

Access Rights Management. Only much Smarter.

Access Rights Management Exchange Logga Manual

Version 9

© 2018 Protected Networks GmbH



1	8MATE Exchange Logga 3
2	System requirements
2.1	The 8MAN architecture 4
2.2	Exchange requirements
	2.2.1 Prepare the PowerShell website
	2.2.2 Enable Exchange Server auditing
2.3	8MAN service account permissions
3	Load the license file and check covered features11
4	Configure the Exchange Logga13
4.1	Add an Exchange Logga configuration
4.2	Customize an Exchange Logga configuration 14
4.3	Select the mailboxes to be monitored 15
4.4	Filter the Exchange Logga events
	4.4.1 Understand the filter principles
	4.4.2 Configure the event filters
4.5	Enable/disable the Exchange Logga 20
5	Evaluate the Exchange Logga data 21
5.1	Monitor activities on mailboxes, calendars, and contacts (report) 21
5.2	View activities in mailboxes, calendars, and contacts (logbook) 23
Keyw	ords 25

1 8MATE Exchange Logga

Background / Value

Microsoft Exchange is used for the central filing and administration of e-mails, appointments, contacts and tasks. As a central solution for enterprise-wide collaboration, not only the question of access rights is relevant, but also a monitoring of the actual activities carried out.

The 8MATE Exchange Logga logs activities of mailbox owners, their delegates and administrators.

Particularly safety-critical are the following actions:

- Hard Delete: Who deleted emails, contacts or calendar entries from the Exchange Server?
- MessageBind: Did an employee from IT look into my emails?
- SendAs: Who sent an email in my name??
- SendOnBehalf: Who sent emails on my behalf?
- SoftDelete: Who (except me) deleted emails in my mailbox?

Services

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

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 Exchange requirements

The 8MATE Exchange Logga supports the following Exchange versions:

- Exchange Server (on-premise) 2013, 2016
- Exchange Online

For the on-premise variants, the servers holding the mailbox databases must primarily use the en-US language. Installing language packs may require a reboot. For more information, visit <u>Microsoft</u>.

8MATE for Exchange is not mandatory - the Exchange Logga can be used independently.

2.2.1 Prepare the PowerShell website

The steps described in this chapter are not required for Exchange Online.

The Exchange Client Access Server (CAS) hosts a site within the IIS, that allows users to access the Exchange Server. It is called "Default Web Site" (2010) or "Exchange Back End" (2013 and higher) and includes the sub-site "PowerShell". This must be configured to allow 8MATE Exchange access.



Start the IIS Manager on the CAS.



Navigate to "Powershell". In Exchange 2010 this can be found under "Default Web Site". In Exchange 2013 it is found under "Exchange Back End". Double-click "Application Settings".

- Control C
 - 1. Select "PS LanguageMode"
 - 2. Click "Edit"
 - 3. Enter the value "FullLanguage".

¥3		Internet Ir	nformation Services (IIS) Manager		
€ O P + TE-8MAN-EXCH + Sites + Exch	nange Back End 🔸 PowerShell 🕨			🗑 🖂 🟠 🔞 -	•
Eile <u>V</u> iew <u>H</u> elp					1
Connections	Auth anti-ation			Actions	
🔍 - 🔝 🖄 😣	Authentication			😧 Help	
Start Page	Group by: No Grouping •				
Application Pools	Name	Status	Response Type		
a Sites	Anonymous Authentication	Disabled			
b Default Web Site	ASP.NET Impersonation	Disabled			
A 🗑 Exchange Back End	Basic Authentication	Enabled	HTTP 401 Challenge		
Autodiscover	Digest Authentication	Disabled	HTTP 401 Challenge		
DocumentPreview	Forms Authentication	Disabled	HTTP 302 Login/Redirect		
þ- 🕐 ecp	Windows Authentication	Enabled	HTTP 401 Challenge		
EWS					
Exchange					
Exchweb					
b g mapi					
Microsoft-Server-ActiveSync OAD					
b 🖓 ova					
b photos					
b Poplman					
PowerShell					
PowerShell-Proxy					
Public					
PushNotifications					
Quarantine					
ReportingWebService					
Reports					
p.i rest					
þ- 💮 Rpc					
p - RpcProxy					
Provide the second s					
b					
p - ync					
p-more	Features View 👘 Content View				
Configuration: 'Exchange Back End/PowerShell' web.confi	ig			91	
and the second					

Activate the desired authentication method. You must later select the same authentication method in the Exchange scan configuration that you activate here.

More useful information on authentication can be found at <u>Microsoft</u>.

Alternatively you can activate the authentication with PowerShell. For example: Activate Windows-authentication (Kerberos)

Get-PowerShellVirtualDirectory | Set-PowerShellVirtualDirectory -WindowsAuthentication \$true



You must restart the IIS in order to apply any changes.

For example in the command line or PowerShell:

iisreset

2.2.2 Enable Exchange Server auditing

The 8MATE Exchange Logga is based on Microsoft's Exchange Mailbox Auditing feature. The Exchange Logga automatically enables auditing for the <u>selected mailboxes</u>.

By recording the events, the mailbox size will increase by 1-2%, according to Microsoft. The Exchange Logga uses the default retention period (AuditLogAgeLimit) of 90 days

2.3 8MAN service account permissions

We recommend using service accounts (dedicated user accounts for 8MAN). This ensures that:

- the access rights of the service accounts are used by 8MAN, for example Active Directory read only without change rights
- it is easy to identify whether an action was performed by 8MAN or by a domain admin
- if the domain admin changes his password, the 8MAN configuration is not affected
- Avoid restrictions through activity limits (for example, Exchange Online allows only three parallel requests).

This approach allows for more detailed concepts by using several service accounts. In general, the more service accounts, the better you can fine tune and keep track of access rights. Please note that more detailed concepts generally also require more administrative efforts. The most basic concept only required one service account whom all required access rights are assigned to.

For 8MAN service accounts, please be sure to activate the option "Password never expires".

Feature	required access rights
8MAN server	The service account requires local administrator rights on the 8MAN server. Is the service account is a member of the domain Admin group, then this requirement is automatically fulfilled. If a server computer becomes a member of the domain (domain join) then the group Domain Admins will become a member of the local administrator group.
SQL Server	The 8MAN setup requires the role "dbcreator" on the SQL server. If you create a data base before, then 8MAN requires the role "dbowner". You can work with either Windows or SQL-server authorization.
Active Directory (AD)-Scan	Every user account requires at least read-only rights in order to be able to generate an AD scan. If you utilize delegation in your organization, then you must add the service account to a group that can read the required OUs.
AD Modify (8MAN Enterprise)	If you work with delegation in your company, you must assign the service account to a group that is allowed to change the relevant OUs. Without delegation: The service account becomes a member of the Domain admin group.
File Server (FS)-Scan	The user account requires access rights in order to be able to read NTFS permissions as well as traverse folder so that it can access the required folders. The service account can become a member of the domain admin group. If the domain admin account does not have access to all folders (for example user folders) then add the service account to the backup operators on the file server.

Feature	required access rights
AD Logga	The service account must be a member of the group "event log reader". Members of the domain admin group also have the required access rights to be able to read event protocols.
FS Logga	No service account is required for the FS-Logga functionality. The "NT Authority system" must have access to the monitored directories. You can find more information regarding required settings in the FS Logga handbook.
8MATE Exchange	To read exchange access rights please add the service account to the group "View-Only Organization Management". To be able to change access rights on the Exchange server please add the service account to the group "Organization Management" (read only rights are included). The service account requires admin rights on the collector server. Further access settings (impersonation, own mailbox) may be required and are contained in the section "Exchange Scans".
8MATE Share Point	The service account must be a member of the group "local adminstrator" of the SharePoint server. The service account must be a member of the SharePoint farm administrator group. The service account requires the special access right "SharePoint_Shell_Access" and must be a member of the local group "WSS_Admin_WPG". The service account requires "full access" to run the web interface. Further access settings are required (Authorization of the SharePoint data base, which is further described in the SharePoint handbook.
8MATE SharePoint (site collection)	The required permissions are described in chapter Accounts for a SharePoint scan via Remote Connector.
8MATE Exchange Logga	The logon account must be a member of the Organization Management and Records Management roles on the selected Exchange Server.

3 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 demoadmin 8MAN-DEMO srv-8man Configuration		
No license available!		~~	
Load license			
Technologies			
Features			
Max. Logbook entry age in days			

8	Pleas	e choose a license f	ile			X
⋲ 🍥 🔻 🕇 퉬 « La	ocal Disk (C:) 🕨 ProgramData 🕨 protected-netv	vorks.com + 8MAN +	licenses	✓ ¢	Search licenses	,P
Organize 🔻 New fold	ler				≣≕ ▼ 🔲	0
☆ Favorites	Name	Date modified	Туре	Size		
Desktop	8Man_20161117125549.license	11/17/2016 1:55 PM	LICENSE File	8 k	(B	
Uownloads						
This PC Image: Constraint of the sector of						
File <u>n</u>	ame: 8Man_20161117125549.license			~	License files (*.license)	~
					Open Cano	el

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.



4 Configure the Exchange Logga

4.1 Add an Exchange Logga configuration

BMAN Configuration				_	On	the start page of the
Back File Server CSV	Import			0	col	nfiguration, select "Scans".
 Select a technology below to ad 	ld a new resource configuration				001	
Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource	File server File Server Resource		
Local Accounts	Monitoring an Active Directory	Logga - Exchange Monitoring an Exchange Server	Monitoring a File Server	Microsoft Dynamics NAV Microsoft Dynamics NAV- access viewer	SP	lect "Logga - Exchange"
SharePoint Sharepoint Resource (Farm Based)	SharePoint SharePoint	SharePoint Online SharePoint Online Site Collection	-		500	eet Logga Exchange .
🖉 Filter				12		
l l l l l l l l l l l l l l l l l l l	8man-demo.local			×		
The domain 8man-demo.lo	ocal will be scanned weekly, Saturday, 9:00	PM [] (More »)				
	d with this domain. Add resource configu	ration *				
(N) 8man-dem	io.local (8man-demo.local)			×		
The domain 8man-demo.log	cal is monitored on SRV-8MAN using acco	unt <u>8man-demo\administrator</u> .				
Refresh data all 1 min	nutes.					
				×		
	-exchange13.8man-demo.local					
The Exchange srv-exchange	e13.8man-demo.local will be scanned On c	demand [] (More»)				
	1			××		
Keady				demoadmin @ localhost 🛀 📰		
8MAN Configuration				_ 🗆 ×	1.	Specify valid credentials for the
						Exchange to be monitored. See
 Select a technology below to ad 	d a new resource Exchange Logga s	election	X			also, required permissions
			and the list when the size			uiso: <u>requirea permissions</u>
Local Accounts	credentials are insufficie	nt to find all resources.	resh the list when the given	Microsoft Dynamics NAV Microsoft Dynamics NAV- access viewer	2.	Optional: Use the filter to find
SharePoint	Credentials 8man-demo\de	moadmin				the desired server
	2 Filter or type IP or Nan	ne	1 🚯			the aconed server.
🕰 Filter	3 O Microsoft Exchange	Name Online	Version Online		3.	Select a server.
	8man-dar			×	Δ	Choose a collector server You

 Choose a collector server. You can only select one collector per Exchange.

If you have added an Exchange Logga configuration, the Logga is initially disabled.

You must <u>enable the Exchange Logga</u> to record events.

Assigned collectors

8MAN

ON O 8man

20

 \otimes

4.2 Customize an Exchange Logga configuration

8MAN Configuration				×
Back File Server CSV Impact Select a technology below to add a new resource configuration Image: Domain Control (Server CSV) Domain Control (Server CSV) Image: Domain Control (Server (Server CSV) Image: Domain Control (Server (Server CSV) Image: Domain Control (Server (Server (Server CSV) Image: Domain Control (Server				
 Select a technology below to add 	a new resource configuration			
Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource	File Server File Server Resource
Local Accounts	Monitoring an Active Directory	Monitoring an Exchange Server	Monitoring a File Server	Microsoft Dynamics NAV Microsoft Dynamics NAV- access viewer
SharePoint ☆ Sharepoint Resource (Farm Based)	SharePoint SharePoint	SharePoint Online SharePoint Online Site Collection		
4 Filter				12
The exchange server 8man-demo.	com 1 mo.com (ExchangeOnline) is monitored	on SRV-8MAN using account sa-8mansc	an@8man-demo.com.	×
Following filters ave been se	t. <u>All mailboxes will be monitored</u> , change Online by using authentication	nechanism <u>Basic</u> .		
Refresh data all • 10 • minut	es.			
Ready				demoadmin @ localhost 🗲 🌁

- 1. Change the name of the configuration.
- 2. Change the credentials used by the Exchange Logga to read the events from the Exchange Server. See also: <u>required</u> <u>permissions</u>.
- 3. Optional: Put filters.
- 1. Choose the authentication method that must match the <u>PowerShell website</u> configuration.
- 2. Set the interval for the data refresh. The events are collected by the collector and passed to the 8MAN server in the defined interval. Default value (recommended): 10 minutes.

8MAN Configuration				_
Back File Server CSV Im	port			0
 Select a technology below to add 	a new resource configuration			
Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource	File server File Server Resource
Local Accounts	Monitoring an Active Directory	Monitoring an Exchange Server	Monitoring a File Server	Microsoft Dynamics NAV Microsoft Dynamics NAV- access viewer
SharePoint ☆ Sharepoint Resource (Farm Based)	SharePoint SharePoint	SharePoint Online SharePoint Online Site Collection		
4 Filter				12
Binan-demo.	com			×
The exchange server 8man-de Following filters have been se The scanner will connect to Ex	mo.com (ExchangeOnline) is monitored o t. <u>All mailboxes will be monitored</u> , change Online by using authentication m	n SRV-8MAN using account <u>sa-8mansca</u> echanisn <mark>Basic. 1</mark>	n@8man-demo.com.	
Refresh data all 10 minut	es. 2			v
Ready				demoadmin © localhost 🗲 🕍

4.3 Select the mailboxes to be monitored

8MAN Configuration				×
Back File Server CSV Im	port			0
 Select a technology below to add 	a new resource configuration			
Active Directory Resource	Easy Connect - CSV Easy Connect - CSV resource	Easy Connect - SQL Easy Connect - SQL resource	Exchange Exchange Resource	File server File Server Resource
Local Accounts Local Accounts of a server	Monitoring an Active Directory	Monitoring an Exchange Server	Monitoring a File Server	Microsoft Dynamics NAV Microsoft Dynamics NAV- access viewer
SharePoint	SharePoint SharePoint	SharePoint Online SharePoint Online Site Collection		
Q Filter Refresh data all ▲ 10 ▶ minut	es.			12
The exchange server 8man-demo. The exchange server 8man-de Following filters have been set The scanner will connect to Ex	com mo.com.(EvchangeOnline) is monitored (All mailboxes will be monitored, 2 change Online by using autoentication m	on SRV-8MAN using account <u>sa-8manscr</u> echanism <u>Basic</u> .	in@8man-demo.com.	×
Refresh data all 4 10 Minut	es.			Ÿ

- 1. The symbol indicates an Exchange Logga configuration.
- 2. Click on the link. By default, all mailboxes are monitored.

1. First select a mode.

Blacklist

By default all mailboxes will be monitored, including those added in the future. You specify which mailboxes are excluded from monitoring.

Whitelist

You explicitly specify which mailboxes are monitored.

2. Click on the plus to add entries.



Exchange Logga Filter Configuration

- 1. Use the search to find desired mailboxes.
- 2. Select the desired mailboxes.
- 3. Click "Add".

×



4.4 Filter the Exchange Logga events

Filter out uninteresting events to record only relevant entries. Filtering here means that filtered out events are not recorded.

This significantly increases the overview and reduces data volumes.

4.4.1 Understand the filter principles

The Exchange Logga Filter is designed as a blacklist filter. Blacklist means here: The Exchange Logga records to the maximum extent. You determine which events are not recorded (discarded).

The filter criteria work additively. An event is rejected if criterion 1 or criterion 2 or criterion 3 applies, or several criteria simultaneously.

The filter criteria are not correlated with each other. The events are evaluated by the Exchange Logga one after the other according to the criteria. In the case of a hit, the event is immediately rejected and no longer checked, regardless of whether another criterion has already been evaluated or not.

Example:

If user A is configured as an "action author" filter, all changes made by him in Exchange will be discarded, even if the actions or roles he has performed are not configured as a filter.

Exchange Logga Filter Configuration

4.4.2 Configure the event filters



SET FILTER CRITERIAS TO LIMIT THE AMOUNT OF DATA COLLECTED BY THE EXCHANGE LOGGA

- 1. The symbol indicates an Exchange Logga configuration.
- 2. Click on the link.

× 1. Filter events from users.

0

2. Select one or more users and drag them to the right column. Events triggered by these users are not recorded (blacklist).

	4 Filter	384	4 Filter
	Name		Name
	2016.03.07Benutzer Test (8man-demo\2.test)	^	
	Aber, Mark (8man-demo\Mark Aber)		
	ADLogga Tester (8man-demo\ATester)		
	Admin Manager (8man-demo\Admin Manager)		
	Administrator (8man-demo\Administrator)		
change events	Alien, Arnold (8man-demo\Arnold Alien)		
1111	Aloe, Vera (8man-demo\Vera Aloe)		
****	Ander, Cori (8man-demo\Cori Ander)		
Action author	Ander, Ole (8man-demo\Ole Ander)		
	🚽 🗞 Andrea Azubi (8man-demo\Andrea.Azubi)		
1111	Aner, Dominik (8man-demo\Dominik Aner)		
ations and miles	Angebrandt, Angie (8man-demo\Angie Angebrandt)		
ctions and rules	Ann Essay (8man-demo\Ann Essay)		
1111	Anna Lyse (8man-demo\Anna Lyse)		
	😞 Anna Ziese (8man-demo\Anna Giese)		
gga monitoring	Ansgar Agentor (8man-demo\AAgentor)		
	🐼 Anton Admin (8man-demo\demoadmin)		
	Apfel, Adam (8man-demo\Adam Apfel)		
	Arbeit, Andi (8man-demo\Andi Arbeit)		
	Arm, Armin (8man-demo\Armin Arm)		
	👃 Aroni, Mark (8man-demo\Mark Aroni)		
	Asil, Claire (8man-demo\Claire Asil)		
	Au Ditor (8man-demo\Au Ditor)		
	Auditor Manager (8man-demo\Auditor Manager)	~	
lease add a comment			
icase add a comment	4		

Exchange Logga Filter Configuration

- × 1. Filter events based on specific login types or actions.
 - 2. Actions (lines) of login types (columns) with an eye icon are recorded.
 - 3. You must enter a comment to save changes to the filter settings.

SET FII	TER CRITERIAS TO LIMIT THE	AMOUNT OF I	DATA COLLECT	ED BY THE EXC	HANGE LOGGA	٢
	A	dministrator	Delegate	Owner		
Exchange events Action author Actions and rules	Copy (1)		4₩ 4 ×	4 % 4 X		
	Create ①		۲	۲		
	FolderBind ①	۲	۲			
	HardDelete ①	۲	۲	۲		
	MessageBind (i)	۲			2	
	Move (i)	۲	۲	۲		
	MoveToDeletedItems ()	۲	۲			
Logga monitoring	SendAs 🛈	۲	۲			
20990	SendOnBehalf 🕕		۲			
	SoftDelete ()	۲	۲	۲		
	Update 🕕	۲	۲	۲		
Please add a comment		A		3	Apply Cance	ı (



4.5 Enable/disable the Exchange Logga



On the start page of the configuration, select "Scans".

- 1. The symbol indicates an Exchange Logga configuration.
- 2. In the desired Exchange Logga configuration, click the switch to enable the Exchange Logga.

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



Cancel



5 Evaluate the Exchange Logga data

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

Background / Value

Events recorded with the 8MATE Exchange Logga can be analyzed in detail and recurrently using the report functions. Specific questions about Exchange changes can be answered faster with the <u>logbook view</u>.

Additional Services

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

Step by step process



1. Select "Start".

2. Click "Exchange Logga Report".

- 8MAN Version: Exchange Logga Report rt-Konfiguration Exchange Logga Report Bere Bitte Ressource(n) auswähle Re Zeitraum Fester Zeitraum 30.10.2017 11:15 - 01.11.2017 11:15 2 Exchange-Ressourcen 7eitra hange13.8man-demo.local ×. Ben ldetyp Alle Administrator, Stellvertreter und Postfach-Be . Benutzer -. Bitte wählen Sie einen oder mehn werden, lassen Sie die Auswahl fri Aktionen Bitte wählen Sie eine oder m werden Jassen Sie die Auswa . Einstellungen Das Ausgabeformat ist <u>XLS</u> × Reportausführung <u>wird manuell gestartet</u> Benutzerdefinierter Speicherpfad ist <u>nicht konfiguriert</u> E-Mail Versenden ist <u>deaktiviert</u>
- 1. optional: Give the report a title and a description.
- 2. Set the period.
- 3. Add the required resources via drag & drop.

- Exchange Logga Report Report configuration Exchange Logga Report Comment Comment Selection of monitored mailboxes × \land Filter Time Period Fixed time span 12/16/2017 2:02 PM - 12/18/2017 2:02 PM Exchange Resources – Please select one or more exchange resources. Logon type All Adr User accounts Mailbox selection for report creation is Please select one or more accounts To search for all accounts leave this field empty currently not possible, because no data events available for Exchange tracers. Actions Please select one or more actions To search for all actions leave this field empty Settings The output format is XLS ~ Report execution mode <u>started manually</u> Custom storage path is <u>not configured</u> Send email is <u>Deactivated</u> Discard
- 1. Select the login type.
 - 2. If you have special users in focus, add them via drag & drop. For all users, leave the selection blank.
 - 3. Optional: Select Actions.

×

- 4. Define output options for the report.
- 5. Start the execution.

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

Background / Value

Events recorded with the 8MATE Exchange Logga can be analyzed in detail and recurrently using the report functions. Specific questions about Exchange changes can be answered faster with the logbook view.

Additional Services

Report: Monitor activities on mailboxes, calendars, and contacts

Step by step process



- 1. Select "Logbook".
- 2. Set the time period for log analysis.
- 3. The filters focus on the events you want to check.
- 4. Select all events of a day (one row).



- 1. Select a cell (an event type) to further narrow your query.
- 2. 8MAN displays a list of all selected events. The "Footprint icon with envelope" identifies events recorded by the Exchange Logga. Select an event.
- 3. 8MAN shows all details about the event.



Α

AD Logga aktivieren 20 deaktivieren 20 Architecture 4 Authentication PowerShell website 6

Ε

Exchange für Logga vorbereiten 8 Logga 3 Logga Ereignisse filtern 17 Logga unterstützte Versionen 5 Exchange Logga Konfiguration hinzufügen 13

F

FullLanguage 6

IIS Manager preparing Exchange scans 6

L

License load 11

Ρ

PowerShell preparing Exchange scans 6 PSLanguageMode 6

S

Service account 9