



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



Access Rights Management

AD Logga Manual

Version 9

© 2018 Protected Networks GmbH

1	Security Monitoring	4
1.1	8MATE AD Logga	5
2	System requirements	7
2.1	The 8MAN architecture	7
2.2	AD Logga requirements	8
2.3	Network requirements and firewall settings	9
2.3.1	Configure the Windows firewall for AD Logga	9
3	Configure Scans and Logga	10
3.1	Configure Active Directory (AD) Logga	10
3.1.1	Enable monitoring for AD Logga	10
3.1.1.1	Configure audit policies for domain controllers (DCs)	10
3.1.1.1.1	Configure audit policies for DCs on server 2008	10
3.1.1.1.2	Configure audit policies for DCs on server 2008 R2 or higher	12
3.1.1.1.3	Configure AD Logga storage settings	16
3.1.1.1.4	Verify the audit policy settings	16
3.1.1.2	Set the size of the Windows event logs	17
3.1.1.3	Set audit permissions in the AD object SACLs	17
3.1.2	Load the license file and check covered features	21
3.1.3	Add an AD Logga configuration	23
3.1.4	Activate/deactivate AD Logga	24
3.1.5	Modify the AD Logga configuration	25
3.1.5.1	Filter AD Logga Events	26
3.1.5.1.1	Understand filtering principles	26
3.1.5.1.2	Configure event filters	27
3.1.6	Delete an AD Logga configuration	31
4	Server	32
4.1	Set the display duration for comment icons	33
4.2	Configure storage time for AD Logga data	34
5	Evaluate AD Logga data	35
5.1	Monitor changes to specific event types	35
5.2	Identify temporary group memberships	39
5.3	Identify locked user accounts	41
5.4	Monitor password resets	43
5.5	Analyze AD Logga events with the logbook	45
5.6	Identify the most recent actions on an account	47
6	Configure alerts	49

6.1 Enable/disable alert sensors 50

6.2 Set alerts for groups 51

6.3 Set alerts for user accounts 53

6.4 Manage alerts 55

7 Contact 8MAN Support 56

8 Disclaimer 57

9 Software license acknowledgments 58

1 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.

At process levels, you gain complete visibility into Access Rights activities. Changes made outside of 8MAN are recorded. Based on the information obtained, your Access Rights Management process can be optimized.

With the included alerts you are informed in real-time of critical events.

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

Active Directory

8MATE AD Logga

Fileserver

8MATE FS Logga

1.1 8MATE AD Logga



The Problem

Changes to Active Directory or file servers are made by a variety of employees. Without full monitoring, security risks and inconsistencies in the processes are created.

Security risks

Security risks often occur when group memberships give unauthorized employees access to sensitive documents. If group memberships are revoked again immediately, the security incident is usually not recognized.

Confusing processes

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

The Solution

8MAN creates transparency of the access rights situation in Active Directory. The AD Logga expands this transparency to include the entire history of access rights changes in your system. This even includes any changes made outside of 8MAN. Security relevant temporary group memberships thereby become completely transparent. Through our configurable reports all activities related to user accounts, objects, groups and attributes become fully traceable and transparent.

This is achieved with the AD Logga

- Giving Administrators a complete picture of all AD activity, allowing them to optimize processes.
- Auditors recognize security incidents and all involved parties. This way the appropriate remedies can be implemented.
- The management has the certainty: With its monitoring, AD Logga provides the data for internal security and process improvements.

With the 8MATE AD Logga, you are constantly monitoring changes to AD. The AD Logga also records changes that were not executed with 8MAN.

The following changes are monitored by AD Logga:

- AD object created / deleted
- AD object moved
- Group, user account or computer account created / deleted
- Group membership changed
- Account enabled / disabled
- Password reset
- Account locked / unlocked
- Attribute changes to AD objects (for example, Group type, Distinguished Name, Department ...)

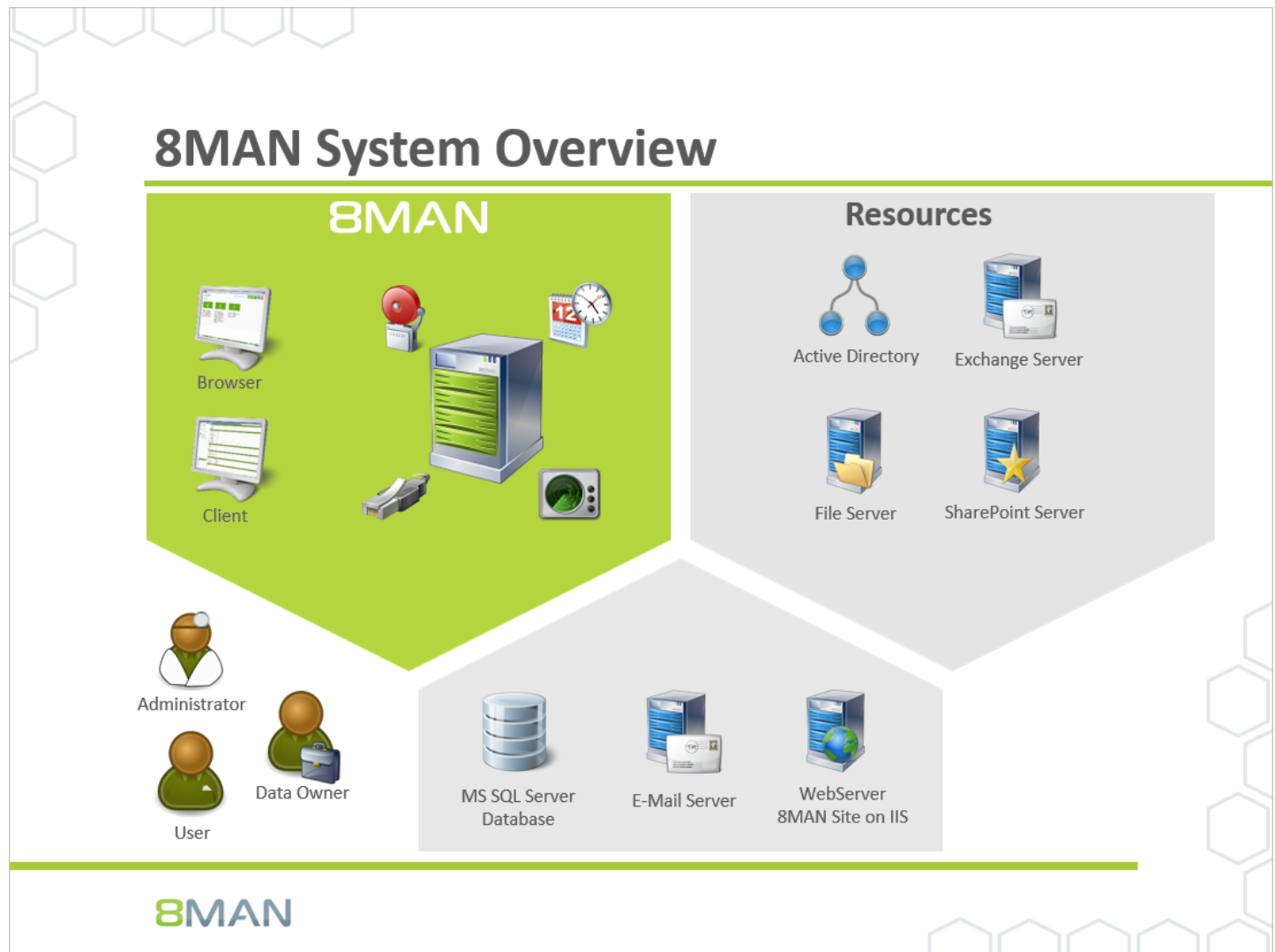
Recorded changes are stored in the 8MAN database and are retrievable via the 8MAN logbook and reports.

The 8MAN AD Logga works without an agent. You do not have to install any extra software on the domain controllers. Supported server versions are described in the [system requirements](#).

The technology used by the 8MATE AD Logga ensures that all events are recorded seamlessly. Short-term failures of the 8MAN collector, e.g. due to maintenance, do not lead to missing events in the 8MAN logbook.

2 System requirements

2.1 The 8MAN architecture



The 8MAN Suite is comprised of three components:

- 8MAN server to process new data and requests from the 8MAN GUI
- Collectors to connect your resource and data systems
- 8MAN graphical user interface (application and configuration module, web interface)

The 8MAN component architecture allows you to run installations across a variety of remote resources in an extremely efficient manner. All individual components are connected with each other via network interfaces. You can even run several components on the same computer.

2.2 AD Logga requirements

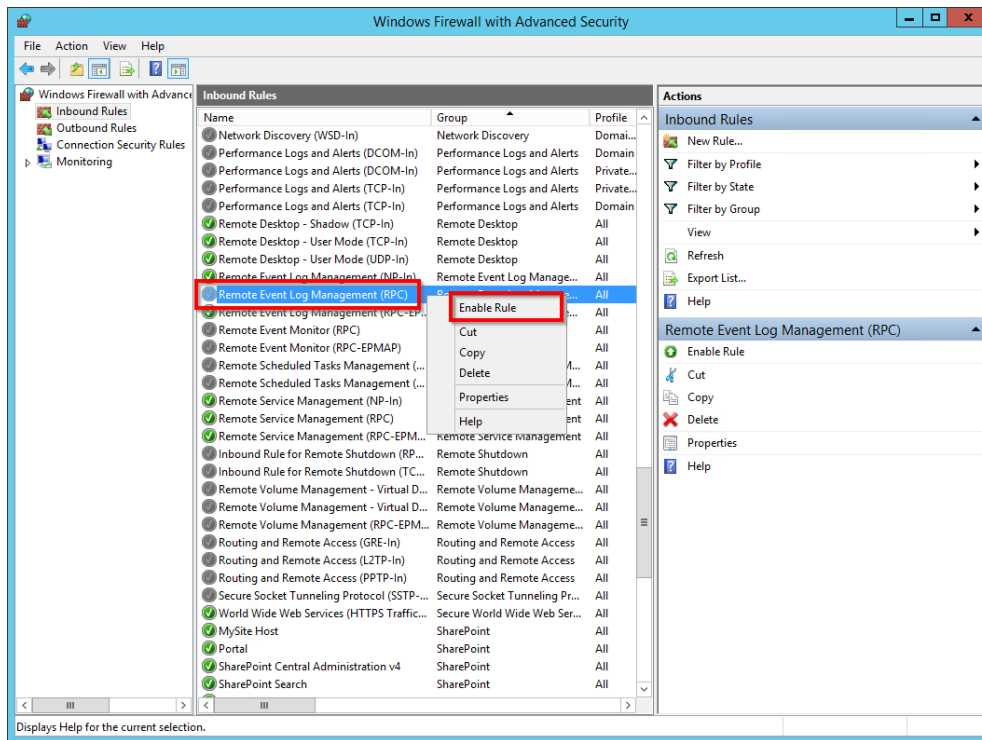
The 8MATE AD Logga supports domain controllers (DCs) that run on the following server versions:

- Microsoft Windows Server 2008 (32-bit and 64-bit), 2008 R2, 2012, 2012 R2 and 2016

The 8MATE Logga does not require a dedicated collector. Even the 8MAN server itself can be used as a collector.

2.3 Network requirements and firewall settings

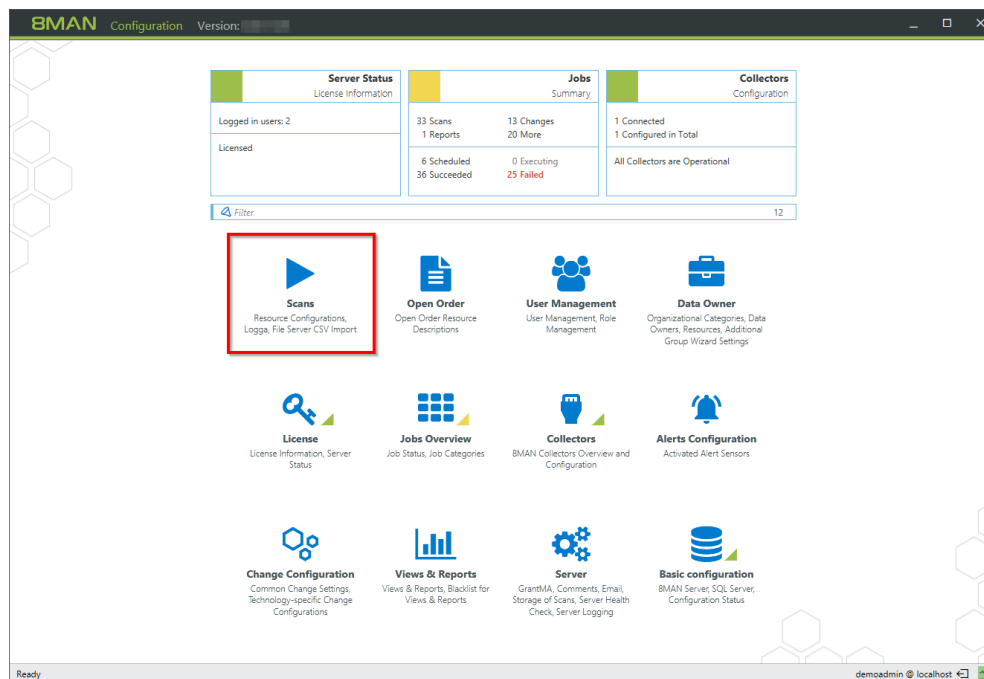
2.3.1 Configure the Windows firewall for AD Logga



If the Windows firewall is applied on the DC that you would like to monitor, then a pre-defined Microsoft rule "Remote Event Log Management (RPC)" must be enabled.

Repeat the process as needed for all DCs that you would like to monitor.

3 Configure Scans and Logga



8MAN scans access rights structures from different resource systems in configurable intervals. The scan results are stored in an SQL data base. Users can access these results quickly via the 8MAN GUI, as they are already located in the data base.

Events that occur in between scans are captured by the 8MATES AD Logga and FS Logga. 8MATES are modules that can be added to 8MAN and require the appropriate license.

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

3.1 Configure Active Directory (AD) Logga

3.1.1 Enable monitoring for AD Logga

3.1.1.1 Configure audit policies for domain controllers (DCs)

In order to be able to access AD Logga functionality you must activate a special audit policy.

If you want to make changes to audit policy you must be a member of the appropriate domain admin or organization admin group.

3.1.1.1.1 Configure audit policies for DCs on server 2008

Before configuring audit policies you should verify that all required categories are activated.

You can activate the required audit policies by running the following commands on every DC with admin rights:

For "Monitor policy changes":

```
auditpol /set /subcategory:{0CCE922F-69AE-11D9-BED3-505054503030} /success:enable
```

For "Directory service changes":

```
auditpol /set /subcategory:{0CCE923C-69AE-11D9-BED3-505054503030} /success:enable
```

For "Managing User Accounts", "Managing computer accounts", "Managing security groups", "Managing distribution groups", "Managing application groups" and "other account management events":

```
auditpol /set /subcategory:{0CCE9235-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9236-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9237-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9238-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9239-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE923A-69AE-11D9-BED3-505054503030} /success:enable
```



Repeat this process for every DC!

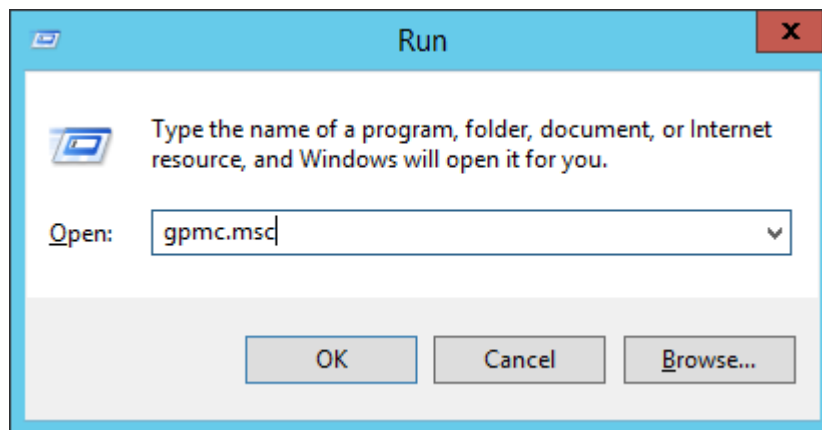
3.1.1.1.2 Configure audit policies for DCs on server 2008 R2 or higher

You can use the group policy editor to manage audit policy on server 2008 R2 or higher. This means you only need to implement the policy once rather than having to repeat it for every DC.

Please note that the activation of audit policy may be delayed on the domain controllers (DCs) depending on your replication interval.

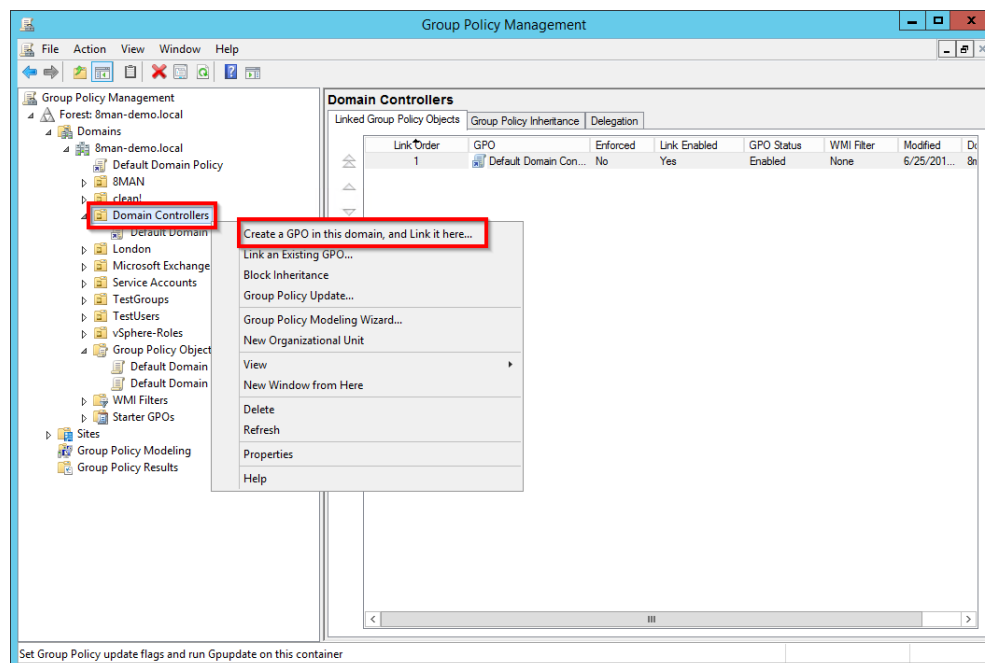
Once you have completed these settings:

- complete a manual policy update with the command "gpupdate /force"
- [Verifying the execution of audit policies](#)



Start managing group policies, by opening:

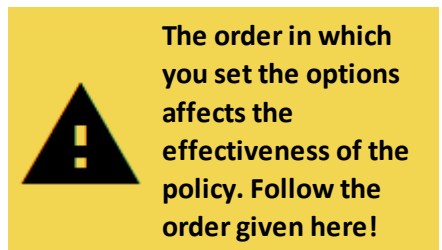
gpmc.msc

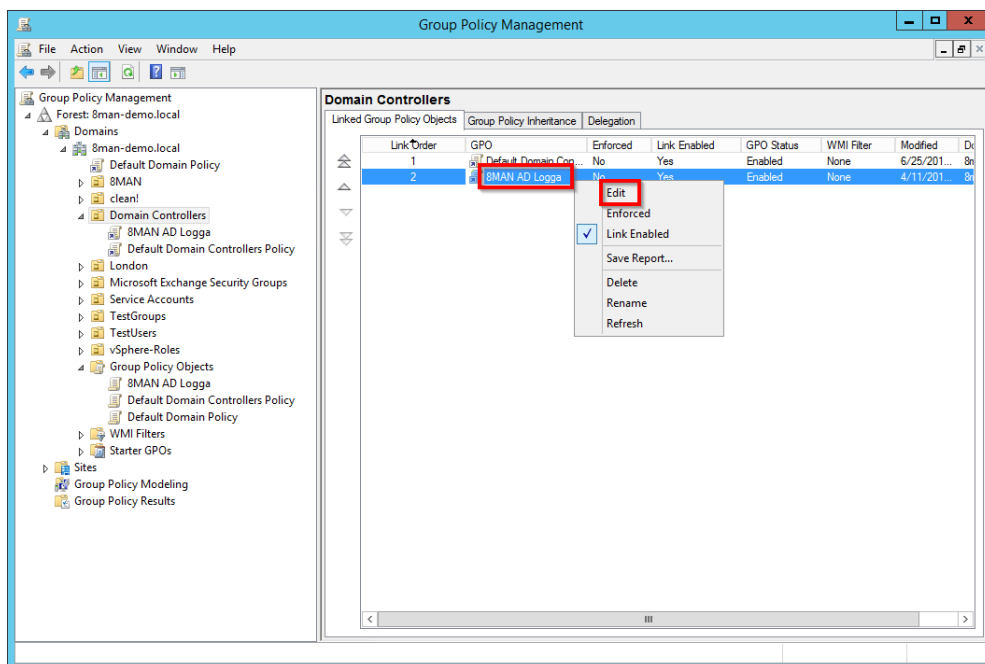


Create a new group policy.

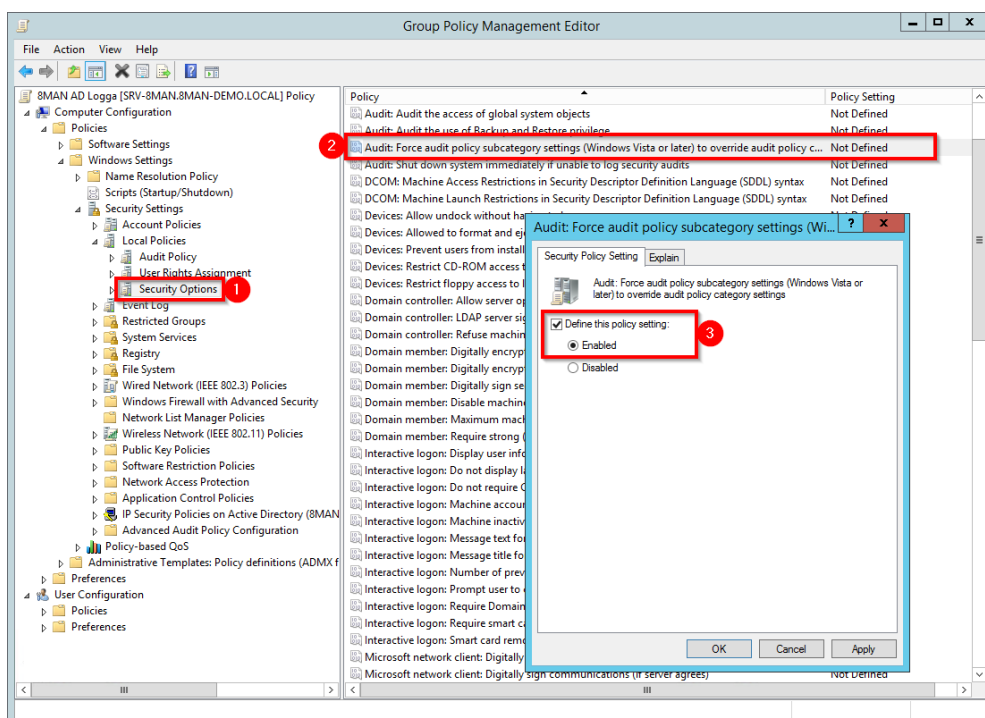
Select the OU in which the DC computer accounts are located. By default they are located in the OU "Domain Controllers".

Please ensure that the newly created policy is applied/winning to the appropriate DCs (hierarchy and order).



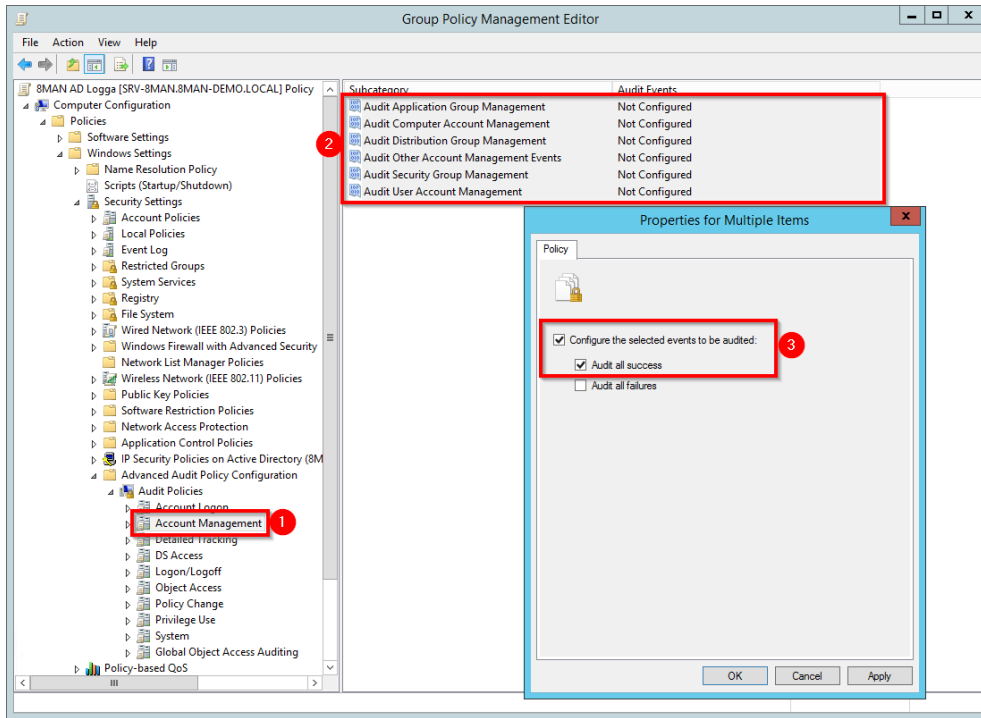


Select the newly created group policy by right clicking and selecting "edit".

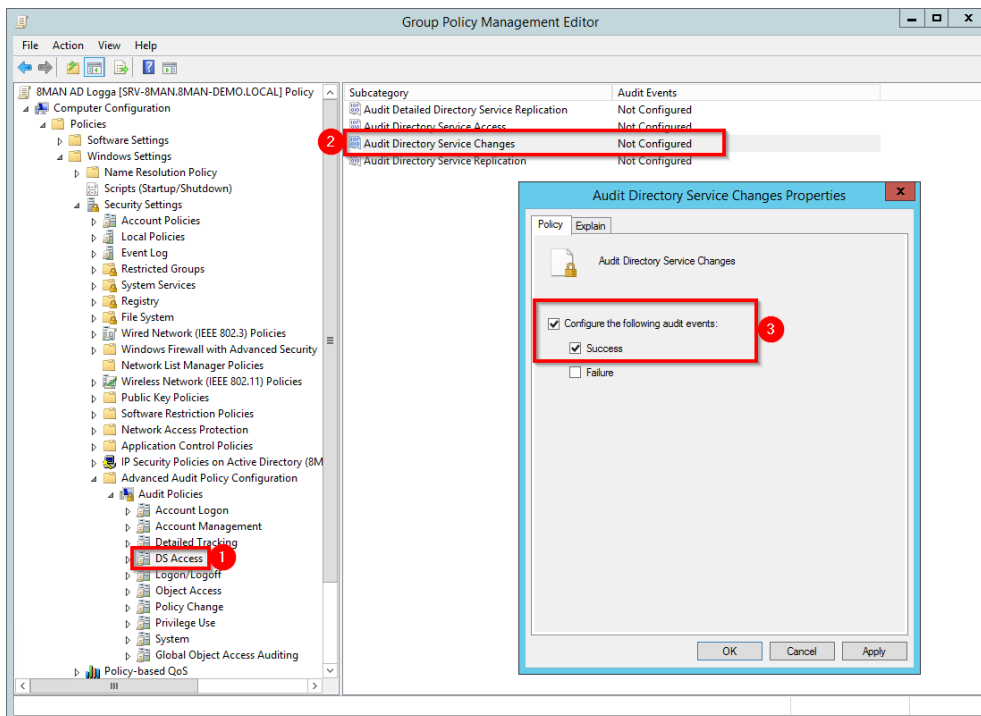


1. Navigate to "security options".
2. Select the policy "Audit: Force audit policy...".
3. You can activate the security policy by right-clicking and selecting "Properties", as shown in the diagram.

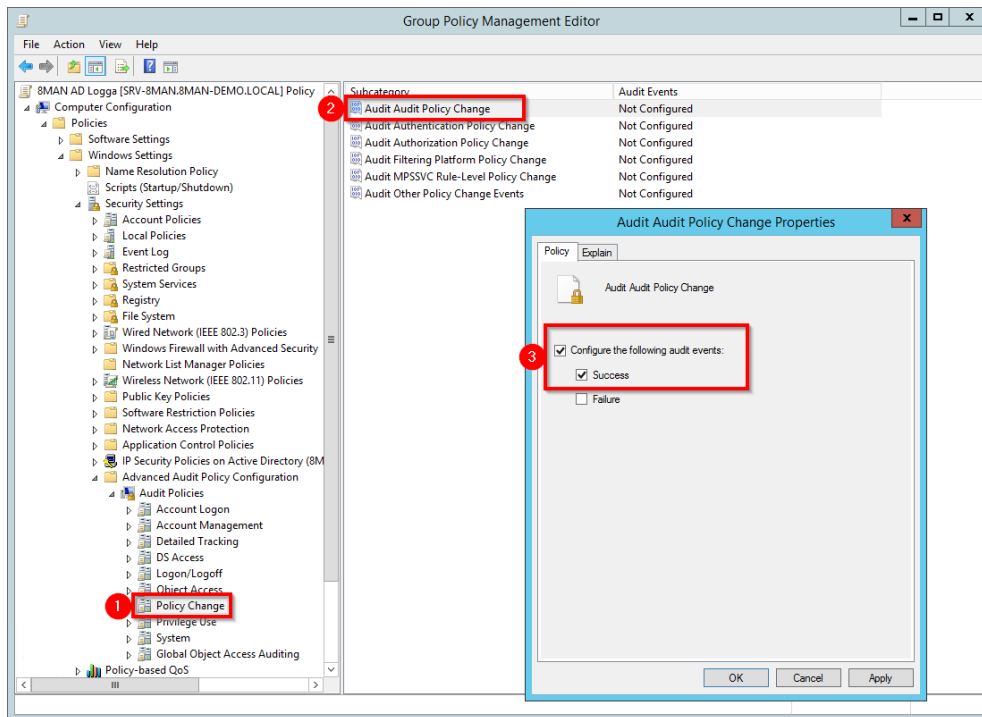
The order in which you set the options affects the effectiveness of the policy. Follow the order given here!



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



1. Navigate to "DS Access".
2. Select the subcategory "Audit Directory Service Changes".
3. You can activate the audit by right-clicking and selecting "Properties", as shown in the diagram.



1. Navigate to "Change policy".
2. Select the subcategory "Audit Audit Policy Change".
3. You can activate the audit by right-clicking and selecting "Properties", as shown in the diagram.

Once you have completed these settings:

- complete a manual policy update with the command "gpupdate /force"
- Verifying the execution of audit policies

3.1.1.1.3 Configure AD Logga storage settings

1000 events require approximately 0.57 MB of storage in the data base.

By default the storage period of AD Logga events is set to 30 days and can be managed under server -> storage of scans.

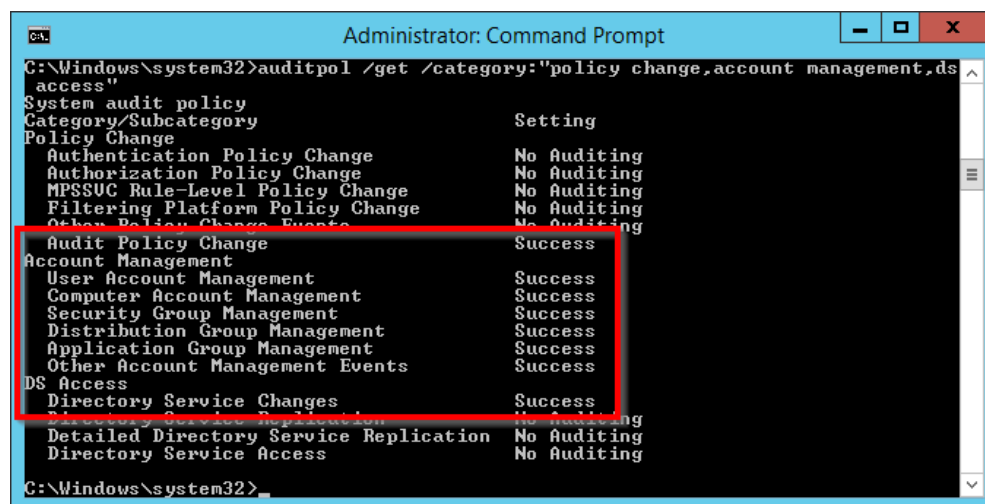
3.1.1.1.4 Verify the audit policy settings

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

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

or

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



```
Administrator: Command Prompt
C:\Windows\system32>auditpol /get /category:"policy change,account management,ds
access"
System audit policy
Category/Subcategory          Setting
Policy Change
  Authentication Policy Change No Auditing
  Authorization Policy Change No Auditing
  MPSSVC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events No Auditing
  Audit Policy Change Success
Account Management
  User Account Management Success
  Computer Account Management Success
  Security Group Management Success
  Distribution Group Management Success
  Application Group Management Success
  Other Account Management Events Success
DS Access
  Directory Service Changes Success
  Directory Service Replication No Auditing
  Detailed Directory Service Replication No Auditing
  Directory Service Access No Auditing
C:\Windows\system32>
```

The marked subcategories must be set to "Success".

3.1.1.2 Set the size of the Windows event logs

To ensure that you don't "lose" any events, you must configure the maximum size for security event logs appropriately. For audit policy settings the storage requirements is roughly 1KB per event.

For example:

For a server outage or maintenance time (of the collector server selected for the AD Logga) of one hour, with approximately 1000 events per hour, the absolute minimum security event log size would be 1MB. Considering the low storage space requirements for 1000 events, the uncertainty of outage times as well as the potential relevance of individual security events we highly recommend that you ensure that enough storage space is available.

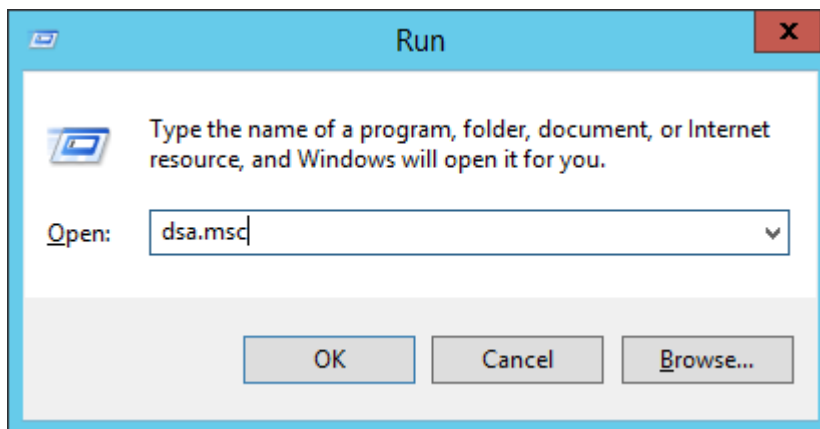
More information on how to manage storage size can be found at [Microsoft](#).

3.1.1.3 Set audit permissions in the AD object SACLs

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

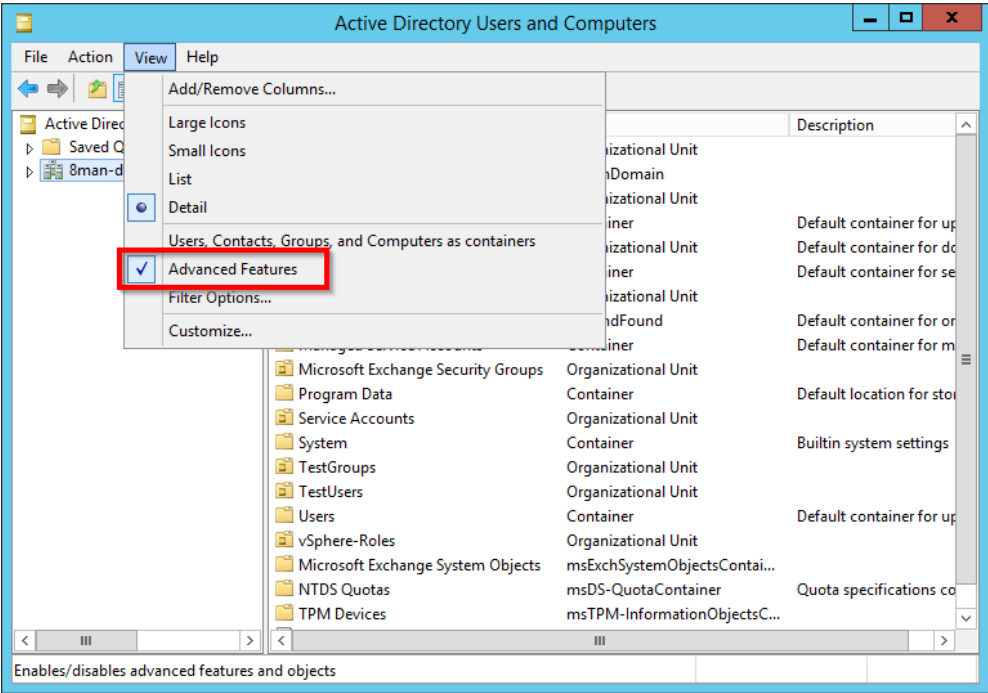
The user right "Manage auditing and security log" is required for the configuration of the SACL (this corresponds to the privilege "SeSecurityPrivilege"). You must be a member of the "event log reader" or domain admin group.

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

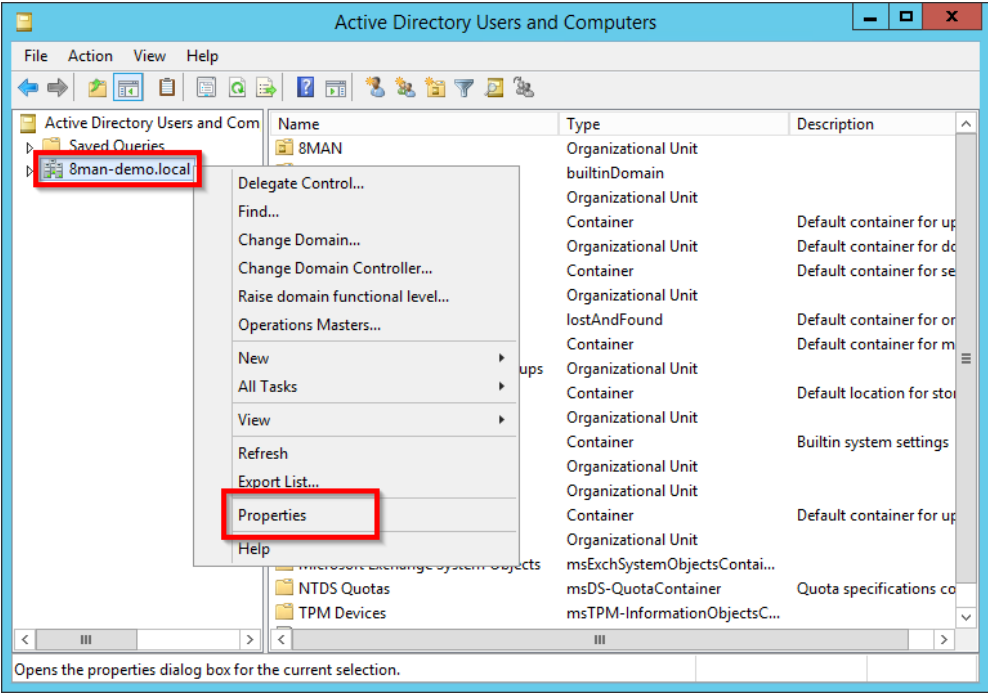


Start the management of Active Directory users and computers on a DC by opening

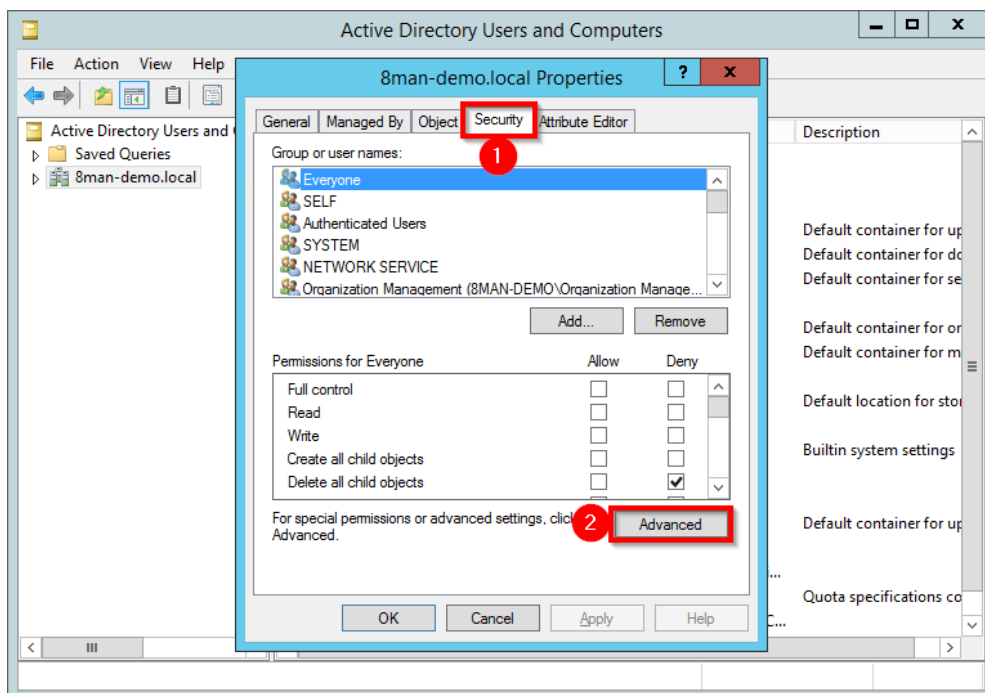
dsa.msc



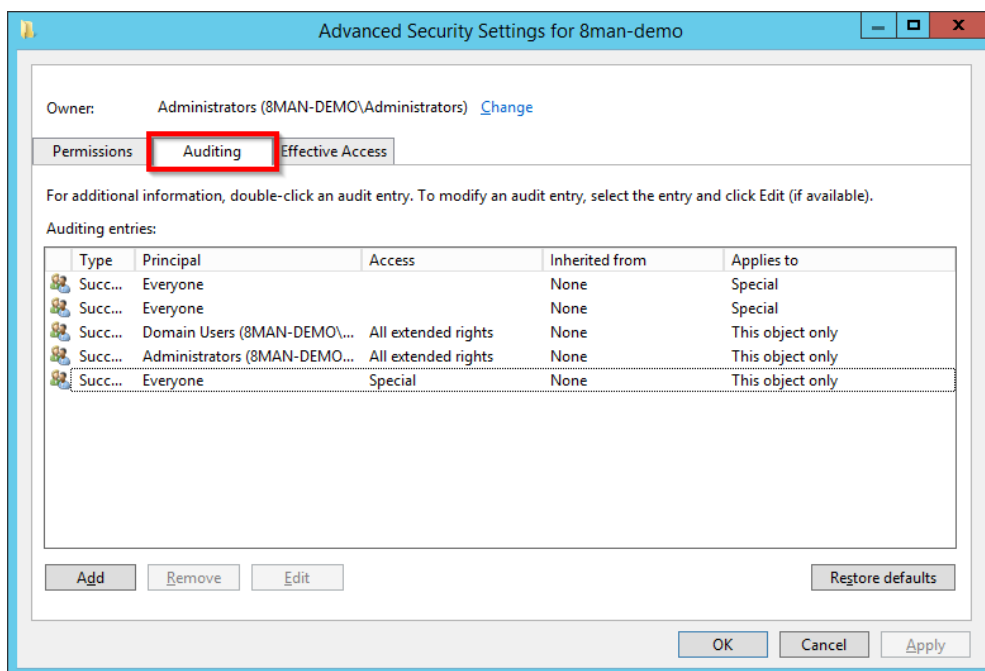
Activate the option "Advanced Features".



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



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



Select the tab "Auditing".

Analyze the existing access rights. Perhaps the required permissions already exist.

If required, expand the access rights of an existing "Everyone" principal or add the desired entry.

Auditing Entry for 8man-demo

Principal: **Everyone** Select a principal

Type: **Success**

Applies to: **This object and all descendant objects**

Permissions:

<input type="checkbox"/> Full control	<input checked="" type="checkbox"/> Create msExchOmaDeviceCapability objects
<input type="checkbox"/> List contents	<input checked="" type="checkbox"/> Delete msExchOmaDeviceCapability objects
<input type="checkbox"/> Read all properties	<input checked="" type="checkbox"/> Create msExchOmaDeviceType objects
<input checked="" type="checkbox"/> Write all properties	<input checked="" type="checkbox"/> Delete msExchOmaDeviceType objects
<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Create msExchOrganizationContainer objects
<input checked="" type="checkbox"/> Delete subtree	<input checked="" type="checkbox"/> Delete msExchOrganizationContainer objects
<input type="checkbox"/> Read permissions	<input checked="" type="checkbox"/> Create msExchPoliciesContainer objects
<input checked="" type="checkbox"/> Modify permissions	<input checked="" type="checkbox"/> Delete msExchPoliciesContainer objects
<input type="checkbox"/> Modify owner	<input checked="" type="checkbox"/> Create msExchProtocolCfghHTTPContainer objects
<input type="checkbox"/> All validated writes	<input checked="" type="checkbox"/> Delete msExchProtocolCfghHTTPContainer objects
<input type="checkbox"/> All extended rights	<input checked="" type="checkbox"/> Create msExchProtocolCfghHTTPFilters objects
<input checked="" type="checkbox"/> Create all child objects	<input checked="" type="checkbox"/> Delete msExchProtocolCfghHTTPFilters objects
<input checked="" type="checkbox"/> Delete all child objects	<input checked="" type="checkbox"/> Create msExchProtocolCfghIMAPContainer objects
<input checked="" type="checkbox"/> Create Computer objects	<input checked="" type="checkbox"/> Delete msExchProtocolCfghIMAPContainer objects
<input checked="" type="checkbox"/> Delete Computer objects	<input checked="" type="checkbox"/> Create msExchProtocolCfghIMContainer objects
<input checked="" type="checkbox"/> Create Contact objects	<input checked="" type="checkbox"/> Delete msExchProtocolCfghIMContainer objects

OK Cancel

At minimum, the following is required:

Principal: "Everyone"

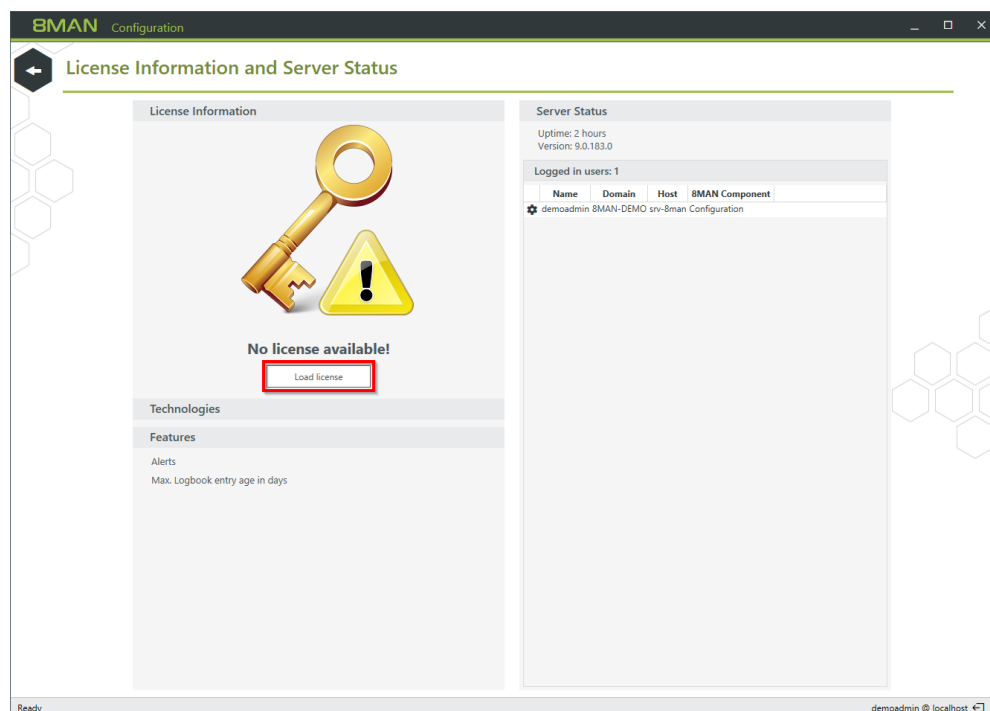
Type: "Successful"

Apply to: "This object and all descendant objects"

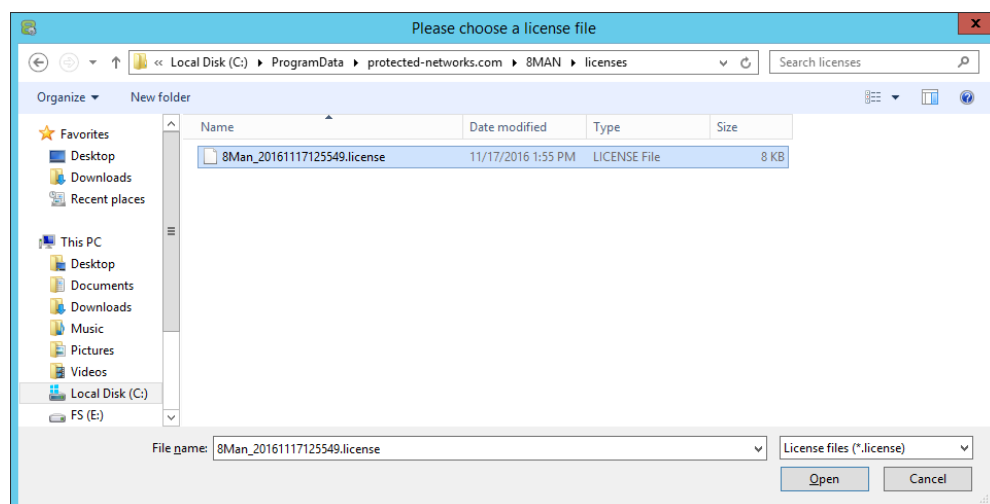
Permissions:

- Write all properties
- Delete
- Delete subtree
- Modify permissions
- Create all child objects
- Delete all child objects

3.1.2 Load the license file and check covered features



Click on "Load license".



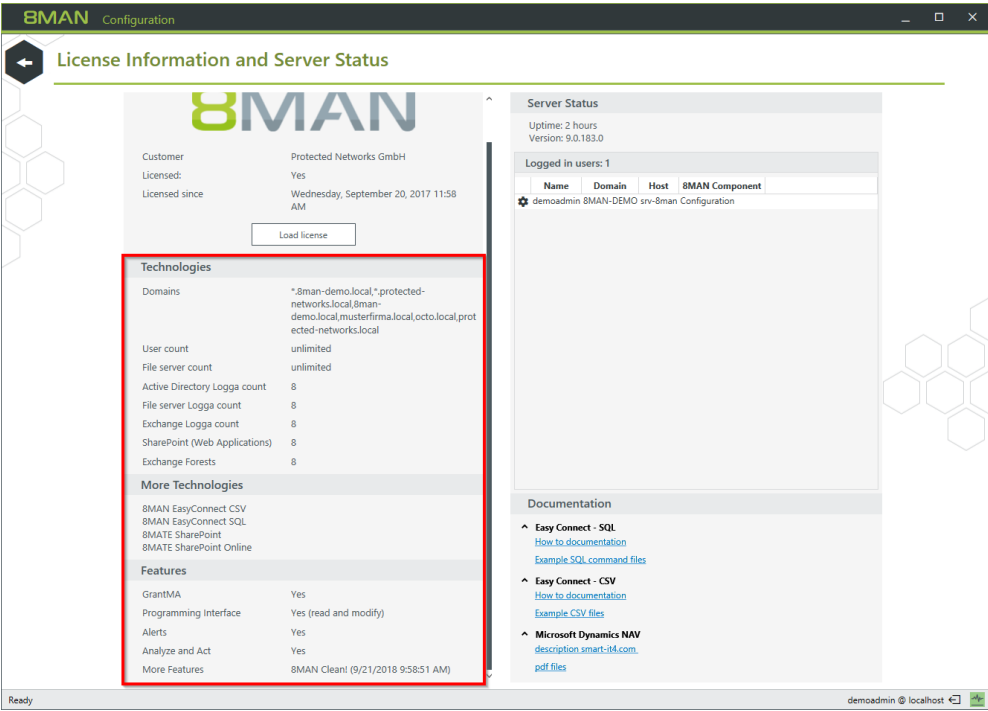
Select the path where your license key is stored.

8MAN license files have the file extension ".license".

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

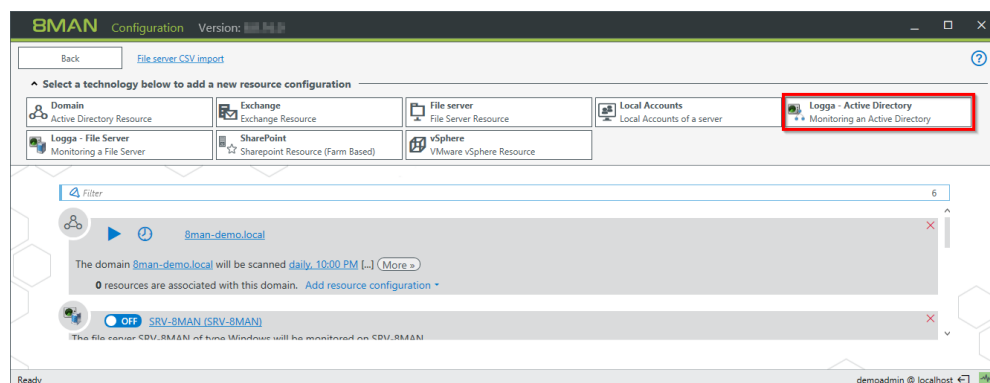
%ProgramData%protected-networks.com\8MAN\licenses

All licensed features are activated immediately.



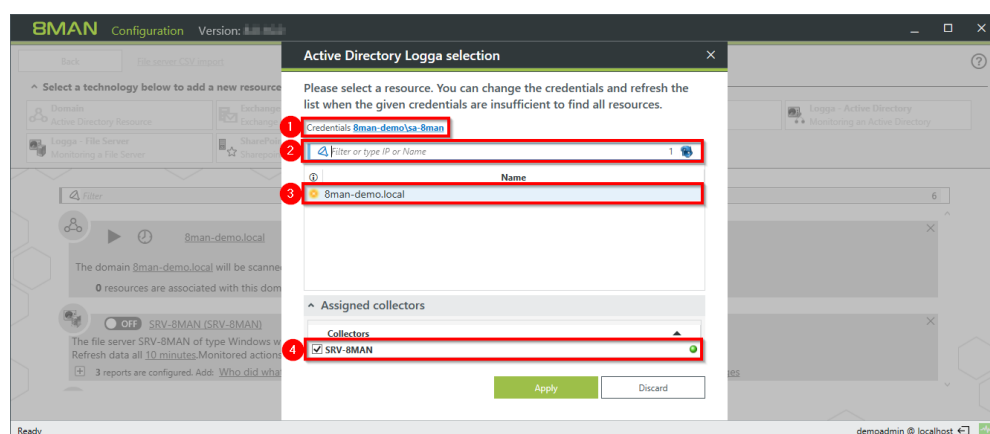
If the license file has been successfully loaded you will see detailed information on licensed features.

3.1.3 Add an AD Logga configuration



On the configuration home page select "Scans".

Select "Logga - Active Directory".

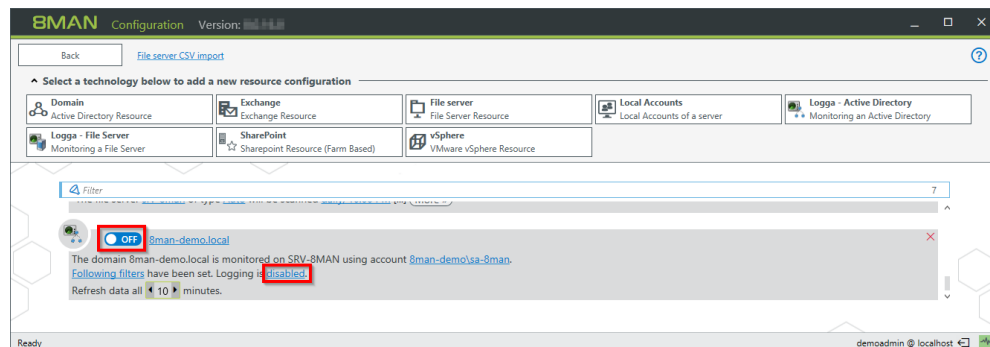


1. Enter valid credentials for the domain that you want to monitor.
2. Use the filters to find the desired domains.
3. Select a domain. Child domains are not monitored. Every domain must be configured separately.
4. Select a collector server. You can only select one collector per domain.

After adding an AD Logga configuration, it initially remains deactivated.

You must activate the AD Logga to record events.

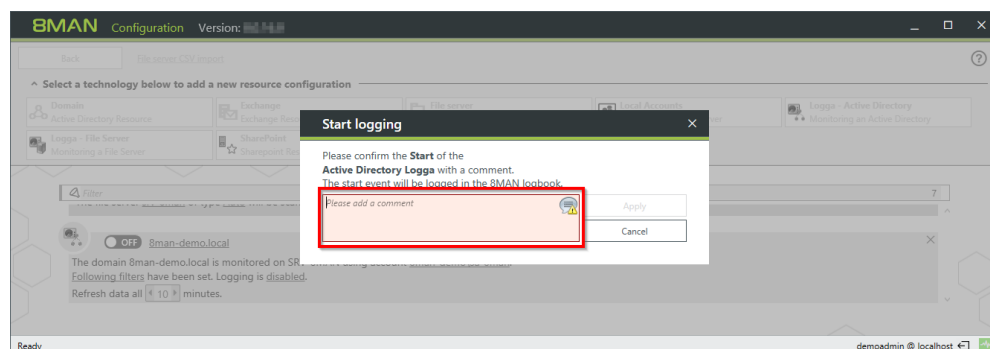
3.1.4 Activate/deactivate AD Logga



On the configuration home page select "Scans".

Click on the switch icon or link of the desired AD Logga configuration in order to activate it.

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

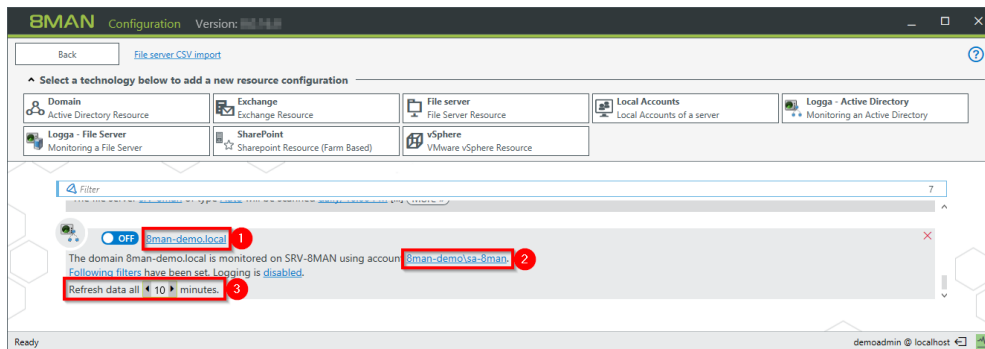


You must enter a comment.

Follow the same steps for deactivation.

3.1.5 Modify the AD Logga configuration

On the configuration home page select "Scans".



1. Give the configuration a different name.
2. Set the account used by AD Logga to read events from the domain controller.
The account must be a member of the group "event log readers" or "domain admins".
You can only change this setting when the Logga is turned off.
3. Determine how frequently Logga data is updated. Events are cached by the collector and transferred to the data base via the 8MAN server in configured intervals.
Standard setting: 10 minutes
Possible values: 1 to 60 minutes.

3.1.5.1 Filter AD Logga Events

You can filter out desired events in order to focus on specific and relevant entries. Filtering means that filtered events will not be displayed.

This allows you to significantly improve your overview and reduce data volume. A typical example are frequent attribute changes of the Exchange server.

You are only able to configure filters if at least one AD scan is stored in the database.

3.1.5.1.1 Understand filtering principles

The AD Logga filter is considered a blacklist filter. In this case, blacklist means: The AD Logga records all possible events. You can determine which results are excluded.

By default the filter is set to the object classes "Service-Connection-Point" and "Print-Queue".

The filter criteria work cumulatively. An event is excluded if criteria 1, or criteria 2, or criteria 3 is fulfilled, or multiple criteria simultaneously.

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

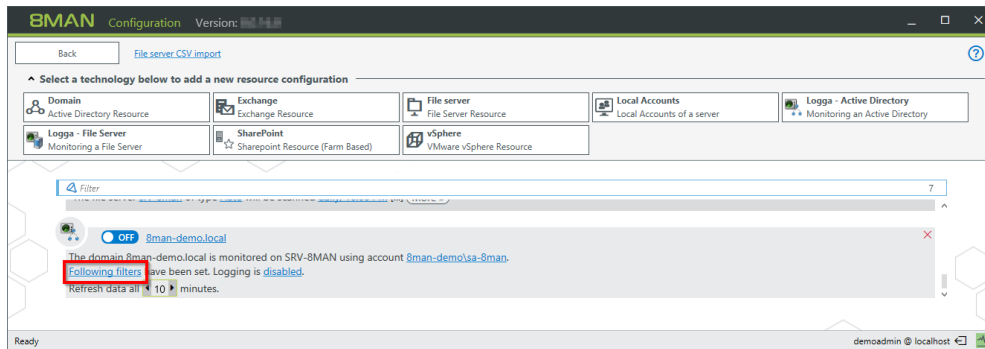
For example:

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

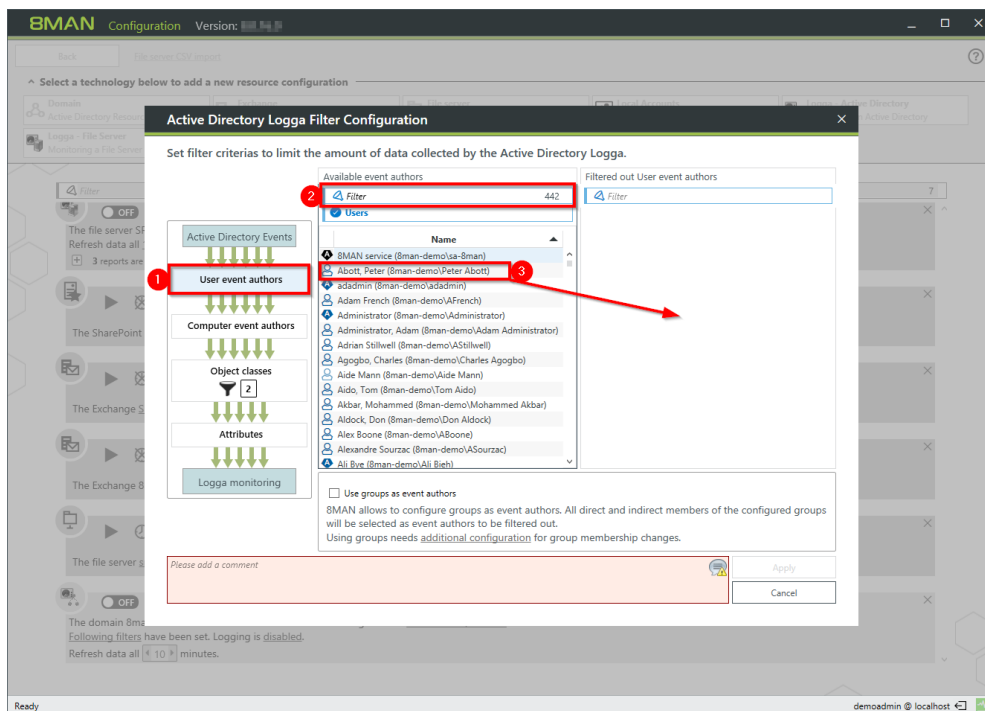
Please note:

Not all security logs include affected object classes or attributes. For example changes to group memberships will not be excluded, even if the object classes "User" and "Group" and the attribute "Member" are configured as filters.

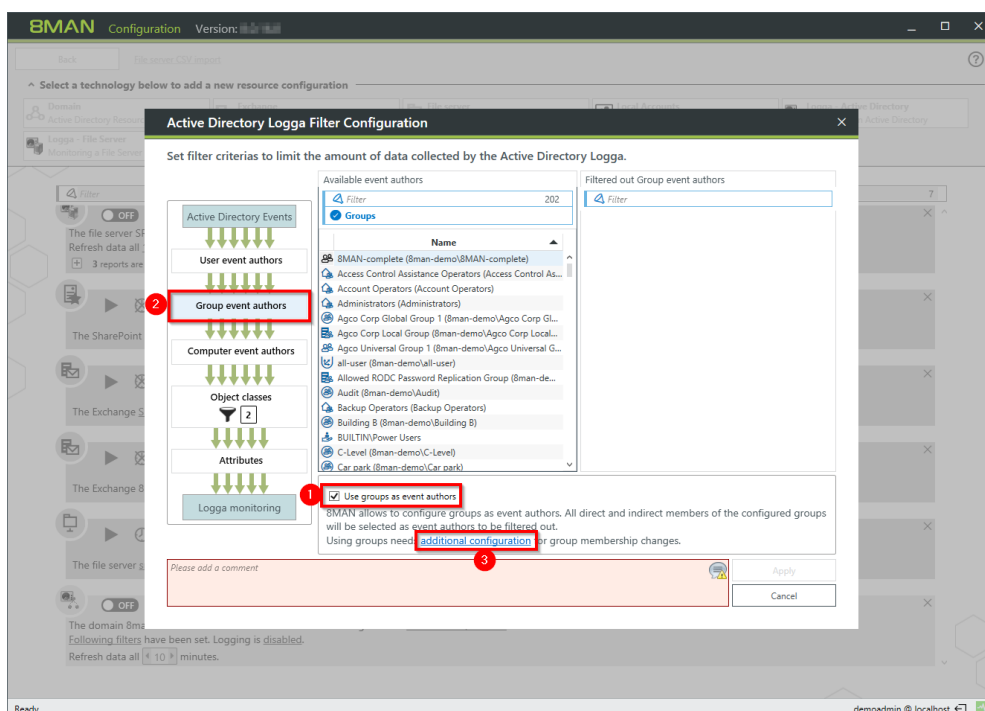
3.1.5.1.2 Configure event filters



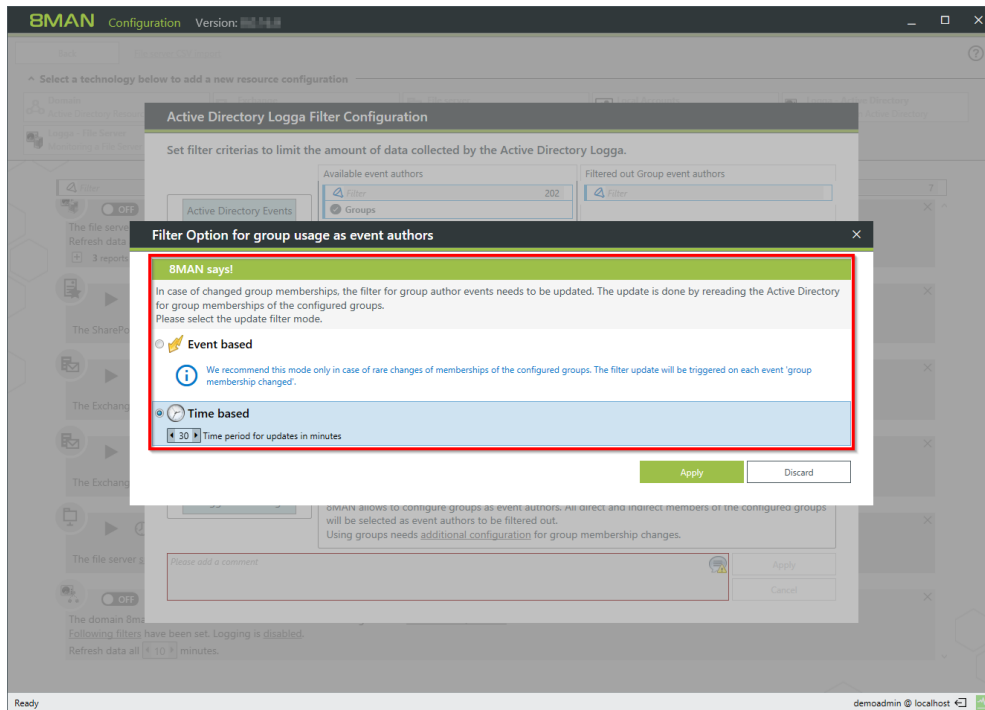
Click on the link "Following filters".



1. Filter events related to specific users.
2. Use the filter to find the desired user. You can search for either display name or CommonName.
3. Select the desired user and move him with drag&drop into the right hand column.



1. You can filter groups as event authors. Activate the option.
2. The filter level is shown. By moving groups into the right hand column with drag & drop, all events of users who are direct or indirect members of that group are filtered and excluded.
3. Click on "additional configuration".



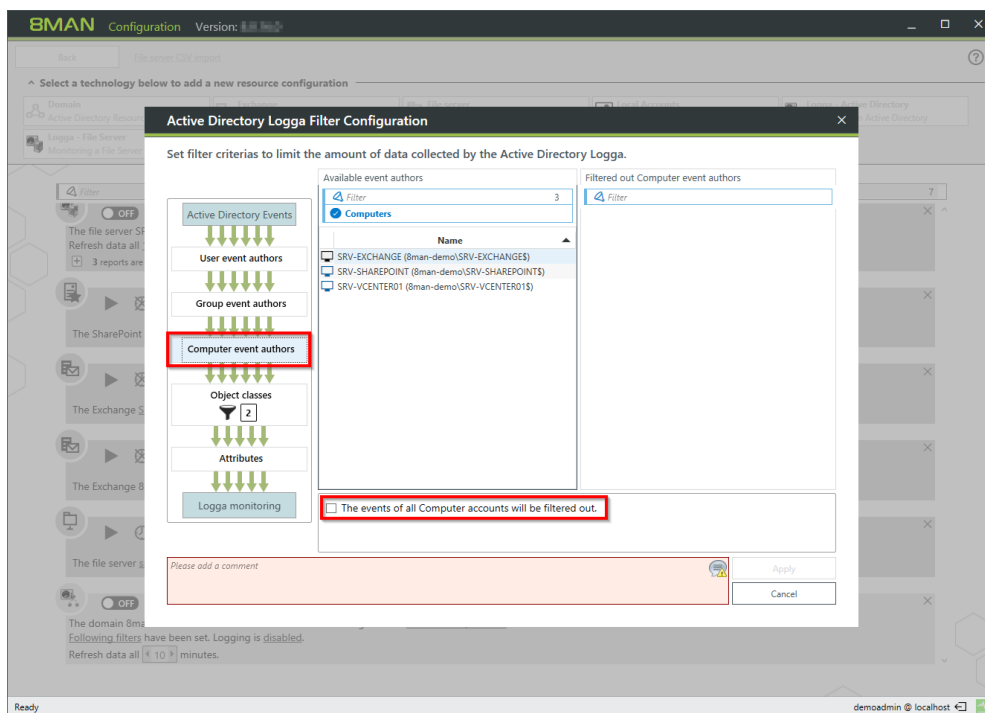
Determine which mode is used by the filter to update group memberships.

Please note the information in the displayed dialog.

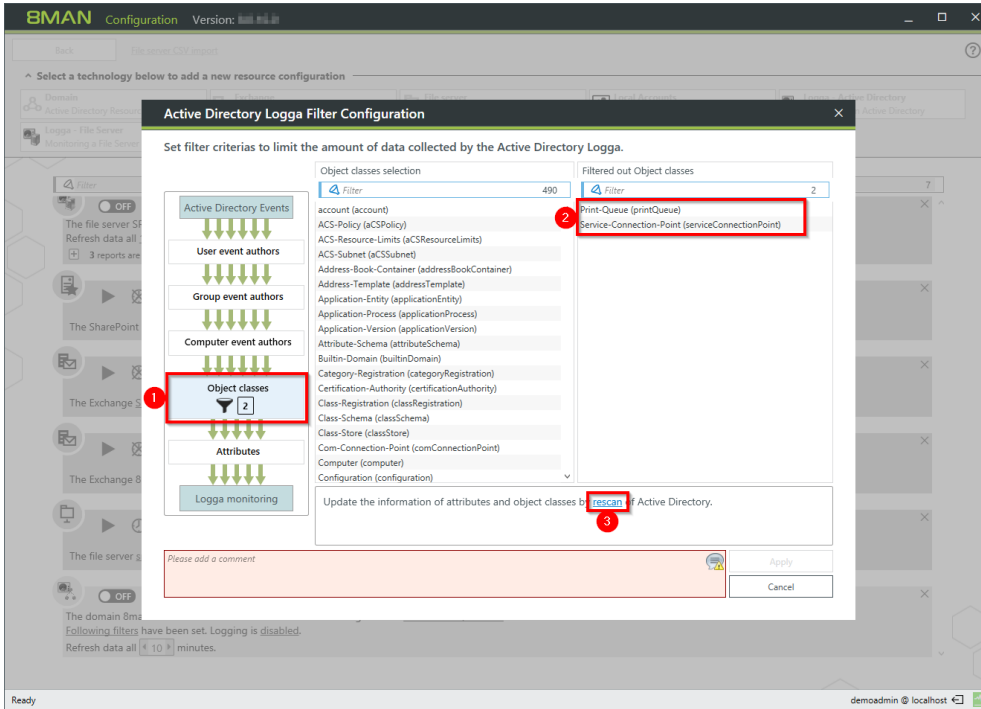
Only use "event-based" if memberships in the filtered groups change rarely.

The update interval for the "time-based" option can be set anywhere between 10 and 1440 min (24h).

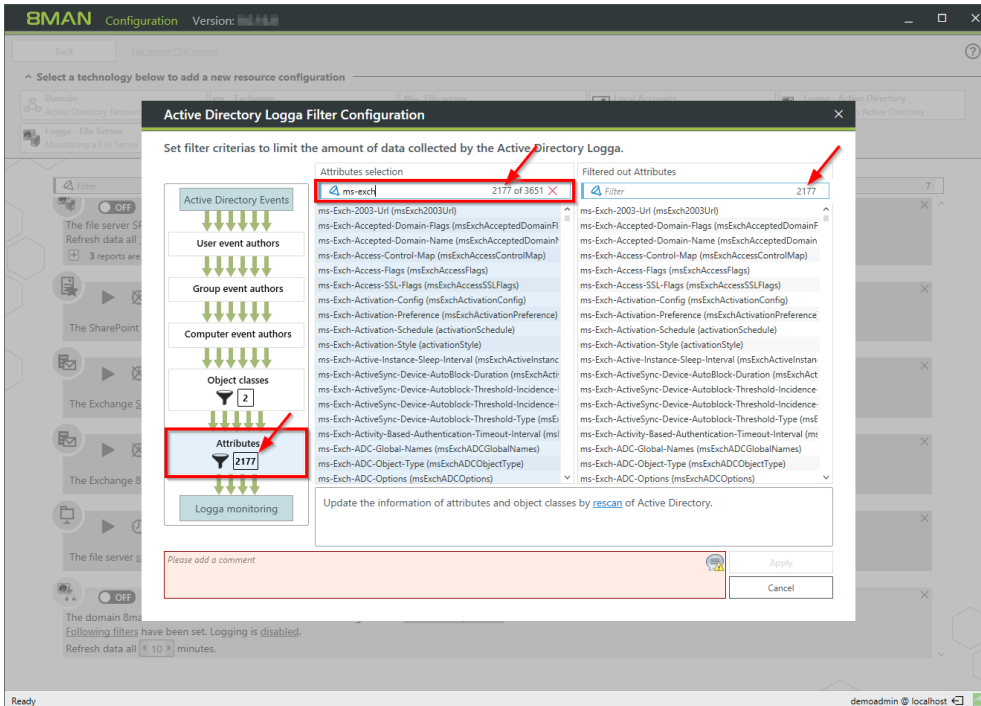
The shorter the interval, the higher the load on your AD.



Filter events for selected or all computer accounts.



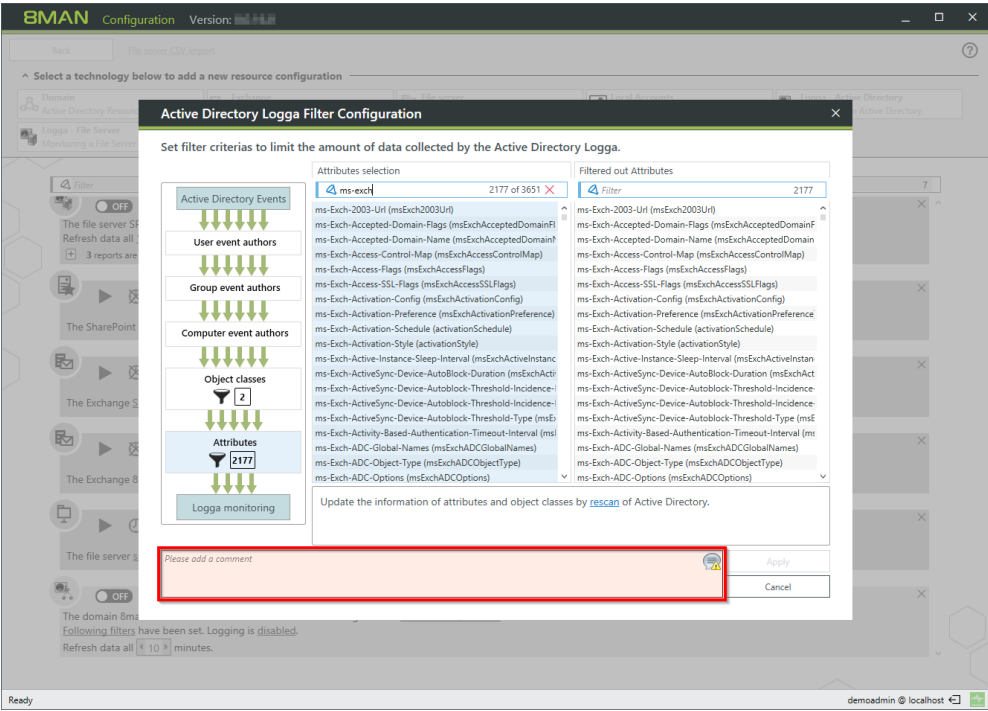
1. Filter the events of specific object classes.
2. By default events relating to the two selected object classes will be filtered.
3. The initial loading (and a rescan) of object classes from AD may take some time. After that the object classes will be loaded from the data base.



Filter events related to specific attributes.

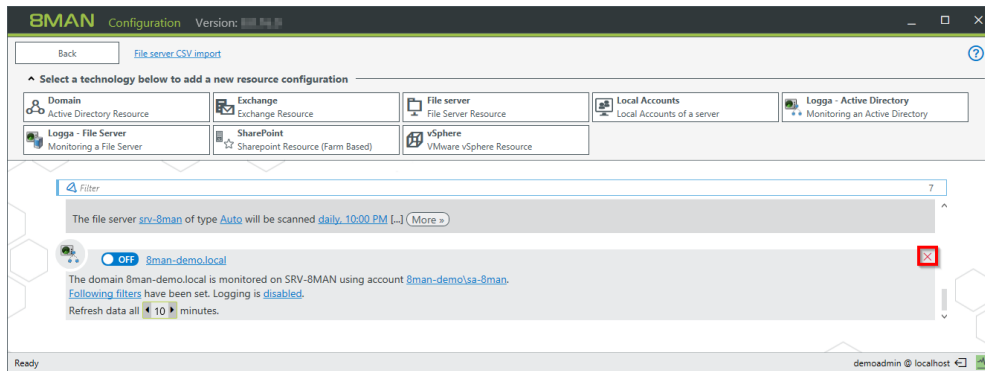
For example:

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



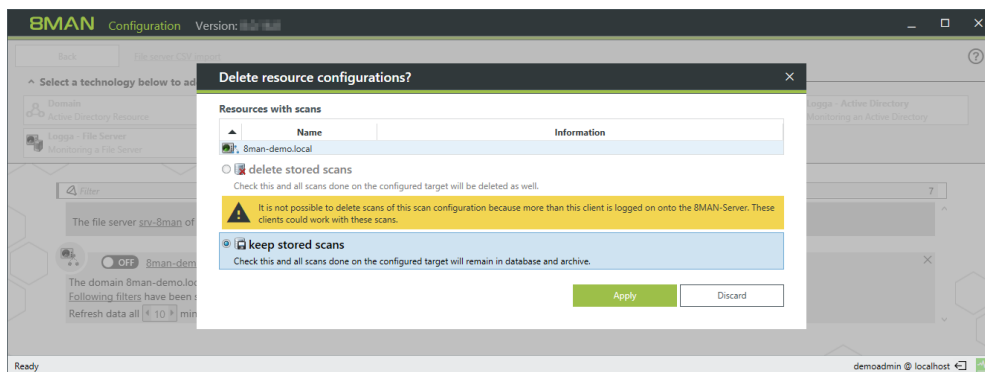
You must enter a comment to apply any changes made to filter settings.

3.1.6 Delete an AD Logga configuration



On the configuration home page select "Scans".

Select the desired AD Logga configuration. Click on the red "X".

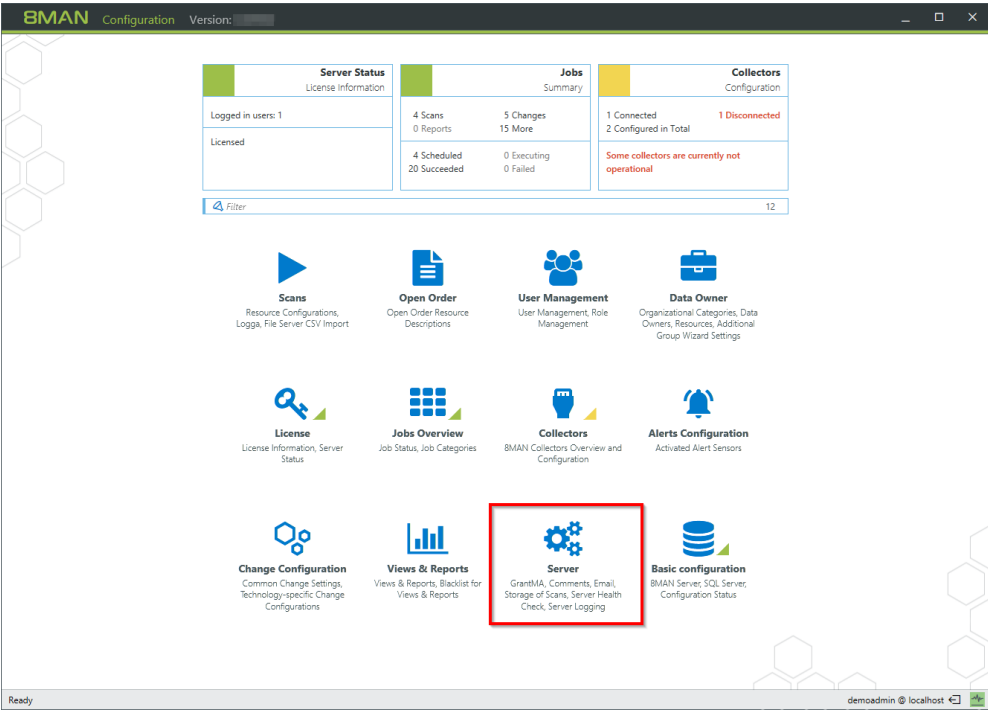


You can decide if you would like to keep or delete the available Logga data.

Deleting is only possible if all user interfaces are closed.

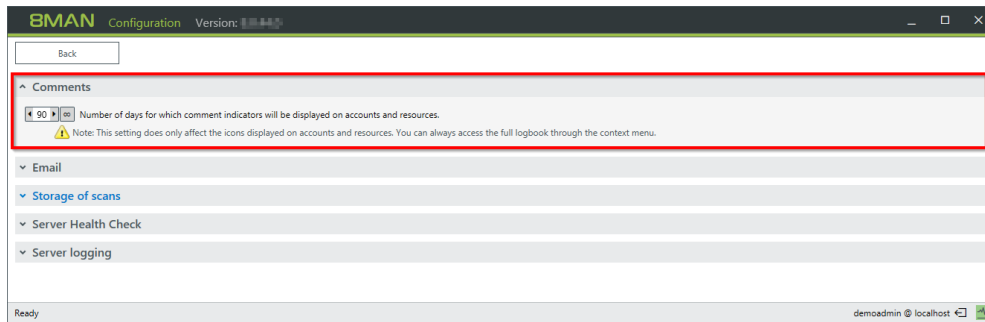
You can identify logged in users in the server status menu.

4 Server



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

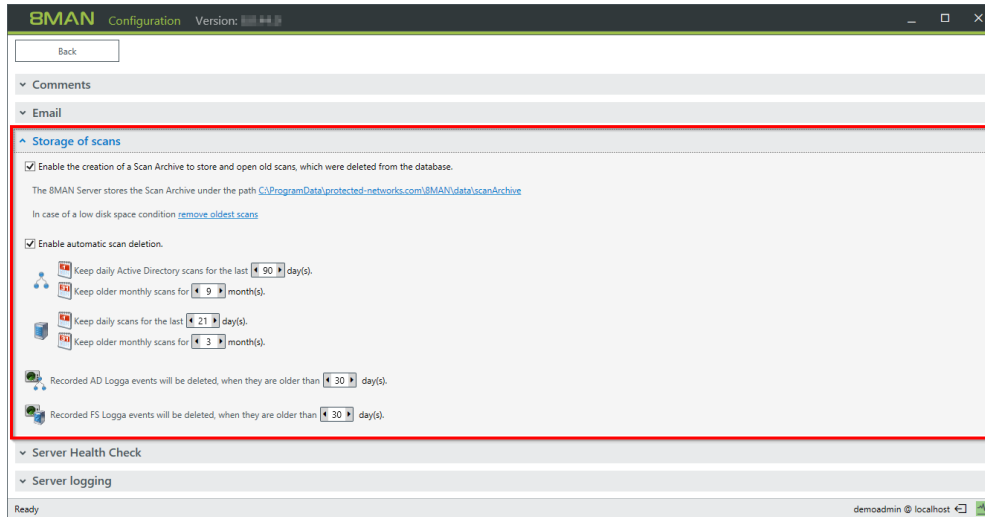
4.1 Set the display duration for comment icons



8MAN shows a note icon for stored comments or AD Logga information.

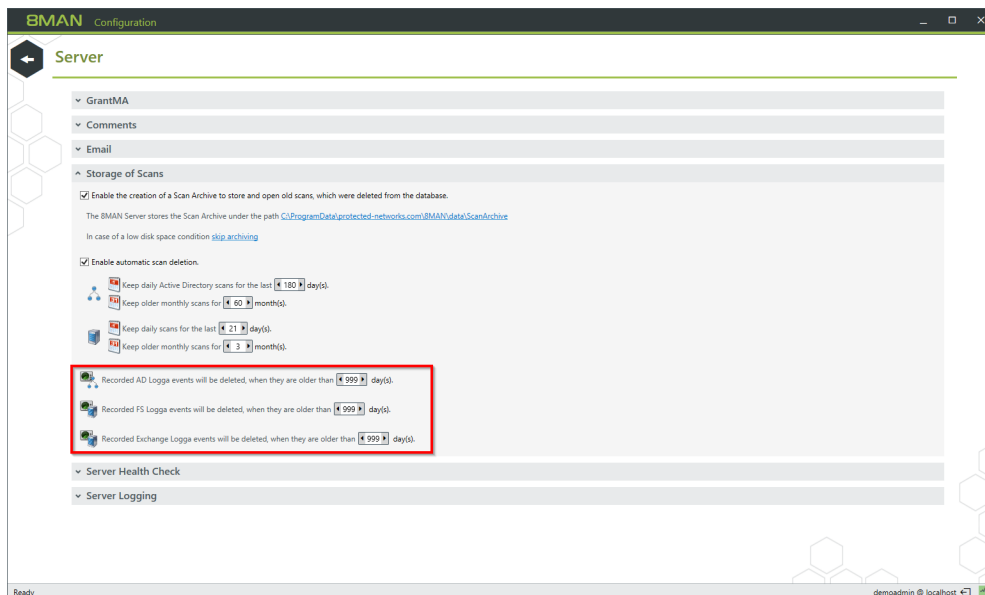
The longer you use 8MAN, the more notes will be created. You can reduce the length of time that notes are displayed, if you see too many notes.

4.2 Configure storage time for AD Logga data



The "Storage of Scans" configuration allows you to determine how long scan and Logga data are stored. This affects the size of your data base and required disk storage.

Please refer to the chapter SQL Express.



Determine how long 8MAN Logga data is stored.

Every event requires approximately:

FS Logga: ca. 50 Bytes

AD Logga: ca. 600 Bytes.

5 Evaluate AD Logga data

5.1 Monitor 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

- Users
- Groups
- Computers

Additionally you are able to filter according to object class and attribute. Please note that these settings are geared towards expert users. If you apply a filter for a rare object this may cause the report to deliver unexpected results.

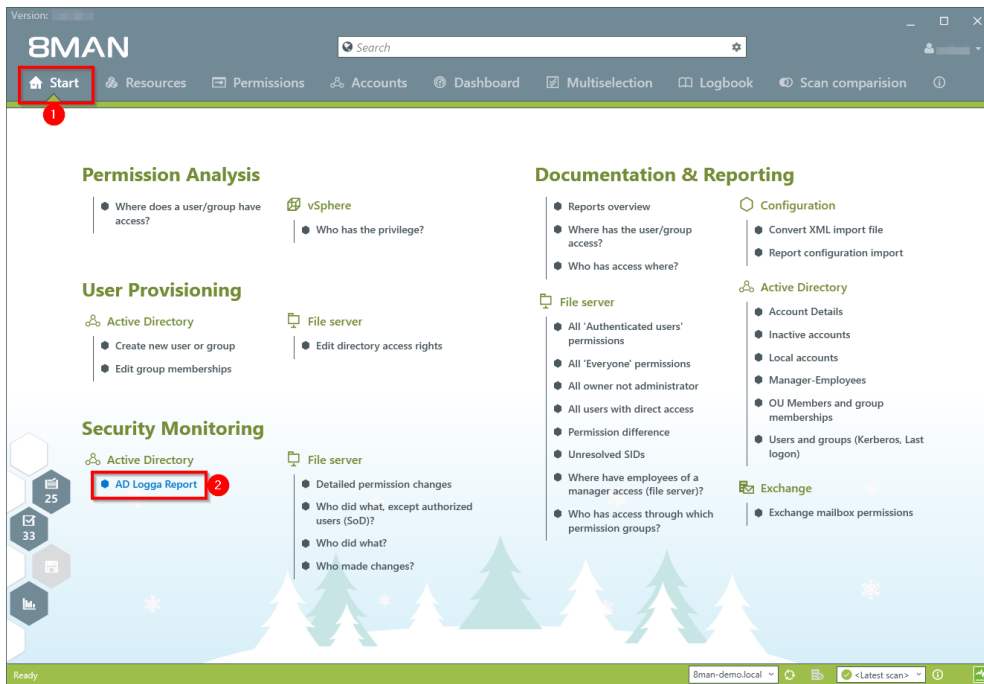
Additional services

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

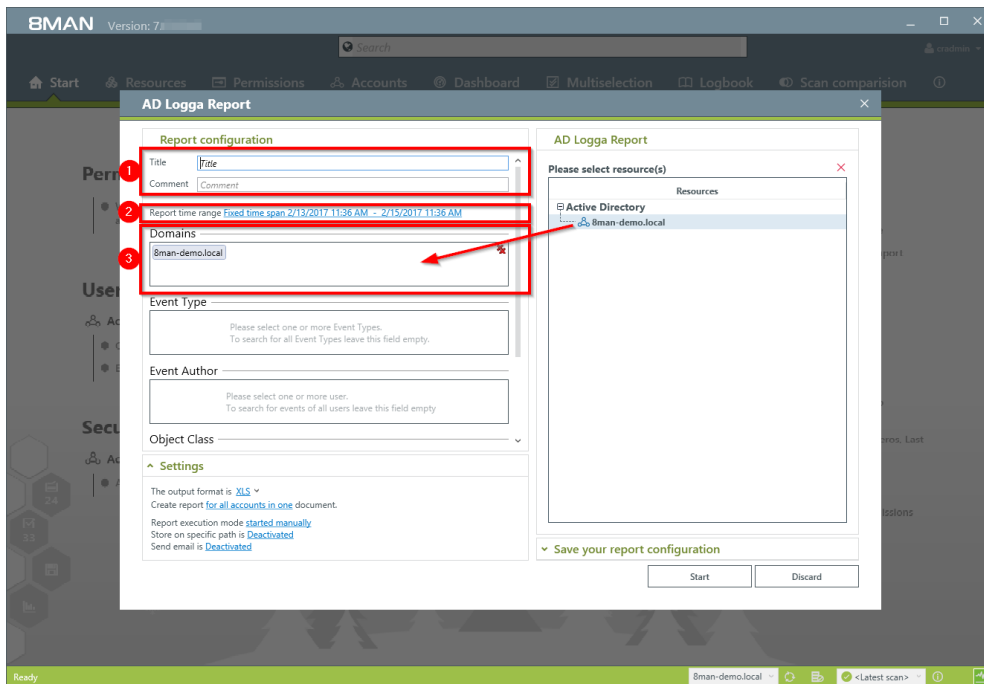
[Set alerts for groups](#)

[Set alerts for user accounts](#)

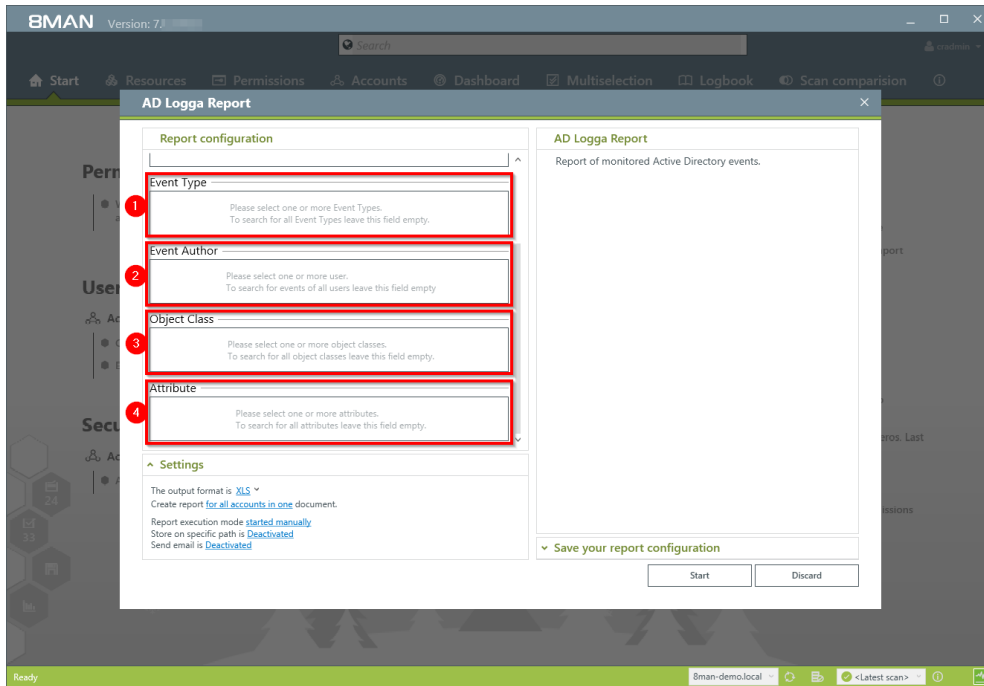
Step by step process



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

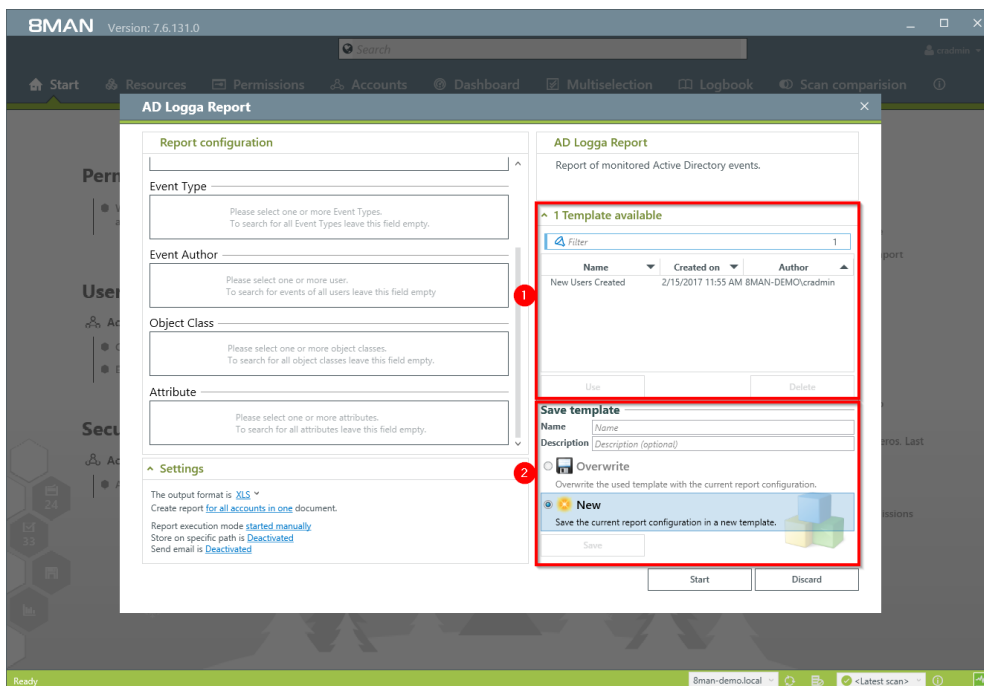


1. Enter a title for the report and add a comment.
2. Define the date range of the report.
3. Select domains whose events should be captured in the report.



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

1. Add the type of events that you would like to include in the report.
2. Add the authors of events that you would like to include in the report.
3. Add all object classes that you would like to include in the report.
4. Add all attributes that you would like to include in the report.



By saving AD Logga report configurations as templates you can save valuable time by reusing complex report configurations.

1. Select an existing template.
2. Save the current configuration as a template.

8MAN Version: 7.6.131.0

Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparison

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 users.
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

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

Use Delete

Save template
Name
Description

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

☒ **New**
Save the current report configuration in a new template.

Start Discard

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

5.2 Identify temporary group memberships

Background / Value

8MATE Logga closes a number of important security gaps. One of the most important one is temporary group memberships. Insider threats grant themselves access to secret directories, copy data and then revert back to the original state after performing their desired actions. Without the AD Logga these types of activities remain undetected.

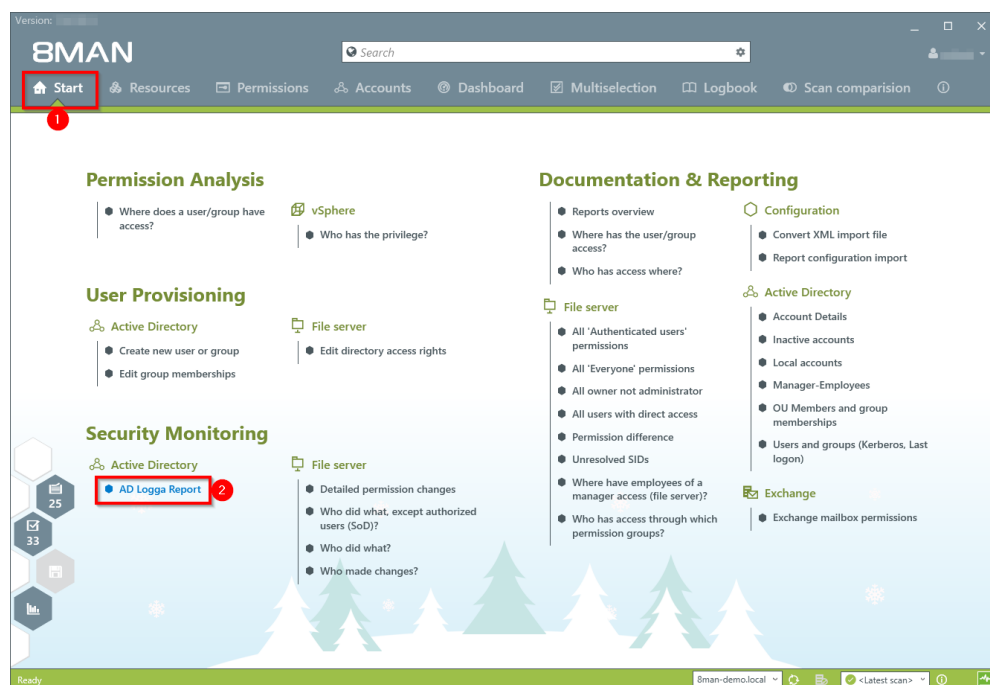
Additional Services

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

[Set alerts for groups](#)

[Set alerts for user accounts](#)

Step by step process



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

Report configuration

Title

Comment

Report time range [Fixed time span 2/13/2017 12:04 PM - 2/15/2017 12:04 PM](#)

Domains

Event Type

Event Author

Object Class

Settings

The output format is [XLS](#)

Create report [for all accounts in one](#) document.

Report execution mode [started manually](#)

Store on specific path is [Deactivated](#)

Send email is [Deactivated](#)

AD Logga Report

Event Type 18

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

1 Template available

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.

5.3 Identify locked user accounts

Background / Value

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

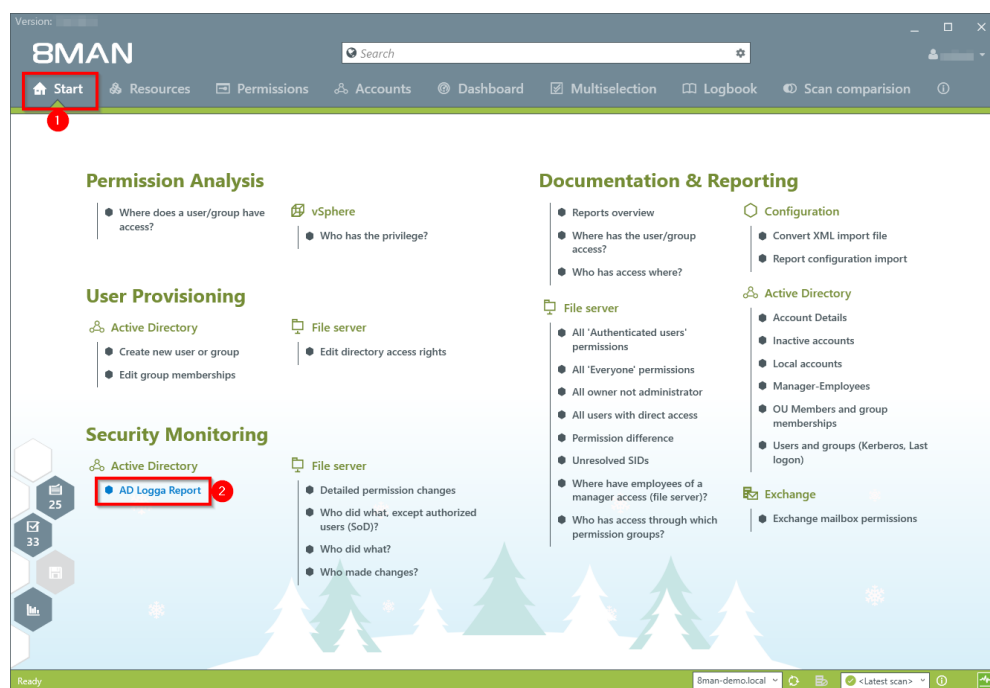
Additional services

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

[Set alerts for groups](#)

[Set alerts for user accounts](#)

Step by step process



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

Report configuration

Title

Comment

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

Domains

Event Type

Event Author

Object Class

Settings

The output format is [XLS](#)

Create report [for all accounts in one](#) document.

Report execution mode started manually

Store on specific path is [Deactivated](#)

Send email is [Deactivated](#)

AD Logga Report

Event Type 18

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

1 Template available

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

5.4 Monitor password resets

Background / Value

With the 8MATE AD Logga you can monitor the process of resetting passwords. Within this process there is an inherent security risk. For example, if a helpdesk employee secretly resets the password of a manager or executive, they can sign on with a temporary password and gain access to sensitive information. The Manager would probably not notice this and only be confused about why his password is no longer valid, perhaps even thinking that he forgot his password, and then simply request a new one from support.

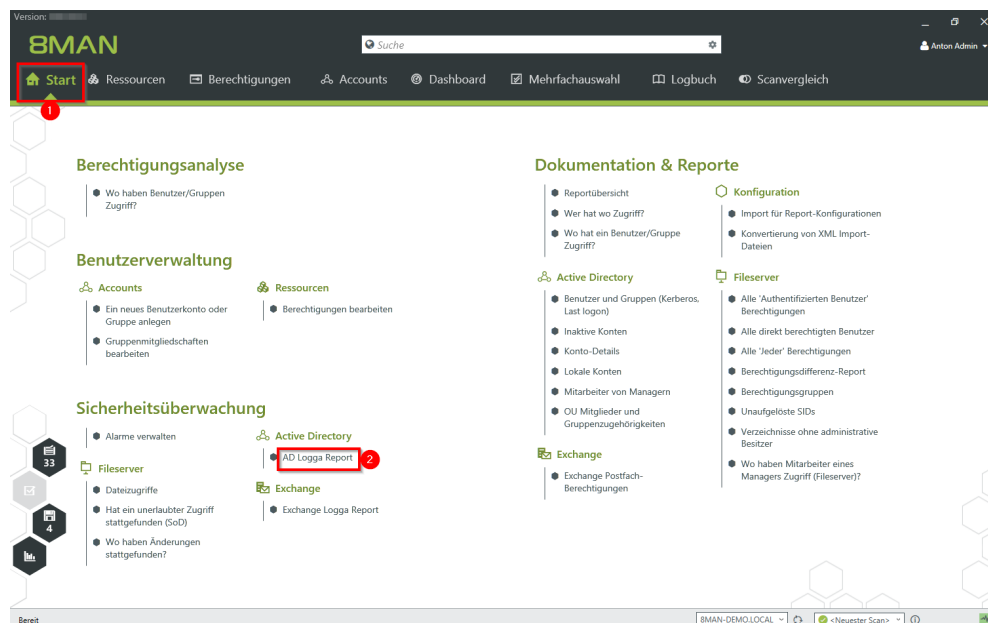
Additional Services

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

[Set alerts for groups](#)

[Set alerts for user accounts](#)

Step by step process



1. Select "Start".

2. Click on "AD Logga Report".

Report-Konfiguration

Titel:

Kommentar:

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

Domänen:

Ereignistyp:

Ereignis-Autor:

Objekt Klasse:

Einstellungen

Das Ausgabeformat ist **XLS**

Reportausführung wird **manuell gestartet**

Speichern ist **deaktiviert**

E-Mail Versenden ist **deaktiviert**

AD Logga Report

Ereignistyp:

Filter:

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.

Zeit	Autor	Objekt	Objektklasse	Ereignis	Attribut Name
26.02.2014 16:56	cradmin (8man-demo/cradmin)	Bino, Al (8man-demo/Al Bino)	User(user)	Kenntwort zurücksetzen	
28.02.2014 15:40:35	cradmin (8man-demo/cradmin)	Zifer, Lou (8man-demo/Lou Zifer)	User(user)	Kenntwort zurücksetzen	
11.03.2014 09:15:01	Administrator (8man-demo/Administrator)	Zifer, Lou (8man-demo/Lou Zifer)	User(user)	Kenntwort zurücksetzen	
13.03.2014 14:50:42	Administrator (8man-demo/Administrator)	Zifer, Lou (8man-demo/Lou Zifer)	User(user)	Kenntwort zurücksetzen	
10.03.2015 11:49:04	neadmin (8man-demo/neadmin)	Borg, Inge (8man-demo/Inge Borg)	User(user)	Kenntwort zurücksetzen	
10.03.2015 12:31:32	neadmin (8man-demo/neadmin)	Borg, Inge (8man-demo/Inge Borg)	User(user)	Kenntwort zurücksetzen	
10.03.2015 15:12:28	Administrator (8man-demo/Administrator)	Krise, Christiane (8man-demo/Christiane Krise)	User(user)	Kenntwort zurücksetzen	
10.03.2015 15:47:05	Administrator (8man-demo/Administrator)	Ander, Ole (8man-demo/Ole Ander)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Aber, Mark (8man-demo/Mark Aber)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Alien, Arnold (8man-demo/Arnold Alien)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Aloe, Vera (8man-demo/Vera Aloe)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Ander, Ole (8man-demo/Ole Ander)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Ander, Cori (8man-demo/Cori Ander)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Aner, Dominik (8man-demo/Dominik Aner)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Angebrandt, Angie (8man-demo/Angie Angebrandt)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Apfel, Adam (8man-demo/Adam Apfel)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Arbeit, Andi (8man-demo/Andi Arbeit)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Arm, Armin (8man-demo/Armin Arm)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Aroni, Mark (8man-demo/Mark Aroni)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Asil, Claire (8man-demo/Claire Asil)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Auer, Karl (8man-demo/Karl Auer)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Auhss, Ann (8man-demo/Ann Auhss)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Autsch, Anke (8man-demo/Anke Autsch)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Azubi, Andy (8man-demo/Andy Azubi)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Baba, Ali (8man-demo/Ali Baba)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Bach, Klara (8man-demo/Klara Bach)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Baer, Johannes (8man-demo/Johannes Baer)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Baer, Roy (8man-demo/Roy Baer)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Baern, Al (8man-demo/Al Baern)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Balken, Don R. (8man-demo/Don R. Balken)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Becher, Joe Kurt (8man-demo/Joe Kurt Becher)	User(user)	Kenntwort zurücksetzen	
10.03.2015 16:50:09	neadmin (8man-demo/neadmin)	Beiter, Walter (8man-demo/Walter Beiter)	User(user)	Kenntwort zurücksetzen	

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

5.5 Analyze AD Logga events with the logbook

Background / Value

By using the reports you can regularly analyze all the tracked events at a detailed level. You can find the information needed much faster by using the logbook.

Additional Services

[Identify temporary group memberships](#)

[Identify locked user accounts](#)

[Monitor password resets](#)

[Set alerts for groups](#)

[Set alerts for user accounts](#)

Step by step process

The screenshot shows the 8MAN Logbuch interface. The top navigation bar includes 'Start', 'Ressourcen', 'Berechtigungen', 'Accounts', 'Dashboard', 'Mehrfachauswahl', 'Logbuch' (highlighted with a red box and number 1), and 'Scanvergleich'. Below the navigation bar, the 'Logbuch' section is active, showing a calendar view for 'Freitag, 7. Oktober 2016'. The calendar has a time range of 'Von 6 Monate zuvor bis Heute' (highlighted with a red box and number 2). The calendar shows various events with icons and numbers. A red box and number 3 highlight the 'Logbuch' tab. A red box and number 4 highlight the 'Logbuch' section. The right pane shows a list of events with columns for 'Zeit', 'Autor', and 'Kommentar'. The events are filtered to show all events of one day (highlighted with a red box and number 4). The bottom status bar shows 'Bereit' and '8MAN-DEMO.LOCAL'.

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.

The screenshot shows the 8MAN Logbuch interface. On the left is a calendar view from Friday, October 7, 2016, to today. The calendar has columns for different event types: Änderungen gesamt, Konto aktiviert, Kennwort zurückgesetzt, Attribut geändert, Benutzer entfernt, Benutzer hinzugefügt, Gruppe erstellt, Berechtigung geändert, Logga Konfiguration, Logga Status-Modulungen, Abrechnung-Katalog, and Sendungen. A red circle '1' highlights a date in the calendar. On the right, a detailed view for Friday, October 7, 2016, is shown. It includes a filter bar and a table of events. A red circle '2' points to the 'Zeit' column header, and a red circle '3' points to the 'Kommentar' column. The table shows events from 'Administrator (8man-demo\Administrator)' and 'cradmin (8man-demo\cradmin)'. Below the table, a specific event is expanded, showing 'Gruppenmitgliedschaft geändert' and 'AD Logga für 8man-demo.local'.

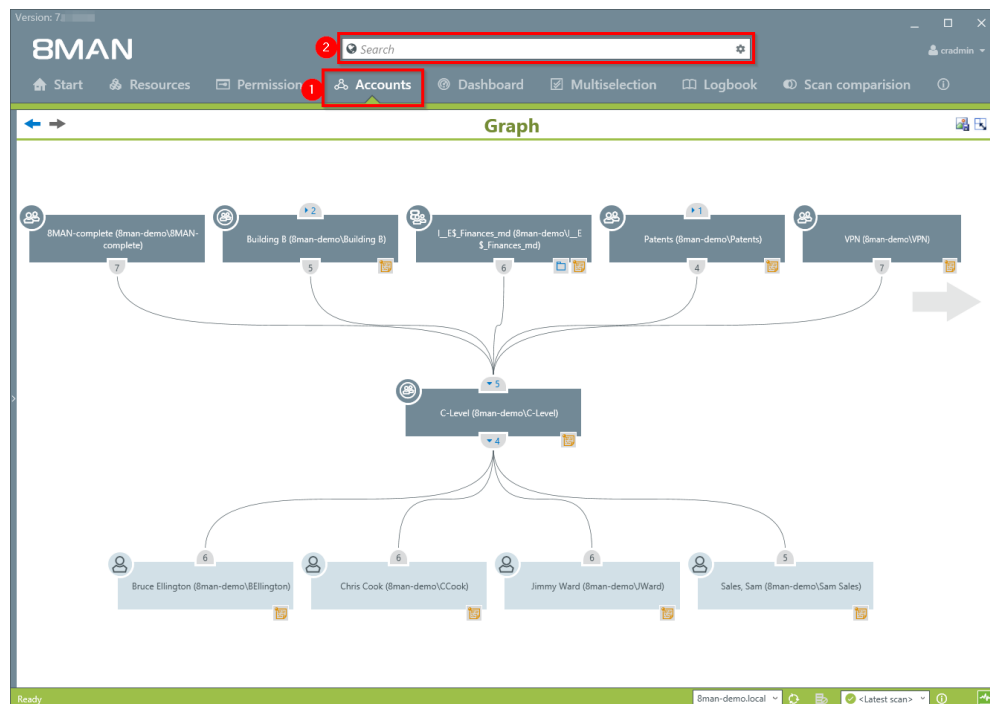
1. Select a cell (an event type) to filter the results to your request.
2. 8MAN displays all results. The footsteps indicate the AD Logga results. Select a result.
3. 8MAN displays all details to the result.

5.6 Identify the most recent actions on an account

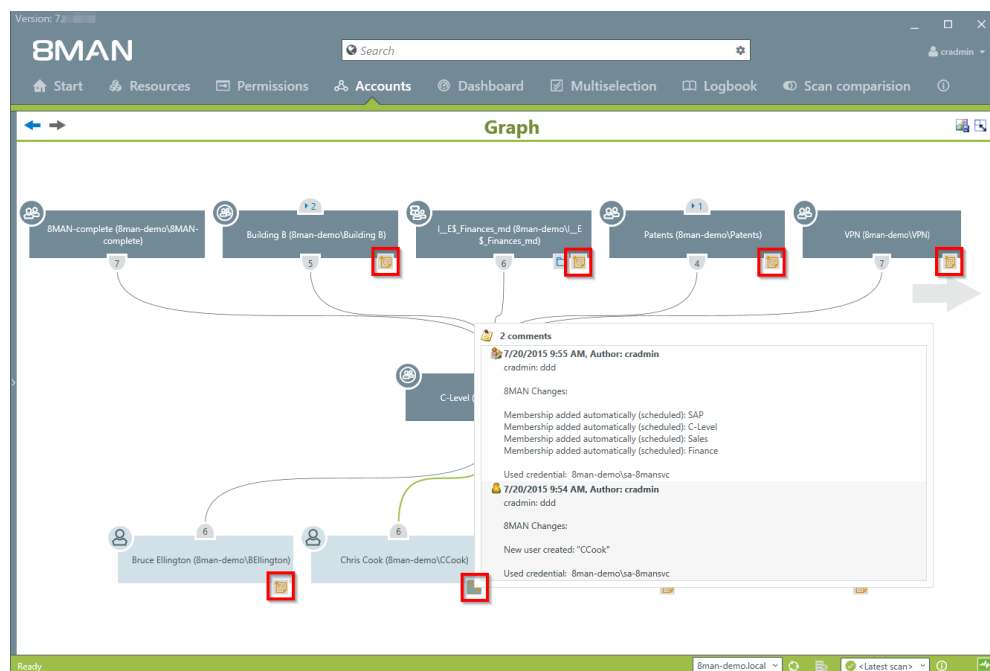
Background / Value

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

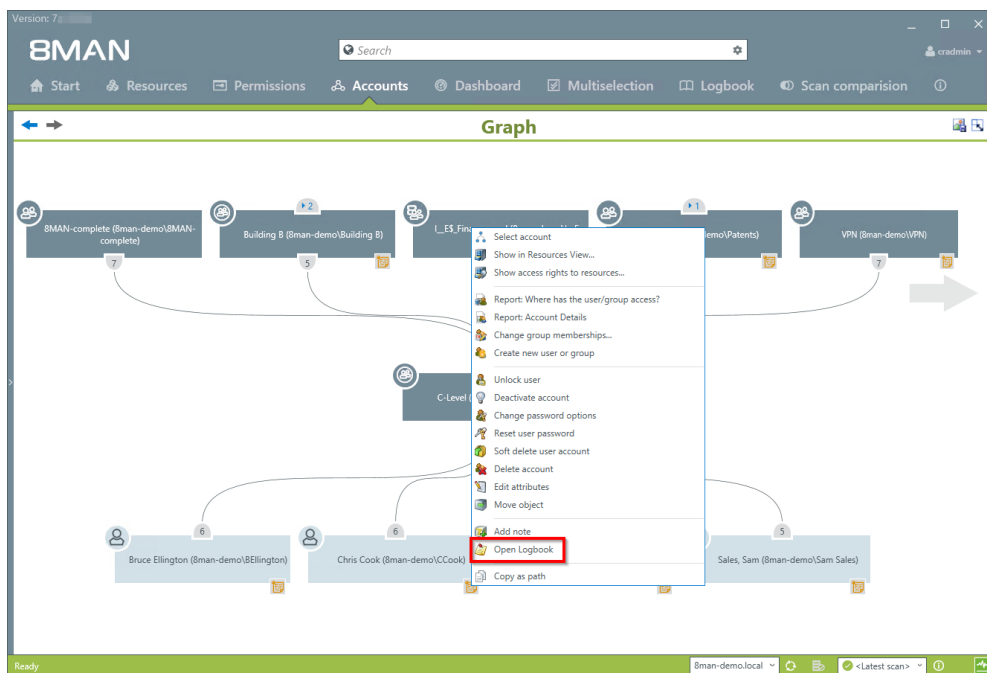
Step by step process



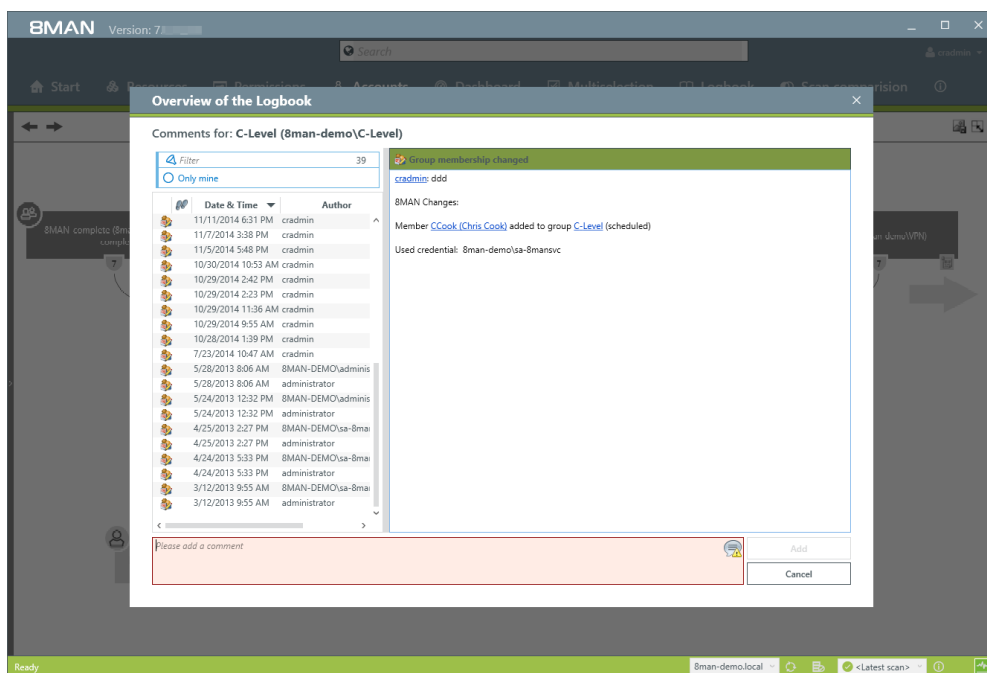
1. Select "Accounts".
2. Search for the desired user or group.



The note icon indicates that activities were recorded in the 8MAN log book. You can hover over the icon to see an overview of the latest activities related to the account.



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



Review past activities related to a user account.

You can enter a comment into the log book.

The footprint icon indicates that these actions were recorded by AD Logga.

6 Configure alerts

The screenshot shows the 8MAN Configuration interface. At the top, there are three summary tables: Server Status, Jobs, and Collectors. Below these are various configuration options represented by icons and text. The 'Alerts Configuration' option, which includes 'Activated Alert Sensors', is highlighted with a red rectangular box.

Server Status	Jobs	Collectors
License Information	Summary	Configuration
Logged in users: 2	48 Scans 1 Reports	1 Connected 1 Configured in Total
Licensed	22 Changes 32 More	All Collectors are Operational
	4 Scheduled 59 Succeeded	
	0 Executing 40 Failed	

Filter 12

- Scans**: Resource Configurations, Logga, File Server CSV Import
- Open Order**: Open Order Resource Descriptions
- User Management**: User Management, Role Management
- Data Owner**: Organizational Categories, Data Owners, Resources, Additional Group Wizard Settings
- License**: License Information, Server Status
- Jobs Overview**: Job Status, Job Categories
- Collectors**: 8MAN Collectors Overview and Configuration
- Alerts Configuration**: Activated Alert Sensors
- Change Configuration**: Common Change Settings, Technology-specific Change Configurations
- Views & Reports**: Views & Reports, Blacklist for Views & Reports
- Server**: GrantMA, Comments, Email, Storage of Scans, Server Health Check, Server Logging
- Basic configuration**: 8MAN Server, SQL Server, Configuration Status

Ready demoadmin @ localhost

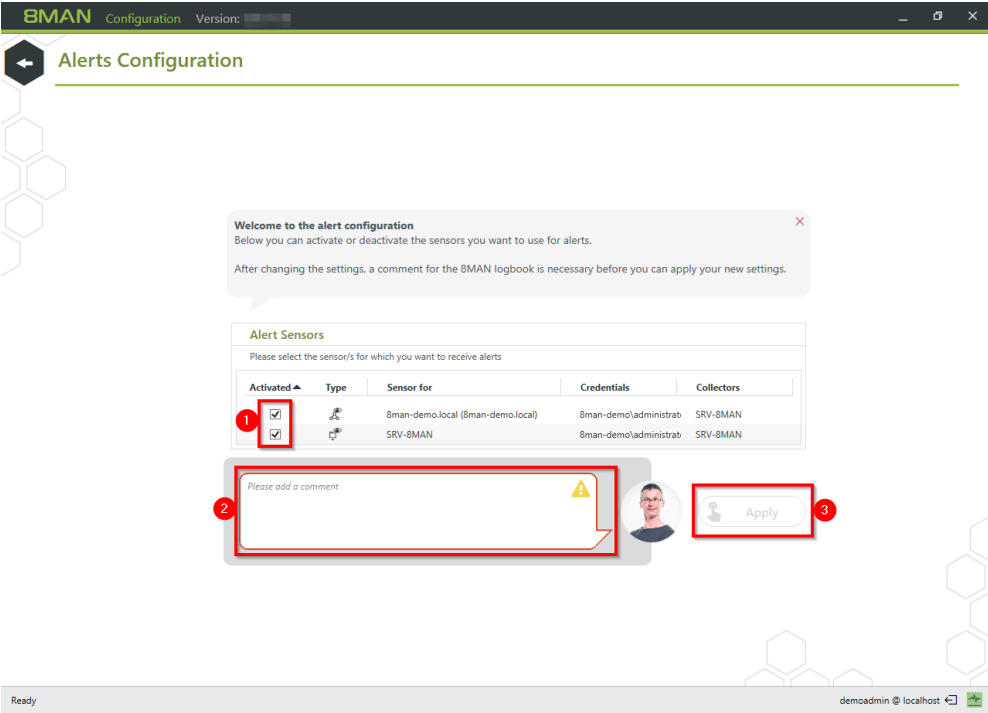
In the "Alerts" category, activate and deactivate the alert sensors.

With active alert sensors, you can create alerts for groups or user accounts.

Manage alerts in the 8MAN user interface.

You need a license for the 8MATE AD Logga or FS Logga.

6.1 Enable/disable alert sensors



- 1. Enable/disable alert sensors.
- 2. You must enter a comment.
- 3. Apply the settings.

Only with active alarm sensors are the alarm configurations effective.

6.2 Set alerts for groups

Background / Value

Employees receive their access rights through group memberships. Especially sensitive groups grant access to secret folders and other important resources. 8MATE AD Logga allows you to actively monitor specific AD groups so that an alert is received if new members are added.

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

Additional services

[Set alerts for user accounts](#)

[Manage alerts](#)

Step by step process



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

Create alert

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

1 **Name** The name is used in the actions to identify the event (e.g. mail subject)
Group memberships changed for Domain Admins (8man-demo\Domain Admins) (max. 70 characters)

2 **Event** Group memberships changed
☒ Observe indirect group memberships

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

☒ **Action** Write to Windows event log

4 New policy to monitor domain admins group.

5 **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.

6.3 Set alerts for user accounts

Background / Value

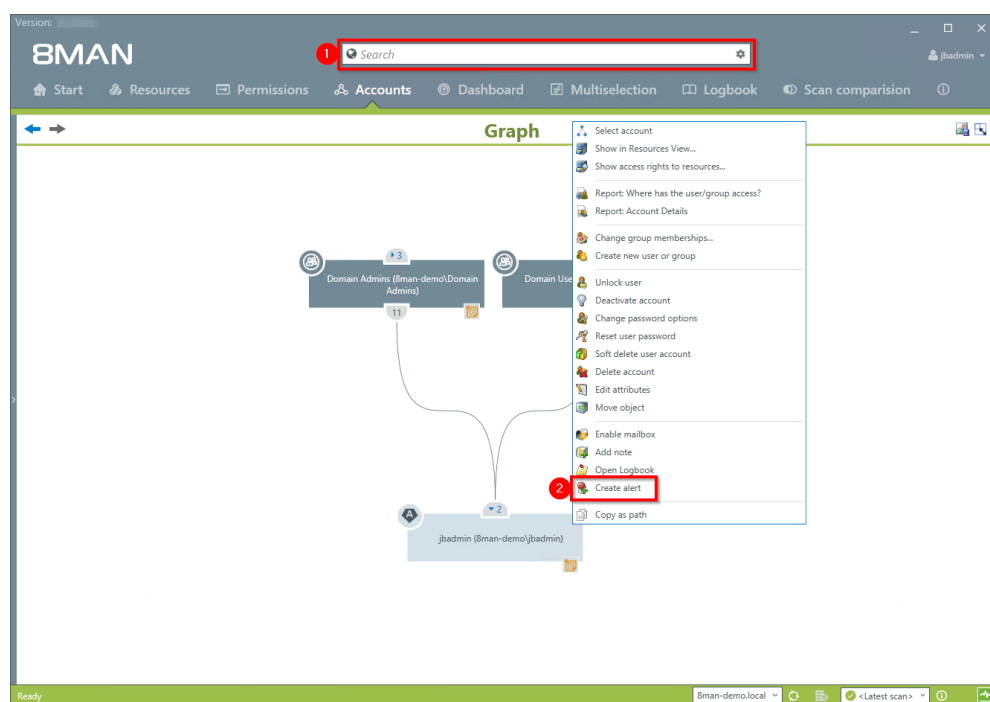
The 8MATE AD Logga allows you to monitor the process of resetting passwords. Within this process there is an inherent security risk. For example, if a helpdesk employee secretly resets the password of a manager or executive, they can sign on with a temporary password and gain access to sensitive information.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

Additional services

[Set alerts for groups](#)

[Manage alerts](#)

Step by step process



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

8MAN Version: 8.0.0.0

Start Resources Permissions Accounts Dashboard Multiselection Logbook Scan comparison

Graph

Create alert

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

1 Name The name is used in the actions to identify the event (e.g. mail subject).
Account locked for jbadmin (8man-demo\jbadmin) max: 10 characters

2 Event Account locked

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

4 Comment Demo

Create Cancel

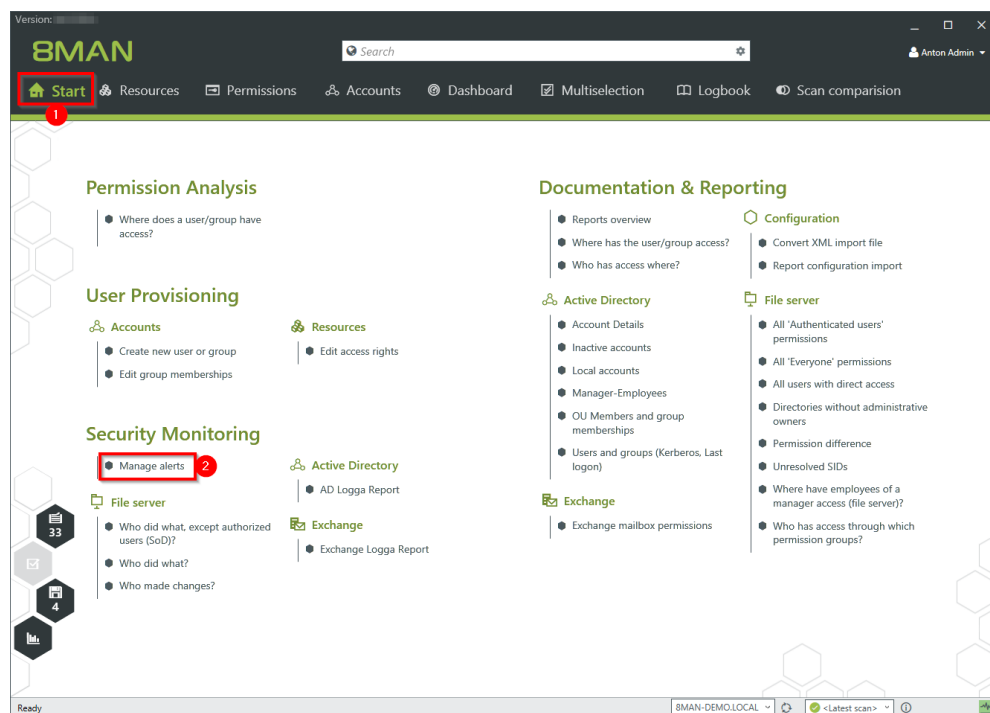
1. Enter a title for the alert.
1. Select an event for which you want to receive the alert.
2. You can select any number of email recipients. Additionally alerts can be displayed in the windows event log.
3. You must enter a comment.
4. Create the alert.

6.4 Manage alerts

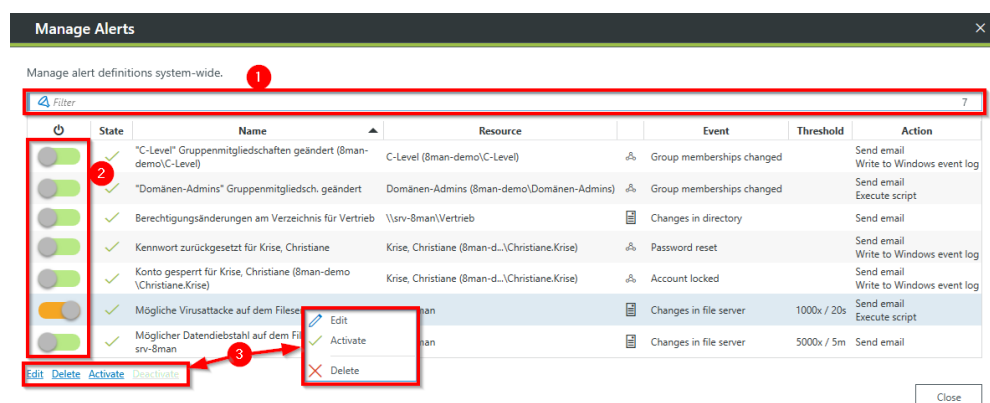
Background / Value

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

Step by step process



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



8MAN shows you all alert configurations.

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

7 Contact 8MAN Support

You can reach our support under the following number:

Germany (German and English)

+49 30 390 6345-99

United Kingdom (English)

+44 12 76 91 99 89

Monday through Friday from 9 am until 5 pm (CET).

E-Mail

support@8man.com

Website

<https://susi.8man.com>

You start on the website with a self-registration. After completion, you can see the publicly accessible content. After registration, you will be assigned to an authorization level by our support team. Only then you can see non-public content and use the ticket system. This process may take some time.

8 Disclaimer

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

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

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

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

Copyright

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

All product and company names are trademarks™ or registered® trademarks of their respective holders even without special marking.

Protected Networks GmbH
Alt-Moabit 73
10555 Berlin

+49 30 390 63 45 - 0

www.protected-networks.com

9 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/LICENSE.txt?at=defaultjquery-tablesort>
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC
<https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE>
- Mustache.js, © 2009 Chris Wanstrath (Ruby), © 2010-2014 Jan Lehnardt (JavaScript) and © 2010-2015 The mustache.js community <https://github.com/janl/mustache.js/blob/master/LICENSE>
- Metro UI CSS 2.0, © 2012-2013 Sergey Pimenov, <https://github.com/olton/Metro-UI-CSS/blob/master/LICENSE>
- Underscore.js, © 2009-2016 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors
<https://github.com/jashkenas/underscore/blob/master/LICENSE>
- Ractive.js, © 2012-15 Rich Harris and contributors, <https://github.com/ractivejs/ractive/blob/dev/LICENSE.md>
- RequireJS, © 2010-2015, The Dojo Foundation, <https://github.com/jrburke/requirejs/blob/master/LICENSE>
- typeahead.js, © 2013-2014 Twitter, Inc, <https://github.com/twitter/typeahead.js/blob/master/LICENSE>
- Select2, © 2012-2015 Kevin Brown, Igor Vaynberg, and Select2 contributors
<https://github.com/select2/select2/blob/master/LICENSE.md>
- bootstrap-datepicker, © Copyright 2013 eternicode <https://github.com/eternicode/bootstrap-datepicker/blob/master/LICENSE>
- RabbitMQ, © Copyright 2007-2013 GoPivotal, <https://www.rabbitmq.com/mpl.html>
- EPPlus, JanKallman, <https://github.com/JanKallman/EPPlus/blob/master/LICENSE>

