8MAN

Access Rights Management. Only much Smarter.

Access Rights Management

User Manual

8.0

Protected Networks

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 2016 we have over 900 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 2017

Publisher

Protected Networks GmbH

Alt-Moabit 73
10555 Berlin

+49 30 390 63 45 - 0

Protected-Networks.com

8MAN.com

Support

+49 30 390 63 45 – 99

helpdesk@8man.com

Knowledge Base

Knowledge Management

Fabian Fischer / Jörg Brandt

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

Got Feedback?

Stephan Brack

CEO Protected Networks

Matthias Schulte-Huxel

CSO Protected Networks

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.

Protected Networks GmbH
Alt-Moabit 73
10555 Berlin

Berlin, May 2017

Content

1. Why?

1.1 Protecting data, information and knowledge

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

Access rights management answers three central questions.

Personal level

Who has access?

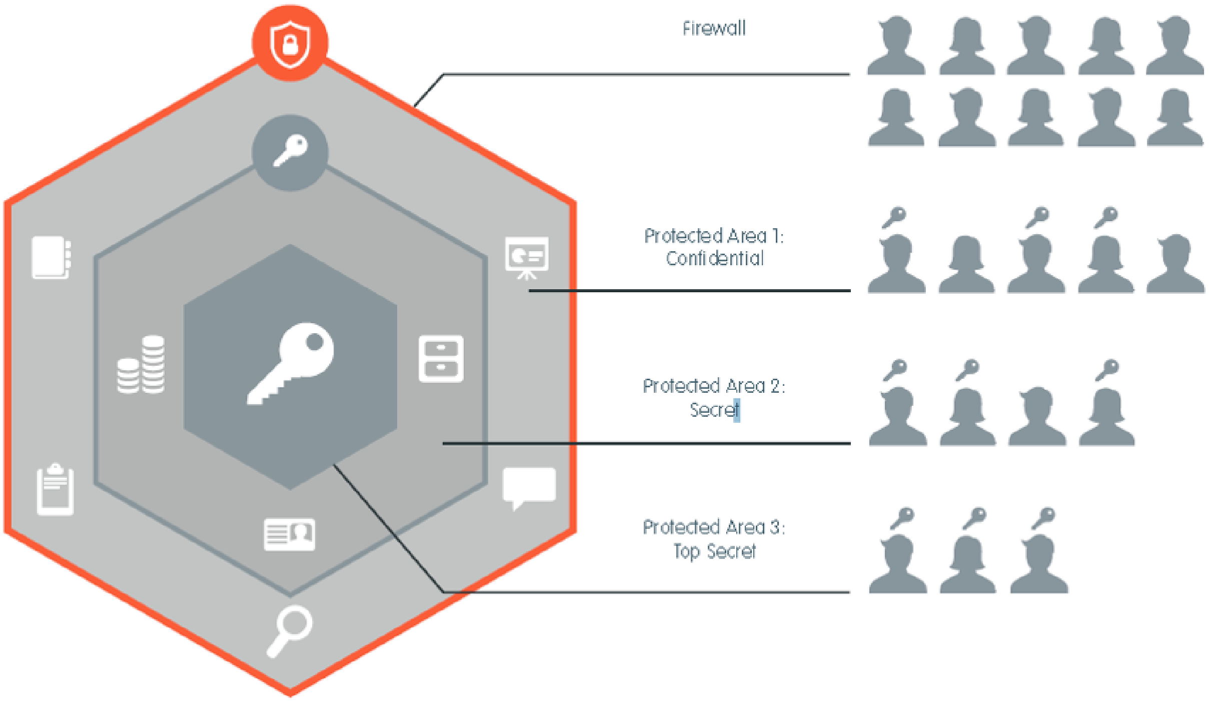
Directory level

What do they have access to?

Decision level:

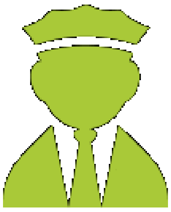
Who should have access to what?

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



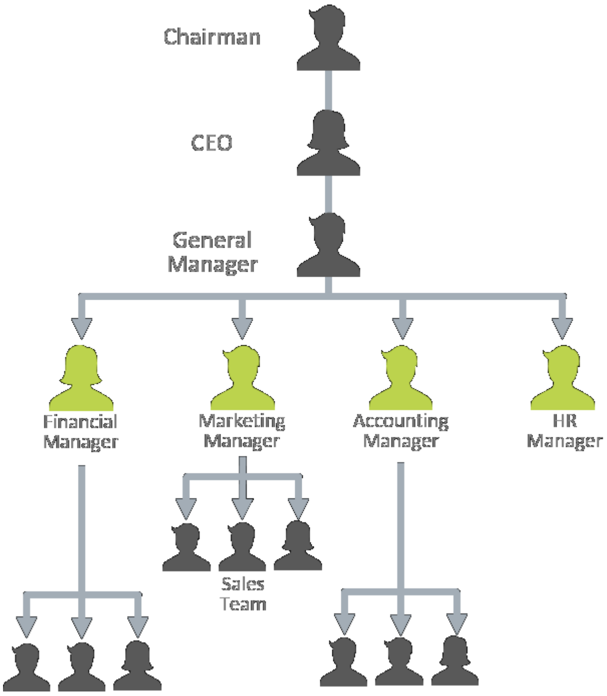
1.2 Decentralize security expertise

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



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

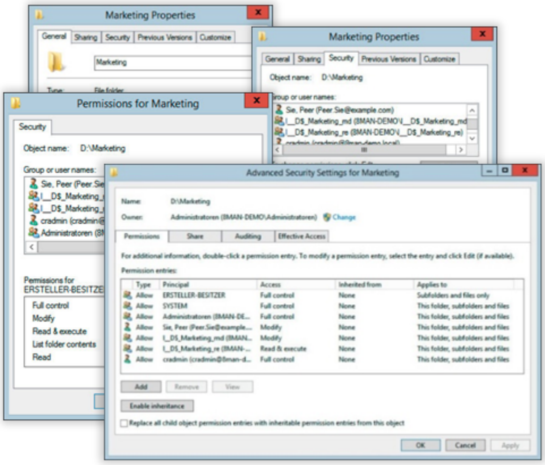
With 8MAN managers become data protectors:



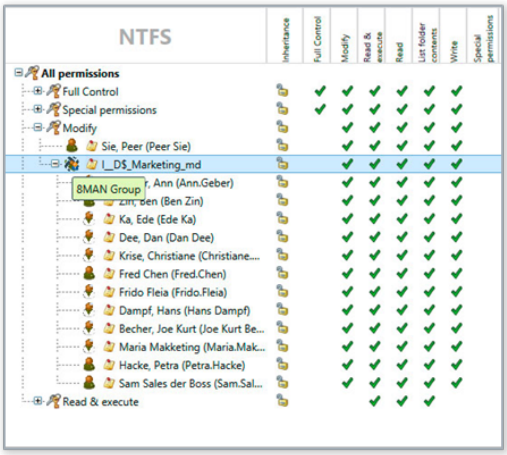
1.3 Simplify Security

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

Access rights management with native tools:


Marketing Properties
Marketing Properties
Permissions for Marketing
Advanced Security Settings for Marketing

8MAN Access Rights Management:

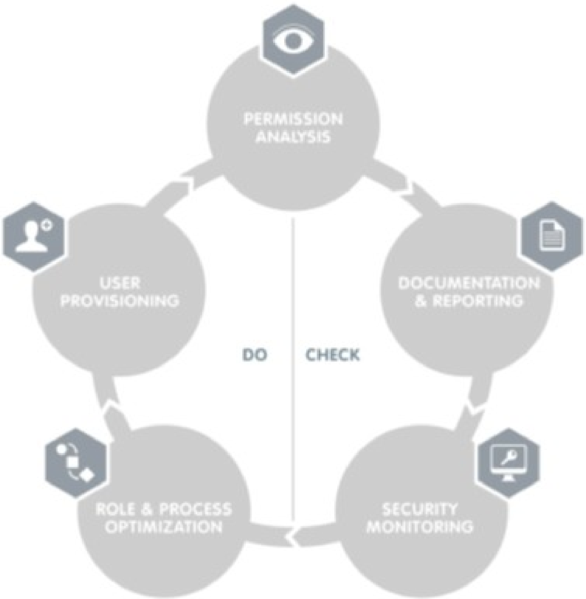


NTFS	Inheritance	Full Control	Modify	Read & execute	Read	List folder contents	Write	Special permissions
All permissions								
Full Control	🔒	✓	✓	✓	✓	✓	✓	
Special permissions	🔒	✓	✓	✓	✓	✓	✓	
Modify	🔒		✓	✓	✓	✓	✓	
Sie, Peer (Peer Sie)	🔒		✓	✓	✓	✓	✓	
I_D$_Marketing_md	🔒		✓	✓	✓	✓	✓	
r, Ann (Ann.Geber)	🔒		✓	✓	✓	✓	✓	
Zin, Ben (Ben Zin)	🔒		✓	✓	✓	✓	✓	
Ka, Ede (Ede Ka)	🔒		✓	✓	✓	✓	✓	
Dee, Dan (Dan Dee)	🔒		✓	✓	✓	✓	✓	
Krise, Christiane (Christiane....	🔒		✓	✓	✓	✓	✓	
Fred Chen (Fred.Chen)	🔒		✓	✓	✓	✓	✓	
Frido Fleia (Frido.Fleia)	🔒		✓	✓	✓	✓	✓	
Dampf, Hans (Hans Dampf)	🔒		✓	✓	✓	✓	✓	
Becher, Joe Kurt (Joe Kurt Be...	🔒		✓	✓	✓	✓	✓	
Maria Makketing (Maria.Mak...	🔒		✓	✓	✓	✓	✓	
Hacke, Petra (Petra.Hacke)	🔒		✓	✓	✓	✓	✓	
Sam Sales der Boss (Sam.Sal...	🔒		✓	✓	✓	✓	✓	
Read & execute	🔒			✓	✓	✓		

8MAN Access Rights Management makes security efficient:

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

2. The Core Disciplines of ARM



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

PERMISSION ANALYSIS

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

DOCUMENTATION & REPORTING

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

SECURITY MONITORING

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

ROLE & PROCESS OPTIMIZATION

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

USER PROVISIONING

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

2.1 Permission Analysis

8MAN analyzes the authorization situation in your company and shows who can access a given resource. In a central view, you can see the group memberships from Active Directory and the access rights to your file servers, SharePoint sites and Exchange. With this knowledge, you are able to take action and protect your company from internal security incidents.

8MAN puts you back in control. One click on the Resource view shows the actual condition of a scanned system and the employees with authorizations for it.

Available in all product versions:

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

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

8MATE for Exchange

8MATE for SharePoint

2.2 Documentation & Reporting

8MAN documents the activities in Active Directory, the file servers, SharePoint and Exchange. You can use the Calendar function to view the activities over the course of time. The mandatory comment function takes the burden off the administrator. Since a short note (a ticket number for instance) is stored, every activity is traceable, even a long time after

To the services

Available in all product versions:

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

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

8MATE for Exchange

8MATE for SharePoint

2.3 Security Monitoring

A great many employees make changes in Active Directory and to the file server. Security risks can arise without comprehensive monitoring. With our Active Directory Logga and File Server Logga, you can record all security-relevant activities in your company network. This allows you to trace what has been done in the network, by whom and when.

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

Active Directory

8MATE AD Logga
8MATE Alerts

Fileserver

8MATE FS Logga

2.4 Role & Process Optimization

The person with the best idea of who should have access and what they should be able to access is the data owner or the supervisor, not the administrator. By introducing a role concept for analysing and granting access rights, you are introducing the data awareness concept and corresponding action into the company.

You can map the organizational chart of your company with the data owner concept and cover all departments. Then you assign employees to the individual data owners. The data owners analyse or assign access rights to their staff.

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

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

There is one Add-On available:

8MATE GranMA: The ARM Self Service Portal

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 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.

3.1.2 +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

3.2 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!

Background / Value

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.

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 Visualizing nested group structures

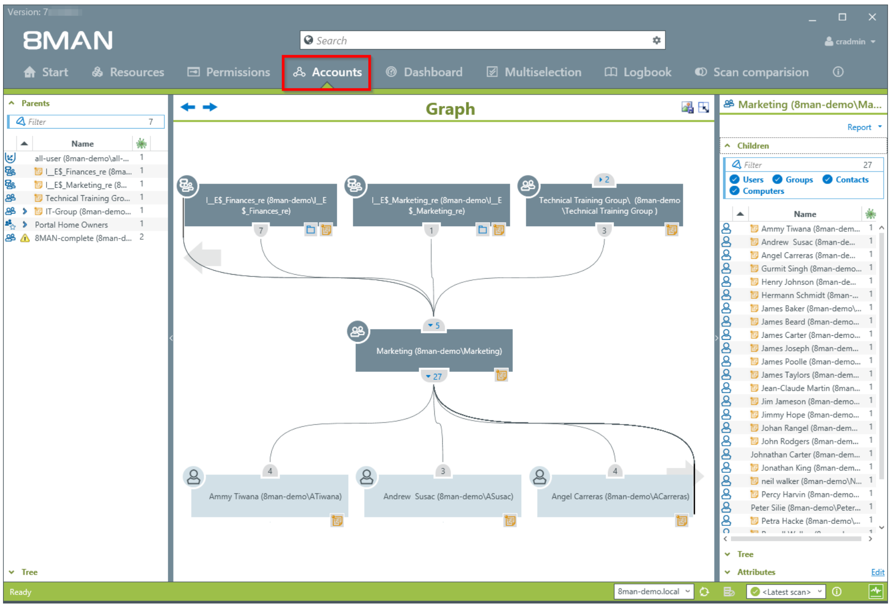
Background / Value

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.

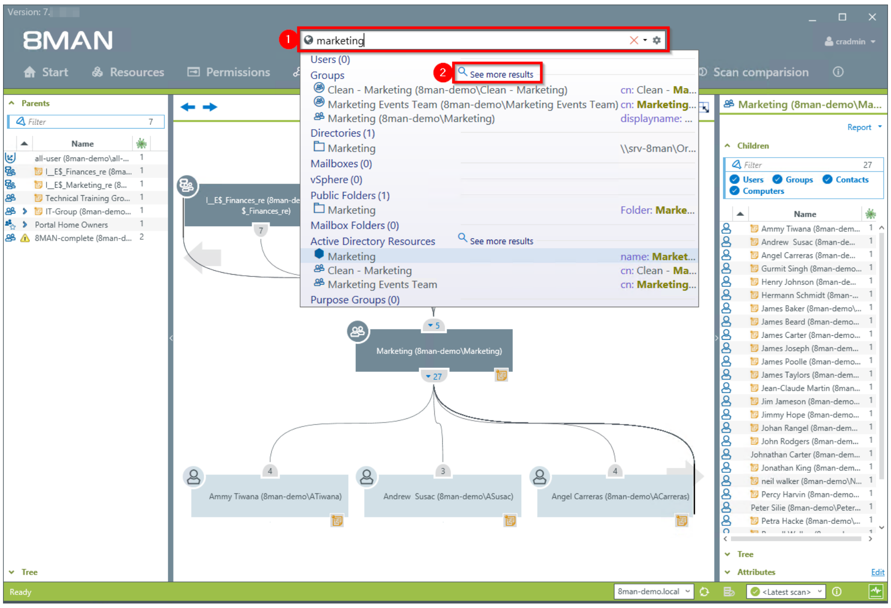
Additional Services

Identifying the depth of nesting in your AD
Identifying recursive groups

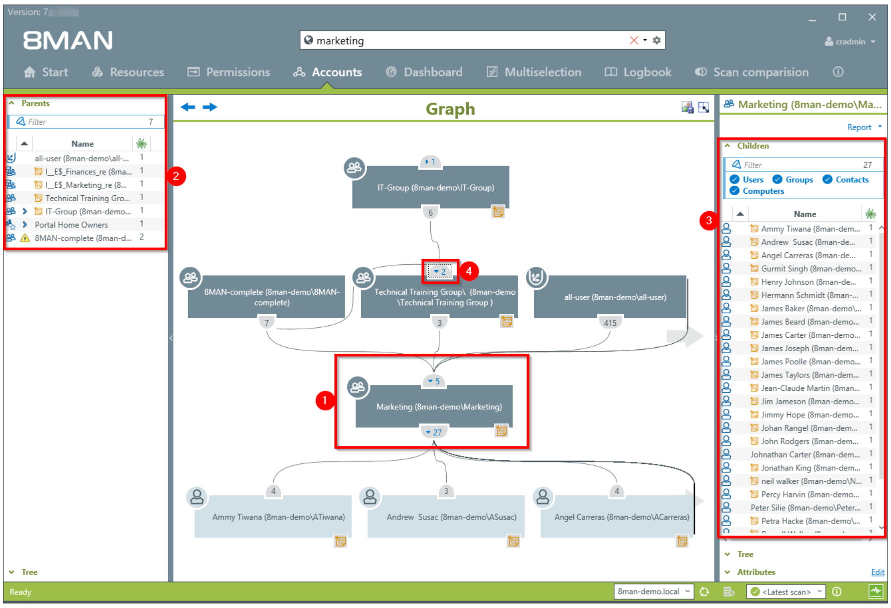
Step by step process



Switch to Accounts in the AD Graph view.


8MAN
marketing
1
2
Start
Resources
Permissions
Scan comparision
cradmin
Users (0)
Groups
See more results
Clean - Marketing (8man-demo\Clean - Marketing) cn: Clean - Ma...
Marketing Events Team (8man-demo\Marketing Events Team) cn: Marketing...
Marketing (8man-demo\Marketing) displayname: ...
Directories (1)
Marketing \\srv-8man\Or...
Mailboxes (0)
vSphere (0)
Public Folders (1)
Marketing Folder: Marke...
Mailbox Folders (0)
Active Directory Resources
See more results
Marketing name: Market...
Clean - Marketing cn: Clean - Ma...
Marketing Events Team cn: Marketing...
Purpose Groups (0)
Parents
Filter 7
Name
all-user (8man-demo\all-... 1
I_E$_Finances_re (8ma... 1
I_E$_Marketing_re (8... 1
Technical Training Gro... 1
IT-Group (8man-demo... 1
Portal Home Owners 1
8MAN-complete (8man-d... 2
I_E$_Finances_re (8man-demo\I_E$_Finances_re)
Marketing (8man-demo\Marketing)
Ammy Tiwana (8man-demo\ATiwana)
Andrew Susac (8man-demo\ASusac)
Angel Carreras (8man-demo\ACarreras)
Marketing (8man-demo\Ma...
Report
Children
Filter 27
Users Groups Contacts Computers
Ammy Tiwana (8man-dem...
Andrew Susac (8man-de...
Angel Carreras (8man-de...
Gurmit Singh (8man-demo...
Henry Johnson (8man-de...
Hermann Schmidt (8man-...
James Baker (8man-demo\...
James Beard (8man-demo...
James Carter (8man-demo...
James Joseph (8man-dem...
James Poolle (8man-demo...
James Taylors (8man-dem...
Jean-Claude Martin (8man...
Jim Jameson (8man-demo...
Jimmy Hope (8man-demo...
Johan Rangel (8man-dem...
John Rodgers (8man-dem...
Johnathan Carter (8man-dem...
Jonathan King (8man-dem...
neil walker (8man-demo\N...
Percy Harvin (8man-demo...
Peter Silie (8man-demo\Peter...
Petra Hacke (8man-demo\...
Tree
Attributes
Edit
Ready
8man-demo.local
<Latest scan>

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".


8MAN
marketing
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
cradmin
Graph
Parents
Filter 7
Name
all-user (8man-demo\all-... 1
I_E$_Finances_re (8ma... 1
I_E$_Marketing_re (8... 1
Technical Training Gro... 1
IT-Group (8man-demo... 1
Portal Home Owners 1
8MAN-complete (8man-d... 2
2
IT-Group (8man-demo\IT-Group)
8MAN-complete (8man-demo\8MAN-complete)
Technical Training Group\ (8man-demo\Technical Training Group)
all-user (8man-demo\all-user)
4
1
Marketing (8man-demo\Marketing)
Ammy Tiwana (8man-demo\ATiwana)
Andrew Susac (8man-demo\ASusac)
Angel Carreras (8man-demo\ACarreras)
3
Marketing (8man-demo\Ma...
Report
Children
Filter 27
Users Groups Contacts Computers
Name
Tree
Attributes
Edit
Ready
8man-demo.local
<Latest scan>

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)

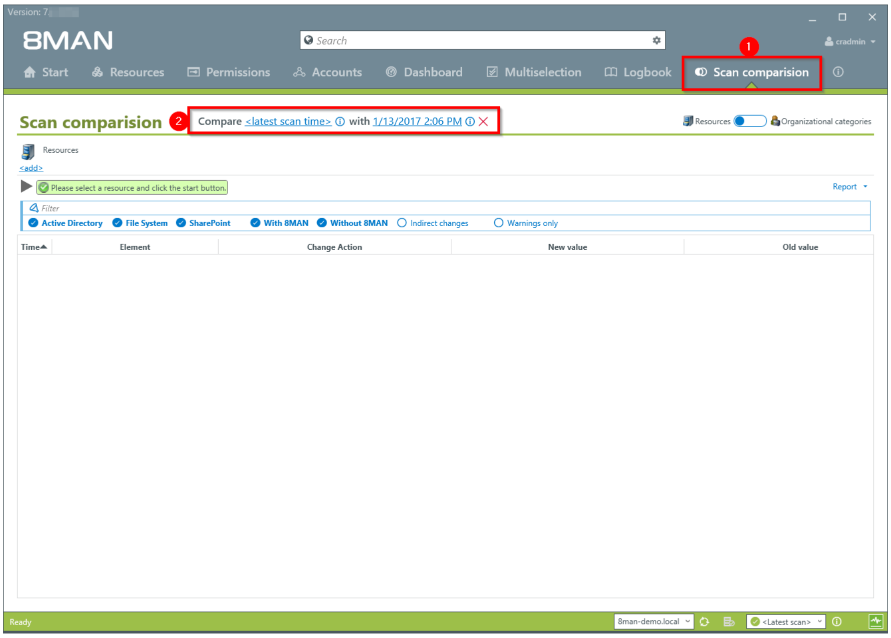
Background / Value

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 Report on Permission Differences.

Step by step process



Compare <latest scan time> with 1/13/2017 2:06 PM

Please select a resource and click the start button.

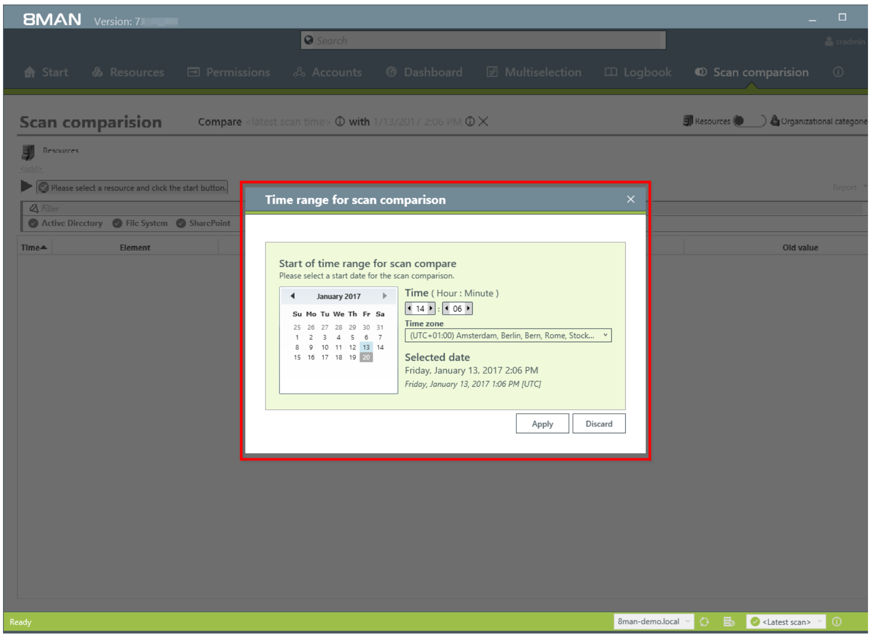
☑ Active Directory ☑ File System ☑ SharePoint ☑ With 8MAN ☑ Without 8MAN ○ Indirect changes ○ Warnings only

Time▲	Element	Change Action	New value	Old value

1. Click on "Scan comparison".

2. Select the two scans that you want to compare.

1.



Time range for scan comparison

Start of time range for scan compare
Please select a start date for the scan comparison.

January 2017

Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	

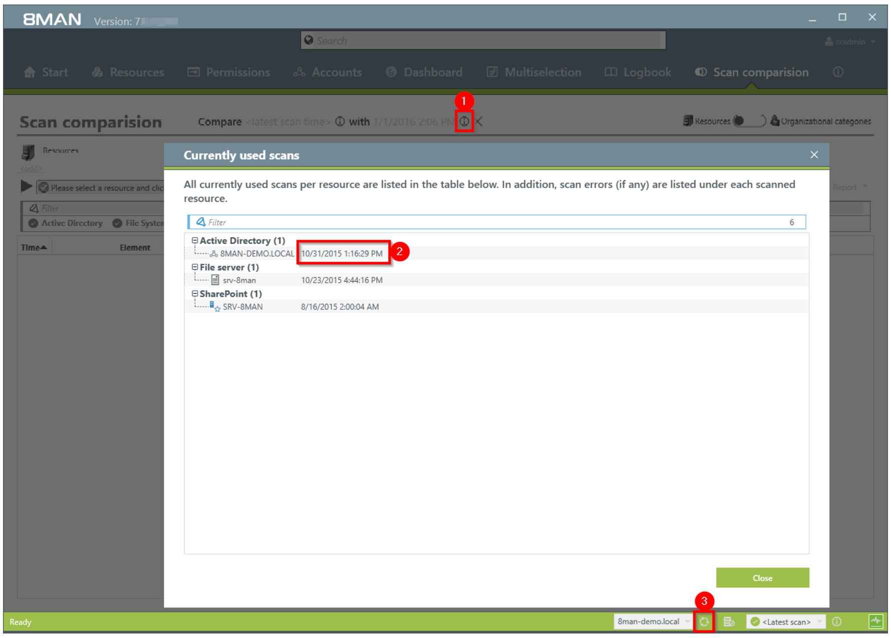
Time (Hour : Minute)
14 : 06

Time zone
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stock...

Selected date
Friday, January 13, 2017 2:06 PM
Friday, January 13, 2017 1:06 PM [UTC]

Apply Discard

Select the date and time of both scans.



Currently used scans

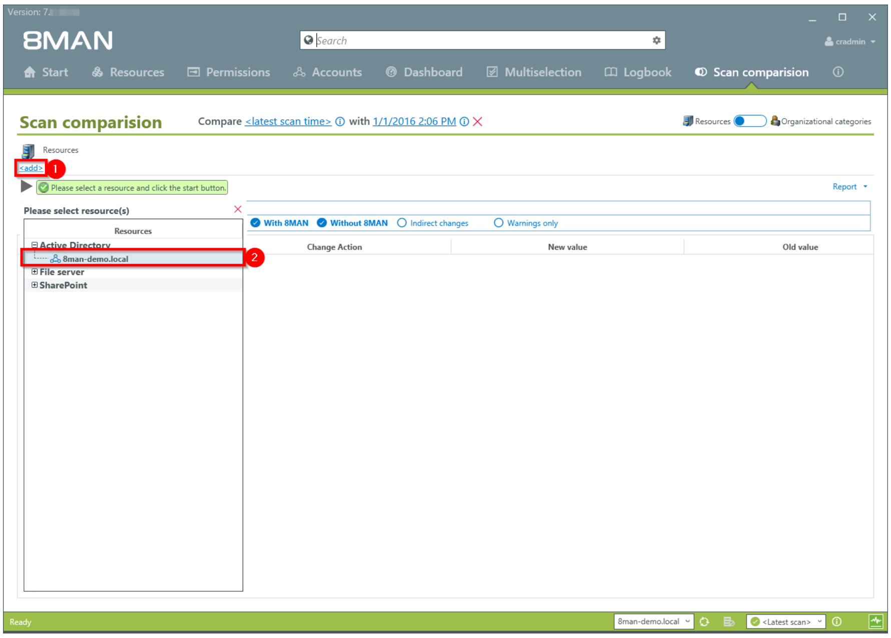
All currently used scans per resource are listed in the table below. In addition, scan errors (if any) are listed under each scanned resource.

Filter 6

Active Directory (1)	
8MAN-DEMO.LOCAL	10/31/2015 1:16:29 PM
File server (1)	
srv-8man	10/23/2015 4:44:16 PM
SharePoint (1)	
SRV-8MAN	8/16/2015 2:00:04 AM

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.*



Scan comparision

Compare <latest scan time> with 1/1/2016 2:06 PM

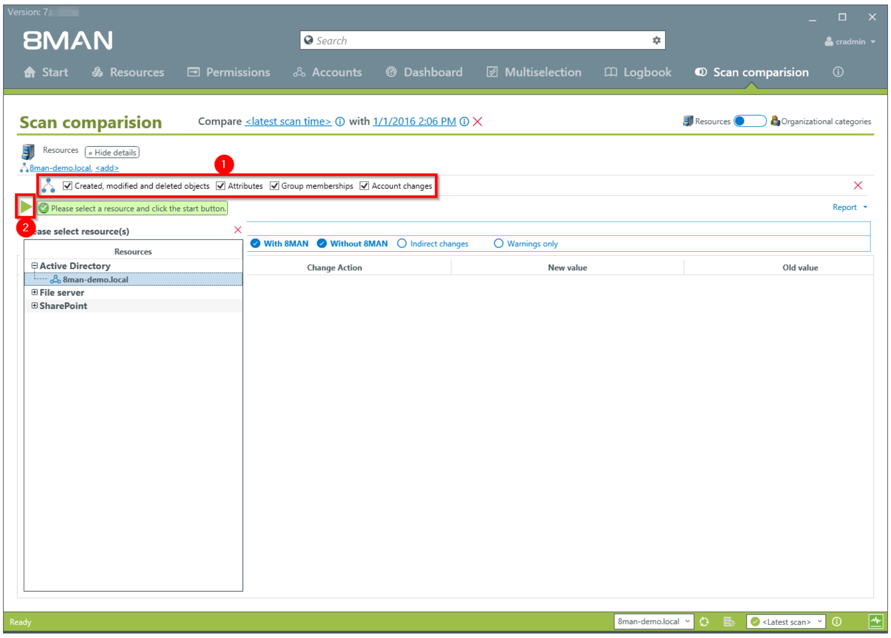
Resources / Organizational categories

Please select a resource and click the start button.

Please select resource(s)

● With 8MAN ● Without 8MAN ○ Indirect changes ○ Warnings only

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



Scan comparision

Compare <latest scan time> with 1/1/2016 2:06 PM

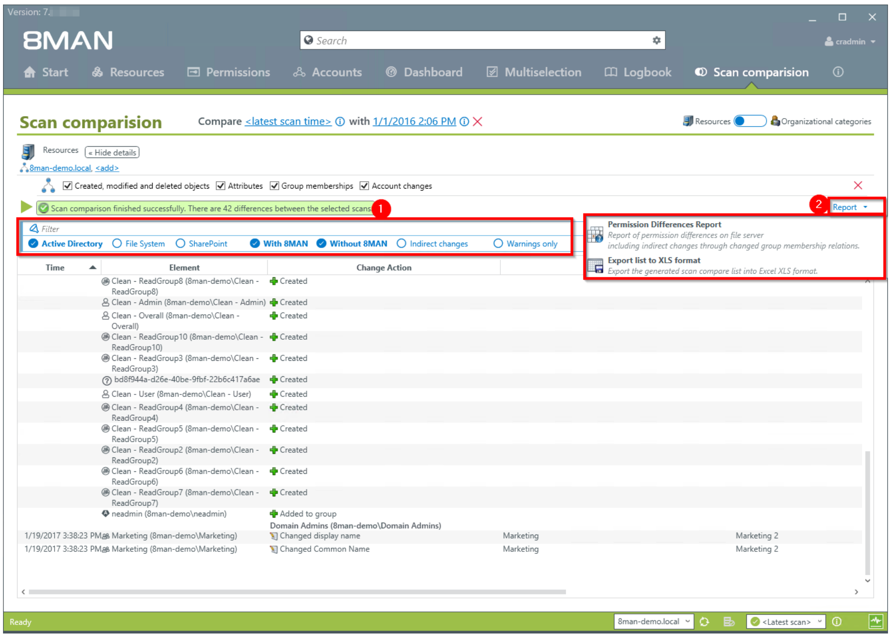
☑ Created, modified and deleted objects ☑ Attributes ☑ Group memberships ☑ Account changes

Please select a resource and click the start button.

ase select resource(s)

● With 8MAN ● Without 8MAN ○ Indirect changes ○ Warnings only

1. *Select the range of the comparison.*
2. *Start the comparison.*



Scan comparision

Compare <latest scan time> with 1/1/2016 2:06 PM

Resources

8man-demo.local, <add>

☑ Created, modified and deleted objects ☑ Attributes ☑ Group memberships ☑ Account changes

Scan comparison finished successfully. There are 42 differences between the selected scans

Filter

● Active Directory ○ File System ○ SharePoint ● With 8MAN ● Without 8MAN ○ Indirect changes ○ Warnings only

Permission Differences Report
Report of permission differences on file server including indirect changes through changed group membership relations.

Export list to XLS format
Export the generated scan compare list into Excel XLS format.

Time	Element	Change Action		
	Clean - ReadGroup8 (8man-demo\Clean - ReadGroup8)	Created		
	Clean - Admin (8man-demo\Clean - Admin)	Created		
	Clean - Overall (8man-demo\Clean - Overall)	Created		
	Clean - ReadGroup10 (8man-demo\Clean - ReadGroup10)	Created		
	Clean - ReadGroup3 (8man-demo\Clean - ReadGroup3)	Created		
	bd8f944a-d26e-40be-9fbf-22b6c417a6ae	Created		
	Clean - User (8man-demo\Clean - User)	Created		
	Clean - ReadGroup4 (8man-demo\Clean - ReadGroup4)	Created		
	Clean - ReadGroup5 (8man-demo\Clean - ReadGroup5)	Created		
	Clean - ReadGroup2 (8man-demo\Clean - ReadGroup2)	Created		
	Clean - ReadGroup6 (8man-demo\Clean - ReadGroup6)	Created		
	Clean - ReadGroup7 (8man-demo\Clean - ReadGroup7)	Created		
	neadmin (8man-demo\neadmin)	Added to group Domain Admins (8man-demo\Domain Admins)		
1/19/2017 3:38:23 PM	Marketing (8man-demo\Marketing)	Changed display name	Marketing	Marketing 2
1/19/2017 3:38:23 PM	Marketing (8man-demo\Marketing)	Changed Common Name	Marketing	Marketing 2

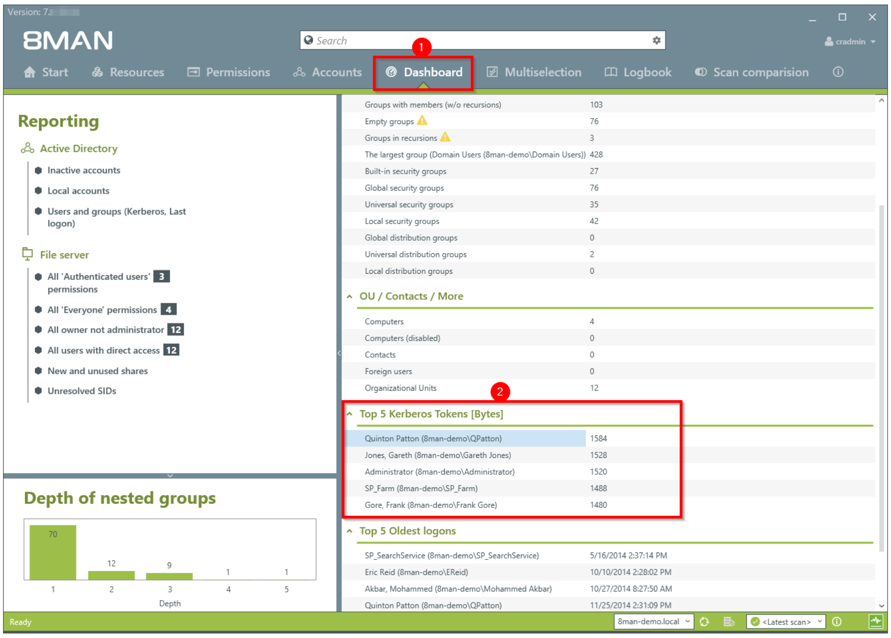
1. *Use filters to focus on specific actions.*
2. *Generate a structured "Permission Differences Report" and / or export the results to .XLS.*

4.1.1.3 Indentify users with excess privileges (on the basis of 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.

Step by step process



Groups with members (w/o recursions)	103
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	42
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

OU / Contacts / More

Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

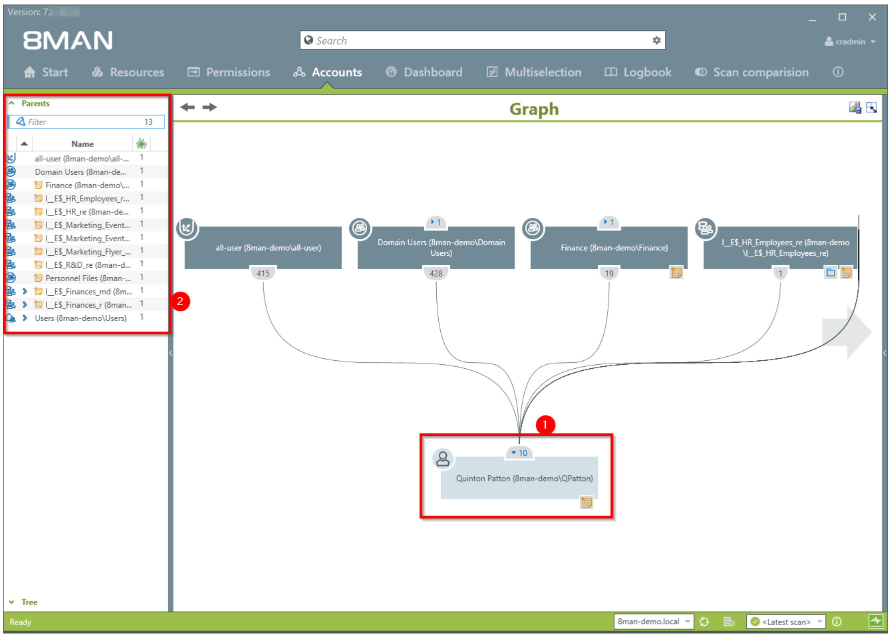
Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584
Jones, Gareth (8man-demo\Gareth Jones)	1528
Administrator (8man-demo\Administrator)	1520
SP_Farm (8man-demo\SP_Farm)	1488
Gore, Frank (8man-demo\Frank Gore)	1480

Top 5 Oldest logons

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

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



Name	
all-user (8man-demo\all-...	1
Domain Users (8man-de...	1
Finance (8man-demo\...	1
I_E$_HR_Employees_r...	1
I_E$_HR_re (8man-de...	1
I_E$_Marketing_Event...	1
I_E$_Marketing_Event...	1
I_E$_Marketing_Flyer_...	1
I_E$_R&D_re (8man-d...	1
Personnel Files (8man-...	1
I_E$_Finances_md (8m...	1
I_E$_Finances_r (8man...	1
Users (8man-demo\Users)	1

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 nested groups based on their nested depth

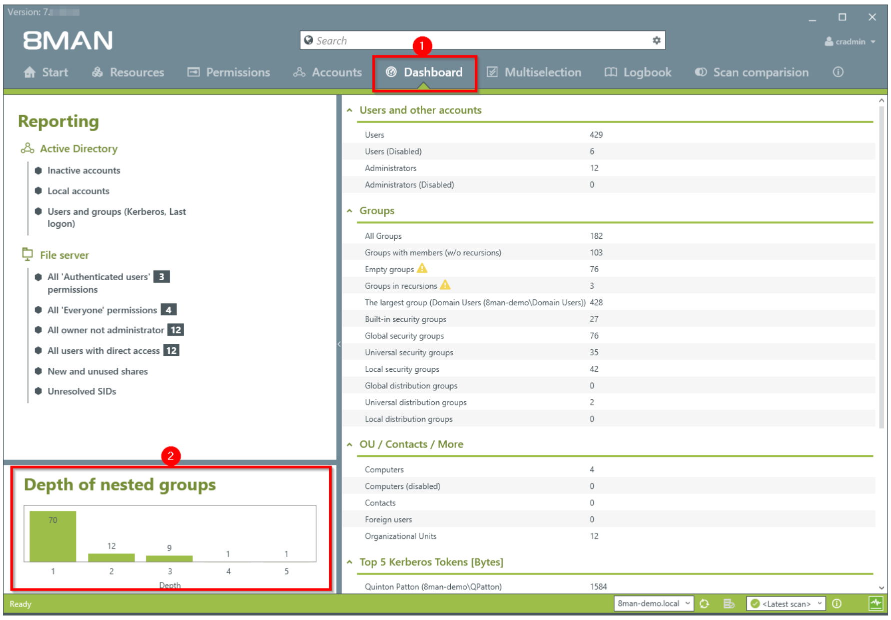
Background / Value

An AD that has grown over years often contains a large number of nested levels. The 8MAN dashboard shows nested groups up to level 10. According to Microsoft best-practice your AD should contain no more than 3 or 4 levels. 8MAN allows you to identify these critical areas of your AD and restructure them with minimal effort. In order to achieve low levels of nesting and maintain a well organized AD structure we recommend creating more groups with specific functionalities.

Additional services

Reducing several groups to one group

Step by step process



Users and other accounts

Users	429
Users (Disabled)	6
Administrators	12
Administrators (Disabled)	0

Groups

All Groups	182
Groups with members (w/o recursions)	103
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	42
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

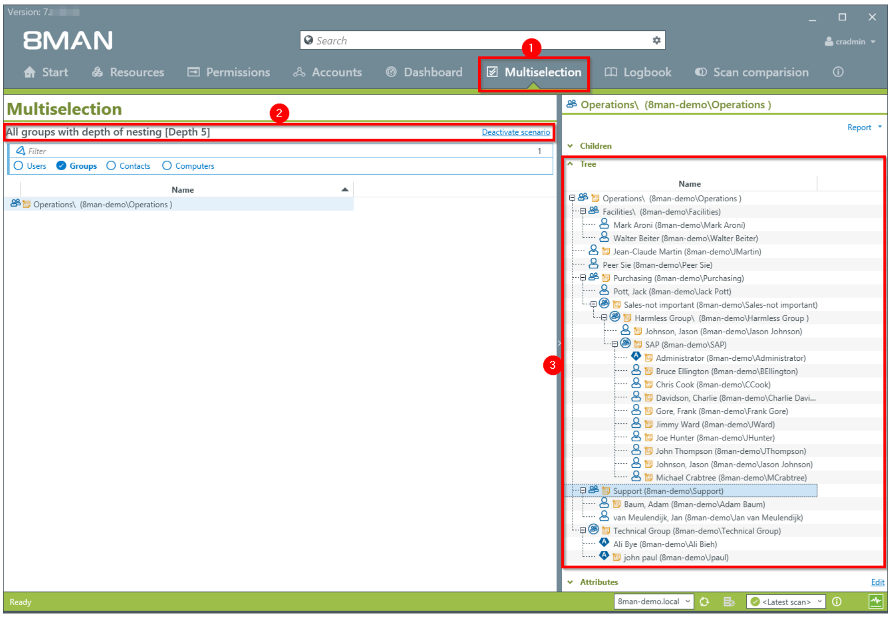
OU / Contacts / More

Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584

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



Multiselection

All groups with depth of nesting [Depth 5] Deactivate scenario

Filter 1

○ Users ● Groups ○ Contacts ○ Computers

Name
Operations\ (8man-demo\Operations)

Operations\ (8man-demo\Operations)

```
Name
⊟ 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)
  ⊟ Purchasing (8man-demo\Purchasing)
      Pott, Jack (8man-demo\Jack Pott)
    ⊟ Sales-not important (8man-demo\Sales-not important)
      ⊟ Harmless Group\  (8man-demo\Harmless Group )
          Johnson, Jason (8man-demo\Jason Johnson)
        ⊟ SAP (8man-demo\SAP)
            Administrator (8man-demo\Administrator)
            Bruce Ellington (8man-demo\BEllington)
            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)
      van Meulendijk, Jan (8man-demo\Jan van Meulendijk)
  ⊟ Technical Group (8man-demo\Technical Group)
      Ali Bye (8man-demo\Ali Bieh)
      john paul (8man-demo\Jpaul)
```

1. 8MAN automatically shows the Multiselection

1. In this scenario 8MAN automatically filters the groups by the selected nested level.

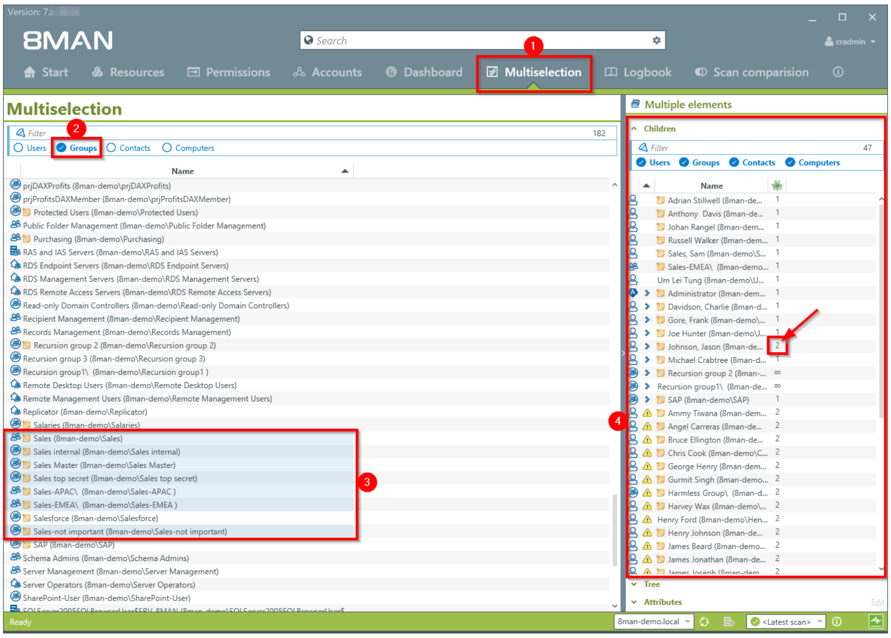
2. You can see the nested levels in the tree graph on the right hand side.

4.1.1.5 List all groups with members

Background / Value

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

Step by step process



Name
prjDAXProfits (8man-demo\prjDAXProfits)
prjProfitsDAXMember (8man-demo\prjProfitsDAXMember)
Protected Users (8man-demo\Protected Users)
Public Folder Management (8man-demo\Public Folder Management)
Purchasing (8man-demo\Purchasing)
RAS and IAS Servers (8man-demo\RAS and IAS Servers)
RDS Endpoint Servers (8man-demo\RDS Endpoint Servers)
RDS Management Servers (8man-demo\RDS Management Servers)
RDS Remote Access Servers (8man-demo\RDS Remote Access Servers)
Read-only Domain Controllers (8man-demo\Read-only Domain Controllers)
Recipient Management (8man-demo\Recipient Management)
Records Management (8man-demo\Records Management)
Recursion group 2 (8man-demo\Recursion group 2)
Recursion group 3 (8man-demo\Recursion group 3)
Recursion group1\ (8man-demo\Recursion group1)
Remote Desktop Users (8man-demo\Remote Desktop Users)
Remote Management Users (8man-demo\Remote Management Users)
Replicator (8man-demo\Replicator)
Salaries (8man-demo\Salaries)
Sales (8man-demo\Sales)
Sales internal (8man-demo\Sales internal)
Sales Master (8man-demo\Sales Master)
Sales top secret (8man-demo\Sales top secret)
Sales-APAC\ (8man-demo\Sales-APAC)
Sales-EMEA\ (8man-demo\Sales-EMEA)
Salesforce (8man-demo\Salesforce)
Sales-not important (8man-demo\Sales-not important)
SAP (8man-demo\SAP)
Schema Admins (8man-demo\Schema Admins)
Server Management (8man-demo\Server Management)
Server Operators (8man-demo\Server Operators)
SharePoint-User (8man-demo\SharePoint-User)

Name	✳
Adrian Stillwell (8man-de...	1
Anthony Davis (8man-de...	1
Johan Rangel (8man-dem...	1
Russell Walker (8man-dem...	1
Sales, Sam (8man-demo\S...	1
Sales-EMEA\ (8man-demo...	1
Um Lei Tung (8man-demo\U...	1
Administrator (8man-dem...	1
Davidson, Charlie (8man-d...	1
Gore, Frank (8man-demo\...	1
Joe Hunter (8man-demo\J...	1
Johnson, Jason (8man-de...	2
Michael Crabtree (8man-d...	1
Recursion group 2 (8man-...	∞
Recursion group1\ (8man-de...	∞
SAP (8man-demo\SAP)	1
⚠ Ammy Tiwana (8man-dem...	2
⚠ Angel Carreras (8man-de...	2
⚠ Bruce Ellington (8man-de...	2
⚠ Chris Cook (8man-demo\C...	2
⚠ George Henry (8man-dem...	2
⚠ Gurmit Singh (8man-demo...	2
⚠ Harmless Group\ (8man-d...	2
⚠ Harvey Wax (8man-demo\...	2
⚠ Henry Ford (8man-demo\Hen...	2
⚠ Henry Johnson (8man-de...	2
⚠ James Beard (8man-demo...	2
⚠ James Jonathan (8man-de...	2
⚠ James Joseph (8man-dem...	2

1. Select Multiselection.

2. Filter by groups.

3. Select the desired groups.

4. You can see an overview of all "children" of all selected groups. 8MAN also indicates if any users are included in multiple groups, for example Jason Johnson.

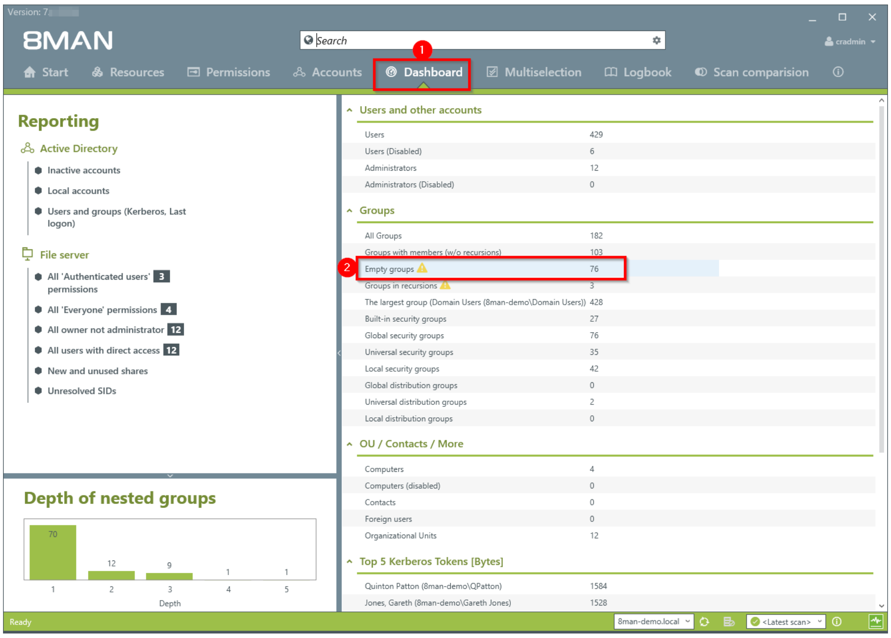
4.1.1.6 Identify empty groups

Background / Value

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

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

Step by step process



Reporting

Active Directory

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

File server

- All 'Authenticated users' permissions 3
- All 'Everyone' permissions 4
- All owner not administrator 12
- All users with direct access 12
- New and unused shares
- Unresolved SIDs

Depth of nested groups

Users and other accounts

Users	429
Users (Disabled)	6
Administrators	12
Administrators (Disabled)	0

Groups

All Groups	182
Groups with members (w/o recursions)	103
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	42
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

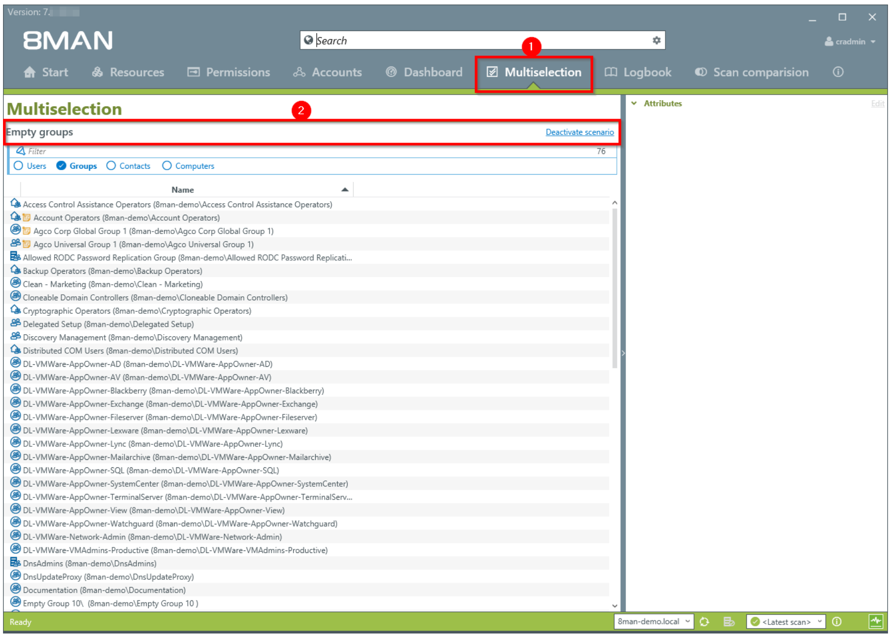
OU / Contacts / More

Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584
Jones, Gareth (8man-demo\Gareth Jones)	1528

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



Multiselection

Empty groups — Deactivate scenario

76

Name
Access Control Assistance Operators (8man-demo\Access Control Assistance Operators)
Account Operators (8man-demo\Account Operators)
Agco Corp Global Group 1 (8man-demo\Agco Corp Global Group 1)
Agco Universal Group 1 (8man-demo\Agco Universal Group 1)
Allowed RODC Password Replication Group (8man-demo\Allowed RODC Password Replicati...
Backup Operators (8man-demo\Backup Operators)
Clean - Marketing (8man-demo\Clean - Marketing)
Cloneable Domain Controllers (8man-demo\Cloneable Domain Controllers)
Cryptographic Operators (8man-demo\Cryptographic Operators)
Delegated Setup (8man-demo\Delegated Setup)
Discovery 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-AppOwner-Blackberry)
DL-VMWare-AppOwner-Exchange (8man-demo\DL-VMWare-AppOwner-Exchange)
DL-VMWare-AppOwner-Fileserver (8man-demo\DL-VMWare-AppOwner-Fileserver)
DL-VMWare-AppOwner-Lexware (8man-demo\DL-VMWare-AppOwner-Lexware)
DL-VMWare-AppOwner-Lync (8man-demo\DL-VMWare-AppOwner-Lync)
DL-VMWare-AppOwner-Mailarchive (8man-demo\DL-VMWare-AppOwner-Mailarchive)
DL-VMWare-AppOwner-SQL (8man-demo\DL-VMWare-AppOwner-SQL)
DL-VMWare-AppOwner-SystemCenter (8man-demo\DL-VMWare-AppOwner-SystemCenter)
DL-VMWare-AppOwner-TerminalServer (8man-demo\DL-VMWare-AppOwner-TerminalServ...
DL-VMWare-AppOwner-View (8man-demo\DL-VMWare-AppOwner-View)
DL-VMWare-AppOwner-Watchguard (8man-demo\DL-VMWare-AppOwner-Watchguard)
DL-VMWare-Network-Admin (8man-demo\DL-VMWare-Network-Admin)
DL-VMWare-VMAdmins-Productive (8man-demo\DL-VMWare-VMAdmins-Productive)
DnsAdmins (8man-demo\DnsAdmins)
DnsUpdateProxy (8man-demo\DnsUpdateProxy)
Documentation (8man-demo\Documentation)
Empty Group 10\ (8man-demo\Empty Group 10)

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

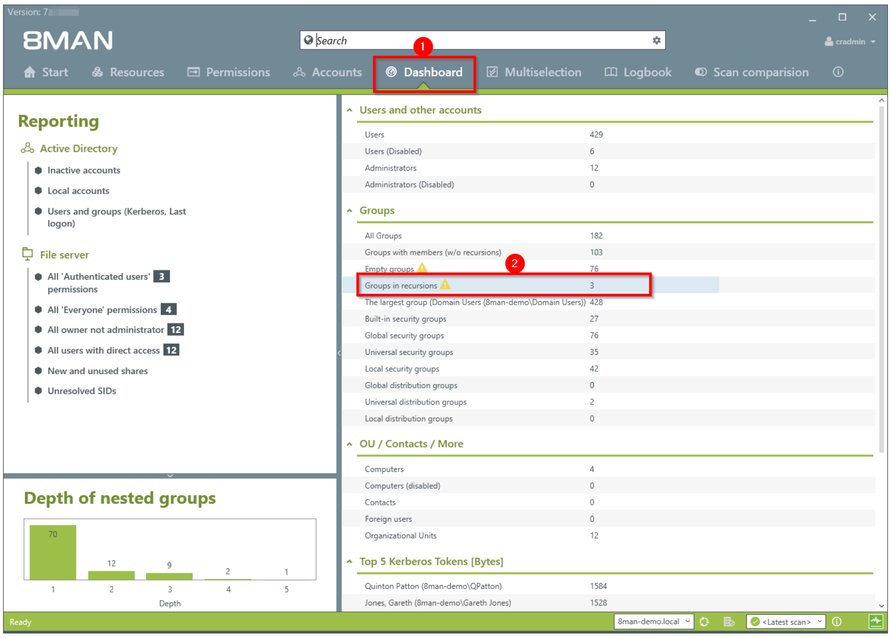
Background / Value

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.

Additional Services

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

Step by step process



Reporting

Active Directory

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

File server

- All 'Authenticated users' permissions 3
- All 'Everyone' permissions 4
- All owner not administrator 12
- All users with direct access 12
- New and unused shares
- Unresolved SIDs

Users and other accounts

Users	429
Users (Disabled)	6
Administrators	12
Administrators (Disabled)	0

Groups

All Groups	182
Groups with members (w/o recursions)	103
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	42
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

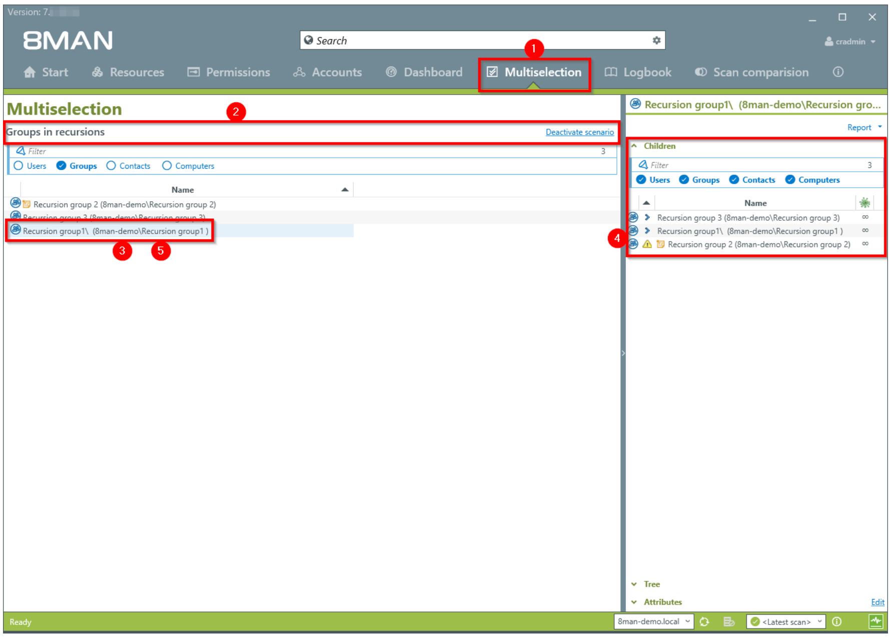
OU / Contacts / More

Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

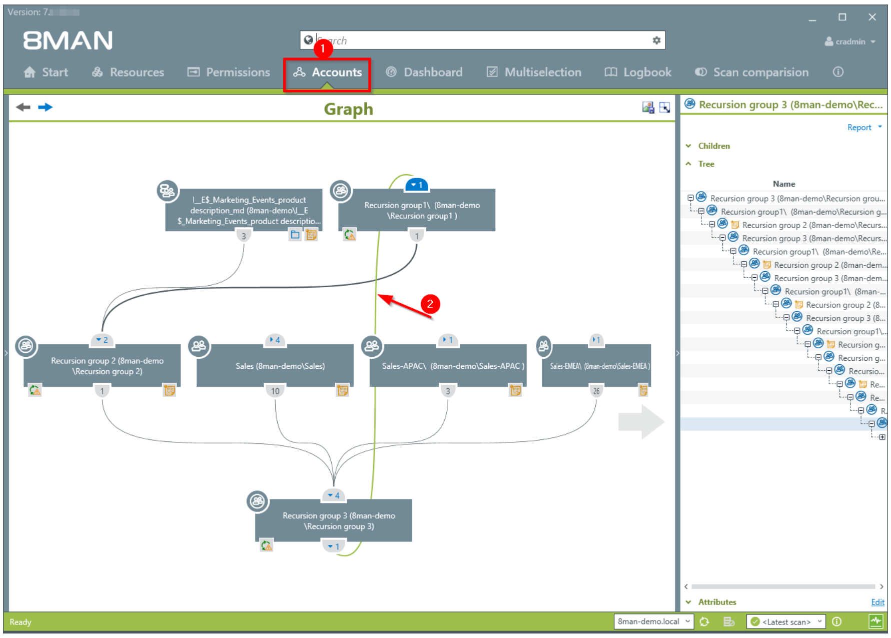
Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584
Jones, Gareth (8man-demo\Gareth Jones)	1528

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


8MAN
Search
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
cradmin
Multiselection
Groups in recursions
Deactivate scenario
Filter
Users
Groups
Contacts
Computers
Name
Recursion group 2 (8man-demo\Recursion group 2)
Recursion group 3 (8man-demo\Recursion group 3)
Recursion group1\ (8man-demo\Recursion group1)
Recursion group1\ (8man-demo\Recursion gro...
Report
Children
Recursion group 3 (8man-demo\Recursion group 3)
Recursion group1\ (8man-demo\Recursion group1)
Recursion group 2 (8man-demo\Recursion group 2)
Tree
Attributes
Edit
Ready
8man-demo.local
<Latest scan>
1
2
3
4
5

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.*


8MAN
Search
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
cradmin
Graph
I__E$_Marketing_Events_product description_md (8man-demo\I__E $_Marketing_Events_product descriptio...
Recursion group1\ (8man-demo \Recursion group1)
Recursion group 2 (8man-demo \Recursion group 2)
Sales (8man-demo\Sales)
Sales-APAC\ (8man-demo\Sales-APAC)
Sales-EMEA\ (8man-demo\Sales-EMEA)
Recursion group 3 (8man-demo \Recursion group 3)
Recursion group 3 (8man-demo\Rec...
Report
Children
Tree
Name
Attributes
Edit
Ready
8man-demo.local
<Latest scan>
1
2

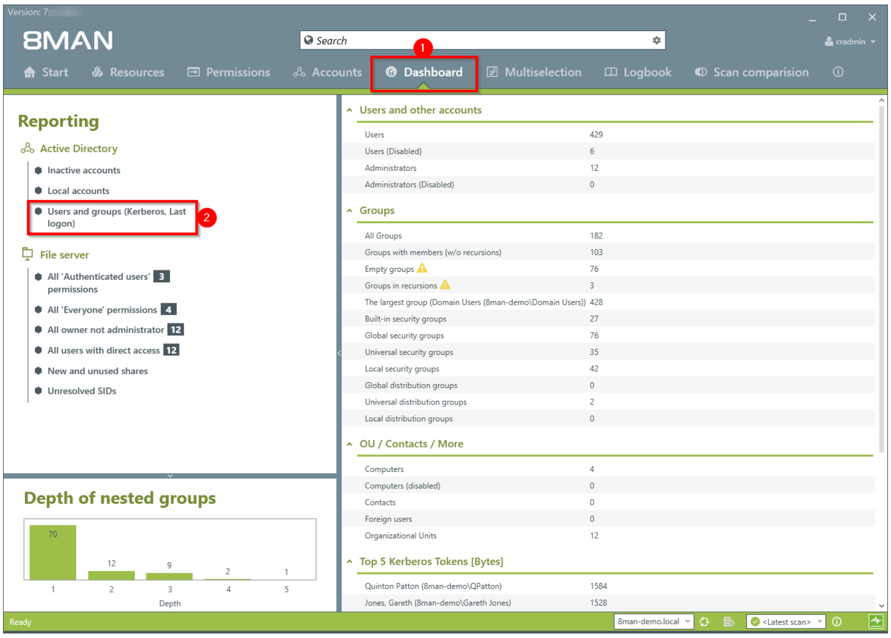
1. *8MAN switches to the account view. You can see an example of a recursion across 3 levels.*
2. *The recursion is indicated by the green line.*

4.1.1.8 Identify all users with passwords that do not expire

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".

Step by step process



Users and other accounts

Users	429
Users (Disabled)	6
Administrators	12
Administrators (Disabled)	0

Groups

All Groups	182
Groups with members (w/o recursions)	103
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	42
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

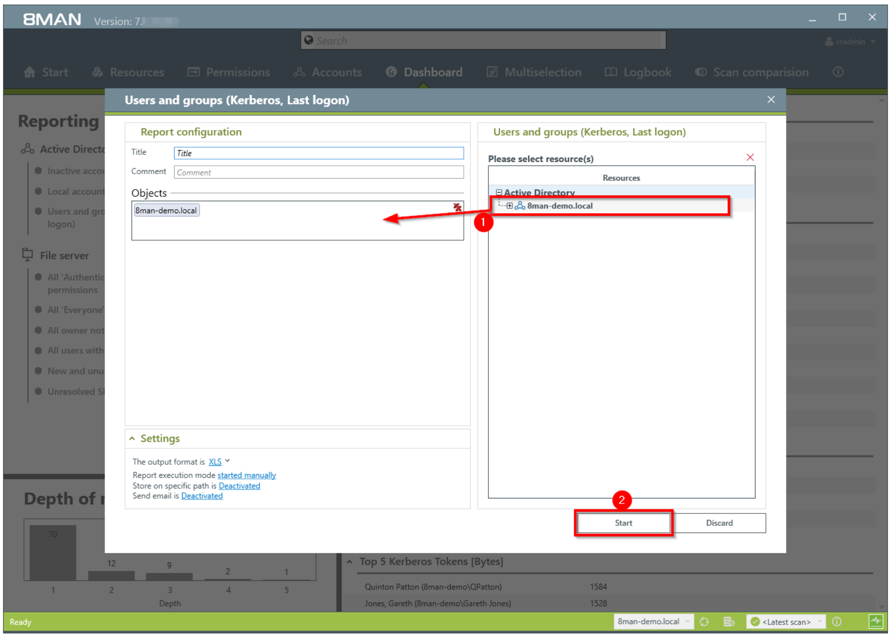
OU / Contacts / More

Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584
Jones, Gareth (8man-demo\Gareth Jones)	1528

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

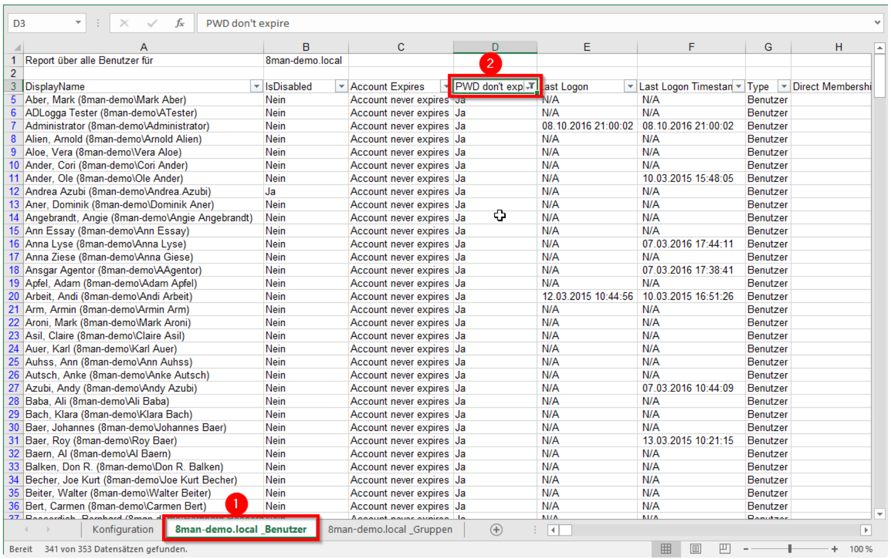


Title: Title
Comment: Comment
Objects: 8man-demo.local

Settings

The output format is XLS
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

1. *Select the range of the report via drag & drop.*
2. *Run the report.*



D3 PWD don't expire

	A	B	C	D	E	F	G	H
1	Report über alle Benutzer für	8man-demo.local						
2								
3	DisplayName	IsDisabled	Account Expires	PWD don't exp	Last Logon	Last Logon Timestan	Type	Direct Membershi
5	Aber, Mark (8man-demo\Mark Aber)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
6	ADLogga Tester (8man-demo\ATester)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
7	Administrator (8man-demo\Administrator)	Nein	Account never expires	Ja	08.10.2016 21:00:02	08.10.2016 21:00:02	Benutzer	
8	Alien, Arnold (8man-demo\Arnold Alien)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
9	Aloe, Vera (8man-demo\Vera Aloe)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
10	Ander, Cori (8man-demo\Cori Ander)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
11	Ander, Ole (8man-demo\Ole Ander)	Nein	Account never expires	Ja	N/A	10.03.2015 15:48:05	Benutzer	
12	Andrea Azubi (8man-demo\Andrea.Azubi)	Ja	Account never expires	Ja	N/A	N/A	Benutzer	
13	Aner, Dominik (8man-demo\Dominik Aner)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
14	Angebrandt, Angie (8man-demo\Angie Angebrandt)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
15	Ann Essay (8man-demo\Ann Essay)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
16	Anna Lyse (8man-demo\Anna Lyse)	Nein	Account never expires	Ja	N/A	07.03.2016 17:44:11	Benutzer	
17	Anna Ziese (8man-demo\Anna Giese)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
18	Ansgar Agentor (8man-demo\AAgentor)	Nein	Account never expires	Ja	N/A	07.03.2016 17:38:41	Benutzer	
19	Apfel, Adam (8man-demo\Adam Apfel)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
20	Arbeit, Andi (8man-demo\Andi Arbeit)	Nein	Account never expires	Ja	12.03.2015 10:44:56	10.03.2015 16:51:26	Benutzer	
21	Arm, Armin (8man-demo\Armin Arm)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
22	Aroni, Mark (8man-demo\Mark Aroni)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
23	Asil, Claire (8man-demo\Claire Asil)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
24	Auer, Karl (8man-demo\Karl Auer)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
25	Auhss, Ann (8man-demo\Ann Auhss)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
26	Autsch, Anke (8man-demo\Anke Autsch)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
27	Azubi, Andy (8man-demo\Andy Azubi)	Nein	Account never expires	Ja	N/A	07.03.2016 10:44:09	Benutzer	
28	Baba, Ali (8man-demo\Ali Baba)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
29	Bach, Klara (8man-demo\Klara Bach)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
30	Baer, Johannes (8man-demo\Johannes Baer)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
31	Baer, Roy (8man-demo\Roy Baer)	Nein	Account never expires	Ja	N/A	13.03.2015 10:21:15	Benutzer	
32	Baern, Al (8man-demo\Al Baern)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
33	Balken, Don R. (8man-demo\Don R. Balken)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
34	Becher, Joe Kurt (8man-demo\Joe Kurt Becher)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
35	Beiter, Walter (8man-demo\Walter Beiter)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	
36	Bert, Carmen (8man-demo\Carmen Bert)	Nein	Account never expires	Ja	N/A	N/A	Benutzer	

Bereit 341 von 353 Datensätzen gefunden.

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.

4.1.1.9 Analyze previous AD structures & situations

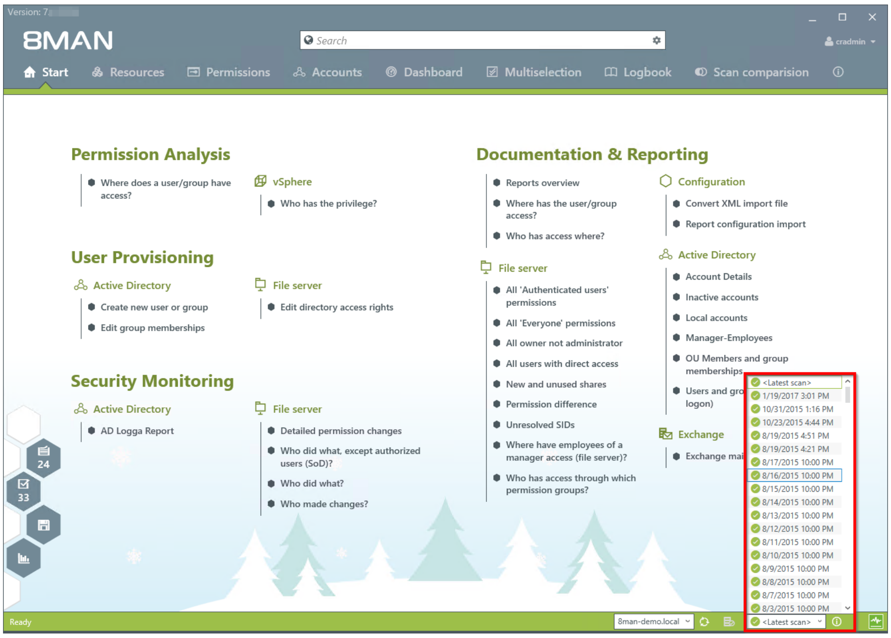
Background / Value

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

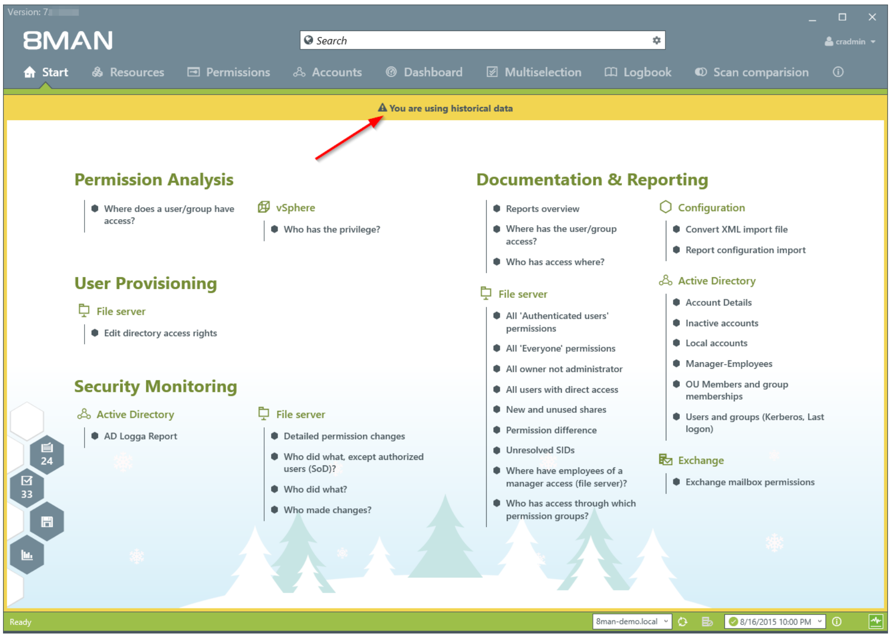
Additional Services

Alternatively you could also compare two scans from different points in time.

Step by step process



Select the desired scan date.



⚠ You are using historical data

Permission Analysis

- Where does a user/group have access?

vSphere

- Who has the privilege?

User Provisioning

File server

- Edit directory access rights

Security Monitoring

Active Directory

- AD Logga Report

File server

- Detailed permission changes
- Who did what, except authorized users (SoD)?
- Who did what?
- Who made changes?

Documentation & Reporting

- Reports overview
- Where has the user/group access?
- Who has access where?

File server

- All 'Authenticated users' permissions
- All 'Everyone' permissions
- All owner not administrator
- All users with direct access
- New and unused shares
- Permission difference
- Unresolved SIDs
- Where have employees of a manager access (file server)?
- Who has access through which permission groups?

Configuration

- Convert XML import file
- Report configuration import

Active Directory

- Account Details
- Inactive accounts
- Local accounts
- Manager-Employees
- OU Members and group memberships
- Users and groups (Kerberos, Last logon)

Exchange

- Exchange mailbox permissions

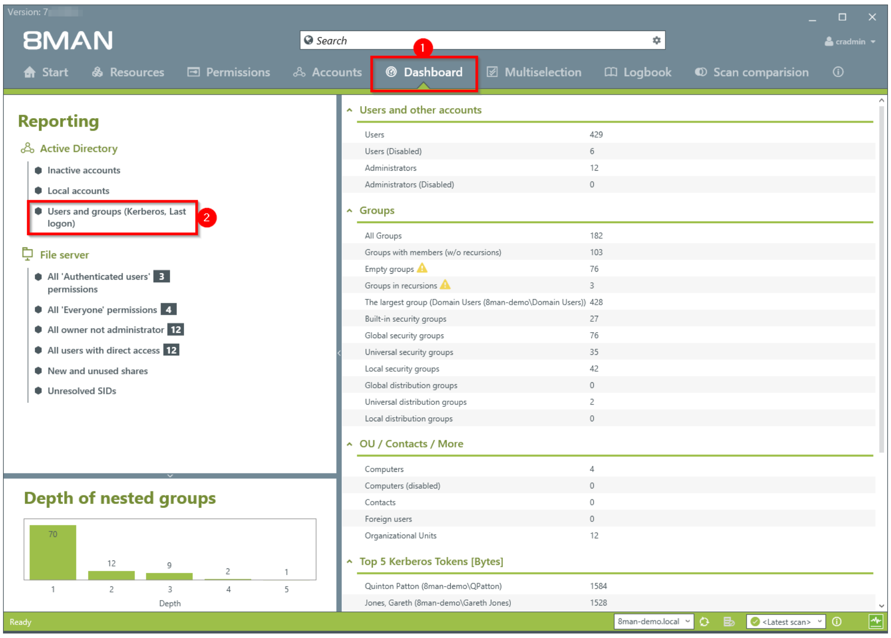
The warning and the orange frame indicate that you are viewing historical information.

4.1.1.10 Identifying 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



Reporting

Active Directory
- Inactive accounts
- Local accounts
- Users and groups (Kerberos, Last logon)

File server
- All 'Authenticated users' permissions 3
- All 'Everyone' permissions 4
- All owner not administrator 12
- All users with direct access 12
- New and unused shares
- Unresolved SIDs

Depth of nested groups

Depth	1	2	3	4	5
	70	12	9	2	1

Users and other accounts

Users	429
Users (Disabled)	6
Administrators	12
Administrators (Disabled)	0

Groups

All Groups	182
Groups with members (w/o recursions)	103
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	42
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

OU / Contacts / More

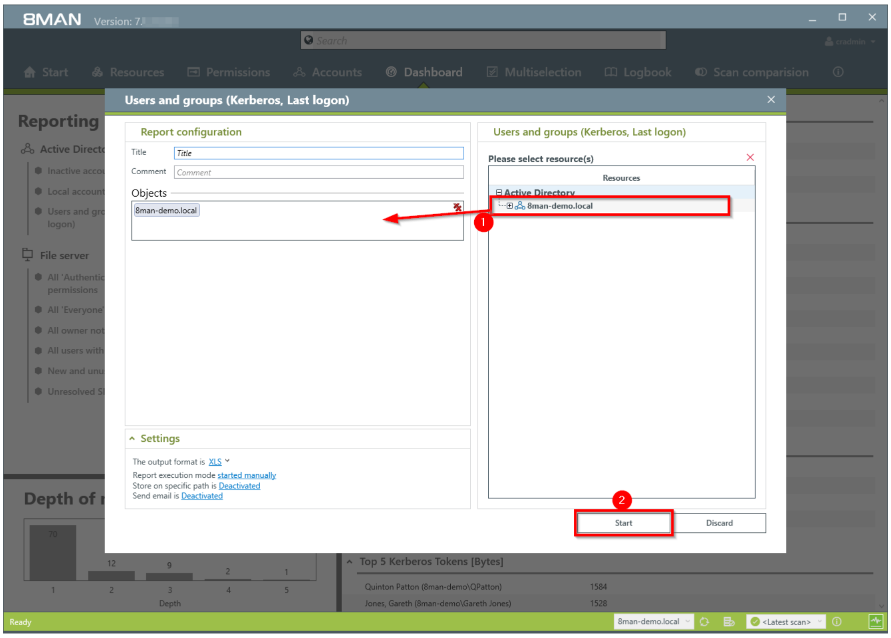
Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584
Jones, Gareth (8man-demo\Gareth Jones)	1528

1. Select the "Dashboard".

2. Click on "Users" and "Groups" in the "Reports" area.



Users and groups (Kerberos, Last logon)

Report configuration

Title: Title

Comment: Comment

Objects: 8man-demo.local

Settings

The output format is XLS

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

Users and groups (Kerberos, Last logon)

Please select resource(s)

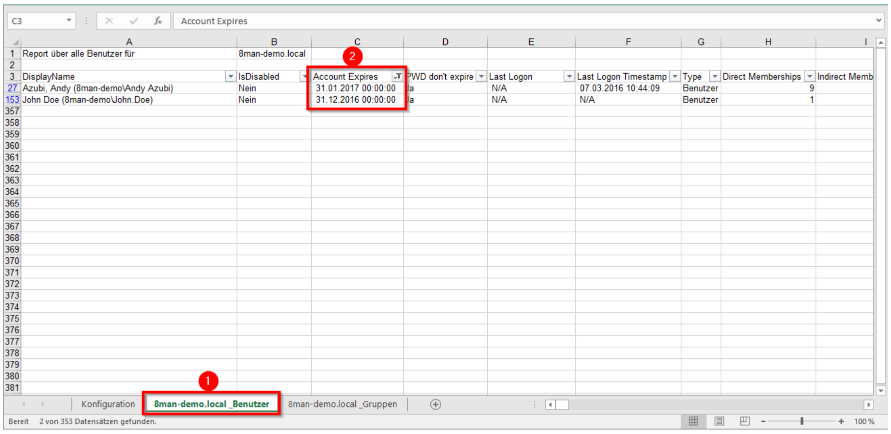
1. Select the range of the report via drag & drop.

1. Run the report.

Open the report in Excel.

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

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



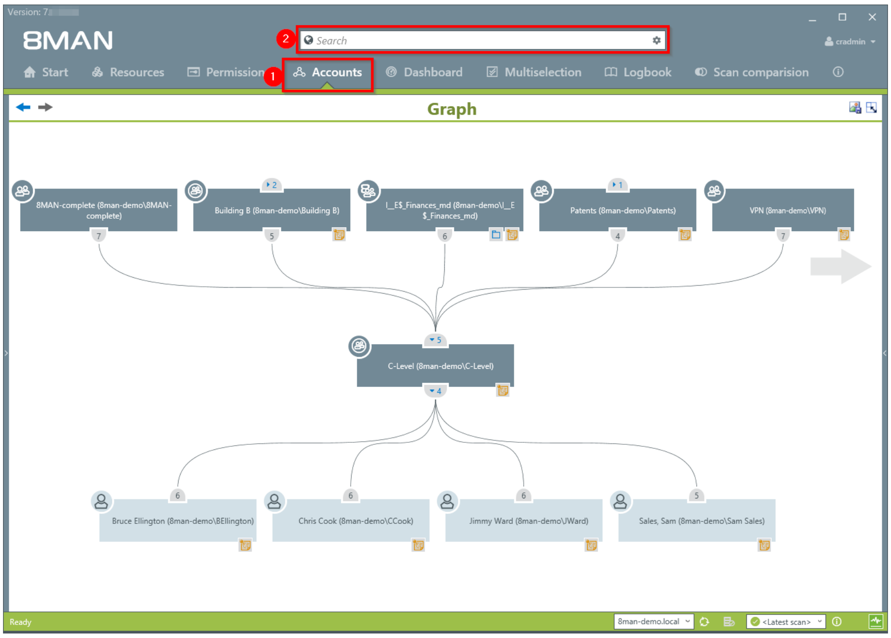
	A	B	C	D	E	F	G	H	I
1	Report über alle Benutzer für	8man-demo.local							
2									
3	DisplayName	IsDisabled	Account Expires	PWD don't expire	Last Logon	Last Logon Timestamp	Type	Direct Memberships	Indirect Memb
27	Azubi, Andy (8man-demo\Andy Azubi)	Nein	31.01.2017 00:00:00	Ja	N/A	07.03.2016 10:44:09	Benutzer	9	
153	John Doe (8man-demo\John.Doe)	Nein	31.12.2016 00:00:00	Ja	N/A	N/A	Benutzer	1	
357									
358									
359									
360									
361									
362									
363									
364									
365									
366									
367									
368									
369									
370									
371									
372									
373									
374									
375									
376									
377									
378									
379									
380									
381									

4.1.1.11 Identifying the most recent actions of a user account or AD group

Background / Value

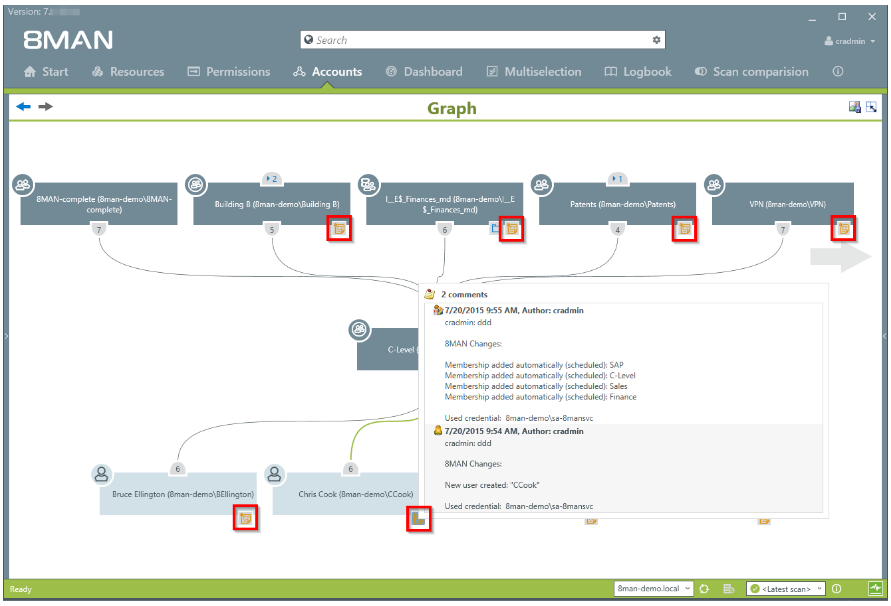
User accounts and AD groups have their own history. This is why it makes sense to review the previously performed actions and changes. 8MAN shows you a quick view of most recent activities or you can jump directly into the log book to receive a full report.

Step by step process


8MAN
Search
cradmin
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
1
2
Graph
8MAN-complete (8man-demo\8MAN-complete)
Building B (8man-demo\Building B)
I__E$_Finances_md (8man-demo\I__E $_Finances_md)
Patents (8man-demo\Patents)
VPN (8man-demo\VPN)
C-Level (8man-demo\C-Level)
Bruce Ellington (8man-demo\BEllington)
Chris Cook (8man-demo\CCook)
Jimmy Ward (8man-demo\JWard)
Sales, Sam (8man-demo\Sam Sales)
Ready
8man-demo.local
<Latest scan>

1. Select "Accounts".

2. Search for the desired user or group.


8MAN
Search
cradmin
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
Graph
8MAN-complete (8man-demo\8MAN-complete)
Building B (8man-demo\Building B)
I__E$_Finances_md (8man-demo\I__E $_Finances_md)
Patents (8man-demo\Patents)
VPN (8man-demo\VPN)
C-Level (
Bruce Ellington (8man-demo\BEllington)
Chris Cook (8man-demo\CCook)
Ready
8man-demo.local
<Latest scan>

2 comments

7/20/2015 9:55 AM, Author: cradmin
cradmin: ddd

8MAN Changes:

Membership added automatically (scheduled): SAP
Membership added automatically (scheduled): C-Level
Membership added automatically (scheduled): Sales
Membership added automatically (scheduled): Finance

Used credential: 8man-demo\sa-8mansvc

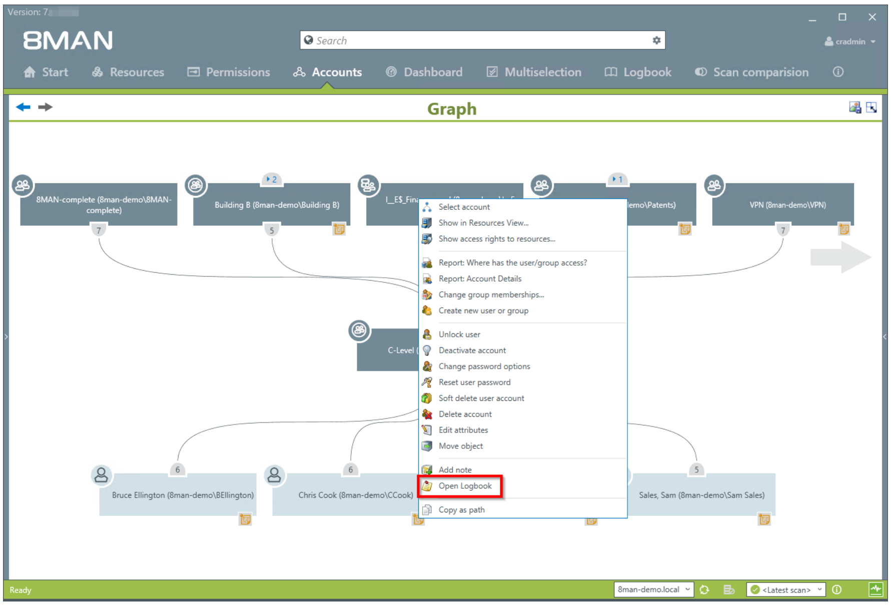
7/20/2015 9:54 AM, Author: cradmin
cradmin: ddd

8MAN Changes:

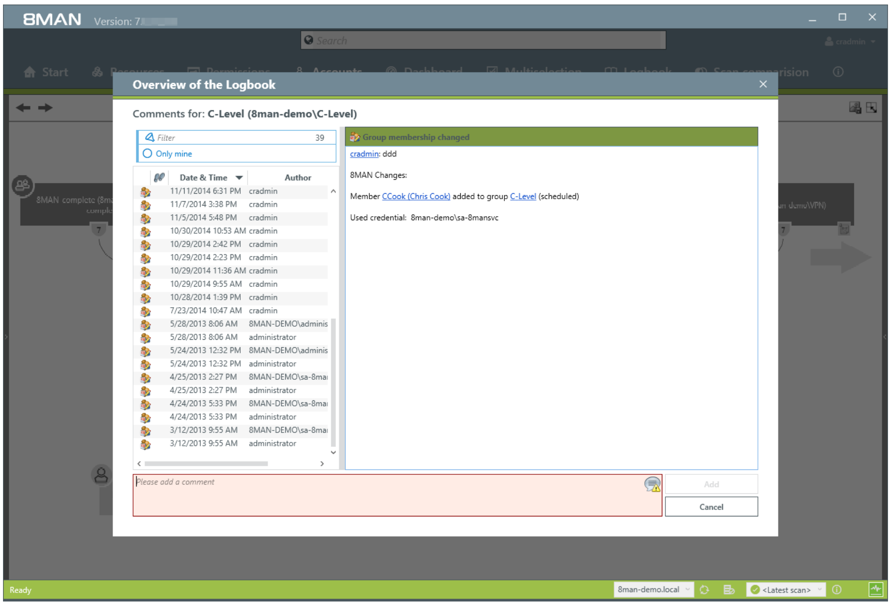
New user created: "CCook"

Used credential: 8man-demo\sa-8mansvc

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.



Comments for: **C-Level (8man-demo\C-Level)**

Date & Time	Author
11/11/2014 6:31 PM	cradmin
11/7/2014 3:38 PM	cradmin
11/5/2014 5:48 PM	cradmin
10/30/2014 10:53 AM	cradmin
10/29/2014 2:42 PM	cradmin
10/29/2014 2:23 PM	cradmin
10/29/2014 11:36 AM	cradmin
10/29/2014 9:55 AM	cradmin
10/28/2014 1:39 PM	cradmin
7/23/2014 10:47 AM	cradmin
5/28/2013 8:06 AM	8MAN-DEMO\adminis
5/28/2013 8:06 AM	administrator
5/24/2013 12:32 PM	8MAN-DEMO\adminis
5/24/2013 12:32 PM	administrator
4/25/2013 2:27 PM	8MAN-DEMO\sa-8mai
4/25/2013 2:27 PM	administrator
4/24/2013 5:33 PM	8MAN-DEMO\sa-8mai
4/24/2013 5:33 PM	administrator
3/12/2013 9:55 AM	8MAN-DEMO\sa-8mai
3/12/2013 9:55 AM	administrator

Group membership changed

cradmin: ddd

8MAN Changes:

Member CCook (Chris Cook) added to group C-Level (scheduled)

Used credential: 8man-demo\sa-8mansvc

Please add a comment

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.

4.2 Fileserver

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 Identifying 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?

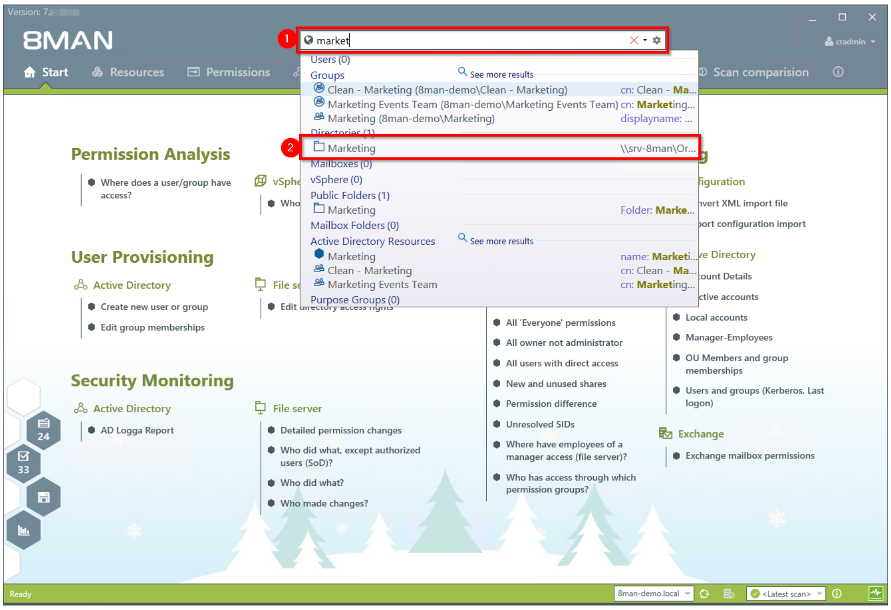
Additional Services

Report: Who has access to what?

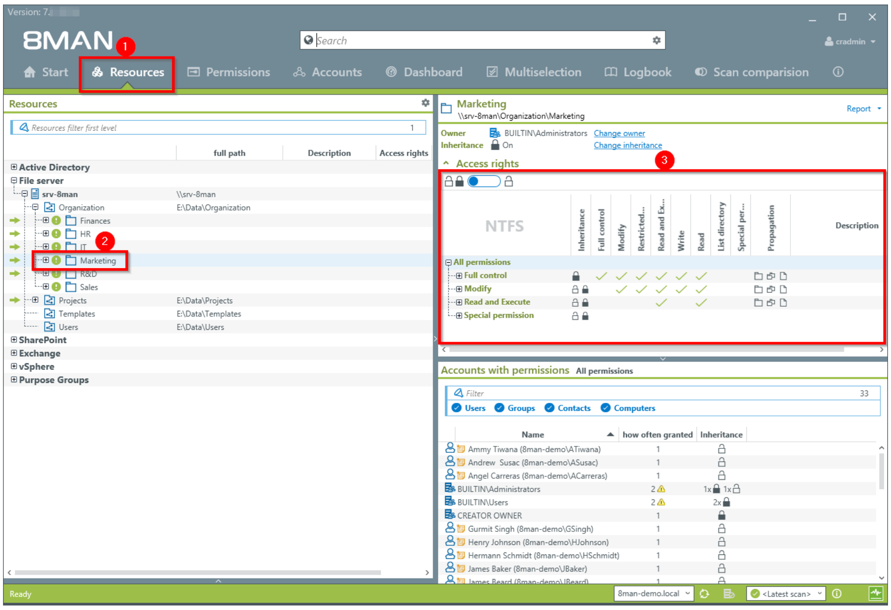
Changing folder permissions

Monitoring access to sensitive data

Step by step process



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



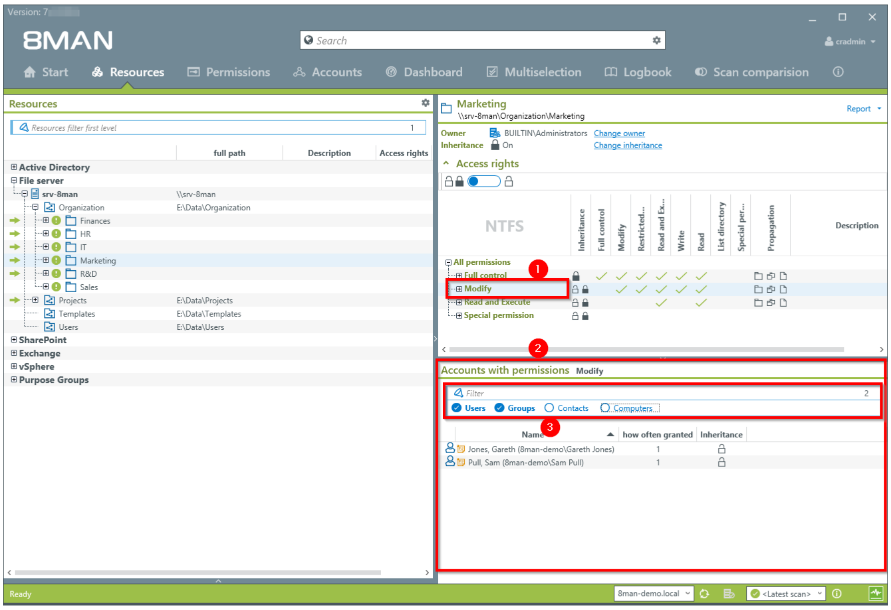
Accounts with permissions All permissions

Filter 33

✓ Users ✓ Groups ✓ Contacts ✓ Computers

Name	how often granted	Inheritance
Ammy Tiwana (8man-demo\ATiwana)	1	🔓
Andrew Susac (8man-demo\ASusac)	1	🔓
Angel Carreras (8man-demo\ACarreras)	1	🔓
BUILTIN\Administrators	2 ⚠	1x 🔒 1x 🔓
BUILTIN\Users	2 ⚠	2x 🔒
CREATOR OWNER	1	🔒
Gurmit Singh (8man-demo\GSingh)	1	🔓
Henry Johnson (8man-demo\HJohnson)	1	🔓
Hermann Schmidt (8man-demo\HSchmidt)	1	🔓
James Baker (8man-demo\JBaker)	1	🔓
James Beard (8man-demo\JBeard)	1	🔓

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.*



Accounts with permissions Modify

Filter 2

✓ Users ✓ Groups ○ Contacts ○ Computers

Name	how often granted	Inheritance
Jones, Gareth (8man-demo\Gareth Jones)	1	🔓
Pull, Sam (8man-demo\Sam Pull)	1	🔓

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 Identifying a user and their access rights

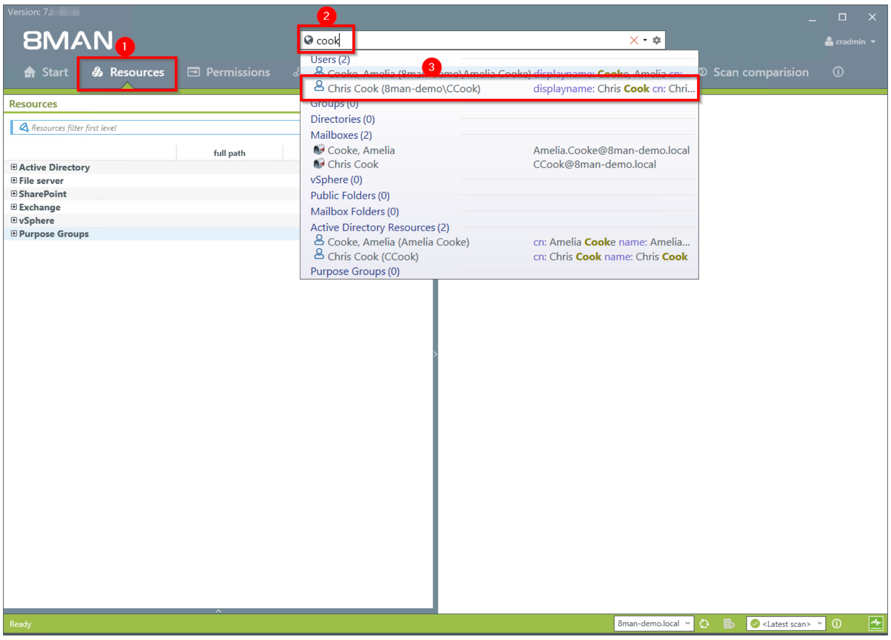
Background / Value

8MAN can also show you the user perspective, and which directories individual users have access to. This is important as it allows you to compare the rights of a given employee to the role that they fill in your organization. Here the "least privilege principle" applies. Employees who have changed departments several times often still have access rights from previous roles that could have been removed after taking on new roles.

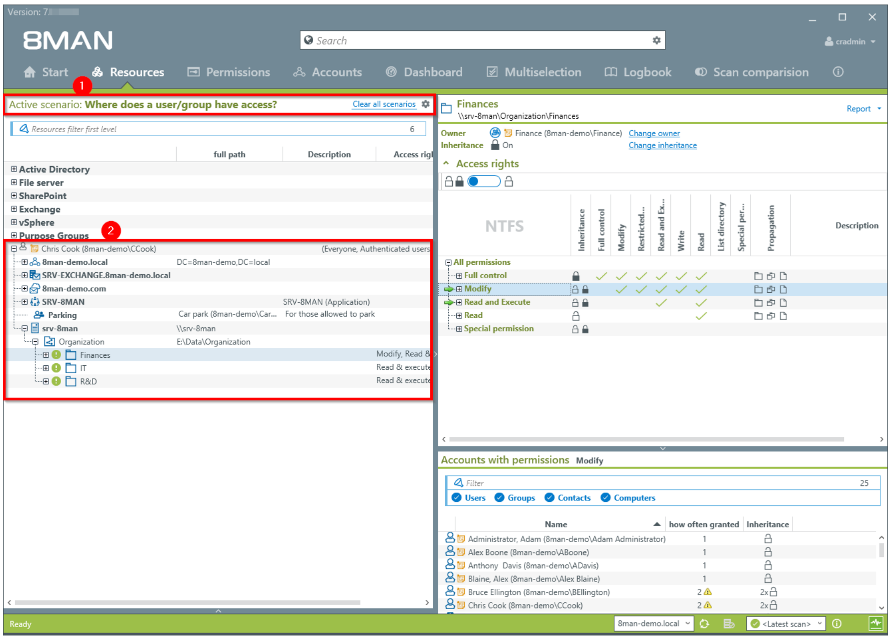
Additional Services

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

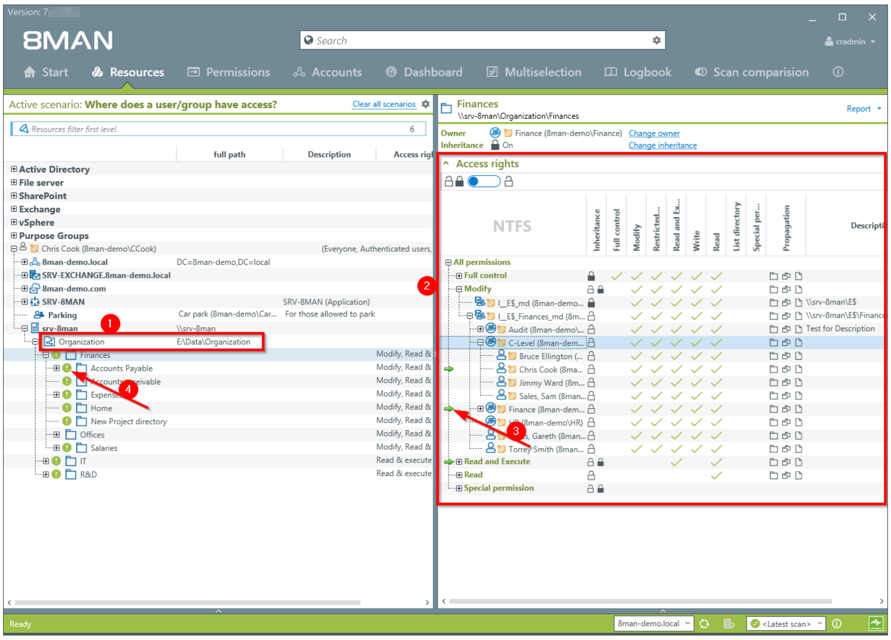
In contrast to the dynamic view in the UI, the report does not show any information related to Active Directory, Exchange, vSphere und Purpose Groups.


Version: 7.
8MAN
1
Start
Resources
Permissions
2
cook
3
Scan comparision
cradmin
Resources
Resources filter first level
full path
Active Directory
File server
SharePoint
Exchange
vSphere
Purpose Groups
Users (2)
Cooke, Amelia (8man-demo\Amelia Cooke) displayname: Cooke, Amelia cn:...
Chris Cook (8man-demo\CCook) displayname: Chris Cook cn: Chri...
Groups (0)
Directories (0)
Mailboxes (2)
Cooke, Amelia Amelia.Cooke@8man-demo.local
Chris Cook CCook@8man-demo.local
vSphere (0)
Public Folders (0)
Mailbox Folders (0)
Active Directory Resources (2)
Cooke, Amelia (Amelia Cooke) cn: Amelia Cooke name: Amelia...
Chris Cook (CCook) cn: Chris Cook name: Chris Cook
Purpose Groups (0)
Ready
8man-demo.local
<Latest scan>

1. *Select "Resources".*
2. *Enter the name of the person whose access rights you want to analyze.*
3. *Select the desired result in the "User" area.*



1. 8MAN activates the scenario "Where does a user/group have access"
2. 8MAN shows all resources that "Chris Cook" can access. In the basic version you can view results for Active Directory and file servers. Depending on which AddOns have been chosen, you can also review access to other resources.



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

4.3 +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

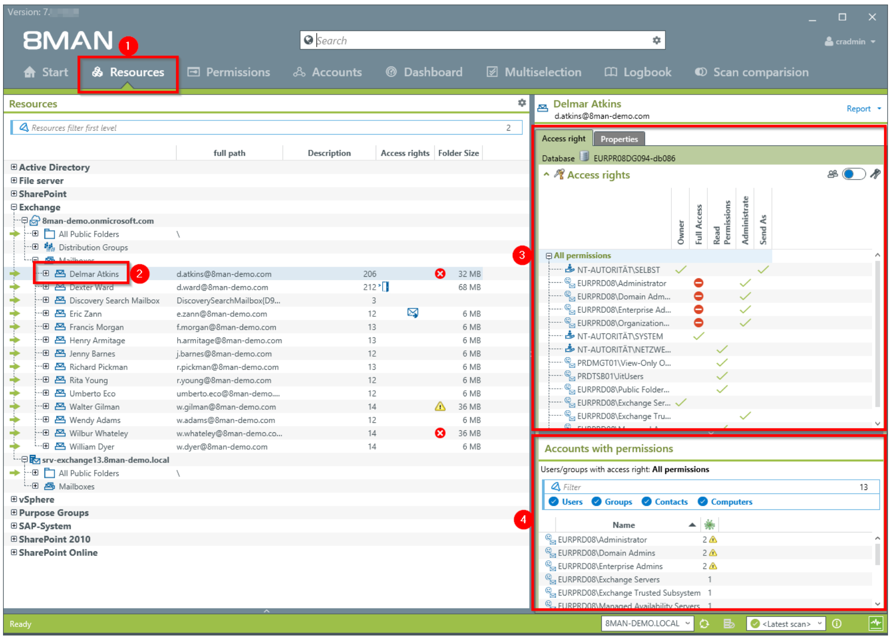
From release 7.5 onward, 8MATE Exchange supports the management of mailing lists.
This way you can easily delegate cumbersome mailing list management tasks to your help desk.

4.3.1.1 Identifying access rights on mailboxes

Background / Purpose

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

Step by step process



Resources

Resources filter first level 2

	full path	Description	Access rights	Folder Size
⊞ Active Directory				
⊞ File server				
⊞ SharePoint				
⊟ Exchange				
⊟ 8man-demo.onmicrosoft.com				
⊞ All Public Folders	\			
⊞ Distribution Groups				
⊟ Mailboxes				
⊞ Delmar Atkins	d.atkins@8man-demo.com		206 ✖	32 MB
⊞ Dexter Ward	d.ward@8man-demo.com		212	68 MB
⊞ Discovery Search Mailbox	DiscoverySearchMailbox{D9...		3	
⊞ Eric Zann	e.zann@8man-demo.com		12	6 MB
⊞ Francis Morgan	f.morgan@8man-demo.com		13	6 MB
⊞ Henry Armitage	h.armitage@8man-demo.com		13	6 MB
⊞ Jenny Barnes	j.barnes@8man-demo.com		12	6 MB
⊞ Richard Pickman	r.pickman@8man-demo.com		13	6 MB
⊞ Rita Young	r.young@8man-demo.com		12	6 MB
⊞ Umberto Eco	umberto.eco@8man-demo....		12	6 MB
⊞ Walter Gilman	w.gilman@8man-demo.com		14 ⚠	36 MB
⊞ Wendy Adams	w.adams@8man-demo.com		12	6 MB
⊞ Wilbur Whateley	w.whateley@8man-demo.co...		14 ✖	36 MB
⊞ William Dyer	w.dyer@8man-demo.com		14	6 MB
⊟ srv-exchange13.8man-demo.local				
⊞ All Public Folders	\			
⊞ Mailboxes				
⊞ vSphere				
⊞ Purpose Groups				
⊞ SAP-System				
⊞ SharePoint 2010				
⊞ SharePoint Online				

Delmar Atkins
d.atkins@8man-demo.com

Database EURPR08DG094-db086

Access rights

	Owner	Full Access	Read Permissions	Administrate	Send As
⊟ All permissions					
NT-AUTORITÄT\SELBST	✓				✓
EURPRD08\Administrator		⛔		✓	
EURPRD08\Domain Adm...		⛔		✓	
EURPRD08\Enterprise Ad...		⛔		✓	
EURPRD08\Organization...		⛔		✓	
NT-AUTORITÄT\SYSTEM		✓			
NT-AUTORITÄT\NETZWE...			✓		
PRDMGT01\View-Only O...			✓		
PRDTSB01\JitUsers			✓		
EURPRD08\Public Folder...			✓		
EURPRD08\Exchange Ser...	✓				
EURPRD08\Exchange Tru...				✓	

Accounts with permissions

Users/groups with access right: **All permissions**

Filter 13

✓ Users ✓ Groups ✓ Contacts ✓ Computers

Name	
EURPRD08\Administrator	2 ⚠
EURPRD08\Domain Admins	2 ⚠
EURPRD08\Enterprise Admins	2 ⚠
EURPRD08\Exchange Servers	1
EURPRD08\Exchange Trusted Subsystem	1
EURPRD08\Managed Availability Servers	1

8MAN-DEMO.LOCAL ✓ <Latest scan>

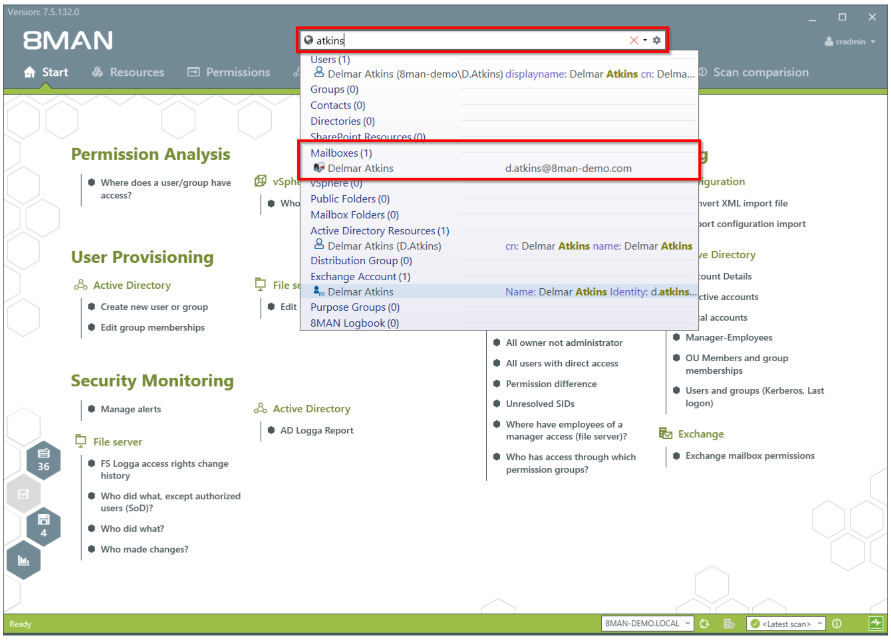
1. *Select "Resources".*
2. *Navigate to the desired mailbox.*
3. *8MAN shows you which users/groups have which rights.*
4. *8MAN shows all accounts with access rights in a flat list.*

4.3.1.2 Identifying mailbox properties

Background / Purpose

8MATE Exchange shows the properties of individual mailboxes.

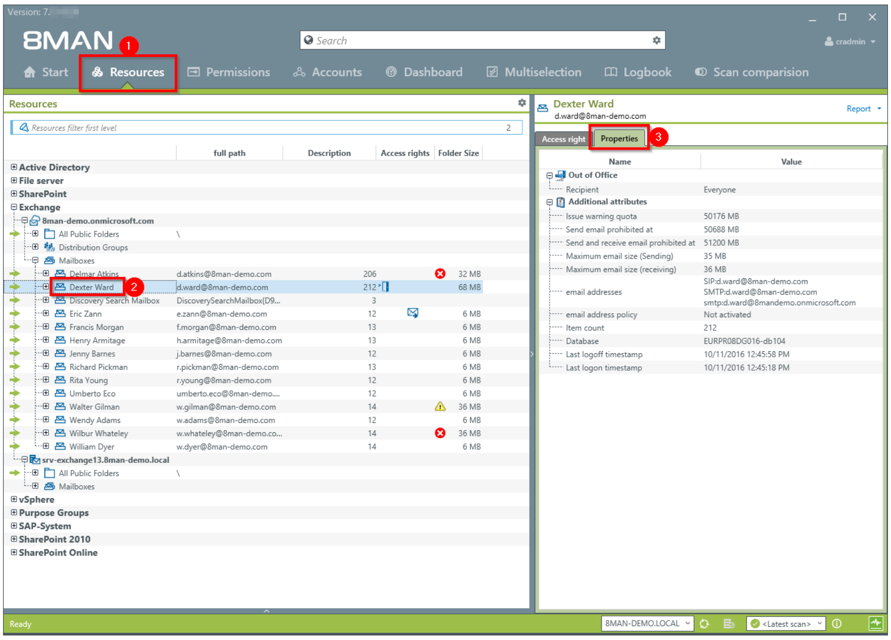
Step by step process



atkins

Users (1)
Delmar Atkins (8man-demo\D.Atkins) displayname: Delmar **Atkins** cn: Delma...
Groups (0)
Contacts (0)
Directories (0)
SharePoint Resources (0)
Mailboxes (1)
Delmar Atkins d.atkins@8man-demo.com
vSphere (0)
Public Folders (0)
Mailbox Folders (0)
Active Directory Resources (1)
Delmar Atkins (D.Atkins) cn: Delmar **Atkins** name: Delmar **Atkins**
Distribution Group (0)
Exchange Account (1)
Delmar Atkins Name: Delmar **Atkins** Identity: d.**atkins**...
Purpose Groups (0)
8MAN Logbook (0)

Use the search field to find the desired mailbox.



	full path	Description	Access rights	Folder Size
Active Directory				
File server				
SharePoint				
Exchange				
8man-demo.onmicrosoft.com				
All Public Folders	\			
Distribution Groups				
Mailboxes				
Delmar Atkins	d.atkins@8man-demo.com	206		32 MB
Dexter Ward	d.ward@8man-demo.com	212		68 MB
Discovery Search Mailbox	DiscoverySearchMailbox{D9...	3		
Eric Zann	e.zann@8man-demo.com	12		6 MB
Francis Morgan	f.morgan@8man-demo.com	13		6 MB
Henry Armitage	h.armitage@8man-demo.com	13		6 MB
Jenny Barnes	j.barnes@8man-demo.com	12		6 MB
Richard Pickman	r.pickman@8man-demo.com	13		6 MB
Rita Young	r.young@8man-demo.com	12		6 MB
Umberto Eco	umberto.eco@8man-demo....	12		6 MB
Walter Gilman	w.gilman@8man-demo.com	14		36 MB
Wendy Adams	w.adams@8man-demo.com	12		6 MB
Wilbur Whateley	w.whateley@8man-demo.co...	14		36 MB
William Dyer	w.dyer@8man-demo.com	14		6 MB
srv-exchange13.8man-demo.local				
All Public Folders	\			
Mailboxes				
vSphere				
Purpose Groups				
SAP-System				
SharePoint 2010				
SharePoint Online				

Dexter Ward
d.ward@8man-demo.com

Name	Value
Out of Office	
Recipient	Everyone
Additional attributes	
Issue warning quota	50176 MB
Send email prohibited at	50688 MB
Send and receive email prohibited at	51200 MB
Maximum email size (Sending)	35 MB
Maximum email size (receiving)	36 MB
email addresses	SIP:d.ward@8man-demo.com SMTP:d.ward@8man-demo.com smtp:d.ward@8mandemo.onmicrosoft.com
email address policy	Not activated
Item count	212
Database	EURPR08DG016-db104
Last logoff timestamp	10/11/2016 12:45:58 PM
Last logon timestamp	10/11/2016 12:45:18 PM

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 Identifying access rights on public folders

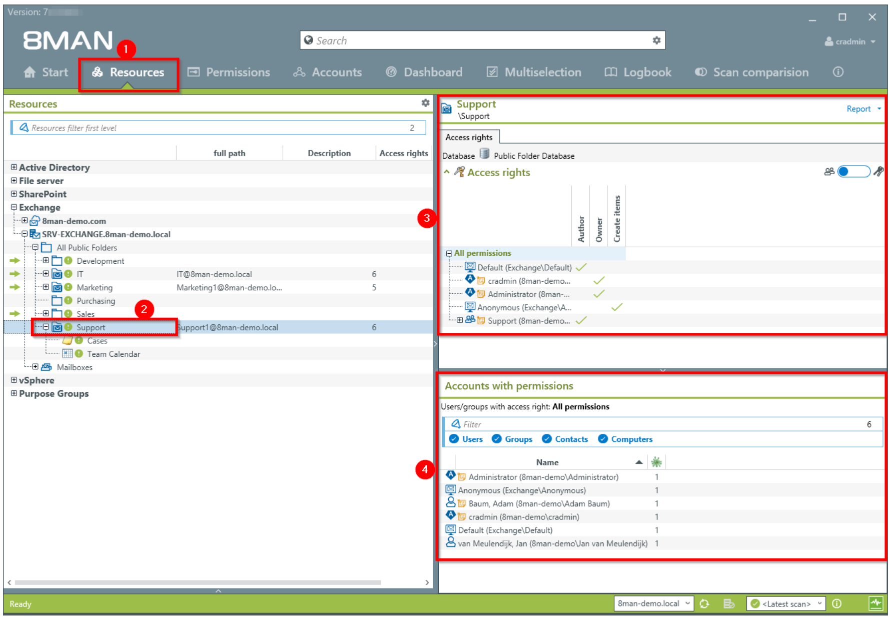
Background / Value

Keeping an overview of access rights to public folders can be extremely challenging with native tools. 8MAN shows you the access rights situation to public folders in the resource view.
Additional Services Report: Who has access to what? Report: Identify Mailbox access rights. Creating a Mailbox, change access rights to email accounts, change out-of office notice, change Mailbox size
Die Berechtigungen auf öffentliche Ordner im Blick zu behalten ist mit Bordmitteln komplex. Mit 8MAN sehen Sie in der Ressourcen-Ansicht die Rechtesituation auf öffentliche Ordner.

Additional services

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

Step by step process



Accounts with permissions

Users/groups with access right: **All permissions**

Name	
Administrator (8man-demo\Administrator)	1
Anonymous (Exchange\Anonymous)	1
Baum, Adam (8man-demo\Adam Baum)	1
cradmin (8man-demo\cradmin)	1
Default (Exchange\Default)	1
van Meulendijk, Jan (8man-demo\Jan van Meulendijk)	1

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.*

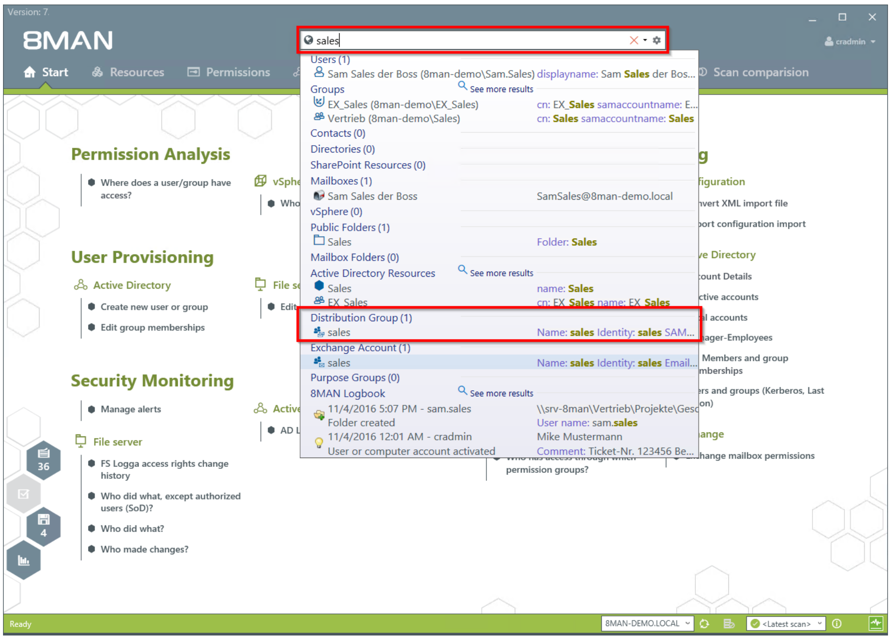
4.3.1.4 Identifying permissions on distribution groups

Background / Value

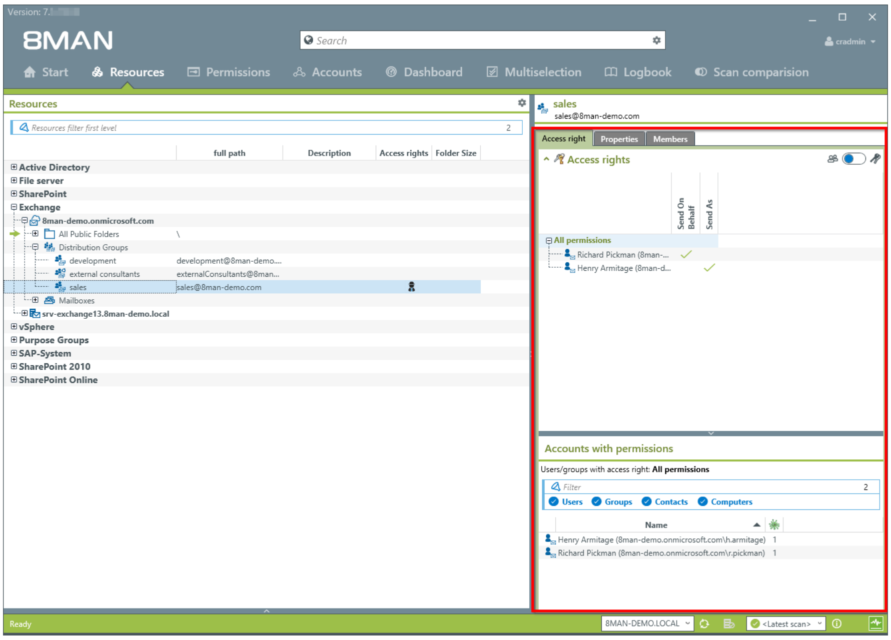
With 8MAN you can quickly check who is allowed to to send Emails from which distribution list. The relevant cases are "send as" and "send on behalf of". The former is the most critical, since it is not easy to identify who actually sent the Email. In the scenario for "send on behalf" the PA or deputy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

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

Step by step process


Version: 7
8MAN
sales
cradmin
Start
Resources
Permissions
Scan comparision
Users (1)
Sam Sales der Boss (8man-demo\Sam.Sales) displayname: Sam Sales der Bos...
Groups
See more results
EX_Sales (8man-demo\EX_Sales) cn: EX_Sales samaccountname: E...
Vertrieb (8man-demo\Sales) cn: Sales samaccountname: Sales
Contacts (0)
Directories (0)
SharePoint Resources (0)
Mailboxes (1)
Sam Sales der Boss SamSales@8man-demo.local
vSphere (0)
Public Folders (1)
Sales Folder: Sales
Mailbox Folders (0)
Active Directory Resources
See more results
Sales name: Sales
EX_Sales cn: EX_Sales name: EX_Sales
Distribution Group (1)
sales Name: sales Identity: sales SAM...
Exchange Account (1)
sales Name: sales Identity: sales Email...
Purpose Groups (0)
8MAN Logbook
See more results
11/4/2016 5:07 PM - sam.sales \\srv-8man\Vertrieb\Projekte\Gesc
Folder created User name: sam.sales
11/4/2016 12:01 AM - cradmin Mike Mustermann
User or computer account activated Comment: Ticket-Nr. 123456 Be...
Permission Analysis
Where does a user/group have access?
User Provisioning
Active Directory
Create new user or group
Edit group memberships
Security Monitoring
Manage alerts
File server
FS Logga access rights change history
Who did what, except authorized users (SoD)?
Who did what?
Who made changes?
36
4
Ready
8MAN-DEMO.LOCAL
<Latest scan>

Use the search field to find the desired Distribution group.



	full path	Description	Access rights	Folder Size
⊞ Active Directory				
⊞ File server				
⊞ SharePoint				
⊟ Exchange				
⊟ 8man-demo.onmicrosoft.com				
⊞ All Public Folders	\			
⊟ Distribution Groups				
development	development@8man-demo....			
external consultants	externalConsultants@8man...			
sales	sales@8man-demo.com			
⊞ Mailboxes				
⊞ srv-exchange13.8man-demo.local				
⊞ vSphere				
⊞ Purpose Groups				
⊞ SAP-System				
⊞ SharePoint 2010				
⊞ SharePoint Online				

sales
sales@8man-demo.com

	Send On Behalf	Send As
⊟ All permissions		
Richard Pickman (8man-...	✓	
Henry Armitage (8man-d...		✓

Accounts with permissions

Users/groups with access right: **All permissions**

Filter 2

✓ Users ✓ Groups ✓ Contacts ✓ Computers

Name	
Henry Armitage (8man-demo.onmicrosoft.com\h.armitage)	1
Richard Pickman (8man-demo.onmicrosoft.com\r.pickman)	1

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

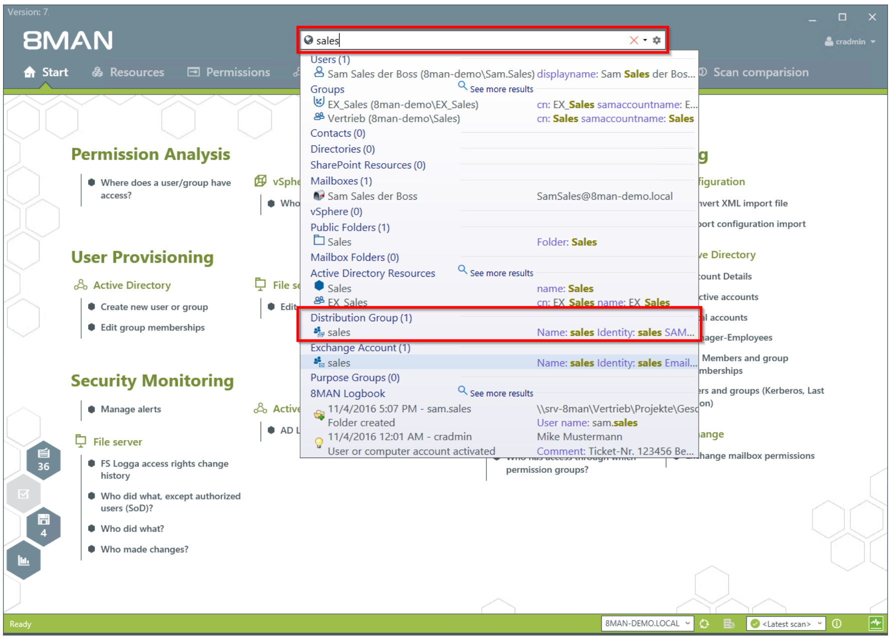
4.3.1.5 Identifying members of distribution groups

Background / Purpose

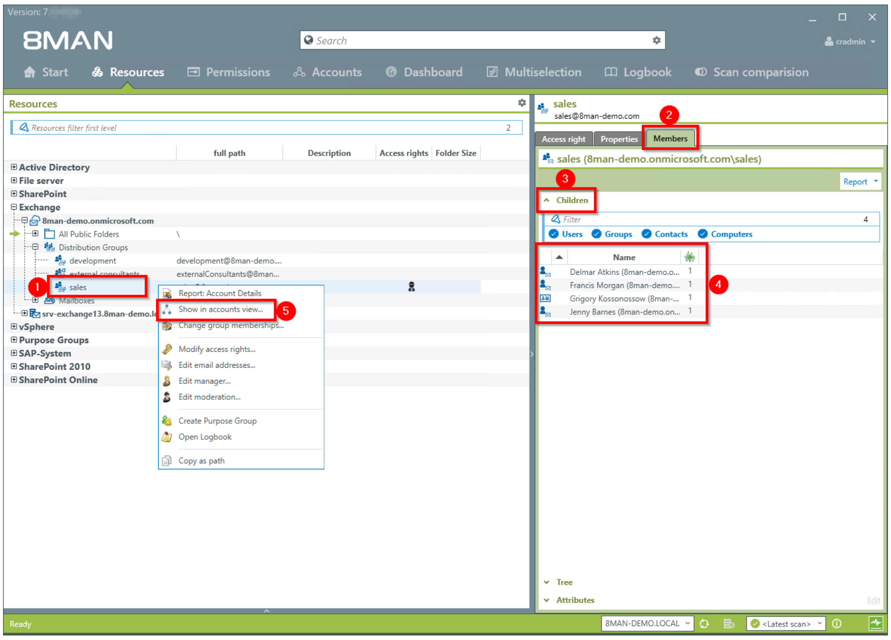
8MAN allows you to display all members and / or recipients of distribution lists. In typical 8MAN fashion this also includes nested group memberships.

This is also possible for dynamic Exchange groups.

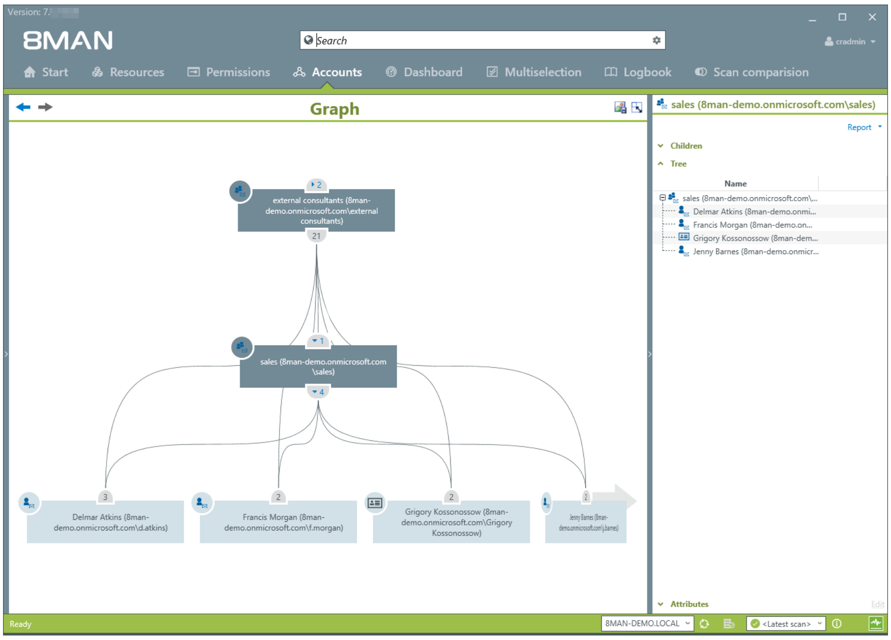
Step by step process


8MAN
Start
Resources
Permissions
Scan comparision
sales
Users (1)
Sam Sales der Boss (8man-demo\Sam.Sales) displayname: Sam Sales der Bos...
Groups
See more results
EX_Sales (8man-demo\EX_Sales) cn: EX_Sales samaccountname: E...
Vertrieb (8man-demo\Sales) cn: Sales samaccountname: Sales
Contacts (0)
Directories (0)
SharePoint Resources (0)
Mailboxes (1)
Sam Sales der Boss SamSales@8man-demo.local
vSphere (0)
Public Folders (1)
Sales Folder: Sales
Mailbox Folders (0)
Active Directory Resources
Sales name: Sales
EX_Sales cn: EX_Sales name: EX_Sales
Distribution Group (1)
sales Name: sales Identity: sales SAM...
Exchange Account (1)
sales Name: sales Identity: sales Email...
Purpose Groups (0)
8MAN Logbook
11/4/2016 5:07 PM - sam.sales \\srv-8man\Vertrieb\Projekte\Gesc
Folder created User name: sam.sales
11/4/2016 12:01 AM - cradmin Mike Mustermann
User or computer account activated Comment: Ticket-Nr. 123456 Be...
Permission Analysis
User Provisioning
Security Monitoring
Ready
8MAN-DEMO.LOCAL

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.*


Version: 7.[redacted]
8MAN
Search
cradmin
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
Graph
2
external consultants (8man-demo.onmicrosoft.com\external consultants)
21
1
sales (8man-demo.onmicrosoft.com\sales)
4
3
Delmar Atkins (8man-demo.onmicrosoft.com\d.atkins)
2
Francis Morgan (8man-demo.onmicrosoft.com\f.morgan)
2
Grigory Kossonossow (8man-demo.onmicrosoft.com\Grigory Kossonossow)
2
Jenny Barnes (8man-demo.onmicrosoft.com\j.barnes)
sales (8man-demo.onmicrosoft.com\sales)
Report
Children
Tree
Attributes
Edit
Ready
8MAN-DEMO.LOCAL
<Latest scan>

Name
sales (8man-demo.onmicrosoft.com\...
Delmar Atkins (8man-demo.onmi...
Francis Morgan (8man-demo.on...
Grigory Kossonossow (8man-dem...
Jenny Barnes (8man-demo.onmicr...

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 Identifying 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

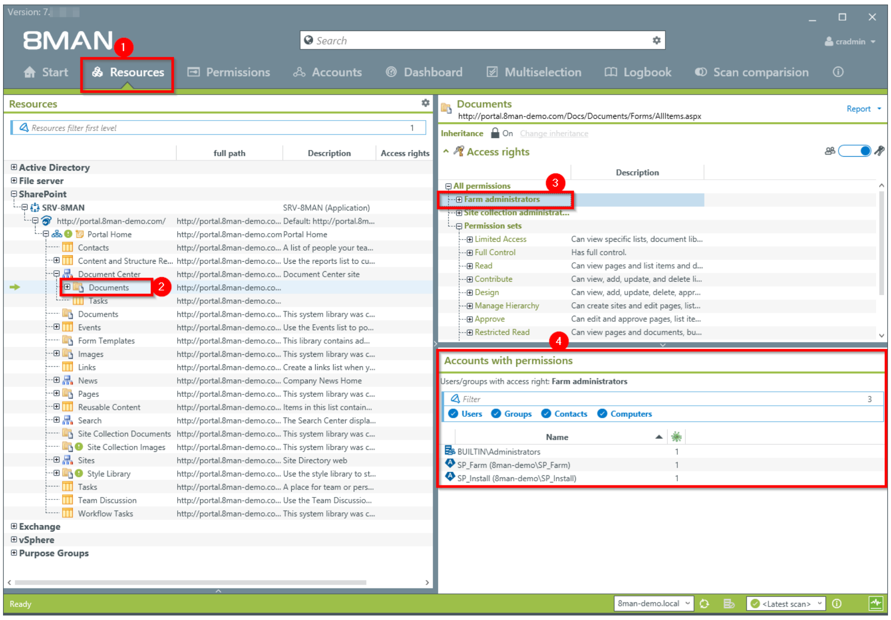
Report: Who has access to what?

Report: What do users/groups have access to?

Changing access rights to SharePoint resources

Setting the naming convention for AD Groups

Step by step process



Resources

Resources filter first level 1

	full path	Description	Access rights
Active Directory			
File server			
SharePoint			
SRV-8MAN		SRV-8MAN (Application)	
http://portal.8man-demo.com/	http://portal.8man-demo.co...	Default: http://portal.8m...	
Portal Home	http://portal.8man-demo.com	Portal Home	
Contacts	http://portal.8man-demo.co...	A list of people your tea...	
Content and Structure Re...	http://portal.8man-demo.co...	Use the reports list to cu...	
Document Center	http://portal.8man-demo.co...	Document Center site	
Documents	http://portal.8man-demo.co...		
Tasks	http://portal.8man-demo.co...		
Documents	http://portal.8man-demo.co...	This system library was c...	
Events	http://portal.8man-demo.co...	Use the Events list to po...	
Form Templates	http://portal.8man-demo.co...	This library contains ad...	
Images	http://portal.8man-demo.co...	This system library was c...	
Links	http://portal.8man-demo.co...	Create a links list when y...	
News	http://portal.8man-demo.co...	Company News Home	
Pages	http://portal.8man-demo.co...	This system library was c...	
Reusable Content	http://portal.8man-demo.co...	Items in this list contain...	
Search	http://portal.8man-demo.co...	The Search Center displa...	
Site Collection Documents	http://portal.8man-demo.co...	This system library was c...	
Site Collection Images	http://portal.8man-demo.co...	This system library was c...	
Sites	http://portal.8man-demo.co...	Site Directory web	
Style Library	http://portal.8man-demo.co...	Use the style library to st...	
Tasks	http://portal.8man-demo.co...	A place for team or pers...	
Team Discussion	http://portal.8man-demo.co...	Use the Team Discussio...	
Workflow Tasks	http://portal.8man-demo.co...	This system library was c...	
Exchange			
vSphere			
Purpose Groups			

Documents
http://portal.8man-demo.com/Docs/Documents/Forms/AllItems.aspx

Report

Inheritance On Change inheritance

Access rights

	Description
All permissions	
Farm administrators	
Site collection administrat...	
Permission sets	
Limited Access	Can view specific lists, document lib...
Full Control	Has full control.
Read	Can view pages and list items and d...
Contribute	Can view, add, update, and delete li...
Design	Can view, add, update, delete, appr...
Manage Hierarchy	Can create sites and edit pages, list...
Approve	Can edit and approve pages, list ite...
Restricted Read	Can view pages and documents, bu...

Accounts with permissions

Users/groups with access right: **Farm administrators**

Filter 3

✓ Users ✓ Groups ✓ Contacts ✓ Computers

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

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

4.4.2 Services for Administrators

4.4.2.1 Identifying divergent access rights in the tree structure

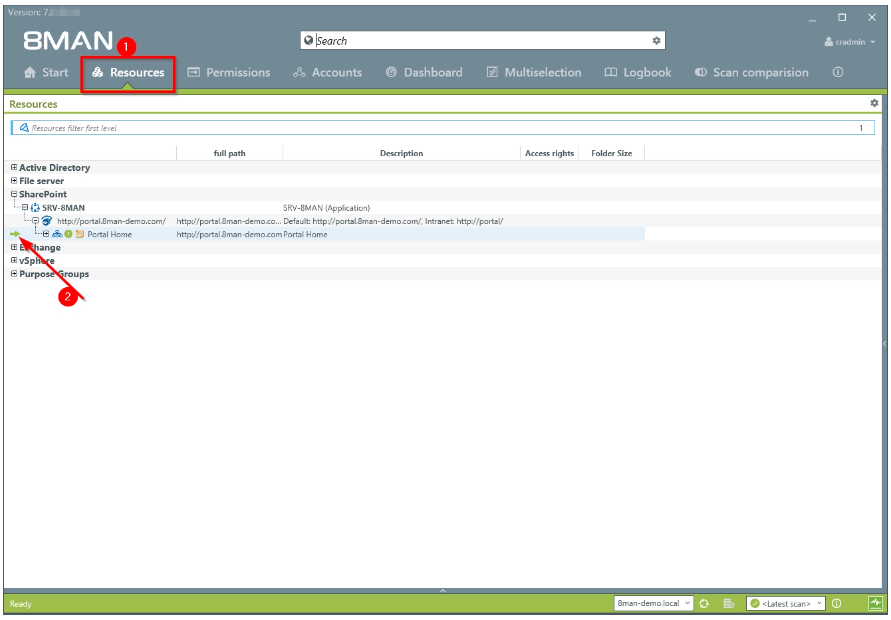
Background / Value

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

Additional Services

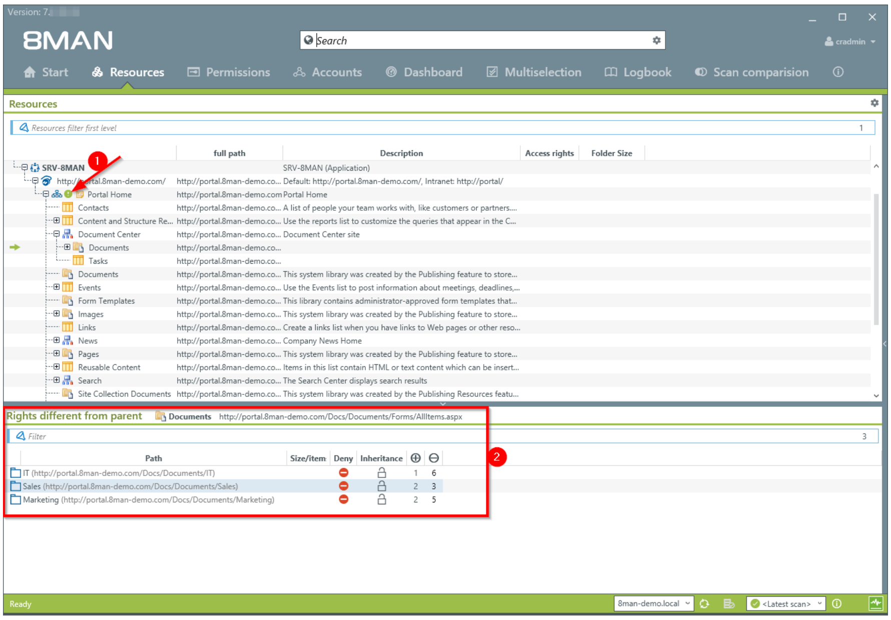
Report: Who has access to what?
Report: What do users/groups have access to?
Changing acsess rights to SharePoint resources
Setting the naming convention for AD Groups

Step by step process



	full path	Description	Access rights	Folder Size
⊞ Active Directory				
⊞ File server				
⊟ SharePoint				
⊟ SRV-8MAN		SRV-8MAN (Application)		
⊟ http://portal.8man-demo.com/	http://portal.8man-demo.co...	Default: http://portal.8man-demo.com/, Intranet: http://portal/		
⊞ Portal Home	http://portal.8man-demo.com	Portal Home		
⊞ Exchange				
⊞ vSphere				
⊞ Purpose Groups				

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



Resources

Resources filter first level 1

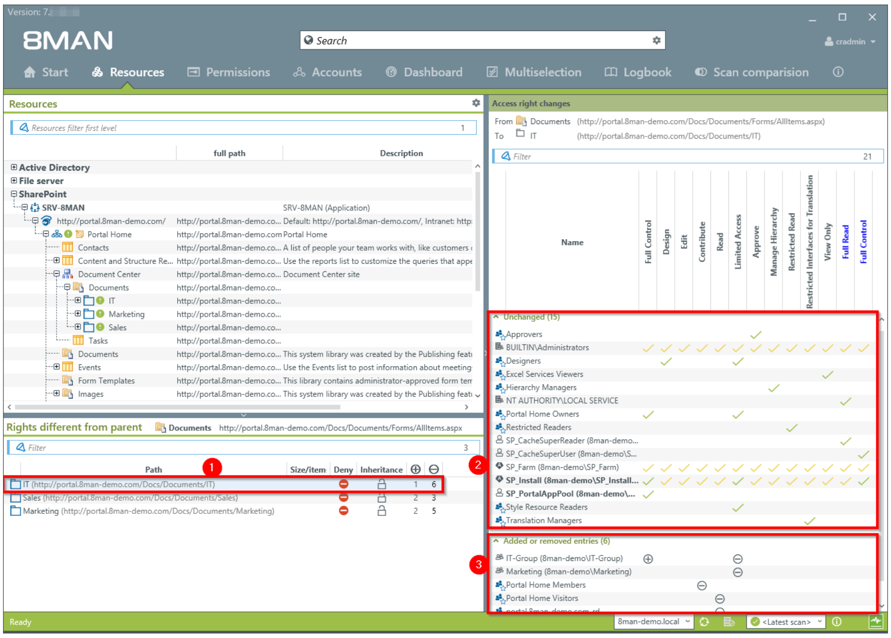
	full path	Description	Access rights	Folder Size
SRV-8MAN		SRV-8MAN (Application)		
http://portal.8man-demo.com/	http://portal.8man-demo.co...	Default: http://portal.8man-demo.com/, Intranet: http://portal/		
Portal Home	http://portal.8man-demo.com	Portal Home		
Contacts	http://portal.8man-demo.co...	A list of people your team works with, like customers or partners....		
Content and Structure Re...	http://portal.8man-demo.co...	Use the reports list to customize the queries that appear in the C...		
Document Center	http://portal.8man-demo.co...	Document Center site		
Documents	http://portal.8man-demo.co...			
Tasks	http://portal.8man-demo.co...			
Documents	http://portal.8man-demo.co...	This system library was created by the Publishing feature to store...		
Events	http://portal.8man-demo.co...	Use the Events list to post information about meetings, deadlines,...		
Form Templates	http://portal.8man-demo.co...	This library contains administrator-approved form templates that...		
Images	http://portal.8man-demo.co...	This system library was created by the Publishing feature to store...		
Links	http://portal.8man-demo.co...	Create a links list when you have links to Web pages or other reso...		
News	http://portal.8man-demo.co...	Company News Home		
Pages	http://portal.8man-demo.co...	This system library was created by the Publishing feature to store...		
Reusable Content	http://portal.8man-demo.co...	Items in this list contain HTML or text content which can be insert...		
Search	http://portal.8man-demo.co...	The Search Center displays search results		
Site Collection Documents	http://portal.8man-demo.co...	This system library was created by the Publishing Resources featu...		

Rights different from parent Documents http://portal.8man-demo.com/Docs/Documents/Forms/AllItems.aspx

Filter 3

Path	Size/item	Deny	Inheritance	⊕	⊖
IT (http://portal.8man-demo.com/Docs/Documents/IT)		⛔	🔓	1	6
Sales (http://portal.8man-demo.com/Docs/Documents/Sales)		⛔	🔓	2	3
Marketing (http://portal.8man-demo.com/Docs/Documents/Marketing)		⛔	🔓	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.*



Resources

Resources filter first level 1

	full path	Description
Active Directory		
File server		
SharePoint		
SRV-8MAN		SRV-8MAN (Application)
http://portal.8man-demo.com/	http://portal.8man-demo.co...	Default: http://portal.8man-demo.com/, Intranet: http:
Portal Home	http://portal.8man-demo.com	Portal Home
Contacts	http://portal.8man-demo.co...	A list of people your team works with, like customers
Content and Structure Re...	http://portal.8man-demo.co...	Use the reports list to customize the queries that appe
Document Center	http://portal.8man-demo.co...	Document Center site
Documents	http://portal.8man-demo.co...	
IT	http://portal.8man-demo.co...	
Marketing	http://portal.8man-demo.co...	
Sales	http://portal.8man-demo.co...	
Tasks	http://portal.8man-demo.co...	
Documents	http://portal.8man-demo.co...	This system library was created by the Publishing featu
Events	http://portal.8man-demo.co...	Use the Events list to post information about meeting
Form Templates	http://portal.8man-demo.co...	This library contains administrator-approved form tem
Images	http://portal.8man-demo.co...	This system library was created by the Publishing featu

Rights different from parent Documents http://portal.8man-demo.com/Docs/Documents/Forms/AllItems.aspx

Filter 3

Path	Size/item	Deny	Inheritance	⊕	⊖
IT (http://portal.8man-demo.com/Docs/Documents/IT)		⛔	🔓	1	6
Sales (http://portal.8man-demo.com/Docs/Documents/Sales)		⛔	🔓	2	3
Marketing (http://portal.8man-demo.com/Docs/Documents/Marketing)		⛔	🔓	2	5

Access right changes

From Documents (http://portal.8man-demo.com/Docs/Documents/Forms/AllItems.aspx)
To IT (http://portal.8man-demo.com/Docs/Documents/IT)

Filter 21

Name	Full Control	Design	Edit	Contribute	Read	Limited Access	Approve	Manage Hierarchy	Restricted Read	Restricted Interfaces for Translation	View Only	Full Read	Full Control
Unchanged (15)													
Approvers							✓						
BUILTIN\Administrators	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Designers		✓				✓							
Excel Services Viewers											✓		
Hierarchy Managers								✓					
NT AUTHORITY\LOCAL SERVICE												✓	
Portal Home Owners	✓					✓							
Restricted Readers									✓				
SP_CacheSuperReader (8man-demo...												✓	
SP_CacheSuperUser (8man-demo\S...													✓
SP_Farm (8man-demo\SP_Farm)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SP_Install (8man-demo\SP_Install...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SP_PortalAppPool (8man-demo\...	✓												
Style Resource Readers						✓							
Translation Managers										✓			
Added or removed entries (6)													
IT-Group (8man-demo\IT-Group)	⊕					⊖							
Marketing (8man-demo\Marketing)						⊖							
Portal Home Members				⊖									
Portal Home Visitors					⊖								
portal.8man-demo.com-rd					⊖								

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: Analyze & Act

4.5.1 Identifying recursive groups using the 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.

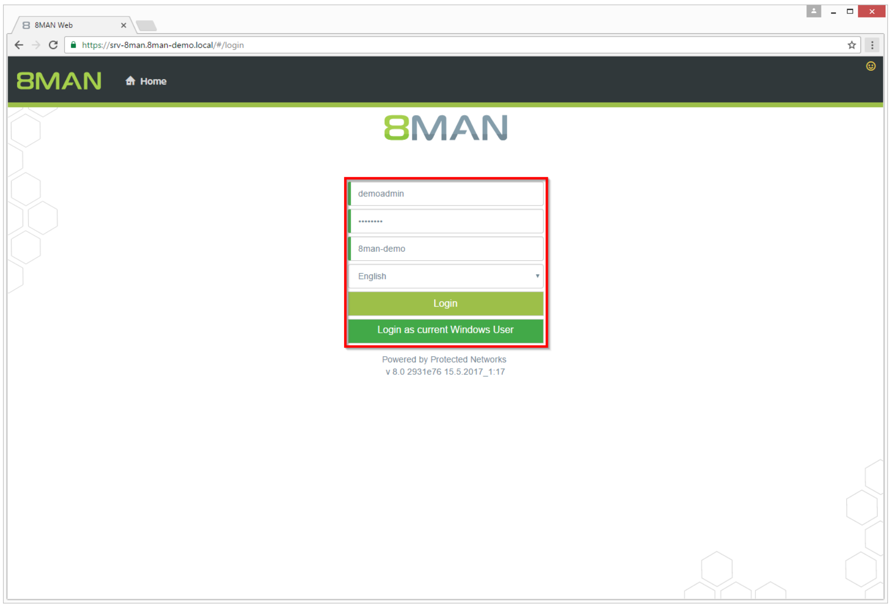
Additional Services

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

Idenitfying recursive groups (using the rich client)

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

Step by step process



https://srv-8man.8man-demo.local/#/login

demoadmin

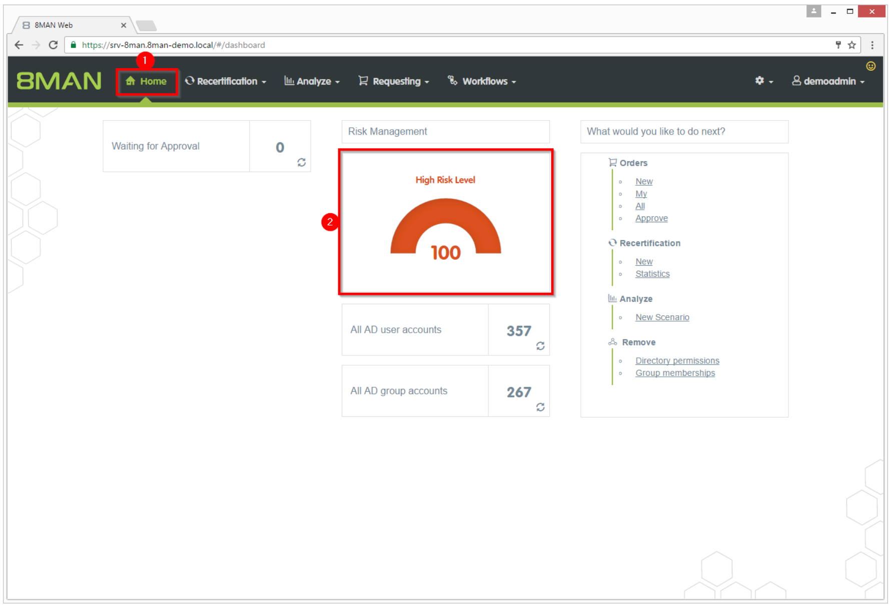
•••••••••

8man-demo

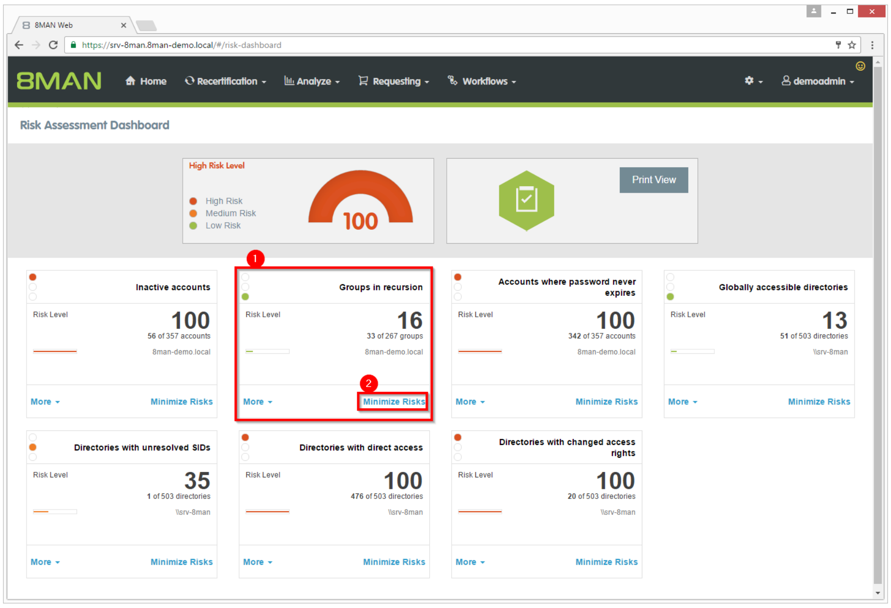
English

Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

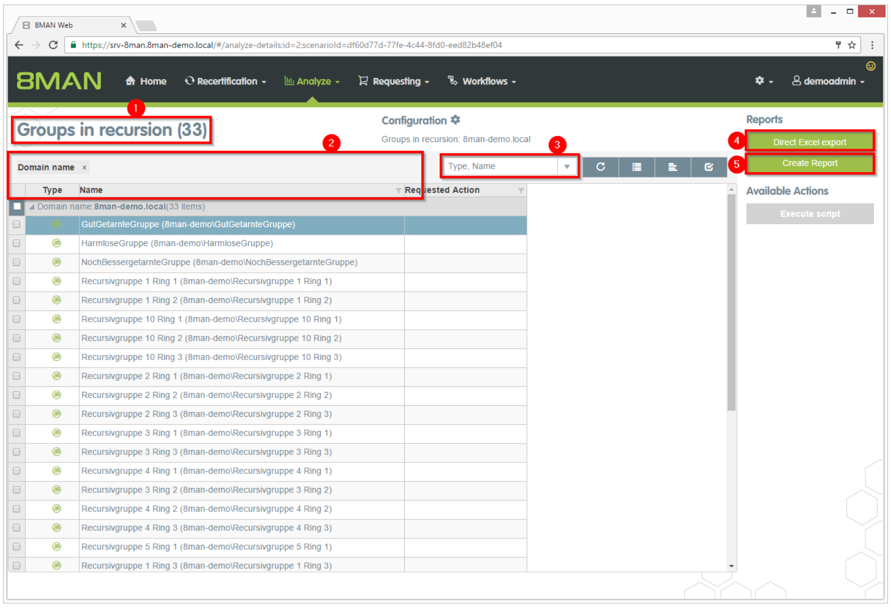
Login to the web client.



1. *After login you see the web client homepage.*
2. *8MAN shows an overall rating in the area "Risk Management".*
   The higher the number the higher the risk level.
   Click the tile.



1. *8MAN shows a rating for the risk factor "Groups in recursion".*
2. *Click "Minimize risks".*



Groups in recursion (33)

Groups in recursion: 8man-demo.local

	Type	Name	Requested Action
■	Domain name:**8man-demo.local**(33 items)		
□		GutGetarnteGruppe (8man-demo\GutGetarnteGruppe)	
□		HarmloseGruppe (8man-demo\HarmloseGruppe)	
□		NochBessergetarnteGruppe (8man-demo\NochBessergetarnteGruppe)	
□		Recursivgruppe 1 Ring 1 (8man-demo\Recursivgruppe 1 Ring 1)	
□		Recursivgruppe 1 Ring 2 (8man-demo\Recursivgruppe 1 Ring 2)	
□		Recursivgruppe 10 Ring 1 (8man-demo\Recursivgruppe 10 Ring 1)	
□		Recursivgruppe 10 Ring 2 (8man-demo\Recursivgruppe 10 Ring 2)	
□		Recursivgruppe 10 Ring 3 (8man-demo\Recursivgruppe 10 Ring 3)	
□		Recursivgruppe 2 Ring 1 (8man-demo\Recursivgruppe 2 Ring 1)	
□		Recursivgruppe 2 Ring 2 (8man-demo\Recursivgruppe 2 Ring 2)	
□		Recursivgruppe 2 Ring 3 (8man-demo\Recursivgruppe 2 Ring 3)	
□		Recursivgruppe 3 Ring 1 (8man-demo\Recursivgruppe 3 Ring 1)	
□		Recursivgruppe 3 Ring 3 (8man-demo\Recursivgruppe 3 Ring 3)	
□		Recursivgruppe 4 Ring 1 (8man-demo\Recursivgruppe 4 Ring 1)	
□		Recursivgruppe 3 Ring 2 (8man-demo\Recursivgruppe 3 Ring 2)	
□		Recursivgruppe 4 Ring 2 (8man-demo\Recursivgruppe 4 Ring 2)	
□		Recursivgruppe 4 Ring 3 (8man-demo\Recursivgruppe 4 Ring 3)	
□		Recursivgruppe 5 Ring 1 (8man-demo\Recursivgruppe 5 Ring 1)	
□		Recursivgruppe 1 Ring 3 (8man-demo\Recursivgruppe 1 Ring 3)	

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- oder CSV-format. Save the report or e-mail it.*

4.5.2 Identifying users with never expiring passwords using the web client

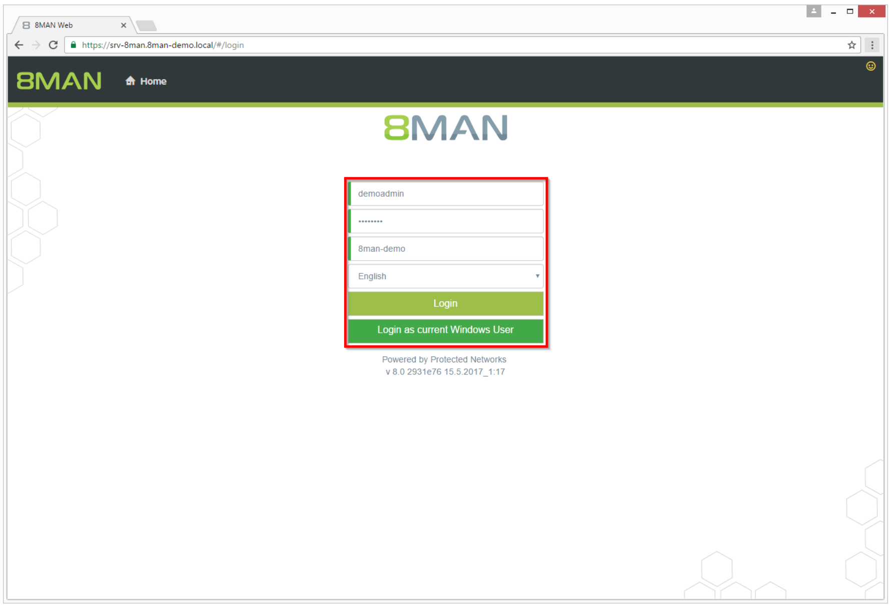
Background / Value

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

Resetting passwords (using the rich client)
Changing password options (using the rich client)

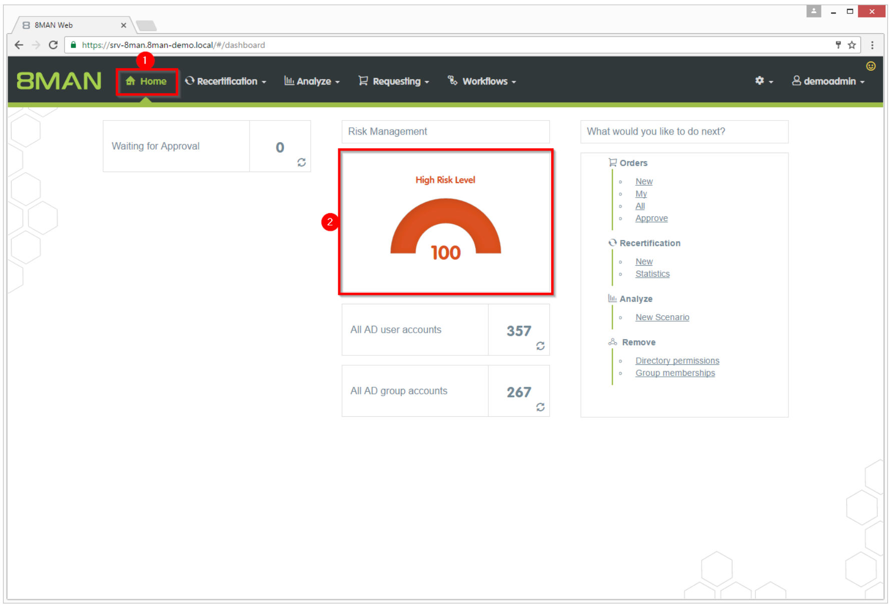
Step by step process


8MAN Web
https://srv-8man.8man-demo.local/#/login
8MAN
Home
8MAN
Login
Login as current Windows User

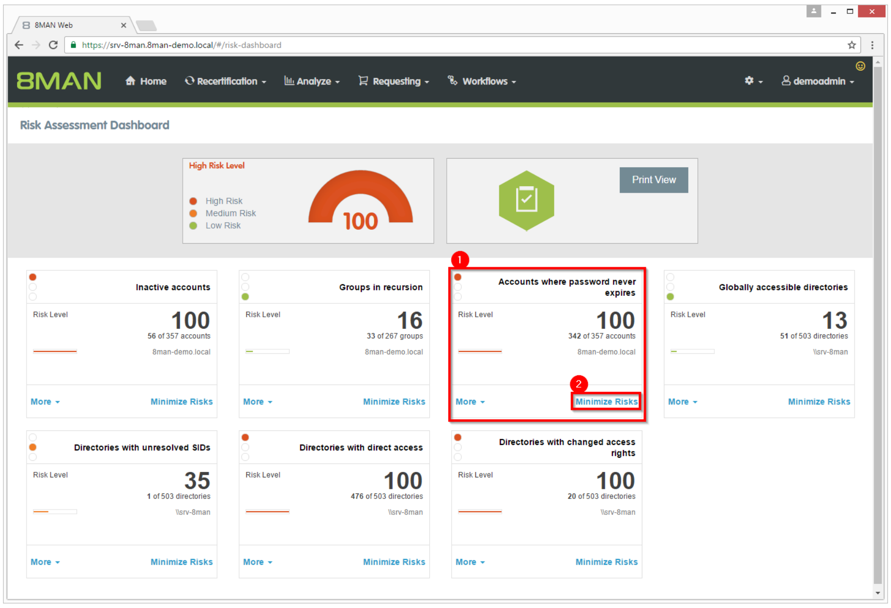
demoadmin
•••••••••
8man-demo
English

Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

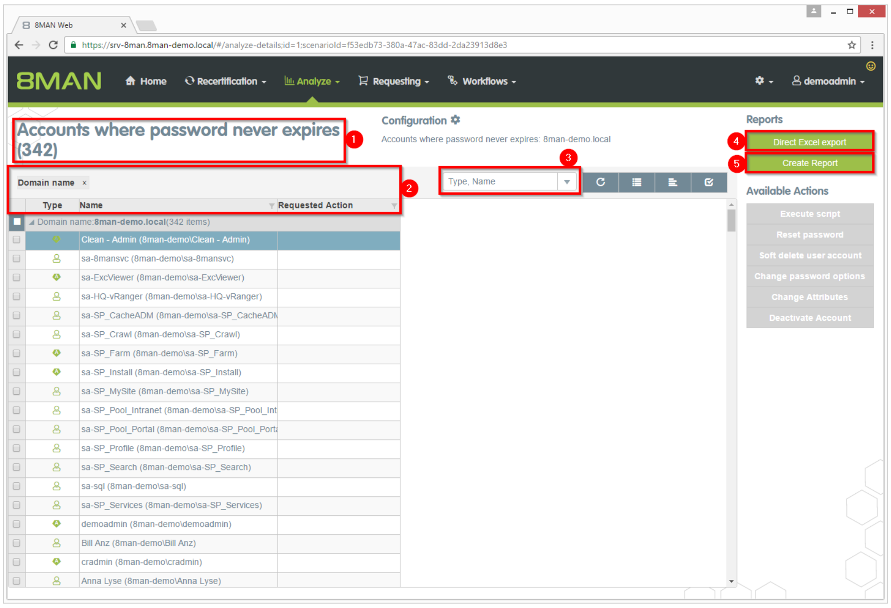
Login to the web client.



1. *After login you see the web client homepage.*
2. *8MAN shows an overall rating in the area "Risk Management".*
   The higher the number the higher the risk level.
   Click on the tile.



1. *8MAN shows a rating for the risk factor "Accounts where password never expires".*
2. *Click on "Minimize risks".*



Accounts where password never expires (342)

Accounts where password never expires: 8man-demo.local

Domain name ×

Type, Name

Domain name:**8man-demo.local**(342 items)

Type	Name	Requested Action
	Clean - Admin (8man-demo\Clean - Admin)	
	sa-8mansvc (8man-demo\sa-8mansvc)	
	sa-ExcViewer (8man-demo\sa-ExcViewer)	
	sa-HQ-vRanger (8man-demo\sa-HQ-vRanger)	
	sa-SP_CacheADM (8man-demo\sa-SP_CacheADM	
	sa-SP_Crawl (8man-demo\sa-SP_Crawl)	
	sa-SP_Farm (8man-demo\sa-SP_Farm)	
	sa-SP_Install (8man-demo\sa-SP_Install)	
	sa-SP_MySite (8man-demo\sa-SP_MySite)	
	sa-SP_Pool_Intranet (8man-demo\sa-SP_Pool_Int	
	sa-SP_Pool_Portal (8man-demo\sa-SP_Pool_Porta	
	sa-SP_Profile (8man-demo\sa-SP_Profile)	
	sa-SP_Search (8man-demo\sa-SP_Search)	
	sa-sql (8man-demo\sa-sql)	
	sa-SP_Services (8man-demo\sa-SP_Services)	
	demoadmin (8man-demo\demoadmin)	
	Bill Anz (8man-demo\Bill Anz)	
	cradmin (8man-demo\cradmin)	
	Anna Lyse (8man-demo\Anna Lyse)	

1. *8MAN lists all accounts where password never expires.*
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- oder CSV-format. Save the report or e-mail it.*

4.5.3 Identifying globally accessible directories using the 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.

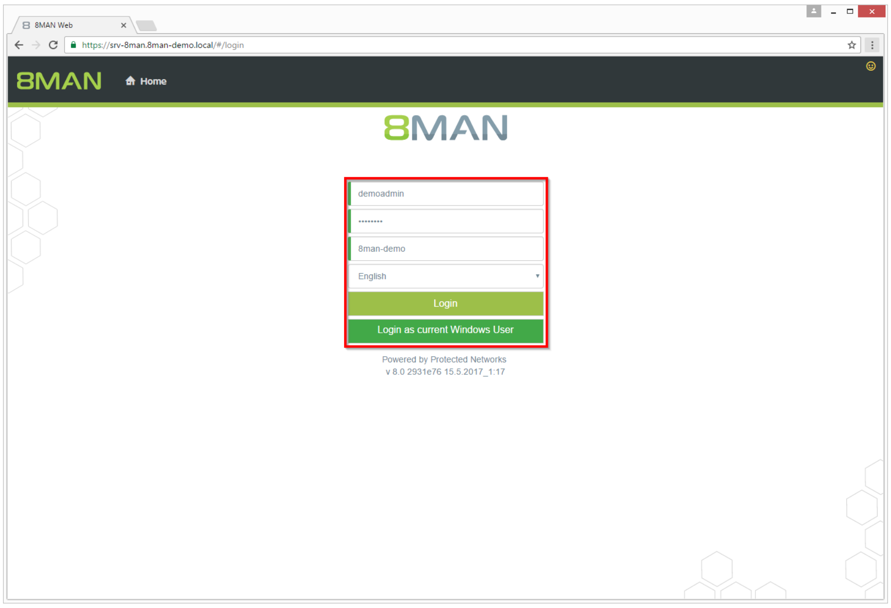
"Everyone accounts" are:

- Everyone
- Authenticated Users
- Domain-Users

Additional Services

Removing permissions from globally accessible directories in bulk

Step by step process


8MAN Web
https://srv-8man.8man-demo.local/#/login
8MAN
Home
8MAN
Login
Login as current Windows User

demoadmin

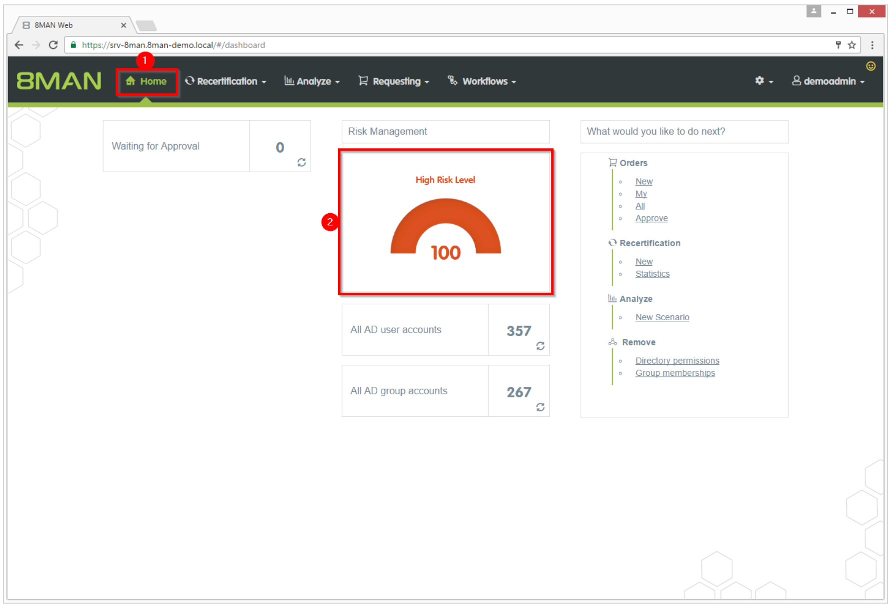
••••••••

8man-demo

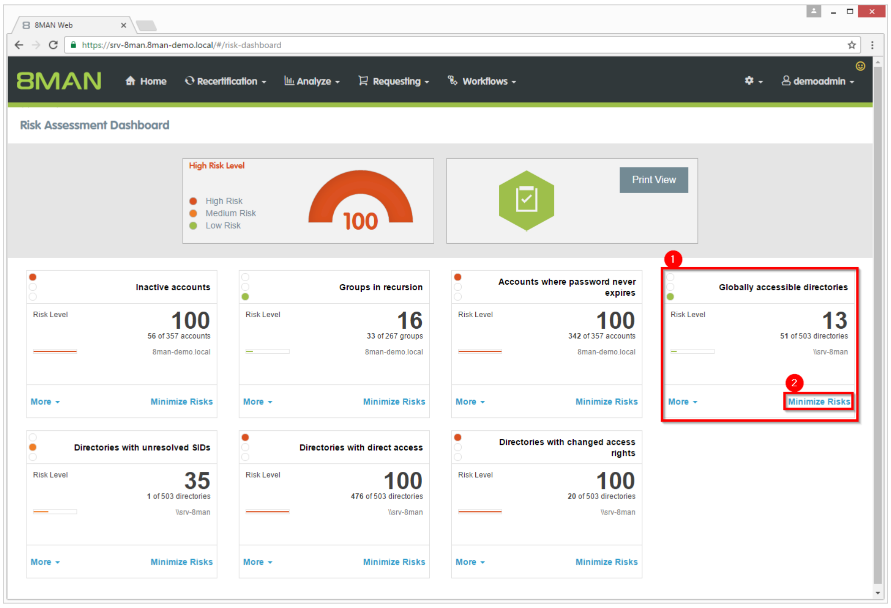
English

Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

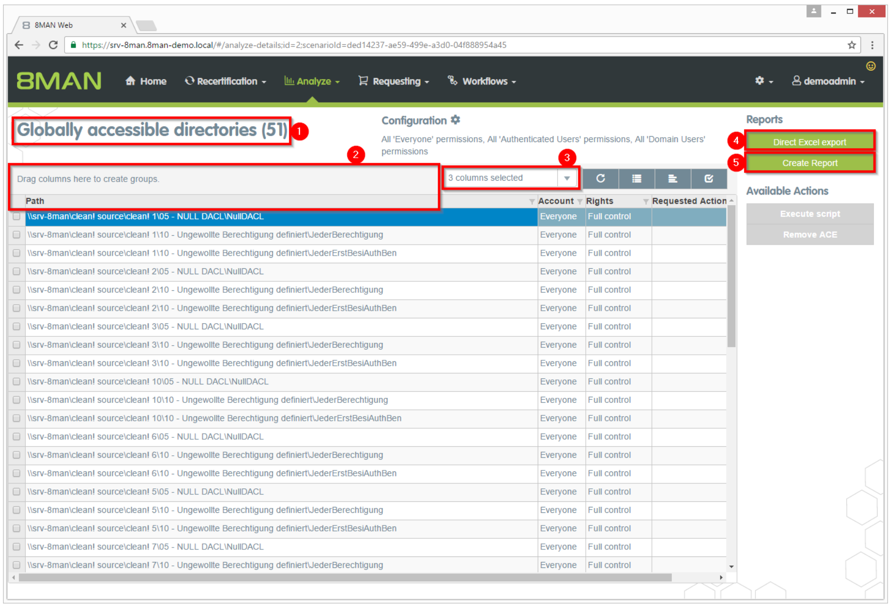
1. *Login to the web client.*



1. *After login you see the web client homepage.*
2. *8MAN shows an overall rating in the area "Risk Management".*
   The higher the number the higher the risk level.
   Click the tile.



1. *8MAN shows a rating for the risk factor "Globally accessible directories".*
2. *Click "Minimize risks".*



Globally accessible directories (51)

Configuration

All 'Everyone' permissions, All 'Authenticated Users' permissions, All 'Domain Users' permissions

Drag columns here to create groups.

3 columns selected

Path	Account	Rights	Requested Action
\\srv-8man\clean! source\clean! 1\05 - NULL DACL\NullDACL	Everyone	Full control	
\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
\\srv-8man\clean! source\clean! 2\05 - NULL DACL\NullDACL	Everyone	Full control	
\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	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\JederBerechtigung	Everyone	Full control	
\\srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
\\srv-8man\clean! source\clean! 10\05 - NULL DACL\NullDACL	Everyone	Full control	
\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
\\srv-8man\clean! source\clean! 6\05 - NULL DACL\NullDACL	Everyone	Full control	
\\srv-8man\clean! source\clean! 6\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
\\srv-8man\clean! source\clean! 6\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
\\srv-8man\clean! source\clean! 5\05 - NULL DACL\NullDACL	Everyone	Full control	
\\srv-8man\clean! source\clean! 5\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
\\srv-8man\clean! source\clean! 5\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
\\srv-8man\clean! source\clean! 7\05 - NULL DACL\NullDACL	Everyone	Full control	
\\srv-8man\clean! source\clean! 7\10 - Ungewollte Berechtigung definiert\JederBerechtigung	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- oder CSV-format. Save the report or e-mail it.*

4.5.4 Identifying inactive accounts using the web client

Background / Value

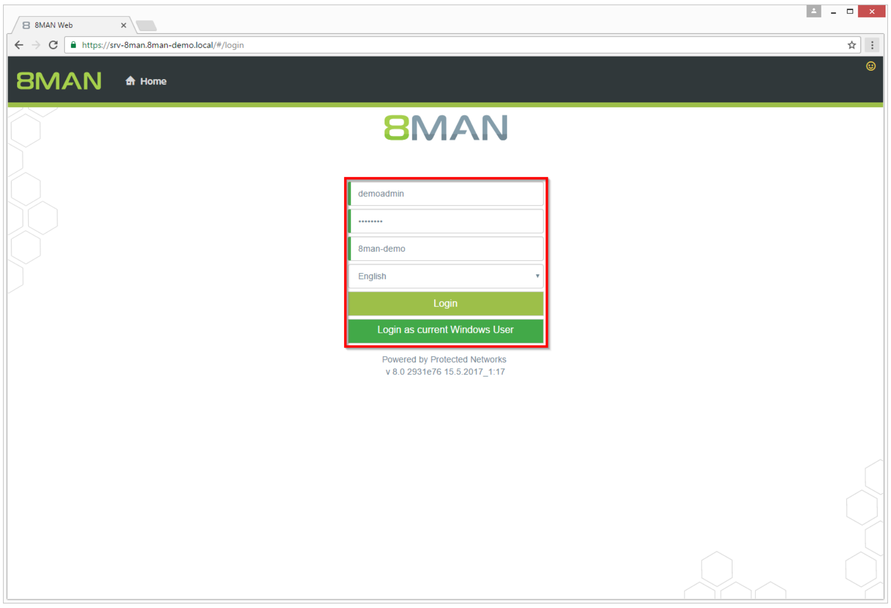
Inactive accounts can be used for data theft and manipulation without being detected. Since most inactive accounts are remnants of past employees, they are often a symptom of a communication problem between HR and IT. 8MAN displays all inactive accounts in Active Directory with a last logon older than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

Additional Services

Report: inactive accounts

Deactivating accounts in bulk (8MATE Analyze & Act and 8MAN Enterprise required)

Step by step process



demoadmin

••••••••

8man-demo

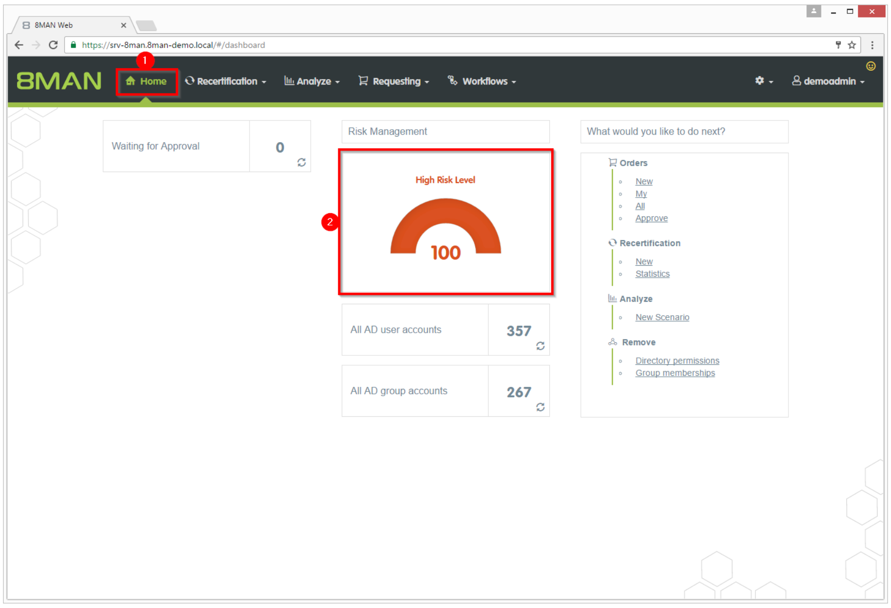
English

Login

Login as current Windows User

Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

Login to the web client.



Waiting for Approval 0

Risk Management

High Risk Level 100

All AD user accounts 357

All AD group accounts 267

What would you like to do next?

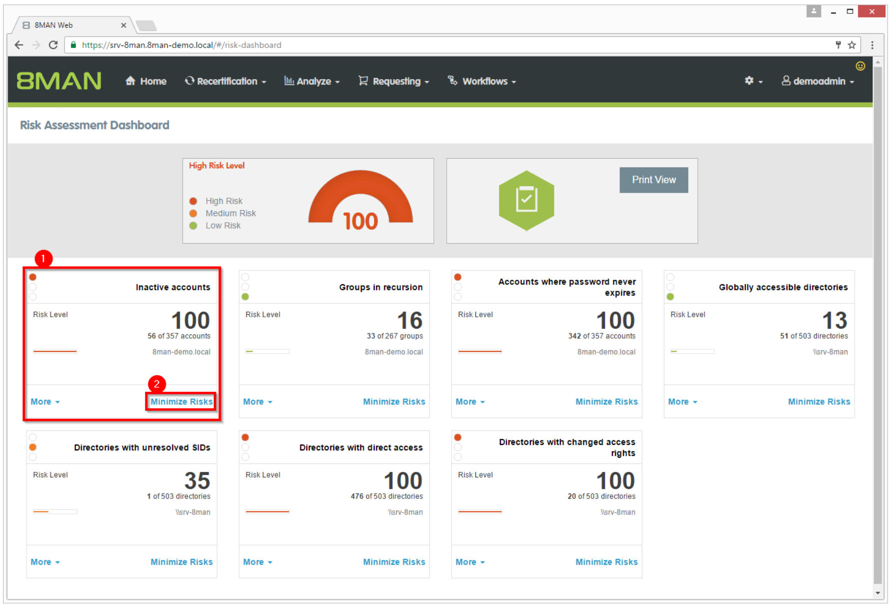
Orders
- New
- My
- All
- Approve

Recertification
- New
- Statistics

Analyze
- New Scenario

Remove
- Directory permissions
- Group memberships

1. *After login you see the web client homepage.*
2. *8MAN shows an overall rating in the area "Risk Management".*
   The higher the number the higher the risk level.
   Click the tile.

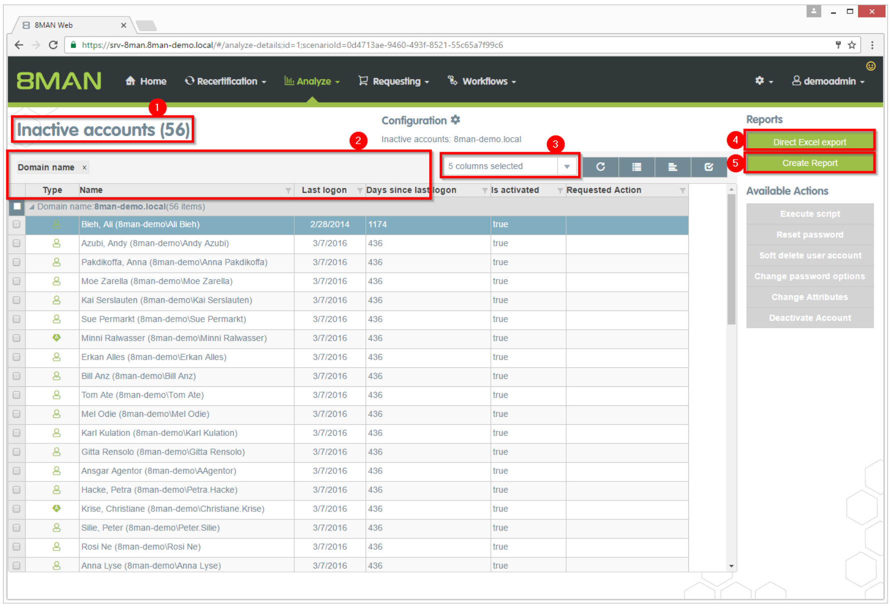


Risk Assessment Dashboard

High Risk Level 100
- High Risk
- Medium Risk
- Low Risk

Tile	Risk Level	Count	Source
Inactive accounts	100	56 of 357 accounts	8man-demo.local
Groups in recursion	16	33 of 267 groups	8man-demo.local
Accounts where password never expires	100	342 of 357 accounts	8man-demo.local
Globally accessible directories	13	51 of 503 directories	\\srv-8man
Directories with unresolved SIDs	35	1 of 503 directories	\\srv-8man
Directories with direct access	100	476 of 503 directories	\\srv-8man
Directories with changed access rights	100	20 of 503 directories	\\srv-8man

1. *8MAN shows a rating for the risk factor "Inactive accounts".*
2. *Click "Minimize risks".*


8MAN Web
https://srv-8man.8man-demo.local/#/analyze-details;id=1;scenarioId=0d4713ae-9460-493f-8521-55c65a7f99c6
8MAN
Home
Recertification
Analyze
Requesting
Workflows
demoadmin
1
2
3
4
5

Inactive accounts (56)

Configuration

Inactive accounts: 8man-demo.local

Domain name ×

5 columns selected

Reports

Direct Excel export

Create Report

Available Actions

Execute script

Reset password

Soft delete user account

Change password options

Change Attributes

Deactivate Account

	Type	Name	Last logon	Days since last logon	Is activated	Requested Action
□	Domain name:**8man-demo.local**(56 items)					
□	👤	Bieh, Ali (8man-demo\Ali Bieh)	2/28/2014	1174	true	
□	👤	Azubi, Andy (8man-demo\Andy Azubi)	3/7/2016	436	true	
□	👤	Pakdikoffa, Anna (8man-demo\Anna Pakdikoffa)	3/7/2016	436	true	
□	👤	Moe Zarella (8man-demo\Moe Zarella)	3/7/2016	436	true	
□	👤	Kai Serslauten (8man-demo\Kai Serslauten)	3/7/2016	436	true	
□	👤	Sue Permarkt (8man-demo\Sue Permarkt)	3/7/2016	436	true	
□	◆	Minni Ralwasser (8man-demo\Minni Ralwasser)	3/7/2016	436	true	
□	👤	Erkan Alles (8man-demo\Erkan Alles)	3/7/2016	436	true	
□	👤	Bill Anz (8man-demo\Bill Anz)	3/7/2016	436	true	
□	👤	Tom Ate (8man-demo\Tom Ate)	3/7/2016	436	true	
□	👤	Mel Odie (8man-demo\Mel Odie)	3/7/2016	436	true	
□	👤	Karl Kulation (8man-demo\Karl Kulation)	3/7/2016	436	true	
□	👤	Gitta Rensolo (8man-demo\Gitta Rensolo)	3/7/2016	436	true	
□	👤	Ansgar Agentor (8man-demo\AAgentor)	3/7/2016	436	true	
□	👤	Hacke, Petra (8man-demo\Petra.Hacke)	3/7/2016	436	true	
□	◆	Krise, Christiane (8man-demo\Christiane.Krise)	3/7/2016	436	true	
□	👤	Silie, Peter (8man-demo\Peter.Silie)	3/7/2016	436	true	
□	👤	Rosi Ne (8man-demo\Rosi Ne)	3/7/2016	436	true	
□	👤	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- oder CSV-format. Save the report or e-mail it.*

5. Documentation & Reporting

5.1 All Technologies

5.1.1 Reporting on 8MAN Access Rights Management activities (Logbook report)

Background / Value

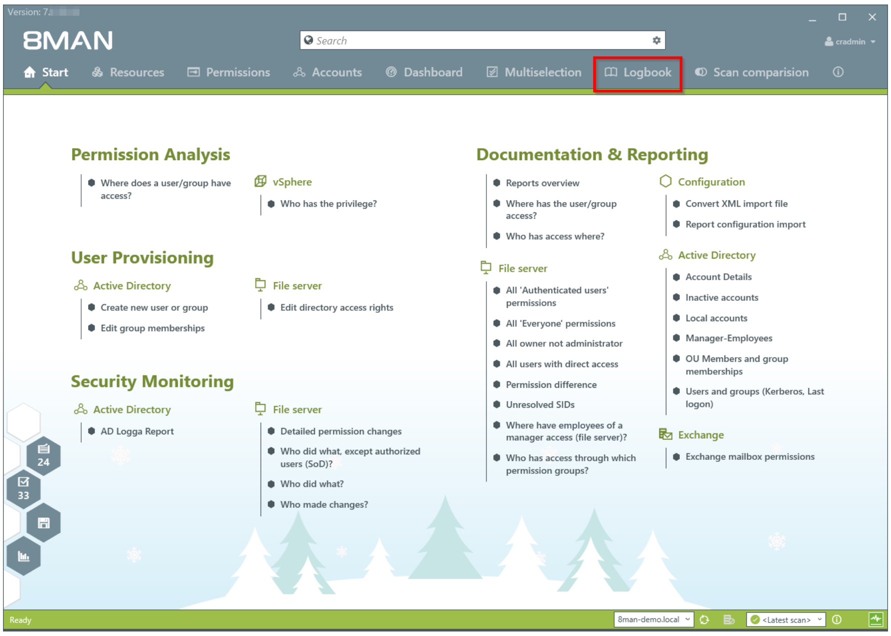
All changes made with 8MAN Enterprise are automatically recorded in the log book. This ensures compliance with a number of legal and best-practice standards and saves the time of manual documentation. The log book report allows you to capture events by person or event type within any desired time period.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

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

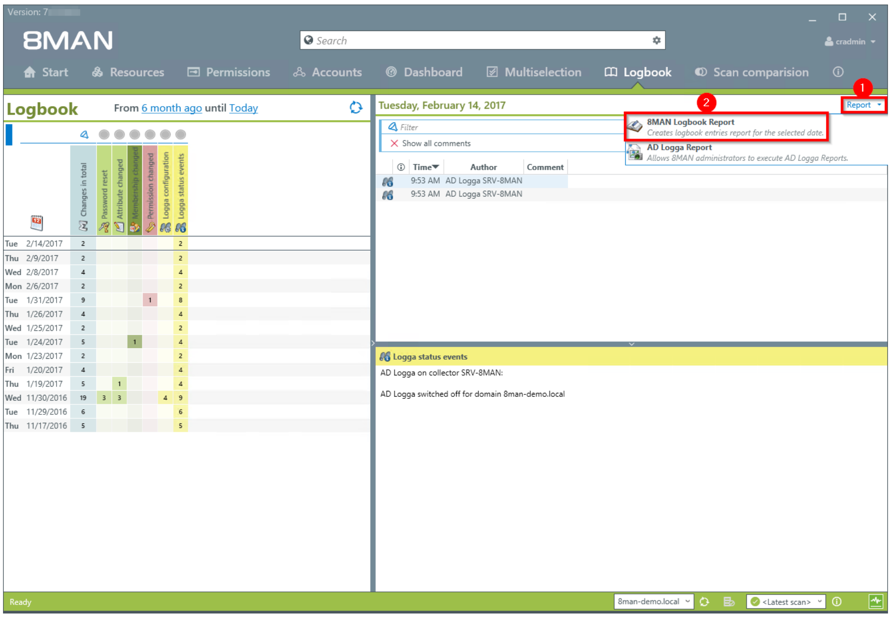
Additional Services

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

Step by step process



Select "Logbook".



Logbook From 6 month ago until Today

		Changes in total	Password reset	Attribute changed	Membership changed	Permission changed	Logga configuration	Logga status events
Tue	2/14/2017	2						2
Thu	2/9/2017	2						2
Wed	2/8/2017	4						4
Mon	2/6/2017	2						2
Tue	1/31/2017	9				1		8
Thu	1/26/2017	4						4
Wed	1/25/2017	2						2
Tue	1/24/2017	5			1			4
Mon	1/23/2017	2						2
Fri	1/20/2017	4						4
Thu	1/19/2017	5		1				4
Wed	11/30/2016	19	3	3			4	9
Tue	11/29/2016	6						6
Thu	11/17/2016	5						5

Tuesday, February 14, 2017

Filter

Show all comments

8MAN Logbook Report
Creates logbook entries report for the selected date.

AD Logga Report
Allows 8MAN administrators to execute AD Logga Reports.

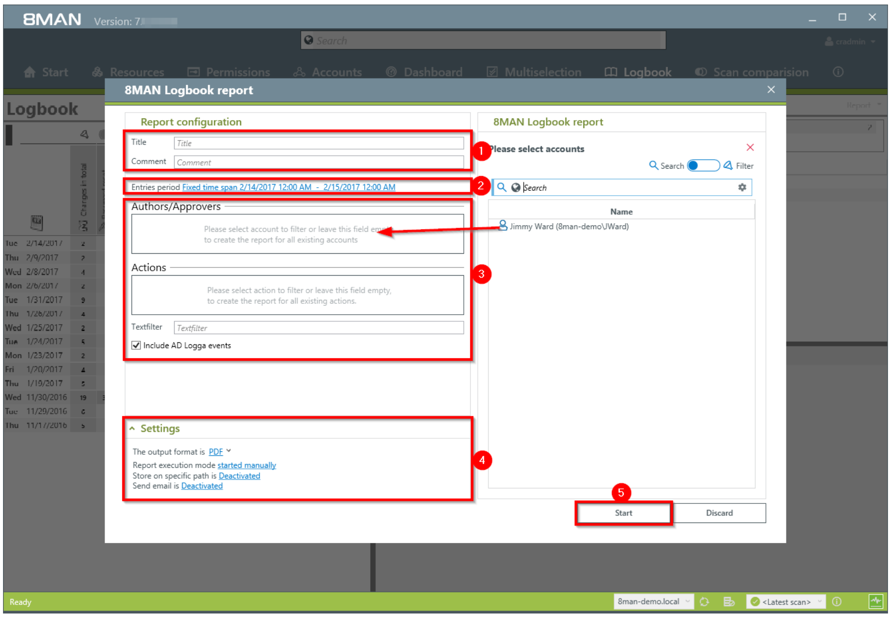
Time	Author	Comment
9:53 AM	AD Logga SRV-8MAN	
9:53 AM	AD Logga SRV-8MAN	

Logga status events

AD Logga on collector SRV-8MAN:

AD Logga switched off for domain 8man-demo.local

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



8MAN Logbook report

Report configuration

Title: Title

Comment: Comment

Entries period Fixed time span 2/14/2017 12:00 AM - 2/15/2017 12:00 AM

Authors/Approvers

Please select account to filter or leave this field empty to create the report for all existing accounts

Actions

Please select action to filter or leave this field empty, to create the report for all existing actions.

Textfilter: Textfilter

☑ Include AD Logga events

Settings

The output format is PDF

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

8MAN Logbook report

Please select accounts

Search / Filter

Search

Name
Jimmy Ward (8man-demo\JWard)

Start | Discard

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

5.2 Active Directory

5.2.1 Reports for Managers

5.2.1.1 Employees of a Manager

Background / Value

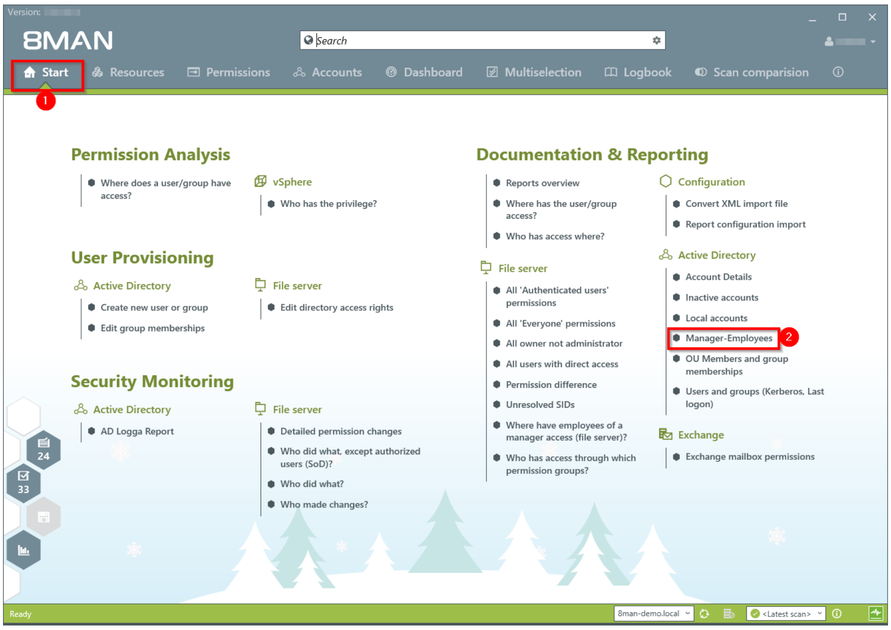
Data Owners that have some knowledge of Active Directory can view attributes and group memberships of their employees.

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

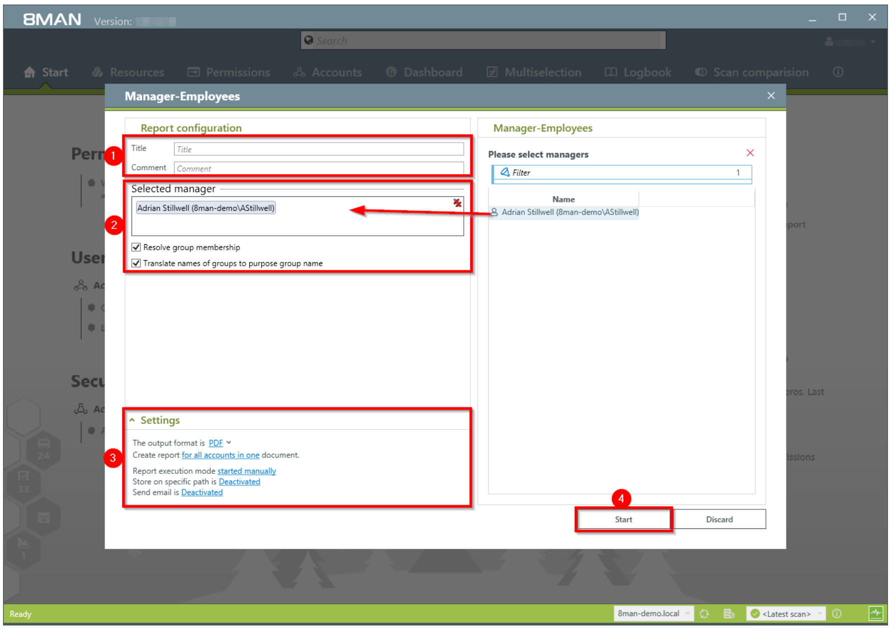
Additional Services

For more detailed information and the inclusion of assigned file server resources we recommend the report:
Where have employees of a manager access (file server)?

Step by step process



1. *Select "Start".*
2. *Click on "Manager-Employees".*



Title: Title
Comment: Comment

Selected manager
Adrian Stillwell (8man-demo\AStillwell)

☑ Resolve group membership
☑ Translate names of groups to purpose group name

Settings
The output format is PDF
Create report for all accounts in one document.
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

Manager-Employees
Please select managers
Filter 1

Name
Adrian Stillwell (8man-demo\AStillwell)

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 Displaying user account details

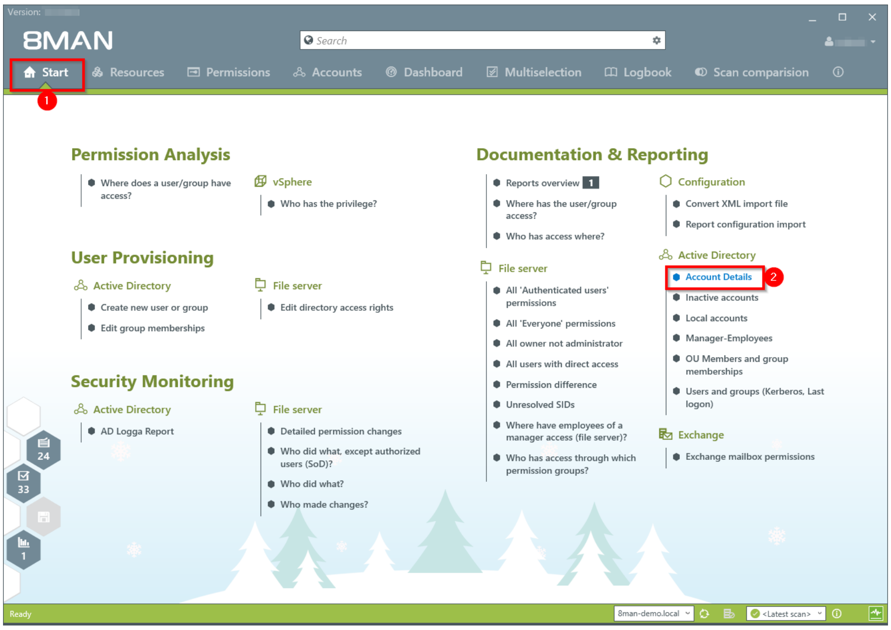
Background / Value

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

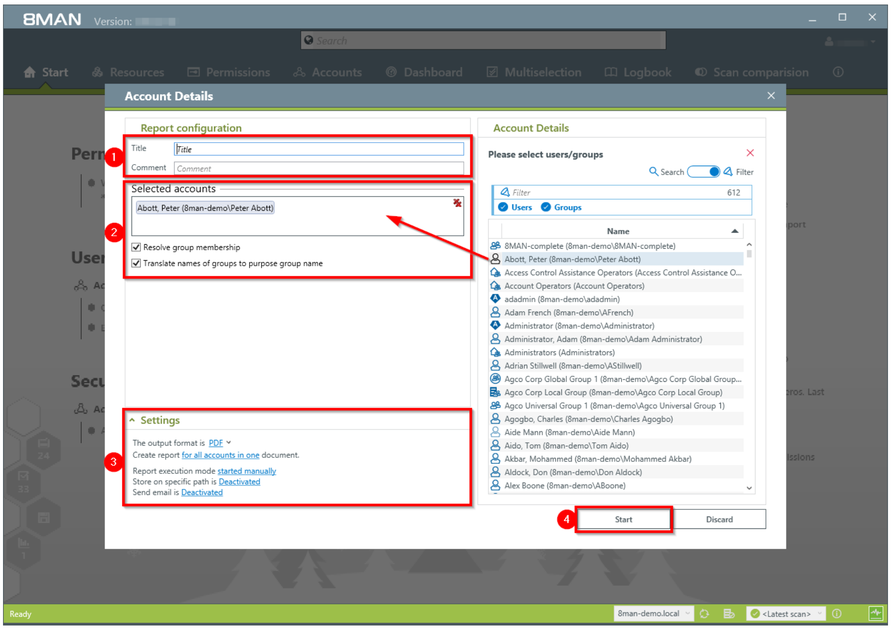
The following information is shown in a structured report:

- Expiration date of the account
- Display name
- User login name
- Common name
- Defined name
- E-mail address
- LDAP ADsPath
- Last login
- Object GUID
- Object SID
- SAM Account Name
- SAM Account type
- Group memberships
- Parents + children

Step by step process



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



Report configuration

Title: Title

Comment: Comment

Selected accounts

Abott, Peter (8man-demo\Peter Abott)

☑ Resolve group membership

☑ Translate names of groups to purpose group name

Settings

The output format is PDF

Create report for all accounts in one document.

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

Account Details

Please select users/groups

Search Filter

Filter 612

Users Groups

Name
8MAN-complete (8man-demo\8MAN-complete)
Abott, Peter (8man-demo\Peter Abott)
Access Control Assistance Operators (Access Control Assistance O...
Account Operators (Account Operators)
adadmin (8man-demo\adadmin)
Adam French (8man-demo\AFrench)
Administrator (8man-demo\Administrator)
Administrator, Adam (8man-demo\Adam Administrator)
Administrators (Administrators)
Adrian Stillwell (8man-demo\AStillwell)
Agco Corp Global Group 1 (8man-demo\Agco Corp Global Group...
Agco Corp Local Group (8man-demo\Agco Corp Local Group)
Agco Universal Group 1 (8man-demo\Agco Universal Group 1)
Agogbo, Charles (8man-demo\Charles Agogbo)
Aide Mann (8man-demo\Aide Mann)
Aido, Tom (8man-demo\Tom Aido)
Akbar, Mohammed (8man-demo\Mohammed Akbar)
Aldock, Don (8man-demo\Don Aldock)
Alex Boone (8man-demo\ABoone)

Start Discard

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 Finding inactive accounts (users or computers)

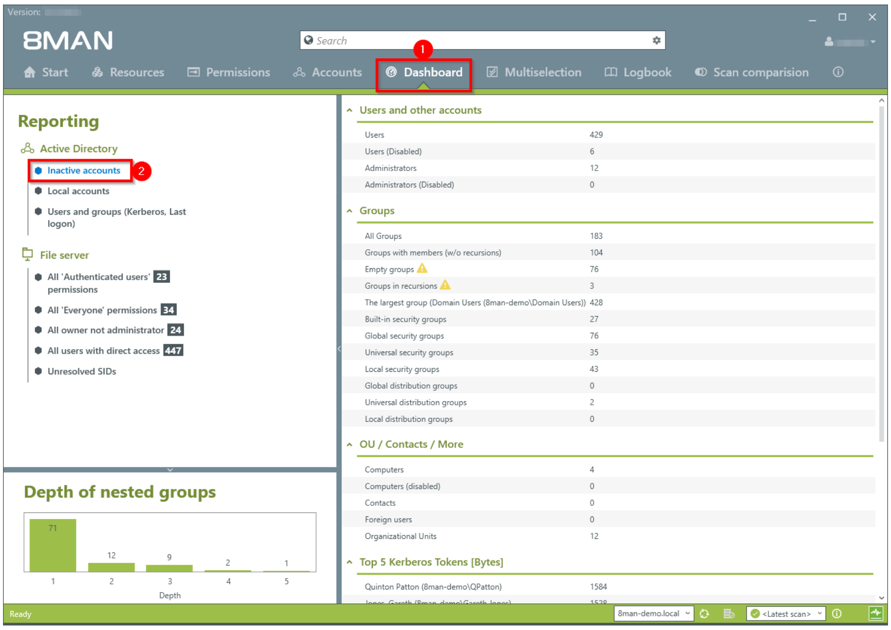
Background / Value

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

Deleting a user and their permission
Deleting a user account by using the "soft delete" feature
Deactivating a user account

Step by step process



Users and other accounts

Users	429
Users (Disabled)	6
Administrators	12
Administrators (Disabled)	0

Groups

All Groups	183
Groups with members (w/o recursions)	104
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	43
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

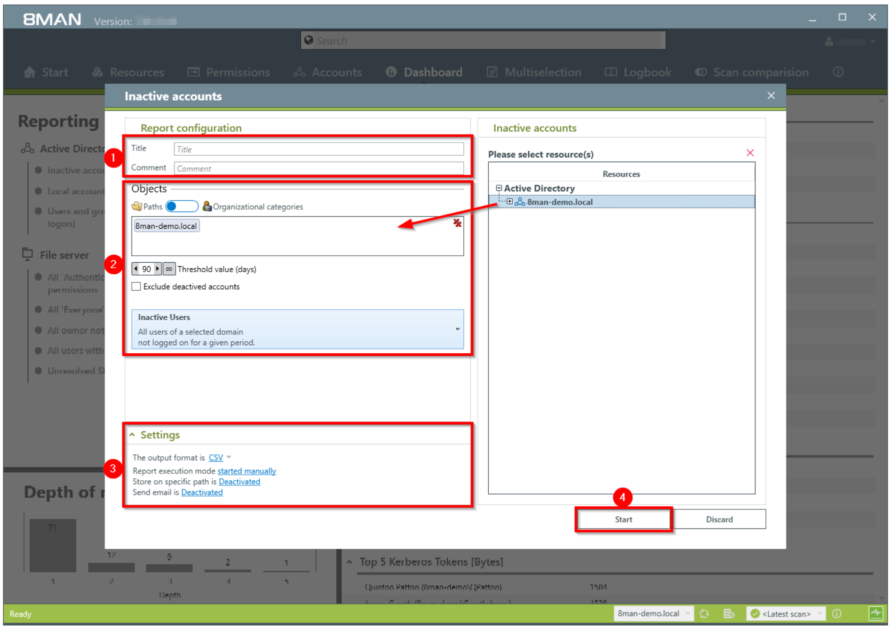
OU / Contacts / More

Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584

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



Inactive accounts

Report configuration

Title: Title

Comment: Comment

Objects

Paths / Organizational categories

8man-demo.local

90 Threshold value (days)

□ Exclude deactived accounts

Inactive Users
All users of a selected domain
not logged on for a given period.

Settings

The output format is CSV
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

Inactive accounts

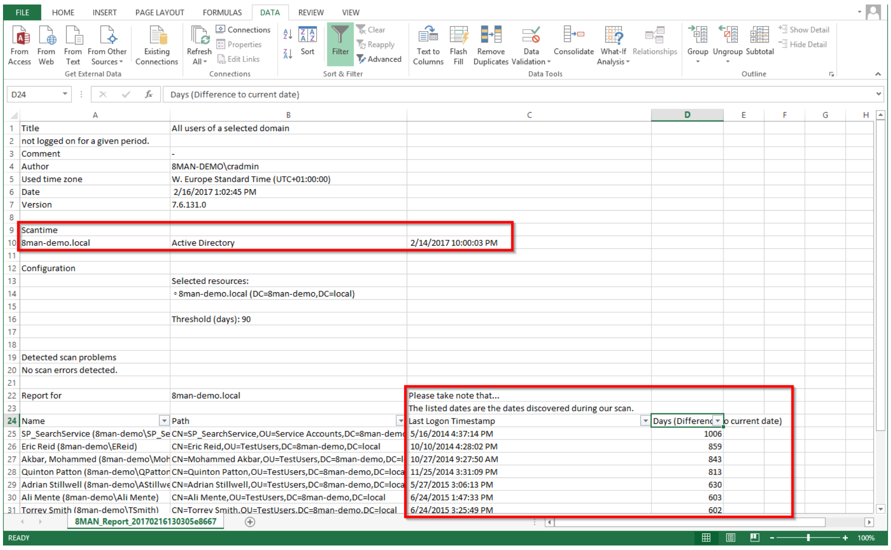
Please select resource(s)

Resources

Active Directory
8man-demo.local

Start | Discard

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



Days (Difference to current date)

	A	B	C	D
1	Title	All users of a selected domain		
2	not logged on for a given period.			
3	Comment	-		
4	Author	8MAN-DEMO\cradmin		
5	Used time zone	W. Europe Standard Time (UTC+01:00:00)		
6	Date	2/16/2017 1:02:45 PM		
7	Version	7.6.131.0		
8				
9	Scantime			
10	8man-demo.local	Active Directory	2/14/2017 10:00:03 PM	
11				
12	Configuration			
13		Selected resources:		
14		◦ 8man-demo.local (DC=8man-demo,DC=local)		
15				
16		Threshold (days): 90		
17				
18				
19	Detected scan problems			
20	No scan errors detected.			
21				
22	Report for	8man-demo.local	Please take note that...	
23			The listed dates are the dates discovered during our scan.	
24	Name	Path	Last Logon Timestamp	Days (Differenc o current date)
25	SP_SearchService (8man-demo\SP_Se	CN=SP_SearchService,OU=Service Accounts,DC=8man-demo	5/16/2014 4:37:14 PM	1006
26	Eric Reid (8man-demo\EReid)	CN=Eric Reid,OU=TestUsers,DC=8man-demo,DC=local	10/10/2014 4:28:02 PM	859
27	Akbar, Mohammed (8man-demo\Moh	CN=Mohammed Akbar,OU=TestUsers,DC=8man-demo,DC=l	10/27/2014 9:27:50 AM	843
28	Quinton Patton (8man-demo\QPatton	CN=Quinton Patton,OU=TestUsers,DC=8man-demo,DC=loca	11/25/2014 3:31:09 PM	813
29	Adrian Stillwell (8man-demo\AStillwe	CN=Adrian Stillwell,OU=TestUsers,DC=8man-demo,DC=loca	5/27/2015 3:06:13 PM	630
30	Ali Mente (8man-demo\Ali Mente)	CN=Ali Mente,OU=TestUsers,DC=8man-demo,DC=local	6/24/2015 1:47:33 PM	603
31	Torrey Smith (8man-demo\TSmith)	CN=Torrey Smith,OU=TestUsers,DC=8man-demo,DC=local	6/24/2015 3:25:49 PM	602

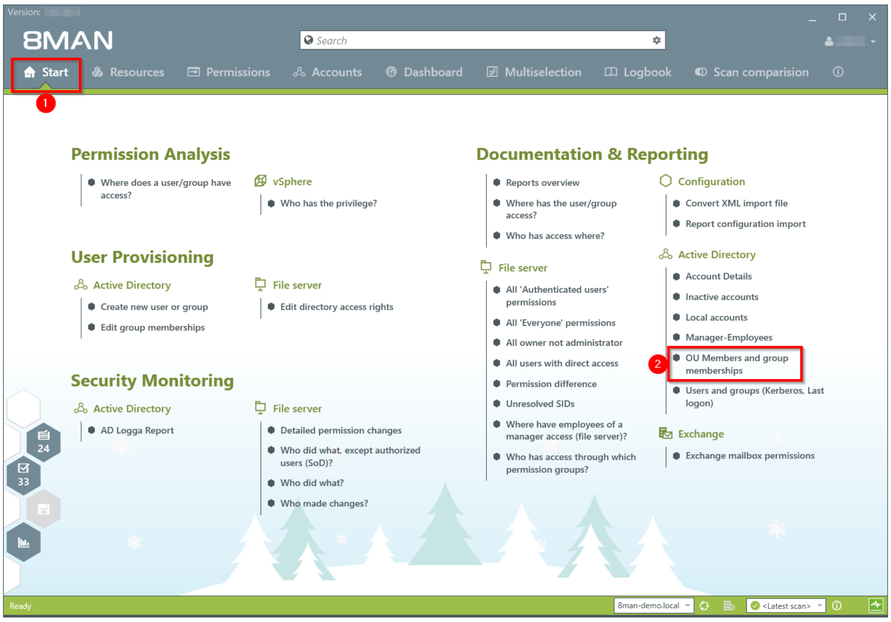
Review the data in the report. If using historical scan data there may be differences in the days since the last login.

5.2.2.3 Report: OU Mitglieder und Gruppenzugehörigkeiten

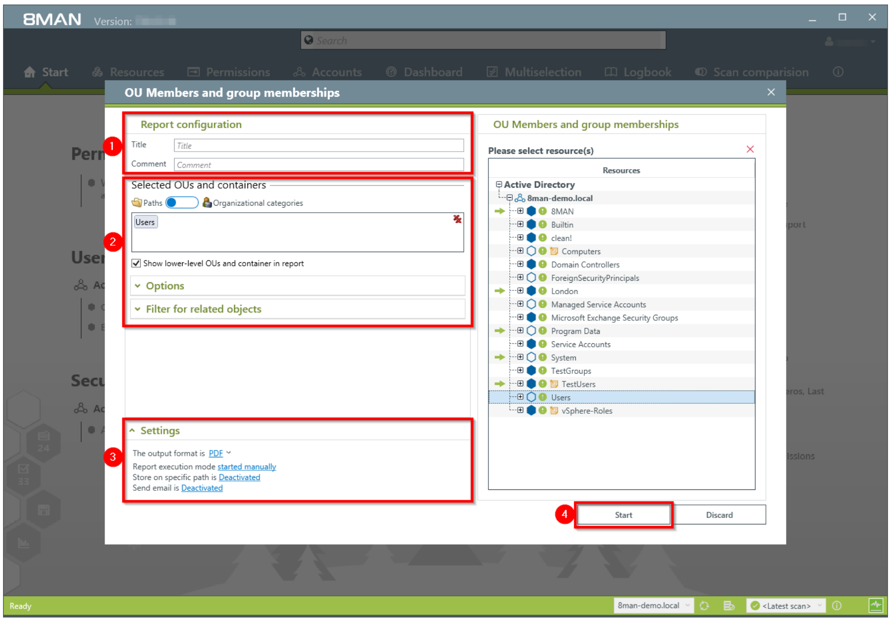
Background / Value

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

Step by step process



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



The output format is PDF
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

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 Identifying users and groups

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.

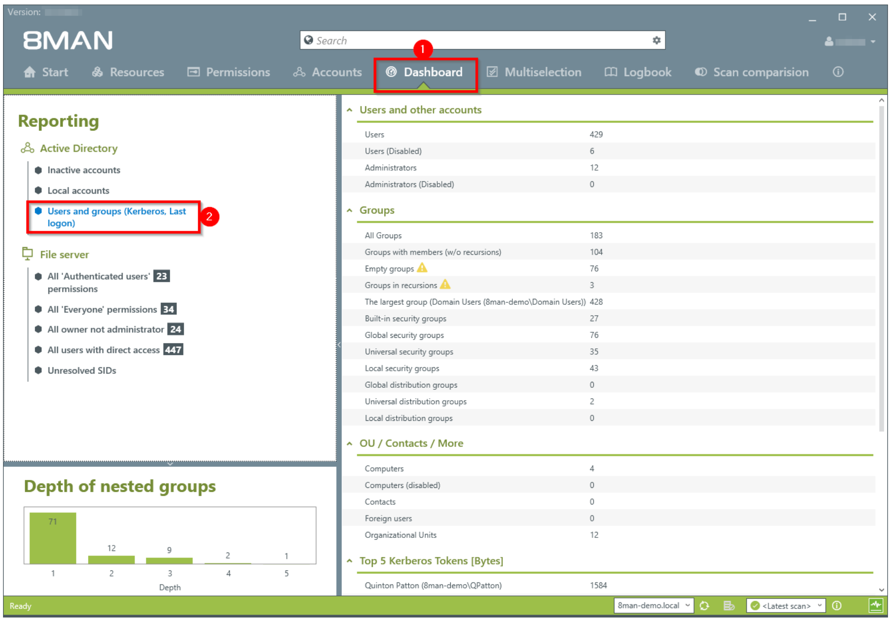
In addition the following information is also displayed:

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

Groups

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

Step by step process



Users and other accounts

Users	429
Users (Disabled)	6
Administrators	12
Administrators (Disabled)	0

Groups

All Groups	183
Groups with members (w/o recursions)	104
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	43
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

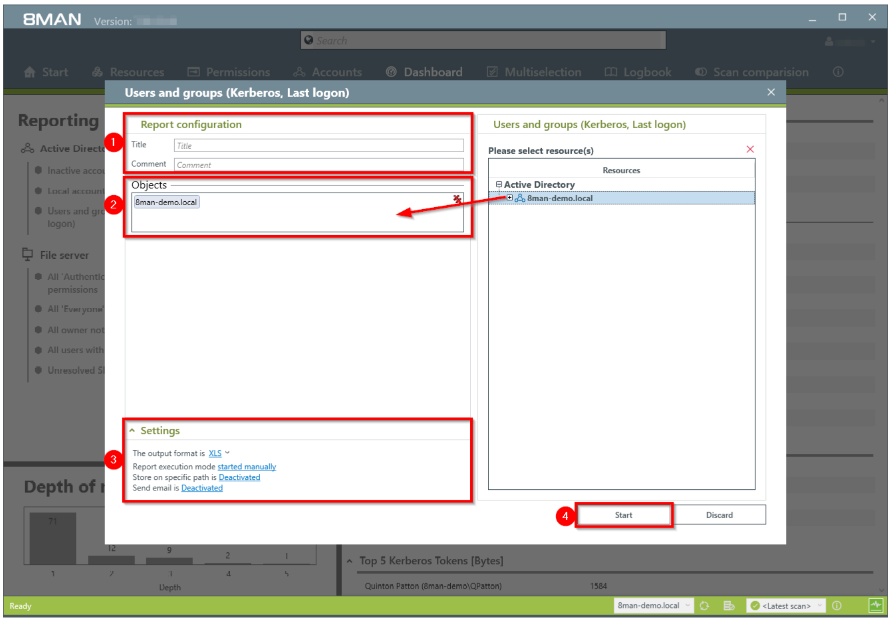
OU / Contacts / More

Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584

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



Users and groups (Kerberos, Last logon)

Report configuration

Title: Title

Comment: Comment

Objects: 8man-demo.local

Users and groups (Kerberos, Last logon)

Please select resource(s)

Resources

Active Directory
- 8man-demo.local

Settings

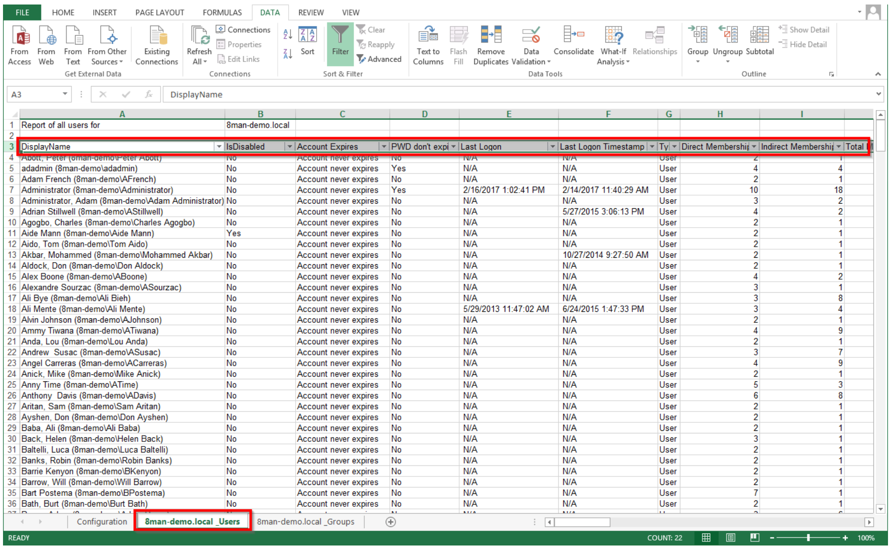
The output format is XLS

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

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.*



A3: DisplayName

	A	B	C	D	E	F	G	H	I
1	Report of all users for	8man-demo.local							
2									
3	DisplayName	IsDisabled	Account Expires	PWD don't expi	Last Logon	Last Logon Timestamp	Ty	Direct Membershi	Indirect Membershi
4	Abott, Peter (8man-demo\Peter Abott)	No	Account never expires	No	N/A	N/A	User	2	1
5	adadmin (8man-demo\adadmin)	No	Account never expires	Yes	N/A	N/A	User	4	4
6	Adam French (8man-demo\AFrench)	No	Account never expires	No	N/A	N/A	User	2	1
7	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
8	Administrator, Adam (8man-demo\Adam Administrator)	No	Account never expires	No	N/A	N/A	User	3	2
9	Adrian Stillwell (8man-demo\AStillwell)	No	Account never expires	No	N/A	5/27/2015 3:06:13 PM	User	4	2
10	Agogbo, Charles (8man-demo\Charles Agogbo)	No	Account never expires	No	N/A	N/A	User	2	1
11	Aide Mann (8man-demo\Aide Mann)	Yes	Account never expires	No	N/A	N/A	User	2	1
12	Aido, Tom (8man-demo\Tom Aido)	No	Account never expires	No	N/A	N/A	User	2	1
13	Akbar, Mohammed (8man-demo\Mohammed Akbar)	No	Account never expires	No	N/A	10/27/2014 9:27:50 AM	User	2	1
14	Aldock, Don (8man-demo\Don Aldock)	No	Account never expires	No	N/A	N/A	User	2	1
15	Alex Boone (8man-demo\ABoone)	No	Account never expires	No	N/A	N/A	User	4	2
16	Alexandre Sourzac (8man-demo\ASourzac)	No	Account never expires	No	N/A	N/A	User	3	1
17	Ali Bye (8man-demo\Ali Bieh)	No	Account never expires	No	N/A	N/A	User	3	8
18	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
19	Alvin Johnson (8man-demo\AJohnson)	No	Account never expires	No	N/A	N/A	User	2	1
20	Ammy Tiwana (8man-demo\ATiwana)	No	Account never expires	No	N/A	N/A	User	4	9
21	Anda, Lou (8man-demo\Lou Anda)	No	Account never expires	No	N/A	N/A	User	2	1
22	Andrew Susac (8man-demo\ASusac)	No	Account never expires	No	N/A	N/A	User	3	7
23	Angel Carreras (8man-demo\ACarreras)	No	Account never expires	No	N/A	N/A	User	4	9
24	Anick, Mike (8man-demo\Mike Anick)	No	Account never expires	No	N/A	N/A	User	2	1
25	Anny Time (8man-demo\ATime)	No	Account never expires	No	N/A	N/A	User	5	3
26	Anthony Davis (8man-demo\ADavis)	No	Account never expires	No	N/A	N/A	User	6	8
27	Aritan, Sam (8man-demo\Sam Aritan)	No	Account never expires	No	N/A	N/A	User	2	1
28	Ayshen, Don (8man-demo\Don Ayshen)	No	Account never expires	No	N/A	N/A	User	2	1
29	Baba, Ali (8man-demo\Ali Baba)	No	Account never expires	No	N/A	N/A	User	2	1
30	Back, Helen (8man-demo\Helen Back)	No	Account never expires	No	N/A	N/A	User	3	1
31	Baltelli, Luca (8man-demo\Luca Baltelli)	No	Account never expires	No	N/A	N/A	User	2	1
32	Banks, Robin (8man-demo\Robin Banks)	No	Account never expires	No	N/A	N/A	User	2	1
33	Barrie Kenyon (8man-demo\BKenyon)	No	Account never expires	No	N/A	N/A	User	2	1
34	Barrow, Will (8man-demo\Will Barrow)	No	Account never expires	No	N/A	N/A	User	2	1
35	Bart Postema (8man-demo\BPostema)	No	Account never expires	No	N/A	N/A	User	7	1
36	Bath, Burt (8man-demo\Burt Bath)	No	Account never expires	No	N/A	N/A	User	2	1

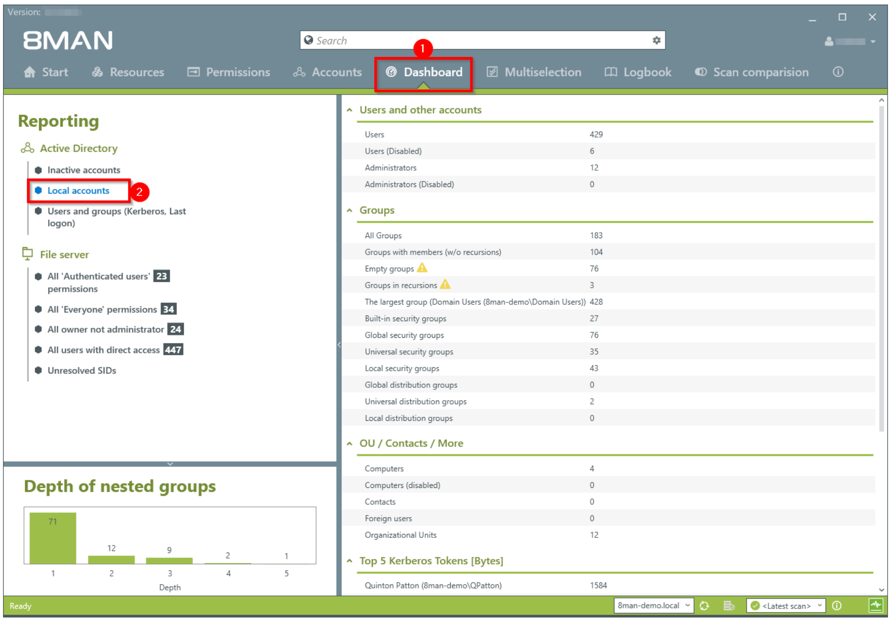
Open the report in Excel and apply the desired filters.

5.2.2.5 Identifying local accounts

Background / Value

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

Step by step process



Users and other accounts

Users	429
Users (Disabled)	6
Administrators	12
Administrators (Disabled)	0

Groups

All Groups	183
Groups with members (w/o recursions)	104
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	43
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

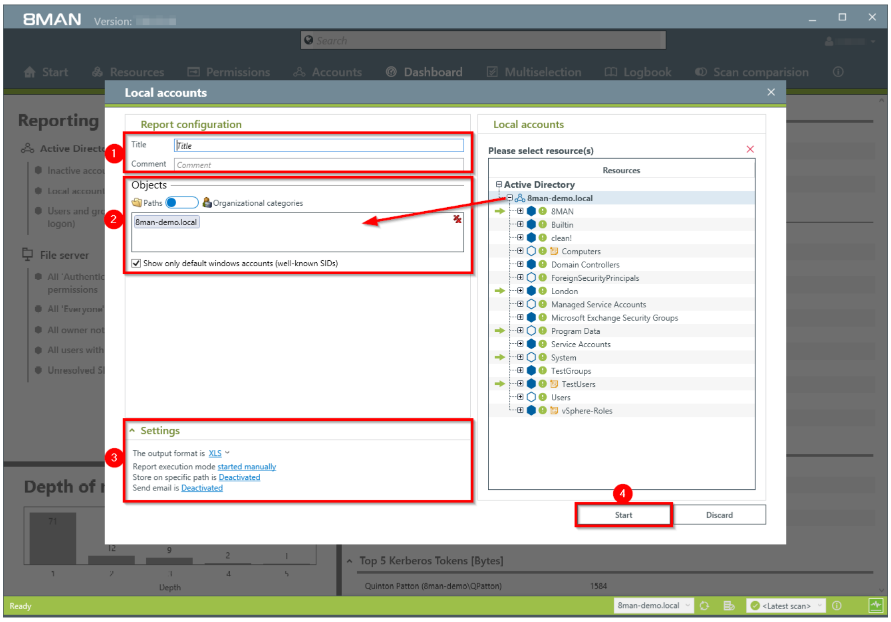
OU / Contacts / More

Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584

1. *Select "Dashboard".*
2. *Click on "Local accounts".*



Title: Title

Comment: Comment

8man-demo.local

☑ Show only default windows accounts (well-known SIDs)

Please select resource(s)

Settings

The output format is XLS
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

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

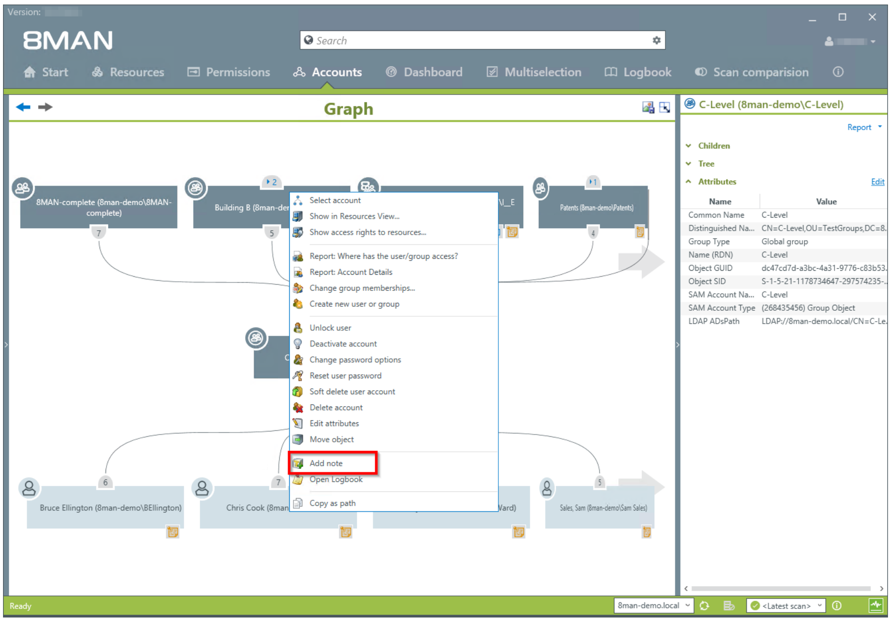
Besides automated documentation and reports 8MAN also includes a number of additional documentation features. These allow you to add post-its to objects manually or give AD groups aliases with the "purpose groups" feature.

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.

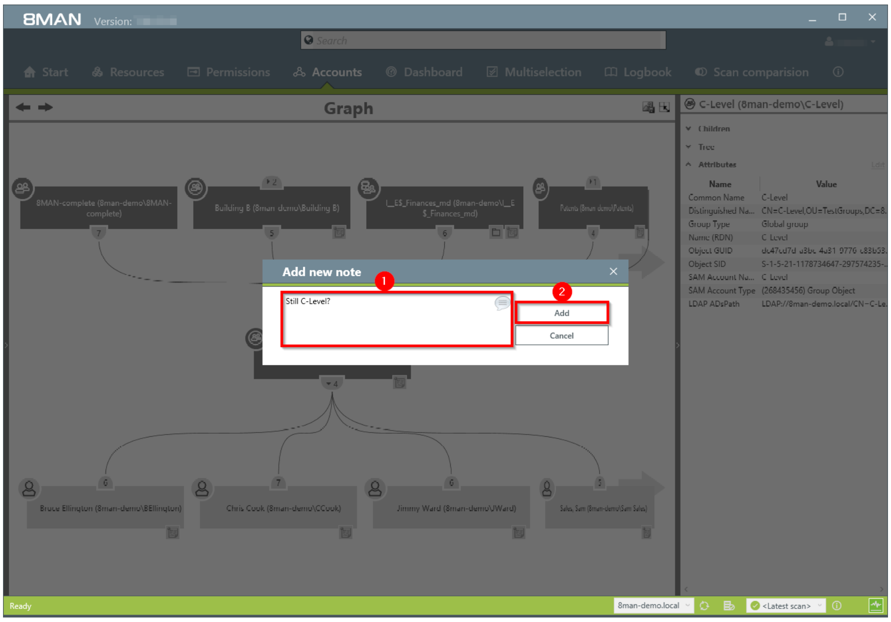
Step by step process



C-Level (8man-demo\C-Level)

Name	Value
Common Name	C-Level
Distinguished Na...	CN=C-Level,OU=TestGroups,DC=8.
Group Type	Global group
Name (RDN)	C-Level
Object GUID	dc47cd7d-a3bc-4a31-9776-c83b53.
Object SID	S-1-5-21-1178734647-297574235-..
SAM Account Na...	C-Level
SAM Account Type	(268435456) Group Object
LDAP ADsPath	LDAP://8man-demo.local/CN=C-Le.

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



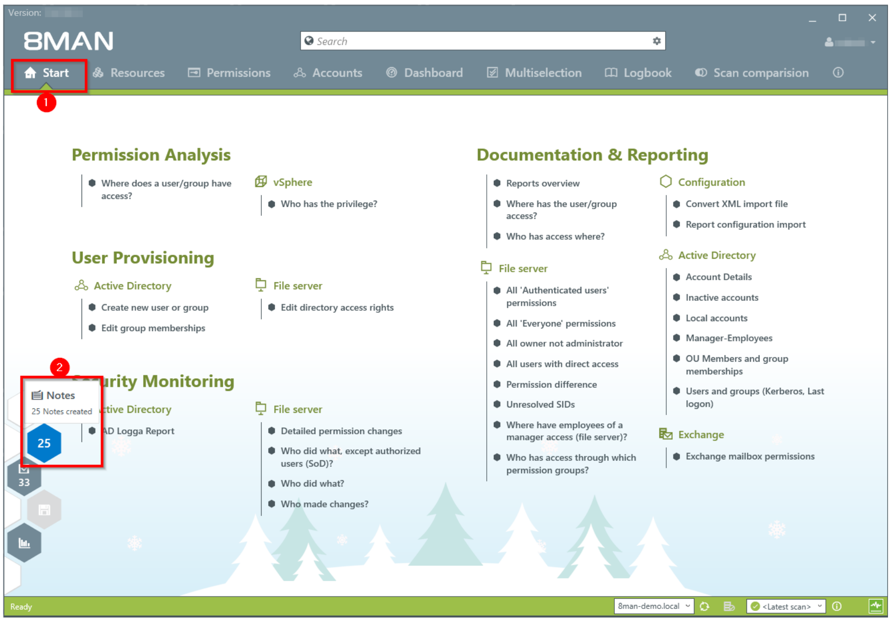
Add new note

Still C-Level?

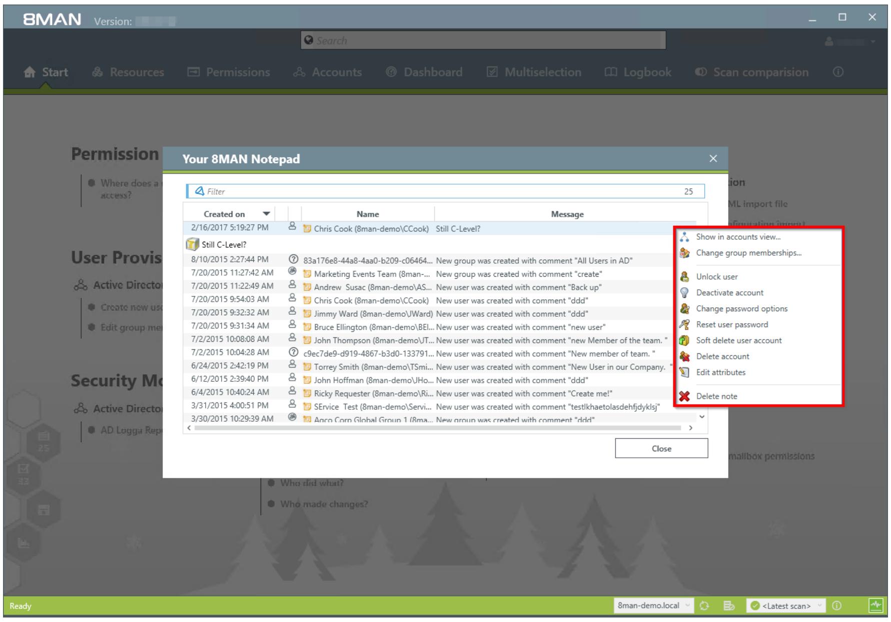
Add

Cancel

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



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



Created on	Name	Message
2/16/2017 5:19:27 PM	Chris Cook (8man-demo\CCook)	Still C-Level?
Still C-Level?		
8/10/2015 2:27:44 PM	83a176e8-44a8-4aa0-b209-c06464...	New group was created with comment "All Users in AD"
7/20/2015 11:27:42 AM	Marketing Events Team (8man-...	New group was created with comment "create"
7/20/2015 11:22:49 AM	Andrew Susac (8man-demo\AS...	New user was created with comment "Back up"
7/20/2015 9:54:03 AM	Chris Cook (8man-demo\CCook)	New user was created with comment "ddd"
7/20/2015 9:32:32 AM	Jimmy Ward (8man-demo\JWard)	New user was created with comment "ddd"
7/20/2015 9:31:34 AM	Bruce Ellington (8man-demo\BEl...	New user was created with comment "new user"
7/2/2015 10:08:08 AM	John Thompson (8man-demo\JT...	New user was created with comment "new Member of the team. "
7/2/2015 10:04:28 AM	c9ec7de9-d919-4867-b3d0-133791...	New user was created with comment "New member of team. "
6/24/2015 2:42:19 PM	Torrey Smith (8man-demo\TSmi...	New user was created with comment "New User in our Company. "
6/12/2015 2:39:40 PM	John Hoffman (8man-demo\JHo...	New user was created with comment "ddd"
6/4/2015 10:40:24 AM	Ricky Requester (8man-demo\Ri...	New user was created with comment "Create me!"
3/31/2015 4:00:51 PM	SErvice Test (8man-demo\Servi...	New user was created with comment "testlkhaetolasdehfjdyklsj"
3/30/2015 10:29:39 AM	Agco Corp Global Group 1 (8ma...	New group was created with comment "ddd"

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: Giving aliases to groups

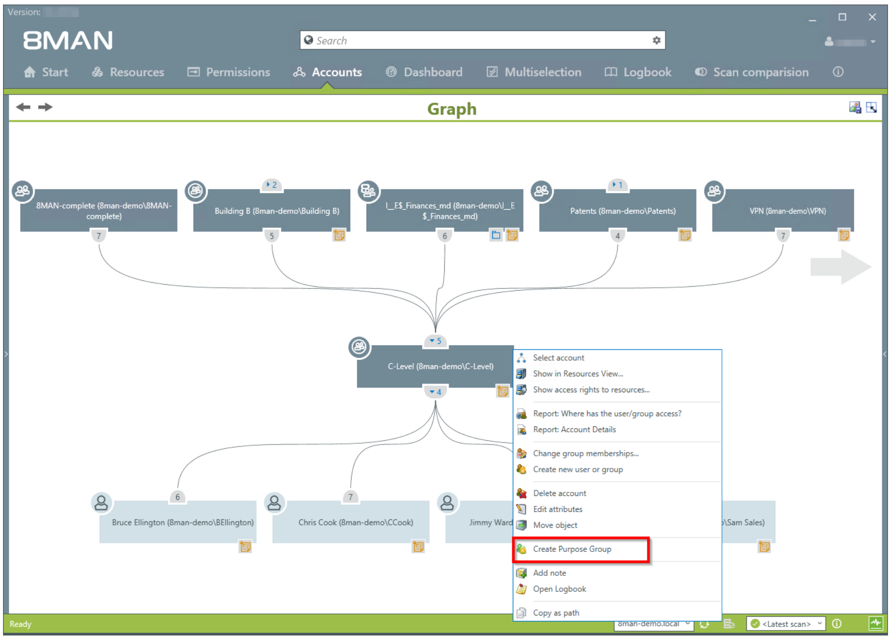
Background / Value

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.

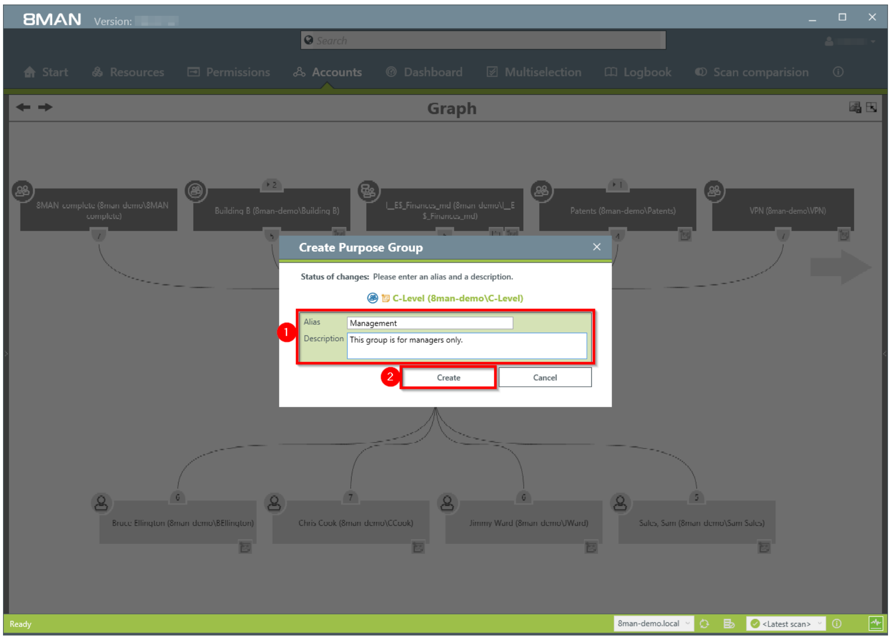
The alias descriptions are only visible in the 8MAN UI. The actual group names remain the same in Active Directory.

5.2.3.2.1 Creating a purpose group

Step by step process


8MAN
Search
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
Graph
8MAN-complete (8man-demo\8MAN-complete)
Building B (8man-demo\Building B)
I_E$_Finances_md (8man-demo\I_E$_Finances_md)
Patents (8man-demo\Patents)
VPN (8man-demo\VPN)
C-Level (8man-demo\C-Level)
Bruce Ellington (8man-demo\BEllington)
Chris Cook (8man-demo\CCook)
Jimmy Ward
\Sam Sales)
Select account
Show in Resources View...
Show access rights to resources...
Report: Where has the user/group access?
Report: Account Details
Change group memberships...
Create new user or group
Delete account
Edit attributes
Move object
Create Purpose Group
Add note
Open Logbook
Copy as path
Ready
8man-demo.local
<Latest scan>

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



Create Purpose Group

Status of changes: Please enter an alias and a description.

C-Level (8man-demo\C-Level)

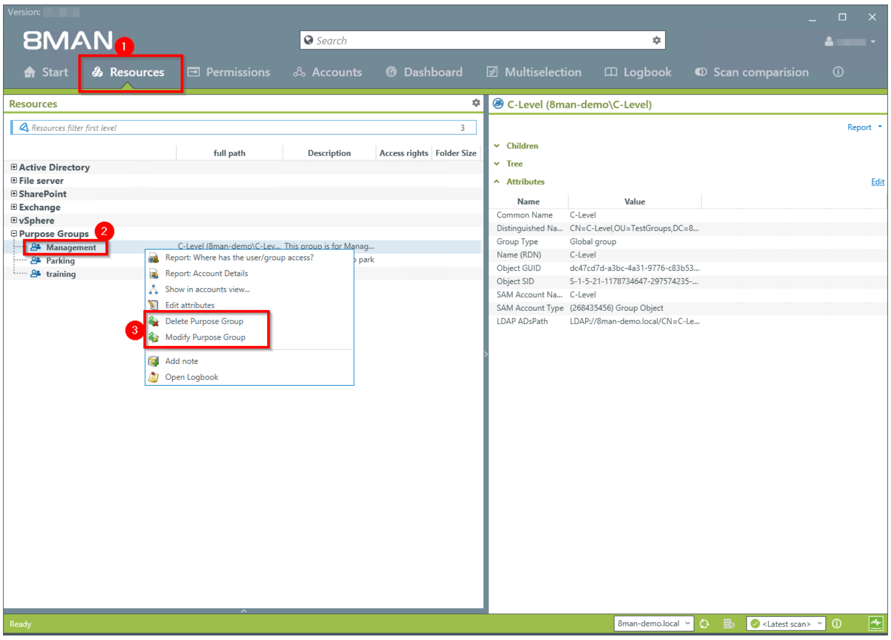
Alias: Management

Description: This group is for managers only.

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

5.2.3.2.2 Deleting or modifying a purpose group

Step by step process



Management: C-Level (8man-demo\C-Lev... This group is for Manag...

C-Level (8man-demo\C-Level)

Name	Value
Common Name	C-Level
Distinguished Na...	CN=C-Level,OU=TestGroups,DC=8...
Group Type	Global group
Name (RDN)	C-Level
Object GUID	dc47cd7d-a3bc-4a31-9776-c83b53...
Object SID	S-1-5-21-1178734647-297574235-...
SAM Account Na...	C-Level
SAM Account Type	(268435456) Group Object
LDAP ADsPath	LDAP://8man-demo.local/CN=C-Le...

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 description in 8MAN. Non changes are made to Active Directory.

5.3 File server

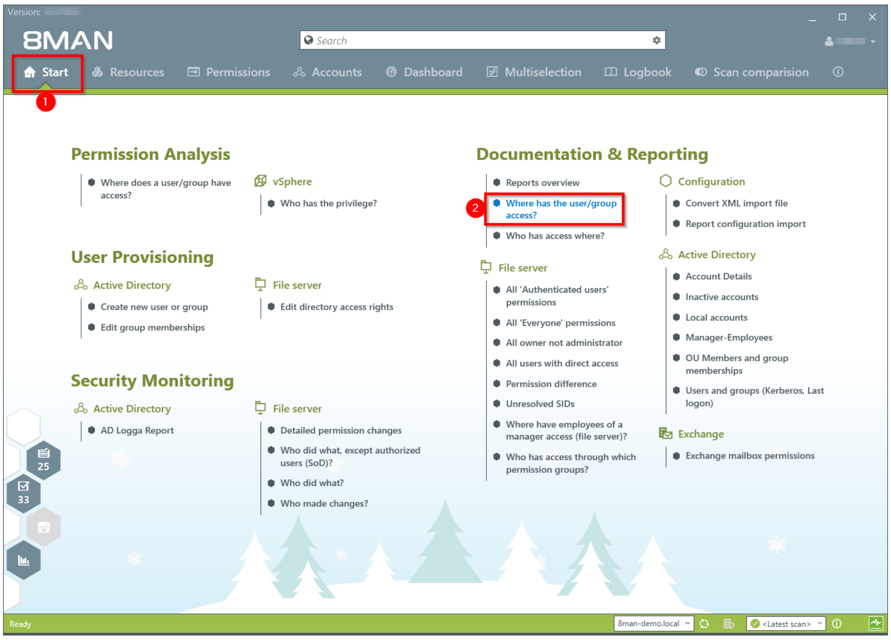
5.3.1 Management Reports

5.3.1.1 Where do users and groups have access?

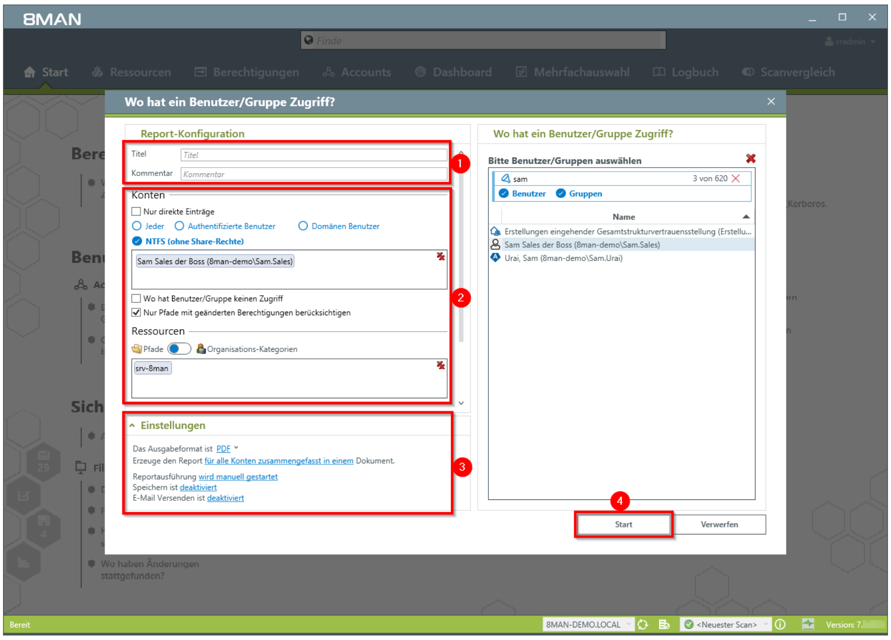
Background / Value

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

Step by step process



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



Wo hat ein Benutzer/Gruppe Zugriff?

Report-Konfiguration

Titel: Titel

Kommentar: Kommentar

Konten

☐ Nur direkte Einträge

○ Jeder ○ Authentifizierte Benutzer ○ Domänen Benutzer

● NTFS (ohne Share-Rechte)

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

☐ Wo hat Benutzer/Gruppe keinen Zugriff

☑ Nur Pfade mit geänderten Berechtigungen berücksichtigen

Ressourcen

Pfade / Organisations-Kategorien

srv-8man

Einstellungen

Das Ausgabeformat ist PDF

Erzeuge den Report für alle Konten zusammengefasst in einem Dokument.

Reportausführung wird manuell gestartet

Speichern ist deaktiviert

E-Mail Versenden ist deaktiviert

Wo hat ein Benutzer/Gruppe Zugriff?

Bitte Benutzer/Gruppen auswählen

sam — 3 von 620

✓ Benutzer ✓ Gruppen

Name
Erstellungen eingehender Gesamtstrukturvertrauensstellung (Erstellu...
Sam Sales der Boss (8man-demo\Sam.Sales)
Urai, Sam (8man-demo\Sam.Urai)

Start | Verwerfen

1. *Enter a title for the report and add a comment.*
2. *Define the range of the report. You are only able to add users where the manager attribute has been set and which have a valid Data Owner configuration.*
3. *Define the desired report settings.*
4. *Start the report.*

5.3.1.2 Who has access to what?

Background / Value

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

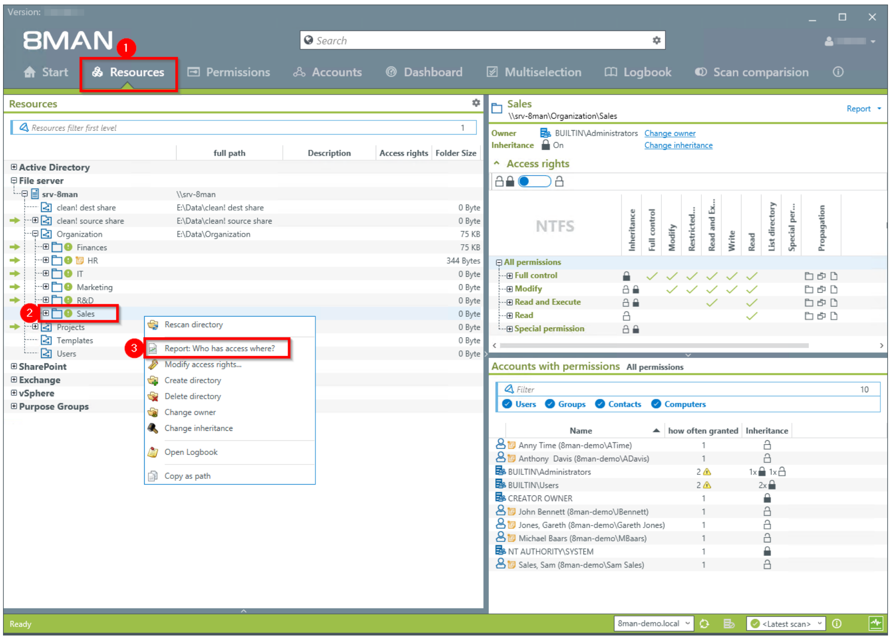
The report allows responsible managers to make information based decisions in order to answer two central questions:

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

Additional Services

Changing directory access rights

Step by step process



	full path	Description	Access rights	Folder Size
Active Directory				
File server				
srv-8man	\\srv-8man			
clean! dest share	E:\Data\clean! dest share			0 Byte
clean! source share	E:\Data\clean! source share			0 Byte
Organization	E:\Data\Organization			75 KB
Finances				75 KB
HR				344 Bytes
IT				0 Byte
Marketing				0 Byte
R&D				0 Byte
Sales				0 Byte
Projects				0 Byte
Templates				0 Byte
Users				0 Byte
SharePoint				
Exchange				
vSphere				
Purpose Groups				

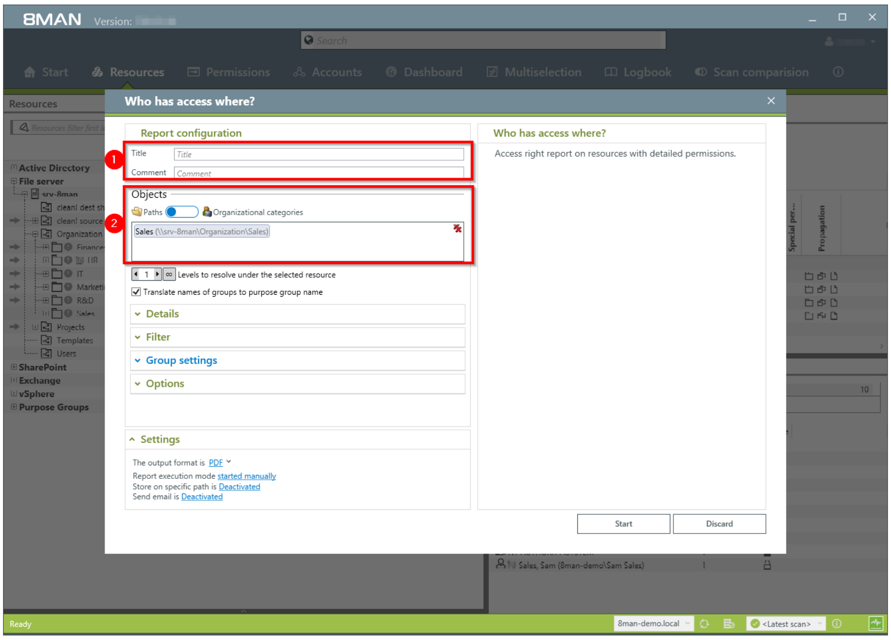
Sales
\\srv-8man\Organization\Sales

Owner BUILTIN\Administrators
Inheritance On

NTFS	Inheritance	Full control	Modify	Restricted...	Read and Ex...	Write	Read	List directory	Special per...	Propagation
All permissions										
Full control	🔒	✓	✓	✓	✓	✓	✓			
Modify	🔓 🔒		✓	✓	✓	✓	✓			
Read and Execute	🔓 🔒				✓		✓			
Read	🔓						✓			
Special permission	🔓 🔒									

Name	how often granted	Inheritance
Anny Time (8man-demo\ATime)	1	🔓
Anthony Davis (8man-demo\ADavis)	1	🔓
BUILTIN\Administrators	2 ⚠	1x🔒 1x🔓
BUILTIN\Users	2 ⚠	2x🔒
CREATOR OWNER	1	🔒
John Bennett (8man-demo\JBennett)	1	🔓
Jones, Gareth (8man-demo\Gareth Jones)	1	🔓
Michael Baars (8man-demo\MBaars)	1	🔓
NT AUTHORITY\SYSTEM	1	🔒
Sales, Sam (8man-demo\Sam Sales)	1	🔓

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.*



Who has access where?

Report configuration

Title: Title

Comment: Comment

Objects

Paths ● Organizational categories

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

1 ∞ Levels to resolve under the selected resource

☑ Translate names of groups to purpose group name

- Details
- Filter
- Group settings
- Options

Settings

The output format is PDF

Report execution mode started manually

Store on specific path is Deactivated

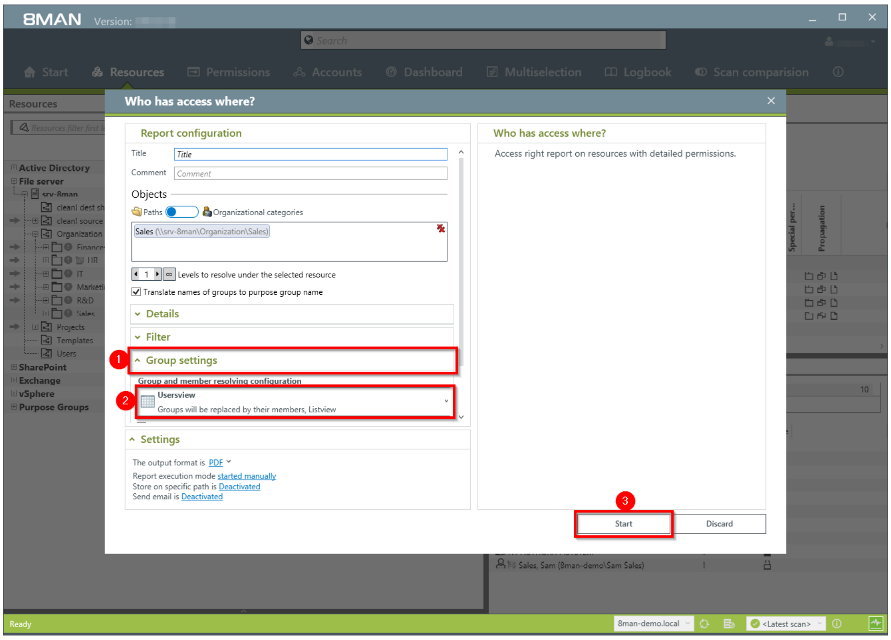
Send email is Deactivated

Who has access where?

Access right report on resources with detailed permissions.

Start | Discard

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.



Who has access where?

Report configuration

Title: Title

Comment: Comment

Objects

Paths ● Organizational categories

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

1 ∞ Levels to resolve under the selected resource

☑ Translate names of groups to purpose group name

- Details
- Filter
- Group settings

Group and member resolving configuration

Usersview
Groups will be replaced by their members, Listview

Settings

The output format is PDF

Report execution mode started manually

Store on specific path is Deactivated

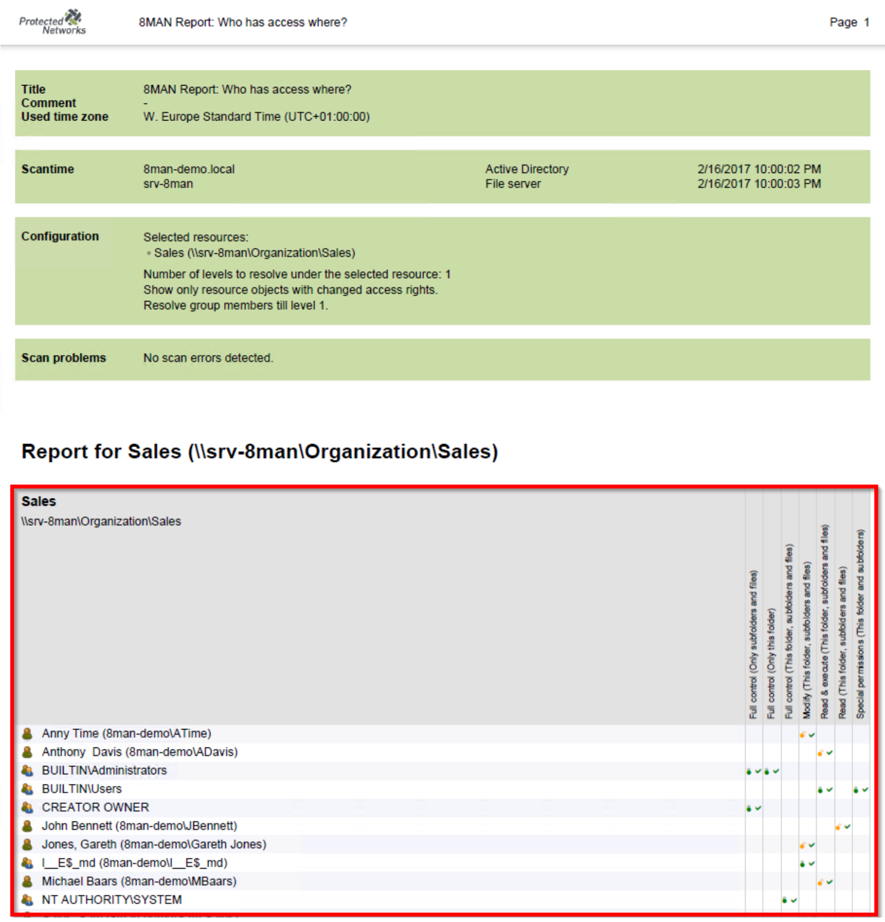
Send email is Deactivated

Who has access where?

Access right report on resources with detailed permissions.

Start | Discard

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.



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.		

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

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

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.

5.3.2 Reports for Administrators

5.3.2.1 Identifying usage of "everyone"

Background / Value

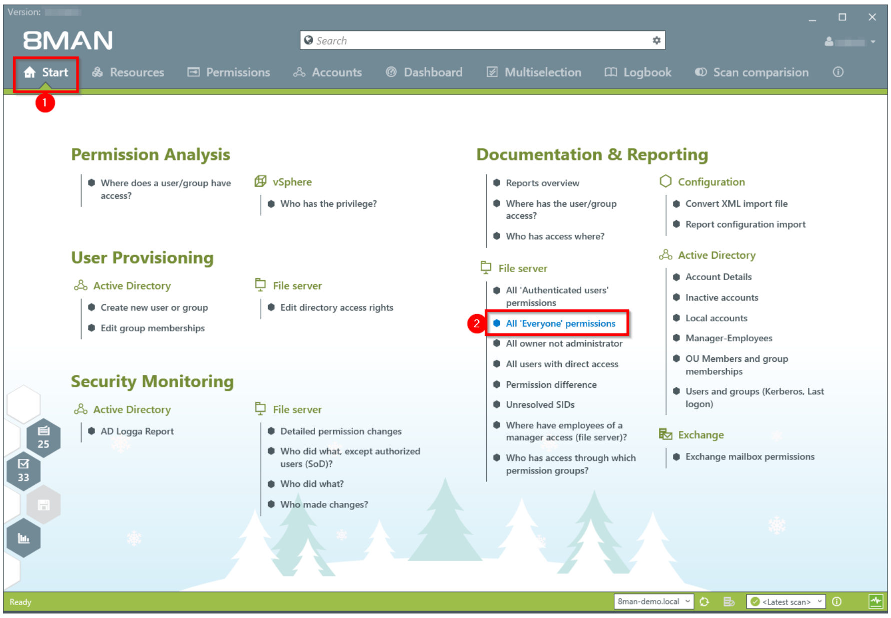
If the "Everyone" account is used for the assignment of access rights, (almost) everyone has access to the connected resources. The consequence is an excessive assignment of access rights and a high probability for unauthorized access. 8MAN displays all access rights for the "Everyone" account. These go against the principle of least privilege and should therefore not be used. Removing the "Everyone" account automatically is not possible. Before manually deleting accounts you should assign groups to the appropriate resources. Afterwards you can add the desired members to the group.

Additional services

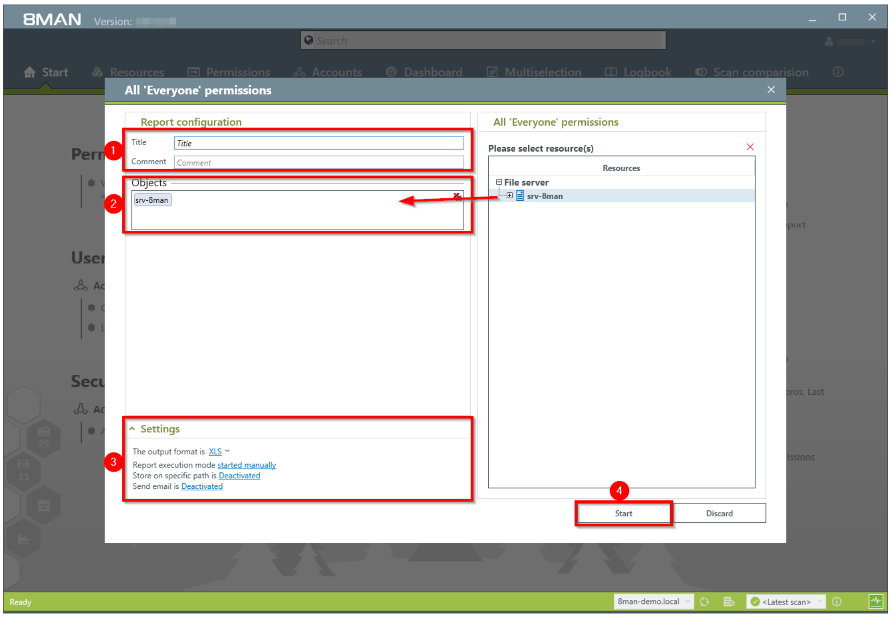
Also keep an eye on the critical Authenticated Users.

Removing permissions from globally accessible directories in bulk

Step by step process



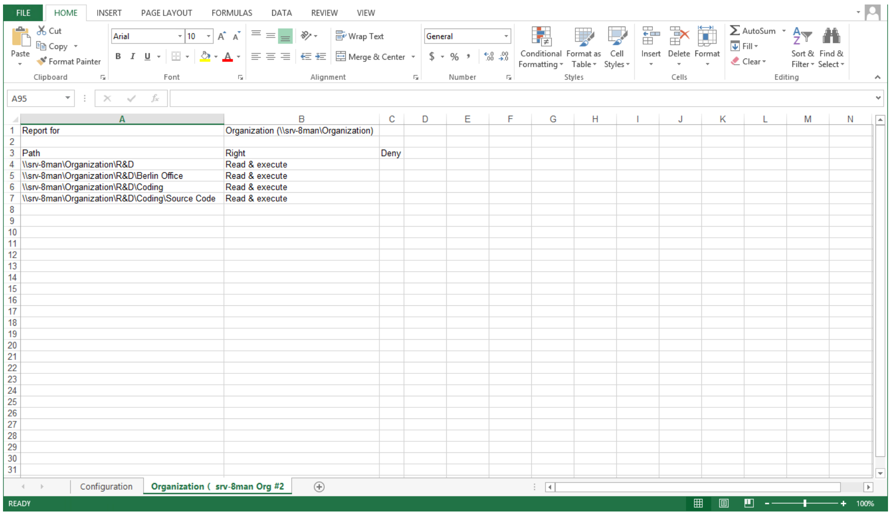
1. Select "Start".
2. Click on "All 'Everyone' permissions".



Title: Title
Comment: Comment

The output format is XLS
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

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.



	A	B	C
1	Report for	Organization (\\srv-8man\Organization)	
2			
3	Path	Right	Deny
4	\\srv-8man\Organization\R&D	Read & execute	
5	\\srv-8man\Organization\R&D\Berlin Office	Read & execute	
6	\\srv-8man\Organization\R&D\Coding	Read & execute	
7	\\srv-8man\Organization\R&D\Coding\Source Code	Read & execute	

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

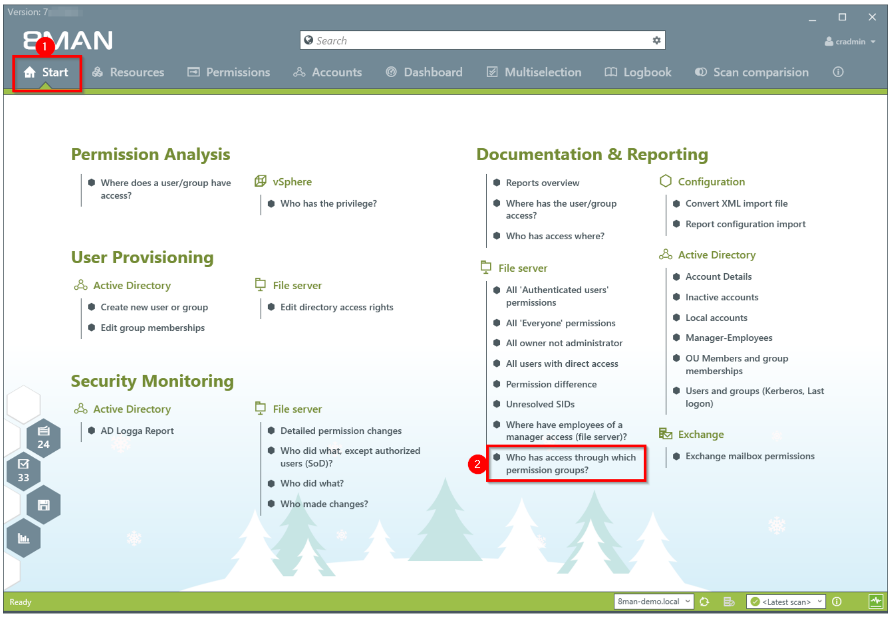
5.3.2.2 Wer kann wo über welche Berechtigungsgruppen zugreifen?

Background / Value

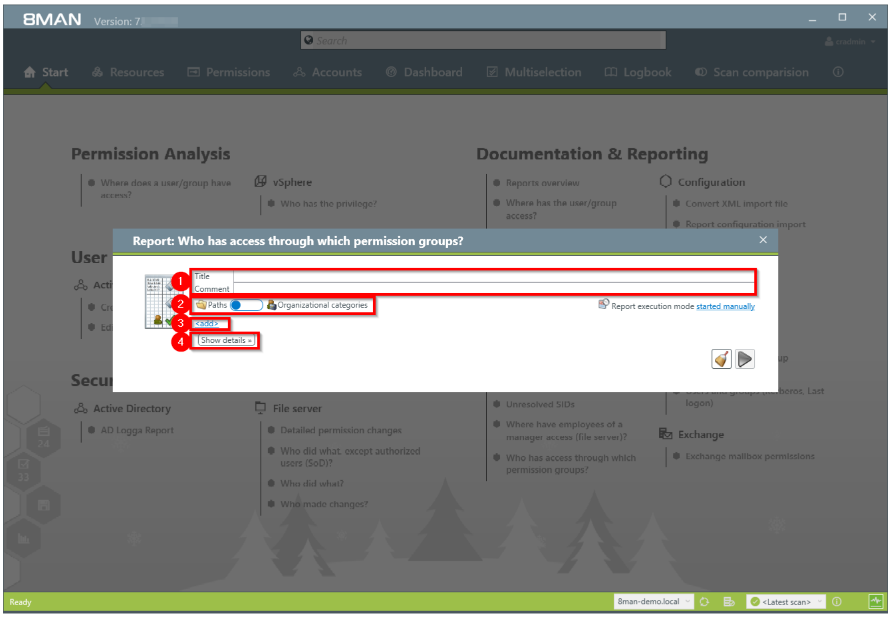
The report "Who has access through which permission groups?" shows the groups that give access to the selected resource and the users that are members of said groups.

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

Step by step process



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



Report: Who has access through which permission groups?

1 Title

Comment

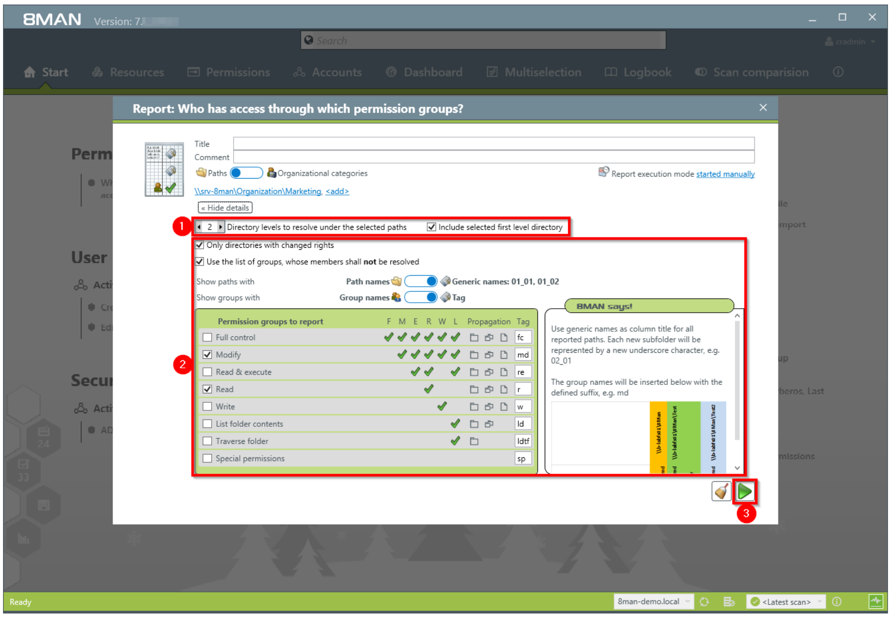
2 Paths ○ Organizational categories

Report execution mode started manually

3 <add>

4 Show details »

1. *Enter a title for the report and add a comment.*
2. *Define whether the report is organized by individual directories or by organizational categories from the Data Owner configuration.*
3. *Define the range of the report.*
4. *Click on "Show details".*



Report: Who has access through which permission groups?

Title

Comment

Paths ○ Organizational categories

Report execution mode started manually

\\srv-8man\Organization\Marketing, <add>

« Hide details

◂ 2 ▸ Directory levels to resolve under the selected paths ☑ Include selected first level directory

☑ Only directories with changed rights

☑ Use the list of groups, whose members shall **not** be resolved

Show paths with Path names ● Generic names: 01_01, 01_02

Show groups with Group names ● Tag

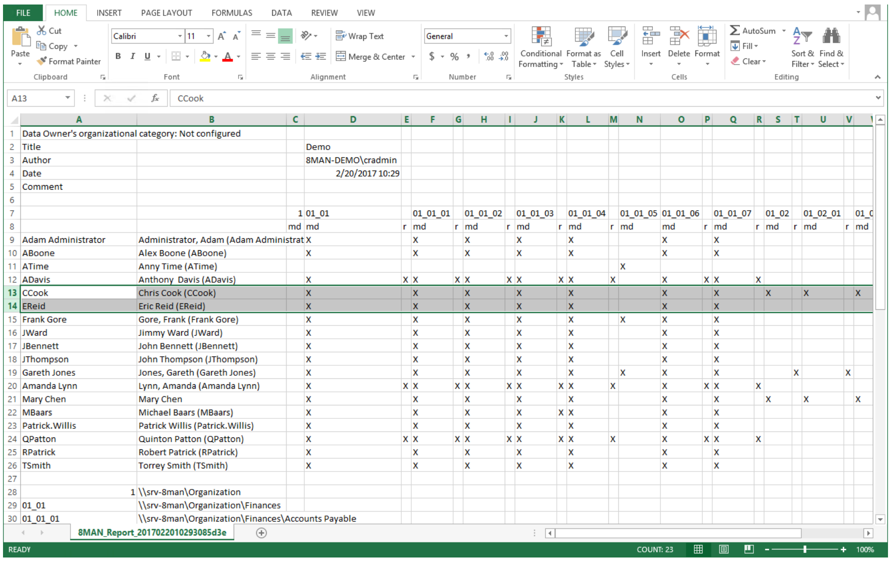
Permission groups to report	F	M	E	R	W	L	Propagation	Tag
□ Full control	✓	✓	✓	✓	✓	✓	🗀 🗗 🗋	fc
☑ Modify		✓	✓	✓	✓	✓	🗀 🗗 🗋	md
□ Read & execute			✓	✓		✓	🗀 🗗 🗋	re
☑ Read				✓			🗀 🗗 🗋	r
□ Write					✓		🗀 🗗 🗋	w
□ List folder contents						✓	🗀 🗗	ld
□ Traverse folder						✓	🗀	ldtf
□ Special permissions								sp

8MAN says!

Use generic names as column title for all reported paths. Each new subfolder will be represented by a new underscore character, e.g. 02_01

The group names will be inserted below with the defined suffix, e.g. md

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.*



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
1	Data Owner's organizational category: Not configured																						
2	Title			Demo																			
3	Author			8MAN-DEMO\cradmin																			
4	Date			2/20/2017 10:29																			
5	Comment																						
6																							
7			1	01_01		01_01_01		01_01_02		01_01_03		01_01_04		01_01_05	01_01_06		01_01_07		01_02		01_02_01		01_0
8			md	md	r	md	r	md	r	md	r	md	r	md	md	r	md	r	md	r	md	r	md
9	Adam Administrator	Administrator, Adam (Adam Administrat		X		X		X		X		X			X		X						
10	ABoone	Alex Boone (ABoone)		X		X		X		X		X			X		X						
11	ATime	Anny Time (ATime)												X									
12	ADavis	Anthony Davis (ADavis)		X	X	X	X	X	X	X	X	X	X		X	X	X	X					
13	CCook	Chris Cook (CCook)		X		X		X		X		X			X		X		X		X		X
14	EReid	Eric Reid (EReid)		X		X		X		X		X			X		X						
15	Frank Gore	Gore, Frank (Frank Gore)		X		X		X		X		X		X	X		X						
16	JWard	Jimmy Ward (JWard)		X		X		X		X		X			X		X						
17	JBennett	John Bennett (JBennett)		X		X		X		X		X			X		X						
18	JThompson	John Thompson (JThompson)		X		X		X		X		X			X		X						
19	Gareth Jones	Jones, Gareth (Gareth Jones)		X		X		X		X		X		X	X		X			X		X	
20	Amanda Lynn	Lynn, Amanda (Amanda Lynn)		X	X	X	X	X	X	X	X	X	X		X	X	X	X					
21	Mary Chen	Mary Chen		X		X		X		X		X			X		X		X		X		X
22	MBaars	Michael Baars (MBaars)		X		X		X		X	X	X			X		X						
23	Patrick.Willis	Patrick Willis (Patrick.Willis)		X		X		X		X		X			X		X						
24	QPatton	Quinton Patton (QPatton)		X	X	X	X	X	X	X	X	X	X		X	X	X	X					
25	RPatrick	Robert Patrick (RPatrick)		X		X		X		X		X			X		X						
26	TSmith	Torrey Smith (TSmith)		X		X		X		X		X			X		X						
27																							
28	1	\\srv-8man\Organization																					
29	01_01	\\srv-8man\Organization\Finances																					
30	01_01_01	\\srv-8man\Organization\Finances\Accounts Payable																					

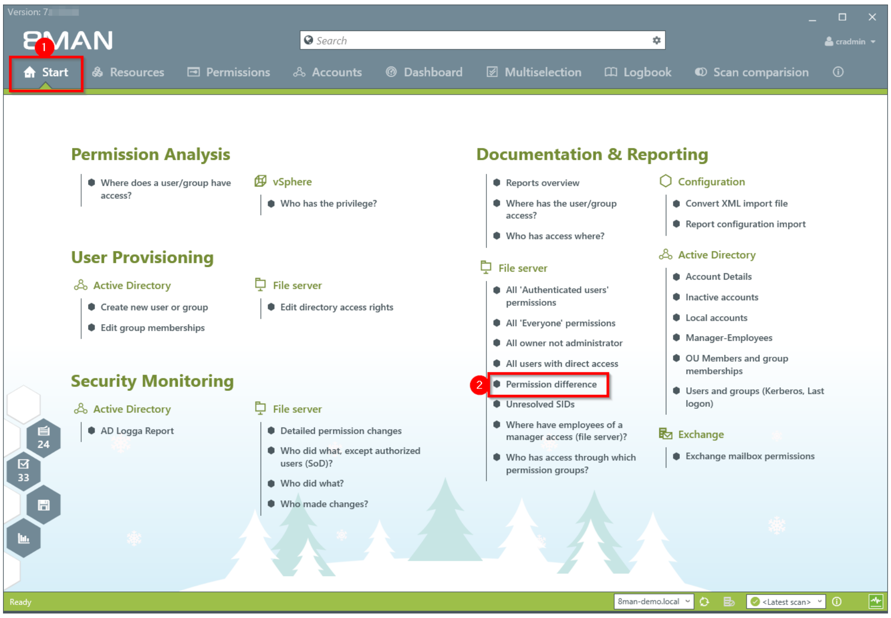
The report contains a list of all user accounts and file server paths, as well as the corresponding access rights groups.

5.3.2.3 Berechtigungsdifferenz-Report

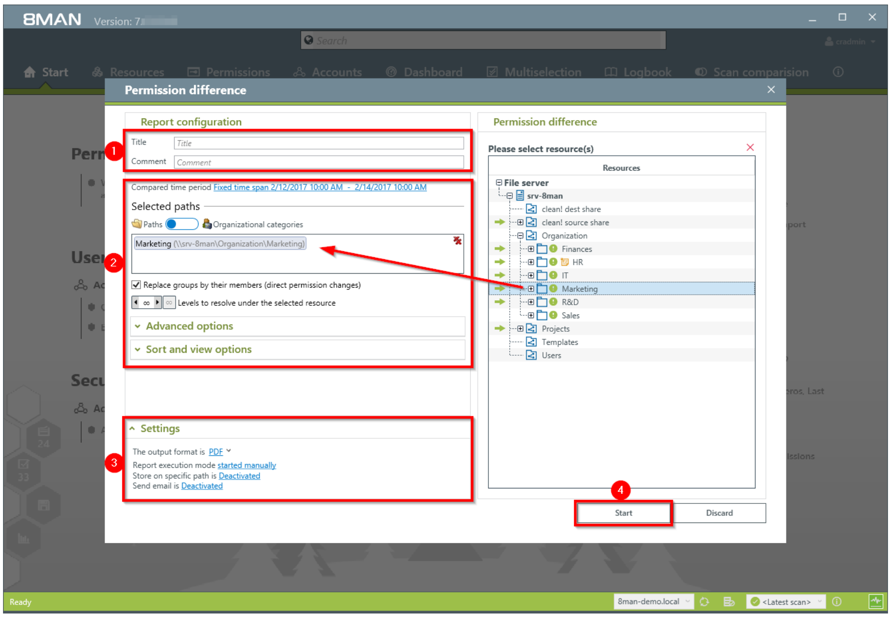
Background / Value

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

Step by step process



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



Title: Title
Comment: Comment
Compared time period Fixed time span 2/12/2017 10:00 AM - 2/14/2017 10:00 AM
Selected paths
Paths ○ Organizational categories
Marketing (\\srv-8man\Organization\Marketing)
☑ Replace groups by their members (direct permission changes)
∞ Levels to resolve under the selected resource

Settings
The output format is PDF
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

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 Identifying 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.

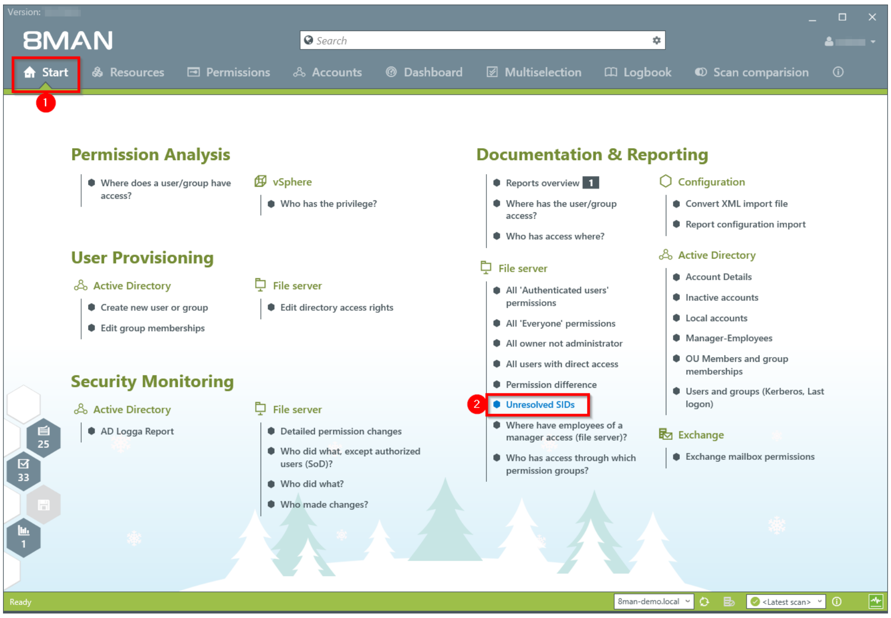
8MAN clearly identifies unresolved SIDs in your system.

Additional Services

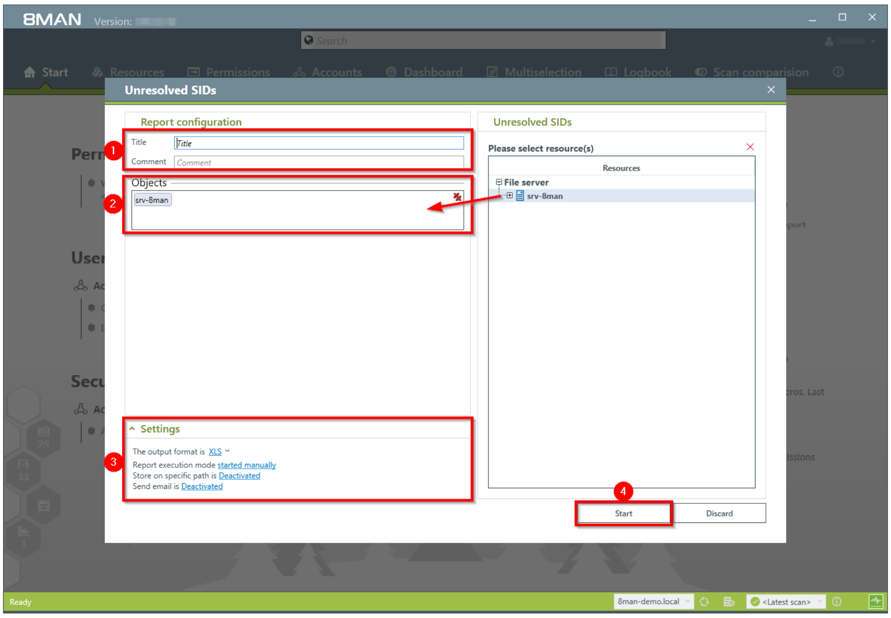
Identifying and deleting unresolved SIDs (using the rich client)

Removing unresolved SIDs in bulk (using the web client)

Step by step process

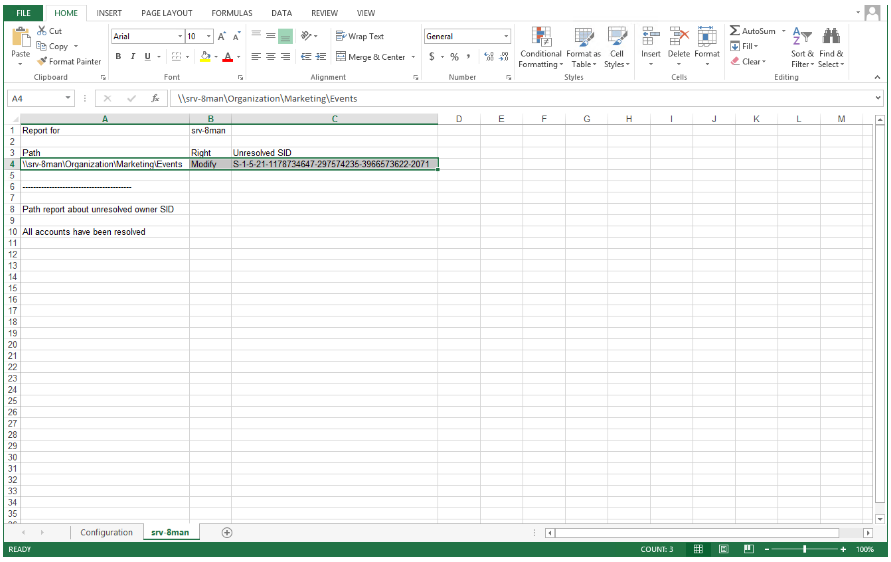


1. Select "Start".
2. Click on "Unresolved SIDs".



The output format is XLS
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

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.



\\srv-8man\Organization\Marketing\Events

	A	B	C
1	Report for	srv-8man	
2			
3	Path	Right	Unresolved SID
4	\\srv-8man\Organization\Marketing\Events	Modify	S-1-5-21-1178734647-297574235-3966573622-2071
5			
6	--		
7			
8	Path report about unresolved owner SID		
9			
10	All accounts have been resolved		

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

5.3.2.5 Identifying users with direct access

Background / Value

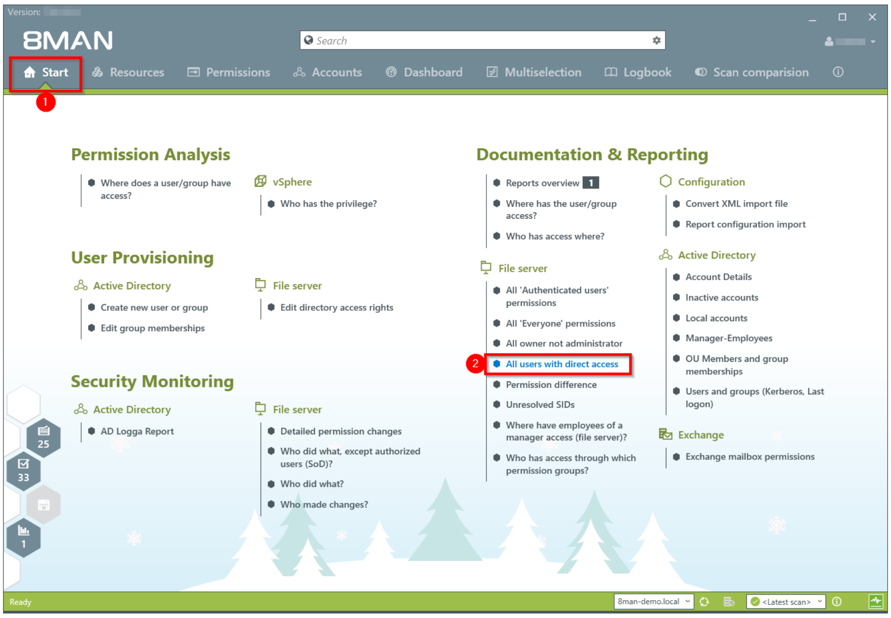
Direct access rights should be avoided at all costs and be replaced by group access rights. Firstly, direct access rights are inefficient because every user has to be managed independently. Secondly, each directory needs to be examined individually to ensure the removal of all direct access rights. 8MAN shows you all direct access rights on your file server(s) in one simple report.

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

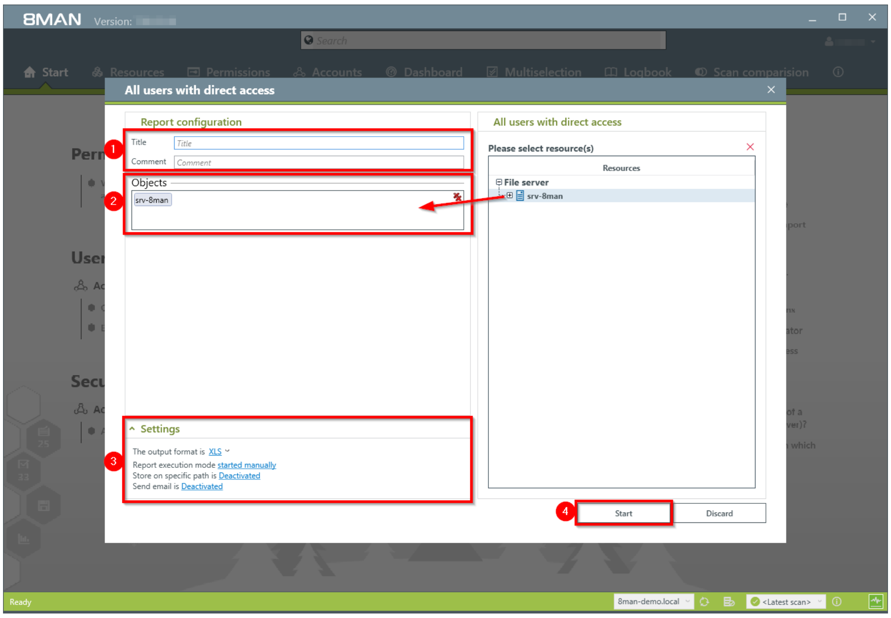
Additional Services

Removing direct access rights (using the rich client)

Step by step process



1. *Select "Start".*
2. *Click on "All users with direct access".*



All users with direct access

Report configuration

Title: Title

Comment: Comment

Objects: srv-8man

Settings

The output format is XLS

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

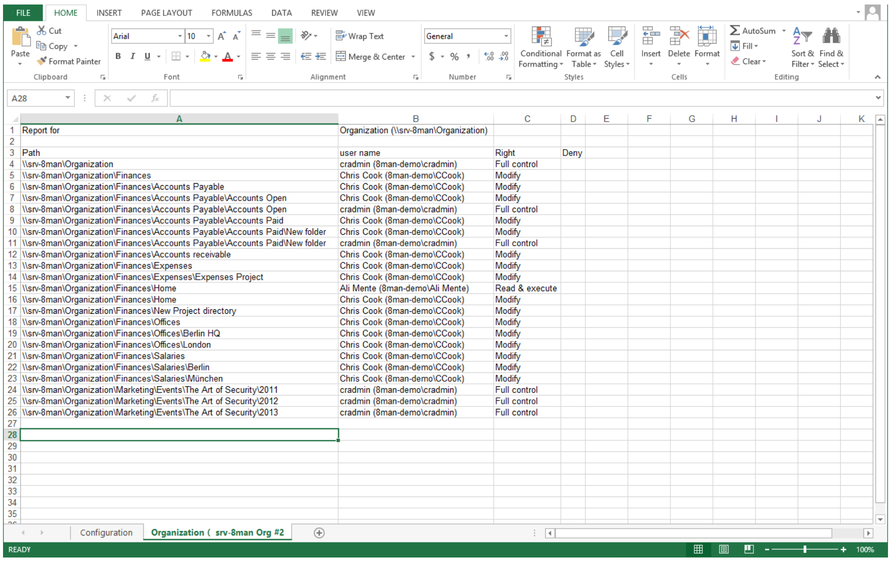
All users with direct access

Please select resource(s)

Resources

- File server
  - srv-8man

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.*



	A	B	C	D
1	Report for	Organization (\\srv-8man\Organization)		
2				
3	Path	user name	Right	Deny
4	\\srv-8man\Organization	cradmin (8man-demo\cradmin)	Full control	
5	\\srv-8man\Organization\Finances	Chris Cook (8man-demo\CCook)	Modify	
6	\\srv-8man\Organization\Finances\Accounts Payable	Chris Cook (8man-demo\CCook)	Modify	
7	\\srv-8man\Organization\Finances\Accounts Payable\Accounts Open	Chris Cook (8man-demo\CCook)	Modify	
8	\\srv-8man\Organization\Finances\Accounts Payable\Accounts Open	cradmin (8man-demo\cradmin)	Full control	
9	\\srv-8man\Organization\Finances\Accounts Payable\Accounts Paid	Chris Cook (8man-demo\CCook)	Modify	
10	\\srv-8man\Organization\Finances\Accounts Payable\Accounts Paid\New folder	Chris Cook (8man-demo\CCook)	Modify	
11	\\srv-8man\Organization\Finances\Accounts Payable\Accounts Paid\New folder	cradmin (8man-demo\cradmin)	Full control	
12	\\srv-8man\Organization\Finances\Accounts receivable	Chris Cook (8man-demo\CCook)	Modify	
13	\\srv-8man\Organization\Finances\Expenses	Chris Cook (8man-demo\CCook)	Modify	
14	\\srv-8man\Organization\Finances\Expenses\Expenses Project	Chris Cook (8man-demo\CCook)	Modify	
15	\\srv-8man\Organization\Finances\Home	Ali Mente (8man-demo\Ali Mente)	Read & execute	
16	\\srv-8man\Organization\Finances\Home	Chris Cook (8man-demo\CCook)	Modify	
17	\\srv-8man\Organization\Finances\New Project directory	Chris Cook (8man-demo\CCook)	Modify	
18	\\srv-8man\Organization\Finances\Offices	Chris Cook (8man-demo\CCook)	Modify	
19	\\srv-8man\Organization\Finances\Offices\Berlin HQ	Chris Cook (8man-demo\CCook)	Modify	
20	\\srv-8man\Organization\Finances\Offices\London	Chris Cook (8man-demo\CCook)	Modify	
21	\\srv-8man\Organization\Finances\Salaries	Chris Cook (8man-demo\CCook)	Modify	
22	\\srv-8man\Organization\Finances\Salaries\Berlin	Chris Cook (8man-demo\CCook)	Modify	
23	\\srv-8man\Organization\Finances\Salaries\München	Chris Cook (8man-demo\CCook)	Modify	
24	\\srv-8man\Organization\Marketing\Events\The Art of Security\2011	cradmin (8man-demo\cradmin)	Full control	
25	\\srv-8man\Organization\Marketing\Events\The Art of Security\2012	cradmin (8man-demo\cradmin)	Full control	
26	\\srv-8man\Organization\Marketing\Events\The Art of Security\2013	cradmin (8man-demo\cradmin)	Full control	

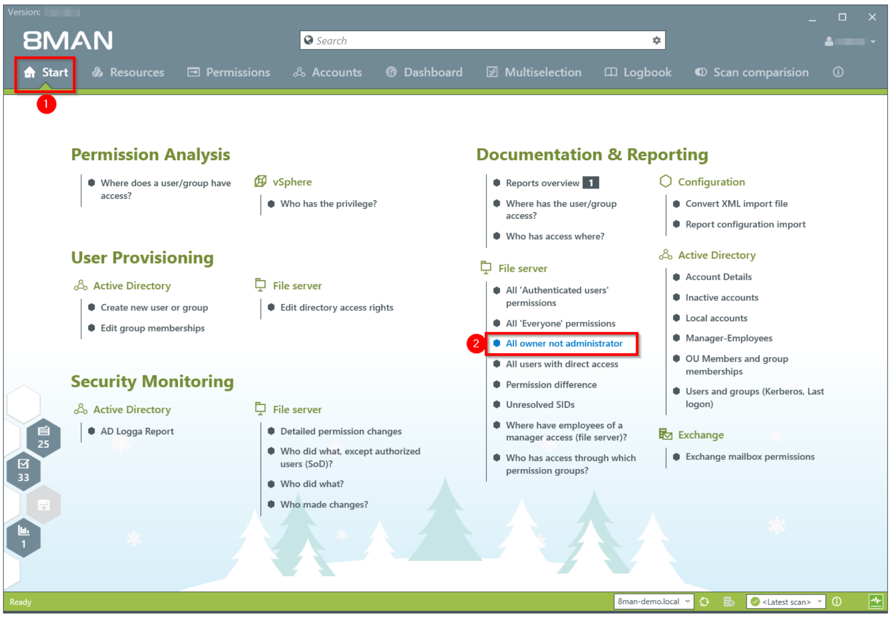
Open the report in Excel. 8MAN lists all directories with direct access rights.

5.3.2.6 Verzeichnisse identifizieren, deren Besitzer nicht Administratoren sind

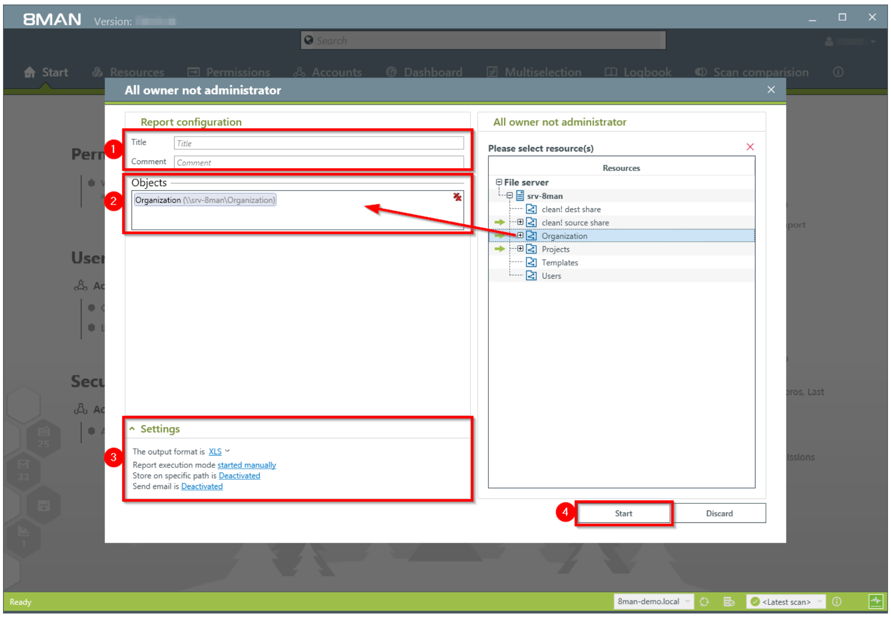
Background / Value

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.

Step by step process



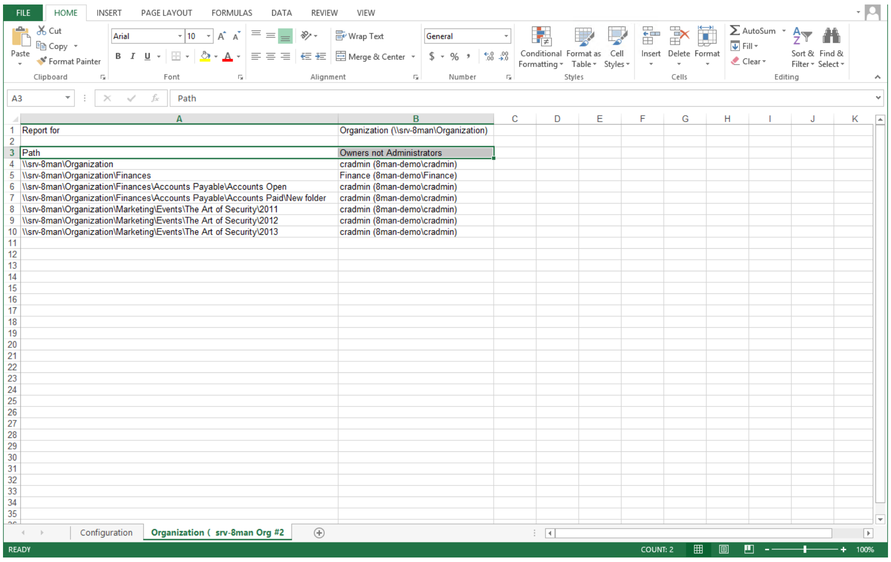
1. *Select "Start".*
2. *Click on "All owner not administrator".*



Organization (\\srv-8man\Organization)

The output format is XLS
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

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



	A	B
1	Report for	Organization (\\srv-8man\Organization)
2		
3	Path	Owners not Administrators
4	\\srv-8man\Organization	cradmin (8man-demo\cradmin)
5	\\srv-8man\Organization\Finances	Finance (8man-demo\Finance)
6	\\srv-8man\Organization\Finances\Accounts Payable\Accounts Open	cradmin (8man-demo\cradmin)
7	\\srv-8man\Organization\Finances\Accounts Payable\Accounts Paid\New folder	cradmin (8man-demo\cradmin)
8	\\srv-8man\Organization\Marketing\Events\The Art of Security\2011	cradmin (8man-demo\cradmin)
9	\\srv-8man\Organization\Marketing\Events\The Art of Security\2012	cradmin (8man-demo\cradmin)
10	\\srv-8man\Organization\Marketing\Events\The Art of Security\2013	cradmin (8man-demo\cradmin)

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

5.3.2.7 Das Konto "Authentifizierte Benutzer" auf Berechtigungen prüfen

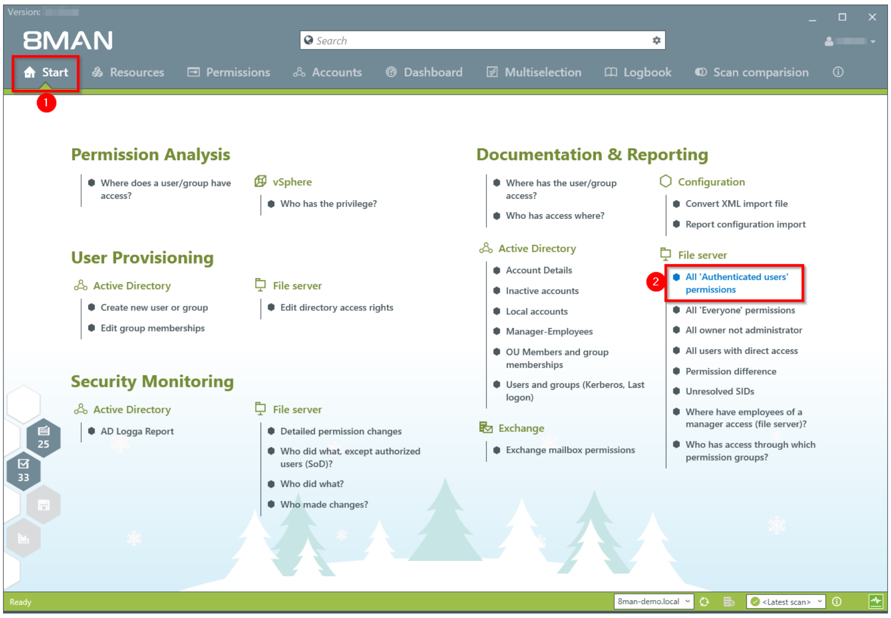
Background / Value

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".

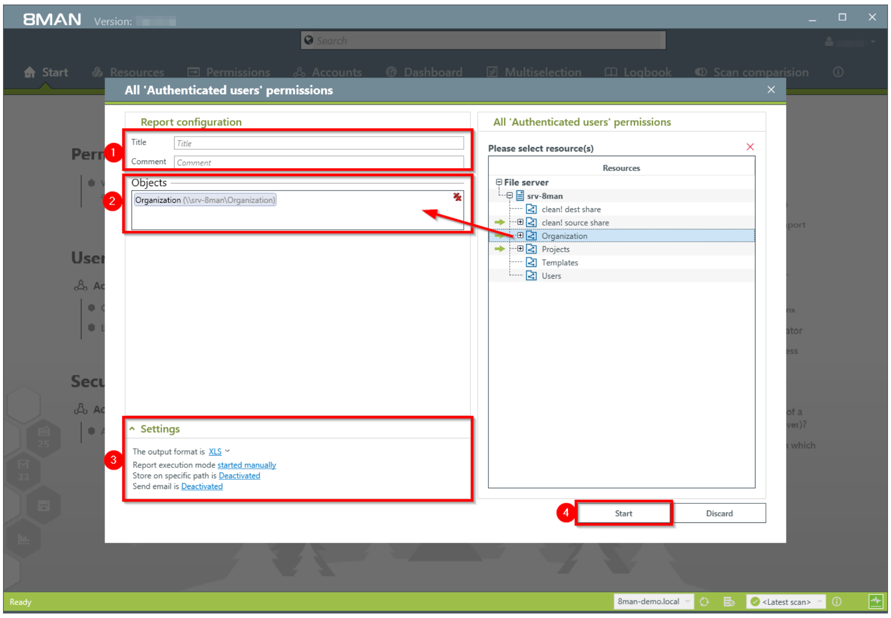
Additional Services

Identifying usage of "everyone"

Step by step process



1. *Select "Start".*
2. *Click on "All 'Authenticated Users' permissions".*



Title: Title

Comment: Comment

Objects

Organization (\\srv-8man\Organization)

Settings

The output format is XLS

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

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

2. Define the range of the report.

3. Define the desired report settings.

4. Start the report.

5.4 +8MATE for Exchange

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

Report: Who has access to what?

Report: Identifying Mailbox access rights

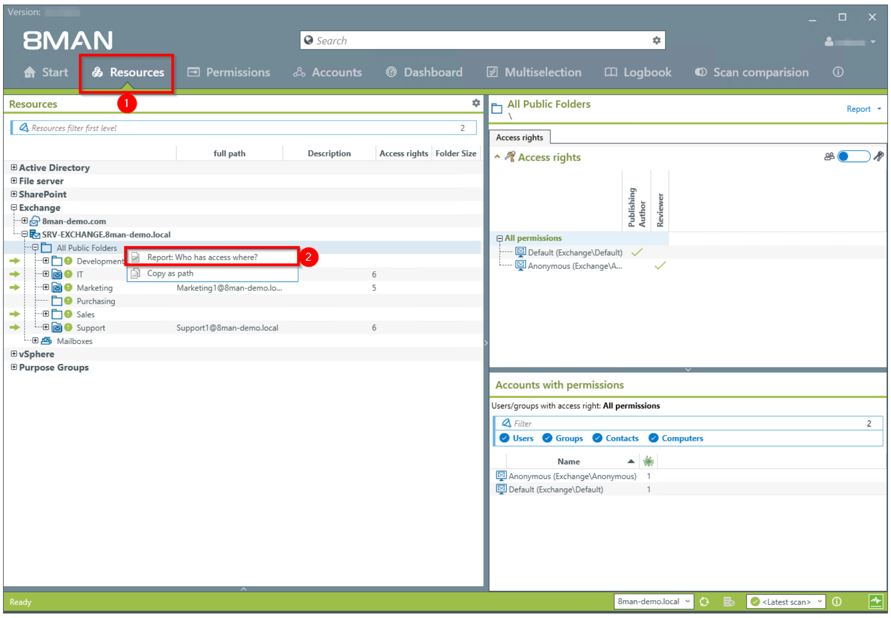
5.4.1 Management Reports

5.4.1.1 Who has access to what?

Background / Value

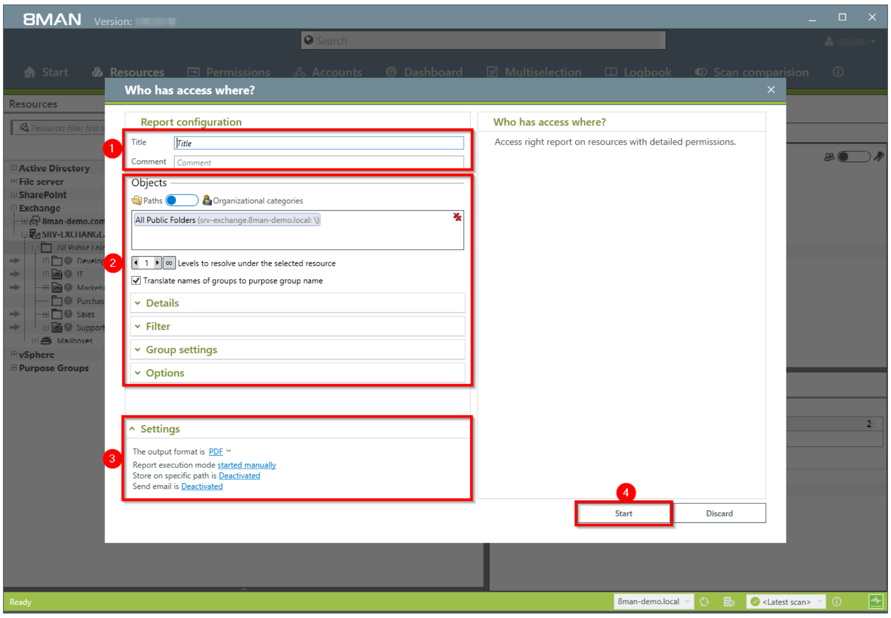
Managers and team leads know best who should have access to what. Having an understanding of your access rights situation is extremely important, especially for public Exchange folders and mailboxes. The report "who has access to what?" provides an overview of all users and their access to public folders. In addition 8MAN highlight the access right "send as", due to its potential risk.

Step by step process



1. Select "Resources".

2. Right click on any or all public folders. Select the report "Who has access where?" from the context menu.



Who has access where?

Report configuration

Title: *Title*

Comment: *Comment*

Objects

Paths / Organizational categories

All Public Folders (srv-exchange.8man-demo.local: \)

1 ∞ Levels to resolve under the selected resource

☑ Translate names of groups to purpose group name

- Details
- Filter
- Group settings
- Options

Settings

The output format is PDF

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

Who has access where?

Access right report on resources with detailed permissions.

Start | Discard

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 Identifying mailbox permissions

Background / Value

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

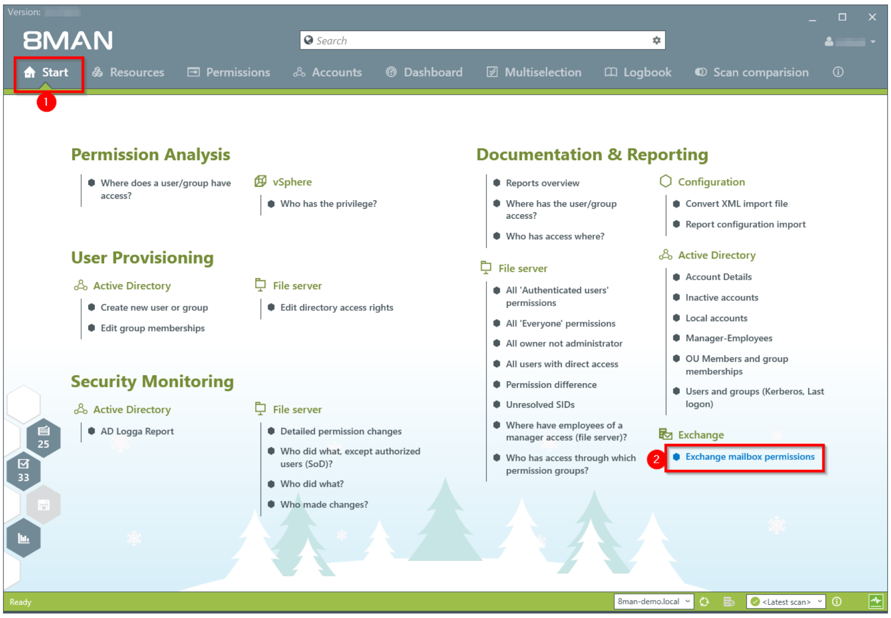
- Mailbox directories and their access rights
- Properties (Mailbox size)
- Deputies for Mailboxes
- Out of Office notices

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

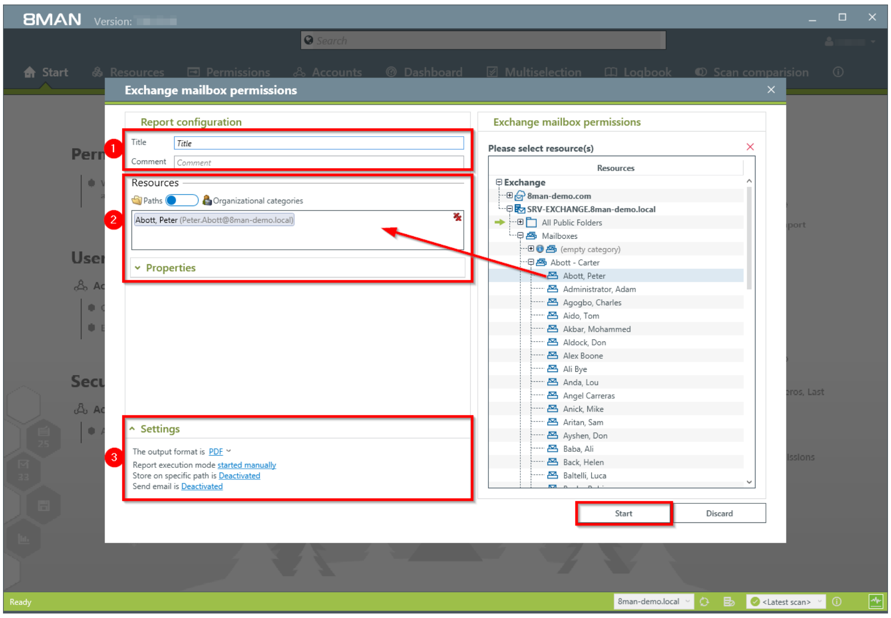
Additional Services

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

Step by step process



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



Title: Title
Comment: Comment

Abott, Peter (Peter.Abott@8man-demo.local)

The output format is PDF
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

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

5.5 +8MATE for Sharepoint

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

Report: Who has access to what?
Report: Where do users and groups have access?

5.5.1 Management Reports

5.5.1.1 Who has access where?

Background / Value

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

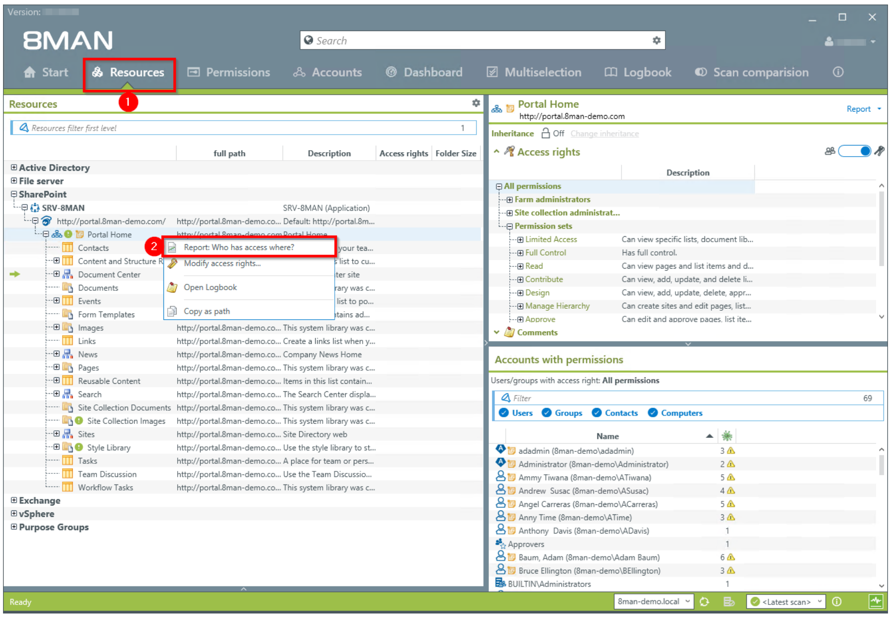
The report allows responsible managers to make information based decisions in order to answer two central questions:

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

Additional Services

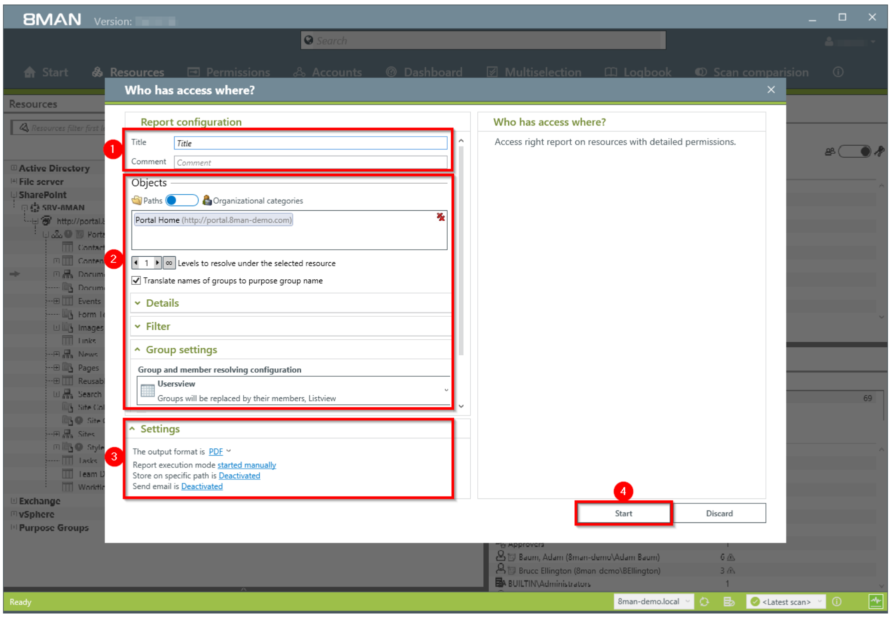
Managing access rights to SharePoint resources

Step by step process



1. Select "Resources".

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



Title: Title
Comment: Comment

Paths / Organizational categories
Portal Home (http://portal.8man-demo.com)
1 Levels to resolve under the selected resource
☑ Translate names of groups to purpose group name

Group and member resolving configuration
Usersview
Groups will be replaced by their members, Listview

The output format is PDF
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

Who has access where?
Access right report on resources with detailed permissions.

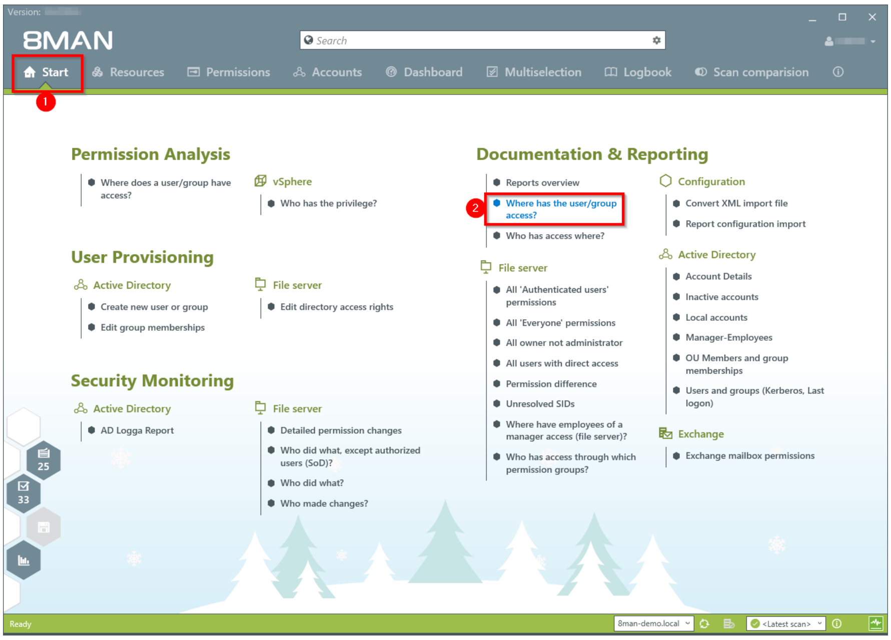
1. *Enter a title for the report and add a comment.*
2. *Define the range of the report. In order to reduce complexity, we recommend selecting "usersview" in the "Group settings" area. All other settings are targeted at expert users.*
3. *Define the desired report settings.*
4. *Start the report.*

5.5.1.2 Where do users and groups have access?

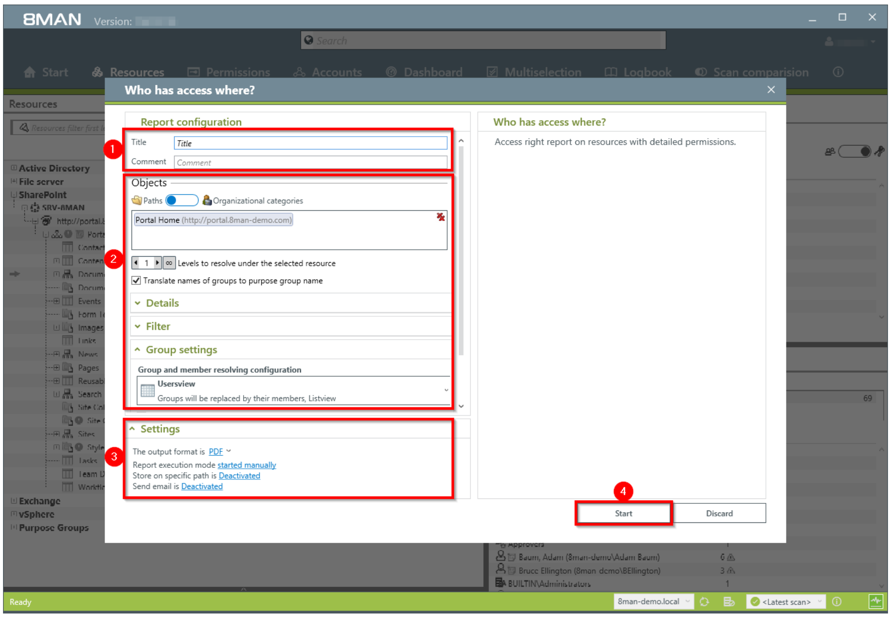
Background / Value

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

Step by step process



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



Who has access where?

Report configuration

Title: Title

Comment: Comment

Objects

Paths / Organizational categories

Portal Home (http://portal.8man-demo.com)

1 Levels to resolve under the selected resource

☑ Translate names of groups to purpose group name

Details

Filter

Group settings

Group and member resolving configuration

Usersview – Groups will be replaced by their members, Listview

Settings

The output format is PDF

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

Who has access where?

Access right report on resources with detailed permissions.

Start | Discard

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.

5.6 +8MATE: Analyze & Act

With Analyze & Act we combine services of Documentation & Reporting and User Provisioning. This includes flexible reports and bulk operations for user accounts and file server directories.
Analyze & Act is accessible via aweb client.

You can find the services in the following areas:

Documentation & Reporting

- All AD accounts
- Accounts with no password expire
- All groups in recursions
- Show directories to which all users have access

User Provisioning

Active Directory

- Deactivating Accounts in bulk
- Changing password options in bulk
- Resetting passwords in bulk
- Changing attributes in bulk
- Executing scripts on user accounts in bulk
- Executing scripts for directories in bulk

File server

- Executing scripts for directories in bulk

5.6.1 Flexible Reporting

Background / Value

With the 8MATE Analyze & Act you can create flexible reports. Initially the reports are based on the following scenarios:

- All AD accounts
- Accounts with no password expire
- All groups in recursions
- Show directories to which all users have access

The "flexible" part refers to the free choice of attributes to be displayed in the report.
E.G.:

- E-Mail
- Telephone number
- Company
- Department
- Description
- Account expiration date

Complementary Services

Once the report has been created you can trigger the following services:

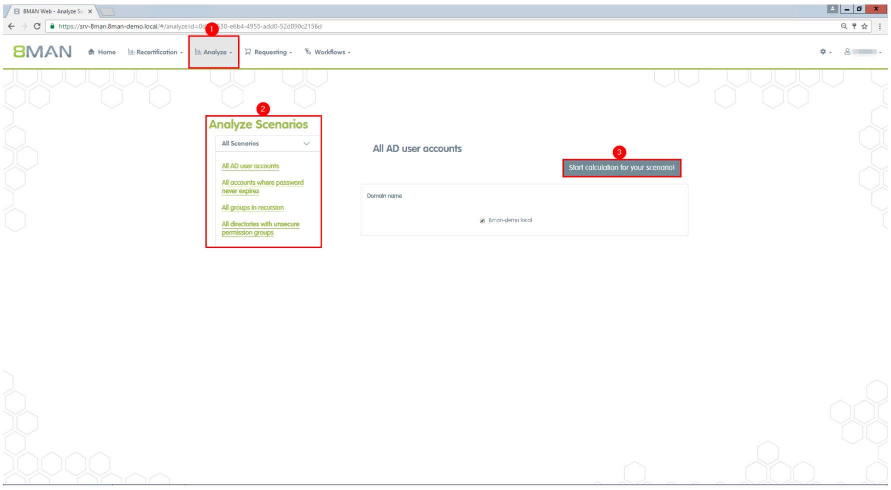
Active Directory

- Deactivate accounts in bulk
- Change password options in bulk
- Reset passwords in bulk
- Change attributes in bulk
- Execute scripts on user accounts in bulk

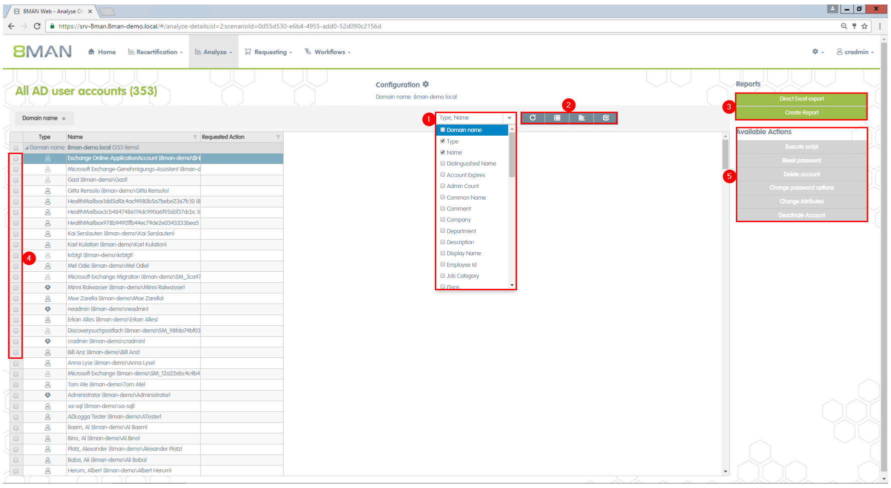
File server

- Execute scripts for directories in bulk

The process in single steps


8MAN Web - Analyse Sc
https://srv-8man.8man-demo.local/#/analyze;id=0d55d530-e6b4-4955-add0-52d090c2156d
8MAN
Home
Recertification
Analyze
Requesting
Workflows
1
2
Analyze Scenarios
All Scenarios
All AD user accounts
All accounts where password never expires
All groups in recursion
All directories with unsecure permission groups
All AD user accounts
3
Start calculation for your scenario!
Domain name
8man-demo.local

1. Click on „Analyze".
2. Pick a scenario.
3. Press "Start the calculation...".



	Type	Name	Requested Action
□	Domain name: 8man-demo.local (353 items)		
□		Exchange Online-ApplicationAccount (8man-demo\$H	
□		Microsoft Exchange-Genehmigungs-Assistent (8man-d	
□		Gast (8man-demo\Gast)	
□		Gitta Rensolo (8man-demo\Gitta Rensolo)	
□		HealthMailbox1dd5af0c4acf4980b5a7bebe2367fc10 (8	
□		HealthMailbox3cb4847486114dc990a6f956bf37dcbc (8	
□		HealthMailbox978b9492ffb44ec79de2e0343333bea5	
□		Kai Serslauten (8man-demo\Kai Serslauten)	
□		Karl Kulation (8man-demo\Karl Kulation)	
□		krbtgt (8man-demo\krbtgt)	
□		Mel Odie (8man-demo\Mel Odie)	
□		Microsoft Exchange Migration (8man-demo\SM_3ca47	
□		Minni Ralwasser (8man-demo\Minni Ralwasser)	
□		Moe Zarella (8man-demo\Moe Zarella)	
□		neadmin (8man-demo\neadmin)	
□		Erkan Alles (8man-demo\Erkan Alles)	
□		Discoverysuchpostfach (8man-demo\SM_98fda74bf03	
□		cradmin (8man-demo\cradmin)	
□		Bill Anz (8man-demo\Bill Anz)	
□		Anna Lyse (8man-demo\Anna Lyse)	
□		Microsoft Exchange (8man-demo\SM_12a22ebc4c4b4	
□		Tom Ate (8man-demo\Tom Ate)	
□		Administrator (8man-demo\Administrator)	
□		sa-sql (8man-demo\sa-sql)	
□		ADLogga Tester (8man-demo\ATester)	
□		Baern, Al (8man-demo\Al Baern)	
□		Bino, Al (8man-demo\Al.Bino)	
□		Platz, Alexander (8man-demo\Alexander Platz)	
□		Baba, Ali (8man-demo\Ali Baba)	
□		Herum, Albert (8man-demo\Albert Herum)	

In the example all AD accounts are shown.

1. You can use the dropdown-menu to choose the listed attributes.
2. You can also group, sort and filter the items.
3. Export the data into Excel or create an 8MAN report.

If you wish to execute bulk operations with any items,

4. activate the checkboxes and
5. chose an action in the "Available Actions" list.

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. This means that you run the risk of serious security risks without comprehensive monitoring.

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.

AD Logga helps you in the following ways

- 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.
- Management needs certainty. AD Logga provides this by capturing relevant internal security data and allows you to improve processes.

6.1.1.1 Monitoring changes to specific event types

Background / Value

The 8MATE AD Logga allows you to monitor current processes in your Active Directory. 8MAN even captures all changes made with native tools including temporary changes. From a security perspective any actions related to event types and event authors are extremely important.

Monitoring of event types

Changes to:

- Attributes
- Users
- Computers
- Groups
- Passwords
- Accounts
- Members

Monitoring of event authors

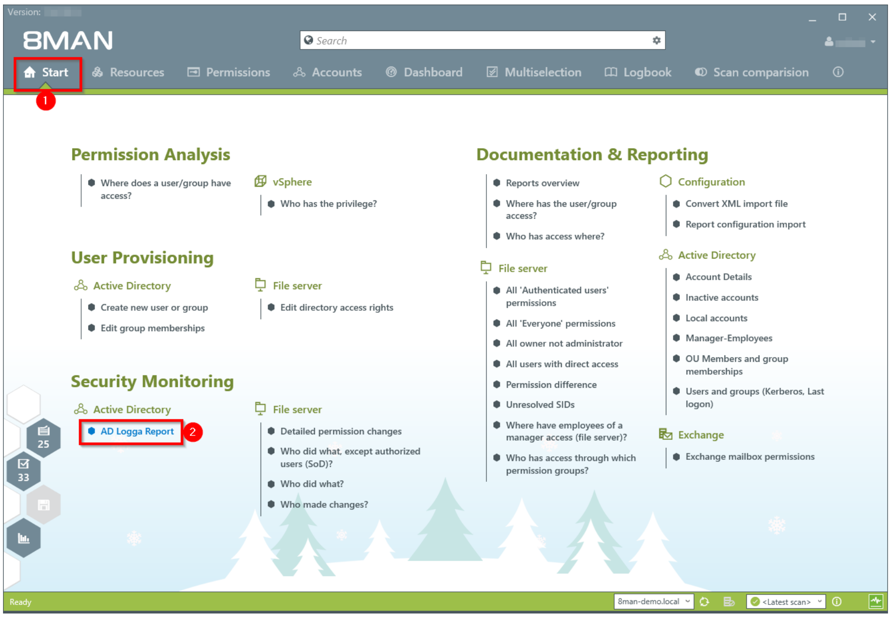
- User
- Group
- Computer

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.

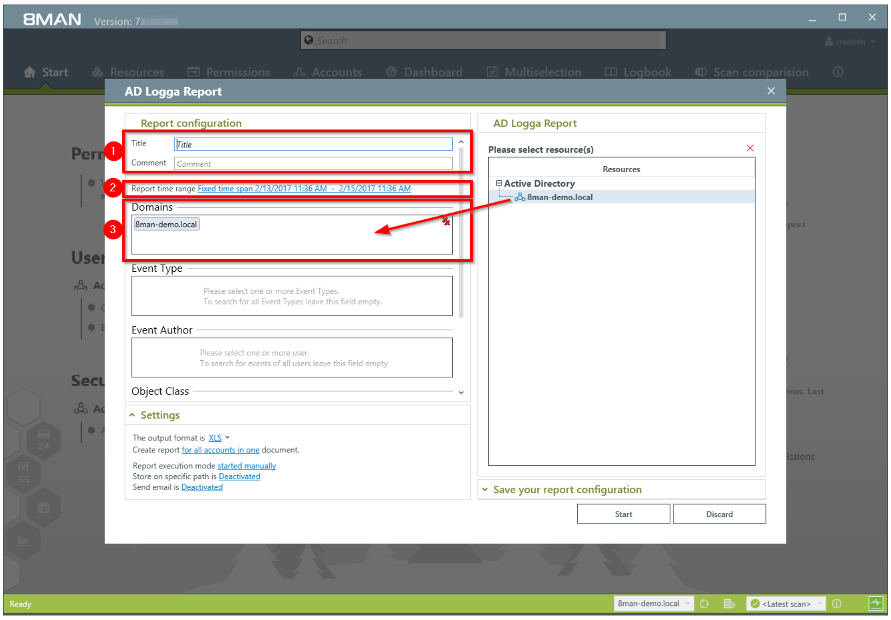
Additional services

Setting alerts for AD objects

Step by step process



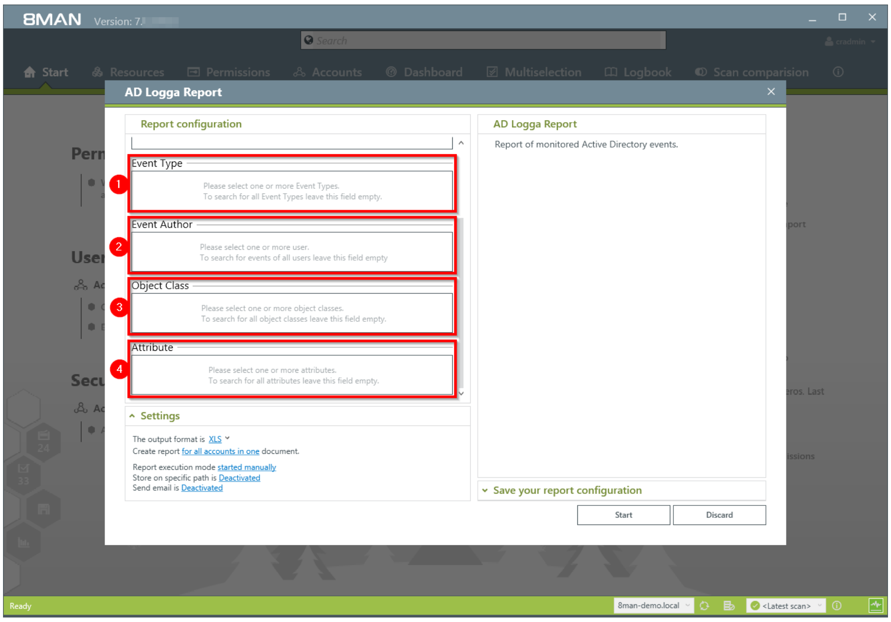
1. Select "Start".
2. Click on "AD Logga Report".



Title: Title
Comment: Comment
Report time range Fixed time span 2/13/2017 11:36 AM - 2/15/2017 11:36 AM
Domains: 8man-demo.local
Event Type: Please select one or more Event Types. To search for all Event Types leave this field empty.
Event Author: Please select one or more user. To search for events of all users leave this field empty

The output format is XLS
Create report for all accounts in one document.
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

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.



Event Type

Please select one or more Event Types.
To search for all Event Types leave this field empty.

Event Author

Please select one or more user.
To search for events of all users leave this field empty

Object Class

Please select one or more object classes.
To search for all object classes leave this field empty.

Attribute

Please select one or more attributes.
To search for all attributes leave this field empty.

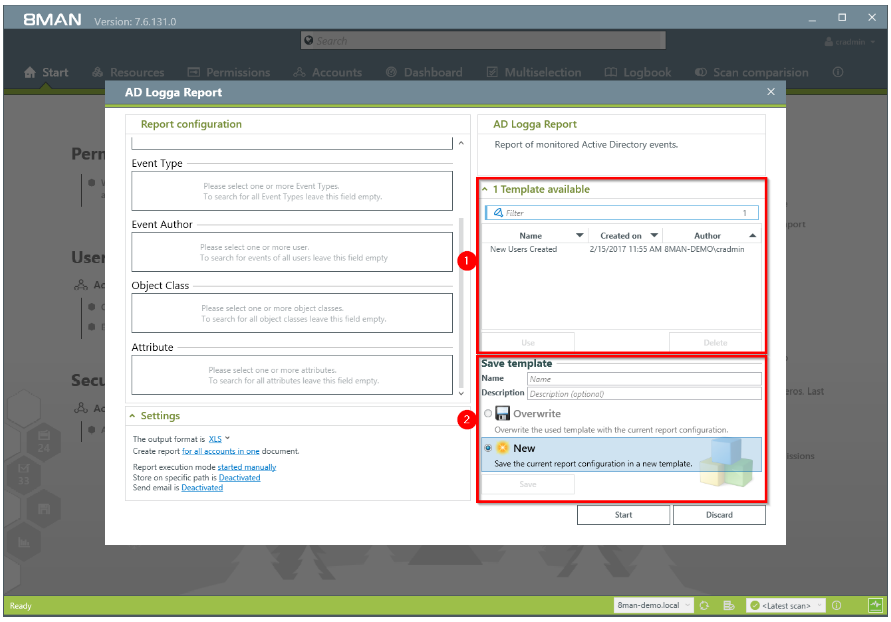
The output format is XLS
Create report for all accounts in one document.
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

AD Logga Report

Report of monitored Active Directory events.

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 reports 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.*



Event Type

Please select one or more Event Types.
To search for all Event Types leave this field empty.

Event Author

Please select one or more user.
To search for events of all users leave this field empty

Object Class

Please select one or more object classes.
To search for all object classes leave this field empty.

Attribute

Please select one or more attributes.
To search for all attributes leave this field empty.

The output format is XLS
Create report for all accounts in one document.
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

AD Logga Report

Report of monitored Active Directory events.

1 Template available

Name	Created on	Author
New Users Created	2/15/2017 11:55 AM	8MAN-DEMO\cradmin

Save template

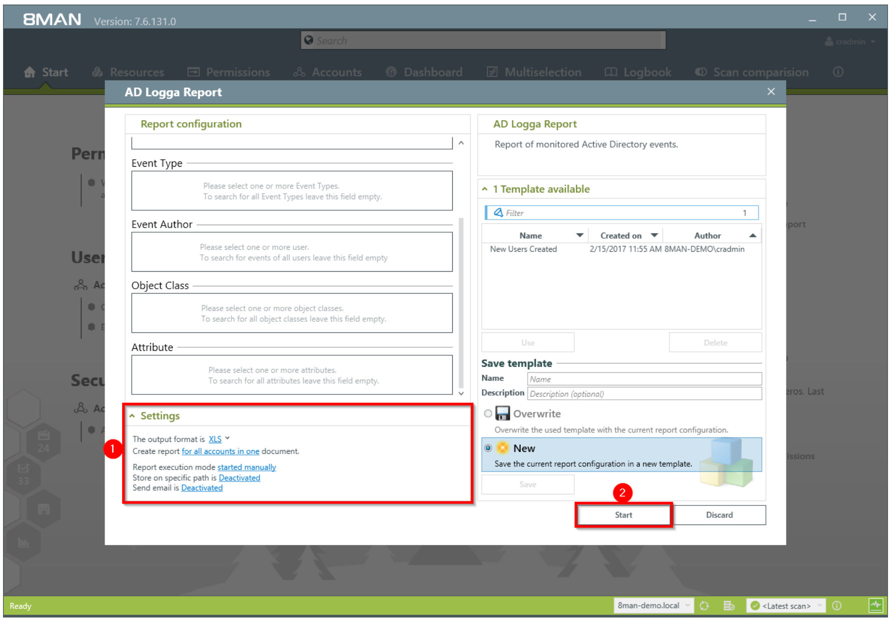
Name: Name
Description: Description (optional)

○ Overwrite
Overwrite the used template with the current report configuration.

● New
Save the current report configuration in a new template.

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.*



AD Logga Report

Report configuration

Event Type
Please select one or more Event Types.
To search for all Event Types leave this field empty.

Event Author
Please select one or more user.
To search for events of all users leave this field empty

Object Class
Please select one or more object classes.
To search for all object classes leave this field empty.

Attribute
Please select one or more attributes.
To search for all attributes leave this field empty.

Settings

The output format is XLS
Create report for all accounts in one document.
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

AD Logga Report

Report of monitored Active Directory events.

1 Template available

Filter 1

Name	Created on	Author
New Users Created	2/15/2017 11:55 AM	8MAN-DEMO\cradmin

Use | Delete

Save template
Name: Name
Description: Description (optional)

○ Overwrite
Overwrite the used template with the current report configuration.

● New
Save the current report configuration in a new template.

Save

Start | Discard

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

6.1.1.2 Identifying temporary group memberships

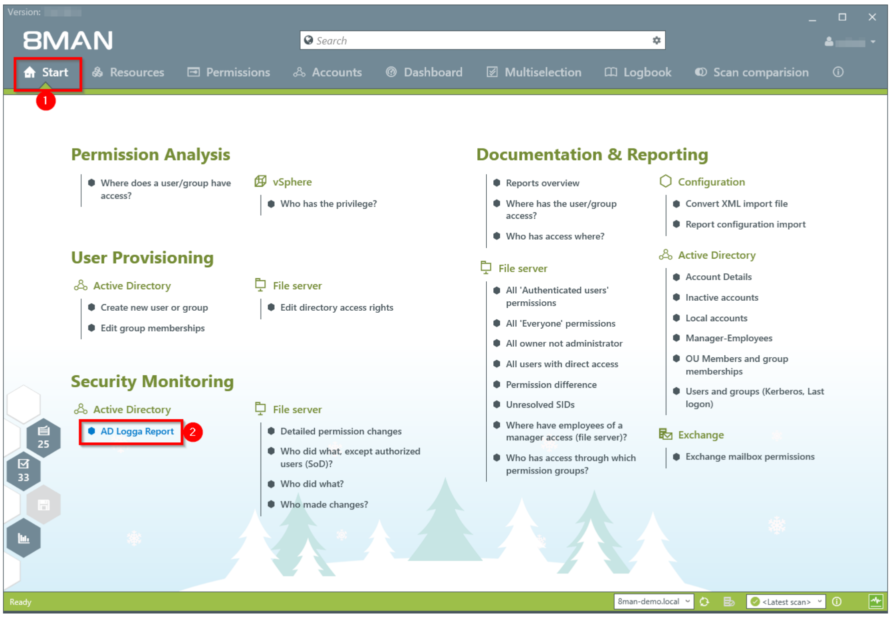
Background / Value

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 the revert back to the original state after performing their desired actions. Without the AD Logga these types of activities remain completely undetected.

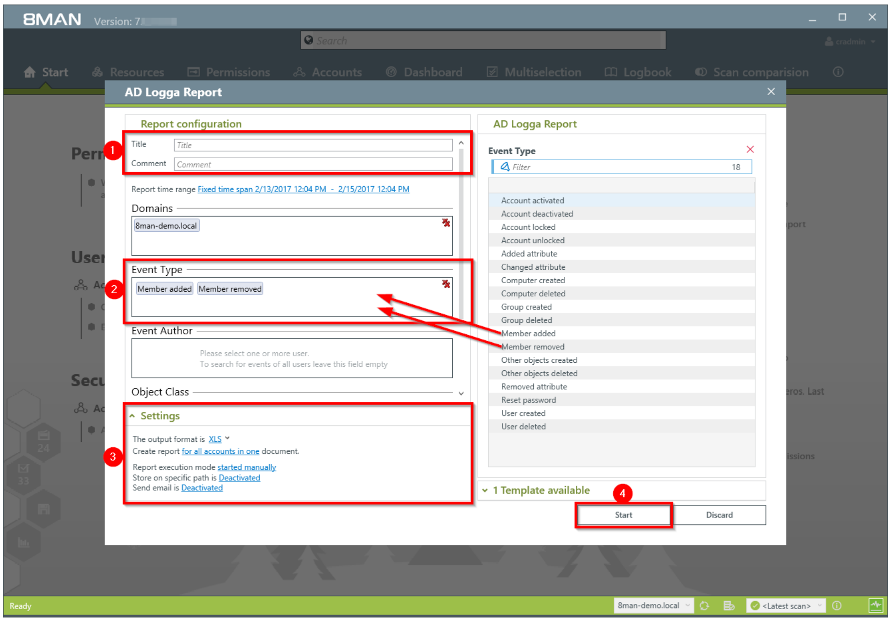
Additional Services

Setting alerts for AD objects

Step by step process



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



AD Logga Report

Report configuration

Title: Title

Comment: Comment

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

Domains: 8man-demo.local

Event Type: Member added, Member removed

Event Author: Please select one or more user. To search for events of all users leave this field empty

Object Class

Settings

The output format is XLS

Create report for all accounts in one document.

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

AD Logga Report

Event Type

Filter 18

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

1 Template available

Start | Discard

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

6.1.1.3 Identifying locked user accounts

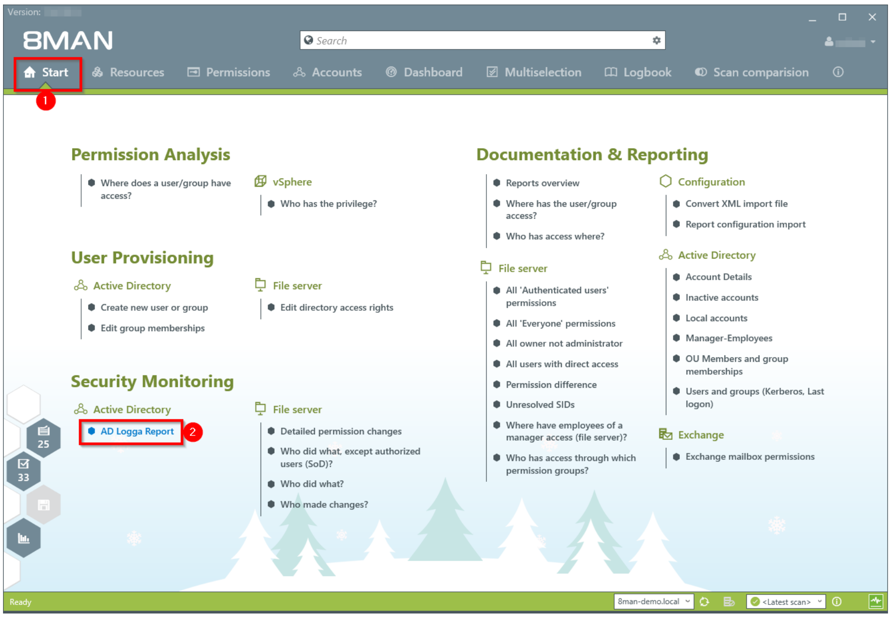
Background / Value

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

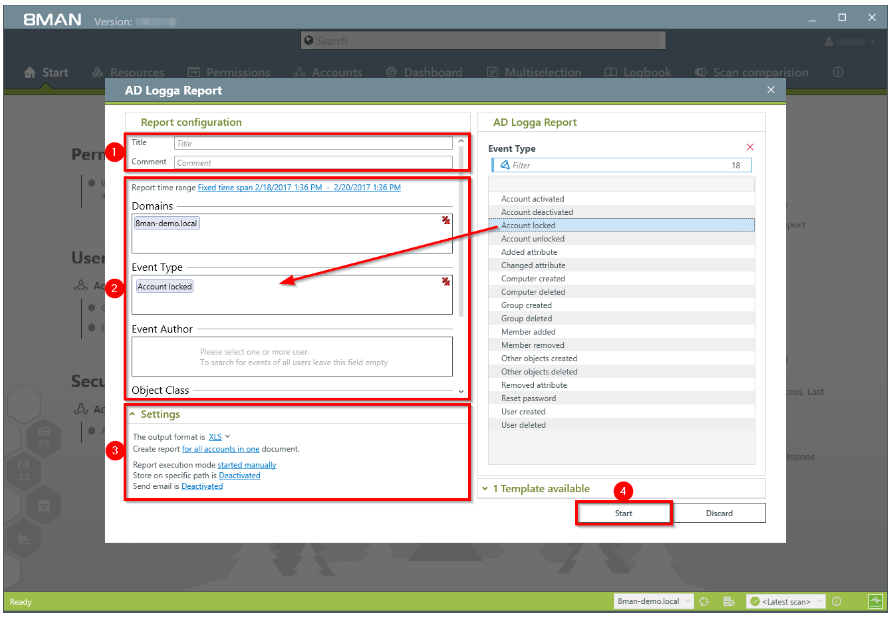
Setting alerts for AD objects

Step by step process



1. Select "Start".

2. Click on "AD Logga Report".



Report configuration

Title: Title

Comment: Comment

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

Domains: 8man-demo.local

Event Type: Account locked

Event Author: Please select one or more user. To search for events of all users leave this field empty

Object Class

Settings

The output format is XLS
Create report for all accounts in one document.
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

AD Logga Report

Event Type

Filter 18

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

1 Template available

Start | Discard

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

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

2. Define the desired report settings.

3. Start the report.

6.1.1.4 Monitoring password resets

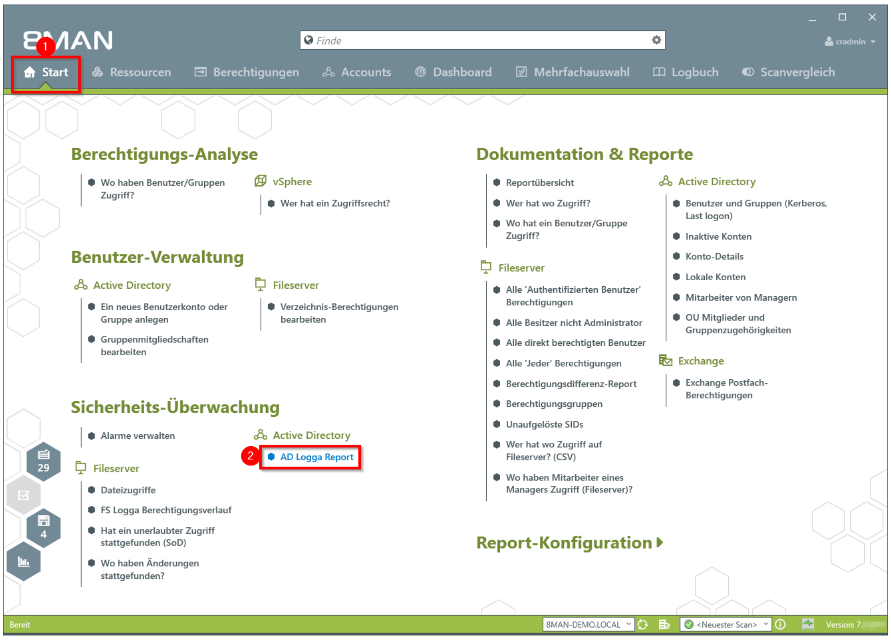
Background / Value

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 is password is no longer valid, perhaps even thinking that he forgot his password, and then simply request a new one from support.

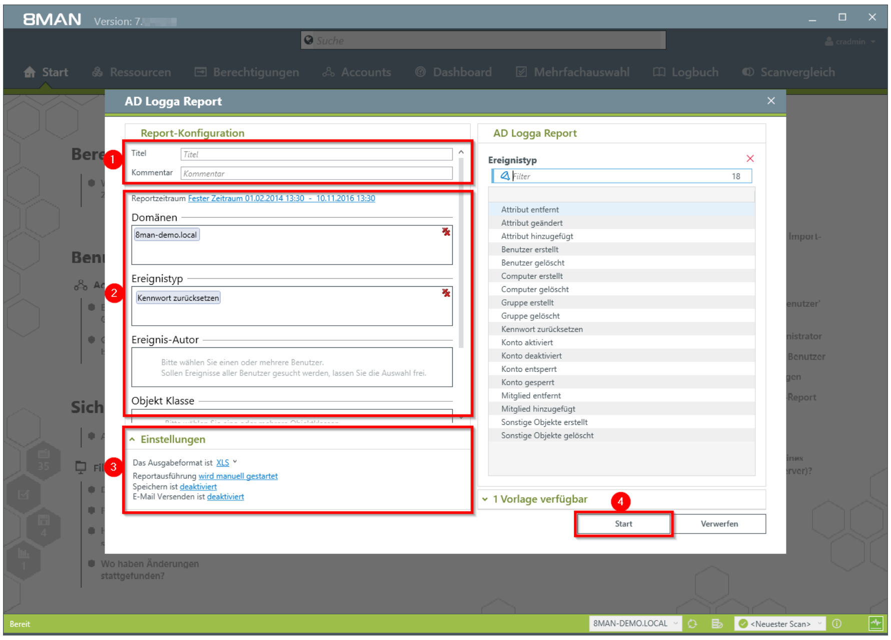
Additional Services

Setting alerts for AD objects

Step by step process


8MAN
1
Finde
cradmin
Start
Ressourcen
Berechtigungen
Accounts
Dashboard
Mehrfachauswahl
Logbuch
Scanvergleich
Berechtigungs-Analyse
Wo haben Benutzer/Gruppen Zugriff?
vSphere
Wer hat ein Zugriffsrecht?
Benutzer-Verwaltung
Active Directory
Ein neues Benutzerkonto oder Gruppe anlegen
Gruppenmitgliedschaften bearbeiten
Fileserver
Verzeichnis-Berechtigungen bearbeiten
Sicherheits-Überwachung
Alarme verwalten
Active Directory
2
AD Logga Report
Fileserver
Dateizugriffe
FS Logga Berechtigungsverlauf
Hat ein unerlaubter Zugriff stattgefunden (SoD)
Wo haben Änderungen stattgefunden?
29
4
Dokumentation & Reporte
Reportübersicht
Wer hat wo Zugriff?
Wo hat ein Benutzer/Gruppe Zugriff?
Fileserver
Alle 'Authentifizierten Benutzer' Berechtigungen
Alle Besitzer nicht Administrator
Alle direkt berechtigten Benutzer
Alle 'Jeder' Berechtigungen
Berechtigungsdifferenz-Report
Berechtigungsgruppen
Unaufgelöste SIDs
Wer hat wo Zugriff auf Fileserver? (CSV)
Wo haben Mitarbeiter eines Managers Zugriff (Fileserver)?
Active Directory
Benutzer und Gruppen (Kerberos, Last logon)
Inaktive Konten
Konto-Details
Lokale Konten
Mitarbeiter von Managern
OU Mitglieder und Gruppenzugehörigkeiten
Exchange
Exchange Postfach-Berechtigungen
Report-Konfiguration
Bereit
8MAN-DEMO.LOCAL
<Neuester Scan>
Version: 7.

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



AD Logga Report

Report-Konfiguration

Titel: Titel

Kommentar: Kommentar

Reportzeitraum Fester Zeitraum 01.02.2014 13:30 - 10.11.2016 13:30

Domänen: 8man-demo.local

Ereignistyp: Kennwort zurücksetzen

Ereignis-Autor: Bitte wählen Sie einen oder mehrere Benutzer. Sollen Ereignisse aller Benutzer gesucht werden, lassen Sie die Auswahl frei.

Objekt Klasse

Einstellungen

Das Ausgabeformat ist XLS
Reportausführung wird manuell gestartet
Speichern ist deaktiviert
E-Mail Versenden ist deaktiviert

AD Logga Report

Ereignistyp

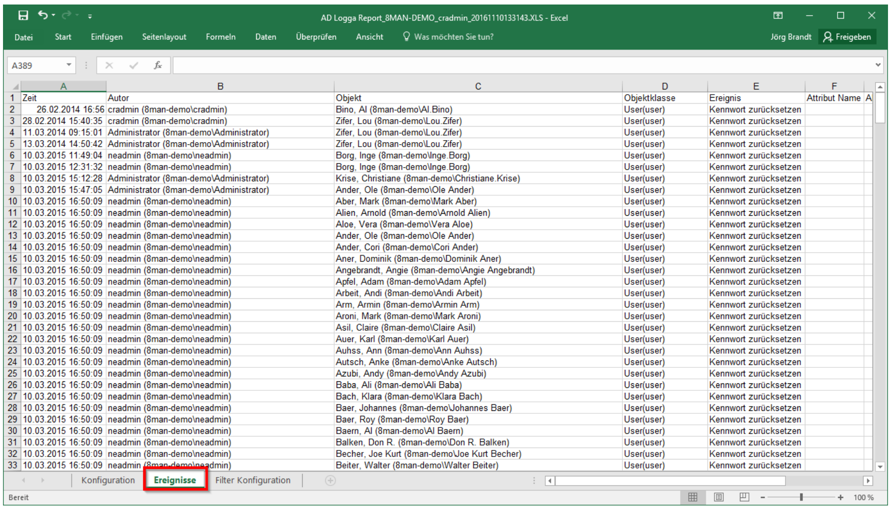
Filter 18

- Attribut entfernt
- Attribut geändert
- Attribut hinzugefügt
- Benutzer erstellt
- Benutzer gelöscht
- Computer erstellt
- Computer gelöscht
- Gruppe erstellt
- Gruppe gelöscht
- Kennwort zurücksetzen
- Konto aktiviert
- Konto deaktiviert
- Konto entsperrt
- Konto gesperrt
- Mitglied entfernt
- Mitglied hinzugefügt
- Sonstige Objekte erstellt
- Sonstige Objekte gelöscht

1 Vorlage verfügbar

Start | Verwerfen

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



	A	B	C	D	E	F
1	Zeit	Autor	Objekt	Objektklasse	Ereignis	Attribut Name
2	26.02.2014 16:56	cradmin (8man-demo\cradmin)	Bino, Al (8man-demo\Al.Bino)	User(user)	Kennwort zurücksetzen	
3	28.02.2014 15:40:35	cradmin (8man-demo\cradmin)	Zifer, Lou (8man-demo\Lou.Zifer)	User(user)	Kennwort zurücksetzen	
4	11.03.2014 09:15:01	Administrator (8man-demo\Administrator)	Zifer, Lou (8man-demo\Lou.Zifer)	User(user)	Kennwort zurücksetzen	
5	13.03.2014 14:50:42	Administrator (8man-demo\Administrator)	Zifer, Lou (8man-demo\Lou.Zifer)	User(user)	Kennwort zurücksetzen	
6	10.03.2015 11:49:04	neadmin (8man-demo\neadmin)	Borg, Inge (8man-demo\Inge.Borg)	User(user)	Kennwort zurücksetzen	
7	10.03.2015 12:31:32	neadmin (8man-demo\neadmin)	Borg, Inge (8man-demo\Inge.Borg)	User(user)	Kennwort zurücksetzen	
8	10.03.2015 15:12:28	Administrator (8man-demo\Administrator)	Krise, Christiane (8man-demo\Christiane.Krise)	User(user)	Kennwort zurücksetzen	
9	10.03.2015 15:47:05	Administrator (8man-demo\Administrator)	Ander, Ole (8man-demo\Ole Ander)	User(user)	Kennwort zurücksetzen	
10	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Aber, Mark (8man-demo\Mark Aber)	User(user)	Kennwort zurücksetzen	
11	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Alien, Arnold (8man-demo\Arnold Alien)	User(user)	Kennwort zurücksetzen	
12	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Aloe, Vera (8man-demo\Vera Aloe)	User(user)	Kennwort zurücksetzen	
13	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Ander, Ole (8man-demo\Ole Ander)	User(user)	Kennwort zurücksetzen	
14	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Ander, Cori (8man-demo\Cori Ander)	User(user)	Kennwort zurücksetzen	
15	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Aner, Dominik (8man-demo\Dominik Aner)	User(user)	Kennwort zurücksetzen	
16	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Angebrandt, Angie (8man-demo\Angie Angebrandt)	User(user)	Kennwort zurücksetzen	
17	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Apfel, Adam (8man-demo\Adam Apfel)	User(user)	Kennwort zurücksetzen	
18	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Arbeit, Andi (8man-demo\Andi Arbeit)	User(user)	Kennwort zurücksetzen	
19	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Arm, Armin (8man-demo\Armin Arm)	User(user)	Kennwort zurücksetzen	
20	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Aroni, Mark (8man-demo\Mark Aroni)	User(user)	Kennwort zurücksetzen	
21	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Asil, Claire (8man-demo\Claire Asil)	User(user)	Kennwort zurücksetzen	
22	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Auer, Karl (8man-demo\Karl Auer)	User(user)	Kennwort zurücksetzen	
23	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Auhss, Ann (8man-demo\Ann Auhss)	User(user)	Kennwort zurücksetzen	
24	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Autsch, Anke (8man-demo\Anke Autsch)	User(user)	Kennwort zurücksetzen	
25	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Azubi, Andy (8man-demo\Andy Azubi)	User(user)	Kennwort zurücksetzen	
26	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Baba, Ali (8man-demo\Ali Baba)	User(user)	Kennwort zurücksetzen	
27	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Bach, Klara (8man-demo\Klara Bach)	User(user)	Kennwort zurücksetzen	
28	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Baer, Johannes (8man-demo\Johannes Baer)	User(user)	Kennwort zurücksetzen	
29	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Baer, Roy (8man-demo\Roy Baer)	User(user)	Kennwort zurücksetzen	
30	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Baern, Al (8man-demo\Al Baern)	User(user)	Kennwort zurücksetzen	
31	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Balken, Don R. (8man-demo\Don R. Balken)	User(user)	Kennwort zurücksetzen	
32	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Becher, Joe Kurt (8man-demo\Joe Kurt Becher)	User(user)	Kennwort zurücksetzen	
33	10.03.2015 16:50:09	neadmin (8man-demo\neadmin)	Beiter, Walter (8man-demo\Walter Beiter)	User(user)	Kennwort zurücksetzen	

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

6.1.1.5 Analysing AD Logga events with the logbook

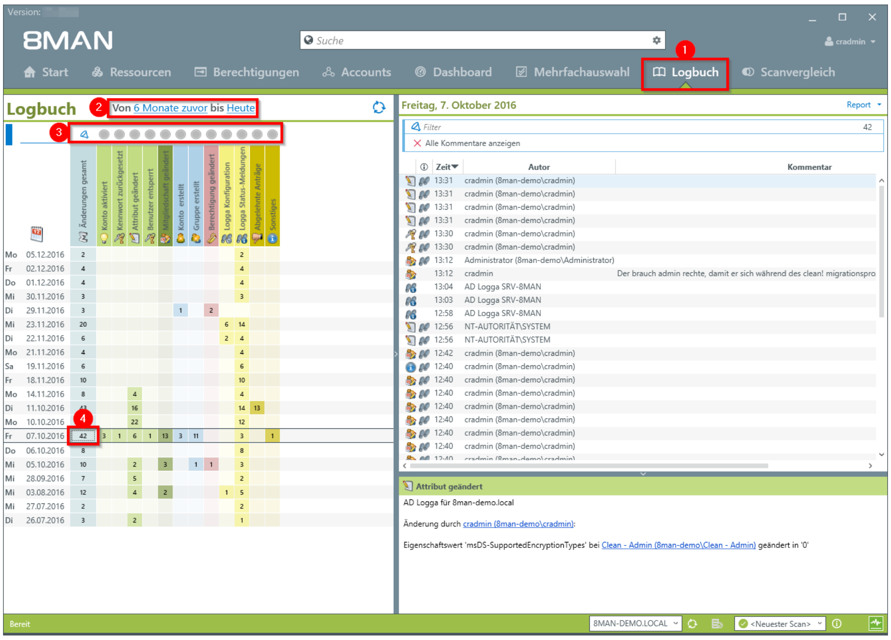
Background / Value

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

Monitoring changes to specific event types
Identifying temporary group memberships
Identifying locked user accounts
Monitoring password resets
Setting Alerts for Active Directory objects

Step by step process



Logbuch

Von 6 Monate zuvor bis Heute

		Änderungen gesamt	Konto aktiviert	Kennwort zurückgesetzt	Attribut geändert	Benutzer entsperrt	Mitgliedschaft geändert	Konto erstellt	Gruppe erstellt	Berechtigung geändert	Logga Konfiguration	Logga Status-Meldungen	Abgelehnte Anträge	Sonstiges
Mo	05.12.2016	2										2		
Fr	02.12.2016	4										4		
Do	01.12.2016	4										4		
Mi	30.11.2016	3										3		
Di	29.11.2016	3						1		2				
Mi	23.11.2016	20									6	14		
Di	22.11.2016	6									2	4		
Mo	21.11.2016	4										4		
Sa	19.11.2016	6										6		
Fr	18.11.2016	10										10		
Mo	14.11.2016	8			4							4		
Di	11.10.2016	43			16							14	13	
Mo	10.10.2016	[illegible]			22							12		
Fr	07.10.2016	42	3	1	6	1	13	3	11			3		1
Do	06.10.2016	8										8		
Mi	05.10.2016	10			2		3		1	1		3		
Mi	28.09.2016	7			5							2		
Mi	03.08.2016	12			4		2				1	5		
Mi	27.07.2016	2										2		
Di	26.07.2016	3			2							1		

Freitag, 7. Oktober 2016

Filter 42

✕ Alle Kommentare anzeigen

Zeit	Autor	Kommentar
13:31	cradmin (8man-demo\cradmin)	
13:31	cradmin (8man-demo\cradmin)	
13:31	cradmin (8man-demo\cradmin)	
13:31	cradmin (8man-demo\cradmin)	
13:30	cradmin (8man-demo\cradmin)	
13:30	cradmin (8man-demo\cradmin)	
13:12	Administrator (8man-demo\Administrator)	
13:12	cradmin	Der brauch admin rechte, damit er sich während des clean! migrationspro
13:04	AD Logga SRV-8MAN	
13:03	AD Logga SRV-8MAN	
12:58	AD Logga SRV-8MAN	
12:56	NT-AUTORITÄT\SYSTEM	
12:56	NT-AUTORITÄT\SYSTEM	
12:42	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	

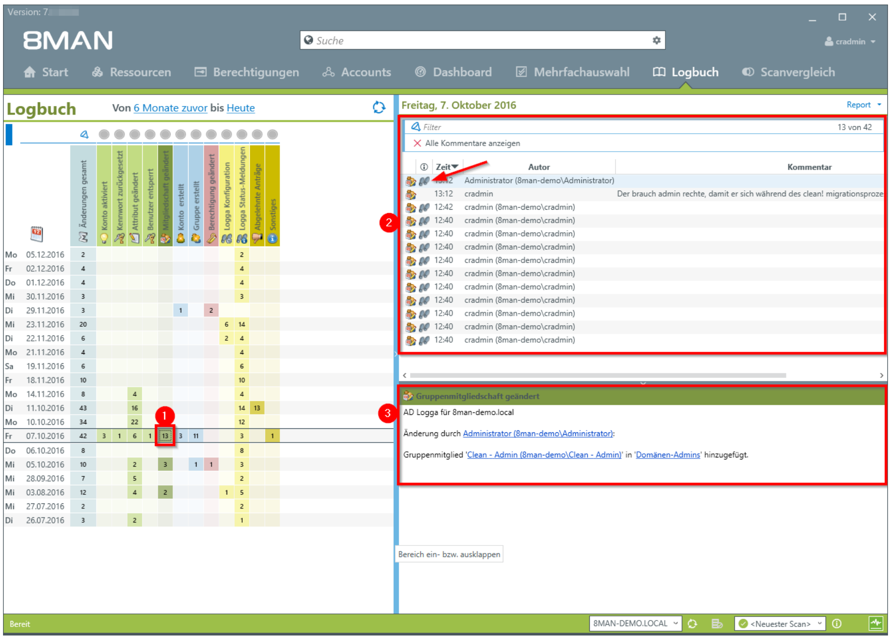
Attribut geändert

AD Logga für 8man-demo.local

Änderung durch cradmin (8man-demo\cradmin):

Eigenschaftswert 'msDS-SupportedEncryptionTypes' bei Clean - Admin (8man-demo\Clean - Admin) geändert in '0'

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.*



Logbuch Von 6 Monate zuvor bis Heute

		Änderungen gesamt	Konto aktiviert	Kennwort zurückgesetzt	Attribut geändert	Benutzer entsperrt	Mitgliedschaft geändert	Konto erstellt	Gruppe erstellt	Berechtigung geändert	Logga Konfiguration	Logga Status-Meldungen	Abgelehnte Anträge	Sonstiges
Mo	05.12.2016	2										2		
Fr	02.12.2016	4										4		
Do	01.12.2016	4										4		
Mi	30.11.2016	3										3		
Di	29.11.2016	3						1		2				
Mi	23.11.2016	20									6	14		
Di	22.11.2016	6									2	4		
Mo	21.11.2016	4										4		
Sa	19.11.2016	6										6		
Fr	18.11.2016	10										10		
Mo	14.11.2016	8			4							4		
Di	11.10.2016	43			16							14	13	
Mo	10.10.2016	34			22							12		
Fr	07.10.2016	42	3	1	6	1	13	3	11			3		1
Do	06.10.2016	8										8		
Mi	05.10.2016	10			2		3		1	1		3		
Mi	28.09.2016	7			5							2		
Mi	03.08.2016	12			4		2				1	5		
Mi	27.07.2016	2										2		
Di	26.07.2016	3			2							1		

Freitag, 7. Oktober 2016

Filter 13 von 42

Alle Kommentare anzeigen

Zeit	Autor	Kommentar
13:12	Administrator (8man-demo\Administrator)	
13:12	cradmin	Der brauch admin rechte, damit er sich während des clean! migrationsproze
12:42	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	
12:40	cradmin (8man-demo\cradmin)	

Gruppenmitgliedschaft geändert

AD Logga für 8man-demo.local

Änderung durch Administrator (8man-demo\Administrator):

Gruppenmitglied 'Clean - Admin (8man-demo\Clean - Admin)' in 'Domänen-Admins' hinzugefügt.

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.*

6.1.2 +8MATE Alerts

8MATE Alerts uses AD Logga monitoring technology and expands this with an alert function. If anyone manipulates sensitive accounts or groups the administrator or any other designated employee with an email address can be informed.

6.1.2.1 Setting 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 Alerts allows you to actively monitor specific AD groups so that an alert is received if new members are added.

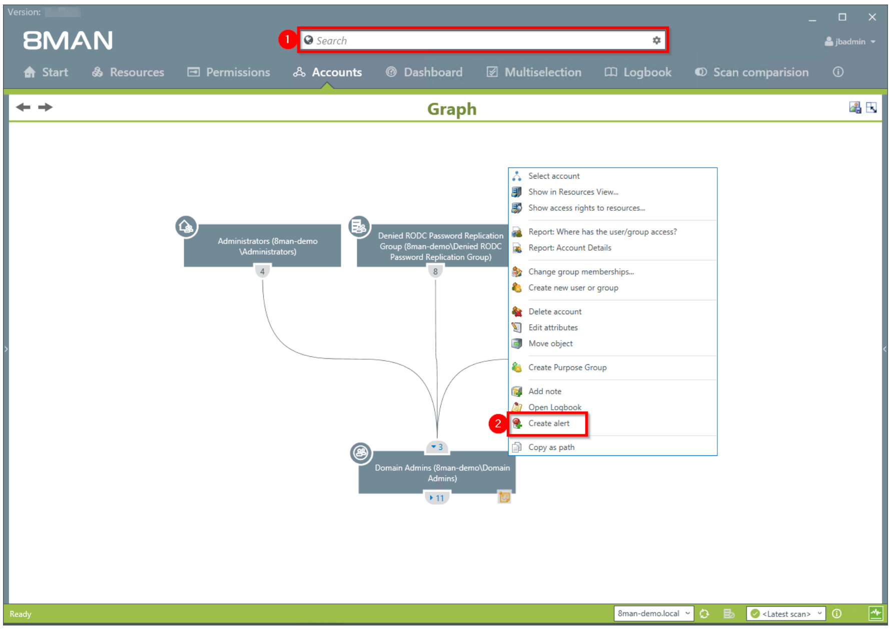
Due to the nested group structures in Active Directory it is important to monitor group memberships, that occur from new indirect memberships. For example: The group "secret data" is a member in the "C-Level" group which is being monitored. 8MATE Alerts will notify you even if members are only added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

Additional services

Setting alerts for user accounts

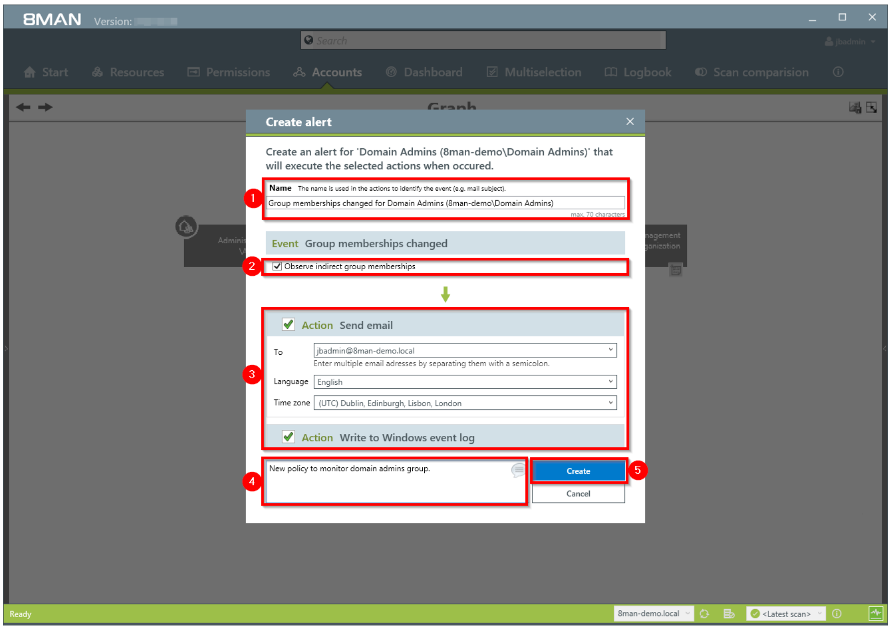
Managing alerts

Step by step process



1. Find the desired group by entering its name into the search field.

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



Create alert

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

Name The name is used in the actions to identify the event (e.g. mail subject).

Group memberships changed for Domain Admins (8man-demo\Domain Admins)

max. 70 characters

Event Group memberships changed

☑ Observe indirect group memberships

☑ Action Send email

To: jbadmin@8man-demo.local

Enter multiple email adresses by separating them with a semicolon.

Language: English

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

☑ Action Write to Windows event log

New policy to monitor domain admins group.

Create

Cancel

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

6.1.2.2 Setting alerts for user accounts

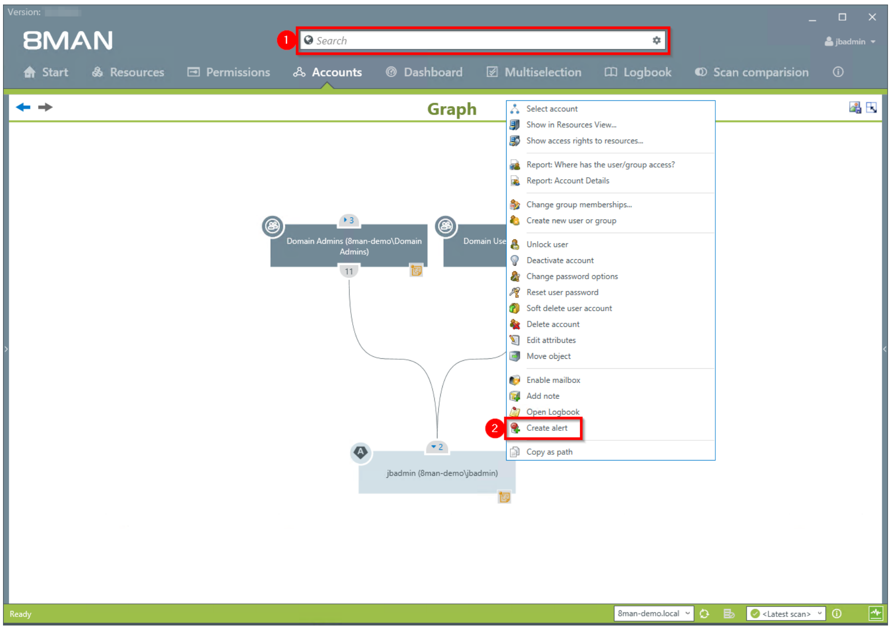
Background / Value

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.

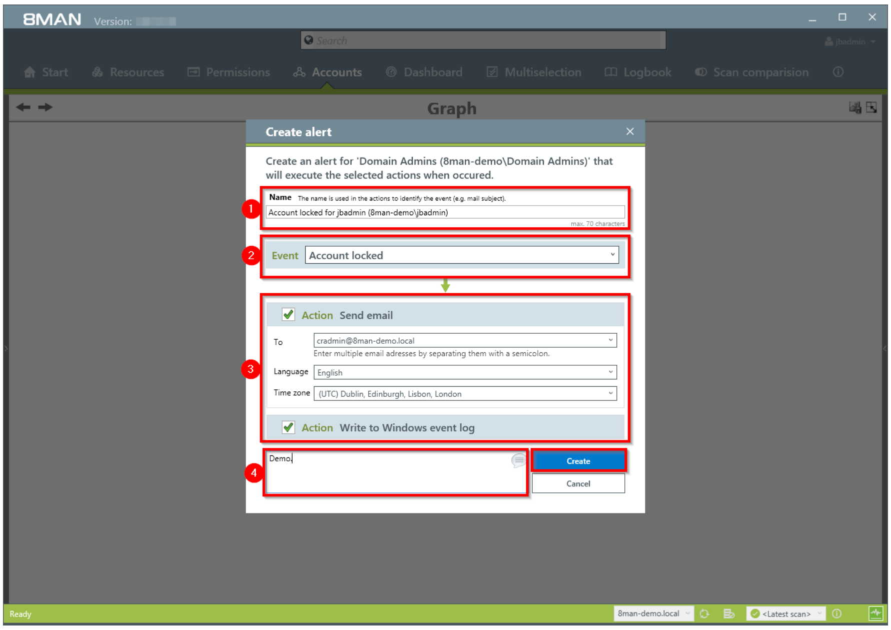
Additional services

Setting alerts for groups

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.*



Create alert

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

Name The name is used in the actions to identify the event (e.g. mail subject).

Account locked for jbadmin (8man-demo\jbadmin)

max. 70 characters

Event: Account locked

☑ Action Send email

To: cradmin@8man-demo.local

Enter multiple email adresses by separating them with a semicolon.

Language: English

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

☑ Action Write to Windows event log

Demo.

Create

Cancel

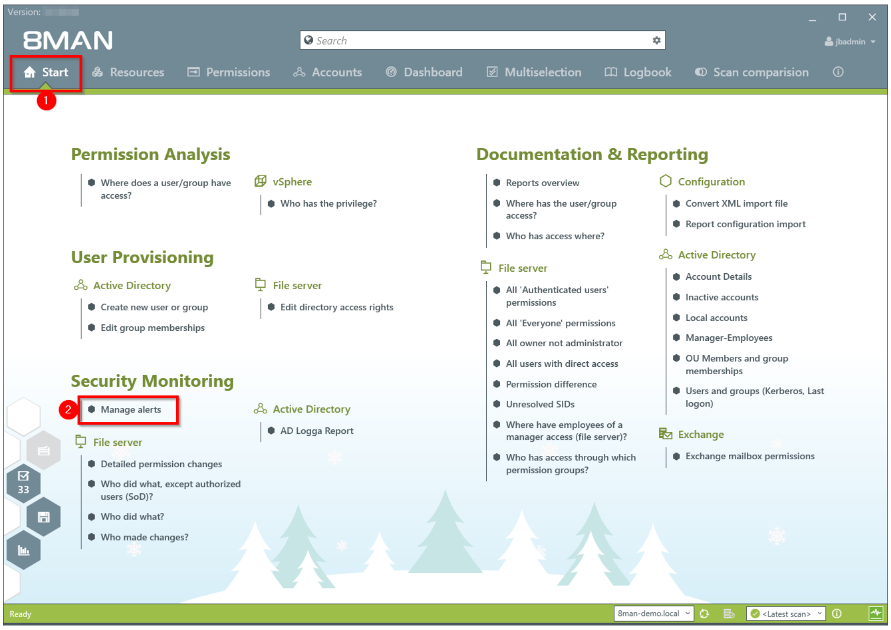
1. *Enter a title for the alert.*
1. *Select an event for which you want to receive the alert.*
2. *You can select any number of email recipients. Additionally alerts can be displayed in the windows event log.*
3. *You must enter a comment.*
4. *Create the alert.*

6.1.2.3 Managing alerts

Background / Value

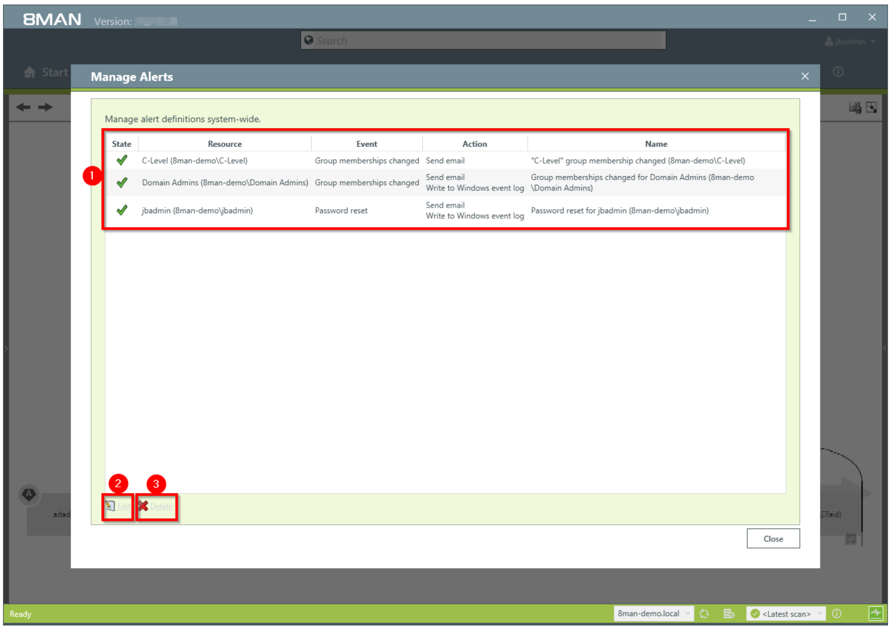
You can modify saved alerts at any time on the 8MAN home page.

Step by step process



1. Select "Start".

2. Click on "Manage alerts".



Manage alert definitions system-wide.

State	Resource	Event	Action	Name
✓	C-Level (8man-demo\C-Level)	Group memberships changed	Send email	"C-Level" group membership changed (8man-demo\C-Level)
✓	Domain Admins (8man-demo\Domain Admins)	Group memberships changed	Send email Write to Windows event log	Group memberships changed for Domain Admins (8man-demo \Domain Admins)
✓	jbadmin (8man-demo\jbadmin)	Password reset	Send email Write to Windows event log	Password reset for jbadmin (8man-demo\jbadmin)

1. 8MAN displays a list of all alerts. Select the desired entry.

2. Edit the existing alert configuration.

3. Delete the alert. The modification of alerts is fully captured in the log book.

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 Monitoring access to sensitive data

Background / Value

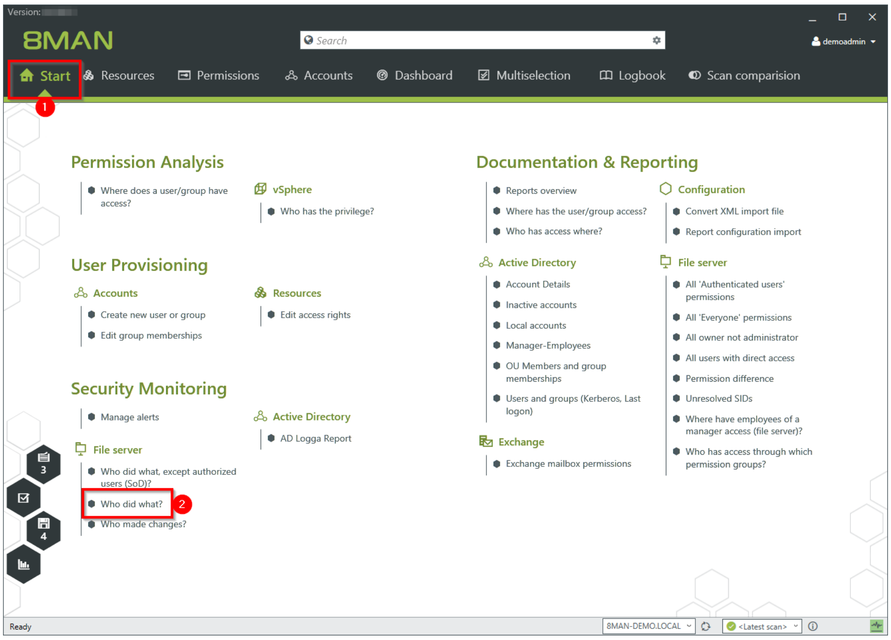
As a first step you have hopefully limited access rights to sensitive directories. As a second step we recommend the continuous monitoring of access by individual users, including the exact actions that they performed. This ensures full process transparency for especially sensitive data and information.

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.

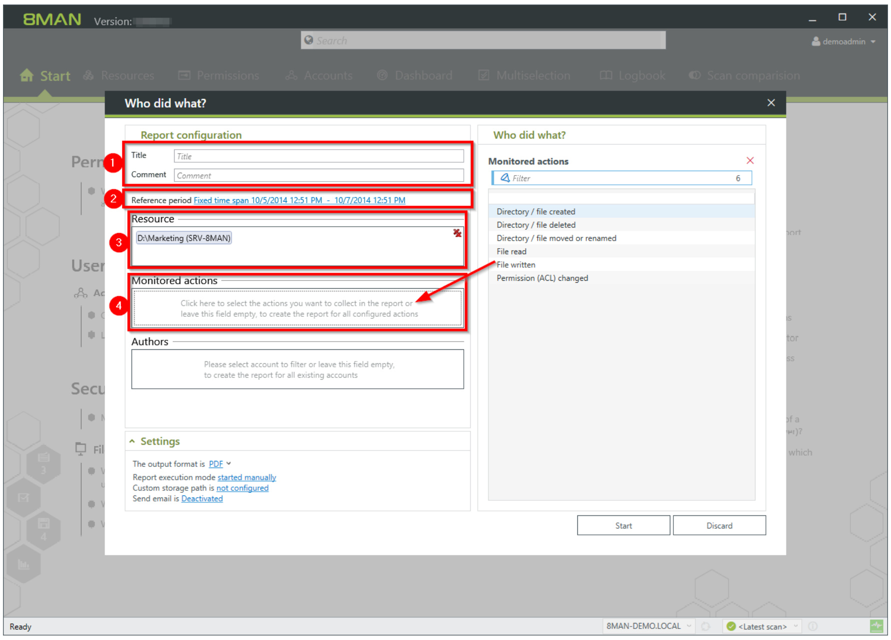
Additional services

Change directory access rights

Step by step process



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


8MAN Version:
Search
demoadmin
Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparision
1
2
3
4
Start
Discard
Ready
8MAN-DEMO.LOCAL
<Latest scan>

Who did what?

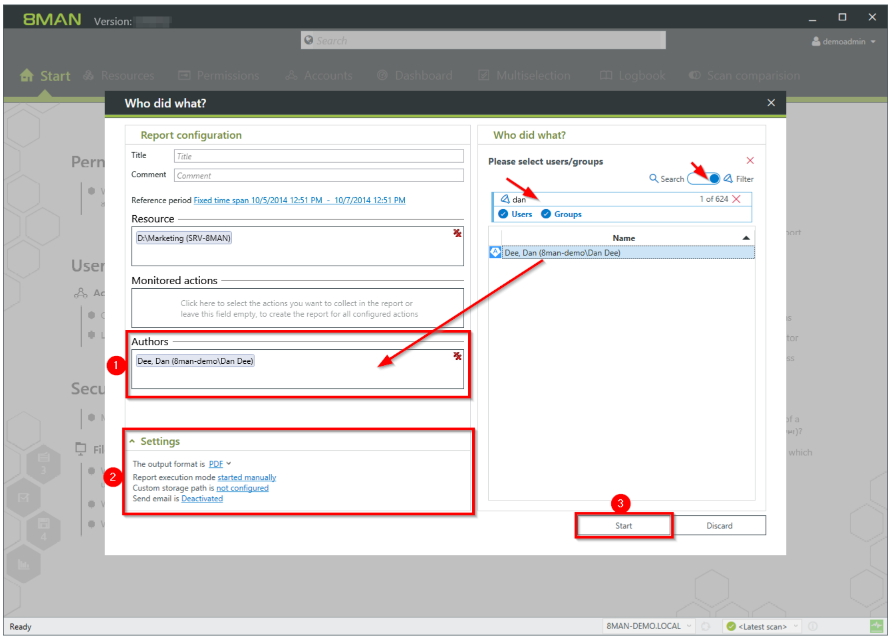
Report configuration

Title: Title
Comment: Comment
Reference period Fixed time span 10/5/2014 12:51 PM - 10/7/2014 12:51 PM
Resource: D:\Marketing (SRV-8MAN)
Monitored actions: Click here to select the actions you want to collect in the report or leave this field empty, to create the report for all configured actions
Authors: Please select account to filter or leave this field empty, to create the report for all existing accounts

Settings
The output format is PDF
Report execution mode started manually
Custom storage path is not configured
Send email is Deactivated

Who did what?
Monitored actions
Filter 6
- Directory / file created
- Directory / file deleted
- Directory / file moved or renamed
- File read
- File written
- Permission (ACL) changed

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.


8MAN Version:
Search
demoadmin
Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparision
1
2
3
Start
Discard
Ready
8MAN-DEMO.LOCAL
<Latest scan>

Who did what?

Report configuration

Title: Title
Comment: Comment
Reference period Fixed time span 10/5/2014 12:51 PM - 10/7/2014 12:51 PM
Resource: D:\Marketing (SRV-8MAN)
Monitored actions: Click here to select the actions you want to collect in the report or leave this field empty, to create the report for all configured actions
Authors: Dee, Dan (8man-demo\Dan Dee)

Settings
The output format is PDF
Report execution mode started manually
Custom storage path is not configured
Send email is Deactivated

Who did what?
Please select users/groups
Search Filter
dan 1 of 624
Users Groups

Name
Dee, Dan (8man-demo\Dan Dee)

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 e-mail
3. Start the report.

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 Applying 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.

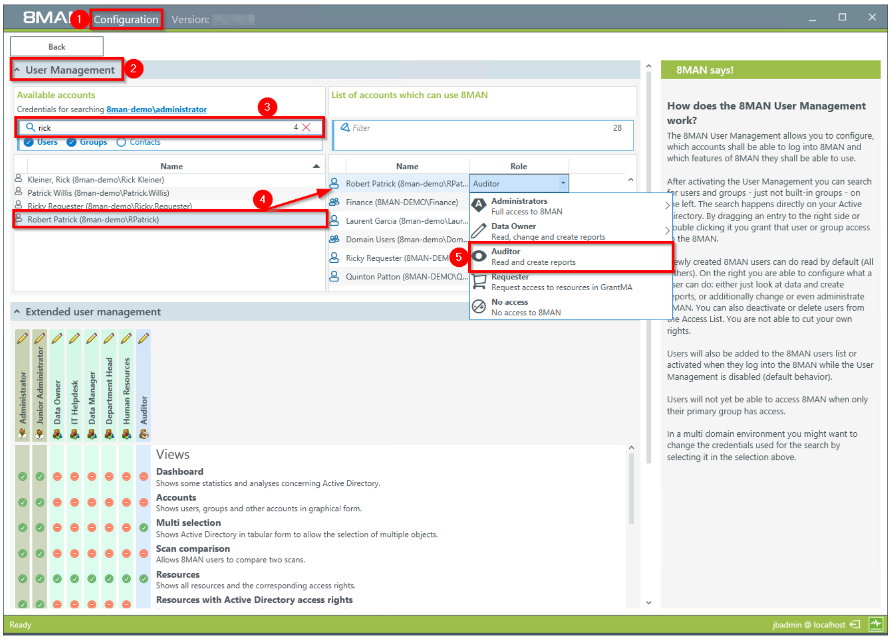
7.1.1.1 Creating a read only account with 8MAN

Background / Value

Involve security officers in the process of access rights management by granting them read-only accecss. This allows them to generate their own reports.

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

Step by step process



Credentials for searching 8man-demo\administrator

rick 4

Name
Kleiner, Rick (8man-demo\Rick Kleiner)
Patrick Willis (8man-demo\Patrick.Willis)
Ricky Requester (8man-demo\Ricky.Requester)
Robert Patrick (8man-demo\RPatrick)

Name	Role
Robert Patrick (8man-demo\RPat...	Auditor
Finance (8MAN-DEMO\Finance)	
Laurent Garcia (8man-demo\Laur...	
Domain Users (8man-demo\Dom...	
Ricky Requester (8MAN-DEM...	
Quinton Patton (8MAN-DEMO\Q...	

Administrators Full access to 8MAN
Data Owner Read, change and create reports
Auditor Read and create reports
Requester Request access to resources in GrantMA
No access No access to 8MAN

Dashboard Shows some statistics and analyses concerning Active Directory.
Accounts Shows users, groups and other accounts in graphical form.
Multi selection Shows Active Directory in tabular form to allow the selection of multiple objects.
Scan comparison Allows 8MAN users to compare two scans.
Resources Shows all resources and the corresponding access rights.
Resources with Active Directory access rights

How does the 8MAN User Management work?

The 8MAN User Management allows you to configure, which accounts shall be able to log into 8MAN and which features of 8MAN they shall be able to use.

After activating the User Management you can search for users and groups - just not built-in groups - on the left. The search happens directly on your Active Directory. By dragging an entry to the right side or double clicking it you grant that user or group access to the 8MAN.

Newly created 8MAN users can do read by default (All others). On the right you are able to configure what a user can do: either just look at data and create reports, or additionally change or even administrate 8MAN. You can also deactivate or delete users from the Access List. You are not able to cut your own rights.

Users will also be added to the 8MAN users list or activated when they log into the 8MAN while the User Management is disabled (default behavior).

Users will not yet be able to access 8MAN when only their primary group has access.

In a multi domain environment you might want to change the credentials used for the search by selecting it in the selection above.

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

7.1.1.2 Scheduling reports

Background / Value

You can involve security personell in the process of access rights management by assigning reports to the relevant security officers. 8MAN sends the reports in the desired frequency. The process is identical for all reports.

We recommend sending a selection of management reports to the role responsible for security. The reports are easy to read and only contain the necessary information.

8MAN Management Reports:

Active Directory

Employees of a Manager
Displaying user account details

File server

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

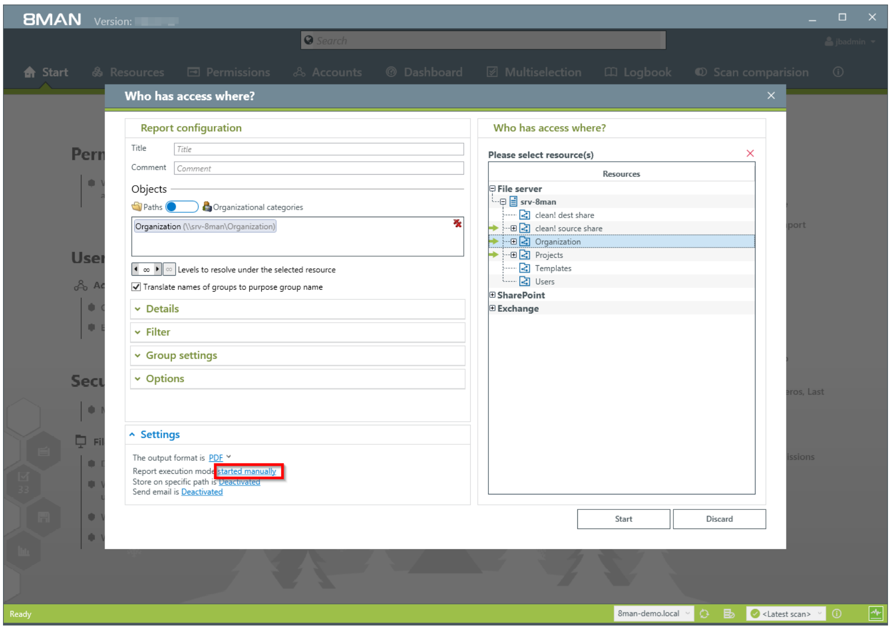
Exchange

Who has access to what?
Identifying mailbox permissions

SharePoint

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

Step by step process



Who has access where?

Report configuration

Title: Title
Comment: Comment

Objects
Paths ○ Organizational categories
Organization (\\srv-8man\Organization)

∞ Levels to resolve under the selected resource
☑ Translate names of groups to purpose group name

Details
Filter
Group settings
Options

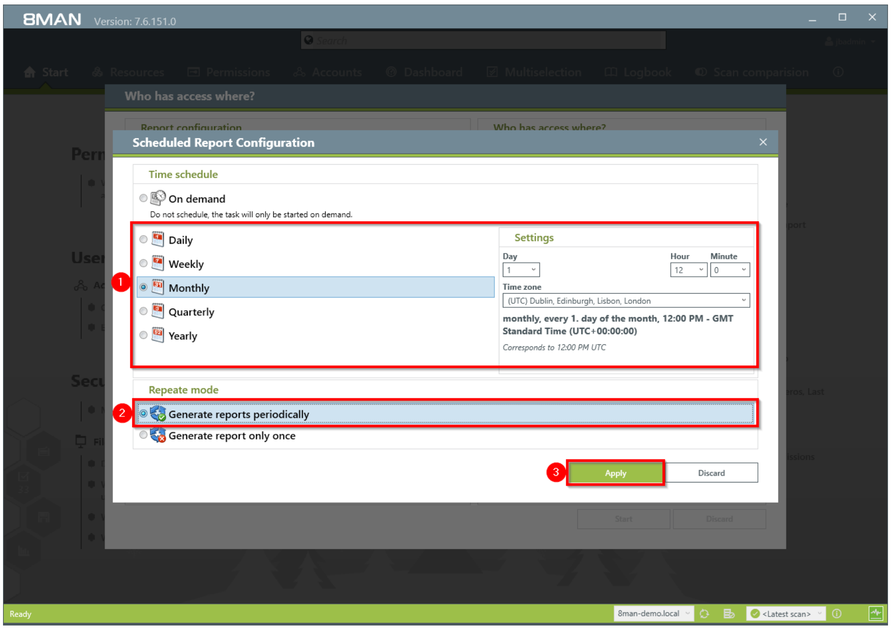
Settings
The output format is PDF
Report execution mode started manually
Store on specific path is Deactivated
Send email is Deactivated

Who has access where?
Please select resource(s)

Resources
- File server
  - srv-8man
    - clean! dest share
    - clean! source share
    - Organization
    - Projects
    - Templates
    - Users
- SharePoint
- Exchange

Start | Discard

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



Scheduled Report Configuration

Time schedule
○ On demand
Do not schedule, the task will only be started on demand.

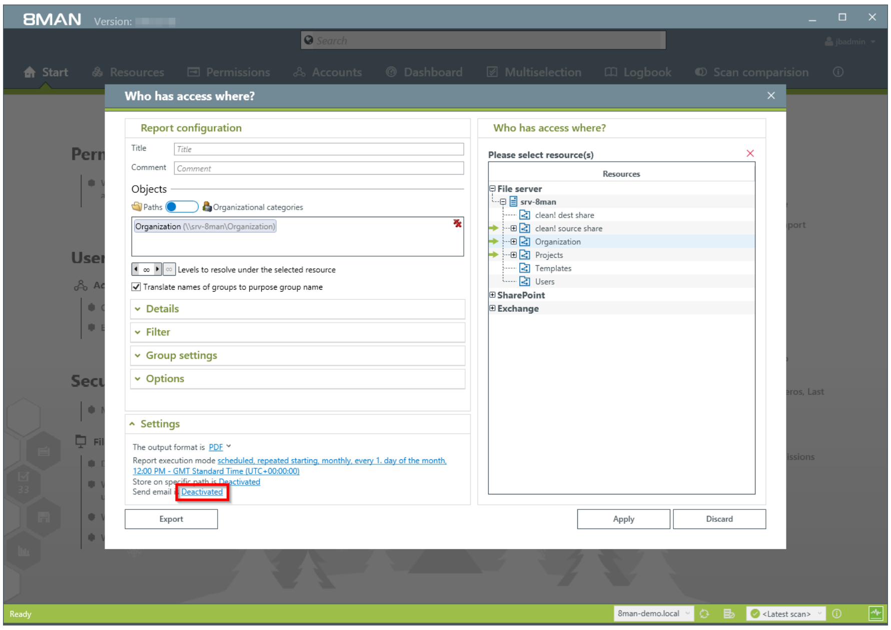
1
○ Daily
○ Weekly
● Monthly
○ Quarterly
○ Yearly

Settings
Day: 1 Hour: 12 Minute: 0
Time zone: (UTC) Dublin, Edinburgh, Lisbon, London
monthly, every 1. day of the month, 12:00 PM - GMT Standard Time (UTC+00:00:00)
Corresponds to 12:00 PM UTC

Repeate mode
2
● Generate reports periodically
○ Generate report only once

3
Apply | Discard

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

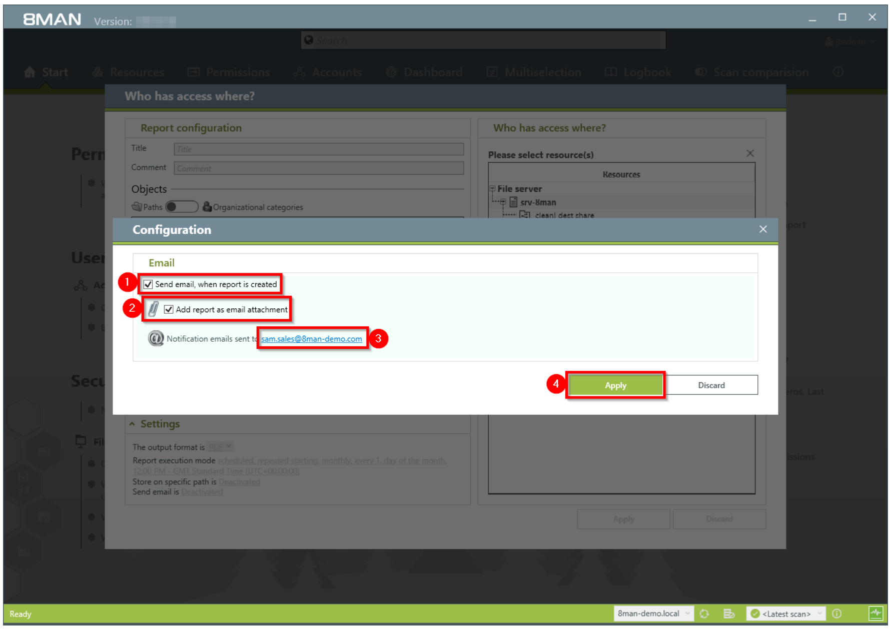


Organization (\\srv-8man\Organization)

☑ Translate names of groups to purpose group name

The output format is PDF
Report execution mode scheduled, repeated starting, monthly, every 1. day of the month, 12:00 PM - GMT Standard Time (UTC+00:00:00)
Store on specific path is Deactivated
Send email is Deactivated

Click on "Deactivated".



☑ Send email, when report is created
☑ Add report as email attachment
Notification emails sent to sam.sales@8man-demo.com

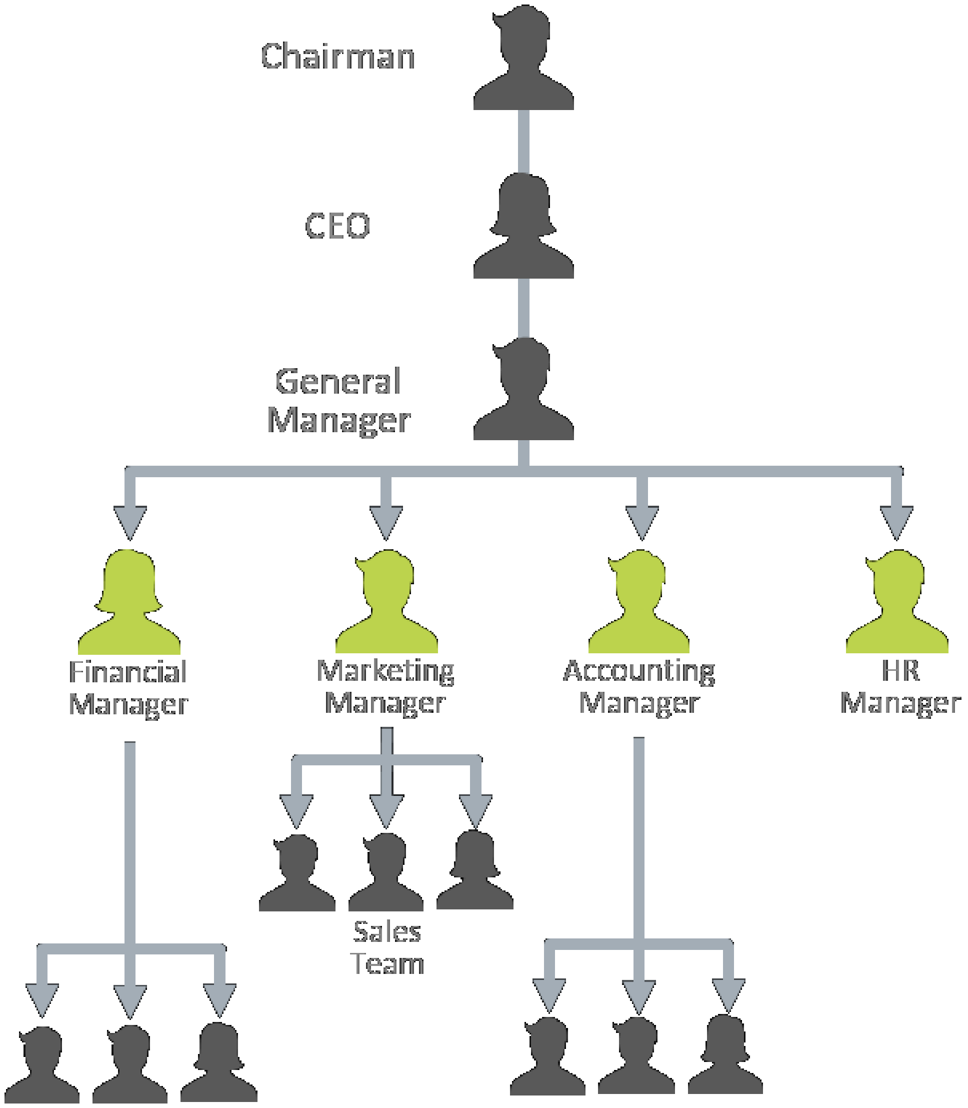
1. Activate emails.
2. Activate the option "Add report as email attachment".
3. Determine who should receive the email. You can enter more than one recipient.
4. Click on "Apply".

7.1.2 Delegating management of directory access rights to data owners

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.



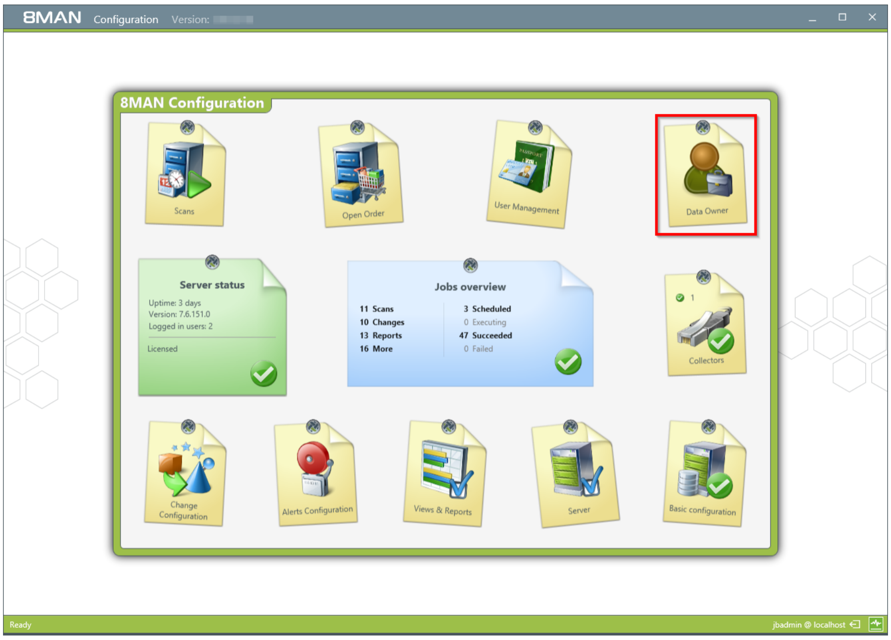
7.1.2.1 Defining data owners and assigning resources

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.

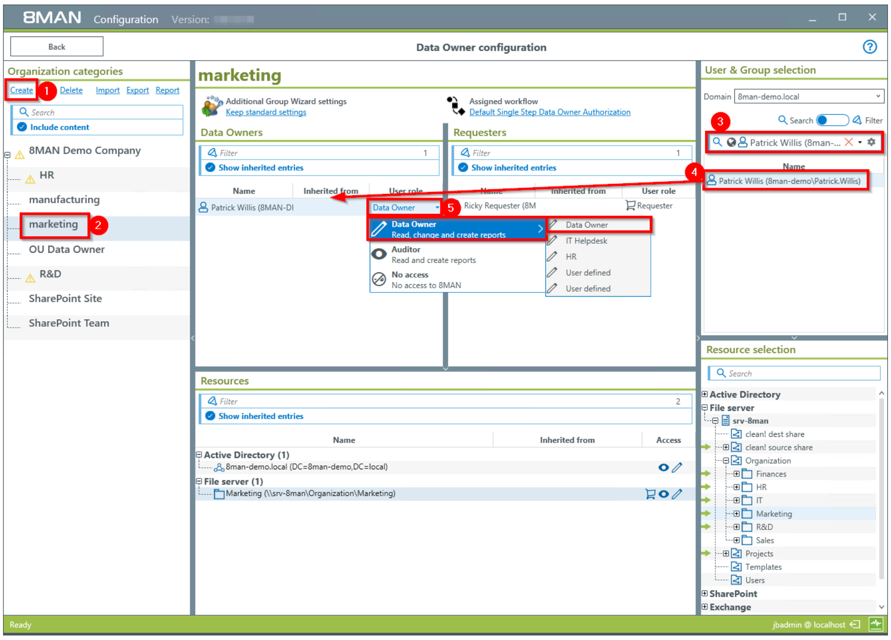
Step by step process



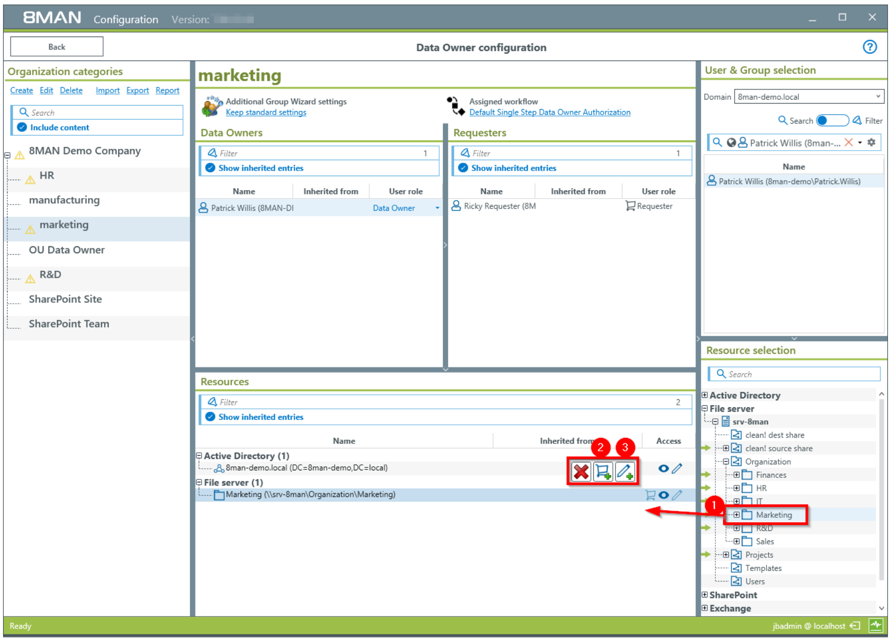
Server status
Uptime: 3 days
Version: 7.6.151.0
Logged in users: 2
Licensed

Jobs overview
11 Scans
10 Changes
13 Reports
16 More
3 Scheduled
0 Executing
47 Succeeded
0 Failed

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



1. Create an organizational category, for example "Marketing".
2. Select the newly created category.
3. Use the search field to find the desired account.
4. Use drag & drop to move the account to the column "Data Owner".
5. Select the desired role in the column "User rights".



1. Use drag & drop to move resources out of the "Resource selection" into the "Resources" section. You are also able to search for resources.
2. Mark the resources as "requestable" in 8MATE GrantMA.
3. Mark the resources as "changeable".

Please note the access to Active Directory is required to use the group wizard.

7.1.2.2 Enabling Data Owners to manage access rights to file server directories

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 Delegating 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

Create a user from a template

Delete a user and their access right Manage attributes

Activate / Deactivate user account

Unlock user

Reset password

Delete user account ("Soft Delete")

Exchange

Create Exchange mailbox

Manage mailbox size

Manage out of office notices

Change access rights to mailboxes

7.1.3.1 Defining your help desk and assigning 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.

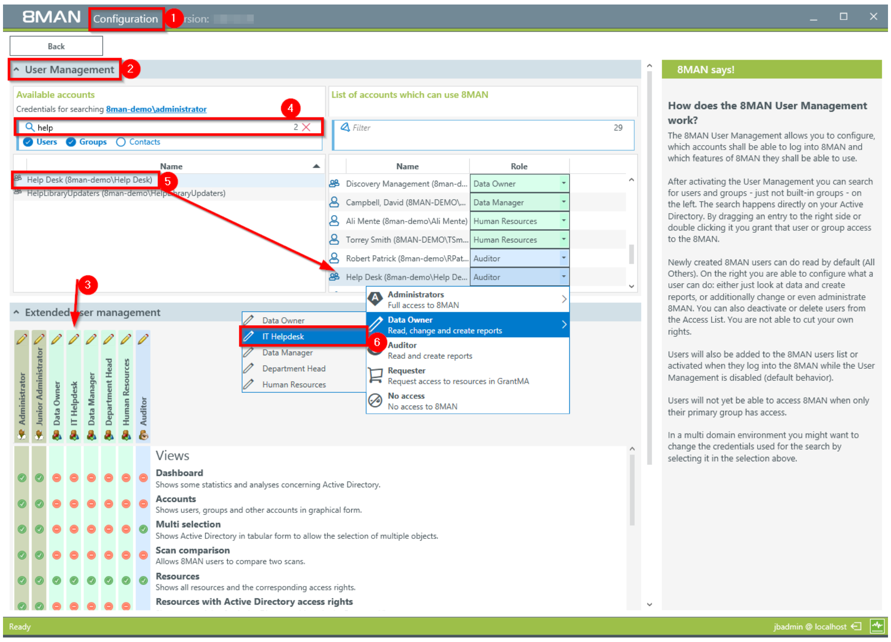
7.1.3.2 Assigning responsibilities to help desk employees

Background / Value

8MAN allows you to define very specific responsibilities to individual help desk employees. The following example shows a typical assignment of responsibilities.

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

Step by step process



Name	Role
Discovery Management (8man-d...	Data Owner
Campbell, David (8MAN-DEMO\...	Data Manager
Ali Mente (8man-demo\Ali Mente)	Human Resources
Torrey Smith (8MAN-DEMO\TSm...	Human Resources
Robert Patrick (8man-demo\RPat...	Auditor
Help Desk (8man-demo\Help De...	Auditor

Views

Dashboard
Shows some statistics and analyses concerning Active Directory.

Accounts
Shows users, groups and other accounts in graphical form.

Multi selection
Shows Active Directory in tabular form to allow the selection of multiple objects.

Scan comparison
Allows 8MAN users to compare two scans.

Resources
Shows all resources and the corresponding access rights.

Resources with Active Directory access rights

How does the 8MAN User Management work?

The 8MAN User Management allows you to configure, which accounts shall be able to log into 8MAN and which features of 8MAN they shall be able to use.

After activating the User Management you can search for users and groups - just not built-in groups - on the left. The search happens directly on your Active Directory. By dragging an entry to the right side or double clicking it you grant that user or group access to the 8MAN.

Newly created 8MAN users can do read by default (All Others). On the right you are able to configure what a user can do: either just look at data and create reports, or additionally change or even administrate 8MAN. You can also deactivate or delete users from the Access List. You are not able to cut your own rights.

Users will also be added to the 8MAN users list or activated when they log into the 8MAN while the User Management is disabled (default behavior).

Users will not yet be able to access 8MAN when only their primary group has access.

In a multi domain environment you might want to change the credentials used for the search by selecting it in the selection above.

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

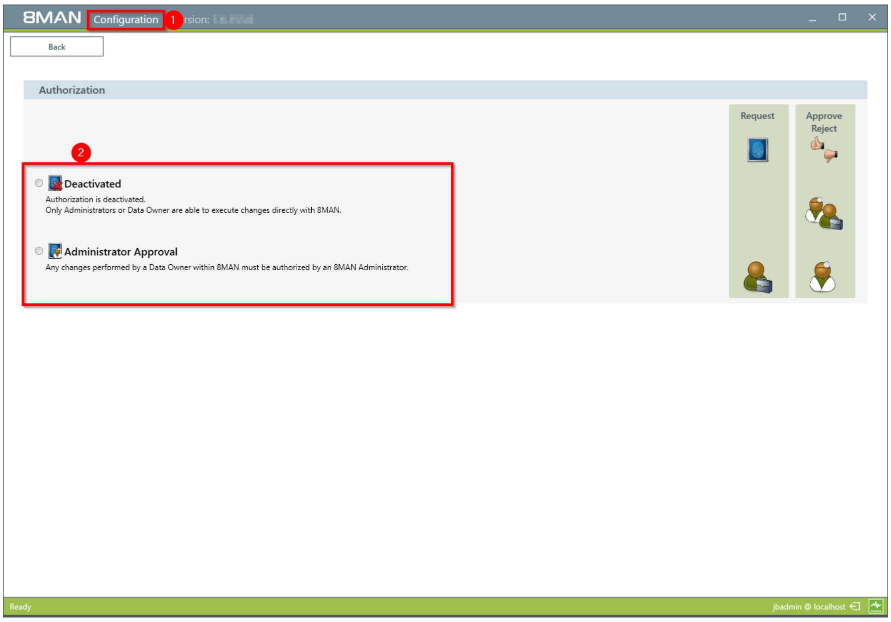
7.2 Creating approval processes

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

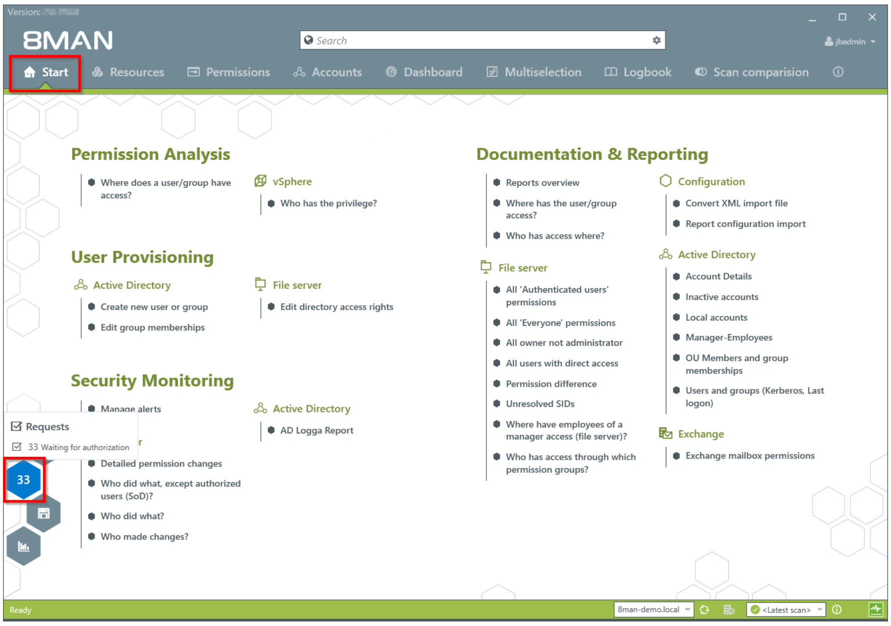


○ Deactivated
Authorization is deactivated.
Only Administrators or Data Owner are able to execute changes directly with 8MAN.

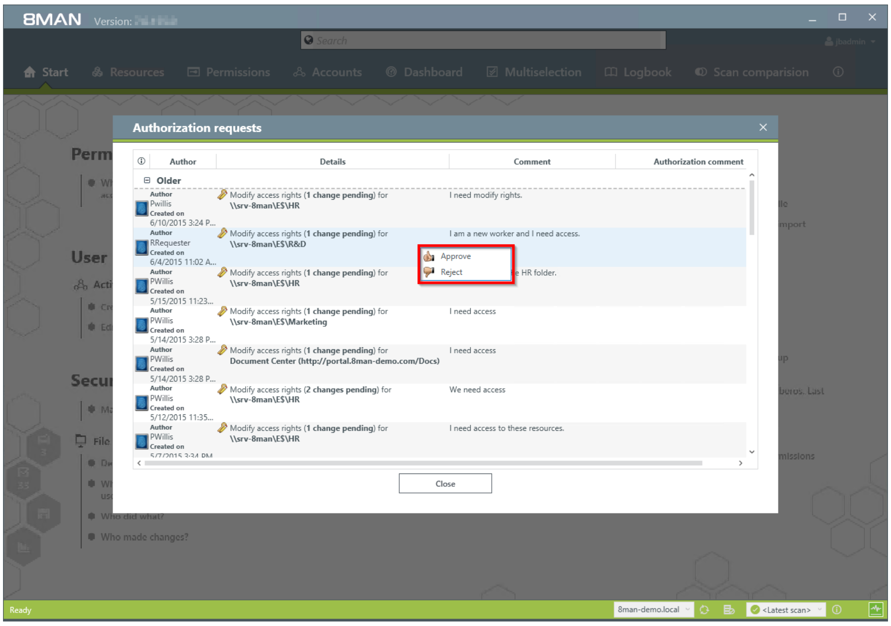
○ Administrator Approval
Any changes performed by a Data Owner within 8MAN must be authorized by an 8MAN Administrator.

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

Activate or deactivate the administrator approval mode.



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

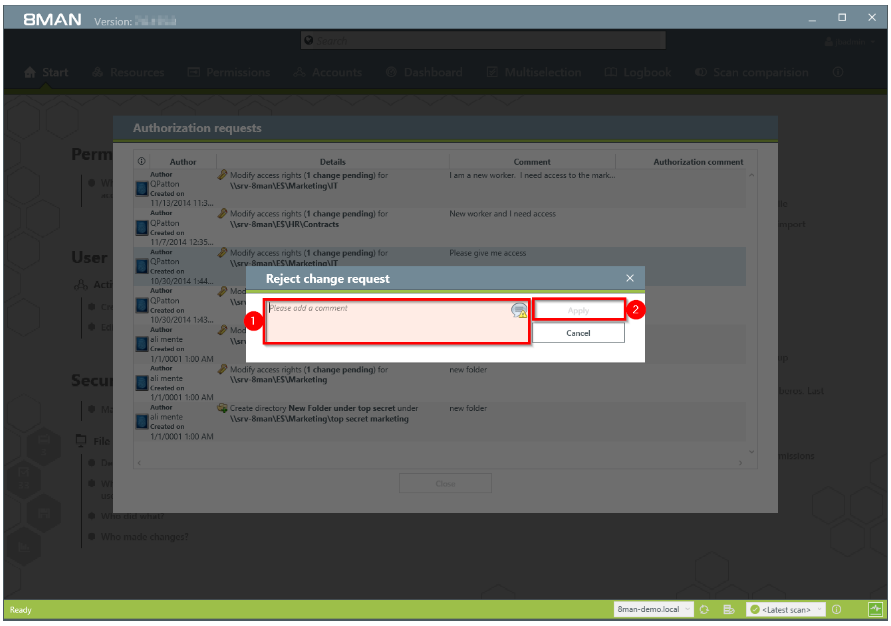


Authorization requests

Older

Author	Details	Comment	Authorization comment
Author Pwillis Created on 6/10/2015 3:24 P...	Modify access rights (**1 change pending**) for **\\srv-8man\E$\HR**	I need modify rights.	
Author RRequester Created on 6/4/2015 11:02 A...	Modify access rights (**1 change pending**) for **\\srv-8man\E$\R&D**	I am a new worker and I need access.	
Author PWillis Created on 5/15/2015 11:23...	Modify access rights (**1 change pending**) for **\\srv-8man\E$\HR**	e HR folder.	
Author PWillis Created on 5/14/2015 3:28 P...	Modify access rights (**1 change pending**) for **\\srv-8man\E$\Marketing**	I need access	
Author PWillis Created on 5/14/2015 3:28 P...	Modify access rights (**1 change pending**) for **Document Center (http://portal.8man-demo.com/Docs)**	I need access	
Author PWillis Created on 5/12/2015 11:35...	Modify access rights (**2 changes pending**) for **\\srv-8man\E$\HR**	We need access	
Author PWillis Created on 5/7/2015 3:34 PM	Modify access rights (**1 change pending**) for **\\srv-8man\E$\HR**	I need access to these resources.	

Right click on a request and make your decision.



Authorization requests

Author	Details	Comment	Authorization comment
Author QPatton Created on 11/13/2014 11:3...	Modify access rights (**1 change pending**) for **\\srv-8man\E$\Marketing\IT**	I am a new worker. I need access to the mark...	
Author QPatton Created on 11/7/2014 12:35...	Modify access rights (**1 change pending**) for **\\srv-8man\E$\HR\Contracts**	New worker and I need access	
Author QPatton Created on 10/30/2014 1:44...	Modify access rights (**1 change pending**) for **\\srv-8man\E$\Marketing\IT**	Please give me access	
Author QPatton Created on 10/30/2014 1:43...	Mod \\srv		
Author ali mente Created on 1/1/0001 1:00 AM	Mod \\srv		
Author ali mente Created on 1/1/0001 1:00 AM	Modify access rights (**1 change pending**) for **\\srv-8man\E$\Marketing**	new folder	
Author ali mente Created on 1/1/0001 1:00 AM	Create directory **New Folder under top secret** under **\\srv-8man\E$\Marketing\top secret marketing**	new folder	

Reject change request

1 Please add a comment

2 Apply

Cancel

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

7.2.2 +8MATE GrantMA: Designing 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 generally doesn't know you should have which access rights.

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.

7.2.2.1 Ressourcenverantwortliche im Webclient definieren

Background / Value

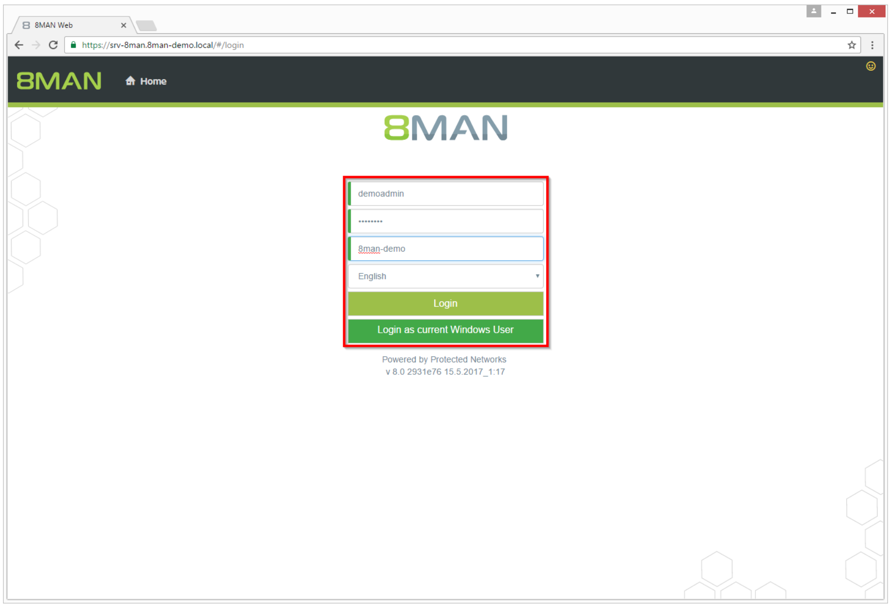
With version 8.0 8MAN releases new features to move the GrantMA configuration into the web client. We inserted the new role "Resource Owner". Assign this role completely using the web client. Due to the requirements of our customers we designed a direct assignment between the Resource Owner and the resource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

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

Additional Services

Defining individual approval workflows

Step by step process



https://srv-8man.8man-demo.local/#/login

demoadmin

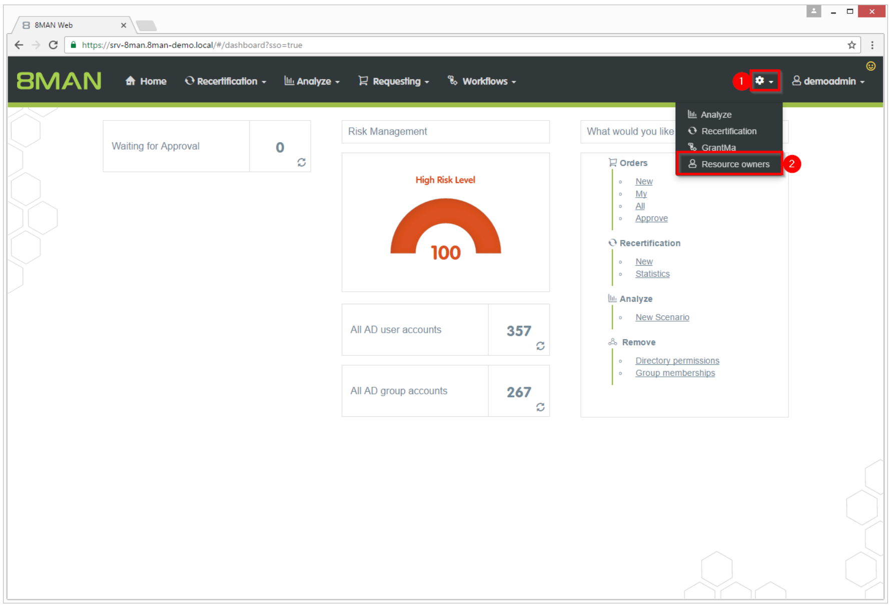
••••••••

8man-demo

English

Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

Login to the web interface with admin credentials.



https://srv-8man.8man-demo.local/#/dashboard?sso=true

Waiting for Approval 0

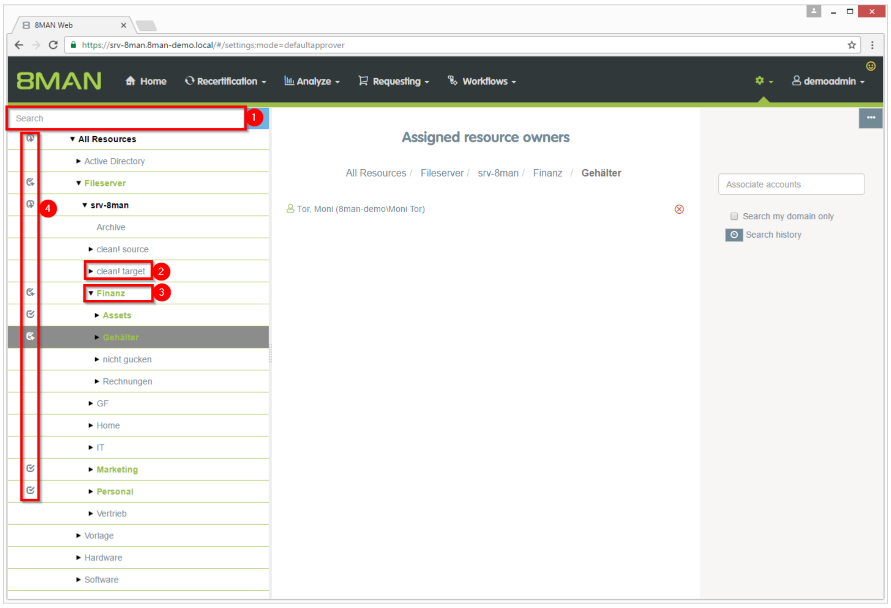
Risk Management

High Risk Level 100

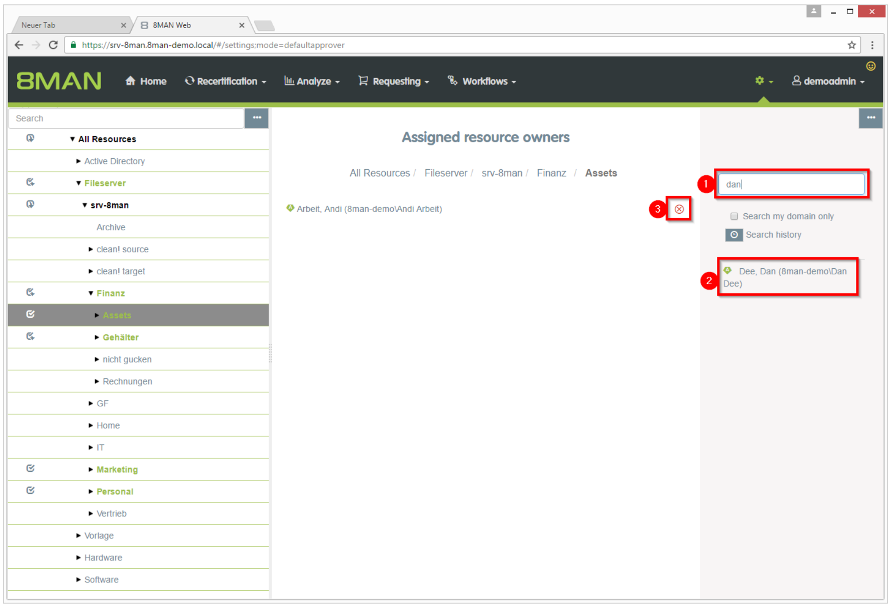
All AD user accounts 357

All AD group accounts 267

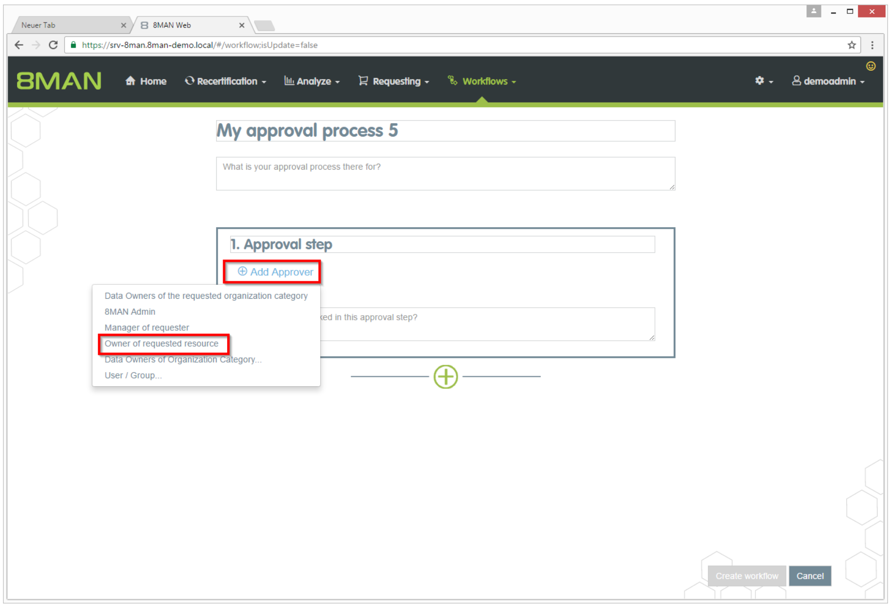
1. *Click the gear-wheel.*
2. *Select "Resource owners".*



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



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



Neuer Tab
8MAN Web
https://srv-8man.8man-demo.local/#/workflow;isUpdate=false
8MAN
Home
Recertification
Analyze
Requesting
Workflows
demoadmin

My approval process 5

What is your approval process there for?

1. Approval step

Add Approver
Data Owners of the requested organization category
8MAN Admin
Manager of requester
Owner of requested resource
Data Owners of Organization Category...
User / Group...
ked in this approval step?
Create workflow
Cancel

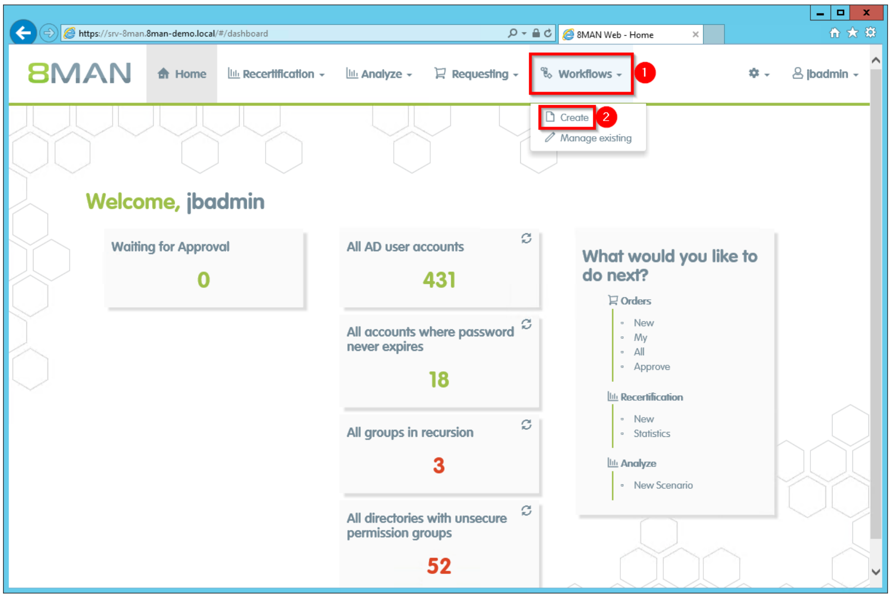
Design individual workflows with the new role resource owner as an approver.

7.2.2.2 Defining individual approval workflows

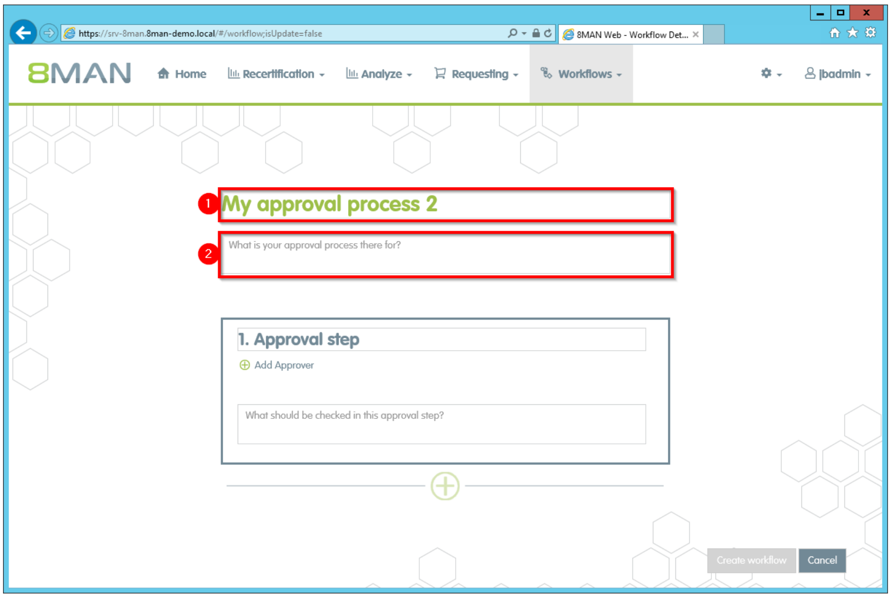
Background / Value

8MATE GrantMA allows you to design individual approval workflows for each organizational category. You can design as many steps in the process as required. The last approver in the process is also the one making the formal change request.

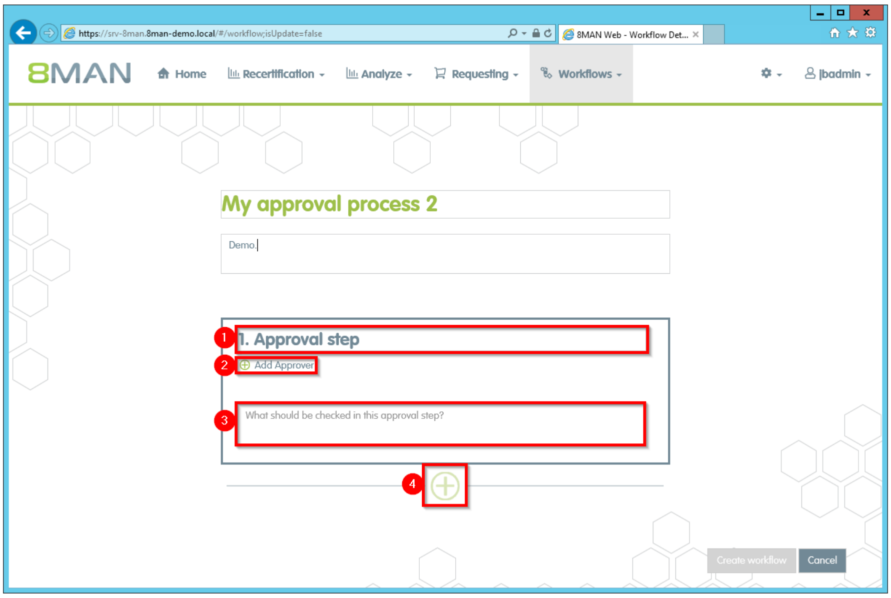
Step by step process



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


https://srv-8man.8man-demo.local/#/workflow;isUpdate=false
8MAN Web - Workflow Det...
8MAN
Home
Recertification
Analyze
Requesting
Workflows
jbadmin
1
My approval process 2
2
What is your approval process there for?
1. Approval step
Add Approver
What should be checked in this approval step?
Create workflow
Cancel

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



My approval process 2

Demo.

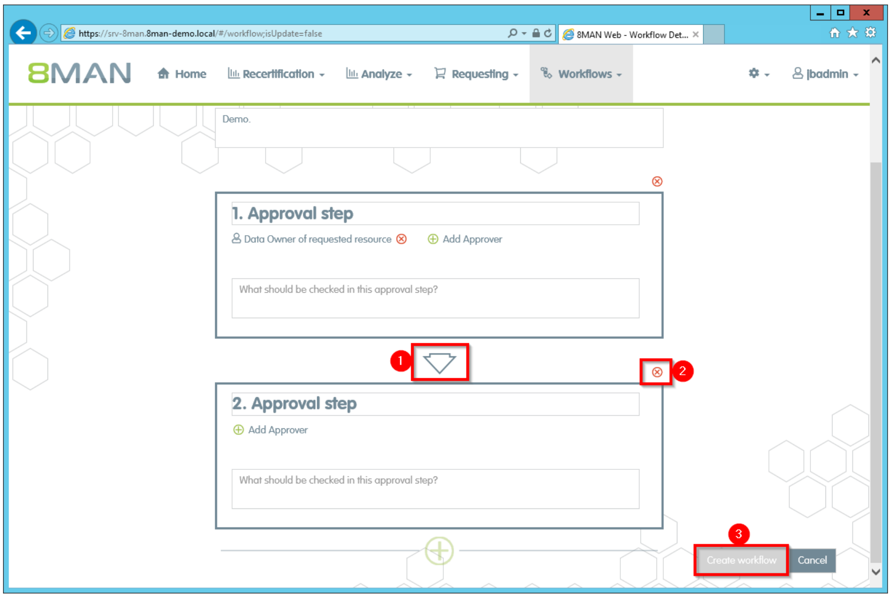
1. Approval step

What should be checked in this approval step?

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.*



Demo.

1. Approval step

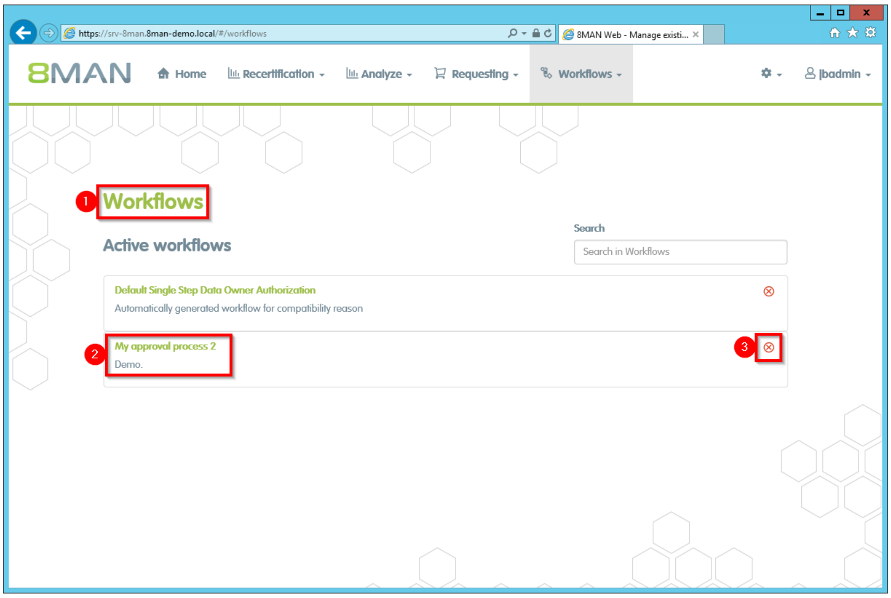
Data Owner of requested resource

What should be checked in this approval step?

2. Approval step

What should be checked in this approval step?

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


https://srv-8man.8man-demo.local/#/workflows
8MAN Web - Manage existi...
8MAN
Home
Recertification
Analyze
Requesting
Workflows
jbadmin
1
Workflows
Active workflows
Search
Search in Workflows
Default Single Step Data Owner Authorization
Automatically generated workflow for compatibility reason
2
My approval process 2
Demo.
3

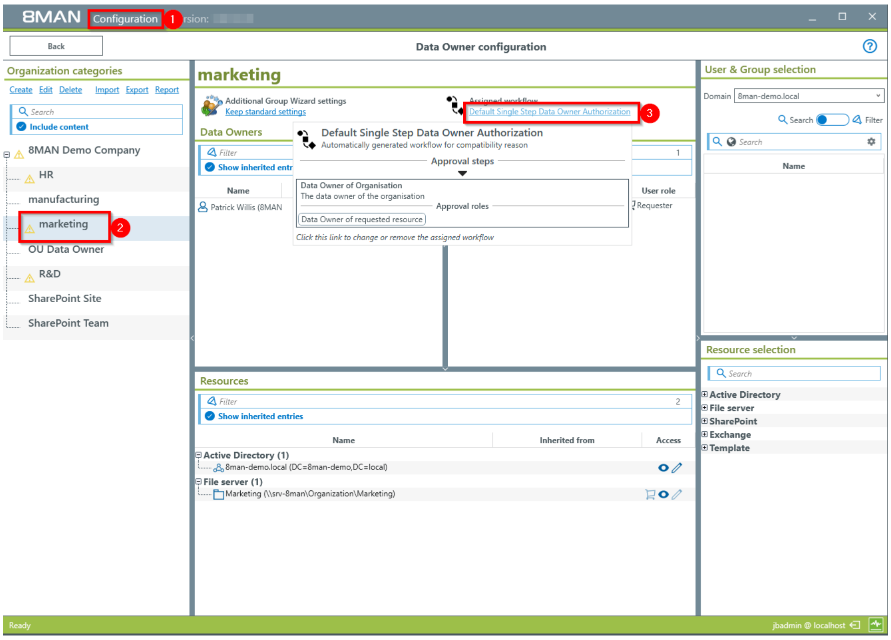
1. You have created a new workflow. 8MAN switches to the "Manage workflows" view.
2. Click on a workflow to make changes.
3. Delete the workflow.

7.2.2.3 Assigning approval workflows to individual resources

Background / Value

Connecting available resources with individual workflows.

Step by step process



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

7.3 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.

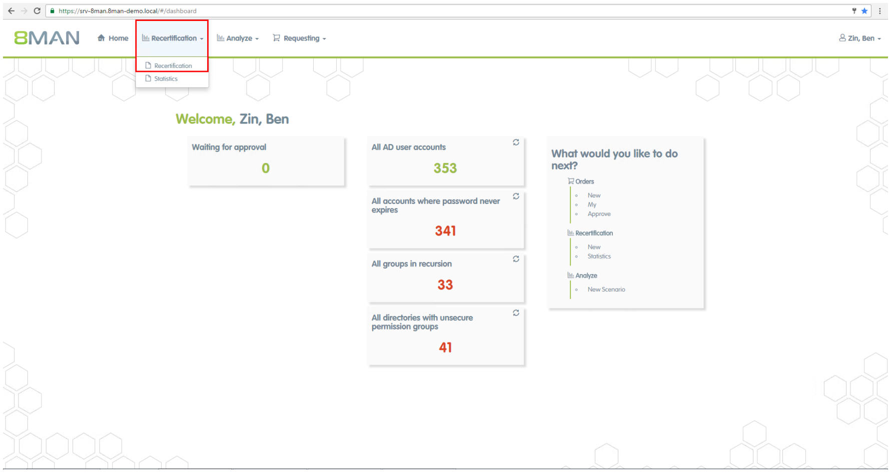
You receive an e-mail with the instructions to the re-certification process. Then you decide for each user and resource if the access right should stay or be removed.

Your desired changes will be transferred automatically to the administrator.

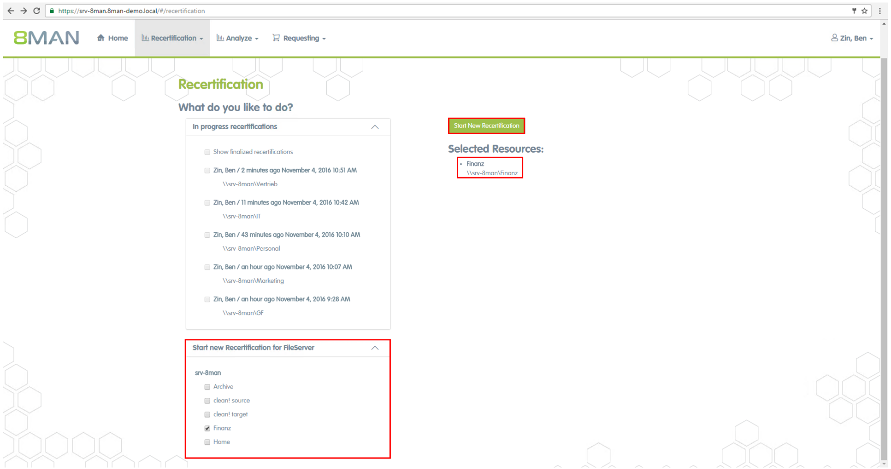
Complementary Services

[Change file server access rights]

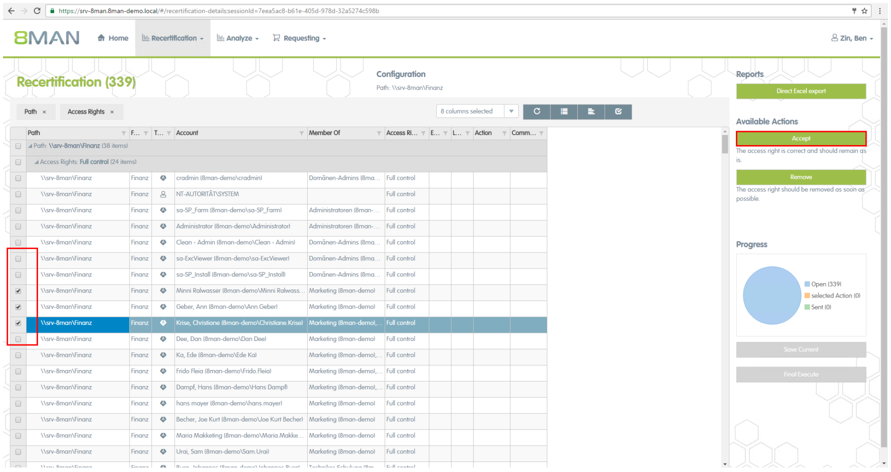
The process in single steps



Click on "Recertification".


https://srv-8man.8man-demo.local/#/recertification
8MAN
Home
Recertification
Analyze
Requesting
Zin, Ben
Recertification
What do you like to do?
In progress recertifications
Show finalized recertifications
Zin, Ben / 2 minutes ago November 4, 2016 10:51 AM
\\srv-8man\Vertrieb
Zin, Ben / 11 minutes ago November 4, 2016 10:42 AM
\\srv-8man\IT
Zin, Ben / 43 minutes ago November 4, 2016 10:10 AM
\\srv-8man\Personal
Zin, Ben / an hour ago November 4, 2016 10:07 AM
\\srv-8man\Marketing
Zin, Ben / an hour ago November 4, 2016 9:28 AM
\\srv-8man\GF
Start new Recertification for FileServer
srv-8man
Archive
clean! source
clean! target
Finanz
Home
Start New Recertification
Selected Resources:
Finanz
\\srv-8man\Finanz

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



https://srv-8man.8man-demo.local/#/recertification-details;sessionId=7eea5ac8-b61e-405d-978d-32a5274c598b

Recertification (339)

Configuration
Path: \\srv-8man\Finanz

	Path	F...	T...	Account	Member Of	Access Ri...	E...	L...	Action	Comm...
□	Path: \\srv-8man\Finanz (38 items)									
□	Access Rights: Full control (24 items)									
□	\\srv-8man\Finanz	Finanz	👥	cradmin (8man-demo\cradmin)	Domänen-Admins (8ma…	Full control				
□	\\srv-8man\Finanz	Finanz	👤	NT-AUTORITÄT\SYSTEM		Full control				
□	\\srv-8man\Finanz	Finanz	👥	sa-SP_Farm (8man-demo\sa-SP_Farm)	Administratoren (8man-…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Administrator (8man-demo\Administrator)	Administratoren (8man-…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Clean - Admin (8man-demo\Clean - Admin)	Domänen-Admins (8ma…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	sa-ExcViewer (8man-demo\sa-ExcViewer)	Domänen-Admins (8ma…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	sa-SP_Install (8man-demo\sa-SP_Install)	Domänen-Admins (8ma…	Full control				
☑	\\srv-8man\Finanz	Finanz	👥	Minni Ralwasser (8man-demo\Minni Ralwass…	Marketing (8man-demo)	Full control				
☑	\\srv-8man\Finanz	Finanz	👥	Geber, Ann (8man-demo\Ann.Geber)	Marketing (8man-demo)	Full control				
☑	\\srv-8man\Finanz	Finanz	👥	Krise, Christiane (8man-demo\Christiane.Krise)	Marketing (8man-demo),…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Dee, Dan (8man-demo\Dan Dee)	Marketing (8man-demo)	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Ka, Ede (8man-demo\Ede Ka)	Marketing (8man-demo),…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Frido Fleia (8man-demo\Frido.Fleia)	Marketing (8man-demo),…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Dampf, Hans (8man-demo\Hans Dampf)	Marketing (8man-demo),…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	hans mayer (8man-demo\hans.mayer)	Marketing (8man-demo)	Full control				
□	\\srv-8man\Finanz	Finanz	👥	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	👥	Urai, Sam (8man-demo\Sam.Urai)	Marketing (8man-demo)	Full control				

Reports

Available Actions

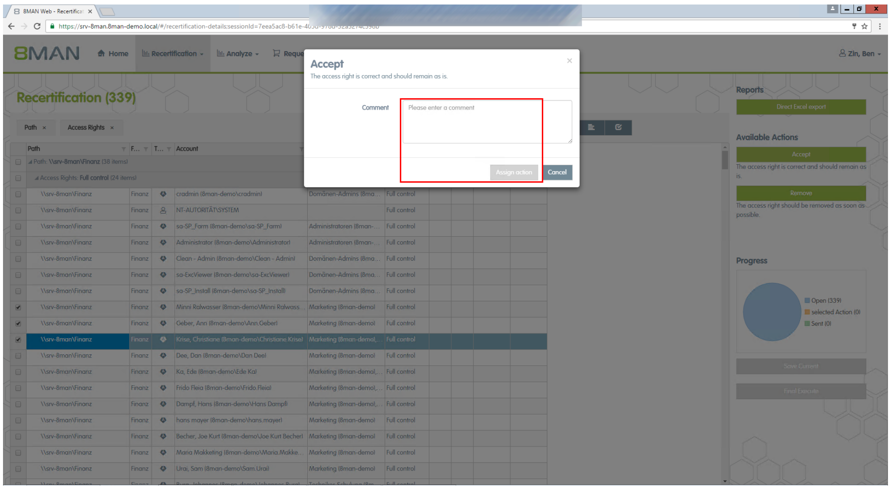
The access right is correct and should remain as is.

The access right should be removed as soon as possible.

Progress

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.



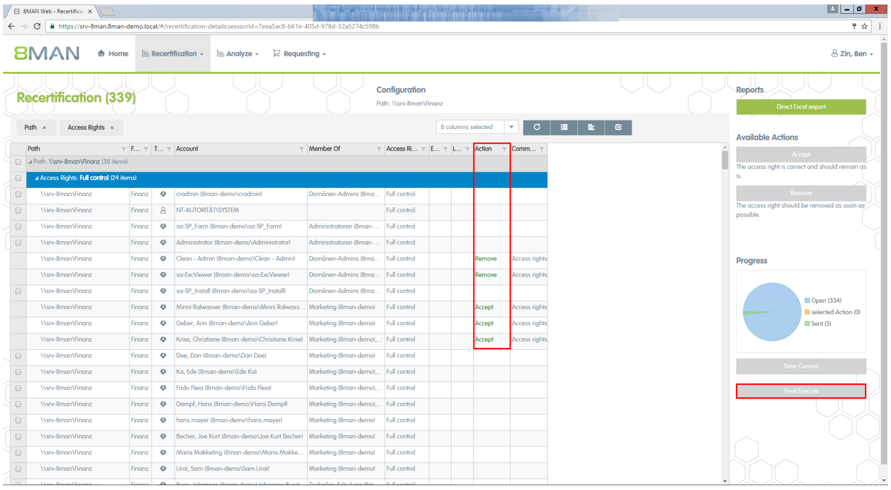
https://srv-8man.8man-demo.local/#/recertification-details;sessionId=7eea5ac8-b61e-405d-978d-32a5274c598b

Accept

The access right is correct and should remain as is.

Comment: Please enter a comment

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



https://srv-8man.8man-demo.local/#/recertification-details;sessionId=7eea5ac8-b61e-405d-978d-32a5274c598b

Recertification (339)

Configuration
Path: \\srv-8man\Finanz

	Path	F...	T...	Account	Member Of	Access Ri...	E...	L...	Action	Comm...
□	Path: \\srv-8man\Finanz (38 items)									
□	Access Rights: Full control (24 items)									
□	\\srv-8man\Finanz	Finanz	👥	cradmin (8man-demo\cradmin)	Domänen-Admins (8ma…	Full control				
□	\\srv-8man\Finanz	Finanz	👤	NT-AUTORITÄT\SYSTEM		Full control				
□	\\srv-8man\Finanz	Finanz	👥	sa-SP_Farm (8man-demo\sa-SP_Farm)	Administratoren (8man-…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Administrator (8man-demo\Administrator)	Administratoren (8man-…	Full control				
	\\srv-8man\Finanz	Finanz	👥	Clean - Admin (8man-demo\Clean - Admin)	Domänen-Admins (8ma…	Full control			Remove	Access rights
	\\srv-8man\Finanz	Finanz	👥	sa-ExcViewer (8man-demo\sa-ExcViewer)	Domänen-Admins (8ma…	Full control			Remove	Access rights
□	\\srv-8man\Finanz	Finanz	👥	sa-SP_Install (8man-demo\sa-SP_Install)	Domänen-Admins (8ma…	Full control				
	\\srv-8man\Finanz	Finanz	👥	Minni Ralwasser (8man-demo\Minni Ralwass…	Marketing (8man-demo)	Full control			Accept	Access rights
	\\srv-8man\Finanz	Finanz	👥	Geber, Ann (8man-demo\Ann.Geber)	Marketing (8man-demo)	Full control			Accept	Access rights
	\\srv-8man\Finanz	Finanz	👥	Krise, Christiane (8man-demo\Christiane.Krise)	Marketing (8man-demo),…	Full control			Accept	Access rights
□	\\srv-8man\Finanz	Finanz	👥	Dee, Dan (8man-demo\Dan Dee)	Marketing (8man-demo)	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Ka, Ede (8man-demo\Ede Ka)	Marketing (8man-demo),…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Frido Fleia (8man-demo\Frido.Fleia)	Marketing (8man-demo),…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	Dampf, Hans (8man-demo\Hans Dampf)	Marketing (8man-demo),…	Full control				
□	\\srv-8man\Finanz	Finanz	👥	hans mayer (8man-demo\hans.mayer)	Marketing (8man-demo)	Full control				
□	\\srv-8man\Finanz	Finanz	👥	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	👥	Urai, Sam (8man-demo\Sam.Urai)	Marketing (8man-demo)	Full control				

Reports

Available Actions

The access right is correct and should remain as is.

The access right should be removed as soon as possible.

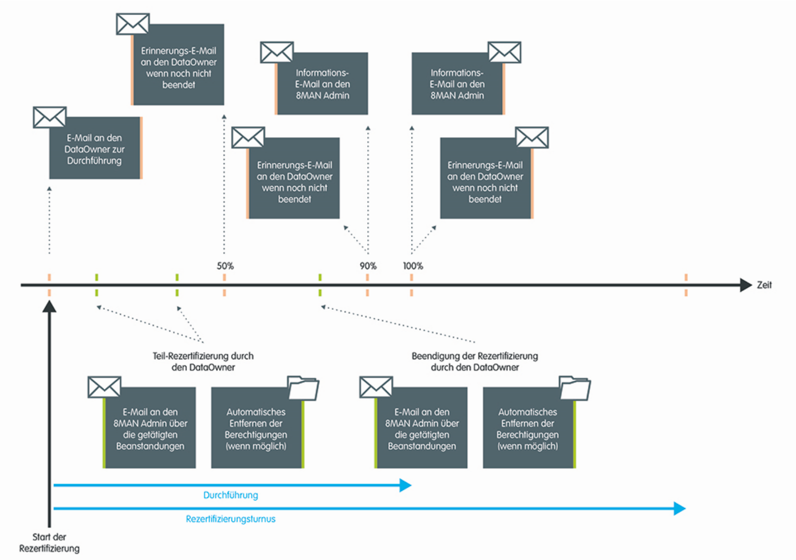
Progress

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.

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

7.3.1 E-mail notifications for recertification


Erinnerungs-E-Mail an den DataOwner wenn noch nicht beendet
E-Mail an den DataOwner zur Durchführung
Informations-E-Mail an den 8MAN Admin
Erinnerungs-E-Mail an den DataOwner wenn noch nicht beendet
Informations-E-Mail an den 8MAN Admin
Erinnerungs-E-Mail an den DataOwner wenn noch nicht beendet
50%
90%
100%
Zeit
Teil-Rezertifizierung durch den DataOwner
Beendigung der Rezertifizierung durch den DataOwner
E-Mail an den 8MAN Admin über die getätigten Beanstandungen
Automatisches Entfernen der Berechtigungen (wenn möglich)
E-Mail an den 8MAN Admin über die getätigten Beanstandungen
Automatisches Entfernen der Berechtigungen (wenn möglich)
Durchführung
Rezertifizierungsturnus
Start der Rezertifizierung

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 Requesting file server access rights from Data Owners

Background / Value

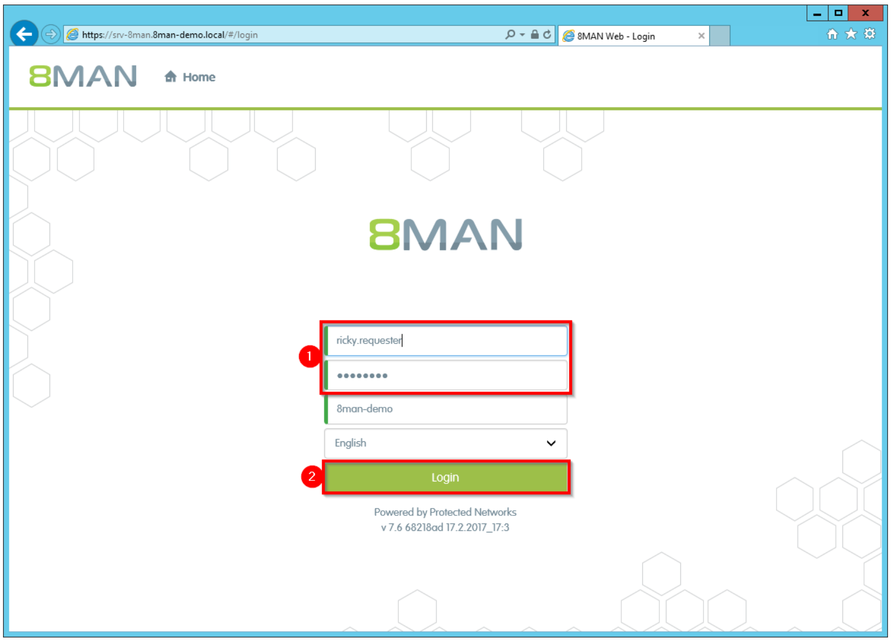
Employees can request access rights to file server directories from Data Owners by using the 8MATE GrantMA self-service portal.

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

Additional Services

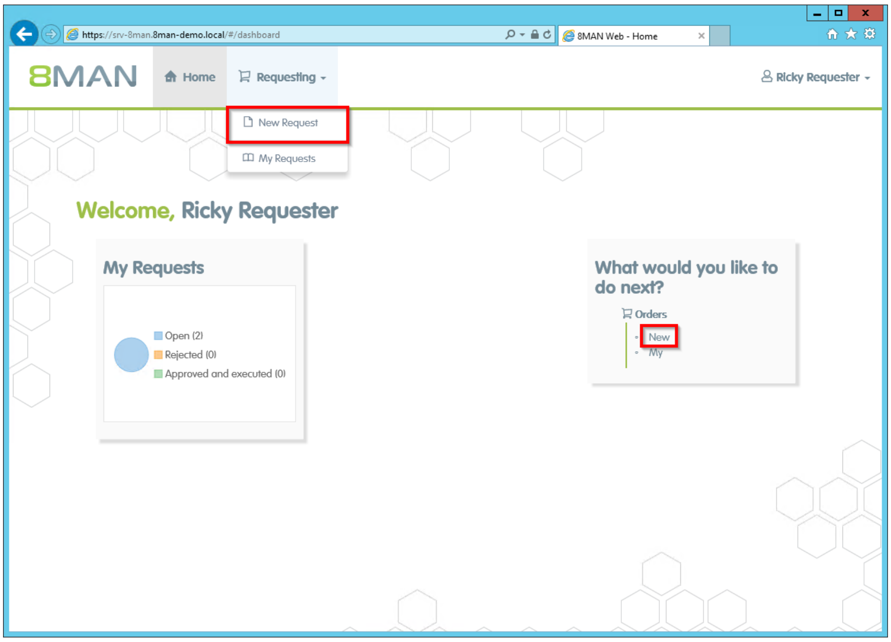
Creating approval workflows

Step by step process


https://srv-8man.8man-demo.local/#/login
8MAN Web - Login
8MAN
Home
8MAN
1
ricky.requester
••••••••
8man-demo
English
2
Login
Powered by Protected Networks
v 7.6 68218ad 17.2.2017_17:3

1. Enter your username and password.

2. Click on "Login".

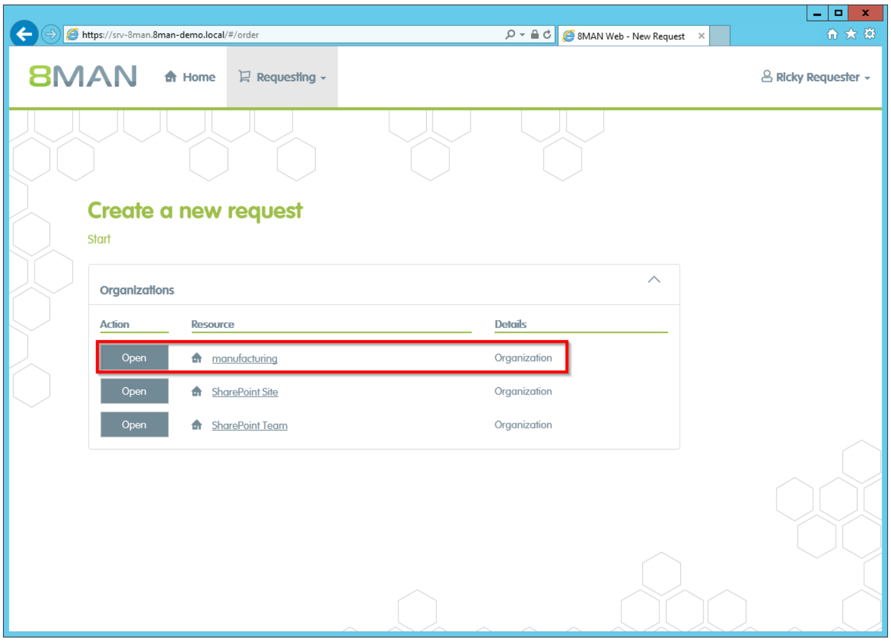


Welcome, Ricky Requester

My Requests

What would you like to do next?

Click on "New Request".



Create a new request

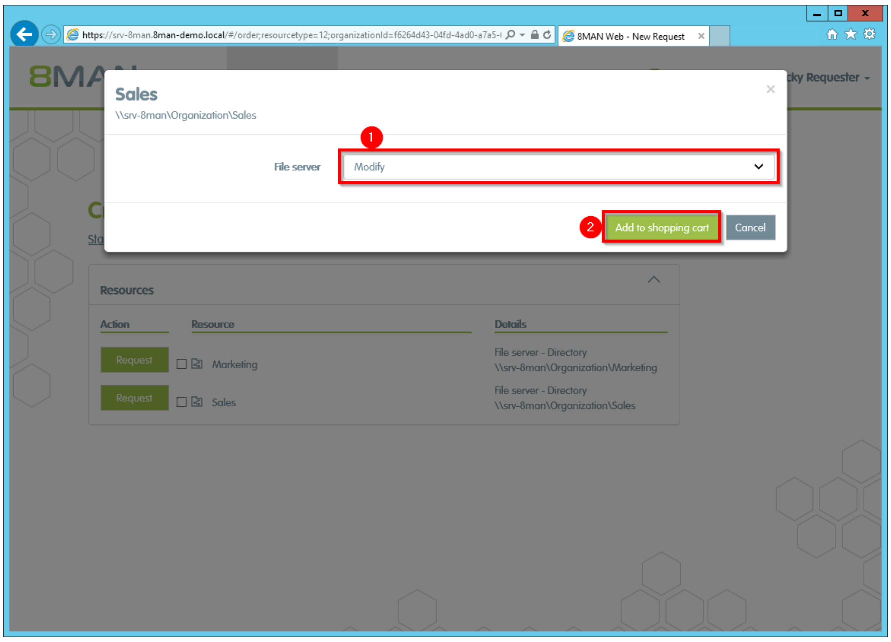
Start

Organizations

Action	Resource	Details
Open	manufacturing	Organization
Open	SharePoint Site	Organization
Open	SharePoint Team	Organization

8MAN will show the person requesting access to new resources the exact resources that are available to them.

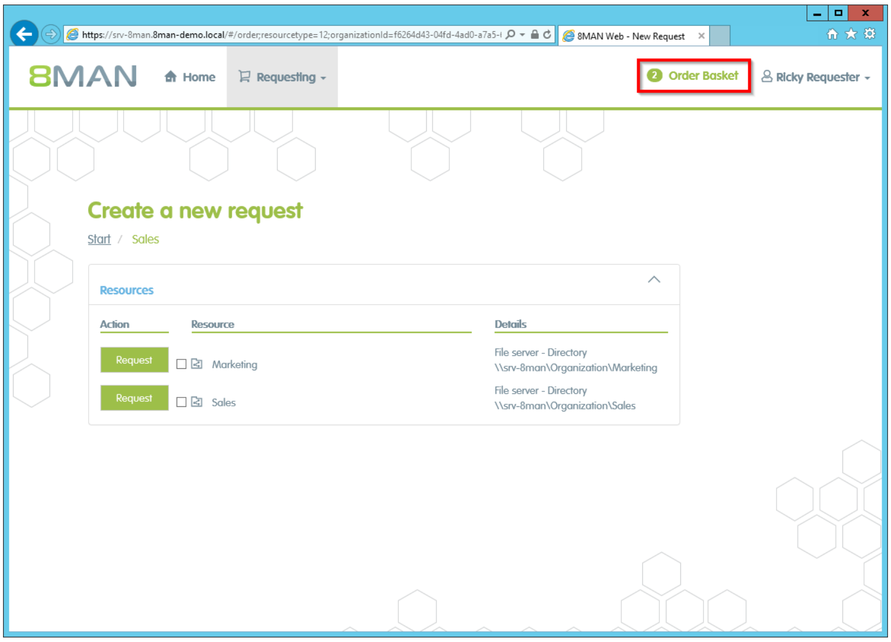
Select the desired resource and click on "order".



https://srv-8man.8man-demo.local/#/order;resourcetype=12;organizationId=f6264d43-04fd-4ad0-a7a5-
8MAN Web - New Request
Sales
\\srv-8man\Organization\Sales
1
File server
Modify
2
Add to shopping cart
Cancel
Resources
Action
Resource
Details
Request
Marketing
File server - Directory
\\srv-8man\Organization\Marketing
Request
Sales
File server - Directory
\\srv-8man\Organization\Sales

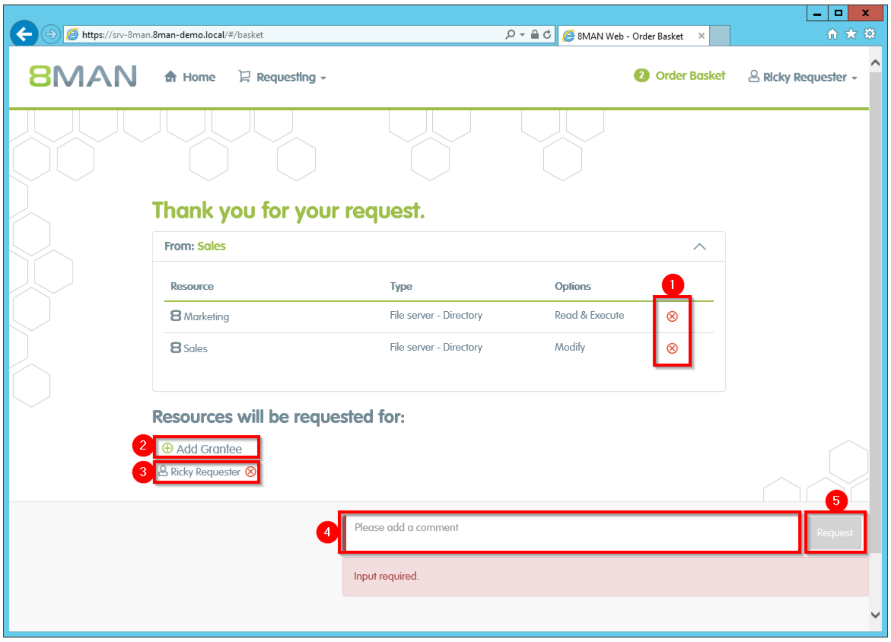
1. Select an access category.

2. Click "add to shopping cart".



Add additional resources if desired.

Click on "Order Basket".



Thank you for your request.

From: Sales

Resource	Type	Options
Marketing	File server - Directory	Read & Execute
Sales	File server - Directory	Modify

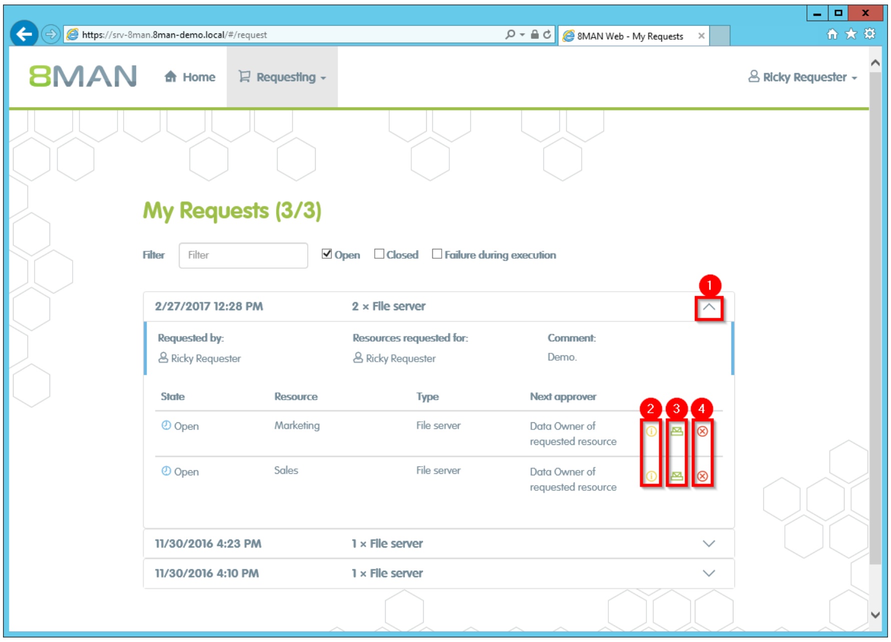
Resources will be requested for:

Ricky Requester

Please add a comment

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.*



My Requests (3/3)

Filter: Filter ☑ Open ☐ Closed ☐ Failure during execution

2/27/2017 12:28 PM 2 × File server

Requested by: Ricky Requester

Resources requested for: Ricky Requester

Comment: Demo.

State	Resource	Type	Next approver
Open	Marketing	File server	Data Owner of requested resource
Open	Sales	File server	Data Owner of requested resource

11/30/2016 4:23 PM 1 × File server

11/30/2016 4:10 PM 1 × File server

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.*

7.4.2 Requesting directories

Background / Value

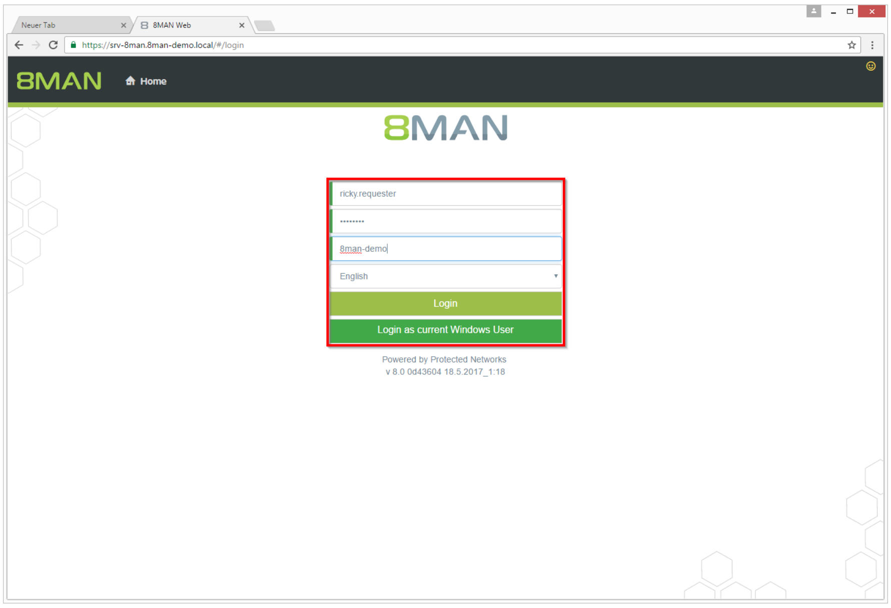
Order new directories using the GrantMA self service portal. This feature is useful for companies that follow restrictive policies for directory creation. We recommend that you allow the creation of directories up to the level three or four below the share only after requesting and approving.

Find resources quickly with the search.

Additional Services

Requesting file server permissions from the data owner

Step by step process


https://srv-8man.8man-demo.local/#/login

ricky.requester

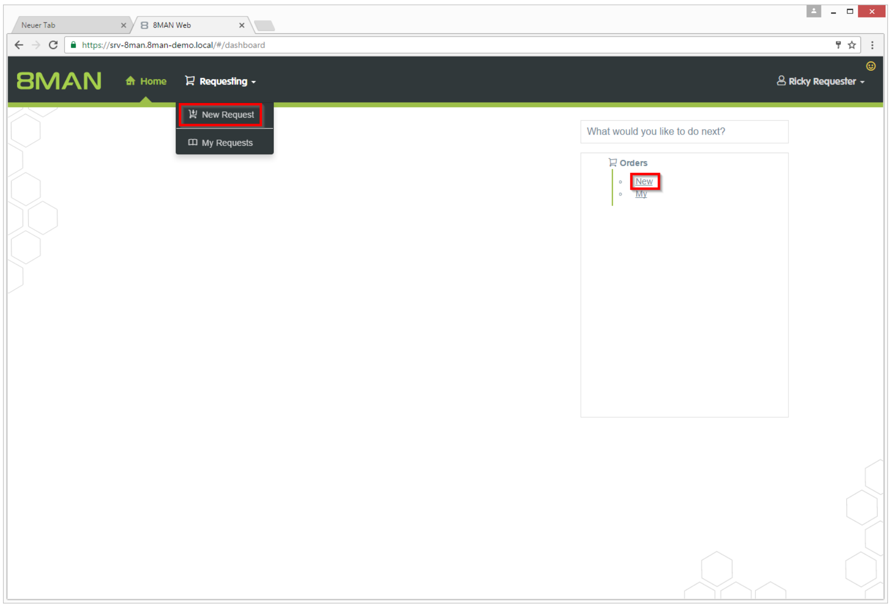
••••••••

8man-demo

English

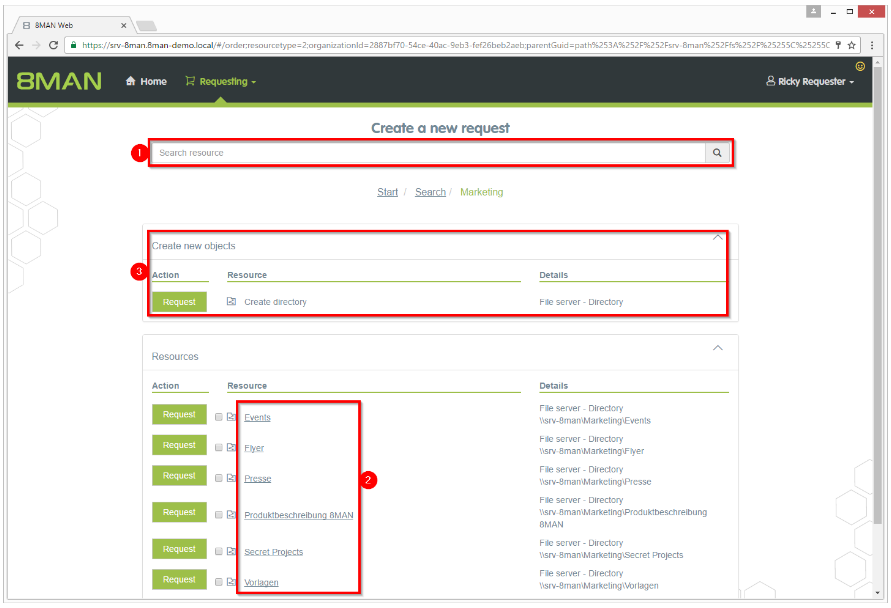
Neuer Tab
8MAN Web
8MAN
Home
8MAN
Login
Login as current Windows User
Powered by Protected Networks
v 8.0 0d43604 18.5.2017_1:18

Log in as the requester.


https://srv-8man.8man-demo.local/#/dashboard

What would you like to do next?

Start a new request.



8MAN Web
https://srv-8man.8man-demo.local/#/order;resourcetype=2;organizationId=2887bf70-54ce-40ac-9eb3-fef26beb2aeb;parentGuid=path%253A%252F%252Fsrv-8man%252Ffs%252F%25255C%25255C
8MAN
Home
Requesting
Ricky Requester
1
2
3

Create a new request

Search resource

Start / Search / Marketing

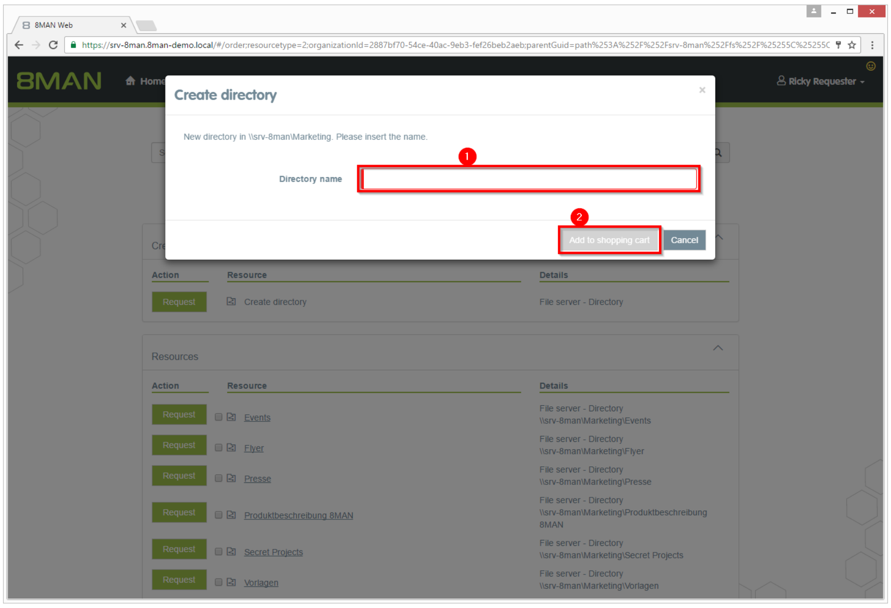
Create new objects

Action	Resource	Details
Request	Create directory	File server - Directory

Resources

Action	Resource	Details
Request	□ Events	File server - Directory \\srv-8man\Marketing\Events
Request	□ Flyer	File server - Directory \\srv-8man\Marketing\Flyer
Request	□ Presse	File server - Directory \\srv-8man\Marketing\Presse
Request	□ Produktbeschreibung 8MAN	File server - Directory \\srv-8man\Marketing\Produktbeschreibung 8MAN
Request	□ Secret Projects	File server - Directory \\srv-8man\Marketing\Secret Projects
Request	□ Vorlagen	File server - Directory \\srv-8man\Marketing\Vorlagen

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



8MAN Web
https://srv-8man.8man-demo.local/#/order;resourcetype=2;organizationId=2887bf70-54ce-40ac-9eb3-fef26beb2aeb;parentGuid=path%253A%252F%252Fsrv-8man%252Ffs%252F%25255C%25255C
8MAN
Home
Ricky Requester
1
2

Create directory

New directory in \\srv-8man\Marketing. Please insert the name.

Directory name

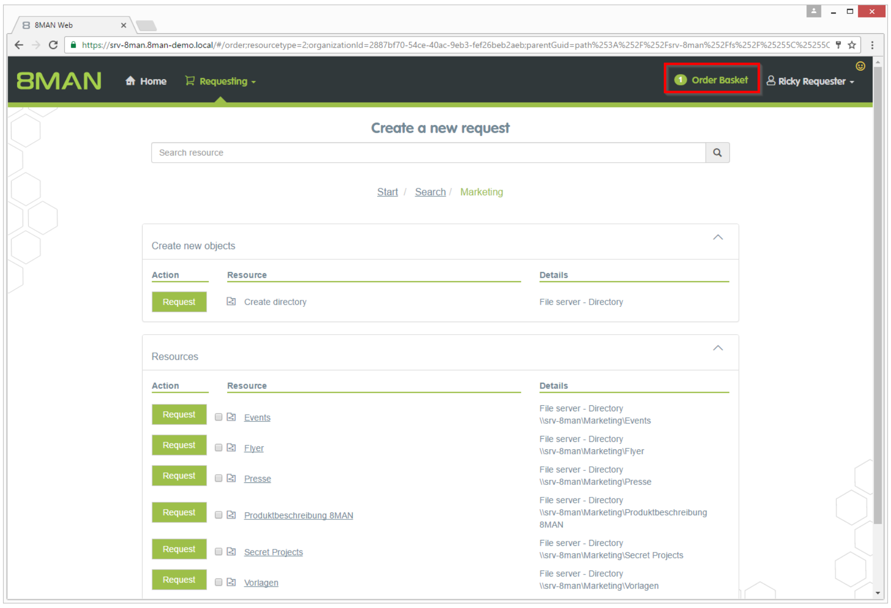
Add to shopping cart | Cancel

Action	Resource	Details
Request	Create directory	File server - Directory

Resources

Action	Resource	Details
Request	□ Events	File server - Directory \\srv-8man\Marketing\Events
Request	□ Flyer	File server - Directory \\srv-8man\Marketing\Flyer
Request	□ Presse	File server - Directory \\srv-8man\Marketing\Presse
Request	□ Produktbeschreibung 8MAN	File server - Directory \\srv-8man\Marketing\Produktbeschreibung 8MAN
Request	□ Secret Projects	File server - Directory \\srv-8man\Marketing\Secret Projects
Request	□ Vorlagen	File server - Directory \\srv-8man\Marketing\Vorlagen

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


8MAN Web
https://srv-8man.8man-demo.local/#/order;resourcetype=2;organizationId=2887bf70-54ce-40ac-9eb3-fef26beb2aeb;parentGuid=path%253A%252F%252Fsrv-8man%252Ffs%252F%25255C%25255C
8MAN
Home
Requesting
1 Order Basket
Ricky Requester

Create a new request

Search resource

Start / Search / Marketing

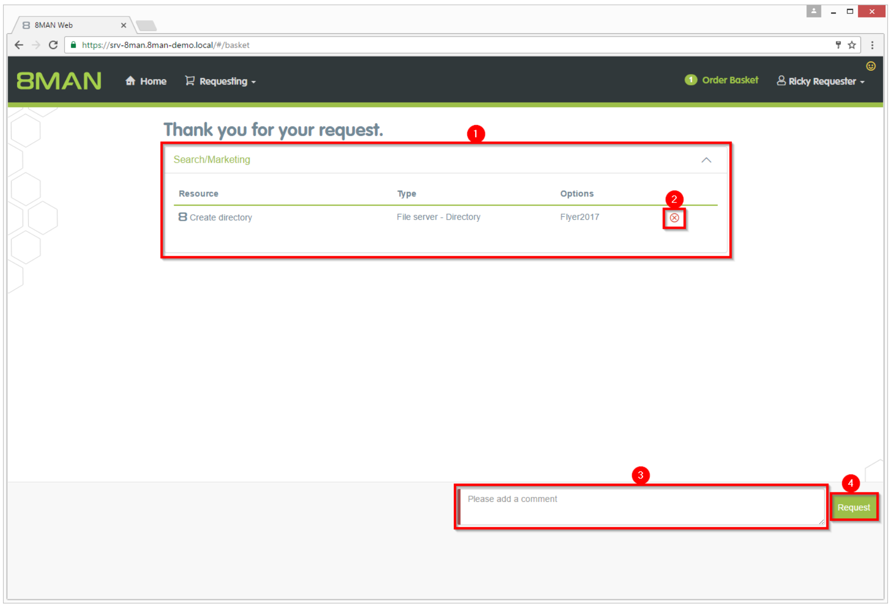
Create new objects

Action	Resource	Details
Request	Create directory	File server - Directory

Resources

Action	Resource	Details
Request	□ Events	File server - Directory \\srv-8man\Marketing\Events
Request	□ Flyer	File server - Directory \\srv-8man\Marketing\Flyer
Request	□ Presse	File server - Directory \\srv-8man\Marketing\Presse
Request	□ Produktbeschreibung 8MAN	File server - Directory \\srv-8man\Marketing\Produktbeschreibung 8MAN
Request	□ Secret Projects	File server - Directory \\srv-8man\Marketing\Secret Projects
Request	□ Vorlagen	File server - Directory \\srv-8man\Marketing\Vorlagen

Click the shopping cart.



Thank you for your request.

Search/Marketing

Resource	Type	Options
Create directory	File server - Directory	Flyer2017

Please add a comment

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

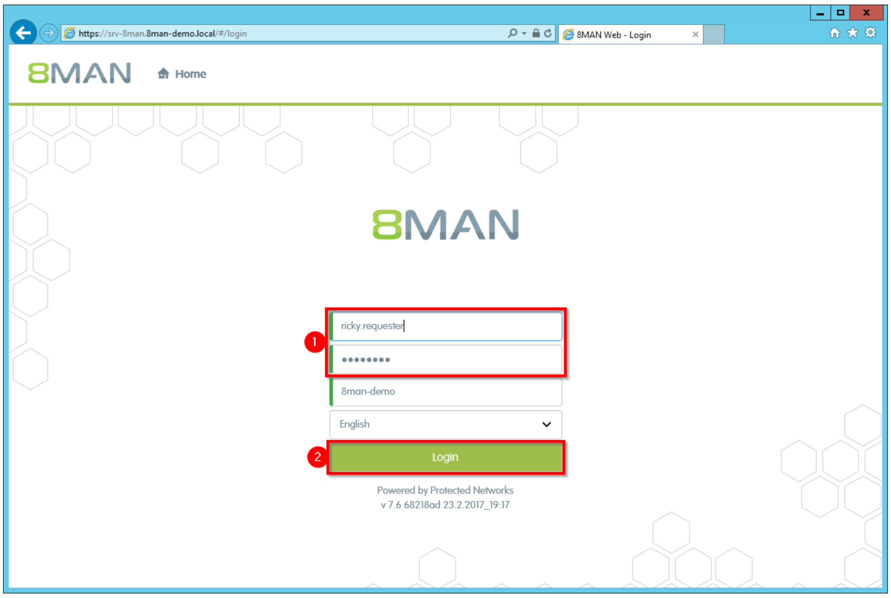
7.4.3 GrantMA: Allowing HR employees to request user account creation from the helpdesk

Background / Value

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

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

Step by step process



ricky.requester

••••••••

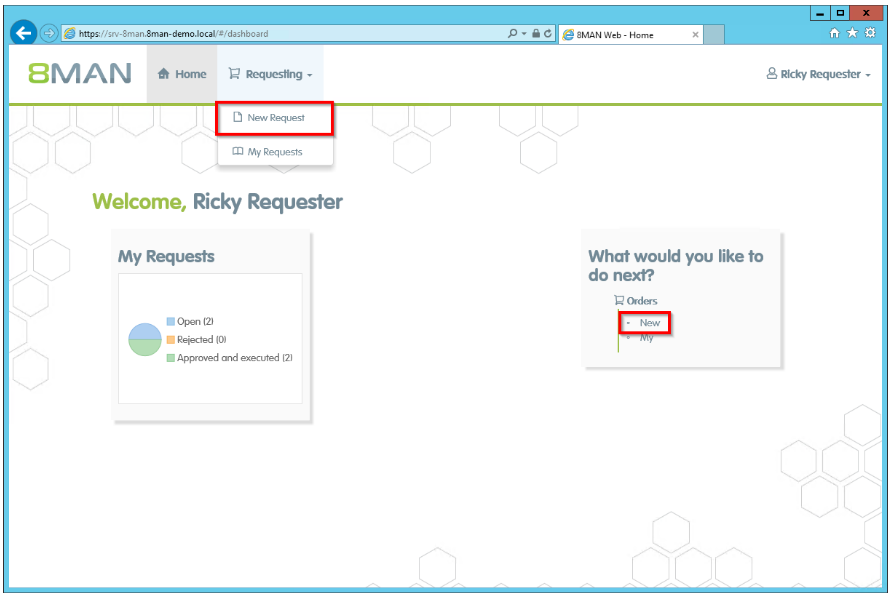
8man-demo

English

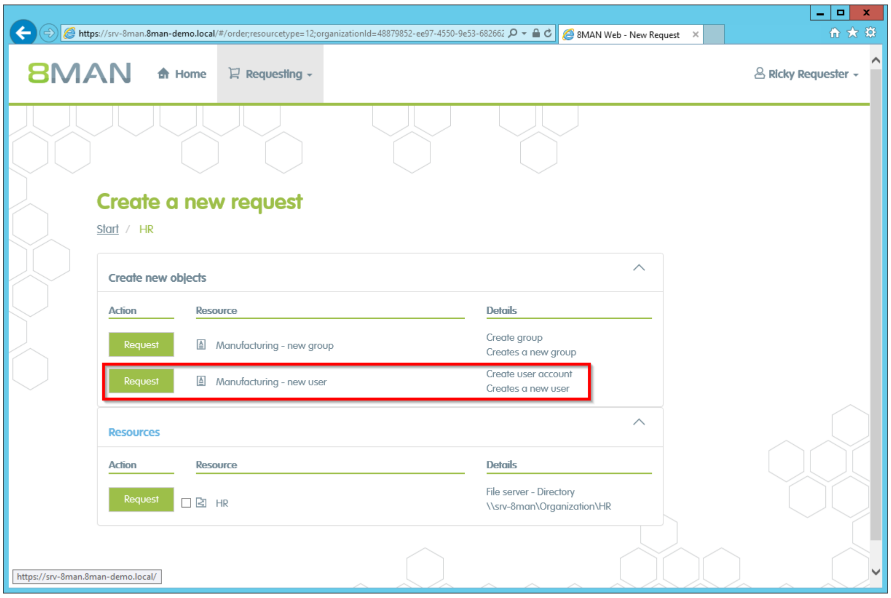
Login

Powered by Protected Networks
v 7.6 68218ad 23.2.2017_19:17

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



Click on "New Request".


https://srv-8man.8man-demo.local/#/order;resourcetype=12;organizationId=48879852-ee97-4550-9e53-68266z
8MAN Web - New Request
8MAN
Home
Requesting
Ricky Requester

Create a new request

Start / HR

Create new objects

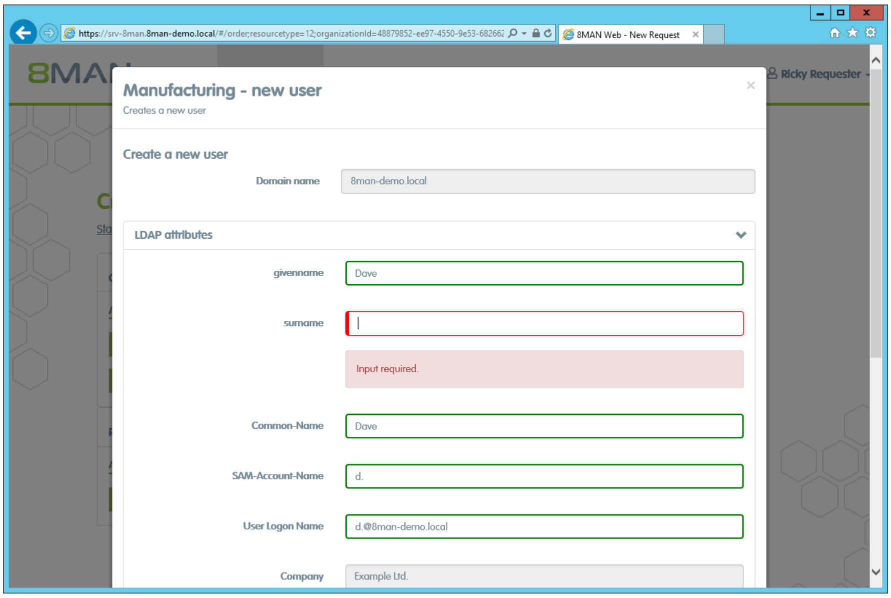
Action	Resource	Details
Request	Manufacturing - new group	Create group Creates a new group
Request	Manufacturing - new user	Create user account Creates a new user

Resources

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

https://srv-8man.8man-demo.local/

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


https://srv-8man.8man-demo.local/#/order;resourcetype=12;organizationId=48879852-ee97-4550-9e53-68266z
8MAN Web - New Request
Ricky Requester
×

Manufacturing - new user

Creates a new user

Create a new user

Domain name: 8man-demo.local

LDAP attributes

givenname: Dave

surname: |

Input required.

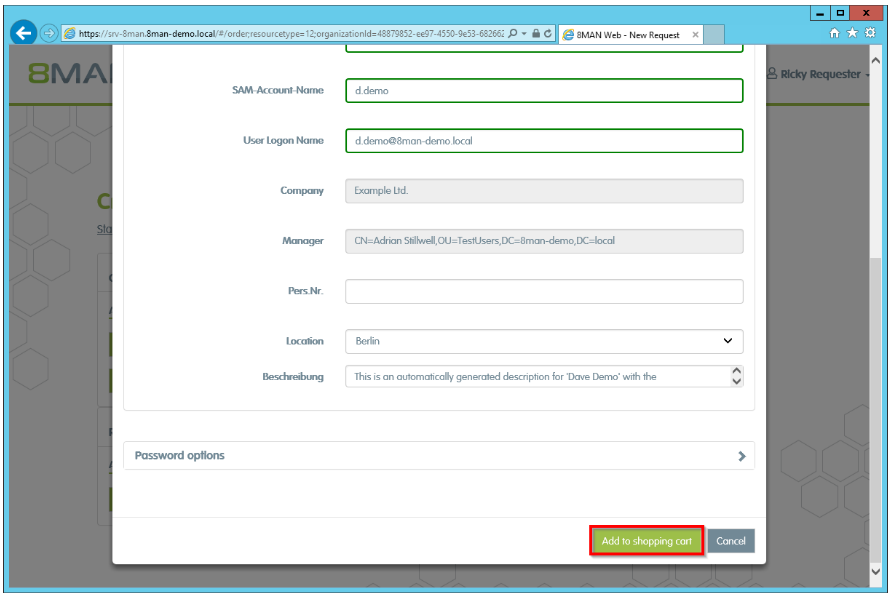
Common-Name: Dave

SAM-Account-Name: d.

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

Company: Example Ltd.

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



SAM-Account-Name: d.demo

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

Company: Example Ltd.

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

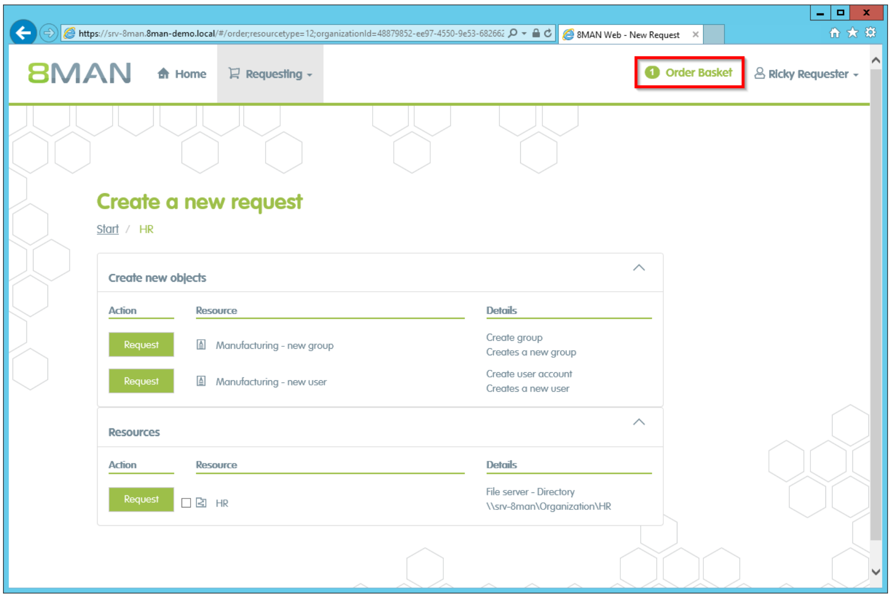
Pers.Nr.:

Location: Berlin

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

https://srv-8man.8man-demo.local/#/order;resourcetype=12;organizationId=48879852-ee97-4550-9e53-68266
8MAN Web - New Request
Ricky Requester
Password options
Add to shopping cart
Cancel

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



Create a new request

Start / HR

Create new objects

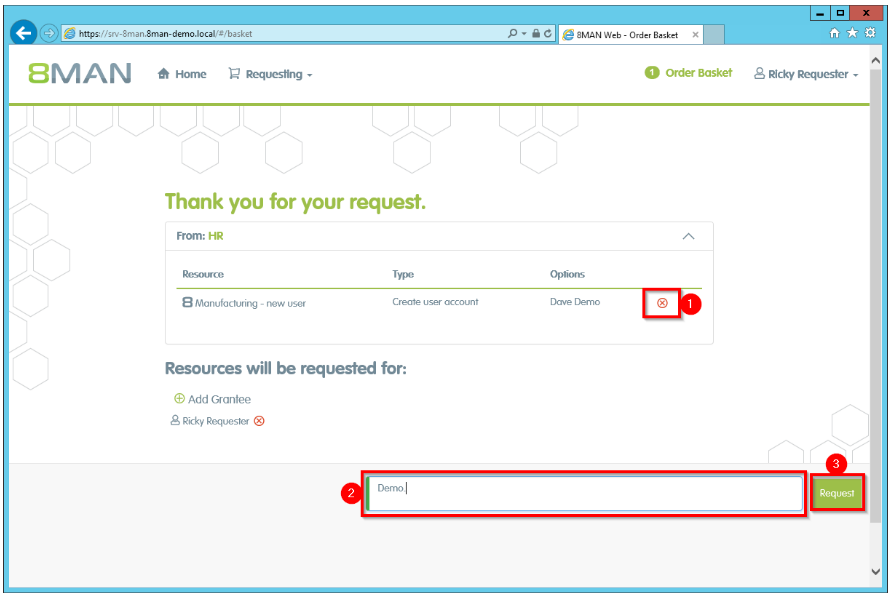
Action	Resource	Details
Request	Manufacturing - new group	Create group Creates a new group
Request	Manufacturing - new user	Create user account Creates a new user

Resources

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

https://srv-8man.8man-demo.local/#/order;resourcetype=12;organizationId=48879852-ee97-4550-9e53-68266
8MAN Web - New Request
8MAN
Home
Requesting
1 Order Basket
Ricky Requester

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



Thank you for your request.

From: HR

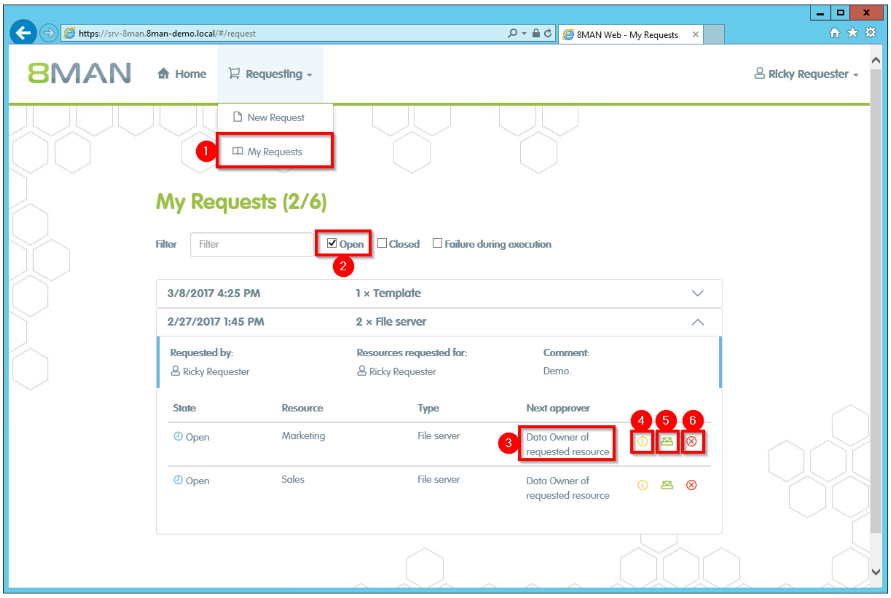
Resource	Type	Options
Manufacturing - new user	Create user account	Dave Demo

Resources will be requested for:

Ricky Requester

Demo.

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



My Requests (2/6)

Filter ☑ Open □ Closed □ Failure during execution

3/8/2017 4:25 PM 1 × Template

2/27/2017 1:45 PM 2 × File server

Requested by: Ricky Requester

Resources requested for: Ricky Requester

Comment: Demo.

State	Resource	Type	Next approver
Open	Marketing	File server	Data Owner of requested resource
Open	Sales	File server	Data Owner of requested resource

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.*

7.5 +8MATE GrantMA Workflows for Data Owner / Administratoren

7.5.1 Informing approvers of new requests via email

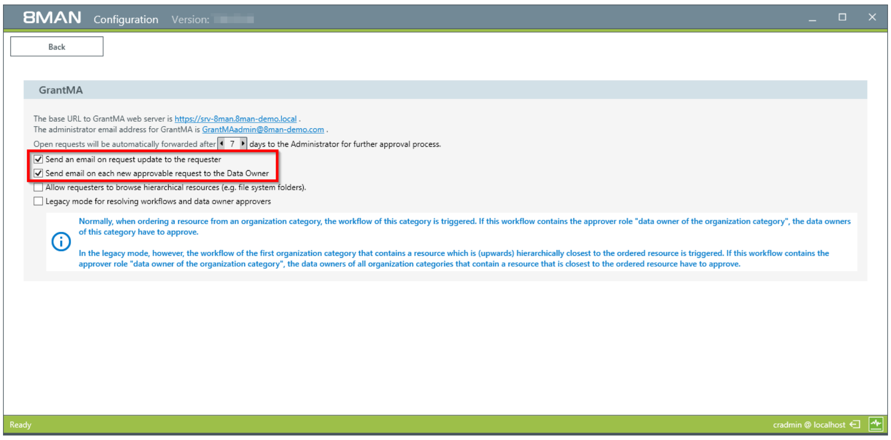
Background / Value

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



GrantMA

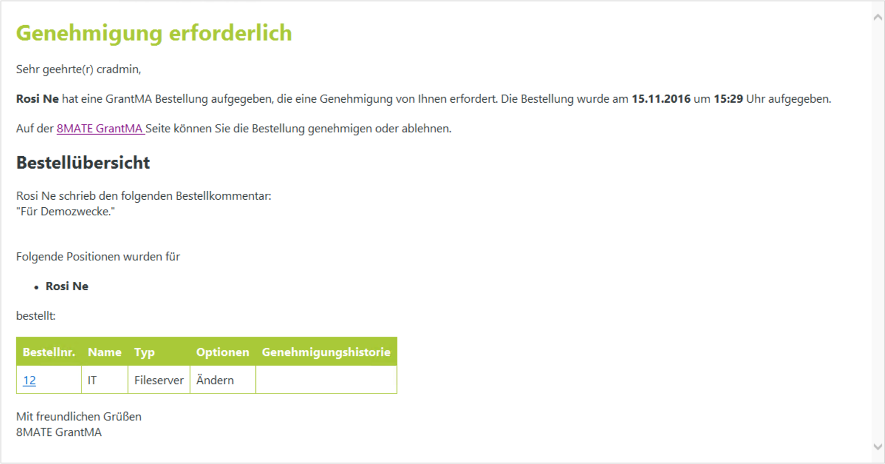
The base URL to GrantMA web server is https://srv-8man.8man-demo.local .
The administrator email address for GrantMA is GrantMAadmin@8man-demo.com .
Open requests will be automatically forwarded after 7 days to the Administrator for further approval process.

☑ Send an email on request update to the requester
☑ Send email on each new approvable request to the Data Owner
□ Allow requesters to browse hierarchical resources (e.g. file system folders).
□ Legacy mode for resolving workflows and data owner approvers

Normally, when ordering a resource from an organization category, the workflow of this category is triggered. If this workflow contains the approver role "data owner of the organization category", the data owners of this category have to approve.

In the legacy mode, however, the workflow of the first organization category that contains a resource which is (upwards) hierarchically closest to the ordered resource is triggered. If this workflow contains the approver role "data owner of the organization category", the data owners of all organization categories that contain a resource that is closest to the ordered resource have to approve.

Navigate to "Change configuration -> GrantMA" in the 8MAN configuration. Activate the Email option. We recommend activating both options so that both the requestor and the approver are kept informed.



Genehmigung erforderlich

Sehr geehrte(r) cradmin,

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

Auf der 8MATE GrantMA Seite können Sie die Bestellung genehmigen oder ablehnen.

Bestellübersicht

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

Folgende Positionen wurden für

- **Rosi Ne**

bestellt:

Bestellnr.	Name	Typ	Optionen	Genehmigungshistorie
12	IT	Fileserver	Ändern	

Mit freundlichen Grüßen
8MATE GrantMA

Example of an Email notification.

7.5.2 Approving or denying a request in the self service portal

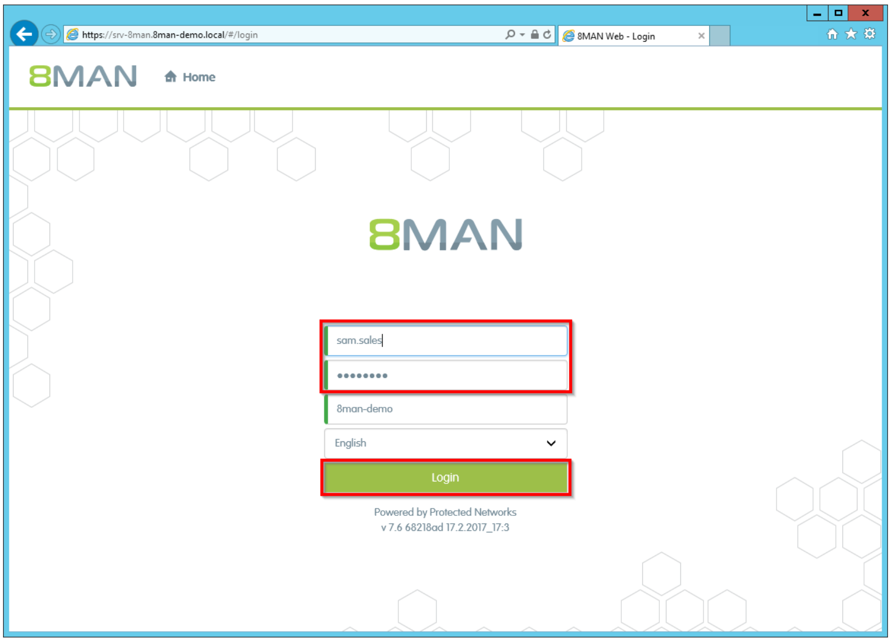
Background / Value

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


https://srv-8man.8man-demo.local/#/login

sam.sales

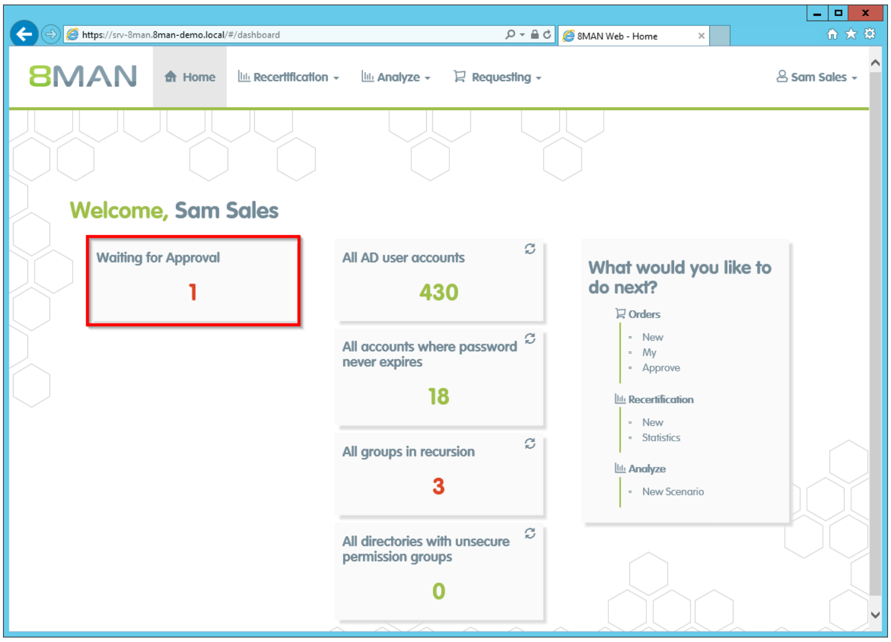
••••••••

8man-demo

English

Powered by Protected Networks
v 7.6 68218ad 17.2.2017_17:3

Log in with approver credentials.



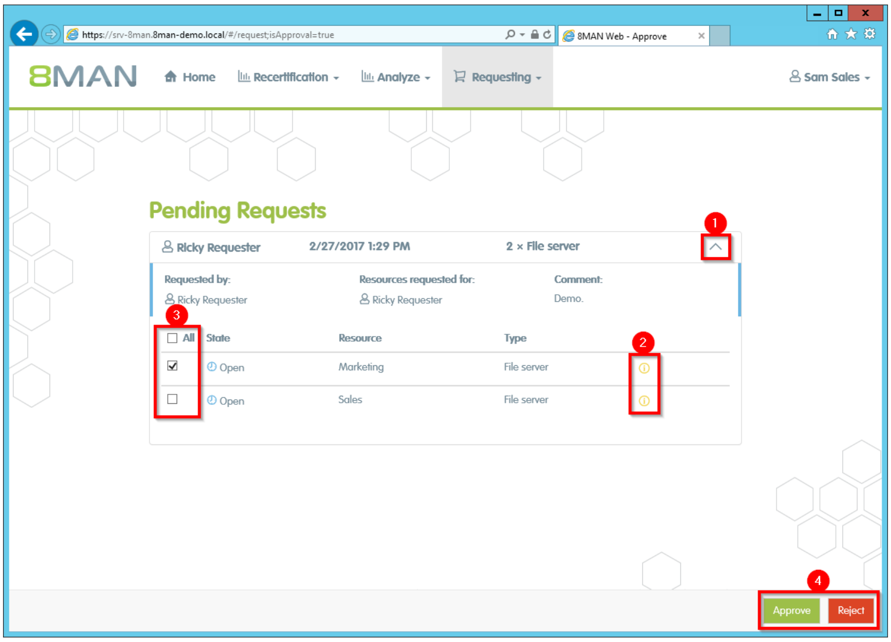
Welcome, Sam Sales

Waiting for Approval	1
All AD user accounts	430
All accounts where password never expires	18
All groups in recursion	3
All directories with unsecure permission groups	0

What would you like to do next?

Click on "Waiting for Approval". In this example there is 1 request waiting for approval.

Click on the tile.



Pending Requests

Ricky Requester 2/27/2017 1:29 PM 2 × File server

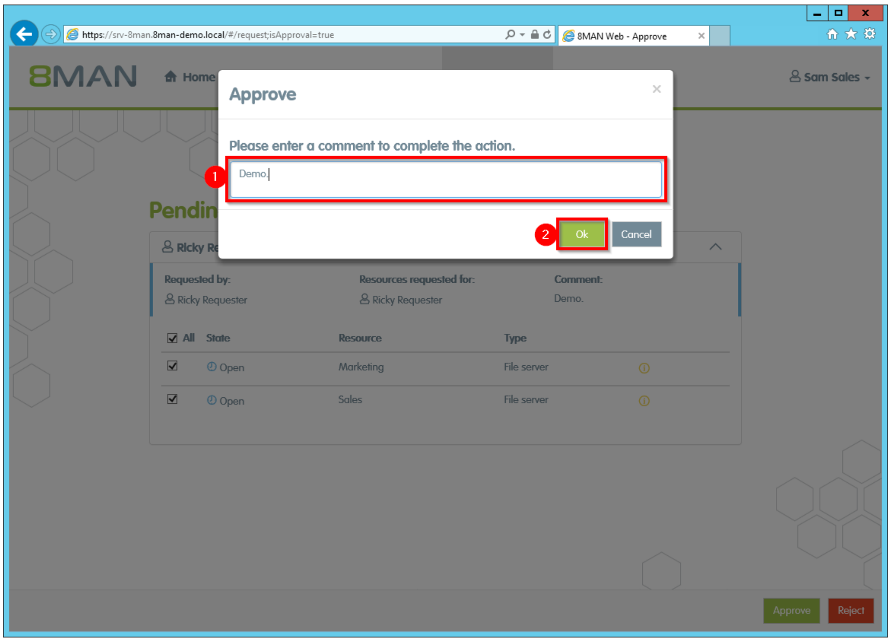
Requested by: Ricky Requester

Resources requested for: Ricky Requester

Comment: Demo.

□ All	State	Resource	Type
☑	Open	Marketing	File server
□	Open	Sales	File server

1. *Open a pending request to see the position.*
2. *View details to the individual positions.*
3. *Select one or more positions.*
4. *Click on "Approve" or "Reject".*



Approve

Please enter a comment to complete the action.

Demo.

Requested by: Ricky Requester

Resources requested for: Ricky Requester

Comment: Demo.

☑ All	State	Resource	Type	
☑	Open	Marketing	File server	ⓘ
☑	Open	Sales	File server	ⓘ

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

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

8. User Provisioning

8.1 Active Directory

8.1.1 Administrator

8.1.1.1 Creating a user account

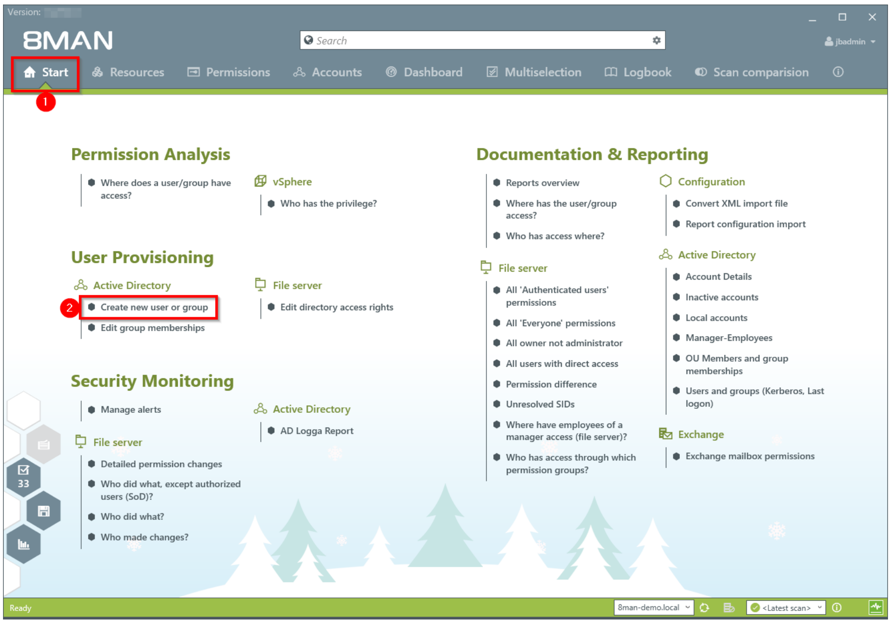
Background / Value

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.

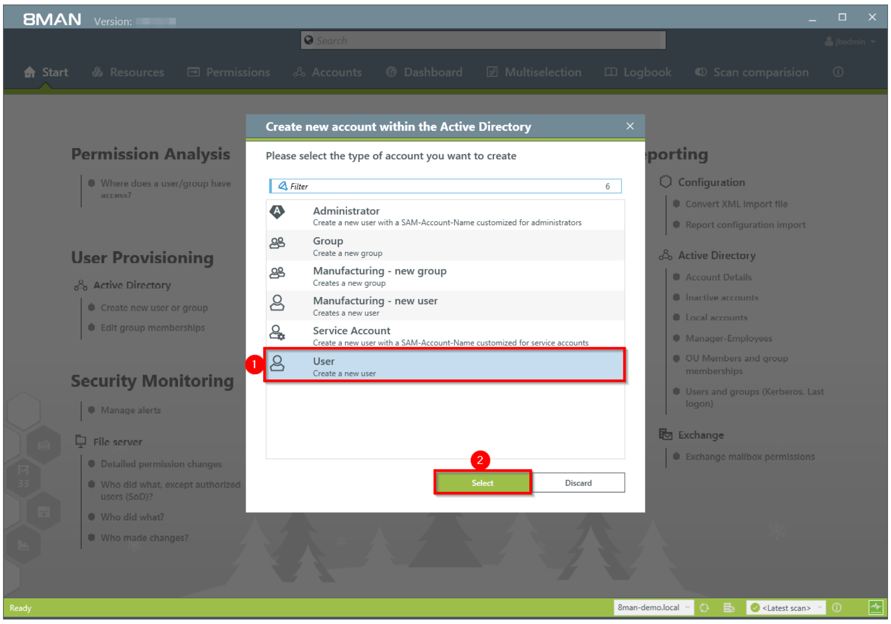
Additional Services

Creating templates for account creation (Part II Technical documentation)

Step by step process



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



Create new account within the Active Directory

Please select the type of account you want to create

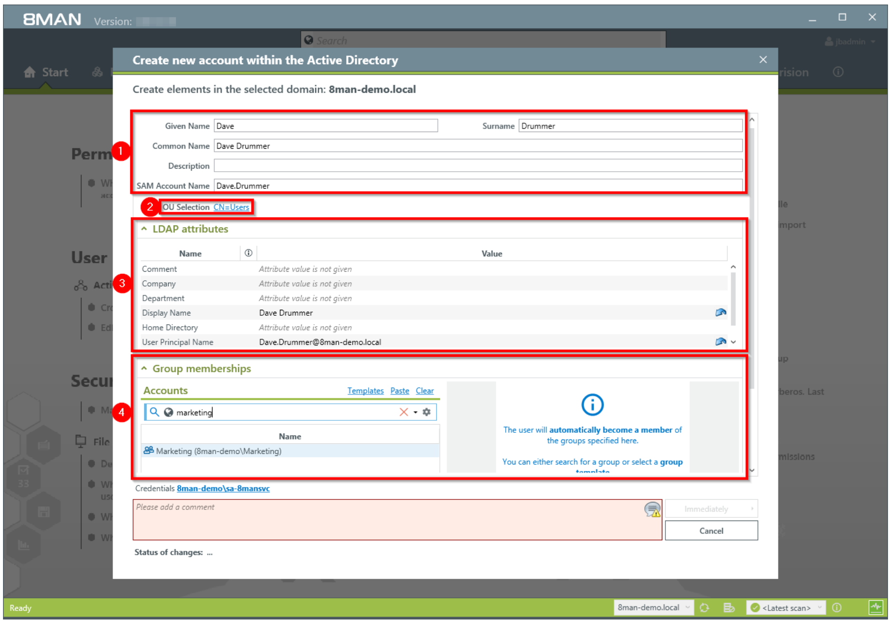
Filter 6

Administrator	Create a new user with a SAM-Account-Name customized for administrators
Group	Create a new group
Manufacturing - new group	Creates a new group
Manufacturing - new user	Creates a new user
Service Account	Create a new user with a SAM-Account-Name customized for service accounts
User	Create a new user

Select | Discard

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".*



Create new account within the Active Directory

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

Given Name: Dave
Surname: Drummer
Common Name: Dave Drummer
Description:
SAM Account Name: Dave.Drummer

OU Selection CN=Users

LDAP attributes

Name	Value
Comment	Attribute value is not given
Company	Attribute value is not given
Department	Attribute value is not given
Display Name	Dave Drummer
Home Directory	Attribute value is not given
User Principal Name	Dave.Drummer@8man-demo.local

Group memberships

Accounts

marketing

Name
Marketing (8man-demo\Marketing)

The user will **automatically become a member** of the groups specified here.

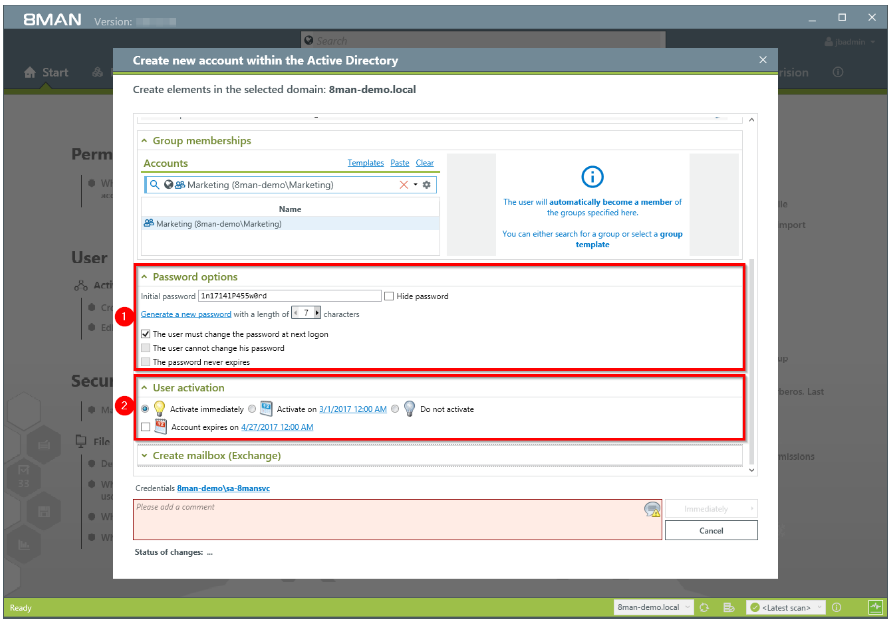
You can either search for a group or select a **group template**.

Credentials 8man-demo\sa-8mansvc

Please add a comment

Status of changes: ...

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.*



Create new account within the Active Directory

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

Group memberships

Accounts — Templates Paste Clear

Marketing (8man-demo\Marketing)

Name
Marketing (8man-demo\Marketing)

The user will **automatically become a member** of the groups specified here.

You can either search for a group or select a **group template**

1 Password options

Initial password 1n17141P455w0rd □ Hide password

Generate a new password with a length of 7 characters

☑ The user must change the password at next logon
□ The user cannot change his password
□ The password never expires

2 User activation

● Activate immediately ○ Activate on 3/1/2017 12:00 AM ○ Do not activate

□ Account expires on 4/27/2017 12:00 AM

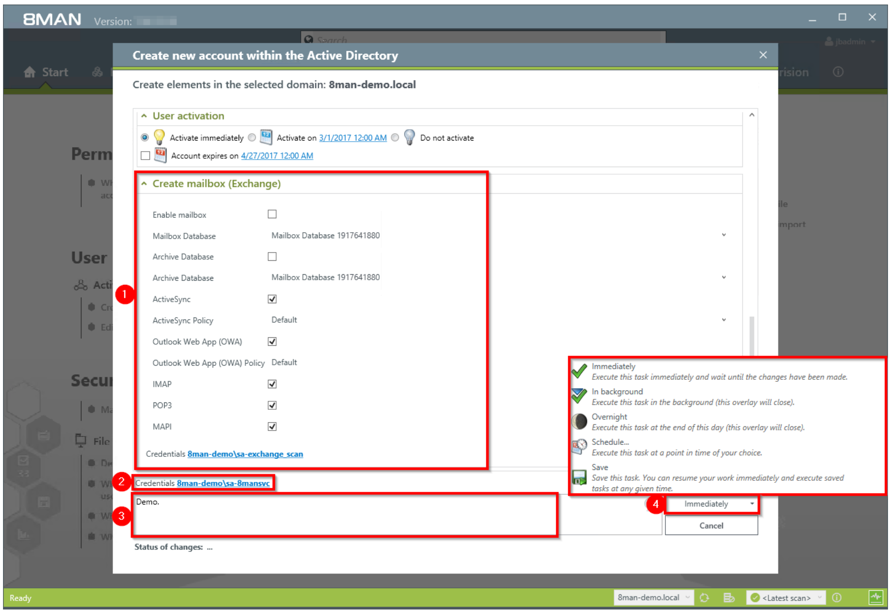
Create mailbox (Exchange)

Credentials 8man-demo\sa-8mansvc

Please add a comment

Status of changes: ...

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



Create new account within the Active Directory

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

User activation

● Activate immediately ○ Activate on 3/1/2017 12:00 AM ○ Do not activate

□ Account expires on 4/27/2017 12:00 AM

1 Create mailbox (Exchange)

Enable mailbox	□
Mailbox Database	Mailbox Database 1917641880
Archive Database	□
Archive Database	Mailbox Database 1917641880
ActiveSync	☑
ActiveSync Policy	Default
Outlook Web App (OWA)	☑
Outlook Web App (OWA) Policy	Default
IMAP	☑
POP3	☑
MAPI	☑

Credentials 8man-demo\sa-exchange_scan

2 Credentials 8man-demo\sa-8mansvc

3 Demo.

Status of changes: ...

Immediately
Execute this task immediately and wait until the changes have been made.

In background
Execute this task in the background (this overlay will close).

Overnight
Execute this task at the end of this day (this overlay will close).

Schedule...
Execute this task at a point in time of your choice.

Save
Save this task. You can resume your work immediately and execute saved tasks at any given time.

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

Sensitive administrative actions should always contain an explanation why the account is being created and/or what it is for. We recommend adding a ticket number and information who requested the account creation.

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

8.1.1.2 Creating groups and adding users

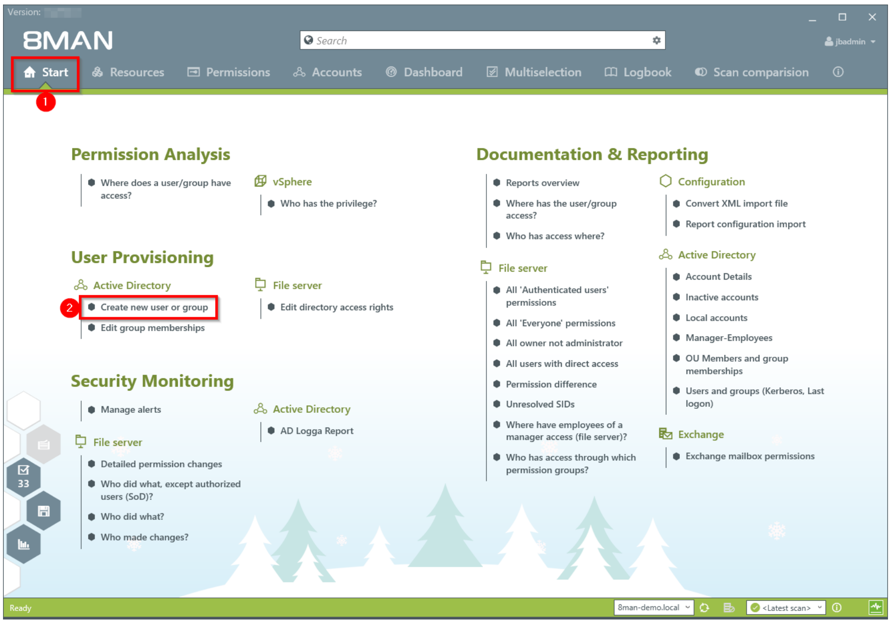
Background / Value

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

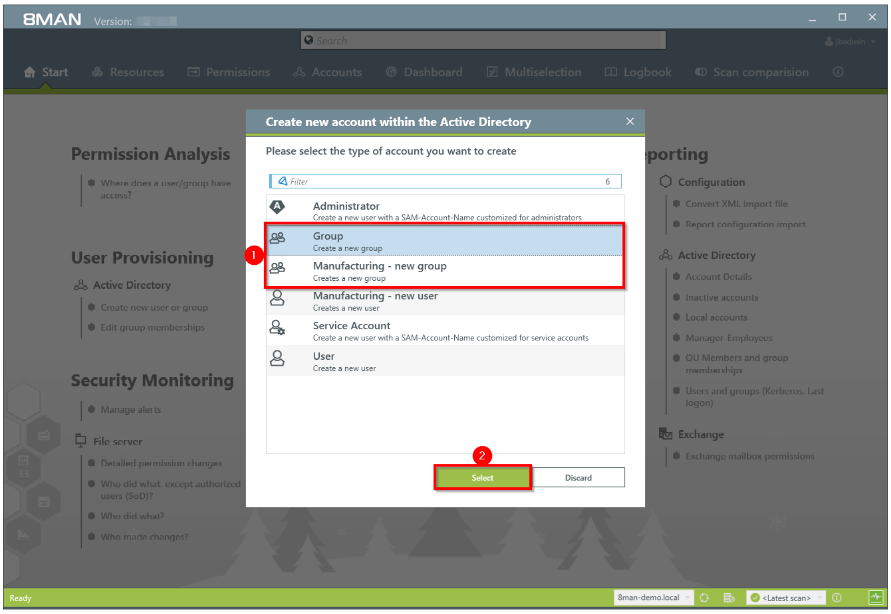
Additional Services

Managing group memberships

Step by step process



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

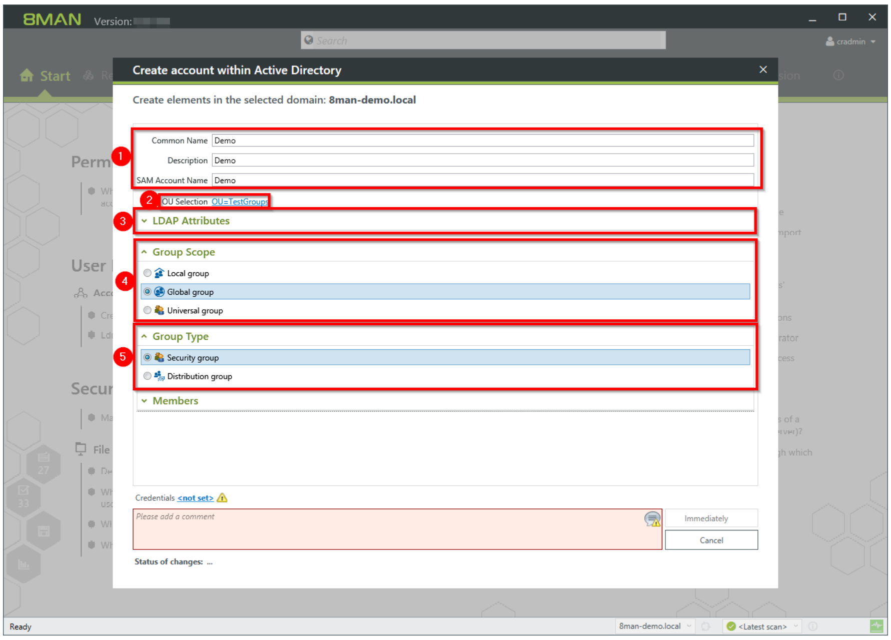

Create new account within the Active Directory

Please select the type of account you want to create

Administrator	Create a new user with a SAM-Account-Name customized for administrators
Group	Create a new group
Manufacturing - new group	Creates a new group
Manufacturing - new user	Creates a new user
Service Account	Create a new user with a SAM-Account-Name customized for service accounts
User	Create a new user

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".*



Create account within Active Directory

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

Common Name: Demo
Description: Demo
SAM Account Name: Demo
OU Selection: OU=TestGroups

LDAP Attributes

Group Scope
○ Local group
● Global group
○ Universal group

Group Type
● Security group
○ Distribution group

Members

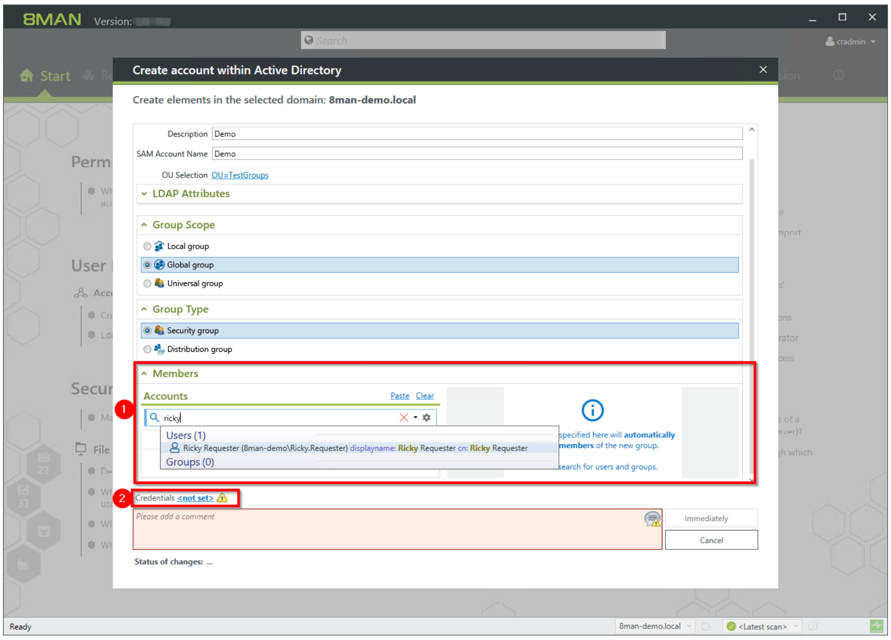
Credentials: <not set>

Please add a comment

Immediately
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.*



Create account within Active Directory

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

Description: Demo
SAM Account Name: Demo
OU Selection: OU=TestGroups

LDAP Attributes

Group Scope
○ Local group
● Global group
○ Universal group

Group Type
● Security group
○ Distribution group

Members

Accounts — Paste — Clear

ricky

Users (1)
Ricky Requester (8man-demo\Ricky.Requester) displayname: Ricky Requester cn: Ricky Requester
Groups (0)

...specified here will **automatically** **members** of the new group.
...search for users and groups.

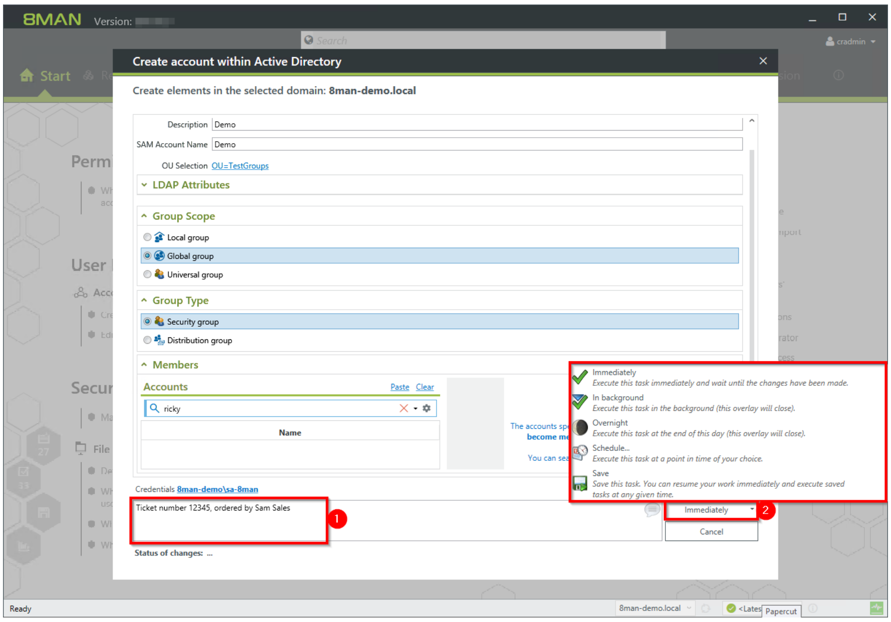
Credentials: <not set>

Please add a comment

Immediately
Cancel

Status of changes: ...

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



Create account within Active Directory

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

Description: Demo

SAM Account Name: Demo

OU Selection: OU=TestGroups

Group Scope: ○ Local group ● Global group ○ Universal group

Group Type: ● Security group ○ Distribution group

Members – Accounts: ricky

Credentials 8man-demo\sa-8man

Ticket number 12345, ordered by Sam Sales

Status of changes: ...

Immediately – Execute this task immediately and wait until the changes have been made.

In background – Execute this task in the background (this overlay will close).

Overnight – Execute this task at the end of this day (this overlay will close).

Schedule... – Execute this task at a point in time of your choice.

Save – Save this task. You can resume your work immediately and execute saved tasks at any given time.

1. *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.

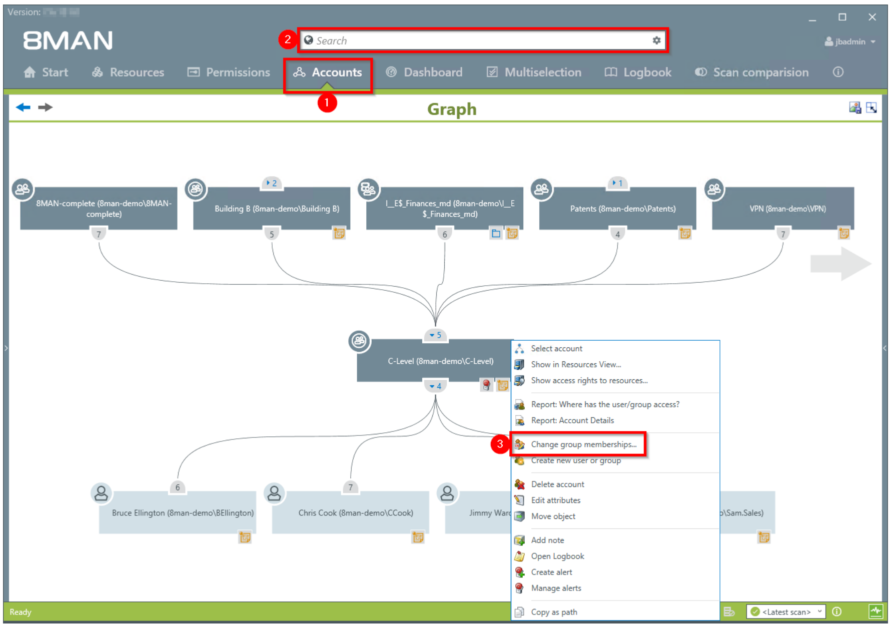
2. *Complete the action immediately or later, or save it as a job.*

8.1.1.3 Managing 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.

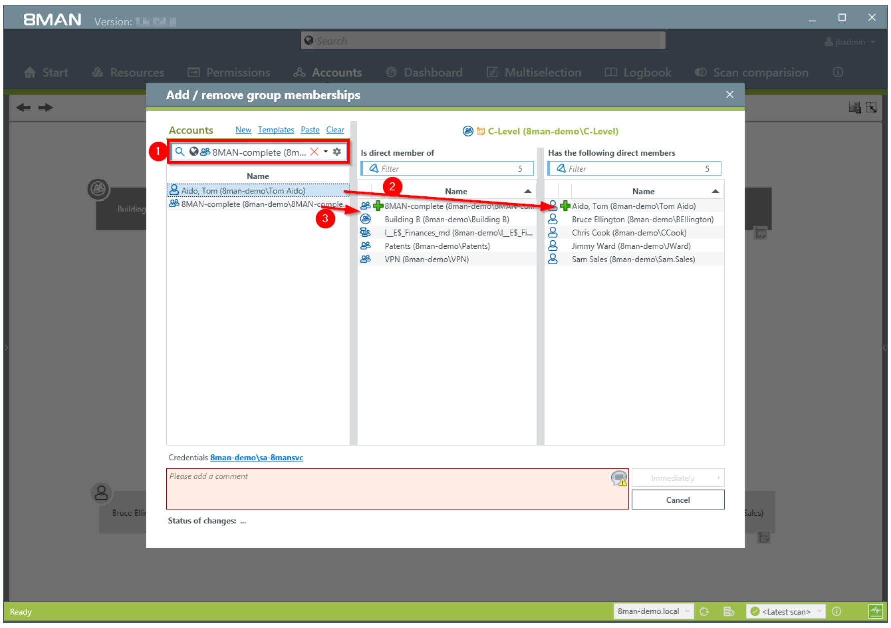
Step by step process



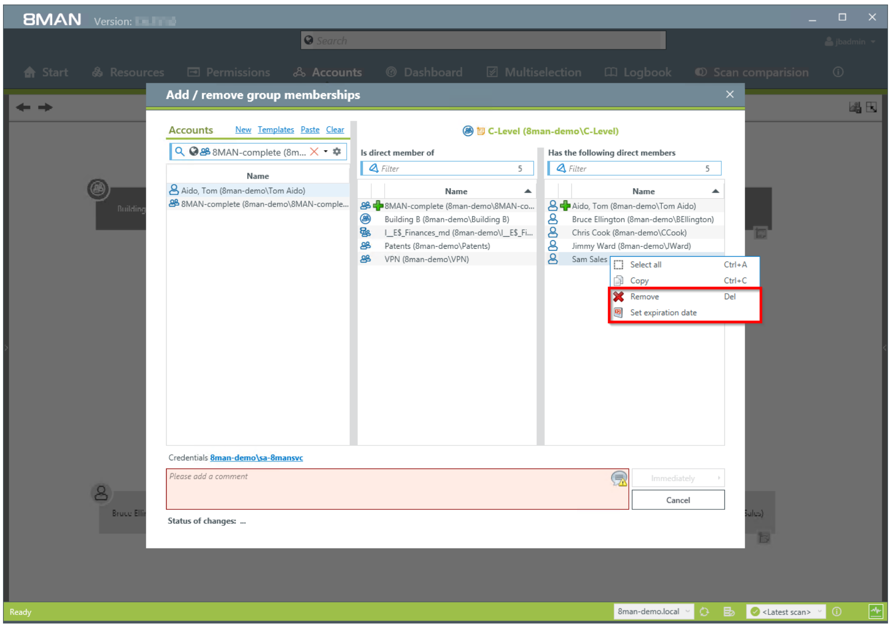
Version:
8MAN
2
Search
jbadmin
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
1
Graph
8MAN-complete (8man-demo\8MAN-complete)
Building 8 (8man-demo\Building 8)
I_E$_Finances_md (8man-demo\I_E$_Finances_md)
Patents (8man-demo\Patents)
VPN (8man-demo\VPN)
C-Level (8man-demo\C-Level)
Bruce Ellington (8man-demo\BEllington)
Chris Cook (8man-demo\CCook)
Jimmy War
\Sam.Sales)
Select account
Show in Resources View...
Show access rights to resources...
Report: Where has the user/group access?
Report: Account Details
3
Change group memberships...
Create new user or group
Delete account
Edit attributes
Move object
Add note
Open Logbook
Create alert
Manage alerts
Copy as path
Ready
<Latest scan>

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.*

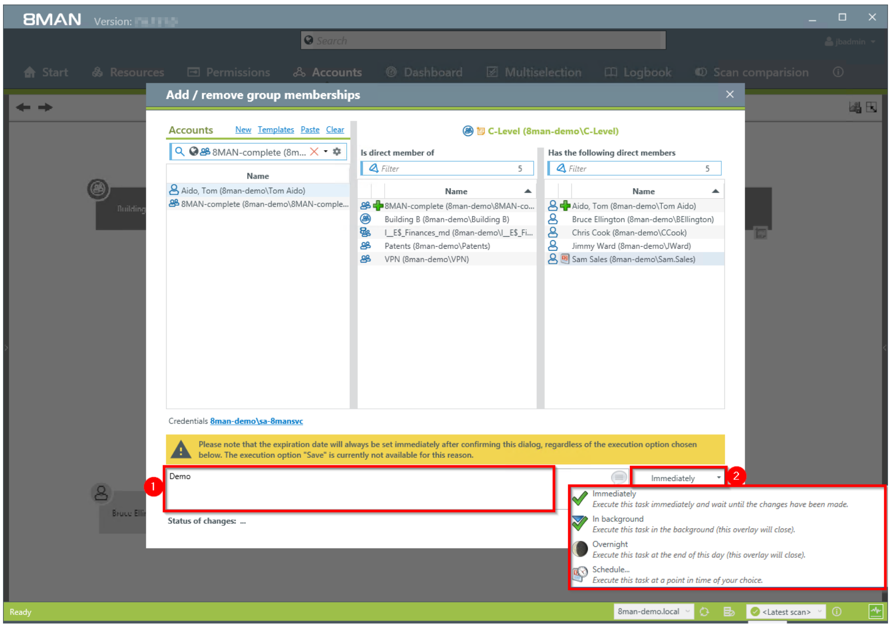
Alternatively you can also select "Edit group memberships" on the 8MAN home page.


8MAN
Add / remove group memberships
Accounts
New
Templates
Paste
Clear
8MAN-complete (8m...
Name
Aido, Tom (8man-demo\Tom Aido)
8MAN-complete (8man-demo\8MAN-comple...
C-Level (8man-demo\C-Level)
Is direct member of
Has the following direct members
Filter
5
8MAN-complete (8man-demo\8MAN-co...
Building B (8man-demo\Building B)
I__E$_Finances_md (8man-demo\I__E$_Fi...
Patents (8man-demo\Patents)
VPN (8man-demo\VPN)
Aido, Tom (8man-demo\Tom Aido)
Bruce Ellington (8man-demo\BEllington)
Chris Cook (8man-demo\CCook)
Jimmy Ward (8man-demo\JWard)
Sam Sales (8man-demo\Sam.Sales)
Credentials 8man-demo\sa-8mansvc
Please add a comment
Immediately
Cancel
Status of changes: ...
1
2
3
Ready
8man-demo.local
<Latest scan>

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).*


8MAN
Add / remove group memberships
Accounts
New
Templates
Paste
Clear
8MAN-complete (8m...
Name
Aido, Tom (8man-demo\Tom Aido)
8MAN-complete (8man-demo\8MAN-comple...
C-Level (8man-demo\C-Level)
Is direct member of
Has the following direct members
Filter
5
8MAN-complete (8man-demo\8MAN-co...
Building B (8man-demo\Building B)
I__E$_Finances_md (8man-demo\I__E$_Fi...
Patents (8man-demo\Patents)
VPN (8man-demo\VPN)
Aido, Tom (8man-demo\Tom Aido)
Bruce Ellington (8man-demo\BEllington)
Chris Cook (8man-demo\CCook)
Jimmy Ward (8man-demo\JWard)
Sam Sales
Select all Ctrl+A
Copy Ctrl+C
Remove Del
Set expiration date
Credentials 8man-demo\sa-8mansvc
Please add a comment
Immediately
Cancel
Status of changes: ...
Ready
8man-demo.local
<Latest scan>

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



Add / remove group memberships

Accounts New Templates Paste Clear

8MAN-complete (8m...

Name
Aido, Tom (8man-demo\Tom Aido)
8MAN-complete (8man-demo\8MAN-comple...

C-Level (8man-demo\C-Level)

Is direct member of

Filter 5

Name
8MAN-complete (8man-demo\8MAN-co...
Building B (8man-demo\Building B)
I__E$_Finances_md (8man-demo\I__E$_Fi...
Patents (8man-demo\Patents)
VPN (8man-demo\VPN)

Has the following direct members

Filter 5

Name
Aido, Tom (8man-demo\Tom Aido)
Bruce Ellington (8man-demo\BEllington)
Chris Cook (8man-demo\CCook)
Jimmy Ward (8man-demo\JWard)
Sam Sales (8man-demo\Sam.Sales)

Credentials 8man-demo\sa-8mansvc

Please note that the expiration date will always be set immediately after confirming this dialog, regardless of the execution option chosen below. The execution option "Save" is currently not available for this reason.

1 Demo

Immediately 2

- Immediately
  Execute this task immediately and wait until the changes have been made.
- In background
  Execute this task in the background (this overlay will close).
- Overnight
  Execute this task at the end of this day (this overlay will close).
- Schedule...
  Execute this task at a point in time of your choice.

Status of changes: ...

8man-demo.local <Latest scan>

1. You must enter a comment.

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

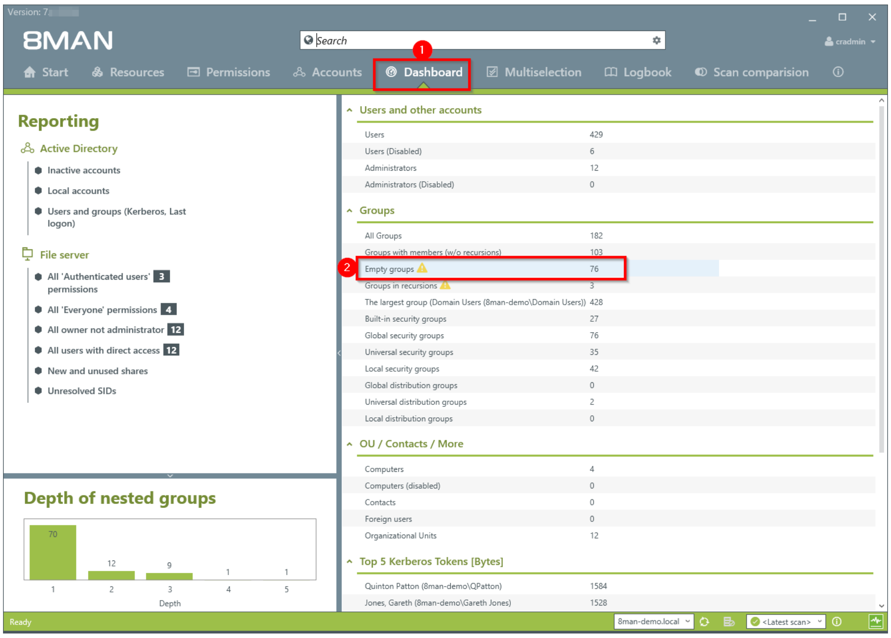
8.1.1.4 Deleting empty groups

Background / Value

Over time, empty groups accumulate in your Active Directory. These reduce performance and diminish transparency. We recommend deleting these groups. 8MAN always deletes user accounts and groups including all permissions on file servers. This prevents unauthorized SIDs and reduces security risks.

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

Step by step process



Reporting

Active Directory

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

File server

- All 'Authenticated users' permissions 3
- All 'Everyone' permissions 4
- All owner not administrator 12
- All users with direct access 12
- New and unused shares
- Unresolved SIDs

Users and other accounts

Users	429
Users (Disabled)	6
Administrators	12
Administrators (Disabled)	0

Groups

All Groups	182
Groups with members (w/o recursions)	103
Empty groups ⚠	76
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	428
Built-in security groups	27
Global security groups	76
Universal security groups	35
Local security groups	42
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

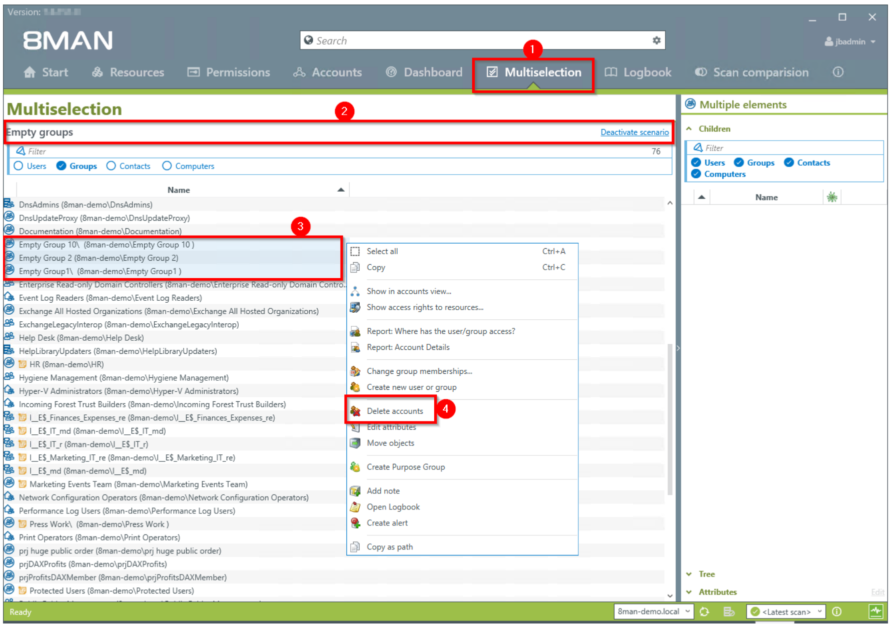
OU / Contacts / More

Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

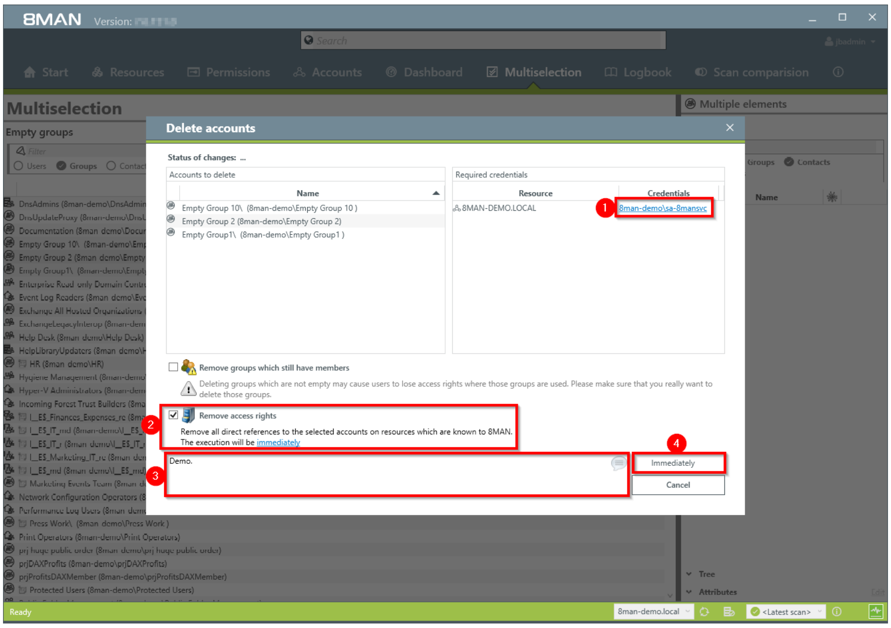
Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584
Jones, Gareth (8man-demo\Gareth Jones)	1528

1. *Switch to the Dashboard.*
2. *Double-click on "Empty groups".*



1. *8MAN automatically switches to the multi-select view.*
2. *The scenario "Empty groups" is active. The listed groups are all empty.*
3. *Select the groups that you are sure can be deleted.*
4. *Right-click and select "Delete Account" from the context menu.*



□ Remove groups which still have members

Deleting groups which are not empty may cause users to lose access rights where those groups are used. Please make sure that you really want to delete those groups.

☑ Remove access rights

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

Demo.

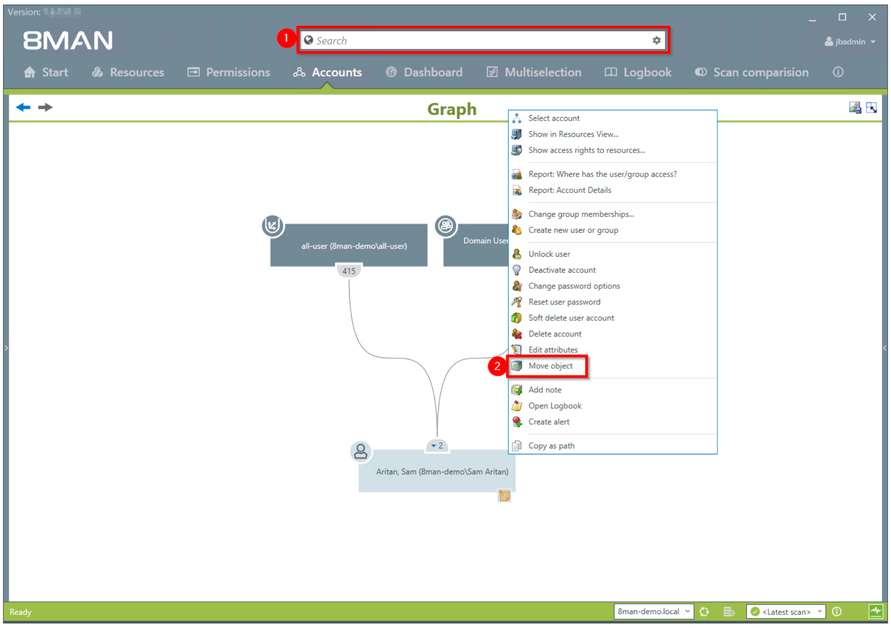
1. *If required change the login which will be used to delete the group in AD.*
2. *Activate the option "Remove access rights" and prevent the occurance of unresolved SIDs.*
3. *You must enter a comment.*
4. *Start the deletion process.*

8.1.1.5 Moving objects in Active Directory

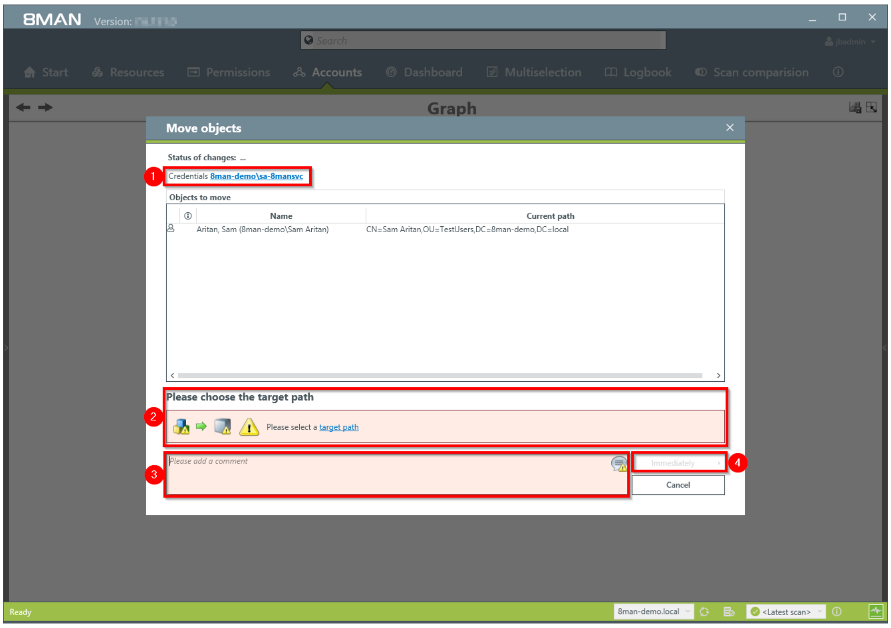
Background / Value

8MAN is able to move objects, meaning user accounts, group accounts and computers from one OU into another. This may be required if one of your users moves location or new group policies are applicable. 8MAN fully documents all movement among OUs.

Step by step process



1. *Use the search field to find the desired object.*
2. *Right-click on the object. You can do this in the "Accounts" view. Then select "move object".*



Status of changes: ...

Credentials 8man-demo\sa-8mansvc

Objects to move

Name	Current path
Aritan, Sam (8man-demo\Sam Aritan)	CN=Sam Aritan,OU=TestUsers,DC=8man-demo,DC=local

Please select a target path

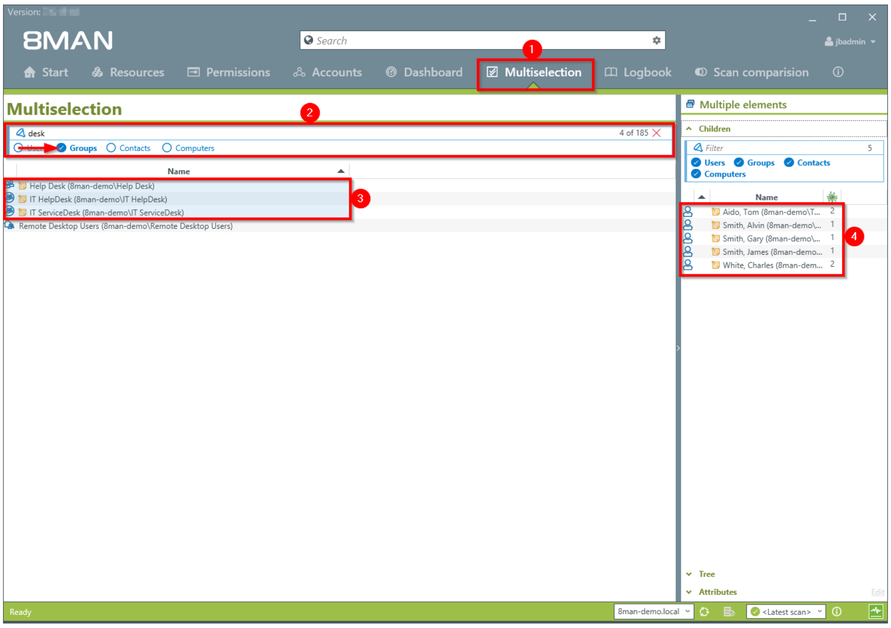
1. *If required change the login which will be used to move the object.*
2. *Select a destination path.*
3. *You must enter a comment.*
4. *Start the process.*

8.1.1.6 Reducing multiple groups to a single group

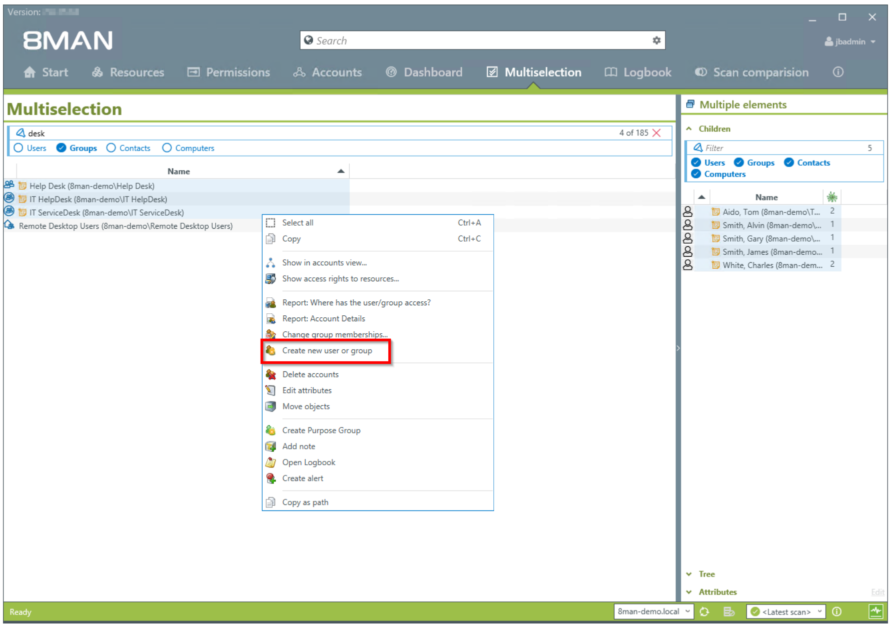
Background / Value

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.

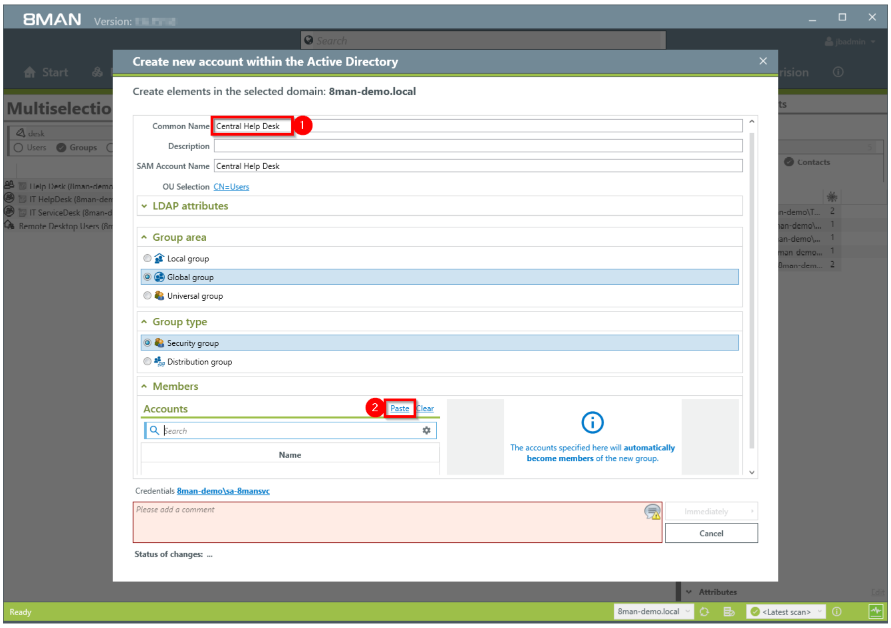
Step by step process


8MAN
Search
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
1
Multiselection
2
desk
4 of 185
Users
Groups
Contacts
Computers
Name
Help Desk (8man-demo\Help Desk)
IT HelpDesk (8man-demo\IT HelpDesk)
IT ServiceDesk (8man-demo\IT ServiceDesk)
Remote Desktop Users (8man-demo\Remote Desktop Users)
3
Multiple elements
Children
Filter
Users
Groups
Contacts
Computers
Name
Aido, Tom (8man-demo\T... 2
Smith, Alvin (8man-demo\... 1
Smith, Gary (8man-demo\... 1
Smith, James (8man-demo... 1
White, Charles (8man-dem... 2
4
Tree
Attributes
Ready
8man-demo.local
<Latest scan>

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



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



Create new account within the Active Directory

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

Common Name: Central Help Desk

Description:

SAM Account Name: Central Help Desk

OU Selection: CN=Users

LDAP attributes

Group area
- ○ Local group
- ● Global group
- ○ Universal group

Group type
- ● Security group
- ○ Distribution group

Members

Accounts — Paste Clear

Name

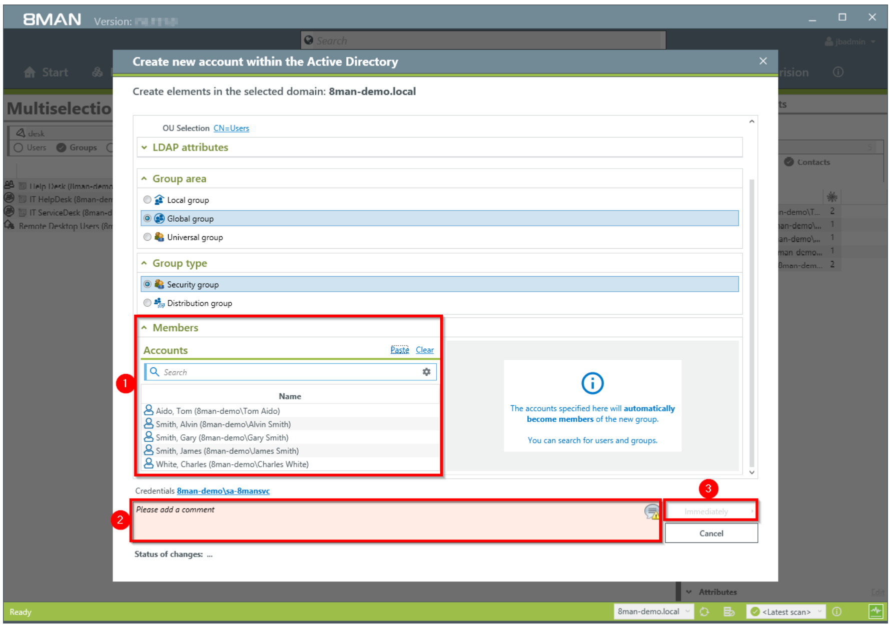
The accounts specified here will **automatically become members** of the new group.

Credentials 8man-demo\sa-8mansvc

Please add a comment

Status of changes: ...

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



Create new account within the Active Directory

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

OU Selection: CN=Users

LDAP attributes

Group area
- ○ Local group
- ● Global group
- ○ Universal group

Group type
- ● Security group
- ○ Distribution group

Members

Accounts — Paste Clear

Name
- Aido, Tom (8man-demo\Tom Aido)
- Smith, Alvin (8man-demo\Alvin Smith)
- Smith, Gary (8man-demo\Gary Smith)
- Smith, James (8man-demo\James Smith)
- White, Charles (8man-demo\Charles White)

The accounts specified here will **automatically become members** of the new group.

You can search for users and groups.

Credentials 8man-demo\sa-8mansvc

Please add a comment

Status of changes: ...

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 Changing password options

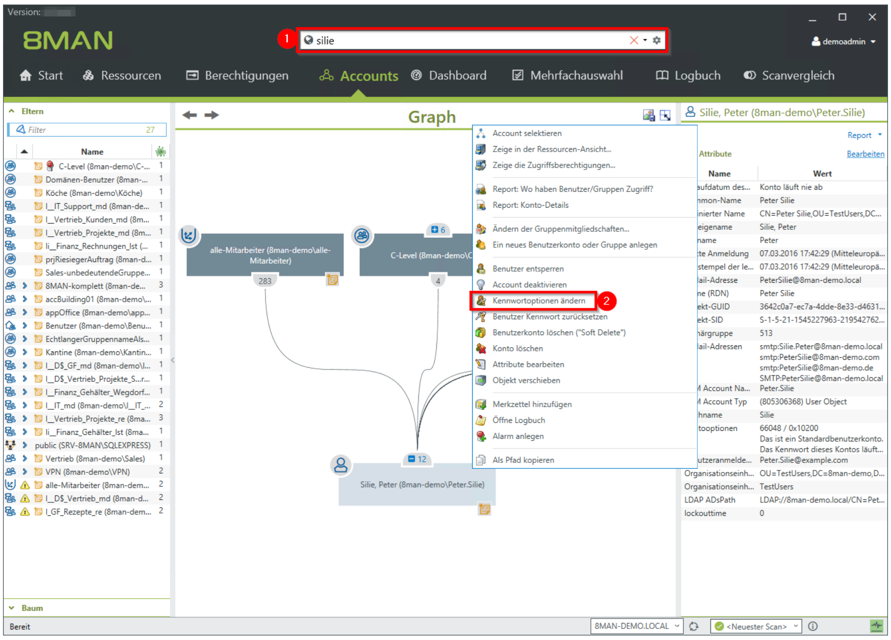
Hintergrund/Mehrwert

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

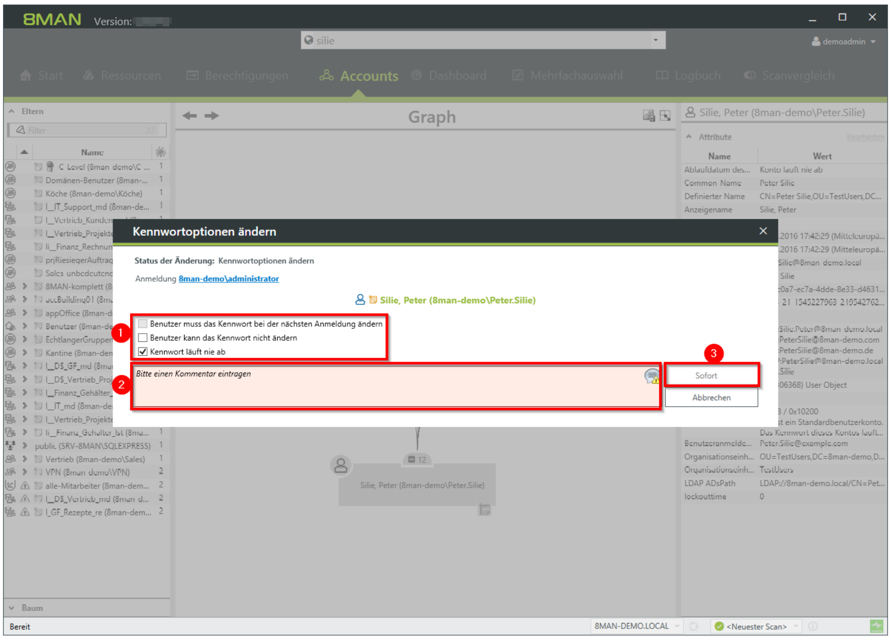
Additional Services

Changing password options in bulk

Step by step process



1. Finden Sie den gewünschten Benutzer mit der Suche.
2. Rechtsklicken Sie den Benutzer, z. B. in der Accounts-Ansicht und wählen "Kennwortoptionen ändern" im Kontextmenü.



Kennwortoptionen ändern

Status der Änderung: Kennwortoptionen ändern

Anmeldung 8man-demo\administrator

Silie, Peter (8man-demo\Peter.Silie)

□ Benutzer muss das Kennwort bei der nächsten Anmeldung ändern
□ Benutzer kann das Kennwort nicht ändern
☑ Kennwort läuft nie ab

Bitte einen Kommentar eintragen

1. Legen Sie Kennwortoptionen fest.
2. Sie müssen einen Kommentar eingeben, z. B. "Ticketnummer", "Beauftragt von" oder "Genehmigt von".
3. Starten Sie das Rücksetzen.

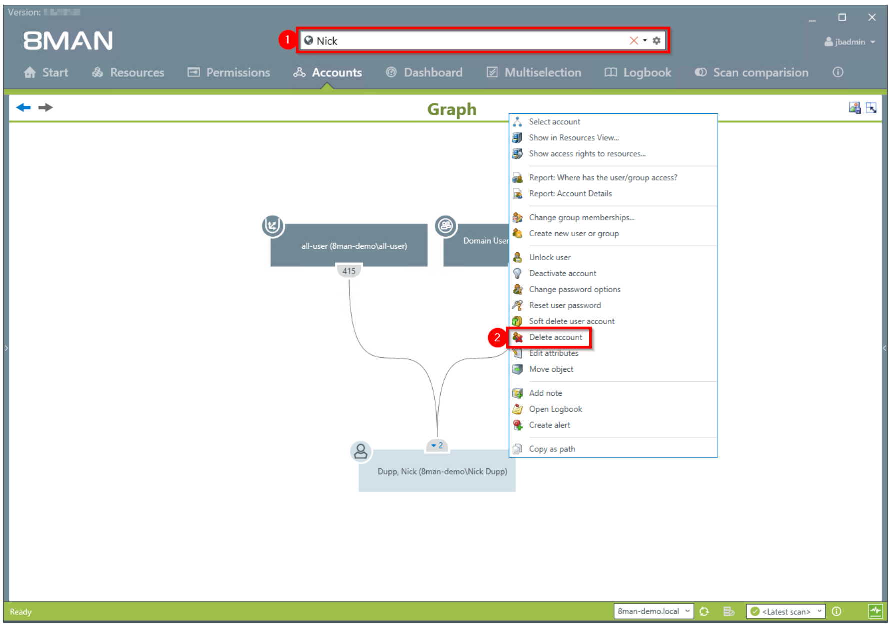
8.1.2 Helpdesk

8.1.2.1 Removing a user and their permissions

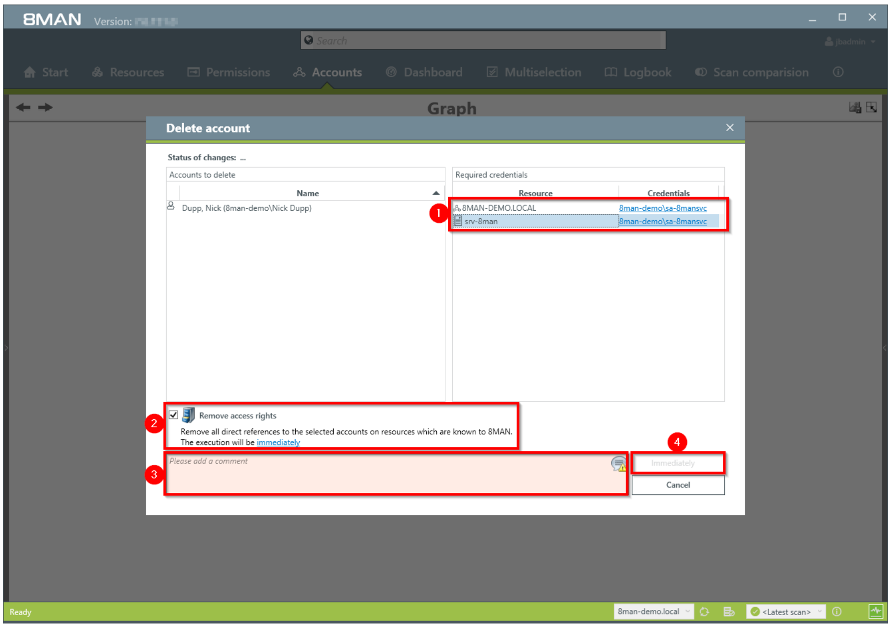
Background / Value

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

Step by step process



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



Delete account

Status of changes: ...

Accounts to delete

Name
Dupp, Nick (8man-demo\Nick Dupp)

Required credentials

Resource	Credentials
8MAN-DEMO.LOCAL	8man-demo\sa-8mansvc
srv-8man	8man-demo\sa-8mansvc

☑ Remove access rights

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

Please add a comment

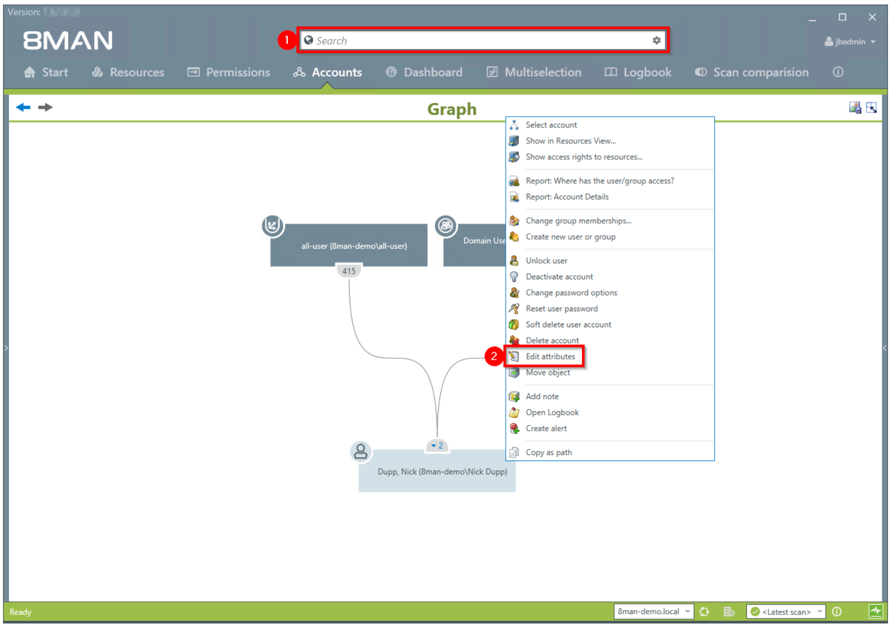
1. *If required change the credentials to remove the access rights.*
1. *Activate the option "Remove access rights" to avoid unresolved SIDs on file servers.*
2. *You must enter a comment, for example "ticket number" or "authorized by".*
3. *Start the process.*

8.1.2.2 Managing group and user attributes

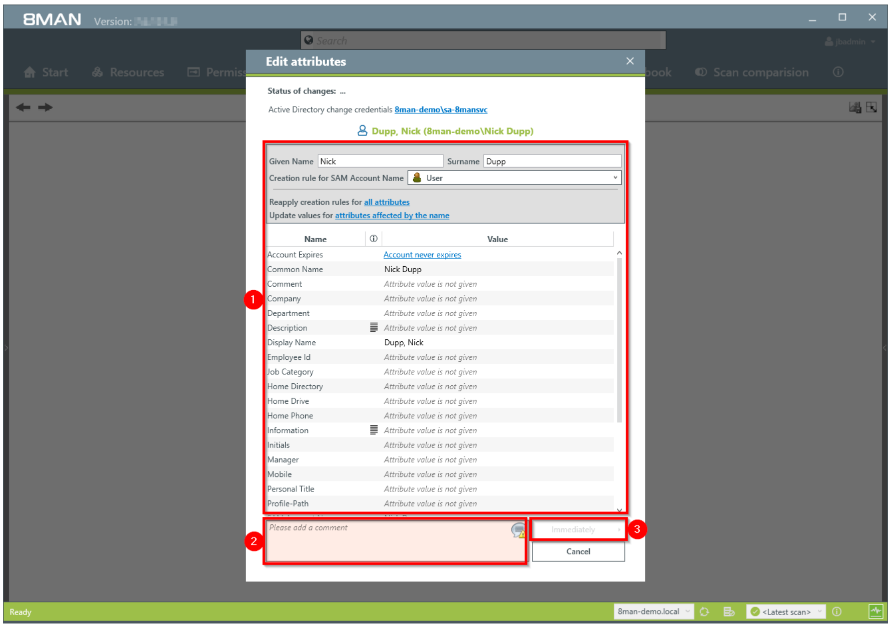
Background / Value

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

Step by step process



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



Edit attributes

Status of changes: ...

Active Directory change credentials 8man-demo\sa-8mansvc

Dupp, Nick (8man-demo\Nick Dupp)

Given Name: Nick   Surname: Dupp

Creation rule for SAM Account Name: User

Reapply creation rules for all attributes

Update values for attributes affected by the name

Name	ⓘ	Value
Account Expires		Account never expires
Common Name		Nick Dupp
Comment		*Attribute value is not given*
Company		*Attribute value is not given*
Department		*Attribute value is not given*
Description	≣	*Attribute value is not given*
Display Name		Dupp, Nick
Employee Id		*Attribute value is not given*
Job Category		*Attribute value is not given*
Home Directory		*Attribute value is not given*
Home Drive		*Attribute value is not given*
Home Phone		*Attribute value is not given*
Information	≣	*Attribute value is not given*
Initials		*Attribute value is not given*
Manager		*Attribute value is not given*
Mobile		*Attribute value is not given*
Personal Title		*Attribute value is not given*
Profile-Path		*Attribute value is not given*

1. *Change the desired attributes.*
2. *You must enter a comment.*
3. *Start or plan the change.*

8.1.2.3 Unlocking user accounts

Background / Value

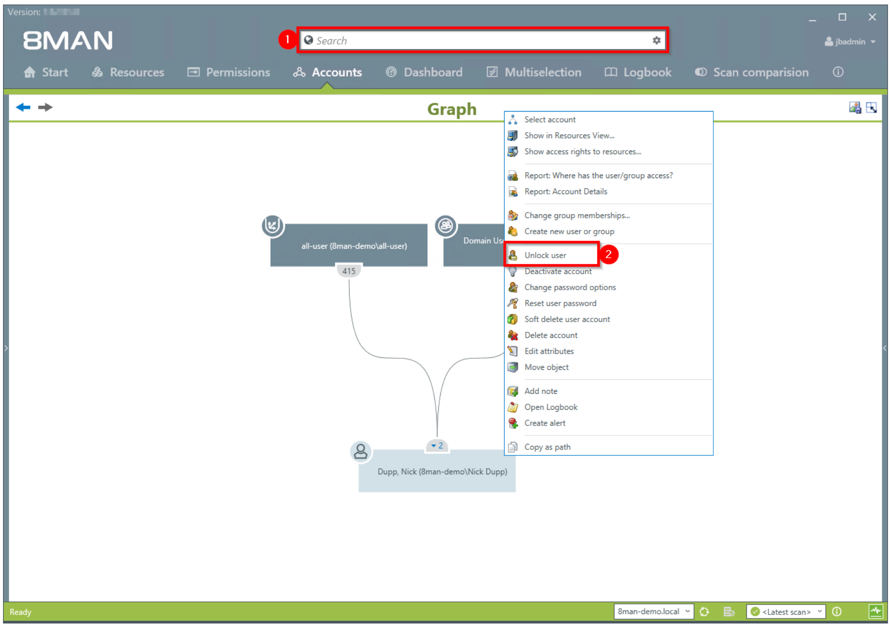
Unlocking user accounts is one of the most frequently performed action of most help desks. 8MAN makes the password reset revision proof. All actions are documented in the logbook.

Additional Services

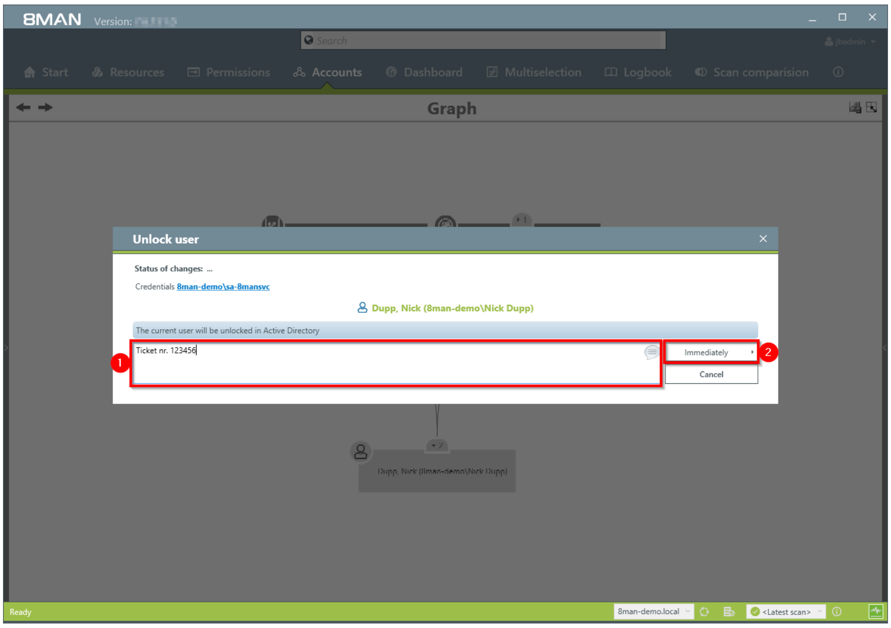
If employees use native tools to unlock a sensitive account, AD Logga will capture all activity. Especially sensitive accounts can be monitored with 8MATE Alerts.

AD Logga: Identifying locked user accounts
8MATE Alerts: Monitoring a user account

Step by step process



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



Unlock user

Status of changes: ...

Credentials 8man-demo\sa-8mansvc

Dupp, Nick (8man-demo\Nick Dupp)

The current user will be unlocked in Active Directory

Ticket nr. 123456

Immediately

Cancel

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

8.1.2.4 Deactivating a user account

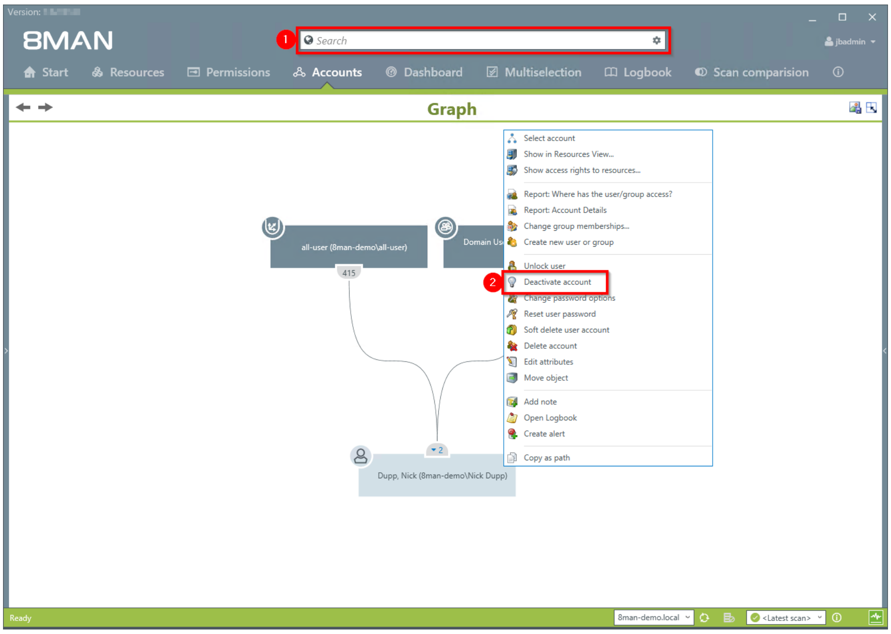
Background / Value

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

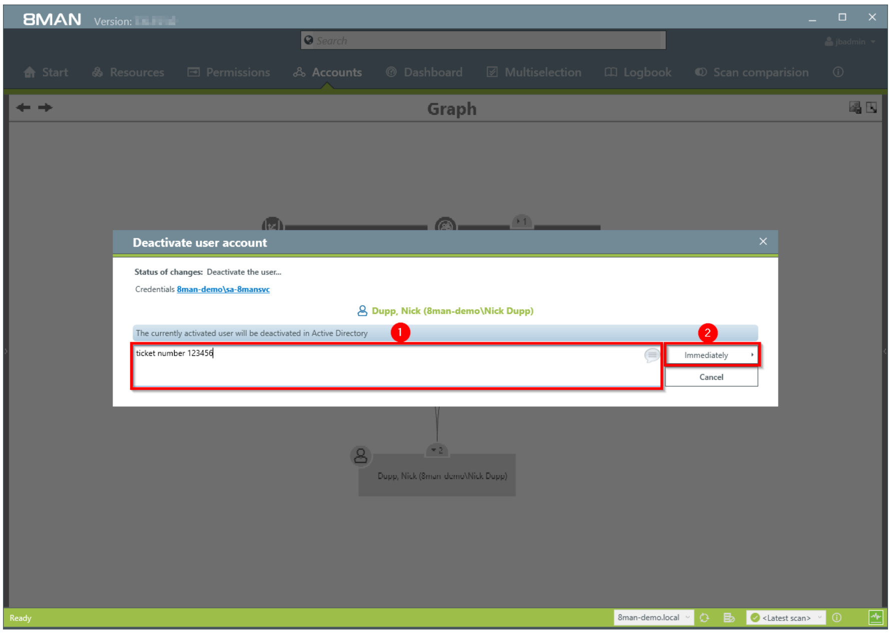
Additional services

Deleting a user with soft delete

Step by step process



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



Deactivate user account

Status of changes: Deactivate the user...

Credentials 8man-demo\sa-8mansvc

Dupp, Nick (8man-demo\Nick Dupp)

The currently activated user will be deactivated in Active Directory

ticket number 123456

Immediately

Cancel

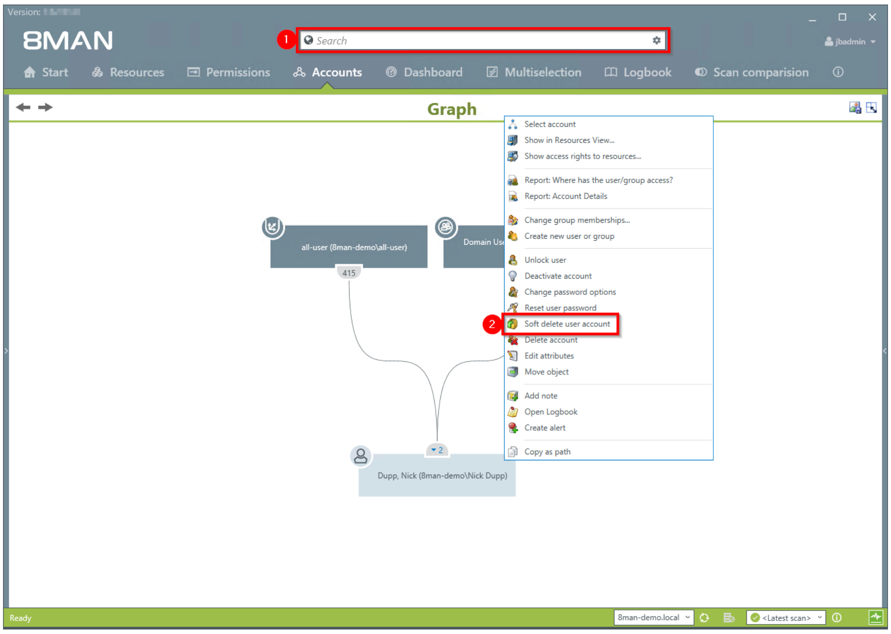
1. *You must enter a comment, for example "ticket number" or "authorized by".*
2. *Start the process.*

8.1.2.5 Deleting a user account by using the "soft delete" feature

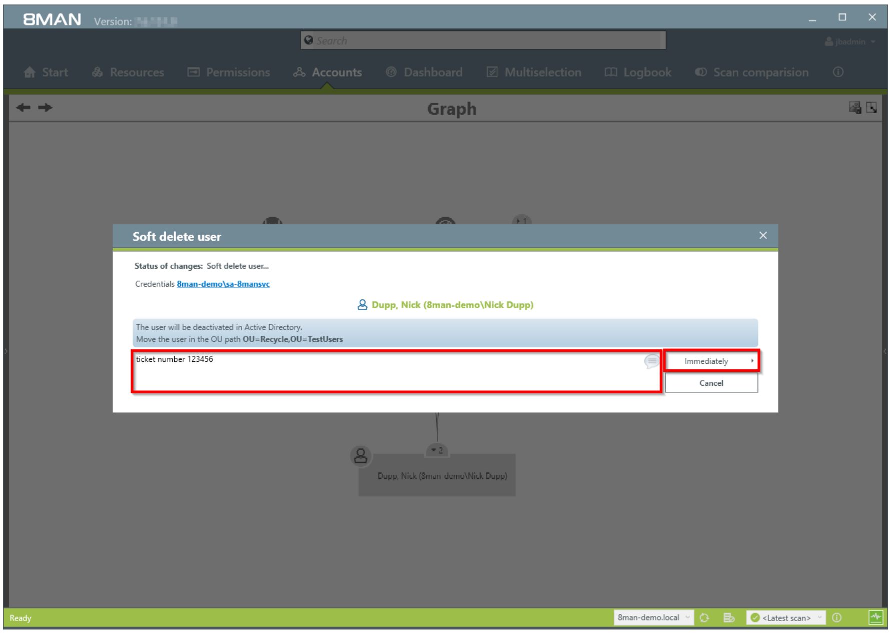
Background / Value

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

Step by step process



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



Soft delete user

Status of changes: Soft delete user...

Credentials 8man-demo\sa-8mansvc

Dupp, Nick (8man-demo\Nick Dupp)

The user will be deactivated in Active Directory.
Move the user in the OU path **OU=Recycle,OU=TestUsers**

ticket number 123456

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

8.1.2.6 Resetting passwords

Background / Value

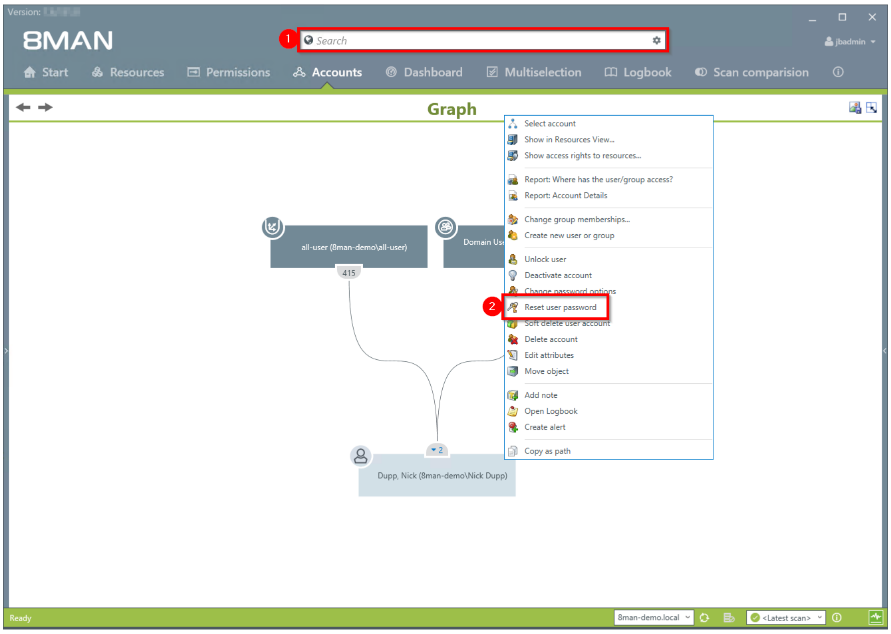
Resetting passwords is one of the most common tasks performed by help desks. 8MAN allows an easy and secure way of resetting passwords. All sensitive actions are documented in the log book. If an employee uses native tools to reset a password and illegally tries to access that user account, the incident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

Additional services

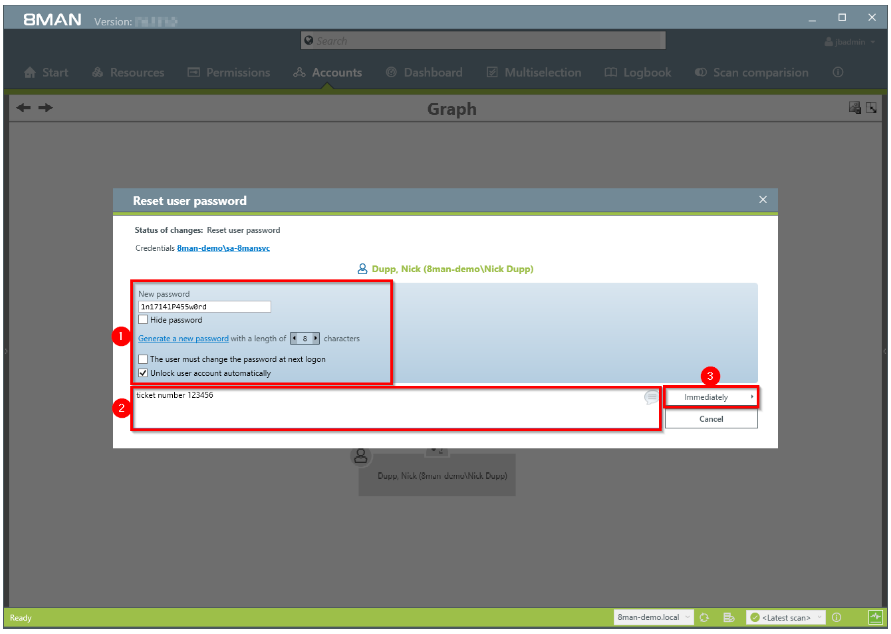
8MATE AD Logga: Identifying locked accounts

8MATE Alerts: Monitoring a user account

Step by step process



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



Status of changes: Reset user password

Credentials 8man-demo\sa-8mansvc

Dupp, Nick (8man-demo\Nick Dupp)

New password: 1n17141P455w0rd

☐ Hide password

Generate a new password with a length of 8 characters

☐ The user must change the password at next logon

☑ Unlock user account automatically

ticket number 123456

Immediately

Cancel

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

8.2 Fileserver

8.2.1 Data Owner

8.2.1.1 Changing folder permissions

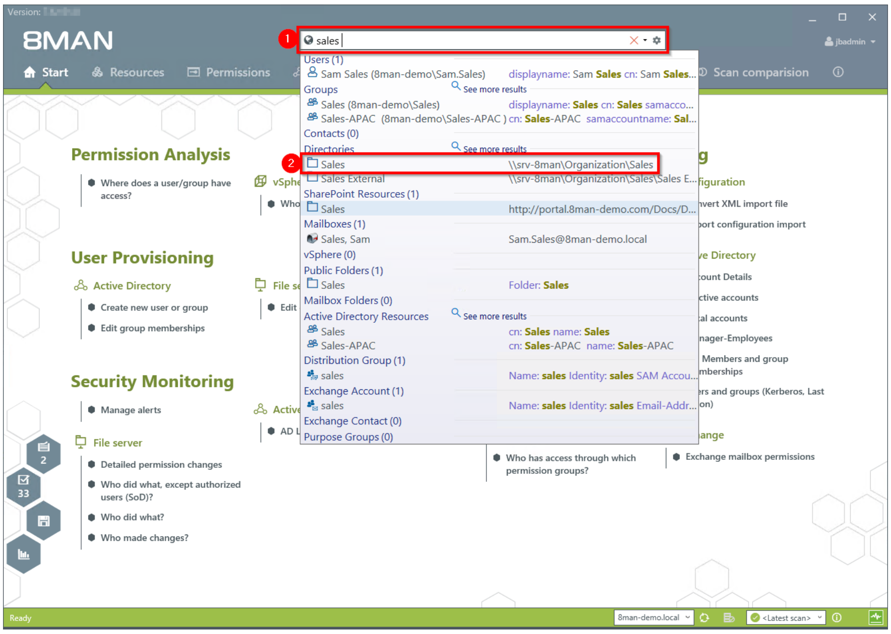
Background / Value

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

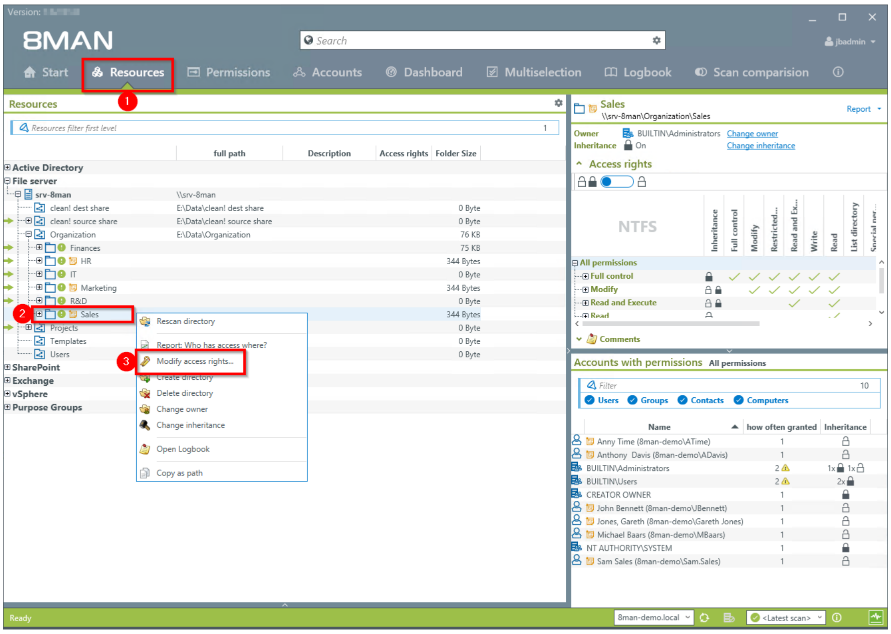
Simply decide what type of access rights you would like to assign: modify or read and execute.

In order to maintain data integrity we recommend assigning change rights only to carefully selected employees.

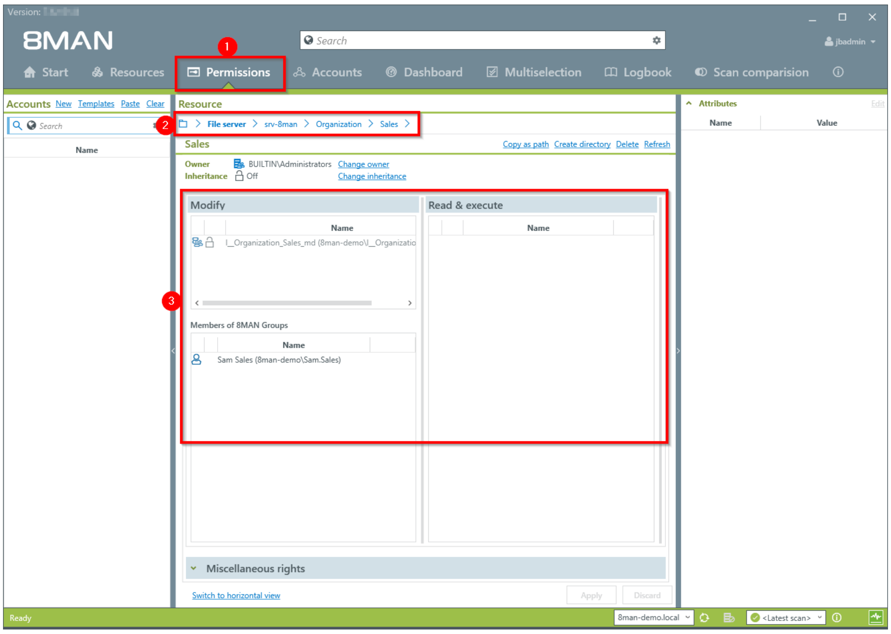
Step by step process


8MAN
Start
Resources
Permissions
Scan comparision
1
sales
Users (1)
Sam Sales (8man-demo\Sam.Sales) displayname: Sam Sales cn: Sam Sales...
Groups
See more results
Sales (8man-demo\Sales) displayname: Sales cn: Sales samacco...
Sales-APAC (8man-demo\Sales-APAC) cn: Sales-APAC samaccountname: Sal...
Contacts (0)
Directories
See more results
2
Sales \\srv-8man\Organization\Sales
Sales External \\srv-8man\Organization\Sales\Sales E...
SharePoint Resources (1)
Sales http://portal.8man-demo.com/Docs/D...
Mailboxes (1)
Sales, Sam Sam.Sales@8man-demo.local
vSphere (0)
Public Folders (1)
Sales Folder: Sales
Mailbox Folders (0)
Active Directory Resources
See more results
Sales cn: Sales name: Sales
Sales-APAC cn: Sales-APAC name: Sales-APAC
Distribution Group (1)
sales Name: sales Identity: sales SAM Accou...
Exchange Account (1)
sales Name: sales Identity: sales Email-Addr...
Exchange Contact (0)
Purpose Groups (0)
Permission Analysis
Where does a user/group have access?
User Provisioning
Active Directory
Create new user or group
Edit group memberships
Security Monitoring
Manage alerts
File server
Detailed permission changes
Who did what, except authorized users (SoD)?
Who did what?
Who made changes?
Who has access through which permission groups?
Exchange mailbox permissions
Ready
8man-demo.local
<Latest scan>

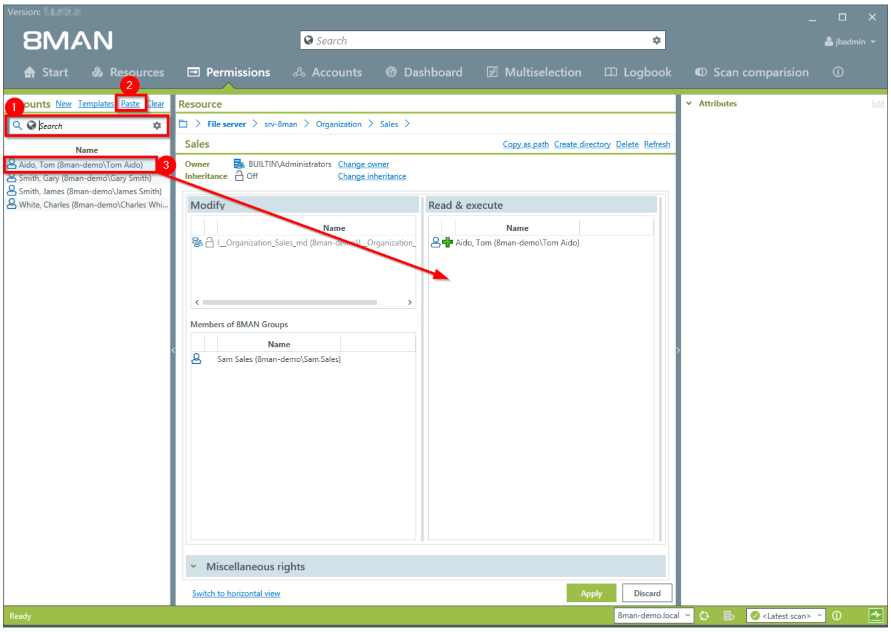
1. *Use the search field to find the desired directory.*
2. *Click on the search result.*



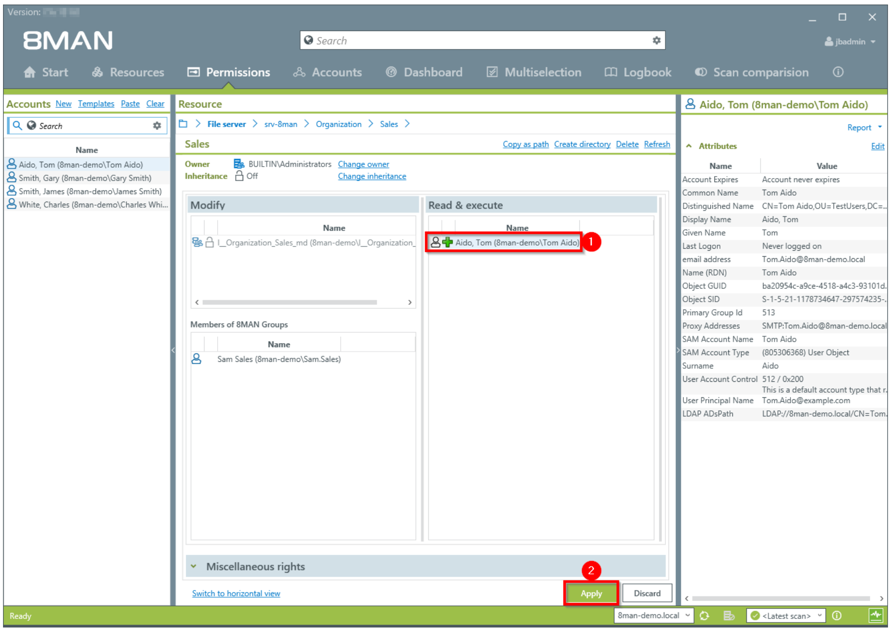
1. 8MAN switches to the "Resources" view.
2. Select a sub-directory if desired by right-clicking on it.
3. Select "Modify access rights...".



1. 8MAN switches to the "Permissions" view.
2. 8MAN shows you the directory that you are working on. You can change this directory.
3. 8MAN shows you all existing access rights in the categories "Modify" and "Read & execute".

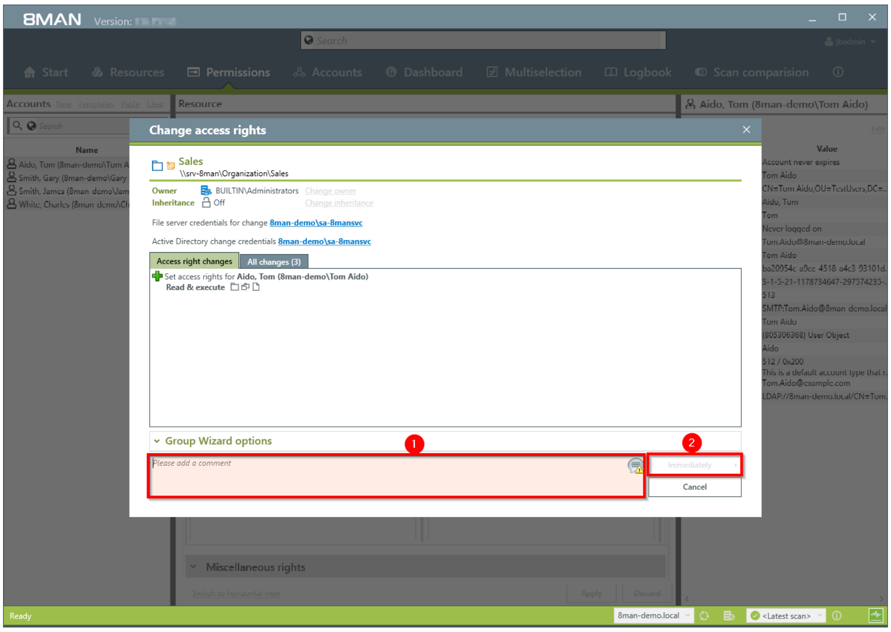

8MAN
Search
jbadmin
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
Accounts New Templates Paste Clear
Search
Name
Aido, Tom (8man-demo\Tom Aido)
Smith, Gary (8man-demo\Gary Smith)
Smith, James (8man-demo\James Smith)
White, Charles (8man-demo\Charles Whi...
Resource
File server > srv-8man > Organization > Sales >
Sales
Copy as path Create directory Delete Refresh
Owner BUILTIN\Administrators Change owner
Inheritance Off Change inheritance
Modify
Name
l__Organization_Sales_md (8man-demo\l__Organization_
Read & execute
Name
Aido, Tom (8man-demo\Tom Aido)
Members of 8MAN Groups
Name
Sam Sales (8man-demo\Sam.Sales)
Miscellaneous rights
Switch to horizontal view
Apply
Discard
Attributes
Edit
Ready
8man-demo.local
<Latest scan>
1
2
3

1. *Use the search field to find the desired user or group.*
2. *You can enter the content into the clipboard, for example an 8MAN Text. 8MAN will then find known objects and filter them from the text.*
3. *Use drag & drop to move the users into a column and assign corresponding access rights.*


8MAN
Search
jbadmin
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
Accounts New Templates Paste Clear
Search
Name
Aido, Tom (8man-demo\Tom Aido)
Smith, Gary (8man-demo\Gary Smith)
Smith, James (8man-demo\James Smith)
White, Charles (8man-demo\Charles Whi...
Resource
File server > srv-8man > Organization > Sales >
Sales
Copy as path Create directory Delete Refresh
Owner BUILTIN\Administrators Change owner
Inheritance Off Change inheritance
Modify
Name
l__Organization_Sales_md (8man-demo\l__Organization_
Read & execute
Name
Aido, Tom (8man-demo\Tom Aido)
Members of 8MAN Groups
Name
Sam Sales (8man-demo\Sam.Sales)
Miscellaneous rights
Switch to horizontal view
Apply
Discard
Aido, Tom (8man-demo\Tom Aido)
Report
Attributes
Edit
Ready
8man-demo.local
<Latest scan>
1
2

Name	Value
Account Expires	Account never expires
Common Name	Tom Aido
Distinguished Name	CN=Tom Aido,OU=TestUsers,DC=..
Display Name	Aido, Tom
Given Name	Tom
Last Logon	Never logged on
email address	Tom.Aido@8man-demo.local
Name (RDN)	Tom Aido
Object GUID	ba20954c-a9ce-4518-a4c3-93101d.
Object SID	S-1-5-21-1178734647-297574235-.
Primary Group Id	513
Proxy Addresses	SMTP:Tom.Aido@8man-demo.local
SAM Account Name	Tom Aido
SAM Account Type	(805306368) User Object
Surname	Aido
User Account Control	512 / 0x200 This is a default account type that r.
User Principal Name	Tom.Aido@example.com
LDAP ADsPath	LDAP://8man-demo.local/CN=Tom.

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



Change access rights

Sales
\\srv-8man\Organization\Sales

Owner BUILTIN\Administrators Change owner
Inheritance Off Change inheritance

File server credentials for change 8man-demo\sa-8mansvc

Active Directory change credentials 8man-demo\sa-8mansvc

Access right changes | All changes (3)

Set access rights for **Aido, Tom (8man-demo\Tom Aido)**
Read & execute

Group Wizard options

Please add a comment

Immediately

Cancel

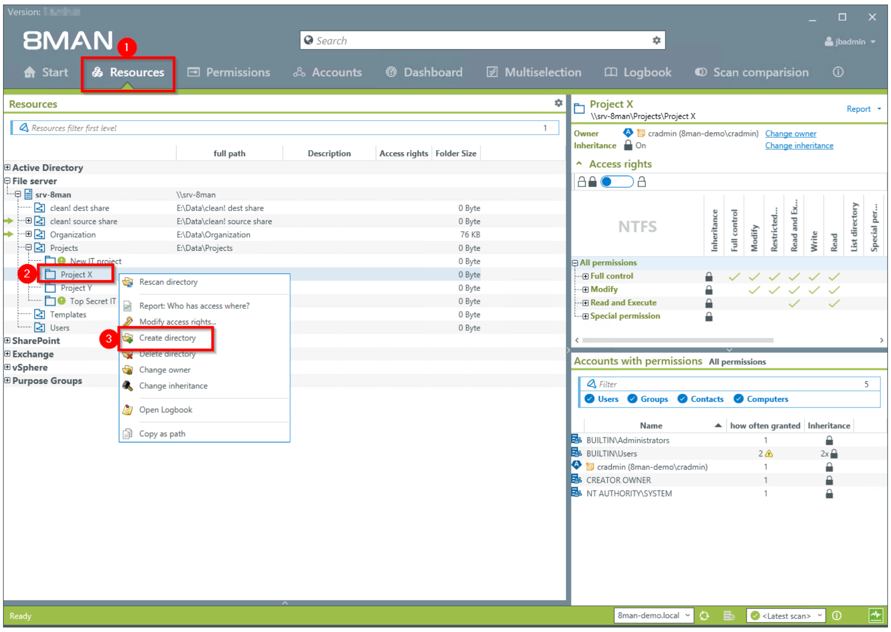
1. *You must enter a comment.*
2. *Start the access rights change.*

8.2.1.2 Creating a protected file server directory

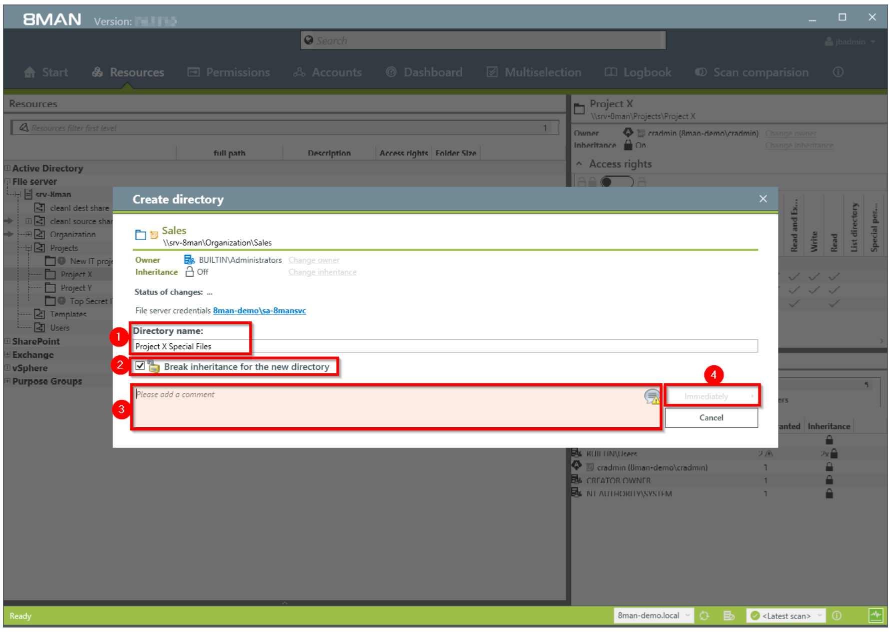
Background / Value

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.

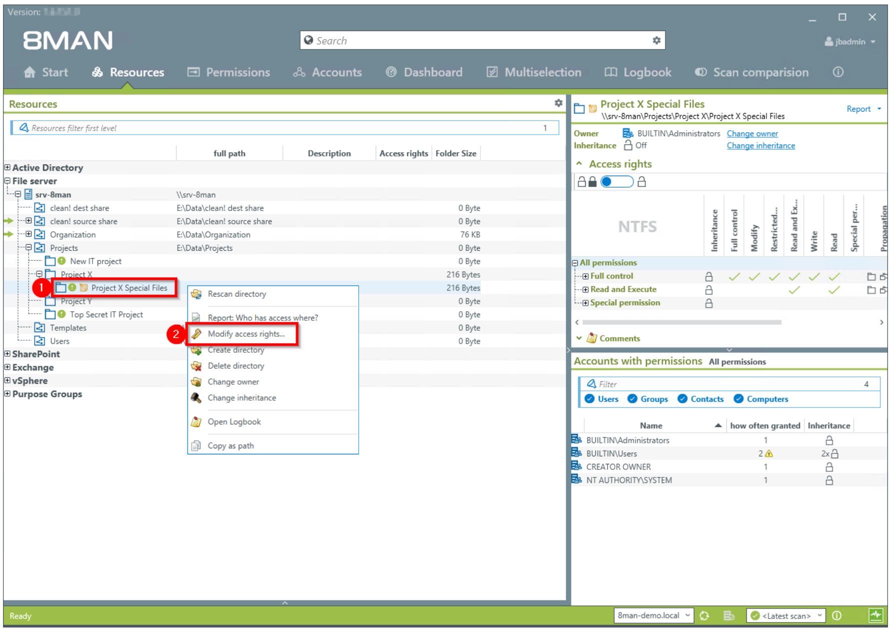
Step by step process



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


Create directory
Sales
\\srv-8man\Organization\Sales
Owner BUILTIN\Administrators
Inheritance Off
Status of changes: ...
File server credentials 8man-demo\sa-8mansvc
Directory name:
Project X Special Files
☑ Break inheritance for the new directory
Please add a comment
Immediately
Cancel
1
2
3
4

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



	full path	Description	Access rights	Folder Size
Active Directory				
File server				
srv-8man	\\srv-8man			
clean! dest share	E:\Data\clean! dest share			0 Byte
clean! source share	E:\Data\clean! source share			0 Byte
Organization	E:\Data\Organization			76 KB
Projects	E:\Data\Projects			0 Byte
New IT project				0 Byte
Project X				216 Bytes
Project X Special Files				216 Bytes
Project Y				0 Byte
Top Secret IT Project				0 Byte
Templates				0 Byte
Users				0 Byte
SharePoint				
Exchange				
vSphere				
Purpose Groups				

Project X Special Files
\\srv-8man\Projects\Project X\Project X Special Files

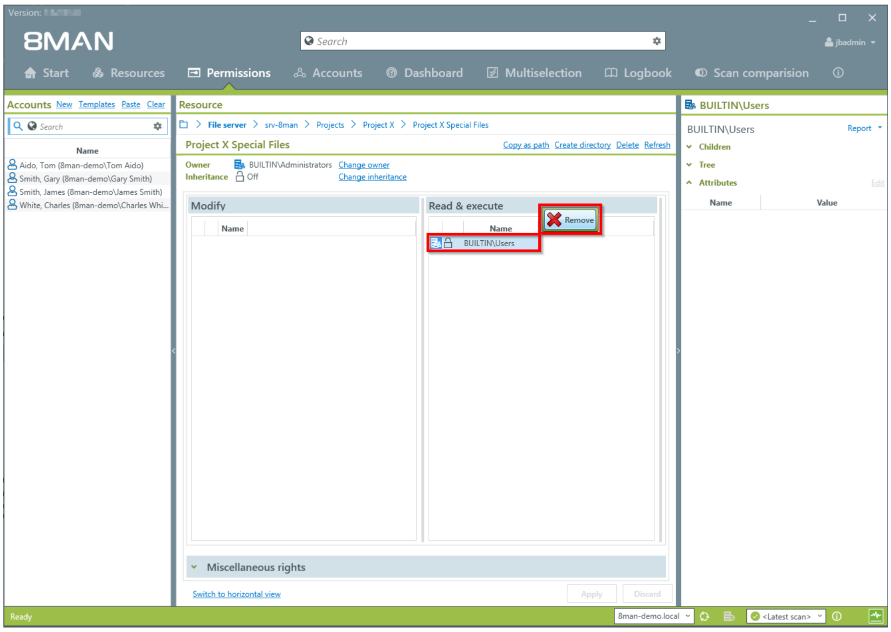
Owner BUILTIN\Administrators Change owner
Inheritance Off Change inheritance

Accounts with permissions All permissions

Name	how often granted	Inheritance
BUILTIN\Administrators	1	
BUILTIN\Users	2 ⚠	2x
CREATOR OWNER	1	
NT AUTHORITY\SYSTEM	1	

1. Navigate to the newly created directory.

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



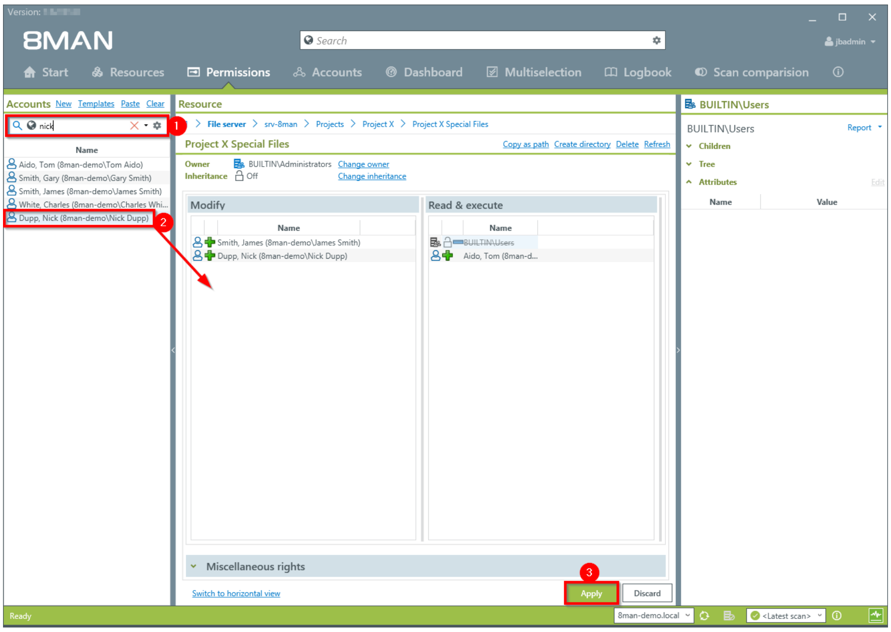
Name
Aido, Tom (8man-demo\Tom Aido)
Smith, Gary (8man-demo\Gary Smith)
Smith, James (8man-demo\James Smith)
White, Charles (8man-demo\Charles Whi...

Project X Special Files

Owner BUILTIN\Administrators Change owner
Inheritance Off Change inheritance

Read & execute: BUILTIN\Users

Remove all unnecessary access rights.



nick

Name
Aido, Tom (8man-demo\Tom Aido)
Smith, Gary (8man-demo\Gary Smith)
Smith, James (8man-demo\James Smith)
White, Charles (8man-demo\Charles Whi...
Dupp, Nick (8man-demo\Nick Dupp)

File server > srv-8man > Projects > Project X > Project X Special Files

Project X Special Files

Owner BUILTIN\Administrators
Inheritance Off

Modify

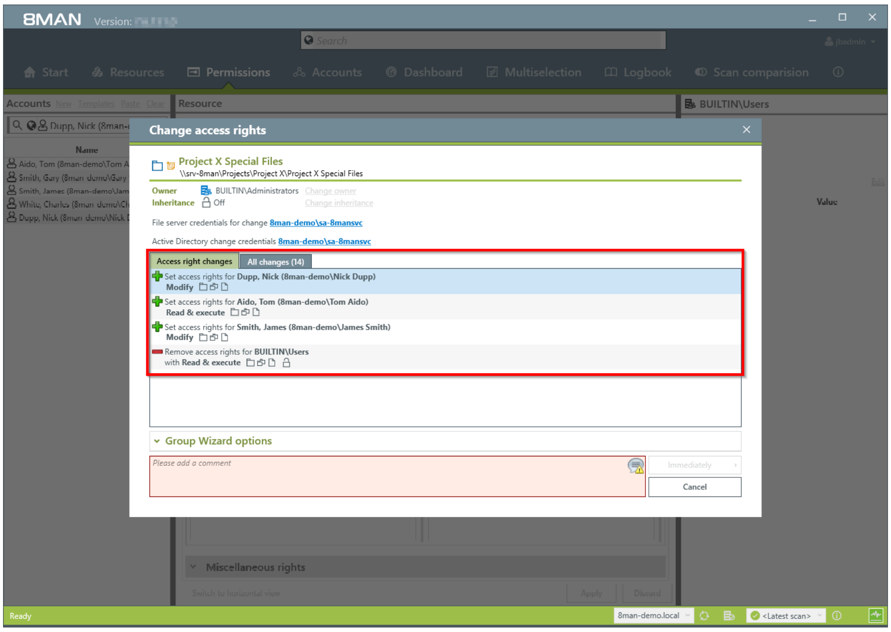
Name
Smith, James (8man-demo\James Smith)
Dupp, Nick (8man-demo\Nick Dupp)

Read & execute

Name
~~BUILTIN\Users~~
Aido, Tom (8man-d...

BUILTIN\Users

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.*



Change access rights

Project X Special Files
\\srv-8man\Projects\Project X\Project X Special Files

Owner BUILTIN\Administrators
Inheritance Off

File server credentials for change 8man-demo\sa-8mansvc

Active Directory change credentials 8man-demo\sa-8mansvc

Set access rights for **Dupp, Nick (8man-demo\Nick Dupp)**
Modify

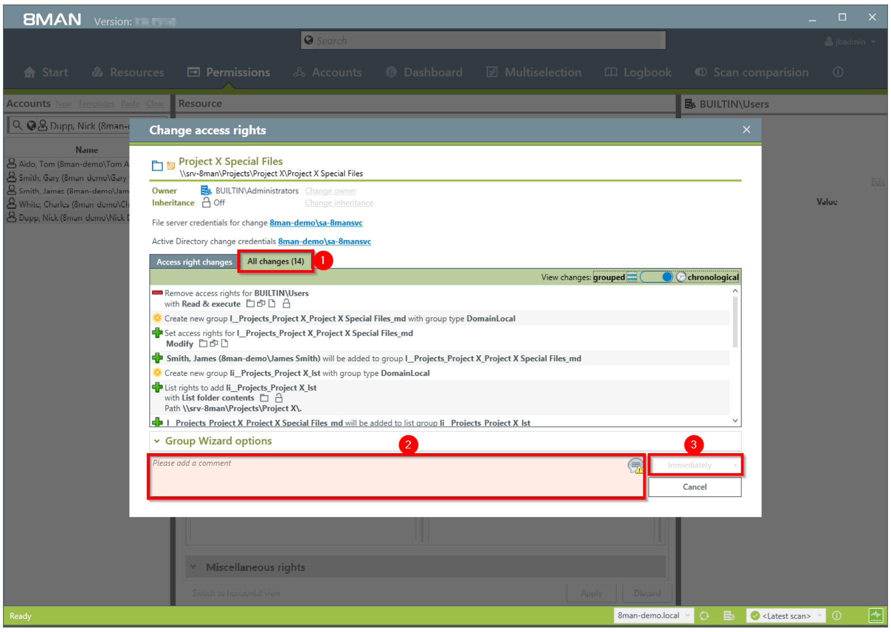
Set access rights for **Aido, Tom (8man-demo\Tom Aido)**
Read & execute

Set access rights for **Smith, James (8man-demo\James Smith)**
Modify

Remove access rights for **BUILTIN\Users**
with **Read & execute**

Please add a comment

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



Change access rights

Project X Special Files
\\srv-8man\Projects\Project X\Project X Special Files

Owner: BUILTIN\Administrators — Change owner
Inheritance: Off — Change inheritance

File server credentials for change 8man-demo\sa-8mansvc

Active Directory change credentials 8man-demo\sa-8mansvc

Access right changes | All changes (14)

View changes: grouped / chronological

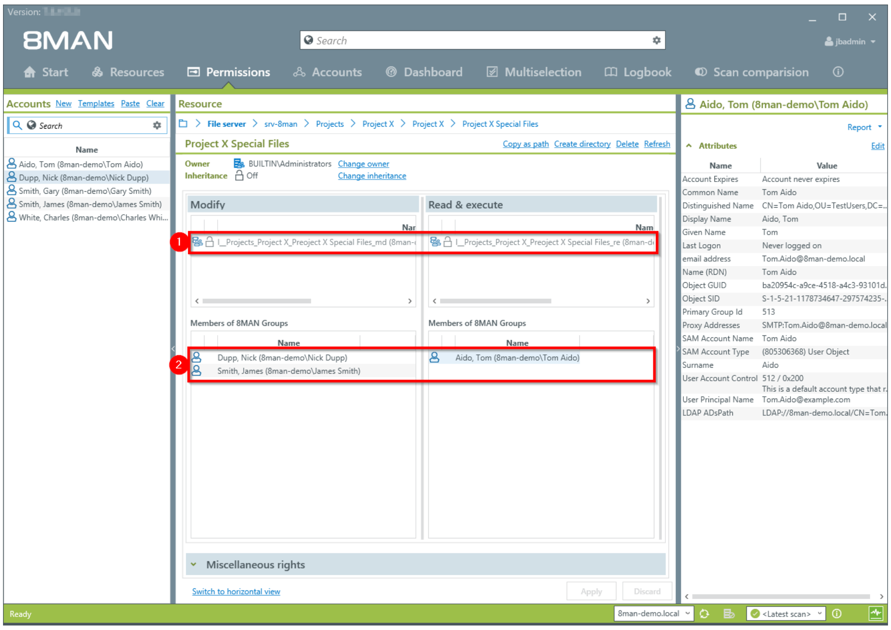
- Remove access rights for **BUILTIN\Users** with **Read & execute**
- Create new group **l_Projects_Project X_Project X Special Files_md** with group type **DomainLocal**
- Set access rights for **l_Projects_Project X_Project X Special Files_md** **Modify**
- **Smith, James (8man-demo\James Smith)** will be added to group **l_Projects_Project X_Project X Special Files_md**
- Create new group **li_Projects_Project X_lst** with group type **DomainLocal**
- List rights to add **li_Projects_Project X_lst** with **List folder contents** Path **\\srv-8man\Projects\Project X\.**
- **l_Projects_Project X_Project X Special Files_md** will be added to list group **li_Projects_Project X_lst**

Group Wizard options

Please add a comment

Immediately | Cancel

1. Click on the tab "All changes". You can then see all individual steps performed by the Group Wizard.
2. You must enter a comment.
3. Start the process.



Accounts:
- Aido, Tom (8man-demo\Tom Aido)
- Dupp, Nick (8man-demo\Nick Dupp)
- Smith, Gary (8man-demo\Gary Smith)
- Smith, James (8man-demo\James Smith)
- White, Charles (8man-demo\Charles Whi...

File server > srv-8man > Projects > Project X > Project X > Project X Special Files

Project X Special Files

Owner: BUILTIN\Administrators — Change owner
Inheritance: Off — Change inheritance

Modify: l_Projects_Project X_Preoject X Special Files_md (8man-
Members of 8MAN Groups: Dupp, Nick (8man-demo\Nick Dupp); Smith, James (8man-demo\James Smith)

Read & execute: l_Projects_Project X_Preoject X Special Files_re (8man-d
Members of 8MAN Groups: Aido, Tom (8man-demo\Tom Aido)

Aido, Tom (8man-demo\Tom Aido) — Attributes

Name	Value
Account Expires	Account never expires
Common Name	Tom Aido
Distinguished Name	CN=Tom Aido,OU=TestUsers,DC=..
Display Name	Aido, Tom
Given Name	Tom
Last Logon	Never logged on
email address	Tom.Aido@8man-demo.local
Name (RDN)	Tom Aido
Object GUID	ba20954c-a9ce-4518-a4c3-93101d.
Object SID	S-1-5-21-1178734647-297574235-.
Primary Group Id	513
Proxy Addresses	SMTP:Tom.Aido@8man-demo.local
SAM Account Name	Tom Aido
SAM Account Type	(805306368) User Object
Surname	Aido
User Account Control	512 / 0x200 This is a default account type that r.
User Principal Name	Tom.Aido@example.com
LDAP ADsPath	LDAP://8man-demo.local/CN=Tom.

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 Removing multiple access rights on file server directories

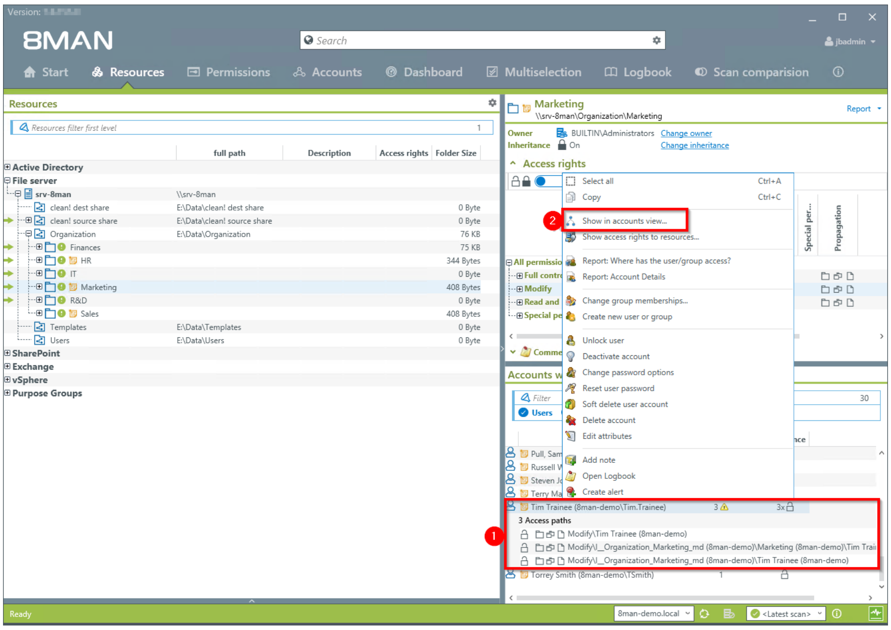
Background / Value

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

Identifying multiple access paths to file server directories

Step by step process



	full path	Description	Access rights	Folder Size
Active Directory				
File server				
srv-8man	\\srv-8man			
clean! dest share	E:\Data\clean! dest share			0 Byte
clean! source share	E:\Data\clean! source share			0 Byte
Organization	E:\Data\Organization			76 KB
Finances				75 KB
HR				344 Bytes
IT				0 Byte
Marketing				408 Bytes
R&D				0 Byte
Sales				408 Bytes
Templates	E:\Data\Templates			0 Byte
Users	E:\Data\Users			0 Byte
SharePoint				
Exchange				
vSphere				
Purpose Groups				

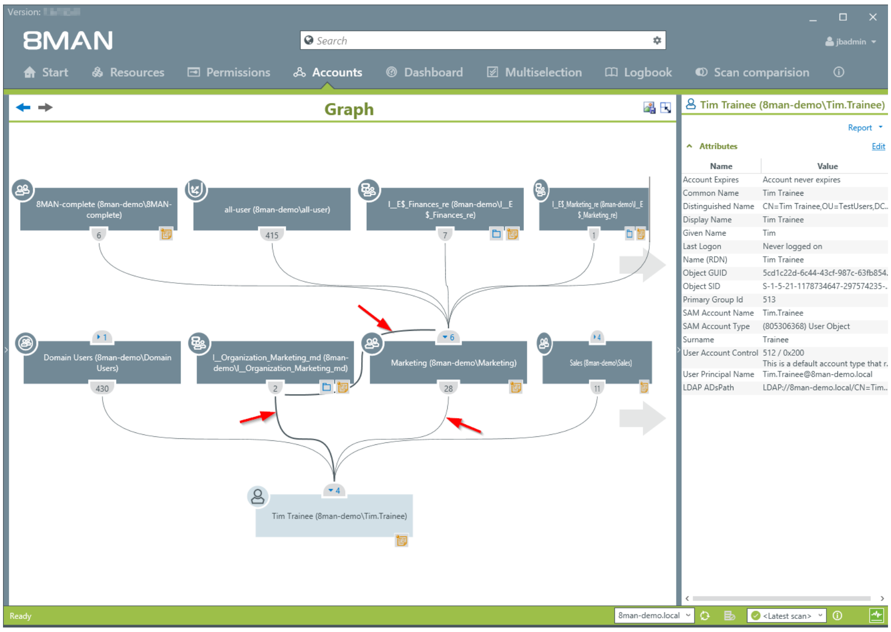
Marketing
\\srv-8man\Organization\Marketing

Owner BUILTIN\Administrators Change owner
Inheritance On Change inheritance

Pull, Sam
Russell W
Steven J
Terry Ma
Tim Trainee (8man-demo\Tim.Trainee) 3 ⚠ 3x
3 Access paths
Modify\Tim Trainee (8man-demo)
Modify\I__Organization_Marketing_md (8man-demo)\Marketing (8man-demo)\Tim Trai
Modify\I__Organization_Marketing_md (8man-demo)\Tim Trainee (8man-demo)
Torrey Smith (8man-demo\TSmith) 1

1. You have identified "Tim Trainee" as having multiple access paths.

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


8MAN
Search
jbadmin
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
Graph
8MAN-complete (8man-demo\8MAN-complete)
6
all-user (8man-demo\all-user)
415
I_E$_Finances_re (8man-demo\I_E$_Finances_re)
7
I_E$_Marketing_re (8man-demo\I_E$_Marketing_re)
1
Domain Users (8man-demo\Domain Users)
1
430
I_Organization_Marketing_md (8man-demo\I_Organization_Marketing_md)
2
Marketing (8man-demo\Marketing)
6
28
Sales (8man-demo\Sales)
11
Tim Trainee (8man-demo\Tim.Trainee)
4
Ready
8man-demo.local
<Latest scan>

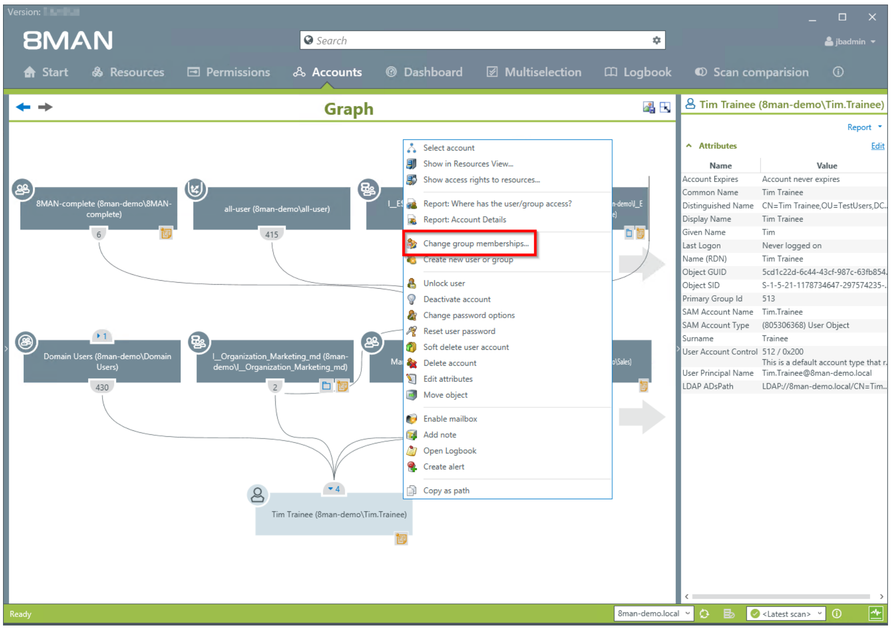
Tim Trainee (8man-demo\Tim.Trainee)

Report

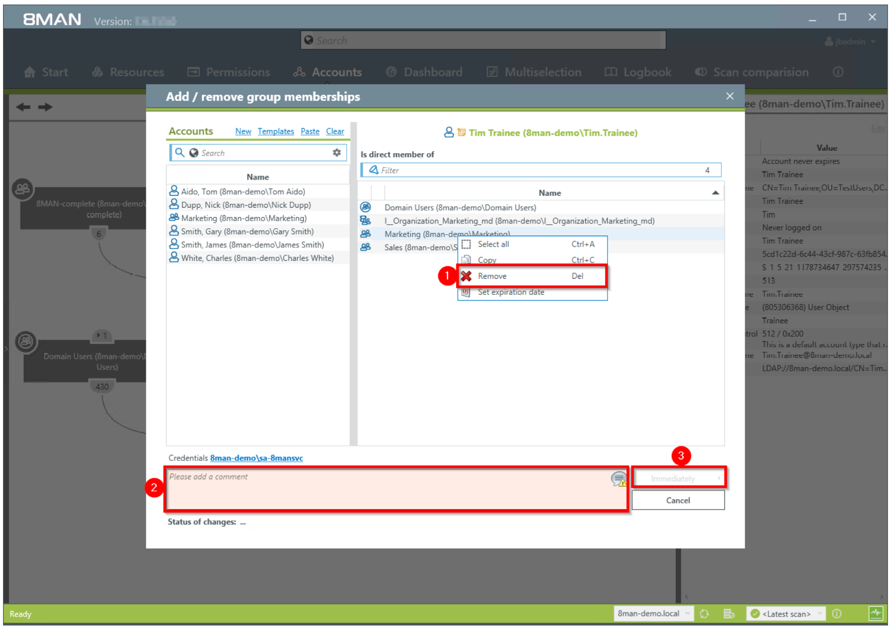
Attributes — Edit

Name	Value
Account Expires	Account never expires
Common Name	Tim Trainee
Distinguished Name	CN=Tim Trainee,OU=TestUsers,DC..
Display Name	Tim Trainee
Given Name	Tim
Last Logon	Never logged on
Name (RDN)	Tim Trainee
Object GUID	5cd1c22d-6c44-43cf-987c-63fb854.
Object SID	S-1-5-21-1178734647-297574235-..
Primary Group Id	513
SAM Account Name	Tim.Trainee
SAM Account Type	(805306368) User Object
Surname	Trainee
User Account Control	512 / 0x200 This is a default account type that r.
User Principal Name	Tim.Trainee@8man-demo.local
LDAP ADsPath	LDAP://8man-demo.local/CN=Tim..

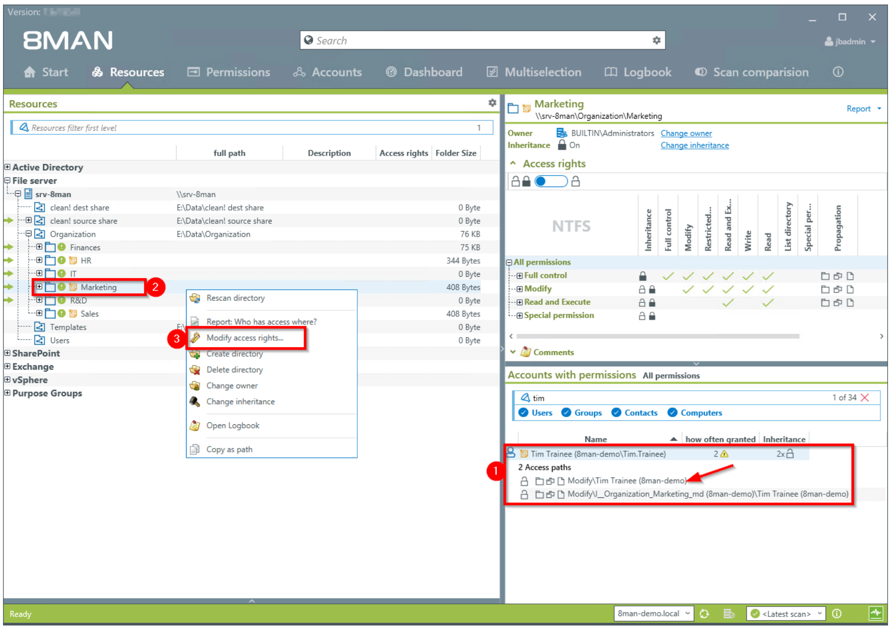
Use the AD graph to analyze multiple access paths.



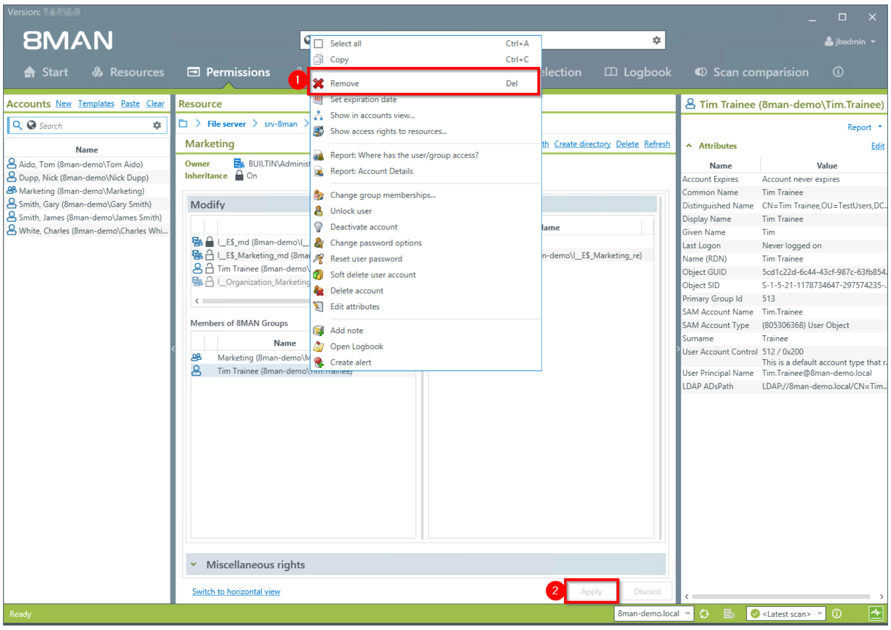
Right-click on the account and select "Change group memberships" from the context menu.


8MAN
Add / remove group memberships
Accounts New Templates Paste Clear
Search
Name
Aido, Tom (8man-demo\Tom Aido)
Dupp, Nick (8man-demo\Nick Dupp)
Marketing (8man-demo\Marketing)
Smith, Gary (8man-demo\Gary Smith)
Smith, James (8man-demo\James Smith)
White, Charles (8man-demo\Charles White)
Tim Trainee (8man-demo\Tim.Trainee)
Is direct member of
Filter
Domain Users (8man-demo\Domain Users)
I_Organization_Marketing_md (8man-demo\I_Organization_Marketing_md)
Marketing (8man-demo\Marketing)
Sales (8man-demo\Sales)
Select all Ctrl+A
Copy Ctrl+C
Remove Del
Set expiration date
Credentials 8man-demo\sa-8mansvc
Please add a comment
Immediately
Cancel
Status of changes: ...
1
2
3
Ready

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


8MAN
Search
Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparision
Resources
Resources filter first level
full path Description Access rights Folder Size
Active Directory
File server
srv-8man
clean! dest share
clean! source share
Organization
Finances
HR
IT
Marketing
R&D
Sales
Templates
Users
SharePoint
Exchange
vSphere
Purpose Groups
Rescan directory
Report: Who has access where?
Modify access rights...
Create directory
Delete directory
Change owner
Change inheritance
Open Logbook
Copy as path
Marketing
\\srv-8man\Organization\Marketing
Owner BUILTIN\Administrators Change owner
Inheritance On Change inheritance
Access rights
NTFS
All permissions
Full control
Modify
Read and Execute
Special permission
Comments
Accounts with permissions All permissions
tim
Users Groups Contacts Computers
Name how often granted Inheritance
Tim Trainee (8man-demo\Tim.Trainee)
2 Access paths
Modify\Tim Trainee (8man-demo)
Modify\I_Organization_Marketing_md (8man-demo)\Tim Trainee (8man-demo)
1
2
3
Ready

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.



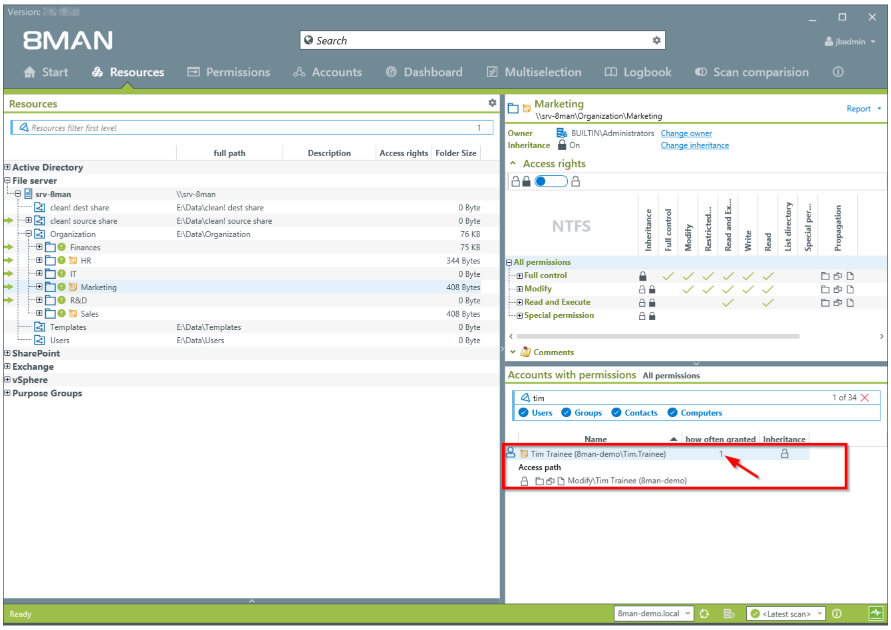
Tim Trainee (8man-demo\Tim.Trainee)

Report

Attributes Edit

Name	Value
Account Expires	Account never expires
Common Name	Tim Trainee
Distinguished Name	CN=Tim Trainee,OU=TestUsers,DC..
Display Name	Tim Trainee
Given Name	Tim
Last Logon	Never logged on
Name (RDN)	Tim Trainee
Object GUID	5cd1c22d-6c44-43cf-987c-63fb854..
Object SID	S-1-5-21-1178734647-297574235-..
Primary Group Id	513
SAM Account Name	Tim.Trainee
SAM Account Type	(805306368) User Object
Surname	Trainee
User Account Control	512 / 0x200 This is a default account type that r..
User Principal Name	Tim.Trainee@8man-demo.local
LDAP ADsPath	LDAP://8man-demo.local/CN=Tim..

1. *Select the desired user and chose "Remove".*
2. *Start the removal process.*



	full path	Description	Access rights	Folder Size
Active Directory				
File server				
srv-8man	\\srv-8man			
clean! dest share	E:\Data\clean! dest share			0 Byte
clean! source share	E:\Data\clean! source share			0 Byte
Organization	E:\Data\Organization			76 KB
Finances				75 KB
HR				344 Bytes
IT				0 Byte
Marketing				408 Bytes
R&D				0 Byte
Sales				408 Bytes
Templates	E:\Data\Templates			0 Byte
Users	E:\Data\Users			0 Byte
SharePoint				
Exchange				
vSphere				
Purpose Groups				

Marketing
\\srv-8man\Organization\Marketing

Report

Owner BUILTIN\Administrators Change owner
Inheritance On Change inheritance

Access rights

NTFS	Inheritance	Full control	Modify	Restricted...	Read and Ex...	Write	Read	List directory	Special per...	Propagation
All permissions										
Full control	🔒	✓	✓	✓	✓	✓	✓			
Modify	🔓🔒		✓	✓	✓	✓	✓			
Read and Execute	🔓🔒				✓		✓			
Special permission	🔓🔒									

Comments

Accounts with permissions All permissions

tim 1 of 34

Users Groups Contacts Computers

Name	how often granted	Inheritance
Tim Trainee (8man-demo\Tim.Trainee)	1	🔓

Access path
Modify\Tim Trainee (8man-demo)

Verify the result in the resource view.

8.2.2.2 Removing 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.

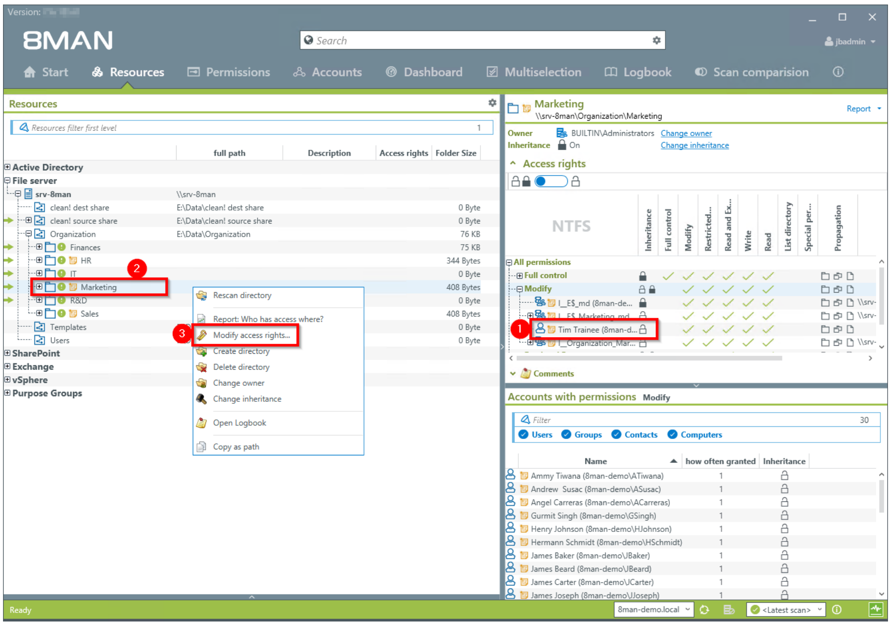
Additional Services

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

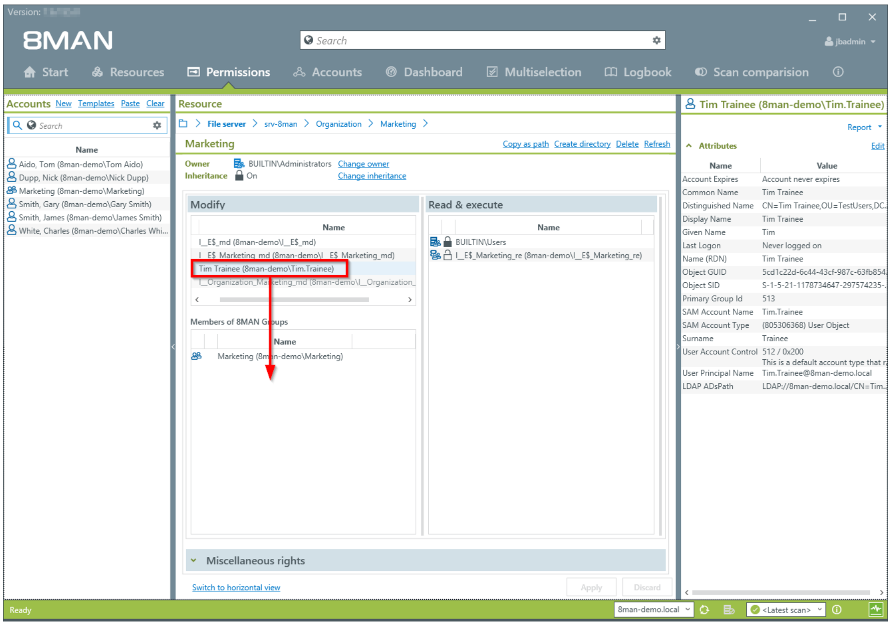
8MATE Clean! Handbook: Replacing direct permissions with group memberships

8MATE Clean! Handbook: Deleting direct access rights

Step by step process



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



Name
Aido, Tom (8man-demo\Tom Aido)
Dupp, Nick (8man-demo\Nick Dupp)
Marketing (8man-demo\Marketing)
Smith, Gary (8man-demo\Gary Smith)
Smith, James (8man-demo\James Smith)
White, Charles (8man-demo\Charles Whi...

Marketing

Owner BUILTIN\Administrators
Inheritance On

Modify

Name
I__E$_md (8man-demo\I__E$_md)
I__E$_Marketing_md (8man-demo\I__E$_Marketing_md)
Tim Trainee (8man-demo\Tim.Trainee)
I__Organization_Marketing_md (8man-demo\I__Organization_

Members of 8MAN Groups

Name
Marketing (8man-demo\Marketing)

Read & execute

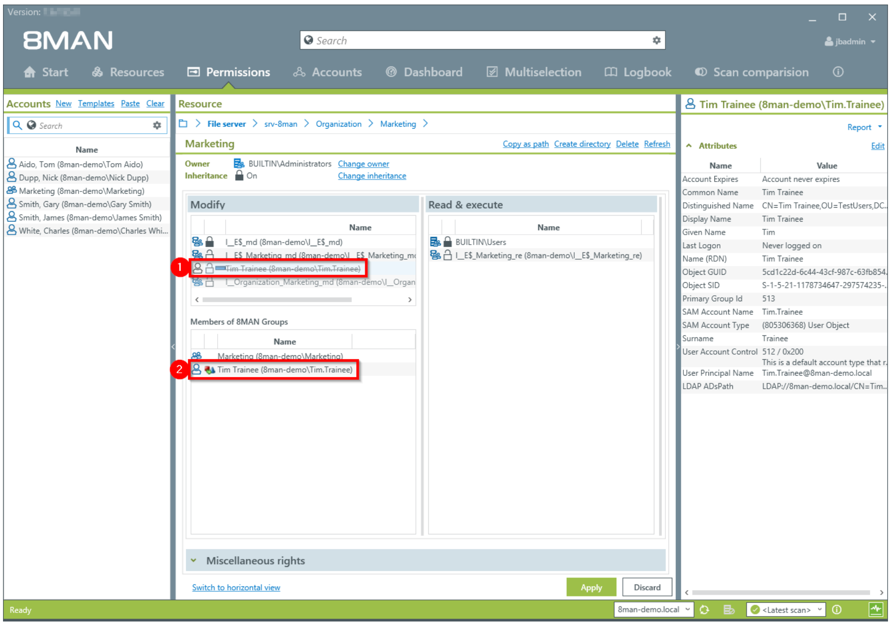
Name
BUILTIN\Users
I__E$_Marketing_re (8man-demo\I__E$_Marketing_re)

Tim Trainee (8man-demo\Tim.Trainee)

Attributes

Name	Value
Account Expires	Account never expires
Common Name	Tim Trainee
Distinguished Name	CN=Tim Trainee,OU=TestUsers,DC...
Display Name	Tim Trainee
Given Name	Tim
Last Logon	Never logged on
Name (RDN)	Tim Trainee
Object GUID	5cd1c22d-6c44-43cf-987c-63fb854...
Object SID	S-1-5-21-1178734647-297574235-...
Primary Group Id	513
SAM Account Name	Tim.Trainee
SAM Account Type	(805306368) User Object
Surname	Trainee
User Account Control	512 / 0x200 This is a default account type that r...
User Principal Name	Tim.Trainee@8man-demo.local
LDAP ADsPath	LDAP://8man-demo.local/CN=Tim...

Drag the user into the 8MAN group.



Name
Aido, Tom (8man-demo\Tom Aido)
Dupp, Nick (8man-demo\Nick Dupp)
Marketing (8man-demo\Marketing)
Smith, Gary (8man-demo\Gary Smith)
Smith, James (8man-demo\James Smith)
White, Charles (8man-demo\Charles Whi...

Marketing

Owner BUILTIN\Administrators
Inheritance On

Modify

Name
I__E$_md (8man-demo\I__E$_md)
I__E$_Marketing_md (8man-demo\I__E$_Marketing_m
~~Tim Trainee (8man-demo\Tim.Trainee)~~
I__Organization_Marketing_md (8man-demo\I__Organ

Members of 8MAN Groups

Name
Marketing (8man-demo\Marketing)
Tim Trainee (8man-demo\Tim.Trainee)

Read & execute

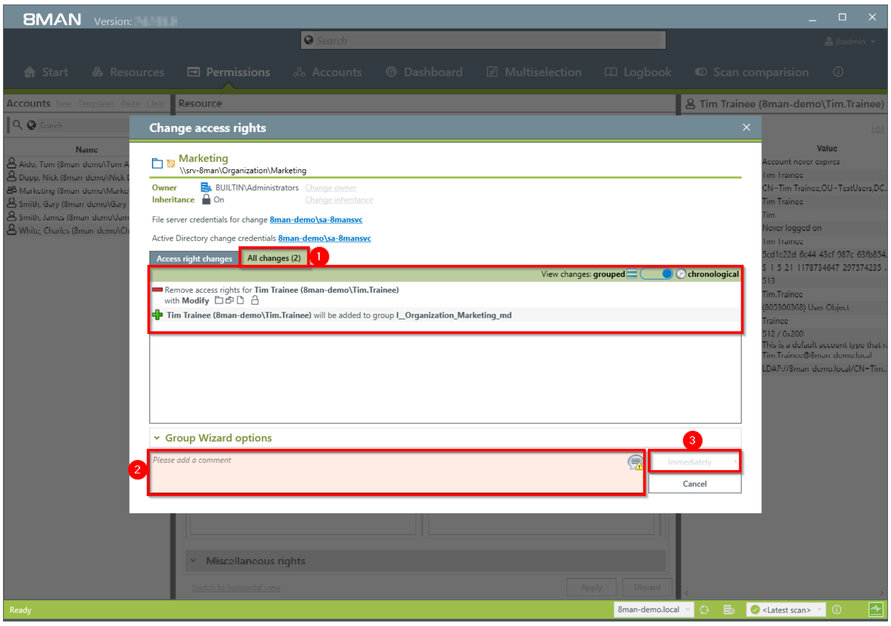
Name
BUILTIN\Users
I__E$_Marketing_re (8man-demo\I__E$_Marketing_re)

Tim Trainee (8man-demo\Tim.Trainee)

Attributes

Name	Value
Account Expires	Account never expires
Common Name	Tim Trainee
Distinguished Name	CN=Tim Trainee,OU=TestUsers,DC...
Display Name	Tim Trainee
Given Name	Tim
Last Logon	Never logged on
Name (RDN)	Tim Trainee
Object GUID	5cd1c22d-6c44-43cf-987c-63fb854...
Object SID	S-1-5-21-1178734647-297574235-...
Primary Group Id	513
SAM Account Name	Tim.Trainee
SAM Account Type	(805306368) User Object
Surname	Trainee
User Account Control	512 / 0x200 This is a default account type that r...
User Principal Name	Tim.Trainee@8man-demo.local
LDAP ADsPath	LDAP://8man-demo.local/CN=Tim...

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



Change access rights

Marketing
\\srv-8man\Organization\Marketing

Owner BUILTIN\Administrators Change owner
Inheritance On Change inheritance

File server credentials for change 8man-demo\sa-8mansvc

Active Directory change credentials 8man-demo\sa-8mansvc

Access right changes | All changes (2)

View changes: grouped / chronological

Remove access rights for **Tim Trainee (8man-demo\Tim.Trainee)** with **Modify**

Tim Trainee (8man-demo\Tim.Trainee) will be added to group **I_Organization_Marketing_md**

Group Wizard options

Please add a comment

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 Removing 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 shows all so called "Broken ACLs" and removes these by reapplying the proper inheritances.

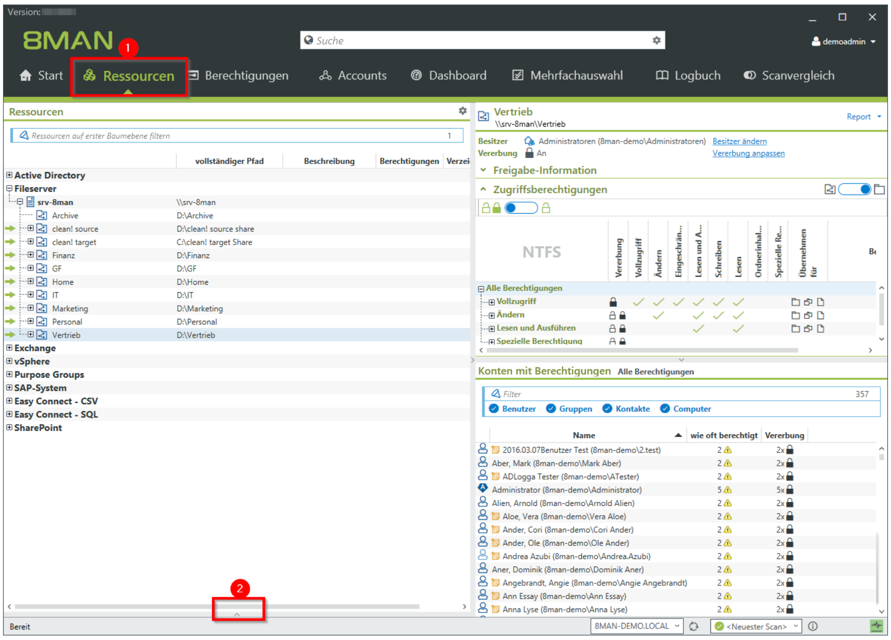
Step by step process

Sogenannte "Broken ACLs" (Access Control Lists) sind Fehler in der NTFS-Vererbung auf dem Fileserver. Die Folgen: Das Unterverzeichnis erhält nicht die korrekt vererbten Berechtigungen, obwohl die Vererbung aktiviert ist. 8MAN zeigt "Broken ACLs" und entfernt diese über die erneute Anwendung der Vererbungsfunktion.

Weiterführende Services

Abweichende Berechtigungen im Bulk entfernen (im Webclient)

Der Prozess in einzelnen Schritten



	vollständiger Pfad	Beschreibung	Berechtigungen	Verzei
⊞ Active Directory				
⊟ Fileserver				
⊟ srv-8man	\\srv-8man			
Archive	D:\Archive			
⊞ clean! source	D:\clean! source share			
⊞ clean! target	C:\clean! target Share			
⊞ Finanz	D:\Finanz			
⊞ GF	D:\GF			
⊞ Home	D:\Home			
⊞ IT	D:\IT			
⊞ Marketing	D:\Marketing			
⊞ Personal	D:\Personal			
⊞ Vertrieb	D:\Vertrieb			
⊞ Exchange				
⊞ vSphere				
⊞ Purpose Groups				
⊞ SAP-System				
⊞ Easy Connect - CSV				
⊞ Easy Connect - SQL				
⊞ SharePoint				

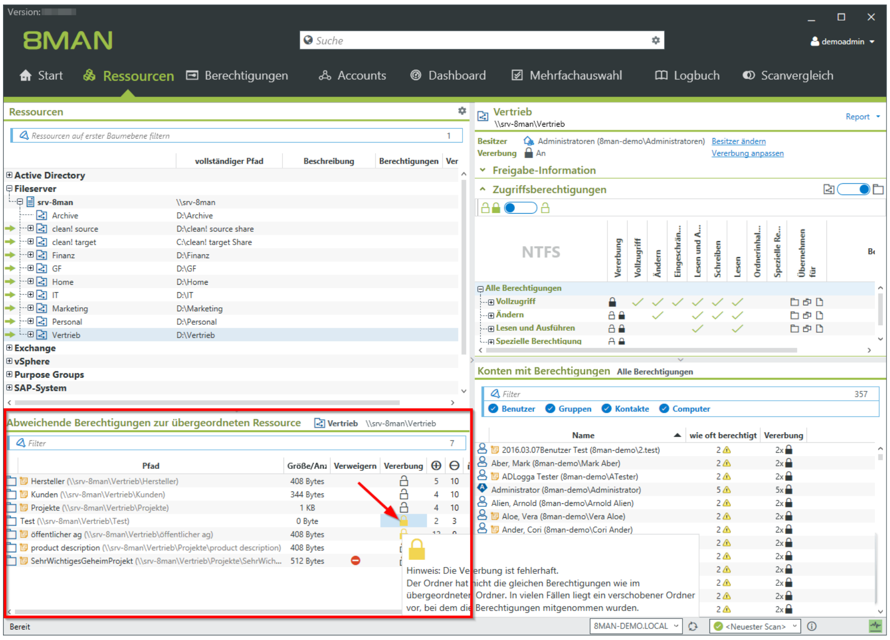
Vertrieb
\\srv-8man\Vertrieb

Besitzer: Administratoren (8man-demo\Administratoren) — Besitzer ändern
Vererbung: An — Vererbung anpassen

NTFS	Vererbung	Vollzugriff	Ändern	Eingeschrän...	Lesen und A...	Schreiben	Lesen	Ordnerinhal...	Spezielle Re...	Übernehmen für
⊟ Alle Berechtigungen										
⊞ Vollzugriff	🔒	✓	✓	✓	✓	✓	✓			
⊞ Ändern	🔓 🔒		✓		✓	✓	✓			
⊞ Lesen und Ausführen	🔓 🔒				✓		✓			
⊞ Spezielle Berechtigung	🔓 🔒									

Name	wie oft berechtigt	Vererbung
2016.03.07Benutzer Test (8man-demo\2.test)	2 ⚠	2x 🔒
Aber, Mark (8man-demo\Mark Aber)	2 ⚠	2x 🔒
ADLogga Tester (8man-demo\ATester)	2 ⚠	2x 🔒
Administrator (8man-demo\Administrator)	5 ⚠	5x 🔒
Alien, Arnold (8man-demo\Arnold Alien)	2 ⚠	2x 🔒
Aloe, Vera (8man-demo\Vera Aloe)	2 ⚠	2x 🔒
Ander, Cori (8man-demo\Cori Ander)	2 ⚠	2x 🔒
Ander, Ole (8man-demo\Ole Ander)	2 ⚠	2x 🔒
Andrea Azubi (8man-demo\Andrea.Azubi)	2 ⚠	2x 🔒
Aner, Dominik (8man-demo\Dominik Aner)	2 ⚠	2x 🔒
Angebrandt, Angie (8man-demo\Angie Angebrandt)	2 ⚠	2x 🔒
Ann Essay (8man-demo\Ann Essay)	2 ⚠	2x 🔒
Anna Lyse (8man-demo\Anna Lyse)	2 ⚠	2x 🔒

1. *Wählen Sie "Ressourcen".*
2. *Klappen Sie den Bereich auf.*



Abweichende Berechtigungen zur übergeordneten Ressource — Vertrieb \\srv-8man\Vertrieb

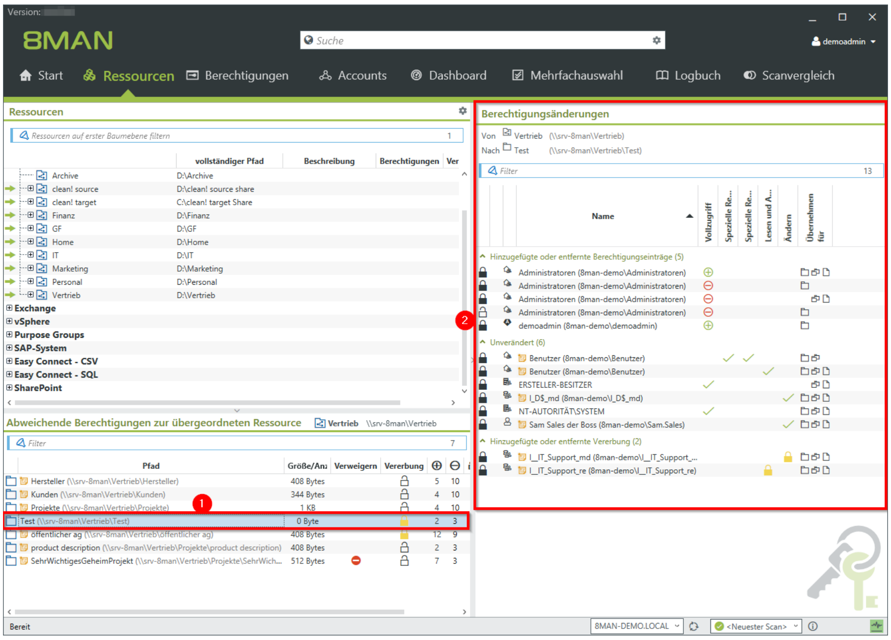
Pfad	Größe/Anz	Verweigern	Vererbung	⊕	⊖
Hersteller (\\srv-8man\Vertrieb\Hersteller)	408 Bytes			5	10
Kunden (\\srv-8man\Vertrieb\Kunden)	344 Bytes			4	10
Projekte (\\srv-8man\Vertrieb\Projekte)	1 KB			4	10
Test (\\srv-8man\Vertrieb\Test)	0 Byte			2	3
öffentlicher ag (\\srv-8man\Vertrieb\öffentlicher ag)	408 Bytes				
product description (\\srv-8man\Vertrieb\Projekte\product description)	408 Bytes				
SehrWichtigesGeheimProjekt (\\srv-8man\Vertrieb\Projekte\SehrWich...	512 Bytes	⊖			

Hinweis: Die Vererbung ist fehlerhaft.
Der Ordner hat nicht die gleichen Berechtigungen wie im übergeordneten Ordner. In vielen Fällen liegt ein verschobener Ordner vor, bei dem die Berechtigungen mitgenommen wurden.

8MAN listet alle Unterverzeichnisse mit abweichenden Berechtigungen auf.

An dem gelben Schloss erkennen Sie eine fehlerhafte Vererbung.

Nutzen Sie die Sortierfunktion in der Spalte "Vererbung".

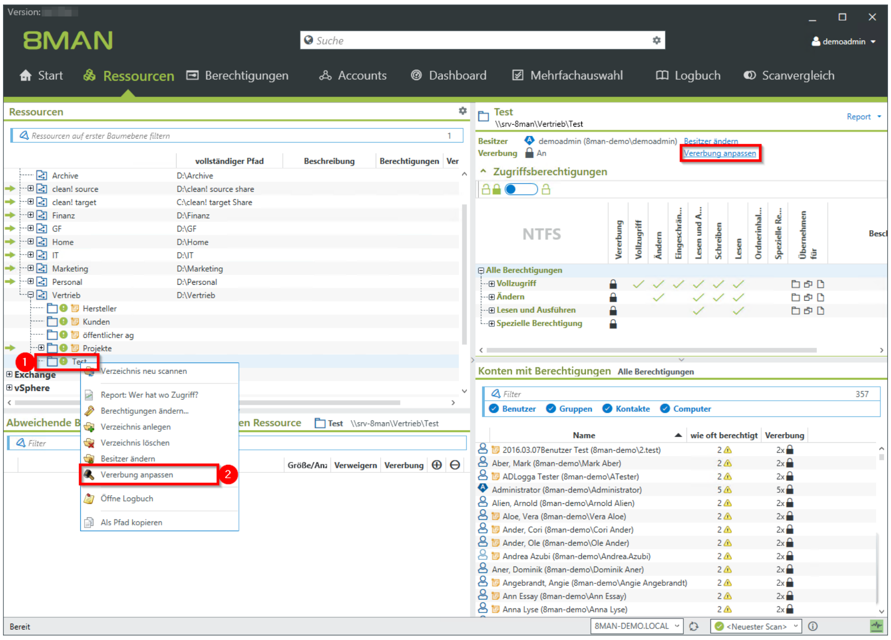


Berechtigungsänderungen

Von Vertrieb (\\srv-8man\Vertrieb)
Nach Test (\\srv-8man\Vertrieb\Test)

Name	Vollzugriff	Spezielle Re...	Spezielle Re...	Lesen und A...	Ändern	Übernehmen für
Hinzugefügte oder entfernte Berechtigungseinträge (5)						
Administratoren (8man-demo\Administratoren)	⊕					
Administratoren (8man-demo\Administratoren)	⊖					
Administratoren (8man-demo\Administratoren)	⊖					
Administratoren (8man-demo\Administratoren)	⊖					
demoadmin (8man-demo\demoadmin)	⊕					
Unverändert (6)						
Benutzer (8man-demo\Benutzer)		✓	✓			
Benutzer (8man-demo\Benutzer)				✓		
ERSTELLER-BESITZER	✓					
I_D$_md (8man-demo\I_D$_md)					✓	
NT-AUTORITÄT\SYSTEM	✓					
Sam Sales der Boss (8man-demo\Sam.Sales)					✓	
Hinzugefügte oder entfernte Vererbung (2)						
I_IT_Support_md (8man-demo\I_IT_Support_...						
I_IT_Support_re (8man-demo\I_IT_Support_re)						

1. *Klicken Sie auf einen Eintrag.*
2. *8MAN zeigt ihnen in allen Details, welche Berechtigungen sich im Vergleich zum übergeordneten Verzeichnis ändern.*



	vollständiger Pfad	Beschreibung	Berechtigungen	Ver
Archive	D:\Archive			
clean! source	D:\clean! source share			
clean! target	C:\clean! target Share			
Finanz	D:\Finanz			
GF	D:\GF			
Home	D:\Home			
IT	D:\IT			
Marketing	D:\Marketing			
Personal	D:\Personal			
Vertrieb	D:\Vertrieb			
Hersteller				
Kunden				
öffentlicher ag				
Projekte				
Test				

Test \\srv-8man\Vertrieb\Test

Test
\\srv-8man\Vertrieb\Test

Besitzer: demoadmin (8man-demo\demoadmin) Besitzer ändern
Vererbung: An Vererbung anpassen

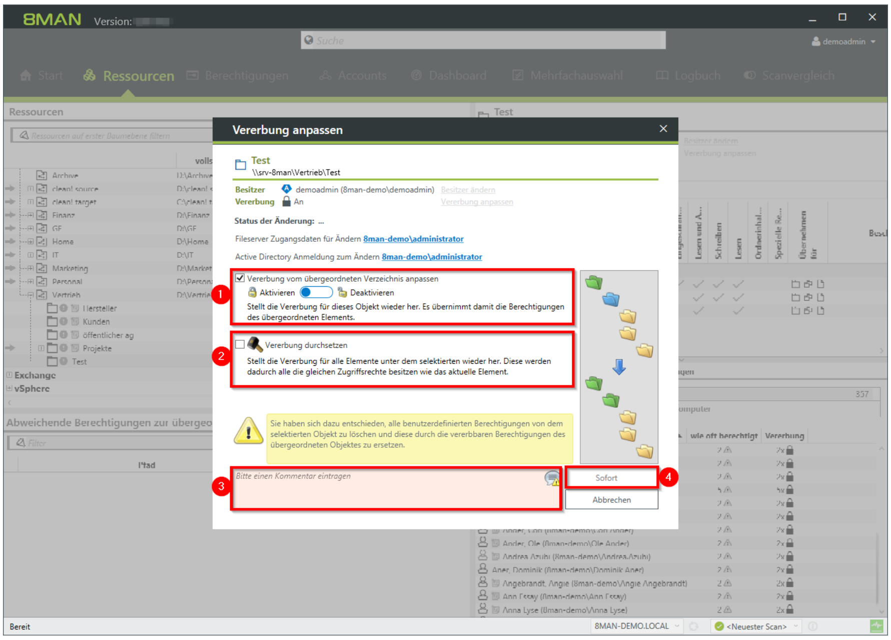
Konten mit Berechtigungen Alle Berechtigungen

Filter 357

☑ Benutzer ☑ Gruppen ☑ Kontakte ☑ Computer

Name	wie oft berechtigt	Vererbung
2016.03.07Benutzer Test (8man-demo\2.test)	2 ⚠	2x 🔒
Aber, Mark (8man-demo\Mark Aber)	2 ⚠	2x 🔒
ADLogga Tester (8man-demo\ATester)	2 ⚠	2x 🔒
Administrator (8man-demo\Administrator)	5 ⚠	5x 🔒
Alien, Arnold (8man-demo\Arnold Alien)	2 ⚠	2x 🔒
Aloe, Vera (8man-demo\Vera Aloe)	2 ⚠	2x 🔒
Ander, Cori (8man-demo\Cori Ander)	2 ⚠	2x 🔒
Ander, Ole (8man-demo\Ole Ander)	2 ⚠	2x 🔒
Andrea Azubi (8man-demo\Andrea.Azubi)	2 ⚠	2x 🔒
Aner, Dominik (8man-demo\Dominik Aner)	2 ⚠	2x 🔒
Angebrandt, Angie (8man-demo\Angie Angebrandt)	2 ⚠	2x 🔒
Ann Essay (8man-demo\Ann Essay)	2 ⚠	2x 🔒
Anna Lyse (8man-demo\Anna Lyse)	2 ⚠	2x 🔒

1. *Navigieren Sie zu dem Unterverzeichnis, bei dem Sie die fehlerhafte Vererbung korrigieren wollen.*
2. *oder 3. Klicken Sie auf "Vererbung anpassen".*



Vererbung anpassen

Test
\\srv-8man\Vertrieb\Test

Besitzer: demoadmin (8man-demo\demoadmin) Besitzer ändern
Vererbung: An Vererbung anpassen

Status der Änderung: ...

Fileserver Zugangsdaten für Ändern 8man-demo\administrator

Active Directory Anmeldung zum Ändern 8man-demo\administrator

☑ Vererbung vom übergeordneten Verzeichnis anpassen
Aktivieren ● Deaktivieren
Stellt die Vererbung für dieses Objekt wieder her. Es übernimmt damit die Berechtigungen des übergeordneten Elements.

☐ Vererbung durchsetzen
Stellt die Vererbung für alle Elemente unter dem selektierten wieder her. Diese werden dadurch alle die gleichen Zugriffsrechte besitzen wie das aktuelle Element.

Sie haben sich dazu entschieden, alle benutzerdefinierten Berechtigungen von dem selektierten Objekt zu löschen und diese durch die vererbbaren Berechtigungen des übergeordneten Objektes zu ersetzen.

Bitte einen Kommentar eintragen

Sofort

Abbrechen

1. *Aktivieren Sie die Vererbung.*
2. *Setzen Sie die Vererbung auf die Unterverzeichnisse durch. Im Beispiel hier für alle Unterverzeichnisse von "Test".*
3. *Sie müssen einen Kommentar eingeben.*
4. *Starten Sie die Ausführung.*

Click on the arrow to view divergent access rights for the activated resource.

Select the desired file server. 8MAN indicates the broken ACLs with a yellow exclamation mark. See example "Home".

Select the identified directory and click on the hammer icon in the top right-hand corner.

Select the identified directory and click on the hammer icon in the top right-hand corner.

Click on the inheritance slide lock to interrupt the chain of inheritance. This way the ACL is renewed. Comment your action and click on "Now".

You can then activate the inheritance.

You can then verify if the broken ACL is still shown.

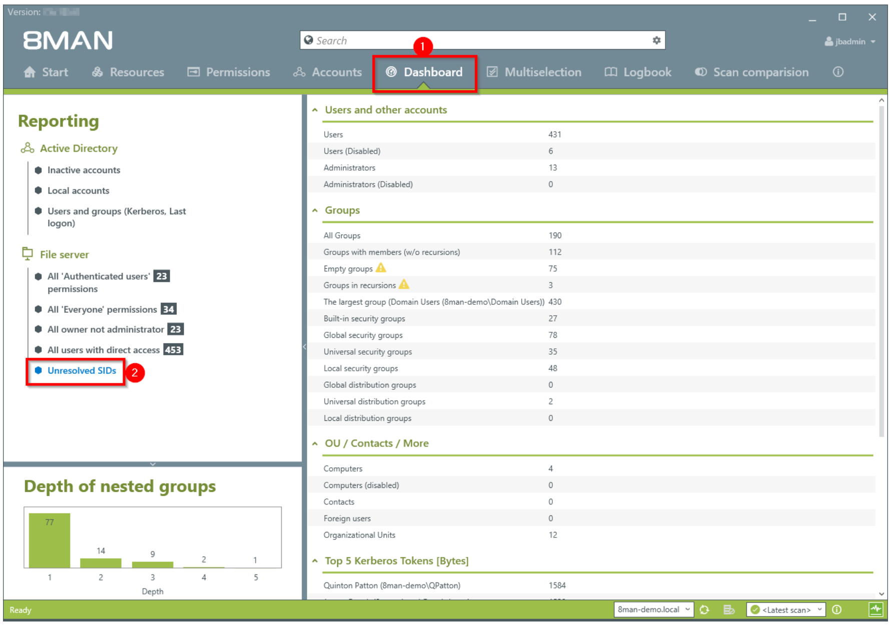
You can sort the entries in the column "Inheritance".

8.2.2.4 Identifying and deleting 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. Unresolved SIDs allow manipulation of the security token. By using unresolved SIDs insider threats can gain access to sensitive resources. 8MAN clearly identifies unresolved SIDs in your system allowing you to easily delete them.

Step by step process



Reporting

Active Directory
- Inactive accounts
- Local accounts
- Users and groups (Kerberos, Last logon)

File server
- All 'Authenticated users' permissions 23
- All 'Everyone' permissions 34
- All owner not administrator 23
- All users with direct access 453
- Unresolved SIDs

Depth of nested groups

Users and other accounts

Users	431
Users (Disabled)	6
Administrators	13
Administrators (Disabled)	0

Groups

All Groups	190
Groups with members (w/o recursions)	112
Empty groups ⚠	75
Groups in recursions ⚠	3
The largest group (Domain Users (8man-demo\Domain Users))	430
Built-in security groups	27
Global security groups	78
Universal security groups	35
Local security groups	48
Global distribution groups	0
Universal distribution groups	2
Local distribution groups	0

OU / Contacts / More

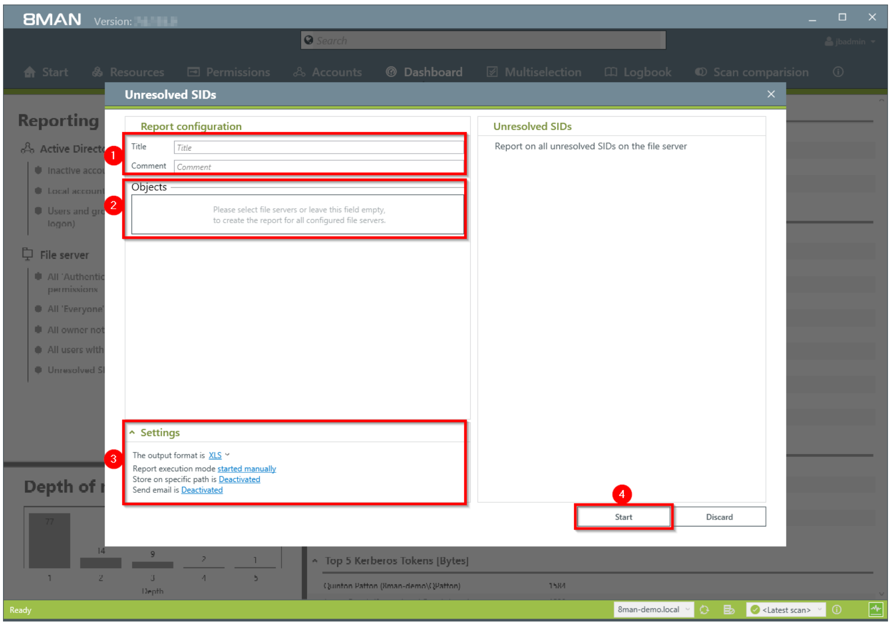
Computers	4
Computers (disabled)	0
Contacts	0
Foreign users	0
Organizational Units	12

Top 5 Kerberos Tokens [Bytes]

Quinton Patton (8man-demo\QPatton)	1584

1. Select "Dashboard".

2. Click on "Unresolved SIDs".



Report configuration

Title: Title

Comment: Comment

Objects

Please select file servers or leave this field empty, to create the report for all configured file servers.

Settings

The output format is XLS

Report execution mode started manually

Store on specific path is Deactivated

Send email is Deactivated

Unresolved SIDs

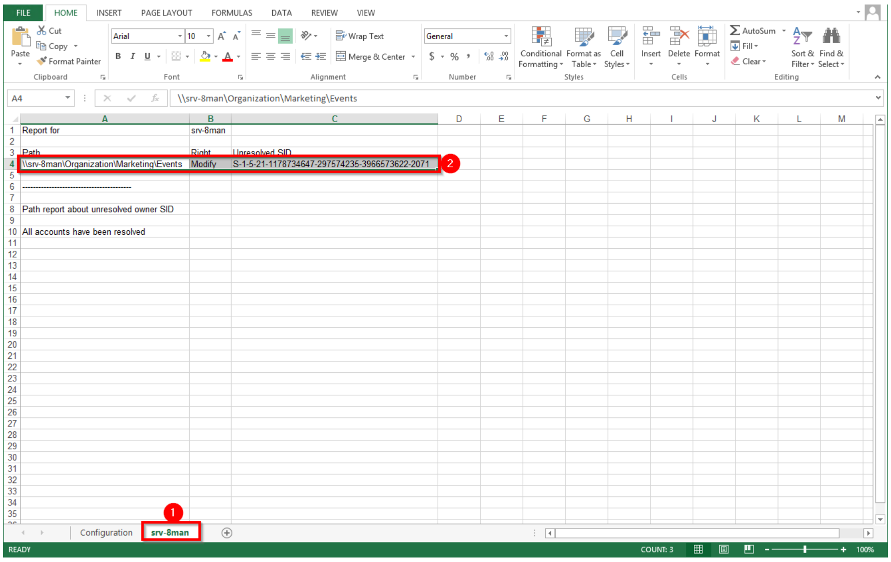
Report on all unresolved SIDs on the file server

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.

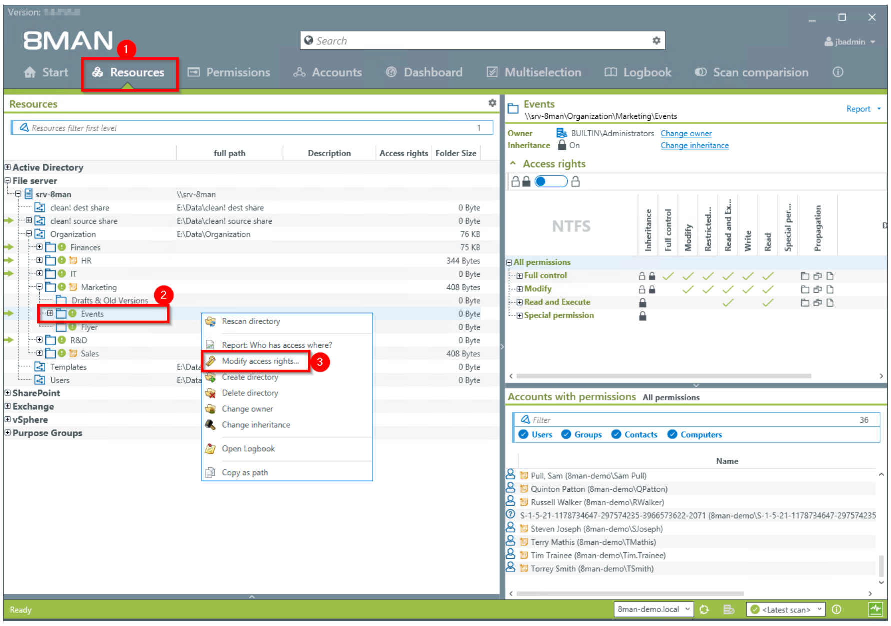


A4 \\srv-8man\Organization\Marketing\Events

	A	B	C
1	Report for	srv-8man	
2			
3	Path	Right	Unresolved SID
4	\\srv-8man\Organization\Marketing\Events	Modify	S-1-5-21-1178734647-297574235-3966573622-2071
5			
6	--		
7			
8	Path report about unresolved owner SID		
9			
10	All accounts have been resolved		

Open the report in Excel.

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



	full path	Description	Access rights	Folder Size
Active Directory				
File server				
srv-8man	\\srv-8man			
clean! dest share	E:\Data\clean! dest share			0 Byte
clean! source share	E:\Data\clean! source share			0 Byte
Organization	E:\Data\Organization			76 KB
Finances				75 KB
HR				344 Bytes
IT				0 Byte
Marketing				408 Bytes
Drafts & Old Versions				0 Byte
Events				0 Byte
Flyer				0 Byte
R&D				0 Byte
Sales				408 Bytes
Templates	E:\Data			0 Byte
Users	E:\Data			0 Byte
SharePoint				
Exchange				
vSphere				
Purpose Groups				

Events
\\srv-8man\Organization\Marketing\Events

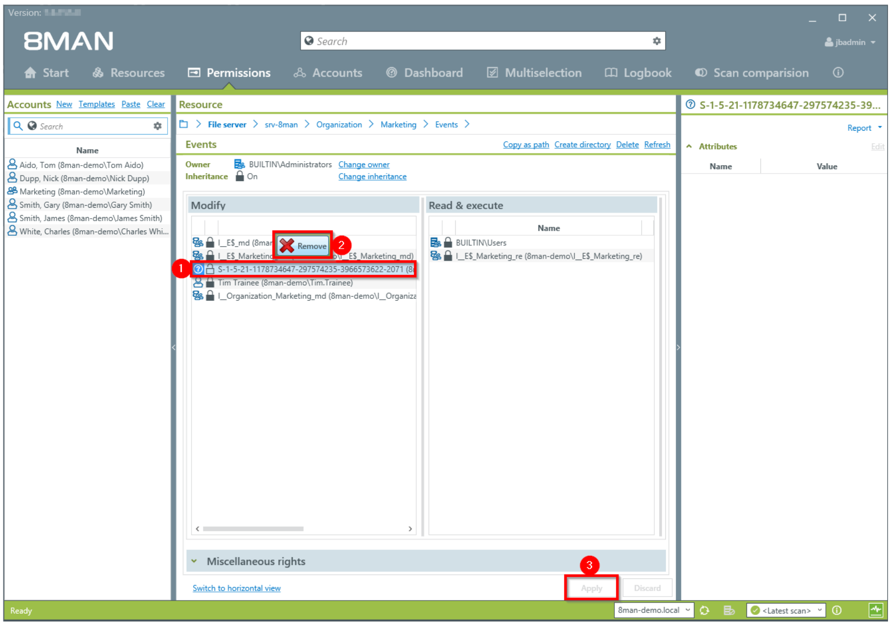
Owner BUILTIN\Administrators Change owner
Inheritance On Change inheritance

NTFS	Inheritance	Full control	Modify	Restricted...	Read and Ex...	Write	Read	Special per...	Propagation
All permissions									
Full control		✓	✓	✓	✓	✓	✓		
Modify			✓	✓	✓	✓	✓		
Read and Execute					✓		✓		
Special permission									

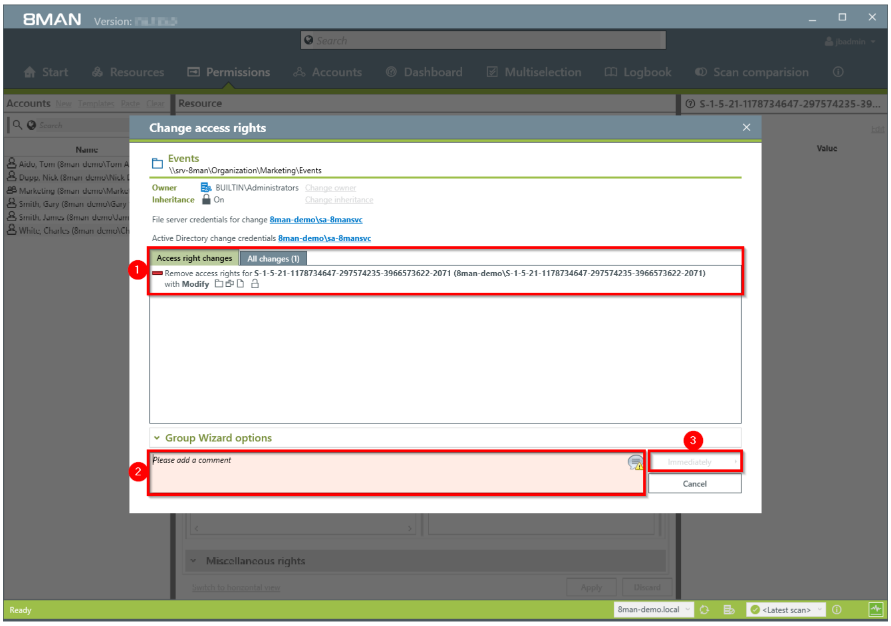
Filter 36

Name
Pull, Sam (8man-demo\Sam Pull)
Quinton Patton (8man-demo\QPatton)
Russell Walker (8man-demo\RWalker)
S-1-5-21-1178734647-297574235-3966573622-2071 (8man-demo\S-1-5-21-1178734647-297574235
Steven Joseph (8man-demo\SJoseph)
Terry Mathis (8man-demo\TMathis)
Tim Trainee (8man-demo\Tim.Trainee)
Torrey Smith (8man-demo\TSmith)

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



1. Select the SID.
2. Click on "Remove".
3. Click on "Apply".



Events
\\srv-8man\Organization\Marketing\Events

Owner BUILTIN\Administrators
Inheritance On

File server credentials for change 8man-demo\sa-8mansvc

Active Directory change credentials 8man-demo\sa-8mansvc

Access right changes | All changes (1)

Remove access rights for **S-1-5-21-1178734647-297574235-3966573622-2071 (8man-demo\S-1-5-21-1178734647-297574235-3966573622-2071)** with **Modify**

1. 8MAN lists all planned changes.

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

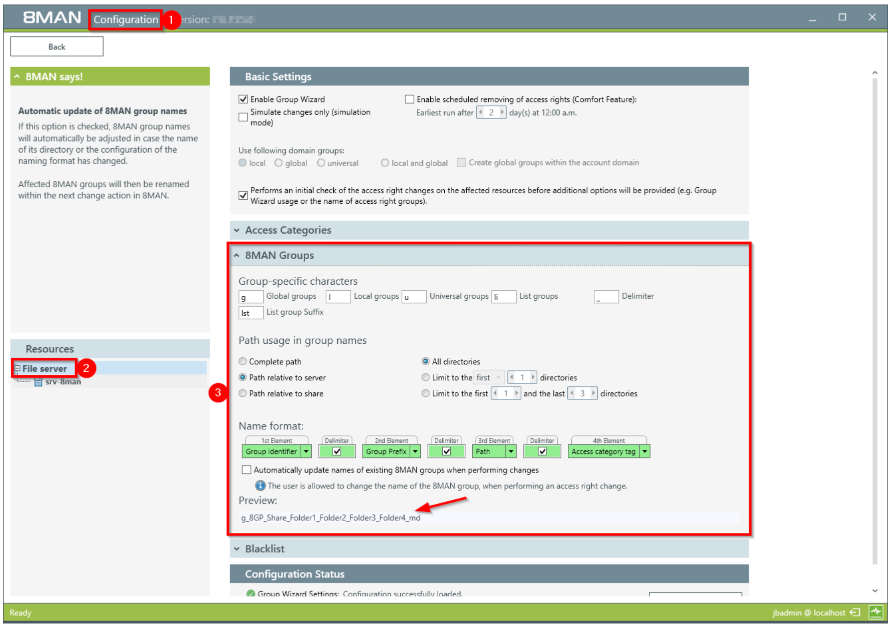
8.2.2.5 Determining naming conventions for access groups

Background / Value

8MAN puts an end to random naming of groups. Administrators determine the appropriate naming convention, which will be used for all AD groups created with 8MAN Group Wizard.

You can determine the naming convention in the 8MAN configuration module.

Step by step process



8MAN says!

Automatic update of 8MAN group names

If this option is checked, 8MAN group names will automatically be adjusted in case the name of its directory or the configuration of the naming format has changed.

Affected 8MAN groups will then be renamed within the next change action in 8MAN.

Resources

File server
srv-8man

Basic Settings

☑ Enable Group Wizard
□ Simulate changes only (simulation mode)
□ Enable scheduled removing of access rights (Comfort Feature):
Earliest run after 2 day(s) at 12:00 a.m.

Use following domain groups:
● local ○ global ○ universal ○ local and global □ Create global groups within the account domain

☑ Performs an initial check of the access right changes on the affected resources before additional options will be provided (e.g. Group Wizard usage or the name of access right groups).

Access Categories

8MAN Groups

Group-specific characters
g Global groups
l Local groups
u Universal groups
li List groups
_ Delimiter
lst List group Suffix

Path usage in group names
○ Complete path
● Path relative to server
○ Path relative to share
● All directories
○ Limit to the first 1 directories
○ Limit to the first 1 and the last 3 directories

Name format:

1st Element	Delimiter	2nd Element	Delimiter	3rd Element	Delimiter	4th Element
Group identifier	☑	Group Prefix	☑	Path	☑	Access category tag

□ Automatically update names of existing 8MAN groups when performing changes

The user is allowed to change the name of the 8MAN group, when performing an access right change.

Preview:
g_8GP_Share_Folder1_Folder2_Folder3_Folder4_md

Blacklist

Configuration Status

Group Wizard Settings: Configuration successfully loaded.

1. *Start the configuration module and navigate to "Change Configuration" ->"File server".*
2. *Select the desired SharePoint resource. You can enter different settings for each resource.*
3. *Determine the naming convention. Please note that 8MAN will show you a preview.*

8.2.2.6 Changing directory ownership

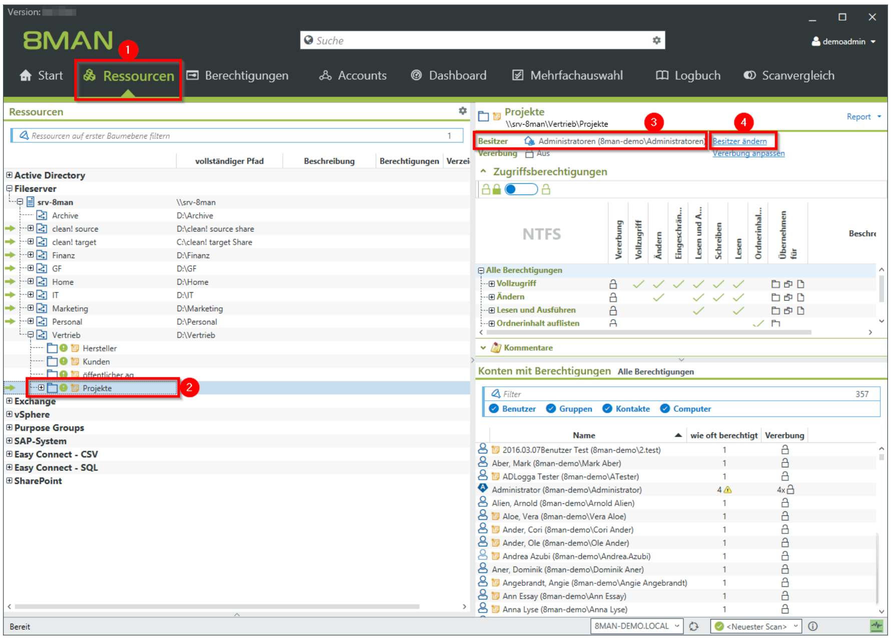
Background / Value

Mit 8MAN ändern Sie einfach den Besitzer von Verzeichnissen. Schließen Sie die User vom Besitz von Verzeichnissen aus, können Sie unerwünschte Berechtigungsänderungen verhindern.

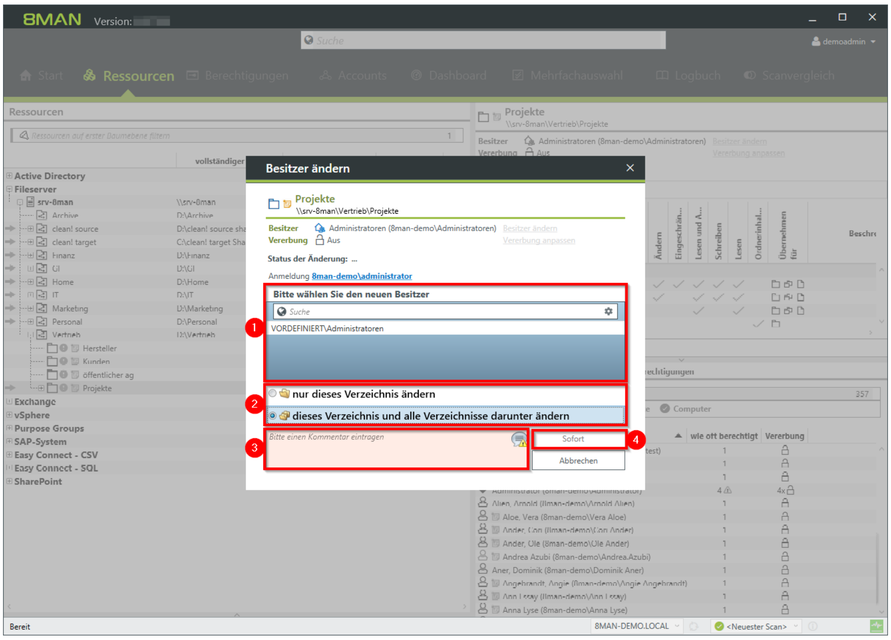
Additional Services

Verzeichnisse identifizieren, deren Besitzer nicht Administratoren sind

Step by step process



1. Wählen Sie "Ressourcen".
2. Navigieren Sie zum gewünschten Verzeichnis. Alternativ nutzen Sie die Suche.
3. 8MAN zeigt Ihnen den aktuellen Besitzer.
4. Klicken Sie auf "Besitzer ändern".


Besitzer ändern
Projekte
\\srv-8man\Vertrieb\Projekte
Besitzer
Administratoren (8man-demo\Administratoren)
Vererbung
Aus
Status der Änderung: ...
Anmeldung 8man-demo\administrator
Bitte wählen Sie den neuen Besitzer
Suche
VORDEFINIERT\Administratoren
○ nur dieses Verzeichnis ändern
● dieses Verzeichnis und alle Verzeichnisse darunter ändern
Bitte einen Kommentar eintragen
Sofort
Abbrechen
1
2
3
4

1. Wählen Sie einen neuen Besitzer.
2. Legen Sie fest, ob die Änderung nur für das aktuelle oder auch für alle untergeordneten durchgeführt wird.
3. Sie müssen einen Kommentar eingeben.
4. Starten Sie die Ausführung.

8.3 +8MATE for Exchange

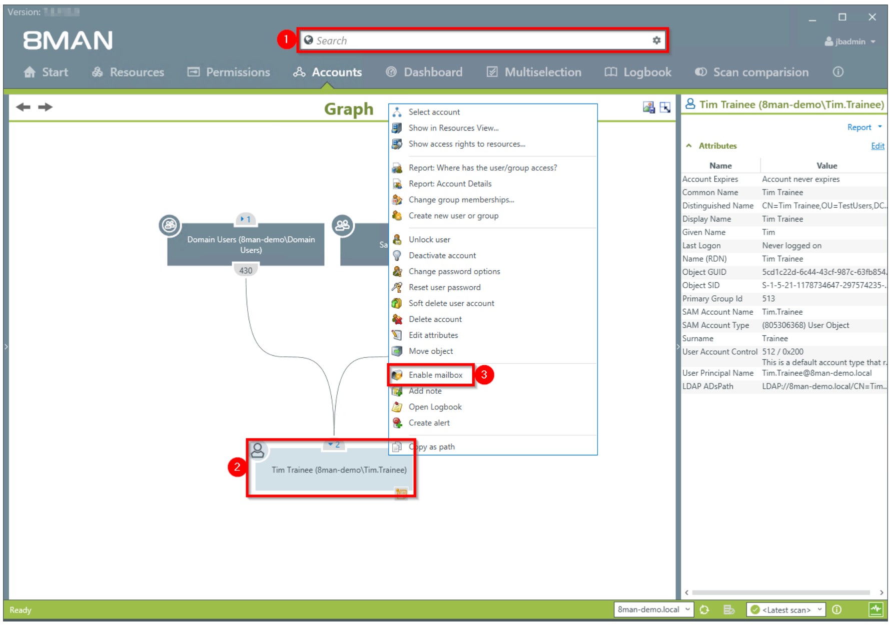
8.3.1 Help Desk

8.3.1.1 Creating a mailbox (email enable users)

Background / Value

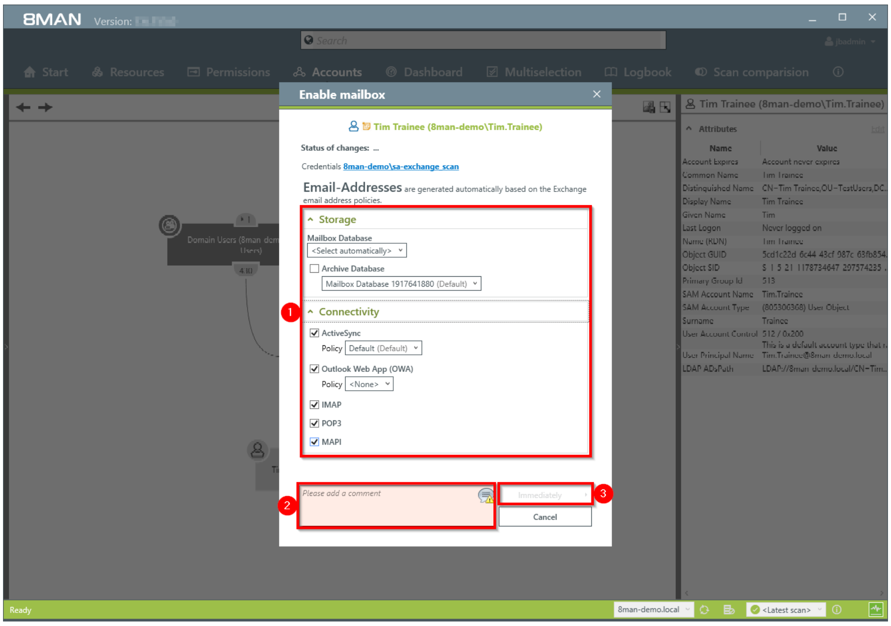
If your license agreement includes 8MATE for Exchange you can create Mailboxes (email enable users) with 8MAN.

Step by step process



Name	Value
Account Expires	Account never expires
Common Name	Tim Trainee
Distinguished Name	CN=Tim Trainee,OU=TestUsers,DC..
Display Name	Tim Trainee
Given Name	Tim
Last Logon	Never logged on
Name (RDN)	Tim Trainee
Object GUID	5cd1c22d-6c44-43cf-987c-63fb854.
Object SID	S-1-5-21-1178734647-297574235-.
Primary Group Id	513
SAM Account Name	Tim.Trainee
SAM Account Type	(805306368) User Object
Surname	Trainee
User Account Control	512 / 0x200 This is a default account type that r.
User Principal Name	Tim.Trainee@8man-demo.local
LDAP ADsPath	LDAP://8man-demo.local/CN=Tim..

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.*



Tim Trainee (8man-demo\Tim.Trainee)

Status of changes: ...

Credentials 8man-demo\sa-exchange_scan

Email-Addresses are generated automatically based on the Exchange email address policies.

Storage

Mailbox Database <Select automatically>

□ Archive Database
Mailbox Database 1917641880 (Default)

Connectivity

☑ ActiveSync
Policy Default (Default)

☑ Outlook Web App (OWA)
Policy <None>

☑ IMAP

☑ POP3

☑ MAPI

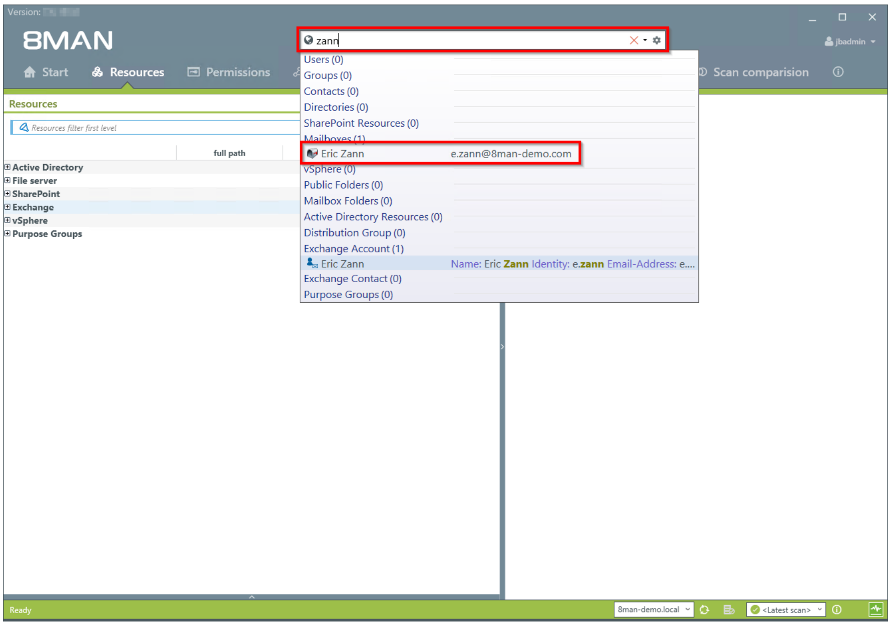
1. *Determine the Exchange options.*
2. *You must enter a comment, for example a ticket number.*
3. *Start the creation of the mailbox.*

8.3.1.2 Changing mailbox permissions

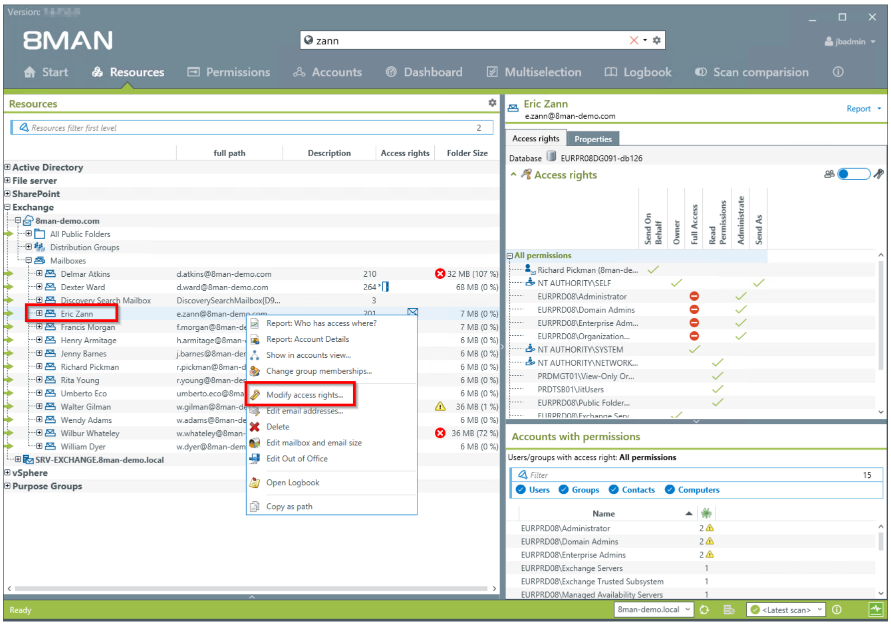
Background / Value

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

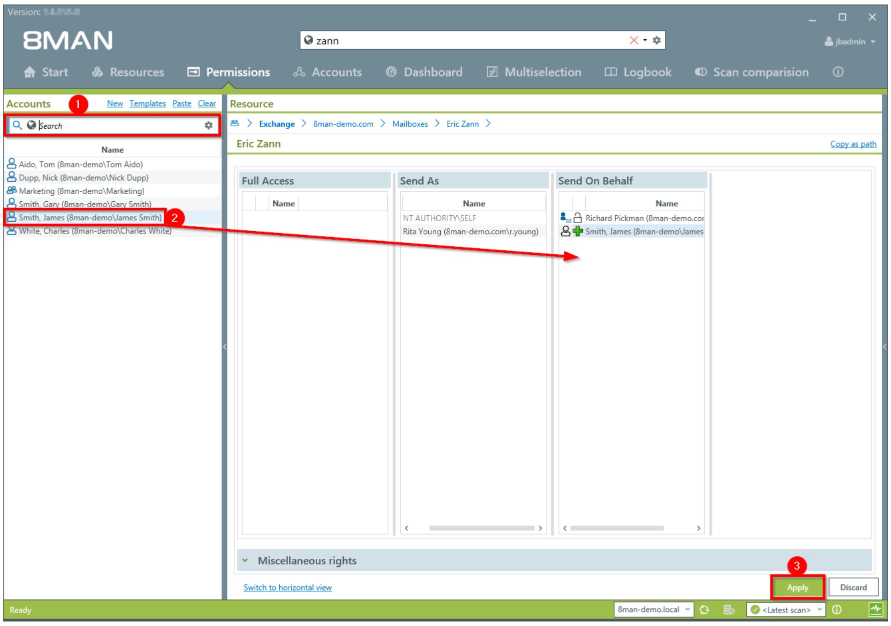
Step by step process



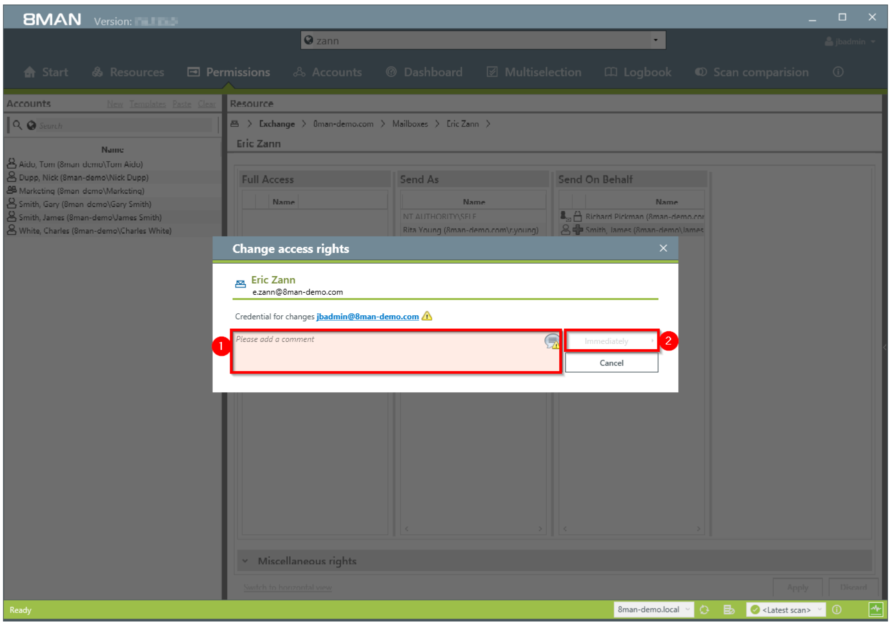
Use the search field to find the desired mailbox.



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


8MAN
zann
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
Accounts
New
Templates
Paste
Clear
Search
Name
Aido, Tom (8man-demo\Tom Aido)
Dupp, Nick (8man-demo\Nick Dupp)
Marketing (8man-demo\Marketing)
Smith, Gary (8man-demo\Gary Smith)
Smith, James (8man-demo\James Smith)
White, Charles (8man-demo\Charles White)
Resource
Exchange > 8man-demo.com > Mailboxes > Eric Zann
Eric Zann
Copy as path
Full Access
Send As
Send On Behalf
NT AUTHORITY\SELF
Rita Young (8man-demo.com\r.young)
Richard Pickman (8man-demo.cor
Smith, James (8man-demo\James
Miscellaneous rights
Switch to horizontal view
Apply
Discard
Ready
8man-demo.local
<Latest scan>
1
2
3

1. Use the search field to find the desired account.
2. Use drag & drop to move the account to an access rights column.
3. Click on "Apply".



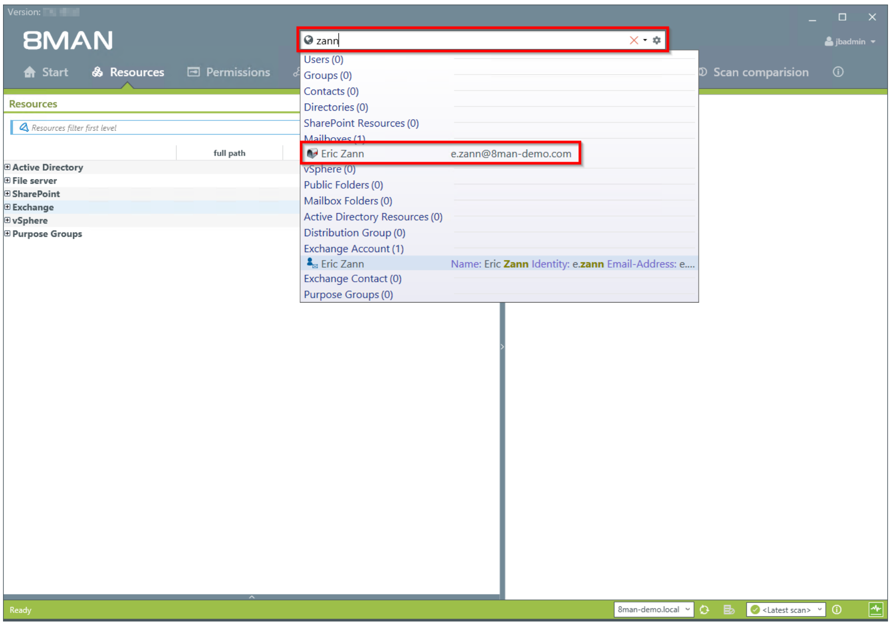
1. You must enter a comment, for example a ticket number.
2. Start the access rights change.

8.3.1.3 Managing out of office notices

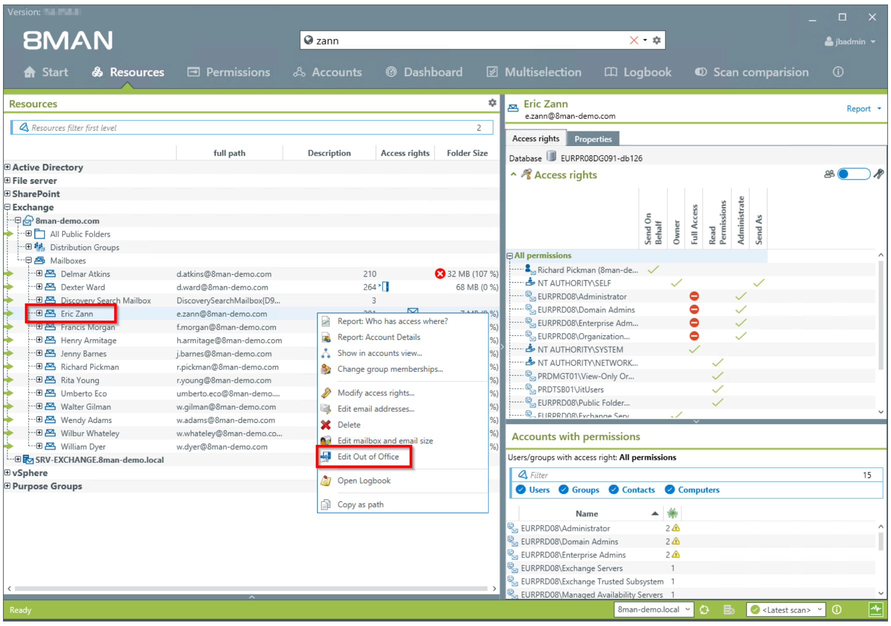
Background / Value

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

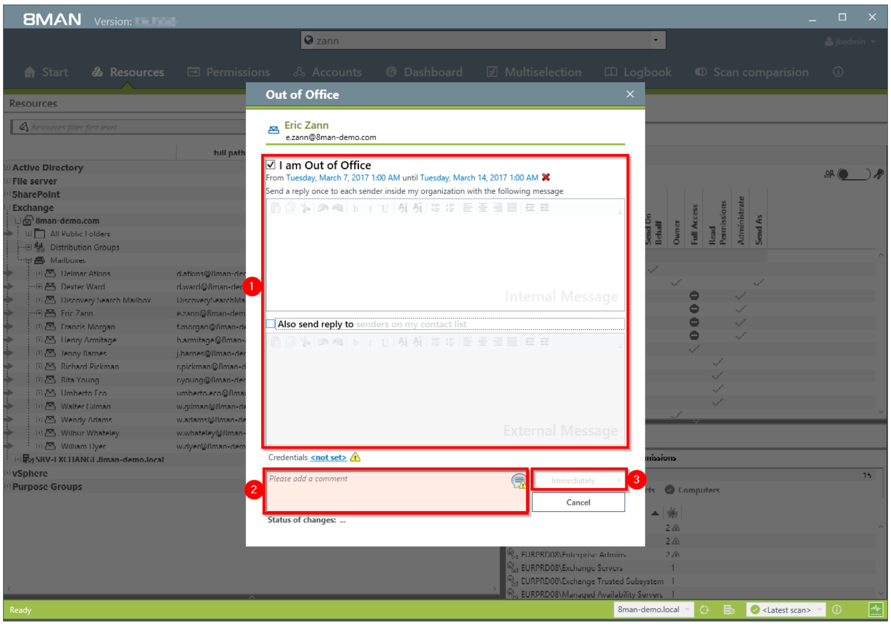
Step by step process



Use the search field to find the desired Mailbox.



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



Out of Office

Eric Zann
e.zann@8man-demo.com

☑ I am Out of Office
From Tuesday, March 7, 2017 1:00 AM until Tuesday, March 14, 2017 1:00 AM
Send a reply once to each sender inside my organization with the following message

□ Also send reply to senders on my contact list

Credentials <not set>

Status of changes: ...

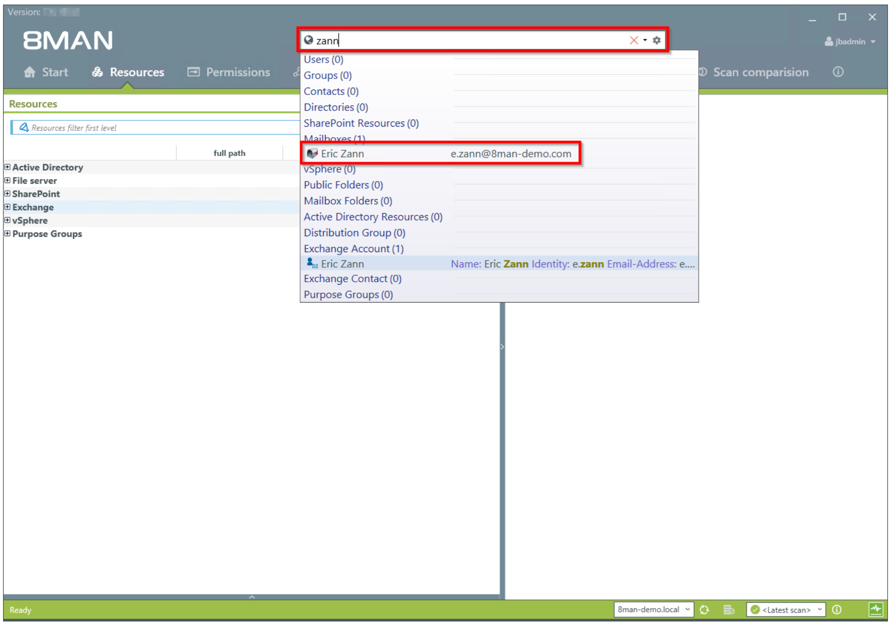
1. *Determine the out of office settings.*
2. *You must enter a comment, for example a ticket number.*
3. *Start the process.*

8.3.1.4 Managing mailbox and email size

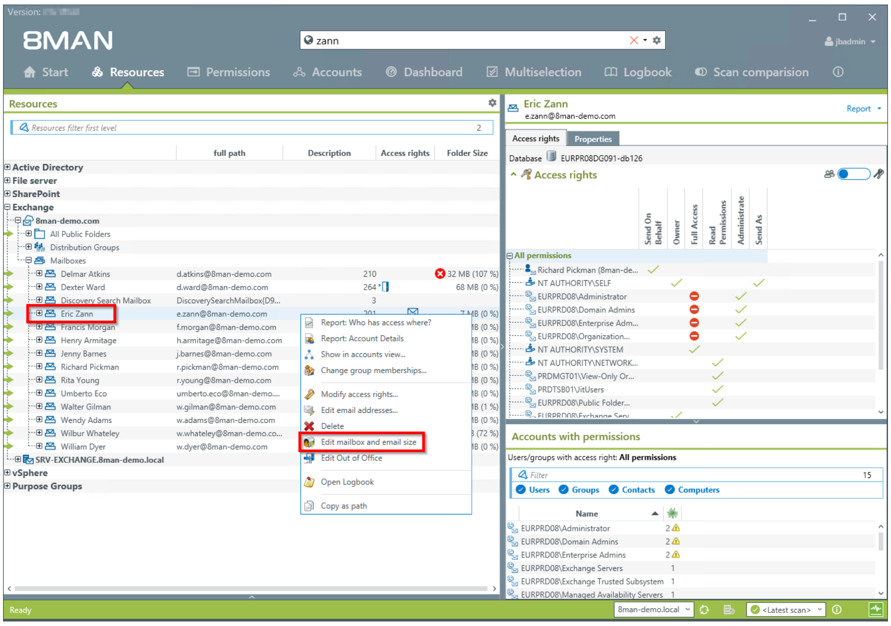
Background / Value

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

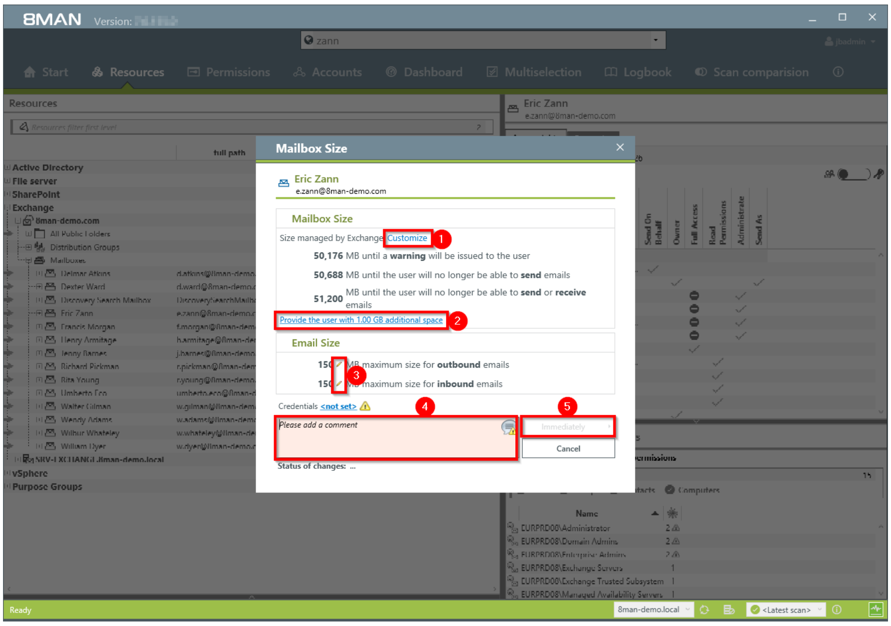
Step by step process



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.



Mailbox Size

Eric Zann
e.zann@8man-demo.com

Mailbox Size

Size managed by Exchange Customize 1

50,176 MB until a **warning** will be issued to the user

50,688 MB until the user will no longer be able to **send** emails

51,200 MB until the user will no longer be able to **send** or **receive** emails

Provide the user with 1.00 GB additional space 2

Email Size

150 MB maximum size for **outbound** emails

150 MB maximum size for **inbound** emails 3

Credentials <not set> 4 5

Please add a comment

Immediately

Cancel

Status of changes: ...

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.*

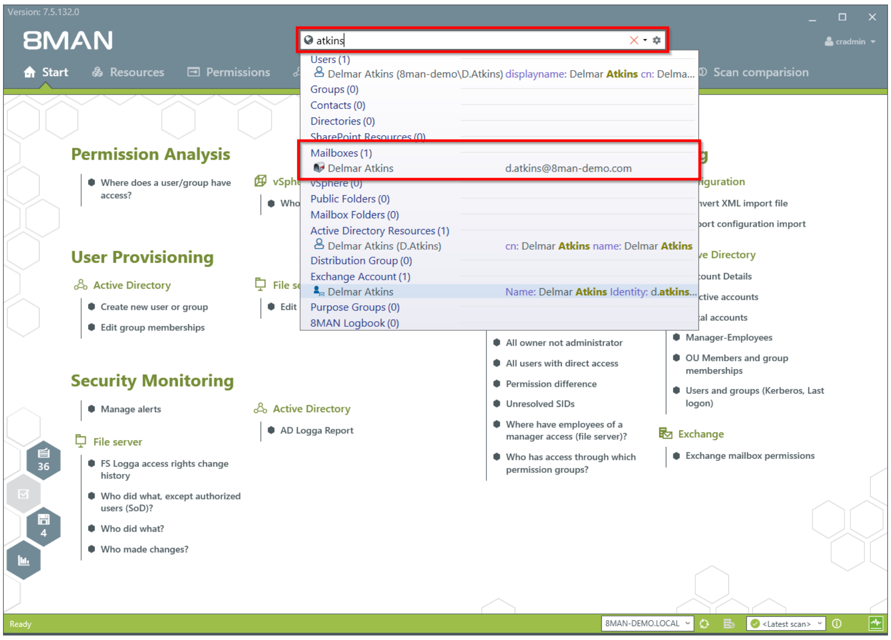
8.3.1.5 Managing email addresses

Background / Value

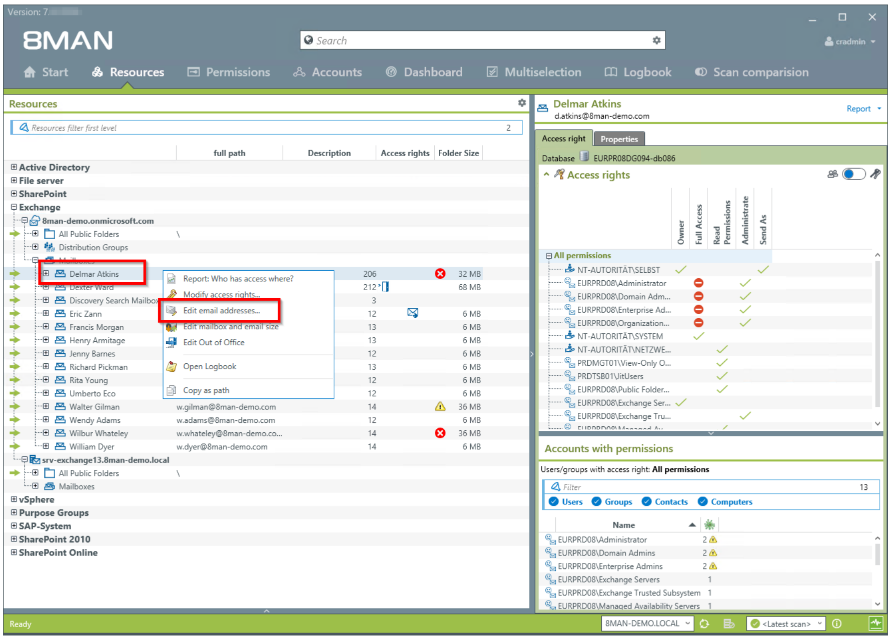
With 8MAN you can assign and remove multiple e-mail addresses to mailboxes, distribution groups and contacts.

The process is documented automatically.

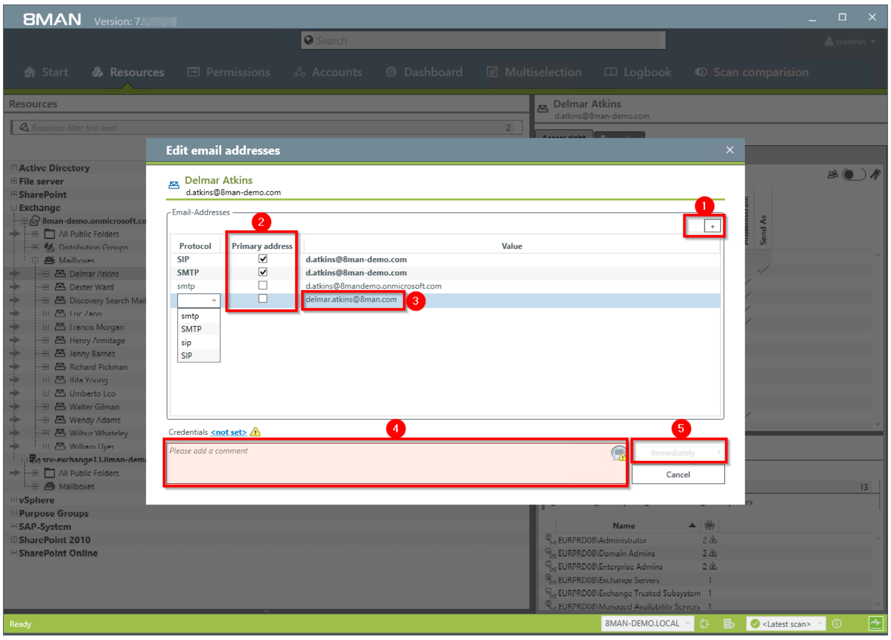
Step by step process



Use the search field to find the desired mailbox.



Right-click on the Mailbox and select "Edit email addresses" from the context menu.



Edit email addresses

Delmar Atkins
d.atkins@8man-demo.com

Email-Addresses

Protocol	Primary address	Value
SIP	☑	d.atkins@8man-demo.com
SMTP	☑	d.atkins@8man-demo.com
smtp	□	d.atkins@8mandemo.onmicrosoft.com
	□	delmar.atkins@8man.com

Credentials <not set>

Please add a comment

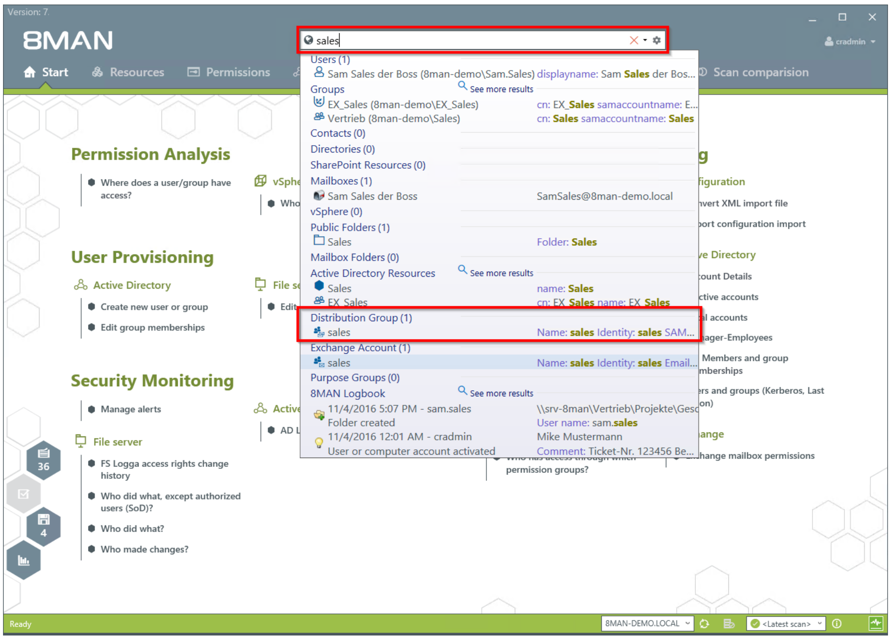
1. Add an email address or delete an existing one.
2. Select the primary email address.
3. Double-click the field where you want to enter or change the address.
4. You must enter a comment, for example the ticket number.
5. Start the process.

8.3.1.6 Managing distribution group memberships

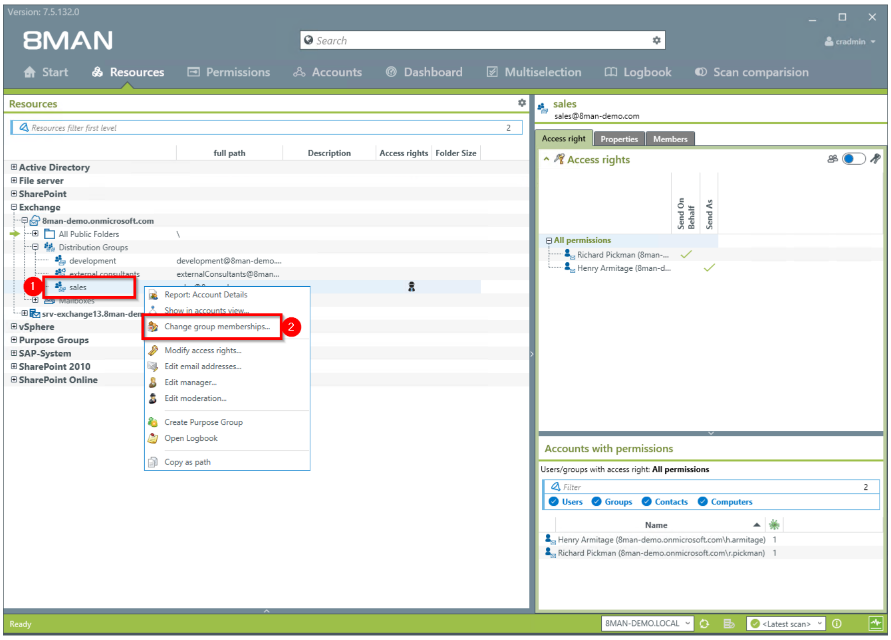
Background / Value

8MAN allows you to manage the members of distribution groups. This includes the addition and removal of recipients as well as the nesting within other groups (parent child relationships). The process is automatically documented.

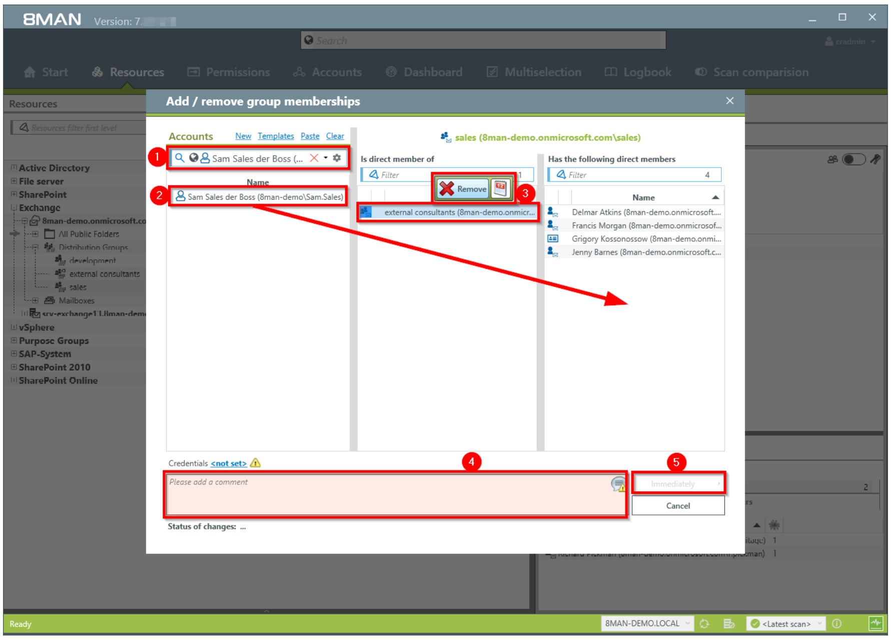
Step by Step process


Version: 7
8MAN
sales
Start
Resources
Permissions
Scan comparision
Users (1)
Sam Sales der Boss (8man-demo\Sam.Sales) displayname: Sam Sales der Boss...
Groups
See more results
EX_Sales (8man-demo\EX_Sales) cn: EX_Sales samaccountname: E...
Vertrieb (8man-demo\Sales) cn: Sales samaccountname: Sales
Contacts (0)
Directories (0)
SharePoint Resources (0)
Mailboxes (1)
Sam Sales der Boss SamSales@8man-demo.local
vSphere (0)
Public Folders (1)
Sales Folder: Sales
Mailbox Folders (0)
Active Directory Resources
Sales name: Sales
EX_Sales cn: EX_Sales name: EX_Sales
Distribution Group (1)
sales Name: sales Identity: sales SAM...
Exchange Account (1)
sales Name: sales Identity: sales Email...
Purpose Groups (0)
8MAN Logbook
11/4/2016 5:07 PM - sam.sales \\srv-8man\Vertrieb\Projekte\Gesc
Folder created User name: sam.sales
11/4/2016 12:01 AM - cradmin Mike Mustermann
User or computer account activated Comment: Ticket-Nr. 123456 Be...
Permission Analysis
Where does a user/group have access?
User Provisioning
Active Directory
Create new user or group
Edit group memberships
Security Monitoring
Manage alerts
File server
FS Logga access rights change history
Who did what, except authorized users (SoD)?
Who did what?
Who made changes?
Ready
8MAN-DEMO.LOCAL
<Latest scan>

Use the search field to find the desired distribution group.



1. *You are focusing on the desired group.*
2. *Right-click on the group and select "Change group memberships".*



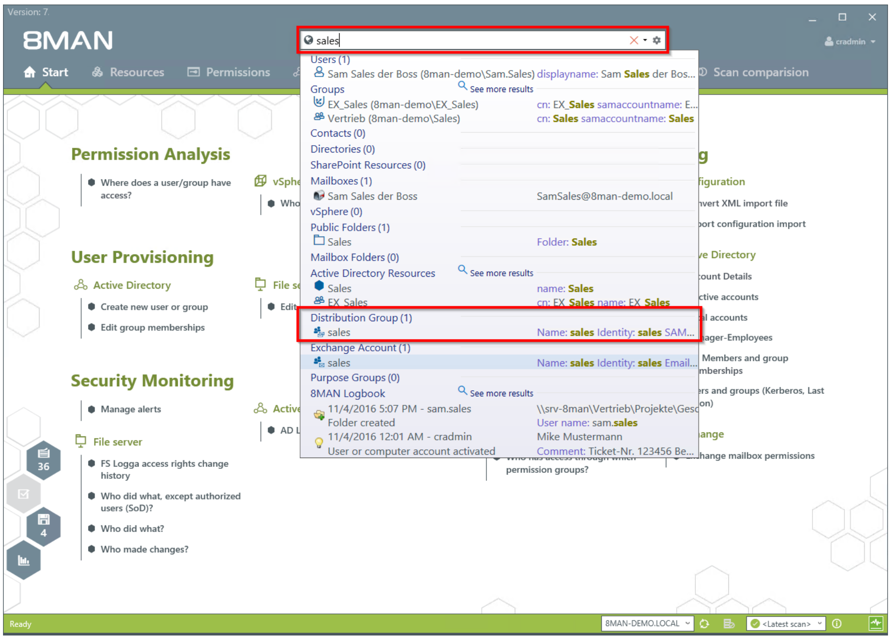
1. *Find an account.*
2. *Use drag & drop to move the account to a column, to assign a group membership.*
3. *You can remove memberships with the "Remove" button.*
4. *You must enter a comment, for example a ticket number.*
5. *Click on "Immediately".*

8.3.1.7 Managing distribution group permissions

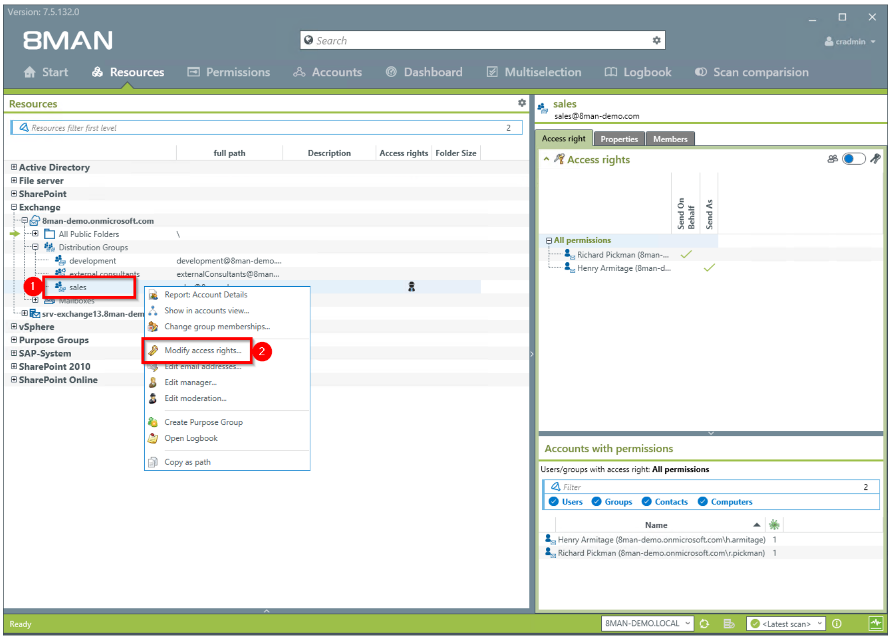
Background / Value

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.

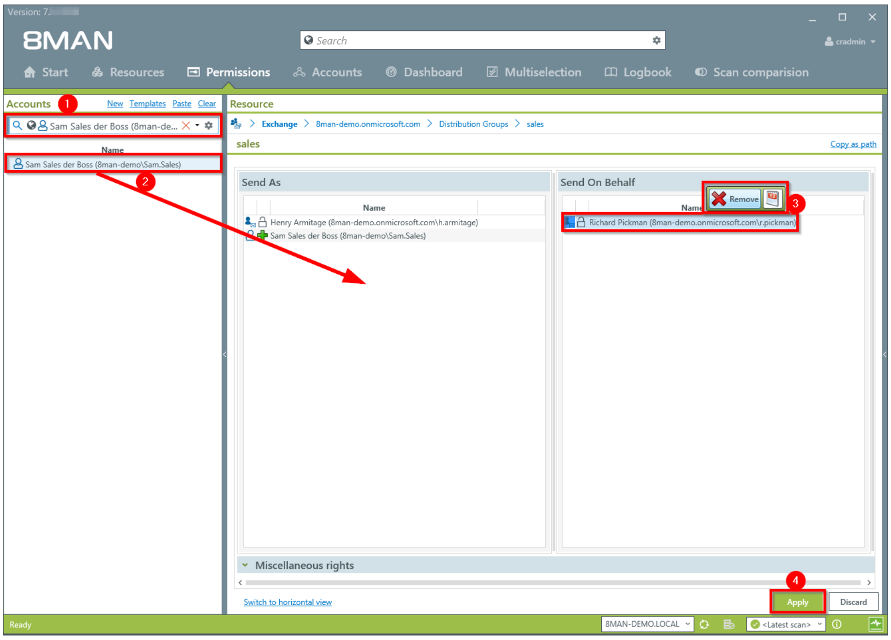
Step by step process



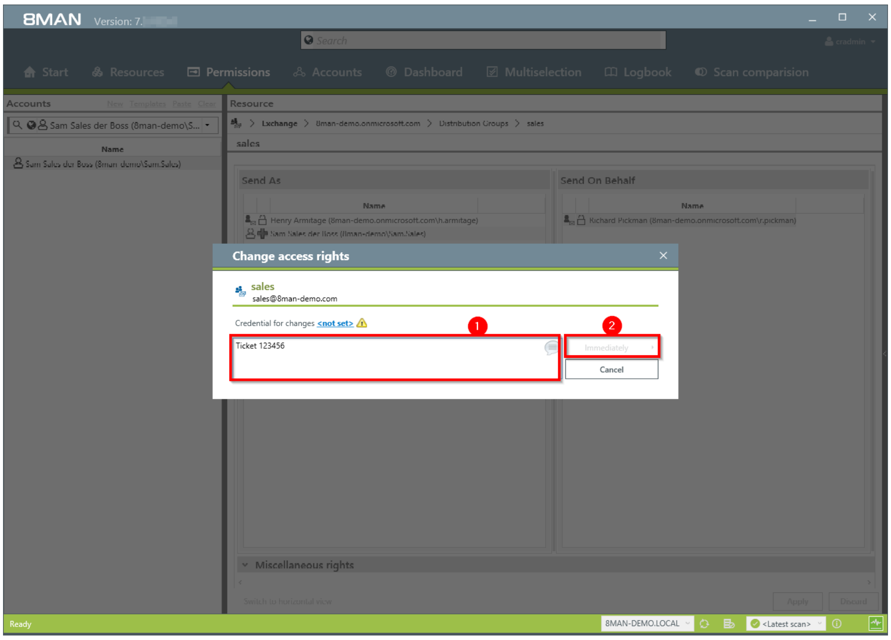
Use the search field to find the desired mailing list.



1. *Find the desired distribution group.*
2. *Right-click on the group and select "Modify access rights" from the context menu.*


8MAN
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
Accounts
New Templates Paste Clear
Sam Sales der Boss (8man-de...
Name
Sam Sales der Boss (8man-demo\Sam.Sales)
Resource
Exchange > 8man-demo.onmicrosoft.com > Distribution Groups > sales
sales
Copy as path
Send As
Name
Henry Armitage (8man-demo.onmicrosoft.com\h.armitage)
Sam Sales der Boss (8man-demo\Sam.Sales)
Send On Behalf
Remove
Richard Pickman (8man-demo.onmicrosoft.com\r.pickman)
Miscellaneous rights
Switch to horizontal view
Apply
Discard
Ready
8MAN-DEMO.LOCAL
<Latest scan>
1
2
3
4

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.

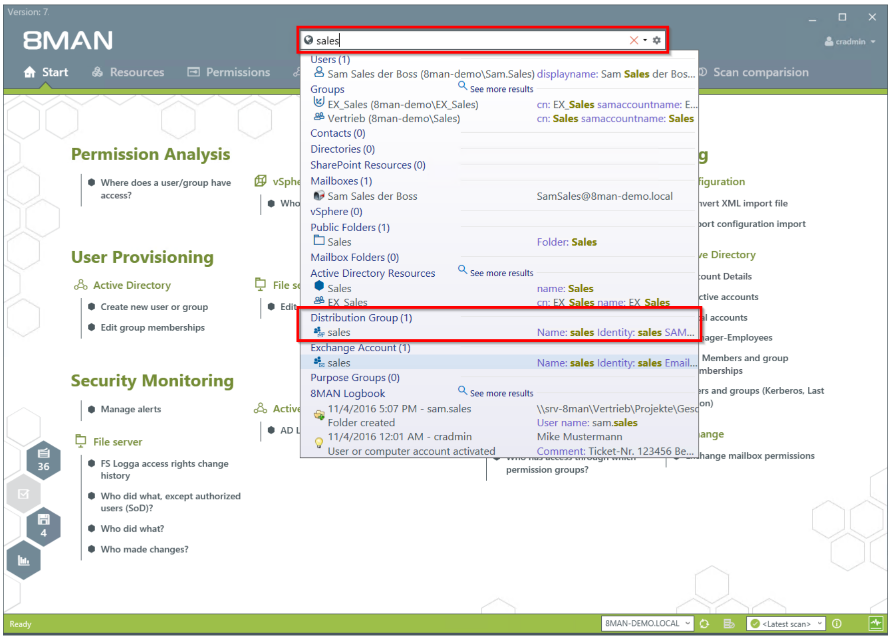
8.3.1.8 Changing the moderation of distribution groups

Background / Purpose

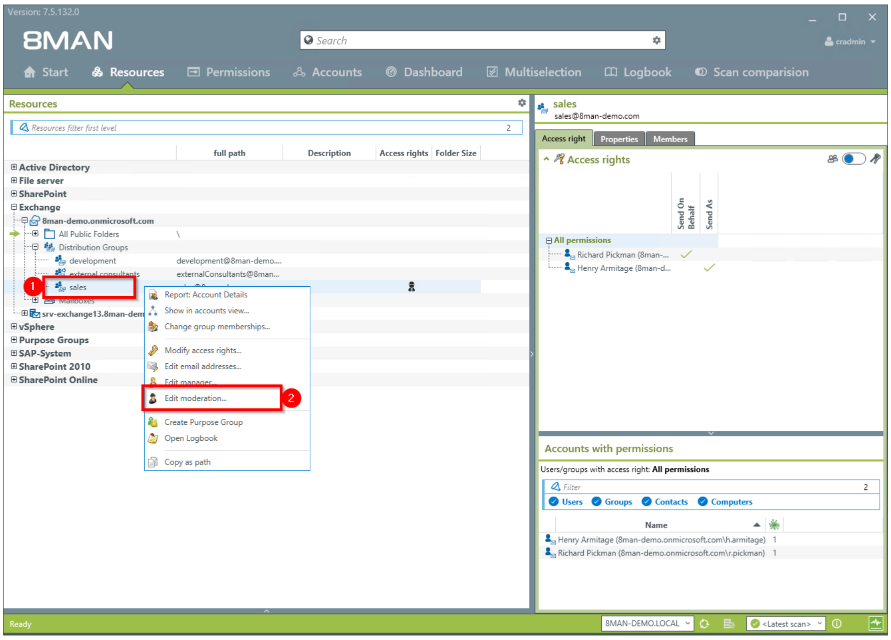
With 8MAN you can quickly modify the moderation of distribution groups. The process will be documented automatically.

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

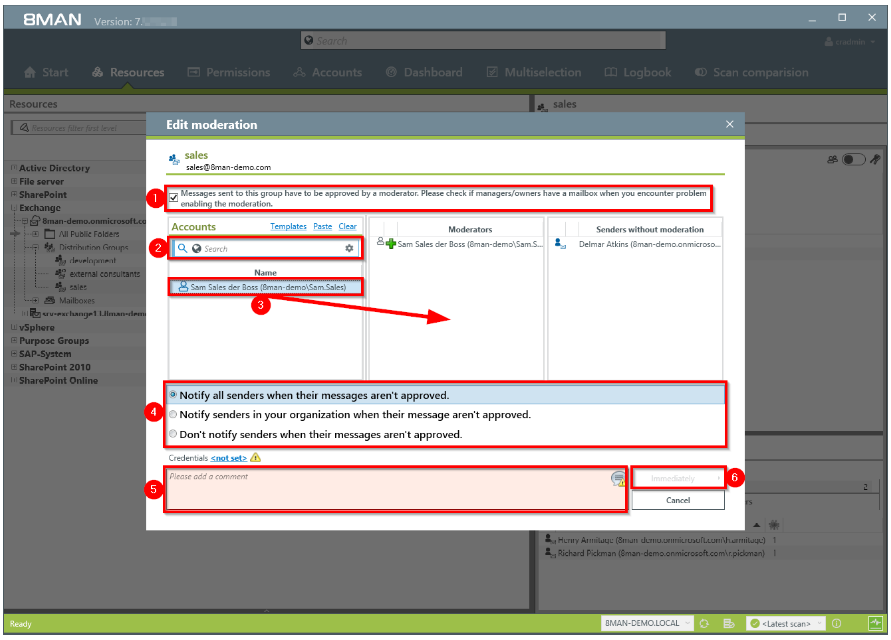
Step by step process



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".*



sales
sales@8man-demo.com

☑ Messages sent to this group have to be approved by a moderator. Please check if managers/owners have a mailbox when you encounter problem enabling the moderation.

Accounts — Templates Paste Clear

Search

Name
Sam Sales der Boss (8man-demo\Sam.Sales)

Moderators
Sam Sales der Boss (8man-demo\Sam.S...

Senders without moderation
Delmar Atkins (8man-demo.onmicroso...

● Notify all senders when their messages aren't approved.
○ Notify senders in your organization when their message aren't approved.
○ Don't notify senders when their messages aren't approved.

Credentials <not set>

Please add a comment

Immediately

Cancel

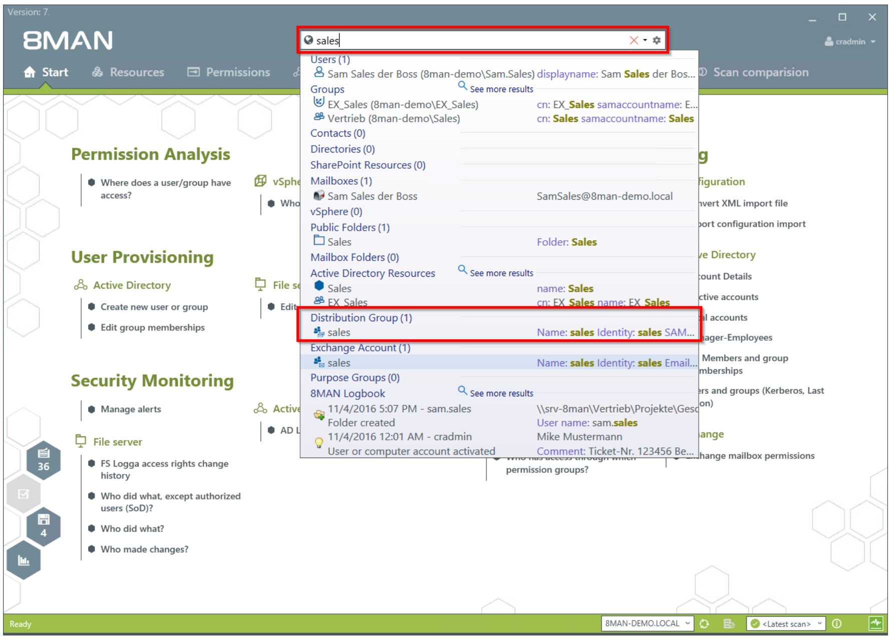
1. *Activate or deactivate the moderation of the distribution group.*
2. *Use the search field to find accounts.*
3. *Use drag & drop to move accounts to the column"Moderators" or "Sender without moderation" (Whitelist).*
4. *Determine the workflow for rejected messages.*
5. *You must enter a comment, for example a ticket number.*
6. *Start the process.*

8.3.1.9 Changing the manager of distribution groups

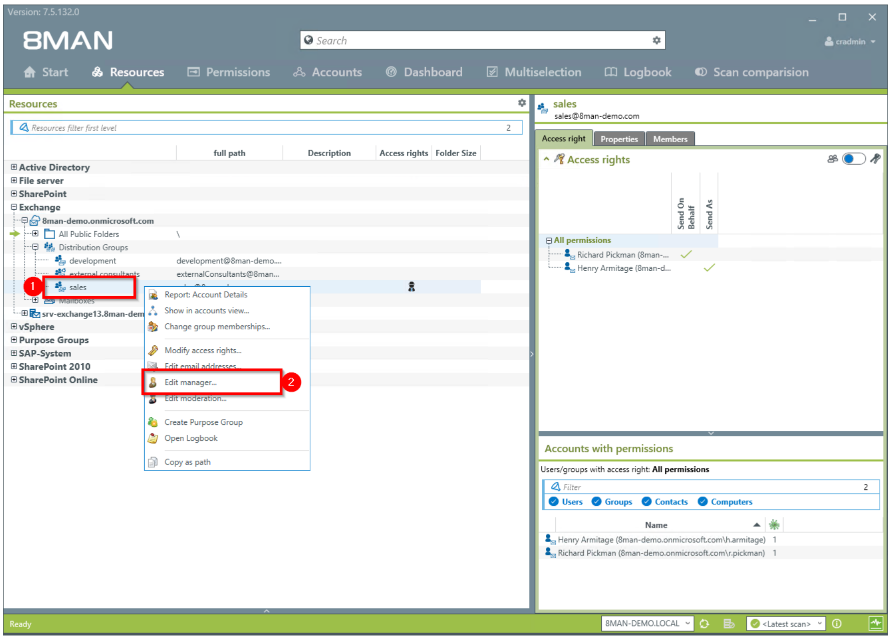
Background / Value

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.

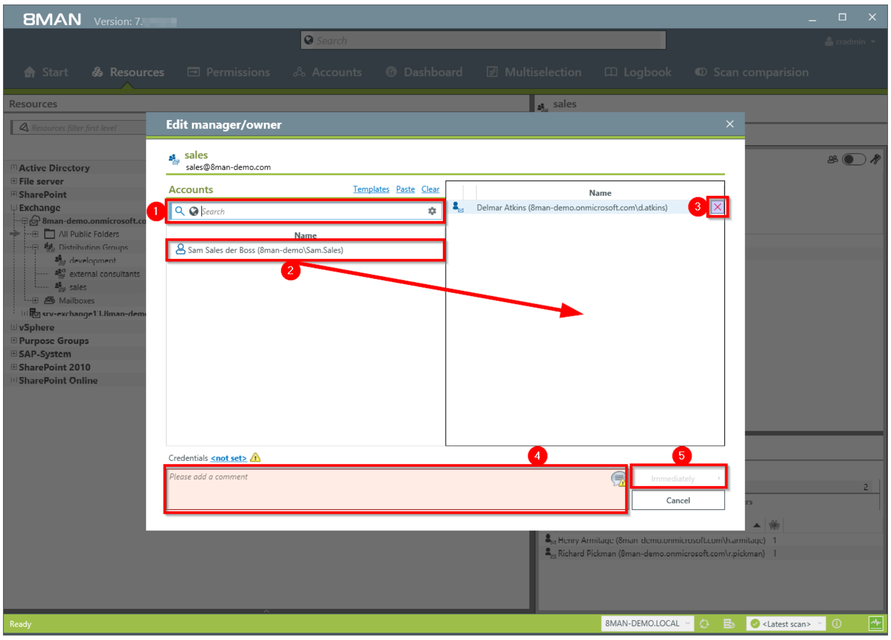
Step by step process


8MAN
sales
Start
Resources
Permissions
Scan comparision
Users (1)
Sam Sales der Boss (8man-demo\Sam.Sales) displayname: Sam Sales der Bos...
Groups
See more results
EX_Sales (8man-demo\EX_Sales) cn: EX_Sales samaccountname: E...
Vertrieb (8man-demo\Sales) cn: Sales samaccountname: Sales
Contacts (0)
Directories (0)
SharePoint Resources (0)
Mailboxes (1)
Sam Sales der Boss SamSales@8man-demo.local
vSphere (0)
Public Folders (1)
Sales Folder: Sales
Mailbox Folders (0)
Active Directory Resources
Sales name: Sales
EX_Sales cn: EX_Sales name: EX_Sales
Distribution Group (1)
sales Name: sales Identity: sales SAM...
Exchange Account (1)
sales Name: sales Identity: sales Email...
Purpose Groups (0)
8MAN Logbook
11/4/2016 5:07 PM - sam.sales \\srv-8man\Vertrieb\Projekte\Gesc
Folder created
11/4/2016 12:01 AM - cradmin Mike Mustermann
User or computer account activated Comment: Ticket-Nr. 123456 Be...
Permission Analysis
User Provisioning
Active Directory
Create new user or group
Edit group memberships
Security Monitoring
Manage alerts
File server
Ready
8MAN-DEMO.LOCAL

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.*

8.4 +8MATE for SharePoint

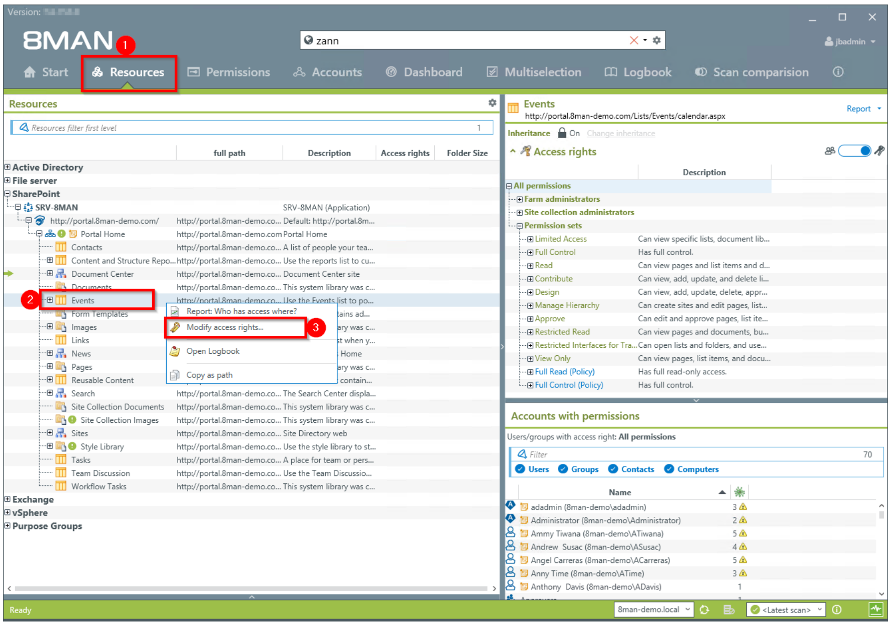
8.4.1 Data Owner

8.4.1.1 Managing 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.

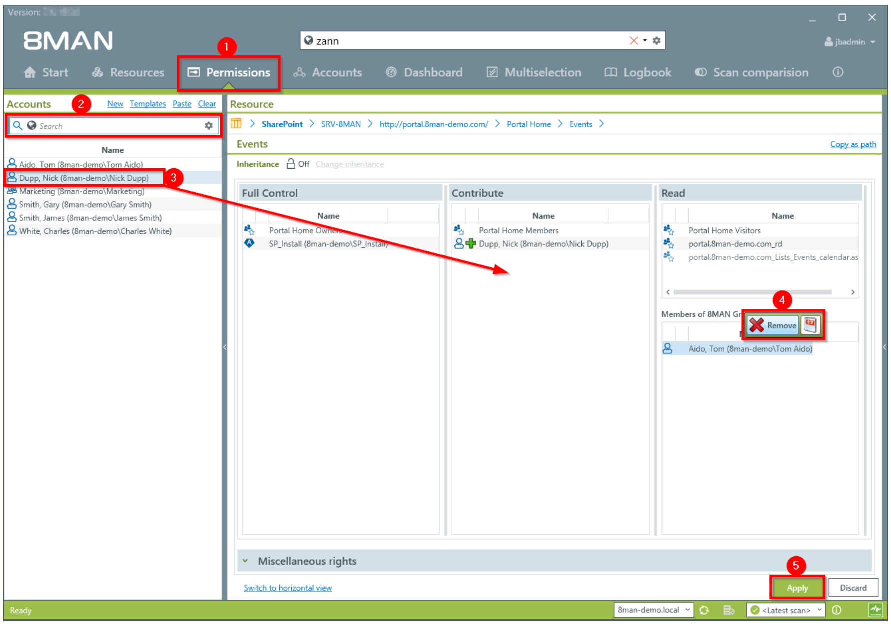
Step by step process



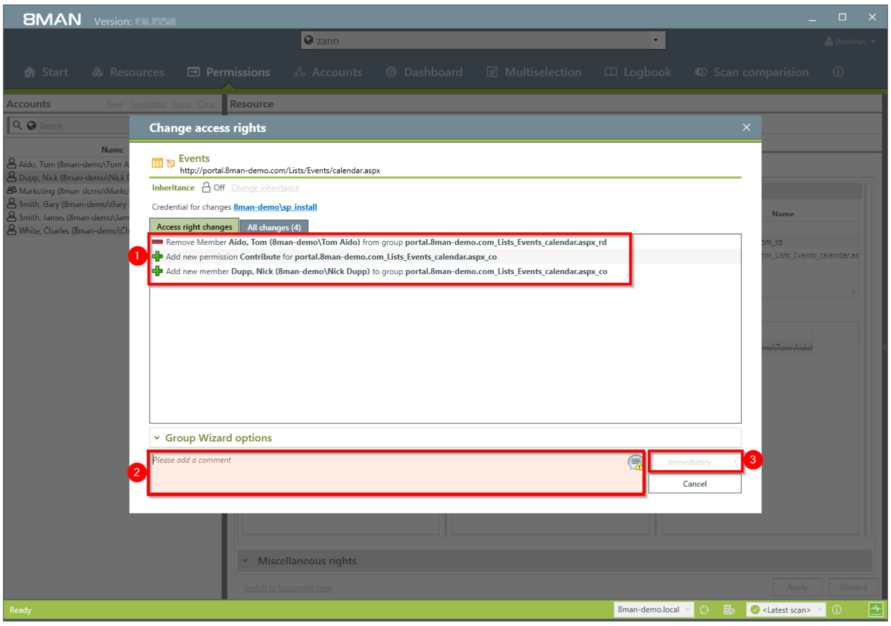
1. Select "Resources".

2. Navigate to the desired resource.

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


8MAN
zann
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
jbadmin
Accounts
New Templates Paste Clear
Search
Name
Aido, Tom (8man-demo\Tom Aido)
Dupp, Nick (8man-demo\Nick Dupp)
Marketing (8man-demo\Marketing)
Smith, Gary (8man-demo\Gary Smith)
Smith, James (8man-demo\James Smith)
White, Charles (8man-demo\Charles White)
Resource
SharePoint > SRV-8MAN > http://portal.8man-demo.com/ > Portal Home > Events
Events
Copy as path
Inheritance Off Change inheritance
Full Control
Portal Home Owners
SP_Install (8man-demo\SP_Install)
Contribute
Portal Home Members
Dupp, Nick (8man-demo\Nick Dupp)
Read
Portal Home Visitors
portal.8man-demo.com_rd
portal.8man-demo.com_Lists_Events_calendar.as
Members of 8MAN Gr
Remove
Aido, Tom (8man-demo\Tom Aido)
Miscellaneous rights
Switch to horizontal view
Apply
Discard
Ready
8man-demo.local
<Latest scan>
1
2
3
4
5

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
Change access rights
Events
http://portal.8man-demo.com/Lists/Events/calendar.aspx
Inheritance Off Change inheritance
Credential for changes 8man-demo\sp_install
Access right changes
All changes (4)
Group Wizard options
Please add a comment
Immediately
Cancel
1
2
3

Remove Member **Aido, Tom (8man-demo\Tom Aido)** from group **portal.8man-demo.com_Lists_Events_calendar.aspx_rd**
Add new permission **Contribute** for **portal.8man-demo.com_Lists_Events_calendar.aspx_co**
Add new member **Dupp, Nick (8man-demo\Nick Dupp)** to group **portal.8man-demo.com_Lists_Events_calendar.aspx_co**

1. *Verify planned changes.*
2. *You must enter a comment.*
3. *Start the change process.*

8.4.2 Administrator

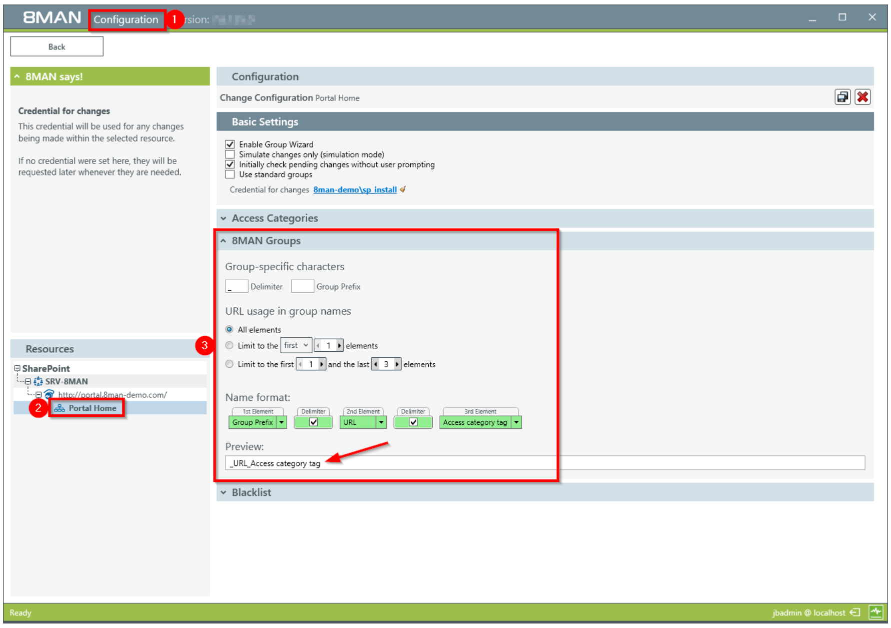
8.4.2.1 Determining naming conventions for access groups

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



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

☑ Enable Group Wizard
☐ Simulate changes only (simulation mode)
☑ Initially check pending changes without user prompting
☐ Use standard groups

Credential for changes 8man-demo\sp_install

Group-specific characters

_ Delimiter; Group Prefix

URL usage in group names

● All elements
○ Limit to the first 1 elements
○ Limit to the first 1 and the last 3 elements

Name format:

1st Element	Delimiter	2nd Element	Delimiter	3rd Element
Group Prefix	☑	URL	☑	Access category tag

Preview:

_URL_Access category tag

1. *Start the configuration module and navigate to "Change Configuration" ->"File server".*
2. *Select the desired SharePoint resource. You can enter different settings for each resource.*
3. *Determine the naming convention. Please note that 8MAN will show you a preview.*

8.5 +8MATE: Analyze & Act

With Analyze & Act we combine services of Documentation & Reporting and User Provisioning. This includes flexible reports and bulk operations for user accounts and file server directories.
Analyze & Act is accessible via aweb client.

You can find the services in the following areas:

Documentation & Reporting

- All AD accounts
- Accounts with no password expire
- All groups in recursions
- Show directories to which all users have access

User Provisioning

Active Directory

- Deactivating Accounts in bulk
- Changing password options in bulk
- Resetting passwords in bulk
- Changing attributes in bulk
- Executing scripts on user accounts in bulk
- Executing scripts for directories in bulk

File server

- Executing scripts for directories in bulk

8.5.1 Deactivating user accounts in bulk

Background / Value

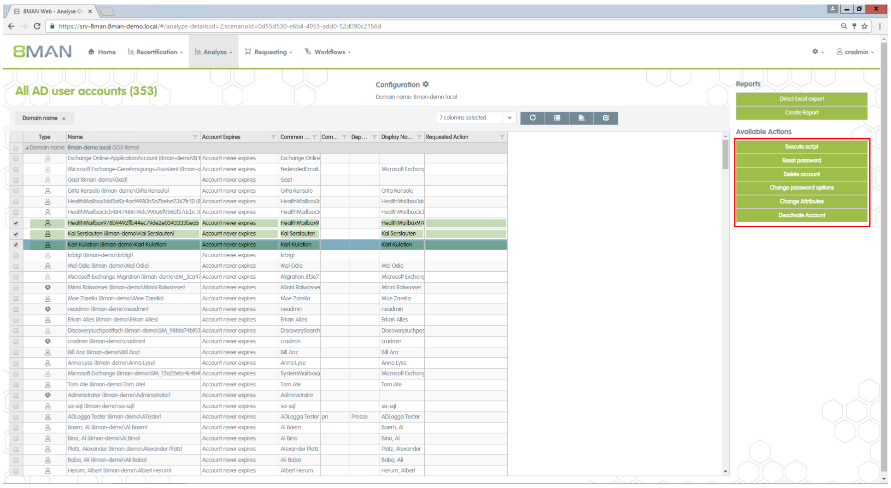
After a security breach it often makes sense to deactivate accounts in bulk. You can do this quickly and easily in the web interface.

Complementary Services

Changing password options in bulk

Deleting accounts in bulk (soft delete)

Step by step process



8MAN Web - Analyse O
https://srv-8man.8man-demo.local/#/analyze-details;id=2;scenarioId=0d55d530-e6b4-4955-add0-52d090c2156d
8MAN
Home
Recertification
Analyze
Requesting
Workflows
cradmin

All AD user accounts (353)

Configuration

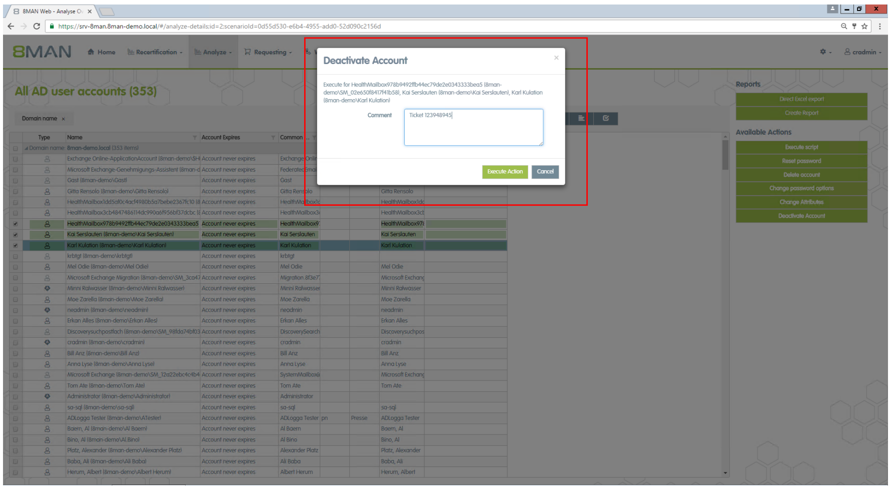
Domain name: 8man-demo.local

Domain name ×

7 columns selected

	Type	Name	Account Expires	Common ...	Com...	Dep...	Display Na...	Requested Action
□	Domain name: 8man-demo.local (353 items)							
□		Exchange Online-ApplicationAccount (8man-demo\$H	Account never expires	Exchange Online				
□		Microsoft Exchange-Genehmigungs-Assistent (8man-d	Account never expires	FederatedEmail.			Microsoft Exchang	
□		Gast (8man-demo\Gast)	Account never expires	Gast				
□		Gitta Rensolo (8man-demo\Gitta Rensolo)	Account never expires	Gitta Rensolo			Gitta Rensolo	
□		HealthMailbox1dd5af0c4acf4980b5a7bebe2367fc10 (8	Account never expires	HealthMailbox1c			HealthMailbox1dc	
□		HealthMailbox3cb4847486114dc990a6f956bf37dcbc (8	Account never expires	HealthMailbox3c			HealthMailbox3cb	
☑		HealthMailbox978b9492ffb44ec79de2e0343333bea5	Account never expires	HealthMailbox97			HealthMailbox978	
☑		Kai Serslauten (8man-demo\Kai Serslauten)	Account never expires	Kai Serslauten			Kai Serslauten	
☑		Karl Kulation (8man-demo\Karl Kulation)	Account never expires	Karl Kulation			Karl Kulation	
□		krbtgt (8man-demo\krbtgt)	Account never expires	krbtgt				
□		Mel Odie (8man-demo\Mel Odie)	Account never expires	Mel Odie			Mel Odie	
□		Microsoft Exchange Migration (8man-demo\SM_3ca47	Account never expires	Migration.8f3e7			Microsoft Exchang	
□		Minni Ralwasser (8man-demo\Minni Ralwasser)	Account never expires	Minni Ralwasser			Minni Ralwasser	
□		Moe Zarella (8man-demo\Moe Zarella)	Account never expires	Moe Zarella			Moe Zarella	
□		neadmin (8man-demo\neadmin)	Account never expires	neadmin			neadmin	
□		Erkan Alles (8man-demo\Erkan Alles)	Account never expires	Erkan Alles			Erkan Alles	
□		Discoverysuchpostfach (8man-demo\SM_98fda74bf03	Account never expires	DiscoverySearch			Discoverysuchpos	
□		cradmin (8man-demo\cradmin)	Account never expires	cradmin			cradmin	
□		Bill Anz (8man-demo\Bill Anz)	Account never expires	Bill Anz			Bill Anz	
□		Anna Lyse (8man-demo\Anna Lyse)	Account never expires	Anna Lyse			Anna Lyse	
□		Microsoft Exchange (8man-demo\SM_12a22ebc4c4b4	Account never expires	SystemMailbox{			Microsoft Exchang	
□		Tom Ate (8man-demo\Tom Ate)	Account never expires	Tom Ate			Tom Ate	
□		Administrator (8man-demo\Administrator)	Account never expires	Administrator				
□		sa-sql (8man-demo\sa-sql)	Account never expires	sa-sql			sa-sql	
□		ADLogga Tester (8man-demo\ATester)	Account never expires	ADLogga Tester	pn	Presse	ADLogga Tester	
□		Baern, Al (8man-demo\Al Baern)	Account never expires	Al Baern			Baern, Al	
□		Bino, Al (8man-demo\Al.Bino)	Account never expires	Al Bino			Bino, Al	
□		Platz, Alexander (8man-demo\Alexander Platz)	Account never expires	Alexander Platz			Platz, Alexander	
□		Baba, Ali (8man-demo\Ali Baba)	Account never expires	Ali Baba			Baba, Ali	
□		Herum, Albert (8man-demo\Albert Herum)	Account never expires	Albert Herum			Herum, Albert	

Click on "Deactivate Account".



Deactivate Account

Execute for HealthMailbox978b9492ffb44ec79de2e0343333bea5 (8man-demo\SM_02e650f8417f41b58), Kai Serslauten (8man-demo\Kai Serslauten), Karl Kulation (8man-demo\Karl Kulation)

Comment: Ticket 123948945

Click on "Execute Action". You must enter a comment, for example a ticket number.

8.5.2 Deleting accounts in bulk (soft delete)

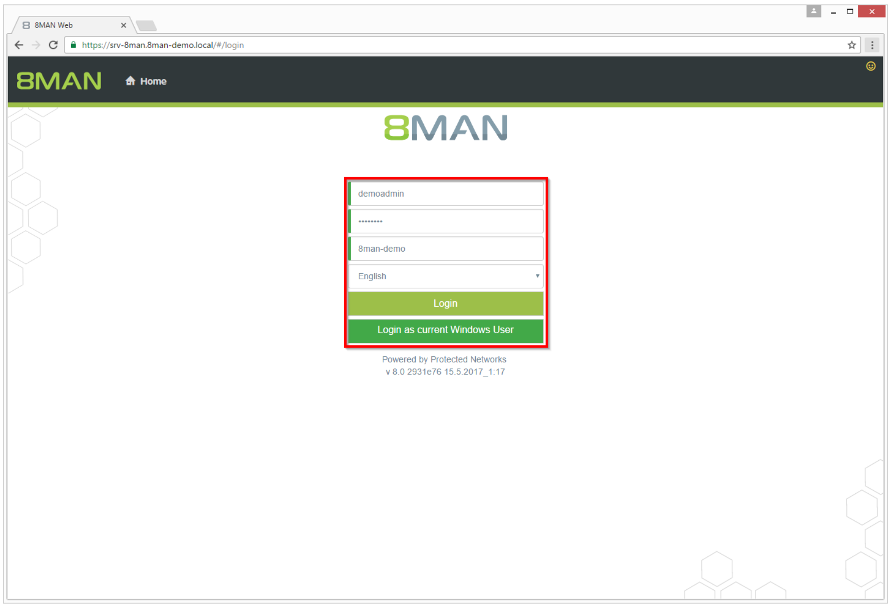
Background / Value

Nach einem Security Breach oder der Auflösung einer Abteilung macht es Sinn, mehrere Konten gleichzeitig zu löschen. Erledigen Sie dies bequem im Webclient.

Additional Services

Kennwort Optionen im Bulk ändern
Konten im Bulk löschen (soft delete)

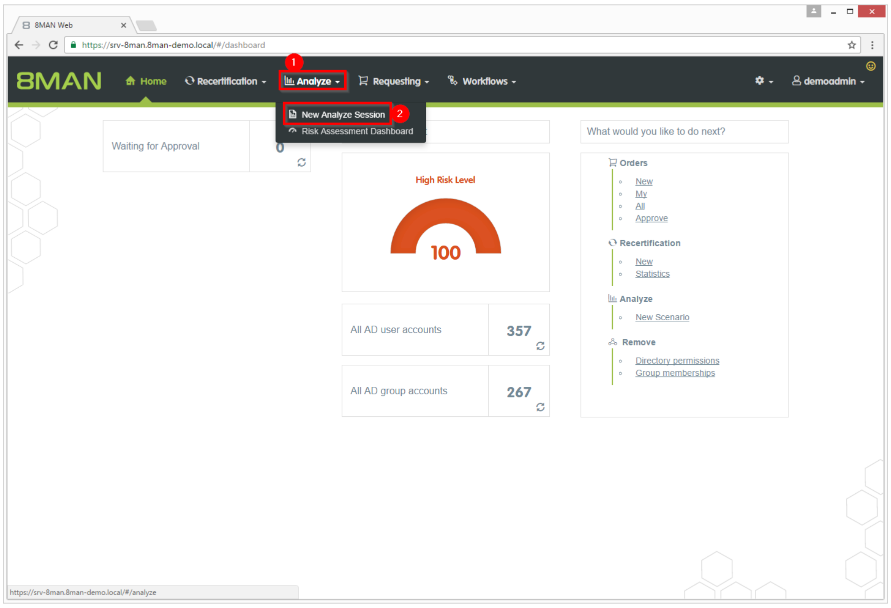
Step by step process


8MAN Web
https://srv-8man.8man-demo.local/#/login
8MAN
Home
8MAN
Login
Login as current Windows User

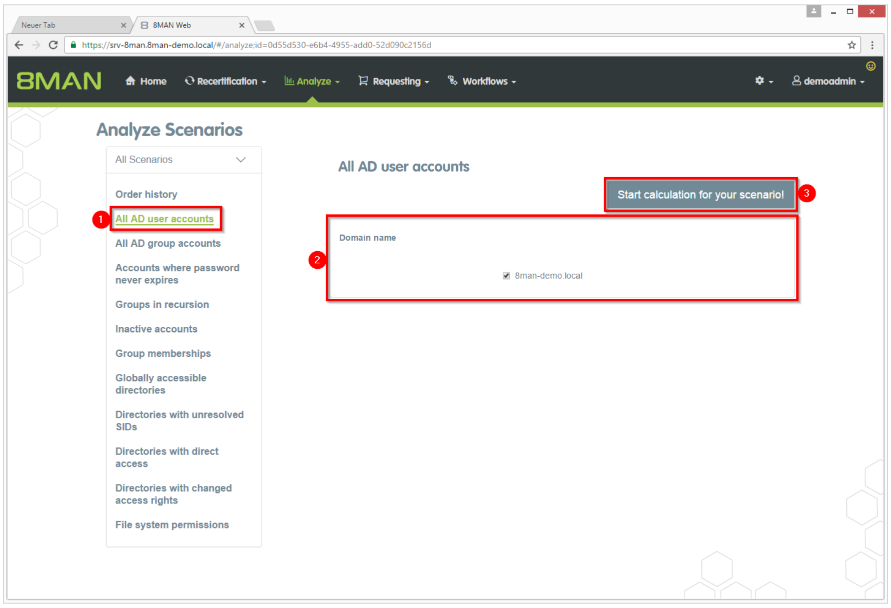
demoadmin
••••••••
8man-demo
English

Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

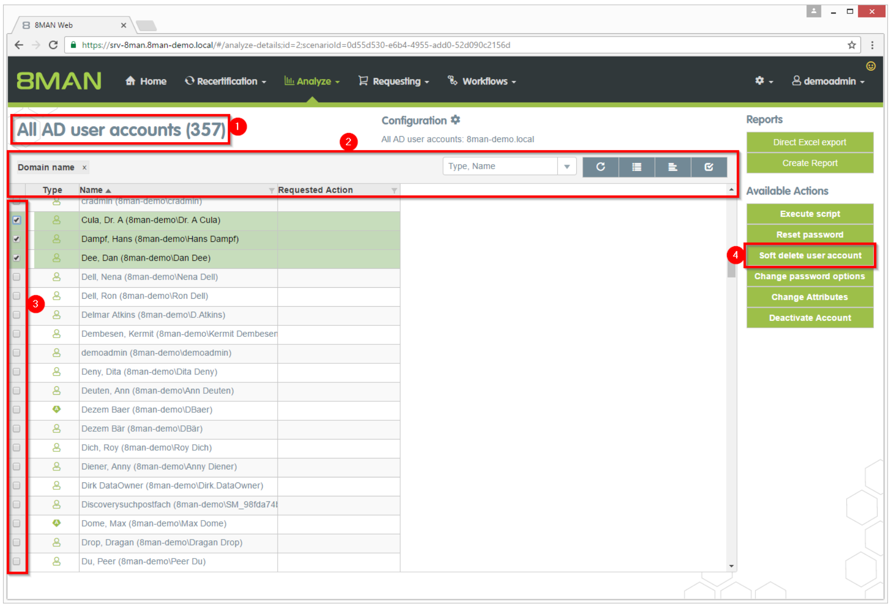
1. *Login to the web client.*



1. *Click "Analyze".*
2. *Click "New Analyze Session".*

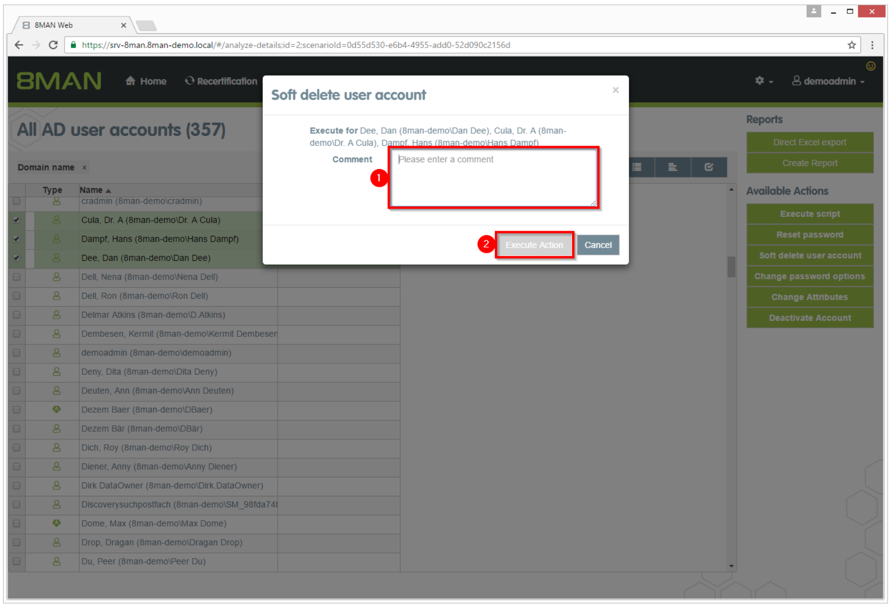

Neuer Tab
8MAN Web
https://srv-8man.8man-demo.local/#/analyze;id=0d55d530-e6b4-4955-add0-52d090c2156d
8MAN
Home
Recertification
Analyze
Requesting
Workflows
demoadmin
Analyze Scenarios
All Scenarios
Order history
1
All AD user accounts
All AD group accounts
Accounts where password never expires
Groups in recursion
Inactive accounts
Group memberships
Globally accessible directories
Directories with unresolved SIDs
Directories with direct access
Directories with changed access rights
File system permissions
All AD user accounts
Start calculation for your scenario!
3
2
Domain name
☑ 8man-demo.local

1. Click "All AD user accounts".
2. Select a domain.
3. Start the calculation.



	Type	Name ▲	Requested Action
□		cradmin (8man-demo\cradmin)	
☑		Cula, Dr. A (8man-demo\Dr. A Cula)	
☑		Dampf, Hans (8man-demo\Hans Dampf)	
☑		Dee, Dan (8man-demo\Dan Dee)	
□		Dell, Nena (8man-demo\Nena Dell)	
□		Dell, Ron (8man-demo\Ron Dell)	
□		Delmar Atkins (8man-demo\D.Atkins)	
□		Dembesen, Kermit (8man-demo\Kermit Dembesen	
□		demoadmin (8man-demo\demoadmin)	
□		Deny, Dita (8man-demo\Dita Deny)	
□		Deuten, Ann (8man-demo\Ann Deuten)	
□		Dezem Baer (8man-demo\DBaer)	
□		Dezem Bär (8man-demo\DBär)	
□		Dich, Roy (8man-demo\Roy Dich)	
□		Diener, Anny (8man-demo\Anny Diener)	
□		Dirk DataOwner (8man-demo\Dirk.DataOwner)	
□		Discoverysuchpostfach (8man-demo\SM_98fda74l	
□		Dome, Max (8man-demo\Max Dome)	
□		Drop, Dragan (8man-demo\Dragan Drop)	
□		Du, Peer (8man-demo\Peer Du)	

1. 8MAN lists all AD accounts.
2. Use sorting, filtering, grouping and column selection to locate the desired rows.
3. Select the desired entries.
4. Click "Soft delete user account".



All AD user accounts (357)

Domain name ×

	Type	Name ▲
□		cradmin (8man-demo\cradmin)
☑		Cula, Dr. A (8man-demo\Dr. A Cula)
☑		Dampf, Hans (8man-demo\Hans Dampf)
☑		Dee, Dan (8man-demo\Dan Dee)
□		Dell, Nena (8man-demo\Nena Dell)
□		Dell, Ron (8man-demo\Ron Dell)
□		Delmar Atkins (8man-demo\D.Atkins)
□		Dembesen, Kermit (8man-demo\Kermit Dembesen
□		demoadmin (8man-demo\demoadmin)
□		Deny, Dita (8man-demo\Dita Deny)
□		Deuten, Ann (8man-demo\Ann Deuten)
□		Dezem Baer (8man-demo\DBaer)
□		Dezem Bär (8man-demo\DBär)
□		Dich, Roy (8man-demo\Roy Dich)
□		Diener, Anny (8man-demo\Anny Diener)
□		Dirk DataOwner (8man-demo\Dirk.DataOwner)
□		Discoverysuchpostfach (8man-demo\SM_98fda74
□		Dome, Max (8man-demo\Max Dome)
□		Drop, Dragan (8man-demo\Dragan Drop)
□		Du, Peer (8man-demo\Peer Du)

Soft delete user account

Execute for Dee, Dan (8man-demo\Dan Dee), Cula, Dr. A (8man-demo\Dr. A Cula), Dampf, Hans (8man-demo\Hans Dampf)

Comment Please enter a comment

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".

8.5.3 Removing unresolved SIDs in bulk

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.

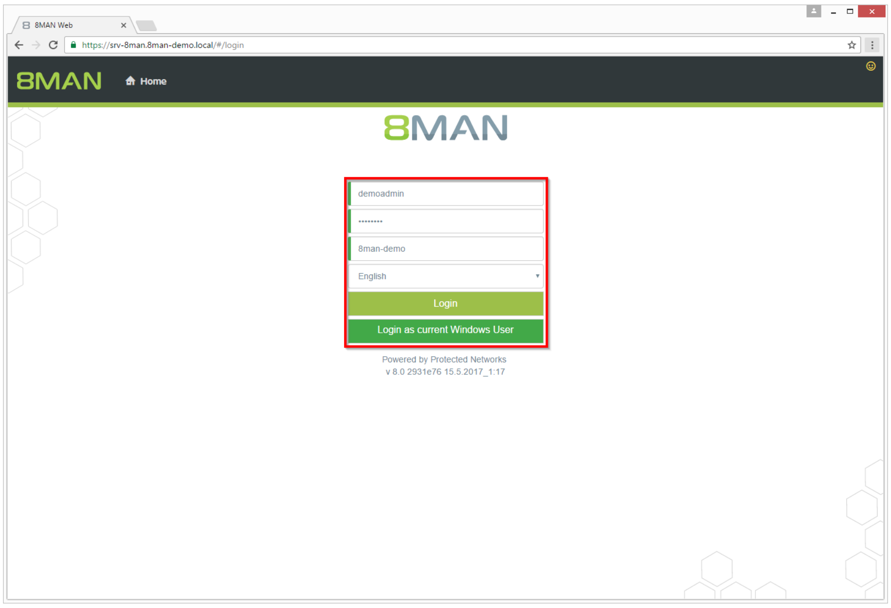
8MAN clearly identifies unresolved SIDs in your system. Delete unresolved SIDs in bulk using Analyze & Act.

Additional Services

Identifying and deleting unresolved SIDs (using the rich client)

Report: Identifying unresolved SIDs (using the rich client)

Step by step process



https://srv-8man.8man-demo.local/#/login

demoadmin

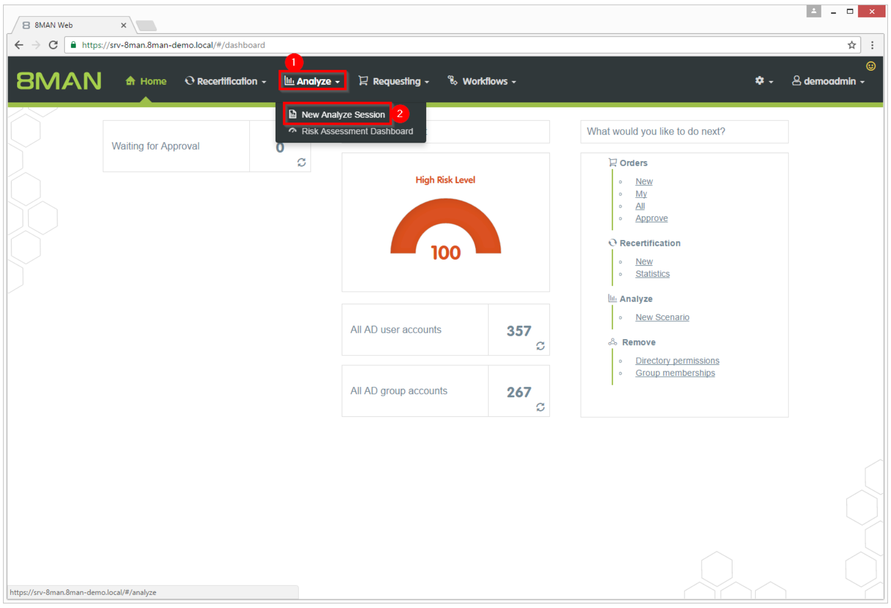
••••••••

8man-demo

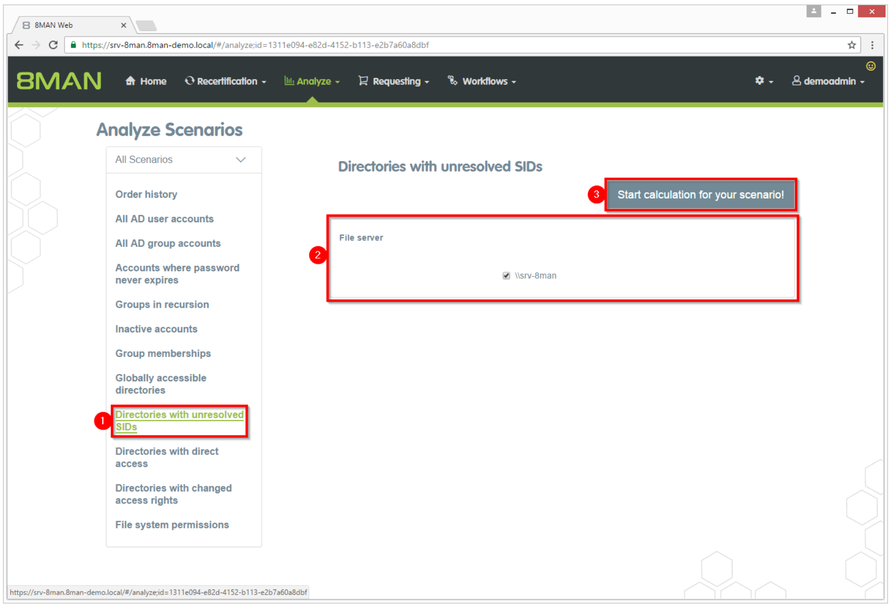
English

Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

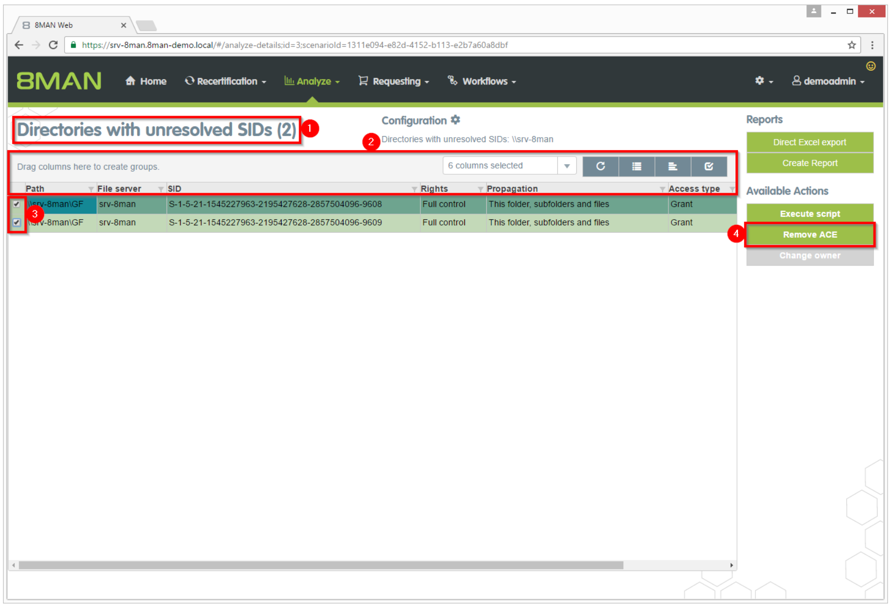
1. *Login to the web client.*



1. *Click "Analyze".*
2. *Click "New Analyze Session".*

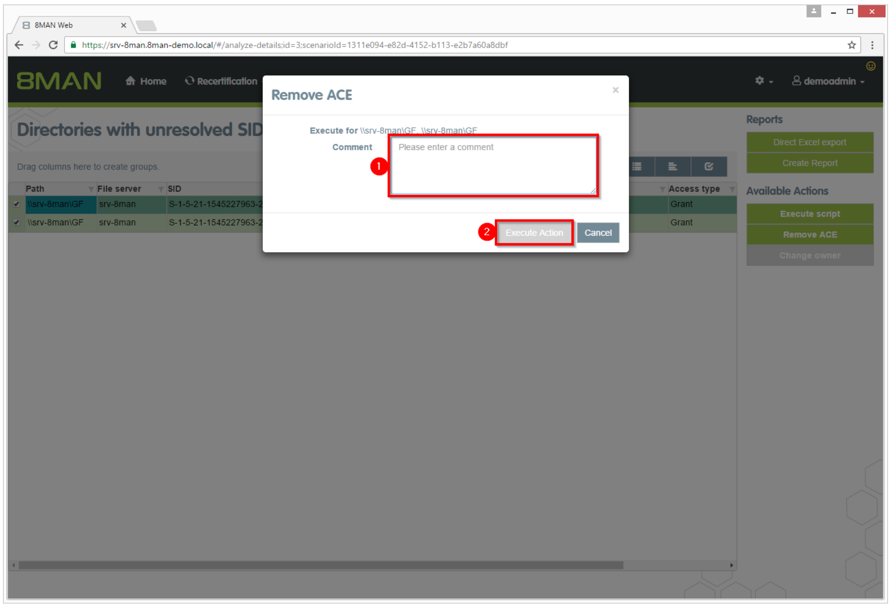

8MAN Web
https://srv-8man.8man-demo.local/#/analyze;id=1311e094-e82d-4152-b113-e2b7a60a8dbf
8MAN
Home
Recertification
Analyze
Requesting
Workflows
demoadmin
Analyze Scenarios
All Scenarios
Order history
All AD user accounts
All AD group accounts
Accounts where password never expires
Groups in recursion
Inactive accounts
Group memberships
Globally accessible directories
1
Directories with unresolved SIDs
Directories with direct access
Directories with changed access rights
File system permissions
Directories with unresolved SIDs
3
Start calculation for your scenario!
2
File server
☑ \\srv-8man
https://srv-8man.8man-demo.local/#/analyze;id=1311e094-e82d-4152-b113-e2b7a60a8dbf

1. *Click "Directories with unresolved SIDs".*
2. *Select a file server.*
3. *Start the calculation.*


8MAN Web
https://srv-8man.8man-demo.local/#/analyze-details;id=3;scenarioId=1311e094-e82d-4152-b113-e2b7a60a8dbf
8MAN
Home
Recertification
Analyze
Requesting
Workflows
demoadmin
Directories with unresolved SIDs (2)
1
Configuration
2
Directories with unresolved SIDs: \\srv-8man
Drag columns here to create groups.
6 columns selected
3
Reports
Direct Excel export
Create Report
Available Actions
Execute script
4
Remove ACE
Change owner

	Path	File server	SID	Rights	Propagation	Access type
☑	\\srv-8man\GF	srv-8man	S-1-5-21-1545227963-2195427628-2857504096-9608	Full control	This folder, subfolders and files	Grant
☑	\\srv-8man\GF	srv-8man	S-1-5-21-1545227963-2195427628-2857504096-9609	Full control	This folder, subfolders and files	Grant

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".*


8MAN Web
https://srv-8man.8man-demo.local/#/analyze-details;id=3;scenarioId=1311e094-e82d-4152-b113-e2b7a60a8dbf
8MAN
Home
Recertification
demoadmin
Directories with unresolved SID
Drag columns here to create groups.
Reports
Direct Excel export
Create Report
Available Actions
Execute script
Remove ACE
Change owner
Remove ACE
1
2
Execute Action
Cancel

Execute for \\srv-8man\GF, \\srv-8man\GF

Comment: Please enter a comment

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".

8.5.4 Changing password options in bulk

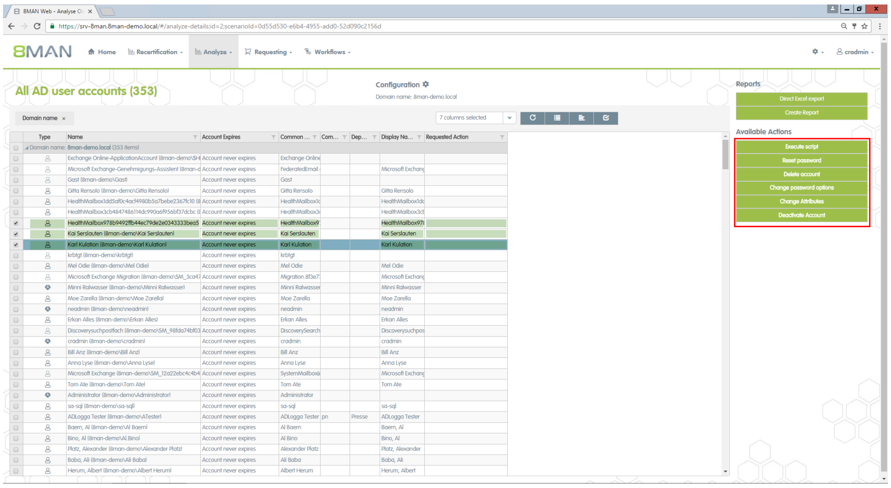
Background / Value

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

Additional Services

Resetting passwords in bulk

Step by step process



All AD user accounts (353)

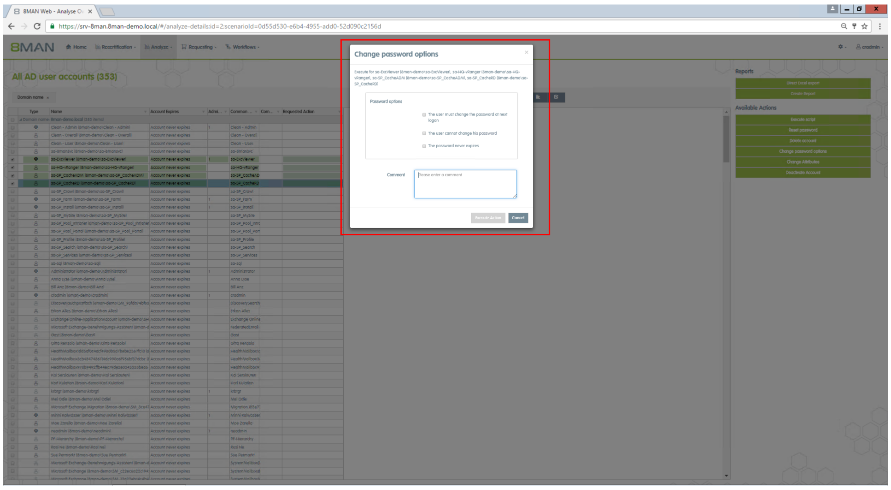
Domain name: 8man-demo.local

Domain name ×

7 columns selected

	Type	Name	Account Expires	Common ...	Com...	Dep...	Display Na...	Requested Action
☐	Domain name: 8man-demo.local (353 items)							
☐		Exchange Online-ApplicationAccount (8man-demo\$H	Account never expires	Exchange Online				
☐		Microsoft Exchange-Genehmigungs-Assistent (8man-d	Account never expires	FederatedEmail.4			Microsoft Exchang	
☐		Gast (8man-demo\Gast)	Account never expires	Gast				
☐		Gitta Rensolo (8man-demo\Gitta Rensolo)	Account never expires	Gitta Rensolo			Gitta Rensolo	
☐		HealthMailbox1dd5af0c4acf4980b5a7bebe2367fc10 (8	Account never expires	HealthMailbox1c			HealthMailbox1dc	
☐		HealthMailbox3cb4847486114dc990a6f956bf37dcbc (8	Account never expires	HealthMailbox3c			HealthMailbox3cb	
☑		HealthMailbox978b9492ffb44ec79de2e0343333bea5	Account never expires	HealthMailbox97			HealthMailbox978	
☑		Kai Serslauten (8man-demo\Kai Serslauten)	Account never expires	Kai Serslauten			Kai Serslauten	
☑		Karl Kulation (8man-demo\Karl Kulation)	Account never expires	Karl Kulation			Karl Kulation	
☐		krbtgt (8man-demo\krbtgt)	Account never expires	krbtgt				
☐		Mel Odie (8man-demo\Mel Odie)	Account never expires	Mel Odie			Mel Odie	
☐		Microsoft Exchange Migration (8man-demo\SM_3ca47	Account never expires	Migration.8f3e77			Microsoft Exchang	
☐		Minni Ralwasser (8man-demo\Minni Ralwasser)	Account never expires	Minni Ralwasser			Minni Ralwasser	
☐		Moe Zarella (8man-demo\Moe Zarella)	Account never expires	Moe Zarella			Moe Zarella	
☐		neadmin (8man-demo\neadmin)	Account never expires	neadmin			neadmin	
☐		Erkan Alles (8man-demo\Erkan Alles)	Account never expires	Erkan Alles			Erkan Alles	
☐		Discoverysuchpostfach (8man-demo\SM_98fda74bf03	Account never expires	DiscoverySearch			Discoverysuchpos	
☐		cradmin (8man-demo\cradmin)	Account never expires	cradmin			cradmin	
☐		Bill Anz (8man-demo\Bill Anz)	Account never expires	Bill Anz			Bill Anz	
☐		Anna Lyse (8man-demo\Anna Lyse)	Account never expires	Anna Lyse			Anna Lyse	
☐		Microsoft Exchange (8man-demo\SM_12a22ebc4c4b4	Account never expires	SystemMailbox{e			Microsoft Exchang	
☐		Tom Ate (8man-demo\Tom Ate)	Account never expires	Tom Ate			Tom Ate	
☐		Administrator (8man-demo\Administrator)	Account never expires	Administrator				
☐		sa-sql (8man-demo\sa-sql)	Account never expires	sa-sql			sa-sql	
☐		ADLogga Tester (8man-demo\ATester)	Account never expires	ADLogga Tester	pn	Presse	ADLogga Tester	
☐		Baern, Al (8man-demo\Al Baern)	Account never expires	Al Baern			Baern, Al	
☐		Bino, Al (8man-demo\Al.Bino)	Account never expires	Al Bino			Bino, Al	
☐		Platz, Alexander (8man-demo\Alexander Platz)	Account never expires	Alexander Platz			Platz, Alexander	
☐		Baba, Ali (8man-demo\Ali Baba)	Account never expires	Ali Baba			Baba, Ali	
☐		Herum, Albert (8man-demo\Albert Herum)	Account never expires	Albert Herum			Herum, Albert	

Click on "Change password options".


8MAN Web - Analyse O
https://srv-8man.8man-demo.local/#/analyze-details;id=2;scenarioId=0d55d530-e6b4-4955-add0-52d090c2156d
8MAN
Home
Recertification
Analyze
Requesting
Workflows
All AD user accounts (353)
Reports
Available Actions
Execute Action
Cancel

Change password options

Execute for sa-ExcViewer (8man-demo\sa-ExcViewer), sa-HQ-vRanger (8man-demo\sa-HQ-vRanger), sa-SP_CacheADM (8man-demo\sa-SP_CacheADM), sa-SP_CacheRD (8man-demo\sa-SP_CacheRD)

Password options

- ☐ The user must change the password at next logon
- ☐ The user cannot change his password
- ☐ The password never expires

Comment: Please enter a comment

Click on "Execute Action". You must enter a comment, for example a ticket number.

8.5.5 Resetting passwords in bulk

Background / Value

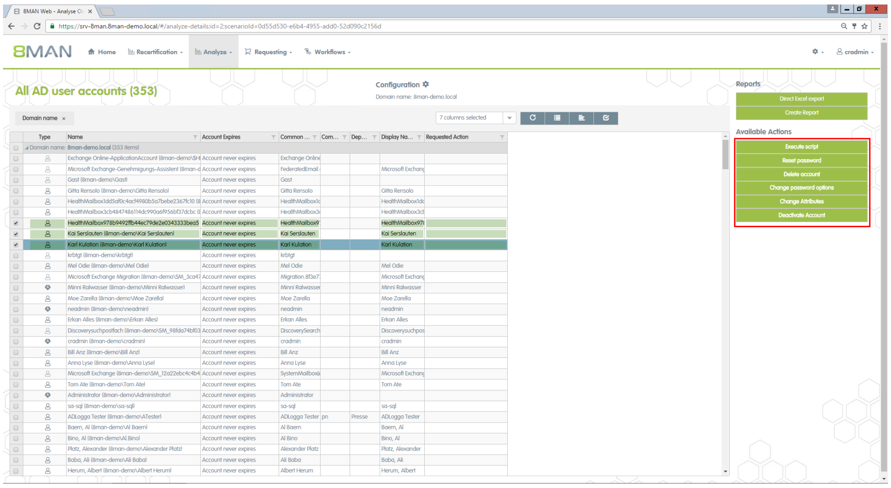
There are many use cases in which the passwords of several users must be reset simultaneously. You can reset passwords in bulk in the web interface.

Additional Services

Deactivating user accounts in bulk

Changing password options in bulk

Step by step process



https://srv-8man.8man-demo.local/#/analyze-details;id=2;scenarioId=0d55d530-e6b4-4955-add0-52d090c2156d

All AD user accounts (353)

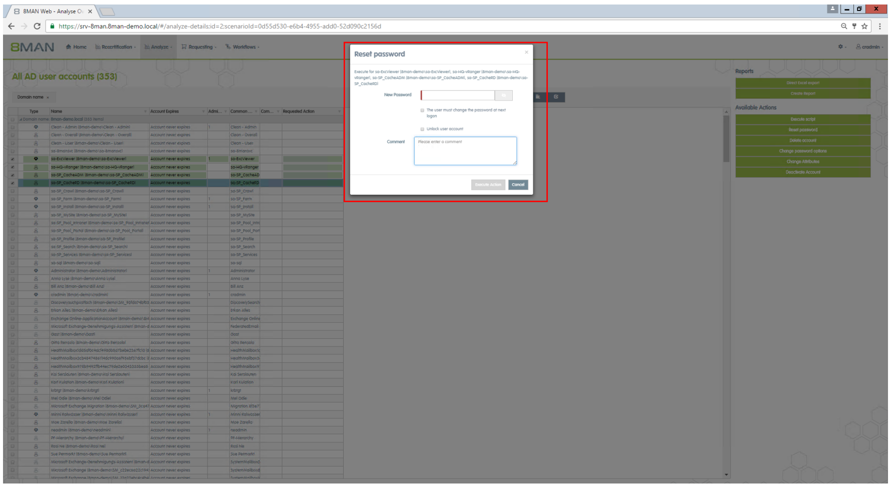
Configuration
Domain name: 8man-demo.local

Domain name ×

7 columns selected

☐	Type	Name	Account Expires	Common ...	Com...	Dep...	Display Na...	Requested Action
☐	Domain name: 8man-demo.local (353 items)							
☐		Exchange Online-ApplicationAccount (8man-demo\$H	Account never expires	Exchange Online				
☐		Microsoft Exchange-Genehmigungs-Assistent (8man-d	Account never expires	FederatedEmail.4			Microsoft Exchang	
☐		Gast (8man-demo\Gast)	Account never expires	Gast				
☐		Gitta Rensolo (8man-demo\Gitta Rensolo)	Account never expires	Gitta Rensolo			Gitta Rensolo	
☐		HealthMailbox1dd5af0c4acf4980b5a7bebe2367fc10 (8	Account never expires	HealthMailbox1c			HealthMailbox1dc	
☐		HealthMailbox3cb4847486114dc990a6f956bf37dcbc (8	Account never expires	HealthMailbox3c			HealthMailbox3cb	
☑		HealthMailbox978b9492ffb44ec79de2e0343333bea5	Account never expires	HealthMailbox97			HealthMailbox97	
☑		Kai Serslauten (8man-demo\Kai Serslauten)	Account never expires	Kai Serslauten			Kai Serslauten	
☑		Karl Kulation (8man-demo\Karl Kulation)	Account never expires	Karl Kulation			Karl Kulation	
☐		krbtgt (8man-demo\krbtgt)	Account never expires	krbtgt				
☐		Mel Odie (8man-demo\Mel Odie)	Account never expires	Mel Odie			Mel Odie	
☐		Microsoft Exchange Migration (8man-demo\SM_3ca47	Account never expires	Migration.8f3e7			Microsoft Exchang	
☐		Minni Ralwasser (8man-demo\Minni Ralwasser)	Account never expires	Minni Ralwasser			Minni Ralwasser	
☐		Moe Zarella (8man-demo\Moe Zarella)	Account never expires	Moe Zarella			Moe Zarella	
☐		neadmin (8man-demo\neadmin)	Account never expires	neadmin			neadmin	
☐		Erkan Alles (8man-demo\Erkan Alles)	Account never expires	Erkan Alles			Erkan Alles	
☐		Discoverysuchpostfach (8man-demo\SM_98fda74bf03	Account never expires	DiscoverySearch			Discoverysuchpos	
☐		cradmin (8man-demo\cradmin)	Account never expires	cradmin			cradmin	
☐		Bill Anz (8man-demo\Bill Anz)	Account never expires	Bill Anz			Bill Anz	
☐		Anna Lyse (8man-demo\Anna Lyse)	Account never expires	Anna Lyse			Anna Lyse	
☐		Microsoft Exchange (8man-demo\SM_12a22ebc4c4b4	Account never expires	SystemMailbox{			Microsoft Exchang	
☐		Tom Ate (8man-demo\Tom Ate)	Account never expires	Tom Ate			Tom Ate	
☐		Administrator (8man-demo\Administrator)	Account never expires	Administrator				
☐		sa-sql (8man-demo\sa-sql)	Account never expires	sa-sql			sa-sql	
☐		ADLogga Tester (8man-demo\ATester)	Account never expires	ADLogga Tester	pn	Presse	ADLogga Tester	
☐		Baern, Al (8man-demo\Al Baern)	Account never expires	Al Baern			Baern, Al	
☐		Bino, Al (8man-demo\Al.Bino)	Account never expires	Al Bino			Bino, Al	
☐		Platz, Alexander (8man-demo\Alexander Platz)	Account never expires	Alexander Platz			Platz, Alexander	
☐		Baba, Ali (8man-demo\Ali Baba)	Account never expires	Ali Baba			Baba, Ali	
☐		Herum, Albert (8man-demo\Albert Herum)	Account never expires	Albert Herum			Herum, Albert	

Click on "Reset Password".



https://srv-8man.8man-demo.local/#/analyze-details;id=2;scenarioId=0d55d530-e6b4-4955-add0-52d090c2156d

All AD user accounts (353)

Reset password

Execute for sa-ExcViewer (8man-demo\sa-ExcViewer), sa-HQ-vRanger (8man-demo\sa-HQ-vRanger), sa-SP_CacheADM (8man-demo\sa-SP_CacheADM), sa-SP_CacheRD (8man-demo\sa-SP_CacheRD)

New Password

☐ The user must change the password at next logon

☐ Unlock user account

Comment: Please enter a comment

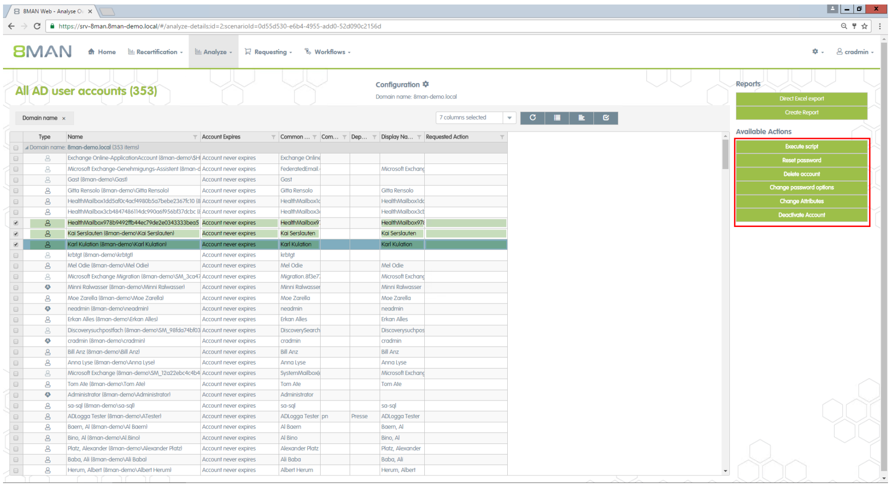
Enter a new Password. Enter a comment, for example a ticket number. Click on "Execute action".

8.5.6 Modifying attributes in bulk

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.

Step by step process



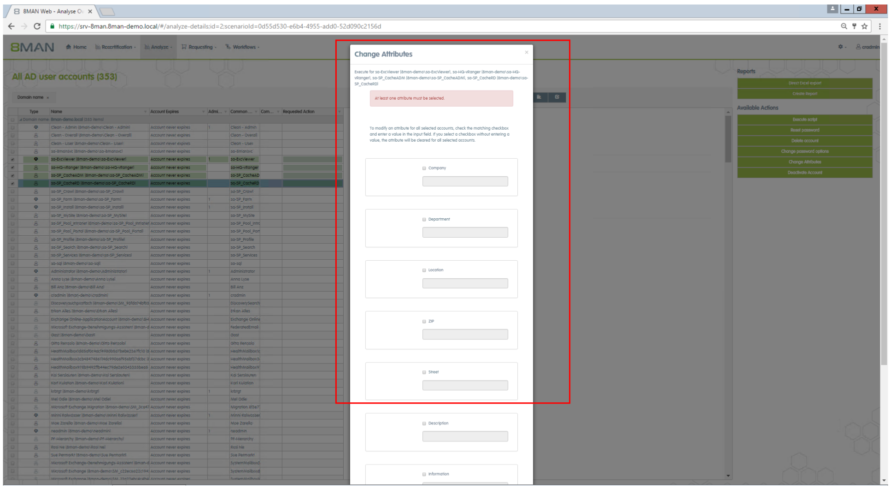
All AD user accounts (353)

Configuration

Domain name: 8man-demo.local

	Type	Name	Account Expires	Common ...	Com...	Dep...	Display Na...	Requested Action
□	Domain name: 8man-demo.local (353 items)							
□		Exchange Online-ApplicationAccount (8man-demo\$H	Account never expires	Exchange Online				
□		Microsoft Exchange-Genehmigungs-Assistent (8man-d	Account never expires	FederatedEmail.			Microsoft Exchang	
□		Gast (8man-demo\Gast)	Account never expires	Gast				
□		Gitta Rensolo (8man-demo\Gitta Rensolo)	Account never expires	Gitta Rensolo			Gitta Rensolo	
□		HealthMailbox1dd5af0c4acf4980b5a7bebe2367fc10 (8	Account never expires	HealthMailbox1c			HealthMailbox1dc	
□		HealthMailbox3cb4847486114dc990a6f956bf37dcbc (8	Account never expires	HealthMailbox3			HealthMailbox3cb	
☑		HealthMailbox978b9492ffb44ec79de2e0343333bea5	Account never expires	HealthMailbox97			HealthMailbox978	
☑		Kai Serslauten (8man-demo\Kai Serslauten)	Account never expires	Kai Serslauten			Kai Serslauten	
☑		Karl Kulation (8man-demo\Karl Kulation)	Account never expires	Karl Kulation			Karl Kulation	
□		krbtgt (8man-demo\krbtgt)	Account never expires	krbtgt				
□		Mel Odie (8man-demo\Mel Odie)	Account never expires	Mel Odie			Mel Odie	
□		Microsoft Exchange Migration (8man-demo\SM_3ca47	Account never expires	Migration.8f3e7			Microsoft Exchang	
□		Minni Ralwasser (8man-demo\Minni Ralwasser)	Account never expires	Minni Ralwasser			Minni Ralwasser	
□		Moe Zarella (8man-demo\Moe Zarella)	Account never expires	Moe Zarella			Moe Zarella	
□		neadmin (8man-demo\neadmin)	Account never expires	neadmin			neadmin	
□		Erkan Alles (8man-demo\Erkan Alles)	Account never expires	Erkan Alles			Erkan Alles	
□		Discoverysuchpostfach (8man-demo\SM_98fda74bf03	Account never expires	DiscoverySearch			Discoverysuchpos	
□		cradmin (8man-demo\cradmin)	Account never expires	cradmin			cradmin	
□		Bill Anz (8man-demo\Bill Anz)	Account never expires	Bill Anz			Bill Anz	
□		Anna Lyse (8man-demo\Anna Lyse)	Account never expires	Anna Lyse			Anna Lyse	
□		Microsoft Exchange (8man-demo\SM_12a22ebc4c4b4	Account never expires	SystemMailbox(			Microsoft Exchang	
□		Tom Ate (8man-demo\Tom Ate)	Account never expires	Tom Ate			Tom Ate	
□		Administrator (8man-demo\Administrator)	Account never expires	Administrator				
□		sa-sql (8man-demo\sa-sql)	Account never expires	sa-sql			sa-sql	
□		ADLogga Tester (8man-demo\ATester)	Account never expires	ADLogga Tester	pn	Presse	ADLogga Tester	
□		Baern, Al (8man-demo\Al Baern)	Account never expires	Al Baern			Baern, Al	
□		Bino, Al (8man-demo\Al.Bino)	Account never expires	Al Bino			Bino, Al	
□		Platz, Alexander (8man-demo\Alexander Platz)	Account never expires	Alexander Platz			Platz, Alexander	
□		Baba, Ali (8man-demo\Ali Baba)	Account never expires	Ali Baba			Baba, Ali	
□		Herum, Albert (8man-demo\Albert Herum)	Account never expires	Albert Herum			Herum, Albert	

Click on "Change Attributes".


8MAN Web - Analyse O
https://srv-8man.8man-demo.local/#/analyze-details;id=2;scenarioId=0d55d530-e6b4-4955-add0-52d090c2156d
8MAN
Home
Recertification
Analyze
Requesting
Workflows
All AD user accounts (353)
Reports
Available Actions

Change Attributes ×

Execute for sa-ExcViewer (8man-demo\sa-ExcViewer), sa-HQ-vRanger (8man-demo\sa-HQ-vRanger), sa-SP_CacheADM (8man-demo\sa-SP_CacheADM), sa-SP_CacheRD (8man-demo\sa-SP_CacheRD)

At least one attribute must be selected.

To modify an attribute for all selected accounts, check the matching checkbox and enter a value in the input field. If you select a checkbox without entering a value, the attribute will be cleared for all selected accounts.

□ Company

□ Department

□ Location

□ ZIP

□ Street

□ Description

□ Information

Activate the checkboxes for the desired attributes and enter the desired value.

8.5.7 Executing scripts on user accounts in bulk

Background / Value

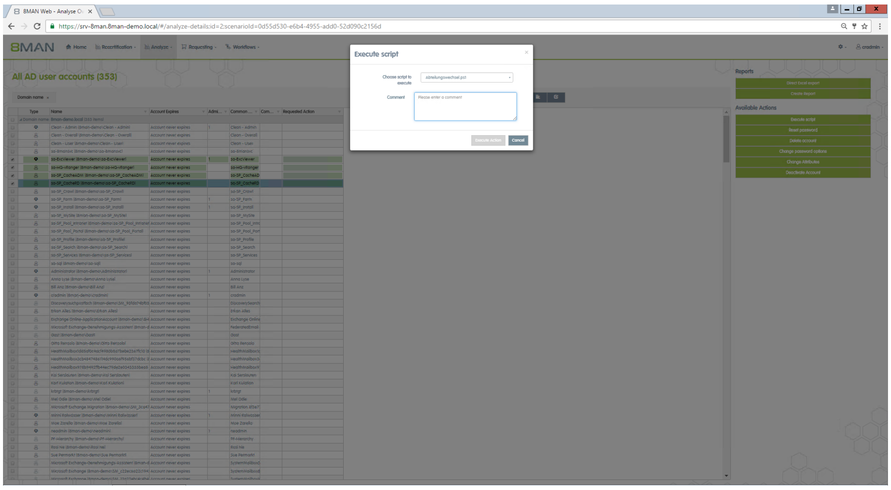
8MATE Analyze & Act allows you to use your own scripts. Just store them in the following directory and you can use them in the 8MAN web client.

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

Additional Services

Executing scripts on directories in bulk

Step by step process



Execute script

Choose script to execute: Abteilungswechsel.ps1

Comment: Please enter a comment

Click on "Execute Script" after you selected the desired AD accounts. Enter a comment for documentation.

8.5.8 Executing scripts for directories in bulk

Background / Value

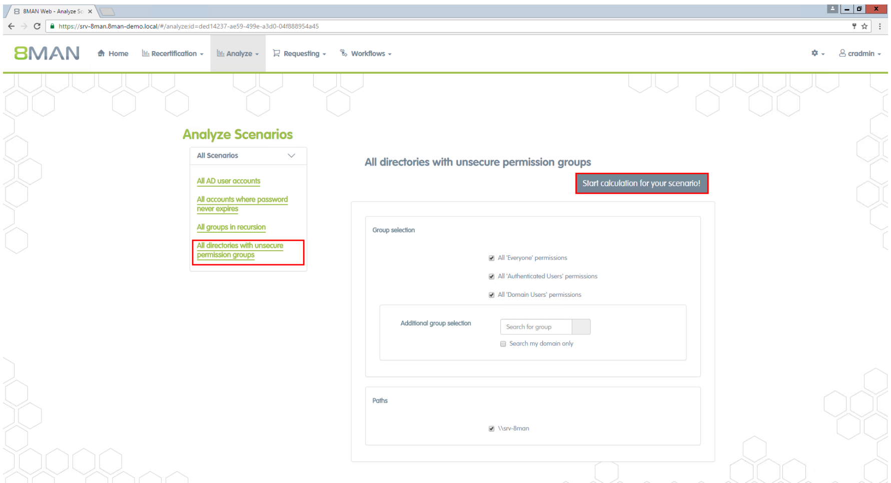
8MATE Analyze & Act allows you to use your own scripts. Just store them in the following directory and you can access them via the 8MAN Web interface.

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

Additional Services

Executing scripts on user accounts in bulk

Step by step process


8MAN Web - Analyze Sc
https://srv-8man.8man-demo.local/#/analyze;id=ded14237-ae59-499e-a3d0-04f888954a45
8MAN
Home
Recertification
Analyze
Requesting
Workflows
cradmin
Analyze Scenarios
All Scenarios
All AD user accounts
All accounts where password never expires
All groups in recursion
All directories with unsecure permission groups
Start calculation for your scenario!
Search for group

All directories with unsecure permission groups

Group selection

☑ All 'Everyone' permissions

☑ All 'Authenticated Users' permissions

☑ All 'Domain Users' permissions

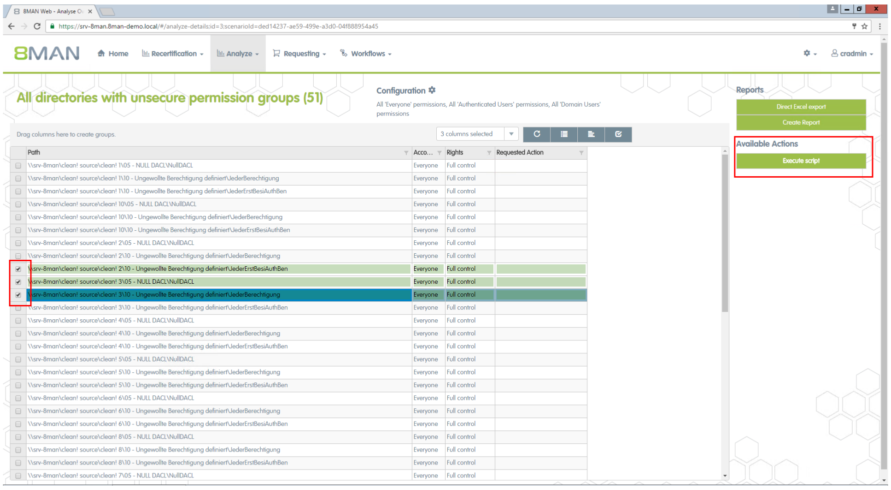
Additional group selection

□ Search my domain only

Paths

☑ \\srv-8man

Click on "All directories with unsecure permission groups". Choose from the parameters on the right and click on "Start Calculation".



All directories with unsecure permission groups (51)

Configuration

All 'Everyone' permissions, All 'Authenticated Users' permissions, All 'Domain Users' permissions

	Path	Acco...	Rights	Requested Action
□	\\srv-8man\clean! source\clean! 1\05 - NULL DACL\NullDACL	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 10\05 - NULL DACL\NullDACL	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 2\05 - NULL DACL\NullDACL	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
☑	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	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\JederBerechtigung	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 4\05 - NULL DACL\NullDACL	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 4\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 4\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 5\05 - NULL DACL\NullDACL	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 5\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 5\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 6\05 - NULL DACL\NullDACL	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 6\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 6\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 8\05 - NULL DACL\NullDACL	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 8\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 8\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
□	\\srv-8man\clean! source\clean! 7\05 - NULL DACL\NullDACL	Everyone	Full control	

Choose the directories you want to use for your script. Click on "Execute Script" and enter your script and comment in the next dialogue.

8.5.9 Removing direct permissions in bulk

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.

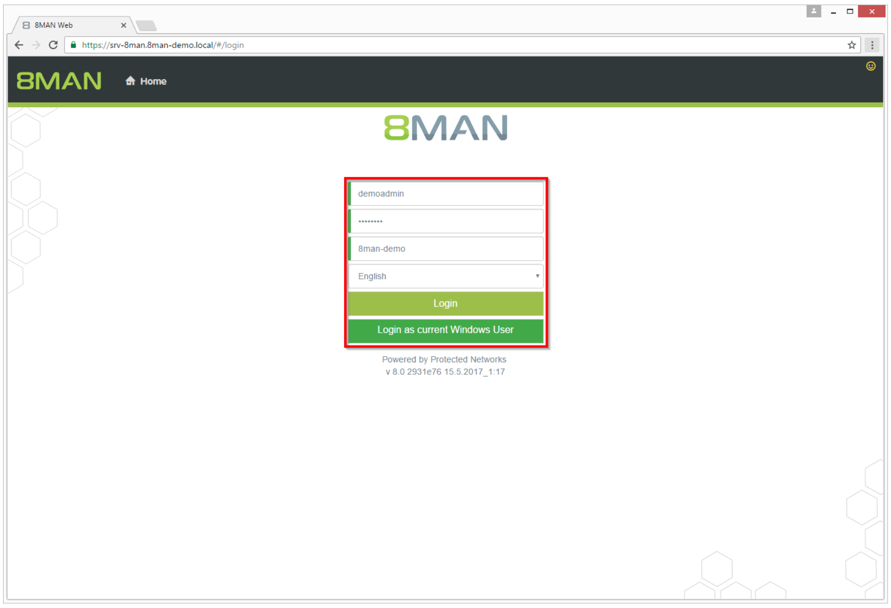
Additional Services

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

Changing password options in bulk

Removing unresolved SIDs in bulk

Step by step process


8MAN Web
https://srv-8man.8man-demo.local/#/login
8MAN
Home
8MAN

demoadmin

••••••••

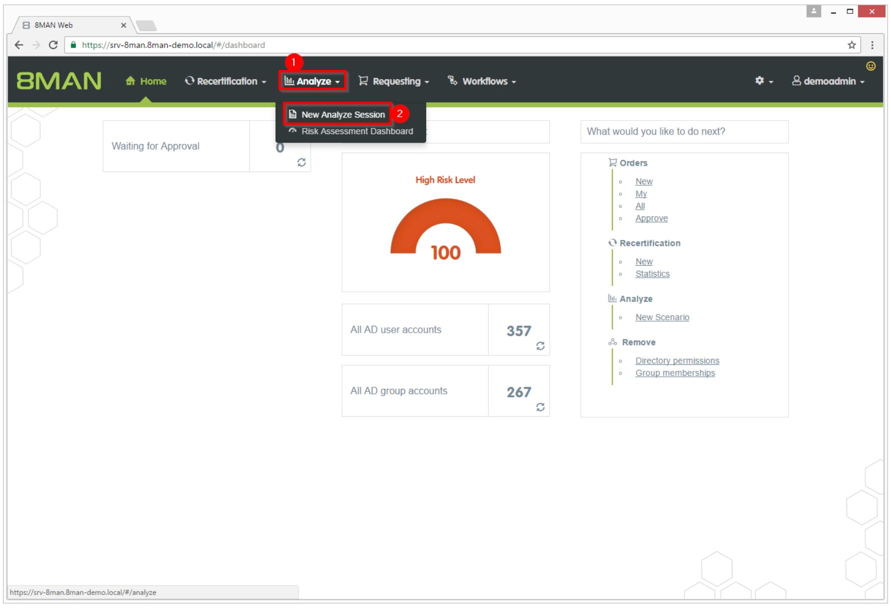
8man-demo

English

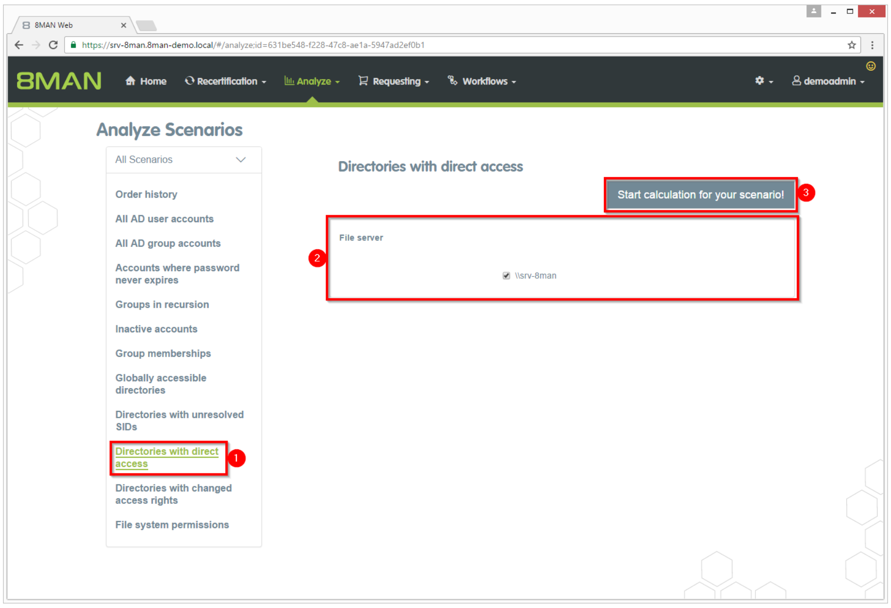
Login
Login as current Windows User

Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

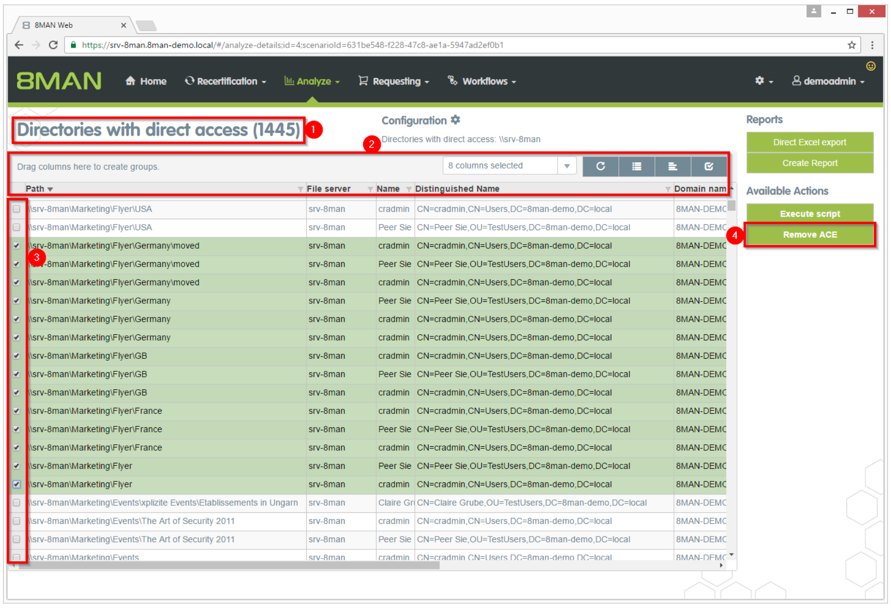
1. Login to the web client.



1. Click "Analyze".
2. Click "New Analyze Session".


8MAN Web
https://srv-8man.8man-demo.local/#/analyze:id=631be548-f228-47c8-ae1a-5947ad2ef0b1
8MAN
Home
Recertification
Analyze
Requesting
Workflows
demoadmin
Analyze Scenarios
All Scenarios
Order history
All AD user accounts
All AD group accounts
Accounts where password never expires
Groups in recursion
Inactive accounts
Group memberships
Globally accessible directories
Directories with unresolved SIDs
Directories with direct access
1
Directories with changed access rights
File system permissions
Directories with direct access
Start calculation for your scenario!
3
File server
2
☑ \\srv-8man

1. Click "Directories with direct access".
2. Select a file server.
3. Start the calculation.



Directories with direct access (1445)

Configuration

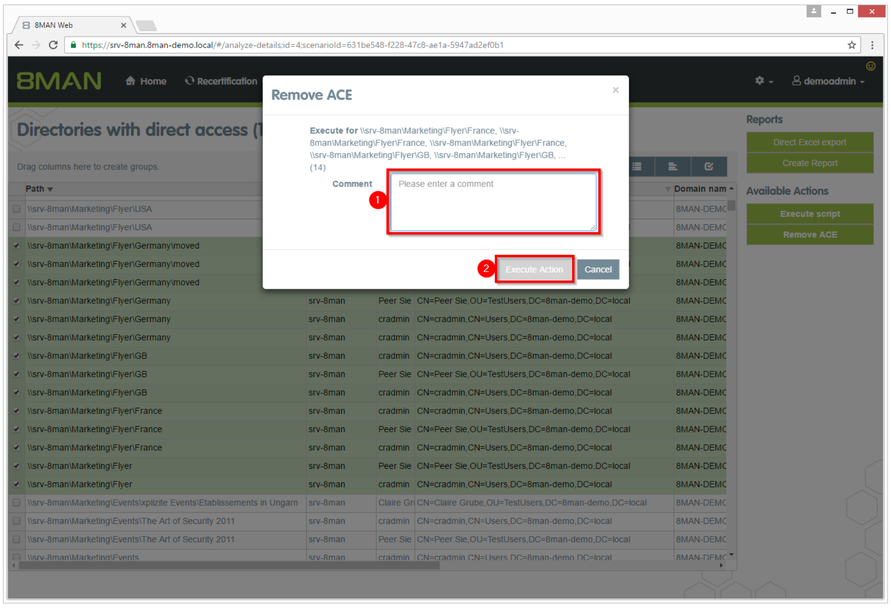
Directories with direct access: \\srv-8man

Drag columns here to create groups.

8 columns selected

	Path	File server	Name	Distinguished Name	Domain nam
□	\\srv-8man\Marketing\Flyer\USA	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
□	\\srv-8man\Marketing\Flyer\USA	srv-8man	Peer Sie	CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\Germany\moved	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\Germany\moved	srv-8man	Peer Sie	CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\Germany\moved	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\Germany	srv-8man	Peer Sie	CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\Germany	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\Germany	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\GB	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\GB	srv-8man	Peer Sie	CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\GB	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\France	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\France	srv-8man	Peer Sie	CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer\France	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer	srv-8man	Peer Sie	CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
☑	\\srv-8man\Marketing\Flyer	srv-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 Gr	CN=Claire Grube,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
□	\\srv-8man\Marketing\Events\The Art of Security 2011	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC
□	\\srv-8man\Marketing\Events\The Art of Security 2011	srv-8man	Peer Sie	CN=Peer Sie,OU=TestUsers,DC=8man-demo,DC=local	8MAN-DEMC
□	\\srv-8man\Marketing\Events	srv-8man	cradmin	CN=cradmin,CN=Users,DC=8man-demo,DC=local	8MAN-DEMC

1. 8MAN lists all direct permissions.
2. Use sorting, filtering, grouping and column selection to locate the desired rows.
3. Select the desired entries.
4. Click "Remove ACE".



Remove ACE

Execute for \\srv-8man\Marketing\Flyer\France, \\srv-8man\Marketing\Flyer\France, \\srv-8man\Marketing\Flyer\France, \\srv-8man\Marketing\Flyer\GB, \\srv-8man\Marketing\Flyer\GB, ... (14)

Comment: Please enter a comment

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".

8.5.10 Removing group memberships in bulk

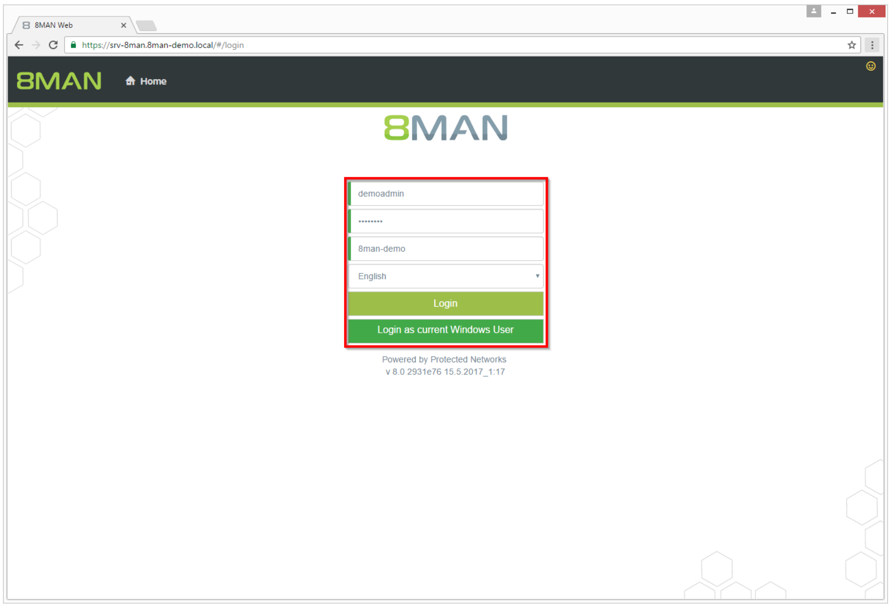
Background / Value

Remove lots of group memberships fast using the web client.

Additional Services

Managing group memberships (using the rich client)

Step by step process


8MAN Web
https://srv-8man.8man-demo.local/#/login
8MAN
Home
8MAN

demoadmin

••••••••

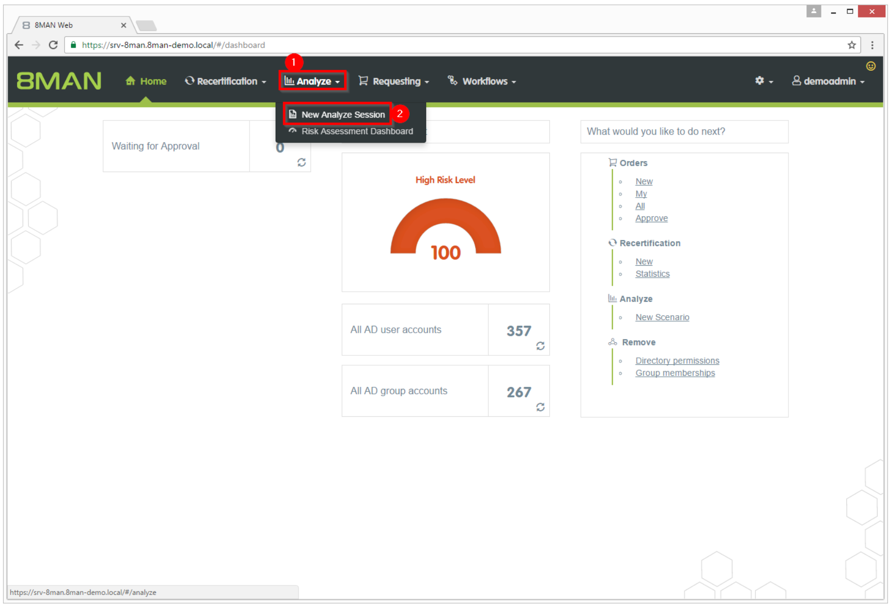
8man-demo

English

Login
Login as current Windows User

Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

1. *Login to the web client.*



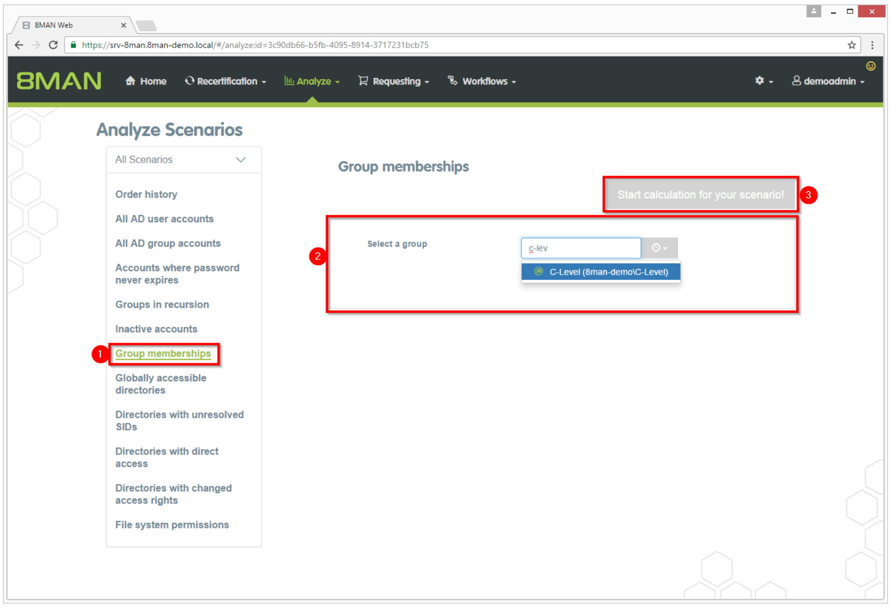
Waiting for Approval 0

High Risk Level 100

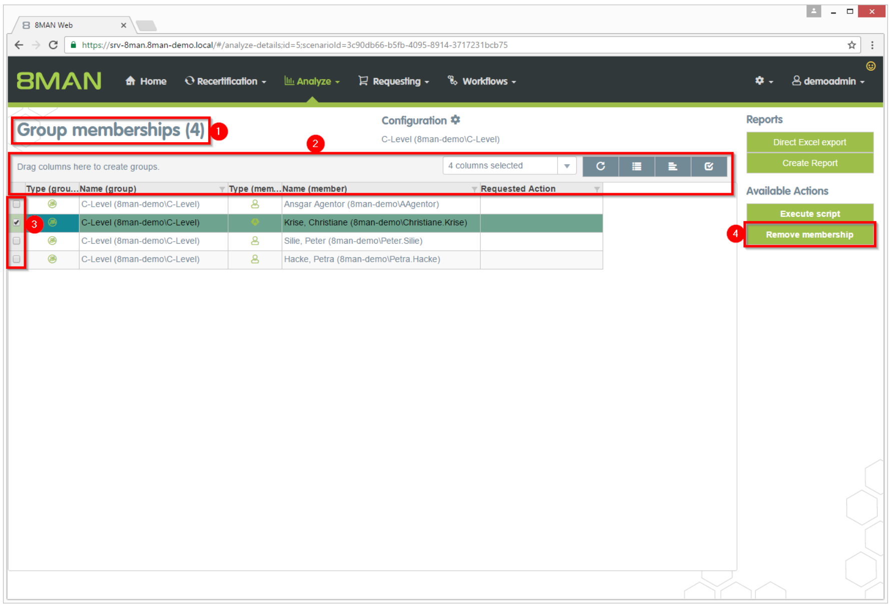
All AD user accounts 357

All AD group accounts 267

1. *Click "Analyze".*
2. *Click "New Analyze Session".*

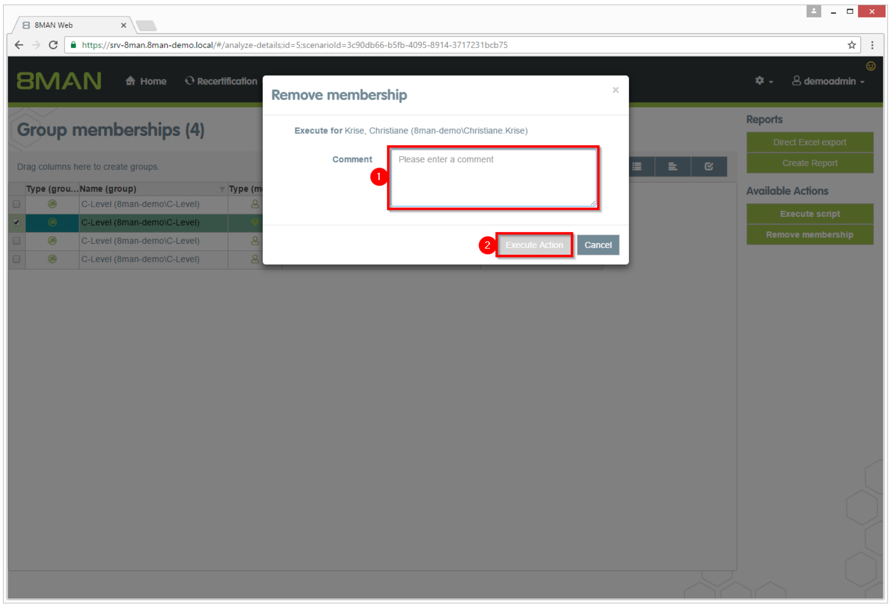

8MAN Web
https://srv-8man.8man-demo.local/#/analyze:id=3c90db66-b5fb-4095-8914-3717231bcb75
8MAN
Home
Recertification
Analyze
Requesting
Workflows
demoadmin
Analyze Scenarios
All Scenarios
Order history
All AD user accounts
All AD group accounts
Accounts where password never expires
Groups in recursion
Inactive accounts
Group memberships
Globally accessible directories
Directories with unresolved SIDs
Directories with direct access
Directories with changed access rights
File system permissions
Group memberships
Start calculation for your scenario!
Select a group
c-lev
C-Level (8man-demo\C-Level)
1
2
3

1. Click "Group memberships".
2. Find a group.
3. Start the calculation.



	Type (grou...	Name (group)	Type (mem...	Name (member)	Requested Action
□		C-Level (8man-demo\C-Level)		Ansgar Agentor (8man-demo\AAgentor)	
☑		C-Level (8man-demo\C-Level)		Krise, Christiane (8man-demo\Christiane.Krise)	
□		C-Level (8man-demo\C-Level)		Sille, Peter (8man-demo\Peter.Sille)	
□		C-Level (8man-demo\C-Level)		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".



Remove membership

Execute for Krise, Christiane (8man-demo\Christiane.Krise)

Comment: Please enter a comment

8MAN Web
https://srv-8man.8man-demo.local/#/analyze-details;id=5;scenarioId=3c90db66-b5fb-4095-8914-3717231bcb75
8MAN
Home
Recertification
demoadmin
Group memberships (4)
Drag columns here to create groups.
Type (grou...
Name (group)
Type (m
C-Level (8man-demo\C-Level)
C-Level (8man-demo\C-Level)
C-Level (8man-demo\C-Level)
C-Level (8man-demo\C-Level)
1
2
Execute Action
Cancel
Reports
Direct Excel export
Create Report
Available Actions
Execute script
Remove membership

1. *Leave a comment.*
2. *Click "Execute Action".*

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

8.5.11 Removing permissions from globally accessible directories in bulk

Background / Value

If "Everyone accounts" are used for the assignment of access rights, (almost) everyone has access to the connected resources. The consequence is an excessive assignment of access rights and a high probability for unauthorized access. These go against the principle of least privilege and should therefore not be used. Before deleting permissions you should assign specific groups to the appropriate resources.

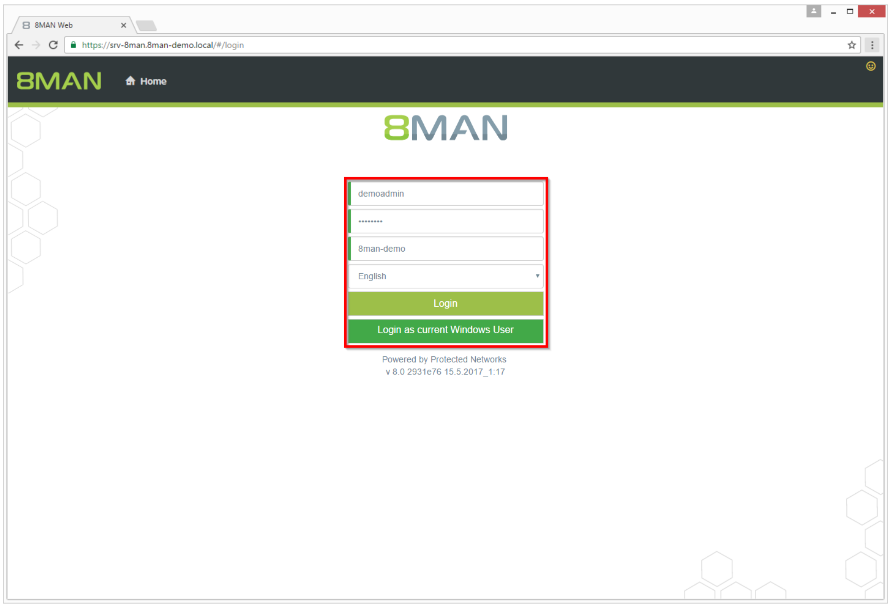
"Everyone accounts" are:

- Everyone
- Authenticated Users
- Domain-Users

Additional Services

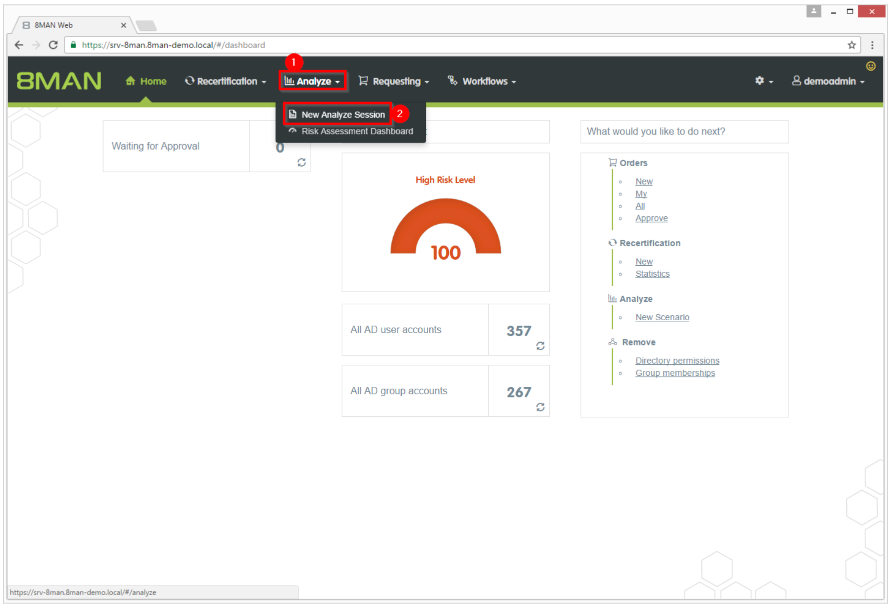
Report: Identifying usage of "Everyone" (using the rich client)
Report: Identifying usage of "Authenticated Users" (using the rich client)

Step by step process

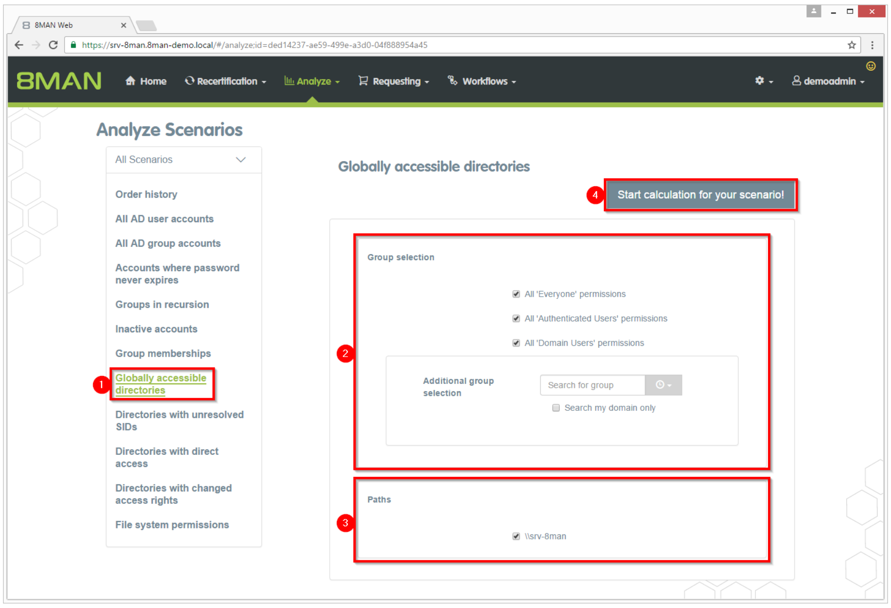

8MAN Web
https://srv-8man.8man-demo.local/#/login
8MAN
Home
8MAN
Login
Login as current Windows User
Powered by Protected Networks
v 8.0 2931e76 15.5.2017_1:17

demoadmin
••••••••
8man-demo
English

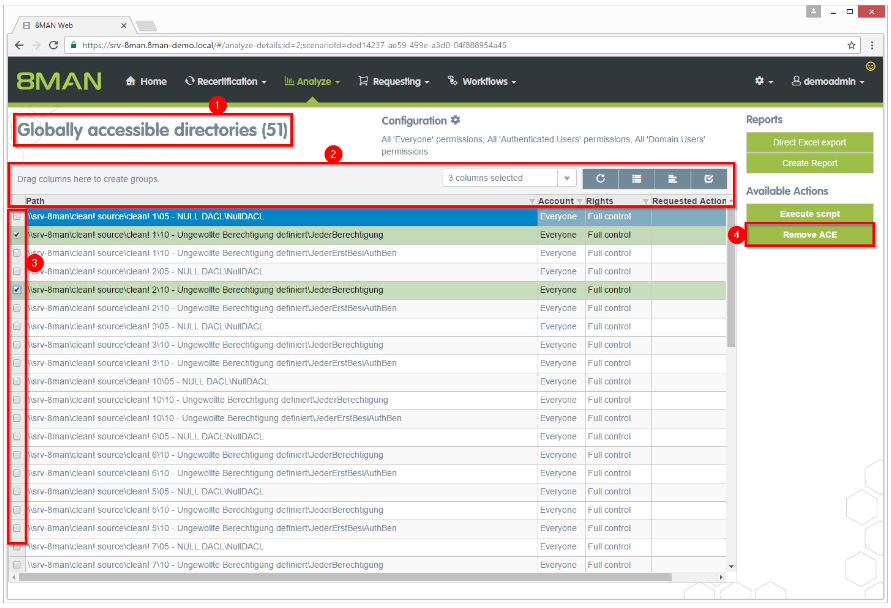
1. *Login to the web client.*



1. Click "Analyze".
2. Click "New Analyze Session".


8MAN Web
https://srv-8man.8man-demo.local/#/analyze:id=ded14237-ae59-499e-a3d0-04f888954a45
8MAN
Home
Recertification
Analyze
Requesting
Workflows
demoadmin
Analyze Scenarios
All Scenarios
Order history
All AD user accounts
All AD group accounts
Accounts where password never expires
Groups in recursion
Inactive accounts
Group memberships
1
Globally accessible directories
Directories with unresolved SIDs
Directories with direct access
Directories with changed access rights
File system permissions
Globally accessible directories
4
Start calculation for your scenario!
Group selection
2
☑ All 'Everyone' permissions
☑ All 'Authenticated Users' permissions
☑ All 'Domain Users' permissions
Additional group selection
Search for group
☐ Search my domain only
Paths
3
☑ \\srv-8man

1. Click "Globally accessible directories".
2. Select groups.
   You can add one additional group. This is very useful for "catch-all" groups, e.g. "mycompany-complete".
3. Select a file server.
4. Start the calculation.



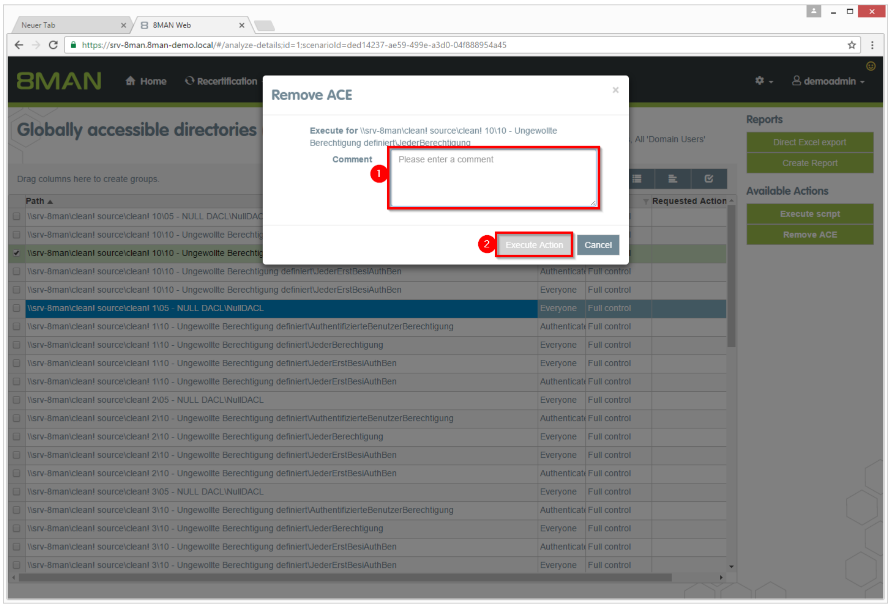
Globally accessible directories (51)

Configuration

All 'Everyone' permissions, All 'Authenticated Users' permissions, All 'Domain Users' permissions

	Path	Account	Rights	Requested Action
☐	\\srv-8man\clean! source\clean! 1\05 - NULL DACL\NullDACL	Everyone	Full control	
☑	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 2\05 - NULL DACL\NullDACL	Everyone	Full control	
☑	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	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\JederBerechtigung	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 10\05 - NULL DACL\NullDACL	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 6\05 - NULL DACL\NullDACL	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 6\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 6\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 5\05 - NULL DACL\NullDACL	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 5\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 5\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 7\05 - NULL DACL\NullDACL	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 7\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	

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".*



Neuer Tab
8MAN Web
https://srv-8man.8man-demo.local/#/analyze-details;id=1;scenarioId=ded14237-ae59-499e-a3d0-04f888954a45
8MAN
Home
Recertification
demoadmin
Globally accessible directories
All 'Domain Users'
Reports
Direct Excel export
Create Report
Available Actions
Execute script
Remove ACE
Drag columns here to create groups.
1
2

Remove ACE

Execute for \\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederBerechtigung

Comment Please enter a comment

Execute Action | Cancel

	Path	Account	Rights	Requested Action
☐	\\srv-8man\clean! source\clean! 10\05 - NULL DACL\NullDAC			
☐	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtig			
☑	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtig			
☐	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Authenticate	Full control	
☐	\\srv-8man\clean! source\clean! 10\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 1\05 - NULL DACL\NullDACL	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\AuthentifizierteBenutzerBerechtigung	Authenticate	Full control	
☐	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 1\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Authenticate	Full control	
☐	\\srv-8man\clean! source\clean! 2\05 - NULL DACL\NullDACL	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\AuthentifizierteBenutzerBerechtigung	Authenticate	Full control	
☐	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 2\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Authenticate	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\AuthentifizierteBenutzerBerechtigung	Authenticate	Full control	
☐	\\srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung definiert\JederBerechtigung	Everyone	Full control	
☐	\\srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Authenticate	Full control	
☐	\\srv-8man\clean! source\clean! 3\10 - Ungewollte Berechtigung definiert\JederErstBesiAuthBen	Everyone	Full control	

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".

9. Threat & Gap Management

9.1 +8MATE Clean!

9.1.1 Identifying file path names that are too long

Background / Value

Placing files on directories whose path name exceeds 260 characters can cause all sorts of problems. Often 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 manually moving these files to the parent directory.

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.2 Archiving old file server data

Background / Value

Access Rights Management should also include archiving old, unused data, since the less data you have, the easier it is to manage. 8MATE Clean allows you to mark data as "old" based upon specified dates. The most commonly used indicator is the last read or write access.

You can decide if old data is moved to another storage system or remain in the old system when you are migrating to new file server systems.

Additional services

If you would like to archive old data we first recommend creating a protected area and storing your old data within.

8MATE Clean handbook: creating a protected area on a file server

8MATE Clean! is managed and operated by our experienced System Engineers.

Contact us for more information: info@8man.com

9.1.3 Pushing permissions to empty sub-directories through inheritance

Background / Value

Empty folders do not need different access rights than their parent directory. 8MATE Clean! removes these , by pushing inherited rights from parent to child folders. This prevents unneccessary load on Kerberos token size and harmonizes your overall access rights situation.

Additional services

8MATE Clean!handbook: Deleting empty directories on a file server

8MATE Clean! is managed and operated by our experienced System Engineers.

Contact us for more information: info@8man.com

9.1.4 Deleting empty directories on the file server

Background / Value

Empty folders can be automatically deleted. This cleans up the overall structure and prevents unnecessary load on The Kerberos token size.

Additional services

If you are not sure of empty folders have been created intentionally please use the following service:

8MATE Clean! handbook: Pushing permissions to empty subdirectories through inheritance

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.5 Correcting non-canonical access rights

Background / Value

Access control entries (ACEs) have a particular order in the DACL depending on their type. Specifically ACEs that deny access are listed before ACEs that grant access. The order of ACEs significantly determines the effective access rights of the user. You may encounter security risks, because applications and programs can not be prevented from writing ACEs in a random order. 8MATE Clean! repairs non-canonical permissions and ensures that standards are reapplied.

Additional services

8MATE Clean! Handbuch: Replacing non-canonical permissions through overarching rights

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.6 Replacing non-canonical permissions through overarching rights

Background / Value

Access control entries (ACEs) have a particular order in the DACL depending on their type. Specifically ACEs that deny access are listed before ACEs that grant access. The order of ACEs significantly determines the effective access rights of the user. You may encounter security risks, because applications and programs can not be prevented from writing ACEs in a random order. 8MATE Clean repairs non-canonical permissions and ensures that standards are reapplied.

Alternative service:

If you would like to ensure that permission differences remain between parent and child directory, please use the following service:

8MATE Clean! handbook: correcting non-canonical permissions

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.7 Automatically replacing critical access rights

Background / Value:

There are a number of groups and accounts in the DACL that should not receive permissions under any circumstances. These include the EVERYONE or CREATOR/OWNER accounts. These critical accounts, as well as special Windows accounts are listed in the 8MAN blacklist and can not be granted permissions with 8MAN.

If critical access rights have been granted without 8MAN, then 8MATE Clean! can automatically replace these for you. You can define which groups and direct permissions are replaced by which access rights and 8MATE Clean! will implement your requirements.

Alternative services

8MATE Clean! handbook:Removing critical access rights automatically

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.8 Identifying zero DACLs and replacing them with higher level permissions

Background / Value

The security descriptor may contain the value "0" for directories. In this case anyone could give themselves access to a directory and its subfolders. Zero DACLs are created through faulty applications that manipulate ACLs.

8MATE Clean! replaces zero DACLs with higher level permissions.

Please note: Zero DACLs can not be replaced on NetAPP or EMC2 servers. These are present by default.

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.9 Replacing divergent access rights on a file server

Background / Value

Microsoft allows a variety of access categories. "Special rights" in particular often unnecessarily complicate access rights assignments through their granularity and variety of combinations. Protected Networks GmbH recommends working only with 3 access rights:

- Full control
- Modify
- Read & execute

8MATE Clean! allows you to change your access rights structure automatically and according to your specifications. This significantly simplifies access management on your file servers.

Additional services

You can change the conventions for creating new permissions to match your ideal standard.

Installations & configuration manual: Selecting the access categories available in 8MAN

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.10 Deleting divergent access rights

Background / Value

Microsoft allows a variety of access categories. "Special rights" in particular often unnecessarily complicate access rights assignments through their granularity and variety of combinations. Protected Networks GmbH recommends working only with 3 access rights:

- Full control
- Modify
- Read & execute

8MATE Clean! allows you to delete all undesired access rights. This way any users that had access to the affected directories only through this permission path, will lose their access rights.

Additional services

8MATE Clean! allows you to modify existing access rights to match your ideal standard.

8MATE Clean! handbook: Replacing divergent access rights

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.11 Automatically removing critical permissions

Background / Value

There are a number of groups and accounts in the DACL that should not be granted permissions. These include the EVERYONE and CREATOR/OWNER accounts. These critical accounts, as well as special Windows accounts are listed in the 8MAN blacklist and can not be granted permissions with 8MAN.

If critical access rights have been granted without 8MAN, then 8MATE Clean!

Alternative Services

8MATE Clean! handbook: Automatically replacing critical access rights

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.12 Deleting 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

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.13 Replacing 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

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.14 Activating inheritance for directories with identical access rights

Background / Value:

Sometimes directories have identical access rights within the same tree, but inheritance is still deactivated. 8MATE Clean! identifies these directories and activates inheritance. This simplifies access management as access rights that are granted later to the parent directory are automatically inherited by sub-directories.

Additional services:

We recommend the following service in order to further reduce Kerberos token load:

8MATE Clean! Handbook: Deleting empty folders on file servers

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.15 Removing permission gaps by aligning directory owners

Background / Value

According to Microsoft best practice administrators should be directory owners. If this is not the case, then the directory owner is automatically granted full access. This access right should be reserved for administrators. 8MATE Clean! ensures all directories have administrators as their owners.

8MATE Clean! is managed and operated by our experienced System Engineers.
Contact us for more information: info@8man.com

9.1.16 Automatically reducing the depth of permissions on file servers

Background / Value

The maximum depth of permissions is defined in 8MAN configuration from the share level on. Any divergent permissions are considered as "too deep" by 8MAN.

8MATE Clean! replaces divergent permissions beyond the defined maximum with the permissions of higher level folders.

It makes sense to harmonize permissions beyond a certain depth as this limits the complexity of directory management and reduces overall IT effort.

8MATE Clean! is managed and operated by our experienced System Engineers.

Contact us for more information: info@8man.com

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 Für Data Owner und Administratoren

10.1.2.1 Accept or reject an inquiery in Matrix 42

Please contact knowledge management for more information.

KM@8MAN.com

11. Appendix

11.1 Software license acknowledgments

- Json.net, © 2006-2014 Microsoft, https://json.codeplex.com/license
- JSON.NET Copyright (c) 2007 James Newton-King https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md
- Irony Copyright (c) 2011 Roman Ivantsov http://irony.codeplex.com/license
- Jint Copyright (c) 2011 Sebastien Ros http://jint.codeplex.com/license
- #ziplib 0.85.5.452, © 2001-2012 IC#Code, http://www.icsharpcode.net/opensource/sharpziplib/
- PDFsharp 1.33.2882.0, © 2005-2012 empira Software GmbH, Troisdorf (Germany), http://www.pdfsharp.net/PDFsharp_License.ashx
- JetBrains Annotations, ©2007-2012 JetBrains, http://www.apache.org/licenses/LICENSE-2.0
- Microsoft Windows Driver Development Kit, © Microsoft, EULA, installed on the computer on which the FS Logga for Windows file servers is installed: C:\Program Files\protected-networks.com\8MAN\driver (Usage only for FS Logga for Windows file server)
- NetApp Manageability SDK, © 2013 NetApp, https://communities.netapp.com/docs/DOC-1152 (Usage only for FS Logga for NetApp Fileserver)
- WPF Shell Integration Library 3.0.50506.1, © 2008 Microsoft Corporation , http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx
- WPF Toolkit Library 3.5.50211.1, © Microsoft 2006-2013, http://wpf.codeplex.com/license
- Bootstrap, © 2011-2016 Twitter, Inc, https://github.com/twbs/bootstrap/blob/master/LICENSE
- jQuery, © 2016 The jQuery Foundation, https://jquery.org/license
- jquery.cookie, © 2014 Klaus Hartl, https://github.com/carhartl/jquery-cookie/blob/master/MIT-LICENSE.txt
- jquery-tablesort, © 2013 Kyle Fox, https://github.com/kylefox/jquery-tablesort/blob/master/LICENSE
- LoadingDots, © 2011 John Nelson, http://johncoder.com
- easyModal.js, © 2012 Flavius Matis, https://github.com/flaviusmatis/easyModal.js/blob/master/LICENSE.txt
- jsTimezoneDetect, © 2012 Jon Nylander https://bitbucket.org/pellepim/jstimezonedetect/src/f9e3e30e1e1f53dd27cd0f73eb51a7e7caf7b378/LICENCE.txt?at=defaultjquery-tablesort
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE
- Mustache.js, © 2009 Chris Wanstrath (Ruby), © 2010-2014 Jan Lehnardt (JavaScript) and © 2010-2015 The mustache.js community https://github.com/janl/mustache.js/blob/master/LICENSE
- Metro UI CSS 2.0, © 2012-2013 Sergey Pimenov, https://github.com/olton/Metro-UI-CSS/blob/master/LICENSE
- Underscore.js, © 2009-2016 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors https://github.com/jashkenas/underscore/blob/master/LICENSE
- Ractive.js, © 2012-15 Rich Harris and contributors, https://github.com/ractivejs/ractive/blob/dev/LICENSE.md

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