



## **8MATE FS Logga Manual**

Version 8.0

## Liability Notice

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.

Trademarks and brands – with or without explicit display – are the intellectual property of the respective brand owners.

Protected Networks GmbH  
Alt-Moabit 73  
10555 Berlin

+49 30 390 63 45 - 0

[www.protected-networks.com](http://www.protected-networks.com)

## Support

+49 30 390 63 45 – 99  
[helpdesk@8man.com](mailto:helpdesk@8man.com)  
<https://susi.8man.com>

8MATE FS Logga – Monitoring of file servers .....	4
1 Installation and Configuration of Collectors.....	5
<b>1.1 FS Logga for Windows File Server</b> .....	5
1.2 FS Logga for NetApp File Server .....	6
1.3 FS Logga für EMC-Fileserver .....	8
2 Configure File Servers to be monitored .....	9
2.1 Windows File Server .....	9
2.2 NetApp File Server .....	9
2.3 EMC File Server .....	14
3 FS Logga Configuration .....	17
3.1 Select file server and collector .....	17
3.2 Monitored actions and data refresh interval .....	20
3.3 NetApp Clustered Data ONTAP Configuration.....	21
3.4 Select a name and the directories to be monitored for the FS Logga report types .....	22
3.5 Report types .....	23
3.6 Activating / Deactivating FS Logga.....	24
3.7 FS Logga settings in the pnTracer.config.xml file .....	25
4 Create FS Logga reports .....	27
4.1 Report types “Who did what”, “Who made changes”, “Who did what, what except authorized users [SoD]” .....	28
4.2 Report “FS Logga access rights change history” .....	30
Appendix .....	32
Appendix I: Troubleshooting .....	32
Appendix II: Software license acknowledgements .....	33

## 8MATE FS Logga – Monitoring of file servers

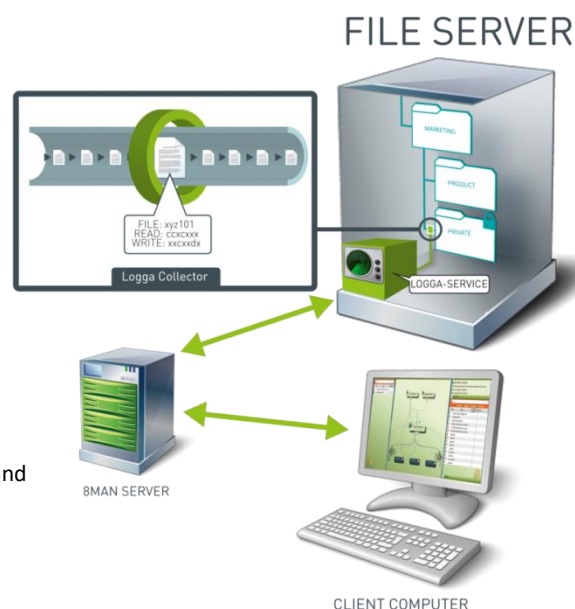
With the FS Logga you can monitor directory and file operations on Windows, NetApp and EMC file servers.

(Not all operating systems and product versions are supported. The restriction you can find in the document “8MAN System Requirements”).

The following operations can be recorded with time stamp, type of operation and user who did the operation:

- File read
- File written
- Directory or file created
- Directory or file deleted
- Directory or file moved or renamed
- ACL changed
- ACL read (switched off by default [activation in the **pnTracer.config.xml** file possible] and not available for NetApp and EMC file servers)

The recorded data are stored in the database of the 8MAN Server and can be displayed in reports in the CSV or XPS format.



# 1 Installation and Configuration of Collectors

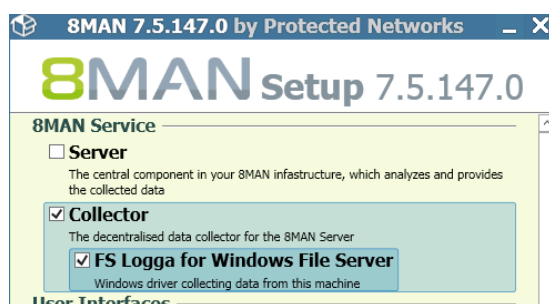
For the FS Logga you need to install collectors. Collectors-for-the-FS-Logga-for-Windows-file-server have additional restrictions. Please check the document 8MAN System Requirements before installing collectors-for-the-FS-Logga-for-Windows-file-server.

Note:

For reasons of performance and stability the FS Logga is not working on the 8MAN Server. (The setup program does not prohibit the installation of a collector for the FS Logga on the 8MAN Server, but the FS Logga will not start on the 8MAN Server.)

## 1.1 FS Logga for Windows File Server

The collector for the FS Logga for Windows File Server needs to be installed on the monitored file server. Therefore you have to select the FS Logga for Windows File Server in the installation process:



When the collector was installed without the FS Logga for Windows File Server and later on you install the the FS Logga for Windows File Server, the 8MAN service on the collector must be restarted.

If Windows Failover Cluster resources should be monitored, then you have to install the collector with the FS Logga for Windows File Server on each node of the cluster.

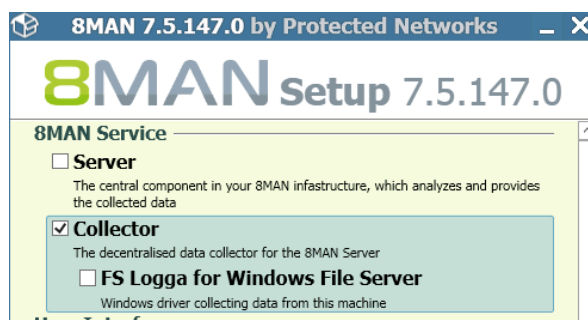
Hardware maintenance:

During a change of hard drives or administration of mount points of the monitored hard drive areas the FS-Logga-for-Windows-file-server has to be switched off (ON/OFF button in the 8MAN scan configuration).

## 1.2 FS Logga for NetApp File Server

The collector for the FS Logga for NetApp File Server can't be installed on the monitored NetApp file server. It has to be installed on a Windows file server. NetApp strongly recommends using a server within the same network segment, because otherwise there may be performance and routing problems.

The FS Logga for NetApp file server needs no driver (Opposite: the FS Logga for Windows File server needs a driver). Therefore you only need to install an 8MAN Collector (If there is already an installed 8MAN Collector or collector for the FS Logga for Windows File Server, then the collector for the FS Logga for NetApp File Server is also installed):



When a NetApp file server is registered in the Active Directory, one of the stored properties is the operating system. This property is used by the collector to detect NetApp file servers and mark it as NetApp file server type in the Logga configuration. By default the operating systems of NetApp file servers are set to "OnTap" and "NetApp" in the collectors configuration file. If your NetApp file servers use other values for the property "operatingSystem", you can adapt the search parameters. Open on the file server where the collector is installed the file **pnCollector.config.xml** under C:\ProgramData\protected-networks.com\8MAN\cfg (if it does not exist, copy it from C:\Program Files\protected-networks.com\8MAN\etc, clear the content and insert the following lines):

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <netapp>
      <NetappOperatingSystems>OnTap,NetApp</NetappOperatingSystems>
    </netapp>
  </tracer>
</config>
```

If your NetApp file servers have different values for the property "operatingSystem" then insert all these values separated by comma. If no or not all NetApp file servers register the property "operatingSystem" in the Active Directory leave the entry empty in the collectors configuration file:

```
(<NetappOperatingSystems></NetappOperatingSystems>).
```

With an empty entry you will get all computers visible for the used account.

### 1.2.1 NetApp 7-Mode

There are policy administrations on the collector computer necessary to enable communication between NetApp and the collector. The following Local Security Policies on the computer, where the collector for the FS Logga for NetApp 7-Mode File Server is running are necessary (under Local Policies\Security Options):

Security Option	Value
Network access: Let Everyone permissions apply to anonymous users	Activated
Network access: Named Pipes that can be accessed anonymously	ntapfprq_<netapp name> (<netapp name> is the name of the NetApp file server)

**Hint:**

For an 8MAN-collector only one 7-Mode NetApp can be configured. Each 7-Mode NetApp needs its own collector.

## 1.2.2 NetApp Clustered Data ONTAP

No additional configurations necessary for the collector running the FS Logga for NetApp Clustered Data ONTAP if data transfer from NetApp to collector should be done without encryption.

If you have configured encrypted data transfer (see chapter 2.2.2.1.2 “Creating the External Engine Configuration”) you also have to adapt the pnTracer.config.xml file on the collector server. For each file server (CIFS server on the NetApp) to be monitored on this collector, the following entry have to be added under <tracer><netapp><ssl><cifsServers>:

**<name of cifs server>**

<switchOn type="System.Boolean">**true**</switchOn>

<protocol type="System.Int32">5</protocol>

<serverCertificateName>**name of certificate from certificate store to use**</serverCertificateName>

**</name of cifs server>**

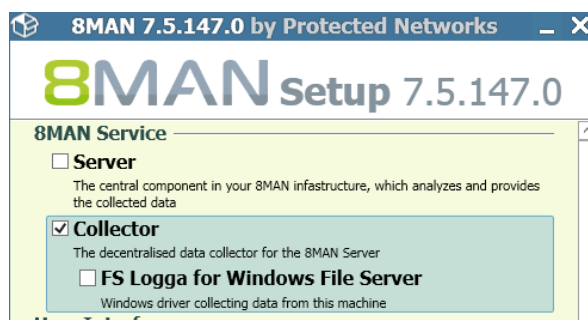
The certificate must be installed in the computers certificate store.

For <protocol> the following values are possible: TLS = 1, TLS1.1 = 2, TLS1.2 = 3, SSL2 = 4, SSL3 = 5. Default is SSL3 (5). Choose a protocol available on both collector and NetApp.

## 1.3 FS Logga für EMC-Fileserver

The collector for the FS Logga for EMC File Server can't be installed on the file server to be monitored. It has to be installed on a Windows server, preferably on the server where the EMC Common Event Enabler (CEE) is installed (for CEE see chapter 2.3.1). EMC strongly recommends using a server within the same network segment, because otherwise there may be performance and routing problems.

The FS Logga for EMC file server does not need drivers or agents on the EMC file server. You only need to install an 8MAN collector:



When an EMC file server is registered in the Active Directory, one of the stored properties is the operating system. This property is used by the collector to detect EMC file servers and mark it as EMC file server type in the Logga configuration. By default two types of operating systems of EMC file servers are set in the collectors configuration file: "EMC File Server" and "EMC Celerra File Server". If your EMC file servers use other values for the property "operatingSystem", you can adapt the search parameters. Open on the file server where the collector is installed the file **pnCollector.config.xml** under C:\ProgramData\protected-networks.com\8MAN\cfg (if it does not exist, copy it from C:\Program Files\protected-networks.com\8MAN\etc, clear the content and insert the following lines):

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <emc>
      <EmcOperatingSystems>EMC File Server,EMC Celerra File Server</EmcOperatingSystems>
    </emc>
  </tracer>
</config>
```

If your EMC file servers have different values for the property "operatingSystem" then insert all these values separated by comma. If no or not all EMC file servers register the property "operatingSystem" in the Active Directory leave the entry empty in the collectors configuration file:

```
(<EmcOperatingSystems></EmcOperatingSystems>).
```

With an empty entry you will get all computers visible for the used account.



## 2 Configure File Servers to be monitored

### 2.1 Windows File Server

No additional configuration necessary.

### 2.2 NetApp File Server

Beside the configuration of the 8MAN collector also on the file server to be monitored special configurations are necessary to enable remote monitoring.

#### 2.2.1 NetApp 7-Mode

##### 2.2.1.1 FPolicy Feature

The FS-Logga for NetApp file server uses the NetApp FPolicy feature. Therefore it has to be activated and properly configured.

Activation of the FPolicy feature:

```
> options fpolicy.enable on
```

Configuration of the FPolicy:

```
> fpolicy create 8ManLogga screen
> fpolicy enable 8ManLogga
> fpolicy options 8ManLogga cifs_setattr on
```

The value "8ManLogga" of the FPolicy has to match with the value in the configuration file **pnTracer.config.xml** on the computer with the installed collector-for-the-FS-Logga-for-NetApp-file-server (C:\Programme \protected-networks.com\8MAN\etc). "8ManLogga" is the default after the installation.

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <netapp>
      <policy>8ManLogga</policy>
    </netapp>
  </tracer>
</config>
```

### 2.2.1.2 Domain-Accounts

For registration of the collector-for-the-FS-Logga-for-NetApp-file-server on the NetApp file server the collector needs to belong to an account that is a member of the group "Backup Operators" of the NetApp Fileserver. Because the collector belongs to the computer account of the file server it is installed on, this account needs to be added to this NetApp group:

```
>useradmin domainuser add <domain\computer-account> -g "Backup Operators"
```

To be able to read the complete paths of the shares an user account is needed, that is member of the "Power Users" group on the NetApp file server:

```
>useradmin domainuser add <domain\user> -g "Power Users"
```

## 2.2.2 NetApp Clusterd Data ONTAP

### 2.2.2.1 FPolicy Feature

The FS-Logga for NetApp file server uses the NetApp FPolicy feature. Therefore it has to be activated and properly configured via CLI.

To configure the Fpolicy feature you have to use an account of role admin or vsadmin on the NetApp.

In all following CLI commands the parameter "<vserver\_name>" has to be changed to the name of the SVM (Storage Virtual Machine) the CIFS-server to be monitored is configured on.

#### 2.2.2.1.1 Creating the Event Configuration

The Event Configuration determines which events will be monitored or not and the monitored protocol (only CIFS is supported by FS-Logga). Please do change only the parameter "<vserver\_name>". All other changes may lead to missing events in the reports or to higher load of collector and NetApp because of processing of not used events.

```
> fpolicy policy event create -vserver <vserver_name> -event-name event_8manlogga_cifs -file-operations create, create_dir, delete, delete_dir, read, write, rename, rename_dir, setattr, open -protocol cifs -filters first-read, first-write, open-with-delete-intent
```

With the following command you can check the result:

```
> fpolicy policy event show
```

#### 2.2.2.1.2 Creating the External Engine Configuration

The External Engine Configuration determines to which server (defined by ip address and port) the events has to be sent by the NetApp. The ip address has to be an address of the FS-Logga collector reachable by the NetApp. The used port must be a free port on the collector.

```
> fpolicy policy external-engine create -vserver <vserver_name> -engine-name engine_8manlogga -
primary-servers <collector-ip> -port 2002 -extern-engine-type asynchronous -ssl-option <ssl-option>
```

For <ssl-option> the values “no-auth” and “server-auth” are supported. If you want encrypted event data transfer between SVM and Logga then choose “server-auth”. In this case additional configurations necessary both on 8MAN collector and on NetApp (see chapter 0 and 2.2.2.4).

With the following command you can check the result:

```
> fpolicy policy external-engine show
```

### 2.2.2.1.3 Creating the FPolicy Configuration

The Fpolicy Configuration is the assembly of Event- and External Engine Configuration.

```
> fpolicy policy create -vserver <vserver_name> -policy-name 8manlogga -events event_8manlogga_cifs -
engine engine_8manlogga -is-mandatory false
```

With the following command you can check the result:

```
> fpolicy policy show
```

### 2.2.2.1.4 Creating the Scope for the Fpolicy

The Scope defines the volumes and hence the shares and their subdirectories and files for which events have to sent for to the FS-Logga. If only certain shares on certain volumes to be monitored, we recommend to use a comma separated list of volumes instead the wildcard (“\*”). This will reduce load for the NetApp and the FS-Logga collector machine.

```
> fpolicy policy scope create -vserver <vserver_name> -policy-name 8manlogga -volumes-to-include "*"
```

### 2.2.2.1.5 Enable Fpolicy

If all above steps were successful you have to enable the Fpolicy. (Even though only one Fpolicy is defined the system requires a sequence number.)

```
> fpolicy enable -vserver <vserver_name> -policy-name 8manlogga -sequence-number 1
```

With the following command you can check the result:

```
> fpolicy show-enabled
```

### 2.2.2.2 Domain Accounts

To read the shares local paths an account is needed which is member of the local group "Power Users" on the NetApp SVM (with this account the Logga should be configured).

```
> vsver cifs users-and-groups local-group add-members -vsver <vsver_name> -group-name
"BUILTIN\Power Users" -member-names <domain\user>
```

The Logga uses the ONTAP API to read Fpolicy data and request the NetApp to start Logging for the external engine. For this the Logga needs an account with restricted access rights on the NetApp. Therefore a new role should be created and the rights of this role will be defined.

In all following CLI commands the parameter „<vsver\_name>“ denotes the name of the SVM where the CIFS server is configured, which has to be monitor.

```
> security login role create -role 8manrole -vsver <vsver_name> -cmd "vsver fpolicy"
> security login role create -role 8manrole -vsver <vsver_name> -cmd "volume" -access readonly
> security login role create -role 8manrole -vsver <vsver_name> -cmd "vsver" -access readonly
> security login role create -role 8manrole -vsver <vsver_name> -cmd "version" -access readonly
```

With the following command you can check the result:

```
> security login role show
```

The account used by the Logga has to be assigned the new role:

```
> security login create -username <domain\username> -application ontapi -authmethod domain -role
8manrole -vsver <vsver_name>
```

With the following command you can check the result:

```
> security login show
```

### 2.2.2.3 Firewall configuration

The Logga uses the ONTAP API **via https** to read Fpolicy data and to request the NetApp to start Logging for the external engine. For this the service https must be configured on a LIF (Logical Interface) of the SVM. This LIF must be reachable by the 8MAN Collector where the Logga will be started.

Wich service is active on which SVM by which firewall policy you find with the following command:

```
> system service firewall policy show
```

Assignment of firewall policies to LIF of a certain SVM can be checked with:

```
> network interface show -vsver <vsver_name> -fields firewall-policy
```

If on a LIF of the SVM there is already a firewall policy active with the service https, then you need only to modify the 'allow-list':

```
> system services firewall policy modify -vserver <vserver_name> -policy <current_firewall_policy> -
service https -allow-list <collector-ip/32>
```

If there is a reason to not change the current firewall policy e.g. it is a default policy, then you can create a copy of this firewall policy, make the necessary change and then assign this new firewall policy to the appropriate LIF:

```
> system services firewall policy clone -vserver <vserver_name> -policy <current_firewall_policy> -
destination-policy 8manlogga_fp

> system services firewall policy modify -vserver <vserver_name> -policy 8manlogga_fp -service https
-allow-list <collector-ip/32>

> network interface modify -vserver <vserver_name> -lif <lif> -firewall-policy 8manlogga_fp
```

Where <collector-ip> is the ip-address of the External-Engine described in chapter 2.2.2.1.2 "Creating the External Engine Configuration"

#### 2.2.2.4 Certificate configuration for encrypted event data transfer

If you have configured encrypted event data transfer between NetApp and Logga (see 2.2.2.1.2 "Creating the External Engine Configuration") then the public certificate of certificate authority that is used to sign the 8MAN collector certificate (see chapter 0) has to be installed on the SVM:

```
> security certificate install -vserver <vserver_name> -type client-ca
```

With the following command you can check if the certificate was installed:

```
> security certificate show
```

## 2.3 EMC File Server

Configurations on the EMC file server and an additional EMC application, the “Common Event Enabler” (CEE) for Windows, is necessary to enable monitoring.

### 2.3.1 Common Event Enabler (CEE)

#### 2.3.1.1 Installation of the CEE

The collector installation needs another EMC® specific framework installation. This framework called “CEE” covers the communication between EMC Data Mover and EMC® CEE framework. The actual installation documents can be found in the EMC documentation center (<https://community.emc.com>).

#### 2.3.1.2 8MAN specific changes for the CEE

In order to have a performant connection between 8MAN collector and CEE both components should run on the same server.

The connection between collector and CEE framework client is controlled with Windows registry entries. Check registry section [HKEY\_LOCAL\_MACHINE\SOFTWARE\EMC\CEE\CEPP].

Create or change the following entries.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] Enabled=(REG\_DWORD) 0x00000001

[HKEY\_LOCAL\_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] EndPoint=(REG\_SZ) "pnTracer"

To apply these changes you need administrator rights. The new values will be active after restarting the CEE service. Use the graphical service management console or the command line call “net [start|stop] “emc cava””.

### 2.3.2 Configuration of the EMC®

The Common Event Enabler (CEE) (see 2.3.1) must be published to EMC®, enable EMC® to forward the events. We recommend to install and start the CEE before configuring the EMC®. This way you can check immediately if these components are connected.

#### 2.3.2.1 Creating and editing cepp.conf file

Create a file named cepp.conf with following content:

```
cifsserver=
surveytime=10
ft level=0
msrpcuser=<the account the CEE service is running under>
pool name=pool1 \
servers=<IP Adresse oder Hostname des Windows Servers auf dem der CEE Service läuft> \
postevents=* \
```

```
option=ignore \
reqtimeout=1000 \
retrytimeout=500
```

Copy this file to the root directory of the EMC® Data Mover:

```
$ server_file <movername> -put cepp.conf cepp.conf
```

### 2.3.2.2 Administer rights of the account of CEE service

For verification of the account the CEE service is running under, on the EMC® you have to administer the rights of this account accordingly.

Procedure according document on <https://www.emc.com/collateral/TechnicalDocument/docu48055.pdf>:

1. Click Start and select Settings > Control Panel > Administrative Tools > EMC VNX File CIFS Management. The EMC VNX File CIFS Management window appears.
2. Perform one of the following:
  - a. If a Data Mover is already selected (name appears after Data Mover Management), go to step 4.
  - b. If a Data Mover is not selected:
    - Right-click Data Mover Management and select Connect to Data Mover.
    - In the Select Data Mover dialog box, select a Data Mover by using one of the following methods:
      - i. In the Look in: list box, select the domain in which the Data Mover that you want to manage is located and select the Data Mover from the list.
      - Or
      - ii. In the Name box, type the computer name, IP address, or the NetBIOS name of the Data Mover.
3. Double-click Data Mover Management, and double-click Data Mover Security Settings.
4. Click User Rights Assignment. The assignable rights appear in the right pane.
5. Double-click EMC Event Notification Bypass. The Security Policy Setting dialog box appears.
6. Click Add. The Select Users or Groups dialog box appears.
7. If necessary, choose the server from the Look in drop-down list. Select the user from the list box.
8. Click Add, and then click OK to close the Select Users or Groups dialog box.
9. Click OK to close the Security Policy Setting dialog box.
10. In the User Rights Assignment list, double-click EMC Virus Checking. The Security Policy Setting dialog box appears.
11. Click Add. The Select Users or Groups window appears.
12. If necessary, choose the server from the Look in drop-down list. Select the user from the list box.
13. Click Add, and then click OK to close the Select Users or Groups dialog box.
14. Click OK to close the Security Policy Setting dialog box.
15. Close the EMC VNX File CIFS Management window.

### 2.3.2.3 Starting the Common Event Publishing Agent (CEPA)

The last step is starting and checking CEPA on EMC®.

- Start  

```
$ server_cepp <movername> -service -start
```

in which:

<movernam> = name of the Data Mover

result:

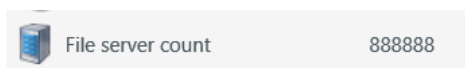
<movernam> : *done*

- Check CEPA status:  
`$ server_cepp <movernam> -service -status`  
 result:  
 <movernam>: *CEPP Started*
- Detailed info:  
`$ server_cepp <movernam> -pool -info`  
 Ergebnis:  
 <movernam>:  
*pool\_name = <pool name>*  
*server\_required = no*  
*access\_checks\_ignored = 0*  
*req\_timeout = 500 ms*  
*retry\_timeout = 50 ms*  
*pre\_events =*  
*post\_events = CreateFile, DeleteFile, RenameFile, FileRead ....*  
*post\_err\_events =*  
 CEPP Servers:  
*IP = <CEE IP>, state = **ONLINE**, vendor = Unknown*



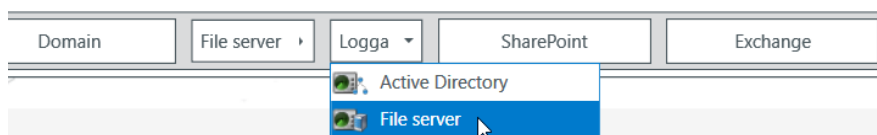
## 3 FS Logga Configuration

The FS Logga configuration is only available for 8MAN administrators. To configure the FS Logga you need a license. If a license exists you can check in the 8MAN configuration under Server status in the License Information area. The “File server Logga count” defines the number of file servers (Windows file server or NetApp file server or both) you can monitor:



### 3.1 Select file server and collector

In the 8MAN Configuration view “Scans” you click on “Logga → Fileserver” and the selection dialog for the file server and collector that should monitor opens:

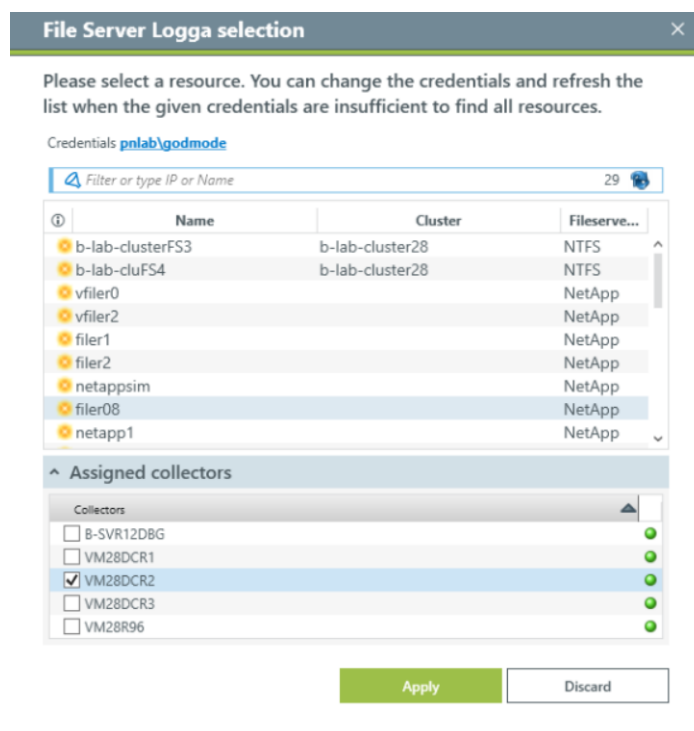


In the Logga selection dialog you can select the following:

- the credentials for the file server search (the default credentials for reading the Active Directory are taken from the Basic configuration)
- the file server to be monitored
- the collector that should monitor

#### 3.1.1 Windows file server, NetApp® and EMC®

Because the available NetApp and EMC file servers are read out of the Active Directory, you have to use an account that is allowed to read Active Directory. For the list of available Windows file servers the used account doesn't matter. It will be listed only these Windows file servers where the FS Logga for Windows File Server is installed and have an active connection to the 8MAN Server.



For Windows file servers you only can select the collector installed on this file server.

Because NetApp and EMC file servers are monitored remotely, depending on your installation, you can choose between different collectors. Per collector you can monitor more than one NetApp or EMC file server, an additional selection as FS Logga for Windows File Server, AD Logga or as file server or AD scanner respectively is possible (how many Logga may run on one collector depends on the performance of the file server the collector is installed on and depends on the data volume each Logga has to process).

#### Note:

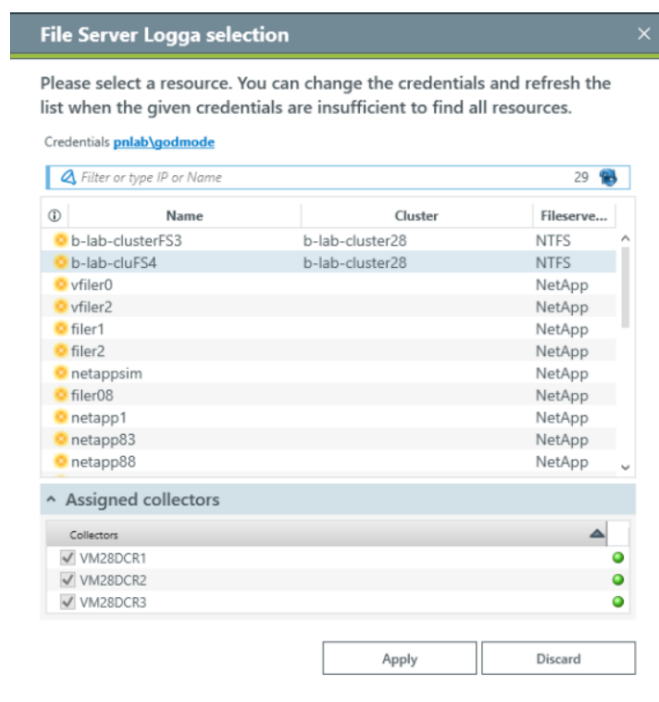
The list of file servers in the Logga selection dialog contains:

- Windows file servers on which the FS Logga for Windows File Server is installed and
- file servers with certain values for the Active Directory attribute "operatingSystem". The default search value of the collector for "operatingSystem" is:
  - "OnTap" and "NetApp" for NetApp file servers and
  - „EMC File Server“ and „EMC Celerra File Server“ for EMC file servers

If in your environment other values are used for the operating system for NetApp or EMC file servers respectively, then you have to adapt the settings for the 8MAN collector in the file **pnCollector.config.xml**, please see chapters "FS Logga for NetApp File Server" and "FS Logga für EMC-Fileserver".

### 3.1.2 Windows Failover Cluster

If the Windows Failover Cluster feature is active on a file server, instead the file server's computer name you will get the active Services/Roles of type File Server in the selection of servers to be monitored (Services on Windows 2008 and Roles in Windows 2012).



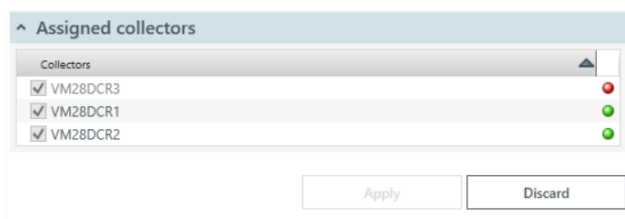
In the collectors overview all nodes of the cluster are preselected. This selection can't be changed because all the Logga must be active on all Nodes to ensure monitoring of cluster resource without interruption.

Please check that all collectors installed on the nodes configured by there name or FQDN (not by IP address).

The following conditions must be fulfilled to ensure successful configuration of monitoring of Services/Roles on Failover clusters:

- An 8MAN collector is installed on all nodes
- On all nodes the FS Logga for Windows File servers ist installed
- All collectors on all nodes are connected to the 8MAN server.

If not all of these conditions are fulfilled for a node, then this node is marked red in the collector's overview and you can not create a Logga configuration:

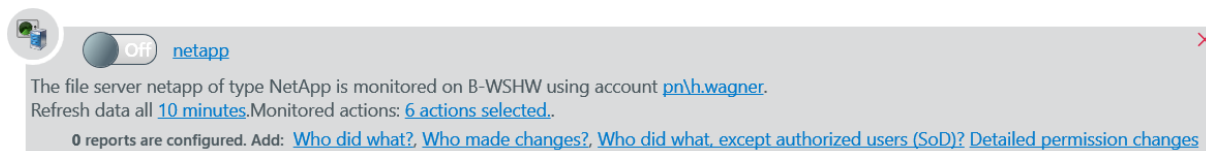


If you have finished configuring a Logga for Failover cluster resources and later on you add additional nodes to the cluster, then the 8MAN changes the Logga configuration and automatically starts monitoring on the new nodes. Automatic start of monitoring on new nodes is successful only if the conditions described above are fulfilled also for the new nodes:

- An 8MAN collector is installed on the new nodes
- On all new nodes the FS Logga for Windows File servers ist installed
- All collectors on the new nodes are connected to the 8MAN server.

## 3.2 Monitored actions and data refresh interval

When you have selected a server in the File Server Logga selection and click on “Apply”. It appears an FS-Logga-configuration-bubble:



The FS-Logga-configuration-bubble consists of:

- The On/Off switch of the Logga:
- The (changeable) name of the configuration:  
[netapp](#)
- The (changeable) account used for NetApp and EMC file servers to read the shares and their local paths:  
[account pn\h.wagner](#).  
**This account has to be member of the power user group on the file server to be monitored (see 2.2.1.2 and 2.2.2.2).**
- the configuration of the interval, the Logga should refresh the collected data to the 8MAN:  
[Refresh data all 10 minutes](#).
- the configuration of the monitored actions:  
[Monitored actions: 6 actions selected](#).
- the list of possible report types:  
[Who did what?](#), [Who made changes?](#), [Who did what, except authorized users \(SoD\)?](#), [Detailed permission changes](#)

Clicking on link for the configuration of the refresh data interval or configuration of the monitored actions the following dialog appears:

**Configuration for the File server Logga**

**Update interval**  
 Refresh data all  minutes.

**Monitored actions**  
 Please select actions you want to log:

	Name
<input checked="" type="checkbox"/>	Permission (ACL) changed
<input checked="" type="checkbox"/>	Directory / file created
<input checked="" type="checkbox"/>	Directory / file deleted
<input checked="" type="checkbox"/>	Directory / file moved or renamed
<input checked="" type="checkbox"/>	File read
<input checked="" type="checkbox"/>	File written

Please add a comment

Here you can change the data refresh interval between 1 to 60 minutes and you can configure the action the Logga should monitor and store in data base. This way you can save space on your data base by deselecting actions you do not need for your reports.

Changes are to be confirmed with comment and will be stored in the 8MAN logbook.

### Hint:

Deselecting actions has no effect on the report types “Who made changes?” and “Detailed permission changes”. These

report types monitor only certain actions. If you have deselected these actions, 8MAN automatically activates these actions when you configure these report types to ensure consistent content for these reports.

### 3.3 NetApp Clustered Data ONTAP Configuration

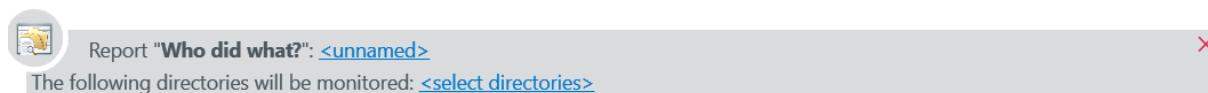
8MAN automatically detects file servers running on NetApp Clustered Data ONTAP. In this case additional configuration items are necessary to configure the Logga.

When you click on one of these items you can change the values:

- Data connection from collector to NetApp:**  
 Here you have to enter the collectors ip address and port. This address and port must be identical to the ones configured in the External-Engine configuration in chapter 2.2.2.1.2 “Creating the External Engine Configuration”. This ip address and port must be available on the collector. This addresss is used to receive the monitoring data from NetApp server.
- NetApp SVM Management:**  
 Enter the ip addresss of the LIF (Logical Interface) of the SVM (Storage Virtual Machine) on which the file server to be monitored is running. The LIF to choose here corresponds to the one configured in chapter 2.2.2.3 “Firewall configuration”.  
 The Credentails have to be of the account configured in chapter 2.2.2.2 “Domain Accounts”.

### 3.4 Select a name and the directories to be monitored for the FS Logga report types

Clicking on one of the links in the list of report types the report configuration bubble appears:



Each report configuration you can give a name clicking on [<unnamed>](#) :

And you have to select the directories to be monitored [<select directories>](#) :

For the monitoring of directories on NetApp or EMC file server you need a special permission to determine the local paths. User accounts being member of the group “Power Users” have such right. Therefore you have to enter in the directory selection dialog the credentials of such a user account.

You can set up a user account as a “Power users” as follows:

With at least one report configuration with at least one configured drive or directory, the FS Logga can be started (see chapter 3.6)

**Note:**

The sum of all directories in all report configurations of one file server should not exceed 512.  
The length of any of the selected directory paths must not exceed 1960 characters.

The recorded data will be stored for 30 days (default) in the 8MAN database and can be used for creating reports in that time. You can change the storage period under 8MAN Configuration → Server → Storage of scans (see document “Installation and Configuration”).

Please note that a longer storage period means that more memory for the 8MAN database is required. For each recorded operation 43 byte are needed.

## 3.5 Report types

### 3.5.1 Who did what?



Report "**Who did what?**": [<unnamed>](#)



The following directories will be monitored: [<select directories>](#)

For the selected directories, subdirectories and the files in there are the following operations recorded:

- File read
- File written
- Directory or file created
- Directory or file deleted
- Directory or file moved or renamed
- ACL changed
- ACL read (switched off by default [activation in the pnTracer.config.xml file possible] and not available for NetApp and EMC file server)

### 3.5.2 Who made changes?



Report "**Who made changes?**": [<unnamed>](#)



The following directories will be monitored: [<select directories>](#)

For the selected directories, subdirectories and the files in there are the following operations recorded:

- File written
- ACL changed

### 3.5.3 Who did what, except authorized users (SoD)?



Report "**Who did what, except authorized users (SoD)?**": [<unnamed>](#)





The following directories will be monitored: [<select directories>](#)

For the selected directories, subdirectories and the files in there are the following operations recorded (the selection of authorized users and groups takes place while creating the report):

- File read
- File written
- Directory or file created
- Directory or file deleted
- Directory or file moved or renamed
- ACL changed
- ACL read (switched off by default [activation in the pnTracer.config.xml file possible] and not available for NetApp and EMC file server)

### 3.5.4 Detailed permission changes


Report "Detailed permission changes": [<unnamed>](#)



The calculation of detailed permission changes can result in high utilization of the monitored file server and collector. For this reason the selecting this report type should be restricted as much as possible. Be aware that not only will the selected directory be monitored, but all of its subdirectories as well.

The following directories will be monitored: [<select directories>](#)


For the selected directories, subdirectories and the files in there the operation “ACL changed” is recorded. The difference to the other report types is that for the operation “ACL changed” not only the operation type but also the detailed changes are recorded (e.g. read access added for user X).

This report type is not available for Windows Failover cluster resources.

#### Hint:

The process to determine the detailed permission changes may influence the performance not only of the 8MAN collector but also the monitored file server. Use this report type only if the detailed permission changes are essential for your business. Restrict the selected directories to the minimum needed. Take into account that (like for each other report type) not only the selected directory will be monitored but also all subdirectories and the files.

## 3.6 Activating / Deactivating FS Logga

Clicking on  you can start or stop the Logga. You will be prompted for a comment which will be recorded in the 8MAN logbook:

**Start logging**

Please confirm the **Start** of the **File Server Logga** with a comment.  
The start event will be logged in the 8MAN logbook.

Please add a comment

Apply

Cancel

You cannot change the credentials when the Logga is ON (only NetApp and EMC file server Logga):

**Warning**

You can change credentials only when the Logga is off

Ok

Please check after switching on the Logga column “Logga status events” of the 8MAN Logbook for startup result information.



## 3.7 FS Logga settings in the pnTracer.config.xml file

### 3.7.1 Filtering of redundant events (reduce amount of collected data)

On user actions like browsing directories or open a file for read or writing a file depending on the application used more or less additional read or write actions are executed by this application. These redundant actions are ignored by the FS Logga if they occur within a specified time frame.

You can configure:

- If the FS Logga should ignore redundant events or not (separate for read and write events)
- The time frame within which the FS Logga regards events as redundant events

By default the redundant read and write events handling is on and the time frame detecting read or write events as redundant events is set to 10 seconds. These settings can be changed. Therefore you open on the file server with installed FS Logga the **pnTracer.config.xml** file under **C:\ProgramData\protected-networks.com\8MAN\cfg** (if they don't exist copy them from **C:\Programme \protected-networks.com\8MAN\etc**, delete the content and paste the following lines):

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <filesystem>
      <redundantEntriesHandling>
        <removeRead type="System.Boolean">true</removeRead>
        <removeWrite type="System.Boolean">true</removeWrite>
        <!-- maximum time-diff in seconds to ignore read or write, default 10 -->
        <maxTimeDiffForReads type="System.Int32">10</maxTimeDiffForReads>
        <maxTimeDiffForWrites type="System.Int32">10</maxTimeDiffForWrites>
      </redundantEntriesHandling>
    </filesystem>
  </tracer>
</config>
```

You can switch off the redundant event handling changing the values for „removeRead“ or „removeWrite“ from “true” to “false”. The time frame can be changed in the lines for „maxTimeDiffForReads“ and „maxTimeDiffForWrites“. The minimum value is 1 (one second) and the maximum value is 60 (60 seconds = 1 minute).

After saving the pnTracer.config.xml file you have to stop and then start the FS Logga so that the changes can take effect.

### 3.7.2 Disable the default non-recording of operations for certain security IDs (SIDs)

The default non-recording of operations for the following security IDs (SIDs) helps to reduce the amount of recorded data.

```
S-1-5-18 NT-AUTHORITY\SYSTEM
S-1-5-19 NT-AUTHORITY\ LOCAL SERVICE
S-1-5-20 NT-AUTHORITY\ NETWORK SERVICE
```

You can also record the operations for these users. Therefore you open on the file server with installed FS Logga the **pnTracer.config.xml** file under **C:\ProgramData\protected-networks.com\8MAN\cfg** (if they don't exist copy them from **C:\Programme \protected-networks.com\8MAN\etc**, delete the content and paste the following lines):

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <windows>
      <suspendfilter type="System.Boolean">true</suspendfilter>
    </windows>
  </tracer>
</config>
```

When you set the value for “suspendfilter” to <false> all operations for the above mentioned SIDs are recorded. The non-recording of operations for individual SIDs is not possible.

After saving the pnTracer.config.xml file you have to stop and then start the FS Logga so that the changes can take effect.

### 3.7.3 Change directory for temporary files of the Logga

By default temporary files the Logga will store under **C:\ProgramData\protected-networks.com\8MAN\**. To change this you can open on the file server with installed FS Logga the **pnTracer.config.xml** file under **C:\ProgramData\protected-networks.com\8MAN\cfg** (if they don't exist copy them from **C:\Programme \protected-networks.com\8MAN\etc**, delete the content and paste the following lines):

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <localStoragePath>E:\other\directory</localStoragePath>
  </tracer>
</config>
```

After saving the pnTracer.config.xml file you have to stop and then start the FS Logga so that the changes can take effect.

## 4 Create FS Logga reports

From the recorded FS Logga data you can create the reports

- Who did what?
- Who made changes?
- Who did what, except authorized users [SoD]?

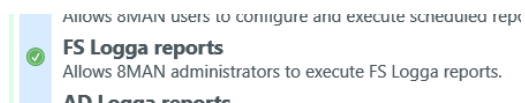
in CSV or XPS format

- FS Logga access rights change history

in XLS format.

### Prerequisites

- FS Logga license
- existing domain scan
- existing scan of the file server
- FS Logga is configured for the file server and report type and records data
- activated FS Logga Reports function (8MAN Configuration → User management → Extended user management; can only be activated and used by 8MAN administrators):



### Open

- 8MAN Homepage (button appears only for configured report types):

### Security Monitoring

#### Active Directory

- AD Logga Report


#### File server

- FS Logga access rights change history
- Who did what, except authorized users (SoD)?
- Who did what?
- Who made changes?

## 4.1 Report types “Who did what”, “Who made changes”, “Who did what, what except authorized users [SoD]”

Dialog (report example “Who did what”, additional parameter for the other 2 reports are listed in the table)

Parameter	Description
Format  Report in format CSV <input checked="" type="checkbox"/> XPS	Selectable report formats: CSV and XPS.
Title	You can enter a title for the AD Logga Report, e.g. for organizing the reports.
Comment	You can for example enter the reason for the report or the person who ordered the report.
1 Available configuration(s)  pnlabnaclu <unnamed> v	You can select a configuration that has been created in the 8MAN configuration. Then out of this configuration a report will be created.
Selected resources <a href="#">&lt;add&gt;</a>	In the appearing dialog you can by double clicking or the context menu select the directories for the report.
Stored data will be searched from <a href="#">10/1/2011 12:00 AM</a> to <a href="#">12/15/2016 3:52 PM</a>	In the appearing dialog you can select the period of time of the recorded data for the report.
<b>Only for “Who made changes?”:</b> Change filter for <a href="#">monitored actions</a>	In the appearing dialog you can select the operations for the report.
<b>Only for “Who did what, except authorized users [SoD]?”:</b> Authorized users/groups <a href="#">&lt;add&gt;</a>	In the appearing dialog you can by double clicking or the context menu select the authorized users and groups for the report.

When you click on  a report in the CSV or XPS format is created. The report you can then save, show or send as an e-mail attachment (prerequisite e-mail: 8MAN Configuration → Server → E-mail → option “Enable sending e-mails” activated):



It is also possible to open the report later in the report overview.

If SIDs are listed in the report you have to scan the domain or the file server (see prerequisites) in order to resolve the SIDs.

## 4.2 Report “FS Logga access rights change history”

This report shows an overview about the rights changes within a specified time period based on the data collected by the 8MATE FS Logga. Also included in the report is an overview about the rights at the start and end time based on the closest scan data.

Configuration:

- For 8MATE FS Logga the report “Detailed permission changes” has to be activated and valid configured
- File server scan for the same server has to be configured and include the observed paths to be able to show the start and end situation

Beside the possibility to start the report directly you can schedule the report for later execution. In this case it's suggested to use a predefined interval instead of a static start and end time.

Like at the “Who has access?” report you can configure the group and user representation and additional attributes to include into the report.

The report can contain the following tables (work sheets):

- Configuration: Summary of used report settings
- Logga configuration changes: Overview about the setting changes for the FS Logga within the specified time frame
- Start situation: Rights overview for the folders at start time
- Logga events: Overview about all Logga events
- Change details: Details for Logga events including Who? What? When? Where?
- 8MAN rights changes: List of all changes executed with 8MAN including comments of the 8MAN user

- End situation: Rights overview for folders at the end time
- Groups and their members: Name and members of the groups that are having rights
- Legend: explanation of the symbols used within the report

**Hint:**

Collecting the necessary data for this report (capturing access right changes) increases memory and performance consumption on the 8MAN collector and may also influence performance on the monitored file server depending on the size (number of subdirectories and files) of the monitored directories. In the FS-Logga configuration you should limit the selection of directories to be monitored for the new report type "Detailed permission changes" to the number necessary for your needs.

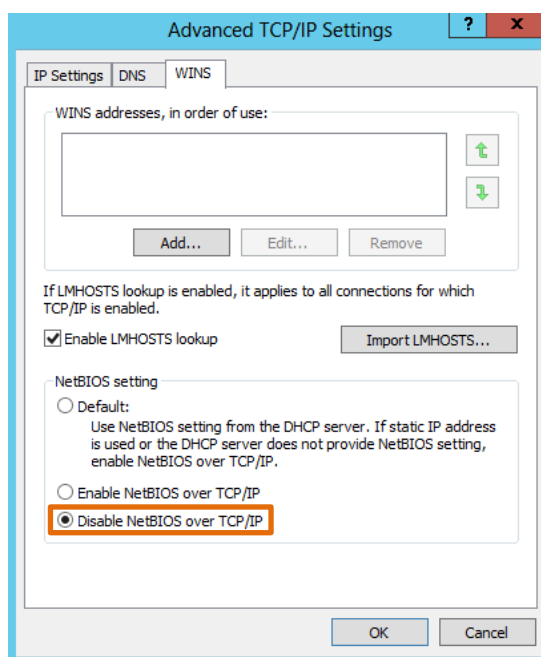
# Appendix

## Appendix I: Troubleshooting

### Problems connecting Logga and NetApp

Disable the NetBIOS over TCP/IP setting

A possible solution for network connection problems is to disable the NetBIOS over TCP/IP setting. In order to disable NetBIOS over TCP/IP go to the computer with installed collector-for-the-FS-Logga-for-NetApp-file-server and open the following dialog Start → Control Panel ( View by: Category ▼ ) → Network and Internet → Network and Sharing Center → Change adapter settings → Ethernet properties → Internet Protocol Version 4 (TCP/IPv4) → Properties → Advanced → WINS → select the NetBIOS over TCP/IP setting:



### Empty report for Windows Failover cluster resource

Shifting file server resource from one node to another node due to cluster service shutdown or node shutdown may lead to connection problems between Logga und underlying Windows system components. This results in missing data delivery from system to Logga.

To solve this issue switch of the Logga for this resource and after 10 seconds switch on again.



## Appendix II: Software license acknowledgements

- Json.net, © 2006-2014 Microsoft, <https://json.codeplex.com/license>
- #ziplib 0.85.5.452, © 2001-2012 IC#Code, <http://www.icsharpcode.net/opensource/sharpziplib/>
- PDFsharp 1.33.2882.0, © 2005-2012 empira Software GmbH, Troisdorf (Germany), [http://www.pdfsharp.net/PDFsharp\\_License.ashx](http://www.pdfsharp.net/PDFsharp_License.ashx)
- JetBrains Annotations, ©2007-2012 JetBrains, <http://www.apache.org/licenses/LICENSE-2.0>
- Microsoft Windows Driver Development Kit, © Microsoft, EULA on the computer with installed FS Logga for Windows File server under: C:\Program Files\protected-networks.com\8MAN\driver (only used for FS Logga for Windows File server)
- NetApp Manageability SDK, © 2013 NetApp, <https://communities.netapp.com/docs/DOC-1152> (only used for FS Logga for NetApp File server)
- WPF Shell Integration Library 3.0.50506.1, © 2008 Microsoft Corporation, <http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx>

### MSDN CODE GALLERY BINARY LICENSE

You are free to install, use, copy and distribute any number of copies of the software, in object code form, provided that you retain:

- all copyright, patent, trademark, and attribution notices that are present in the software,
- this list of conditions, and
- the following disclaimer in the documentation and/or other materials provided with the software.

The software is licensed “as-is.” You bear the risk of using it. No express warranties, guarantees or conditions are provided. To the extent permitted under your local laws, the implied warranties of merchantability, fitness for a particular purpose and non-infringement are excluded. This license does not grant you any rights to use any other party’s name, logo, or trademarks. All rights not specifically granted herein are reserved.

v061708

- WPF Toolkit Library 3.5.50211.1, © Microsoft 2006-2013, <http://wpf.codeplex.com/license>
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC; <https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE>
- Mustache.js, © 2009 Chris Wanstrath (Ruby) and © 2010-2014 Jan Lehnardt (JavaScript), <https://github.com/janl/mustache.js/blob/master/LICENSE>
- jQuery, © 2014 The jQuery Foundation, <https://jquery.org/license/>
- Metro UI CSS 2.0, © 2012-2013 Sergey Pimenov, <https://github.com/olton/Metro-UI-CSS/blob/master/LICENSE>
- LoadingDots, © 2011 John Nelson, <http://www.johncoder.com>
- Underscore.js, © 2009-2014 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors <https://github.com/jashkenas/underscore/blob/master/LICENSE>
- easyModal.js, © 2013 Flavius Matis, <https://github.com/flaviusmatis/easyModal.js>
- jsTimezoneDetect, © 2012 Jon Nylander, project maintained at <https://bitbucket.org/pellepim/jstimezonedetect>; <https://bitbucket.org/pellepim/jstimezonedetect/src/f9e3e30e1e1f53dd27cd0f73eb51a7e7caf7b378/LICENSE.txt?at=defaultjquery-tablesort>
- jquery-tablesort, © 2013 Kyle Fox, <https://github.com/kylefox/jquery-tablesort>