

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?





CEO Protected Networks



Matthias Schulte-Huxel

CSO Protected Networks

hallies aufe- Jem

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

1	Why?	14	
1.1	Protecting data, information and knowledge15		
1.2	Decentralize security expertise	16	
1.3	Simplify Security		
2	The Core Disciplines of ARM	19	
2.1	Permission Analysis	21	
2.2	Documentation & Reporting		
2.3	Security Monitoring	23	
2.4	Role & Process Optimization	24	
2.5	User Provisioning	25	
3	Additional ARM disciplines	27	
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	
4	Permission analysis	41	
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 Indentify overpriviledged users (based on Keroberos 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 serve	er	73
	4.2.1 S	ervices 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 S	ervices 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
		lelp Desk	

	4.3.1.1	Identify access rights on mailboxes	
	4.3.1.2	Identify mailbox properties	
	4.3.1.3	Identify access rights on public folders	
	4.3.1.4	Identify permissions on distribution groups	
	4.3.1.5	Identify members of distribution groups	101
4.4	+8MAT	E 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	+8MAT	E for Dynamics NAV	106
	4.5.1	Analyze Dynamics NAV permissions	106
5	Docum	nentation & Reporting	108
5.1	All Tec	hnologies	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 und 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	



	5.2.3.1	Add notes to user accounts and groups	125
	5.2.3.2	Purpose Groups: Give aliases to groups	
	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 serve	er	131
	5.3.1 N	lanagement 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?	
	5.3.2 R	eports for Administrators	137
	5.3.2.1	Identify usage of "everyone"	
	5.3.2.2	Who has access through which permission groups?	
	5.3.2.3	Permission differences	
	5.3.2.4	Identify unresolved SIDs	
	5.3.2.5	Identify direct permissions	
	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 N	lanagement 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 N	lanagement Reports	156
	5.5.1.1	Who has access where?	156
	5.5.1.2	Where do users and groups have access?	158
6	Security	Monitoring	160
6.1	Active Di	rectory	

	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	Fileserve	r	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	e	204
	6.3.1 N	Nonitor 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
7	Role & F	Process Optimization	210
7.1	Delegati	on of tasks	211
	7.1.1 A	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 Administr	ato.r. 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 O	wner: Recertification of existing access rights	235
	7.3.1	E-mail notifications for recertification	238
7.4	+8MAT	E 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	+8MAT	E 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
8	User P	Provisioning	266
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 H	lelpdesk	. 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 D	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 serve	er	349
	8.2.1 D	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 A	dministrator	. 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	
	8.2.2.7	Identify errors in inheritance in Analyze & Act and fix them in bulk …	
8.3	+8MA1	E for Exchange	
	8.3.1	Help Desk	
	8.3.1.1	Create a mailbox (e-mail enable users)	
	8.3.1.2	Change mailbox permissions	
	8.3.1.3	Manage out of office notices	
	8.3.1.4	Manage mailbox and e-mail size	
	8.3.1.5	Manage e-mail addresses	
	8.3.1.6	Manage distribution group memberships	
	8.3.1.7	Manage distribution group permissions	
	8.3.1.8	Modify moderation of distribution groups	
	8.3.1.9	Change the manager of distribution groups	
	8.3.1.1	Create and delete contacts	
8.4	+8MAT	E for SharePoint	
	8.4.1	Data Owner	
	8.4.1.1	Manage SharePoint permissions	
	8.4.2	Administrator	
	8.4.2.1	Create SharePoint groups	
	8.4.2.2	Determine naming conventions for access groups	
9	Threat	t & Gap Management	406
9.1	+8MA1	E Clean!	407
	9.1.1	Identify file path names that are too long	
	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
10	8MAN	Application Integration	424
_		Application Integration	
_	+8MAT		425
_	+8MAT	E Matrix 42 For Employees	425 . 425
_	+8MAT 10.1.1 10.1.1.1	E Matrix 42 For Employees	425 425 425
_	+8MAT 10.1.1 10.1.1.1	E Matrix 42 For Employees Order Fileserver Access Rights with Matrix 42 For Data Owners and Administrators	425 . 425 . 425 . 425
_	+8MAT 10.1.1 10.1.1.1 10.1.2 10.1.2.1	E Matrix 42 For Employees Order Fileserver Access Rights with Matrix 42 For Data Owners and Administrators	425 . 425 . 425 . 425 . 425
10.1 11	+8MAT 10.1.1 10.1.1.1 10.1.2 10.1.2.1 Appen	 For Employees Order Fileserver Access Rights with Matrix 42 For Data Owners and Administrators Accept or reject an inquiery in Matrix 42 	425 . 425 . 425 . 425 . 425 . 425 426







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?

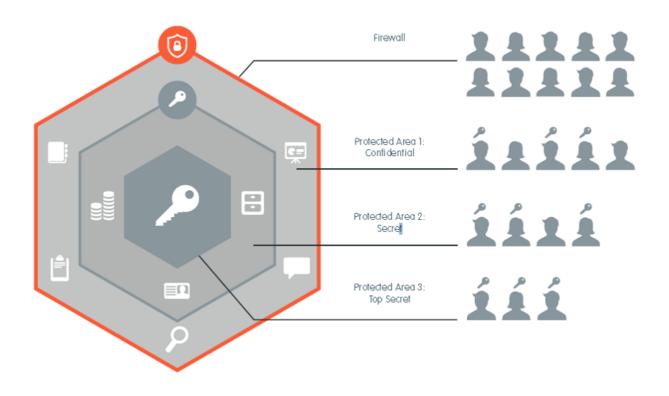
Directory level

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.



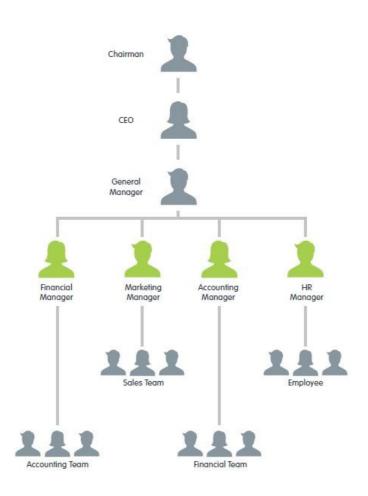
1.2 Decentralize security expertise

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:

Marketing Properties General Sharing Security Previous Versions Cust Full Contro List folder contents Write Special permission NTFS Modify Read & Read General Sharing Security Pre L Marketing Object name: D. Marke 🗆 🎢 All per - - R Full Control **** ъ -**** **** ons for Ma **** - - - R Special per 6 → → → → Modify → → → ▲ △ Sie, Peer (Peer Sie) → → → ▲ △ I_DS_Marketing_md Ъ ъ 6 8 8MAN Group r, Ann (Ann.Geber) 2 ********** D 5 Ka, Ede (Ede Ka) Dee, Dan (Dan Dee) ъ Permi Share Auditing Effective Access ъ Krise, Christiane (Christiane..... ъ Permission entries: Type Principal 22, Allow ERSTELLE 23, Allow StSTEM 24, Allow Administr 24, Allow LDS, Ma 24, Allow LDS, Ma 24, Allow LDS, Ma 24, Allow Cradmin (🌲 ඵ Fred Chen (Fred.Chen) 30 30 Access Full control Full control Full control Modify Modify Read & exec Full control -BESTZER None None None None Frido Fleia (Frido.Fleia) Prido Fieia (Frido-Fieia) Dampf, Hans (Hans Dampf) Pape (Hans (Hans Dampf) Pape (Hans (Hans Dampf) Maria Makketing (Maria.Mak... Read & e Add Re Sam Sales der Boss (Sam.Sal... 30 30 Enable inheritance - Read & execute OK. Cancel App

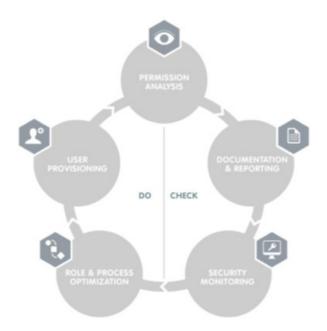
8MAN Access Rights Management makes security efficient:

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: <u>8MATE for Exchange</u>

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 securityrelevant 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 addons:

Active Directory

Fileserver

8MATE FS Logga

8MATE AD 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 <u>8MATE GrantMA</u> 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: <u>8MATE GranMA</u>: The ARM Self 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

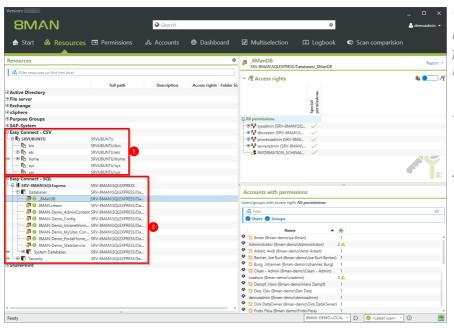
Background / Value

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"

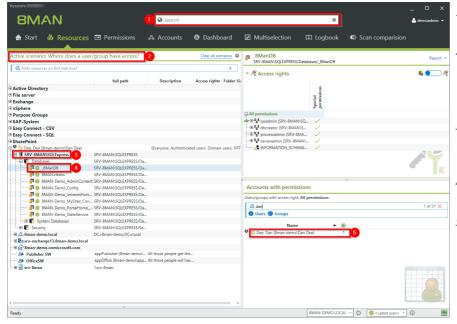
3.1.4.1 Analysing Easy Connect resources



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.

34 | Access Rights Management



- 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 8MANtypical style.



3.1.4.2 Create a report for an Easy Connect Resource

- 8MAN \varTheta Sec ۵ 🔒 Start & Re: 🖃 Pe SRVUBUNTU Report ∧ 𝑘 Access rights full path Active Dir File serve Exchange Syphere Special permissions All permission - sq Accounts with perr Users/groups with access right: All per dan Users Groups 0 of 3 🗙 OCAL 🗸 🗘 🙋 <Latest sca ~ (i) □ × 8MAN Vers Who has access wh Who has access where? 4 Access right report on res Objects a Paths 🔵 🔵 🔒 Organizational cate SRVUBUNTU • • • • Levels to resolve under the selected re tes of groups to purpose group name ✓ Translate ✓ Details ✓ Filter Group setting: ~ Options Settings tput format is <u>PDF</u> ~ execution mode <u>started m</u> i storage path is <u>not config</u> mail is <u>Deactivated</u>
- 1. Choose "Resource" view
 - 2. Select a resource, e.g. "SRVUBUNTU".
 - •••• 3. Choose the report: "Who has access where?" from the context menu.

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

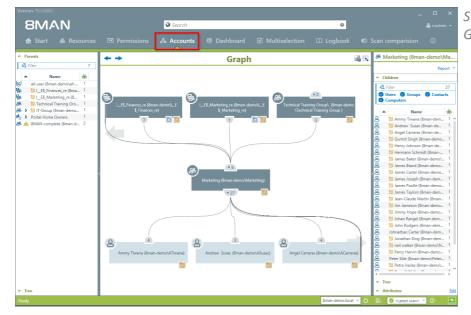
Background / Value

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.

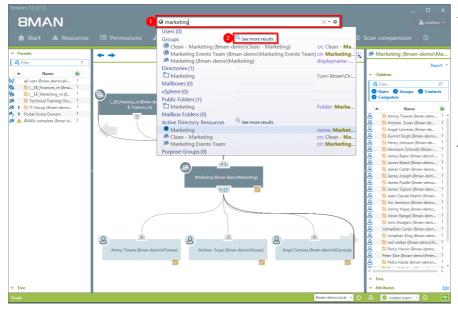
Additional Services

Identifying the depth of nesting in your AD Identifying recursive groups

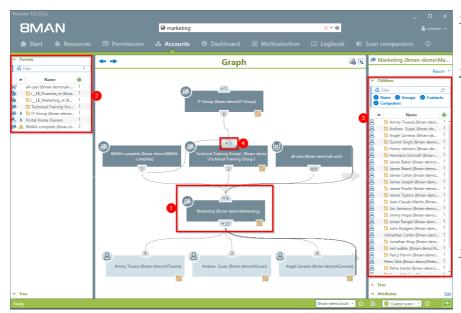
Step by step process



Switch to Accounts in the AD Graph view.



- 1. Find the AD group by entering its name into the search field. For example: "Marketing". Select the desired result from the Activer Directory Resources section of the drop-down.
- 2. If you can't find your resource click on "show further results".



- 1. The "Marketing" group is the focus of the following analysis.
- 2. Above the group you see 4 other groups in the AD graph that the "Marketing Group is a member in, the so-called "parents". All "parent" groups, both direct and indirect, are listed on the left-hand side. Indirect "parents" are indicated by a blue arrow.
- 3. On the right hand side you can see the name of the group listed at the top. Underneath it you can see a list of all "children", both direct and indirect, of the group.
- 4. You can open and close the individual branches on the AD graph by clicking on the icon. The number listed indicates the number of direct "parents" or "children".

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.

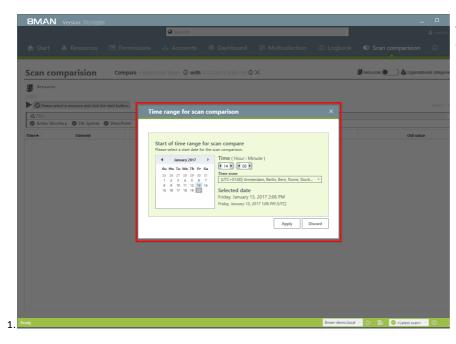
Additional Services

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 <u>Report on Permission</u> <u>Differences</u>.

ersion: 7.								_ 🗆 ×
8MA	١N		Search			\$	0	
							Scan comparision	ו ()
Scan co	mparision	2 Compare <u><late< u=""></late<></u>	est scan time> () with	<u>1/13/2017 2:06 PM (</u>	0×		🗿 Resources 💽 🛔 Organi	zational categories
Resources								
Please sei	lect a resource and click t	he start button.						Report +
A Filter	ctory 🥑 File System	SharaPoint 👩 1	Vith 8MAN 🛛 🖉 Without 87		O Warnings only			
Time	Element		Change Action		New value		Old va	lue
ady						8man-demo.loca	I 👻 🚯 🛛 😺 <latest scan<="" td=""><td>» * O 🛛 🛧</td></latest>	» * O 🛛 🛧

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

46 | Access Rights Management



Select the date and time of both scans.

	<u> </u>	Search						
can comparision	Compare <latest scan="" t<="" td=""><td>time></td><td>1 /2016 2:06 PM 💿</td><td>×</td><td></td><td>🗐 Resources 🌘</td><td>) 🎝 Organiza</td><td>tional categ</td></latest>	time>	1 /2016 2:06 PM 💿	×		🗐 Resources 🌘) 🎝 Organiza	tional categ
Resources	Currently used scans							
Please select a resource and clic Filter	All currently used scans po resource.	er resource are li	sted in the table b	elow. In addition, scan	errors (if any) are li	sted under ea	ach scanned	Repo
Active Directory SFile System	A Filter						6	-
	Active Directory (1)							-
me Element		0/31/2015 1:16:29 PM	2					
	E File server (1)	0/23/2015 4:44:16 PM	-					
	B SharePoint (1)	012012013 414110114						
	SRV-8MAN 8/	/16/2015 2:00:04 AM						
							Close	I
							Close	I

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.

Start & Resources Permissions & Accounts @ Dashboard 🗹 Multiselection 🅮 Logbook 👁 Scan comparision 🔘				Search			٥		🚔 cradı
Compare <latest scan="" time=""> () with 1/1/2016 2.06 PM () × Resources Image: Compare <latest scan="" time=""> () with 1/1/2016 2.06 PM () × Resources Image: Compare Image: Compare <th></th><th></th><th></th><th>• pearch</th><th></th><th></th><th>*</th><th></th><th></th></latest></latest>				• pearch			*		
Resources								Scan comparision	
Resources									
Sector resource and dick the start buttoon Sector resource (s)	an co	mparision	Compare <u><latest< u=""></latest<></u>	scan time> () with	<u>1/1/2016 2:06 PM</u> ()	×		🗿 Resources 🔵 🔄 🖨 Organiza	ional categ
Resources and chick the state buttown Resources Image: Chick the state of	Resources								
Resources									0
Resources Writes BMAN © Underst Changes O Wornings Only 2 Active Directory Change Action New value Old value 3 Brain denotad Directory Old model Old value 3 File server Signar denotad New value Old value									керо
Achine Interiory Okange Action New value Old value File genorer Spane Point Spane Action New value Old value	ease select i			8MAN 🥏 Without 8M	MAN O Indirect changes	O Warnings only			
SharePoint 2	Active Dir			Change Action		New value		Old valu	
SharePoint			2						
	Janareroin	n							
Britan dana kari u 🗛 🔍 🖉 🖓 dana ana ang									
							Sman-dame lac		v

- 8MAN Search ۵ o s Compare <latest scan time> ① with 1/1/2016 2:06 PM ① × 🎒 Res Scan comparision :es 💽 🛔 (Resources (Hide details) Cres **∀**G mberships 🗹 Account changes × With 8MAN Ø Without 8MAN O Indirect changes O War Ne Old val ⊡Act E File server ocal 🕤 这 📑 🥝 < Lat
- Select the range of the comparison.
- 2. Start the comparison.

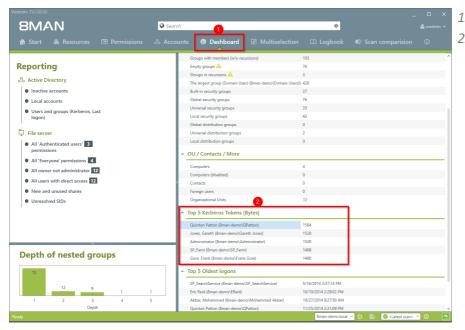
BM/			Search			-		å cradm
	& Resource						Scan comparision	
can co	omparision	Compare <u><lat< u=""></lat<></u>	est scan time> () with	<u>1/1/2016 2:06 PM</u> ()	×		🗿 Resources 🔵 🔄 👌 Organizati	onal catego
	s (« Hide details)							
	local, <u><add></add></u>							
			Group memberships 🗹	-				
Scan co	omparison finished succe	essfully. There are 42 difference	ces between the selected scans	0				2 Report
Filter	0.5				0		differences on file server	
Active Di	rectory O File System	m 🔾 SharePoint 🥑	With 8MAN 🥑 Without 8	AN () Indirect changes	O Warnings only		anges through changed group membersi	hip relation:
Time	A	Element		nge Action		Export list to XLS for Export the generated	ormat scan compare list into Excel XLS format.	
	Clean - ReadG ReadGroup8)	roup8 (8man-demo\Clean -	💠 Created					
		n (8man-demo\Clean - Admin						
	윤 Clean - Overa Overall)	II (8man-demo\Clean -	🖶 Created					
	ReadGroup10							
	(e) Clean - Read ReadGroup3)	Froup3 (8man-demo\Clean -	💠 Created					
	② bd8f944a-d2	6e-40be-9fbf-22b6c417a6ae	💠 Created					
		8man-demo\Clean - User)	💠 Created					
	Clean - Read ReadGroup4)	6roup4 (8man-demo\Clean -	🖶 Created					
	ReadGroup5)	iroup5 (8man-demo\Clean -	Created					
	@ Clean - ReadG ReadGroup2)	iroup2 (8man-demo\Clean -	💠 Created					
	@ Clean - ReadG ReadGroup6)	Froup6 (8man-demo\Clean -	💠 Created					
	ReadGroup7)	6roup7 (8man-demo\Clean -						
	Paradel Par	an-demo\neadmin)	Added to group Domain Admins (8man-dem	o\Domain Admins)				
9/2017 3:38	3:23 PM& Marketing (8n	nan-demo\Marketing)	Changed display name	o (Pornani riallillib)	Marketing		Marketing 2	
9/2017 3:38	8:23 PMas Marketing (8n	nan-demo\Marketing)	S Changed Common Name		Marketing		Marketing 2	
_								

- 1. Use filters to focus on specific actions.
- 2. Generate a structured "Permission Differences Report" and / or export the results to .XLS.

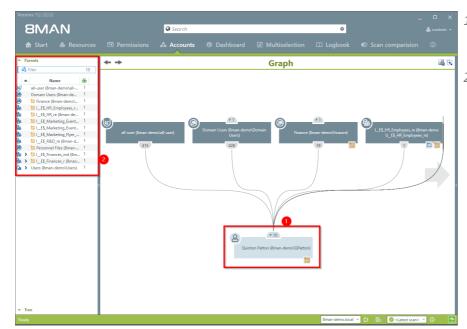
4.1.1.3 Indentify overpriviledged users (based on Keroberos token size)

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.



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



- 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

8MAN	Search	\$	
🍙 Start & Resources 🖃 Permissi	ons 🖧 Accounts 🞯 Dashboard 🗹 !		
Reporting	 Users and other accounts 		
	Users	429	
Active Directory	Users (Disabled)	6	
Inactive accounts	Administrators	12	
Local accounts	Administrators (Disabled)	0	
 Users and groups (Kerberos, Last logon) 	 Groups 		
103017	All Groups	182	
File server	Groups with members (w/o recursions)	103	
All 'Authenticated users' 3	Empty groups 🛕	76	
permissions	Groups in recursions 🛕	3	
All 'Everyone' permissions	The largest group (Domain Users (8man-		
All owner not administrator 12	Built-in security groups	27	
All users with direct access 12	Global security groups	76 35	
_	Universal security groups Local security groups	35	
New and unused shares	Global distribution groups	**	
Unresolved SIDs	Universal distribution groups	2	
	Local distribution groups	0	
	 OU / Contacts / More 		
2	Computers	4	
Depth of nested groups	Computers (disabled)	0	
-	Contacts	0	
70	Foreign users	0	
12 9	Organizational Units	12	
1 2 3 4	Top 5 Kerberos Tokens [Bytes]		
Depth	Quinton Patton (8man-demo\QPatton)	1584	
		8man-demo.local 👻 🔅 📑 🥝 <latest s<="" td=""><td>can> 🖌 🕕</td></latest>	can> 🖌 🕕

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



8MAN	Search	 	\$	
		☑ Multiselection	n 🕮 Logbook 🛛 Scan comparision	
ultiselection	2	8	Operations\ (8man-demo\Operations)	
groups with depth of nesting [Depth 5]		Deactivate scenario		Repo
Filter		1 *	Children	
Users Groups O Contacts O Computers		^	Tree	
			Name	
Name	*	6	A 10 Operations\ (8man-demo\Operations)	
Operations\ (8man-demo\Operations)			⊕ 🏶 Facilities∖ (8man-demo\Facilities)	
			🐣 Mark Aroni (8man-demo\Mark Aroni)	
			& Walter Beiter (8man-demo\Walter Beiter)	
			··· 🐣 💹 Jean-Claude Martin (8man-demo\JMartin)	
			···· 🐣 Peer Sie (8man-demo\Peer Sie)	
			면 쯔 📁 Purchasing (8man-demo\Purchasing)	
			Pott, Jack (8man-demo\Jack Pott)	
			😕 😈 Johnson, Jason (8man-demo\Jason Johnson) 	
			SAP (sman-demo\SAP) SAP (sman-demo\Administrator)	
		3	- Administrator (aman-demo(Administrator)	
			& 10 Chris Cook (8man-demo\CCook)	
			🐣 🗾 Davidson, Charlie (8man-demo\Charlie Davi	
			🔒 🔯 Gore, Frank (8man-demo\Frank Gore)	
			🐣 📁 Jimmy Ward (8man-demo\JWard)	
			🐣 🔟 Joe Hunter (8man-demo\JHunter)	
			🐣 📁 John Thompson (8man-demo\JThompson)	
			🐣 🔯 Johnson, Jason (8man-demo\Jason Johnson)	
			🐣 💯 Michael Crabtree (8man-demo\MCrabtree)	
			🕀 🎒 Support (8man-demo\Support)	
			🐣 💯 Baum, Adam (8man-demo\Adam Baum)	
			um 2 van Meulendijk, Jan (8man-demo\Jan van Meulendijk)	
			19 Sechnical Group (8man-demo\Technical Group)	
			Ali Bye (8man-demo\Ali Bieh) John paul (8man-demo\Jpaul)	
			🐨 🐨 jonn paul (oman-demo'Upaul)	
		•	Attributes	

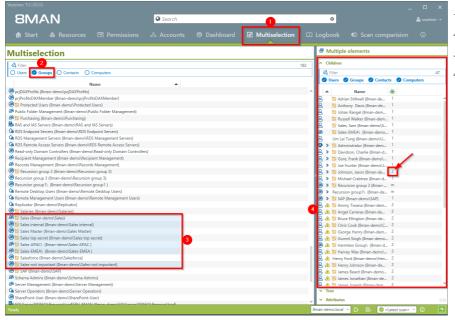
- 1. 8MAN automatically shows the Multiselection
- 1. In this scenario 8MAN automatically filters the groups by the selected nested level.
- 2. You can see the nested levels in the tree graph on the right hand side.

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



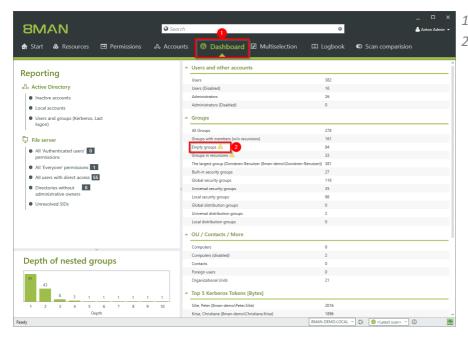
- 1. Select Multiselection.
- 2. Filter by groups.
- *3. Select the desired groups.*
- 4. You can see an overview of all "children" of all selected groups. 8MAN also indicates if any users are included in multiple groups, for example Jason Johnson.

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.





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

54 | Access Rights Management

8MAN	Search		۵			
		☑ Multiselection	🕮 Logbook			
Multiselection	2		✓ Attributes			E
Empty groups		Deactivate so	enario			
🕰 Filter			76			
O Users 🕑 Groups O Contacts O Computers						
Name						
Access Control Assistance Operators (8man-demo\Access Control Assista	nce Operators)		^			
Account Operators (8man-demo\Account Operators)						
Agco Corp Global Group 1 (8man-demo\Agco Corp Global Group 1)						
8 10 Agco Universal Group 1 (8man-demo\Agco Universal Group 1)						
Allowed RODC Password Replication Group (8man-demo\Allowed RODC	Password Replicati					
la Backup Operators (8man-demo\Backup Operators)						
Ø Clean - Marketing (8man-demo\Clean - Marketing)						
Cloneable Domain Controllers (8man-demo\Cloneable Domain Controlle	rs)					
Cryptographic Operators (8man-demo\Cryptographic Operators)						
Selegated Setup (8man-demo\Delegated Setup)						
Biscovery Management (8man-demo\Discovery Management)						
Distributed COM Users (8man-demo\Distributed COM Users)			>			
DL-VMWare-AppOwner-AD (8man-demo\DL-VMWare-AppOwner-AD)						
DL-VMWare-AppOwner-AV (8man-demo\DL-VMWare-AppOwner-AV)						
DL-VMWare-AppOwner-Blackberry (8man-demo\DL-VMWare-AppOwne						
DL-VMWare-AppOwner-Exchange (8man-demo\DL-VMWare-AppOwner						
DL-VMWare-AppOwner-Fileserver (8man-demo\DL-VMWare-AppOwner						
DL-VMWare-AppOwner-Lexware (8man-demo\DL-VMWare-AppOwner-I						
DL-VMWare-AppOwner-Lync (8man-demo\DL-VMWare-AppOwner-Lync)						
DL-VMWare-AppOwner-Mailarchive (8man-demo\DL-VMWare-AppOwn						
DL-VMWare-AppOwner-SQL (8man-demo\DL-VMWare-AppOwner-SQL) DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppOv						
DL-VMWare-AppOwner-SystemCenter (aman-demo\DL-VMWare-AppO DL-VMWare-AppOwner-TerminalServer (8man-demo\DL-VMWare-AppO DL-VMWare-AppOwner-TerminalServer (8man-demo\DL-VMWare-AppO DL-VMWare-AppOwner-SystemCenter (aman-demo\DL-VMWare-AppO DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppO DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppO DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppO DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppO DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppO DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppO DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppO DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppO DL-VMWare-AppO (8man-demo) DL-VMWare-AppO (8man						
DL-VMWare-AppOwner-TerminalServer (8man-demo\DL-VMWare-AppC DL-VMWare-AppOwner-View (8man-demo\DL-VMWare-AppOwner-View			- 1			
DL-VMWare-AppOwner-View (8man-demo\DL-VMWare-AppOwner-View BL-VMWare-AppOwner-Watchquard (8man-demo\DL-VMWare-AppOwner-View)			- 1			
DL-VMWare-AppOwner-Watchguard (aman-demo\DL-VMWare-AppOwn DL-VMWare-Network-Admin (8man-demo\DL-VMWare-Network-Admin			- 1			
DL-VMWare-VMAdmins-Productive (8man-demo\DL-VMWare-VMAdmin DL-VMWare-VMAdmins-Productive (8man-demo\DL-VMWare-VMAdmin			- 1			
DisAdmins (8man-demo\DisAdmins)	a manufacture]					
DnsUpdateProxy (8man-demo\DnsUpdateProxy)						
Documentation (8man-demo\Documentation)						
Empty Group 10\ (8man-demo\Empty Group 10)						
Ready			8man-demo.local	 O E O <latest scan=""></latest> 	~ O	-

- 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.

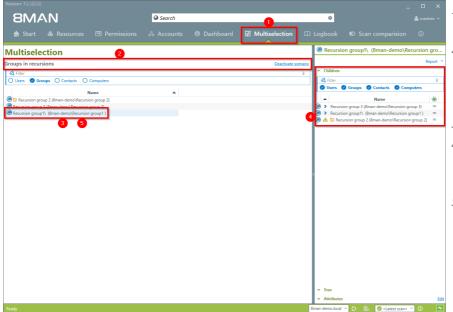
Additional Services

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 <u>nested group levels</u>. <u>Identify groups in recursion</u> (web client)

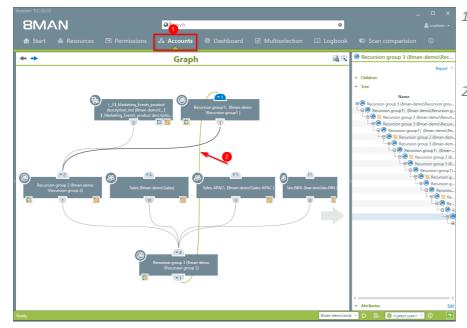
8MAN	@ Search	\$	
	& Accounts @ Dashboard 🗹		
	 Users and other accounts 		^
Reporting	Users	429	
Active Directory	Users (Disabled)	6	
Inactive accounts	Administrators	12	
Local accounts	Administrators (Disabled)	0	
 Users and groups (Kerberos, Last logon) 	 Groups 		
logoly	All Groups	182	
📮 File server	Groups with members (w/o recursions)	103	
All 'Authenticated users' 3	Empty groups	2 76	
permissions	Groups in recursions 🛕	3	
All 'Everyone' permissions	The largest group (Domain Users (8ma		
All owner not administrator 12	Built-in security groups	27 76	
All users with direct access	Global security groups Universal security groups	35	
New and unused shares	Local security groups	42	
Unresolved SIDs	Global distribution groups	0	
Unresolved SIDs	Universal distribution groups	2	
	Local distribution groups	0	
	 OU / Contacts / More 		
	Computers	4	
	Computers (disabled)	0	
Depth of nested groups	Contacts	0	
	Foreign users	0	
70	Organizational Units	12	
12 9 2	 Top 5 Kerberos Tokens [Bytes]	
1 2 3 4	5 Quinton Patton (8man-demo\QPatton	1584	
Depth	Jones, Gareth (8man-demo\Gareth Jon	· · · · · · · · · · · · · · · · · · ·	~
		8man-demo.local	💌 🚯 😸 🖉 < Latest scan> 👻 🕕 🌁

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

56 Access Rights Management



- 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: Administrate 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 <u>nested group levels</u>.

Idenitfy recursive groups (rich client)

Break the circle by <u>managing group memberships</u> (rich client) or <u>removing group memberships</u> (web client).

B BMAN Web x ← → C B Scher https://sv-8man.8man-demo.local/#/dashboard/my-employees	Ý	Go to the Risk Assessment
SMAN A Codat O Recertification · Lit: Analyze · W Requests · % Workflows ·	🌣 🗸 🖉 Anton Admin -	Dashboard.
Requests Warning for Approval <	If Administrator	

B 8MAN Web x ← → C B Sicher https://srv-8m	an Grans-demo local/V/dashboard/trak-dashboard	± - □ X ☆ :
	t 🗘 Recertification + 🔟 Analyze + 🦞 Requests + 🖏 Workflows +	🌣 🗸 👷 Anton Admin -
	Risk Assessment Dashboard	
	High Risk High Risk High Risk 1000	
	100 Accounts where password never expires 369 of 582 accounts 100 Brand-deno local More + Meininze Risks	
	100 Directories with unresolved SDr. 2 of 66 directories vary draw 99 Non-compliant user accounts 377 of 352 accounts Brain demo local 15 Groups in recursion Wary draw More - Minimize Risks More - Minimize Risks More - Minimize Risks	

- 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.

В	MA	N ♠ Home ↔ Recertification → 🔟 Analyze → 🗎 F	Requesting + 🖏 Workflows +	🗢 🗸 🐣 demoadm
G	roups	s in recursion (33)	Configuration Configuration Configuration Configuration Configuration: 8man-demo.local	A Direct Excel export
Dor	nain name	e x	Type, Name 💌 C	E C 5 Create Report
	Туре	Name	▼ Requested Action ▼	 Available Actions
P	i Domain r	name:8man-demo.local(33 items)		Execute script
0	0	GutGetarnteGruppe (8man-demo\GutGetarnteGruppe)		
	۲	HarmloseGruppe (8man-demo\HarmloseGruppe)		
1	۲	NochBessergetarnteGruppe (8man-demo\NochBessergetarnteGruppe)		
	۲	Recursivgruppe 1 Ring 1 (8man-demo\Recursivgruppe 1 Ring 1)		
9	۲	Recursivgruppe 1 Ring 2 (8man-demo\Recursivgruppe 1 Ring 2)		
3	۲	Recursivgruppe 10 Ring 1 (8man-demo\Recursivgruppe 10 Ring 1)		
	۲	Recursivgruppe 10 Ring 2 (8man-demo\Recursivgruppe 10 Ring 2)		
	۲	Recursivgruppe 10 Ring 3 (8man-demo\Recursivgruppe 10 Ring 3)		
9	0	Recursivgruppe 2 Ring 1 (8man-demo\Recursivgruppe 2 Ring 1)		
	۲	Recursivgruppe 2 Ring 2 (8man-demo\Recursivgruppe 2 Ring 2)		
	۲	Recursivgruppe 2 Ring 3 (8man-demo\Recursivgruppe 2 Ring 3)		
	۲	Recursivgruppe 3 Ring 1 (8man-demo\Recursivgruppe 3 Ring 1)		
	۲	Recursivgruppe 3 Ring 3 (8man-demo\Recursivgruppe 3 Ring 3)		
9	۲	Recursivgruppe 4 Ring 1 (8man-demo\Recursivgruppe 4 Ring 1)		
)	۲	Recursivgruppe 3 Ring 2 (8man-demo\Recursivgruppe 3 Ring 2)		
0	۲	Recursivgruppe 4 Ring 2 (8man-demo\Recursivgruppe 4 Ring 2)		
	۲	Recursivgruppe 4 Ring 3 (8man-demo\Recursivgruppe 4 Ring 3)		
	۲	Recursivgruppe 5 Ring 1 (8man-demo\Recursivgruppe 5 Ring 1)		

- 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

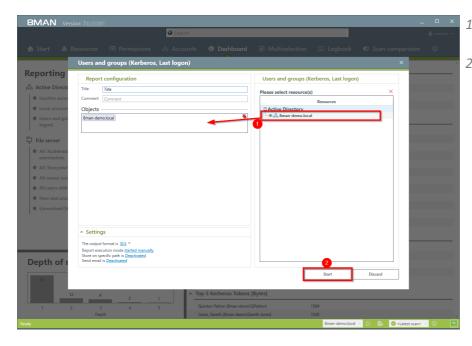
One key security requirement within any organization is that passwords are changed regularly. 8MAN scans your domain for user accounts where this requirement has not been activated. You can view this information in our reports for "Users" an "Groups".

Additional Services

Reset passwords Change password options Identify users with never expiring password (web client) Change password options in bulk (web client)

8MAN	Search	_ C X
	Accounts Obshboard Multiselection II Log	
Reporting	 Users and other accounts 	
	Users 429	
A Active Directory	Users (Disabled) 6	
Inactive accounts	Administrators 12	
Local accounts	Administrators (Disabled) 0	
Users and groups (Kerberos, Last logon)	 Groups 	
	All Groups 182	
File server	Groups with members (w/o recursions) 103	
All 'Authenticated users'	Empty groups 🗛 76	
permissions	Groups in recursions 🛕 3	
All 'Everyone' permissions	The largest group (Domain Users (8man-demo\Domain Users)) 428	
All owner not administrator	Built-in security groups 27	
All users with direct access 12	Global security groups 76	
	 Universal security groups 35 	
New and unused shares	Local security groups 42	
Unresolved SIDs	Global distribution groups 0	
	Universal distribution groups 2 Local distribution groups 0	
	Local distribution groups 0	
	OU / Contacts / More	
~	Computers 4	
Double of constant succession	Computers (disabled) 0	
Depth of nested groups	Contacts 0	
	Foreign users 0	
70	Organizational Units 12	
12 9 2	 Top 5 Kerberos Tokens [Bytes] 	
1 2 3 4	Quinton Patton (8man-demo\QPatton) 1584	
Depth	Jones, Gareth (8man-demo\Gareth Jones) 1528	
ty	8man-	demo.local - 🚯 📑 🥥 < Latest scan> - 🕕

- 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.

4	A	B	С	D	E	F	G	H
	Report über alle Benutzer für	8man-demo.local		2	_			
	DisplayName	IsDisabled 🔻	Account Expires	PWD don't exp -T	ast Logon 🛛 👻	Last Logon Timestan *	Type 💌	Direct Members
	Aber, Mark (8man-demo\Mark Aber)	Nein	Account never expires		N/A	N/A	Benutzer	
	ADLogga Tester (8man-demo\ATester)	Nein	Account never expires	Ja	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	
i	Ander, Cori (8man-demo\Cori 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	
5	Ann Essay (8man-demo\Ann Essay)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
6	Anna Lyse (8man-demo\Anna Lyse)	Nein	Account never expires	Ja	N/A	07.03.2016 17:44:11	Benutzer	
7	Anna Ziese (8man-demo\Anna Giese)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
3	Ansgar Agentor (8man-demo\AAgentor)	Nein	Account never expires	Ja	N/A	07.03.2016 17:38:41	Benutzer	
9	Apfel, Adam (8man-demo\Adam Apfel)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
0	Arbeit, Andi (8man-demo\Andi Arbeit)	Nein	Account never expires	Ja	12.03.2015 10:44:56	10.03.2015 16:51:26	Benutzer	
1	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	
3	Asil, Claire (8man-demo\Claire Asil)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
4	Auer, Karl (8man-demo\Karl Auer)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
5	Auhss, Ann (8man-demo\Ann Auhss)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
6	Autsch, Anke (8man-demo\Anke Autsch)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
7	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		N/A	N/A	Benutzer	
0	Baer, Johannes (8man-demo\Johannes Baer)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
1	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		N/A	N/A	Benutzer	
	Balken, Don R. (8man-demo\Don R. Balken)	Nein	Account never expires		N/A	N/A	Benutzer	
	Becher, Joe Kurt (8man-demo\Joe Kurt Becher)	Nein	Account never expires		N/A	N/A	Benutzer	
	Beiter, Walter (8man-demo\Walter Beiter)	Nein	Account never expires		N/A	N/A	Benutzer	
	Bert, Carmen (8man-demo\Carmen Bert)	Nein	Account never expires		N/A	N/A	Benutzer	
	Dasaardiah Damhard /Oman d		Account neuror ouniron		MI/A	MI/A	Denutrar	

- Open the report in Excel.
- 1. Select the tab "User".
- 2. Filter the column "PWD don't expire" by positive entries.

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



4.1.1.10 Identify users with never expiring password (web client)

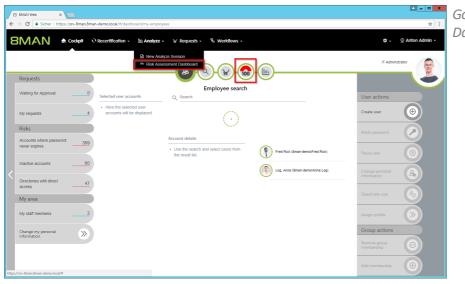
Background / Value

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.

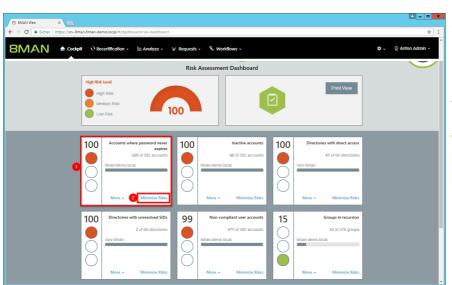
Additional Services

<u>Reset passwords</u> (rich client) <u>Change password options</u> (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.

`		https://srv-8man.8man-demo.local/#/analyze-details:id=1:scenar	ef53edb73-380a-47ac-83dd-2da23913d8e3	\$
8	MA	N 🖨 Home 🔍 Recertification - 🔟 Analyz	- 、 户 Requesting - 🔏 Workflows -	🌣 🗸 🐣 demoadmin 🕤
<u>.</u>	scoup	ts where password never expire	Configuration 🌣	Reports
	42)	is where password never expire	Accounts where password never expires, ornan-demo.local	Direct Excel export
-	<u>,</u>			5 Create Report
01	main name	x	2 Type, Name 🗸 C 📰	E C Available Actions
	Туре	Name y Requested	action v	Execute script
	4 Domain na	ame:8man-demo.local(342 items) Clean - Admin (8man-demo\Clean - Admin)		Reset password
	8	sa-8mansvc (8man-demo\sa-8mansvc)		
	•	sa-ExcViewer (8man-demo\sa-ExcViewer)		
	8	sa-HQ-vRanger (8man-demo\sa-HQ-vRanger)		
	8	sa-SP CacheADM (8man-demo\sa-SP CacheADM		
	8	sa-SP_Crawl (8man-demo\sa-SP_Crawl)		
	\$	sa-SP_Farm (8man-demo\sa-SP_Farm)		
	•	sa-SP_Install (8man-demo\sa-SP_Install)		
	8	sa-SP_MySite (8man-demo\sa-SP_MySite)		
	8	sa-SP_Pool_Intranet (8man-demo\sa-SP_Pool_Int		
	8	sa-SP_Pool_Portal (8man-demo\sa-SP_Pool_Porta		
	8	sa-SP_Profile (8man-demo\sa-SP_Profile)		
	8	sa-SP_Search (8man-demo\sa-SP_Search)		
	8	sa-sql (8man-demo\sa-sql)		
	8	sa-SP_Services (8man-demo\sa-SP_Services)		
	•	demoadmin (8man-demo\demoadmin)		
	8	Bill Anz (8man-demo\Bill Anz)		
	•	cradmin (8man-demo\cradmin)		

- 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

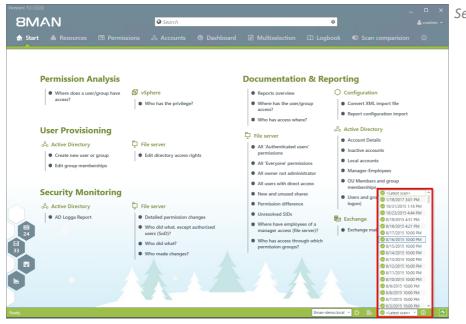
Background / Value

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

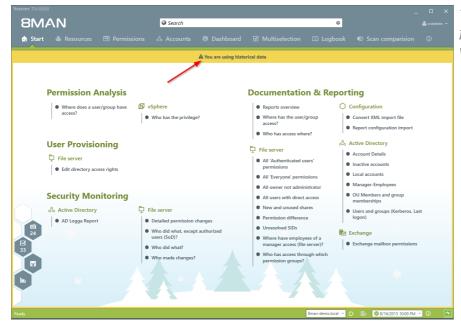
Alternatively you could also <u>compare two scans from different points in time</u>.

Step by step process



Select the desired scan date.

64 | Access Rights Management



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.

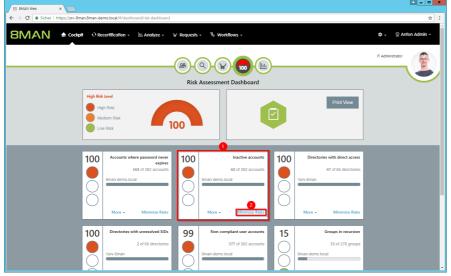
Additional Services

<u>Report: inactive accounts</u> <u>Deactivate accounts in bulk</u> (web client)

Step by step process

BMAN & cockpit	े Recertification - 🔟 Analyza	e + ₩ Requests + 🧐 Workflows +		\$ -	👳 Anton Admin 👻
		nalyze Session ssessment Dashboard		IT Adminst	rator
Requests					
Waiting for Approval0	Selected user accounts	Employee search		User actions	
My requests4	Here the selected user accounts will be displayed.	\odot		Create user	•
Risks				Reset password	\triangleright
Accounts where password369		Account details Use the search and select users from the result list.	Fred Rick (8man-demol/Fred.Rick)	Pause user	
Inactive accounts60			Log, Anna (8man-demolAnna Log)	- Change personal information	
Directories with direct 47 access 47 My area				Deactivate user	8
My staff members2				Assign profile	
Change my personal				Group actions	
	7				Θ
				Add membership	(\bullet)

o 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.

	MA	N 🖨 Home 🕂 Recertification -	🔟 Analyze 🗸	🛛 Requesting 🗸	🗞 Workflows 🗸			🌣 🗸 🐣 demoadmin 🗸
) In	active	accounts (56)		Configuration	🔅	•		A Direct Excel export
Don	nain name	x			5 columns selected	3 ▼ C I II	e c	5 Create Report
	Туре	Name	▼ Last logon	T Days since last logo	on 🕆 Is activated	T Requested Action	Y	Available Actions
1	i Domain ni	ame:8man-demo.local(56 items)						Execute script
1								
9	8	Azubi, Andy (8man-demo\Andy Azubi)	3/7/2016	436	true			
3	8	Pakdikoffa, Anna (8man-demo\Anna Pakdikoffa)	3/7/2016	436	true			
]	8	Moe Zarella (8man-demo\Moe Zarella)	3/7/2016	436	true			
	8	Kai Serslauten (8man-demo\Kai Serslauten)	3/7/2016	436	true			
	8	Sue Permarkt (8man-demo\Sue Permarkt)	3/7/2016	436	true			Deactivate Account
	•	Minni Ralwasser (8man-demo\Minni Ralwasser)	3/7/2016	436	true			
3	8	Erkan Alles (8man-demo\Erkan Alles)	3/7/2016	436	true			
	8	Bill Anz (8man-demo\Bill Anz)	3/7/2016	436	true			
	8	Tom Ate (8man-demo\Tom Ate)	3/7/2016	436	true			
	8	Mel Odie (8man-demo/Mel Odie)	3/7/2016	436	true			
3	8	Karl Kulation (8man-demo\Karl Kulation)	3/7/2016	436	true			
	8	Gitta Rensolo (8man-demo\Gitta Rensolo)	3/7/2016	436	true			
	8	Ansgar Agentor (8man-demo\AAgentor)	3/7/2016	436	true			
	8	Hacke, Petra (8man-demo\Petra.Hacke)	3/7/2016	436	true			
0	•	Krise, Christiane (8man-demo\Christiane.Krise)	3/7/2016	436	true			
	8	Silie, Peter (8man-demo\Peter.Silie)	3/7/2016	436	true			
	8	Rosi Ne (8man-demo\Rosi Ne)	3/7/2016	436	true			
	8	Anna Lyse (8man-demo\Anna Lyse)	3/7/2016	436	true		_	

- 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.

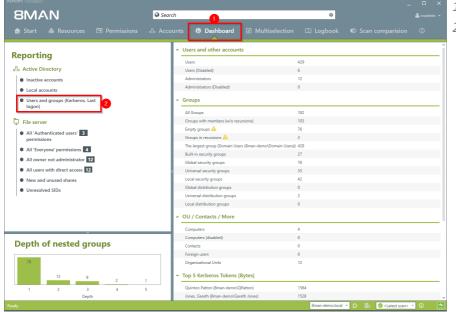


4.1.1.13 Identify temporary user accounts

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".

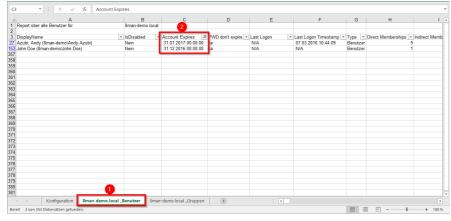
Step by step process



- 1. Select the "Dashboard".
- Click on "Users" and "Groups" in the "Reports" area.

	ion: 7.	Q Search				👗 cradmin
	Users and groups (Kerberos,	Last logon)			×	
orting	Report configuration		Users and groups (Ke	erberos, Last logon)	
tive Directo	Title Title		Please select resource(s)		×	
active accou	Comment Comment			Resources		
ocal account	Objects		E Active Directory			
Jsers and gro	8man-demo.local	*		1		
ogon)			•			
e server						
ul 'Authentic						
all'Authentic permissions						
II 'Everyone'						
ll owner not						
l users with						
w and unu						
resolved Si						
	 Settings 					
	The output format is XLS Y					
	Report execution mode started manually Store on specific path is Deactivated					
th of r	Send email is Deactivated					
				Start	Discard	
				Start	Discard	
			(D + 1		_	
12	9 2 1	 Top 5 Kerberos Tokens 				
2		Quinton Patton (8man-demo)		1584		
		Jones, Gareth (8man-demo\G				

 Select the range of the report via drag & drop.
 Run the report.



Open the report in Excel.

1. Select the tab "User".

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

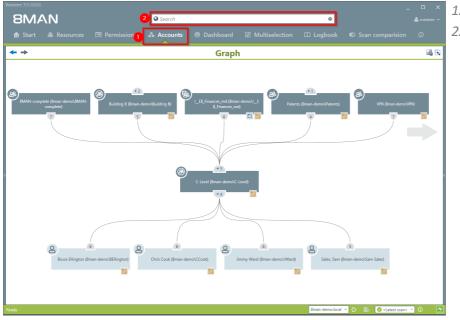


4.1.1.14 Identify the most recent actions on an account

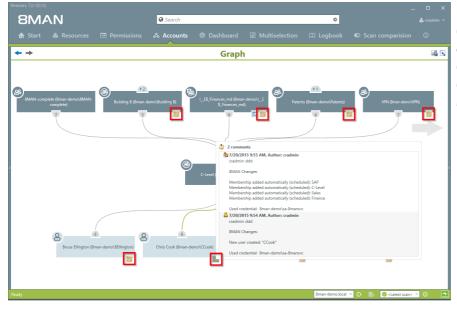
Background / Value

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



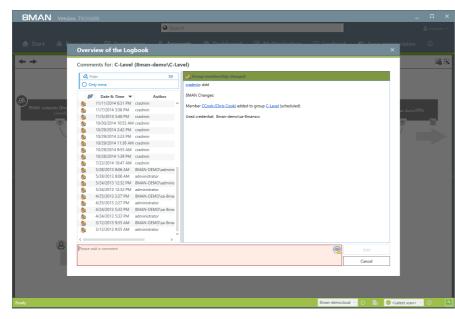
- 1. Select "Accounts".
- 2. Search for the desired user or group.



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.



8MAN

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.

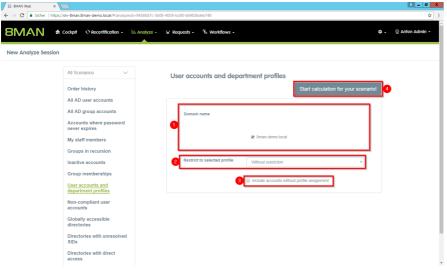
To be able to use the compliance functions, you must have created at least one department profile.

Additional Services

<u>Create a new department profile (Administrator)</u> <u>Assign a department profile to users</u>

/1	B 8MAN Web ×					- 0 ×	1
÷	→ C Sicher https://srv-8man.8man-demo.local/#/	'dashboard/analyze-list				☆ :	1.
8		n - 🔟 Analyze - 🖌 Requests -	% Work	dlows -		🗘 🗸 👳 👳 Anton Admin 👻	2.
	Requests				2	IT Administrator	3
	Waiting for Approval0	Analysis scenarios	ysis and	recertif	ication	Recertification	Э.
	My requests4	Select a scenario. Hover with your mouse over a scenario to s	iee a descrip	tion.		Recettification	
	Risks					Statistics	
	Non-compliant user	Order history	0	⊙	All AD user accounts		
	Accounts where password 369 never expires	All AD group accounts	\odot	\odot	Accounts where password never expires		
	Inactive accounts60	My staff members	⊝	€	Groups in recursion		
	My area	Inactive accounts	\odot	\odot	Group memberships		
	My staff members2	User accounts and department profiles	0	O	Non-compliant user accounts		
	Change my personal S	Globally accessible directories	\odot	\odot	Directories with unresolved SIDs		
		Directories with direct access	\odot	⊕	Directories with changed access rights		
		File system permissions	⊝				

- 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.

SMAN Cockpt	_	yze - `₩ Requests - ® Woi				
	n premes (e)	Configuration	•		Reports	
		Selected resource	es: 8man-demo.local		Direct Excel export	
ofile ×	0	2	5 columns selected	- C I E C 3	Create Report	
Type Name	Non-compliant	Accepted deviations	Y	Unaccepted deviations	Execute script	
a Profile: Sales(2 items)					Reset password	
A Sam Sales (8man-demo	Sam.Sales) false					
Ellos, Mark (8man-demo	Mark Ellos) true			The group membership 'Vertrieb (8man-demo\Sale		
Profile:Marketing(3 items)					Pause user	
Erkan Alles (8man-demo	· · · · ·				Change password options	
Pepe Roni (8man-demo)	1 / / / / / / / / / / / / / / / / / / /				Change personal information	
Pott, Jack (8man-demoly	lack Pott) false				Deactivate user	
Profile:HelpDesk(1 items)	and West					
8 Tor, Moni (8man-demo\).	foni Tor) false	The property 'Department' has the w	rong value " instead of Helpu		Remove group membership	
					Add membership	
					Remove department profile	
					Assign profile	

- 1. 8MAN shows you which user accounts are non-compliant.
- 2. User accounts are compliant when exceptions have been accepted by a controller.
- User accounts are noncompliant 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

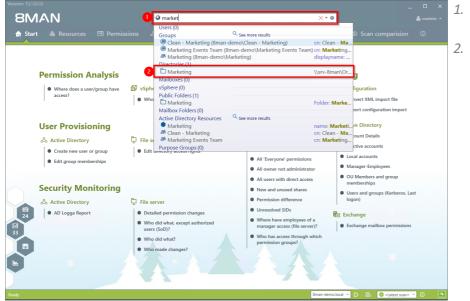
8MAN quickly shows you all access rights on file server directories. Initially you should focus on the directories containing the most sensitive data. You siomply need to know: Who has access?

Additional Services

Report: Who has access to what? Modify folder permissions Monitor access to sensitive data

Step by step process

8MAN



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

8MAN ₁		Search			\$			
🚖 Start 💩 Resou	rces 🖃 Permissions							
Resources			\$	Marketing				Report
\land Resources filter first level			1	Owner BullTINVAdministrators Char	nge owner			
	full path	Description	Access rights	Inheritance 🔒 On Char	nge inheritance			
Active Directory				 Access rights 	3			
File server				AA 🔵 DA				
😳 🗐 srv-8man	\\srv-8man							
🕀 🛃 Organization	E:\Data\Organization			e 5	Modify Restricted Read and Ex	Write Read List directory Special per	5	
→ I III III Finances				NTFS Inheritance	Modify Restricted Read and Ex	Write Read List directory Special per	Propagation	Descripti
🔶 🗁 🖽 🚱 🛅 HR 👝					Modify Restrictes Read and	Write Read List dir Special	bed	bescripti
i-eo fin				1 문	Re: Re:	Sp. Lis Rei	- ¥	
Harketing				All permissions				
▶ •••• 🙂 🛄 R&D				🗄 Full control 🛛 🔒 🧹	~~~	11	000	
🗄 🖽 🕒 🛅 Sales				🕀 Modify 🔒 🔒	~~~	11	000	
▶ … 🕀 🛃 Projects	E:\Data\Projects			⊞ Read and Execute 🛛 🔒 🔒	~	~	000	
Templates	E:\Data\Templates			Special permission 🛛 🔒 🔒				
🛃 Users	E:\Data\Users							
SharePoint								
8 Exchange				2				_
B vSphere				Accounts with permissions All perm	issions			
Purpose Groups								
				A Filter				33
				🔮 Users 🔮 Groups 🥥 Contacts 🔮	Computers			
				Name	 how often gran 	ited Inheritance		
				ammy Tiwana (8man-demo\ATiwana)	1	A		
				Andrew Susac (8man-demo\ASusac)	1	8		
				angel Carreras (8man-demo\ACarreras)	1	a		
				BUILTIN\Administrators	2 🕰	1x 🔒 1x 🔒		
				BUILTIN\Users	2 🕰	2x 🔒		
				CREATOR OWNER	1			
				aurmit Singh (8man-demo\GSingh)	1	a		
				8 Henry Johnson (8man-demo\HJohnson)) 1	a		
				8 Wermann Schmidt (8man-demo\HSchmi	idt) 1	a		
				8 James Baker (8man-demo\JBaker)	1	a		
	^		,	A lames Reard (Sman, demo) (Reard)	1	A		
					8man-demo.local	- 0 B	Catest scan>	• 0

- 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.

8MAN		Search						٥				
📥 Start 💩 Resou												
Resources			۵	Marketing								Report
Resources filter first level			1	Visro-8man\Organization\Marko Owner B BUILTIN\Administ Inheritance On	rators	Change Change		nce				
Active Directory	full path	Description	Access rights	 Access rights 								
Active Directory File server												
□ File server	\\srv-8man											
G Grganization	E:\Data\Organization									~		
→ ····⊞	E: Data Organization			NTFS	Inheritance	Full control Modify	Restricted	Read and Ex	Write Read	List directory	Special per Propagation	Descriptio
→ ···· 🕀 🕒 🛅 Marketing				All permissions								
→				E Full control	a	~ ~	11	.7	10		000	
					8.8		13	2			000	
→ ···· E	E:\Data\Projects			Read and Execute	8.0			2			000	
Templates	E:\Data\Templates			B Special permission	88							
Users	E:\Data\Users											
SharePoint												
Exchange				< 2								
vSphere				Accounts with permissions	Mod	ify						
Purpose Groups						,						
				A Filter								2
				🕑 Users 🕑 Groups 🔘 Co	ntacts	0.6	mputer	\$				
				Name					anted I			
				A Jones, Gareth (8man-demo)			now or	ten gi	inted i	A	Le	
				Sones, Gareth (8man-demo)		Jones)				A		
				📥 🕑 Pull, Sam (8man-demo\Sam	Pull)			1				
<	^											
											Catest scan	· · 0 ·

- 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

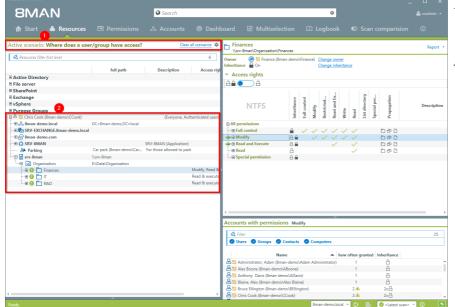
8MAN

Alternatively, you can capture the same information in a report: <u>Which resources does a user have</u> <u>access to?</u>

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

Version: 7.	2			
8MANn	@ cook	× • \$	🚔 cradmin 👻	
	Users (2)	Cooko) disalayaamo: Cooko, Amelia sa		
🔒 Start 💩 Resources 🖃 Permissions		Cooke) displayeame: Cooke, Amelia ce: displayname: Chris Cook cn: Chri	🛛 Scan comparision 🛛 🛈	1
Resources	Chris Cook (8man-demo\CCook)	displayname: Chris Cook cn: Chri		-
Resources filter first level	Directories (0)			
Resources filter first level	Mailboxes (2)			
full path	Cooke, Amelia	Amelia.Cooke@8man-demo.local		
Active Directory	Chris Cook	CCook@8man-demo.local		
File server	vSphere (0)			
SharePoint	Public Folders (0)			
Exchange vSphere	Mailbox Folders (0)			
Vsphere Purpose Groups	Active Directory Resources (2)			
B Purpose Groups	Cooke, Amelia (Amelia Cooke)	cn: Amelia Cooke name: Amelia		
	Chris Cook (CCook)	cn: Chris Cook name: Chris Cook		
	Purpose Groups (0)			
	1			
^				-
Ready		8man-demo.local 🛩	🔅 🖶 🥝 «Latest scan» 👻 🕕 🧮	J

- 1. Select "Resources".
- 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.

		ి Accounts	⑦ Dasht		☑ Multiselect		шı							
ctive scenario: Where does a us	er/group have access?	Clear	all scenarios 🌣	Finar	nces Bman\Organization\Fina	inces								Report
🔇 Resources filter first level			6	Owner Inheritance	🙆 📁 Finance (8ma				owner inherit					
	full path	Description	Access rigi	 Acces 			5	nange	inhent	ance	_	_		
Active Directory					2									
File server				8ê 💽	A									
SharePoint												~		
Exchange						ace	2		Restricted Read and Ex			List directory	Propagation	
VSphere			_		NTFS	itar	out	à.	and a			il i	a be	Descr
Purpose Groups		17 A .	henticated users,			Inheritance	Full control	Modify	Restricted Read and Ex	Write	Read	ist	do J	
- D & 8man-demo.local	DC=8man-demo.DC=local	(Everyone, Aut	nenticated users,	All perr	- lesla -	-	-	~		>	<u> </u>		n 🗠	
······································			-		control		. /	1.	/ /	1	1		D & C	
⊕ 🖓 8man-demo.com			2	- B Mod		8.8	× .	2	2.5	- Ž	2		000	
		SRV-8MAN (Application)			2 I_E\$_md (8man-d			2	2 X	Č,	2			\\srv-8man\E\$
& Parking	Car park (8man-demo\Car		k .		1_E\$_Finances_mo			2	10					\\srv-8man\E\$\Fin
🕀 🗐 sry-8man	\\srv-8man				E 🕑 🔟 Audit (8man-de									Test for Descriptio
- 🕀 🛃 Organization	E:\Data\Organization				C-Level (8man-			1	11	1	1		000	
- 🕀 😝 🔲 Finances			Modify, Read &		名 📁 Bruce Ellingt	ion (🔒		1.	11	~	\checkmark		000	1
- 🕀 🚯 🛅 Accounts Payable			Modify, Read &	-	🐣 📁 Chris Cook (1.	11	~	\checkmark		000	1
····· 🕒 🚺 Kcounty eivable			Modify, Read &		🔒 📁 Jimmy Ward	(8m 🔒		1.	11	~	\checkmark		000	1
🕀 🕒 🛅 Expense			Modify, Read &		📖 呂 📁 Sales, Sam (A			\sim .	/ /	~	\checkmark		000	1
🔒 🛅 Home			Modify, Read &	-0	🗄 🥮 🐻 Finance (8man-			 	/ /				000	
😣 🛅 New Project directory			Modify, Read &		20 19 (8man-dem			~ `	/ /				000	
- B D Offices			Modify, Read & Modify, Read &		- A Gareth ()				/ /				000	
L			Read & execute		A Torrey Smith (8			~ `	/ /	\sim	1		000	
			Read & execute	Read	d and Execute	88			~		1		000	
			Near of everyte		a cial permission	A A A					~		000	
				spec	cial permission									

- 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

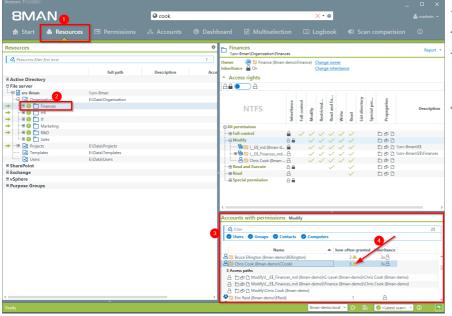
4.2.2.1 Identify multiple access paths to file server directories

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

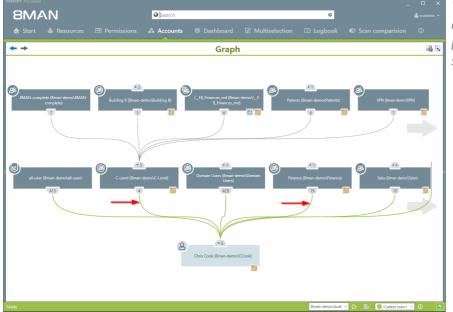


- 1. Select "Resources".
- 2. Select a directory.
- 3. 8MAN shows you all access rights of the selected user in a flat list.
- 4. The yellow warning indicates multiple access rights. Click on it.



8MAN		🛛 cook			ו\$		
🚖 Start & Resourc	es 🖃 Permissions						
esources				ances			Report -
Resources filter first level Active Directory	full path	Description	1 Owner Acce	v-8man\Organization\Finances Bill Finance (8man-de nce Do Construction cess rights	; mo\Finance) <u>Change owner</u> <u>Change inherita</u>	000	
File server			100 C				
	\\srv-8man						
→ B O Crganization → B O C Finances → B O C HR → B O C HR	E\Data\Organization			NTFS	Select all		I+A Description
				ermissions Ill control	A Show in accounts vie		
Templates Users	E:\Data\Projects E:\Data\Templates E:\Data\Users		œ	8 1_ES_md (8man-d 6 8 10 L_ES_Finances_md 6 8 10 Chris Cook (8man 6			n\E\$ n\E\$\Finances
E SharePoint	C (D 818 (03615						
∋ Exchange			>		t change group memo	erships	
BvSphere					🖞 🔒 Create new user or g	roup	
⊞ Purpose Groups			<		Unlock user Deactivate account Change password op		
			Accou	nts with permissions	Mot 👸 Soft delete user acco		
					Bolt delete user acco Belete account	with the second s	
			4, Fi 🕑 U	ilter sers 🥏 Groups 🥑 Conta			25
			8	Name	🔯 Add note Filin 🖄 Open Logbook		
			■ 3 Acc 3 Acc 3 C	Chris Cook (8man-demo\CCool ess paths 기 라 다 Modify\J_E\$_Finances	k) 5_md (8man-demo)\C-Level (8r 5_md (8man-demo)\Finance (8r	3 ▲ 3x 🗎 nan-demo)\Chris Cook (8man-de man-demo)\Chris Cook (8man-de	
			> • • • • • •	ric Reid (8man-demo\EReid)		1 8	

- 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

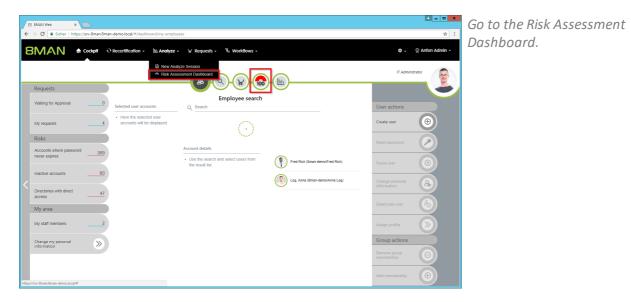
If "Everyone accounts" are used for the assignment of access rights, (almost) everyone has access to the connected resources. The consequence is an excessive assignment of access rights and a high probability for unauthorized access. These go against the principle of least privilege and should therefore 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





- 1 D X 🗢 🗸 👳 Anton Ad Q Re ШĿ, ₩ Requests + ۴. ۱ 100 100 100 as with direct acces Ö 100 99 15 ed SIDs C Ŏ 2 0 changed access rights C
- 8MAN shows a rating for the risk factor "Globally accessible directories".
 Click "Minimize risks".

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

8	BMAN 🕈 Home 🛛 Recertification - 🔟 Analyze - 🗜	Requesting -	🗞 Workflows 🗸				🌣 🗸 🐣 demoadmi
		Configuratio	on 🜩				Reports
(Blobally accessible directories (51)	-	permissions, All 'Authenti	icated Users'	permissions, All	'Domain Users'	Direct Excel export
1	2	permissions		3			Create Report
D	rag columns here to create groups.		3 columns selected		C 🔳	E 6	Greate Report
	Path			Account	Rights	Requested Action -	Available Actions
J	\srv-8man\clean! source\clean! 1\05 - NULL DACL\NullDACL			Everyone	-		
	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederBerechtigi	ung		Everyone	Full control		
	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederErstBesiA	uthBen		Everyone	Full control		
	\\srv-8man\clean1 source\clean1 2\05 - NULL DACL\NullDACL			Everyone	Full control		
	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederBerechtig	ung		Everyone	Full control		
	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederErstBesiA	uthBen		Everyone	Full control		
	\\srv-8man\clean! source\clean! 3\05 - NULL DACL\NullDACL			Everyone	Full control		
	\\srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung definiert\JederBerechtig	ung		Everyone	Full control		
	\\srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung definiert\JederErstBesiA	uthBen		Everyone	Full control		
	\\srv-8man\clean1 source\clean1 10\05 - NULL DACL\NullDACL			Everyone	Full control		
	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederBerechtig	gung		Everyone	Full control		
	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederErstBesi	AuthBen		Everyone	Full control		
	\\srv-8man\cleanI source\cleanI 6\05 - NULL DACL\NuIIDACL			Everyone	Full control		
	\\srv-8man\clean! source\clean! 6\10 - Ungewollte Berechtigung definiert\JederBerechtig	ung		Everyone	Full control		
	\\srv-8man\clean! source\clean! 6\10 - Ungewollte Berechtigung definiert\JederErstBesiA	uthBen		Everyone	Full control		
	\\srv-8man\clean1 source\clean1 5\05 - NULL DACL\NullDACL			Everyone	Full control		
	\\srv-8man\clean! source\clean! 5\10 - Ungewollte Berechtigung definiert\JederBerechtig	ung		Everyone	Full control		
	\\srv-8man\clean1 source\clean1 5\10 - Ungewollte Berechtigung definiert\JederErstBesiA	uthBen		Everyone	Full control		
	\\sry-8man\cleanI source\cleanI 7\05 - NULL DACL\NullDACL			Everyone	Full control		

- 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

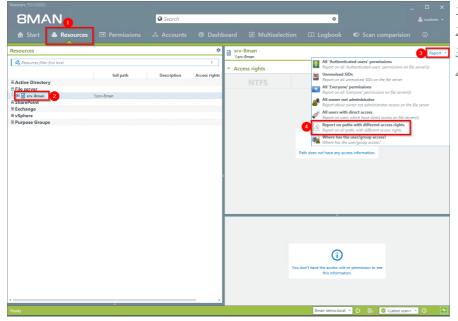
Background / Value

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



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



8MAN Ve			
	Search		
Resources	 Report on paths with different access rights 		×
Resources filter first la	Report configuration	Report on paths with different access r	ights
	Title Title	Please select resource(s)	×
Active Directory BFile server	Comment Comment	Resources	
🕂 🕀 🖹 srv-8man	Objects -	Active Directory	
U SharePoint	2 srv-8man	Server	
⊕ vSphere		SharePoint	
I Purpose Groups		⊕ Exchange ⊕ vSphere	
	 Settings 		
	The output format is XLS *		
	Report execution mode <u>started manually</u> Store on specific path is <u>Deactivated</u>		
	Send email is Deactivated	3	
		Start	Discard
		>	
Ready		8man-demo.local	🗠 🕒 📑 🥥 < Latest scan> 🕐 🕕 🦉

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

Fro		Existing Connections Refresh All - Detrillies Connections	Text to Flash		nsolidate What-If Rela	tionships Grou	up Ungroup Subtotal
43	• • × ~	f paths with different access rights					
	A	В	С	D	E	F	
	srv-8man 2						
Ì	paths with different access righ	(×	Access explicitly denie	 Inheritance activate 	Inheritance corrupte *	ACL extend *	Added entries
	Finances	\\srv-8man\Organization\Finances	No	On	No	Yes	BUILTINVAdministrators;1_E5_Fit
	Accounts Payable	\\srv-8man\Organization\Finances\Accounts Payable	No	On	No	Yes	BUILTIN\Administrators;BUILTIN\
	Accounts receivable	\\srv-8man\Organization\Finances\Accounts receivable	No	On	No	Yes	BUILTIN/Administrators; BUILTIN/
	Expenses	\\snv-8man\Organization\Finances\Expenses	No	On	No	Yes	BUILTIN/Administrators; BUILTIN/
	Expenses Project	\\srv-8man\Organization\Finances\Expenses\Expenses Project	No	On	No	No	
	Home	\\srv-8man\Organization\Finances\Home	No	On	No	Yes	BUILTIN/Administrators:BUILTIN/
	Invoices	\\sry-8man\Organization\Finances\Invoices	No	Off	No	Yes	BUILTIN/Users: E\$ Finances
	Berlin	\\srv-8man\Organization\Finances\Invoices\Berlin	No	On	No	Yes	BUILTIN/Administrators BUILTIN
	New Project directory	\\srv-8man\Organization\Finances\New Project directory	No	On	No	Yes	BUILTIN\Administrators:BUILTIN
	Salaries	\\srv-8man\Organization\Finances\Salaries	No	On	No	Yes	BUILTIN/Administrators: BUILTIN/
	Berlin	\\srv-8man\Organization\Finances\Salaries\Berlin	No	On	No	Yes	BUILTIN\Administrators
	München	\\srv-8man\Organization\Finances\Salaries\München	No	On	No	Yes	BUILTIN/Administrators
	HR	\\srv-8man\Organization\HR	No	On	No	Yes	BUILTIN/Administrators BUILTIN/
	Contracts	\\srv-8man\Organization\HR\Contracts	No	On	No	No	DOIL INVIGINING TRADE OF
	Employees	\\srv-8man\Organization\HR\Employees	No	On	No	Yes	I E\$ HR Employees re (8man-
	Legal	\\srv-8man\Organization\HR\Legal	No	On	No	Yes	I ES HR Legal re (8man-demo
	Salaries	\\srv-8man\Organization\HR\Salaries	No	On	No	No	I_L3_IIK_Legal_re (oman-demo
	Galaries IT	\\srv-8man\Organization\T	No	On	No	Yes	BUILTIN/Administrators: BUILTIN/
	Install	\\srv-8man\Organization\T\Install	No	On	No	No	BUIL INVAUMINIStrators, BUIL INV
	Support	\\srv-8man\Organization\IT\Support	No	On	No	No	
	Support Marketing	\\srv-8man\Organization\II\Support \\srv-8man\Organization\Marketing	No	On	No	Yes	BUILTIN/Administrators: BUILTIN/
	Marketing Events	\\srv-8man\OrganiZation\Warketing \\srv-8man\OrganiZation\Marketing\Events	No	On	No	Yes	
				Off		Yes	I_E\$_Marketing_Events_fc (8ma BUILTIN/Administrators:BUILTIN/
	Product Description	\\srv-8man\Organization\Marketing\Events\Product Description	No	Ott	No	Yes	
	Flyer R&D	\\srv-8man\Organization\Marketing\Flyer			No		I_ES_Marketing_Flyer_re (8man
		\\srv-8man\Organization\R&D	No	On	No	Yes	BUILTIN\Administrators;BUILTIN\
	Source Code	\\srv-8man\Organization\R&D\Coding\Source Code	No	On	No	Yes	BUILTINVAdministrators
	Sales	\\srv-8man\Organization\Sales	No	On	No	Yes	BUILTIN/Administrators; BUILTIN/
	New IT project	\\srv-8man\Projects\New IT project	No	On	No	Yes	BUILTIN/Administrators;BUILTIN/
	Top Secret IT Project	\\second an\Projects\Top Secret IT Project	No	On	No	Yes	BUILTIN/Administrators;BUILTIN/

-

Z A A Z 10

1

- 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".

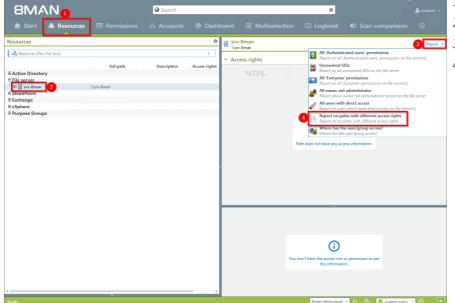
2. The results show the directories with defective ACLs.



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.



- 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"

8MAN Ve						
		❷ Search				
🚖 Start &						
					· · · · ·	_
Resources	Report on paths with differen	t access rights			×	
Resources filter first la	Report configuration		Report on paths with	n different access ri	ghts	
	Title		Please select resource(s)		×	
Active Directory File server	Comment Comment			Resources		
	Objects		Active Directory			
U SharePoint	2 srv-8man	ž	File server			
[⊕] vSphere			SharePoint			
I Purpose Groups			Exchange VSphere			
	 Settings 					
	The output format is XLS *					
	Report execution mode started manually					
	Store on specific path is <u>Deactivated</u> Send email is <u>Deactivated</u>			- 6		
				Start	Discard	
				Start	Discard	
					_	
		2				
Ready	~			8man-demo.local	× 0- B- ⊘ <lat< td=""><td>test scan> 🕜 🚺</td></lat<>	test scan> 🕜 🚺

- 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.

om From From From Other cess Web Text Sources - Get External Data	Existing Connections Connections Connections Connections Connections Connections Connections Connections Connections Connections Connections Connections Connections Connections	Text to Flash		nsolidate What-If Rela	tionships Grou	p Ungroup Subtotal
3 * : × ~	f paths with different access rights					
٨	8	C	D	F	E	
srv-8man	0		0			
paths with different access right	×	Access explicitly denie	Inhoritanco activate a	Inheritance comunity	ACL extend x	Added optrion
Finances	\\srv-8man\Organization\-inances	No	On	No	Yes	BULTINVAdministrators:1 ES Fil
Accounts Payable	\\srv-8man\Organization\Finances\Accounts Payable	No	On	No	Yes	BUILTIN/Administrators: BUILTIN/
Accounts receivable	\\srv-8man\Organization\Finances\Accounts receivable	No	On	No	Yes	BUILTIN/Administrators BUILTIN/
Expenses	\\srv-8man\Organization\Finances\Expenses	No	On	No	Yes	BUILTIN/Administrators: BUILTIN/
Expenses Project	\\srv-8man\Organization\Finances\Expenses\Expenses Project	No	On	No	No	
Home	\\srv-8man\Organization\Finances\Home	No	On	No	Yes	BUILTIN/Administrators:BUILTIN/
Invoices	\\srv-8man\Organization\Finances\Invoices	No	Off	No	Yes	BUILTIN\Users;I E\$ Finances
Berlin	\\srv-8man\Organization\Finances\Invoices\Berlin	No	On	No	Yes	BUILTIN/Administrators:BUILTIN/
New Project directory	\\srv-8man\Organization\Finances\New Project directory	No	On	No	Yes	BUILTIN/Administrators:BUILTIN/
Salaries	\\srv-8man\Organization\Finances\Salaries	No	On	No	Yes	BUILTIN/Administrators; BUILTIN/
Berlin	\\srv-8man\Organization\Finances\Salaries\Berlin	No	On	No	Yes	BUILTINVAdministrators
München	\\srv-8man\Organization\Finances\Salaries\München	No	On	No	Yes	BUILTIN\Administrators
HR	\\srv-8man\Organization\HR	No	On	No	Yes	BUILTIN\Administrators;BUILTIN\
Contracts	\\srv-8man\Organization\HR\Contracts	No	On	No	No	
Employees	\\srv-8man\Organization\HR\Employees	No	On	No	Yes	I E\$ HR Employees re (8man-
Legal	\\srv-8man\Organization\HR\Legal	No	On	No	Yes	I ES_HR_Legal_re (8man-demo
Salaries	\\srv-8man\Organization\HR\Salaries	No	On	No	No	
п	\\srv-8man\Organization\/T	No	On	No	Yes	BUILTIN/Administrators; BUILTIN/
Install	\\srv-8man\Organization\IT\Install	No	On	No	No	
Support	\\srv-8man\Organization\IT\Support	No	On	No	No	
Marketing	\\srv-8man\Organization\Marketing	No	On	No	Yes	BUILTIN/Administrators;BUILTIN/
Events	\\srv-8man\Organization\Marketing\Events	No	On	No	Yes	I_E\$_Marketing_Events_fc (8ma
Product Description	\\srv-8man\Organization\Marketing\Events\Product Description	No	Off	No	Yes	BUILTIN/Administrators; BUILTIN/
Flyer	\\srv-8man\Organization\Marketing\Flyer	No	On	No	Yes	I_ES_Marketing_Flyer_re (8man
R&D	\\srv-8man\Organization\R&D	No	On	No	Yes	BUILTIN\Administrators;BUILTIN\
Source Code	\\srv-8man\Organization\R&D\Coding\Source Code	No	On	No	Yes	BUILTINVAdministrators
Sales	\\srv-8man\Organization\Sales	No	On	No	Yes	BUILTIN/Administrators;BUILTIN/
New IT project	\\srv-8man\Projects\New IT project	No	On	No	Yes	BUILTIN/Administrators;BUILTIN/
Top Secret IT Project	\\second pan\Projects\Top Secret IT Project	No	On	No	Yes	BUILTIN/Administrators;BUILTIN/

- 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.

Refresh All • Conn 2↓ ZAZ Z↓ Sort • ₽•□ ? A 4 Bata sny-8m paths with different acc Finances ess explicitly d N 2↓ Sort A to Z N Z↓ Sort Z to A Yes Yes Yes Yes Yes Yes Yes Yes Yes No Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes Sort by Cole ■ (Selec I_E\$_HR_Employ I_E\$_HR_Legal BUILTING OK Cancel No No On No On No On No On No On No No No No No

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

FILE HOME INSERT PA	GE LAYOUT FORMULAS DATA REVIEW VIEW					- 0
Access Web Text Sources - Co	Existing nections All + Connections 21 212 Reap Properties All - Sort Filter Adva	ply Text to Flash R	emove Data Co plicates Validation *	nsolidate What-If Rela	tionships Grou	p Ungroup Subtotal
Get External Data	Connections Sort & Filter		Data Tools			Outline 🙀 🖌
D3 * : 🗙 🗸 .	fx Inheritance activated					,
A	В	C	D	E	F	
srv-8man						
paths with different access right 🕶		Access explicitly denie				Added entries
	\\srv-8man\Organization\Finances\Invoices \\srv-8man\Organization\Marketing\Events\Product Description	No No	Off	No No	Yes	BUILTIN/Users;I_E\$_Finances_Ir BUILTIN/Administrators;BUILTIN/L
13 Product Description	vsiv-omaniorganizationmarketing/Events/Product Description	NU	UI	140	Tes	DOIL 11199000000000000000000000000000000000
4						
5						
6						
7						
8						
9						
1						
2						
3						
4						
5						
6						
8						
9						
0						
1						
2						
3 4						
5						
6						
7						
8						
59						
50						
Configuration	1-srv-8man (+)		•			Þ

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



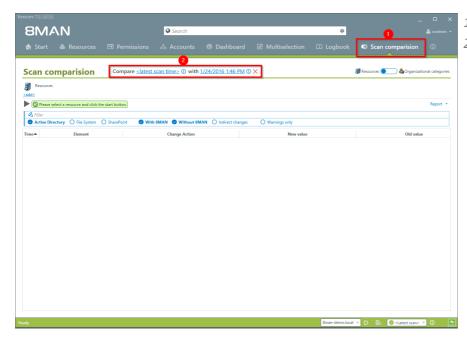
4.2.2.5 Compare two different access rights situations (Scan Comparison)

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.

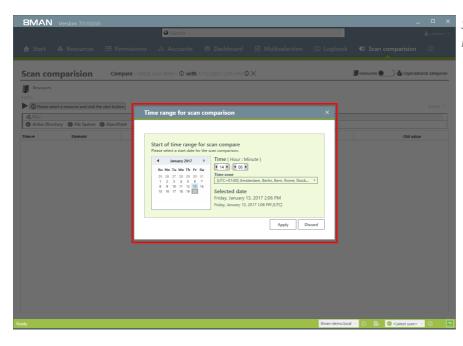
Additional Services

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 <u>Security Monitoring</u>. Alternatively you can also <u>compare two</u> <u>scans from different points in time</u>.



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

88 Access Rights Management



Select the date and time of both scans.

8MAN Version: 7.	
Search	
🏫 Start 💩 Resources 📼 Permissions 👶 Accounts 🛞 Dashboar	
Scan comparision Compare statest scan times: () with 1/24/2016 1:46 PM	C Resources C & Organizational categories
Resources Currently used scans	
O Prove sector a resource are listed in the table below. I resource.	n addition, scan errors (if any) are listed under each scanned
Active Directory (6
Ilme	Old value
File server (1) Image: Simple serve	
♥ SharePoint (1) 	
	Close Indiana
Ready	8man-demo.local 👻 🔕 🛛 🛃 🥥 <latest scan=""> 🛸 🕕</latest>

The comparison always compares existing scans.

- 1. Click on the information icon.
- 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.

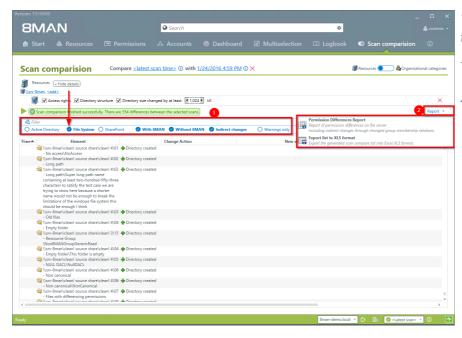
8MAN

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

BMAN		0.0 1					
		Search			÷		📥 cra
						Scan co	mparision
can comparision	Compare <latest< td=""><td>scan time> ① with</td><td>1/24/2016 1·46 PM (</td><td>X</td><td></td><td>🔳 Resources 🔵</td><td>A Organizational cat</td></latest<>	scan time> ① with	1/24/2016 1·46 PM (X		🔳 Resources 🔵	A Organizational cat
Resources	compare <u>statest</u>	Jean antes () when	<u>17242010 1.401111</u> (a nesources	
Please select a resource and clici	the start button.						Rep
lease select resource(s)	×						
Resources	🥑 With	n 8MAN 🥑 Without 8M	IAN () Indirect changes	O Warnings only			
Active Directory File server	Image: Accounts Image: Accounts						
B SharePoint							
DisnarePoint							

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

8MAN		Search	_		۵		
						Scan comparision	
Scan comparision	Compare <u><latest< u=""></latest<></u>	<u>scan time></u> () with	<u>1/24/2016 4:32 PM</u> ()	×		🗊 Resources 🔵 🔓 Organizat	onal categories
Resources («Hide details)	1						
🗐 🗹 Access rights 🖌 Directory :		anged by at least 1,024	4 kB				×
Please select a resource and click the							Report *
2 lease select resource(s)	× 🖉 With	8MAN 🕝 Without 8M	AN O Indirect changes	O Warnings only			
Resources Active Directory File server		Change Action		New value		Old value	
sry-8man SharePoint							
SharePoint							
					8man-demo.loca		- O
eady					oman-demo.loca	👻 😳 📑 🥝 <latest scan=""></latest>	<u> </u>



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.



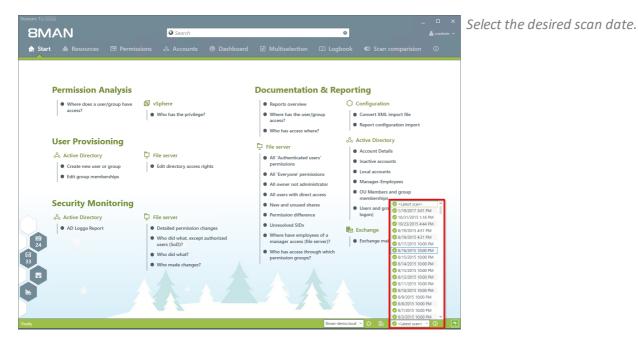
4.2.2.6 Analyze historical access rights situations

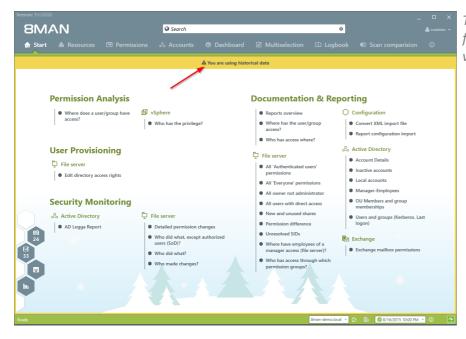
Background / Value

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.





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

4.2.2.7 Identify the last activities on a directory

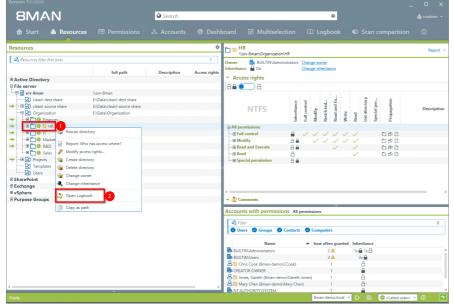
Background / Value

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.

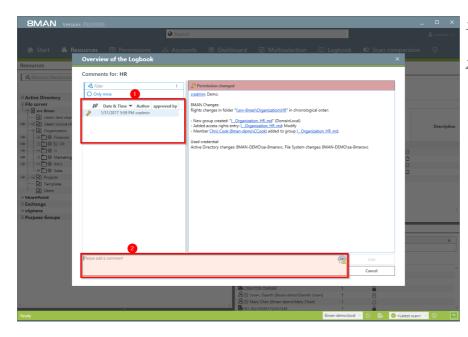
8MAN 1		Finde				¢							
🔒 Start 💩 Ressou	ırcen 🖃 Berechtigung												
essourcen:				\$	Marketing								Report
🔇 Ressourcen-Filter erste Ebene	vollständiger Pfad	Beschreibung	Berechtigungen	1 Verzeichnisgröße	Besitzer 🏠 Administratoren Vererbung 🔒 Aus		lemo∖/	\dmini:	stratore			ndern anpasser	
Active Directory					 Freigabe-Information 								
Fileserver					 Zugriffsberechtigung 	en						2	1 🔵
🖓 📄 srv-8man	\\srv-8man				AA 🕥 A								
Archive	D:\Archive			0 Byte									
 Clean! source Clean! target 	D:\clean! source share			0 Byte					- u			Übernehmen für	
Clean! target Clean! target Clean! target	C:\clean! target Share D:\Finanz			0 Byte 3 KB	NTES	Vererbung	Vollzugriff	-	Eingeschrän	Schreiben		-He	
Finanz	D:\Finanz D:\GF			3 KB 1 KB	INTIS	rerb	2	Ändern	en la	ie i	Lesen	E .	
- E A Home	D:\Home			0 Byte		Vc	٨	Ň	<u>a</u> <u>a</u>	Sc	5	9.5	
► ···· ··· ···························	DAIT			3 KB	Alle Berechtigungen								
🕀 🛃 Marketing	D:\Marketing			3 KB	Vollzugriff	a	\checkmark	\checkmark	~ ~	/ /		000	
Events	oronancong			968 Bytes	Andern	8		\sim	~	\sim		000	
🕀 🕒 🛅 💯 Flyer				412 Bytes	·-· ⊞ Lesen und Ausführen	a			~		\sim	000	
Presse				4 Bytes	>⊕ Spezielle Berechtigung	a	\checkmark	\sim	\sim	~		6 C	
😳 📇 🦁 Produktbeschre	ibung			412 Bytes									
Secret Projects	_			408 Bytes									
▶ ····⊞ 🛅 /orlagen	3			628 Bytes									
68 🛃 Per				2 Bytes									
🕨 🕀 🛃 Ver 🎒 1 Kommenta	r			2 KB									
	14:44, Erstellt von: cradmin												
B Exchange cradmin: neu	es projekt												
B vSphere	durch 8MAN:												
Purpose Gro													
	chnis unterhalb wurde erzeugt: \\srv-8n	an\Marketing\Vorlager	New Folder123										
SharePoint Verwendete	Anmeldung: 8man-demo\administrator												
shareronit	-												
					<								
	^				8MAN-DEMO.LOCAL -	_		^		_	_	🐓 Ven	

- 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.

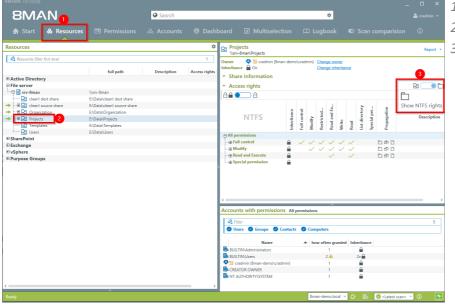
4.2.2.8 Identify share permissions

Background / Value

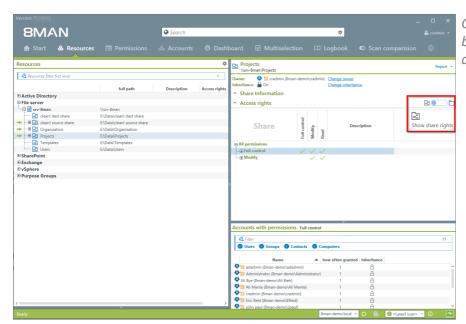
8MAN shows both: share permissions as well as NTFS permissions. In the standard view the NTFS permissions are listed.

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

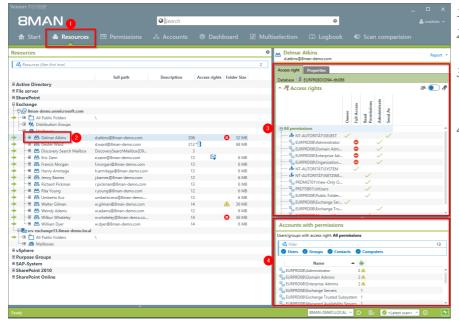
Who as access to which mailbox? 8MATE Exchange shows you all access rights in the resources view.

Additional Services

Report: <u>"Who has access to what?"</u> Report <u>"Identifying mailbox permissions"</u>

Step by step process

8MAN



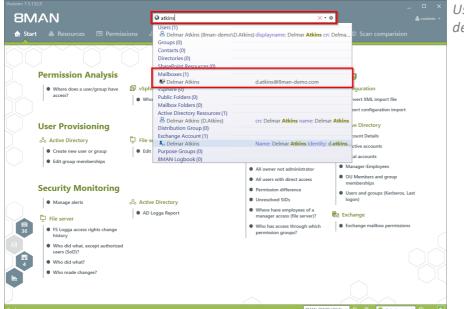
- 1. Select "Resources".
- 2. Navigate to the desired mailbox.
- 3. 8MAN shows you which users/groups have which rights.
- 4. 8MAN shows all accounts with access rights in a flat list.

Identify mailbox properties 4.3.1.2

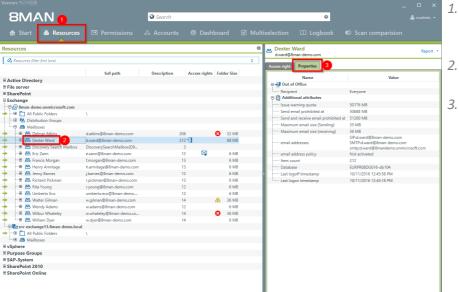
Background / Purpose

8MATE Exchange shows the properties of individual mailboxes.

Step by step process



Use the search field to find the desired mailbox.



8MAN-DEMO.LOCAL - 😥 🖶 🥥 <Latest scan> - 🚺

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

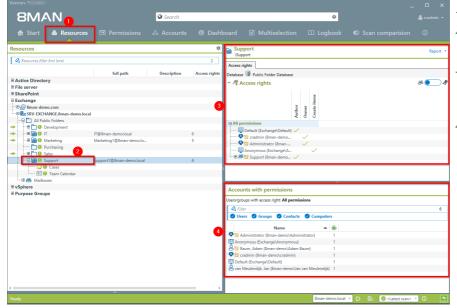
4.3.1.3 Identify access rights on public folders

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: <u>Who has access to what?</u> Report: <u>Identifying Mailbox access rights</u> <u>Creating a Mailbox</u> <u>Changing access rights to email accounts</u> <u>Changing out-of office notice</u> <u>Changing Mailbox size</u>



- 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.



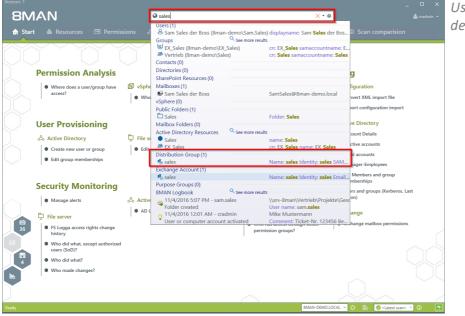
4.3.1.4 Identify permissions on distribution groups

Background / Value

With 8MAN you can quickly check who is allowed to 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.

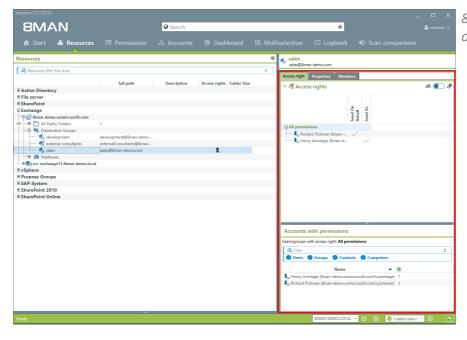
Displaying these access rights is also possible with dynamic Exchange groups.

Step by step process



Use the search field to find the desired Distribution group.

| Access Rights Management



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

MAN

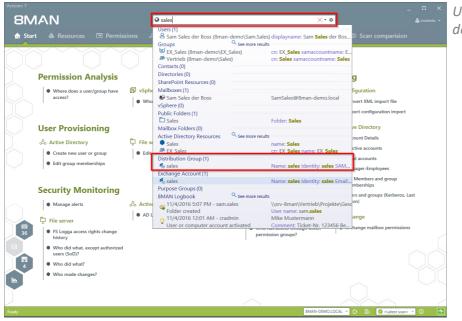
4.3.1.5 Identify members of distribution groups

Background / Purpose

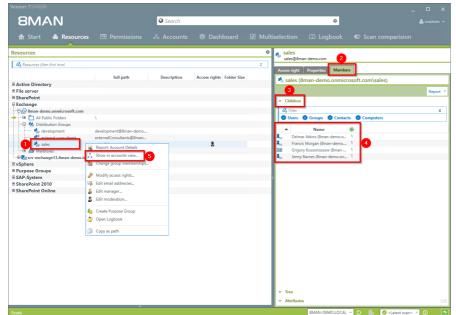
8MAN allows you to display all members and / or recipients of distribution lists. In typical 8MAN fashion this also includes nested group memberships.

This is also possible for dynamic Exchange groups.

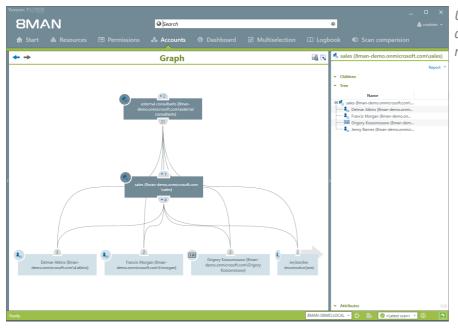
Step by step process



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 8MANs 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

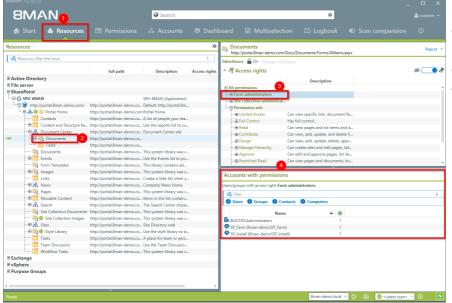
4.4.1.1 Identify access rights on SharePoint resources

Background / Value

8MATE for SharePoint i 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: <u>Who has access to what?</u> Report: <u>What do users/groups have access to?</u> <u>Changing access rights to SharePoint resources</u> <u>Setting the naming convention for AD Groups</u>



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

4.4.2 Services for administrators

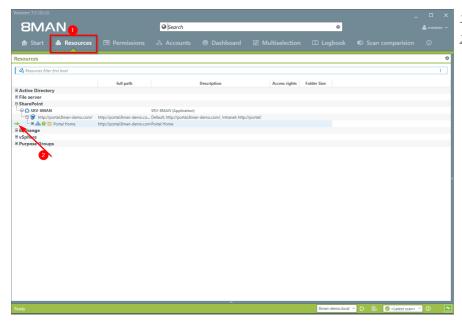
4.4.2.1 Identify divergent access rights in the tree structure

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: <u>Who has access to what?</u> Report: <u>What do users/groups have access to?</u> <u>Change acsess rights to SharePoint resources</u> <u>Set the naming convention for AD Groups</u>



- 1. Select "Resources".
- 2. The green arrow indicates that some of the subdirectories contain divergent access rights.



/ersion: 7	MAN		Searce	h				٥		
Resourc	es									
\land Reso	urces filter first level									;
	_	full path		Descr	iption		Access rights	Folder Size		
	RV-8MAN	Ton poor	SRV-8MAN (App		iption		neces rights	Torder blee		
	http://wrtal.8man-demo.com	1/ http://portal.8man-demo.co			com/ Intran	ati http://partal/				
	B also 9 10 Portal Home	http://portal.8man-demo.co		ortacomanification	ocomy, muan	ec map?/ponav				
	Contacts	http://portal.8man-demo.co			with Dise must					
		Re http://portal.8man-demo.co								
	······································	http://portal.8man-demo.co			the queries of	iat appear in the	6			
	Documents	http://portal.8man-demo.co		er site						
	Tasks	http://portal.8man-demo.co								
	Documents									
		http://portal.8man-demo.co								
	- 🕀 🔟 Events	http://portal.8man-demo.co								
	Form Templates	http://portal.8man-demo.co								
	···· 🕀 🛐 Images	http://portal.8man-demo.co								
	Links	http://portal.8man-demo.co			links to Web	pages or other re	50			
	🕀 👫 News	http://portal.8man-demo.co								
	····································	http://portal.8man-demo.co								
	🕀 🎹 Reusable Content	http://portal.8man-demo.co	Items in this list	contain HTML or	text content	which can be inse	ert			
	·· 🕀 📇 Search	http://portal.8man-demo.co								
	🛅 Site Collection Docume	nts http://portal.8man-demo.co	This system libra	iry was created by	r the Publishi	ing Resources fea	tu			
1	· · · · · · · ·				~					_
ghts d	ifferent from parent 🛛 🚨	Documents http://portal.8m	an-demo.com/Doc	:s/Documents/Fo	rms/AllItems	aspx				
🛿 Filter										
	Path		Size/item D	eny Inheritance		2				
						-				
	o://portal.8man-demo.com/Docs			• A						
	http://portal.8man-demo.com/D				2 3					
Market	ting (http://portal.8man-demo.co	om/Docs/Documents/Marketing)		- A	2 5					
_										

- 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.

T START 69 Resources																
Image: Marketing Interpretation Marketing Interpretation Image: Image: <th< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th<>																
A Resources filter first level			1	1								ms/Al	Illtems	s.aspx)		
	full with		Description	1	to the second se	in-de	mo.co	om/Do	:s/Do	cumer	.ts/IT)					
ctive Directory	Tur paul		Description	~	4 Filter											
				11										E		
				11										atic		
		DV DMAN (Ameliantic		11										and and a		
				11		_				2		dhy	Pg	£.		
			nam democonte, intranec map	11		ft.			ť.	. 3	ve.	E a	Re	ę.	ê T	1
			and some the solid line as a family of the	11	Name	5	2 Eisi	git	8 7	A A	pro	Ŧ	ted	ace	0	11
						÷	ă		6	ite a	Api	age	tric	te ,	ŝ	
			ustomize the queries that appr	11		-			-	5		lan	Res	-		
		Jocument Center site		11								~		ted		
				а.										ţ.		
				- L										2°		
				- I	 Unchanged (15) 						_					_
				- 1	Approvers						1					
				. 1	B BUILTIN\Administrators											
							2			- 5	, î.,					
					Excel Services Viewers										/	
												1				
····· @ 🖳 Images	http://portal.8man-demo.co T	his system library was	created by the Publishing feat	· ~												/
	, in the second s		>	_	A Portal Home Owners											
nts different from parent	Documents http://portal.8map-	-demo.com/Docs/Doci	iments/Forms/Allitems.asny		Restricted Readers	Ť.,							.1			
	occurrents index becaused			_									× .			7
Filter			3												Ť	
Besk		Size (item Dame I		2												/
				-1							11					
				_			× .			· · ·	×.	×	× .			×
			0 2 3	- 1		Ť.,										
.marketing (http://portal.8man-demo.com	./ Uocs/ Uocuments/Marketing)	9	□ 2 S	1						~				1		
					- Andributor Hundgers	_	_		_	_	_	_	_	Ě	_	_
				1	 Added or removed entries (6) 						_					_
					# IT-Group (8man-demo\IT-Group)	æ				E	,					
				3		9										
				٦	Marketing (8man-demo\Marketing)			6	Ð	e	,					

- 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.

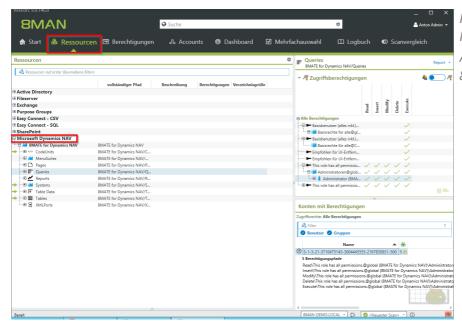
The Add-on Dynamics NAV integrates the authorization analysis of the ERP system in 8MAN. In the usual way you see all access rights in a flat list. In the first step, the module provides Services in the area of Permission Analysis and Documentation & Reporting.

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





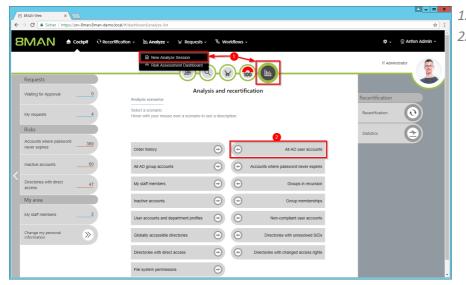
5.1 All Technologies

5.1.1 Flexible reports (web client)

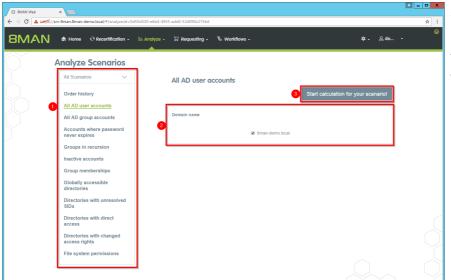
Background / Value

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



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



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

8	MA	N 🕈 Home O Recertification - 🔟 Analyze -	문 Requesting +	% Workflows -		÷	- & de
Al	AD	user accounts (433)	Configura All AD user :	tion 🌣 accounts: 8man-demo.local	2		Reports 3 Direct Excel export
Don	nain name	9 ×		Type, Name	- C 🔳	E C	Create Report
	Туре	Name	T Requested Action	Y			Available Actions
4	Domain n	name:8man-demo.local(433 items)		-			Execute script
		Clean - Admin (8man-demo\Clean - Admin)					
	8	Clean - Overall (8man-demo\Clean - Overall)					
	8	Clean - User (8man-demo\Clean - User)					
	•	sa-8mansvc (8man-demo\sa-8mansvc)					
	•	sa-Exchange_scan (8man-demo\sa-Exchange_scan)					
	8	SP_CacheSuperReader (8man-demo\SP_CacheSuperReader)					Deactivate Account
	•	SP_Install (8man-demo\SP_Install)					
	8	SP_CacheSuperUser (8man-demo\SP_CacheSuperUser)					
	8	SP_PortalAppPool (8man-demo\SP_PortalAppPool)					
	•	SP_Farm (8man-demo\SP_Farm)					
	8	SP_ProfileSync (8man-demo\SP_ProfileSync)					
	8	SP_ProfilesAppPool (8man-demo\SP_ProfilesAppPool)					
	8	SP_SearchContent (8man-demo\SP_SearchContent)					
	8	SP_SearchService (8man-demo\SP_SearchService)					
	8	SP_Services (8man-demo\SP_Services)					
	8	Anny Time (8man-demo\ATime)					
	8	Barrie Kenyon (8man-demo\BKenyon)					
	8	Harold Williams (8man-demo\HWilliams)					

- 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)

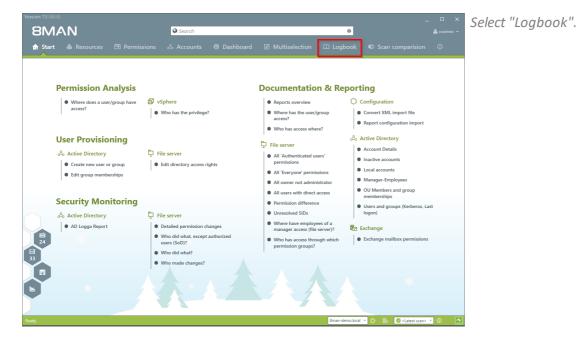
Background / Value

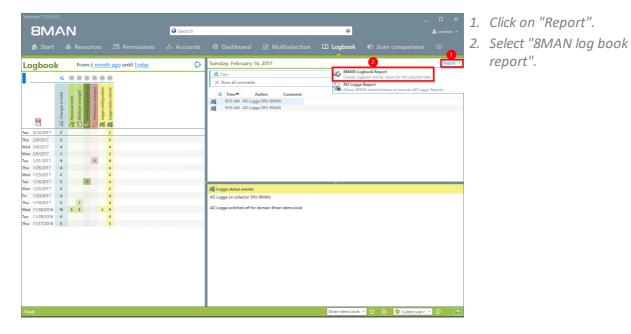
All changes made with 8MAN Enterprise are automatically recorded in the log book. This ensures compliance with a number of legal and best-practice standards and saves the time of manual documentation. The log book report allows you to capture events by person or event type within any desired time period.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

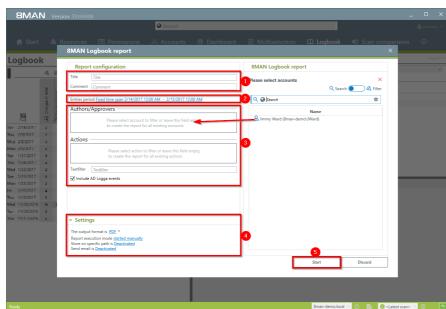
If your license agreement includes 8MAN Visor as well as 8MATE AD Logga, AD events will be recorded in the log book.

Additional Services

The <u>security monitoring</u> features expands documentation to include any administrative actions performed outside of 8MAN.







- 1. Enter a title for the report and add a comment.
- 2. Select the desired timeperiod for the report.

report".

- 3. Define the range of the report.
- 4. Define the desired report settings.
- 5. Start the report.



5.2 Active Directory

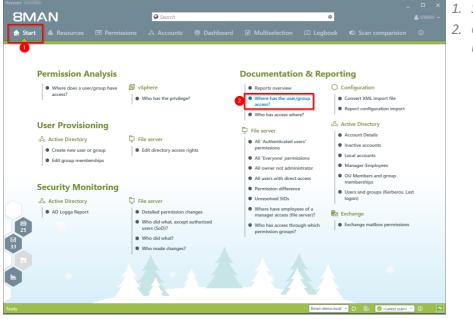
5.2.1 Management reports

5.2.1.1 Where do users and groups have access?

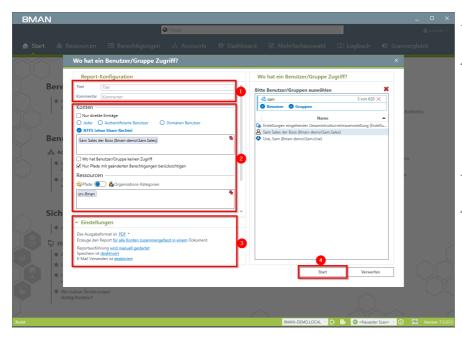
Background / Value

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



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



- 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

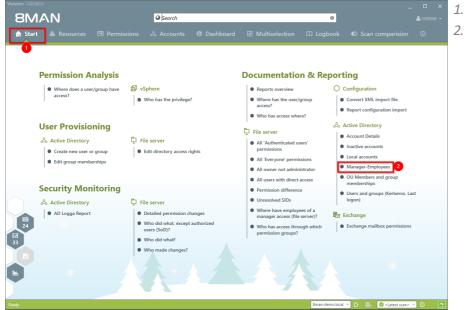
Data Owners that have some knowledge of Active Directory can view attributes and group memberships of their employees.

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

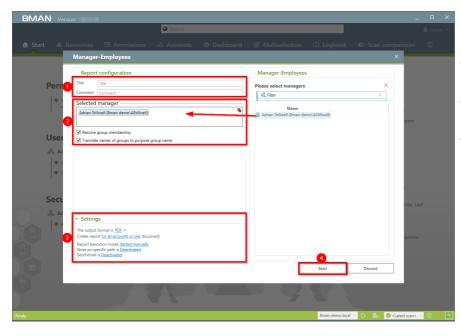
Additional Services

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)?



- 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

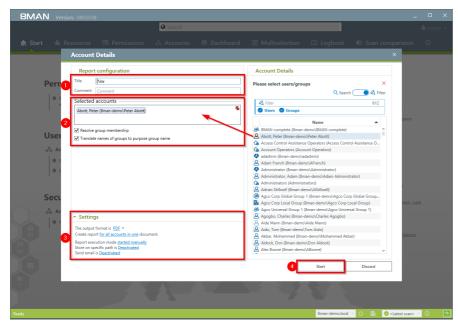
• Object GUID

- Object SID
- SAM Account Name
- SAM Account type
- Group memberships
- Parents + children
- Purpose Group names

BMAN	Search		_ □ ×	1. Select "Sto
Start & Resources 🖃 Permis		rd 🗵 Multiselection 🕮 Logi		2. Click on "A
Permission Analysis		Documentation & Re	porting	
Where does a user/group have access?	Ø vSphere ● Who has the privilege?	Reports overview Mere has the user/group access?	Configuration Convert XML import file Report configuration import	
User Provisioning & Active Directory Create new user or group Edit group memberships	 File server Edit directory access rights 	 Who has access where? File server All 'Authenticated users' permissions All 'Everyone' permissions All owner not administrator 	Active Directory Account Details Inactive accounts Local accounts Manager-Employees	
Security Monitoring	File server	All users with direct access Permission difference Unresolved SIDs	 OU Members and group memberships Users and groups (Kerberos, Last logon) 	
AD Logga Report	 Detailed permission changes Who did what, except authorized users (SoD)? 	 Where have employees of a manager access (file server)? Who has access through which permission groups? 	Exchange	
	Who did what? Who made changes?			
		8man-d	emo.local 👻 😥 📑 🥥 <latest scan=""> 👻 🕕 🌁</latest>	

Step by step process

"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)

BMAN Start & Resources ⊡ Permiss	ions 🖧 Accounts	Dashboard Multiselection	🕮 Logbook 🛛 🛛 Scan comparision	
eporting	~ L	Isers and other accounts		
		Users	429	
Active Directory		Users (Disabled)	6	
Inactive accounts		Administrators	12	
Local accounts		Administrators (Disabled)	0	
Users and groups (Kerberos, Last	^ G	iroups		
logon)	1	All Groups	183	
File server		Groups with members (w/o recursions)	104	
All 'Authenticated users' 23		Empty groups 🛕	76	
permissions		Groups in recursions 🛕	3	
All 'Everyone' permissions 34		The largest group (Domain Users (8man-demo\Domain Users))		
All owner not administrator 24		Built-in security groups	27	
		Global security groups	76	
All users with direct access 447		Universal security groups	35	
Unresolved SIDs		Local security groups	43	
		Global distribution groups	0	
		Universal distribution groups	2	
		Local distribution groups	0	
	^ <u>c</u>)U / Contacts / More		
~		Computers	4	
epth of nested groups		Computers (disabled)	0	
eptil et netted groups		Contacts	0	
71		Foreign users	0	
		Organizational Units	12	
12 9 2	1 ^ T	op 5 Kerberos Tokens [Bytes]		
1 2 3 4	5	Quinton Patton (8man-demo\QPatton)	1584	
Depth		lanar Garath (Rease dame)Garath lanar)	8man-demo.local Y 🔅 📑 🖉 <latest scan=""></latest>	• • 0

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

8MAN Version:	
Search	
	I ፼ Multiselection □ Logbook © Scan comparision ◎ ×
Report configuration	Inactive accounts
& Active Directr. Title Tate	
Inactive acco Comment Comment	Please select resource(s) × Resources
Local account Objects	B Active Directory
Uxerx and gro	ີ່⊕ _d G _o 8man-demo.local
Bman-demo.local	
File server	
All Authentic	
permissions	
All 'Everyone' Inactive Users	
All owner not All users of a selected domain ort logged on for a given period.	
An users with Unresolved 5.	-
∧ Settings	
The output format is CSV ~	
Report execution mode <u>started manually</u> Store on specific path is <u>Deactivated</u>	
Depth of I Send email is Deactivated	4
	Start Discard
12 0 2 1 A Top 5 Kerberos Token	is [Bytes]
1 2 3 4 5 Quinton Patton (Ilman-dem	io\C/Patton) 15И
Ready	Sman-demo.local V () Eo (Vatest scan> V ()
neady	onen ocholocal 1 () ES (Vicatest scanz 1 ()

- 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.

rom From From From Other Ccess Web Text Sources - Get External Data		Tet to Flash Remove Data Consolidate What If Rela Columns Fill Duplicates Validation * Analysis * Data Tools	tionships Group Ungroup Subtotal
			· Owne ·
24 \bullet : $\times \checkmark f_{\rm W}$	Days (Difference to current date)		
A	В	c	D E F G
Title	All users of a selected domain		
not logged on for a given period.			
Comment			
Author	8MAN-DEMO\cradmin		
Used time zone	W. Europe Standard Time (UTC+01:00:00)		
Date	2/16/2017 1:02:45 PM		
Version	7.6.131.0		
Scantime			
8man-demo.local	Active Directory	2/14/2017 10:00:03 PM	
Configuration			
	Selected resources:		
	* 8man-demo.local (DC=8man-demo,DC=local)		
	Threshold (days): 90		
Detected scan problems			
No scan errors detected.			
Report for	8man-demo.local	Please take note that	
		The listed dates are the dates discovered during our scan.	
	Path 🔻	Last Logon Timestamp	 Days (Differenc - o current date)
SP_SearchService (8man-demo\SP_S	e CN=SP_SearchService,OU=Service Accounts,DC=8man-dem		1006
Eric Reid (8man-demo\EReid)	CN=Eric Reid,OU=TestUsers,DC=8man-demo,DC=local	10/10/2014 4:28:02 PM	859
	h CN=Mohammed Akbar,OU=TestUsers,DC=8man-demo,DC=I	10/27/2014 9:27:50 AM	843
Akbar, Mohammed (8man-demo\Mo		11/25/2014 3:31:09 PM	813
Akbar, Mohammed (8man-demo\Mo Quinton Patton (8man-demo\QPatto	n CN=Quinton Patton, OU=TestUsers, DC=8man-demo, DC=loca		
Akbar, Mohammed (8man-demo\Mo Quinton Patton (8man-demo\QPatto Adrian Stillwell (8man-demo\AStillw	e CN=Adrian Stillwell, OU=TestUsers, DC=8man-demo, DC=loca		630
Akbar, Mohammed (8man-demo\Mc Quinton Patton (8man-demo\QPatto Adrian Stillwell (8man-demo\AStillw Ali Mente (8man-demo\Ali Mente)	CN=Adrian Stillwell,OU=TestUsers,DC=8man-demo,DC=loca CN=Ali Mente,OU=TestUsers,DC=8man-demo,DC=local	6/24/2015 1:47:33 PM	603
Akbar, Mohammed (8man-demo\Mo Quinton Patton (8man-demo\QPatto Adrian Stillwell (8man-demo\AStillw	CN=Adrian Stillwell,OU=TestUsers,DC=8man-demo,DC=loca CN=Ali Mente,OU=TestUsers,DC=8man-demo,DC=local CN=Torrev Smith.OU=TestUsers.DC=8man-demo.DC=local		

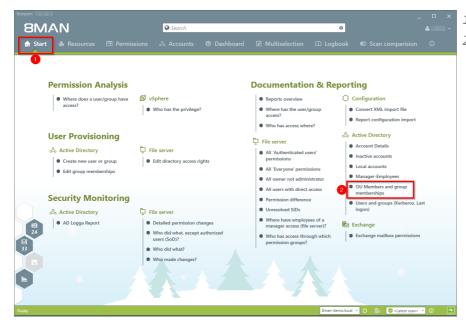
Review the data in the report. If using historical scan data there may be differences in the days since the last login.

8MAN

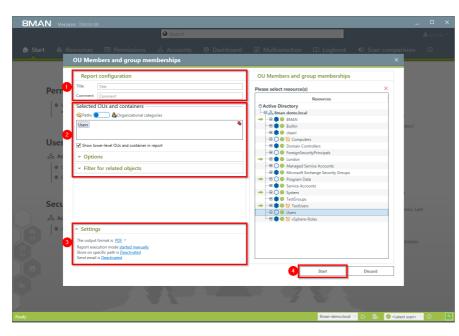
5.2.2.3 OU members und group memberships

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.



- 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

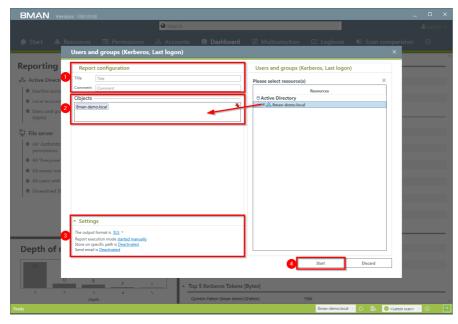
Groups

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

BMAN ♠ Start & Resources ⊡	Search	ts 🕜 Dashboard 🛛 🗹 Mult	¢ iselection □□ Logbook		
Reporting		Users and other accounts			
reporting		Users	429		
Active Directory		Users (Disabled)	6		
Inactive accounts		Administrators	12		
Local accounts		Administrators (Disabled)	0		
Users and groups (Kerberos, Last logon)	2	Groups			
	-	All Groups	183		
File server		Groups with members (w/o recursions)	104		
All 'Authenticated users' 23		Empty groups 🛕	76		
permissions		Groups in recursions 🛕	3		
All 'Everyone' permissions 34		The largest group (Domain Users (8man-demo)			
All owner not administrator 24		Built-in security groups	27		
		Global security groups	76		
All users with direct access 447		Universal security groups	35		
Unresolved SIDs		Local security groups	43		
		Global distribution groups	0		
		Universal distribution groups	2		
		Local distribution groups	0		
	^	OU / Contacts / More			
		Computers	4		
Depth of nested group	S	Computers (disabled)	0		
		Contacts	0		
71		Foreign users	0		
		Organizational Units	12		
1 2 3	2 1	Top 5 Kerberos Tokens [Bytes]			
Depth		Quinton Patton (8man-demo\QPatton)	1584		
ty			8man-demo.local	 O Eb C<latest scan=""></latest> 	~ ()

- 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.

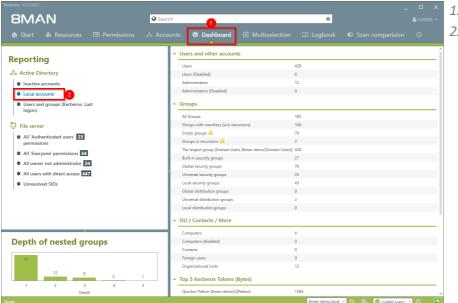
In From From Other Existing Refeath	Connections Properties Cdit Links	Sort Filter				anships	Group Ungroup Subtot	* Show Detail
Get External Data C	onnections	Sort & Filter		Data Tor	ols		Outline	6
🔹 👻 🗄 🗙 🗸 🌾 🛛 DisplayNan	ie							
	В	6	D			G	н	
Report of all users for	8man-demo local	C C	U	C	r	0	n	
report of all users for	ornan-denio.rocar							
DisplayName	 IsDisabled 	Account Expires	PWD don't expl	Last Logon	Last Logon Timestamp	Tv Y D	Direct Membershir - In	direct Membershir - Tota
Apolt, Peter roman-gemovineter Apolti	NO	Account never expires	TNO .	N/A	N/A	User	2	
adadmin (8man-demo\adadmin)	No	Account never expires	Yes	N/A	N/A	User	4	4
Adam French (8man-demo\AFrench)	No	Account never expires	No	N/A	N/A	User	2	1
Administrator (8man-demo\Administrator)	No	Account never expires	Yes	2/16/2017 1:02:41 PM	2/14/2017 11:40:29 AM	User	10	18
Administrator, Adam (8man-demo\Adam Administrat	or) No	Account never expires	No	N/A	N/A	User	3	2
Adrian Stillwell (8man-demo\AStillwell)	No	Account never expires	No	N/A	5/27/2015 3:06:13 PM	User	4	2
Agogbo, Charles (8man-demo\Charles Agogbo)	No	Account never expires	No	N/A	N/A	User	2	1
Aide Mann (8man-demo\Aide Mann)	Yes	Account never expires	No	N/A	N/A	User	2	1
Aido, Tom (8man-demo\Tom Aido)	No	Account never expires	No	N/A	N/A	User	2	1
Akbar, Mohammed (8man-demo\Mohammed Akbar)	No	Account never expires	No	N/A	10/27/2014 9:27:50 AM	User	2	1
Aldock, Don (8man-demo\Don Aldock)	No	Account never expires	No	N/A	N/A	User	2	1
Alex Boone (8man-demo\ABoone)	No	Account never expires	No	N/A	N/A	User	4	2
Alexandre Sourzac (8man-demo\ASourzac)	No	Account never expires	No	N/A	N/A	User	3	1
Ali Bye (8man-demo\Ali Bieh)	No	Account never expires	No	N/A	N/A	User	3	8
Ali Mente (8man-demo\Ali Mente)	No	Account never expires	No	5/29/2013 11:47:02 AM	6/24/2015 1:47:33 PM	User	3	4
Alvin Johnson (8man-demo\AJohnson)	No	Account never expires	No	N/A	N/A	User	2	1
Ammy Tiwana (8man-demo\ATiwana)	No	Account never expires	No	N/A	N/A	User	4	9
Anda, Lou (8man-demo\Lou Anda)	No	Account never expires	No	N/A	N/A	User	2	1
Andrew Susac (8man-demo\ASusac)	No	Account never expires	No	N/A	N/A	User	3	7
Angel Carreras (8man-demo\ACarreras)	No	Account never expires	No	N/A	N/A	User	4	9
Anick, Mike (8man-demo\Mike Anick)	No	Account never expires	No	N/A	N/A	User	2	1
Anny Time (8man-demo\ATime)	No	Account never expires	No	N/A	N/A	User	5	3
Anthony Davis (8man-demo\ADavis)	No	Account never expires	No	N/A	N/A	User	6	8
Aritan, Sam (8man-demo\Sam Aritan)	No	Account never expires	No	N/A	N/A	User	2	1
Ayshen, Don (8man-demo\Don Ayshen)	No	Account never expires	No	N/A	N/A	User	2	1
Baba, Ali (8man-demo\Ali Baba)	No	Account never expires	No	N/A	N/A	User	2	1
Back, Helen (8man-demo\Helen Back)	No	Account never expires	No	N/A	N/A	User	3	1
Baltelli, Luca (8man-demo\Luca Baltelli)	No	Account never expires	No	N/A	N/A	User	2	1
Banks, Robin (8man-demo\Robin Banks)	No	Account never expires	No	N/A	N/A	User	2	1
Barrie Kenyon (8man-demo\BKenyon)	No	Account never expires	No	N/A	N/A	User	2	1
Barrow, Will (8man-demo\Will Barrow)	No	Account never expires	No	N/A	N/A	User	2	1
Bart Postema (8man-demo\BPostema)	No	Account never expires	No	N/A	N/A	User	7	1
Bath, Burt (8man-demo\Burt Bath)	No	Account never expires	No	N/A	N/A	User	2	1
Configuration 8man-demo.local	Heere Rmon.do	mo.local Groups	(+)				•	
eman-demo.local	vsers sman-de	monocar_oroups	T	: •				

Open the report in Excel and apply the desired filters.

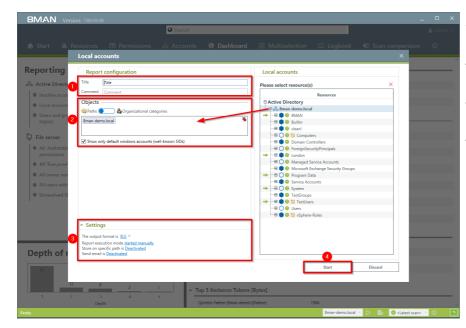
5.2.2.5 Identify local accounts

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.



- 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.

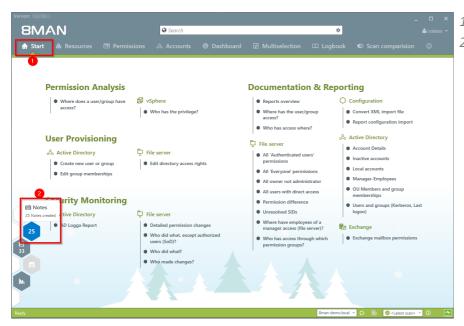
Step by step process



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

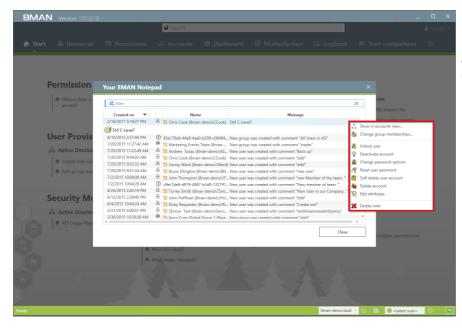


- 1. Add a comment.
- 2. Click on "Add".



8MAN

- 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

Version:	_					
8MAN	<u> </u>	Search		\$		
🏦 Start & Re	esources 🖃 Permissions 🖧 A				🛛 Scan comparision 🛛 🛈	
Resources			🗢 🙆 C-Level (8m	nan-demo\C-Level)		
Resources filter first level		3]		1	Report -
	full path De	scription Access rights Folder Siz	e Children			
Active Directory File server			 Tree Attributes 			
SharePoint						Edit
Exchange			Name	Value		
vSphere			Common Name	C-Level CN=C-Level,OU=TestGroups,DC=8		
Purpose Groups 2			Distinguished Na Group Type	Global group	-	
🎥 Management	C-Level (8man-demo\C-Lev This grou		Name (RDN)	C-Level		
A Parking	Report: Where has the user/group access?	o park	Object GUID	dc47cd7d-a3bc-4a31-9776-c83b53		
i 🐣 training	Report: Account Details		Object SID	S-1-5-21-1178734647-297574235-		
	Show in accounts view		SAM Account Na			
	Edit attributes			e (268435456) Group Object		
	👝 🍇 Delete Purpose Group		LDAP ADsPath	LDAP://8man-demo.local/CN=C-Le		
	3 a Modify Purpose Group					
			>			
	🔯 Add note					
	Øpen Logbook					
			1			
			1			
	^					
				8man-demo.local ~	🔅 🖶 🥝 <latest scan=""> 👻 🕕</latest>	-

- 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

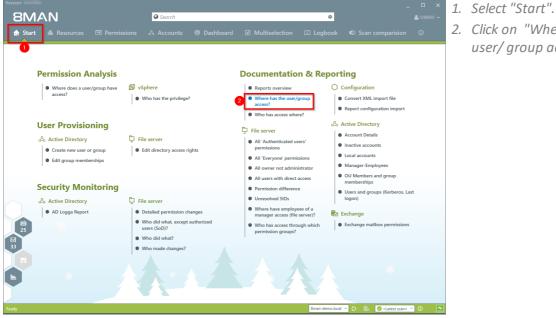
5.3.1 **Management reports**

Where do users and groups have access? 5.3.1.1

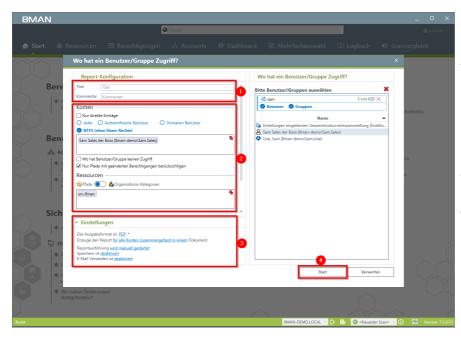
Background / Value

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



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



- 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

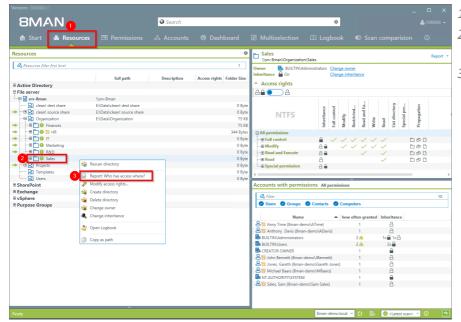
Data owners and managers know who should have access to which resources. Full transparency is very important especially for directories containing sensitive information. The report "Who has access to what?" gives you a full overview of all access rights (for example "read only" and "write") including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

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

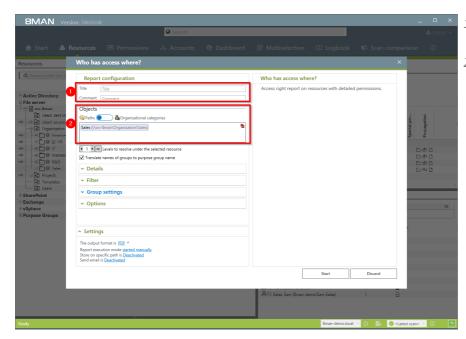
- Who should have access to what? (Increase in data security)
- Which access rights should exist? (improvement of data integrity)

Additional Services

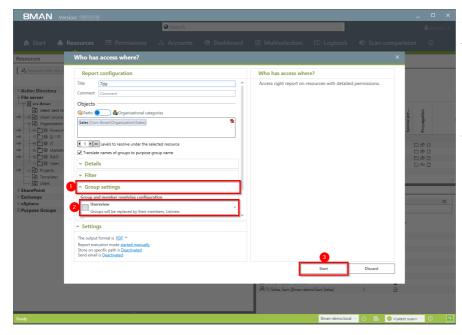
Changing directory access rights



- 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.



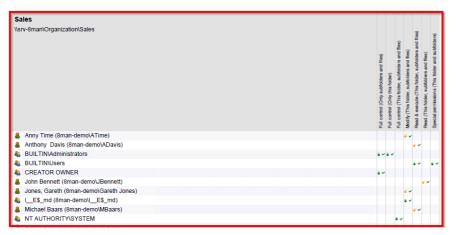
8MAN

- 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 Comment Used time zone	8MAN Report: Who has access where? - 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)

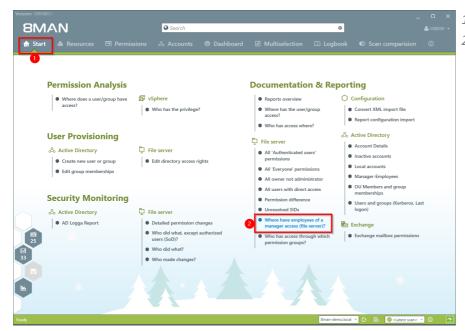


5.3.1.3 Where do employees of a manager have access to?

Background / Value

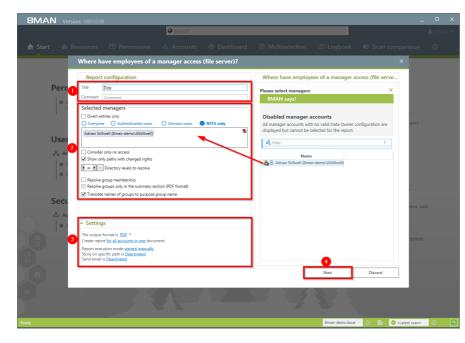
8MAN includes a special data owner report for file servers. This allows you to connect Active Directory users with the attribute "Manager" to specific resources on file servers.

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

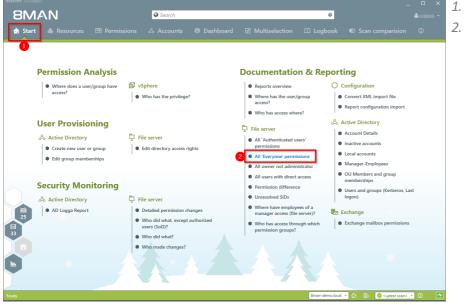
5.3.2.1 Identify usage of "everyone"

Background / Value

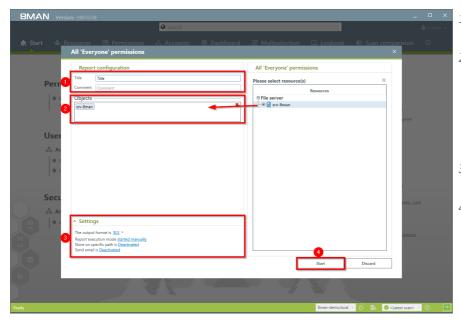
If the "Everyone" account is used for the assignment of access rights, (almost) everyone has access to the connected resources. The consequence is an excessive assignment of access rights and a high probability for unauthorized access. 8MAN displays all access rights for the "Everyone" account. These 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 <u>Authenticated Users</u>. <u>Identify globally accessible directories</u> (web client) <u>Remove "everyone" permissions in bulk</u> (web client)



- 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.

Copy *	Λ΄ Α΄ Ξ Ξ 🚽 ≫·· 📑 Wrap Te		Gene		٣	R	P	-	Delete Forma	∑ AutoSum ↓ Fill +	Sort & Fi	H
* Format Painter B I U - 🖽 - 🖄 -	🔺 - 📰 🕾 🐨 🔁 Merge 8	2 Center	- 5-	% *	58 4 9	Conditional Fe Formatting *		s* *	v v	t 🍭 Clear 🕶	Filter * Se	
Clipboard 12 Font	rs Alignment		6	Number	G	St	rles		Cells	E	Editing	
\bullet : $\times \checkmark f_X$												
А	в	С	D	E	F	G	H	1.1	J	K L	M	N
leport for	Organization (\\srv-8man\Organization)											
Path	Right	Deny										
srv-8man\Organization\R&D	Read & execute Read & execute											
srv-8man\Organization\R&D\Berlin Office srv-8man\Organization\R&D\Coding	Read & execute Read & execute											
srv-8man/Organization/R&D/Coding/Source Code												
 Configuration Organization (s 	rv-8man Org #2 🛞					E 4						

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



5.3.2.2 Who has access through which permission groups?

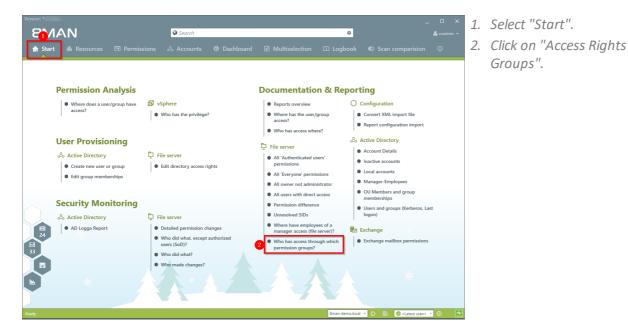
Background / Value

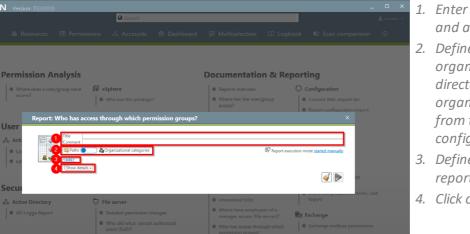
The report "Who has access through which permission groups?" shows the groups that give access to the selected resource and the users that are members of said groups.

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

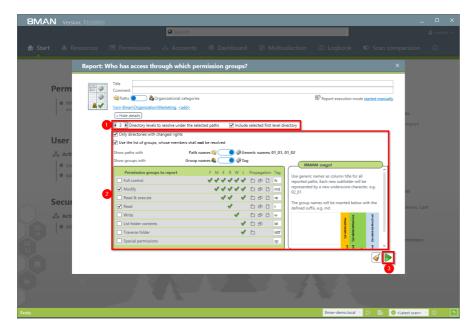
Step by step process

8MAN





- 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.

ast	La Copy -	$\begin{array}{c c} bhi & \mathbf{v} & 11 & \mathbf{v} & \mathbf{A}^* & \mathbf{A}^* & \equiv \\ I & \underline{\mathbf{U}} & \mathbf{v} & \underline{\mathbf{W}} & \mathbf{v} & \underline{\mathbf{A}}^* & \mathbf{v} & \equiv \\ \end{array}$	-	♥ + ■ Wrap Text E +E ■ Merge & Cer	iter	General		* 50 i	* 00	Conditiona Formatting			Cel		Delete Fo	orma v	The provided HTML Notice Prov	~	9		Find & Select *	
	Clipboard %	Font G		Alignment		G 1	Vurr	iber	5		51	tyles			Cells				Editin	ıg		
13		√ f _* CCook		-														_		-		
	A	B	С	D	E	F	G	н	1	J	K	L	М	N	0	Ρ	Q	R	S	T	U N	V
		nal category: Not configured		-																		
	itle			Demo																		
	luthor			8MAN-DEMO\cradmin																		
	Date			2/20/2017 10:2	9																	
ç	Comment																					
				01 01														-	01 02		02 01	
			md			01_01_01 md		01_01_02 md		01_01_03 md		01_01_04 md			01_01_06 md	r i	01_01_07	r r		r mo		r
	dam Administrator	Administrator, Adam (Adam Admin				X		X	1	x		x			x				na	r me		4
	Boone	Alex Boone (ABoone)	istrat	x		x		X		x		x			x	,						
				X		x		x		X	1	x		x	x		x					
	Time Davis	Anny Time (ATime)		x		x	x			x	x		x		x	x		x				
		Anthony Davis (ADavis)		x		X		x		x					x			× >		x	_	÷
	Cook Reid	Chris Cook (CCook) Eric Reid (EReid)		x		x		X		x		x x			x	,		-	`	×		
	rank Gore	Gore, Frank (Frank Gore)		x		X		x	-	x		x			x		x	-	-		_	÷
	Ward	Jimmy Ward (JWard)		x		x		x		x		x			x	5						
		John Bennett (JBennett)		x		x		X		x		x			x	,						
	Bennett Thompson	John Bennett (JBennett) John Thompson (JThompson)		x		x		x		x		x			x							
	areth Jones	Jones, Gareth (Gareth Jones)		x		x		x		x		x			x	5				x		x
	areth Jones Imanda Lynn	Lynn, Amanda (Amanda Lynn)		x	x		x				x		x		x	x		x			- '	×
	Ananda Lynn Aarv Chen			x		x		X		x		x	×		x			^ >	,	x		
	/lary Chen //Baars	Mary Chen Michael Baars (MBaars)		x		x		x			x				x			-'	·	×		
	/Baars /atrick.Willis	Patrick Willis (Patrick.Willis)		x		x x		x x		x x		x x			x x	,						
	Patrick. Willis	Quinton Patton (QPatton)		x	x		x				x		x		x	x		x				
	Patton	Robert Patrick (RPatrick)		x	×	x		x	^	x		x	^		x			^				
	Smith	Torrey Smith (TSmith)		x		x		x		x		x			x	5						
ì	30000	roney amon (ramith)		^		^		^		^	ť	^			^	H	^					
		1 \\srv-8man\Organization																				
_	1 01	\\srv-8man\Organization \\srv-8man\Organization\Finances																				
	1 01 01	\\srv-8man\Organization\Finances	0.000	unte Davable																		
		ort_2017022010293085d3e (+)	MCCO	unts rayable						: •												

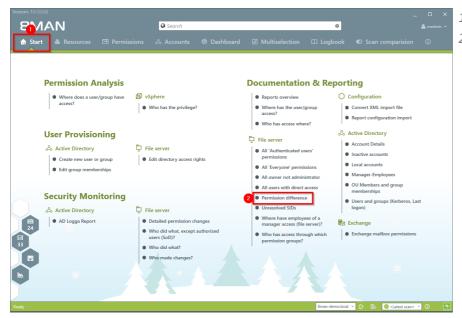
The report contains a list of all user accounts and file server paths, as well as the corresponding access rights groups.



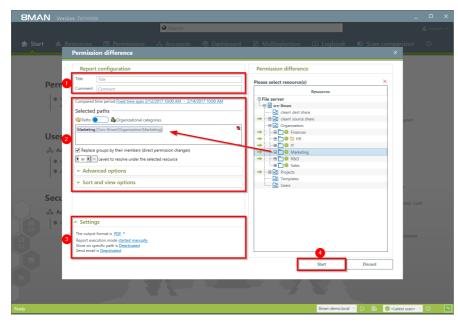
5.3.2.3 Permission differences

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.



- 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

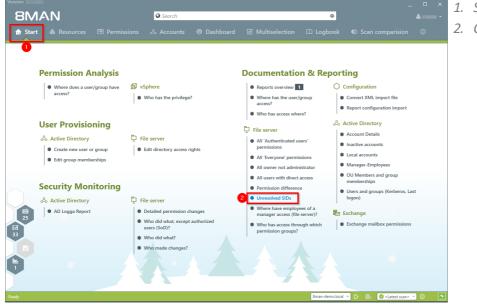
SIDs (Security Identifiers) are character strings that are used to identify user and group accounts in
Active Directory. SIDs become unresolved when users or groups with direct access rights are deleted in
AD. By using unresolved SIDs insider threats can gain access to sensitive resources.
8MAN clearly identifies unresolved SIDs in your system.

Additional Services

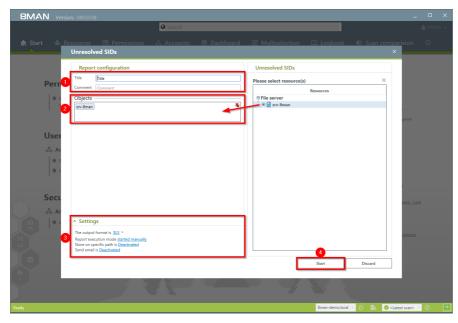
Identify and delete unresolved SIDs (rich client) Remove unresolved SIDs in bulk (web client)

Step by step process

8MAN



- 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.

		* ▲* = = ₩ ₩rap Text ▲ • = = = € € € ₩ Marge & Center •	General		E Conditional F	format as Cell	Insert De	elete Format	AutoSum	Sort & Find & Filter * Select *
Clipboard G Fon		G Alignment G	Number	6				ells		Filter * Select *
		Organization\Marketing\Events	Humber			cyic 2			Lu	ining
		C	D	E	F	G	н і	J	К	L M
eport for	srv-8man		-			· ·			IX.	C 101
ath		Unresolved SID								
		Unresolved SID S-1-5-21-1178734647-297574235-3966573622-20	71							
	- ,moony	20101010101010100000000000000000000000								
ath report about unresolved owner SID										
Il accounts have been resolved										
accounts have been resolved										
 Configuration srv-8m 	ian 🤆	÷			4					

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.

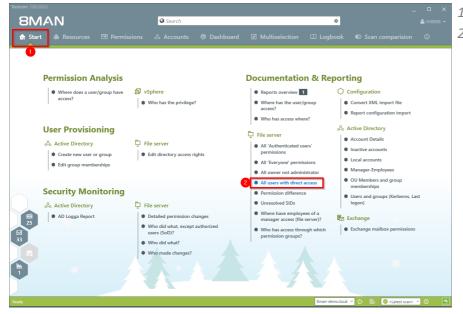
8MAN strictly adheres to Microsoft Best Practice and assigns a group for every access right.

Additional Services

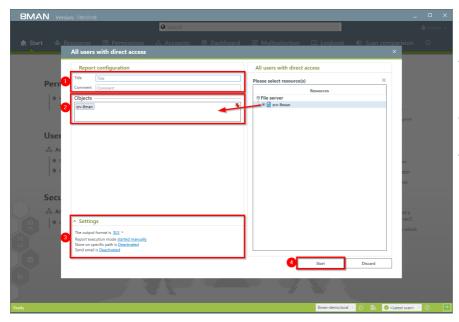
<u>Remove direct permissions</u> (rich client) <u>Remove direct permissions in bulk</u> (web client)

Step by step process

8MAN



- 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.

V Format Painter	Wrap Text General Merge & Center	Formatting	 Tabl 		×	Delete Format	∑ AutoS ↓ Fill × Clear</th <th>Sort & Find & Filter * Select *</th> <th></th>	Sort & Find & Filter * Select *	
Clipboard & Font & Aligni	nent G Number	6	Styles			Cells		Editing	
	В	с	D	E	F	G	н		ł
Report for	Organization (\\srv-8man\Organization)	C C	U	C	r	6	n	I J	
cepoir ior	Organization (Nsiv-ornamOrganization)								
Path	user name	Right	Deny						
srv-8man\Organization	cradmin (8man-demo\cradmin)	Full control	Deny						
\srv-8man\Organization\Finances	Chris Cook (8man-demo\CCook)	Modify							
siv-omanorganization/Finances/ srv-8man/Organization/Finances/Accounts Payable	Chris Cook (8man-demo/CCook)	Modify							
siv-oman(organization) mances/Accounts Payable \srv-8man(Organization)Finances/Accounts Payable/Accounts Open	Chris Cook (8man-demo/CCook)	Modify							
srv-8man\Organization\Finances\Accounts Payable\Accounts Open	cradmin (8man-demo\cradmin)	Full control							
srv-8manlOrganization/Finances/Accounts Payable/Accounts Paid	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\Accounts Payable\Accounts Paid\New folder	Chris Cook (8man-demo\CCook)	Modify							
srv-8man\Organization\Finances\Accounts Payable\Accounts Paid\New folder	cradmin (8man-demo\cradmin)	Full control							
srv-smanlOrganization/Finances/Accounts receivable	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\Expenses	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\Expenses\Expenses Project	Chris Cook (8man-demo\CCook)	Modify							
srv-sman(Organization) Finances Lopenses Lopenses 1 Toject	Ali Mente (8man-demo/Ali Mente)	Read & execute							
\srv-8man\Organization\Finances\Home	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\New Project directory	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\Offices	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\Offices\Berlin HQ	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\Offices\London	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\Salaries	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\Salaries\Berlin	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Finances\Salaries\München	Chris Cook (8man-demo\CCook)	Modify							
\srv-8man\Organization\Marketing\Events\The Art of Security\2011	cradmin (8man-demo\cradmin)	Full control							
\srv-8man\Organization\Marketing\Events\The Art of Security\2012	cradmin (8man-demo\cradmin)	Full control							
\srv-8man\Organization\Marketing\Events\The Art of Security\2013	cradmin (8man-demo\cradmin)	Full control							
,									
Configuration Organization (srv-8man Org #2		4							

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

5.3.2.6 Identify directories whose owners are not administrators

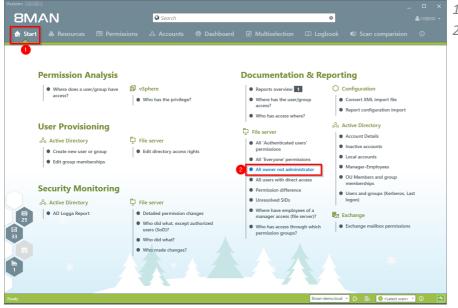
Background / Value

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

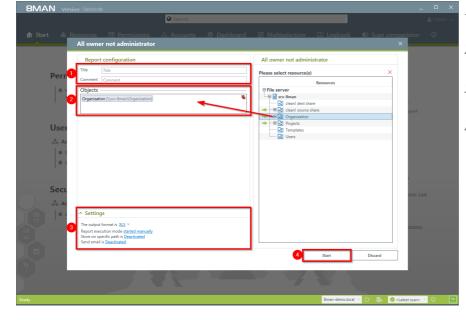
Step by step process



Select "Start". 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.





$\begin{array}{c c c c c c c c c c c c c c c c c c c $	Wrap Text General Merge & Center Number Number	* Co *** For	nditional Fo matting + T Styl	able * Styles *		Delete Form	Clear *	Sort & Find Filter * Sele	
▼ : × ✓ & Path									
A	В	с	D	E	F	G	н	J	к
Report for	Organization (\\srv-8man\Organization)								
Path	Owners not Administrators								
srv-8man\Organization	cradmin (8man-demo\cradmin)								
srv-8man\Organization\Finances	Finance (8man-demo/Finance)								
srv-8man\Organization\Finances\Accounts Payable\Accounts Open	cradmin (8man-demo\cradmin)								
Isrv-8man\Organization\Finances\Accounts Payable\Accounts Paid\New folder Isrv-8man\Organization\Marketing\Events\The Art of Security\2011	cradmin (8man-demo\cradmin) cradmin (8man-demo\cradmin)								
siv-omaniOrganization/Warketing/Events/The Art of Security/2011	cradmin (8man-demo/cradmin)								
srv-8man\Organization\Marketing\Events\The Art of Security\2013	cradmin (8man-demo/cradmin)								
· · · · · ·									
Configuration Organization (srv-8man Org #2			-						

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

5.3.2.7 Identify usage of "Authenticated Users"

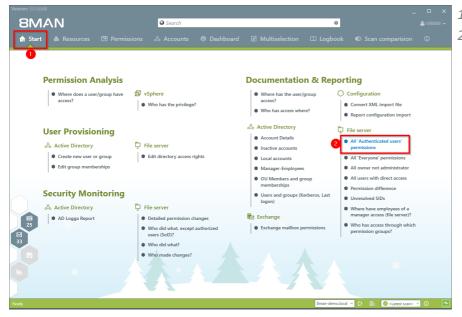
Background / Value

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

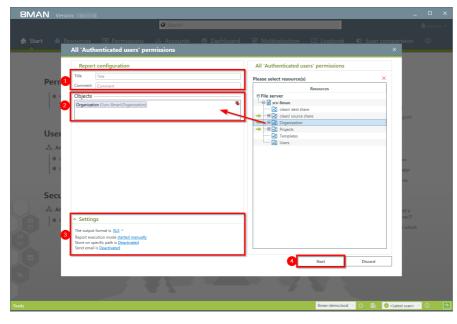
Additional Services

<u>Identify usage of "everyone"</u> <u>Identify globally accessible directories</u> (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: <u>Who has access to what?</u> Report: <u>Identifying Mailbox access rights</u>



5.4.1 Management Reports

5.4.1.1 Who has access to what?

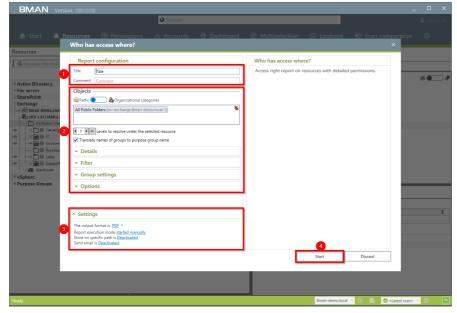
Background / Value

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.

SMAN Search
Resources Image: Constraint of the local state of the local
A Resources filter first level 2 Access rights Access rights B Active Directory Bille sarver
Access rights Access rights 81 Active Directory Bill path Description Access rights Folder Size A Access rights B Acces
full path Description Access rights Folder Size
© Active Directory EFIe server
B File server T Scharabolist
E ShareBoint
응 SharePoint 문 방송 등 2019 % 20
™⊕⊗ 8man-demo.com 2 ₹ ₹ 2
SRV-EXCHANGE.8man-demo.local
- H I I Copy as path 6
→ + ⊕ 🗑 ♥ Marketing 1 ♥ @marketing 1 ₪ @marketing 1 ♥ @marketing 1 ₪ @marketing
······································
"™Z Z MANDONS' D MAND
a vapnere B Purpose Groups
Accounts with permissions
Users/groups with access right All permissions
Q Filter 2
🕲 Users 🕲 Groups 🕲 Contacts 🕲 Computers
Name 🔺 🗰
Anonymous (Exchange\Anonymous) 1
Default (Exchange\Default) 1
Ready 8man-demolocal 🗸 🗘 🖶 🙋 clatest scanz 👻 🛈

- 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

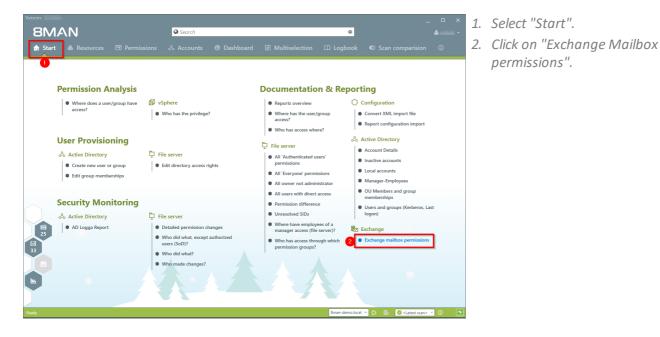
8MAN generates a variety of reports that shows Mailbox access rights. These include:

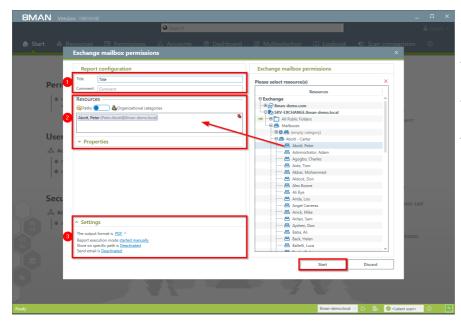
- Mailbox directories and their access rights
- Properties (Mailbox size)
- Deputies for Mailboxes
- Out of Office notices

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?".





- 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: <u>Where do users and groups have access?</u>

5.5.1 Management Reports

5.5.1.1 Who has access where?

Background / Value

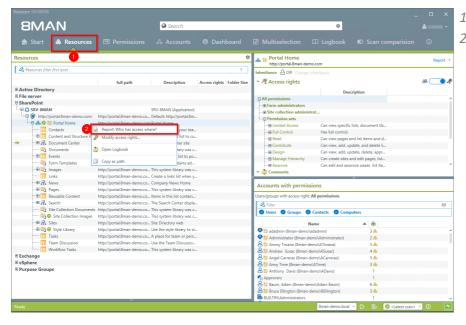
Managers and team leads know best who should have access to what. Having an understanding of your access rights situation is extremely important, especially for sensitive SharePoint resources. The report "Who has access to what?" provides an overview of all users and their access to SharePoint.

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)

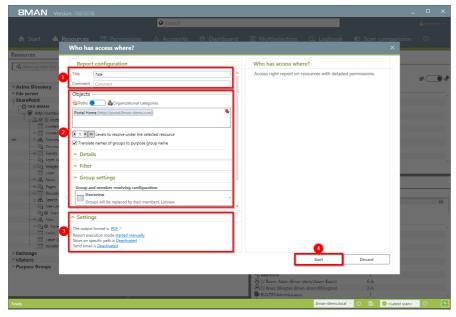
Additional Services

Managing access rights to SharePoint resources



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





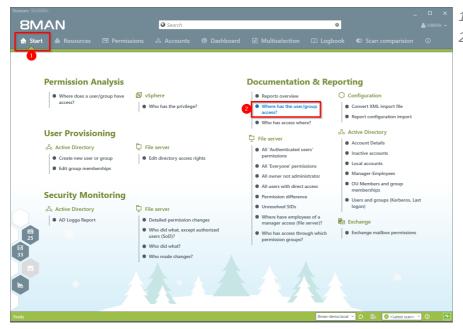
- 1. Enter a title for the report and add a comment.
- 2. Define the range of the report. In order to reduce complexity, we recommend selecting "usersview" in the "Group settings" area. All other settings are targeted at expert users.
- 3. Define the desired report settings.
- 4. Start the report.

5.5.1.2 Where do users and groups have access?

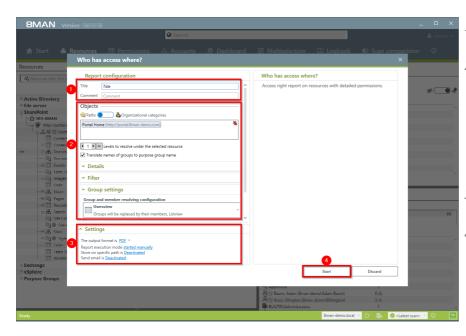
Background / Value

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".
- 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 tracable 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

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.

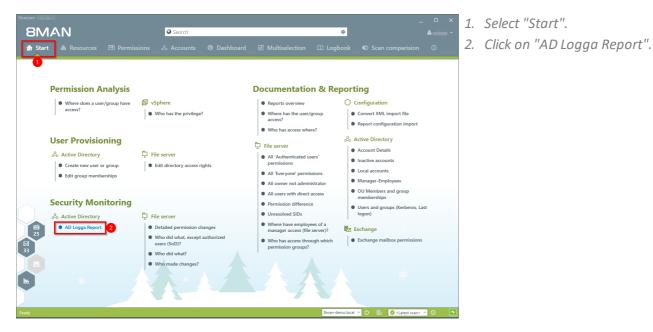
Additional services

Analyze AD Logga events with the logbook Set alerts for groups Set alerts for user accounts

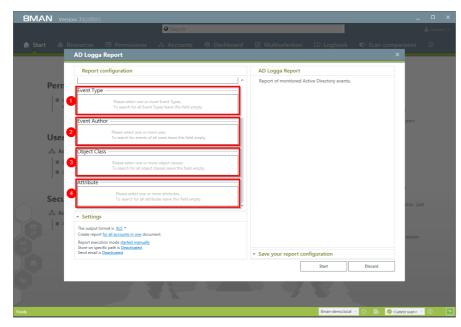
Monitoring of event authors

- Users
- Groups
- Computers





- 8MAN AD Logga Repor AD Logga Report Please select resource(s Per Re Active Direct Use Event Author Object Class Settings The output format is XLS ~ Create report for all account Report execution mode started a Store on specific path is <u>Deactive</u> Send email is <u>Deactive</u> Save your report configuration Start Discard 8man-demo.local ~ 🛞 🛃 🥝 <Latest scan> ~ (
- 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.

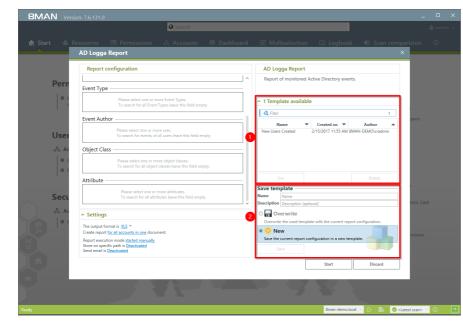


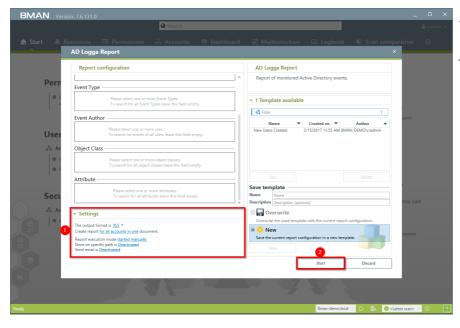
Define the range of the report by setting filters. By definition filters exclude the selected data.

- 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.

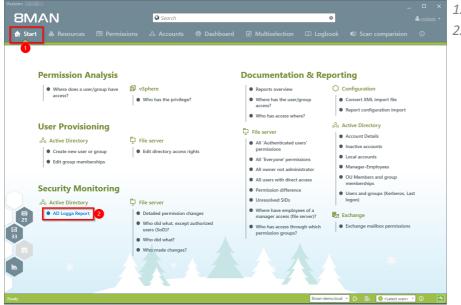
6.1.1.2 Identify temporary group memberships

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.

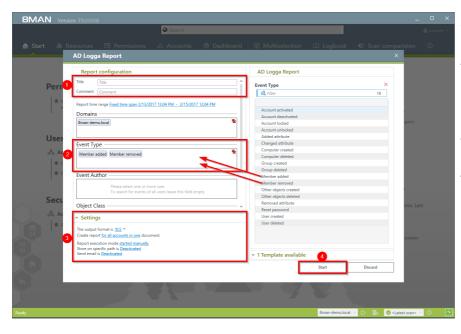
Additional Services

Analyze AD Logga events with the logbook Set alerts for groups Set alerts for user accounts



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





- 1. Enter a title for the report and add a comment.
- 2. Define the range of the report. For the event type select "member added" and "member removed".
- 3. Define the desired report settings.
- 4. Start the report.

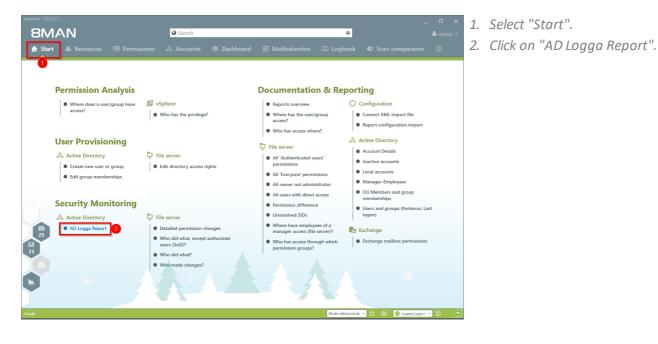
6.1.1.3 Identify locked user accounts

Background / Value

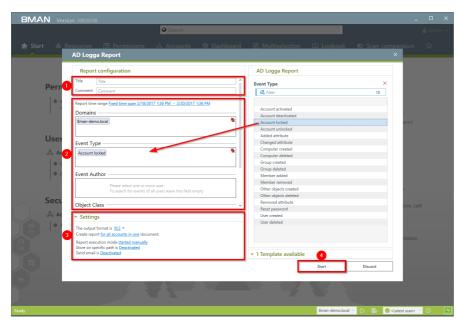
In the best case scenario, an attempted login with someone elses account ends with a locked user account. The AD Logga shows you from which computer the attack occurred.

Additional services

Analyze AD Logga events with the logbook Set alerts for groups Set alerts for user accounts







- 1. Enter a title for the report and add a comment.
- Define the range of the report.
 For the event type select "Account locked"
- 2. Define the desired report settings.
- *3. Start the report.*

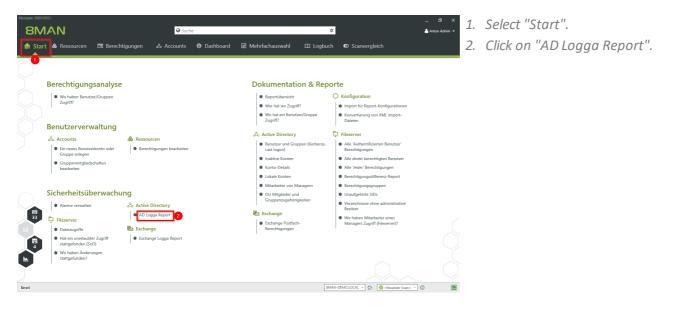
6.1.1.4 Monitor password resets

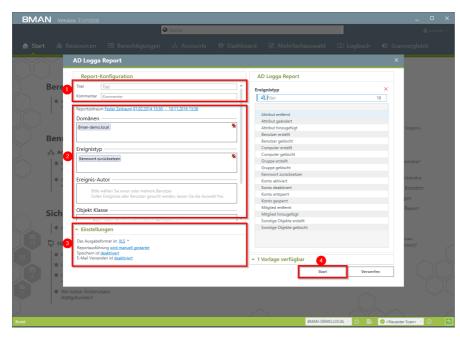
Background / Value

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





- 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.

ıtei Start Einfügen Seitenlayout Formeln Daten Ü	berprüfen Ansicht 🛛 Was möchten Sie tun?		Jörg Bran	dt 🛛 🖓 Freigeb
89 * : × ✓ fx				
AB	С	D	E	F
Zeit Autor	Objekt	Objektklasse	Ereignis	Attribut Name
26.02.2014 16:56 cradmin (8man-demo\cradmin)	Bino, Al (8man-demo\Al.Bino)	User(user)	Kennwort zurücksetzen	
28.02.2014 15:40:35 cradmin (8man-demo\cradmin)	Zifer, Lou (8man-demo\Lou.Zifer)	User(user)	Kennwort zurücksetzen	
11.03.2014 09:15:01 Administrator (8man-demo\Administrator)	Zifer, Lou (8man-demo\Lou.Zifer)	User(user)	Kennwort zurücksetzen	
13.03.2014 14:50:42 Administrator (8man-demo\Administrator)	Zifer, Lou (8man-demo\Lou.Zifer)	User(user)	Kennwort zurücksetzen	
10.03.2015 11:49:04 neadmin (8man-demo\neadmin)	Borg, Inge (8man-demoVinge.Borg)	User(user)	Kennwort zurücksetzen	
10.03.2015 12:31:32 neadmin (8man-demo\neadmin)	Borg, Inge (8man-demo\Inge.Borg)	User(user)	Kennwort zurücksetzen	
10.03.2015 15:12:28 Administrator (8man-demo\Administrator)	Krise, Christiane (8man-demo\Christiane.Krise)	User(user)	Kennwort zurücksetzen	
10.03.2015 15:47:05 Administrator (8man-demo\Administrator)	Ander, Ole (8man-demo\Ole Ander)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Aber, Mark (8man-demo\Mark Aber)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Alien, Arnold (8man-demo\Arnold Alien)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Aloe, Vera (8man-demo\Vera Aloe)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Ander, Ole (8man-demo\Ole Ander)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Ander, Cori (8man-demo\Cori Ander)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Aner, Dominik (8man-demo\Dominik Aner)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Angebrandt, Angie (8man-demo\Angie Angebrandt)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Apfel, Adam (8man-demo\Adam Apfel)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Arbeit, Andi (8man-demo\Andi Arbeit)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Arm, Armin (8man-demo\Armin Arm)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Aroni, Mark (8man-demo\Mark Aroni)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Asil, Claire (8man-demo\Claire Asil)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Auer, Karl (8man-demo\Karl Auer)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Auhss, Ann (8man-demo\Ann Auhss)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Autsch, Anke (8man-demo\Anke Autsch)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Azubi, Andy (8man-demo\Andy Azubi)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Baba, Ali (8man-demo\Ali Baba)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Bach, Klara (8man-demo\Klara Bach)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Baer, Johannes (8man-demo/Johannes Baer)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Baer, Roy (8man-demo\Roy Baer)	User(user)	Kennwort zurücksetzen	
0.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Baern, Al (8man-demo\Al Baern)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Balken, Don R. (8man-demo\Don R. Balken)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo\neadmin)	Becher, Joe Kurt (8man-demo/Joe Kurt Becher)	User(user)	Kennwort zurücksetzen	
10.03.2015 16:50:09 neadmin (8man-demo)neadmin)	Beiter, Walter (8man-demo\Walter Beiter)	User(user)	Kennwort zurücksetzen	
Konfiguration	(+)			

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

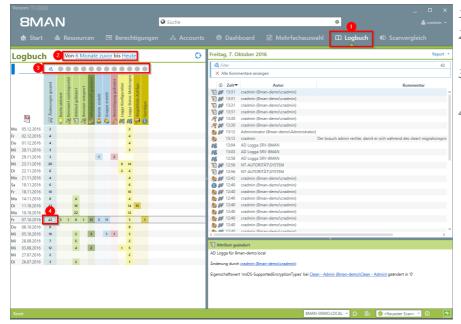
6.1.1.5 Analyze AD Logga events with the logbook

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



- 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.

	sion: 7 8M	A	N	9	Suche ¢
					ふ Accounts ® Dashboard 🗹 Mehrfachauswahl 🎞 Logbuch 🔍 Scanvergleich
Lc	gbuc	n	Von <u>6 Monate a</u>	<u>uvor</u> bis <u>Heute</u>	C Freitag, 7. Oktober 2016 Report
		٩			A filter 13 von 4 X Alle Kommentare anzeigen
-		🕅 Änderungen gesamt	 Konto aktiviert Kennwort zurückgesetzt Attribut geändert Benutzer entsperitt Konto essient 	Gruppe Berech Logga Logga Abgele Sonstig	Commentar Kommentar Kommentar Kommentar Kommentar Soft 2 Administrate/O Rem-demo/Administrate/O Soft 2 Administrate/O Rem-demo/Administrate/O Rem-demo/Administ
Mo	05.12.2016	2		2	Iz40 cradmin (8man-demo\cradmin) Iz40 cradmin (8man-demo\cradmin)
r	02.12.2016	4		4	S M 12:40 cradmin (smar-demo)cradmin)
	01.12.2016	4		4	San Martin (Sman-demo\cradmin)
Mi	30.11.2016	3		3	🎭 💋 12:40 cradmin (8man-demo\cradmin)
Di	29.11.2016	3 20	1	2 6 14	S and the second
Mi Di	23.11.2016 22.11.2016	20		2 4	aradmin (8man-demo\cradmin)
	21.11.2016	4		4	🎭 💋 12:40 cradmin (8man-demo\cradmin)
Sa	19.11.2016	6		6	
Fr	18.11.2016	10		10	<
Mo	14.11.2016	8	4	4	😂 Gruppenmitgliedschaft geändert
Di	11.10.2016	43	16	14 13	AD Logga für 8man-demo.local
Mo	10.10.2016	34	22	12	
Fr	07.10.2016	42	3 1 6 1 13 3	11 3 1	Änderung durch Administrator (8man-demo\Administrator):
	06.10.2016	8		8	Gruppenmitglied 'Clean - Admin (8man-demo\Clean - Admin)' in 'Domänen-Admins' hinzugefügt.
	05.10.2016	10	2 3	1 1 3	
	28.09.2016	7	5 4 2	2	
Mi Mi	03.08.2016 27.07.2016	12	a 2	2	
Di	26.07.2016	3	2	2	
Ben	ait				Berech ein- box, auslappen

- 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.

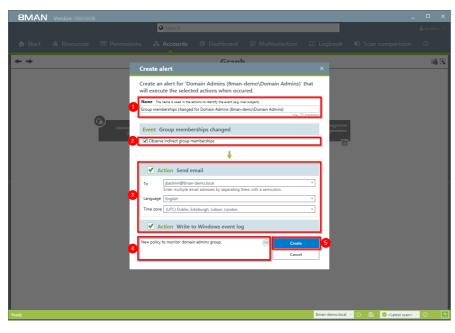
Additional services

Set alerts for user accounts Manage alerts



- 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.





- 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.

8MAN Version:								
		Search						
🏠 Start & Resources								
+ +			Graph	1			a a	18
	Cre	ate alert			×			
	viil Acc 2 Ev 5 3 La	execute the select: The The rame is used in the select: The The rame is used in the select: The The rame is used in the select s	ed actions when occu ktions to identify the event (e.g. m Bman-demolybadmin) ed the mail	nas, 7	that			
Ready	4 Der		to Windows event log	Create Cancel		C B (station)	9 0	4

- 1. Enter a title for the alert.
- 1. Select an event for which you want to receive the alert.
- 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

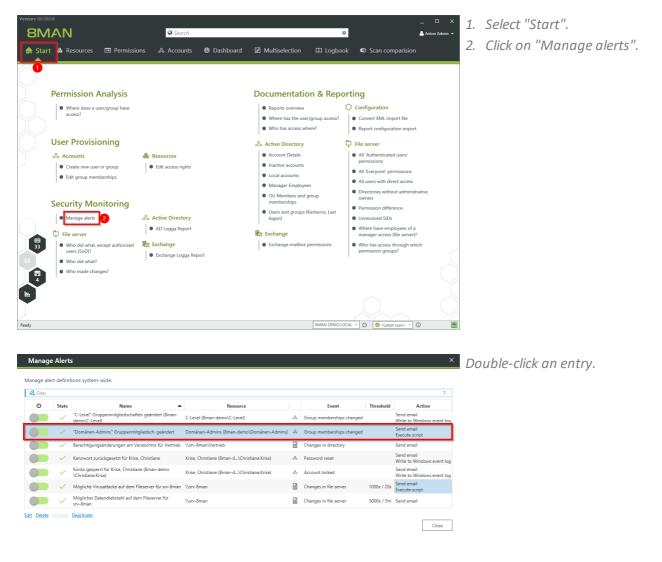
Background / Value

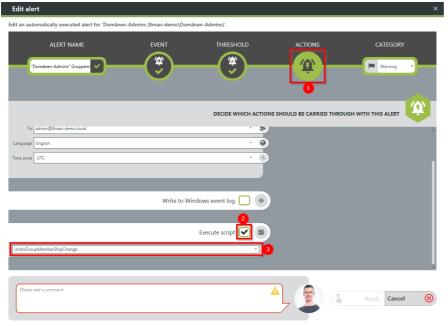
Run a script after the FS Logga or AD Logga has triggered an alert. For example, you monitor a securitycritical group for membership changes and the script automatically resets memberships back to default.

Additional Services

Manage alerts

Step by step process





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

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

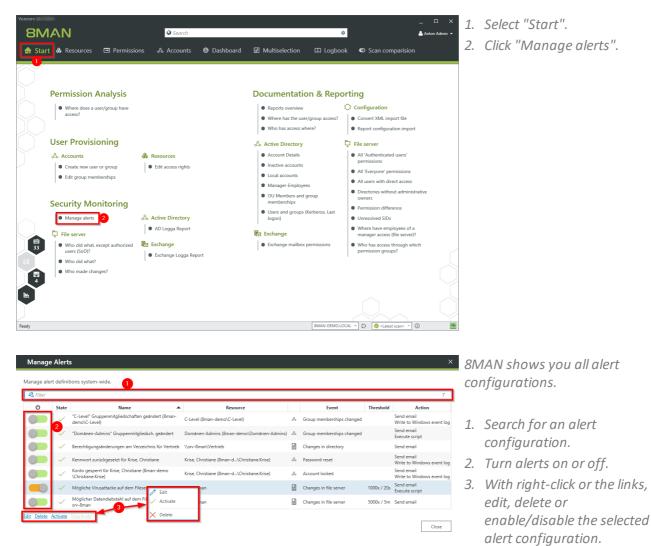
180 Access Rights Management

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



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 date including the involved actors.
- The executive department can be certain: The FS Logga provides all necessary data for more security and process improvement and makes security related incidents completely transparent.

6.2.1.1 Monitor access to sensitive data

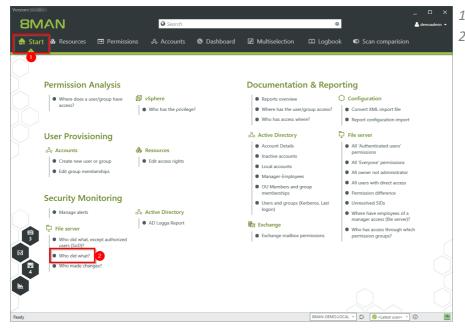
Background / Value

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.

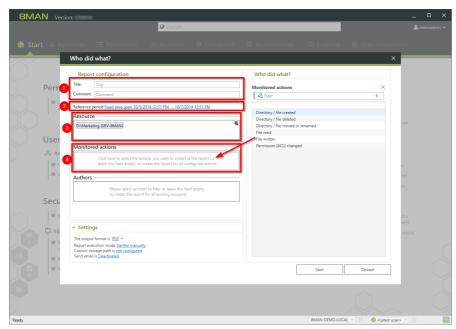
Additional services

Change directory access rights

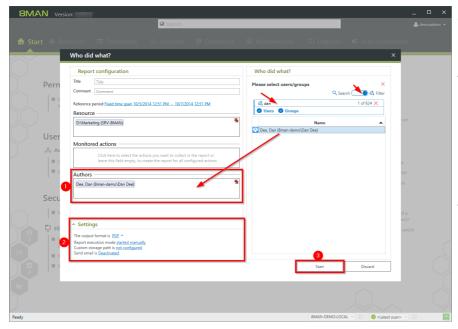
Step by step process



- 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.

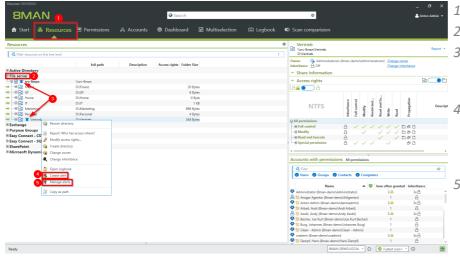
6.2.1.2 Enable alerts for file server directories

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.

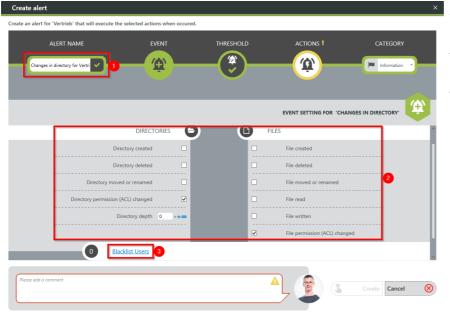
Additional Services

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



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





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

Blacklist Users

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

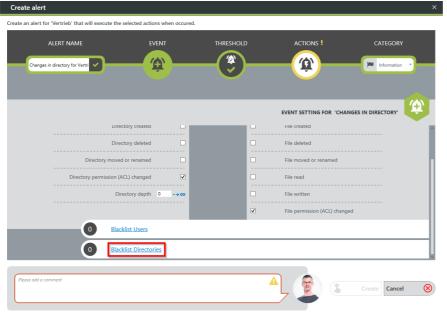
AVAILABLE USERS		THESE USERS WILL NOT BE CONS	1
Q @ A Sam Sales (8man-demo∖Sam.Sales)	× • \$	4 Filter	1
Name		Nam Sales (8man-demo\Sam.Sales)	3
	-		

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 dragand-drop to add users to the blacklist.
- 3. Use the "Del" key to remove users from the blacklist.
- 4. Click "Apply" to save the changes.



Optional:
 Select "Blacklist Directories".

Blacklist Directories

8MAN

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

AVAILABLE DIRECTORIES BELOW 'VERTRIEB'	THESE DIRECTOR	RIES WILL NOT BE CONSIDERE	
↓ Filter	🖉 Filter		1
e Hersteller	\\srv-8man\Vert	rieb\Projekte 3	4 🗉
 6 Kunden 6 öffentlicher ag 			
🕀 🛄 🚱 Projekte	2		
	→		
			5
			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.
- 2. Use double-click or dragand-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 'Vertri	eb' that will execute the se	elected actions when occure	d.		
ALERT Changes in directo	NAME	EVENT	THRESHOLD		CATEGORY
				NS SHOULD BE CARRIED THE	ROUGH WITH THIS ALERT
To admin@8man-c Language English Time zone (UTC +01:00) Ar	iemo.local nsterdam, Berlin, Bern, Rom, Str	sckholm, Wien	Send email 🖉 🖉 	2	
		Write to Wir	ndows event log ✔ 🐠 Execute script ✔ 🖪]3]0	
Please add a comment					Create Cancel 🛞

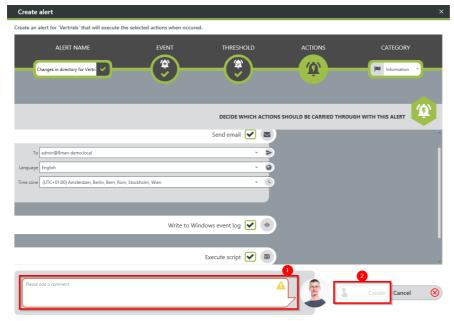
- 1. Choose Actions. Here you specify which actions are executed when an alert is triggered. You must activate at least one action (arrows).
- 2. Activate the option if an email should be sent in case of an alert. The content of the emails can be customized. This is analogous to the recertification emails.
- 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.

× Choose a category.

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

Create an alert for 'Vertrieb' that will execute the	e selected actions when occure	d.		
ALERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY
Changes in directory for Vertri	- 😨 -	- 🕃 -		Information Information Warning Critical
		DECIDE WHICH ACTIONS	S SHOULD BE CARRIED THROU	SH WITH THIS ALERT
		Send email 🔽 💌		^
To admin@8man-demo.local		<u>× ></u>		
Language English		~ @		
Time zone (UTC+01:00) Amsterdam, Berlin, Bern, Rom,	Stockholm, Wien	~ (L)		
	Write to Wi	ndows event log 🔽 🌵		
		Execute script 🖌 🗊		~
Please add a comment				Create Cancel 🛞

Create alert



- 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)

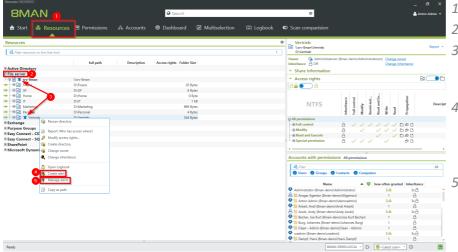
Background / Value

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.

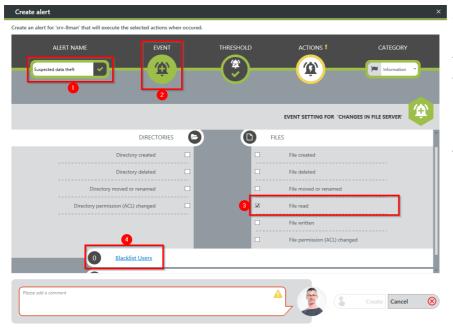
Data theft: A user account reads an unusually large number of files in a short period of time.

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



- 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.



- I. 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".

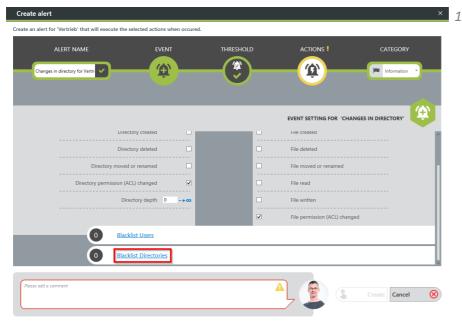
hoose one or more users below which are not considered for the alert AVAILABLE USERS Q Search Q Filter Q @ @ Sam Sales (@man-demo\Sam.Sales) X • Q Name Sam Sales (@man-demo\Sam.Sales) Q Sam Sales (@man-demo\Sam.Sales)

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 dragand-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.



A optional:
 Select "Blacklist directories".

Blacklist Directories

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

AVAILABLE DIRECTORIES BELOW 'VERTRIEB'	THES	E DIRECTORIES WILL NOT BE CO	ISIDERED
🖉 Filter	4	Filter	1
Hersteller		srv-8man\Vertrieb\Projekte	4 🖬
C Sunden			_
Offentlicher ag Offentlicher ag Orojekte	2		
	→		
			5

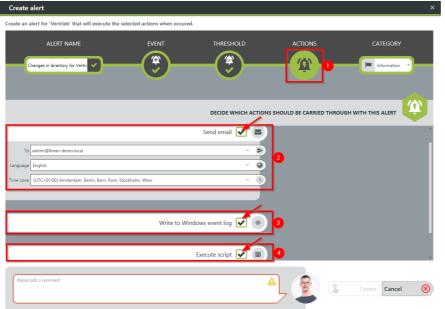
optional:

Use the blacklist to define which directories are not monitored.

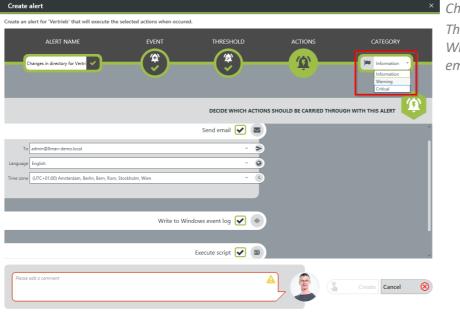
- Use the filter function to find the desired directories. When you filter, the tree view changes to a result list of the directory paths.
- 2. Use double-click or dragand-drop to add directories to the blacklist.
- 3. Use the "Delete" key to remove directories from the blacklist.
- 4. Enable or disable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

Create alert			×
Create an alert for 'srv-8man' that will execute the se	elected actions when occured.		
ALERT NAME	EVENT	THRESHOLD ACTIONS !	CATEGORY
WHEN YOU NEED AN A	LERTING FOR A SET NUMBER OF E	VENTS WITHIN A SET PERIOD OF TIME, THEN MAKE	A THRESHOLD SETTING
20	On Off	Turn threshold on	
3 (#	Yes 🚺 No	caused by the same initiator	
4	10,000 -+	Required number of events to trigger alert	
0	60 -+ Seconds 👻	Limit monitoring to a period of time	
	Alert when 10000 events are initiated	by <u>the same initiator</u> within a <u>duration of 60 Seconds</u>	Your threshold is set
Plesse add a comment		A , 🔹 3	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.



- 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.
 - Enable the execution of a script. To activate this option, a script configuration for alerts must be stored.



Choose a category.

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

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

Create alert						×
Create an alert for 'Ve	ertrieb' that will execute the selected a	ctions when occured.				
	ERT NAME	EVENT	THRESHOLD	ACTIONS	CATEGORY	2
		Si	DECIDE WHICH ACTIONS S	HOULD BE CARRIED THROU	JGH WITH THIS ALERT	
To admin@8m	nan-demo.local		, N			
Language English			~ @			
Time zone (UTC+01:0	10) Amsterdam, Berlin, Bern, Rom, Stockholm, W	lien	~ <u>(</u>			
		Write to Windows	event log 🖌 🐠			
		Exec	ute script 🖌 🔳			~
Please add a comm	ient		A		2 Create Cancel	\otimes

6.2.1.4 Enable alerts for data deletion (file server)

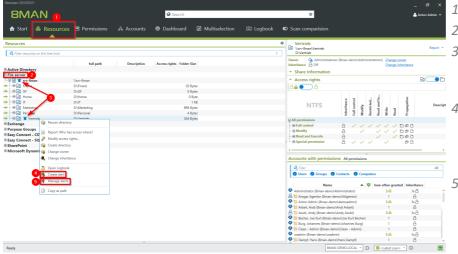
Background / Value

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.

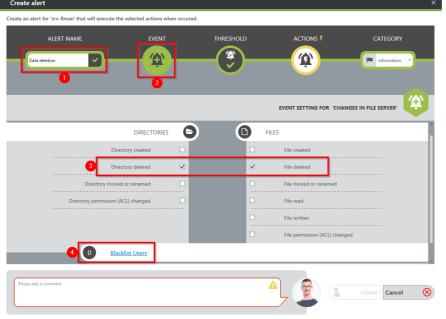
Data deletions: A user account deletes very many files in a short period of time.

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



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



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

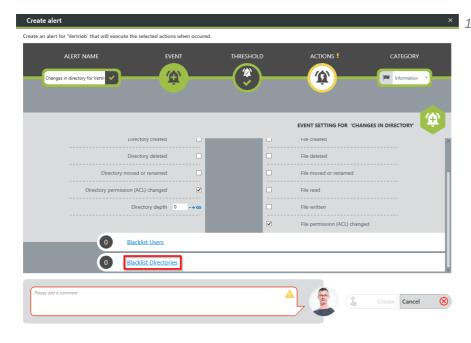
AVAILABLE USERS Q. Search Q. A. Filte Q Q. Sam Sales (8man-demo/Sam.Sales) X • \$ Name Amage: Sam Sales (8man-demo/Sam.Sales)]	THESE USERS WILL NOT BE CONSIDERED Filter Same Same Sales (&man-demo/Sam.Sales) 3	1
			4 Apply Discard

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 dragand-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".

Blacklist Directories

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

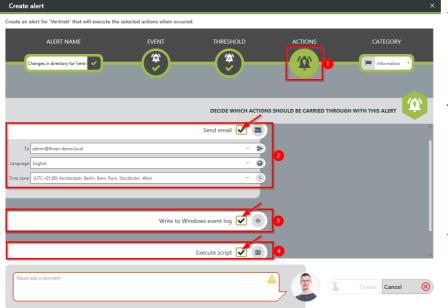
AVAILABLE DIRECTORIES BELOW 'VERTRIEB'	THESE DI	RECTORIES WILL NOT BE CONSIDE	ERED
A Filter	🕰 Filter	r	1
Hersteller • 9 Kunden	Listv-8r	man\Vertrieb\Projekte	4 🗉
☐ 9 öffentlicher ag			
D PIOJEKCE			
	-		
			5

optional:

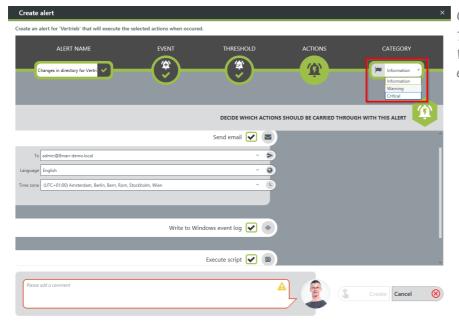
Use the blacklist to define which directories are not monitored.

- Use the filter function to find the desired directories. When you filter, the tree view changes to a result list of the directory paths.
- 2. Use double-click or dragand-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.

- rt for 'srv-8man' that will execute the se ALERT NAME Ŷ (îr) spected data theft Information WHEN YOU NEED AN ALERTING FOR A SET NUMBER OF EVENTS WITHIN A SET PERIOD OF TIME, THEN MAKE A THRESHOLD SETTING Ċ On Off 45 Yes 🕖 No 10,000 -+ 60 -+ Seconds ~ Your threshold is set Cancel \otimes
- 1. Select Threshold.
- 2. Enable threshold.
- 3. Activate the option.
- 4. Define how many events within a period trigger the alert.



- 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.
 - Enable the execution of a script. To activate this option, a script configuration for alerts must be stored.



× Choose a category.

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

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

Create an alert for 'Vertrieb' that will execute the selected action	ns when occured.			
		\sim	ACTIONS	CATEGORY
Changes in directory for Vertri	÷)(Û.	Information *
_	-	_	_	
	DEC	CIDE WHICH ACTIONS SHOUL	D BE CARRIED THROUGH WITH	THIS ALERT
	Send e	email 🗹 💌		^
To admin@8man-demo.local		~ >		
Language English		× 0		
Time zone (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien		v k		
	Write to Windows even	nt log 🗹 🐠		
	Execute s	script 🖌 🗉		~
C			2	
Please add a comment				eate Cancel 🛞



Create alert

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

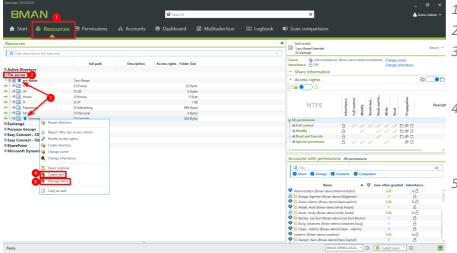
Background / Value

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.

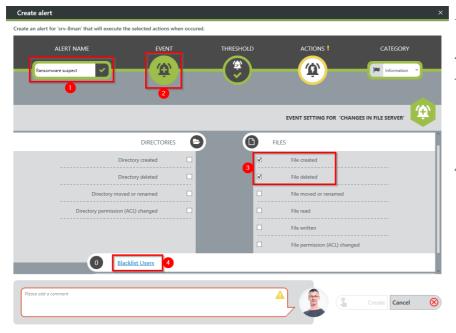
Ransomware Attack: The combination of file creation and deletion by one user account.

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



- 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.



- I. 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".

R	acl	zlie	+ 1	lee	100
	aci	1112		20	

Please choose one or more users below which are not considered for the alert	
AVAILABLE USERS Q. Search) Q. Filter	HESE USERS WILL NOT BE CONSIDERED
1 Q Q Sam Sales (8man-demo\Sam.Sales) X ★	Filter
Name	Name
	8 Sam Sales (8man-demo\Sam.Sales)
	4
	4 Apply Discard
	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 dragand-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.

alert for vertileb that will execute		hen occured.				
ALERT NAME	EVENT		THRESHOLD			CATEGORY
Changes in directory for Vertri	A		-(😰)-		<u>(</u> <u> </u>	Information 🔻
_	_	-	_	-	_	(4
					EVENT SETTING FOR 'CHANG	
	virectory created			_	File created	
C	irectory deleted				File deleted	
Directory mo	wed or renamed				File moved or renamed	
Directory permissio	n (ACL) changed	✓			File read	
	Directory depth 0	-+∞]	File written	
				2	File permission (ACL) changed	
0	lacklist Users					
0	lacklist Directories					
		· · · · ·				
add a comment						
						Create Cancel

1. optional: Select "Blacklist directories".

Blacklist Directories

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

	AVAILABLE DIRECTORIES BELOW 'VERTRIEB'	THESE DIRECTORIES WILL NOT BE CONSI	1
	Versiener Skunden Serier Orden Serier Orden Orden		
		+	
5			

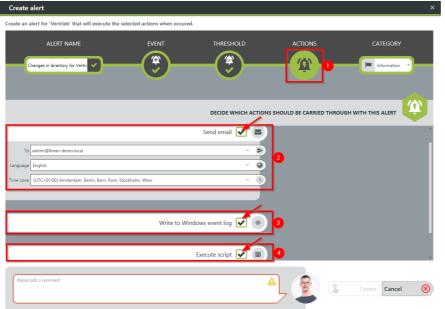
optional:

Use the blacklist to define which directories are not monitored.

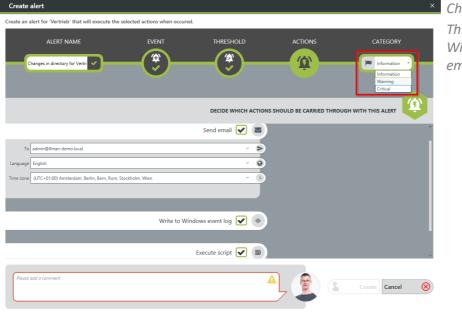
- Use the filter function to find the desired directories. When you filter, the tree view changes to a result list of the directory paths.
- 2. Use double-click or dragand-drop to add directories to the blacklist.
- 3. Use the "Delete" key to remove directories from the blacklist.
- 4. Enable or disable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

Create alert			×
Create an alert for 'srv-8man' that will execute the se	lected actions when occured.		
ALERT NAME	EVENT	THRESHOLD ACTIONS !	CATEGORY
WHEN YOU NEED AN AL	ERTING FOR A SET NUMBER OF I	EVENTS WITHIN A SET PERIOD OF TIME, THEN MAKE A	THRESHOLD SETTING
20	On Off	Turn threshold on	
3 (#	Yes 🚺 No	caused by the same initiator	
4	10,000 -+	Required number of events to trigger alert	
0	60 -+ Seconds 🗸	Limit monitoring to a period of time	
	Alert when 10000 events are initiate	d by the same initiator within a duration of 60 Seconds	Your threshold is set
Please add a comment		A , (2) &	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.
 - Define how many events within a period trigger the alert.



- 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.



Choose a category.

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

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

Create alert						×
Create an alert for 'Vertrieb' that will execute the	elected actions when occure	ed.				
ALERT NAME	EVENT	THRESHOLD		ACTIONS	CATEGORY	
Changes in directory for Vertri	-(*)	-(*)-		Û)	Information Y	
	_	DECIDE WHICH A	CTIONS SHOU	LD BE CARRIED THR	OUGH WITH THIS ALERT	Ŷ
		Send email 🖌	≥)			^
To admin@8man-demo.local		~	•			
Language English		~	0			
Time zone (UTC+01:00) Amsterdam, Berlin, Bern, Rom, S	ockholm, Wien	~	•			
	Write to Wi	indows event log 🔽 🤇	40			
		Execute script 🖌				~
			0		2	
Please add a comment			A		Create Cancel	\otimes

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

<u>Create a report about activities on mailboxes, calendars, and contacts</u> <u>View activities in mailboxes, calendars, and contacts (logbook)</u>



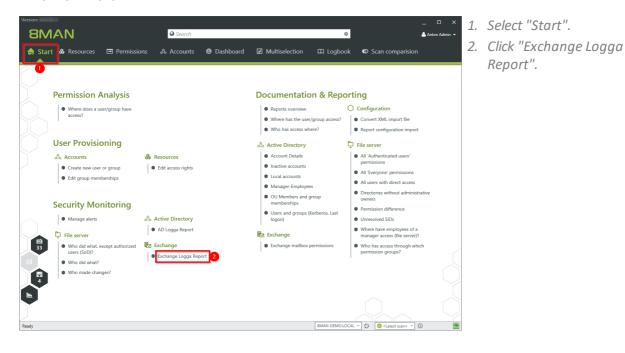
6.3.1.1 Monitor activities on mailboxes, calendars, and contacts (report)

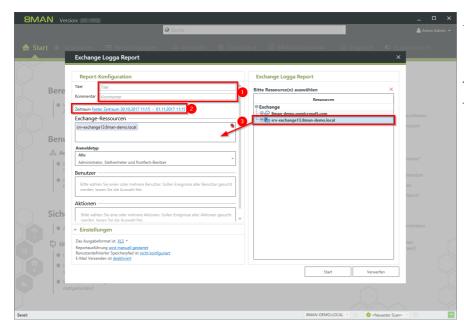
Background / Value

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 <u>logbook</u> <u>view</u>.

Additional Services

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





- □ × 1. optional:
 - *Give the report a title and a description.*
 - 2. Set the period.
 - 3. Add the required resources via drag & drop.

		Exchange	e Logga Report	
mment Comment		Selection of	f monitored mailboxes	
ne Period Fixed time span 12/16/20	017 2:02 PM - 12/18/2017 2:02 PM	🖉 Filter		
change Resources				
📻 Please selec	t one or more exchange resources.			
gon type				
All		, <mark>1</mark>		
dministrator, delegate and mailbo	x owner			
ser accounts			1.0.0	
	ne or more accounts Il accounts leave this field empty.		pox selection for re ntly not possible, b	
l o search for a		carre		
		ever	its available for Exe	change tracers.
tions			its available for Exe	change tracers.
ctions Please select c	one or more actions all actions leave this field empty.	ever 3	its available for Exe	change tracers.
ctions Please select c			its available for Exe	change tracers.
tions Please select o To search for a			its available for Ex	change tracers.
tions	all actions leave this field empty.		its available for Exe	change tracers.

- 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.

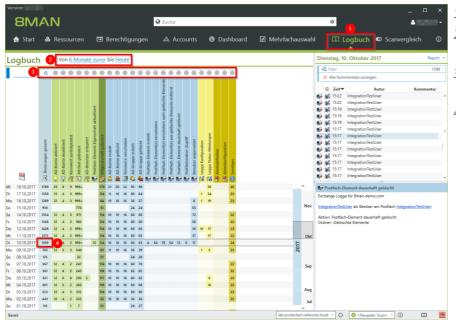
6.3.1.2 View activities in mailboxes, calendars, and contacts (logbook)

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.

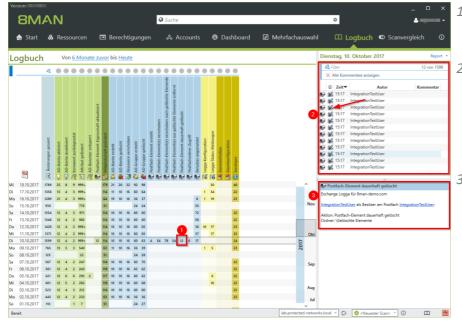
Additional Services

Report: Monitor activities on mailboxes, calendars, and contacts



- 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).

208 | Access Rights Management



- 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.

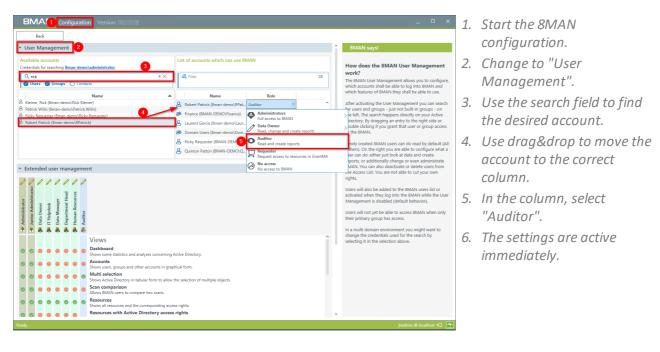


7.1.1.1 Create a read only account with 8MAN

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.



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

<u>Who has access to what?</u> <u>Where do employees of a manager have access to?</u> <u>Where do users and groups have access?</u>

Exchange

Who has access to what? Identifying mailbox permissions

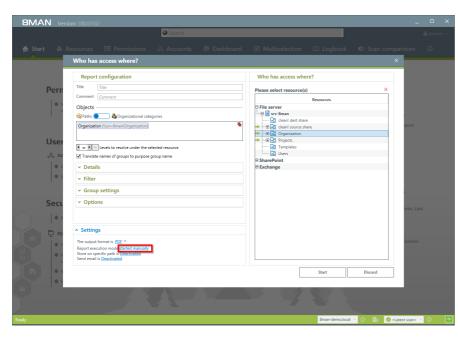
SharePoint

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



Step by step process

8MAN Version: 7.6.151

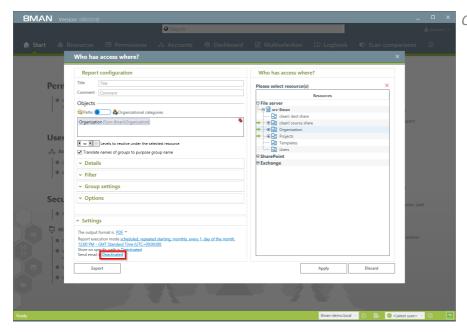


Select the desired report. Click on "started manually" in the "Settings" area.

🚖 Start 💩 Ro		
Pern	Report configuration Who has access where? Scheduled Report Configuration ×	
* <u>}</u>	Time schedule Sign of demand Do not solvedule, the task will only be started on demand.	
User	Daily Settings Image: Constraint of the set o	
0 C 0 C	Monthly Monthly Marxies M	
Sect	Repeate mode	
	C Generate report only once	
문민	dant Oncerd	
Ready	Sman-demo.local 👻 🔅 📑 🖉 <latest scan=""> 🝸 🛈</latest>	

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

216 | Access Rights Management



Click on "Deactivated".

8MAN Vers				
🔒 Start 🐁				
	Report configuration	Who has access where?		
Pern	Title	Please select resource(s)	×	
l e v	Comment	Kesources		
	Objects	File server		
	Configuration	REI cleani dest share	×	
User				
.& Ac	Email Send email, when report is created			
	2 M ≥ Add report as email attachment			
• ¢ • ¢				
	Notification emails sent to sam.sales@8man-demo.com			
Secu				
		4 Apply	Discard	
	 Settings 			
	The output format is PDF *			
	Report execution mode scheduled, repeated starting, monthly, every 1, day of the month (1240 PM - 6Ms Standard Time (UTC + 000400)) Store on specific path is Deschvated			
	Send email is Deactivated			
) (m) • v			Discard	
<u> </u>				
Den de		Sman dame lacal	L C E C data	

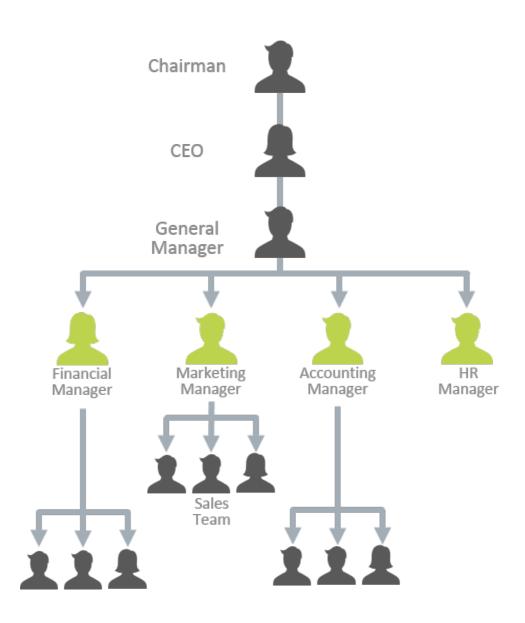
- 1. Activate emails.
- 2. Activate the option "Add report as email attachment".
- 3. Determine who should receive the email. You can enter more than one recipient.
- 4. Click on "Apply".

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.



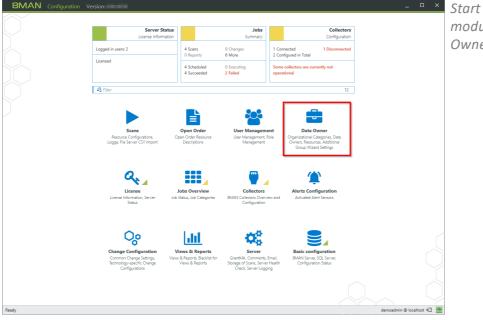
7.1.2.1 Define Data Owners and assign resources

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".



BMAN Configuration Ver		_ 🗆 ×
Back	Data Owner configuration	0
Organization categories	marketing	User & Group selection
Control Delete Impact Exact Report Q. Seach MAN Demo Company MR manufacturing OU Data Owner A RBD SharePoint Site SharePoint Site	Additional Group Wizerd settings Data Owners Additional Settings Data Owners Name Inherited gam Data Owner Name Reducestor Name	Domain Braan-demolocal Contain Braan-demolocal Contain Contained and
SharePoint Team	Resources A filter Show header derives Rame Inductive filter B Active Directory (1) C Silve and Organization Marketing) C Silve and Organization Marketing C Silve and	Resource selection

- 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".

BMAN Configuration Vers		_ 🗆 ×
Back	Data Owner configuration	0
Organization categories	marketing	User & Group selection
Create Edit Delete Import Export Report Q Search Include content	Additional Group Wizard settings Actigned workflow Chenit Savig Step Data Owner Authorization Data Owners Requesters	Domain 8man-demo.local v Q Search 💽 Q Filter
MAN Demo Company All R manufacturing OU Data Owner ARD SharePoint Site SharePoint Team	A filter 1 Show inherited entries 1 Name Inherited from User role Parick Wills (BMAN-D) Data Owner A Ricky Requester (BM	Q Q Atrick Wills (Bman × • ♥) Name ∄ Patrick Wills (Bman-demo/Patrick Wills)
Ready	Resources	Resource selection

- 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	Exchange
Unlocking user accounts	Creating a mailbox (email enable users)
Resetting passwords	Managing mailbox and email size
Modifying group and user attributes	Managing out of office notices
Deactivating a user account	Changing mailbox permissions
Deleting a user account by using the "soft delete" feature	
Removing a user and their 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. Todo 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.

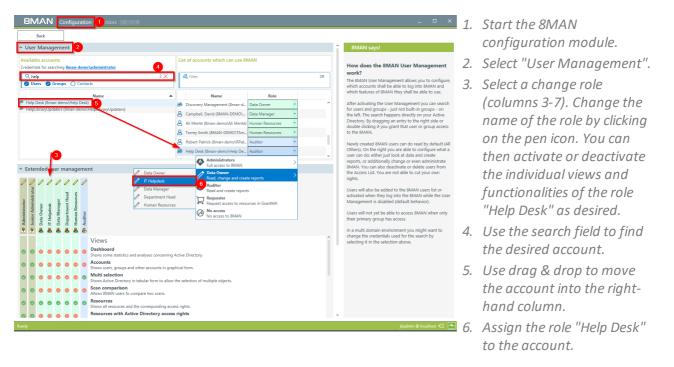


7.1.3.2 Assign responsibilities to help desk employees

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.



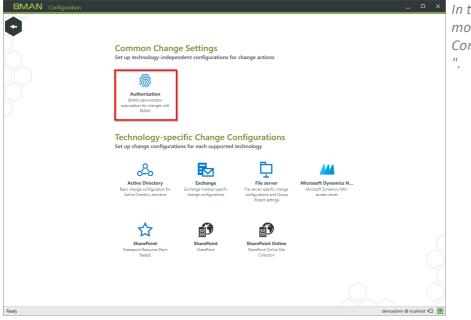
7.2 Create approval processes

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

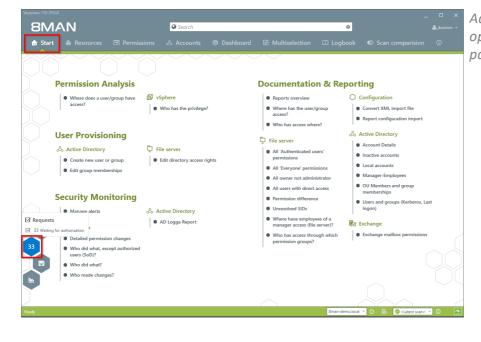


In the 8MAN configuration module select "Change Configuration">"Authorization

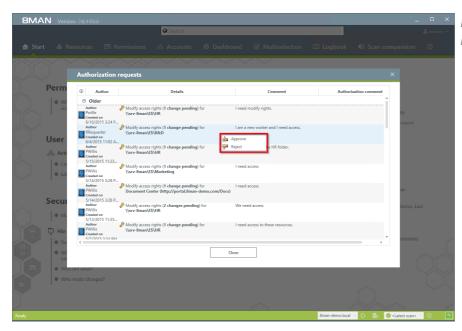


BMAN Configuration Version:	- • × Activate the admin approval mode.	istrator
Authorization Comparison Com	Request Approve Reject	
For Activated Any changes performed by a Data Owner within BMAN must be authorized by an BMAN Administrator.	& *	
Rade	demonstrating & localizers of T	

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



226 | Access Rights Management



Right click on a request and make your decision.

- You must enter a comment.
 Click "Apply".

8MAN

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.

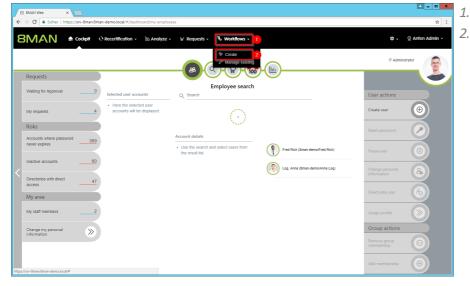
If more complex workflows with several decision-makers are required to grant access rights, you can also quickly map them.

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



Select "Workflows".
 Click on "Create".

- Market in sporred process free for?
 I Add Approval step?
 What is your approval process free for?
 Center workflow
 Cancel
 Cancel
 Cancel
 Cancel
 Cancel
 Cancel
 Cancel
 Cancel
 Cancel
 Cancel
- Give the workflow a title.
 Give a short, concise description of the workflow's purpose.



				_ _ ×
🗲 🕞 🙋 https://srv-8man.8man-demo.loca	l/#/workflow;isUpdate=false	- ۵	🖴 🖒 🔏 8MAN Web - Workflow D	let× îr ☆ 🔅
8MAN 🏶 Home	🔟 Recertification 👻 🔟 Analyze	→ ☐ Requesting →	% Workflows -	🌣 👻 😤 įbadmin 🗸
	My approval proce	ss 2		
	Demo.			
	1. Approval step			
\bigcirc	2 Add Approver			
	3 What should be checked in this appro	oval step?		
		4		
				Create workflow Cancel

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

You can also add multiple approvers for any step, which can be useful in case of vacation or illness.

- 3. Describe the approval step.
- 4. Add any additional steps in the approval process.
- 1. Add an additional step.
- 2. Delete an approval step.
- 3. Generate the workflow.

					>	x
C 🕀 🛞 🦉 https://srv-8man.8man-demo.loca	/#/workflow;isUpdate=false	,Ω + <u>A</u> (🖒 🥖 8MAN Web - V	Vorkflow Det ×	fh ★	¢3
8MAN A Home	🔟 Recertification 🗸 🔟 Analyze 🗸 🗒	Requesting - 🤎	🗄 Workflows -		💠 👻 😕 įbadmin 🗸	^
	Demo.			8		
\land	1. Approval step					
		dd Approver				
\bigcirc	What should be checked in this approval step?					
	0	7		82		
	2. Approval step					
	Add Approver					
	What should be checked in this approval step?]		
				Cre	3 ate workflow Cancel	•

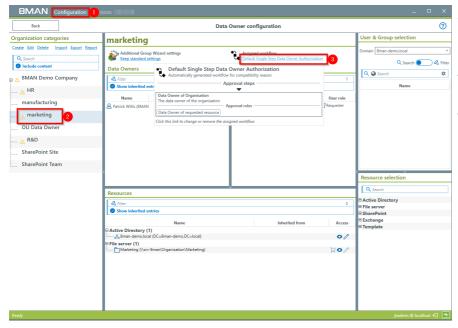
				_ 0
🗲 🕀 💋 http	s://srv-8man.8man-demo.local/#/workflows) - C	🖥 🖒 💋 8MAN Web - Manage existi 🗙	
8 MA	N 🕈 Home 🔟 Recertification -	🔟 Analyze 🗸 🏼 🗎 Requesting 🗸	% Workflows -	🌣 🗸 🙁 įbadmin
	Workflows		Search	
	Active workflows		Search in Workflows	
Õ	Default Single Step Data Owner Authorization Automatically generated workflow for compatibility	reason		8
	My approval process 2 Demo.			3
Ť				
				$\hat{\mathbf{O}}$

- 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.



- 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.

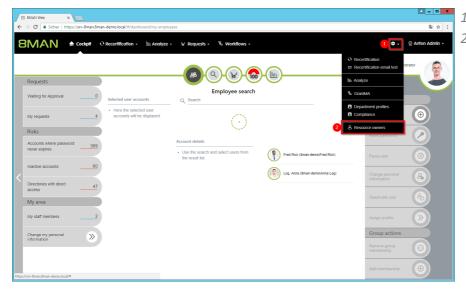
The functionality is deactivated by default. Please contact support for activating.

Additional Services

Defining individual approval workflows

SMAN Web × ← → C ▲ https://srv-8man.8man-demo.local/#/login		 4 = □ × 3 ÷ 	Login to the web interface with
		۵	admin credentials.
Õ	8MAN		
	demoadmin mini- Emaa-demo English • Login as current Windows User Powered by Protected Networks v 8.0 2931e76 15.5 2017_1:17		





- 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.

88	MAN Web ×			A = 0 ×
$\leftarrow \Rightarrow$	C https://srv-8man.8man-demo.local/#/settings:mo	de=defaultapprover		\$
81	MAN 🕈 Home 🔍 Recertification -	🕍 Analyze + 🛛 Requesting + 🐁 Workflows +		© ≉ - ∆ demoadmin -
Search	n 🖸			
æ.	▼ All Resources	Assigned resource owners		
	 Active Directory 	All Resources / Fileserver / srv-8man / Finanz / Gehälter		
¢,	▼ Fileserver	Antesources/ thesever/ sivenan/ thanz / Genater		Associate accounts
ଦ	4 ▼ srv-8man	A Tor, Moni (8man-demo/Moni Tor)	8	Search my domain only
	Archive			Search history
	cleant source			
	cleant target 2			
¢,	▼ Finanz 3			
C	► Assets			
	Gehaller			
	Inicht gucken Rechnungen			
	► GE			
	► Home			
	• IT			
G	Marketing			
C	► Personal			
_	 Vertrieb 			
	► Vorlage			
	 Hardware 			
	► Software			

8MAN

Neuer Tab			_ = □ ×
< > 08N	https://srv-8man.8man-demo.local/#/settingsmo https://srv-8man.8man-demo.local/#/settingsmo Home		☆ : © * ~ & demoadmin ~
Search	All Resources Active Directory	Assigned resource owners	-
e. D	Fileserver srv-8man	All Resources / Fileserver / srv-8man / Finanz / Assets	
	Archive	Arbeit, Andi (8man-demo'Andi Arbeit)	Search my domain only
¢,	► cleant target ▼ Finanz		2 Dee, Dan (8man-demo\Dan Dee)
¢.	Assets Gehätter Incht gucken		
	Rechnungen GF		
	► Home ► IT		
© ©	Marketing Personal Vertrieb		
	VorlageHardware		
	► Software		

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

NeuerTab X B SMAN Web X € → C ■ https://urv.8man.8man.demo.local/*/worlfuburisUpdate=faile	Design individual workflows
Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of the approval type? Image: Antice of the requested conduction of type? Image: Antice of the requested cond	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.

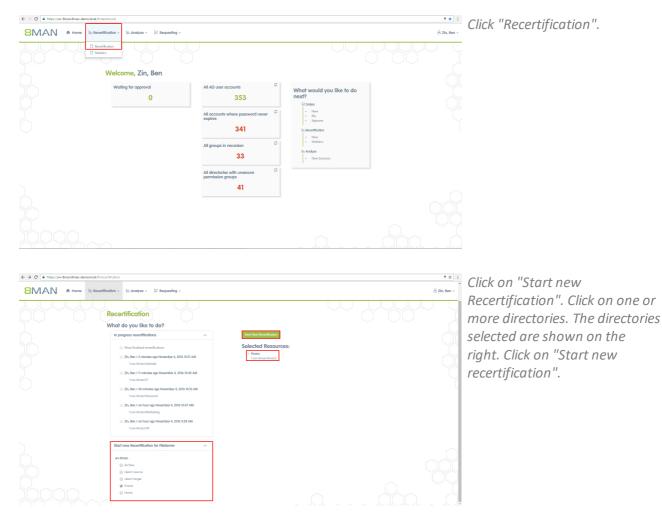
You receive an email with the instructions to the re-certification process. Then you decide for each user and resource if the access right should stay or be removed.

Your desired changes will be transferred automatically to the administrator.

Complementary Services

Change file server access rights

The process in single steps



Re	certification (3	39)	Y	5 8		Configuration						Reports Direct Excel export
Pa	th × Access Rights ×						8	columns	selected	• C =	L C	Available Actions
	ath	Υ F Υ	T T	Account	Member Of	Access R 1	E 1	r I 1	Action	T Comm T		Accest
	Path: \\sev-8man\Finanz (38 in											The access right is correct and should r
	at Access Rights: Full control G											5.
	\\srv-8man\finanz	Finanz		cradmin (8man-demo\cradmin)	Domänen-Admins (8ma.							Remove The access right should be removed as
	\\srv-8man\/finanz	Finonz		NT-AUTORITÄT\SYSTEM		full control						possible.
	\\srv-8man\Vinanz	Finonz		so-SP_farm (Brnan-derno\sa-SP_farm)	Administratoren I8mon	full control						
	\\srv-8man\Finanz	Finonz	٥	Administrator (8man-demo\Administrator)	Administratoren IBmon	. Full control						
3	\\srv-8man\Finanz	Finonz		Clean - Admin I8man-demo\Clean - Admini	Domänen-Admins (8ma.							Progress
	\\srv-8man\Finanz	Finanz	٥	so-ExcViewer (8mon-demo\so-ExcViewer)	Domänen-Admins (8ma.							
	\\srv-8man\Finanz	Finanz		sa-SP_install (Bman-demo\sa-SP_install)	Domänen-Admins (8mg.							Copen (339)
	\\srv-8man\Finanz	Finanz	0	Minni Ralwasser (8man-demo/Winni Ralwass	Marketing (8man-demo)							selected Ac
	\\srv-8man\Finanz	Finanz	0	Geber, Ann (8man-demo\Ann.Geber)	Marketing (8man-demol							III Sent 10
	\\srv-8man\/inanz	Finanz	۰	Krise, Christiane (8man-demo/Christiane Krise)	Marketing (8man-demol,	. full control						
	\\srv-8man\/linanz	Finonz	0	Dee, Dan (8man-demo\Dan Deel	Marketing (8man-demol							Save Current
	\\srv-8manVinanz	Finonz		Ka, Ede (8man-demo\8de Ka)	Marketing (Brnan-demol,							Some Carrier
	\\srv-8man\Finanz	Finonz		Frido Fleia (Bman-demo\Frido.Fleia)	Marketing (Brnan-demol,							
	\\srv-8man\Finanz	Finanz	٥	Dampf, Hans I8man-demo'Hans Damp®	Marketing (Bman-demol,	Full control						
	\\srv-8man\Finanz	Finanz	٥	hans mayer (8man-demo\hans.mayer)	Marketing (Bman-demo)	Full control						
	\\srv-8man\Finanz	Finanz	٥	Becher, Joe Kurt (8man-demo'Joe Kurt Becher)	Marketing (8man-demo)	Full control						
	\\srv-8man\Finanz	Finanz	•	Maria Makketing (8man-demo/Maria Makke	Marketing (8man-demo)	Full control						
	\\srv-8man\Finanz	Finanz	Φ	Urai, Sam (8man-demo\Sam.Urai)	Marketing (8man-demo)	Full control						

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.

← ⇒				certification-details:essionId=7eea5ac8-b51e- Iffication - III: Analyze - III Reque	Accept The occess right is correct	and should re	main os is.	×		¥ ☆] : & Zin, Ben - Reports
	th × Access Rights ×				Comm	int Ples	zse enler a comment		r (Reports Direct Excel export Available Actions
	hath .			Account		_				Accest
0	# Path: \\srv-8man\Finanz (38 in						Assign action	Concel		The access right is correct and should remain as
	J Access Rights: Full control (2-							CORRE		8.
				cradmin (Bman-demo)cradmini						Remove The access right should be removed as soon on
			8							possible.
	\\srv-8man\/finanz		0	so-SP_Farm (Brnan-demo\sa-SP_Farm)	Administratoren (8mon	Full control				
			0	Administrator (8man-demo\Administrator)	Administratoren (8man					
			0	Clean - Admin I&man-demo\Clean - Admini	Domänen-Admine (8ma					Progress
			0	so-ExcViewer (8mon-demo\so-ExcViewer)	Domôneo-Admins @mo					
			0	so SP_install (Eman-dema\sa-SP_install	Domônen-Admins @mo					
			0	Minni Rolwasser @man-demo\Minni Rolwass .	Marketing (Bman-demol					Open (339) selected Action (0)
			\$	Geber, Ann I8man-demo\Arm.Geberi	Marketing (Bman-demol					III Sent XX
8	\\srv-8man\/inanz	Finanz	\$	Krise, Oxistiane (Bman-demo\Christiane Krise)	Marketing (8man-demo),	Full control				
8	\\srv-8man\\finanz	Finanz	0							
			Φ	Ka, Ede (8man-demo\Ede Kal	Marketing (8man-dems).	Full control				
			0	findo fileia Iliman-demo\findo.fileial	Marketing (Bman-dems), .	full control				
	Visrv-8mon/Finonz		0	Dompé, Hons Illiman-damo/Hons Dampé	Marketing (Bman-demo), .					
			0	hans mayer (8man-demo\hans.mayer)	Marketing (Bman-demo)					
			•	Becher, Joe Kurt (8man-demo/Joe Kurt Becher)	Marketing (Bman-demol					
			0	Maria Makketing (Eman-demo/Maria Makke	Marketing (Bman-demo)					
			0	Urai, Sam (Bman-demo\Sam.Urai)	Marketing (8man-demol					
			0							

	C https://srv-8man.8m	an-demo.lo	cal/#/n	ecertification-details;sessionId=7eea5ac8-b61e→	405d-978d-32a5274c598b						7
Bl	MAN 🐽	ome lin	Recer	tification - 🖿 Analyze - 🗜 Reques	sting -						S zin, t
Re	certification (3	39)				Configuration ath: \\srv-8man\Fina	anz			ŲŲ	Reports Direct Excel export
Pa	fh × Access Rights ×						8 columns	selected	• C 🔳	2 C	Available Actions
Р	ath	т Е т	T 1	Account	Member 01	Access Ri Y E.	T L T	Action 1	Comm Y		havet
3 4	Path: Warv-&manVFinanz (38 in	ems)									 The access right is correct and should remain
1	# Access Rights: Full control (2										is.
	\\srv-8man\Finanz	Finanz	0	cradmin (8man-demo\cradmin)	Domänen-Admins @ma	Full control					Remove
	\\srv-8man\Finanz	Finonz	8	NT-AUTORITÄT\SYSTEM		Full control					The access right should be removed as soon possible.
	\\srv-8man\Finanz	Finanz	•	sa-SP_Farm (Bman-demo\sa-SP_Farm)	Administratoren (8man	Full control					
	\\srv-8man\Finanz	Finanz	φ	Administrator (8man-demo\Administrator)	Administratoren (8man	Full control					
	\\srv-8man\Finang	Finanz	φ	Clean - Admin (8man-demo\Clean - Admin)	Domänen-Admins (8ma	Full control		Remove	Access rights		Progress
	\\srv-8man\finanz	Finanz	φ	so-ExcViewer (8mon-demo/so-ExcViewer)	Domânen-Admins (8ma	full control		Remove	Access rights		
	\\srv-8man\/linanz	Finonz	ø	sa-SP_Install (Bman-demo\sa-SP_Install	Domânen-Admins (8ma	full control					
	\\srv-8man\Finanz	Finonz	•	Minni Rolwasser (8man-demo/Minni Rolwass	Marketing (Bman-demol	Full control		Accept	Access rights		Open (334) selected Action II
	\\srv-8man\Finanz	Finonz	φ	Geber, Ann (8man-demo\Ann.Geber)	Marketing (Bman-demol	Full control		Accept	Access rights		III Sent (5)
	\\srv-8man\Finanz	Finanz	φ	Krise, Christiane (8man-demo/Christiane Krise)	Marketing (8man-demol,	Full control		Accept	Access rights		
	\\srv-8man\Finanz	Finanz	ø	Dee, Dan (8man-demo\Dan Deel	Marketing (8man-demo)	Full control					
	\\srv-8man\finanz	Finanz	φ	Ka, Ede (8man-demo\Ede Ka)	Marketing (8man-demol, .	. Full control					Sove Current
	\\srv-8man\/linanz	Finonz	ø	frido fleia I8man-demoVrido.fleial	Marketing (8man-demol, .	full control					Final Execute
	\\srv-8man\Finanz	Finonz	0	Dampf, Hans I8man-demoVHans Damp®	Marketing (Bman-demol,	. Full control					
	\\srv-8man\Finanz	Finonz	٥	hars mayer (8man-demo\hars.mayer)	Marketing (Bman-demol	Full control					
	\\srv-8man\Finanz	Finanz	ø	Becher, Joe Kurt (8man-demo/Joe Kurt Becher)	Marketing (8man-demol	Full control					
	\\srv-8man\Finanz	Finanz	ø	Maria Makketing (Bman-demo/Maria Makke	Marketing (8man-demol	Full control					

Do the same for the permissions you want to remove. Your decision is marked in the colum "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.

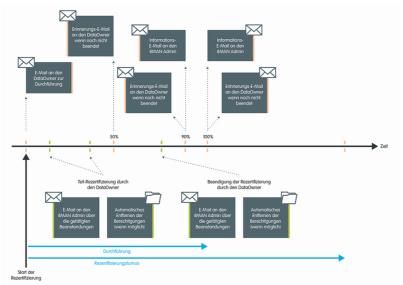


E SMAN Web , Beretters X

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.

8MAN

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

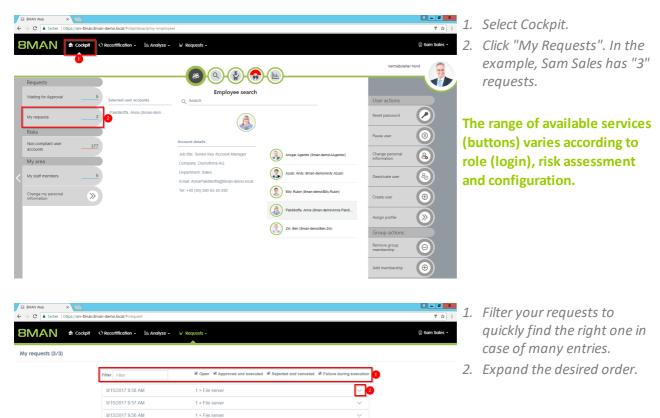
Keep track of your orders. Cancel orders or resend notifications to the approver.

Additional Services

Overview of all cockpit services

1

8MAN



MAN 🗕	Cockpit O Recertification -	≜ Analyze + ₩	Requests -			© Sam Sale
y requests (3/3)						
	Filter		Open Approved and execute	d 🗷 Rejected and canceled 🗷 F	ailure during execution	
	9/15/2017 9:58 AM		1 × File server		^	
	Requested by: 음 Sam Sales der Bost		Resources requested for: A Sam Sales der Boss	Comment: Kann die ExelTabelle ni benötige Ändern-Recht		
	1 State	Resource	Туре	Next approver		
	Ø Open	Berlin \\srv- 8man\Finanz\F	File server	Data owner of requested organization category		
	9/15/2017 9:57 AM		1 × File server		~	
	9/15/2017 9:56 AM		1 × File server		\sim	

- 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

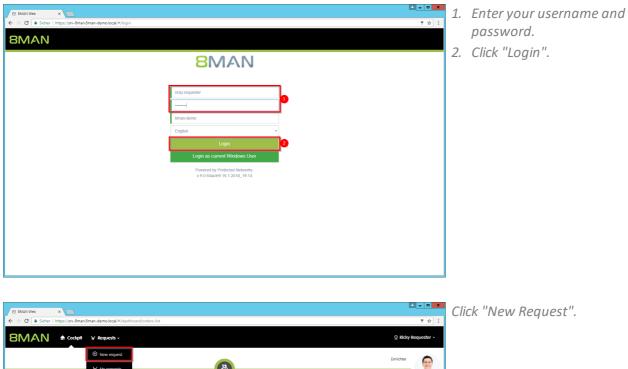
Background / Value

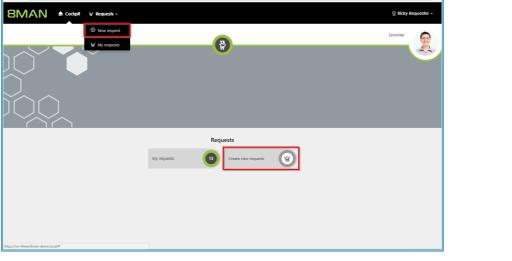
Employees can request access rights to file server directories from Data Owners by using the 8MATE GrantMA self-service portal.

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)







					_ 🗆 🗙
(ttps://srv-8man.8man-dem	o.local/#/order	요 - 음 C 🥭 8M	AN Web - New Request 🛛 🛛 🛛 🛛	
8 M	AN 🕈 Ho	me 🏾 🛱 Requesting 🗸			🐣 Ricky Requester 🗸
	Create a ne	ew request			
	Start	· · · ·			
\leq					
	Organizations			^	
\bigvee	Action R	esource	 Details		
	Open 🛃	manufacturing	Organization		
	Open	SharePoint Site	Organization		
	Open 🔓	SharePoint Team	Organization		

8MAN shows you as the applicant exactly the resources that can be ordered. Select the desired resource and click on "order".

8M	Sales \\srv-8man\Organization\Sales	File server	1 Modify		b - New Request X	n ★ C × day Requester +
	C Sta Resources				Add to shopping cart	Cancel
	Action Resource Request C 23 Marketing Request C 23 Sales			Details File server - Directory \\srv-8man\Organization\M File server - Directory \\srv-8man\Organization\S		

- 1. Select an access category.
- 2. Click "add to shopping cart".

		-demo.local/#/order;resourcet;		J-16264.142 0464 4-40 -7				• ×
8M		Home Request		u=1020445-0410-4000-01		Order	_	
[]	Create a Start / Sales	new request	ł					
	Resources					^		
\leq	Action	Resource			Details			
	Request	🗋 🛃 Marketing			File server - Directory \\srv-8man\Organization	Warketing		
\cup	Request	🗆 🛃 Sales			File server - Directory \\srv-8man\Organization	\Sales		
								\bigcirc

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

← ⊖ <i>@</i> https://srv-8ma	n.8man-demo.local/#/basket		ව - 🔒 එ 🏉 8MAN Web -	Order Basket ×	- □ × ☆ ☆
8MAN	🕈 Home 🛛 🗎 Requesting -			2 Order Basket	A Ricky Requester -
	Thank you for your	request.			
	From: Sales			^	
	Resource	Туре	Options		
	8 Marketing	File server - Directory	Read & Execute	8	
	8 Sales	File server - Directory	Modify	8	
2	Resources will be reques	ted for:			
					5
	4	Please add a comment			Request
		Input required.			
					~

- 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.

(-) @ https://srv-8m	an.8man-demo.local/#/re	quest		・ P 🔒 C 🏉 8MAN Web - I	My Requests X	<u> </u>
8MAN	🔒 Home 🕽	2 Requesting -				🖉 Ricky Requester 👻
	My Reque		Dpen 🗆 Closed 💷 Failure du	ring execution		
	2/27/2017 12:28	PM	2 × File server			
	Requested by:		Resources requested for:	Comment: Demo.		
	State	Resource	Туре	Next approver	000	
	(2) Open	Marketing	File server	Data Owner of requested resource	0 🖂 🛛	
	Open	Sales	File server	Data Owner of requested resource	0 🖴 🛛	
	11/30/2016 4:23	PM	1 × File server		~	
	11/30/2016 4:10	PM	1 × File server		\sim	
					ĬÒÒ	

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.

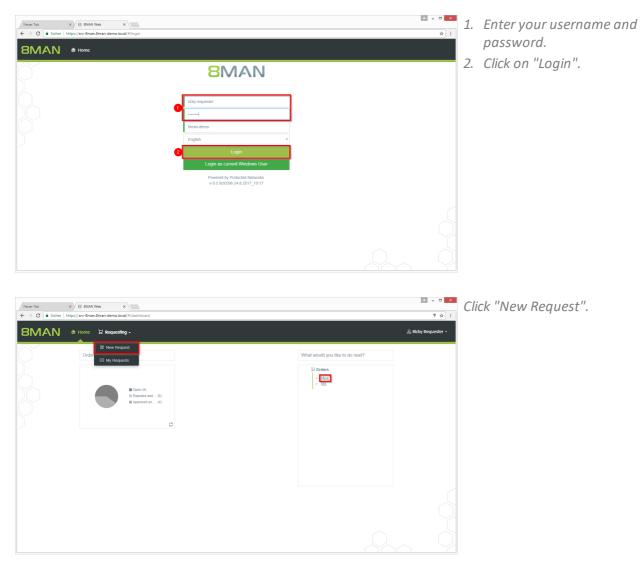
7.4.3 Request group memberships

Background / Value

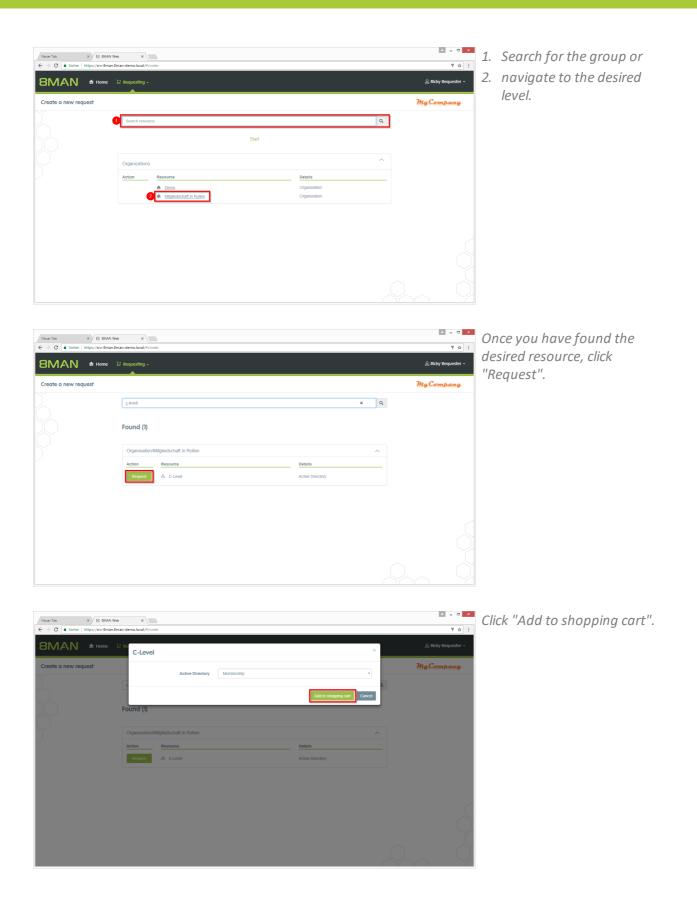
Employees can request group memberships by using the 8MATE GrantMA self-service portal. You can configure a variety of approval workflows and involve the relevant decision makers, depending on your security requirements.

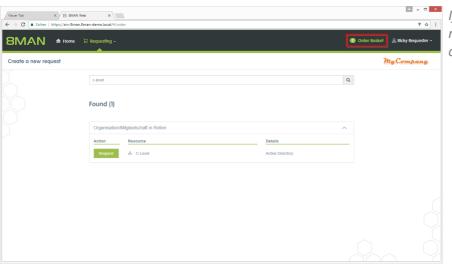
Additional Services

<u>Create approval workflows</u> (administrator)









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

NeuerTab × 8 8 ← → C	MAN Web × 3man.8man-demo.local/#/basket			₽ - □ ₽ ☆
8MAN 🗕 Hon	ne 🏽 🗜 Requesting -			🕕 Order Basket 🛛 🕹 Ricky Requester 🗸
Thank you for your reques	ŧ.			MyCampany
	Thank you for you	r request.		
	Resource	Туре	Options	<u>^</u>
	B C-Level	Active Directory	Membership	
	Resources will be reque	ested for:		
	8 Ricky Requester 8			
		-	Please add a comment	6
		4		Reques

4 - 0 × Neuer Tab X B 8MAN Web × → C 🔒 sid 9 ☆ : 8MAN . . 용 Ricky I My Requests (5/9) **МуСотрану** Filter Filte 9/1/2017 2:20 PM Requested by: & Ricky Reque 234 8/31/2017 5:40 PM 1 × Active Directo 8/4/2017 2:55 PM 2 × Hardwar 7/6/2017 3:05 PM 1 × File server 7/6/2017 2:59 PM 1 × File serve < 1.

8MAN

- 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

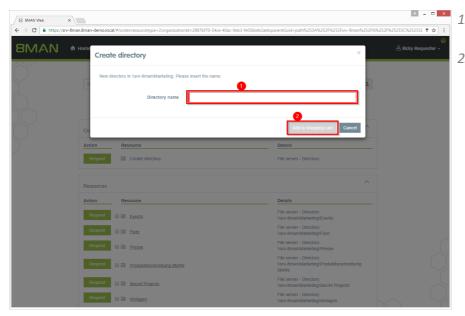
		▲ – □ X	Log in as the requester.
		ष छे: :	
	8MAN		
	ncky requester fiman-demo English • Login Login as current Windows User Powered by Protected Networks v 9.0 66acle9 16.1.2018_19.14		
		▲ = 0 X	
B 8MAN Web × ← → C ■ Sicher https://snv-8man.8man-demo.local/#/dashboard/orders-list		9 x :	Start a new request.
8MAN ♠ codpit ¥ Requests -		ୁ Ricky Requester •	
Maraguest	•	Ender	
	Requests		

reate new requests

8MAN

/		은 Ricky Reque
	Create a new	w request
	Search resource	٩
	Start / Search /	/ Markoting
	Create new objects	^
	Action Resource	Details
	Request Create directory	File server - Directory
	Resources	^
	Action Resource	Details
	Request Events	File server - Directory \\srv-8man\Marketing\Events
		File server - Directory
	Request Elver	\\srv-8man\Marketing\Flyer
	Request P Fiver Request R Presse 2	\\srv-8man\Marketing\F}yer File server - Directory \\srv-8man\Marketing\Presse
		File server - Directory
	Request R Presse 2	File server - Directory Visro-Brann Marketing/Presse File server - Directory Visro-Brann Marketing/Produktbeschreibung

- 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.

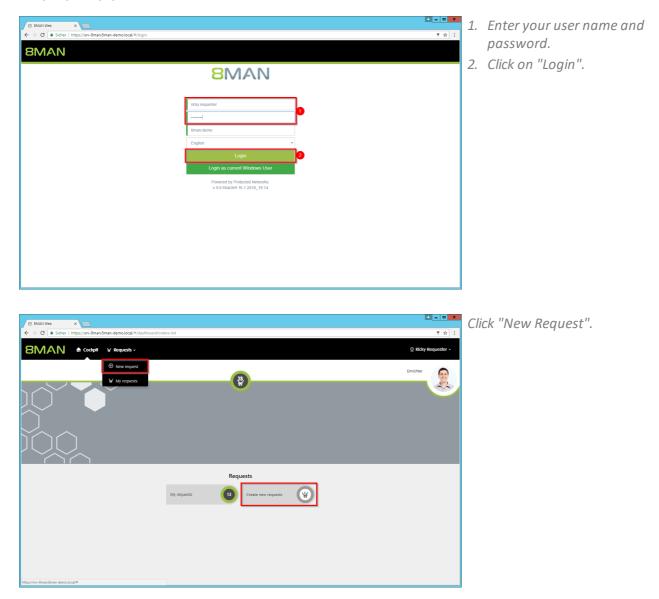
				▲ - □ ×	Cl	ick the shopping cart.
	Iman&man-demo.local/#/order:resourcetype=2:organizat	ionid=288/bt70-54ce-40ac-9eb3-tet26beb2ae		ssket 🖉 Ricky Requester →		
	Search resource	Create a new request	Q			
		Start / Search / Marketing				
	Create new objects		^			
	Action Resource		Details			
	Request Create directory		File server - Directory			
	Resources		^			
	Action Resource		Details			
	Request Events		File server - Directory \\srv-8man\Marketing\Events			
	Request Elyer		File server - Directory \\srv-8man\Marketing\Flyer			
	Request 📄 🖻 Presse		File server - Directory \\srv-8man\Marketing\Presse			
	Request	AN	File server - Directory \\srv-8man\Marketing\Produktbeschreibung 8MAN			
	Request Request Request		File server - Directory \\srv-8man\Marketing\Secret Projects			
	Request 🛛 🔁 Vorlagen		File server - Directory \\srv-8man\Marketing\Vorlagen			
B 8MAN Web ×				4 - 0 ×	1	8MAN will show you the
← → C https://srv-8	Iman.8man-demo.local/#/basket			₹☆ : ©	<u> </u>	order basket with your
8MAN	ती Home 🛛 Requesting -		Order	Basket 🖉 Ricky Requester 🗸		requests.
	Thank you for your req	uest.			2	Alternatively, delete your
	Search/Marketing		^		2.	request.
	Resource	Туре	Options 2			
	8 Create directory	File server - Directory	Flyer2017		3.	You must enter a comment,
				l		e.g. a ticket number.
					4	Close your request.
			3	0		
		Please add a	comment	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.





				_ _ ×
	s://srv-8man.8man-demo	.local/#/order;resourcetype=12;organizationId=48879852-ee97-4550-9e	53-682662 🔎 👻 🔒 🖒 🏉 8MAN Web - New Request	× îr ★ 0
8 MA	N 🕈 Hor	me 🏼 📜 Requesting -		🖉 Ricky Requester 👻
ço				
	Create a n	iew request		
	Start / HR			
\leq				
	Create new obje	cts	^	
\subseteq	Action	Resource	Details	
	Request	園 Manufacturing - new group	Create group Creates a new group	
\cup	Request	A Manufacturing - new user	Create user account Creates a new user	
	Resources		^	
	Action	Resource	Details	
	Request	B) HR	File server - Directory \\srv-8man\Organization\HR	
https://srv-8man.8n	nan-demo.local/			

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

ester 🗸

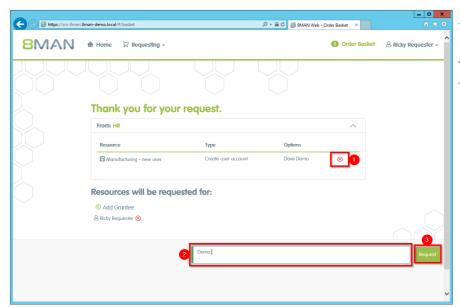
Enter the relevant information for the new user. Fields indicated in red are mandatory or contain invalid entries.

Co Co Matps://srv 8MA	∃man 3man-demolocal (#/order;esourcetype=12;ergan SAM-Account-Name User Logon Name	uztionidi-4837852-ee97-4550-9e53-683562 P = ≧ C Ø Ø SMAN Web - Nev Request > d demo		_ □ ×	After entering all required information click on "Add to shopping cart".
	User Logon Hame	a.aemoeoman-aemo.iocai			
C	Company	Example Ltd.			
Sta	Manager	CN=Adrian Stillwell,OU=TestUsers,DC=8man-demo,DC=local			
	Pors.Nr.				
	Location	Berlin	~		
	Beschreibung	This is an automatically generated description for 'Dave Demo' with the	0		
-	Password options		>		
			1		
		Add to shopping cort	Concel		

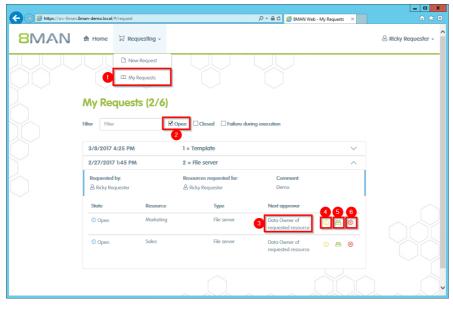
E S Attps	s://srv-8man. 8man-dem	o.local/#/order;resourcetype=12;organizationId=48879852-ee97-4550-9e	53-682662 🔎 👻 🖨 🖒 🧭 8MAN Web - New Re	uest × 👘 ★ 🔅
8 M <i>A</i>	N 🕈 Ho	me 🏼 📙 Requesting -	0	Order Basket & Ricky Requester -
r i		new request		
	Start / HR			
	Create new obje	ects	^	
\bigcup	Action	Resource	Details	
	Request	Manufacturing - new group	Create group Creates a new group	
\bigcup	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

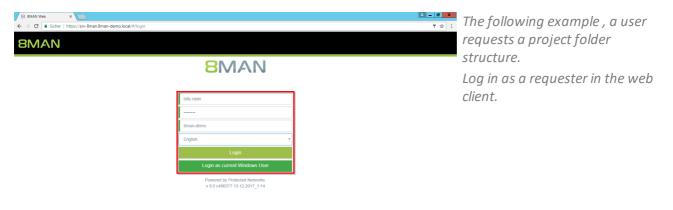
In addition to ordering user accounts, authorizations, directories or freely definable objects (OpenOrder), other script-based services can now be ordered via the web client.

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.

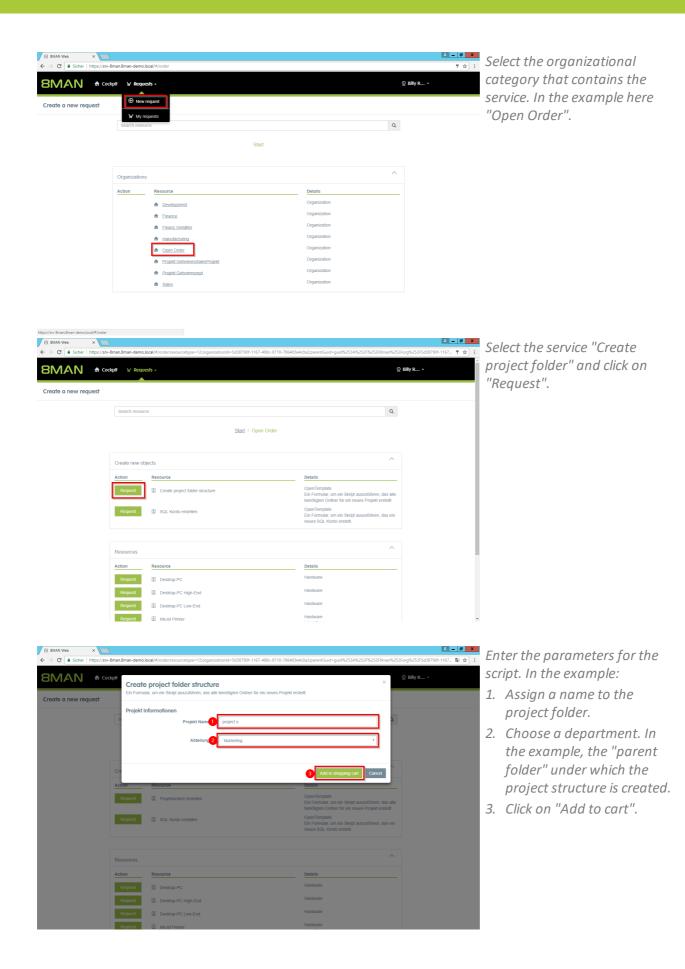
Additional Services

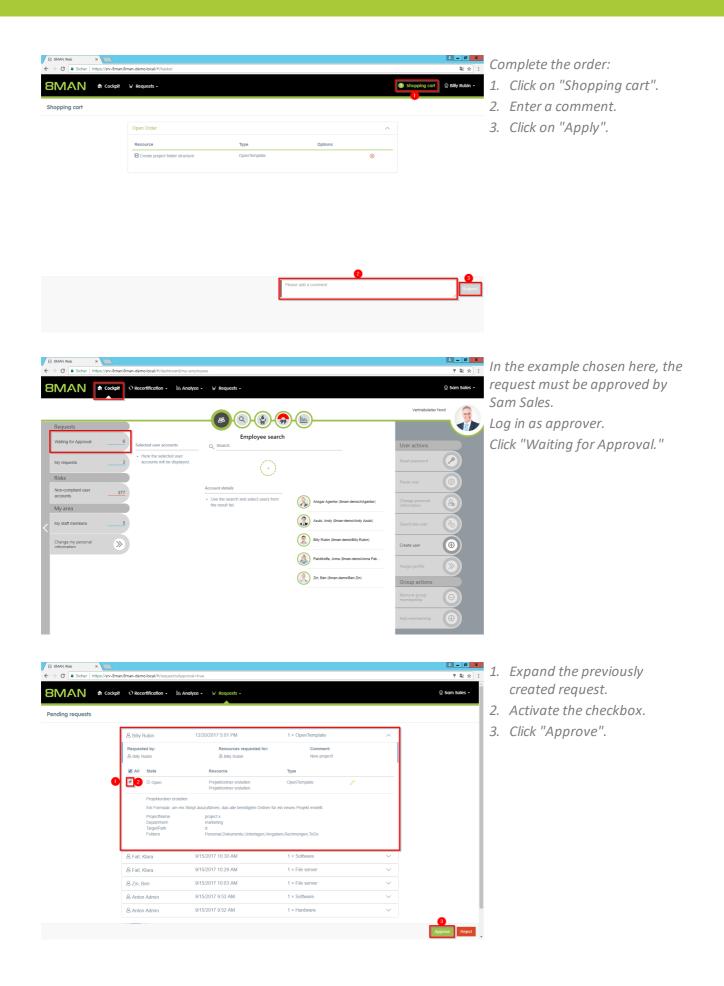
Configure a script-based service for requesting (Administrator)

Step by step process









8MAN

8MA			Search		\$			📥 Anton Admin 👻
🏫 Start 💩	Resources Permissions	ి Accounts	🕲 Dashboard 🛛 🗹	Multiselection 🛱 Log	book 🛛 🛛 Scan compa	ision		
esources	0			\$	▲ \\srv-8man\Marketing			Report
A Filter resources on .	first tree level full path	Description	Access rights Folder Size	1		(8man-demo\Administra		
Active Directory	tuli path	Description	Access rights Folder Size		Inheritance 🔒 Off		Change in	heritance
ile server					 Share Information 			
🖯 📄 🌋 srv-8man	\\srv-8man				 Access rights 			200
- 🕀 🛃 Finanz	D:\Finanz		20 Bytes		AA COA			
🕀 🛃 GF	D:\GF		6 Bytes					
🕀 🛃 Home	D/\Home		0 Byte				×	s.
🖷 🔄 п [2]	3 DAT		1 KB		NTFS	Inheritance Full control Modify Restricted	Vead and Ex Nrite Vead	ropagation
🗉 🛃 Marketing	Rescan directory		896 Bytes		INTIS	full conf Modify Restricte	bead a Write bead	ă.
- H C Personal	Nescan directory		4 Bytes			Rew Marine	8 × 8	ž
- 🕀 🛃 🌋 Vertrieb	Report: Who has access where?		344 Bytes		All permissions			
change urpose Groups	Modify access rights				- Full control		111	
	Create directory				Modify	8 🗸		00
asy Connect - CS asy Connect - SQ					Read and Execute	a	\checkmark \checkmark	000
					> E Special permission	A ✓ ✓ ✓	~	6° D
licrosoft Dynami	Change inheritance				4			
	Open Logbook					~		
	R Create alert				Accounts with permission	S All permissions		
					A Filter			34
	Copy as path				Users O Groups O C			34
					Ousers O Groups O C	ontacts 🔮 Compute	ß	
					Name		often granted li	
					Administrator (8man-demo\Ad		3 🗥	3× 🖰
					Anton Admin (8man-demo)		3 🗥	3x 🗄
					🔷 🔟 Arbeit, Andi (8man-demo\A		1	8
					Secher, Joe Kurt (8man-den		2 🕰	2×8
					 Burg, Johannes (8man-dem Clean - Admin (8man-demo 		1	8 8
					 Clean - Admin (8man-demo cradmin (8man-demo\cradmin 		3 🚯	3x 🔒
					cradmin (8man-demo\cradmin Signal Bampf, Hans (8man-demo\)		2 🕰	2x 🔂
					 Dampt, Hans (8man-demo) Dee, Dan (8man-demo)/Dan 		2 00	2×0
					Dee, Dan (sman-demo)Dan Dirk DataOwner (8man-demo)Dan		1	8
					Dink DataOwner (oman-den			

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.

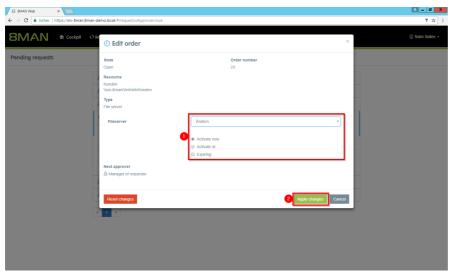
Additional Services

Overview of all cockpit services

Step by step process

B 8MAN Web × ← → C Sicher https://srv-8man.8r	nan-demo.local/#/dashboard/my-employ	rees			E = Ø ×	Cli	ick "Waiting for Approval." In
	O Recertification - III: Analyze -	- 'H' Requests -			👳 Sam Sales 🗸		e example shown, 5 requests
Requests Wating for Approval My requests Ricks Non-compliant user accounts My area My staff members Change my personal	Selected user accounts • Here the selected user account will be displayed.	Count deals	Image: Agentar (Iman-demol/Algentar) Image: Agentar (Iman-demol/Algentar) Image: Agentar (Iman-demol/Angentar) Image: Agentar (Iman-demol/	Vertrebstelet User actions Reset passord Pause user Change personal Change per		Th (b ro	e waiting for approval. he range of available services uttons) varies according to le (login), risk assessment nd configuration.
B BAAN Web x ← → C ■ Scher http://ww-bman.br BMAN ♠ codopt	nan-demo.local/#/requestsisApprovali-tru Q Recertification - Lili: Analyze -				부 (미) X 약 ☆ : Q Sam Sales -		Expand an order to see the items.
Pending requests	Artion Admin Artion Admin	9/15/2017 10.30 AM 9/15/2017 10.29 AM 9/15/2017 10.29 AM 10/15/2017 0.29 AM Resource Resource Resource (Amdem Yany-Bmamberhieb/Kunden) 9/15/2017 9.52 AM	1 × Software N 1 × File server N 1 × File server N Adenti at Ger Neise Im Vestreit, PSN: COBE0746592271 Type File server 1 × Software N 1 × Hardware N			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.





9/15/2017 10:30 AM

9/15/2017 10:29 AM

9/15/2017 10:03 AM

Reso

Kunder \\srv-8r

9/15/2017 9:53 AM 9/15/2017 9:52 AM

Resources & Zin, Ber

B 8MAN Web × ← → C ■ Sicher | https://srv-

Pending requests

8MAN & cockpit

01

& Fall, Klara

& Fall, Klara & Zin, Ben

Requested by 음 Zin, Ben

& Anton Admin

용 Anton Admin

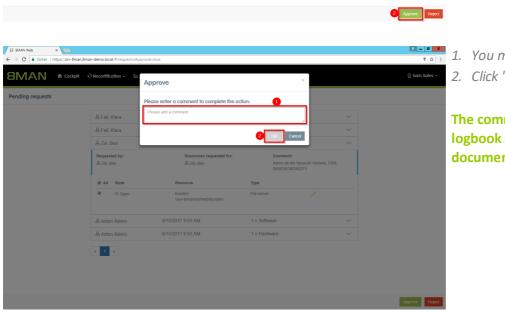
You can edit the order request.

- 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".

👳 Sam Sales 🗸



1 × Software

1 × File serve

1 × File serve

Type

File ser

1 × Hardward

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

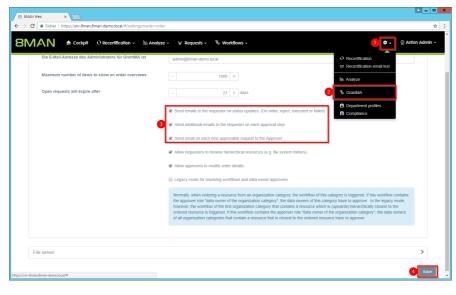
Background / Value

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

Additional services

Creating / Changing approval processes

Step by step process



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

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.

Example of an email notification.

Folgende Positionen wurden für	

Sehr geehrte(r) cradmin,

Bestellübersicht

"Für Demozwecke.

• Rosi Ne bestellt: Bestellnr. Name Typ Optionen

Rosi Ne schrieb den folgenden Bestellkommentar:

Genehmigung erforderlich

Auf der <u>8MATE GrantMA</u> Seite können Sie die Bestellung genehmigen oder ablehnen.

 Bestellnr.
 Name
 Typ
 Optionen
 Genehmigungst

 12
 IT
 Fileserver
 Ändern
 Mit freundlichen Grüßen

 8MATE GrantMA
 Status
 Status
 Status
 Status



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.

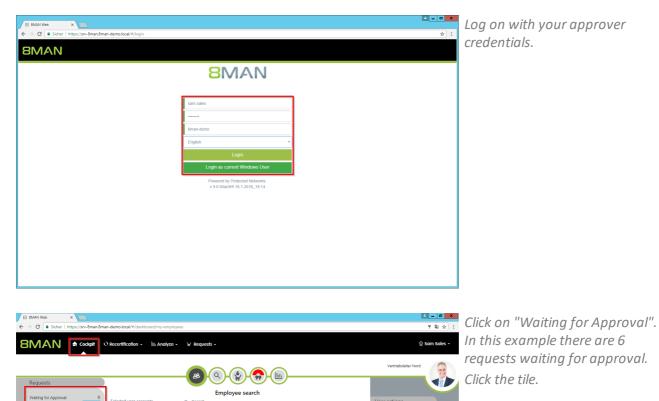
Additional Services

Defining individual approval workflows

Step by step process

>>

Change my per information



Ansgar Agentor (8man-demo/AAgento Azubi, Andy (8man-demo/Andy Azubi) Bity Rubin (8man-demo/Bity Rubin)

Pakdkoffa, Anna (8man-demolAnna Pak

2

•

	nan.8 man-demo.local /#/request;isAp		오 두 🔒 Ċ 💋 8MAN Web	- Approve X	× ☆ ☆
8MAN			questing -	- Approve	🐣 Sam Sales 🗸
	Pending Requ	iests		0	
	Ricky Requester	2/27/2017 1:29 PM	2 × File server		
	Requested by: & Ricky Requester	Resources requested for:	Comment: Demo.		
	All State	Resource	Туре	2	
<pre>h</pre>	Open	Marketing	File server	0	
\sim	Open (2)	Sales	File server	0	
					4
					Approve Reject

- 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".

	O Recertification +	Approve	×		© Sam∶
ding requests		Please enter a comment to complete the ac	tion.		
	& Fall, Klara	Please add a comment			
	& Fall, Klara		2 CK Cancel	-	
	& Zin, Ben		Cancel		
	Requested by: 음 Zin, Ben	Resources requested for: & Zin, Bon	Comment: Aaron ist der Neu 008E0974639227	e im Vertireb, PSN: '1	
	🖉 All State	Resource	Туре		
	🖉 🕐 Open	Kunden Nisry-Bman/Wertrieb/Kunden	File server		
	음 Anton Admin	9/15/2017 9:53 AM	1 × Software		
	용 Anton Admin	9/15/2017 9:52 AM	1 × Hardware		
	a 1 x				

You must enter a comment.
 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

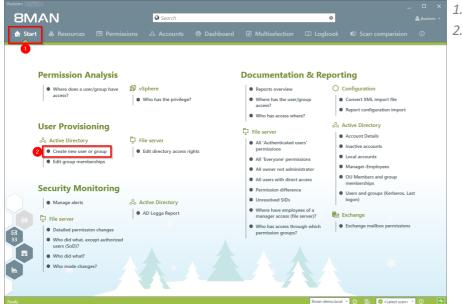
Background / Value

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

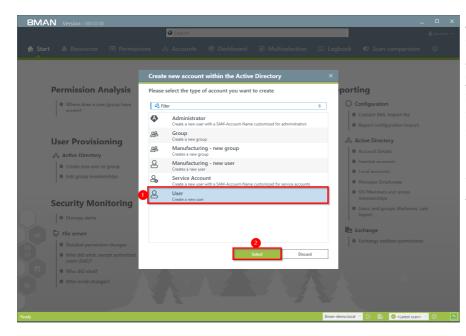
Customize templates for account creation (please refer: Templates Manual)

Step by step process



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

268 | Access Rights Management



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".

8MAN Versi	on:					_ □
		Search				
🏫 Start 💩 🛙	Create new account	t within the Active Directory				rision ①
Tr Start 69	Create elements in the	selected domain: 8man-demo.local				rision ()
	Given Name Dave		Surname Dru	ummer	^	
Perm	Common Name Dave D	rummer				
Perm	Description					
• W1	SAM Account Name Dave.D	rummer				
363	2 OU Selection CN=Us	25				lle .
	 LDAP attributes 					mport
User	Name	0	Value			
User	Comment	Attribute value is not given				
o ^S o Acti	3 Company	Attribute value is not given				
• cr	Department	Attribute value is not given				
	Display Name	Dave Drummer			<i>></i>	
• Edi	Home Directory	Attribute value is not given				
	User Principal Name	Dave.Drummer@8man-demo.local			⊘ n ∨	10
Secur	 Group membershi 	ps				a þ
Secu	Accounts	Templates Paste Clear				beros. Last
• Ma	4 Q @ marketing	× • \$		\bigcirc		
File		Name	The user	r will automatically become a member of the groups specified here.		
De De	A Marketing (8man-demo	\Marketing)	You can	either search for a group or select a group		missions
M			Too can	tomalata	~	
33 • Wr Use	Credentials 8man-demo\sa-8	imansvc				
🗐 🖷 🗰 🗰	Please add a comment			imm 🖳		
• wi					Cancel	2
	Status of changes:					
Ready				8man-demo.local 🗠	0 B 🥑 🛛	atest scan> 🕜 🕕

8MAN

- 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.

- EMAN

 Create new account within the Active Directory

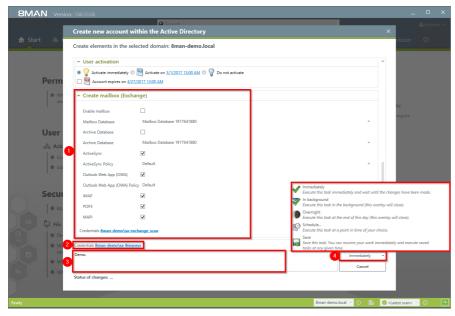
 Create elements in the selected domain: 8man-demo.local

 Perm

 Create elements in the selected domain: 8man-demo.local

 Image: Create elements in the selected domain: 6man-demo.local

 Image: Create eleme
- 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.

270 | Access Rights Management

8.1.1.2 Create groups and add users

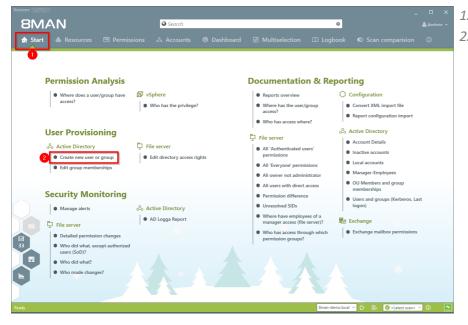
Background / Value

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

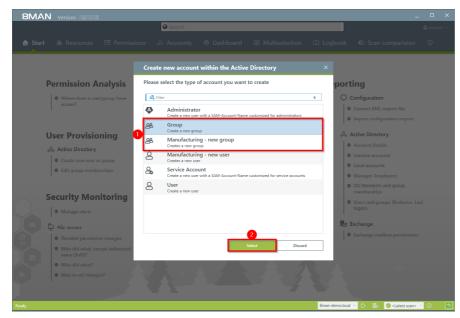
Additional Services

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".



8MAN Versi	@ Search	ا» ۵ هـ
🕈 Start 💩 Re	Create account within Active Directory ×	
	Create elements in the selected domain: 8man-demo.local	
	Common Name Demo	
Perm	Description Demo	
• wr	SAM Account Name Demo	
acc	2 OU Selection <u>OU=TestGroups</u>	
	V LDAP Attributes	
\leq	↑ Group Scope	
User	s tocal group	
Acce	© 🚱 Global group	
Cre	🛇 🍓 Universal group	
0 Ld	∧ Group Type	
	💿 🍇 Security group	
Secur	Star Distribution group	
Secur	✓ Members	
Ma		
📮 File		
27 DP		
• Wr		
USC	Credentials <u>knot set</u>	
e Wi		
• Wi	Cancel	
•	Status of changes:	

- 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.

8MAN Versie	@ Search	_ L >
🔒 Start 💩 Re	Create account within Active Directory	sion 0
	Create elements in the selected domain: 8man-demo.local	
	Description Demo	
Perm	SAM Account Name Demo	
Perm	OU Selection QU=TestGroups	
I WE	 LDAP Attributes 	
Sec.		e
	^ Group Scope	nport
(Lines)	 	
User	type undeal group	
Acce		S
Cre	 Group Type 	ons
U La	& Security group	rator
	🔘 🎭 Distribution group	cess
Cogu	 Members 	
Secur	Accounts Rate Slear	
		s of a
- mar	Users (1) specified here will automatically Ricky Requester (8man-demo\Ricky.Requester) displayname: Ricky Requester cn: Ricky Requester members of the new group.	aver)?
File	Groups (0) search for users and groups.	gh which
27 • DH		
33 W	2 Credentials < <u>not set></u>	and the second
• wi	Please add a comment	
U Wr	Cancel	
bu .	Status of changes:	
Ready	8man-demo.local 🗠 🔿 🥝 klatest	scan> > ①

- 1. You can designate users while creating the group.
- 2. Determine the login information for creating the new group in AD.

272 | Access Rights Management

8MAN

8MAN Versio	on:			_ 🗆 ×
	Search			🚔 cradmin 👻
	Create account within Active Directory			
💼 Start 💩 Re	Create elements in the selected domain: 8man-demo.local			sion U
	Description Demo		^	
	SAM Account Name Demo			
Perm	OU Selection OU TestGroups			
l • wr	 LDAP Attributes 			
acc				
	* Group Scope			nport
	S Local group			npore
User	 Inversal group Inversal group 			
& Acco				5'
	 Group Type 			
• tdi	💿 🍓 Security group			ons
1 * Lui	💿 🎭 Distribution group			rator
	^ Members		/ Immediately	DESS
Secur	Accounts Paste Clear		 Execute this task immediately and wait until the cha In background 	inges have been made.
I ● Ma	Q ricky X - 🌣		Execute this task in the background (this overlay will	l close).
	Name	The accounts sp become me		will close).
27 📮 File		You can see	Schedule Execute this task at a point in time of your choice.	
De De			Save	
• Wr	Credentials 8man-demo\sa-8man		Save this task. You can resume your work immediate tasks at any given time.	ely and execute saved
	Ticket number 12345, ordered by Sam Sales		Immediately 2	
• wr			Cancel	
	Status of changes:			
		~		
Ready			8man-demo.local · O O <lated o<="" th=""><th></th></lated>	

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

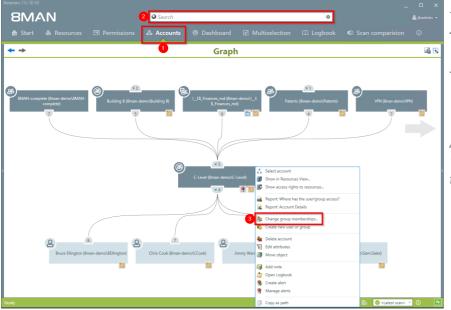
Background / Value

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



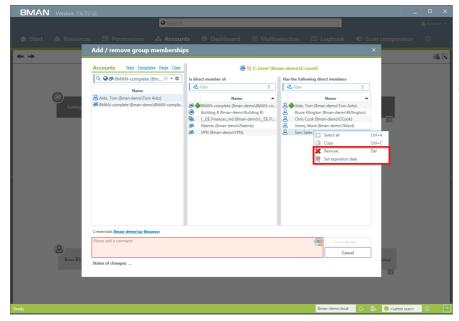
- 1. Select "Accounts".
- 2. Use the search field to find the desired account.
- 3. Right-click on the account and select "Change group memberships" in the context menu.

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

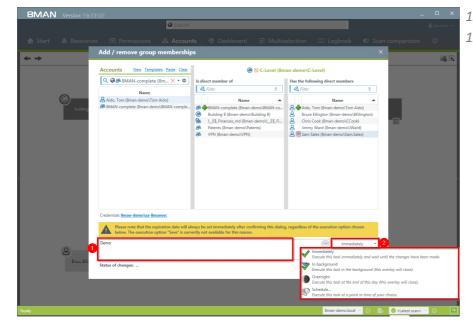
- <complex-block>

 Contrain
 <t
 - 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).

274 | Access Rights Management



Right-click and use the context menu to remove memberships (parents and children) immediately or on a designated date.



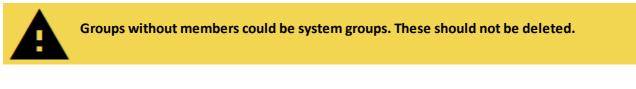
8MAN

- 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.

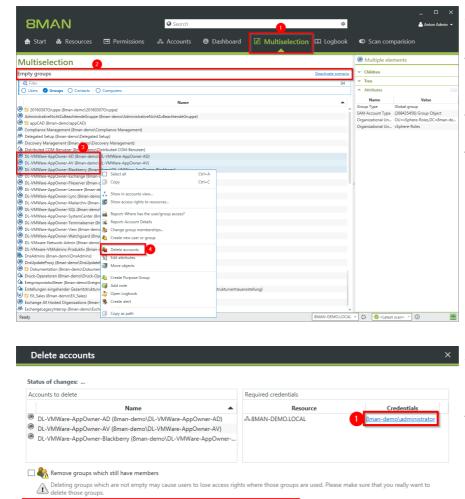


Step by step process

8MAN	Search	_ 🗆	× 1.	Select "Dashboard".
🖨 Start 💰 Resources 🖃 Permissions	& Accounts 🔞 Dashboard 🗹 Multiseled	ction 🛱 Logbook 🐠 Scan comparision	2.	Double-click on "Empt
Reporting	 Users and other accounts 		Î	groups".
	Users	382		
Active Directory	Users (Disabled)	16		
Inactive accounts	Administrators	26		
Local accounts	Administrators (Disabled)	0		
 Users and groups (Kerberos, Last logon) 	 Groups 		_	
	All Groups	278		
📮 File server	Groups with members (w/o recursions)	161		
All 'Authenticated users' 0 permissions	Empty groups A 2 Groups in recursions A	84 33		
All 'Everyone' permissions	The largest group (Domänen-Benutzer (8man-demo)	Domänen-Benutzer)) 381		
All users with direct access	Built-in security groups	27		
	Global security groups	116		
Directories without administrative owners	< Universal security groups	35		
Unresolved SIDs	Local security groups	98	_	
 Unresolved SIDs 	Global distribution groups	0		
	Universal distribution groups	2	_	
	Local distribution groups	0		
	OU / Contacts / More		_	
~	Computers	8		
	Computers (disabled)	2		
Depth of nested groups	Contacts	0		
	Foreign users	0		
43	Organizational Units	21		
8 3 1 1 1 1 1	1 Top 5 Kerberos Tokens [Bytes]		_	
1 2 3 4 5 6 7 8 9	10 Silie, Peter (8man-demo\Peter.Silie)	2016		
Depth	Krise, Christiane (8man-demo\Christiane.Krise)	1896	~	
dy		8MAN-DEMO.LOCAL 👻 💭 👩 <latest scan=""> 🗡 🛈</latest>	-de-	

© 2018 Protected Networks GmbH

276 | Access Rights Management



- 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 occurance of unresolved SIDs.

Cancel

1

Immediately

 \otimes

Remove all direct references to the selected accounts on resources which are known to 8MAN. The execution will be <u>immediately</u>

8MAN

✓ I Remove access rights

Please add a comment

Scripting

Delete accounts	:				
Status of changes:					
Remove groups which still have members					
$\overline{\Delta M}$ Deleting groups which are not empty may cause users to lose access rights where those groups are used. Please make sure that you delete those groups.	really want to				
☑ 🗐 Remove access rights					
Remove all direct references to the selected accounts on resources which are known to 8MAN. The execution will be <u>immediately</u>					
 Scripting 	the selected accounts on resources which are known to 8MAN.				
Execute script before change action					
None	Ŷ				
Execute script after change action					
None	Ý				
2 3					
Please add a comment	ncel 🛞				

- 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

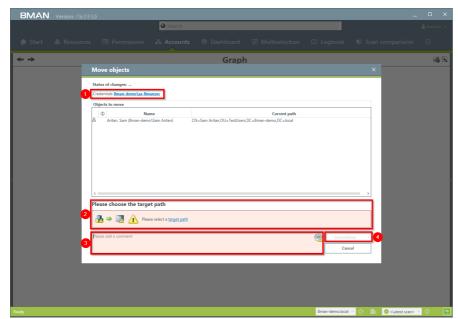
Background / Value

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.
- 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.

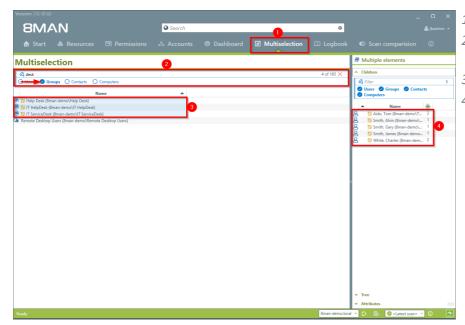


8.1.1.6 Reduce multiple groups to one group

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



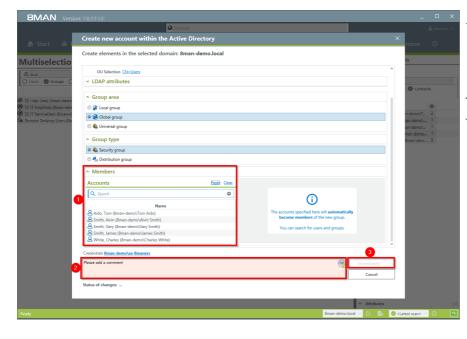
- 1. Select "Multiselection".
- 2. Apply filters to find the desired groups.
- *3. Select the groups.*
- Select all desired users and copy them into the clipboard. (For example CTRL+A and CTRL+C).

Version.									
8MAN	Search			۵					
Start 💩 Resources 🖃 Permissi			Multiselection						
Multiselection		Instante Image: Contraction of the comparison of the com							
4 desk				4 of 185 🗙	∧ Children				
O Users @ Groups O Contacts O Computers					🕰 Filter	▲ jkadmin + on ① 5 Contacts mol(T_2 2 mol(T_2 1 1 mol(T_1 1 1 mol(T_1 1 1 1 1 1 1 1 1 1 1			
Name						▲ jbadmin + ① 5 5 5 2 1 1			
B 19 Help Desk (8man-demo\Help Desk)	-				Computers				
B 10 IT HelpDesk (8man-demo\/T HelpDesk)					 Name 	*			
IT ServiceDesk (8man-demo\IT ServiceDesk)					Aido, Tom (8man-demo\T	. 2			
lemote Desktop Users (8man-demo\Remote Desktop Users)	Select all				Smith, Alvin (8man-demo\.				
	🗊 Сору	Ctrl+C			Smith, Gary (8man-demo)				
	Show in accounts view				Smith, James (8man-demo				
	Show access rights to resources				White, chanes (offian-defin.				
	Report: Where has the user/group	access?							
	Report: Account Details								
	🇞 Change group memberships								
	🗞 Create new user or group				>				
	🍇 Delete accounts								
	Edit attributes								
	Move objects								
	🍪 Create Purpose Group								
	Add note								
	🎒 Open Logbook								
	😤 Create alert								
	Copy as path								
					× Tree				
					 Attributes 	Edit			
Ready				8man-demo.loci	al 👻 📀 📑 🥝 «Latest scan» 🕚	- 0 🔤			

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

8MAN Versi			
	Search		
🍙 Start &	Create new account within the Active Directory		× rision ①
	Create elements in the selected domain: 8man-demo.local		
Multiselectio			ts
4 desk	Common Name Central Help Desk		11
🔿 Users 🕑 Groups 🤇	Description		3
	SAM Account Name Central Help Desk		Contacts
25 III Help Desk (Ilman-demo III HelpDesk (8man-dem III HelpDesk (8man-dem III ServiceDeck (8man-d Remote Desktop Users (8m	OU Selection CN=Users		
B IT ServiceDeck (8man+d	 LDAP attributes 		n-demo\T 2
Remote Desktop Users (8n)	 Group area 		an-demo\ 1
	second group		man demo 1
			8man-dem 2
	🔘 🍓 Universal group		
	↑ Group type		
	🐵 🍓 Security group		
	💿 🧌 Distribution group		
	 Members 		
	Accounts 2 Paste Clear		
	Q Bearch 🗢	\bigcirc	
	Name	The accounts specified here will automatically become members of the new group.	
	Credentials 8man-demo\sa-8mansvc		
	Please add a comment	Immediately	-
		Cancel	
	Status of changes:		
			_
		8man-demo.local - O Ba	
		8man-demo.local 🗠 🕒 🖶	📀 <latest scan=""> 🝸 🕕 🚦</latest>

- 1. Name the new group.
- 2. In the "Members" area click on "Paste".



8MAN

- 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

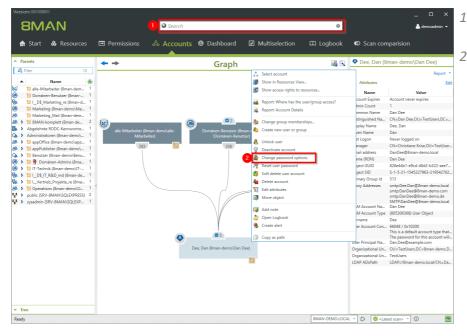
Passwords should be changed regularly. Set the required password options.

Additional Services

Change password options in bulk (web client)

Step by step process

✓ Tree Ready



- 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.

SIVIAIN Version:	Q	earch			🔔 demoadmin 👻
∧ Parents	+ +	Graph		🔣 🛛 🖗 Dee, Dan (i	
A Filter 18				Attributes	
▲ Name *				Name	Value
🖯 👘 alle Mitarbeiter (8man dem 1				Account Expires	Account never expires
) 回 Domänen-Benutzer (8man 1				Admin Count	1
I_D\$_Marketing_re (8man-d 1				Common Name	Dan Dee
Marketing (8man-demo\Ma 1				Distinguished Na	CN=Dan Dee,OU=TestUsers,DC=
B 🗇 Marketing_Mail (8n					Dan
	e password options				×
Abgelehnte RODC-Ker					r logged on
	changes: Change password options				Ihristiano Kriso,OU-TostUsi
appOffice (8man d) Credentia	ls 8man-demo\administrator				lee@8man-demo.local
> DappPublisher (8mail)		_			Dee
, > 10 Benutzer (8man de		💠 💹 Dee, Dan (8man-demo\I	an Dee)		44b1 c9cd 48d2 b322 acc7
> 10 🖻 Domänen-Adm	ser must change the password at next logo				-21-1545227963-21954276
	iser must change the password at next logo iser cannot change his password	n			
				•	:Dee.Dan@8man-demo.loca
	assword never expires			3	:DanDee@8man-demo.com :DanDee@8man-demo.de
* ≥ public (SRV-8MAN\SC	ld a comment		Ģ	Immediately	hDanDee@8man-demo.loc.
🕈 👂 sysadmin (SRV-8MAN				Cancel	06368) User Object
					_
		Dee, Dan (8man-demo\Dan Dee)		Organizational Un.	. OU-TestUsers,DC-8man demo,D . TestUsers
		B		LDAP ADsPath	LDAP://8man-demo.local/CN=Da

- 1. Set password options.
- 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

<u>Change password options in bulk</u> (web client) <u>Delete accounts in bulk (soft delete)</u> (web client)

Step by step process

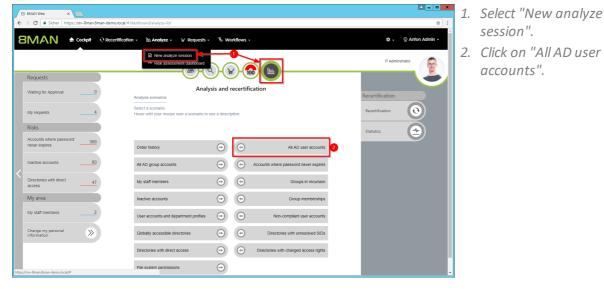
All AD user accounts All AD group accounts Accounts where passw never expires

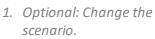
ation - 🔟 Ar

🖌 Requests + 🛚 🐁 Wo

All AD user accounts

R 8





🌣 🗸 👳 Anto

- 2. Set options for the scenario.
- 3. Click on "Start calculation".

8	BMAN Web	×		_ - •
	C 🕯	Sicher https://srv-8man.8man-demo.local/#/analyze-details;id=1:scen	old=0d55d530-e6b4-4955-add0-52d090c2156d	ф 2
8	MA	N 🖨 Cockpit O Recertification - 🔟 Analyze -	الا Requests + الله الله الله الله الله الله الله ال	🌣 🗸 👷 Anton Admin
411	AD use	r accounts (382)		
			Configuration 🌣	Reports
		0	Selected resources: 8man-demo.local	Direct Excel export
om	ain name	x	Type, Name 💌 C 🗮 🖹 😢	Create Report
	Туре	Name TRequested Action	т	 Reset password
4		ame:8man-demo.local(382 items)		Pause user
	•	Clean - Admin (8man-demo\Clean - Admin)		Change personal informat
	8	Clean - User (8man-demo\Clean - User)		
	8	sa-HQ-vRanger (8man-demolsa-HQ-vRanger)		3 Deactivate user
ł		sa-8mansvc (8man-demo/sa-8mansvc)		Remove group members
	8	sa-SP_Crawl (8man-demo\sa-SP_Crawl)		Add membership
	8	sa-SP_Profile (8man-demo\sa-SP_Profile)		Assign profile
		sa-ExcVlewer (8man-demolsa-ExcVlewer)		
	8	sa-SP_Pool_Intranet (8man-demo\sa-SP_Pool_Intr		Execute script
	8	Anna Lyse (8man-demo\Anna Lyse) sa-SP Search (8man-demo\sa-SP Search)		Soft delete user account
	8 8	Sa-SP_Search (eman-demoisa-SP_Search) Clean - Overall (8man-demoiClean - Overall)		Change password option
	••	Administrator (8man-demo\Administrator)		
	8	Bill Anz (8man-demo\Bill Anz)		
	•	Anton Admin (8man-demo/demoadmin)		
	8	sa-SP CacheADM (8man-demoisa-SP CacheAD)		

- 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

<u>Change password options in bulk</u> (web client) <u>Delete accounts in bulk (soft delete)</u> (web client)

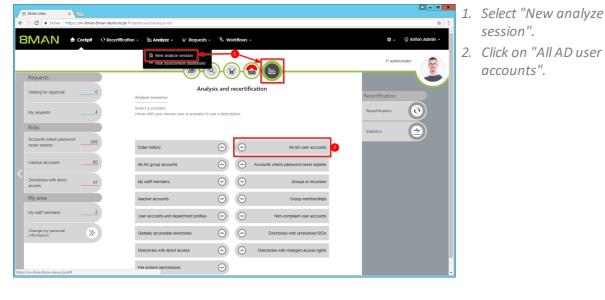
₩ Requests - 🛞 Wo

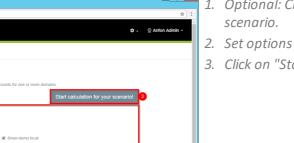
All AD user accounts

ation - 🔟 Ar

Step by step process

All AD user accounts All AD group accounts Accounts where passw never expires





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

18 E ->	C P	× Sicher https://srv-8man.8man-demo.local/#/analyze-details:id=1:scer		
31	MA		W Requests + 🖏 Workflows +	🌣 🗸 👳 Anton Admi
14	AD user	r accounts (382)		
		0	Configuration 4 Selected resources: 8man-demo local	Reports Direct Excel export
ma	in name	x	Type, Name 🔻 C 📰 🖹 🕑	Create Report
	Туре	Name TRequested Action	T	 Reset password
4 E		ame:8man-demo.local(382 items)		Pause user
	•	Clean - Admin (8man-demo\Clean - Admin)		Change personal informa
_	8	Clean - User (8man-demo)Clean - User)		
	8	sa-HQ-vRanger (8man-demolsa-HQ-vRanger)		Deactivate user
2	8	sa-8mansvc (8man-demo'sa-8mansvc)		Remove group members
	8	sa-SP_Crawl (8man-demolsa-SP_Crawl)		Add membership
	8	sa-SP_Profile (8man-demo\sa-SP_Profile)		Assign profile
	\$	sa-ExcViewer (8man-demo\sa-ExcViewer)		
	8	sa-SP_Pool_Intranet (8man-demo\sa-SP_Pool_Intr		Execute script
	8	Anna Lyse (8man-demo\Anna Lyse)		3 Soft delete user accour
	8	sa-SP_Search (8man-demo\sa-SP_Search)		Change password optio
	80	Clean - Overall (8man-demo\Clean - Overall)		
	•	Administrator (8man-demo\Administrator)		
	8	Bill Anz (8man-demo\Bill Anz)		
	\$	Anton Admin (8man-demo\demoadmin)		
	8	sa-SP_CacheADM (8man-demolsa-SP_CacheADN		
	85	Discoverysuchpostfach (8man-demo\SM_98fda74b		

- 1. Use sorting, filtering, grouping and column selection to locate the desired rows.
- 2. Select the desired entries.
- 3. Click "Soft delete user account".

- Advantage
 A control integration-demonschare demonschale (Virpragere derialisied = takenariolder 005555350 = 4064-4055 = 4865 430000021556
 A control integration-demonschare demonschare (Virpragere derialisied = takenariolder 005555530 = 4064-4055 = 4865 430000021556
 A control integration demonschare demonschare (Virpragere derialisied = takenariolder 005555530 = 4064-4055 = 4865 430000021556
 A control integration demonschare demonschare (Virpragere derialisied = takenariolder 005555530 = 4064-4055 = 4865 430000021556
 A control integration demonschare demonschare (Virpragere derialisied = takenariolder 00555530 = 4064 4055 = 4865 43000002
 A control integration demonschare demonschare (Virpragere derialisied = takenario)
 A control integration demonschare demonschare (Virpragere derialisied = takenario)
 A control integration demonschare demonschare (Virpragere derialisied = takenario)
 A control demonschare demonschare (Virpragere derialisied = takenario)
 A control demonschare demonschare (Virpragere derialisied = takenario)
 A control demonschare demonschare (Virpragere derivers derivers derivers)
 A control demonschare demonschare (Virpragere derivers)
 A co
- 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)

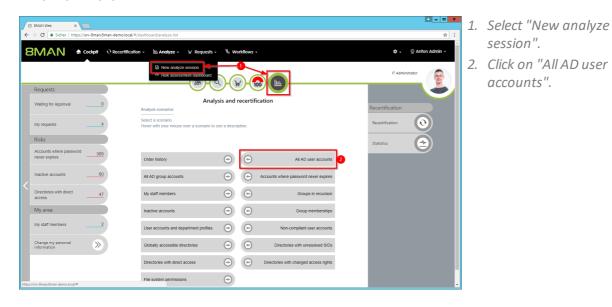
Background / Value

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



	×				-
Sicher h	https://srv-oman.oman-demo.idcai/#/analy.	28:10=00550550-60	04-4955-8000-52009	0021500	
MAN	🖨 Cockpit 🛛 Q Recertification 🗸	🔟 Analyze 🗸	₩ Requests +	% Workflows -	🗢 🗸 👷 Anton Adm
v analyze sessi	on				
		-			
	All Scenarios V		All AD user	r accounts	
•	Order history		Create a list of all	Active Directory user accounts for one or more domains.	
	All AD user accounts			Start calculation for	your scenario! 3
	All AD group accounts				
			Domain name		
	Accounts where password never expires	2			
	My staff members			🗷 8man-demo.local	
	Groups in recursion				
	Inactive accounts				
	Group memberships				
	User accounts and department profiles				
	Non-compliant user				
	accounts				
	Globally accessible directories				
	Directories with unresolved				
	SIDs				
	Directories with direct				
	access				

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

3 81 ->	C 🔒	X Sicher https://srv-8man.8man-demo.local/#/analyze-detailsid=1.scen	old=0d55d530-e6b4-4955-add0-52d090c2156d	
31	MA	N 🖨 Cockpit 🕂 Recertification - 🖽 Analyze -	₩ Requests + % Workflows +	🌣 🗸 💿 Anton Adn
AII A	AD user	accounts (382)		
			Configuration 🌣	Reports
		0	Selected resources: 8man-demo.local	Direct Excel export
oma	ain name		Type, Name 💌 C 🗉 🖭	Create Report
	Туре	Name T Requested Action	Y	 Reset password
a E	Domain na	me:8man-demo.local(382 items)		Pause user
	•	Clean - Admin (8man-demolClean - Admin)		Change personal inform
	8	Clean - User (8man-demo\Clean - User)		
	8	sa-HQ-vRanger (8man-demo\sa-HQ-vRanger)		Deactivate user
2	8	sa-8mansvc (8man-demo'sa-8mansvc)		Remove group member
	8	sa-SP_Crawl (8man-demo\sa-SP_Crawl)		Add membership
	8	sa-SP_Profile (8man-demo\sa-SP_Profile)		
	•	sa-ExcViewer (8man-demo\sa-ExcViewer)		Assign profile
	8	sa-SP_Pool_Intranet (8man-demo\sa-SP_Pool_Intr		Execute script
	8	Anna Lyse (8man-demo\Anna Lyse)		Soft delete user accou
	8	sa-SP_Search (8man-demoisa-SP_Search)		3 Change password optio
	Bo	Clean - Overall (8man-demo\Clean - Overall)		
	•	Administrator (8man-demo\Administrator)		
	8	Bill Anz (8man-demo\Bill Anz)		
	•	Anton Admin (8man-demoidemoadmin)		
	8	sa-SP_CacheADM (8man-demolsa-SP_CacheADN		
	80	Discoverysuchpostfach (8man-demo\SM_98fda74b		

- 1. Use sorting, filtering, grouping and column selection to locate the desired rows.
- 2. Select the desired entries.
- 3. Click "Change password options".

- BMAN We Code I intro (intro dema demole and intervented descende taxon of des
- 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 is 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

<u>Change password options in bulk</u> (web client) <u>Reset passwords in bulk</u> (web client)

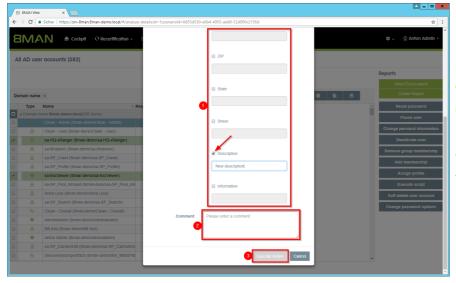
B 8MAN Web × ► ← → C ● Sicher https://stv-8man.8man-demo.local/#/d	lashboard/analyze-list		▲ _ □ ×	1.	Select "New analyze
SMAN & cockpit O Recertification	n → 🔟 Analyze → 😾 Requests →	°₀ Workflows ~	🗘 🤟 🍳 Anton Admin 🗸	2	session".
Requests Waiting for Approval 0	Risk assessment dashboard	and recertification	IT Administrator	2.	Click on "All AD user accounts".
	Analysis scenarios Select a scenario. Hover with your mouse over a scenario to see a	a description.	Recertification		
Accounts where password 369 never expires 60		All AD user accounts	Statistics		
Directories with direct		Groups in recursion			
My area My staff members 2		Group memberships Group memberships Non-compliant user accounts			
Change my personal S		Directories with unresolved SIDs			
https://srv-8man.Bman-demo.local/#		Directories with changed access rights			

	×	id=0d55d530-e6b4-4955-add0-52d030c2156d	± = □ ☆
8MAN		landossosoletan nesse autorezonado z saor Ma Analyze - Vr Requests - %, Workflows -	⊶ © Anton Admin -
New analyze sessi	on		
ſ	All Scenarios Crider history All AD user accounts All AD user accounts All AD group accounts Accounts where password never expires My staff members Groups in recursion Inactive accounts Group memberships User accounts and department profiles Non-compliant user accounts Globally accessible directories Directories with unresolved sibs Directories with direct accessible accessible directories Directories with direct accessible directories Directories	All AD user accounts Trate a list of all Active Directory user accounts for one or more domains. Comain name	ariol 3

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

ser accounts (38	×2)								
				juration 🌣 d resources: 8man-demo.lo	cal				Reports Direct Excel export
me ×				Type, Name		C 🔳	E C		Create Report
Name		Requested Action	T					-	Reset password
n name:8man-demo.l	ocal(382 items)							- 1	Pause user
Clean - User (8n	an-demo\Clean - User)							3	Change personal inform
sa-HQ-vRanger	8man-demolsa-HQ-vRanger)								Deactivate user
sa-8mansvc (8m	an-demo'sa-8mansvc)								Remove group member
									Add membership
									Assign profile
sa-SP_Pool_Intr	anet (8man-demo\sa-SP_Pool_Ir	ntr							Execute script
									Soft delete user acco
									Change password opt
Clean - Overall (3man-demo\Clean - Overall)								
Administrator (8)	nan-demo\Administrator)								Change personal information
									information
Bill Anz (8man-d Anton Admin (8r	an-demoldemoadmin)								Change the account infor
	Name Name: Iman-demo.lo Clean - Admin (8 Clean - User (8m sa-Bransve (8m sa-SP_Crank (8m sa-SP_Crank (8m sa-SP_Crank (8m sa-SP_Crank (8m sa-SP_Crank (8m sa-SP_Crank (8m sa-SP_Crank (8m sa-SP_Crank (8m sa-SP_Crank (8m))	Same Clean Admin (brank demo (back) (502 & 6ms)) Clean Admin (brank demo (back) Admin (brank de	Name Registed Action Name demoloci(302 terms) Citan - Admin (Imma-domolCican - Admin) Citan - Admin (Imma-domolCican - User) Set Hold - Administration (Imma-domolCican - User) Sa Hold - Manager (Imma-domolCican - User) Set Hold - Administration (Imma-domolCican - User) Sa Hold - Manager (Imma-domolCican - User) Set Hold - Administration (Imma-domolCican - User) Sa Hong - Card (Imma-domolCican - Set Control (Imma-domolCica	Isame Requested Action v Isame: Branckens Jocal/302 firms) Clean. After (Rman demolClean - After (Rman demolClean - After (Rman demolClean - User) Isame (Rman demolClean - User) Isame (Rman demolClean - User) Isame Action demolClean - User) Isame (Rman demolClean - User) Isame (Rman demolClean - User) Isame (Rman demolClean - User) Isame Action demols AFD Actions Isame (Rman demole Arrows) Isame (Rman demole Arrows) Isame (Rman demole Arrows) Isa B-Typefile (Rman demole AFD Actions) Isame (Rman demole AFD Actions) Isame (Rman demole Arrows) Isa B-Typefile (Rman demole Arrows) Isame (Rman demole Arrows) Isame (Rman demole Arrows) Isame (Rman demole Arrows) Isa B-Typefile (Rman demole Arrows) Isame (Rman demole Arrows) Isame (Rman demole Arrows) Isame (Rman demole Arrows) Isa B-Typefile (Rman demole Arrows) Isame (Rman demole Arrows) Isame (Rman demole Arrows) Isame (Rman demole Arrows) Isa B-Typefile (Rman demole Arrows) Isame (Rman demole Arrows) Isame (Rman demole Arrows) Isame (Rman demole Arrows)	Imme Requested Action Variance Eminanciema.ideexia/decal/202 Zermin) Cleans - Admin Mandema/Cleans - Admin Mandema/Cleans - Admin Mandema/Cleans - User) Cleans - Marine Indema/Cleans - User) Sea House Cleans - Admin Mandema/Cleans - User) Sea House Cleans - Admin Mandema/Cleans - User) Sea House Cleans - Admin Mandema/Cleans - User) Sea House Cleans - Admin Mandema/Cleans - User) Sea House Cleans - Admin Mandema/Cleans - User) Sea Sea Profile (Imma-demonals Sea P., Chroll) Sea Sea P., Chrolle (Imma - Admina) Sea Sea P., Pool (Immark Cleans - Admina) Sea Sea P., Chroll (Imma - Admina) Ama Lyse (Imma - Admina) Lyse) Sea Sea P., Cleans - Admina) Sea Sea P., Cleans - Admina) Sea Sea P., Cleans - Admina)	Name PRequested Action v Name: Endam. Admini (Riman demosicilization - User) Clean - Marine (Riman demosicilization - User) Clean - Marine (Riman demosicilization - User) Sa Horave (Riman demosicilization - User) Sa Horave (Riman demosicilization - User) Sa Horave (Riman demosicilization - User) Sa Horave (Riman demosicilization - User) Sa Horave (Riman demosicilization - User) Sa Sa P., Dorate (Riman demosicilization - User) Sa Sa P., Dorate (Riman demosis Sa P., Dorate) Sa Sa P., Profile (Riman demosis Sa P., Dorate) Sa Sa P., Pool (Riman demosis Sa P., Pool	Name Requisited Action Chana. Admin (dama demolosal)/02 (timm) Chana. Mana (dama demolosal)/04 (timm) Chana. Mana (dama demolosal-10-Matager) Sa Hours (finan demolosal-10-Matager) Sa Hours (finan demolosal-10-Matager) Sa Hours (finan demolosal-10-Matager) Sa Hours (finan demolosal-10-Matager) Sa Hours (finan demolosal-10-Matager) Sa Bor, Drottle (finan demolosal SP, Drott) Sa SP, Pool (finan demolosal SP, Pool (Image: Requested Action Chain: Administration (Sean Action (Sean Act	Name FRquested Action Name France Mana demolocal SIZ terms) Clean. Admin (and motical set) Set Clean. Mana (and motical set) Set as How (finan demolocal set) Set as Banarys (finan demolocal set) Set as Particles (finan demolocal set) Set as Banarys (finan demolocal set) Set as Parti (finan demolocal set) Set

- 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 <u>knowledgebase</u> (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

8MAN

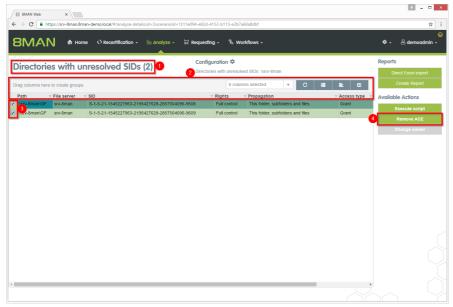
B 8MAN Web ×		L _ O X
← → C ■ Sicher https://srv-8man. SMAN ♠ Cockpit	Brean-demolocal/#/databoan/(analyze-list © Reccetification = <u>Ma</u> Analyze - W Requests = % Workflows =	🖈 🗄
	New analyze session Arcan second end of the second end of	IT Adminstrator
Requests Waiting for Approval	2 Analysis and recertification Directories with unresolved SID:	Recertification
My requests	Create a list of directories that have access control entries (ACE) from accounts that can not be resolved by Active Directory (AD). You can remove ACE's in bulk.	Recertification
Risks		Statistics
Accounts where password 361	Order history Order Al AD user accounts	
Inactive accounts6	All AD group accounts	
Directories with direct 4	7 My staff members Groups in recursion	
My area	Inactive accounts 💿 💿 Group memberships	
My staff members	2 User accounts and department profiles Non-compliant user accounts	
Change my personal Second	Globally accessible directories 💿 🕞 Directories with unresolved SIDs 2	
	Directories with direct access \bigcirc \bigcirc Directories with changed access rights	
https://srv-8man.8man-demo.local/#/analyzejid=131	File system permissions	

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

· · · · · · · · · · · · · · · · · · ·					a - D
← → C Sicher https;	//srv-8man.8man-demo.local/#/analyze	xid=1311e094-e82	d-4152-b113-e2b7a6	0a8dbf	兌
8MAN 🗕	Cockpit O Recertification -	🔟 Analyze 🗸	₩ Requests +	% Workflows -	- 🔍 Anton Admin -
New analyze session					
	All Scenarios \checkmark		Directories	with unresolved SIDs	
	Order history			ectories that have access control entries (ACE) from accounts that can not be resolved by Active u can remove ACE's in bulk.	
	All AD user accounts			Start calculation for your scenariol	2
	All AD group accounts	- I			1
	Accounts where password never expires		File server		
	My staff members			✓ Visrv-8man	
	Groups in recursion				
	Inactive accounts				-
	Group memberships				
	User accounts and department profiles				
	Non-compliant user accounts				
	Globally accessible directories				
	Directories with unresolved SIDs				
	Directories with direct access				

- 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".



B 8MAN Web X			≜ = □ ×	1.
	d=3:scenariold=1311e094-e82d-4152-b113-e2b7a60a8dbf		± : ⊕	2.
8MAN ♠ Home ♥ Recertification Re	emove ACE	×	♥ - A demoadmin -	
Directories with unresolved SID	Execute for \\srv-8man\GF, \\srv-8man\GF Comment Please enter a comment		Reports Direct Excel export	The
Drag columns here to create groups.			Greate Report	
Path ▼ File server ▼ SID ✓ Nsrv-8man\GF srv-8man S-1-5-21-1545227963-2		Grant		the
✓ \\srv-8man\\GF srv-8man S-1-5-21-1545227963-2	2 Execute	Action Grant	Remove ACE	the
_			Change owner	"Jc
		,		

- . 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)

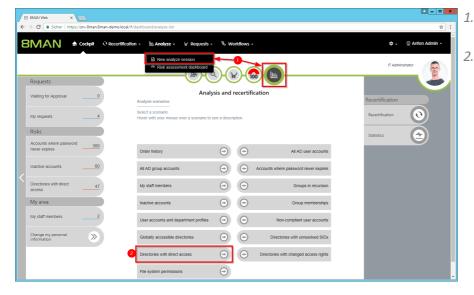
Background / Value

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.

<u>Change password options in bulk</u> (web client) <u>Remove unresolved SIDs in bulk</u> (web client)



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

	s://srv-8man.8man-demo.local/#/analyz			▲ ■ ■ ×
				A
8MAN 4	Cockpit O Recertification -	🔟 Analyze 🗸	∀ Requests - 🖏 Workflows - 🗘	🗸 👳 Anton Admin 🗝
New analyze session				
	All Scenarios V		Directories with direct access	
	Order history		Create a list of directories where users have direct permissions. This approach disrupts the best practices of entitlement and can lead to security risks, You can remove direct permissions in bulk.	
	All AD user accounts		Start calculation for your scenario!	2
	All AD group accounts Accounts where password		File server	1
	never expires My staff members	0		
	Groups in recursion		🐼 Visrv-8man	
	Inactive accounts			-
	Group memberships User accounts and			
	department profiles			
	Non-compliant user accounts			
	Globally accessible directories			
	Directories with unresolved SIDs			
	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".

I Analyze -)	र Requesting + 🐁 Workflows +	🌣 ~ 🛆 demoadm
	Configuration 🌣	Reports
	2 Directories with direct access: \\srv-8man	Direct Excel export
	8 columns selected 💌 C 🗮	E C Create Report
¥ File server	V Name V Distinguished Name	y Domain nam Available Actions
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC Execute script
srv-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
n srv-8man	Claire Gr CN=Claire Grube,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
srv-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
	Andyze X Plesever Sry-6man Sry-6man Sry-6man Sry-6man Sry-6man	Configuration Configur



Remove	e ACE	×		
rectories with direct access (1 🛛 🛛				
	recute for list.	8man/Marketing/Flyer/France, \\srv-		Reports
	nan\Marketing\F	Iyer\France, \\srv-8man\Marketing\Flyer\France,		
g columns here to create groups. (14		ting\Flyer\GB, \\srv-8man\Marketing\Flyer\GB,	= <u></u> C	Create Report
ath v	Comment	Please enter a comment	T Domain nam +	Available Actions
srv-8man\Marketing\Flyer\USA	•	9 1	8MAN-DEMC	Execute script
srv-8man\Marketing\Flyer\USA		h	8MAN-DEMC	
srv-8man\Marketing\Flyer\Germany\moved			8MAN-DEMC	Remove ACE
srv-8man\Marketing\Flyer\Germany\moved		2 Execute Action Cancel	8MAN-DEMC	
srv-8man\Marketing\Flyer\Germany\moved			8MAN-DEMC	
srv-8man\Marketing\Flyer\Germany srv	v-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=loca	al 8MAN-DEMC	
srv-8man\Marketing\Flyer\Germany srv	v-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC	
srv-8man\Marketing\Flyer\Germany srv	v-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC	
srv-8man\Marketing\Flyer\GB srv	v-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC	
srv-8man\Marketing\Flyer\GB srv	v-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=loca	al 8MAN-DEMC	
srv-8man\Marketing\Flyer\GB srv	v-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC	
srv-8man\Marketing\Flyer\France srv	v-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC	
srv-8man\Marketing\Flyer\France srv	v-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=loca	al 8MAN-DEMC	
srv-8man\Marketing\Flyer\France srv	v-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC	
srv-8man\Marketing\Flyer srv	v-8man	Peer Sie CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=loca	al 8MAN-DEMC	
srv-8man\Marketing\Flyer srv	v-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC	
srv-8man\Marketing\Events\xplizite Events\Etablissements in Ungarn srv	-8man	Claire Gri CN=Claire Grube,OU=TestUsers,DC=8man-demo,DC=	local 8MAN-DEMC	
srv-8man\Marketing\Events\The Art of Security 2011 srv	v-8man	cradmin CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC	
	v-8man			

- 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)

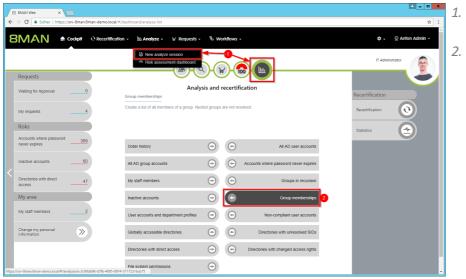
Background / Value

Remove lots of group memberships fast using the web client.

Additional Services

Managing group memberships (rich client)

Step by step process



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

Core a list of all members decursion only All AD user accounts All AD group accounts Accounts where passavord never expires All AD group accounts Accounts where passavord never expires All AD group accounts Accounts where passavord never expires All AD group accounts All AD gr	ıp.
All Scenarios Order history All AD user accounts All AD group accounts All AD group accounts All AD group accounts All AD group accounts An ever expires My staff members Groups in recursion Inactive accounts department profiles Non-compliant user accounts Globally accossible	
Unecomes Directories with unresolved SIDs	



88	MAN We	b ×						4 - 0
← →	C	https://srv-8man.8man-demo.local/4	//analyze-detail	s:id=5:scenariold=3c90db66-b5fb-4095-89	14-3717231bcb75			\$
81	M	N 🕈 Home 🔍 Recei	rtification +	🔟 Analyze 🗸 🄀 Requesting 🗸	🗞 Workflows 🗸			🌣 🖌 🐣 demoadmin 🗸
Gr		memberships (4)		Configuratio	n ‡			Reports
Gr	pup	memberships (4)		C-Level (8man-	-demo\C-Level)			Direct Excel export
Drag	columns	here to create groups.			4 columns selected	✓ C III	E 6	Create Report
Тур	oe (grou	Name (group)	Type (mem.	.Name (member)	T Requested Act	ion T		Available Actions
	۲	C-Level (8man-demo\C-Level)	8	Ansgar Agentor (8man-demo\AAgentor)				Execute script
3		C-Level (8man-demo\C-Level)		Krise, Christiane (8man-demo\Christiane	e.Krise)			Remove membership
	8	C-Level (8man-demo\C-Level) C-Level (8man-demo\C-Level)	8	Sille, Peter (8man-demo\Peter.Sille) Hacke, Petra (8man-demo\Petra.Hacke)				

- 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".

	🔨 🔊 🕈 Home 🔍 Reci	Remo	ove member	rship	×	🌣 🖌 🛆 demoadn
quo	memberships (4)	Ð	tecute for Krise, Ch	ristiane (8man-demo\Christiane.Krise)		Reports
	s here to create groups.		Comment	Please enter a comment		Direct Excel expor
pe (gro	uName (group)	Type (mi	•	1		Available Actions
8	C-Level (8man-demo\C-Level)	8				Execute script
0	C-Level (8man-demo\C-Level)	*				
8	C-Level (8man-demo\C-Level) C-Level (8man-demo\C-Level)	8		2 Execute Acti	on Cancel	

- 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

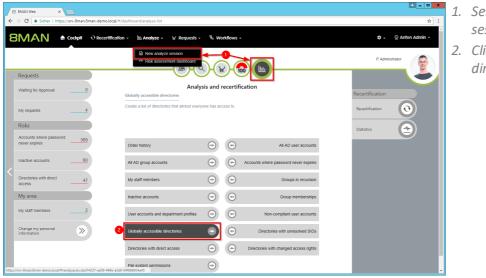
If "Everyone accounts" are used for the assignment of access rights, (almost) everyone has access to the connected resources. The consequence is an excessive assignment of access rights and a high probability for unauthorized access. These go against the principle of least privilege and should therefore 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

<u>Report: Identify usage of "Everyone"</u> (rich client) <u>Report: Identify usage of "Authenticated Users"</u> (rich client)



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



🔨 🔿 🛔 Cockpit 🔍 Recertification -	🔟 Analyze 🗸 🖌 Requests 🗸 🖏 Workflows 🗸 🔹 💭 Anton A
All Scenarios 🗸 🗸	Globally accessible directories
Order history	Create a list of directories that almost everyone has access to.
All AD user accounts	Start calculation for your scenario
All AD group accounts	
Accounts where password never expires	Group selection
My staff members	All "Everyone" permissions
Groups in recursion	All 'Authenticated Users' permissions
Inactive accounts	All 'Domain Users' permissions
Group memberships	
User accounts and department profiles	Additional group Search for group O -
Non-compliant user accounts	
Globally accessible directories	
Directories with unresolved SIDs	Paths
Directories with direct	2

- 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.

BMAN 🗕 🗠	me 🕂 Recertification 🗸 🔟 Ana	lyze - 🛛 🛛 Requesting -	🗞 Workflows -				\$- &	demoadmin
Globally accessib	le directories (51)	Configurat All 'Everyone 2 permissions	ion 💠 ' permissions, All 'Authent	icated Users'	permissions, All 'I	Domain Users'		Excel export
rag columns here to create groups	8.		3 columns selected	Ŧ	C 🔳	E C	1	te Report
Path				Account	Rights Y	Requested Action	Available A	ctions
\\srv-8man\clean! source\clean! 1	1/05 - NULL DACL/NullDACL				Full control			ute script
\srv-8man\cleanI source\cleanI 1	I\10 - Ungewollte Berechtigung definiert\J	ederBerechtigung		Everyone	Full control		4 Rem	ove ACE
sry-8man\clean! source\clean! 1	I\10 - Ungewollte Berechtigung definiert\J	ederErstBesiAuthBen		Everyone	Full control			
av-8man\clean1 source\clean1 2	2/05 - NULL DACL/NUIDACL			Everyone	Full control			
\\srv-8man\cleanI source\cleanI 2	2\10 - Ungewollte Berechtigung definiert\J	ederBerechtigung		Everyone	Full control			
\\srv-8man\clean! source\clean! 2	2\10 - Ungewollte Berechtigung definiert\J	ederErstBesiAuthBen		Everyone	Full control			
\\srv-8man\clean1 source\clean1 3	3/05 - NULL DACL/NUIDACL			Everyone	Full control			
\\srv-8man\clean! source\clean! 3	3\10 - Ungewollte Berechtigung definiertU	ederBerechtigung		Everyone	Full control			
\srv-8man\clean! source\clean! 3	3\10 - Ungewollte Berechtigung definiert\J	ederErstBesiAuthBen		Everyone	Full control			
\\srv-8man\cleanI source\cleanI 1	10/05 - NULL DACL/NullDACL			Everyone	Full control			
\\srv-8man\clean! source\clean! 1	10\10 - Ungewollte Berechtigung definiert	JederBerechtigung		Everyone	Full control			
\srv-8man\clean! source\clean! 1	10\10 - Ungewollte Berechtigung definiert	JederErstBesiAuthBen		Everyone	Full control			
\srv-8man\clean1 source\clean1 6	5/05 - NULL DACL/NullDACL			Everyone	Full control			
\srv-8man\clean! source\clean! 6	3\10 - Ungewollte Berechtigung definiert\J	ederBerechtigung		Everyone	Full control			
\\srv-8man\clean! source\clean! 6	5\10 - Ungewollte Berechtigung definiert\J	ederErstBesiAuthBen		Everyone	Full control			
\srv-8man\cleanI source\cleanI 5	5/05 - NULL DACL/NullDACL			Everyone	Full control			
\srv-8man\clean! source\clean! 5	5\10 - Ungewollte Berechtigung definiert\J	ederBerechtigung		Everyone	Full control			
				Everyone	Full control			
\\srv-8man\clean! source\clean! 5	5\10 - Ungewollte Berechtigung definiert\J	ederErstBesiAutnBen		Lveryone	1 un conta or			

- 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".

O https://srv-8man.8man-demo.local/#/analyze-detailsi	d=1;scenariold=ded14237-ae59-499e-a3d0-04f888954a	45		\$
	move ACE		×	🌣 🚽 🗟 demoadmin
be all a supervisite to all us at a visual				Reports
lobally accessible directories	Execute for \\srv-8man\clean! source\clean! 10 Berechtigung definiert\.lederBerechtigung	10 - Ungewollte	, All 'Domain Users'	Direct Excel export
	Comment Please enter a comment			
g columns here to create groups.	0		I L C	
ath 🛦			TRequested Actio	Available Actions
srv-8man\clean! source\clean! 10\05 - NULL DACL\NullDAC				
srv-8man\cleanI source\cleanI 10\10 - Ungewollte Berechtic		Execute Action Canc		
srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtic	2	Execute Action Cano	el .	
srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung d	efiniertWederErstBesiAuthBen	Authenticat(Full	control	
srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung d	efiniertUederErstBesiAuthBen	Everyone Full		
srv-8man\cleanI source\cleanI 1\10 - Ungewollte Berechtigung de	Iniert/AuthentifizierteBenutzerBerechtigung	Authenticat(Full)		
srv-8man\cleanI source\cleanI 1\10 - Ungewollte Berechtigung de	IniertJederBerechtigung	Everyone Full	control	
srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung de	finiert\JederErstBesiAuthBen	Everyone Full		
srv-8man\cleanI source\cleanI 1\10 - Ungewollte Berechtigung de	IniertUederErstBeslAuthBen	Authenticat(Full)	control	
srv-8man\clean! source\clean! 2\05 - NULL DACL\NullDACL		Everyone Full		
srv-8man\cleanI source\cleanI 2\10 - Ungewollte Berechtigung de	finiert\AuthentifizierteBenutzerBerechtigung	Authenticate Full		
srv-8man\cleanI source\cleanI 2\10 - Ungewollte Berechtigung de	Inlert\JederBerechtigung	Everyone Full		
srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung de	Iniert\JederErstBesiAuthBen	Everyone Full		
srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung de	iniert\JederErstBesiAuthBen	Authenticat(Full)		
srv-8man\clean1 source\clean1 3\05 - NULL DACL\NullDACL		Everyone Full		
srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung de		Authenticate Full		
srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung de		Everyone Full		
srv-8man\cleanI source\cleanI 3\10 - Ungewollte Berechtigung de	InlertUederErstBesiAuthBen	Authenticate Full		

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)

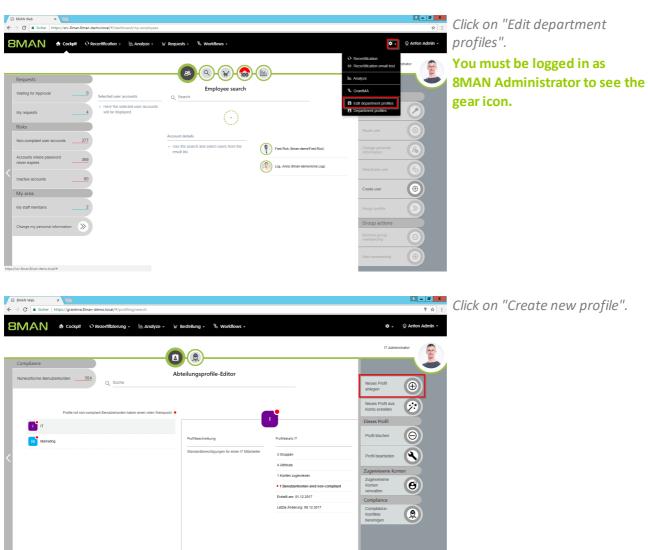
Background / Value

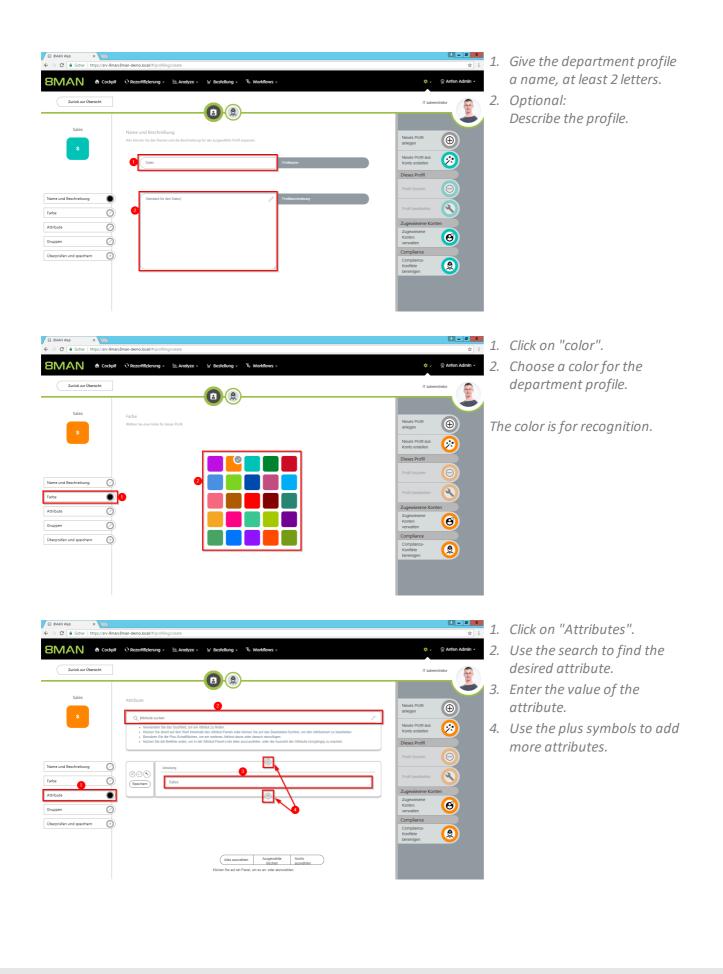
8MAN sets new standards in the field of user provisioning: With the introduction of departmental profiles, department heads, together with the management and the compliance officer, define the scope of action of employees in the company.

Department profiles can contain attributes and group memberships.

Additional Services

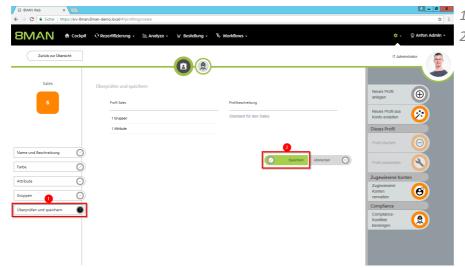
Assign a department profile to users (Cockpit) Determine permissions deviating from the department profile (compliance check)







S MAN Web x S Man Mapping Menalization (%)profiling/cruste S MAN A Cockpit O Recentificierung - Ma Analyze - V Bestellung - % Worldows -	1. Click on "Groups". 2. Find the desired group.
Zurkk arr Übersicht (1) (2) Sales Groppen (2) S (2) (2) Q (2) (2) Name und Beschreibung (2) (2) Farle (2) (2) Kathout (2) (2) (2) Groppen (2) (2) Groppen (2) (2) Groppen (2) (2) Uberpolden und speichem (2)	 Administrative Administrating Administrating Administrating



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

8MAN

÷	O Sicher https://srv-8man.8mar	n-demo.local/#/dashboard/analyze-list				☆
8	SMAN & cockpit Q	Recertification - Manalyze - W Requests -	% w	orkflows		🌩 🗸 🝥 Anton Admin -
		New analyze session Risk assessment dashboard				IT Adminstrator
	Requests					
	Waiting for Approval0	Analysis scenarios	sis and	recerti	fication	Recertification
	My requests4	Select a scenario. Hover with your mouse over a scenario to	see a descr	iption.		Recertification
	Risks					Statistics
	Accounts where password	Order history	•	\odot	All AD user accounts	
	Inactive accounts60	All AD group accounts	Ð	T	Accounts where password never expires	
	Directories with direct47	My staff members	⊖	\odot	Groups in recursion	
	My area	Inactive accounts	0	\odot	Group memberships	
	My staff members 2	User accounts and department profiles	0	I	Non-compliant user accounts	
	Change my personal S	Globally accessible directories	0	\odot	Directories with unresolved SIDs	
ľ		2 Directories with direct access	•	\odot	Directories with changed access rights	
		File system permissions	(\rightarrow)			

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

·	×			- -
← → C Sicher ht	ttps://srv-8man.8man-demo.local/#/analyz	1311e094-e82d-4152-b113-e2b7a60a8dbf		\$
8MAN	✿ Cockpit ① Recertification →	Analyze - W Requests - % Workflows -	¢- 9	2 Anton Admin -
New analyze sessio	20			i.
New unuiyze sessio				
	All Scenarios V	Directories with unresolve	ed SIDs	
	Order history	Create a list of directories that have access Directory (AD). You can remove ACE's in t	a control entries (ACE) from accounts that can not be resolved by Active	
	All AD user accounts		Start calculation for your scenariol 2	
	All AD group accounts			
	Accounts where password never expires	File server		
	My staff members		Visrv-8man	
	Groups in recursion			
	Inactive accounts			
	Group memberships			
	User accounts and department profiles			
	Non-compliant user accounts			
	Globally accessible directories			
	Directories with unresolved SIDs			
	Directories with direct access			

Directories with unresolved SIDs (2)

0

- 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.

± _ 0 X

• • • • •

3. Click "Execute Script".

- MANY We
 Metric Market demokration of Market demokration
- 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

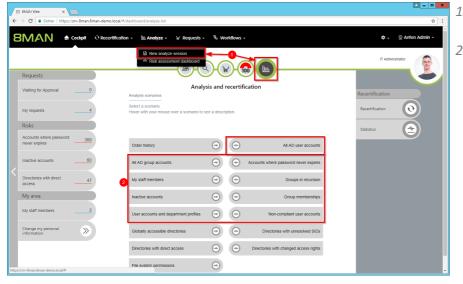
Further necessary steps and details for configuring scripts can be found in the Installation and Configuration Manual.

Additional Services

Execute scripts on directories in bulk (web client)

Step by step process

8MAN



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

B 8MAN Web					<u>▲</u> = □ ×
← → C 🔒 Sicher htt	ps://srv-8man.8man-demo.local/#/analyze	kid=0d55d530-e6t	04-4955-add0-52d09	0c2156d	☆ :
8MAN	🖨 Cockpit 🛛 Recertification +	🔟 Analyze 🗸	₩ Requests +	% Workflows - ∳ -	👳 Anton Admin -
New analyze sessio	n				
	All Scenarios V		All AD user	r accounts	
	Order history		Create a list of all	Active Directory user accounts for one or more domains.	
	All AD user accounts			Start calculation for your scenario!	
	All AD group accounts		Domain name		
	Accounts where password never expires	0			
	My staff members			8man-demo.local	
	Groups in recursion				
	Inactive accounts				
	Group memberships				
	User accounts and department profiles				
	Non-compliant user accounts				
	Globally accessible directories				
	Directories with unresolved SIDs				
	Directories with direct access				

8 8MAN Web

All AD user accounts (382)

0

¥ R

- 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".

- - X

🄹 - 👳 An

C II E C

- Analyses
 Control of the second data of the
- 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)

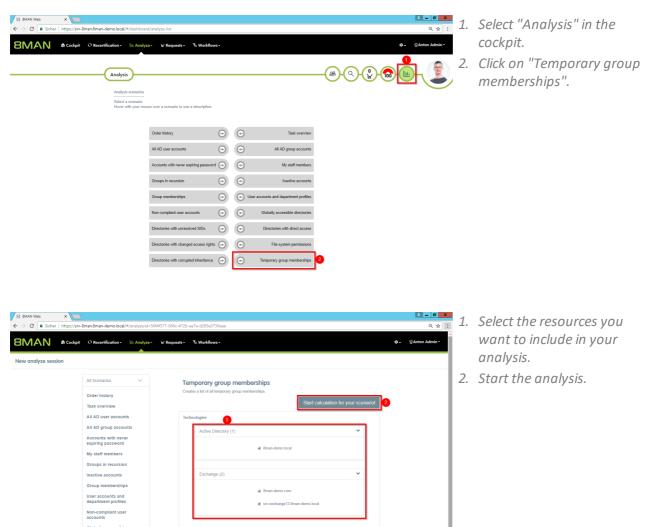
Background / Value

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





Directories with unresolv SIDs Directories with direct access Directories with changed access rights

B 8MAN Web X								A - 0 X
← → C ■ Sicher http	os//grantma.8man-demo.local/#/ana)	yze-details;id=1;scenariold=50f4f	377-586c-472b-aa7a-d283e3730ea					\$
8MAN	Cockpit O Recertification -	hii Analyze - 🖌 Reque	ils - 🐁 Workflows -					💠 - ©Anton Admin -
Temporary group m	emberships (1)							
			Configuration 🌣				Repor	rts
			Selected resources: 8	man-demo.local				Direct Excel export
Technology ×			6	columns selected 🛛 👻	C II 1	C		Create Report
	T Group type Group name	T Account ty	Account name	T Expire date T Re	quested Action	T	2	Remove expiration date
A Technology Active Dire SMAN-DEMO LOCAL				12/31/2018			3 R	temove group membership
SMAN-DEMO.LOCAL	C-Level (8man-dem	lo/G-Level)	Aloe, Vera (8man-demo/Vera Aloe	12/31/2018			4	Change expiration date
							_	

- 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.

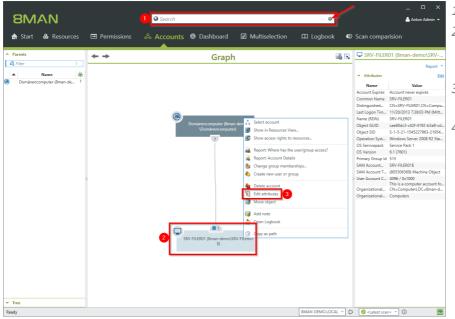
8.1.1.20 Edit computer accounts

Background / Value

Maintain computer accounts comfortably and documented within 8MAN.

Additional Services

Delete computer accounts



- 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".



Status of changes: Active Directory change (credentials <u>8man-demo\administrator</u>
C	SRV-FILER01 (8man-demo\SRV-FILER01\$)
Name	① Value 1
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 comme	ent A Immediately

- 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

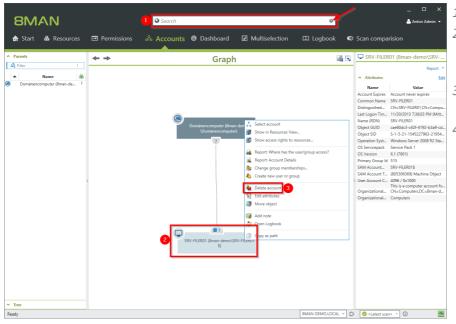
Background / Value

Delete computer accounts comfortably and documented within 8MAN.

Additional Services

Edit computer accounts

Step by step process



ed crede

& 8MAN-DEMO.LOCAL

Resource

Immediately

Credentials

Cancel

 \otimes

- 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.



Delete account

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

✓ I Remove access rights

lease add a con

Scripting

Name

Remove all direct references to the selected accounts on resources which are known to 8MAI The execution will be immediately

Status of changes: ..

Accounts to delete

8.1.2 Helpdesk

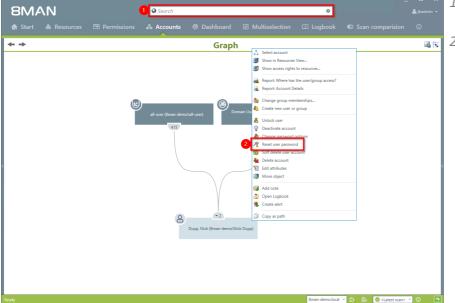
8.1.2.1 Reset passwords

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.

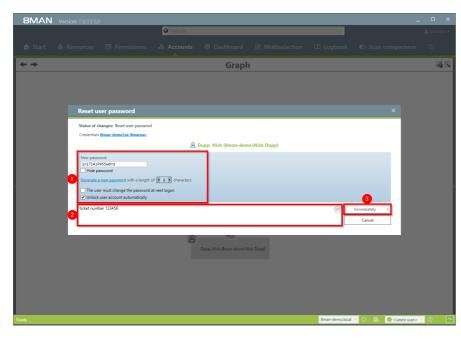
Additional services

8MATE AD Logga: Identify locked accounts 8MATE AD Logga: Monitor a user account



- 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.

316 | Access Rights Management



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

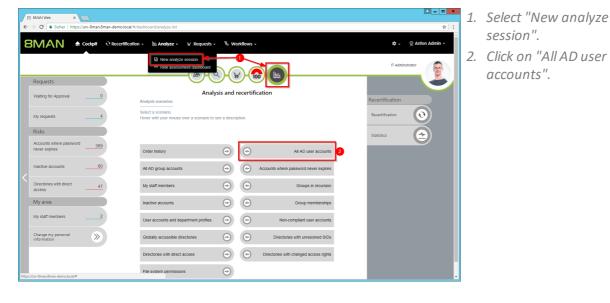
8.1.2.2 Reset passwords in bulk (web client)

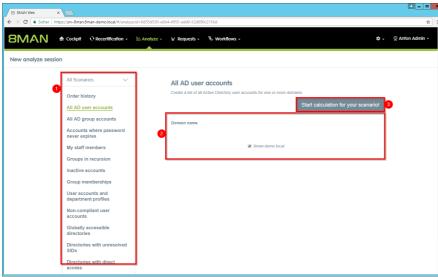
Background / Value

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)



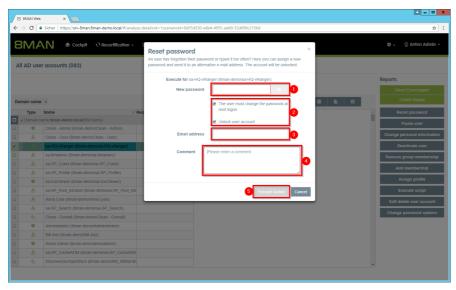


- 1. Optional: Change the scenario.
- 2. Set options for the scenario.
- 3. Click on "Start calculation".

8MAN

	MA			-4955-add0-52d090c2156d					☆ 후 - ② Anton Admin
AII A	AD USE	r accounts (382)	Config	uration 🌣					Reports
		0		resources: 8man-demo.local					Direct Excel export
-				The Mars		E	C		
oma	iin name	x		Type, Name	 C 🔳		B		
_	Туре	Name TRequested Action	Υ					3	Reset password
⊿ E	Domain ni O	ame:8man-demo.local(382 items)						п.	Pause user
	* 8	Clean - Admin (8man-demo\Clean - Admin) Clean - User (8man-demo\Clean - User)							Change personal informati
	~	sa-HQ-vRanger (8man-demolsa-HQ-vRanger)							Deactivate user
	8	sa-8mansvc (8man-demolsa-8mansvc)							
2	8	sa-SP Crawl (8man-demolsa-SP Crawl)							Remove group membersh
	8	sa-SP Profile (8man-demolsa-SP Profile)							Add membership
	•	sa-ExcViewer (8man-demo\sa-ExcViewer)							Assign profile
	8	sa-SP_Pool_Intranet (8man-demo\sa-SP_Pool_Intr							Execute script
	8	Anna Lyse (8man-demo\Anna Lyse)							Soft delete user account
	8	sa-SP_Search (8man-demoisa-SP_Search)							
	80	Clean - Overall (8man-demo\Clean - Overall)							Change password option
	•	Administrator (8man-demo\Administrator)							Reset password
	8	Bill Anz (8man-demo\Bill Anz)							An user has forgotten their
	\$	Anton Admin (8man-demoidemoadmin)							password or typed it too ofte Here you can assign a new
	8	sa-SP_CacheADM (8man-demolsa-SP_CacheADN							password and send it to an
	80	Discoverysuchpostfach (8man-demo\SM_98fda74b							alternative e-mail address. Th account will be unlocked.

- 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

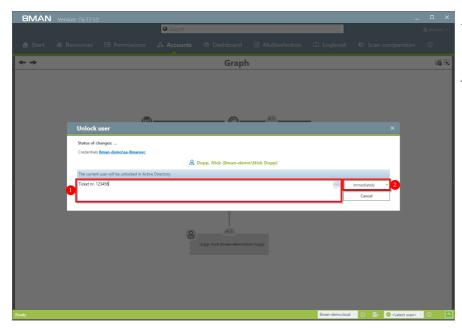
If employees use native tools to unlock a sensitive account, AD Logga will capture all activity. Especially sensitive accounts can be monitored with AD Logga <u>alerts</u>.

8MATE AD Logga: Identify locked user accounts 8MATE AD Logga: Monitor a user account



- 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.

320 | Access Rights Management



- 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

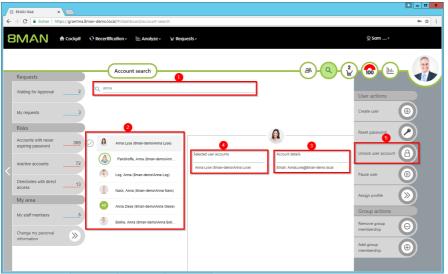
Reset users' passwords (Cockpit)

Step by step process

B BMAN Web × ★ → C Sicher https://grantma.8mai	-demo.local/#/dashboard/account-search		ণ দ্ব
	Recettification - 🔟 Analyze - 🖌 Requests -	Q	Sam •
Requests Waiting for Approval2	Account search		ections
My requests 3		Create	user 🕒
Risks		Reset p	assword
Accounts with never	Anna Lyse (8man-demolAnna Lyse)		
Inactive accounts 72	Pakdkoffa, Anna (8man-demolAnn Selected user accounts		user account
Directories with direct	Anna Lyse (8man-demolAnna Lyse) Log, Anna (8man-demolAnna Log)	Email: AnnaLyse@8man-demo.local Pause u	iser 🕕
access 13 My area	Nass, Anna (8mm-demolAnna Nass)	Assign	profile 🔊
My staff members 5	Anna Ziese (8man-demolAnna Giese)	Group	o actions
	Bolika, Anna (8man-demolAnna Boli	Remove membe	
Change my personal information		Add gr membe	

- 1. Choose Cockpit.
- 2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See <u>Changing Attributes (Web</u> <u>Client)</u>.
- 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".

B 8MAN Web ← → C ■ Sicher	×	nan-demo.local/#	/dashboard/account-search			· - 미 X
8MAN	A Cockpit		Unlock user accour	11 Anna Lyse (8man-demolAnna Lyse)		2 5am
Requests Waiting for Approval My requests	2	Q anna	Comment	Please enter a comment		User actions Create user
Risks Accounts with never expiring password	368		Cancel na Lyse (âman-demolAnna Lyse)	Selected user accounts	Execute Action 3	Reset password
C Inactive accounts Directories with directories	72 t13	Contraction Contraction	akdikoffa, Anna (8man-demolAnn g, Anna (8man-demolAnna Log) ss, Anna (8man-demolAnna Nass)	Anna Lyse (ôman-demolAnna Lyse)	Email: AnnaLyse@8man-demo.local	Pause user
My area	5		na Ziese (Sman-demolAnna Giese) Ika, Anna (Sman-demolAnna Boli			Assign profile Group actions Remove group membership
Change my personal information	»					Add group membership



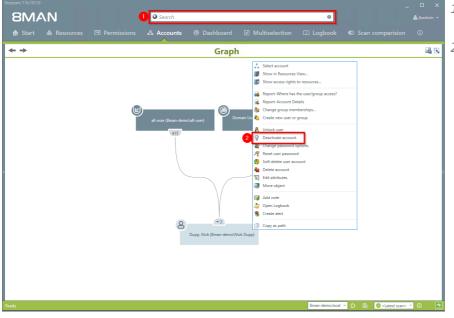
8.1.2.5 Deactivate an user account

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.

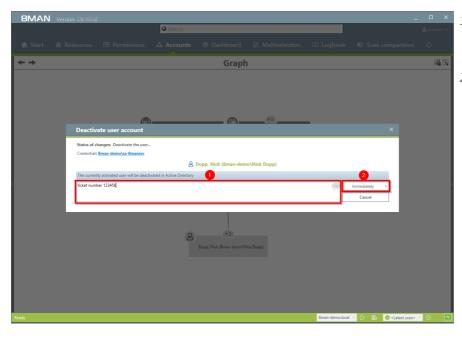
Additional services

Delete a user with soft delete Deactivate accounts in bulk (web client)



- 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.

324 | Access Rights Management



- 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

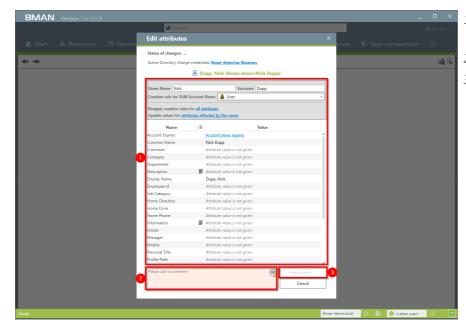
With 8MAN you can easily manage attributes for users accounts in a flat list. All actions are automatically documented.

Additional Services

Modify attributes in bulk (web client)



- 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.



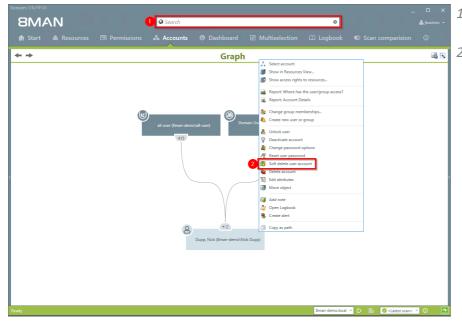
8.1.2.7 "Soft" delete a user

Background / Value

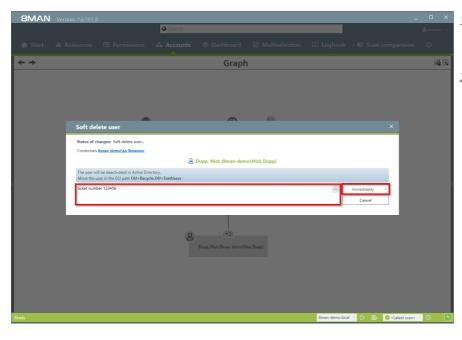
When deleting a user with "soft delete" all of their access rights remain intact. The account is moved to a "Recycle-OU" and deactivated. This account can no longer be used since the "Recycle-OU" is part of a strictly limited group policy.

Further Services

Set the "recycle-OU"



- 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.



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



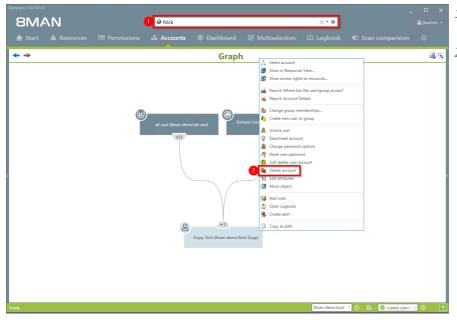
8.1.2.8 Remove a user and its permissions

Background / Value

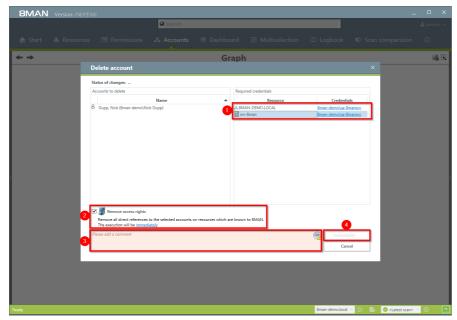
With 8MAN you can delete the user from AD and remove all of their access rights on the file server in one easy action.

Additional Services

Remove direct permissions in bulk (web client)



- 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 revisionproof password reset. The safety-critical action is recorded in the logbook.

Additional Services

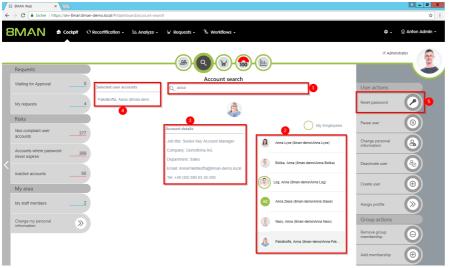
Overview of all cockpit services

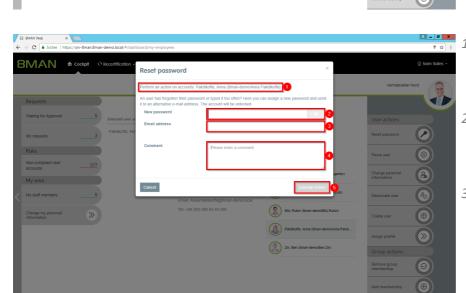
Step by step process

B 8MAN Web X			≜ <u>-</u> 5 ×
← → C	8man-demo.local/#/dashboard/account-	search	\$
	O Recertification 🗸 🔟 Analyze	₂ - ¥ Requests - [®] ‰ Workflows -	🗢 🗸 🔍 Anton Admin -
0			IT Administrator
Requests			
Waiting for Approval	Selected user accounts	Account search	User actions
My requests	Here the selected user accounts will be displayed.	(\cdot)	Reset password
Risks			Pause user
Non-compliant user37 accounts	7	Account details Use the search and select users from	Change personal
Accounts where password 36	9	the result list.	information
< never expires			Deactivate user
Inactive accounts6	<u>0</u>		Create user
My area			Create User
My staff members	2		Assign profile
Change my personal			Group actions
mormation			Remove group membership
			Add membership

1. Choose Cockpit.

- 2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See <u>Changing Attributes (Web</u> <u>Client)</u>.
- 3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner 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

 smsts 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.
 - 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)

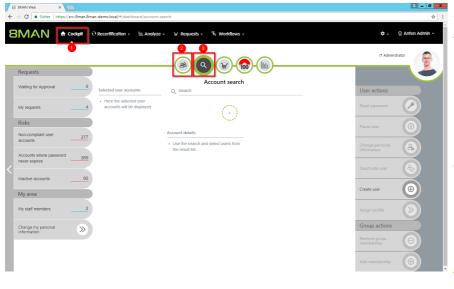
Background / Value

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 <u>Changing Attributes (Web</u> <u>Client)</u>.
- 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".

	O Recertification -	Change personal	information	×		👳 Sam Sale
		Perform an action on account	s: Pakdikoffa, Anna (8man-demo'Anna Pakdikoffa)		Vertriebsleiter	r Nord
Requests		Change the account informati Company	n for a user.			
Waiting for Approval 5	Selected user a	Department	Sales		User actions	
My requests3	Pakdikoffa, An	Location	Sales		Reset password	
Risks					Pause user	
Non-compliant user377		ZIP		2 gentor)	Change personal	
My area		Street			information	
My staff members5		Description		kzubi)	Deactivate user	8
Change my personal Second		Information		bin)	Create user	(+)
		Comment	Please enter a comment	nna Pakdi	Assign profile	
					Group actions	
					Remove group membership	Θ
		Cancel			Add membership	Œ

- 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 <u>knowledgebase</u> (login required).



8.1.3.3 Deactivate users (cockpit)

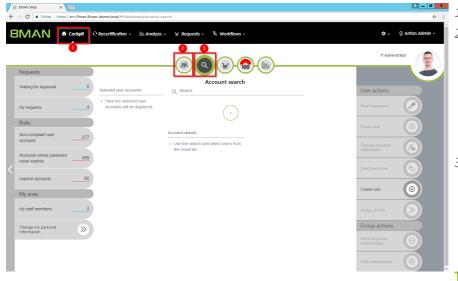
Background / Value

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 <u>Changing Attributes (Web</u> Client).
- 3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner 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".



8 8MAN Web ×			1 – 0 X
\in \ni \mathcal{C} $\left[$ $\$ Sicher $\left $ https://srv-8man.8man-demo.local/#/dasht	oard/my-employees		₹☆]:
SMAN & Cockpit O Recertification -	Deactivate user	×	© Sam Sales →
	Perform an action on accounts: Pakdikoffa, Anna (8man-demo\Anna		Vertriebsleiter Nord
Requests	Comment Please enter a comment		
Waiting for Approval5 Selected user at			User actions
My requests3 Pakdikoffa, Anr	Cancel	3 Everate Action	Reset password
Risks			Pause user
Non-compliant user	Account details		
My area	Job title: Senior Key Account Manager Company: Demofirma AG	Ansgar Agentor (8man-demolAAgentor)	Change personal Information
My staff members 5	Company, Demonitria AG Department: Sates Email: AnnaPakdikoffa@Sman-demo.local	Azubi, Andy (Bman-demolAndy Azubi)	Deactivate user
Change my personal S	Tet: +49 (30) 390 63 45-292	Bity Rubin (8man-demo\Bity Rubin)	Create user
		Pakdikoffa, Anna (Sman-demoVAnna Pakdi	Assign profile
		Zin, Ben (8man-demolBen.Zin)	
			Remove group membership
			Add membership

- 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)

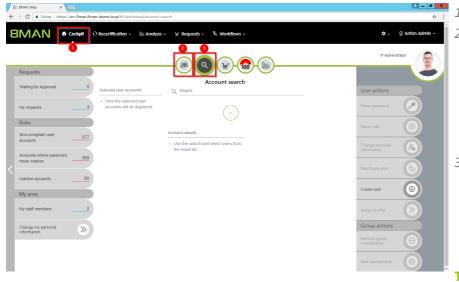
Background / Value

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.

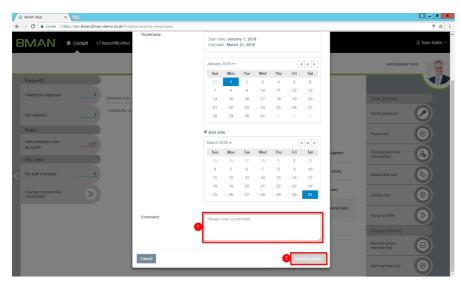
- 2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See <u>Changing Attributes (Web</u> Client).
- 3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

- 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".



B 8MAN Web X											±	- 0 ×
← → C 🔒 Sicher https://srv-8man.8r	man-demo.local/#/da	shboard/my-employees										₹ ☆
8MAN 🕈 Cockpit	O Recertification	Pause user							×		्र San	n Sales +
		Perform an action on accounts: Pail When you pause an employee, you						ng the st	to log on		Vertriebsleiter Nord	8
Requests		to the domain.	To toke all pe	11113310113	tor a po	100 01 011	ic, includi	ng uic a	and to log on			
Waiting for Approval	5 Selected user	Timeframe		te:Janua e: March							User actions	
My requests	Pakdikoffa, A		January	2018 🔻				-			Reset password	
Risks			Sun	Mon	Tue	Wed	Thu	Fri	Sat		Pause user	
Non-compliant user371	<u>z</u>		31 7	1 8	2 9	3 10	4 11	5 12	6 13			
My area		•	14	15	16	17	18 25	19	20	Agentor)	Change personal information	
My staff members	5		21 28	22 29	23 30	24 31	1	26 2	27 3	(Azubi)	Deactivate user	
Change my personal			🖲 End da	te						ubin)		
information			March 2	018 🔻				-			Create user	
			Sun	Mon	Tue	Wed	Thu	Fri	Sat	Anna Pakdi	Assign profile	
			25 4	26 5	27 6	28 7	1	2	3 10		Assign prome	
			11	12	13	14	15	16	17			
			18 25	19 26	20 27	21 28	22 29	23 30	24		Remove group membership	
											Add membership	
		Comment	Please (inter a co	mment							_

- 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".



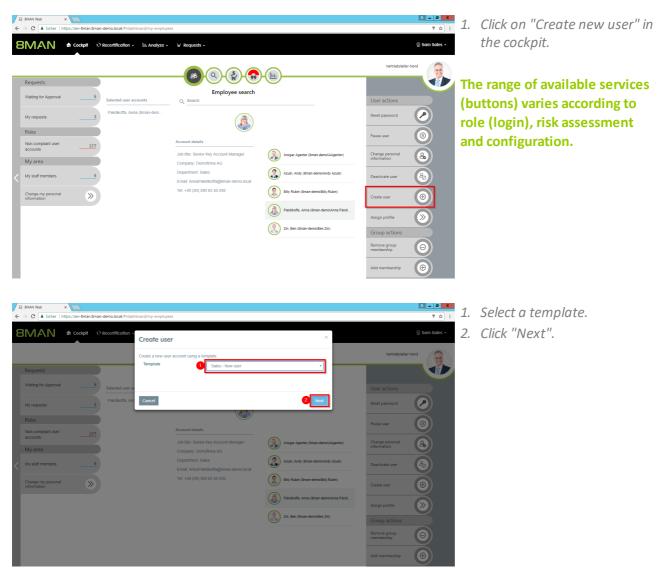
8.1.3.5 Create a new user (cockpit)

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



3 8MAN Web ×					A - C
→ C Sicher https://srv-8man.8mar	n-demo.local/#/dashboa	rd/my-employees			7
BMAN 🏘 cockpit 🥹		reate user		×	© Sam Sai
		ate a new user account using a ter	nplate.		Vertriebsleiter Nord
Requests		Domain name	8man-demo.local		
Waiting for Approval5	Selected user a	LDAP Attributes		~	User actions
My requests 3	Pakdikoffa, Ar	Vorname			Reset password
			Input required.		
Non-compliant user 377		Nachname			Pause user
Accounts My area				Agentor)	Change personal A
My staff members 5			Input required.	(Azubi)	Deactivate user
		Common-Name		ubin)	
Change my personal Sector Change my personal		SAM-Account-Name			Create user
		Benutzeranmeldename	.@8man-demo.local	Anna Pakdi	Assign profile
		Firma	Example Ltd.		Group actions
		Manager	CN=Dörte Harry,OU=TestUsers,DC=8man-demo,DC		Remove group membership
		Pers.Nr. 0	Cre-Done Hany, OU-rescosers, DC=8man-demo, DC		Add membership
		Pers.Nr. U			

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".

7	B 8MAN Web ×						± _ Ø _
÷	- > C Sicher https://srv-8man.8ma	an-demo.local/#/dashb	oard/my-employees				루 ☆
8		C Recertification	SAM-Account-Name				👳 Sam Sales 🗸
			Benutzeranmeldename	.@8man-demo.local			
			Firma	Example Ltd.		Vertriebsleiter I	Nord
	Requests Waiting for Approval 5		Manager	CN=Dörte Harry,OU=TestUsers,DC=8man-demo,DC			
	waiting for Approvar	Selected user a	Pers.Nr. 🕲				
	My requests3	Pakdikoffa, Ar	Standort 0			Reset password	
	Risks			Berlin •		Pause user	
	Non-compliant user 377 accounts		Beschreibung	Dies ist eine automatisch generierte Beschreibung für 11 mit dem SAM-Account-	Agentor)	Change personal	
	My area					information	
<	My staff members5		Password options		> (Azubi)	Deactivate user	8
	Change my personal Second		Erzeuge Postfach (Exchange)	> ubin)	Create user	(
			Comment	Please enter a comment	Anna Pakdi	Assign profile	
			•			Group actions	
			L	-		Remove group membership	Θ
		Ľ	Cancel	2 Execute	Action	Add membership	•



8.1.3.6 Assign a department profile to users (cockpit)

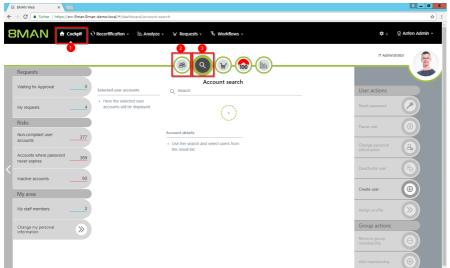
Background / Value

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

<u>Create a new department profile</u> <u>Determine permissions deviating from the department profile (Compliance Check)</u>

Step by step process

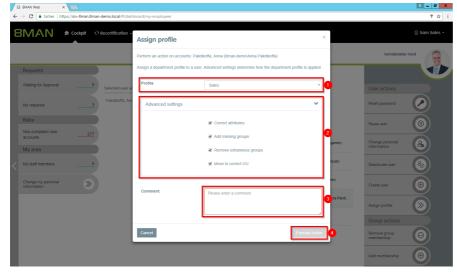


1. Choose Cockpit.

- 2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Manager" attribute. See <u>Changing Attributes (Web</u> <u>Client)</u>.
- 3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner Configuration.

	2 Anton Admin -
Requests Variang for Approval My requests My requests My requests Monocompliant user accounts where password 308 Inactive accounts My area My area <th></th>	

- 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)

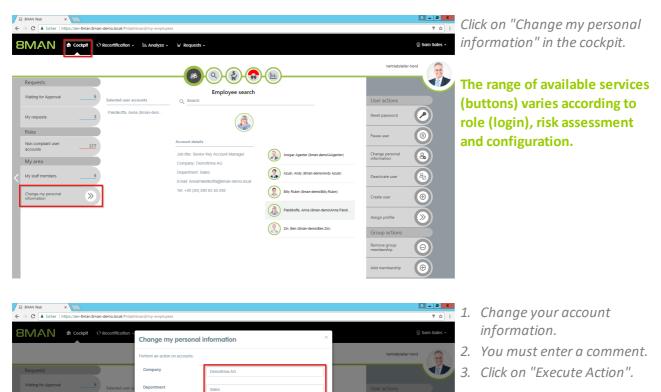
Background / Value

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



 (\black)

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 <u>knowledgebase</u> (login required).

user 377	ZIP			Pause user	0	dialo
	Street		gentor)	Change personal information	a	dialo admi
ers <u>5</u>	Description	Der Boss	(zubi)	Deactivate user	8	an ad
rsonal 📎			bin)	Create user	•	confi made foun (logii
	Comment	Please enter a comment	nna Pakdi	Assign profile		mad
				Group actions Remove group		foun
	Cancel	6	Execute Action	Add membership		(logii

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

B 8MAN Web × ★ → C Sicher https://srv-8man.8n	nan-demo.local/#/dashboard/my-emplo	vyees		= ■ × ₹ ☆ :	CII	ick
	O Recertification - Analyze	+ ₩ Requests +		© Sam Sales +	СО	ck
				Vertriebsleiter Nord	Th	e k
Requests		<u> </u>	99- Luu			an
		Employee sea	rch			
Waiting for Approval 5	Selected user accounts	Q Search		User actions	t to	yо
My requests3	Pakdikoffa, Anna (8man-dem	(B)		Reset password		
Risks				Pause user		
Non-compliant user 377		Account details		Pause user	Th	le r
Accounts My area		Job title: Senior Key Account Manager	Ansgar Agentor (8man-demolAAgentor)	Change personal A	(h	utt
	5	Company: Demofirma AG Department: Sales	Azubi, Andy (8man-demolAndy Azubi)			
My staff membersE	2	Email: AnnaPakdikoffa@8man-demo.loc	al O	Deactivate user	ro	le (
Change my personal S		Tel: +49 (30) 390 63 45-292	Billy Rubin (8man-demo\Billy.Rubin)	Create user	an	d d
			Pakdikoffa, Anna (8man-demo\Anna Pakdi			
				Assign profile		
			Zin, Ben (8man-demolBen.Zin)	Group actions		
				Remove group membership		
				Add membership		
	nan-demo.local/#/analyze-details:id=2:	cenarioid=5f0d76a6-ea1a-403d-8efe-5153314a • W Requests •	5132	्रि के सिंह के कि	1. 2.	Se A d
my start memoers (s)			2	Reports		
Domain name ×		3 colum	ns selected 🔻 C 🗏 🖻 🖻		З.	E
Type Name		quested Action		Create Report		Ρ
A Domain name:8man-demo.local(5 item Ansgar Agentor (8man-dem				Execute script	_	
Azubi, Andy (8man-demo\A				Reset password	4.	Р
Billy Rubin (8man-demo\Bill Billy Rubin (8man-demo\Bill Billy Rubin (8man-demo\Bill				Soft delete user account		Se
Zin, Ben (8man-demo\Ben.2				Pause user Change password options		50
				Change personal information		

lick on "My employees" in the ockpit.

The button shows you how many employees are assigned to you.

- . Select employees.
- Adjust which columns are displayed.
- *Export the list to Excel or PDF.*
- Perform actions on the selected employee accounts.



8.1.3.9 Add group memberships (cockpit)

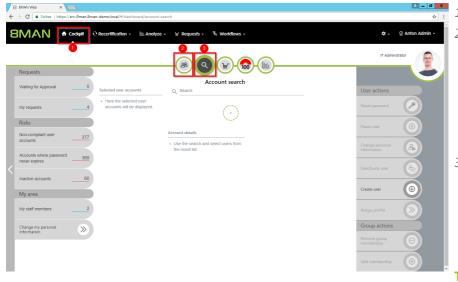
Background / Value

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 <u>Changing Attributes (Web</u> Client).
- 3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner 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".



٤	B 8MAN Web × ►						₽ ₽ X
8		Recertification -			×		्र Sam Sales +
			Perform an action on accounts: Pa	akdikoffa, Anna (8man-demolAnna Pakdikoffa)		Vertriebsleiter	Nord
	Requests		Add one or more group membersh	search users.	2		
	Waiting for Approval5	Selected user a		Search my domain only	_	User actions	
I	My requests3	Pakdikoffa, Ant		Sales-EMEA (8man-demo\Sales-EMEA (8) Sales-APAC (8man-demo\Sales-APAC) (8)		Reset password	
	Risks				4	Pause user	
	Non-compliant user		Comment	Please enter a comment	(gentor)	Change personal	
	My area						
<	My staff members5		Cancel		5 tzubi) Execute Action	Deactivate user	&
	Change my personal Second				bin)	Create user	Œ
					a, Anna (8man-demolAnna Pakdi	Assign profile	>
				Zin, Ben (8man-demolBen.Zin)		
						Remove group membership	0
						Add membership	•

- 1. 8MAN shows you which accounts you have selected.
- Search for groups.
 optional:
 - Remove already selected groups.
- 4. You must enter a comment.
- 5. Click on "Execute Action".



8.1.3.10 Remove group memberships (cockpit)

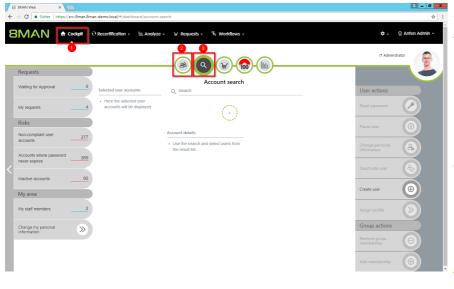
Background / Value

Overrides are often caused by group memberships. In the cockpit, you can quickly remove group memberships.

Additional Services

Overview of all cockpit services

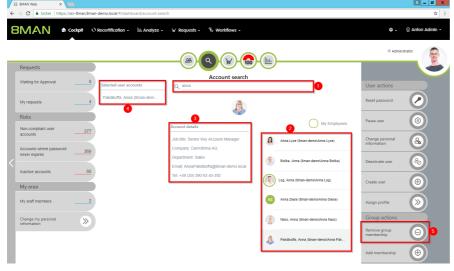
Step by step process

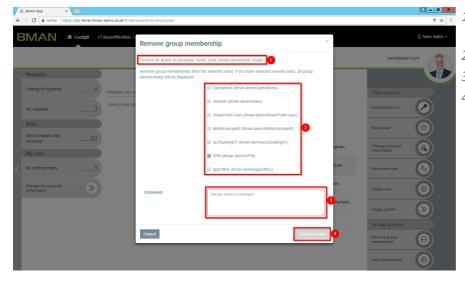


1. Choose Cockpit.

- 2. Choose "Employee search". Employees are assigned to you by an administrator through the Active Directory "Supervisor" attribute. See <u>Changing Attributes (Web</u> <u>Client)</u>.
- 3. Choose Manage users. Users are assigned to you by an administrator through the Data Owner 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".





- Image: 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

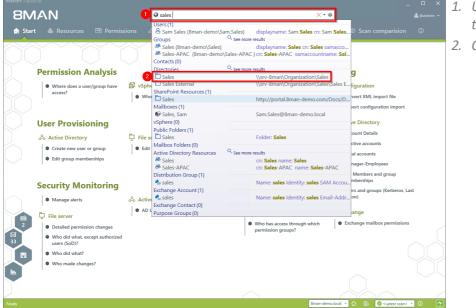
8.2.1.1 Grant and remove file server access rights

Background / Value

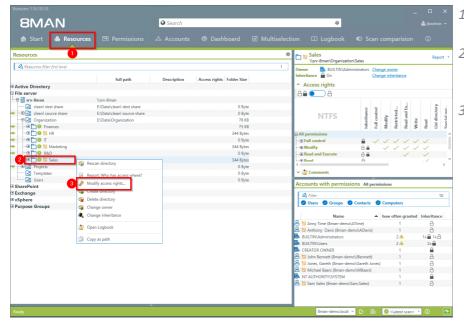
Access rights should be easy to assign and revoke. You can do this quickly and easily for the employees in your department. You don't need any special knowledge of Active Directory and / or file servers.

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.



- 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...".

Start					
Image: Start Resources Image: Start Im	8MAN	Search	۵		
Name Name Name Sales One: BULTNAdministrator Orange context Comparization, Sales, Office context Comparization, Sales, Office context Modify Read & execute Image: Name Image: Name Same: Same: Same: Same: Image: Name Same: Same: Same: Same:		🖃 Permissions 🚕 Accounts 🔞 Da			
Name Sales Caya a path Center directory. Delete: Befereb Owner Ballist TWAdministratory: Charge const: Intercentions: Constraints: Constraints	ounts New Templates Paste Clear	Resource		▲ Attributes	Edit
Name Bull INAdministratory Charge context Charge indextance Modify Read & execute Modify Name Image: Comparization_Sales_med (Image context) Name Members of BMAN Groups Name Members of BMAN Groups Name Sam Sales (Image context) Sam Sales (Image context)	Search 2	□ > File server > srv-8man > Organization > Sales >		Name	Value
Interface Other Modify Read & execute Image: Comparization_Sale_Infd (Image-demoly_Comparization_Sale_Infd (Image-demoly_Co	Name		Copy as path Create directory Delete Refresh		
Name Image: Constration_Sale_und (Iman-demo)_Organization		Owner Bull LTINVAdministrators Change owner Inheritance Off Change inheritance			
 COgnitation_Sale_und ((man-demo)Oognitation Mombers of BMAN Groups Name Sam Sale ((man-demo)(San Salec)) 		Modify	Read & execute		
Image: Solution of BMANA Groups Name Image: Solution of Solution			Name		
Members of BMAN Groups Name Sam Salet (Bman-demolSam Salet)		1_Organization_Sales_md (aman-demo)_Organizatio			
Members of BMAN Groups Name Sam Saler (Ilman-demol Sam Saler)					
Name Sam Sates (Bman-demolSam Sates)	•				
Sam Sales (Iman-demolSam.Sales)					
✓ Miscellaneous rights				>	
✓ Miscellaneous rights					
✓ Miscellaneous rights					
✓ Miscellaneous rights					
✓ Miscellaneous rights					
 Miscellaneous rights 					
 Miscellaneous rights 					
✓ Miscellaneous rights					
✓ Miscellaneous rights			1		
		 Miscellaneous rights 			
Switch to horizontal view Apply Discard		Switch to horizontal view			
Ready 🛛 🕅 🔂 🔂 🛃 🖉 < Latest scanz 💌 🛈	dy	Î.	8man-demo.loc	I 👻 💿 📑 🙋 «Latest scan»	- 0 🛃

- 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".

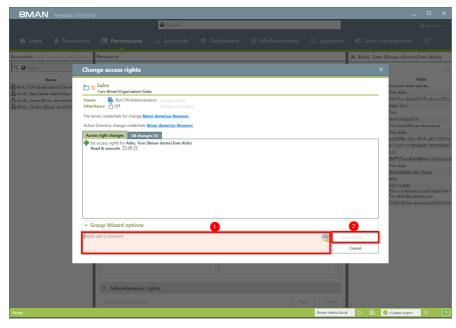
8MAN

			. 🗆 ×
8MAN	© Search 🌣		å jbadmin 👻
🖨 Start & Resources	■ Permissions & Accounts		0
	Resource	✓ Attributes	

- 1. Use the search field to find the desired user or group.
- 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.

	🖻 Permissions 🖧 Accounts 🐵 Das			
Accounts New Templates Paste Clear	Resource		Aido, Tom (8man-demo\Tom Aido)
🔍 🥝 Search 🌼	🗈 > File server > srv-8man > Organization > Sales >			Report
Name	Sales	Copy as path Create directory Delete Refresh	▲ Attributes	
Aido, Tom (8man-demo\Tom Aido)	Owner BUILTIN\Administrators Change owner		Name	Value
Smith, Gary (8man-demo\Gary Smith)	Inheritance Off Change inheritance		Account Expires	Account never expires
Smith, James (8man-demo\James Smith)	(Common Name	Tom Aido
White, Charles (8man-demo\Charles Whi	Modify	Read & execute	Distinguished Name	CN=Tom Aido,OU=TestUsers,I
	Name	Name	Display Name	Aido, Tom
		Aido, Tom (8man-demo\Tom Aido)	Given Name	Tom
	Sales_md (8man-demo\)_Organization_	🛎 👎 Aido, Tom (8man-demo\Tom Aido)	Last Logon	Never logged on
			email address	Tom.Aido@8man-demo.local
			Name (RDN)	Tom Aido
			Object GUID	ba20954c-a9ce-4518-a4c3-931
			Object SID	S-1-5-21-1178734647-297574
	Members of 8MAN Groups		Primary Group Id Proxy Addresses	513 SMTP:Tom.Aido@8man-demo
			SAM Account Name	
	Name		SAM Account Type	(805306368) User Object
	Sam Sales (8man-demo\Sam.Sales)		Sumame	Aido
			User Account Contro	
			oser riccount contro	This is a default account type t
				Tom.Aido@example.com
			LDAP ADsPath	LDAP://8man-demo.local/CN=
	 Miscellaneous rights 	2		
	Switch to horizontal view	Apply Discard		

- 1. The user is added to the column.
- 2. Click on "Apply".



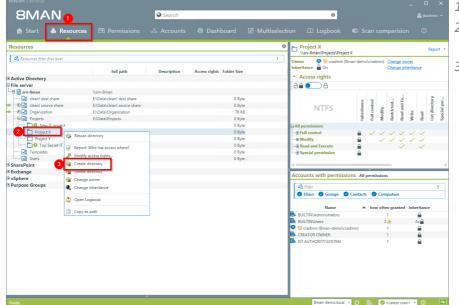
- 1. You must enter a comment.
- 2. Start the access rights change.



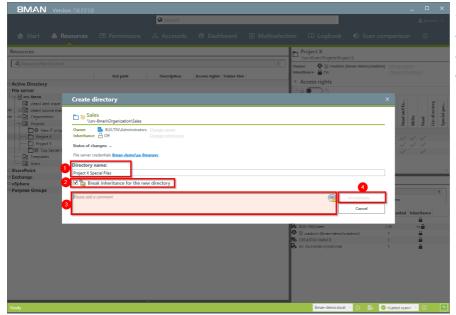
8.2.1.2 Create a protected file server directory

Background / Value

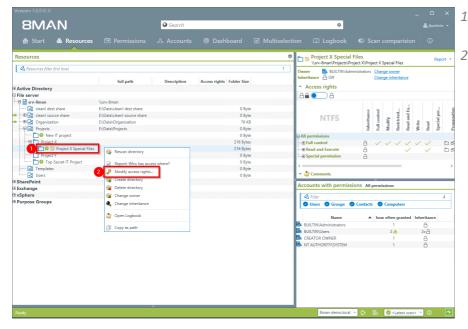
Managers and team leads can use 8MAN quickly and easily to create protected file server directories. This is done by creating a directory, removing all inheirited rights and then adding new access rights. The result is a protected directory that only selected users have access to.



- 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.



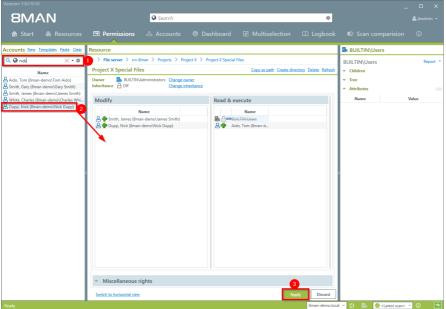
1. Navigate to the newly created directory.

2. Right-click on the directory and select "Modify access rights..." from the context menu.

Version:			
8MAN	Search	\$	
🖨 Start & Resources	🖻 Permissions 👶 Accounts 🔞 Da		
Start & Resources Accounts New Templates Paste Clear Contents New Templates Paste Clear Amounts New Templates Paste Clear Bride Templates Templates Paste Clear Bride Templates Templates Templates Bride Templates Templates Paste Templates Paste Templates Paste Templates Paste Templates	Resource > File server > cr>dman > Projects > Project X > P Project X Special Files Over		Can comparision Can comparision Caldron Caldron Caldron Tree A turbutes Mame Value
	 Miscellaneous rights 		
	Switch to horizontal view	Apply Discard	
Ready		8man-demo.loca	al 👻 🕞 😸 🖉 < Latest scan> 👻 🚯 🌁

8MAN

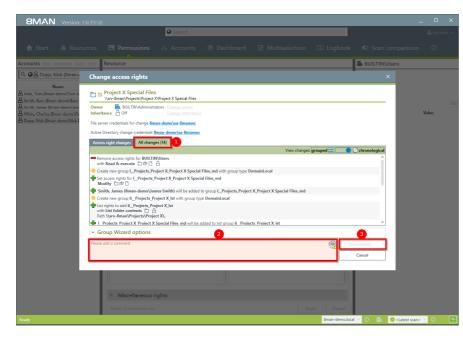
Remove all unnecessary access rights.



- 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 Version:	100	-		×
	Search			~
🍙 Start 🖓 Resou				
Accounts New Templates Paste	Gese Resource	\Users		
Q @ & Dupp, Nick (8man-	Change access rights			
Name	Project X Special Files (sn-8mai/Pojects/Poject X/Special Files			
Smith, Jamec (Sman-demo\Jam & White, Charles (Sman-demo\Ch	Owner BullTIN/Administrators Change owner Inheritance Off Change inheritance	Ň	/aluc	
A Dupp, Nick (8man demo\Nick (File server credentials for change 8man-demo\sa-8mansvc			
	Active Directory change credentials 8man-demo\sa-8mansec			
	Access right changes (14)			
	Modify DD D Set access rights for Aido, Tom (8man-demo\Tom Aido)			
	Read & execute D D D			
	P Set access rights for Smith, James (8man-demo\James Smith) Modify □ ▷ □			
	Remove access rights for BUILTIN\Users with Read & execute □ □ □ □ □			
		1		
				50
	✓ Group Wizard options			
	Please add a camment			
	Cancel			
	 Miscellaneous rights 			
Durch	Switch to horizontal view Apply Bacard	Catest scan>	0	
Ready	Sman-demolocal Q Ex	Vatest scan>	-W	

8MAN lists all planned access right changes. In the following example "Sam Sales" receives "change" rights to a new protected directory.



- 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.

	🖻 Permissions 🖧 Accounts 🔞 Dasl			
Accounts New Templates Paste Clear	Resource		Aido, Tom (8	3man-demo∖Tom Aido)
Q 😡 Search 🌼	🛅 🗧 File server 🗧 srv-8man 🎽 Projects 🎽 Project X 🎽 Proj	ect X > Project X Special Files		Report
Name	Project X Special Files	Copy as path Create directory Delete Refresh	 Attributes 	
Aido, Tom (8man-demo\Tom Aido) Dupp, Nick (8man-demo\Nick Dupp)	Owner BUILTIN\Administrators Change owner Inheritance Off Change inheritance		Name Account Expires	Value Account never expires
Smith, Gary (8man-demo\Gary Smith) Smith, James (8man-demo\James Smith) White, Charles (8man-demo\Charles Whi		Read & execute	Common Name Distinguished Name Display Name	Tom Aido CN=Tom Aido,OU=TestUsers,I Aido, Tom
	Nar Bar Projects_Project X_Preoject X Special Files_md (8man	Nam	Given Name Last Logon	Tom Never logged on
			email address Name (RDN) Object GUID	Tom Aido@8man-demo.local Tom Aido ba20954c-a9ce-4518-a4c3-931
	Members of 8MAN Groups	Members of 8MAN Groups	Object SID Primary Group Id Proxy Addresses	S-1-5-21-1178734647-297574 513 SMTP:Tom.Aido@8man-demo
	Name Dupp, Nick (8man-demo\Nick Dupp) Smith_lames (8man-demo\lames Smith)	Aido, Tom (8man-demo\Tom Aido)	SAM Account Name SAM Account Type Sumame	Tom Aido (805306368) User Object Aido
	Smith, James (8man-demo\James Smith)		User Account Control	512 / 0x200 This is a default account type 1 Tom.Aido@example.com
			LDAP ADsPath	LDAP://8man-demo.local/CN:
	 Miscellaneous rights 		1	
	Switch to horizontal view			

8MAN

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

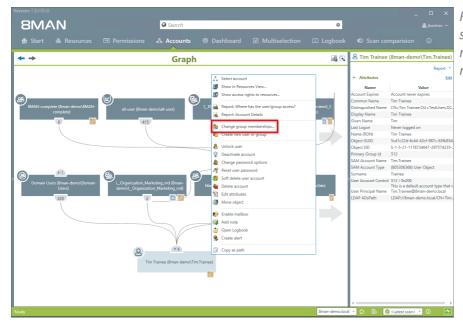
8MAN		🛛 Search			۵				
🚖 Start 💩 Resource									
Resources				🌩 🛅 🃷 Mar	keting -8man\Organization\Marketing			Repo	ort
A Resources filter first level				Owner	-sman\Organization\Warketing				-
	full path	Description	Access rights Folder Size	Inheritance	On Chan	ige owner ige inheritance			
Active Directory				Access	s rights				
ile server				A A 🔵	Select all	Ctrl+A			
🗄 📑 srv-8man	\\srv-8man				Copy	Ctrl+C			
····· 🛃 clean! dest share	E:\Data\clean! dest share		0 Byte			-	- 2	5	
🕀 🛃 clean! source share	E:\Data\clean! source share		0 Byte		2 🙏 Show in accounts view	1	Special per	Propagation	
	E:\Data\Organization		76 Ki		Show access rights to resou	irces	ecia	obai	
- 🕀 📩 🥹 Finances			75 K8				Sp	Pro	
🕀 🛅 😉 💹 HR			344 Byte		sio 🔬 Report: Where has the user	/group access?			
🗄 🛅 🕒 IT			0 Byte		tre 🙀 Report: Account Details		C	100	
🎛 🛅 🚯 📁 Marketing			408 Byte				- 0	100	
🔁 🕒 R&D			0 Byte		nd 춹 Change group membership	IS	C	100	
🗄 🕀 🎦 😉 💴 Sales			408 Byte	Special	pe 🗞 Create new user or group				
····· 🛃 Templates	E:\Data\Templates		0 Byte						
🛃 Users	E:\Data\Users		0 Byte		🔒 Unlock user				
harePoint				🎽 🛩 🏄 Comi	me 👷 Deactivate account				
kchange					Change password options		_	_	-
Sphere				Accounts	Reset user password				_
urpose Groups				A Filter	-			1	0
				Ø Users					
				O OACH	A Delete account				
					Edit attributes		nce		
				🔒 过 Pull, Si			ice.		
				Russel	am 🙀 Add note				
				A Steven					
				Stever	Ma 😤 Create alert				
					ainee (8man-demo\Tim.Trainee)	2.0 2.1	-		-
				3 Access		3 🕰 3x 🖞	2		
					Modify\Tim Trainee (8man-dem				
					Modify\J_Organization_Market				Ira
					Modify\J_Organization_Market			demo)	_
				🛎 🛂 Torrey	Smith (8man-demo\TSmith)	1 8			
									,
	^	·							P

1. You have identified "Tim Trainee" as having <u>multiple</u> <u>access paths</u>.

2. Right-click on the account and select "Show in account view" from the context menu.

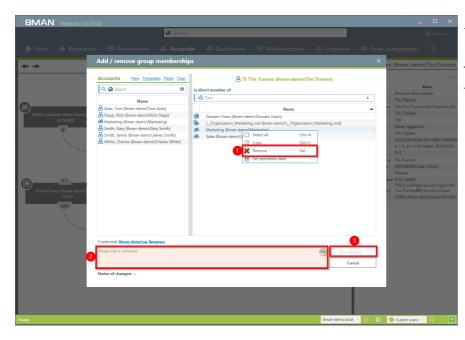


Use the AD graph to analyze multiple access paths.

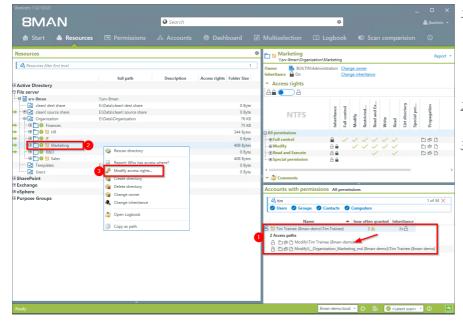


Right-click on the account and select "Change group memberships" from the context menu.

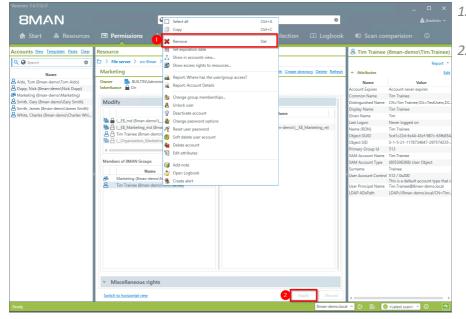
8MAN



- 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.



- 1. Select the desired user and chose "Remove".
- <u>8 Tim Trainee (8man-demo\Tim.Trainee)</u> 2. Start the removal process.

Resources			1	Marketing	Marketing	1						Repor
Active Directory File server	full path	Description	1 Access rights Folder Size	Owner BUILTINVAdmin Inheritance On ^ Access rights A a a a a a a a a a a a a a a a a a a a	istrators	Chang	e owner e inherit	ince				
Big Srv-8man Clean! dest share Clean! source share	\\srv-8man E:\Data\clean! dest share E:\Data\clean! source share E:\Data\Organization		0 Byte 0 Byte 76 KB 75 KB	NTFS	Inheritance	Full control	Modify Restricted	Read and Ex	Write Read	List directory	Special per Propagation	
			344 Bytes O Byte 408 Bytes O Byte 408 Bytes	All permissions Full control Modify Read and Execute Special permission							05 05 05	D.
SharePoint Exchange	E:\Data\\Templates E:\Data\Users		0 Byte 0 Byte	 ✓ ⁽/₂) Comments Accounts with permissio 	ns All p	ermiss	ions					_
vSphere Purpose Groups				tim Users Groups Name Name	Contacts	0	Compute		ited In	heritanc		f 34 🗙
				Access path	nee (8man	-demo)					

Verify the result in the resource view.

8MAN

8.2.2.2 Remove direct permissions

Background / Value

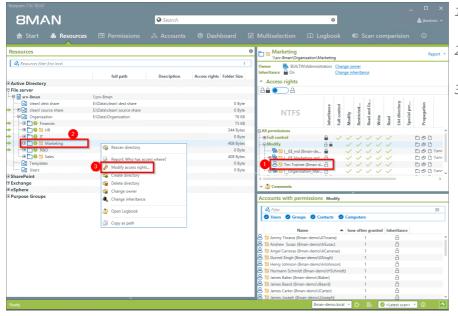
Direct access rights should be avoided at all costs and replaced by group access rights. Firstly, direct access rights are inefficient because every user is managed independently. Secondly, each directory needs to be examined individually to ensure the removal of all direct access rights. 8MAN shows 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

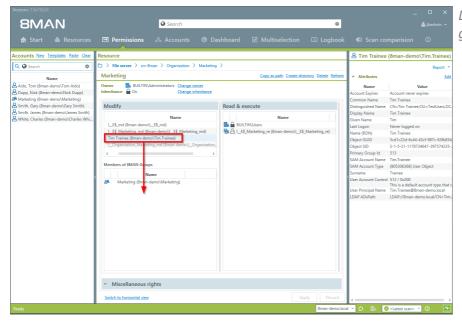
Remove direct permissions in bulk (web client)

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



- 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.

★ Start & Resources • Start & Resources • Permissions & Accounts @ Dashboard @ Multiselection ① Logbook @ Scan comparision @ • Start & Resource • Start & Resources • Start & Resource • Resource • Resource Primesty Resources Resource					
Counts Har Tampiates Parts Care B. Tim Trainee (Braan-demo\Tim.Trainee Adds. Tim Bisan-demo\Tim.Side Dign Same Tim Trainee Marketing Core Tim. Dign. Same Tim. Same	8MAN	Search	\$		
Q Score Construction Characterization > Adds Marketing > Report Adds, Tom (Bean-dero) Tom Adds) Owner BUILTINA/dministrature Carge as path Create directory Released Adds: Tom (Bean-dero) Tom Adds) Adds, Tom (Bean-dero) Tom Adds) Owner BUILTINA/dministrature Carge as path Create directory Released Adds: Tom Tailee Company Released Adds: Tom Tailee Company Released Adds: Tom Tailee Company Released Company Released Adds: Tom Tailee Company Released Company		🖻 Permissions 🖧 Accounts 🔞 Das			
Name Marketing Cargo anath Create directory Dieter Berler Add, Ton (Bran-denv) Ton Add) Ommer Build TINA-denvisor Cargo anet: Cargo in theritance Congo in theritance Cargo in theritance Congo in there is a congo in the cong in the congo in the cong in the cong in	Accounts New Templates Paste Clear	Resource		🐣 Tim Trainee	(8man-demo\Tim.Trainee
Adds, Tom (Bana-dem/Vick Dig) Owner & BULTIN/Administrator: Charge conter Name Name Name Account Expires Account Expires Account Expires Account Expires Account Expires Account Expires Name Name Name Name Account Expires Name Account Expires Name Name <td< td=""><td>🔍 🖗 Search 🌼</td><td>\Box $>$ File server $>$ srv-8man $>$ Organization $>$ Marketing</td><td>></td><td></td><td>Report</td></td<>	🔍 🖗 Search 🌼	\Box $>$ File server $>$ srv-8man $>$ Organization $>$ Marketing	>		Report
3 db Comer, Gener, denvil Comero, Sange, Lander, Carage, Carage, Lander, Carage, Carag	Name	Marketing	Copy as path Create directory Delete Refresh	 Attributes 	E
Andreining (Granz-demol/Martello) Section (Granz-demol/Martello) <	Aido, Tom (8man-demo\Tom Aido)	Owner BUILTIN\Administrators Change owner		Name	Value
Senit, Auge (Bran-demolyars) senith Senit, Juses (Bran-demolyars) senith Senit, Juses (Bran-demolyars) senith Senith, Juses (Bran-demolyars) senith Senith, Lass, Marketing, rel Senith, Lass, Marketing, rel Seni	Dupp, Nick (8man-demo\Nick Dupp)	Inheritance On Change inheritance		Account Expires	Account never expires
S white, Charles (Brand-demo)Lates (white) White, Charles (Brand-demo)L		(n		Common Name	Tim Trainee
Name Name White, Charles (Brann-demo)(Charles White Strain LS, and (Brann-demo)(LS, Marketing, rel) Given Tameedemo) Tim Transee Strain Charles (Brann-demo)(LS, Marketing, rel) Given Tameedemo) Charles (Brann-demo)(LS, Marketing, rel) None (RDA) Strain Charles (Brann-demo)(LS, Marketing, rel) Given Tameedemo) Charles (Brann-demo)(LS, Marketing, rel) None (RDA) Members of IMAN Groups None (Brann-demo)(LS, Marketing, rel) Stat Account Name Tim Transee Members of IMAN Groups Name Stat Account Name Tim Transee Members of IMAN Groups Name (Brann-demo)(LS, Marketing, rel) Stat Account Name Tim Transee Members of IMAN Groups Name (Brann-demo)(LS, Marketing, rel) Stat Account Name Tim Transee Members of IMAN Groups Name (Brann-demo)(LS, Marketing, rel) Tim Transee Stat Account Name Stat Account Name Withing Charles (Brann-demo)(LS, Marketing) Tim Transee Stat Account Name Stat Account Name Stat Account Name Withing Charles (Brann-demo)(LS, Marketing) Withing Charles (Brann-demo)(LS, Marketing, rel) Diver Ningel Brance Stat Account Name Withing Charles (Brann-demo)(LS, Market		Modify	Read & execute	Distinguished Name	
y mide, Libbles (MM-demo)_Libbles (MM-demo)_Libb		Name	Nama		
She A 15 Marketing, ref (Branchemo) LE Marketing, ref (Branchemo)LES Marketing, ref (Dio) Neuer (Dio) Tim Transee She A Cognition Marketing, ref (Dio) She Add Add Add Add Add Add Add Add Add Ad	White, Charles (8man-demo\Charles Whi				
Object GUD Serit2046444-9697-058 Object GUD Serit2046444-9697-058 Object GUD Serit204644-9697-058 Object GUD Serit204644-969 Object GUD Serit204644-969 Object GUD Serit2046444-969 Object GUD Serit204644-969 Object GUD Serit204644 Object GUD Serit204644 Object GUD Serit204644 Object GUD Serit20464 Object GUD Serit204644 Object GUD Serit204644 Serit204 Serit20464 Serit204 Serit20					
Image: Conjunction Making on Edimension (J_Organ Image: Conjunction (J_O			S [(_cs_marketing_re (oman-demo\(_cs_marketing_re)		
Anne					
Members of BMAN Groups SAM Account Yue 0003060 User Opicet User Principal Nam Maccount Stame Y Miscellaneous rights Smith to horizontal view					
Members of BMAN Groups Sank Account Type (B0200260) User Object. 36 Mercelons Groups 36 Mercelons Groups 37 Mercelons Groups 38 Mercelons Groups 39 Mercelons Groups 30 Mercelons Groups <td></td> <td><pre></pre></td> <td></td> <td></td> <td></td>		<pre></pre>			
Name Somme Trained B Matching from d-month/Matching) Wer Account type It C Somme The is a default account type It User Account type It The is a default account type It User Account type It The is a default account type It User Account type It The is a default account type It User Account type It The is a default account type It User Account type It The is a default account type It User Account type It The is a default account type It V Miscellaneous rights Smith to horizontal vier Apply		Members of 8MAN Groups			
A Metation (Reached Materice) Dear Accessed Central S12 / 2000 Dis is a default account type it User Accessed Central Transee Braan-demo (Unit Trainee) User Accessed Central Transee Braan-demo (Unit Trainee) V Miscellaneous rights Settich to horizontal sizer Apply Decad					
Constraints in the decided values The is a default account type it User Principal Parter The is a default account type it User Parter The is a default account type it User Parter The is a default account type it User Parter The is a default account type it User Parter The is a default account type it User Parter The is a default account type it User Parter The is a default account type it User Parter The is a default account type it User Parter The is a default account type it User The is a default acco		٢			
V Miscellaneous rights Switch to horizontal siew Apply Discal					This is a default account type th
✓ Miscellaneous rights Smith to horizontal view Apply Decard		Z S 🚯 Tim Trainee (8man-demo\Tim.Trainee)			
		 Miscellaneous rights 			
eady 8man-demolocal V 🗘 Eb 🖉 <latest scan=""> V 🛈</latest>		Switch to horizontal view	Apply Discard	<	
	Ready		8man-demo.loci	- 0 B 0	<latest scan=""> * ()</latest>

- 1. The direct access right for "Tim Trainee" will be removed.
- 2. The group membership will be assigned.
- 3. Click on "Apply".

8MAN Version:		
	Search	
🏚 Start 💩 Resou		
Accounts New Templates Paste	Cear Resource & Tim 1	Trainee (8man-demo\Tim.Traine
🔍 Q Search	Change access rights	
Name & Aido, Tom (8man demo\Tom A & Dupp, Nick (8man demo\Nick I & Marketing (8man demo\Marke & Smith, Gary (8man demo\Gary	Image: Stand	Value Account never expires I im Trainee CN-Tim Trainee,OU-TestUsers,I Tim Trainee
Smith, James (8man demoVJam & White, Charles (8man demoVCh	File server credentials for change Bman-demolya-Bmanosc Active Directory charge credentials <u>Bman-demolya-Bmanosc</u> Access right changes (7)	Tim Never logged on Tim Trainee Sed1c22d 6c44 43cf 987c 63fb3
	View Charges: grouped = View Charges: grouped = Cchronolog Remove access rights for Tim Trainee (Imaan demo\Tim,Trainee) with Modify to Charges Tim Trainee (Imaan-demo\Tim,Trainee) will be added to group [_Organization_Marketing_md	(c) 1 S 1 1787364/T 20737422 D13 Tim Truince (80300300) User Okjeut Truince Truince Truin is a default account type th Tim Truince@Imme dema local LDAP//9mail dema local/CN+T
2	Group Wizard options G Generate Generate	
	Miscollancous rights Instance Apply Disad c	
Ready	8man-demo.local 🔟 🔘 👘	🗈 🖉 < Latest scan> 🕤 🕕 🦉

- 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

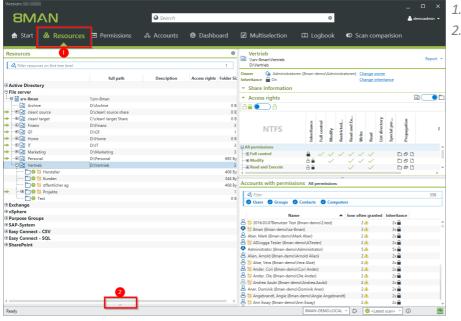
Background / Value

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

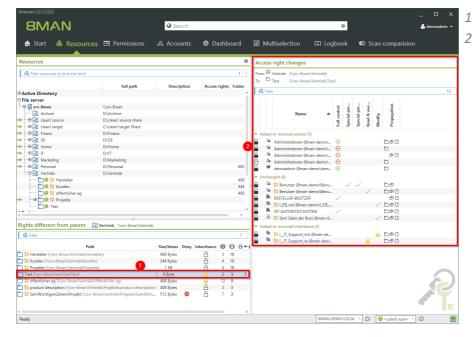


- 1. Click "Resources".
- 2. Expand the frame.

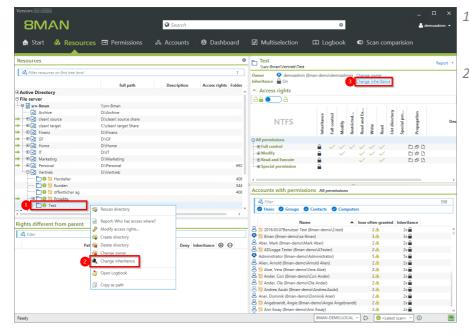
Version:			l														-	
8MAN		😧 Se	arch							٥							å (demoadmin
📅 Start & Resource	s 🖻 Permissions	ሔ Acco	ounts @) Dash	boar	d	Multiselection	ធរ	ogb	ook		D S	Scar	n coi	mpa	risio	1	
esources						\$	Vertrieb											
A Filter resources on first tree level						1	\\srv-8man\Vertrieb D:\Vertrieb											Repor
	full path	Desci	ription Ac	ccess righ	ts Fo	lder	Owner 🛕 Administratore	n (8man-	demo	\Adm	inistrat	oren)			<u>wner</u> nheritar	nce		
Active Directory						^	 Share Information 											
File server																		_
🖽 📑 srv-8man	\\srv-8man						 Access rights 											2 🔍
Archive	D:\Archive					1	ae 🗩 a											
→ ···· ⊕] clean! source	D:\clean! source share																	
► ····	C:\clean! target Share					-						j.			≥		=	
► ···· ⊕ Finanz	D:\Finanz					- 1		inheritance	full control		Restricted	Read and Ex			ist directory	pecial per	Propagation	
▶⊕ 🔄 GF	D:\GF					-	NTFS	it.	E O	Modify	1.	5		-	ii.	3	ő	
Home	D:\Home					- 1		he	÷.	fod	s	2	Write	Read	ž	ĕ	đ	
▶	D:\/T					-		-	-	2	22	~	>	22	-	ŝ	•	
Marketing	D:\Marketing					- 1	All permissions											
	D:\Personal					692	Full control	<u> </u>	\sim	\sim	\checkmark	\checkmark	\checkmark	\checkmark			000	
······································	D:\Vertrieb					092	⊞ Modify	a 🔒		\sim		\sim	\sim	\sim) 🕫 🗅	
10 10 Hersteller	jo:(vertrieb					408	Read and Execute	a 🔒				\checkmark		\checkmark		C) 🗗 🗋	
						344	<											
🛅 😉 💹 Kunden							Accounts with permissio	me All			-							
🛄 🤁 😕 öffentlicher ag						408	Accounts man permissio	115 741	permi	221011				_				
→ ····⊞ □ 9 10 Projekte							A Filter											358
🛄 😉 Test						~	🛛 Users 🖉 Groups 🖉	Contacts	. 0	Com	nuter							
						>	Le contre a sussitir e											
Rights different from parent	Vertrieb \\sru-8man\\/ertrieb						Name					how c	often	gran	ted Ir	nherita	nce	
				_		_	🐣 📁 2016.03.07Benutzer Test (8man-dei	mo\2.1	est)			24	6		2x		
A Filter						7	🚯 📁 8man (8man-demo\sa-8m						34	6		3x 🖬		
			I	0			Aber, Mark (8man-demo\Ma						20	6		2x		
Path			Deny Inherita				a DLogga Tester (8man-de	mo\ATes	ter)				20	2		2x		
🗋 💯 Hersteller (\\srv-8man\Vertrieb\Hers		408 Bytes	8	5			Administrator (8man-demo\						54			5x		
🔰 😈 Kunden (\\srv-8man\Vertrieb\Kunde		344 Bytes	< a				Alien, Arnold (8man-demo\A						24			2x		
🛅 💹 Projekte (\\srv-8man\Vertrieb\Projek	te)	1 KB	- No A		10		Stand (Sman-demo)						24			2x		
Test (\\srv-8man\Vertrieb\Test)		0 Byte		2	3	2	Ander, Cori (8man-demo)						20			2x		
📩 🔯 öffentlicher ag (\\srv-8man\Vertrieb)	öffentlicher ag)	408 Bytes	<u></u>	12			Ander, Ole (8man-demo)						24			2x		
1 0 product description (\\srv-8man\Ver	trieb\Projekte\product description)	408 Bytes	A	2	3		Ander, Ole (Sman-demov						20			2x		
🐂 💹 SehrWichtigesGeheimProjekt (\\srv-8	Bman\Vertrieb\Projekte\SehrWich	512 Bytes		7	3					9								
			_				Aner, Dominik (8man-demo)				10		24			2x		
							🐣 🔟 Angebrandt, Angie (8man			ngeb	randt)		24			2x		
£				_	_	>	🐣 📁 Ann Essay (8man-demo\A						24		_	2x		
										10.LO		0		🕗 <la< td=""><td></td><td></td><td>0</td><td></td></la<>			0	

8MAN lists all subdirectories with different permissions. At the yellow lock you recognize a corrupted inheritance.

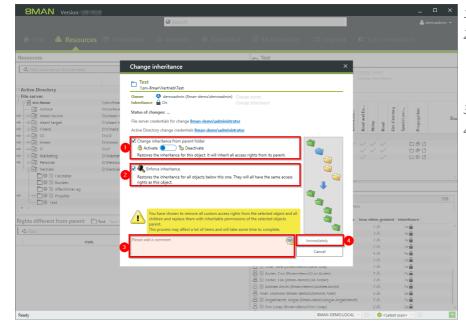




- 1. Select an entry.
- 2. 8MAN shows you in all details which permissions are different compared to the parent directory.



 Select the subdirectory where you want to correct the corrupted inheritance.
 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.

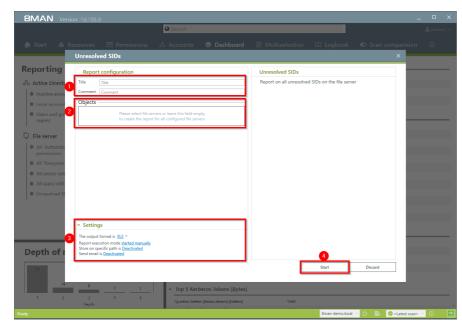
By using unresolved SIDs insider threats can gain access to sensitive resources. 8MAN clearly identifies unresolved SIDs in your system allowing you to delete them.

Additional Services

<u>Remove unresolved SIDs in bulk</u> (web client)

8MAN	Search		۵		
🗙 Start 💩 Resources 🖃 Permissi	ons & Accounts 😨 Dashboard	☑ Multiselection			
Reporting	 Users and other accounts 				
Active Directory	Users	431			
	Users (Disabled)	6			
Inactive accounts	Administrators	13			
Local accounts	Administrators (Disabled)	0			
 Users and groups (Kerberos, Last logon) 	Groups				
logon,	All Groups	190			
File server	Groups with members (w/o recursions)	112			
All 'Authenticated users' 23	Empty groups 🛕	75			
permissions	Groups in recursions 🛆	3			
All 'Everyone' permissions 34	The largest group (Domain Users (8man-d				
All owner not administrator 23	Built-in security groups	27			
	Global security groups	78			
All users with direct access 453	Universal security groups	35			
Unresolved SIDs 2	Local security groups	48			
	Global distribution groups	0			
	Universal distribution groups Local distribution groups	0			
	Local distribution groups	0			
	OU / Contacts / More				
~	Computers	4			
Depth of nested groups	Computers (disabled)	0			
	Contacts	0			
77	Foreign users	0			
	Organizational Units	12			
	 Top 5 Kerberos Tokens [Bytes] 				
1 2 3 4 Depth	5 Quinton Patton (8man-demo\QPatton)	1584			
tv			8man-demo.local	 O Eb <latest scan=""></latest> 	v 0

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

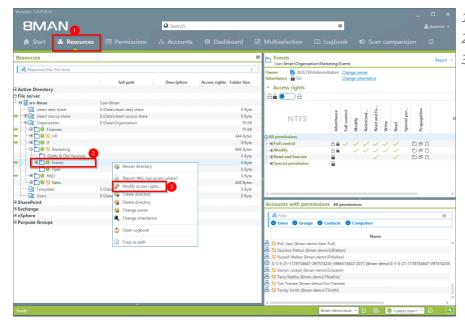


- 1. Enter a title for the report and add a comment.
- 2. Define the range of the report.
- 3. Define the desired report settings.
- 4. Start the report.

✓ Format Painter	m + <u>M</u> + <u>A</u>	▲ ■ ■ ● ● ● Wrap Text [] ↓ ■ ■ ■ ● <td< th=""><th>\$ * % '</th><th>00 4.0</th><th>Formatting *</th><th>Format as Cell Table * Styles *</th><th>Insert Delete</th><th>Format</th><th>∑ AutoSum ↓ Fill ~ Clear *</th><th>Filter * Sel</th><th>nd & lect *</th></td<>	\$ * % '	00 4.0	Formatting *	Format as Cell Table * Styles *	Insert Delete	Format	∑ AutoSum ↓ Fill ~ Clear *	Filter * Sel	nd & lect *
Clipboard & F	Font	G Alignment G	Number	6	5	ityles	Cells		Ed	liting	
▼ : × √ f _k		Organization\Marketing\Events	D	E	F	G H	4 I	J	К		м
Report for	srv-8man	C.		6	r.	0 1	1 1	5	n.		m
Path	Diaht	Unresolved SID									
		S-1-5-21-1178734647-297574235-3966573622-207	1 2								
Path report about unresolved owner SI	ID										
All accounts have been resolved											
	•										
Configuration srv-	8man (4)			4						

- Open the report in Excel.
- 1. Switch to the file server tab.
- 2. All unresolved SIDs are listsed in the report.

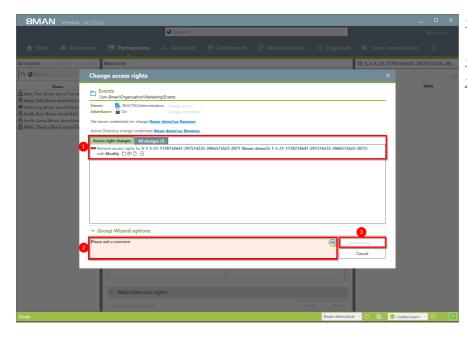




- 1. Select "Resources".
- 2. Select an affected directory.
- 3. Right-click on the directory and select "Modify access rights" from the context menu.

A Start A Resources Permissions A Accounts Department Department

- . Select the SID.
- 2. Click on "Remove".
- B. Click on "Apply".



- 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.

8MAN Configuration 1 asion:	- 😐 × 1. Start the configuration
Back A 8MAN says! Basic Settings	module and navigate to
Automatic update of BMAN group names if this option is checked, BMAN group names will automatically be adjuted in case the name if solice of the configuration in BMAN. We adjute the configuration in BMAN. We adjute the next change action in BMAN. We adjute the next change action in BMAN. Automatic update of BMAN group names will automatically be adjuted in case the name of a directory or provide the access right (changes on the affected resources before additional option Weadjute of the name of access right groups). Automatic update of BMAN group names within the next change action in BMAN. Automatically adjute of the access right groups). Automatically adjute of the access right groups). Automat	 >"File server". 2. Select the desired SharePoint resource. You can enter different settings
Group-specific characters g Global groups Local groups in List groups divid Path usage in group names Complete gath All directories Path relative to server Limit to the first ind the last indiced of the mark of the first indiced of the server Structures Backdact server Wroteman Name format: Wroteman Goog here Bit advectories Automatidally update names of the BMAN groups when performing on access right charge in an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups, when performing an access right charge in the same of the BMAN groups in the same of the BMAN groups in the same of the BMAN groups in the s	preview.
Configuration Status 🕲 Group Woard Settinge: Configuration successfully loaded.	· · · ·

8.2.2.6 Change directory ownership

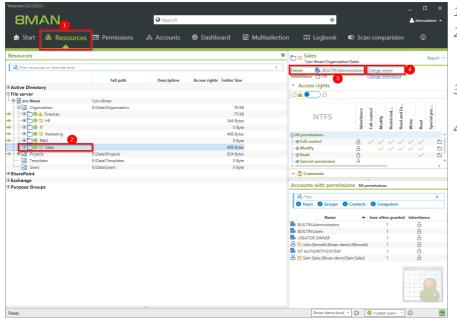
Background / Value

With 8MAN, you simply change the owner of directories. If you exclude users from ownership of directories, you can prevent unwanted permission changes.

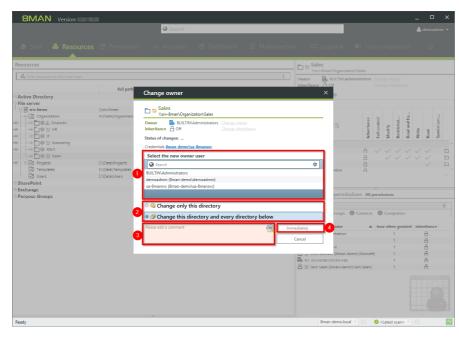
Additional Services

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

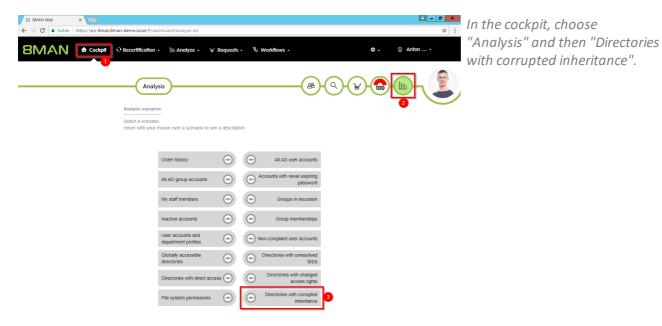
Background / Value

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





8MAN Web × C	8man-demo.local/#/ana	alyzerid=5d0af5ba-0e59-4513-bcba-247343879a87	± _ □
MAN 🕈 Cockpit	O Recertification -	Im Analyze - W Requests - % Workflows -	💠 - 👰 Anton
ew analyze session			
All Scenarios	\sim	Directories with corrupted inheritance	
Order history Task overview		Generate a list of directories with enabled inheritance where permission	ons are inconsistent with the parent folder. Start calculation for your scenario!
All AD user accounts All AD group accounts		File server	0
Accounts with never expiring password			
My staff members Groups in recursion			
Inactive accounts			
Group memberships			
User accounts and department profiles			
Non-compliant user accounts			
Globally accessible directories			
Directories with unres	plved		

- 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".

8 8MAN Web ×		
← → C 🔒 Sicher https://srv-8man.8man-demo.local/#/analyze-details;id=1;sc	enariold=5d0af5ba-0e59-4513-bcba-247343879a87	☆ :
8MAN 🕈 Cockpit 🔍 Recertification - 🖆 Analyze	- 🖌 Requests - 🔌 Workflows -	🗢 - 👳 Anton
Directories with corrupted inheritance (1)		
	Configuration 🌣	Reports
	Selected resources: \\srv-8man	Direct Excel export
Drag columns here to create groups.	4 columns selected 🔹 C	E E Create Report
	C	Available Actions
Path		Ider Size y Owr
Isrv-8man/Marketing/Projekt X/Dokumente/Testordner für Vererbungsfehler	Testordner für Vererbungsfehler 0	Byte Kris 2 Execute script
		Enforce inheritance
4		

8 8MAN Web ×				≜ = □ ×
\leftarrow \rightarrow C \blacksquare Sicher https://srv-8man.8man-demo.local/#/analyze-details:id=	1:scenariold=5d0af5ba-0e59	-4513-bcba-247343879a87		☆ :
SMAN A Cockpit O Recertification -	orce inheritance		×	🌣 🗸 👳 Anton Admin 🗸
Directories with corrupted inheritance (2)	Takes all access right inheritance for all sele	Markeling/Projekt XDokumente ts from the parent directory and restores the octed directories and their sub directories. All es contained therein will have the same		Reports Direct Excel export
Drag columns here to create groups. Path Path Path	Comment	Please enter a comment		Creste Report Available Actions Execute script
				Enforce Interstance

You can see for which directories the inheritance is enforced again. You must enter a comment.



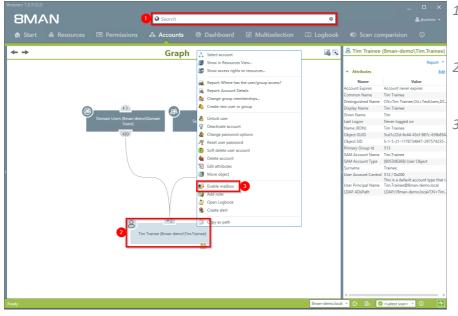
8.3 +8MATE for Exchange

8.3.1 Help Desk

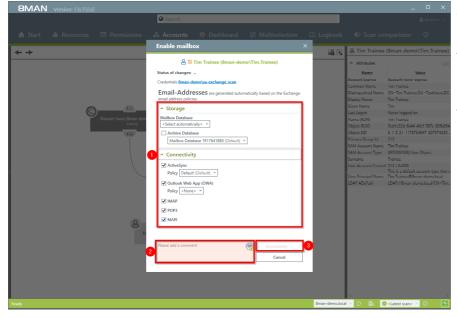
8.3.1.1 Create a mailbox (e-mail enable users)

Background / Value

If your license agreement includes 8MATE for Exchange you can create Mailboxes (email enable users) with 8MAN.



- 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.

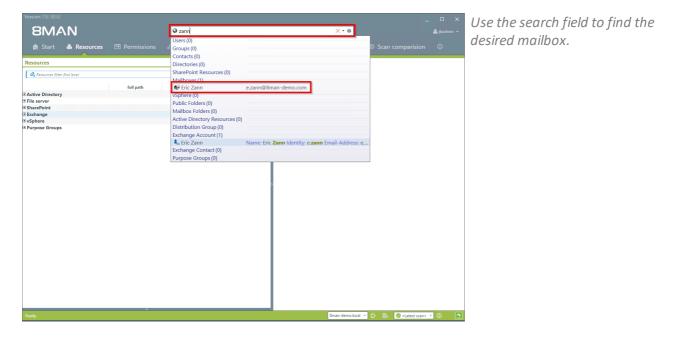


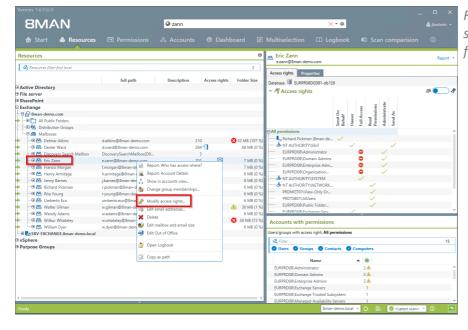
8.3.1.2 Change mailbox permissions

Background / Value

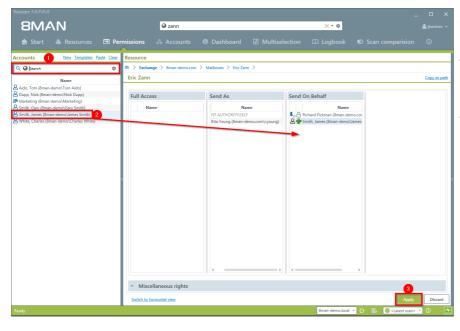
8MATE Exchange displays the access rights to Mailboxes in the resource view. Mailbox access rights are shown as follows: "Owner", "Full access", Read Access rights" and "Administrate". Additionally you can also assign the following access rights to individual users: "Full access", "Send as" and "Receive as".

Step by step process

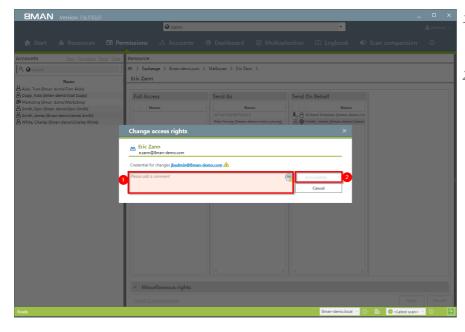




Right-click on the mailbox and select "Modify access rights" from the context menu.



- 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.

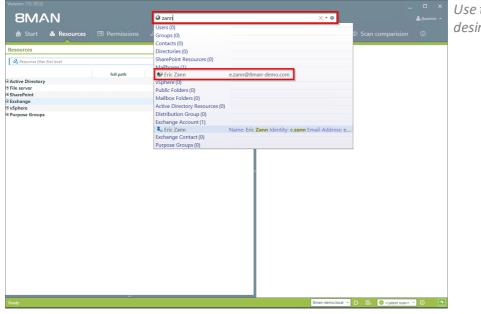


8.3.1.3 Manage out of office notices

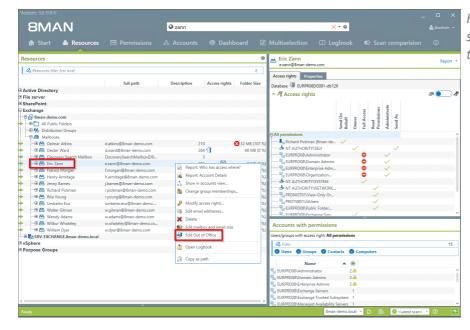
Background / Value

8MAN allows help desk to set out of office notices for employees without gaining access to email content.

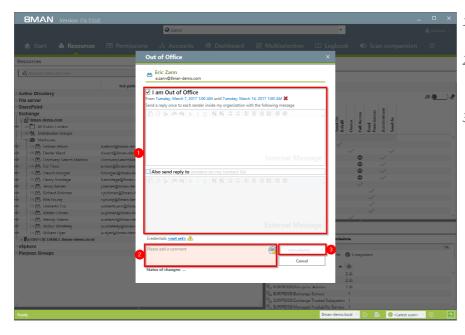
Step by step process



Use the search field to find the desired mailbox.



Right-click on the mailbox and select "Edit Out of Office" from the context menu.



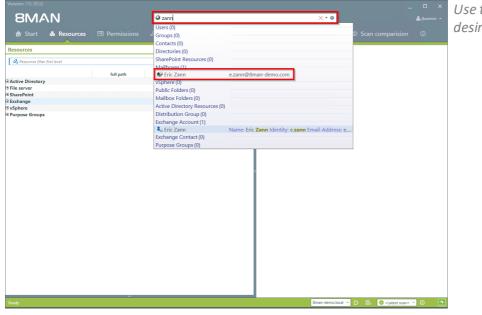
- 1. Determine the out of office settings.
- 2. You must enter a comment, for example a ticket number.
- 3. Start the process.

8.3.1.4 Manage mailbox and e-mail size

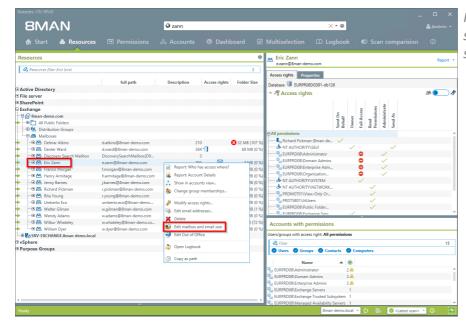
Background / Value

Managing mailbox size is a common task for help desk. 8MAN allows you to make these quickly and efficiently.

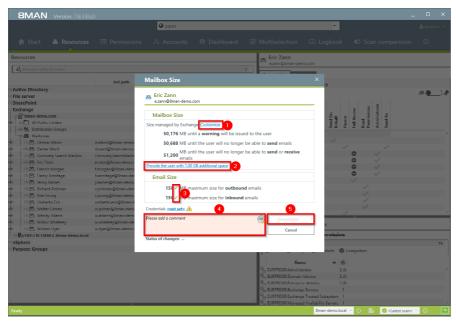
Step by step process



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.



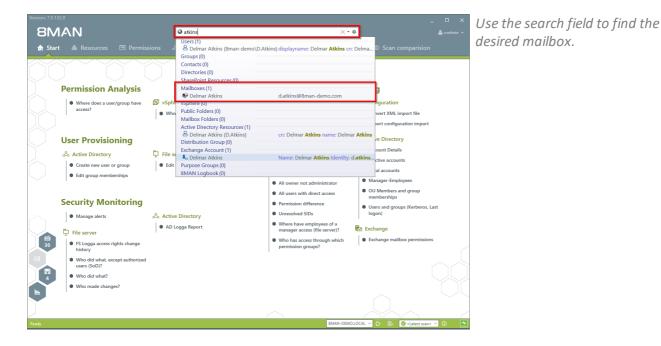
8.3.1.5 Manage e-mail addresses

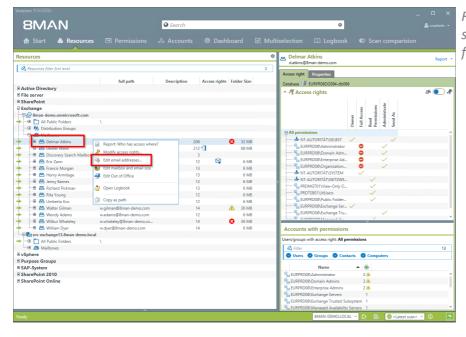
Background / Value

With 8MAN you can assign and remove multiple email addresses to mailboxes, distribution groups and contacts.

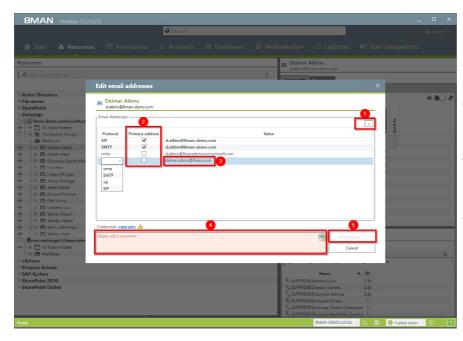
The process is documented automatically.

Step by step process





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.

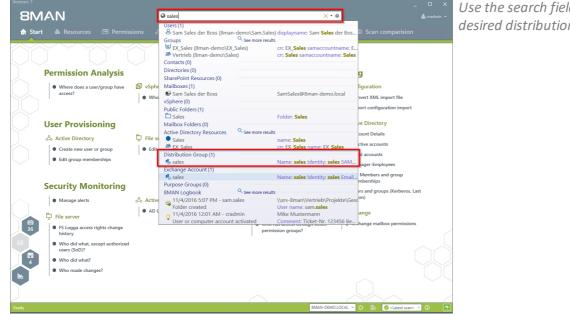


Manage distribution group memberships 8.3.1.6

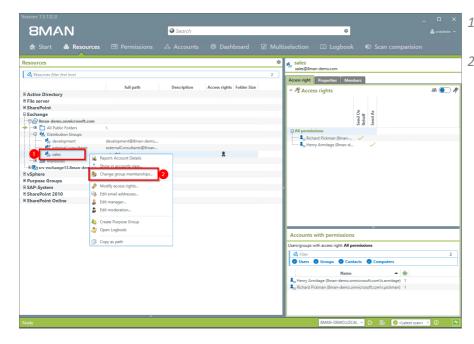
Background / Value

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".

8MAN Version: 7.		
	Search	
🏠 Start & Resou	rces 🖻 Permissions 🙏 Accounts 🔞 Dashboard 📝 Multiselection 🕮 Logbook 🔍 Scan comparision	
Resources	Add / remove group memberships ×	
Resources	Add / remove group memberships × × Accounts the transitis tatis Car New Same States der Boss (× • • • • • • • • • • • • • • • • •	¢ • 1
	ng provins / second provins (second second	
Ready	BMAN-DEMOLOCAL 🗠 🖒 📑 🖉 «Latest scan»	<mark>~</mark> () 💆

- 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".

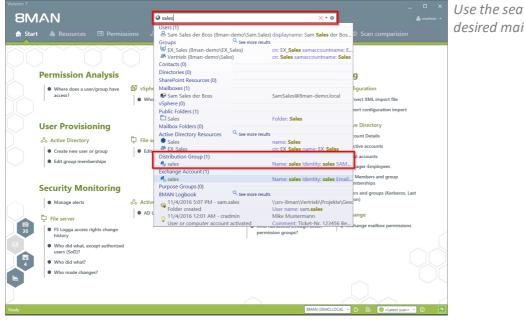


8.3.1.7 Manage distribution group permissions

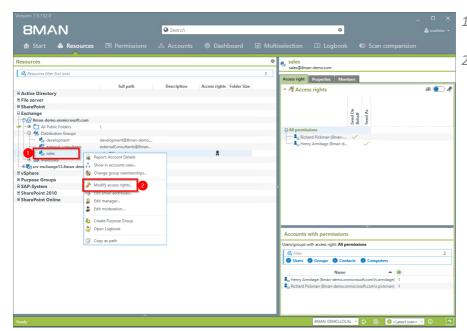
Background / Value

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.

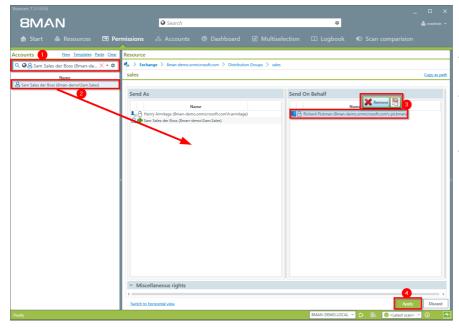
Step by step process



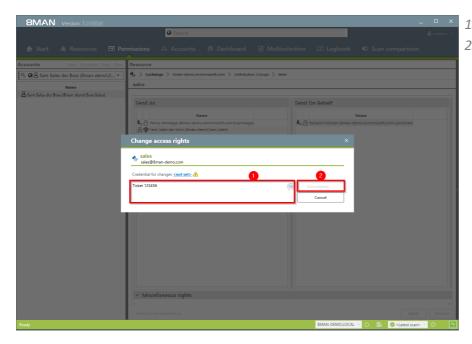
Use the search field to find the desired mailing list.



- 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.

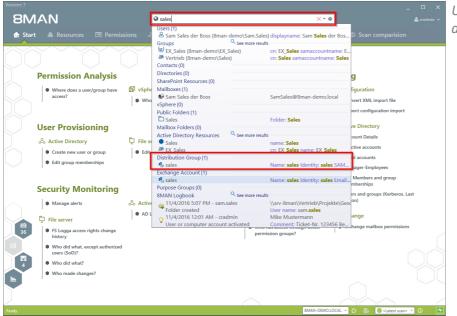
If no moderators are nominated the role is filled out by the manager of the group.

Additional Services

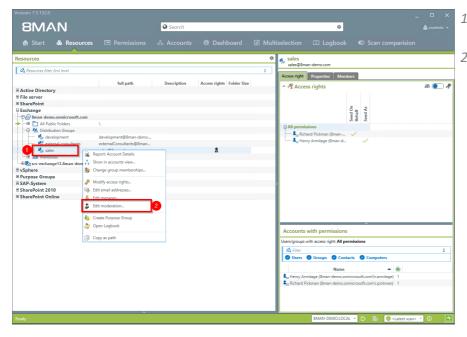
Display distribution group properties Change the manager of distribution groups

The change also works for dynamic Exchange groups.

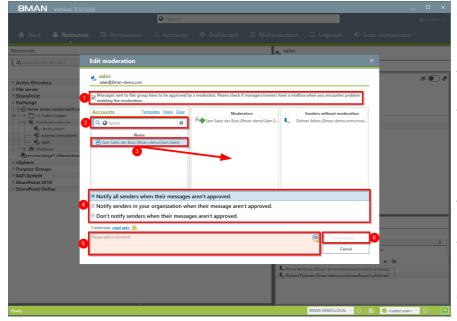
Step by step process



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

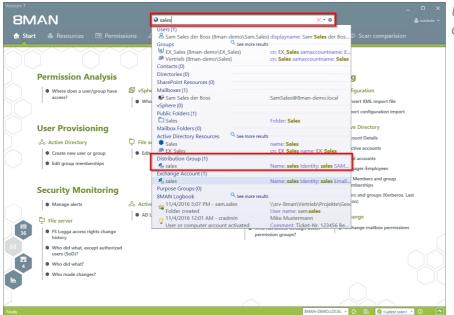
8MAN allows you to quickly change managers for distribution groups. The process is automatically documented. In the default settings, managers are the only ones allowed to change the configuration.

The change also works for dynamic Exchange groups.

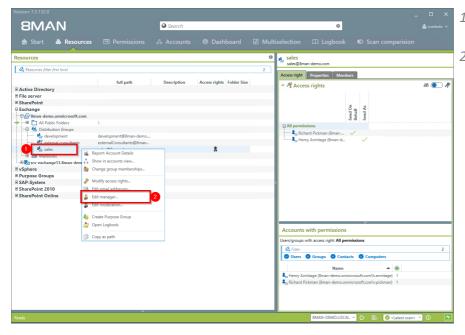
Additional Services

Display distribution group properties Modify moderation of distribution groups

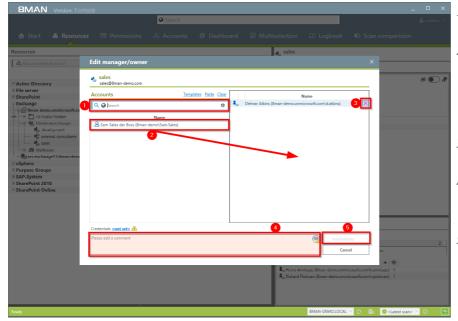
Step by step process



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

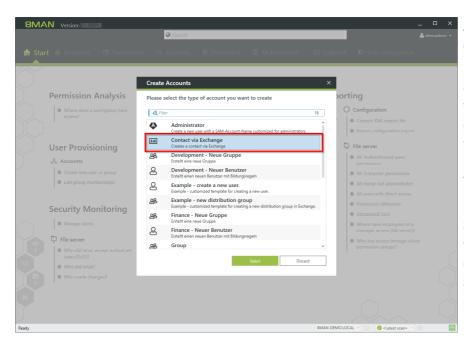
With 8MAN, you can documented create contacts and manage them quickly, e.g. to add them to distribution groups.

Additional Services

Manage distribution group memberships

	2 • • •		_
SMAN	♀ Search ons & Accounts @ Dashboard		 demosdmin • bok Ø Scan comparision
Permission Analysis Where does a user/group have access?	vSphere Who has the privilege?	Documentation & Reports overview • Reports overview • Where has the user/group access? • Who has access where?	Configuration Convert XML import file Report configuration import
User Provisioning & Accounts • Create new user or group • Edit group memberships	Resources Edit access rights	 Active Directory Account Details Inactive accounts Local accounts Manager-Employees OU Members and group 	 File server All 'Authenticated users' permissions All 'Everyone' permissions All owner not administrator All owner with direct access
Security Monitoring	 Active Directory AD Logga Report 	memberships Users and groups (Kerberos, Last logon) Ex Exchange Exchange mailbox permissions	Permission difference Unresolved SIDs Where have employees of a manager access (file server)? Who has access through which permission groups?
Users (50)? • Who did what? • Who made changes?			

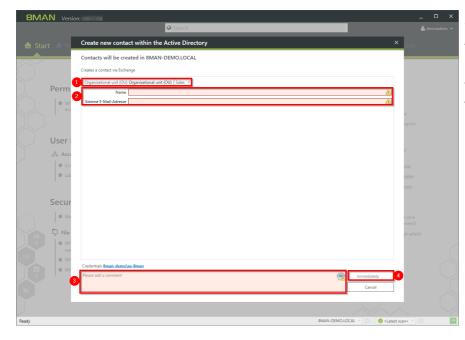
- 1. Select "Start".
- 2. Click "Create new user or group".



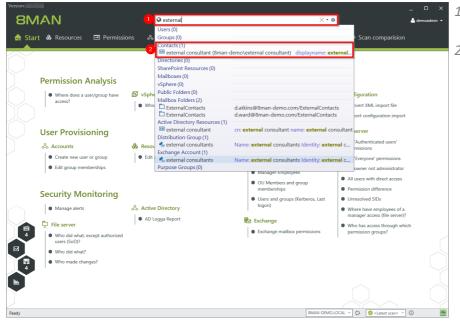
Select a template to create a contact.

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.



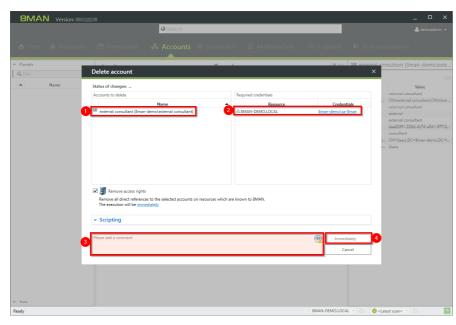
- 1. Specify an OU.
- 2. Enter names and email addresses.
- 3. You must enter a comment.
- 4. Start the execution.



- 1. Use the search to find a contact.
- 2. Click on the search result.

★ Start ♣ Resources □ Permissions ▲ Accounts ֎ Dashboard ☑ Multiselection □ Logbook ● Scan comparision ▲ Parents ▲ → ● Graph ☑ □ external consultant (Bman-demo/ee ▲ Name ★ ● Graph ☑ □ external consultant (Bman-demo/ee ▲ Name ★ ● Comono Name external consultant □ Disposible Num. Checkernal consultant Disposible Num. Comono Name □ Graph ☑ □ ■ external consultant Disposible Num. Comono Name □ Graph ■ external consultant □ Comono Name ■ external consultant	Version:								_ 🗆 ×
Prenets Graph	BIN	<i>F</i> \IN		Search	•		¢		📤 demoadmin 👻
Contract consultant (Brear-demo Userend consultant (Brear	🚖 Start	💩 Resources	Permissions	Accounts	Ø Dashboard	Multiselection	🛱 Logbook	O Scan con	nparision
Name A Attributes <			+ +	1	Graph		a 13	😐 external co	nsultant (8man-demo\exte
A Sect recent Version Bayert Arcan blaue Bayert Arcan b									Report -
Commo Name external consultant Diriging Mass. Of externa		Name 🛞							Edit
Image: Second Secon			<		Veternal consult.	Select accord to the second to	KCEESI ⁷	Common Name Distinguished Na Display Name Given Name Name (RDN) Object GUID Surname Organizational Un	external consultant CN=external consultant,CN=User external external external consultant consultant CN=Users,DC=8man-demo,DC=L.
■ Inter ØMAN-DEMOLICAL ♦ <td< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th>8MAN-DEMO LOCA</th><th></th><th>est scan> v (i)</th></td<>							8MAN-DEMO LOCA		est scan> v (i)

- 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

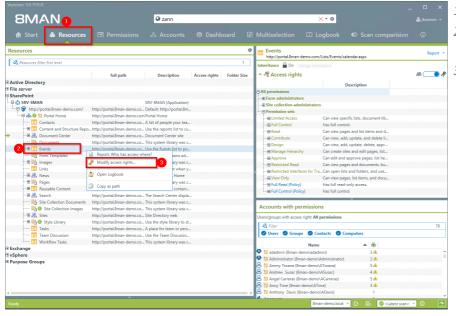
8.4.1 Data Owner

8.4.1.1 Manage SharePoint permissions

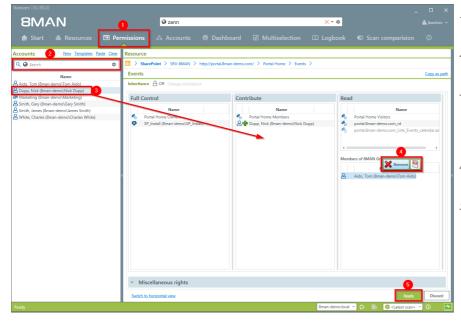
Background / Value

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".

8MAN Version:					_ 🗆 ×
	🛛 zann			·	
🚖 Start 💩 Resources 🖃 Peri					
Accounts New Templates Paste Clear	Resource				
Change acces	s rights				
Dogo, Nok Grand-drukvik (Markeing Brand-drukvik (Smith, Sary Brand-drukvik (s Bman-demokyp-Install si Altonome (so) Alko, Tom (Bman-demoky) Tom Aldo) fr ion Contribute for portal Aman-demok Dapp, Nick (Bman-demok) Mick Dupp) popp, Nick (Bman-demok) Mick Dupp) d options	om group portal.8man-dem :om_Lists_Events_calendar.a	spx_co		
Ready				8man-demo.local ~	🗦 📑 🖉 < Latest scan> 🕤 🕕 🌁

8MAN

- 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

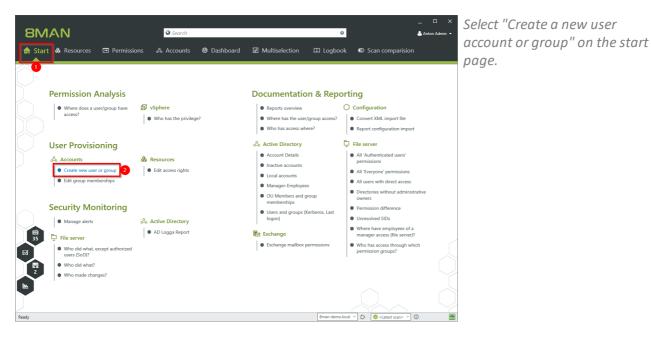
Background / Value

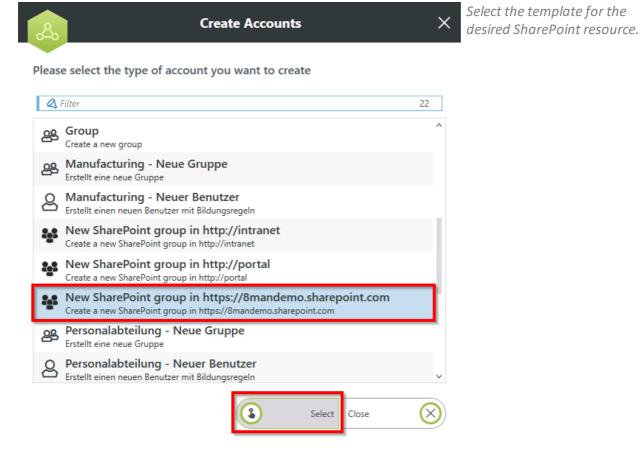
SharePoint groups can exist separately from Active Directory on a SharePoint server. Use the SharePoint Remote Connector to easily create new SharePoint groups.

Related Services

Managing access rights to SharePoint resources

Step by step process





8	Create Accounts	×
New SharePoint group in https://8ma Accounts will be created in https://8m	ndemo.sharepoint.com (Create a new SharePoint group in https://8mandemo.sharepoint.com) nandemo.sharepoint.com.	
Create a new SharePoint grou	IP	
Name Description		
Owning web site collection	Teamwebsite (https://8mandemo.sharepoint.com)	<u>3</u>
Owner Who can see the members of this group?	deal X = SharePoint Accounts (0)	
Who can modify the group memberships?	SharePoint Online Accounts (1)	-
 Membership requests 		
Credentials < <u>not set></u>		
Please add a comment	A F Immediately Close	\bigotimes

- 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.



Name		
	New SharePoint group for demo	
Description		
Owning web site collection	Teamwebsite (https://8mandemo.sharepoint.com)	v
Owner	Dexter Ward (https://8mandemo.sharepoint.com)	× D
Who can see the members of this group?	Group members	v
Who can modify the group memberships?	Owners	v
Membership requests	Owners Members	

- 1. Select who can see the members of the group.
- 2. Select who can edit the group memberships.

Create Accounts
w SharePoint group in https://8mandemo.sharepoint.com (Create a new SharePoint group in https://8mandemo.sharepoint.com) .counts will be created in https://8mandemo.sharepoint.com.
Create a new SharePoint group

Name	New SharePoint group for demo	
Description		
Owning web site collection	Teamwebsite (https://8mandemo.sharepoint.com) *	I
Owner	Dexter Ward (https://8mandemo.sharepoint.com)	
Who can see the members of this group?	Group members v	1
Who can modify the group memberships?	Owners v	
 Membership requests 		l
Allow requests to join/leave the group		I
Auto accept		I
Send requests to the following e-mail addresse	; d.ward@8man.com	I
		1
2		
Credentials d.ward@8man-demo.com	3	
Demo.		_
	Immediately Close))
-		

- × 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

8MAN Configuration 1 rsion:	NUTRO	×
Back		
* 8MAN says!	Configuration	
Credential for changes This credential will be used for any changes being made within the selected resource. If no credential were set here, they will be requested later whenever they are needed.	Change Configuration Portal Home Basic Settings Smultet changes only (smulation mode) Smultet changes only (smulation mode) I initially check perding changes without user prompting Use standard groups Credential for changes Binan-Genology.install 	
	 Access Categories 	
	 8MAN Groups 	
	Group-specific characters Construction Con	
Resources 3	Limit to the first v (1) elements	
C SharePoint	Umit to the first 1 1 and the last 4 3 p elements Name format: Turburer: Turburer: <tr< td=""><td></td></tr<>	
Ready		jbadmin @ localhost 🗲 🌁

- 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.

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



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!)

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



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

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



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

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.



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

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



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

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 you 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



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 you file servers and turns them into group memberships.

This has the following advantages:

Direct permissions cause unresolved SIDs wehen 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

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



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.

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.



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

10.1.2 For Data Owners and Administrators

10.1.2.1 Accept or reject an inquiery in Matrix 42

Please contact knowledge management for more information.

KM@8MAN.com







11.1 Software license acknowledgments

- Json.net, © 2006-2014 Microsoft, <u>https://json.codeplex.com/license</u>
- JSON.NET Copyright (c) 2007 James Newton-King <u>https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md</u>
- 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), <u>http://www.pdfsharp.net/PDFsharp_License.ashx</u>
- JetBrains Annotations, © 2007-2012 JetBrains, <u>http://www.apache.org/licenses/LICENSE-2.0</u>
- 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\protectednetworks.com\8MAN\driver (Usage only for FS Logga for Windows file server)
- NetApp Manageability SDK, © 2013 NetApp, <u>https://communities.netapp.com/docs/DOC-1152</u> (Usage only for FS Logga for NetApp Fileserver)
- WPF Shell Integration Library 3.0.50506.1, © 2008 Microsoft Corporation , <u>http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx</u>
- WPF Toolkit Library 3.5.50211.1, © Microsoft 2006-2013, <u>http://wpf.codeplex.com/license</u>
- Bootstrap, © 2011-2016 Twitter, Inc, https://github.com/twbs/bootstrap/blob/master/LICENSE
- jQuery, © 2016 The jQuery Foundation, <u>https://jquery.org/license</u>
- jquery.cookie, © 2014 Klaus Hartl, <u>https://github.com/carhartl/jquery-cookie/blob/master/MIT-LICENSE.txt</u>
- jquery-tablesort, © 2013 Kyle Fox, <u>https://github.com/kylefox/jquery-tablesort/blob/master/LICENSE</u>
- LoadingDots, © 2011 John Nelson, <u>http://johncoder.com</u>
- easyModal.js, © 2012 Flavius Matis, <u>https://github.com/flaviusmatis/easyModal.js/blob/master/LICENSE.txt</u>
- jsTimezoneDetect, © 2012 Jon Nylander
 <u>https://bitbucket.org/pellepim/jstimezonedetect/src/f9e3e30e1e1f53dd27cd0f73eb51a7e7caf7b378/</u> LICENCE.txt?at=defaultjquery-tablesort
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC <u>https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE</u>
- Mustache.js, © 2009 Chris Wanstrath (Ruby), © 2010-2014 Jan Lehnardt (JavaScript) and © 2010-2015 The mustache.js community <u>https://github.com/janl/mustache.js/blob/master/LICENSE</u>
- Metro UI CSS 2.0, © 2012-2013 Sergey Pimenov, <u>https://github.com/olton/Metro-UI-CSS/blob/master/LICENSE</u>
- Underscore.js, © 2009-2016 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors <u>https://github.com/jashkenas/underscore/blob/master/LICENSE</u>
- Ractive.js, © 2012-15 Rich Harris and contributors, <u>https://github.com/ractivejs/ractive/blob/dev/LICENSE.md</u>

428 | Access Rights Management

- RequireJS, © 2010-2015, The Dojo Foundation, <u>https://github.com/jrburke/requirejs/blob/master/LICENSE</u>
- typeahead.js, © 2013-2014 Twitter, Inc, <u>https://github.com/twitter/typeahead.js/blob/master/LICENSE</u>
- Select2, © 2012-2015 Kevin Brown, Igor Vaynberg, and Select2 contributors <u>https://github.com/select2/select2/blob/master/LICENSE.md</u>
- bootstrap-datepicker, © Copyright 2013 eternicode <u>https://github.com/eternicode/bootstrap-datepicker/blob/master/LICENSE</u>
- RabbitMQ, © Copyright 2007-2013 GoPivotal, <u>https://www.rabbitmq.com/mpl.html</u>
- EPPlus, JanKallman, <u>https://github.com/JanKallman/EPPlus/blob/master/LICENSE</u>

