

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

		50
7	Contact 8MAN Support	F C
6.4	Manage alerts	. 55
6.3	Set alerts for user accounts	. 53
6.2	Set alerts for groups	. 51
0.1	Enable/disable alert sensors	. 50

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

Fileserver

8MATE AD Logga

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 tracable and transparent.

This is achieved with the AD Logga

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

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 <u>system requirements</u>.

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

File Action View Help					
🗢 🔿 🙍 📾 🔛					
Prindows Firewall with Advance Inbound Rules					Actions
Name Name		Group	Profile	~	Inbound Rules
Outbound Rules Oktwork Discov	ery (WSD-In)	Network Discovery	Domai		Mar New Rule
Connection Security Rules	gs and Alerts (DCOM-In)	Performance Logs and Alerts	Domain		
P a Monitoring Performance Lo	gs and Alerts (DCOM-In)	Performance Logs and Alerts	Private		Y Filter by Profile
Performance Lo	gs and Alerts (TCP-In)	Performance Logs and Alerts	Private		
Performance Lo	gs and Alerts (TCP-In)	Performance Logs and Alerts	Domain		▼ Filter by Group
🖉 Remote Deskto	p - Shadow (TCP-In)	Remote Desktop	All		View
🔮 Remote Deskto	p - User Mode (TCP-In)	Remote Desktop	All		
🖉 Remote Deskto	p - User Mode (UDP-In)	Remote Desktop	All		Q Refresh
Remote Event L	og Management (NP-In)	Remote Event Log Manage	All		📑 Export List
Remote Event L	og Management (RPC) og Management (RPC-EP.	Enable Rule	All		P Help
Remote Event N	Aonitor (RPC)	Cut	All		Remote Event Log Management (RPC)
Remote Event N	Nonitor (RPC-EPMAP)	Conv	All		G Enable Rule
🚳 Remote Schedu	led Tasks Management (Delete /	All		K Ca
Remote Schedu	led Tasks Management (/	All		a Cut
🖉 Remote Service	Management (NP-In)	Properties ent	All		Copy
🖉 Remote Service	Management (RPC)	Help ent	All		🔀 Delete
Remote Service	Management (RPC-EPM	Kemote Service Management	All		Properties
Inbound Rule fo	or Remote Shutdown (RP	Remote Shutdown	All		
Minbound Rule fo	or Remote Shutdown (TC	Remote Shutdown	All		и нер
Remote Volume	e Management - Virtual D	Remote Volume Manageme	All		
Remote Volume	Management - Virtual D	Remote Volume Manageme	All	_	
Remote Volume	Management (RPC-EPM	Remote Volume Manageme	All	=	
W Routing and Re	mote Access (GRE-In)	Routing and Remote Access	All		
W Routing and Re	mote Access (L2TP-In)	Routing and Remote Access	All		
WRouting and Re	mote Access (PPTP-In)	Kouting and Remote Access	All		
Secure Socket T	unneiing Protocol (SSTP	Secure Socket Tunneling Pr	All		
World Wide We	b Services (HTTPS Traffic	Secure world Wide Web Ser	All		
In the second seco		ShareDoint			
SharePoint Cen	tral Administration v4	SharePoint	Δ11		
SharePoint Sear	ch	SharePoint	All	_	
				×	
Displays Help for the surrent colection			1		
Displays meip for the current selection.					

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 Configuration V	ersion:				×	8MAN scans access rights
	Server Status License Information		Jobs Summary	Colle	rctors uration	structures from different resource
	Logged in users: 2	33 Scans 1 Reports	13 Changes 20 More	1 Connected 1 Configured in Total		The scan results are stored in an
	Licibeu	6 Scheduled 36 Succeeded	0 Executing 25 Failed	All Collectors are Operational		SQL data base. Users can access
	🔾 Filter				12	these results quickly via the 8MAN
						GUI, as they are already located in
						the date base.
	Scans Resource Configurations, Logga, File Server CSV Import	Open Order Open Order Resource Descriptions	User Managemen User Management, Ro Management	nt Data Owner De Organizational Categories, Dat Owners, Resources, Additional Group Wizard Settings	a	
						Events that occur in between scans
	Q.			(are captured by the 8MATES AD
	License License Information, Server Jo	Jobs Overview ob Status, Job Categories	Collectors 8MAN Collectors Overvie	w and Activated Alert Sensors		Logga and FS Logga. 8MATES are
	Status		Configuration			modules that can be added to
						8MAN and require the appropriate
	O°	<u>lılı</u>	Q S			license.
	Change Configuration Common Change Settings, View	Views & Reports	Server GrantMA, Comments, E	mail, BASIC configuration Mail, 8MAN Server, SQL Server,		
	iecnnology-specific Change Configurations	views & Reports	storage of Scans, Server I Check, Server Loggin	Health Configuration Status Ng		Click on "Scans" to configure
Ready					demoadmin @ localhost 🕣 🏄	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:{0CCE9238-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9238-69AE-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"
- <u>Verifying the execution of audit policies</u>

	Run 🗙	Start managing group policies, by opening:
<u>O</u> pen:	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	gpmc.msc
	OK Cancel <u>B</u> rowse	
Window Help	Group Policy Management	Create a new group policy.

File Action View Window Help			- 8	
				Select the OU in which the DC
 Group Policy Management A A Forest: 8man-demo.local A A Commiss 	Domain Controllers Linked Group Policy Objects Group Policy Inhe	ritance Delegation		computer accounts are located. By
⊿ 🙀 8man-demo.local 🛒 Default Domain Policy ▷ 🖬 8MAN	Link Order GPO	Enforced Link Enabled G ain Con No Yes E	PO Status WMI Filter Modified D nabled None 6/25/201 8	"Domain Controllers".
Denain Controllers Default Domain Denain Controllers Default Domain Default Domain	n this domain, and Link it here g GPO g defo /pdate /odeling Wizard tional Unit			Please ensure that the newly created policy is applied/winning to the appropriate DCs (hierarchy and order).
Default Domain Default Domain WMI filter Diffust CPOs Starter GPOs Stres Stres Refresh Group Policy Modeling Decurities	from Here			
Group Policy Results				The order in which
	<	п	>	you set the options affects the effectiveness of the policy. Follow the
Set Group Policy update flags and run Gpupdate on this cor	tainer			order given here!

R



_ 🗆 X Group Policy Management Editor File Action View Help 🔶 🧆 🙍 📰 🗙 🖾 🗟 🖬 8MAN AD Logga [SRV-8MAN.8MAN-DEMO.LOCAL] Policy Policy Setting 🔺 👰 Computer Configuration Not Defined ⊿ 📫 Policies Fonces
 Software Settings
 Windows Settings
 Software Resolution Policy 2 Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy c... Not Defined DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax
 DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax
 DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax Not Defined Not Defined Scripts (Startup/Shutdo ⊿ 🚡 Security Settings Account Policies
 Account Policies
 Account Policies
 Account Policies
 Audit Policy
 Audit Policy
 Security Options Devices: Allow undock without hat Audit: Force audit policy subcategory settings (Wi... ? × Devices: Prevent users from insta Devices: Restrict CD-ROM access Security Policy Setting Explain Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Devices: Restrict floppy access to Domain controller: Allow server vent Log Event Log
Restricted Groups Domain controller: LDAP server si Domain controller: Refuse machin Define this policy setting System Services Enabled > a system services > Registry > Registry > Registry > III System > III Wired Network (IEEE 802.3) Policies Domain member: Digitally encry Disabled Domain member: Digitally encry Domain member: Digitally sign s Windows Firewall with Advanced Security
 Network List Manager Policies 🗟 Domain member: Disable mach 🗿 Domain member: Maximum m Network List Manager Policies
 Wireless Network (IEE 802.11) Policies
 Public Key Policies
 Software Restriction Policies
 Network Access Protection
 Application Control Policies
 Software Software Policies on Active Directory (SMA
 Associated with Policie Conferentiation Control Policies 🖏 Domain member: Require strong 🖏 Interactive logon: Display user in 🔄 Interactive logon: Do not display Interactive logon: Do not require
 Interactive logon: Do not require
 Interactive logon: Machine accou
 Interactive logon: Machine inacti Advanced Audit Policy Configuration Interactive logon: Message text fo Administrative Templates: Policy definitions (ADMX Interactive logon: Message tele lo Interactive logon: Number of prev Preferences
 User Configuration
 Policies
 Preferences linteractive logon: Prompt user to Interactive logon: Require Dom Interactive logon: Require smart Interactive logon: Smart card ren OK Cancel Apply Microsoft network client: Digitall Microsoft network client: Digitally sign communication ons or server agrees

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!

 Image: SMAN AD Logga [SKV-BMAN.8MAN-DEMO.LOCAL] Policy

 Image: Software Settings

 Image: Software Settings

 Image: Windows Settings

 Image: Windows Settings

 Image: Software Sof

Scripts (Startup/Shutdown)

A Registry
 Mired Network (IEEE 802.3) Policies
 Windows Firewall with Advanced Security
 Network List Manager Policies
 Wireles Network (IEEE 802.1) Policies
 Dublic Key Policies

Action Control Policies
 Security Policies on Active Directory (8M
 Advanced Audit Policy Configuration
 Align Audit Policies

Software Restriction Policies
 Network Access Protection

Account l Account Logon

Detailed Tracki
 DS Access
 DS Access
 Object Access
 Policy Change
 Privilege Use

Invinege use
 System
 Solution
 Solution

Scripts (Startup/Shutd
 Security Settings
 Security Settings
 Local Policies
 Local Policies
 Event Log
 Restricted Groups
 System Services

Registry

File Action View Help

🔶 🧼 🙇 📰 🗟 🖬

1. Navigate to account management.

_ 🗆 X

- 2. Use multi-select and select all subcategories.
- 3. Activate the audit by rightclicking and selecting "Properties", as shown in the diagram.



Group Policy Management Editor

Policy

71

Not Configured Not Configured

Not Configured Not Configured Not Configured

Not Configured

Configure the selected events to be audited: Audit all success

Properties for Multiple Ite

OK Cancel Apply

Audit Application Group Management
 Audit Computer Account Management

Audit Distribution Group Management

Audit User Account Management

Audit Other Account Management Events Audit Security Group Management

- 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.

J.	Group Policy Management Ed	itor	_ 🗆 X	1.	Navigate to "Change policy".
File Action View Help					5 51 7
🗢 🔿 🙇 📰 🔒 🛛 🖬				2.	Select the subcategory "Audit
Image: String	Subcateonov Mudit Audit Policy Change Audit Authentication Policy Change Audit Authorization Policy Change Audit MPSSVC Rule-Level Policy Change Audit Other Policy Change Events Policy Change Events	Audit Events Not Configured Not Configured Not Configured Not Configured Not Configured Audit Audit Policy Change Properties Explain Audit Audit Policy Change orfigure the following audit events: Success Follure		2. 3.	Select the subcategory "Audit Audit Policy Chang". 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"
- <u>Verifying the execution of audit policies</u>

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: C	ommand Prompt 📃 🗖 🗙
C:\Windows\system32>auditpol /get /catego access" System audit policy Category/Subcategory Policy Change Authentication Policy Change	ry:"policy change,account management,ds ∧ Setting No Auditing
Authorization Policy Change MPSSUC Rule-Level Policy Change Filtering Platform Policy Change Other Policy Change Functo	No Auditing ≡ No Auditing No Auditing No Auditing
Audit Policy Change Account Management User Account Management Computer Account Management Security Group Management Distribution Group Management Application Group Management Other Account Management Events DS Access Directory Service Changes	Success Success Success Success Success Success Success Success
Detailed Directory Service Replication Directory Service Access C:\Windows\system32>_	No Auditing No Auditing

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.

	Run 🗙	Start the management of Active Directory users and computers on
Open:	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. dsa.msc v	DC by opening dsa.msc
	OK Cancel <u>B</u> rowse	

а

Activate the option "Advanced Features".

Active Directory Users and Computers							
File Action View	w Help						
🗢 🔿 🖄	Add/Remove	Columns					
Active Direc	Large Icons			Description ^			
Saved Q	Small Icons		izational Unit				
⊳ 🚔 8man-d	List		Domain				
•	Detail		izational Unit				
	Users Contract	Course of Course to constrain of the	iner	Default container for up			
	Users, Contact	s, Groups, and Computers as containers	izational Unit	Default container for do			
\checkmark	Advanced Fea	tures	iner	Default container for se			
	Filter Options.		izational Unit				
	Customize		hdFound	Default container for or			
			iner	Default container for m			
		Microsoft Exchange Security Groups	Organizational Unit	BANK CALL			
		Program Data	Container	Default location for stor			
		Service Accounts	Organizational Unit	B 1947 - 1			
		System	Container	Builtin system settings			
		I lestGroups	Organizational Unit				
		I lestUsers	Organizational Unit	De la ser e			
		Users	Container	Default container for up			
		Vsphere-Roles	Organizational Unit				
		Initrosoft Exchange System Objects	msexenoystemObjectsContal	Queta energifications co			
		TPM Devices	msD3-QuotaContainer	Quota specifications co			
			ms revelation objectsc	▼			
Enables/disables advanced features and objects							



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

8MAN

| 18

	Active Directory Users and Computers	_ 🗆 X
File Action View Help Image: Strain S	8man-demo.local Properties ? X General Managed By Object Security Group or user names: 1	Description
	SELF Authenticated Users SYSTEM AuthORK SERVICE Organization Management (8MAN-DEMO\Organization Manage	Default container for up Default container for do Default container for se
	Add Remove Permissions for Everyone Allow Deny	Default container for or Default container for m =
	Full control Read Write Create all child objects	Default location for stor Builtin system settings
	Delete all child objects Image: Constraint of the second settings, clicities For special permissions or advanced settings, clicities Image: Constraint of the second settings, clicities Advanced Advanced	Default container for up
< 111	OK Cancel Apply Help C	· Quota specifications co

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

		Adva	nced Security Settin	ngs for 8man-demo	
Ow Pe For	ner: rmissions additiona	Administrators (8MAN-DEMO Auditing Effective Ac	(Administrators) <u>Chang</u> cess lit entry. To modify an a	je udit entry, select the ent	ry and click Edit (if available).
	Type Succ Succ Succ Succ Succ	Principal Everyone Domain Users (8MAN-DEMO\ Administrators (8MAN-DEMO Everyone	Access All extended rights All extended rights Special	Inherited from None None None None None	Applies to Special Special This object only This object only This object only
	Add	<u>R</u> emove <u>E</u> dit			Restore defaults OK Cancel

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.



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

License Information	Server Status	
	Uptime: 2 hours Version: 9.0.183.0	
	Logged in users: 1	
	Name Domain Host 8MAN Component tdemoadmin 8MAN-DEMO srv-8man Configuration	
No license available		
Load license		
Technologies		
Features		
Max. Logbook entry age in days		

8	Please	choose a license fi	le			x
📀 💿 🔻 🛉 퉬 « Loc	al Disk (C:) → ProgramData → protected-netwo	rks.com 🕨 8MAN 🕨	licenses	~ ¢	Search licenses	P
Organize 🔻 New folder	r				i 🕶 🖬	0
☆ Favorites	Name	Date modified	Туре	Size		
Desktop	8Man_20161117125549.license	11/17/2016 1:55 PM	LICENSE File	8	KB	
Downloads Recent places						
This PC Desktop Documents Music F Pictures Videos Local Disk (C:) F (E:) V						
File <u>n</u> ar	me: 8Man_20161117125549.license			~	License files (*.license)	¥
					<u>O</u> pen Cancel	

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%protectednetworks.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

8MAN Configuration	Version:			×	On the configuration home page
Back File server CSV	import			0	select "Scans".
 Select a technology below to ad 	d a new resource configuration				
Active Directory Resource	Exchange Exchange Resource	File server File Server Resource	Local Accounts	Monitoring an Active Directory	
Monitoring a File Server	SharePoint ☆ Sharepoint Resource (Farm Based)	VSphere VMware vSphere Resource			Select "Logga - Active Directory".
A film		-		6	
& Paulo				^	
	nan-demo.local			×	
The domain 8man-demo.k	ocal will be scanned <u>daily. 10:00 PM</u> [] (Mo	re »)			
U resources are associa	ated with this domain. Add resource config	uration *			
The file carver SPV-8MAN	<u>N (SRV-8MAN)</u> In the manitored on SPV-:	ΜΔΝ		× ,	
<u></u>					
Ready				demoadmin © localhost 🕣 🌁	
BMAN Configuration	Version:			×	1. Enter valid credentials for the
Back File server CSV	Active Director	/ Logga selection	×		domain that you want to
^ Select a technology below to ad	d a new resource Please select a re	ource. You can change the crede	ntials and refresh the		
Active Directory Resource	list when the give	n credentials are insufficient to fi	nd all resources.	Logga - Active Directory Monitoring an Active Directory	monitor.
Logga - File Server Monitoring a File Server	Share Cal 2 A Filter or type IP o	r Name	1 🛞		2. Use the filters to find the desired
		Name			domains.
A Filter	3 Sman-demo.loc	3		6	2. Calculation de maine Childrede maine
	nan-demo.local			×	3. Select a domain. Chila domains
The domain 8man-demo.k	ocal will be scanne				are not monitored. Every
0 resources are associa	ated with this dom Assigned colle	ctors			domain must be configured
OFF SRV-8MAN	V (SRV-8MAN)		•	×	senarately
The file server SRV-8MAN of Refresh data all <u>10 minutes</u>	of type Windows w Monitored actions		0		Separatery.
+ 3 reports are configured.	Add: Who did wha	Apply	Discard		4. Select a collector server. You can
					only select one collector per
Ready				demoadmin © localhost 🕣 🔛	domain
					a o mann.

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

You must <u>activate the AD Logga</u> to record events.

3.1.4 Activate/deactivate AD Logga

Configuration V	ersion:			-	
Back File server CSV im	iport				
 Select a technology below to add 	a new resource configuration				
Active Directory Resource	Exchange Exchange Resource	File server File Server Resource	Local Accounts	Logga - Active Directory Monitoring an Active Directory	
Monitoring a File Server	SharePoint ☆ Sharepoint Resource (Farm Based)	VSphere VMware vSphere Resource			
\sim	\sim				
A Filter				1	7
	, pe <u>nere</u> nin de seannes <u>sang, recern</u> en				^
The domain 8man-demo.loca	.local Il is monitored on SRV-8MAN using accou	unt <u>8man-demo\sa-8man</u> .		×	
Refresh data all 4 10 Minu	ites.				Î.
				demonstrate (Albert	1 mar 1

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.

_	Υοι	u m	nust	ente	er a	COI	nm	ent	

Follow the same steps for deactivation.

8MAN Configuration Version:			×	Vou must a
Back Bit server CSV import Select a technology below to add a new resource confi	iguration		0	Tou must e
Domain Active Directory Resource	Start logging	Local Accounts	er Logga - Active Directory	Follow the
A faiter Correction of the Server Correction of the Server	Please confirm the Start of the Active Directory Logga with a comment. The start event will be loaned in the <u>SMAN loabook</u> .	Apply Cancel	T A	deactivatio
leady			demoadmin @ localhost 🕣 🔤	

3.1.5 Modify the AD Logga configuration

On the configuration home page select "Scans".

8MAN Configuration	/ersion:			-		×
Back File server CSV in	nport					?
 Select a technology below to add 	a new resource configuration					
Active Directory Resource	Exchange Exchange Resource	File server File Server Resource	Local Accounts	Logga - Active Directory Monitoring an Active Directo	y	
Monitoring a File Server	SharePoint	VSphere VMware vSphere Resource				
		-				
A Filter					7	
	, e	and Carole and			^	
					~	
OFF Bman-demo	<u>b.local</u>				^	\sim
The domain 8man-demo.loc	al is monitored on SRV-8MAN using accou	in 8man-demo\sa-8man. 2				
Following filters have been s	et. Logging is <u>disabled</u> .				1	
Refresh data all 10 Minutes.						
Ready				demoadmin @ lo	calhost 🗧	- ~~
Ready				demoadmin @ lo	calhost €	- <u>*</u>

- 1. Give the configuration a different name.
- 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.

on the link "Following filters".

3.1.5.1.2 Configure event filters

8MAN Configuration V	ersion:			-	o x
Back File server CSV im	zort				0
 Select a technology below to add 	a new resource configuration				
Active Directory Resource	Exchange Exchange Resource	File server File Server Resource	Local Accounts	Logga - Active Directory Monitoring an Active Directory	
Logga - File Server Monitoring a File Server	SharePoint ☆ Sharepoint Resource (Farm Based)	VSphere VMware vSphere Resource			
\sim \sim	\sim				
A Filter					7
	pe <u></u>	In (more ")			^
				×	(
Comparing the second seco					



- 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".

8MAN



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 "timebased" option can be set anywhere between 10 and 1440 min (24h). The shorter the interval, the higher the load on your AD.

Logga - File Server	Active Directory Logga			🗙 🖪 Active Directory
Monitoring a File Server	Set filter criterias to limit	the amount of data collected by the Active Direct	tory Logga.	
A Eilter		Available event authors	Filtered out Computer event authors	7
		4 Filter 3	4 Filter	× ^
The file sequer SI	Active Directory Events	Computers		
Refresh data all '	+++++	Name	►	
+ 3 reports are	User event authors	SRV-EXCHANGE (8man-demo\SRV-EXCHANGE\$)		
	111111	SRV-SHAREPOINT (8man-demo\SRV-SHAREPOINT\$)		
	Group event authors			×
The SharePoint				
	Computer event authors			
				\times
X	Object classes			
The Exchange S	Y 2			
				\times
	Attributes			
The Exchange 8	++++			
-	Logga monitoring	The events of all Computer accounts will be filtered	ed out.	
				\times
71 61	Please add a comment		Apply	
The file server s			YAK MARKA	
The file server <u>s</u>				
The file server s			Cancel	×

Filter events for selected or all computer accounts.

8MAN

Active Directory Logga Filter Configuration

+++++

User event authors

roup event autho

er event authors

......

Y 2

Attributes

Set filter criterias to limit the amount of data collected by the Active Directory Logga
Object classes selection
Filtered c

account (account) ACS-Policy (aCSPolicy) ACS-Resource-Limits (aCSReso ACS-Subnet (aCSSubnet) Address-Book-Container (addr

A Filter

lass-Store (cl

ter)

Filtered out Ol

Active Directory

Cancel

BMAN Configuration

OFF.

The file server Refresh data a + 3 reports a

OFF

- 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".

BMAN
Configuration

Select a technology below to all

Select a technology below to all

Delete resource configurations?

Select a technology below to all

Delete resource configurations?

Select a technology below to all

Delete resource configurations?

Select a technology below to all

Delete resource configurations?

Select a technology below to all

Delete resource configurations?

Select a technology below to all

Delete resource configurations?

Name

Information

Image: Active Bine delete store

Image: Configuration delete store

Image: Configuration

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

BMAN Configuration V	/ersion:				_ 0	× Click "Serve
						related to c
	Server Status License Information		Jobs Summary	Colle	ectors juration	storage be
	Logged in users: 1	4 Scans	5 Changes	1 Connected 1 Discon	nected	storuge, ne
	Licensed	4 Scheduled	0 Executing 0 Failed	Some collectors are currently not		logs.
			orunca	operational		
	🖏 Filter				12	
						
	Scare			nt Data Owner		
	Resource Configurations, C Logga, File Server CSV Import	Open Order Resource Descriptions	User Management, R Management	ole Organizational Categories, Da Owners, Resources, Additiona Group Wizard Settings	ta al	
	0		-			
	License License Information, Server Job Status	Jobs Overview Status, Job Categories	Collectors 8MAN Collectors Overvi Configuration	Alerts Configuration aw and Activated Alert Sensors		
				_		
	Q	<u>htt</u>	O ₀			
	Change Configuration Common Change Settings, View Technology-specific Change Configurations	/iews & Reports vs & Reports, Blacklist for Views & Reports	Server GrantMA, Comments, I Storage of Scans, Server Check, Server Loggi	imail, Health Configuration Status		
						\sum
Ready					demoadmin @ localhost 🗲	1 24
,						

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 Configuration Version:	8MAI
Back	comn
Comments	inforr
▲ 90 ≥ ∞ Number of days for which comment indicators will be displayed on accounts and resources. ▲ Note: This setting does only affect the icons displayed on accounts and resources. You can always access the full logbook through the context menu.	The lo
✓ Email	more
✓ Storage of scans	roduc
V Server Health Check	Teuuc
✓ Server logging	notes
	many
Reedy demoedmin @ localhost 🔄 🚆	í.

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

BMAN Configuration Version:	The "Sto
Back	confiqu
* Comments	determ
r ← Email	, ueternin
* Storage of scans	Logga d
C Enable the creation of a Scan Archive to store and open old scans, which were deleted from the database.	the size
The 8MAN Server stores the Scan Archive under the path <u>CuProgramDatalprotected-networks.com/8MAN/datalacanArchive</u>	roquiro
In case of a low disk space condition remove oldest scans	required
☑ Inable automatic scan deletion.	
Rep daily Active Directory scans for the last 40 P day(s).	Dianaa
•• 📜 Keep older monthly scans for 💶 🗩 month(s).	Please r
Except daily scans for the last 1 21 a day(s).	Express
A keep older monthly scans for < 3 month().	
Recorded AD Logga events will be deleted, when they are older than (30) day(s).	
Recorded FS Logga events will be deleted, when they are older than (30) day(s).	
✓ Server Health Check	
✓ Server logging	
Resdy demosdmin @ localhost 🖯 🎽	

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.

▼ GrantMA	
* Comments	
▼ Email	
 Storage of Scans 	
☑ Enable the creation of a Scan Archive to store and open old scans, which were deleted from the database. The BMAN Server stores the Scan Archive under the path <u>CUProgram Data protected - networks com/UMAN/data/Scan&rchive</u>	
In case of a low disk space condition slop archiving	
☑ Enable automatic scan deletion.	
Rep daily Active Directory scars for the last € 100 p day(s). Image: Rep alder monthly scars for € 60 p month(s).	
Image: Seep daily scans for the last II 21 pt day(s). Image: Image: Seep date monthly scans for Image: Image Topology and the second scans for Image Topology.	
Recorded AD Logga events will be deleted, when they are older than (\$ 999.) day(s).	
Recorded Exchange Logga events will be deleted, when they are older than (1999) day(s).	
✓ Server Health Check	
 Server Logging 	

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

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

35

Monitoring of event authors

- Groups
- Computers

• Users

Step by step process





- 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.

8MAN

Access Rights Management. Only much Smarter.

36



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

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



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

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

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

8MAN Version: 7.6.131. **⊘** Se AD Logga Report Report configuration AD Logga Report Report of monitored Active Directory events Per Event Type • ^ 1 Template available 🗳 Filter Event Author -----N Created on Author 2/15/2017 11:55 AM 8MAN-DEMO\c . Name ers Created Please select one or more user. To search for events of all users leave this field e Newl Use Object Class . Attribute — Save template
Name
Name
Description
Description Sec 🛛 🔚 Overwrite Settings The output format is <u>XLS</u> * Create report <u>for all accounts in one</u> docu Report execution mode <u>started manually</u> Store on specific path is <u>Deactivated</u> Send email is <u>Deactivated</u> 💿 🔼 New 8man-demo.local 🕤 🐼 📑 🥥 <Latest scan> 🛸



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".



- 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 elses account ends with a locked user account. The AD Logga shows you from which computer the attack occurred.

Additional services

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

Step by step process



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





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



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





- 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.

⊟ 5-					AD Log	ga Report_8M	IAN-DEMO_cradmin_20161110133143						
Datei S	Start Einfügen	Seitenlayout	Formeln	Daten	Überprüfen		♀ Was möchten Sie tun?				õrg Branc	lt 🗛 Freigel	ben
A389	• : × ·	√ f _x											
4	A		в				С		D	E		F	
1 Zeit	Autor				Ol	jekt			Objektklasse	Ereignis		Attribut Name	e A
26.02	2014 16:56 cradm	nin (8man-demo\cr	admin)		Bi	no, Al (8man	-demo\Al.Bino)		User(user)	Kennwort zurück	setzen		
28.02.201	14 15:40:35 cradm	nin (8man-demo\cr	admin)		Zif	er, Lou (8ma	n-demo\Lou.Zifer)		User(user)	Kennwort zurück	setzen		
11.03.201	14 09:15:01 Admir	nistrator (8man-dei	mo\Adminis	trator)	Zif	er, Lou (8ma	n-demo\Lou.Zifer)		User(user)	Kennwort zurück	setzen		
13.03.201	14 14:50:42 Admir	nistrator (8man-dei	mo\Adminis	trator)	Zif	er, Lou (8ma	n-demo\Lou.Zifer)		User(user)	Kennwort zurück	setzen		
10.03.201	15 11:49:04 neadr	nin (8man-demo\n	eadmin)		Bo	rg, Inge (8m	an-demo\lnge.Borg)		User(user)	Kennwort zurück	setzen		
10.03.201	15 12:31:32 neadr	nin (8man-demo\n	eadmin)		Bo	rg, Inge (8m	an-demo\lnge.Borg)		User(user)	Kennwort zurück	setzen		
10.03.201	15 15:12:28 Admir	nistrator (8man-der	mo\Adminis	trator)	Kr	se, Christian	e (8man-demo\Christiane.Krise)		User(user)	Kennwort zurück	setzen		
10.03.201	15 15:47:05 Admir	nistrator (8man-dei	mo\Adminis	trator)	Ar	der, Ole (8m	an-demo\Ole Ander)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		At	er, Mark (8n	nan-demo\Mark Aber)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Al	en, Arnold (I	man-demo\Arnold Alien)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		AJ	be, Vera (8m	an-demo\Vera Aloe)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ar	der. Ole (8m	an-demo\Ole Ander)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ar	der. Cori (8r	nan-demo\Cori Ander)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ar	er. Dominik	(8man-demo\Dominik Aner)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ar	gebrandt, A	ngie (8man-demo\Angie Angebrand	it)	User(user)	Kennwort zurück	setzen		
10 03 201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ar	fel Adam (8	man-demo\Adam Apfel)	/	User(user)	Kennwort zurück	setzen		
10 03 201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ar	beit. Andi (8	man-demo\Andi Arbeit)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ar	m. Armin (8r	nan-demo\Armin Arm)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ar	oni. Mark (8r	nan-demo\Mark Aroni)		User(user)	Kennwort zurück	setzen		
10 03 201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		As	il Claire (8n	an-demo\Claire Asil)		User(user)	Kennwort zurück	setzen		
10 03 201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		A	er Karl (8m	an-demo\Karl Auer)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Δι	hes Ann (8	man-demo\Ann Auhss)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		A	tsch Anke	8man-demo\Anke Autsch)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Az	ubi Andy (8	man-demo\Andy Azubi)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ba	ha Ali (8ma	n-demo\Ali Baha)		Llear(user)	Kennwort zurlick	cetzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ba	ch Klara (8	man-demo/klara Bach)		User(user)	Kennwort zurück	cetzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ba	er Johanne	(8man-demo) Johannes Baer)		User(user)	Kennwort zurück	cetzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Ba	er Roy (8m	an-demo/Roy Baer)		User(user)	Kennwort zurück	cotzon		
10.03.201	15 16:50:09 neadr	nin (8man.demo\n	eadmin)		Ba	ern Al (8ms	n-demo\Al Baern)		User(user)	Kennwort zurück	cotzon		
10.03.201	15 16:50:00 neadr	nin (8man-demo\n	eadmin)		B	Ikan Don P	(8man.demo\Don P. Balken)		Llear(user)	Konnwort zurück	eetzen		
10.03.201	15 16:50:09 needs	nin (8man-demo\n	eadmin)		Ba	cher Joe Ki	it (8man-demo\loe Kurt Becher)		User(user)	Kennwort zurück	setzen		
10.03.201	15 16:50:09 neadr	nin (8man-demo\n	eadmin)		Be	iter, Walter	8man-demo\Walter Beiter)		User(user)	Kennwort zurück	setzen		
	Konfiguratio	n Ereignisse	Filter Ko	onfiguration				÷ •					Þ
ereit										田 田 - -	- 1	+ 10	00 %

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

Version:					×
8M	AN		🛛 Suche	*	
🔒 Start	& Ressourcen	🖻 Berechtigungen	🖧 Accounts	© Dashboard ☑ Mehrfachauswahl 邱 Logbuch	Scanvergleich
Logbuch	2 Von 6 Monate	zuvor bis Heute	¢.	reitag, 7. Oktober 2016	Report -
				A Filter	42
<u> </u>	4 0 0 0 0 0 0			× Alle Kommentare anzeigen	
	it ietzt diert	ngen			
	esarr ert errt geån	eänd atior feldu träge		Zeit Autor Autor Autor	Kommentar
	en g iert ande ände vtsp	elit telit igur igur			
	ung aktiv ort z ort z er el er el	erst tiguu Konl Konl hute hute		M 13:31 cradmin (8man-demo) cradmin)	
	nder nnw nutz nutz	nto rech gga ggele nstig			
63	Z AL	S B B B B B		M 13:30 cradmin (8man-demo\cradmin)	
	3 1 16 1 16 2 5	a 🕰 🖉 86 86 🔁 🙂		M 13:30 cradmin (8man-demo\cradmin)	
Mo 05.12.2016	2	2		🗞 💋 13:12 Administrator (8man-demo\Administrator)	
Fr 02.12.2016	4	4		13:12 cradmin Der brauch admin rechte, damit e	r sich während des clean! migrationspro
Do 01.12.2016	4	4		13:04 AD Logga SRV-8MAN	
Mi 30.11.2016	3	3		13:03 AD Logga SRV-8MAN	
Di 29.11.2016	3 1	1 2		NG 12:58 AD Logga SRV-8MAN	
Mi 23.11.2016	20	6 14		🛐 💋 12:56 NT-AUTORITÄT\SYSTEM	
Di 22.11.2016	6	2 4		🛐 💋 12:56 NT-AUTORITÄT\SYSTEM	
Mo 21.11.2016	4	4	>	b 🔊 12:42 cradmin (8man-demo\cradmin)	
Sa 19.11.2016	6	6		🚯 🔊 12:40 cradmin (8man-demo\cradmin)	
Fr 18.11.2016	10	10		b 😥 12:40 cradmin (8man-demo\cradmin)	
Mo 14.11.2016	8 4	4		🎭 😥 12:40 cradmin (8man-demo\cradmin)	
Di 11.10.2016	16	14 13		Se 🕼 12:40 cradmin (8man-demo\cradmin)	
Mo 10.10.2016	4 22	12		Il 12:40 cradmin (8man-demo\cradmin)	
Fr 07.10.2016	42 3 1 6 1 13 3	3 11 3 1		IV 12:40 cradmin (8man-demo\cradmin)	
Do 06.10.2016	8	8			Ű
Mi 05.10.2016	10 2 3	1 1 3			>
Mi 28.09.2016	7 5	2		Attribut geändert	
Mi 03.08.2016	12 4 2	1 5		N leases für Smae demo least	
Mi 27.07.2016	2	2		to bogga for ornan-demolocal	
Di 26.07.2016	3 2	1		Anderung durch cradmin (8man-demo\cradmin):	
				insershaftswart 'mrDS-SupportedEesenstionTunes' hai Class - Admin (Rman-demo) Class - /	(dmin) considert in '0'
				agenschenswert insolo-supported charyprion ypes bei <u>clean - Admin (oman-demo/clean - A</u>	demonstration of the second se
			I		
Bereit				8MAN-DEMO.LOCAL 🛩 🔿 📑	🖉 <neuester scan=""> 👻 🚺 🌁</neuester>

- 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.

Vei										
	8M/	٩N			6	Suche			\$	
									wahl 🕮 Logbuc	h 🛛 Scanvergleich
Lo	ogbuch	Von <u>6 N</u>	Aonate zu	vor bis <u>Heu</u>	te	٥	Freitag, 7. Oktober a	2016		Report 👻
		4					🗳 Filter			13 von 42
		ti l	t	# 5			× Alle Kommentare an	zeigen		
		geset	t ginde	inder tion Idung	jġe		③ Zeit▼	Autor		Kommentar
		n ges ert urück inder	tsper aft ge	elit g gel gural s-Me	Antri		administ 🔊 🔊 🖓	rator (8man-demo\Administrat	or)	
		unge ort zu t geä	dsch erste	tigun Konfi Statu	hnte		13:12 cradmin	(Penan dama) cradmin)	Der brauch admin rechte, d	lamit er sich während des clean! migrationsproze
		nder nnwn tribu	itgle into	uppe 99a 99a	ogele	6	2:42 cradmin	(8man-demo\cradmin)		
	63	AJ A	8 8 8 8 19 8 8 8	5 8 9 9 5 8 8 8	S So	2	🇞 🔊 12:40 cradmin	(8man-demo\cradmin)		
Mo	05 12 2016	2		2			춼 🔊 12:40 cradmin	(8man-demo\cradmin)		
Fr	02.12.2016	4		4			🎒 🔊 12:40 cradmin	(8man-demo\cradmin)		
Do	01.12.2016	4		4			S (12:40 cradmin)	(8man-demo\cradmin)		
Mi	30.11.2016	3		3			> 12:40 cradmin	(8man-demo\cradmin)		
Di	29.11.2016	3	1	2			8 M 12:40 cradmin	(8man-demo\cradmin)		
Mi	23.11.2016	20		6 14			b 🔊 12:40 cradmin	(8man-demo\cradmin)		
Di	22.11.2016	6		2 4			b 🔊 12:40 cradmin	(8man-demo\cradmin)		
Mo	21.11.2016	4		4		×				
Sa	18 11 2016	10		5			<			, ,
Mo	14.11.2016	8 4		4			A Gruppenmitaliedecha	ft geändert	v	
Di	11.10.2016	43 16	-	14	13	6	AD Logga für Sman-demo	local		
Mo	10.10.2016	34 22	L	12			Ab cogga for onian-denio	local		
Fr	07.10.2016	42 3 1 6	1 13 3	11 3	1		Änderung durch Administ	ator (8man-demo\Administrati	or):	
Do	06.10.2016	8	-	8			Gruppenmitglied 'Clean - /	Admin (8man-demo\Clean - Ad	Imin)' in 'Domänen-Admins' hir	nzugefügt.
Mi	05.10.2016	10 2	3	1 1 3						
Mi	28.09.2016	7 5		2						
Mi	27.07.2016	2	2	1 5		_				
Di	26.07.2016	3 2		1						
							Rereich ein- hzw. ausklappe	D		
							ocrean an ozw. auskiappe			
			_					_		-
Bei	eit							8M	AN-DEMO.LOCAL -	🖶 🖉 <neuester scan=""> 👻 🛈 🏄</neuester>
	-									

- 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.

8MAN Ver						
		♀ Searcl	h			🚔 cradmin
	Overview of the Logbook					X
+ +	Comments for: C-Level (8man-d	emo\C-Lev	vel)			
	4 Filter	39	Sroup membership changed			
	() Only mine		cradmin: ddd			
	🔊 Date & Time 🔻 🗛	uthor	8MAN Changes:			
B	11/11/2014 6:31 PM cradmin 11/11/2014	^	Member (Cook (Chris Cook) added to group C-Level (scheduled)			
8MAN complete (8n	11/7/2014 3:38 PM cradmin		member <u>cease (emp cook)</u> added to group <u>c cerer</u> (circulated)			an demo\VPN)
compi	11/5/2014 5:48 PM cradmin		Used credential: 8man-demo\sa-8mansvc			
7	10/30/2014 10:53 AM cradmin					7 12
	10/29/2014 2:42 PM cradmin					
	10/29/2014 2:23 PM cradmin					
	10/29/2014 11:36 AM cradmin					
	\$10/29/2014 9:55 AM cradmin					
	10/28/2014 1:39 PM cradmin					
	7/23/2014 10:47 AM cradmin					
	5/28/2013 8:06 AM 8MAN-DEM	0\adminis				
2	5/28/2013 8:06 AM administrate	or				
	5/24/2013 12:32 PM 8MAN-DEM	U\adminis				
	5/24/2013 12:32 PM administrate	or o				
	4/25/2013 2:27 PM 8MAIN-DEM 4/25/2013 2:27 PM	U\sa-amai				
	4/25/2013 2:27 PM administration 4/24/2012 5:22 PM PMAN DEM	Chen Repair				
	4/24/2013 5:33 PM 0MAIN-DEM 4/24/2012 5:23 PM administration 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	U\sa-omai				
	2/12/2012 0:55 AM 2MAN DEM	Olica Repair				
	3/12/2013 9:55 AM administrate	v (sa+oinai				
	w 5/12/2010 5/55 / W 4411113/44	. v				
	<	>				
ă	Please add a comment					
				24	Plud	
					Cancel	
		_				
				10101008		
				8man-demo.loc	al 🗠 🗘 🛃	🕗 <latest scan=""> 🝸 🕕</latest>

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.

8MAN

Access Rights Management. Only much Smarter.

| 48

6 Configure alerts

BMAN Configuration Ve	ersion:				×	In the "Alerts" category, activate
						and deactivate the alert sensors.
	Server Status License Information		Jobs Summary	Colle	ration	With active alort concorr, you can
	Logged in users: 2	48 Scans	22 Changes 32 More	1 Connected 1 Configured in Total		with active alert sensors, you can
	Licensed	4 Scheduled	0 Executing	All Collectors are Operational		create alerts for <u>groups</u> or <u>user</u>
		59 Succeeded	40 Failed			<u>accounts</u> .
	🛿 Filter				12	Manage alerts in the 8MAN user
				—		interface.
	Scans Resource Configurations, C Longa, File Server CSV Import	Open Order Open Order Resource	User Manageme User Management, R Management	ent Data Owner Role Organizational Categories, Data Owners Resources Additional	1	
	Logge, the better cost import	Descriptions	management	Group Wizard Settings		You need a <u>license</u> for the 8MATE
			_		1	AD Logga or FS Logga.
	Q, _			l 🌔		
	License License Information, Server Job	Jobs Overview Status, Job Categories	Collectors 8MAN Collectors Overvi	ew and Activated Alert Sensors		
	Status		Configuration			
	Qo	111	⊂ ¢°			
	Change Configuration N Common Change Settings, View	/iews & Reports is & Reports, Blacklist for	Server GrantMA, Comments, B	Basic configuration Email, BMAN Server, SQL Server,		
	Technology-specific Change Configurations	Views & Reports	Storage of Scans, Server Check, Server Loggi	Health Configuration Status		
Ready					demoadmin © localhost 🕣 🎂	

© 2018 Protected Networks GmbH

8MAN

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.



Configure alerts

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



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



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

Configure alerts

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



- 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.





- 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.



- Manage Alerts Manage alert definitions system-wide. 🗳 Fi ሪ State Name . Resource Event Threshold Action "C-Level" Gruppe demo\C-Level) mitgliedschaften geändert (8man-Send email Write to Windows event log A Group memberships changed C-Level (8man-demo\C-Level) Send email Execute script \bigcirc "Domänen-Admins" Gruppenmitgliedsch. geändert Domänen-Admins (8man-demo\Domänen-Admins) 💩 Group memberships changed Changes in directory Send email Berechtigungsänderungen am Verzeichnis für Vertrieb \\srv-8man\Vertrieb Send email Write to Windows event log Krise, Christiane (8man-d...\Christiane.Krise) A Password reset Kennwort zurückgesetzt für Krise, Christiane Konto gesperrt für Krise, Christiane (8man-demo \Christiane.Krise) Send email Write to Windows event log Krise, Christiane (8man-d...\Christiane.Krise) Account locked 1000x / 20s Send email Execute script Changes in file server Mögliche Virusattacke auf dem File Möglicher Datendi srv-8man Activ Changes in file server 5000x / 5m Send email Close
- 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 nonpublic 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, <u>https://json.codeplex.com/license</u>
- JSON.NET Copyright (c) 2007 James Newton-King <u>https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md</u>
- Irony Copyright (c) 2011 Roman Ivantsov http://irony.codeplex.com/license
- Jint Copyright (c) 2011 Sebastien Ros http://jint.codeplex.com/license
- #ziplib 0.85.5.452, © 2001-2012 IC#Code, http://www.icsharpcode.net/opensource/sharpziplib/
- PDFsharp 1.33.2882.0, © 2005-2012 empira Software GmbH, Troisdorf (Germany), <u>http://www.pdfsharp.net/PDFsharp_License.ashx</u>
- JetBrains Annotations, © 2007-2012 JetBrains, 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, <u>https://communities.netapp.com/docs/DOC-1152</u> (Usage only for FS Logga for NetApp Fileserver)
- WPF Shell Integration Library 3.0.50506.1, © 2008 Microsoft Corporation , <u>http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx</u>
- WPF Toolkit Library 3.5.50211.1, © Microsoft 2006-2013, http://wpf.codeplex.com/license
- Bootstrap, © 2011-2016 Twitter, Inc, https://github.com/twbs/bootstrap/blob/master/LICENSE
- jQuery, © 2016 The jQuery Foundation, <u>https://jquery.org/license</u>
- jquery.cookie, © 2014 Klaus Hartl, <u>https://github.com/carhartl/jquery-cookie/blob/master/MIT-LICENSE.txt</u>
- jquery-tablesort, © 2013 Kyle Fox, https://github.com/kylefox/jquery-tablesort/blob/master/LICENSE
- LoadingDots, © 2011 John Nelson, <u>http://johncoder.com</u>
- easyModal.js, © 2012 Flavius Matis, <u>https://github.com/flaviusmatis/easyModal.js/blob/master/LICENSE.txt</u>
- jsTimezoneDetect, © 2012 Jon Nylander <u>https://bitbucket.org/pellepim/jstimezonedetect/src/f9e3e30e1e1f53dd27cd0f73eb51a7e7caf7b378/LICENCE.txt?</u> <u>at=defaultjquery-tablesort</u>
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC <u>https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE</u>
- Mustache.js, © 2009 Chris Wanstrath (Ruby), © 2010-2014 Jan Lehnardt (JavaScript) and © 2010-2015 The mustache.js community 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 <u>https://github.com/jashkenas/underscore/blob/master/LICENSE</u>
- 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 <u>https://github.com/select2/select2/blob/master/LICENSE.md</u>
- bootstrap-datepicker, © Copyright 2013 eternicode <u>https://github.com/eternicode/bootstrap-datepicker/blob/master/LICENSE</u>
- RabbitMQ, © Copyright 2007-2013 GoPivotal, <u>https://www.rabbitmq.com/mpl.html</u>
- EPPlus, JanKallman, https://github.com/JanKallman/EPPlus/blob/master/LICENSE

| 59

8MAN