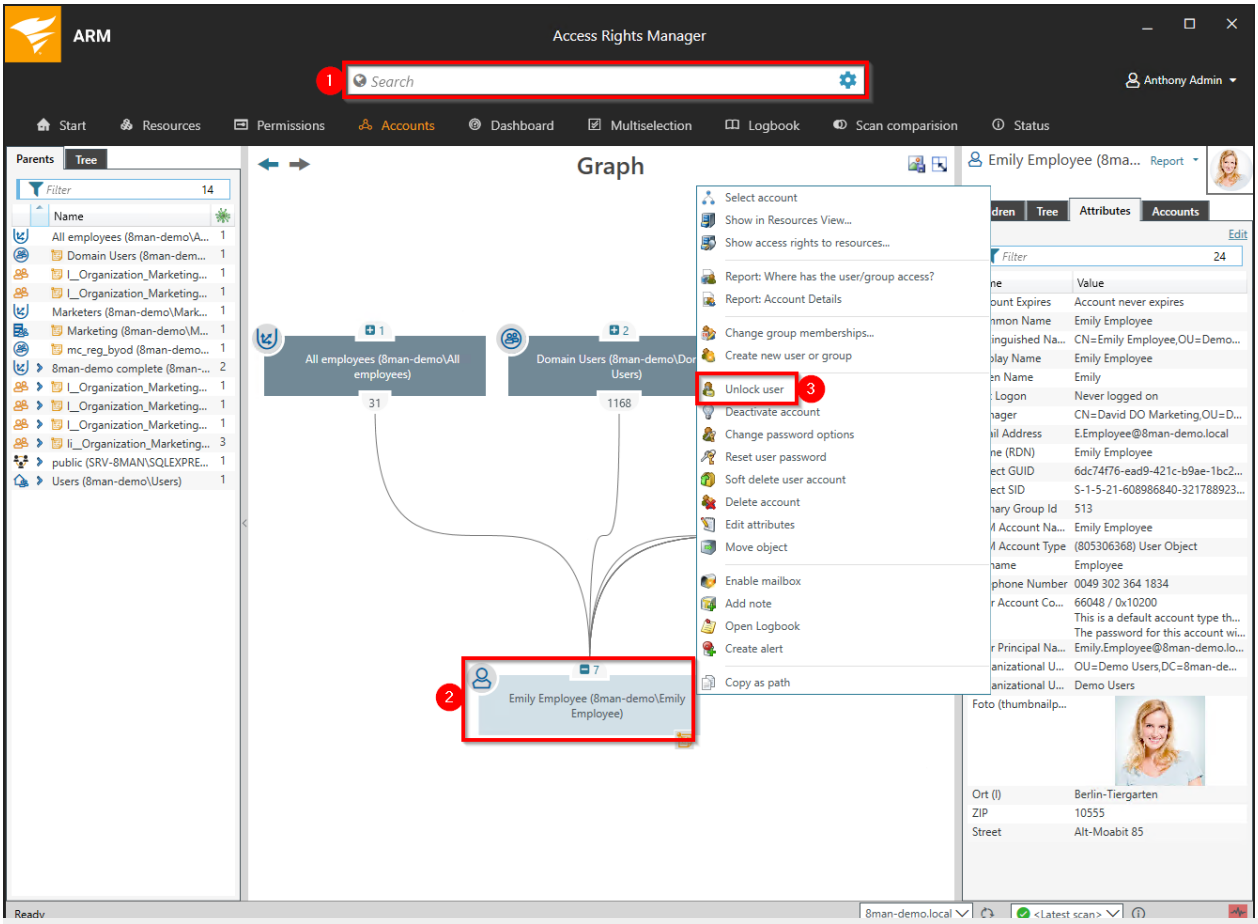
Related features

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

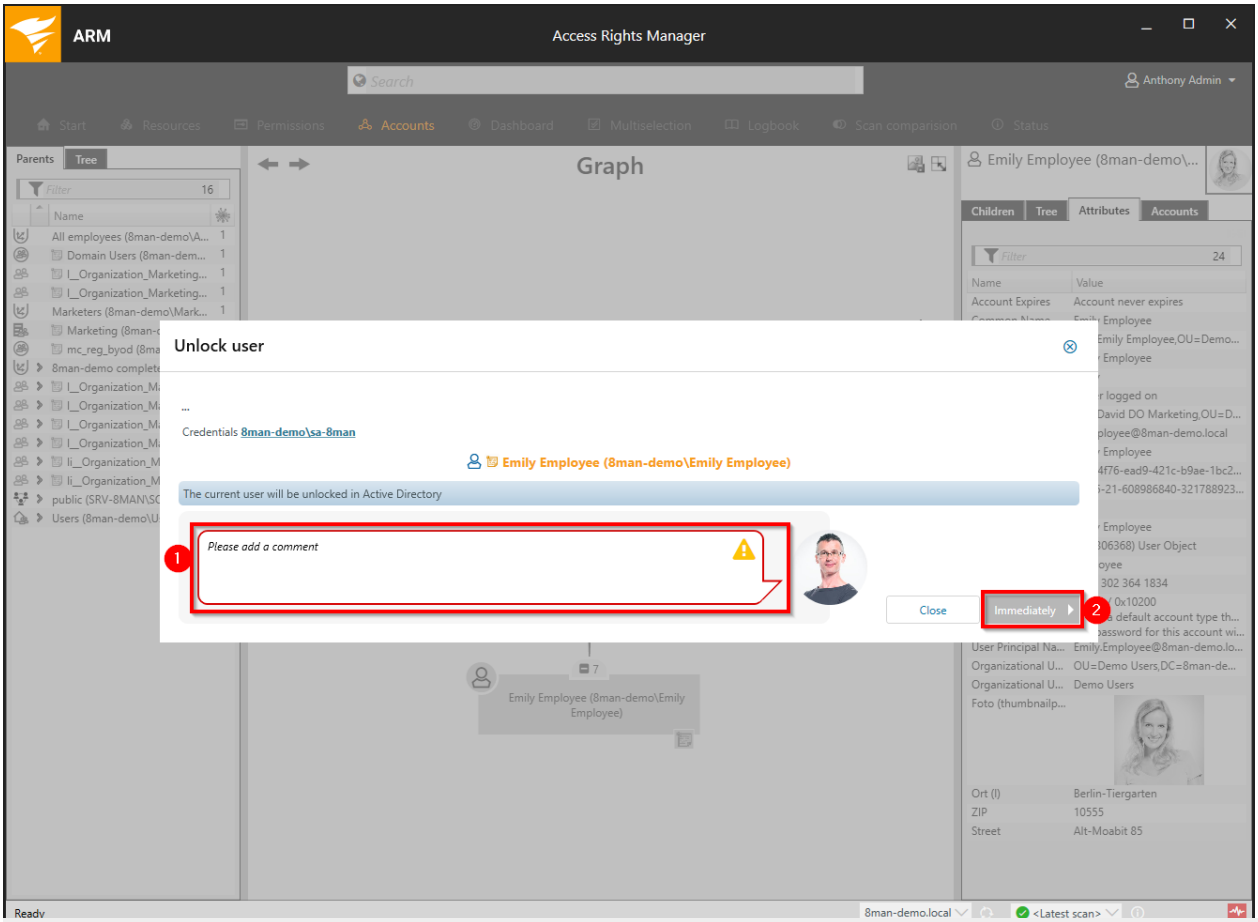
AD Logga: Set alerts for user accounts

Step-by-step process



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.



1. You must enter a comment.
2. Start the unlocking process.

Background / Value

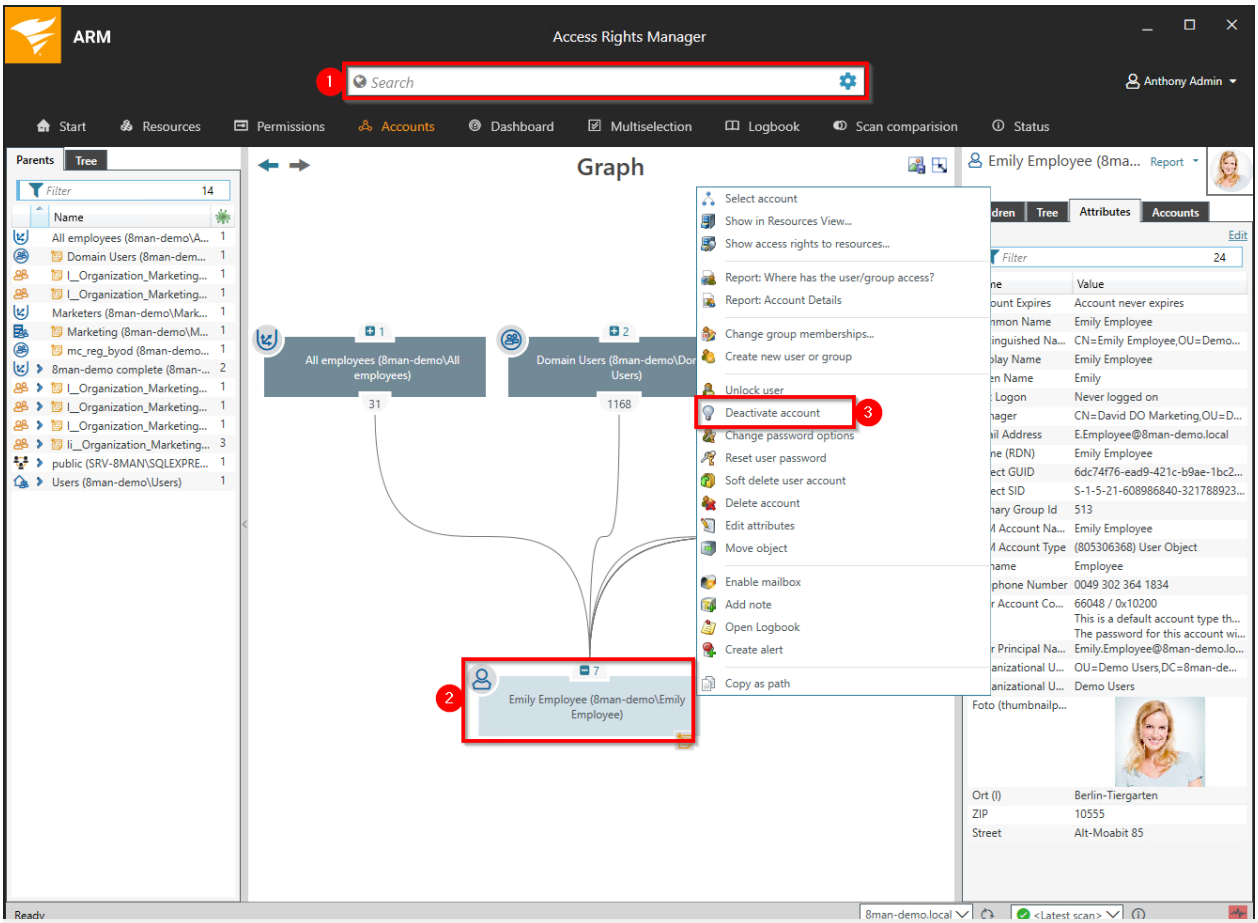
If you deactivate an account with ARM, this is equivalent to a normal deactivation with on-board resources. The user account remains in the OU. The process is documented in the logbook.

Related features

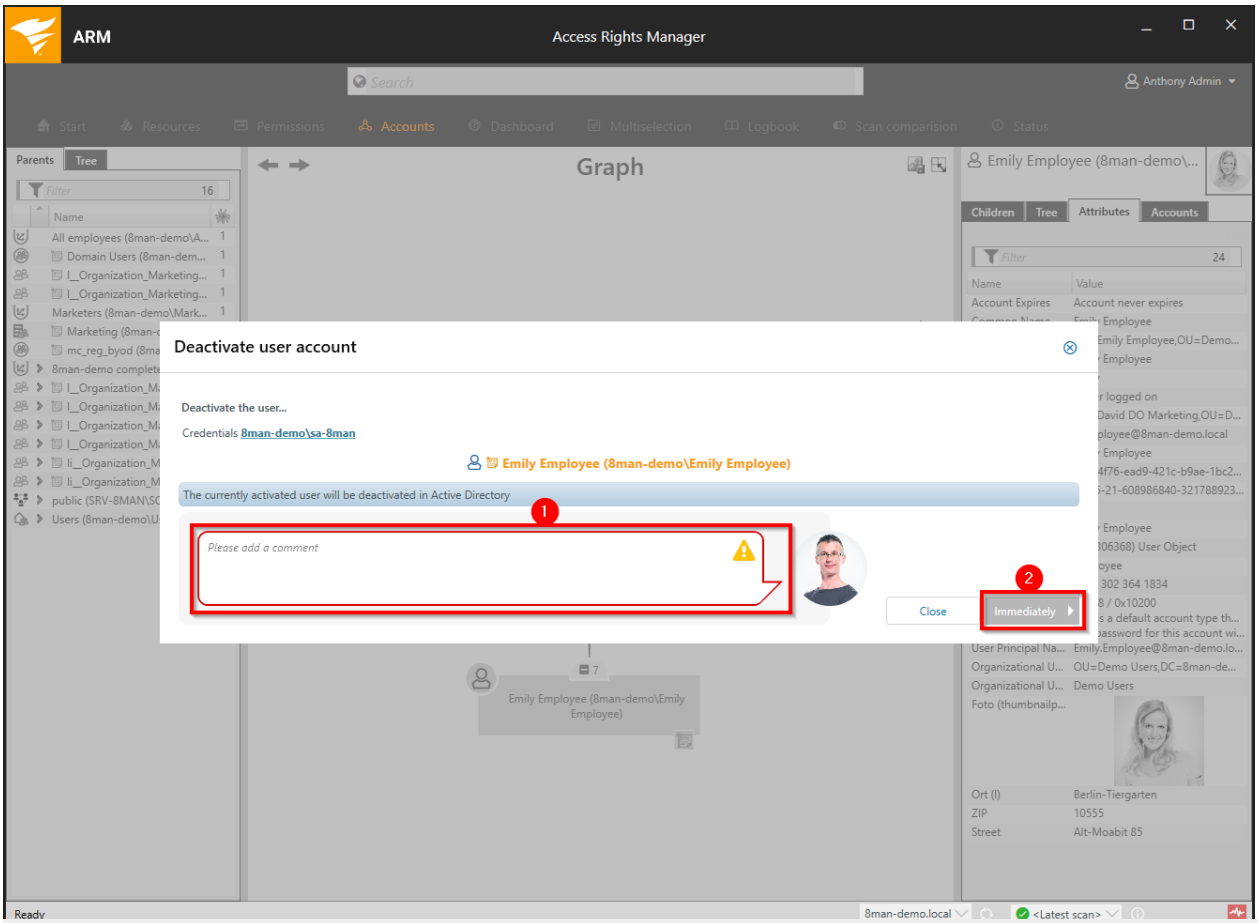
Delete a user with soft delete

Deactivate accounts in bulk (web client)

Step-by-step process



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

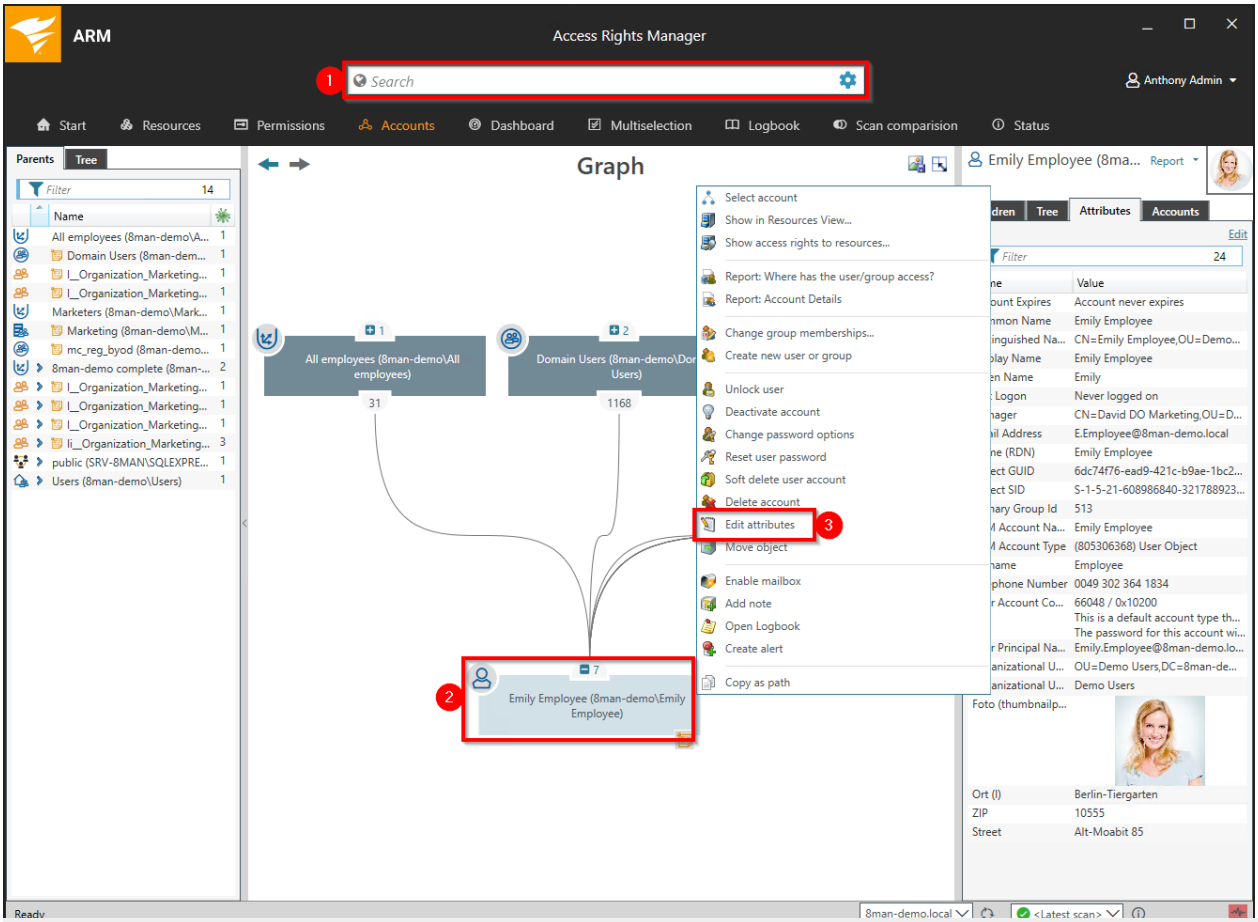
Background / Value

With ARM you can easily manage attributes for users, groups or computers. All actions are automatically documented.

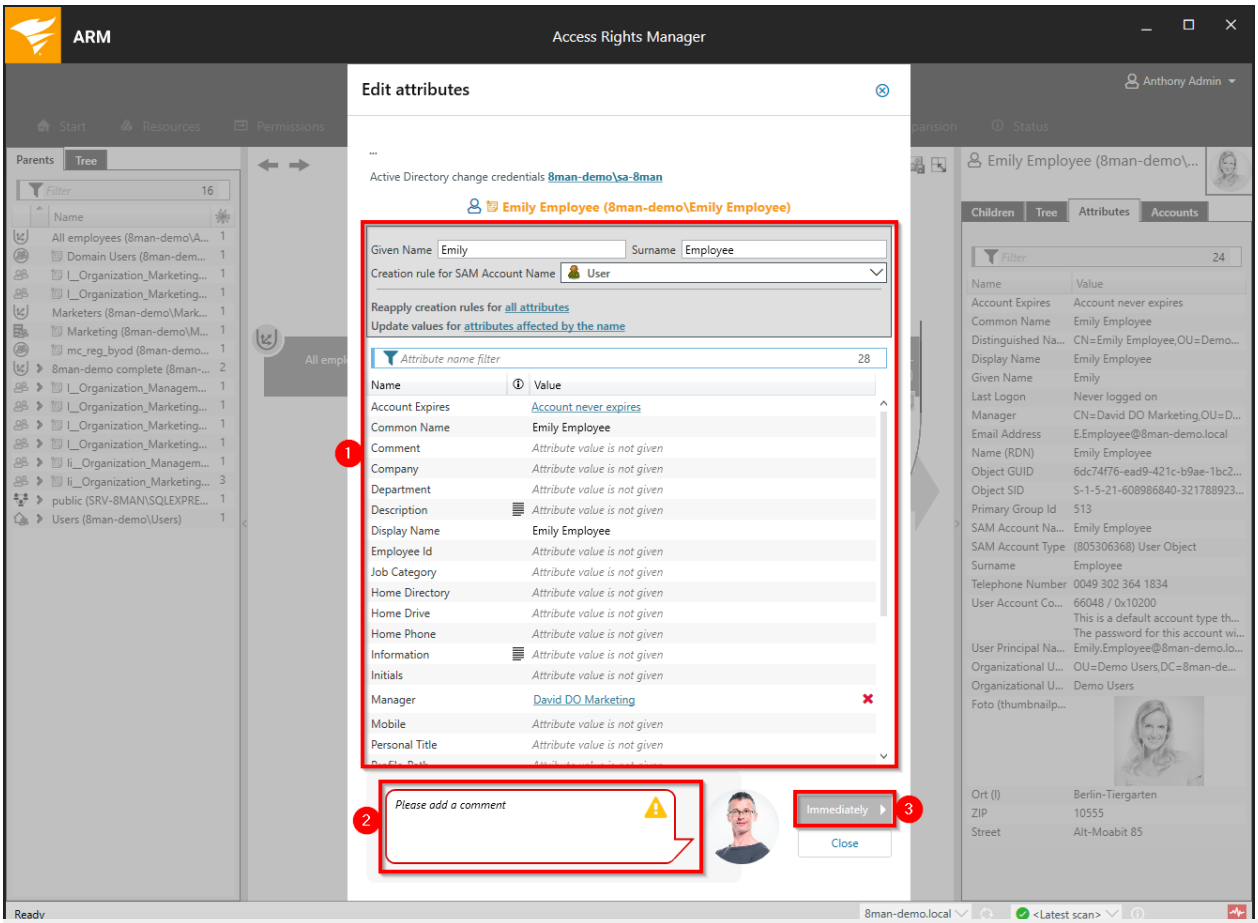
Related features

Modify attributes in bulk (web client)

Step-by-step process



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.



1. Change the desired attributes.

Which attributes are available depends on the account type and on your configuration of additional attributes.

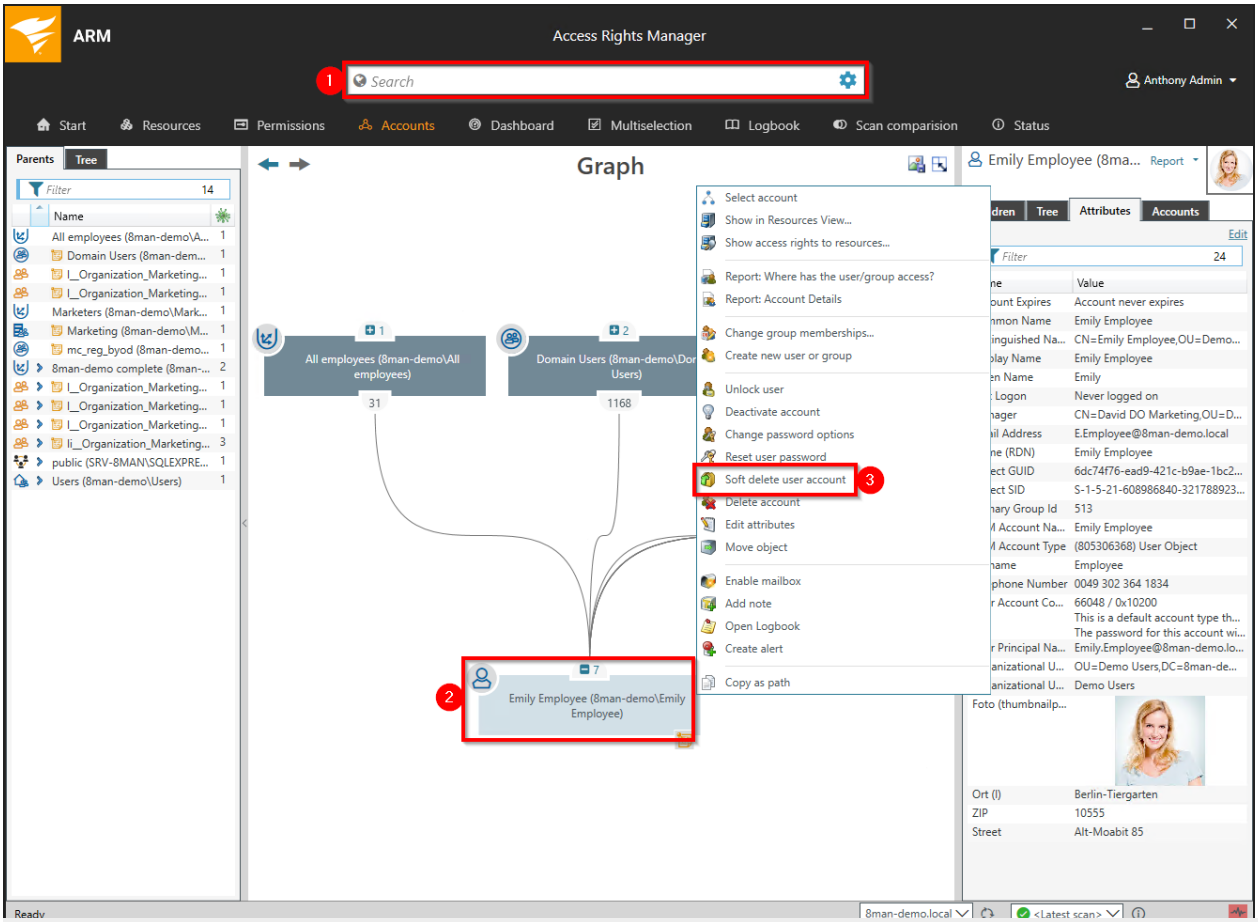
2. You must enter a comment.
3. Start the execution.

Background / Value

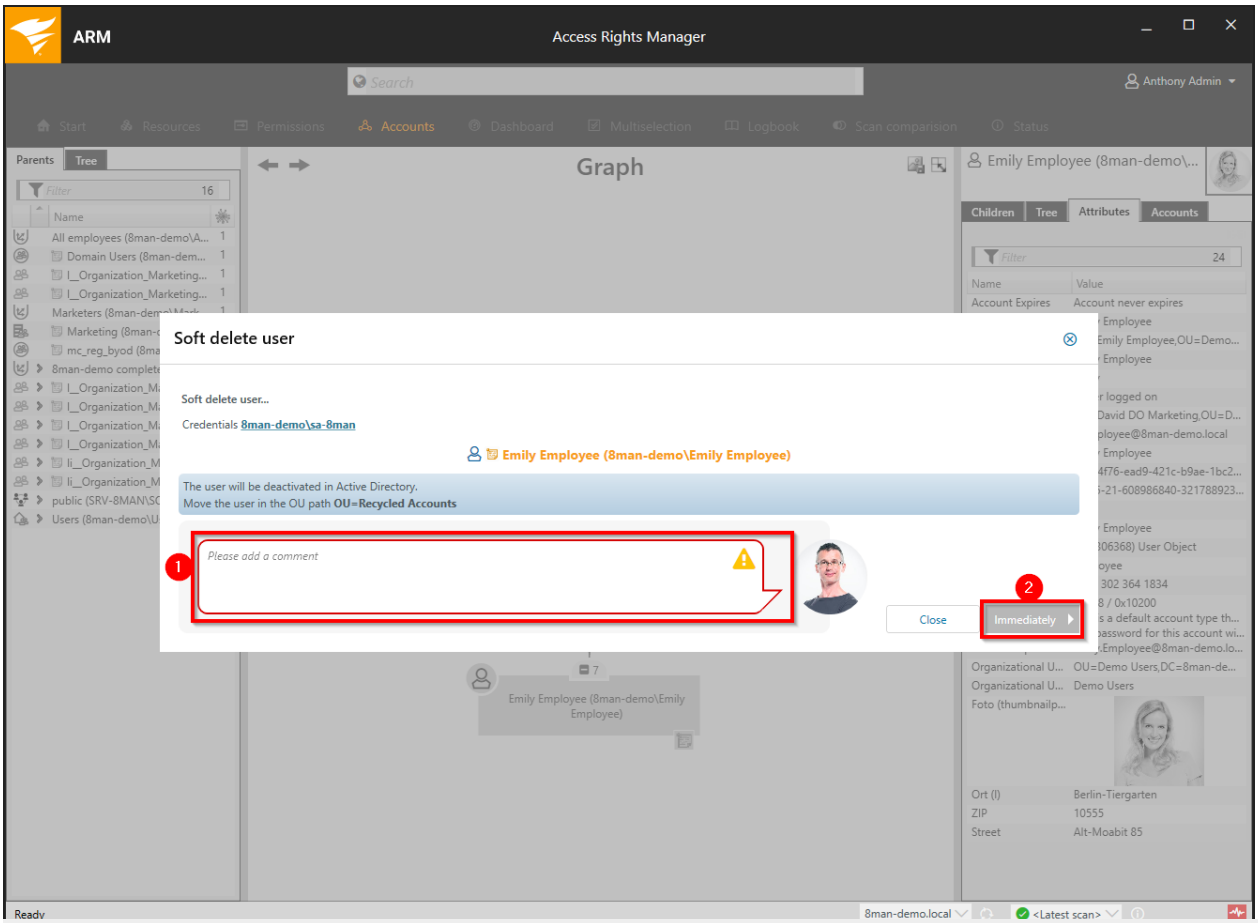
If a user is deleted with "Soft Delete", all his access rights are retained. The account is moved to a "Recycling OU" and deactivated. This account can no longer be used for a login. Set a strictly limited Group Policy for the "Recycling OU".

How to set the "Recycling OU" is described in the chapter "AD change configuration".

Step-by-step process



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

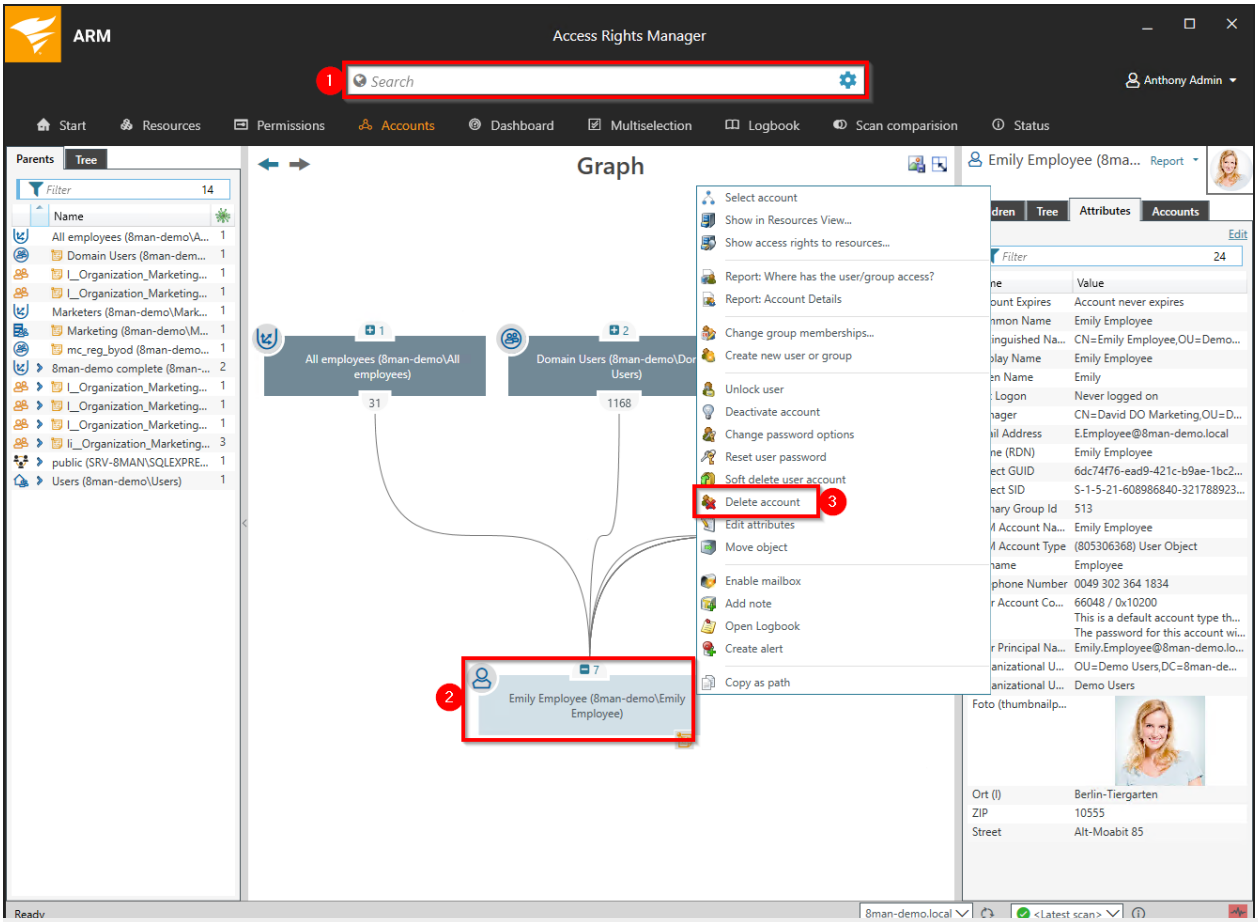
Background / Value

With ARM you can delete the user from AD and remove all of their access rights on the file server in one easy action.

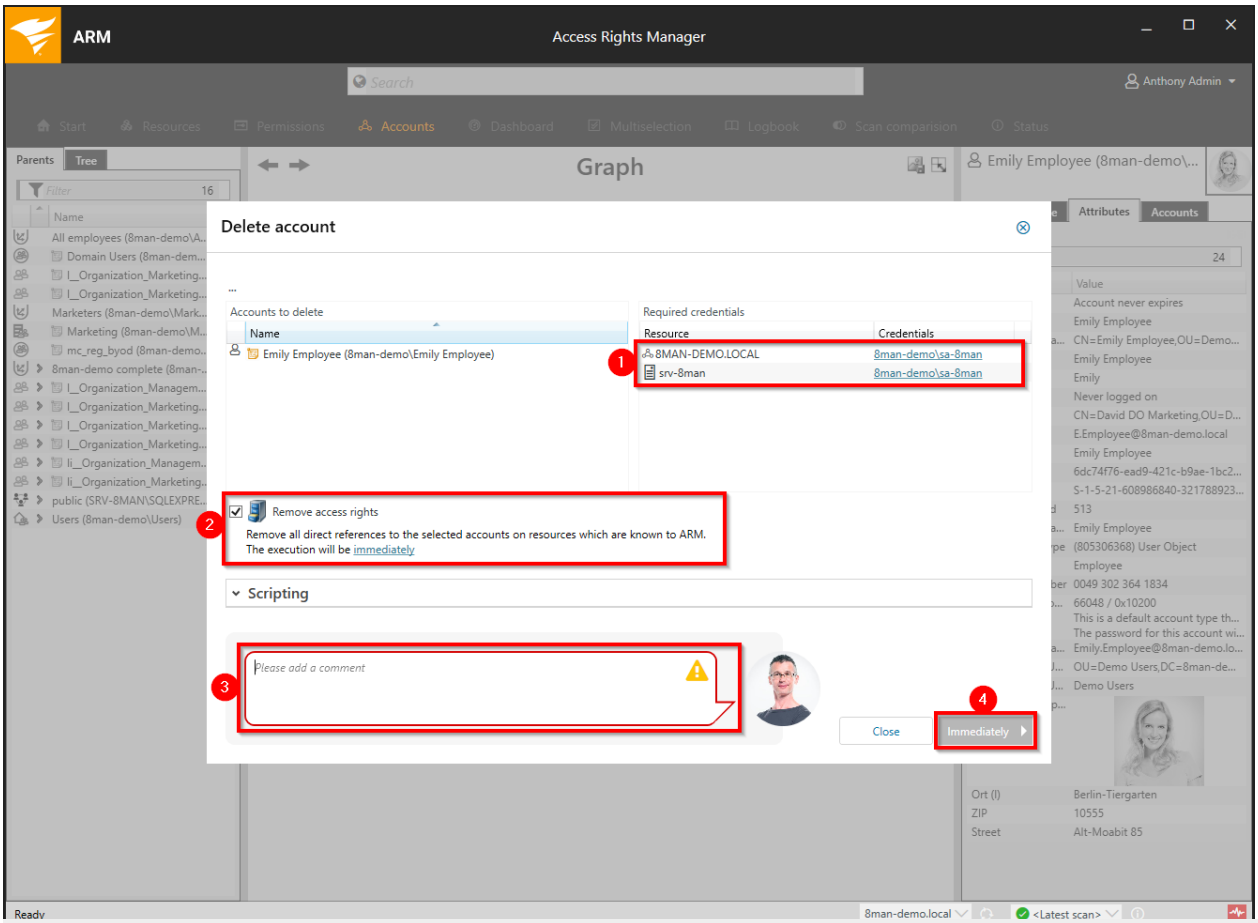
Related features

Remove direct permissions in bulk (web client)

Step-by-step process



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.



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.

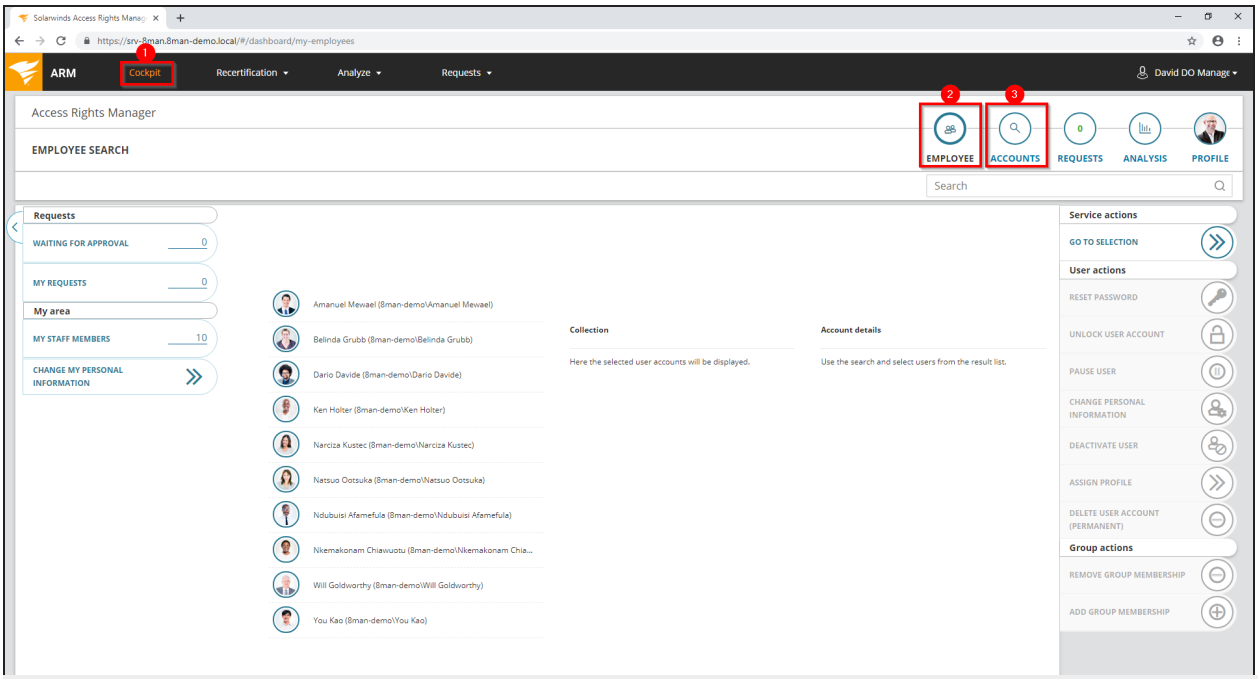
Data Owner/Manager

Reset users' passwords (cockpit)

Background / Value

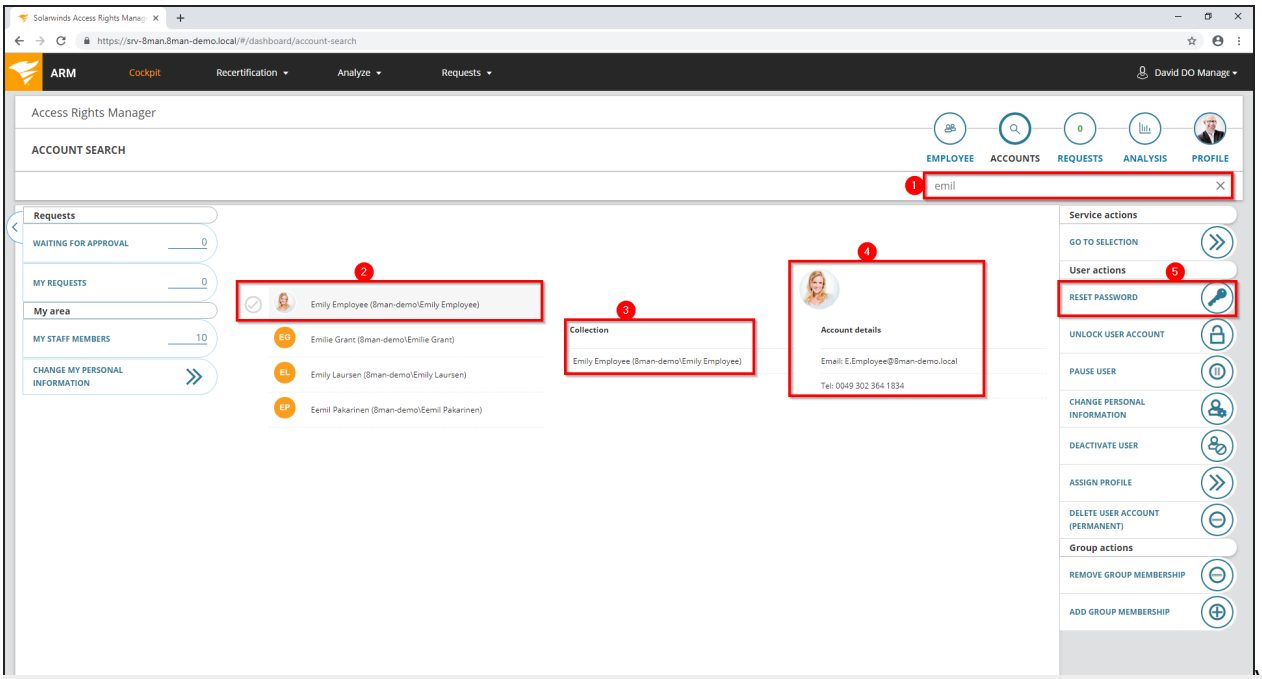
Resetting passwords is one of the most common Helpdesk operations. ARM also allows you to delegate password resets to data owners or managers. The security-critical action is recorded in the logbook.

Step-by-step process

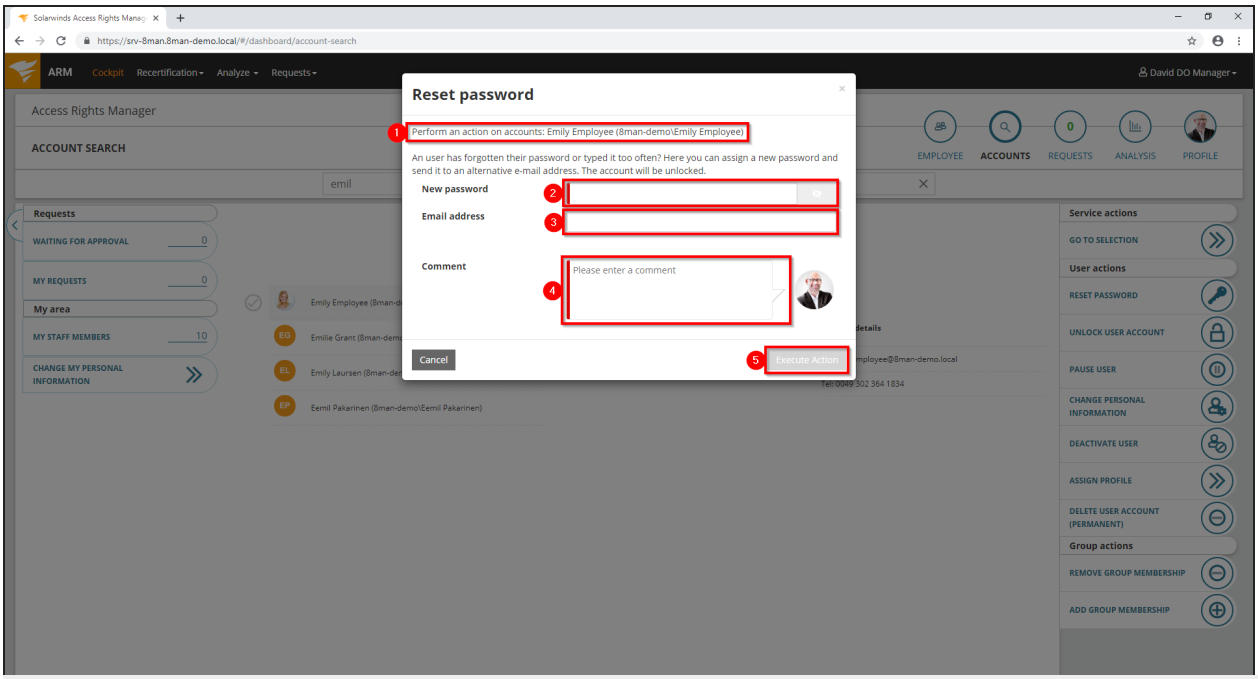


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

The range of available services (buttons) varies according to role (login), risk assessment and configuration.



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

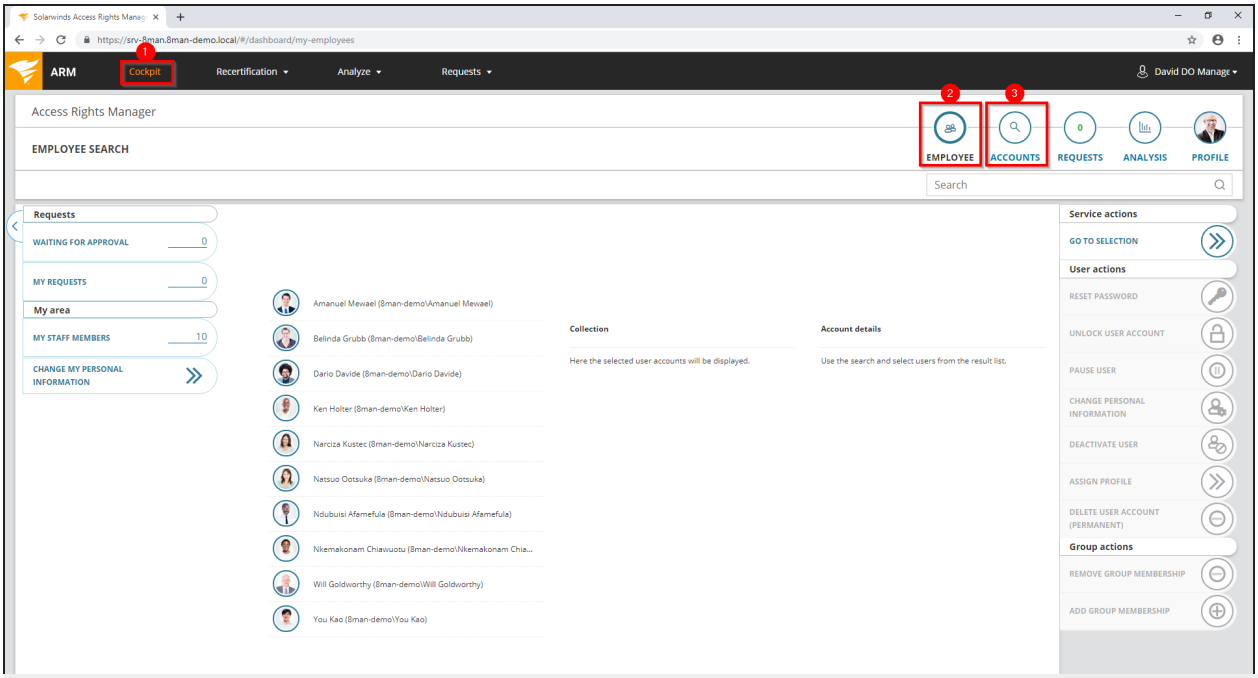
These options are always activated if logged in as a non-administrative user.

Change account data of users (cockpit)

Background / Value

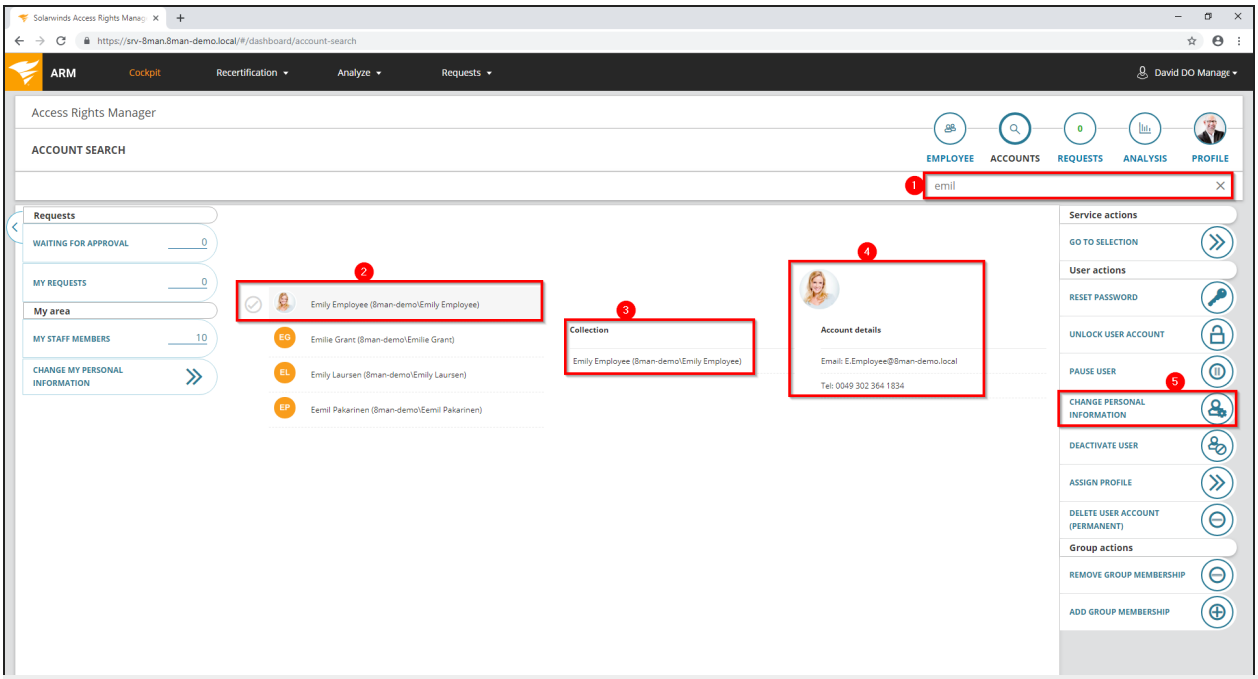
With ARM, you can quickly and easily change user account information, even from multiple users in one go. The actions are documented auditable.

Step-by-step process

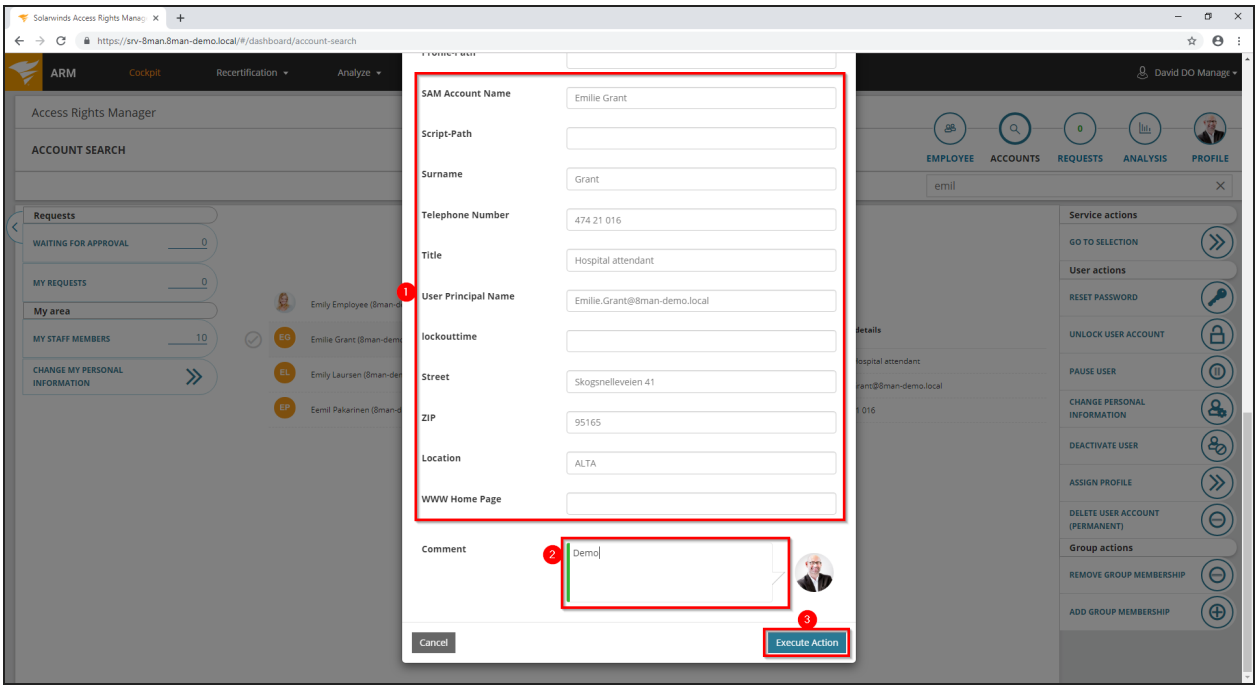


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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".



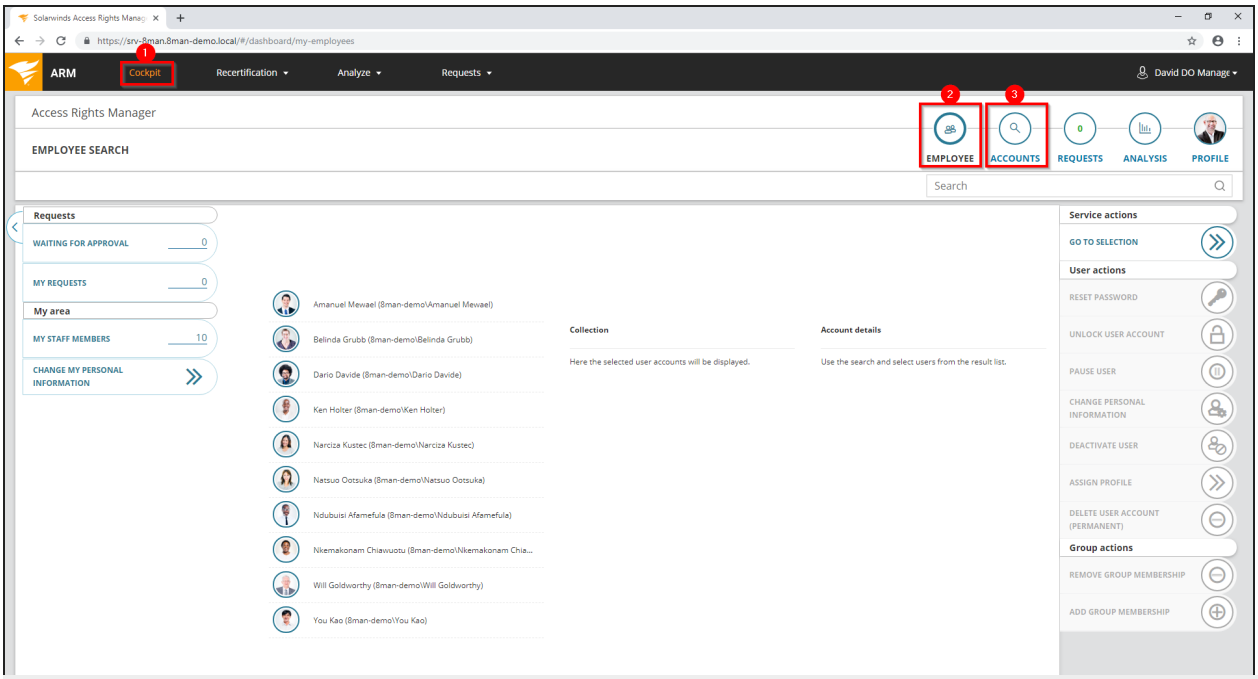
1. Enter the desired changes.
2. You must enter a comment.
3. Click on "Execute Action".

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.

Background / Value

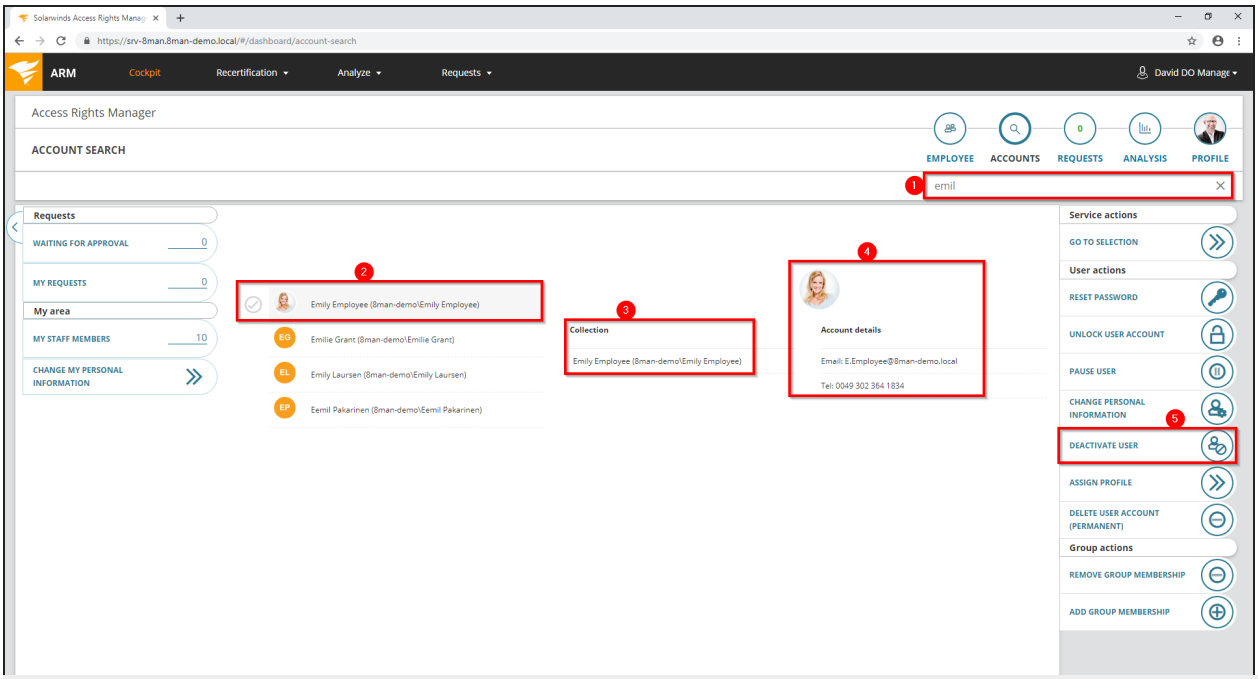
Disable a user in a few steps with ARM. Disable a user account early on discharge.

Step-by-step process

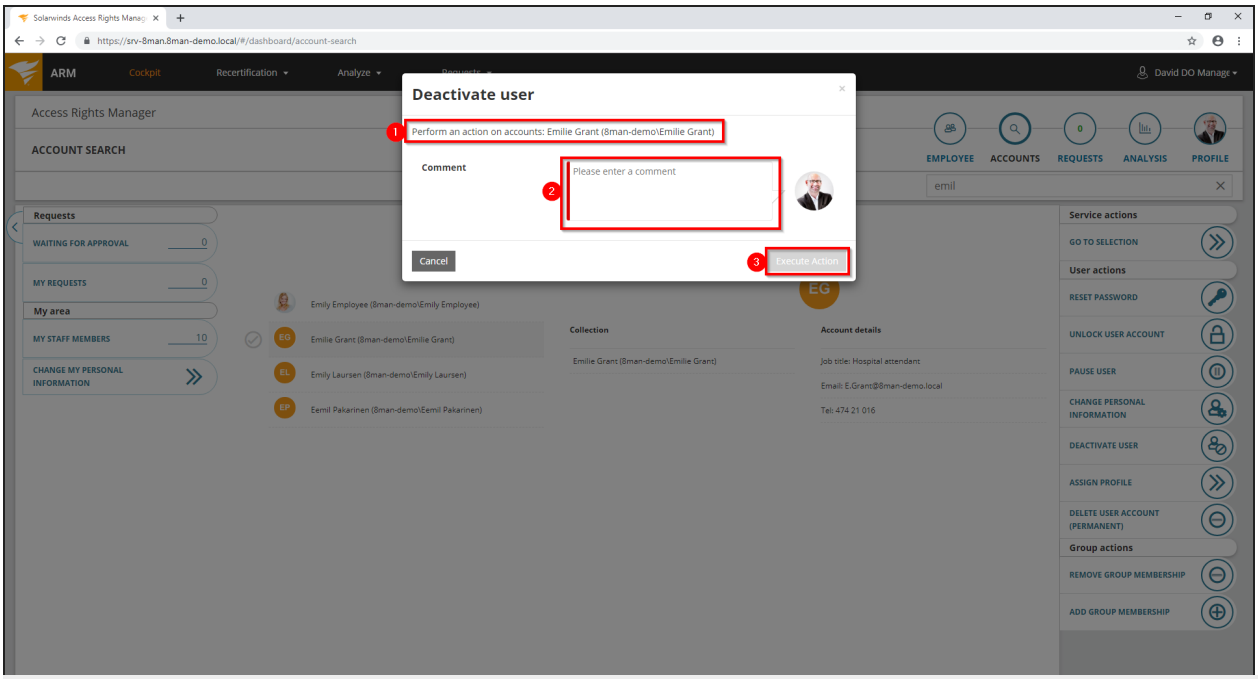


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

The range of available services (buttons) varies according to role (login), risk assessment and configuration.



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".



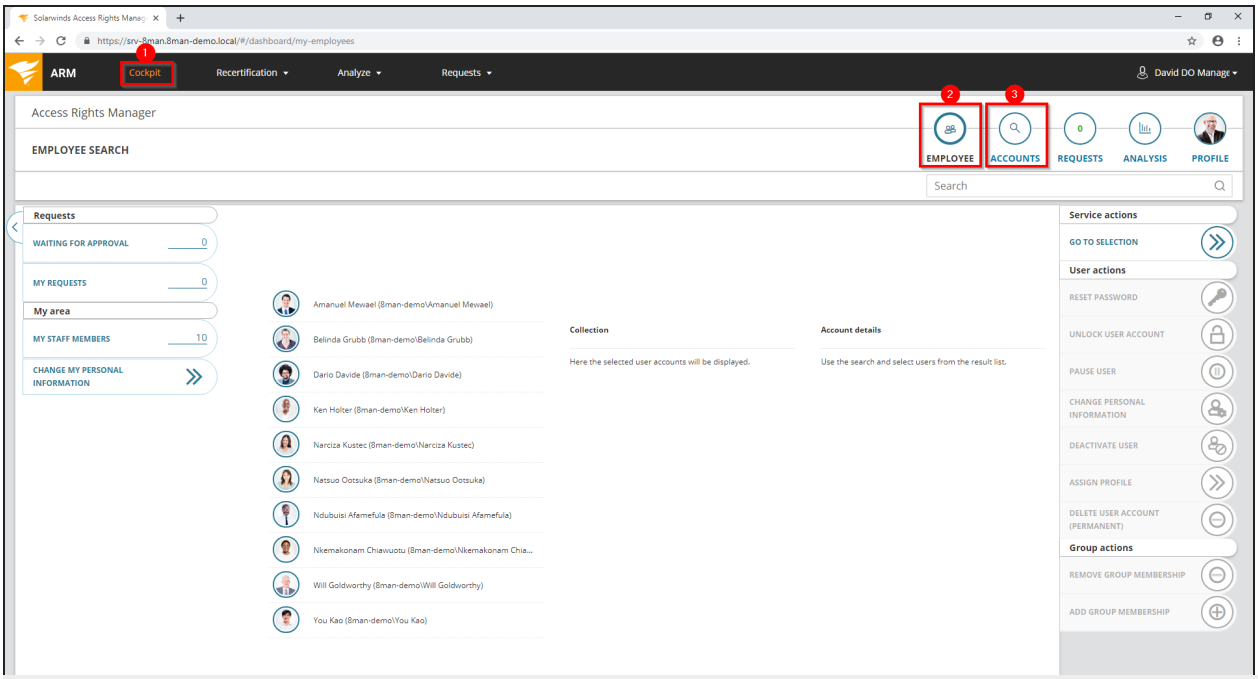
1. ARM shows you which accounts you have selected and want to deactivate.
2. You must enter a comment.
3. Click on "Execute Action".

Pause user (cockpit)

Background / Value

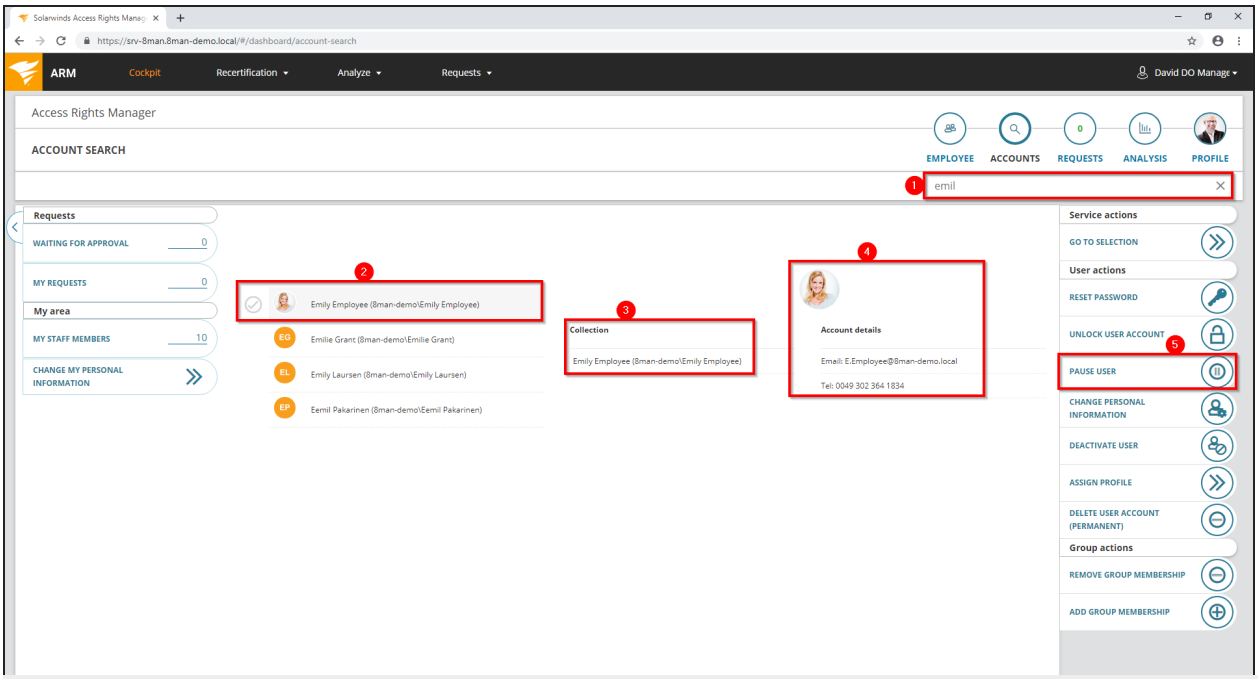
Pause an employee in a few simple and quick steps, e.g. at parental leave.

Step-by-step process

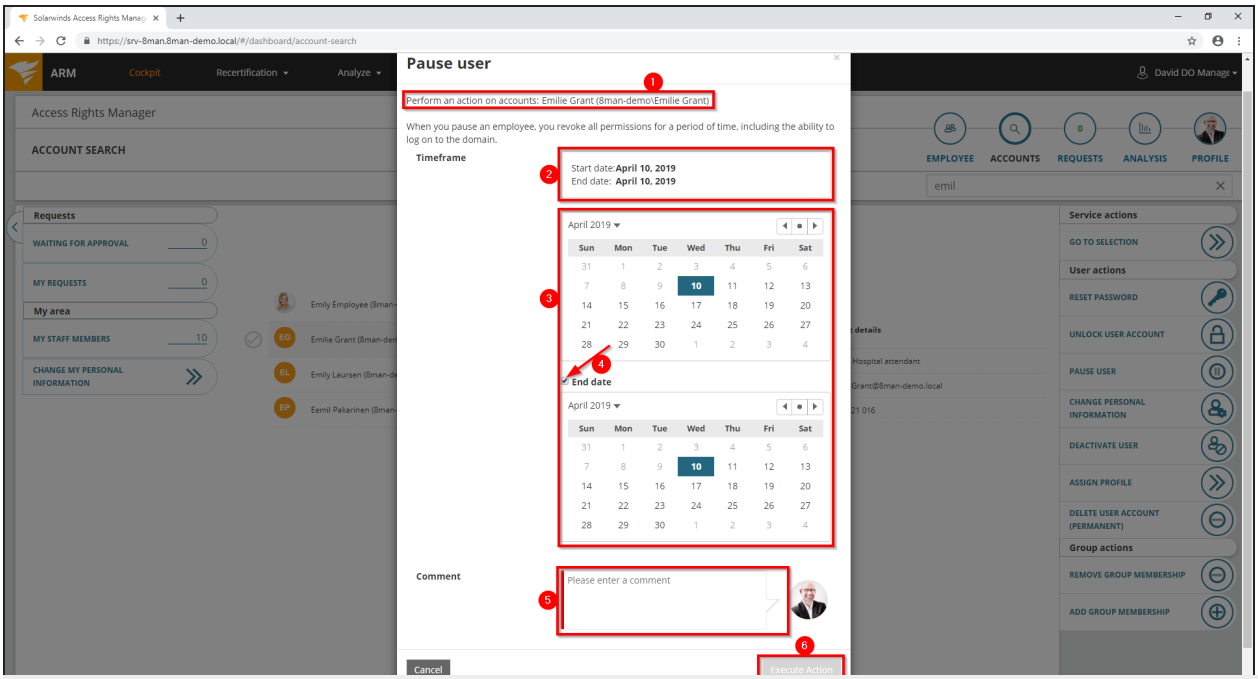


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

The range of available services (buttons) varies according to role (login), risk assessment and configuration.



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".



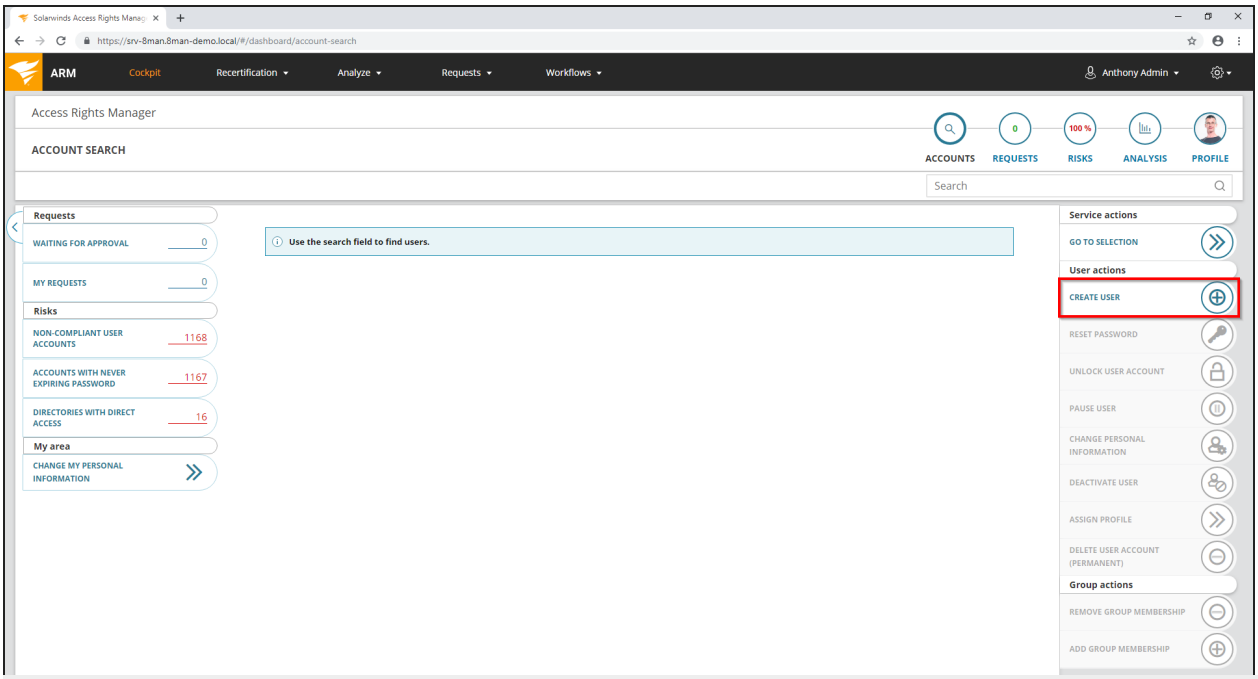
1. ARM shows you which accounts you have selected and want to pause.
2. ARM shows the start and end dates.
3. Set the beginning and the end.
4. If the break is perpetual, deactivate the option "End date".
5. You must enter a comment.
6. Click on "Execute Action".

Create a new user (cockpit)

Background / Value

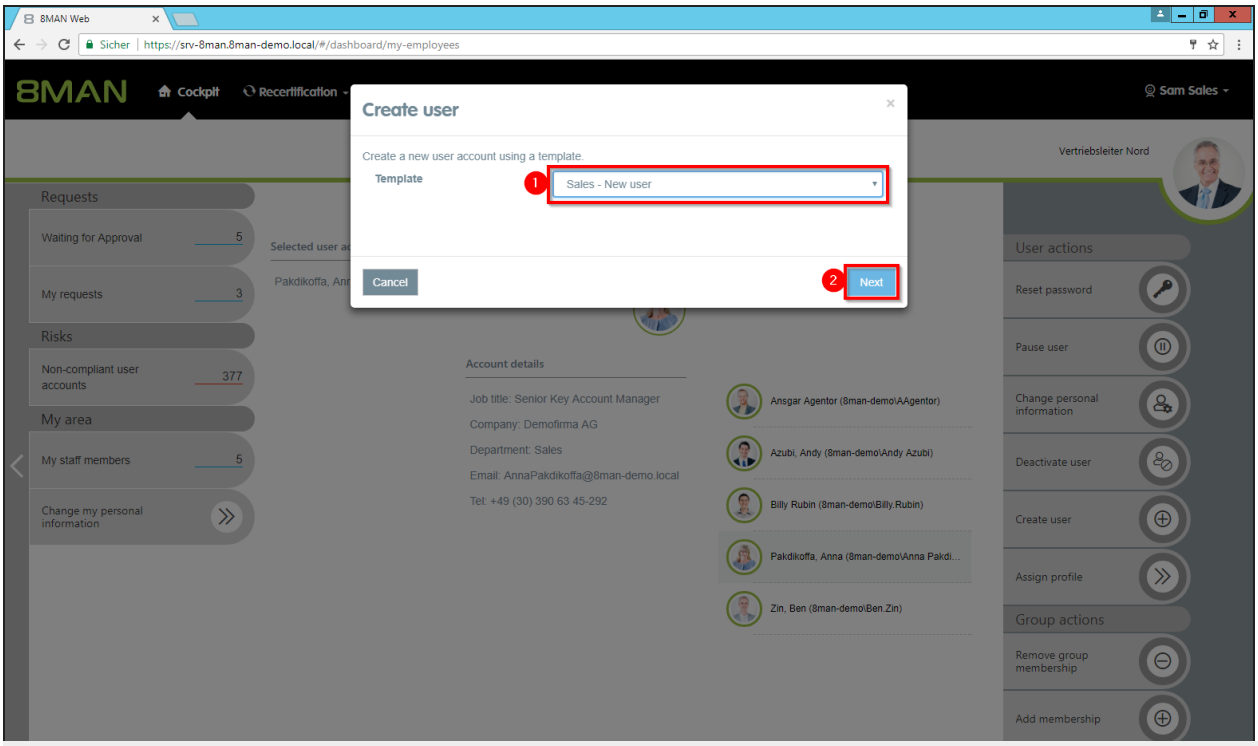
Create a new user in the web client. The creation is based on templates predefined by an administrator and is therefore efficient and standardized.

Step-by-step process

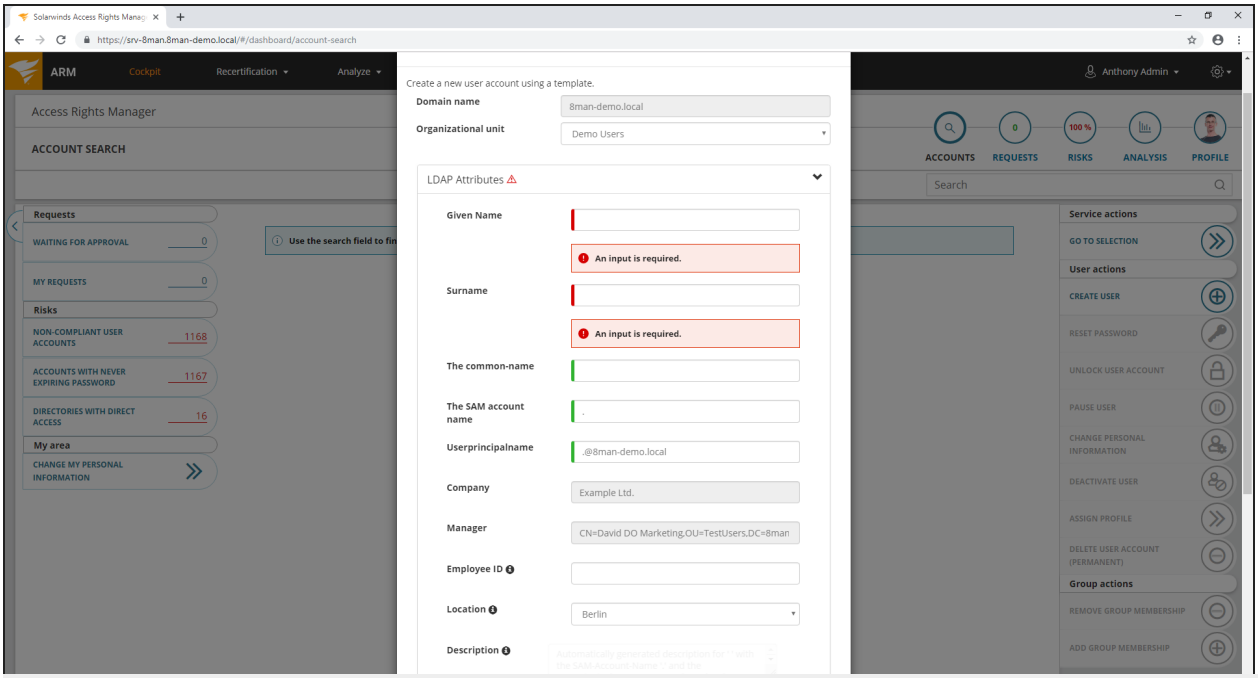


Click on "Create user" in the cockpit.

The range of available services (buttons) varies according to role (login), risk assessment and configuration.

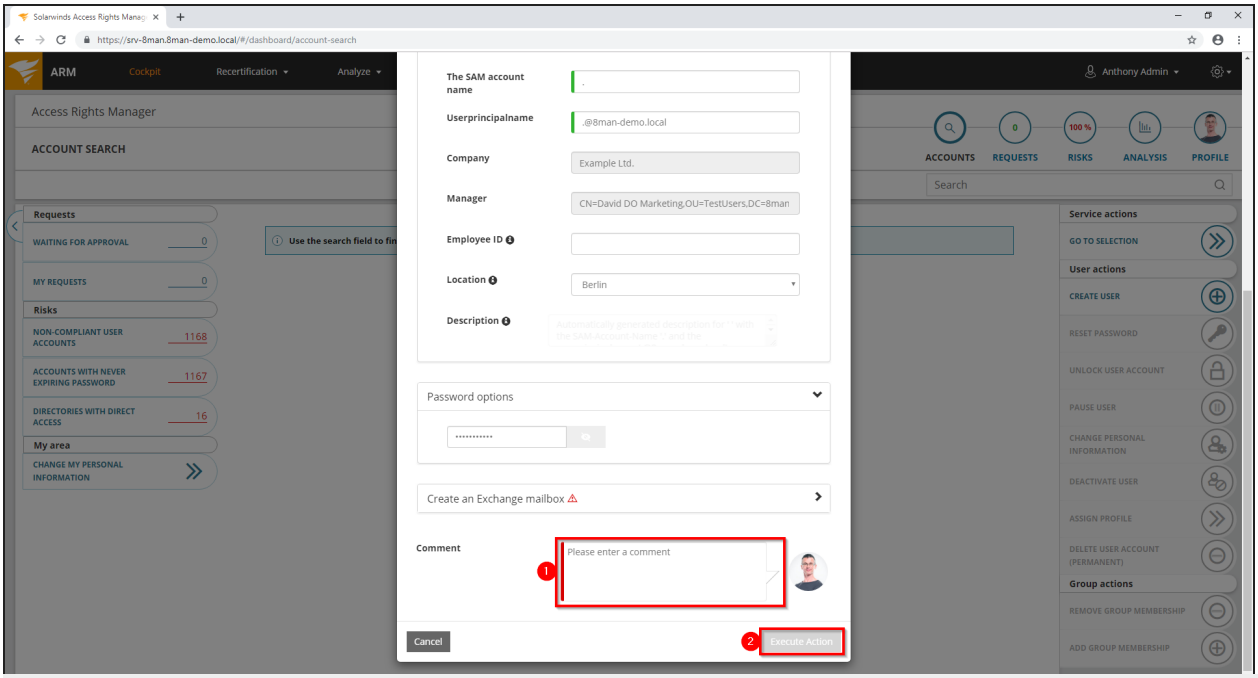


1. Select a template.
2. Click "Next".



Enter the required information.

The amount of information required here can vary widely. User templates must be created by an administrator.



1. You must enter a comment.
2. Click on "Execute Action".

Assign a department profile to users (cockpit)

Background / Value

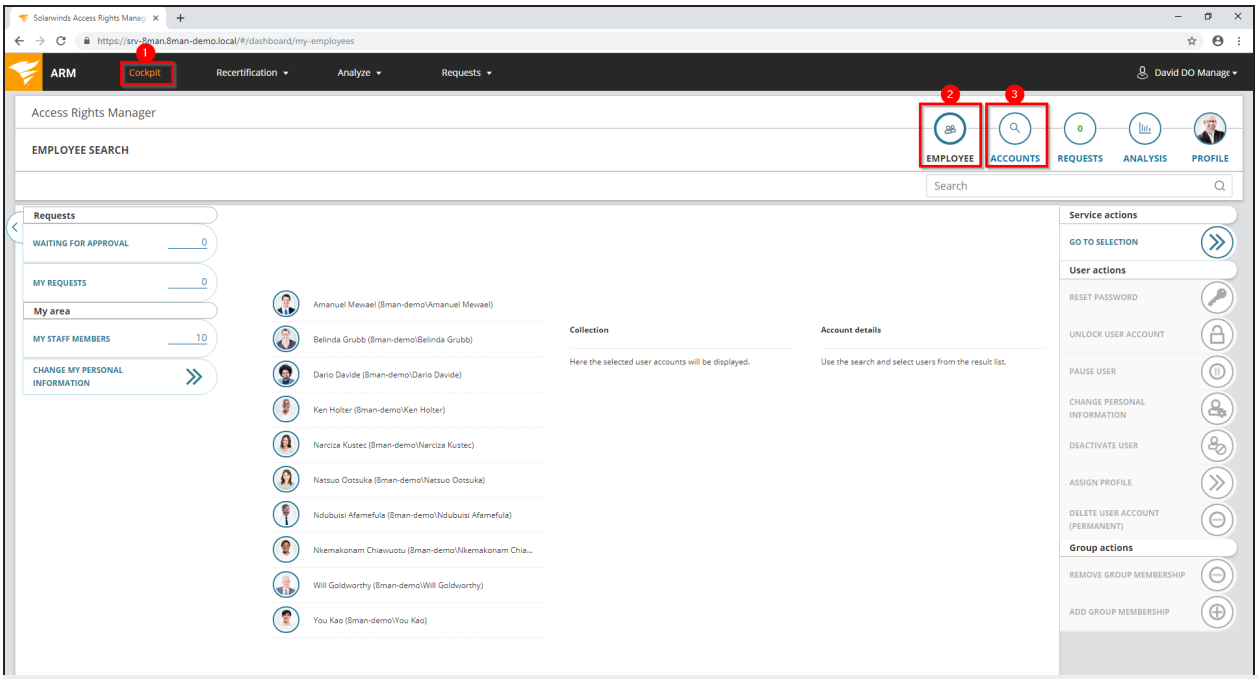
With a department profile, you can assign a basic set of permissions to a user in just a few clicks. If the employee changes department, the supervisor can easily apply his department profile to the corresponding user account.

Related features

Create a new department profile

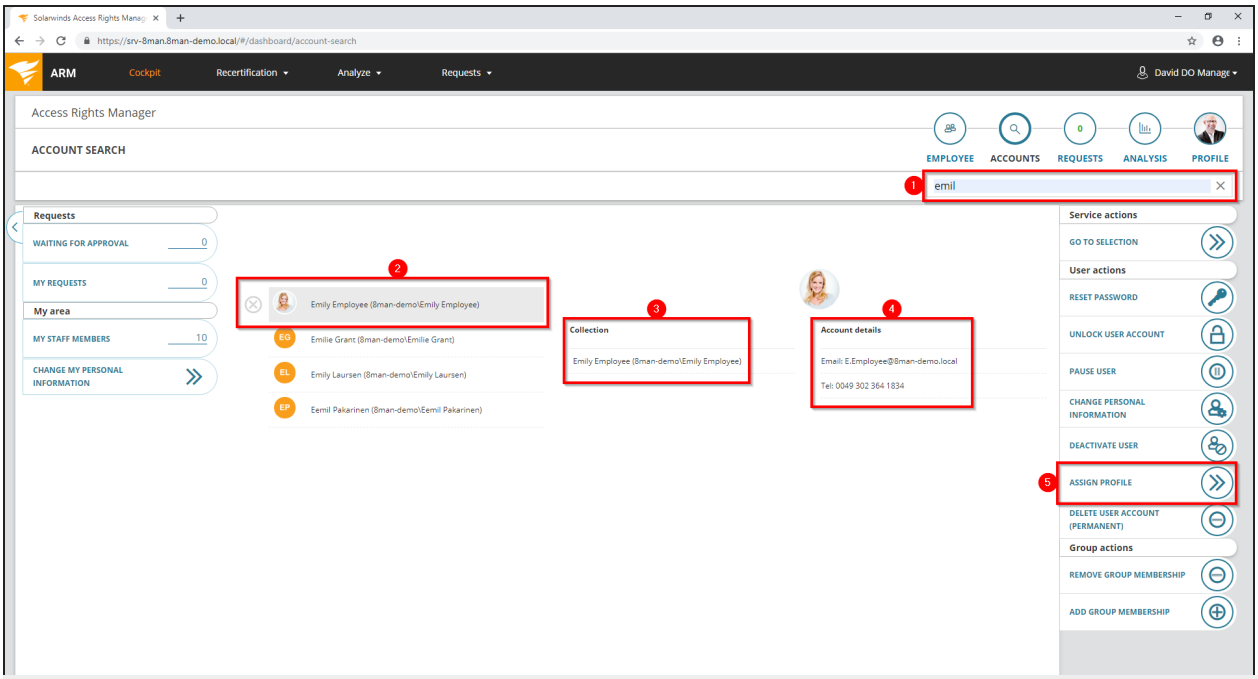
Determine permissions deviating from the department profile (Compliance Check)

Step-by-step process

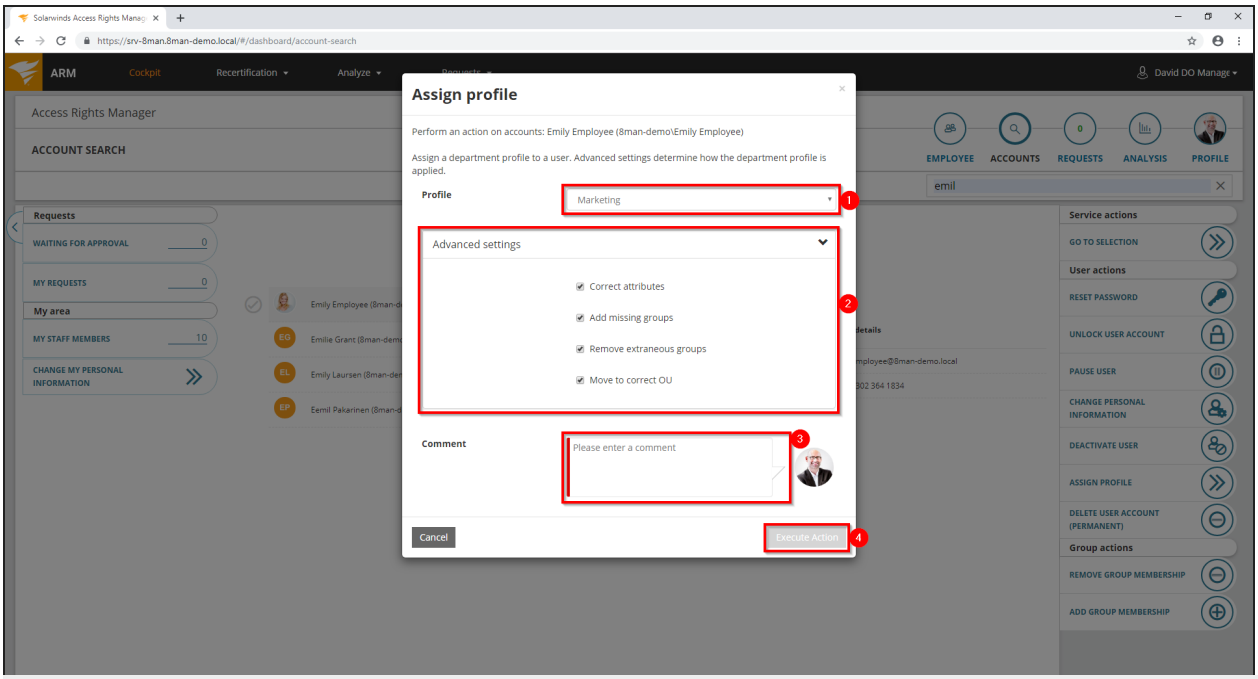


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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 "Assign profile".



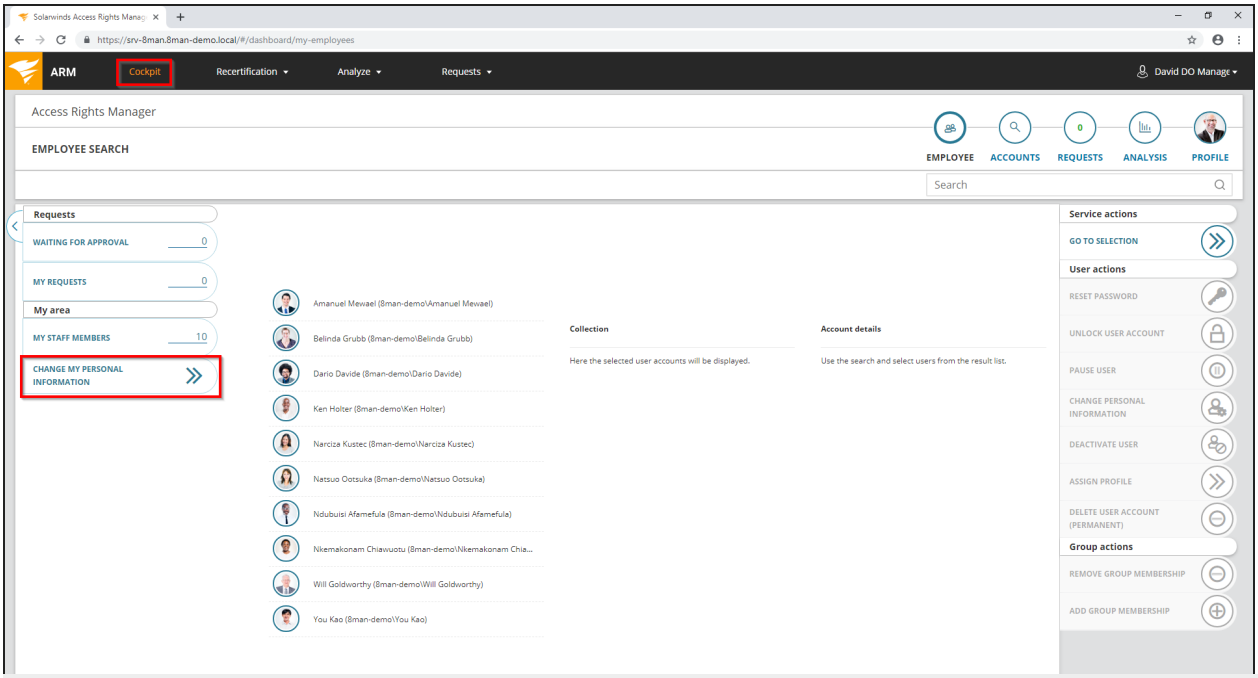
1. Choose a department profile.
2. In the advanced settings, specify how the department profile is applied.
3. You must enter a comment.
4. Click on "Execute Action".

Change your own account information (cockpit)

Background / Value

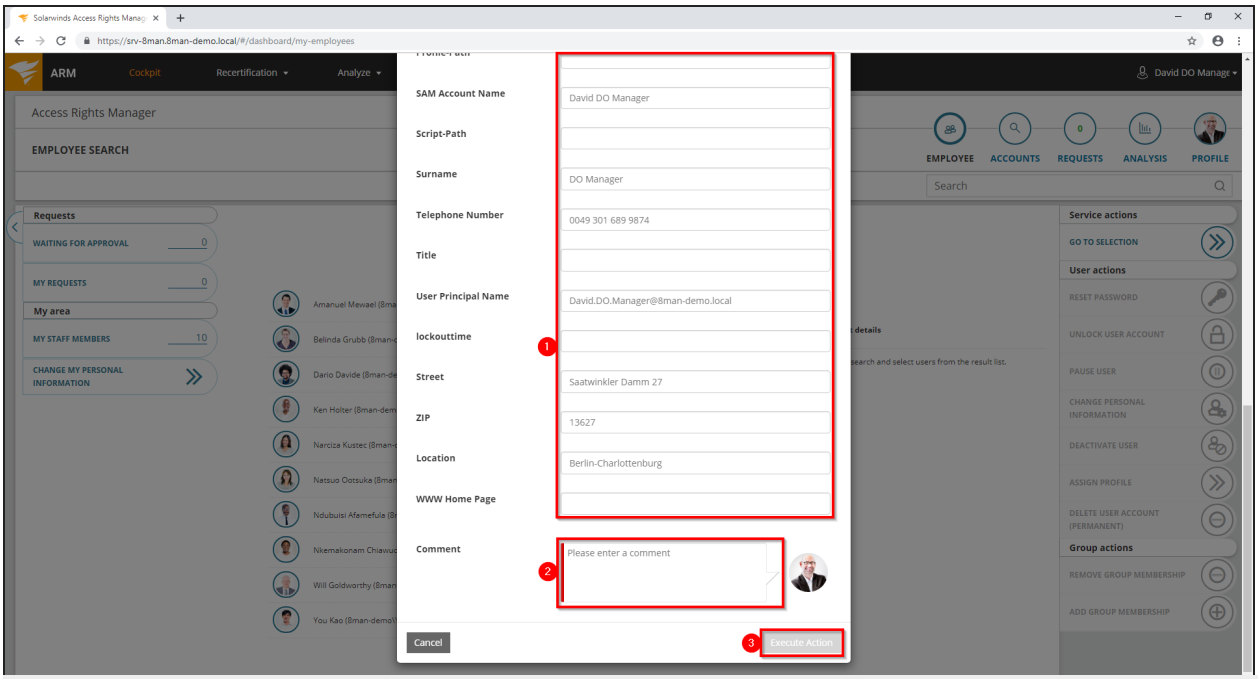
With ARM you can quickly and easily change your own account information. The actions are documented in the logbook.

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.



1. Change your account information.
2. You must enter a comment.
3. Click on "Execute Action".

The attributes displayed in the dialog can be adjusted by an administrator. Please refer to the chapter Set attributes available to web client scenarios.

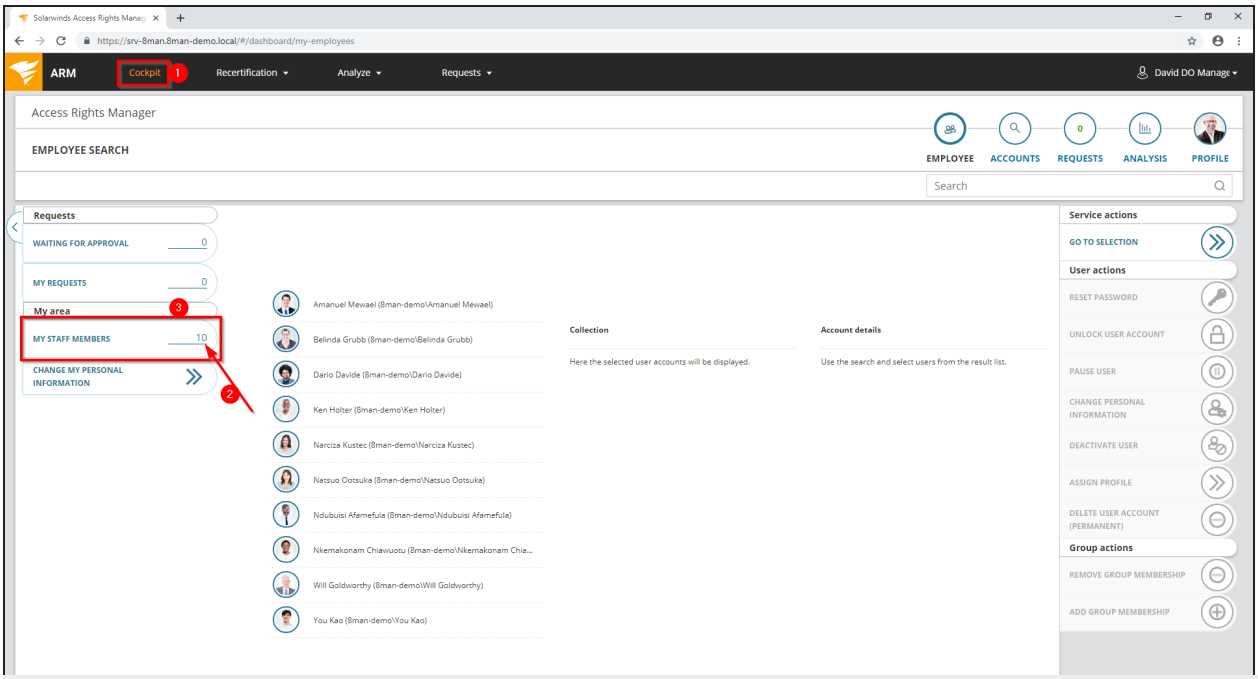
Manage my employees (cockpit)

Background / Value

With ARM you can quickly and easily manage your assigned employees. Actions are documented in the logbook.

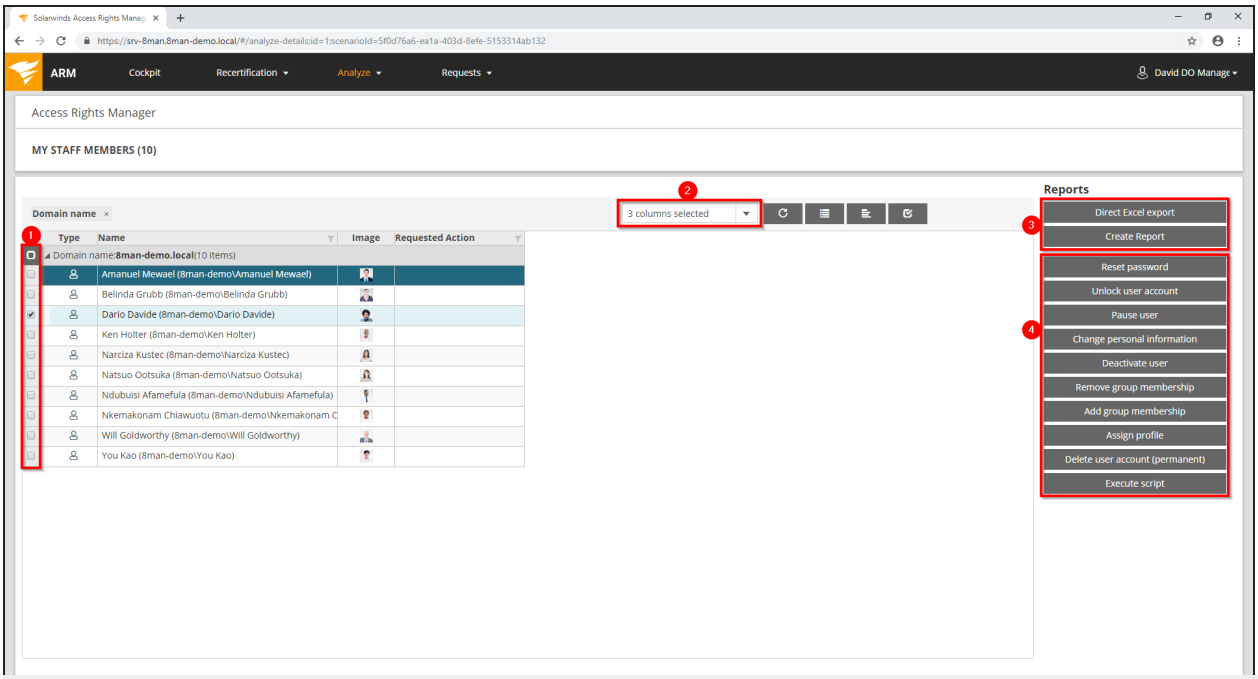
> Employees are users which attribute "Manager" in Active Directory is assigned to you. Ask your administrator.

Step-by-step process



1. Select "Cockpit".
2. The number on the button indicates how many employees are assigned to you.
3. Click "My staff members".

> The range of available services (buttons) varies according to role (login), risk assessment and configuration.



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.

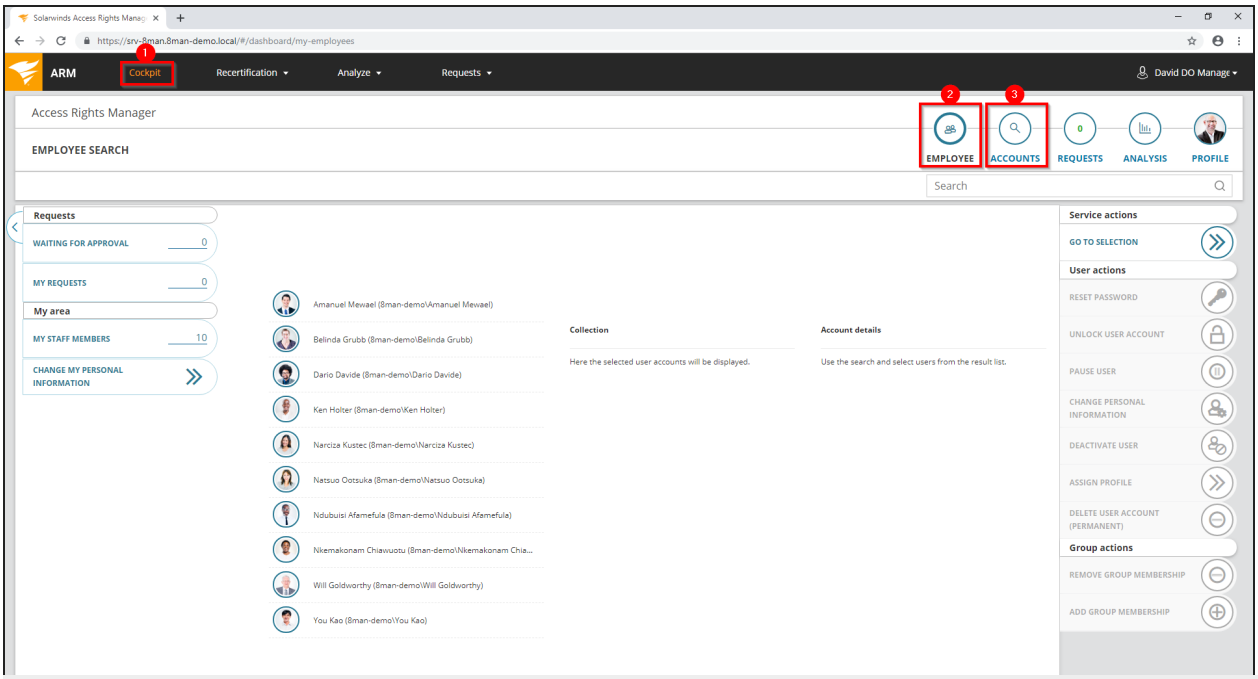
The range of available services (buttons) varies according to configuration.

Add group memberships (cockpit)

Background / Value

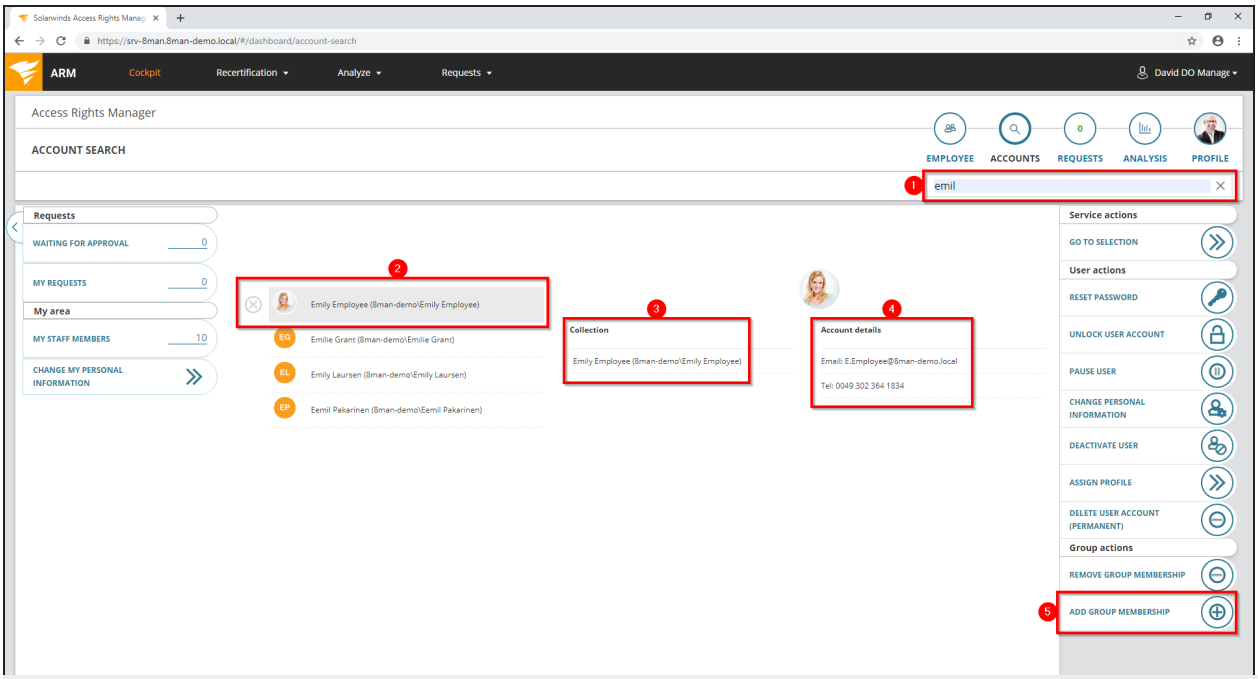
If a manager finds that his employee lacks group membership, he can add it in a few simple steps.

Step-by-step process

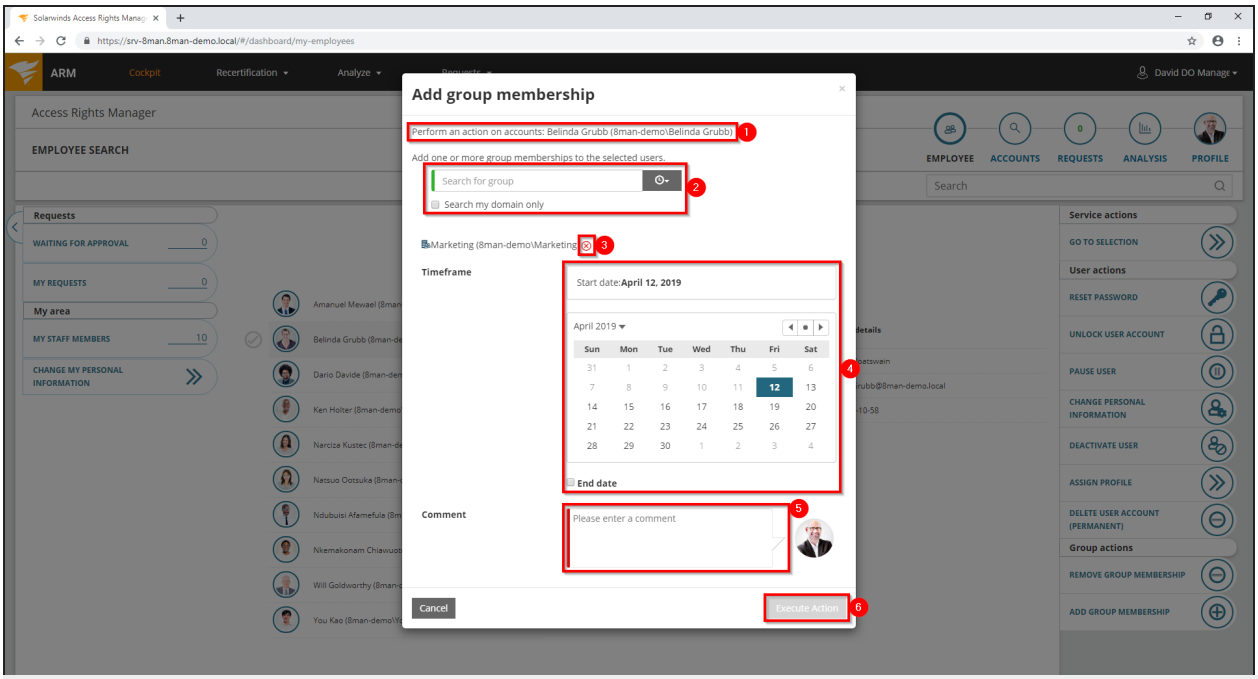


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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".



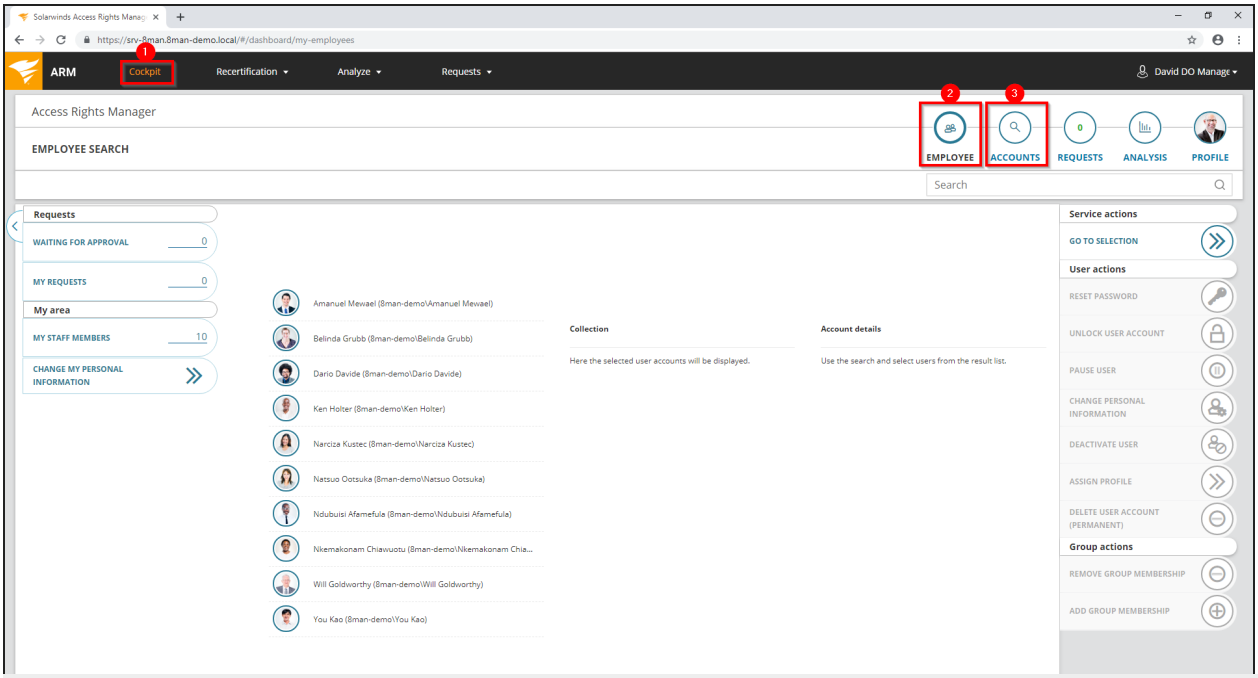
1. ARM shows you which accounts you have selected.
2. Search for and add groups.
3. Optional: Remove already selected groups.
4. You can set a start and end date for the group memberships.
5. You must enter a comment.
6. Click on "Execute Action".

Remove group memberships (cockpit)

Background / Value

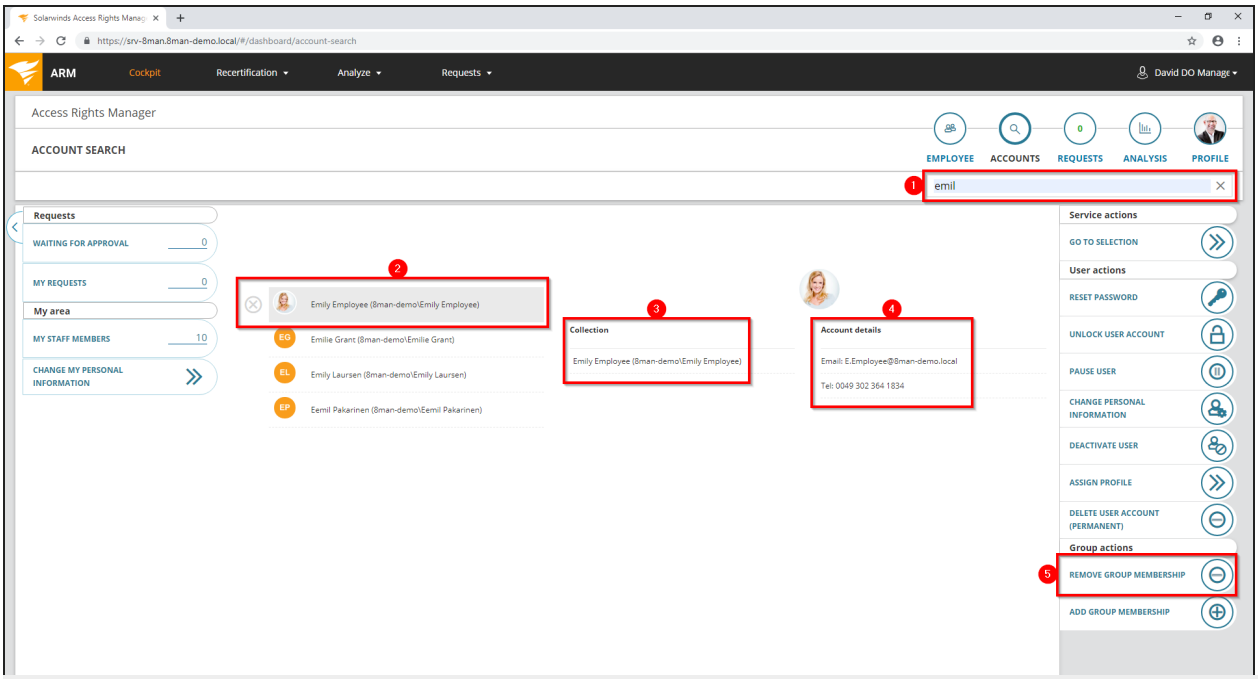
Excessive access rights are often caused by group memberships. In the cockpit, you can quickly remove group memberships.

Step-by-step process

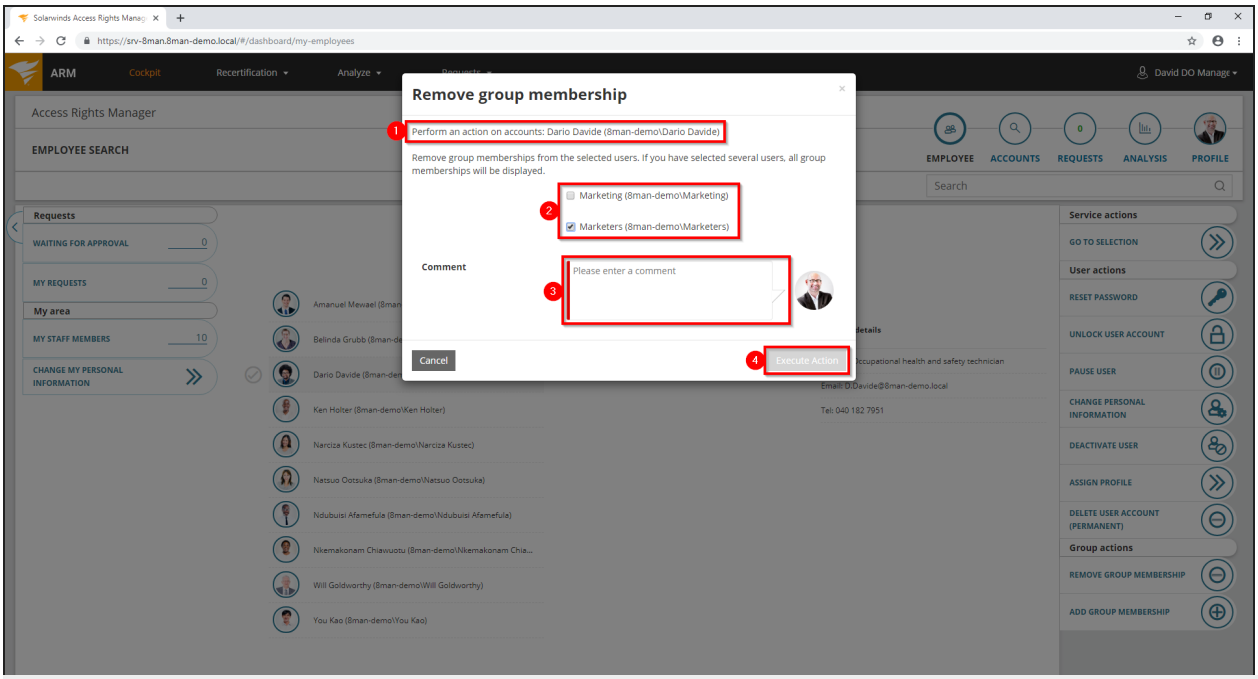


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute.
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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 "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

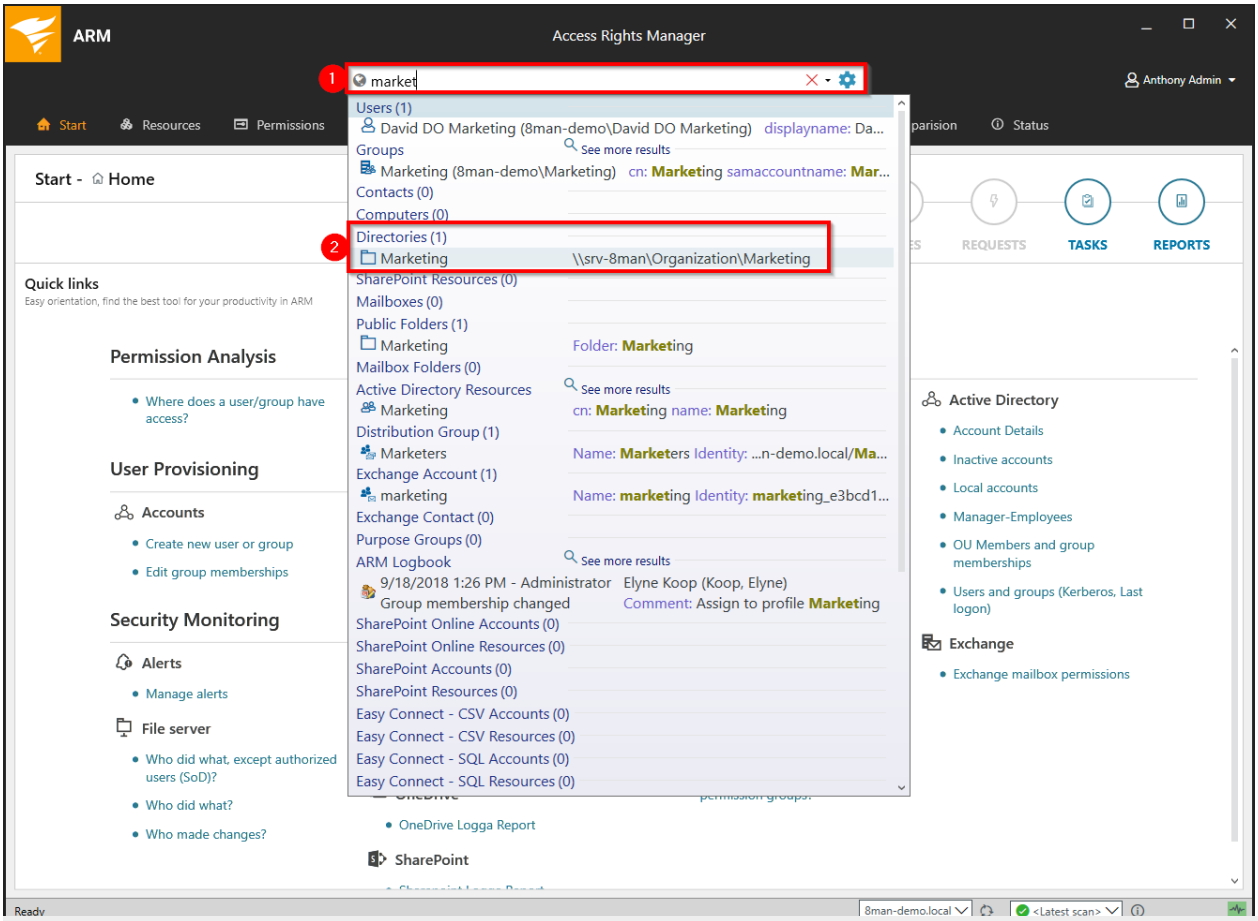
Background / Value

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.

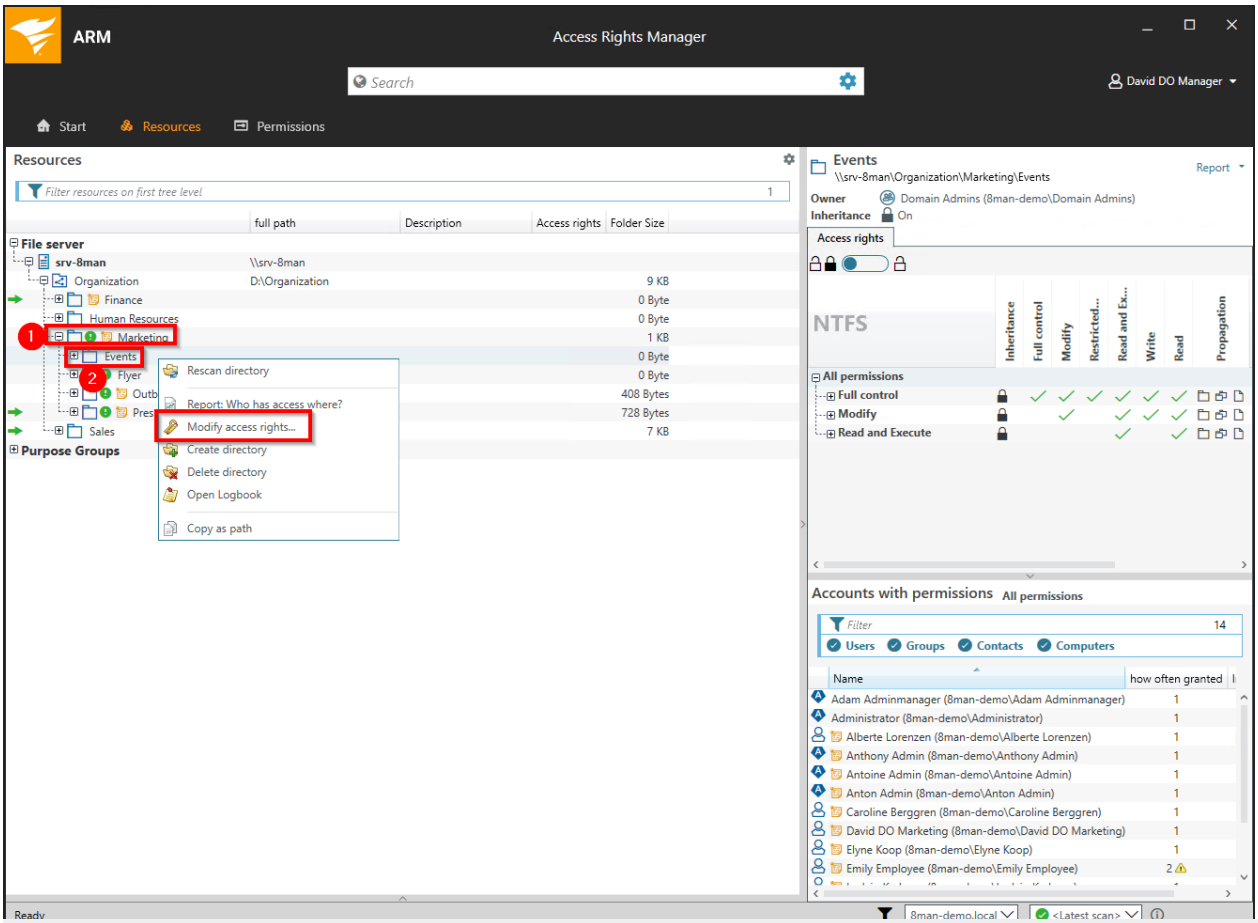
Simply decide what type of access rights you would like to assign: modify or read.

> In order to maintain data integrity we recommend assigning modify permissions only to carefully selected employees.

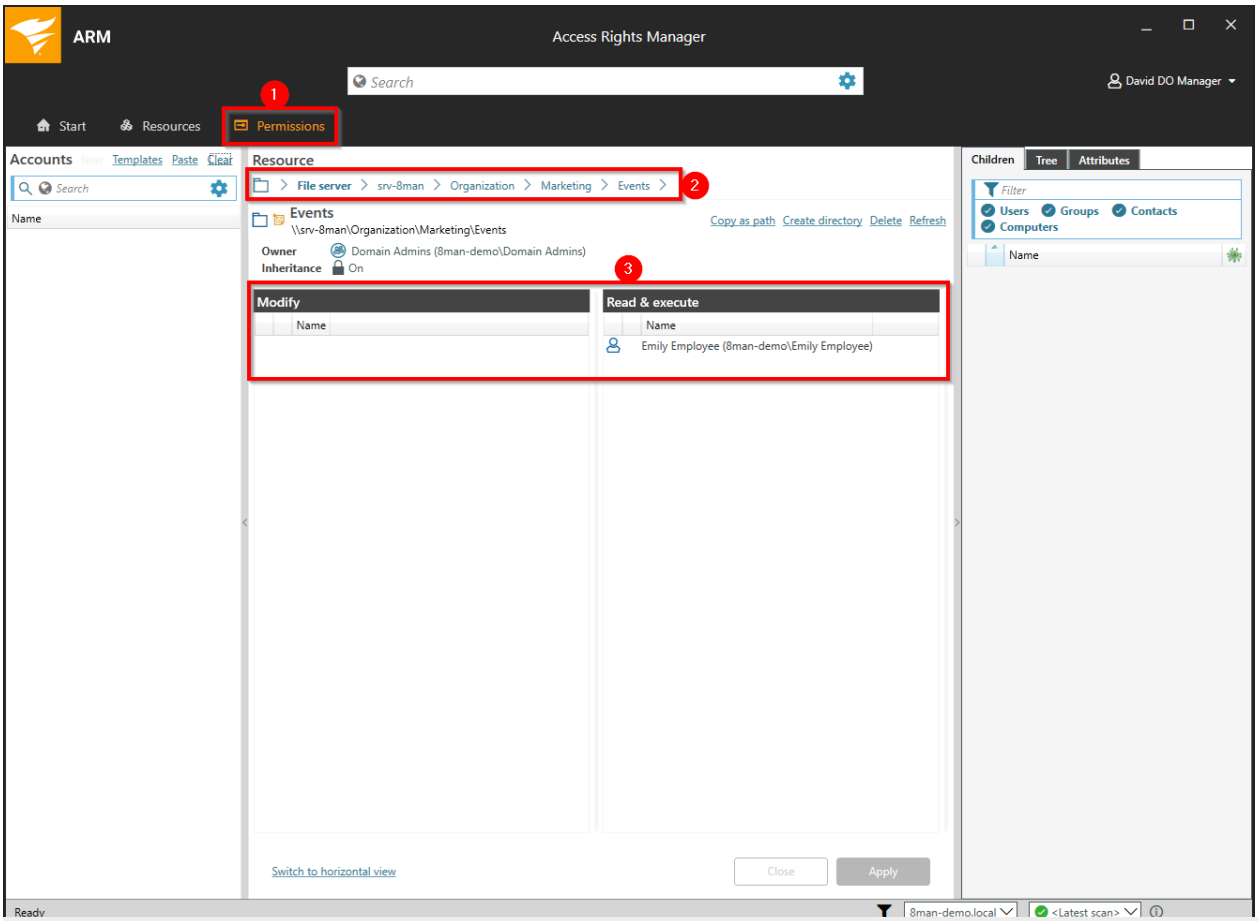
Step-by-step process



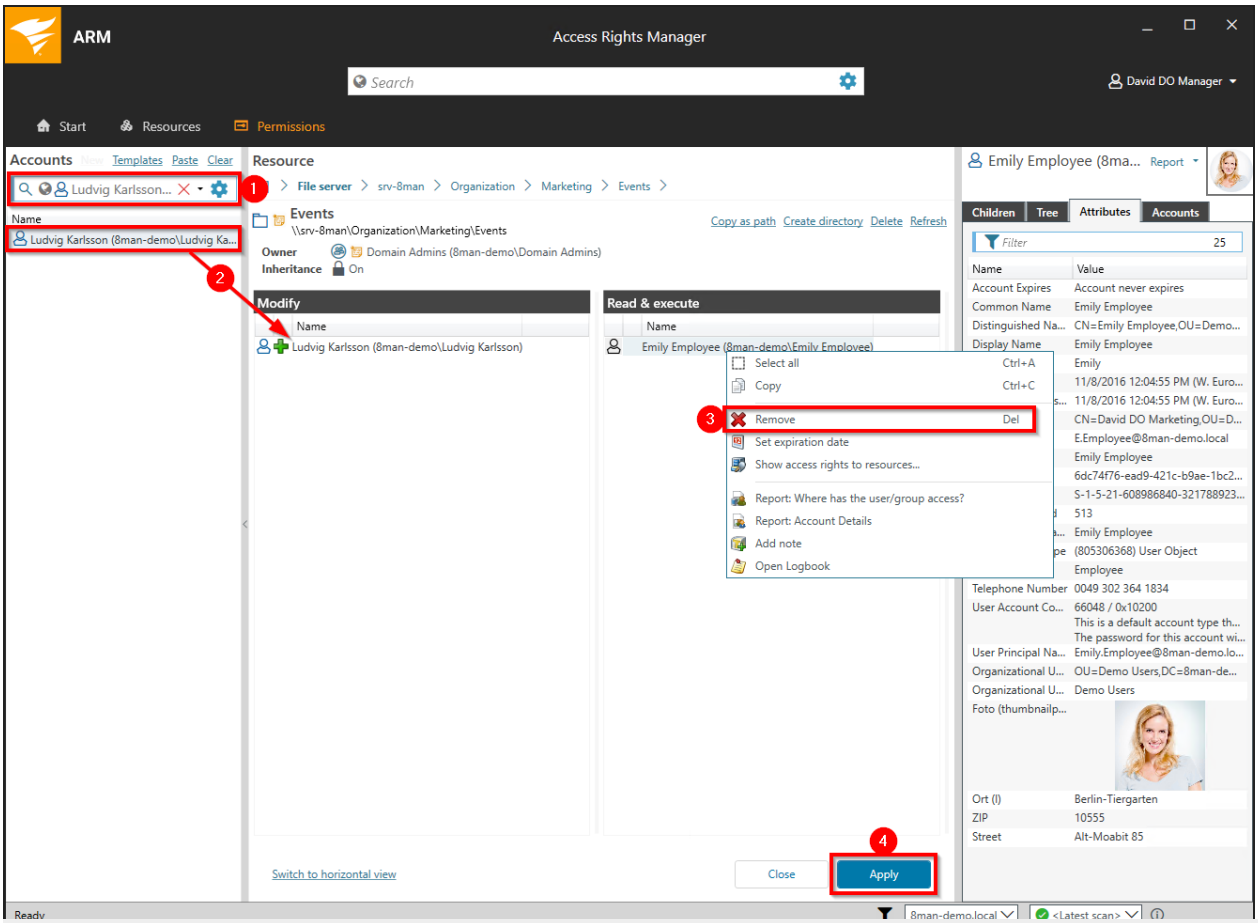
1. Use the search field to find the desired directory.
2. Click on the search result in the directories section.



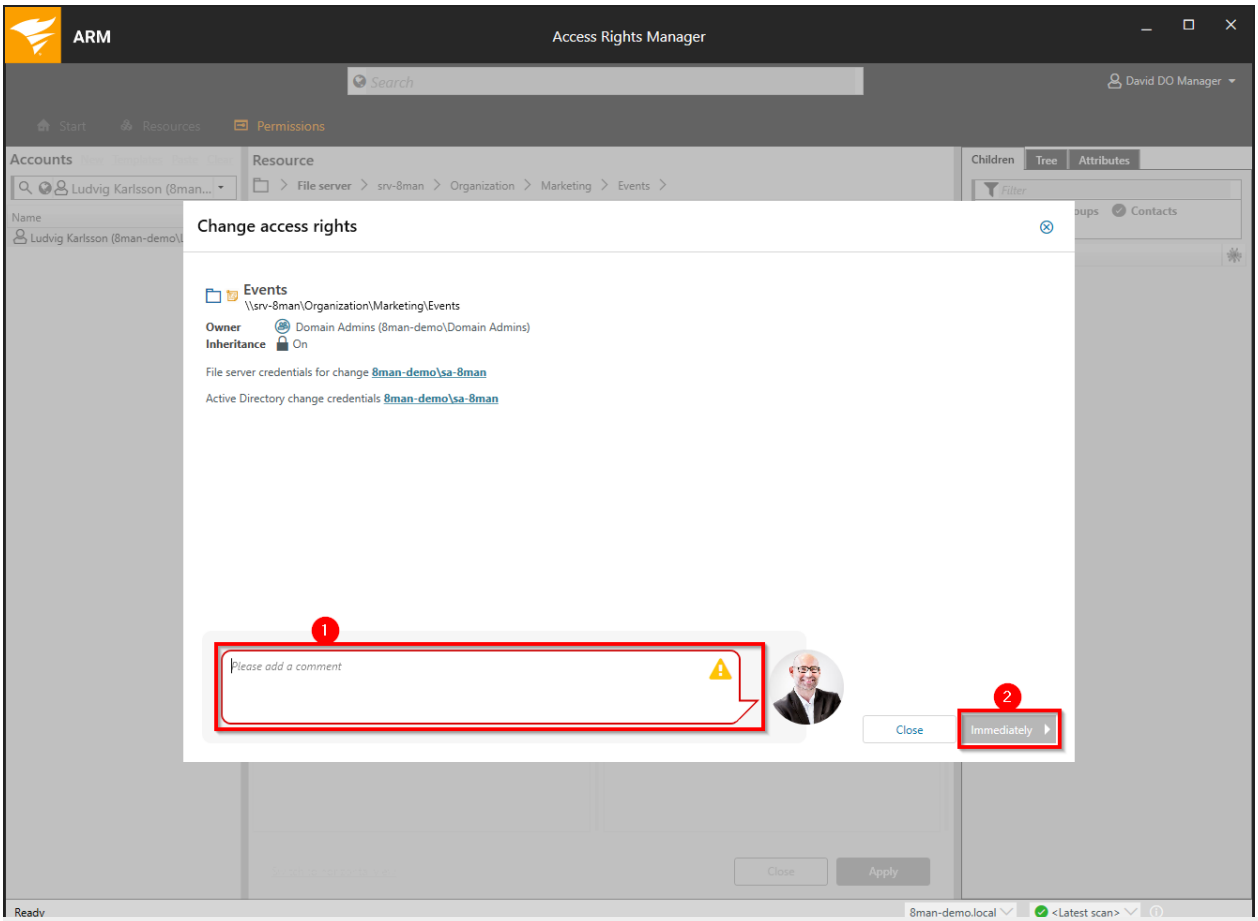
1. ARM switches to the "Resources" view with the desired directory in focus.
2. Select a sub-directory if desired by right-clicking on it.
3. Select "Modify access rights...".



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".



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".



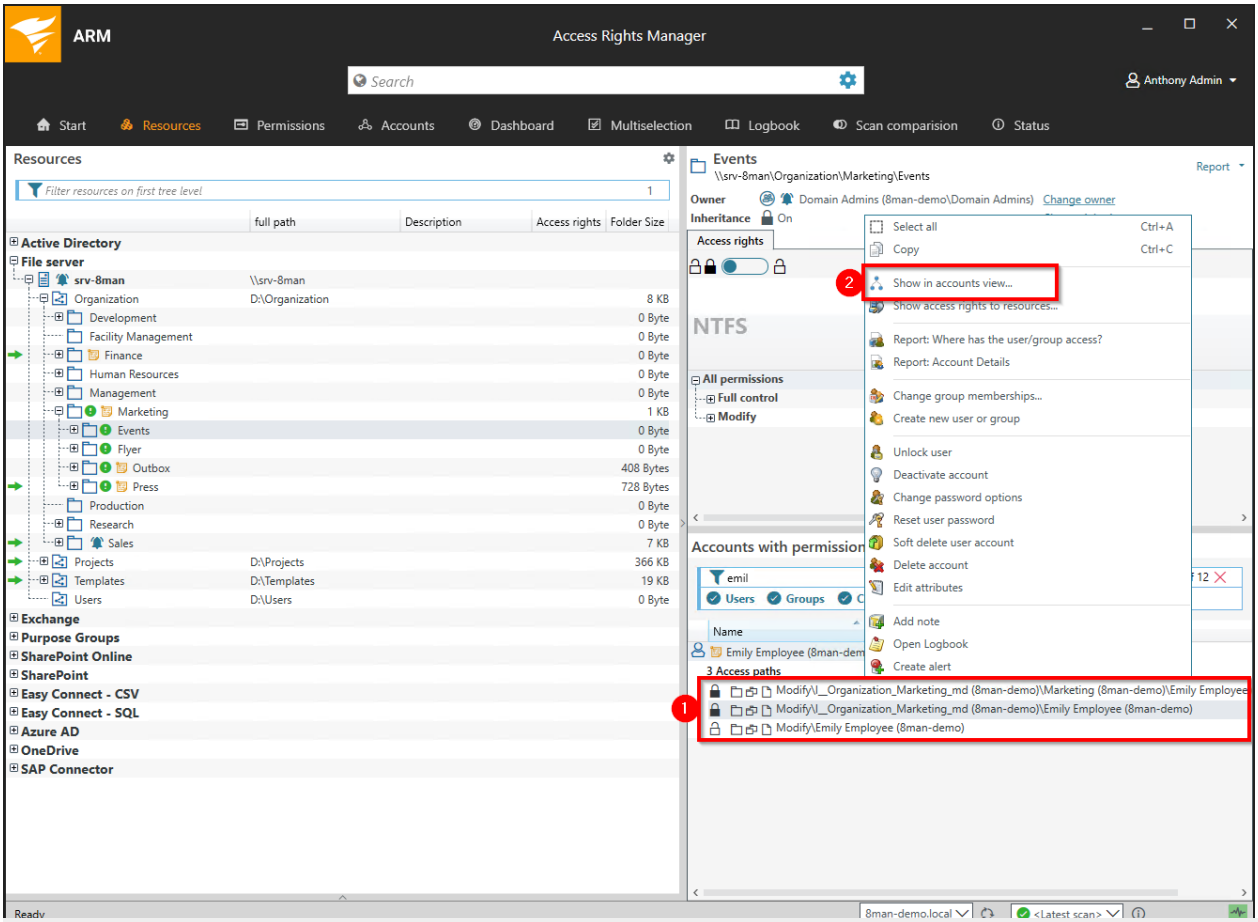
1. You must enter a comment.
2. Start the execution.

Remove multiple access paths to file server directories

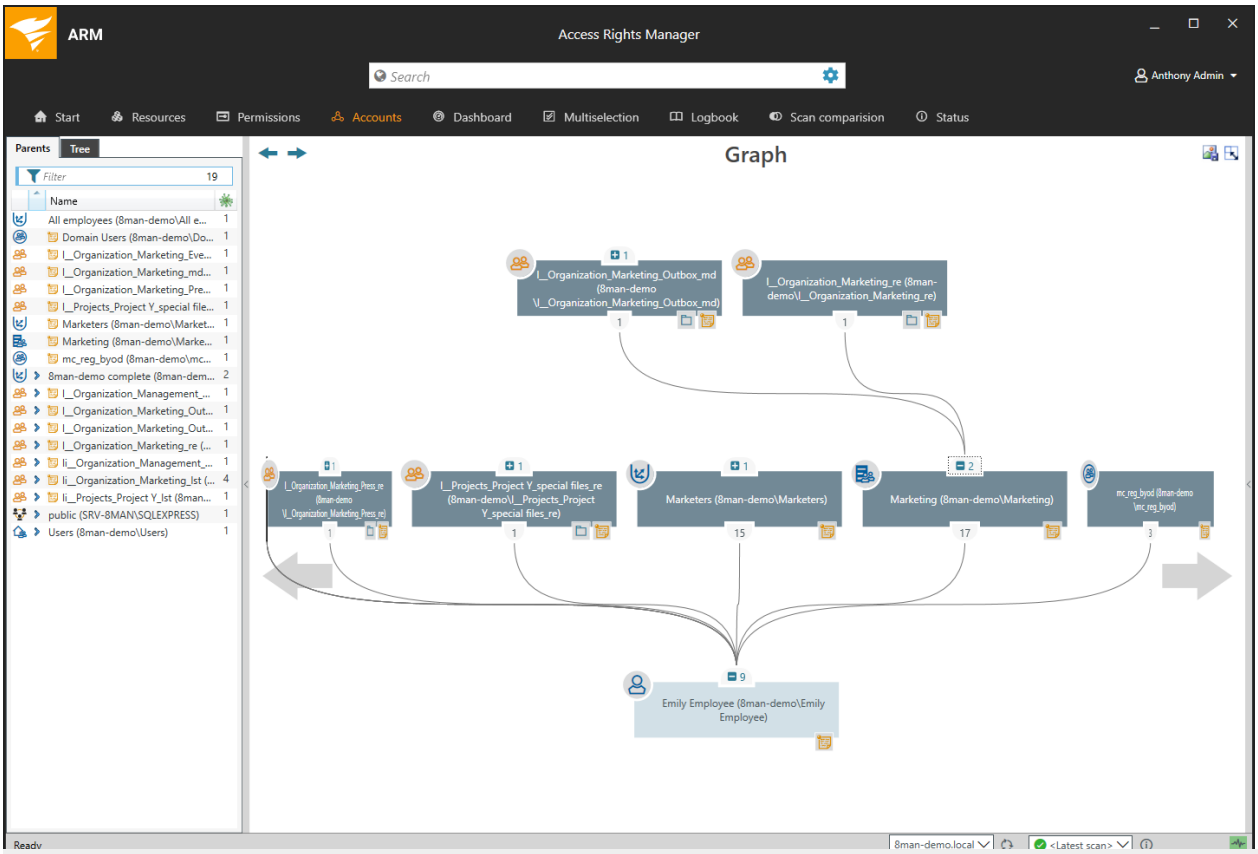
Background / Value

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.

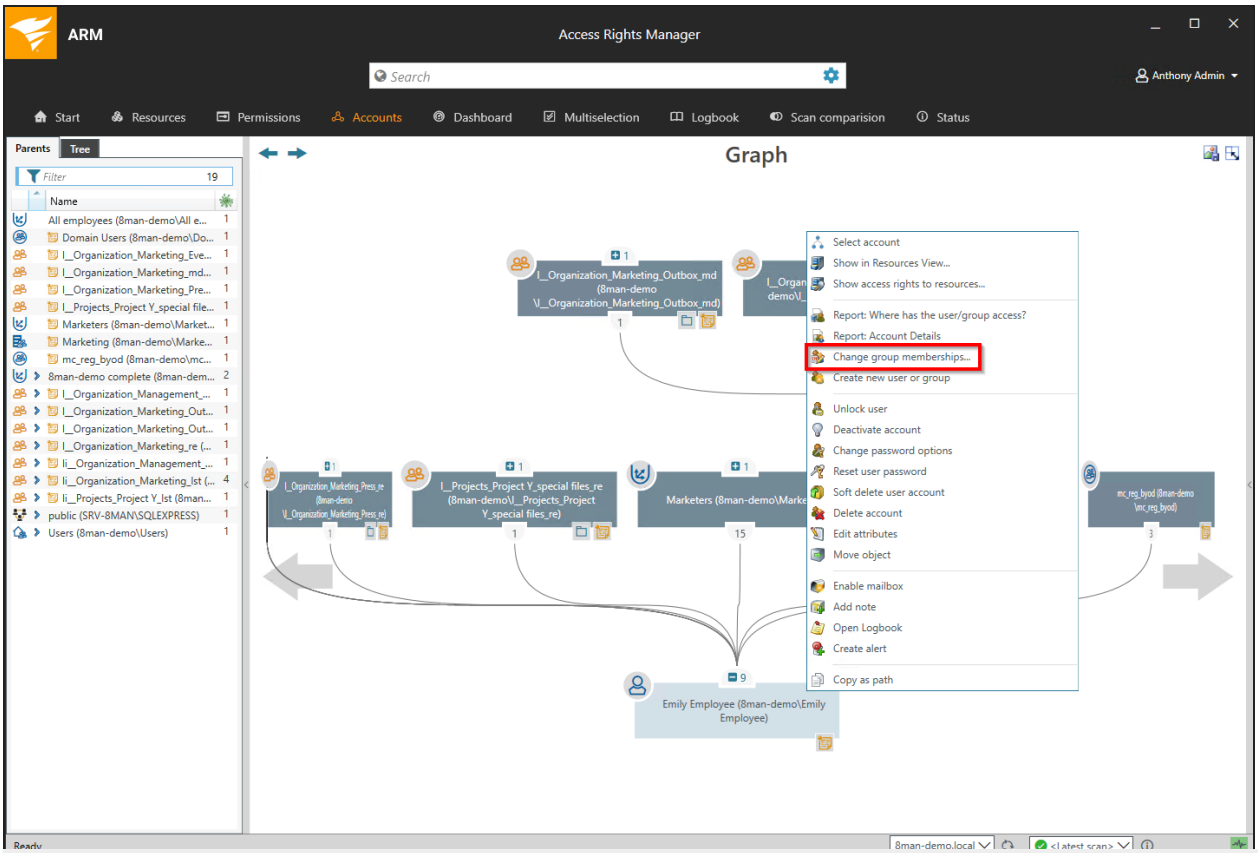
Step-by-step process



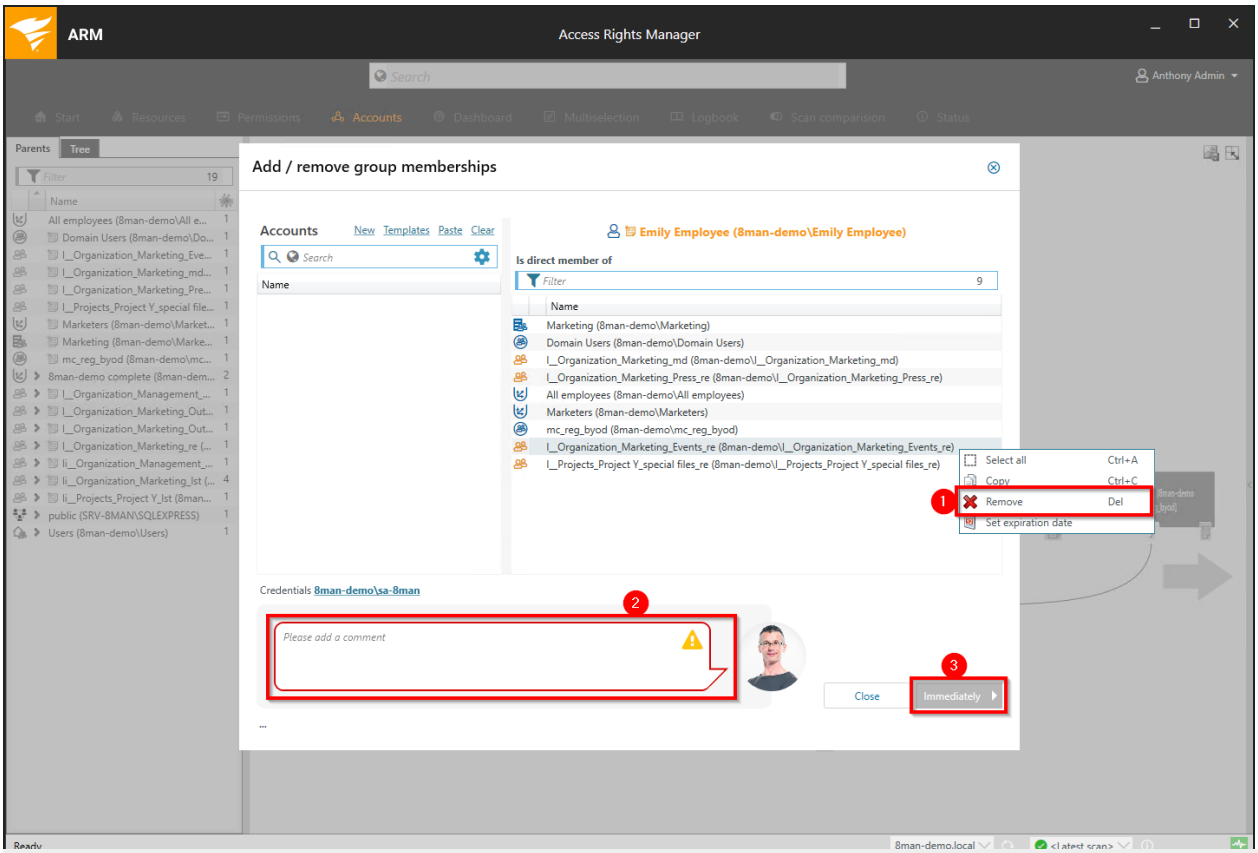
1. You have identified "Emily Employee" as having multiple access paths.
2. Right-click on the account and select "Show in account view" from the context menu.



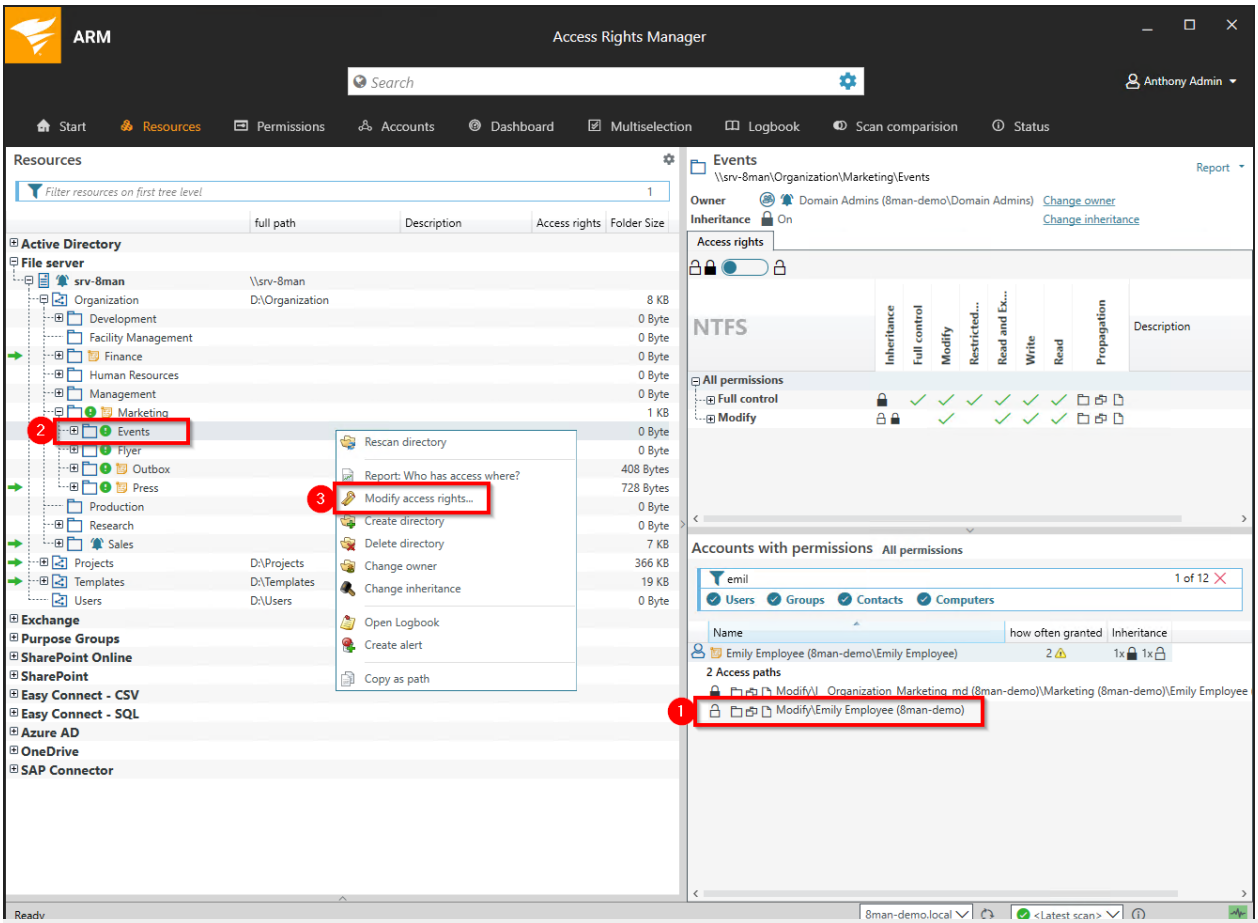
Use the AD graph to analyze multiple access paths.



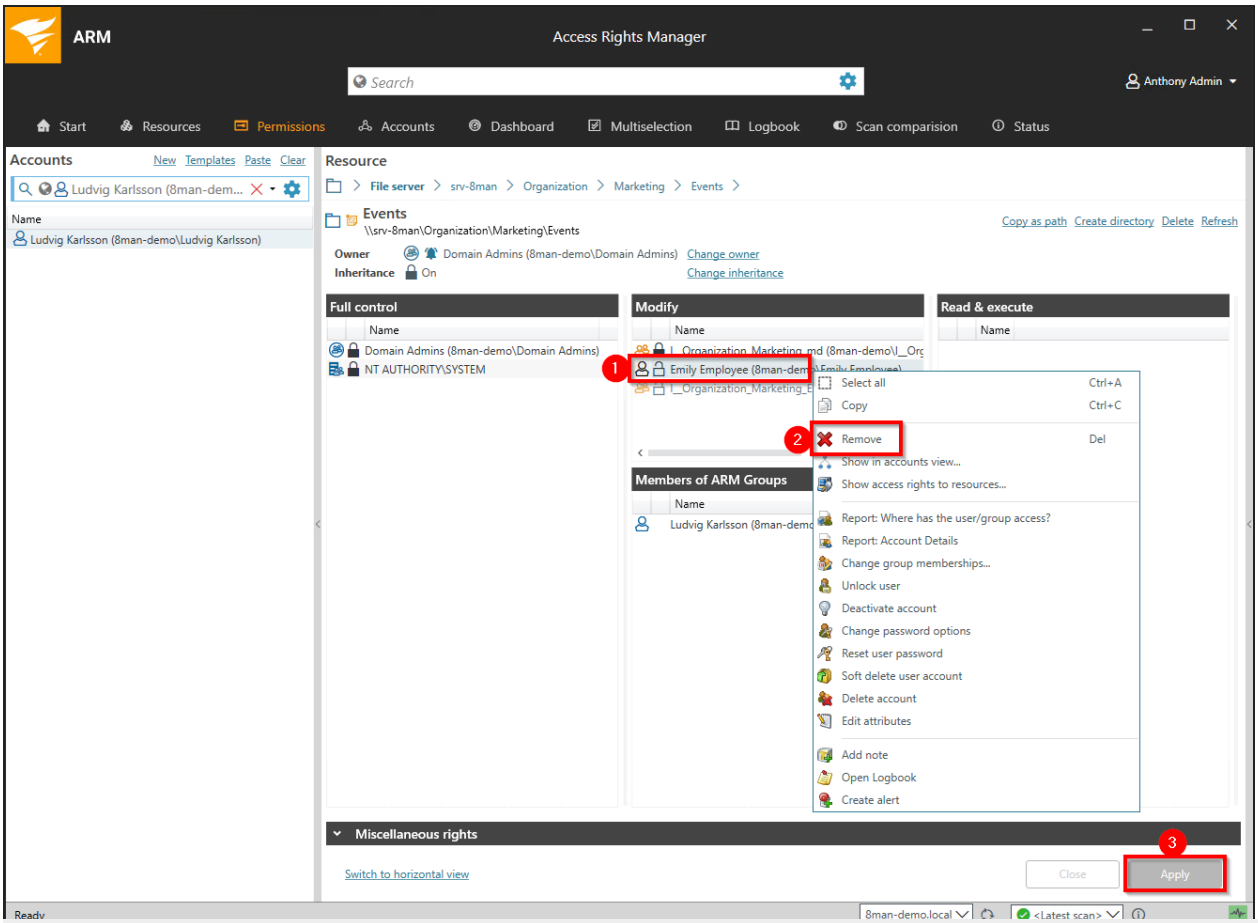
Right-click on the account and select "Change group memberships" from the context menu.



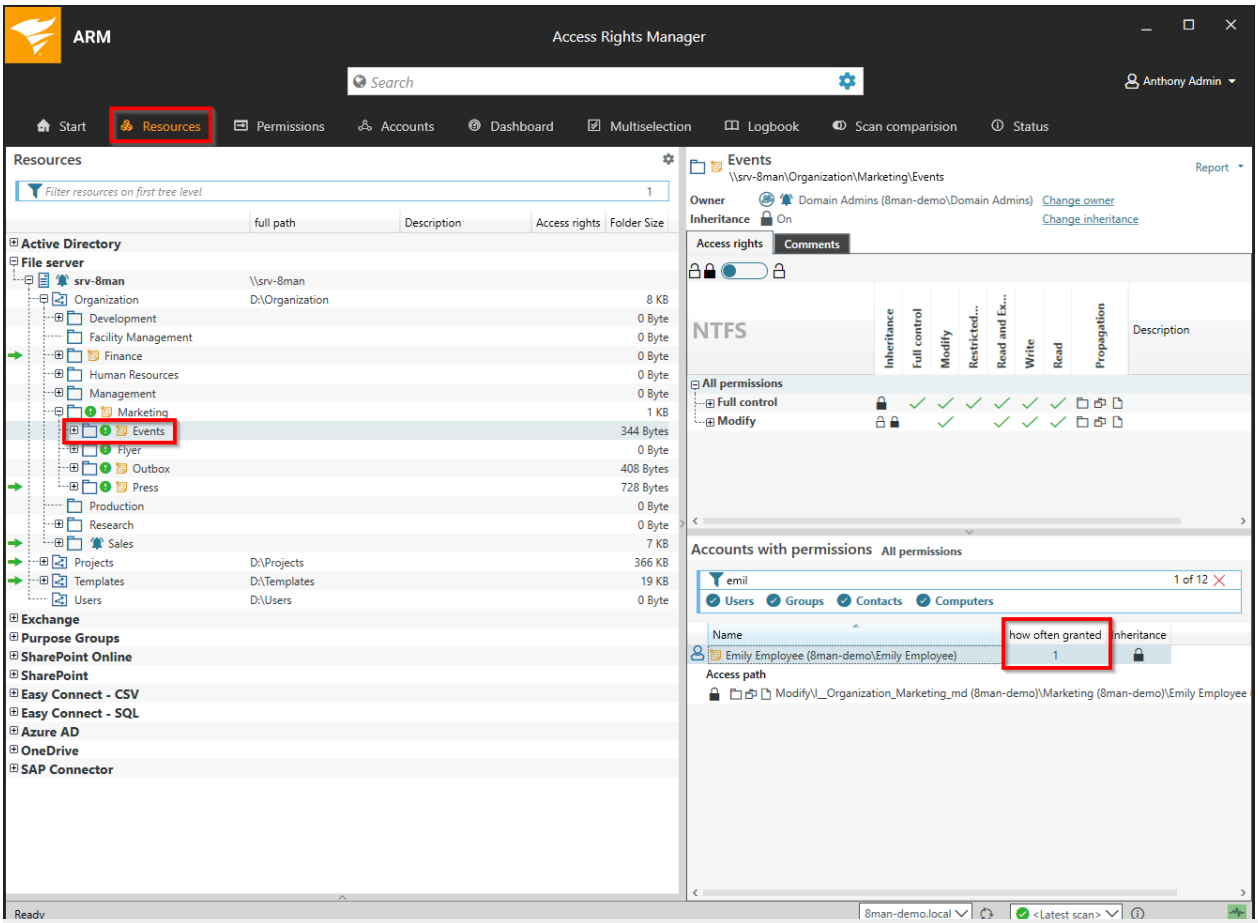
1. Remove the unnecessary group membership.
2. You must enter a comment.
3. Start the process.



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.



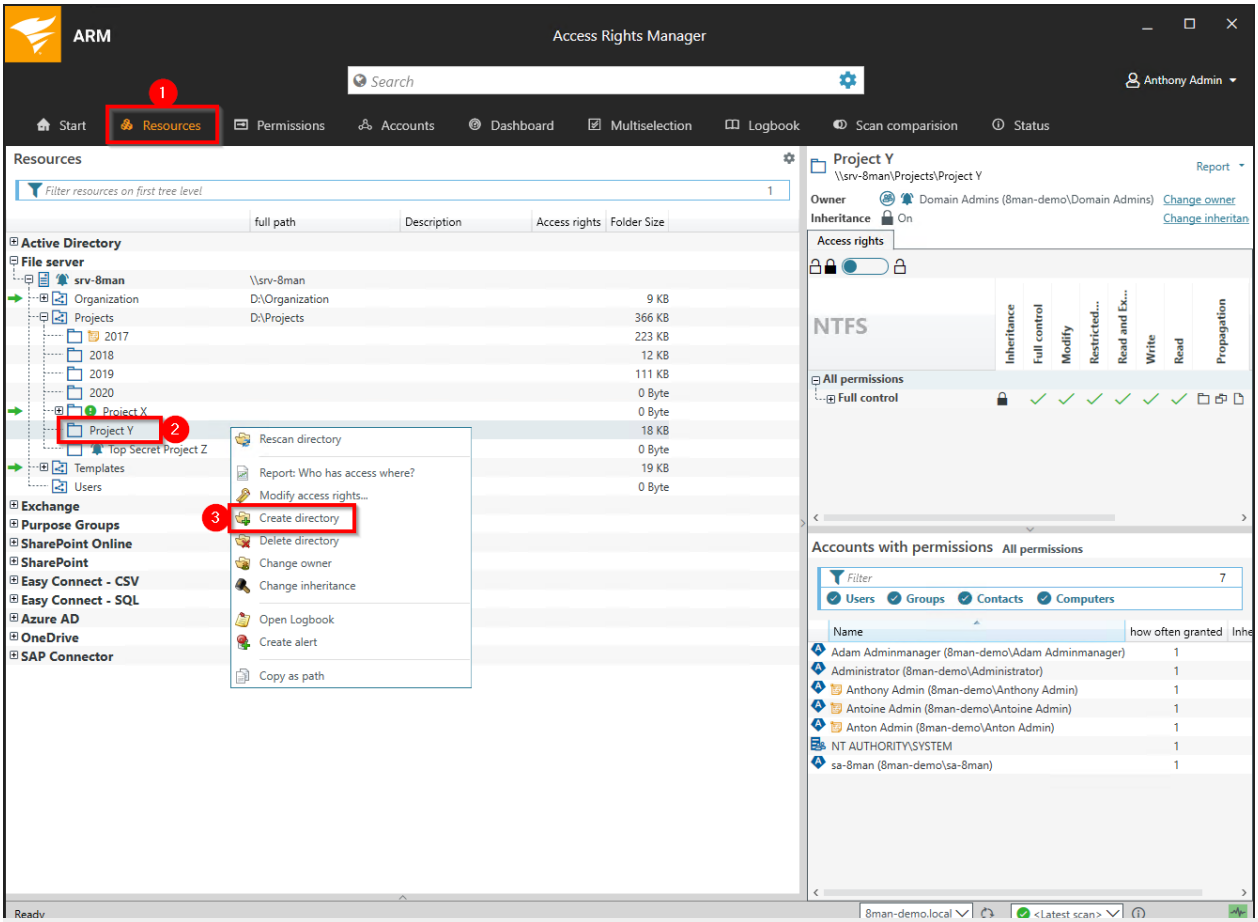
Verify the result in the resource view.

Create a protected file server directory

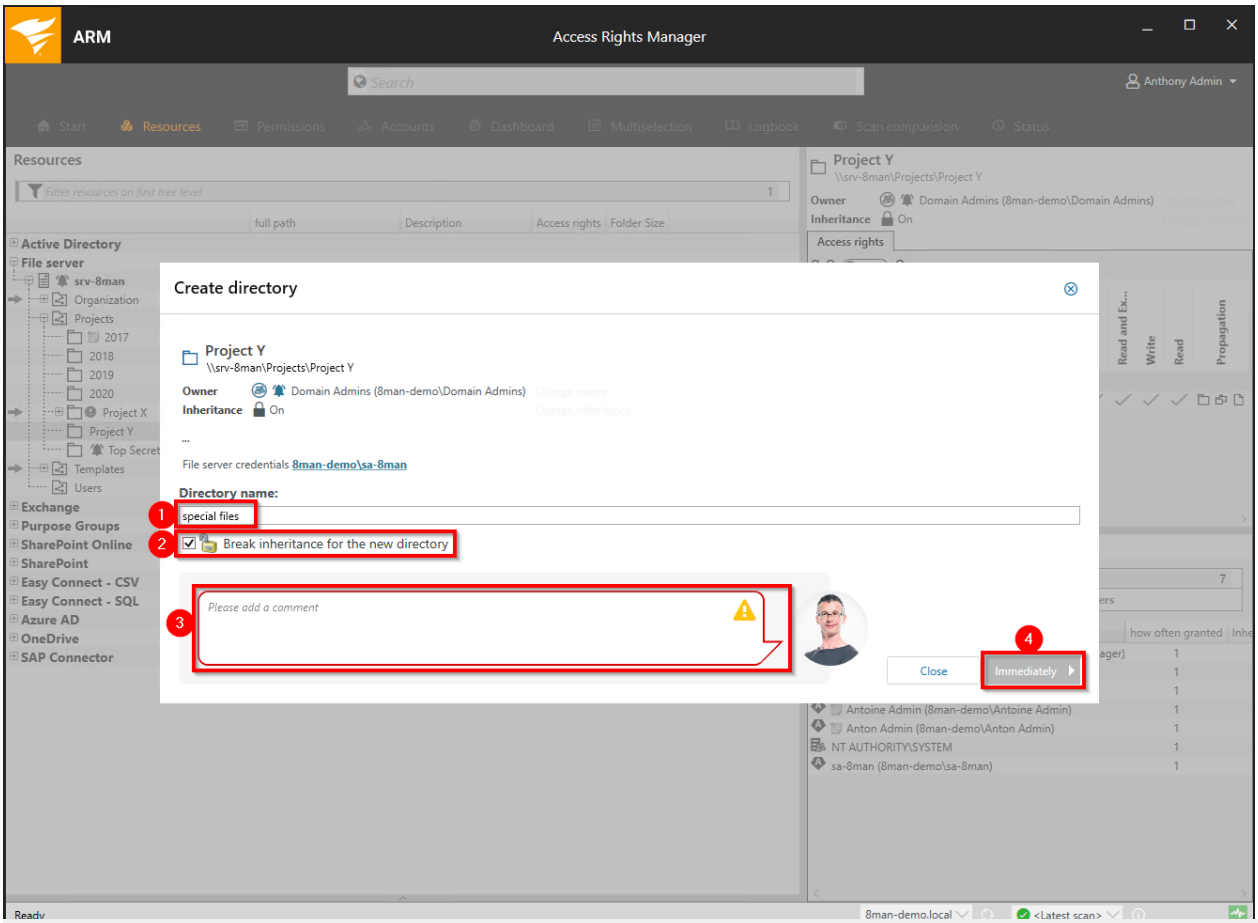
Background / Value

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.

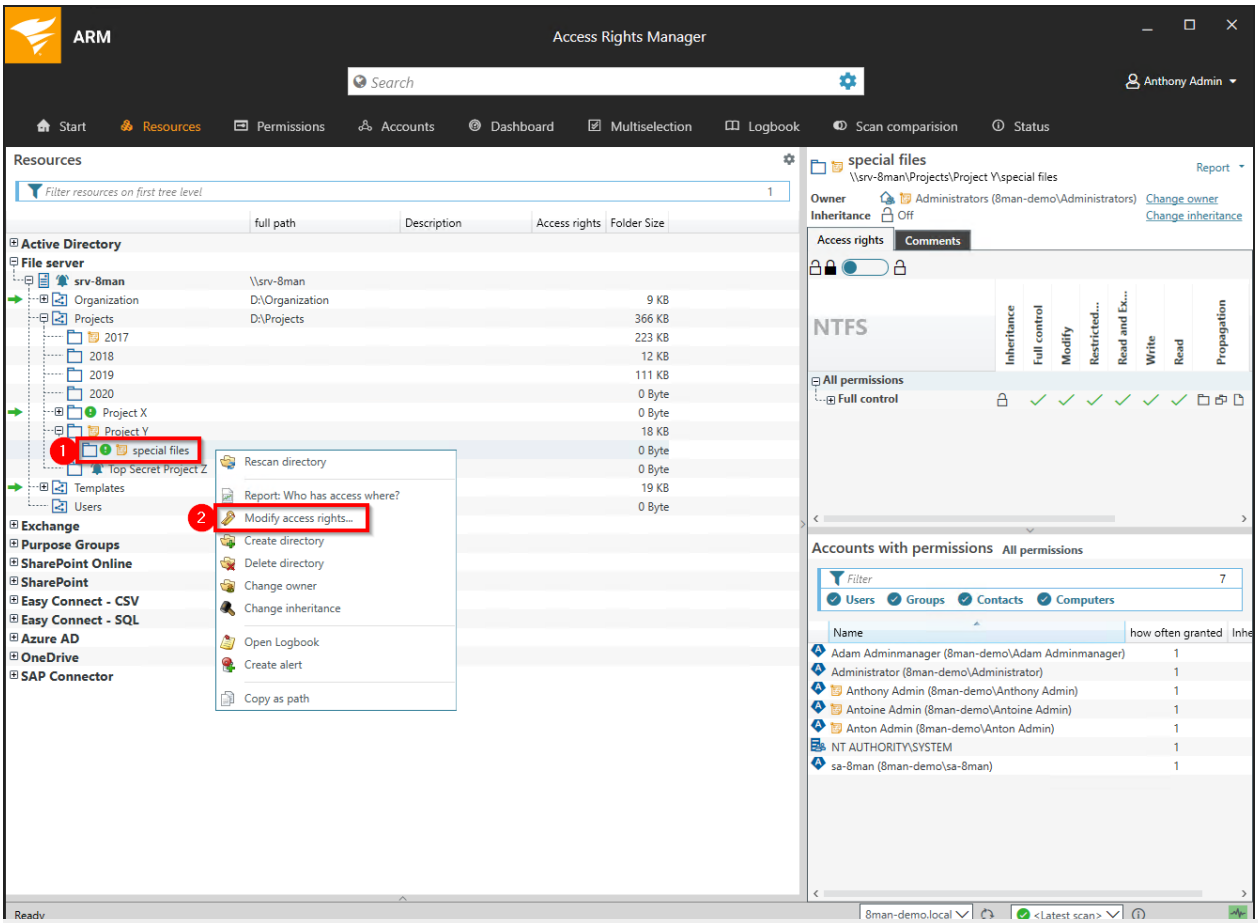
Step-by-step process



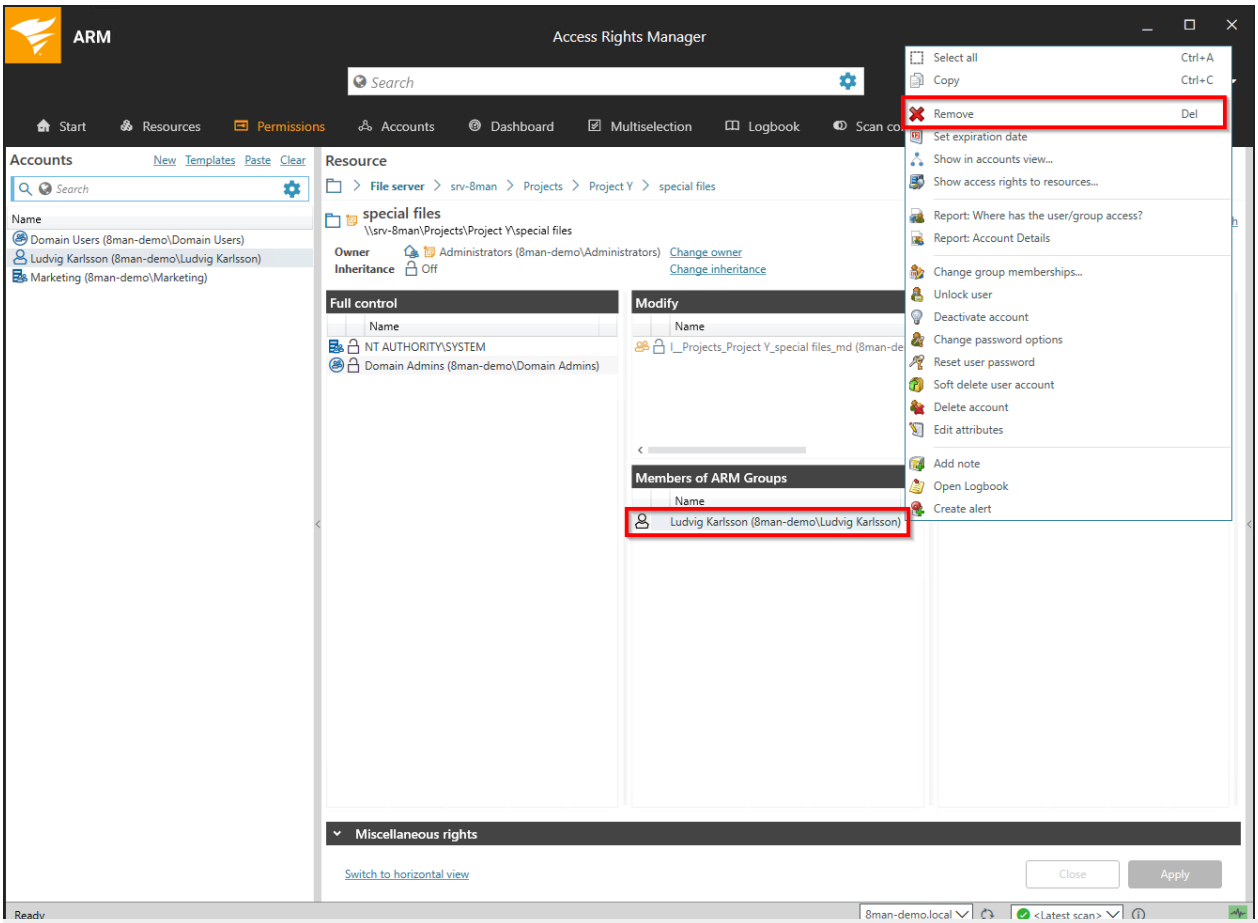
1. Select "Resources".
2. Navigate to the desired folder.
3. Right-click on the desired object and select "Create directory" from the context menu.



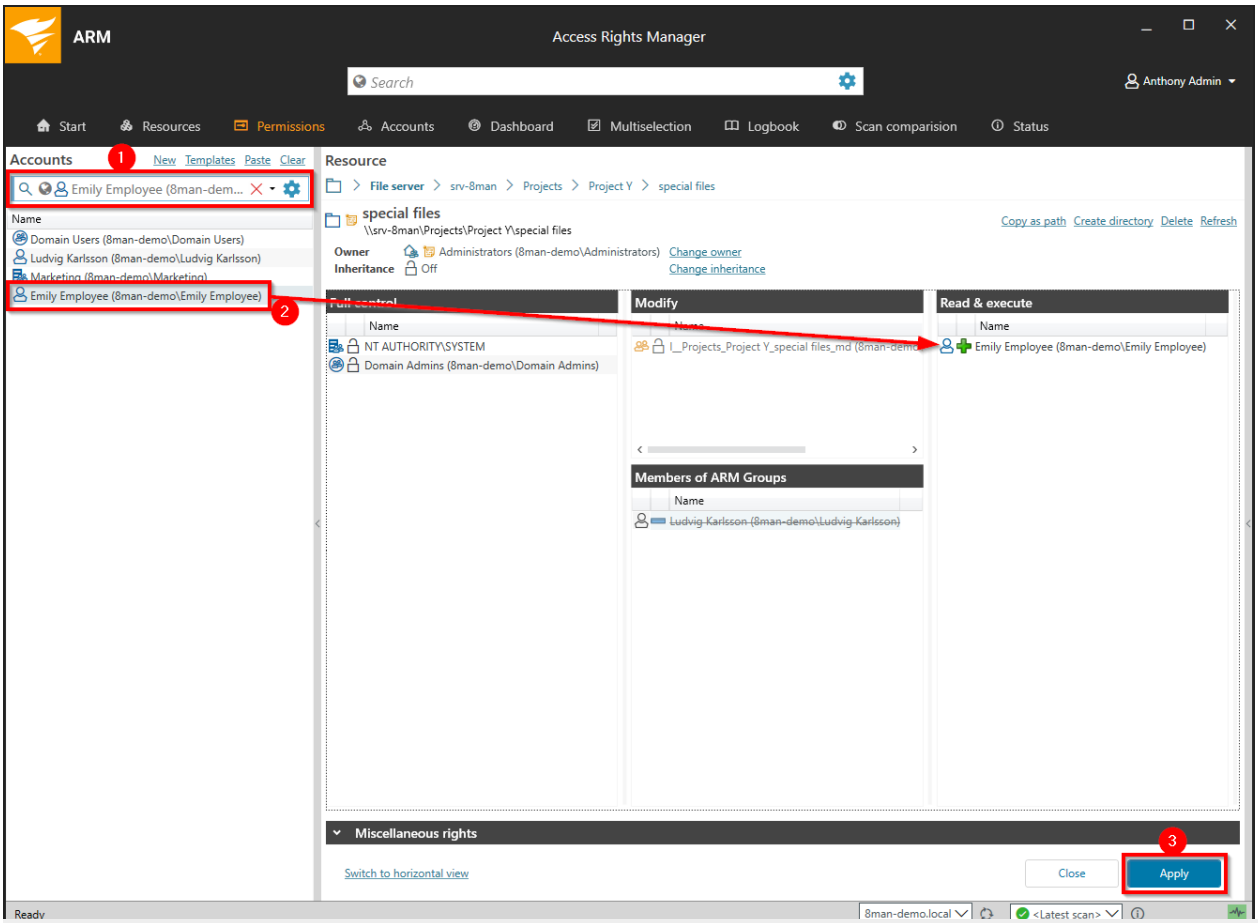
1. Name the directory.
2. Activate the option.
3. You must enter a comment.
4. Start the creation of a new directory.



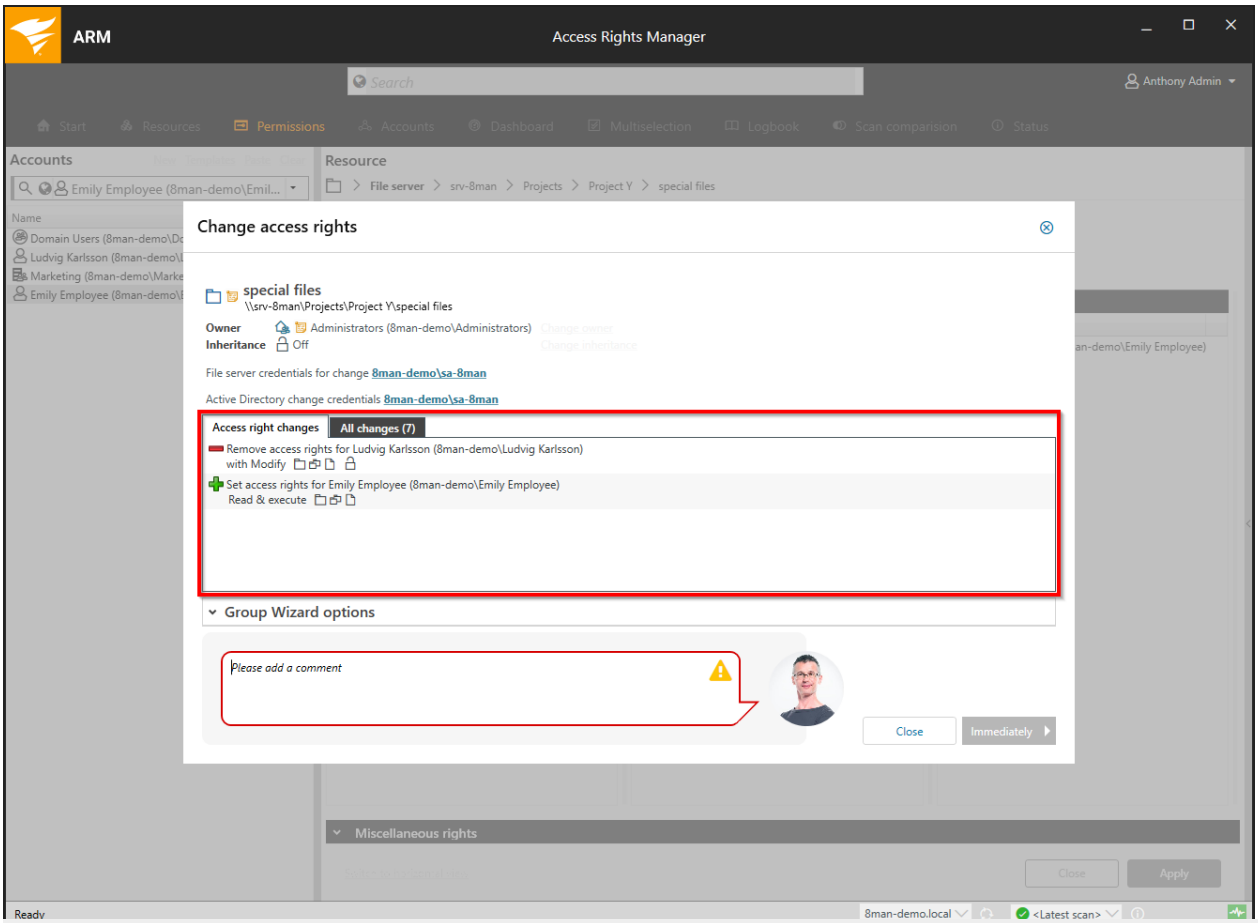
1. Navigate to the newly created directory.
2. Right-click on the directory and select "Modify access rights..." from the context menu.



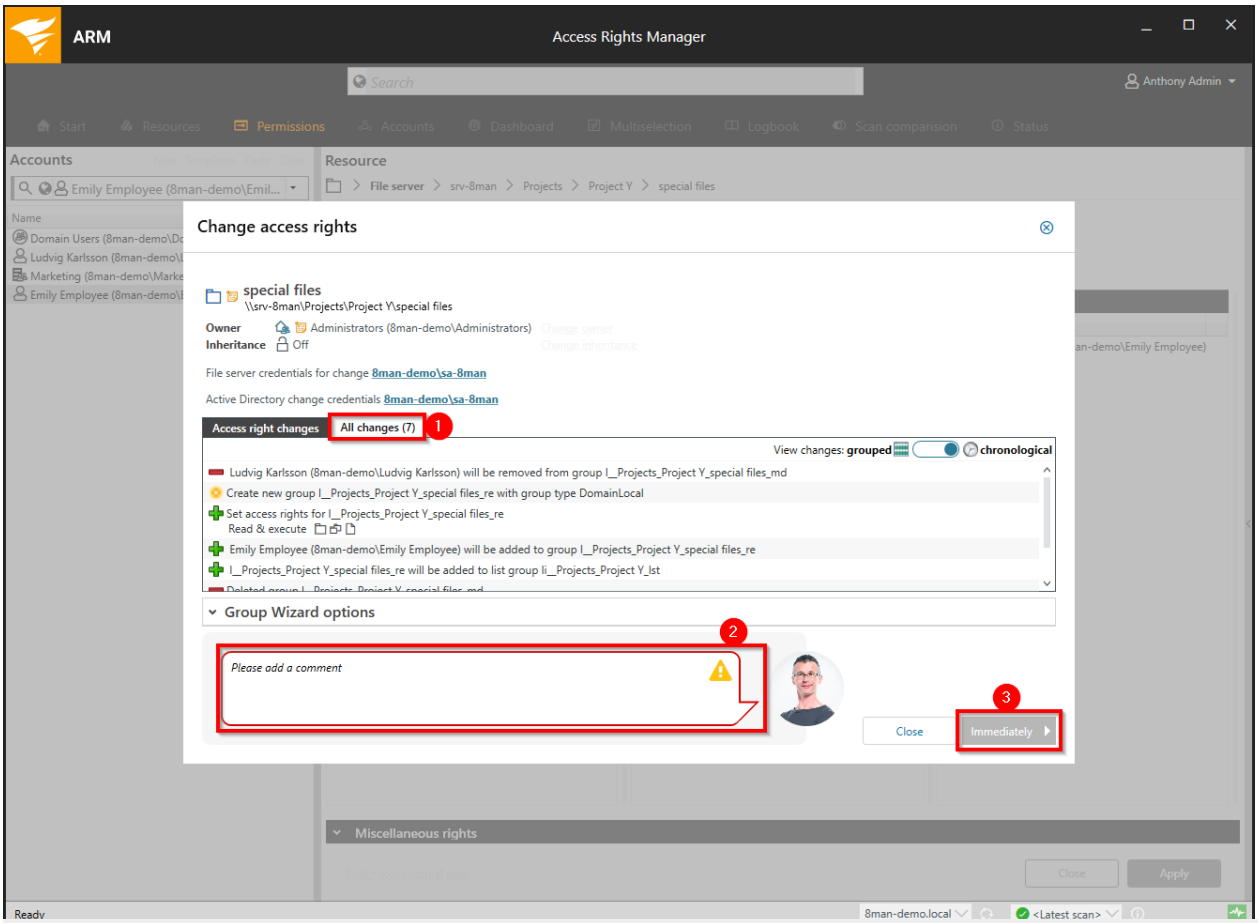
Remove all unnecessary access rights.



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 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

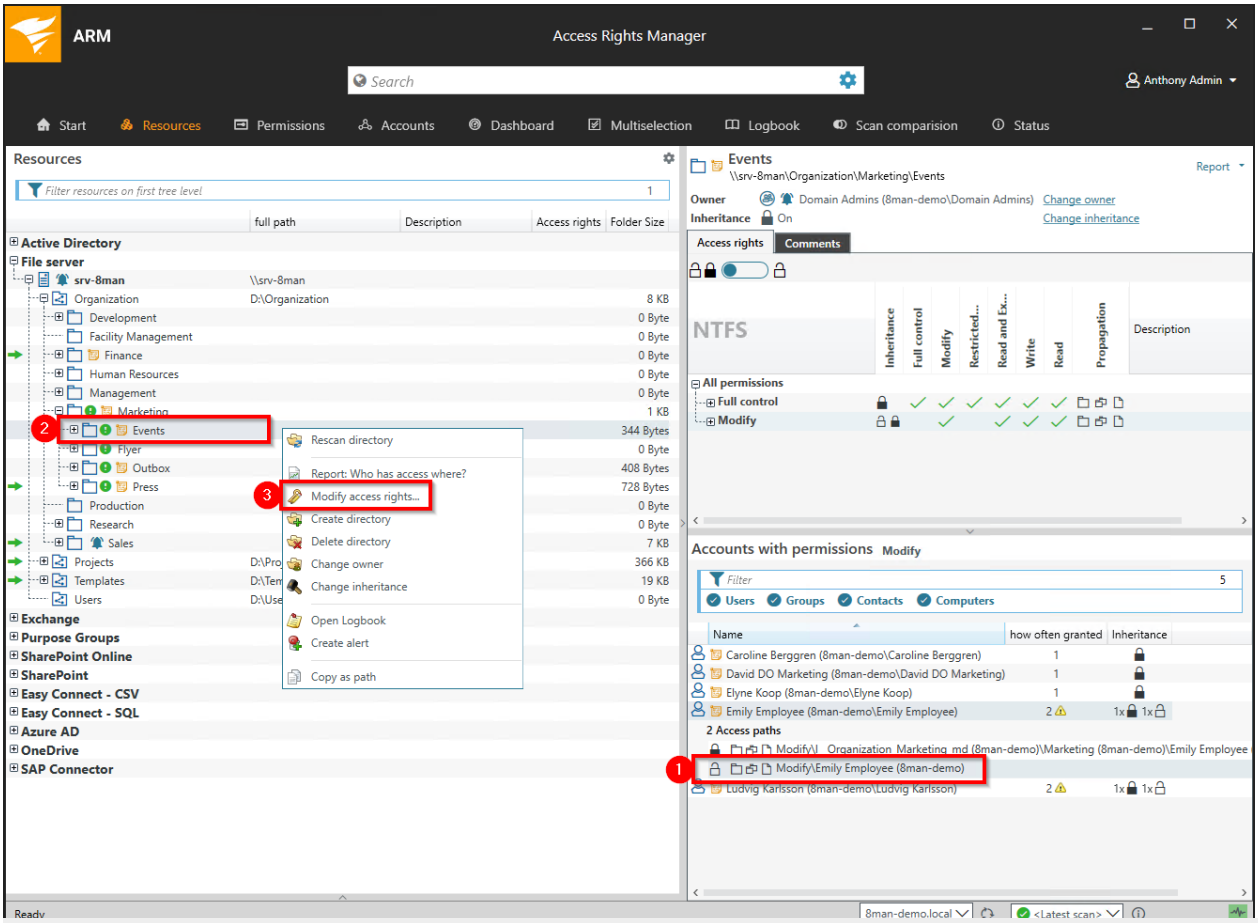
Background / Value

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.

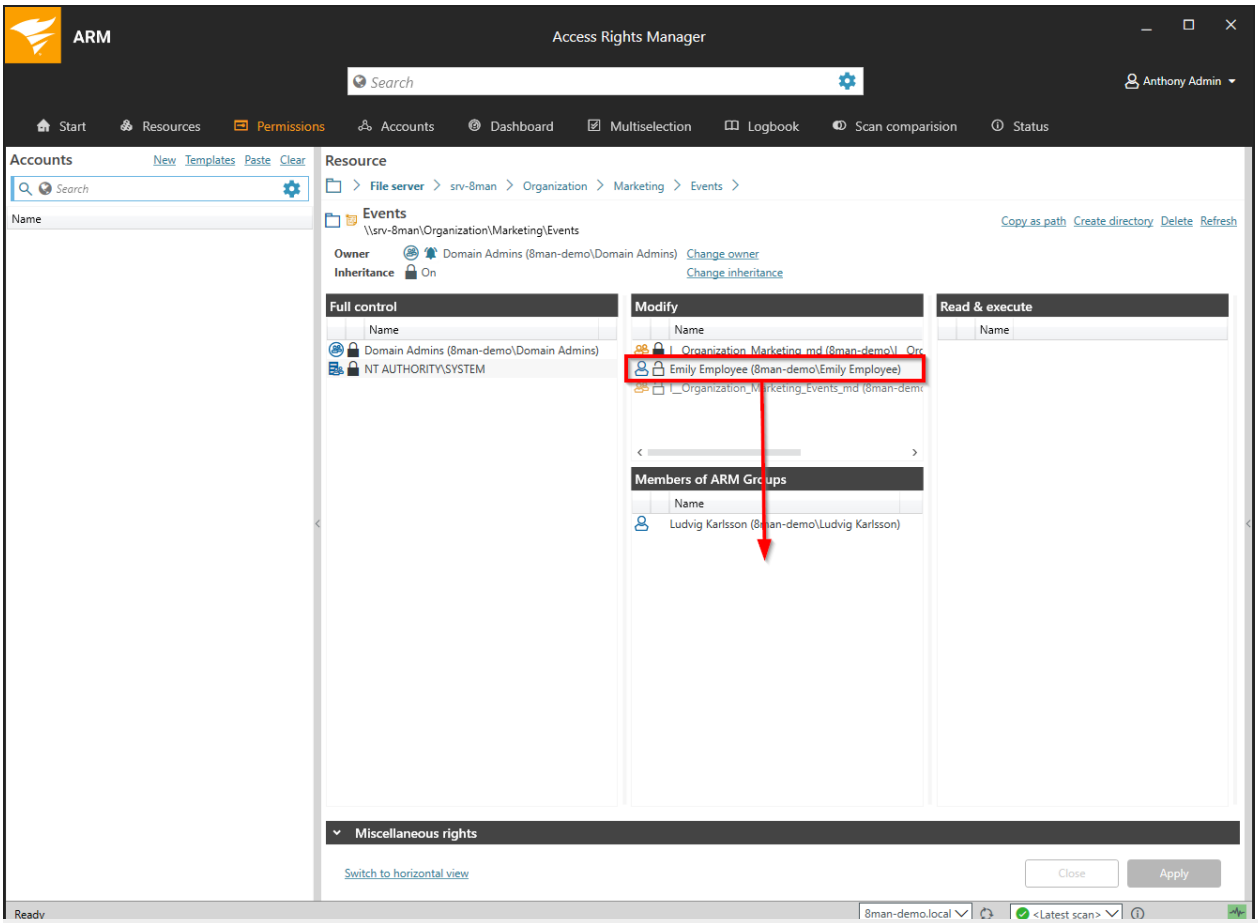
Related features

Remove direct permissions in bulk (web client)

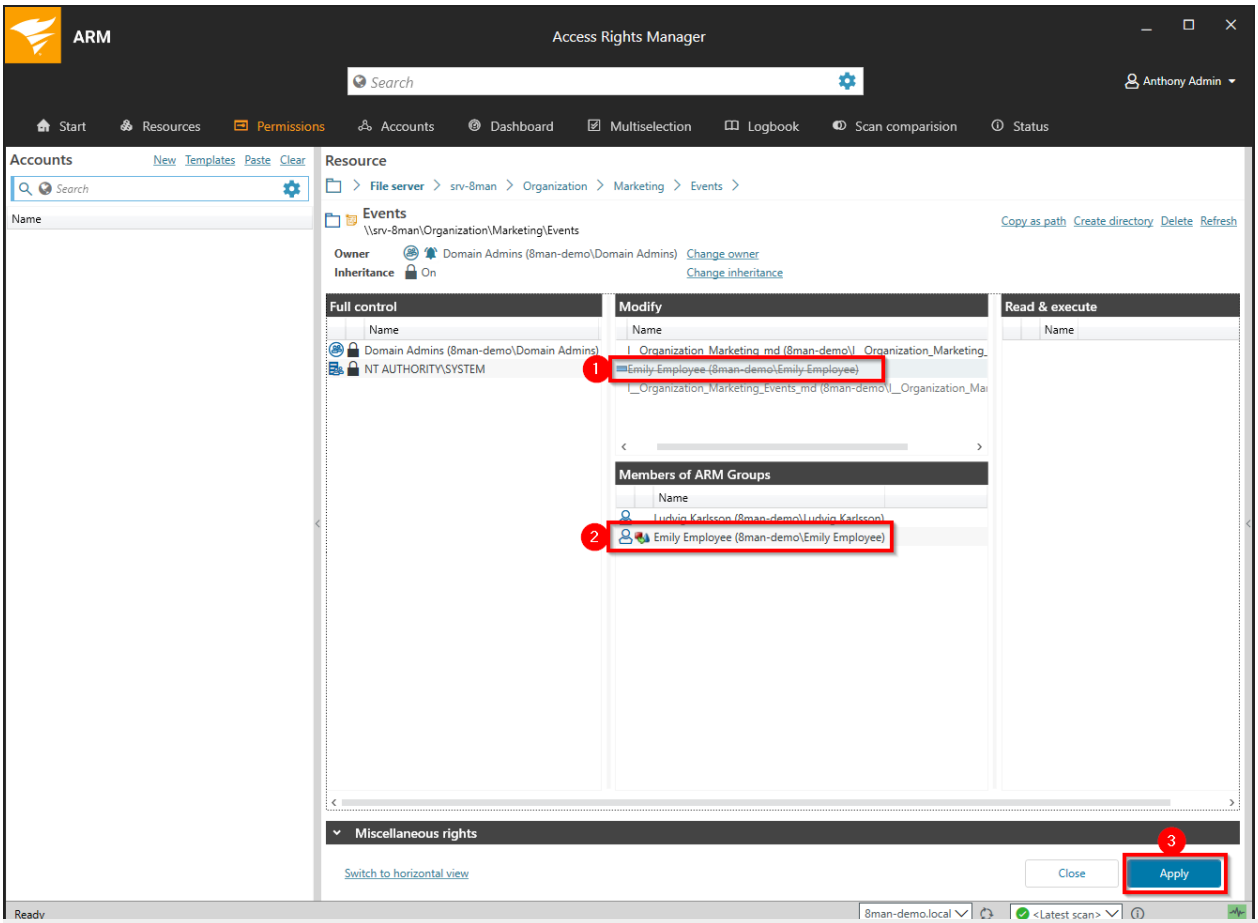
Step-by-step process



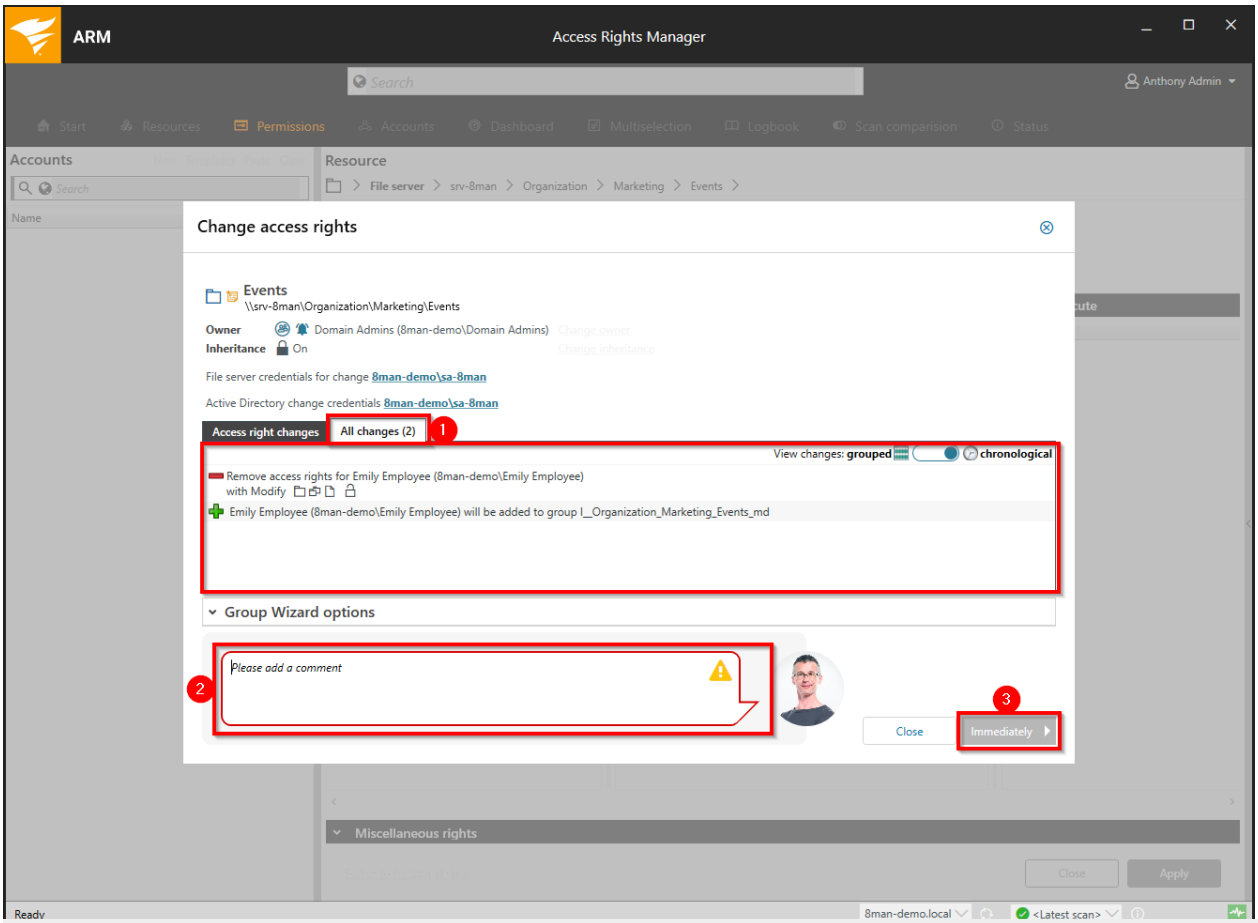
1. You have identified direct access rights.
2. Right-click on the affected directory.
3. Select "Modify access rights..." from the context menu.



Drag the user into the ARM group.



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

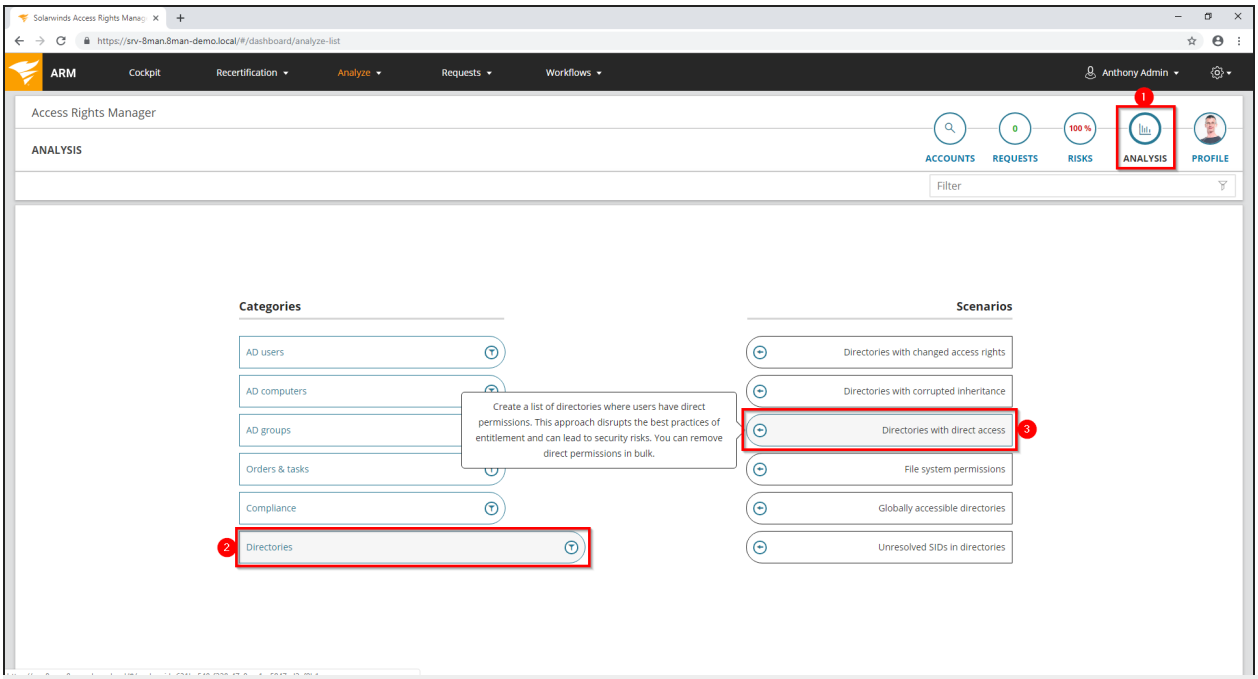
Direct permissions should be avoided and replaced by group permissions. Firstly, direct access rights are inefficient because every user is managed independently. Secondly, with native tools every directory needs to be examined individually to ensure the removal of all direct permissions. ARM shows you all direct access rights on your file server(s). You can remove them in bulk using the web client.

Related features

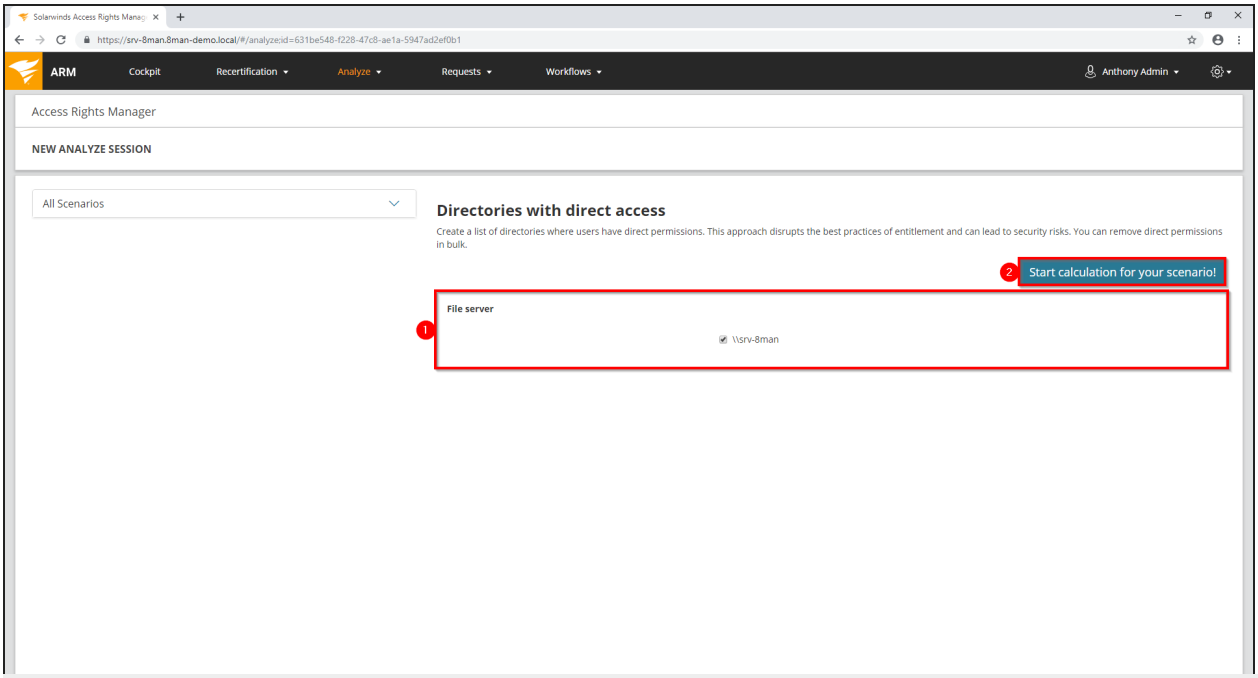
Change password options in bulk (web client)

Remove unresolved SIDs in bulk (web client)

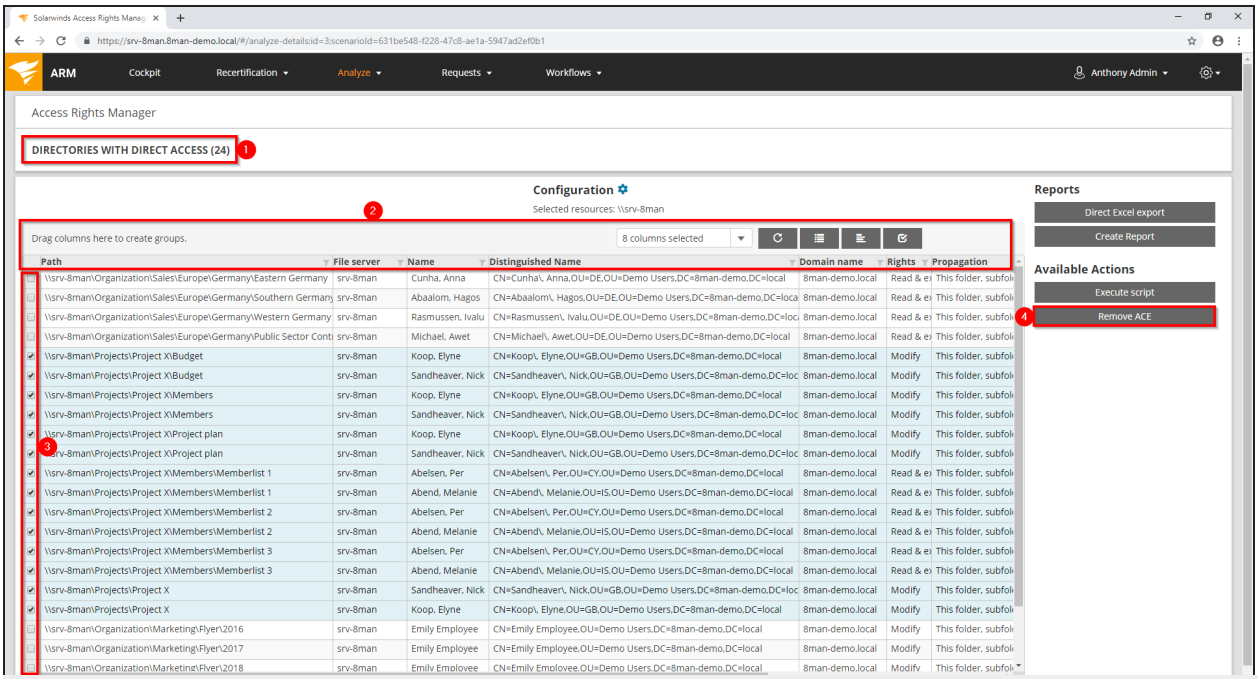
Step-by-step process



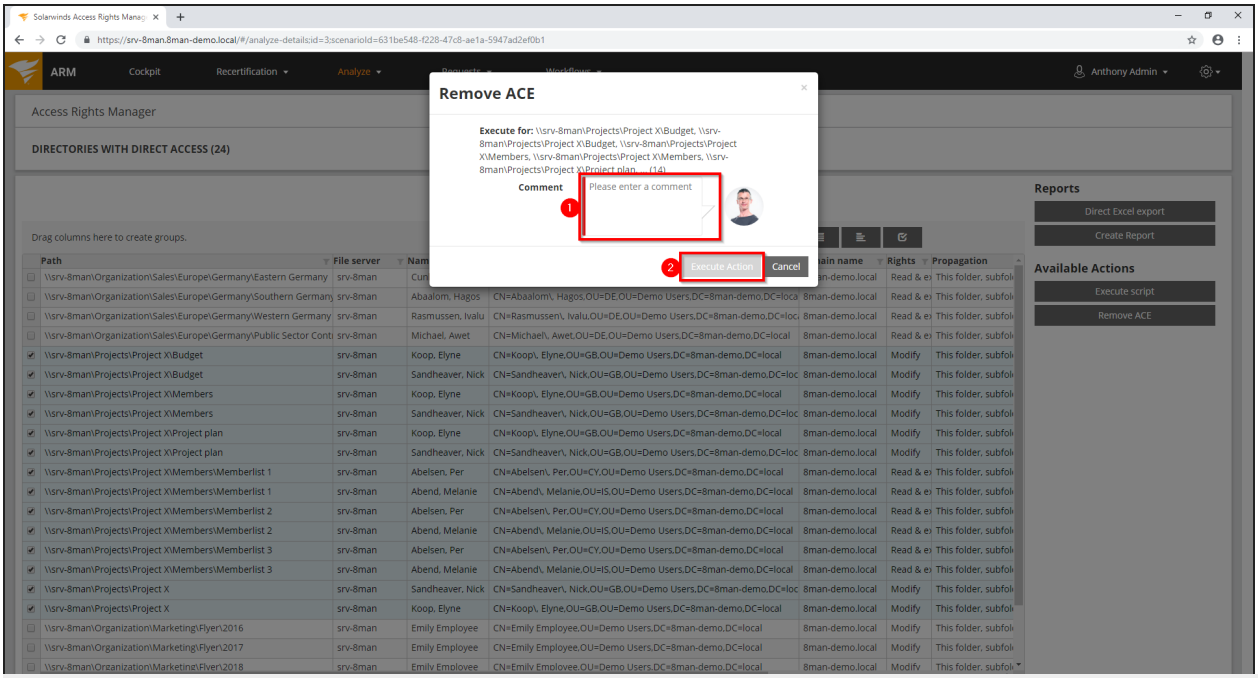
1. Select "Analysis".
2. Select the category "Directories".
3. Click "Directories with direct access".



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

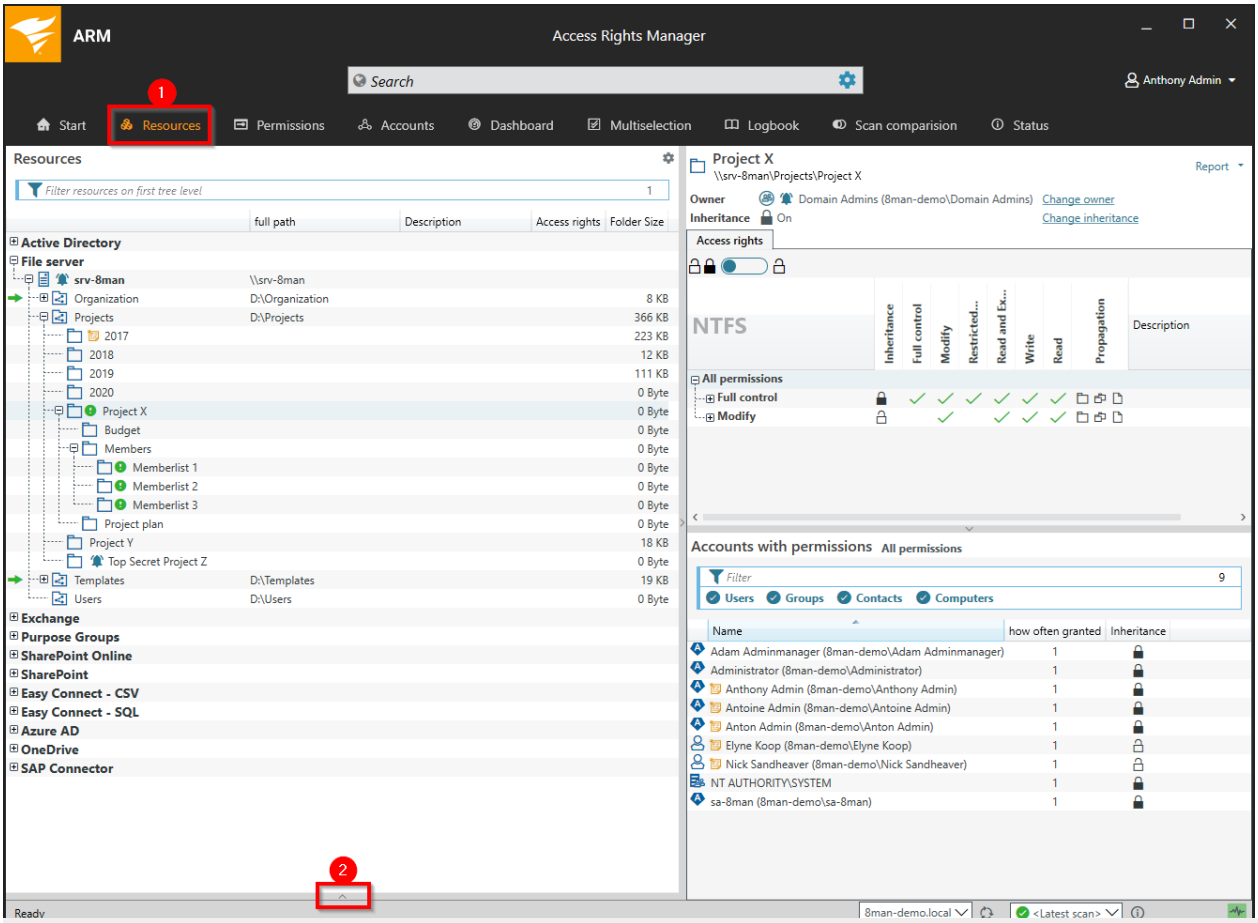
Background / Value

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.

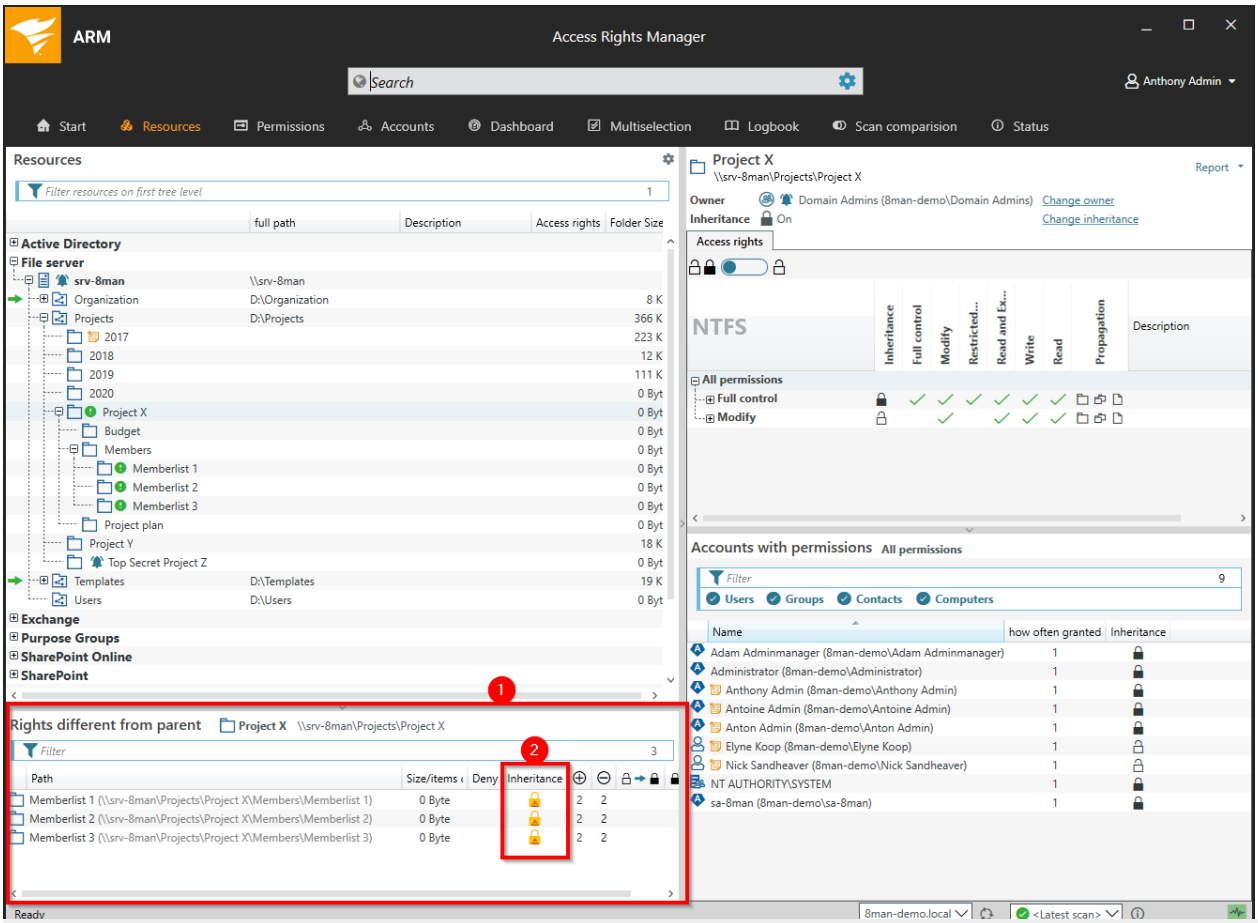
Related features

Identify errors in inheritance in the webclient and fix them in bulk

Step-by-step process

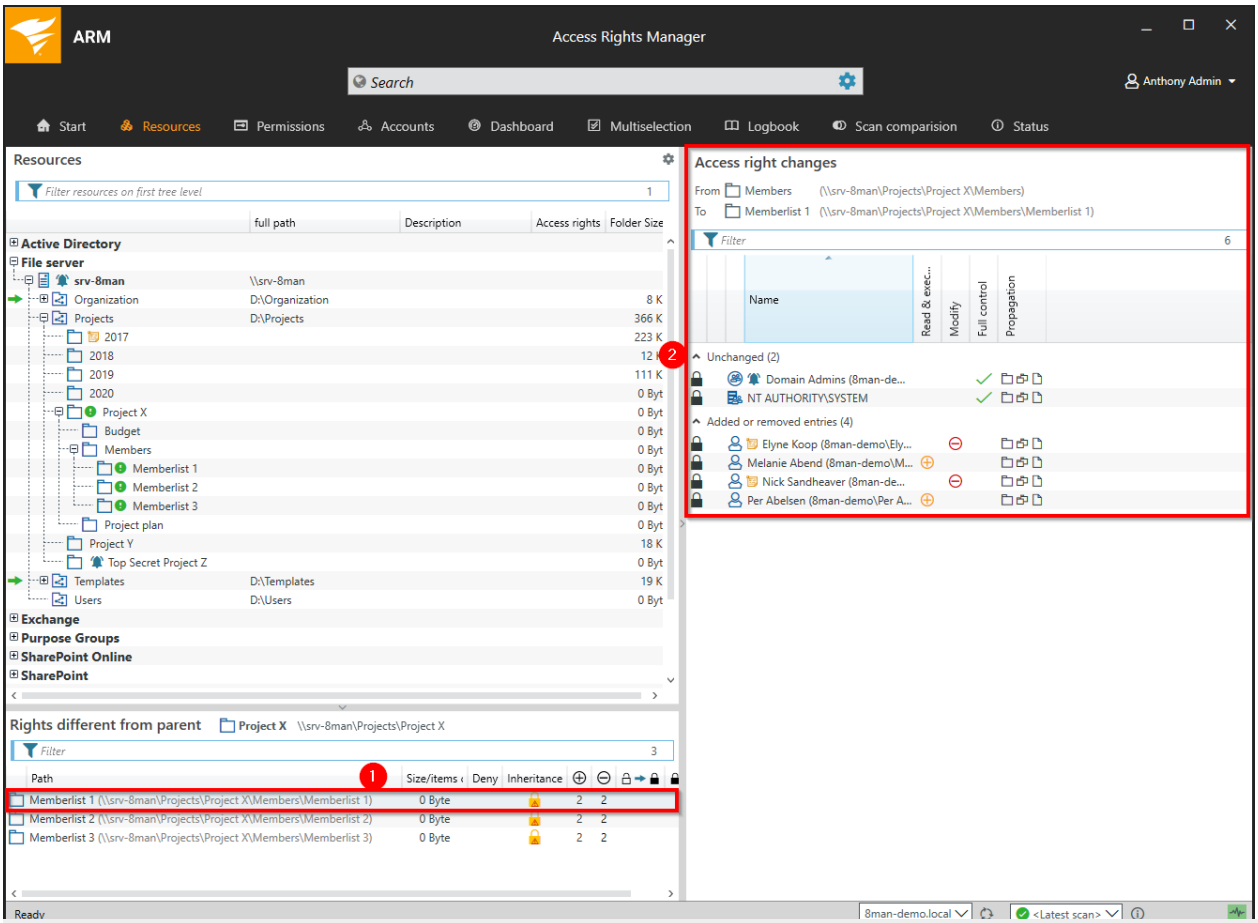


1. Select "Resources".
2. Expand the frame.

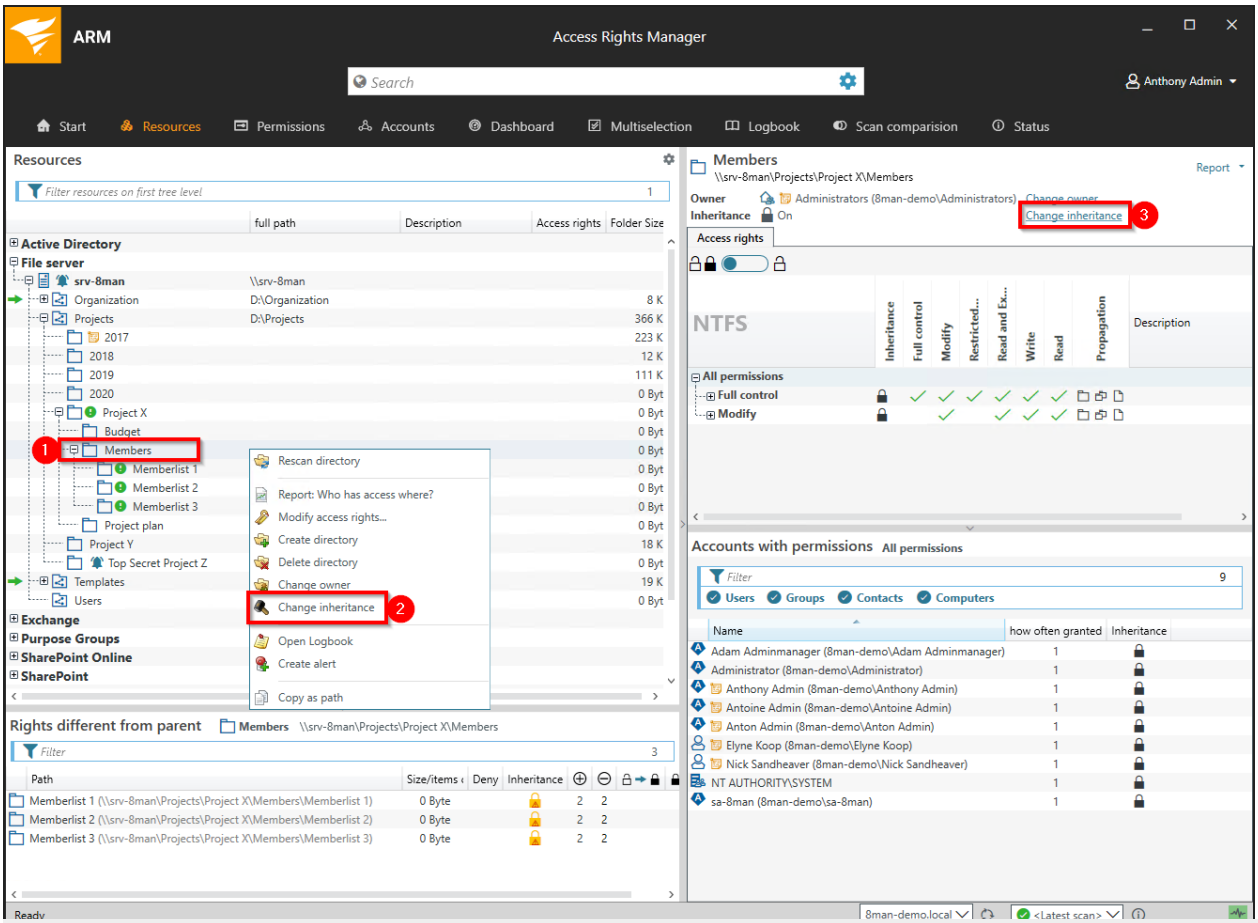


1. ARM lists all subdirectories with deviating permissions.
2. The yellow lock indicates a corrupted inheritance.

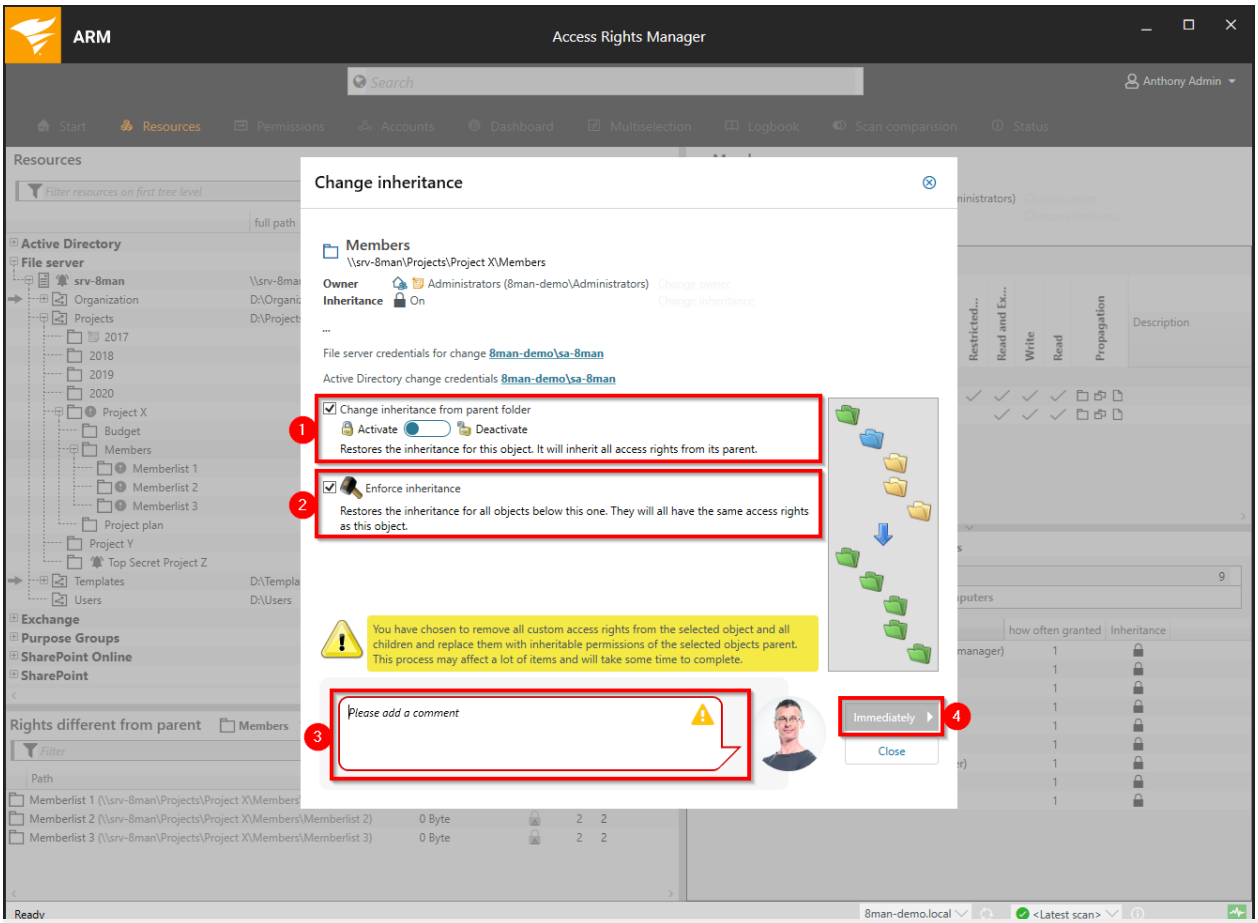
Use the sort function in the "Inheritance" column for long lists.



1. Select an entry.
2. ARM shows you in all details which permissions are different compared to the parent directory.



1. Select the subdirectory where you want to correct the corrupted inheritance.
2. or 3. Click "Change Inheritance".



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

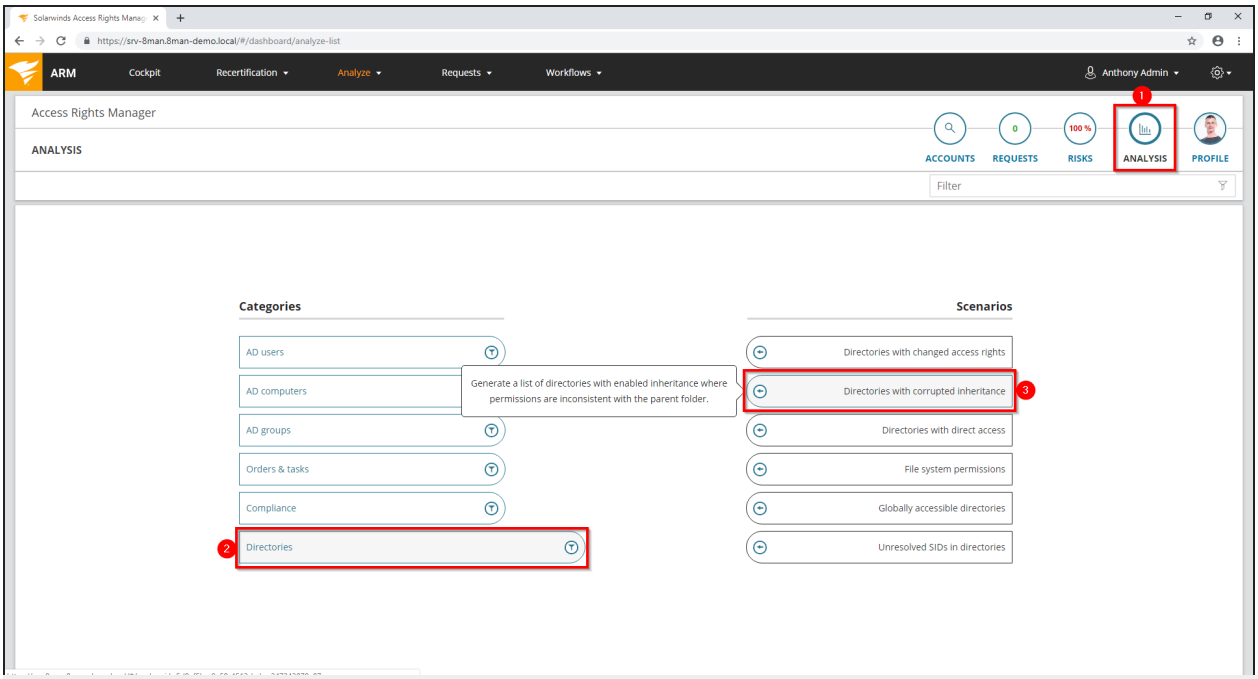
Errors in the inheritance of file server permissions often occur when employees copy or move directories. This can lead to unwanted access.

With the "Directories with corrupted inheritance" scenario, you can identify corrupted inheritance in a few clicks and eliminate them in one go.

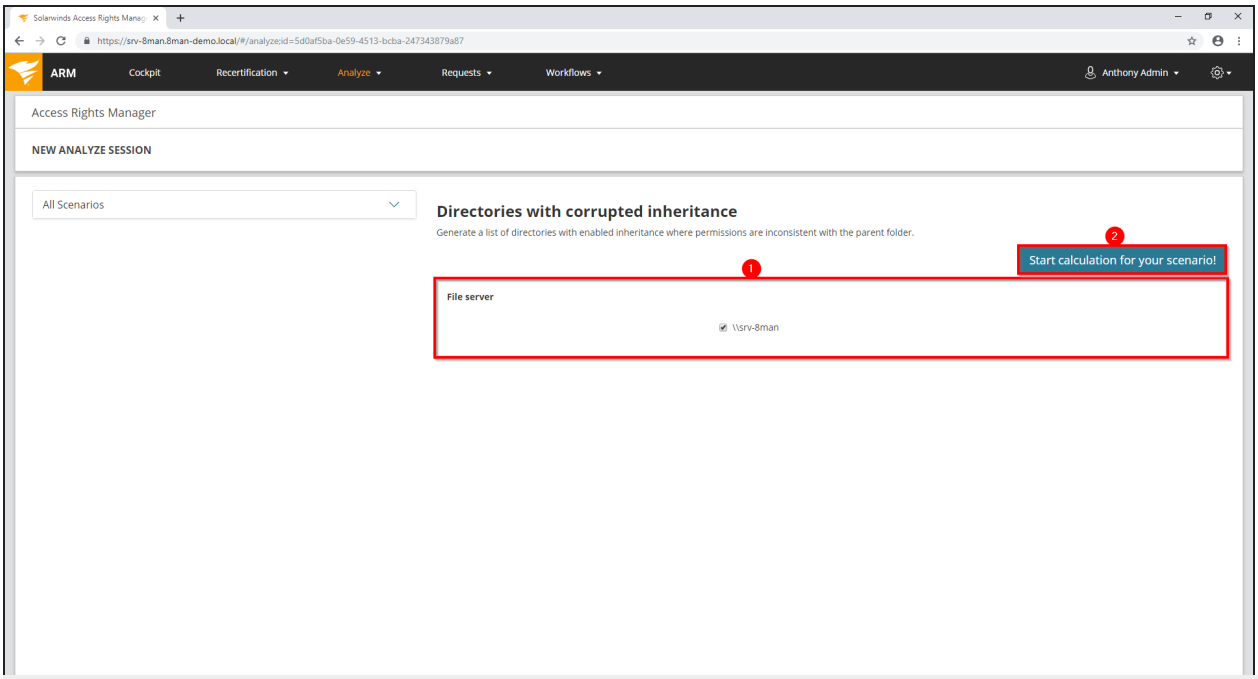
Related features

Identify corrupted inheritance

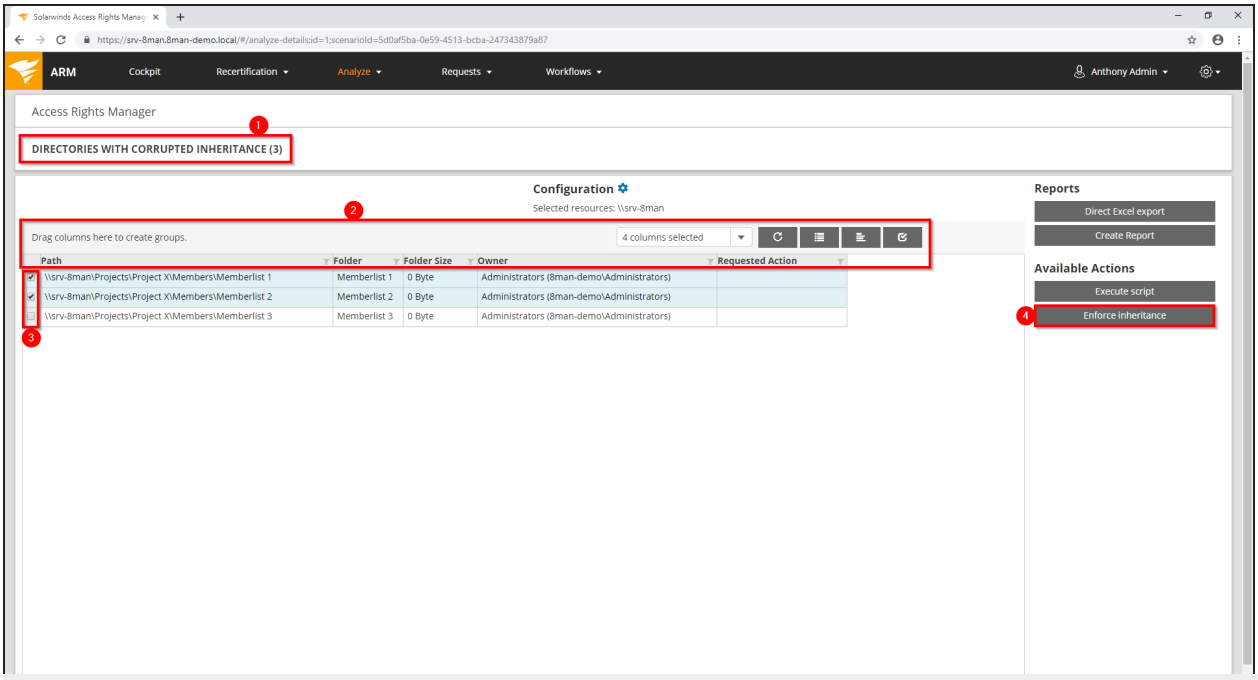
Step-by-step process



1. In the cockpit, choose "Analysis".
2. Select the category "Directories".
3. Click "Directories with corrupted inheritance".

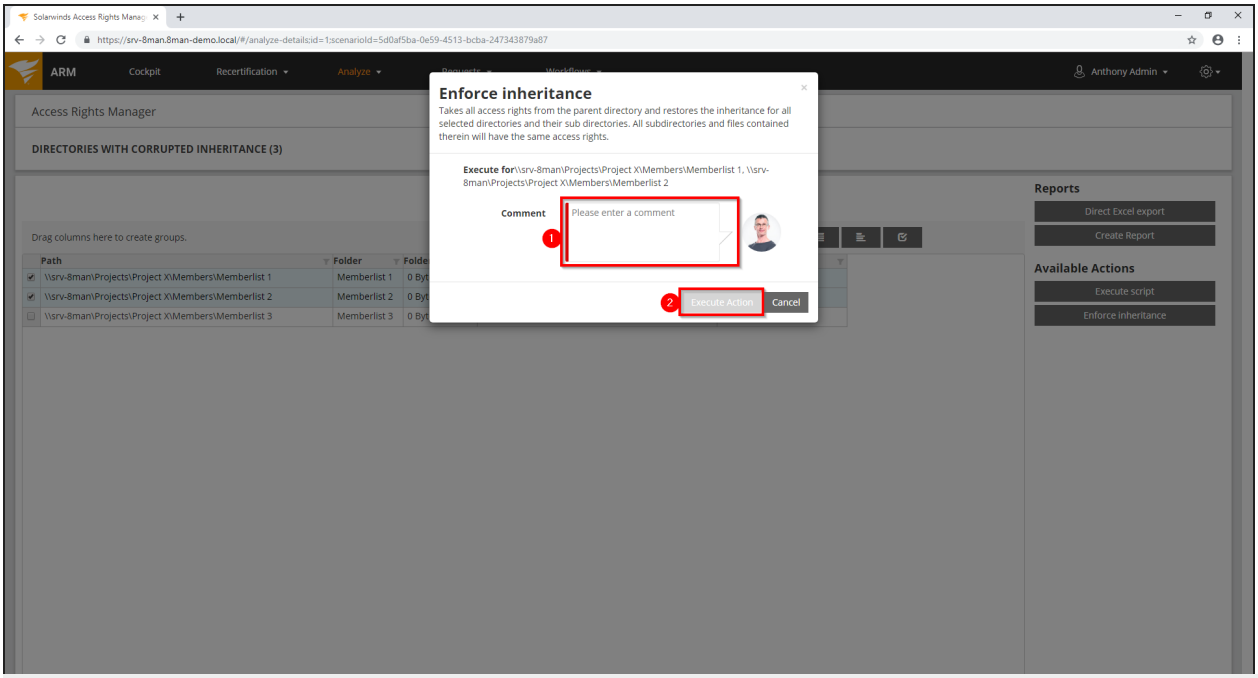


1. Determine which file servers are included in your analysis.
2. Start the calculation.



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

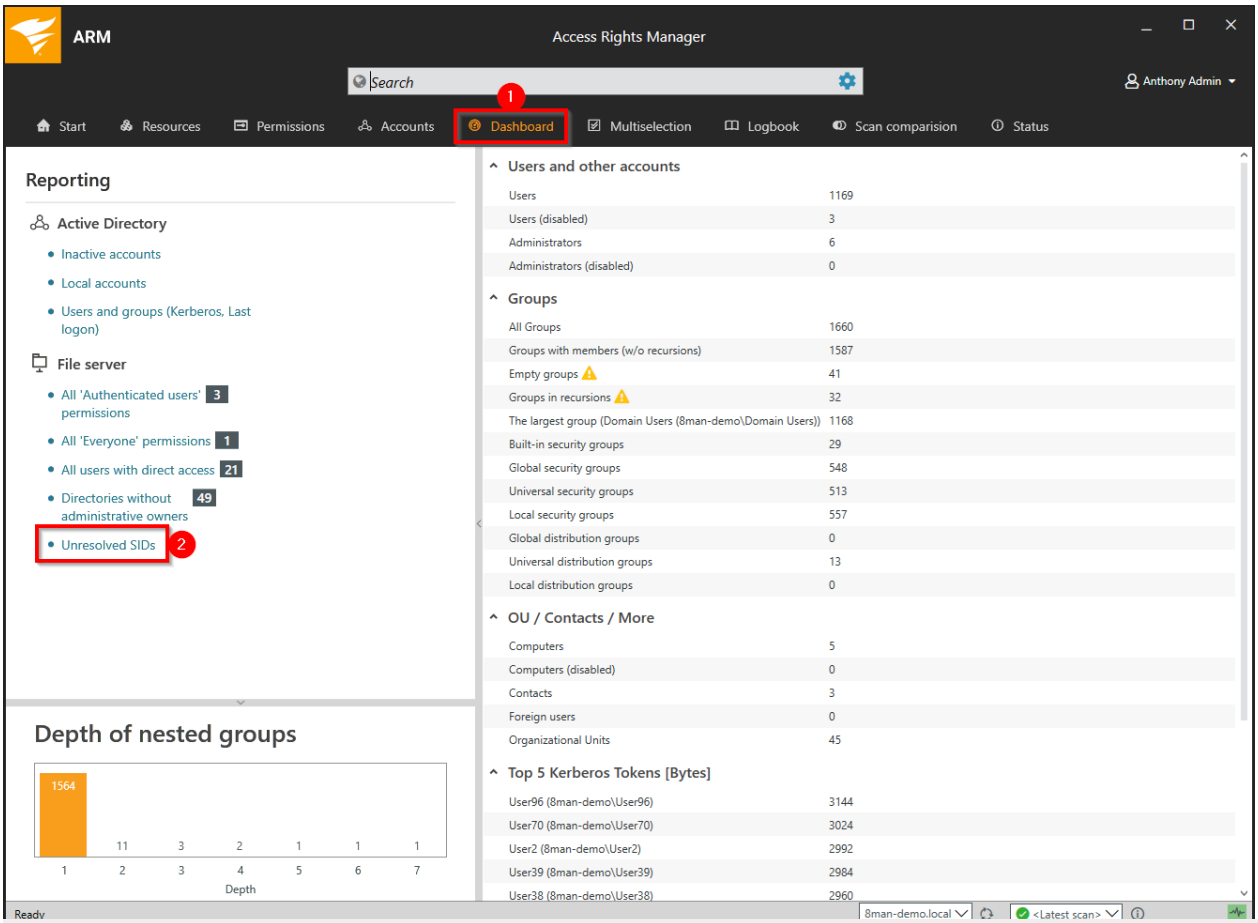
SIDs (Security Identifiers) are character strings that are used to identify user and group accounts in Active Directory. SIDs become unresolved when users or groups with direct access rights on file servers are deleted in AD.

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.

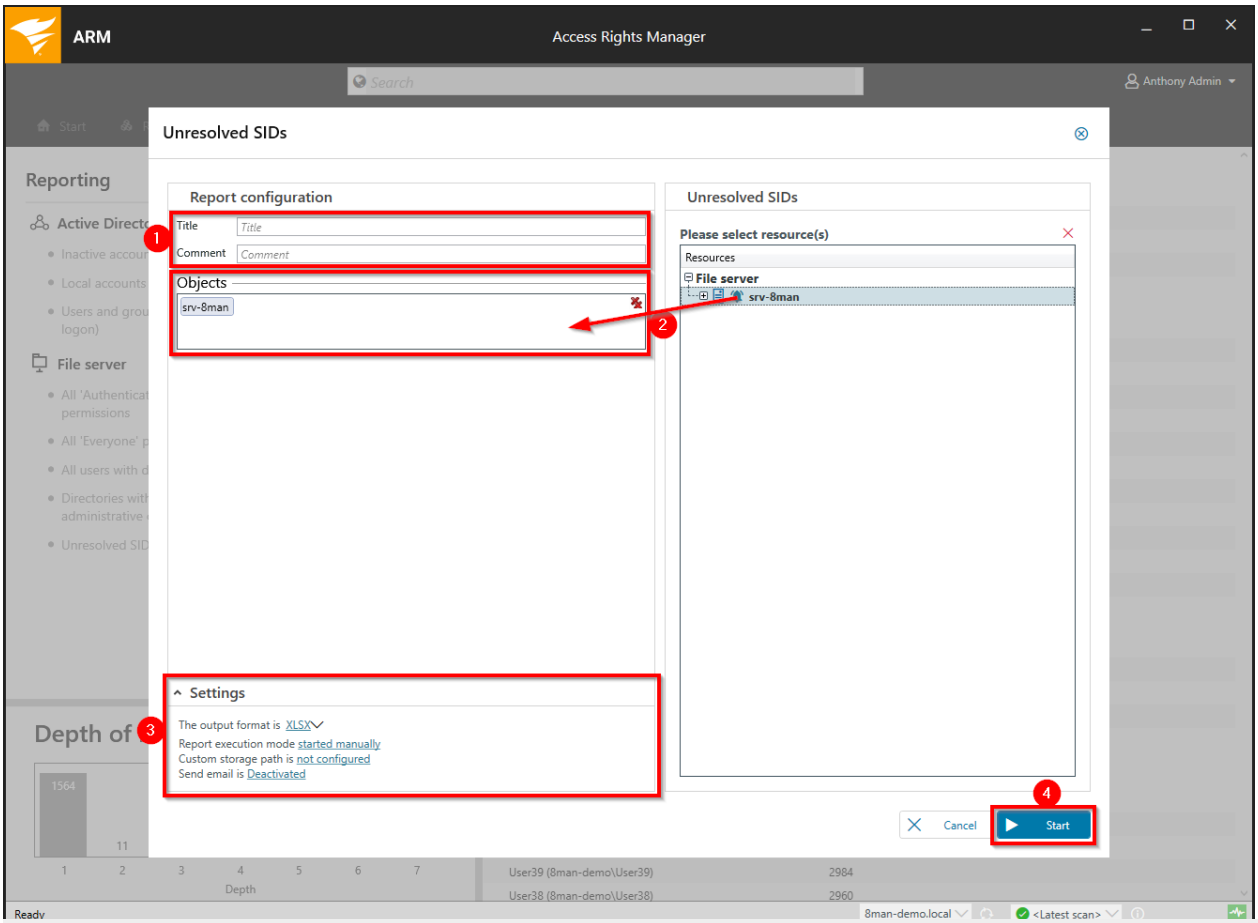
Related features

Remove unresolved SIDs in bulk (web client)

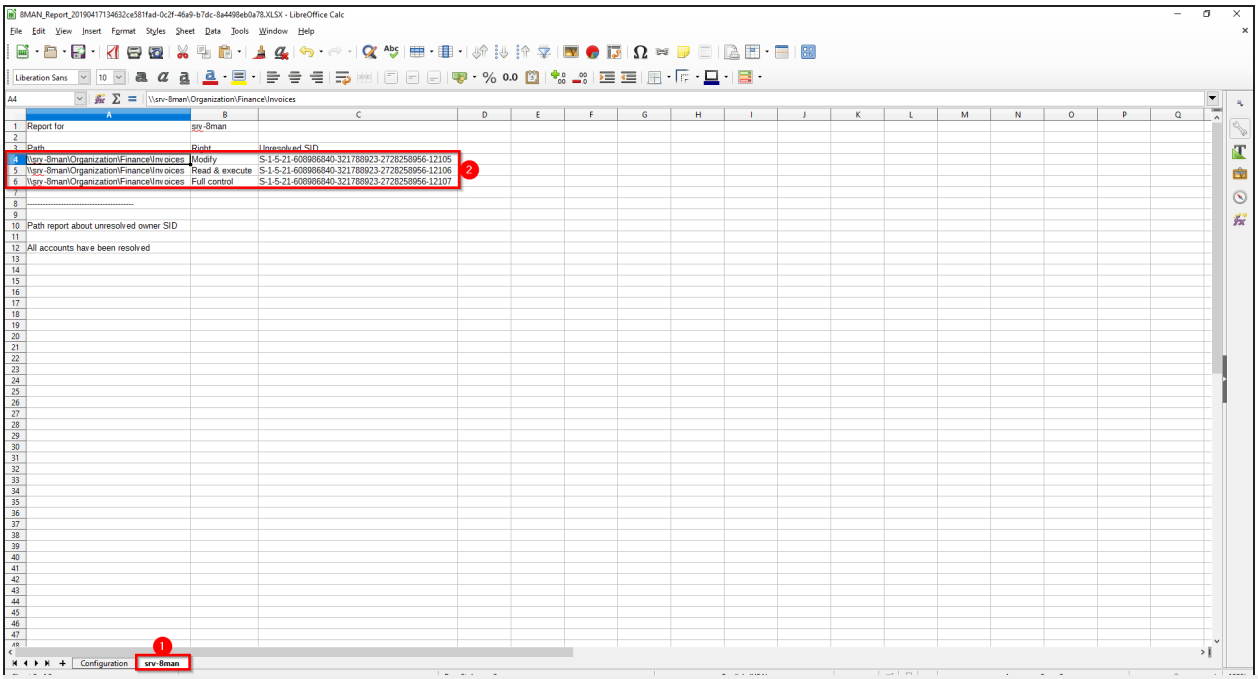
Step-by-step process



1. Select "Dashboard".
2. Click on "Unresolved SIDs".

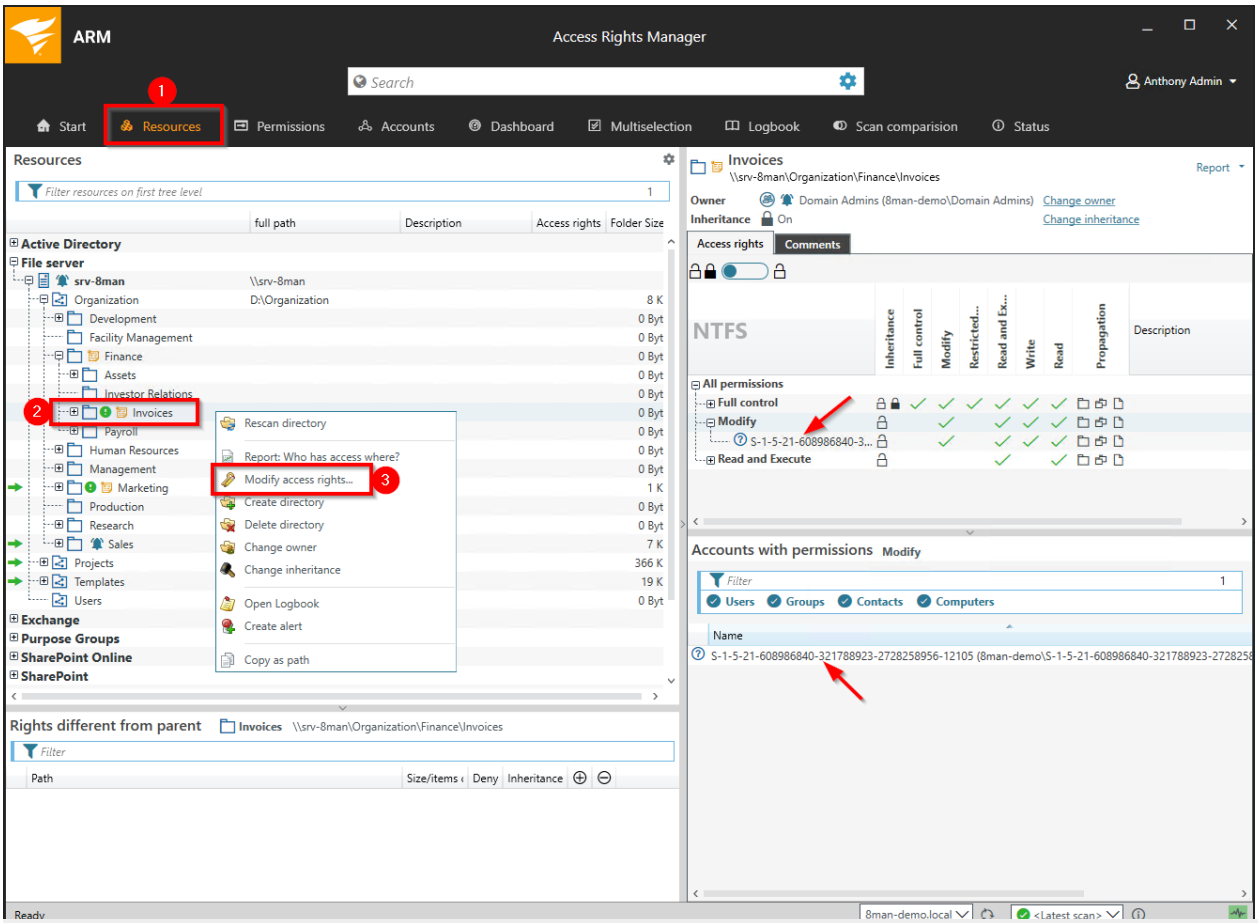


1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired report settings.
4. Start the report.

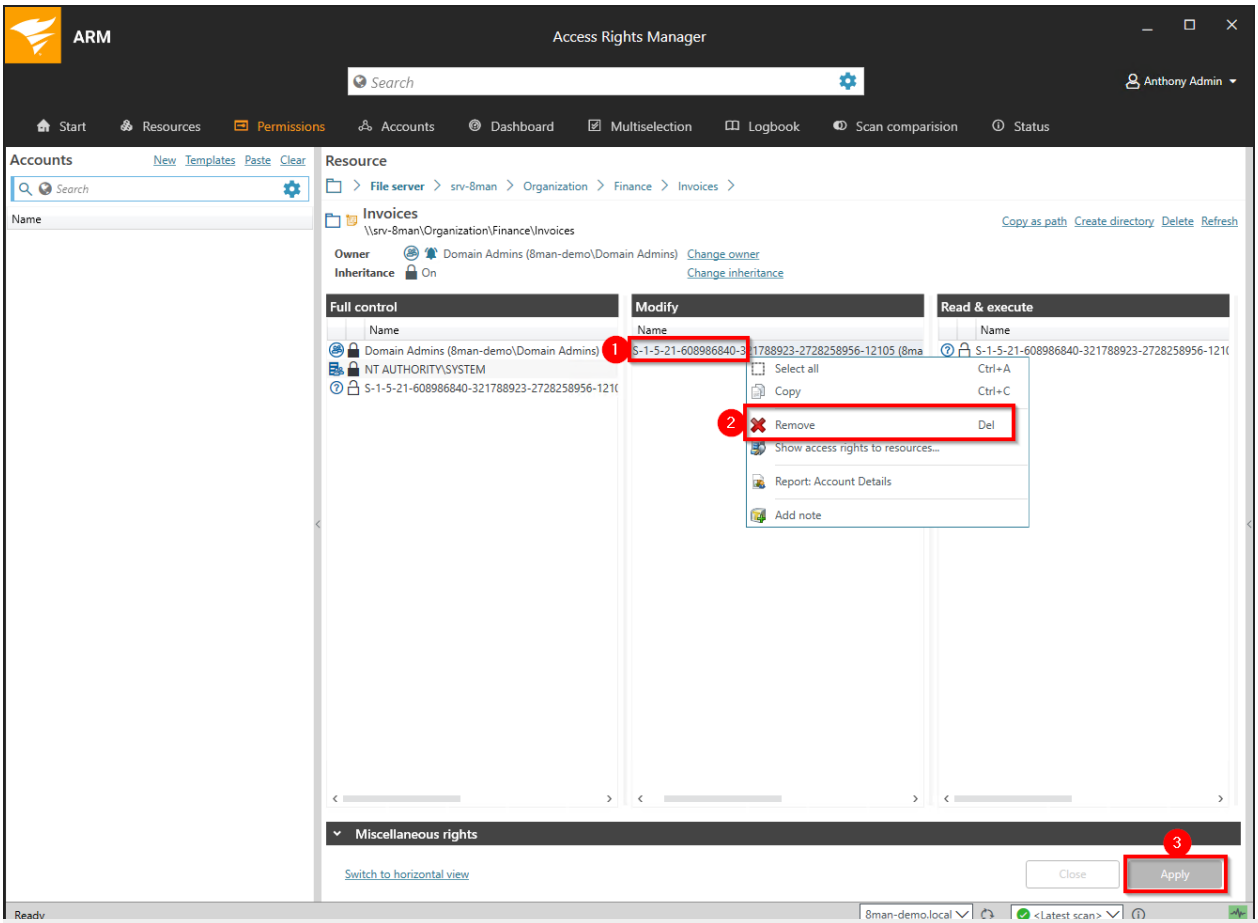


Open the report in your spreadsheet application.

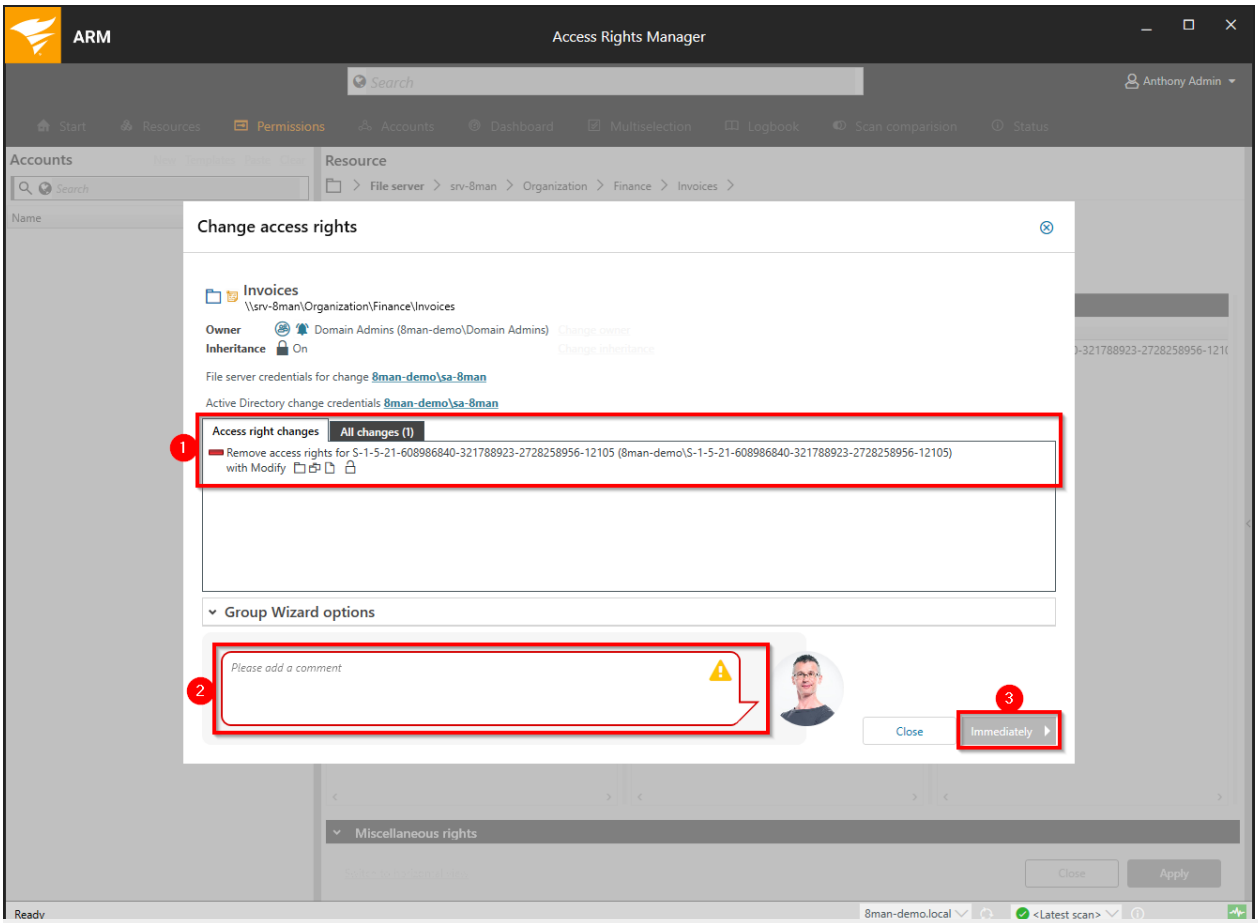
1. Switch to the file server tab.
2. All unresolved SIDs are listed in the report.



1. Select "Resources".
2. Select an affected directory.
3. Right-click on the directory and select "Modify access rights..." from the context menu.



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.

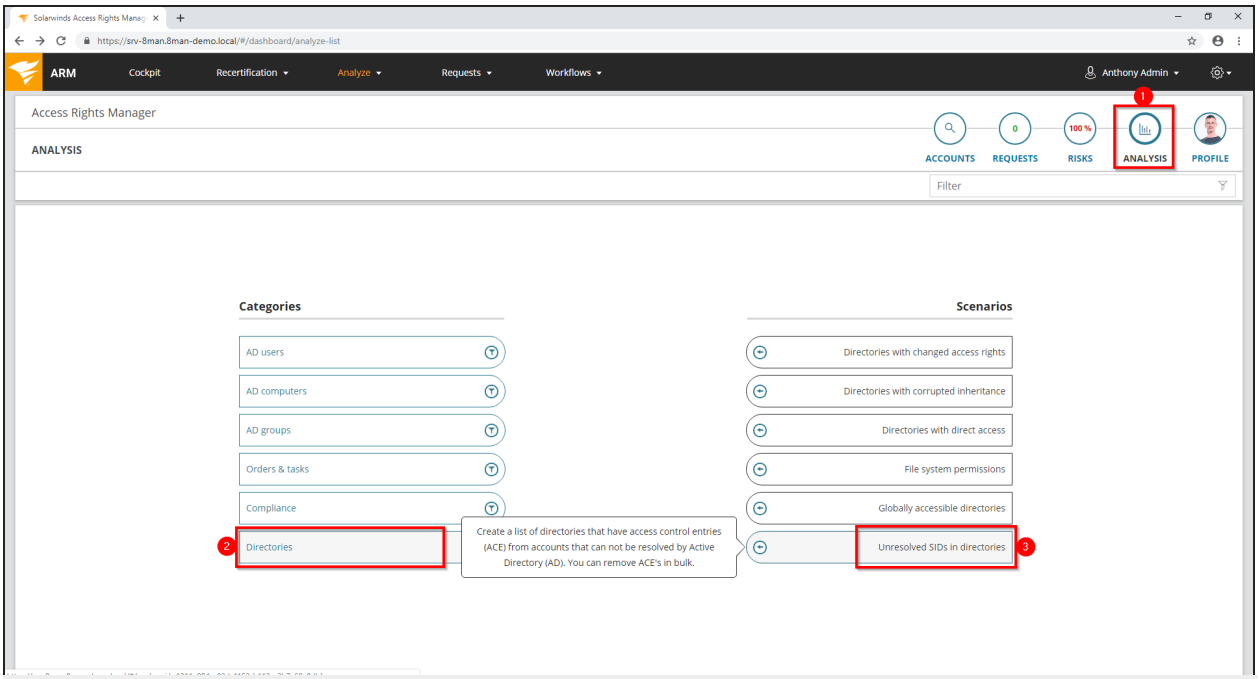
ARM clearly identifies unresolved SIDs in your system. Delete unresolved SIDs in bulk using the web client.

Related features

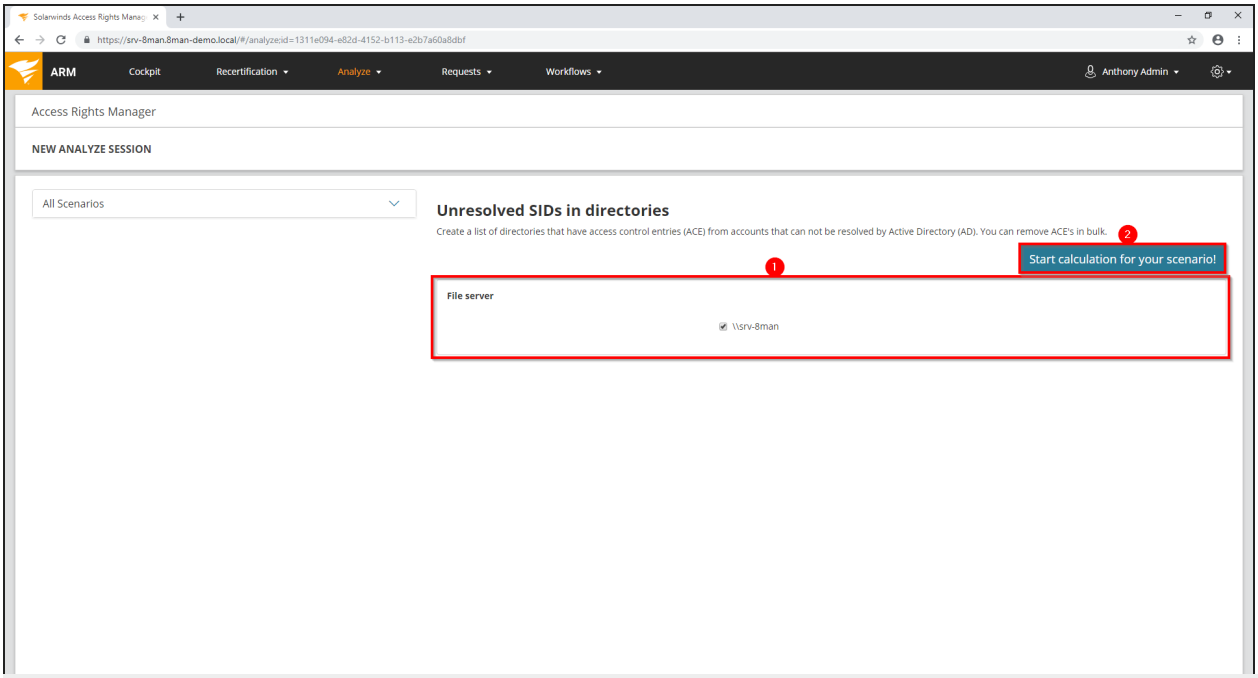
Identify and delete unresolved SIDs (rich client)

Report: Identify unresolved SIDs (rich client)

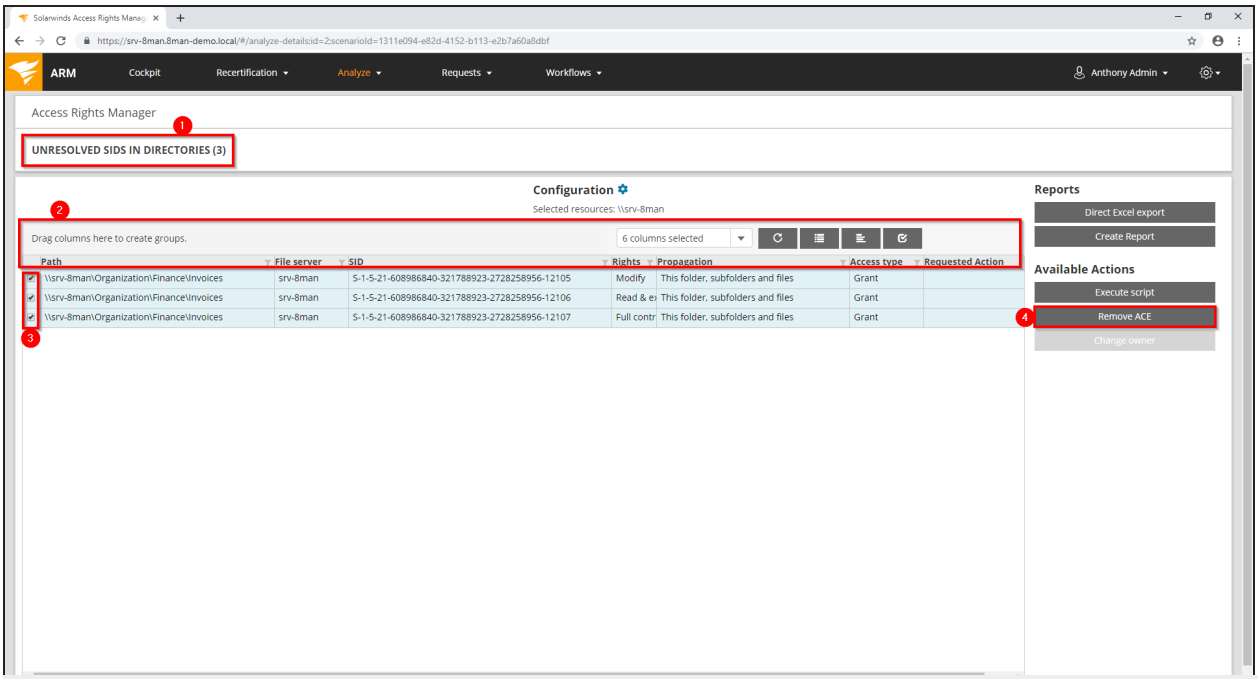
Step-by-step process



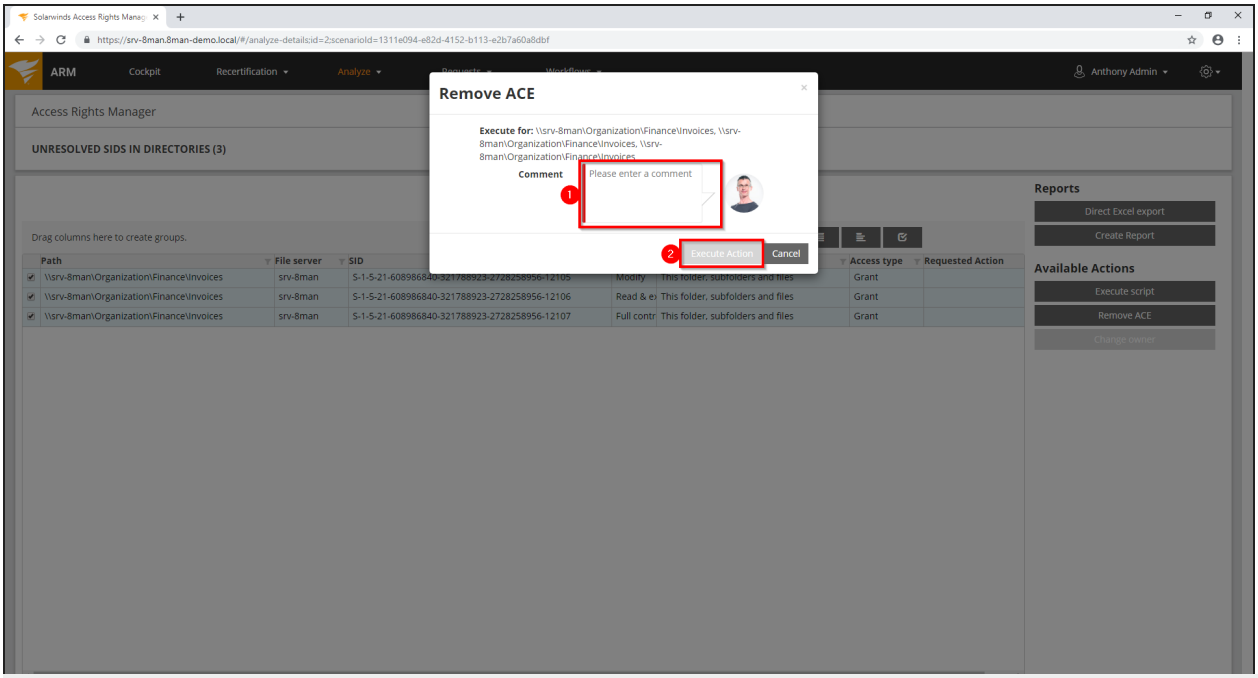
1. Select "Analysis".
2. Select the category "Directories".
3. Click "Unresolved SIDs in directories".



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:

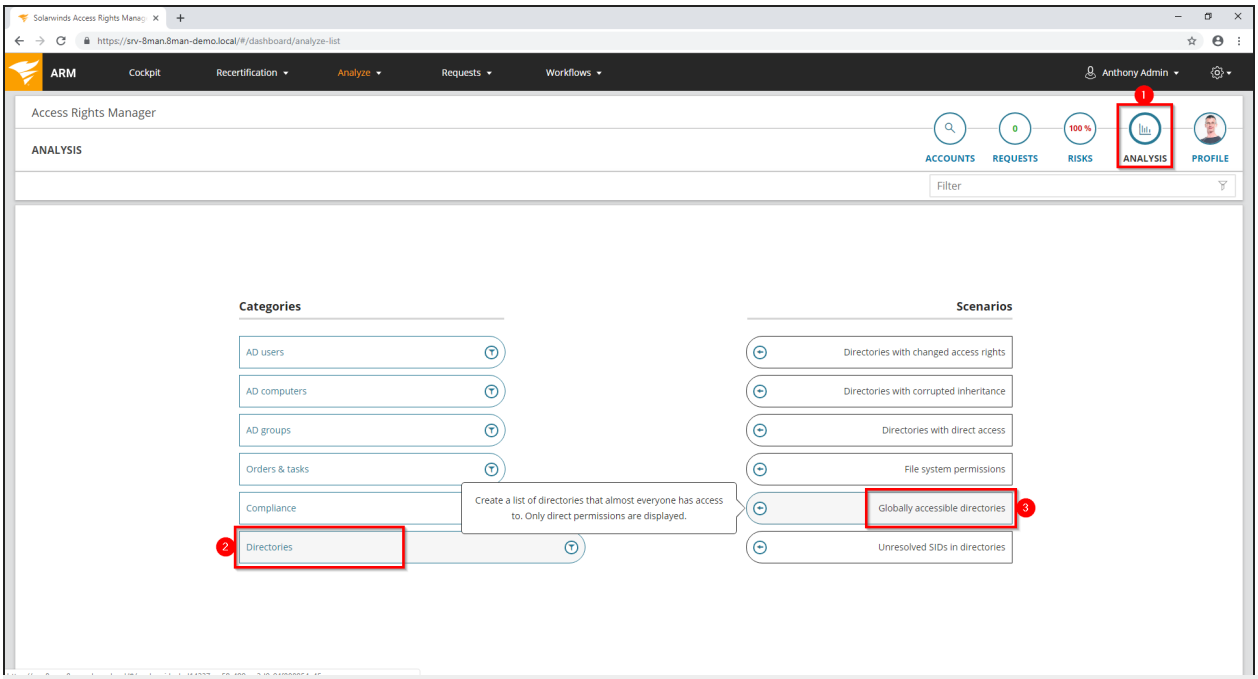
- Everyone
- Authenticated Users
- Domain-Users

Related features

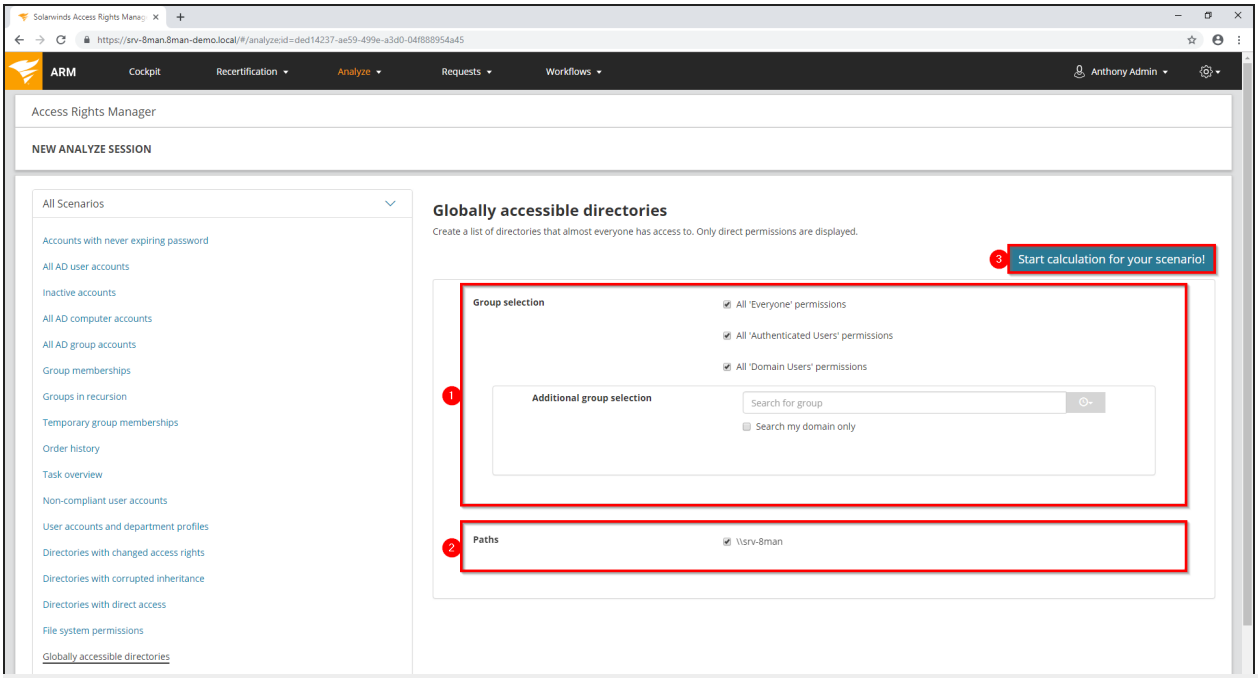
Report: Identify usage of "Everyone" (rich client)

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".

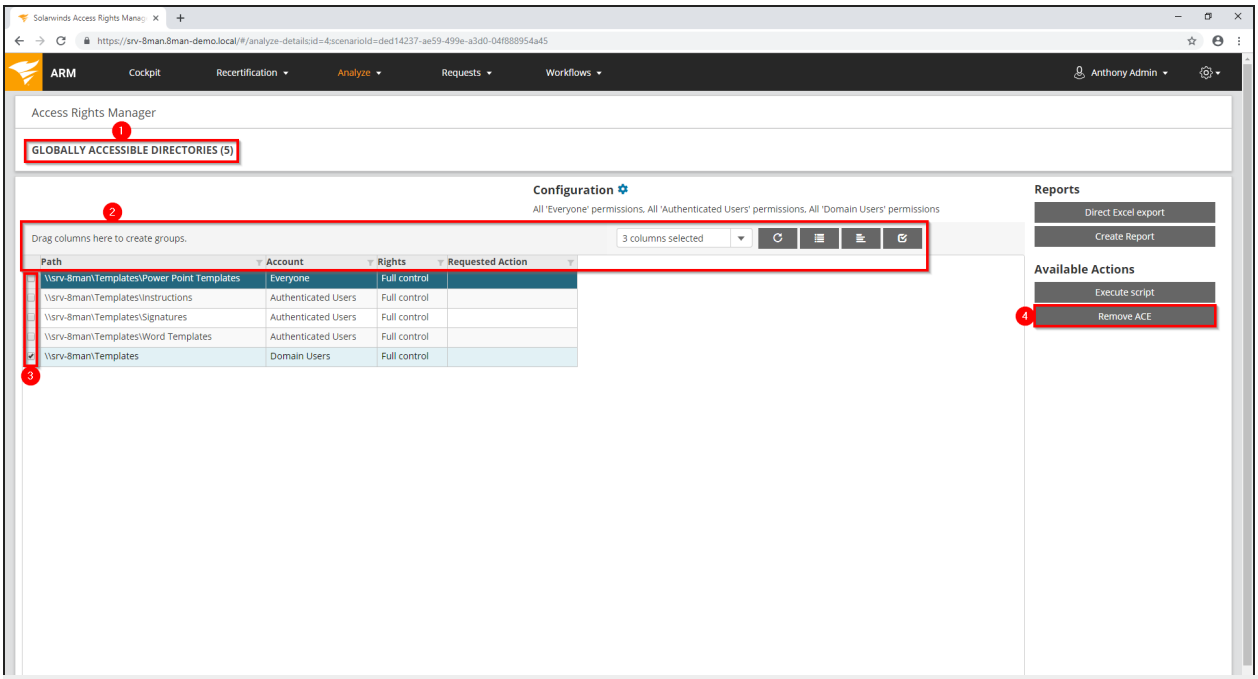


1. Select security principals.
   You can add one additional group. This is very useful for "catch-all" groups, e.g. "mycompany-

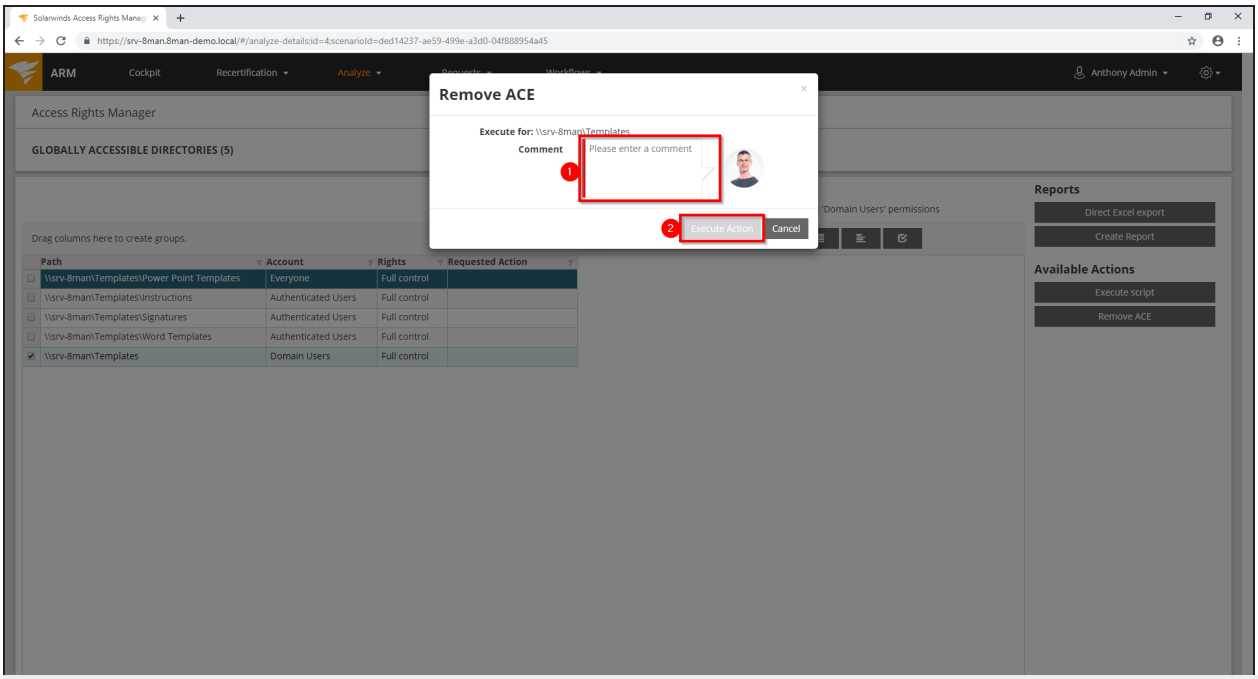
complete".

The scenario only considers direct access control entries (ACEs). Group nesting is not resolved.

2. Select the file servers.
3. Start the calculation.



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

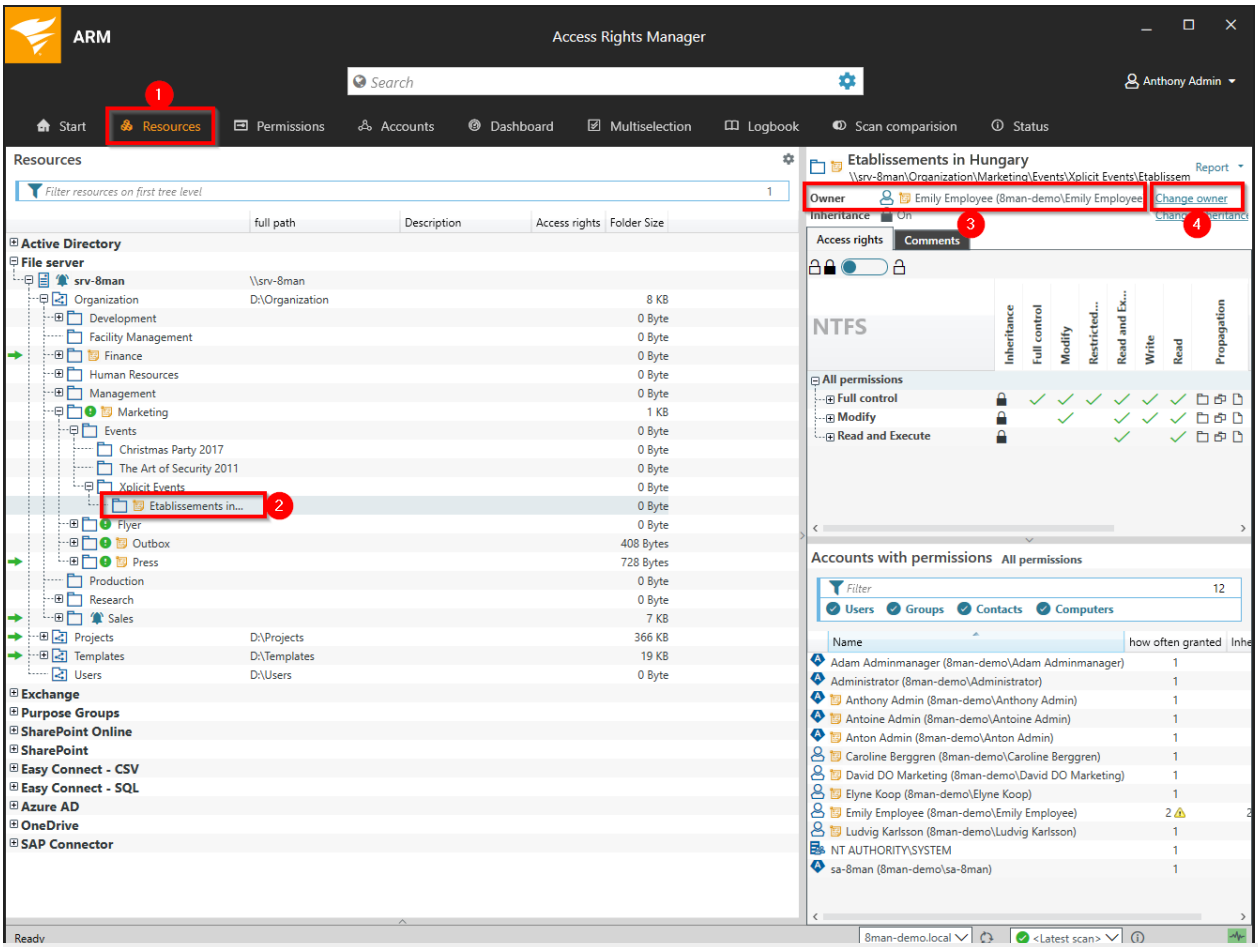
Background / Value

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.

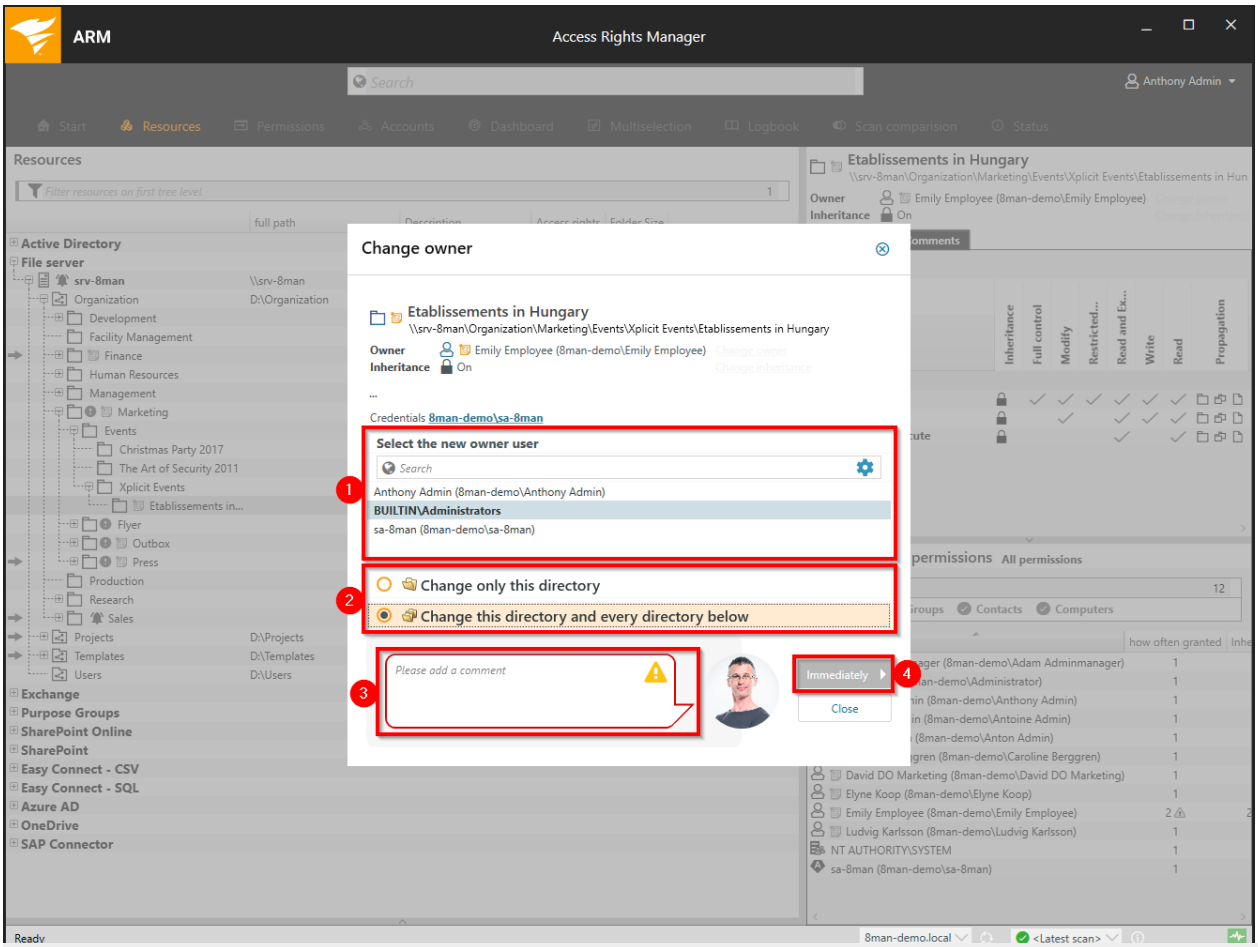
Related features

Identify directories whose owners are not administrators (report)

Step-by-step process



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)

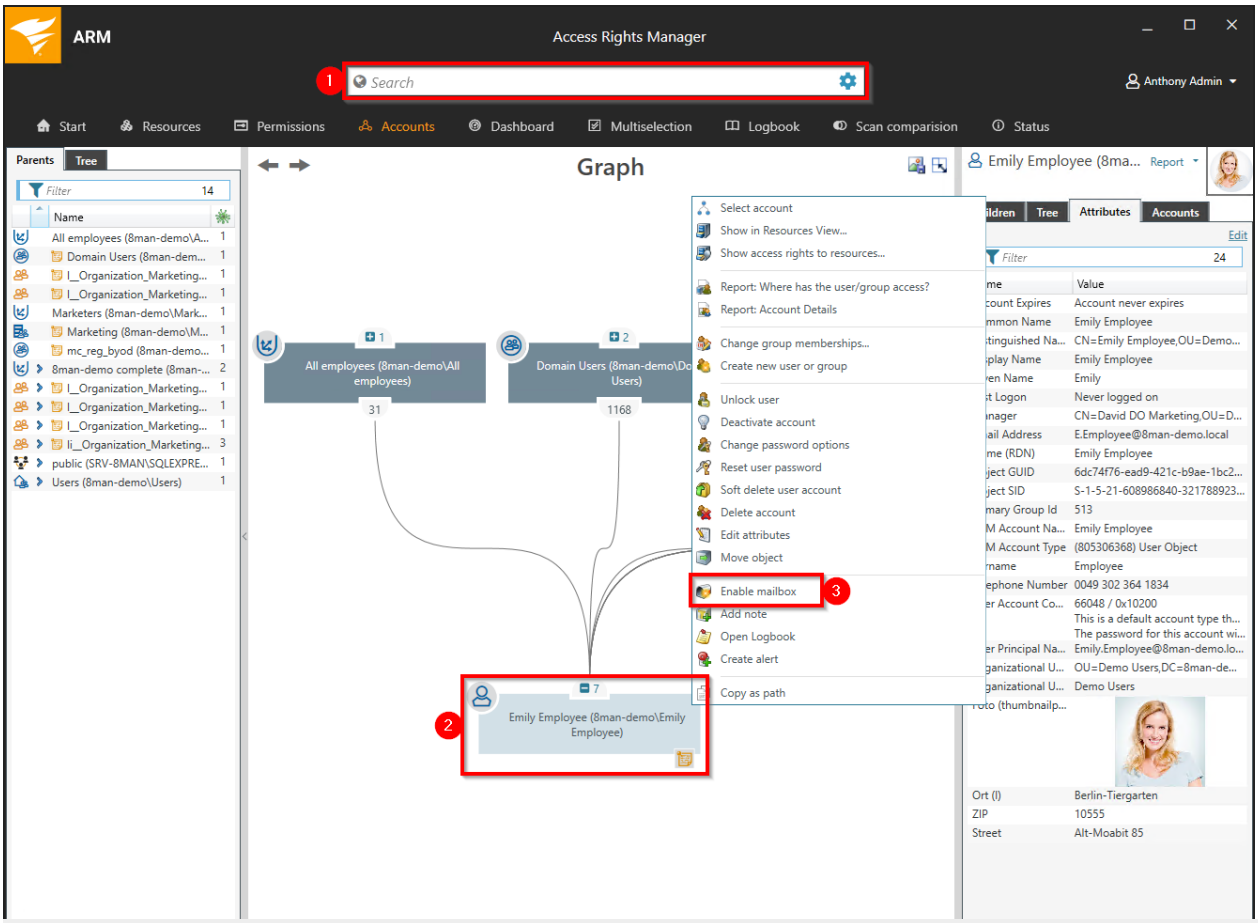
Background / Value

With ARM you can create mailboxes (email enable accounts) in Exchange (on-premise).

Related features

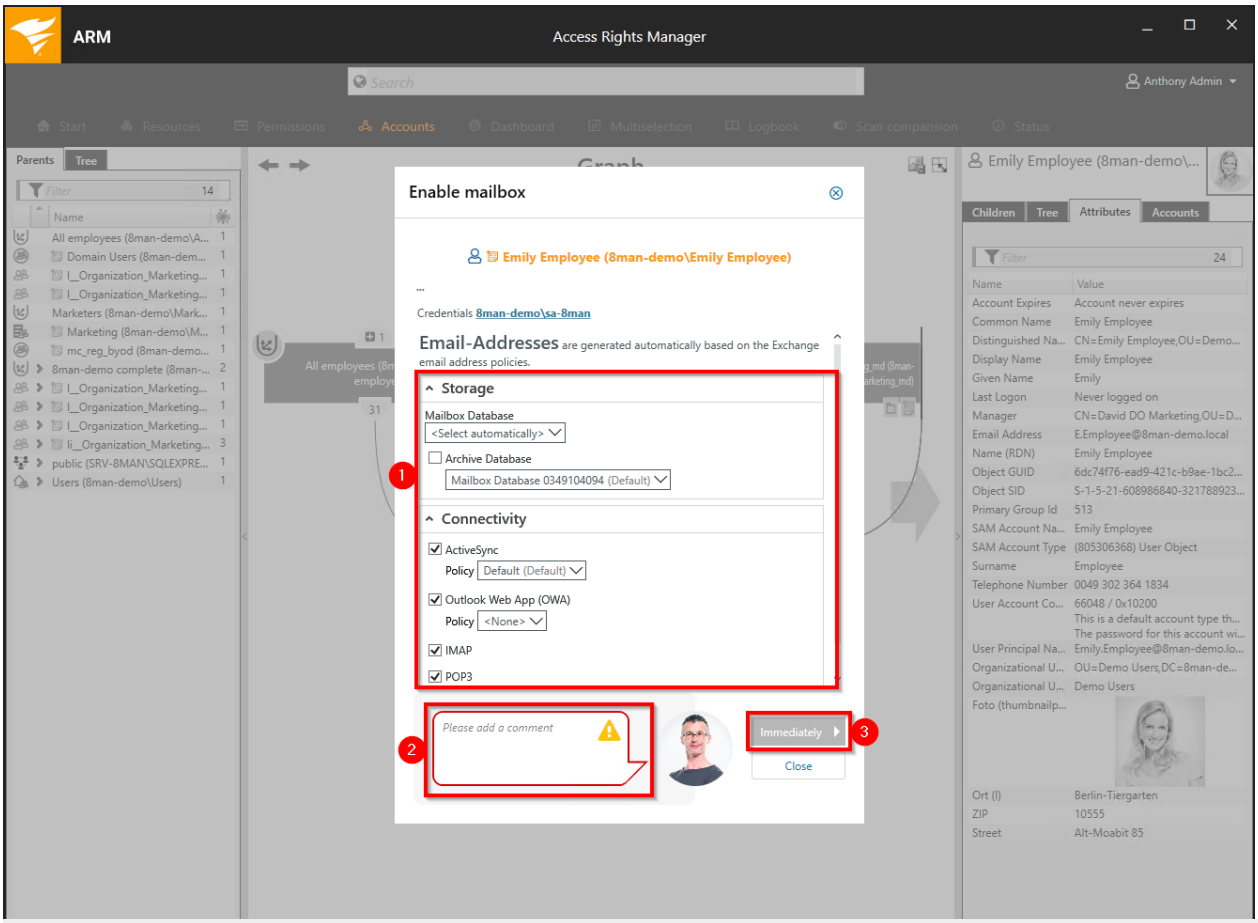
Create a mailbox in Exchange Online

Step-by-step process



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.

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.



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

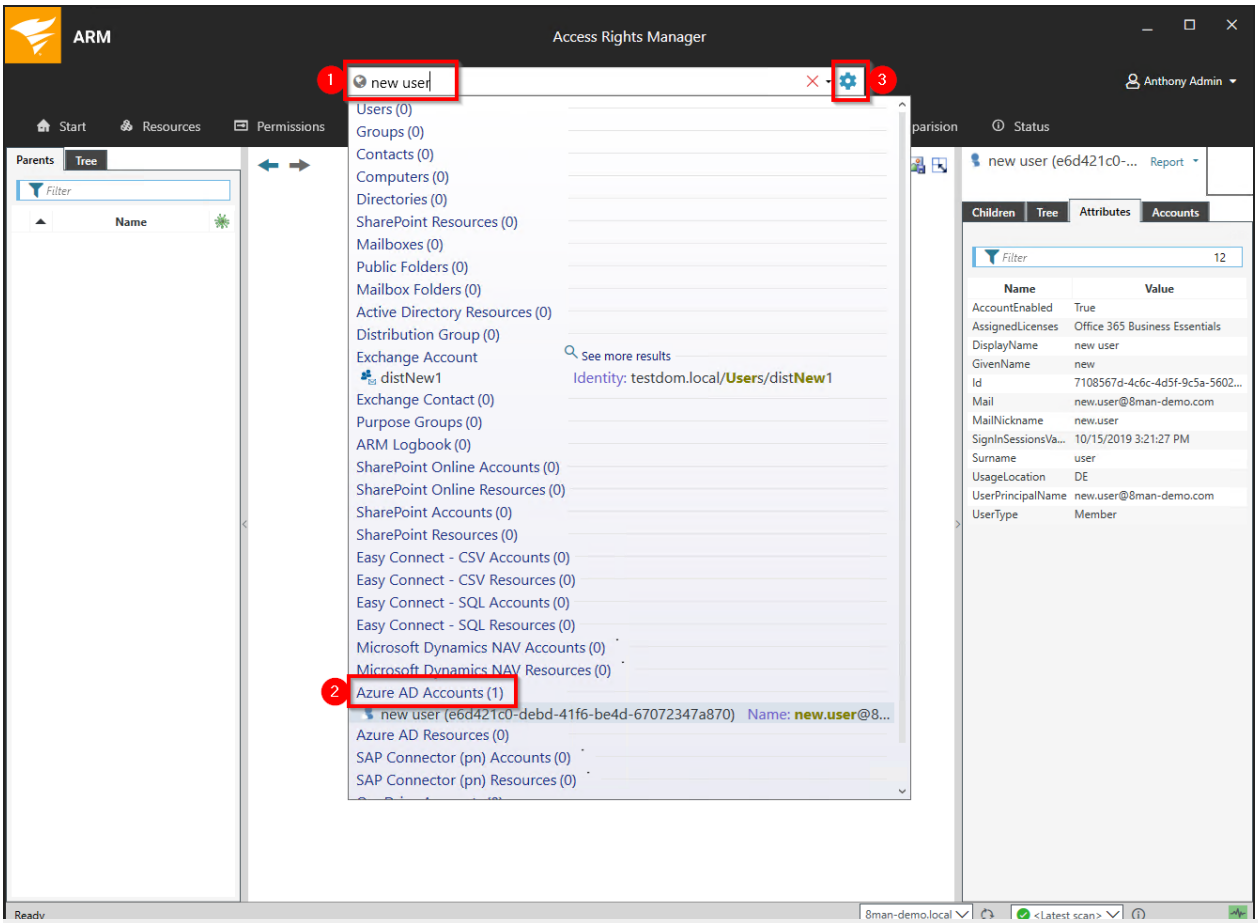
With ARM you can create mailboxes in Exchange Online by assigning an Office 365 license that includes Exchange Online.

Related features

[Create a new user account in Azure Active Directory]

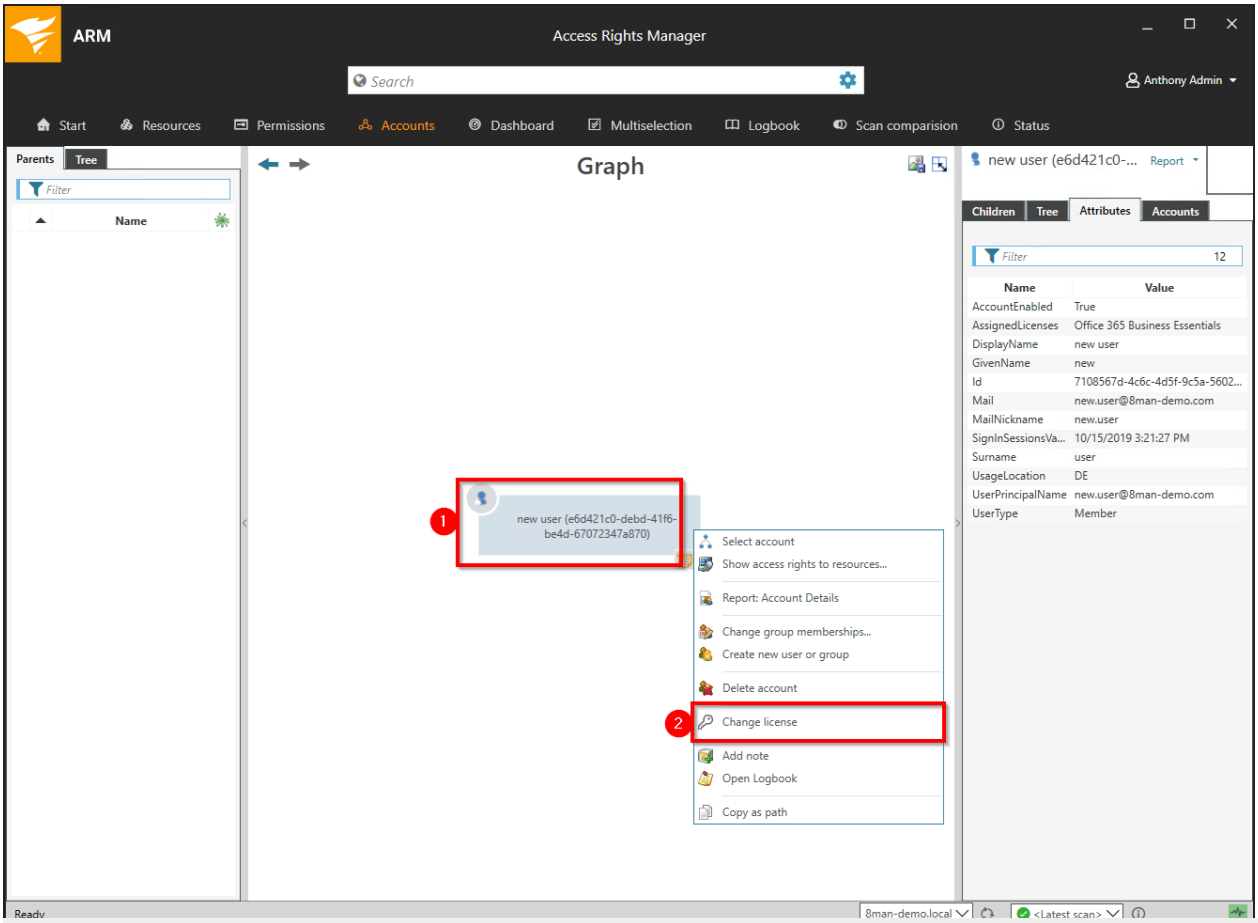
[Create a mailbox in Exchange on-premise]

Step-by-step process

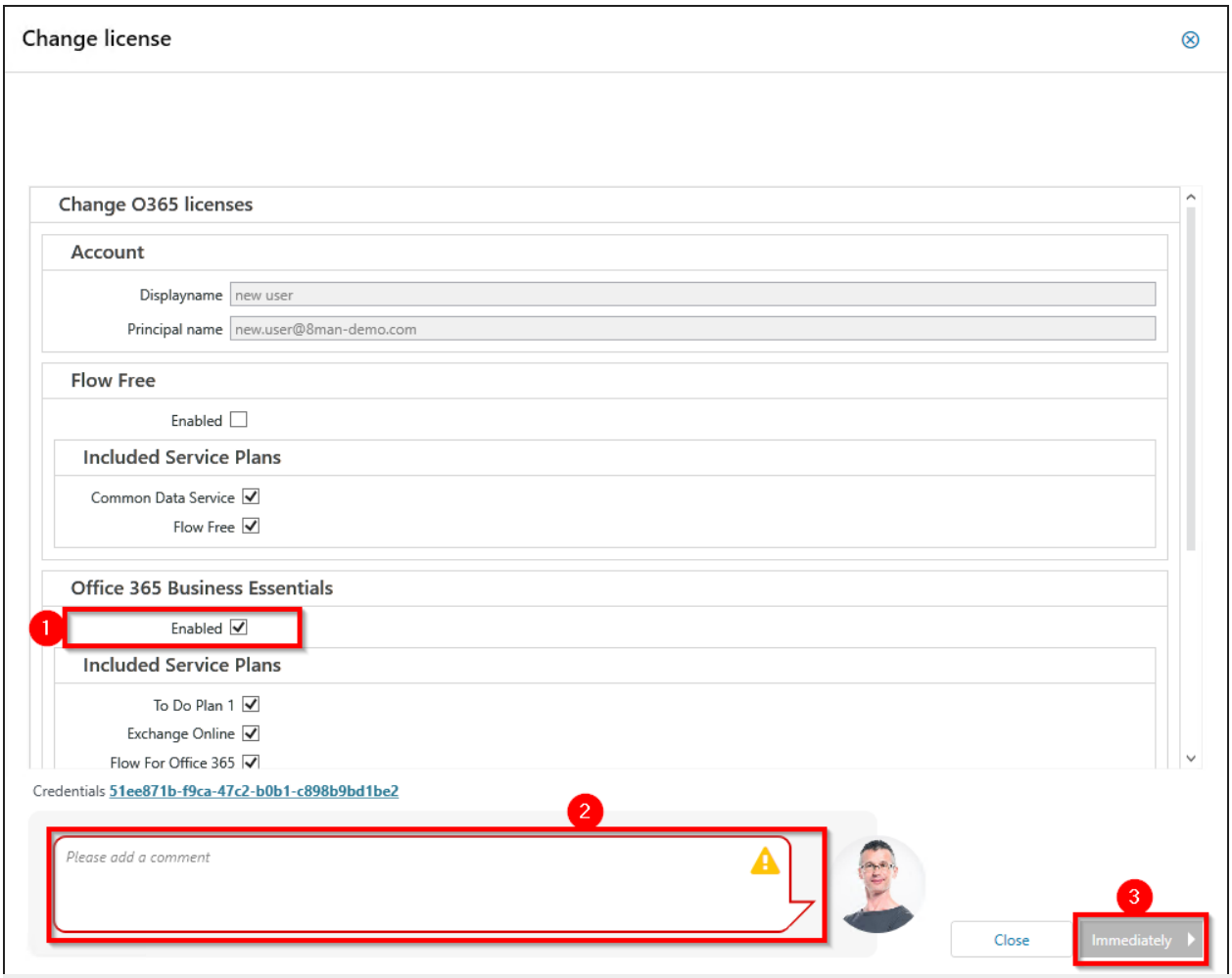


1. Use the search in Accounts view to find the desired user.
2. Find the desired user in the section "Azure AD Accounts".
3. If needed, configure the search options to include Azure AD Accounts in the search results.

You need a configured and scanned Azure AD resource to perform this action. Please see Azure AD scans.



1. Right-click on the desired user tile.
2. Select Change license.



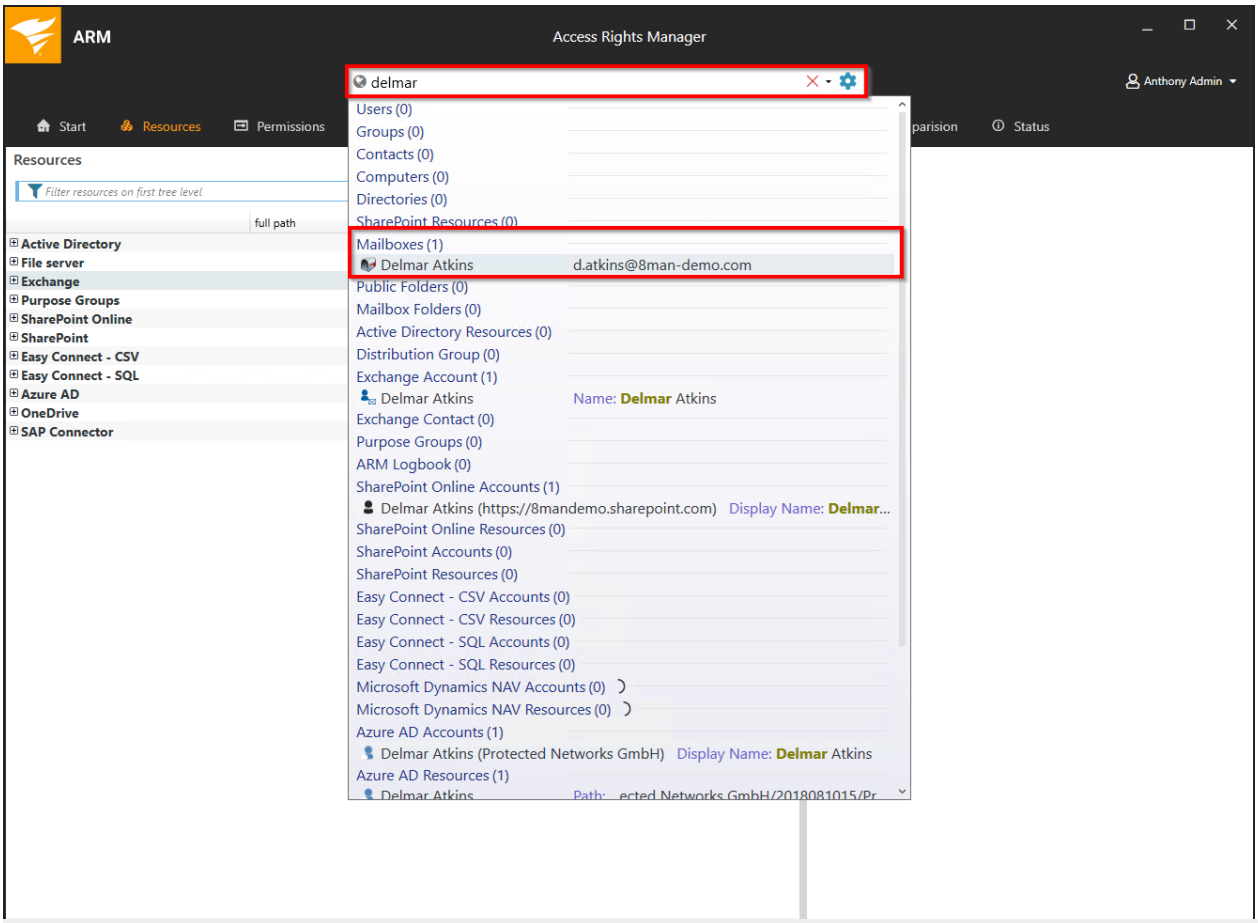
1. Activate a license that includes Exchange Online.
2. You must enter a comment.
3. Start the process.

Change mailbox permissions

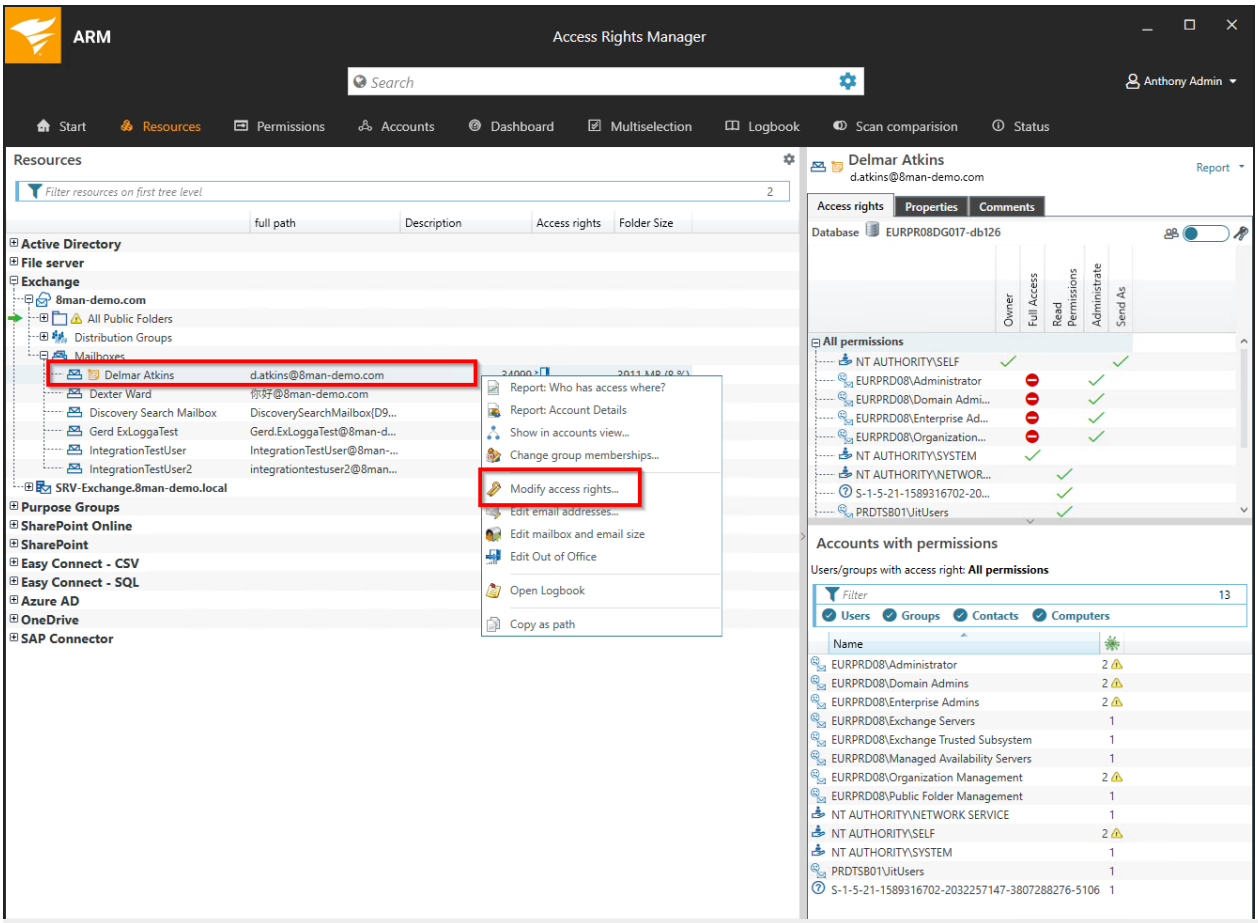
Background / Value

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".

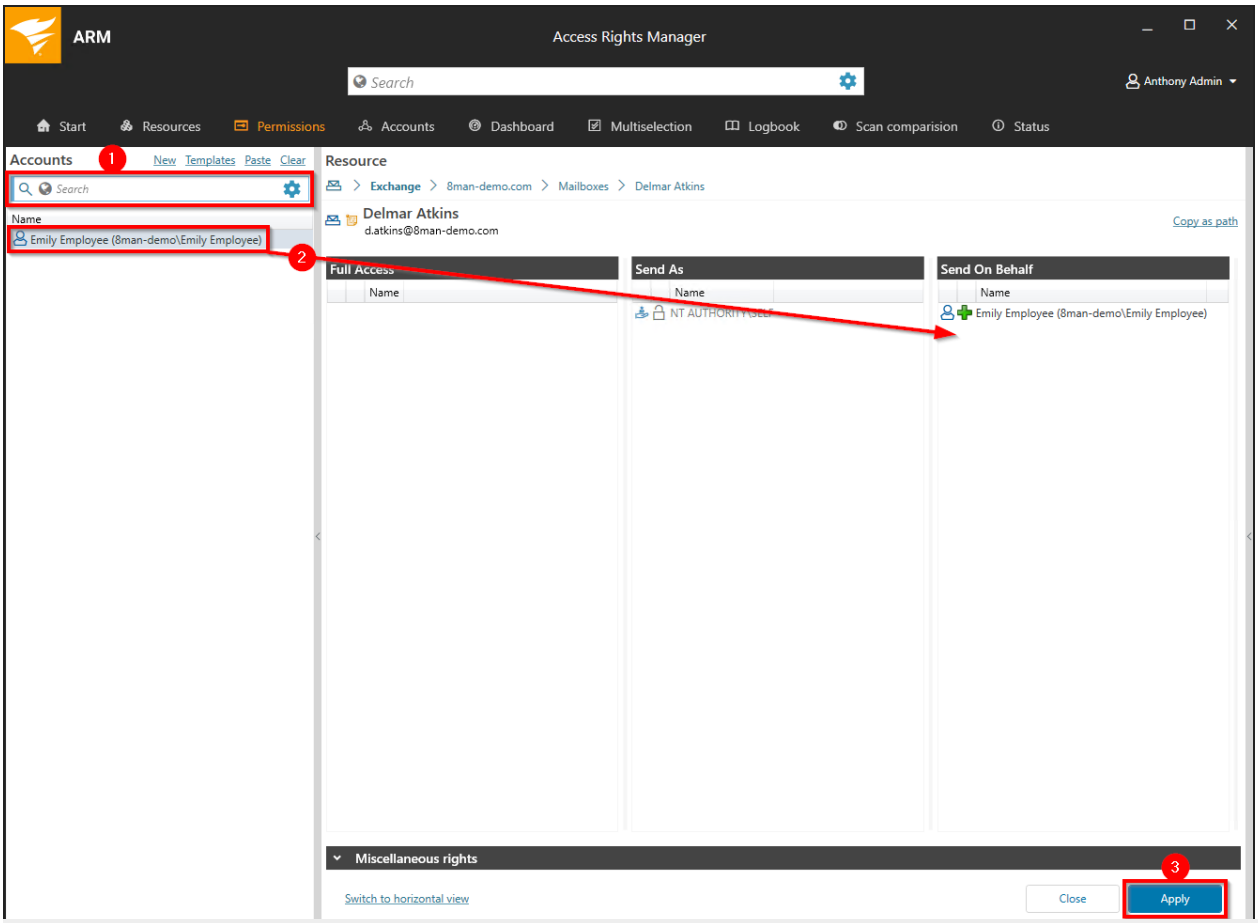
Step-by-step process



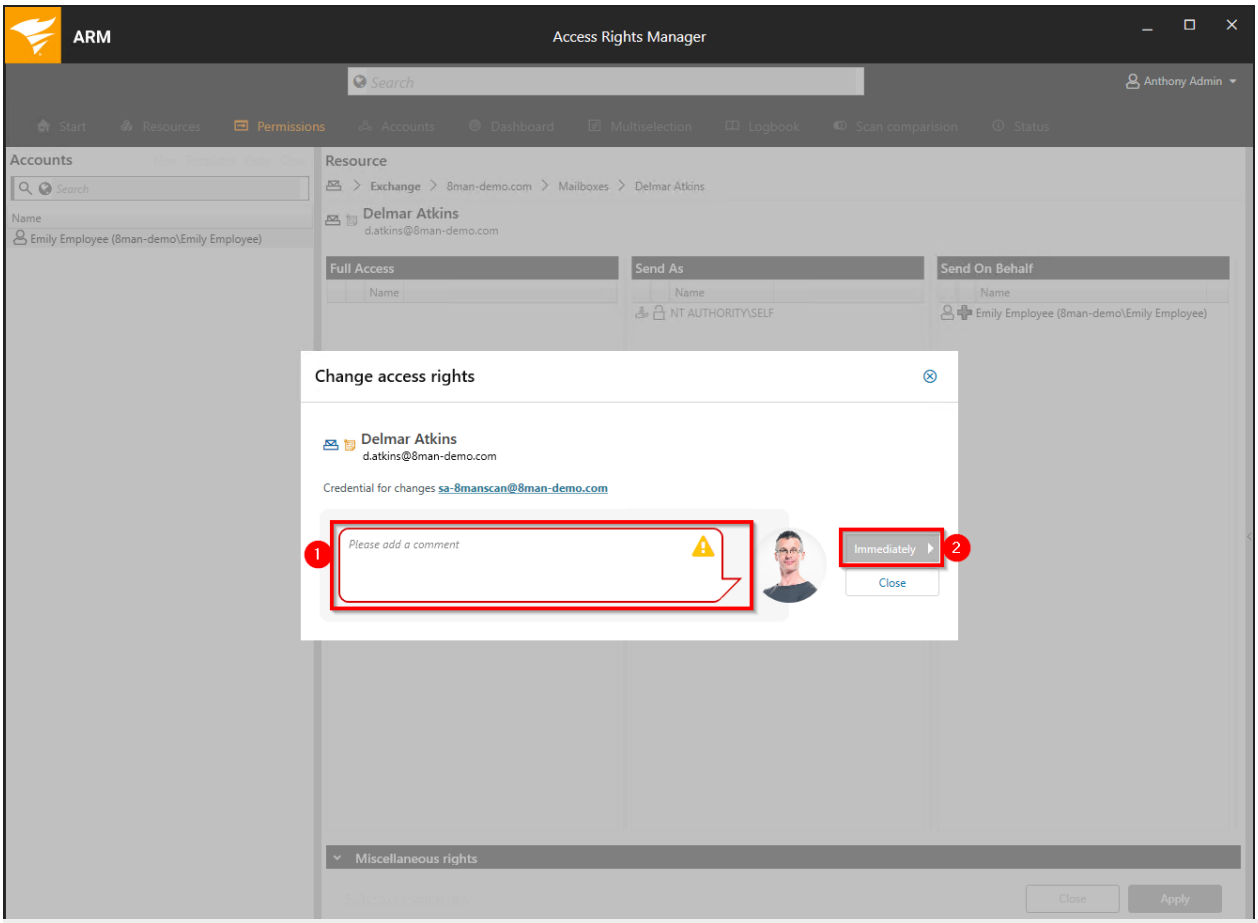
Use the search field to find the desired mailbox.



Right-click on the mailbox and select "Modify access rights" from the context menu.



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".



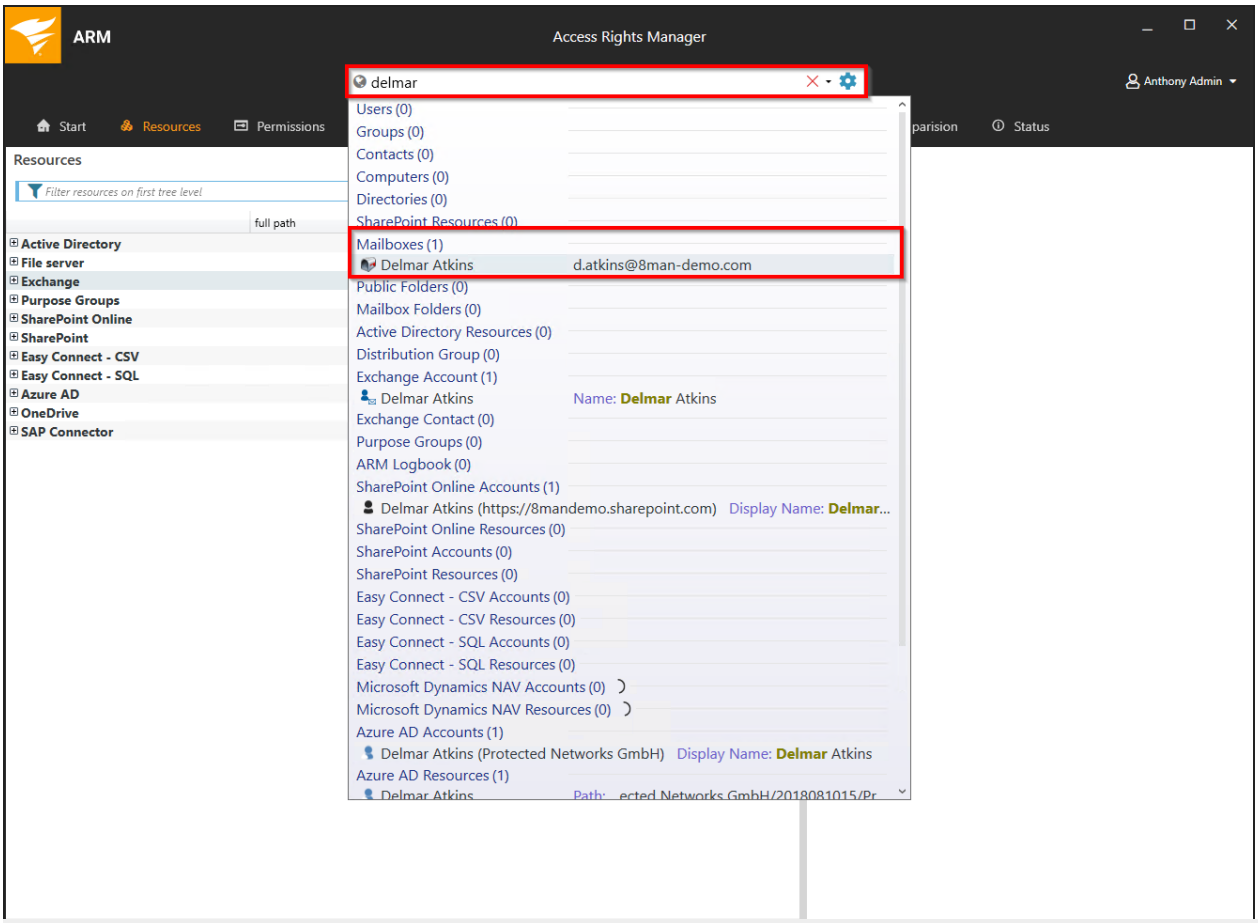
1. You must enter a comment, for example a ticket number.
2. Start the process.

Manage out of office notices

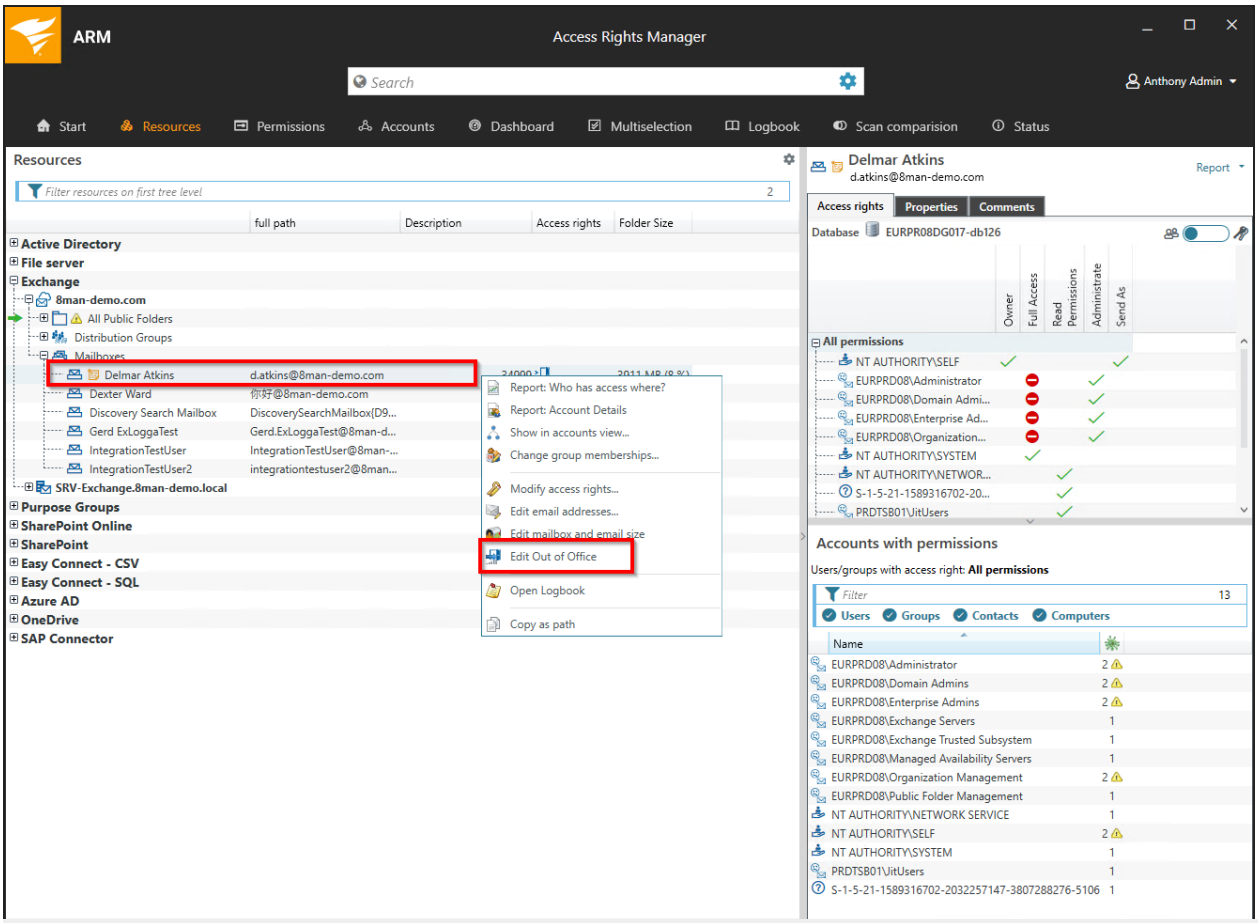
Background / Value

ARM allows help desk to set out of office notices for employees without gaining access to email content.

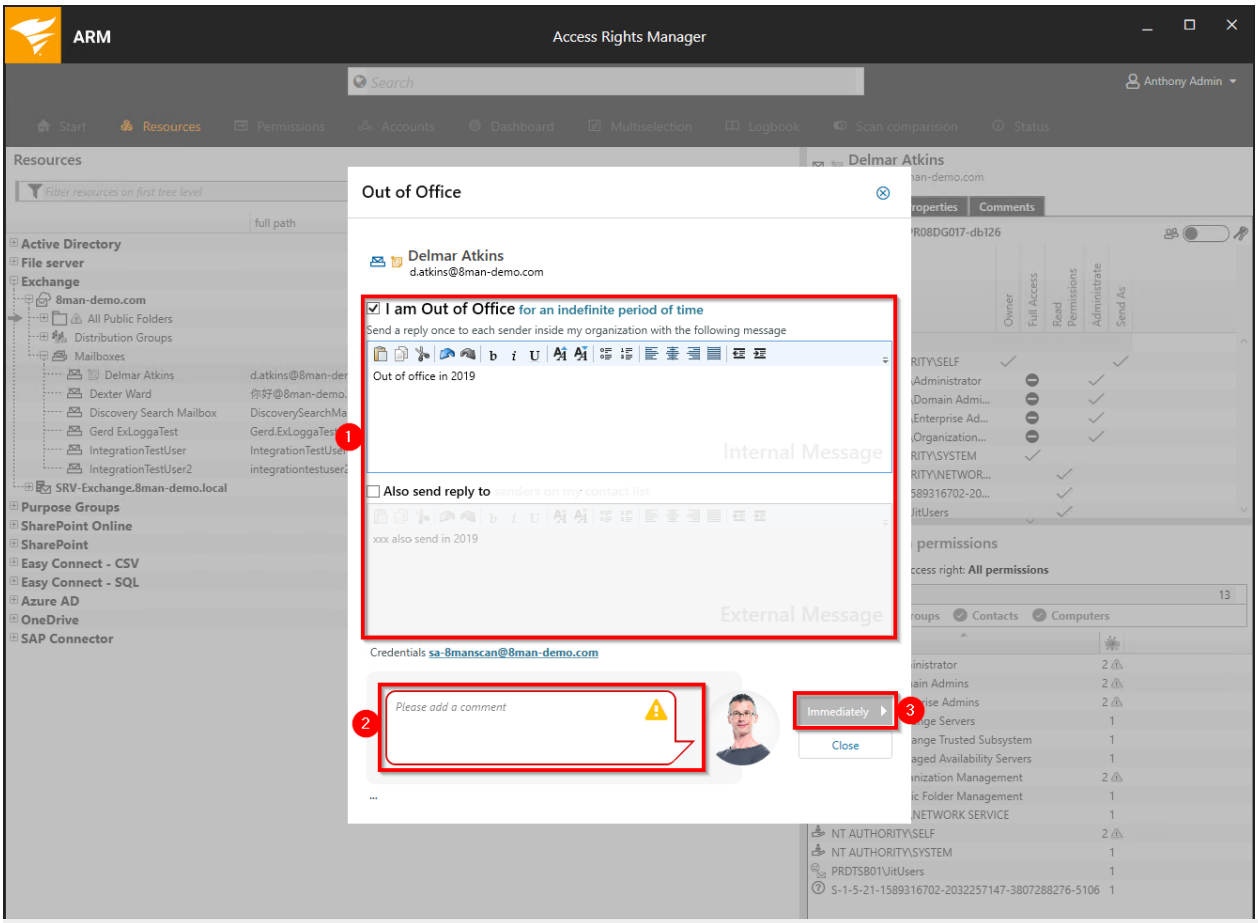
Step-by-step process



Use the search field to find the desired mailbox.



Right-click on the mailbox and select "Edit Out of Office" from the context menu.



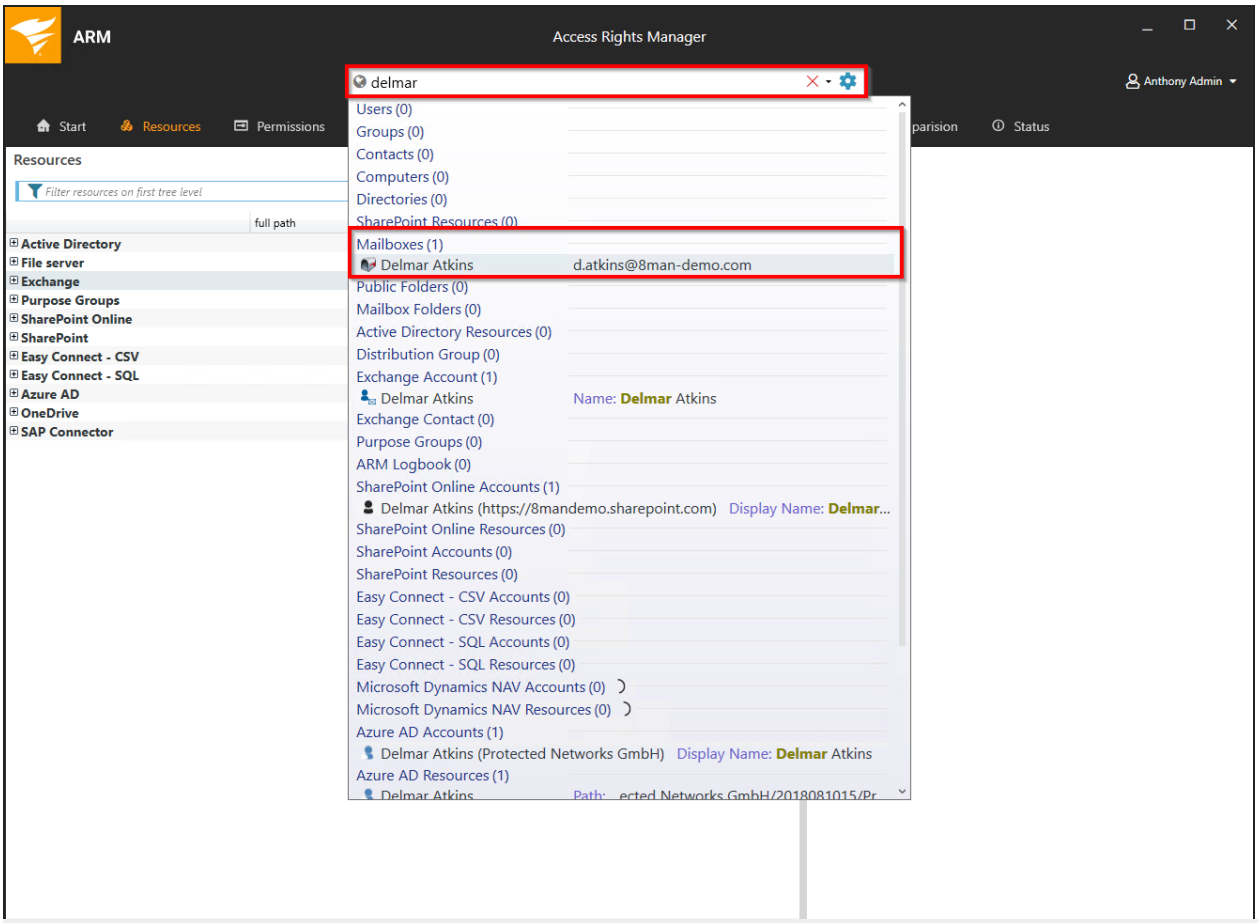
1. Determine the out of office settings.
2. You must enter a comment, for example a ticket number.
3. Start the process.

Manage mailbox and email size

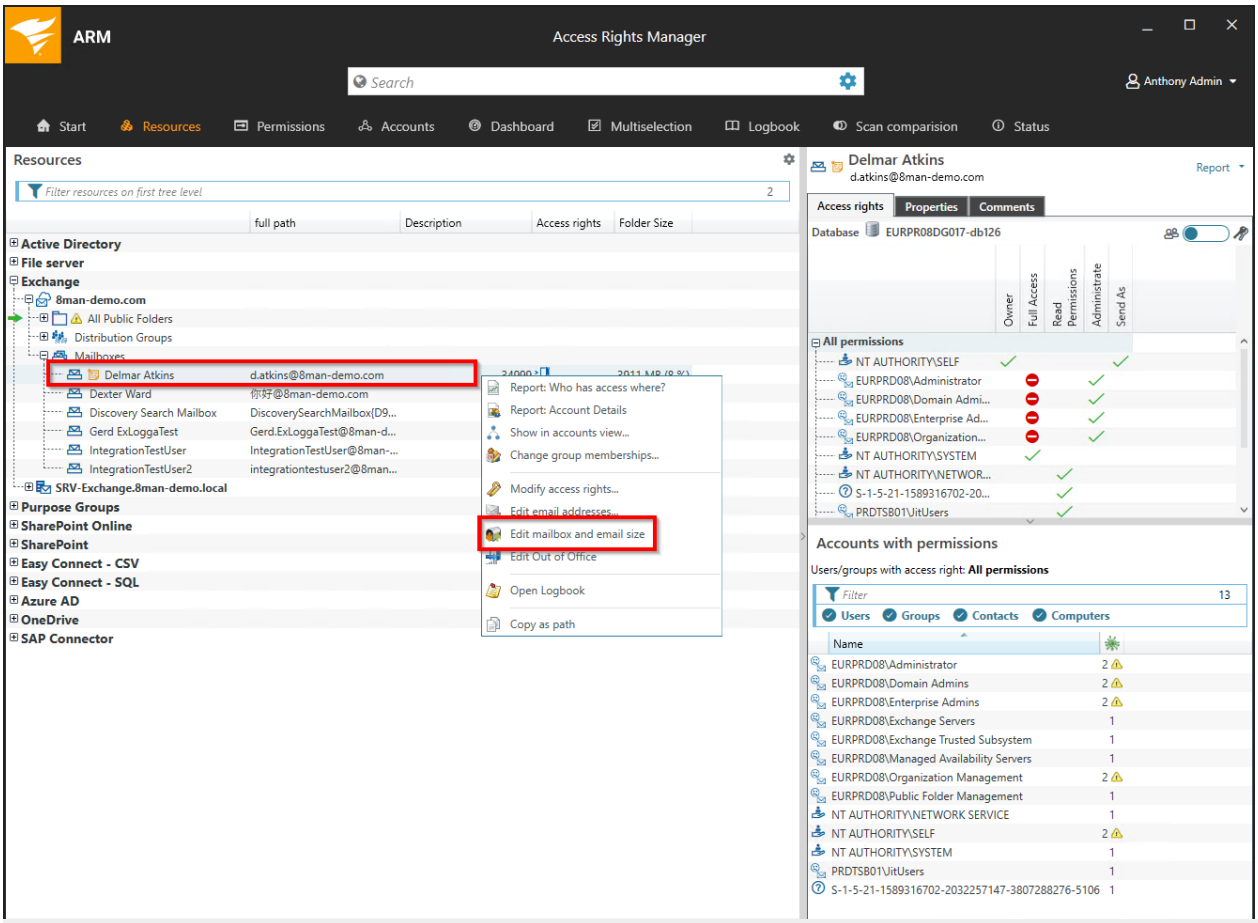
Background / Value

Managing mailbox size is a common task for help desk. ARM allows you to make these quickly and efficiently.

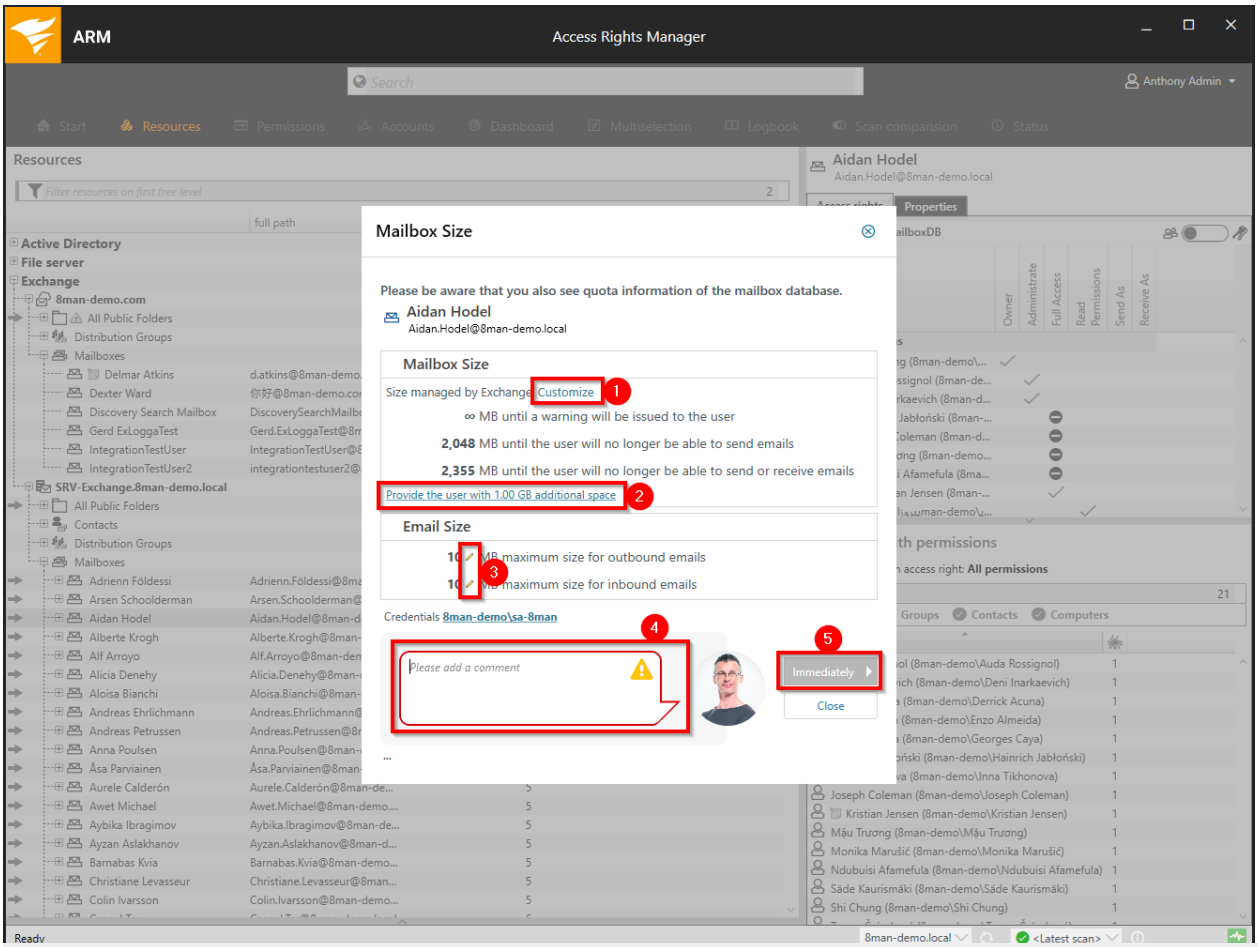
Step-by-step process



Use the search field to find the desired mailbox.



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 massages 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.

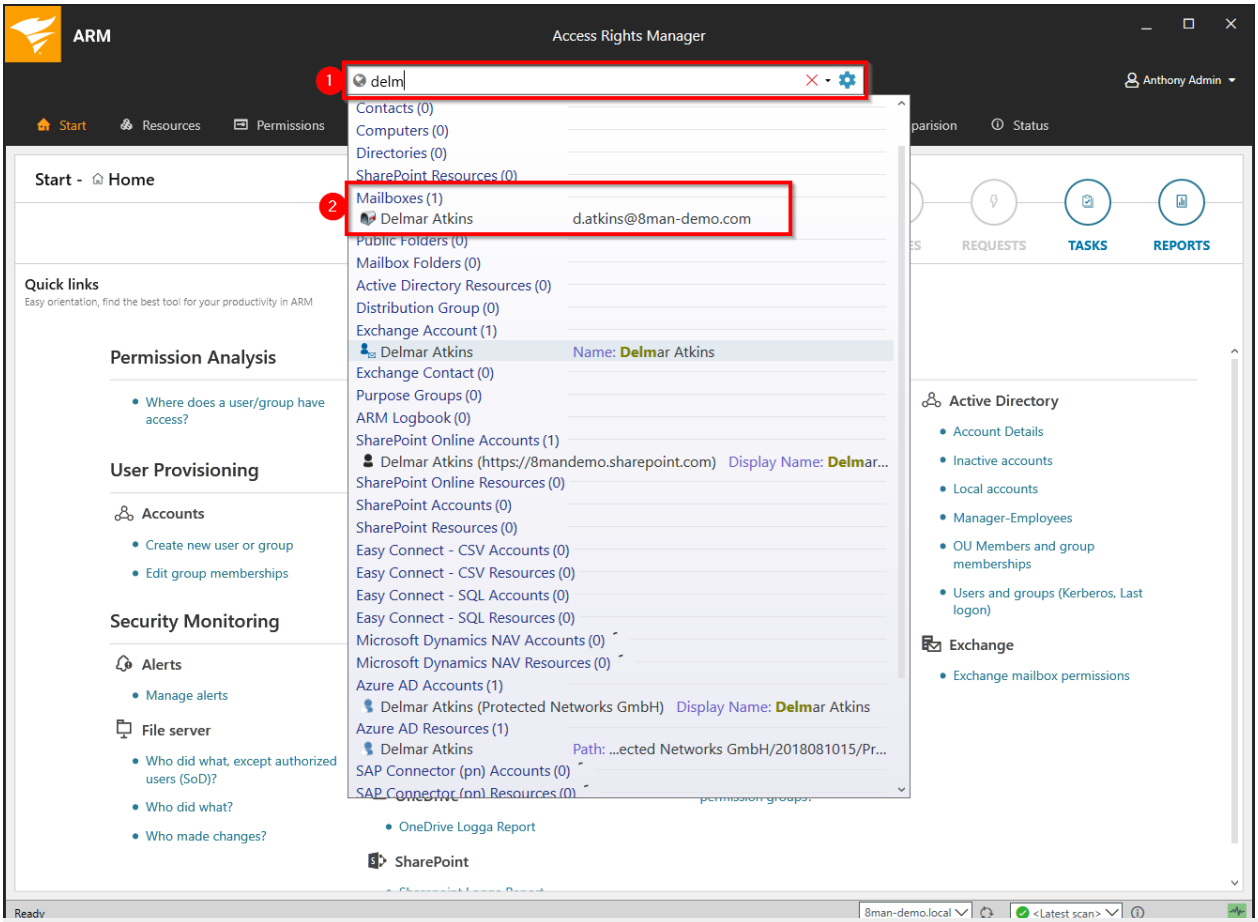
Manage email addresses

Background / Value

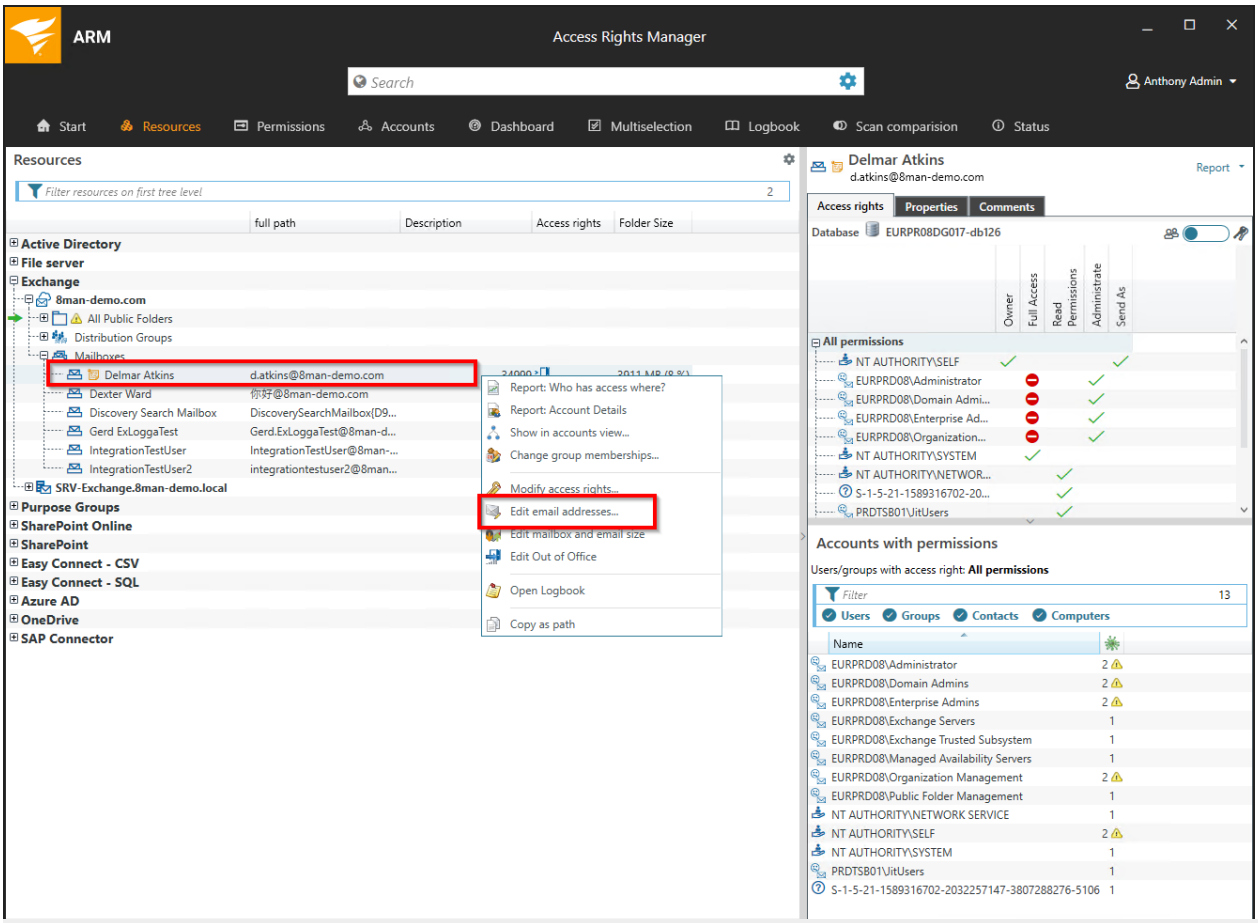
With ARM you can assign and remove multiple email addresses to mailboxes, distribution groups and contacts.

The process is documented automatically.

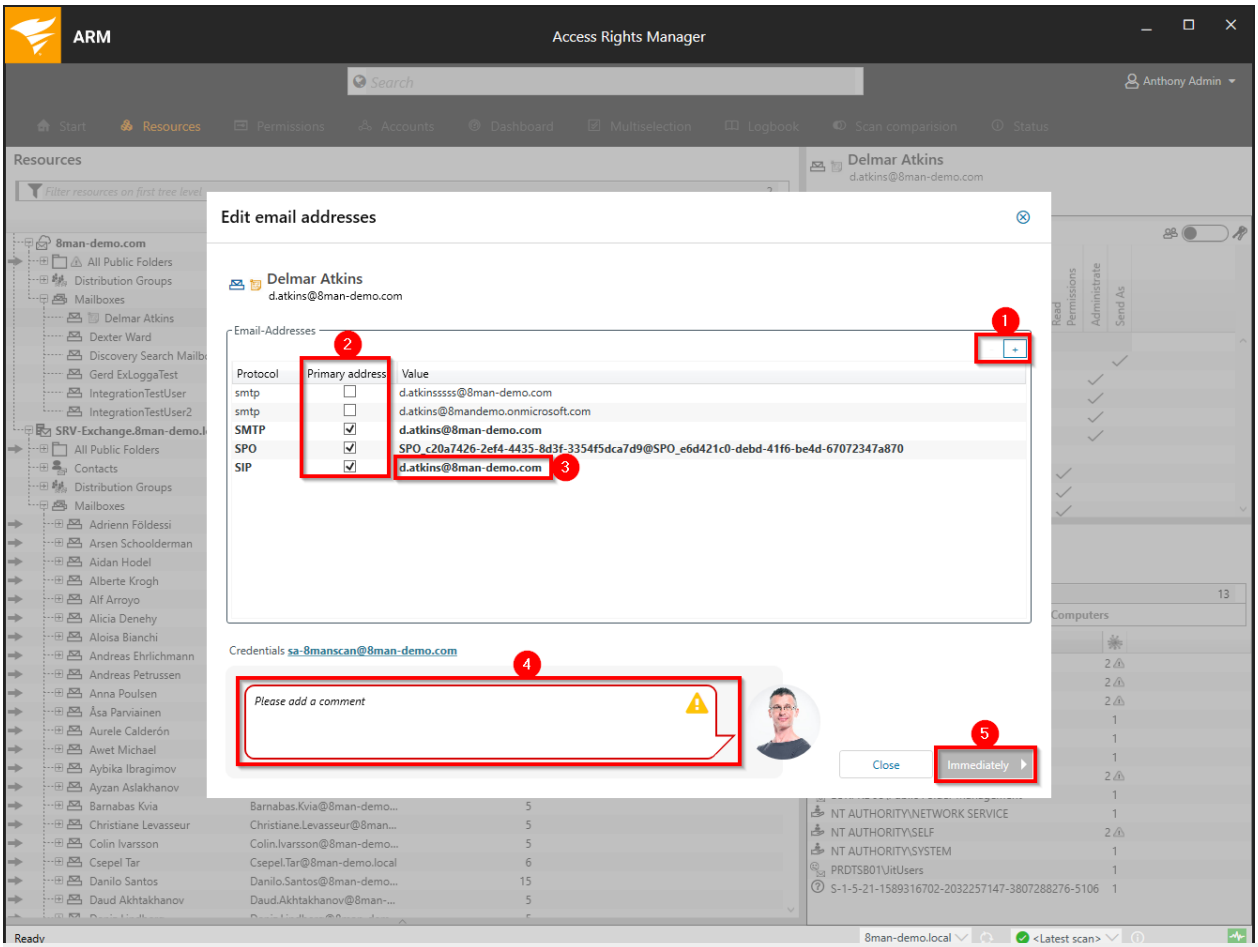
Step-by-step process



Use the search field to find the desired mailbox.



Right-click on the Mailbox and select "Edit email addresses" from the context menu.



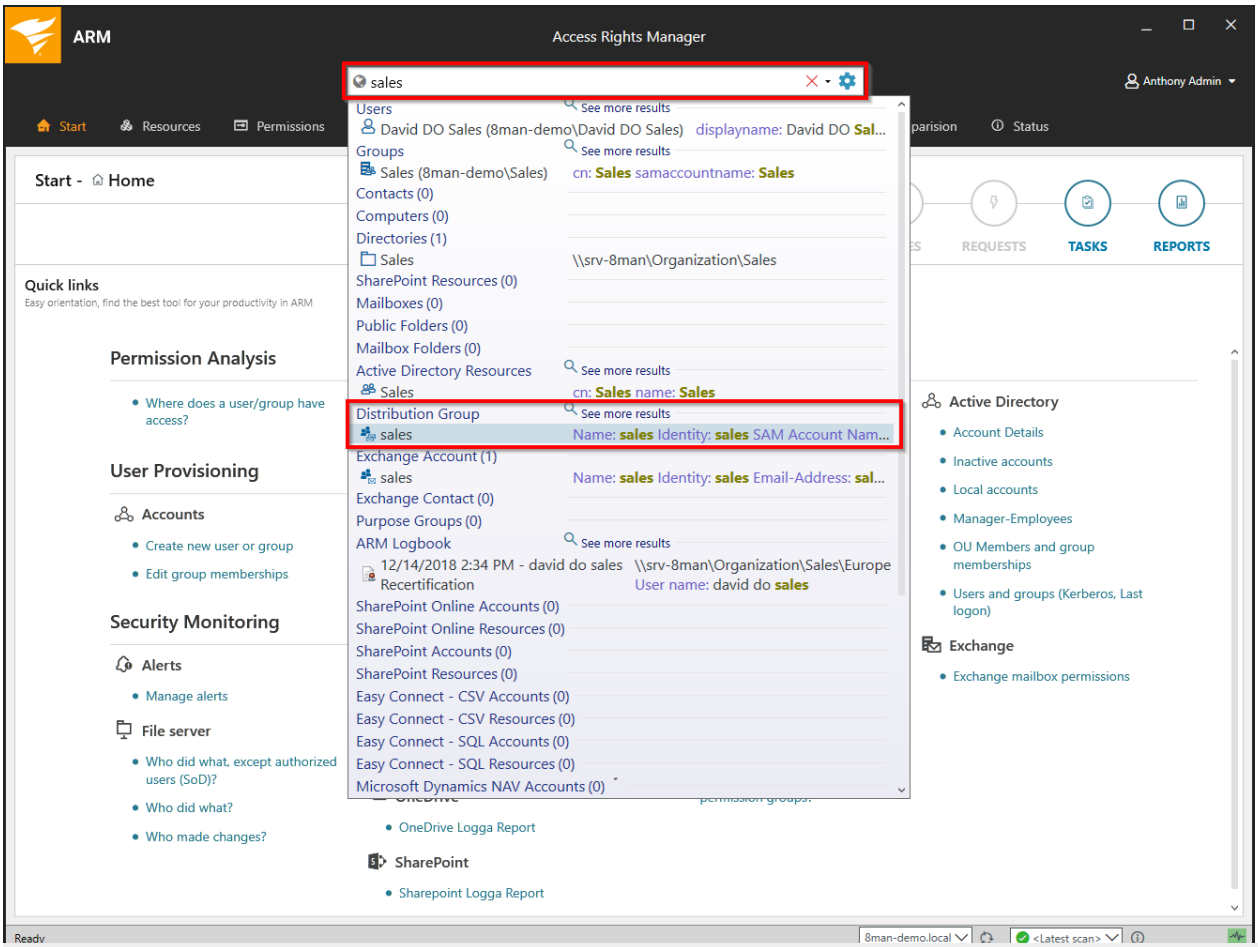
1. Add an email address or delete an existing one.
2. Set the primary address.
3. Double-click the field where you want to enter or change the address.
4. You must enter a comment, for example the ticket number.
5. Start the process.

Manage distribution group memberships

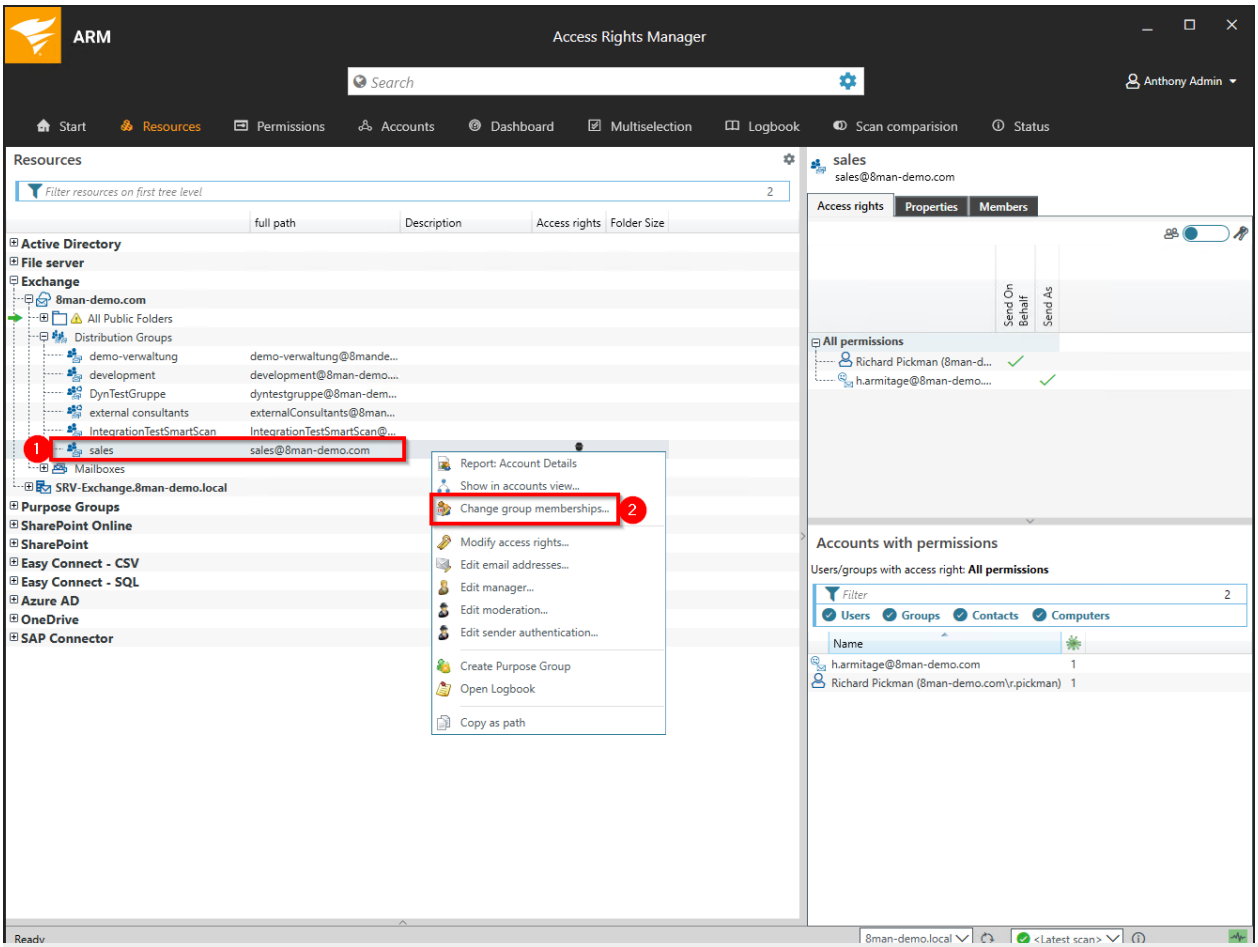
Background / Value

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.

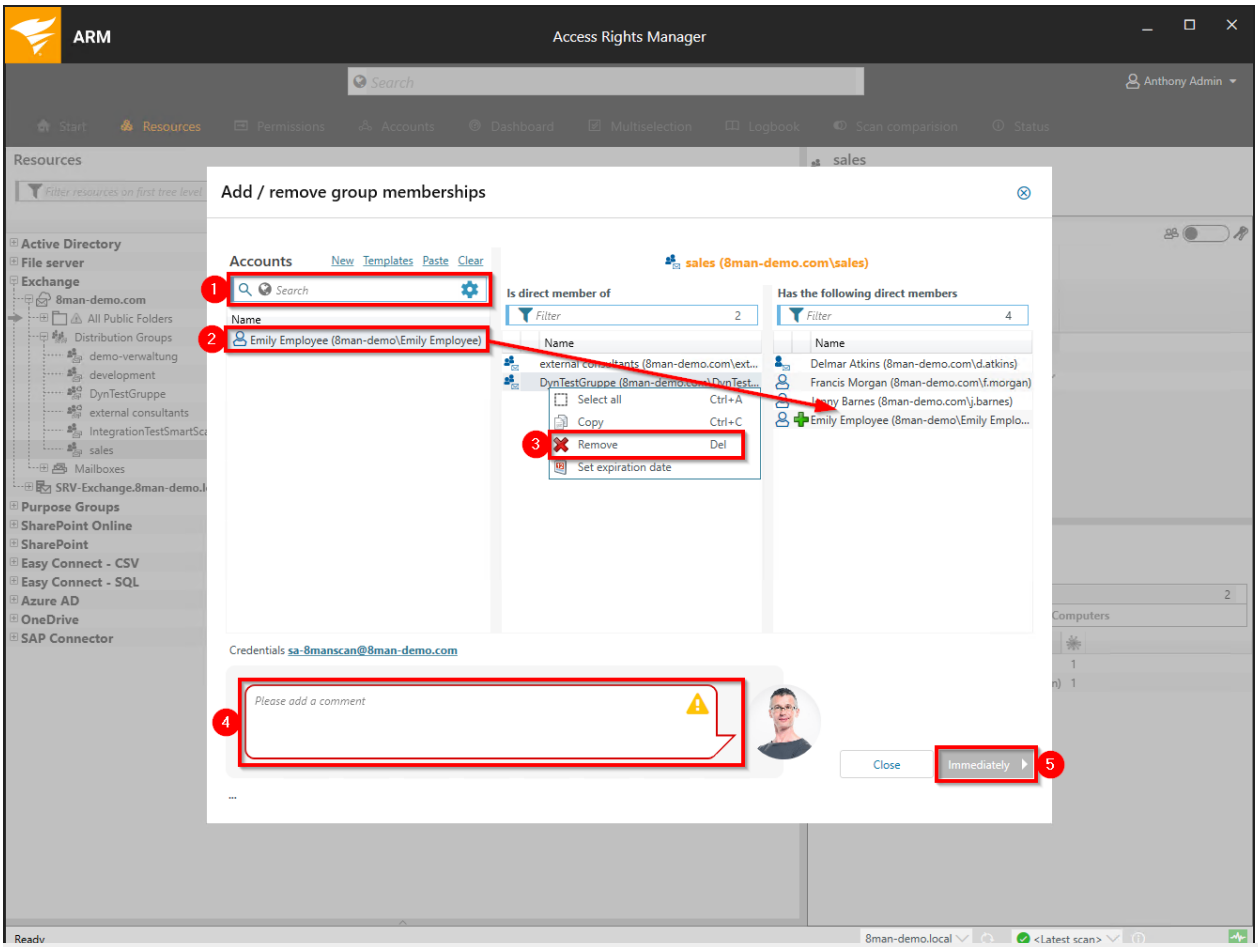
Step-by-Step process



Use the search field to find the desired distribution group.



1. ARM focuses on the desired group.
2. Right-click on the group and select "Change group memberships".



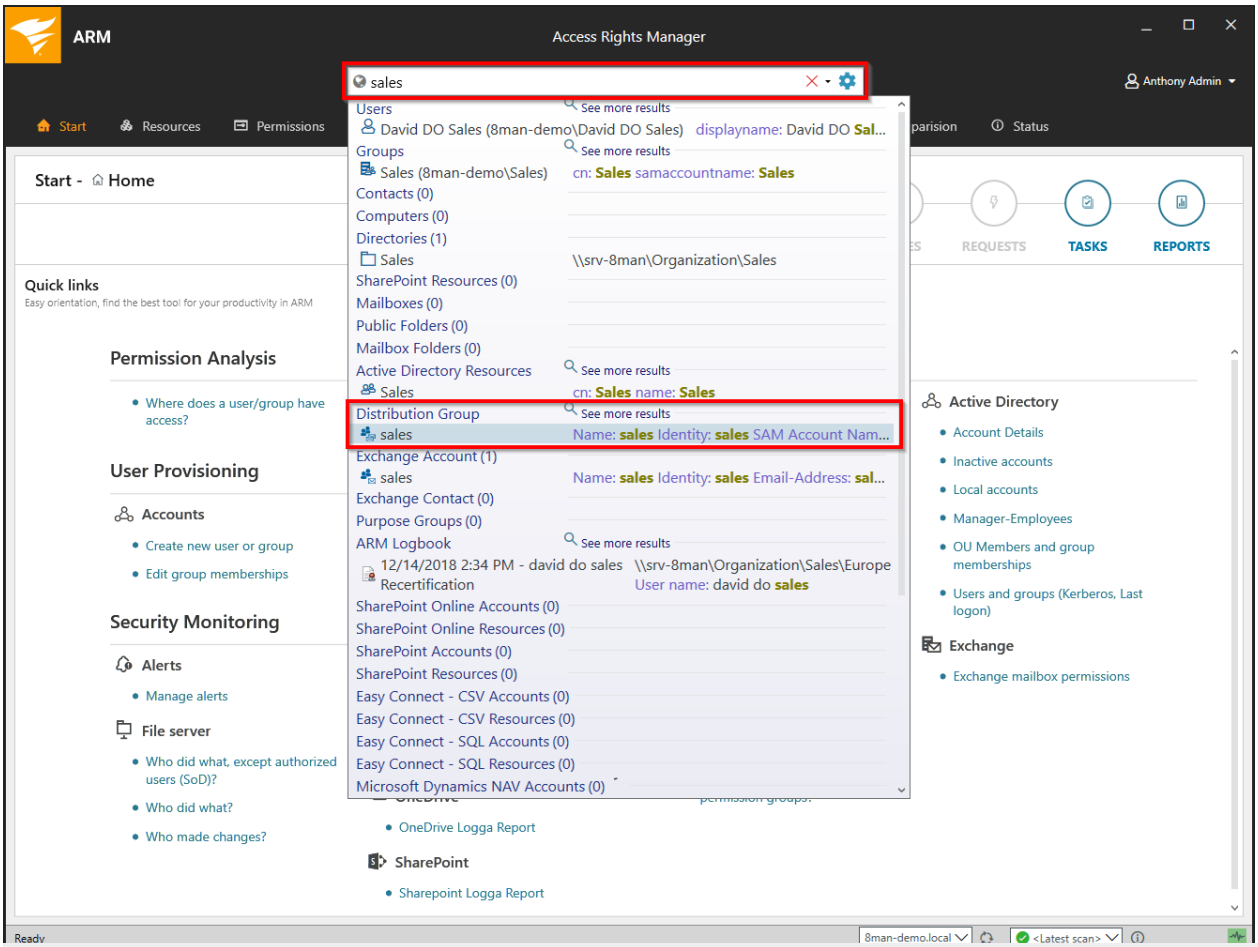
1. Use the search to find the desired account.
2. Use drag & drop to move the account to a column, to assign a group membership.
3. To remove a membership use right-click and then select "Remove" from the context menu.
4. You must enter a comment, for example a ticket number.
5. Start the process.

Manage distribution group permissions

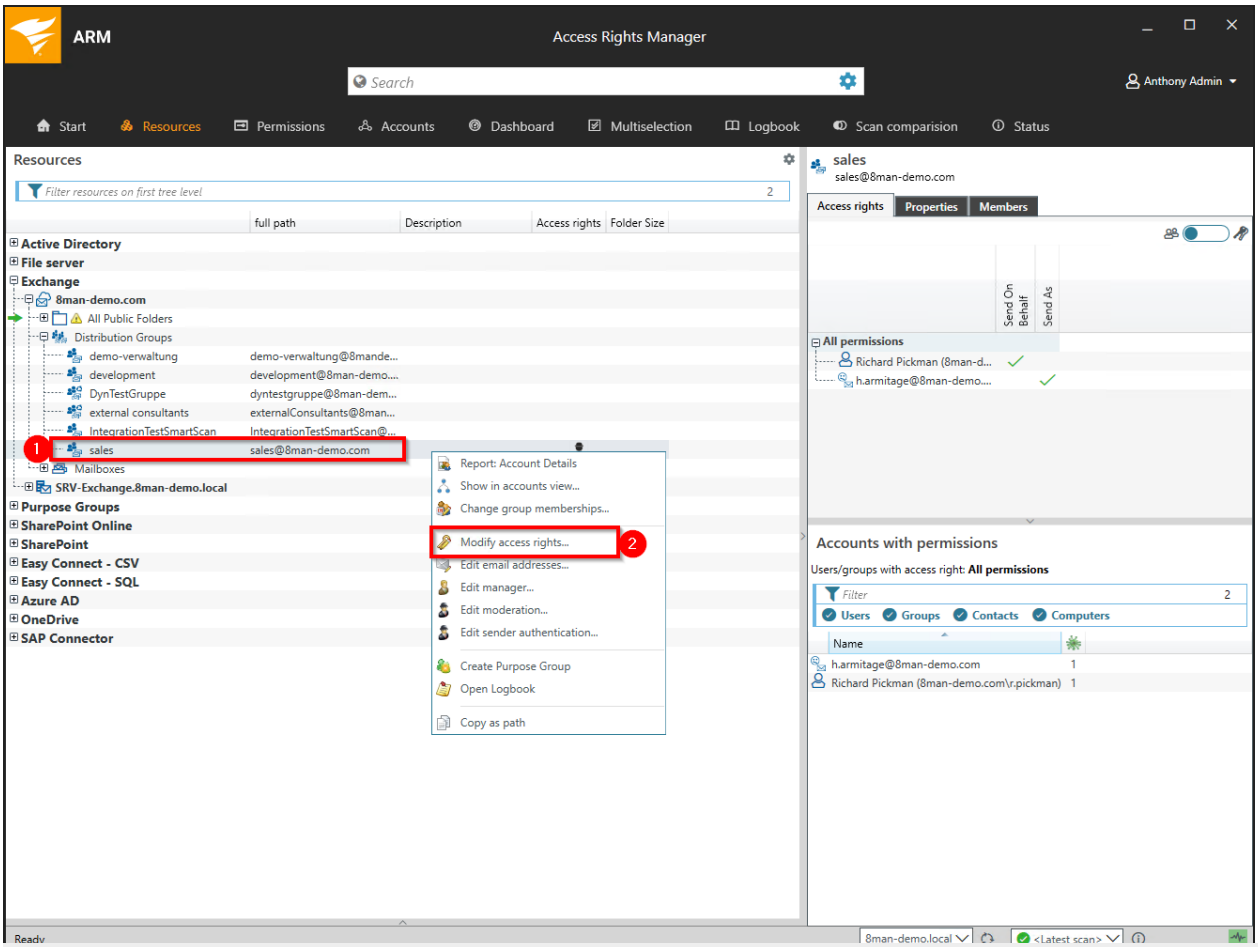
Background / Value

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.

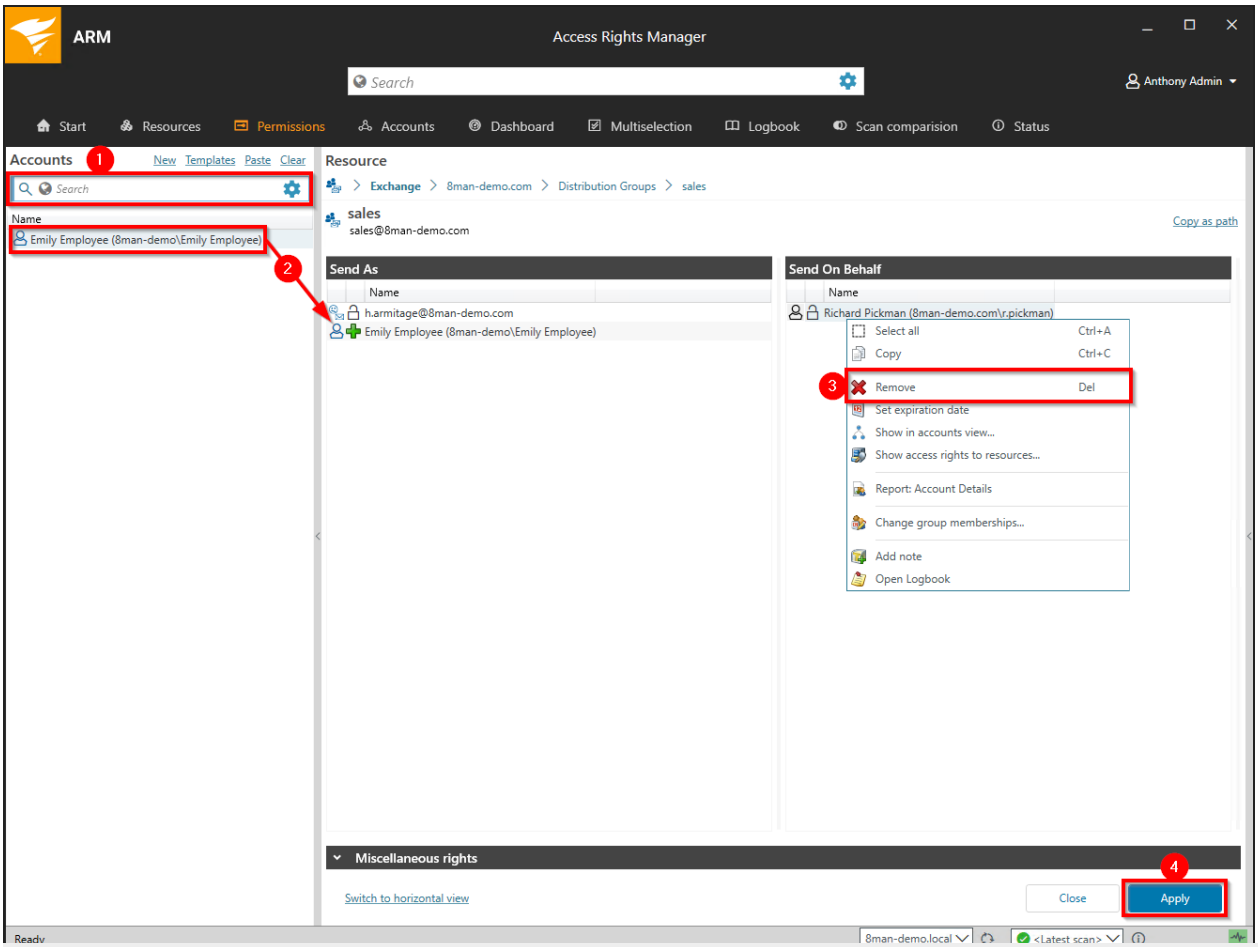
Step-by-step process



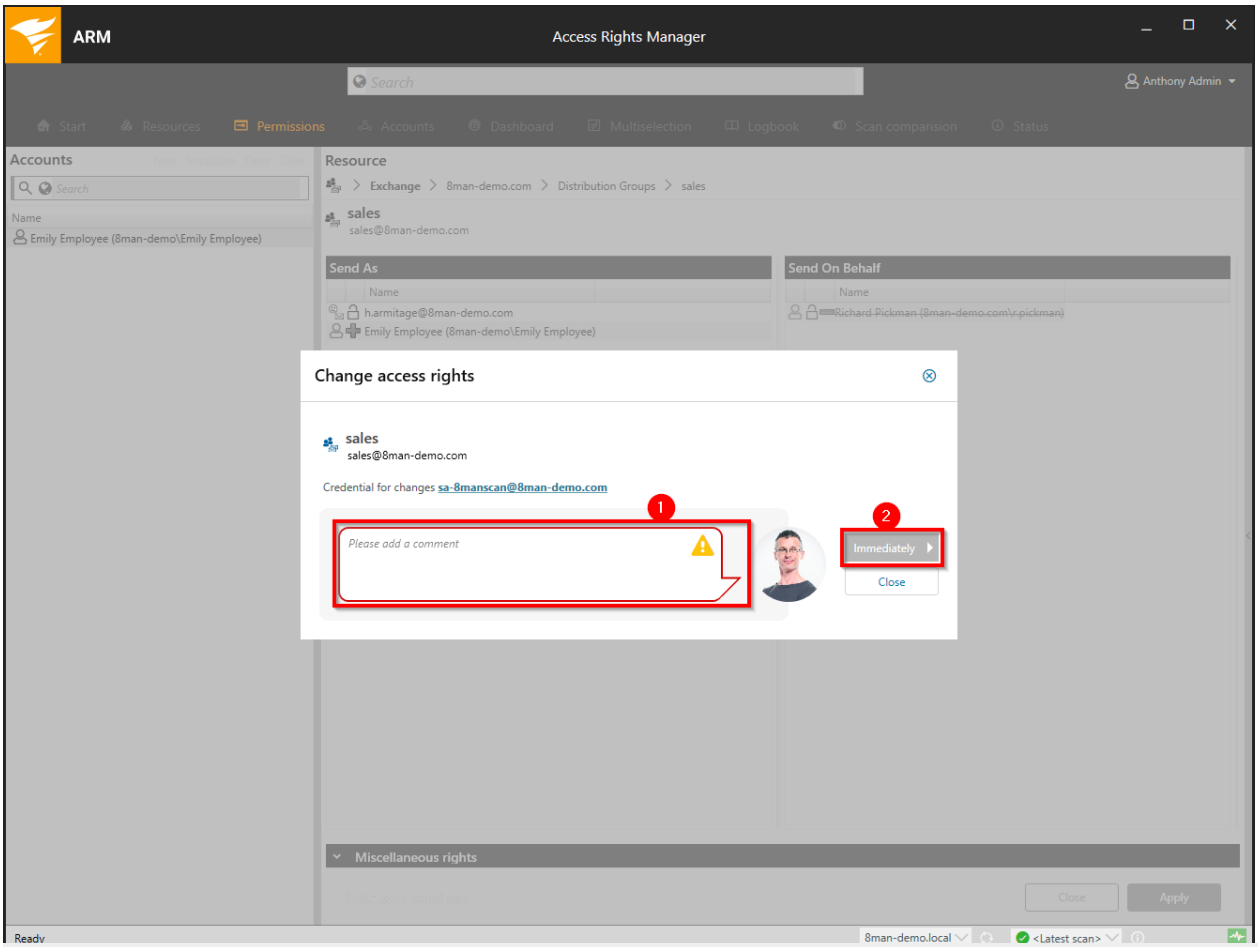
Use the search field to find the desired mailing list.



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.

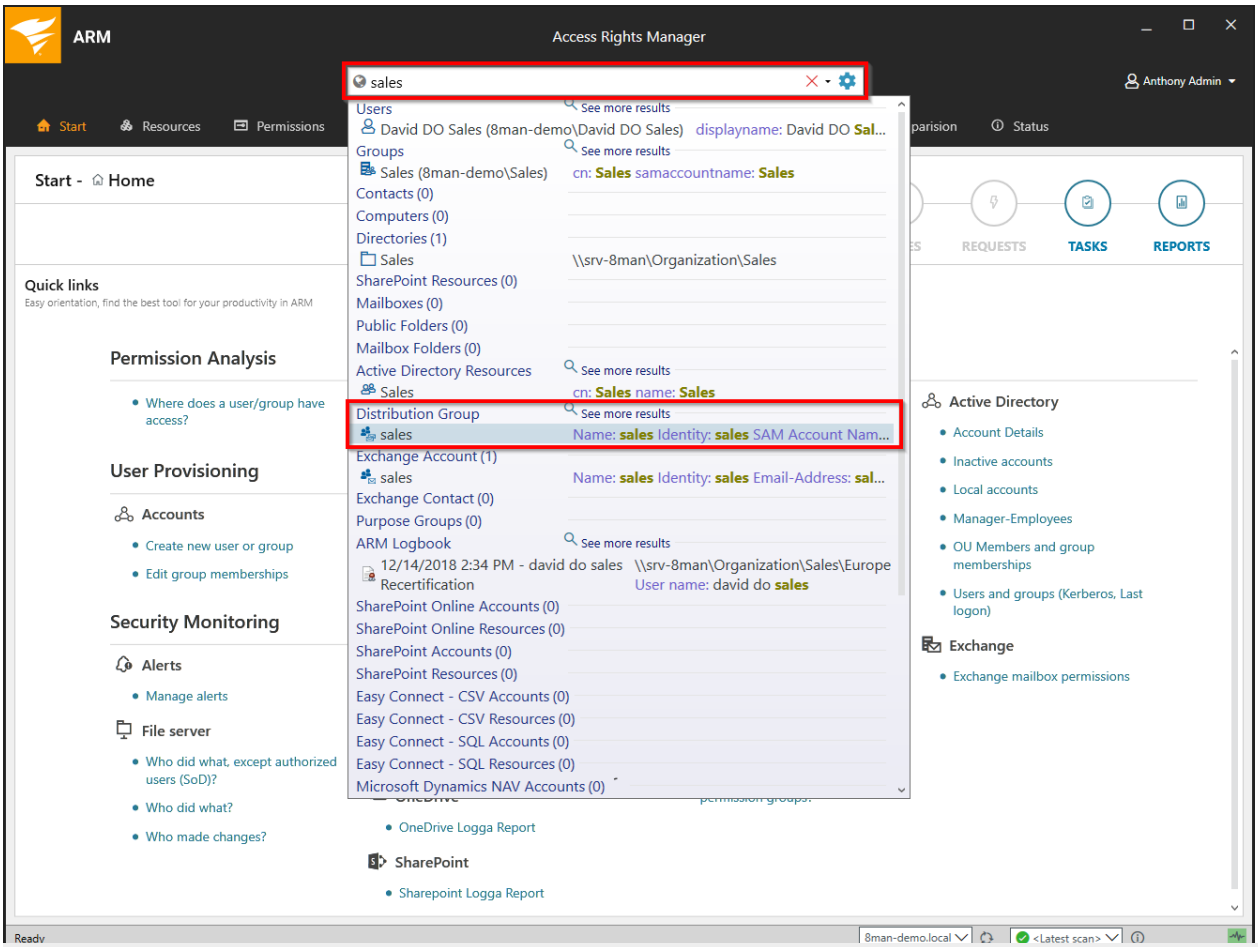
If no moderators are nominated the role is filled out by the manager of the group.

ⓘ The change also works for dynamic Exchange groups.

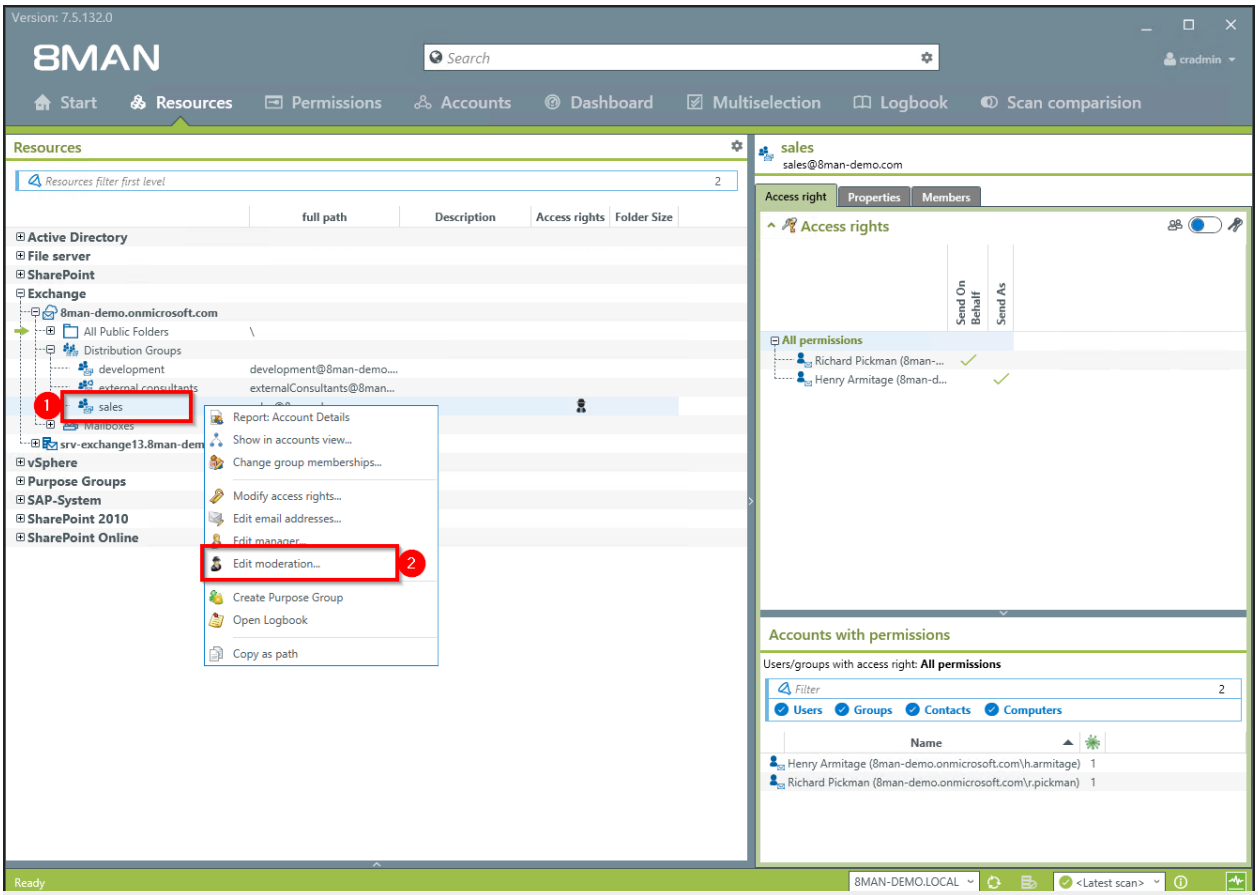
Related features

Change the manager of distribution groups

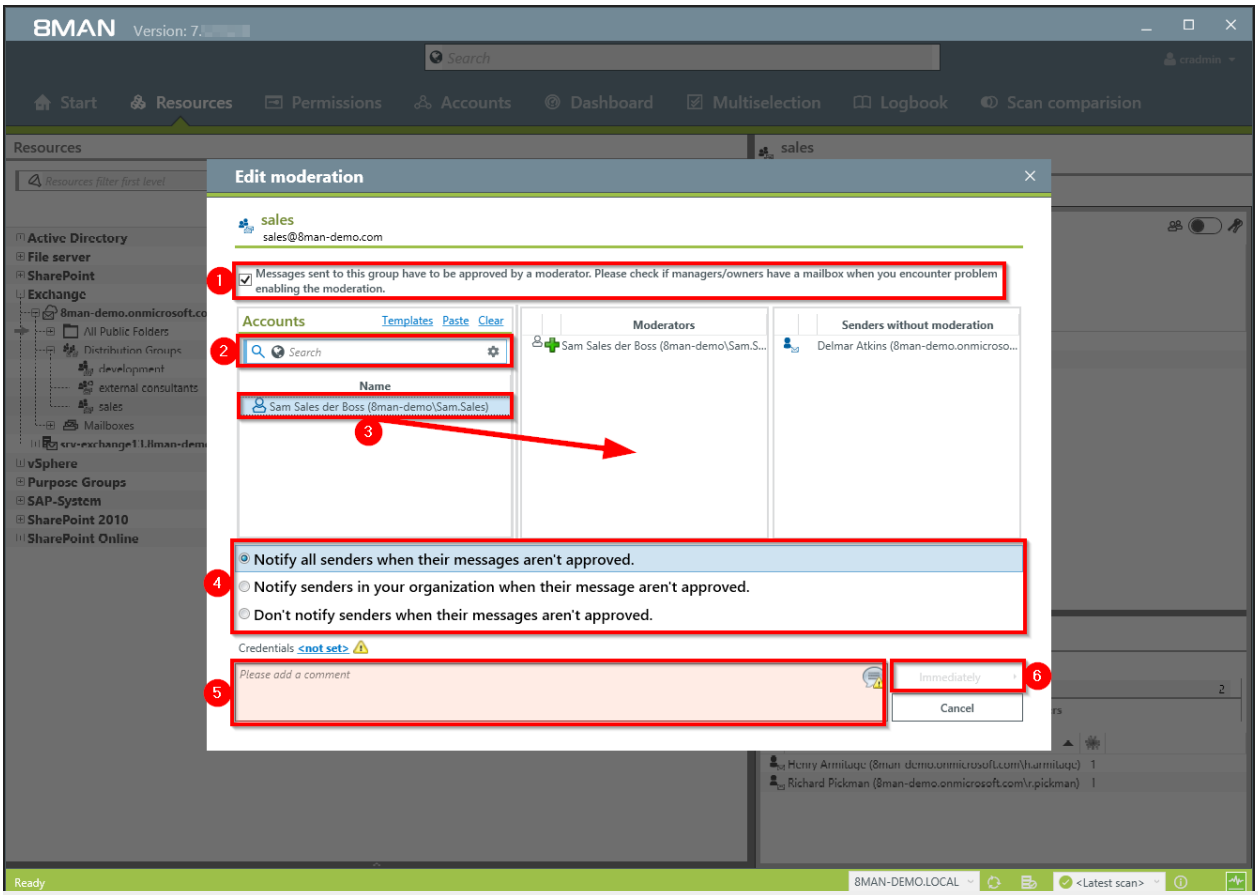
Step-by-step process



Use the search field to find the desired distribution group.



1. You are focusing in the desired group.
2. Right-click on a group and select "Edit moderation".



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.

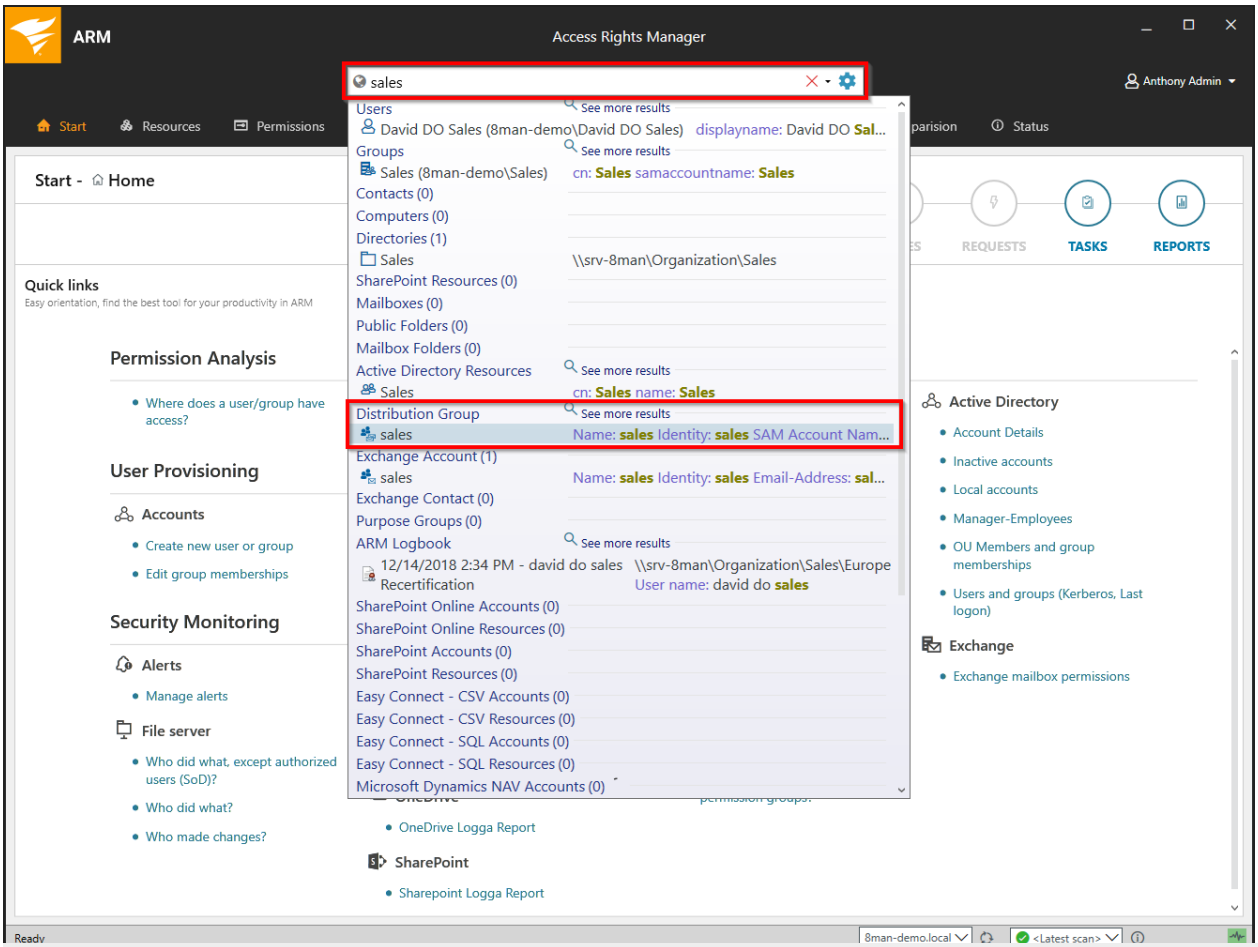
The change also works for dynamic Exchange groups.

Related features

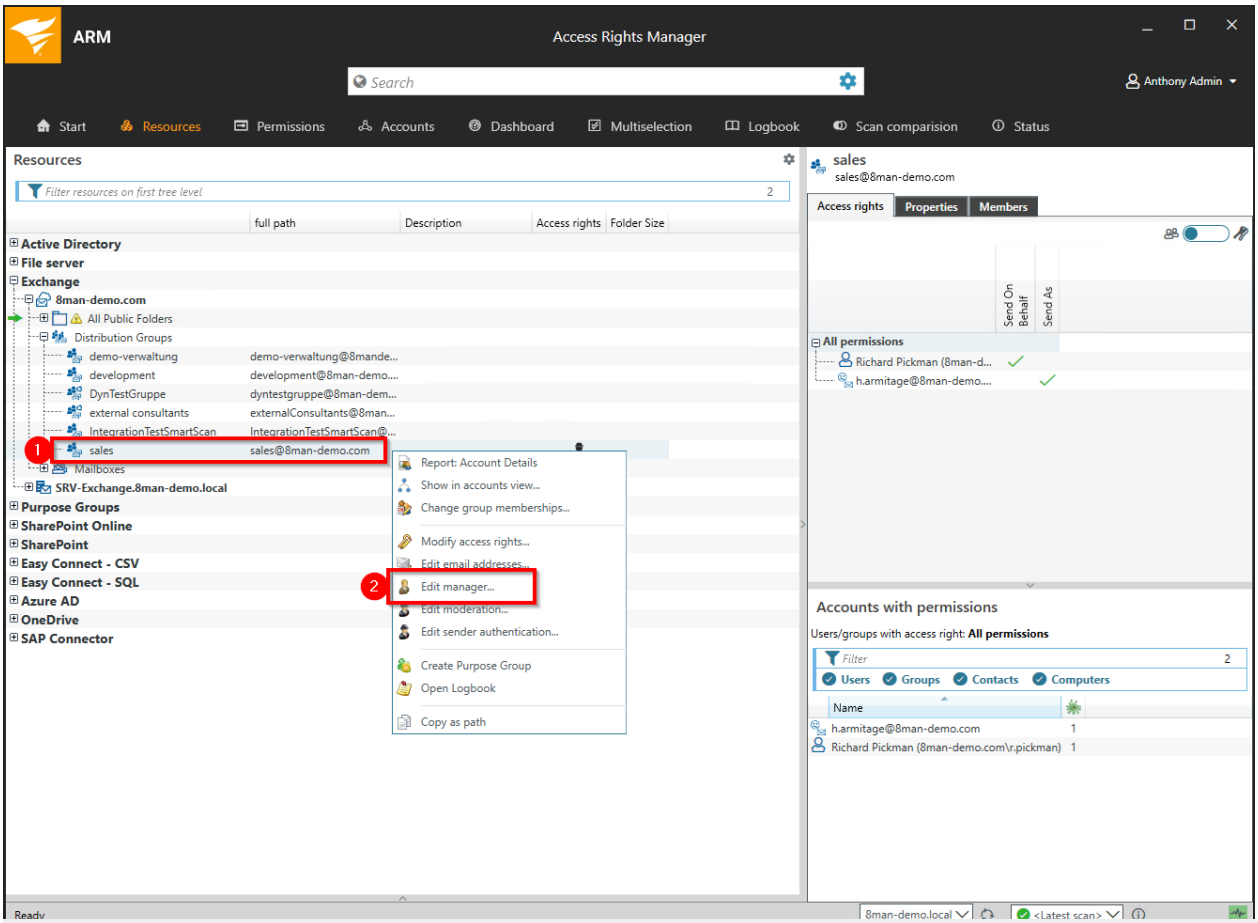
Manage distribution group memberships

Modify moderation of distribution groups

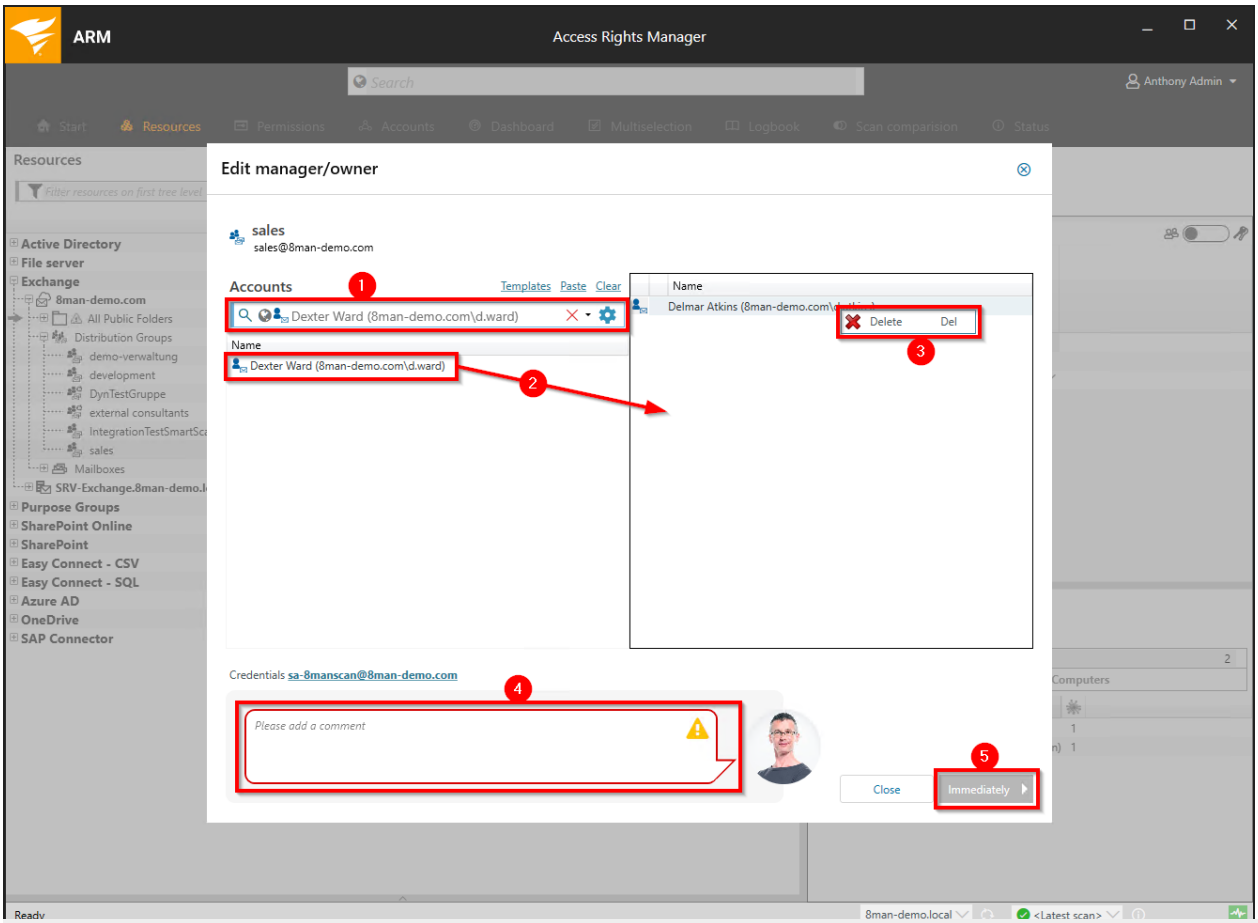
Step-by-step process



Use the search field to find the desired distribution group.



1. ARM expands the tree and focuses on the desired group.
2. Right-click on the group and select "Edit manager...".



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.

ARM provides a sample template for the creation of contacts. You must customize this template before you can use it. See Customize ARM templates.

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

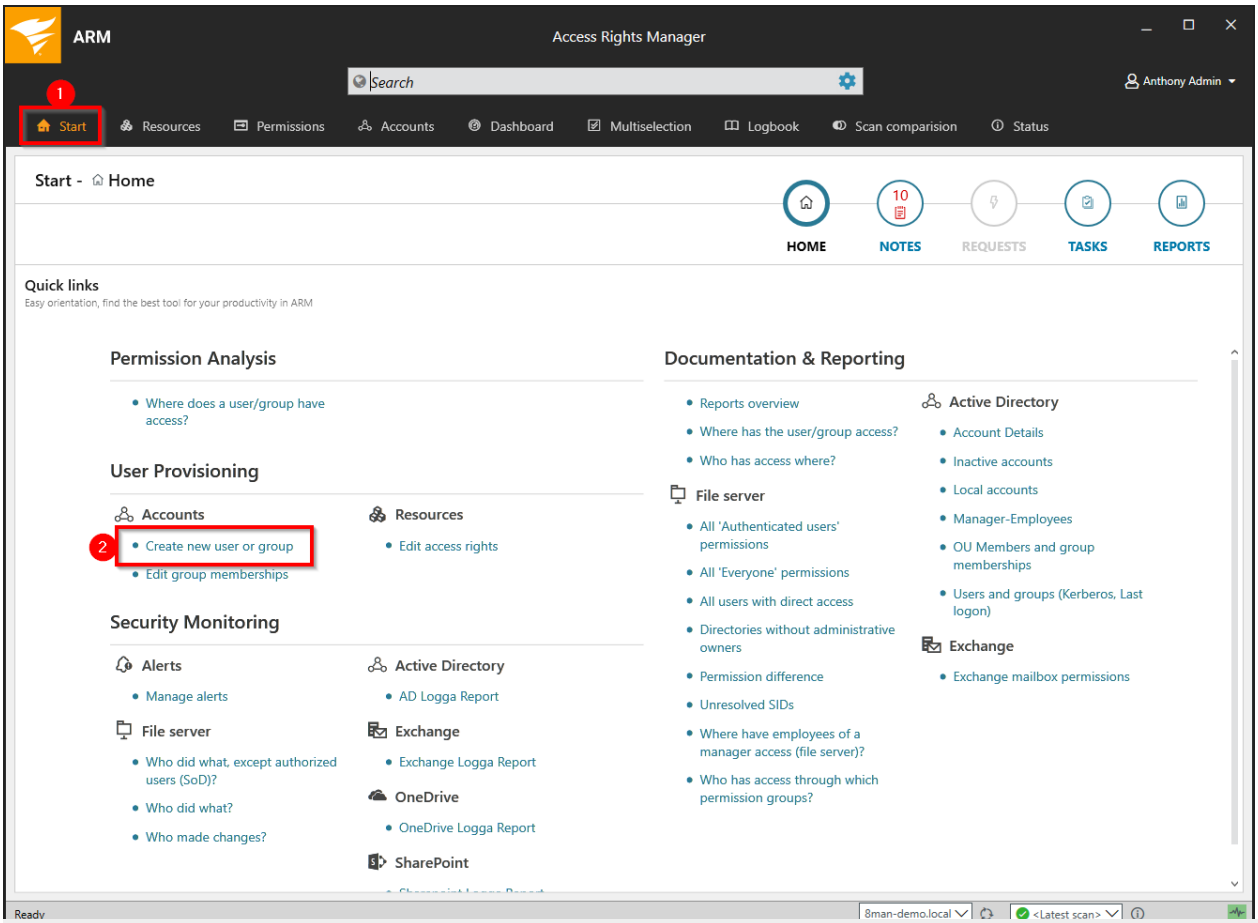
Background / Value

SharePoint groups can exist separately from Active Directory on a SharePoint server. With ARM you can easily create new SharePoint groups.

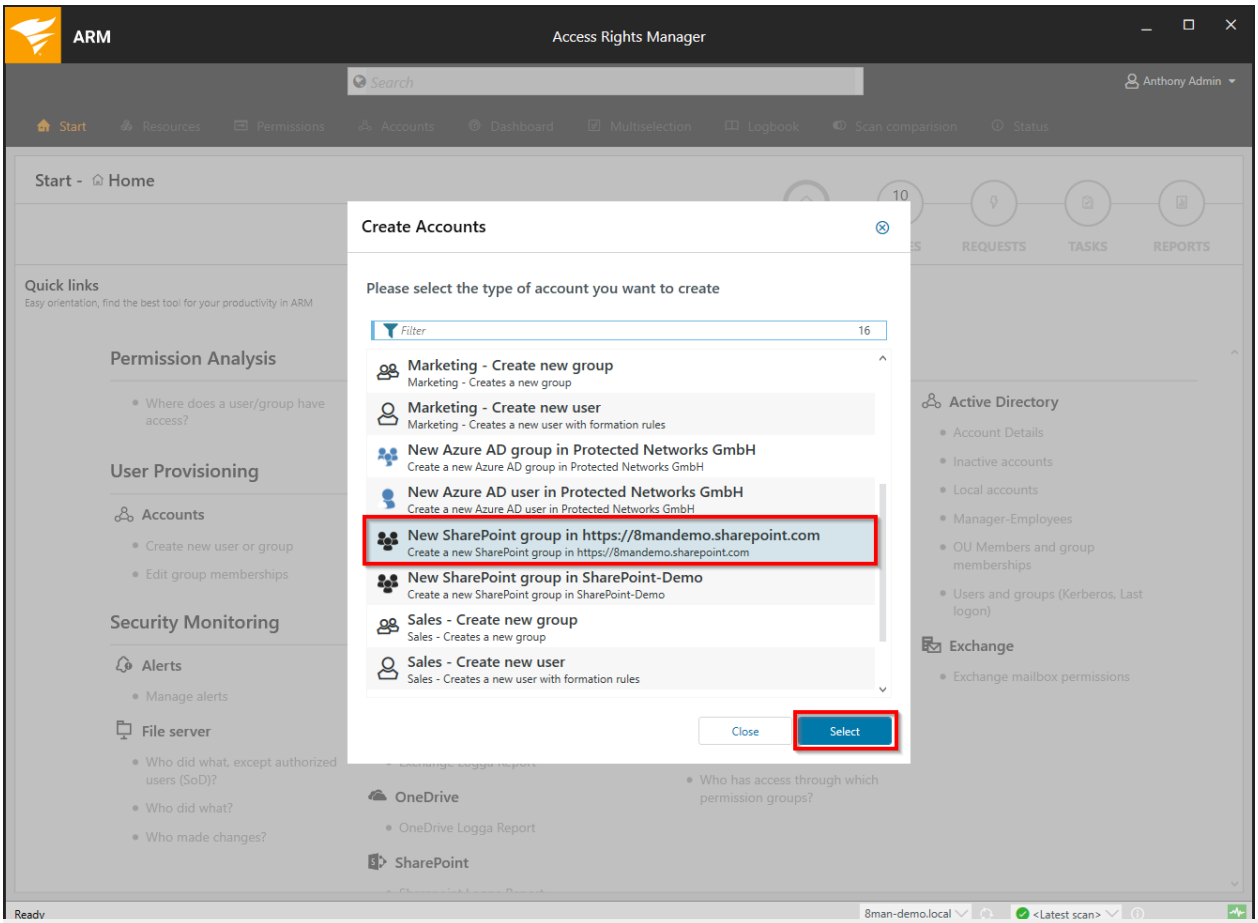
Related features

Manage SharePoint permissions

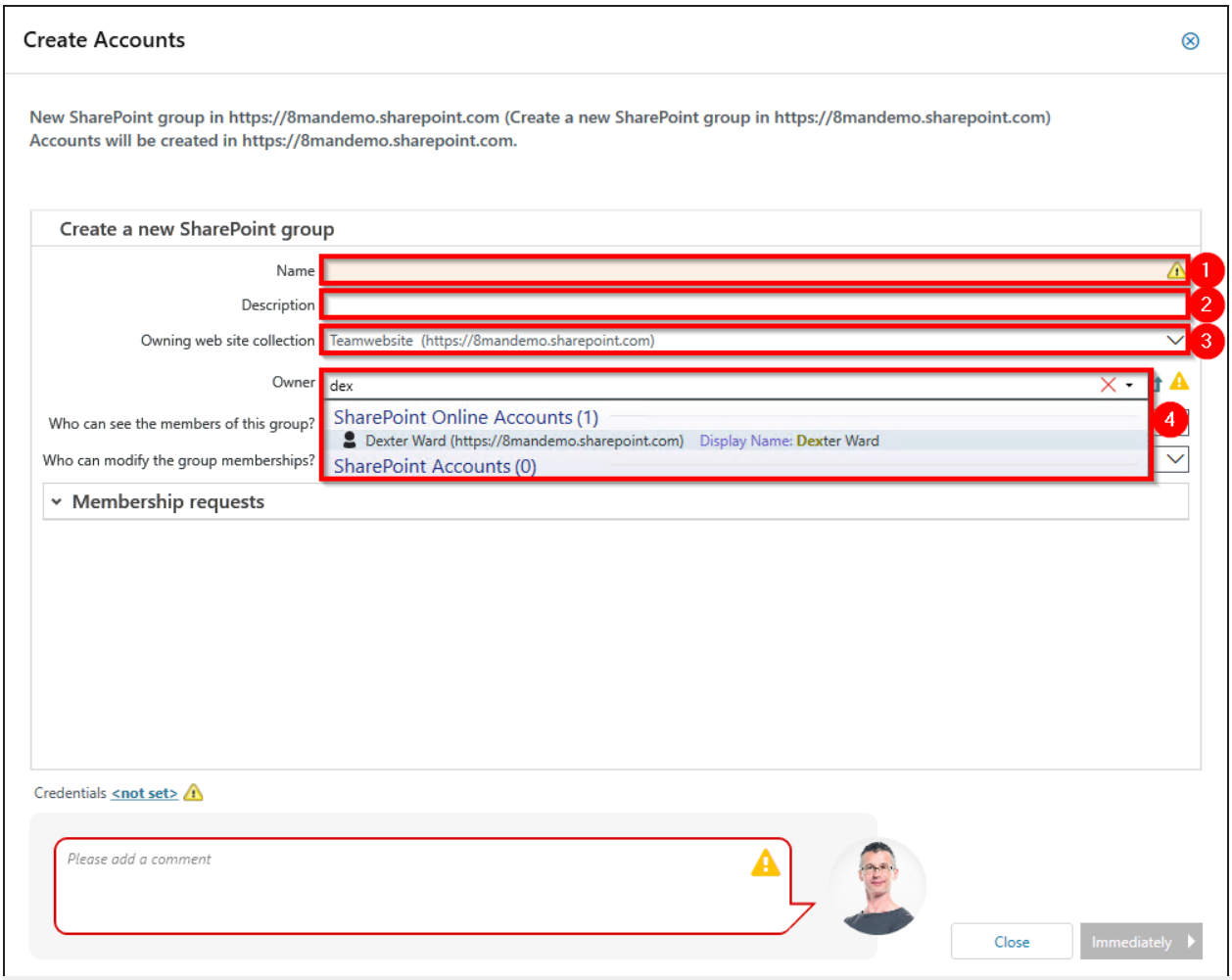
Step-by-step process



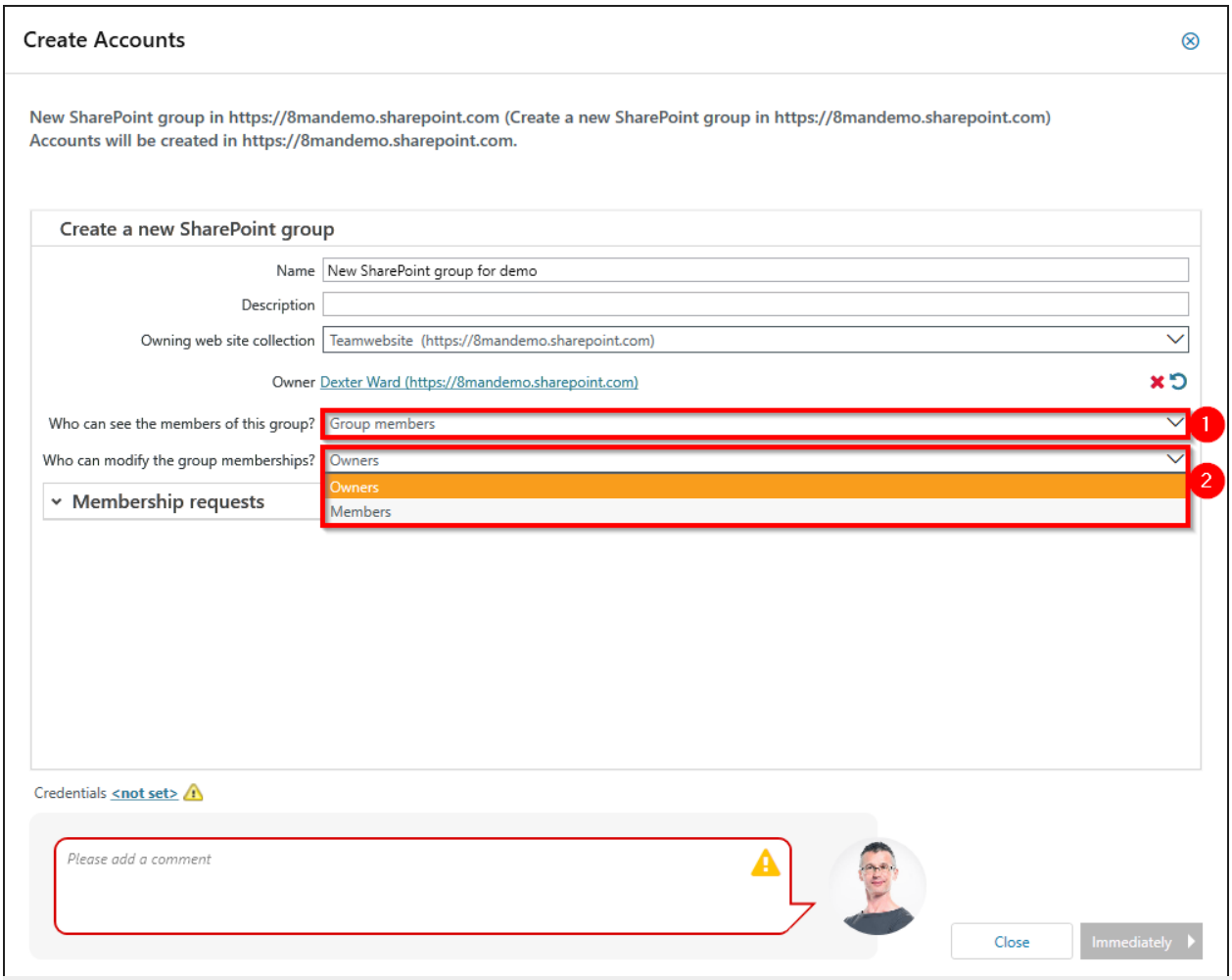
Select "Create a new user account or group" on the start page.



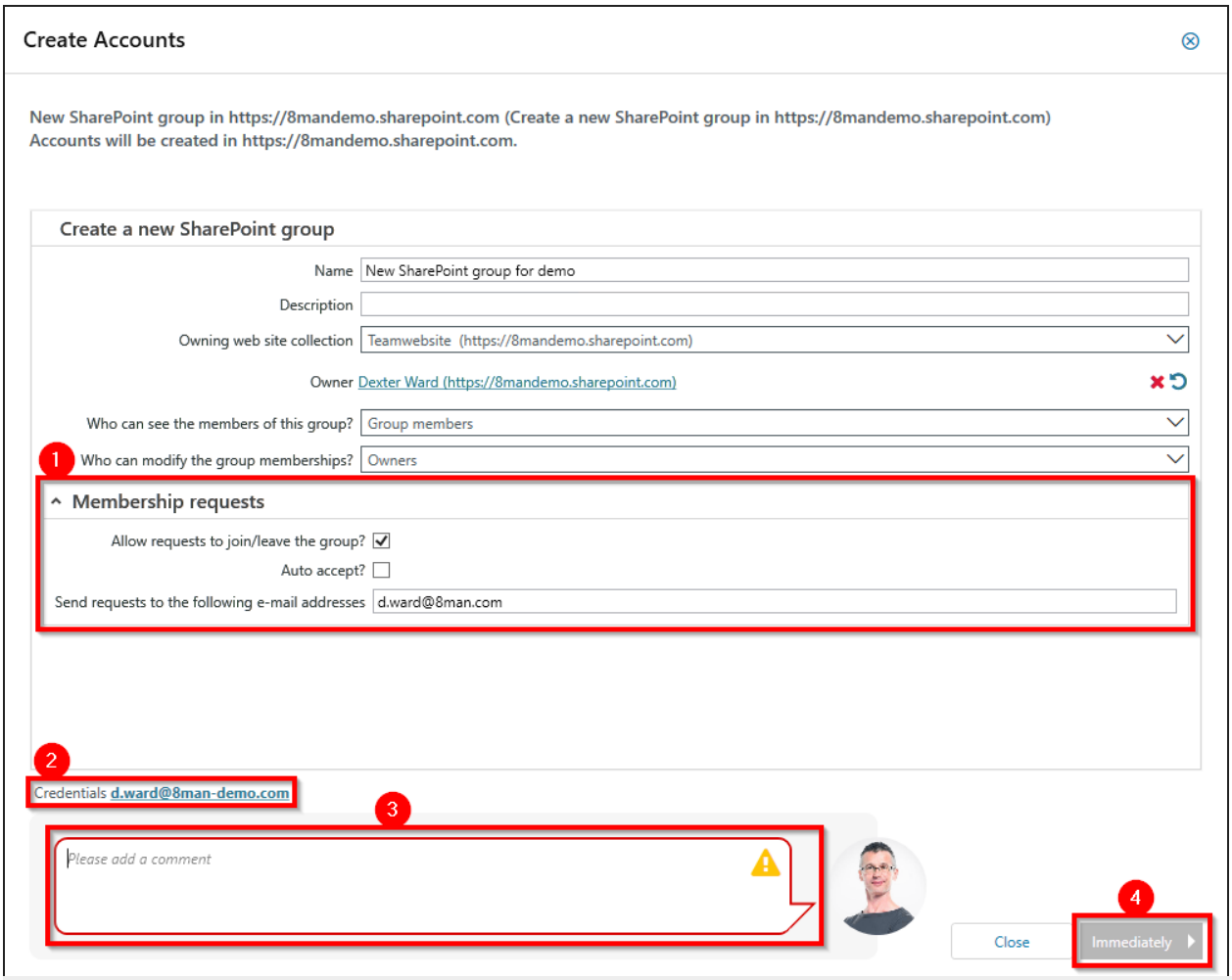
Select the template for the desired SharePoint resource.



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.



1. Select who can see the members of the group.
2. Select who can edit the group memberships.



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.

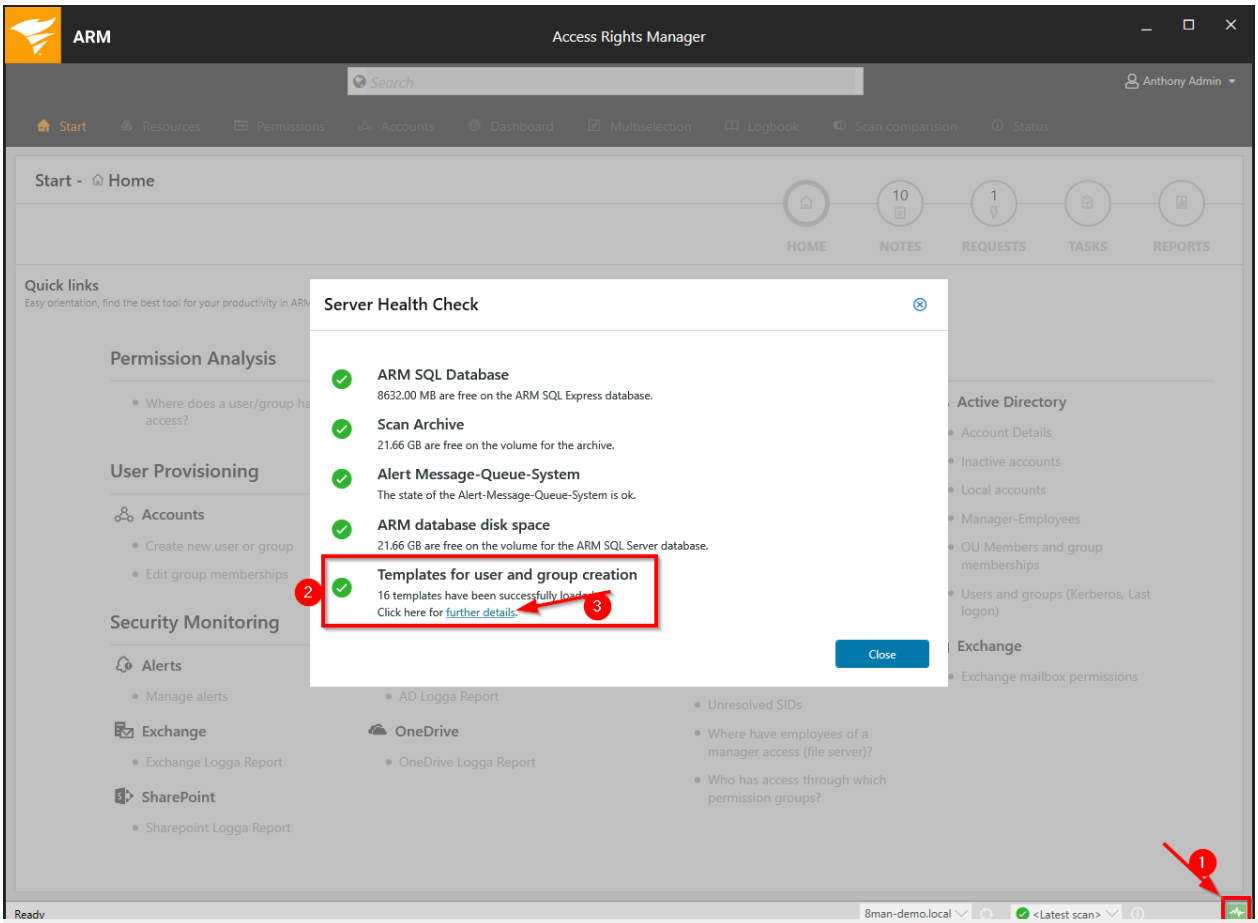
Load templates in ARM

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.



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
TextField	Yes	Yes	Yes	Yes
TextArea	Yes	Yes	Yes	Yes
DropDownList	Yes	Yes	Yes	Yes
FixedValue	Yes	Yes	Yes	Yes
Checkbox	Yes	Yes	No	Yes
Radio	No	No	No	Yes
AccountSearchTextField	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

"Type":	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 here.
Default value:	
Example:	**"Type": TextArea**

"Label":	The label of the input field to be displayed.
Optional:	yes
Characteristics:	
Possible values:	any text
Default value:	
Example:	**"Label": "['en-us:name', 'de-de:Name', 'fr-fr:Nom']"**

"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 "ZoeRossmaesslerOeker".

<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": "l",
    "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 overriden 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:	**true** or **false**
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,

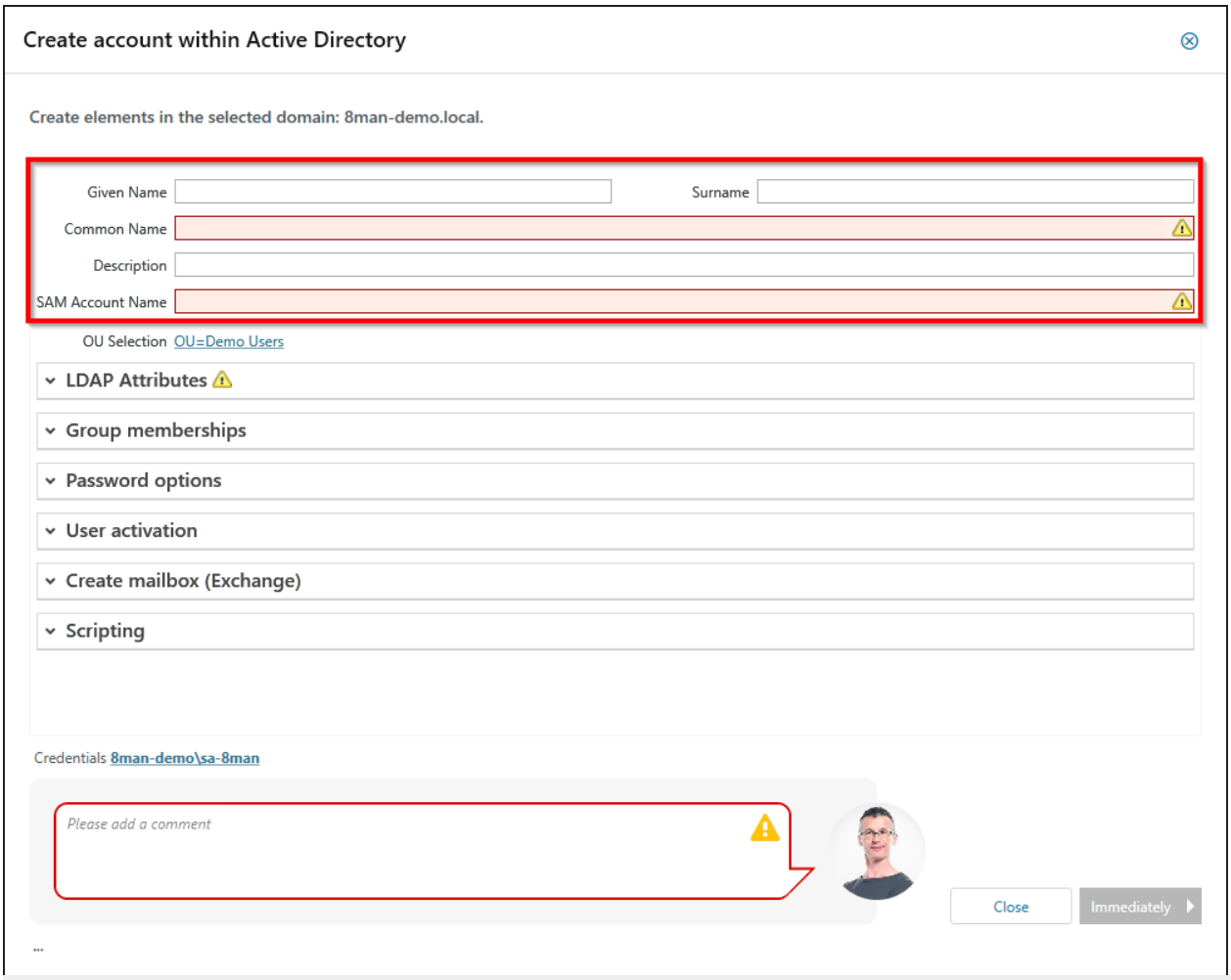
"Label": "Create distribution group",

}

Customize templates for new users

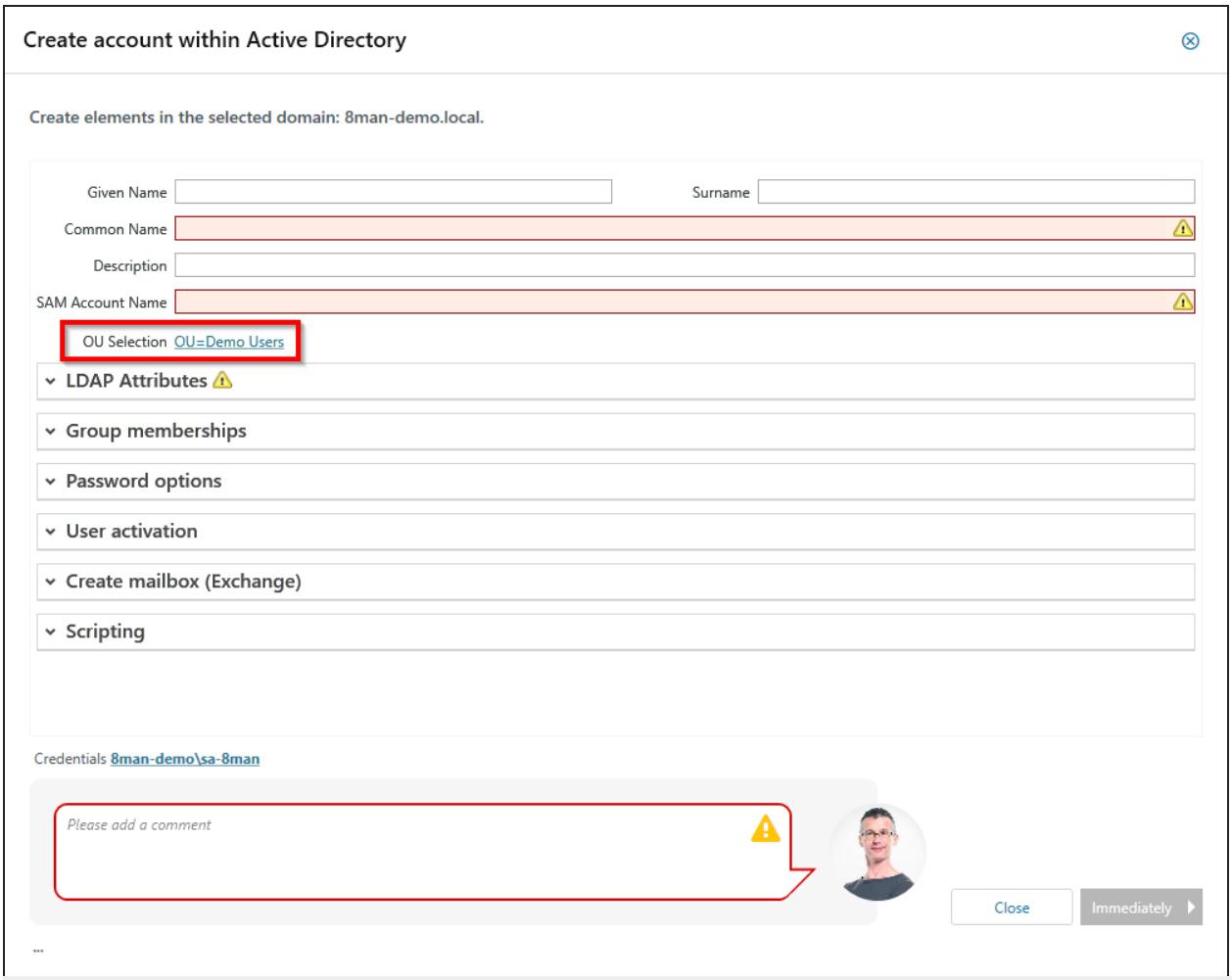
Customize templates according to your needs to standardize, simplify and accelerate the creation of new users.

Enter Name and OU



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.



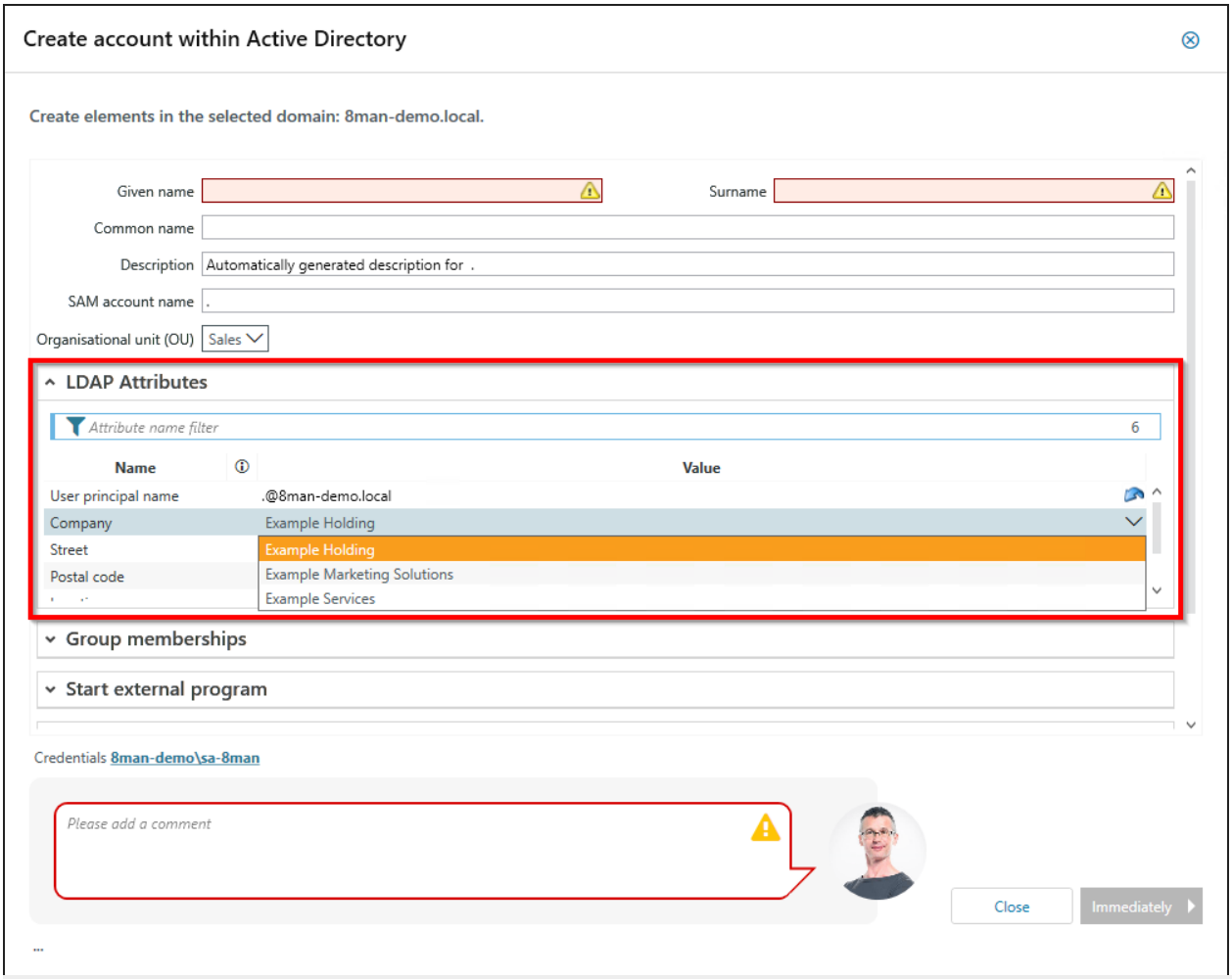
To select the OU in which the new user is stored. A click on the link opens up an OU-selector.

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



In the LDAP Attributes area, further entries can be made for these.

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 ("**l**") are set. The user cannot edit these values.

Example

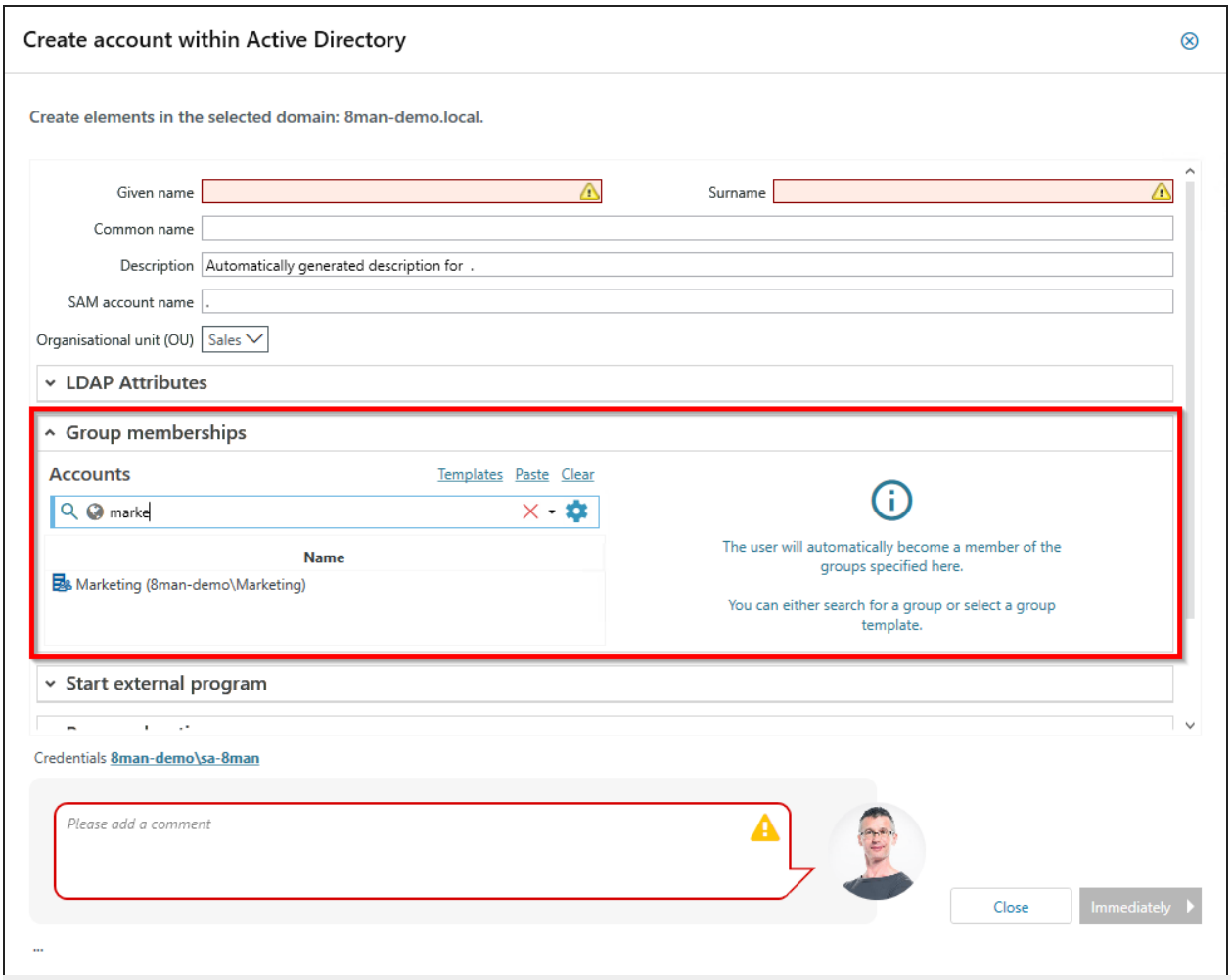
"LdapAttributes": [

{

"Name": "sn", *//Assignment, the following definition for the input of the attribute "sn"*

```
    "Definition": {
        /* property listing
        .
        . */
    }
  }
]
```

Assign group memberships

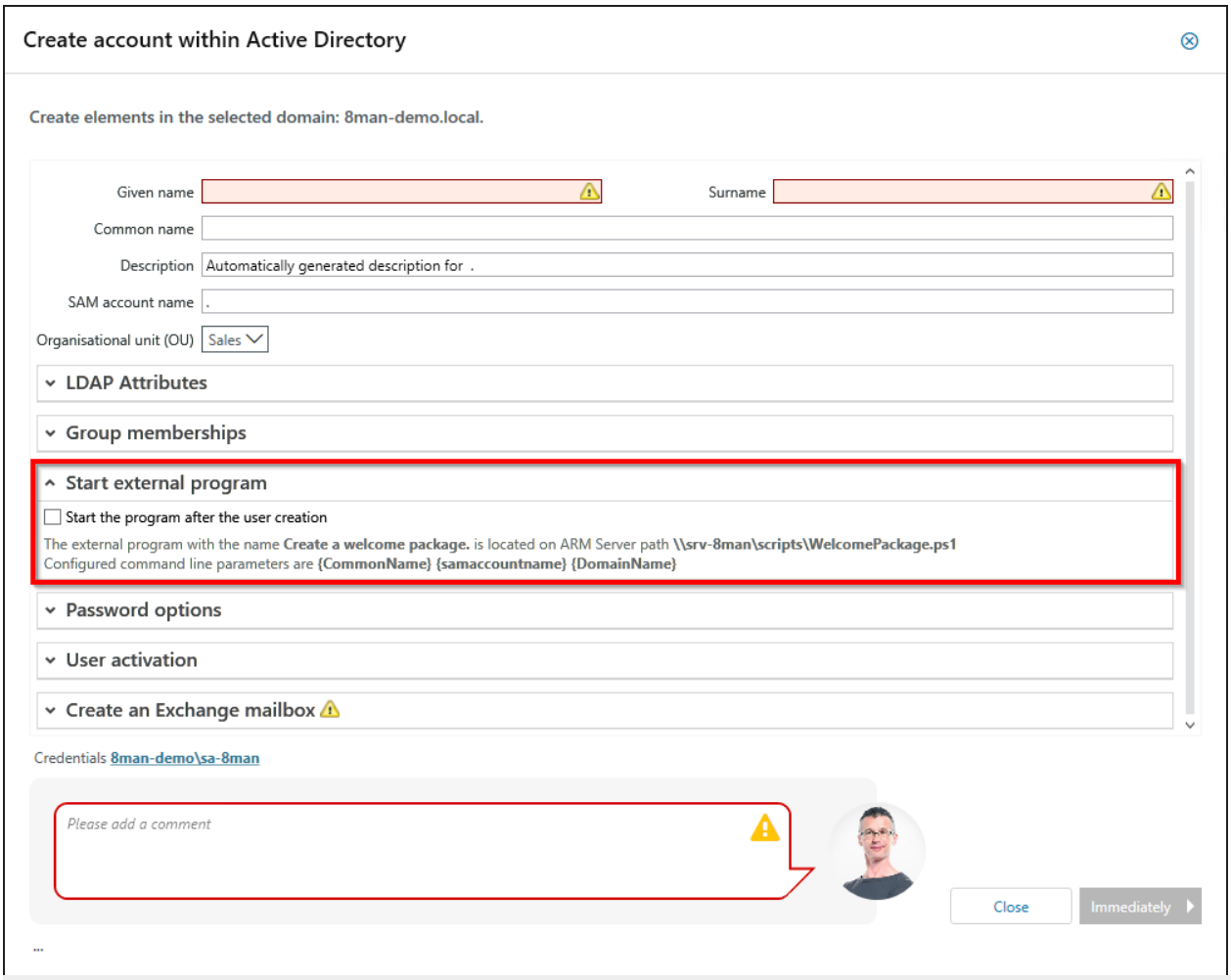


In the group memberships area ("**Memberof**"), you can define in which groups the new user should become a member. Add the SIDs of the desired groups to the Accounts list.

Example

```
"Memberof": {
    "IsHiddenFromRequester": false,
    "IsHidden": false,
    "Accounts": [
        "sid:///ad/S-1-5-21-1545227963-2195427628-2857504096-1440"
    ]
},
```

Run an external program

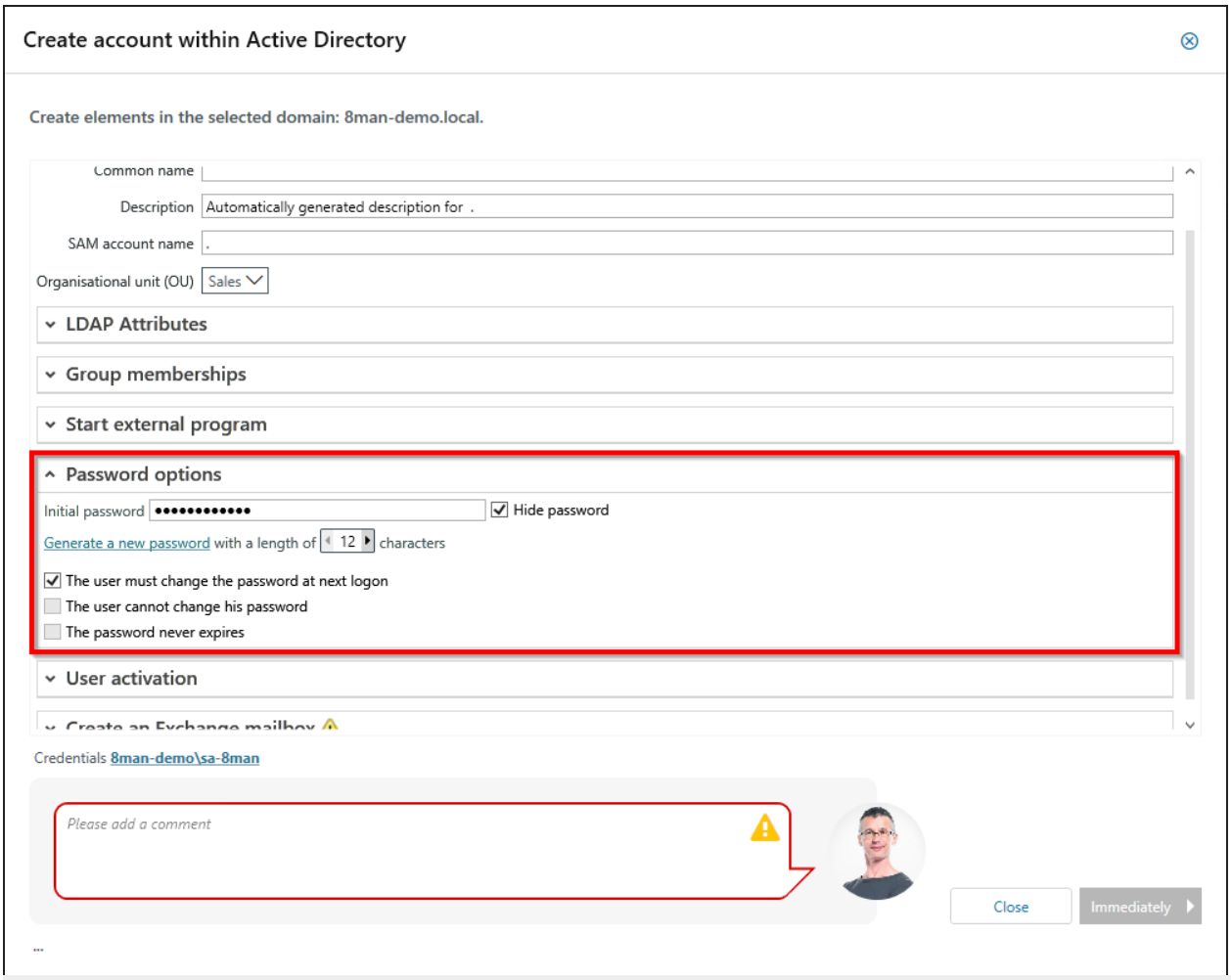


In the Execute external program ("**ScriptOptions**") section, you can specify that a program (script) is executed after creating the new user.

Example

```
"ScriptOptions" : {
    "IsHiddenFromRequester": false,
    "IsScriptEnabledDefault": true,
    "DisplayName": "Create a welcome package",
    "Path": "\\\\srv-8man\\scripts\\WelcomePackage.ps1",
    "CommandLineParameters": "{CommonName} {samaccountname} {DomainName}"
},
```

Enter password options

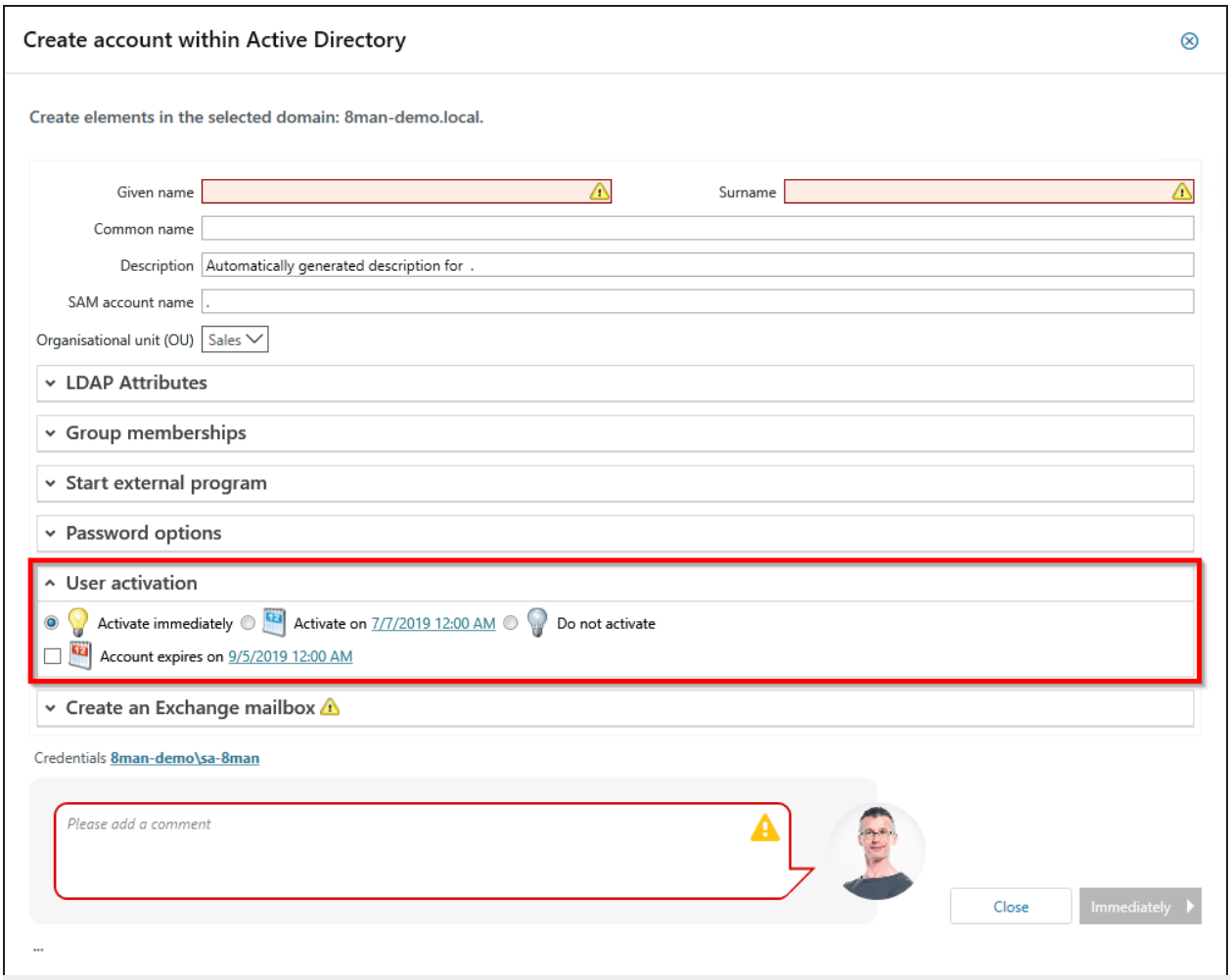


In the password options section, you specify how the initial password ("**InitialPassword**") and the password options ("**PasswordOptions**") are preset.

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



In the Activation section, you determine whether the activation options ("**ActivationOptions**") are hidden.

Example

"ActivationOptions": {

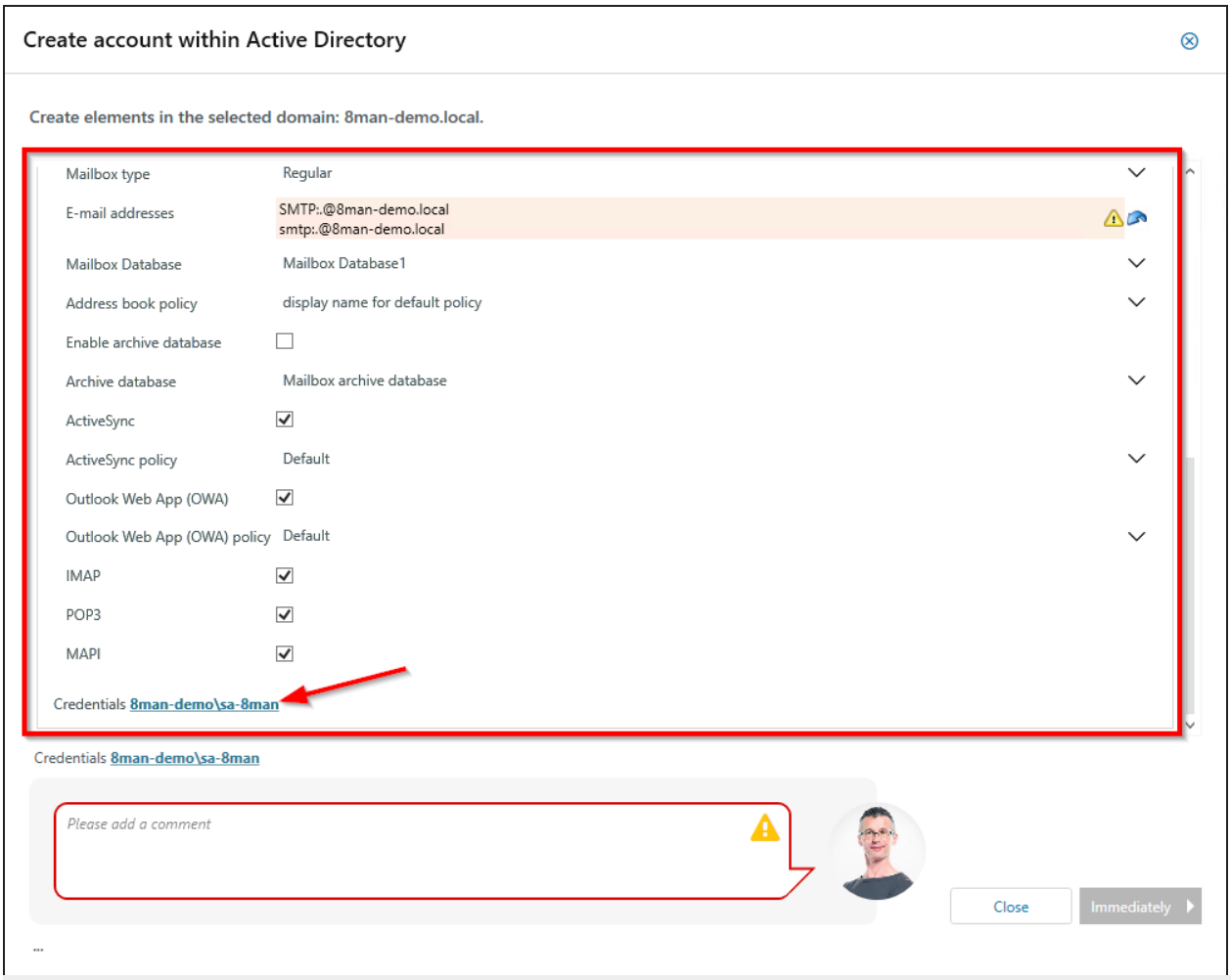
"IsHidden": false,

"IsHiddenFromRequester": true

"AccountActivationState": "Immediately" *// possible values: Immediately, Later, Inactive*

},

Create an Exchange mailbox



In the section "Modules", you email-enable the user. You can define Exchange mailbox settings in the same step. The entire section is optional.

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"
            }
            ]
    }
```

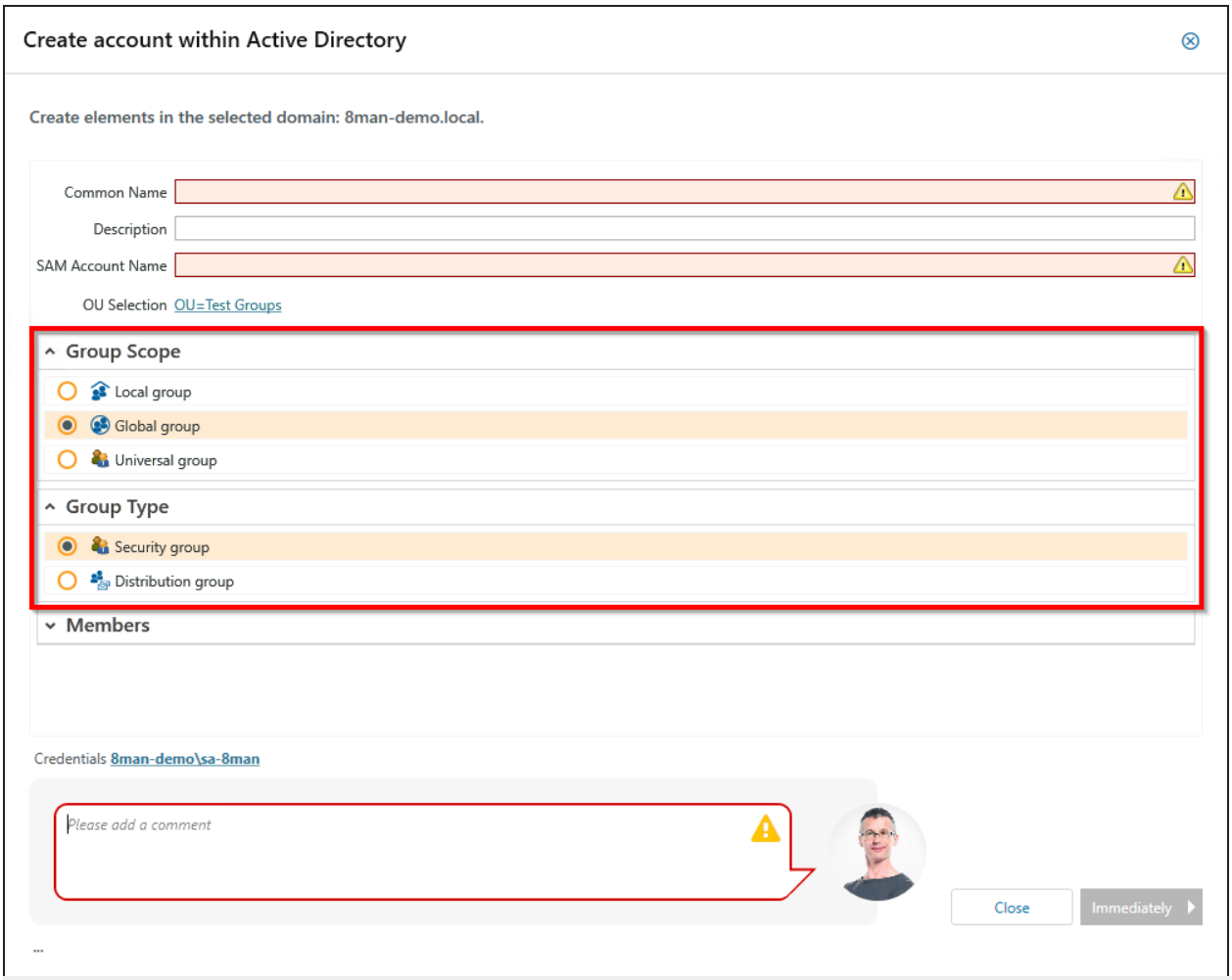
```
},
{
    "Name": "ActivateImap",
    "Definition": {
        "Type": "Checkbox",
        "DefaultValue": "true",
        "Label": "IMAP"
    }
},
{
    "Name": "ActivatePop",
    "Definition": {
        "Type": "Checkbox",
        "DefaultValue": "true",
        "Label": "POP3"
    }
},
{
    "Name": "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)



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",

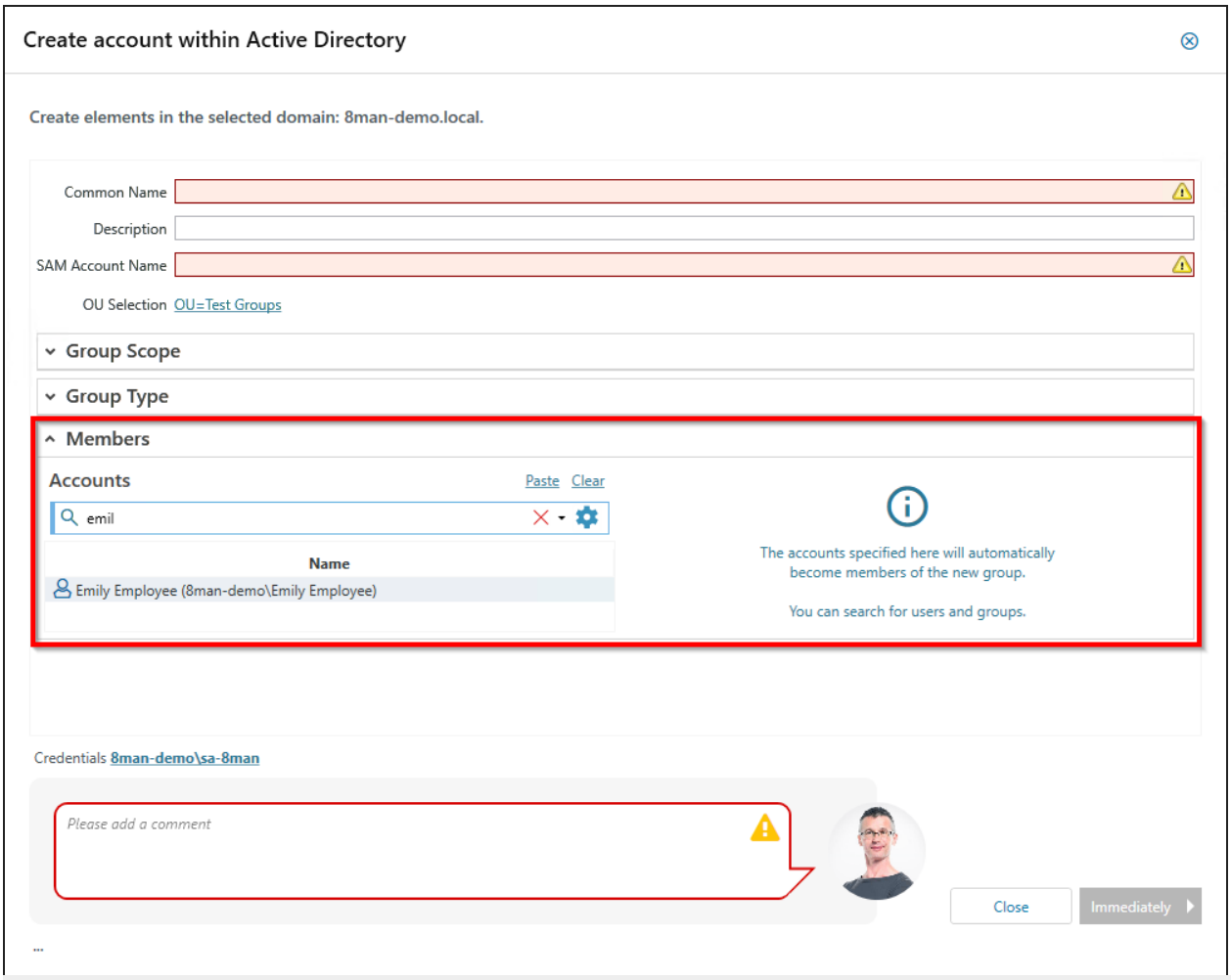
// Hide the area GroupTypeOptions to prevent user changes.

"IsHidden": false,

"IsHiddenFromRequester": false

},

Preset group members

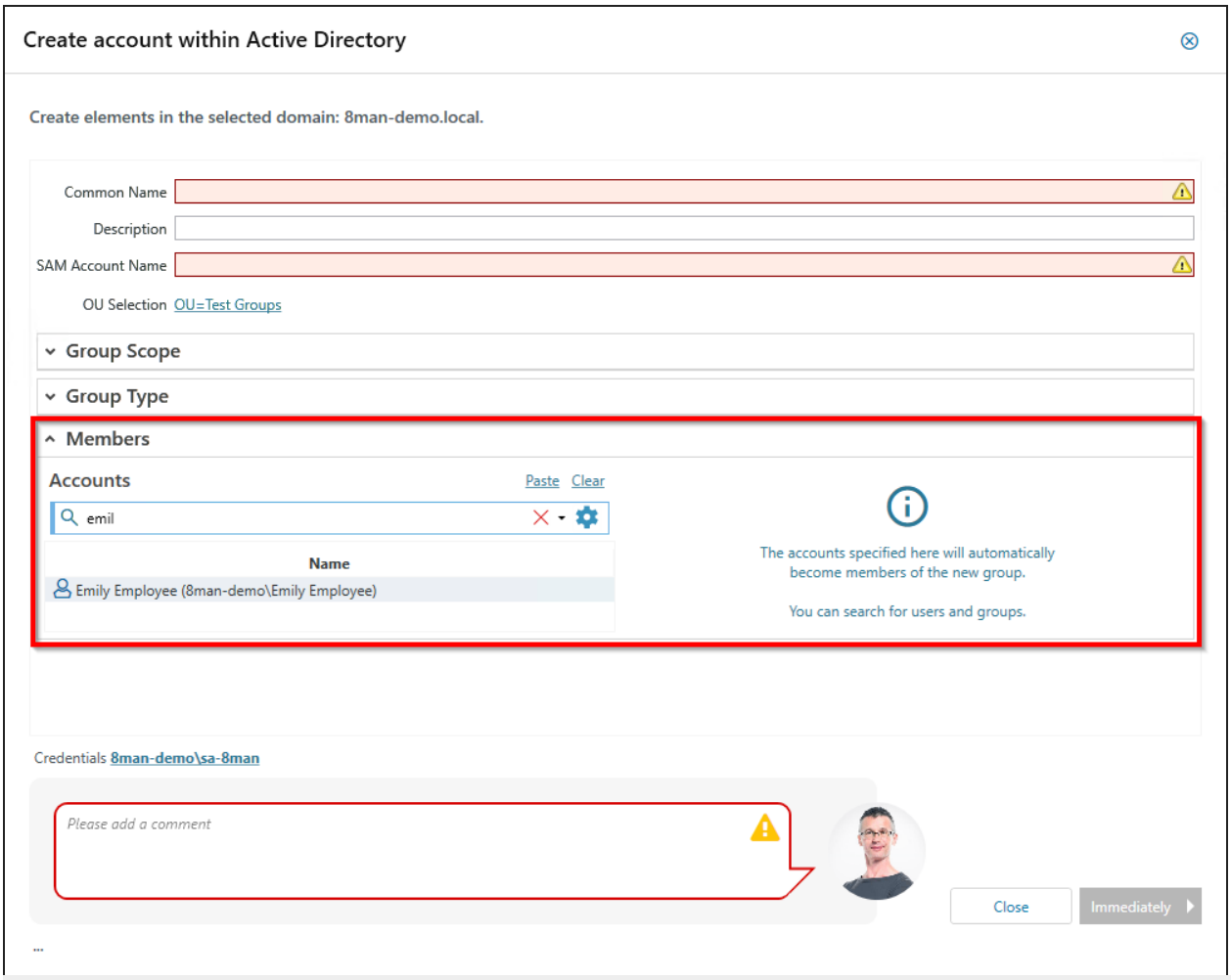


In the **"members**" section, define which members are already preset.

Example

```
"Members" : {
    "Accounts" :[
        "sid:///ad/S-1-5-21-2680840348-2237289205-2993809228-13534"
    ]
}
```

Enable email (create distribution group) in Exchange



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

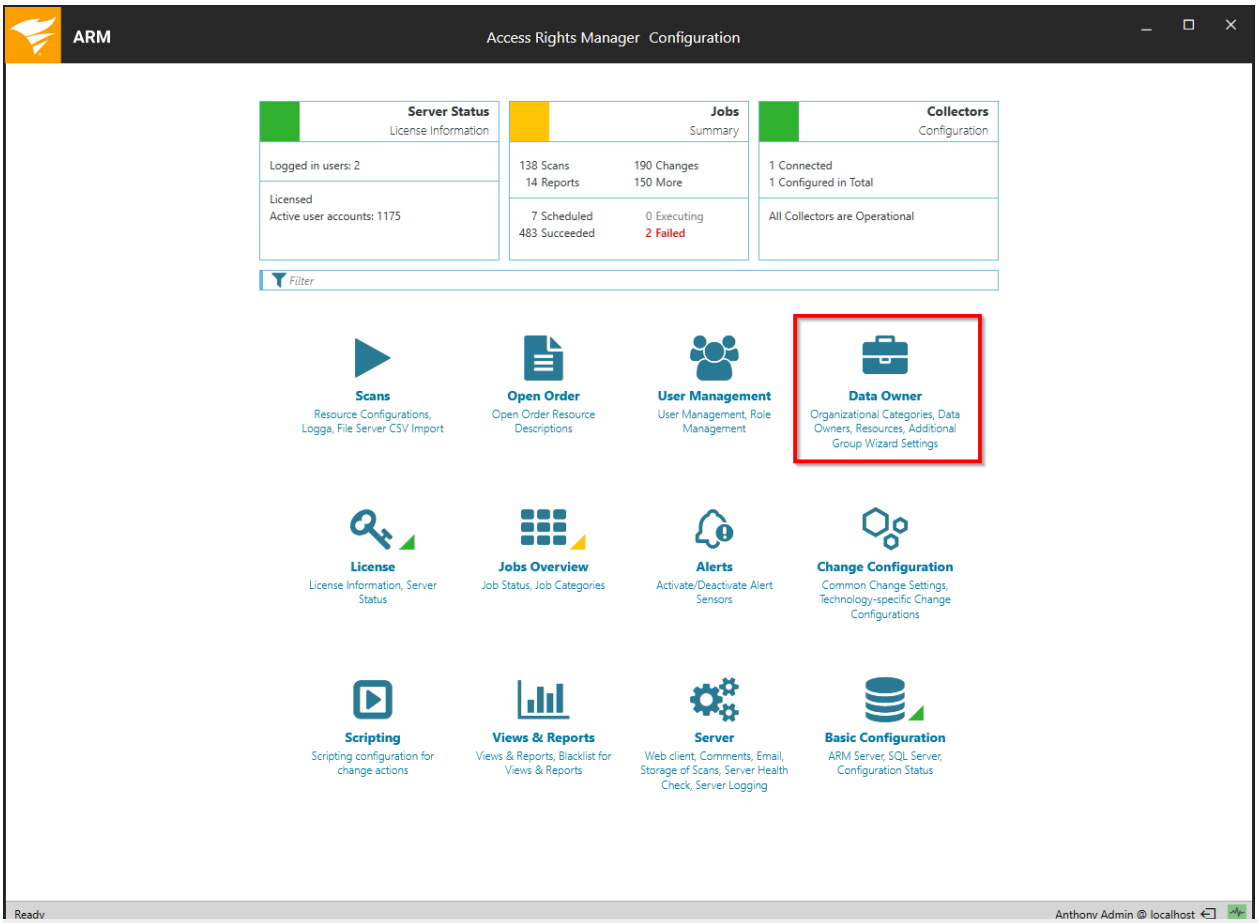

```
[{
    "TemplateType": "CreateMailContact",
    "Version": 1,
    "Id": "2adee521-9423-464e-a52b-0d20a54ec4f6",
    "DisplayName": "Create contact",
```

```
    "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
        }
```

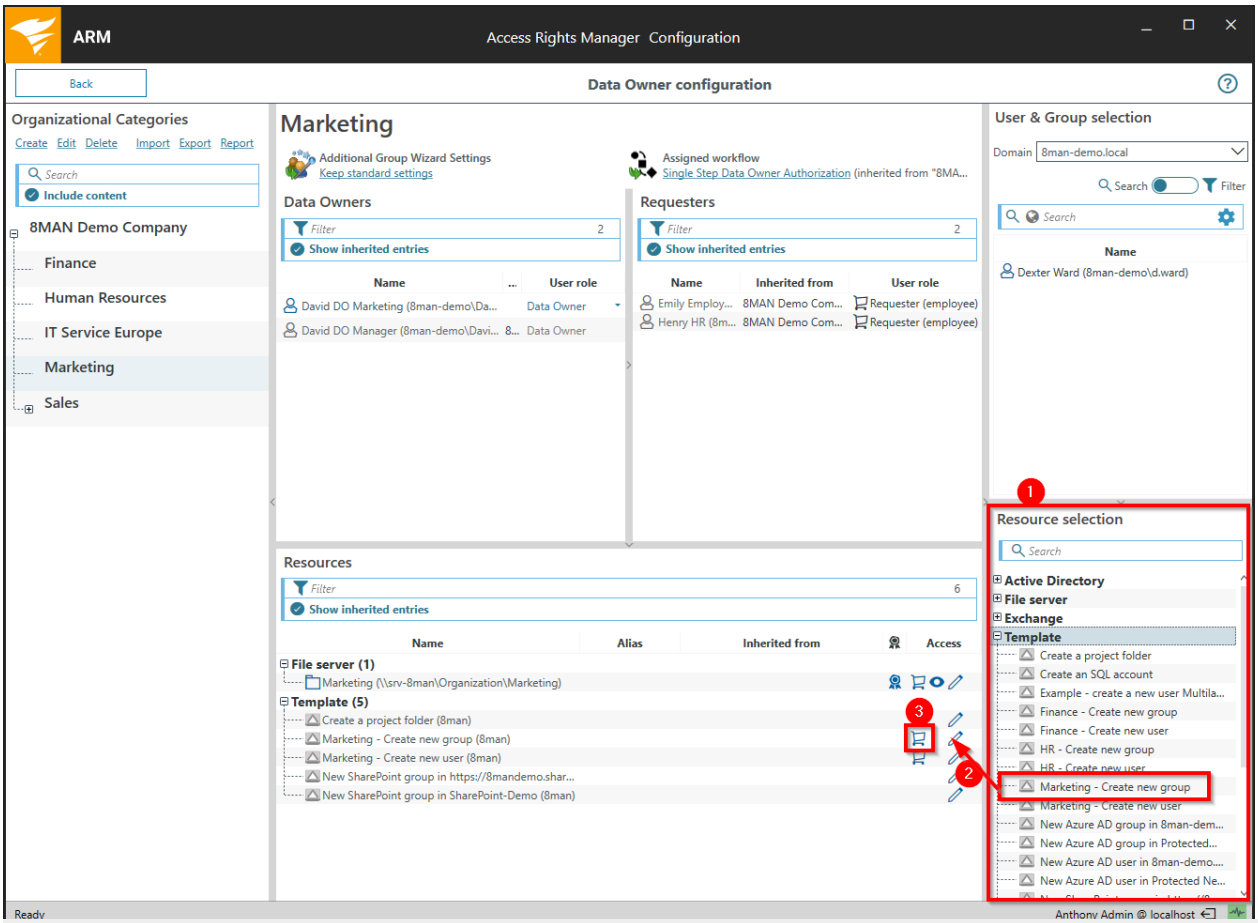
```
    }
},
{
    "Name": "externalemailaddress",
    "Definition": {
        "Type": "TextField",
        "Label": "External email address",
        "IsRequired": true,
        "IsEnabled": true,
        "Constraints": {
            "MaxLength": 200,
            "ValidationRule": "[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+\\.[A-Za-z]{2,6}"
            }
        }
    }
  ]
}
]
```

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.



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,givenname)"
        }
    }
},
{
    "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.

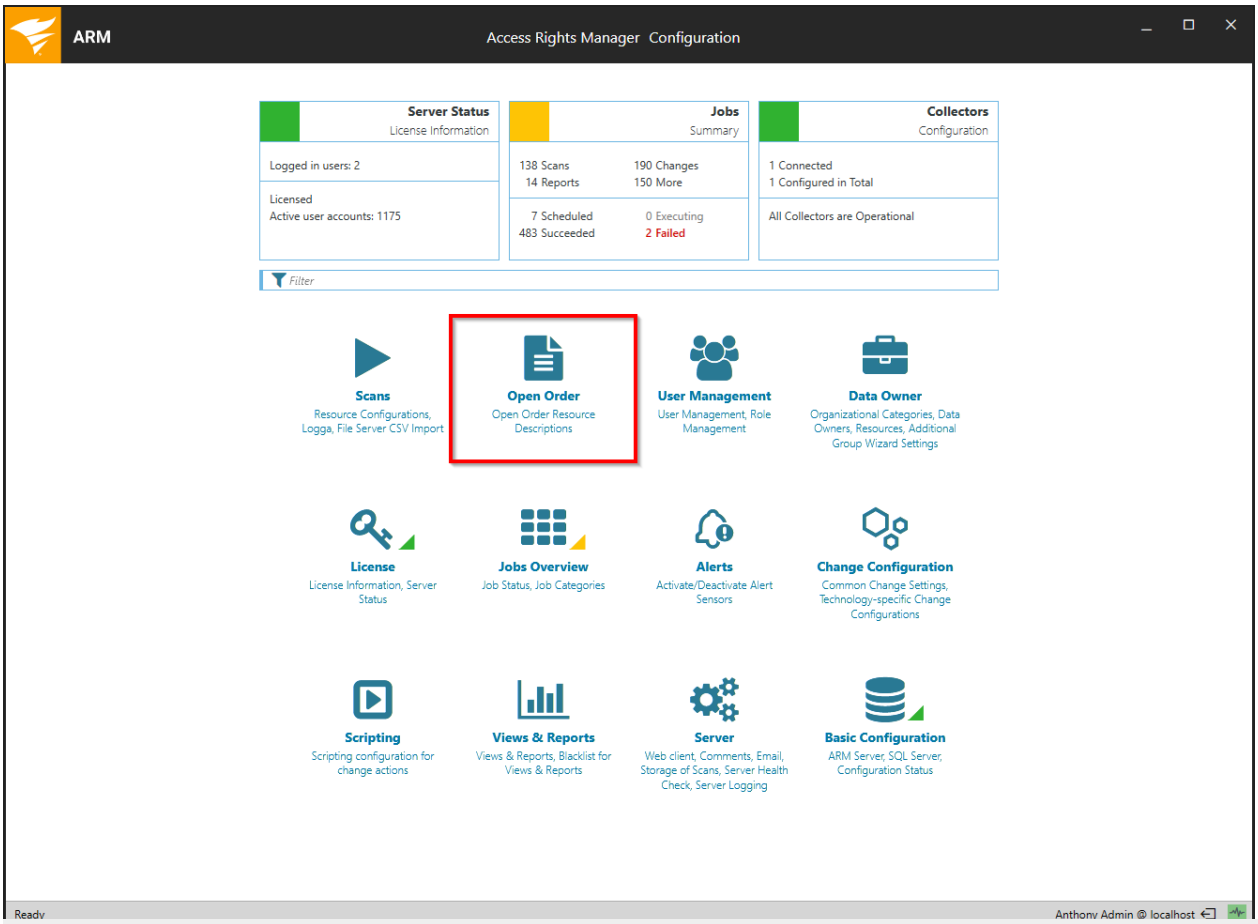
For more information on the structure of the XML resource configuration, see the Open Order manual.

Example

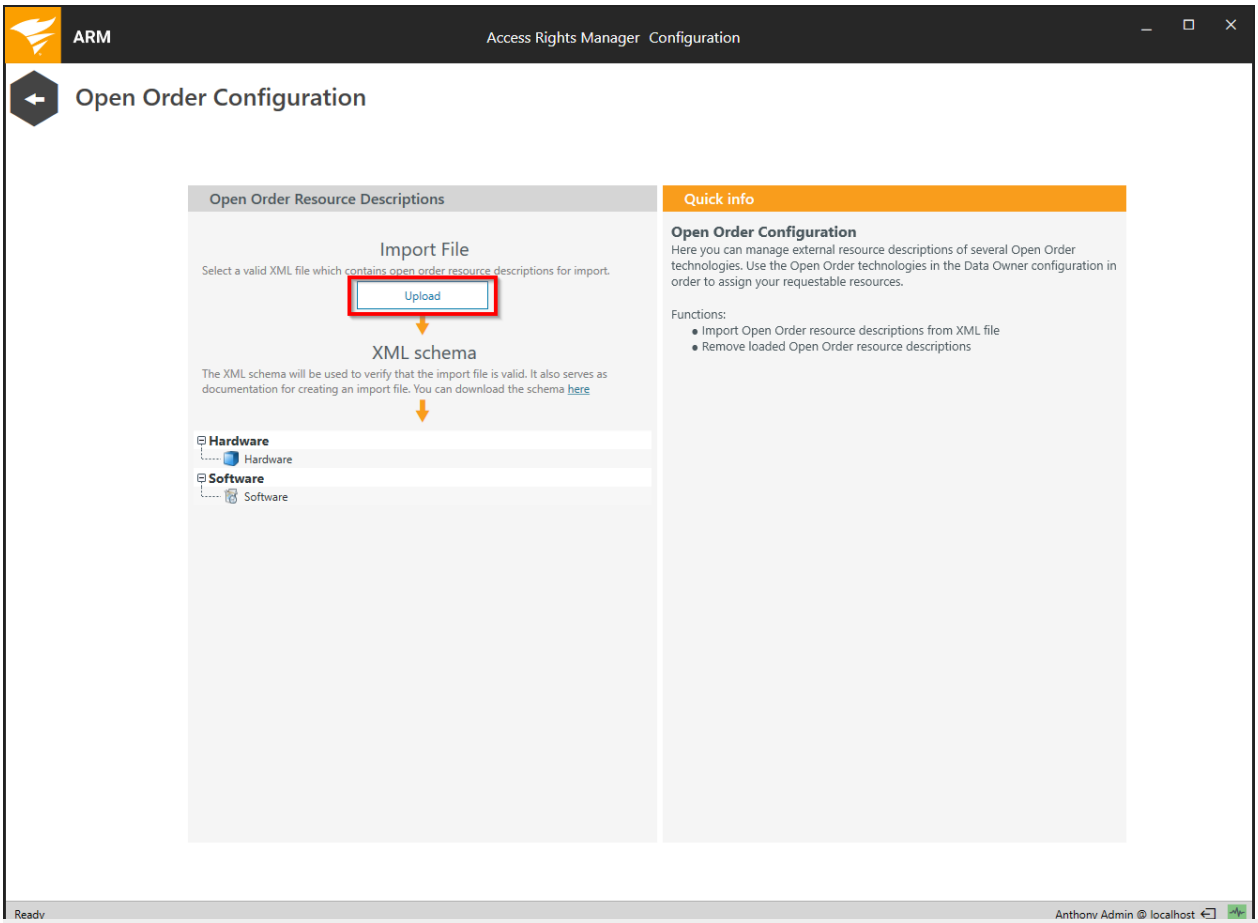
```
<?xml version="1.0" encoding="utf-8"?>
<resourceImport Version="3">
    <technology Id="D54C16F2-42C1-477A-BD20-3285158F68D3" Name="Hardware" IconId="2"
Color="#0000be">
        <definitions>
            <permissionSets>
                <permissionSet PermissionSetId="1" Description="['en-US:Buy','de-DE:Kaufen']" />
                <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" 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 Custom" TypeId="3" TemplateID="E3865726-6FDF-489E-
A7D5-4ABBA5B2BF83" />
            </resource>
        </root>
```

```
    </data>
  </technology>
</resourceImport>
```

Upload an XML resource configuration to the Data Owner configuration

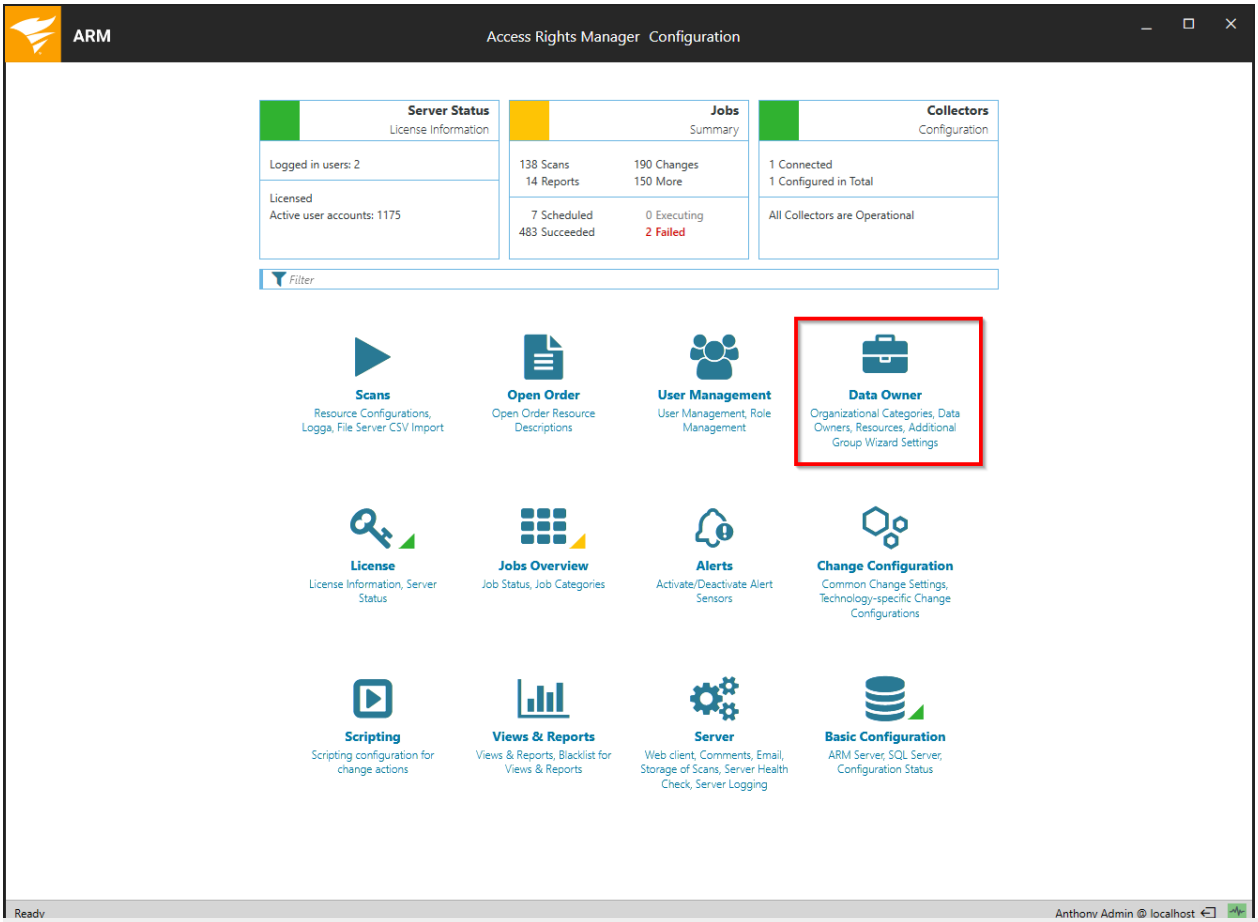


In the ARM configuration, click "Open Order".

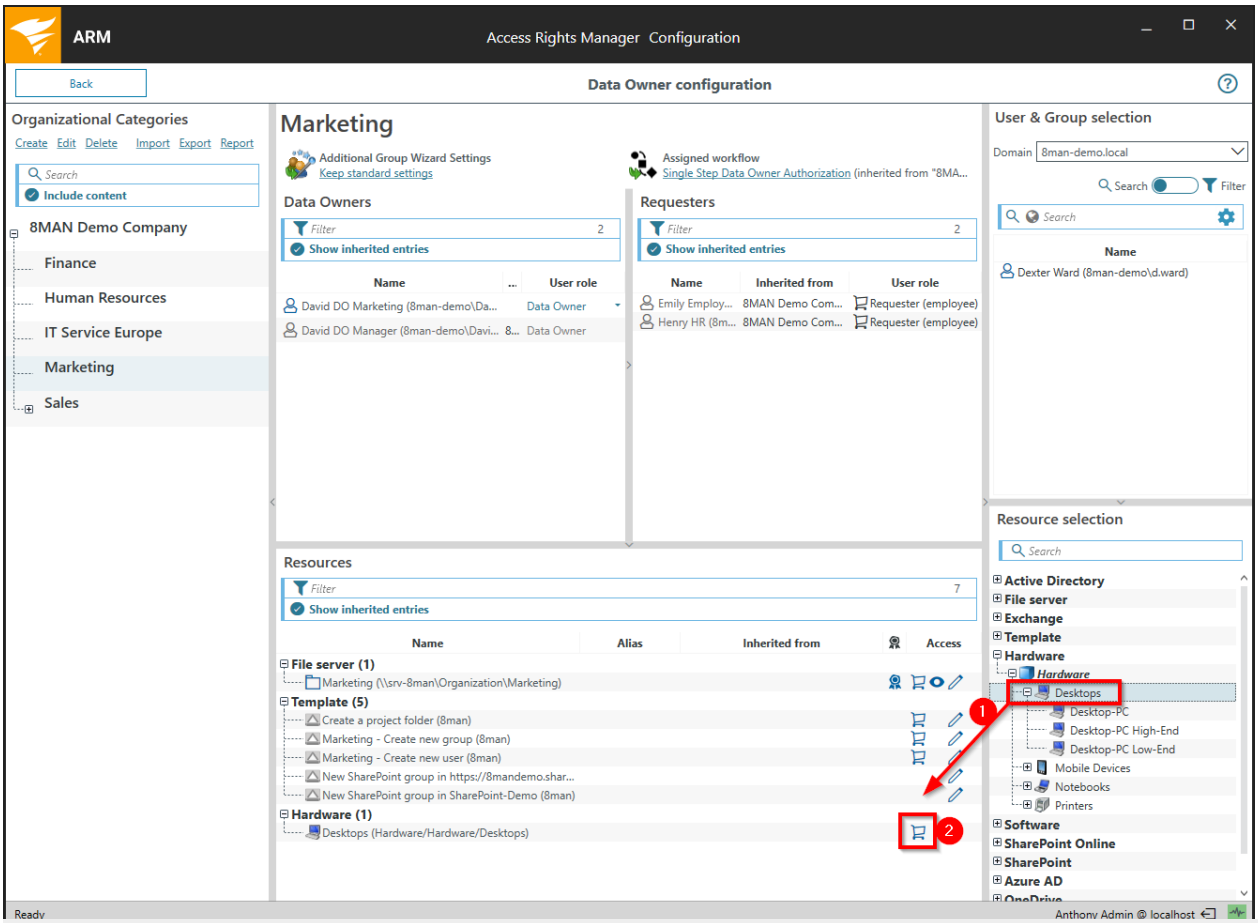


Click "Upload" to import the XML Resource Configuration. After successful import, the resources are available in the Data Owner configuration and can be assigned to organizational categories.

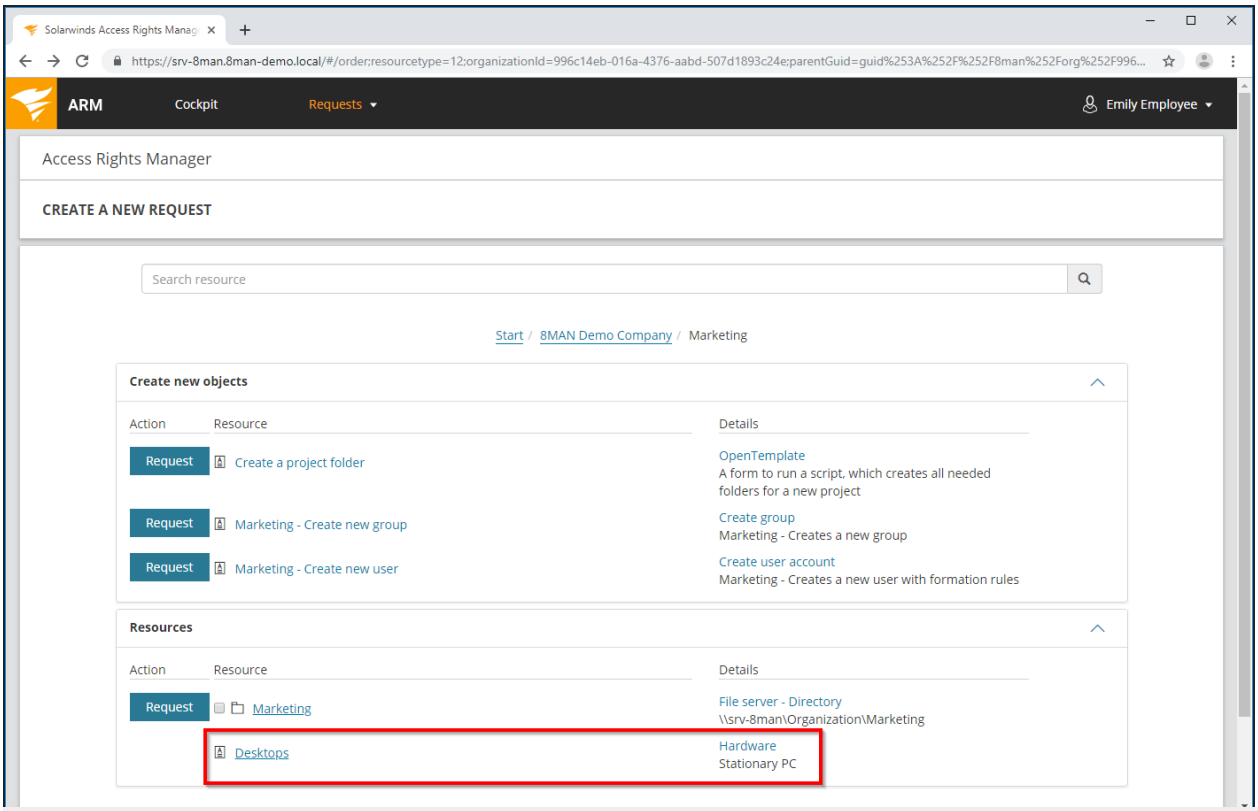
Set the open order resource to requestable



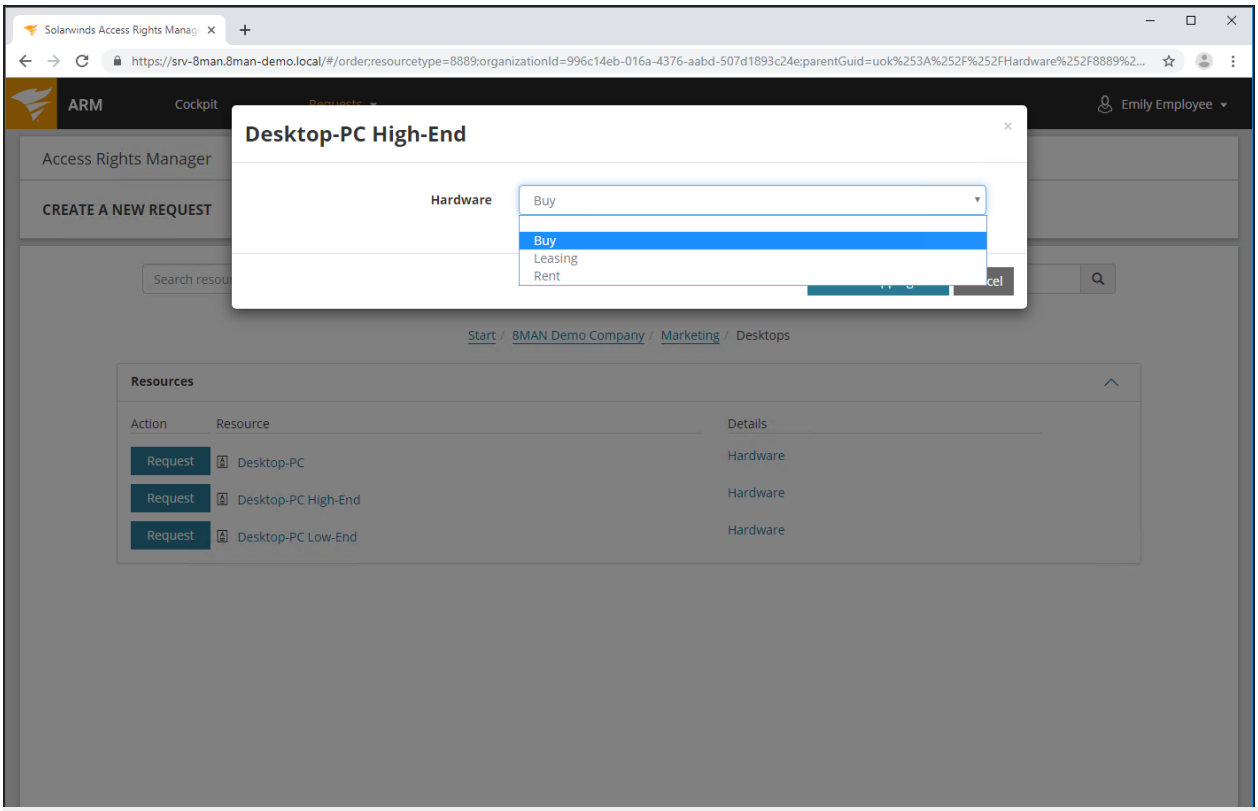
In the ARM configuration, click "Data Owner".



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.