8MAN

Access Rights Management. Only much Smarter.

Access Rights Management

Exchange Logga Manual

Version 9

© 2018 Protected Networks GmbH

Protected Networks

© 2018 Protected Networks GmbH

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?

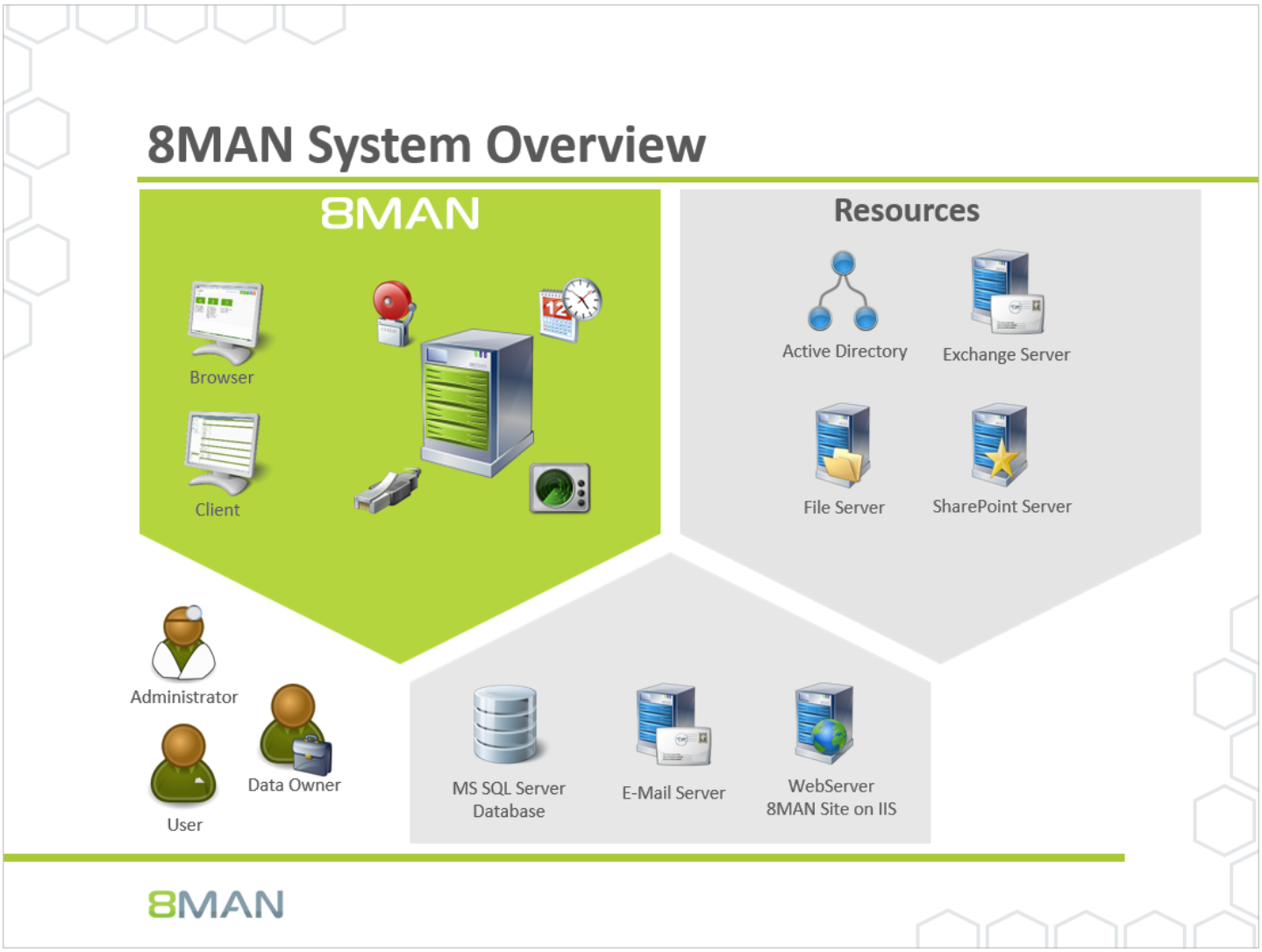
Services

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

© 2018 Protected Networks GmbH

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.

© 2018 Protected Networks GmbH

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 Microsoft.

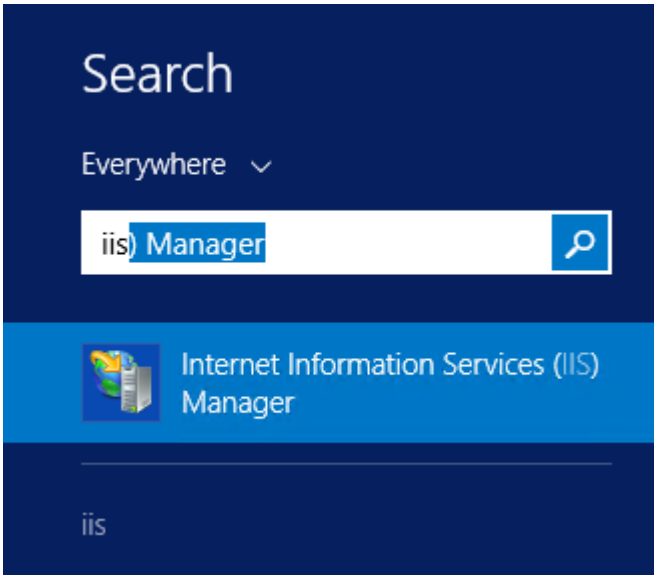
8MATE for Exchange is not mandatory - the Exchange Logga can be used independently.

© 2018 Protected Networks GmbH

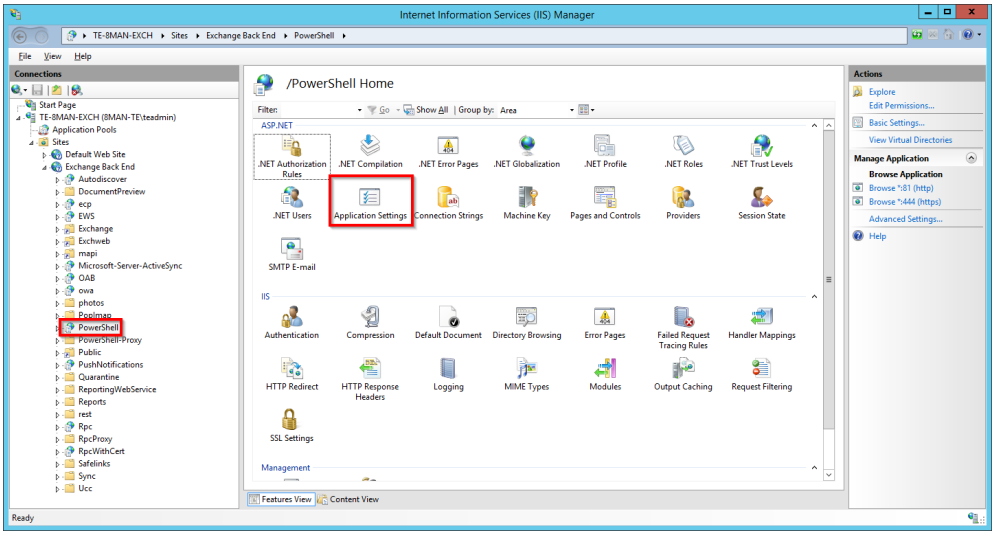
2.2.1 Prepare the PowerShell website

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.

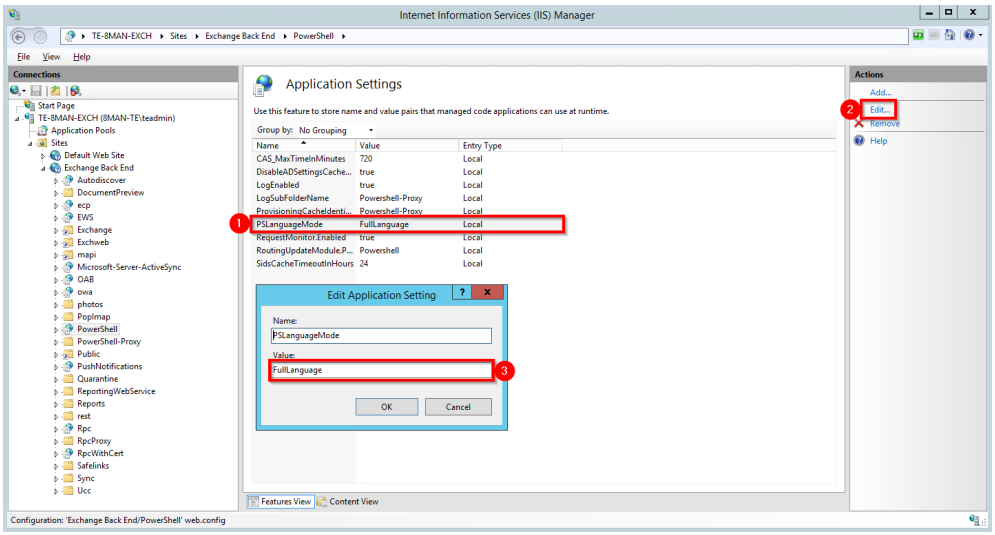


Start the IIS Manager on the CAS.

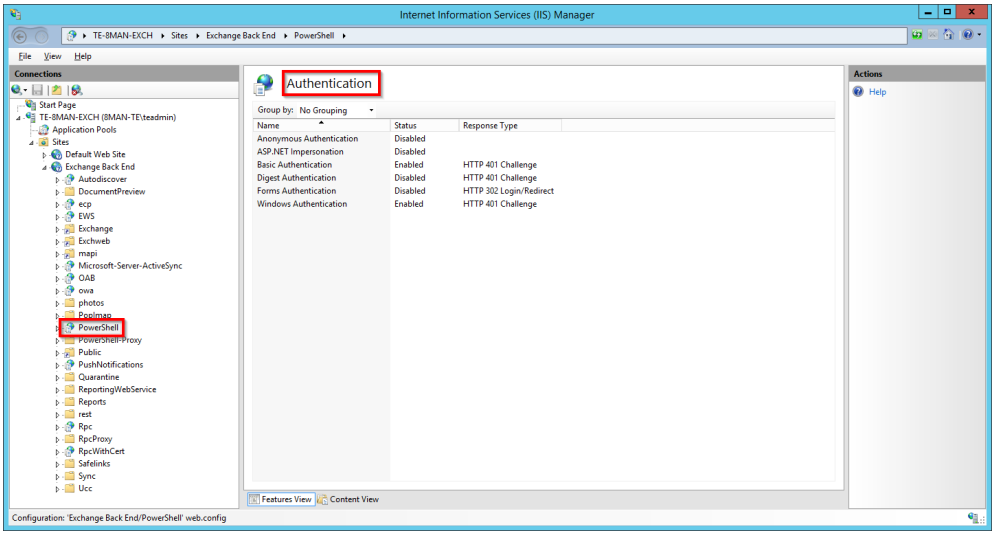


Navigate to "Powershell". In Exchange 2010 this can be found under "Default Web Site". In Exchange 2013 it is found under „Exchange Back End". Double-click "Application Settings".

© 2018 Protected Networks GmbH



1. *Select "PS LanguageMode"*
2. *Click "Edit"*
3. *Enter the value "FullLanguage".*



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 Microsoft.

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
```

© 2018 Protected Networks GmbH

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 selected mailboxes.

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

© 2018 Protected Networks GmbH

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".

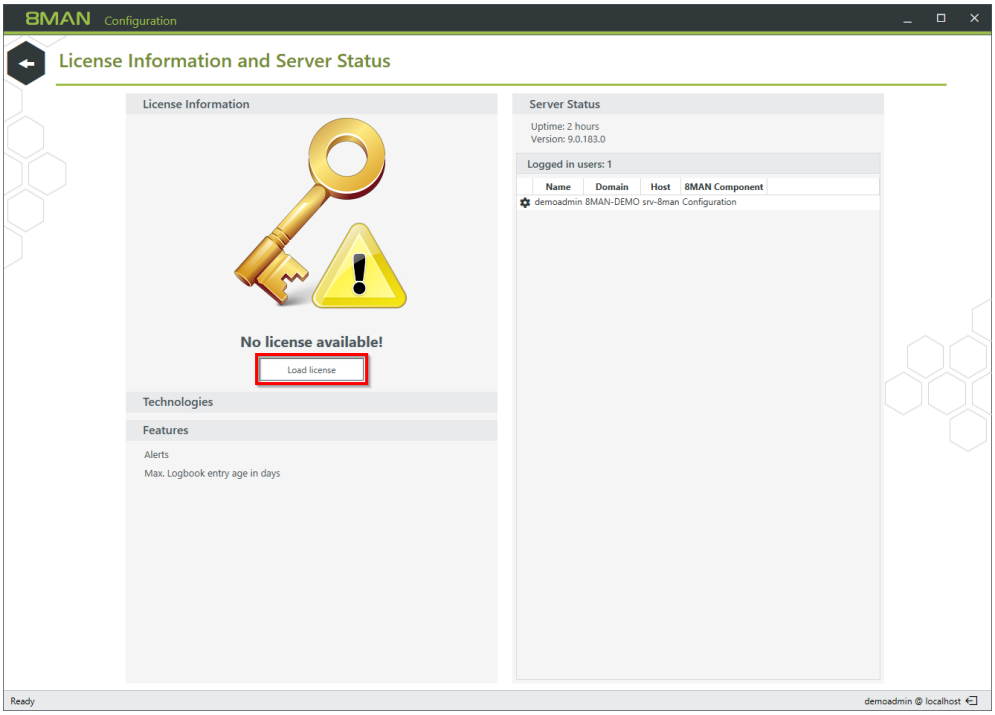
Feature	required access rights
8MAN server	The service account requires local administrator rights on the 8MAN server. Is the service account is a member of the domain Admin group, then this requirement is automatically fulfilled. If a server computer becomes a member of the domain (domain join) then 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.

© 2018 Protected Networks GmbH

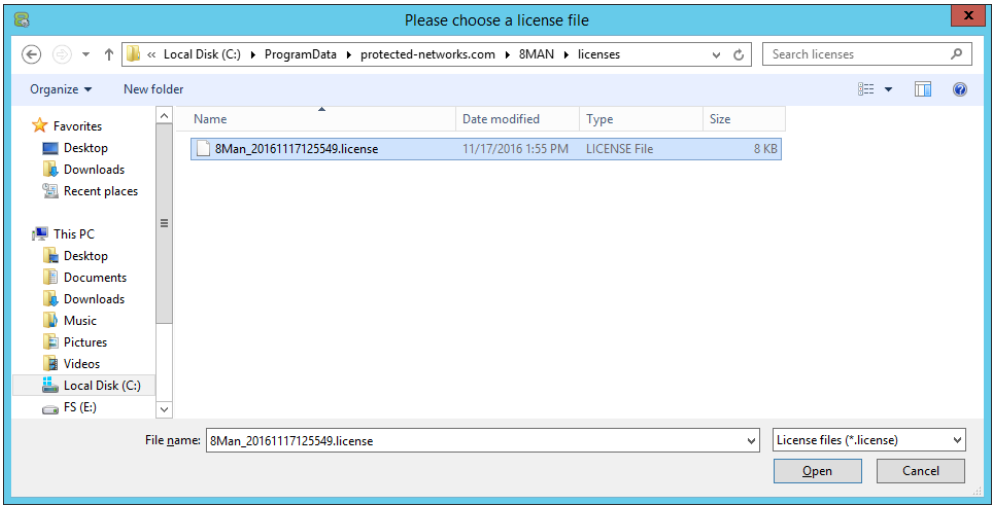
Feature	required access rights
AD Logga	The service account must be a member of the group "event log reader". Members of the domain admin group also have the required access rights to be able to read event protocols.
FS Logga	No service account is required for the FS-Logga functionality. The "NT Authority 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 SharePoint	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.

© 2018 Protected Networks GmbH

3 Load the license file and check covered features



Click on "Load license".



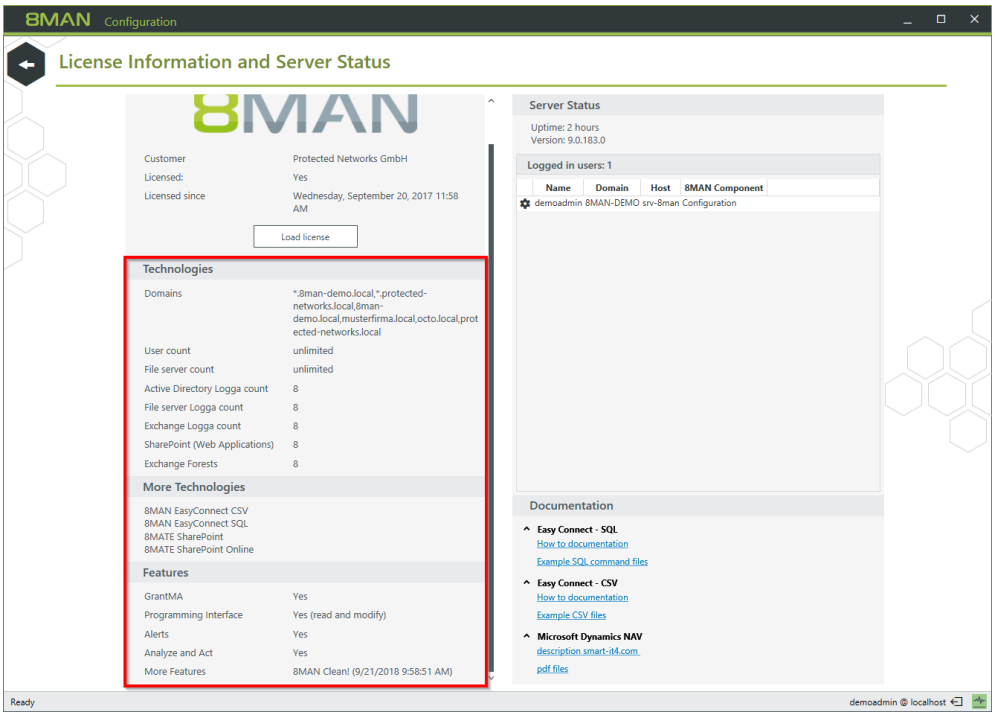
Select the path where your license key is stored.

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

After clicking on open, the license key will be copied to **`%ProgramData%protected-networks.com\8MAN\licenses`**

All licensed features are activated immediately.

© 2018 Protected Networks GmbH

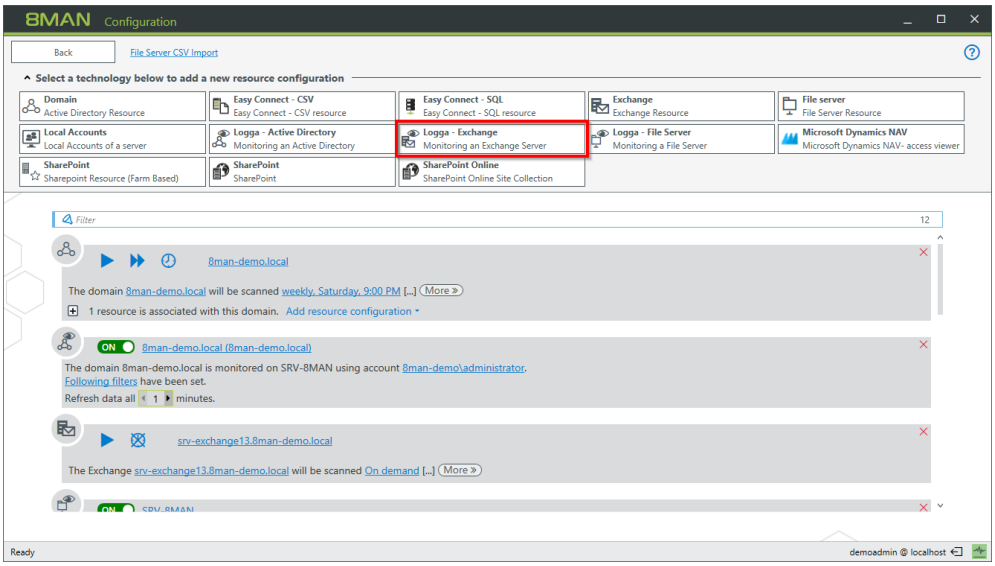


If the license file has been successfully loaded you will see detailed information on licensed features.

© 2018 Protected Networks GmbH

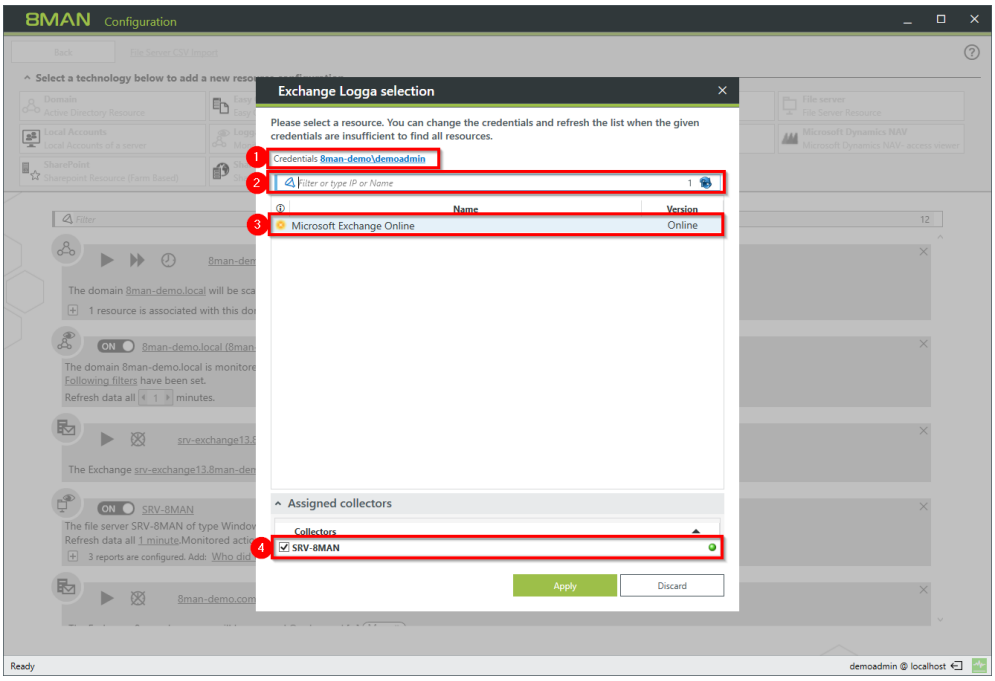
4 Configure the Exchange Logga

4.1 Add an Exchange Logga configuration



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

Select "Logga - Exchange".



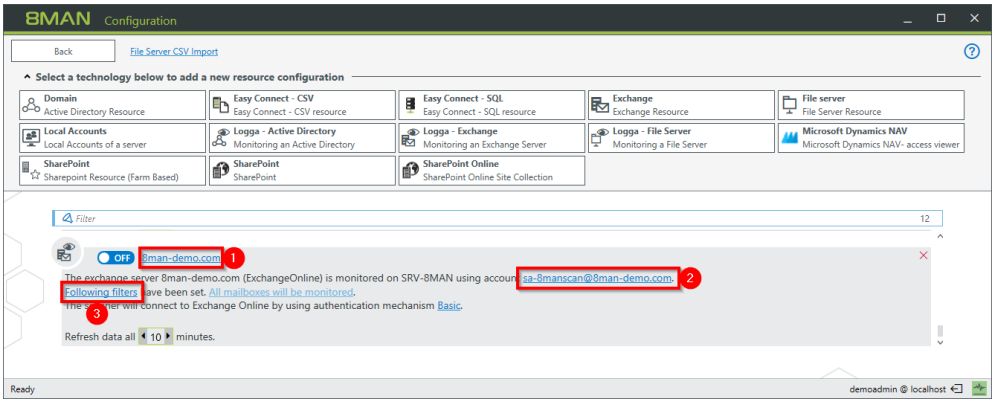
1. *Specify valid credentials for the Exchange to be monitored. See also: required permissions*
2. *Optional: Use the filter to find the desired server.*
3. *Select a server.*
4. *Choose a collector server. You can only select one collector per Exchange.*

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

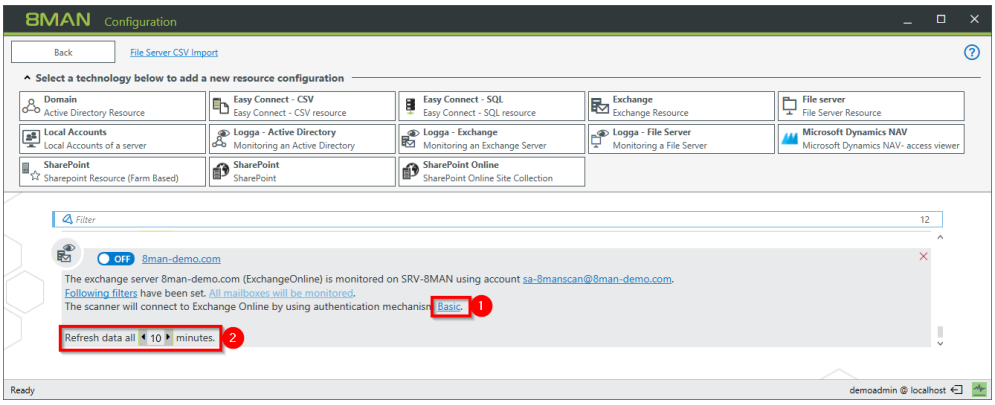
You must enable the Exchange Logga to record events.

© 2018 Protected Networks GmbH

4.2 Customize an Exchange Logga configuration



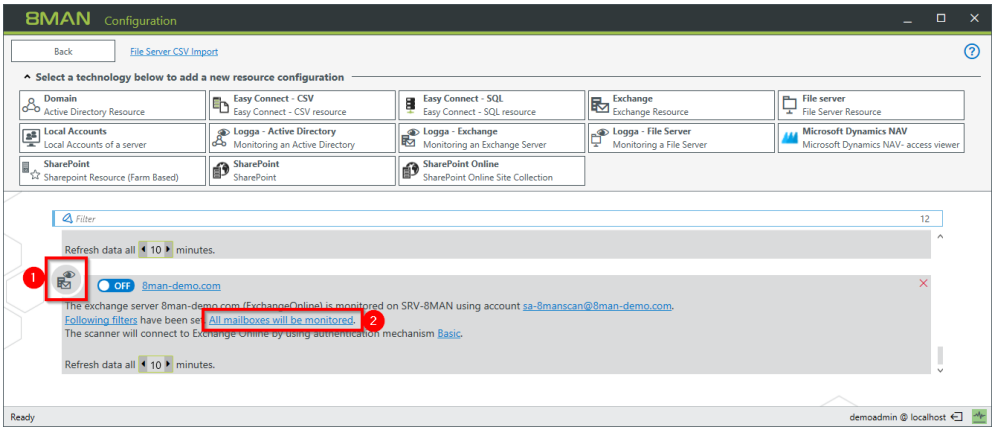
1. *Change the name of the configuration.*
2. *Change the credentials used by the Exchange Logga to read the events from the Exchange Server. See also: required permissions.*
3. *Optional: Put filters.*



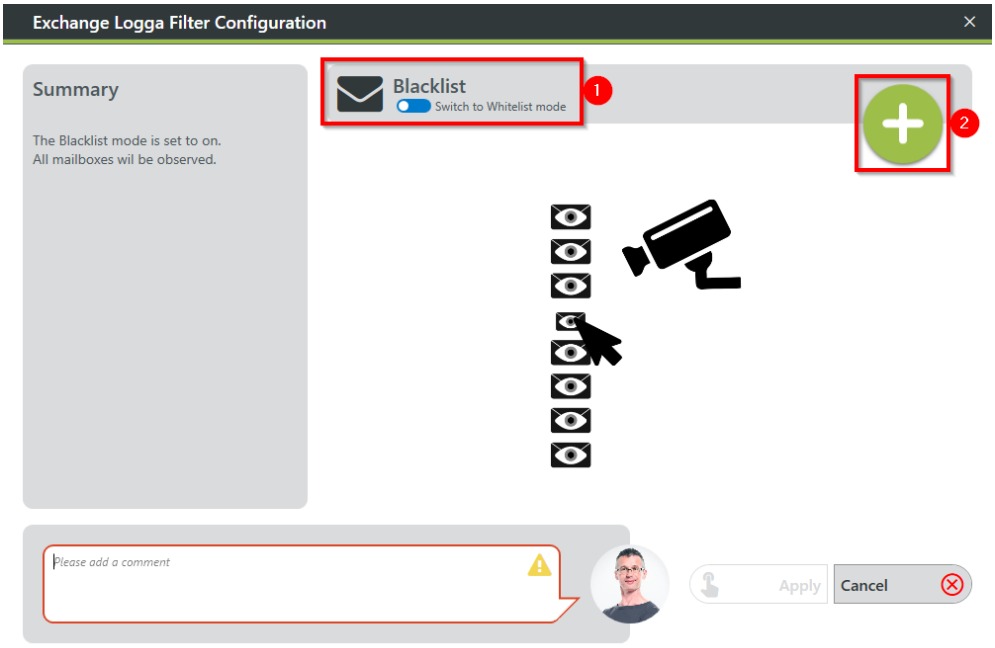
1. *Choose the authentication method that must match the PowerShell website configuration.*
2. *Set the interval for the data refresh. The events are collected by the collector and passed to the 8MAN server in the defined interval. Default value (recommended): 10 minutes.*

© 2018 Protected Networks GmbH

4.3 Select the mailboxes to be monitored



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



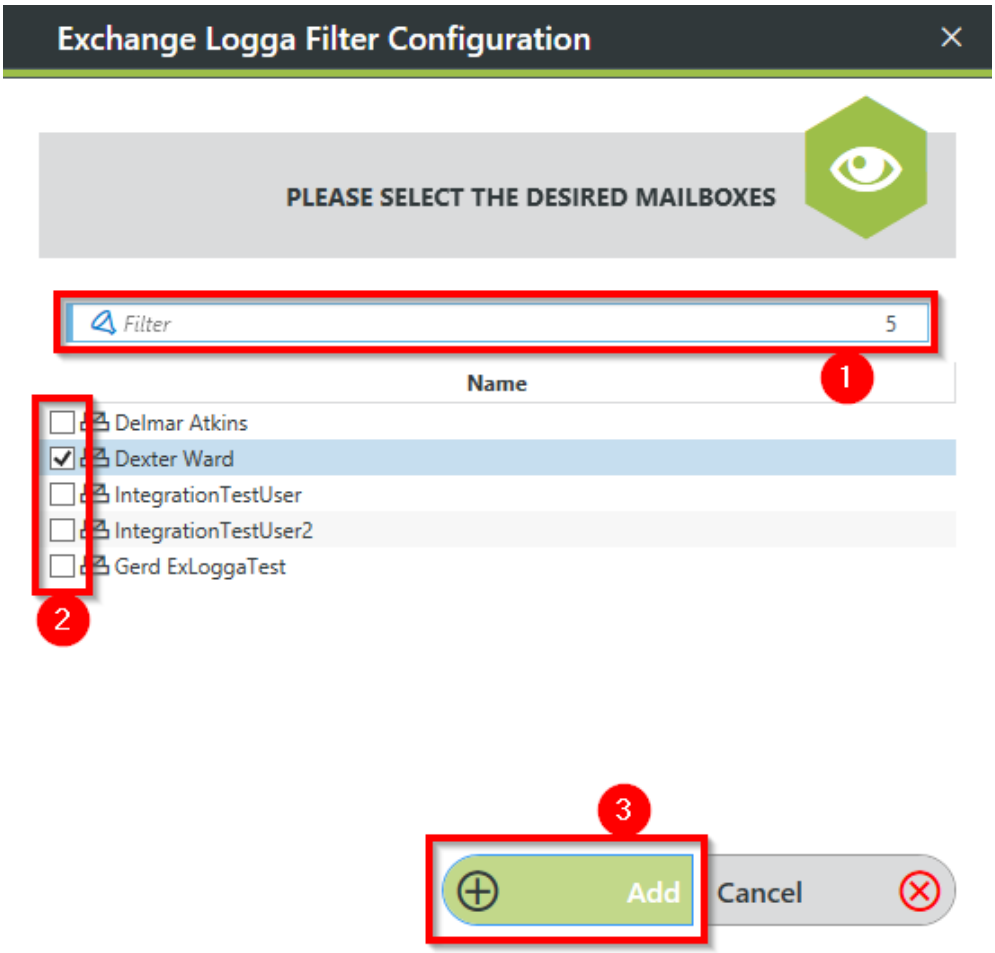
1. *First select a mode.*

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

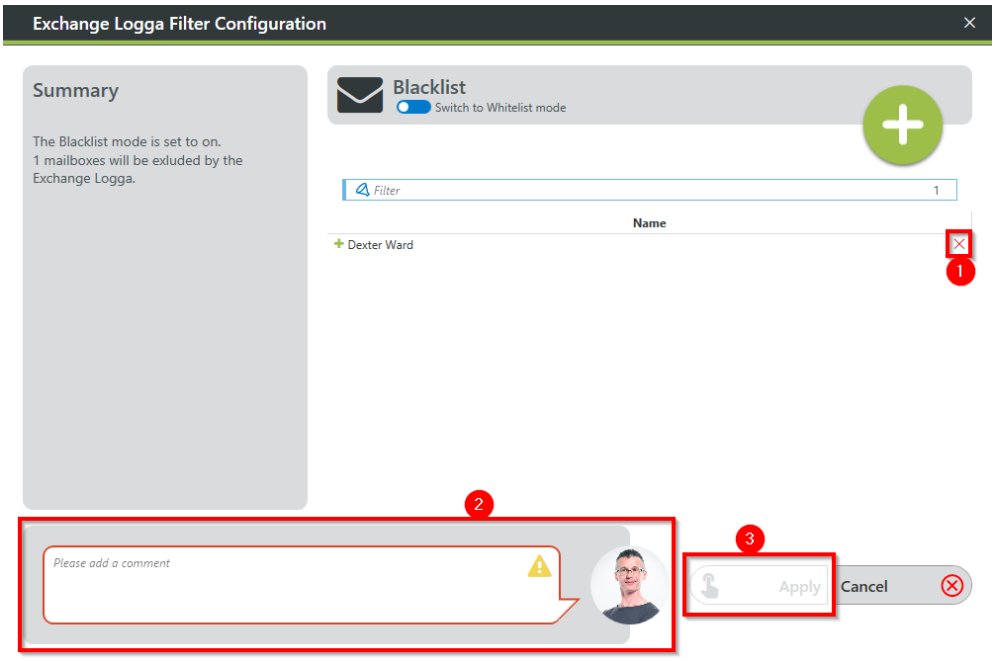
   Whitelist
   You explicitly specify which mailboxes are monitored.

2. *Click on the plus to add entries.*

© 2018 Protected Networks GmbH



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



1. *Klicken Sie auf das "X", um Einträge zu entfernen.*
2. *Sie müssen einen Kommentar eingeben.*
3. *Klicken Sie auf "Anwenden", um Ihre Konfiguration zu speichern.*

© 2018 Protected Networks GmbH

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).

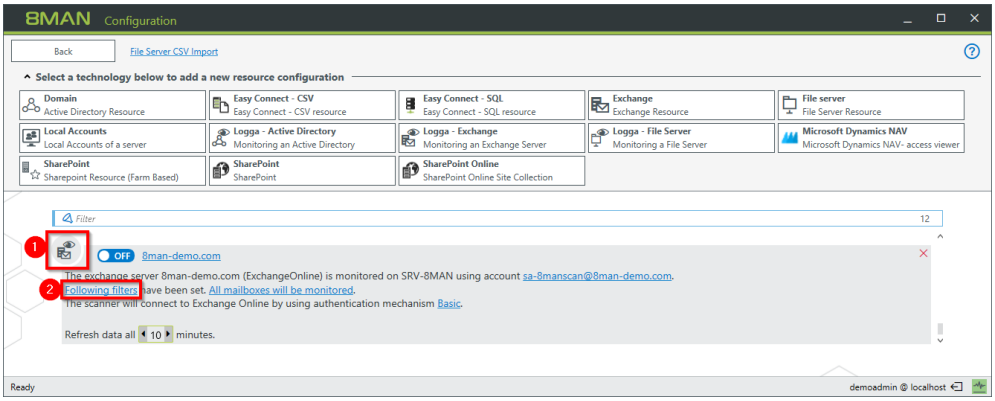
The filter criteria work additively. An event is rejected if criterion 1 or criterion 2 or criterion 3 applies, or several criteria simultaneously.

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.

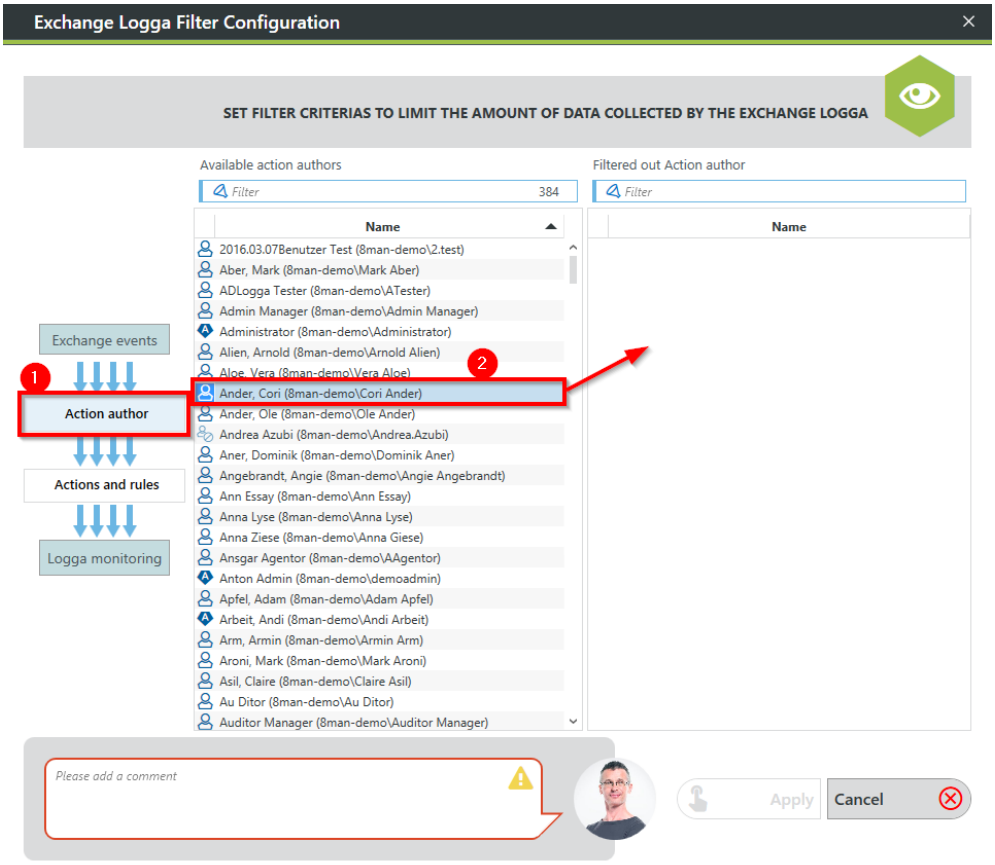
Example:
If user A is configured as an "action author" filter, all changes made by him in Exchange will be discarded, even if the actions or roles he has performed are not configured as a filter.

© 2018 Protected Networks GmbH

4.4.2 Configure the event filters

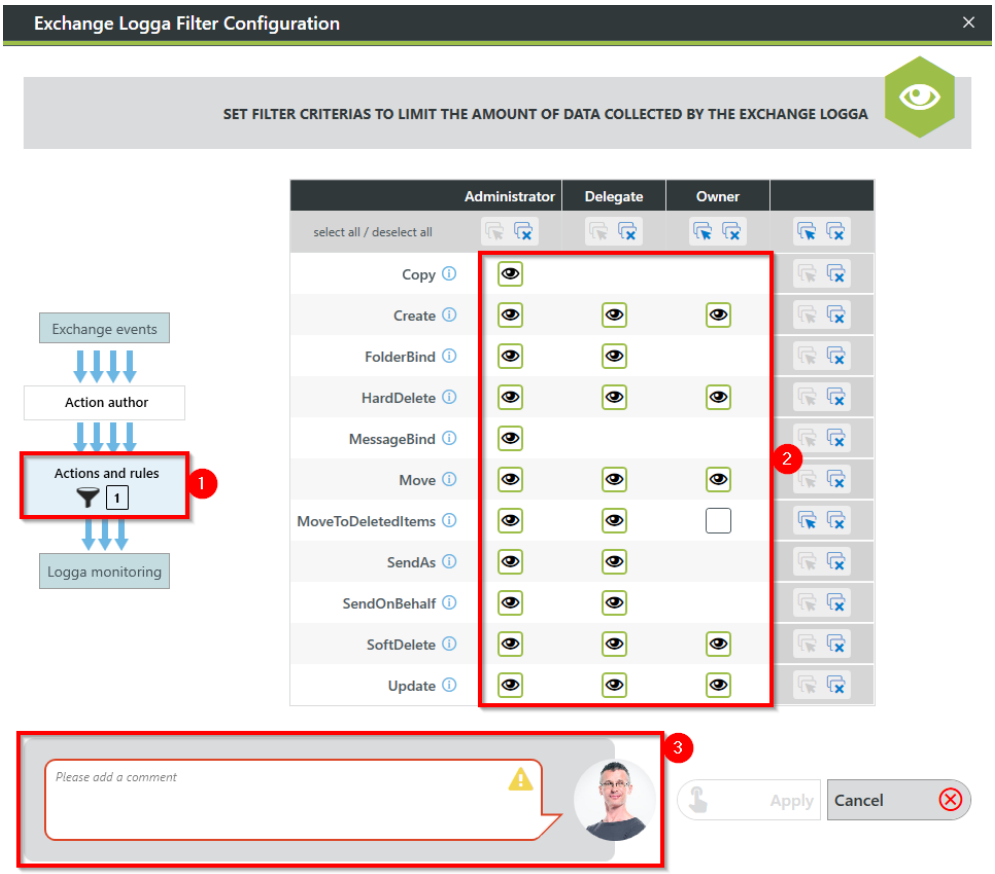


1. *The symbol indicates an Exchange Logga configuration.*
2. *Click on the link.*



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

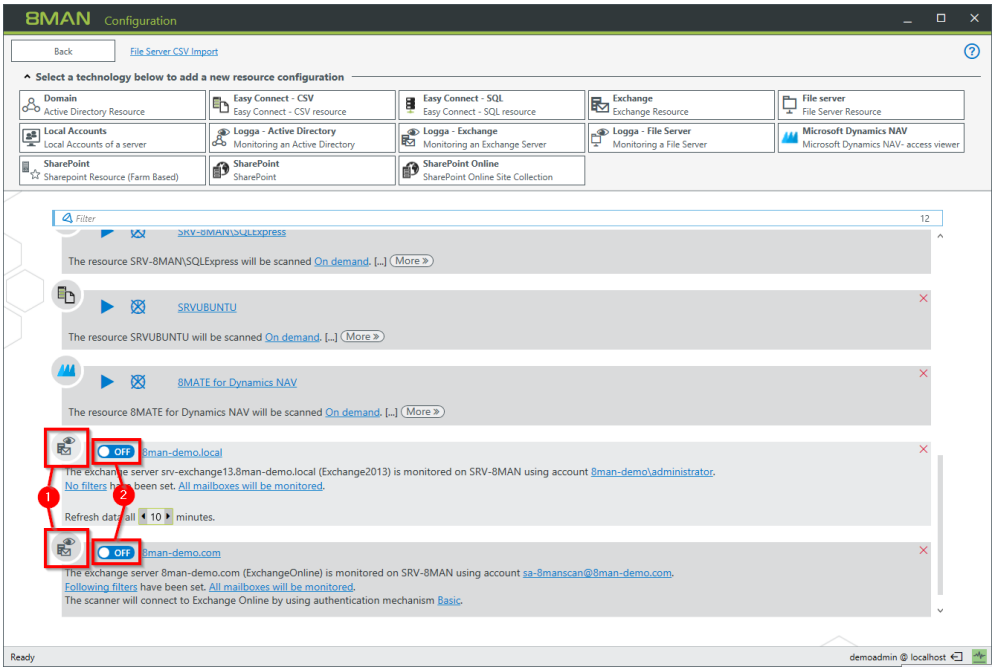
© 2018 Protected Networks GmbH



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.*

© 2018 Protected Networks GmbH

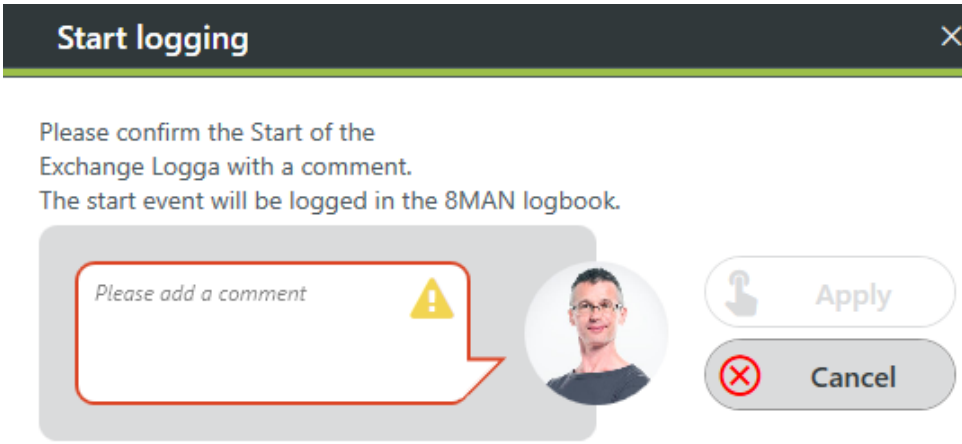
4.5 Enable/disable the Exchange Logga



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.



You must enter a comment.

Proceed in the same way for deactivation.

© 2018 Protected Networks GmbH

5 Evaluate the Exchange Logga data

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

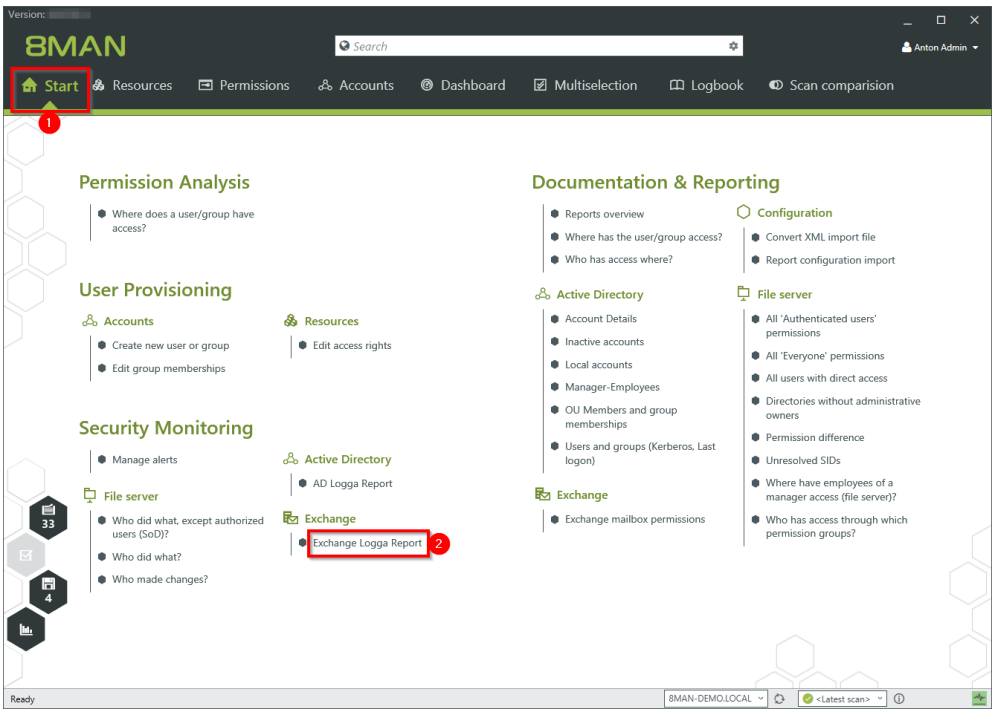
Background / Value

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 logbook view.

Additional Services

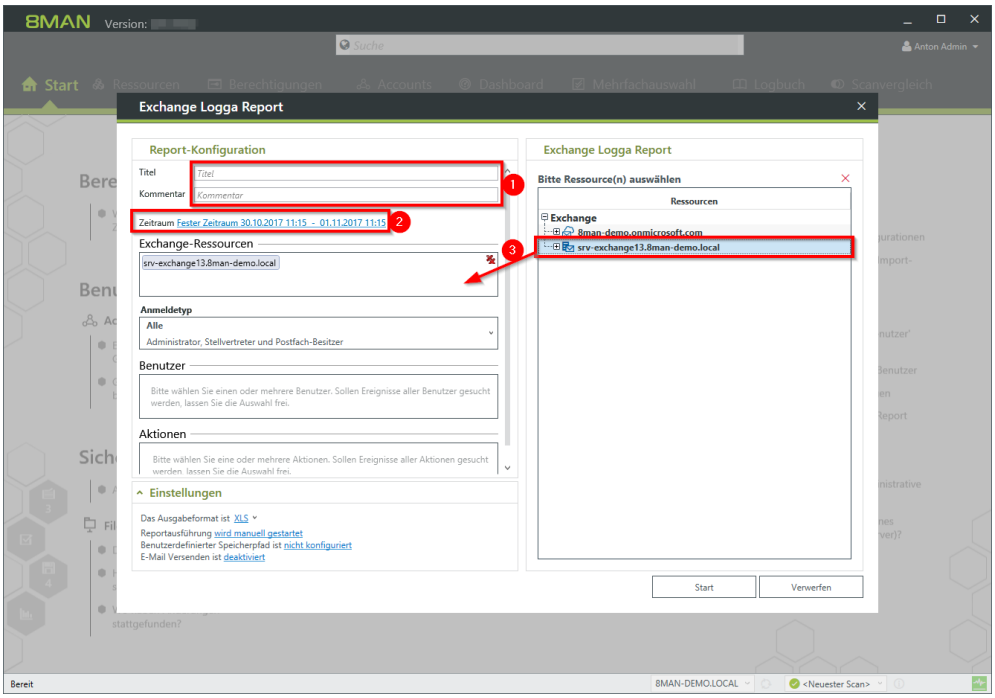
View activities in mailboxes, calendars, and contacts (logbook)

Step by step process

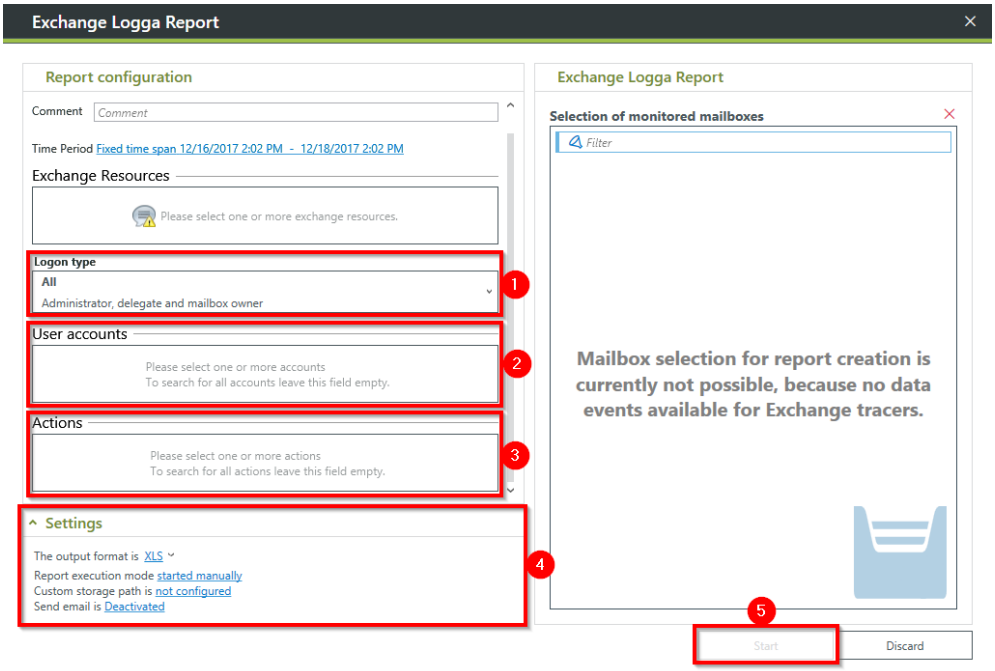


1. *Select "Start".*
2. *Click "Exchange Logga Report".*

© 2018 Protected Networks GmbH



1. *optional:*
   Give the report a title and a description.
2. *Set the period.*
3. *Add the required resources via drag & drop.*



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.*

© 2018 Protected Networks GmbH

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

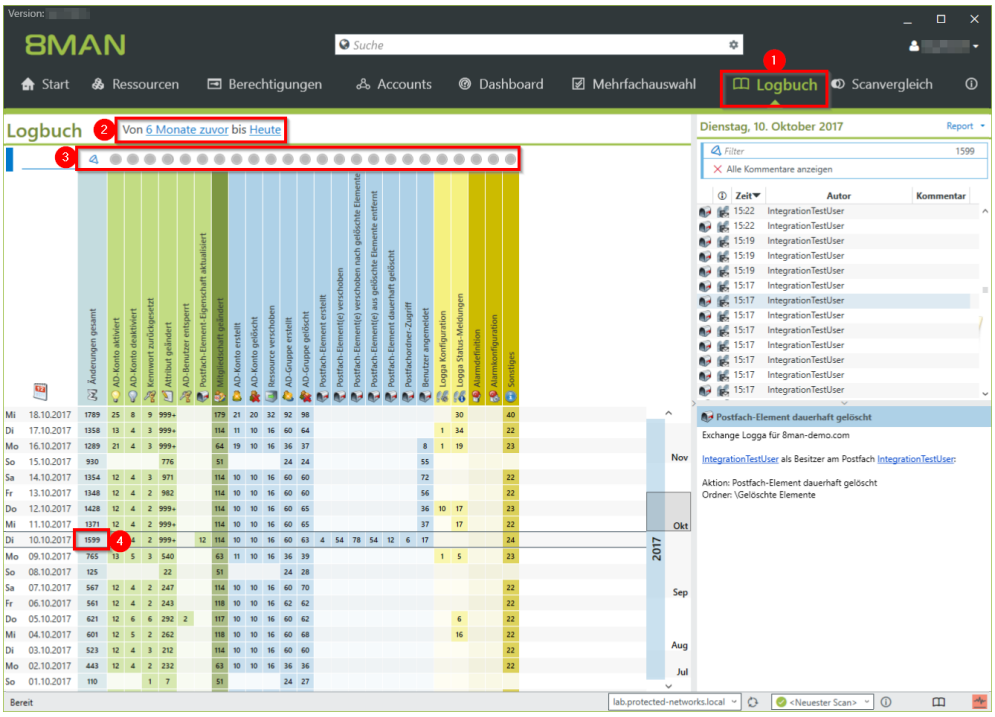
Background / Value

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.

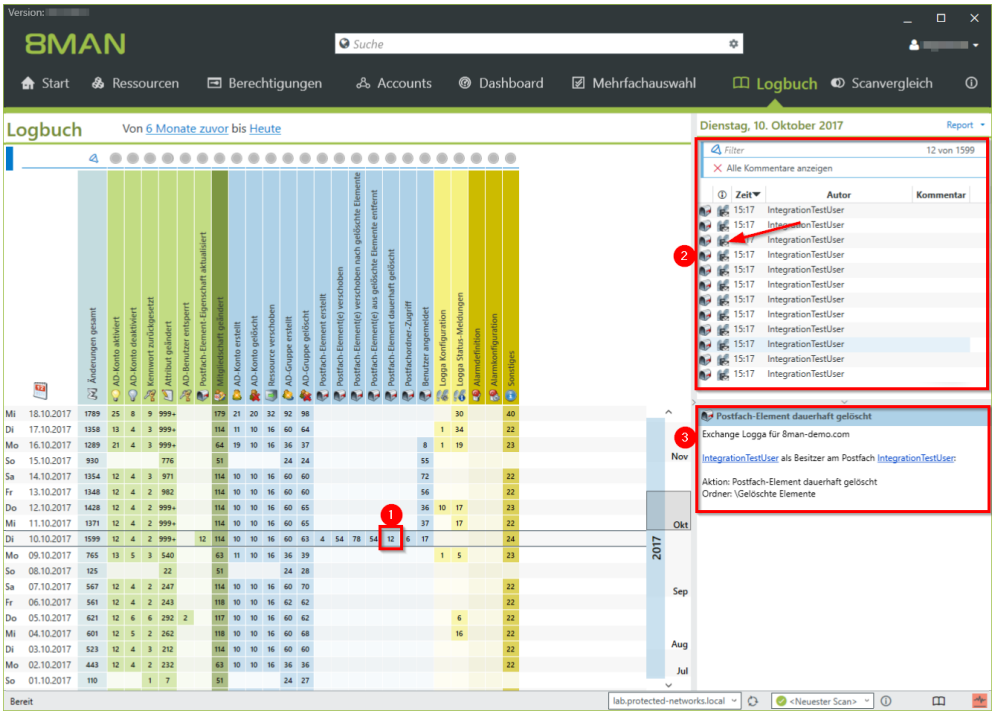
Additional Services

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.*

© 2018 Protected Networks GmbH

© 2018 Protected Networks GmbH

A

E

F

I

L

P

S

© 2018 Protected Networks GmbH