



Access Rights Management. **Only much Smarter.**



# Access Rights Management User Manual

Version 9

© 2018 Protected Networks GmbH

# Access Rights Management: For a Secure Network

We started in 2009 with the mission to raise our client's IT Security level. We knew IT Security does not end with the firewall, but with a protected network from within.

As of 2018 we have over 1200 satisfied customers: 8MAN Access Rights Management has become a standard in companies and institutions worldwide.

This would not have been possible without the help of our clients, partners and distributors: Thank you all for the good collaboration!

In this document you find our whole product range: The 8MAN World. Please contact us if you have any questions.

Berlin 2018

## **Publisher**

*Protected Networks GmbH*

*Alt-Moabit 73  
10555 Berlin*

*+49 30 390 63 45 - 0*

*Protected-Networks.com  
8MAN.com*

## **Support**

*+49 30 390 63 45 – 99  
helpdesk@8man.com  
Knowledge Base*

## **Knowledge Management**

*Fabian Fischer / Jörg Brandt*

*T: +49 30 390 63 45-41  
T: +49 30 390 63 45-81*

*Got Feedback?*



**Stephan Brack**

**CEO Protected Networks**

A stylized, handwritten signature in black ink, appearing to read 'S. Brack'.



**Matthias Schulte-Huxel**

**CSO Protected Networks**

A stylized, handwritten signature in black ink, appearing to read 'Matthias Schulte-Huxel'.



# Liability Notice

Information provided in this document may change at any given time and without prior notice. Its provision does not entail any kind of legal obligation at Protected Networks's end.

The usage of Protected Networks's software 8MAN is outlined in an End User Licence Agreement (EULA). 8MAN must only be used in accordance with its stipulations.

Without prior written consent from Protected Networks this document must not be partially or entirely reproduced, transmitted or translated, be it by electronic, mechanical, manual or optical means.

This document should be considered part of a framework consisting of Protected Networks's Terms & Conditions, EULA and Privacy Statement to be found on their website.

## Copyright

8MAN is the registered trademark of a software solution and its related documents and is the intellectual property of Protected Networks.

Protected Networks GmbH  
Alt-Moabit 73  
10555 Berlin

Berlin, July 2018

<b>1</b>	<b>Why?</b>	<b>14</b>
1.1	Protecting data, information and knowledge	15
1.2	Decentralize security expertise	16
1.3	Simplify Security	17
<b>2</b>	<b>The Core Disciplines of ARM</b>	<b>19</b>
2.1	Permission Analysis	21
2.2	Documentation & Reporting	22
2.3	Security Monitoring	23
2.4	Role & Process Optimization	24
2.5	User Provisioning	25
<b>3</b>	<b>Additional ARM disciplines</b>	<b>27</b>
3.1	Resource Integration	29
3.1.1	+8MATE for Exchange	30
3.1.2	+8MATE for SharePoint	31
3.1.3	+8MATE for Dynamics NAV	32
3.1.4	Easy Connect - integrating any resources	33
3.1.4.1	Analysing Easy Connect resources	33
3.1.4.2	Create a report for an Easy Connect Resource	35
3.2	8MAN Application Integration	36
3.2.1	+8MATE Matrix 42	37
3.3	Threat & Gap Management	38
3.3.1	8MATE Clean!	39
<b>4</b>	<b>Permission analysis</b>	<b>41</b>
4.1	Active Directory	42
4.1.1	Services for Administrators	43
4.1.1.1	Visualize nested group structures	43
4.1.1.2	Compare two different access rights situations (Scan Comparison)	45
4.1.1.3	Identify overprivileged users (based on Kerberos token size)	49
4.1.1.4	Identify nesting depth of groups	50
4.1.1.5	View members of different groups in one list	52

4.1.1.6	Identify empty groups .....	53
4.1.1.7	Identify recursive groups .....	55
4.1.1.8	Identify recursive groups (web client) .....	57
4.1.1.9	Identify users with never expiring passwords .....	59
4.1.1.10	Identify users with never expiring password (web client) .....	61
4.1.1.11	Analyze historical AD structures .....	63
4.1.1.12	Identify inactive accounts (web client) .....	65
4.1.1.13	Identify temporary user accounts .....	67
4.1.1.14	Identify the most recent actions on an account .....	69
4.1.1.15	Determine permissions deviating from the department profile (Compliance Check) (web client) .....	71
4.2	File server .....	73
4.2.1	Services for administrators und data owners .....	74
4.2.1.1	Identify access rights on a file server directory .....	74
4.2.1.2	Identify the permissions of a user .....	76
4.2.2	Services for administrators .....	78
4.2.2.1	Identify multiple access paths to file server directories .....	78
4.2.2.2	Identify globally accessible directories (web client) .....	80
4.2.2.3	Identify corrupted inheritance .....	82
4.2.2.4	Identify folders with special protection .....	85
4.2.2.5	Compare two different access rights situations (Scan Comparison) .....	87
4.2.2.6	Analyze historical access rights situations .....	91
4.2.2.7	Identify the last activities on a directory .....	92
4.2.2.8	Identify share permissions .....	94
4.3	+8MATE for Exchange .....	95
4.3.1	Help Desk .....	96

4.3.1.1	Identify access rights on mailboxes .....	96
4.3.1.2	Identify mailbox properties .....	97
4.3.1.3	Identify access rights on public folders .....	98
4.3.1.4	Identify permissions on distribution groups .....	99
4.3.1.5	Identify members of distribution groups .....	101
4.4	+8MATE for SharePoint .....	102
4.4.1	Services for administrators and data owners .....	103
4.4.1.1	Identify access rights on SharePoint resources .....	103
4.4.2	Services for administrators .....	104
4.4.2.1	Identify divergent access rights in the tree structure .....	104
4.5	+8MATE for Dynamics NAV .....	106
4.5.1	Analyze Dynamics NAV permissions .....	106
<b>5</b>	<b>Documentation &amp; Reporting .....</b>	<b>108</b>
5.1	All Technologies .....	109
5.1.1	Flexible reports (web client) .....	109
5.1.2	Report on 8MAN Access Rights Management activities (Logbook report) .....	111
5.2	Active Directory .....	113
5.2.1	Management reports .....	113
5.2.1.1	Where do users and groups have access? .....	113
5.2.1.2	Employees of a manager .....	115
5.2.2	Reports for administrators .....	117
5.2.2.1	Display user account details .....	117
5.2.2.2	Find inactive accounts (users or computers) .....	119
5.2.2.3	OU members and group memberships .....	121
5.2.2.4	Users and groups report .....	122
5.2.2.5	Identify local accounts .....	124
5.2.3	Organizational help for administrators .....	125

5.2.3.1	Add notes to user accounts and groups .....	125
5.2.3.2	Purpose Groups: Give aliases to groups .....	128
5.2.3.2.1	Create a purpose group .....	128
5.2.3.2.2	Delete or modify a purpose group .....	130
5.3	File server .....	131
5.3.1	Management reports .....	131
5.3.1.1	Where do users and groups have access? .....	131
5.3.1.2	Who has access to what? .....	133
5.3.1.3	Where do employees of a manager have access to? .....	136
5.3.2	Reports for Administrators .....	137
5.3.2.1	Identify usage of "everyone" .....	137
5.3.2.2	Who has access through which permission groups? .....	139
5.3.2.3	Permission differences .....	141
5.3.2.4	Identify unresolved SIDs .....	142
5.3.2.5	Identify direct permissions .....	144
5.3.2.6	Identify directories whose owners are not administrators .....	146
5.3.2.7	Identify usage of "Authenticated Users" .....	148
5.4	+8MATE for Exchange .....	150
5.4.1	Management Reports .....	151
5.4.1.1	Who has access to what? .....	151
5.4.1.2	Identify mailbox permissions .....	153
5.5	+8MATE for Sharepoint .....	155
5.5.1	Management Reports .....	156
5.5.1.1	Who has access where? .....	156
5.5.1.2	Where do users and groups have access? .....	158
<b>6</b>	<b>Security Monitoring .....</b>	<b>160</b>
6.1	Active Directory .....	161

6.1.1	+8MATE AD Logga .....	161
6.1.1.1	Report: monitor changes in Active Directory .....	162
6.1.1.2	Identify temporary group memberships .....	166
6.1.1.3	Identify locked user accounts .....	168
6.1.1.4	Monitor password resets .....	170
6.1.1.5	Analyze AD Logga events with the logbook .....	172
6.1.1.6	Set alerts for groups .....	174
6.1.1.7	Set alerts for user accounts .....	176
6.1.1.8	Run a script after an alert .....	178
6.1.1.9	Manage alerts .....	180
6.2	Fileserver .....	181
6.2.1	+8MATE FS Logga .....	181
6.2.1.1	Monitor access to sensitive data .....	182
6.2.1.2	Enable alerts for file server directories .....	184
6.2.1.3	Enable alerts for suspected data theft (file server) .....	189
6.2.1.4	Enable alerts for data deletion (file server) .....	194
6.2.1.5	Enable alerts for suspected cases on ransomware (file server) .....	199
6.3	Exchange .....	204
6.3.1	Monitor Exchange activities .....	204
6.3.1.1	Monitor activities on mailboxes, calendars, and contacts (report) .....	205
6.3.1.2	View activities in mailboxes, calendars, and contacts (logbook) .....	207
<b>7</b>	<b>Role &amp; Process Optimization .....</b>	<b>210</b>
7.1	Delegation of tasks .....	211
7.1.1	Apply an 8MAN account to a specific security role or data owner .....	212
7.1.1.1	Create a read only account with 8MAN .....	213
7.1.1.2	Schedule reports .....	214

7.1.2	Assign the administration of folder rights to a Data Owner (Manager) .....	217
7.1.2.1	Define Data Owners and assign resources .....	218
7.1.2.2	Enable Data Owners to manage file server permissions .....	220
7.1.3	Delegate user provisioning processes to the help desk .....	221
7.1.3.1	Define your help desk and assign resources with 8MAN .....	222
7.1.3.2	Assign responsibilities to help desk employees .....	223
7.2	Create approval processes .....	224
7.2.1	The simple authorization process. Approving and rejecting actions as an Administrator .....	224
7.2.2	+8MATE GrantMA: design complex approval flows .....	227
7.2.2.1	Define individual approval workflows .....	228
7.2.2.2	Assigning approval workflows to individual resources .....	231
7.2.2.3	Assigning resource owners using the web client .....	232
7.3	Data Owner: Recertification of existing access rights .....	235
7.3.1	E-mail notifications for recertification .....	238
7.4	+8MATE GrantMA workflows for employees .....	239
7.4.1	Manage my requests (cockpit) .....	240
7.4.2	Request file server access rights .....	242
7.4.3	Request group memberships .....	246
7.4.4	Request new directories .....	249
7.4.5	Create a user account as an HR employee .....	252
7.4.6	Order script-based services .....	256
7.5	+8MATE GrantMA: workflows for data owner/administrators .....	260
7.5.1	Approve or reject requests (cockpit) .....	260
7.5.2	Informing approvers of new requests via email .....	262
7.5.3	Approving or denying a request in the self service portal .....	263
<b>8</b>	<b>User Provisioning .....</b>	<b>266</b>
8.1	Active Directory .....	267
8.1.1	Administrator .....	267
8.1.1.1	Create an user account .....	267
8.1.1.2	Create groups and add users .....	270

8.1.1.3	Manage group memberships .....	273
8.1.1.4	Delete empty groups .....	275
8.1.1.5	Move objects in Active Directory .....	278
8.1.1.6	Reduce multiple groups to one group .....	279
8.1.1.7	Change password options .....	281
8.1.1.8	Deactivate user accounts in bulk (web client) .....	283
8.1.1.9	Delete accounts in bulk (soft delete) (web client) .....	285
8.1.1.10	Change password options in bulk (web client) .....	287
8.1.1.11	Modify attributes in bulk (web client) .....	289
8.1.1.12	Remove unresolved SIDs in bulk (web client) .....	292
8.1.1.13	Remove direct permissions in bulk (web client) .....	295
8.1.1.14	Remove group memberships in bulk (web client) .....	298
8.1.1.15	Remove "everyone" permissions in bulk (web client) .....	300
8.1.1.16	Create a new department profile (administrator) .....	303
8.1.1.17	Execute scripts for directories in bulk (web client) .....	306
8.1.1.18	Execute scripts on user accounts in bulk (web client) .....	308
8.1.1.19	Edit temporary group memberships (web client) .....	310
8.1.1.20	Edit computer accounts .....	312
8.1.1.21	Delete computer accounts .....	314
8.1.2	Helpdesk .....	315
8.1.2.1	Reset passwords .....	315
8.1.2.2	Reset passwords in bulk (web client) .....	317
8.1.2.3	Unlock an user account .....	319
8.1.2.4	Unlock user accounts (web client) .....	321



8.1.2.5	Deactivate an user account .....	323
8.1.2.6	Modify group and user attributes .....	325
8.1.2.7	"Soft" delete a user .....	327
8.1.2.8	Remove a user and its permissions .....	329
8.1.3	Data Owner/Manager .....	331
8.1.3.1	Reset users' passwords (cockpit) .....	331
8.1.3.2	Change account data of users (cockpit) .....	333
8.1.3.3	Deactivate users (cockpit) .....	335
8.1.3.4	Pause user (cockpit) .....	337
8.1.3.5	Create a new user (cockpit) .....	339
8.1.3.6	Assign a department profile to users (cockpit) .....	341
8.1.3.7	Change your own account information (cockpit) .....	343
8.1.3.8	Manage my employees (cockpit) .....	344
8.1.3.9	Add group memberships (cockpit) .....	345
8.1.3.10	Remove group memberships (cockpit) .....	347
8.2	File server .....	349
8.2.1	Data owner .....	349
8.2.1.1	Grant and remove file server access rights .....	349
8.2.1.2	Create a protected file server directory .....	353
8.2.2	Administrator .....	357
8.2.2.1	Remove multiple access rights on file server directories .....	357
8.2.2.2	Remove direct permissions .....	361
8.2.2.3	Remove corrupted inheritance .....	364
8.2.2.4	Identify and delete unresolved SIDs .....	367
8.2.2.5	Determine naming conventions for access groups .....	371

8.2.2.6	Change directory ownership .....	372
8.2.2.7	Identify errors in inheritance in Analyze & Act and fix them in bulk .....	374
8.3	+8MATE for Exchange .....	377
8.3.1	Help Desk .....	377
8.3.1.1	Create a mailbox (e-mail enable users) .....	377
8.3.1.2	Change mailbox permissions .....	379
8.3.1.3	Manage out of office notices .....	381
8.3.1.4	Manage mailbox and e-mail size .....	383
8.3.1.5	Manage e-mail addresses .....	385
8.3.1.6	Manage distribution group memberships .....	387
8.3.1.7	Manage distribution group permissions .....	389
8.3.1.8	Modify moderation of distribution groups .....	391
8.3.1.9	Change the manager of distribution groups .....	393
8.3.1.10	Create and delete contacts .....	395
8.4	+8MATE for SharePoint .....	399
8.4.1	Data Owner .....	399
8.4.1.1	Manage SharePoint permissions .....	399
8.4.2	Administrator .....	401
8.4.2.1	Create SharePoint groups .....	401
8.4.2.2	Determine naming conventions for access groups .....	404
9	<b>Threat &amp; Gap Management .....</b>	<b>406</b>
9.1	+8MATE Clean! .....	407
9.1.1	Identify file path names that are too long .....	407
9.1.2	Archive old file server data .....	408
9.1.3	Push permissions to empty sub-directories through inheritance .....	409
9.1.4	Delete empty file server directories .....	410
9.1.5	Correct non-canonical access rights .....	411

9.1.6	Replace non-canonical permissions through overarching rights .....	412
9.1.7	Automatically replace critical access rights .....	413
9.1.8	Identify NULL DACLs and replace them with higher level permissions .....	414
9.1.9	Replace divergent access rights on a file server .....	415
9.1.10	Delete divergent access rights .....	416
9.1.11	Automatically remove critical permissions .....	417
9.1.12	Remove direct permissions .....	418
9.1.13	Replace direct permissions with group memberships .....	419
9.1.14	Activate inheritance for directories with identical access rights .....	420
9.1.15	Remove permission gaps by aligning directory owners .....	421
9.1.16	Automatically reduce the depth of permissions on file servers .....	422
<b>10</b>	<b>8MAN Application Integration .....</b>	<b>424</b>
10.1	+8MATE Matrix 42 .....	425
10.1.1	For Employees .....	425
10.1.1.1	Order Fileserver Access Rights with Matrix 42 .....	425
10.1.2	For Data Owners and Administrators .....	425
10.1.2.1	Accept or reject an inquiry in Matrix 42 .....	425
<b>11</b>	<b>Appendix .....</b>	<b>426</b>
11.1	Software license acknowledgments .....	427
	Keywords .....	0

# 1. Why?



## 1.1 Protecting data, information and knowledge

Your firewall protects you from external threats. 8MAN access rights management protects data, information and knowledge within your network.

**Access rights management answers three central questions:**

### Personal level

Who has access?

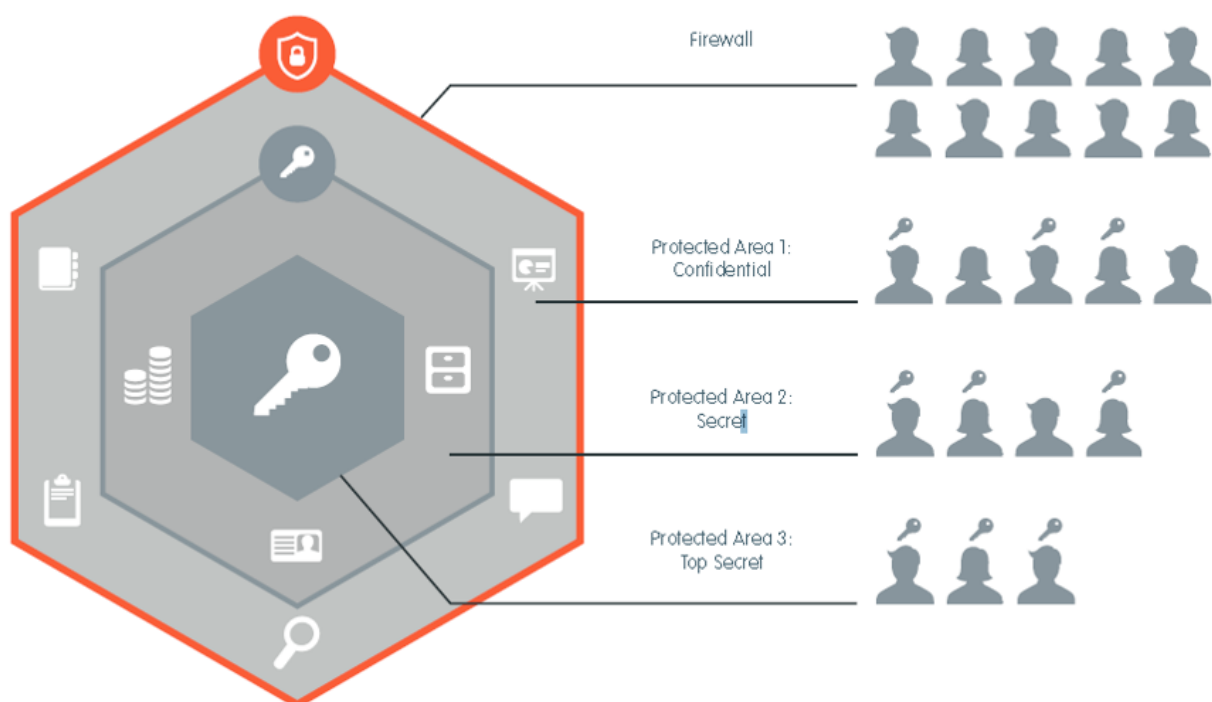
### Directory level

What do they have access to?

### Decision level

Who should have access to what?

**Access rights management prevents unauthorized access to data and optimizes security relevant processes within your company network.**



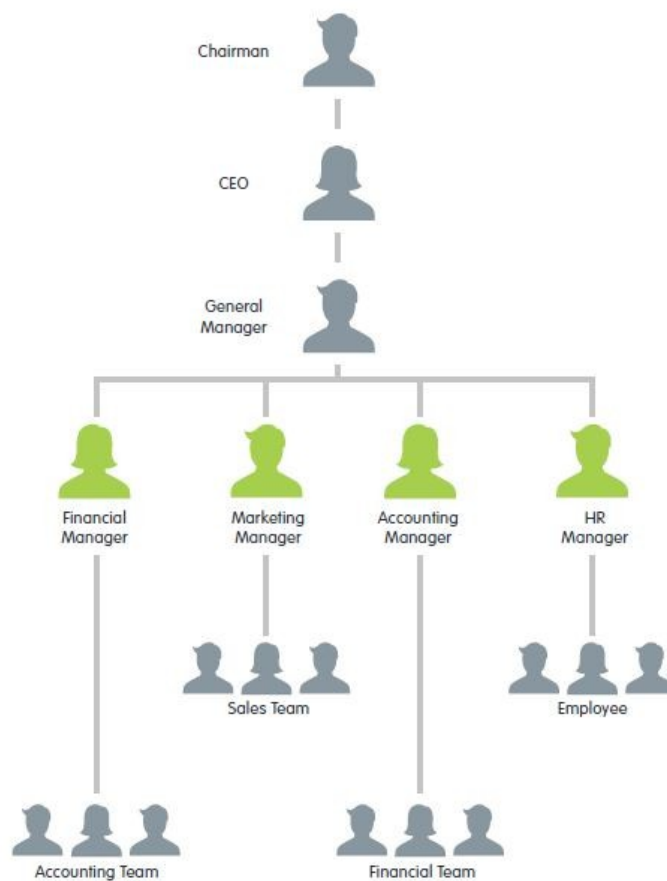
## 1.2 Decentralize security expertise

Security officers usually don't know where important data is stored or who has access to it.



8MAN access rights management delegates this responsibility to decision makers within your organization. They assign access rights and hold security expertise within your company.

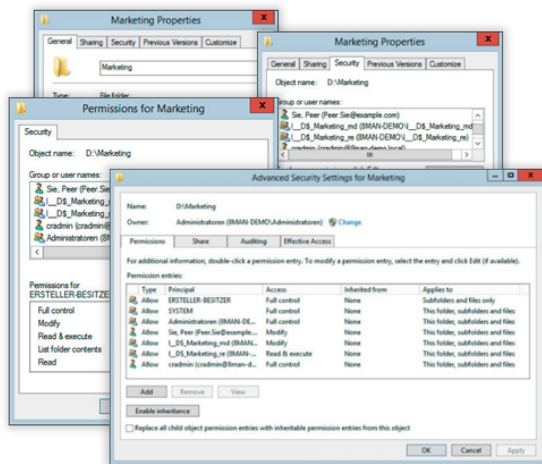
**With 8MAN managers become data protectors:**



## 1.3 Simplify Security

Security measures are usually not adhered to if they are cumbersome and inefficient. Access Rights Management automates processes and unifies two opposing forces: Security + Efficiency.

**Access rights management with native tools:**



**8MAN Access Rights Management:**

NTFS		Inheritance	Full Control	Modify	Read & execute	Read	Write	Special permissions
<b>All permissions</b>								
Full Control			✓	✓	✓	✓	✓	✓
Special permissions			✓	✓	✓	✓	✓	✓
Modify			✓	✓	✓	✓	✓	✓
Sie, Peer (Peer Sie)			✓	✓	✓	✓	✓	✓
<b>L_DS_Marketing_md</b>			✓	✓	✓	✓	✓	✓
BMAN Group			✓	✓	✓	✓	✓	✓
Ann (Ann.Geber)			✓	✓	✓	✓	✓	✓
Ben Zin			✓	✓	✓	✓	✓	✓
Ka, Ede (Ede Ka)			✓	✓	✓	✓	✓	✓
Dee, Dan (Dan Dee)			✓	✓	✓	✓	✓	✓
Krise, Christiane (Christiane...)			✓	✓	✓	✓	✓	✓
Fred Chen (Fred.Chen)			✓	✓	✓	✓	✓	✓
Frido Fleia (Frido.Fleia)			✓	✓	✓	✓	✓	✓
Dampf, Hans (Hans Dampf)			✓	✓	✓	✓	✓	✓
Becher, Joe Kurt (Joe Kurt Be...)			✓	✓	✓	✓	✓	✓
Maria Makketing (Maria.Mak...)			✓	✓	✓	✓	✓	✓
Hacke, Petra (Petra.Hacke)			✓	✓	✓	✓	✓	✓
Sam Sales der Boss (Sam.Sal...)			✓	✓	✓	✓	✓	✓
Read & execute			✓	✓	✓	✓	✓	✓

**8MAN Access Rights Management makes security efficient:**

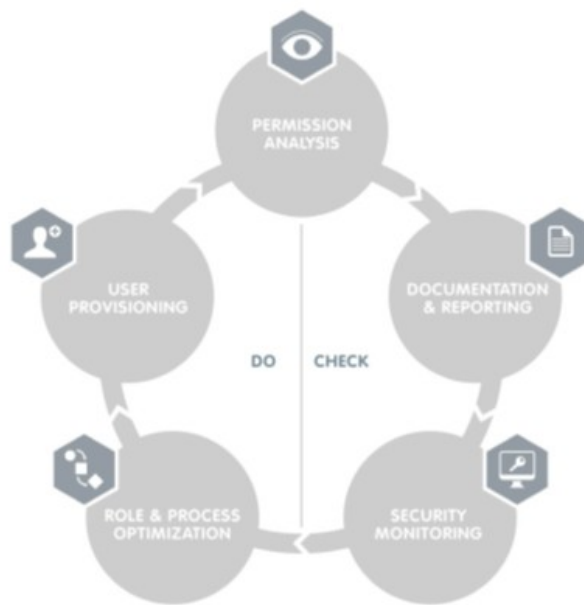
Task	With Native Tools	With 8MAN
Capture the access rights situation in your network	n/a	3 minutes
Track every change to permissions and access rights	n/a	2 minutes
Make security relevant processes in a network transparent	n/a	2 minutes
Implementation of standard processes:		
User Provisioning, Documentation and audit-proof reports	Per request, inconsistent and time consuming	Automated, standardized and fast





## 2. The Core Disciplines of ARM





**8MAN Access Rights Management is based on five core disciplines:**

### PERMISSION ANALYSIS

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

### DOCUMENTATION & REPORTING

Records any access rights activity in our logbook and creates audit proof reports

### SECURITY MONITORING

Monitors security relevant actions in Active Directory and on your file servers.

### ROLE & PROCESS OPTIMIZATION

Shortens your access rights management process and involves only the most important actors.

### USER PROVISIONING

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

## 2.1 Permission Analysis



8MAN 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 and Exchange. With this knowledge, you are able to take action and protect your company from internal security incidents.

8MAN 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.

### **Available in all product versions:**

Permission Analysis is part of every 8MAN Version for Active Directory and file server.

If you want to analyze and administrate other technologies with 8MAN we recommend the following Add-On's:

[8MATE for Exchange](#)

[8MATE for SharePoint](#)

### 2.2 Documentation & Reporting



8MAN documents the activities in Active Directory, the file servers, SharePoint and Exchange. 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

[To the services](#)

#### **Available in all product versions:**

Documentation and Reporting is part of every 8MAN Version for Active Directory and file server.

If you want to analyze and administrate other technologies with 8MAN we recommend the following Add-On's:

[8MATE for Exchange](#)

[8MATE for SharePoint](#)

## 2.3 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 Active Directory Logga, File Server Logga and Exchange Logga, 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 8MAN are recorded. Based on the information obtained, your Access Rights Management process can be optimized. With Alerts (FS and AD Logga) you are informed proactive of critical events.

Security Monitoring can be combined with all base versions. It can be added with the following add-ons:

### Active Directory

[8MATE AD Logga](#)

### Fileserver

[8MATE FS Logga](#)

### Exchange

[8MATE Exchange Logga](#)

## 2.4 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 administrator. By introducing a role concept for analysing 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 analyse or assign access rights to their staff.

An employee can use the [8MATE GrantMA](#) add-on module to request access rights via a Web portal. The data owner then decides on the access rights in the department with a simple workflow.

### **Role & Process Optimization is only available for 8MAN Enterprise:**

There is one Add-On available:

[8MATE GranMA](#): The ARMSelf Service Portal

[workflows for employees](#)

[To the services](#)

## 2.5 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 virtual servers as defined in the AD groups are issued at the same time. 8MAN generates a suitable email account so that the new colleague can start work immediately. 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.





# 3. Additional ARM disciplines





### **Threat & Gap Management**

Removes security relevant permission errors automatically and standardizes the access rights system according to your demands.



### **8MAN Ressource Integration**

Enables the administration of additional resources.



### **8MAN Application Integration**

Enables the automatic collaboration with other applications in your software landscape.

### 3.1 Resource Integration



#### Resource Integration

Enables the administration of additional resources.

### 3.1.1 +8MATE for Exchange



#### Problem

The administration of permissions with Microsoft Exchange is complex. The available Microsoft resources do not allow for a holistic view of access rights to public files and mailboxes. The administration of access rights is cumbersome and time-consuming.

#### Solution

8MATE for Exchange enables you to expand 8MAN to email resources. Thus, analysis and administration of permissions take place centrally and in line with the access management for other applications. In the familiar 8MAN overview, you see at a glance who is authorised to access public folders, mailboxes, mailbox folders and, for instance, calendars.

The administration of Exchange is essential to the onboarding process. The setup of mailboxes and assignment of permissions takes place right in 8MAN. Changes made with 8MAN are documented and are audit-proof.

Apart from the analysis and administration of permissions in Exchange, 8MATE has additional features:

- The ability to create Out-of-Office notifications without accessing an email account.
- Listing of proxies for mailboxes and Send As permissions.
- Administration of mail box sizes

### 3.1.2 +8MATE for SharePoint



#### Problem

The analysis and administration of authorisations on SharePoint is a complex matter. The on-board Microsoft resources do not allow for a holistic view of the authorised permissions of individual SharePoint resources. The administration of permissions is cumbersome and time-consuming. Changes that have been made in the permission structure are not discernible.

#### Solution

8MATE for SharePoint integrates all SharePoint resources in 8MAN. The analysis and administration of permissions takes place centrally and in line with the access rights management of other applications. You will benefit immensely from 8MAN's unique ability to display, analyse and change access rights. 8MAN displays the permissions in a tree structure. This allows you to quickly see who is authorised to access a given SharePoint resource. Using the scan comparison report, you can find out who has made changes to permissions and what they were, and you obtain a protocol of all activities that have been undertaken. 8MATE for SharePoint allows you to assign all permissions in the 8MAN interface. By using the Group Wizard and assigning naming conventions, you can standardise your authorisation assignment process.

### 3.1.3 +8MATE for Dynamics NAV



#### Problem

Microsoft Dynamics NAV contains business information that not everyone should see. Depending on the development stage of the ERP solution, project budgets, purchase price lists, annual balance sheets or personal data of employees, suppliers or customers are stored there.

Efficient access rights management is difficult with on-board resources. Users are members of various authorization groups, which in turn can be members of other authorization groups. In addition, the ERP solution uses company-specific permission sets, which are also used to assign access rights. If you want to know which users have which access rights, a corresponding number of sources have to be consolidated. The answer to the actually very simple question: "Who has access to where" becomes a costly and time-consuming search project.

#### Solution

8MATE Dynamics NAV integrates the permission analysis of the ERP system into 8MAN. As usual, all access rights are displayed in a flat list. In the first step, the module offers services in the area of Permission Analysis and Documentation & Reporting:

##### *Permission Analysis*

- Identify access rights to NAV resources
- Identify multiple access rights
- Analyzing the access rights situation from the past

##### *Documentation & Reporting*

- Report: Who has access where?
- Report: Where do users/groups have access?

### 3.1.4 Easy Connect - integrating any resources

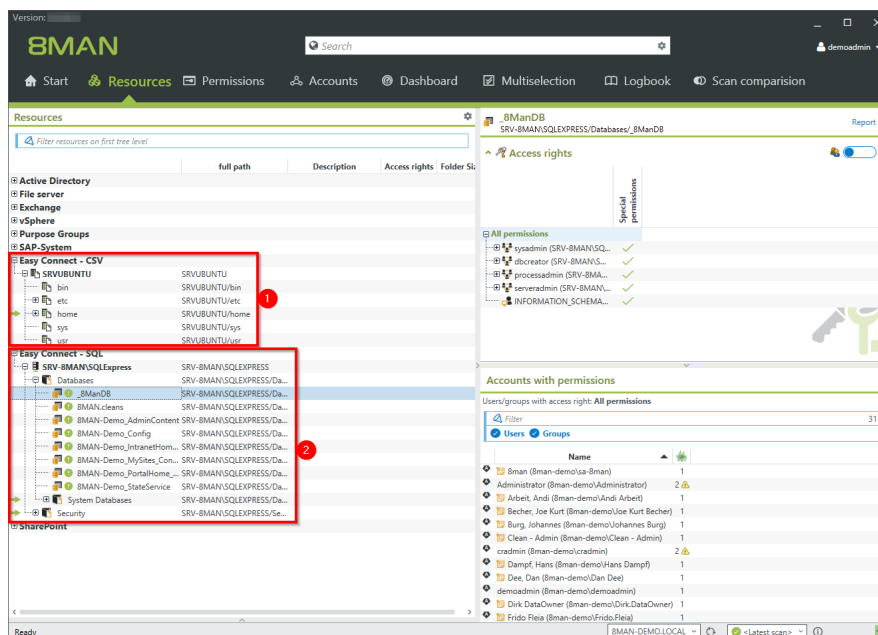
#### Background / Value

Integrate further resources to 8MAN with Easy Connect. You will get the 8MAN-typical overview, analysis and reporting functionalities for these. The question "Who has access where?" can be answered more comprehensive and much easier with one single solution. Import data from a CSV-file or via SQL-scripts manual or automatically.

The following reports are supported for Easy Connect resources:

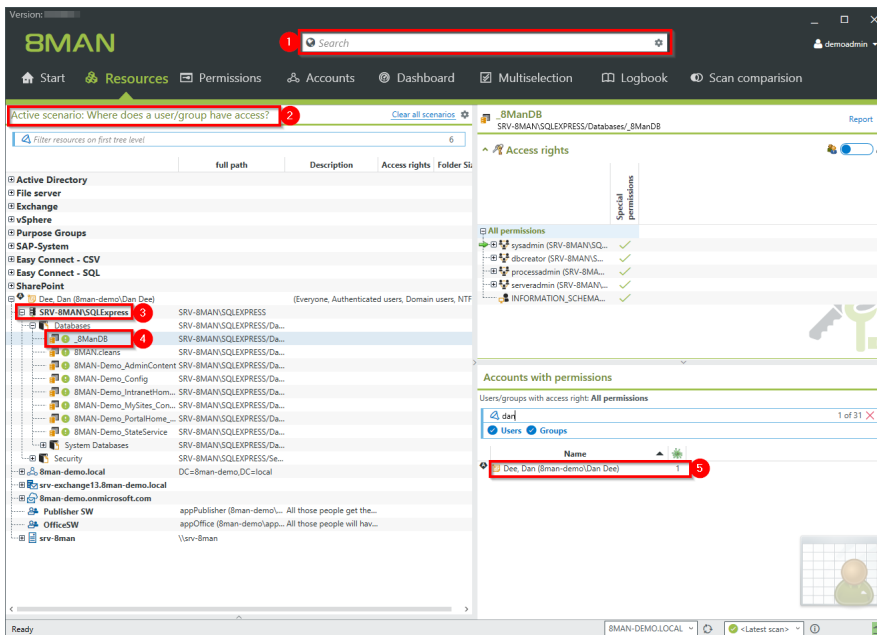
- "Who has access where?"
- "Where has the user/group access?"
- "Account Details"

#### 3.1.4.1 Analysing Easy Connect resources



The example shows access rights information imported from a Linux file system and a MS SQL-server.

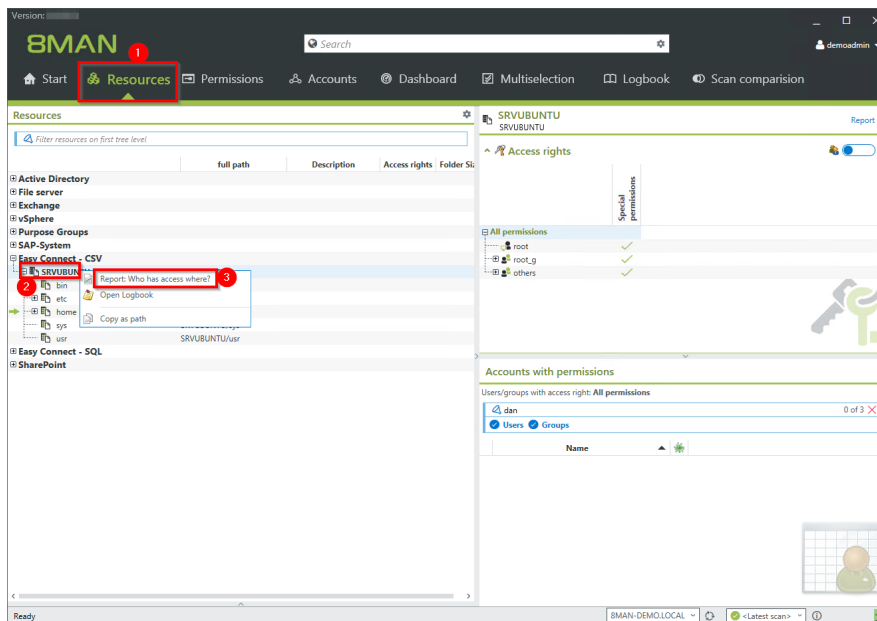
1. Linux file system information are imported from a CSV-file.
2. SQL-server access rights information are imported via SQL-script.



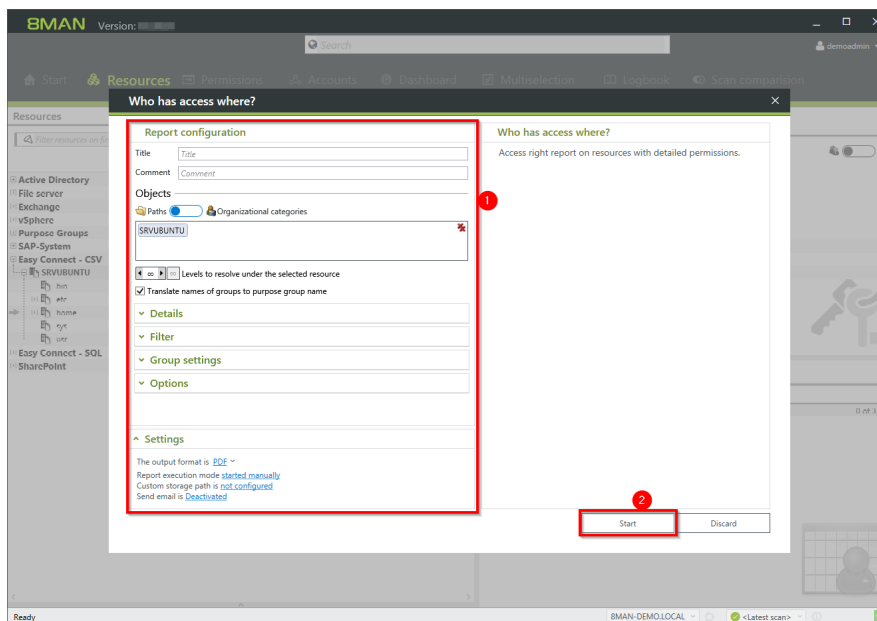
1. 8MAN search includes easy connect resources.
2. The scenario "Where does a user/group have access?" includes Easy Connect resources.
3. The scenario includes the imported SQL-server resource.
4. Navigate through Easy Connect resources.
5. Access rights of the desired user are shown in 8MAN-typical style.



### 3.1.4.2 Create a report for an Easy Connect Resource



1. Choose "Resource" view
2. Select a resource, e.g. "SRVUBUNTU".
3. Choose the report: "Who has access where?" from the context menu.



1. Configure the report. Options are the same as on any "built-in" resource.
2. Start the report.

### 3.2 8MAN Application Integration



#### **8MAN Application Integration**

Enables the automatic collaboration with other applications in your software landscape.

### 3.2.1 +8MATE Matrix 42



The 8MATE Matrix42 connects 8MAN with the IT Service Management Solution Matrix 42. In the solution built by Futuredat GmbH employees can order file server permissions by using the Matrix42 self service portal. Data Owners or Administrators check the order in a standardized process. In case of approval 8MAN starts automatically and creates the desired permissions on the file server. The whole process follows Microsoft Best Practice: For each permission an Active Directory group is created. All activities are tracked in Matrix42 and the 8MAN logbook.

### 3.3 Threat & Gap Management



#### Threat & Gap Management

Removes security relevant permission errors automatically and standardizes the access rights system according to your demands.

### 3.3.1 8MATE Clean!



#### Problem

The correction of permission inconsistencies and mistakes on file servers is only possible with extreme difficulty and effort. The implementation of best practices to solve these issues frequently fails at two hurdles: knowledge and time. Furthermore, classic Access Rights Management (ARM) has always only been focusing at the folder level.

#### Solution

The 8MATE Clean! starts a process that leads to a secure and standardized file server and permissions structure. Through a series of clear decisions and parameters, you define how security and structural problems will be resolved in your environment. Your requirements and the 8MAN best practices will be automatically implemented. Additionally, the archiving of stale or obsolete data is possible. The benefit being, the lesser the data, the simpler the administration.

#### What does 8MATE Clean! achieve?

- Archives old file server data
- Removes automatically critical permissions
- Remove or replace direct permissions
- Standardizes existing permissions on your file server

**8MATE Clean! Is only available in combination with professional services. Please contact your local sales representative for further information.**



## 4. Permission analysis



### 4.1 Active Directory

Active Directory is the leading system for administrators in Windows networks. 8MAN focuses on the analysis of users and groups and also on the creation of these objects. This happens in a scalable way across your entire domain and organizational structure. The 8MANgroup wizard can automatically create the appropriate security groups in Active directory.



## 4.1.1 Services for Administrators

### 4.1.1.1 Visualize nested group structures

#### Background / Value

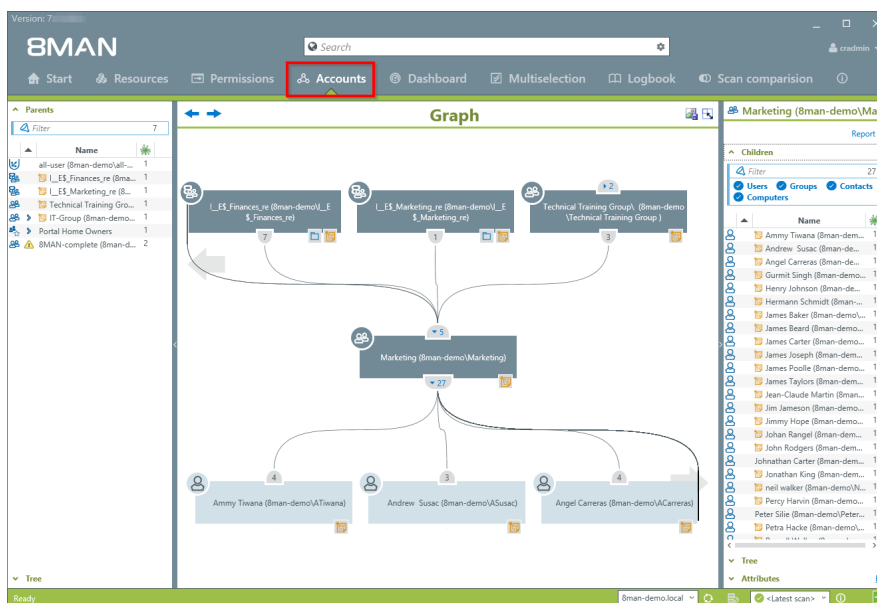
One of the most important concepts of every Active Directory (AD) is group structure. Administrators use groups to assign access rights to resources to individual users. This can create recursions or loops in your group structure. For example: The group "Marketing" assigns access rights to the appropriate file server directories for that department. At the same time this group is also a member (in a recursion) of the group "4th floor WiFi". The 8MAN graph shows and highlights the recursion within your Active Directory thereby helping you recognize errors and correct mistakes.

#### Additional Services

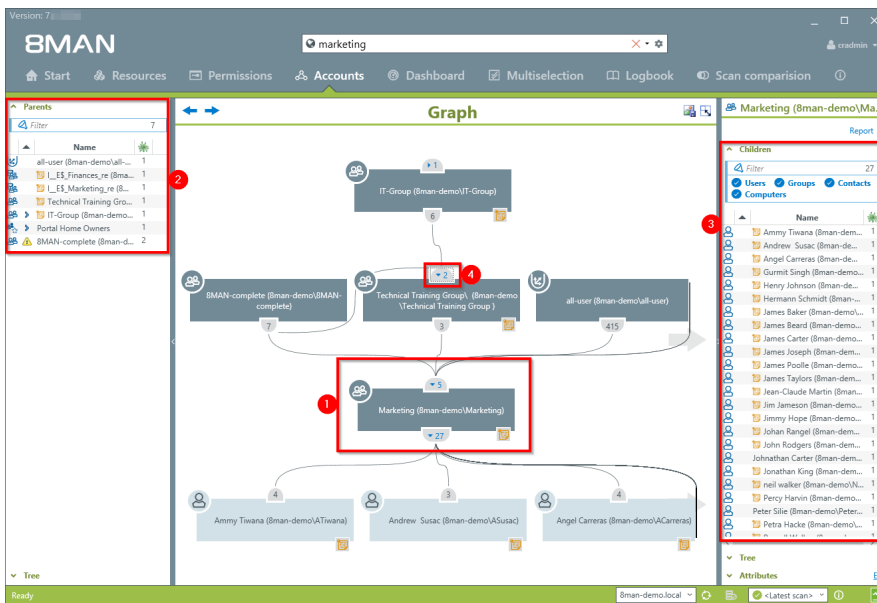
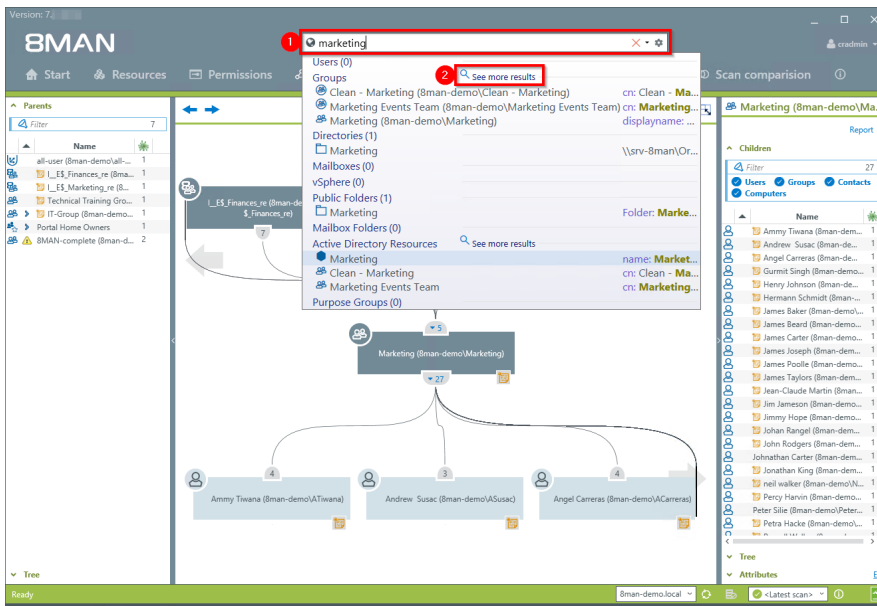
[Identifying the depth of nesting in your AD](#)

[Identifying recursive groups](#)

#### Step by step process



Switch to Accounts in the AD Graph view.



### 4.1.1.2 Compare two different access rights situations (Scan Comparison)

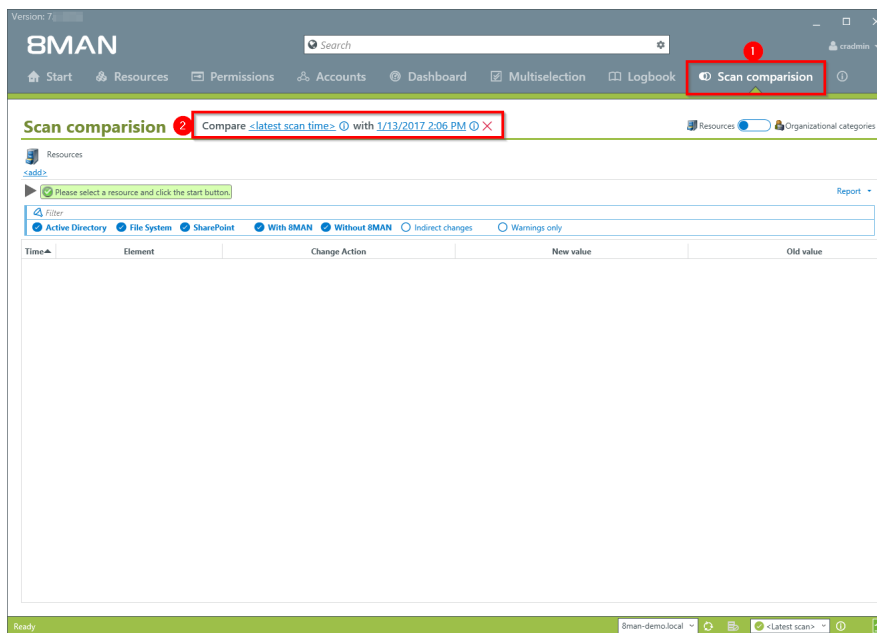
#### Background / Value

The scan comparison compares AD scans at two different points in time and shows you how your access rights situation has changed.

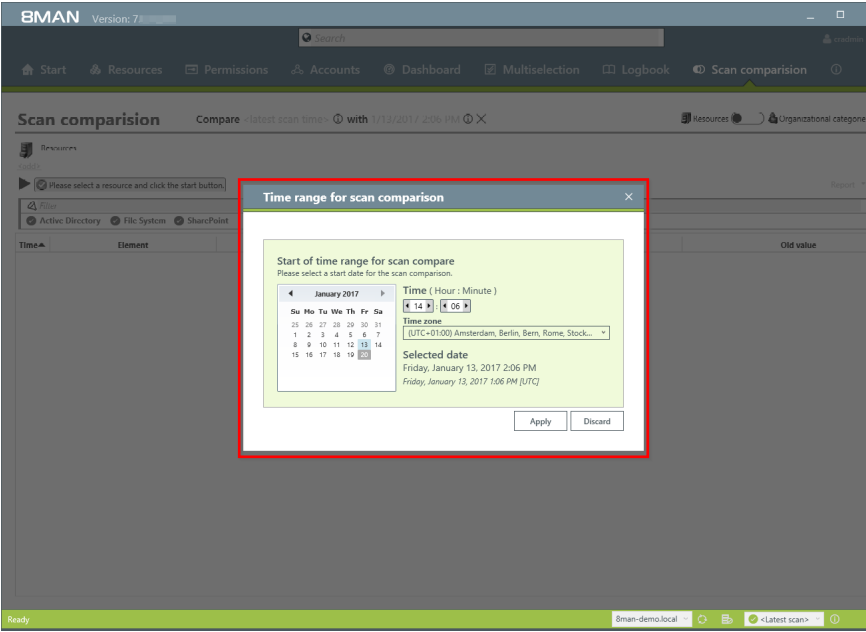
#### Additional Services

The scan comparison only takes two separate points in time into account. In order to be able to monitor all administrative actions made within a given time period to access rights on file servers you would require the 8MATE FS Logga. Alternatively to the Scan comparison you can use the [Report on Permission Differences](#).

#### Step by step process

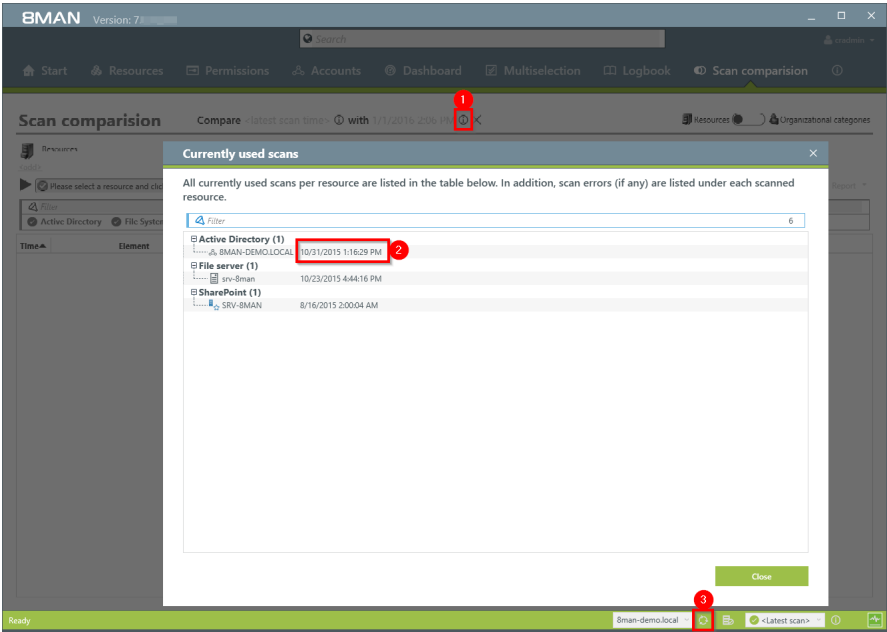


1. Click on "Scan comparison".
2. Select the two scans that you want to compare.



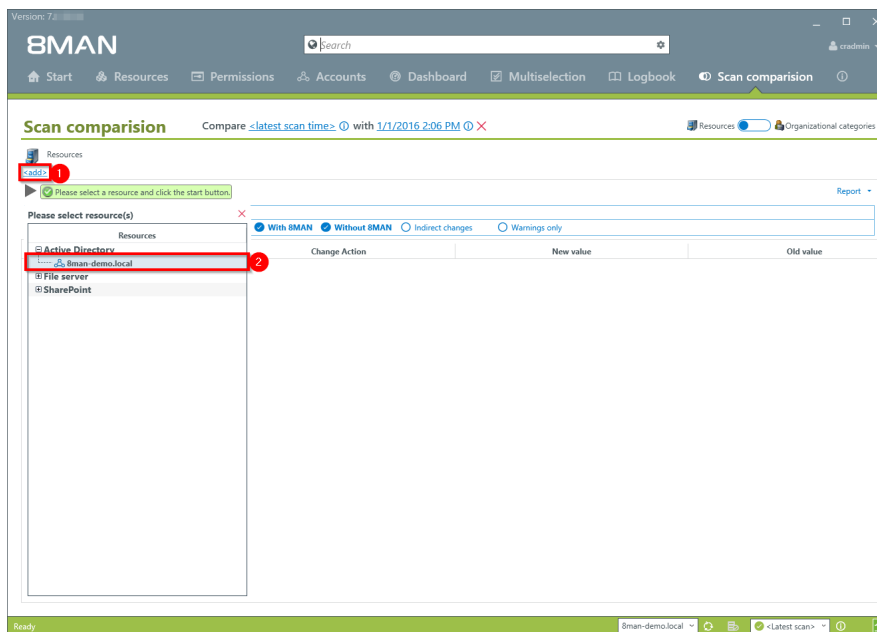
Select the date and time of both scans.

1. Ready

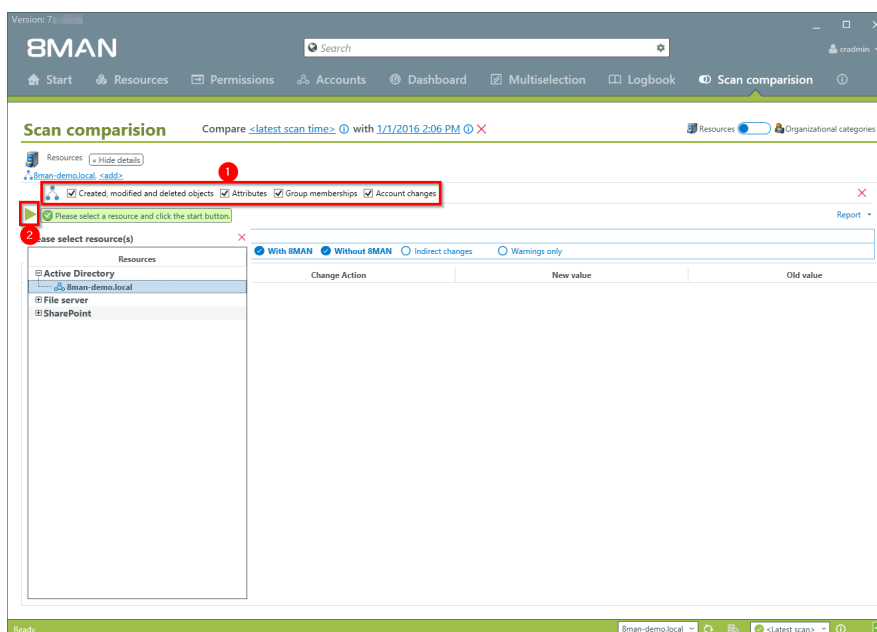


The comparison always compares existing scans.

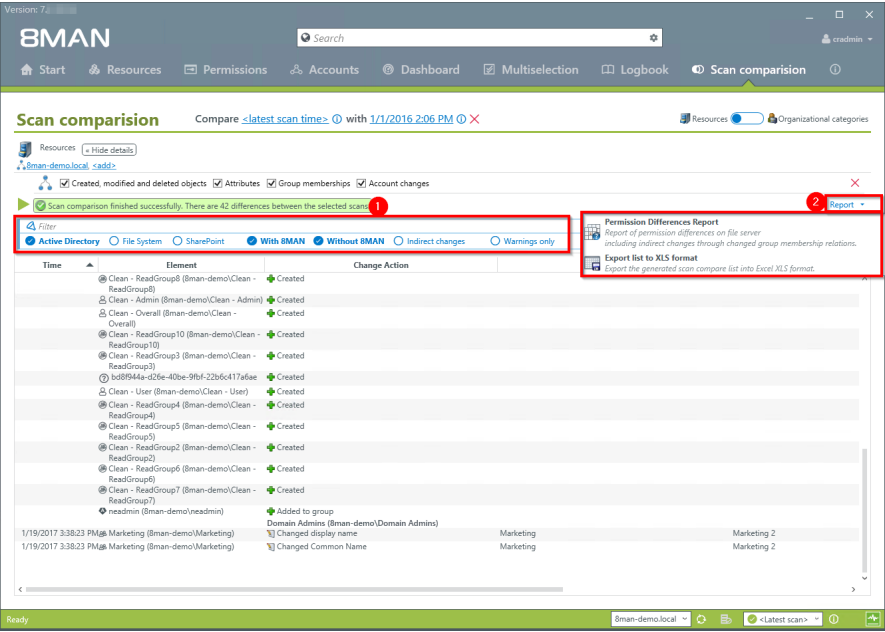
1. Click on the information symbol.
2. Date and time of the selected scan is indicated on the right-hand side.
3. In order to maximize accuracy you should run a current AD Scan before starting the scan comparison.



1. Click on "add resources".
2. Select 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" and /or export the results to .XLS.

### 4.1.1.3 Identify overprivileged users (based on Kerberos token size)

#### Background / Value

The size of a Kerberos token is a good indicator for identifying users with excessive access rights. The more group memberships a user has, the bigger their Kerberos token. Even if a group membership does not automatically grant privileges, it is worthwhile analyzing the listed users. Additionally, if a user exceeds his maximum Kerberos token size he can no longer register on the network.

#### Step by step process

Version: 7.0.0

8MAN

Start Resources Permissions Accounts **Dashboard** Multiselection Logbook Scan comparison

Reporting

Active Directory

- Inactive accounts
- Local accounts
- Users and groups (Kerberos, Last login)

File server

- All 'Authenticated users' permissions
- All 'Everyone' permissions
- All owner not administrator
- All users with direct access
- New and unused shares
- Unresolved SIDs

Depth of nested groups

Groups with members (w/o recursions) 103

Empty groups 76

Groups in recursions 3

The largest group (Domain Users (Bman-demo\Domain Users)) 428

Built-in security groups 27

Global security groups 76

Universal security groups 35

Local security groups 42

Global distribution groups 0

Universal distribution groups 2

Local distribution groups 0

OU / Contacts / More

Computers 4

Computers (disabled) 0

Contacts 0

Foreign users 0

Organizational Units 12

**Top 5 Kerberos Tokens (Bytes)**

Quinton Patton (Bman-demo\QPatton)	1594
Jones, Gareth (Bman-demo\Gareth Jones)	1528
Administrator (Bman-demo\Administrator)	1520
SP_Farm (Bman-demo\SP_Farm)	1488
Gore, Frank (Bman-demo\Frank Gore)	1480

Top 5 Oldest logons

SP_SearchService (Bman-demo\SP_SearchService)	5/16/2014 2:37:14 PM
Eric Reid (Bman-demo\EReid)	10/10/2014 2:28:02 PM
Akbar, Mohammed (Bman-demo\Mohammed Akbar)	10/27/2014 8:27:50 AM
Quinton Patton (Bman-demo\QPatton)	11/25/2014 2:31:09 PM

Ready Bman-demo.local

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

Version: 7.0.0

8MAN

Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparison

Parents

Filter 12

Name

- all-user (Bman-demo\all-user) 1
- Domain Users (Bman-demo\Domain Users) 1
- Finance (Bman-demo\Finance) 1
- L\_ES\_HR\_Employees\_re (Bman-demo\L\_ES\_HR\_Employees\_re) 1
- L\_ES\_HR\_re (Bman-demo\L\_ES\_HR\_re) 1
- L\_ES\_Marketing\_Event (Bman-demo\L\_ES\_Marketing\_Event) 1
- L\_ES\_Marketing\_Files (Bman-demo\L\_ES\_Marketing\_Files) 1
- L\_ES\_R&D\_re (Bman-demo\L\_ES\_R&D\_re) 1
- Personnel Files (Bman-demo\Personnel Files) 1
- L\_ES\_Finances\_md (Bman-demo\L\_ES\_Finances\_md) 1
- L\_ES\_Finances\_v (Bman-demo\L\_ES\_Finances\_v) 1
- Users (Bman-demo\Users) 1

Graph

all-user (Bman-demo\all-user) 415

Domain Users (Bman-demo\Domain Users) 428

Finance (Bman-demo\Finance) 19

L\_ES\_HR\_Employees\_re (Bman-demo\L\_ES\_HR\_Employees\_re) 10

Quinton Patton (Bman-demo\QPatton) 10

Ready Bman-demo.local

1. 8MAN 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. If a group is very large, we recommend a flat list view.

#### 4.1.1.4 Identify nesting depth of groups

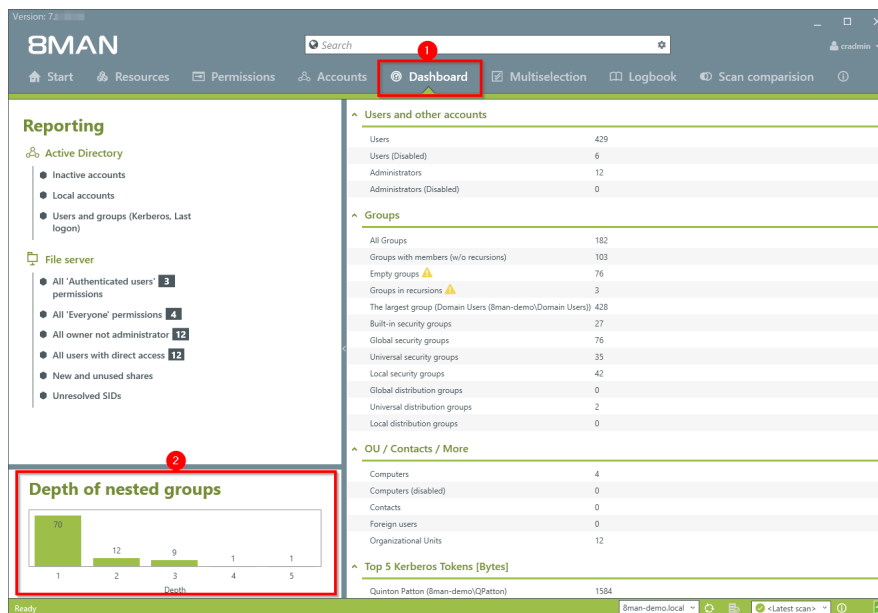
##### Background / Value

An AD that has grown over years often contains a large number of nested levels. The 8MAN dashboard shows nested groups up to level 10. According to Microsoft best-practice your AD should contain no more than 3 or 4 levels. 8MAN 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.

##### Additional services

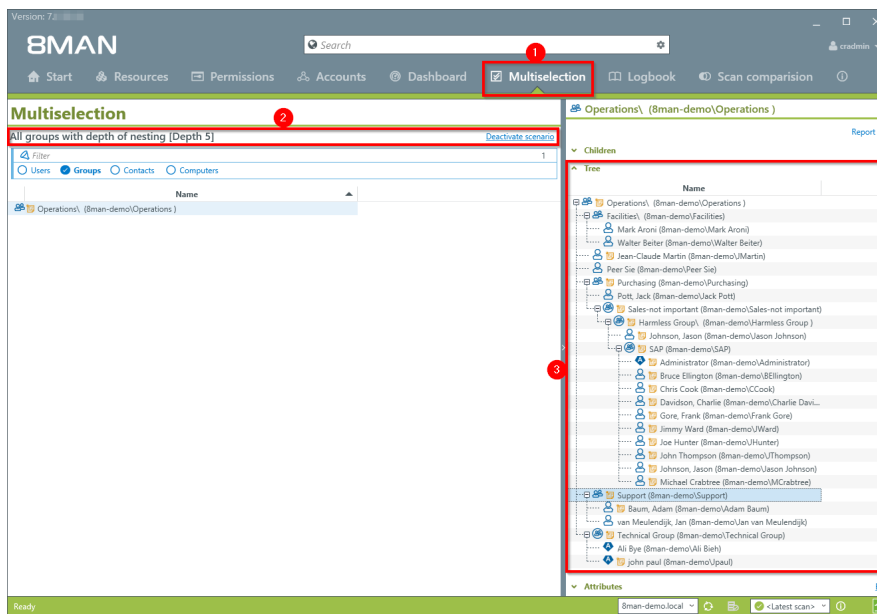
[Reducing several groups to one group](#)

##### Step by step process



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





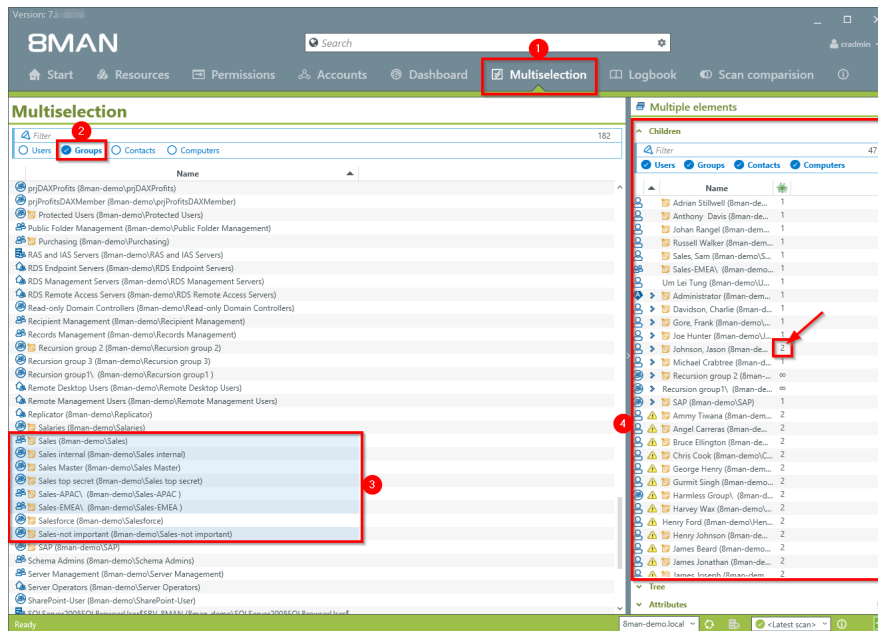
1. 8MAN automatically shows the Multiselection
1. In this scenario 8MAN automatically filters the groups by the selected nested level.
2. You can see the nested levels in the tree graph on the right hand side.

### 4.1.1.5 View members of different groups in one list

#### Background / Value

Multiselection allows you to select several groups allowing you an overview of all members.

#### Step by step process



1. Select Multiselection.
2. Filter by groups.
3. Select the desired groups.
4. You can see an overview of all "children" of all selected groups. 8MAN also indicates if any users are included in multiple groups, for example Jason Johnson.

### 4.1.1.6 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.

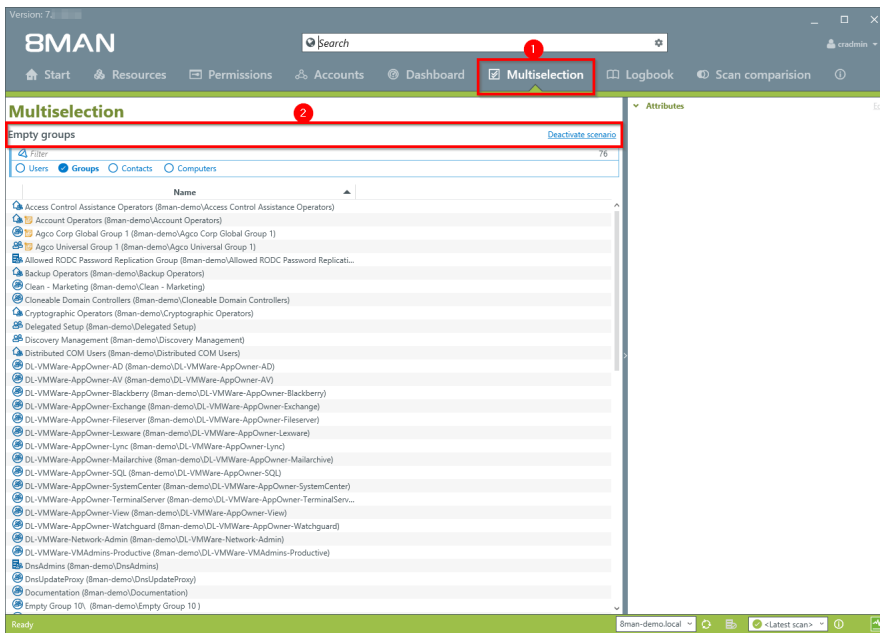


**Groups without members could include system groups. These should not be deleted.**

#### Step by step process

The screenshot displays the 8MAN software interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard' (highlighted with a red box and a red circle with the number 1), 'Multiselection', 'Logbook', and 'Scan comparison'. The 'Dashboard' section is active, showing a 'Reporting' sidebar on the left with 'Active Directory' and 'File server' categories. The main content area displays 'Users and other accounts' and 'Groups' sections. In the 'Groups' section, 'Empty groups' is highlighted with a red box and a red circle with the number 2. The 'Groups' section also lists 'All Groups', 'Groups with members (w/o recursions)', 'Groups in recursions', and 'The largest group (Domänen-Benutzer (8man-demo\Domänen-Benutzer))'. The 'Depth of nested groups' bar chart is visible in the bottom left corner.

1. Select the Dashboard.
2. Click on "Empty Groups".



1. 8MAN automatically shows the Multiselection.
2. The scenario "Empty Groups" is active. The listed Groups are all empty.

### 4.1.1.7 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. 8MAN automatically identifies all recursions in your system. We highly recommend removing the recursion by breaking the chain of circular group memberships.

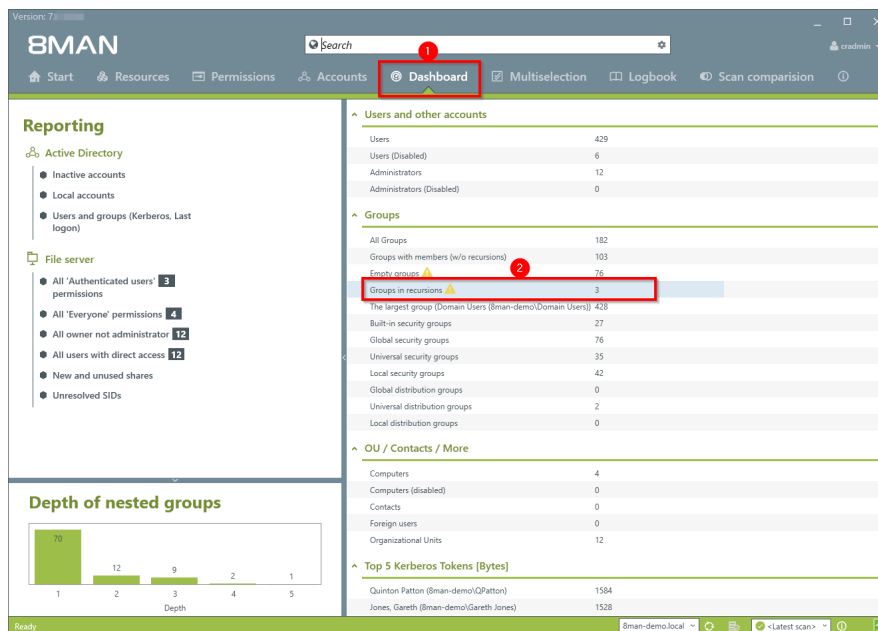
**TIPP: Only administrate with 8MAN and recursions can not happen anymore.**

#### Additional Services

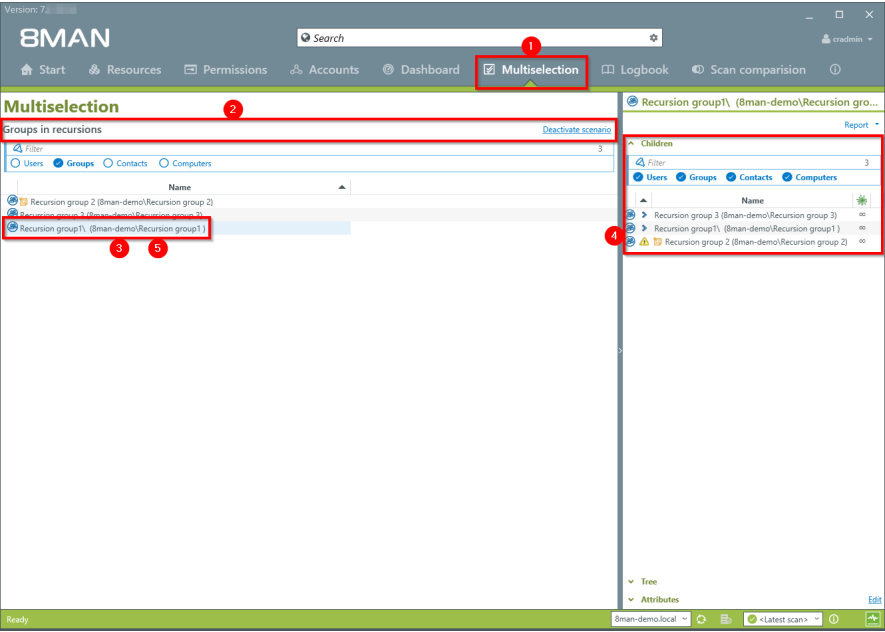
The deeper your group structure the more likely you are to have circular nested group structures. We therefore recommend keeping an eye on the number of nested group levels.

Identify groups in recursion (web client)

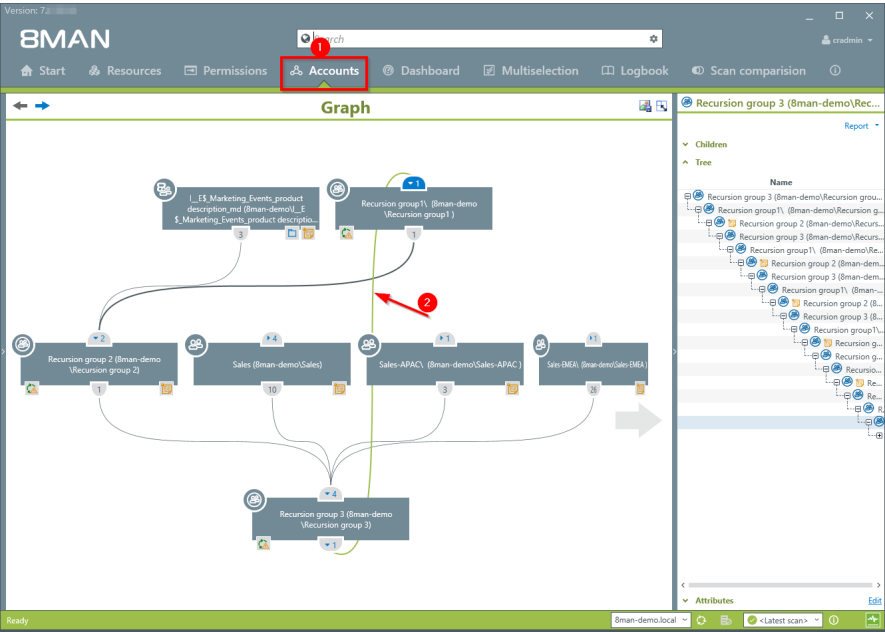
#### Step by step process



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



1. 8MAN automatically selects Multiselection.
2. The scenario "groups in recursions" is active. 8MAN lists all groups included in the recursion.
3. Click on a Group.
4. 8MAN lists all users and groups in the selected recursion
5. Double-click on a group.



1. 8MAN switches to the account view. You can see an example of a recursion across 3 levels.
2. The recursion is indicated by the green line.

#### 4.1.1.8 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. 8MAN automatically identifies all recursions in your system. We highly recommend removing the recursion by breaking the chain of circular group memberships.

**TIP: Administrative only with 8MAN and recursions can no longer occur.**

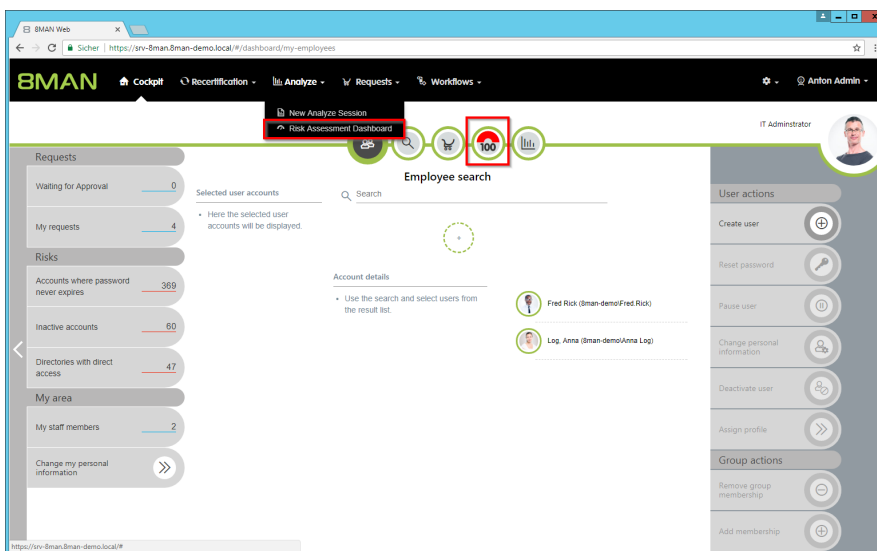
##### Additional Services

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.

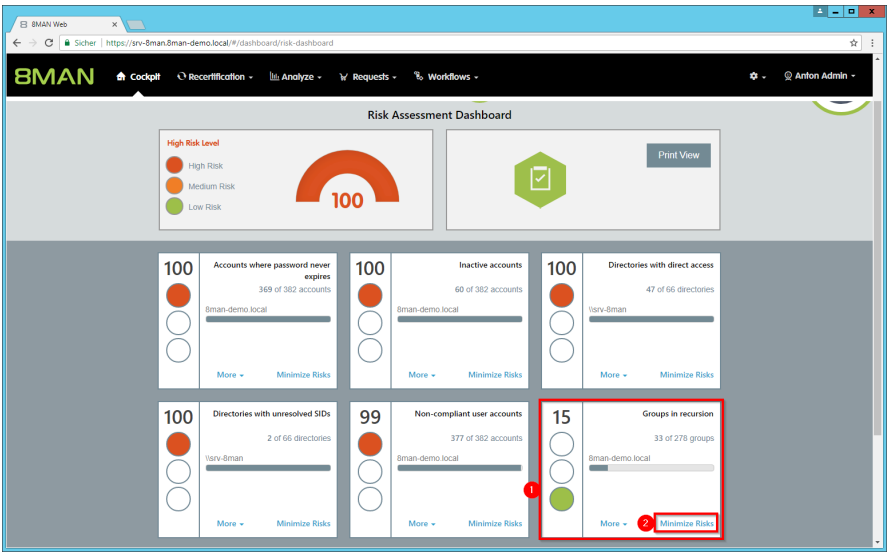
Identify recursive groups (rich client)

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

##### Step by step process

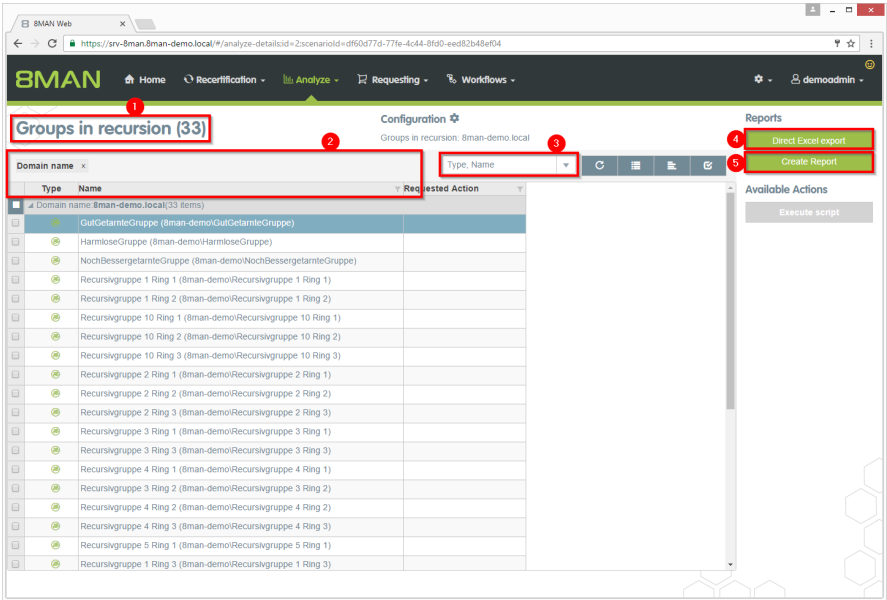


*Go to the Risk Assessment Dashboard.*



1. 8MAN 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. 8MAN 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.



#### 4.1.1.9 Identify users with never expiring passwords

##### Background / Value

One key security requirement within any organization is that passwords are changed regularly. 8MAN scans your domain for user accounts where this requirement has not been activated. You can view this information in our reports for "Users" and "Groups".

##### Additional Services

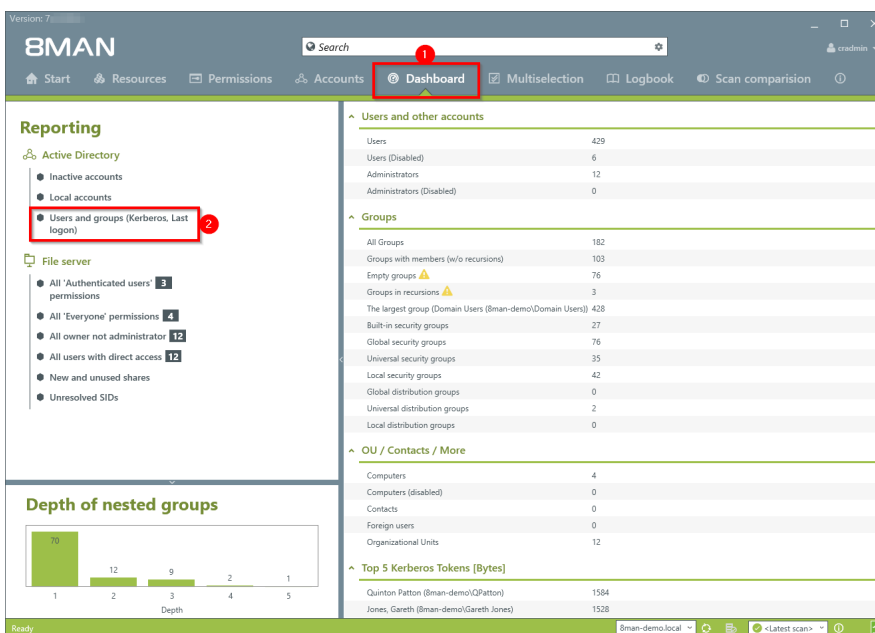
[Reset passwords](#)

[Change password options](#)

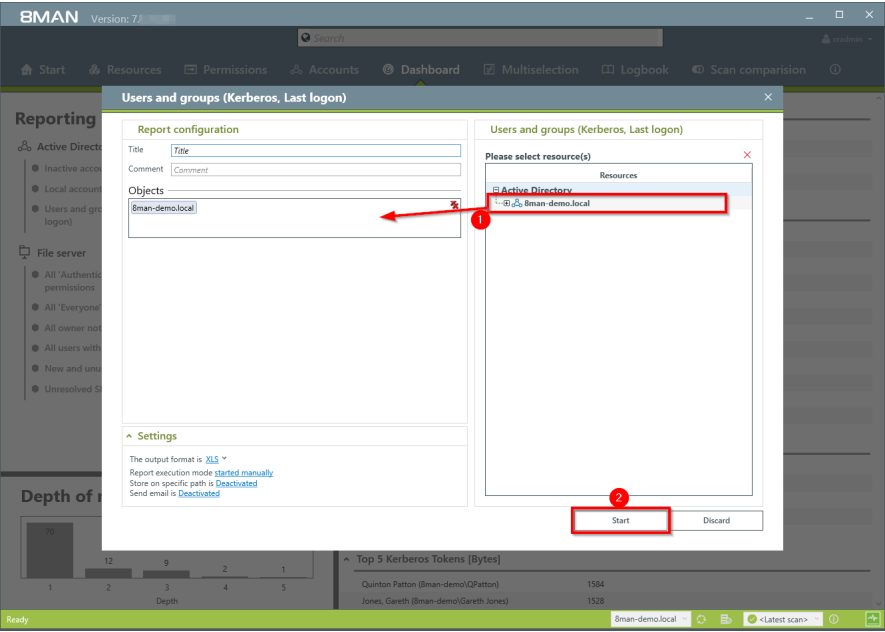
[Identify users with never expiring password](#) (web client)

[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.

PWDon't expire							
Report über alle Benutzer für	8man-demo.local						
DisplayName	IsDisabled	Account Expires	PWDon't exp.	Last Logon	Last Logon Timestamp	Type	Direct Members
Aber, Mark (8man-demo\Mark Aber)	Nein	Account never expires	N/A	N/A	N/A	Benutzer	
ADLogga Tester (8man-demo\ATester)	Nein	Account never expires	N/A	N/A	N/A	Benutzer	
Administrator (8man-demo\Administrator)	Nein	Account never expires	Ja	08.10.2016 21:00:02	08.10.2016 21:00:02	Benutzer	
Alien, Arnold (8man-demo\Arnold Alien)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Aloe, Vera (8man-demo\Vera Aloe)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Ander, Coni (8man-demo\Coni Ander)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Ander, Ole (8man-demo\Ole Ander)	Nein	Account never expires	Ja	N/A	10.03.2015 15:48:05	Benutzer	
Andrea Azubi (8man-demo\Andrea Azubi)	Ja	Account never expires	Ja	N/A	N/A	Benutzer	
Aner, Dominik (8man-demo\Dominik Aner)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Angebrandt, Angie (8man-demo\Angie Angebrandt)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Ann Essay (8man-demo\Ann Essay)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Anna Lyse (8man-demo\Anna Lyse)	Nein	Account never expires	Ja	N/A	07.03.2016 17:44:11	Benutzer	
Anna Ziese (8man-demo\Anna Ziese)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Ansgar Agentor (8man-demo\Aagentor)	Nein	Account never expires	Ja	N/A	07.03.2016 17:38:41	Benutzer	
Apfel, Adam (8man-demo\Adam Apfel)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Arbeit, Andi (8man-demo\Andi Arbeit)	Nein	Account never expires	Ja	12.03.2015 10:44:56	10.03.2015 16:51:26	Benutzer	
Arm, Armin (8man-demo\Armin Arm)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Aroni, Mark (8man-demo\Mark Aroni)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Asil, Claire (8man-demo\Claire Asil)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Auer, Karl (8man-demo\Carl Auer)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Auhss, Ann (8man-demo\Ann Auhss)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Autsch, Anke (8man-demo\Anke Autsch)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Azubi, Andy (8man-demo\Andy Azubi)	Nein	Account never expires	Ja	N/A	07.03.2016 10:44:09	Benutzer	
Baba, Ali (8man-demo\Ali Baba)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Bach, Klara (8man-demo\Klara Bach)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Baer, Johannes (8man-demo\Johannes Baer)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Baer, Roy (8man-demo\Roy Baer)	Nein	Account never expires	Ja	N/A	13.03.2015 10:21:15	Benutzer	
Baern, Al (8man-demo\Al Baern)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Balken, Don R. (8man-demo\Don R. Balken)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Becher, Joe Kurt (8man-demo\Joe Kurt Becher)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Beiter, Walter (8man-demo\Walter Beiter)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Bert, Carmen (8man-demo\Carmen Bert)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
Bert, Carmen (8man-demo\Carmen Bert)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	

Open the report in Excel.

- 1. Select the tab "User".
- 2. Filter the column "PWDon't expire" by positive entries.

We recommend setting your security requirements so that passwords must be changed at least every 90 days.

#### 4.1.1.10 Identify users with never expiring password (web client)

##### Background / Value

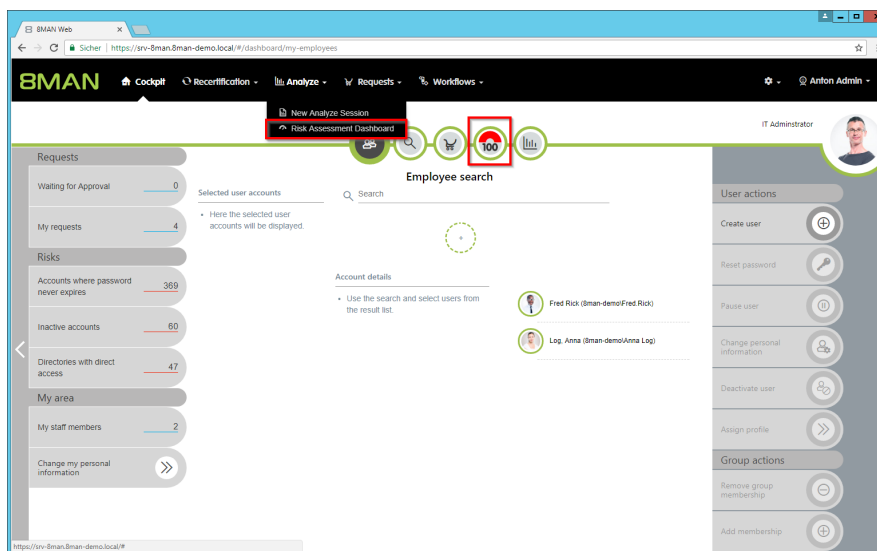
One key security requirement within any organization is that passwords are changed regularly. Use the scenario to find accounts where this requirement has not been activated. View this information in the web interface and create reports.

##### Additional Services

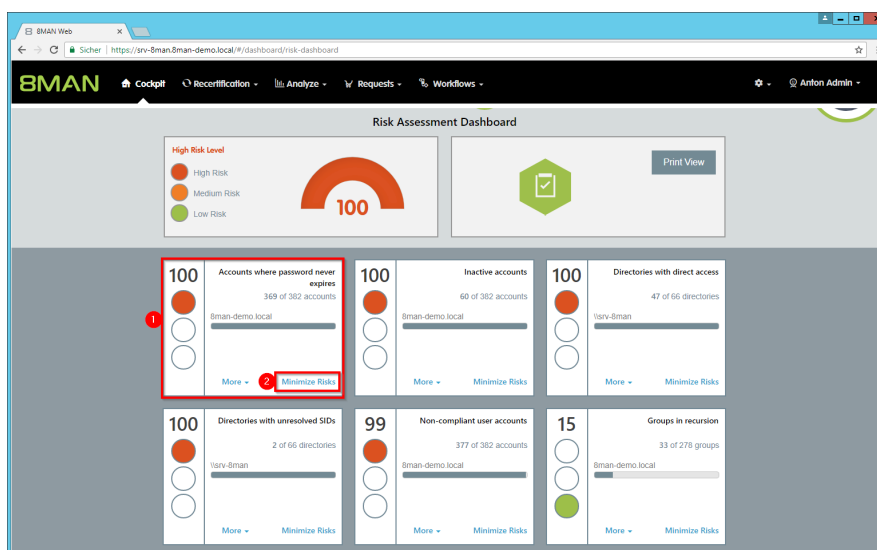
[Reset passwords](#) (rich client)

[Change password options](#) (rich client)

##### Step by step process

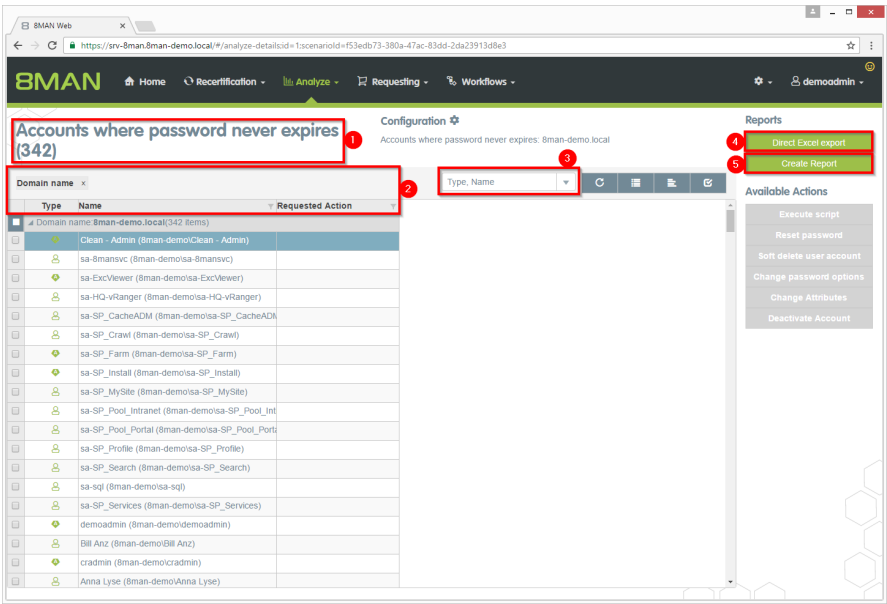


Go to the Risk Assessment Dashboard.



1. 8MAN 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. 8MAN 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.

### 4.1.1.11 Analyze historical AD structures

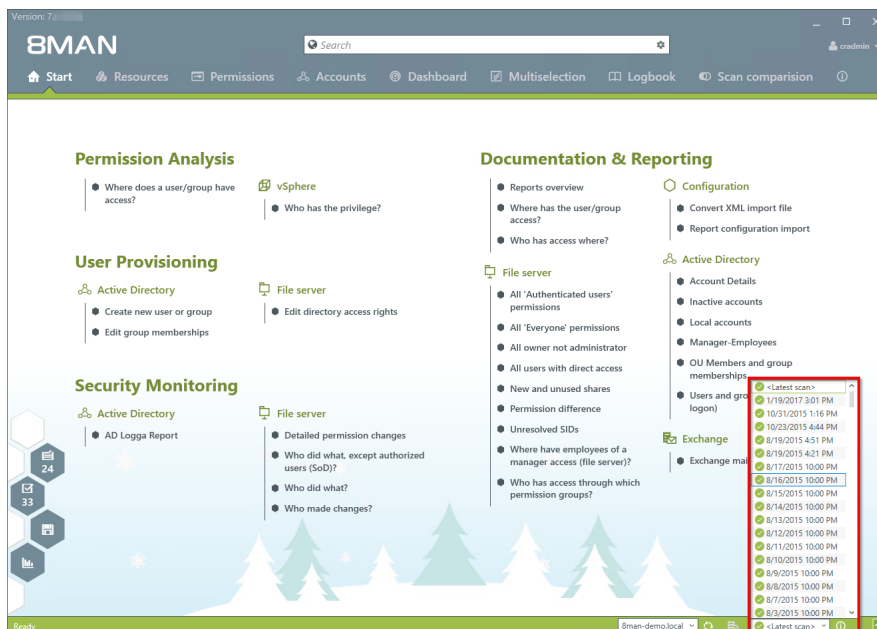
#### Background / Value

After the occurrence of data breaches and other security incidents it is often useful to review historical AD structures. This allows you to understand who had access and who could not possibly have had access during a given point in time. 8Man allows you to access historical scans in the usual "Look and Feel" to understand the security implications of AD access rights at the time of the incident.

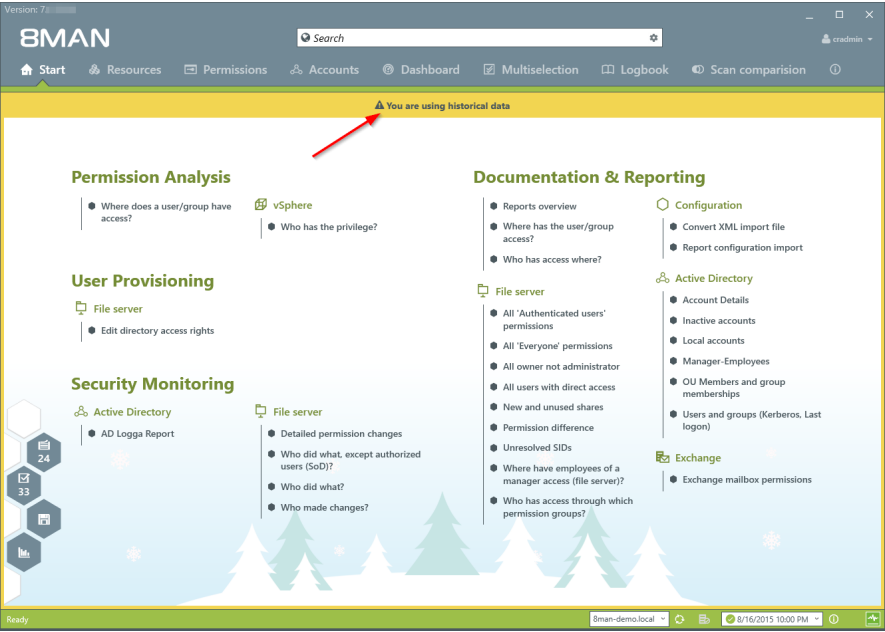
#### Additional Services

Alternatively you could also [compare two scans from different points in time](#).

#### Step by step process



Select the desired scan date.



The warning and the orange frame indicate that you are viewing historical information.

#### 4.1.1.12 Identify inactive accounts (web client)

##### Background / Value

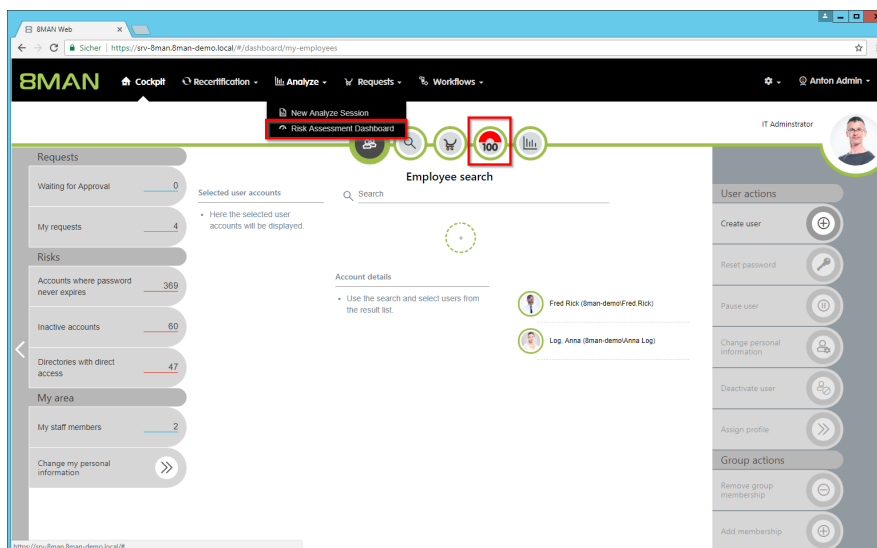
Inactive accounts can be used for data theft and manipulation without being detected. Since most inactive accounts are remnants of past employees, they are often a symptom of a communication problem between HR and IT. 8MAN displays all inactive accounts in Active Directory with a last logon older than 30 days. Remove or deactivate accounts that are no longer needed.

##### Additional Services

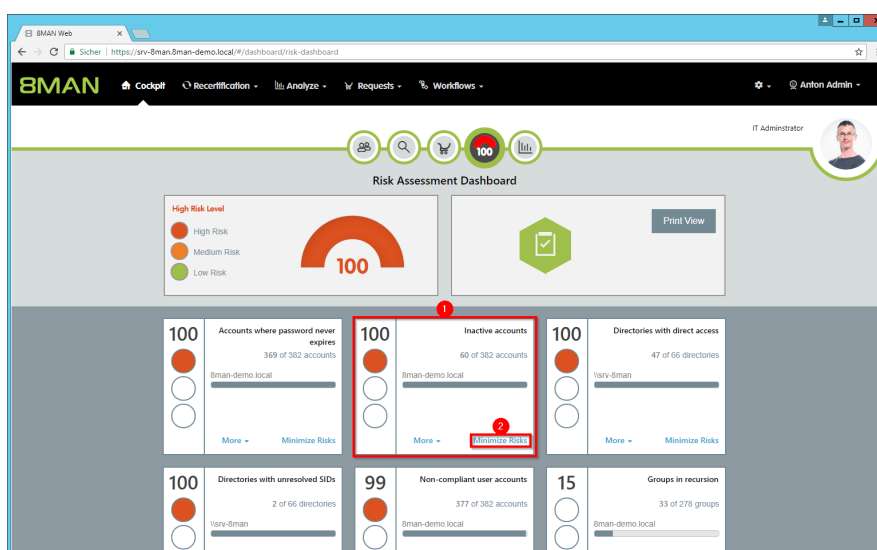
[Report: inactive accounts](#)

[Deactivate accounts in bulk](#) (web client)

##### Step by step process

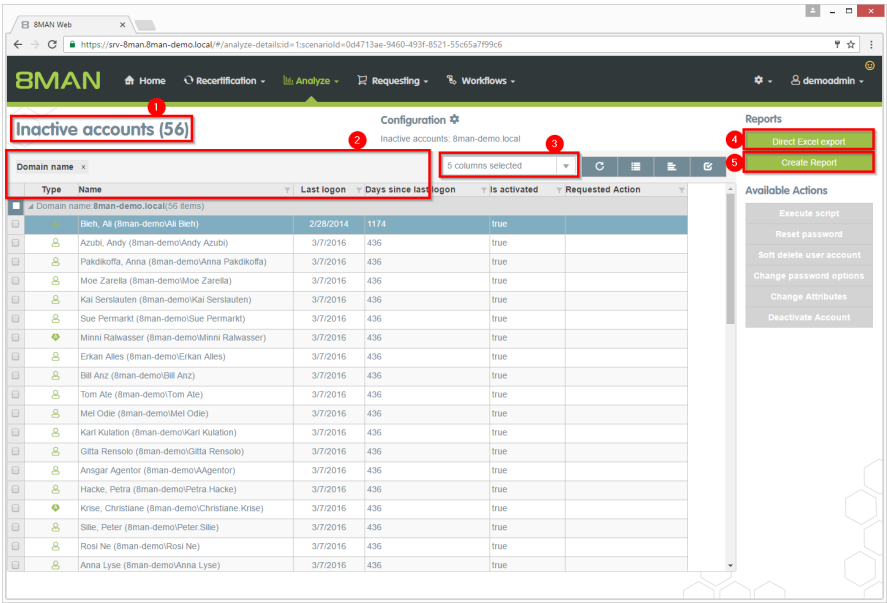


Go to the Risk Assessment Dashboard.



1. 8MAN 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. 8MAN 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.

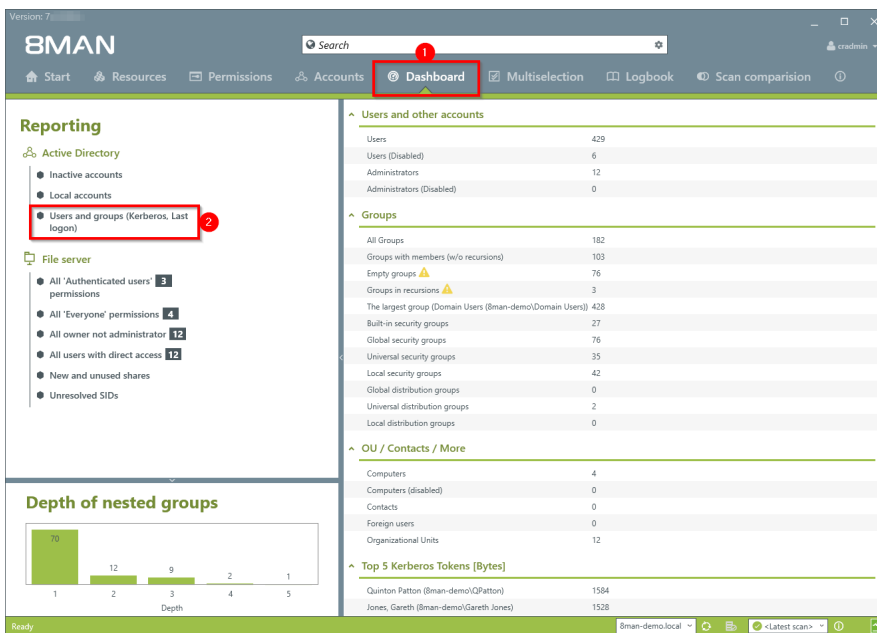


#### 4.1.1.13 Identify temporary user accounts

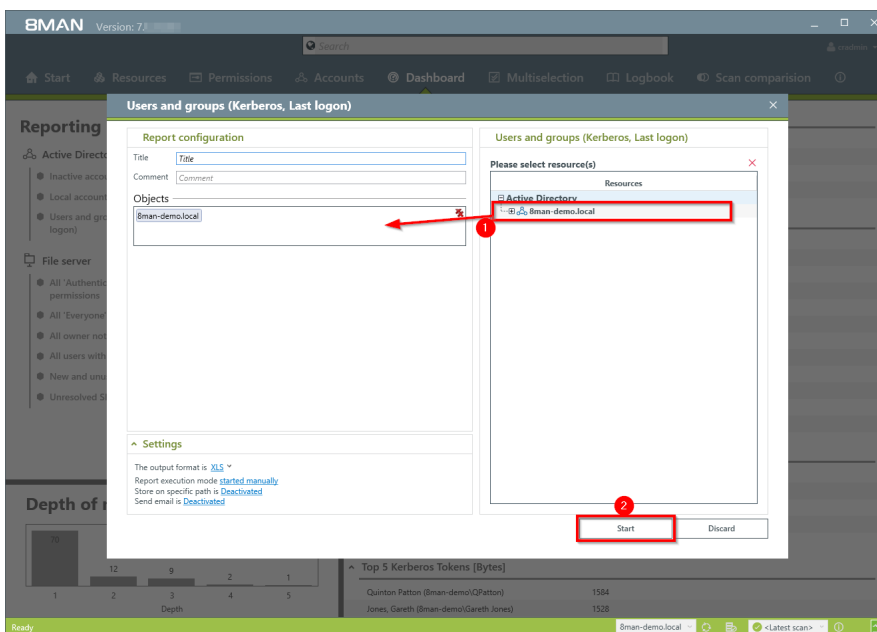
##### Background / Value

User accounts for external employees or interns should only exist temporarily. 8MAN 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.
1. Run the report.

The screenshot shows an Excel spreadsheet with the following data:

Report über alle Benutzer für	8man-demo.local	Account Expires	PWD don't expire	Last Logon	Last Logon Timestamp	Type	Direct Memberships	Indirect Memb
Display/Name	IsDisabled	31 01 2017 00:00:00	a	N/A	07 03 2016 10:44:09	Benutzer		9
Acubi, Andy (8man-demo\Andy Acubi)	Nein	31 12 2016 00:00:00	a	N/A	N/A	Benutzer		1
John Doe (8man-demo\John Doe)	Nein							

The bottom left corner shows the '8man-demo.local\_Benutzer' tab selected.

Open the report in Excel.

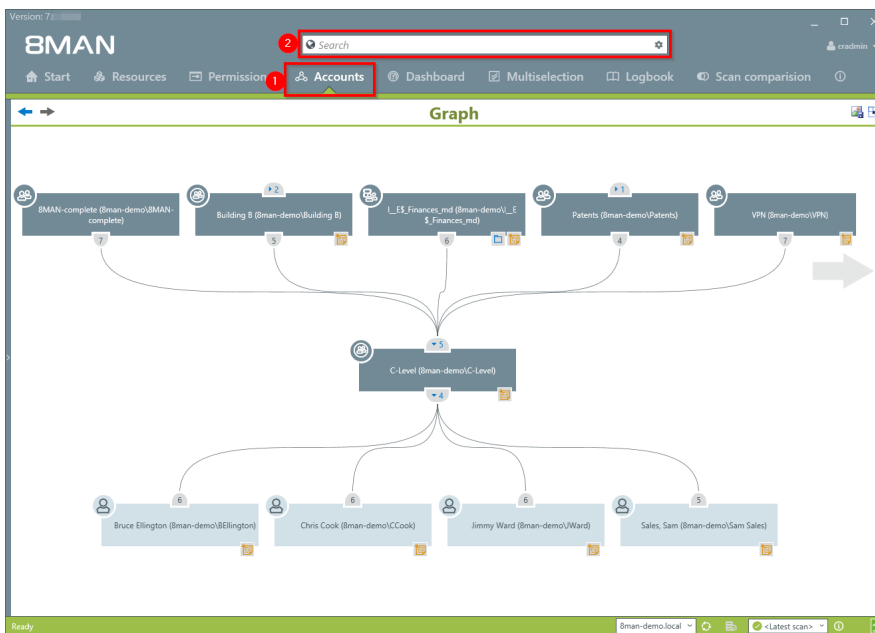
1. Select the tab "User".
  2. Filter the column "Account expires" by positive entries.
- We recommend checking with your HR department if any of these accounts are still needed.

#### 4.1.1.14 Identify the most recent actions on an account

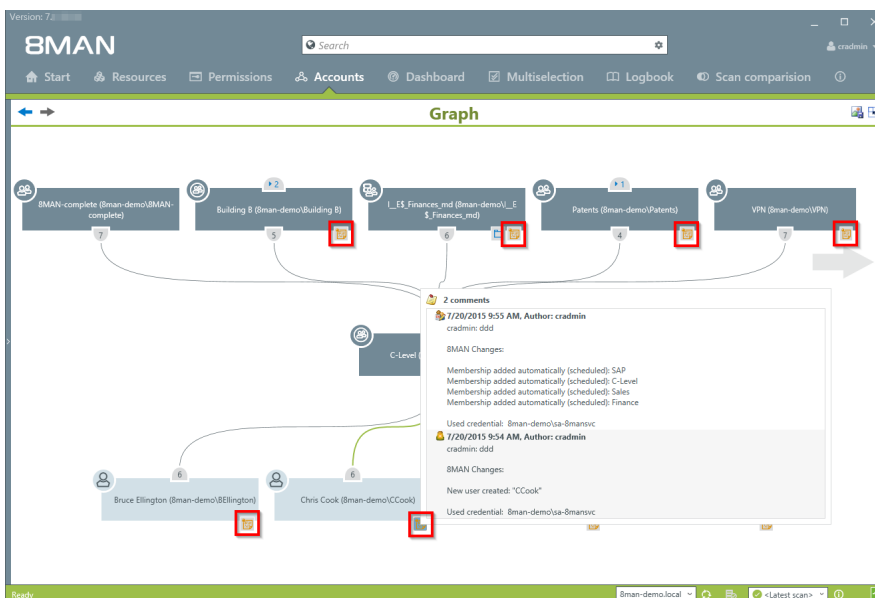
## Background / Value

User accounts and AD groups have their own history. This is why it makes sense to review the previously performed actions and changes. 8MAN shows you a quick view of most recent activities or you can jump directly into the log book to receive a full report.

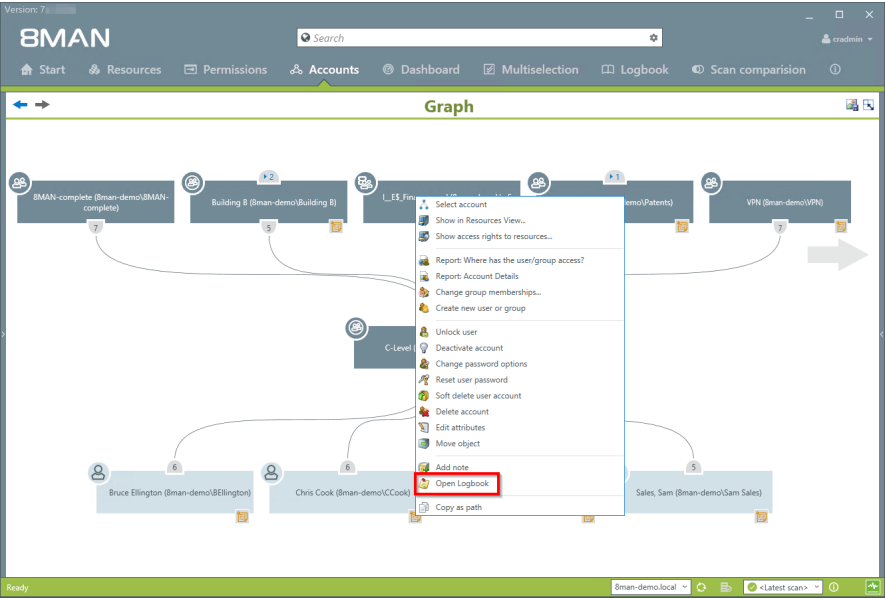
## Step by step process



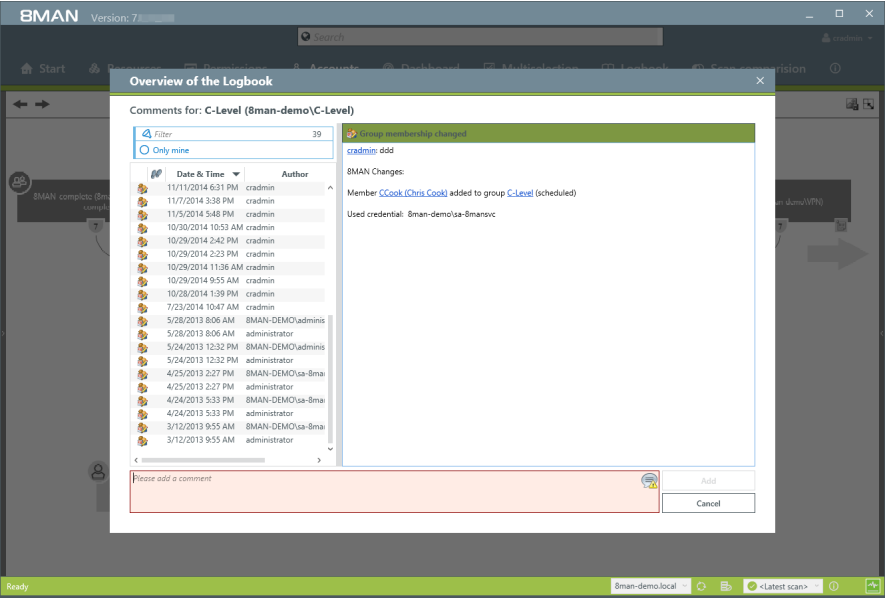
1. Select "Accounts".
2. Search for the desired user or group.



*The note icon indicates that activities were recorded in the 8MAN 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.  
You can enter a comment into the log book.  
The footprint icon indicates that these actions were recorded by AD Logga.

#### 4.1.1.15 Determine permissions deviating from the department profile (Compliance Check) (web client)

##### Background / Value

8MAN 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.

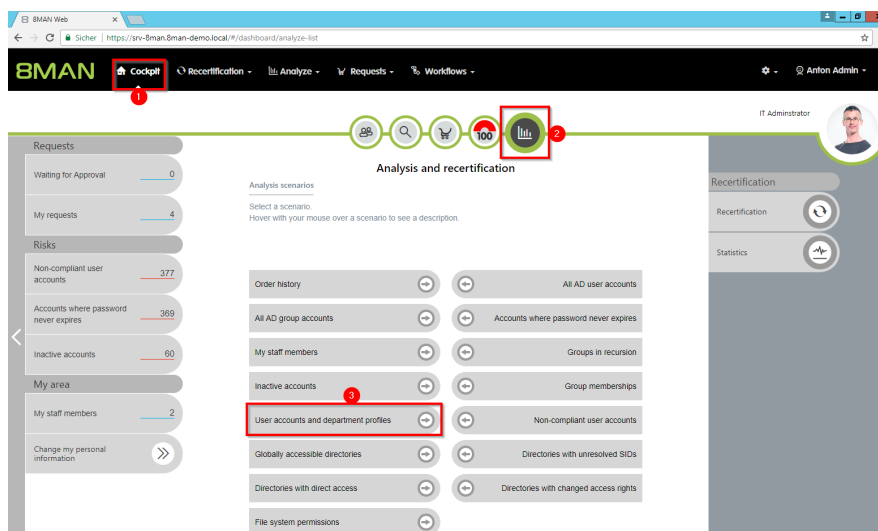
To be able to use the compliance functions, you must have created at least one department profile.

##### Additional Services

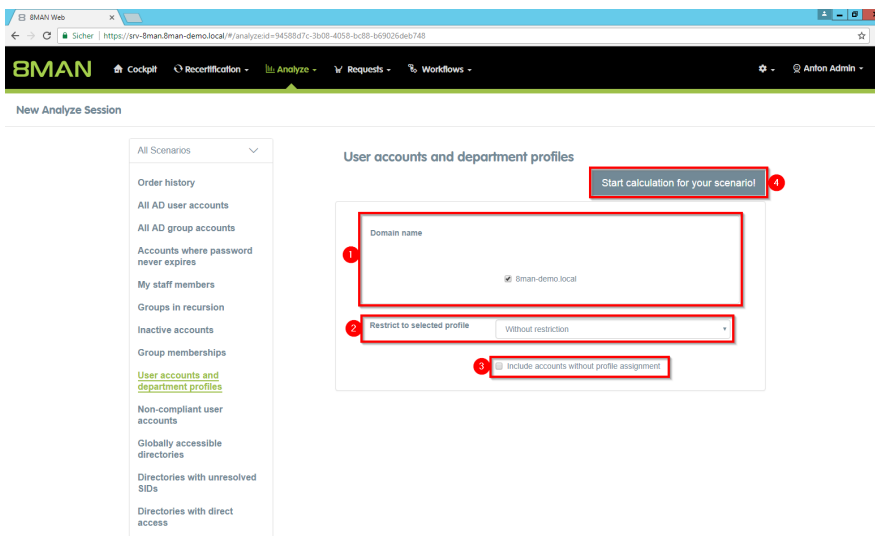
[Create a new department profile \(Administrator\)](#)

[Assign a department profile to users](#)

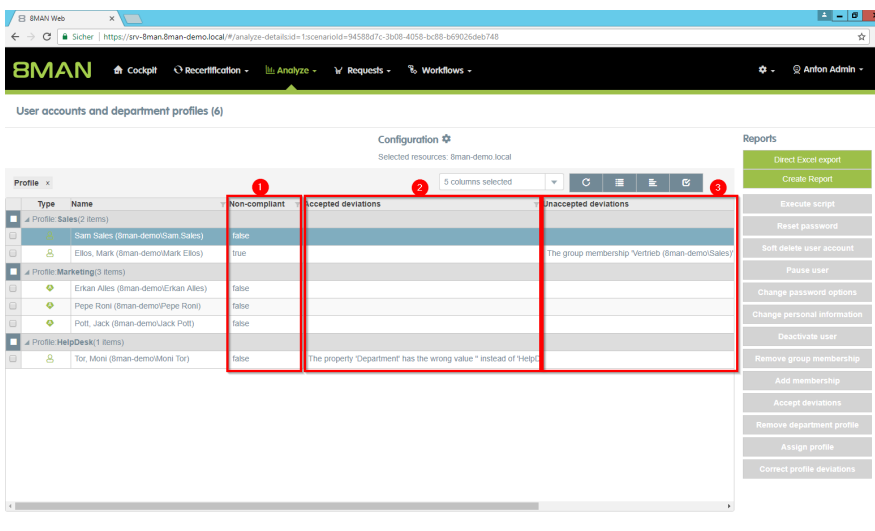
##### Step by step process



1. Select Cockpit.
2. Click "Analyze and recertification".
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.



1. 8MAN shows you which user accounts are non-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".

## 4.2 File server

8MAN shows all access rights to file server directories. Administrators and Data Owners can change permission in user friendly workflows. In addition 8MAN identifies and highlights security risks such as multiple or direct access rights, defective ACLs and unresolved SIDs.

## 4.2.1 Services for administrators und data owners

### 4.2.1.1 Identify access rights on a file server directory

#### Background / Value

8MAN quickly shows you all access rights on file server directories. Initially you should focus on the directories containing the most sensitive data. You simply need to know: Who has access?

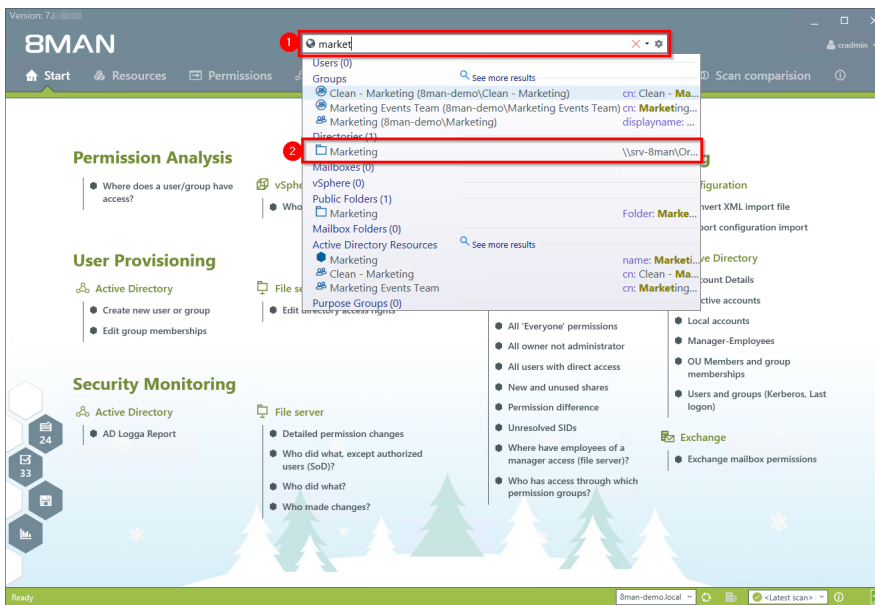
#### Additional Services

[Report: Who has access to what?](#)

[Modify folder permissions](#)

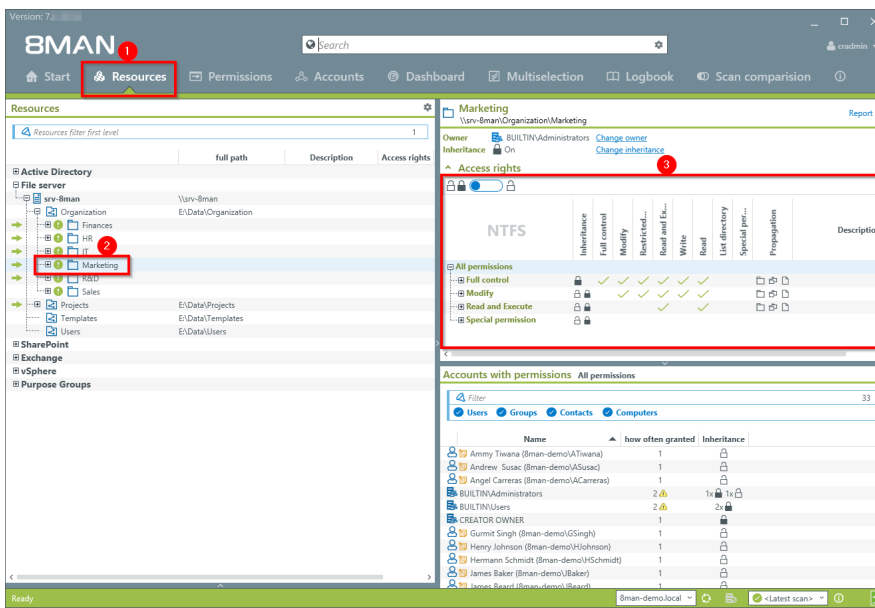
[Monitor access to sensitive data](#)

#### Step by step process

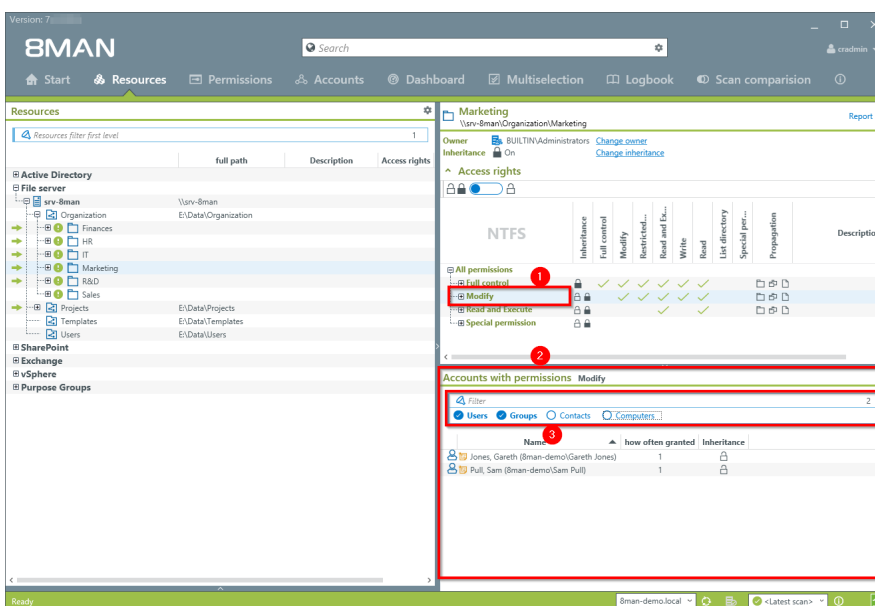


1. Search for the desired directory.
2. You can find your search result in the directory section.





1. 8MAN switches to the resource view.
2. You are focusing on the desired directory.
3. 8MAN displays all access rights that exist for the chosen directory.



1. Select an access category filter. In this example the "Modify" filter has been chosen.
2. 8MAN lists all accounts with "Modify" access rights to the Marketing directory.
3. You can add additional filters for users, groups, contacts and computers to narrow down the results further.

#### 4.2.1.2 Identify the permissions of a user

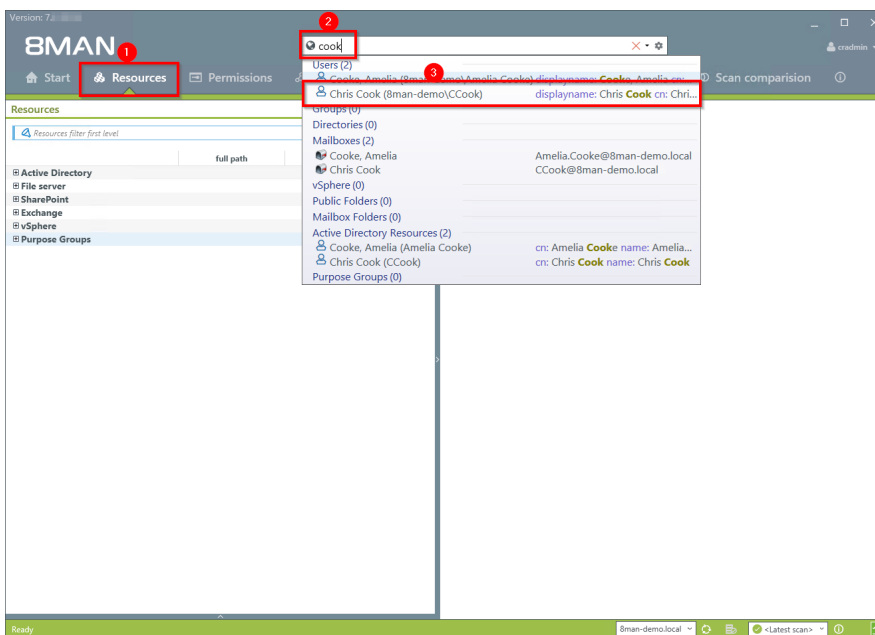
##### Background / Value

8MAN can also show you the user perspective, and which directories 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.

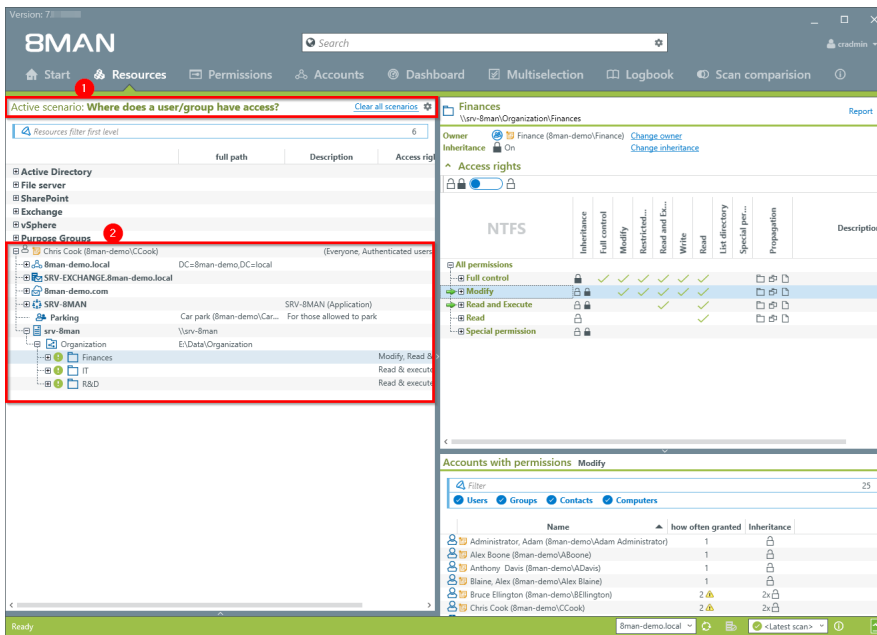
##### Additional Services

Alternatively, you can capture the same information in a report: [Which resources does a user have access to?](#)

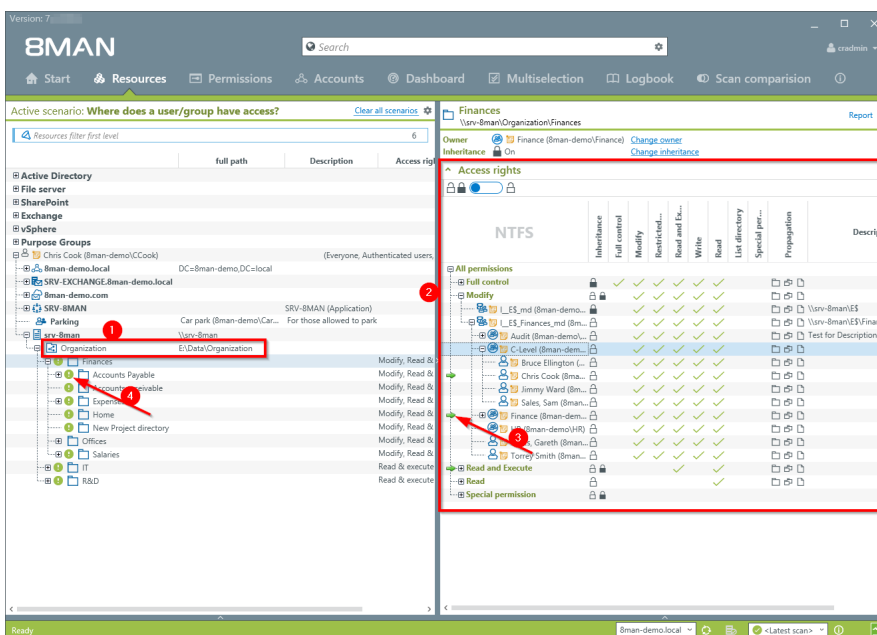
**In contrast to the dynamic view in the UI, the report does not show any information related to Active Directory, Exchange und Purpose Groups.**



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. 8MAN activates the scenario "Where does a user/group have access"
2. 8MAN shows all resources that "Chris Cook" can access. In the basic version you can view results for Active Directory and file servers. Depending on which AddOns have been chosen, you can also review access to other resources.



1. 8MAN shows all directories that "Chris Cook" can access on the file server. In this example we have focused on the "Finance" directory.
2. 8MAN shows the access rights for the "Finance" directory.
3. The green arrow indicates the user "Chris Cook". This helps you identify which resources "Chris Cook" can access, based upon the individual permission paths.
4. The green circle with the exclamation mark shows that the access rights on this directory differ from the "parent" directory.

## 4.2.2 Services for administrators

### 4.2.2.1 Identify multiple access paths to file server directories

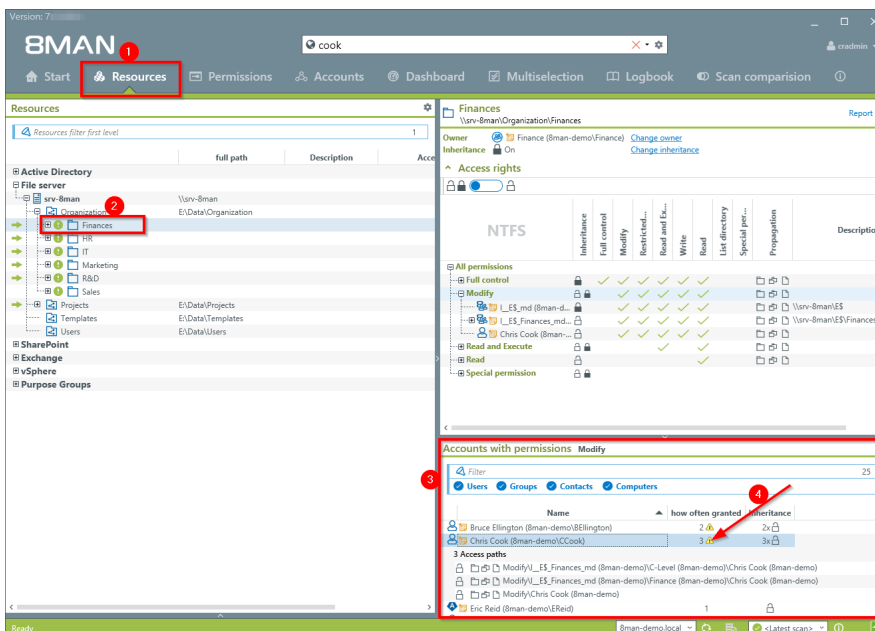
#### Background / Value

Multiple access paths to file server directories are often a consequence of confusing group structures and direct access rights. Access to resources should only be granted using group memberships.

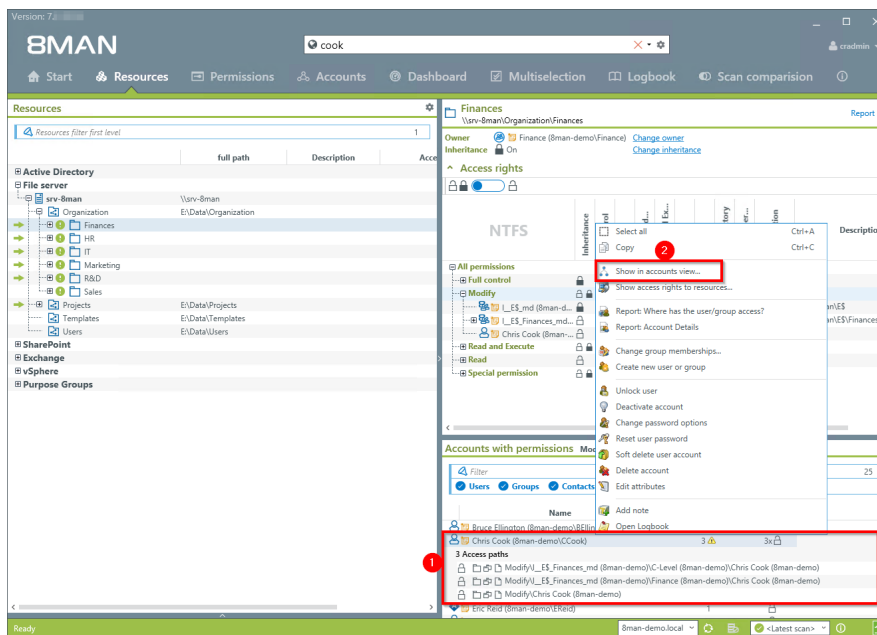
#### Additional services

[Remove multiple access paths to file server directories](#)

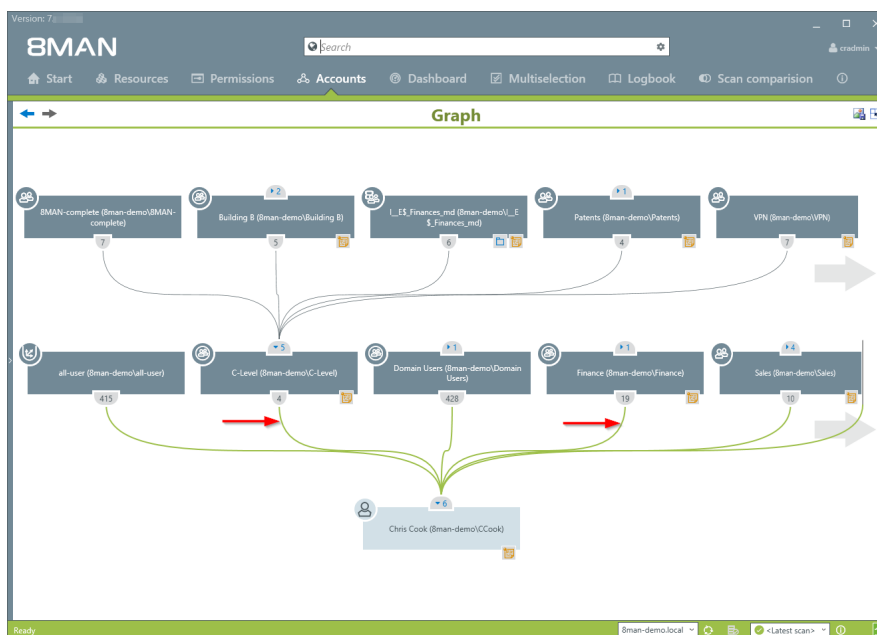
#### Step by step process



1. Select "Resources".
2. Select a directory.
3. 8MAN shows you all access rights of the selected user in a flat list.
4. The yellow warning indicates multiple access rights. Click on it.



1. 8MAN shows the different permission paths (in example 3) through which "Chris Cook" has access to the directory in question.
2. Right-click on the user to open the context menu. Select "Show in accounts view".



You can use the AD graph to analyze how these multiple permission paths are structured.

#### 4.2.2.2 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.

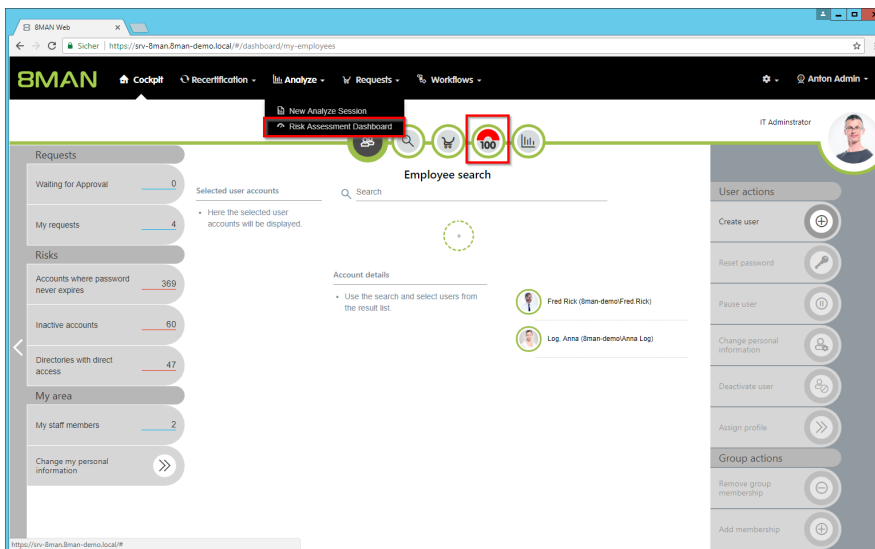
"Everyone accounts" are:

- Everyone
- Authenticated Users
- Domain-Users

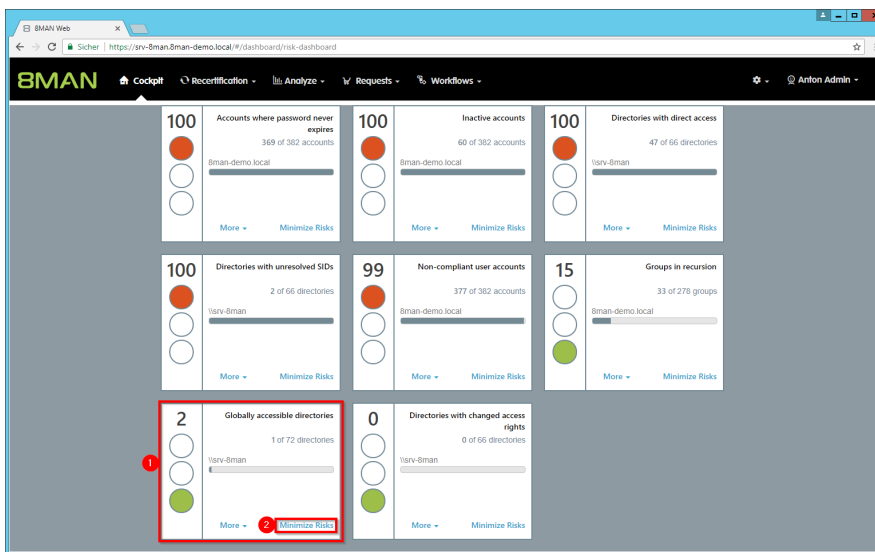
##### Additional Services

[Remove permissions from globally accessible directories in bulk](#)

##### Step by step process

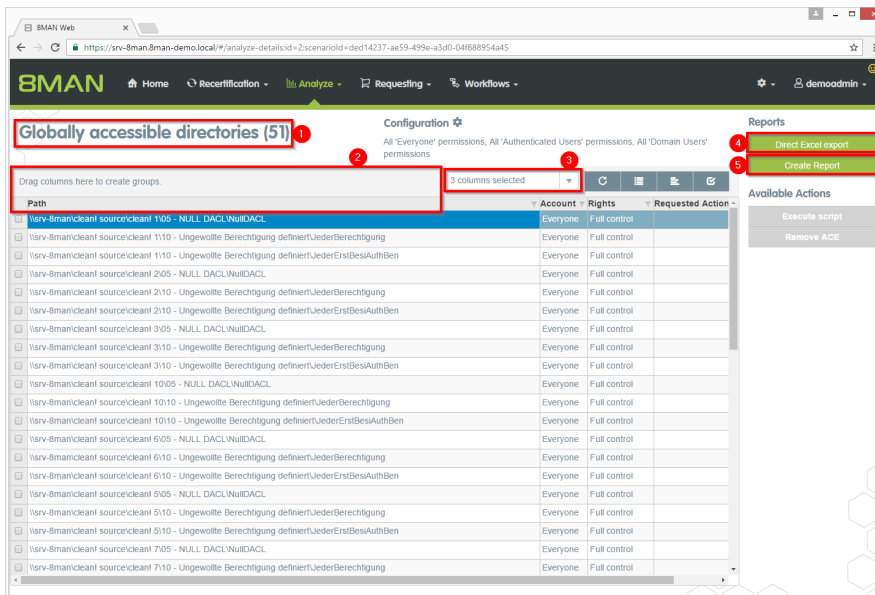


*Go to the Risk Assessment Dashboard.*



1. 8MAN 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. 8MAN 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.

### 4.2.2.3 Identify corrupted inheritance

#### Background / Value

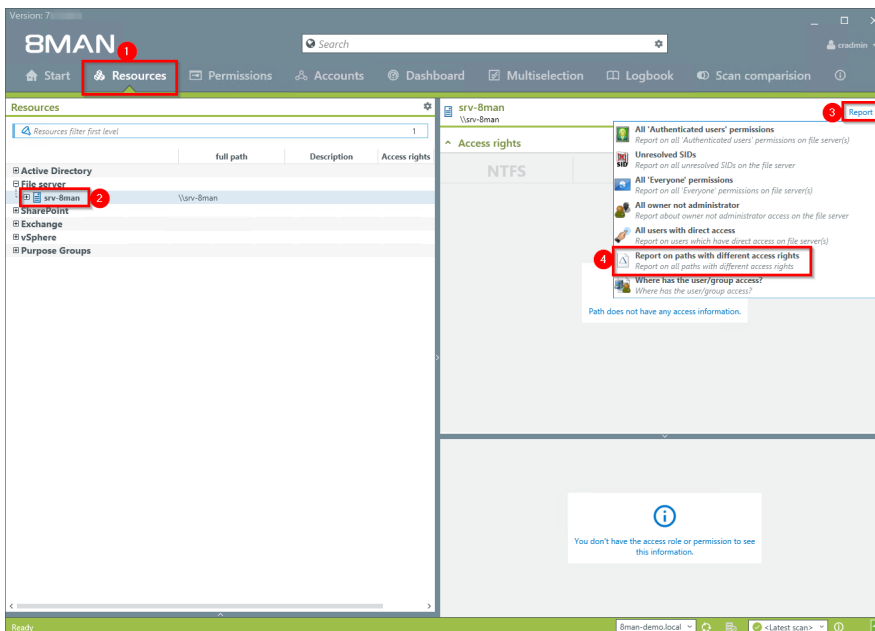
Broken ACLs (Access Control Lists) interfere with the NTFS inheritance on the fileserver. The consequences: The subdirectory does not get the correctly inherited permissions, even though the inheritance is enabled.

8MAN shows you broken ACLs in a report.

#### Additional Services

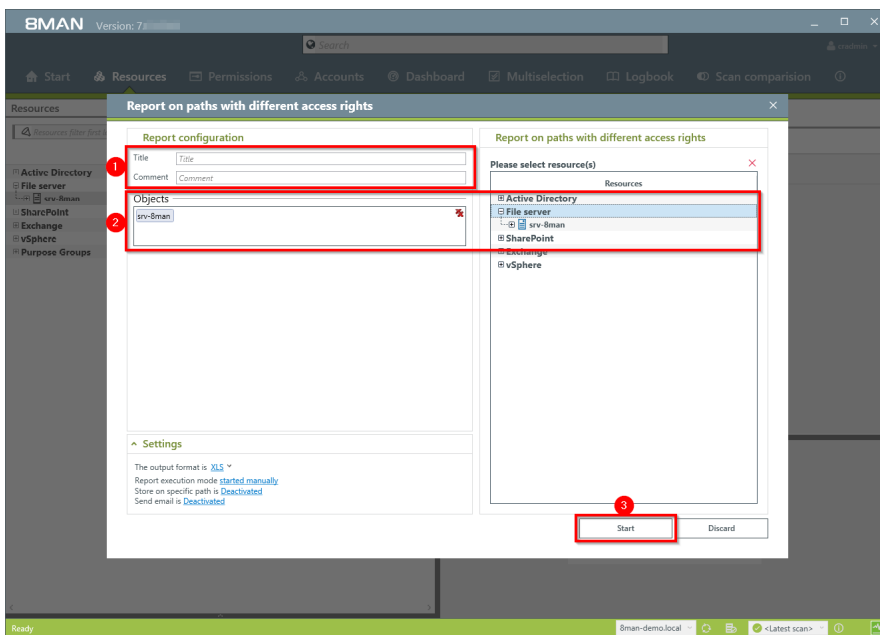
[Remove corrupted inheritance](#)

#### Step by step process

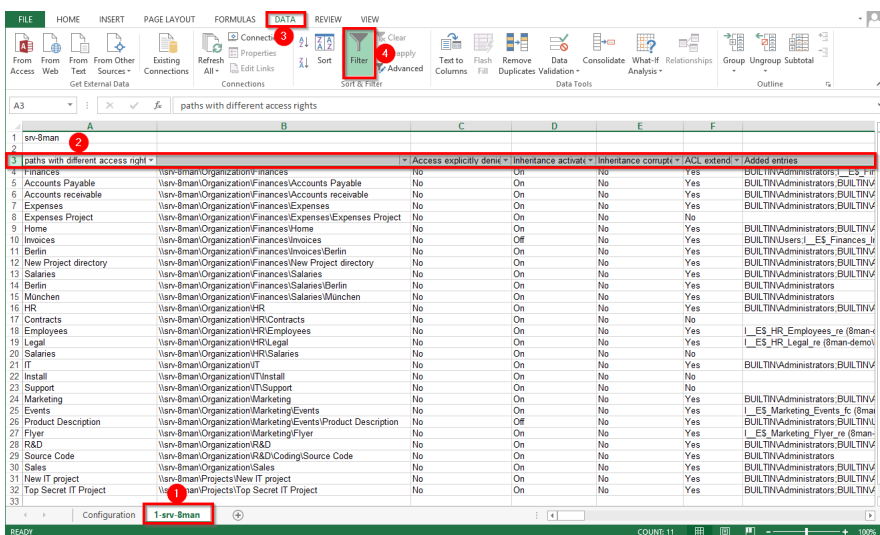


1. Select "Resources".
2. Select the desired file server.
3. Click on "Report".
4. Select "report on all sub-directories with different access rights".



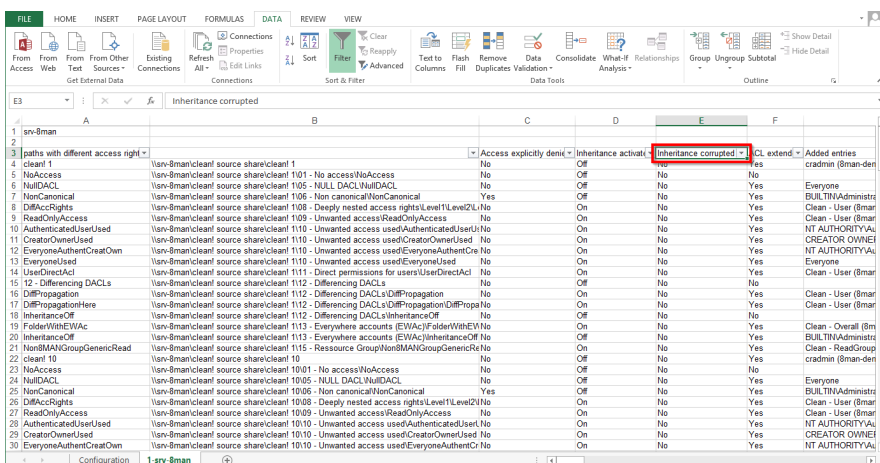


1. You can name the report and add a comment.
2. You can change the range of the report.
3. Start the report creation.



Open the .XLS file with Excel.

1. Select the tab of the selected resource
2. Select the third line and add a filter.



1. Activate the column "inheritance corrupted" by selecting "yes".
2. The results show the directories with defective ACLs.

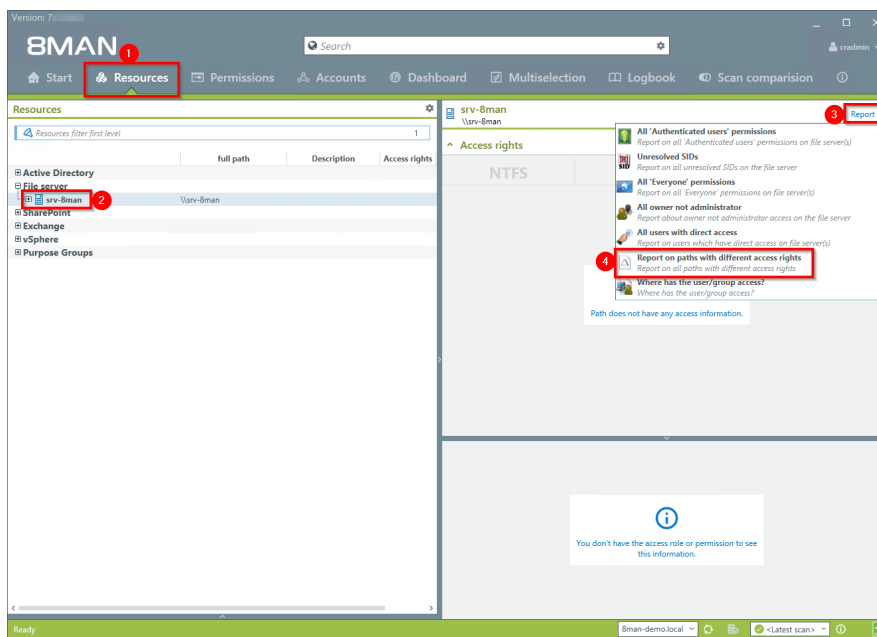


#### 4.2.2.4 Identify folders with special protection

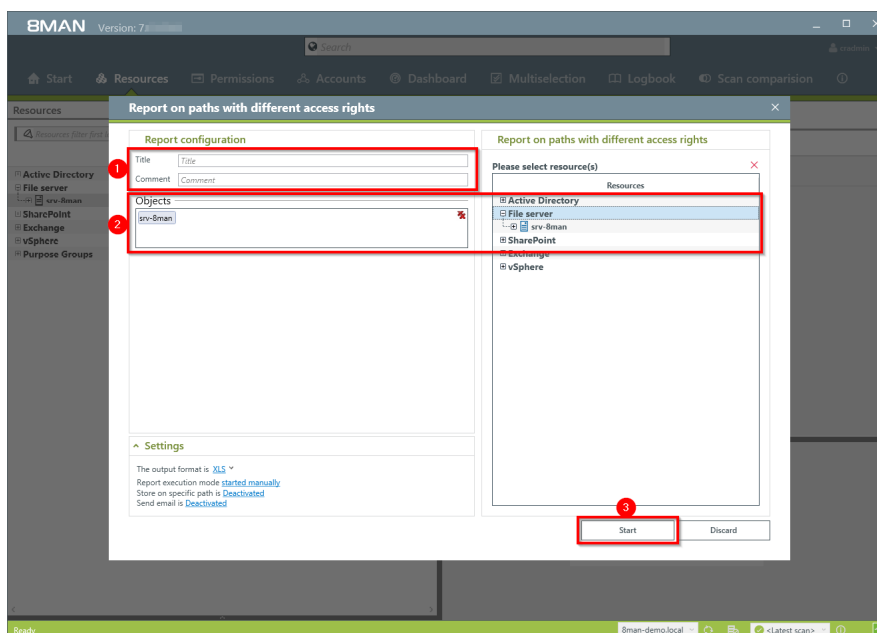
##### Background / Value

Sub-directories often contain different access rights compared to its "parent" directory. 8MAN shows all directories where these rights differ. Broken inheritances are often an indicator of highly restricted directories.

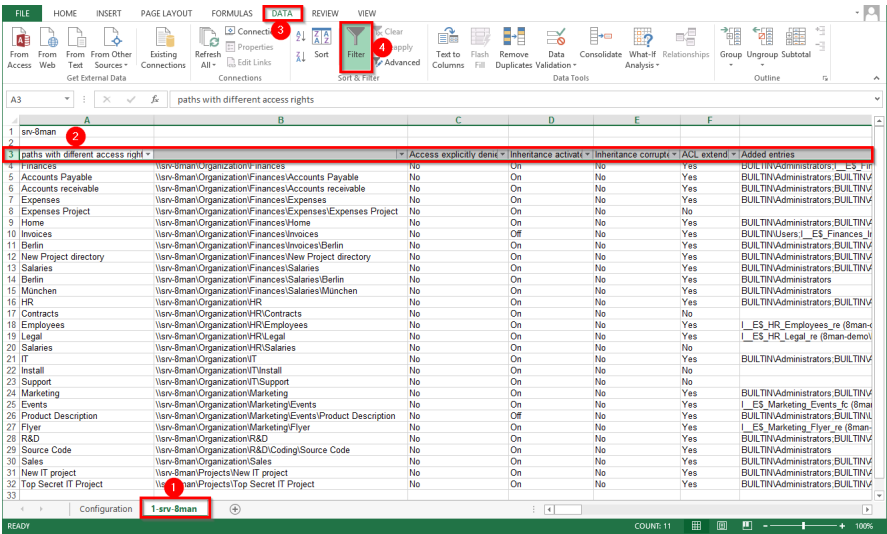
##### Step by step process



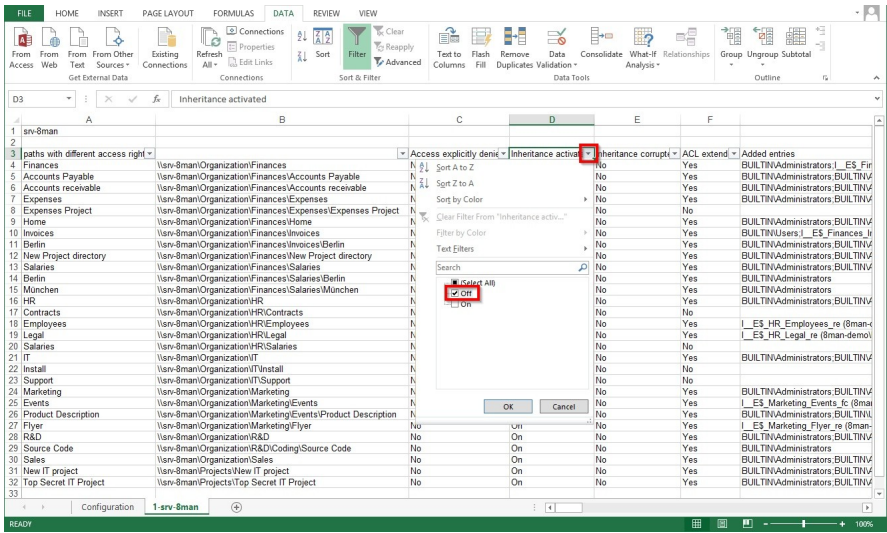
1. Select "Resources"
2. Select the desired file server.
3. Click on "Report"
4. Select the report "Report on all sub-directories with different access rights"



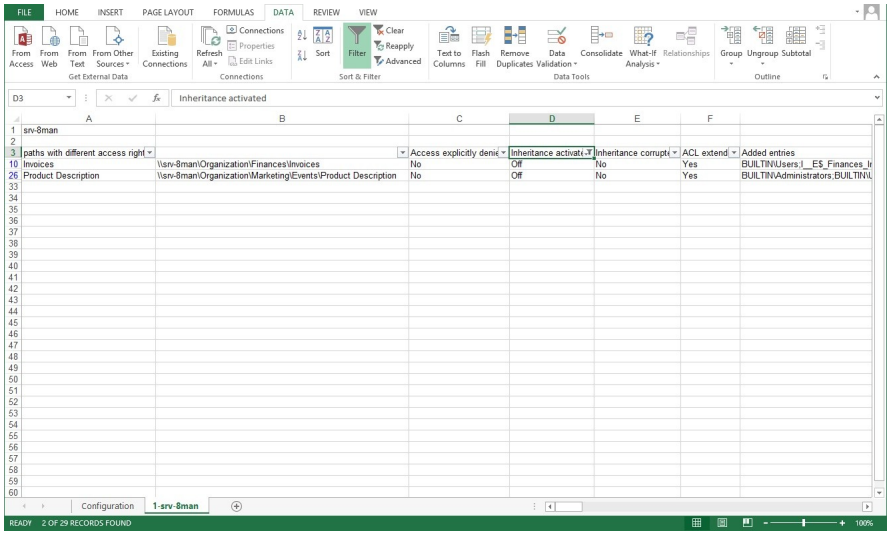
1. You can name the report and add a comment.
1. If desired you can adjust the range of the report.
2. Start the report.



1. Open the .XLS file with Excel.
2. Click on the tab of the selected resource.
3. Select the third line
4. Add a filter.



Select a filter in the column "inheritance set" to "off".



You will see a list of all directories for which inheritance has been broken.

#### 4.2.2.5 Compare two different access rights situations (Scan Comparison)

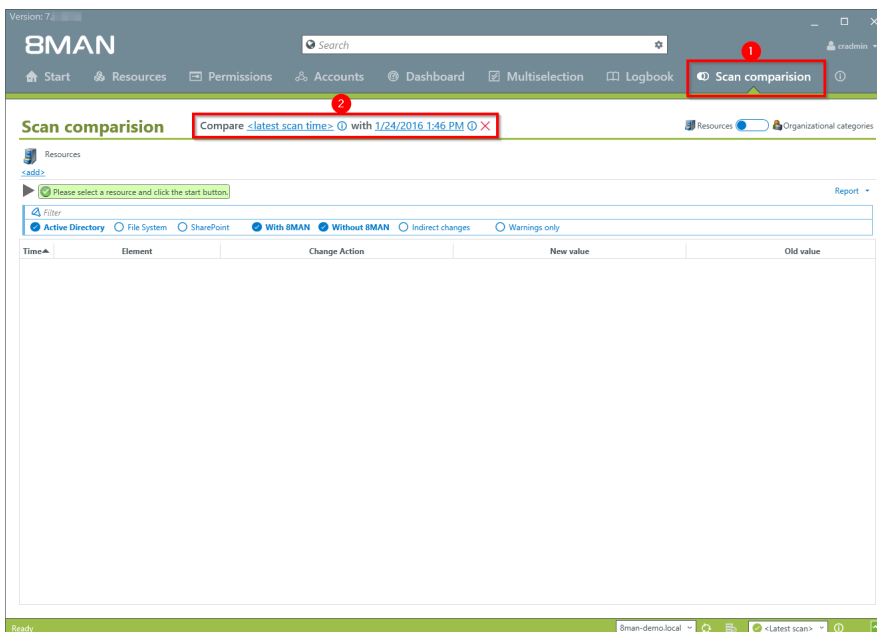
##### Background / Value

The scan comparison compares file server scans at two different points in time and shows you how your access file server environment has changed.

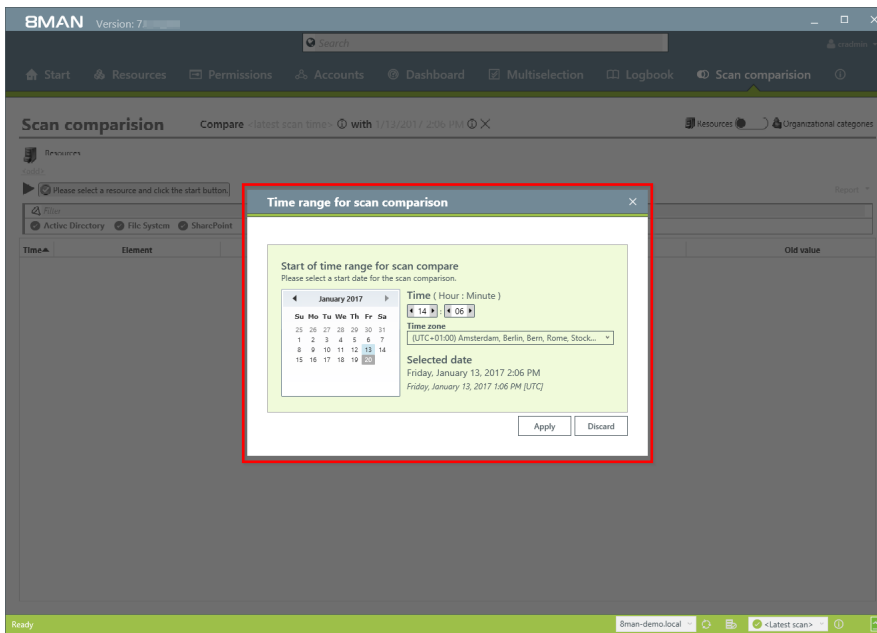
##### Additional Services

The scan comparison only takes two separate points in time into account. In order to be able to monitor all administrative actions made within a given time period to access rights on file servers you would require the 8MATE FS Logga as noted in [Security Monitoring](#). Alternatively you can also [compare two scans from different points in time](#).

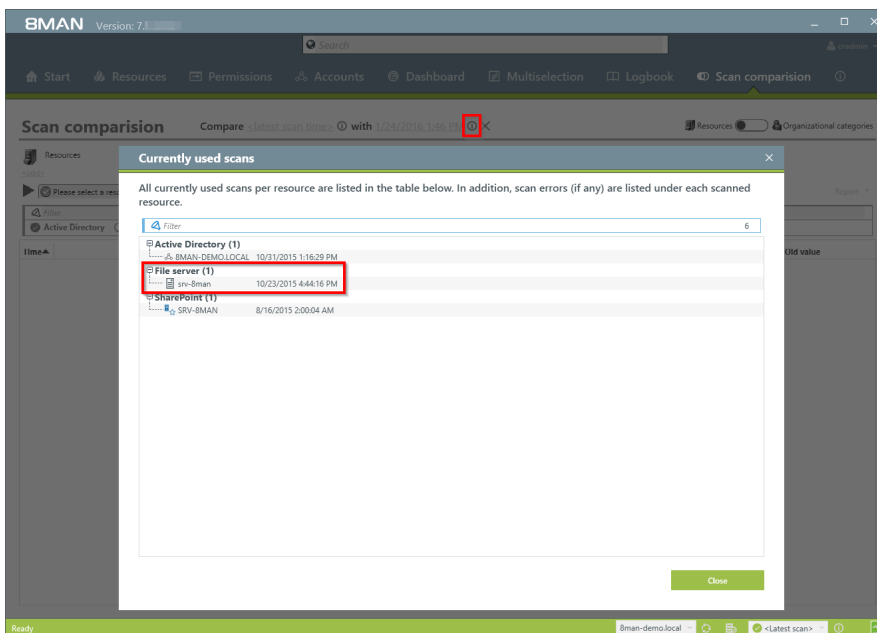
##### Step by step process



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



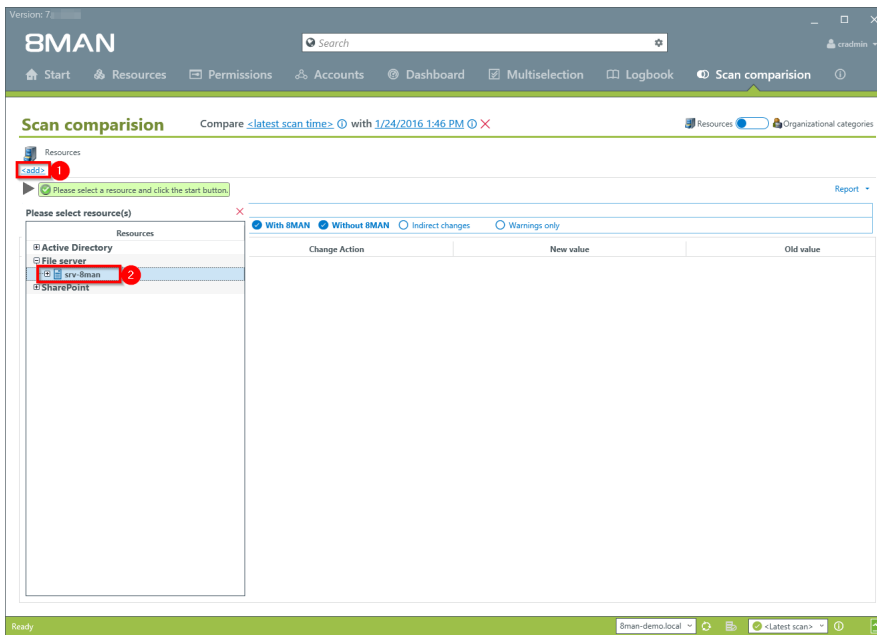
Select the date and time of both scans.



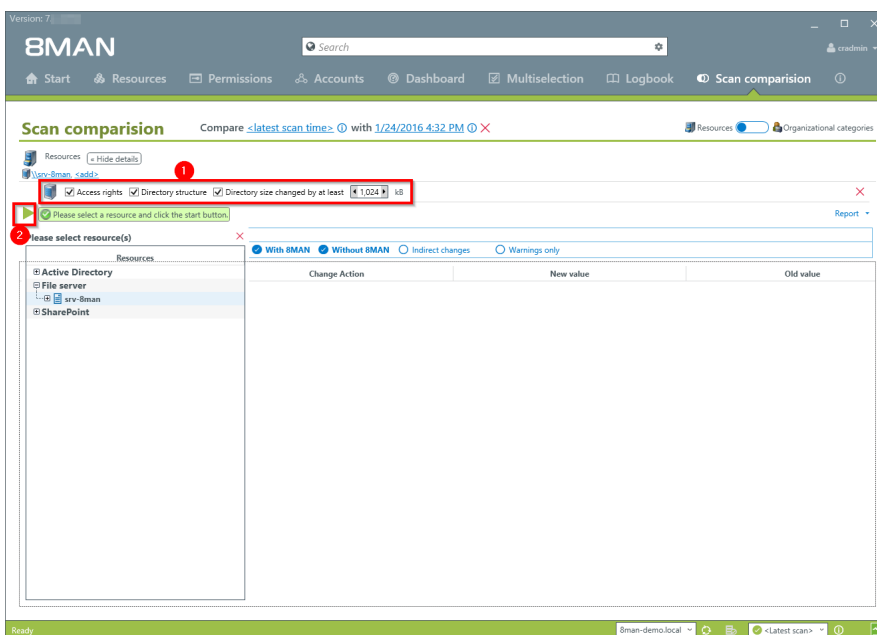
The comparison always compares existing scans.

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

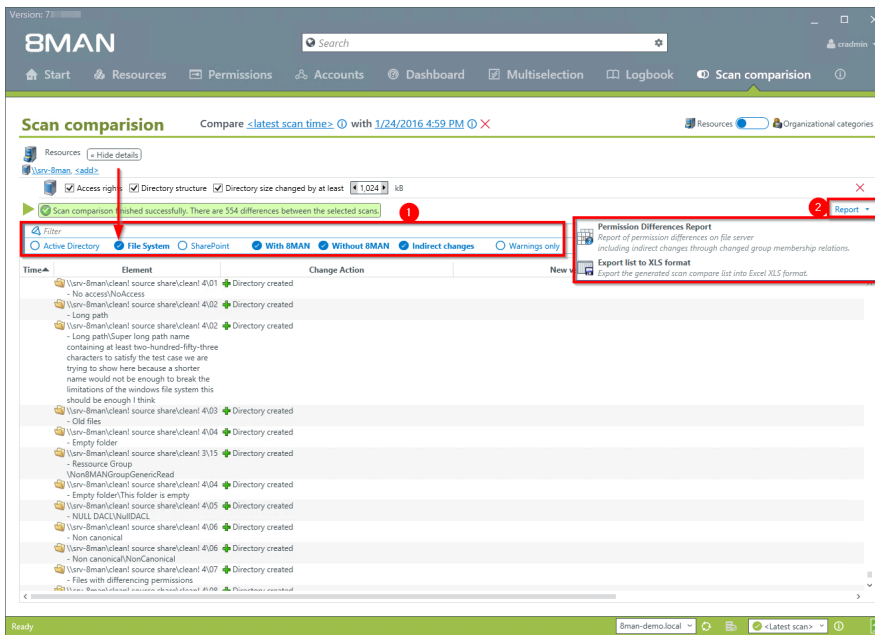
In order to maximize accuracy you should run a current AD Scan before starting the scan comparison.



1. Click on "add resources".
2. Select the desired resource by double clicking on it.



1. Once you have added all required resources you can add the desired parameters.
2. Click on the Play icon.



The scan comparison displays the results

1. Use filters to focus on specific actions.
2. Click on "report" to generate a structured scan comparison report and / or export the results to .XLS.



### 4.2.2.6 Analyze historical access rights situations

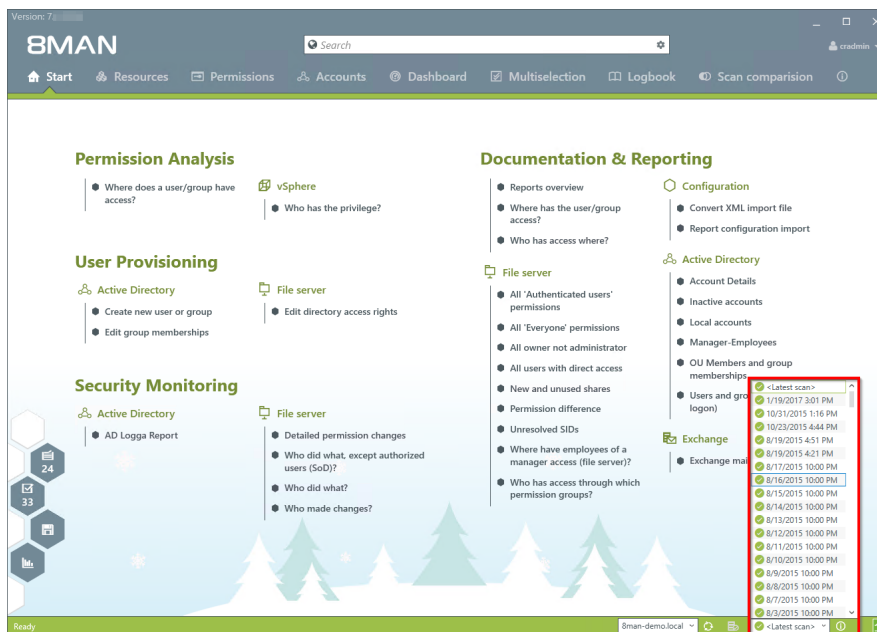
#### Background / Value

After the occurrence of data breaches and other security incidents it is often useful to review historical access rights. This allows you to understand who had access and who could not possibly have had access during a given point in time. 8MAN allows you to access historical scans in the usual "Look and Feel" to understand the security implications of AD access rights at the time of the incident.

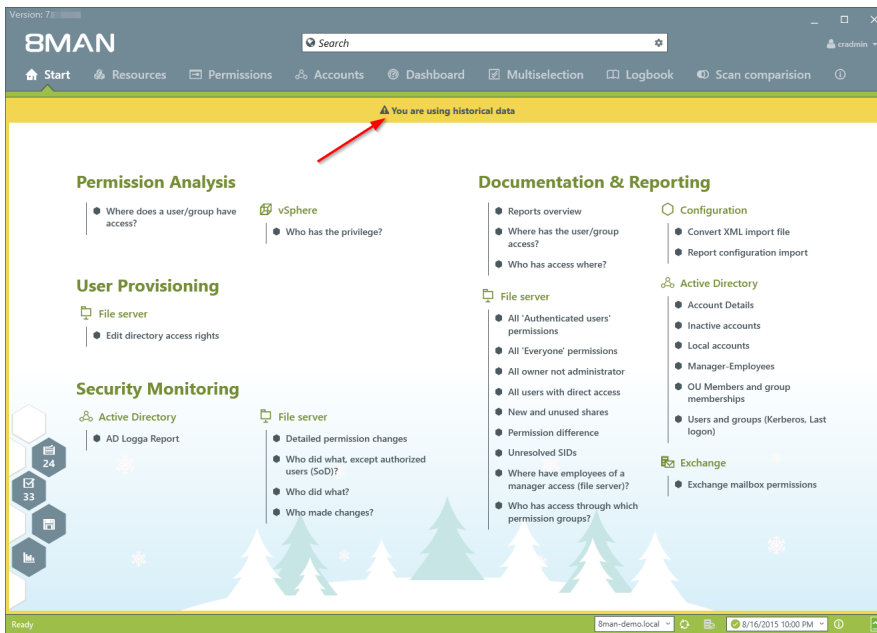
#### Additional Services

Alternatively you could also [compare two scans from different points in time](#).

#### Step by step process



Select the desired scan date.



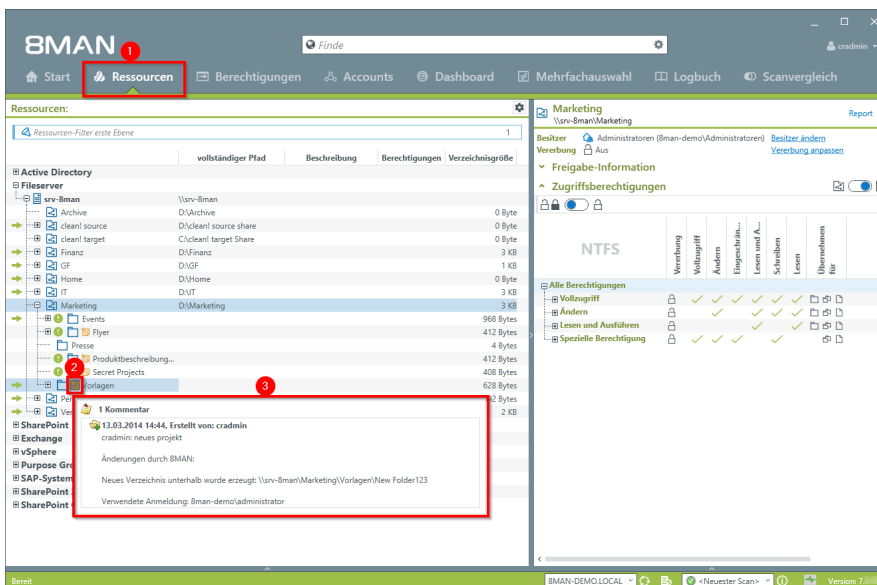
The warning sign and orange frame indicate that you are viewing historical information.

#### 4.2.2.7 Identify the last activities on a directory

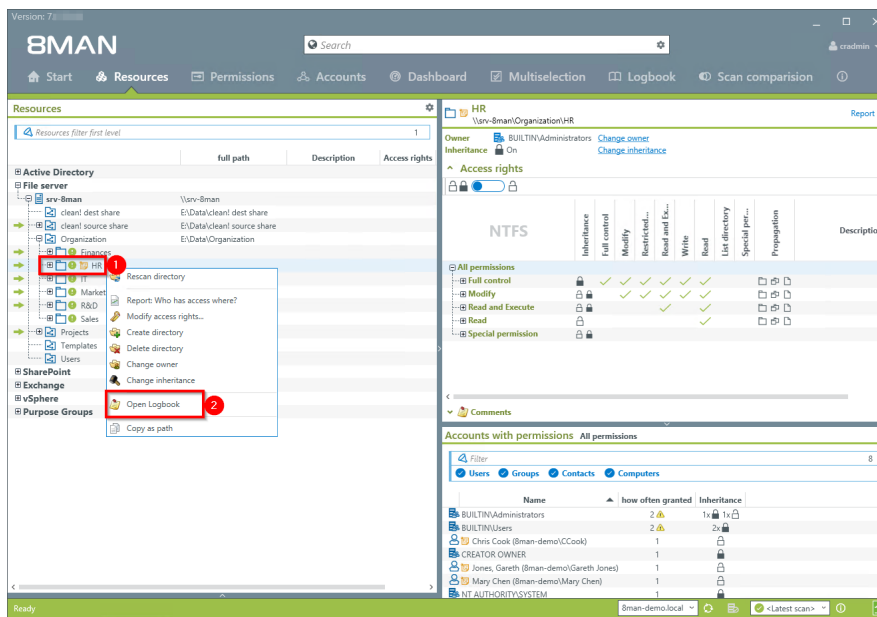
##### Background / Value

File server directories have their own history. This is why it makes sense to review the previously performed actions and changes. 8MAN shows you a quick view of most recent activities or you can jump directly into the log book to receive a full report.

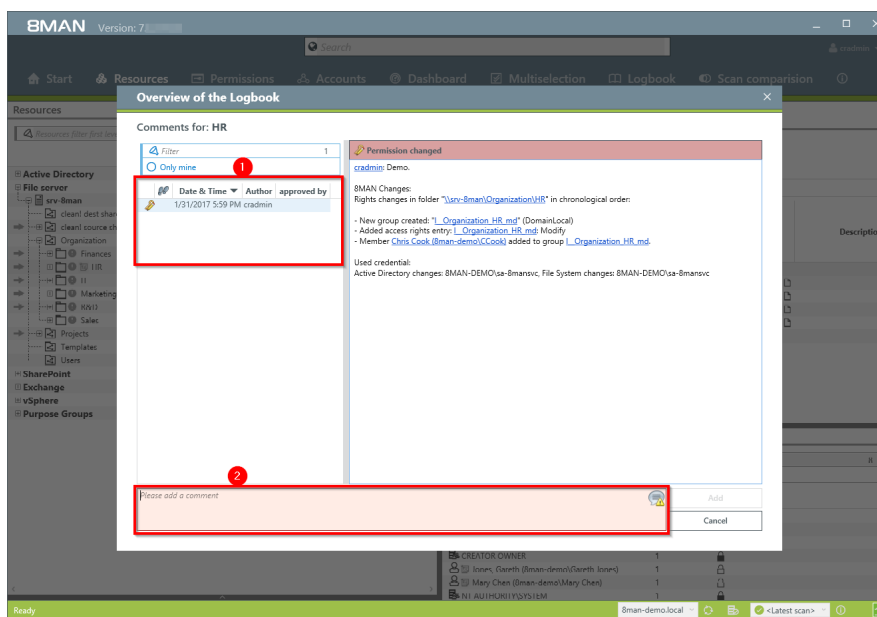
##### Step by step process



1. Select "Resources".
2. The note icon indicates that the object contains comments. You can hover over the note for a quick preview.
3. 8MAN 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 into the logbook.

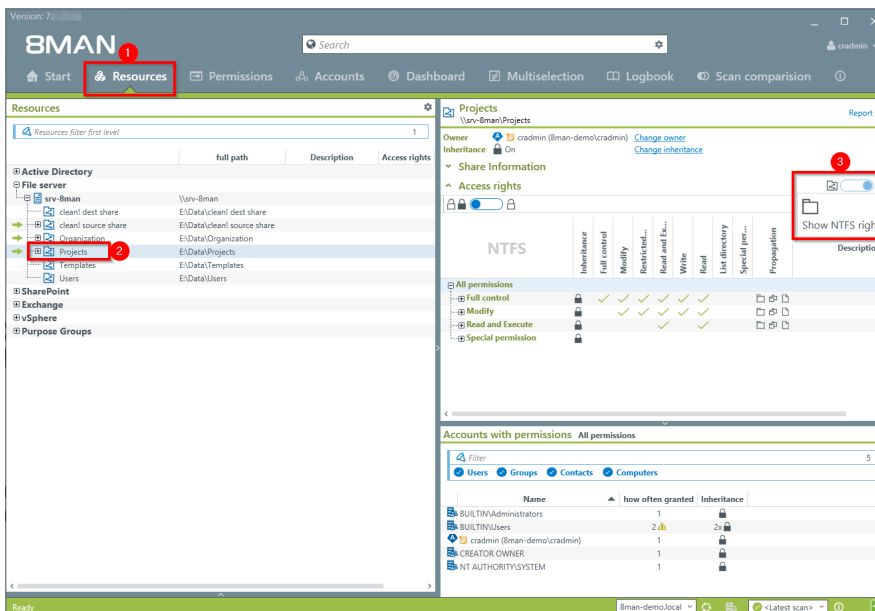
### 4.2.2.8 Identify share permissions

#### Background / Value

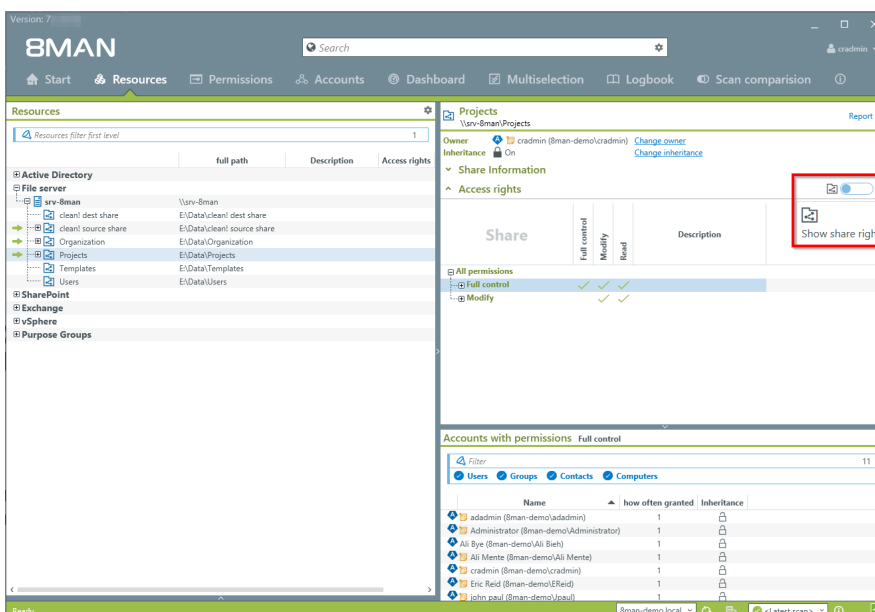
8MAN shows both: share permissions as well as NTFS permissions. In the standard view the NTFS permissions are listed.

When considering share permissions and NTFS permissions it is always the lesser permissions that will be relevant to the User. For this reason we recommend always setting share permissions to full access and using NTFS permissions to set more granular permissions.

#### Step by step process



1. Select "Resources".
2. Select a share.
3. By default 8MAN shows NTFS permissions.



Click on the slider to toggle back and forth between share and NTFS permissions.

### 4.3 +8MATE for Exchange

8MATE for Exchange expands 8MAN to include Exchange resources. This way the analysis and administration of access rights are standardized across various resources and systems. 8MAN shows you an overview, where you can see access rights to folders, email accounts, email folders or calendars on one easy to read screen.

The administration of exchange is closely connected to the onboarding process. The creation of Email Inboxes and the assignment of access rights happens directly in 8MAN. All changes are documented in revision proof reports.

Besides analysis and administration of access rights for Exchange, 8MATE for Exchange contains additional features:

- Generation of out-of-office messages without having access to the Emailaccount
- Listing of substitutes and deputies for Inboxes and "send as" access rights
- Administration of Account size and storage
- Management of mailing lists incl. members, managers and moderators
- Management of contacts
- Management of Mailboxes
- Making changes to Email addresses

### 4.3.1 Help Desk

#### 4.3.1.1 Identify access rights on mailboxes

#### Background / Purpose

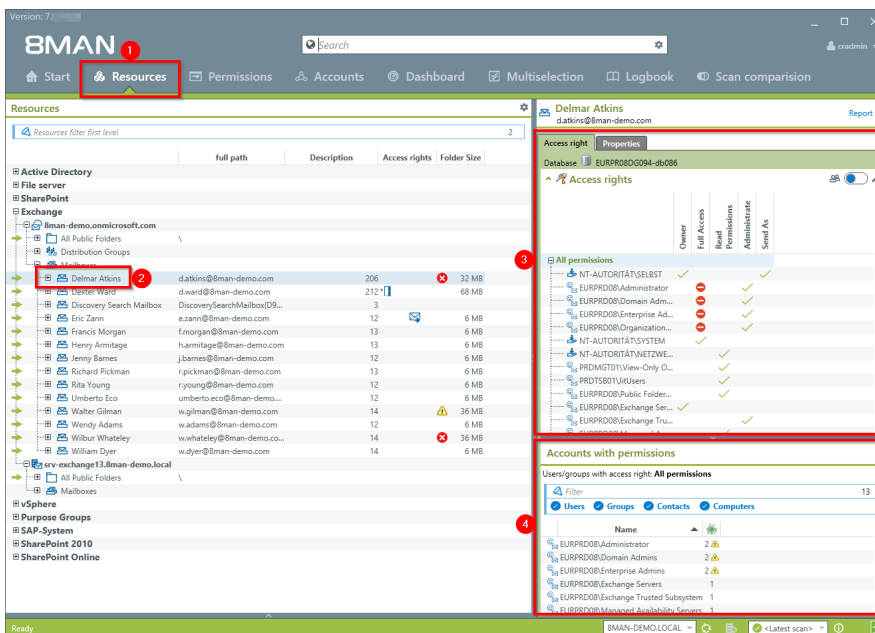
Who has access to which mailbox? 8MATE Exchange shows you all access rights in the resources view.

#### Additional Services

Report: ["Who has access to what?"](#)

Report: ["Identifying mailbox permissions"](#)

#### Step by step process



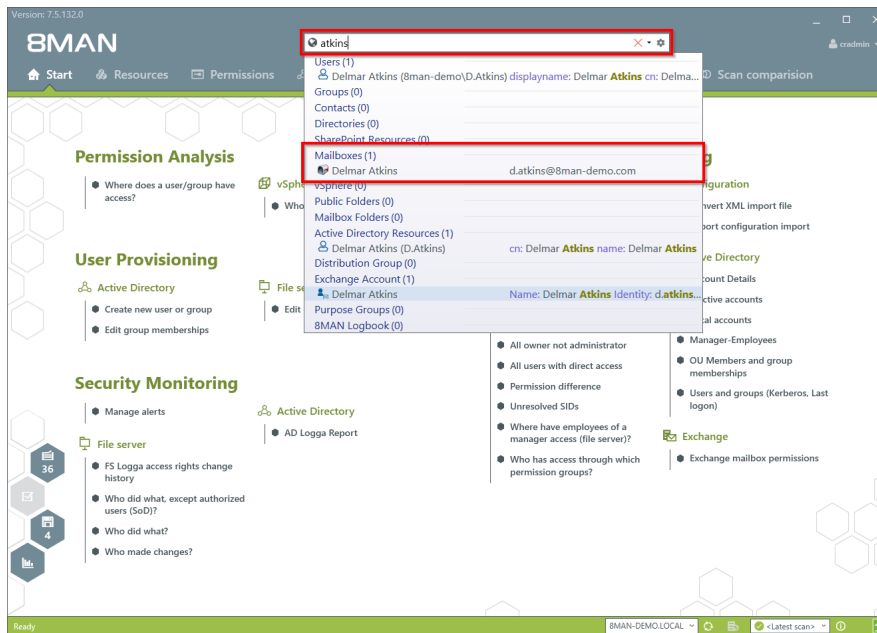
1. Select "Resources".
2. Navigate to the desired mailbox.
3. 8MAN shows you which users/groups have which rights.
4. 8MAN shows all accounts with access rights in a flat list.

### 4.3.1.2 Identify mailbox properties

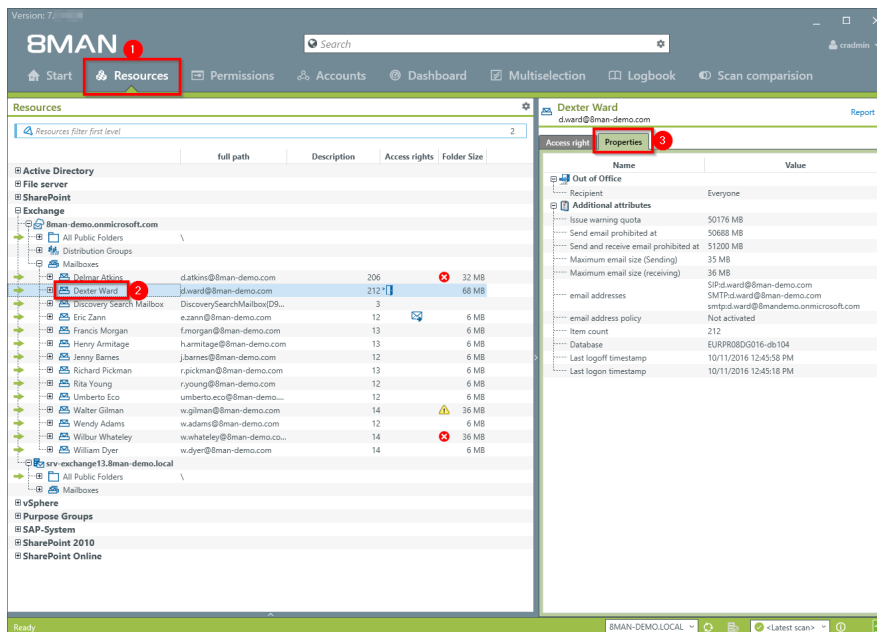
#### Background / Purpose

8MATE Exchange shows the properties of individual mailboxes.

#### Step by step process



Use the search field to find the desired mailbox.



1. 8MAN automatically changes to the resource view.
2. You are focusing on the desired mailbox.
3. Click on the tab "properties".

### 4.3.1.3 Identify access rights on public folders

#### Background / Value

Keeping an overview of access rights to public folders can be extremely challenging with native tools. 8MAN shows you the access rights situation to public folders in the resource view.

#### Additional services

Report: [Who has access to what?](#)

Report: [Identifying Mailbox access rights](#)

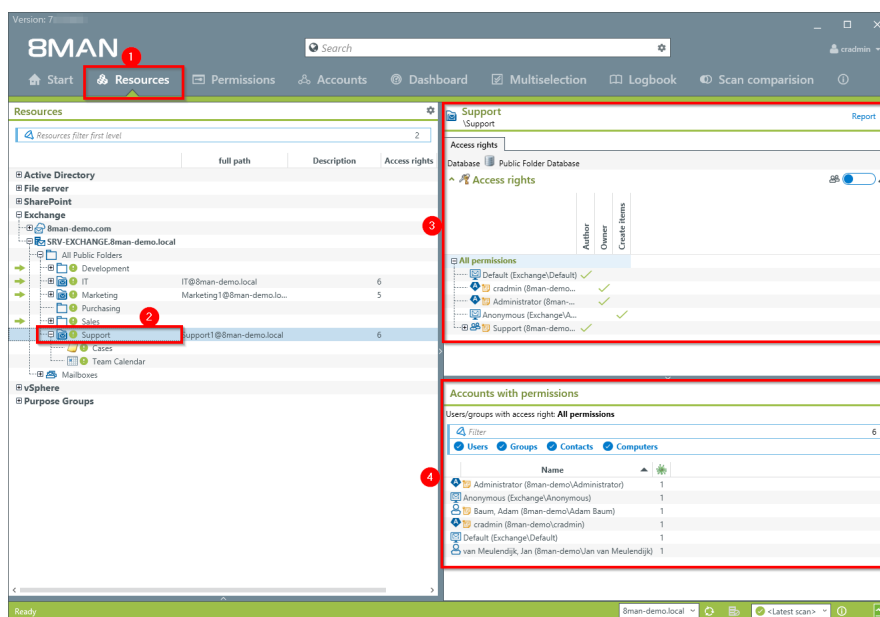
[Creating a Mailbox](#)

[Changing access rights to email accounts](#)

[Changing out-of office notice](#)

[Changing Mailbox size](#)

#### Step by step process



1. Select "Resources".
2. Navigate to the desired public folder.
3. 8MAN shows which users/groups have which access rights.
4. 8MAN shows accounts with access rights in a flat list view.



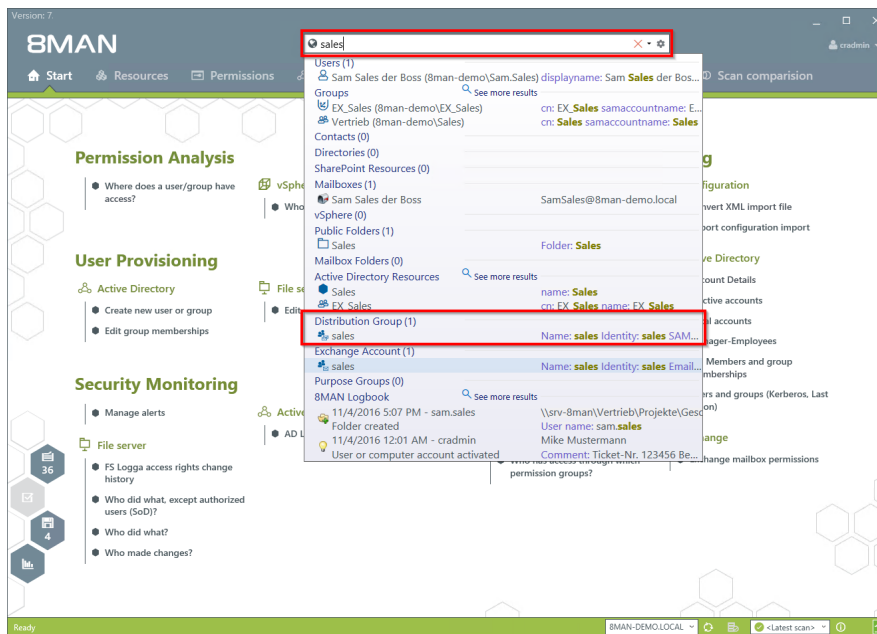
#### 4.3.1.4 Identify permissions on distribution groups

##### Background / Value

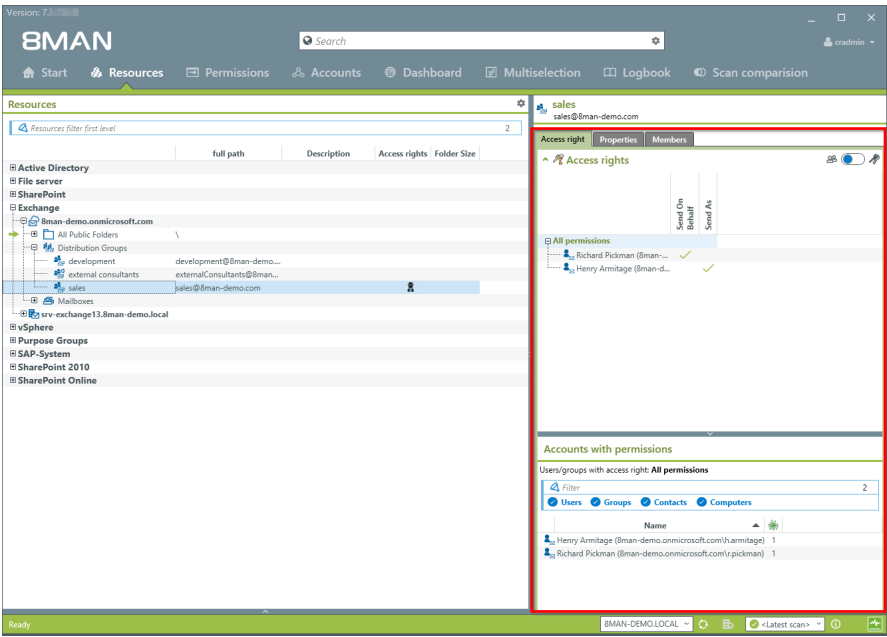
With 8MAN you can quickly check who is allowed to send Emails from which distribution list. The relevant cases are "send as" and "send on behalf of". The former is the most critical, since it is not easy to identify who actually sent the Email. In the scenario for "send on behalf" the PA or deputy sending the email is clearly recognizable.

Displaying these access rights is also possible with dynamic Exchange groups.

##### Step by step process



Use the search field to find the desired Distribution group.



8MAN shows all access rights on the right-hand side.

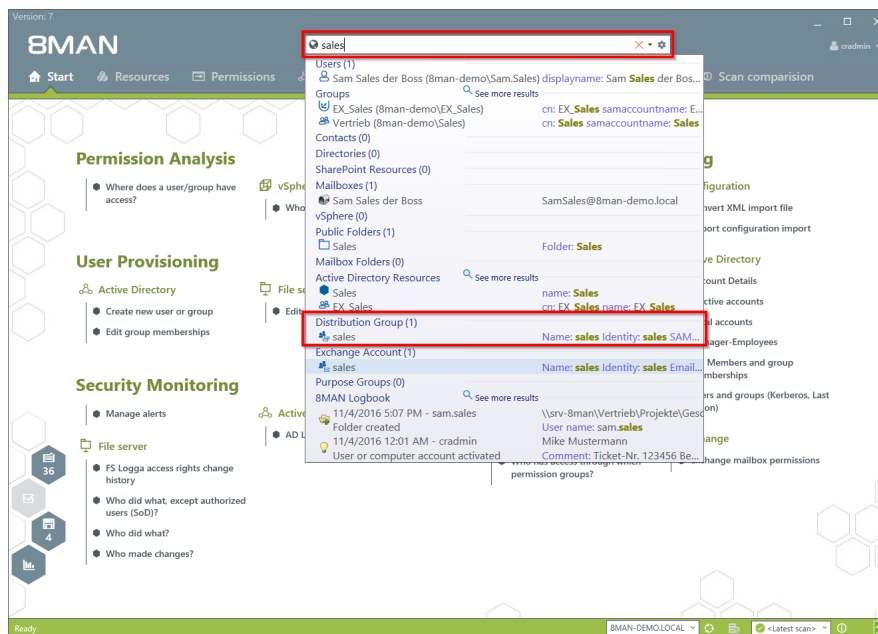
### 4.3.1.5 Identify members of distribution groups

#### Background / Purpose

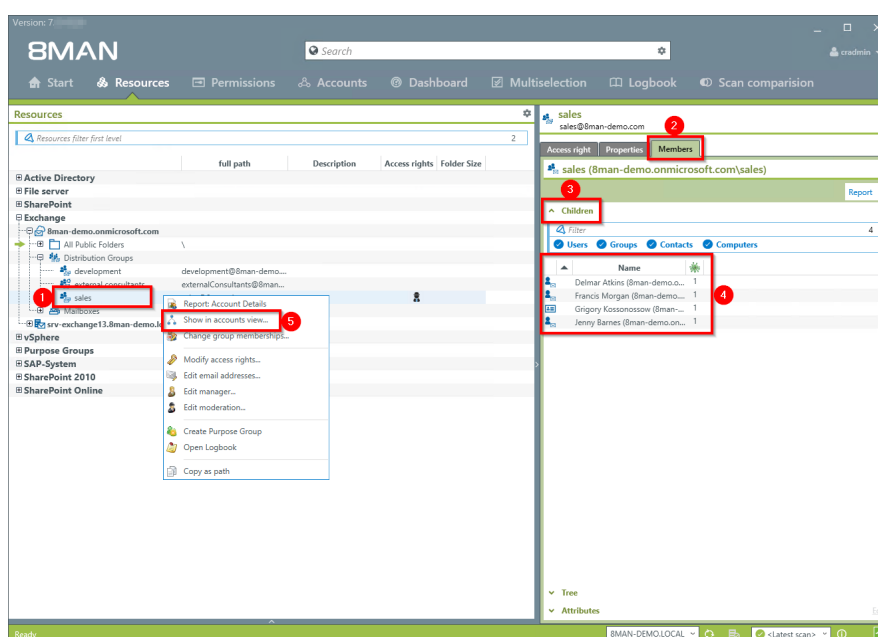
8MAN allows you to display all members and / or recipients of distribution lists. In typical 8MAN fashion this also includes nested group memberships.

This is also possible for dynamic Exchange groups.

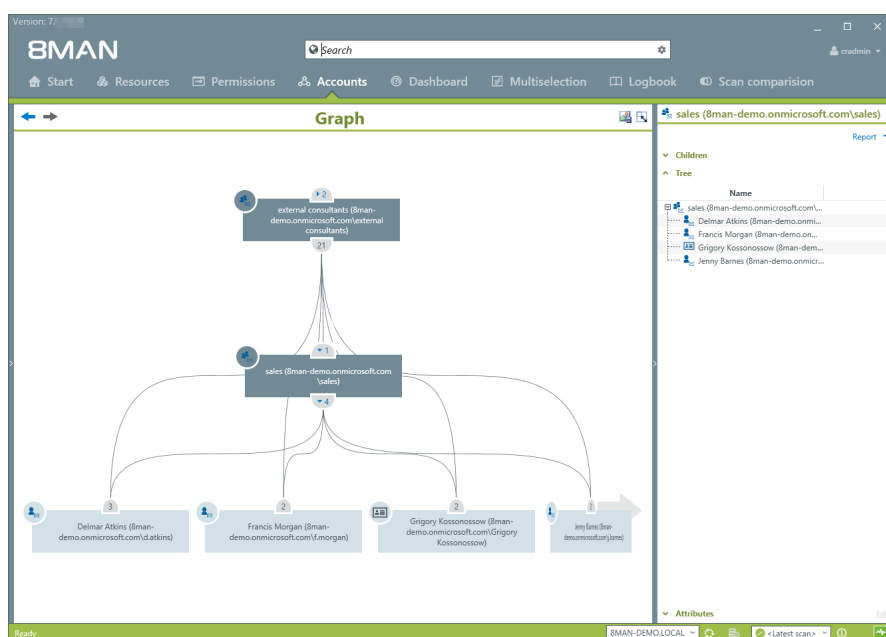
#### Step by step process



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 recursions and group memberships.*

## 4.4 +8MATE for SharePoint

8MATE for SharePoint integrates all SharePoint resources within 8MAN. This way the analysis and administration of access rights are standardized across various resources and systems. Your organization benefits of 8MAN's capabilities to display information quickly and concisely allowing you to make changes with a few simple clicks.

8MAN shows access rights in a tree structure. This allows you to quickly see who has access to which SharePoint resources. The scan comparison report tells you which changes have been made to access rights and provides you with revision proof reports of all historical activities.

8MATE for SharePoint allows you to assign access rights to SharePoint resources within the 8MAN UI. You can also standardize group assignment and naming conventions with the 8MAN Group Wizard.

## 4.4.1 Services for administrators and data owners

### 4.4.1.1 Identify access rights on SharePoint resources

#### Background / Value

8MATE for SharePoint identifies all SharePoint access rights within 8MAN. This way the analysis and administration of access rights are standardized across various resources and systems.

#### Additional Services

Report: [Who has access to what?](#)

Report: [What do users/groups have access to?](#)

[Changing access rights to SharePoint resources](#)

[Setting the naming convention for AD Groups](#)

#### Step by step process

The screenshot shows the 8MAN interface with the following components:

- Resources Pane (Left):** A tree view showing the hierarchy of resources. The 'Documents' resource is selected and highlighted with a red box and a red circle labeled '2'.
- Access rights Pane (Right):** A list of permissions for the selected resource. The 'Farm administrators' permission is selected and highlighted with a red box and a red circle labeled '3'.
- Accounts with permissions Table (Bottom Right):** A table showing the accounts that have access to the resource. The table has columns for 'Name' and 'Count'.

Name	Count
BUILTIN\Administrators	1
SP_Farm (8man-demo\SP_Farm)	1
SP_Install (8man-demo\SP_Install)	1

1. Select "Resources".
2. Navigate to the desired SharePoint resource .
3. Select an access right.
4. 8MAN displays the accounts with access rights in a flat list.

## 4.4.2 Services for administrators

### 4.4.2.1 Identify divergent access rights in the tree structure

#### Background / Value

Just like file servers, SharePoint resources also inherit access rights. 8MAN shows divergent access rights, regardless of whether they were added or removed. If the chain of inheritance is broken, 8MAN will show this in the SharePoint tree structure. You can make corrections or leave them as is, if the directory has special protection requirements.

#### Additional Services

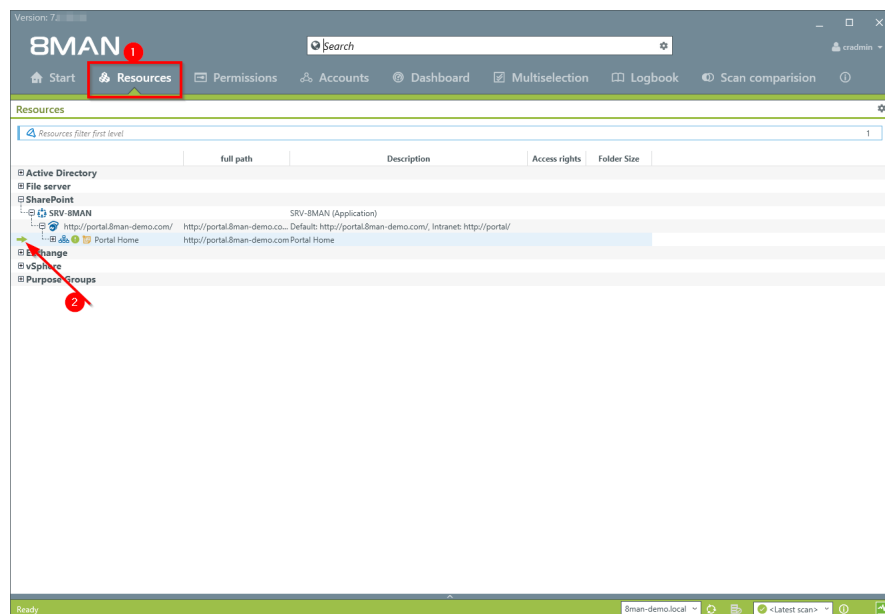
Report: [Who has access to what?](#)

Report: [What do users/groups have access to?](#)

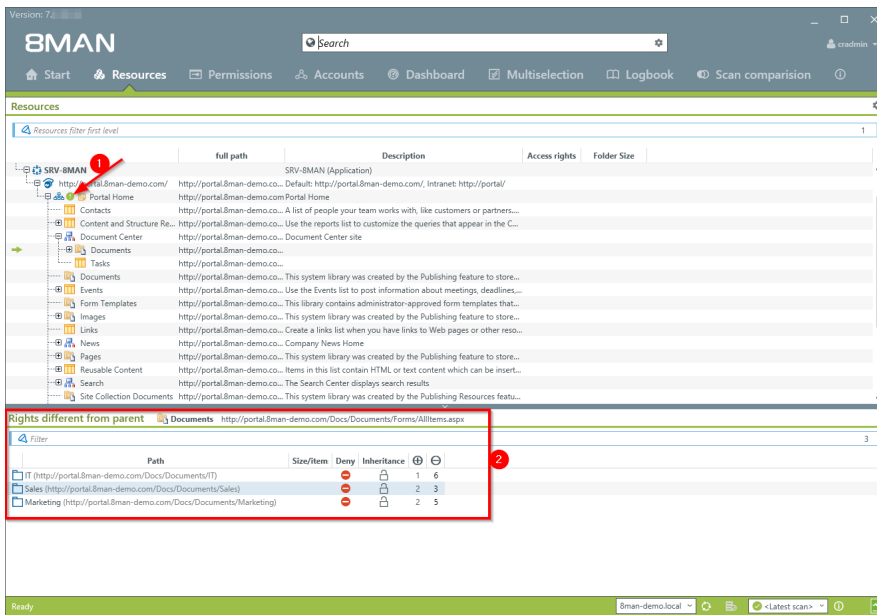
[Change access rights to SharePoint resources](#)

[Set the naming convention for AD Groups](#)

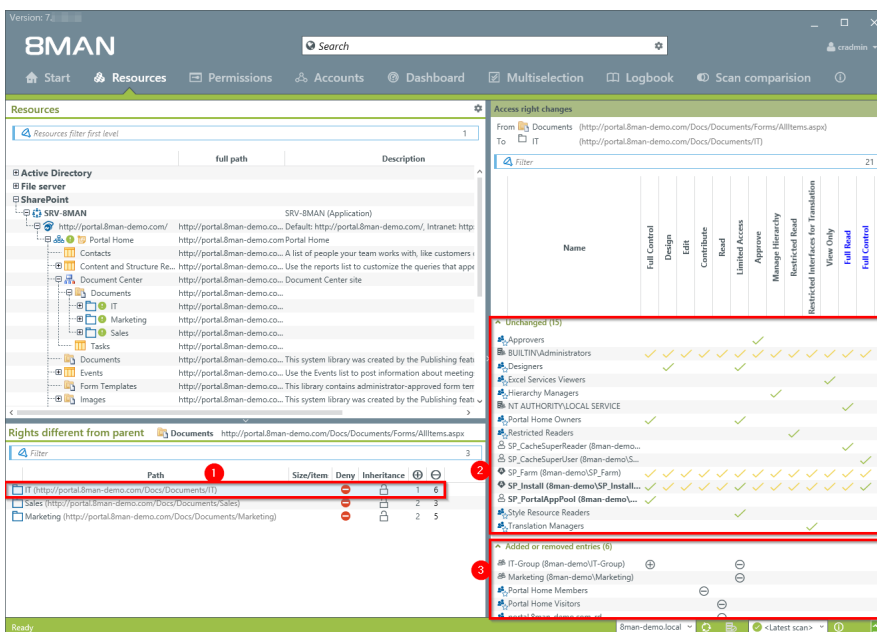
#### Step by step process



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. 8MAN shows all access rights, which correspond to the "parent" directory.
3. 8MAN shows all divergent access rights. A "Plus" signifies added access rights while a "Minus" signifies removed access rights.

## 4.5 +8MATE for Dynamics NAV

### 4.5.1 Analyze Dynamics NAV permissions

Microsoft Dynamics NAV includes business information that not everyone should see. Depending on the usage stage of the ERP solution, project budgets, purchasing price lists, annual balances or personal data from employees, suppliers or customers are stored.

Efficient authorization management is difficult with native tools. Users are members of various authorization groups, which in turn can be members of further authorization groups. In addition, the ERP solution uses company-specific authorization records, which are also granted access rights. If you want to know which users have which access rights, you need to consolidate a sufficient number of sources. The answer to the really very simple question: "Who has where access?" Becomes a costly and time-intensive search project.

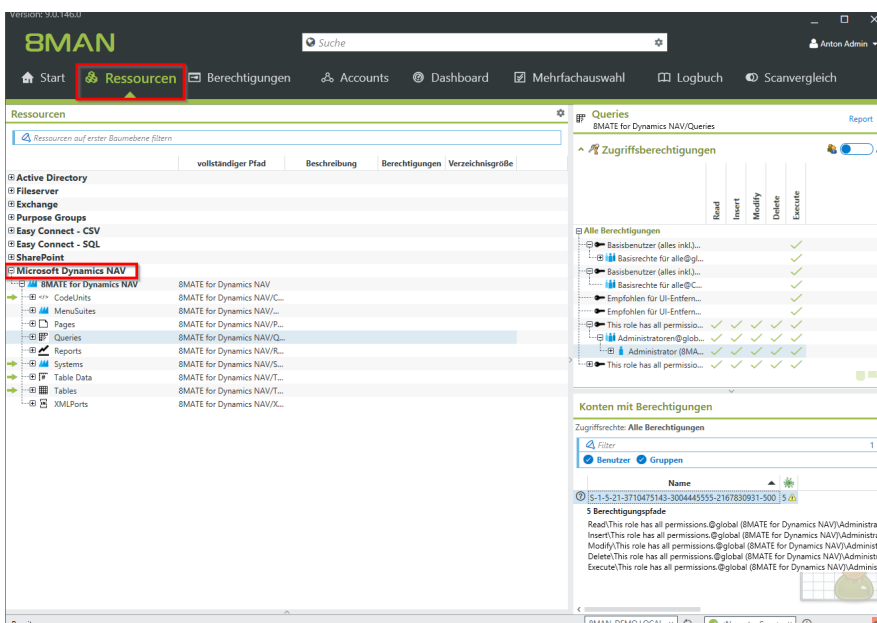
The Add-on Dynamics NAV integrates the authorization analysis of the ERP system in 8MAN. In the usual way you see all access rights in a flat list. In the first step, the module provides Services in the area of Permission Analysis and Documentation & Reporting.

#### Permission Analysis

- Identify access rights to NAV resources
- Identify multiple access paths
- Analyze the authorization situation from the past

#### Documentation & Reporting

- Report: Who has access where?
- Report: Where has the user/group access?



*In Resources, navigate to Microsoft Dynamics NAV. All permissions are displayed 8MAN typical.*





## 5. Documentation & Reporting



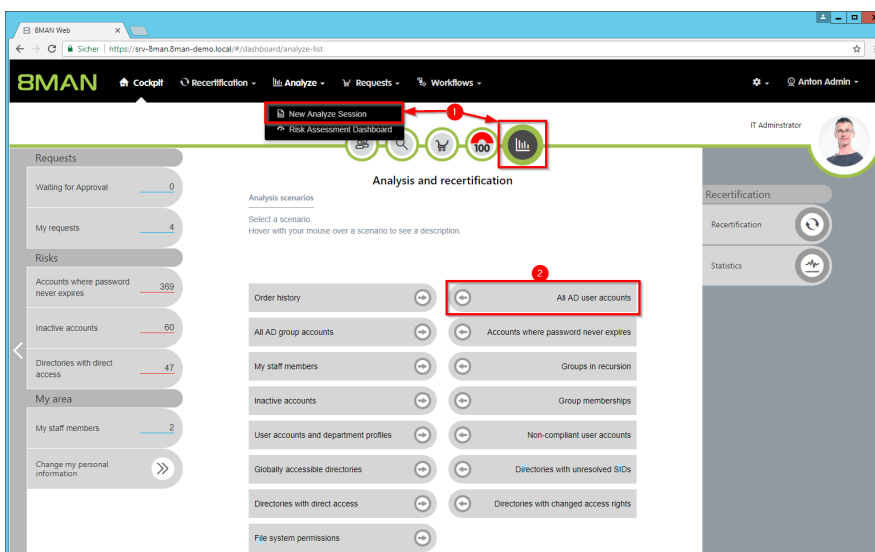
## 5.1 All Technologies

### 5.1.1 Flexible reports (web client)

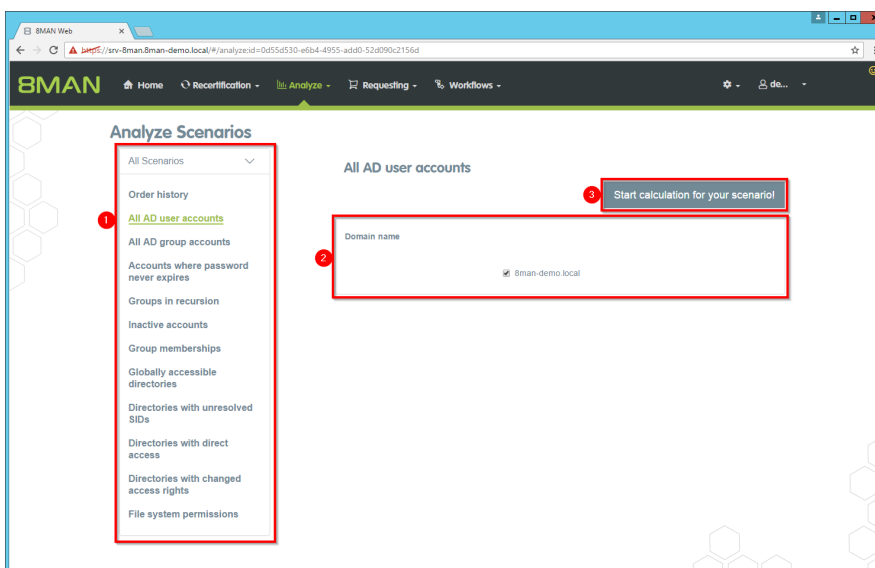
#### Background / Value

With Analyze & Act, you create flexible reports via the web client. 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.

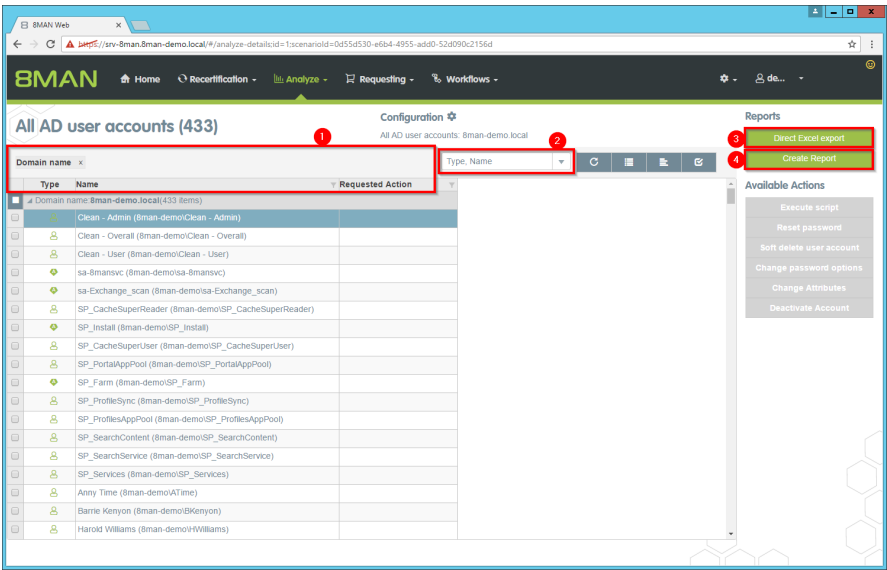
#### Step by step process



1. Click "New Analyze Session".
2. Click "All AD user accounts".



1. Optional: Change the scenario.
2. Set options for the scenario.
3. Click "Start calculation".



1. Use groupings, sorts and filters to define the report content.
2. Select the columns for the report.
3. Export the report directly to the Excel format.
4. Create a report in PDF or CSV format, which you store on the file system or send by email.

## 5.1.2 Report on 8MAN Access Rights Management activities (Logbook report)

### Background / Value

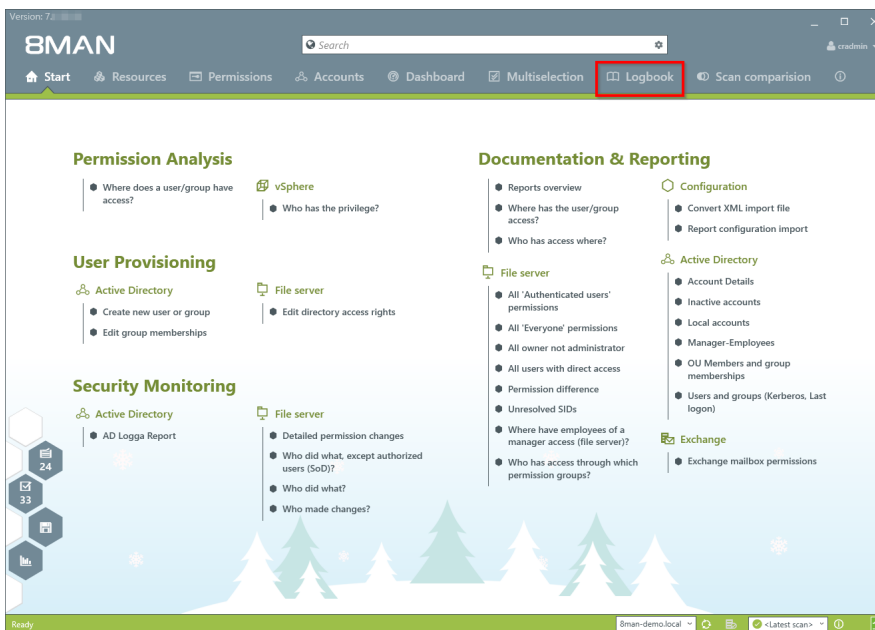
All changes made with 8MAN Enterprise are automatically recorded in the log book. This ensures compliance with a number of legal and best-practice standards and saves the time of manual documentation. The log book report allows you to capture events by person or event type within any desired time period. This ensures fully transparent processes and documentation.

If your license agreement includes 8MAN Visor as well as 8MATE AD Logga, AD events will be recorded in the log book.

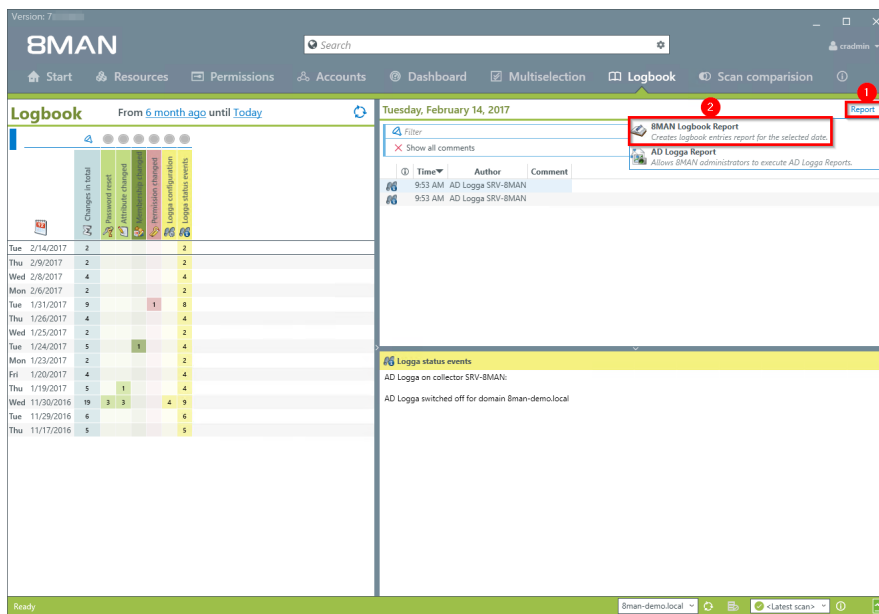
### Additional Services

The [security monitoring](#) features expands documentation to include any administrative actions performed outside of 8MAN.

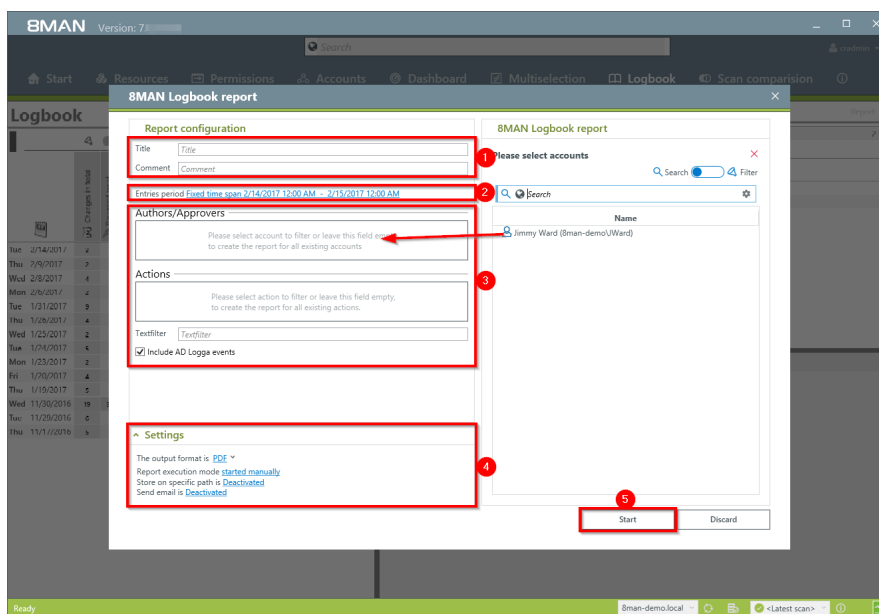
### Step by step process



Select "Logbook".



1. Click on "Report".
2. Select "8MAN log book 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.

## 5.2 Active Directory

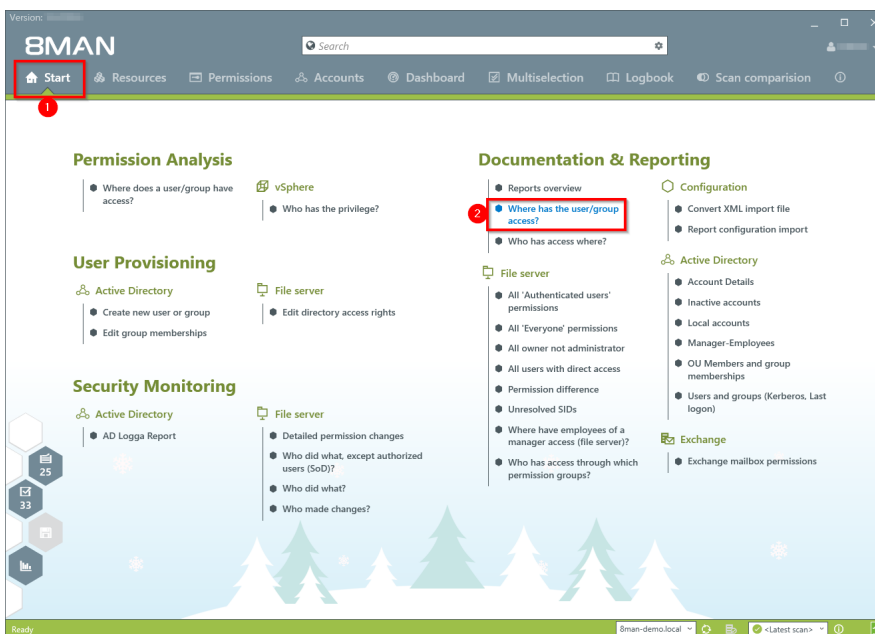
### 5.2.1 Management reports

#### 5.2.1.1 Where do users and groups have access?

#### Background / Value

The report "where do users / groups have access?" Lists all access rights of user and group accounts to selected file server directories.

#### Step by step process



1. Select "Start".
2. Click on "Where has the user/group access?".

**Report-Konfiguration**

Titel

Kommentar

☐ Nur direkte Einträge

☐ Jeder ☐ Authentifizierter Benutzer ☐ Domänen Benutzer

☒ NTFS (ohne Share-Rechte)

Sam Sales der Boss (Bman-demo\Sam.Sales)

☐ Wo hat Benutzer/Gruppe keinen Zugriff

☒ Nur Pläne mit geänderten Berechtigungen berücksichtigen

**Ressourcen**

☐ Platz ☒ Organisations-Kategorien

grn-Bman

**Einstellungen**

Das Ausgabeformat ist PDF \*

Erzeuge den Report für alle Konten zusammengefasst in einem Dokument.

Reportausführung wird manuell gestartet

Speichern ist deaktiviert

E-Mail Versenden ist deaktiviert

**Bitte Benutzer/Gruppen auswählen**

Bitte Benutzer/Gruppen auswählen 3 von 620 X

☒ Benutzer ☒ Gruppen

Name

Erstellungen eingehender Gesamtstrukturvertrauensstellung (Erstell...

Sam Sales der Boss (Bman-demo\Sam.Sales)

Urai, Sam (Bman-demo\Sam.Urai)

Start Verwerfen

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.



### 5.2.1.2 Employees of a manager

#### Background / Value

Data Owners that have some knowledge of Active Directory can view attributes and group memberships of their employees.

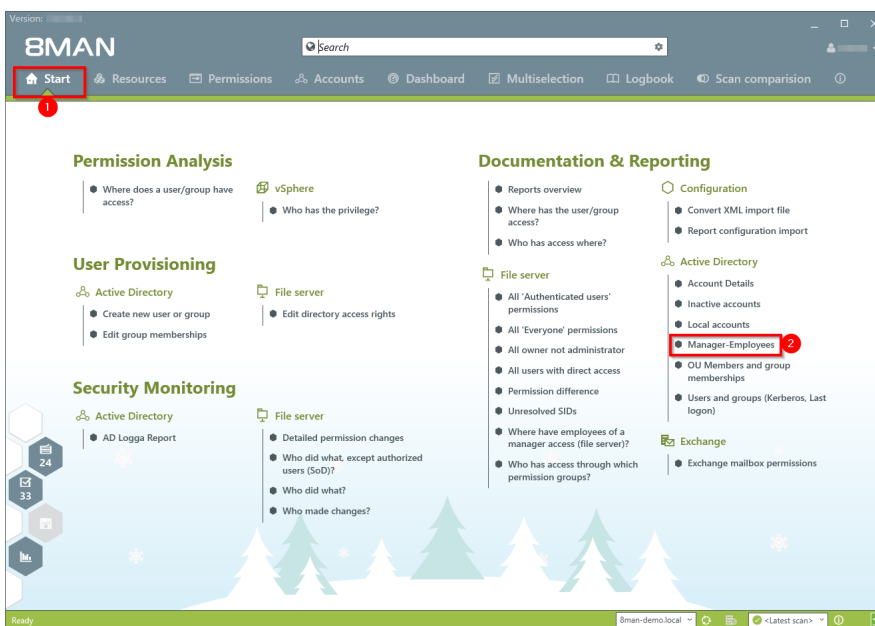
The report utilizes information from the attribute "manager" in Active Directory.

#### Additional Services

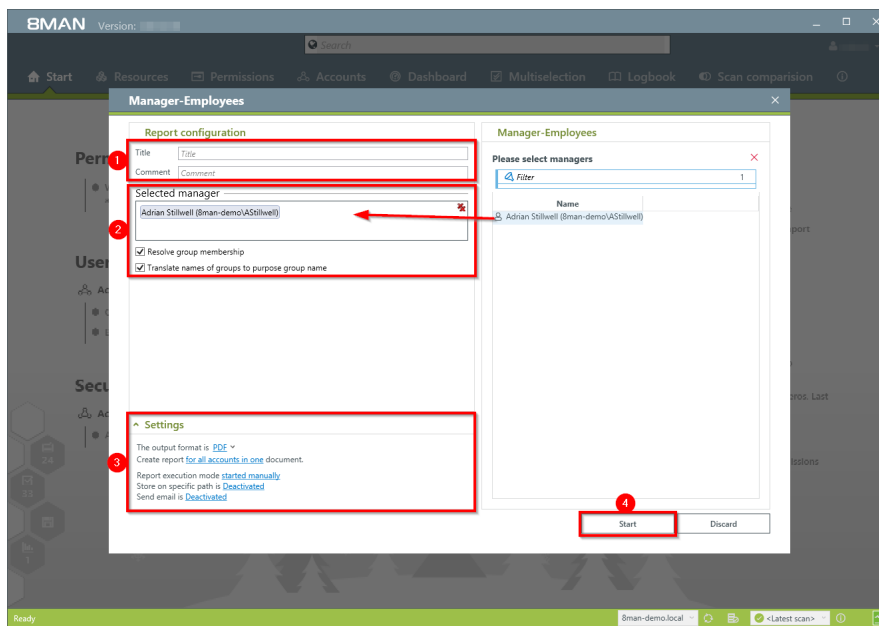
For more detailed information and the inclusion of assigned file server resources we recommend the report:

[Where have employees of a manager 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.

## 5.2.2 Reports for administrators

### 5.2.2.1 Display user account details

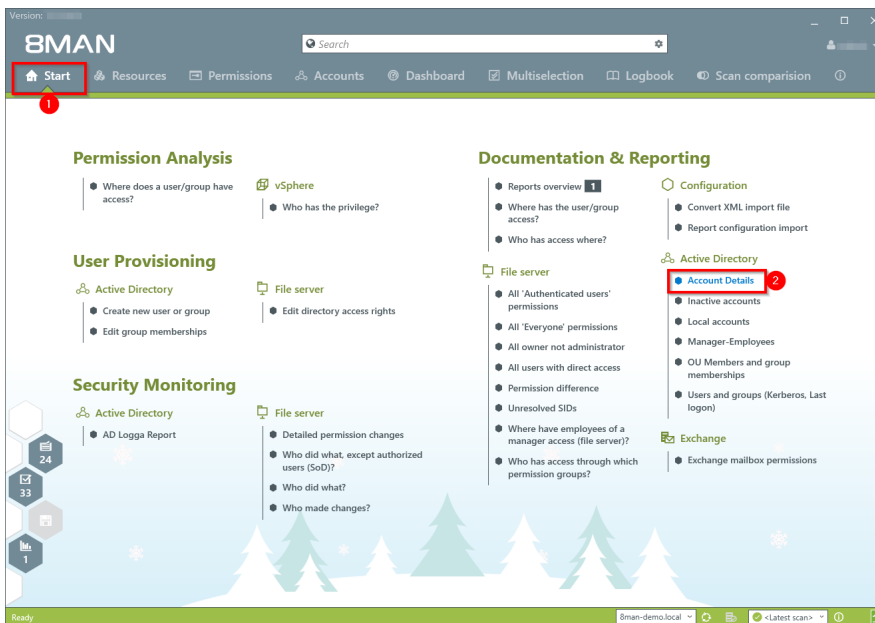
#### Background / Value

Capturing account details is key to a professional Active Directory Management.

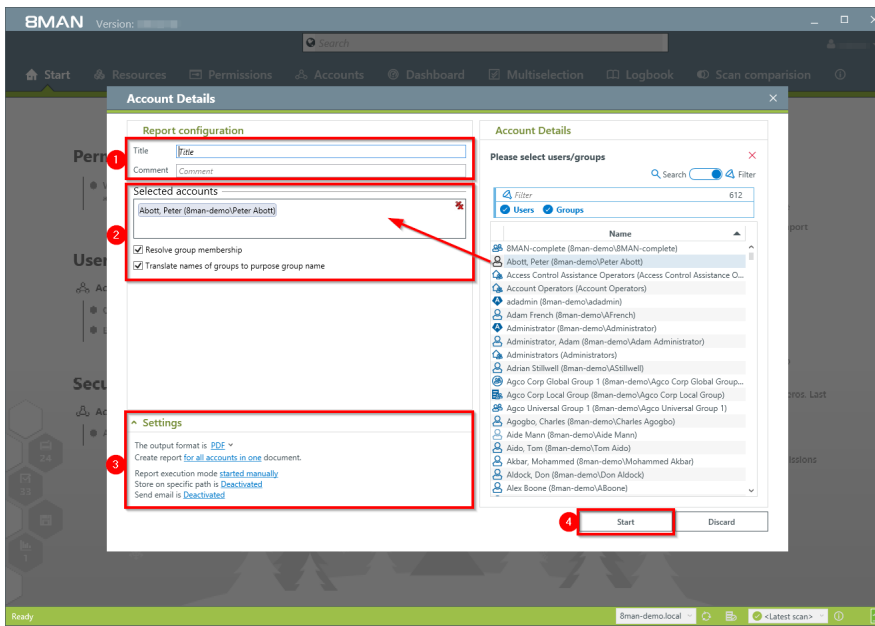
The following information is shown in a structured report:

- 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

#### 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.
3. Define the desired report settings.
4. Start the report.

### 5.2.2.2 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. 8MAN displays all inactive accounts in Active Directory. You can delete or deactivate old and redundant accounts.

#### Additional Services

[Delete a user and his permissions](#)

["Soft" delete a user account](#)

[Deactivate a user account](#)

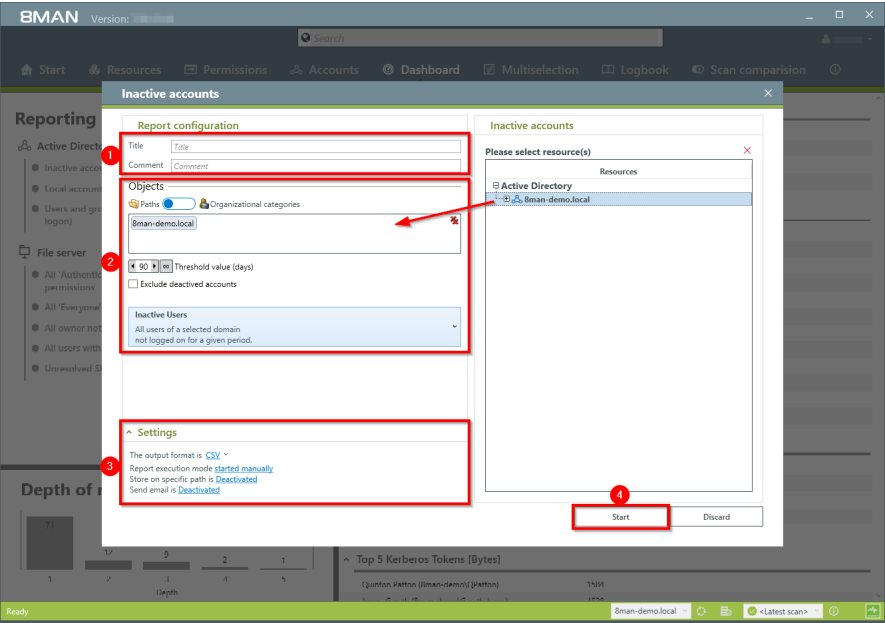
[Identify inactive accounts](#) (web client)

[Deactivate user accounts in bulk](#) (web client)

#### Step by step process

The screenshot shows the 8MAN web interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard' (highlighted with a red box and number 1), 'Multiselection', 'Logbook', 'Scan comparison', and a user profile icon. The left sidebar shows 'Reporting' with 'Active Directory' expanded, where 'Inactive accounts' is highlighted with a red box and number 2. Below this, 'File server' permissions are listed. The main content area displays 'Users and other accounts' with a table showing counts for Users (429), Users (Disabled) (6), Administrators (12), and Administrators (Disabled) (0). It also shows 'Groups' with counts for All Groups (183), Groups with members (104), Empty groups (76), Groups in recursions (3), and various security groups. At the bottom, 'OU / Contacts / More' and 'Top 5 Kerberos Tokens [Bytes]' are visible.

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.

Days (Difference to current date)			
Name	Path	Last Logon Timestamp	Days (Difference to current date)
SP_SearchService (8man-demo\SP_Se	CN=SP_SearchService,OU=Service Accounts,DC=8man-demo	5/16/2014 4:37:14 PM	1006
Eric Reid (8man-demo\EReid)	CN=Eric Reid,OU=TestUsers,DC=8man-demo,DC=local	10/10/2014 4:28:02 PM	859
Albar, Mohammed (8man-demo\Moh	CN=Mohammed Albar,OU=TestUsers,DC=8man-demo,DC=local	10/27/2014 9:27:50 AM	843
Quinton Patton (8man-demo\QPatt	CN=Quinton Patton,OU=TestUsers,DC=8man-demo,DC=local	11/25/2014 3:31:09 PM	813
Adrian Stillwell (8man-demo\AS	CN=Adrian Stillwell,OU=TestUsers,DC=8man-demo,DC=local	5/27/2015 3:06:13 PM	630
Ali Mente (8man-demo\Ali Mente)	CN=Ali Mente,OU=TestUsers,DC=8man-demo,DC=local	6/24/2015 1:47:33 PM	603
Torrey Smith (8man-demo\TSmith)	CN=Torrey Smith,OU=TestUsers,DC=8man-demo,DC=local	6/24/2015 3:25:49 PM	602

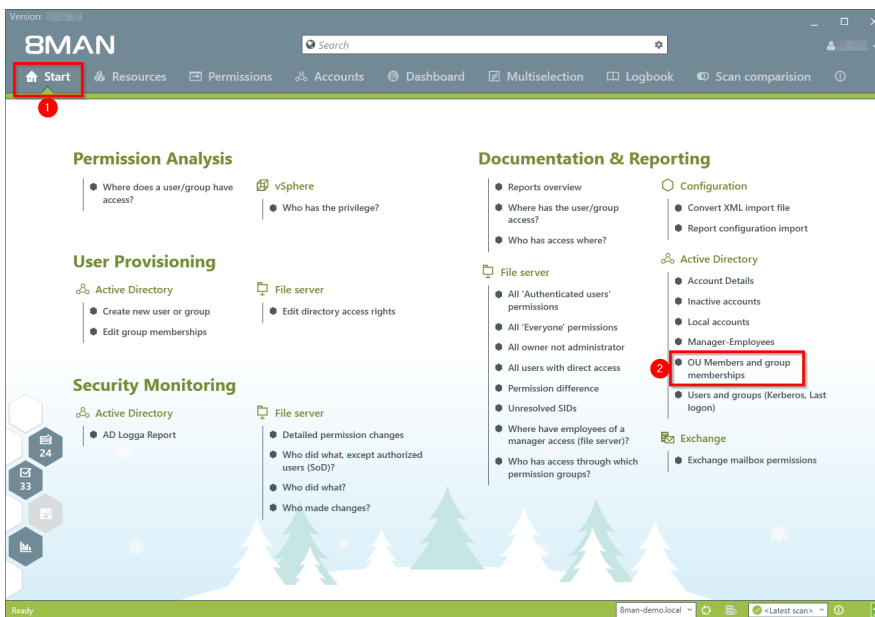
Review the data in the report. If using historical scan data there may be differences in the days since the last login.

### 5.2.2.3 OU members und group memberships

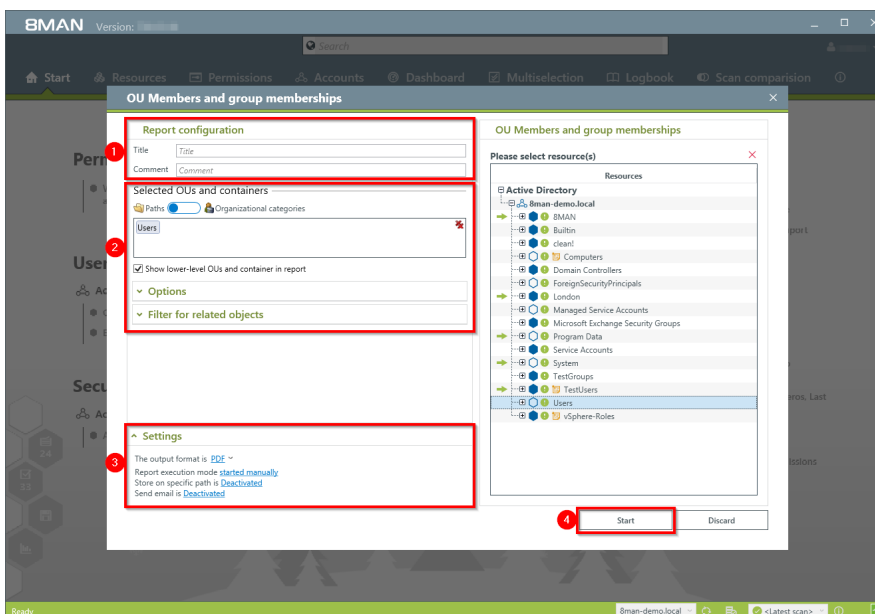
#### Background / Value

8MAN allows a quick review of any groups and user contained in an Organisational Unit (OU). This ensures that you can obtain a complete overview of all users and groups within any OU.

#### 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 of the report.
3. Define the desired report settings.
4. Start the report.

### 5.2.2.4 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.

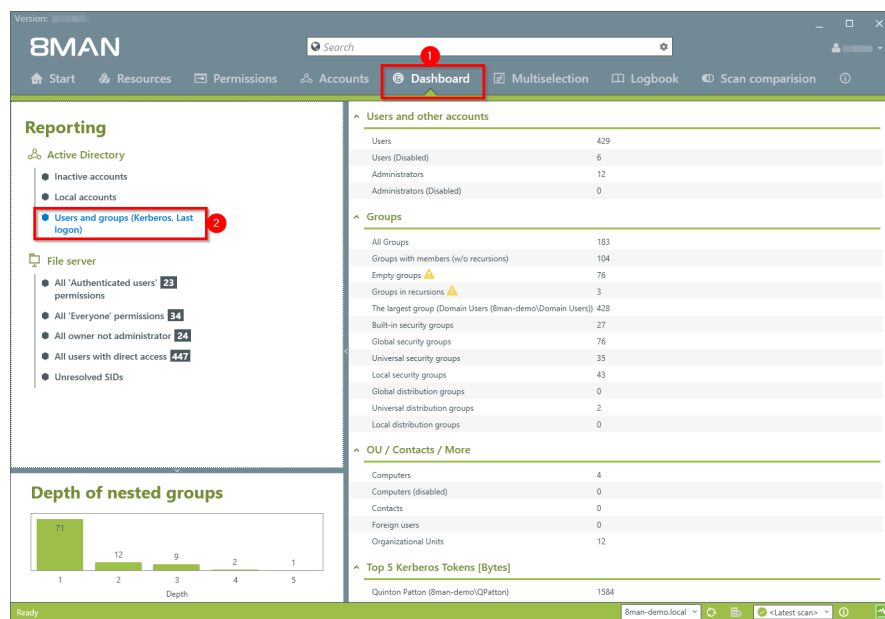
In addition the following information is also displayed:

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

#### Groups

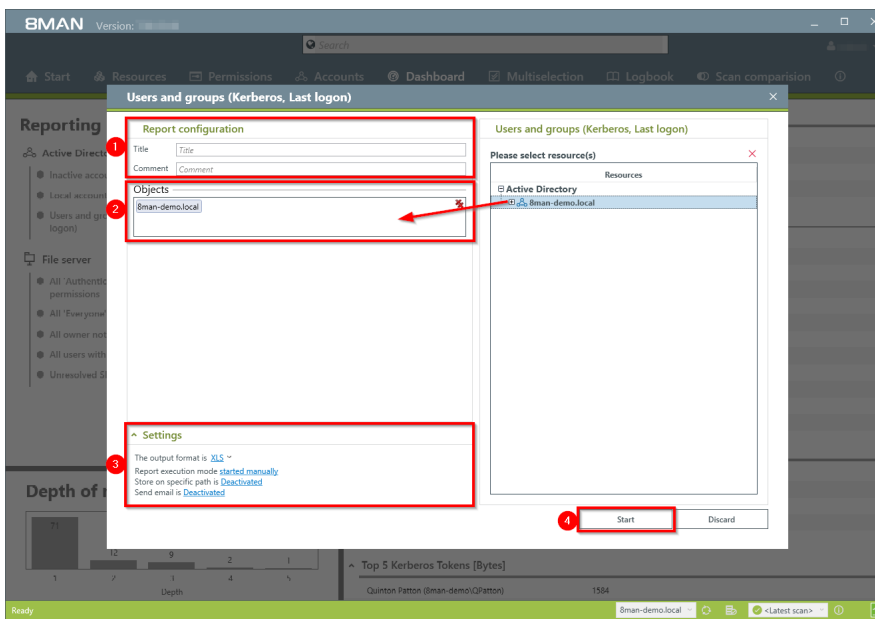
Displays direct and indirect group memberships as well as group scope (local, global, universal)

#### 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 report settings.
4. Start the report.

Display Name	Disabled	Account Expires	PWD don't expir	Last Logon	Last Logon Timestamp	Type	Direct Membership	Indirect Membership	Total
1 Report of all users for Bman-demo.local									
4 Admin User (Bman-demo/Admin User)	No	Account never expires	No	N/A	N/A	User	2	1	3
5 adadmin (Bman-demo/adadmin)	No	Account never expires	Yes	N/A	N/A	User	4	1	5
6 Adam French (Bman-demo/AFrench)	No	Account never expires	No	N/A	N/A	User	2	1	3
7 Administrator (Bman-demo/Administrator)	No	Account never expires	Yes	2/16/2017 1:02:41 PM	2/14/2017 11:40:29 AM	User	10	18	28
8 Administrator, Adam (Bman-demo/Adam Administrator)	No	Account never expires	No	N/A	N/A	User	3	2	5
9 Adrian Stillwell (Bman-demo/ASStillwell)	No	Account never expires	No	N/A	5/27/2015 3:06:13 PM	User	4	2	6
10 Agobho, Charles (Bman-demo/Charles Agobho)	No	Account never expires	No	N/A	N/A	User	2	1	3
11 Ade Mann (Bman-demo/Ade Mann)	Yes	Account never expires	No	N/A	N/A	User	2	1	3
12 Ado, Tom (Bman-demo/Tom Ado)	No	Account never expires	No	N/A	N/A	User	2	1	3
13 Akbar, Mohammed (Bman-demo/Mohammed Akbar)	No	Account never expires	No	N/A	10/27/2014 9:27:50 AM	User	2	1	3
14 Aldock, Don (Bman-demo/Don Aldock)	No	Account never expires	No	N/A	N/A	User	2	1	3
15 Alex Boone (Bman-demo/ABoone)	No	Account never expires	No	N/A	N/A	User	4	2	6
16 Alexandre Sourzac (Bman-demo/ASourzac)	No	Account never expires	No	N/A	N/A	User	3	1	4
17 Ali Eye (Bman-demo/Ali Esh)	No	Account never expires	No	N/A	N/A	User	3	8	11
18 Ali Menta (Bman-demo/Ali Menta)	No	Account never expires	No	5/29/2013 11:47:02 AM	6/24/2015 1:47:33 PM	User	3	4	7
19 Alan Johnson (Bman-demo/Alan Johnson)	No	Account never expires	No	N/A	N/A	User	2	1	3
20 Ammy Twana (Bman-demo/ATwana)	No	Account never expires	No	N/A	N/A	User	4	9	13
21 Anda, Lou (Bman-demo/Lou Anda)	No	Account never expires	No	N/A	N/A	User	2	1	3
22 Andrew, Susac (Bman-demo/ASusac)	No	Account never expires	No	N/A	N/A	User	3	7	10
23 Angel Carreras (Bman-demo/ACarreras)	No	Account never expires	No	N/A	N/A	User	4	9	13
24 Anick, Mike (Bman-demo/AMick)	No	Account never expires	No	N/A	N/A	User	2	1	3
25 Arny Time (Bman-demo/ATime)	No	Account never expires	No	N/A	N/A	User	5	3	8
26 Anthony Davis (Bman-demo/ADavis)	No	Account never expires	No	N/A	N/A	User	6	8	14
27 Artian, Sam (Bman-demo/Sam Artian)	No	Account never expires	No	N/A	N/A	User	2	1	3
28 Ayshen, Don (Bman-demo/Don Ayshen)	No	Account never expires	No	N/A	N/A	User	2	1	3
29 Baba, Ali (Bman-demo/Ali Baba)	No	Account never expires	No	N/A	N/A	User	2	1	3
30 Back, Helen (Bman-demo/Helen Back)	No	Account never expires	No	N/A	N/A	User	3	1	4
31 Batek, Luca (Bman-demo/Luca Batek)	No	Account never expires	No	N/A	N/A	User	2	1	3
32 Banks, Robin (Bman-demo/Robin Banks)	No	Account never expires	No	N/A	N/A	User	2	1	3
33 Barne Kenyon (Bman-demo/BKenyon)	No	Account never expires	No	N/A	N/A	User	2	1	3
34 Barrow, Will (Bman-demo/WBarrow)	No	Account never expires	No	N/A	N/A	User	2	1	3
35 Bart Postema (Bman-demo/BPostema)	No	Account never expires	No	N/A	N/A	User	7	1	8
36 Bath, But (Bman-demo/But Bath)	No	Account never expires	No	N/A	N/A	User	2	1	3

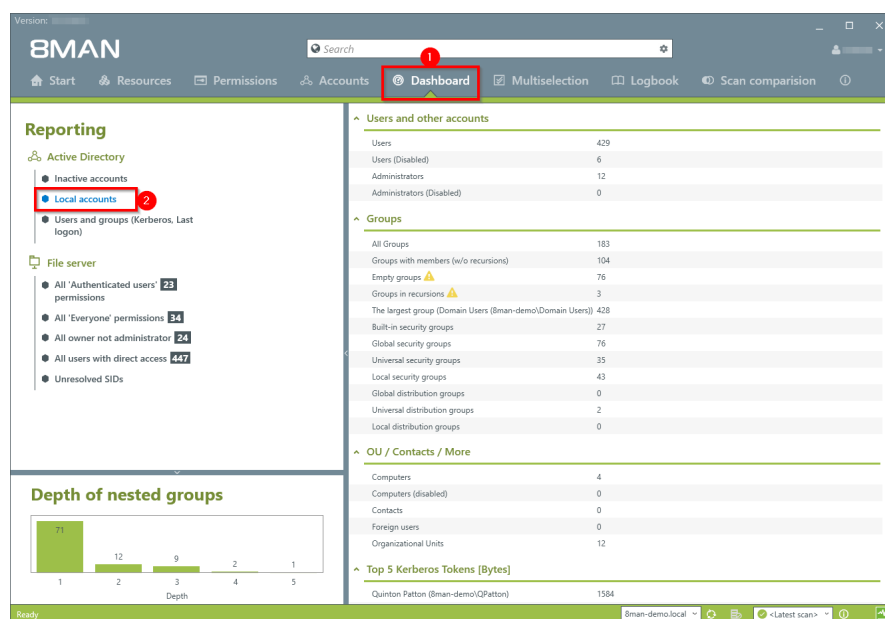
Open the report in Excel and apply the desired filters.

### 5.2.2.5 Identify local accounts

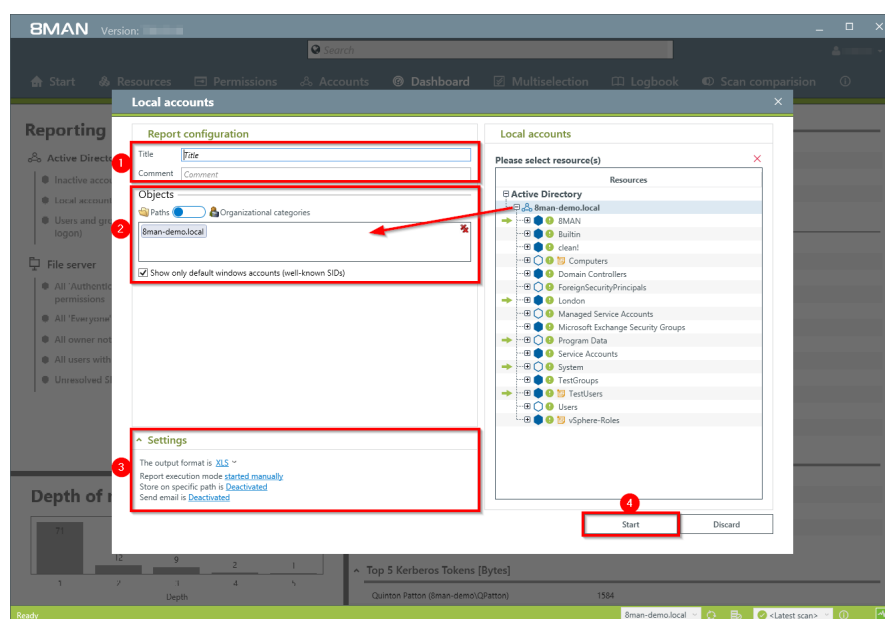
#### Background / Value

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.

#### 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.
3. Define the desired report settings.
4. Start the report.

### 5.2.3 Organizational help for administrators

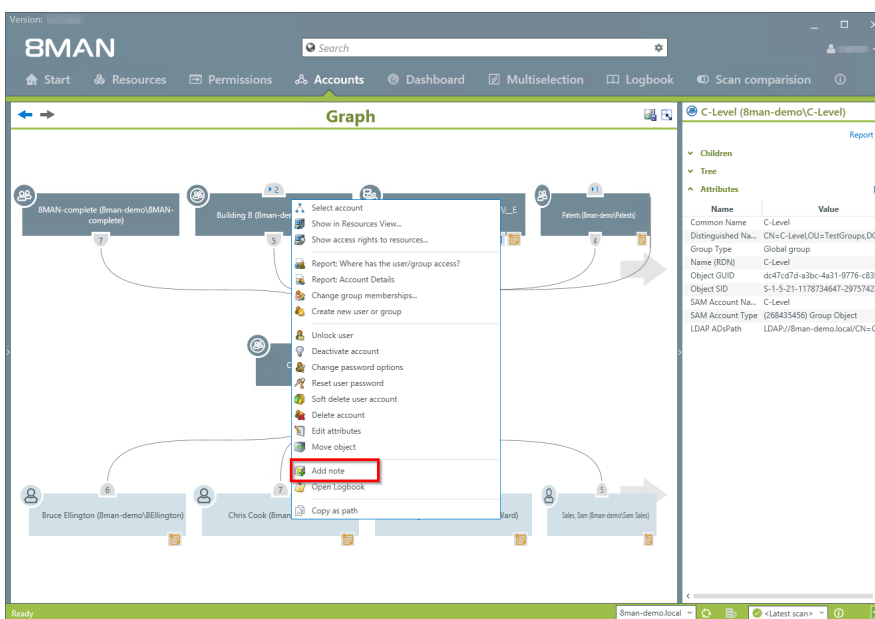
Besides automated documentation and reports 8MAN also includes a number of additional documentation features. These allow you to add post-its to objects manually or give AD groups aliases with the "purpose groups" feature.

#### 5.2.3.1 Add notes to user accounts and groups

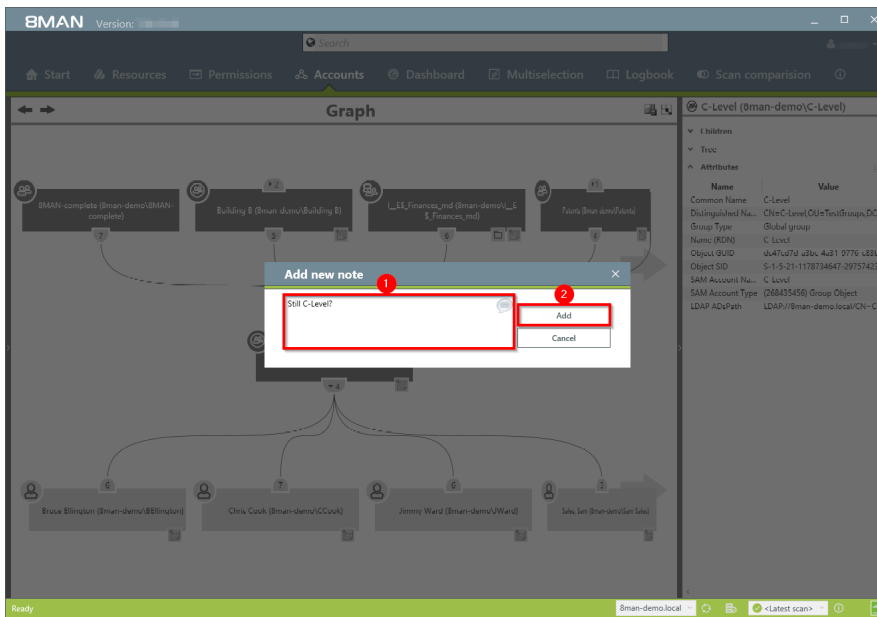
##### Background / Value

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

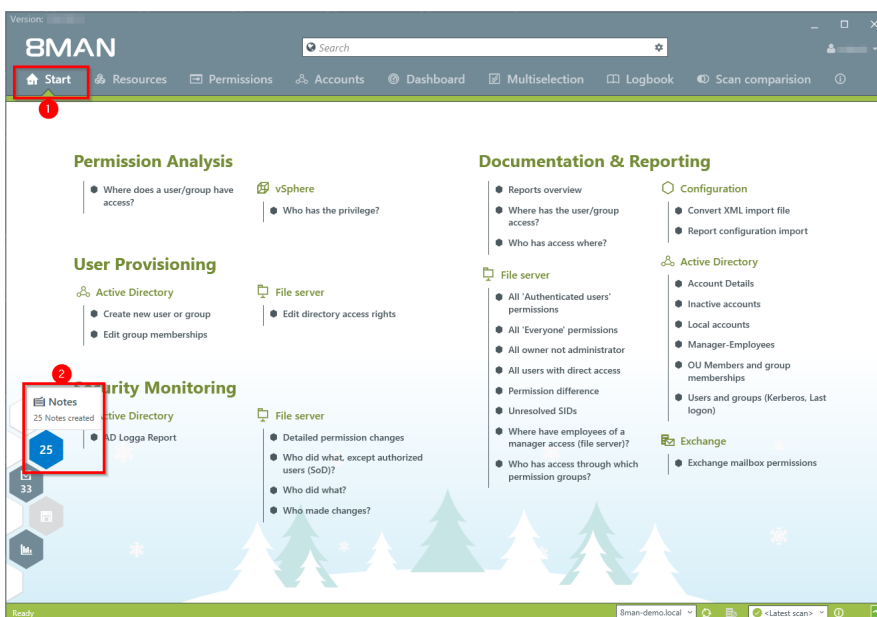
##### Step by step process



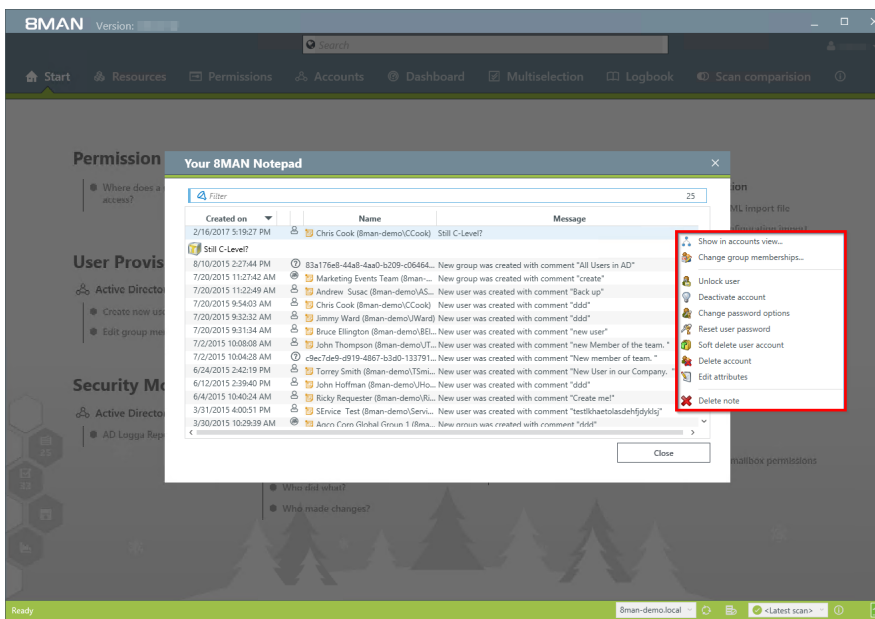
Right-click on an account and select "Add Note" from the context menu.



1. Add a comment.
2. Click on "Add".



1. Select "Start".
2. Click on the hexagon to access your notes.



The list shows all notes. You can trigger a number of different functionalities by right clicking on the note.

### 5.2.3.2 Purpose Groups: Give aliases to groups

#### Background / Value

Purpose groups add clear descriptions to AD groups. Normally these groups have very technical naming convention and so it is often difficult for an Administrator to tell what the purpose of an AD group is. Adding aliases can make the picture much clearer.

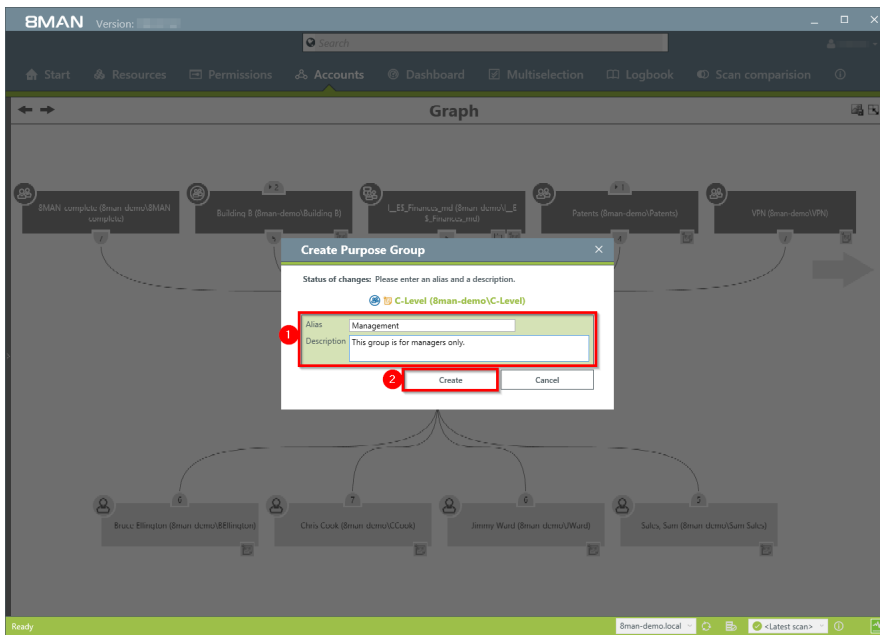
**The alias descriptions are only visible in the 8MAN UI. The actual group names remain the same in Active Directory.**

#### 5.2.3.2.1 Create a purpose group

##### Step by step process



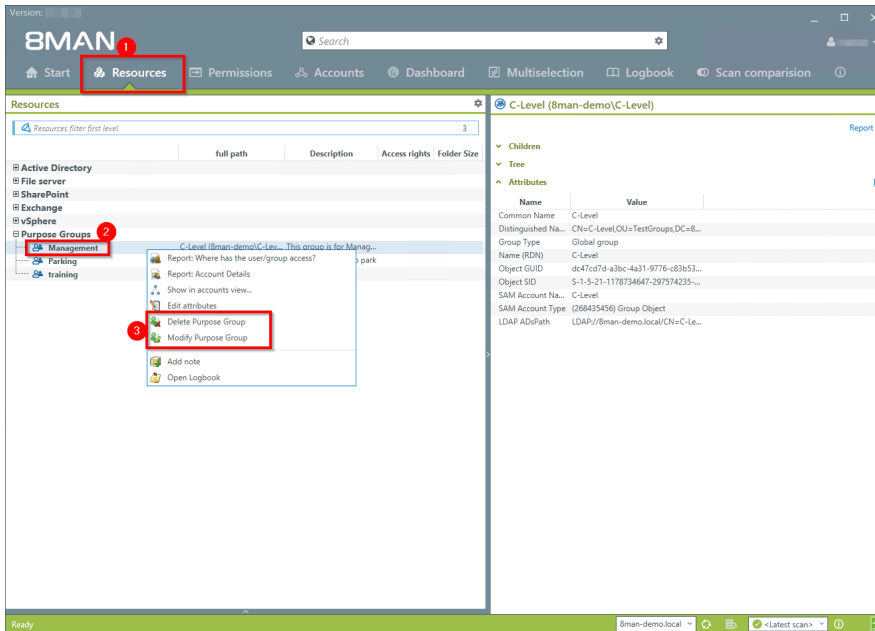
*Right-click on an AD group.  
Select "Create Purpose Group"  
from the context menu.*



1. Give the AD group an alias and add a description for the group.
2. Click on "Create".

## 5.2.3.2.2 Delete or modify a purpose group

## Step by step process



1. Select "Resources".
2. Select the desired purpose group by right-clicking on it.
3. Select "Delete Purpose Group" or "Modify Purpose Group" from the context menu.

The removal process only affects the purpose group, the added alias in 8MAN. Non changes are made to Active Directory.



## 5.3 File server

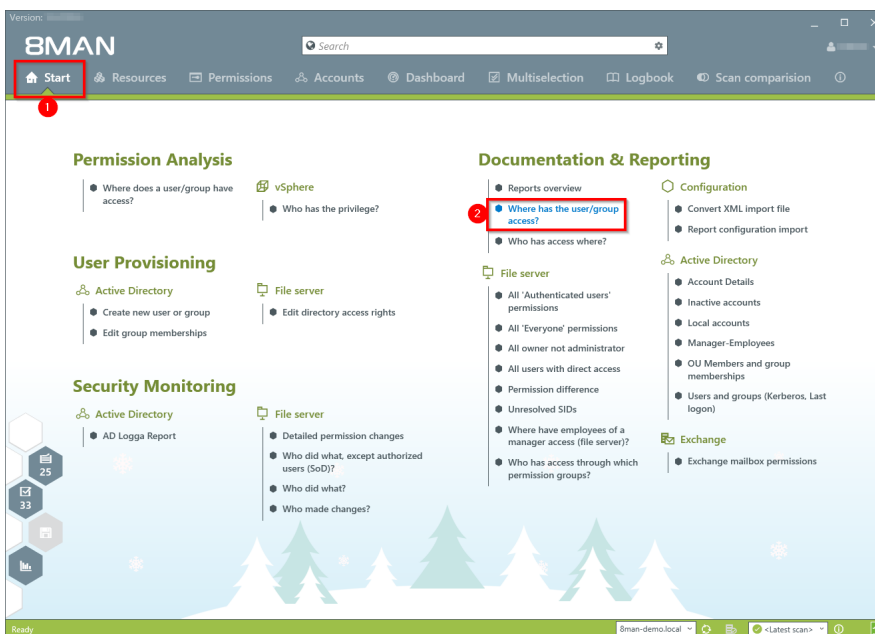
### 5.3.1 Management reports

#### 5.3.1.1 Where do users and groups have access?

#### Background / Value

The report "where do users / groups have access?" Lists all access rights of user and group accounts to selected file server directories.

#### Step by step process



1. Select "Start".
2. Click on "Where has the user/group access?".

**Report-Konfiguration**

Titel

Kommentar

☐ Nur direkte Einträge

☐ Jeder ☐ Authentifizierter Benutzer ☐ Domänen Benutzer

☒ NTFS (ohne Share-Rechte)

Sam Sales der Boss (Bman-demo\Sam.Sales)

☐ Wo hat Benutzer/Gruppe keinen Zugriff

☒ Nur Pläne mit geänderten Berechtigungen berücksichtigen

**Ressourcen**

☐ Platz ☒ Organisations-Kategorien

grn-Bman

**Einstellungen**

Das Ausgabeformat ist PDF

Erzeuge den Report für alle Konten zusammengefasst in einem Dokument.

Reportausführung wird manuell gestartet

Speichern ist deaktiviert

E-Mail Versenden ist deaktiviert

**Bitte Benutzer/Gruppen auswählen**

Bitte Benutzer/Gruppen auswählen

3 von 620

Name

Erstellungen eingehender Gesamtstrukturvertrauensstellung (Erstell...

Sam Sales der Boss (Bman-demo\Sam.Sales)

Urai, Sam (Bman-demo\Sam.Urai)

Start Verwerfen

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.

### 5.3.1.2 Who has access to what?

#### Background / Value

Data owners and managers know who should have access to which resources. Full transparency is very important especially for directories containing sensitive information. The report "Who has access to what?" gives you a full overview of all access rights (for example "read only" and "write") including users who can execute these access rights.

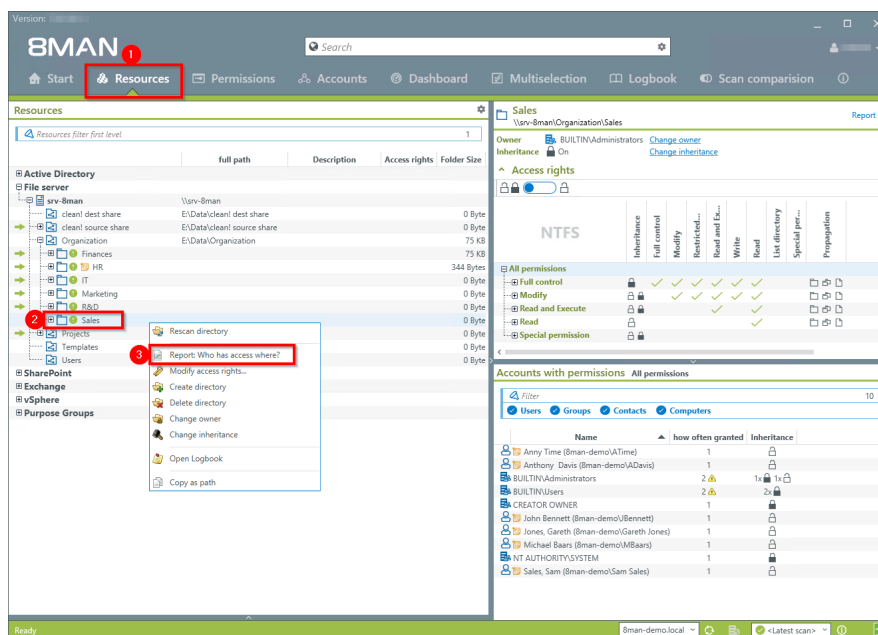
The report allows responsible managers to make information based decisions in order to answer two central questions:

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

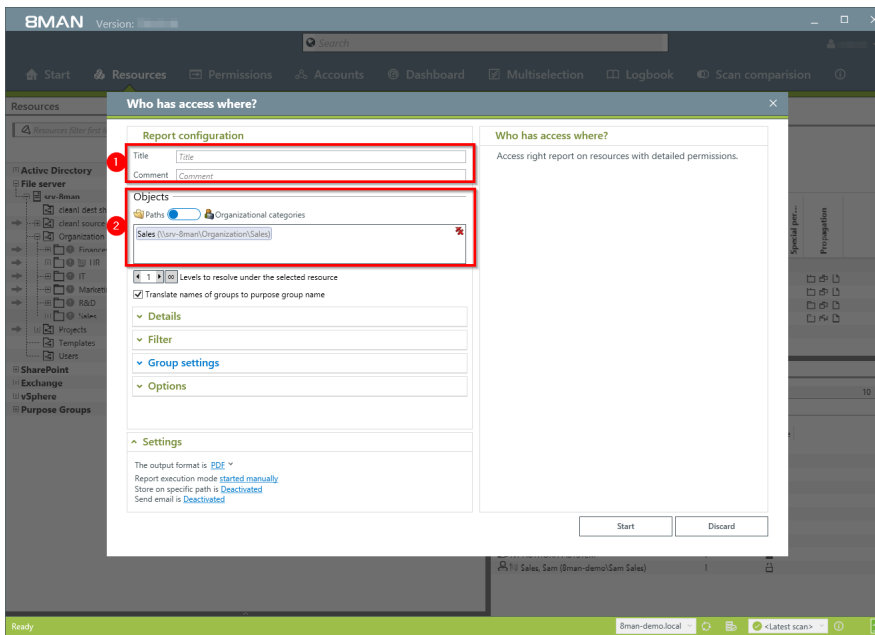
#### Additional Services

##### Changing directory access rights

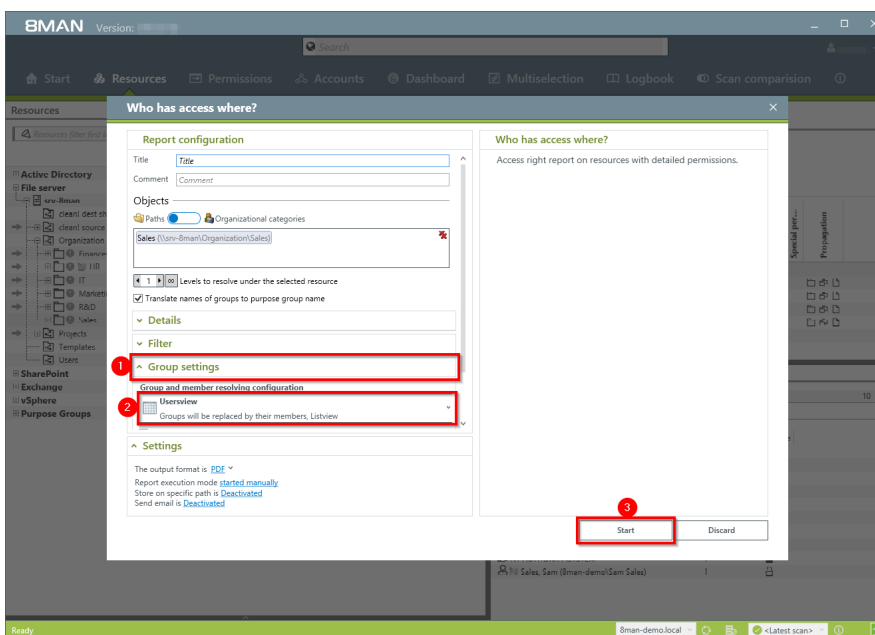
#### Step by step process



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.



1. Open "Group Settings".
2. In order to reduce complexity we recommend selecting the user view. All other settings are targeted at expert users.
3. Start the report.

Protected Networks			
8MAN Report: Who has access where?			
Page 1			
Title	8MAN Report: Who has access where?		
Comment	-		
Used time zone	W. Europe Standard Time (UTC+01:00:00)		
Scantime	8man-demo.local srv-8man	Active Directory File server	2/16/2017 10:00:02 PM 2/16/2017 10:00:03 PM
Configuration	Selected resources: + Sales (\\srv-8man\\Organization\\Sales) Number of levels to resolve under the selected resource: 1 Show only resource objects with changed access rights. Resolve group members till level 1.		
Scan problems	No scan errors detected.		

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 & write". This ensures a higher level of data integrity.

Report for Sales (\\srv-8man\\Organization\\Sales)

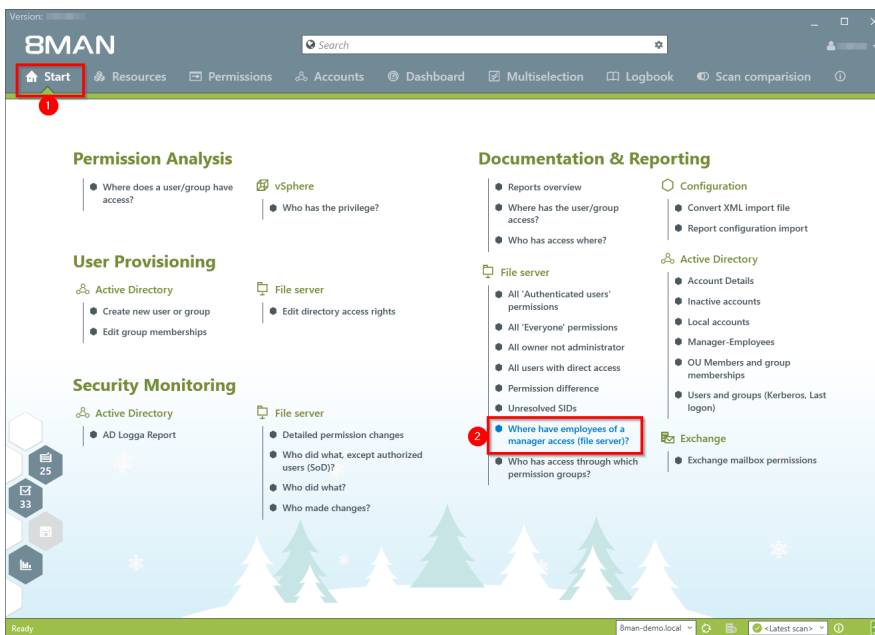
Sales									
\\srv-8man\\Organization\\Sales									
				Full control (Only subfolders and files)	Full control (Only this folder)	Full control (This folder, subfolders and files)	Modify (This folder, subfolders and files)	Read & execute (This folder, subfolders and files)	Read (This folder, subfolders and files)
Anny Time (8man-demo\\ATime)									
Anthony Davis (8man-demo\\ADavis)									
BUILTIN\\Administrators									
BUILTIN\\Users									
CREATOR OWNER									
John Bennett (8man-demo\\JBennett)									
Jones, Gareth (8man-demo\\Gareth Jones)									
I_!_E\$_md (8man-demo\\!_E\$_md)									
Michael Baars (8man-demo\\MBaars)									
NT AUTHORITY\\SYSTEM									

### 5.3.1.3 Where do employees of a manager have access to?

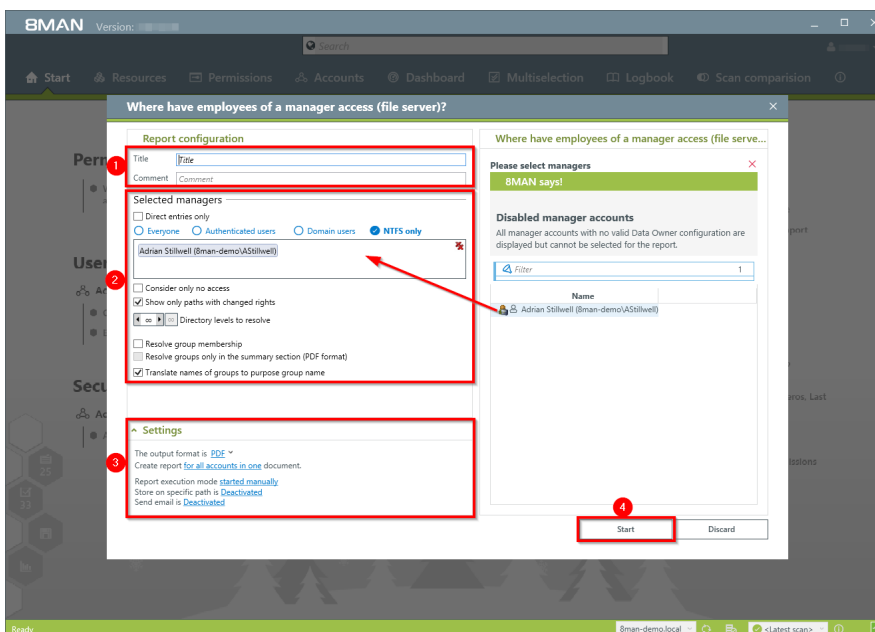
#### Background / Value

8MAN includes a special data owner report for file servers. This allows you to connect Active Directory users with the attribute "Manager" to specific resources on file servers.

#### 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.

## 5.3.2 Reports for Administrators

### 5.3.2.1 Identify 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. 8MAN displays all access rights for the "Everyone" account. These go against the principle of least privilege and should therefore not be used. Removing the "Everyone" account automatically is not possible. Before manually deleting accounts you should assign groups to the appropriate resources. Afterwards you can add the desired members to the group.

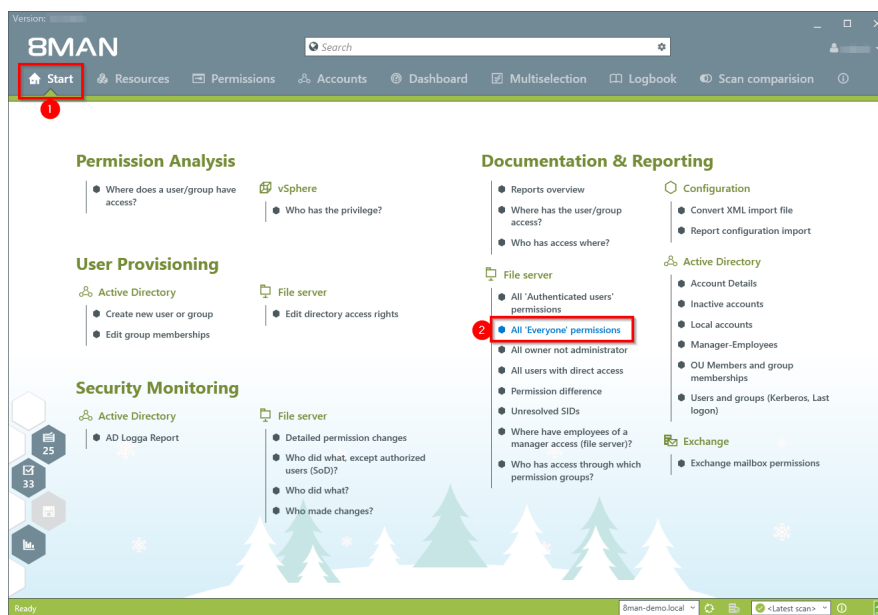
#### Additional services

Also keep an eye on the critical [Authenticated Users](#).

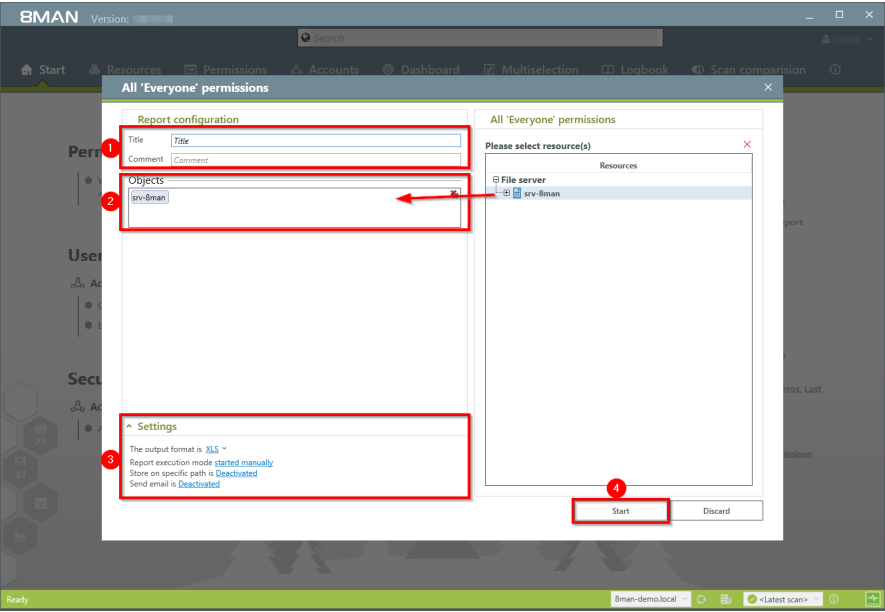
[Identify globally accessible directories](#) (web client)

[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. 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.

Report for	Organization	Path	Right	Deny		
Organization (\srv-8man\Organization)						
Path	Right	Deny				
\srv-8man\Organization\R&D	Read & execute					
\srv-8man\Organization\R&D\Berlin Office	Read & execute					
\srv-8man\Organization\R&D\Coding	Read & execute					
\srv-8man\Organization\R&D\Coding\Source Code	Read & execute					

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



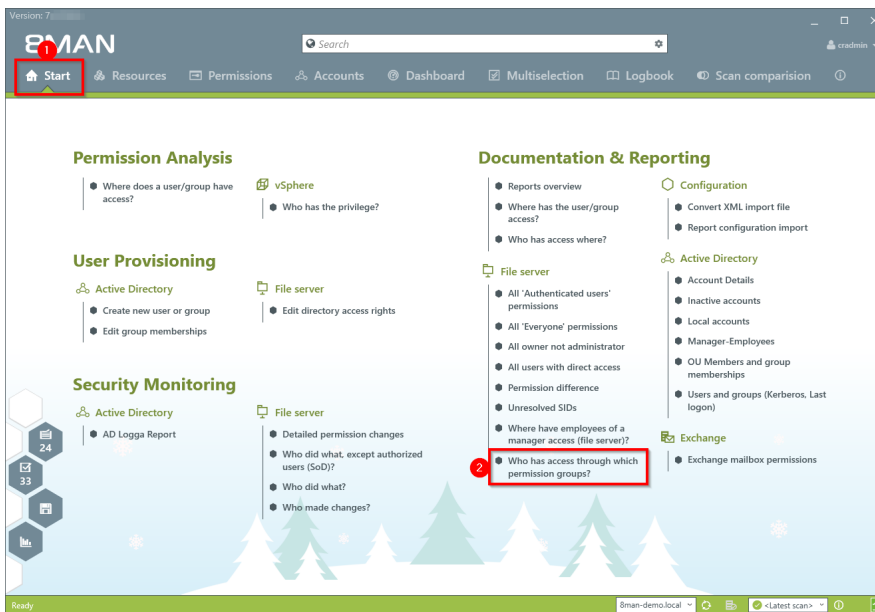
### 5.3.2.2 Who has access through which permission groups?

#### Background / Value

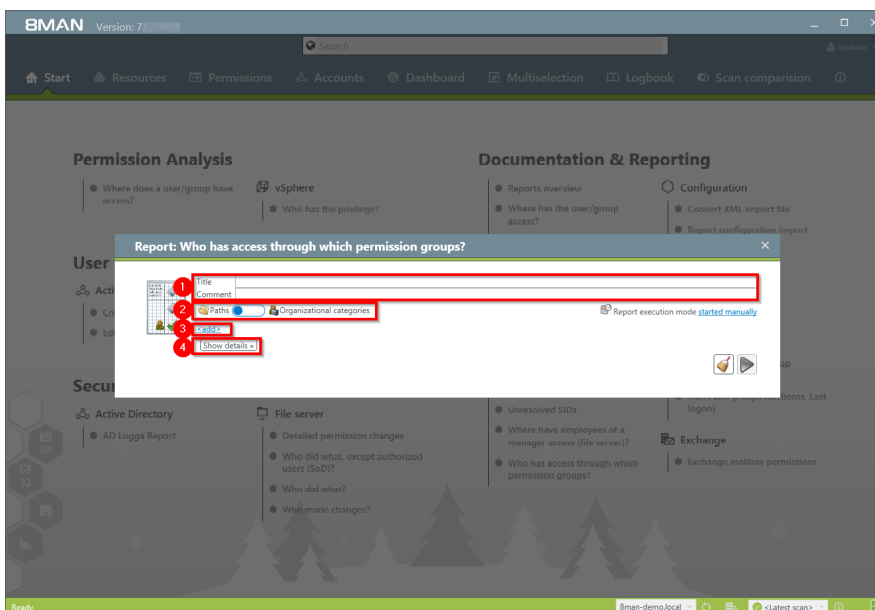
The report "Who has access through which permission groups?" shows the groups that give access to the selected resource and the users that are members of said groups.

Instead of analyzing individual directories you could also view this information in the Organizational Categories section of the Data Owner configuration.

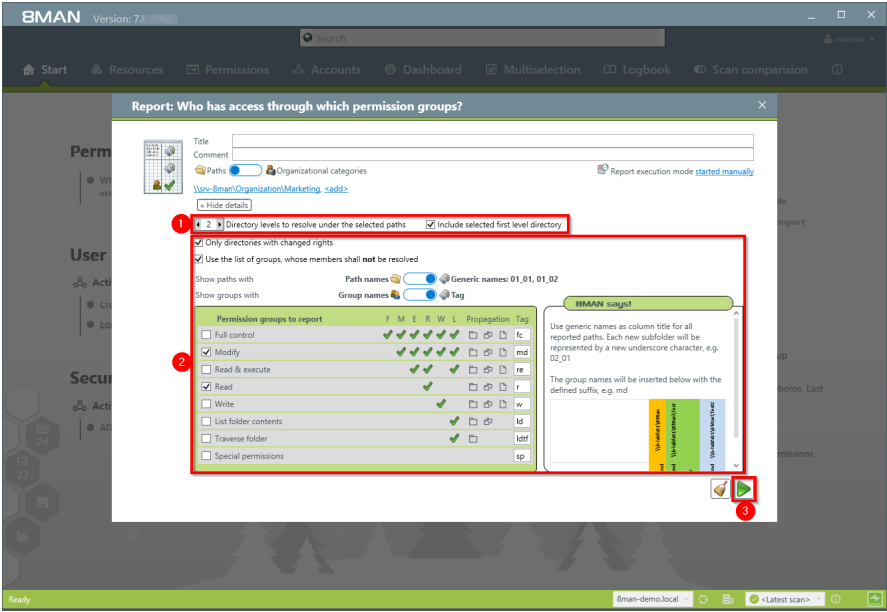
#### Step by step process



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.
1. Add more filters and properties to specify the report further.
2. Start the report.

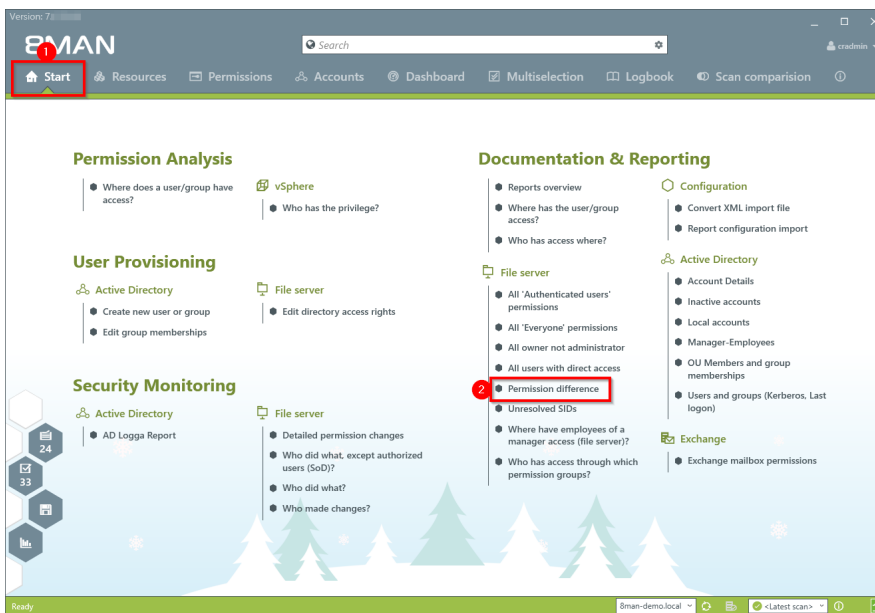
The report contains a list of all user accounts and file server paths, as well as the corresponding access rights groups.

### 5.3.2.3 Permission differences

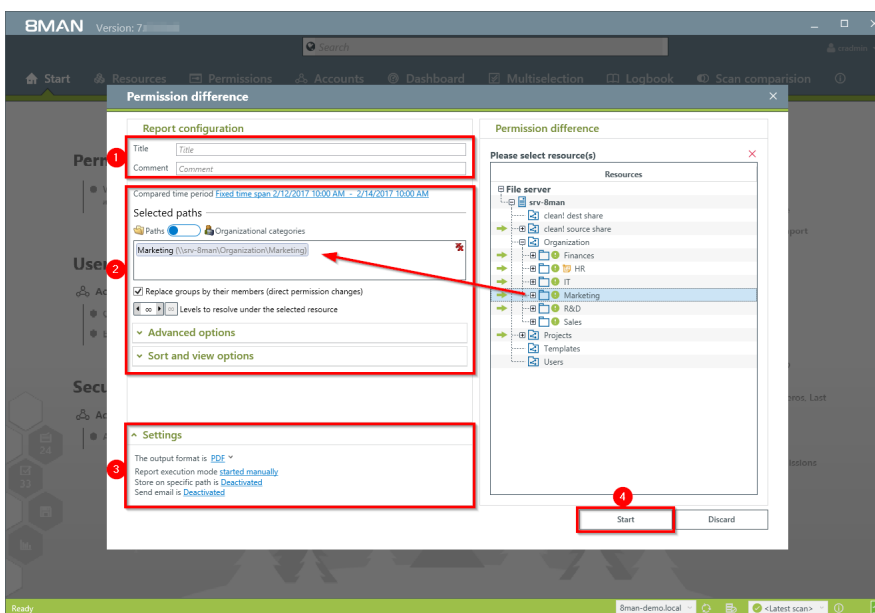
#### Background / Value

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.

#### 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.
1. Define the desired report settings.
2. Start the report.

### 5.3.2.4 Identify 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.

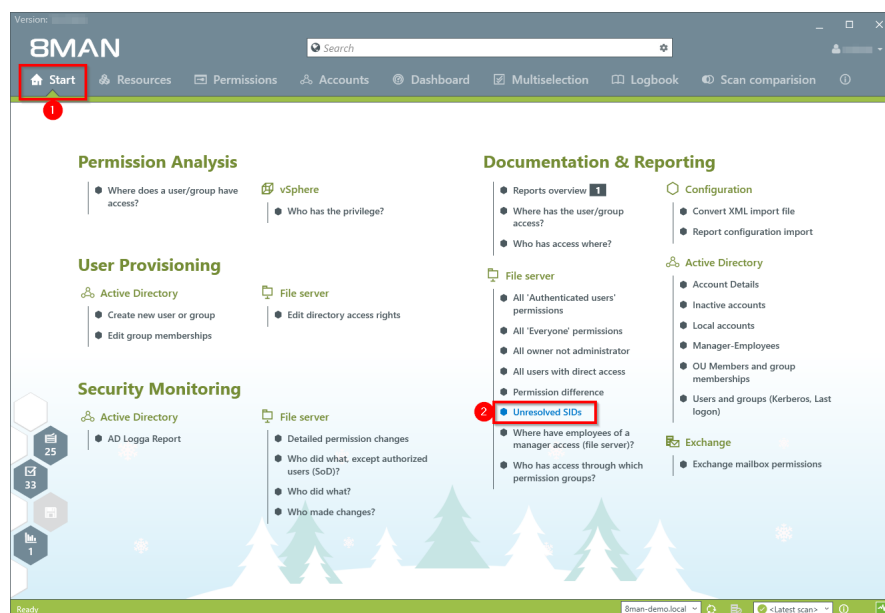
8MAN clearly identifies unresolved SIDs in your system.

#### Additional Services

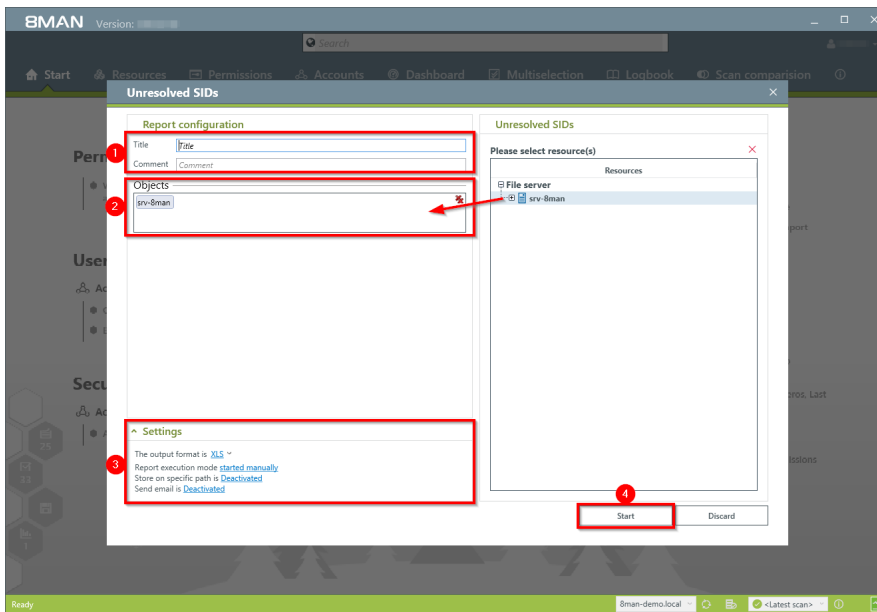
[Identify and delete unresolved SIDs](#) (rich client)

[Remove unresolved SIDs in bulk](#) (web client)

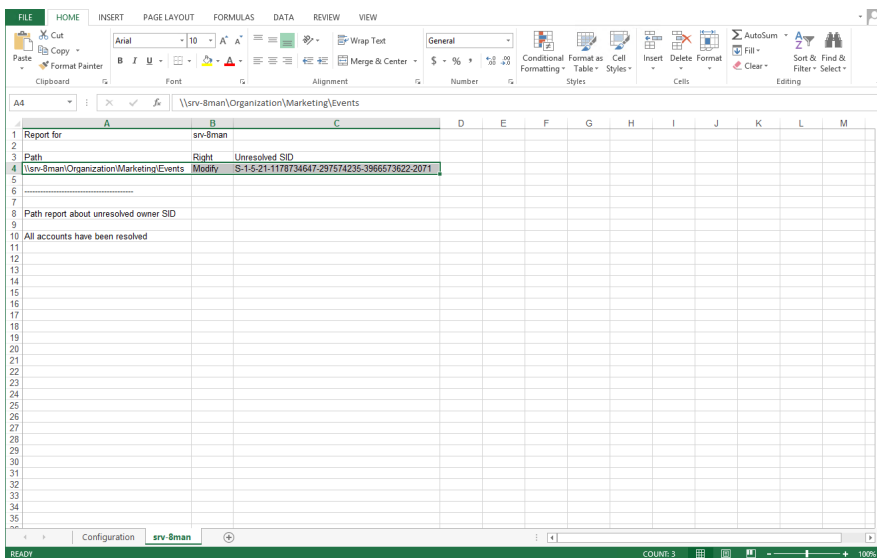
#### Step by step process



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 report settings.
4. Start the report.



Open the report in Excel. In this example an unresolved SID is identified for the directory "IT".

### 5.3.2.5 Identify 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. 8MAN shows you all direct permissions on your file server(s) in one simple report.

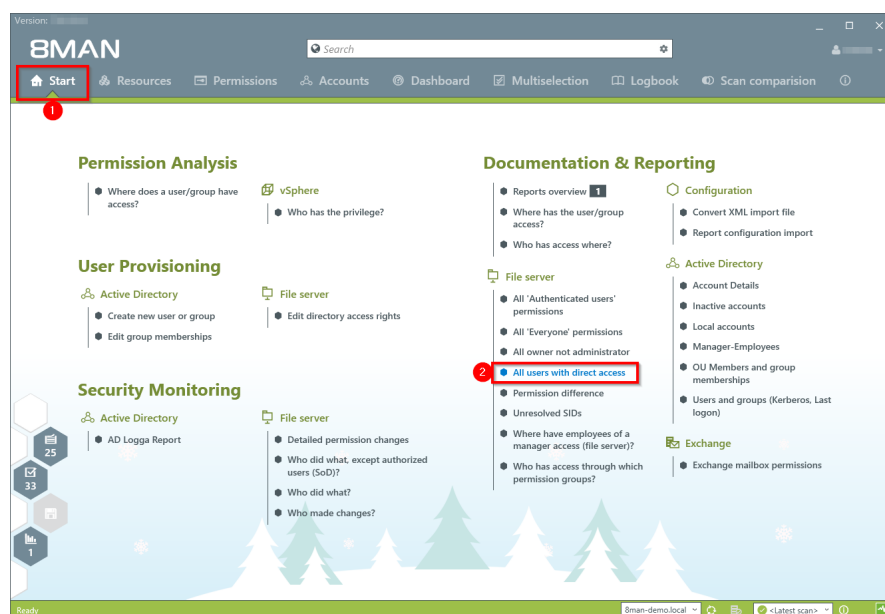
**8MAN strictly adheres to Microsoft Best Practice and assigns a group for every access right.**

#### Additional Services

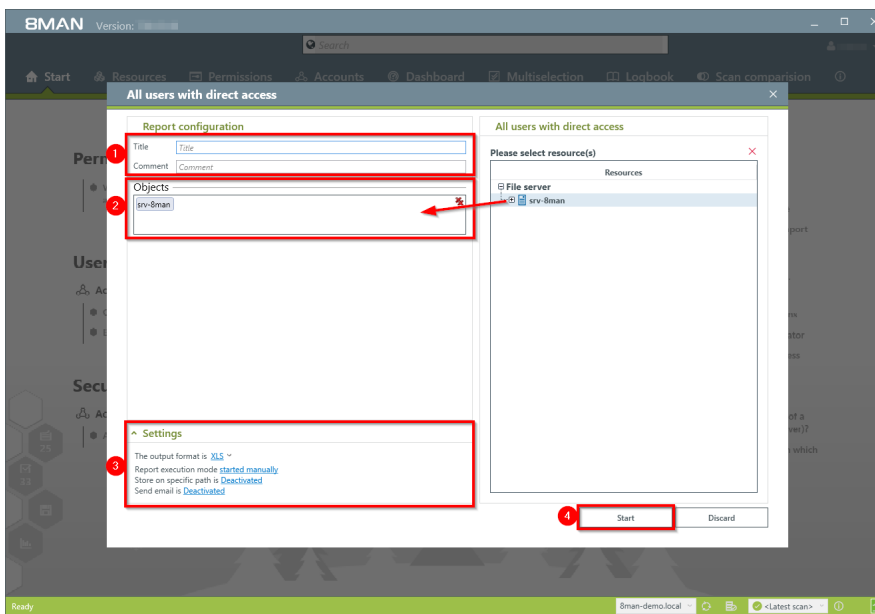
[Remove direct permissions](#) (rich client)

[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 including the dates and times of comparison.
3. Define the desired report settings.
4. Start the report.

Report for	Organization (\\svr-8man\\Organization)	C	D	E	F	G	H	I	J	K
Path	user name	Right	Deny							
\\svr-8man\\Organization	cradmin (8man-demo\\cradmin)	Full control								
\\svr-8man\\Organization\\Finances	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Accounts Payable	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Accounts Payable\\Accounts Open	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Accounts Payable\\Accounts Open	cradmin (8man-demo\\cradmin)	Full control								
\\svr-8man\\Organization\\Finances\\Accounts Payable\\Accounts Paid	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Accounts Payable\\Accounts Paid\\New folder	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Accounts Payable\\Accounts Paid\\New folder	cradmin (8man-demo\\cradmin)	Full control								
\\svr-8man\\Organization\\Finances\\Accounts receivable	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Expenses	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Expenses\\Expenses Project	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Home	Ali Mente (8man-demo\\Ali Mente)	Read & execute								
\\svr-8man\\Organization\\Finances\\New Project directory	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Offices	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Offices\\Berlin HQ	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Offices\\London	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Salaries	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Salaries\\Berlin	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Finances\\Salaries\\Munich	Chris Cook (8man-demo\\CCook)	Modify								
\\svr-8man\\Organization\\Marketing\\Events\\The Art of Security\\2011	cradmin (8man-demo\\cradmin)	Full control								
\\svr-8man\\Organization\\Marketing\\Events\\The Art of Security\\2012	cradmin (8man-demo\\cradmin)	Full control								
\\svr-8man\\Organization\\Marketing\\Events\\The Art of Security\\2013	cradmin (8man-demo\\cradmin)	Full control								

Open the report in Excel. 8MAN lists all directories with direct access rights.

### 5.3.2.6 Identify directories whose owners are not administrators

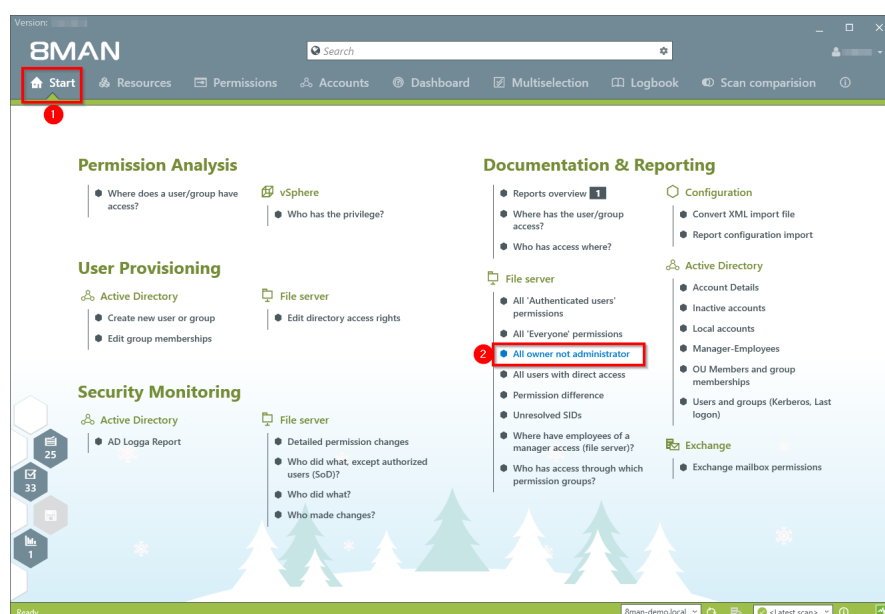
#### Background / Value

8MAN shows you all directories where the owner is not a local administrator group. By excluding these owners you can avoid undesired access right changes.

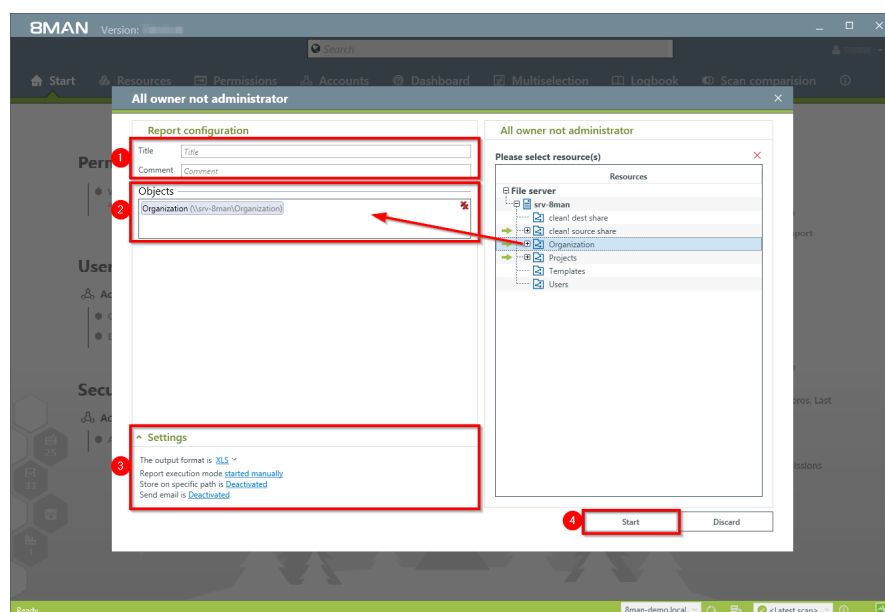
#### Additional Services

[Change directory ownership](#)

#### Step by step process

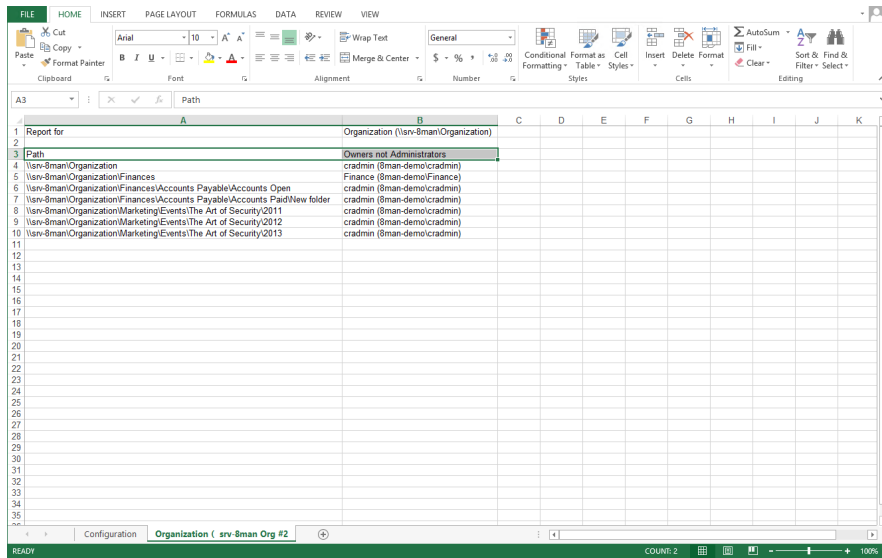


1. Select "Start".
2. Click on "All owner not administrator".



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.





Path	Owners not Administrators
Varv-8man/Organization	cradmin (8man-demo/cradmin)
Varv-8man/Organization/Finance	Finance (8man-demo/Finance)
Varv-8man/Organization/Finance/Accounts Payable/Accounts Open	cradmin (8man-demo/cradmin)
Varv-8man/Organization/Finance/Accounts Payable/Accounts Paid/New folder	cradmin (8man-demo/cradmin)
Varv-8man/Organization/Marketing/Events/The Art of Security/2011	cradmin (8man-demo/cradmin)
Varv-8man/Organization/Marketing/Events/The Art of Security/2012	cradmin (8man-demo/cradmin)
Varv-8man/Organization/Marketing/Events/The Art of Security/2013	cradmin (8man-demo/cradmin)

*Open the report in Excel. 8MAN lists all directories whose owners not administrators.*

### 5.3.2.7 Identify usage of "Authenticated Users"

#### Background / Value

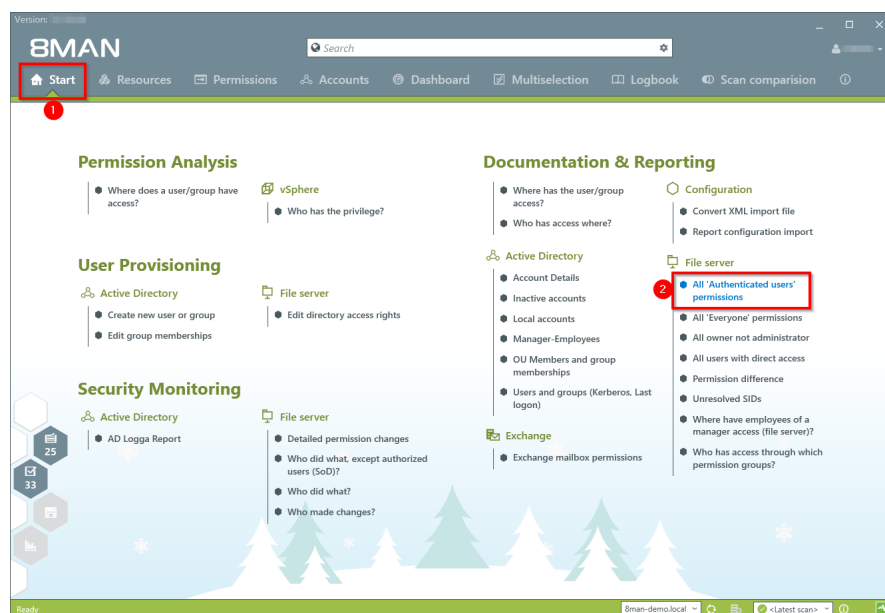
The report shows all directories where the account "Authenticated Users" has access. Just like the "Everyone" account, this technical user account should never be used to grant access to sensitive resources. Scan the report for sensitive directories and remove the access rights for "Authenticated Users".

#### Additional Services

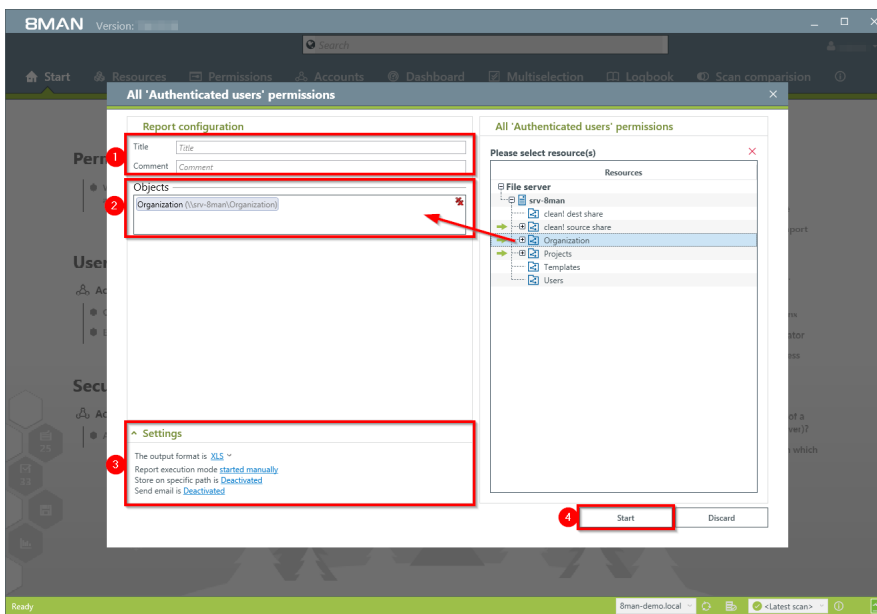
[Identify usage of "everyone"](#)

[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.

### 5.4 +8MATE for Exchange

In the areas of Documentation & Reporting the AddOn 8MATE for Exchange provides the following functionality.

Report: [Who has access to what?](#)

Report: [Identifying Mailbox access rights](#)

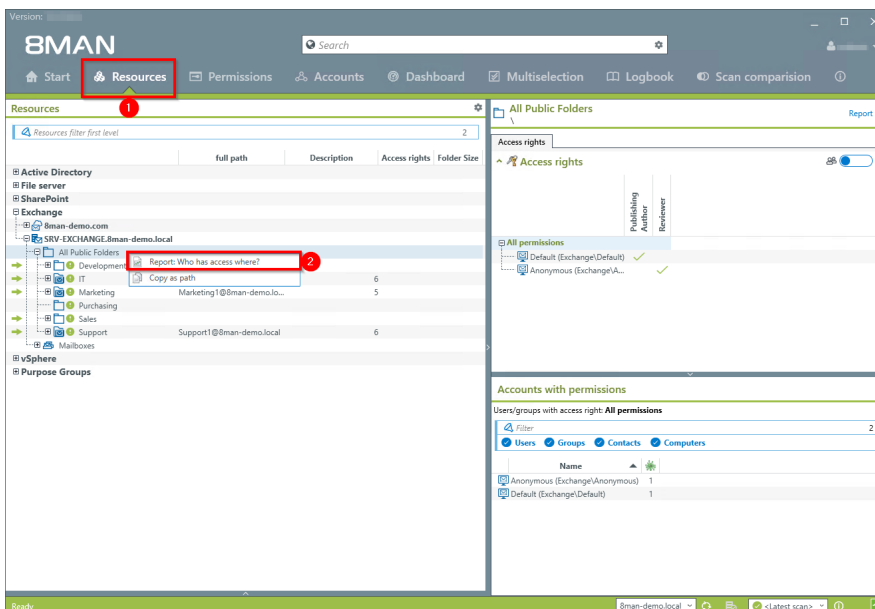
## 5.4.1 Management Reports

### 5.4.1.1 Who has access to what?

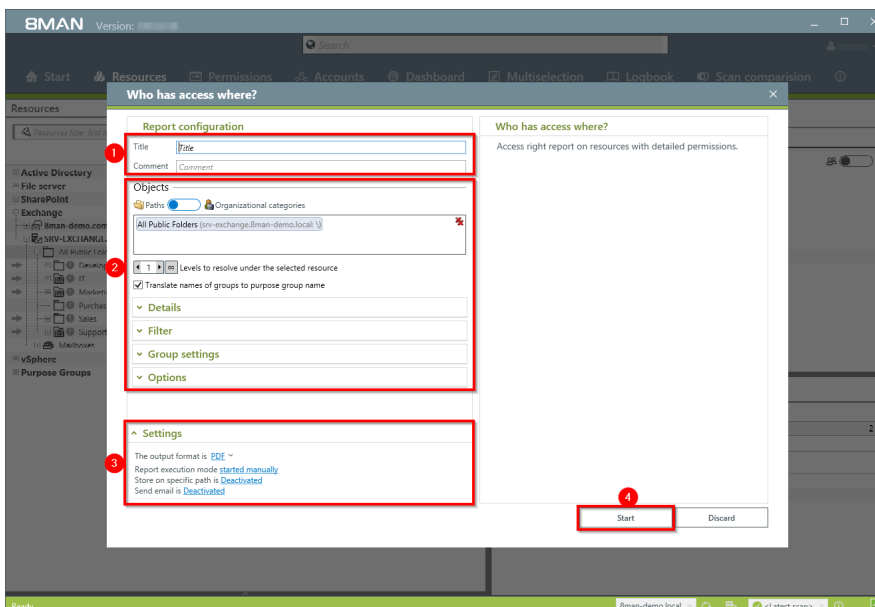
#### Background / Value

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 to what?" provides an overview of all users and their access to public folders. In addition 8MAN highlight the access right "send as", due to its potential risk.

#### 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 report settings.
4. Start the report.



### 5.4.1.2 Identify mailbox permissions

#### Background / Value

8MAN generates a variety of reports that shows Mailbox access rights. These include:

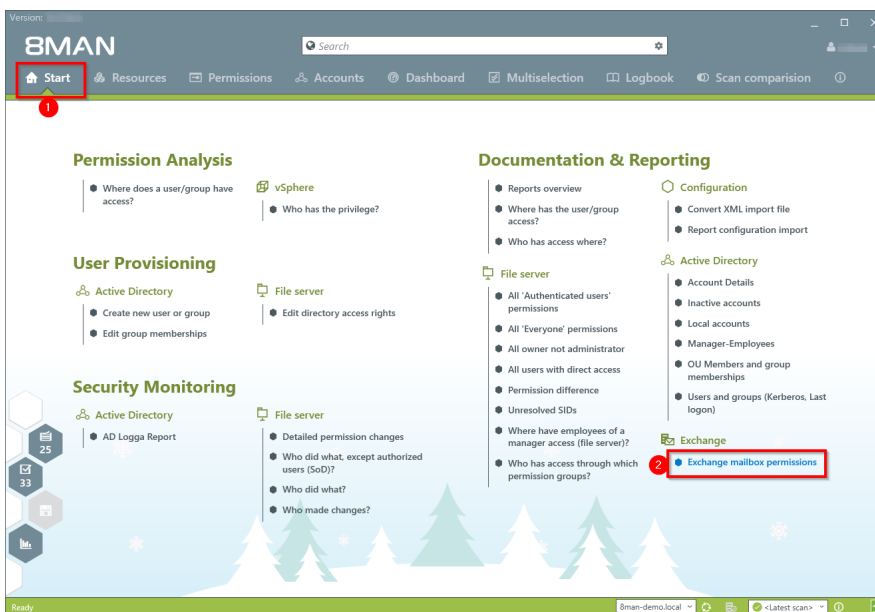
- Mailbox directories and their access rights
- Properties (Mailbox size)
- Deputies for Mailboxes
- Out of Office notices

Mailboxes and their directories require a high degree of security. However, in practice they often contain excessive access rights. It is extremely important to maintain an overview of these rights as folders often contain sensitive Emails.

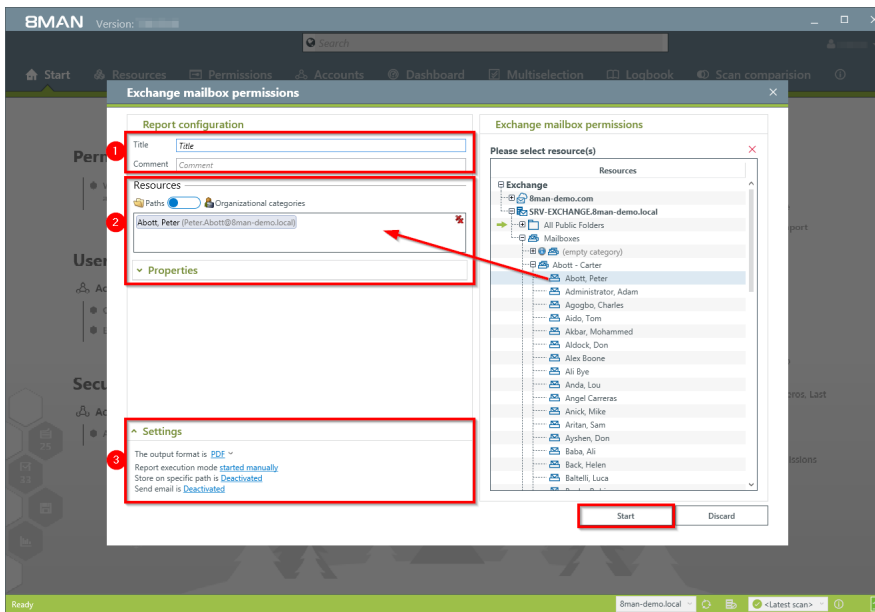
#### Additional Services

"Send As" access rights are shown in the report ["Who has access to what?"](#).

#### Step by step process



1. Select "Start".
2. Click on "Exchange Mailbox 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.



## 5.5 +8MATE for Sharepoint

In the areas of Documentation & Reporting the AddOn 8MATE for Exchange provides the following functionality.

Report: [Who has access to what?](#)

Report: [Where do users and groups have access?](#)

## 5.5.1 Management Reports

### 5.5.1.1 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 SharePoint resources. The report "Who has access to what?" provides an overview of all users and their access to SharePoint.

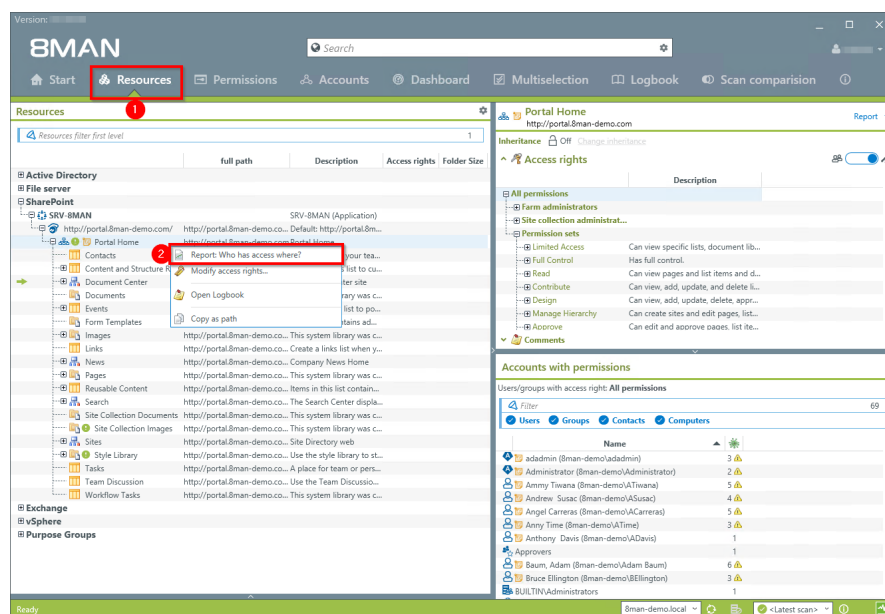
The report allows responsible managers to make information based decisions in order to answer two central questions:

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

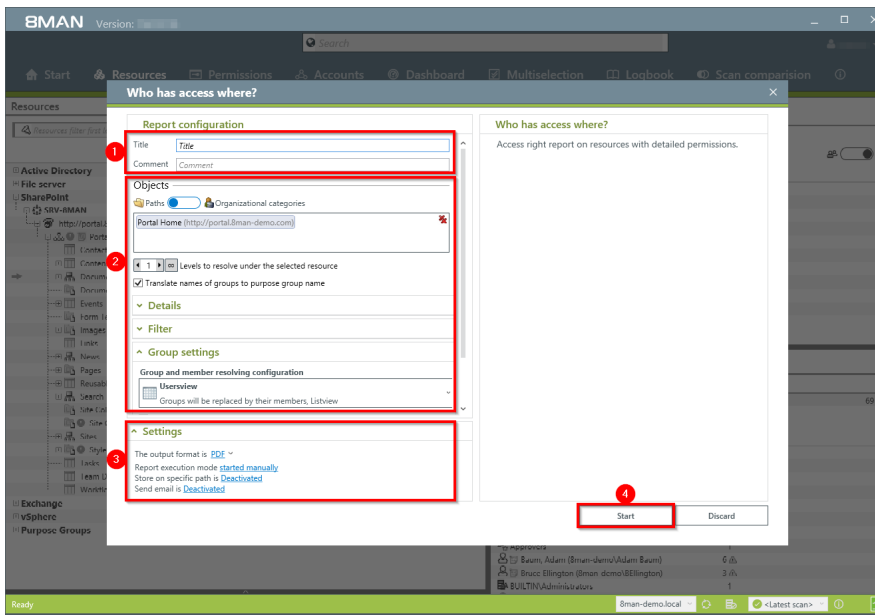
#### Additional Services

[Managing access rights to SharePoint resources](#)

#### Step by step process



1. Select "Resources".
2. Right-click on a SharePoint resource. Select the report "Who has access to what?" from the context menu.



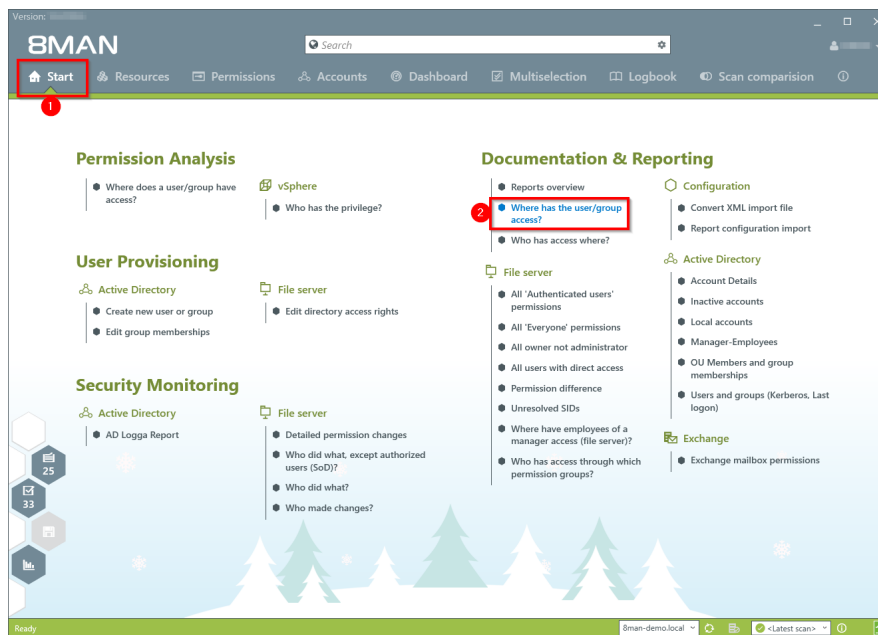
1. Enter a title for the report and add a comment.
2. Define the range of the report. In order to reduce complexity, we recommend selecting "usersview" in the "Group settings" area. All other settings are targeted at expert users.
3. Define the desired report settings.
4. Start the report.

### 5.5.1.2 Where do users and groups have access?

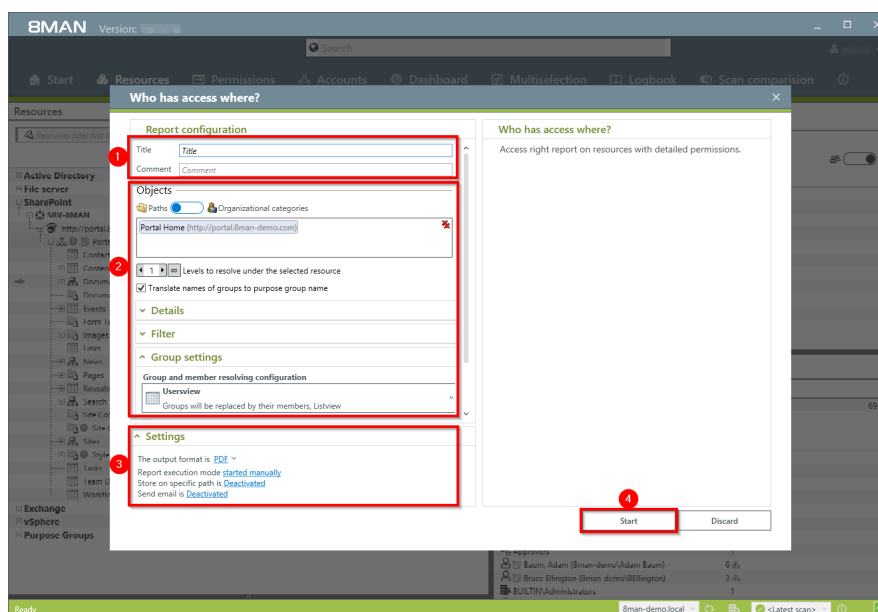
#### Background / Value

The report "Where has the user/group access?" lists the access rights of user and group accounts to selected file server directories in one simple document.

#### Step by step process



1. Select "Start".
2. Click on "Where do Users/Groups have access?".



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 report settings.
4. Start the report.



## 6. Security Monitoring



## 6.1 Active Directory

### 6.1.1 +8MATE AD 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.

##### *Confusing processes*

Confusing processes can only be improved if the current process can be analyzed and understood. Who manages group memberships and resets passwords? Where do problems occur and where is more coordination required. Analyzing past mistakes can be very beneficial in designing a solid process for group assignments.

#### The solution

8MAN 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 8MAN. 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 traceable and transparent.

#### This is achieved with the AD Logga

- Giving Administrators a complete picture of all AD activity, allowing them to optimize processes.
- 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.

### 6.1.1.1 Report: monitor changes in Active Directory

#### Background / Value

The 8MATE AD Logga allows you to monitor current processes in your Active Directory. 8MAN 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 extremely 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. Please note that these settings are geared towards expert users. If you apply a filter for a rare object this may cause the report to deliver unexpected results.**

#### Additional services

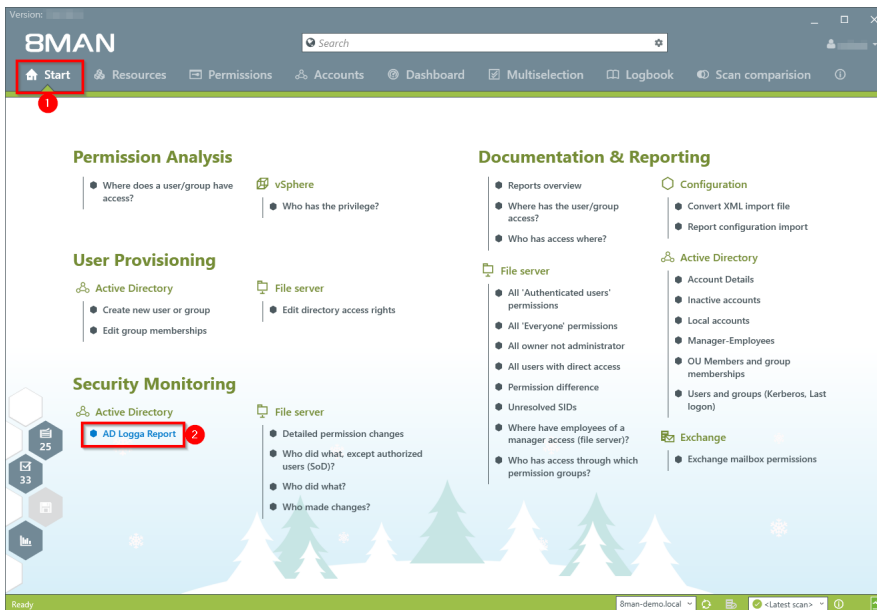
[Analyze AD Logga events with the logbook](#)

[Set alerts for groups](#)

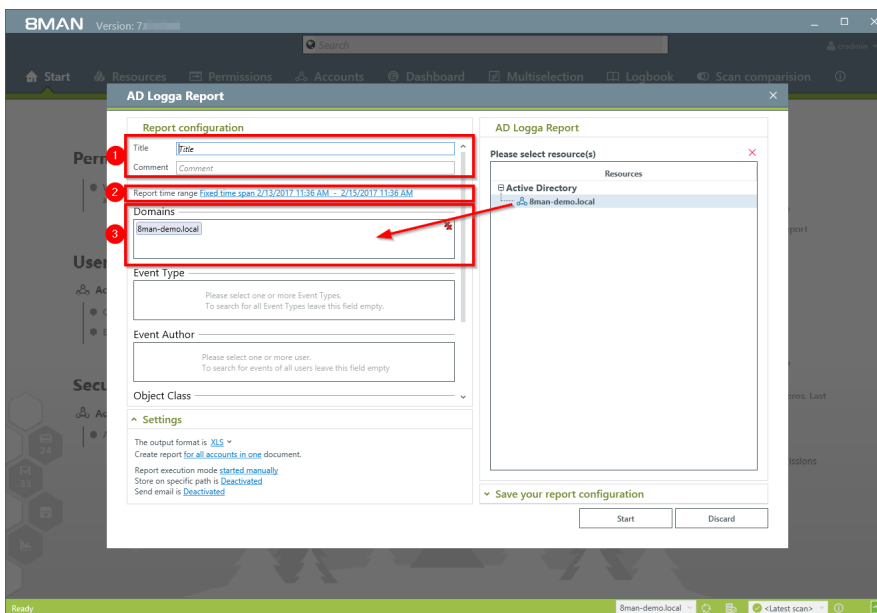
[Set alerts for user accounts](#)



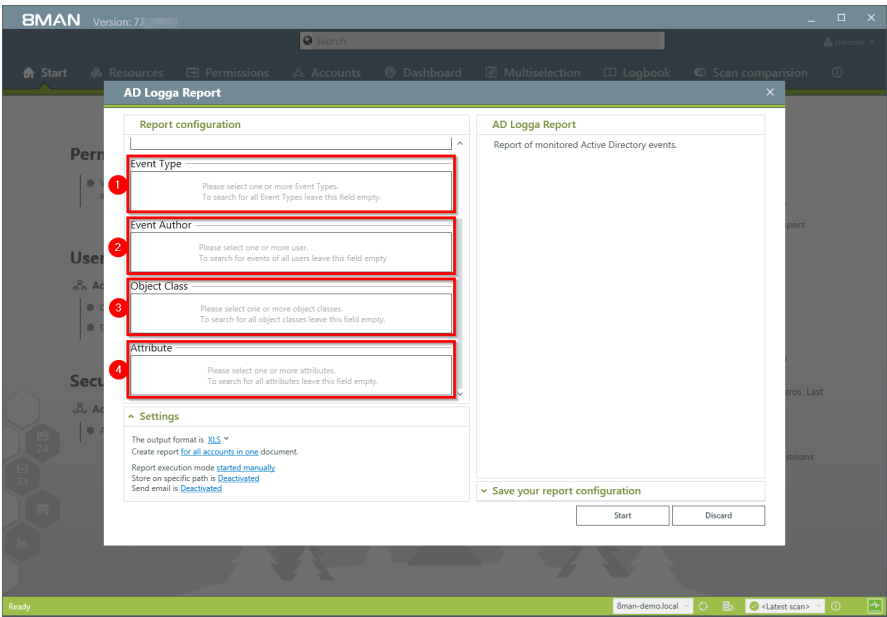
## Step by step process



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

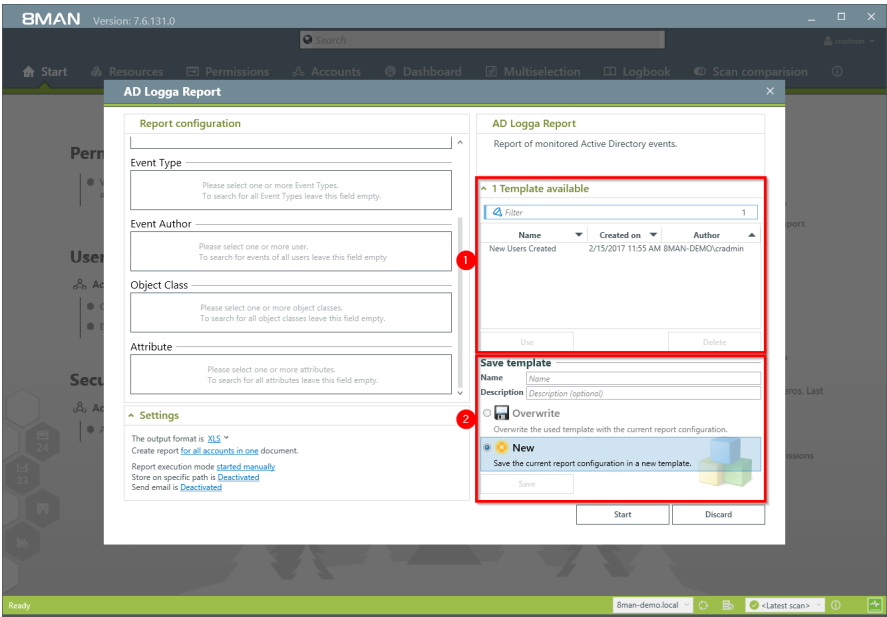


1. Enter a title for the report and add a comment.
2. Define the date range of the report.
3. Select domains whose events should be captured in the report.



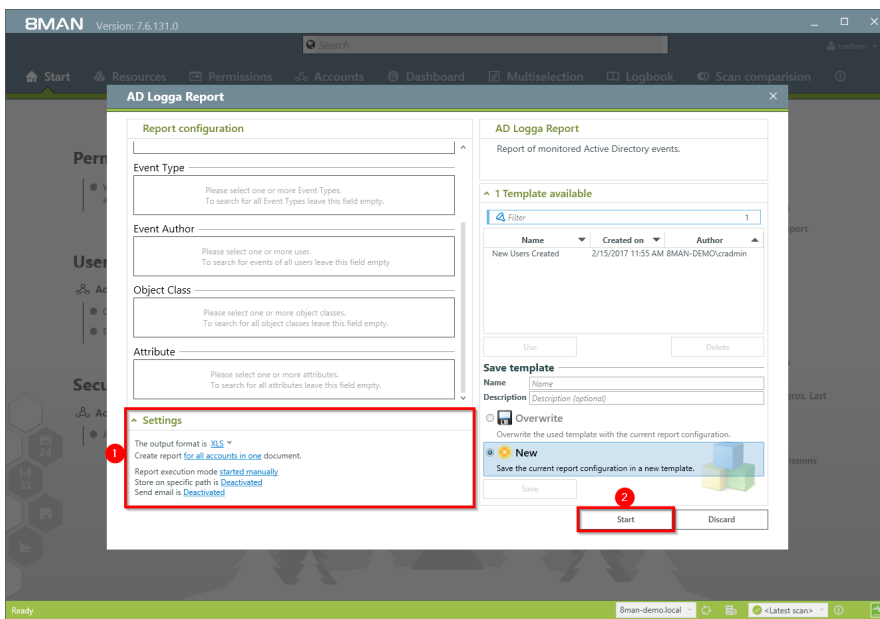
Define the range of the report by setting filters. By definition filters exclude the selected data.

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 report settings.
2. Start the report.

### 6.1.1.2 Identify temporary group memberships

#### Background / Value

8MATE 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.

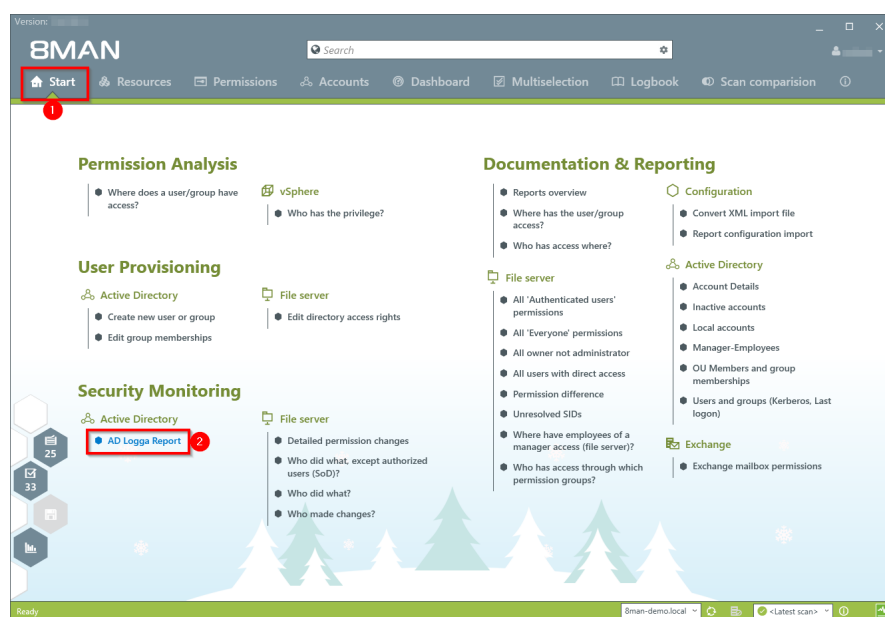
#### Additional Services

[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".

**Report configuration**

Title

Comment

Report time range **Fixed time span** 2/13/2017 12:04 PM - 2/15/2017 12:04 PM

Domains

Event Type

Event Author

Object Class

**Settings**

The output format is **XLS**

Create report for **all accounts in one** document.

Report execution mode **started manually**

Store on specific path is **Deactivated**

Send email is **Deactivated**

**AD Logga Report**

Event Type  18

Account activated  
Account deactivated  
Account locked  
Account unlocked  
Added attribute  
Changed attribute  
Computer created  
Computer deleted  
Group created  
Group deleted  
Member added  
Member removed  
Other objects created  
Other objects deleted  
Removed attribute  
Reset password  
User created  
User deleted

1 Template available

**Start** Discard

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 report settings.
4. Start the report.

### 6.1.1.3 Identify locked user accounts

#### Background / Value

In the best case scenario, an attempted login with someone else's account ends with a locked user account. The AD Logga shows you from which computer the attack occurred.

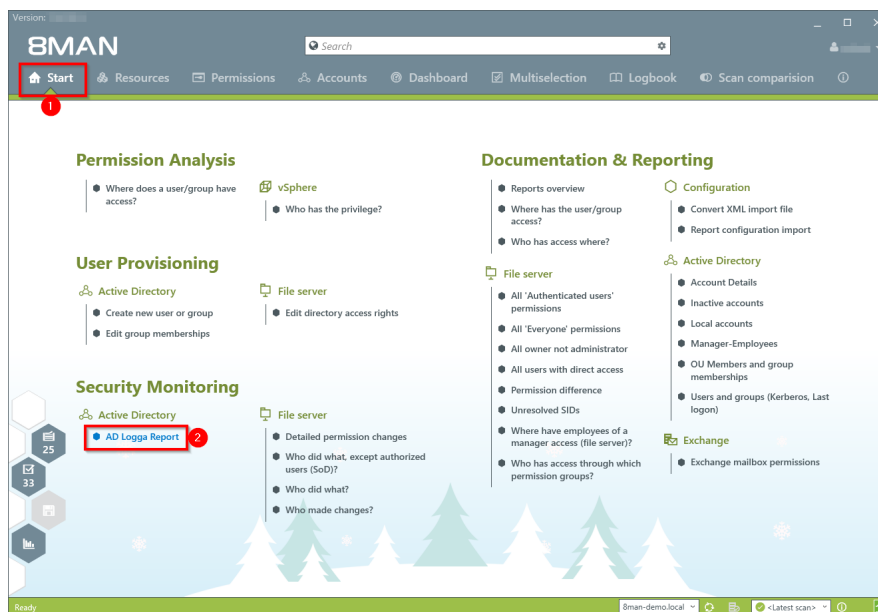
#### Additional services

[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".

**Report configuration**

Title

Comment

Report time range Fixed time span 2/18/2017 1:36 PM - 2/20/2017 1:36 PM

Domains

Event Type

Event Author

Object Class

**Settings**

The output format is [XLS](#)

Create report for all accounts in one document.

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

**AD Logga Report**

Event Type  18

- Account activated
- Account deactivated
- Account locked
- Account unlocked
- Added attribute
- Changed attribute
- Computer created
- Computer deleted
- Group created
- Group deleted
- Member added
- Member removed
- Other objects created
- Other objects deleted
- Removed attribute
- Reset password
- User created
- User deleted

1 Template available

1. Enter a title for the report and add a comment.

1. Define the range of the report.  
For the event type select "Account locked"

2. Define the desired report settings.

3. Start the report.

### 6.1.1.4 Monitor password resets

#### Background / Value

With the 8MATE 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.

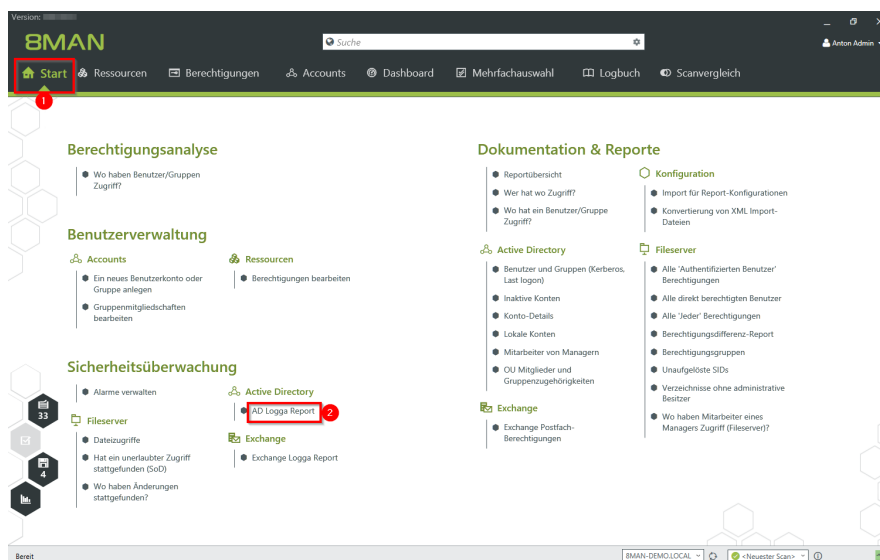
#### Additional Services

[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".



**Report-Konfiguration**

1 Titel

2 Kommentar

Reportzeitraum **Fester Zeitraum** 01.02.2014 13:30 – 10.11.2016 13:30

Domänen

Ereignistyp

Ereignis-Autor

Objekt Klasse

**Einstellungen**

Das Ausgabeformat ist **XLS**

Reportausführung wird **manuell gestartet**

Speichern ist **deaktiviert**

E-Mail Versenden ist **deaktiviert**

**AD Logga Report**

Ereignistyp

Attribut entfernt

Attribut geändert

Attribut hinzugefügt

Benutzer erstellt

Benutzer gelöscht

Computer erstellt

Computer gelöscht

Gruppe gelöscht

Kennwort zurücksetzen

Konto aktiviert

Konto deaktiviert

Konto entspert

Konto gesperrt

Mitglied entfernt

Mitglied hinzugefügt

Sonstige Objekte erstellt

Sonstige Objekte gelöscht

1 Vorlage verfügbar

4 **Start** Verwerfen

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.

Zeit	Autor	Objekt	Objektklasse	Ereignis	Attribut Name
26.02.2014 16:56	cradmin (Bman-demo/cradmin)	Bino, Al (Bman-demo/Al Bino)	User(user)	Kennwort zurücksetzen	
28.02.2014 15:40:35	cradmin (Bman-demo/cradmin)	Zifer, Lou (Bman-demo/Lou Zifer)	User(user)	Kennwort zurücksetzen	
11.03.2014 09:15:01	Administrator (Bman-demo/Administrator)	Zifer, Lou (Bman-demo/Lou Zifer)	User(user)	Kennwort zurücksetzen	
13.03.2014 14:50:42	Administrator (Bman-demo/Administrator)	Zifer, Lou (Bman-demo/Lou Zifer)	User(user)	Kennwort zurücksetzen	
10.03.2015 11:49:04	readmin (Bman-demo/readmin)	Borg, Inge (Bman-demo/Inge Borg)	User(user)	Kennwort zurücksetzen	
10.03.2015 12:31:32	readmin (Bman-demo/readmin)	Borg, Inge (Bman-demo/Inge Borg)	User(user)	Kennwort zurücksetzen	
10.03.2015 15:12:28	Administrator (Bman-demo/Administrator)	Krise, Christiane (Bman-demo/Christiane Krise)	User(user)	Kennwort zurücksetzen	
10.03.2015 15:47:05	Administrator (Bman-demo/Administrator)	Ander, Ole (Bman-demo/Ole Ander)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09	readmin (Bman-demo/readmin)	Aber, Mark (Bman-demo/Mark Aber)	User(user)	Kennwort zurücksetzen	
11.03.2015 16:50:09	readmin (Bman-demo/readmin)	Alien, Arnold (Bman-demo/Arnold Alien)	User(user)	Kennwort zurücksetzen	
12.03.2015 16:50:09	readmin (Bman-demo/readmin)	Aloe, Vera (Bman-demo/Vera Aloe)	User(user)	Kennwort zurücksetzen	
13.03.2015 16:50:09	readmin (Bman-demo/readmin)	Ander, Ole (Bman-demo/Ole Ander)	User(user)	Kennwort zurücksetzen	
14.03.2015 16:50:09	readmin (Bman-demo/readmin)	Ander, Con (Bman-demo/Con Ander)	User(user)	Kennwort zurücksetzen	
15.03.2015 16:50:09	readmin (Bman-demo/readmin)	Aner, Dominik (Bman-demo/Dominik Aner)	User(user)	Kennwort zurücksetzen	
16.03.2015 16:50:09	readmin (Bman-demo/readmin)	Angebrandt, Angie (Bman-demo/Angie Angebrandt)	User(user)	Kennwort zurücksetzen	
17.03.2015 16:50:09	readmin (Bman-demo/readmin)	Apfel, Adam (Bman-demo/Adam Apfel)	User(user)	Kennwort zurücksetzen	
18.03.2015 16:50:09	readmin (Bman-demo/readmin)	Arbet, Andi (Bman-demo/Andi Arbet)	User(user)	Kennwort zurücksetzen	
19.03.2015 16:50:09	readmin (Bman-demo/readmin)	Arm, Armin (Bman-demo/Armin Arm)	User(user)	Kennwort zurücksetzen	
20.03.2015 16:50:09	readmin (Bman-demo/readmin)	Aroni, Mark (Bman-demo/Mark Aroni)	User(user)	Kennwort zurücksetzen	
21.03.2015 16:50:09	readmin (Bman-demo/readmin)	Astil, Clane (Bman-demo/Clane Astil)	User(user)	Kennwort zurücksetzen	
22.03.2015 16:50:09	readmin (Bman-demo/readmin)	Auer, Karl (Bman-demo/Karl Auer)	User(user)	Kennwort zurücksetzen	
23.03.2015 16:50:09	readmin (Bman-demo/readmin)	Auhss, Ann (Bman-demo/Ann Auhss)	User(user)	Kennwort zurücksetzen	
24.03.2015 16:50:09	readmin (Bman-demo/readmin)	Autsch, Anke (Bman-demo/Anke Autsch)	User(user)	Kennwort zurücksetzen	
25.03.2015 16:50:09	readmin (Bman-demo/readmin)	Azuba, Andy (Bman-demo/Andy Azuba)	User(user)	Kennwort zurücksetzen	
26.03.2015 16:50:09	readmin (Bman-demo/readmin)	Baba, Ali (Bman-demo/Ali Baba)	User(user)	Kennwort zurücksetzen	
27.03.2015 16:50:09	readmin (Bman-demo/readmin)	Bach, Klara (Bman-demo/Klara Bach)	User(user)	Kennwort zurücksetzen	
28.03.2015 16:50:09	readmin (Bman-demo/readmin)	Baer, Johannes (Bman-demo/Johannes Baer)	User(user)	Kennwort zurücksetzen	
29.03.2015 16:50:09	readmin (Bman-demo/readmin)	Baer, Roy (Bman-demo/Roy Baer)	User(user)	Kennwort zurücksetzen	
30.03.2015 16:50:09	readmin (Bman-demo/readmin)	Baern, Al (Bman-demo/Al Baern)	User(user)	Kennwort zurücksetzen	
31.03.2015 16:50:09	readmin (Bman-demo/readmin)	Balken, Don R. (Bman-demo/Don R. Balken)	User(user)	Kennwort zurücksetzen	
32.03.2015 16:50:09	readmin (Bman-demo/readmin)	Becher, Joe Kurt (Bman-demo/Joe Kurt Becher)	User(user)	Kennwort zurücksetzen	
33.03.2015 16:50:09	readmin (Bman-demo/readmin)	Beiter, Walter (Bman-demo/Walter Beiter)	User(user)	Kennwort zurücksetzen	

Open the report in Excel. On the tab "events" you can see a list of all passwords that have been reset.

### 6.1.1.5 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.

#### Additional Services

[Identify temporary group memberships](#)

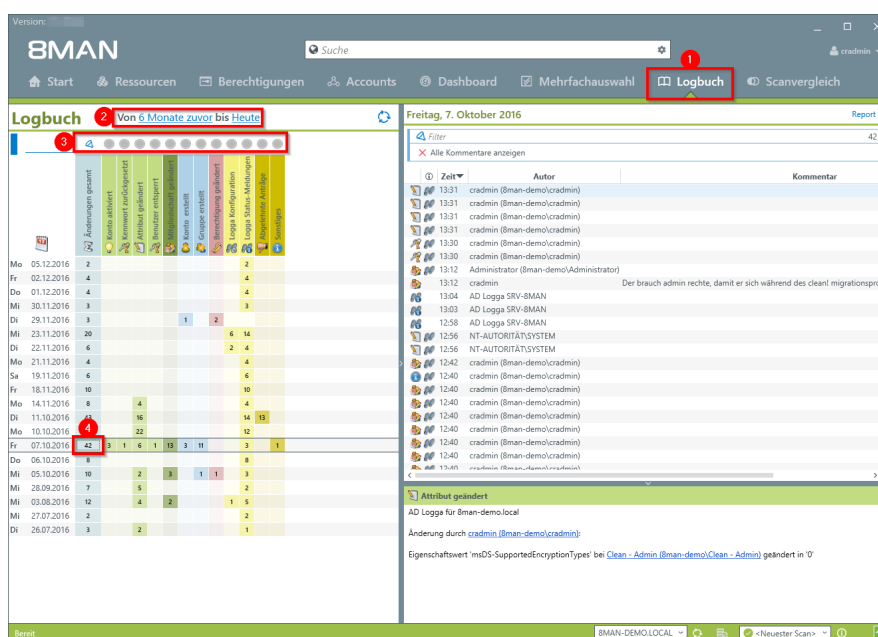
[Identify locked user accounts](#)

[Monitor password resets](#)

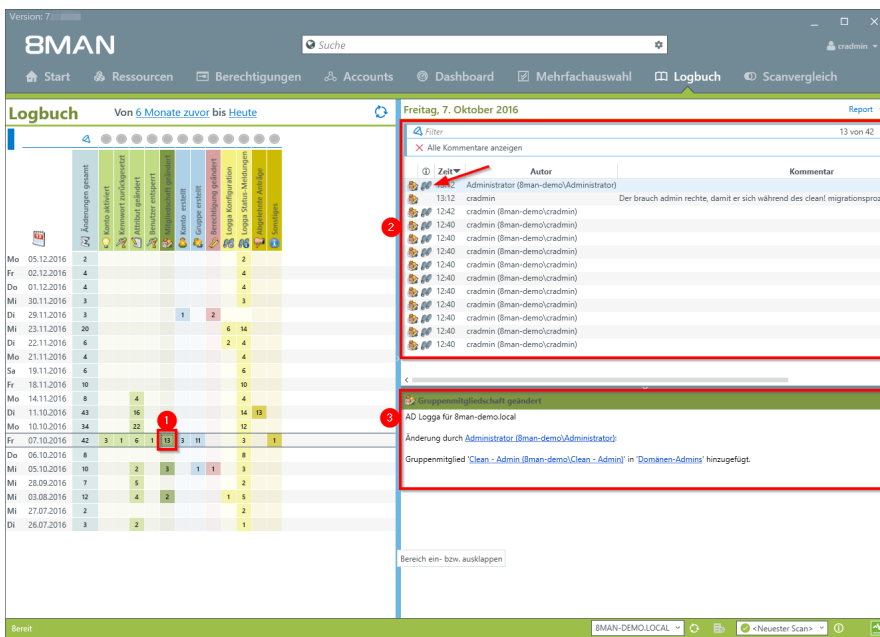
[Set alerts for groups](#)

[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.



1. Select a cell (an event type) to filter the results to your request.
2. 8MAN displays all results. The footsteps indicate the AD Logga results. Select a result.
3. 8MAN displays all details to the result.

### 6.1.1.6 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. 8MATE AD Logga allows you to actively monitor specific AD groups so that an alert is received if new members are added.

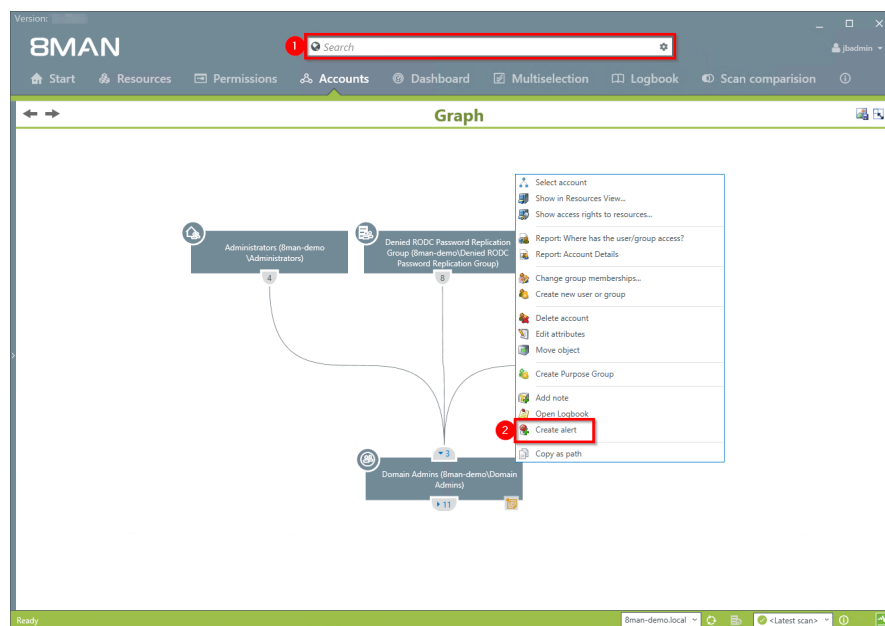
Due to the nested group structures in Active Directory it is important to monitor group memberships, that occur from new indirect memberships. For example: The group "secret data" is a member in the "C-Level" group which is being monitored. 8MATE AD Logga alerts will notify you even if members are only added to the "secret data" group since these users are also indirect members of the "C-Level" group.

#### Additional services

[Set alerts for user accounts](#)

[Manage alerts](#)

#### Step by step process



1. Find the desired group by entering its name into the search field.
2. Right click on the group and select "Create alert" from the context menu.

**BMAN** Version: 1.0.0

Search

Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparison

**Create alert**

Create an alert for 'Domain Admins (8man-demo\Domain Admins)' that will execute the selected actions when occurred.

**Name** The name is used in the actions to identify the event (e.g. mail subject)  
Group memberships changed for Domain Admins (8man-demo\Domain Admins)

**Event** Group memberships changed

☒ Observe indirect group memberships

**Action** Send email

To: jadmin@8man-demo.local  
Enter multiple email addresses by separating them with a semicolon.

Language: English

Time zone: (UTC) Dublin, Edinburgh, Lisbon, London

**Action** Write to Windows event log

New policy to monitor domain admins group.

**Create** **Cancel**

1. Name the alert and add a comment.
2. Activate the checkbox to include indirect group memberships in the alert functionality.
3. You can select any number of email recipients. Additionally alerts can be displayed in the windows event display.
4. You must enter a comment.
5. Create the alert.

### 6.1.1.7 Set alerts for user accounts

#### Background / Value

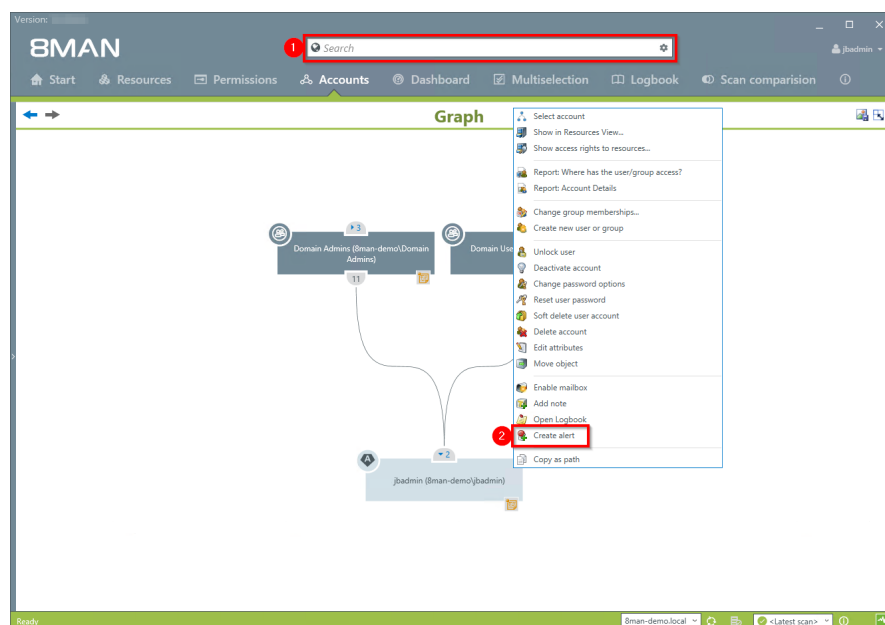
The 8MATE AD Logga allows you to monitor the process of resetting passwords. Within this process there is an inherent security risk. For example, if a helpdesk employee secretly resets the password of a manager or executive, they can sign on with a temporary password and gain access to sensitive information. In this scenario the designated users are informed.

#### Additional services

[Set alerts for groups](#)

[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.

**BMAN** Version: [version]

Search

Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparison

**Graph**

**Create alert**

Create an alert for 'Domain Admins (8man-demo\Domain Admins)' that will execute the selected actions when occurred.

1 **Name** The name is used in the actions to identify the event (e.g. mail subject).  
Account locked for jadmin (8man-demo\jadmin) [max. 70 characters]

2 **Event** Account locked

3 **Action Send email**  
To cadmin@8man-demo.local  
Enter multiple email addresses by separating them with a semicolon.  
Language English  
Time zone (UTC) Dublin, Edinburgh, Lisbon, London

4 **Action Write to Windows event log**  
Demo

**Create** **Cancel**

Ready 8man-demo.local <Latest scan>

1. Enter a title for the alert.
1. Select an event for which you want to receive the alert.
2. You can select any number of email recipients. Additionally alerts can be displayed in the windows event log.
3. You must enter a comment.
4. Create the alert.

6.1.1.8 Run a script after an alert

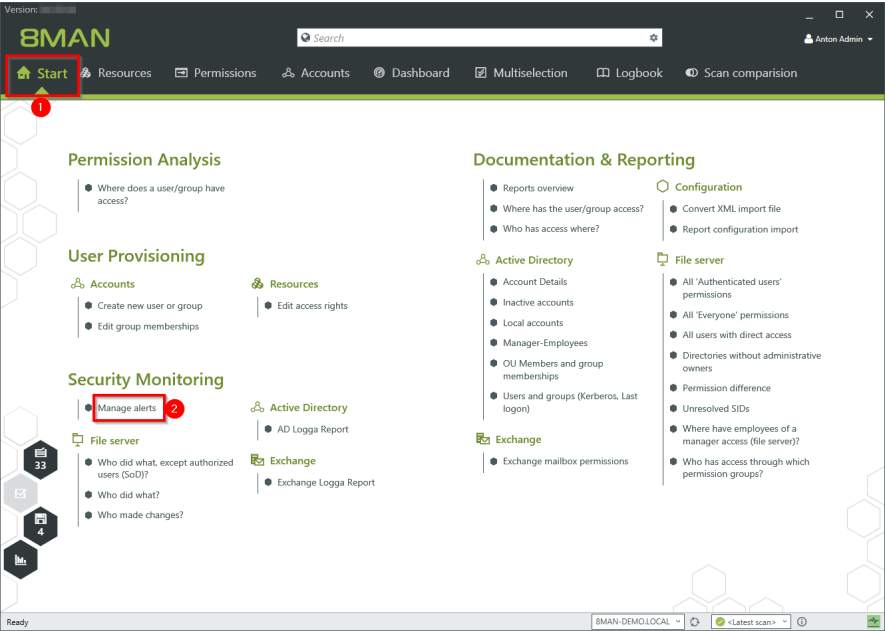
Background / Value

Run a script after the FS Logga or AD Logga has triggered an alert. For example, you monitor a security-critical group for membership changes and the script automatically resets memberships back to default.

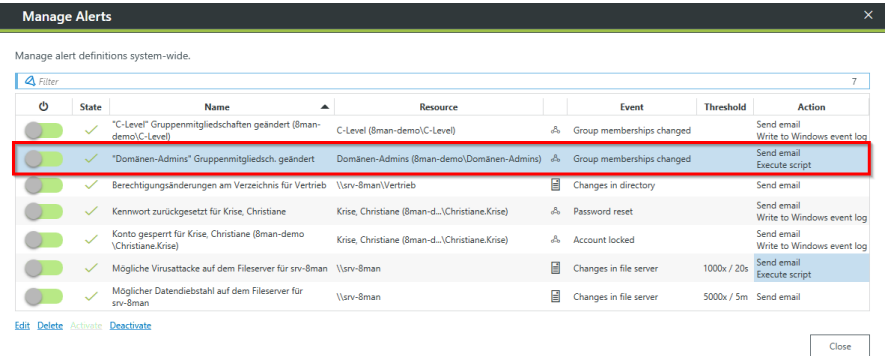
Additional Services

Manage alerts

Step by step process



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



Double-click an entry.



Edit alert

Edit an automatically executed alert for 'Domänen-Admins (8man-demo\Domänen-Admins)'.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
"Domänen-Admins" Gruppen				Warning

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

To: admin@8man-demo.local

Language: English

Time zone: UTC

Write to Windows event log ☐

Execute script ☒

UndoGroupMembershipChange

Please add a comment

Apply Cancel

1. Choose Actions.
2. Enable script execution.
3. Select a script.

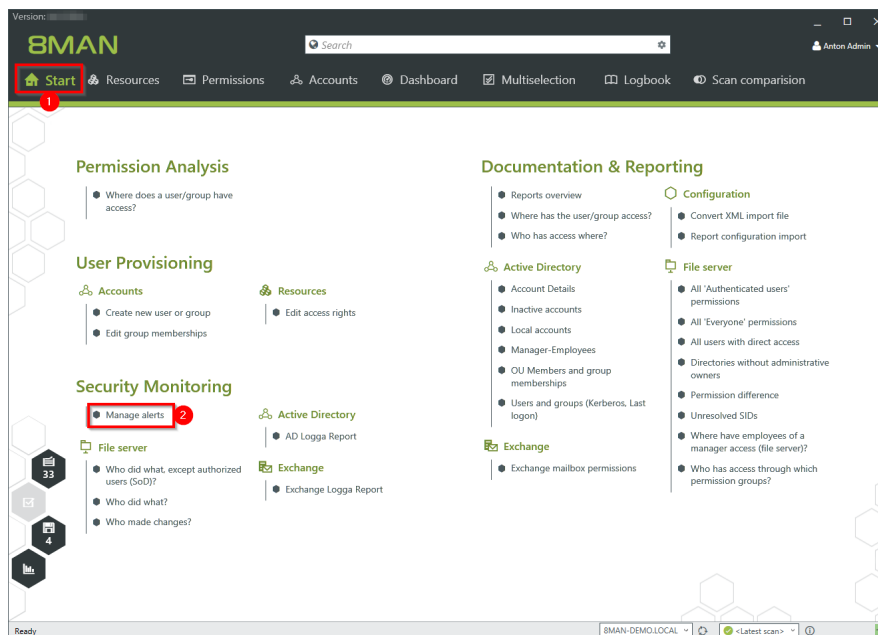
To activate the option, a script configuration for alerts must be stored.

### 6.1.1.9 Manage alerts

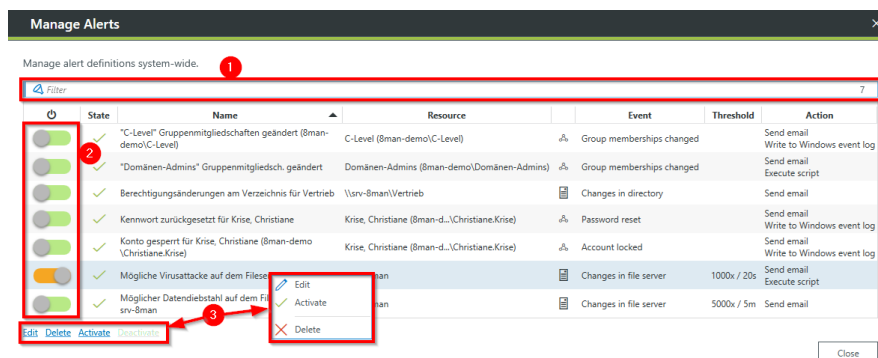
#### Background / Value

You can modify saved alerts at any time on the 8MAN home page.

#### Step by step process



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



8MAN shows you all alert configurations.

1. Search for an alert configuration.
2. Turn alerts on or off.
3. With right-click or the links, edit, delete or enable/disable the selected alert configuration.

## 6.2 Fileserver

### 6.2.1 +8MATE FS 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

8MAN 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 8MAN are captured. Temporary access rights and other changes with security implications become understandable immediately.

By configuring reports you can identify differences in your access rights structure. Access and changes of sensitive data, including deleting copying, moving and modifying are logged with the FS Logga.

#### This is what you can achieve with the FS Logga

- Administrators get a full picture of all actions being performed on a given file server. This allows you to optimize access rights processes.
- Auditors can easily identify security incidents related to sensitive data including the involved actors.
- The executive department can be certain: The FS Logga provides all necessary data for more security and process improvement and makes security related incidents completely transparent.

### 6.2.1.1 Monitor access to sensitive data

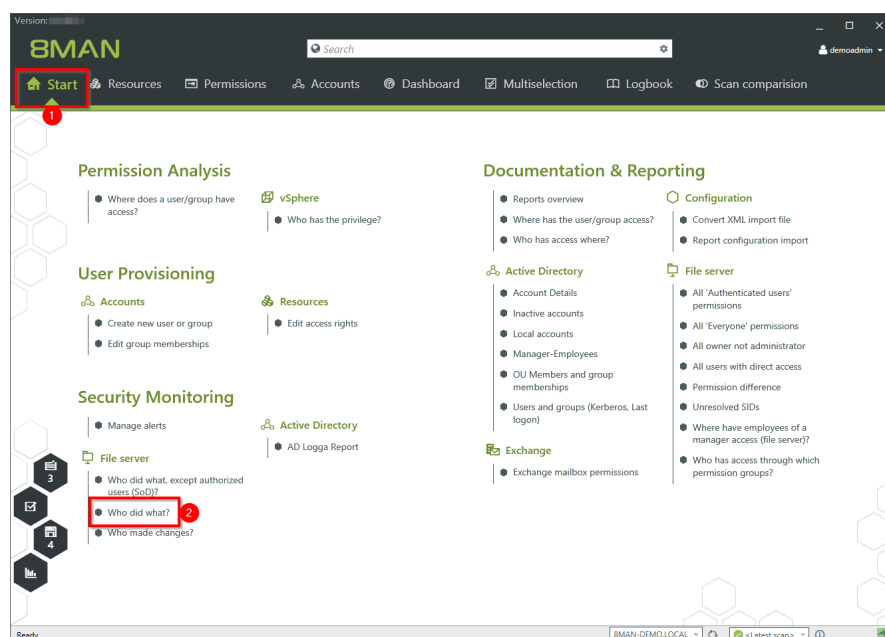
#### Background / Value

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. As of version 8.0, the FS Logga reports can be executed in a timed manner. In addition, we have installed additional filter options. In previous versions, filter functions could only be applied to the finished Excel report.

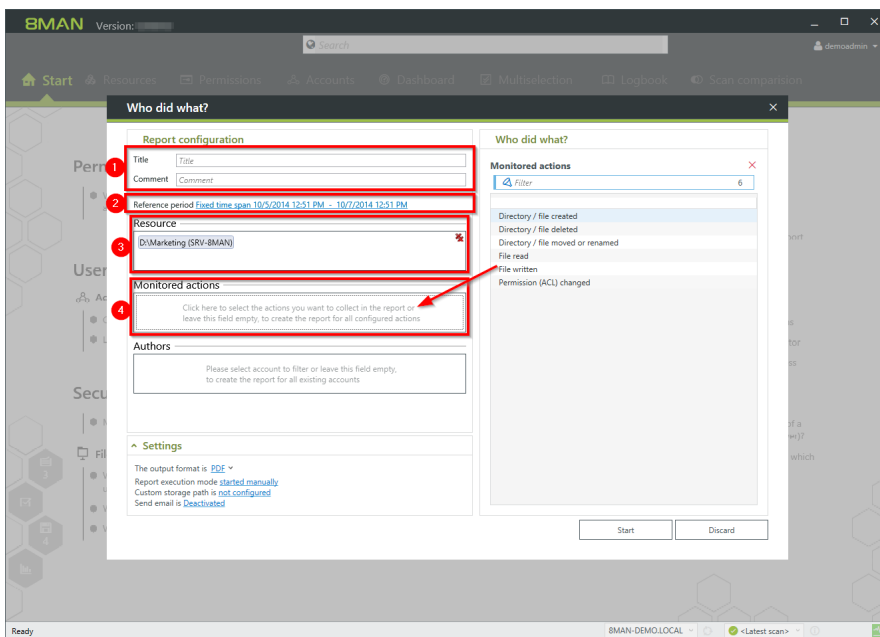
#### Additional services

[Change directory access rights](#)

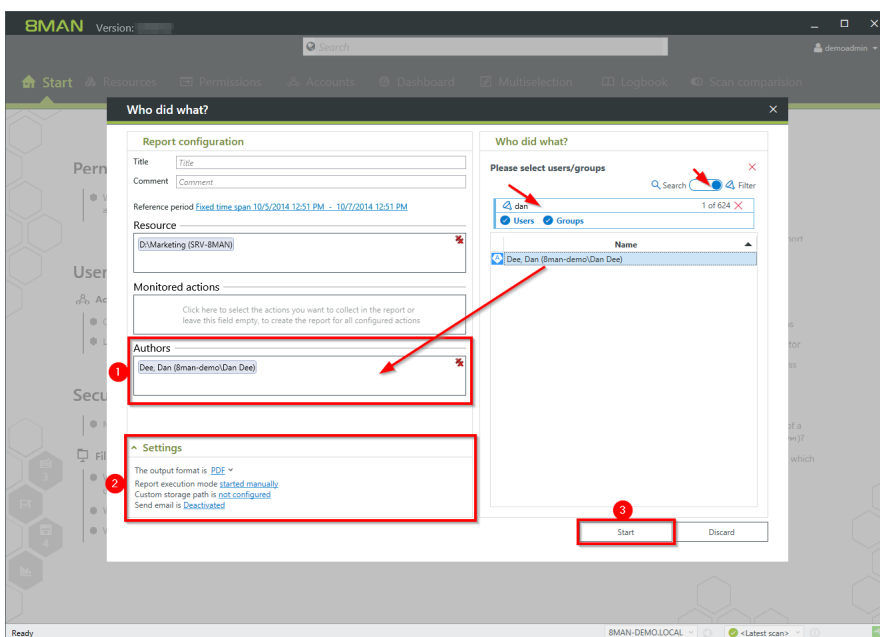
#### Step by step process



1. Select "Start".
2. Click on "Who did what?".



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.



1. Add authors. Use filter and search to find the desired users.
2. Define the desired output settings:
  - Format: PDF or XLS
  - Scheduling of regular reports
  - Saving location
  - send via email
3. Start the report.

### 6.2.1.2 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, 8MAN sends an alert to the data controller.

#### Additional Services

[Enable alerts for suspected data theft \(file server\)](#)

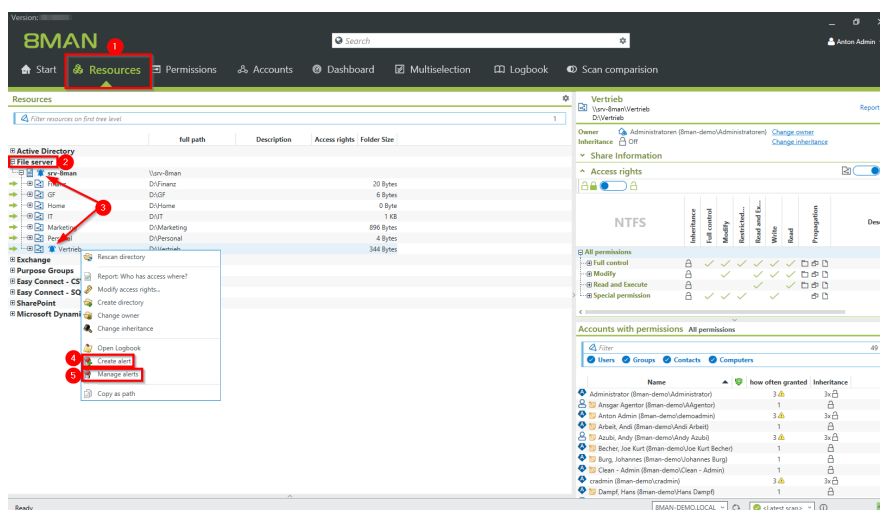
[Enable alerts for data deletion \(file server\)](#)

[Enable alerts for suspected cases on ransomware \(file server\)](#)

[Run a script after an alert](#)

Manage alerts

#### Step by step process



1. Choose Resources.
2. Expand the "file server".
3. Already configured alerts are displayed with a bell symbol.
4. Right-click on a resource and select "Create alert" in the context menu to create a new alert.
5. Right-click a resource and select Manage alerts in the context menu to customize or delete existing alerts.

**Create alert**

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS !	CATEGORY
Changes in directory for Vertrieb ✓				Information

EVENT SETTING FOR 'CHANGES IN DIRECTORY'

DIRECTORIES	FILES
Directory created <input type="checkbox"/>	File created <input type="checkbox"/>
Directory deleted <input type="checkbox"/>	File deleted <input type="checkbox"/>
Directory moved or renamed <input type="checkbox"/>	File moved or renamed <input type="checkbox"/>
Directory permission (ACL) changed <input checked="" type="checkbox"/>	File read <input type="checkbox"/>
Directory depth 0 -> +∞	File written <input type="checkbox"/>
	File permission (ACL) changed <input checked="" type="checkbox"/>

0 **Blacklist Users**

Please add a comment

Create Cancel

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

**Blacklist Users**

Please choose one or more users below which are not considered for the alert

AVAILABLE USERS	THESE USERS WILL NOT BE CONSIDERED
<p>Search Filter</p> <p>Sam Sales (8man-demo\Sam.Sales)</p> <p>Sam Sales (8man-demo\Sam.Sales)</p>	<p>Filter 1</p> <p>Sam Sales (8man-demo\Sam.Sales)</p>

Apply Discard

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.

**Create alert**

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS !	CATEGORY
Changes in directory for Vertrieb ✓				Information

**EVENT SETTING FOR 'CHANGES IN DIRECTORY'**

Directory created	<input type="checkbox"/>	File created	<input type="checkbox"/>
Directory deleted	<input type="checkbox"/>	File deleted	<input type="checkbox"/>
Directory moved or renamed	<input type="checkbox"/>	File moved or renamed	<input type="checkbox"/>
Directory permission (ACL) changed	<input checked="" type="checkbox"/>	File read	<input type="checkbox"/>
Directory depth 0 - +∞		File written	<input type="checkbox"/>
		File permission (ACL) changed	<input checked="" type="checkbox"/>

0 [Blacklist Users](#)

0 [Blacklist Directories](#)

Please add a comment

Create Cancel

Optional:  
Select "Blacklist Directories".

**Blacklist Directories**

Please choose one or more directories below which are not considered for the alert

**1 AVAILABLE DIRECTORIES BELOW 'VERTRIEB'**

Filter

- Hersteller
- Kunden
- öffentlicher.ag
- Projekte

**THESE DIRECTORIES WILL NOT BE CONSIDERED**

Filter

- \srv-8man\Vertrieb\Projekte

Apply Discard

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 "Del" key to remove directories from the blacklist.
4. Enable or disable the monitoring of subdirectories.
5. Click "Apply" to save the changes.



Create alert

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Vertrieb ✓	✓	✓	✓ <b>1</b>	Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email ☒ **2**

To: admin@bman-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Rom, Stockholm, Wien

Write to Windows event log ☒ **3**

Execute script ☒ **4**

Please add a comment

Create Cancel

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. 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.

Create alert

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Vertrieb ✓	✓	✓	✓	Information <b>1</b>

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email ☒

To: admin@bman-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Rom, Stockholm, Wien

Write to Windows event log ☒

Execute script ☒

Please add a comment

Create Cancel

Choose a category.

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

Create alert

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME

Changes in directory for Vertrieb

EVENT

THRESHOLD

ACTIONS

CATEGORY

Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To

admin@8man-demo.local

Language

English

Time zone

(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log

Execute script

Please add a comment

Create

Cancel

1. You must specify a reason for the alert configuration in order to save it.
2. Click on "Create".

### 6.2.1.3 Enable alerts for suspected data theft (file server)

#### Background / Value

To efficiently capture security incidents, 8MAN focuses on user-initiated file server events. If these occur in unusually high numbers and additionally in a short period of time, 8MAN proactively informs all those responsible.

Data theft: A user account reads an unusually large number of files in a short period of time.

#### Additional Services

[Enable alerts for file server directories](#)

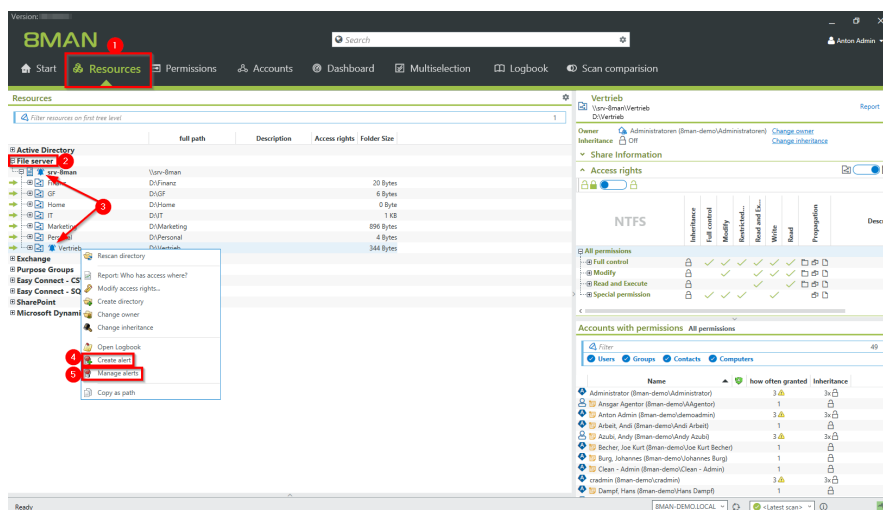
[Enable alerts for data deletion \(file server\)](#)

[Enable alerts for suspected cases on ransomware \(file server\)](#)

[Run a script after an alert](#)

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.

**Create alert**

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS !	CATEGORY
Changes in directory for Vertrieb ✓				Information

**EVENT SETTING FOR 'CHANGES IN DIRECTORY'**

Directory created	<input type="checkbox"/>	File created	<input type="checkbox"/>
Directory deleted	<input type="checkbox"/>	File deleted	<input type="checkbox"/>
Directory moved or renamed	<input type="checkbox"/>	File moved or renamed	<input type="checkbox"/>
Directory permission (ACL) changed	<input checked="" type="checkbox"/>	File read	<input type="checkbox"/>
Directory depth 0 - +∞		File written	<input type="checkbox"/>
		File permission (ACL) changed	<input checked="" type="checkbox"/>

0 [Blacklist Users](#)

0 [Blacklist Directories](#)

Please add a comment

Create Cancel

- optional:  
Select "Blacklist directories".

**Blacklist Directories**

Please choose one or more directories below which are not considered for the alert

**1 AVAILABLE DIRECTORIES BELOW 'VERTRIEB'**

Filter

- Hersteller
- Kunden
- öffentlicher ag
- Projekte

**THESE DIRECTORIES WILL NOT BE CONSIDERED**

Filter

- \srv-sman\Vertrieb\Projekte

Apply Discard


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


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


Create alert

Create an alert for 'srv-8man' that will execute the selected actions when occurred.

ALERT NAME: Suspected data theft ✓

EVENT:  ✓

THRESHOLD:  1

ACTIONS:  !

CATEGORY: Information

WHEN YOU NEED AN ALERTING FOR A SET NUMBER OF EVENTS WITHIN A SET PERIOD OF TIME, THEN MAKE A THRESHOLD SETTING

2 ☐ On ☒ Off Turn threshold on

3 ☒ Yes ☐ No caused by the same initiator

4 10,000 - + Required number of events to trigger alert

60 - + Seconds Limit monitoring to a period of time

Alert when 10000 events are initiated by the same initiator within a duration of 60 Seconds

Your threshold is set

Please add a comment


Create Cancel


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


Create alert

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME: Changes in directory for Vertrieb ✓

EVENT:  ✓

THRESHOLD:  ✓

ACTIONS:  1

CATEGORY: Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email ☒ 2

To: admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log ☒ 3

Execute script ☒ 4

Please add a comment

Create Cancel

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. 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.

**Create alert** ×

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Vertrieb ✓	✓	✓	✓	<div>Information</div> <div>Information</div> <div>Warning</div> <div>Critical</div>

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email ☒

To: admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log ☒

Execute script ☒

Please add a comment

Choose a category.

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

**Create alert** ×

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Vertrieb ✓	✓	✓	✓	Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email ☒

To: admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log ☒

Execute script ☒

Please add a comment

1. You must specify a reason for the alert configuration in order to save it.
2. Click "Apply".

### 6.2.1.4 Enable alerts for data deletion (file server)

#### Background / Value

To efficiently capture security incidents, 8MAN focuses on user-initiated file server events. If these occur in unusually high numbers and additionally in a short period of time, 8MAN proactively informs all those responsible.

Data deletions: A user account deletes very many files in a short period of time.

#### Additional Services

[Enable alerts for file server directories](#)

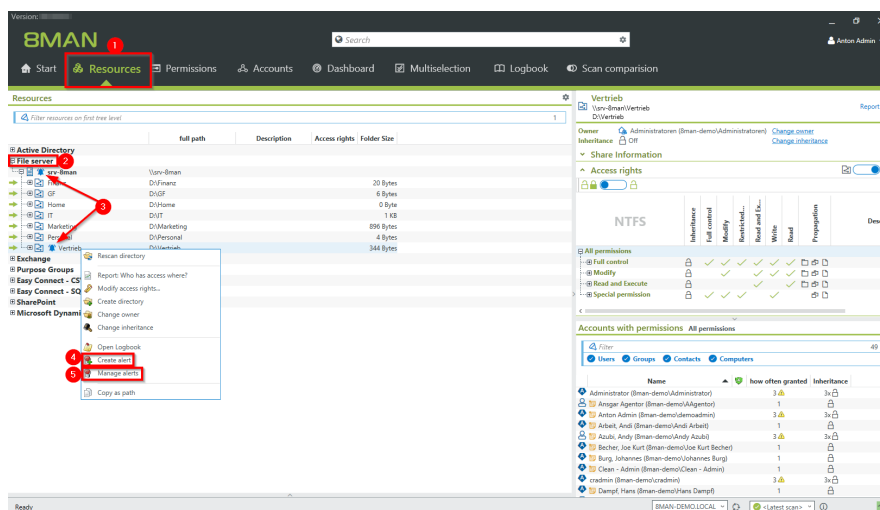
[Enable alerts for suspected data theft \(file server\)](#)

[Enable alerts for suspected cases on ransomware \(file server\)](#)

[Run a script after an alert](#)

Manage alerts

#### Step by step process



1. Choose Resources.
2. Expand the "file server".
3. Already configured alerts are displayed with a bell symbol.
4. Right-click on a resource and select "Create alert" in the context menu to create a new alert.
5. Right-click a resource and select Manage alerts in the context menu to customize or delete existing alerts.



Create alert

Create an alert for 'srv-8man' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Data deletion				Information

EVENT SETTING FOR 'CHANGES IN FILE SERVER'

DIRECTORIES	FILES
Directory created	File created
Directory deleted	File deleted
Directory moved or renamed	File moved or renamed
Directory permission (ACL) changed	File read
	File written
	File permission (ACL) changed

0 Blacklist Users

Please add a comment

Create Cancel

1. Give the alert configuration a name.
2. Choose "Event".
3. Define which events trigger an alert. For data deletions typically: "directory deleted" and "file deleted".
4. Optional: Click on "Blacklist user".

Blacklist Users

Please choose one or more users below which are not considered for the alert

AVAILABLE USERS	THESE USERS WILL NOT BE CONSIDERED
<p>Search Filter</p> <p>Sam Sales (8man-demo\Sam.Sales)</p> <p>Sam Sales (8man-demo\Sam.Sales)</p>	<p>Filter 1</p> <p>Sam Sales (8man-demo\Sam.Sales)</p>

Apply Discard

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.

1. optional:  
Select "Blacklist directories".


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


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


Create alert

Create an alert for 'srv-8man' that will execute the selected actions when occurred.

ALERT NAME: Suspected data theft ✓

EVENT:  ✓

THRESHOLD:  1

ACTIONS:  !

CATEGORY: Information

WHEN YOU NEED AN ALERTING FOR A SET NUMBER OF EVENTS WITHIN A SET PERIOD OF TIME, THEN MAKE A THRESHOLD SETTING

2 ☐ On ☒ Off Turn threshold on

3 ☒ Yes ☐ No caused by the same initiator

4 10,000 - + Required number of events to trigger alert

60 - + Seconds Limit monitoring to a period of time

Alert when 10000 events are initiated by the same initiator within a duration of 60 Seconds

Your threshold is set

Please add a comment


Create Cancel


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


Create alert

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME: Changes in directory for Vertrieb ✓


EVENT:  ✓

THRESHOLD:  ✓

ACTIONS:  1

CATEGORY: Information


DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT


Send email ☒  2

To: admin@man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log ☒  3

Execute script ☒  4

Please add a comment

Create Cancel

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. 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.

Create alert

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME

Changes in directory for Vertrieb

EVENT

THRESHOLD

ACTIONS

CATEGORY

Information

Information

Warning

Critical

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To

admin@8man-demo.local

Language

English

Time zone

(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log

Execute script

Please add a comment

Create

Cancel

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

Create alert

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME

Changes in directory for Vertrieb

EVENT

THRESHOLD

ACTIONS

CATEGORY

Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email

To

admin@8man-demo.local

Language

English

Time zone

(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log

Execute script

Please add a comment

Create

Cancel

1. You must specify a reason for the alert configuration in order to save it.
2. Click "Apply".

### 6.2.1.5 Enable alerts for suspected cases on ransomware (file server)

#### Background / Value

To efficiently capture security incidents, 8MAN focuses on user-initiated file server events. If these occur in unusually high numbers and additionally in a short period of time, 8MAN proactively informs all those responsible.

Ransomware Attack: The combination of file creation and deletion by one user account.

#### Additional Services

[Enable alerts for file server directories](#)

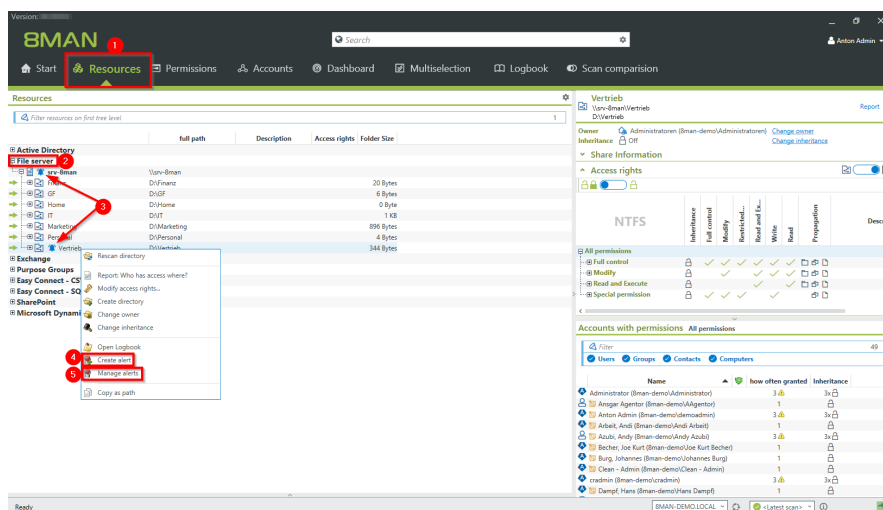
[Enable alerts for suspected data theft \(file server\)](#)

[Enable alerts for data deletion \(file server\)](#)

[Run a script after an alert](#)

Manage alerts

#### Step by step process



1. Choose Resources.
2. Expand the "file server".
3. Already configured alerts are displayed with a bell symbol.
4. Right-click on a resource and select "Create alert" in the context menu to create a new alert.
5. Right-click a resource and select Manage alerts in the context menu to customize or delete existing alerts.

Create an alert for 'srv-8man' that will execute the selected actions when occurred.

ALERT NAME: Ransomware suspect ✓

EVENT: [Bell icon]

THRESHOLD: [Bell icon]

ACTIONS: [Bell icon]

CATEGORY: Information

EVENT SETTING FOR "CHANGES IN FILE SERVER"

DIRECTORIES:

- Directory created ☐
- Directory deleted ☐
- Directory moved or renamed ☐
- Directory permission (ACL) changed ☐

FILES:

- File created ☒
- File deleted ☒
- File moved or renamed ☐
- File read ☐
- File written ☐
- File permission (ACL) changed ☐

0 Blacklist Users

Please add a comment

Create Cancel

1. Give the alert configuration a name.
2. Choose "Event".
3. Define which events trigger an alert. Typical for ransomware: a combination of "file created" and "file deleted".
4. optional:  
Click on "Blacklist users".

Blacklist Users

Please choose one or more users below which are not considered for the alert

AVAILABLE USERS

Search Filter

Sam Sales (8man-demo\Sam.Sales)

Name

Sam Sales (8man-demo\Sam.Sales)

THESE USERS WILL NOT BE CONSIDERED

Filter 1

Name

Sam Sales (8man-demo\Sam.Sales)

Apply Discard

- 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.

**Create alert**

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS !	CATEGORY
Changes in directory for Vertrieb ✓				Information

**EVENT SETTING FOR 'CHANGES IN DIRECTORY'**

Directory created	<input type="checkbox"/>	File created	<input type="checkbox"/>
Directory deleted	<input type="checkbox"/>	File deleted	<input type="checkbox"/>
Directory moved or renamed	<input type="checkbox"/>	File moved or renamed	<input type="checkbox"/>
Directory permission (ACL) changed	<input checked="" type="checkbox"/>	File read	<input type="checkbox"/>
Directory depth 0 -> +∞		File written	<input type="checkbox"/>
		File permission (ACL) changed	<input checked="" type="checkbox"/>

0 [Blacklist Users](#)

0 [Blacklist Directories](#)

Please add a comment

Create Cancel

- optional:  
Select "Blacklist directories".

**Blacklist Directories**

Please choose one or more directories below which are not considered for the alert

**1 AVAILABLE DIRECTORIES BELOW 'VERTRIEB'**

Filter

- Hersteller
- Kunden
- öffentlicher ag
- Projekte

**THESE DIRECTORIES WILL NOT BE CONSIDERED**

Filter

- \srv-sman\Vertrieb\Projekte

Apply Discard


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


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


Create alert

Create an alert for 'srv-8man' that will execute the selected actions when occurred.

ALERT NAME: Suspected data theft ✓

EVENT:  ✓

THRESHOLD:  1

ACTIONS:  !

CATEGORY: Information

WHEN YOU NEED AN ALERTING FOR A SET NUMBER OF EVENTS WITHIN A SET PERIOD OF TIME, THEN MAKE A THRESHOLD SETTING

2 ☐ On ☒ Off Turn threshold on

3 ☒ Yes ☐ No caused by the same initiator

4 10,000 - + Required number of events to trigger alert

60 - + Seconds Limit monitoring to a period of time

Alert when 10000 events are initiated by the same initiator within a duration of 60 Seconds

Your threshold is set

Please add a comment


Create Cancel


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


Create alert

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME: Changes in directory for Vertrieb ✓

EVENT:  ✓

THRESHOLD:  ✓

ACTIONS:  1

CATEGORY: Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email ☒ 2

To: admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log ☒ 3

Execute script ☒ 4

Please add a comment

Create Cancel

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. 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.



**Create alert** ×

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Vertrieb ✓	✓	✓	✓	<div>Information</div> <div>Information</div> <div>Warning</div> <div>Critical</div>

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email ☒

To: admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log ☒

Execute script ☒

Please add a comment

Choose a category.

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

**Create alert** ×

Create an alert for 'Vertrieb' that will execute the selected actions when occurred.

ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Vertrieb ✓	✓	✓	✓	Information

DECIDE WHICH ACTIONS SHOULD BE CARRIED THROUGH WITH THIS ALERT

Send email ☒

To: admin@8man-demo.local

Language: English

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Write to Windows event log ☒

Execute script ☒

Please add a comment

1. You must specify a reason for the alert configuration in order to save it.
2. Click "Apply".

### 6.3 Exchange

#### 6.3.1 Monitor Exchange activities

##### Background / Value

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 8MATE 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?

##### Services

[Create a report about activities on mailboxes, calendars, and contacts](#)

[View activities in mailboxes, calendars, and contacts \(logbook\)](#)

### 6.3.1.1 Monitor activities on mailboxes, calendars, and contacts (report)

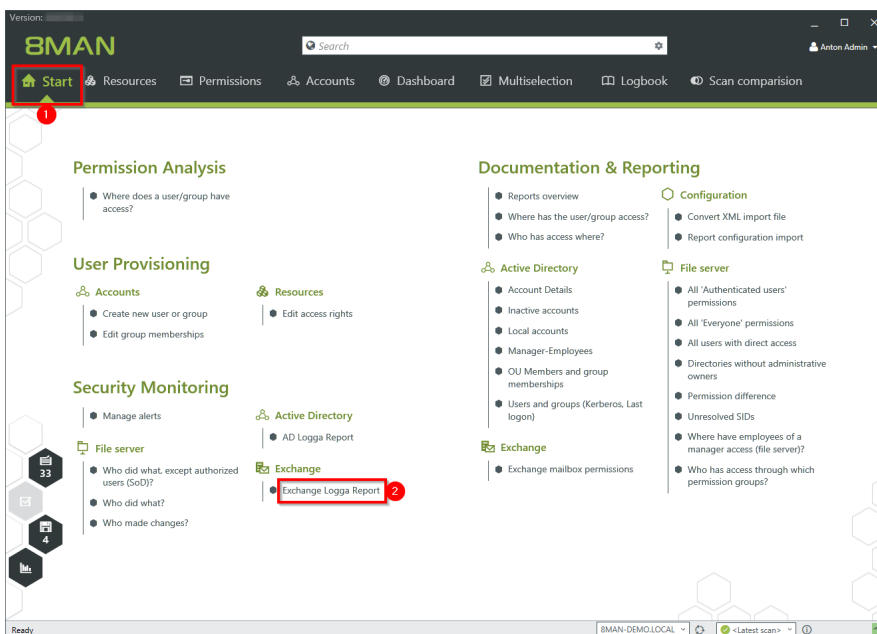
#### Background / Value

Events recorded with the 8MATE 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](#).

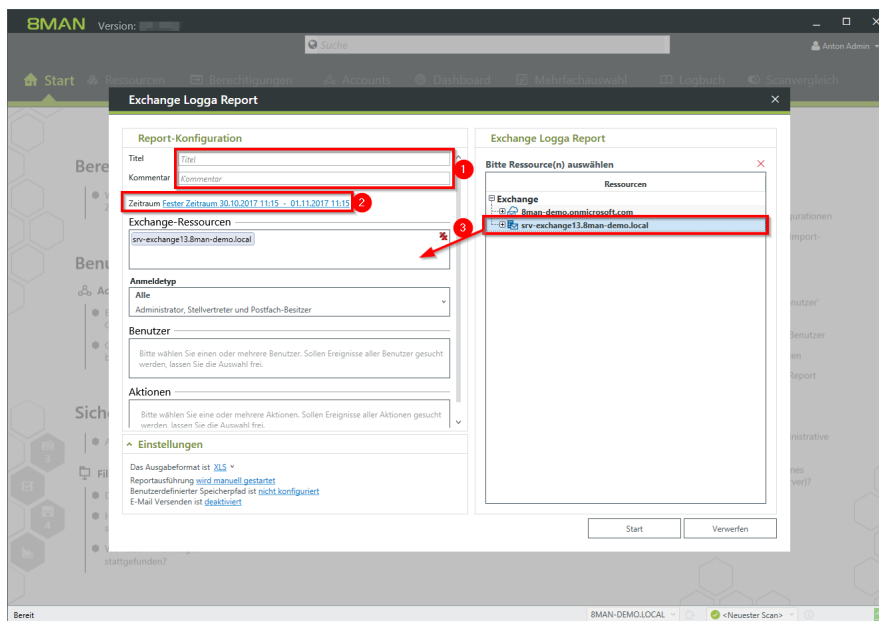
#### Additional Services

[View activities in mailboxes, calendars, and contacts \(logbook\)](#)

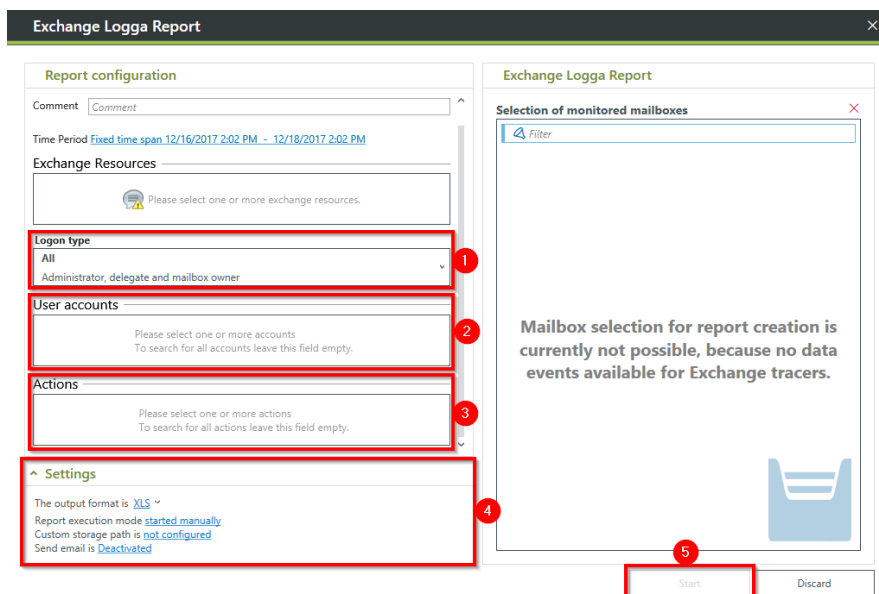
#### Step by step process



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.

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

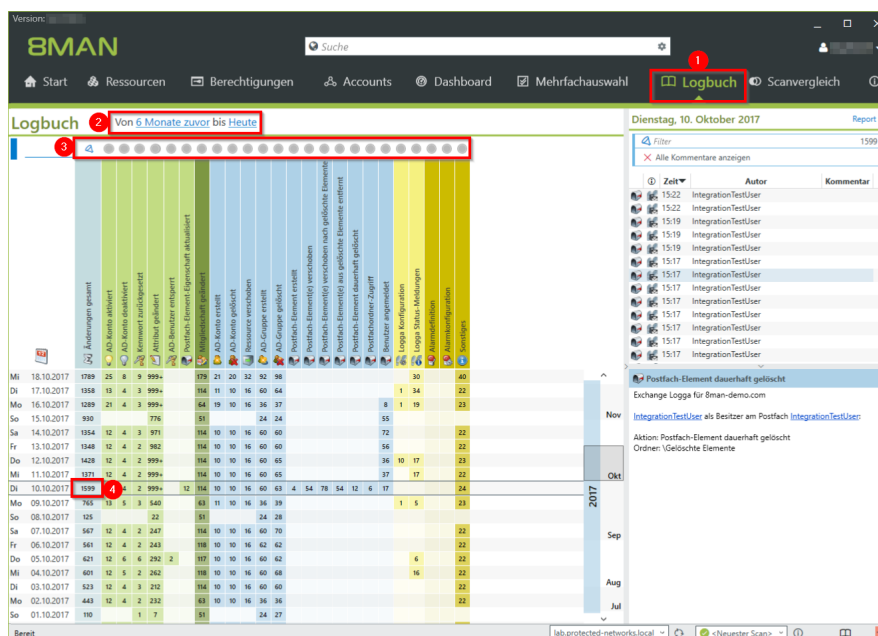
#### Background / Value

Events recorded with the 8MATE 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.

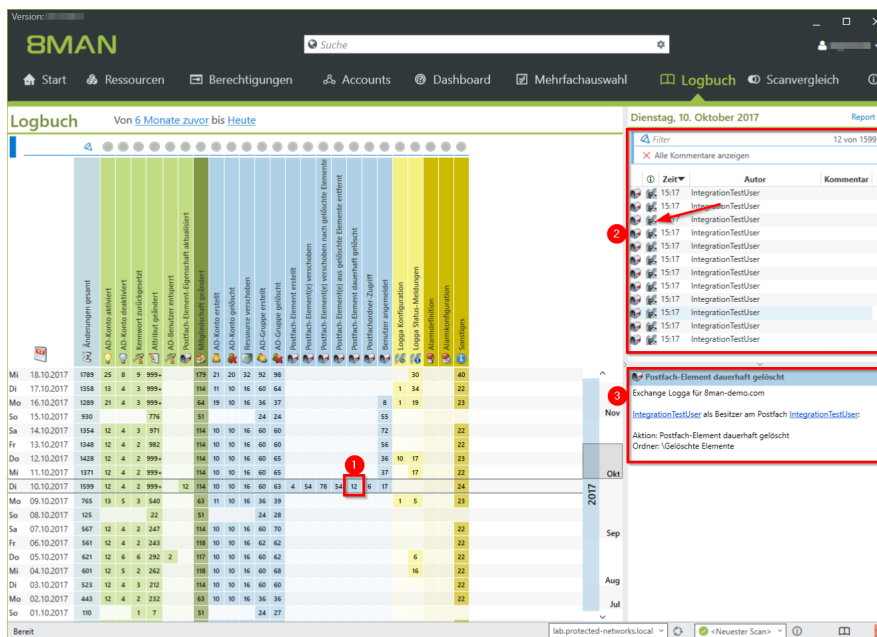
#### Additional Services

Report: [Monitor activities on mailboxes, calendars, and contacts](#)

#### Step by step process



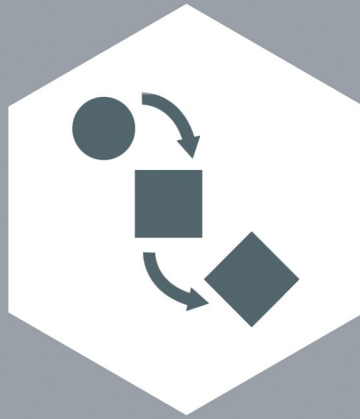
1. Select "Logbook".
2. Set the time period for log analysis.
3. The filters focus on the events you want to check.
4. Select all events of a day (one row).



1. Select a cell (an event type) to further narrow your query.
2. 8MAN displays a list of all selected events. The "Footprint icon with envelope" identifies events recorded by the Exchange Logga. Select an event.
3. 8MAN shows all details about the event.



## 7. Role & Process Optimization





## 7.1 Delegation of tasks

8MAN includes a variety of functionality that can benefit users who are not Administrators. 8MAN 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 8MAN 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

### 7.1.1 Apply an 8MAN account to a specific security role or data owner

#### Background / Value

There are two possibilities of involving data security officers and auditors in security related processes.

- Grant the user read only access to 8MAN.
- Define which reports are relevant and 8MAN will send them to the user automatically in the desired frequency.

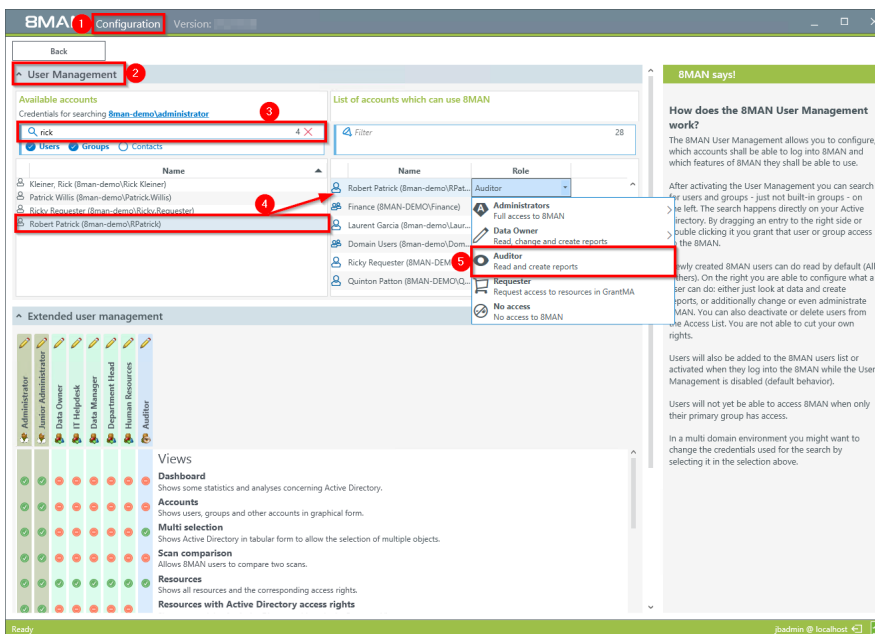
### 7.1.1.1 Create a read only account with 8MAN

#### 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 8MAN configuration module. You can find more detailed information in the Installation and Configuration Manual, chapter Managing 8MAN Users.

#### Step by step process



1. Start the 8MAN configuration.
2. Change to "User Management".
3. Use the search field to find the desired account.
4. Use drag&drop to move the account to the correct column.
5. In the column, select "Auditor".
6. The settings are active immediately.

### 7.1.1.2 Schedule reports

#### Background / Value

You can involve security personell in the process of access rights management by assigning reports to the relevant security officers. 8MAN 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.

#### 8MAN Management Reports:

##### Active Directory

[Employees of a Manager](#)

[Displaying user account details](#)

##### File server

[Who has access to what?](#)

[Where do employees of a manager have access to?](#)

[Where do users and groups have access?](#)

##### Exchange

[Who has access to what?](#)

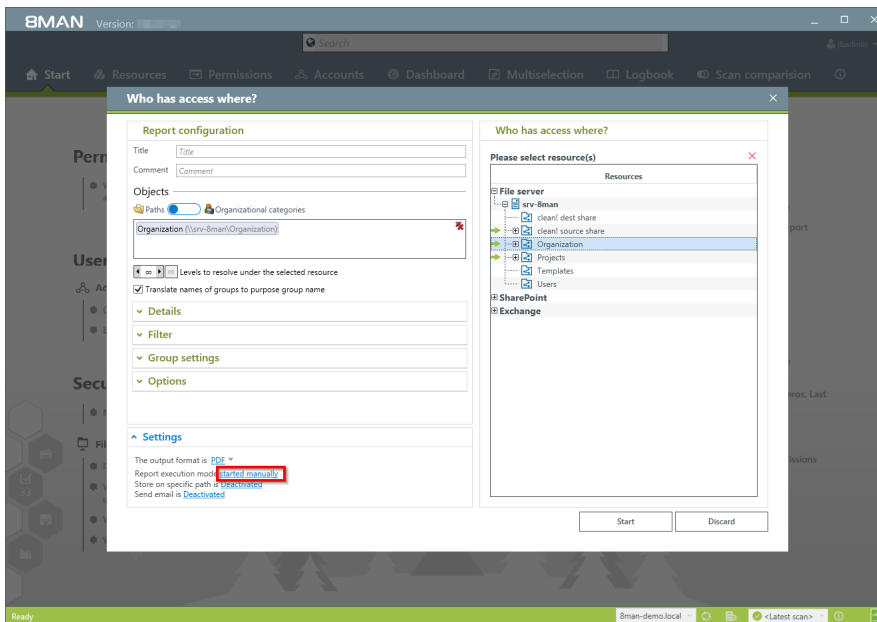
[Identifying mailbox permissions](#)

##### SharePoint

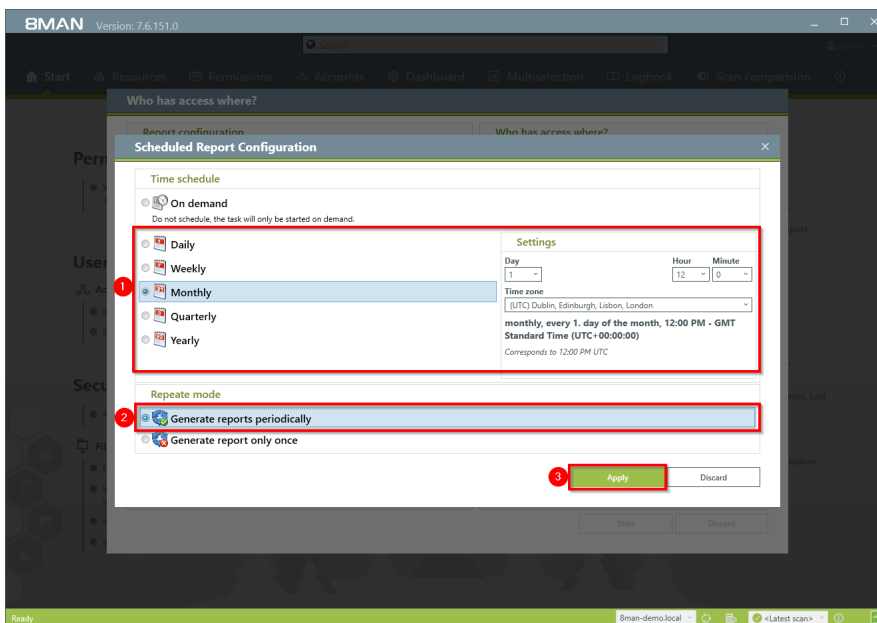
[Who has access where?](#)

[Where do users and groups have access?](#)

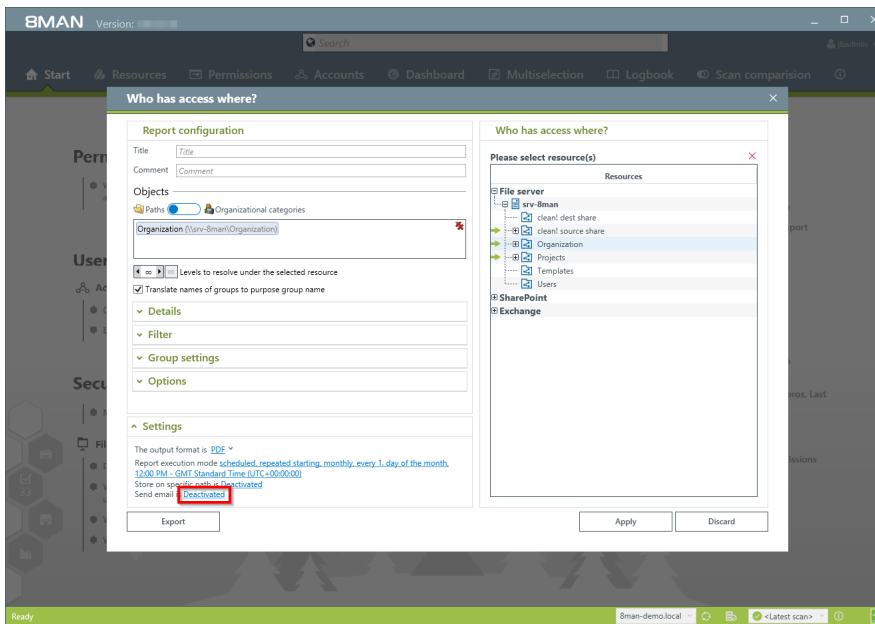
## Step by step process



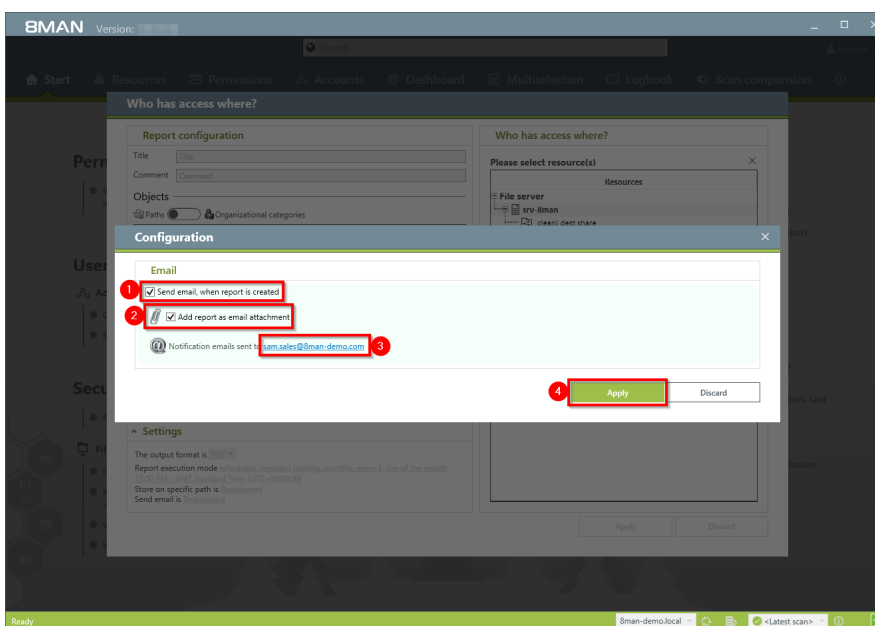
Select the desired report. Click on "started manually" in the "Settings" area.



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



Click on "Deactivated".



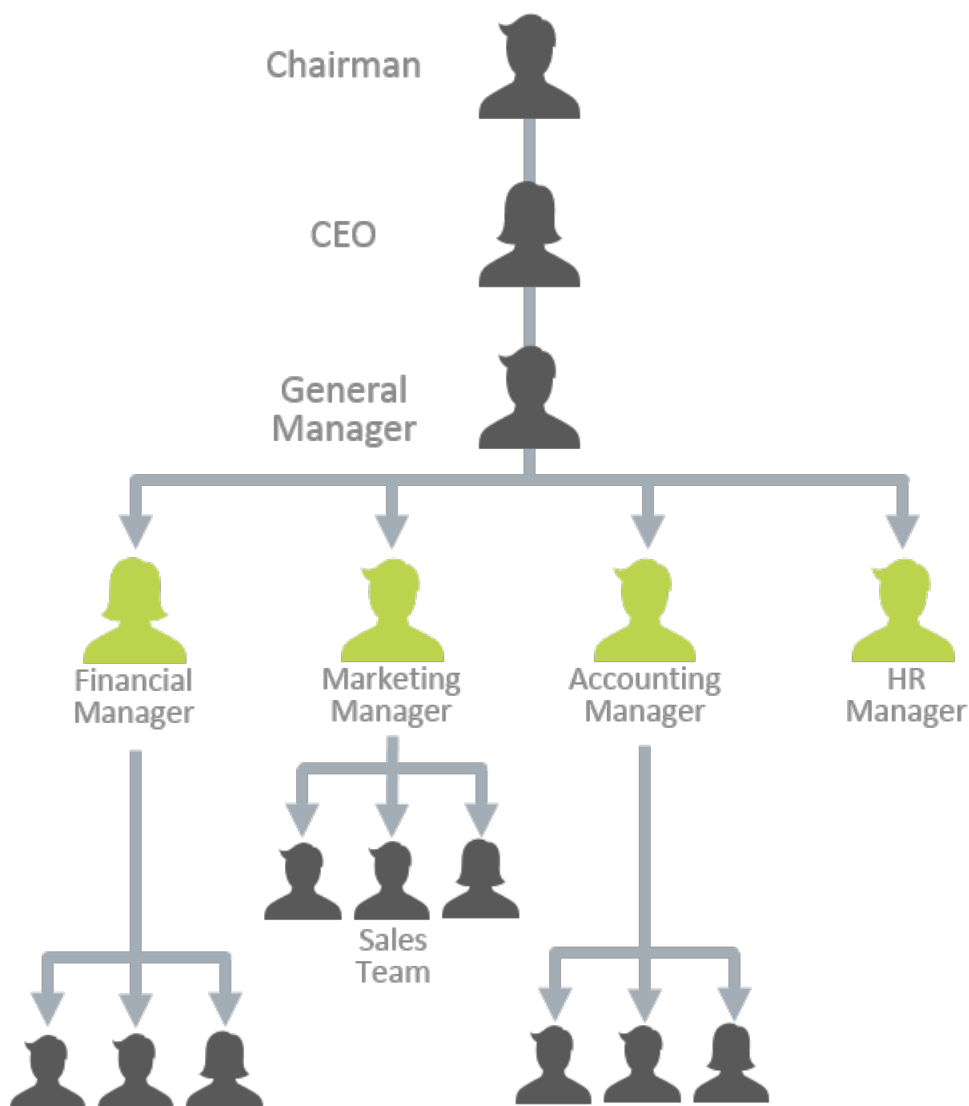
1. Activate emails.
2. Activate the option "Add report as email attachment".
3. Determine who should receive the email. You can enter more than one recipient.
4. Click on "Apply".

### 7.1.2 Assign the administration of folder rights to a Data Owner (Manager)

#### 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 in your organization. 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.**



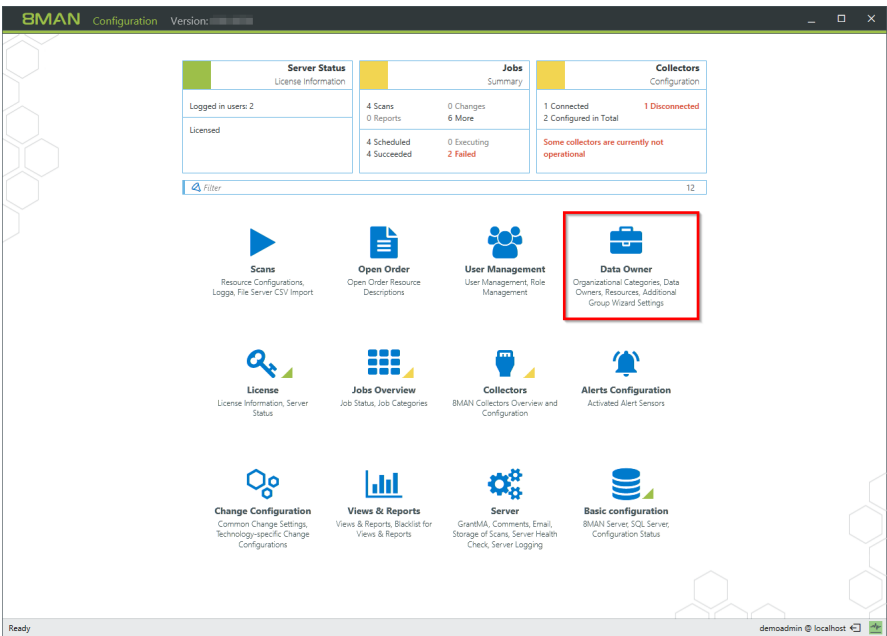
7.1.2.1 Define Data Owners and assign resources

Background / Value

Data Owners and Managers have the responsibility to protect digital resources in their departments. 8MAN allows you to delegate this individual responsibility effectively. The following example shows a typical configuration.

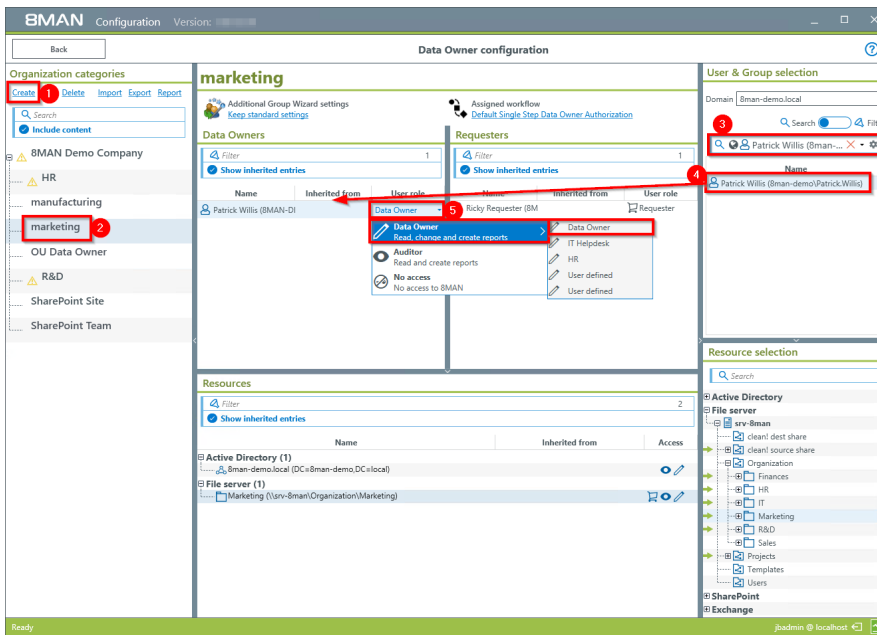
These settings can be found in the 8MAN configuration module. You can find more detailed information in the Handbook for Installation and Configuration, chapter Managing 8MAN Users ff. and Data Owner ff.

Step by step process

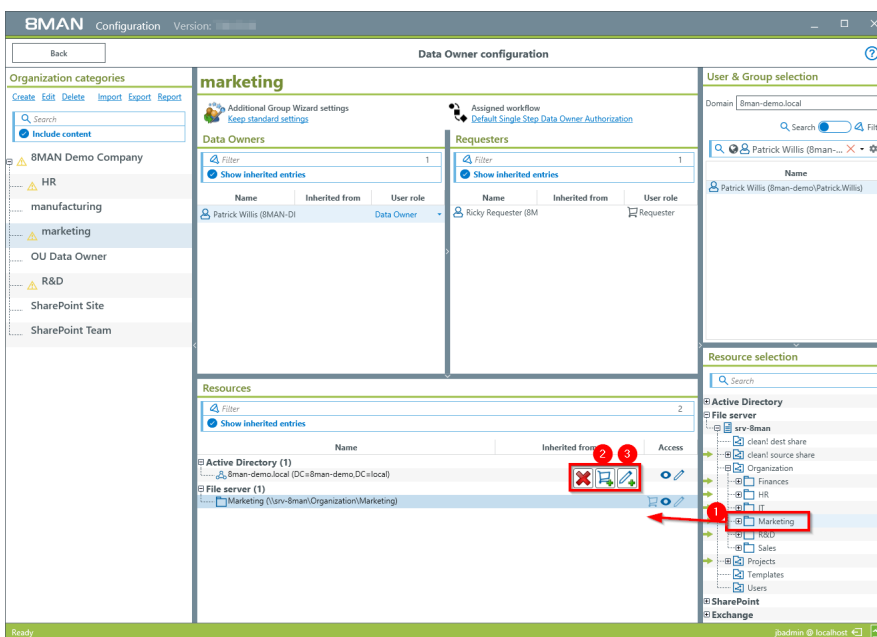


Start the 8MAN configuration module and select "Data Owner".





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 rights".



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 8MATE GrantMA.
  3. Mark the resources as "changeable".
- Please note the access to Active Directory is required to use the group wizard.

### 7.1.2.2 Enable Data Owners to manage file server permissions

#### Background / Value

8MAN 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 (8MAN Visor) and change (8MAN Enterprise) access rights to file servers for their employees and areas of responsibility.

These settings can be found in the 8MAN configuration module. You can find detailed information in the Handbook for Installation and Configuration, chapter Managing 8MAN Users ff. and Data Owner ff.

### 7.1.3 Delegate user provisioning processes to the help desk

User provisioning processes are easy to delegate. With 8MAN 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 8MAN

##### Active Directory

[Unlocking user accounts](#)

[Resetting passwords](#)

[Modifying group and user attributes](#)

[Deactivating a user account](#)

[Deleting a user account by using the "soft delete" feature](#)

[Removing a user and their permissions](#)

##### Exchange

[Creating a mailbox \(email enable users\)](#)

[Managing mailbox and email size](#)

[Managing out of office notices](#)

[Changing mailbox permissions](#)

### 7.1.3.1 Define your help desk and assign resources with 8MAN

#### Background / Value

8MAN relieves Administrators and allows the delegation of standard processes to your help desk. To do this, you must define help desk responsibilities and assign a domain.

These settings can be found in the 8MAN configuration module. You can find detailed information in the Handbook for Installation and Configuration, chapter Managing 8MAN Users ff. and Data Owner ff.

### 7.1.3.2 Assign responsibilities to help desk employees

#### Background / Value

8MAN 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 8MAN configuration module. You can find more detailed information in the Handbook for Installation and Configuration, chapter Managing 8MAN Users ff.

#### Step by step process

The screenshot shows the 8MAN Configuration module with the 'User Management' section active. The interface includes a search bar, a list of accounts, a role selection dropdown, and a list of roles. Red arrows and numbers 1 through 6 indicate the steps for assigning responsibilities to help desk employees.

Name	Role
Discovery Management (Bman-d...	Data Owner
Campbell, David (BMAN-DEMO...	Data Manager
Ali Mente (Bman-demo/Ali Mente)	Human Resources
Torrey Smith (BMAN-DEMO/TSm...	Human Resources
Robert Patrick (Bman-demo/RPat...	Auditor
Help Desk (Bman-demo/Help De...	Auditor

Extended user management roles:

- Administrator
- Junior Administrator
- Data Owner
- IT Helpdesk
- Data Manager
- Department Head
- Human Resources
- Auditor

Views:

- Dashboard
- Accounts
- Multi selection
- Scan comparison
- Resources
- Resources with Active Directory access rights

1. Start the 8MAN configuration module.
2. Select "User Management".
3. Select a change role (columns 3-7). Change the name of the role by clicking on the pen icon. You can then activate or deactivate the individual views and functionalities of the role "Help Desk" as desired.
4. Use the search field to find the desired account.
5. Use drag & drop to move the account into the right-hand column.
6. Assign the role "Help Desk" to the account.

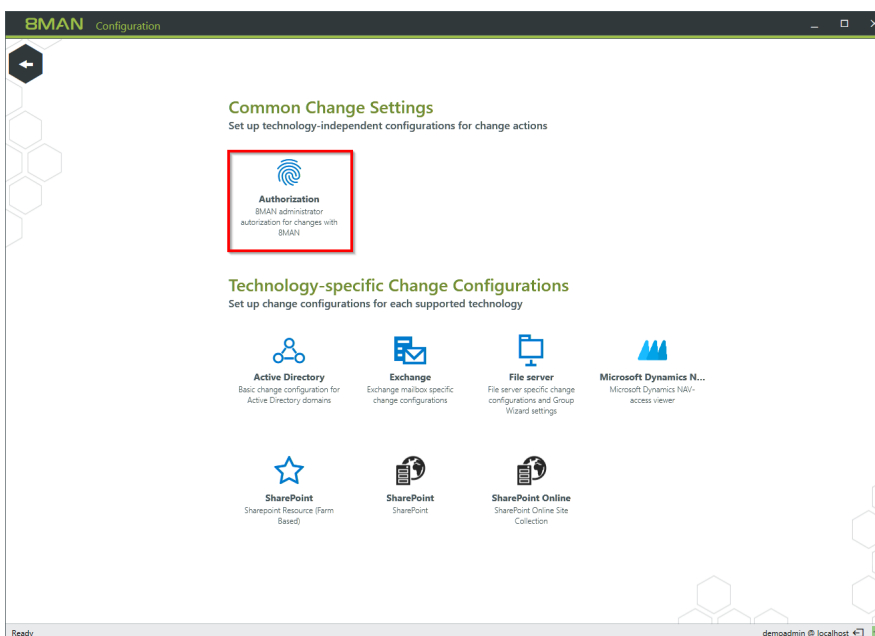
## 7.2 Create approval processes

### 7.2.1 The simple authorization process. Approving and rejecting actions as an Administrator

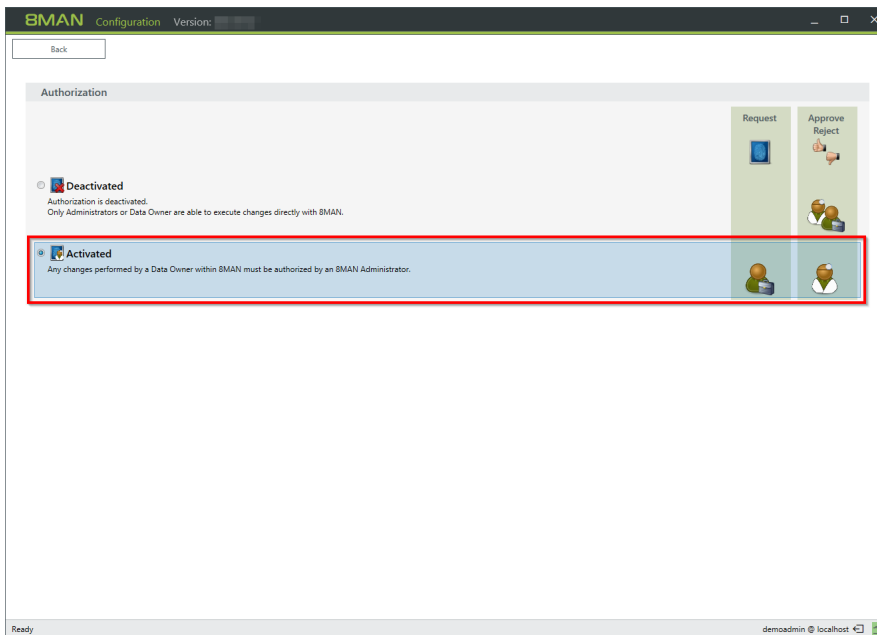
#### Background / Value

8MAN 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 highly 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.

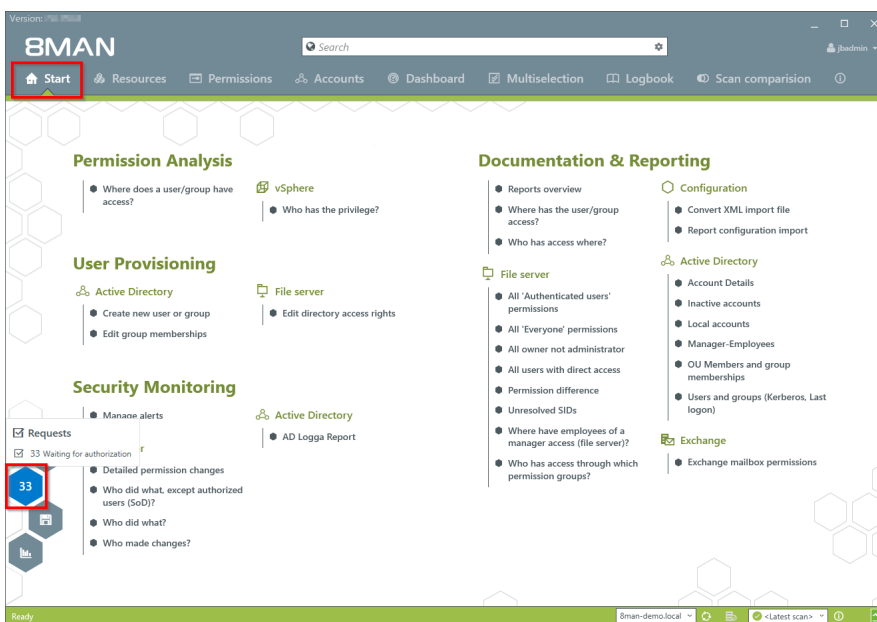
#### Step by step process



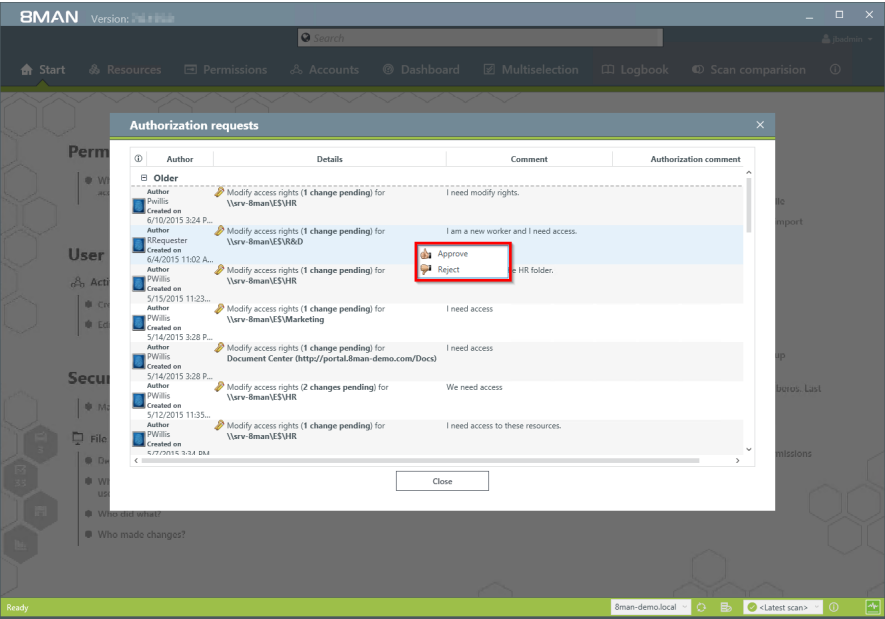
*In the 8MAN configuration module select "Change Configuration">"Authorization".*



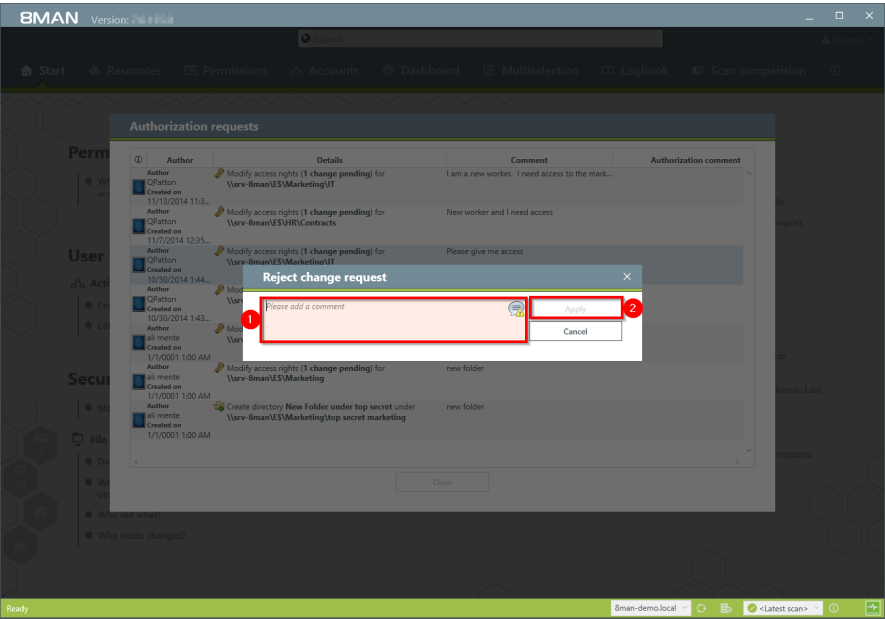
Activate the administrator approval mode.



Administrators are able to see open requests on the home page. Click on the hexagon.



Right click on a request and make your decision.



1. You must enter a comment.
2. Click "Apply".



### 7.2.2 +8MATE GrantMA: design complex approval flows



#### 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. 8MATE 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 8MAN log book.

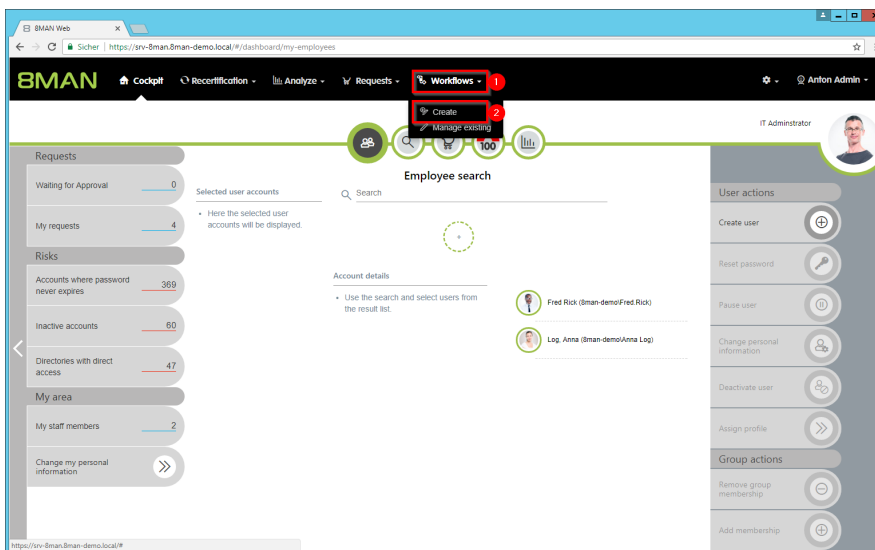
**If more complex workflows with several decision-makers are required to grant access rights, you can also quickly map them.**

### 7.2.2.1 Define individual approval workflows

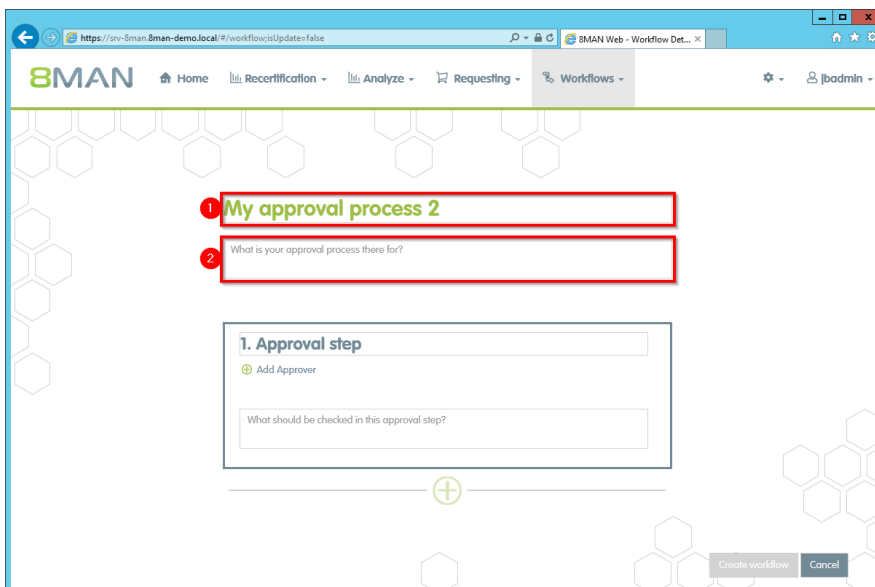
#### Background / Value

8MATE 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.

The screenshot displays the 8MAN Web Workflow Designer interface. The browser's address bar indicates the URL: `https://sv-8man.8man-demo.local/#/workflow/updatefalse`. The top navigation bar features the 8MAN logo and several menu items: Home, Recertification, Analyze, Requesting, and Workflows. The main workspace is titled "My approval process 2" and contains a text input field labeled "Demo". Below the workspace, a workflow diagram is shown with four steps, each highlighted with a red box and a numbered circle: 1. "1. Approval step", 2. "Add Approver", 3. "What should be checked in this approval step?", and 4. A plus icon in a box. The bottom right corner of the interface includes "Create workflow" and "Cancel" buttons.

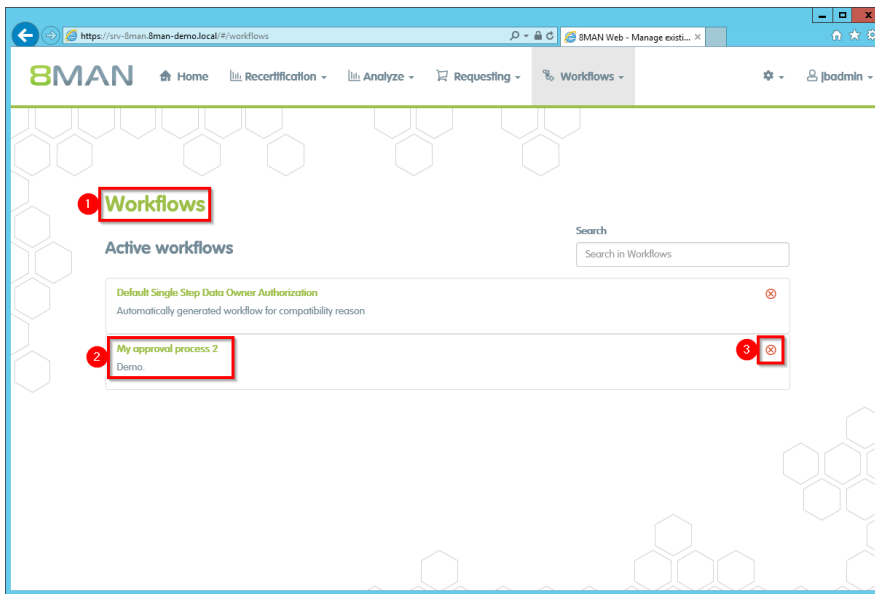
1. Name the approval step.
2. Add one or more approvers

**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.

The screenshot displays the 8MAN Web Workflow Designer interface. The browser address bar shows the URL: `https://my-8man.8man-demo.local/#/workflows/updates/false`. The top navigation bar includes links for Home, Recertification, Analyze, Requesting, and Workflows. The main content area shows a workflow diagram with two 'Approval step' boxes. The first step is labeled '1. Approval step' and the second is '2. Approval step'. Both steps have a text input field for 'What should be checked in this approval step?'. Red annotations highlight specific UI elements: a red box labeled '1' around a diamond icon, a red box labeled '2' around a gear icon, and a red box labeled '3' around a 'Create workflow' button.

1. Add an additional step.
2. Delete an approval step.
3. Generate the workflow.



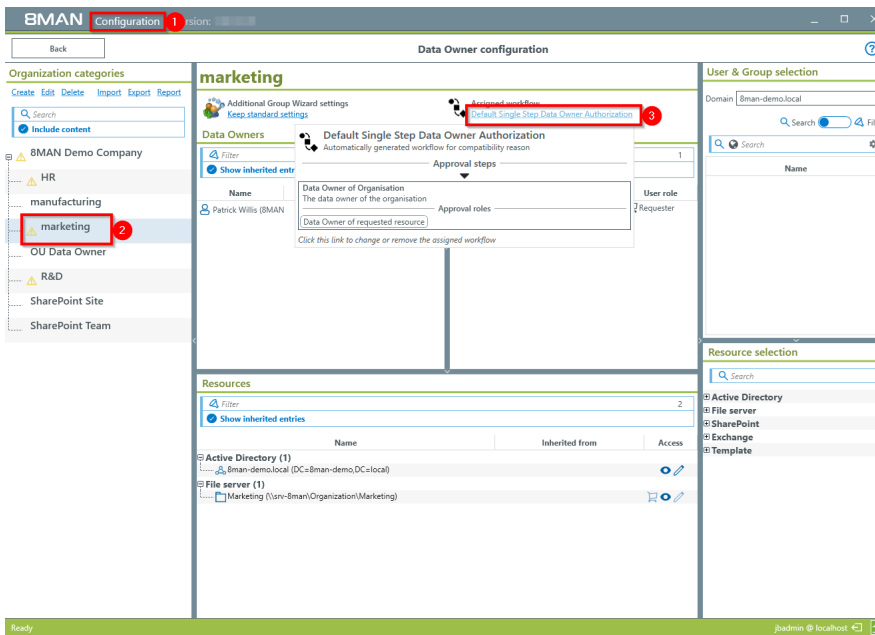
1. You have created a new workflow. 8MAN switches to the "Manage workflows" view.
2. Click on a workflow to make changes.
3. Delete the workflow.

### 7.2.2.2 Assigning approval workflows to individual resources

#### Background / Value

Connecting available resources with individual workflows.

#### Step by step process



1. Start the 8MAN configuration module and select "Data Owner".
2. Select an organizational category.
3. Assign the desired workflow.

### 7.2.2.3 Assigning resource owners using the web client

#### Background / Value

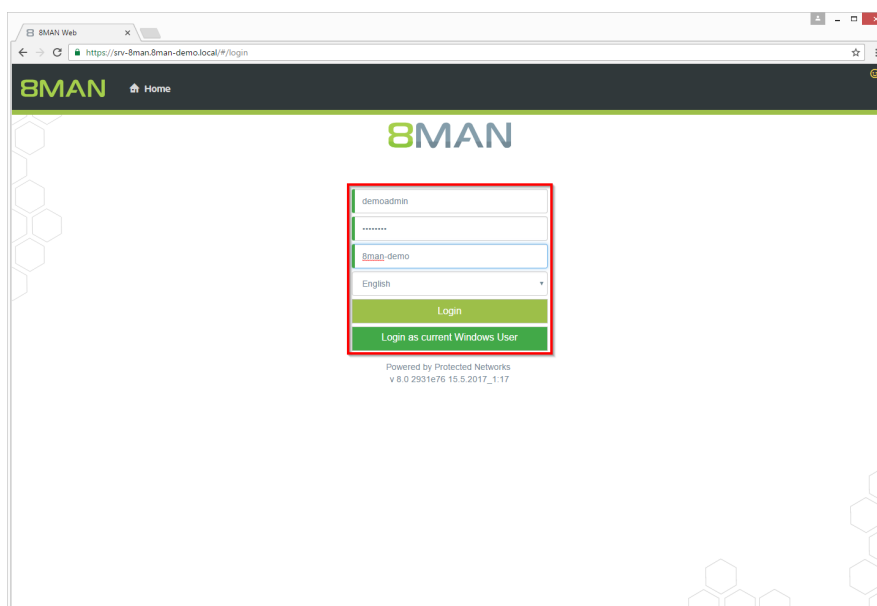
With version 8.0 8MAN releases new features to move the GrantMA configuration into the web client. We inserted the new role "Resource Owner". Assign this role completely using the web client. Due to the requirements of our customers we designed a direct assignment between the Resource Owner and the resource - without the need of creating organizational categories in the data owner configuration.

**The functionality is deactivated by default. Please contact support for activating.**

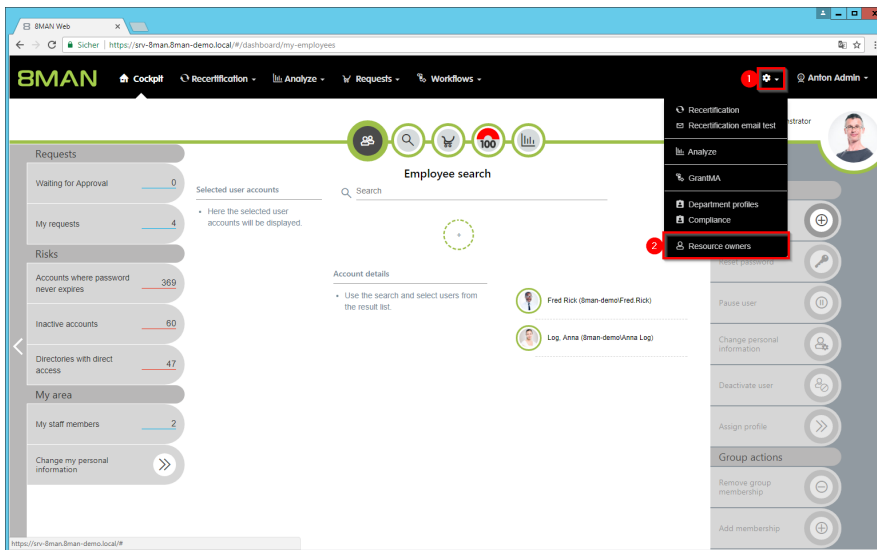
#### Additional Services

[Defining individual approval workflows](#)

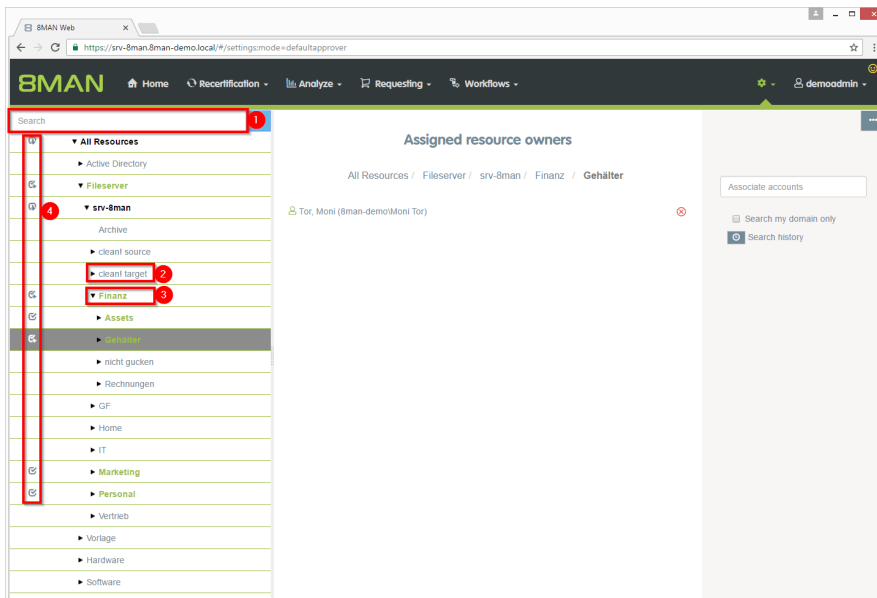
#### Step by step process



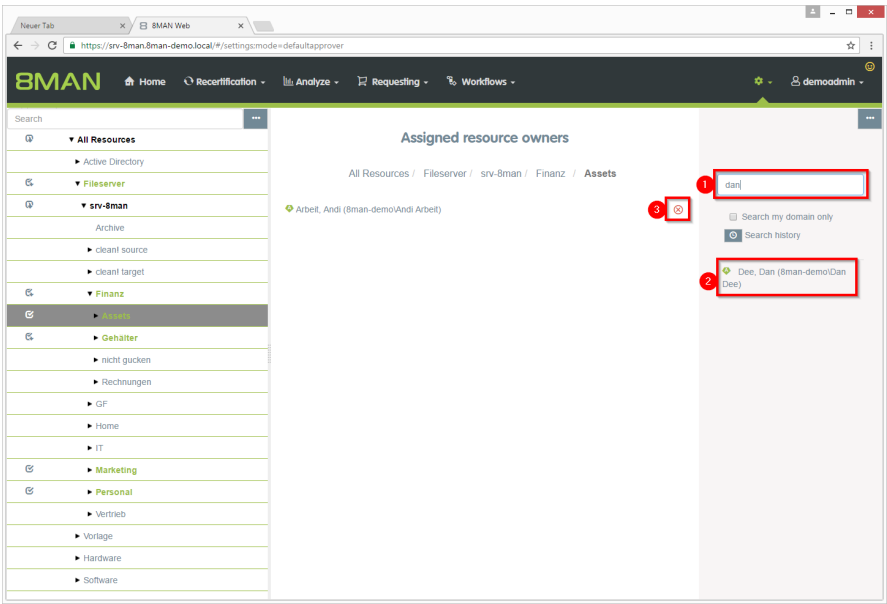
*Login to the web interface with admin credentials.*



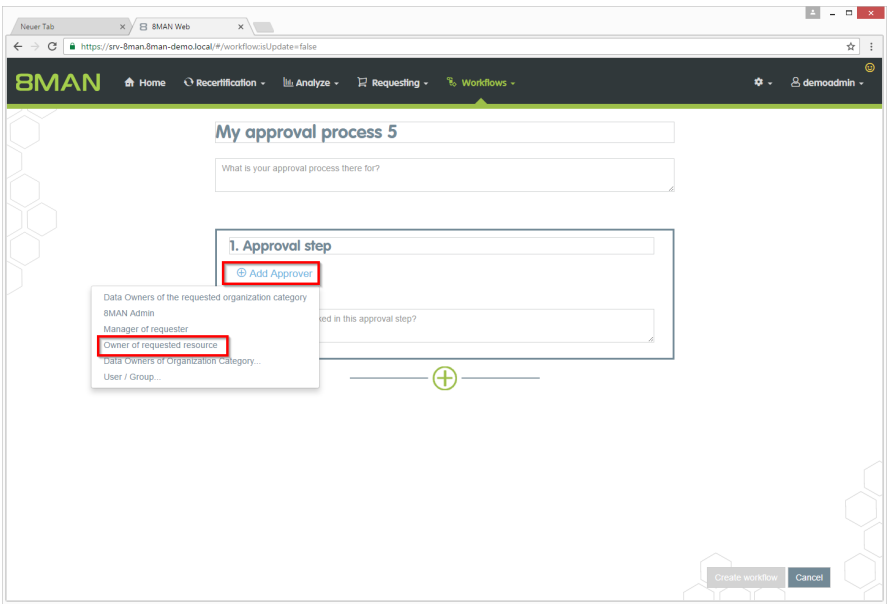
1. Click the gear-wheel.
2. Select "Resource owners".



1. Search for resources or alternatively navigate through the tree.
2. Gray text color indicates that no resource owner is assigned to the directory.
3. Green text color indicates an existing assignment.
4. The icons indicate assignments and assignments in subdirectories.



1. Find an user or a group.
2. Click a search result to set an assignment.
3. Delete an existing assignment.



Design individual workflows  
with the new role resource owner as an approver.



## 7.3 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.

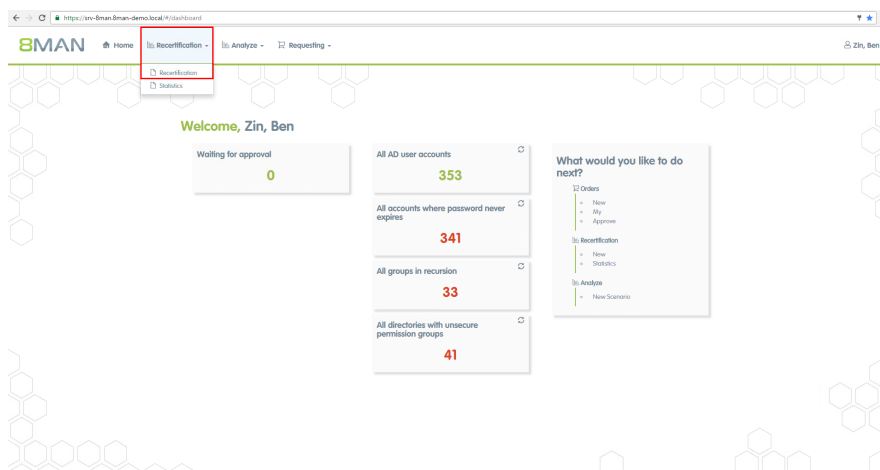
You receive an email with the instructions to the re-certification process. Then you decide for each user and resource if the access right should stay or be removed.

**Your desired changes will be transferred automatically to the administrator.**

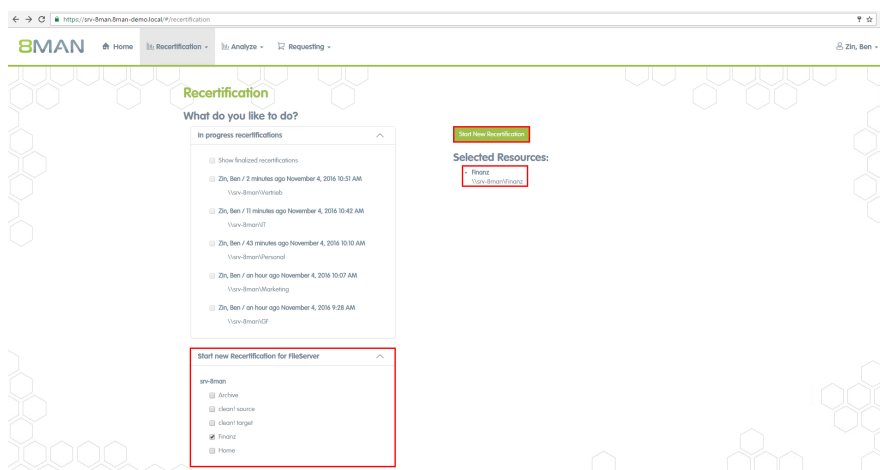
### Complementary Services

[Change file server access rights](#)

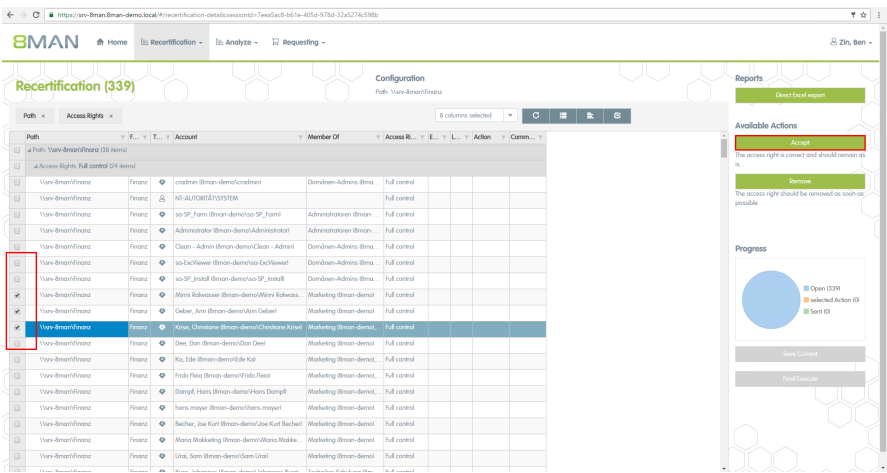
### The process in single steps



Click "Recertification".

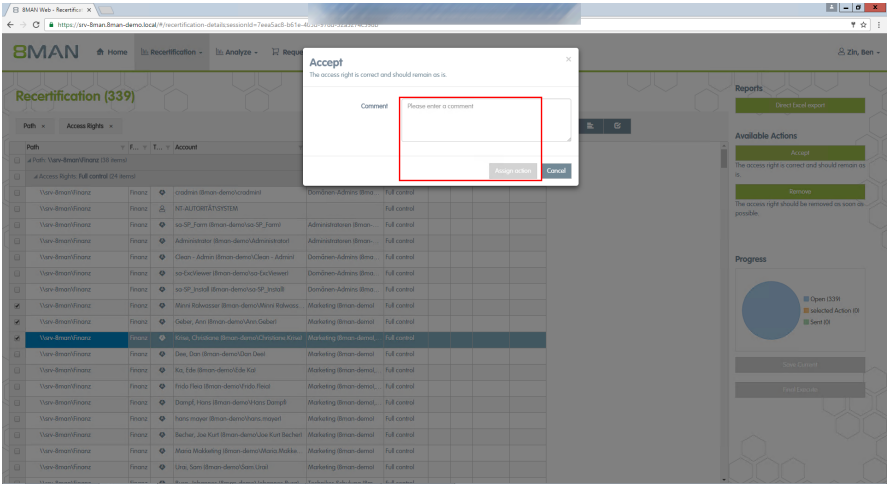


Click on "Start new Recertification". Click on one or more directories. The directories selected are shown on the right. Click on "Start new recertification".

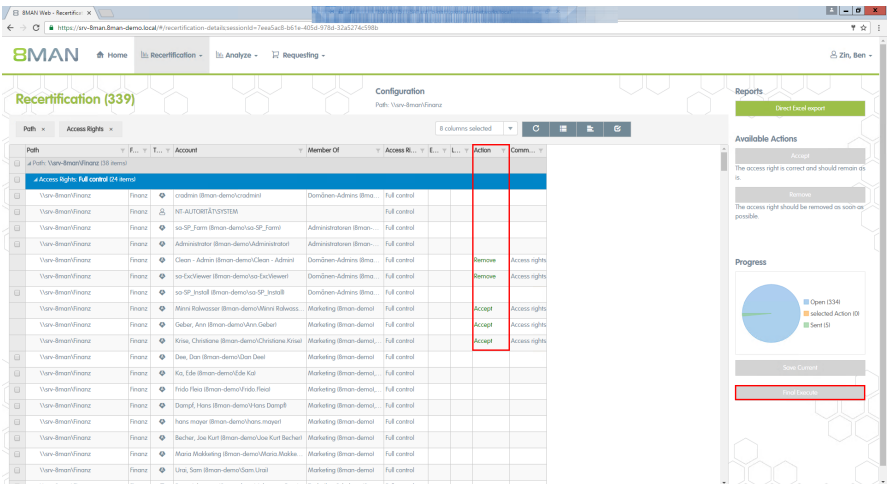


You can either accept or remove the permissions. Activate all Users which should keep their permissions first. Click on "Accept".

Subdirectories are only displayed, if they contain deviating permissions.




Please fill in a comment. Your notes will be saved in the system for documentation.



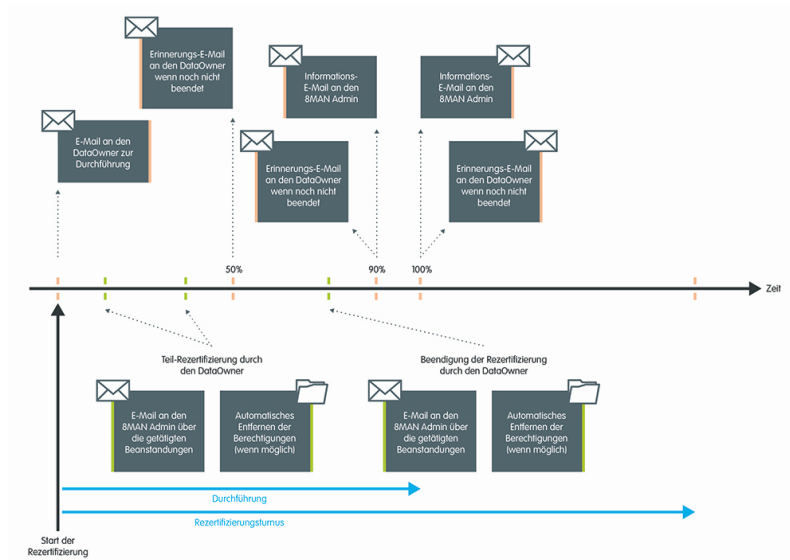
Do the same for the permissions you want to remove. Your decision is marked in the column "action". Click on "Final Execute". The Administrator gets a list of your decisions for implementation.

Temporary permissions of user accounts, which are also authorized with a permission that never expires, will become ineffective and not be shown in the marked column above.

 If you click on "Final execute" your administrator receives almost every time an email with your desired changes. This is why we recommend to do the recertification in one go.



### 7.3.1 E-mail notifications for recertification



*8MAN sends you an automatic reminder when the recertification is complete.*



**If you don't finish the recertification within the period, 8MAN stops the process and you and your administrator receive an email about the missing execution.**

## 7.4 +8MATE GrantMA workflows for employees

By using the 8MATE GrantMA self-service portal, employees are able to request access to individual resources in your organization. The next few pages contain examples of some some common workflows.

### Service overview

[Requesting file server access rights from Data Owners](#)

Initiating an order through procurement (Open Order)

[HR requests a user account creation from help desk](#)

### 7.4.1 Manage my requests (cockpit)

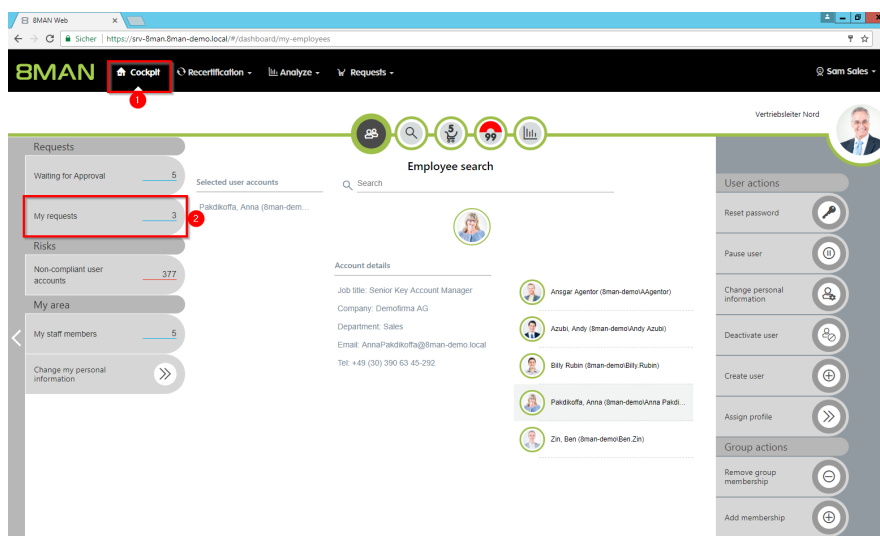
#### Background / Value

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

#### Additional Services

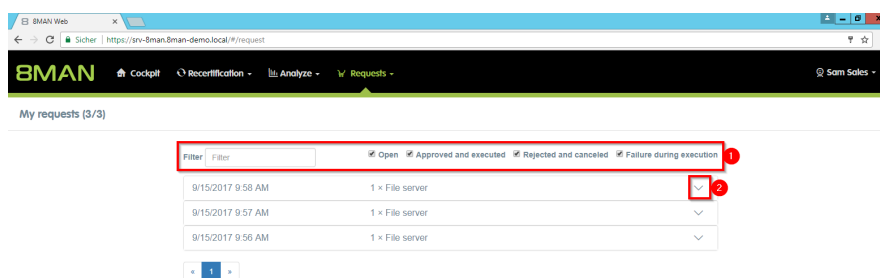
Overview of all cockpit services

#### Step by step process

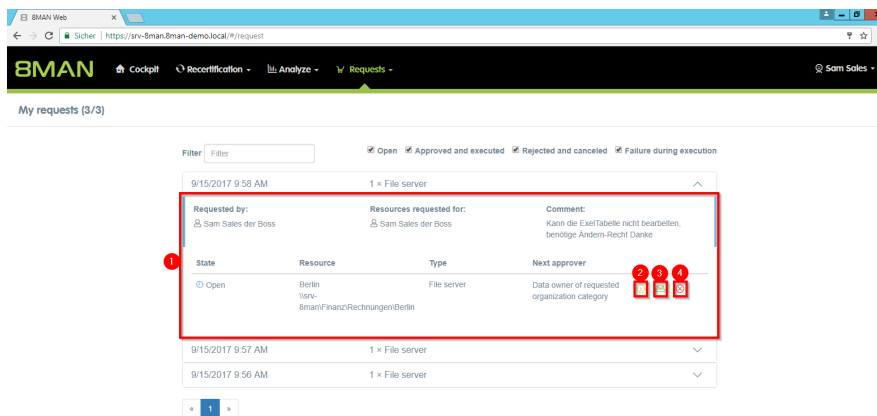


1. Select Cockpit.
2. Click "My Requests". In the example, Sam Sales has "3" requests.

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 order.



1. 8MAN 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.

## 7.4.2 Request file server access rights

### Background / Value

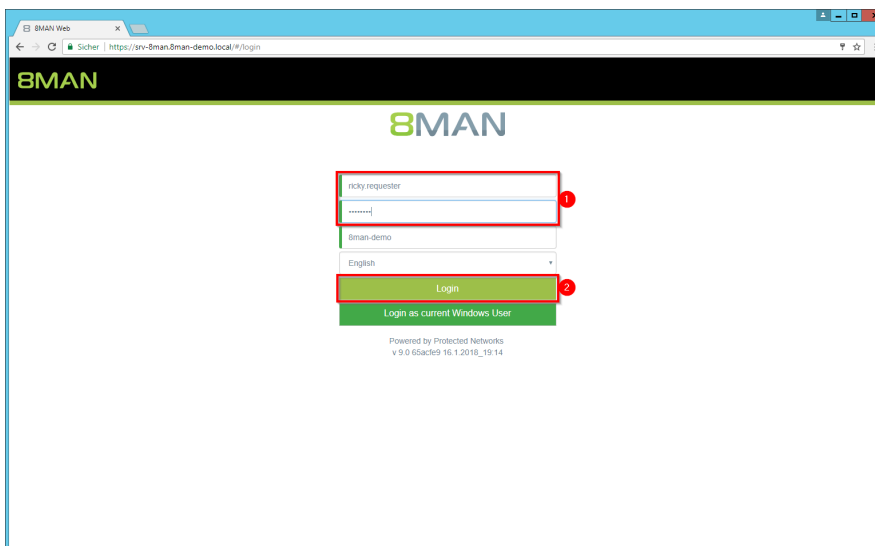
Employees can request access rights to file server directories from Data Owners by using the 8MATE GrantMA self-service portal.

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

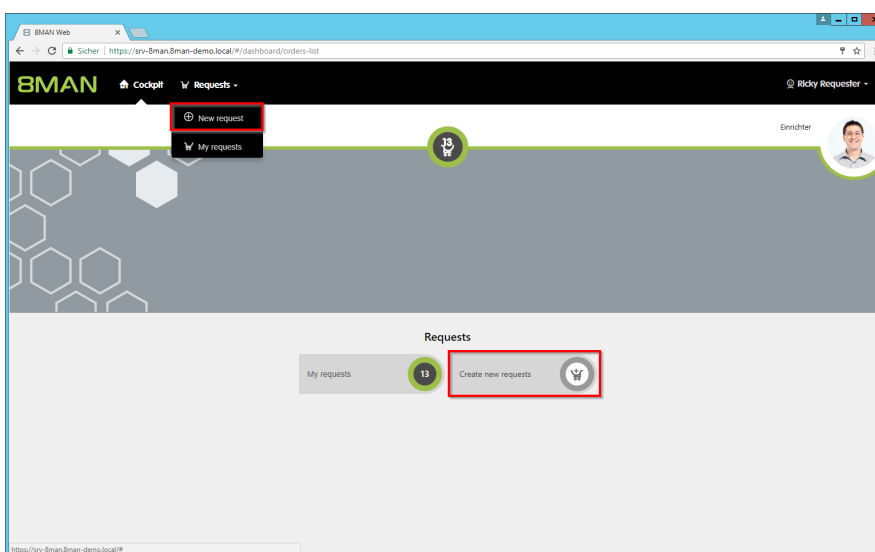
### Additional Services

[Creating approval workflows](#) (Administrator)

### Step by step process

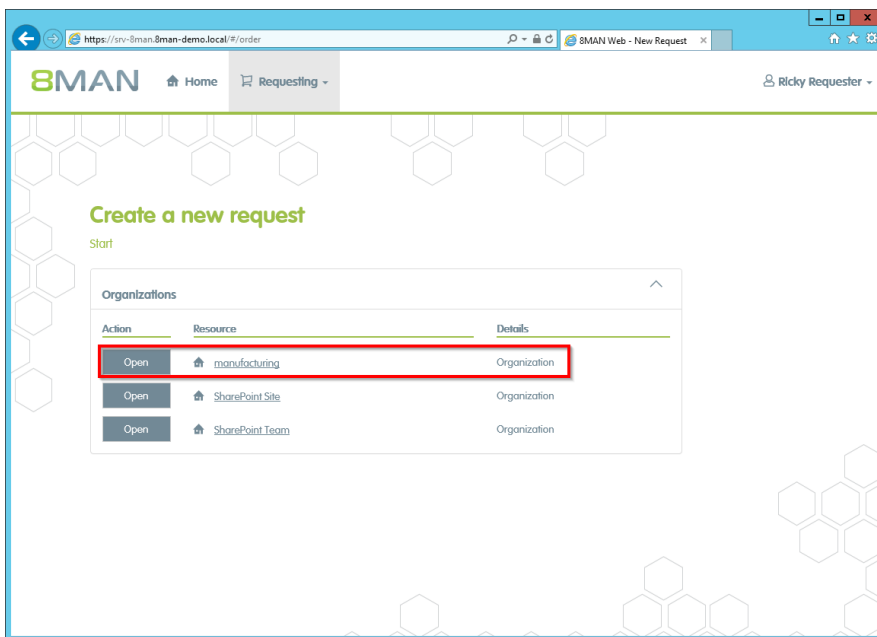


1. Enter your username and password.
2. Click "Login".



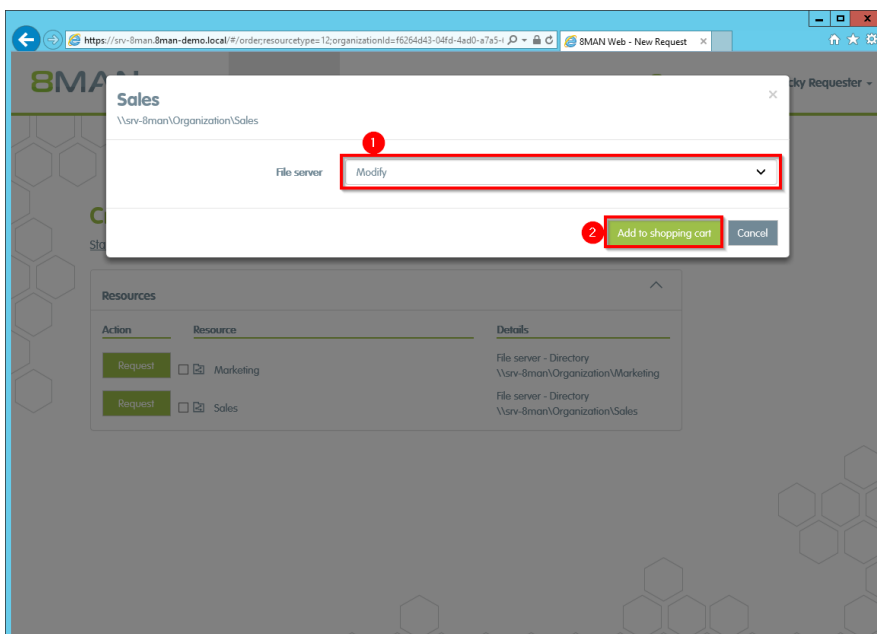
Click "New Request".





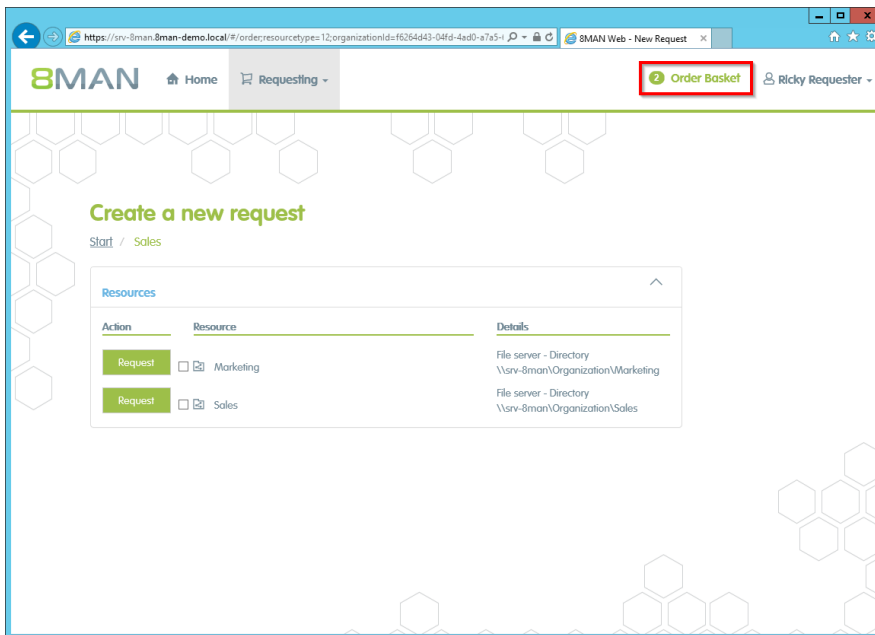
8MAN shows you as the applicant exactly the resources that can be ordered.

Select the desired resource and click on "order".



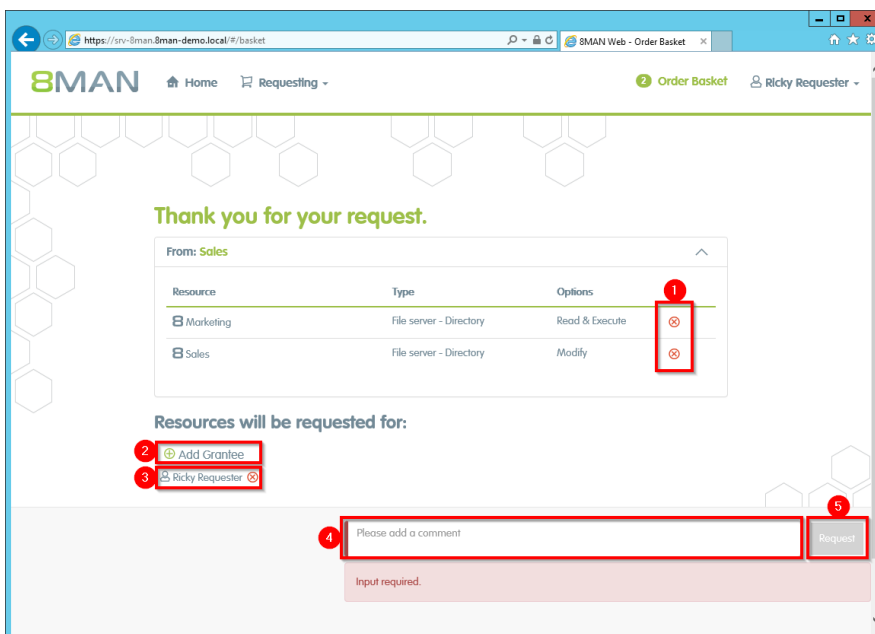
1. Select an access category.

2. Click "add to shopping cart".

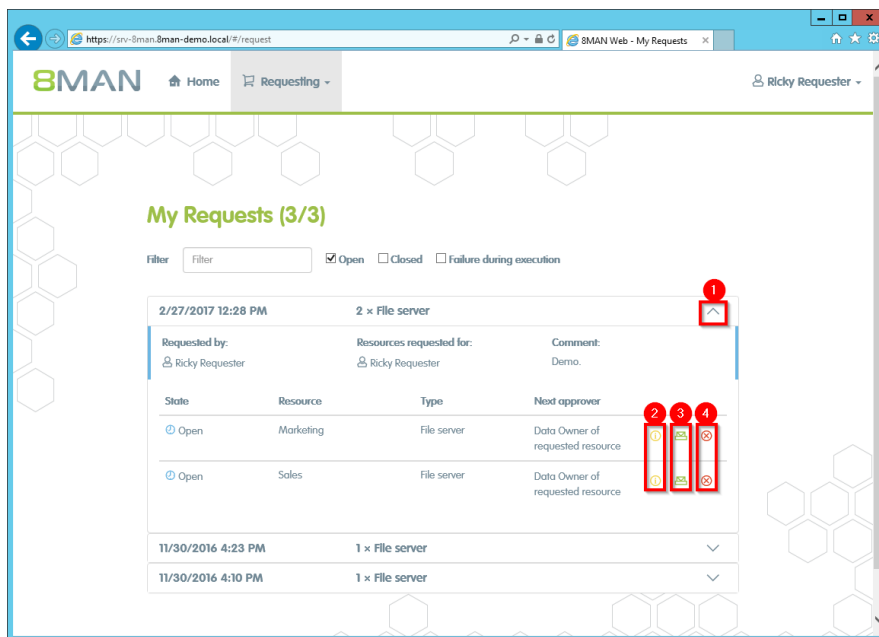


Add additional resources if desired.

Click on "Order Basket".



1. Delete the order entries.
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.
5. Start the request.



Once confirmed, 8MAN shows you an overview of your requests.

1. Open or close the detail view of an order.
2. You can see more details.
3. Resend a notification email to the approver.
4. Cancel your order.

### 7.4.3 Request group memberships

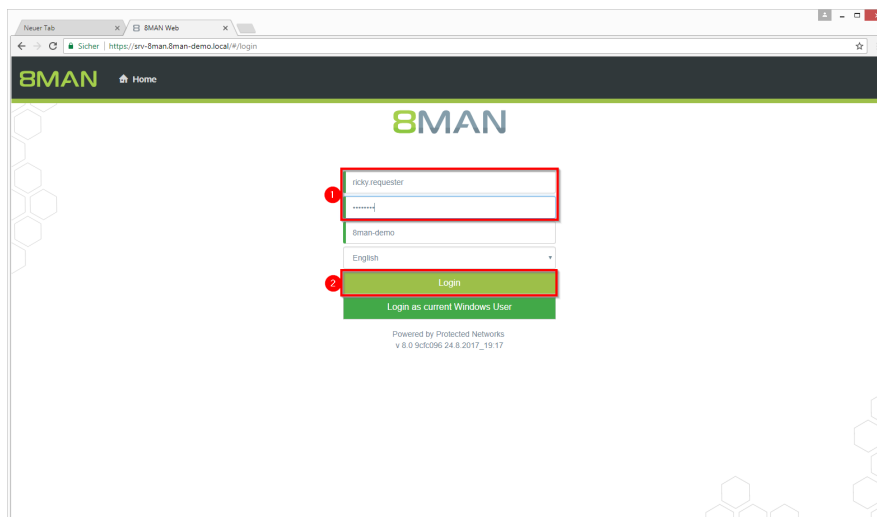
#### Background / Value

Employees can request group memberships by using the 8MATE GrantMA self-service portal. You can configure a variety of approval workflows and involve the relevant decision makers, depending on your security requirements.

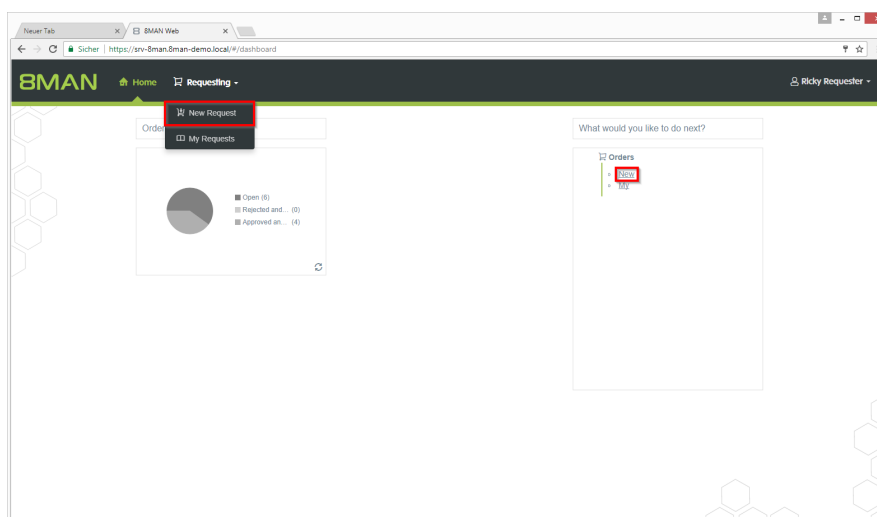
#### Additional Services

[Create approval workflows](#) (administrator)

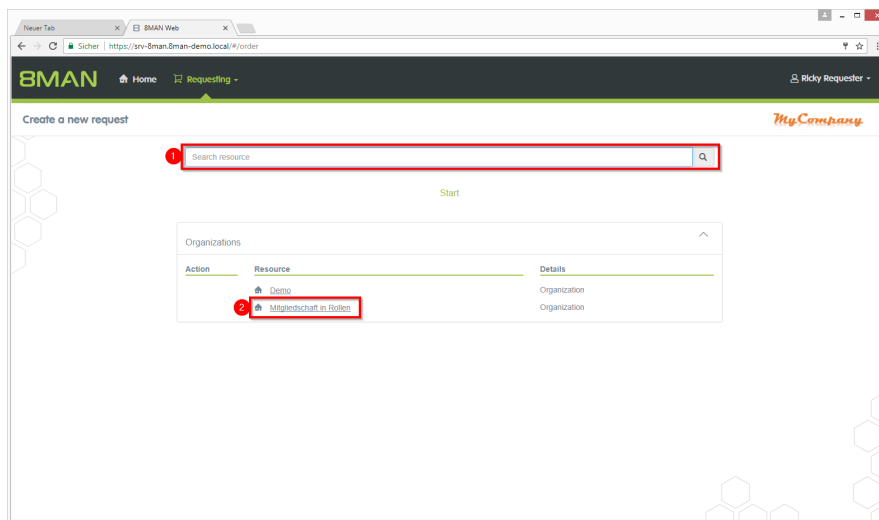
#### Step by step process



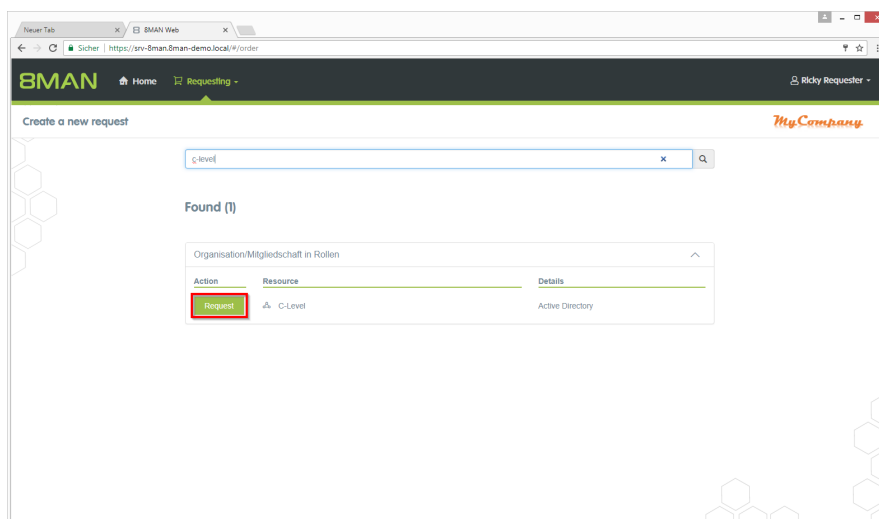
1. Enter your username and password.
2. Click on "Login".



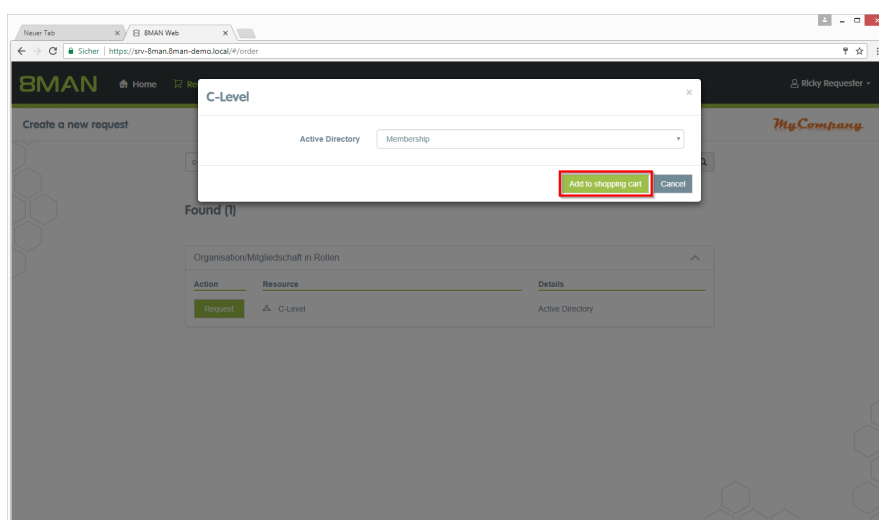
Click "New Request".



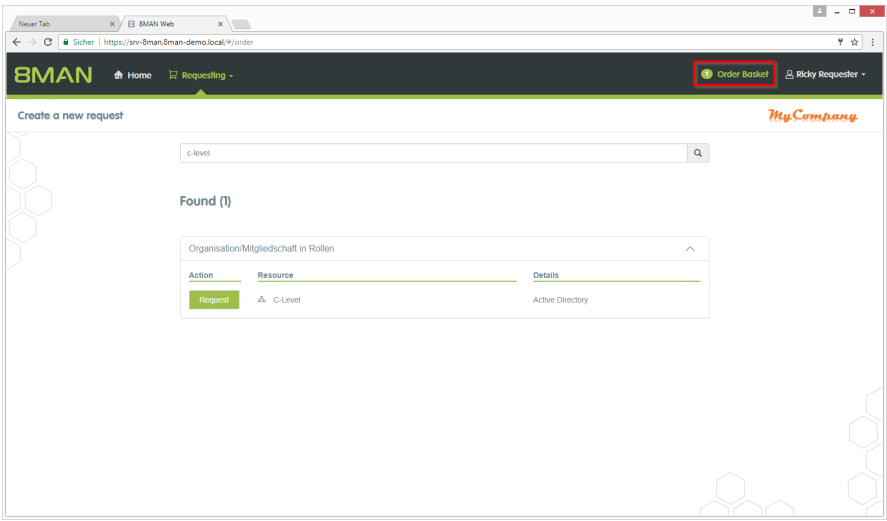
1. Search for the group or
2. navigate to the desired level.



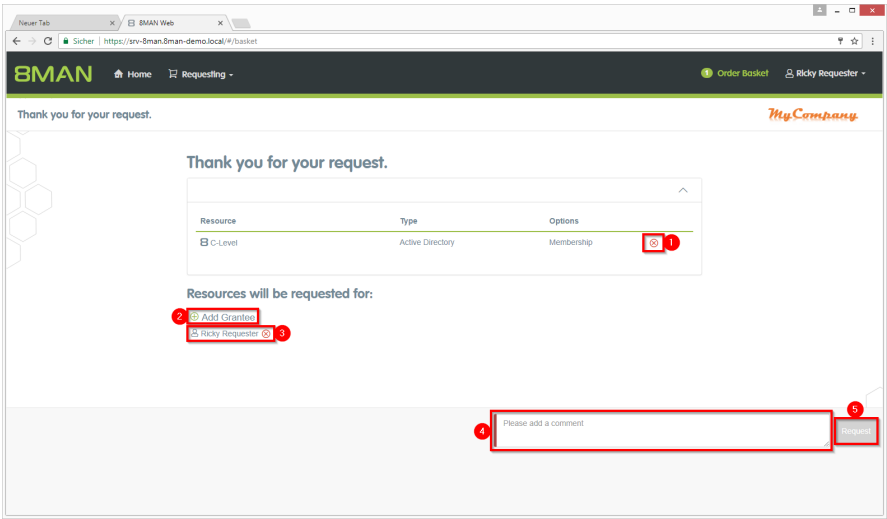
Once you have found the desired resource, click "Request".



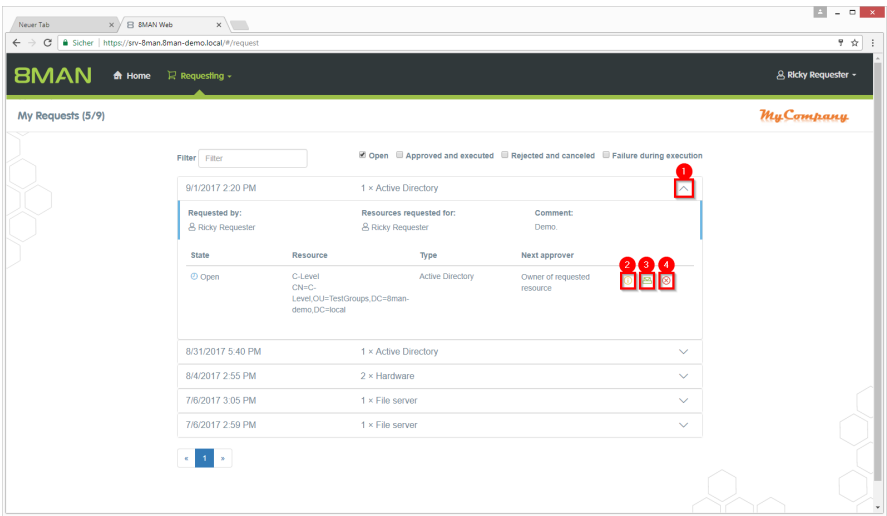
Click "Add to shopping cart".



If necessary, add additional resources to your request. Click on "Order Basket".



1. If necessary, delete items from your purchase order.
2. Add recipients to your request. You can order 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, 8MAN 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.

## 7.4.4 Request new directories

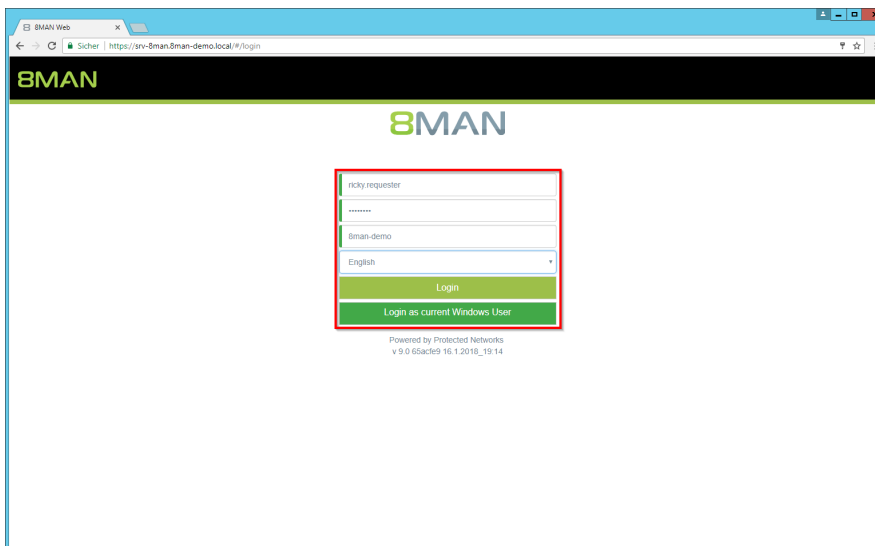
### Background / Value

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. Find resources quickly with the search.

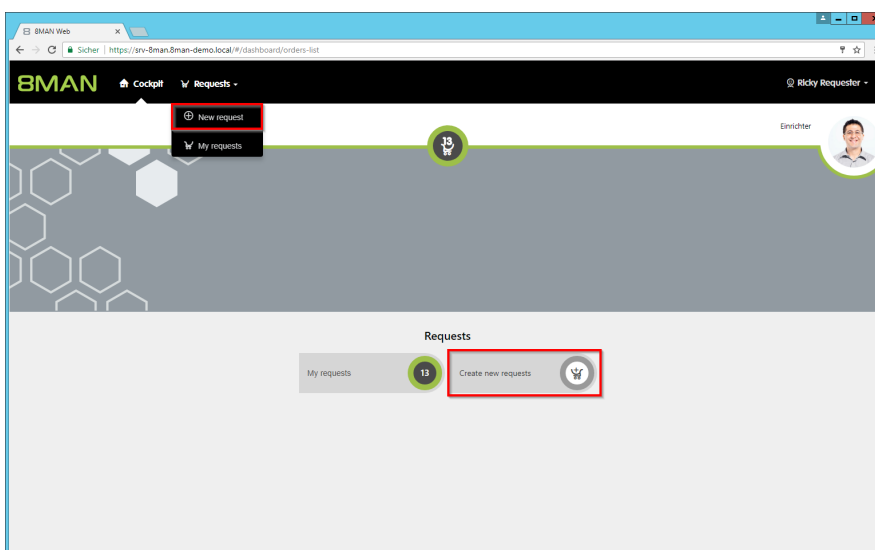
### Additional Services

[Request file server permissions](#)

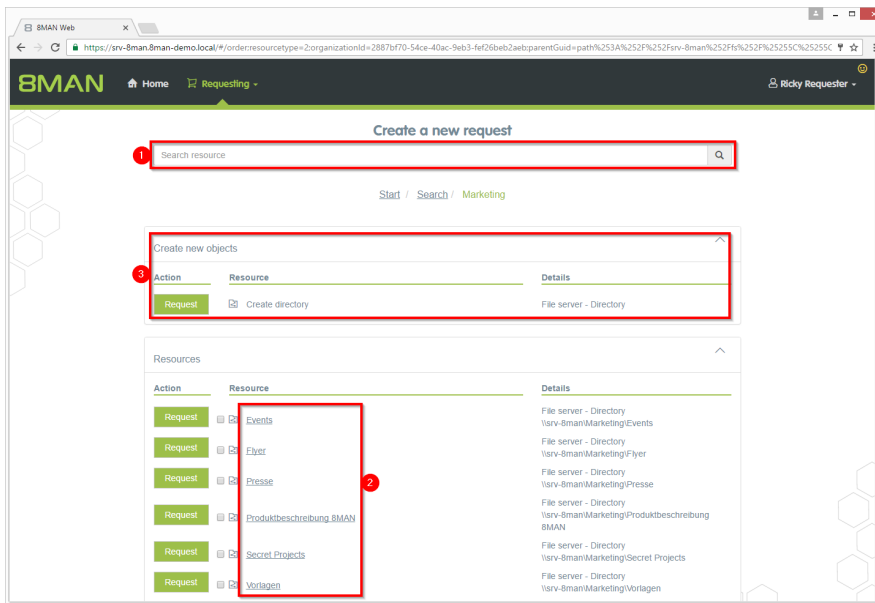
### Step by step process



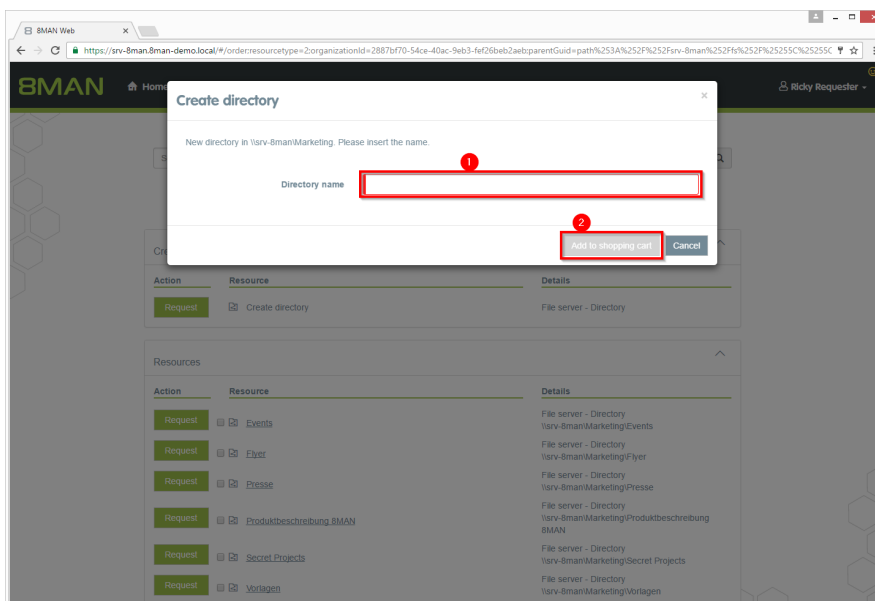
*Log in as the requester.*



*Start a new request.*

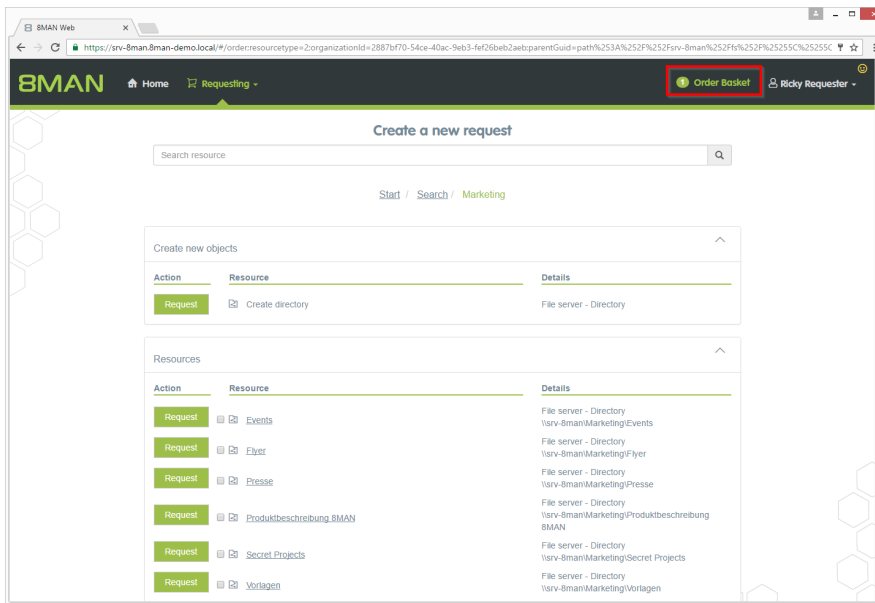


1. Find the desired resource.
2. Alternatively: Navigate to the desired resource.
3. Click "Request" in the "Create new objects" area.

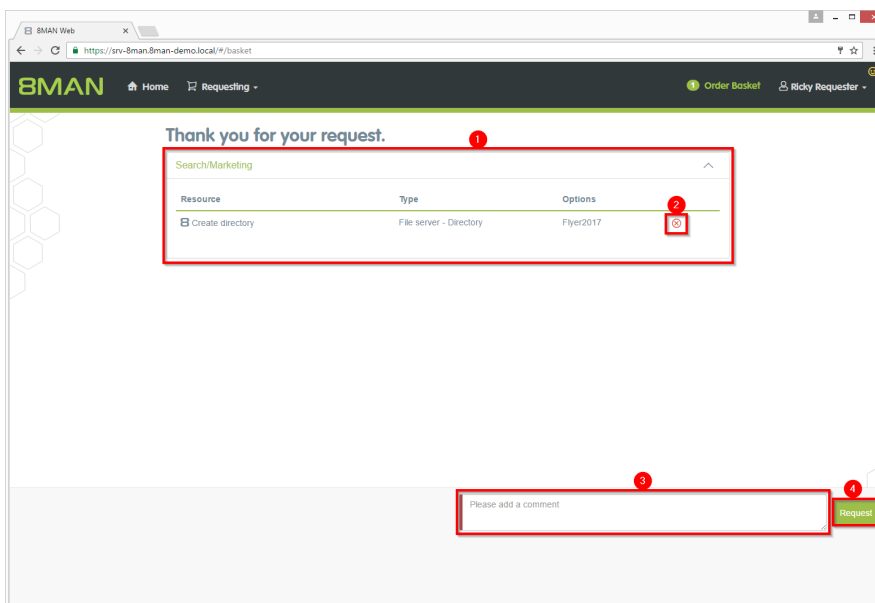


1. Give the new directory a name.
2. Place the order in the shopping cart.





Click the shopping cart.



1. 8MAN will show you the order basket with your requests.
2. Alternatively, delete your request.
3. You must enter a comment, e.g. a ticket number.
4. Close your request.

### 7.4.5 Create a user account as an HR employee

#### Background / Value

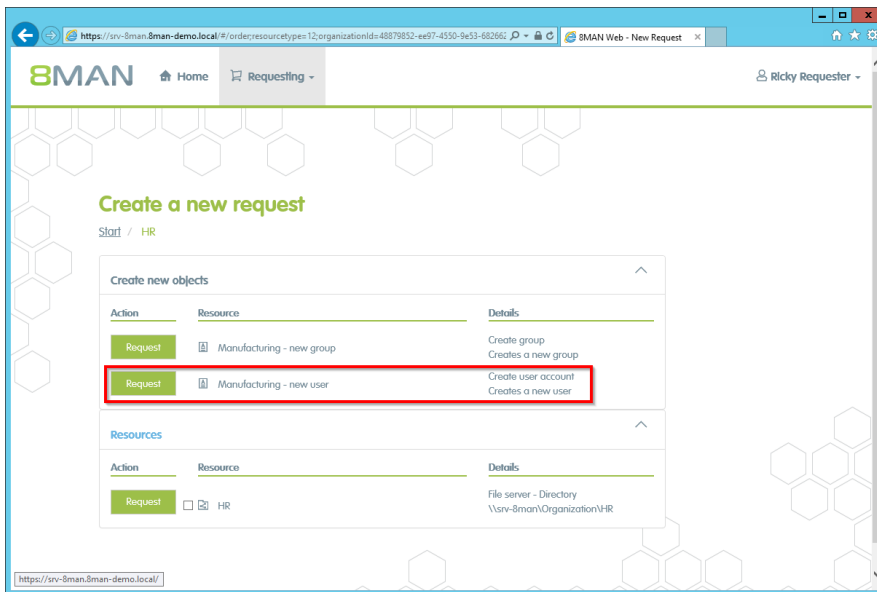
The 8MATE GrantMA self-service portal allows HR employees to create user accounts for new employees. Instead of sending user information to IT, the entry and creation of a new user account are combined into one simple step. IT simply has to approve the request.

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

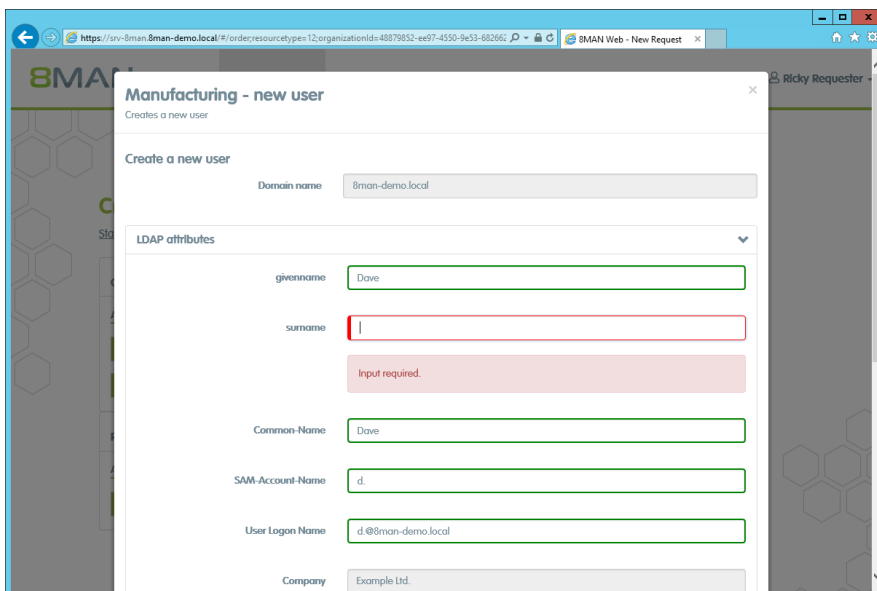
#### Step by step process

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.

8MAN Web - New Request

SAM-Account-Name: d.demo

User Logon Name: d.demo@8man-demo.local

Company: Example Ltd.

Manager: CN=Adrian Stillwell,OU=TestUsers,DC=8man-demo,DC=local

Pers.Nr.:

Location: Berlin

Beschreibung: This is an automatically generated description for 'Dave Demo' with the

Password options

Add to shopping cart Cancel

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

8MAN Home Requesting - Order Basket

Create a new request

Start / HR

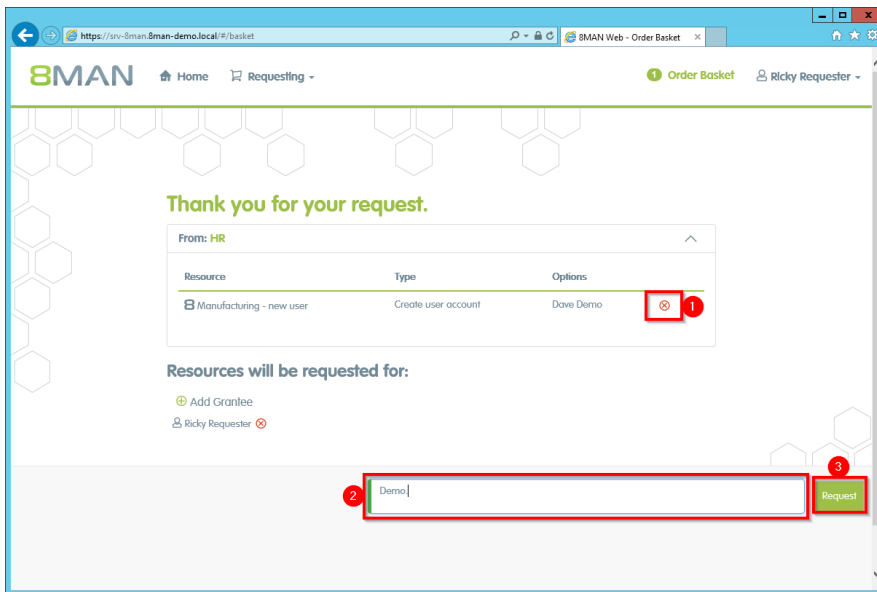
Create new objects

Action	Resource	Details
Request	Manufacturing - new group	Create group Creates a new group
Request	Manufacturing - new user	Create user account Creates a new user

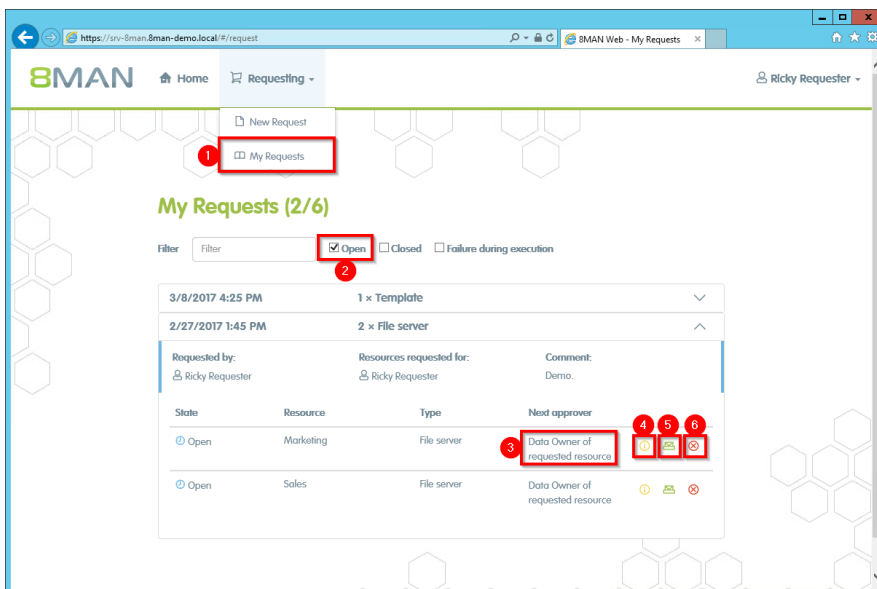
Resources

Action	Resource	Details
Request	HR	File server - Directory \\srv-8man\Organization\HR

Add additional resources if desired. Click on "Order Basket".



1. You can delete an order entry.
2. You must enter a comment.
3. Start the order.



1. Select "My Requests" to view all requests.
2. Filter by "Open".
3. You can see which approvals are next in line.
4. View additional details.
5. Resend a notification email to the approver.
6. Cancel your order.

## 7.4.6 Order script-based services

### Background / Value

In addition to ordering user accounts, authorizations, directories or freely definable objects (OpenOrder), other script-based services can now 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 workflow, the script is started automatically.

### Additional Services

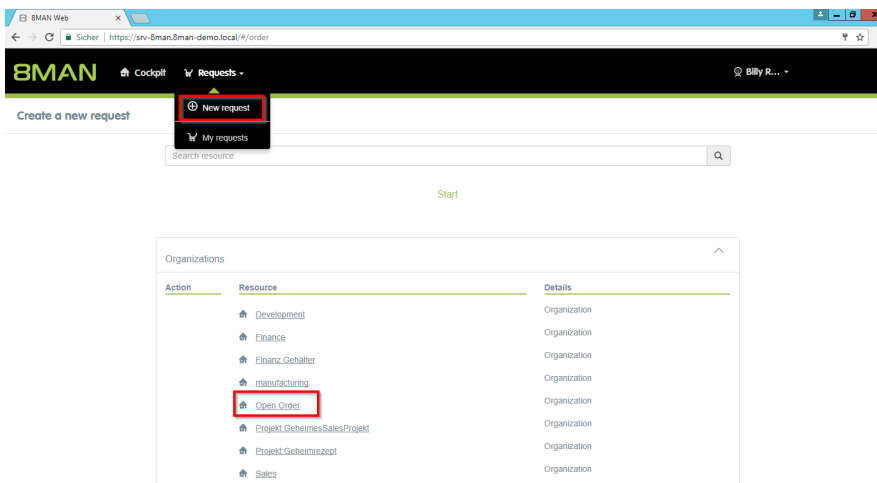
[Configure a script-based service for requesting \(Administrator\)](#)

### Step by step process

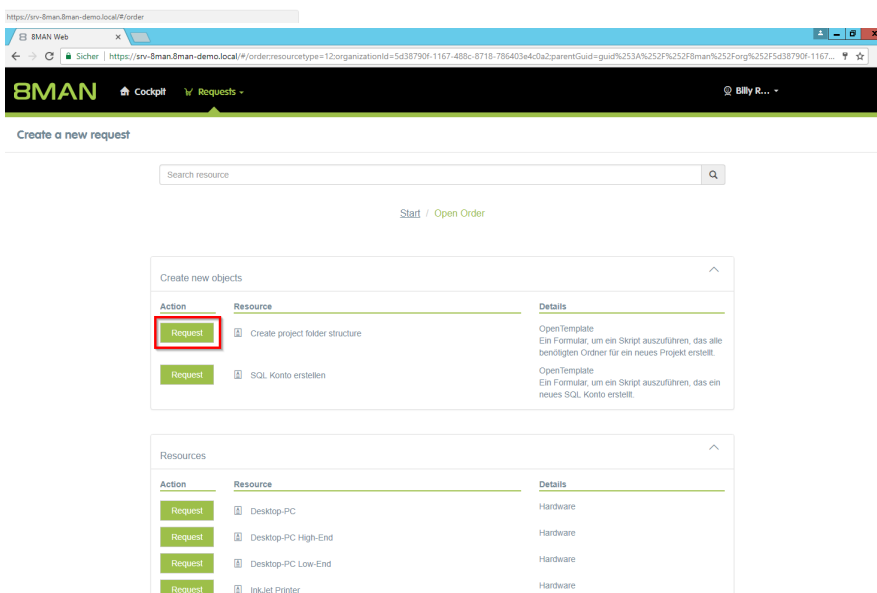


*The following example, a user requests a project folder structure.*

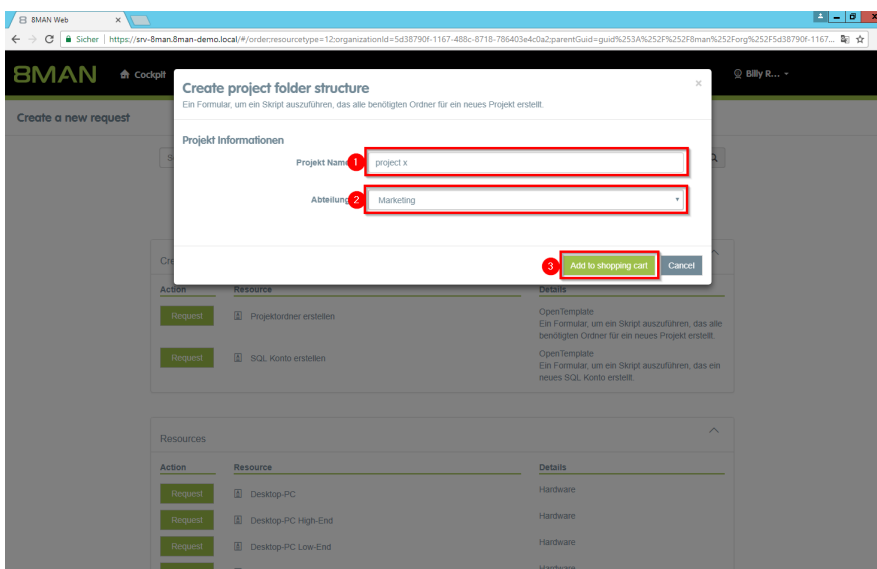
*Log in as a requester in the web client.*



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

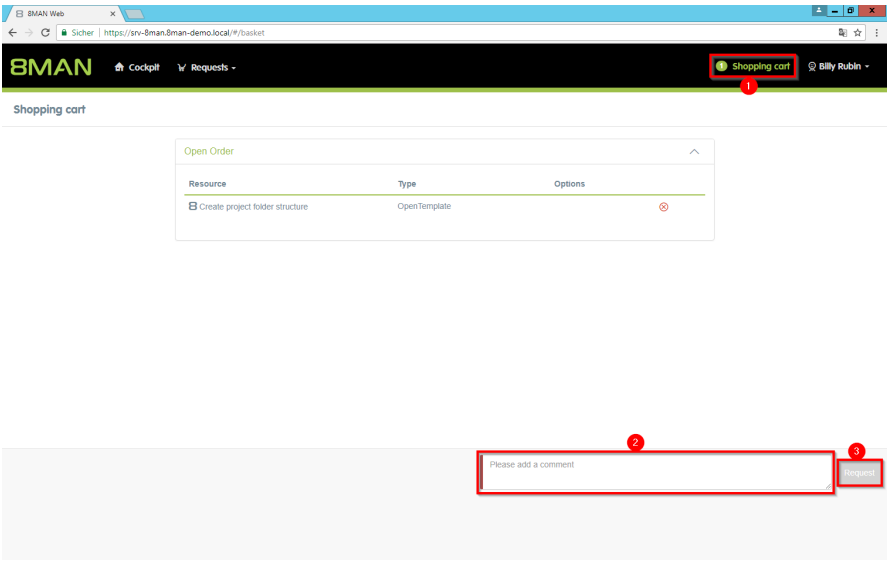


Select the service "Create project folder" and click on "Request".

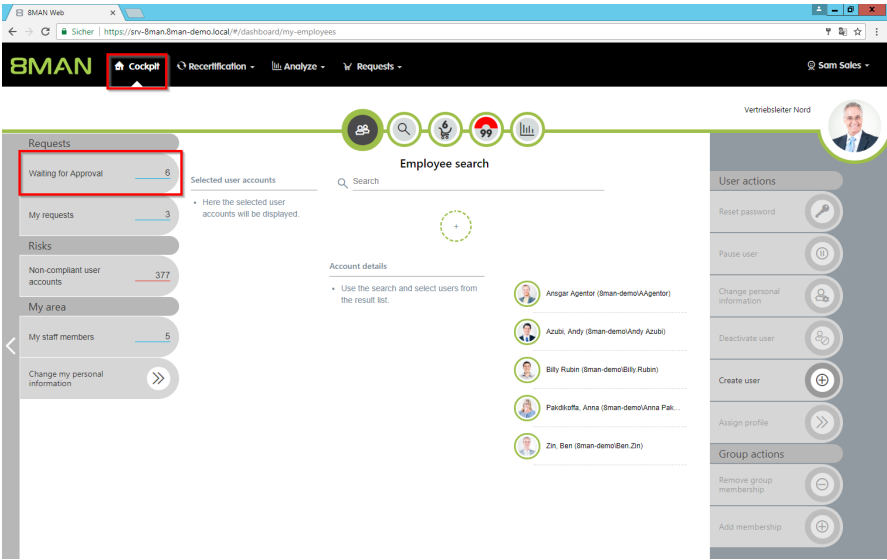


Enter the parameters for the script. In the example:

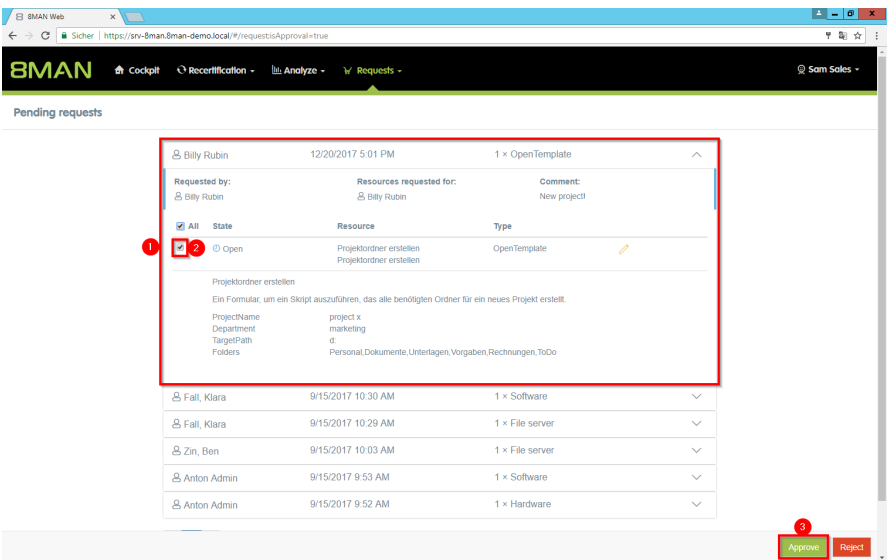
1. Assign a name to the project folder.
2. Choose a department. In the example, the "parent folder" under which the project structure is created.
3. Click on "Add to cart".



- Complete the order:
1. Click on "Shopping cart".
  2. Enter a comment.
  3. Click on "Apply".

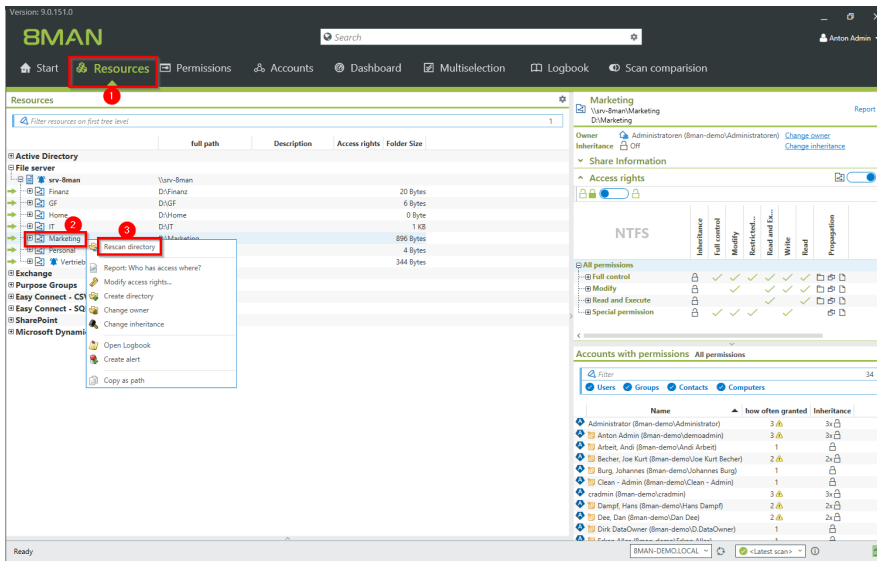


- In the example chosen here, the request must be approved by Sam Sales.
- Log in as approver.
- Click "Waiting for Approval."



1. Expand the previously created request.
2. Activate the checkbox.
3. Click "Approve".





The folder structure is generated by script "outside" of 8MAN. In order for the new folders to be visible, the corresponding directory must be rescanned.

## 7.5 +8MATE GrantMA: workflows for data owner/administrators

### 7.5.1 Approve or reject requests (cockpit)

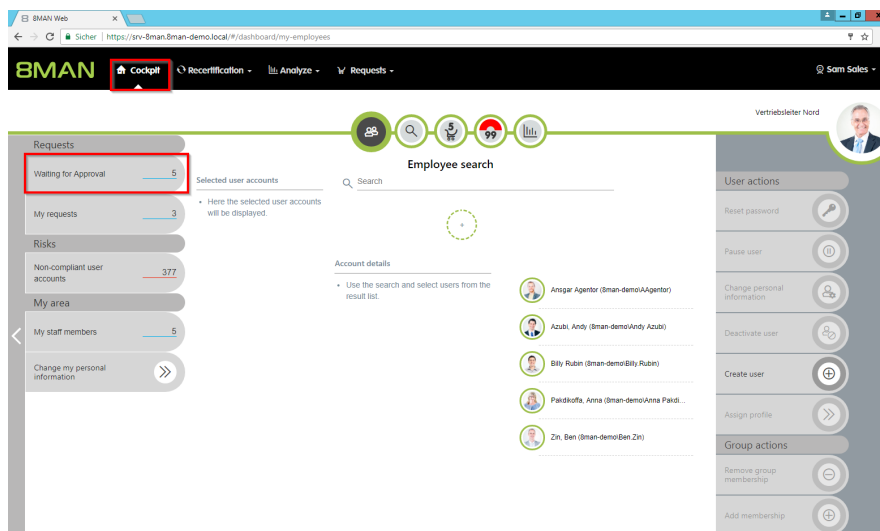
#### Background / Value

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.

#### Additional Services

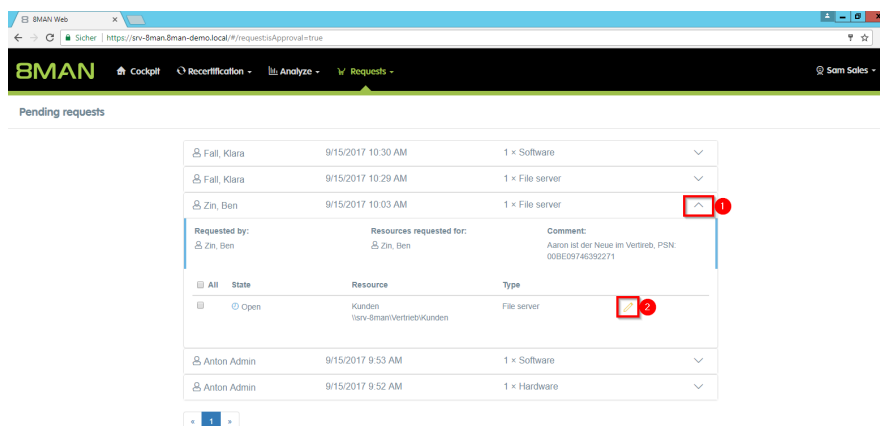
Overview of all cockpit services

#### Step by step process

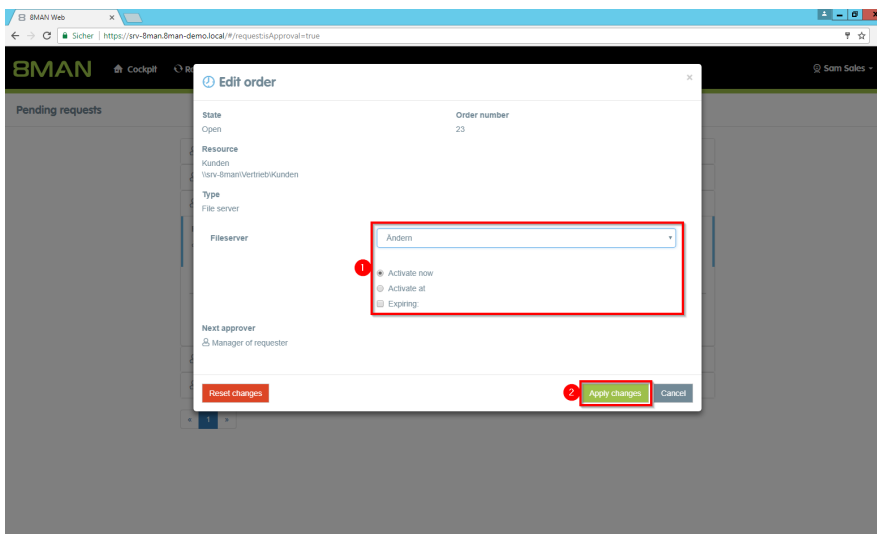


Click "Waiting for Approval." In the example shown, 5 requests are waiting for approval.

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

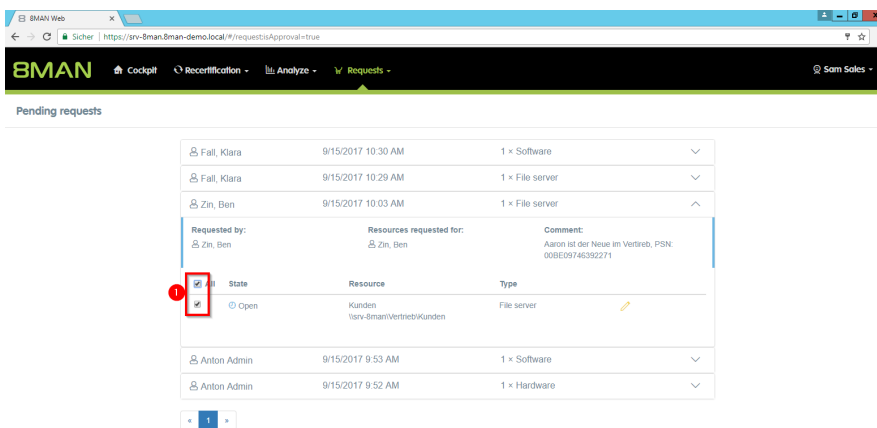


1. Expand an order to see the items.
2. Get details about the items. Depending on the configuration, you will see a pencil or information symbol.  
Pencil: You can customize the order.  
Info: You see the details. Click on the pencil icon.

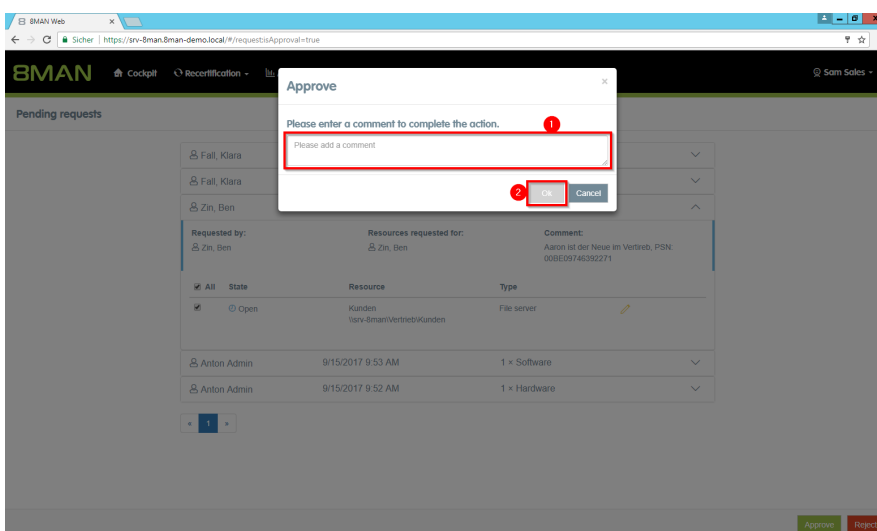
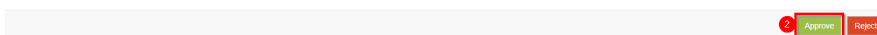


You can edit the order request.

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.

7.5.2 Informing approvers of new requests via email

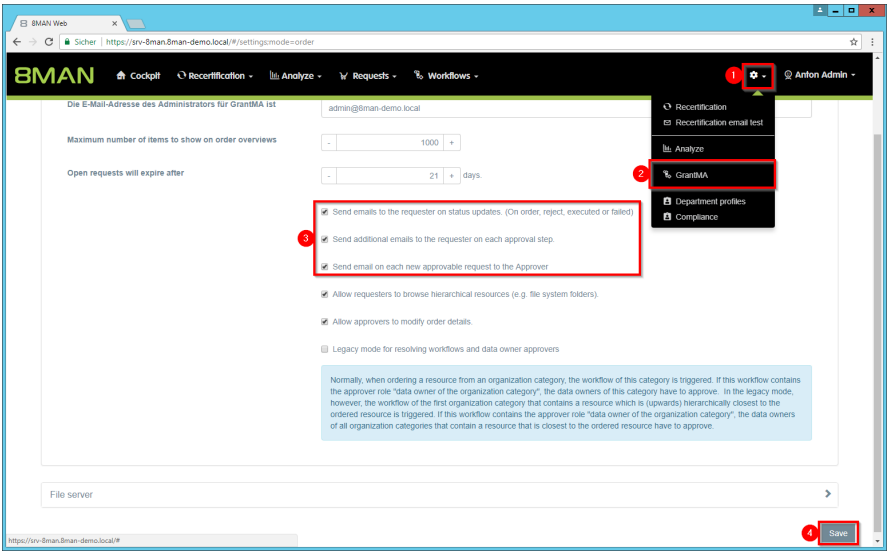
Background / Value

To prevent approvers from having to proactively check for open approval requests on the 8MAN home page, we recommend activating approval emails.

Additional services

[Creating / Changing approval processes](#)

Step by step process



Log into the web client as an 8MAN 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.

**Genehmigung erforderlich**

Sehr geehrte(r) cradmin,

**Rosi Ne** hat eine GrantMA Bestellung aufgegeben, die eine Genehmigung von Ihnen erfordert. Die Bestellung wurde am **15.11.2016** um **15:29** Uhr aufgegeben.

Auf der [8MATE GrantMA](#) Seite können Sie die Bestellung genehmigen oder ablehnen.

**Bestellübersicht**

Rosi Ne schrieb den folgenden Bestellkommentar:  
"Für Demozwecke."

Folgende Positionen wurden für

- **Rosi Ne**

bestellt:

Bestellnr.	Name	Typ	Optionen	Genehmigungshistorie
<a href="#">12</a>	IT	Fileserver	Ändern	

Mit freundlichen Grüßen  
8MATE GrantMA

Example of an email notification.

### 7.5.3 Approving or denying a request in the self service portal

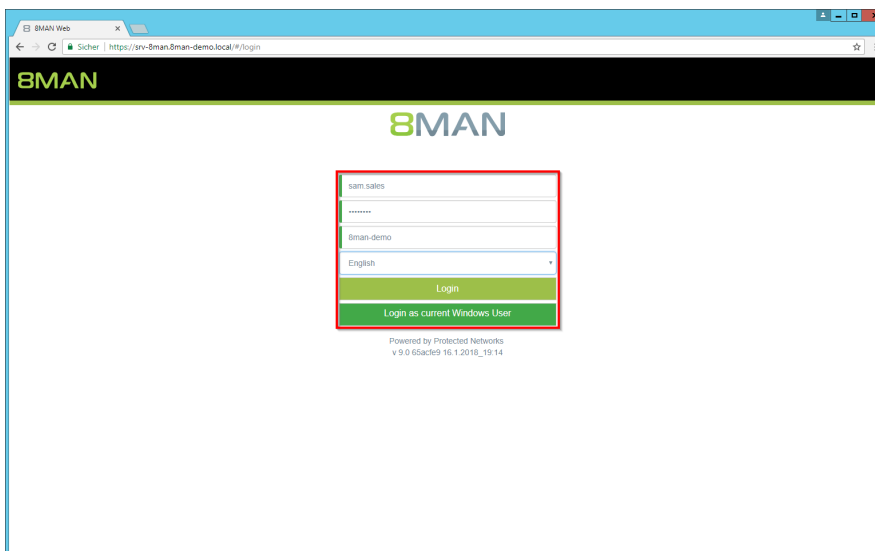
#### Background / Value

Depending on the chosen settings, you will receive approval requests for individual ordering processes. This allows administrators and data owners to stay in the loop.

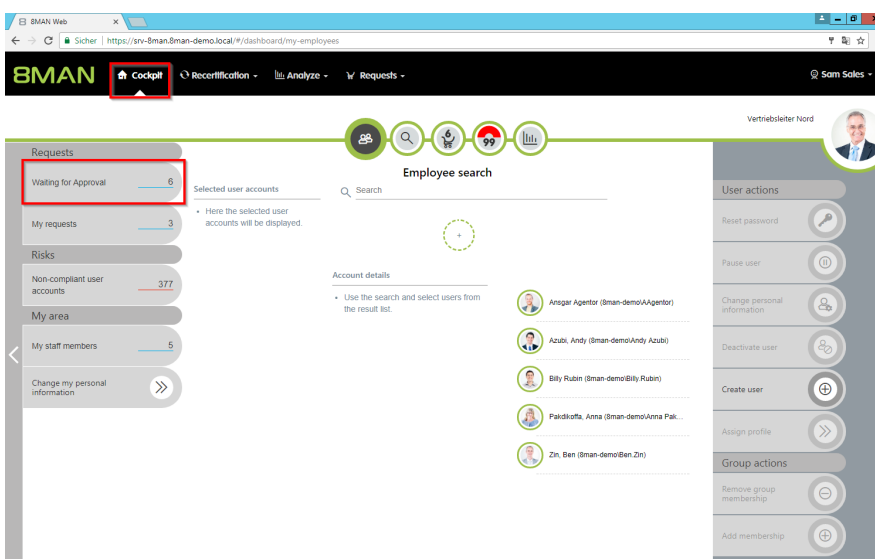
#### Additional Services

##### Defining individual approval workflows

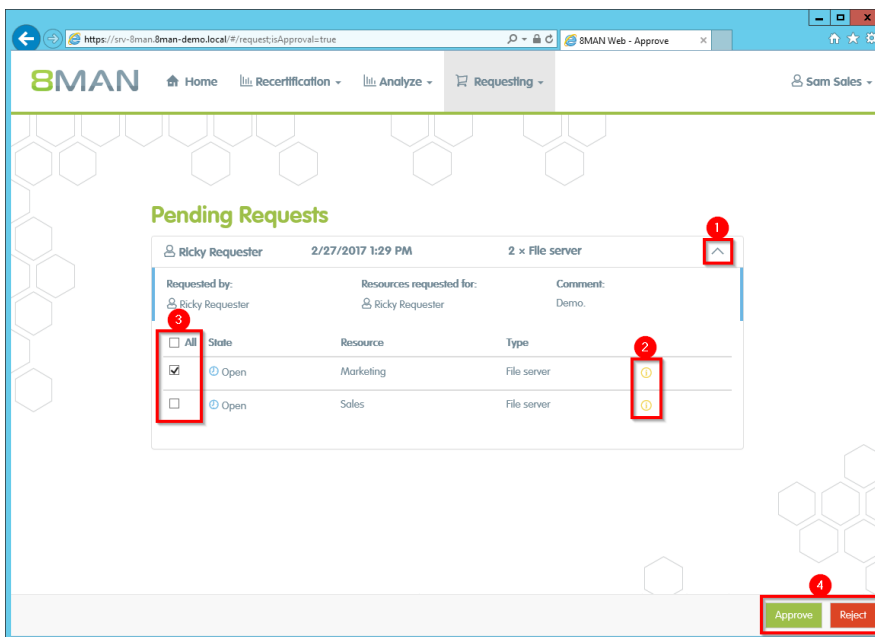
#### Step by step process



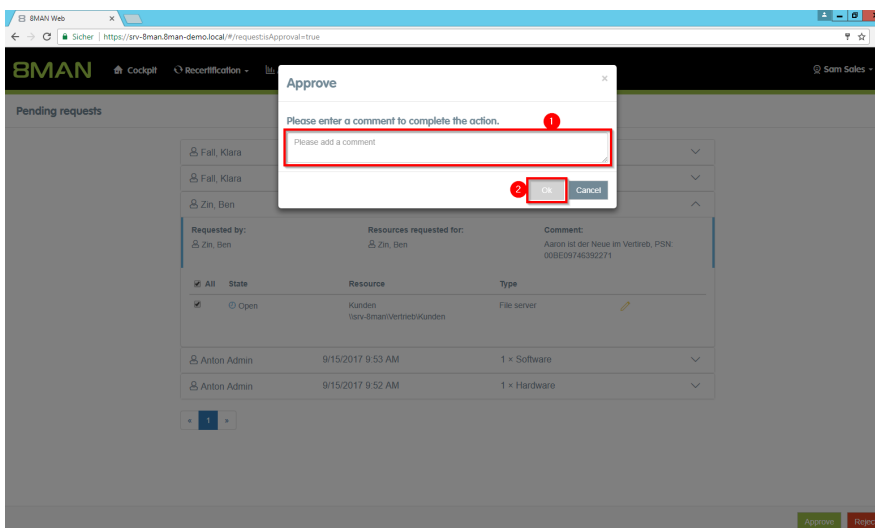
Log on with your approver credentials.



Click on "Waiting for Approval".  
In this example there are 6 requests waiting for approval.  
Click the tile.



1. Open a pending request to see the items.
2. View details of an item.
3. Select one or more items.
4. Click "Approve" or "Reject".



1. You must enter a comment.
2. Click on "OK".

The comment is stored in the logbook and ensures revision-proof documentation.



## 8. User Provisioning





## 8.1 Active Directory

### 8.1.1 Administrator

#### 8.1.1.1 Create an user account

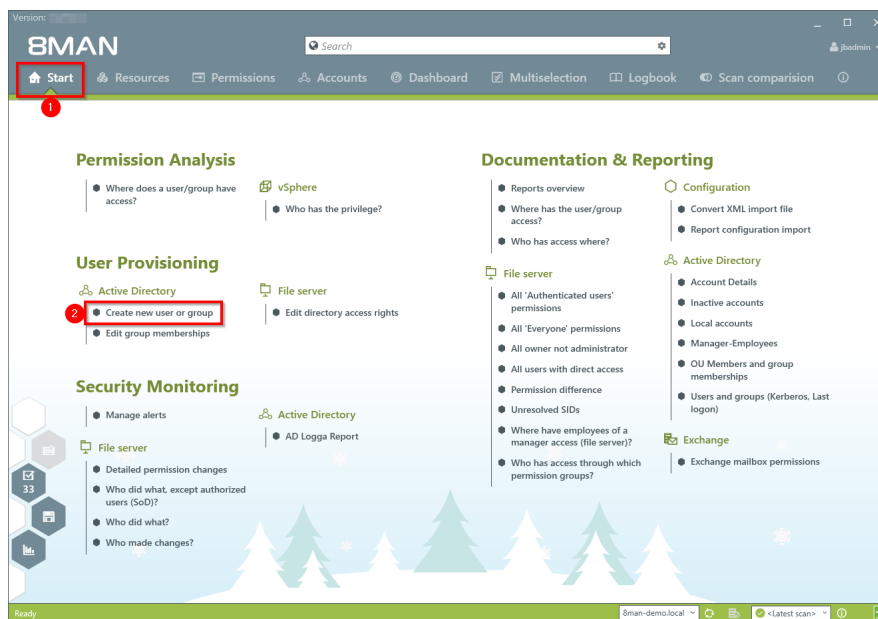
#### Background / Value

With 8MAN you can quickly create standardized user accounts. You can specify this process by creating the appropriate templates for different roles and then delegate it to your help desk.

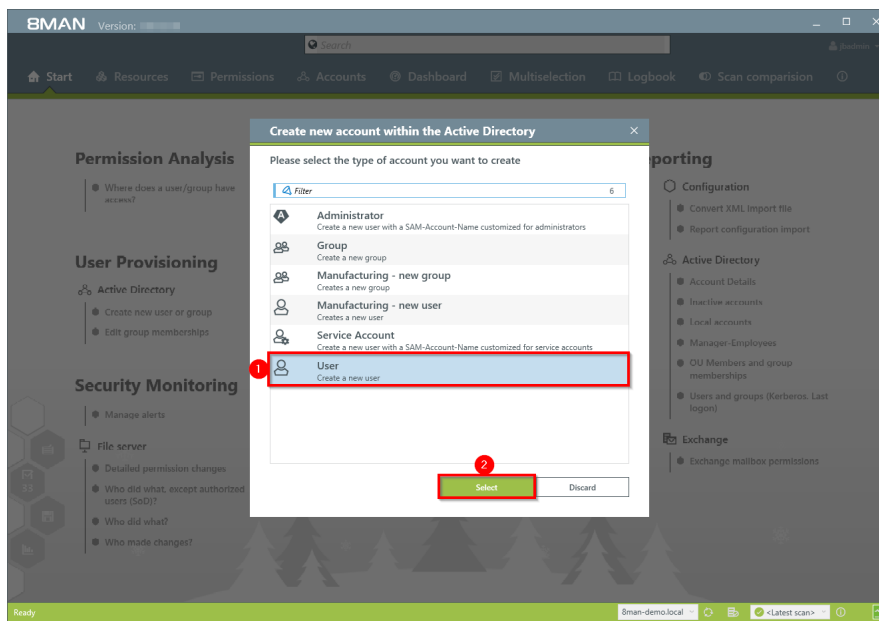
#### Additional Services

Customize templates for account creation (please refer: Templates Manual)

#### Step by step process

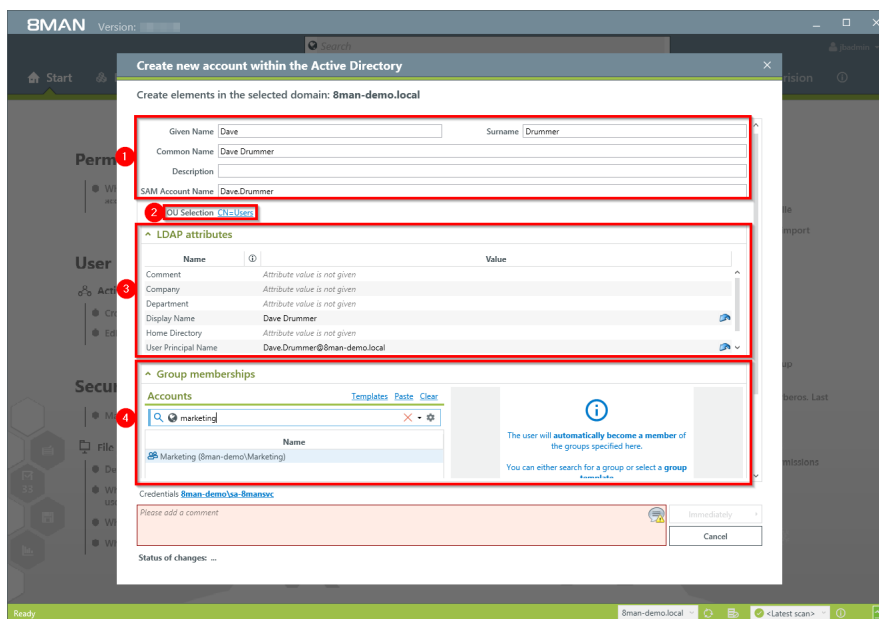


1. Click "Start".
2. Click "Create new user or group".

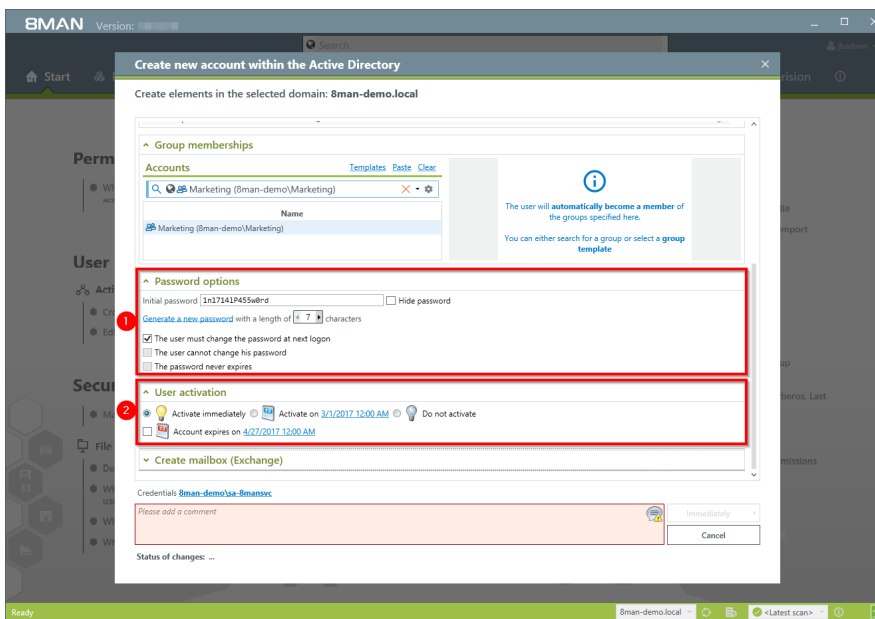


8MAN offers 4 standard templates. You can generate as many of your own templates as you wish. We recommend using templates as a foundation as this simplifies and speeds up the process.

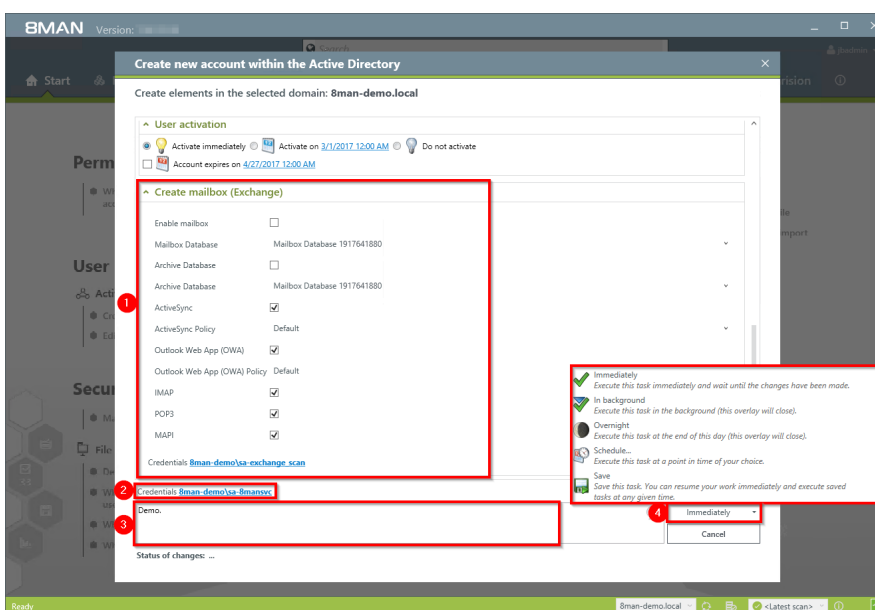
1. Select a User template.
2. Click on "select".



1. Enter the required information.
2. Modify the OU if desired.
3. Add any additional LDAP attributes.
4. You can designate group memberships while creating the user.



1. Determine your password options.
2. 8MAN allows you to decide when you want to activate or deactivate the account.



1. Determine the email settings. You are able to email activate it later, if you create the account without a mailbox.
2. Determine which credentials are used in order to create the new account in AD.
3. 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.**

4. Complete the action immediately or later, or save the job and complete it later.

### 8.1.1.2 Create groups and add users

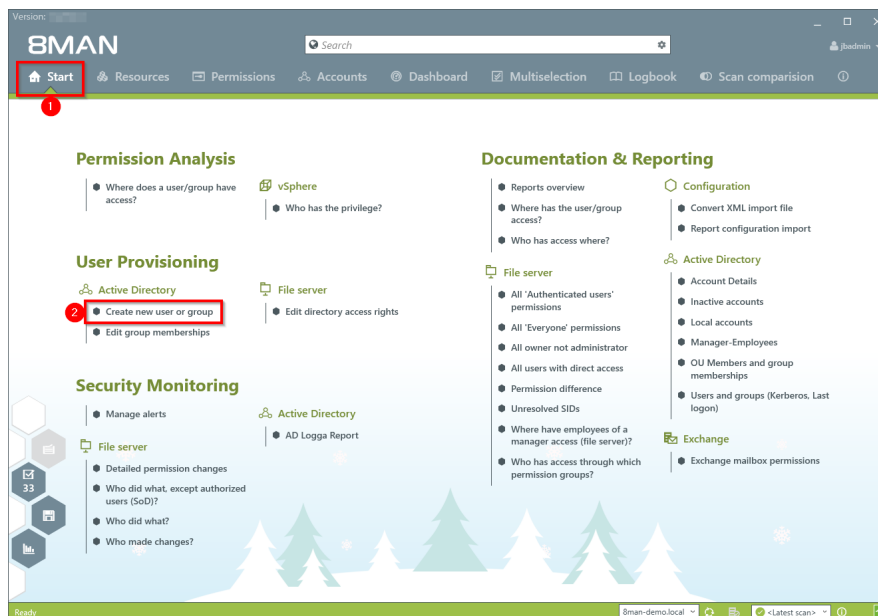
#### Background / Value

8MAN allows you to create standardized groups quickly and easily. Each process is automatically documented.

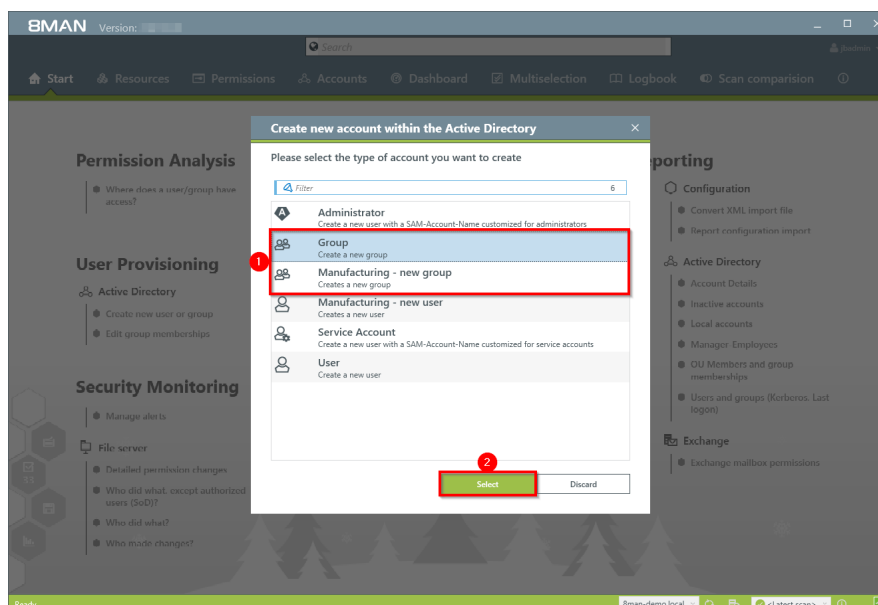
#### Additional Services

##### Manage group memberships

#### Step by step process



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



8MAN offers 4 standard templates. You can generate as many of your own templates as you wish. We recommend using adapted templates as a foundation as this simplifies, standardizes and speeds up the process.

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

1. Enter the required information.

2. Change the OU if desired.

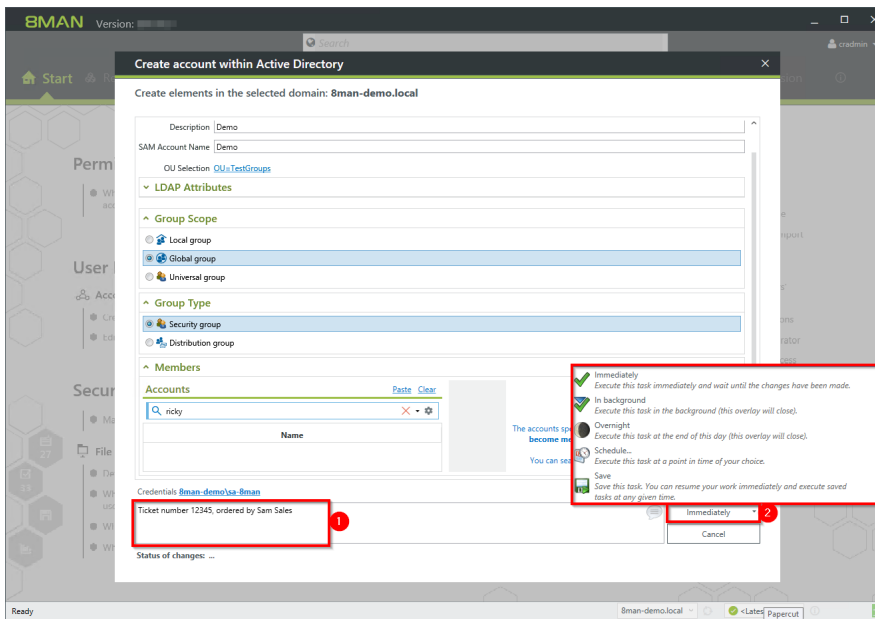
3. Add additional LDAP attributes.

4. Determine the group scope.

5. Determine the group type.

1. You can designate users while creating the group.

2. Determine the login information 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.

### 8.1.1.3 Manage group memberships

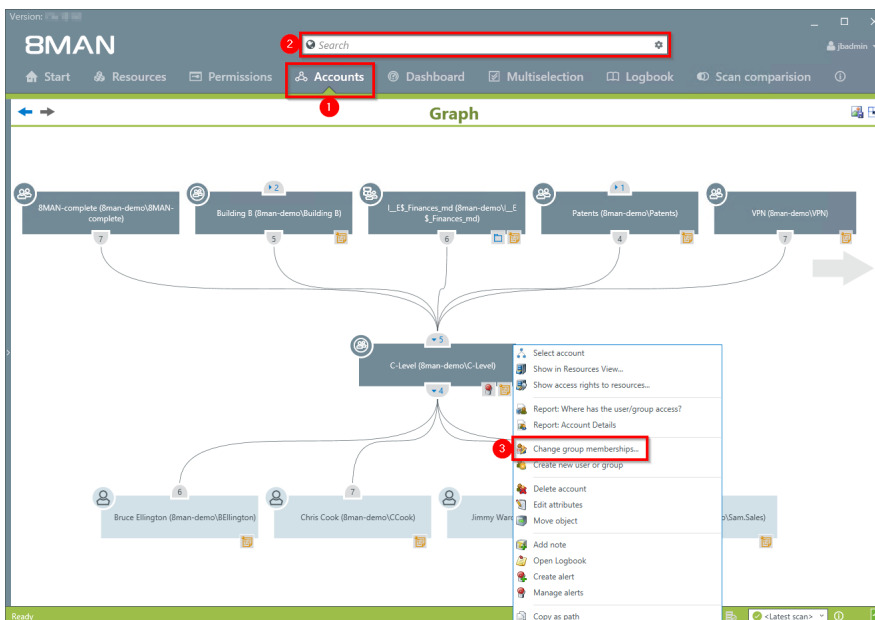
#### Background / Value

8MAN allows you to manage group memberships quickly and easily. You can also see which group(s) the group is a member of.

#### Additional Services

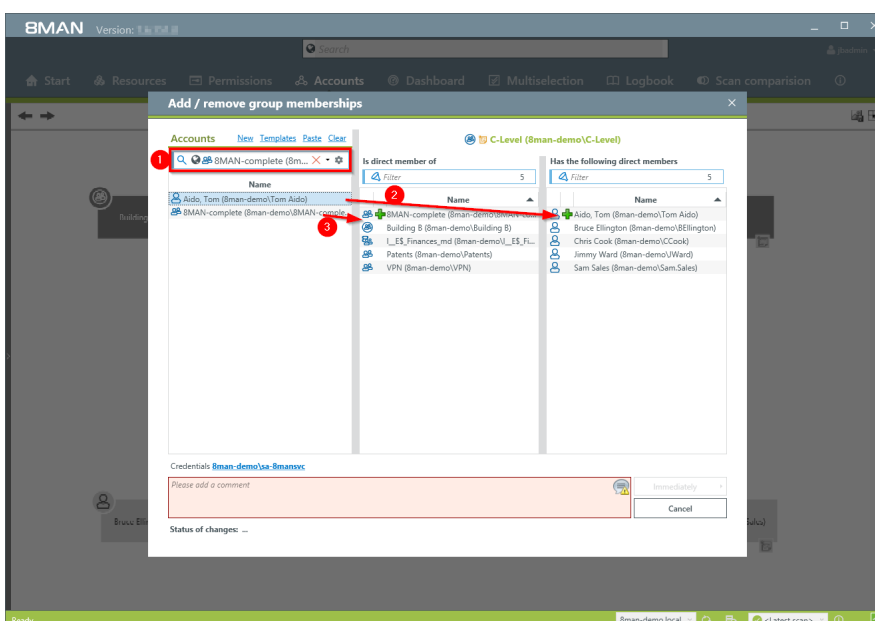
[Remove group memberships in bulk](#) (web client)

#### Step by step process

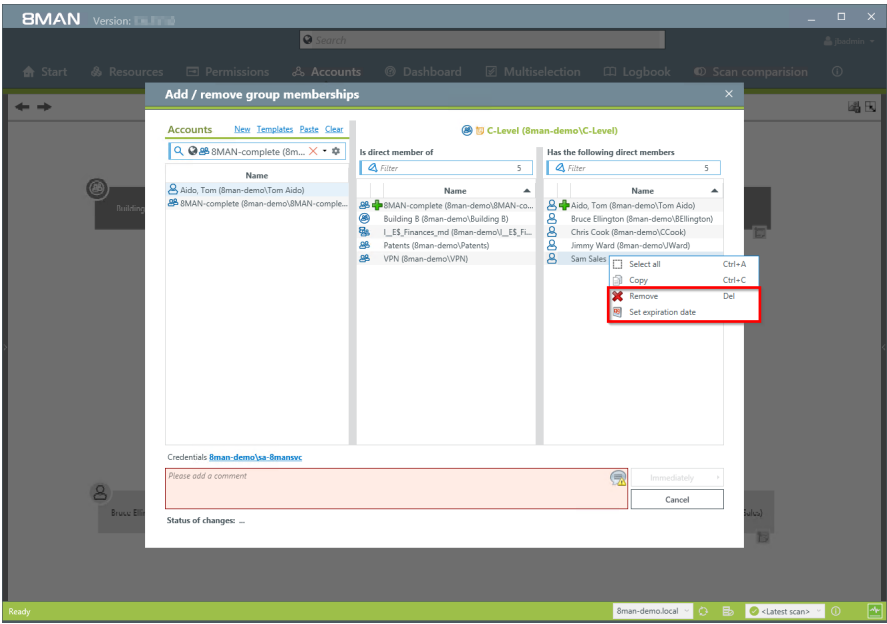


1. Select "Accounts".
2. Use the search field to find the desired account.
3. Right-click on the account and select "Change group memberships" in the context menu.

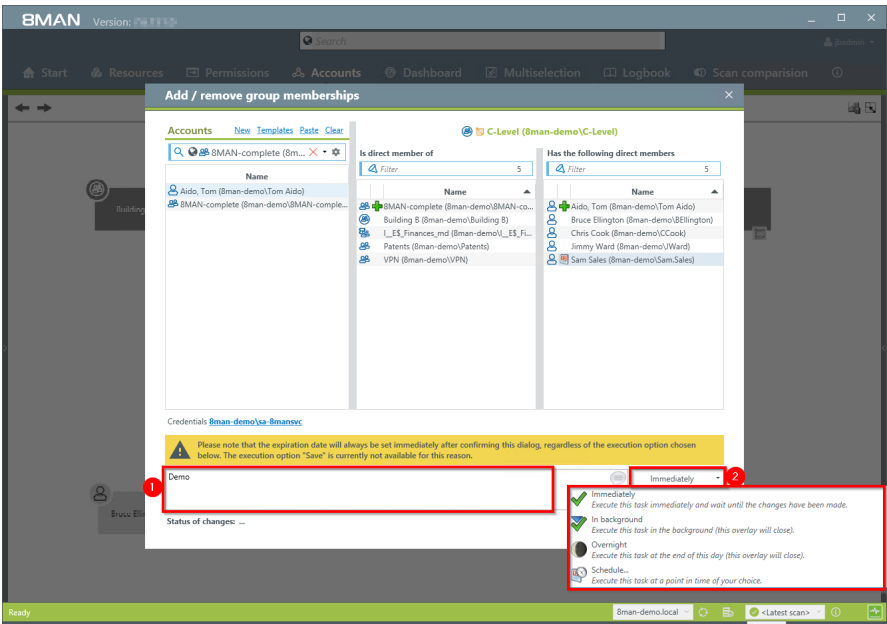
Alternatively you can also select "Edit group memberships" on the 8MAN home page.



1. Use the search field to find the desired user or group.
2. Use drag & drop to move users and groups into the right column to add new group members (children).
3. Use drag & drop to move a group to the middle column. This creates a new group membership (parent).



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.
- 1. Make changes immediately or save and schedule them for later.



### 8.1.1.4 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. 8MAN can delete user accounts and groups including all (direct) permissions on file servers. This prevents unauthorized SIDs and reduces security risks.

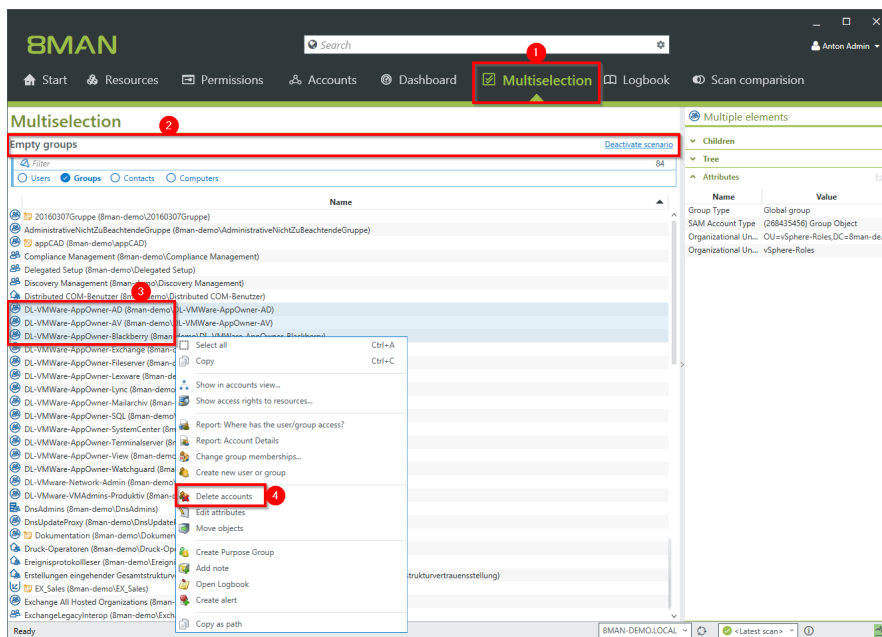


**Groups without members could be system groups. These should not be deleted.**

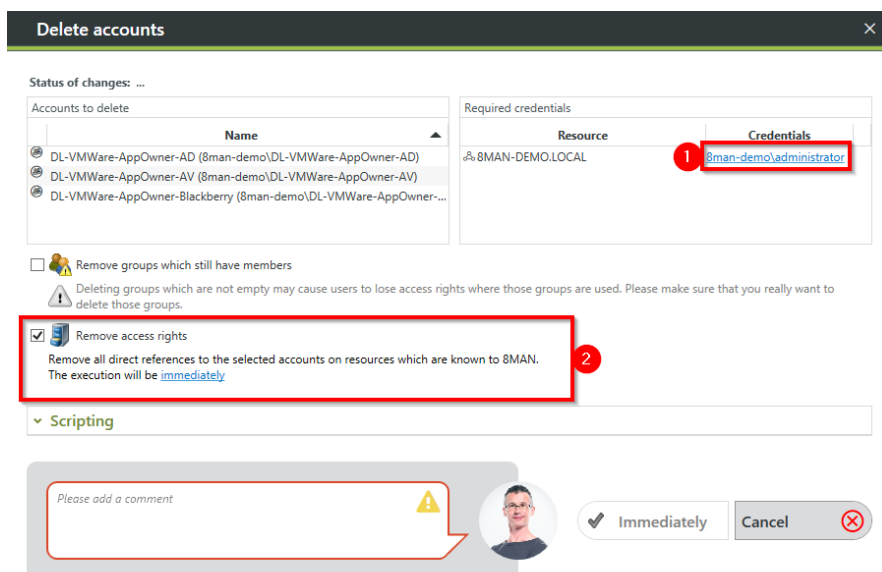
#### Step by step process

The screenshot displays the 8MAN user provisioning interface. The top navigation bar includes 'Start', 'Resources', 'Permissions', 'Accounts', 'Dashboard' (highlighted with a red box and a red circle with the number 1), 'Multiselection', 'Logbook', and 'Scan comparison'. The left sidebar shows 'Reporting' with sections for 'Active Directory' and 'File server'. The main content area shows a table of 'Users and other accounts' and 'Groups'. The 'Groups' section is expanded, showing a list of groups. The 'Empty groups' entry is highlighted with a red box and a red circle with the number 2. The 'Depth of nested groups' bar chart shows the distribution of group depths.

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



1. 8MAN automatically switches to "Multiselection".
2. The scenario "Empty groups" is active. All listed groups are empty.
3. Select the groups that you know are safe to delete.
4. Right-click and select "Delete Account" 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 occurrence of unresolved SIDs.

The screenshot shows a 'Delete accounts' dialog box. At the top, there's a title bar 'Delete accounts' with a close button. Below it, a section 'Status of changes: ...' contains two options: 'Remove groups which still have members' (unchecked) and 'Remove access rights' (checked). A warning icon and text are present below the first option. The 'Remove access rights' option has a sub-note: 'Remove all direct references to the selected accounts on resources which are known to 8MAN. The execution will be immediately'. A red circle with the number '1' is placed over the word 'immediately'. Below this is a 'Scripting' section with two dropdown menus: 'Execute script before change action' and 'Execute script after change action', both set to 'None'. A red box highlights this section. At the bottom, there's a comment field with the placeholder 'Please add a comment', a user profile picture, and a red circle with the number '2' next to it. To the right of the comment field is a 'Cancel' button with a red 'X' icon. A red circle with the number '3' is placed over the 'Immediately' button, which has a checkmark icon.

1. Choose whether to run a script before or after deleting.

*See also: Configure scripts*

1. You must enter a comment.

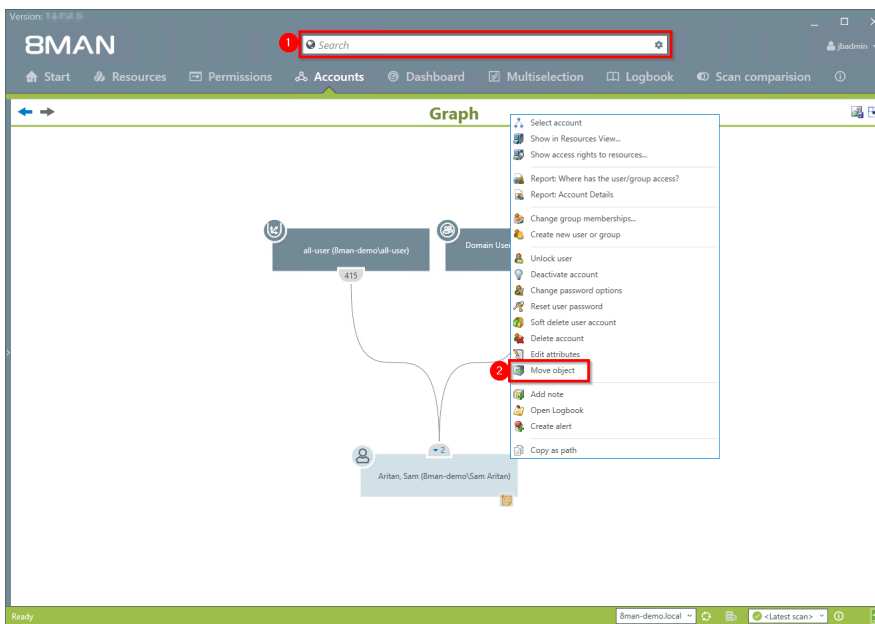
2. Start the deletion process.

### 8.1.1.5 Move objects in Active Directory

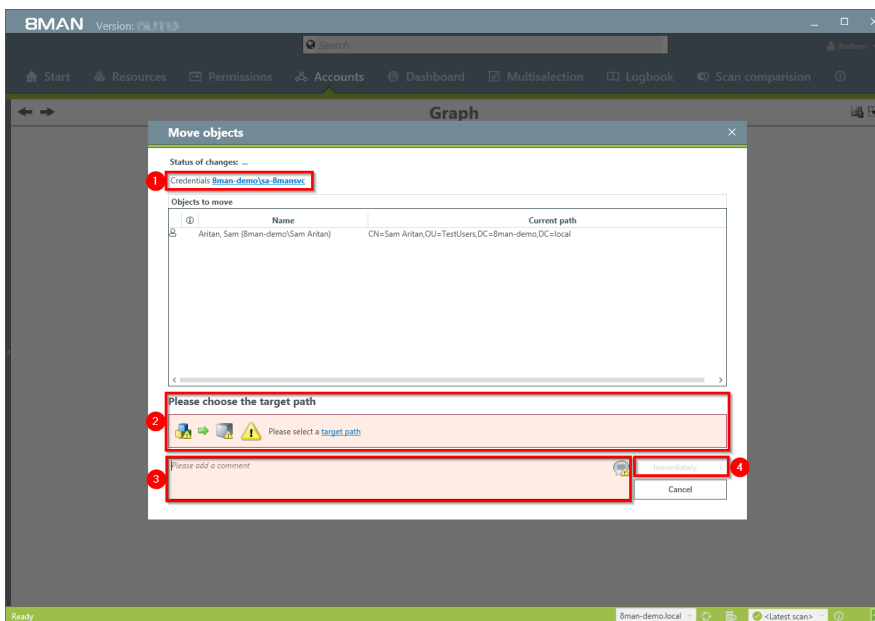
#### Background / Value

8MAN 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. 8MAN 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. Then select "move object".



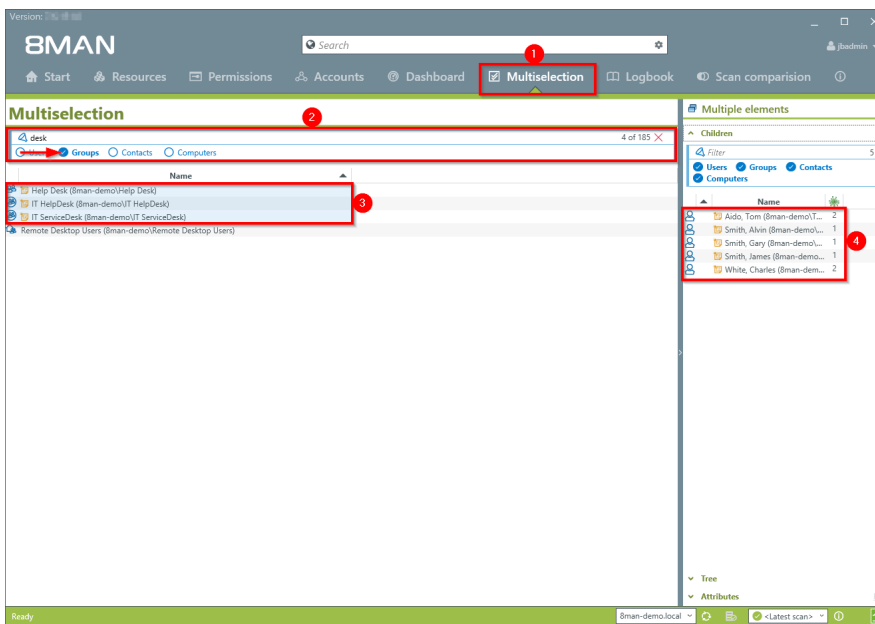
1. If required change the login which will be used to move the object.
2. Select a destination path.
3. You must enter a comment.
4. Start the process.

### 8.1.1.6 Reduce multiple groups to one group

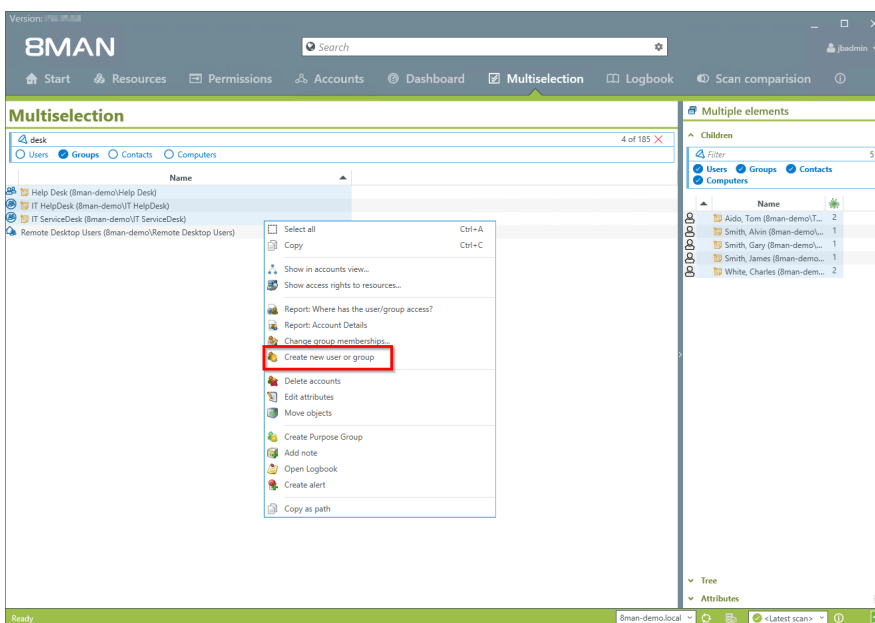
#### Background / Value

On organized AD should have a limited number of groups. 8MAN allows you to easily combine historically accumulated and unnecessary groups. The following example shows the creation of a central help desk group. 8MAN allows you to simply copy all of the desired members and then combine them into one group.

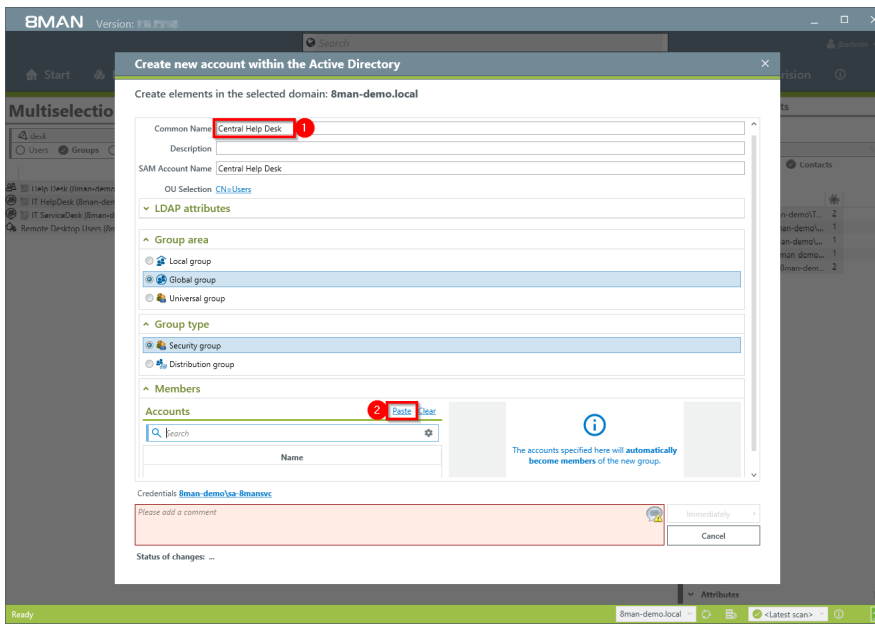
#### Step by step process



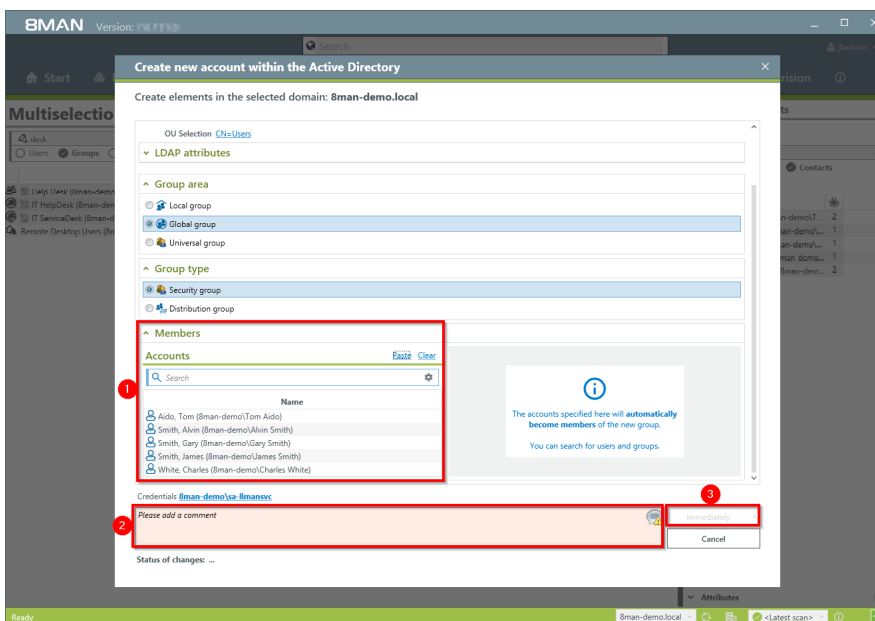
1. Select "Multiselection".
2. Apply filters to find the desired groups.
3. Select the groups.
4. Select all desired users and copy them into the clipboard. (For example CTRL+A and CTRL+C).



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



1. Name the new group.
2. In the "Members" area 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 with the creation of a new group.

### 8.1.1.7 Change password options

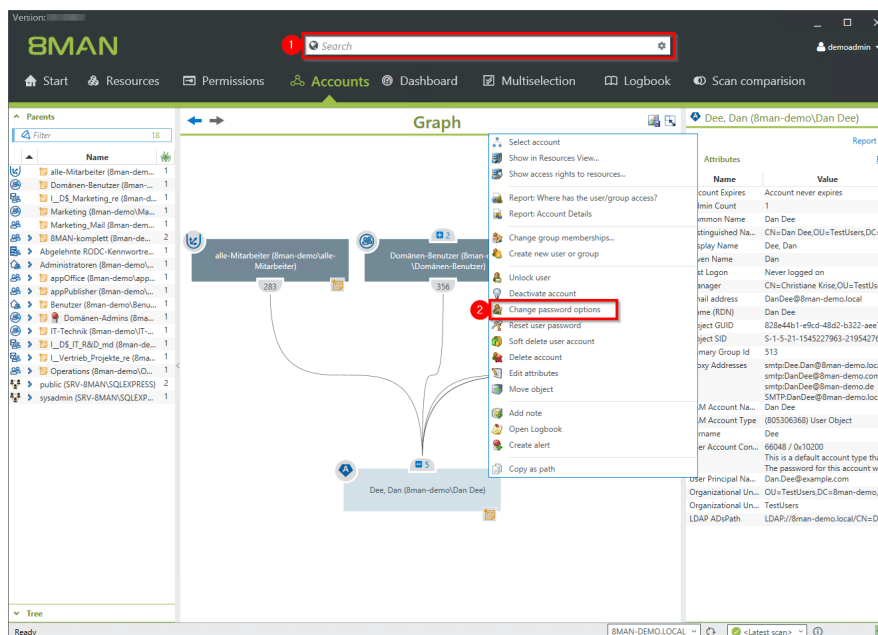
#### Hintergrund/Mehrwert

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

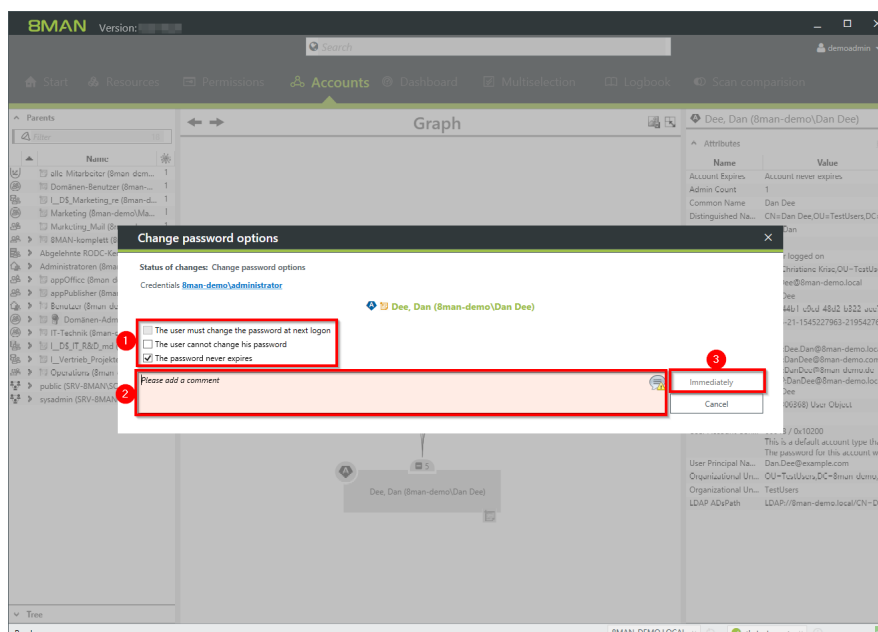
#### Additional Services

[Change password options in bulk](#) (web client)

#### Step by step process



1. Find the desired user with the search.
2. Right-click the user, for example, in Accounts view, and choose "Change Password Options" from the context menu.



1. Set password options.
2. You must enter a comment, such as "Ticket number," "Ordered by", or "Approved by".
3. Start the execution.





### 8.1.1.8 Deactivate user accounts in bulk (web client)

#### Background / Value

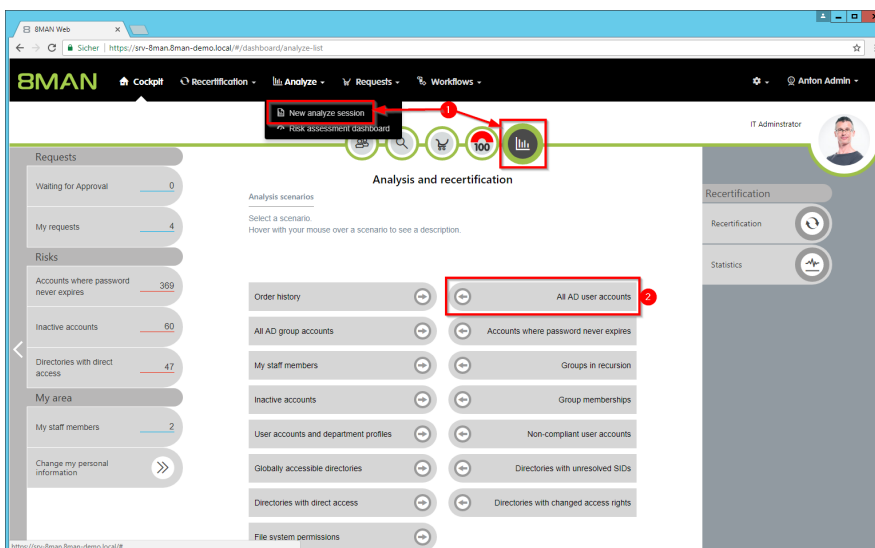
After a security breach it often makes sense to deactivate accounts in bulk. You can do this quickly and easily in the web interface.

#### Complementary Services

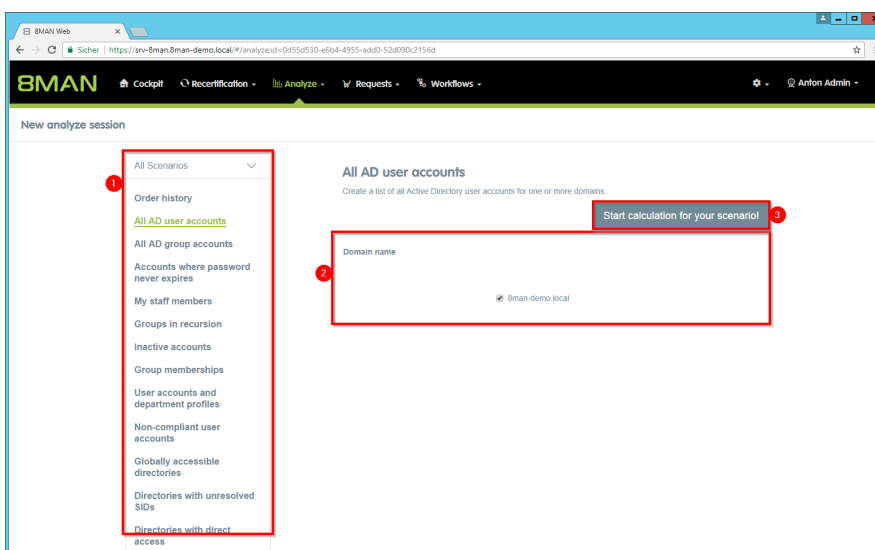
[Change password options in bulk](#) (web client)

[Delete accounts in bulk \(soft delete\)](#) (web client)

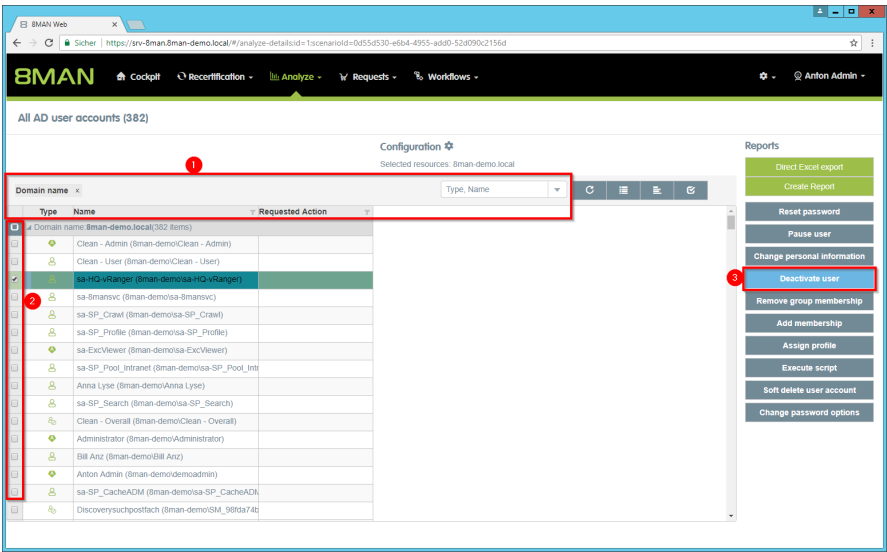
#### Step by step process



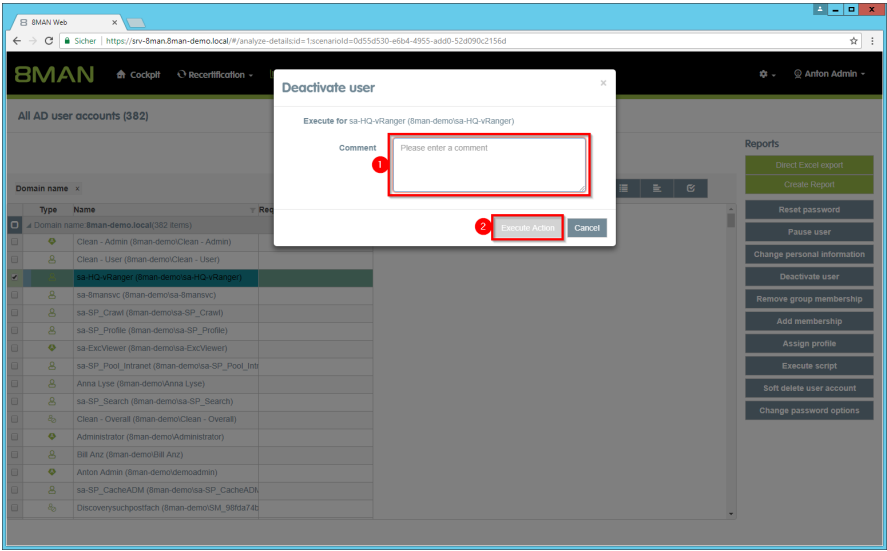
1. Select "New analyze session".
2. Click on "All AD user accounts".



1. Optional: Change the scenario.
2. Set options for the scenario.
3. Click on "Start calculation".



1. Use sorting, filtering and grouping functions to narrow down your selection.
2. Select the desired entries.
3. Click "Disable user".



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

The job is transferred to the 8MAN server and executed there. 8MAN shows the status in the job overview.

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

#### Background / Value

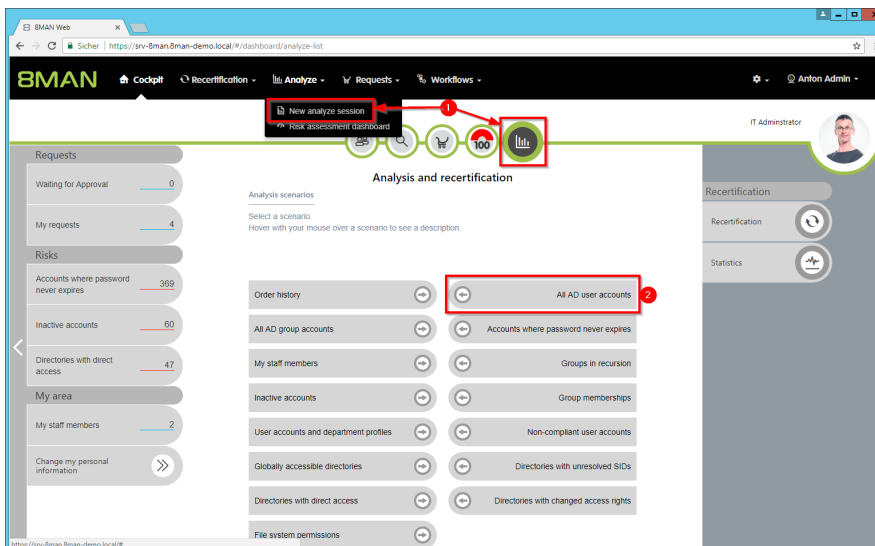
After a security breach or the dissolution of a department, it makes sense to delete several accounts at the same time. Do this conveniently in the web client.

#### Additional Services

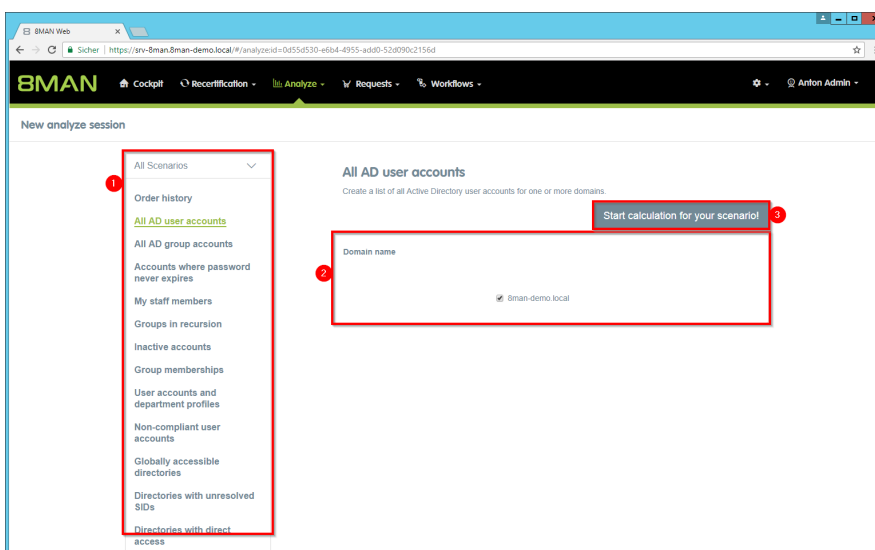
[Change password options in bulk](#) (web client)

[Delete accounts in bulk \(soft delete\)](#) (web client)

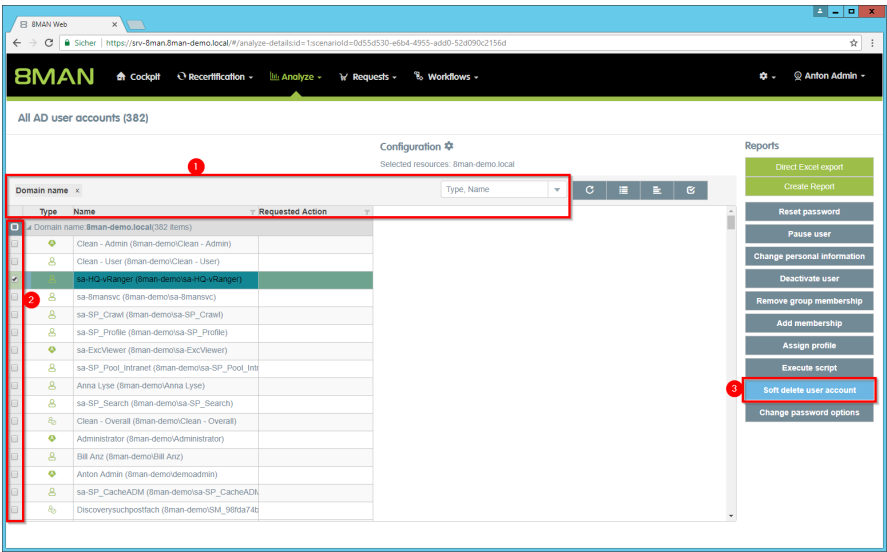
#### Step by step process



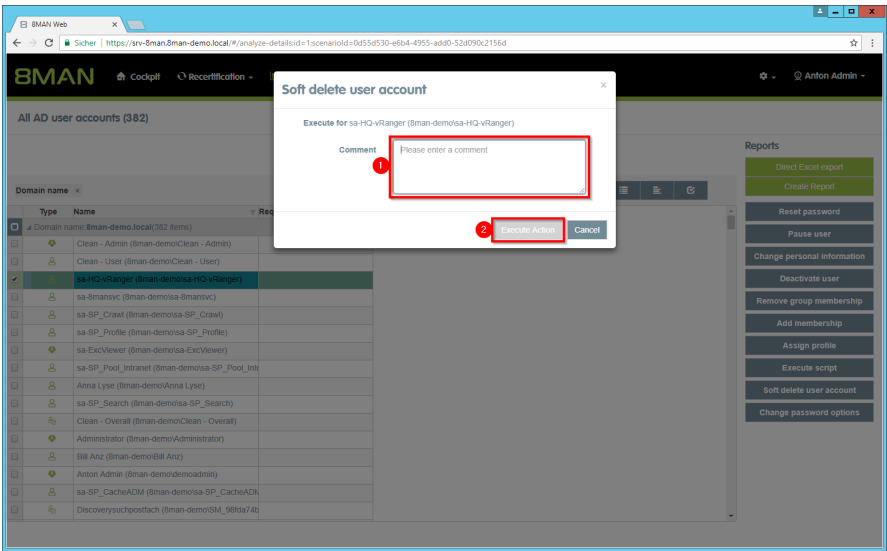
1. Select "New analyze session".
2. Click on "All AD user accounts".



1. Optional: Change the scenario.
2. Set options for the scenario.
3. Click on "Start calculation".



1. Use sorting, filtering, grouping and column selection to locate the desired rows.
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 8MAN server and executed there. You can find the status in "Jobs overview".

### 8.1.1.10 Change password options in bulk (web client)

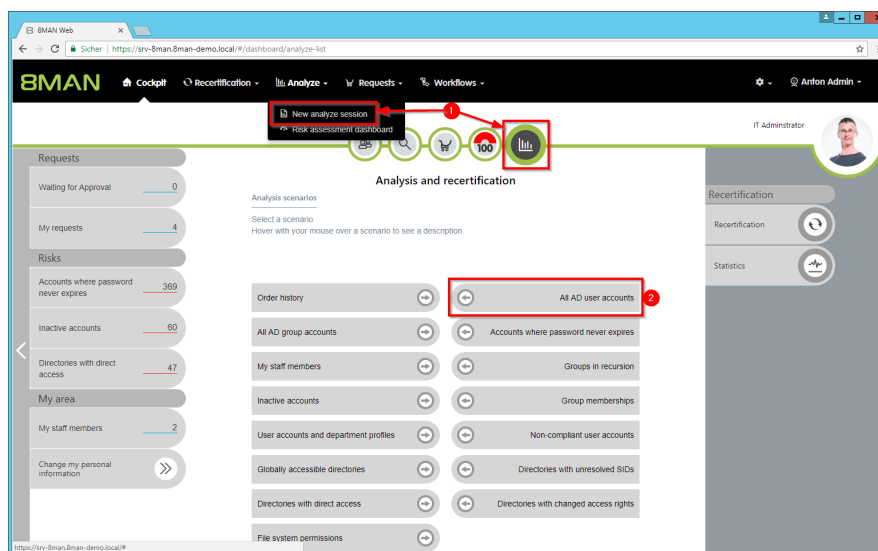
#### Background / Value

Passwords must be changed regularly. You can manage password options across your entire organization, quickly and easily in the 8MAN web interface.

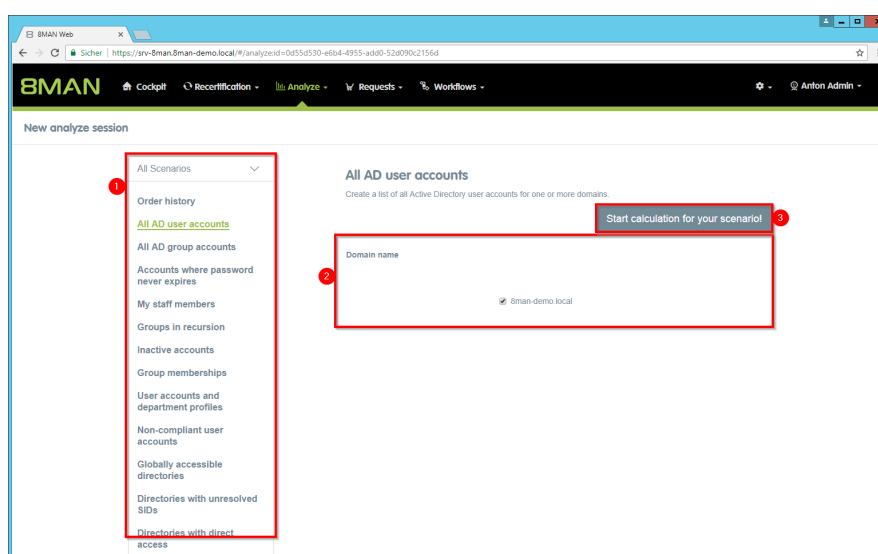
#### Additional Services

[Reset passwords in bulk](#) (web client)

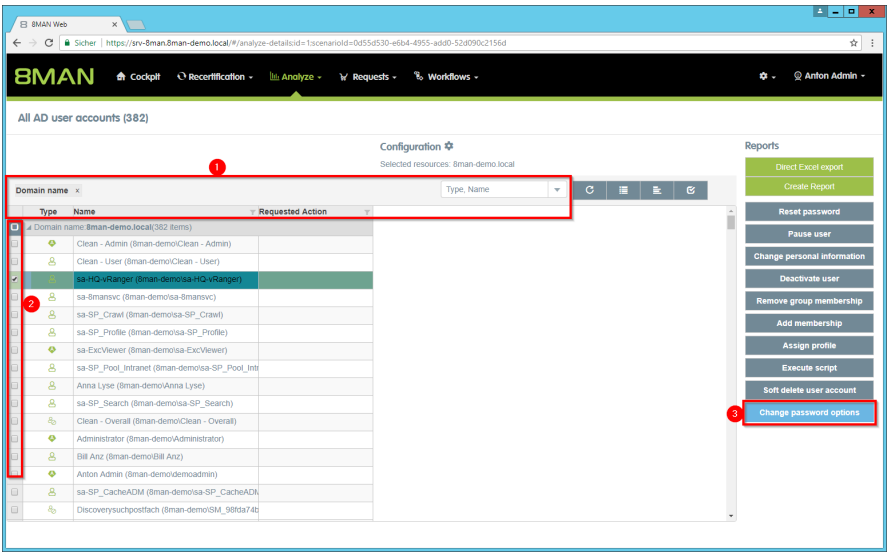
#### Step by step process



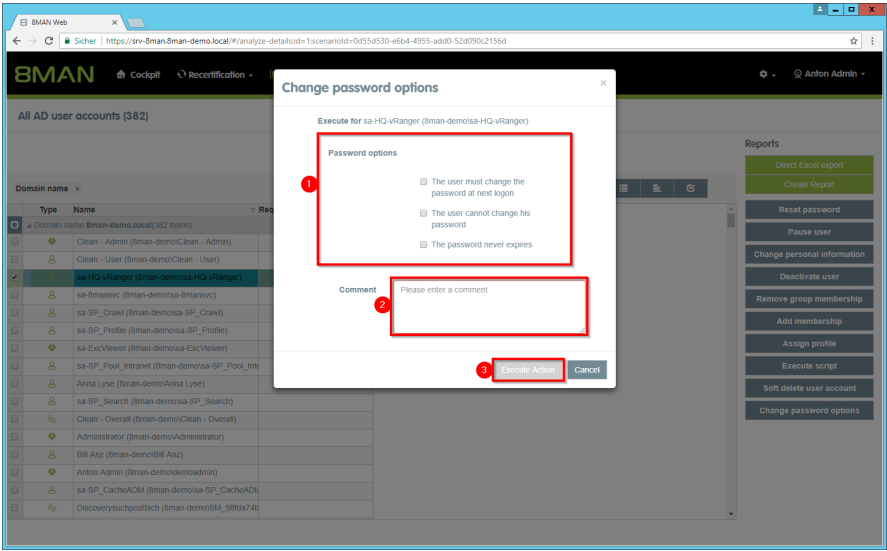
1. Select "New analyze session".
2. Click on "All AD user accounts".



1. Optional: Change the scenario.
2. Set options for the scenario.
3. Click on "Start calculation".



1. Use sorting, filtering, grouping and column selection to locate the desired rows.
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 8MAN server and executed there. You can find the status in "Jobs overview".

### 8.1.1.11 Modify attributes in bulk (web client)

#### Background / Value

With 8MAN you can change AD attributes in bulk. This can be relevant during reorganizations such as a merger and / or address change.

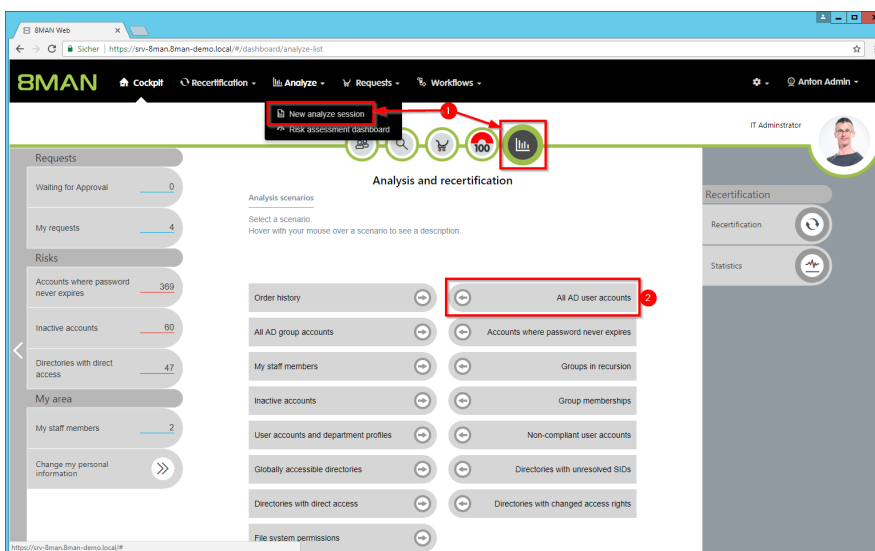
8MAN provides a standard set of modifiable attributes. For each 8MAN role, you can specify which attributes are displayed and can therefore be changed. Please contact our support in such cases.

#### Additional Services

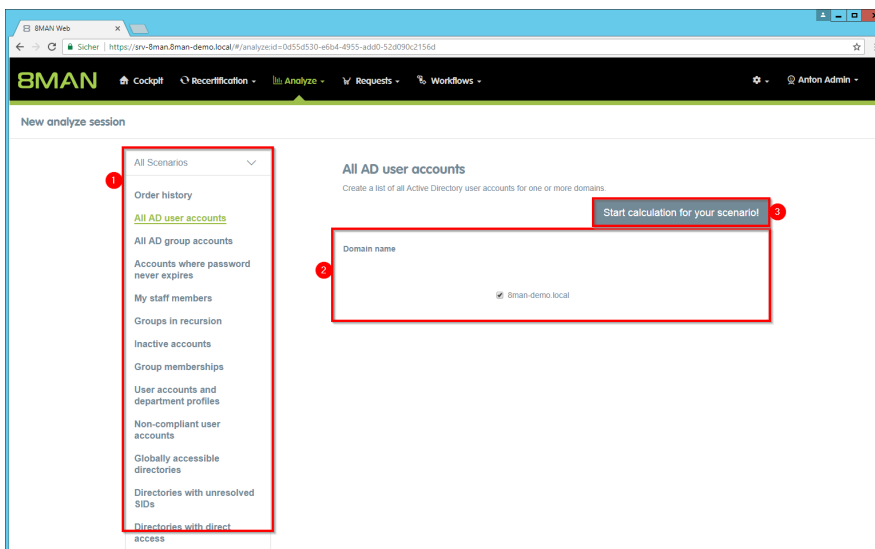
[Change password options in bulk](#) (web client)

[Reset passwords in bulk](#) (web client)

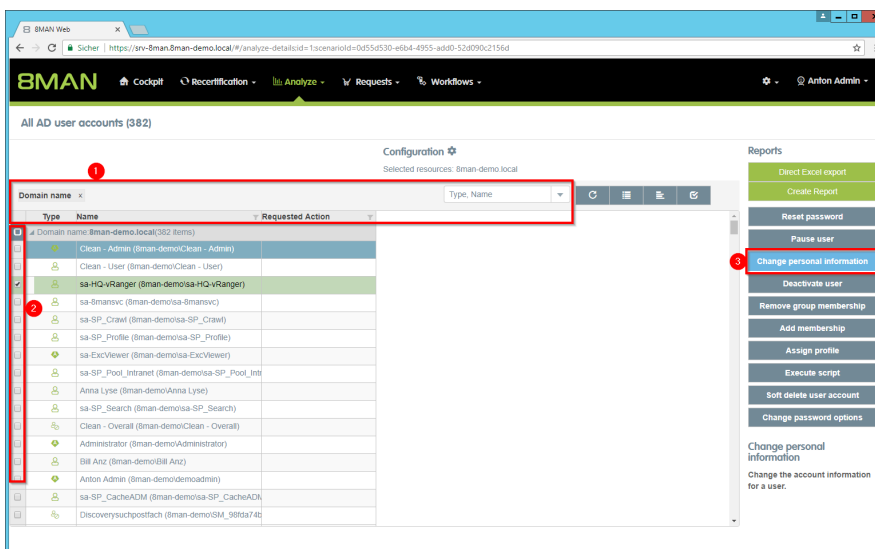
#### Step by step process



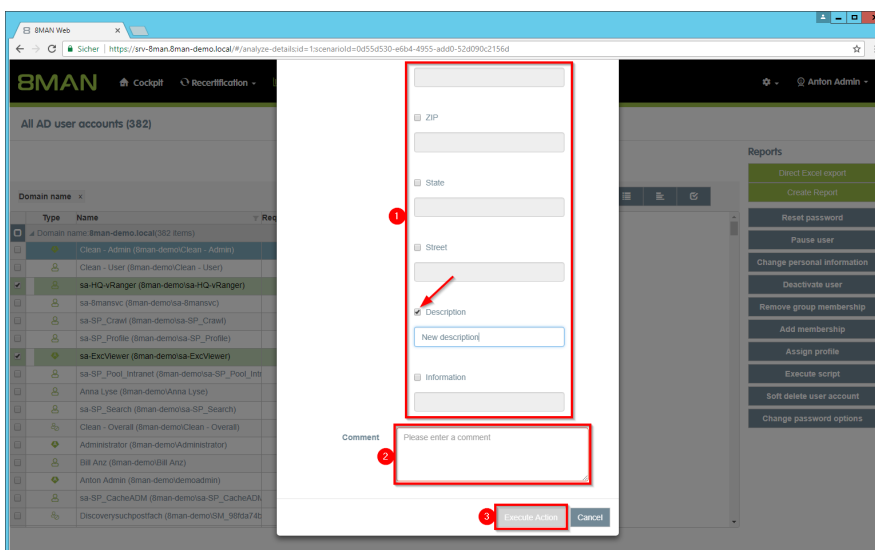
1. Select "New analyze session".
2. Click on "All AD user accounts".



1. Optional: Change the scenario.
2. Set options for the scenario.
3. Click on "Start calculation".



1. Use sorting, filtering, grouping and column selection to locate the desired rows.
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 do not specify a value, the contents of the attributes are deleted.

2. You must enter a comment.
3. Click "Execute Action".

The job will be transferred to the 8MAN server and executed there. You can find the status in "Jobs overview".



*The attributes displayed in the dialog can be adjusted per role. For this purpose, an adjustment of the configuration file must be made. Instructions can be found in our [knowledgebase](#) (login required).*

### 8.1.1.12 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.

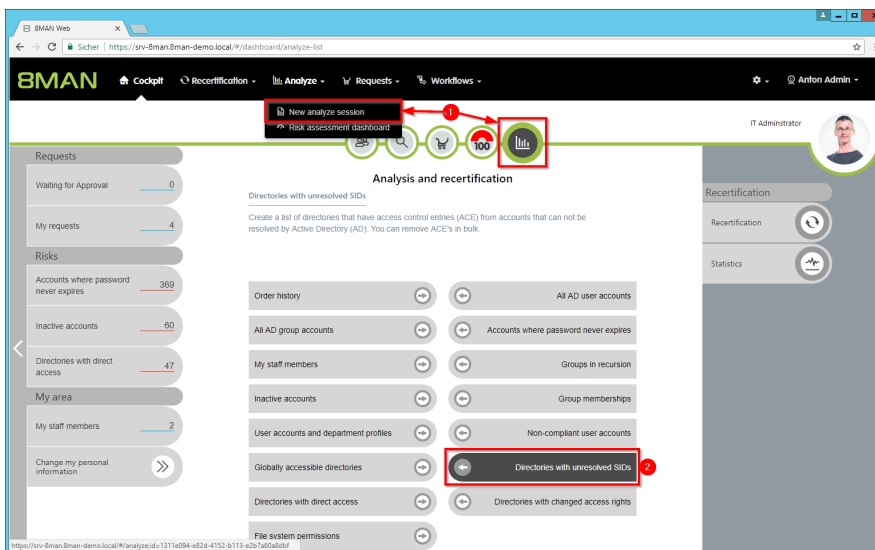
8MAN clearly identifies unresolved SIDs in your system. Delete unresolved SIDs in bulk using Analyze & Act.

#### Additional Services

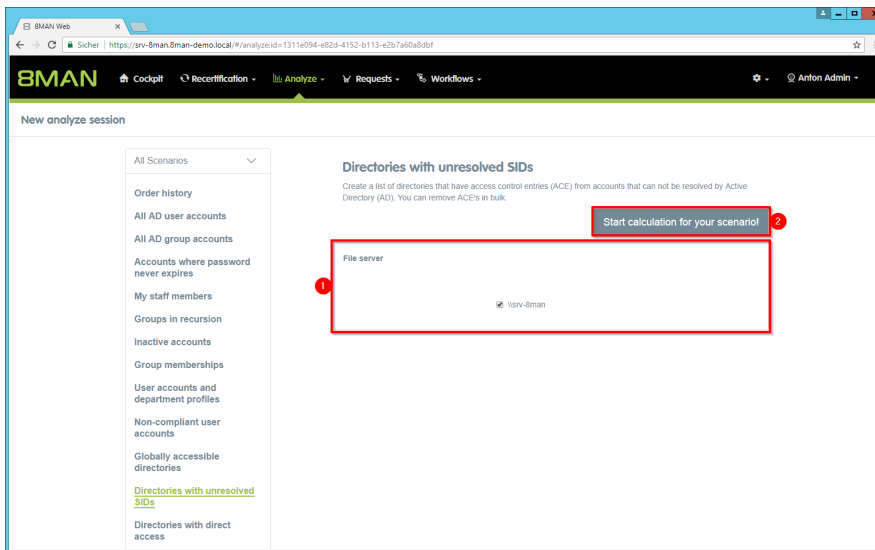
[Identify and delete unresolved SIDs](#) (rich client)

[Report: Identify unresolved SIDs](#) (rich client)

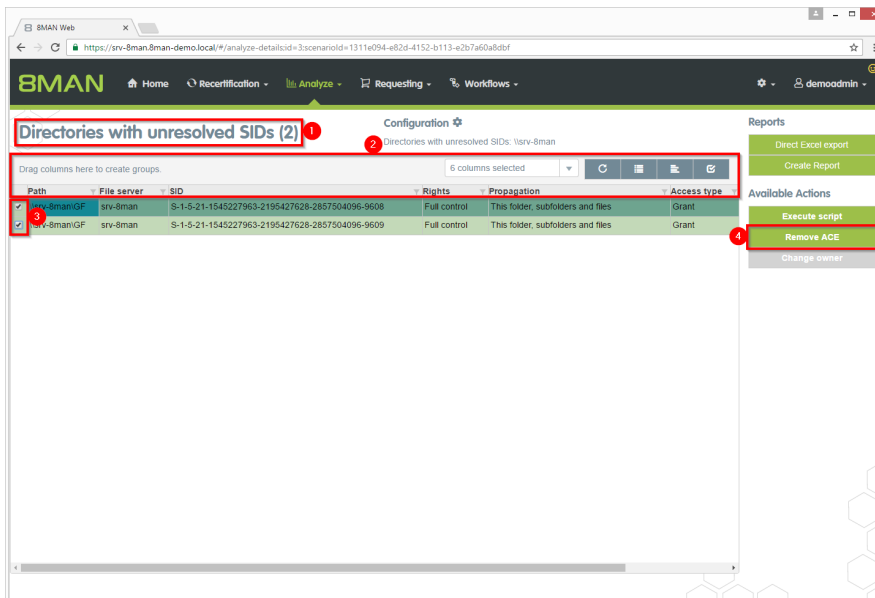
#### Step by step process



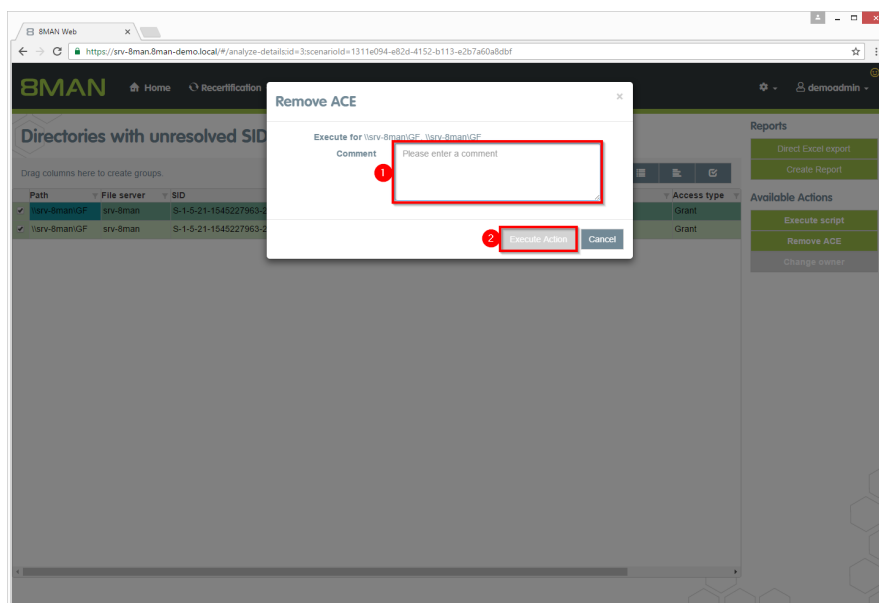
1. Select "New analyze session".
2. Click "Directories with unresolved SIDs".



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



1. 8MAN 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 8MAN server and executed there. You can find the status in "Jobs overview".*

### 8.1.1.13 Remove direct permissions in bulk (web client)

#### Background / Value

Direct permissions should be avoided at all costs and replaced by group permissions. 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 permissions. 8MAN shows you all direct access rights on your file server(s). You can remove them in bulk using the web client.

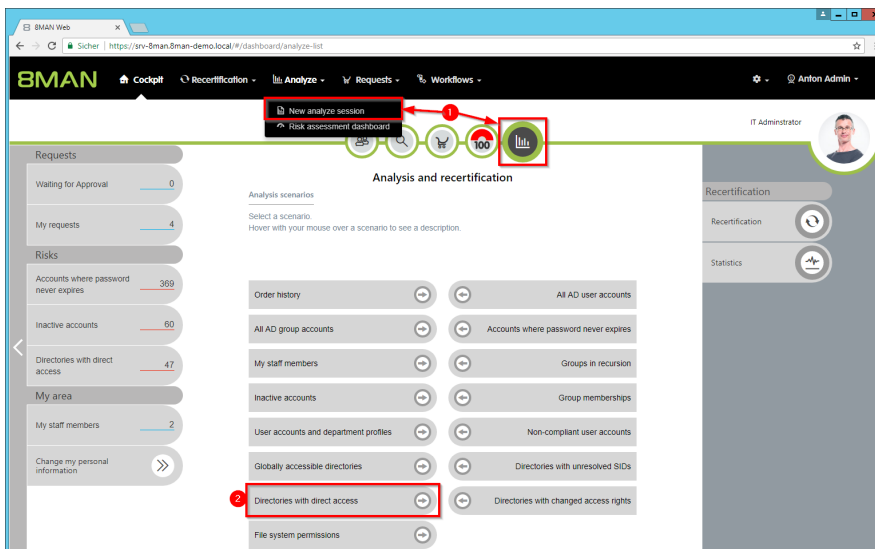
#### Additional Services

8MATE Clean! allows you to automatically remove direct access rights and turn them into group memberships.

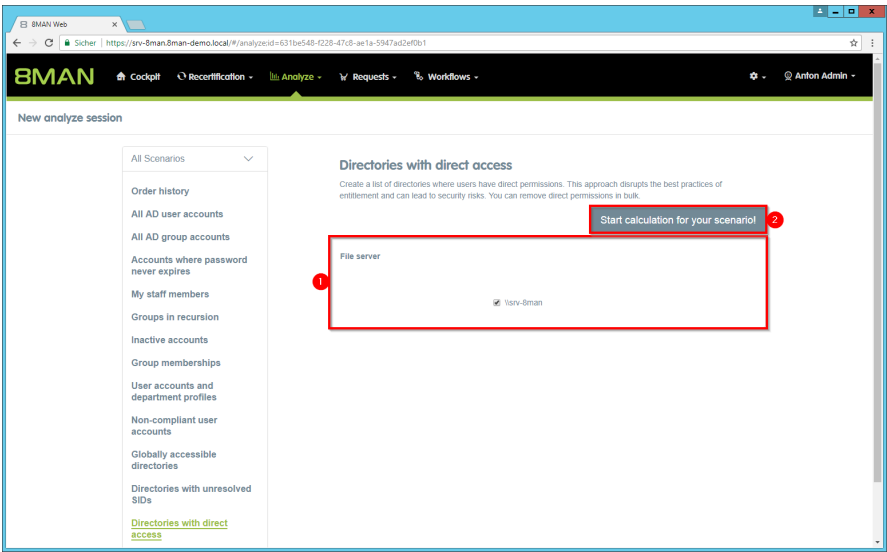
[Change password options in bulk](#) (web client)

[Remove unresolved SIDs in bulk](#) (web client)

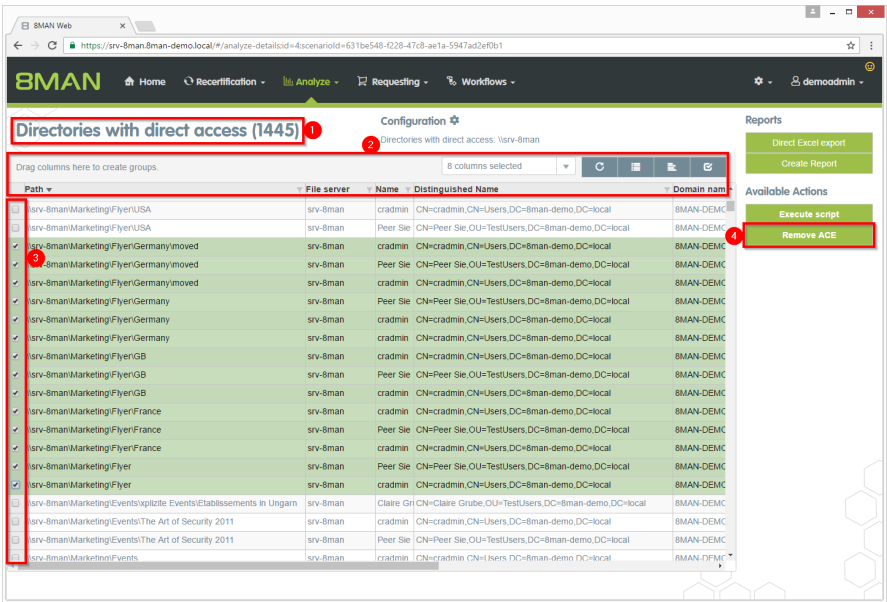
#### Step by step process



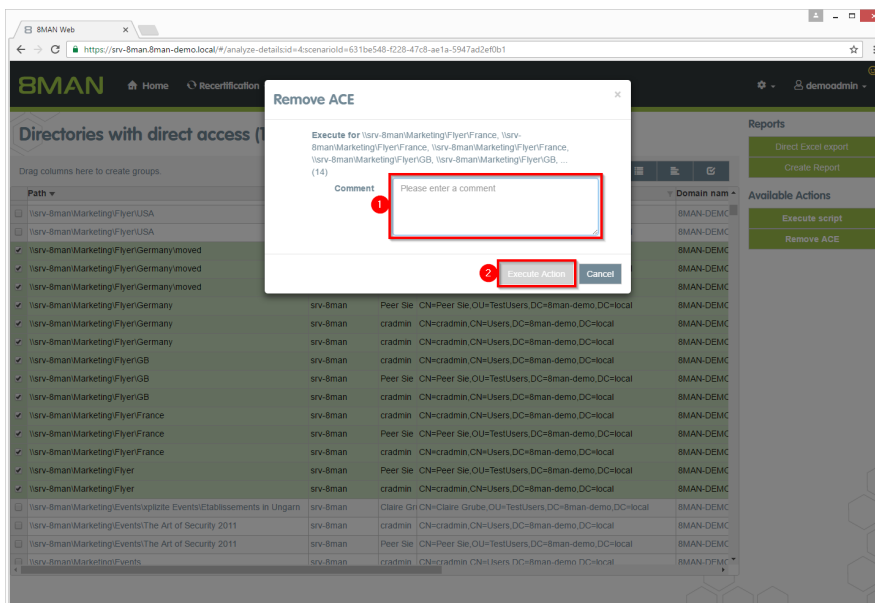
1. Select "New analyze session".
2. Click "Directories with direct access".



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



1. 8MAN 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 8MAN server and executed there. You can find the status in "Jobs overview".*

### 8.1.1.14 Remove group memberships in bulk (web client)

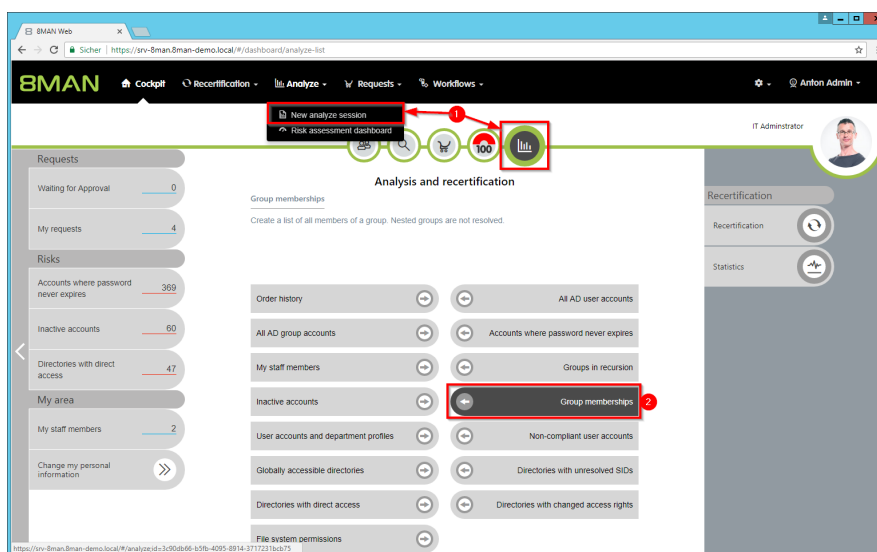
#### Background / Value

Remove lots of group memberships fast using the web client.

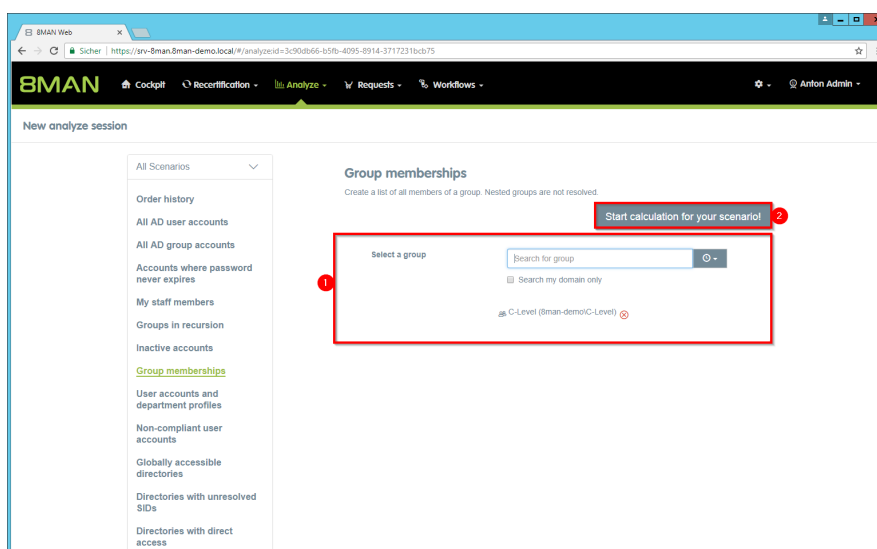
#### Additional Services

[Managing group memberships](#) (rich client)

#### Step by step process

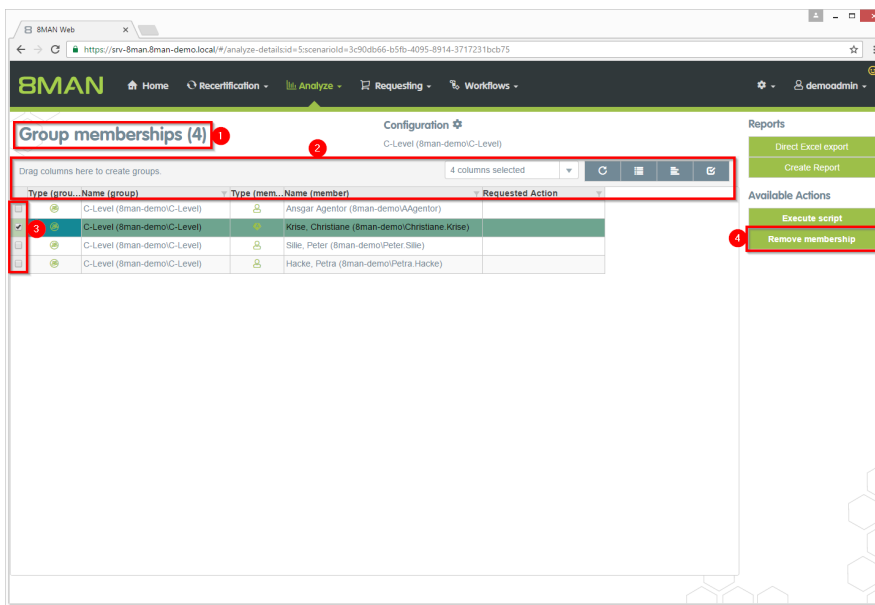


1. Select "New analyze session".
2. Click "Group memberships".

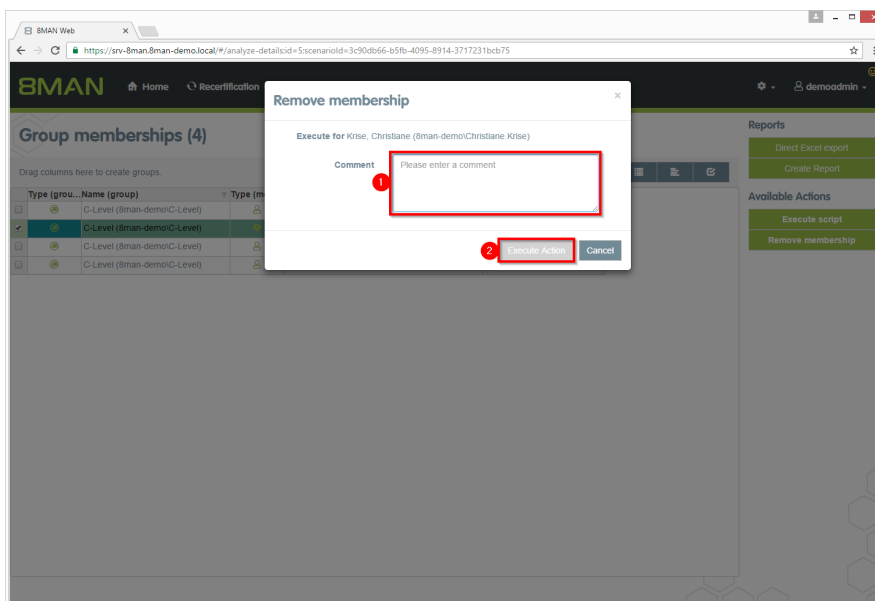


1. Find a group.
2. Start the calculation.





1. 8MAN 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 8MAN server and executed there. You can find the status in "Jobs overview".

### 8.1.1.15 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:

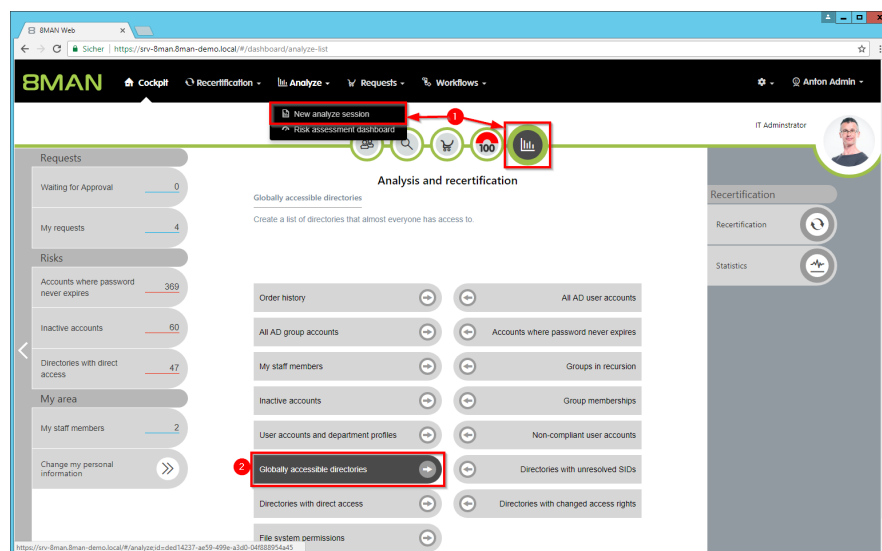
- Everyone
- Authenticated Users
- Domain-Users

#### Additional Services

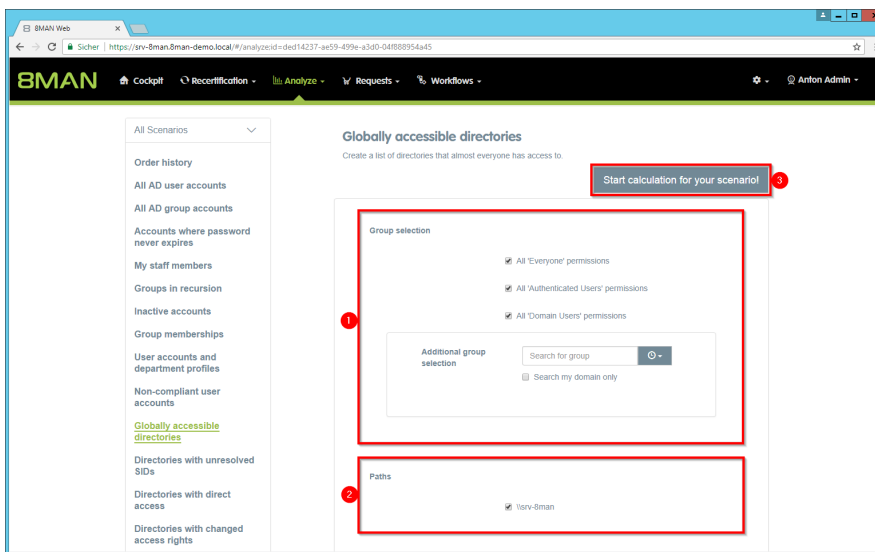
[Report: Identify usage of "Everyone" \(rich client\)](#)

[Report: Identify usage of "Authenticated Users" \(rich client\)](#)

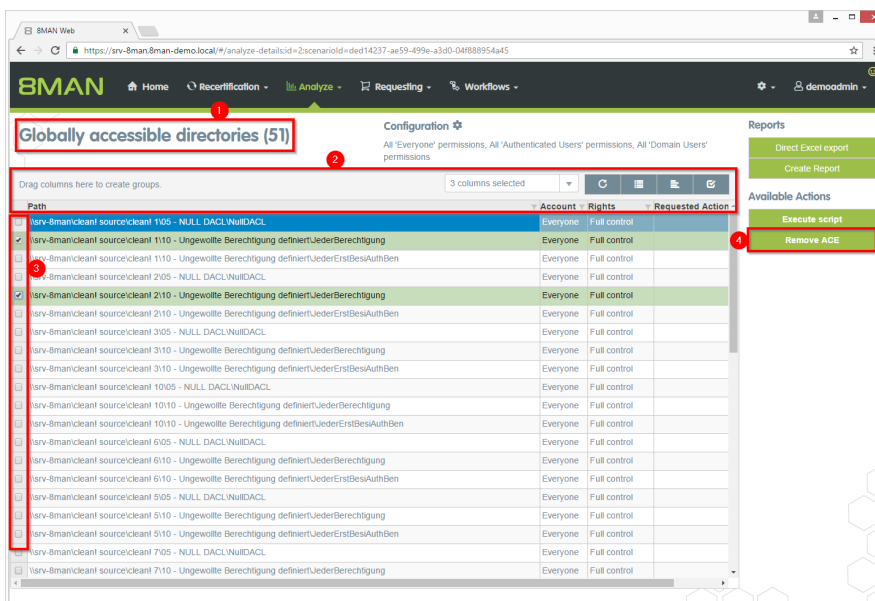
#### Step by step process



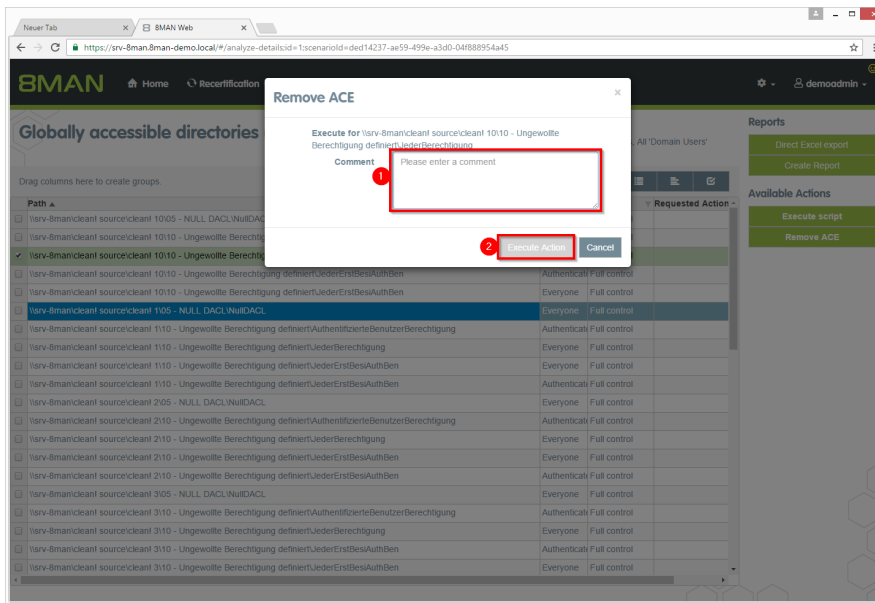
1. Select "New analyze session".
2. Click "Globally accessible directories".



1. Select groups.  
You can add one additional group. This is very useful for "catch-all" groups, e.g. "mycompany-complete".
2. Select the file servers.
3. Start the calculation.



1. 8MAN 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 8MAN server and executed there. You can find the status in "Jobs overview".

### 8.1.1.16 Create a new department profile (administrator)

#### Background / Value

8MAN 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.

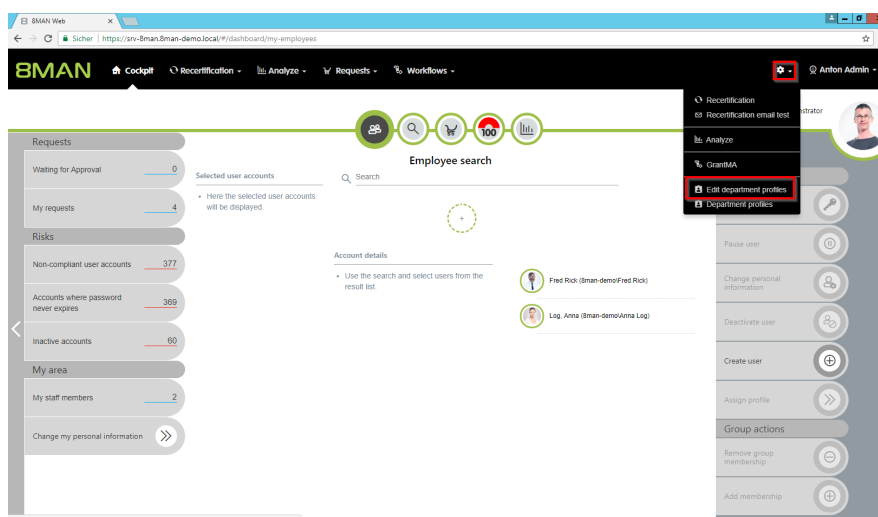
Department profiles can contain attributes and group memberships.

#### Additional Services

[Assign a department profile to users \(Cockpit\)](#)

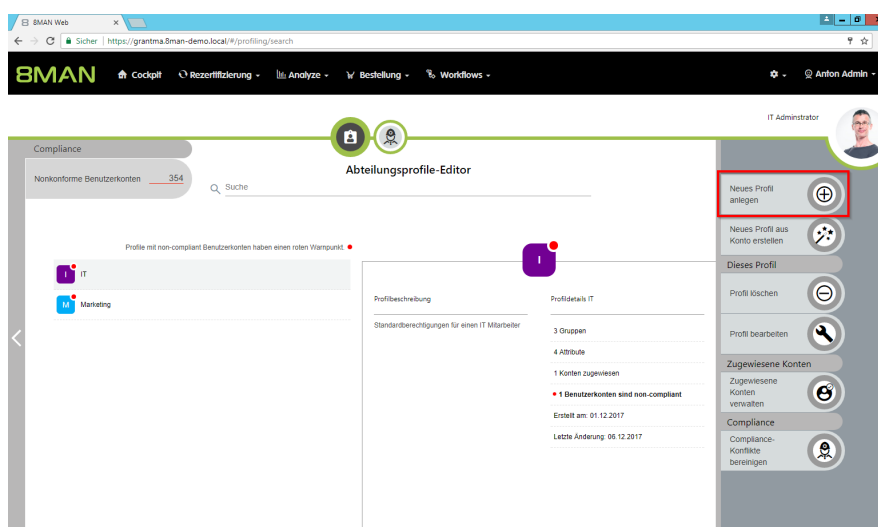
[Determine permissions deviating from the department profile \(compliance check\)](#)

#### Step by step process

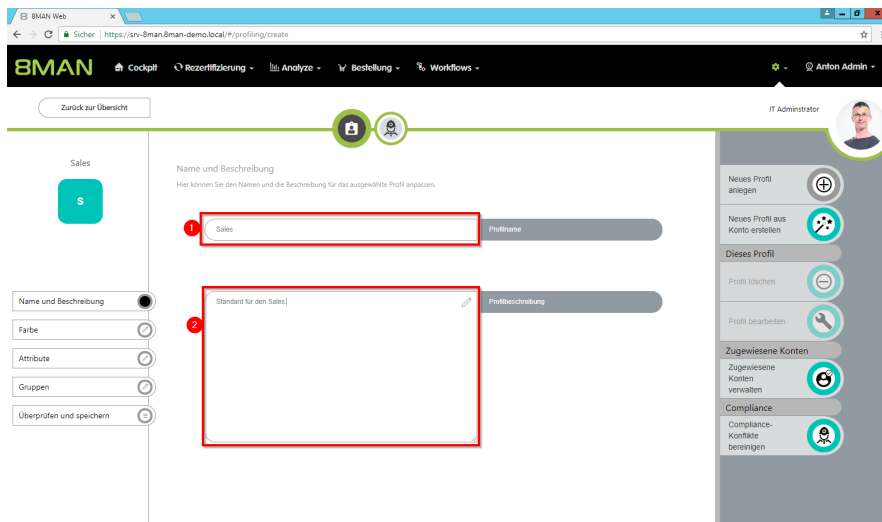


Click on "Edit department profiles".

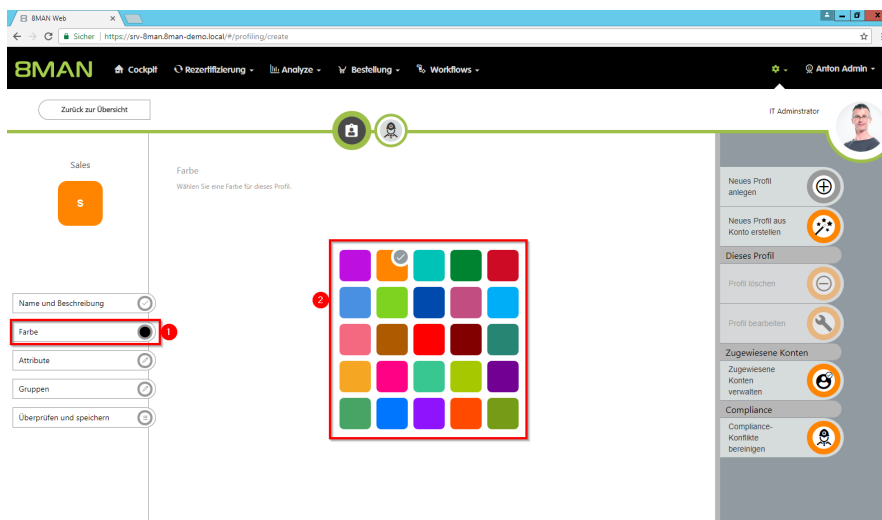
You must be logged in as 8MAN Administrator to see the gear icon.



Click on "Create new profile".

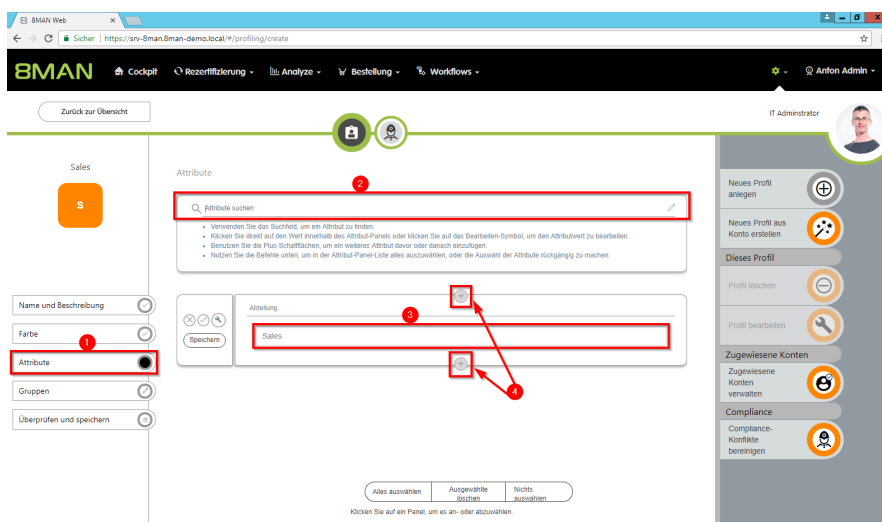


1. Give the department profile a name, at least 2 letters.
2. Optional:  
Describe the profile.

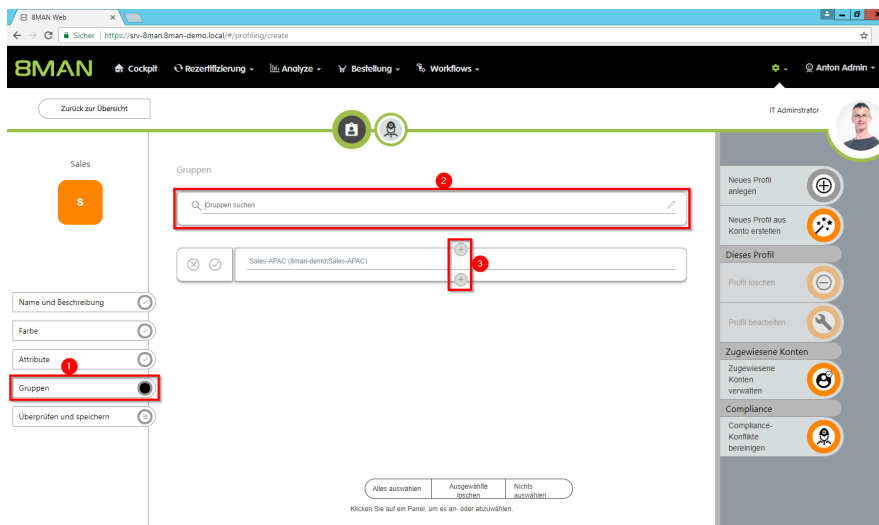


1. Click on "color".
2. Choose a color for the department profile.

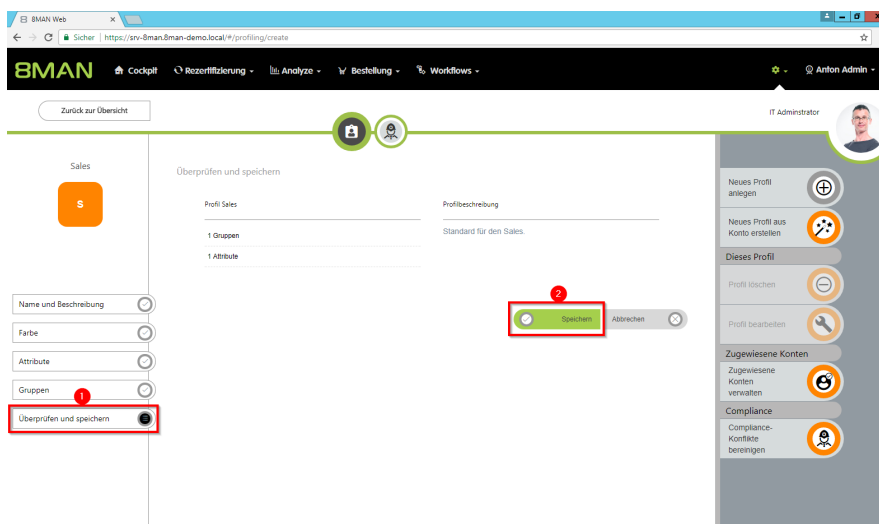
The color is for recognition.



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. Click on "Review and save".
2. Click "Save" to create the department profile.

### 8.1.1.17 Execute scripts for directories in bulk (web client)

#### Background / Value

Use self-created scripts on directories. 8MAN opens up space for very individual requirements. Put your scripts in the following directory to use with 8MAN:

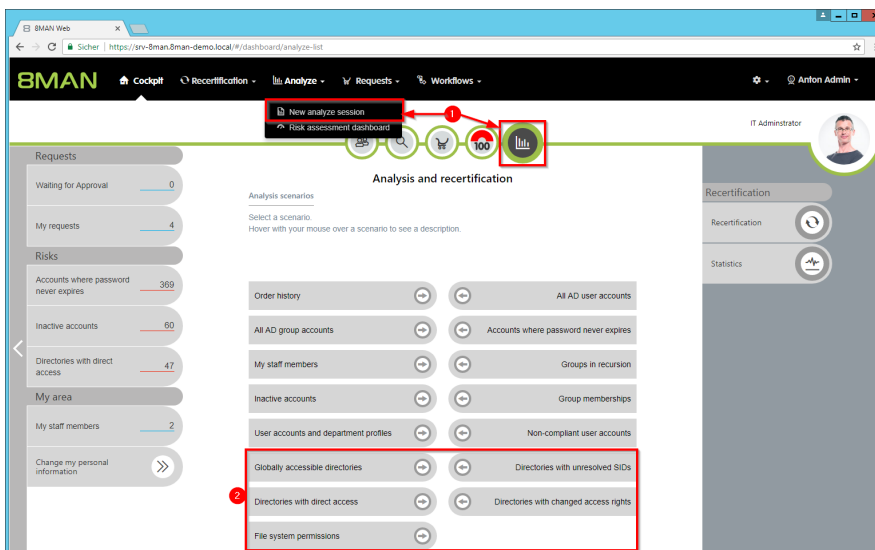
`%ProgramData%\protected-networks.com\8MAN\scripts\analyze`

Further necessary steps and details for configuring scripts can be found in the Installation and Configuration Manual.

#### Additional Services

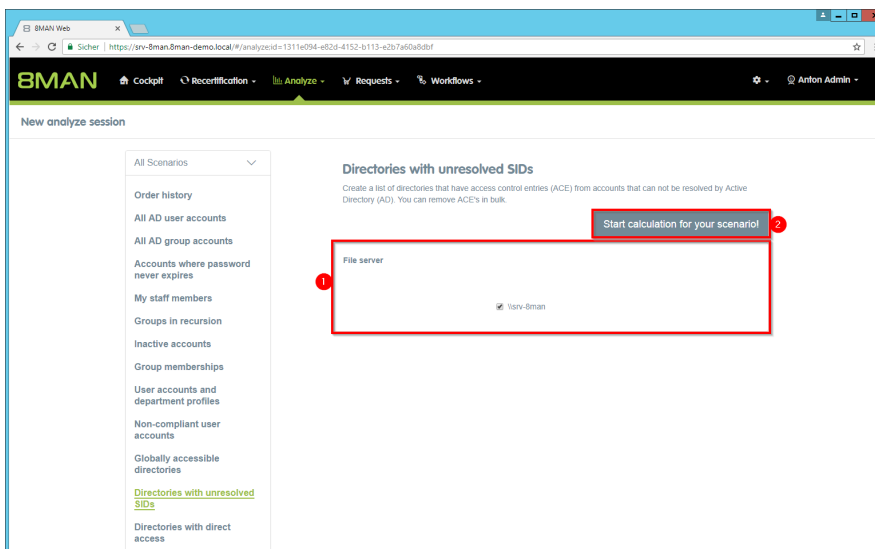
[Execute scripts on user accounts in bulk](#) (web client)

#### Step by step process

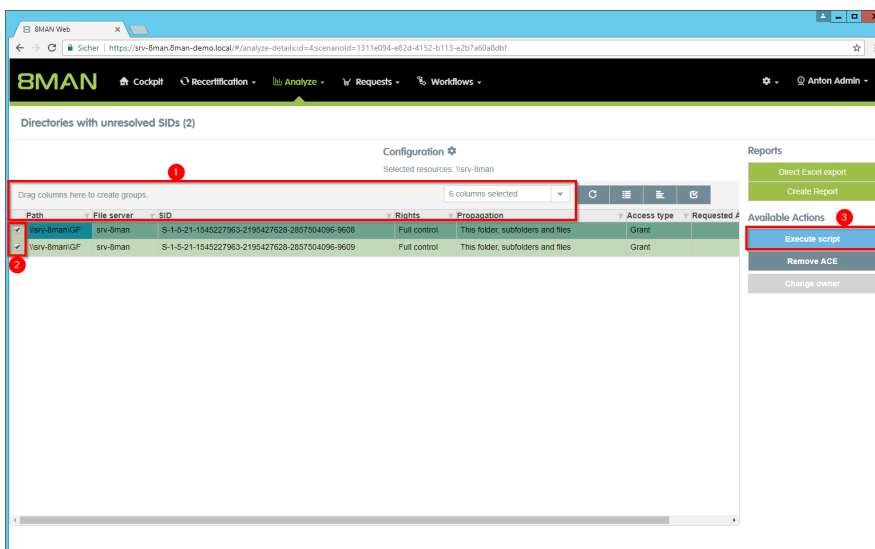


1. Select "New analyze session".
2. Choose a scenario with directories in focus.

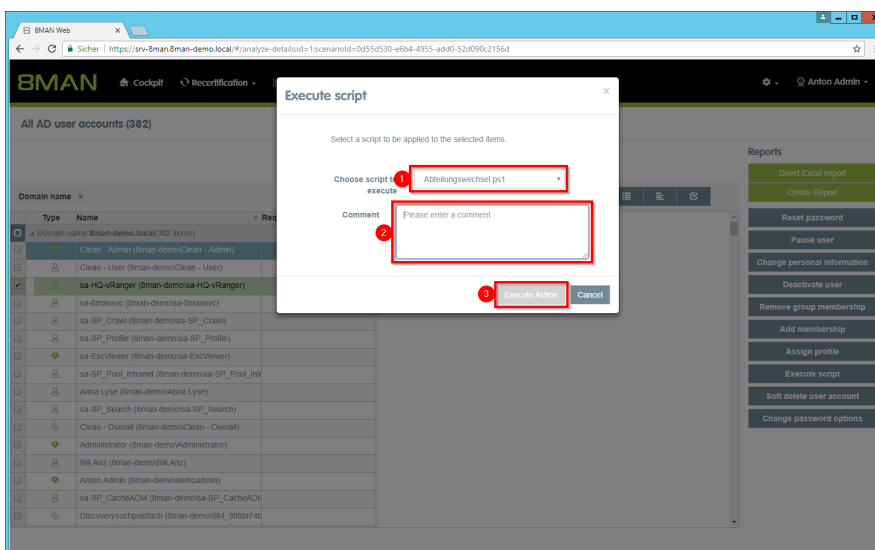




1. Set the scenario options.
2. Start the calculation.



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



1. Select a script.
2. You must enter a comment.
3. Click on "Execute action".

### 8.1.1.18 Execute scripts on user accounts in bulk (web client)

#### Background / Value

Use self-created scripts on directories. 8MAN opens up space for very individual requirements. Put your scripts in the following directory to use with 8MAN:

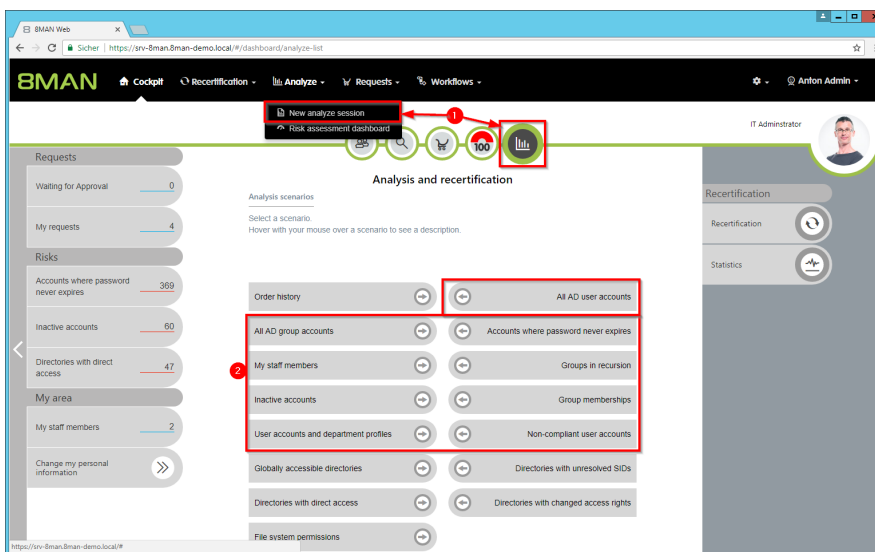
%ProgramData%\protected-networks.com\8MAN\scripts\analyze

Further necessary steps and details for configuring scripts can be found in the Installation and Configuration Manual.

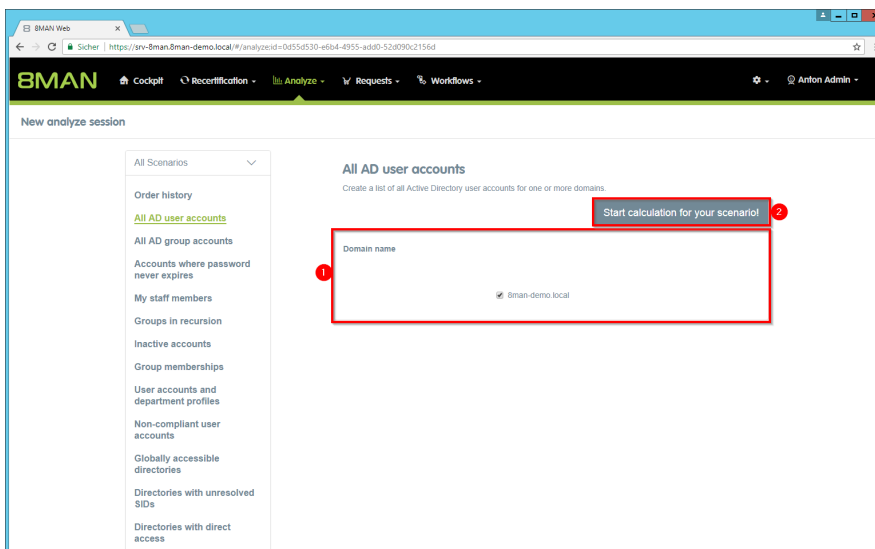
#### Additional Services

[Execute scripts on directories in bulk](#) (web client)

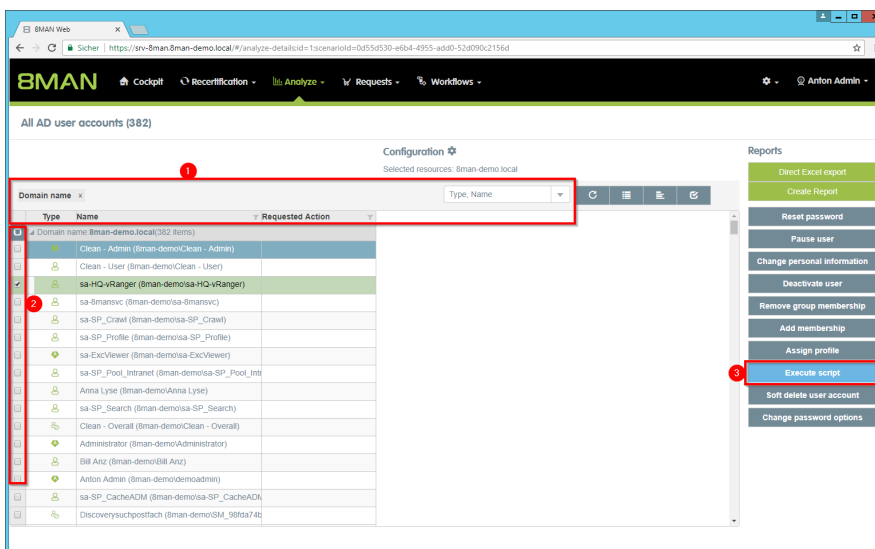
#### Step by step process



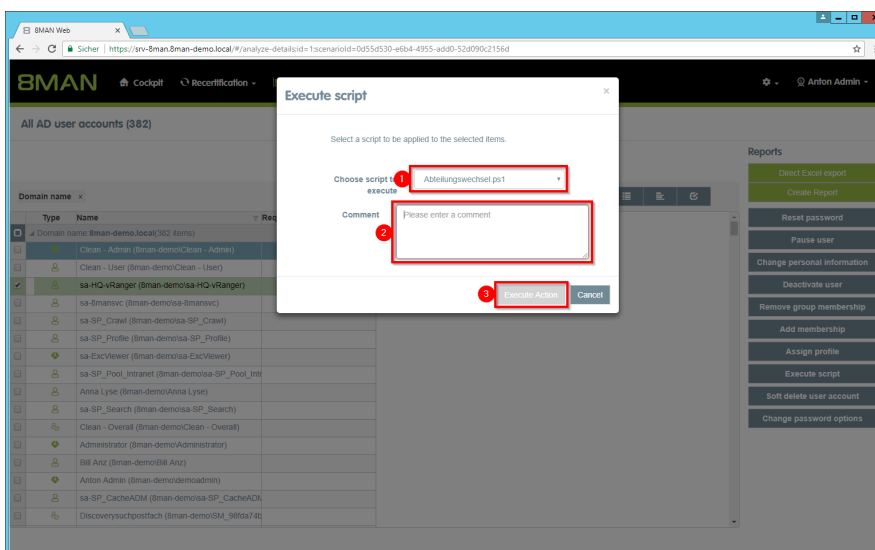
1. Select "New analyze session".
2. Choose a scenario with accounts in focus.



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.
2. You must enter a comment.
3. Click on "Execute action".

### 8.1.1.19 Edit temporary group memberships (web client)

#### Background / Value

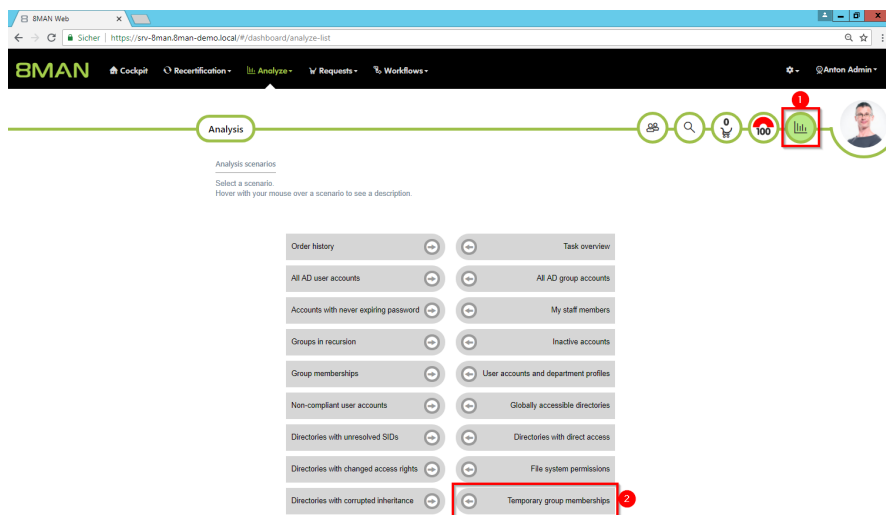
Simply change the expiration date of temporary group memberships or convert them to a permanent membership. You can also easily remove temporary memberships.

#### Related Services

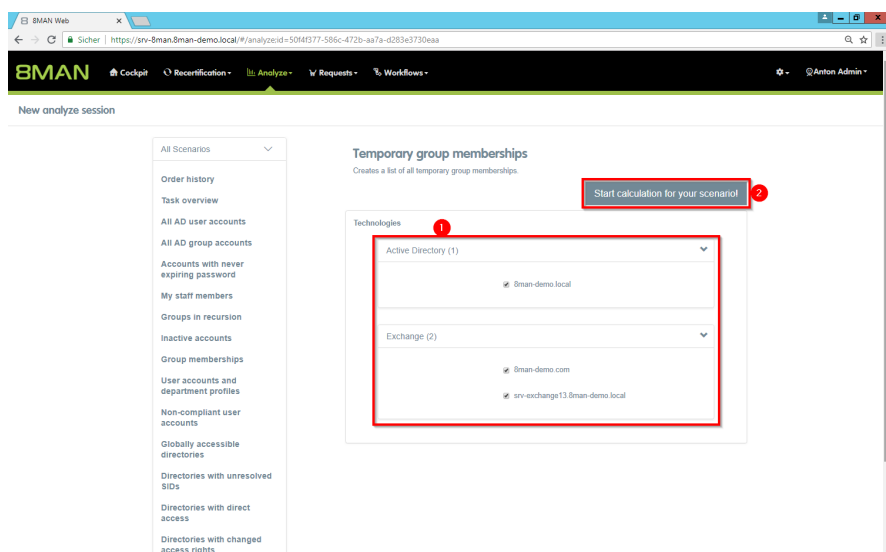
[Remove group memberships \(cockpit\)](#)

[Add group memberships \(cockpit\)](#)

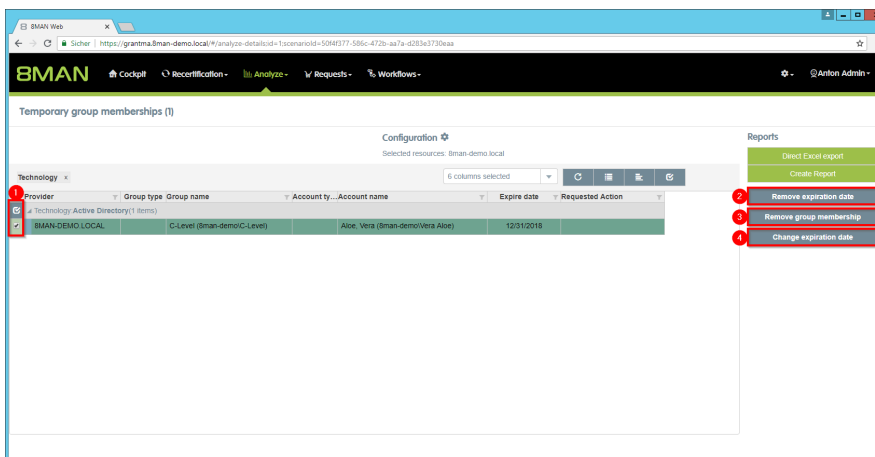
#### Step by step process



1. Select "Analysis" in the cockpit.
2. Click on "Temporary group memberships".



1. Select the resources you want to include in your analysis.
2. Start the analysis.



1. Select the required group memberships.
2. Remove the expiration date. This is how you convert the temporary membership into a permanent group membership.
3. End the group membership immediately (before the expiration date).
4. Change the expiration date.

### 8.1.1.20 Edit computer accounts

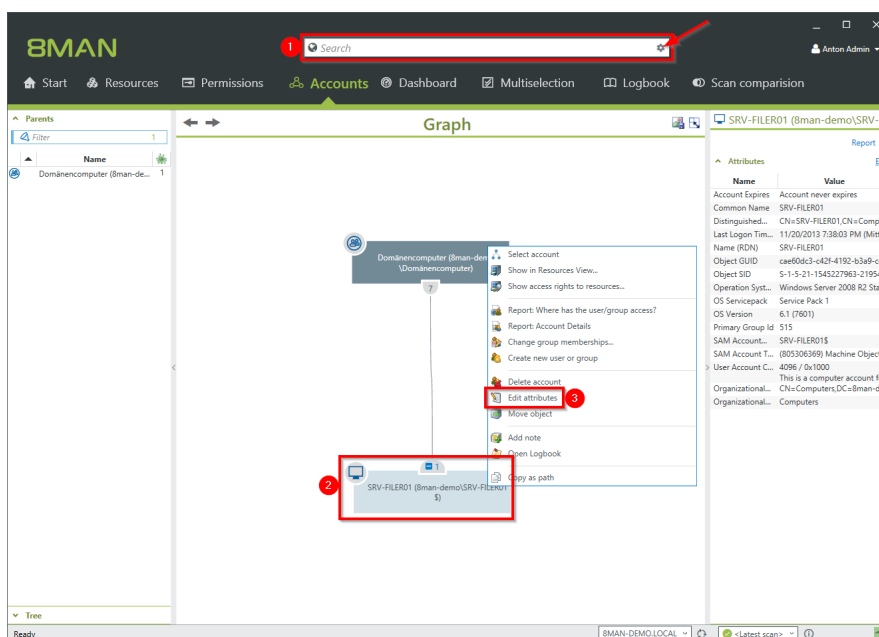
#### Background / Value

Maintain computer accounts comfortably and documented within 8MAN.

#### Additional Services

[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".

Edit attributes

Status of changes: ...

Active Directory change credentials [8man-demo\administrator](#)

SRV-FILER01 (8man-demo\SRV-FILER01\$)

Name	Value
Common Name	SRV-FILER01
Comment	Attribute value is not given
Company	Attribute value is not given
Department	Attribute value is not given
Description	demo description
Display Name	Attribute value is not given
Information	Attribute value is not given
managedby	Attribute value is not given
operationsystem	Attribute value is not given
OS Servicepack	Service Pack 1
OS Version	6.1 (7601)
SAM Account Name	SRV-FILER01\$
Script-Path	Attribute value is not given

Please add a comment

1. Change the attributes.  
8MAN loads a standard set of attributes. If additional attributes of computer accounts are to be loaded in 8MAN, please contact our support.
2. You must enter a comment.
3. Start the execution.

8.1.1.21 Delete computer accounts

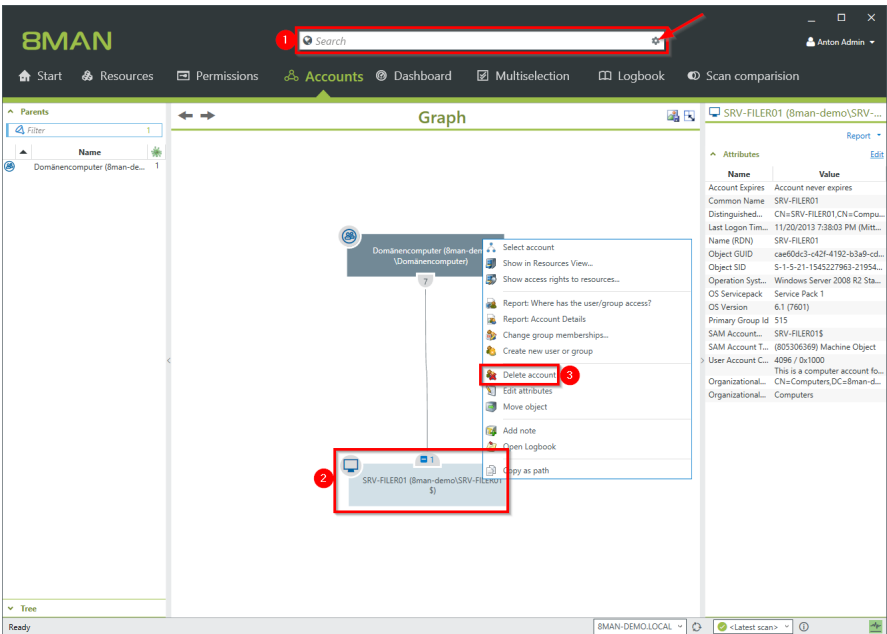
Background / Value

Delete computer accounts comfortably and documented within 8MAN.

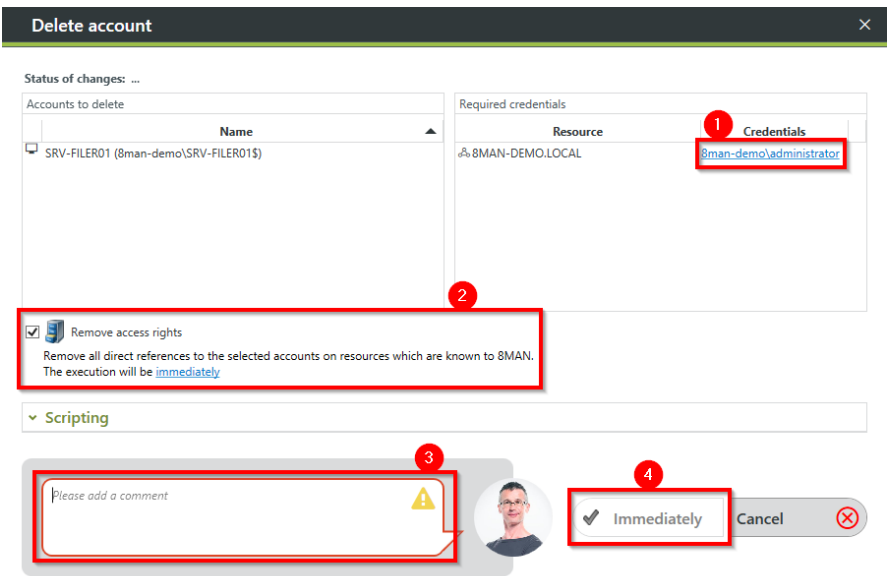
Additional Services

[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.



## 8.1.2 Helpdesk

### 8.1.2.1 Reset passwords

#### Background / Value

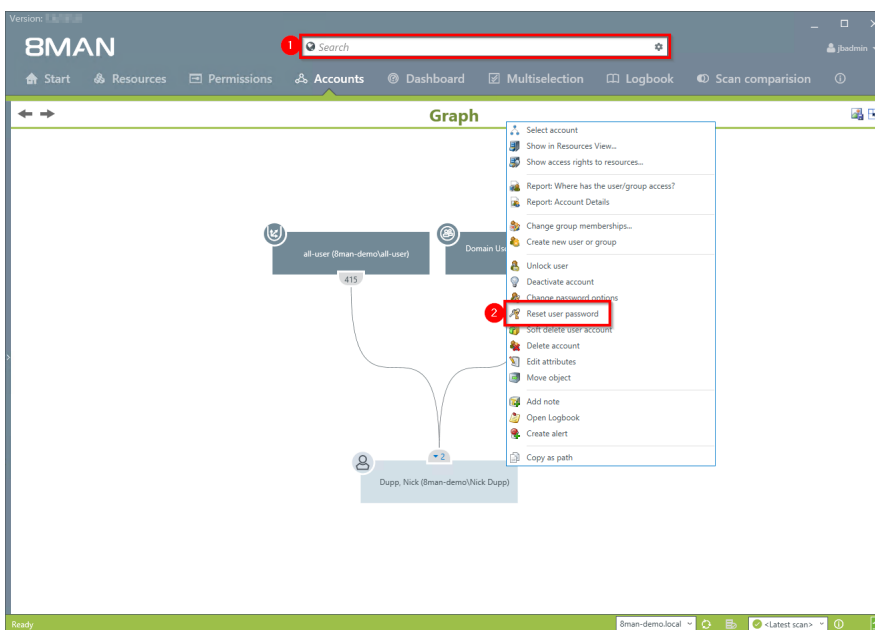
Resetting passwords is one of the most common tasks performed by help desks. 8MAN allows an easy and secure way of resetting passwords. All sensitive actions are documented in the log book. If an employee uses native tools to reset a password and illegally tries to access that user account, the incident is captured with AD Logga. Especially sensitive user accounts can be monitored with 8MATE AD Logga alerts.

#### Additional services

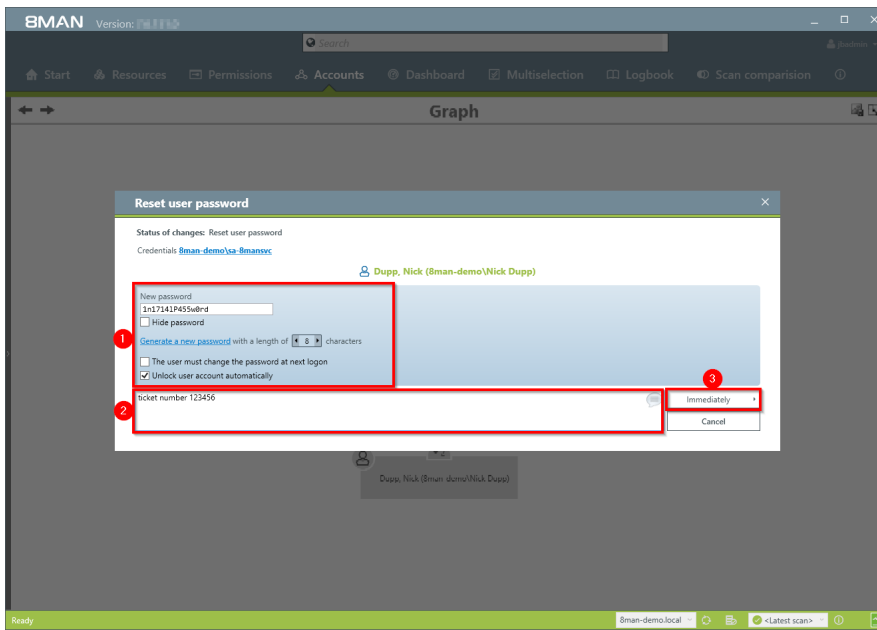
[8MATE AD Logga: Identify locked accounts](#)

[8MATE AD Logga: Monitor a user account](#)

#### Step by step process



1. Use the search field to find the desired user.
2. Right-click on the user and select "reset user password". You can do this in the accounts view.



1. Determine your password options.
2. You must enter a comment, for example "ticket number" or "authorized by".
3. Start the reset process.

### 8.1.2.2 Reset passwords in bulk (web client)

#### Background / Value

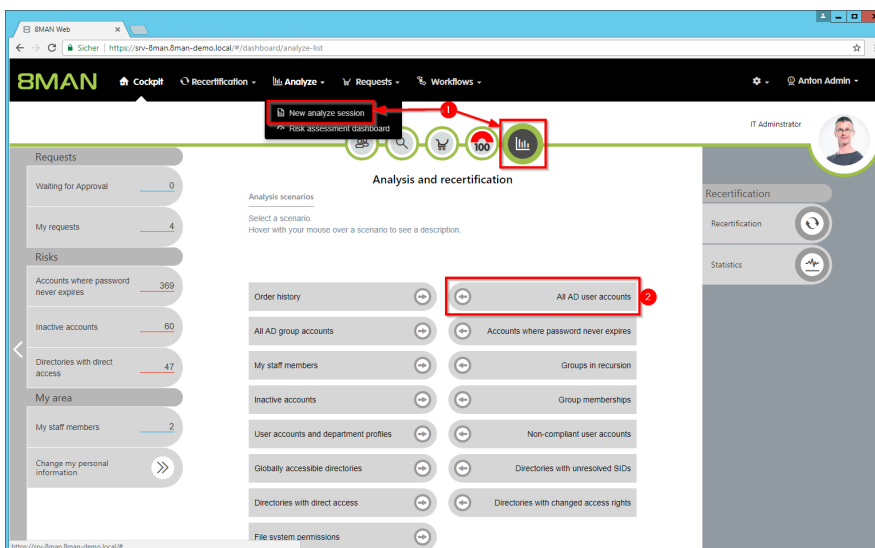
There are many use cases in which the passwords of several users must be reset simultaneously. You can reset passwords in bulk in the web interface.

#### Additional Services

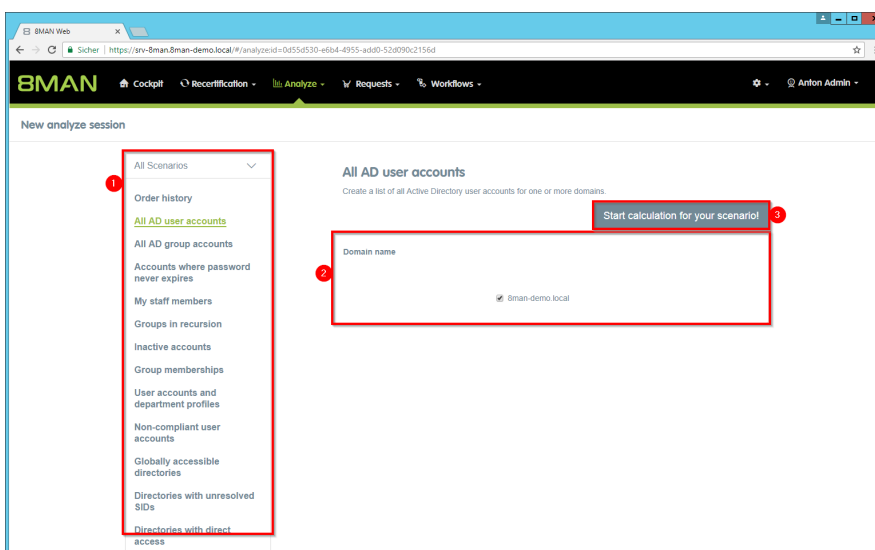
[Deactivate user accounts in bulk](#) (web client)

[Change password options in bulk](#) (web client)

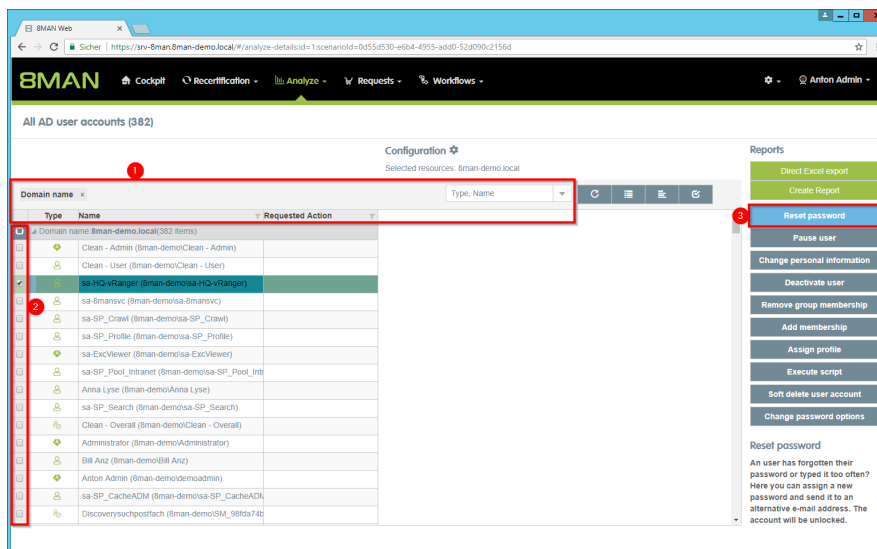
#### Step by step process



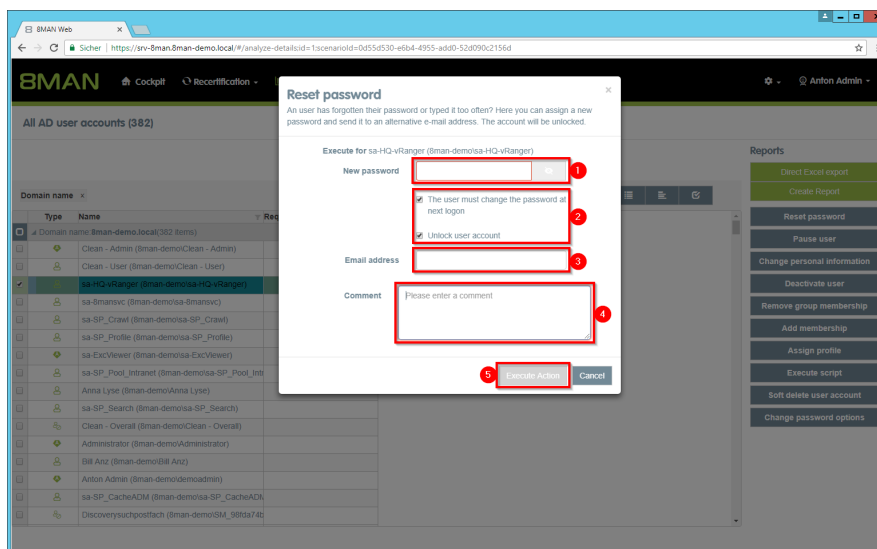
1. Select "New analyze session".
2. Click on "All AD user accounts".



1. Optional: Change the scenario.
2. Set options for the scenario.
3. 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 8MAN administrators. For all other 8MAN 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 8MAN server and executed there. 8MAN shows the status in the "Jobs overview".

### 8.1.2.3 Unlock an user account

#### Background / Value

Unlocking user accounts is one of the most frequently performed action of most help desks. 8MAN makes the password reset revision proof. All actions are documented in the logbook.

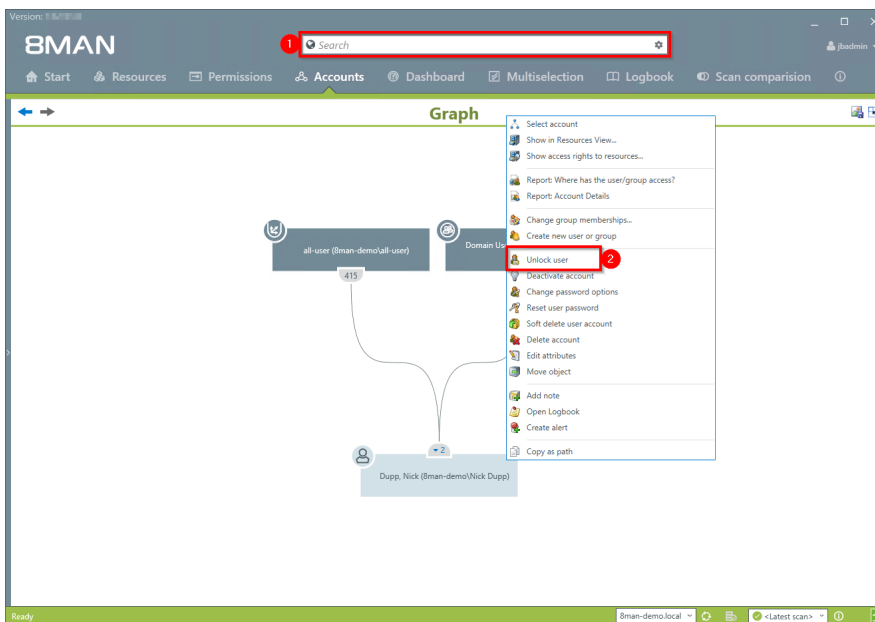
#### Additional Services

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](#).

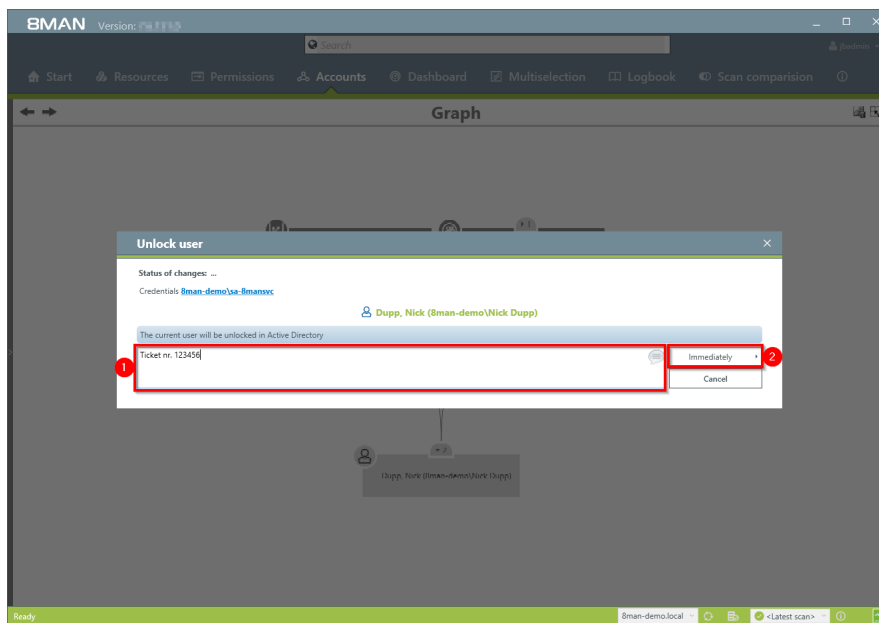
[8MATE AD Logga: Identify locked user accounts](#)

[8MATE AD Logga: Monitor a user account](#)

#### Step by step process



1. Use the search field to find the desired user or group.
2. Right-click on the user or group and select "Unlock user" from the context menu. You can do this in the accounts view.



1. You must enter a comment, for example "ticket number" or "authorized by".
2. Start the unlocking process.

### 8.1.2.4 Unlock user accounts (web client)

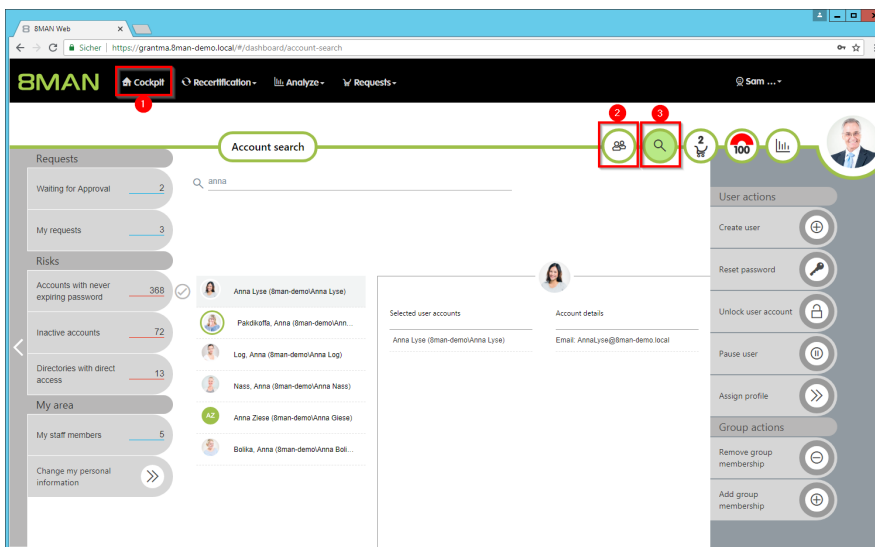
#### Background / Value

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.

#### Related Services

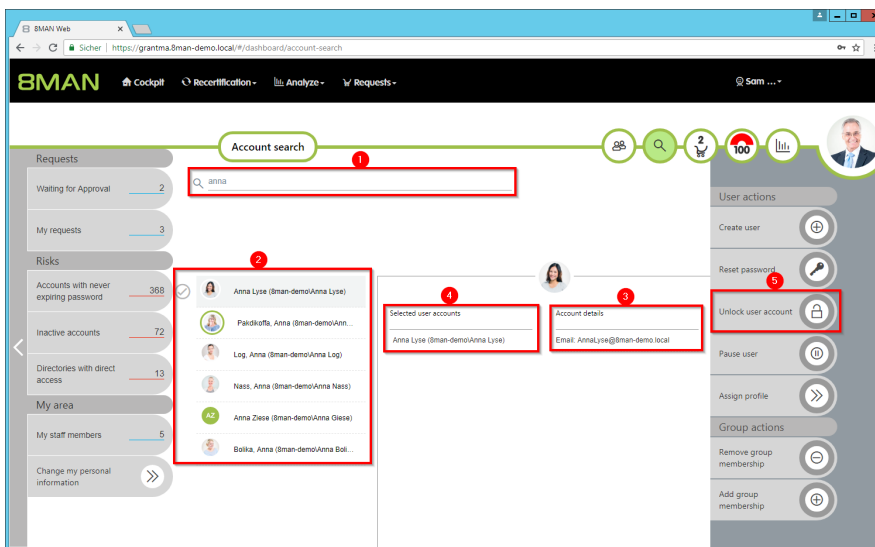
[Reset users' passwords \(Cockpit\)](#)

#### Step by step process

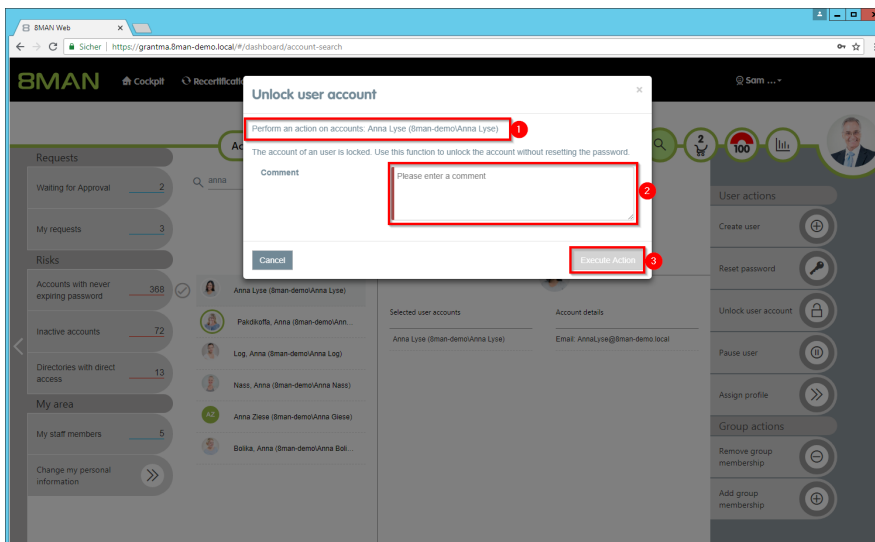


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See [Changing Attributes \(Web Client\)](#).
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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. 8MAN 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. 8MAN shows you on which accounts the action should be performed.
2. You must enter a comment.
3. Click "Execute action".



### 8.1.2.5 Deactivate an user account

#### Background / Value

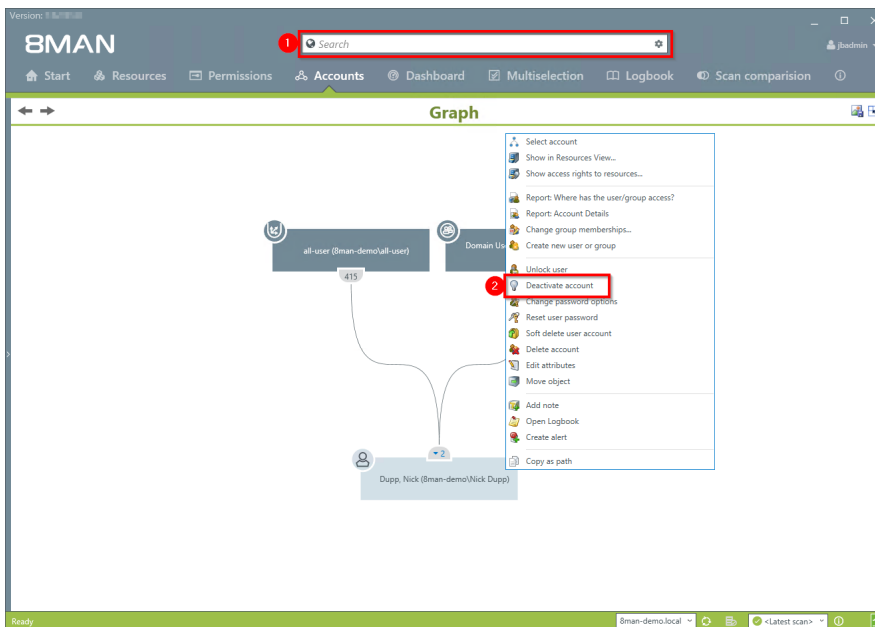
If you deactivate an account with 8MAN, this is equivalent to a normal deactivation in Active Directory. The user account remains in the OU.

#### Additional services

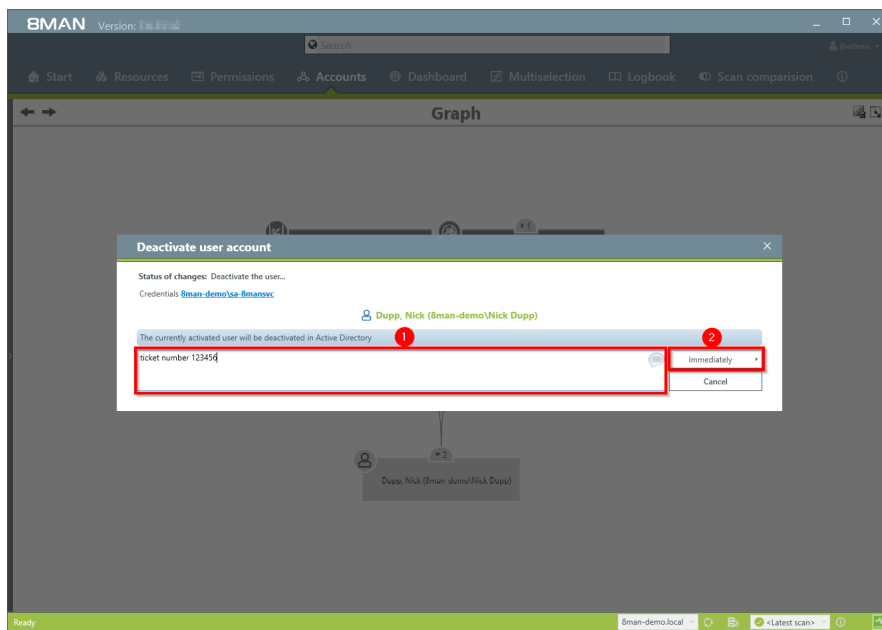
[Delete a user with soft delete](#)

[Deactivate accounts in bulk](#) (web client)

#### Step by step process



1. Use the search field to find the desired user.
2. Right-click on the user and select "deactivate account" from the context menu. You can do this in the accounts view.



1. You must enter a comment, for example "ticket number" or "authorized by".
2. Start the execution.

### 8.1.2.6 Modify group and user attributes

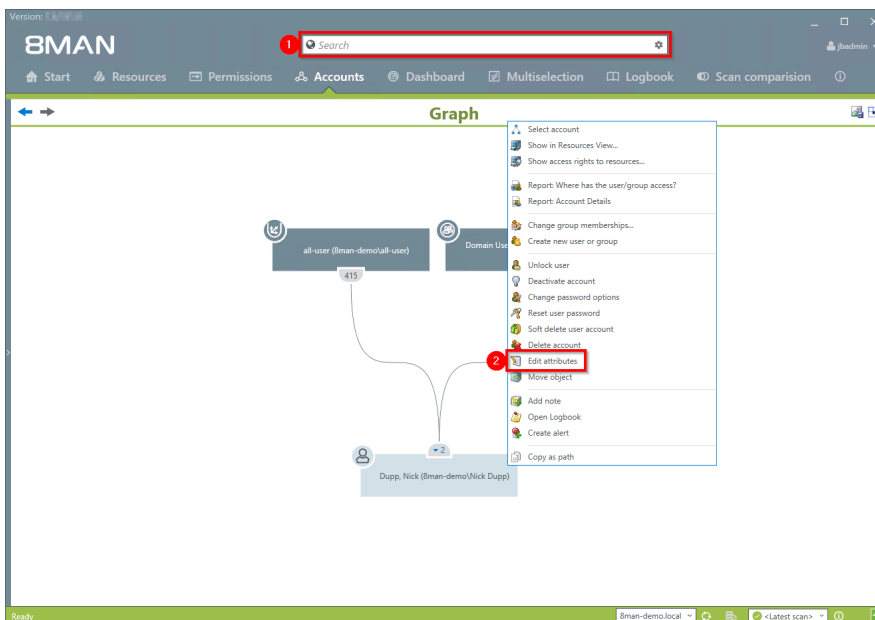
#### Background / Value

With 8MAN you can easily manage attributes for users accounts in a flat list. All actions are automatically documented.

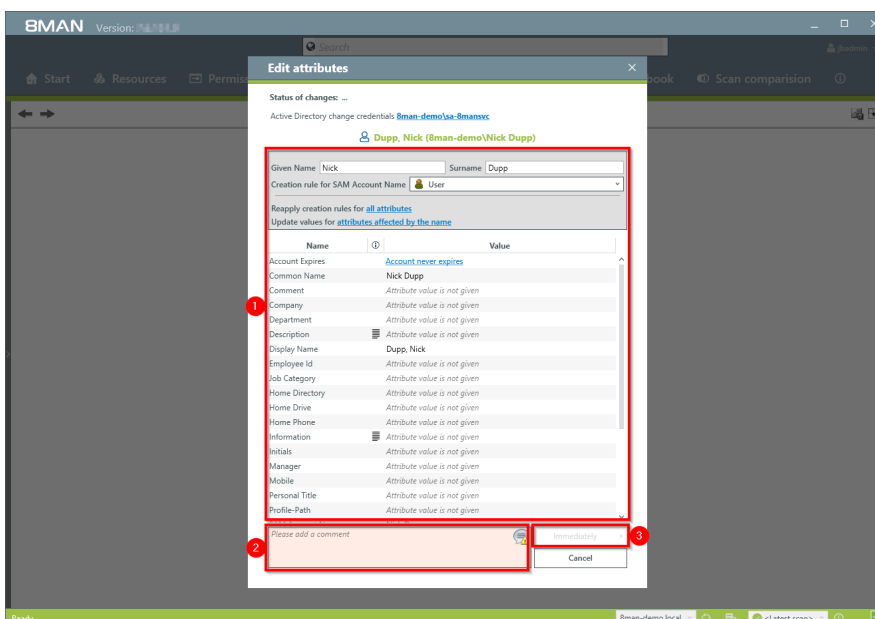
#### Additional Services

Modify attributes in bulk (web client)

#### Step by step process



1. Use the search field to find the desired user or group.
2. Right-click on the user or group. You can do this in the accounts view.



1. Change the desired attributes.
2. You must enter a comment.
3. Start the execution.



### 8.1.2.7 "Soft" delete a user

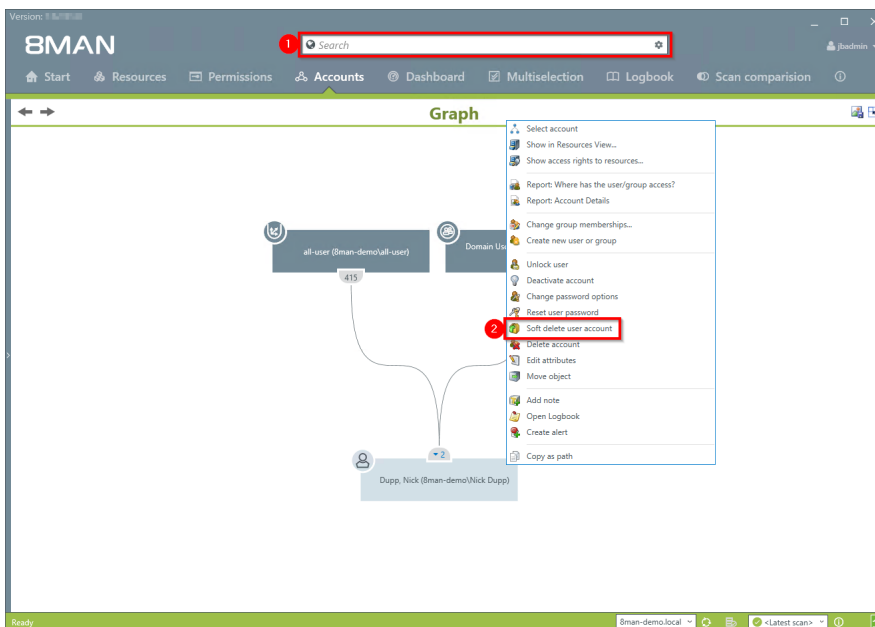
#### Background / Value

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

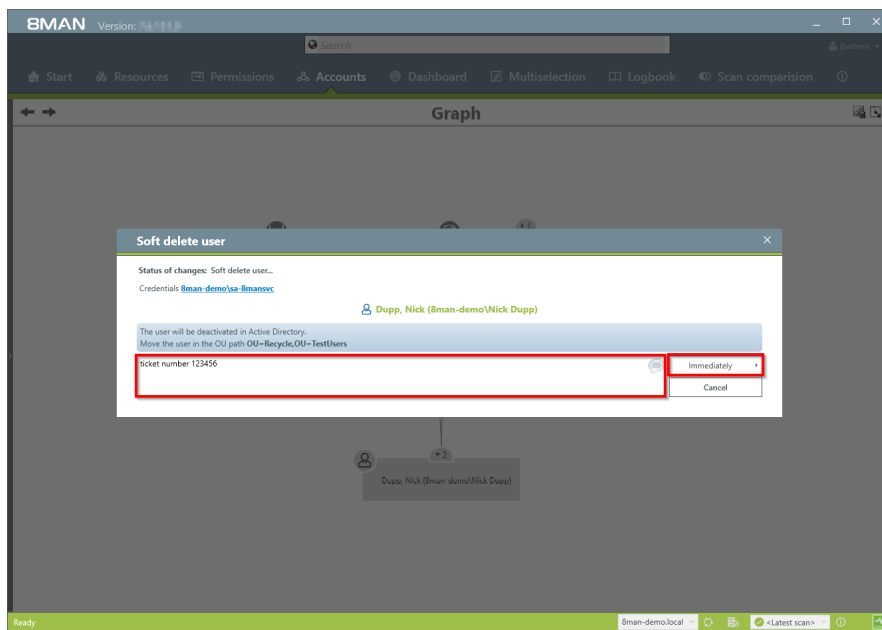
#### Further Services

Set the "recycle-OU"

#### Step by step process



1. Use the search field to find the desired user.
2. Right-click on the user and select "soft delete account" from the context menu. You can do this in the accounts view.



1. You must enter a comment, for example "ticket number" or "authorized by".
2. Start the process.

### 8.1.2.8 Remove a user and its permissions

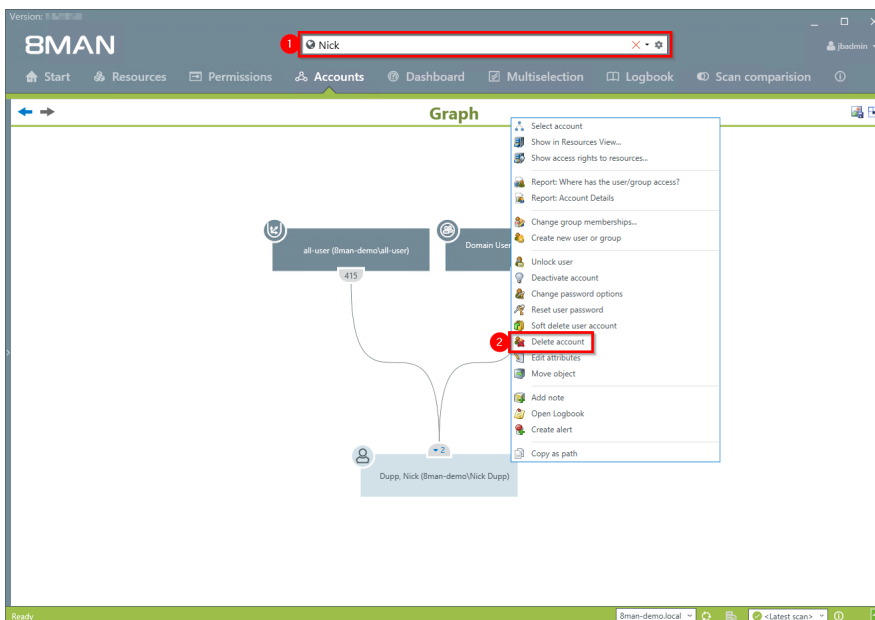
#### Background / Value

With 8MAN you can delete the user from AD and remove all of their access rights on the file server in one easy action.

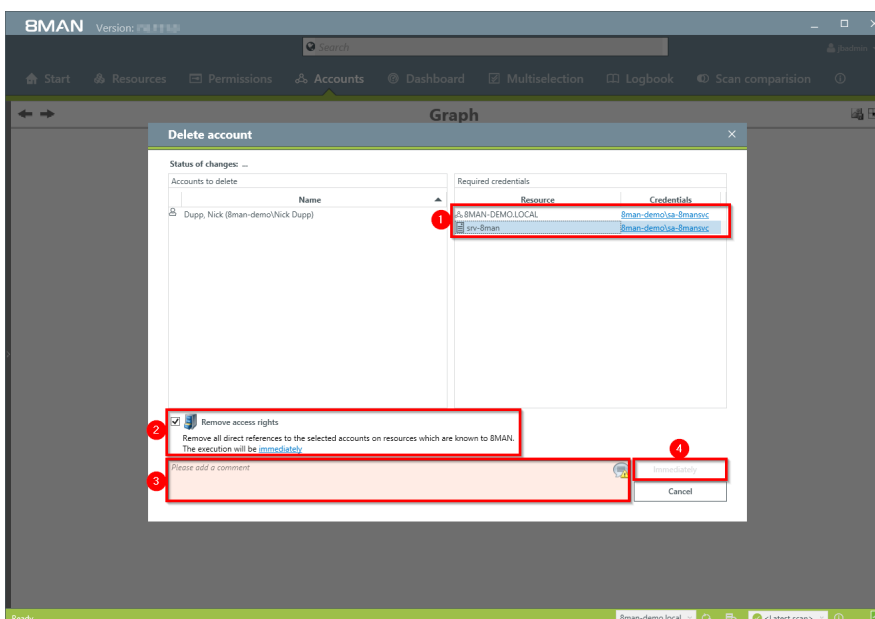
#### Additional Services

[Remove direct permissions in bulk](#) (web client)

#### Step by step process



1. Use the search field to find the desired user.
2. Right-click on the user and select "Delete account" from the context menu. You can do this in the accounts view.



1. If required change the credentials to remove the access rights.
1. Activate the option "Remove access rights" to avoid unresolved SIDs on file servers.
2. You must enter a comment, for example "ticket number" or "authorized by".
3. Start the process.





## 8.1.3 Data Owner/Manager

### 8.1.3.1 Reset users' passwords (cockpit)

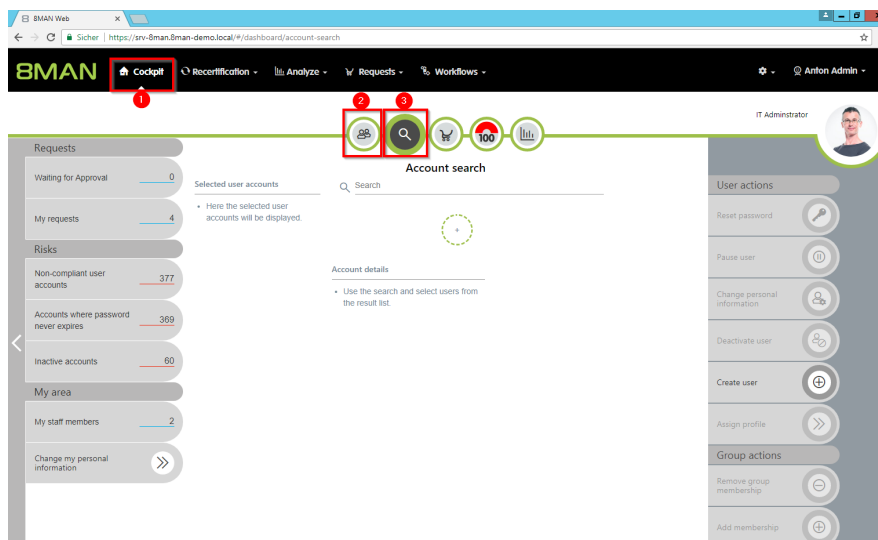
#### Background / Value

Resetting passwords is one of the most common operations in the help desk. 8MAN enables revision-proof password reset. The safety-critical action is recorded in the logbook.

#### Additional Services

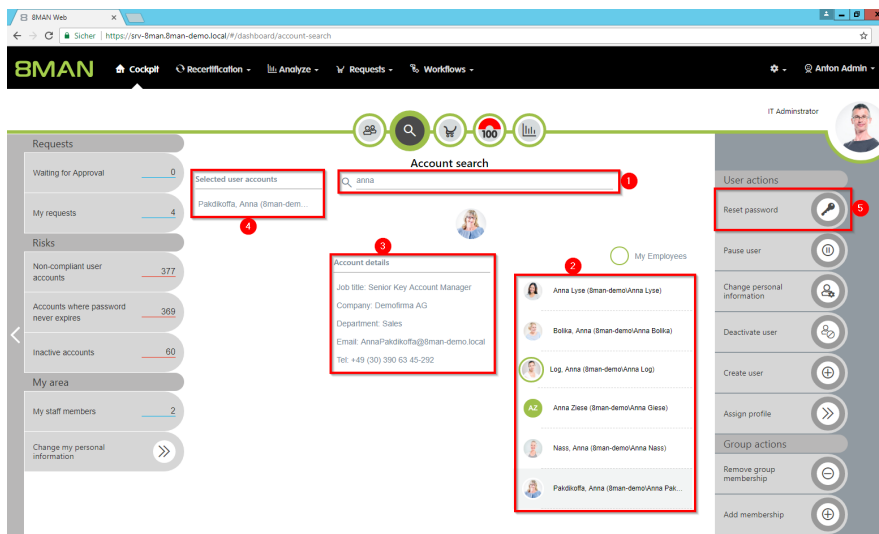
Overview of all cockpit services

#### Step by step process

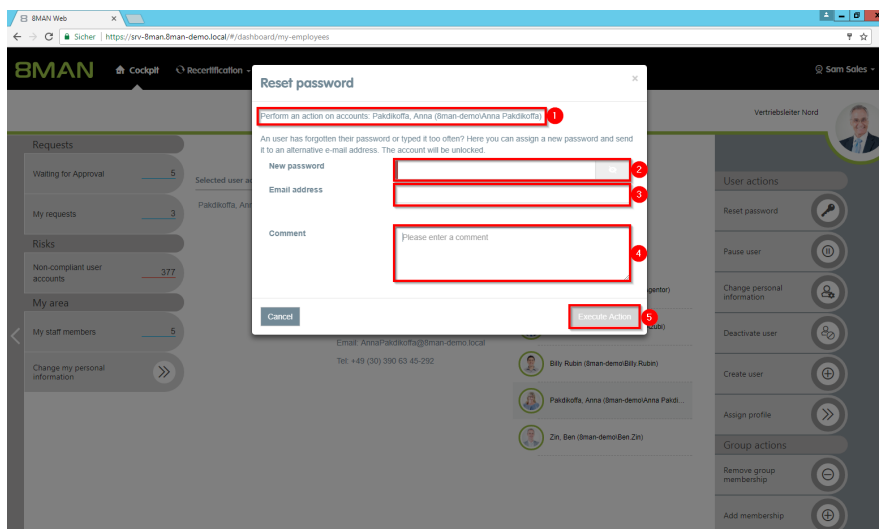


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See [Changing Attributes \(Web Client\)](#).
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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. 8MAN 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 "Reset Password".



1. 8MAN 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".

### 8.1.3.2 Change account data of users (cockpit)

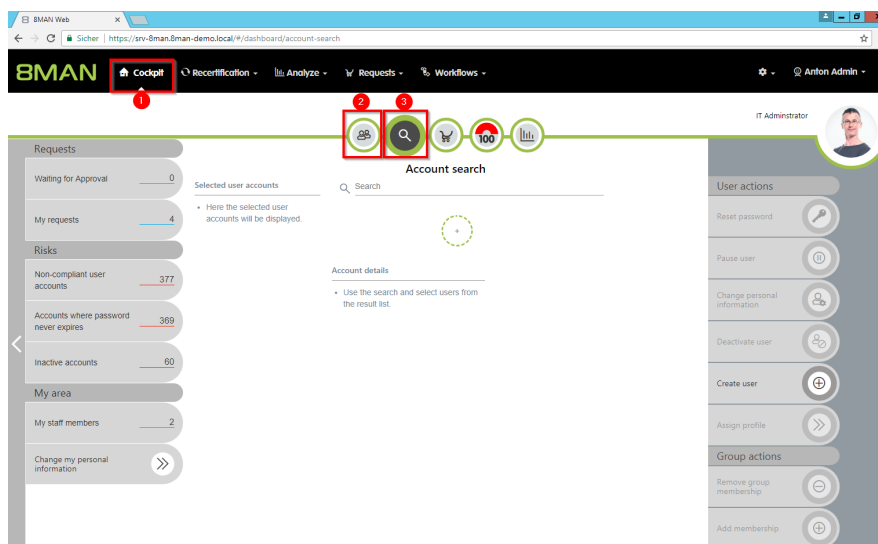
#### Background / Value

With 8MAN, you can quickly and easily change user account information, even from multiple users in one go. The actions are documented auditable.

#### Additional Services

Overview of all cockpit services

#### 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. See [Changing Attributes \(Web Client\)](#).
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.
1. Select one or more users.
2. 8MAN shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
3. In the collection you can see already selected users.
4. Click "Change personal information".

8MAN Web

https://sn-8man.8man-demo.local/#/dashboard/my-employees

8MAN

Cockpit

Reconciliation

Perform an action on accounts: Pakdikofka, Anna (8man-demo/Anna Pakdikofka)

Change the account information for a user

Company: Demofirma AG

Department: Sales

Location:

ZIP:

Street:

Description:

Information:

Comment: Please enter a comment

Cancel

Execute Action

Vertreter Nord

User actions

Reset password

Pause user

Change personal information

Deactivate user

Create user

Assign profile

Group actions

Remove group membership

Add membership

1. 8MAN shows you which accounts you have selected.
2. Enter the desired changes.
3. You must enter a comment.
4. 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 our [knowledgebase](#) (login required).

### 8.1.3.3 Deactivate users (cockpit)

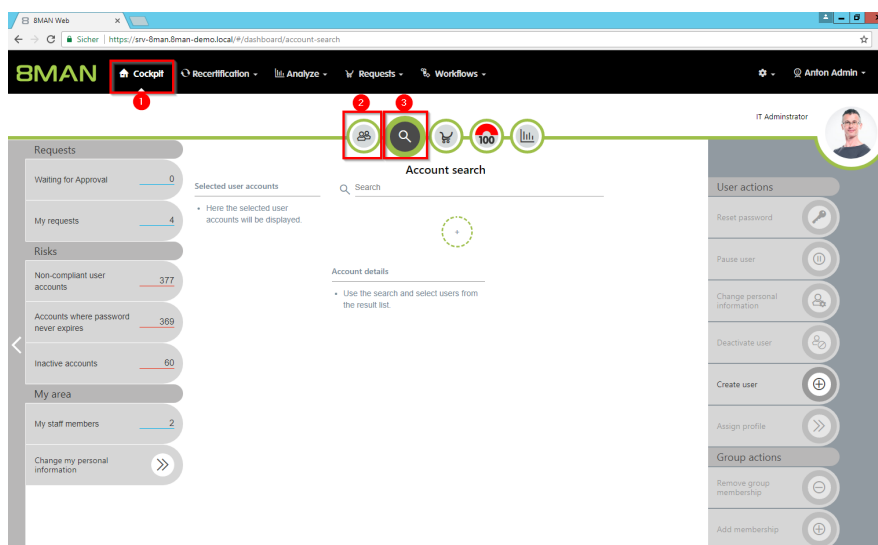
#### Background / Value

Disable a user in a few steps with 8MAN. Disable a user account early on discharge.

#### Additional Services

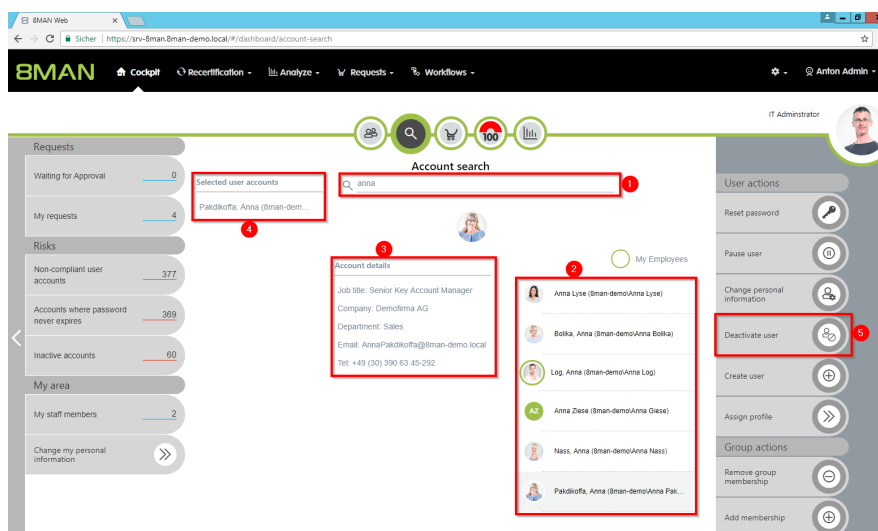
Overview of all cockpit services

#### Step by step process

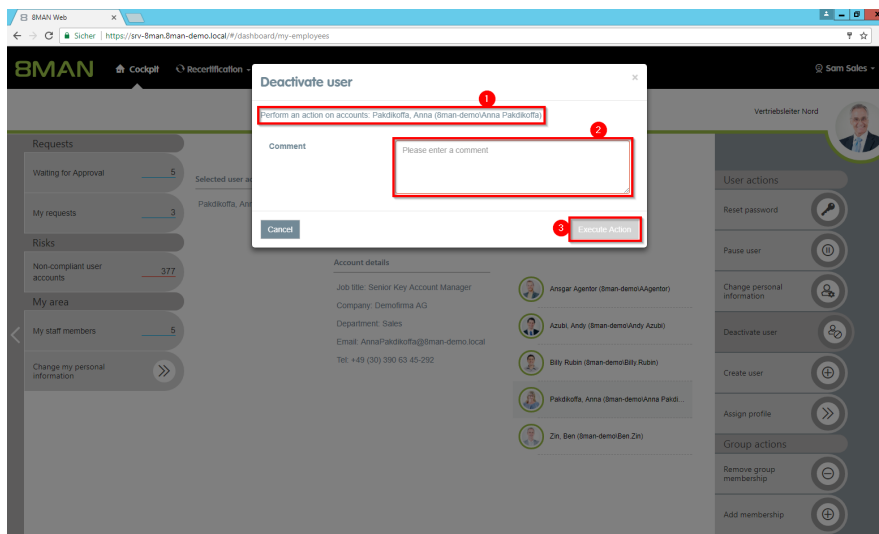


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See [Changing Attributes \(Web Client\)](#).
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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.
1. Select one or more users.
2. 8MAN shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
3. In the collection you can see already selected users.
4. Click "Deactivate user".



1. 8MAN shows you which accounts you have selected and want to deactivate.
2. You must enter a comment.
3. Click on "Execute Action".

### 8.1.3.4 Pause user (cockpit)

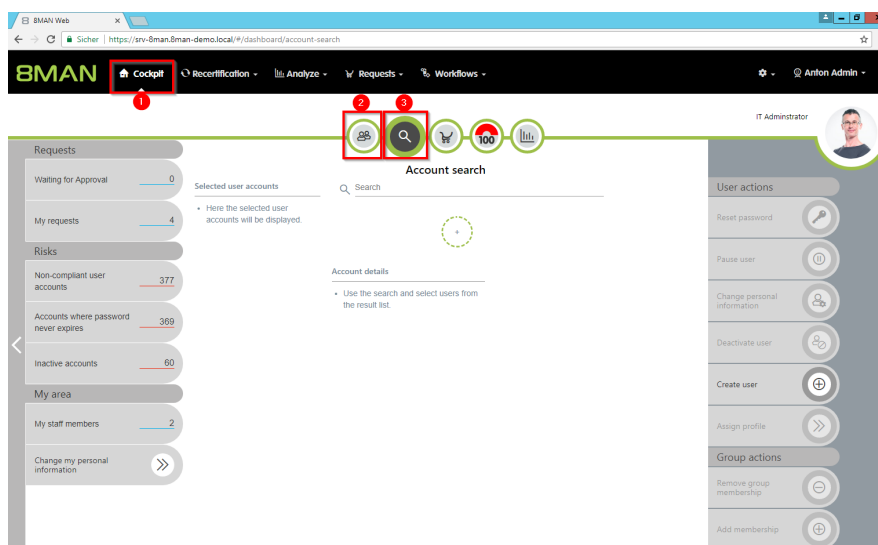
#### Background / Value

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

#### Additional Services

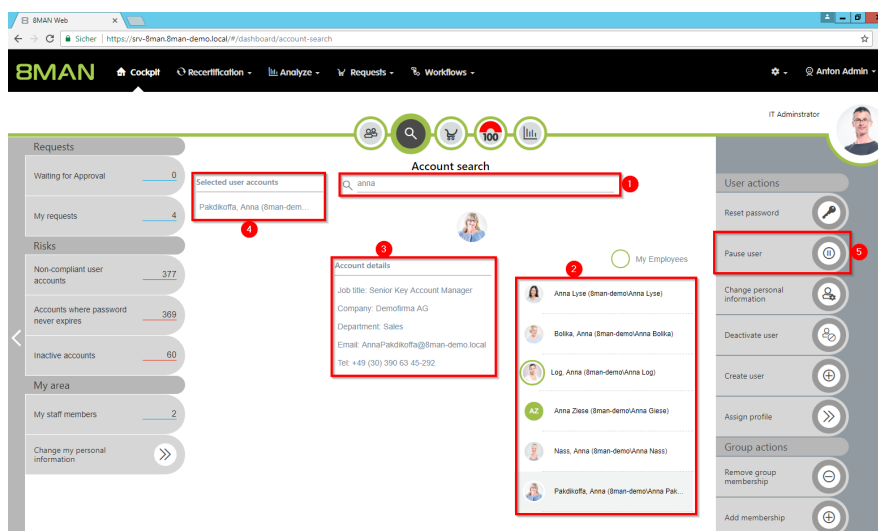
Overview of all cockpit services

#### Step by step process

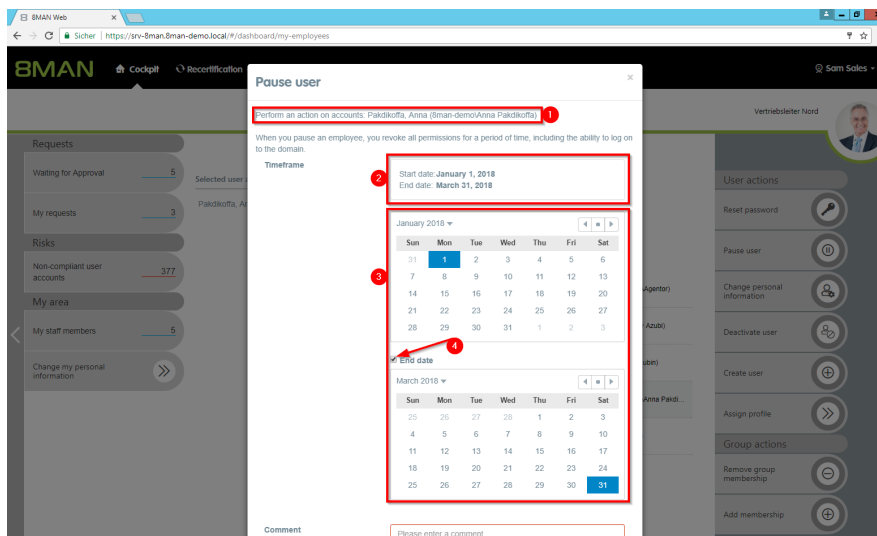


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See [Changing Attributes \(Web Client\)](#).
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

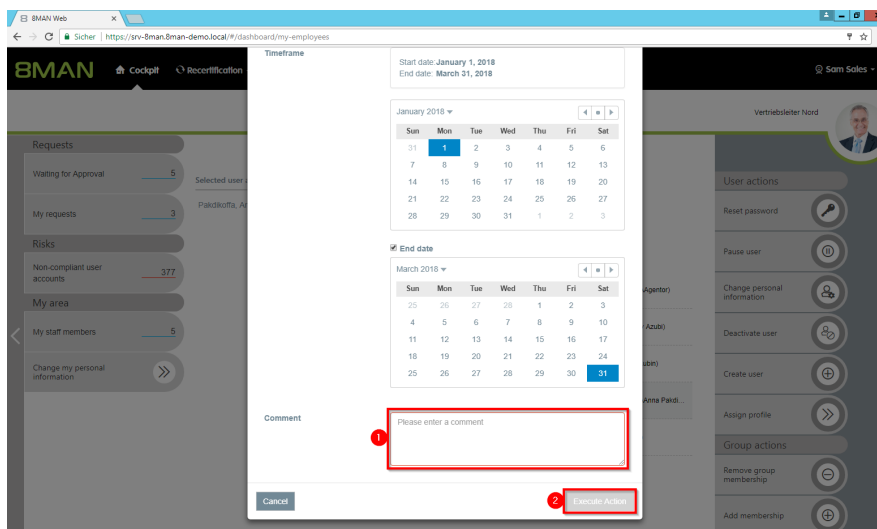
The range of available services (buttons) varies according to role (login), risk assessment and configuration.



1. Use the search to filter a long list of employees or search for users.
1. Select one or more users.
2. 8MAN shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
3. In the collection you can see already selected users.
4. Click "Pause user".



1. 8MAN shows you which accounts you have selected and want to pause.
2. 8MAN shows the start and end dates.
3. Choose the beginning and the end.
4. If the break is perpetual, deactivate the option "End date".



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



### 8.1.3.5 Create a new user (cockpit)

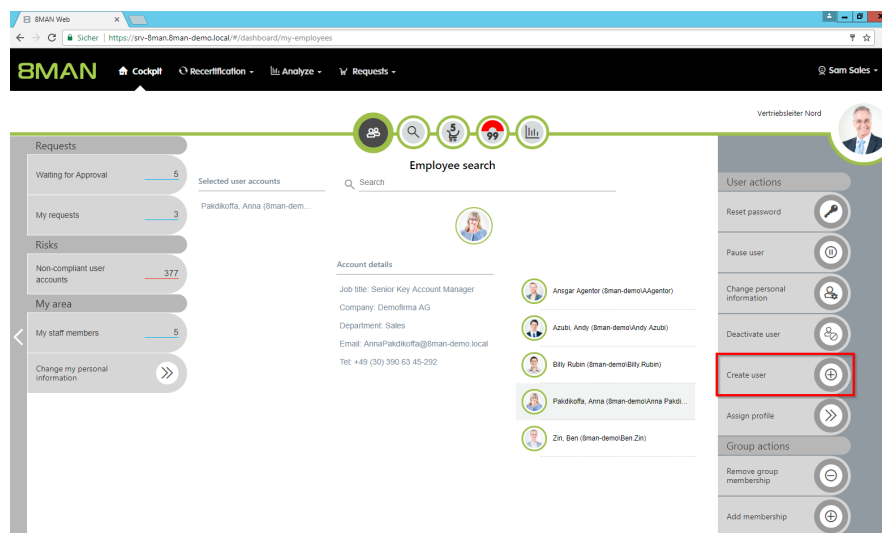
#### Background / Value

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

#### Additional Services

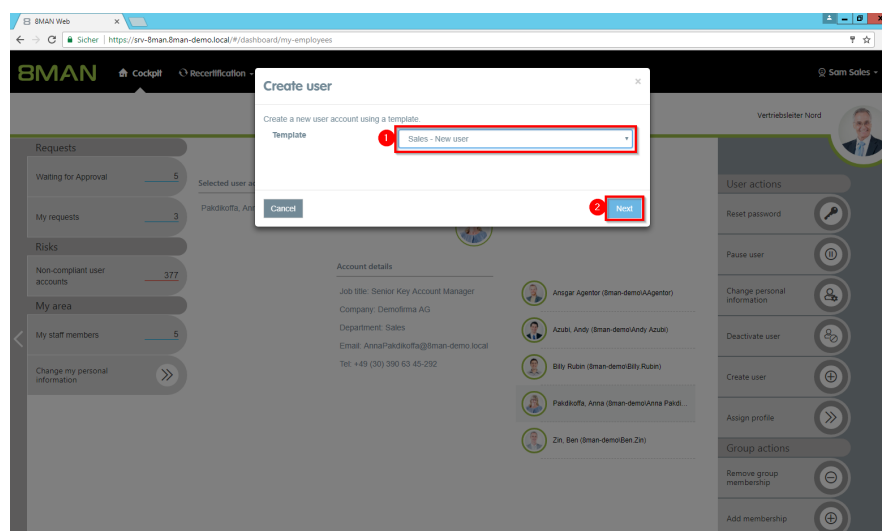
Overview of all cockpit services

#### Step by step process



1. Click on "Create new 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".

### 8.1.3.6 Assign a department profile to users (cockpit)

#### Background / Value

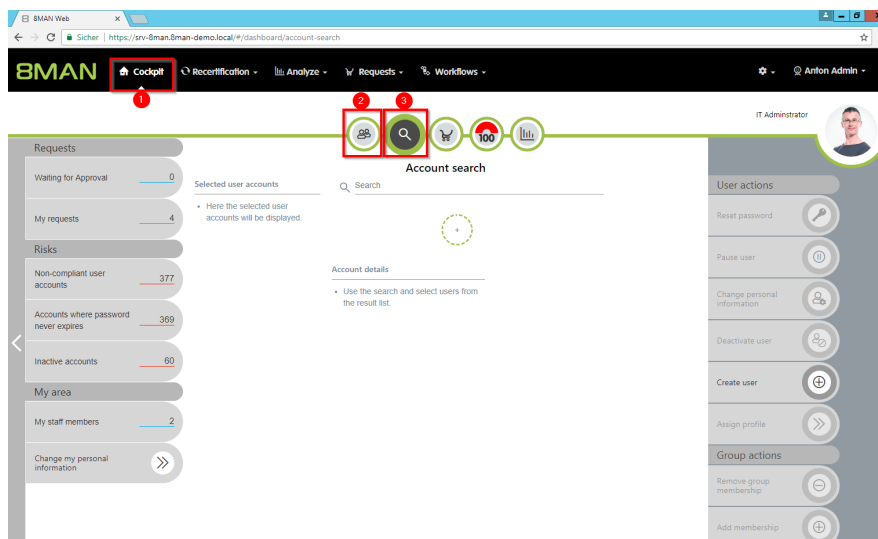
With a department profile, you can assign a basic set of permissions to a user in just a few clicks. If the employee changes department, the supervisor can easily apply his department profile to the corresponding user account.

#### Additional Services

[Create a new department profile](#)

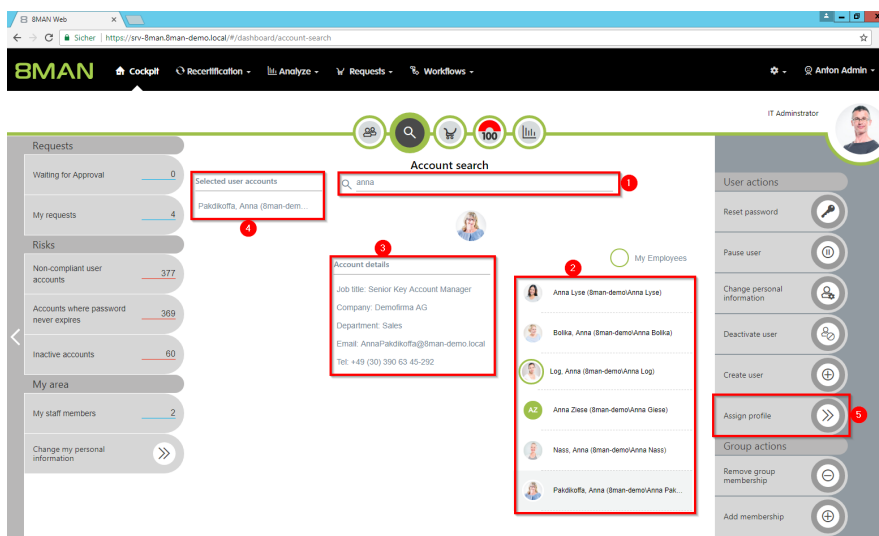
[Determine permissions deviating from the department profile \(Compliance Check\)](#)

#### Step by step process

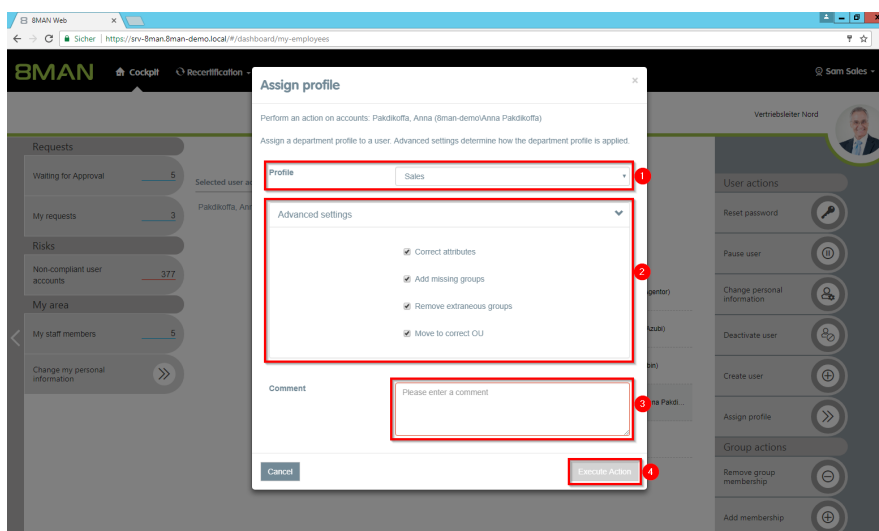


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See [Changing Attributes \(Web Client\)](#).
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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.
1. Select one or more users.
2. 8MAN shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
3. In the collection you can see already selected users.
4. 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".

### 8.1.3.7 Change your own account information (cockpit)

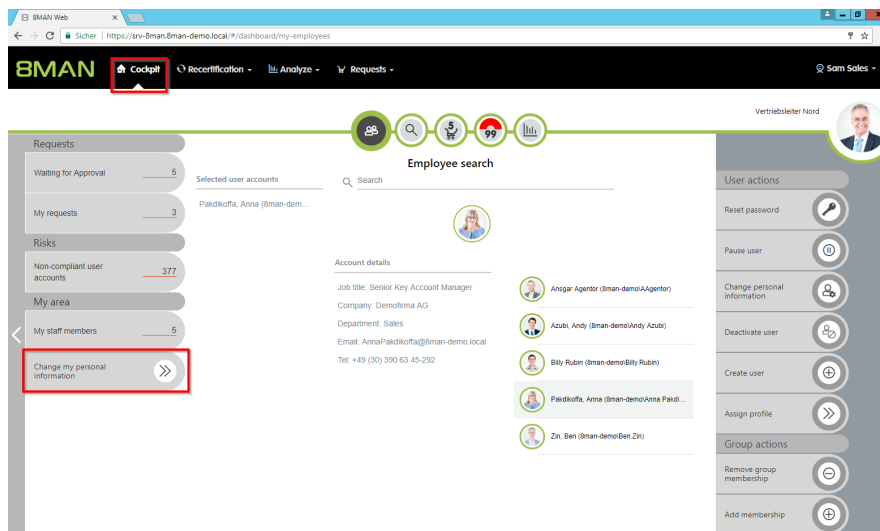
#### Background / Value

With 8MAN you can quickly and easily change your own account information. The actions are documented auditable.

#### Additional Services

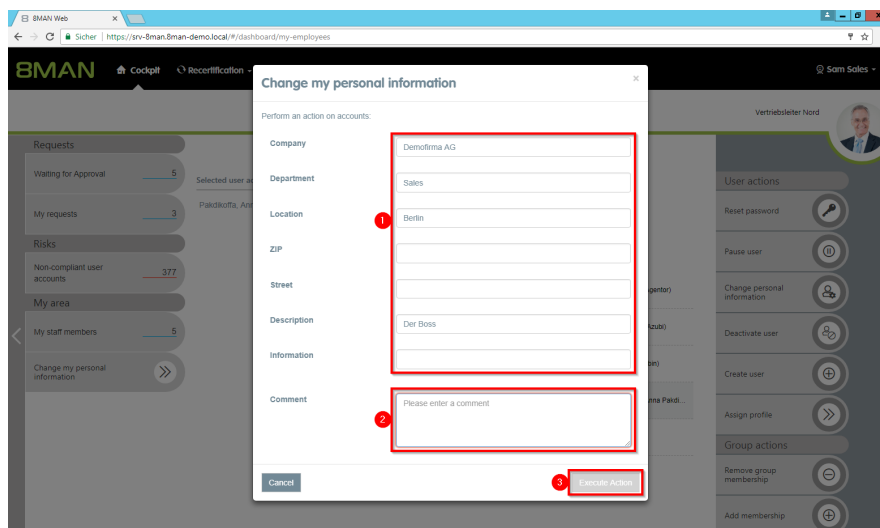
Overview of all cockpit services

#### 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. For this purpose, an adjustment of the configuration file must be made. Instructions can be found in our [knowledgebase](#) (login required).

8.1.3.8 Manage my employees (cockpit)

Background / Value

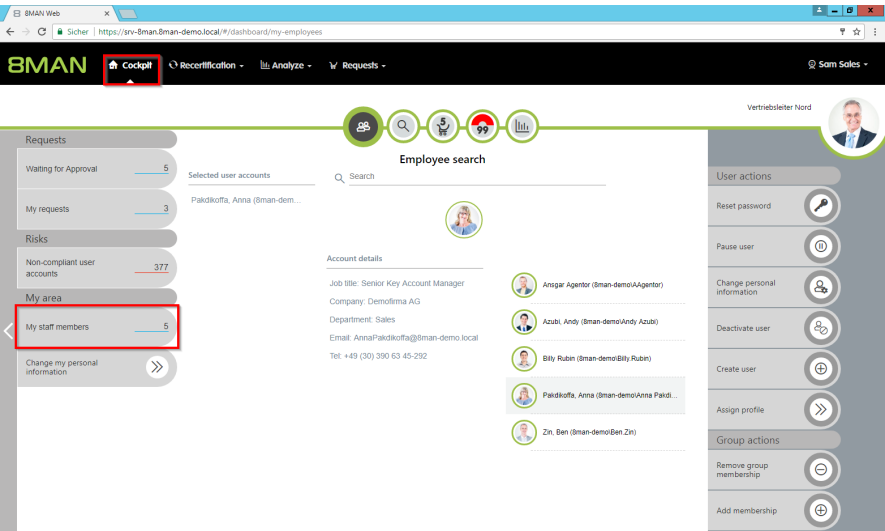
With 8MAN you can quickly and easily manage your assigned employees. Actions are documented for the revision.

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

Additional Services

Overview of all cockpit services

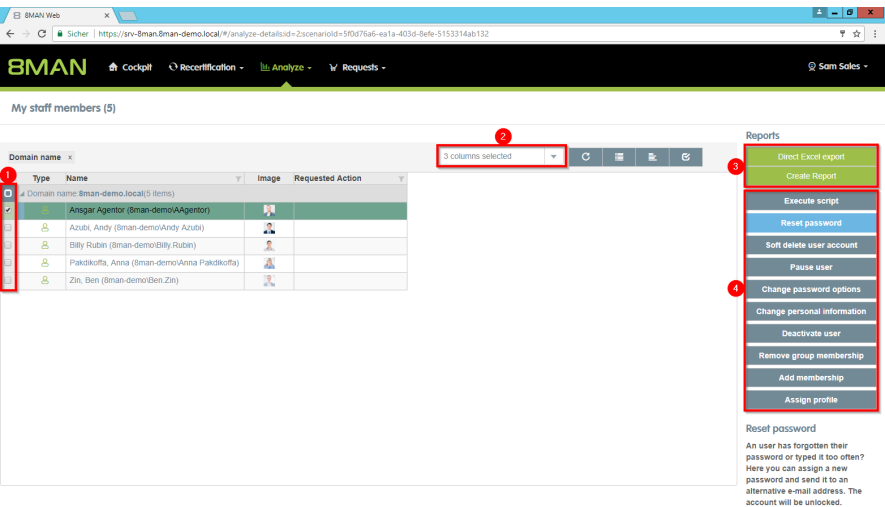
Step by step process



Click on "My employees" in the cockpit.

The button shows you how many employees are assigned to you.

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.

### 8.1.3.9 Add group memberships (cockpit)

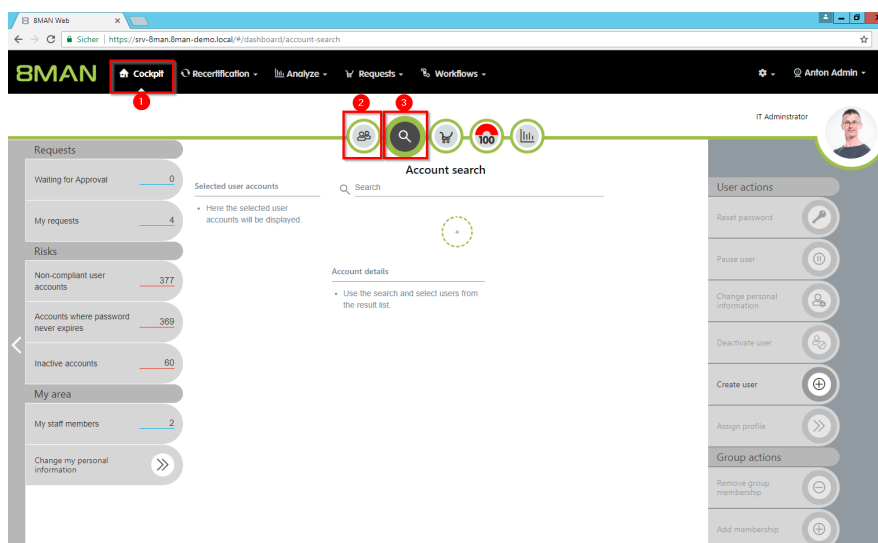
#### Background / Value

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

#### Additional Services

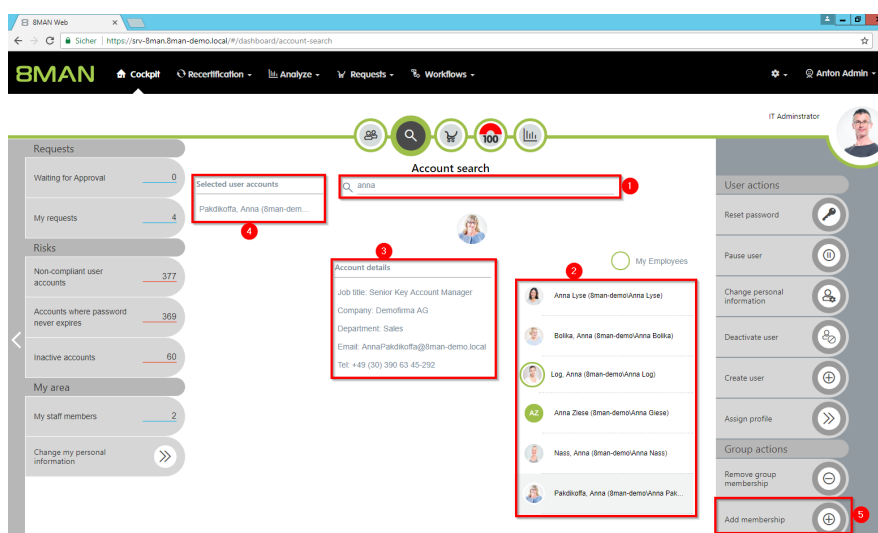
Overview of all cockpit services

#### Step by step process

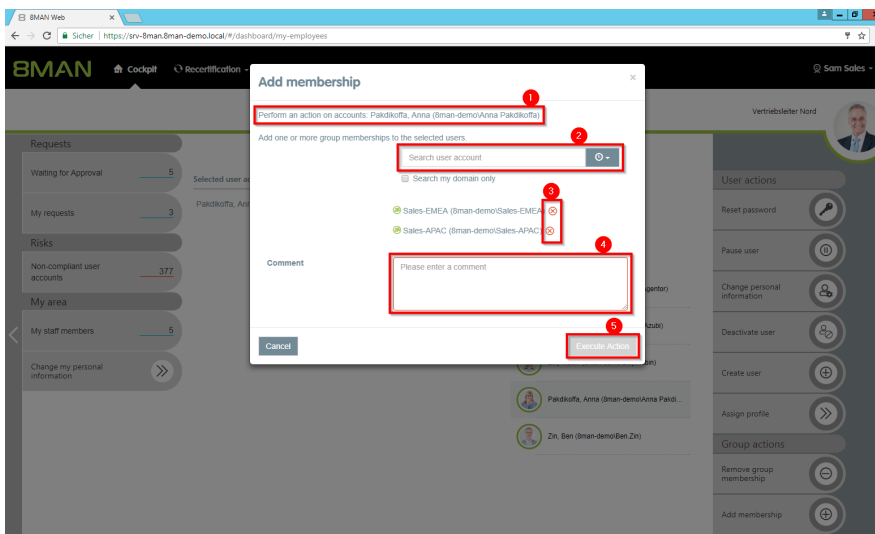


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Supervisor" attribute. See [Changing Attributes \(Web Client\)](#).
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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.
1. Select one or more users.
2. 8MAN shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
3. In the collection you can see already selected users.
4. Click "Add group memberships".



1. 8MAN shows you which accounts you have selected.
2. Search for groups.
3. optional:  
Remove already selected groups.
4. You must enter a comment.
5. Click on "Execute Action".



### 8.1.3.10 Remove group memberships (cockpit)

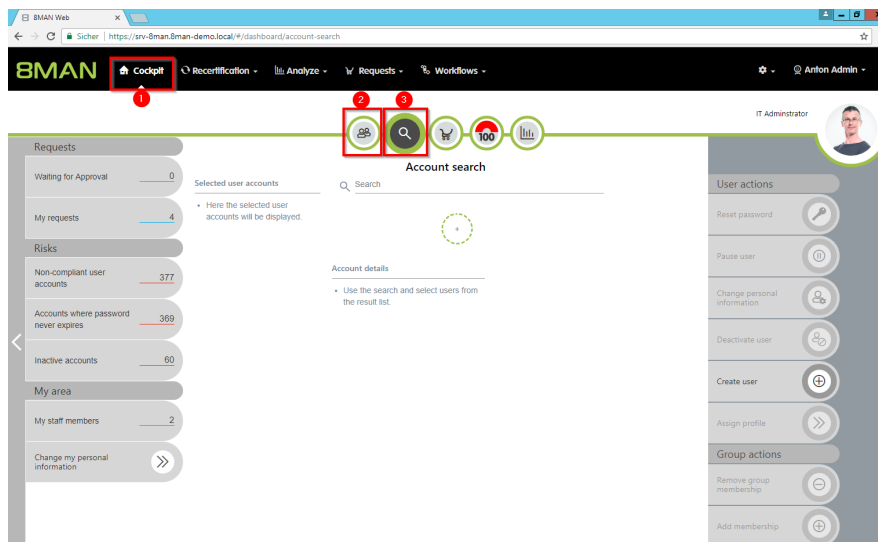
#### Background / Value

Overrides are often caused by group memberships. In the cockpit, you can quickly remove group memberships.

#### Additional Services

Overview of all cockpit services

#### Step by step process

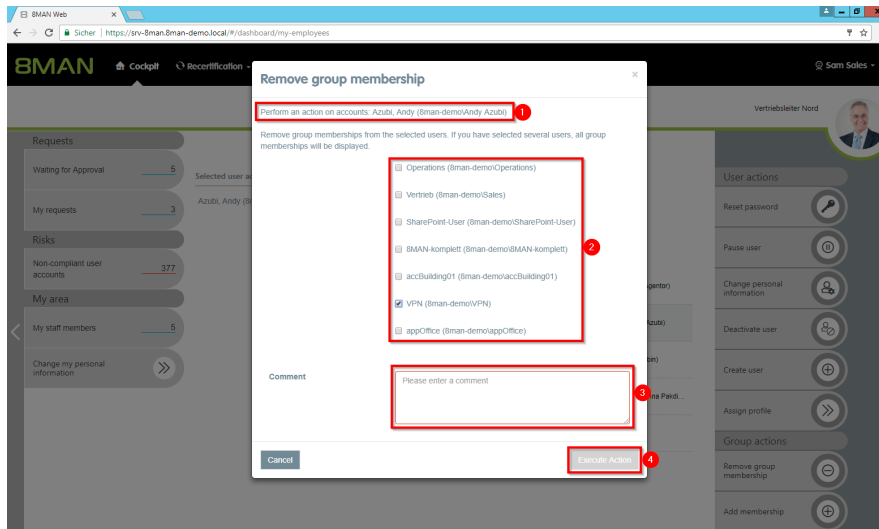


1. Choose Cockpit.
2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Supervisor" attribute. See [Changing Attributes \(Web Client\)](#).
3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

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.
1. Select one or more users.
2. 8MAN shows you the information (attributes) of the selected user. If you have selected more than one user, only the common attributes will be displayed.
3. In the collection you can see already selected users.
4. Click "Remove group memberships".



1. 8MAN shows you which accounts you have selected.
2. Select at least one group.
3. You must enter a comment.
4. Click "Execute Action".

## 8.2 File server

### 8.2.1 Data owner

#### 8.2.1.1 Grant and remove file server access rights

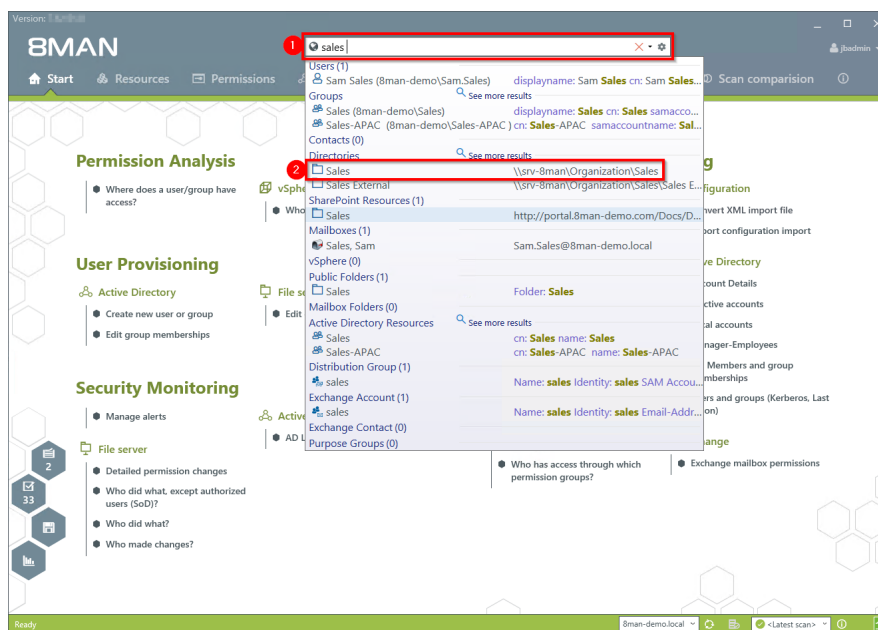
##### Background / Value

Access rights should be easy to assign and revoke. You can do this quickly and easily for the employees in your department. You don't need any special knowledge of Active Directory and / or file servers.

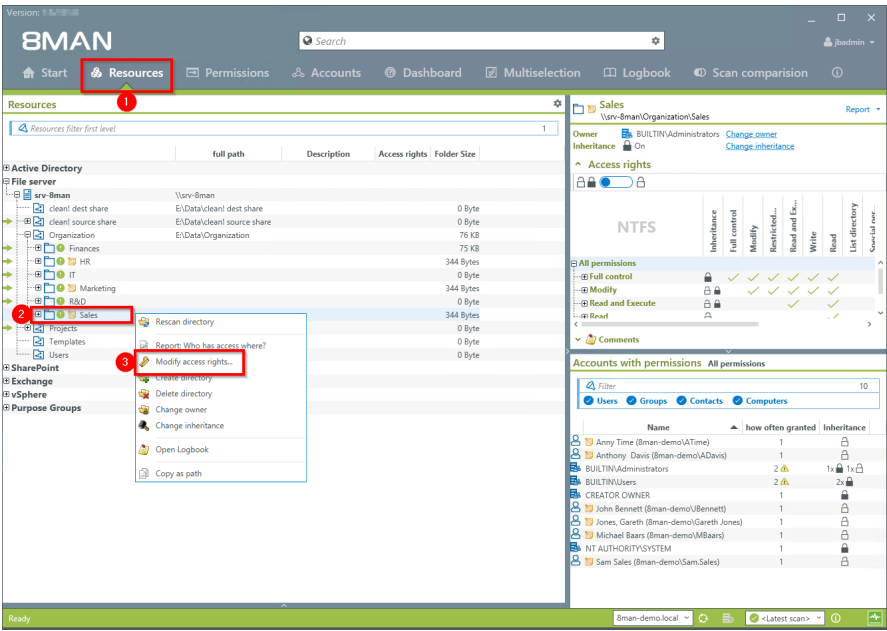
Simply decide what type of access rights you would like to assign: modify or read and execute.

**In order to maintain data integrity we recommend assigning change rights only to carefully selected employees.**

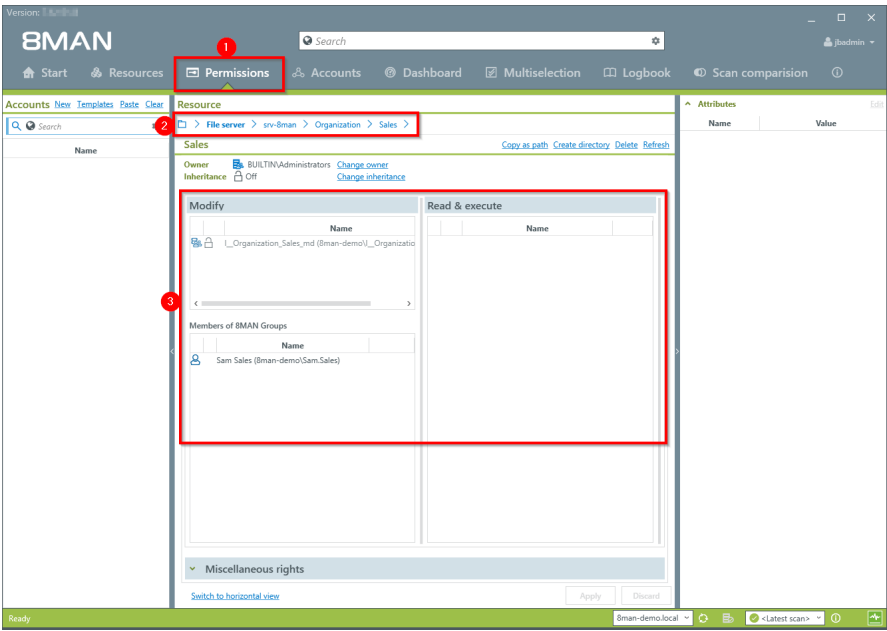
##### Step by step process



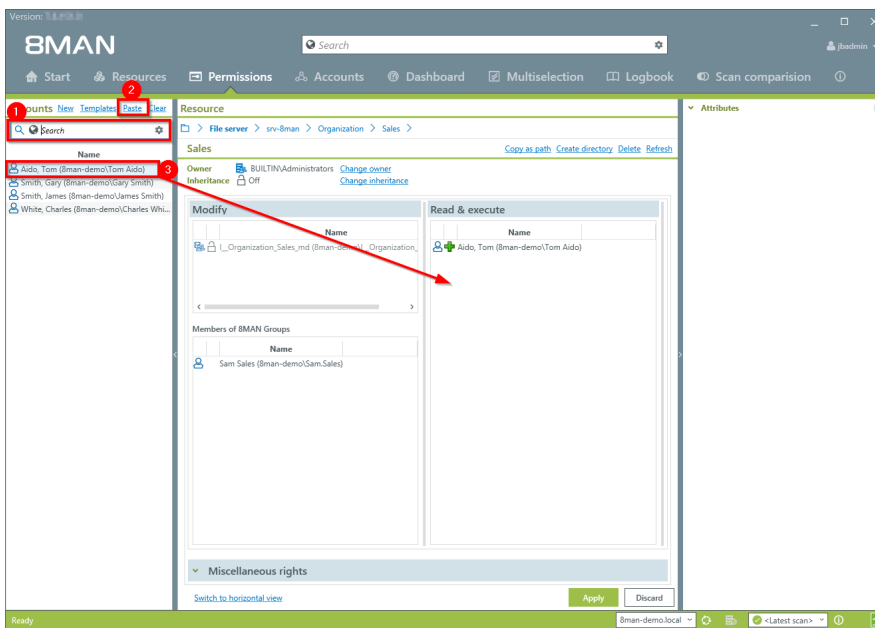
1. Use the search field to find the desired directory.
2. Click on the search result.



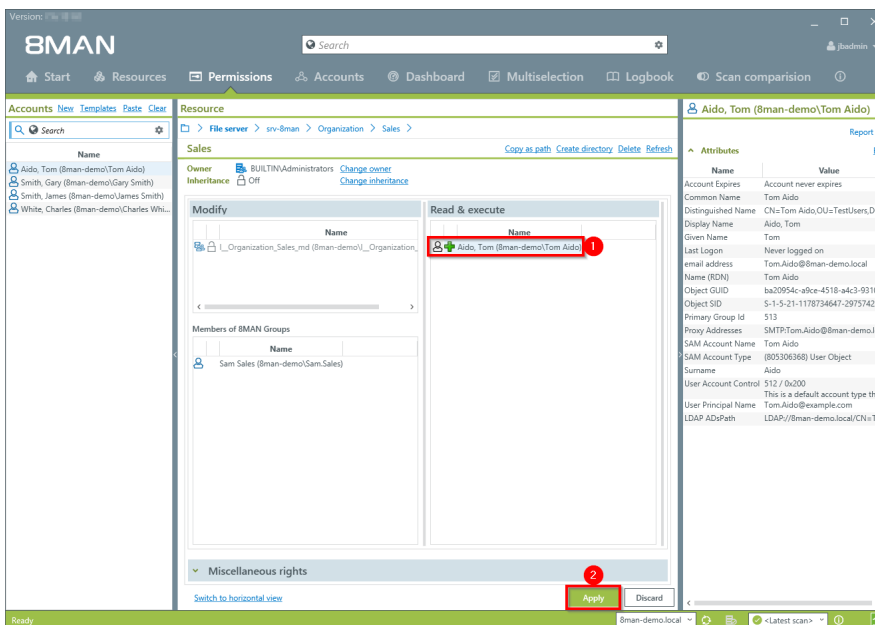
1. 8MAN switches to the "Resources" view.
2. Select a sub-directory if desired by right-clicking on it.
3. Select "Modify access rights..."



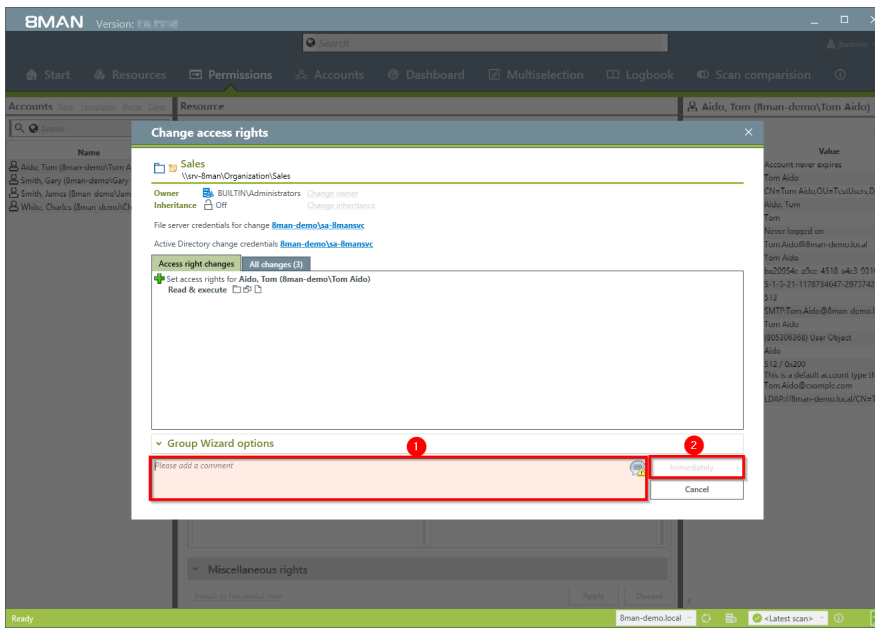
1. 8MAN switches to the "Permissions" view.
2. 8MAN shows you the directory that you are working on. You can change this directory.
3. 8MAN shows you all existing access rights in the categories "Modify" and "Read & execute".



1. Use the search field to find the desired user or group.
2. You can enter the content into the clipboard, for example an 8MAN Text. 8MAN will then find known objects and filter them from the text.
3. Use drag & drop to move the users into a column and assign corresponding access rights.



1. The user is added to the column.
2. Click on "Apply".



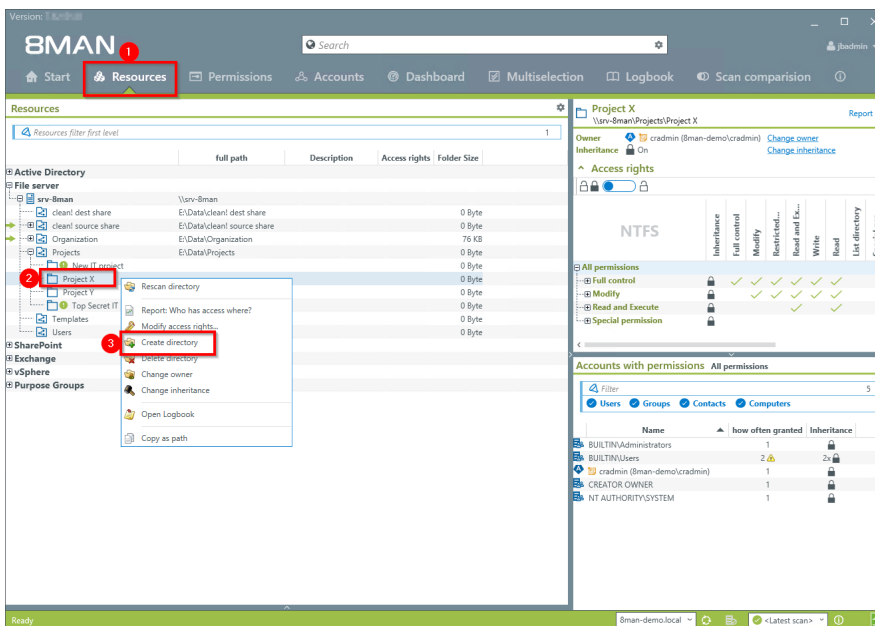
1. You must enter a comment.
2. Start the access rights change.

### 8.2.1.2 Create a protected file server directory

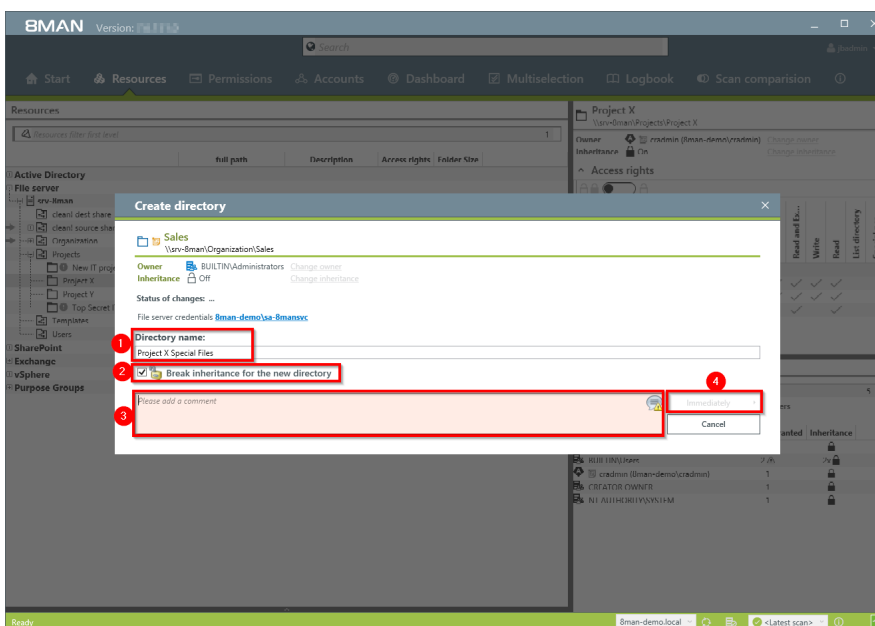
#### Background / Value

Managers and team leads can use 8MAN quickly and easily to 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.

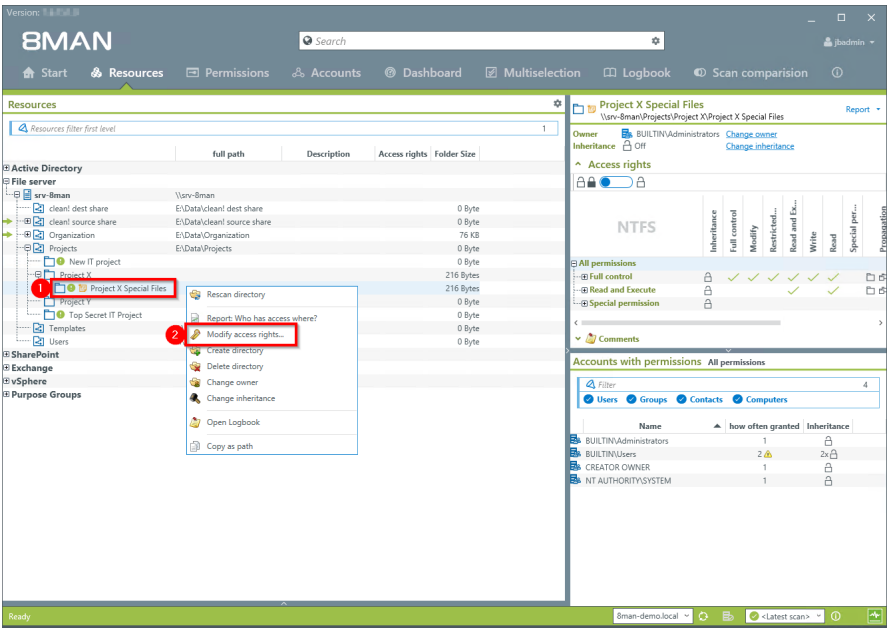
#### Step by step process



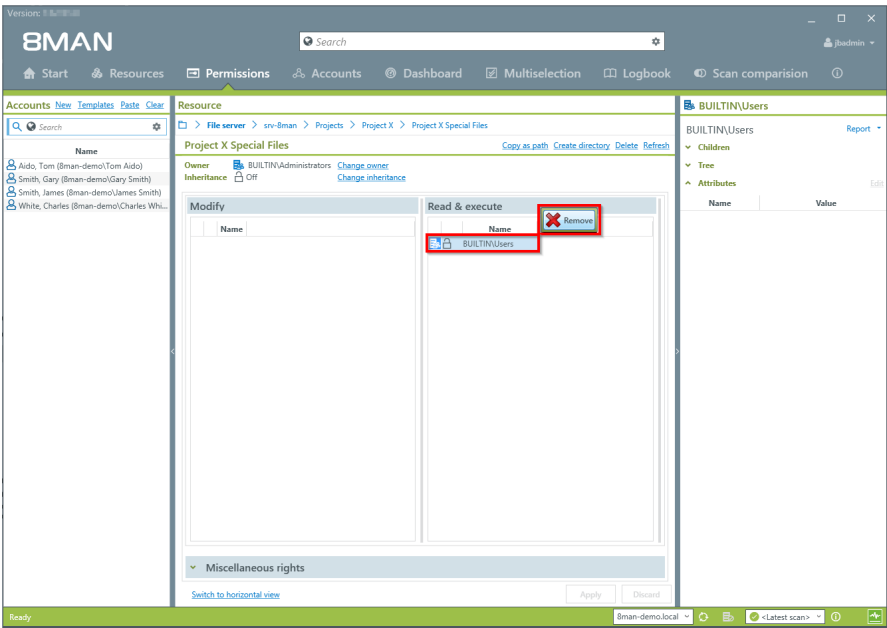
1. Select "Resources".
2. Navigate to the desired folder.
3. Right-click on the desired object and select "Create directory" from the context menu.



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

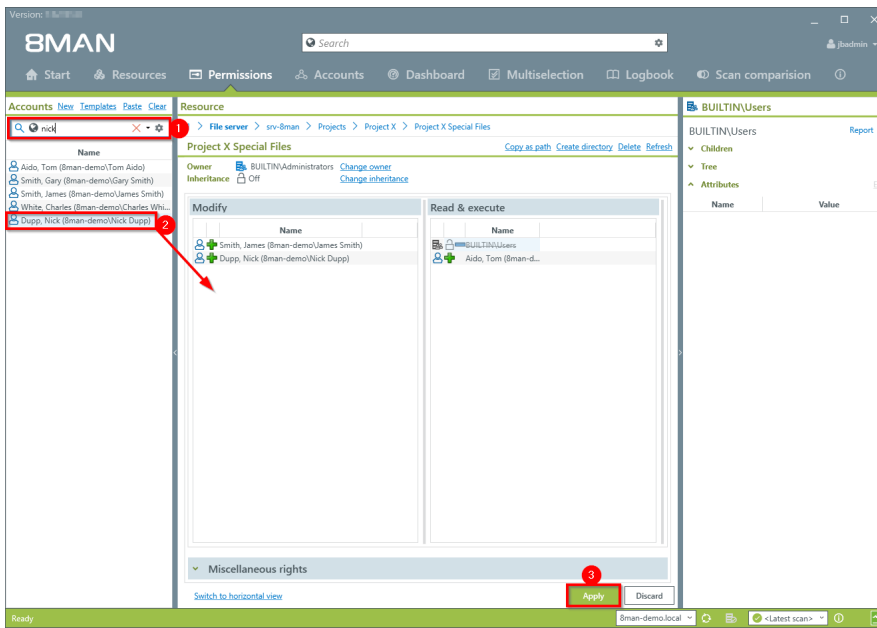


1. Navigate to the newly created directory.
2. Right-click on the directory and select "Modify access rights..." from the context menu.

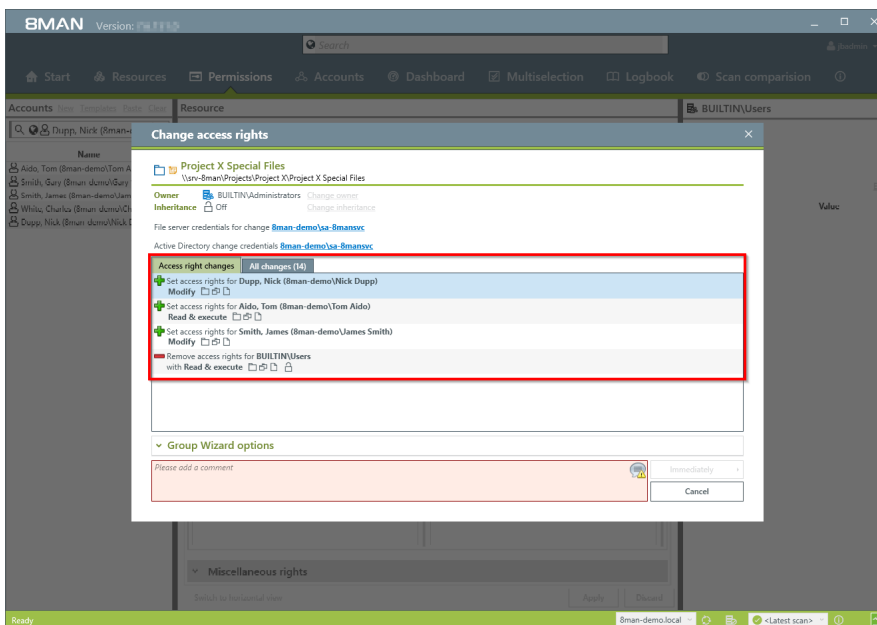


Remove all unnecessary access rights.

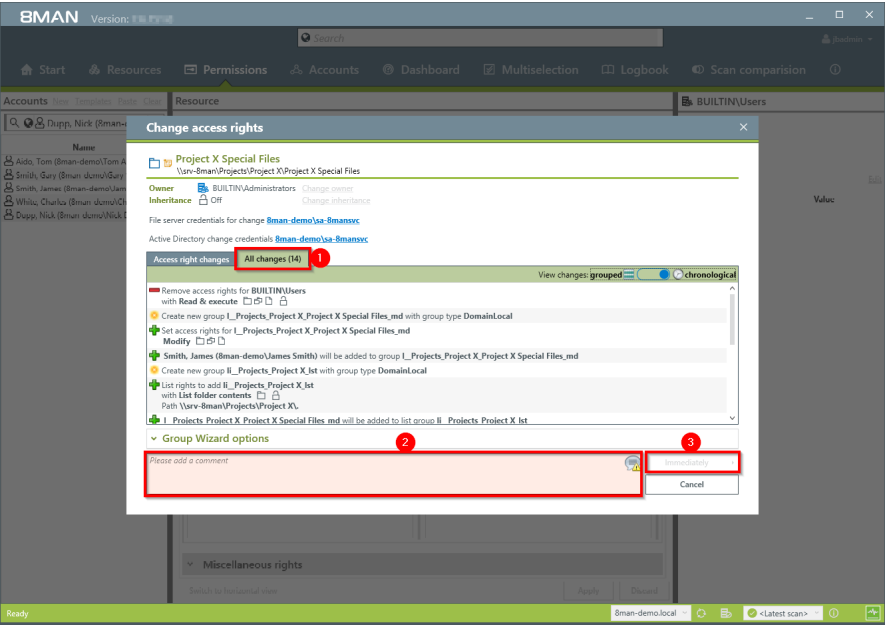




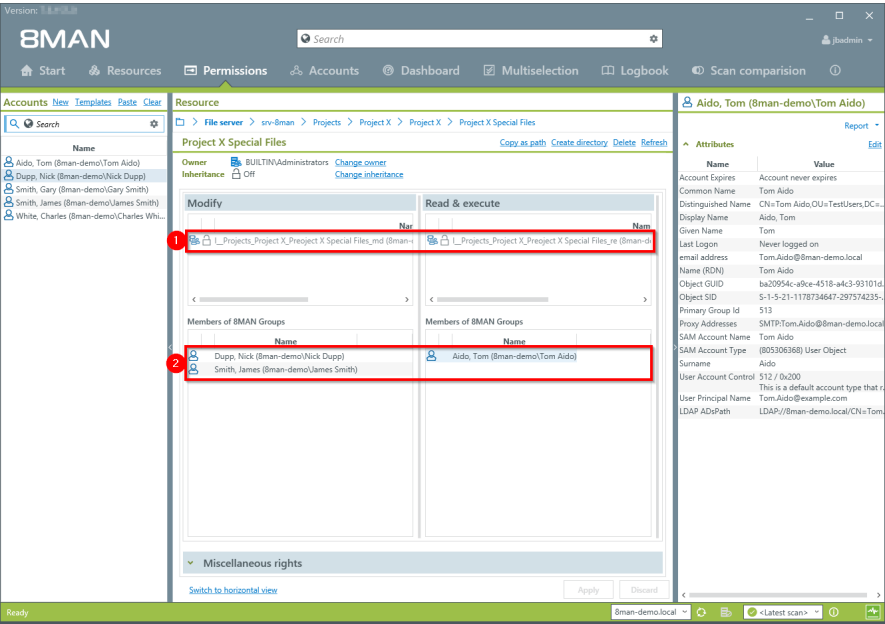
1. Use the search field to find the desired users and groups.
2. Use drag & drop to move the desired accounts into the access rights columns.
3. Start the process.



8MAN lists all planned access right changes. In the following example "Sam Sales" receives "change" rights to a new protected directory.



1. Click on the tab "All changes". You can then see all individual steps performed by the Group Wizard.
2. You must enter a comment.
3. Start the process.



After the execution, 8MAN will show you the result.

1. New, automatically created groups.
2. Members of the new groups.

## 8.2.2 Administrator

### 8.2.2.1 Remove multiple access rights on file server directories

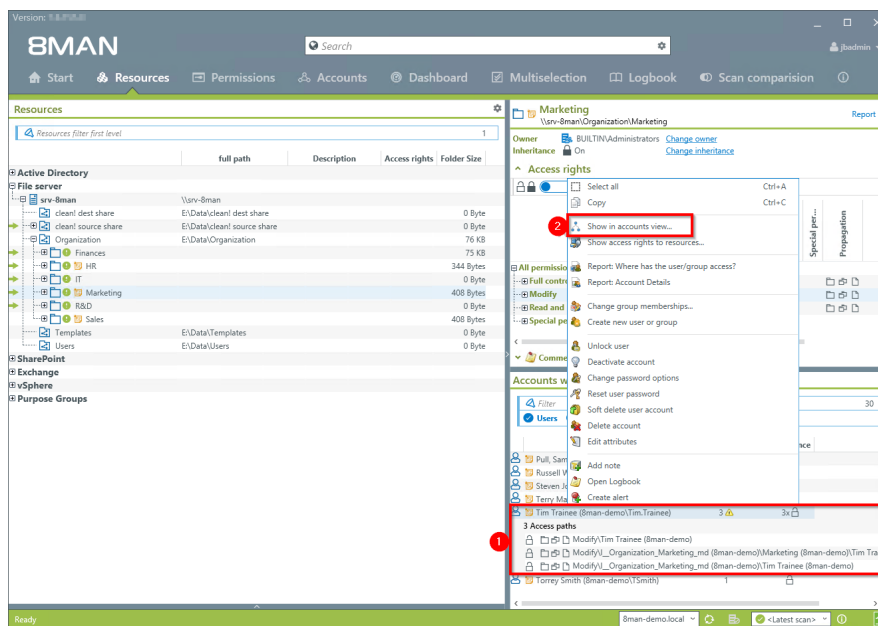
#### Background / Value

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. 8Man allows you to remove multiple access rights quickly and easily.

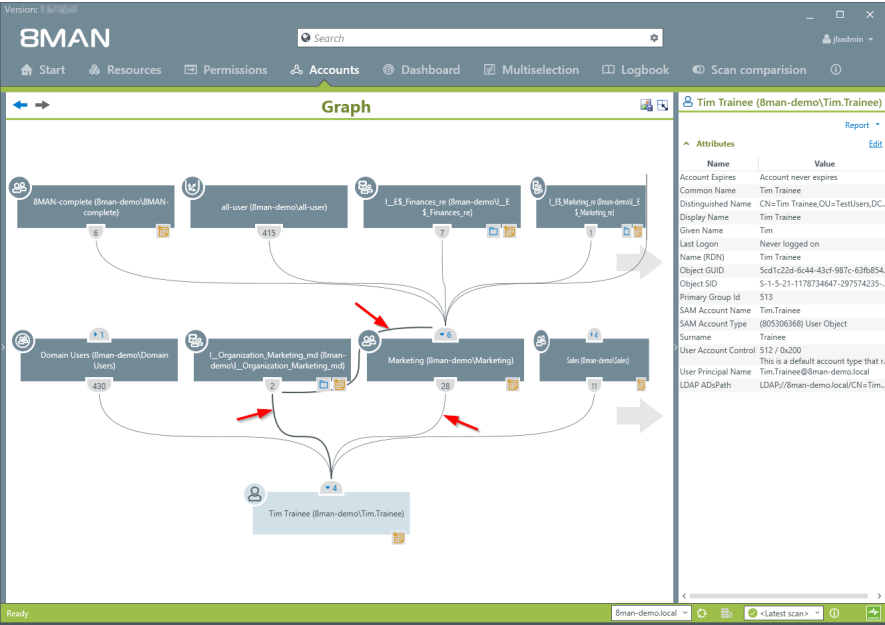
#### Additional services

##### Identify multiple access paths to directories

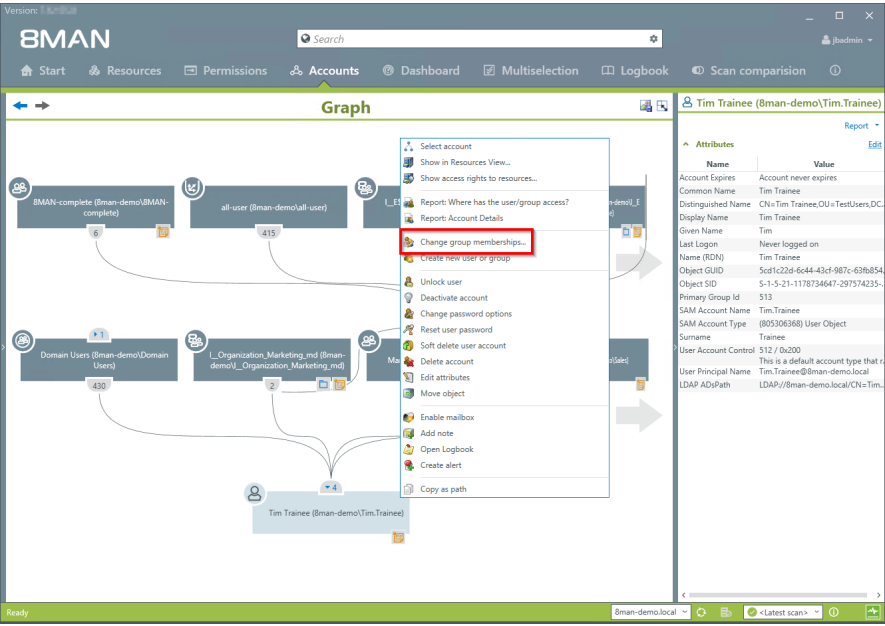
#### Step by step process



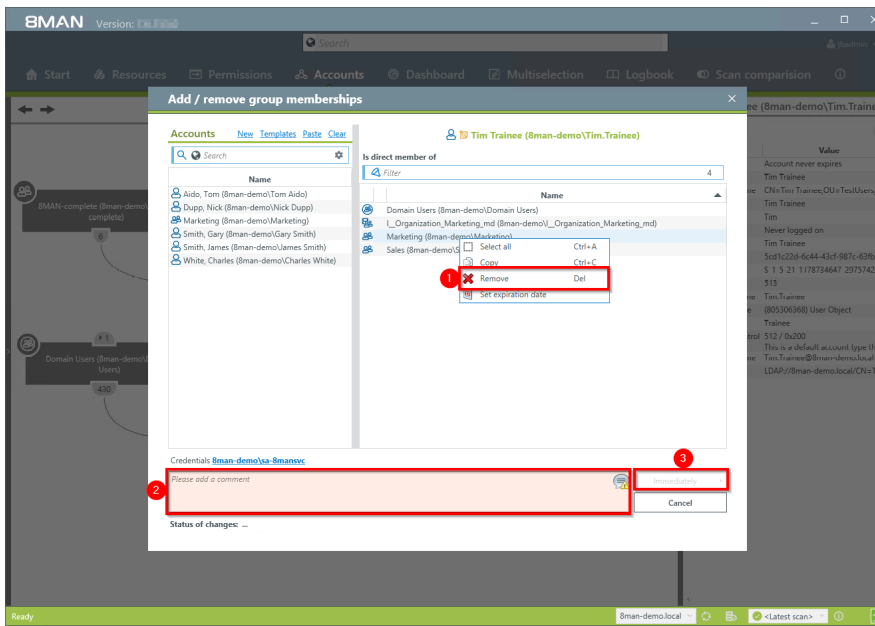
1. You have identified "Tim Trainee" as having multiple access paths.
2. Right-click on the account and select "Show in account view" from the context menu.



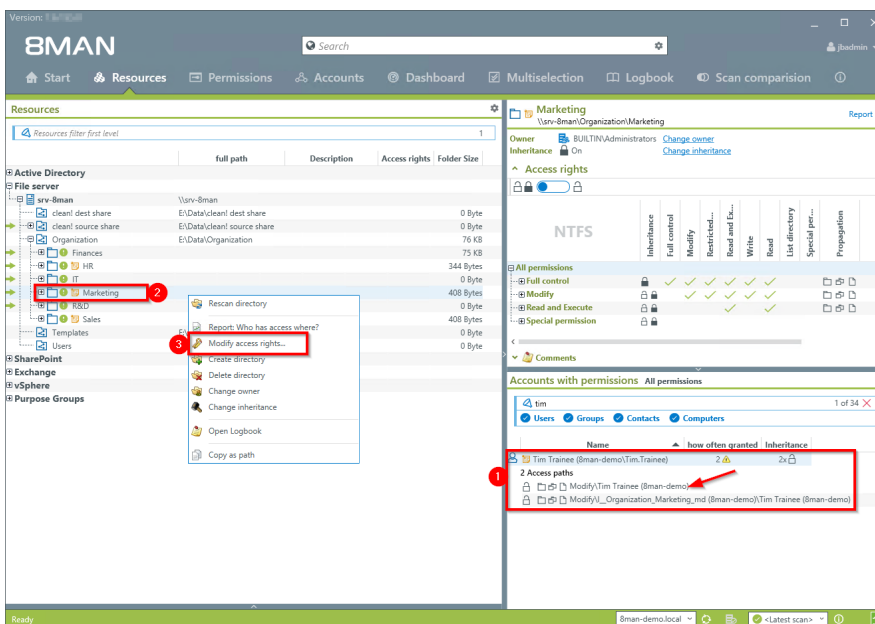
Use the AD graph to analyze multiple access paths.



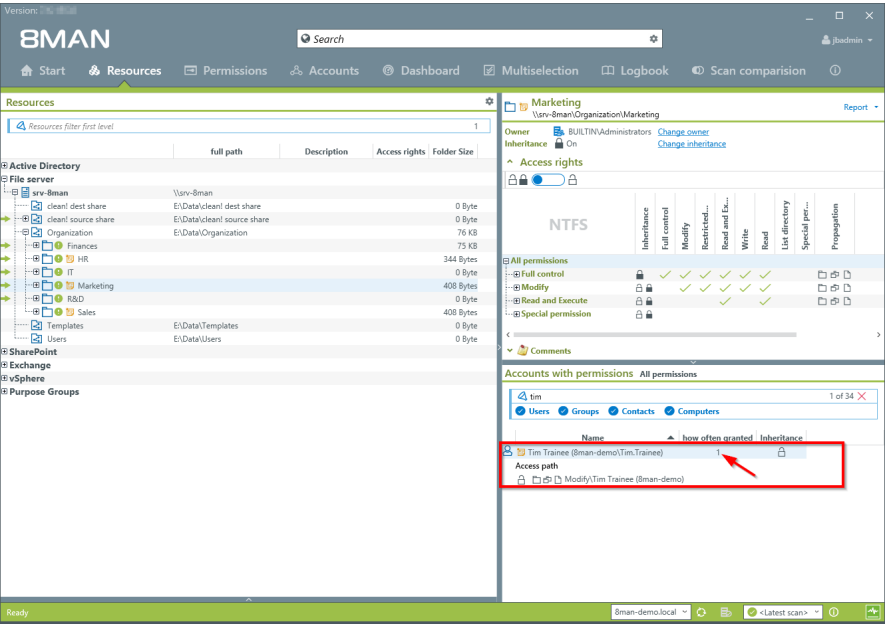
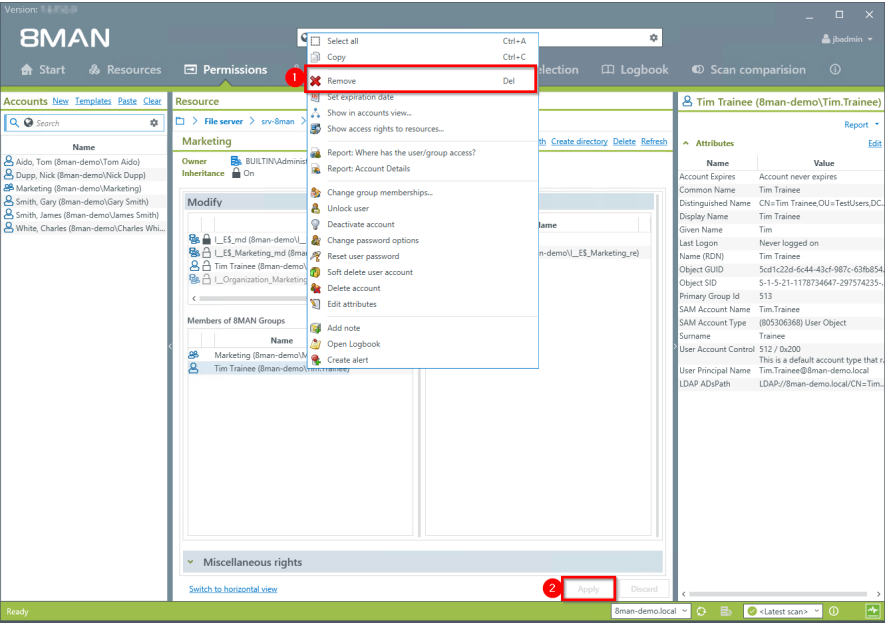
Right-click on the account and select "Change group memberships" from the context menu.



1. Remove the 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 access rights.
2. Right-click on the desired directory.
3. Select "Change access rights" from the context menu.



## 8.2.2.2 Remove direct permissions

### Background / Value

Direct access rights should be avoided at all costs 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. 8MAN 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.

### Additional Services

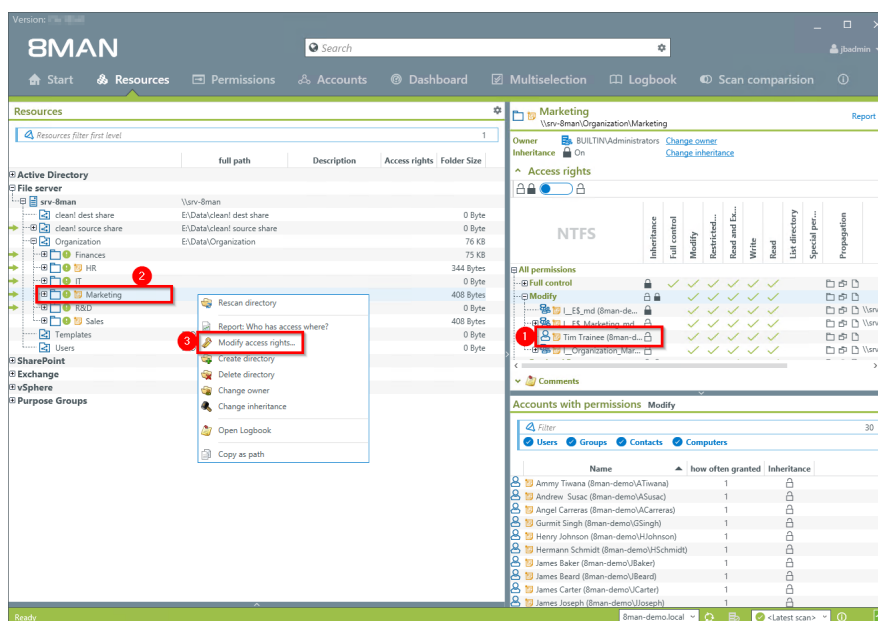
[Remove direct permissions in bulk](#) (web client)

8MATE Clean! allows you to automatically remove direct access rights and turn them into group memberships.

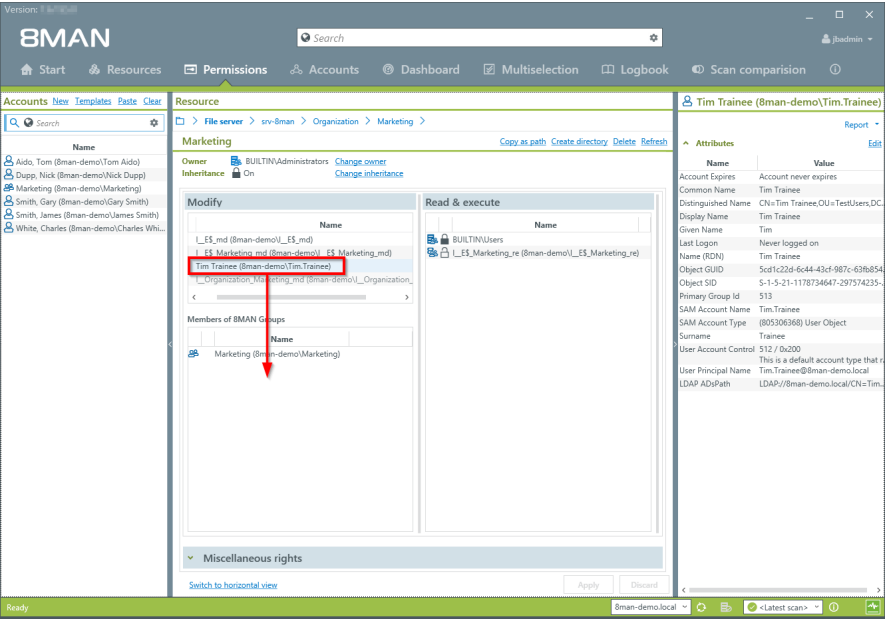
[8MATE Clean! Handbook: Replacing direct permissions with group memberships](#)

[8MATE Clean! Handbook: Deleting direct access rights](#)

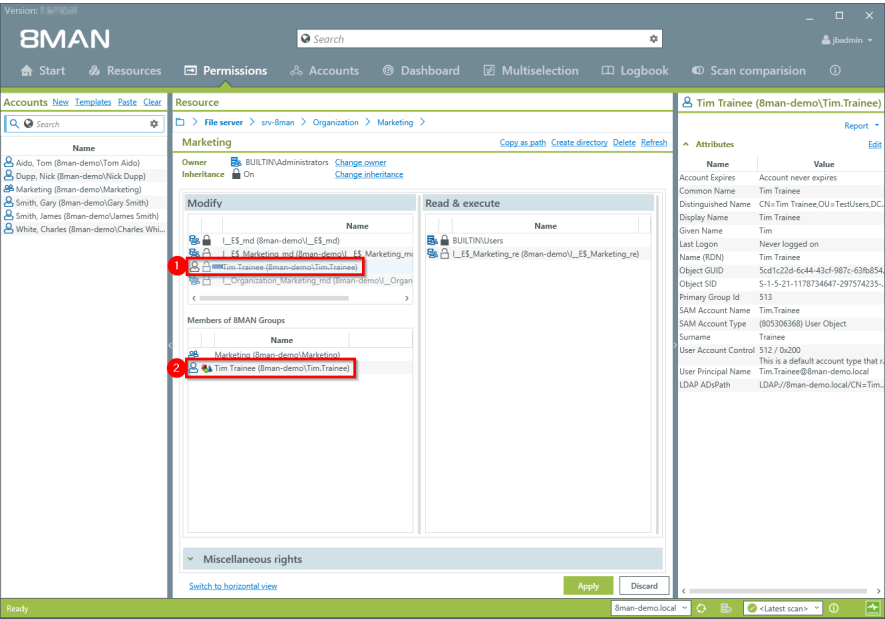
### Step by step process



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

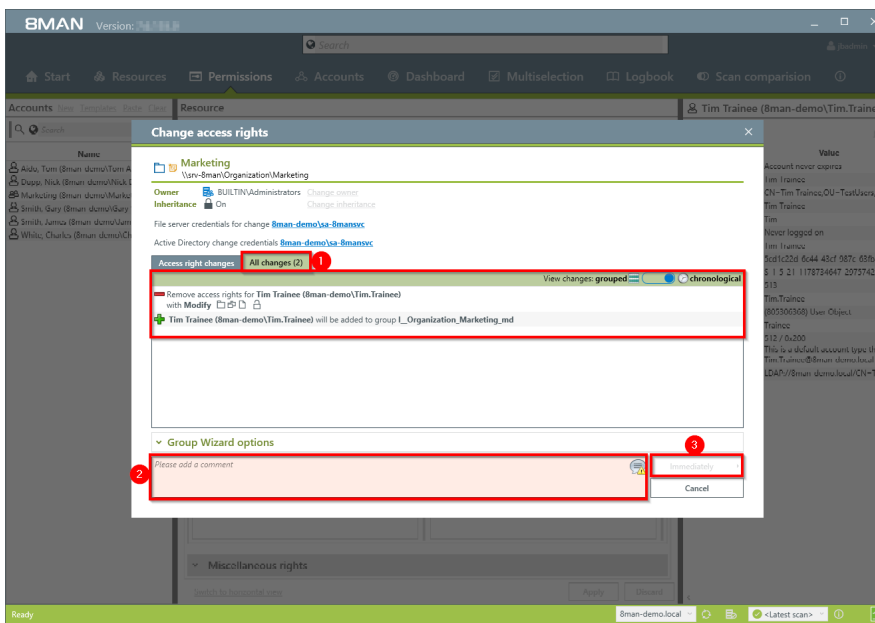


Drag the user into the 8MAN group.



1. The direct access right for "Tim Trainee" 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 change process.

### 8.2.2.3 Remove corrupted inheritance

#### Background / Value

Broken ACLs (Access Control Lists) interfere with NTFS inheritances on file servers. As a consequence the sub-directory will not receive the correct inheritance, despite this feature being activated. 8MAN displays "Broken ACLs" and removes them by reapplying the inheritance.

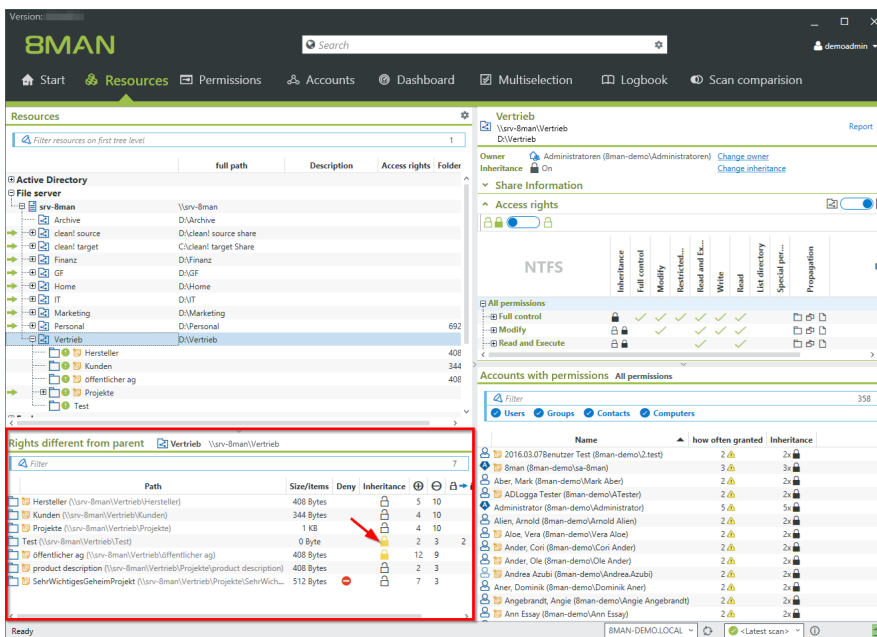
#### Weiterführende Services

Remove differing permissions in bulk (web client)

#### Step by step process

The screenshot shows the 8MAN web client interface. The top navigation bar has a 'Resources' tab highlighted with a red box and a red circle with the number 1. The left sidebar shows a tree view of file servers, with the 'Vertrieb' folder highlighted by a red box and a red circle with the number 2. The main content area displays the details for the 'Vertrieb' folder, including 'Share Information', 'Access rights', and 'Accounts with permissions'.

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



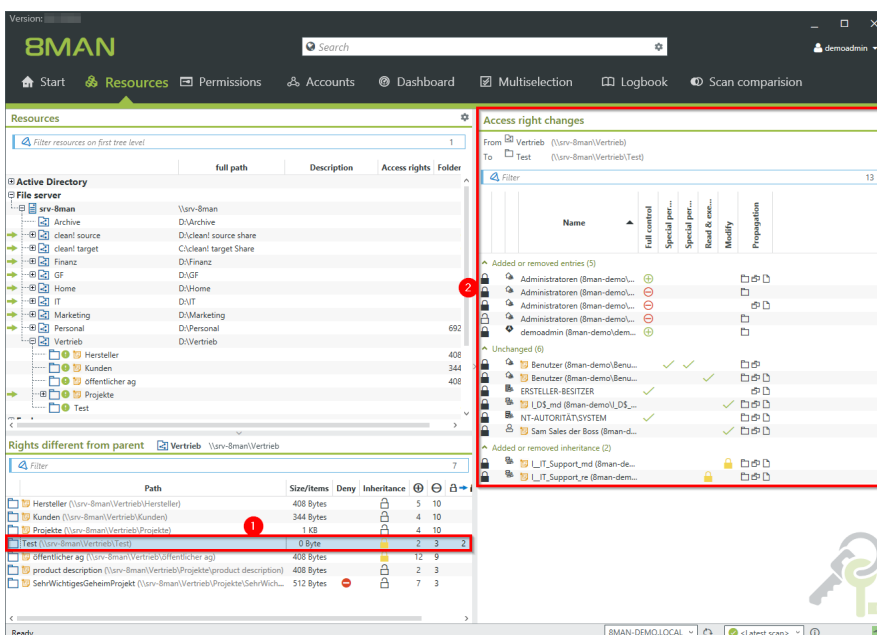
8MAN lists all subdirectories with different permissions. At the yellow lock you recognize a corrupted inheritance.

Use the sort function in the "Inheritance" column.

Path	Size/Items	Deny	Inheritance
Hersteller (\\srv-8man\Vertrieb\Hersteller)	408 Bytes	5	10
Kunden (\\srv-8man\Vertrieb\Kunden)	344 Bytes	4	10
Projekte (\\srv-8man\Vertrieb\Projekte)	1 KB	4	10
Test (\\srv-8man\Vertrieb\Test)	0 Byte	2	3
öffentlicher ag (\\srv-8man\Vertrieb\öffentlicher ag)	408 Bytes	12	9
product description (\\srv-8man\Vertrieb\Projekte\product description)	408 Bytes	2	3
SehrWichtigesGeheimProjekt (\\srv-8man\Vertrieb\Projekte\SehrWich...	512 Bytes	7	3

8MAN lists all subdirectories with different permissions. At the yellow lock you recognize a corrupted inheritance.

Use the sort function in the "Inheritance" column.

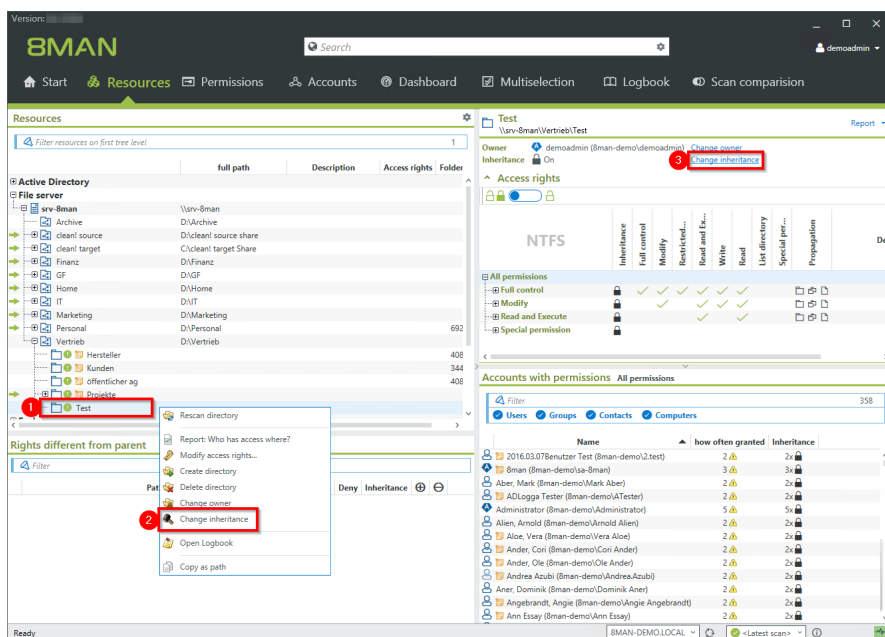


1. Select an entry.

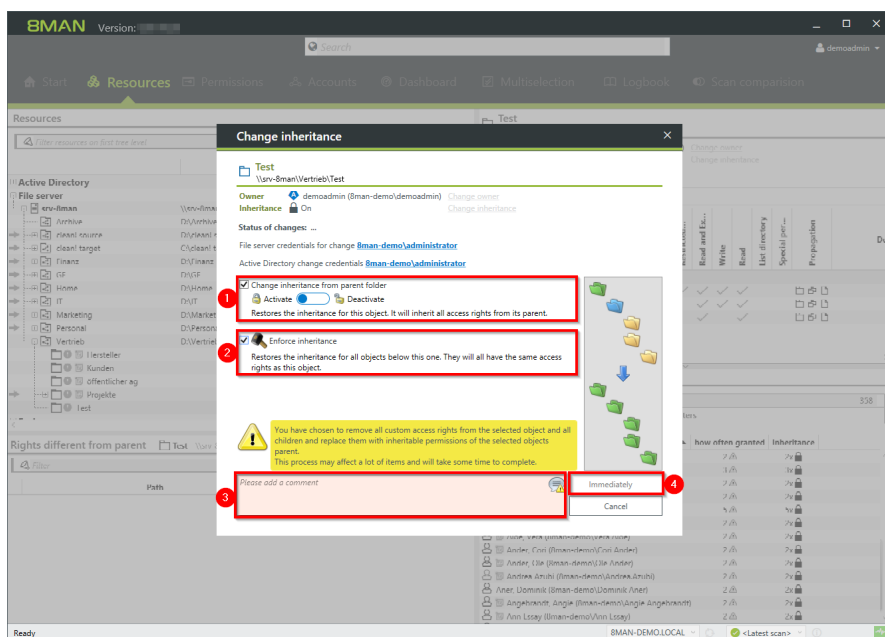
2. 8MAN shows you in all details which permissions are different compared to the parent directory.

Name	Full control	Special per...	Read & exe...	Modify	Propagation
Administratoren (Bman-demo\Administratoren)	✓	✓	✓	✓	✓
Administratoren (Bman-demo\Administratoren)	✓	✓	✓	✓	✓
Administratoren (Bman-demo\Administratoren)	✓	✓	✓	✓	✓
Administratoren (Bman-demo\Administratoren)	✓	✓	✓	✓	✓
demoadmin (Bman-demo\demoadmin)	✓	✓	✓	✓	✓
Benutzer (Bman-demo\Benutzer)	✓	✓	✓	✓	✓
Benutzer (Bman-demo\Benutzer)	✓	✓	✓	✓	✓
ERSTELLER-BESITZER	✓	✓	✓	✓	✓
LD5_md (Bman-demo\LD5_md)	✓	✓	✓	✓	✓
NT-AUTORITÄT\SYSTEM	✓	✓	✓	✓	✓
Sam Sales der Boss (Bman-d...	✓	✓	✓	✓	✓
LT_Support und (Bman-de...	✓	✓	✓	✓	✓
LT_Support_ze (Bman-dem...	✓	✓	✓	✓	✓

1. Select an entry.
2. 8MAN 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. In the example here for all subdirectories of "Test".
3. You must enter a comment.
4. Start the execution.

## 8.2.2.4 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 are deleted in AD.

By using unresolved SIDs insider threats can gain access to sensitive resources. 8MAN clearly identifies unresolved SIDs in your system allowing you to delete them.

### Additional Services

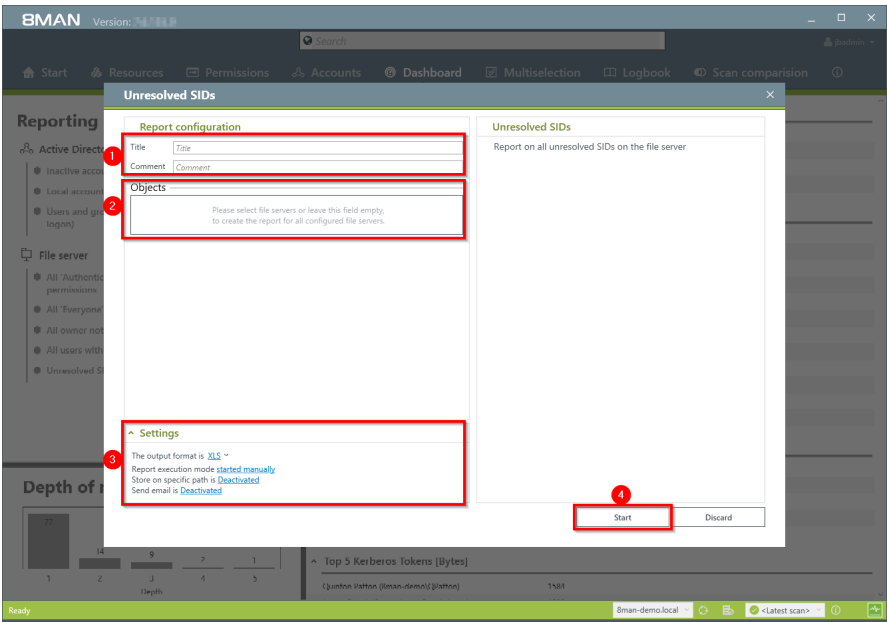
[Remove unresolved SIDs in bulk](#) (web client)

### Step by step process

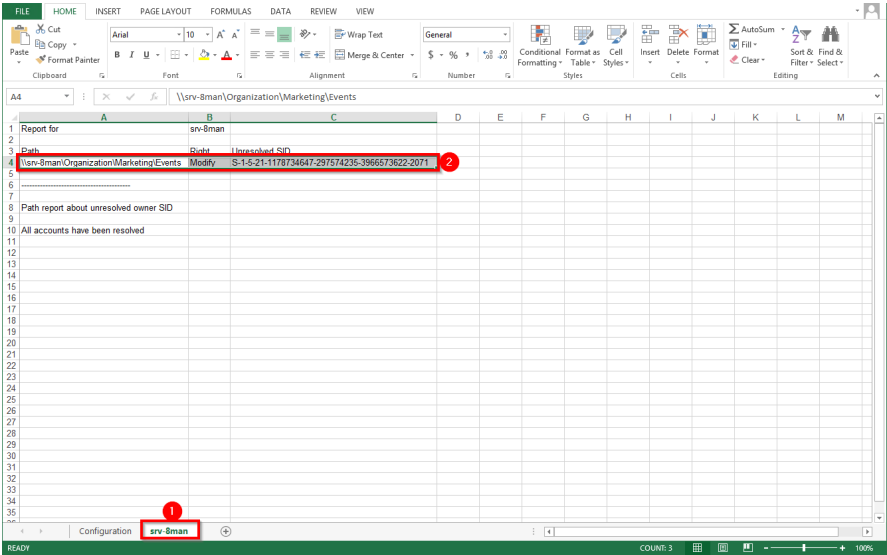
The screenshot shows the 8MAN web client interface. The 'Dashboard' tab is selected in the top navigation bar. On the left sidebar, under 'Reporting', the 'Unresolved SIDs' section is highlighted with a red box and a red circle with the number 2. The main content area displays a table of 'Users and other accounts' and 'Groups'. The 'Unresolved SIDs' section is also visible in the bottom left corner of the main content area.

Category	Item	Count
Users and other accounts	Users	431
	Users (Disabled)	6
	Administrators	13
	Administrators (Disabled)	0
Groups	All Groups	190
	Groups with members (w/o recursions)	112
	Empty groups	75
	Groups in recursions	3
	The largest group (Domain Users (8man-demo\Domain Users))	430
	Built-in security groups	27
	Global security groups	78
	Universal security groups	35
	Local security groups	48
	Global distribution groups	0
	Universal distribution groups	2
	Local distribution groups	0
OU / Contacts / More	Computers	4
	Computers (disabled)	0
	Contacts	0
	Foreign users	0
	Organizational Units	12
	Top 5 Kerberos Tokens [Bytes]	1584

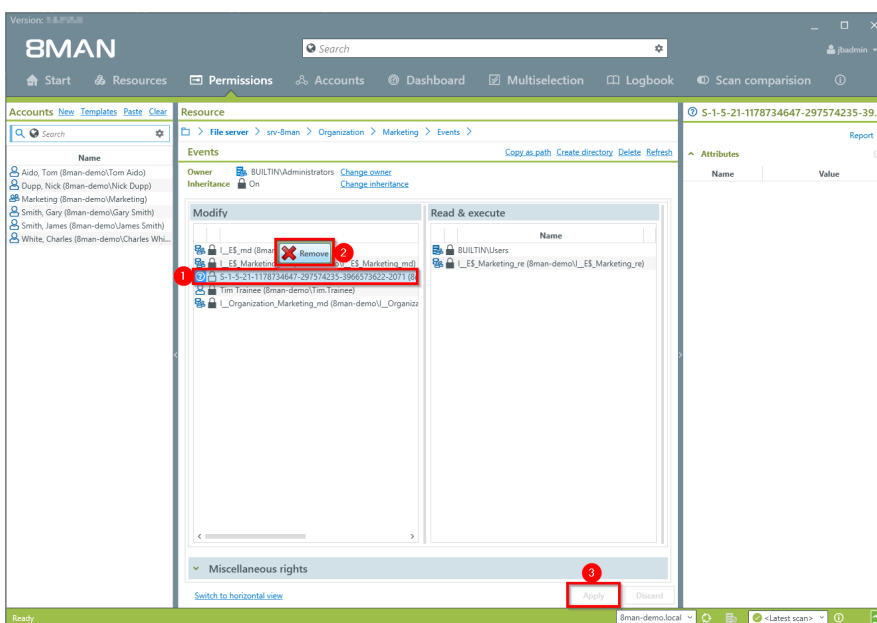
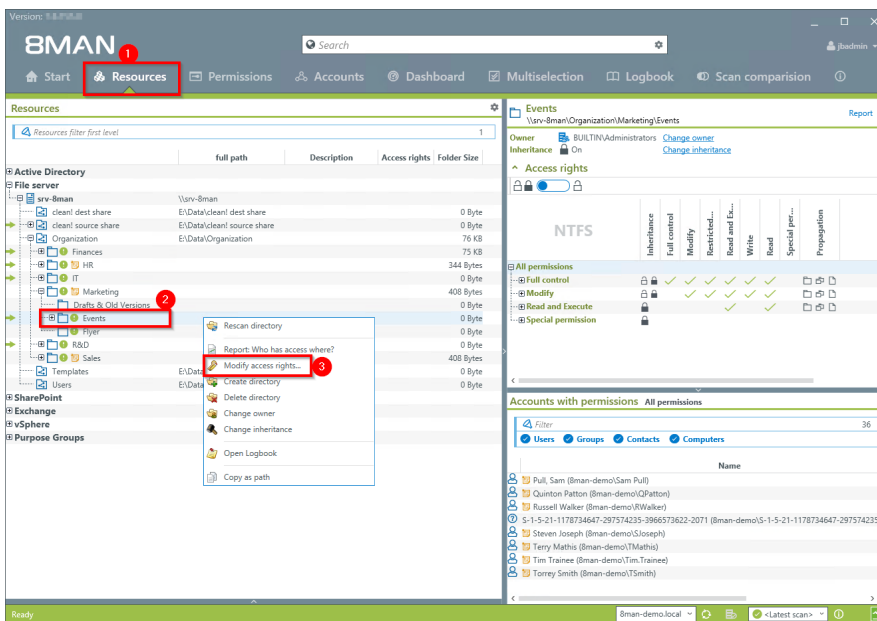
1. Select "Dashboard".
2. Click on "Unresolved SIDs".

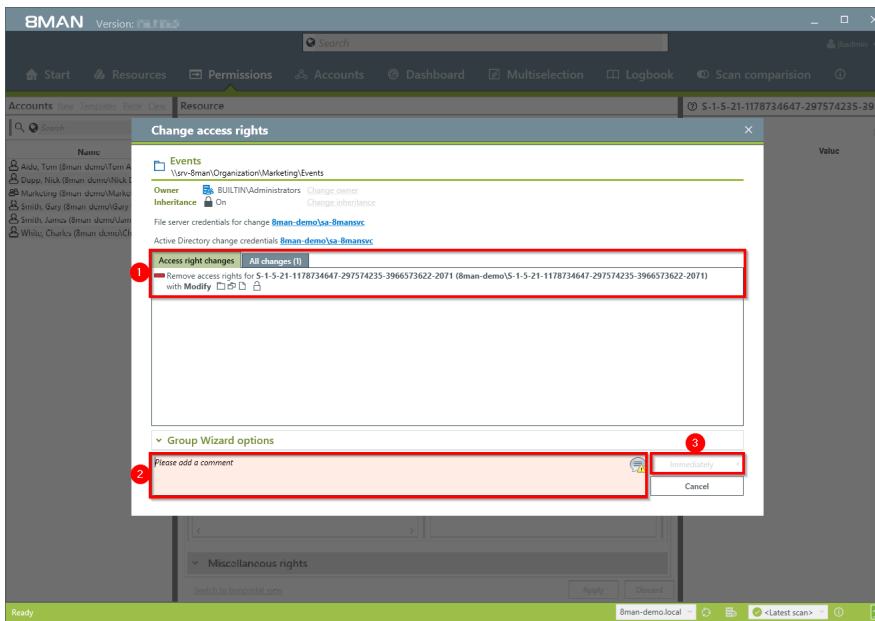


1. Enter a title for the report and add a comment.
2. Define the range of the report.
3. Define the desired report settings.
4. Start the report.



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





1. 8MAN lists all planned changes.

1. You must enter a comment.

2. Start the removal process.



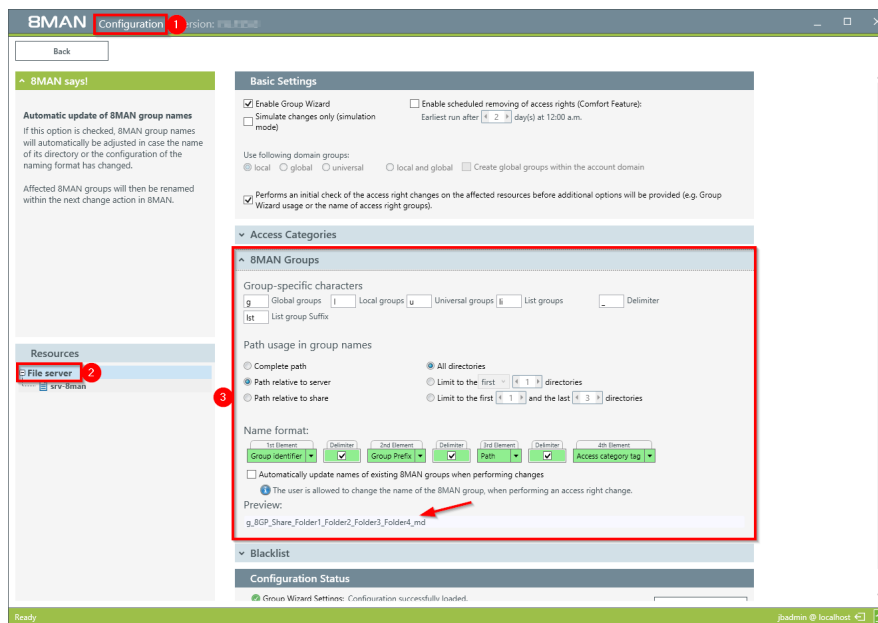
### 8.2.2.5 Determine naming conventions for access groups

#### Background / Value

8MAN puts an end to random naming of groups. Administrators determine the appropriate naming convention, which will be used for all AD groups created with 8MAN Group Wizard.

You can determine the naming convention in the 8MAN configuration module.

#### Step by step process



1. Start the configuration module and navigate to "Change Configuration" - >"File server".
2. Select the desired SharePoint resource. You can enter different settings for each resource.
3. Determine the naming convention. Please note that 8MAN will show you a preview.

### 8.2.2.6 Change directory ownership

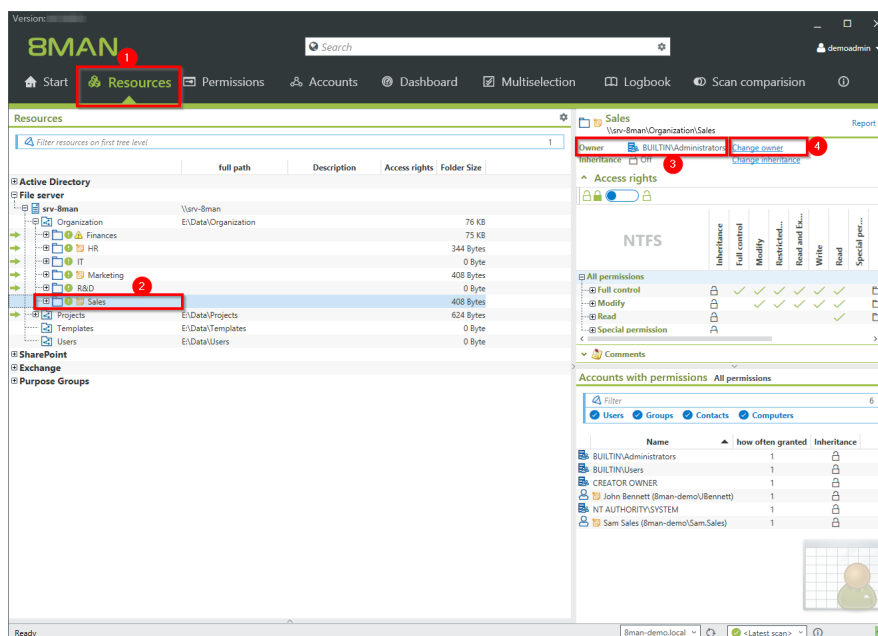
#### Background / Value

With 8MAN, you simply change the owner of directories. If you exclude users from ownership of directories, you can prevent unwanted permission changes.

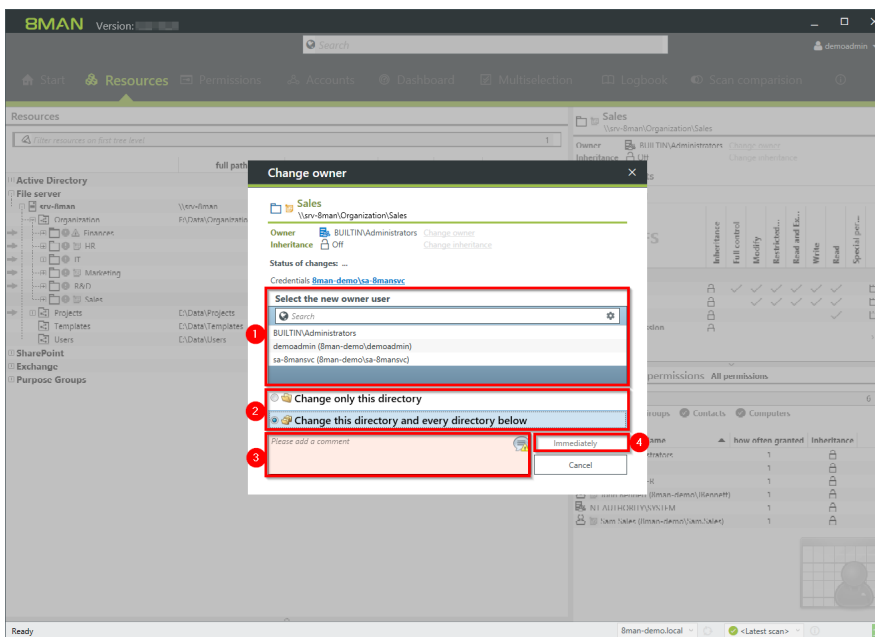
#### Additional Services

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. 8MAN 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.

### 8.2.2.7 Identify errors in inheritance in Analyze & Act and fix them in bulk

#### Background / Value

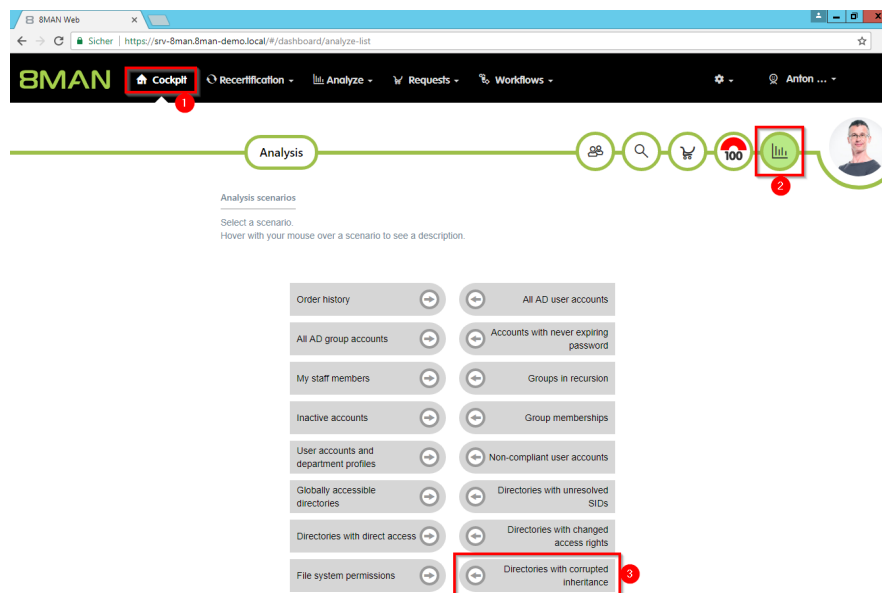
Errors in the inheritance of file server permissions often occur when employees copy or move directories. This can lead to unwanted access.

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

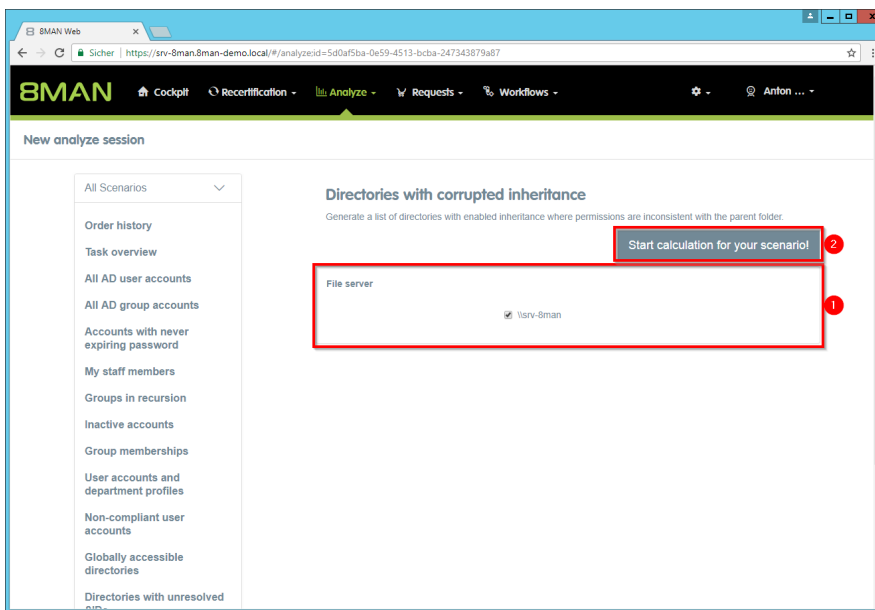
#### Related services

Schedule recurring change tasks

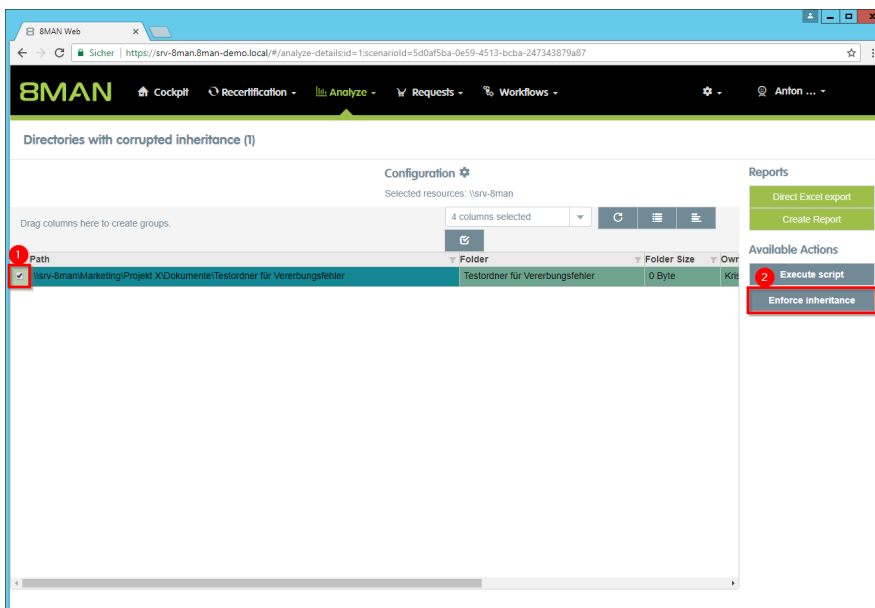
#### Step by step process



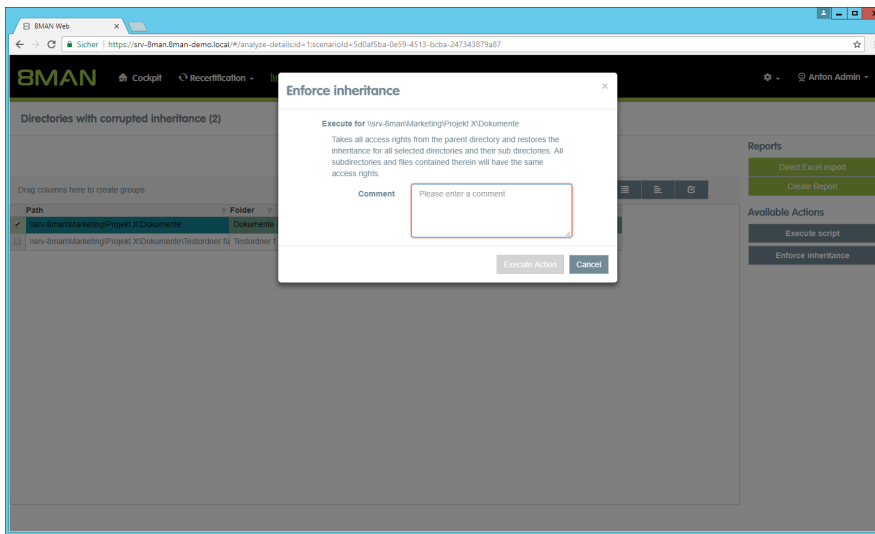
*In the cockpit, choose "Analysis" and then "Directories with corrupted inheritance".*



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



1. Select the directories for which you want to correct the inheritance errors.
2. Click "Enforce Inheritance".



*You can see for which directories the inheritance is enforced again.*

*You must enter a comment.*

## 8.3 +8MATE for Exchange

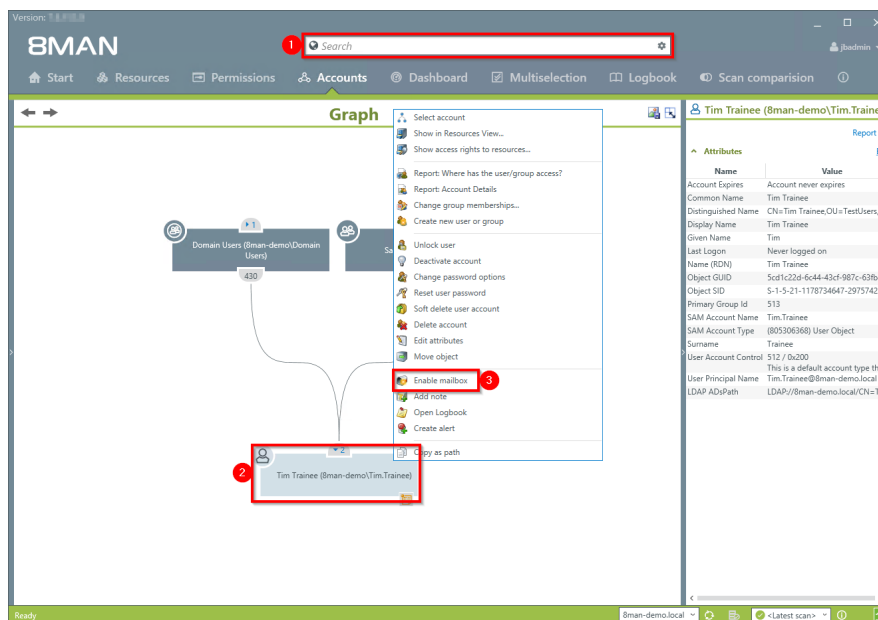
### 8.3.1 Help Desk

#### 8.3.1.1 Create a mailbox (e-mail enable users)

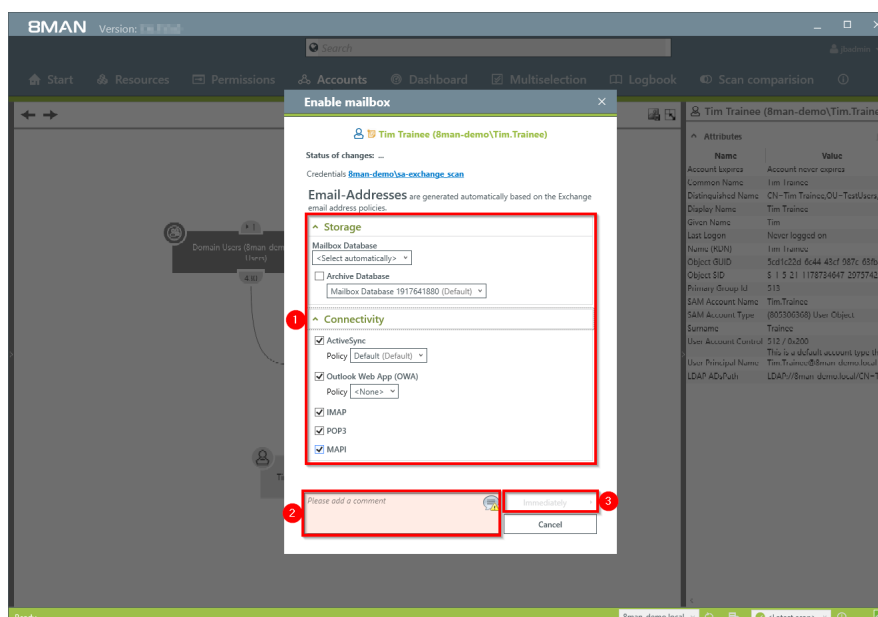
##### Background / Value

If your license agreement includes 8MATE for Exchange you can create Mailboxes (email enable users) with 8MAN.

##### Step by step process



1. Select the desired User or distribution group (type: universal).
2. Right-click on the user. You can do this in the Accounts view.
3. Click on "Enable mailbox" from the context menu. This option is only available if no mailbox has been created yet.



1. Determine the Exchange options.
2. You must enter a comment, for example a ticket number.
3. Start the creation of the mailbox.



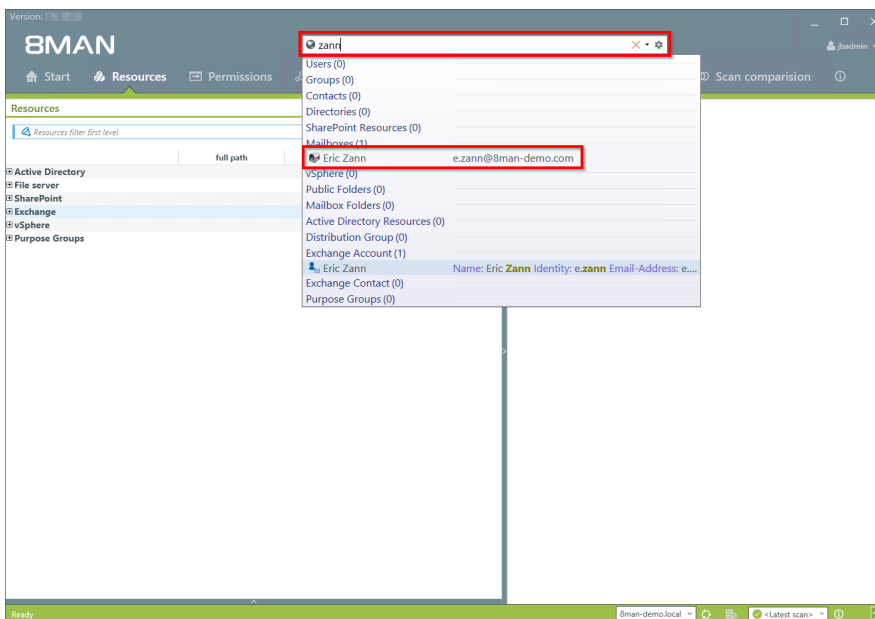


### 8.3.1.2 Change mailbox permissions

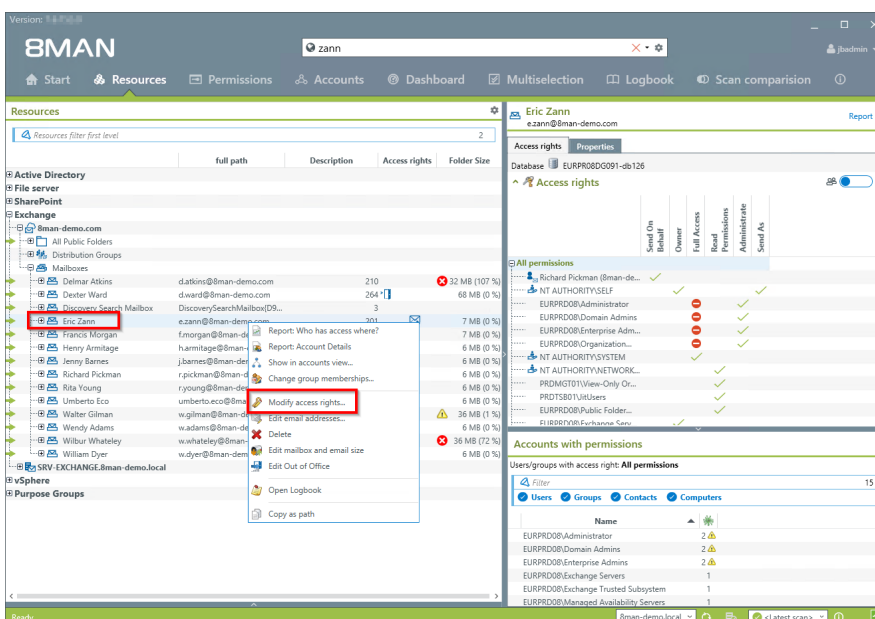
#### Background / Value

8MATE Exchange displays the access rights to Mailboxes in the resource view. Mailbox access rights are shown as follows: "Owner", "Full access", "Read Access rights" and "Administrate". Additionally you can also assign the following access rights to individual users: "Full access", "Send as" and "Receive as".

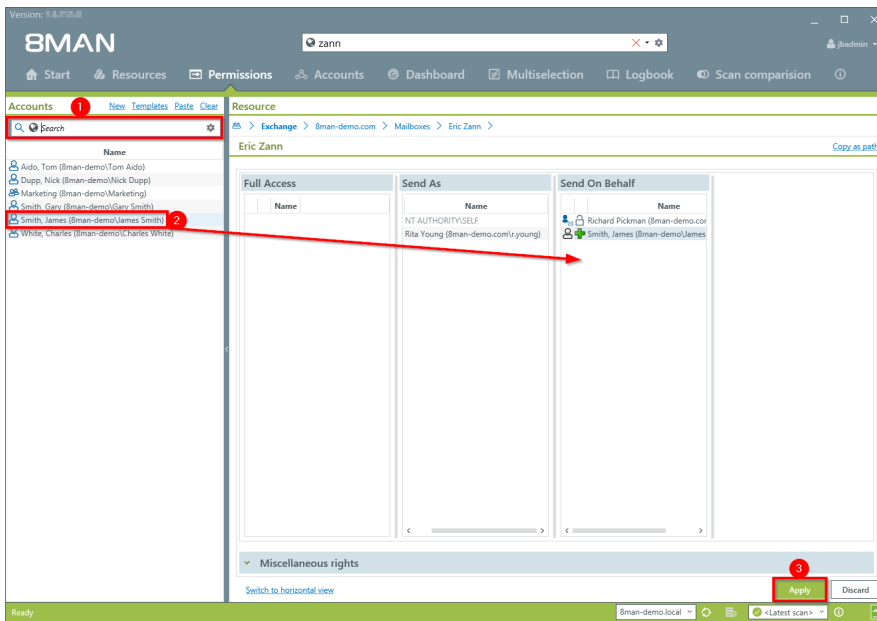
#### Step by step process



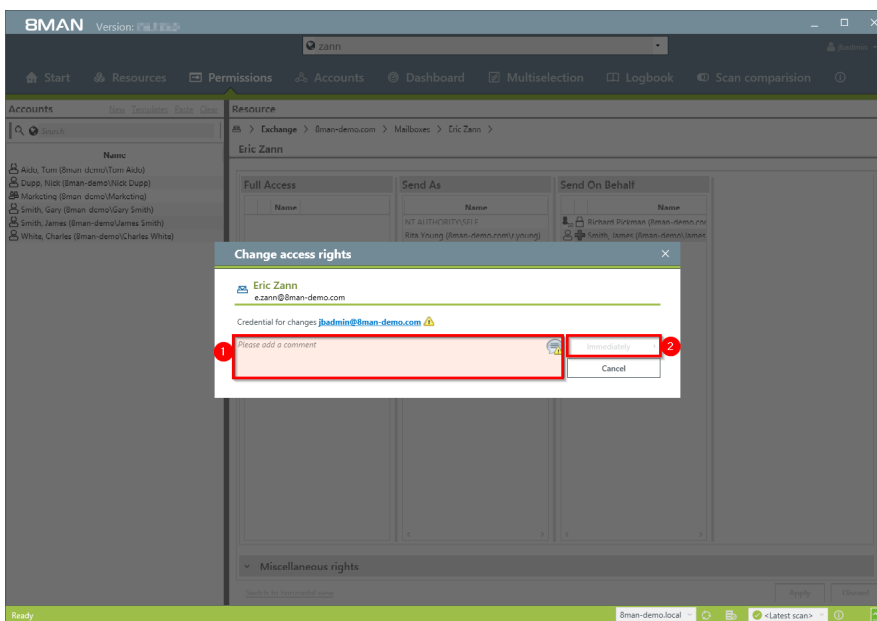
Use the search field to find the desired mailbox.



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".



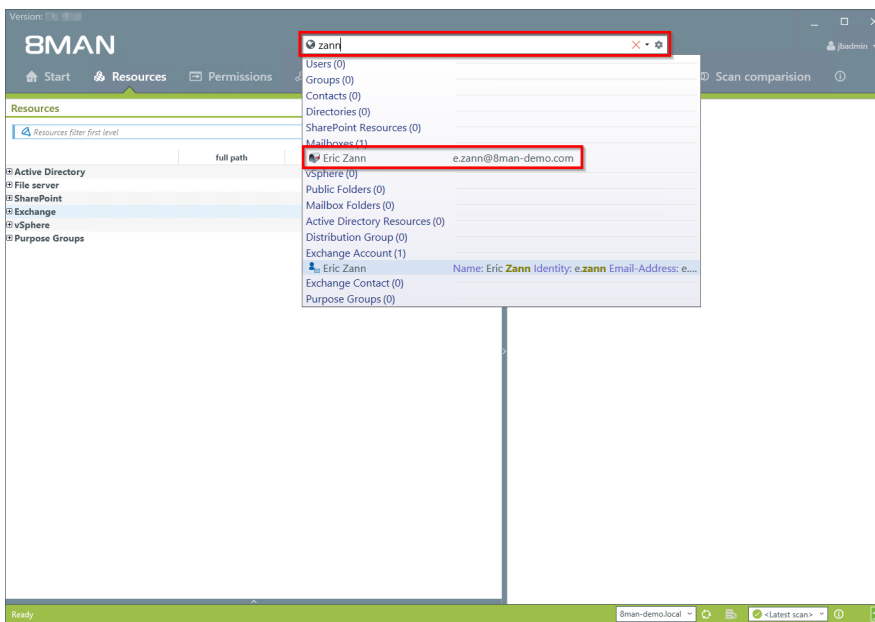
1. You must enter a comment, for example a ticket number.
2. Start the access rights change.

### 8.3.1.3 Manage out of office notices

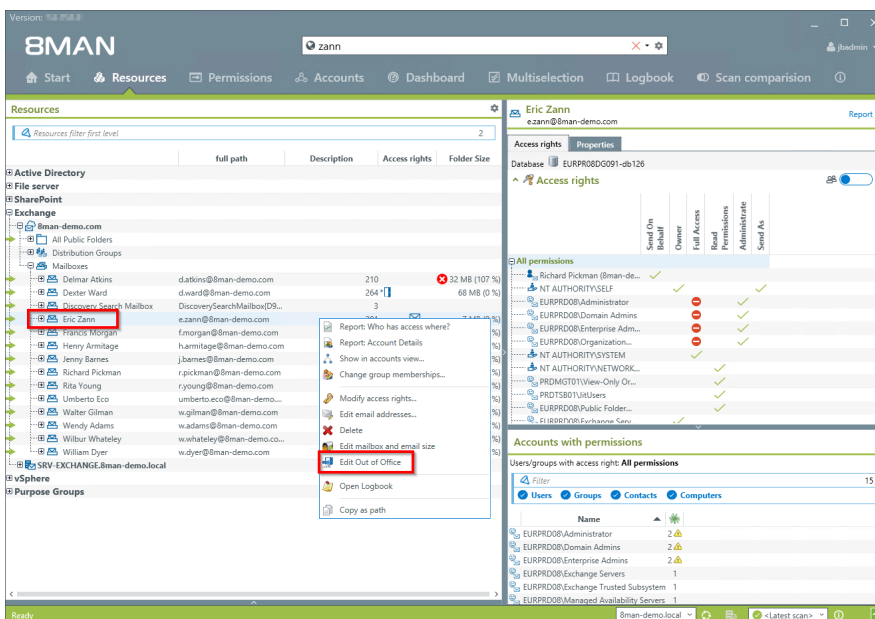
#### Background / Value

8MAN allows help desk to set out of office notices for employees without gaining access to email content.

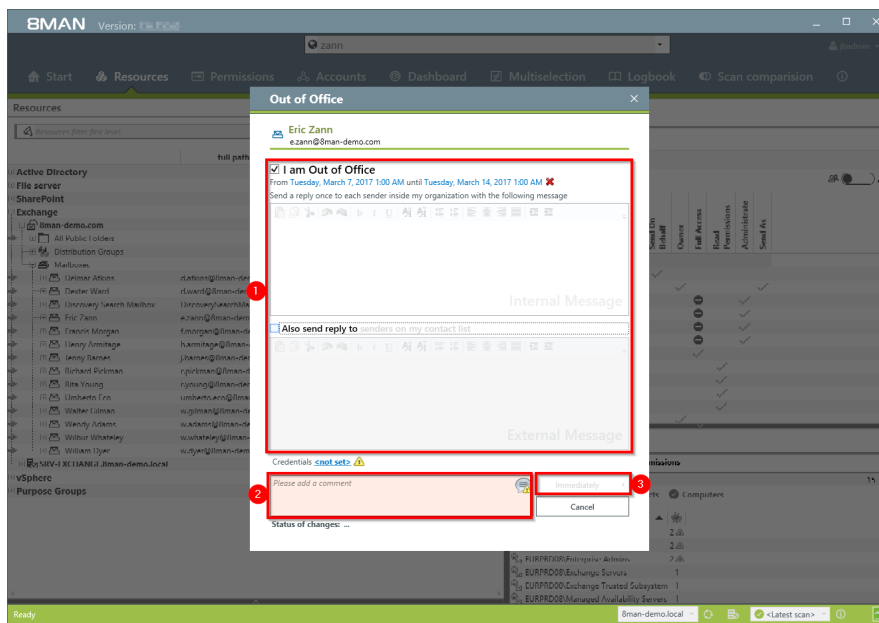
#### Step by step process



Use the search field to find the desired mailbox.



Right-click on the mailbox and select "Edit Out of Office" from the context menu.



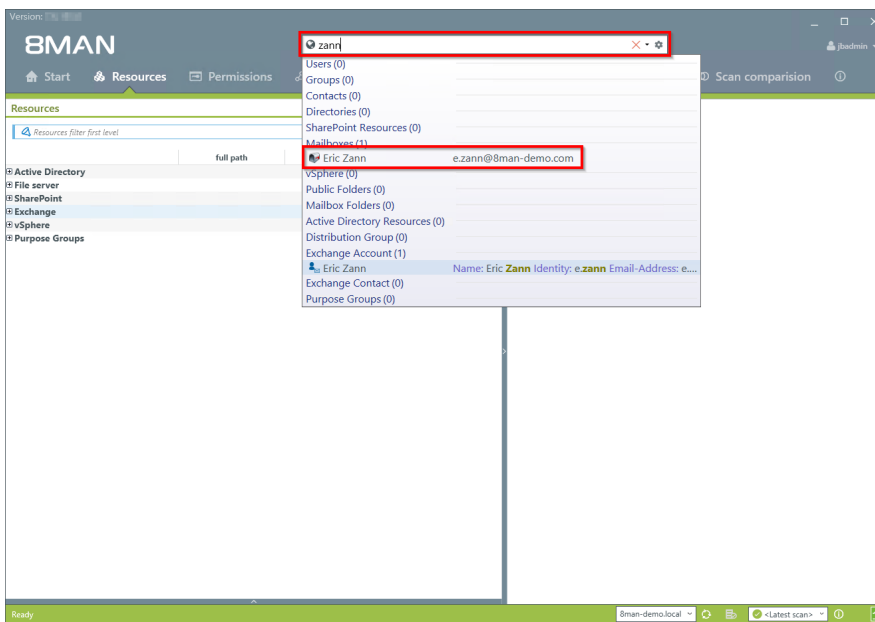
1. Determine the out of office settings.
2. You must enter a comment, for example a ticket number.
3. Start the process.

### 8.3.1.4 Manage mailbox and e-mail size

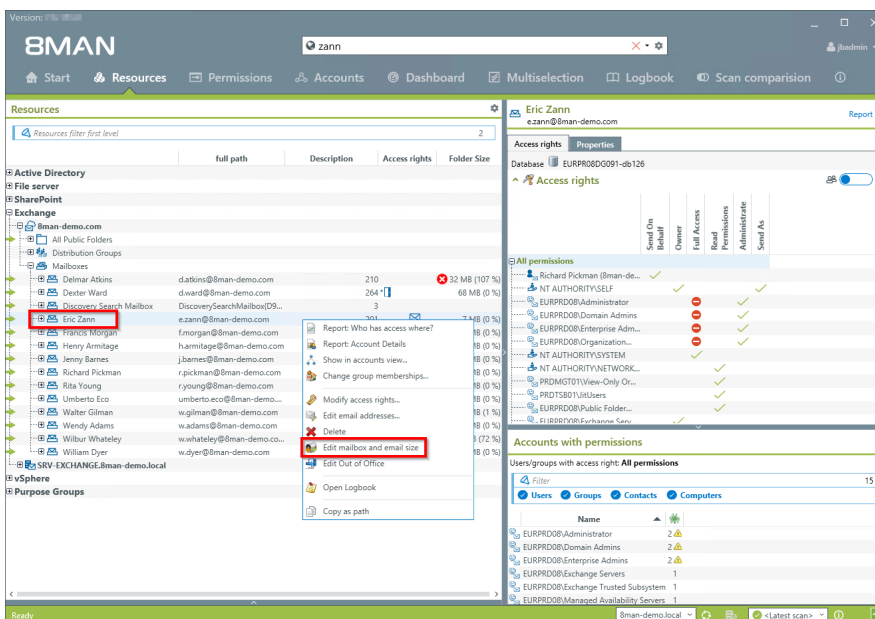
#### Background / Value

Managing mailbox size is a common task for help desk. 8MAN allows you to make these quickly and efficiently.

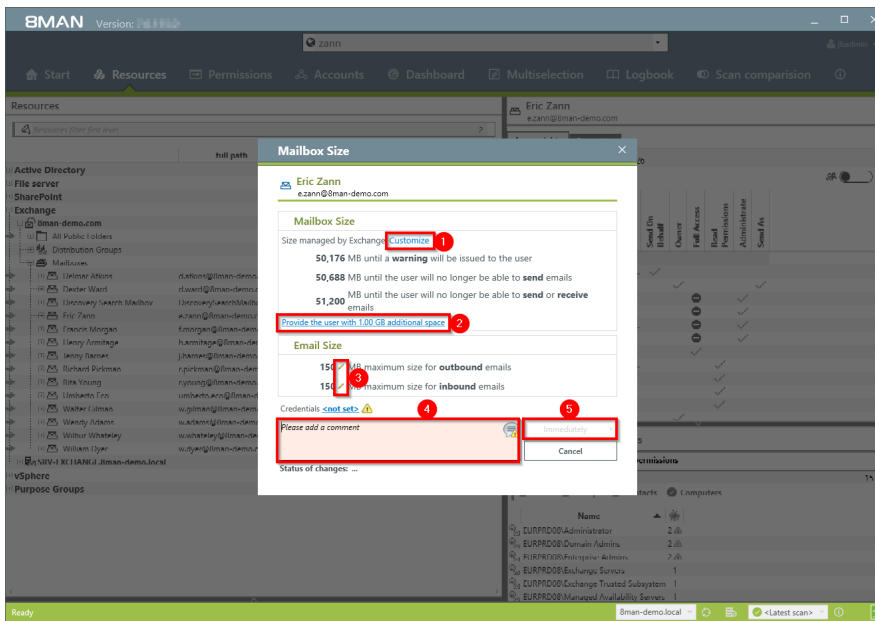
#### Step by step process



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 size.
2. Quickly add 1 GB of storage. The increments can be adjusted in the configuration module.
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.

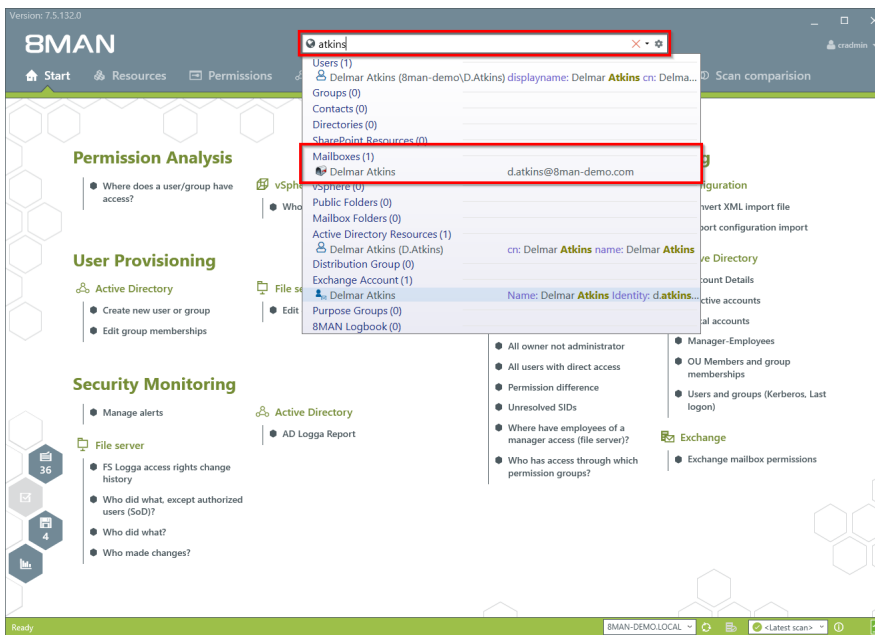
### 8.3.1.5 Manage e-mail addresses

#### Background / Value

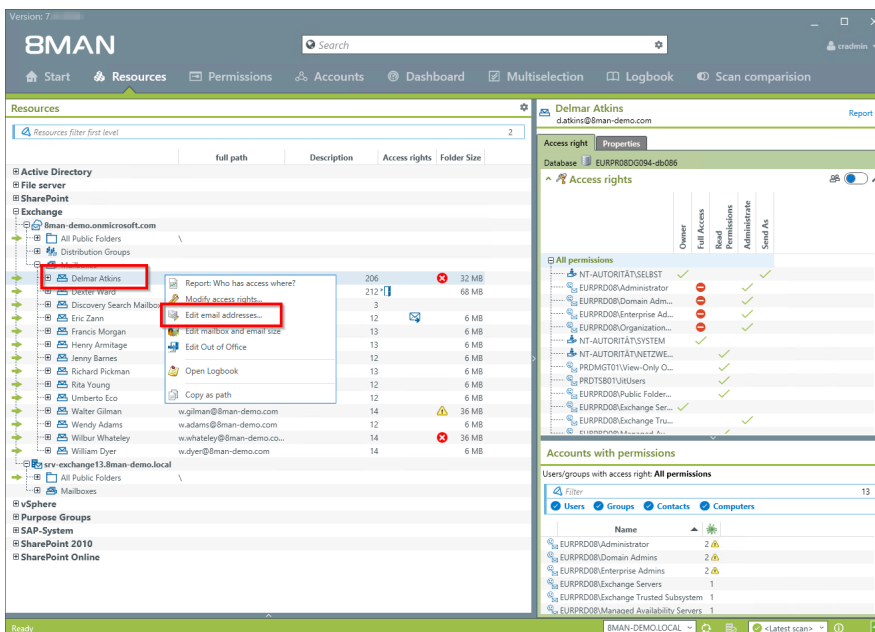
With 8MAN you can assign and remove multiple email addresses to mailboxes, distribution groups and contacts.

The process is documented automatically.

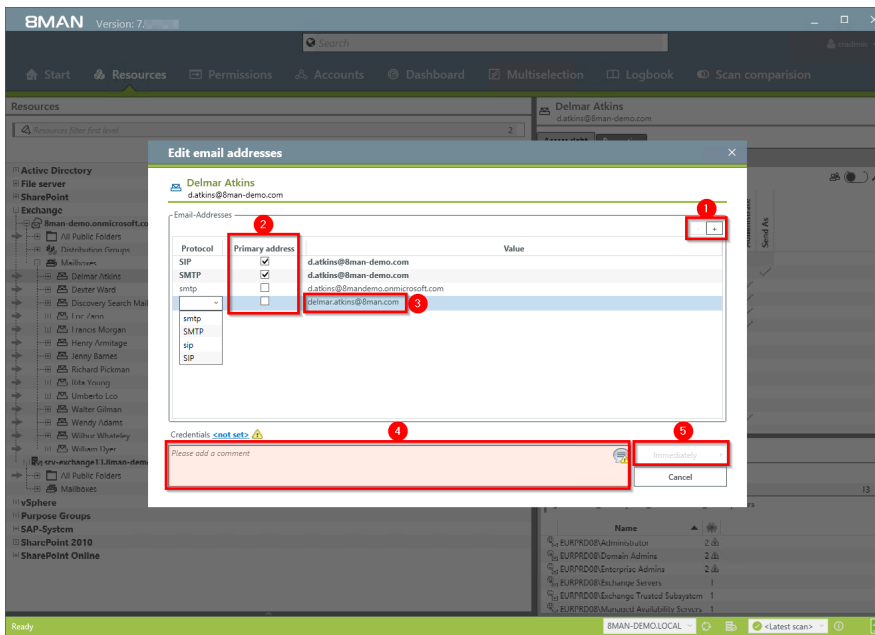
#### Step by step process



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. Select the primary email 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.

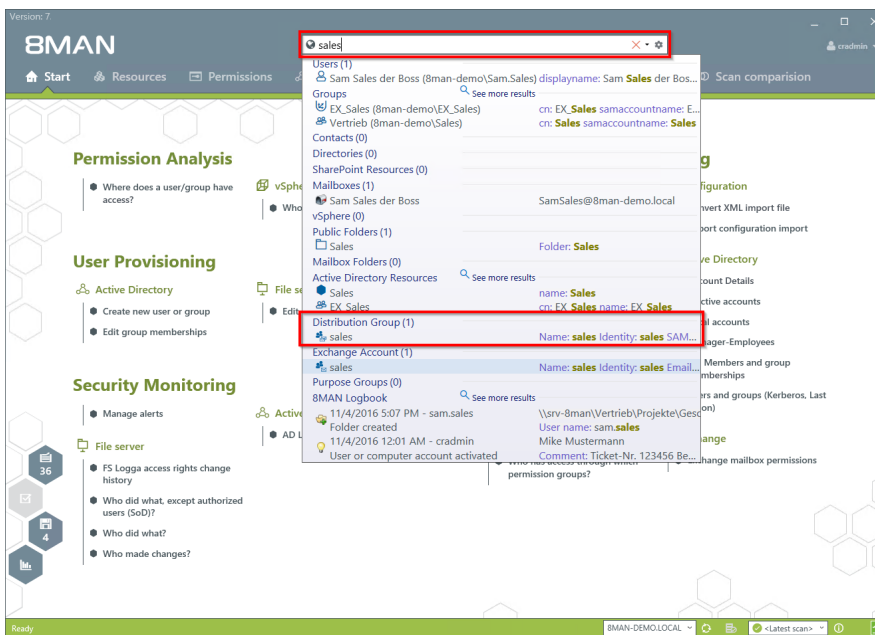


### 8.3.1.6 Manage distribution group memberships

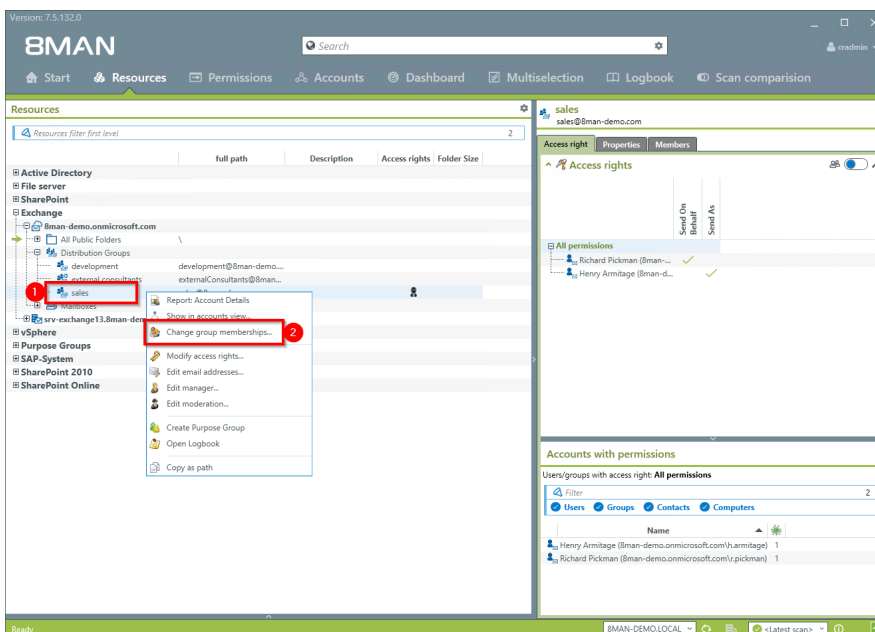
#### Background / Value

8MAN 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.

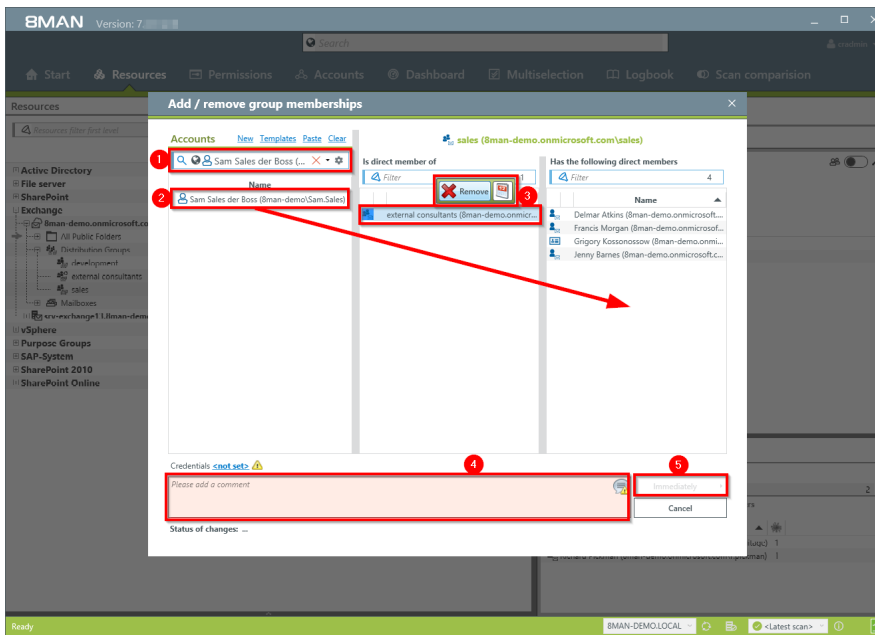
#### Step by Step process



Use the search field to find the desired distribution group.



1. You are focusing on the desired group.
2. Right-click on the group and select "Change group memberships".



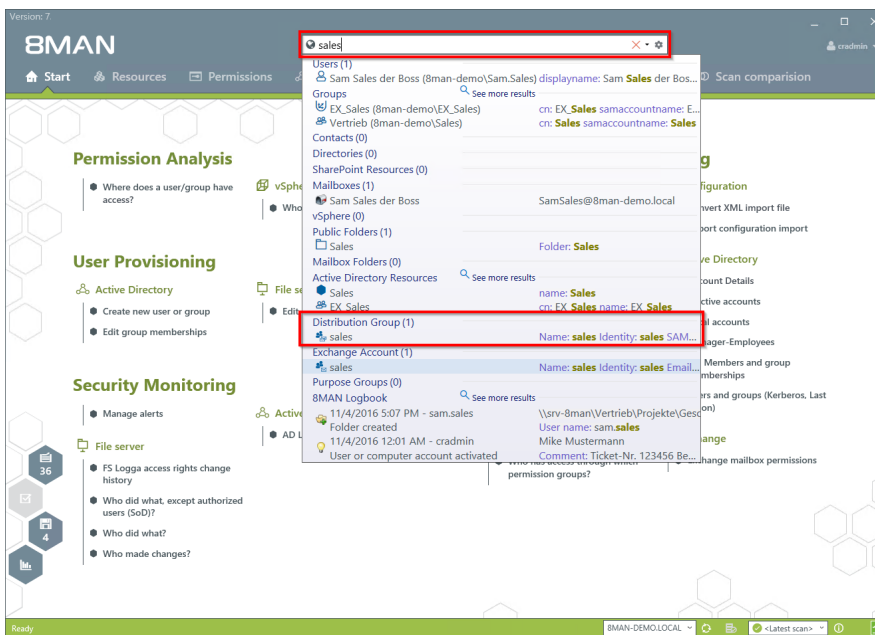
1. Find an account.
2. Use drag & drop to move the account to a column, to assign a group membership.
3. You can remove memberships with the "Remove" button.
4. You must enter a comment, for example a ticket number.
5. Click on "Immediately".

### 8.3.1.7 Manage distribution group permissions

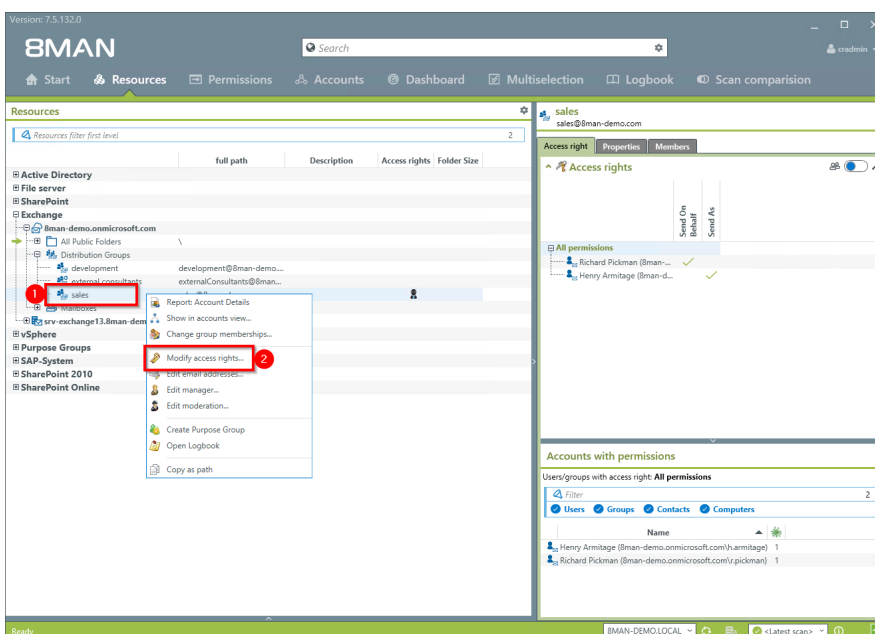
#### Background / Value

8MAN 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.

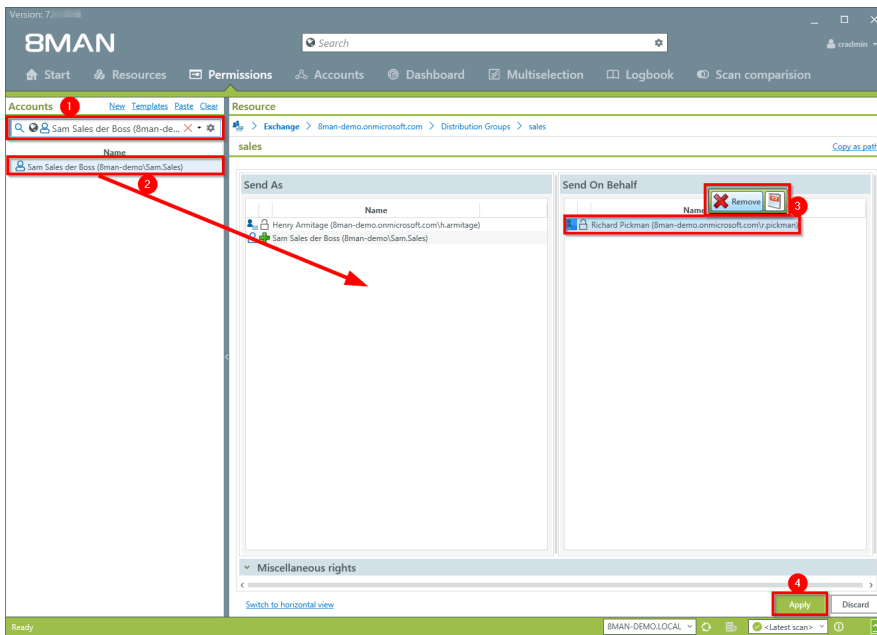
#### Step by step process



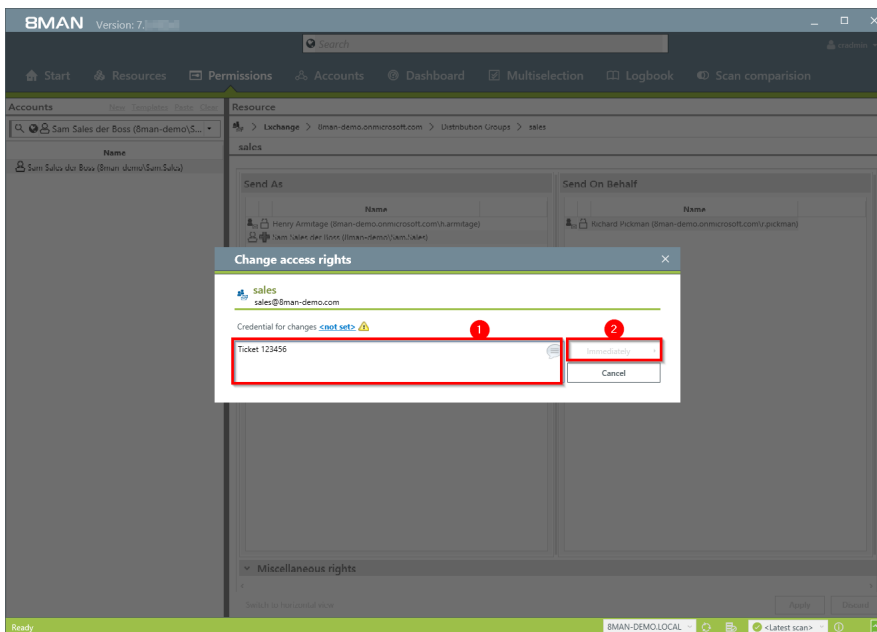
Use the search field to find the desired mailing list.



1. Find 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. Select an entry and use the context menu to remove a permission.
4. Click on "Apply".



1. Enter a comment .
2. Start the access rights change.

### 8.3.1.8 Modify moderation of distribution groups

#### Background / Purpose

With 8MAN 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.

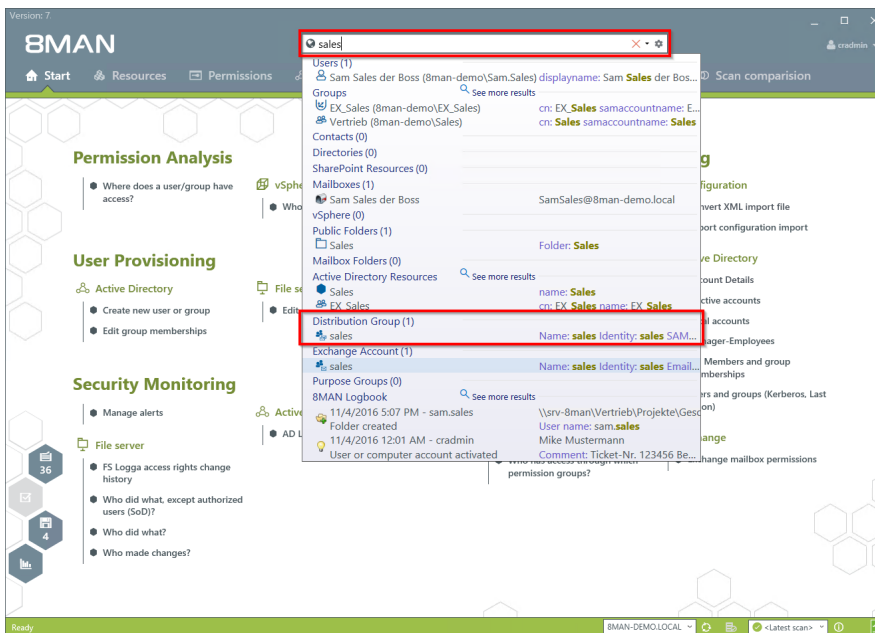
#### Additional Services

Display distribution group properties

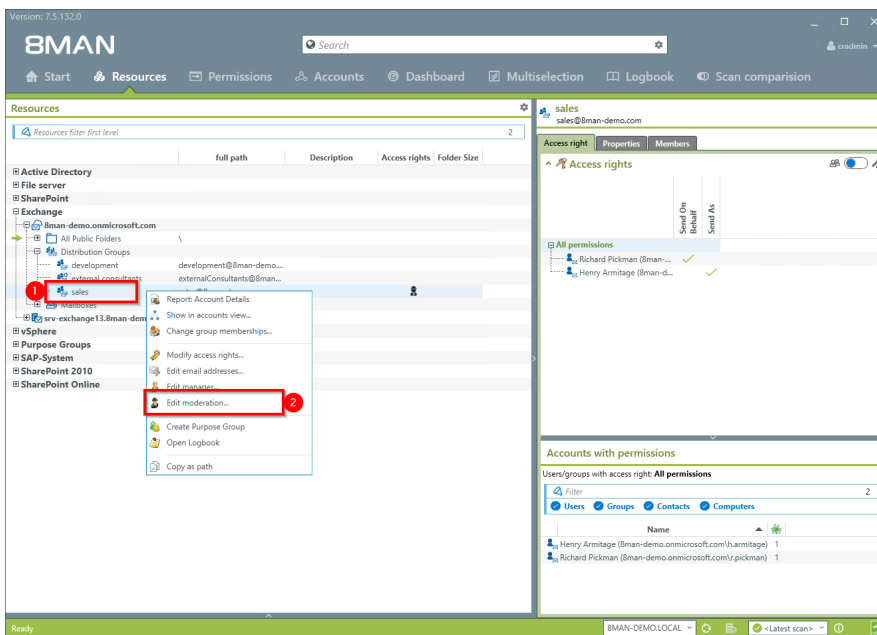
[Change the manager of distribution groups](#)

The change also works for dynamic Exchange groups.

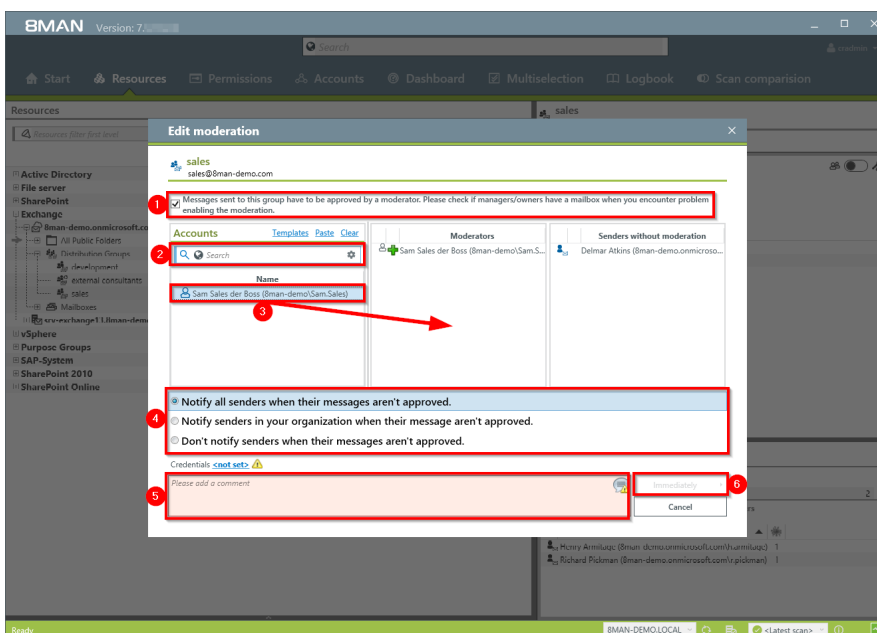
#### Step by step process



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, for example a ticket number.
6. Start the process.

### 8.3.1.9 Change the manager of distribution groups

#### Background / Value

8MAN 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.

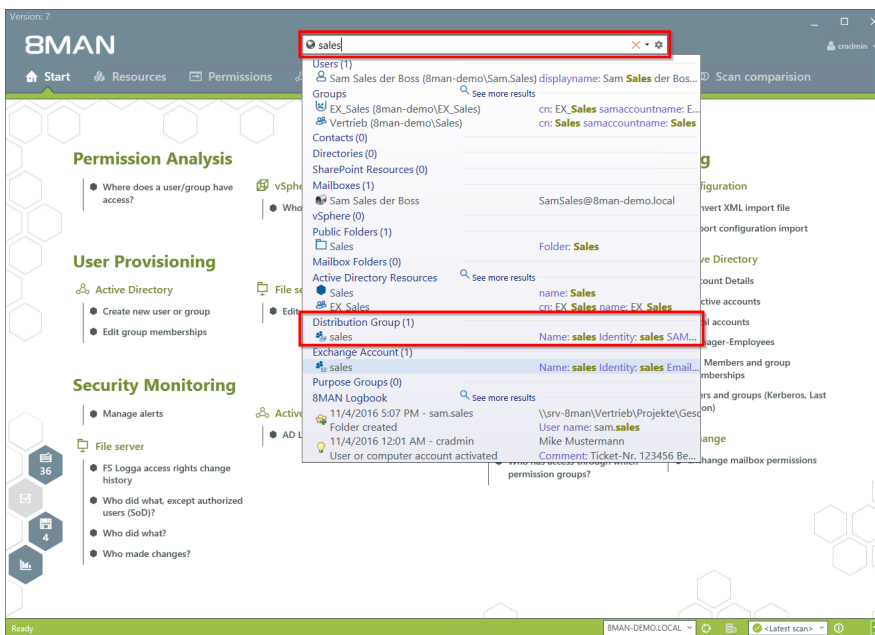
The change also works for dynamic Exchange groups.

#### Additional Services

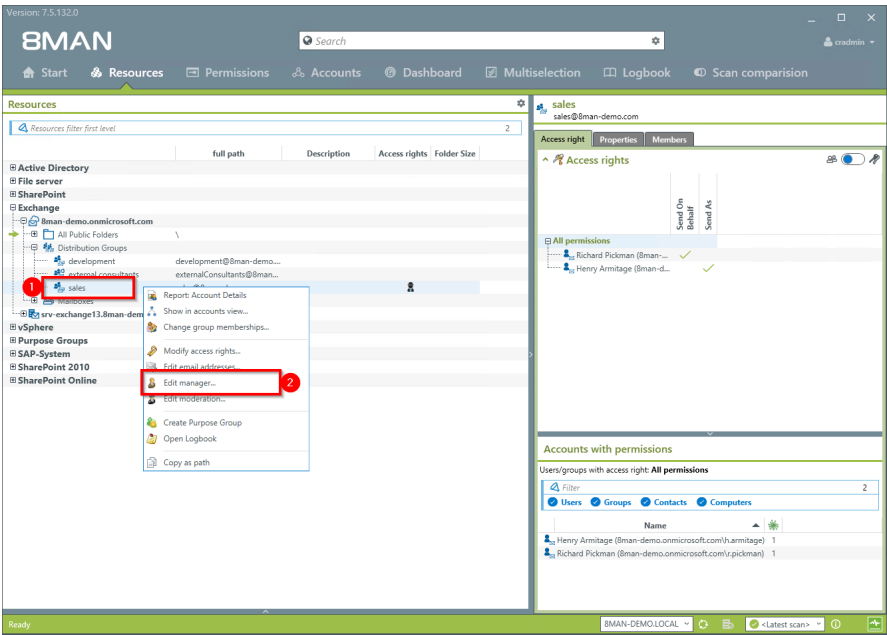
Display distribution group properties

[Modify moderation of distribution groups](#)

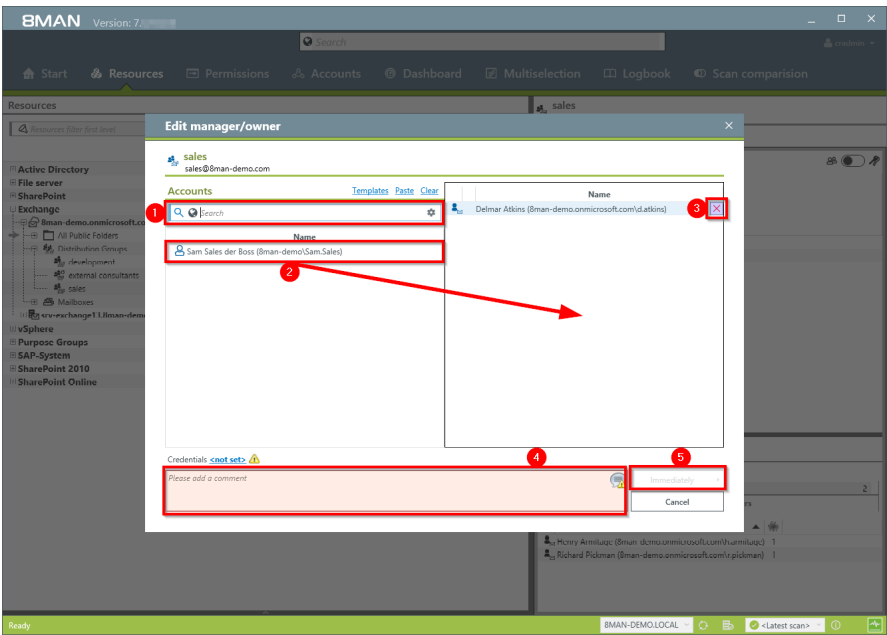
#### Step by step process



Use the search field to find the desired distribution group.



1. You are focusing 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 move accounts to the column "Moderators" or "Send without moderation" (Whitelist).
3. You can also remove accounts.
4. You must enter a comment, for example a ticket number.
5. Start the process.



### 8.3.1.10 Create and delete contacts

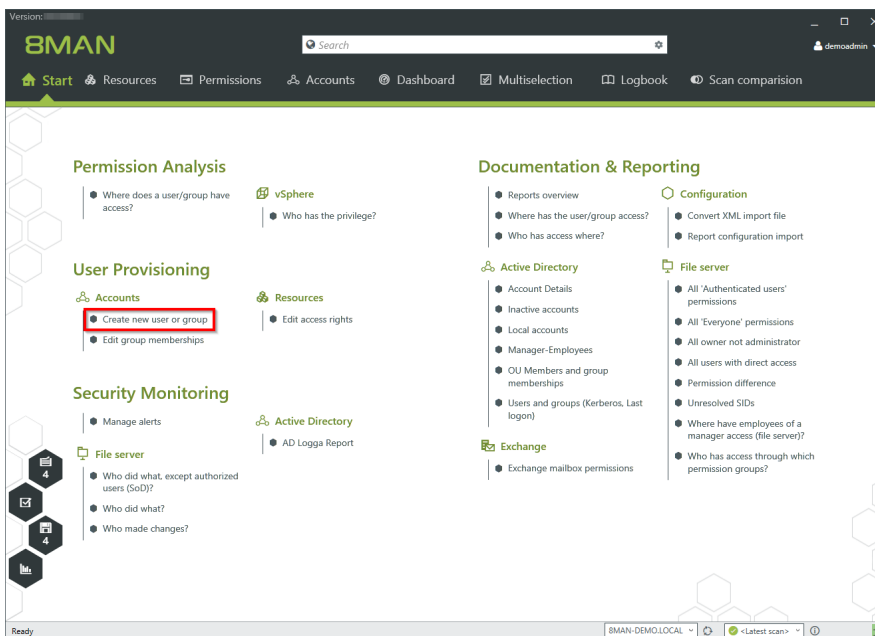
#### Background / Value

With 8MAN, you can documented create contacts and manage them quickly, e.g. to add them to distribution groups.

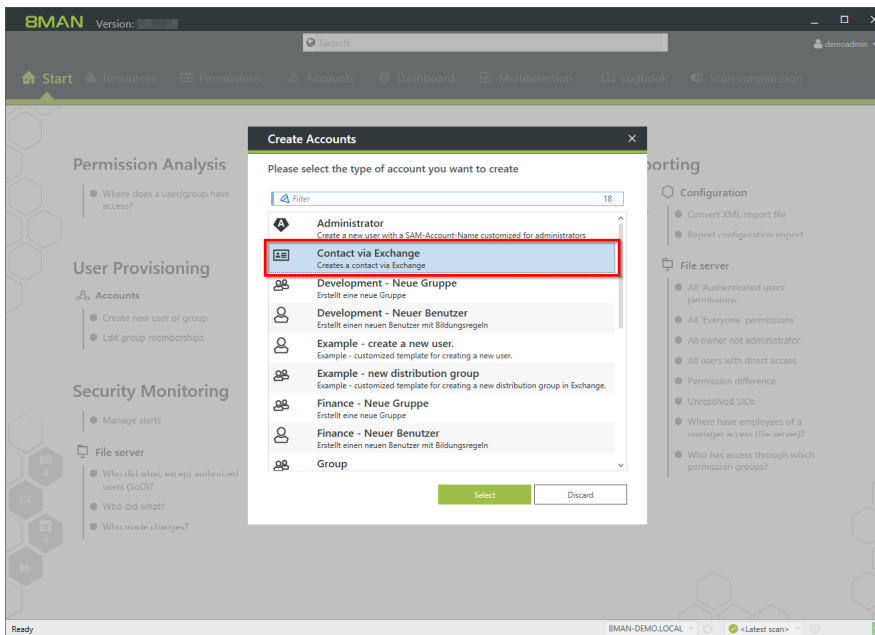
#### Additional Services

##### Manage distribution group memberships

#### Step by step process



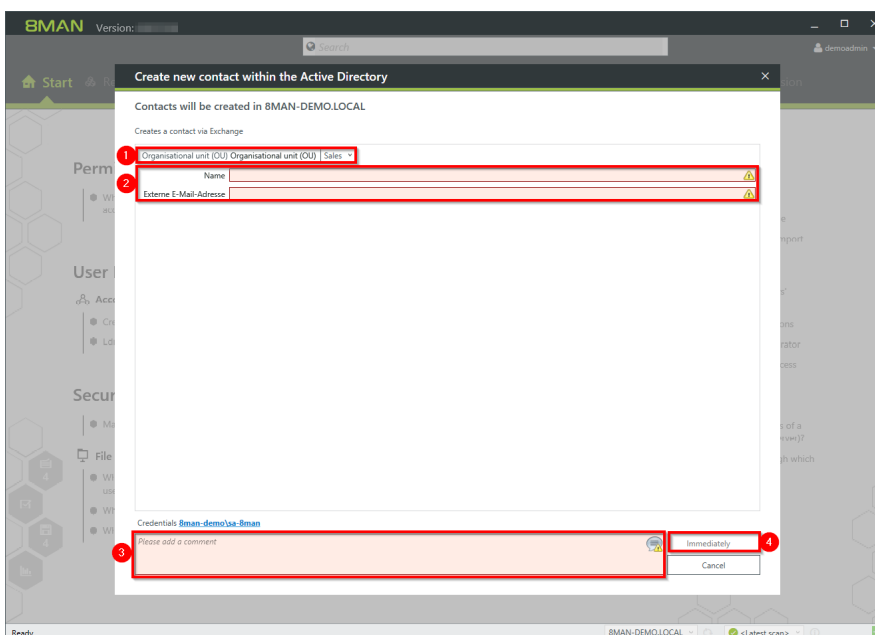
1. Select "Start".
2. Click "Create new user or group".



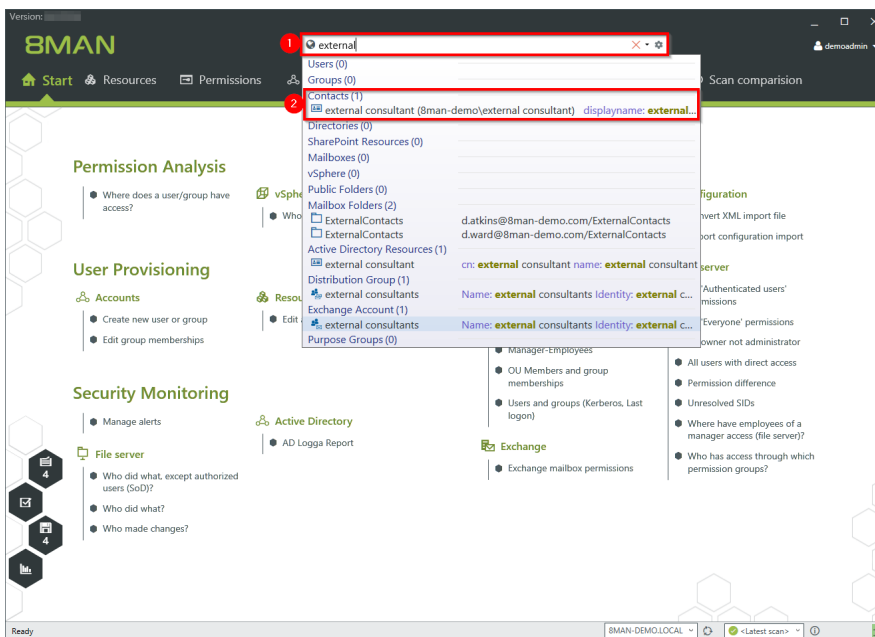
Select a template to create a contact.

8MAN provides a sample template for the creation of contacts. You must customize this template before you can use it. See Customizing Templates Manual.

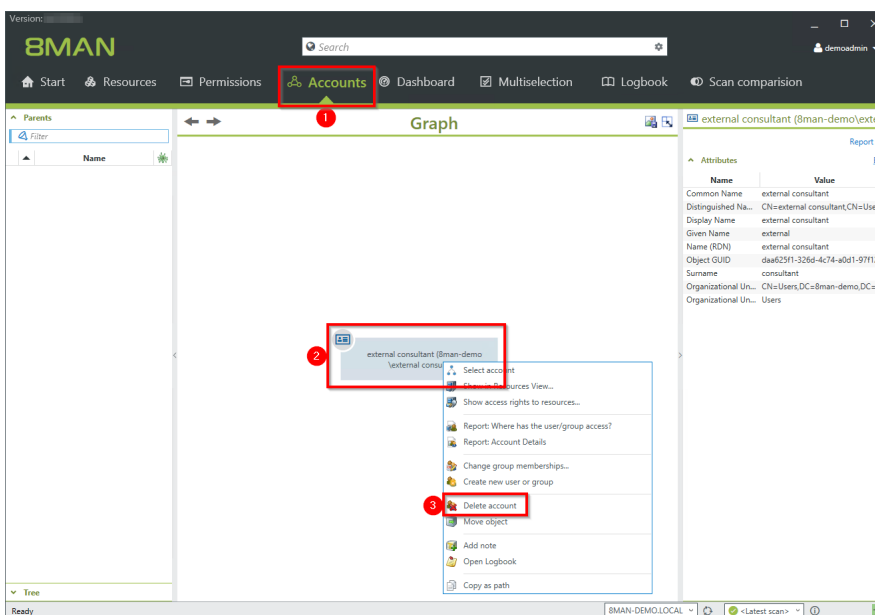
8MAN creates contacts using the Exchange Powershell connection. A license for the 8MATE for Exchange is required.



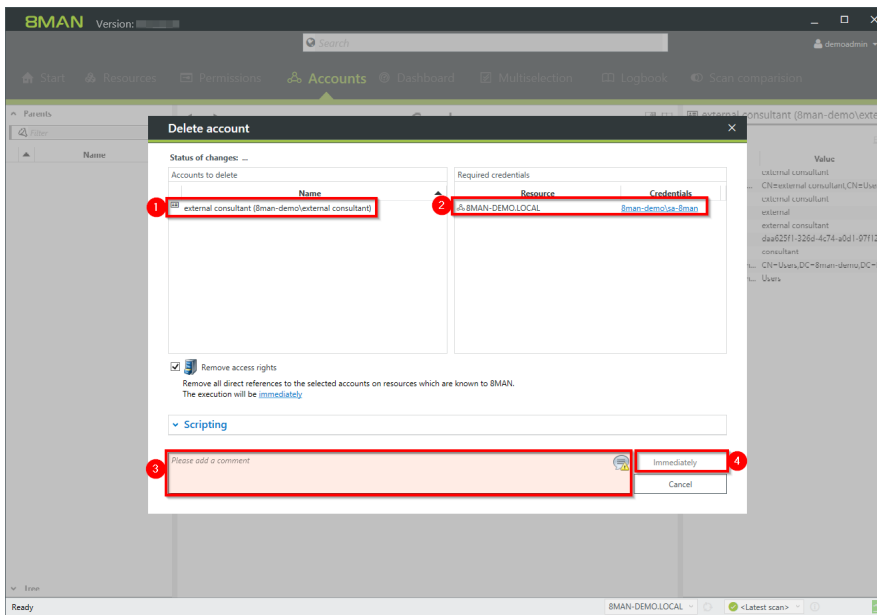
1. Specify an OU.
2. Enter names and email addresses.
3. You must enter a comment.
4. Start the execution.



1. Use the search to find a contact.
2. Click on the search result.



1. 8MAN switches to the Accounts view.
2. Right-click the contact.
3. Select Delete account.



1. 8MAN shows the contact to be deleted.
2. 8MAN shows the login with which the contact is deleted. If necessary, specify other credentials.
3. You must enter a comment.
4. Start the execution.

**You do not need an 8MATE for Exchange license to delete contacts.**

## 8.4 +8MATE for SharePoint

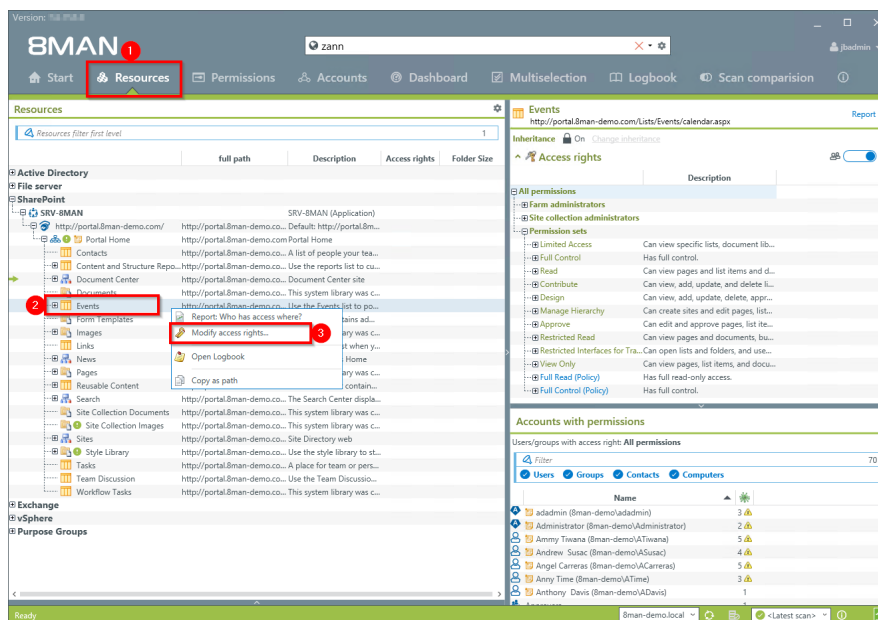
### 8.4.1 Data Owner

#### 8.4.1.1 Manage SharePoint permissions

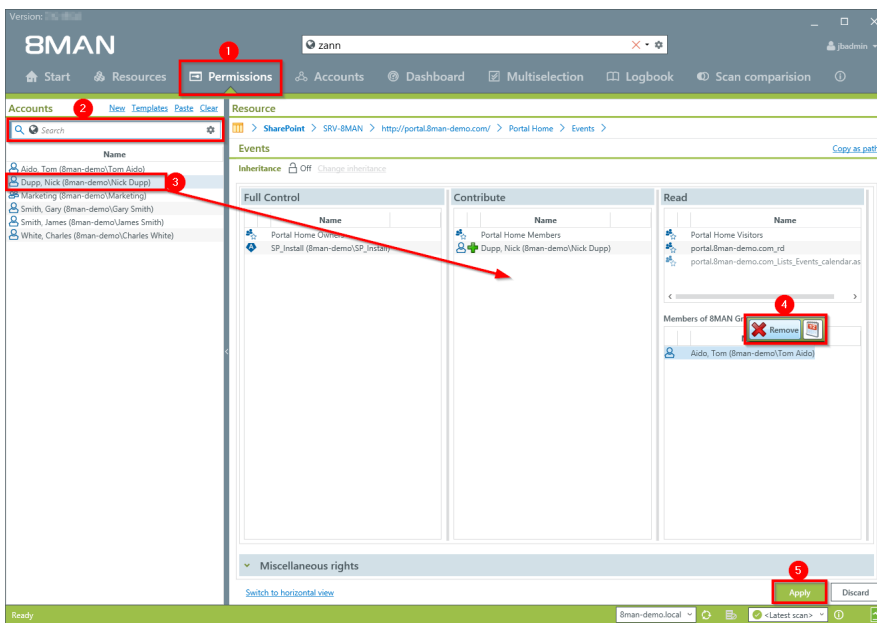
##### Background / Value

8MATE for SharePoint integrates all SharePoint resources into 8MAN. This way 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.

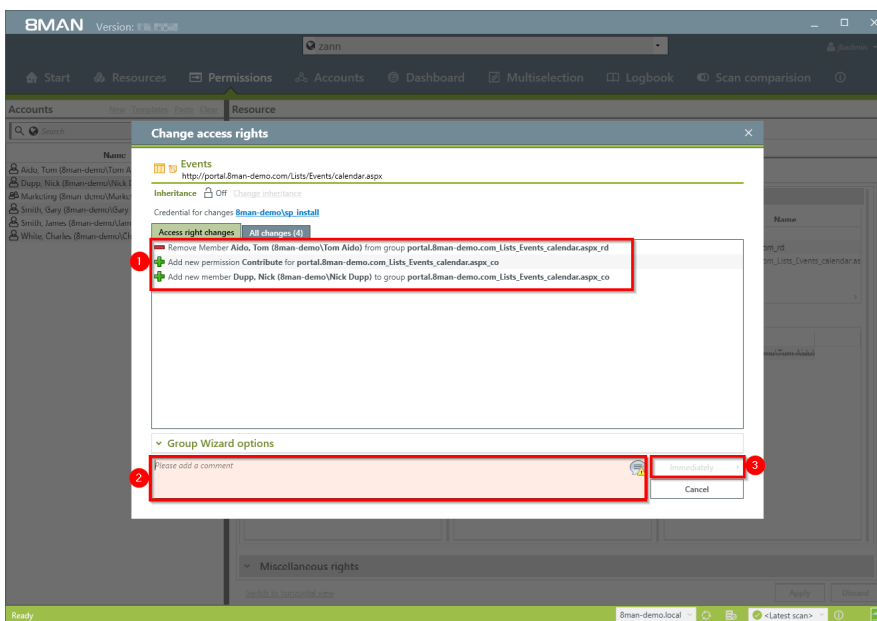
##### Step by step process



1. Select "Resources".
2. Navigate to the desired resource.
3. Right-click on the resource and select "Modify access rights" from the context menu.



1. 8MAN switches to the "Permissions" view.
2. Use the search field to find the desired accounts.
3. Use drag & drop to move an account into an access column to assign access rights.
4. Use the context menu to remove a user.
5. Click on "Apply".



1. Verify planned changes.
2. You must enter a comment.
3. Start the change process.

## 8.4.2 Administrator

### 8.4.2.1 Create SharePoint groups

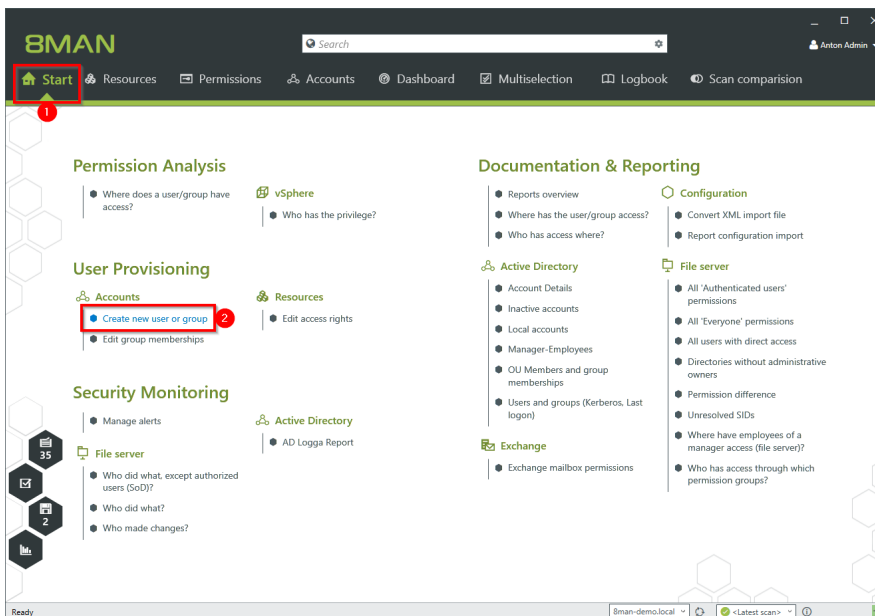
#### Background / Value

SharePoint groups can exist separately from Active Directory on a SharePoint server. Use the SharePoint Remote Connector to easily create new SharePoint groups.

#### Related Services

[Managing access rights to SharePoint resources](#)

#### Step by step process



Select "Create a new user account or group" on the start page.

Create Accounts

×

Please select the type of account you want to create

Filter

22

Group

Create a new group

Manufacturing - Neue Gruppe

Erstellt eine neue Gruppe

Manufacturing - Neuer Benutzer

Erstellt einen neuen Benutzer mit Bildungsregeln

New SharePoint group in http://intranet

Create a new SharePoint group in http://intranet

New SharePoint group in http://portal

Create a new SharePoint group in http://portal

New SharePoint group in https://8mandemo.sharepoint.com

Create a new SharePoint group in https://8mandemo.sharepoint.com

Personalabteilung - Neue Gruppe

Erstellt eine neue Gruppe

Personalabteilung - Neuer Benutzer

Erstellt einen neuen Benutzer mit Bildungsregeln

Select

Close

×

Select the template for the desired SharePoint resource.

Create Accounts

×

New SharePoint group in https://8mandemo.sharepoint.com (Create a new SharePoint group in https://8mandemo.sharepoint.com)  
Accounts will be created in https://8mandemo.sharepoint.com.

Create a new SharePoint group

Name

Description

Owning web site collection

Owner

Who can see the members of this group?

Who can modify the group memberships?

Membership requests

Credentials [not set](#)

Please add a comment

Immediately

Close

×

1. Specify a name for the new group.
2. Optional: Enter a description.
3. Select the site collection to which the group is assigned.
4. Use the search to specify an owner.



**Create Accounts** ✕

New SharePoint group in <https://8mandemo.sharepoint.com> (Create a new SharePoint group in <https://8mandemo.sharepoint.com>)  
Accounts will be created in <https://8mandemo.sharepoint.com>.

**Create a new SharePoint group**

Name:

Description:

Owning web site collection:

Owner: [Dexter Ward \(https://8mandemo.sharepoint.com\)](https://8mandemo.sharepoint.com) ✕ ↺


Who can see the members of this group? 1

Who can modify the group memberships? 2

Membership requests: 2

Credentials [<not set>](#) ⚠

Please add a comment ⚠

  ✕

1. Select who can see the members of the group.
2. Select who can edit the group memberships.

**Create Accounts** ✕

New SharePoint group in <https://8mandemo.sharepoint.com> (Create a new SharePoint group in <https://8mandemo.sharepoint.com>)  
Accounts will be created in <https://8mandemo.sharepoint.com>.

**Create a new SharePoint group**

Name:

Description:

Owning web site collection:

Owner: [Dexter Ward \(https://8mandemo.sharepoint.com\)](https://8mandemo.sharepoint.com) ✕ ↺

Who can see the members of this group?

Who can modify the group memberships? 1

Membership requests: 1


Allow requests to join/leave the group? ☒

Auto accept? ☐

Send requests to the following e-mail addresses:

Credentials [d.ward@8man-demo.com](#) 2

Demo. 3

 4 ✕

1. Determine how membership requests are handled.
2. Specify credentials that have the permissions to create the new group on SharePoint.
3. You must enter a comment.
4. Start the execution.

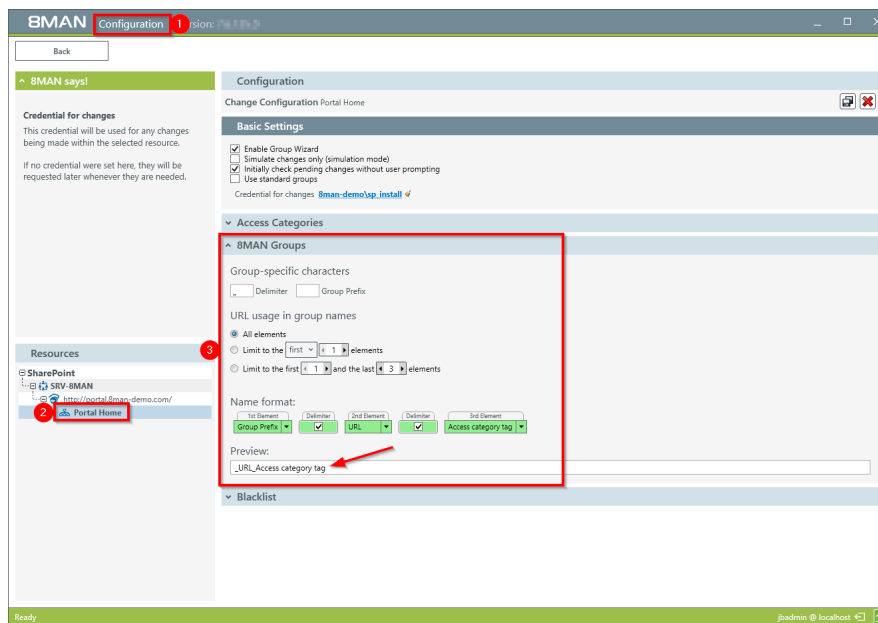
### 8.4.2.2 Determine naming conventions for access groups

#### Background / Value

8MAN puts an end to random naming of groups. Administrators determine the appropriate naming convention, which will be used for all AD groups created with 8MAN.

**Only SharePoint 2010 and 2013 with the 8MATE using the server side object model.**

#### Step by step process



1. Start the configuration module and navigate to "Change Configuration" - >"File server".
2. Select the desired SharePoint resource. You can enter different settings for each resource.
3. Determine the naming convention. Please note that 8MAN will show you a preview.



# 9. Threat & Gap Management



## 9.1 +8MATE Clean!

### 9.1.1 Identify file path names that are too long

#### Background / Value

Placing files on directories whose path name exceeds 260 characters cause all sorts of problems. Programs can't access them and editing functions such as "copy" or "delete" become unavailable.

8MATE Clean! shows all files on directory paths that are too long. We recommend shortening the folder names and/or moving the affected directories to a higher level.

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.2 Archive old file server data

#### Background / Value

Access Rights Management should also include archiving old, unused data, since the less data you have, the easier it is to manage. 8MATE Clean allows you to mark data as "old" based upon specified dates. The most commonly used indicator is the last read or write access.

You can decide if old data is moved to another storage system or remain in the old system when you are migrating to new file server systems.

#### Additional services

If you would like to archive old data we first recommend creating a protected area and storing your old data within.

[8MATE Clean handbook: creating a protected area on a file server](#)

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.3 Push permissions to empty sub-directories through inheritance

#### Background / Value

Empty folders do not need different access rights than their parent directory. The 8MATE Clean! removes them by inheriting the rights of parent folders. This harmonizes the authorization situation on the file server.

#### Additional services

[Deleting empty directories on a file server](#) (MATE Clean!)

8MATE Clean! is managed and operated by our experienced System Engineers.

Contact us for more information: [info@8man.com](mailto:info@8man.com)

### 9.1.4 Delete empty file server directories

#### Background / Value

Empty folders can be automatically deleted. This cleans up the overall structure and prevents unnecessary load on The Kerberos token size.

#### Additional services

If you are not sure of empty folders have been created intentionally please use the following service:

[8MATE Clean! handbook: Pushing permissions to empty subdirectories through inheritance](#)

8MATE Clean! is managed and operated by our experienced System Engineers.

Contact us for more information: [info@8man.com](mailto:info@8man.com)



### 9.1.5 Correct non-canonical access rights

#### Background / Value

Access control entries (ACEs) have a particular order in the DACL depending on their type. Specifically ACEs that deny access are listed before ACEs that grant access. The order of ACEs significantly determines the effective access rights of the user. You may encounter security risks, because applications and programs can not be prevented from writing ACEs in a random order. 8MATE Clean! repairs non-canonical permissions and ensures that standards are reapplied.

#### Additional services

[8MATE Clean! Handbuch: Replacing non-canonical permissions through overarching rights](#)

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.6 Replace non-canonical permissions through overarching rights

#### Background / Value

Access control entries (ACEs) have a particular order in the DACL depending on their type. Specifically ACEs that deny access are listed before ACEs that grant access. The order of ACEs significantly determines the effective access rights of the user. You may encounter security risks, because applications and programs can not be prevented from writing ACEs in a random order. 8MATE Clean repairs non-canonical permissions and ensures that standards are reapplied.

#### Alternative service:

If you would like to ensure that permission differences remain between parent and child directory, please use the following service:

[8MATE Clean! handbook: correcting non-canonical permissions](#)

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.7 Automatically replace critical access rights

#### Background / Value:

There are a number of groups and accounts in the DACL that should not receive permissions under any circumstances. These include the EVERYONE or CREATOR/OWNER accounts. These critical accounts, as well as special Windows accounts are listed in the 8MAN blacklist and can not be granted permissions with 8MAN.

If critical access rights have been granted without 8MAN, then 8MATE Clean! can automatically replace these for you. You can define which groups and direct permissions are replaced by which access rights and 8MATE Clean! will implement your requirements.

#### Alternative services

[8MATE Clean! handbook:Removing critical access rights automatically](#)

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.8 Identify NULL DACLs and replace them with higher level permissions

#### Background / Value

The security descriptor may contain the value "0" for directories. In this case anyone could give themselves access to a directory and its subfolders. Zero DACLs are created through faulty applications that manipulate ACLs.

8MATE Clean! replaces zero DACLs with higher level permissions.

**Please note: Zero DACLs can not be replaced on NetAPP or EMC2 servers. These are present by default.**

8MATE Clean! is managed and operated by our experienced System Engineers.

Contact us for more information: [info@8man.com](mailto:info@8man.com)

### 9.1.9 Replace divergent access rights on a file server

#### Background / Value

Microsoft allows a variety of access categories. "Special rights" in particular often unnecessarily complicate access rights assignments through their granularity and variety of combinations. Protected Networks GmbH recommends working only with 3 access rights:

- Full control
- Modify
- Read & execute

8MATE Clean! allows you to change your access rights structure automatically and according to your specifications. This significantly simplifies access management on your file servers.

#### Additional services

You can change the conventions for creating new permissions to match your ideal standard.

Installations & configuration manual: Selecting the access categories available in 8MAN

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.10 Delete divergent access rights

#### Background / Value

Microsoft allows a variety of access categories. "Special rights" in particular often unnecessarily complicate access rights assignments through their granularity and variety of combinations. Protected Networks GmbH recommends working only with 3 access rights:

- Full control
- Modify
- Read & execute

8MATE Clean! allows you to delete all undesired access rights. This way any users that had access to the affected directories only through this permission path, will lose their access rights.

#### Additional services

8MATE Clean! allows you to modify existing access rights to match your ideal standard.

[8MATE Clean! handbook: Replacing divergent access rights](#)

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.11 Automatically remove critical permissions

#### Background / Value

There are a number of groups and accounts in the DACL that should not be granted permissions. These include the EVERYONE and CREATOR/OWNER accounts. These critical accounts, as well as special Windows accounts are listed in the 8MAN blacklist and can not be granted permissions with 8MAN.

If critical access rights have been granted without 8MAN, then 8MATE Clean!

#### Alternative Services

[8MATE Clean! handbook: Automatically replacing critical access rights](#)

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.12 Remove direct permissions

#### Background / Value

Direct permissions are inefficient because users need to be managed individually. Direct permissions cause unresolved SIDs when user accounts are deleted. These can then be used by other users to gain unauthorized access to sensitive data. Direct permissions also increase the length of the ACL on your file server and consequently the time needed to verify whether a user will get access to the requested resource. They should be avoided and replaced with group permissions.

8MATE Clean! identifies all direct permissions on your file servers and deletes them.

#### Alternative services

If you still want the accounts with direct permissions to have access, we recommend replacing the direct access rights:

[8MATE Clean! Handbook: Replacing direct permissions with group memberships](#)

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**



### 9.1.13 Replace direct permissions with group memberships

#### Background / Value

Direct permissions are inefficient because users need to be managed individually. They should be avoided and replaced with group permissions. 8MATE Clean! identifies all direct permissions on your file servers and turns them into group memberships.

This has the following advantages:

Direct permissions cause unresolved SIDs when user accounts are deleted. These can then be used by other users to gain unauthorized access to sensitive data. Direct permissions also increase the length of the ACL on your file server and consequently the time needed to verify whether a user will get access to the requested resource.

#### Alternative services:

If access should be removed for accounts with direct access, then we recommend deleting all direct permissions.

[8MATE Clean! Handbook: Deleting direct permissions](#)

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.14 Activate inheritance for directories with identical access rights

#### Background / Value:

Sometimes directories have identical access rights within the same tree, but inheritance is still deactivated. 8MATE Clean! identifies these directories and activates inheritance. This simplifies access management as access rights that are granted later to the parent directory are automatically inherited by sub-directories.

#### Additional services:

We recommend the following service in order to further reduce Kerberos token load:

[8MATE Clean! Handbook: Deleting empty folders on file servers](#)

8MATE Clean! is managed and operated by our experienced System Engineers.

Contact us for more information: [info@8man.com](mailto:info@8man.com)

### 9.1.15 Remove permission gaps by aligning directory owners

#### Background / Value

According to Microsoft best practice administrators should be directory owners. If this is not the case, then the directory owner is automatically granted full access. This access right should be reserved for administrators. 8MATE Clean! ensures all directories have administrators as their owners.

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**

### 9.1.16 Automatically reduce the depth of permissions on file servers

#### Background / Value

The maximum depth of permissions is defined in 8MAN configuration from the share level on. Any divergent permissions are considered as "too deep" by 8MAN.

8MATE Clean! replaces divergent permissions beyond the defined maximum with the permissions of higher level folders.

It makes sense to harmonize permissions beyond a certain depth as this limits the complexity of directory management and reduces overall IT effort.

**8MATE Clean! is managed and operated by our experienced System Engineers.**

**Contact us for more information: [info@8man.com](mailto:info@8man.com)**



# 10. 8MAN Application Integration



## **10.1 +8MATE Matrix 42**

### **10.1.1 For Employees**

#### **10.1.1.1 Order Fileserver Access Rights with Matrix 42**

Please contact knowledge management for more information.

[KM@8MAN.com](mailto:KM@8MAN.com)

### **10.1.2 For Data Owners and Administrators**

#### **10.1.2.1 Accept or reject an inquiry in Matrix 42**

Please contact knowledge management for more information.

[KM@8MAN.com](mailto:KM@8MAN.com)

# 11. Appendix





## 11.1 Software license acknowledgments

- Json.net, © 2006-2014 Microsoft, <https://json.codeplex.com/license>
- JSON.NET Copyright (c) 2007 James Newton-King  
<https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md>
- Irony Copyright (c) 2011 Roman Ivantsov <http://irony.codeplex.com/license>
- Jint Copyright (c) 2011 Sebastien Ros <http://jint.codeplex.com/license>
- #ziplib 0.85.5.452, © 2001-2012 IC#Code, <http://www.icsharpcode.net/opensource/sharpziplib/>
- PDFsharp 1.33.2882.0, © 2005-2012 empira Software GmbH, Troisdorf (Germany),  
[http://www.pdfsharp.net/PDFsharp\\_License.ashx](http://www.pdfsharp.net/PDFsharp_License.ashx)
- JetBrains Annotations, ©2007-2012 JetBrains, <http://www.apache.org/licenses/LICENSE-2.0>
- Microsoft Windows Driver Development Kit, © Microsoft, EULA, installed on the computer on which the FS Logga for Windows file servers is installed: C:\Program Files\protected-networks.com\8MAN\driver (Usage only for FS Logga for Windows file server)
- NetApp Manageability SDK, © 2013 NetApp, <https://communities.netapp.com/docs/DOC-1152> (Usage only for FS Logga for NetApp Fileserver)
- WPF Shell Integration Library 3.0.50506.1, © 2008 Microsoft Corporation ,  
<http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx>
- WPF Toolkit Library 3.5.50211.1, © Microsoft 2006-2013, <http://wpf.codeplex.com/license>
- Bootstrap, © 2011-2016 Twitter, Inc, <https://github.com/twbs/bootstrap/blob/master/LICENSE>
- jQuery, © 2016 The jQuery Foundation, <https://jquery.org/license>
- jquery.cookie, © 2014 Klaus Hartl, <https://github.com/carhartl/jquery-cookie/blob/master/MIT-LICENSE.txt>
- jquery-tablesort, © 2013 Kyle Fox, <https://github.com/kylefox/jquery-tablesort/blob/master/LICENSE>
- LoadingDots, © 2011 John Nelson, <http://johncoder.com>
- easyModal.js, © 2012 Flavius Matis,  
<https://github.com/flaviusmatis/easyModal.js/blob/master/LICENSE.txt>
- jsTimezoneDetect, © 2012 Jon Nylander  
<https://bitbucket.org/pellepim/jstimezonedetect/src/f9e3e30e1e1f53dd27cd0f73eb51a7e7caf7b378/LICENSE.txt?at=defaultjquery-tablesort>
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC  
<https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE>
- Mustache.js, © 2009 Chris Wanstrath (Ruby), © 2010-2014 Jan Lehnardt (JavaScript) and © 2010-2015 The mustache.js community <https://github.com/janl/mustache.js/blob/master/LICENSE>
- Metro UI CSS 2.0, © 2012-2013 Sergey Pimenov, <https://github.com/olton/Metro-UI-CSS/blob/master/LICENSE>
- Underscore.js, © 2009-2016 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors  
<https://github.com/jashkenas/underscore/blob/master/LICENSE>
- Ractive.js, © 2012-15 Rich Harris and contributors,  
<https://github.com/ractivejs/ractive/blob/dev/LICENSE.md>

- RequireJS, © 2010-2015, The Dojo Foundation, <https://github.com/jrburke/requirejs/blob/master/LICENSE>
- typeahead.js, © 2013-2014 Twitter, Inc, <https://github.com/twitter/typeahead.js/blob/master/LICENSE>
- Select2, © 2012-2015 Kevin Brown, Igor Vaynberg, and Select2 contributors <https://github.com/select2/select2/blob/master/LICENSE.md>
- bootstrap-datepicker, © Copyright 2013 eternicode <https://github.com/eternicode/bootstrap-datepicker/blob/master/LICENSE>
- RabbitMQ, © Copyright 2007-2013 GoPivotal, <https://www.rabbitmq.com/mpl.html>
- EPPlus, JanKallman, <https://github.com/JanKallman/EPPlus/blob/master/LICENSE>