



RELEASE NOTES

V4.0.101 from 06.12.2011

Christian Zander

protected-networks.com GmbH
Alt-Moabit 73
D-10555 Berlin

+49 (30) 390 63 45 - 0
info@protected-networks.com
www.protected-networks.com

LIABILITY NOTICE

Information provided in this manual may change at any given time and without prior notice. Its provision does not entail any kind of legal obligation at protected-networks.com's end.

The usage of protected-networks.com'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.com 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.com'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.com. Trademarks and brands – with or without explicit display – are the intellectual property of the respective brand owners.

RELEASE NOTES

Limitations in the evaluation version

In addition to the temporal limitation of the use of 8MAN all reports are limited to 100 lines. XPS access rights reports are limited to 300 lines.

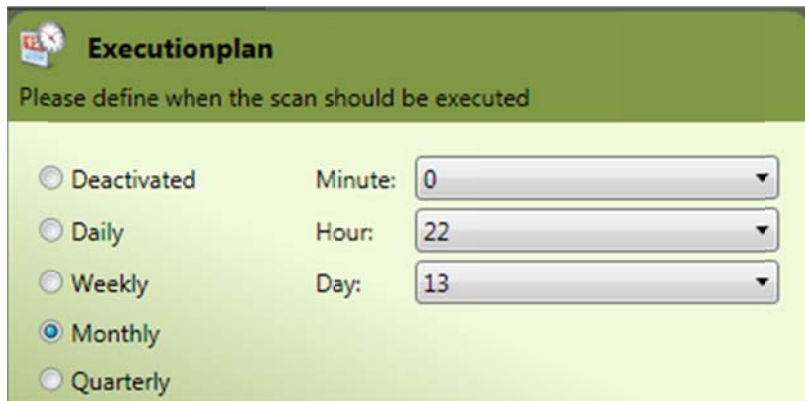
- Extended settings for scheduled tasks 4
- Global Logbook..... 4
- SharePoint – Scan Preparation 6
- SharePoint – Resource-View 111
- Group Reorts 15
- File Server Selection to Limit the Amount of Data 16
- Global Search with Logical Filter 17
- Active Directory - Soft-Delete & User Recovery 17
- Active Directory View – Selection History 17
- Create Users and Groups - Extensions 18
- Scan Comparison - Extensions..... 19
- Logga - File Server Monitoring (Beta-Version) 21
- Logga – Access Reports 25

4.0.101 FROM 06.12.2011

Extended settings for scheduled tasks

All scheduled tasks within 8MAN can now be set at monthly or quarterly intervals. This is applicable for scheduled reports, and scheduled scans for domains and file system.

Please note that the setting in greater than or equal to 29 days in specific modes for any of the scheduled task will not start automatically (eg: 29th of February (without a leap year) or the 31st of April).



Global Logbook

Global Logbook is available in version 4.0.



All system changes are shown in 8MAN's Global Logbook. The information within can be refined through the use of filters.

Reference

8MAN's Data Owner is not available for the Global Logbook.
Self-Generated user comments are not displayed.

By default the Logbook shows the last six months of activity. This time span can also be configured as desired. If (for example) the time span is configured for a period of more than one year, the item line on the left side margin will change to a quarterly preview.

From 6/15/2011 15 Until 12/12/2011 15

If you need to see all of the entries for a particular day, then click the all on filter



SharePoint – Scan Preparation

SharePoint site collections with "demand-based authentication" (Claims-Based Authentication) are not yet supported by 8MAN scanner.

Scan Account

For SharePoint to be able to scan it requires a User, which must meet the following requirements:

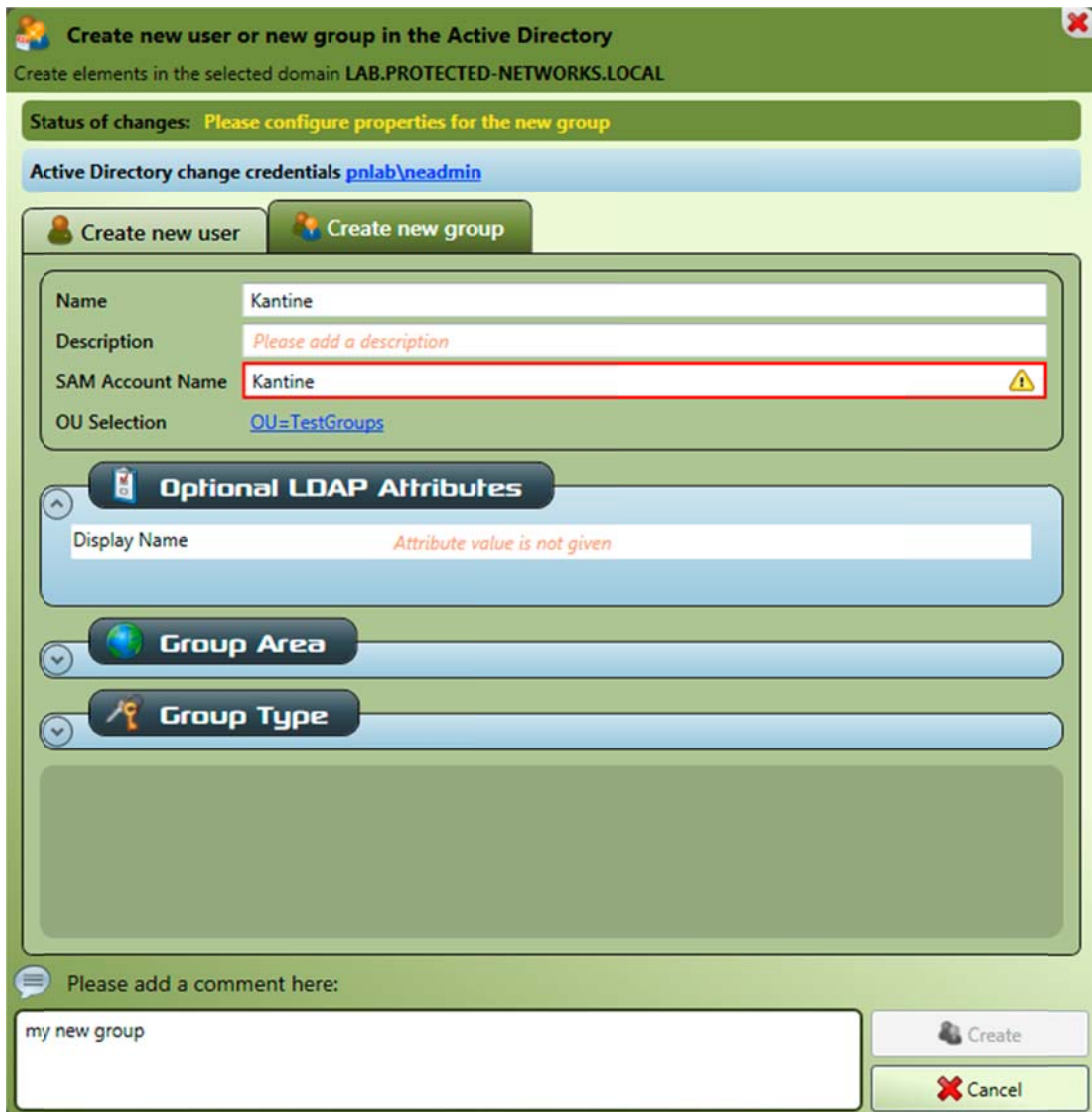
Conditions

The user must be a Member of the local Administrator group for each SharePoint server.

The User must have full access to each web application. A separate permission policy including additional access rights is also possible for each Web application with "Read All" access.

In connection here are some instructions on how you can create a SA- Service Account user:

In the first step you can create a new SA with the "Create new User/Group" option.



Create new user or new group in the Active Directory

Create elements in the selected domain **LAB.PROTECTED-NETWORKS.LOCAL**


Status of changes: **Please configure properties for the new group**

Active Directory change credentials [pnlab\neadmin](#)

Create new user | **Create new group**

Name: Kantine

Description: *Please add a description*

SAM Account Name: Kantine 

OU Selection: [OU=TestGroups](#)

Optional LDAP Attributes

Display Name: *Attribute value is not given*

Group Area

Group Type

Please add a comment here:

my new group

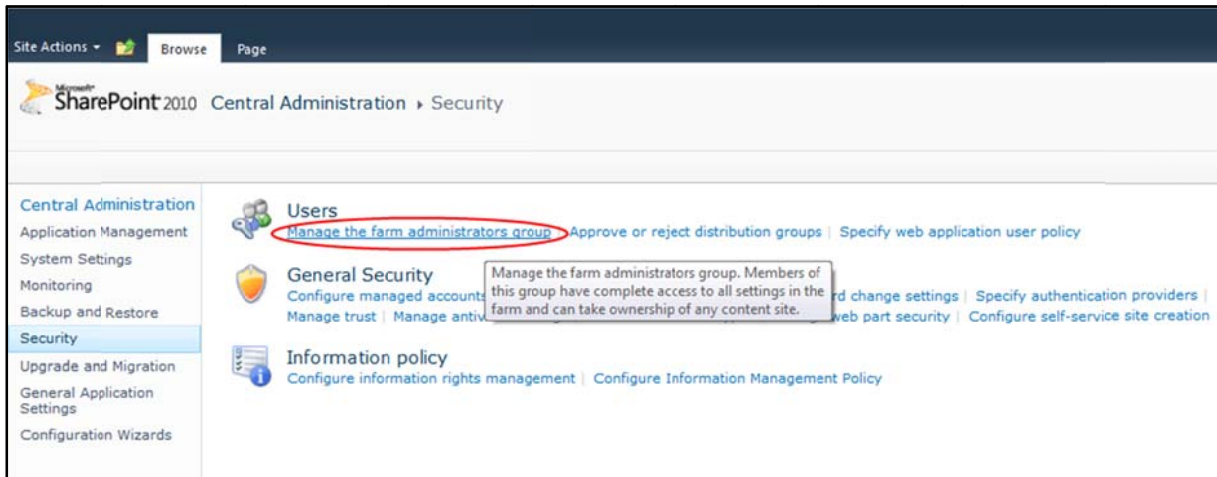
Create | **Cancel**

This newly created user must be placed in the local Administrators group for all SharePoint servers.

Authorisation Assignment

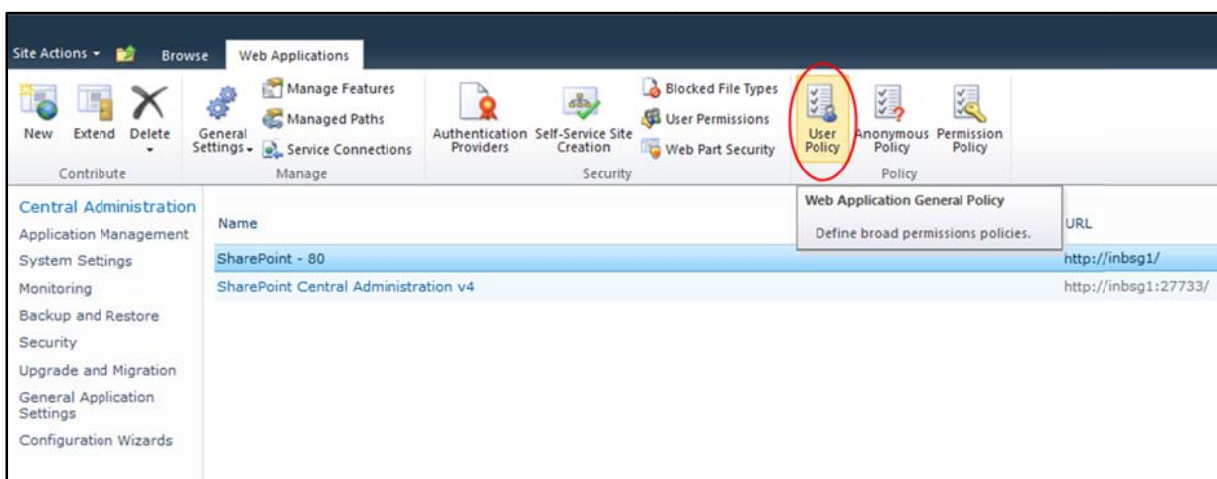
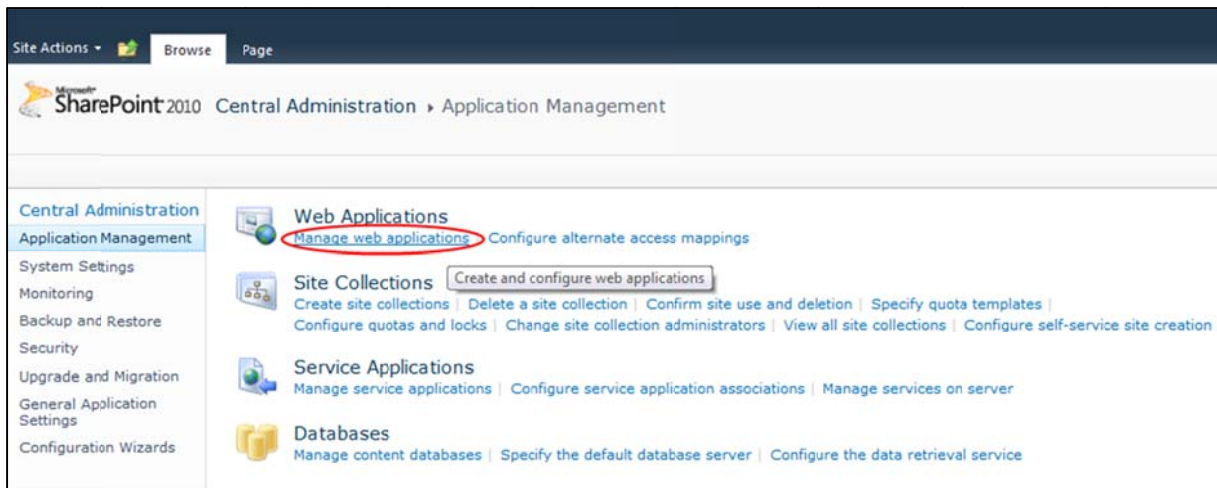
Farm Administrator

The scan account must be added to the Central Administrators for SharePoint, in the farm Administrators Group.



Web Application Policy – Full Read

At present all web Applications with Scan Account must have policies with “Full Read” entitled, otherwise the whole content cannot be fully scanned.



Optional Access Rights

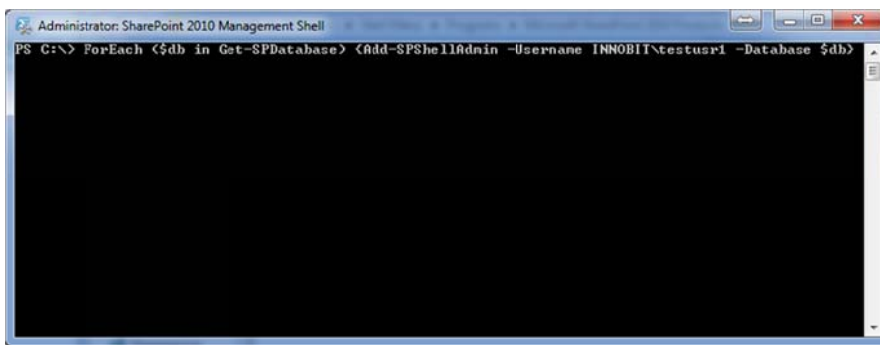
In special circumstances (When SharePoint has not been configured based on best practices) the following permissions may be required:

- **SharePoint Shell Administrator**

The "SharePoint 2010 Management Shell" extends the use of the Scan Account permissions.

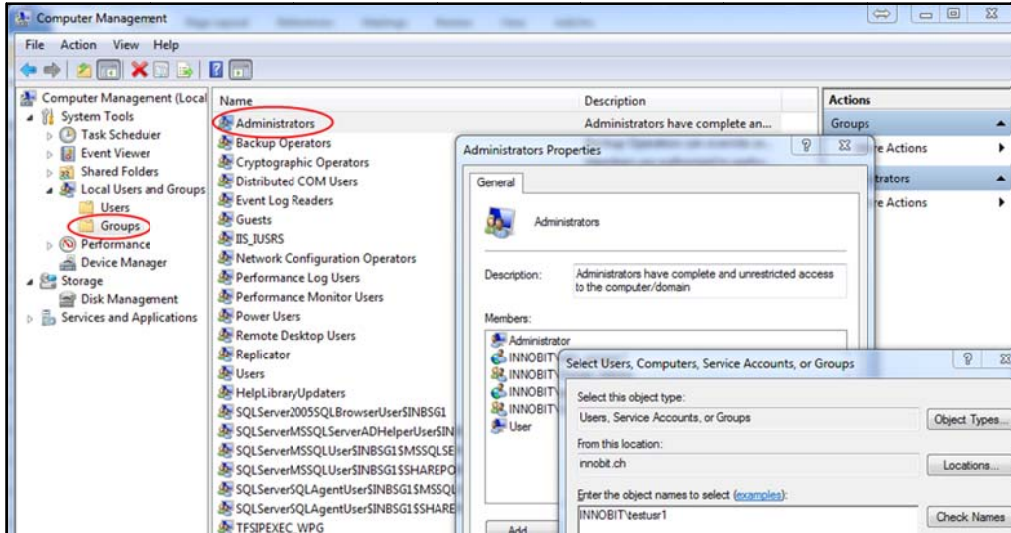
"SharePoint_Shell_Access"- will give the account special access on all databases. The account will also be added on the local Group "WSS_Admin_WPG" in the SharePoint-Server. Therefore the following command must be executed in the "SharePoint 2010 Management Shell":

```
ForEach ($db in Get-SPDatabase) {Add-SPShellAdmin -Username <User account> -Database $db}
```



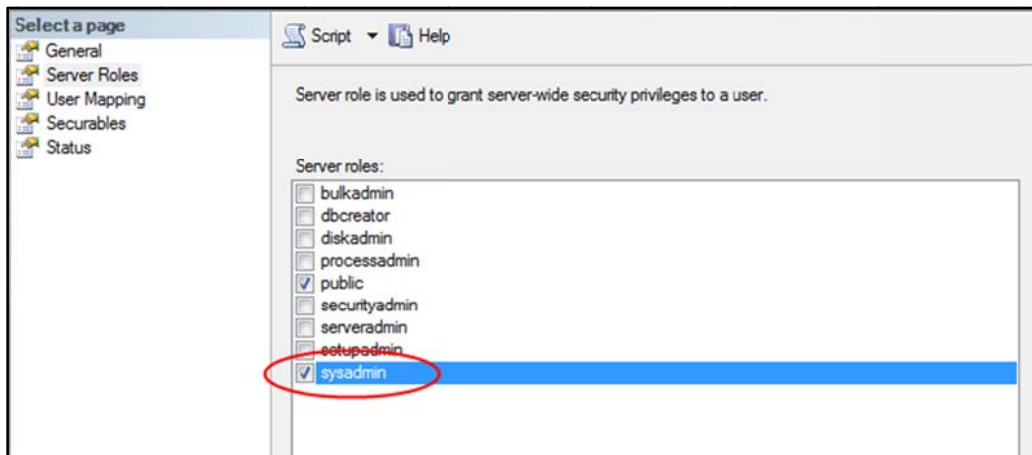
- Local Administrator

Eventually you will need to add the Scan Account on all SharePoint –Servers in the local Administrators group.



- Database Server System Administrator

Some special cases may require that the Scan Account on the Database-server is Administer entitled.



- Web Application Policy – Full Control

Until now the 8MAN SharePoint Connector was only able to read unrequired permissions. After expansion of the connector to manage permissions, it may be needed eventually.

For this reason Section 3.2 Performs with "Full Control" instead of the usual "Full Read".

SharePoint – Resource-View

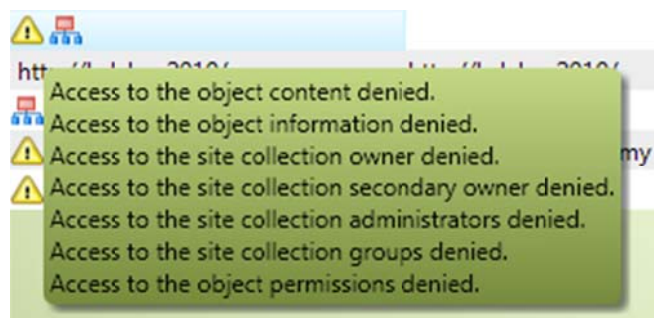
8MAN’s Resource-View for SharePoint Functionality has been extended. This is based upon the well-known File Server representation.

Resources			
	full path	Description	Rig
+ File server			
- SharePoint			
+ B-TEST12			
- B-LABSP2010			
http://b-labsp2010:42095/	http://b-labsp2010:42095/	Default: http://b-labsp2...	
+ Root Site Collection	http://b-labsp2010:42095		
! Root Site Collection			
http://b-labsp2010/	http://b-labsp2010/	Default: http://b-labsp2...	
+ Homepage	http://b-labsp2010		
! Homepage			
! Meine Website	http://b-labsp2010/my		
! Meine Website			

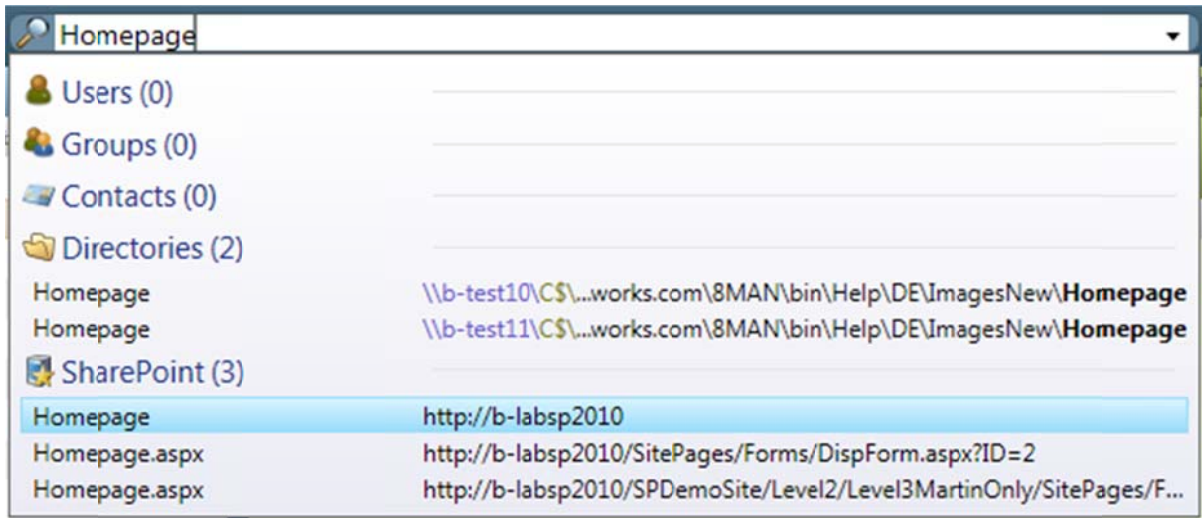
Briefly Summarised:

- The tree breaks down the different levels from (Farm → Web Site → Web Site Compilation → Element). In contrast to the file server, data is loaded to the last level - a distinction between directories and files in SharePoint do not exist.
- The green exclamation mark indicates a lost inheritance. The authorisation layer can thereby change this permission, however it must not necessarily.
- The green arrow indicates an inheritance broken below the selected element.

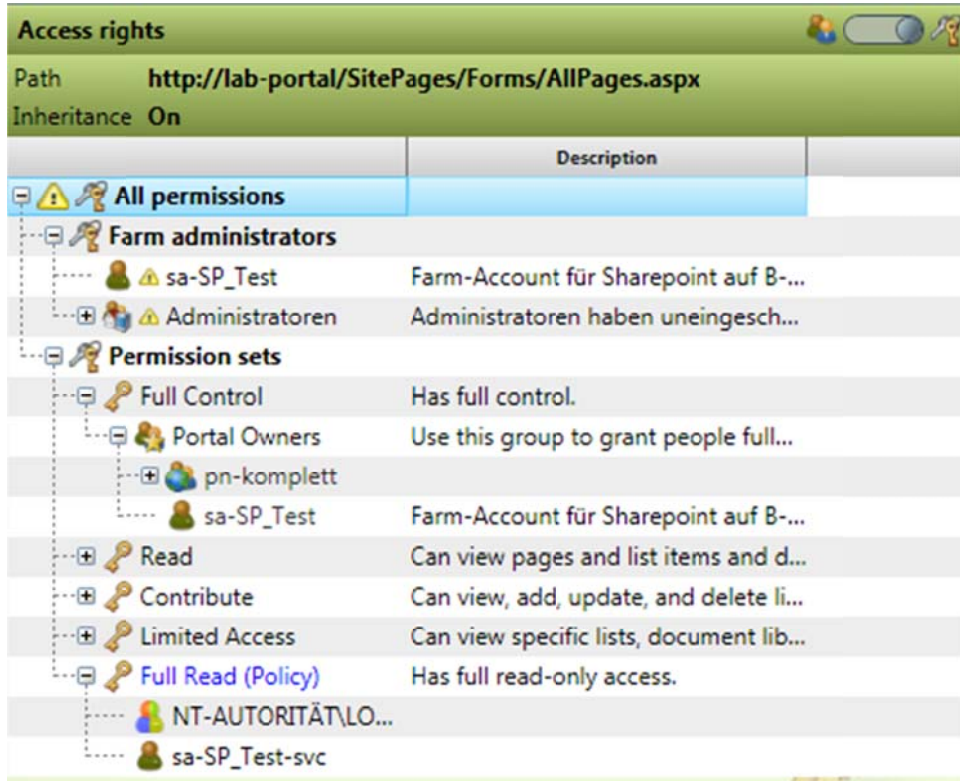
The yellow exclamation point indicates that data is read from the SharePoint specific information could not be read. This can also affect properties such as the object name.



Looking for a specific SharePoint item? You can use 8MAN’s search function to quickly find SharePoint elements.



When you choose the resource view, a SharePoint item's corresponding authorisation information is displayed on the right side. It should be noted that the authorisation concept has been greatly changed in comparison to the File Server representation and therefore has some specific differences.

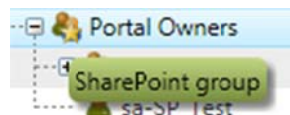


In SharePoint, there are several levels of permissions that define the access rights.

Existing authorisation levels:

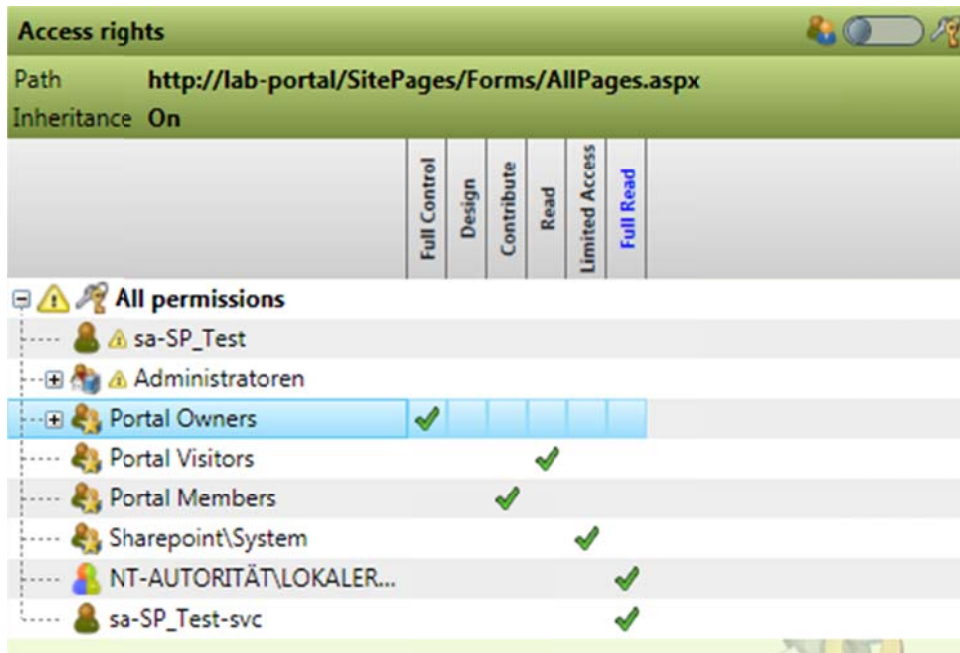
- Farm Administrators - these users have no access to the selected element, but can at any time allow themselves, a user or group access and then remove it.
- Site Collection Administrators - these users have access to all elements of the corresponding site collection no matter what level.
- Policies (in blue) - Policies can be set individually for each Web application and apply to all elements below it.
- Policy level - policy levels can be set individually for each site and are the primary authorisation means.

Besides the familiar Active Directory groups in SharePoint additional groups are also present. These groups are marked with an asterisk. SharePoint groups can contain Active Directory groups and users.



A yellow exclamation mark is also present, when any of the SharePoint information could not be read or if the information is incomplete.

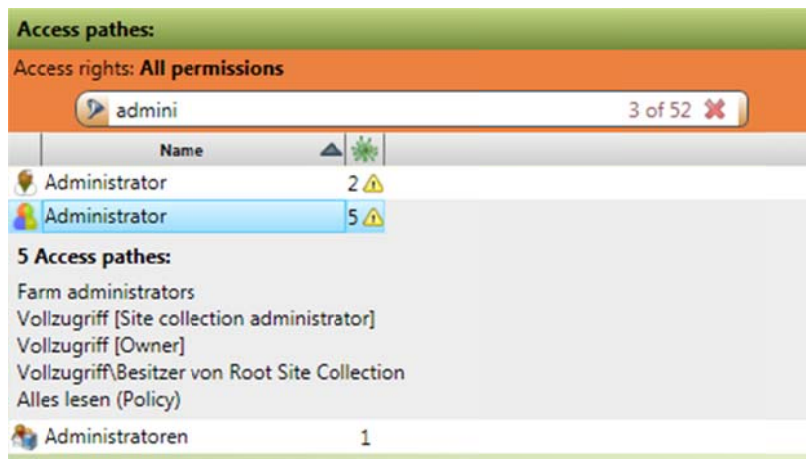
In addition to the illustration in permissions categories can also be a represented by authorised users or groups. Please press the Slider-button on the top right.



The columns correspond to the levels of policy and guidelines, which lines the legitimate users or groups. If a user or group is fitted with additional rights, (i.e. owner or site collection administrator) it is highlighted.

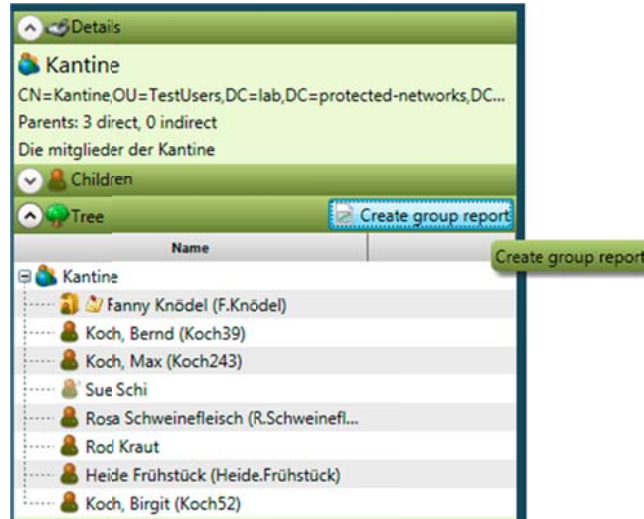


If you want to know who actually has access to a particular element, then you can get this information from the display on the bottom right. As usual, you can filter and view the various permission paths.



Group Reports

In the Active Directory view as well as in the multiple selections, you can create a report for either a selected group or several groups these reports contain information about any group and its members.



Just click the button in the children-tree-view on the right side. The report is launched automatically. After successfully creating the report, it is then displayed in 8MAN's status bar that a new report is available.



Click on this icon to open the report overview. The last generated report will be listed. The report itself contains a summary of group characteristics, the second part contains a list of members. It is distinguished by groups, users and disabled users:

- User ⚠ Lock, John
- Deactivated User ⚠ (Deactivated) J. Lock
- Group 🏠 Site

protected-networks.com 8MAN Report - Group members report
12/12/2011 1:41:03 PM
pn/w.wagner
Page 1

Report Configuration

Selected groups
Kantine

Scan time
Active Directory Scan LAB.PROTECTED-NETWORKS.LOCAL (12/11/2011 10:00:05 PM)

Groups - Properties

Kantine

Name	Kantine
Direct members	8
Group Type	Global group
Description	Die mitglieder der Kantine

Groups - Members

Kantine Direct members: 8, Indirect members: 0

<ul style="list-style-type: none"> ⚠ (deactivated) F.Knödel ⚠ Heide Frühstück ⚠ Koch, Bernd ⚠ Koch, Birgit 	<ul style="list-style-type: none"> ⚠ Koch, Max ⚠ R.Schweinefleisch ⚠ Rod Kraut ⚠ (deactivated) Sue Schi
--	---

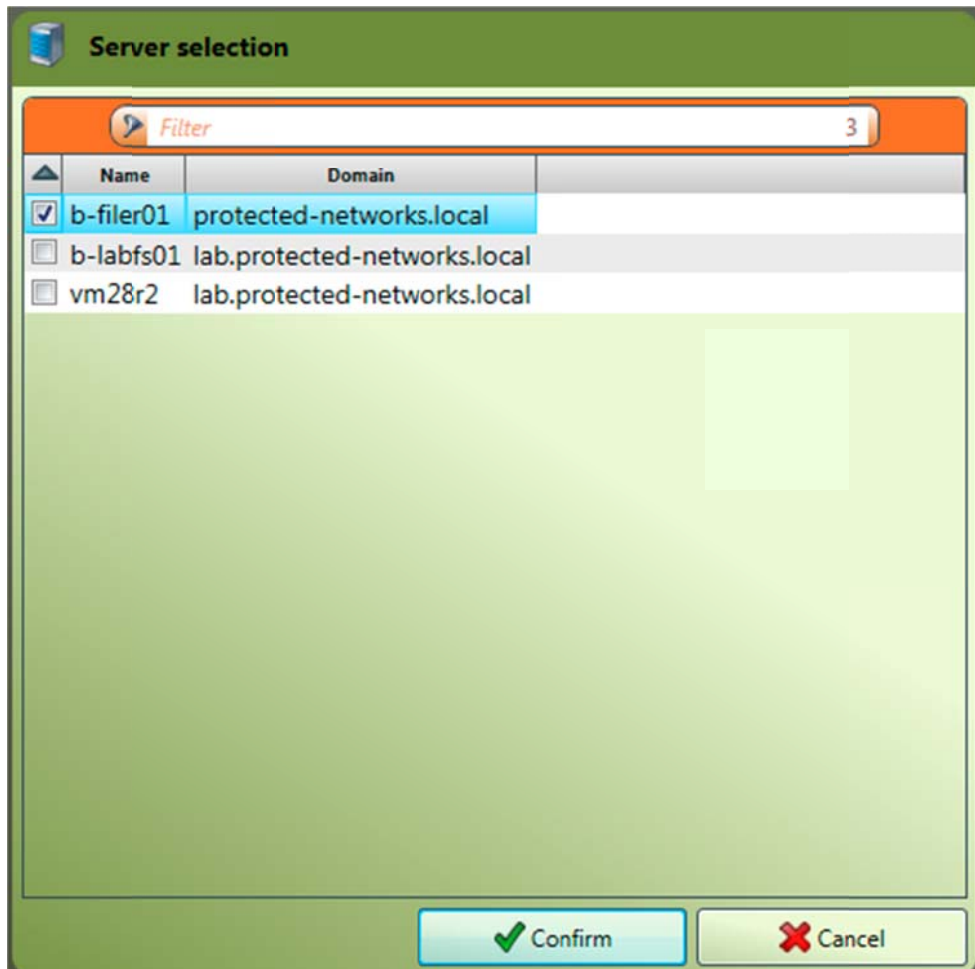
File Server Selection to Limit the Amount of Data

The 8MAN now offers the ability to filter the amount of File Servers to scan. This feature can improve the clarity, only by carefully selecting the file servers that are of interest to you.

The function can be accessed via the icon next to the domain selection.



It will open the following dialog window:



Select the desired file server. The selection will be stored for your user account and applies even after a reboot of 8MAN.

When a custom selection is made the icon changes:



Global Search with Logical Filter

The Smart Scan does not show the number of matches found, unless the complete list of results is completely visible. But every result that is found in the database is immediately displayed in the GUI. The search is also much quicker and creates less strain on the SQL server.

The intelligent search has been further enhanced by the addition of extra functionality:

- It is possible to browse a SharePoint server.
- The Sharepoint and Active Directory search is a full text search.
- The intelligent search no longer pays attention to accent marks.
- If only one keyword is specified, only the directory is searched. Thus in the search word "temp" only "C: \ temp \" is found, and not "C: \ Temp \ texts \". If there is more than one search word, then the search becomes a full text search.
- For separate words with spaces, searches will be conducted for both words.
- Any case with a "-" should be at the beginning of a word, and cannot be followed by a "."
- A "" " packaged strings are interpreted as a search word.

Active Directory - Soft-Delete & User Recovery

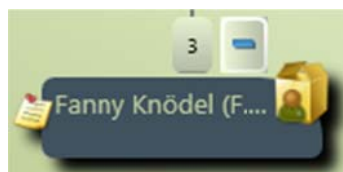
"soft delete" means the simultaneous deactivation and move a selected user in a so-called trash-OU. You can set the domain configuration under 8MAN scan, a trash-to OE.

This OU is used to store trash from disabled users of their Active Directories.

Soft-Delete

After you have configured an 8MAN OU domain in which you want to move the "soft Deleted" user to, you can now put users into the OU-paper basket.

This feature is available in the Active Directory style by selecting a user in the Graph view. In Soft Delete this user is first disabled and then moved into the previously set trash OU. His original OU is secured. The user is then shown as a "box" representing his/her Soft-Delete state.



The group memberships of users in "soft delete" folders are not deleted.

Restore

Here previously "soft deleted" users can be restored back to their original states.

Active Directory View – Selection History

From version 4.0 it is possible move back or forward between the selected users or groups within Active Directory. This selection history is remembered and you can select it with the forward-backwards buttons which refer to following or previous Active Directory objects.



The history of all previously selected objects will be saved when you exit this view and are restored when you open the view again. The settings are only valid for the duration of the logged on 8MAN client user.

Create Users and Groups - Extensions

With Group Creation, you can now explicitly specify the SAM account name. This makes it possible to create multiple groups with the same CN in Active Directory (for example if they are in different organisational units). The only requirement is that the SAM account name must be unique.

The SAM account name is set automatically preset with the name (CN) and can be changed manually if this already exists in the following example:

Create new user or new group in the Active Directory
 Create elements in the selected domain **LAB.PROTECTED-NETWORKS.LOCAL**

Status of changes: **Please configure properties for the new user**

Active Directory change credentials [pnlab\neadmin](#)

Create new user | **Create new group**

Given Name: Surname:
 Common Name:
 SAM Account Name: Naming rule:
 Description:
 OU Selection: [OU=TestUsers](#)

Optional LDAP Attributes

Password Options

User Activation

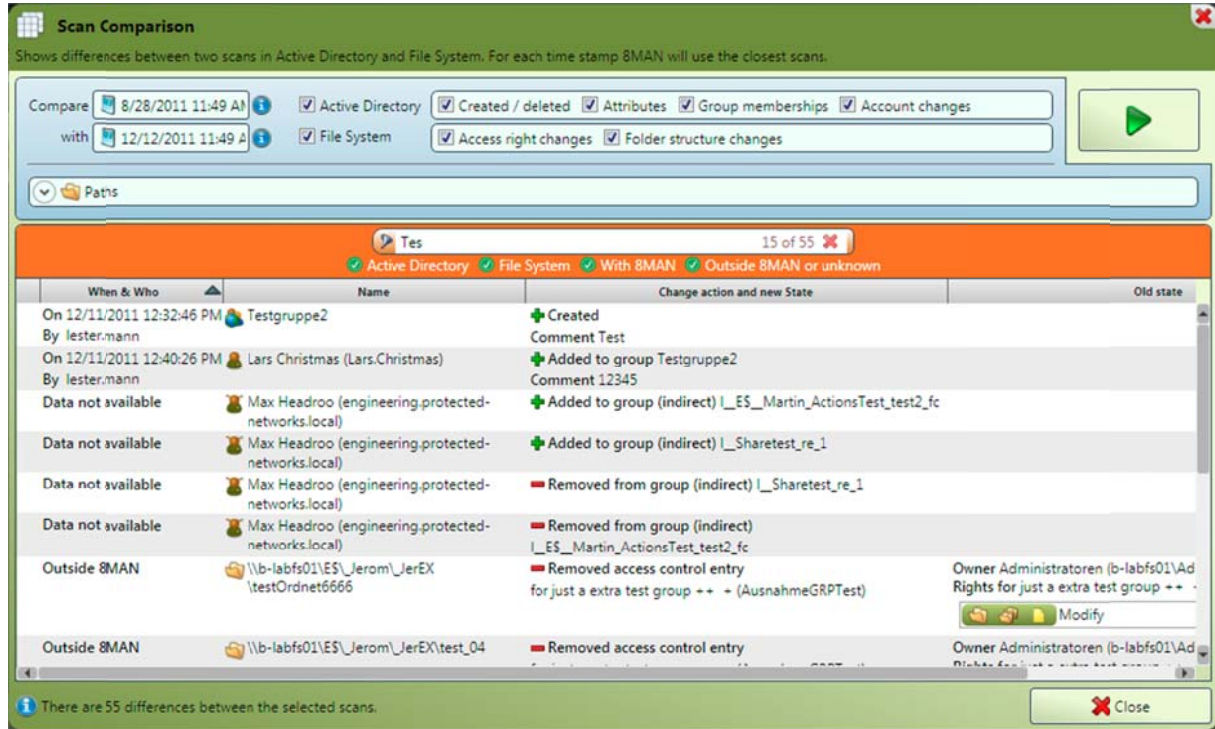
- Activate immediately
- Do not activate
- Activate on [12/14/2011 2:00:00 PM](#)

Please add a comment here:

Create | **Cancel**

Scan Comparison - Extensions

The scan will now compare old and new sates side by side on the table, without a detailed view. A line must be selected in order to reveal more information



The information about the date and the time and the author of a change is now displayed again in the first row, if it is available. The message "Outside of 8MAN" means that the corresponding change was definitely not made or documented with 8MAN. Also "Data not Available" can also appear. This is always the case if need be used to determine time and author of additional log tables, but these are not available. In this case, it cannot be clearly determined whether the changes have arisen implicitly by an 8MAN action or from an external source. "Data not available" can also appear in these circumstances. This additional data is available only for scans that were created from 8MAN version 4.0.101 with the option "supportOriginalScanData" activated (see below).

Pnserver.config.xml with the following settings in the, the accuracy can be improved with such Author information:

Since the scanning is done on the basis of comparison in the database of existing data and changes made by 8MAN, any changes are always shown on the last scan. This may in some cases lead to changes this are not recognised as 8MAN changes (see release notes for version 3.5.55 from 08/04/2011)

This discrepancy can be avoided if changes are made in the pnserver.config.xml with the following settings:

```
<scanCompare>
  <supportOriginalScanData type="System.Boolean">true</supportOriginalScanData>
  <performDirectlyAfterScan type="System.Boolean">>false</performDirectlyAfterScan>
</scanCompare>
```

The first entry "SupportOriginalScanData" ensures that 8MAN creates copies of scanned images in the database. This ensures that the described deviation no longer occurs in the scan data of the comparison period. The second "performDirectlyAfterScan" entry sets the date in which the copy is made - either directly after the scan, or until

the first or subsequent changes. For performance reasons, the default for both is "false".

Set "supportOriginalScanData" to "true" if you want to use more accurate author information. Set "performDirectlyAfterScan" to "true" if you need make a lot of changes (Changes should occur in only some of the created copies).

If you only make a few changes using 8MAN, you can however change the setting to "false" if you want to leave the settings as before.

In the current version the following restrictions are observed

Because the file server has different types of rights, (standard and specific rights) in some cases, comments cannot be assigned to the corresponding ACE entry.

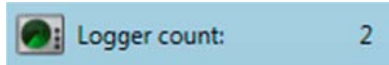


In addition, two or more ACE's can correspond to a single entry. Nevertheless, they are shown as a change in authorization management.

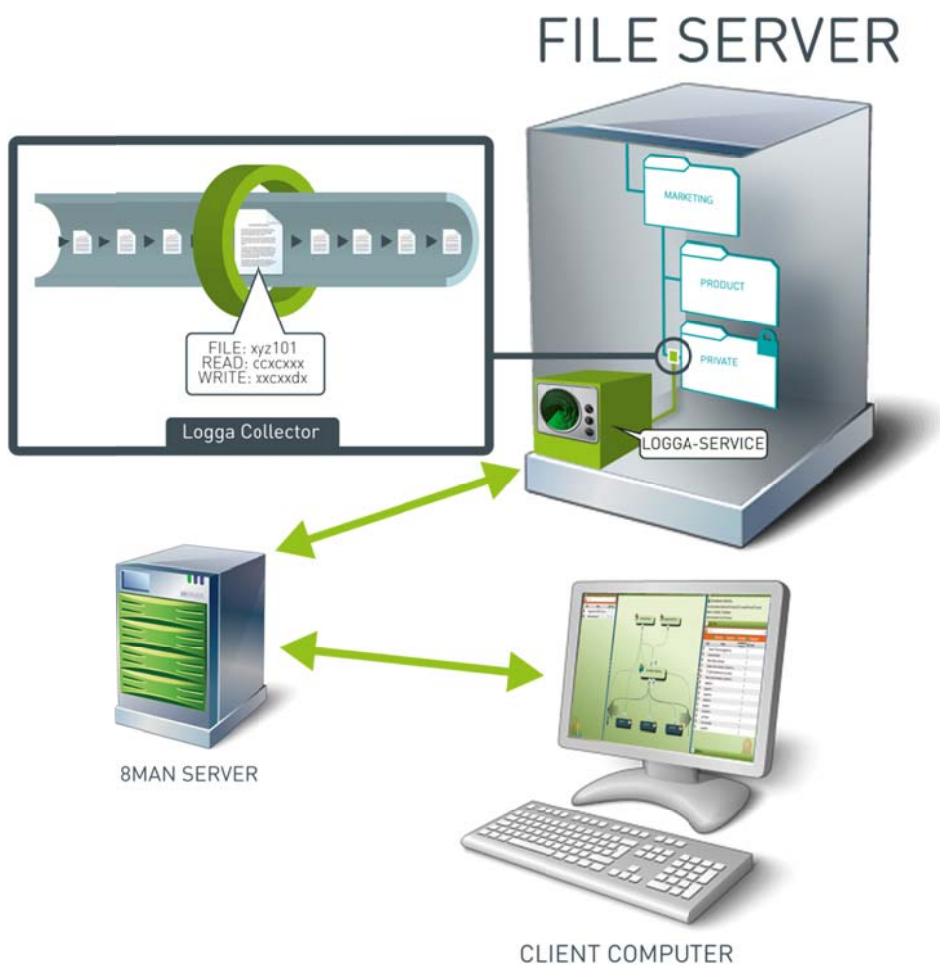
When forced access rights are consequently deleted or when groups are changed and their respective memberships within are also changed, these will be displayed as "Outside of 8MAN"

Logga - File Server Monitoring (Beta-Version)

With 8MAN you can now configure File Server to monitor file operations. This requires a valid license for the use of Logga functionality. To do this - go to the 8MAN configuration under server status in the license-information-list. The number of "loggas" describes how many servers you can configure 8MAN with Logga. The number of reports that can be generated however is not restricted.



The 8MAN Logga is approximately equivalent to a file server 8MAN collector with expanded functionality for monitoring. The 8MAN Logga is installed first on a file server as an 8MAN Logga collector.



Logga file server installed on the 8MAN server

The setup program does support the installation of a collector on the 8MAN Logga server, but it is strongly discouraged due to performance reasons. The damage can lead to instability of the 8MAN server or the entire system.

Please note the changed system requirements!

The following file actions are recorded by; file action, time and the user who made the change.

```
File Read
File Write
File Generated
File Moved
File Access Denied
ACL Changed
ACL Read (Turned off by Default)
```

The recorded data is automatically transferred to the 8MAN database on the 8MAN server. These data reports can be used as needed but will be rescinded after a period of up to 30 days. If you want to change this time period, then you need to change the entry for "maximumDataAgeDays" in the pnServer.config.xml file on the 8MAN server:

```
<config>
..
  <tracer>
    <db>
      <cleanUp>
        <maximumDataAgeDays type="System.Int32">30</maximumDataAgeDays>
      </cleanUp>
    </db>
  ..
```

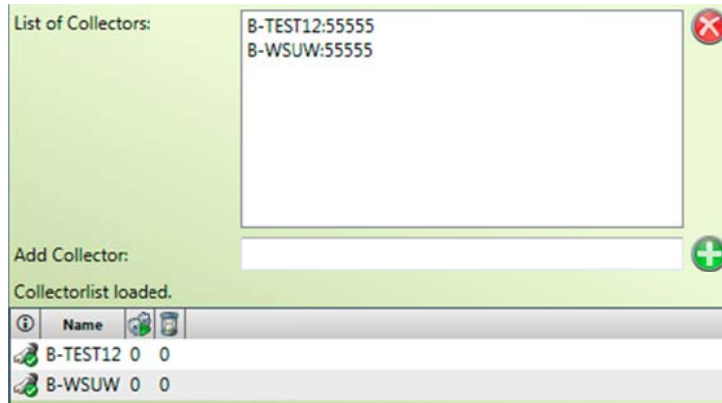
Restriction on the Amount of Data Recorded

You can reduce the amount of data by restricting the actions recorded file, on the file actions you need for your reports. To do this go to the configuration file on the installed **pnCollector.config.xml** Logga file server. Under **ThValSect** all file actions, which contain a **true** are recorded by the Logga-File Server.

```
<tracer>
  <windows>
    <SysInfo>
    <ThValSect>
  ...
    <read type="System.Boolean">true</read>
    <readwrite type="System.Boolean">true</readwrite>
    <create type="System.Boolean">true</create>
    <move type="System.Boolean">true</move>
    <aclwrite type="System.Boolean">true</aclwrite>
  ...
```

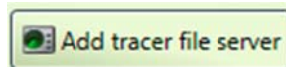
Configuration

In the 8MAN configuration first step the Logga-Collectors are connected to the 8MAN system. These then connect to the previously installed Logga file server in the list of 8MAN collectors.



The default port is 55555 and must be stated separately. The collector-status must be marked in the green list so that the server recognizes the remote 8MAN Logga-collector and can be used for the subsequent configuration. Please also note that the Logga functionality must be turned on via User Management. The Logga is available only to the 8MAN Administrators role.

In the configuration panel, you can now add a scan by clicking the Logga configuration button:



After selecting a file server, a new entry in the 8MAN scan list is created:

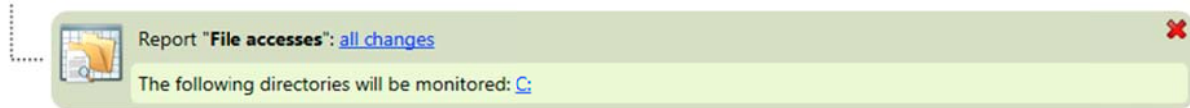


The configuration consists mainly of selecting the file server with the awarded names and a list of Report-Configurations. File Servers which can monitor 3 different report types are available. Each report types are configurable in any number of reports. The selection of the monitored directories is made with Report-Configuration. The reports can normally only be created and saved in 8MAN.

Once Report-Configuration is created with one or more directories, the Logga-File Server begins with recording the actions file. Deleting all report configurations ensures the continuation of data recording.

Report-Types

File Requests



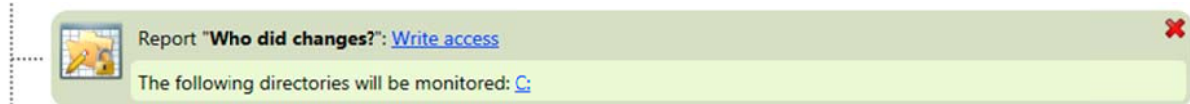
It records all changes to the configured directories. These can then be listed in a later report.

An unauthorised access has taken place - Segregation of Duty (SoD)



It will record all changes to the configured directories, which were executed by users who do not belong to your selected users or user groups. Selection of allowed users and groups takes place later in the report generation, but not within this configuration.

Where changes have occurred?



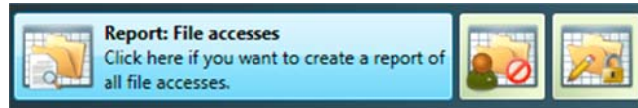
Here you can select directories in the Logga-File Server in order to create a report later in which only file write requests are listed.

Reference

An adjustment in the configuration directory may not be limited to subdirectories in the reporting. If you are in the directory selection, entire drives (i.e. C:) or root directories, then the report can only be for the entire device respectively. The selected directory and all subdirectories will be created.

Logga – Access Reports

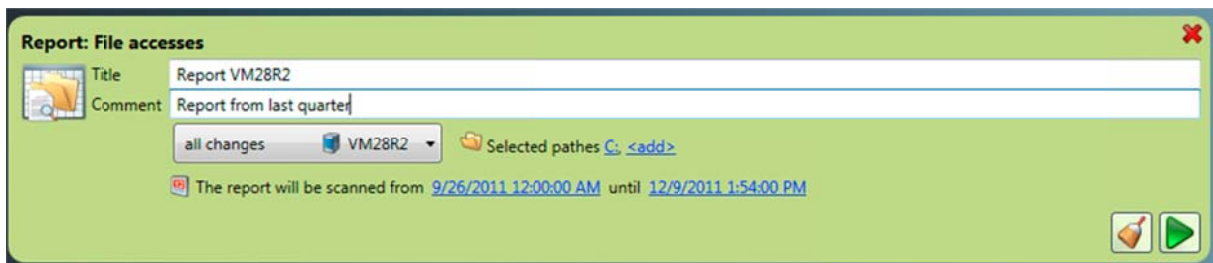
On the home page of 8MAN you get a selection of all previously configured Logga report types available. If you have configured, for example, only SoD reports, then you only the button to create SoD Reports is available.



Reference

The integration of local accounts into the Logga-File Server can only be done properly with a previous 8MAN file servers scan. If this were not done, there is an indication in the reports and the accounts are with their security identifier (SID) listed in the report.

After choosing a report type on the homepage, the Report dialog box opens:



You can download the recording period for the report to further restrict or deselect the previously selected directories. The report generated can then be stored as usual, or sent via email. Below you can see an example of SoD.

protected-networks.com
8MAN Tracer Report - File accesses
12/13/2011 3:18:59 PM
pn\u.wagner
Page 1

Report Configuration

Monitored file server
VM28R2ST

Configured folders to check
D:\testing

Collect data between times
Start time: 12/6/2011 11:11:28 AM
End time: 12/13/2011 2:15:02 PM

Monitored file actions in folder D:\testing

	Statistics	
ICSHarpCode.SharpZipLib.dll	D:\testing\Server\Debug\ICSharpCode.SharpZipLib.dll 9 x Read	
12/13/2011 12:35:24 PM	NT AUTHORITY\SYSTEM	Read
12/13/2011 12:35:24 PM	NT AUTHORITY\SYSTEM	Read
12/13/2011 12:35:24 PM	NT AUTHORITY\SYSTEM	Read
12/13/2011 12:35:24 PM	NT AUTHORITY\SYSTEM	Read
12/13/2011 12:35:24 PM	NT AUTHORITY\SYSTEM	Read
12/13/2011 12:35:24 PM	NT AUTHORITY\SYSTEM	Read

All file operations are grouped per file. There is also a list of statistics for each file access (number of different file actions). The latest file actions are displayed in the list first.