8MAN

Access Rights Management. Only much Smarter.

Access Rights Management

Release Notes

Version 8.0

Protected Networks

1 Innovations according to product groups

8.0	8MAN Visor	8MAN Visor DO	8MAN Enterprise
Comprehensive changes			
New colors for better contrast and visibility for all UIs	✓	✓	✓
Permission Analysis			
Risk Assessment Dashboard - central overview of risks	8MATE Analyze & Act	8MATE Analyze & Act	8MATE Analyze & Act
Documentation & Reporting			
8MATE Analyze & Act: new scenarios and flexible reports	8MATE Analyze & Act	8MATE Analyze & Act	8MATE Analyze & Act
Security Monitoring			
Scheduling and filtering FS Logga reports	8MATE FS Logga	8MATE FS Logga	8MATE FS Logga
8MATE FS Logga supports SSL for NetApp C-Mode	8MATE FS Logga	8MATE FS Logga	8MATE FS Logga
Role & Process Optimization			
Assigning resource owners using the web client, importing and exporting the configuration	✗	✗	8MATE GrantMA
Requesting directories using the self service portal	✗	✗	8MATE GrantMA
Single Sign On to the self service portal	✗	✗	8MATE GrantMA

8.0	8MAN Visor	8MAN Visor DO	8MAN Enterprise
User Provisioning			
8MATE Analyze & Act: new bulk operations	✗	✗	8MATE Analyze & Act
Executing scripts before and after changes	✗	✗	✓
Ressource Integration			
8MATE Sharepoint: executing changes in SharePoint 2016 & Online	8MATE SharePoint	8MATE SharePoint	8MATE SharePoint
Easy Connect:Importing access rights from additional resources	✓	✓	✓
8MAN Konfiguration			
New homepage layout and search	✓	✓	✓
Configuring scripts	✗	✗	✓
Configuring the SharePoint Remote Connector	8MATE SharePoint	8MATE SharePoint	8MATE SharePoint

2 Permission Analysis

2.1 Risk Assessment Dashboard - central overview of risks

Background / Value

Incorrect permissions and settings cause security risks. The new risk assessment dashboard visualizes the top risk factors with the highest impact on security. Start with an overall rating. Create a risk assessment report with one click. Drill down into deeper analyzes with one more click.

8MAN displays the following risk factors:

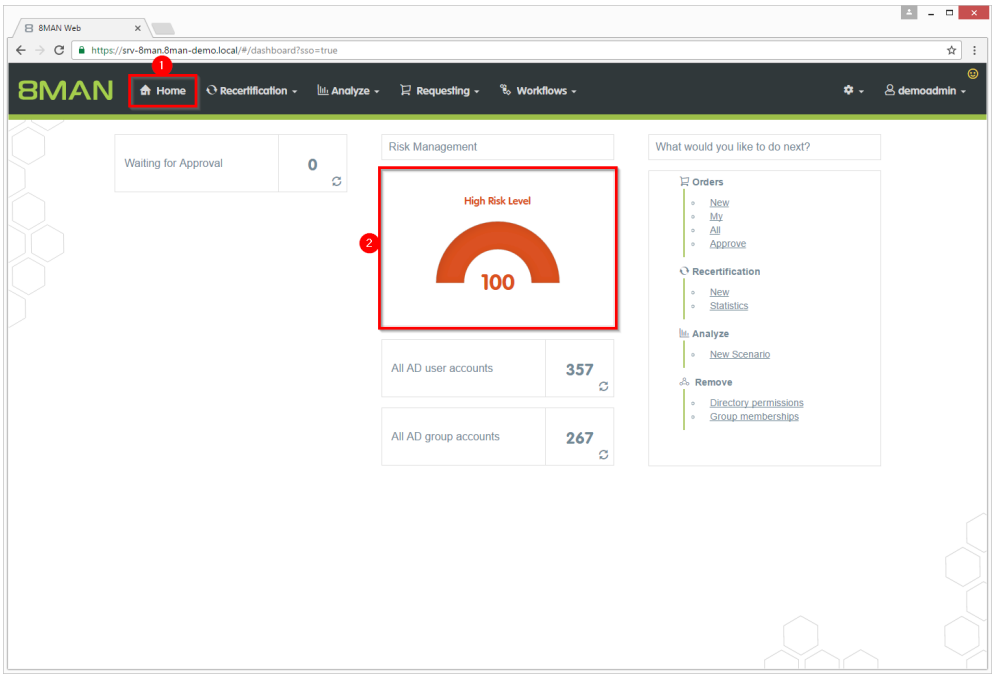
- inactive accounts
- groups in recursion
- accounts with never expiring passwords
- globally accessible directories
- directories with unresolved SIDs
- directories with direct permissions
- directories with differing access rights

Additional Services

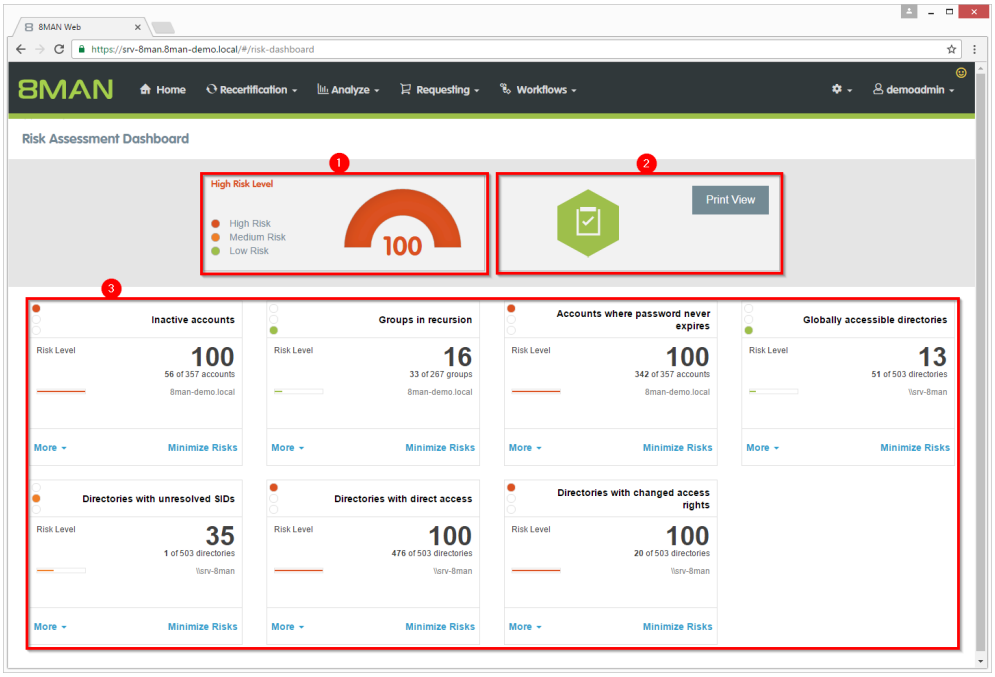
You can start a lot of analyzes, reports and actions from the risk assessment dashboard. The following table faces the web client services to similar rich client services.

8MAN Visor Editionen	
Rich Client	**Web Client (Analyze & Act)**
Report: inactive accounts	Identifying inactive accounts
identifying groups in recursion	Identifying groups in recursion
Report: identifying users with never expiring passwords	Identifying users with never expiring passwords
Report: identifying direct permissions	Identifying globally accessible directories
Report: identifying unresolved SIDs	Identifying unresolved SIDs
Report: everyone permissions	Identifying direct permissions
Report: authenticated users permissions	Identifying directories with differing permissions
8MAN Enterprise	
Rich Client	**Web Client (Analyze & Act)**
Resetting passwords	Resetting passwords in bulk
Removing a user and his permissions	Changing password options in bulk
Modifying users and groups attributes	Deactivating accounts in bulk
Unlocking an user	Deleting accounts in bulk (soft delete)
Deactivating an user	Removing group memberships in bulk
Changing password options of an user	Removing direct permissions in bulk
Modifying group memberships	Removing permissions from globally accessible directories in bulk
	Modifying attributes in bulk
	Removing unresolved SIDs in bulk
	Removing differing permissions in bulk
	Executing scripts on user accounts in bulk
	Executing scripts on directories in bulk

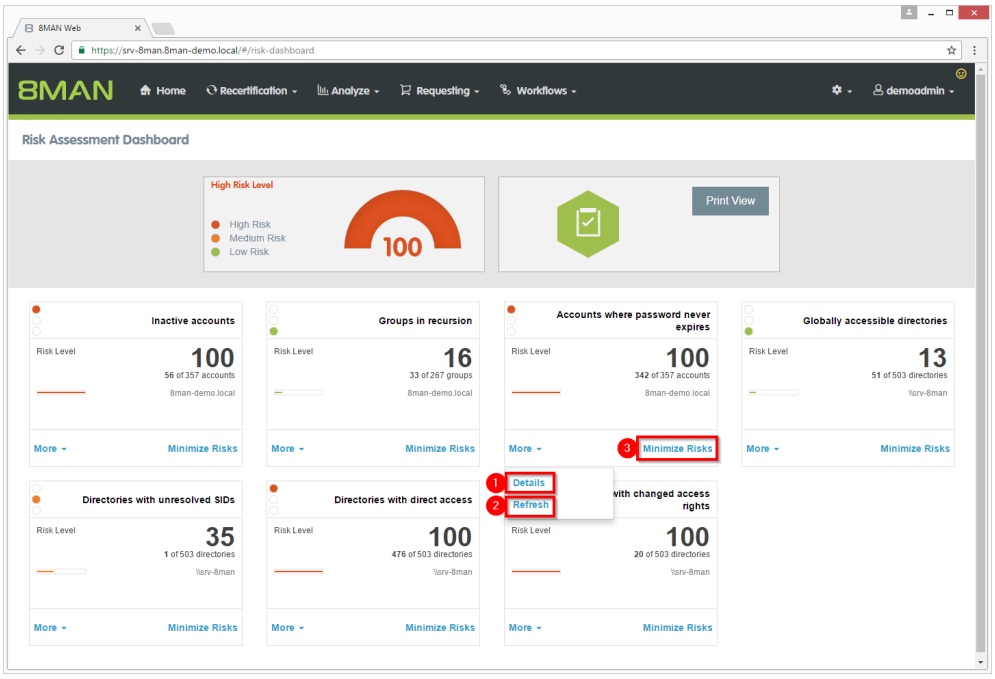
Step by step process



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



1. *8MAN shows an overall rating.*
2. *The print view offers an overview of all risk factors including explanations. Create a comprehensive risk assessment report with on click.*
3. *8MAN shows all risk factors with related ratings.*



1. *Get more details and explanations of the risk factor.*
2. *Recalculate the risk factor. This may take some time.*
3. *Start the scenario.*

2.1.1 Identifying inactive accounts using the web client

Background / Value

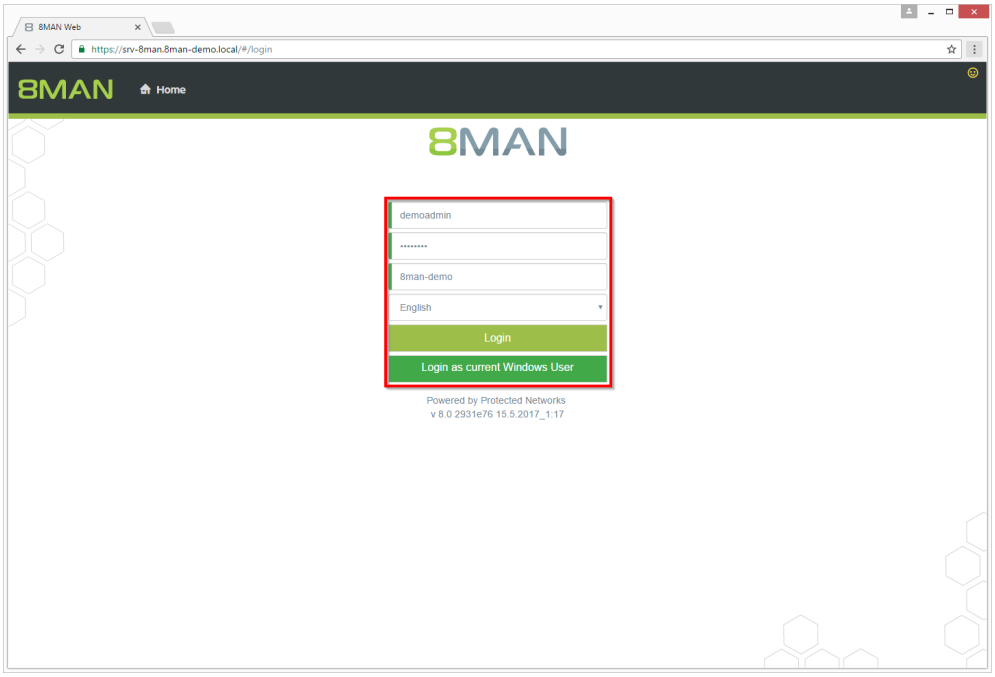
Inactive accounts can be used for data theft and manipulation without being detected. Since most inactive accounts are remnants of past employees, they are often a symptom of a communication problem between HR and IT. 8MAN displays all inactive accounts in Active Directory with a last logon older than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

Additional Services

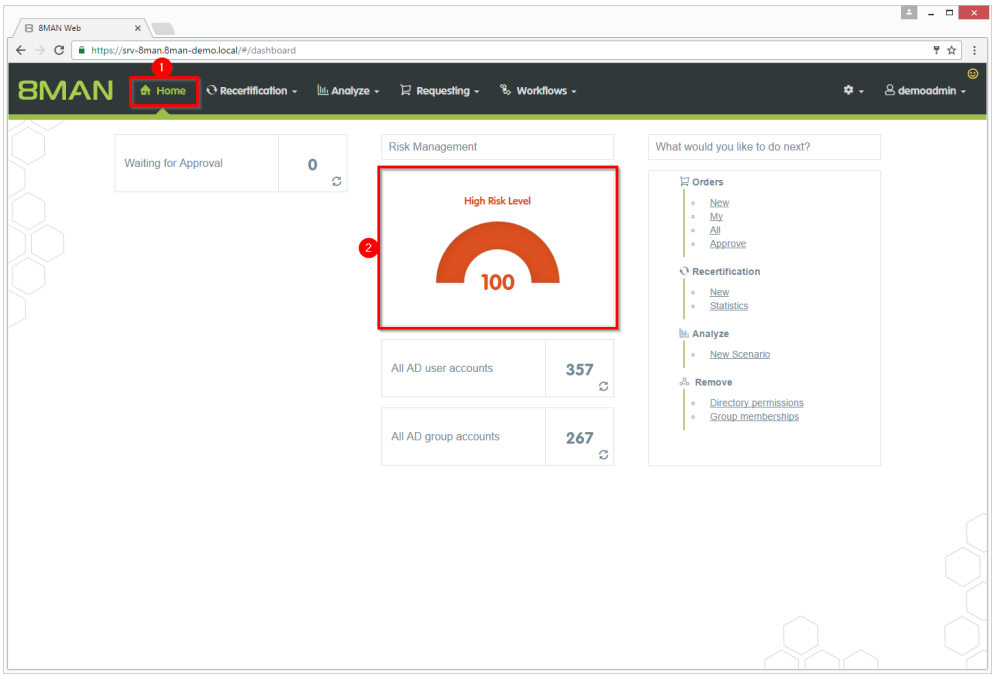
Report: inactive accounts

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

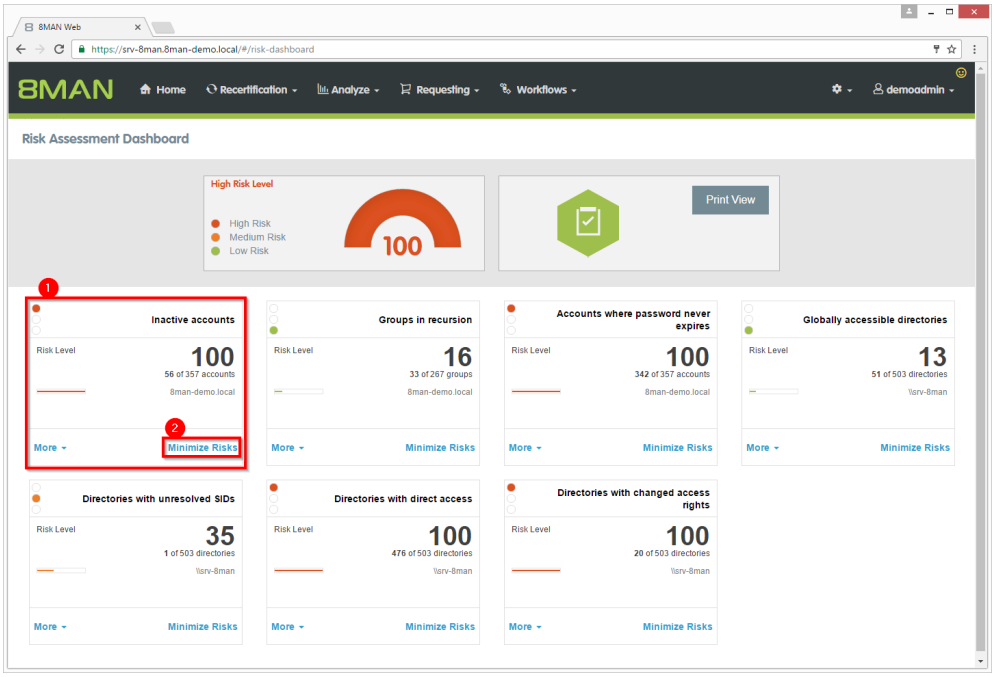
Step by step process



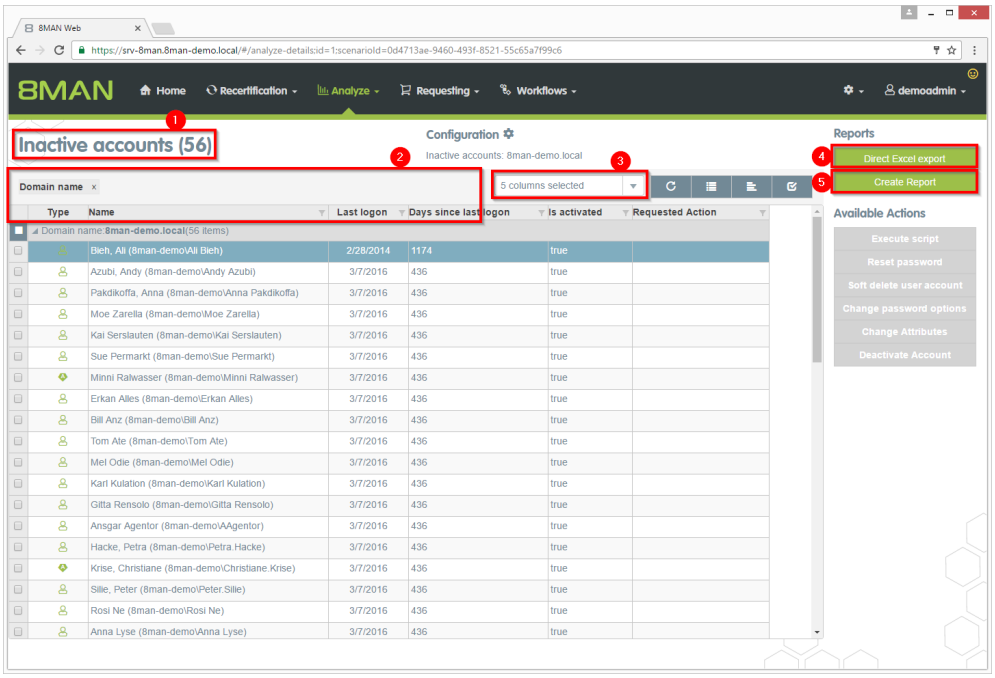
Login to the web client.



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 "Inactive accounts".*
2. *Click "Minimize risks".*



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.*

2.1.2 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.

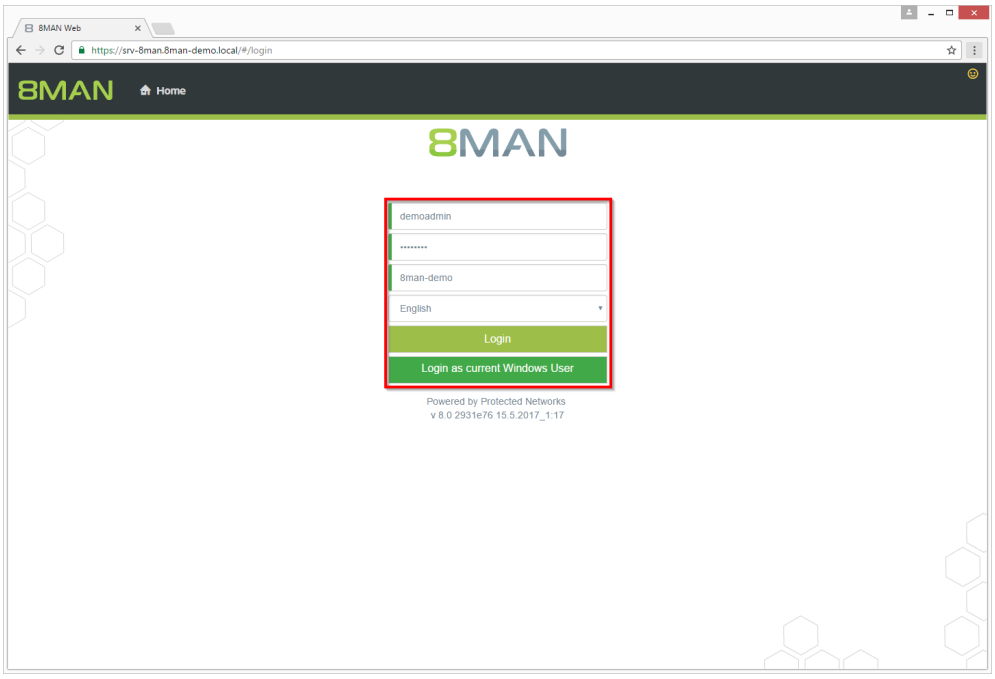
Additional Services

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.

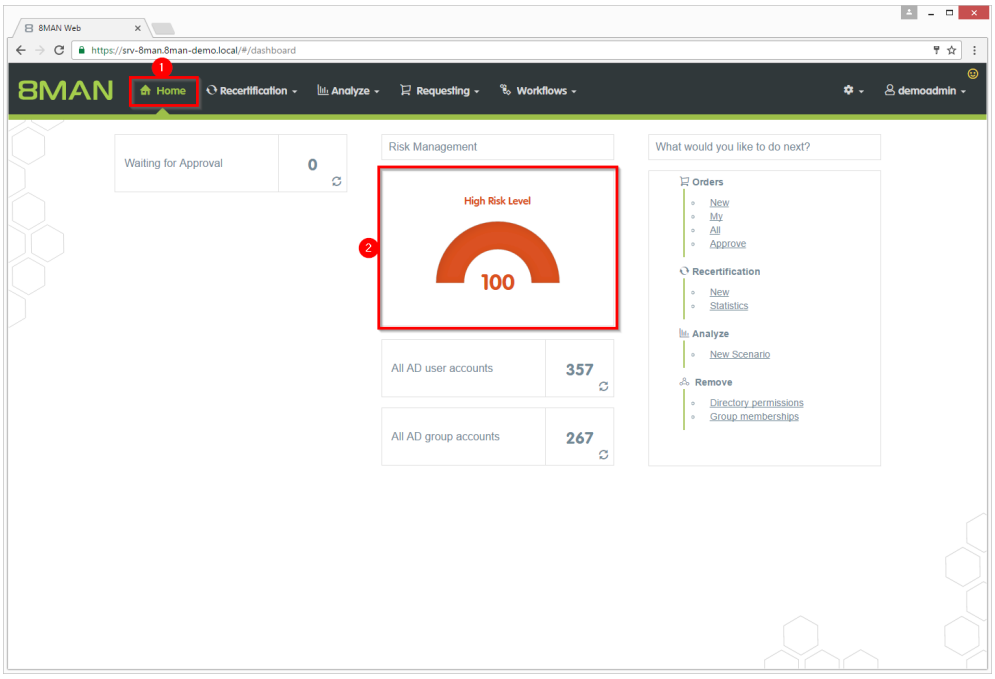
Idenitfying recursive groups (using the rich client)

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

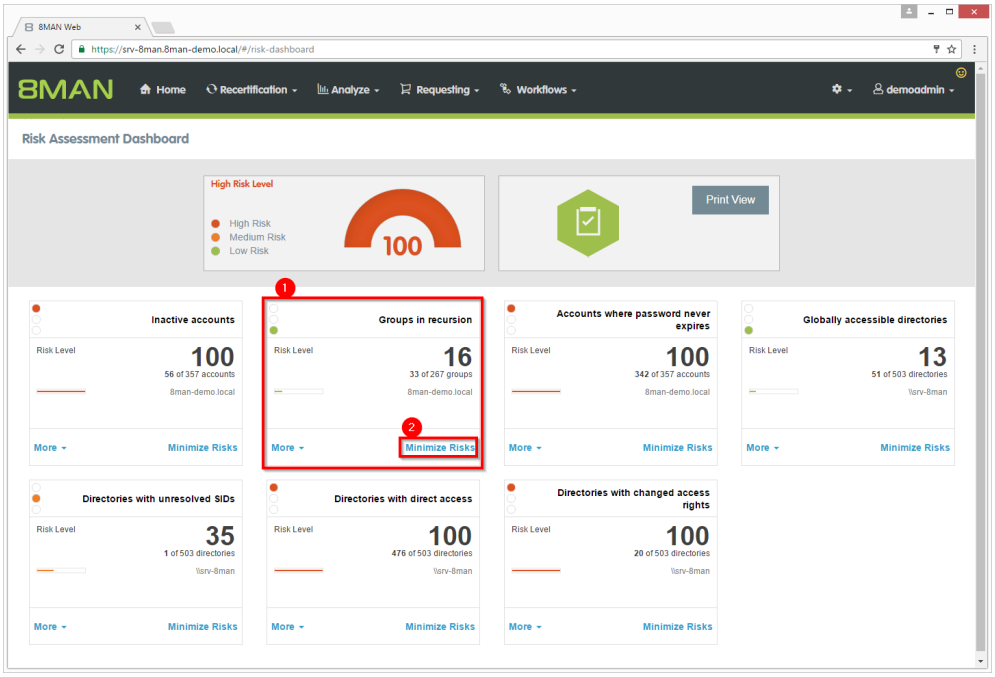
Step by step process



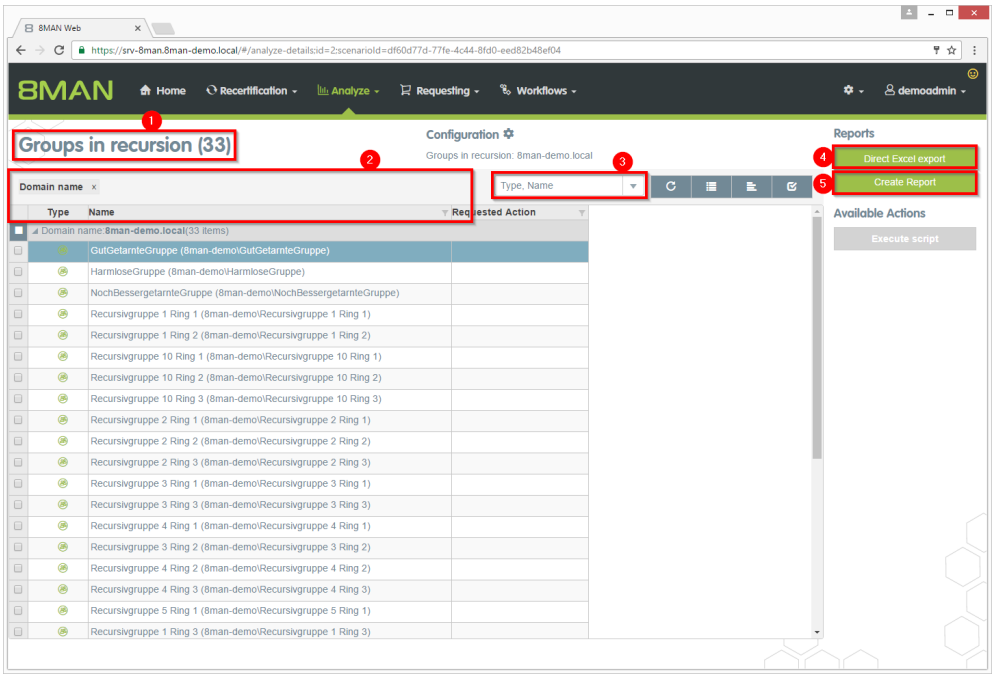
Login to the web client.



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".*



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.*

2.1.3 Identifying users with never expiring passwords using the web client

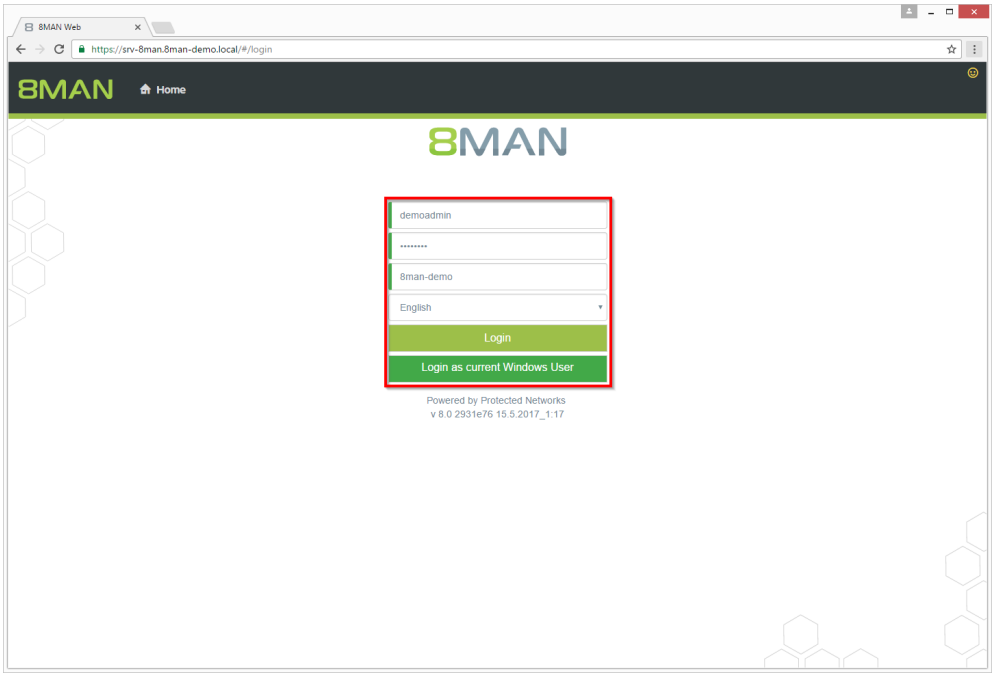
Background / Value

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.

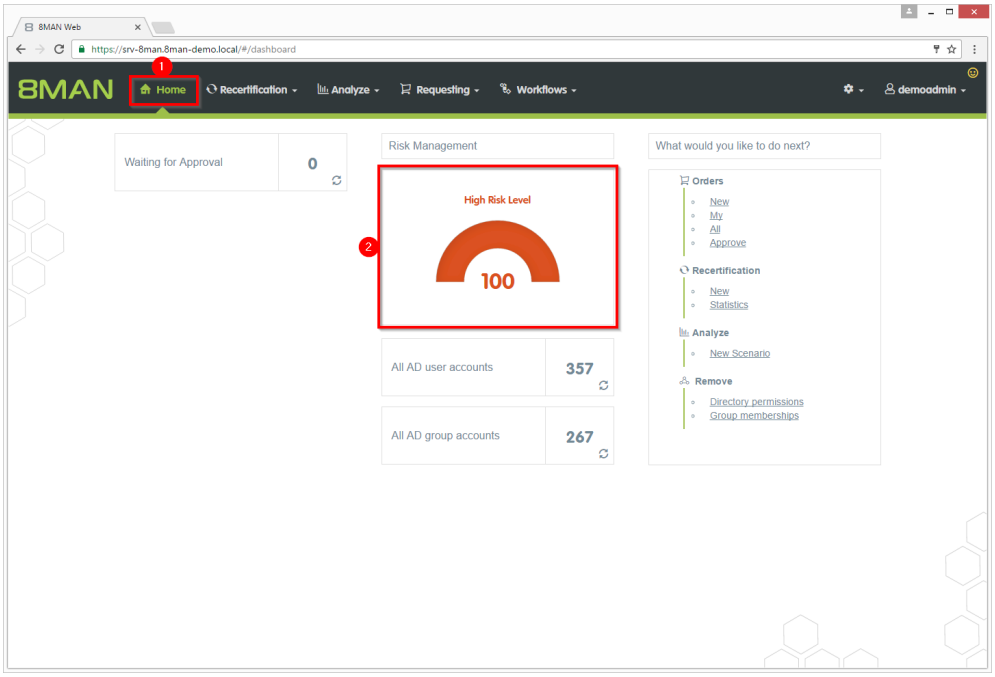
Additional Services

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

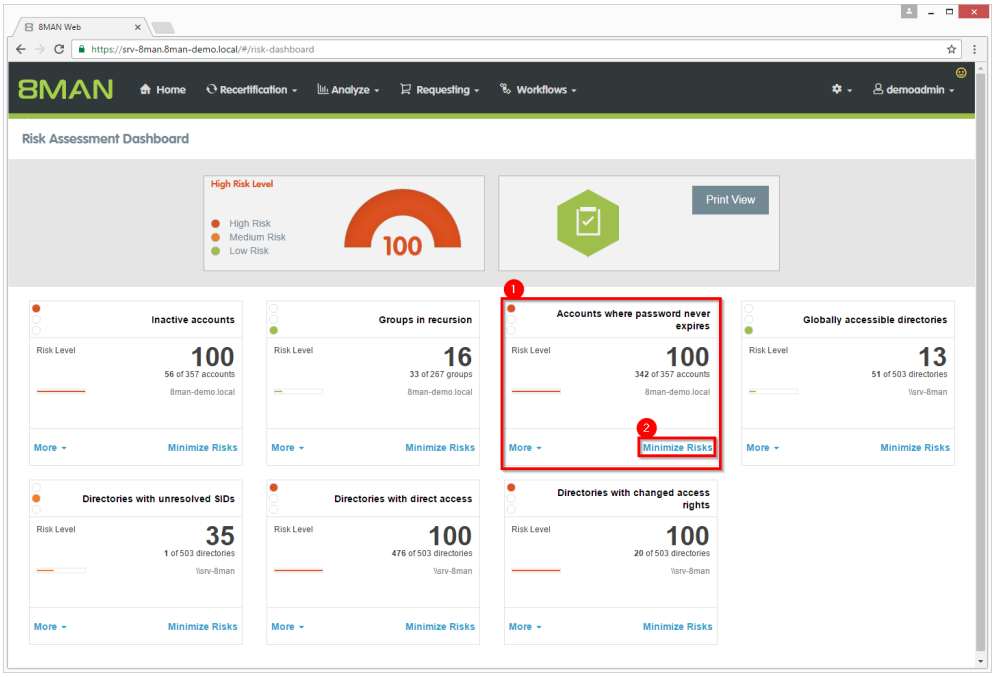
Step by step process



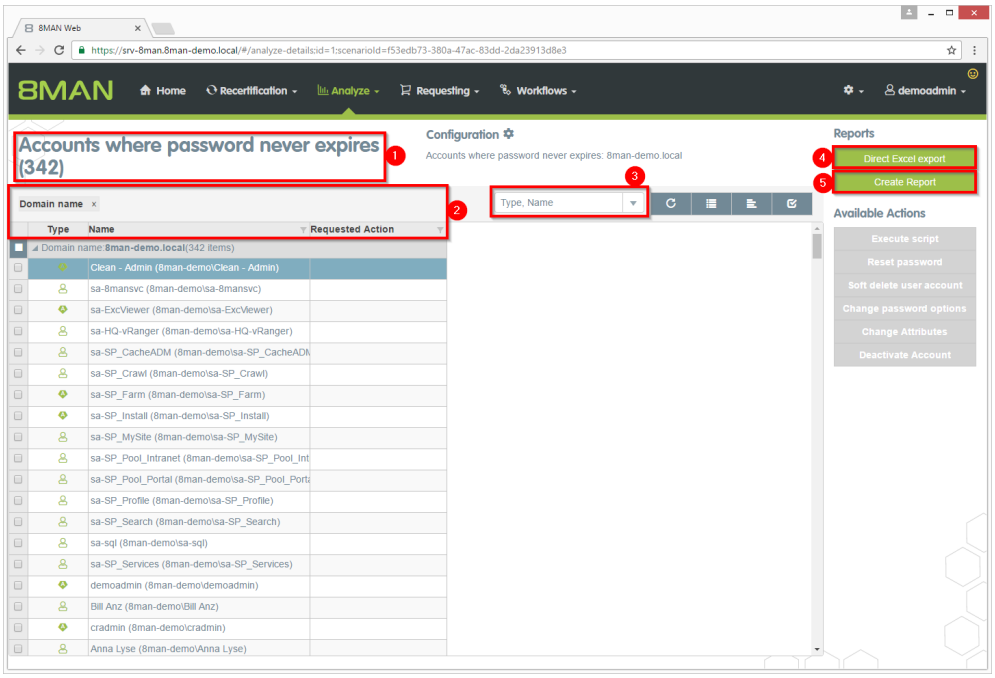
Login to the web client.



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".*



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.*

2.1.4 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.

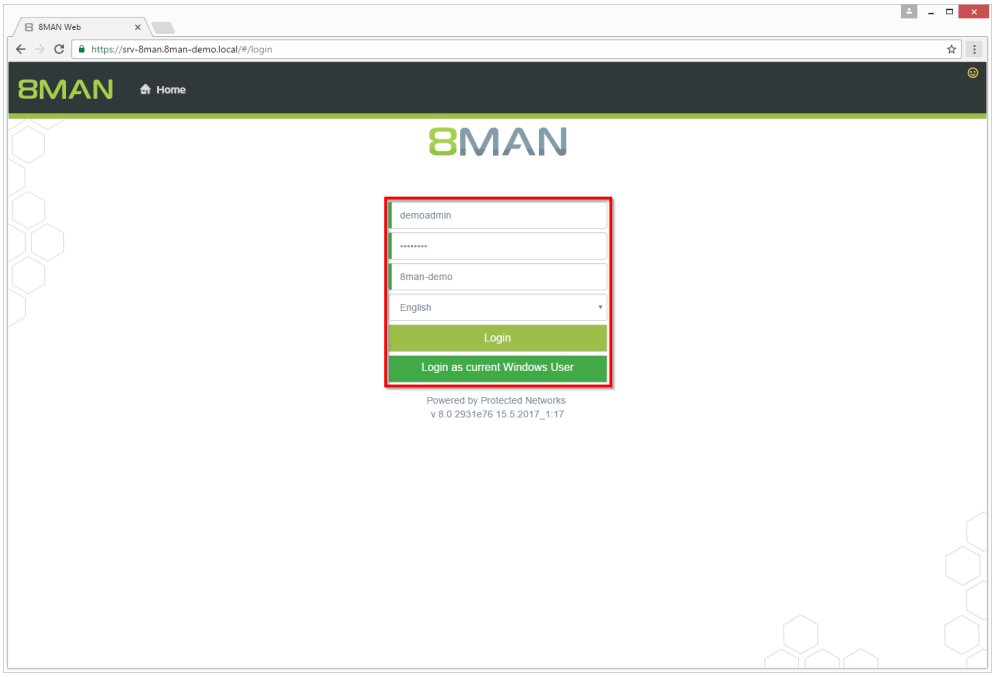
"Everyone accounts" are:

- Everyone
- Authenticated Users
- Domain-Users

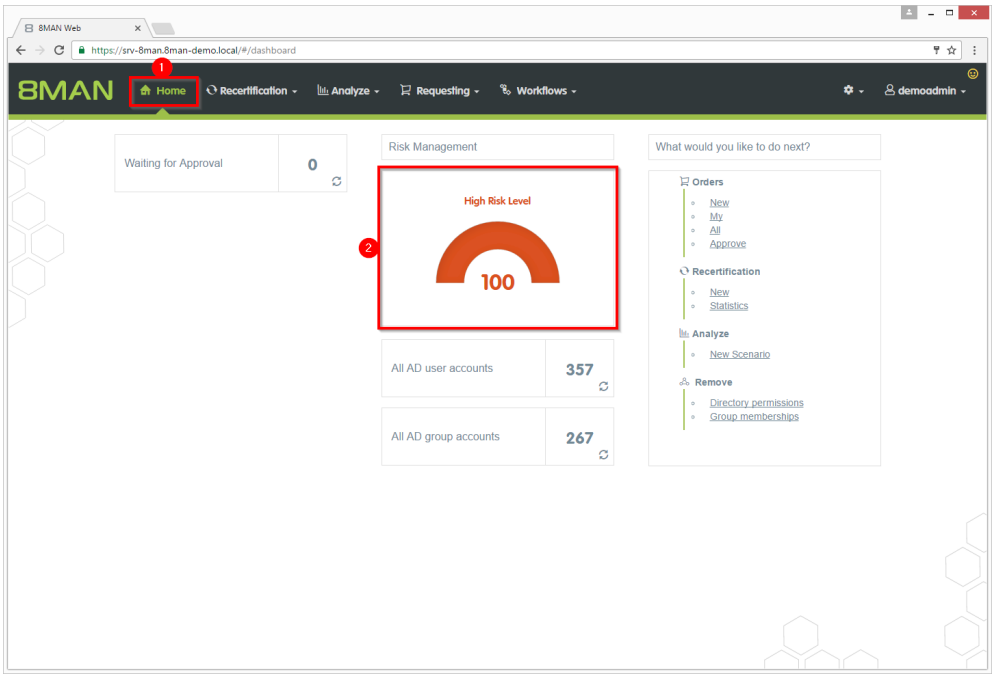
Additional Services

Removing permissions from globally accessible directories in bulk

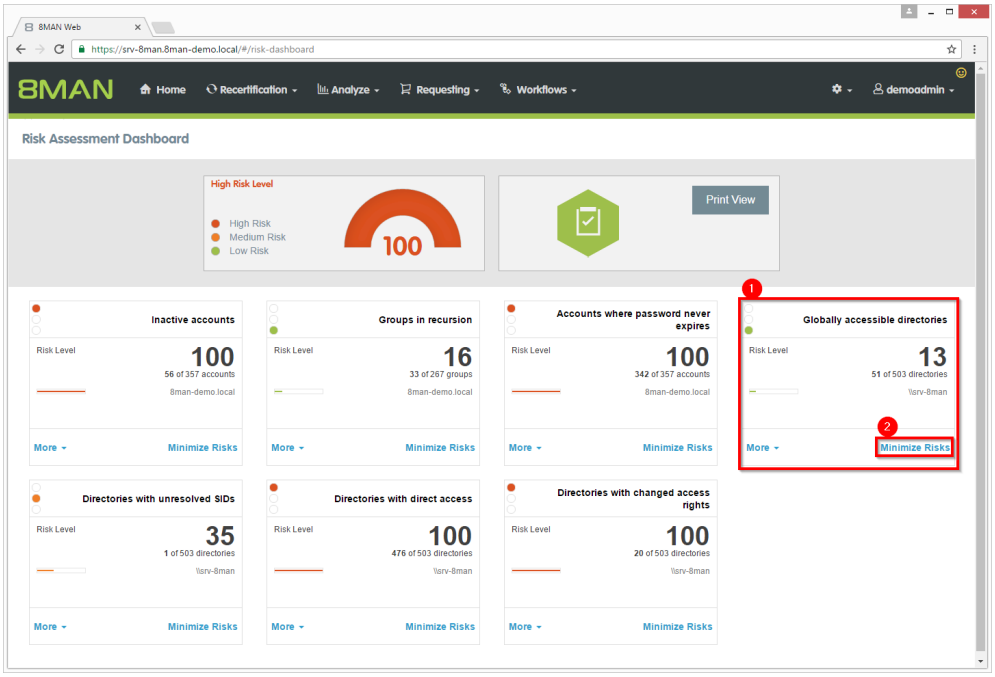
Step by step process



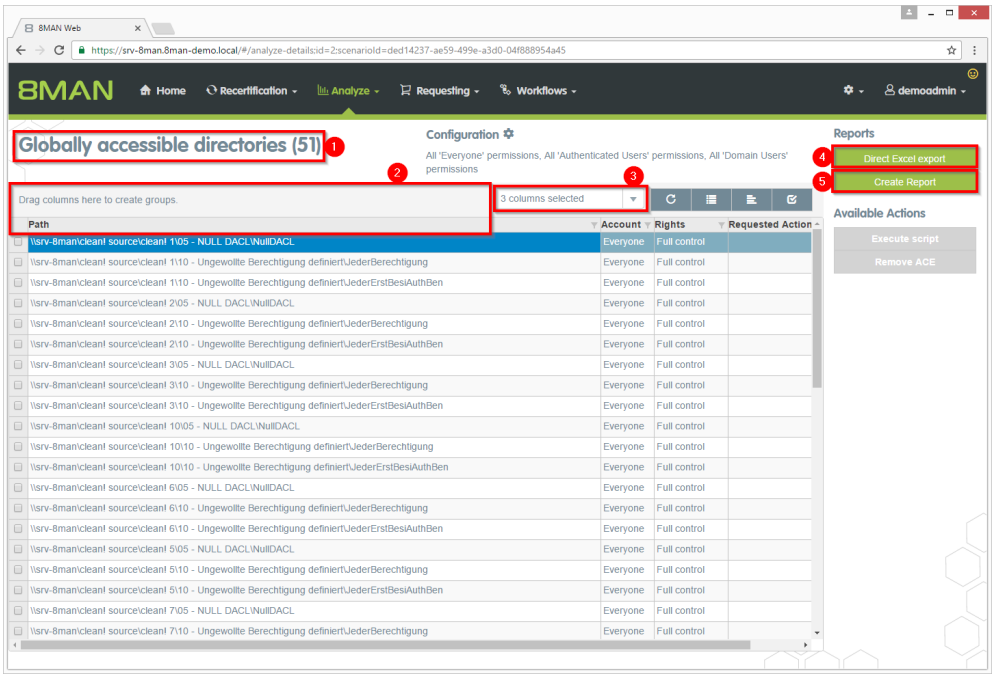
1. *Login to the web client.*



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".*



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.*

2.1.5 Identifying unresolved SIDs using the web client

Background / Value

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

8MAN clearly identifies unresolved SIDs in your system.

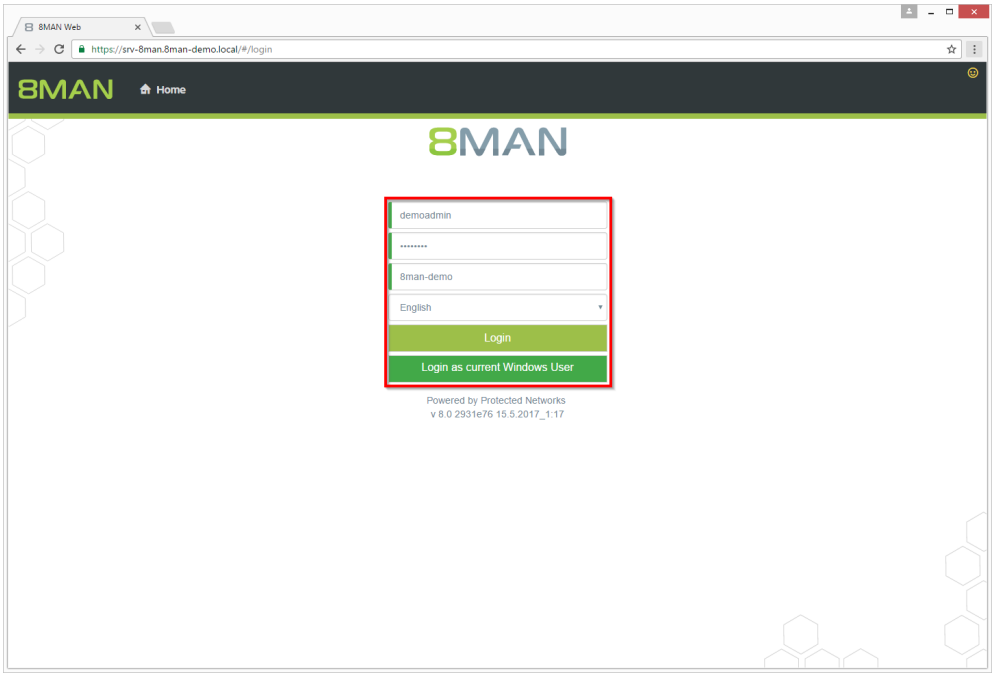
Additional Services

Identifying and deleting unresolved SIDs (using the rich client)

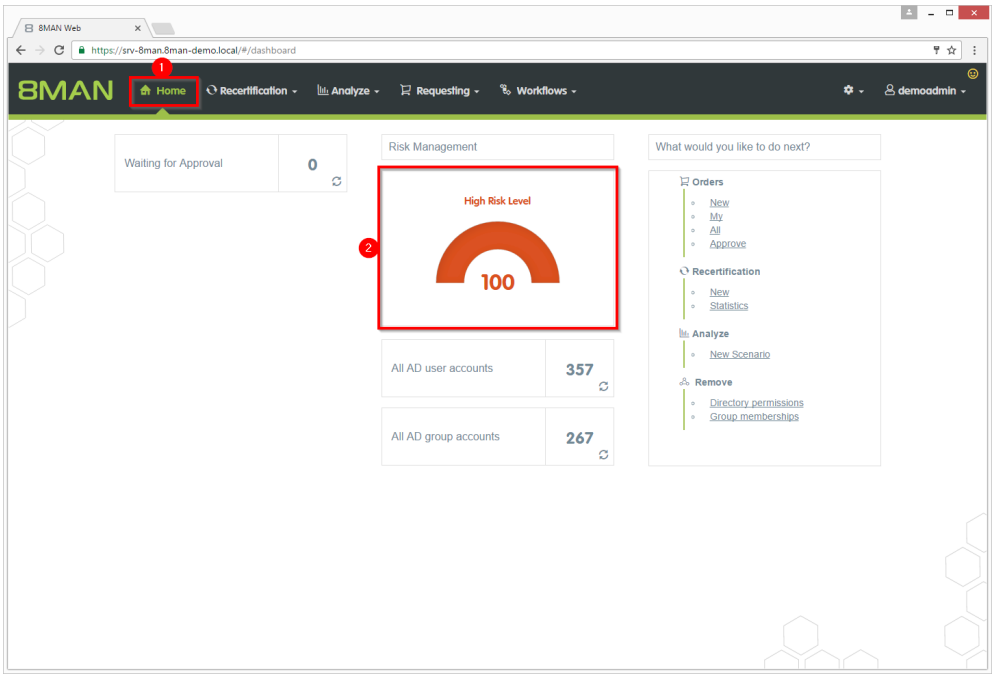
Removing a user and their permissions (using the rich client)

Removing unresolved SIDs in bulk (using the web client)

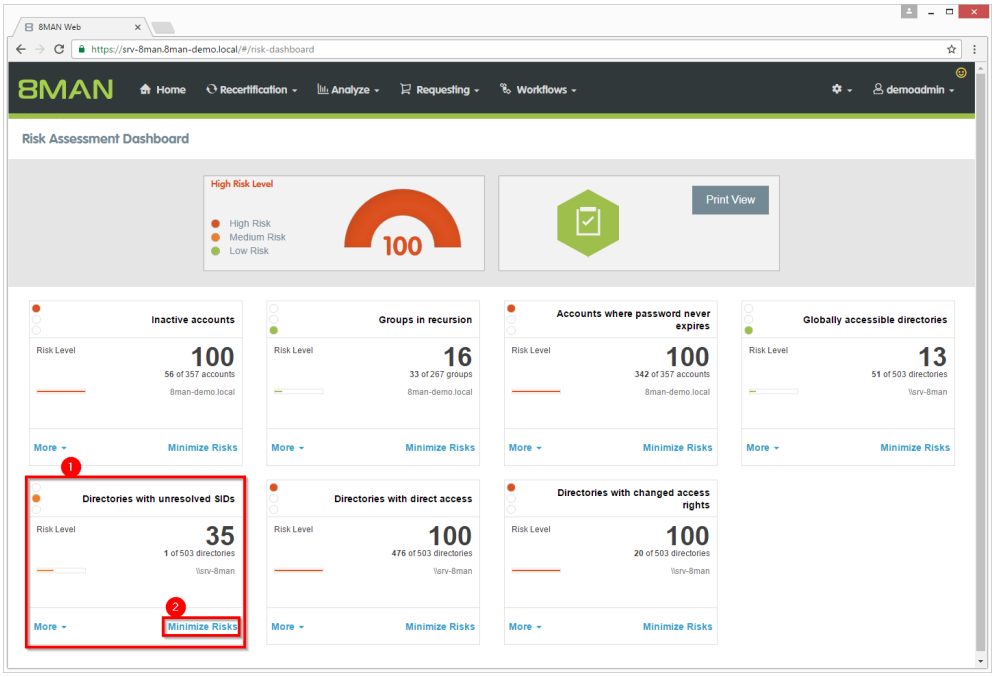
Step by step process



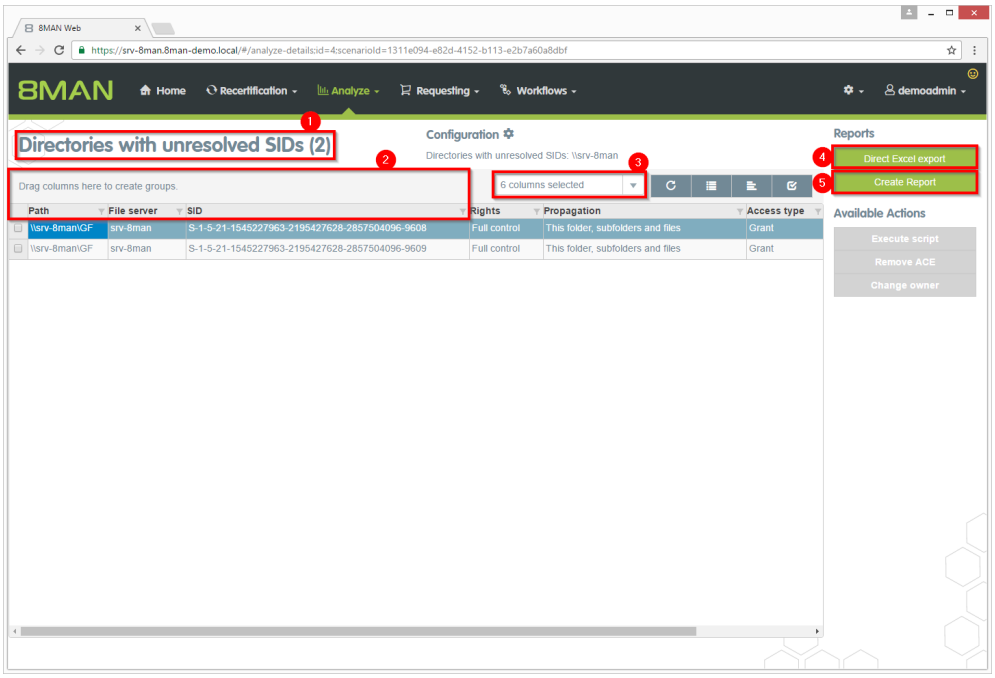
1. *Login to the web client.*



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 "Directories with unresolved SIDs".*
2. *Click "Minimize risks".*



1. *8MAN lists all unresolved SIDs.*
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.*

2.1.6 Identifying direct permissions using the web client

Background / Value

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

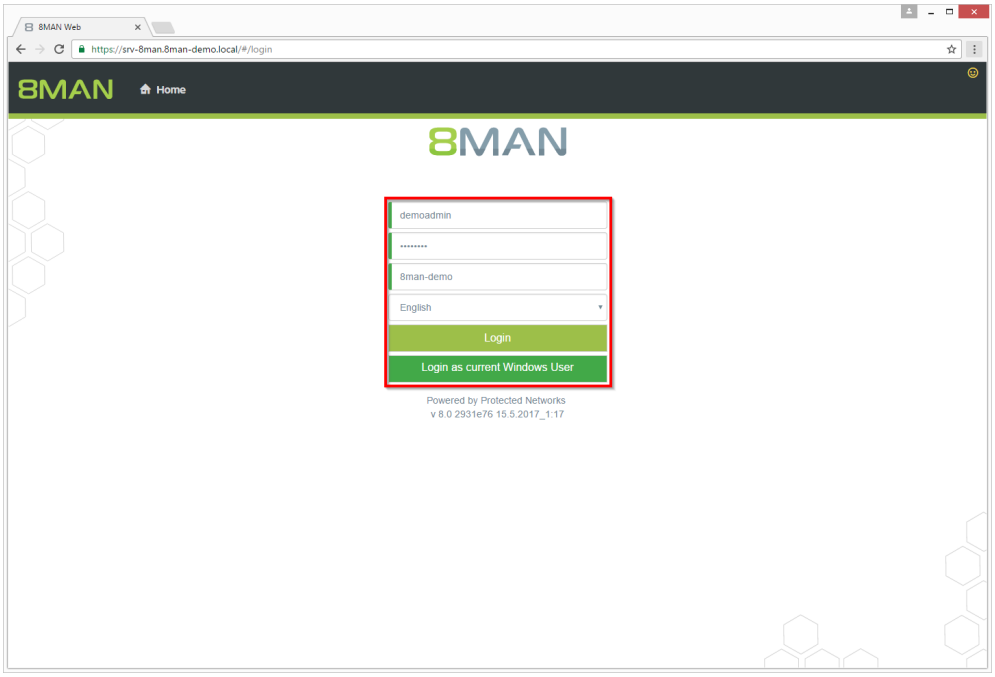
8MAN strictly adheres to Microsoft Best Practice and assigns a group for every access right.

Additional Services

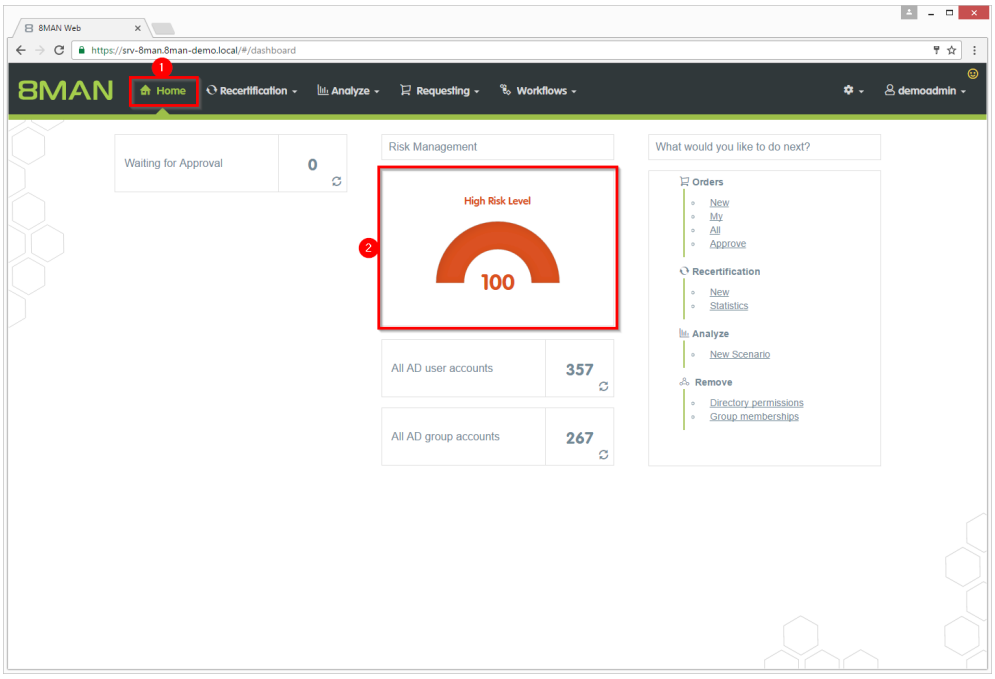
Removing direct permissions in bulk

Using the 8MATE clean! you can replace direct permissions with group memberships automatically.

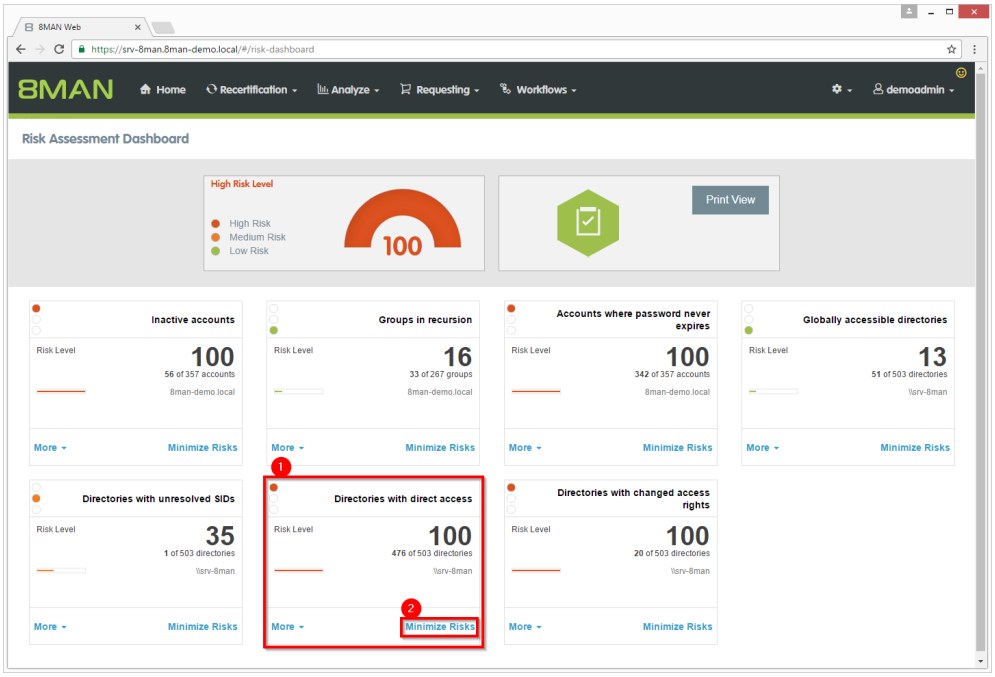
Step by step process



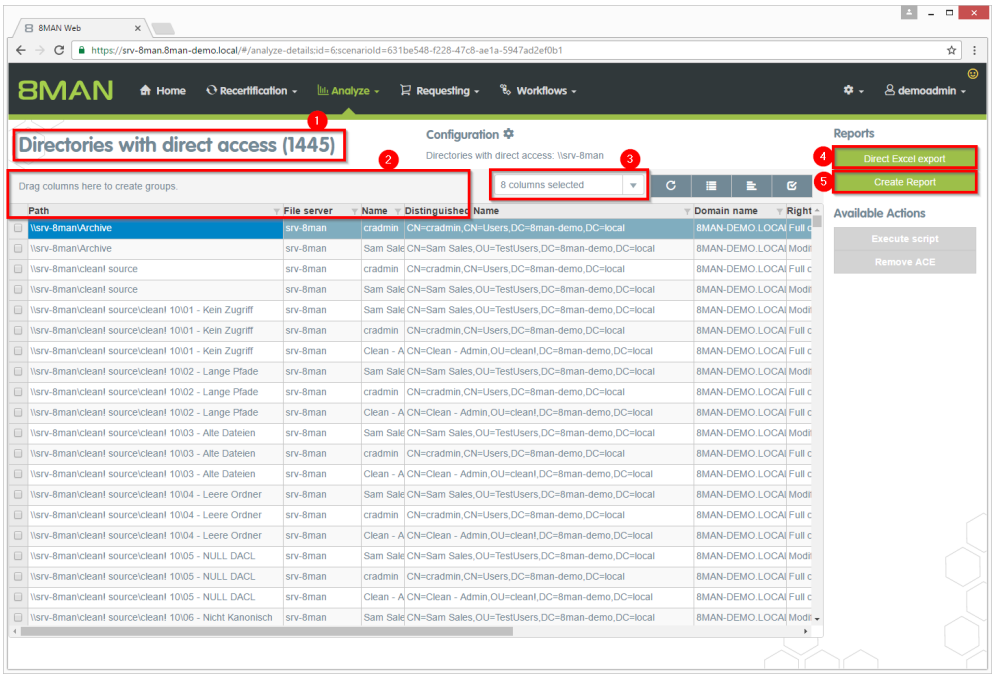
1. *Login to the web client.*



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 "Directories with direct access".*
2. *Click "Minimize risks".*



1. *8MAN lists all direct permissions.*
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.*

2.1.7 Identifying directories with differing permissions

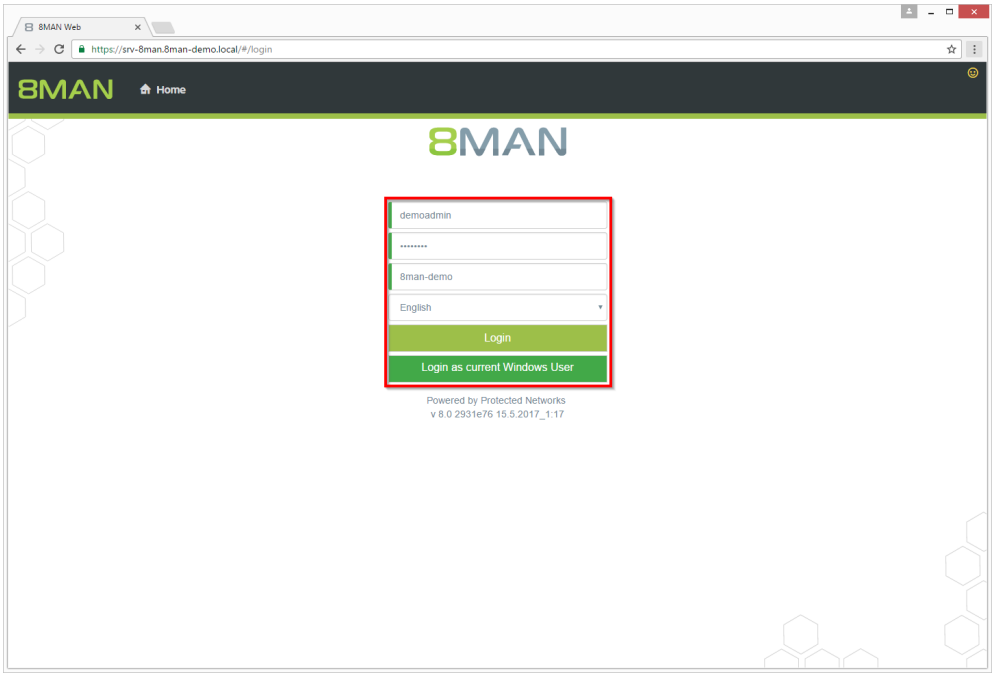
Background / Value

As part of best practices you should assign differing permissions unto the third or fourth level below share. Every directory below this level should inherit permissions. Assigning differing permissions to the deepest levels creates a confusing and complex access rights situation forcing excessive permissions.

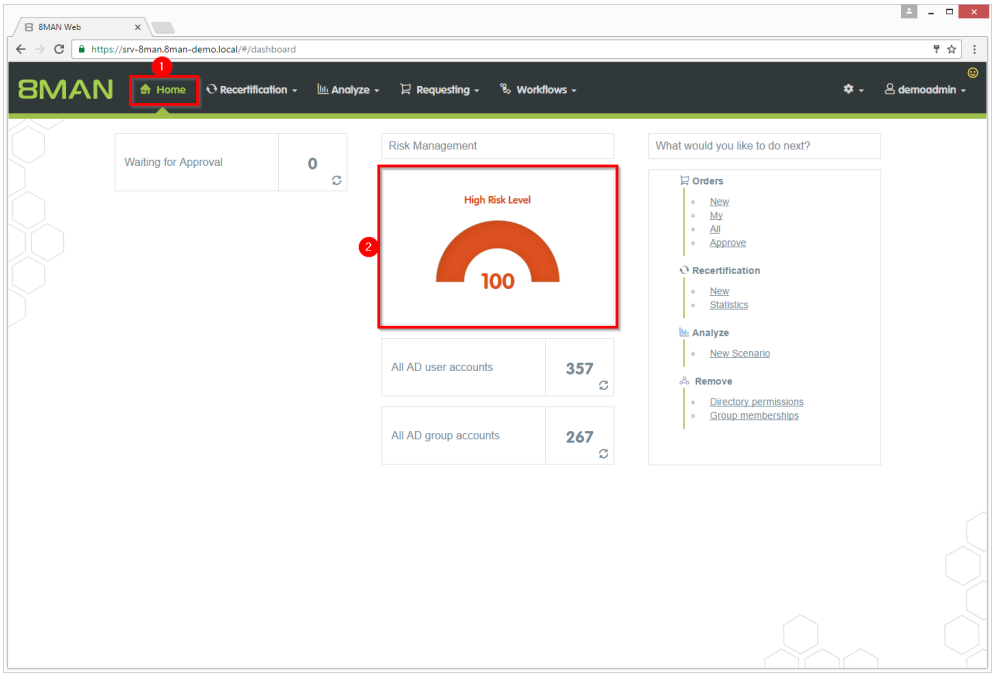
Additional Services

Removing corrupted inheritance (using the rich client)
Removing differing permissions in bulk (using the webclient)

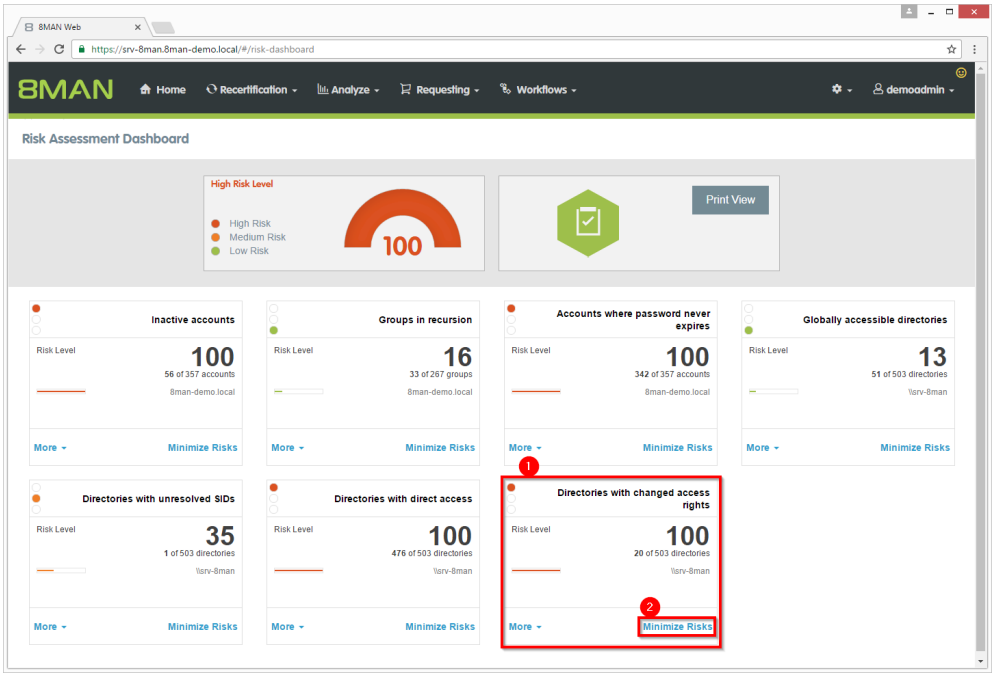
Step by step process



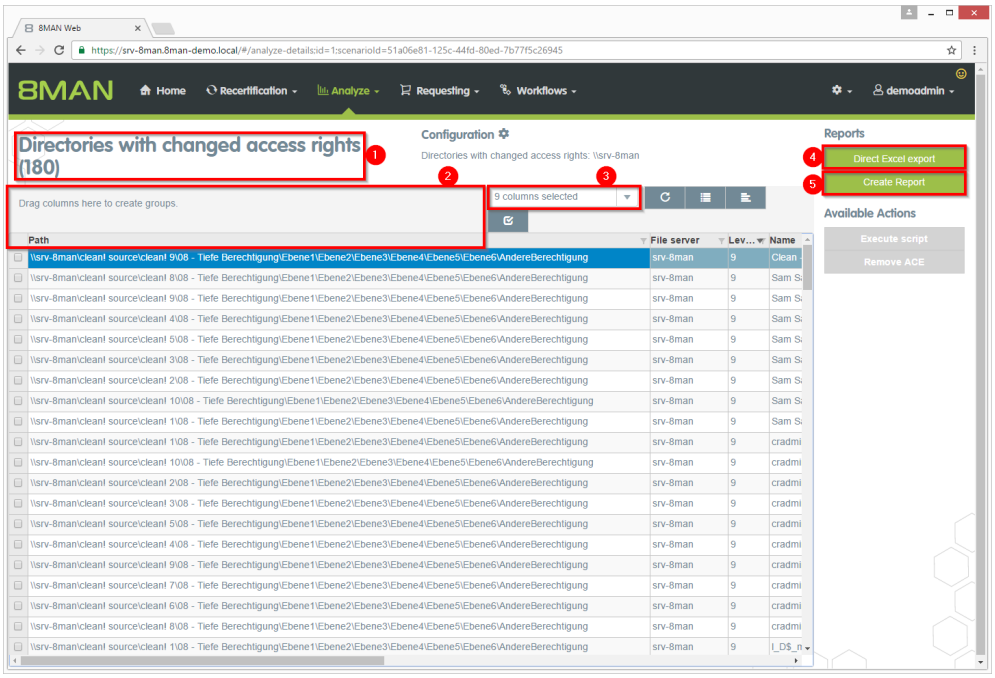
1. *Login to the web client.*



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 "Directories with direct access".*
2. *Click "Minimize risks".*



1. *8MAN lists all directories with differing permissions.* **8MAN lists differing permissions deeper than level 3 below share.**
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.*

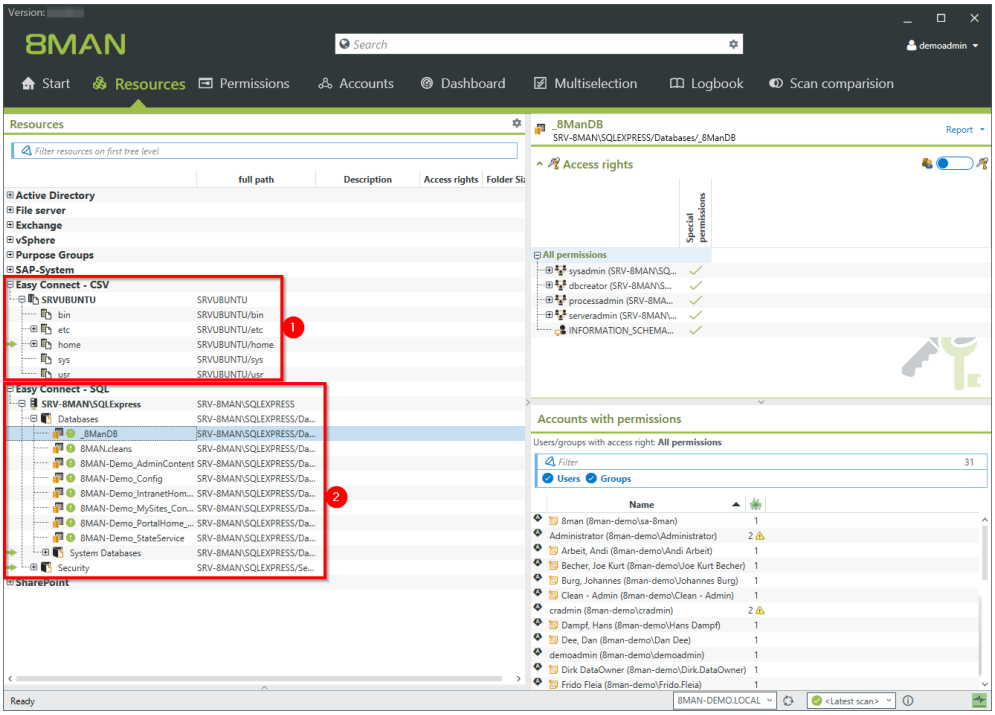
3 Resource Integration

3.1 Easy Connect - integrating any resources

Background / Value

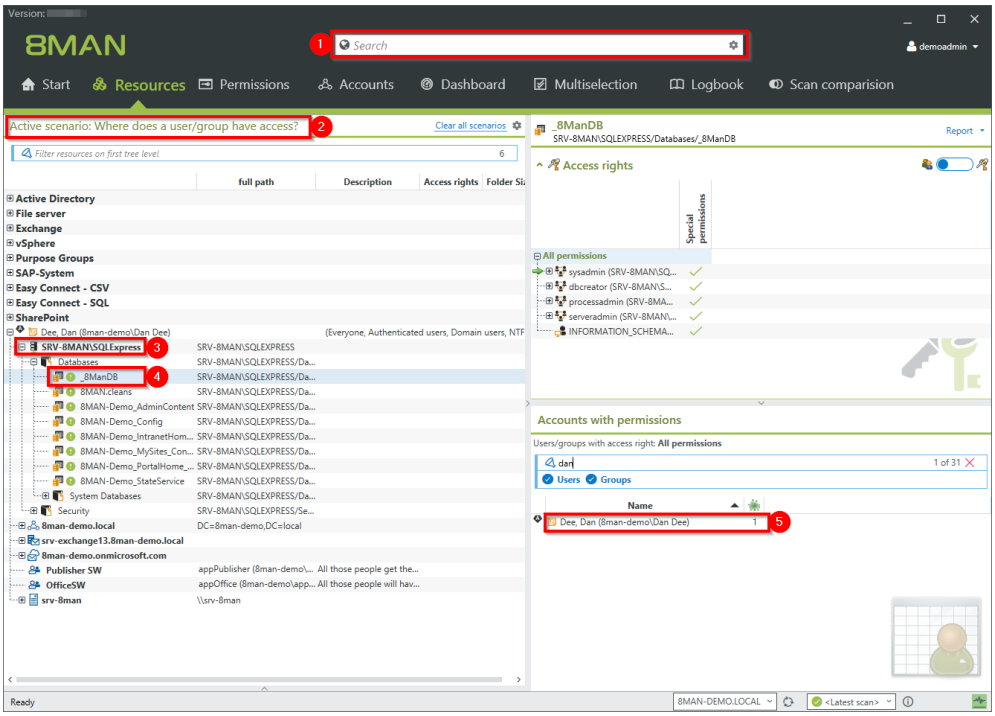
Integrate further resources to 8MAN with Easy Connect. You will get the 8MAN-typical overview, analysis and reporting functionalities for these. The question "Who has access where?" can be answered more comprehensive and much easier with one single solution. Import data from a CSV-file or via SQL-scripts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

3.1.1 Analysing Easy Connect resources



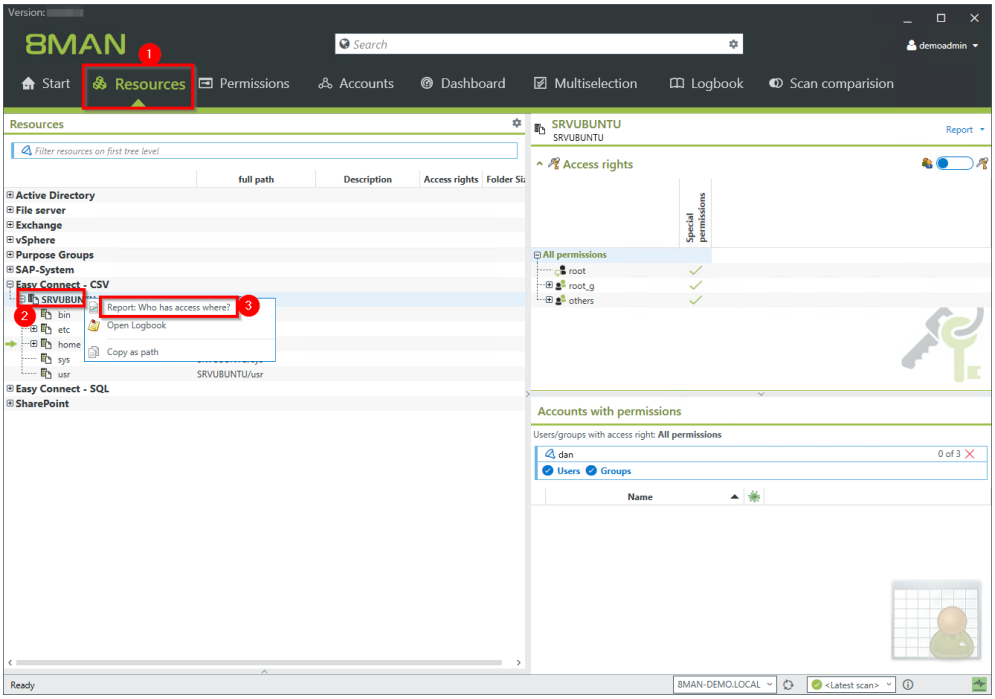
The example shows access rights information imported from a Linux file system and a MS SQL-server.

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

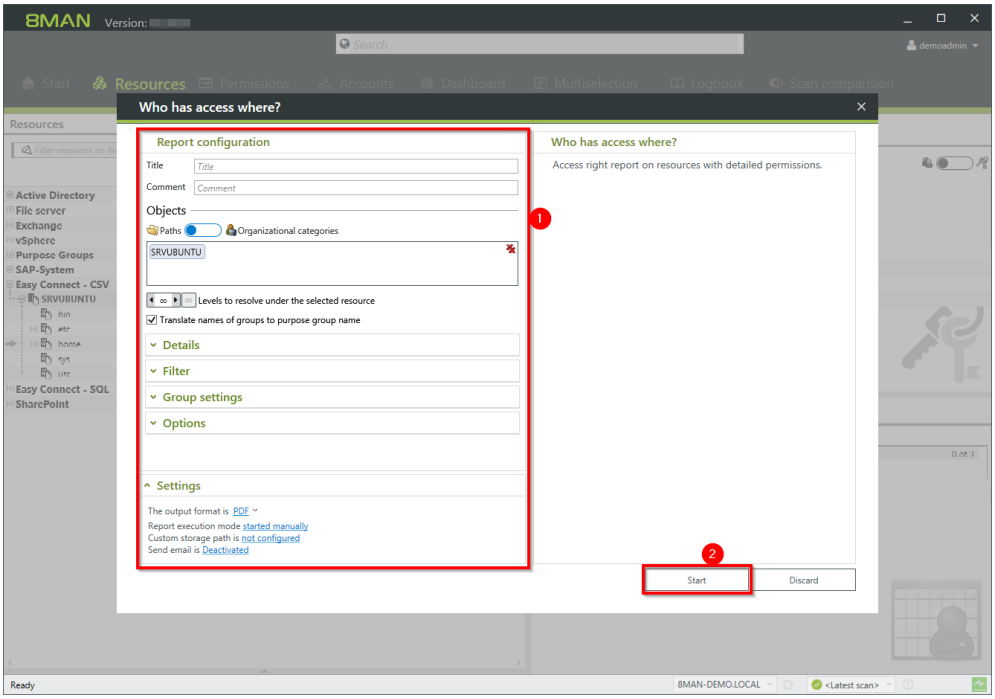


1. *8MAN search includes easy connect resources.*
2. *The scenario "Where does a user/group have access?" includes Easy Connect resources.*
3. *The scenario includes the imported SQL-server resource.*
4. *Navigate through Easy Connect resources.*
5. *Access rights of the desired user are shown in 8MAN-typical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

3.1.2 Creating a report for an Easy Connect resource

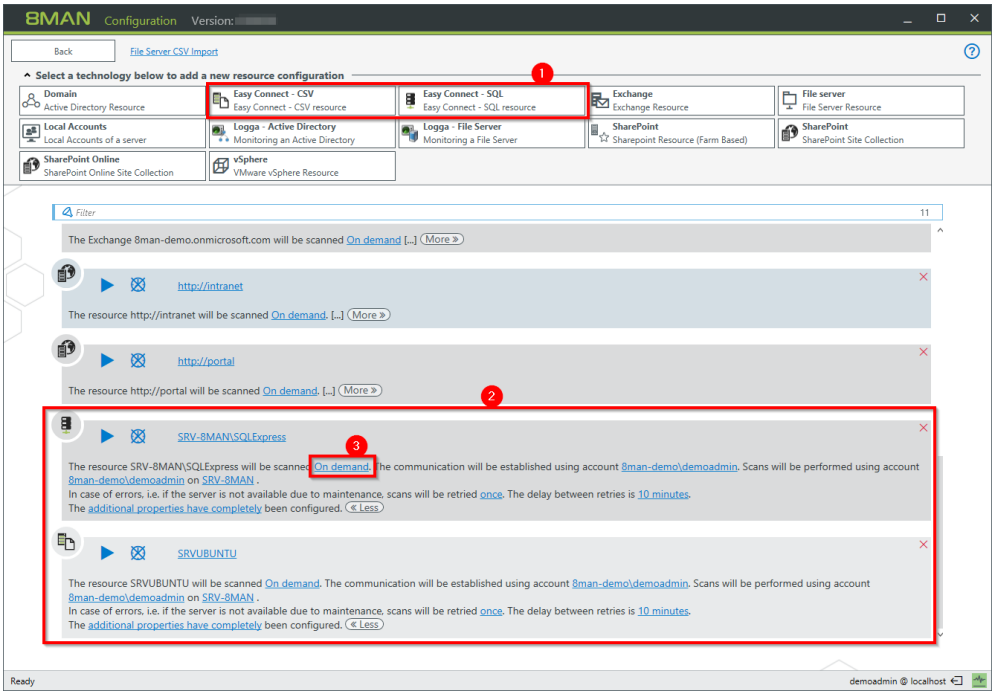


1. *Choose "Resource" view*
2. *Select a resource, e.g. "SRVUBUNTU".*
3. *Choose the report: "Who has access where?" from the context menu.*



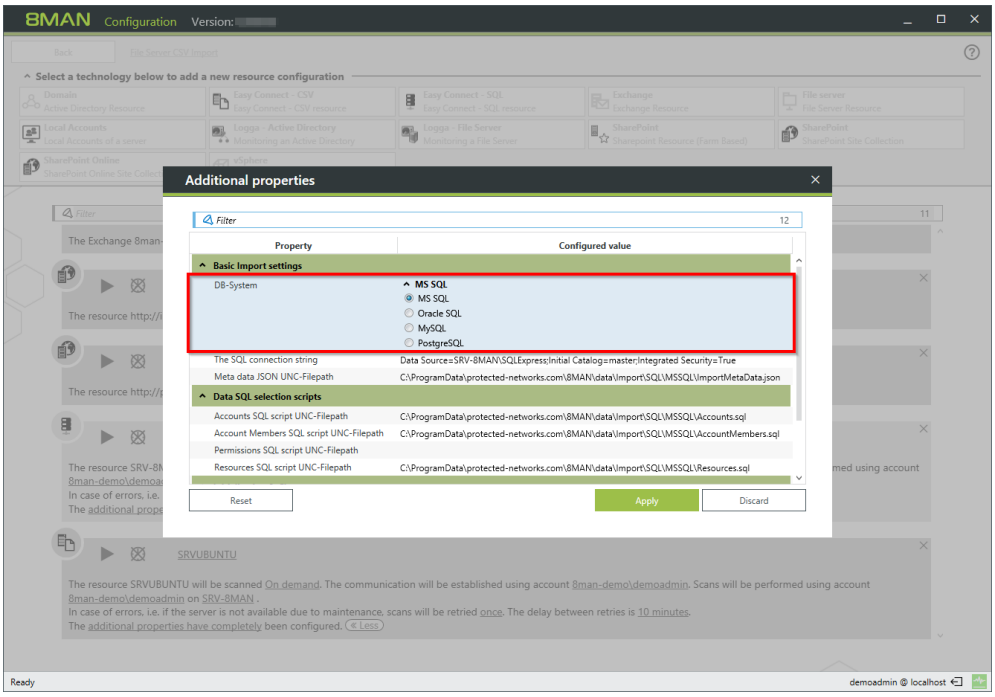
1. *Configure the report. Options are the same as on any "built-in" resource.*
2. *Start the report.*

3.1.3 Integrating Easy Connect ressources



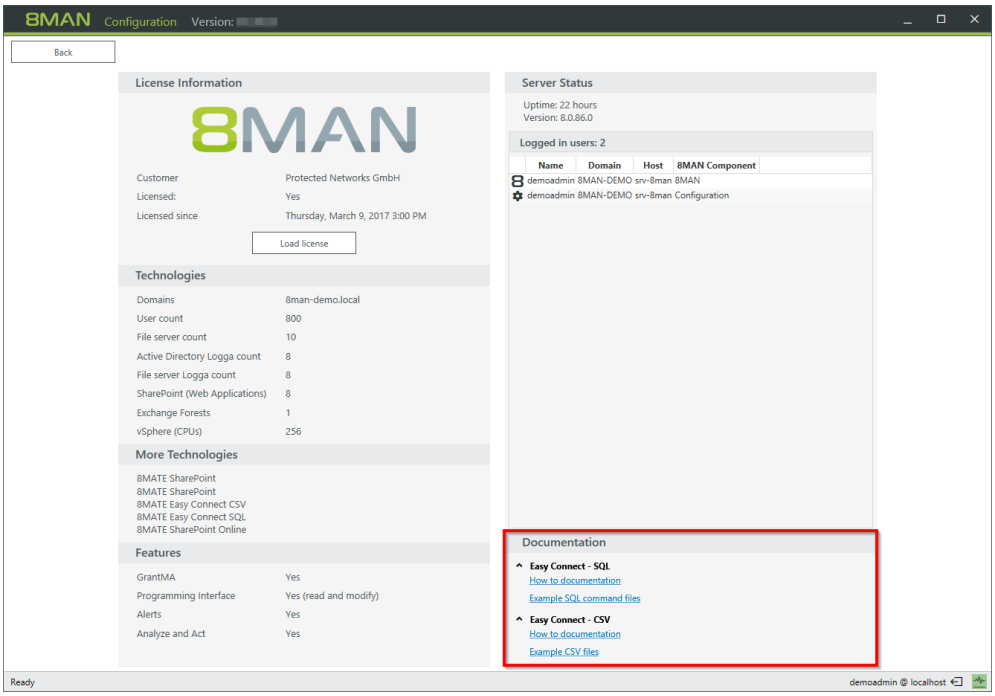
Click "Scans" on the 8MAN configuration module homepage.

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



8MAN supports the following SQL-server:

- *Microsoft SQL*
- *Oracle SQL*
- *MySQL*
- *PostgreSQL*



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

3.2 8MATE for SharePoint 8.0 - Supporting 2016 and Online

Microsoft offers two ways of ineracting with a SharePoint Server:

- Server Side Object Model (SSOM)
- Client Side Object Model (CSOM)

8MAN uses until version 7.5 the Server Side Object Model only. A component installation (collector) on the SharePoint server is needed. If you are using SharePoint Online or a hosted SharePoint service you are not allowed to install anything on the SharePoint server. In future we will change to the Client Side Object Model where no component installation is needed. The Server Side Object Model will be supported until 8MAN version 8.5. Both Models can be used at the same time for different SharePoint servers.

How 8MAN 7.6 supports SharePoint:

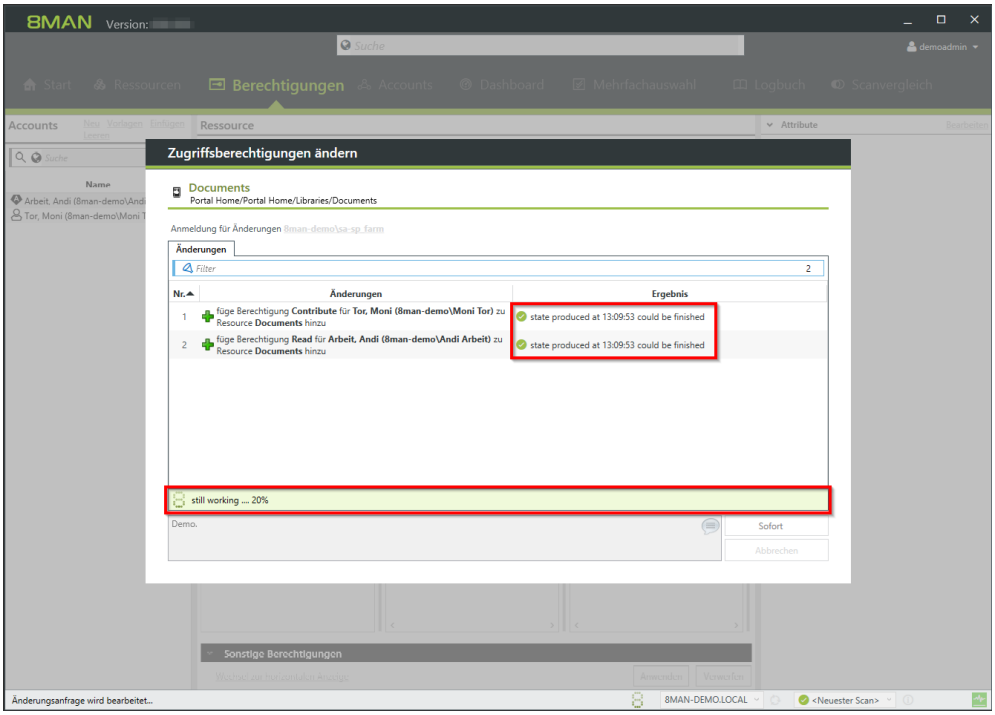
	SharePoint 2010	SharePoint 2013	SharePoint 2016	SharePoint Online
SSOM (farm based) Read and Modify	✓	✓	✗	✗
CSOM - SharePoint Remote Connector Read and Modify*	✓	✓	✓	✓

* Modify includes changing SharePoint access rights and SharePoint group memberships. Creating SharePoint groups automatically by the group wizard is not supported.

8MAN users use the GUI for SharePoint resources as before. A new progress indicator for executing status on changes is added.

For configuring the new remote connector please see: Configuring the SharePoint Remote Connector.

3.2.1 8MATE SharePoint - Progress indicator for changes



8MAN displays the progress while executing changes on SharePoint resources.

4 User Provisioning

4.1 8MAN Enterprise - Executing scripts before and after changes

Background / Value

Integrate scripts into 8MAN Enterprise and execute them before and after changes. Automate standard processes and increase efficiency.

Add scripts to the following change tasks:
Creating an user account
Managing group memberships
Moving objects in Active Directory
Removing a user and their permissions
Modifying group and user attributes
Creating groups and adding users
Deactivating a user account

Provide scripts using the 8MAN configuration module.

4.2 New bulk operations

4.2.1 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.

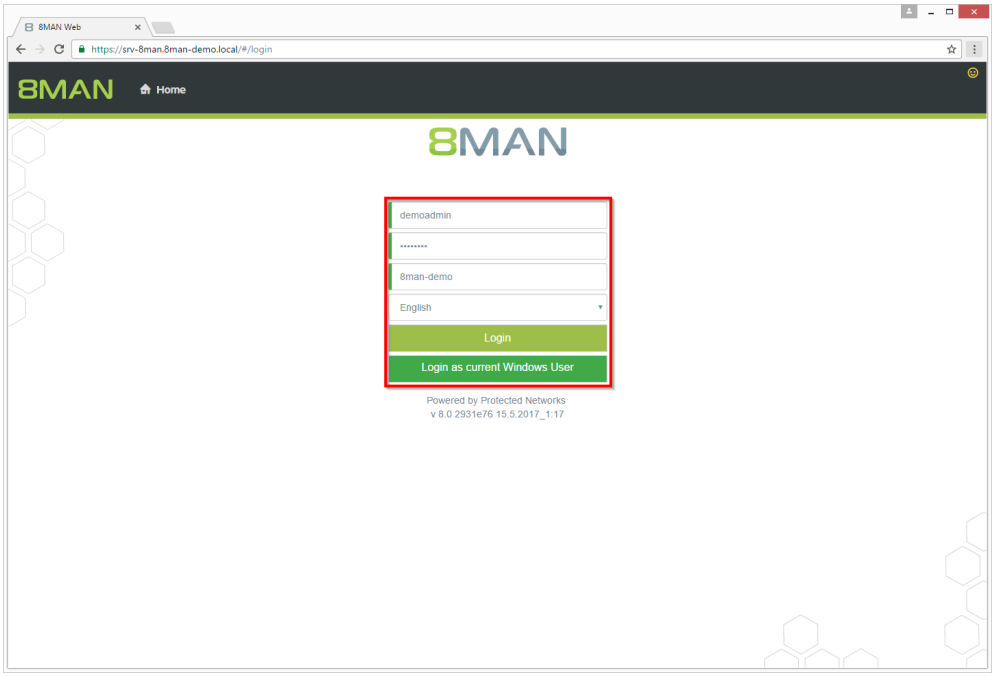
"Everyone accounts" are:

- Everyone
- Authenticated Users
- Domain-Users

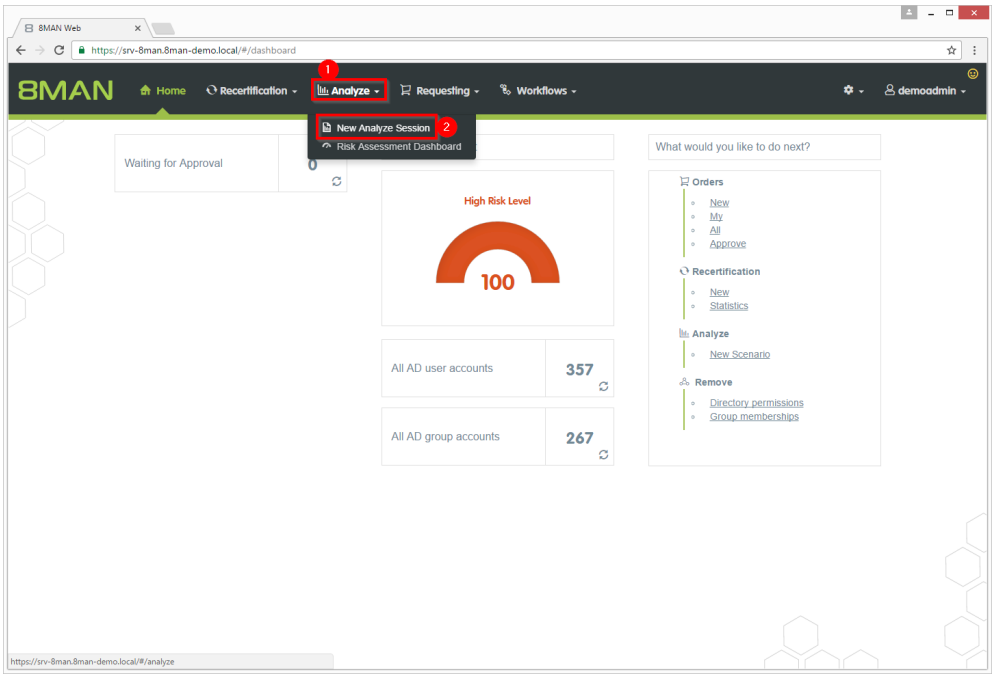
Additional Services

Report: Identifying usage of "Everyone" (using the rich client)
Report: Identifying usage of "Authenticated Users" (using the rich client)

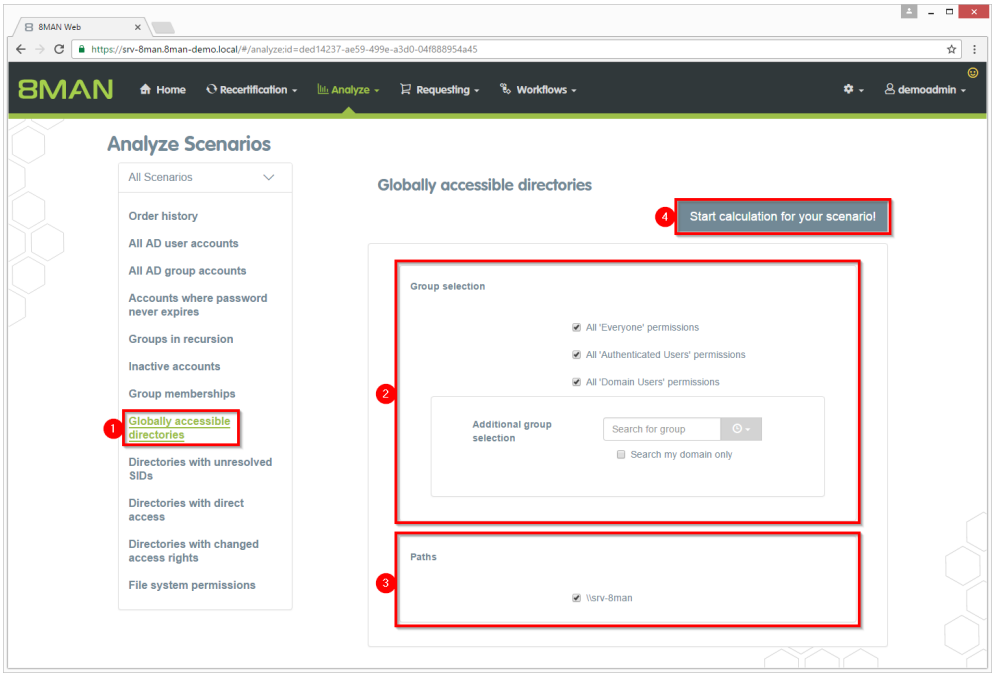
Step by step process



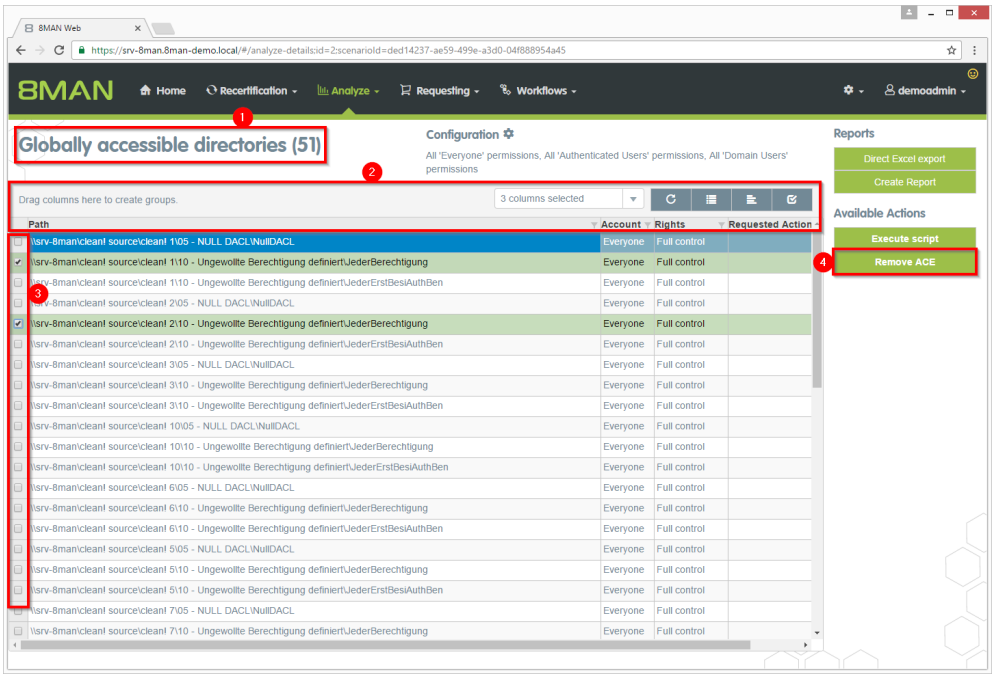
1. *Login to the web client.*



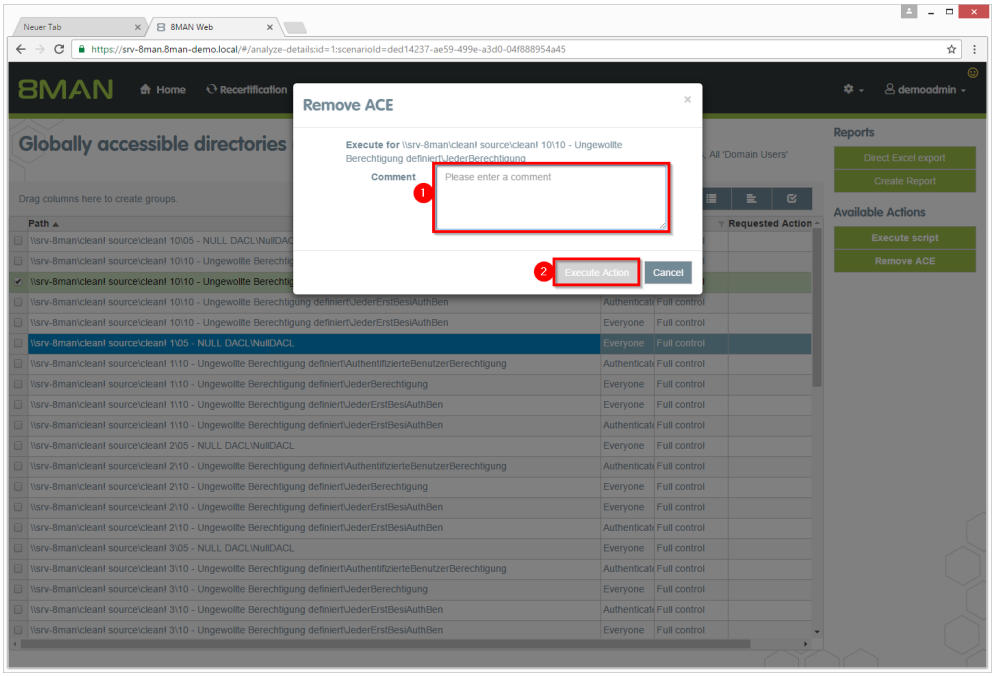
1. *Click "Analyze".*
2. *Click "New Analyze Session".*



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.*



1. *8MAN lists all globally accessible directories.*
2. *Use sorting, filtering, grouping and column selection to locate the desired rows.*
3. *Select the desired entries.*
4. *Click "Remove ACE".*



1. *Leave a comment.*
2. *Click "Execute Action".*

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

4.2.2 Removing direct permissions in bulk

Background / Value

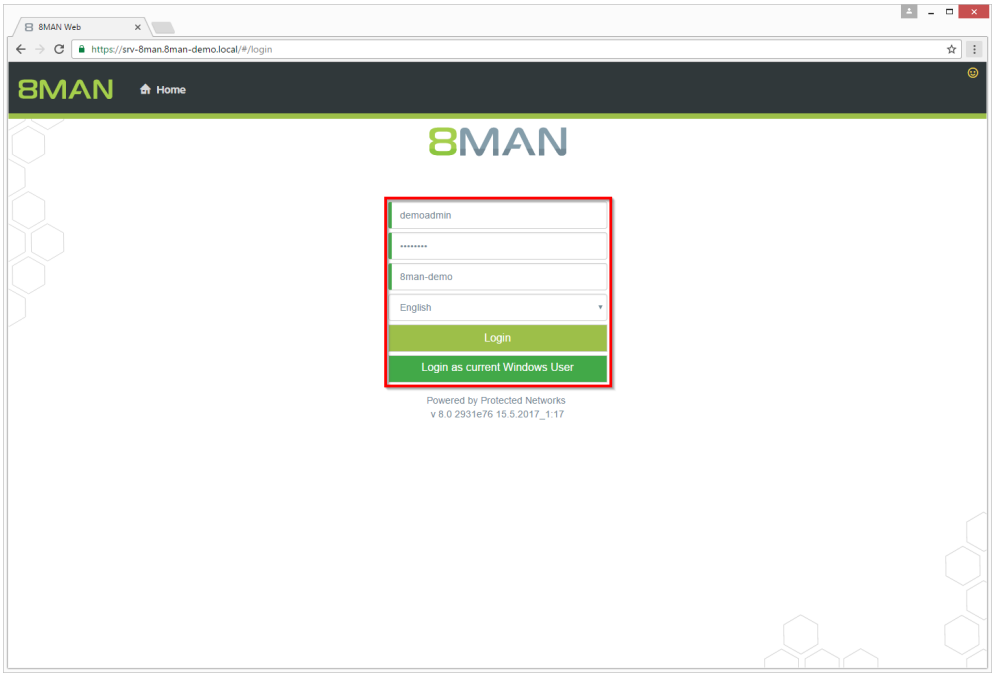
Direct permissions should be avoided at all costs and replaced by group permissions. Firstly, direct access rights are inefficient because every user is managed independently. Secondly, each directory needs to be examined individually to ensure the removal of all direct permissions. 8MAN shows you all direct access rights on your file server(s). You can remove them in bulk using the web client.

Additional Services

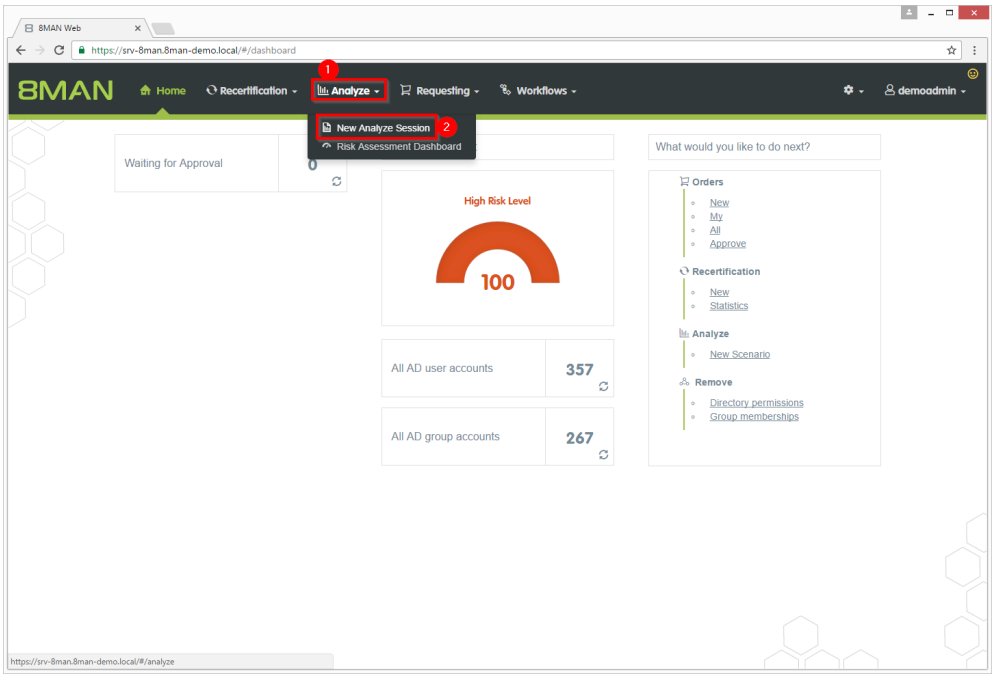
8MATE Clean! allows you to automatically remove direct access rights and turn them into group memberships.

Changing password options in bulk
Removing unresolved SIDs in bulk

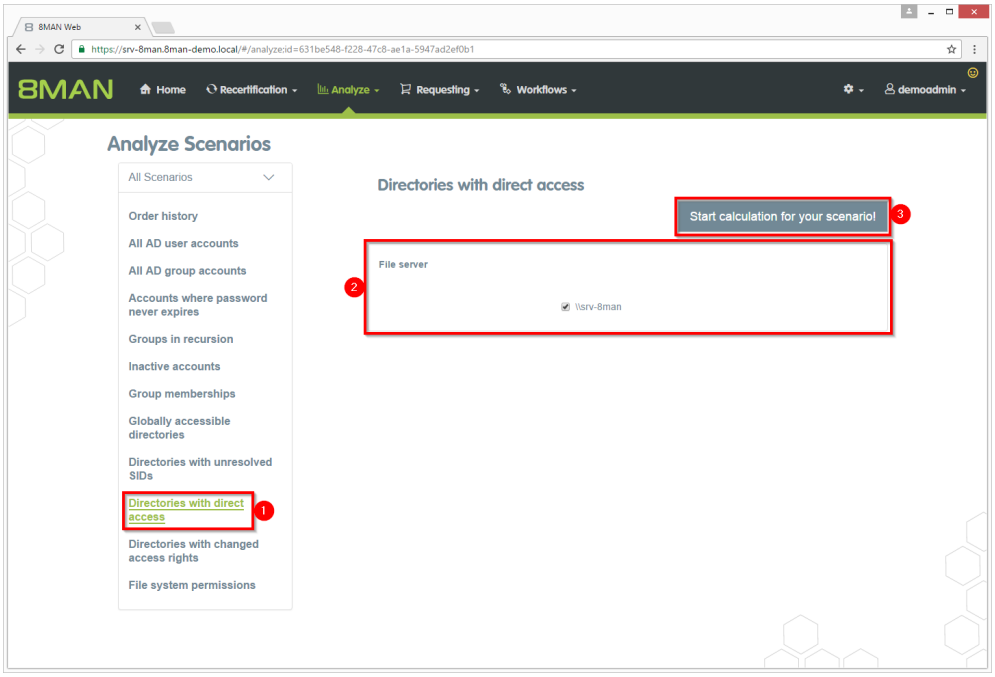
Step by step process



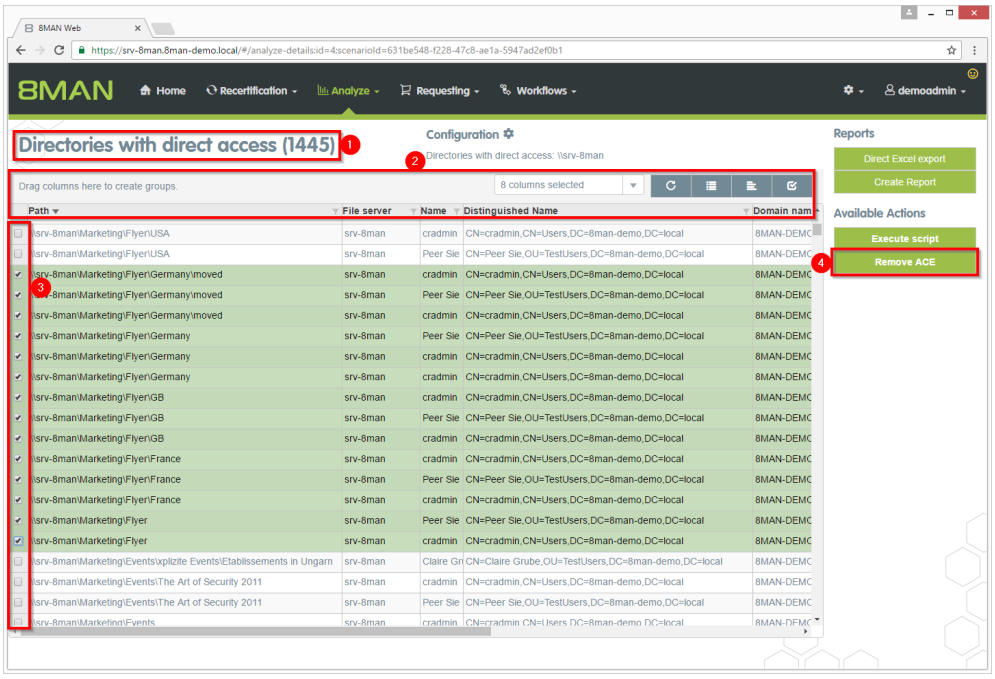
1. *Login to the web client.*



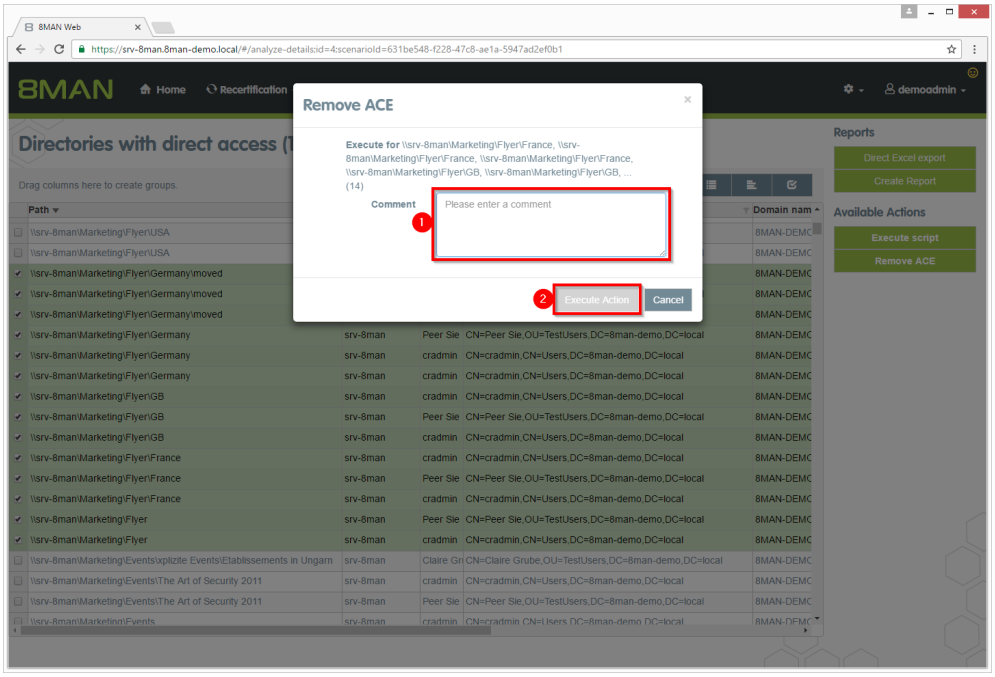
1. *Click "Analyze".*
2. *Click "New Analyze Session".*



1. *Click "Directories with direct access".*
2. *Select a file server.*
3. *Start the calculation.*



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".*



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".

4.2.3 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.

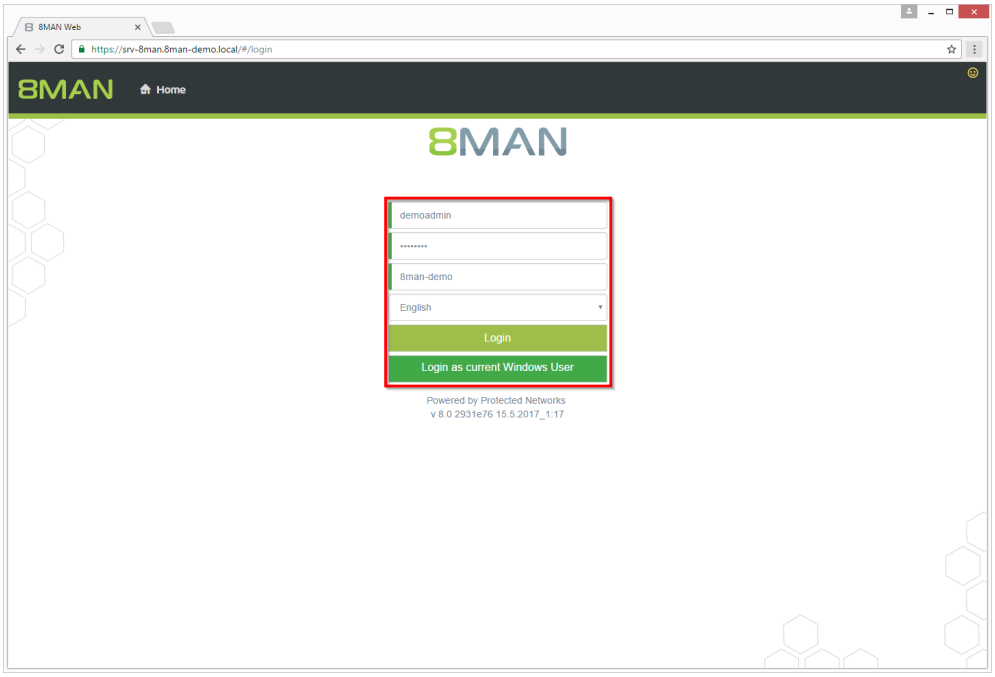
8MAN clearly identifies unresolved SIDs in your system. Delete unresolved SIDs in bulk using Analyze & Act.

Additional Services

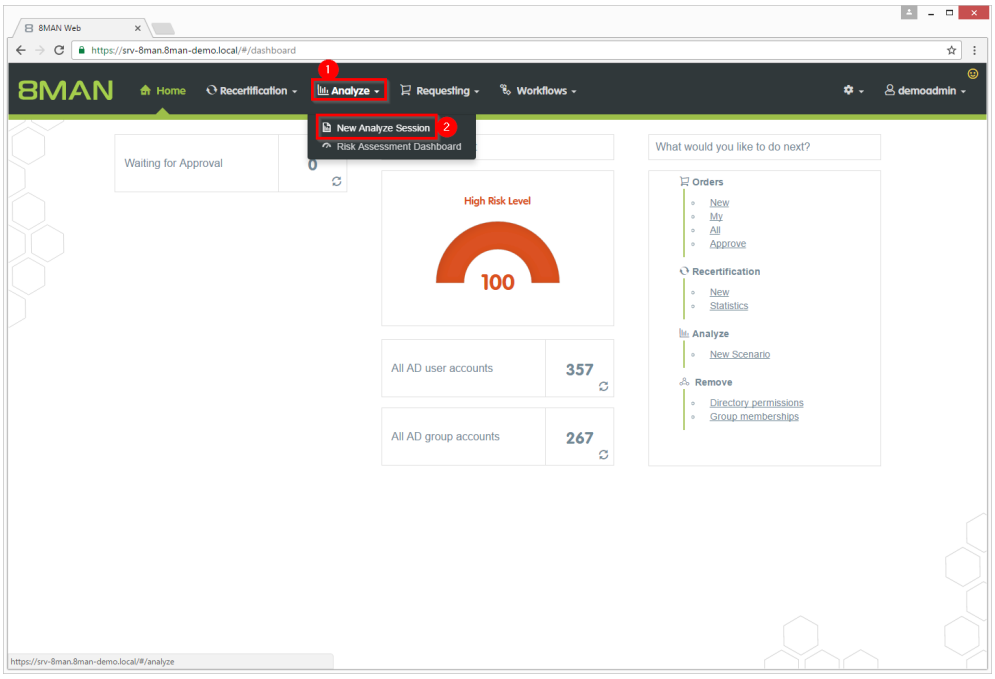
Identifying and deleting unresolved SIDs (using the rich client)

Report: Identifying unresolved SIDs (using the rich client)

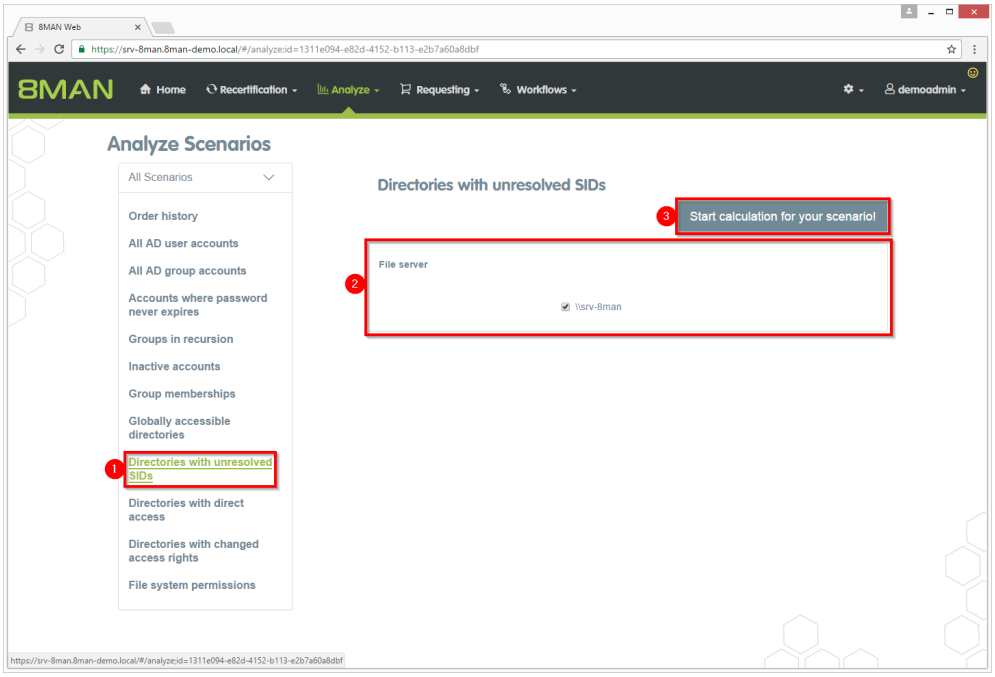
Step by step process



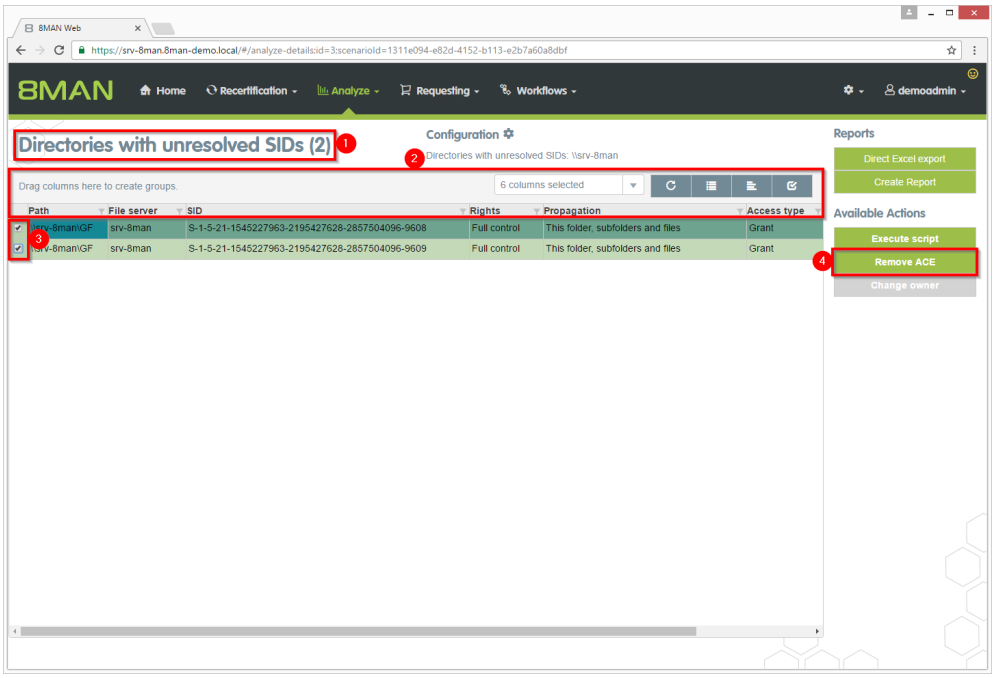
1. *Login to the web client.*



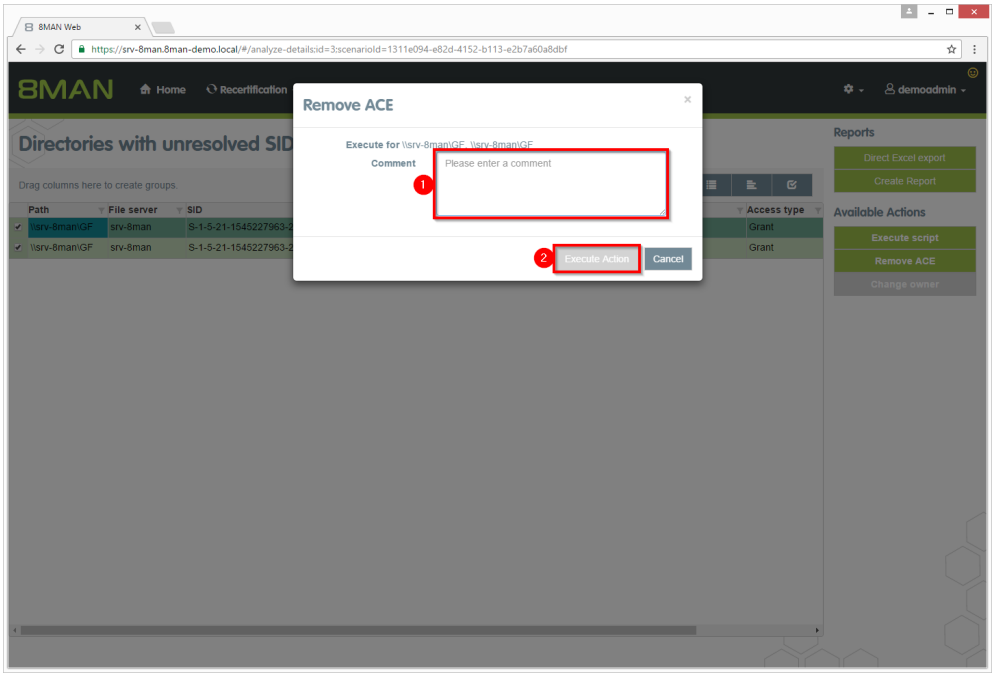
1. *Click "Analyze".*
2. *Click "New Analyze Session".*



1. *Click "Directories with unresolved SIDs".*
2. *Select a file server.*
3. *Start the calculation.*



1. *8MAN lists all Directories with unresolved SIDs.*
2. *Use sorting, filtering, grouping and column selection to locate the desired rows.*
3. *Select the desired entries.*
4. *Click "Remove ACE".*



1. *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".

4.2.4 Removing differing permissions in bulk

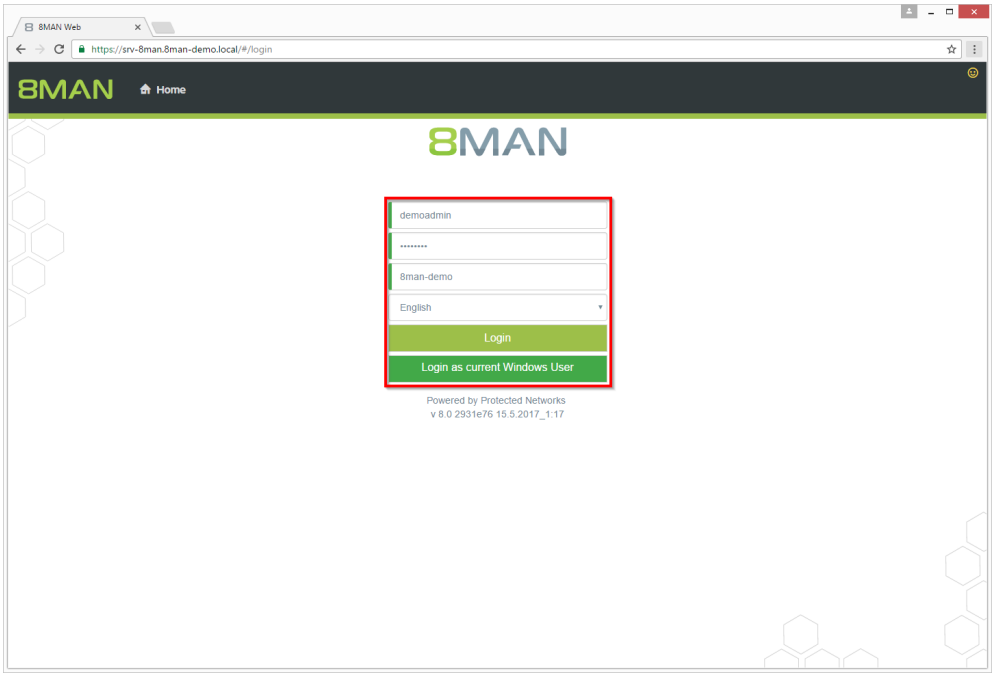
Background / Value

It is part of best practices assigning differing permissions just unto the third or fourth level below share. All directories below this level should inherit their permissions. Assigning differing permissions unto the deepest levels of directories increases the error-proneness.

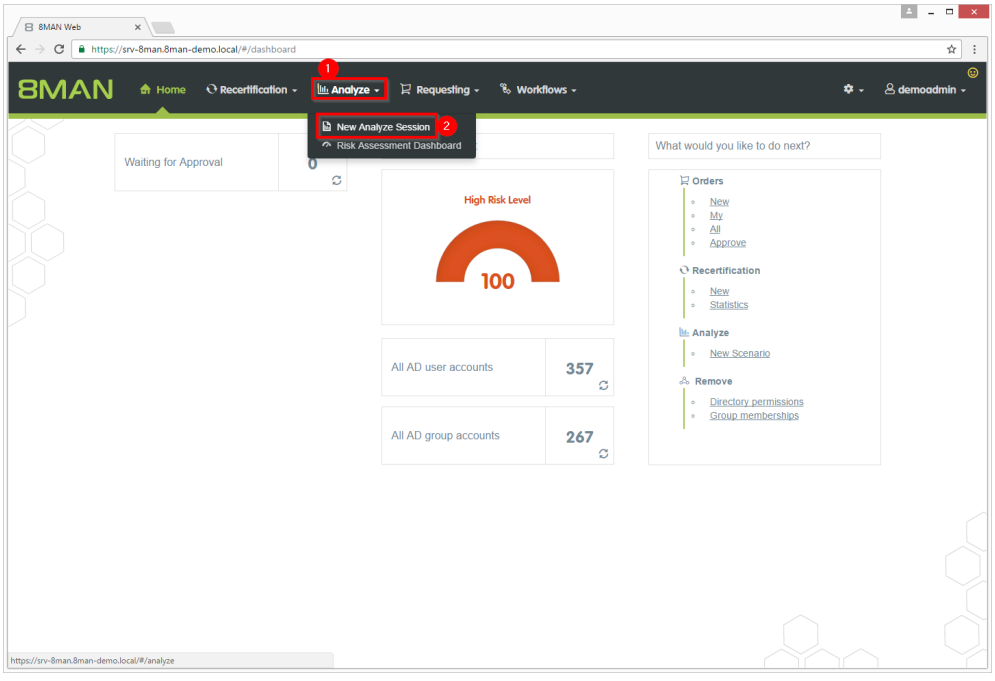
Additional Services

Removing corrupted inheritance (using the rich client)

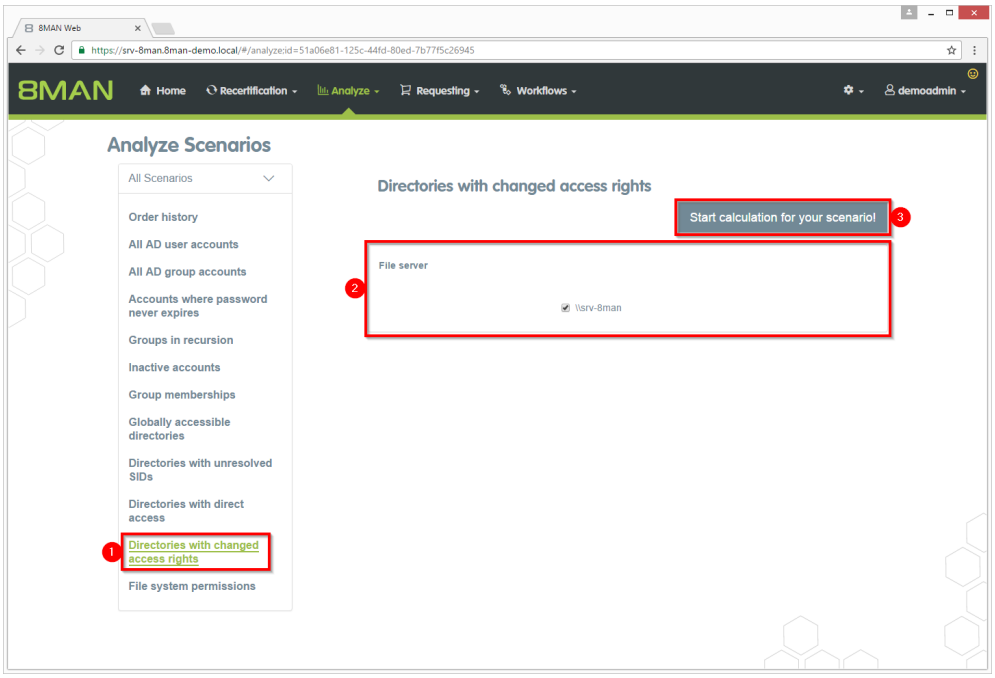
Step by step process



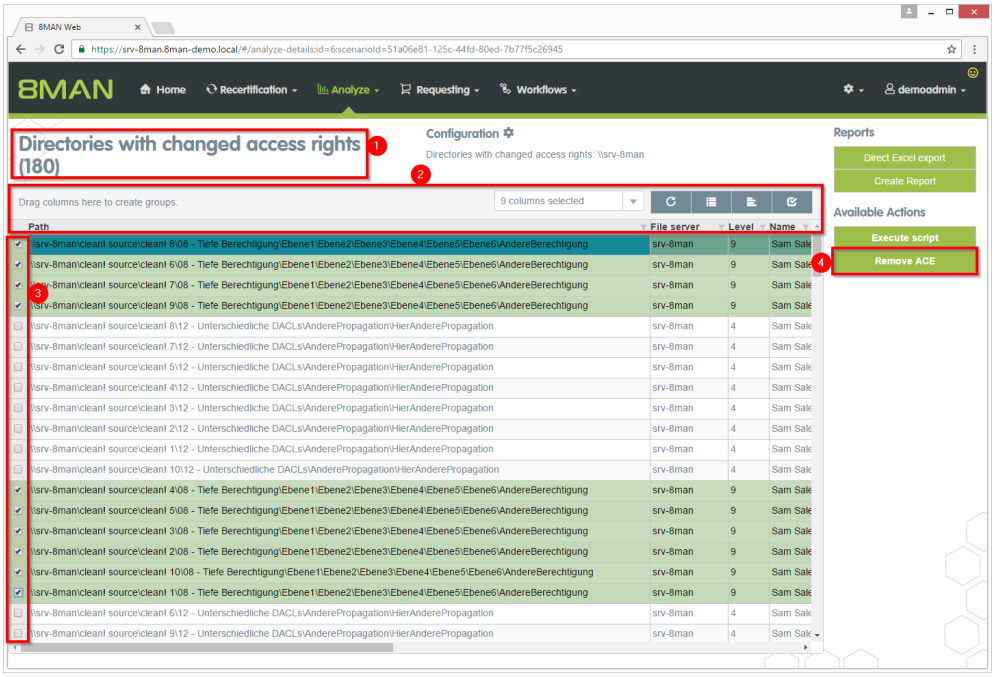
1. *Login to the web client.*



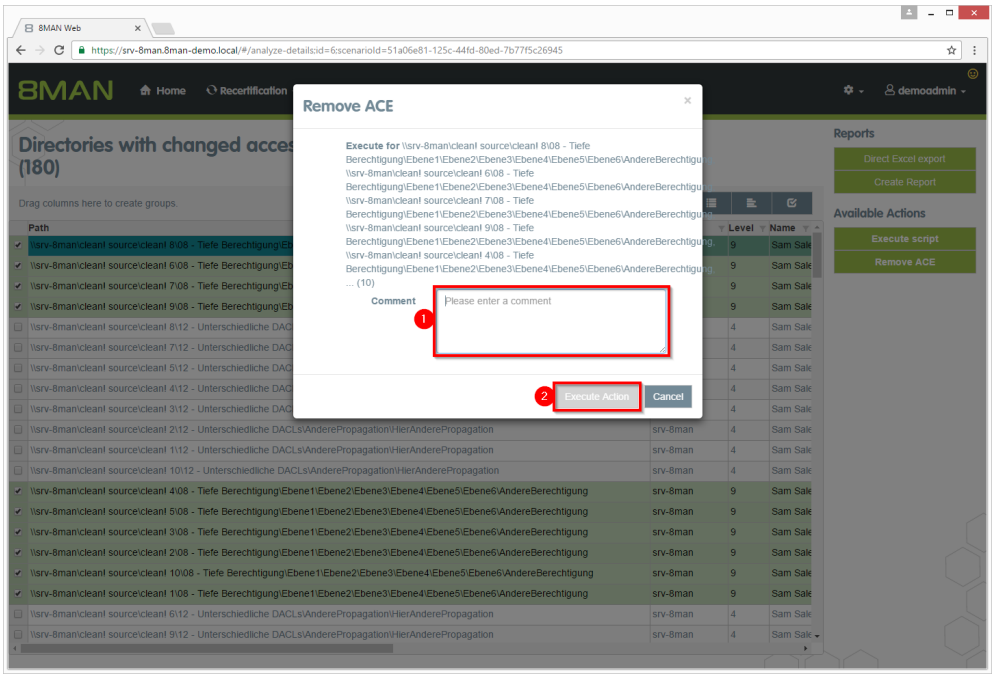
1. *Click on "Analyze".*
2. *Click on "New Analyze Session".*



1. *Click on "Directories with changed access rights".*
2. *Select a file server.*
3. *Start the calculation.*



1. *8MAN lists all directories with differing permissions.*
   8MAN lists differing permissions in directories deeper than level 3 below share.
2. *Use sorting, filtering, grouping and column selection to locate the desired rows.*
3. *Select the desired entries.*
4. *Click on "Remove ACE".*



1. *Leave a comment.*
2. *Click on "Execute Action".*

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

4.2.5 Removing permissions using the webclient

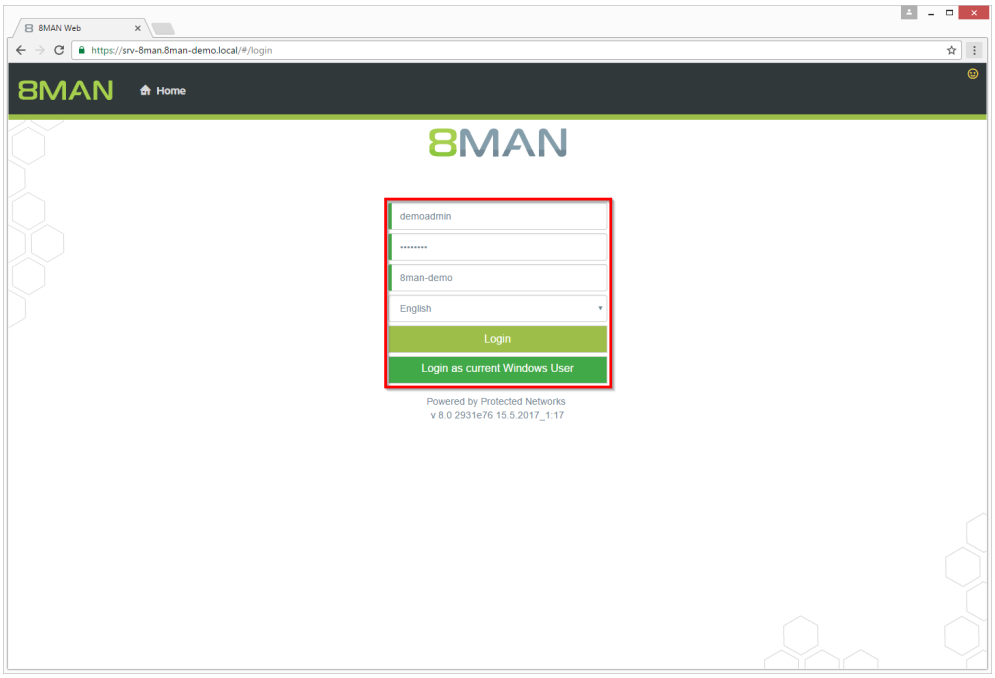
Background / Value

Excessive permissions are everyday business in access rights management. Set manager into the role of a data owner and 8MAN enables them to remove permissions on resources they are responsible for. The web client enables non technical managers to master access rights.

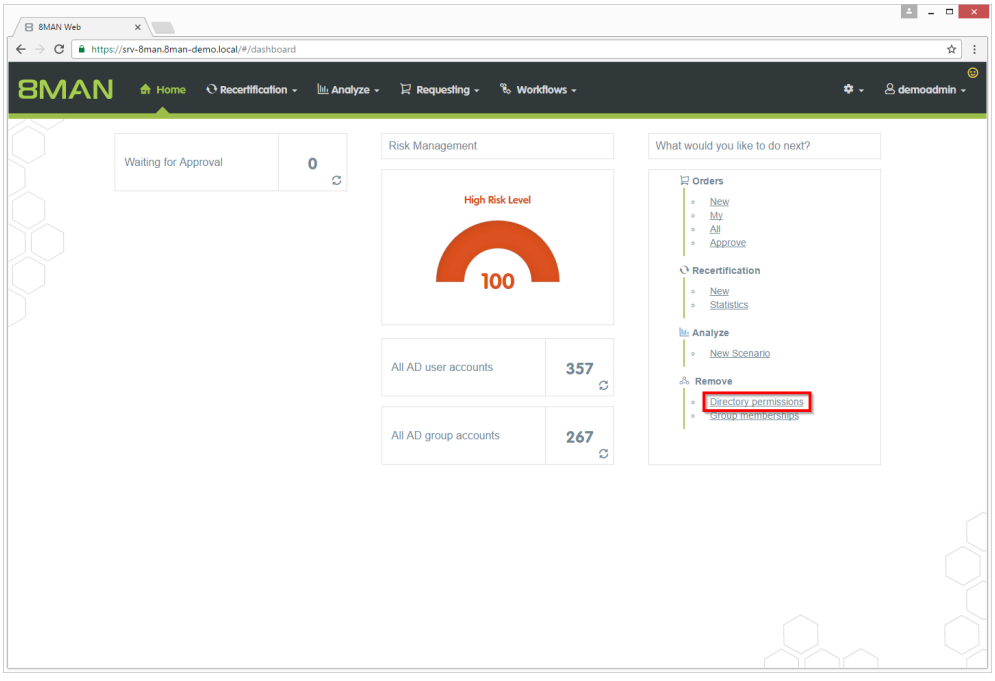
Additional Services

Removing group memberships using the webclient

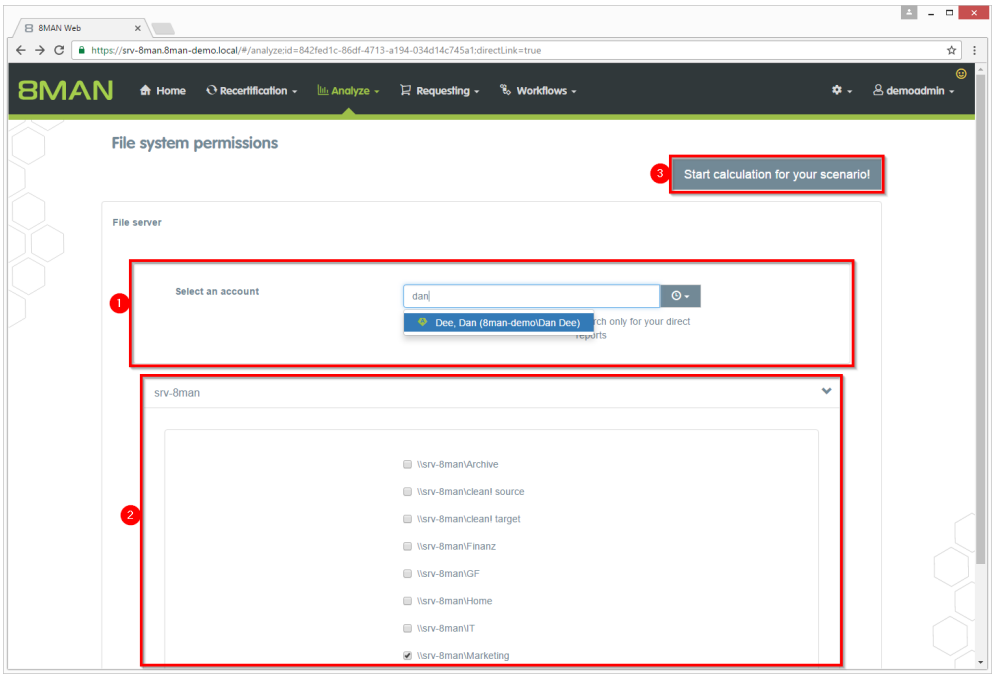
Step by step process



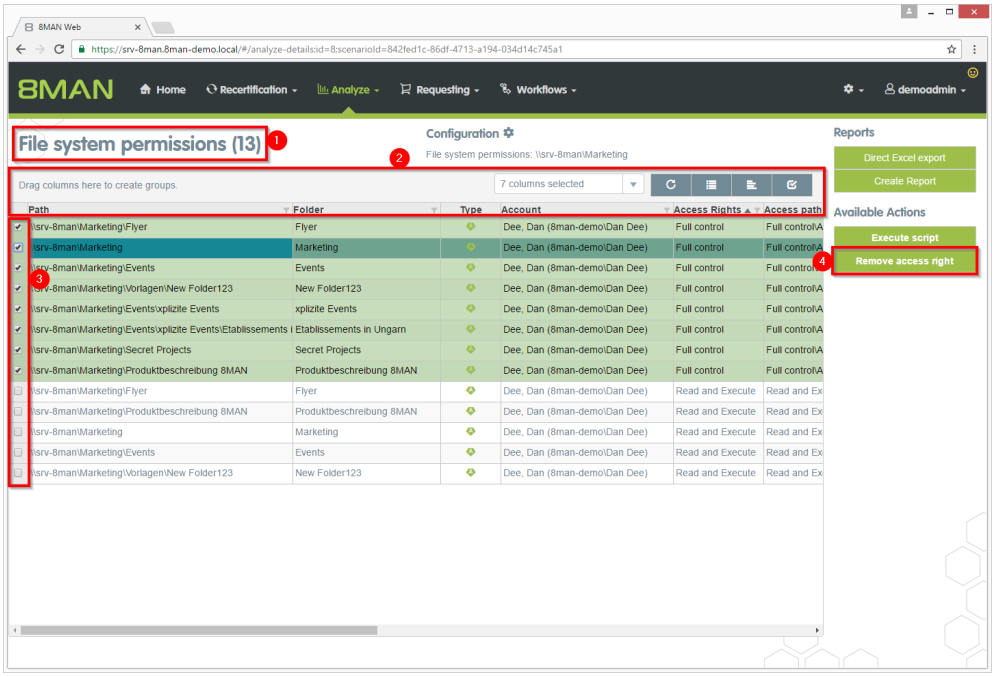
1. *Login to the web client.*



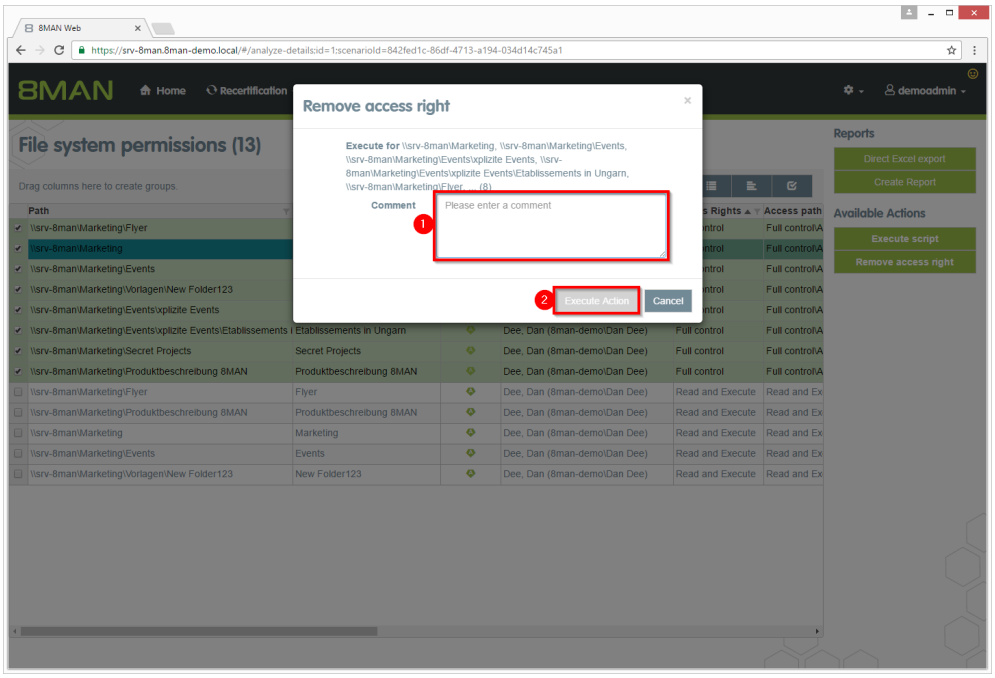
1. *Click on "Directory permissions".*



1. *Optional: Select an account. Leave this field empty to list all accounts with permissions.*
2. *Select at least one resource. Use the configuration module to define resources available to data owners. 8MAN administrators may change all resources.*
3. *Start the calculation.*



1. *8MAN lists all permissions of the previously selected user, shares and their subdirectories.*
2. *Use sorting, filtering, grouping and column selection to locate the desired rows.*
3. *Select the desired entries.*
4. *Click on "Remove access right".*



1. *Leave a comment.*
2. *Click on "Execute Action".*

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

4.2.6 Removing group memberships using the webclient

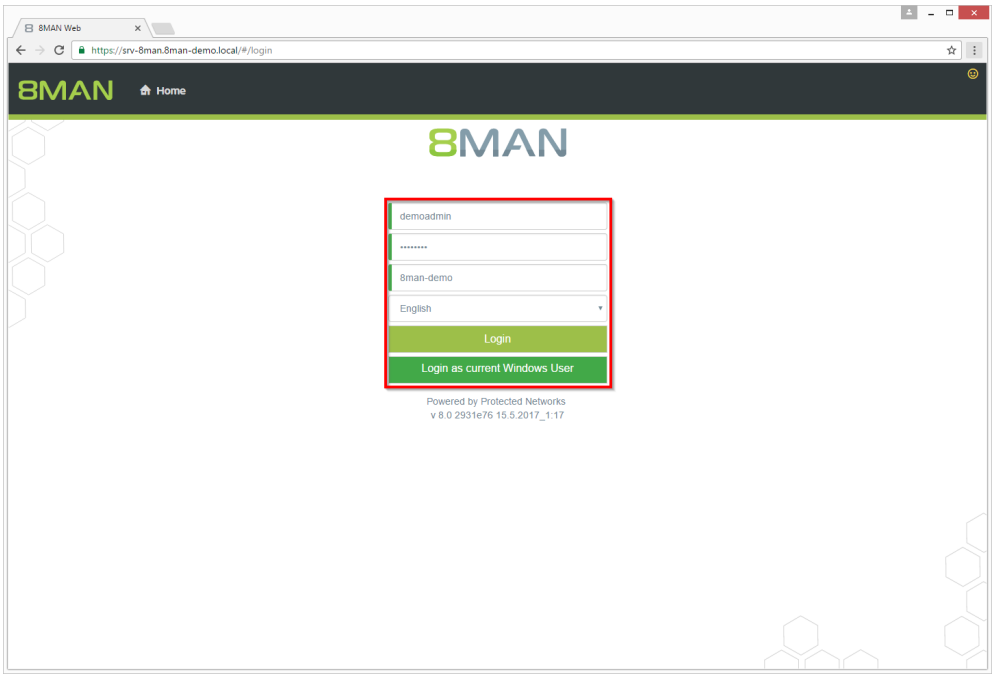
Background / Value

Excessive permissions are everyday business in access rights management. Set manager into the role of a data owner and 8MAN enables them to remove group memberships they are responsible for. The web client enables non technical managers to master access rights.

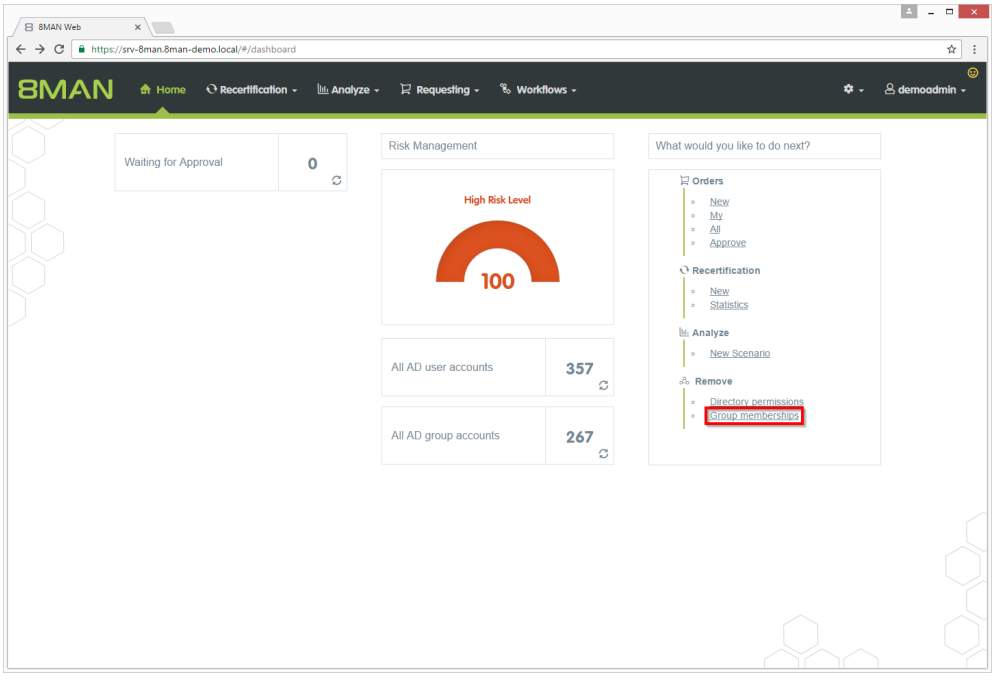
Additional Services

Removing permissions using the webclient

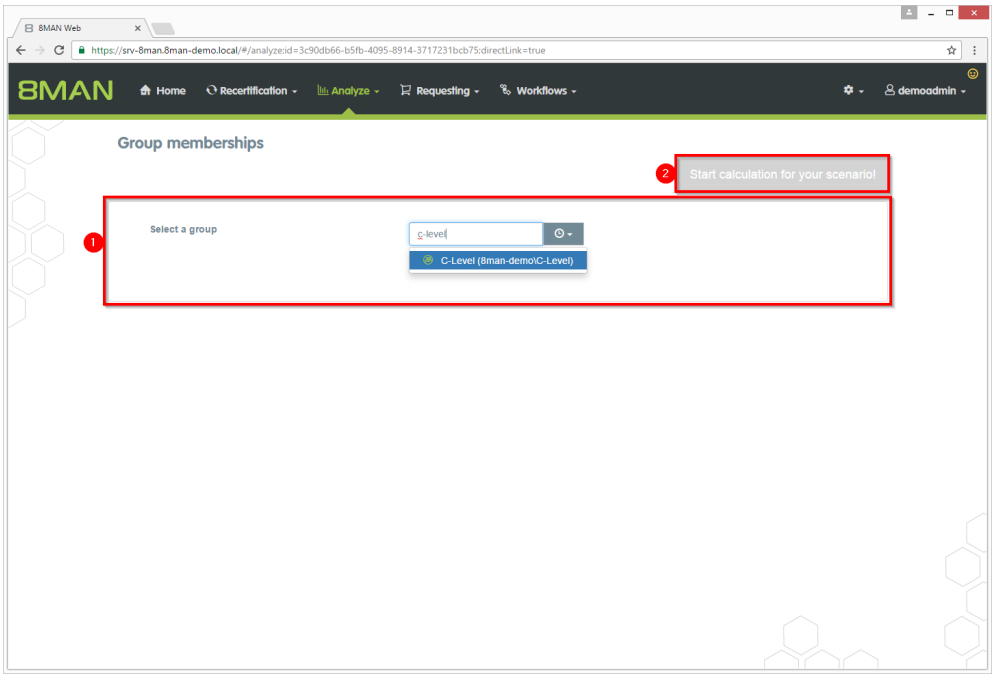
Step by step process



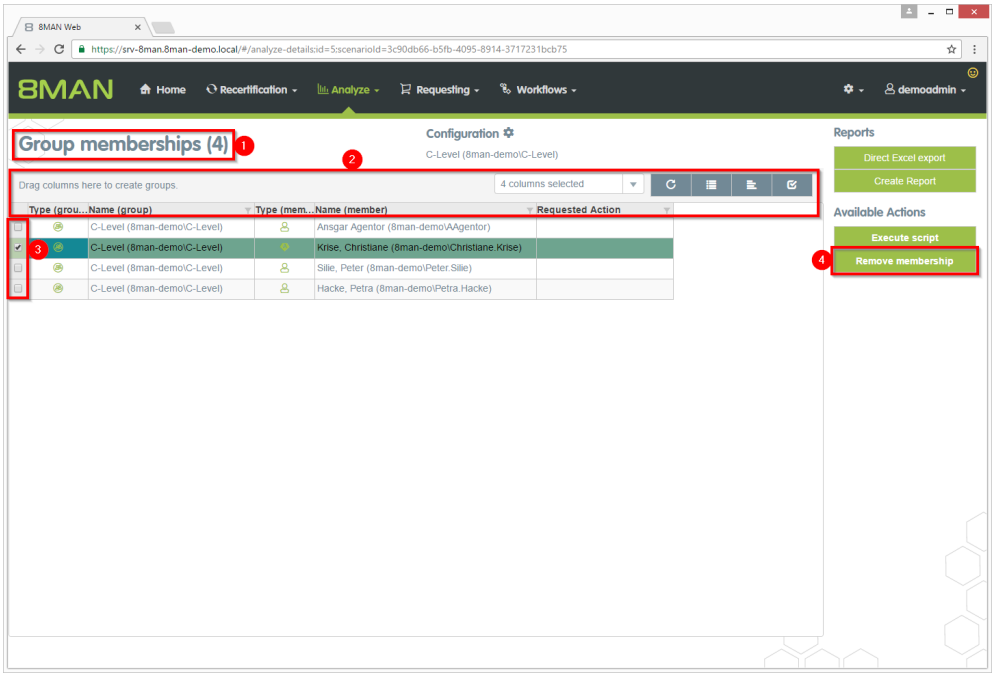
1. *Login to the web client.*



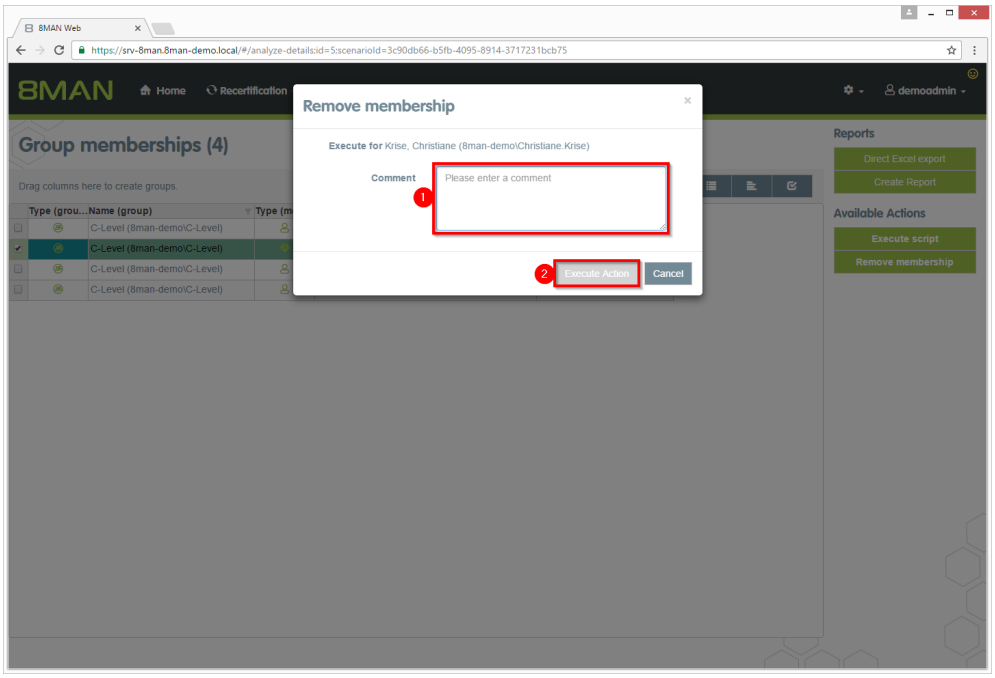
Click "Group memberships".



1. *Find the group from which you want to remove members.*
2. *Start the calculation.*



1. *8MAN lists all members of the previously selected group.*
2. *Use sorting, filtering, grouping and column selection to locate the desired rows.*
3. *Select the desired entries.*
4. *Click "Remove membership".*



1. *Leave a comment.*
2. *Click "Execute Action".*

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

5 Role & Process Optimization

5.1 8MATE GrantMA

5.1.1 Assigning resource owners using the web client

Background / Value

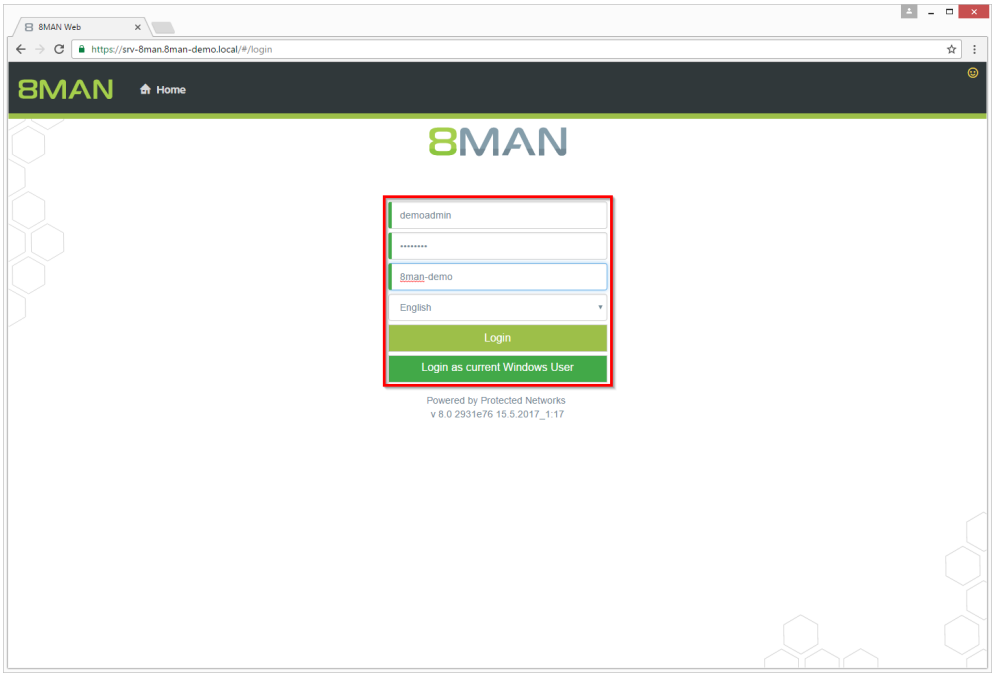
With version 8.0 8MAN releases new features to move the GrantMA configuration into the web client. We inserted the new role "Resource Owner". Assign this role completely using the web client. Due to the requirements of our customers we designed a direct assignment between the Resource Owner and the resource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

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

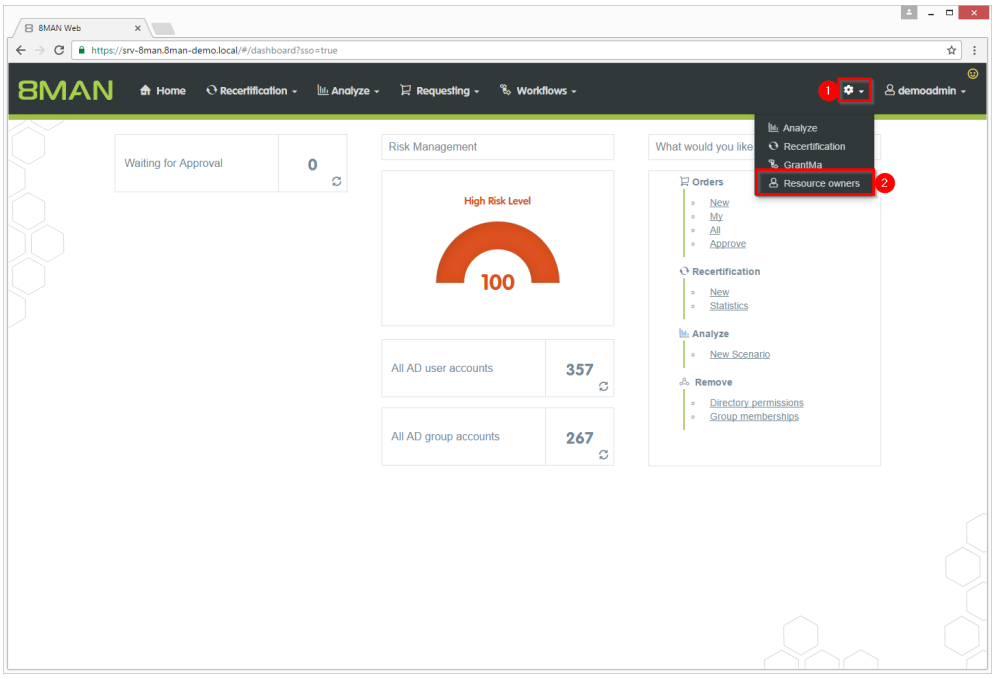
Additional Services

Defining individual approval workflows

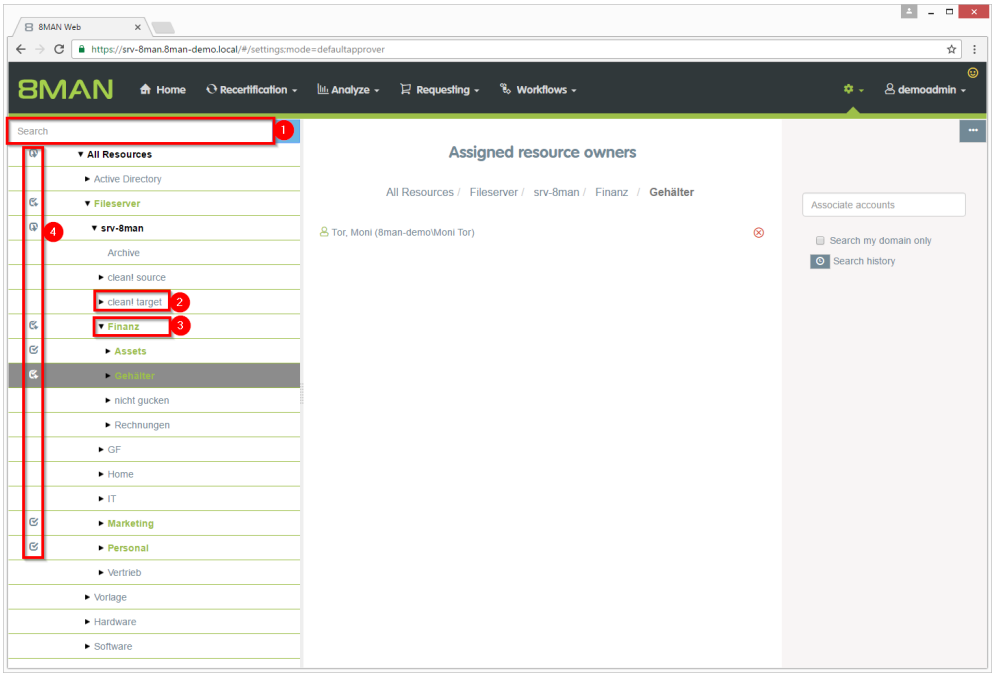
Step by step process



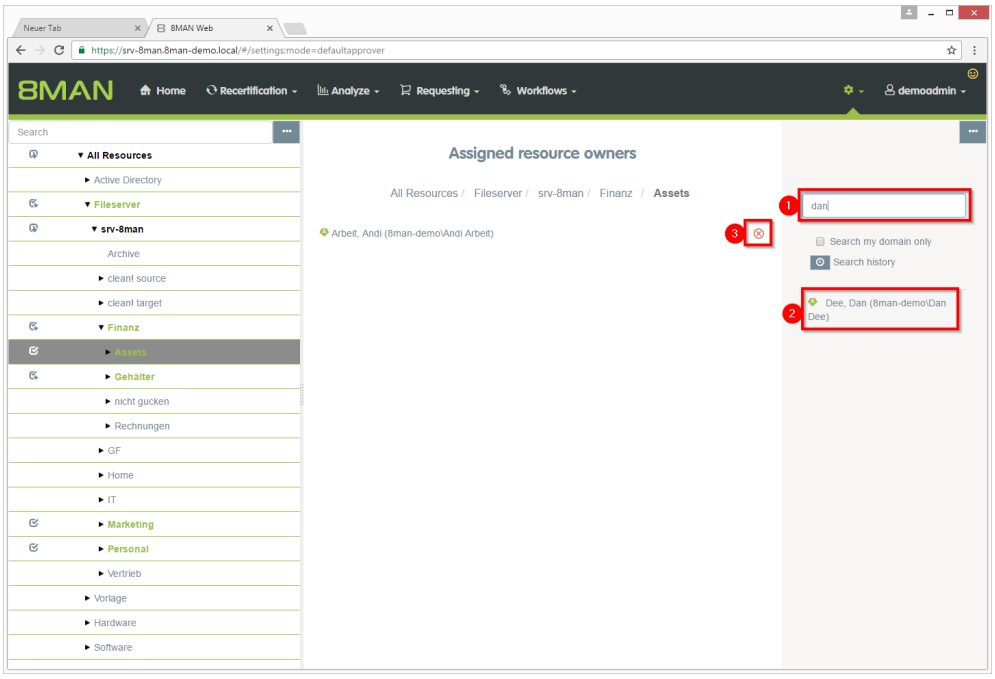
Login to the web interface with admin credentials.



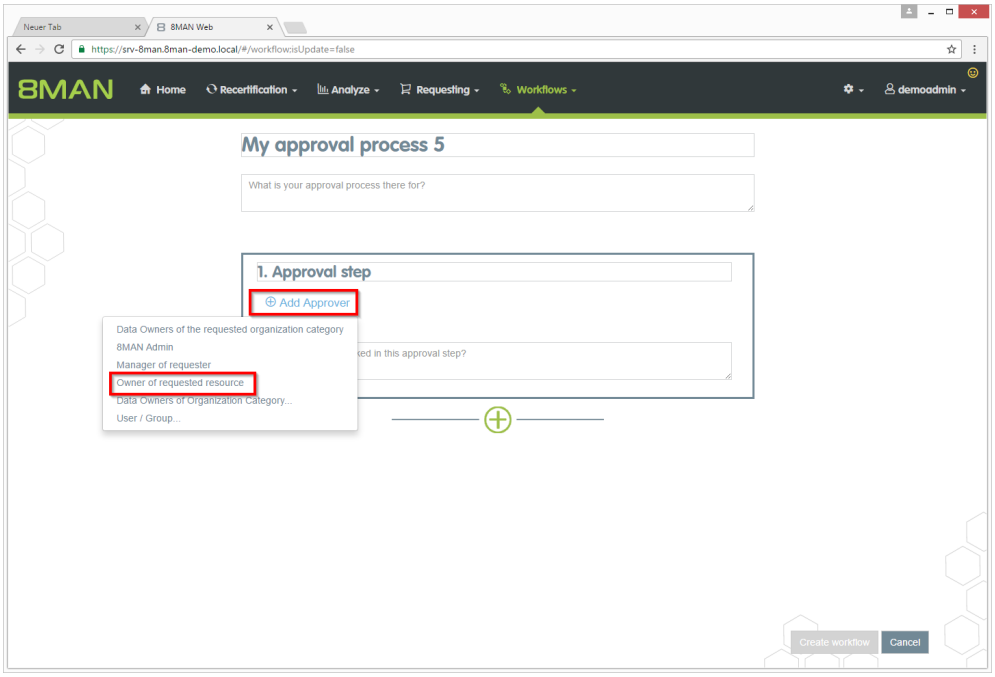
1. *Click the gear-wheel.*
2. *Select "Resource owners".*



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



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



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

5.1.2 Importing and exporting resource owner configurations

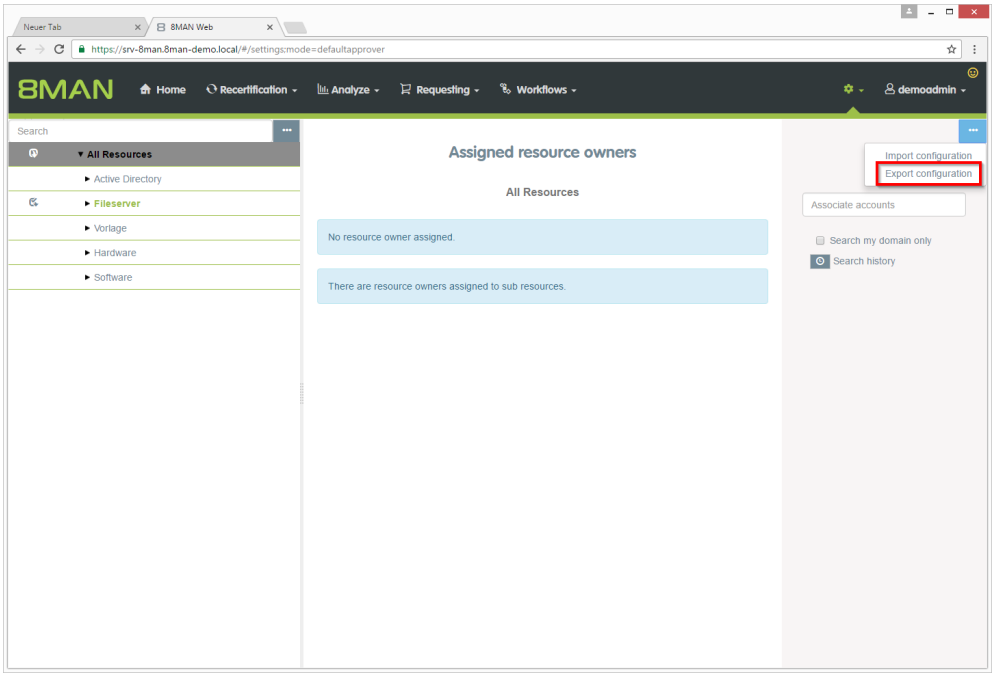
Background / Value

Automate and accelerate the assignment of resource owners by editing a CSV-file. Import/export the assignments to transfer the configuration from one system to another, for example from a testing to a productive environment.

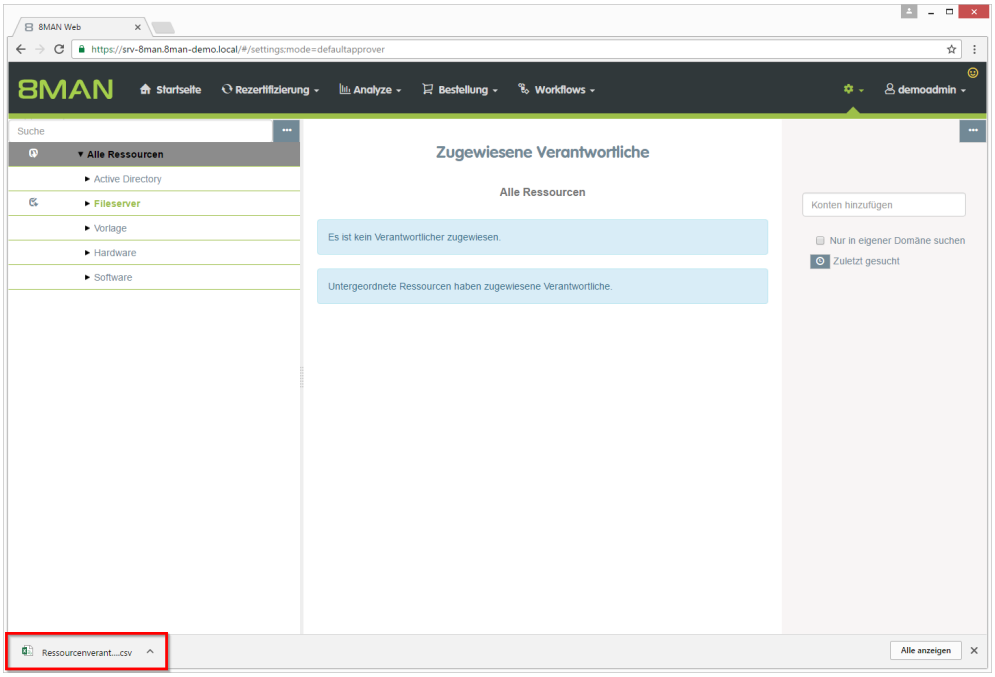
Additional Services

Defining individual approval workflows

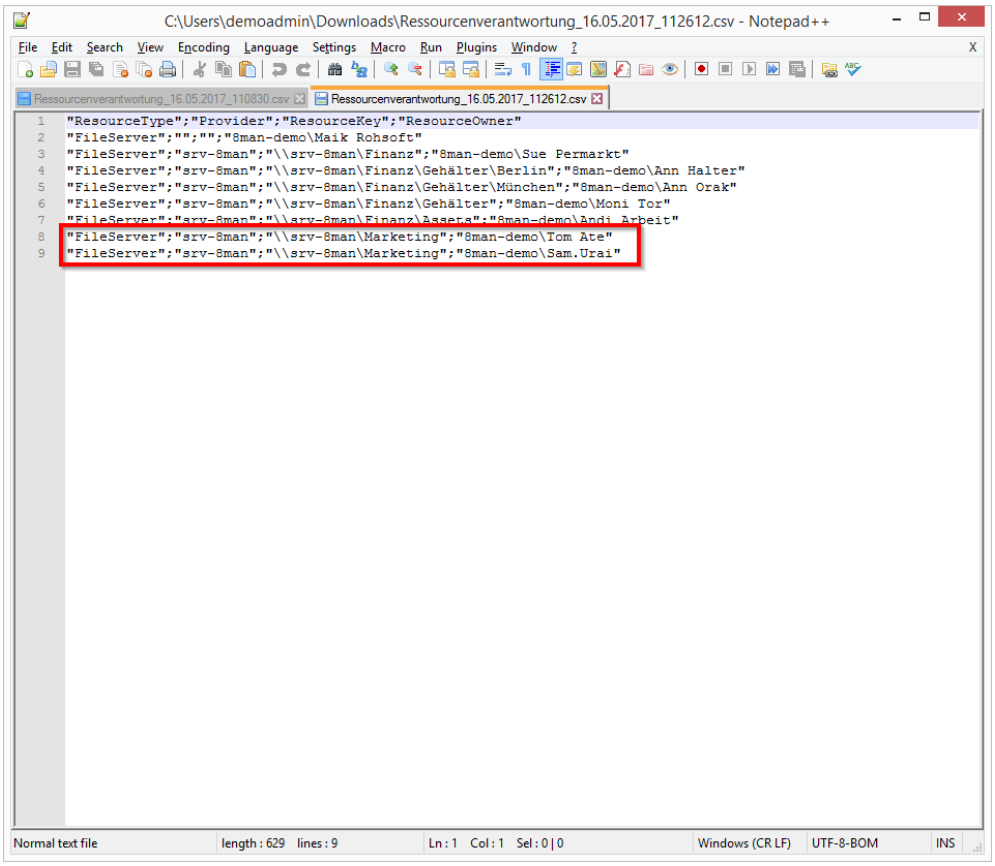
Step by step process



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

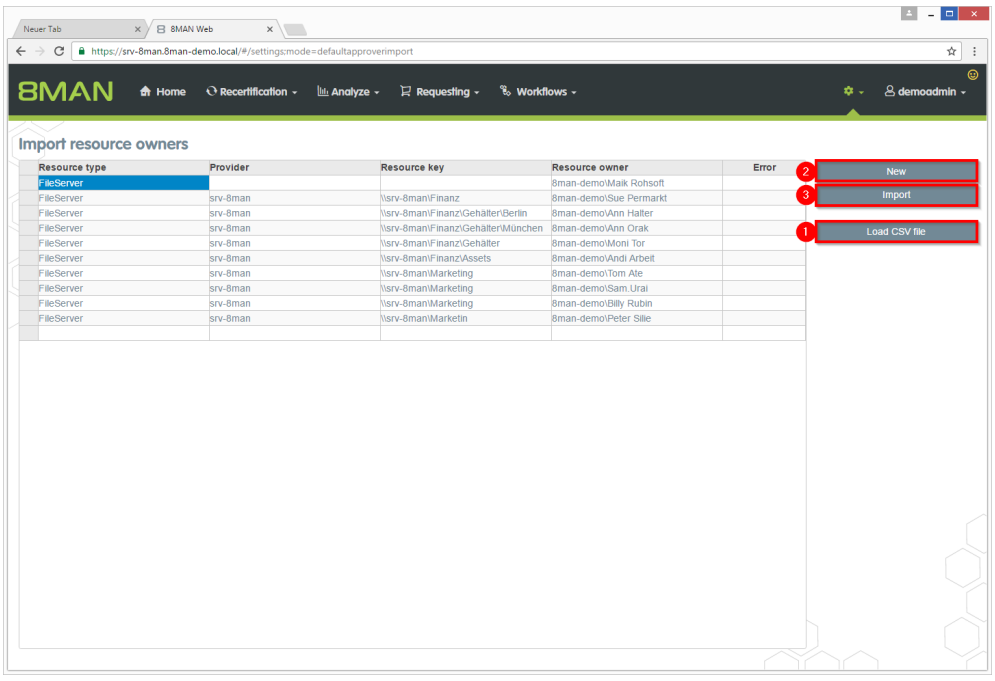


The export file is handled as a download. Displaying and saving of the file depends on the browser.

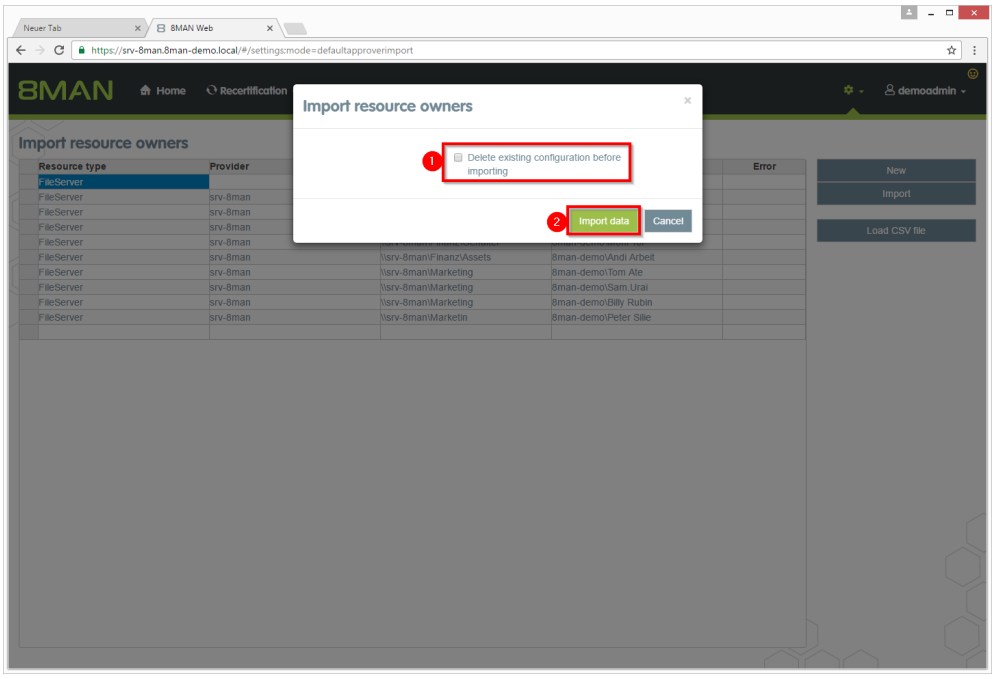


You can edit the CSV-file.

Please note that the assignment is always one-to-one.

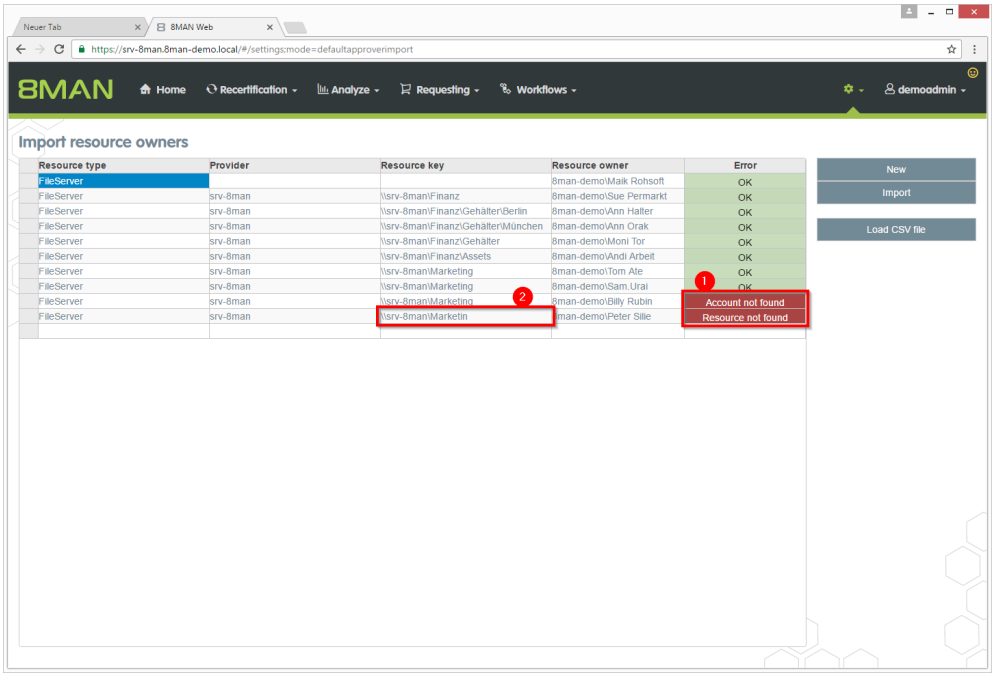


1. *Load a CSV-file.*
2. *Clear the loaded list.*
3. *Click "Import".*



1. ***Option activated:***
   The existing configuration will be deleted before the import.

   Option deactivated:
   The existing configuration will be retained. The import will be added. No duplicates will be generated.
2. *Start the import process.*



1. *8MAN shows you where errors occurred during import.*
2. *Edit the fields of the table to fix small errors immediately.*

5.1.3 Requesting directories

Background / Value

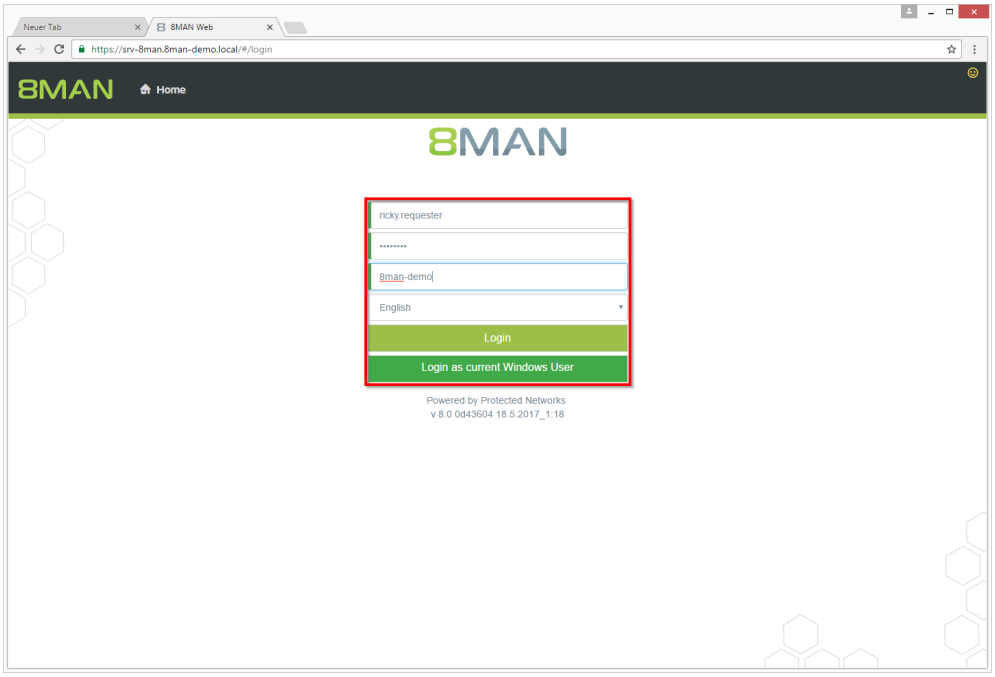
Order new directories using the GrantMA self service portal. This feature is useful for companies that follow restrictive policies for directory creation. We recommend that you allow the creation of directories up to the level three or four below the share only after requesting and approving.

Find resources quickly with the search.

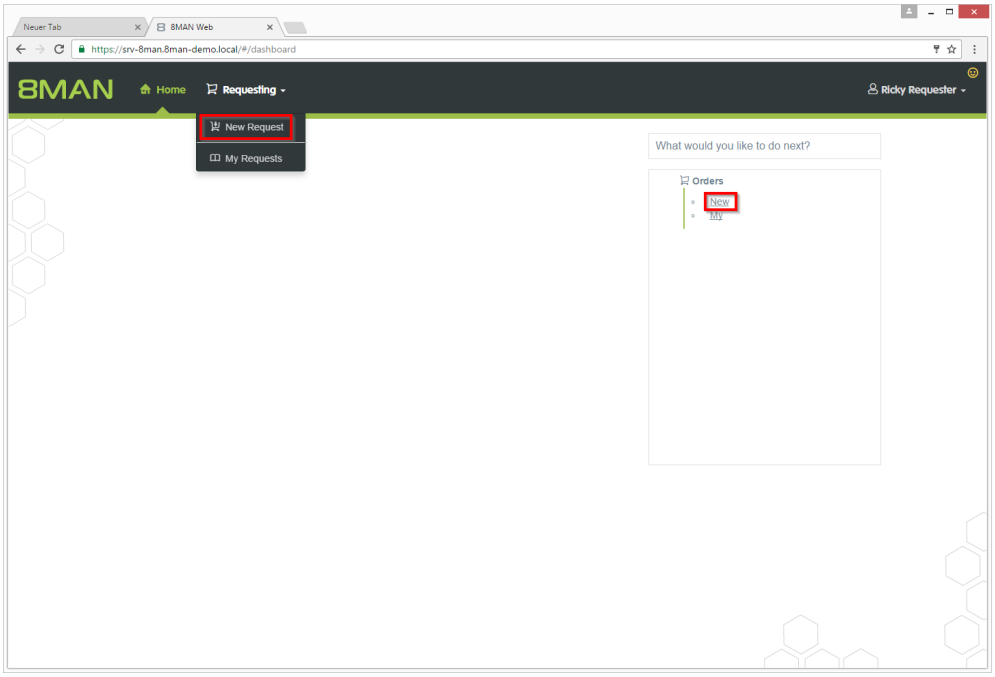
Additional Services

Requesting file server permissions from the data owner

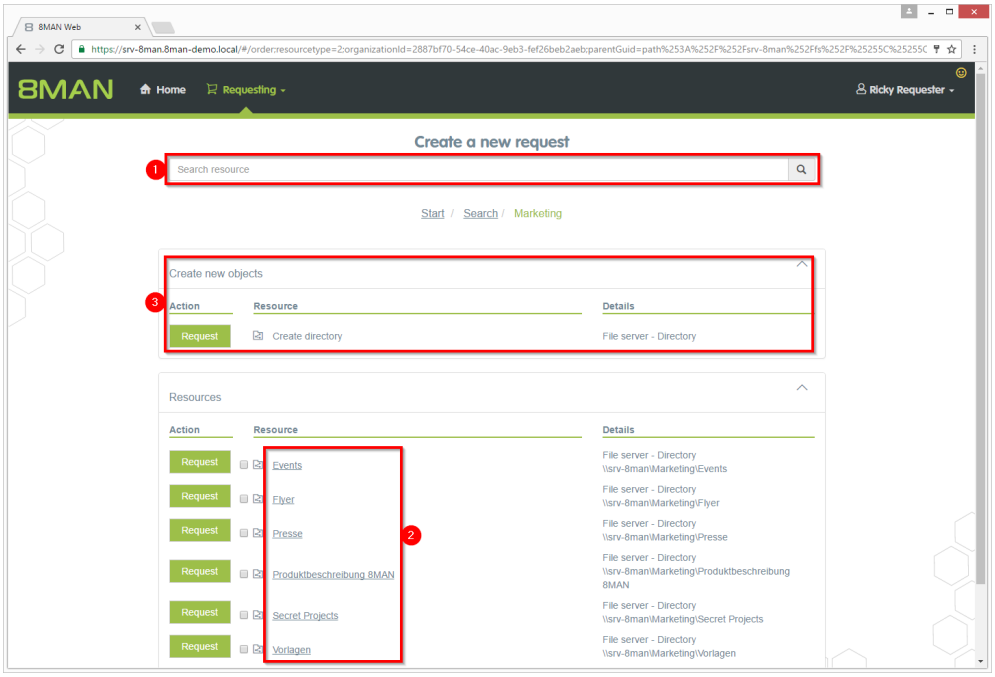
Step by step process



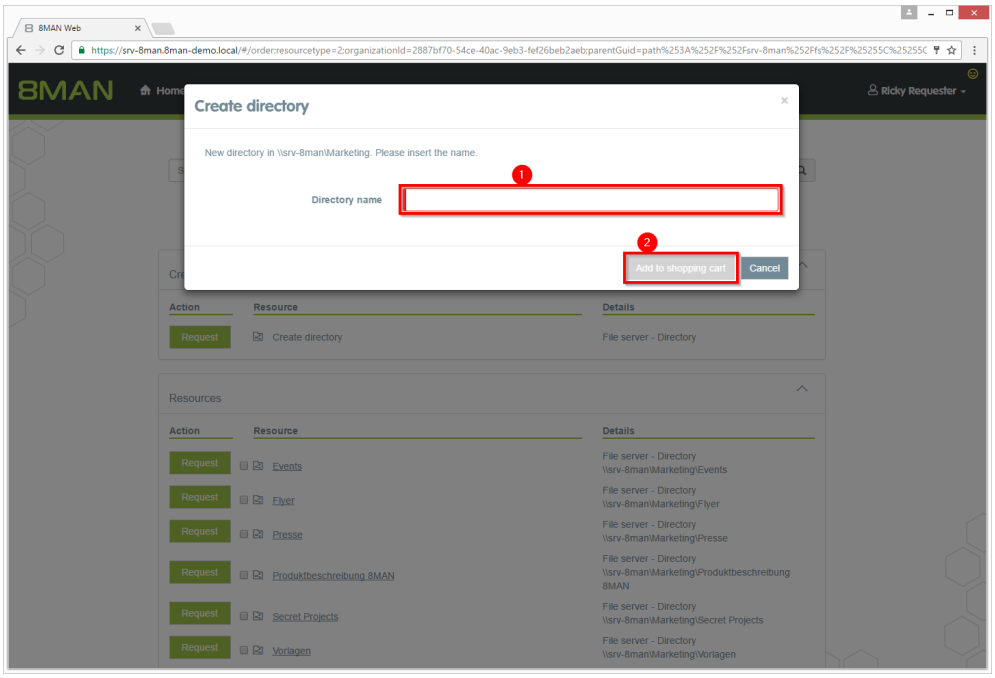
Log in as the requester.



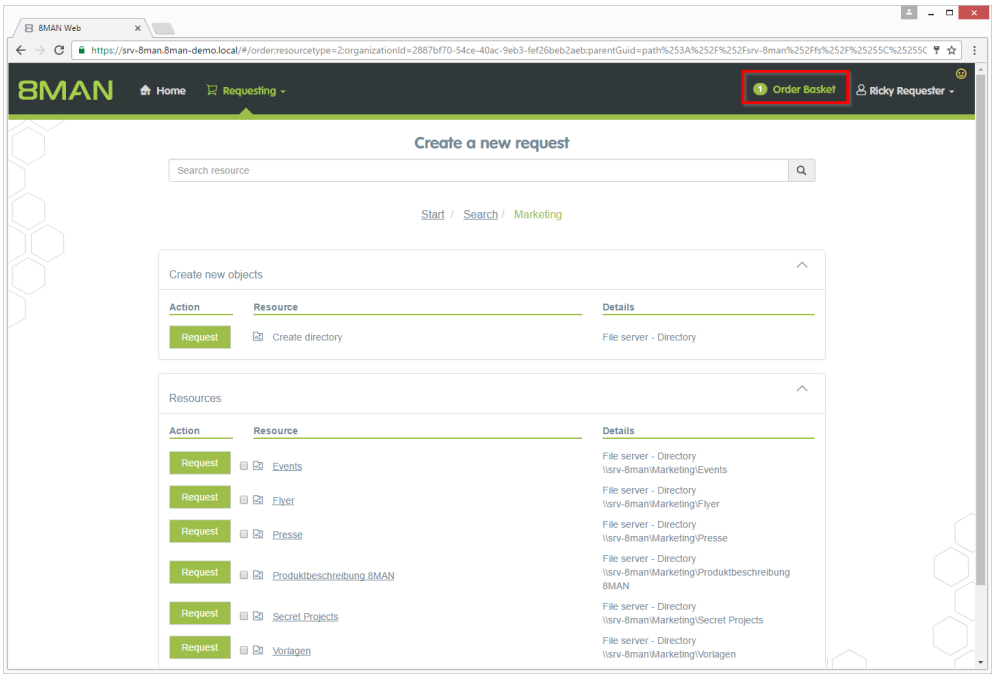
Start a new request.



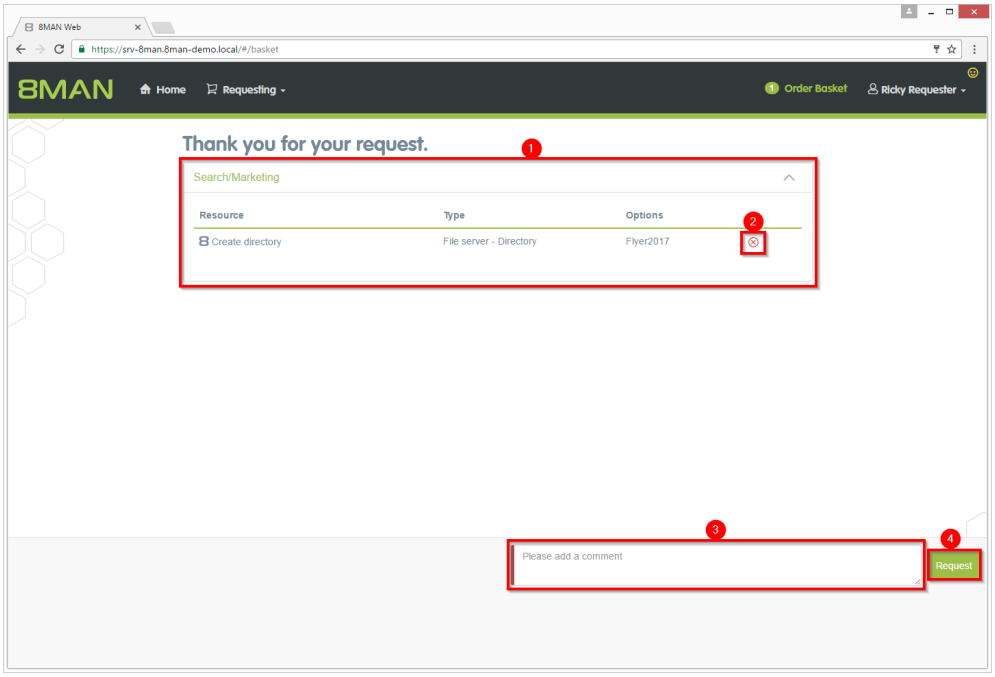
1. *Find the desired resource.*
2. *Alternatively: Navigate to the desired resource.*
3. *Click "Request" in the "Create new objects" area.*



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



Click the shopping cart.

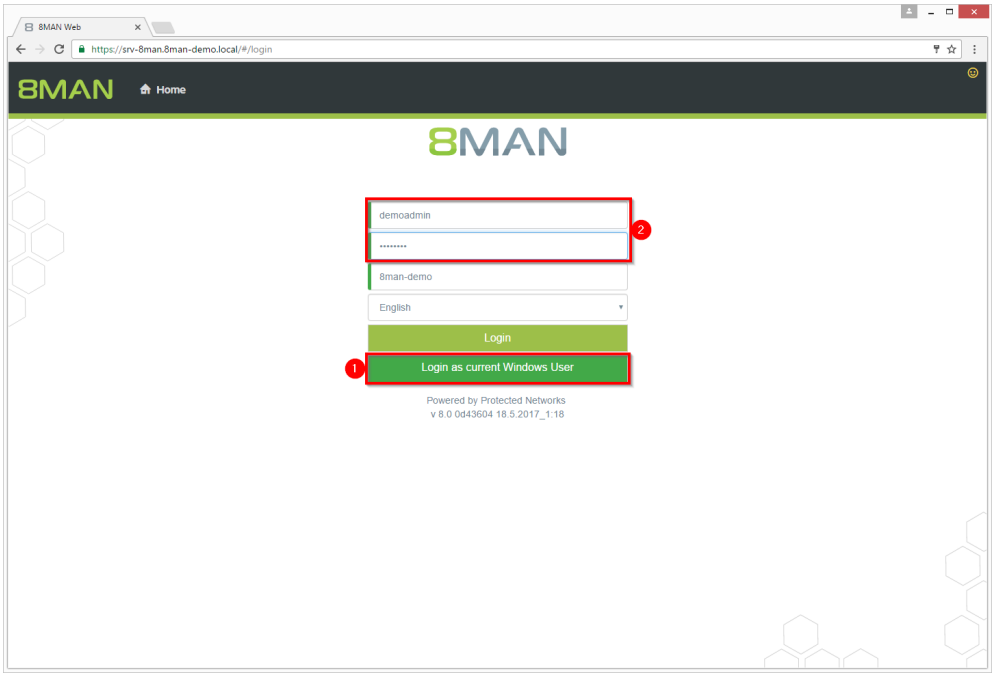


1. *8MAN will show you the order basket with your requests.*
2. *Alternatively, delete your request.*
3. *You must enter a comment, e.g. a ticket number.*
4. *Close your request*.

5.1.4 Single Sign On to the web client

Background / Value

With the version 8.0 we introduce Single Sign On (SSO) for the 8MATE GrantMA. Windows logon information is automatically transferred to the Web client. It is no longer necessary to enter user name and password. This increases the ease of use. Alternatively, other credentials may be used.



1. *Login as current Windows user.*
2. *Login with alternate credentials.*

6 Security Monitoring

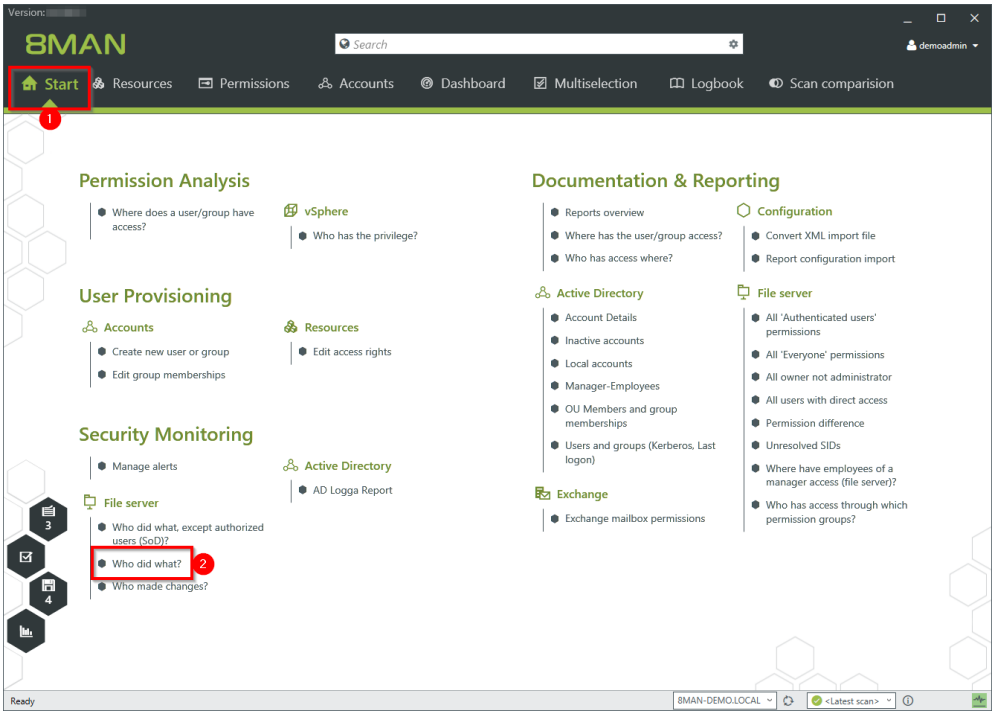
6.1 Scheduling and filtering FS Logga reports

Background / Value

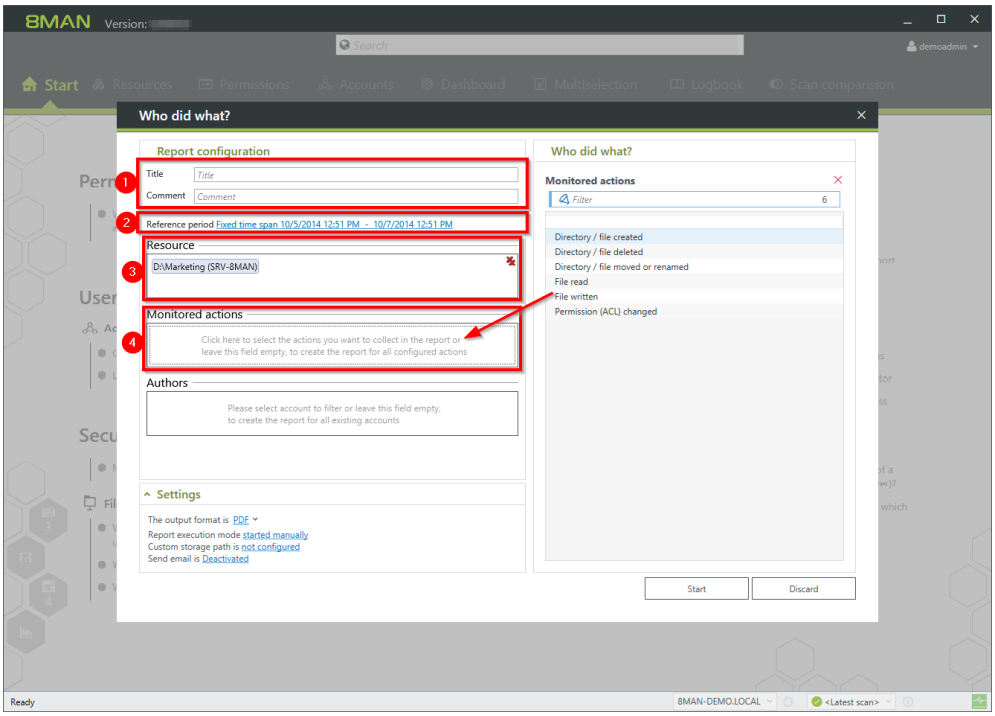
As of version 8.0, the FS Logga reports can be executed in a timed manner. In addition, we have installed additional filter options. In previous versions, filter functions could only be applied to the finished Excel report.

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.

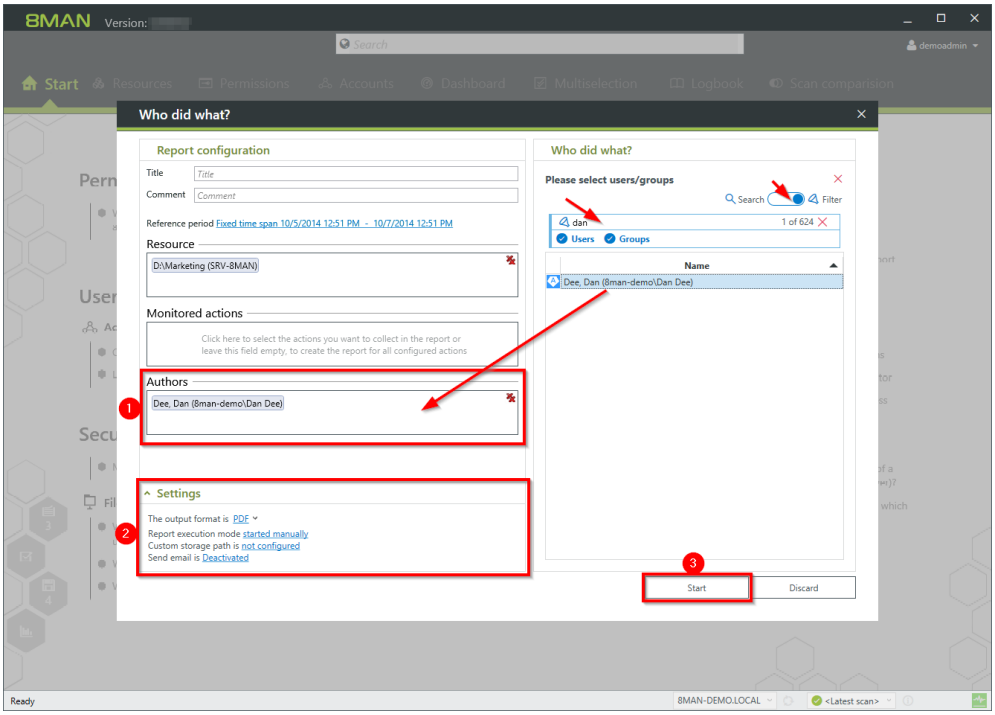
Step by step process



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



1. *Enter a title for the report and add a comment.*
2. *Specify the period of time for logging events in the report.*
3. *Add resources. You can only add resources that are included in the FS Logga configuration.*
4. *Add recorded actions.*



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

6.2 8MATE FS Logga - SSL-support for NetApp C-Mode

The 8MATE FS Logga now supports SSL for NetApp C-Mode.

The system requirements for the FS-Logga have been adapted.

7 8MAN Application Integration

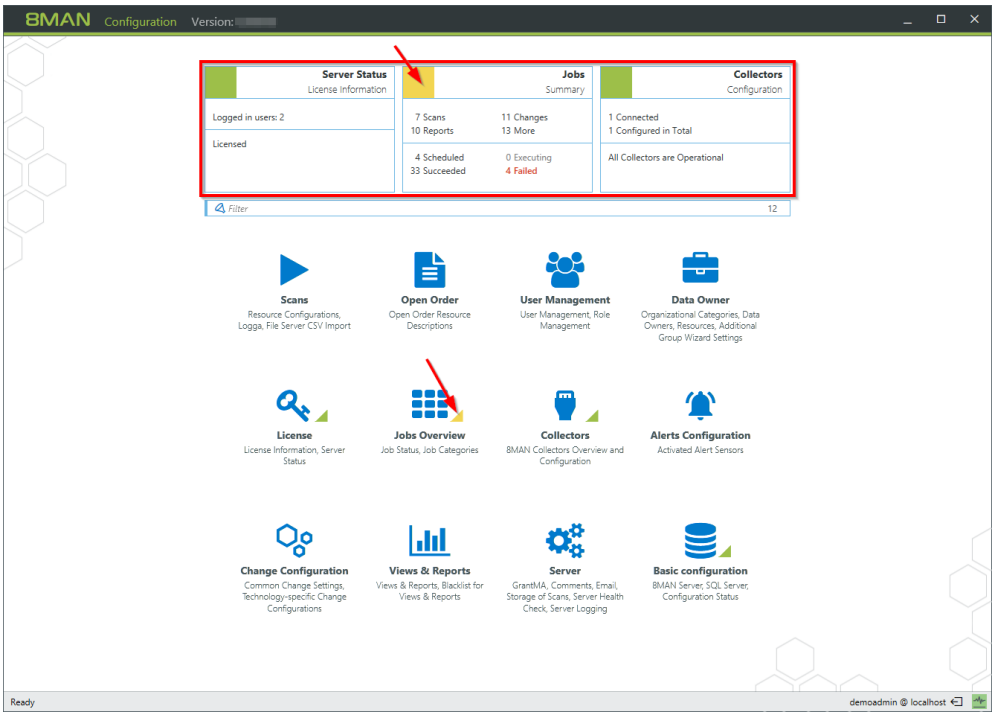
7.1 8MATE Programming Interface

8MAN webAPI supports a new function: "Reset password". The most frequently occurring request to the help desk can now be integrated into ordering systems like "ServiceNow" or "Matrix42".

8 8MAN Konfiguration

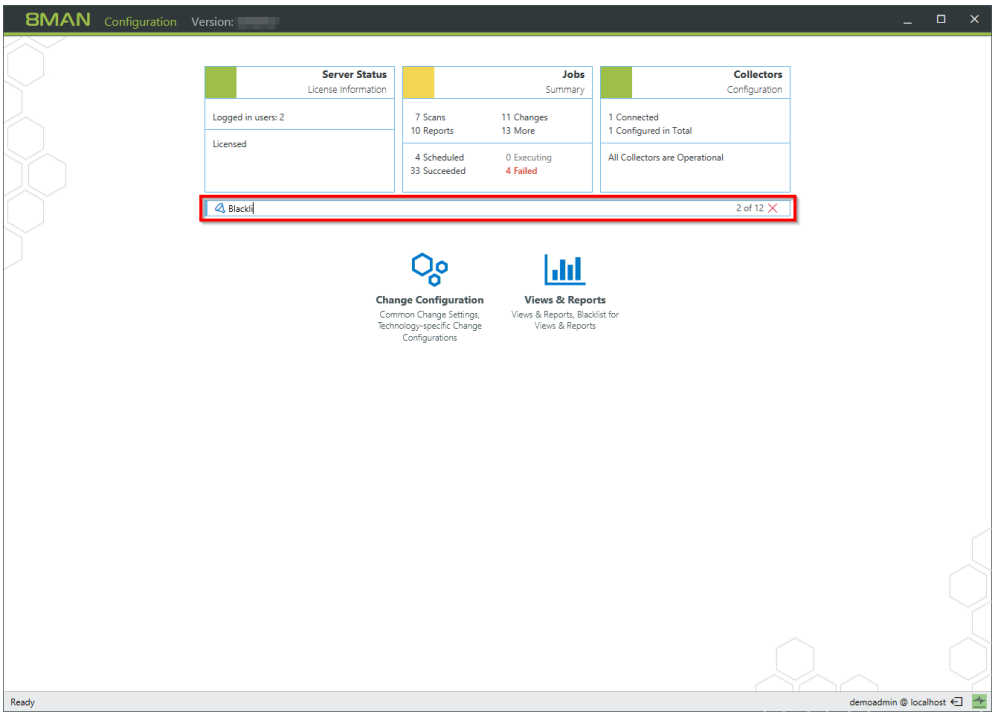
8.1 New homepage layout

The 8MAN configuration homepage and the change configuration will have new layouts and functions.

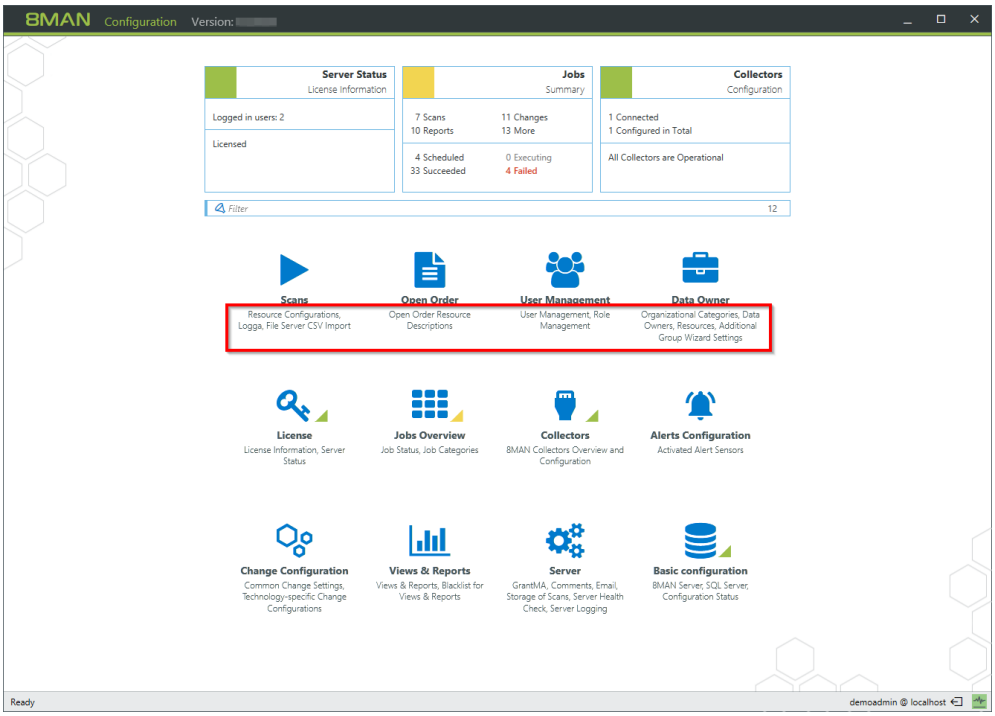


The status information is bundled in the upper tiles.

The colors indicate the current status.



Find the desired setting options quickly with the new filter function.



The new descriptions of the categories show you which settings are included.

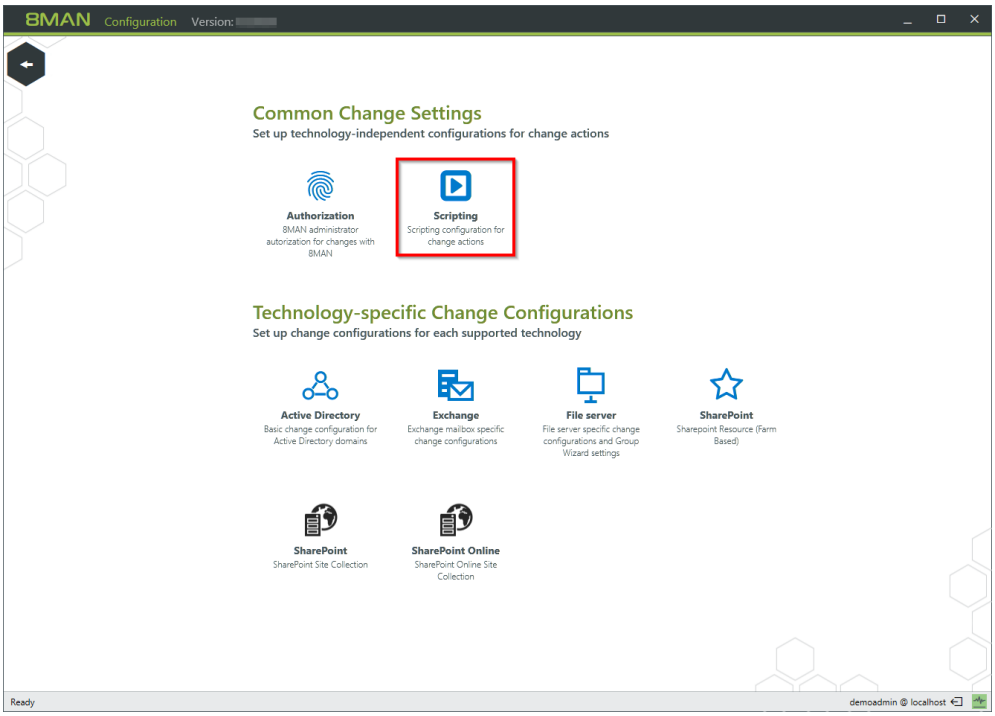
8.2 Configuring scripts

Scripts must be stored in the following directory:

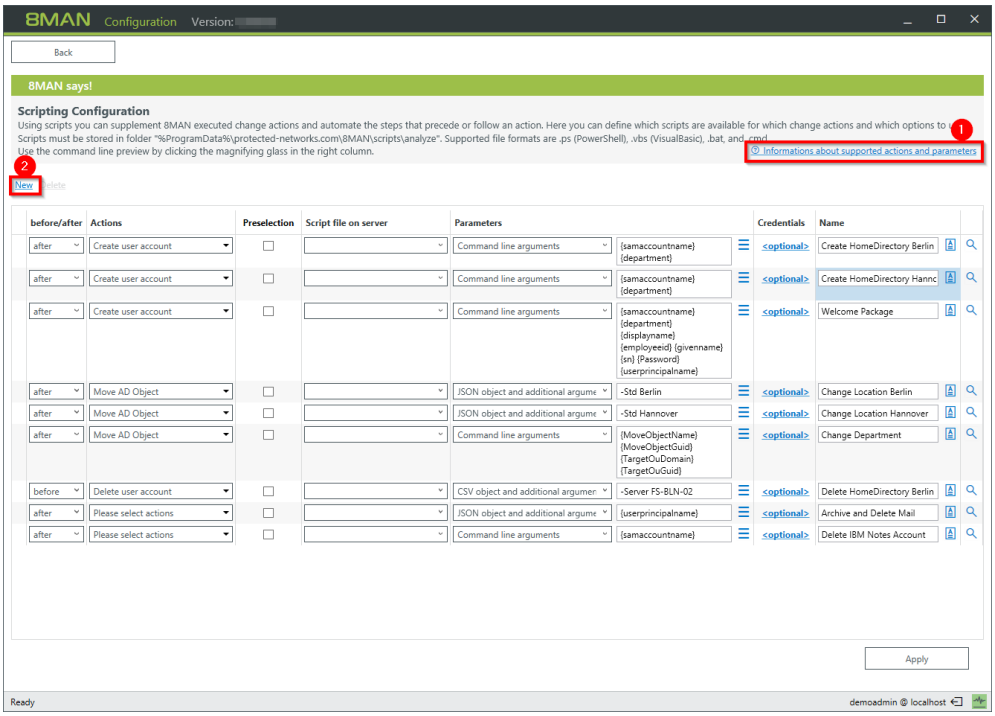
%ProgramData%\protected-networks.com\8MAN\scripts\analyze

Supported file types are:

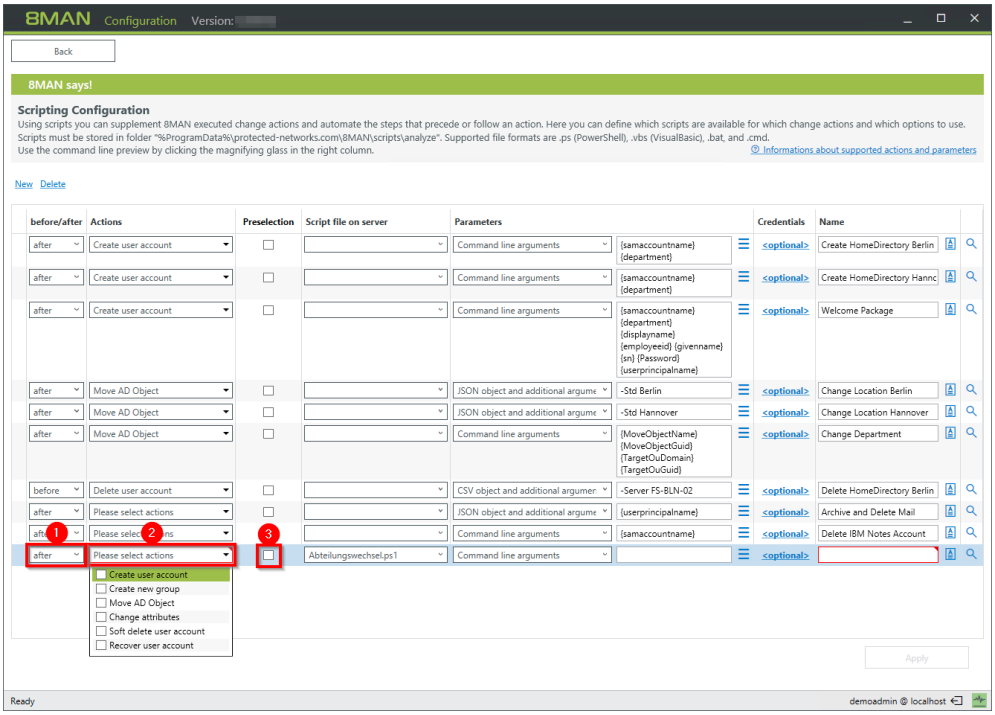
- .ps (PowerShell)
- .vbs (VisualBasic)
- .bat
- .cmd
- .js (nodejs.exe)
- .exe



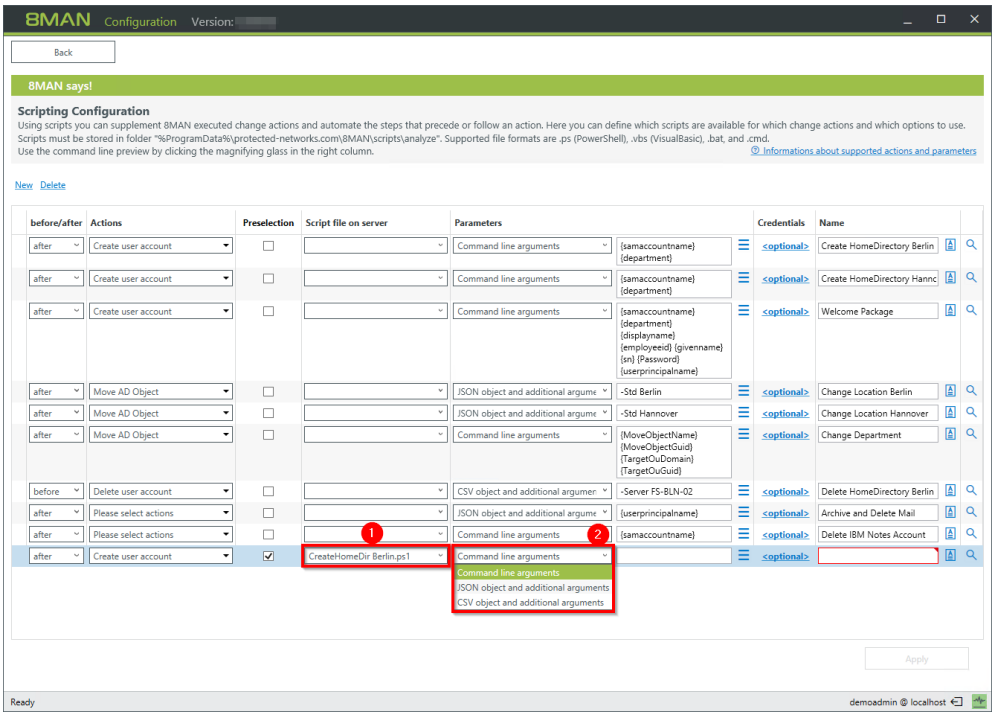
Navigate to "Change-Configuration" -> "Scripting".



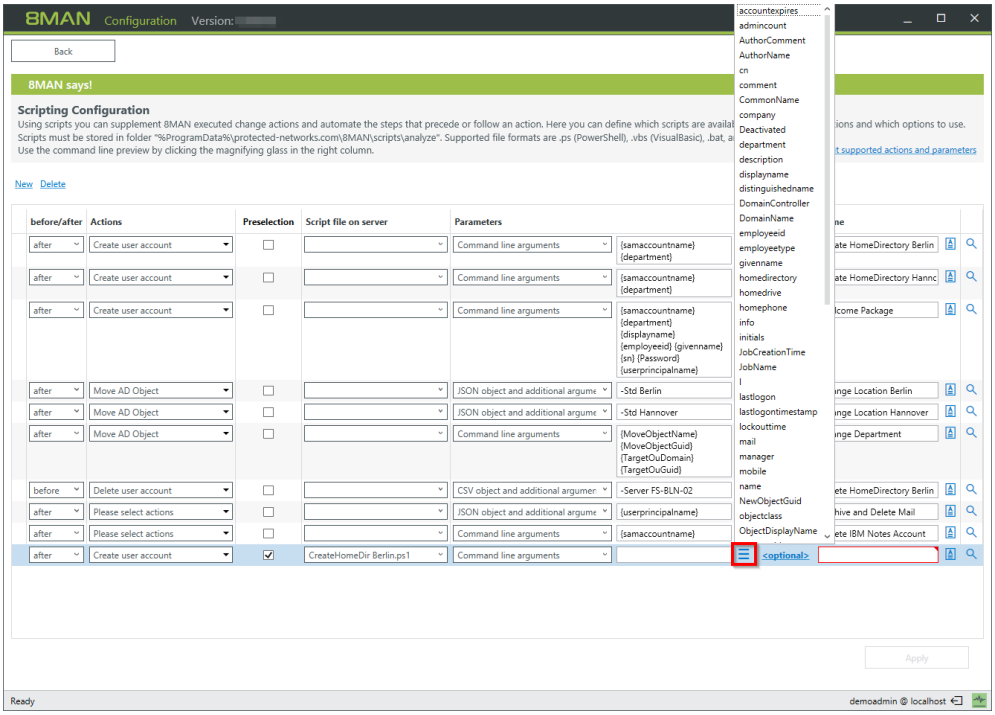
1. *8MAN shows you a list of all the supported change actions before or after which scripts can be executed, as well as available parameters.*
2. *Create a new script configuration.*



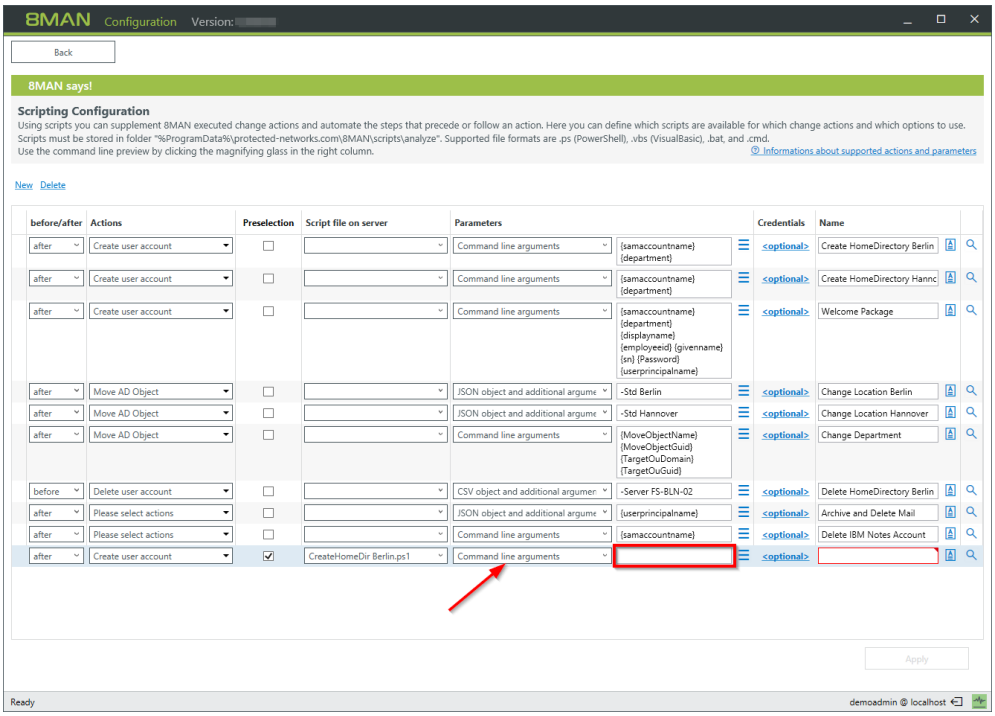
1. *Select whether to run the script before or after the action. The selection filters the available actions (column 2).*
2. *Select an action for which you want to make a script available.*
3. *If you have several scripts available for an action, specify the default settings for the 8MAN users in the drop-down menu.*



1. *Select a script file.*
2. *Select how 8MAN passes the parameters to the script. You can select the parameters directly or pass them as JSON or CSV objects.*



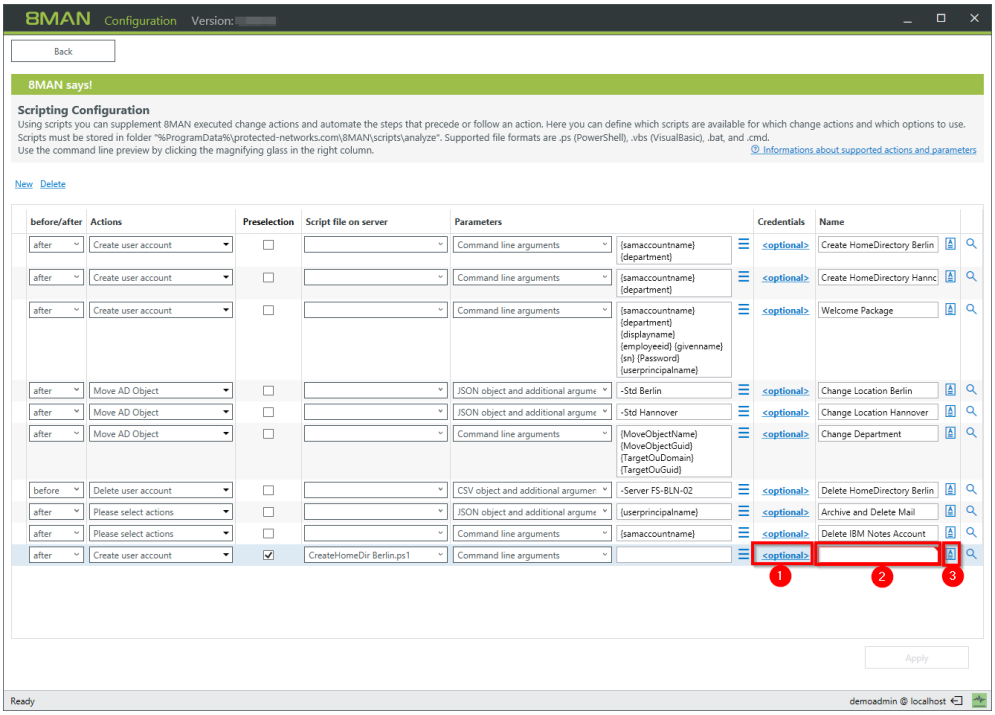
Select the command line parameters.



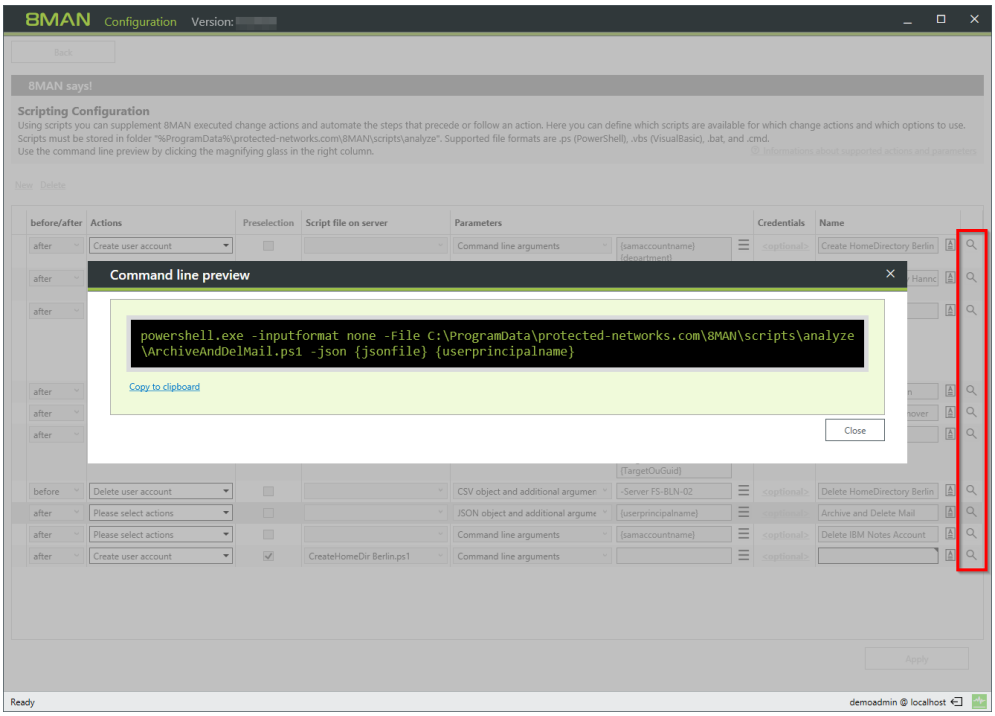
Select the type of data transfer to the script. Using a JSON or CSV object as a selection causes the script to provide a temporary file that contains the object data in the selected format.

For information on the available parameters in the CSV / JSON objects, please contact support.

Use the command line preview for a detailed view of passing.



1. *Specify credentials to run the script. If you do not specify any, the credentials from the base configuration are used.*
2. *Give the script assignment a unique name for the selection in the 8MAN user interface.*
3. *Leave a description.*



Get a command line preview at any time.

8.3 Configuring the SharePoint Remote Connector

With the 8MATE for SharePoint, you can integrate SharePoint as a resource into 8MAN Access Rights Management.

For a transitional period, we offer two SharePoint modules in version 8.0, which can also be operated simultaneously:

1. Previous 8MATE for SharePoint

- uses the Server Side Object Model (SSOM)
- Requires a local installation on the SharePoint server
- Supports only the SharePoint versions 2010 and 2013 (on premise)
- Is no longer supported with the 8MAN version 8.5

2. 8MATE for SharePoint with SharePoint Remote Connector

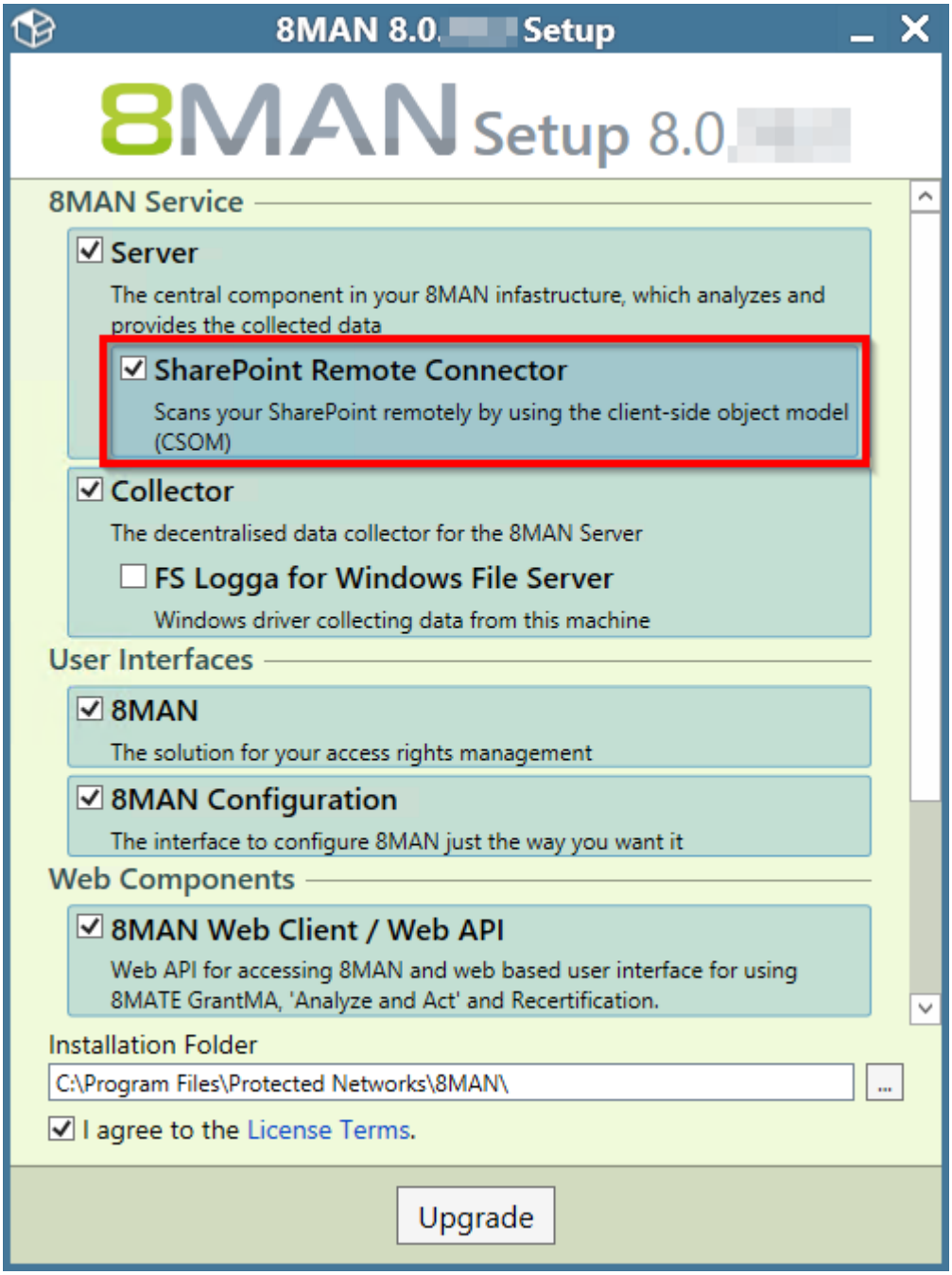
- uses the Client Side Object Model (CSOM)
- No installation on the SharePoint server is required
- Supports SharePoint versions 2010, 2013, 2016, and SharePoint Online

For the 8MATE for SharePoint you need an appropriate license. The section "Load the product license" describes how to check the license scope and, if necessary, reload a license file.

The system requirements must be fulfilled. See Chapter "SharePoint requirements".

For an overview of the required access rights, please refer to chapter "Setting up service accounts for 8MAN".

8.3.1 Installing the SharePoint Remote Connector



Enable the SharePoint Remote Connector.

You install an additional 8MAN server component. No additional installation of dedicated collectors is required.

8.3.2 Accounts for a SharePoint scan via Remote Connector

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

1. "Process Account"

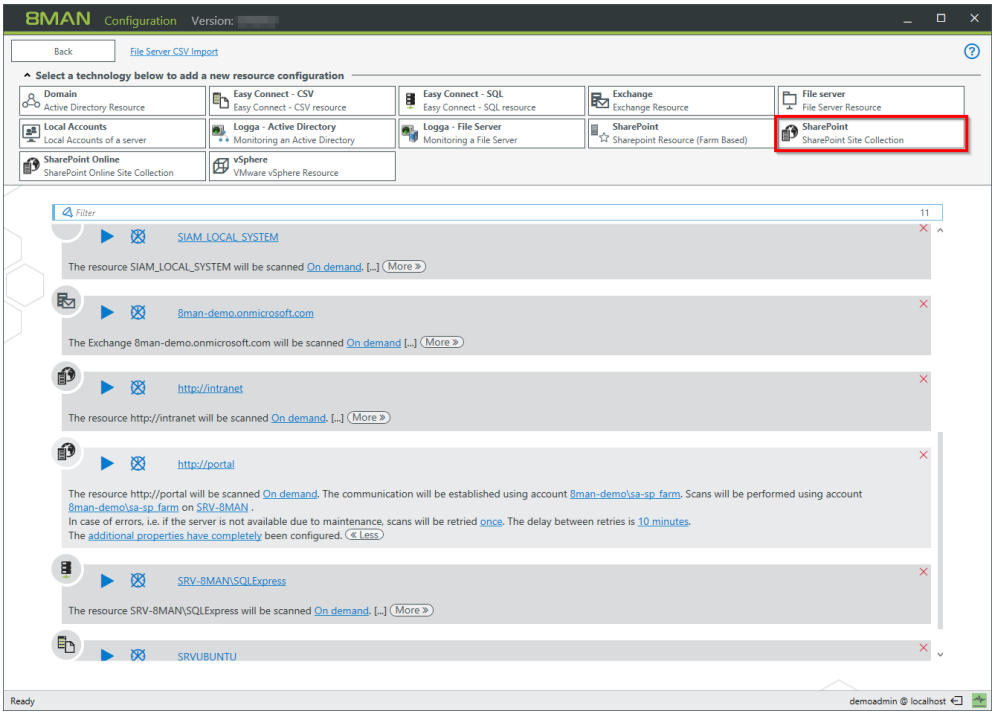
The "Process account" is used to execute the scan process on the selected collector. This account must have local administrative rights and interactive logon privileges on the collector.

2. "Scan Account"

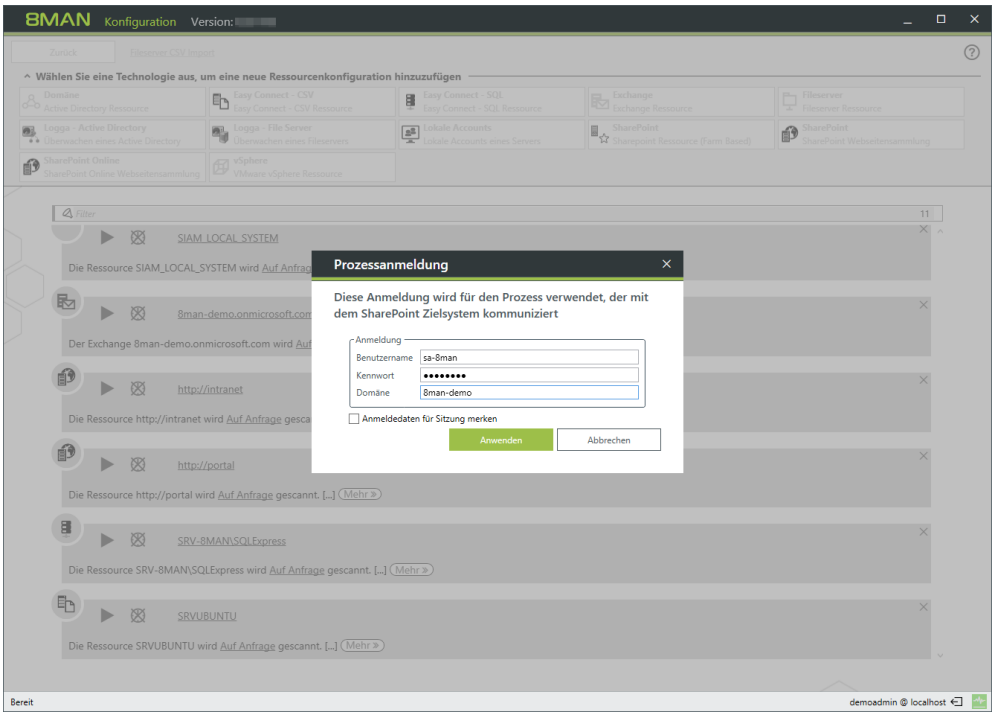
The "scan account" is used for the actual scan. This account must always be the same as the owner account registered for the site collection (= primary site collection administrator). The corresponding user account is defined when a site collection is created and can only be viewed or changed via the SharePoint central administration.
Navigate in the Central Administration to:
application management -> site collections -> Change site collection administrators -> Selection of the site collection -> Primary site collection administrator

If the primary site collection administrator's credentials are not accessible, other SharePoint accounts can also be used for the scan. Please contact our support team in these cases.

8.3.3 Adding a SharePoint Scan via Remote Connector



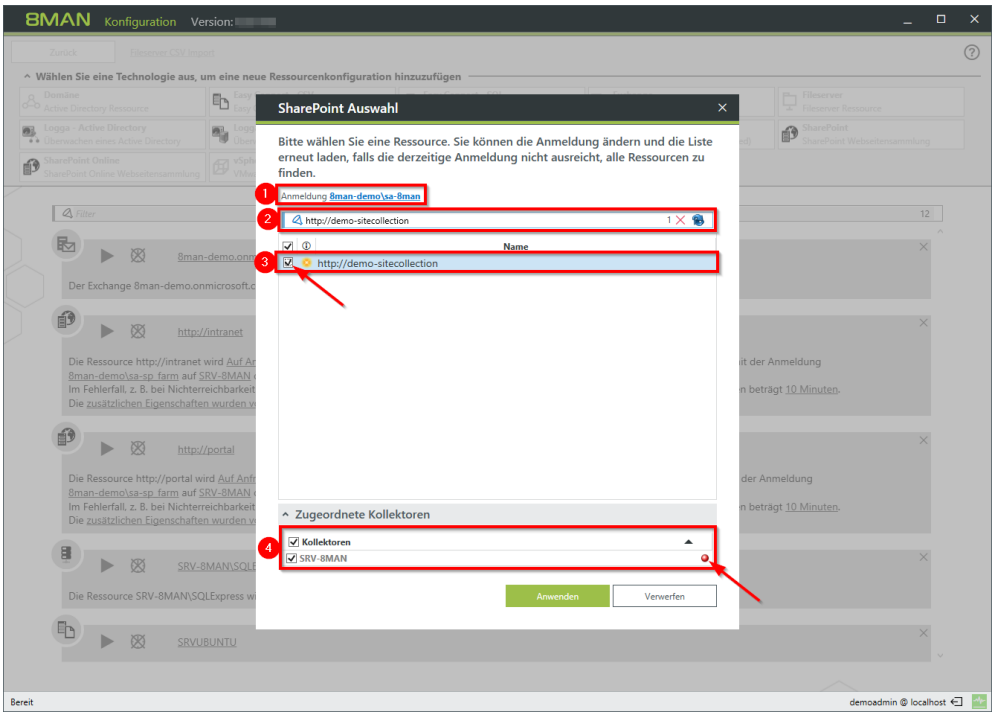
Add a scan configuration.



Specify the credentials for the "Process Account".

The account is not used to scan the SharePoint site collection. This account will be set up in a later step.

After successfully checking the "Process account", the selection of available resources opens.



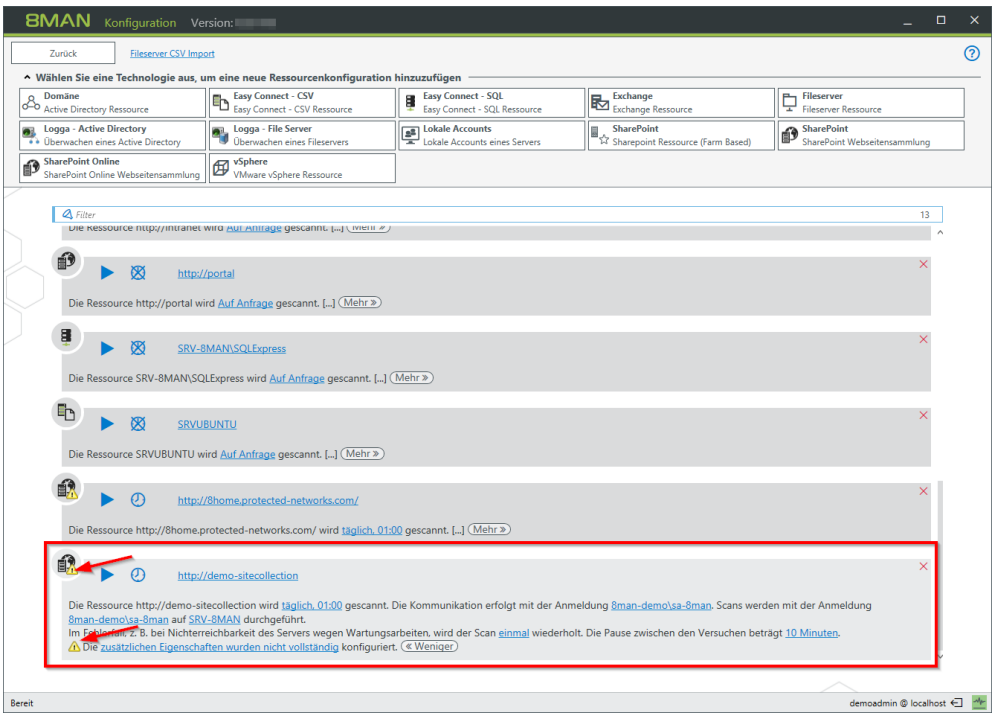
1. *If necessary, change the "Process account".*
2. *Specify the URL of the site collection. Confirm your entry with the ENTER key.*

SharePoint does not provide an interface that allows 8MAN to get URLs of site collections.

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

Collector indicator green:
A connection to the specified SharePoint URL was successful. This does not mean that all content can be completely scanned. Please refer to the information on the scan account required in the next step.

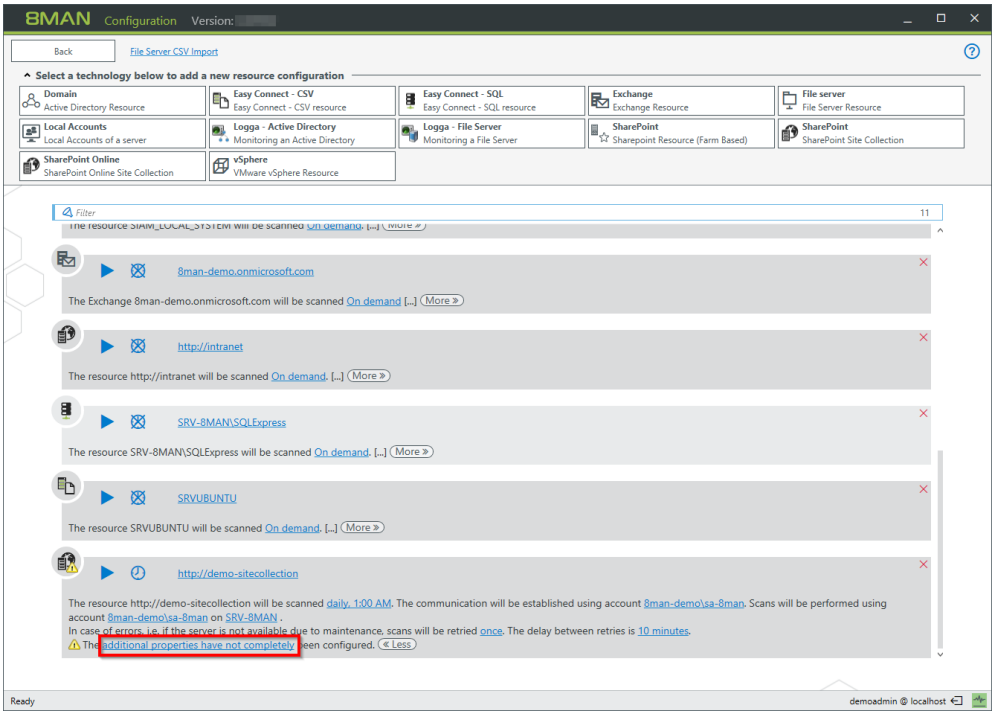
Collector indicator red:
Unable to successfully connect to the specified SharePoint URL. You can still save the settings and correct them in the following step.



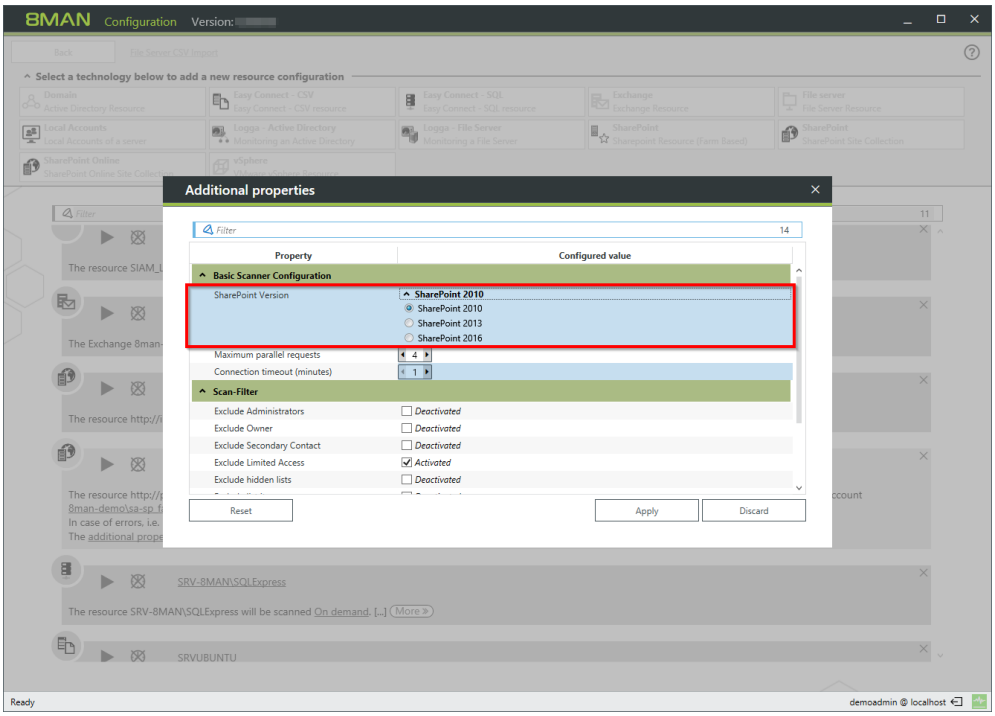
You have created a new SharePoint configuration.

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

8.3.4 Configuring additional properties

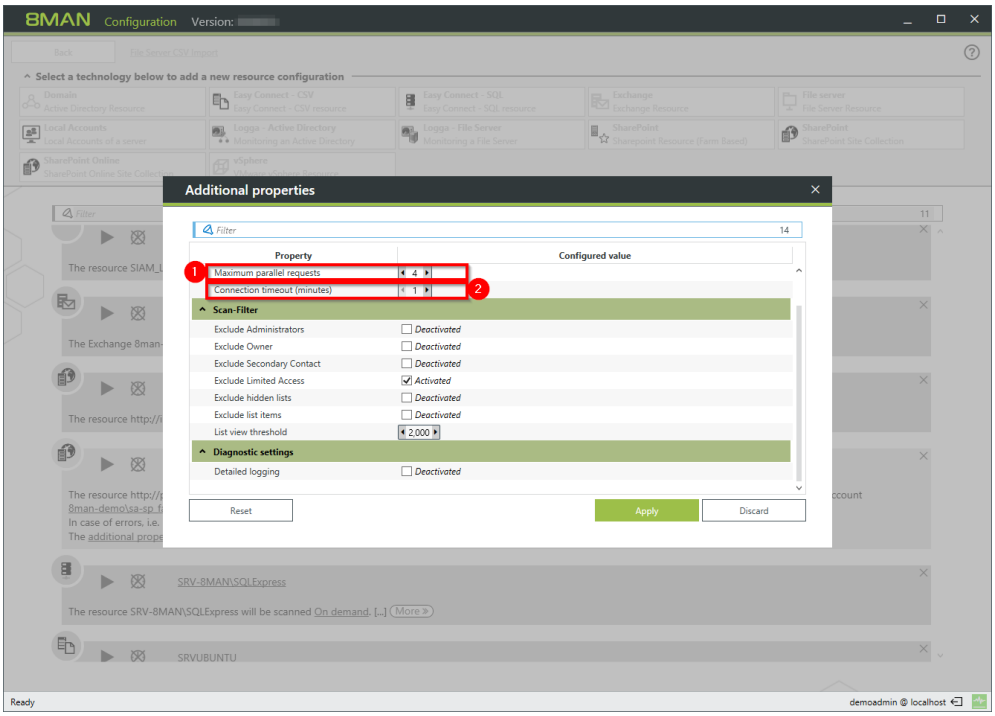


Click the link.



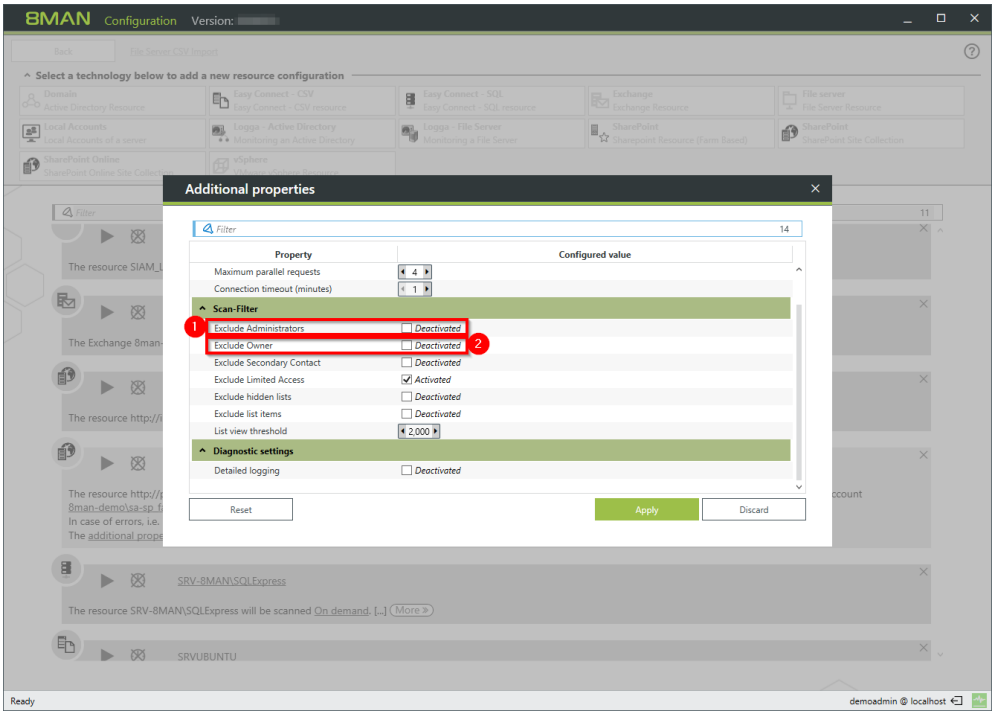
Select the SharePoint version.

To communicate with the SharePoint system, 8MAN uses Microsoft components that are specific to the version of the SharePoint system that is used. Specifying the correct SharePoint version ensures that all information is shared correctly with the SharePoint system. If the configured version of SharePoint differs from the actual version, this may result in incomplete or incorrect data.



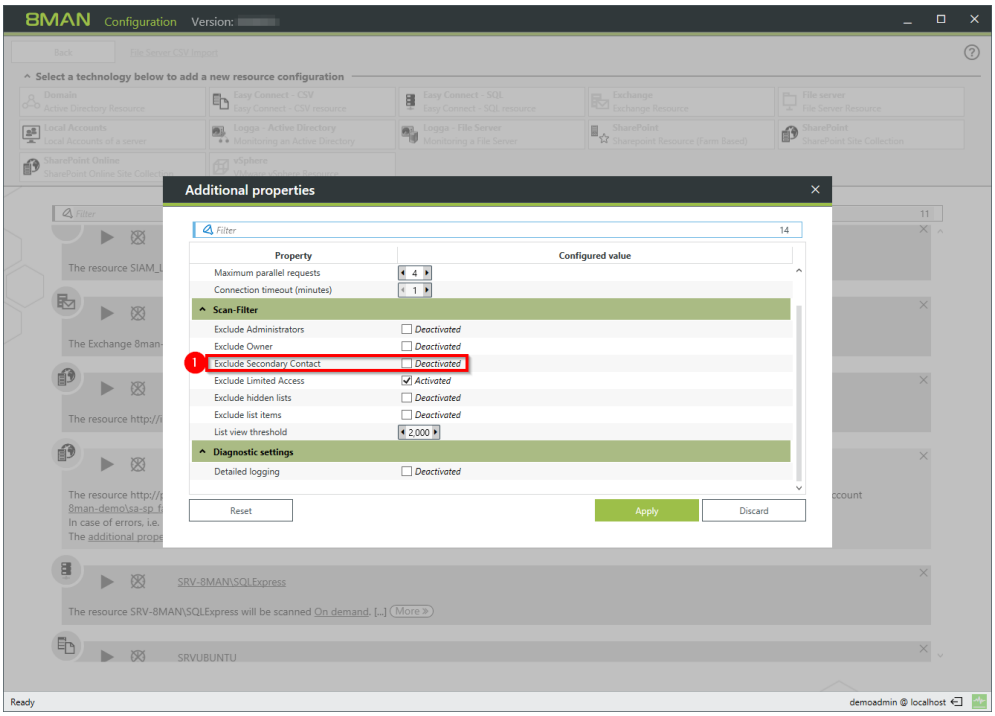
1. *Determine how many maximum parallel requests the scan will perform. The higher the number, the higher the scanning speed and the load on the SharePoint Server. Possible values: 1 to 10*

2. *Determine how long 8MAN waits for the connection to the SharePoint Server. Possible values: 1 to 10, Recommended: 2 min*

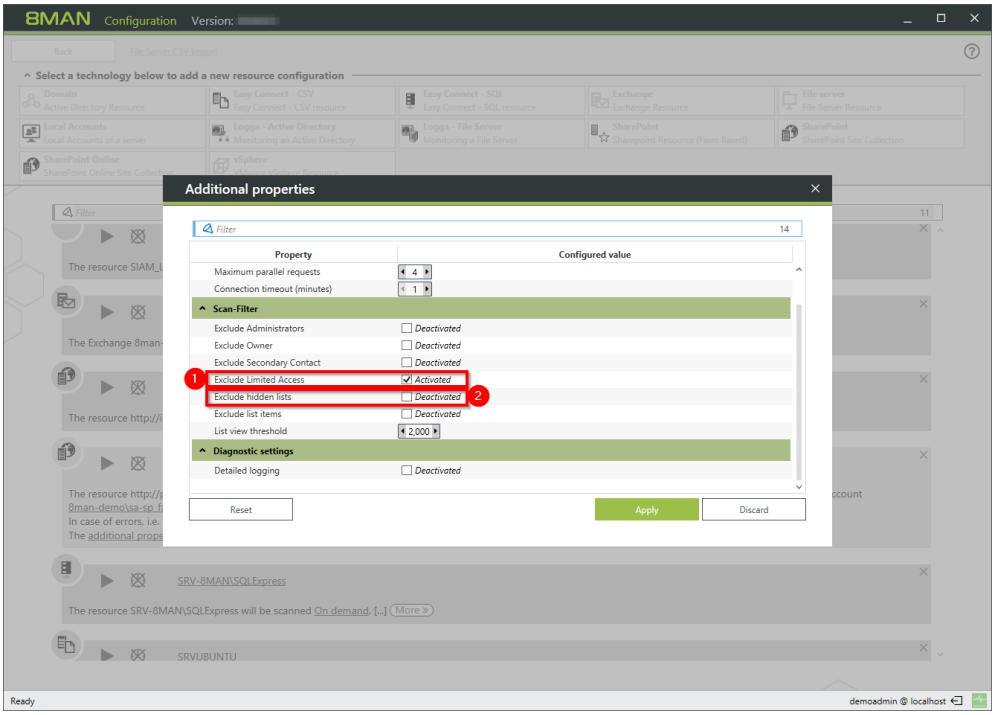


1. ***Option enabled:***
   8MAN excludes administrators from the scan. They are not available in views and reports.

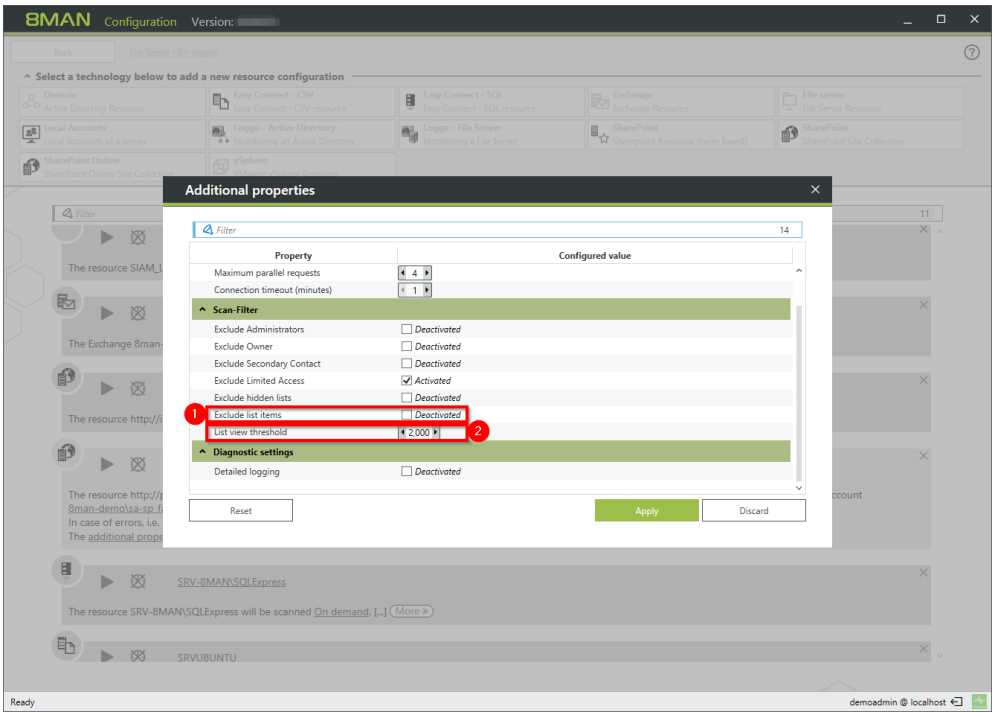
2. ***Option enabled:***
   8MAN excludes owner from the scan. They are not available in views and reports.
   This option is not effective for SharePoint 2010. Microsoft does not provide the information about the owner in this release.



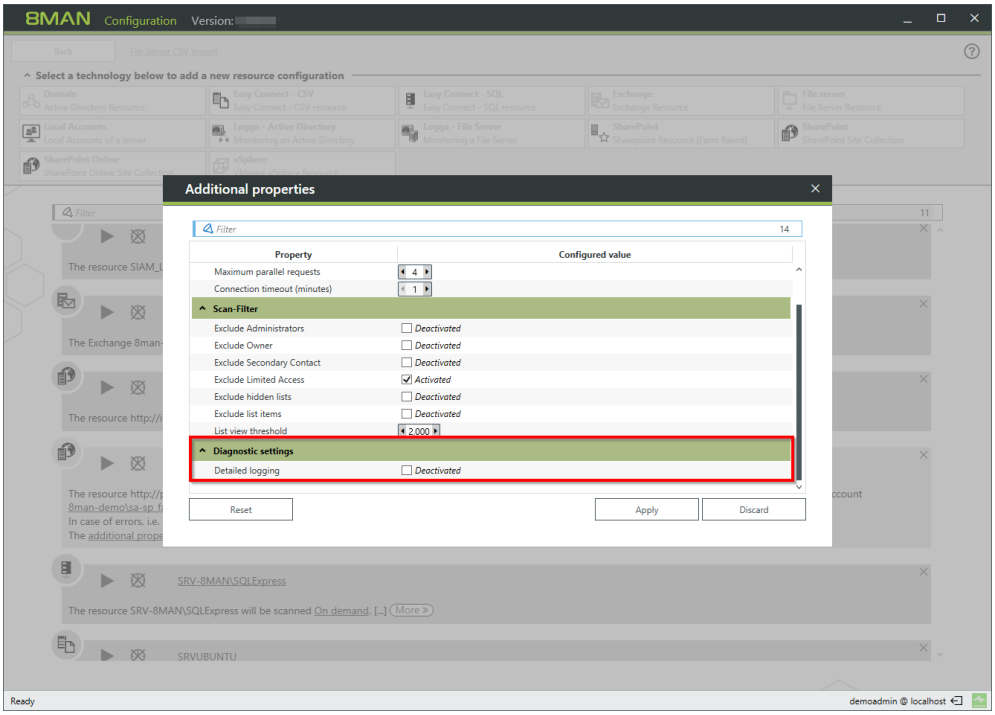
1. ***Option enabled:***
   8MAN excludes secondary contacts from the scan. They are not available in views and reports.
   The secondary contact is optional in SharePoint. The option is ineffective if no secondary contact is entered.
   This option is not effective for SharePoint 2010. Microsoft does not provide the secondary contact information in this release.



1. ***Option enabled:***
   8MAN excludes the limited access from the scan. This information is not available in views and reports.
   Limited access is automatically granted by the SharePoint system to a large extent, ensuring that SharePoint users can navigate through the system.
2. ***Option enabled:***
   8MAN excludes hidden lists from the scan. They are not available in views and reports.



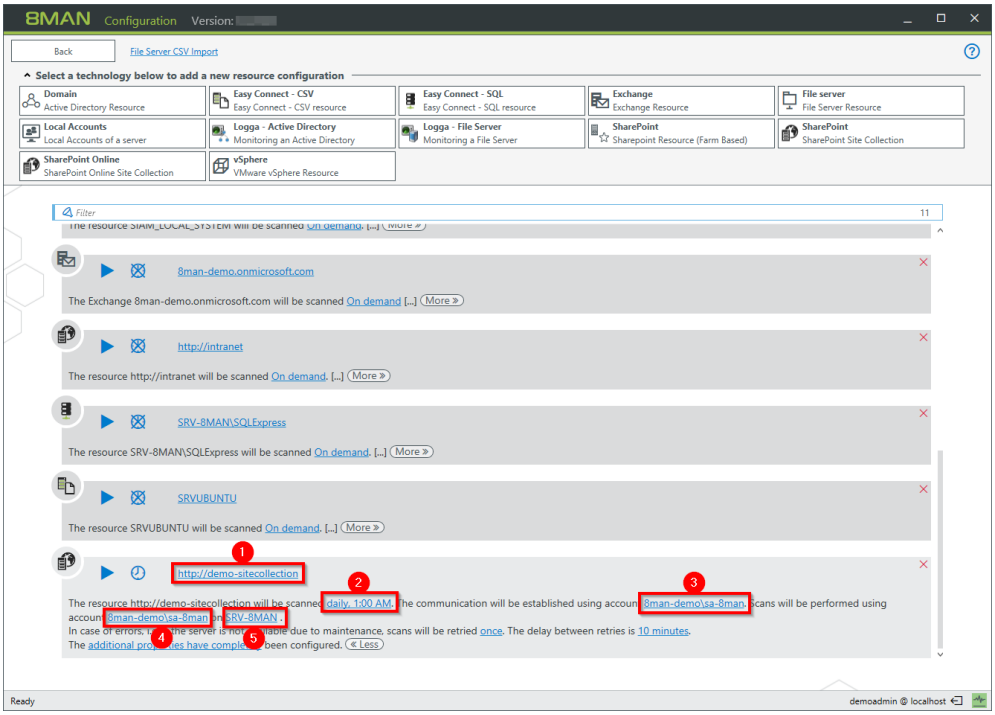
1. ***Option enabled:***
   8MAN excludes list items from the scan. They are not available in views and reports.
2. *With the threshold value for reading list elements, you determine how many list elements are read at maximum.*



Enable the option for extended error analysis only.

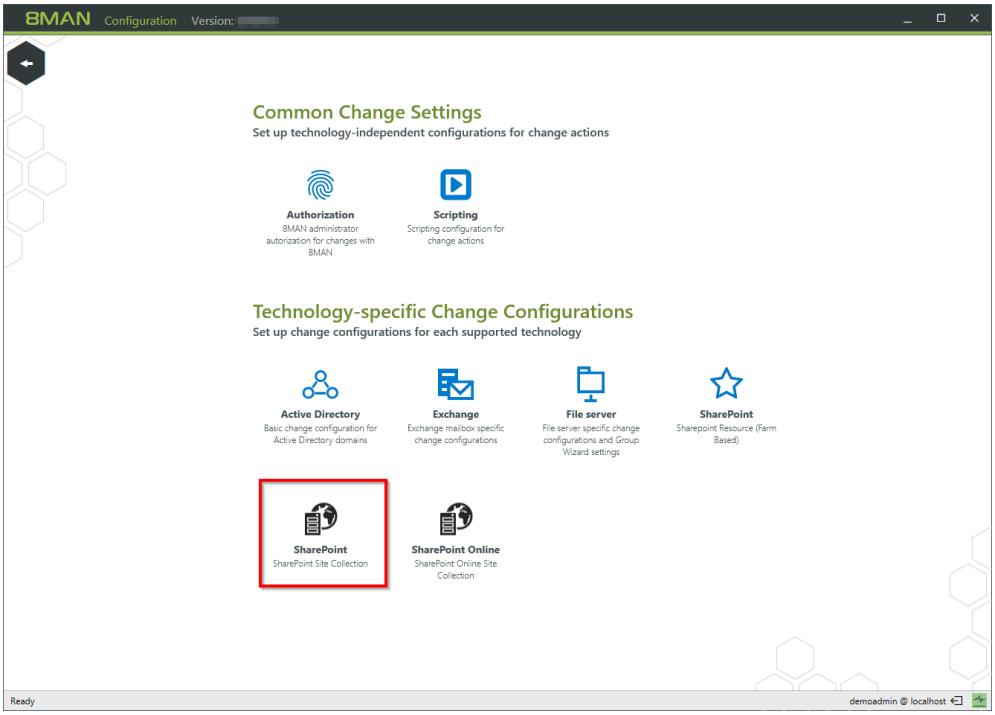
If this option is enabled, the scan speed will slow down and the size of the log file of the 8MAN server will increase faster.

8.3.5 Customizing a SharePoint scan configuration



1. *Change the SharePoint Scan configuration name.*
2. *Change scheduling for scanning.*
3. *Change the "Process Account".*
4. *Change the "Scan Account".*
5. *Change the collector that runs the scan.*

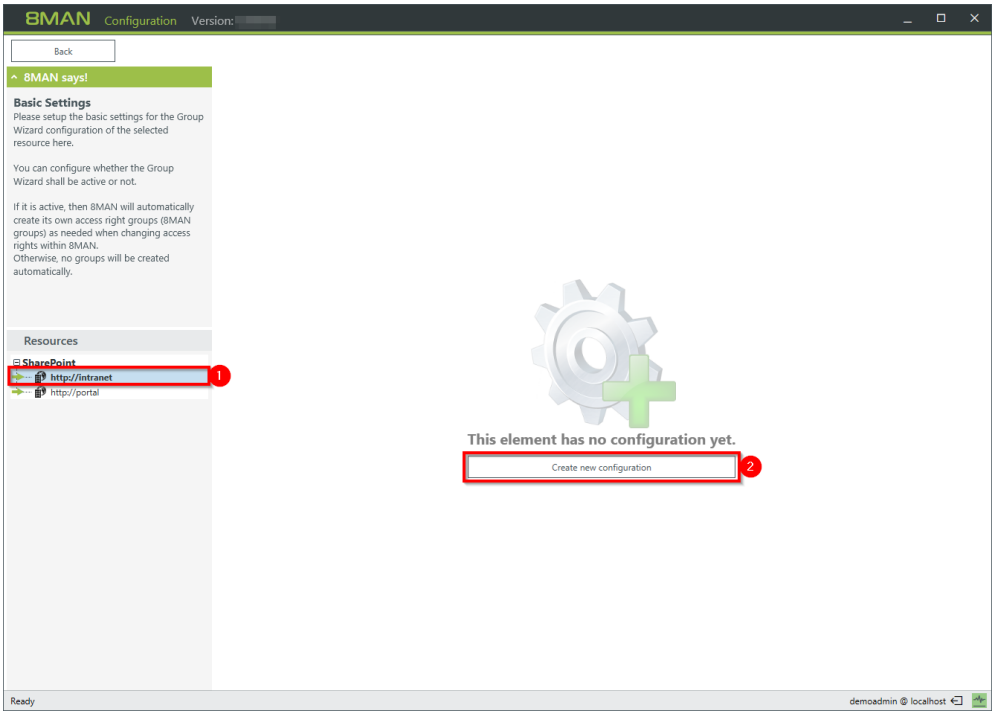
8.4 SharePoint change configuration



In the 8MAN configuration, navigate to "Change Configuration" -> "SharePoint".

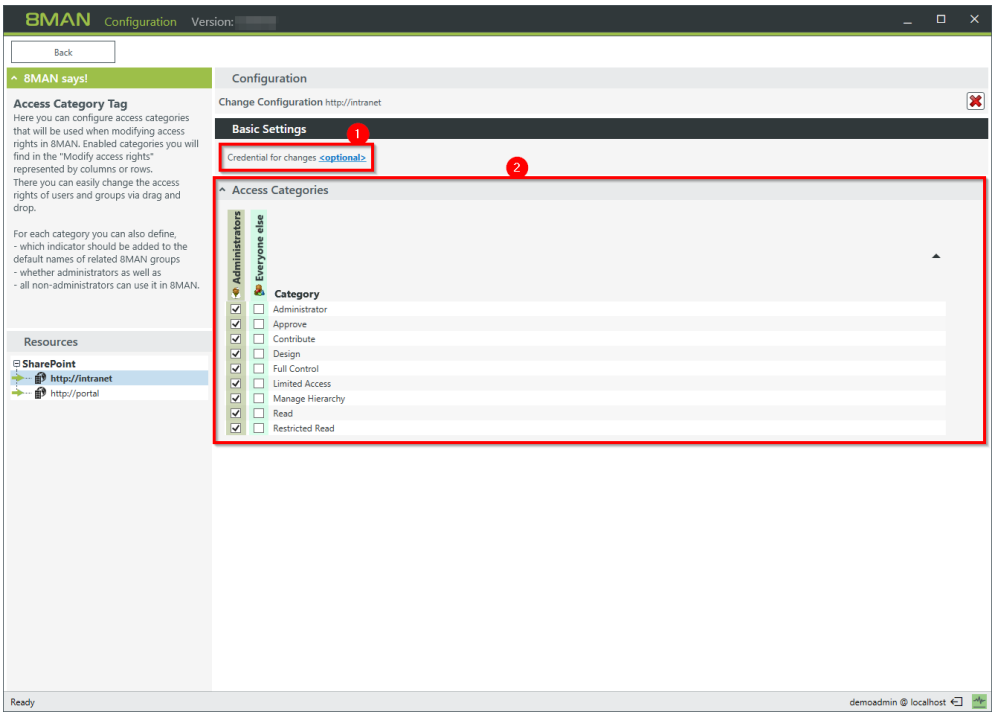
You must have run at least one SharePoint scan to create a change configuration.

Adding a SharePoint change configuration



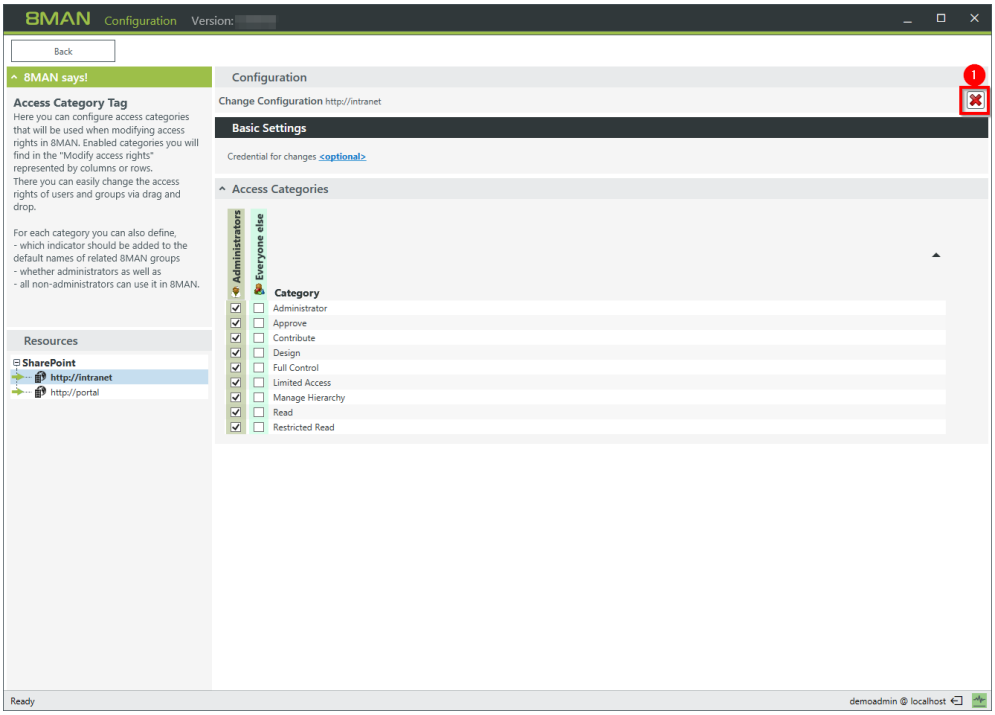
1. *Select a SharePoint resource.*
2. *Click "Create new configuration".*

Modify a SharePoint change configuration



1. *Specify which credentials are used to make changes to the SharePoint resource.*
   If you do not specify any, the 8MAN users are prompted for each change.
2. *Determine which access categories are available for 8MAN users to change access rights. Define a set for 8MAN administrators and another for all 8MAN modify user roles (See also: 8MAN user management).*

Delete a SharePoint Change configuration



1. *Delete a SharePoint change configuration.*