TEMASOFT FileMonitor

Contents

1 Introduction

1.1 About TEMASOFT FileMonitor

TEMASOFT FileMonitor is an advanced, file monitoring solution that delivers insight into the file and process / application related activity on Windows and NAS machines, enabling a broad array of use cases covering security, business continuity, data leakage prevention and compliance needs. Unlike any other file monitoring solution, TEMASOFT FileMonitor is capable of monitoring copy operations and file content duplication, through sophisticated on-disk and in-memory correlations based on how processes manipulate data. Through TEMASOFT FileMonitor, IT admins are able to:

Monitor

- Basic file and folder operations: read, write, delete, attributes change, security attributes change (changes to the file ACL);
- Advanced file operations: file copy and file content duplication, irrespective of the application responsible for copying the file and how it performs the actual copy (via a file copy API, or via read / write sequences), as well as irrespective of the destination of the new file (network, USB / removable storage device, etc.) as well as file renamed, file archived, file uploaded by browser and file attached to an email (via Outlook);
- Applications and process activity: process creation and process termination;
- User activity related to files and applications;
- The activity of users with administrative privileges;
- The files being changed;
- File integrity through file content hashing.

Alert

- Through real time actions when a certain activity is generated.

Report

- Through 100+ customizable, predefined reports and report templates.

Integrate

- By writing the information being collected to the Windows™ Event Log or in csv log files, TEMASOFT FileMonitor integrates with any existing SIEM solution.

For all the above monitoring events, TEMASOFT FileMonitor delivers actionable information about the following details:

- Timestamp;
- Source computer;
- User responsible for the action;
- What the action was (file write, file copy, process started, etc.);
- Full path and names of file(s) was/were involved;
- PID and source executable of the process involved;
- Content hash of the file(s);
- Details about the operation (like the attributes for a file attribute change event);
- Special flags (like signal when the operation was performed by a user with administrative privileges, or when a file was modified because of the event, or when a file was copied on removable storage device, etc.).

1.2 How TEMASOFT FileMonitor works

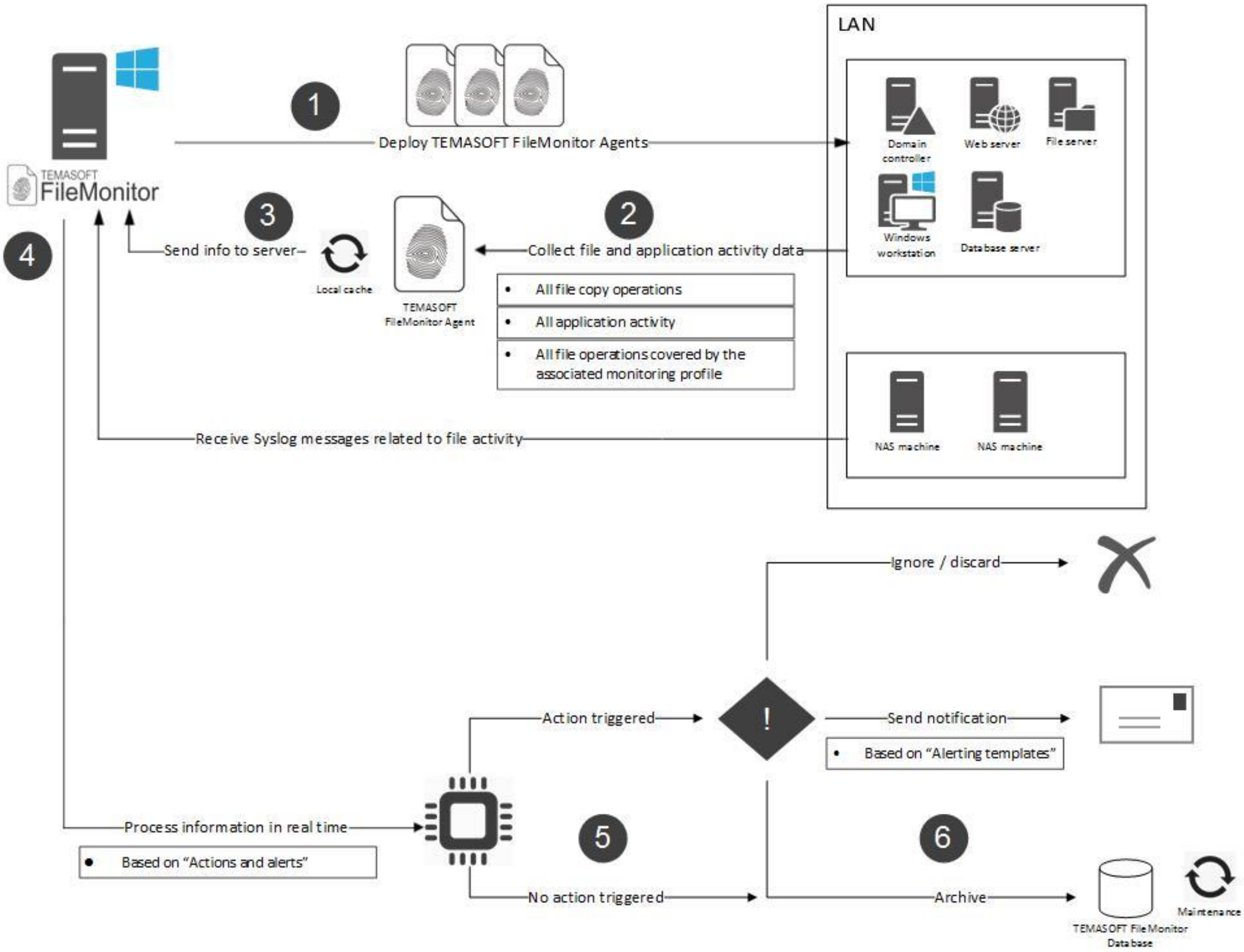

LAN
1
Deploy TEMASOFT FileMonitor Agents
TEMASOFT
FileMonitor
Domain controller
Web server
File server
Windows workstation
Database server
3
Send info to server
Local cache
TEMASOFT FileMonitor Agent
2
Collect file and application activity data
4
• All file copy operations
• All application activity
• All file operations covered by the associated monitoring profile
Receive Syslog messages related to file activity
NAS machine
NAS machine
Ignore / discard
Action triggered
!
Send notification
• Based on "Alerting templates"
Process information in real time
• Based on "Actions and alerts"
5
6
No action triggered
Archive
TEMASOFT FileMonitor Database
Maintenance

Figure 1: How TEMASOFT FileMonitor works

TEMASOFT FileMonitor is a file monitoring solution managed by a web interface, which uses a Microsoft SQL Server Database to store the collected data.

TEMASOFT FileMonitor uses FileMonitor Agents to record information about the file activity on the Windows computers being monitored. To monitor NAS devices, the product uses a Syslog receiver which captures file activity messages sent by those devices. The monitoring data is transmitted (securely from Agents) to the FileMonitor Server Service which processes the details and eventually saves the information in the Microsoft SQL Server™ database. Next, the FileMonitor user interface will expose the information, as well as provide support for configuring the product and delivering the configurations to the FileMonitor Agents via the FileMonitor Server Service.

The FileMonitor Sever Service requires domain administrative credentials to be able to manage the FileMonitor Agents in the domain. It also requires the running user to possess CREATE ANY DATABASE right on the Microsoft SQL Server™ instance and DB_OWNER right on each of the product databases to be able to create, update and maintain the TEMASOFT FileMonitor database(s). The product installer attempts to set these privileges automatically.

TEMASOFT FileMonitor components

The main components of the product are:

a) The FileMonitor Server: this handles the management and storage aspects of the product and needs to be deployed once in every environment or domain. It consists of the following components:
    a. The web user interface: this is a web application that delivers functionality to manage the product features, as well as perform data analysis and reporting;
    b. The FileMonitor database(s): one or multiple Microsoft SQL Server™ databases which are created by the product on installation or when the database is updated. Every moment there can be only one active database. This database holds the monitoring data collected and conveyed by the FileMonitor Agents;
    c. The FileMonitor Server service: this component is responsible for performing the actual management of the agents, including communication, storage of the information being recorded by the agents, as well as interacting with the web user interface;
b) The FileMonitor Agent: this is the operational component that performs the file monitoring functionality and must be deployed on every Windows computer that needs to be monitored. It makes use of a kernel-mode driver or other similar modules (depending on the target operating system) that perform all the necessary operations to record and deliver the expected information.

2 Installing TEMASOFT FileMonitor

This chapter presents the necessary steps to take, to install the TEMASOFT FileMonitor Serer and deploy the FileMonitor Agents, as well as typical deployment scenarios.

2.1 Getting started

The TEMASOFT FileMonitor Server installer is delivered as an executable which runs on Windows x64 architectures. To get started, you need to run this installer. Please review the “System requirements” sub-chapter first.

2.2 System requirements

TEMASOFT FileMonitor Server

Software environment:

- Operating systems: Windows 7 and 10, Windows Server 2012R2 and newer x64 only architecture;
  Please note that we do not support the “Home edition” for any of the above desktop operating systems. Also, we do not support the Core editions of the server operating systems.
- Software prerequisites (installed automatically if not present):
    - HTML5 browser: Internet Explorer 10 or newer, Google Chrome, Mozilla Firefox, Safari, Edge;
    - Browser minimum width: 1440px;
    - Microsoft SQL Server™ 2008 or newer - or the Express edition of Microsoft SQL Server™ 2012 or newer. We recommend using a dedicated production SQL Server 2012 or newer. We recommend that the Microsoft SQL Server database files reside on an SSD.;
    - Microsoft IIS 7 or newer;
        - No other site or service running on port 1753 TCP;
    - Microsoft Visual C++ 2019 Redistributable Package;
    - Microsoft .Net Framework 4.5.2;
    - Asp.net MVC5;
    - WebDeploy 3.0;

Hardware environment:

Minimum requirements:

- CPU: 2 cores;
- Memory: 4 GB RAM;
- HDD storage: 10 GB HDD;
- NIC: 1Gb;
- Video: 1440 px width.

Recommended:

- CPU: 4 cores;
- Memory: 8 GB RAM;
- HDD Storage: 30 GB;
- NIC: 1Gb.

The default ports used by the Server components are:

- TCP 1753 used by the web interface;
- TCP 47521 used by the service;
- UDP 514 used by the Syslog receiver.

FileMonitor Agent

Software environment:

- Operating systems:
  - Windows 7 and 10, Windows Server 2008R2 and newer, x86 or x64 architecture;

  Please note that we do not support the "Home edition" for any of the above desktop operating systems. We do not support Window 8 and 8.1.
- Software prerequisites:
  - Microsoft Visual C++ 2019 Redistributable Package;
  - Microsoft .Net Framework 4.5.1;

Hardware environment:

Minimum requirements:

- CPU: 1 core 2Ghz CPU;
- Memory: 1 GB;
- HDD storage: 10 GB;
- NIC: 100Mb.

Recommended:

- CPU: 4 core CPU;
- Memory: 4GB;
- HDD Storage: 20GB;
- NIC: 1Gb.

The Agent component only uses dynamic outbound TCP ports to connect to the Server components.

2.3 Deployment scenarios

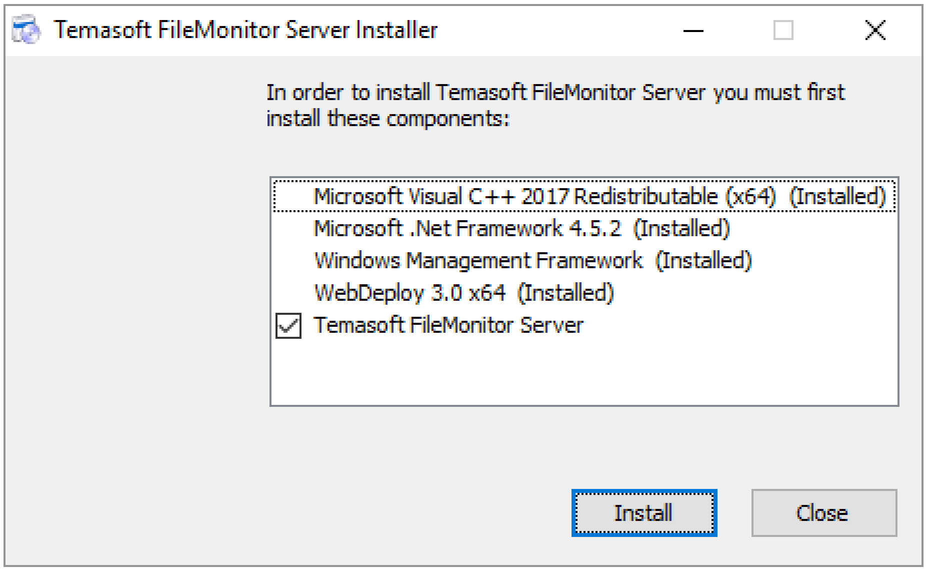
The TEMASOFT FileMonitor Server can be installed on any computer that meets the FileMonitor Server minimum system requirements. It can, then, be utilized to deploy the FileMonitor Agents across the network on any computer that meets the FileMonitor Agent minimum system requirements. Typically, the product can be deployed in both Active Directory domain and in workgroup environments.

2.4 Installing TEMASOFT FileMonitor Server

These are the steps needed to install TEMASOFT FileMonitor Server:

Installation Wizard

- Run the installer by double-clicking on the FileMonitorServerInstaller.exe program. The installer will unpack the necessary files;
- The installer detects any missing software prerequisites and then lists all software prerequisites and their status. Click "Install" to install any missing software prerequisites; for this step it is recommended to have an active internet connection, as some of the missing prerequisites might need to be downloaded from the internet.

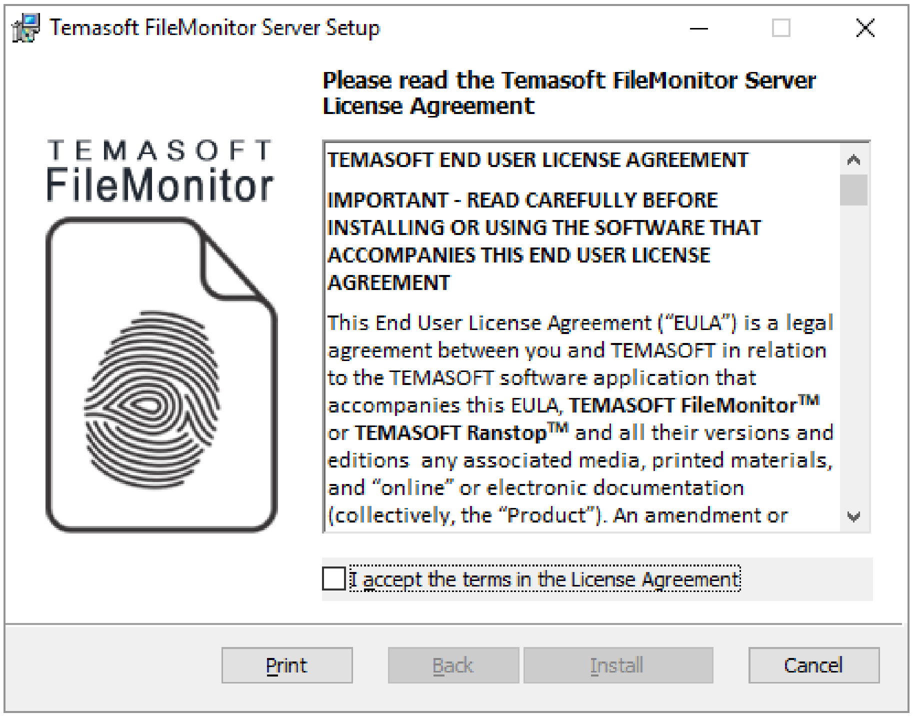


In order to install Temasoft FileMonitor Server you must first install these components:

Microsoft Visual C++ 2017 Redistributable (x64) (Installed)
Microsoft .Net Framework 4.5.2 (Installed)
Windows Management Framework (Installed)
WebDeploy 3.0 x64 (Installed)
☑ Temasoft FileMonitor Server

Figure 2: Installation prerequisites

- Once all the prerequisites are installed, the installer will run the product installer;
- The first dialog presents the EULA and requires you to read and accept its terms to be able to continue with the installation and to use the product. Tick the "I accept the terms in the License Agreement" checkbox and click "Install" to continue;



Please read the Temasoft FileMonitor Server License Agreement

TEMASOFT END USER LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY BEFORE INSTALLING OR USING THE SOFTWARE THAT ACCOMPANIES THIS END USER LICENSE AGREEMENT

This End User License Agreement ("EULA") is a legal agreement between you and TEMASOFT in relation to the TEMASOFT software application that accompanies this EULA, **TEMASOFT FileMonitor™** or **TEMASOFT Ranstop™** and all their versions and editions any associated media, printed materials, and "online" or electronic documentation (collectively, the "Product"). An amendment or

□ I accept the terms in the License Agreement

Figure 3: Installation license agreement

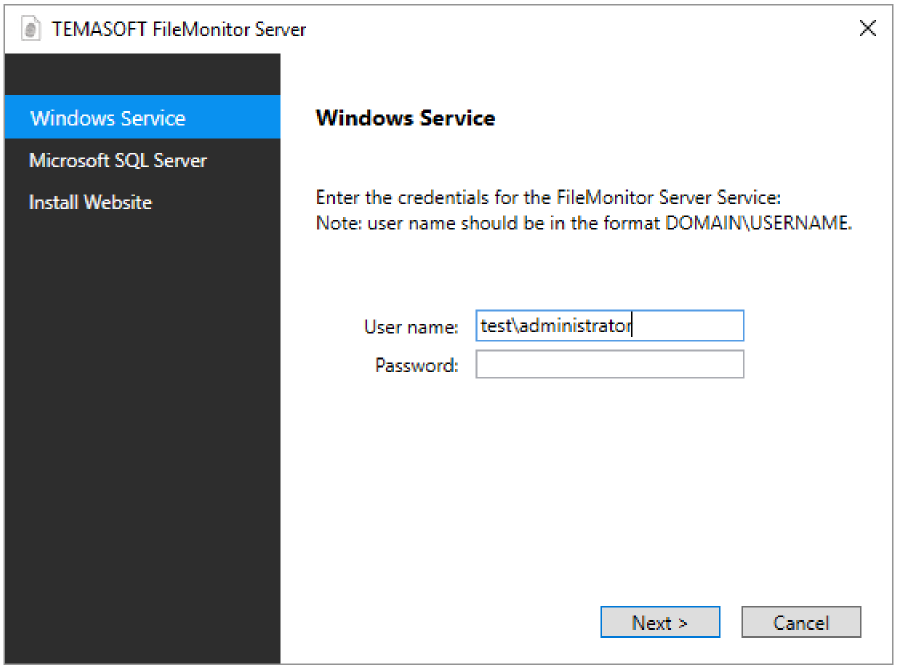
- Next, the installation will perform the necessary operations and display the "Installation Completed" dialog. Click "Finish" to complete the installation. The "Default Configuration Wizard" will start.

The settings required for the Default Configuration Wizard differ depending on the deployment scenario. Please continue reading the deployment scenario that fits your IT environment.

Default Configuration Wizard

- "Windows Service" section: please enter the credentials of a local or domain Administrator, in the format DOMAIN\USERNAME. The credentials are validated when clicking "Next". You cannot skip this step. If the credentials are invalid, the installation will not proceed.

  The Default Configuration Wizard will register the Windows service FileMonitor Server to run under these credentials. The service requires administrative credentials mainly to access and register the necessary resources used to communicate with FileMonitor Agents and other components.



Windows Service

Enter the credentials for the FileMonitor Server Service:
Note: user name should be in the format DOMAIN\USERNAME.

User name: test\administrator
Password:

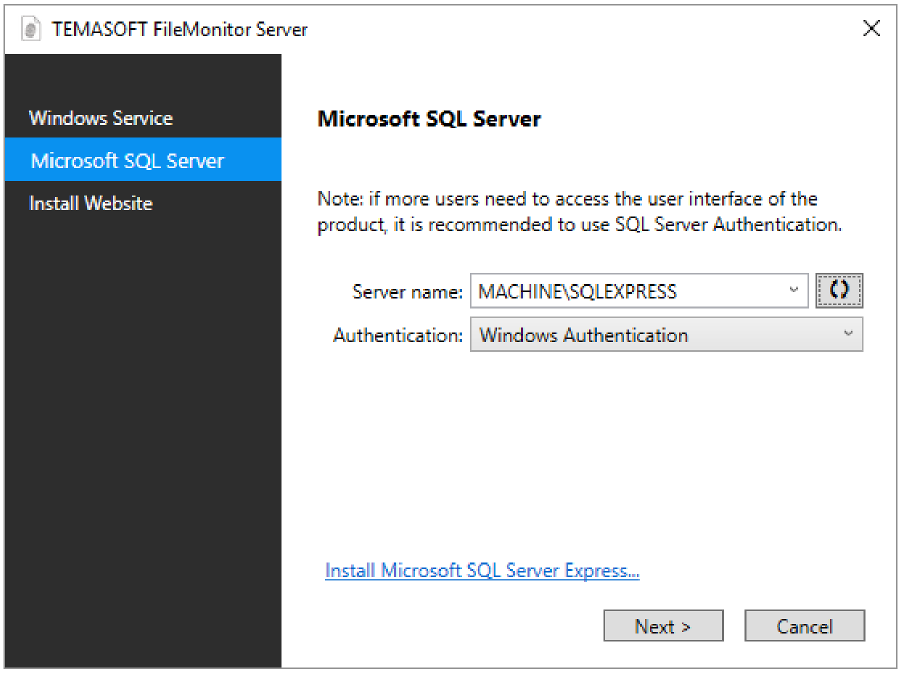
Figure 4: Default Configuration Wizard – Windows Service section

- “Microsoft SQL Server” section: Please select one of the existing Microsoft SQL Server instances. If no existing Microsoft SQL Server instance is selected, there is a link that allows you to manually install Microsoft SQL Server Express 2017 or 2014 depending on your version of Microsoft Windows operating system. Once you select a database instance, next you need to select the type of authentication.

  In case SQL Server Authentication is used, you will need to provide the credentials of a Microsoft SQL Server user account with CREATE ANY DATABASE right. This user should also have the DB_OWNER role on every database that will be created by the product. The installer will verify if these privileges are set and will attempt to set them automatically if not already set.

  If Windows Authentication is used to access the database, it is recommended to use a user who is member of the Administrators group, as, by default, this group has all the necessary rights to perform the necessary database operations. The Default Configuration Wizard will verify the Microsoft SQL Server settings before proceeding and prompt to correct any errors.

  Important note: if you need to allow other users to access the web interface of FileMonitor, it is recommended to use SQL Server Authentication. If you want to use Windows Authentication and allow more users, you must manually configure the SQL Server to add the necessary access rights to the FileMonitor database(s), for each additional user.



TEMASOFT FileMonitor Server

Microsoft SQL Server

Note: if more users need to access the user interface of the product, it is recommended to use SQL Server Authentication.

Server name: MACHINE\SQLEXPRESS

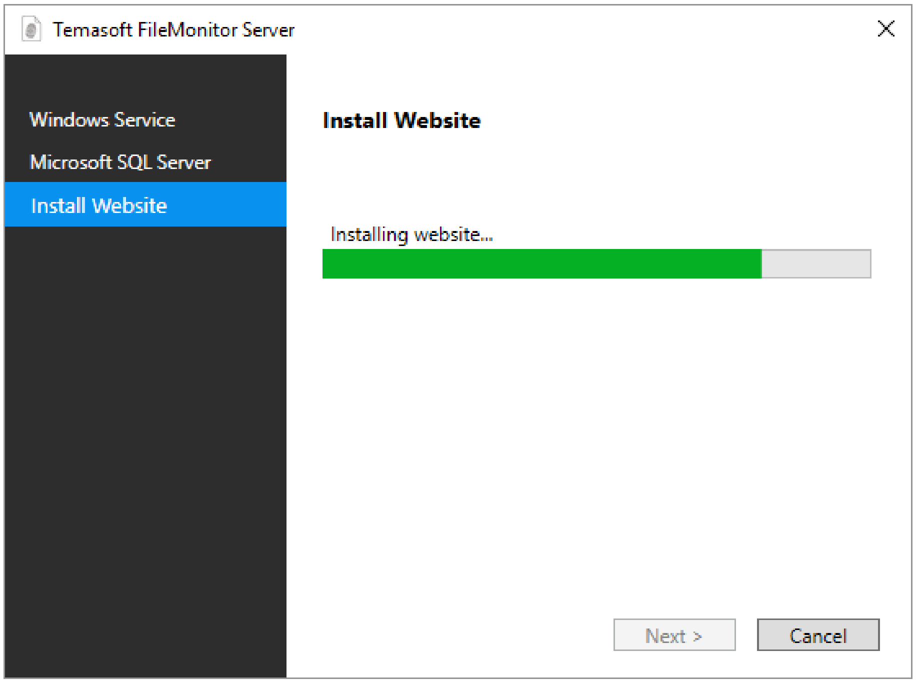
Authentication: Windows Authentication

Install Microsoft SQL Server Express...

Figure 5: Default Configuration Wizard – Microsoft SQL Server section

- "Install Website" section: There is no user input required for this section and the subsequent steps. The wizard will enable IIS locally, configure it accordingly and then will deploy the necessary files for TEMASOFT FileMonitor Server. The website will run on TCP port 1753 by default.

  The web interface uses by default HTTP protocol. If you want to use HTTPS, you need to generate a certificate (self-signed or commercial) for the machine where the FileMonitor Server is installed, then open IIS Manager, install the certificate, choose FileMonitor site and create a binding for port 443 and assign the certificate. Once HTTPS is working, the HTTP binding can be removed.



Temasoft FileMonitor Server

Install Website

Installing website...

Figure 6: Default Configuration Wizard - Install Website section

Deploying Agents,setup the Syslog receiver

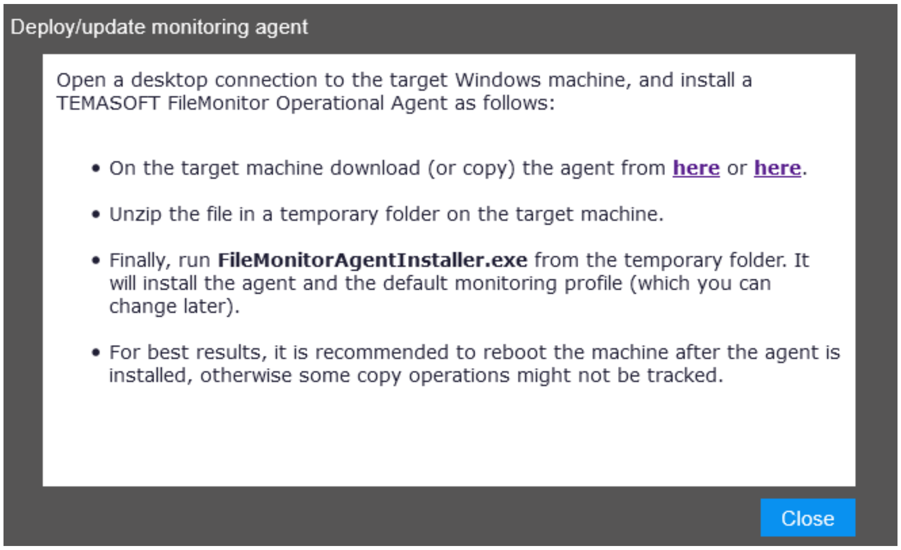
The next step, after having installed the TEMASOFT FileMonitor Server, is to deploy agents on the computers that need to be monitored. Setup the Syslog receiver if you need to monitor NAS devices.

2.5 Installing TEMASOFT FileMonitor Agent

The Agents can be installed manually or automatically in an AD environment, through Group Policies or other external tools.

To deploy the Agent manually you need to press the “Plus” ⊕ button from the “Monitored machines” section of the “Settings” page. The interface will display the following instructions that you need to follow:

- Open a desktop connection to the target Windows machine.
- On the target machine download (or copy) the agent from the presented link.
- Unzip the file in a temporary folder on the target machine.
- Finally, run **FileMonitorAgentInstaller.exe** from the temporary folder. It will install the agent and the default monitoring profile (which you can change later).
- For best results, it is recommended to reboot the machine after the agent is installed, otherwise some copy operations might not be tracked.

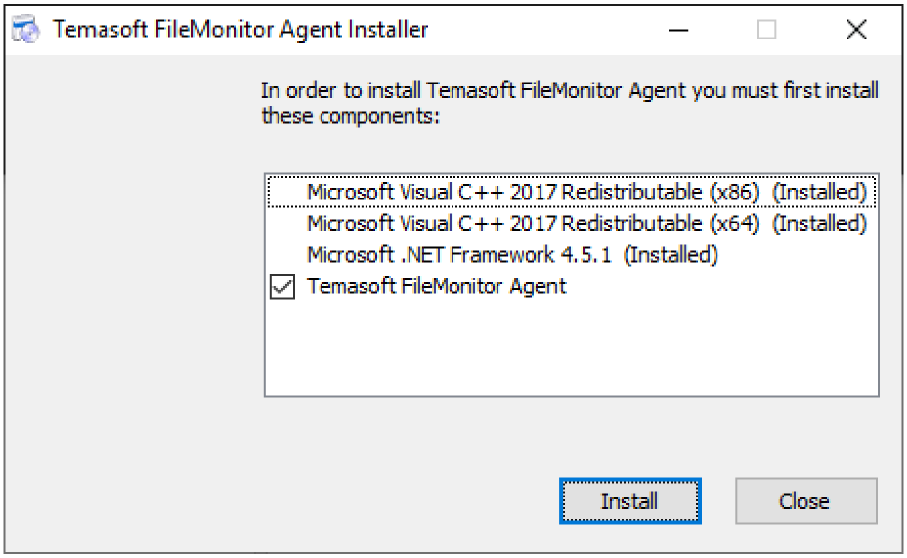


Deploy/update monitoring agent

Open a desktop connection to the target Windows machine, and install a TEMASOFT FileMonitor Operational Agent as follows:

- On the target machine download (or copy) the agent from **here** or **here**.
- Unzip the file in a temporary folder on the target machine.
- Finally, run **FileMonitorAgentInstaller.exe** from the temporary folder. It will install the agent and the default monitoring profile (which you can change later).
- For best results, it is recommended to reboot the machine after the agent is installed, otherwise some copy operations might not be tracked.

Figure 7: Deploying an agent



Temasoft FileMonitor Agent Installer

In order to install Temasoft FileMonitor Agent you must first install these components:

- Microsoft Visual C++ 2017 Redistributable (x86) (Installed)
- Microsoft Visual C++ 2017 Redistributable (x64) (Installed)
- Microsoft .NET Framework 4.5.1 (Installed)
- ☑ Temasoft FileMonitor Agent

Figure 8: Agent Installer - Prerequisites

To install the agent using the Group Policy or other tools, you can use the msi version of the installer as follows:

1. Copy AgentInstaller.msi from [C]:\Program Files (x86)\Temasoft\FileMonitor Server\Agents\Kits to a location you would like to use to start the deployment process;
2. On the target machines, make sure you first install the prerequisites mentioned in paragraph 2.2, FileMonitor Agent;
3. Deploy the msi using the following parameters:

```
/qn  SERVER_ADDRESSES="[SERVER HOSTNAME];[SERVER IP]" SERVER_PORT="47521"
```

Where SERVER HOSTNAME and SERVER IP are the NetBios name and IP v4 address of the machine on which TEMASOFT FileMonitor Server is installed.

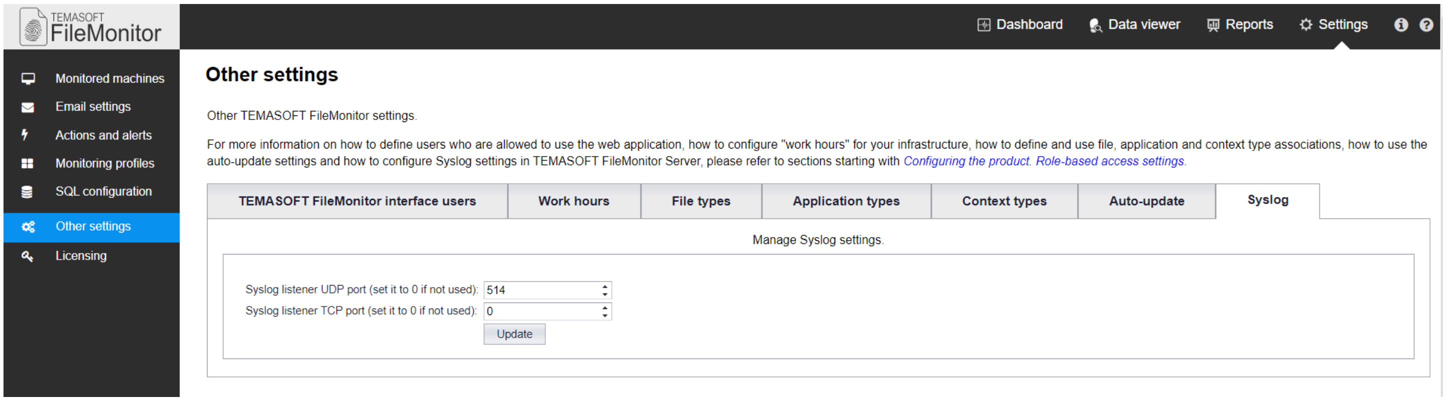
From the “Monitored machines” section, you can also invoke the “Redeploy/Update agent” action for a given machine you to reinstall or update the agent.

2.6 Monitoring file activity on Network Attached Storage (NAS) or Storage Area Networks (SAN)

TEMASOFT FileMonitor uses Windows agents to monitor file, user and application activity on remote machines. There are cases when the storage that needs to be monitored does not reside on a file server, or on a computer, like in the case of virtualized storage, SAN or NAS environments. You cannot install an agent in those cases, but TEMASOFT FileMonitor enables you to monitor those locations as well.

For NAS devices produced by QNAP or Synology, TEMASOFT FileMonitor has the ability to collect the syslog messages related to file activity that those devices generate. To enable the processing of those messages, you must follow these steps:

- From the web interface of the product, navigate to the Settings->Other Settings->Syslog page and set the Syslog listener port(s). By default, the UDP port 514 is enabled. If you do not want to listen for Syslog messages on a specific protocol, set its value to 0;
- Open the logging settings on your NAS device and enable logging for all the components/protocols that are related to file activity on that device;
- Set the logging system on your NAS machine to send Syslog messages to the IP address of the TEMASOFT FileMonitor Server and to the port/protocol specified in the first step.



Other settings

Other TEMASOFT FileMonitor settings.

For more information on how to define users who are allowed to use the web application, how to configure "work hours" for your infrastructure, how to define and use file, application and context type associations, how to use the auto-update settings and how to configure Syslog settings in TEMASOFT FileMonitor Server, please refer to sections starting with *Configuring the product. Role-based access settings.*

Manage Syslog settings.

Syslog listener UDP port (set it to 0 if not used): 514

Syslog listener TCP port (set it to 0 if not used): 0

Figure 9: Configure Syslog ports

To monitor storage on other devices (apart from Windows and the NAS devices mentioned earlier), please take the following approach:

- Deploy FileMonitor agents on all computers that can work with data hosted on NAS /SAN storage;
- Make sure that you enable “monitor all copy operations” on those computers;
- Filter view in “Data viewer” in the FileMonitor Server user interface as follows:
  - Enter the UNC path, or part of the UNC path corresponding to the remote storage in the edit box below the “File Name” field, and / or “Destination File Name” field. Click the “Pin” button next to the edit box and select the “Contains” operator;
  - This will enable real time monitoring of the activity on that storage;
  - For more information on how to use the Data viewer, please refer to Chapter 6 “Data analysis”.
- Modify the Path centric report template and include the UNC path above, as a filtering condition, as explained in the description of the template. You will be able to report on the activity on the remote storage using this report. For more information on how to use reports, please refer to Chapter 7 “Reporting”

2.7 Testing you installation

At this point, you should have a FileMonitor Server installation up and running, as well as several FileMonitor agents, deployed on your environment.

To test the deployment, please follow the below steps (if you have not noticed any errors during the previous stages):

- Open the FileMonitor Server console: http://[MACHINE NAME]:1753 (where MACHINE NAME is the machine on which the TEMASOFT FileMonitor server has been installed. You can also replace “[MACHINE NAME]” with the appropriate IP address of the TEMASOFT FileMonitor Server);
- On first run, the browser may ask for credentials when starting the UI- depending on the configuration of the browser. If this happens, please provide the credentials of the user who installed the product.
- Next, you will see a Quick Start Guide (Setup Wizard) that will instruct you on how to proceed further.
- Navigate to the “Data viewer” tab;
- Take note of the information present in the grid view on this tab. If you do not see any information, then something is wrong. Please refer to Chapter 10 “Troubleshooting” to identify the problem;
- If there is information, you may want to verify that it comes from all the FileMonitor agents:
  - Enter the name (one at a time) of each computer that is monitored, in the edit box below the “computer” label;
  - Click the “pin” icon ▼ and select the “contains” operator;
  - Note if there is any information present;
  - Repeat the step for each computer that is monitored

- If for at least one, there is no information present, please verify that:
    - ○ The computer is online
    - ○ The computer is reachable via the network
- If the computer is both online and can be reached, but there is still no information coming from it, please refer to chapter 10 “Troubleshooting” to identify the problem.

2.8 Upgrading from a previous version

Due to the number of changes in the current version of TEMASOFT FileMonitor, it is not possible to upgrade from the previous versions (2016-2019). If you use an older version of FileMonitor, you need to uninstall it completely, including the agents, then you can install the new version.

3 Configuring the product

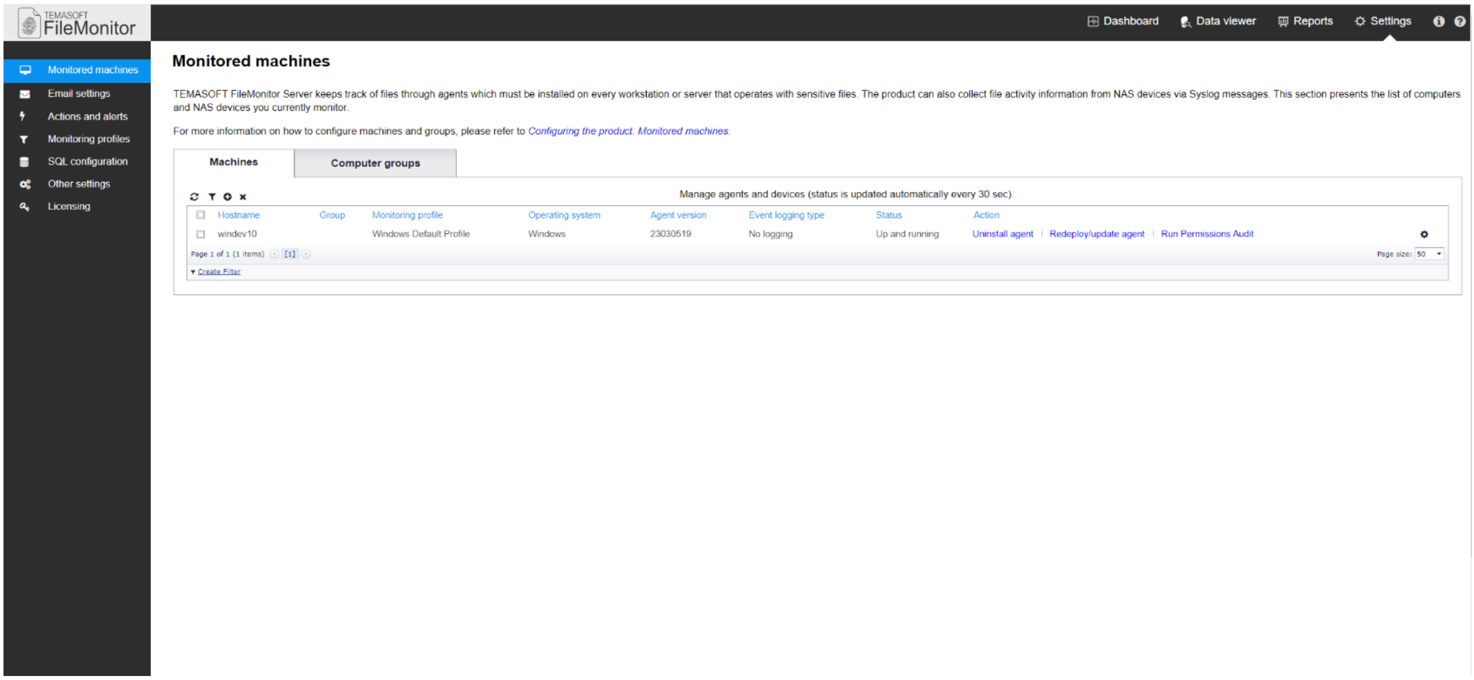
This chapter presents how to configure each aspect of the product, from configuring the machines to be monitored, and thus start collecting information, to reporting and changing licensing information.

3.1 Monitored machines

Adding computers to be monitored is the first step after the installation process, and an important part of deploying the solution in your environment.

Viewing the list of machines to be monitored

- ○ Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- ○ Navigate to the “Settings” page;
- ○ Click on the “Monitored computers” menu option;
- ○ The interface has two tabs, one for computers, and the other for groups.



Monitored machines

TEMASOFT FileMonitor Server keeps track of files through agents which must be installed on every workstation or server that operates with sensitive files. The product can also collect file activity information from NAS devices via Syslog messages. This section presents the list of computers and NAS devices you currently monitor.

For more information on how to configure machines and groups, please refer to *Configuring the product. Monitored machines.*

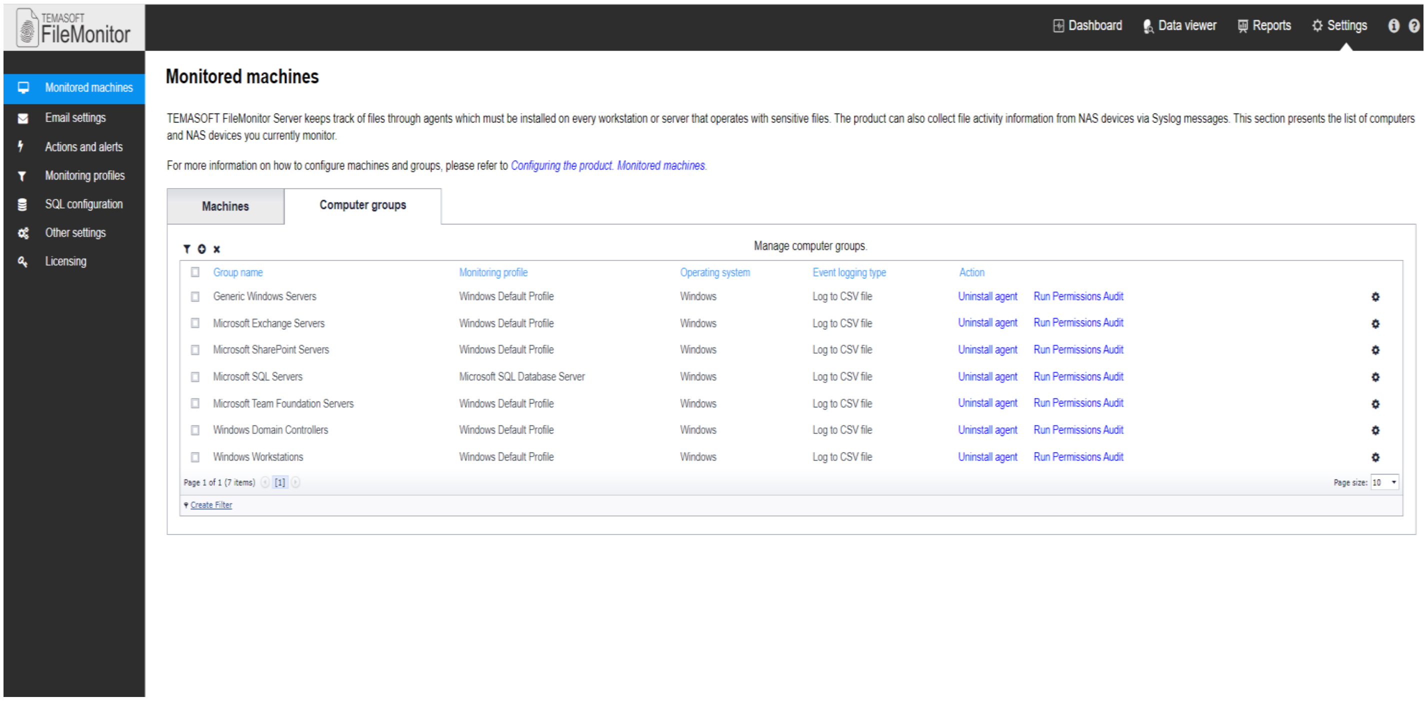
Manage agents and devices (status is updated automatically every 30 sec).

□	Hostname	Group	Monitoring profile	Operating system	Agent version	Event logging type	Status	Action
□	windev10		Windows Default Profile	Windows	23030519	No logging	Up and running	Uninstall agent | Redeploy/update agent | Run Permissions Audit

Page 1 of 1 (1 items) [1] Page size: 50

Figure 10: The list of monitored machines

- When selecting the “Computers” tab, a list of computers to be monitored will be displayed.
- The “Groups” tab contains predefined and preconfigured groups of computers. It also supports adding new groups. Please use these groups to centrally manage the settings (authentication and monitoring profile) of multiple computers to be monitored. The list of groups contains the following items by default:
    - Generic Windows Servers – default group for Windows machines
    - Microsoft Exchange™ Servers – default group for Microsoft Exchange™ servers;
    - Microsoft SharePoint™ Servers – default group for Microsoft SharePoint™ servers;
    - Microsoft SQL™ Servers – Default group for Microsoft SQL™ servers;
    - Microsoft Team Foundation Servers™ - Default group for Microsoft Team Foundation™ servers;
    - Windows Domain Controllers – Default group for domain controllers running Windows operating systems;



Monitored machines

TEMASOFT FileMonitor Server keeps track of files through agents which must be installed on every workstation or server that operates with sensitive files. The product can also collect file activity information from NAS devices via Syslog messages. This section presents the list of computers and NAS devices you currently monitor.

For more information on how to configure machines and groups, please refer to *Configuring the product. Monitored machines*.

Manage computer groups.

□	Group name	Monitoring profile	Operating system	Event logging type	Action		
□	Generic Windows Servers	Windows Default Profile	Windows	Log to CSV file	Uninstall agent	Run Permissions Audit	⚙
□	Microsoft Exchange Servers	Windows Default Profile	Windows	Log to CSV file	Uninstall agent	Run Permissions Audit	⚙
□	Microsoft SharePoint Servers	Windows Default Profile	Windows	Log to CSV file	Uninstall agent	Run Permissions Audit	⚙
□	Microsoft SQL Servers	Microsoft SQL Database Server	Windows	Log to CSV file	Uninstall agent	Run Permissions Audit	⚙
□	Microsoft Team Foundation Servers	Windows Default Profile	Windows	Log to CSV file	Uninstall agent	Run Permissions Audit	⚙
□	Windows Domain Controllers	Windows Default Profile	Windows	Log to CSV file	Uninstall agent	Run Permissions Audit	⚙
□	Windows Workstations	Windows Default Profile	Windows	Log to CSV file	Uninstall agent	Run Permissions Audit	⚙

Page 1 of 1 (7 items) [1]

Page size: 10

Create Filter

Figure 11: The list of computer groups

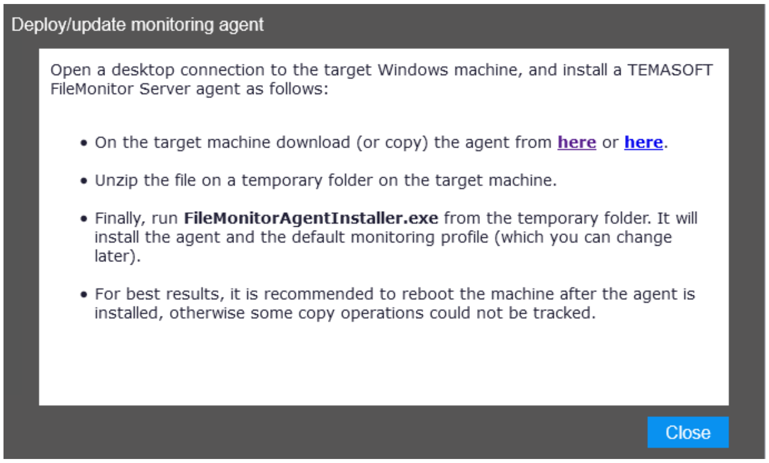
- Windows Workstations – Default group for workstations running Windows operating systems.

Adding computers individually

To add computers individually, hover over the “Plus” icon ⊕ and follow the next steps which are also displayed in the pop-up window:

- If there is already a version of FileMonitor agent installed on the target machine, uninstall it and continue with the next steps;
- On the target machine download the deployment package which contains the agent, from the links presented in the pop-up window. If you already downloaded it, you can also use the copied package;
- U Unzip the file on a temporary folder on the target machine.
- Finally, run FileMonitorAgentInstaller.exe from the temporary folder. It will install the agent and the default monitoring profile (which you can change later).

- For best results, it is recommended to reboot the machine after the agent is installed, otherwise some copy operations could not be tracked.



Deploy/update monitoring agent

Open a desktop connection to the target Windows machine, and install a TEMASOFT FileMonitor Server agent as follows:

- On the target machine download (or copy) the agent from **here** or **here**.
- Unzip the file on a temporary folder on the target machine.
- Finally, run **FileMonitorAgentInstaller.exe** from the temporary folder. It will install the agent and the default monitoring profile (which you can change later).
- For best results, it is recommended to reboot the machine after the agent is installed, otherwise some copy operations could not be tracked.

Figure 12: Add or edit monitored computer

When the agent is activated, it will automatically connect to the TEMASOFT FileMonitor Server and a corresponding entry will be automatically added to the Monitored machines list. By default, the newly installed agents will use the monitoring profile named “Windows Default Profile”.

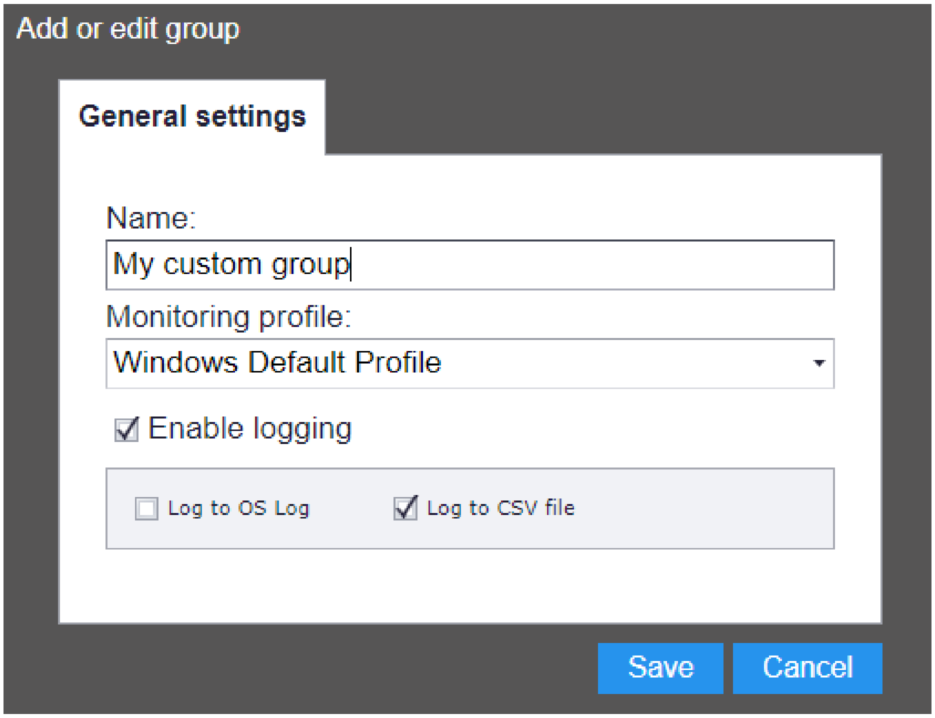
Last, but not least, when a new version of the agent is available, you will see a notification and a button to deploy the updated agent in Settings > Monitored machines.

QNAP and Synology NAS devices are automatically added to the Monitored machines list if the TEMASOFT FileMonitor Server starts receiving Syslog messages from those devices.

Adding custom group containers for centralized management of monitored computers

TEMASOFT FileMonitor allows definition of group containers for the monitored computers. The group containers enable administration of multiple hosts by providing the ability to configure the monitoring profile for each group. Then, when adding computers to be monitored, simply add them to a group and there will be no need to specify monitoring profiles or credentials for them. To create custom groups, please follow this procedure:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the “Settings” page;
- Click on the “Monitored computers” menu option;
- Select the “Groups” tab;
- Click the “Plus” button ⊕ - a new dialog will open;
  - Enter a name for the group;
  - Select a Monitoring Profile. You can also create custom monitoring profiles and use them. For more information, please see subchapter 3.2 Monitoring Profiles;
  - Optional: Enable additional logging to CSV or Windows Event Log for integration with SIEM or other solutions;
  - Click “Save” to save your custom group.



Name: My custom group

Monitoring profile: Windows Default Profile

☑ Enable logging

□ Log to OS Log ☑ Log to CSV file

Figure 13: Add or edit group

Additional operations available for the list of monitored computers

Filtering

The list of monitored computers can be filtered based on the following parameters:

- Hostname – string matching using string operators – enables filtering of computers with similar names or IPs;
- Group – string matching using string operators – enables filtering of computers belonging to the same group;
- Profile – string matching using string operators – enables filtering of computers that have the same monitoring profile assigned;
- Type – Windows or NAS – enables filtering of computers of the same type;
- Status – string matching using string operators – enables filtering of computers that have, or do not have a certain status.

To filter the list of computers, please perform the following steps:

- Click on the "Filter" button - a new dialog will open. Please see chapter 6, subchapter "Using Filters" on information on how to build a filter.

Deleting ✖

Use the "Delete" button to remove computers from the list of monitored machines. Select the computers that you want to remove, and then click the "Delete" button. The computers will be removed from the list, but the TEMASOFT FileMonitor Agent will NOT be uninstalled. If it is still active, it might register and show up again. Hence this operation is useful when you want to reassign some licenses, or when you want to remove the agents that are offline. For all the other cases otherwise please just uninstall the agent by using the "Uninstall" link in the "Actions" column.

Deletion can also be achieved by hovering over the "Gear" ⚙ icon of the corresponding entry that needs to be deleted, and selecting "delete item".

Refreshing the view

The view automatically refreshes the information every 30 seconds, but you can also use the “Refresh” button to reload the list of computers to be monitored. You might want to use this button when deploying TEMASOFT FileMonitor Agents on remote computers, while waiting for a status update.

Sorting the view

The user interface allows sorting of the list of monitored computers based on any available column. Simply click on the column that you wish to sort on. A triangle indicating the sort order will appear next to the name of the column. Clicking again, will reverse the sort order.

Available actions for monitored computers

Other actions are available for each entry in the list, under the “Actions” column:

- “Uninstall agent” will remove the TEMASOFT FileMonitor Agent from the remote computer, but keep the computer in the list. You can re-install the agent at a later stage, without having to add the computer again.
- “Redeploy/update agent” will (re)install the latest version of the agent automatically.

The “Status” column shows the status of the monitored machines. For NAS devices, the only possible status is “Ignored (license limit exceeded)”.

3.2 Monitoring profiles

The monitoring profiles are very important for performing file activity auditing operations, as they instruct the TEMASOFT FileMonitor Agent, which folders and files to monitor. There can be only one monitoring profile assigned to a computer or to a group of computers. Hence, the monitoring profile must be built in such a way as to cover all the paths that are required to be monitored.

NAS devices cannot be associated monitoring profiles.

TEMASOFT FileMonitor Server comes with a list of predefined monitoring profiles as follows:

Default monitoring profiles for Windows

Name	Description	Monitored paths and extensions	Excluded paths
Windows Default Profile	Windows monitoring profile will monitor by default the system folder, several Windows subfolders, and the program files folders	[Windows]\inf*, [Windows]\Security*, Windows]\Tasks*, [System]*, [Program Files]*, [Program Files (x86)]*, **.doc, **.docx, **.pdf, **.ppt, **.pptx, **.xls, **.xlsx, **.avi, **.mp4, **.flw, **.mkv, **.asf, **.ogg, **.zip, **.rar, **.gz, **.7z, **.tar, **.oxps, **.pptm, **.pmd, **.pub, **.epub, **.mht, **.dot, **.dotx, **.dotm, **.docm, **.ppsn, **.vsdm, **.vsd, **.txt, **.csv, **.xml, **.bmp, **.jpeg, **.jpg, **.gif, **.tiff, **.png, **.svg, **.mp3, **.wav, **.inf, **.sys, **.ini, **.rtf, **.torrent, **.mpg, **.mpeg, **.vob	[CommonApplicationData]\Temasoft*, [ProgramFilesX86]\Temasoft*
Windows Compliance	This monitoring profile includes the Windows monitoring profile. In addition, you need to configure the folders where the data that falls under the scope of the regulation	Those of Windows monitoring profile and the extensions of documents. Template: please add the paths where the data that makes the scope of the compliance regulation resides.	Those of Windows monitoring profile

	resides. For example, the folder containing ePHI for HIPAA compliance, the folder containing cardholder information for PCI DSS, etc.		
Windows Web Servers	This monitoring profile includes the Windows monitoring profile and adds the web server relevant paths.	Those of Windows monitoring profile, Template, please add the "Inetpub" folder (i.e. c:\Inetpub\*)	Those of Windows monitoring profile
Oracle Database Servers	This template includes the Windows monitoring profile. In addition, you need to add the following paths to this profile: ORACLE_HOME/net80/admin ORACLE_HOME/network/admin. For less granular monitoring, simply add the ORACLE_HOME folder.	Those of Windows monitoring profile, Template: please add the path to your Oracle home folder.	Those of Windows monitoring profile
Microsoft SQL Database Servers	This template includes the Windows monitoring profile. In addition, you need to add the SQL Server database storage folders to this profile, in order to monitor changes on .mdf and .ldf files.	Those of Windows monitoring profile, Template: please add the path to your .ldf and .mdf files.	Those of Windows monitoring profile,

Figure 73: List of default monitoring profiles for Windows

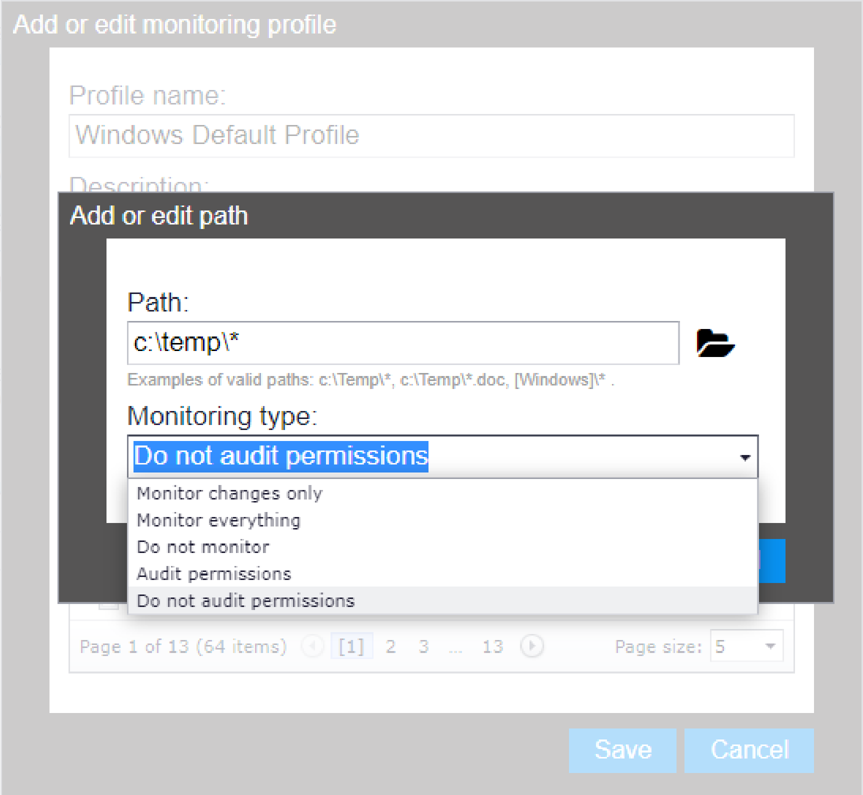
Irrespective of the monitoring profile chosen (even if no profile is set), the agent will monitor all the file copy and process tracking operations occurring on the agent machine.

Adding monitoring profiles

The default monitoring profiles cover generic use cases. For best coverage of specific requirements, please create your own monitoring profiles. You can build monitoring profiles only for Windows computers. In order to do that, follow these steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the “Settings” page;
- Click on the “Monitoring profiles” menu option;
- Click on the “Plus” button ⊕. A new dialog will appear. Please fill in the necessary information:
    - Profile name: this field is used to identify the profile so that it can be assigned to computers or groups, when configuring targets to be monitored;
    - Profile description: this optional field allows you to describe what the profile is being used for;
    - Next, select the paths that will be covered by this monitoring profile. Click the “Plus” button corresponding with the list of monitored paths ⊕;
        - The state of the row being edited will change. Enter the desired path in the edit box belonging to the column called “Path”. For more information on supported inputs for valid paths, please see the next paragraph - “Adding paths to monitoring profiles”;
        - Next, select the monitoring type. Available monitoring types are:
            - Monitor changes only: this option will only record file write, file renamed, file attribute changes and file security option changes as well as file create / deleted for folders;

  - Monitor everything: this option will record all supported file operation types for the files residing in this path;
  - Do not monitor: this option allows you to exclude this path from monitoring. This is useful if you want to monitor a certain folder, but you want to exclude one of its subfolders from monitoring;
  - Audit permissions: this option will enable auditing of the access rights for the designated files and folders;
  - Do not audit permissions: this option will exclude the specified folders and files from access rights auditing;
  - Click on “Update” link to save this path;
  - Repeat the above four steps to add more paths to this monitoring profile;
- Click “Save” to save your monitoring profile. The new profile will appear in the list of monitoring profiles, as well as an option when choosing the monitoring profile for a computer to be monitored, or a group of computers.



Add or edit monitoring profile

Profile name: Windows Default Profile

Description:

Add or edit path

Path: c:\temp\*

Examples of valid paths: c:\Temp\*, c:\Temp\*.doc, [Windows]* .

Monitoring type: Do not audit permissions

Page 1 of 13 (64 items) [1] 2 3 ... 13 Page size: 5

Figure 14: Add or edit monitoring profile

Note: you can edit a monitoring profile by clicking on the corresponding “Gear” ⚙ icon. This action will open the add/edit monitoring profile dialog in Figure 14.

Adding paths to monitoring profiles

When following the procedure to create a monitoring profile as described in the paragraph above, you need to add or edit paths belonging to the monitoring profiles. To ensure easy configuration across various computers in various languages (where the names of the same folders you would want to monitor are different with each computer) or having the system on various drives, we support adding paths as environmental variables. Please follow the rules below, to edit or add a path to a monitoring profile:

- You can use environmental variables, such as “Windows” – the path to the “Windows” folder enclosed between “[“ and “]”;

- When adding a path, you must end it with “*”;
- The interface supports file expressions as the cmd tool in Windows; (for example, “?” Replaces a character);
- Examples of supported, valid inputs as paths:
    - C:\Important folder*
    - [Windows]*
    - [System]*
    - [System]\Drivers*
- Please see a list of supported environmental variables below:

Member name	**Description**
AdminTools	The file system directory that is used to store administrative tools for an individual user. The Microsoft Management Console (MMC) will save customized consoles to this directory, and it will roam with the user. Added in the .NET Framework 4.
CDBurning	The file system directory that acts as a staging area for files waiting to be written to a CD. Added in the .NET Framework 4.
CommonAdminTools	The file system directory that contains administrative tools for all users of the computer. Added in the .NET Framework 4.
CommonApplicationData	The directory that serves as a common repository for application-specific data that is used by all users.
CommonDesktopDirectory	The file system directory that contains files and folders that appear on the desktop for all users. This special folder is valid only for Windows NT systems. Added in the .NET Framework 4.
CommonDocuments	The file system directory that contains documents that are common to all users. This special folder is valid for Windows NT systems, Windows 95, and Windows 98 systems with Shfolder.dll installed. Added in the .NET Framework 4.
CommonMusic	The file system directory that serves as a repository for music files common to all users. Added in the .NET Framework 4.
CommonOemLinks	This value is recognized in Windows Vista for backward compatibility, but the special folder itself is no longer used. Added in the .NET Framework 4.
CommonPictures	The file system directory that serves as a repository for image files common to all users. Added in the .NET Framework 4.
CommonProgramFiles	The directory for components that are shared across applications.

	To get the x86 common program files directory on a non-x86 system, use the ProgramFilesX86 member.
CommonProgramFilesX86	The **Program Files** folder. Added in the .NET Framework 4.
CommonPrograms	A folder for components that are shared across applications. This special folder is valid only for Windows NT, Windows 2000, and Windows XP systems. Added in the .NET Framework 4.
CommonStartMenu	The file system directory that contains the programs and folders that appear on the **Start** menu for all users. This special folder is valid only for Windows NT systems. Added in the .NET Framework 4.
CommonStartup	The file system directory that contains the programs that appear in the **Startup** folder for all users. This special folder is valid only for Windows NT systems. Added in the .NET Framework 4.
CommonTemplates	The file system directory that contains the templates that are available to all users. This special folder is valid only for Windows NT systems. Added in the .NET Framework 4.
CommonVideos	The file system directory that serves as a repository for video files common to all users. Added in the .NET Framework 4.
Fonts	A virtual folder that contains fonts. Added in the .NET Framework 4.
LocalApplicationData	The directory that serves as a common repository for application-specific data that is used by the current, non-roaming user.
LocalizedResources	The file system directory that contains localized resource data. Added in the .NET Framework 4.
NetworkShortcuts	A file system directory that contains the link objects that may exist in the **My Network Places** virtual folder. Added in the .NET Framework 4.
PrinterShortcuts	The file system directory that contains the link objects that can exist in the **Printers** virtual folder. Added in the .NET Framework 4.
ProgramFiles	The program files directory.

	On a non-x86 system, passing ProgramFiles to the GetFolderPath method returns the path for non-x86 programs. To get the x86 program files directory on a non-x86 system, use the ProgramFilesX86 member.
ProgramFilesX86	The x86 **Program Files** folder. Added in the .NET Framework 4.
Resources	The file system directory that contains resource data. Added in the .NET Framework 4.
SendTo	The directory that contains the Send To menu items.
StartMenu	The directory that contains the Start menu items.
System	The System directory.
SystemX86	The Windows **System** folder. Added in the .NET Framework 4.
Windows	The Windows directory or SYSROOT. This corresponds to the %windir% or %SYSTEMROOT% environment variables. Added in the .NET Framework 4.

Figure 15: List of supported environment variables as paths

Prioritization of processing when there are conflicting paths, in a monitoring profile

What are conflicting paths?

The monitoring profile can contain as many paths or file extensions as needed. Hence, it may be the case when a certain operation involves a file that matches multiple paths defined in the monitoring profile. For example, an executable file located in Program Files, would match a monitoring profile that has the following two paths defined: "[Program files]*" and "**.exe". In this case, the file matches multiple paths. If these paths have different monitoring settings, then the paths are conflicting. With the above example, the [Program files]* may be excluded from monitoring ("Do not monitor", while the "**.exe" may be configured for "monitor everything".

In this case, the program needs to know what to do with the file that matches both path definitions: ignore it, or log it. Hence, we have defined a prioritization based on the type of monitoring configured for the matching paths.

If for an action that involves a file, for which there are conflicting paths configured (it matches more than one path in the monitoring profile, and those paths are configured differently), the program will use the following priority: "Do not monitor", followed by "Monitor Everything", followed by "Monitor changes only". Hence, if a file matches paths covering all these configurations, it will be ignored. If it matches paths configured for monitoring changes or everything, it will be monitored for everything (including file read operations).

Export existing monitoring profiles

To export the existing monitoring profiles, please click the "Export" button, icon 💾. A zip file with the necessary data will be created and downloaded by the browser to the default download location.

Import monitoring profiles

To import monitoring profiles, please click the “Import” button, icon ⤒. This action will open a dialog which will allow selection of the file storing the monitoring profiles to import. The dialog expects an XML file and allows import of one monitoring profile at a time. Such a file is created by using the “export monitoring profiles” option, however, the format in that case is a zip archive of multiple XML files (one for each exported monitoring profile). Hence, you need to unzip the exported file and select the desired XML file. The XML files have the same name as the original monitoring profile.

Assign monitoring profiles to computers to be monitored, or to computer groups

Once custom monitoring profiles are in place, please follow the steps described in chapter 3 subchapter 1 “Monitored computers” to use them with the computers you want to monitor.

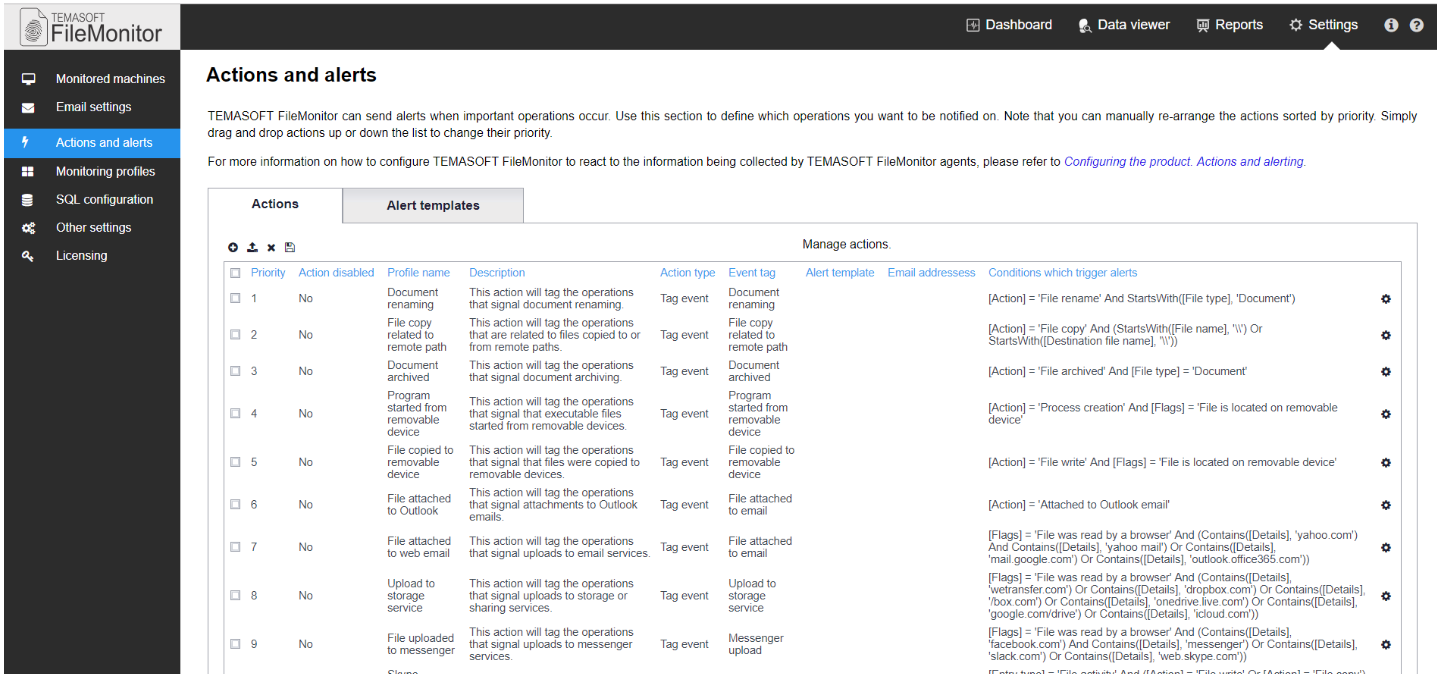
3.3 Actions and alerting

This section describes how to configure TEMASOFT FileMonitor to react to the information being collected by TEMASOFT FileMonitor agents. As soon as information is collected on the computers to be monitored, it is sent by the TEMASOFT FileMonitor Agent to the TEMASOFT FileMonitor Server. Upon receiving the information, the TEMASOFT FileMonitor Server can act on the information in various ways. By default, provided you do not configure anything in this section, the information will be archived in the database and no further actions are taken. However, you can configure the product to ignore or alert on certain type of information, based on various parameters that will be described in this chapter. This allows you to get an email when a certain folder is being accessed, or when a certain file is modified, which is very useful for various use cases. For example, if you run a website, then you will find it useful to have a notification whenever a configuration file for the web server or the website itself changes (or when the source file of the website changes – potential “defacing” attack).

To work to manage the actions and alerts, please follow these steps:

- ○ Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- ○ Navigate to the “Settings” page;
- ○ Click on the “Actions and alerts” menu option;

A list of defined actions and alerts will be presented, together with all the needed management options.



Actions and alerts

TEMASOFT FileMonitor can send alerts when important operations occur. Use this section to define which operations you want to be notified on. Note that you can manually re-arrange the actions sorted by priority. Simply drag and drop actions up or down the list to change their priority.

For more information on how to configure TEMASOFT FileMonitor to react to the information being collected by TEMASOFT FileMonitor agents, please refer to *Configuring the product. Actions and alerting*.

□	Priority	Action disabled	Profile name	Description	Action type	Event tag	Alert template	Email addressess	Conditions which trigger alerts
□	1	No	Document renaming	This action will tag the operations that signal document renaming.	Tag event	Document renaming			[Action] = 'File rename' And StartsWith([File type], 'Document')
□	2	No	File copy related to remote path	This action will tag the operations that are related to files copied to or from remote paths.	Tag event	File copy related to remote path			[Action] = 'File copy' And (StartsWith([File name], '\\') Or StartsWith([Destination file name], '\\'))
□	3	No	Document archived	This action will tag the operations that signal document archiving.	Tag event	Document archived			[Action] = 'File archived' And [File type] = 'Document'
□	4	No	Program started from removable device	This action will tag the operations that signal that executable files started from removable devices.	Tag event	Program started from removable device			[Action] = 'Process creation' And [Flags] = 'File is located on removable device'
□	5	No	File copied to removable device	This action will tag the operations that signal that files were copied to removable devices.	Tag event	File copied to removable device			[Action] = 'File write' And [Flags] = 'File is located on removable device'
□	6	No	File attached to Outlook	This action will tag the operations that signal attachments to Outlook emails.	Tag event	File attached to email			[Action] = 'Attached to Outlook email'
□	7	No	File attached to web email	This action will tag the operations that signal uploads to email services.	Tag event	File attached to email			[Flags] = 'File was read by a browser' And (Contains([Details], 'yahoo.com') And Contains([Details], 'yahoo mail') Or Contains([Details], 'mail.google.com') Or Contains([Details], 'outlook.office365.com'))
□	8	No	Upload to storage service	This action will tag the operations that signal uploads to storage or sharing services.	Tag event	Upload to storage service			[Flags] = 'File was read by a browser' And (Contains([Details], 'wetransfer.com') Or Contains([Details], 'dropbox.com') Or Contains([Details], '/box.com') Or Contains([Details], 'onedrive.live.com') Or Contains([Details], 'google.com/drive') Or Contains([Details], 'icloud.com'))
□	9	No	File uploaded to messenger	This action will tag the operations that signal uploads to messenger services.	Tag event	Messenger upload			[Flags] = 'File was read by a browser' And (Contains([Details], 'facebook.com') And Contains([Details], 'messenger') Or Contains([Details], 'slack.com') Or Contains([Details], 'web.skype.com'))

Figure 16: Actions and alerts

Default actions

By default, there is a single action defined in the product, but its state is disabled. If enabled, the action will cause the product to ignore the process and file activity of users containing “NT Authority” or “$” in order to reduce noise generated by normal system operations of the system or computer accounts. You should enable this action if you find such noise in the data you are receiving. Note, however, that there may be potentially dangerous operations that run in the system security context that you should watch for. You can further narrow down the operations being ignored by adding more conditions to the filter of the action, as described in this chapter.

Default alerting templates

The alerting templates regulate how the email notifications are being built. You can define custom alerting profiles that fit various use cases and then assign these alerting templates to actions and alerts. By default, there is an alerting template that defines the notification as follows:

- Email subject: FileMonitor Message for activity recorder on {Computer}
- Email body: This is an e-mail message sent automatically by FileMonitor for file activity on {COMPUTER}
  Event information:
  Timestamp: {TIMESTAMP}
  Event type: {STATUS}
  Target file/folder: {FILE NAME}
  Process information: {EXECUTABLE PATH}
  Action: {ACTION}
  User name: {USERNAME}

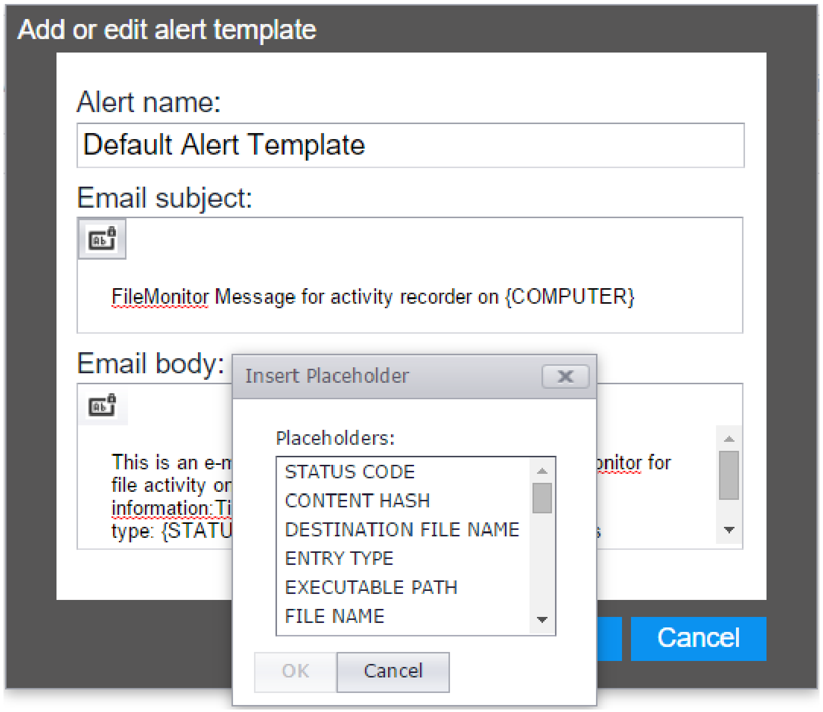
The event-specific parameters, or placeholders, presented above, will cause the email notification to get populated with the values of those fields for the specific event that triggered the notification. For more information on the available event-specific fields, their meaning and possible values, please see chapter 6, subchapter "Event Fields"

If you need more information in the alerting template, included either in the subject or email body, please change the default template, or create a custom one.

Creating custom alerting templates

To create a custom alerting profile, please follow these steps:

- Click on the "Alert templates" tab
- Click on the "Plus" button, icon ⊕ and a new dialog will appear:
  - Enter a name for the template;
  - Enter free text in the field "Email subject" to define the subject of the notification;
  - Enter free text in the field "Email body" to define the body of the email;
  - To insert event-specific information, or placeholders, in the subject or body of the email, please click on the "label" button, icon . A list of available placeholders will appear, and you can select and insert items by clicking on the "ok" button;
  - Click "Save" when done, to save the alerting template. The template can now be assigned to an existing or a new action, on the "Actions" tab.



Add or edit alert template

Alert name:
Default Alert Template

Email subject:
FileMonitor Message for activity recorder on {COMPUTER}

Email body:
This is an e-m onitor for
file activity or
information: Ti
type: {STATU

Figure 17: Add or edit an alerting template

To edit an existing alerting template, please click the corresponding “Gear” button, icon ⚙ to open the dialog in Figure 17.

To delete an existing alerting template, please select it, by ticking the corresponding tick box, and click the “Delete” button, icon ✖ .

Adding / editing actions

Prerequisites

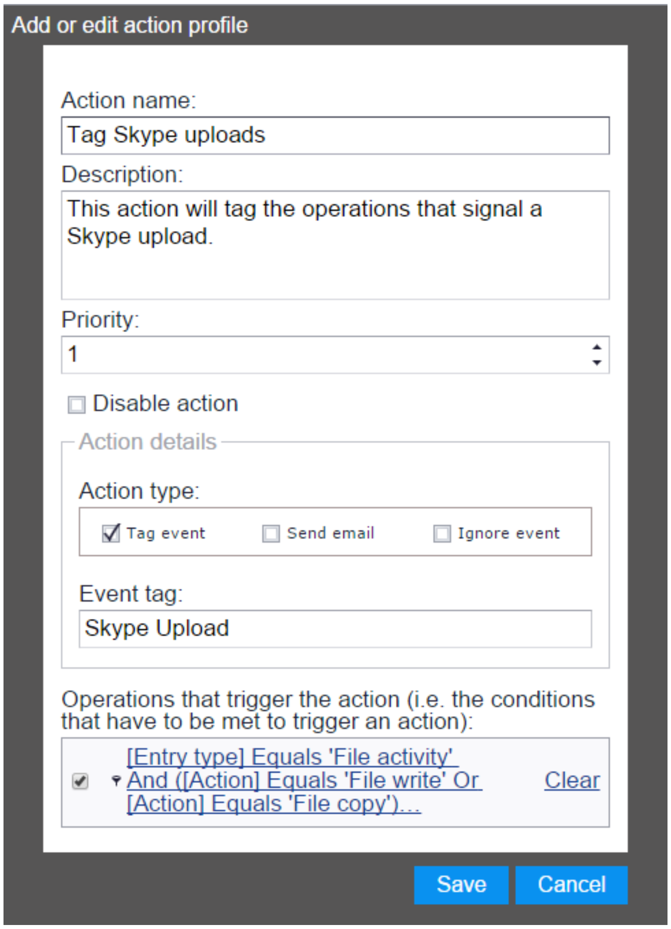
- First, identify the information that you want to be alerted on. For example, when a certain file is copied, or the ACL for files in a certain folder changes;
- Visit chapter 6, subchapter “Event Fields” to find the relevant fields that you need to use for building the appropriate condition for your requirement. In the above example, the condition would be Action = File copy or Action = File security changed;
- Now you know how to match the specifics of your use case to the inners of the product and enable this action to be triggered only in the specific circumstances that you are interested in.

Adding actions

- Click on the “Actions” tab;
- Click on the “Plus” button, icon ⊕, a new dialog will appear;
- Enter a name for the action;
- Optional: enter a description to expand on the use of this action;
- Select a priority:

  Important note: Each event sent to TEMASOFT FileMonitor Server can match a single “Action”. Or, the other way around, if an event comes in, and there are multiple actions that would be triggered by this event, only the action with the lowest priority value (highest priority) will trigger. Hence, priorities are important. You can select them when creating or editing an action, or by dragging actions up and down in the main view. When using this system, for best results, it is advised to have more granular actions with lower priority value (higher priority) and more generic actions with higher priority value (lower priority). Thus, the granular rules will trigger first and leave the rest for the more generic rules.

- Optional: Disable action: tick this tick box if you want to save the action, but not enable it. This is helpful if you are creating configurations for multiple instances, or if you want to have an organized structure of actions you may need, and only enable the ones you want, when you want.
- Action details: here is where you define what the action does:
    - Ignore event: if you tick this tick box, the events that match this action will be ignored; they will not show up in the reports and data viewer;
    - Optional: Event tag: This field enables you to tag the events that match the conditions of this rule with a label. This makes it very easy to find this information at a later stage, or report on it. For example, you can tag all events that involve copying binaries to Windows folder as "important". Then simply create a report and select a condition like Tag = "important" to report on this information;
    - Alert templates: select an alert template which will define how the notification will look like, and what information will the notification contain. Please see the previous section on alerting templates for more details. If you are not sure what to do, please use the default alert template;
    - Email addresses: enter the email addresses that you want the notification to be sent to, when an event that matches the condition of the alert will be collected;
- Define the conditions that need to be met for this action to trigger: click on the "Create Filter" link. A new dialog will appear. Please see chapter 6, subchapter "Using Filters" for information on how to build filters. Please see chapter 6, subchapter "Event Fields" for information on the fields available as filtering conditions, and their possible values.



Add or edit action profile

Action name:
Tag Skype uploads

Description:
This action will tag the operations that signal a Skype upload.

Priority:
1

☐ Disable action

Action details

Action type:
☑ Tag event ☐ Send email ☐ Ignore event

Event tag:
Skype Upload

Operations that trigger the action (i.e. the conditions that have to be met to trigger an action):
☑ [Entry type] Equals 'File activity' And ([Action] Equals 'File write' Or [Action] Equals 'File copy')... Clear

Figure 18: Add or edit action. Example.

Action item options

Hover over the corresponding “Gear” button, icon ⚙to bring up the menu containing the item related options:

- Edit: click on edit if you want to edit this action;
- Delete: click on delete if you want to delete this action; Alternately, you can delete an action by selecting it via the corresponding tick box, and clicking the “Delete” button, icon ✖ ;
- Make a copy: click this option if you want a copy of the action to be created. This is useful when you need to create multiple actions with similar conditions: you can create one, then create copies of it which you can briefly edit to match your needs.

Export existing actions

- To export the existing actions, please click the “Export” button, icon 💾. A zip file with the necessary data will be created and downloaded by the browser to the default download location.

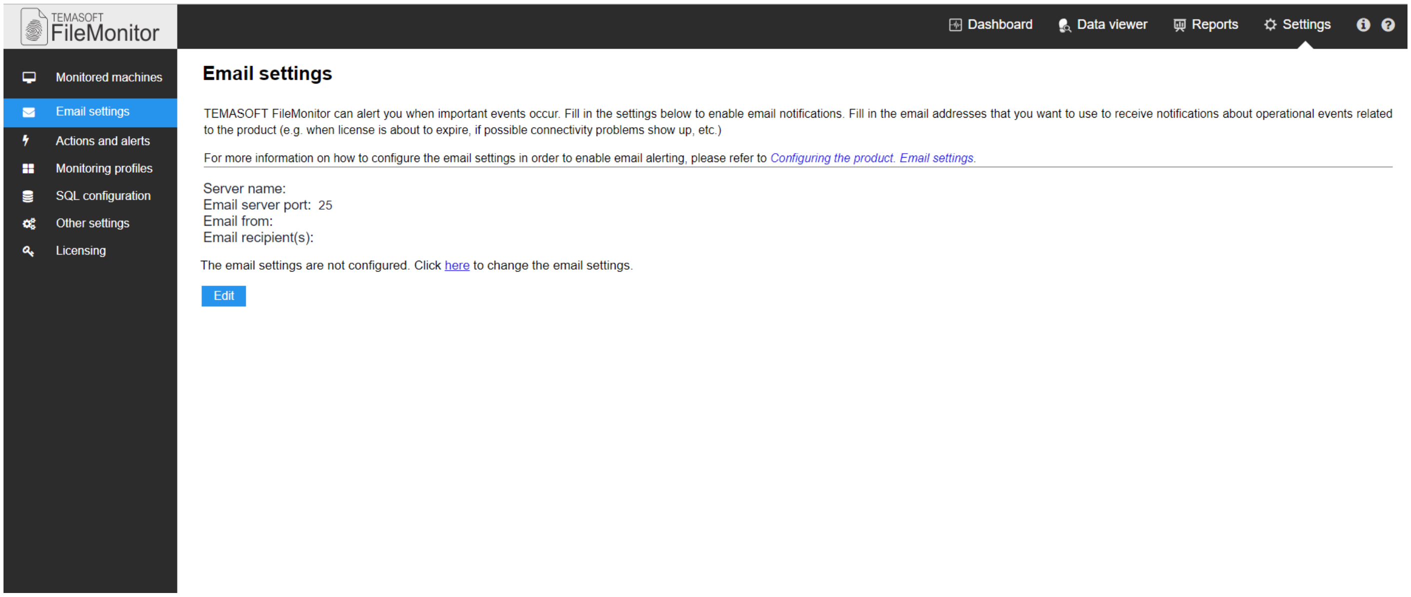
Import existing actions

- To import monitoring profiles, please click the “Import” button, icon ⤒. This action will open a dialog which will allow selection of the file storing the monitoring profiles to import. The dialog expects an XML file and allows import of one action at a time. Such a file is created by using the “export monitoring profiles” option, however, the format in that case is a zip archive of multiple XML files (one for each exported action). Hence, you need to unzip the exported file and select the desired XML file. The XML files have the same name as the original action.

3.4 Email settings

This section describes the configurations needed for enabling email alerting.

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the “Settings” page;
- Select “Email settings” in the left menu;



Email settings

TEMASOFT FileMonitor can alert you when important events occur. Fill in the settings below to enable email notifications. Fill in the email addresses that you want to use to receive notifications about operational events related to the product (e.g. when license is about to expire, if possible connectivity problems show up, etc.)

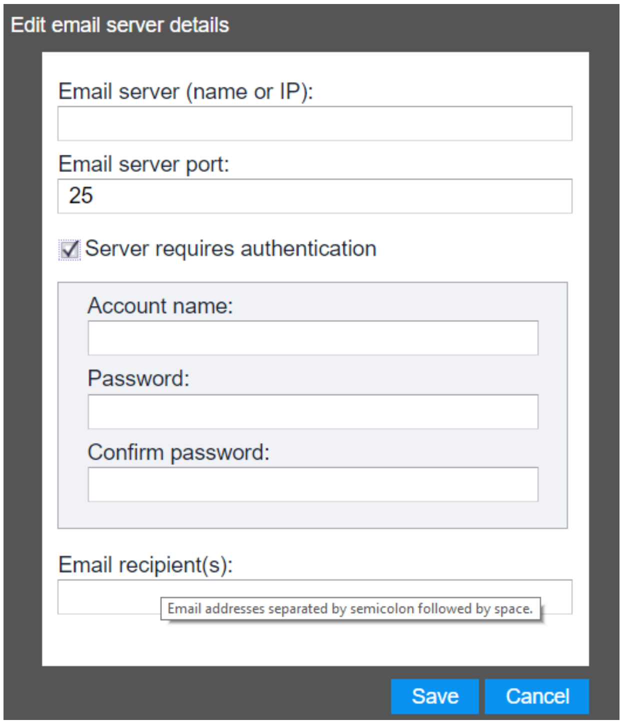
For more information on how to configure the email settings in order to enable email alerting, please refer to *Configuring the product. Email settings.*

Server name:
Email server port: 25
Email from:
Email recipient(s):

The email settings are not configured. Click here to change the email settings.

Figure 19: Email settings page

- Click on the "Edit" button and a new dialog will appear;
    - Enter the name or IP of an email server;
    - Enter the email server communication port;
    - If the server requires authentication, please tick the tick box "Server requires authentication"
        - The dialog will present the authentication options:
            - Account name: enter the account name that you want to use;
            - Password: the password for the account name that you want to use;
            - Confirm password: enter the above password again, for confirmation;
- Email recipient(s): please enter here the email addresses of the administrator(s) of TEMASOFT FileMonitor. These email addresses will be used for system notifications about updates, licensing, and eventual product issues; Please note that these email addresses will NOT be used for notifications generated because of a product action, as defined in chapter 3, subchapter "Actions and alerting". Email addresses for those notifications are defined in the action settings. For more information, please see chapter 3, subchapter "Actions and alerting".
- Click "Save" to save the settings.


Edit email server details

Email server (name or IP):

Email server port: 25

☑ Server requires authentication

Account name:

Password:

Confirm password:

Email recipient(s):

Email addresses separated by semicolon followed by space.

Figure 20: Email server details configuration

3.5 Database settings

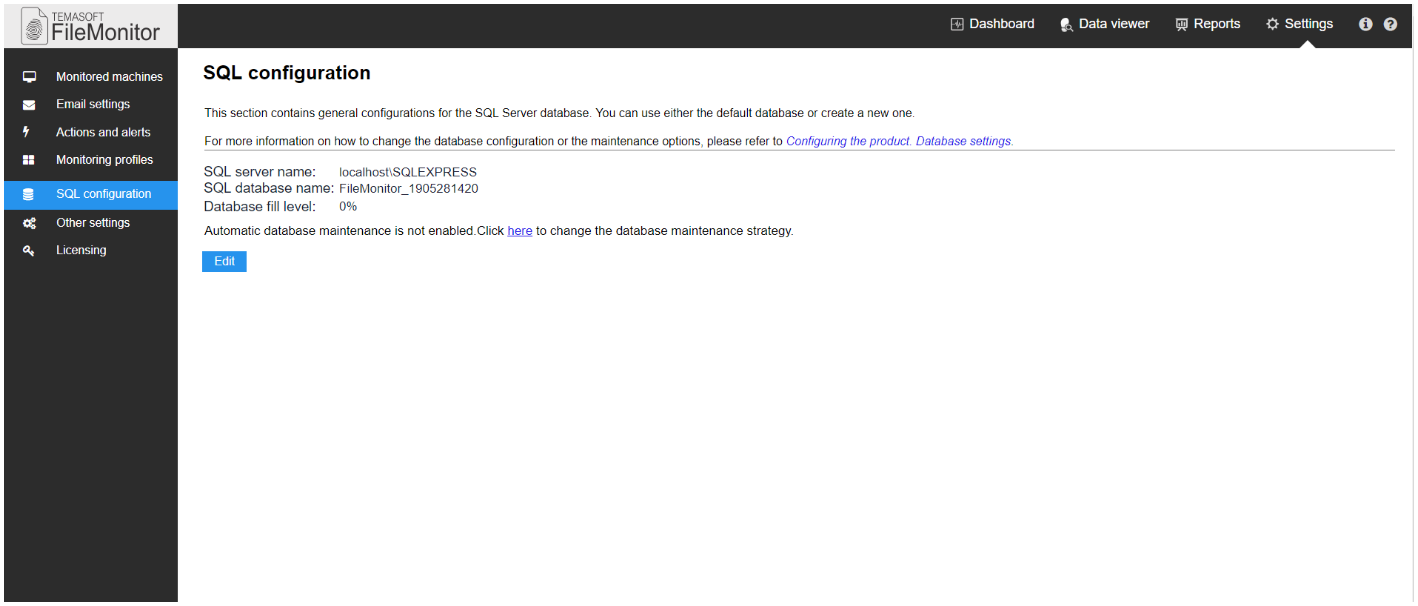
TEMASOFT FileMonitor Server stores the file and application activity received from TEMASOFT FileMonitor Agents, in an SQL Server database. The post install configuration wizard allows configuring the database on an existing Microsoft SQL Server™ instance (including existing Express or Compact editions). Using this option implies filling in information about the type of authentication to be used (Windows integrated, or SQL Server authentication) together with the necessary details such as user name and password, if the case. TEMASOFT FileMonitor Server requires DBO rights on the TEMASOFT FileMonitor database and CREATE_DATABASE right on the database server. Alternately, if there are no such instances available, the wizard can deploy an SQL Server Express edition on the machine and use it as database backend.

Changing / adding an SQL Server configuration

If you have skipped the above step during the post install configuration, or if you wish to change the database backend configuration or the maintenance options, you can do so in the "Settings" section of the TEMASOFT FileMonitor Server Console by following the below steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace "localhost" with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the "Settings" page;
- Select "SQL Configuration" in the left menu;

- A new page will be displayed showing the current SQL Server settings and database maintenance options;



SQL configuration

This section contains general configurations for the SQL Server database. You can use either the default database or create a new one.

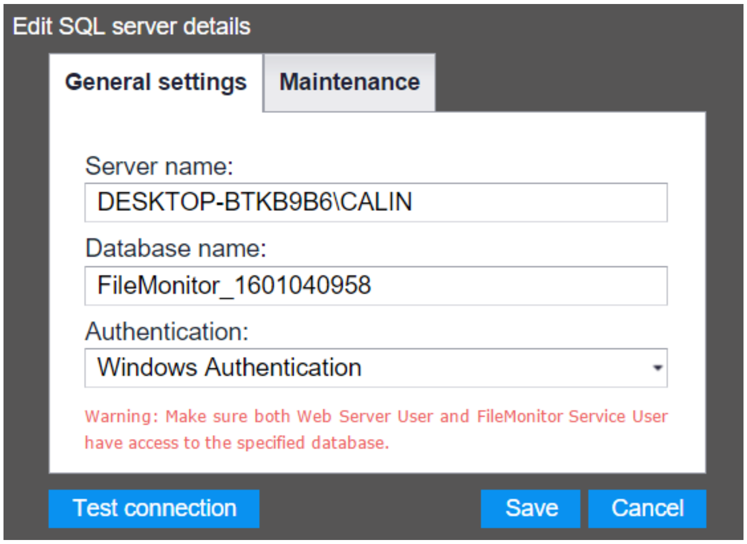
For more information on how to change the database configuration or the maintenance options, please refer to *Configuring the product. Database settings.*

SQL server name: localhost\SQLEXPRESS
SQL database name: FileMonitor_1905281420
Database fill level: 0%

Automatic database maintenance is not enabled.Click here to change the database maintenance strategy.

Figure 21: SQL Configuration page

- To change or add an SQL Server configuration please click the "Edit" button;
  - A new dialog will appear;
  - Enter the SQL Server instance name;
    - If you are running SQL Server on a custom port, enter that port after the SQL Server instance name, separated by a comma (example: MySQLInstance1,1200)
  - Select the authentication type: Windows integrated or SQL Server authentication;
  - Enter a name for the TEMASOFT FileMonitor Database;
  - If the latter, provide an SQL Server logon and password with enough rights to:
    - Connect to the SQL Server instance;
    - Create database;
    - Take ownership of the database to perform maintenance, if needed;
  - Optional (recommended): Click the "test connection" button to make sure the settings are correct;
  - Click "Save" to save your configuration.



Server name: DESKTOP-BTKB9B6\CALIN

Database name: FileMonitor_1601040958

Authentication: Windows Authentication

Warning: Make sure both Web Server User and FileMonitor Service User have access to the specified database.

Figure 22: SQL server details

Important note: The database configured in this section will be used to store newly collected information. However, the UI layers exposing TEMASOFT FileMonitor data, such as Reporting or Data viewer, allow independent connectivity to other (distinct) TEMASOFT FileMonitor databases. You can see the current database being used by these UI layers at the top of the corresponding page and you can change the current database from there. More information will be provided in the corresponding sections of this manual for reporting and data analysis.

Changing / adding database maintenance options

The database containing the TEMASOFT FileMonitor data can grow large in time and this may influence the performance of reporting or data collection. In such circumstances, it is advised to implement a database maintenance policy, depending on the retention needs and available hardware resources. To implement a database maintenance policy, please follow these steps:

- Click the “Edit” button on the page in Figure 22 showing the current SQL Server settings and database maintenance options;
- On the dialog in Figure 22, navigate to the “Maintenance” tab;
- Tick the “Enable database maintenance” tick box; New options will become available via two radio buttons: database rotation and database cleanup;
    - Choose rotation to rotate the databases (create a new database) when certain criteria are met;
        - Select when to perform database rotation (weekly or monthly);
        - Set a limit to the number of databases created by the database rotation mechanism;
    - Choose cleanup if you do not need to store information for more than a certain period;
        - Choose when the cleanup operation runs: daily, weekly, monthly;
- Click “Save” to save your configuration.

Notes on database maintenance

The database maintenance jobs work in the following way:

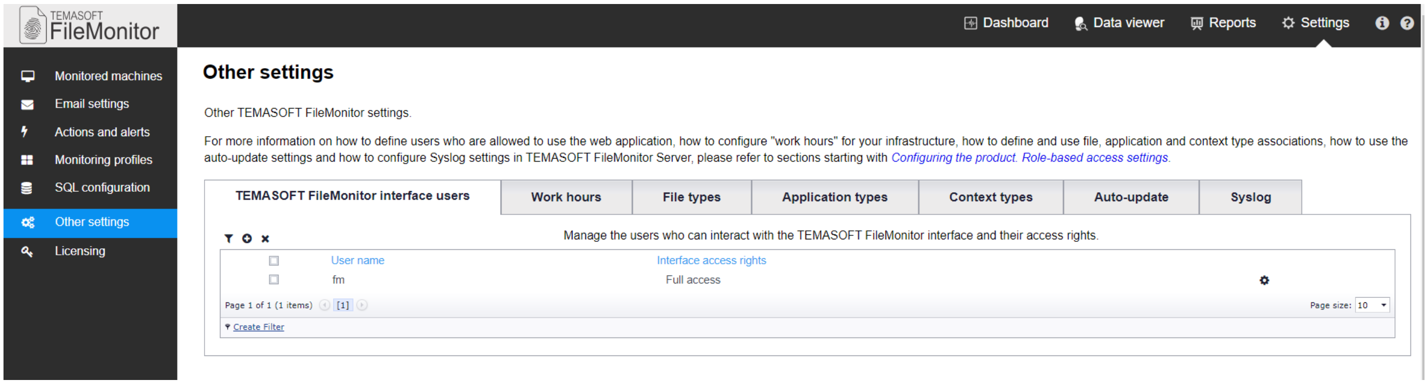
- If the database maintenance is on, TEMASOFT FileMonitor will execute an index defragmentation operation between 00:00 and 01:00 AM, if the average fragmentation of the indexes is over 25%;
- When using SQL Server Express – where there is a 10 GB limitation for the database size – the database rotation schedule may be ignored, because TEMASOFT FileMonitor will automatically rotate the database when it reaches the maximum allowed database size; If the database does not reach the maximum size, the rotation operations take place as scheduled (weekly or monthly), between 00:00 and 01:00 AM;

- The DB cleanup operation runs as scheduled (daily, weekly, monthly) between 00:00 and 01:00 AM; If an operation is missed because the server is down between 00:00 and 1:00 AM, then the cleanup operation will run immediately after the sever is started;

3.6 Role-based access settings

Role-base access to the TEMASOFT FileMonitor Console allows definition of the Windows users who can use the web application, as well as the type of access granted to each allowed user: no access, full access or read-only access. Read-only access allows the user to view the data, but prevents him or her from changing the product configuration. To configure role-based access to the TEMASOFT FileMonitor Server Console, please follow the below steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the “Settings” page;
- Click on “Other settings” in the left menu; A new view will load;
- Navigate to the “Users” tab;
- The tab contains a list of users who have access to the TEMASOFT FileMonitor Server Console, and their access rights. By default, the user who has installed TEMASOFT FileMonitor Server has full access and will be listed as such in this view;



Other settings

Other TEMASOFT FileMonitor settings.

For more information on how to define users who are allowed to use the web application, how to configure "work hours" for your infrastructure, how to define and use file, application and context type associations, how to use the auto-update settings and how to configure Syslog settings in TEMASOFT FileMonitor Server, please refer to sections starting with *Configuring the product. Role-based access settings.*

Manage the users who can interact with the TEMASOFT FileMonitor interface and their access rights.

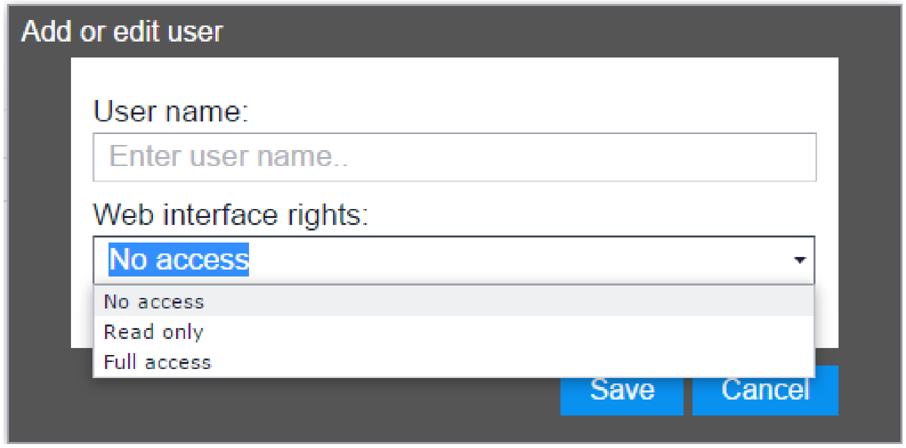
	User name	Interface access rights
□	fm	Full access

Figure 23: Manage role-based access

Adding or editing user access rights

You can add new users and assign rights by clicking on the “Plus” button, icon ⊕. A new dialog will open.

- Enter the user name you wish to assign rights to access the TEMASOFT FileMonitor Server Console;
- Enter the desired right. Possible values:
    - No access: this will prevent the user from accessing the TEMASOFT FileMonitor Server Console;
    - Access interface read-only: this will allow the user to access the TEMASOFT FileMonitor Server Console and view the information collected by TEMASOFT FileMonitor agents. It will not allow the user to modify anything;
    - Full access: this option will give the user full access to all the functions of TEMASOFT FileMonitor Server Console;
    - Click on the “Save” to save your configuration.



Add or edit user

User name:

Enter user name..

Web interface rights:

No access

Figure 24: Add or edit user access rights

For editing an entry, please use the following steps:

- Hoover the “gear” button, icon ⚙ corresponding to the entry that you want to edit;
- The “Edit” and “Delete” options will become available.

Deleting users

To remove a user from the list, simply select him /her by ticking the corresponding tick box and click the “Delete” button. Alternately, you can delete entries by hovering the “Gear” button and selecting the “delete” option.

Filtering the view

When managing rights for many user accounts, the filter functionality will allow you to find users or access rights easily. Please follow this procedure:

- Click on the “Filter” button, icon ▼ ;
- A new dialog will open, allowing you to create a filter based on the following parameters:
  - User name: this is the user name of the users who have access rights assigned;
  - Web interface access: this represents the type of access that is assigned to the users. Possible values: No access, Access interface read-only and full access.
  - For example, if you want to only see the users who have full access, create a filter with a condition like “Web interface access = Full access”

For more information on how to use the Filter Builder dialog, please see chapter 6, subchapter “Using filters”.

Sorting the view

You can sort the list of users based on their names, by clicking on the “user name” column name link. Alternately, you can sort the view based on the type of access right, by clicking the “Web interface access” column name link in the view.

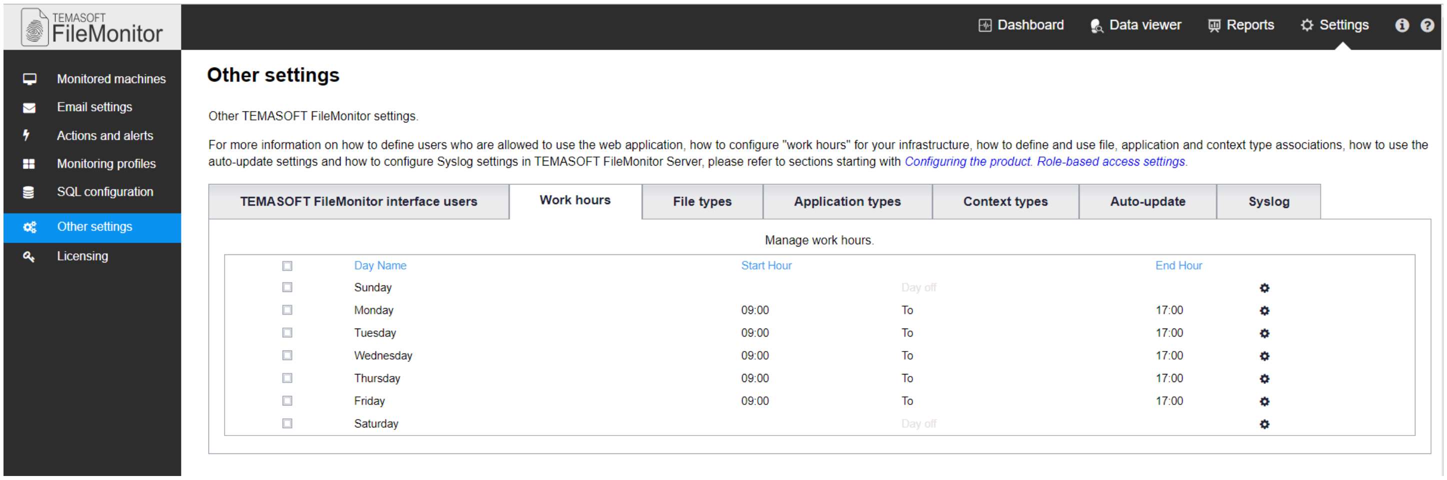
3.7 Normal work hours settings

This section describes how to configure “work hours” for your infrastructure. These settings enable TEMASOFT FileMonitor to act differently on important operations, depending on whether they were carried out during or outside work hours. When configuring “actions and alerts” as per chapter 3, subchapter “Actions and Alerts”, you can create a triggering condition for the actions, that would assess if the time of occurrence is during our outside the configured “work hours" of your business infrastructure by using the "In work hours" parameter and the "true" or "false" values. For example, such a condition may be: "File name" contains "my important file" and "In work hours" equals "False".

To configure normal work hours, please follow the below steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace "localhost" with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the "Settings" page;
- Click on "Other settings" in the left menu; A new view will load;
- Navigate to the "Work hours" tab;

A list of the days of the week, together with the configured time interval, will appear. By default, the work hours are configured to include Monday to Friday from 9 AM to 5PM.



Other settings

Other TEMASOFT FileMonitor settings.

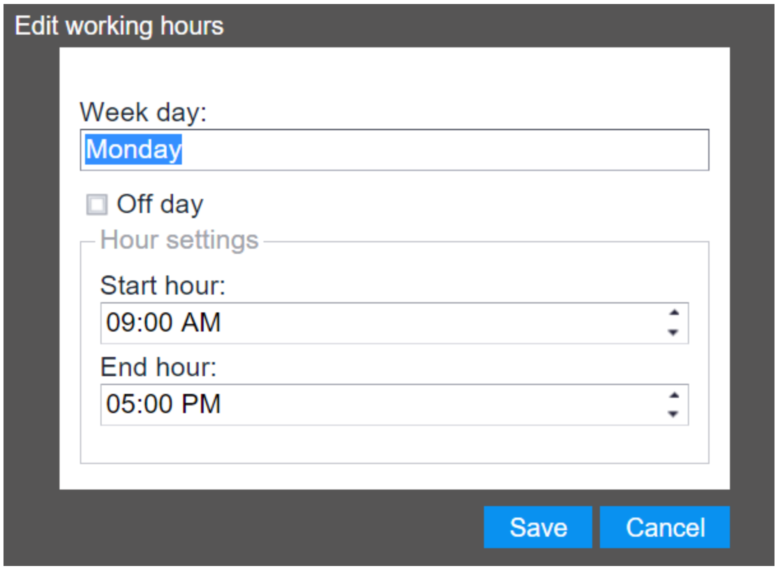
For more information on how to define users who are allowed to use the web application, how to configure "work hours" for your infrastructure, how to define and use file, application and context type associations, how to use the auto-update settings and how to configure Syslog settings in TEMASOFT FileMonitor Server, please refer to sections starting with *Configuring the product. Role-based access settings.*

Manage work hours.

□	Day Name	Start Hour		End Hour	
□	Sunday		Day off		⚙
□	Monday	09:00	To	17:00	⚙
□	Tuesday	09:00	To	17:00	⚙
□	Wednesday	09:00	To	17:00	⚙
□	Thursday	09:00	To	17:00	⚙
□	Friday	09:00	To	17:00	⚙
□	Saturday		Day off		⚙

Figure 25: Configuring normal work hours

- Next, you can adjust the interval for a day of the week by hovering over the "Gear" button, icon ⚙ corresponding to the day that you wish to edit and selecting the "Edit" option. You can also select multiple days (for example Monday to Friday) and click the same button corresponding to any of the selected days. This will cause the settings to apply to all the selected items, after the configuration is made in the dialog which appears;
- A new dialog will appear which will allow configuring:
  - The day as a day off – using the "Off day" tick box;
  - The work hours (if the day is not a day off) interval:
    - Start hour: the time when the work hours begin;
    - End hour: the time when the work hours end;
  - Click "Save" to save your settings.



Edit working hours

Week day: Monday

□ Off day

Hour settings

Start hour: 09:00 AM

End hour: 05:00 PM

Figure 26: Configuring work hour's details

For more information on fields available for actions, reporting and data viewing filters, please see chapter 6, subchapter "Event fields".

3.8 File types settings

This section describes how to define and use file type associations. File type associations are made based on the extension of the files which make the scope of the file-related activity. Defining such associations allow you to configure TEMASOFT FileMonitor to take action differently or present the information in the reports or data viewer differently, depending on the file extension. For example, you might want to see files being created in Windows system folders, but only if they are executables or binaries (which may pose a threat outside Windows updating or similar management tasks) while you would want to ignore other files being created there (as they are created as part of normal Windows operations).

TEMASOFT FileMonitor comes with a predefined list of file type associations, as follows:

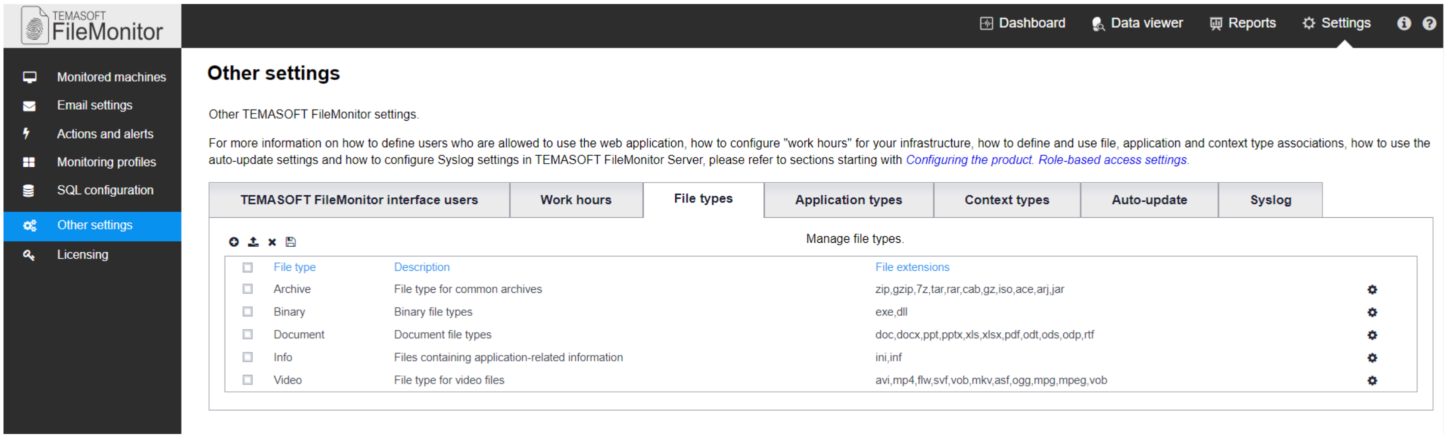
File type	**Extensions**
Archive	zip, gzip, 7z, tar, rar, cab, gz, iso, ace, arj, jar
Document	doc, docx, txt, csv, ppt, pptx, xls, xlsx, pdf, odt, ods, odp, rtf
Binary	exe, dll
Videos	avi,mp4,flw,svf,vob,mkv,asf,ogg,mpg,mpeg,vob

Figure 27: List of default file types

You can add more file type associations, or edit the currently available ones by following these steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace "localhost" with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the "Settings" page;
- Click on "Other settings" in the left menu; A new view will load;
- Navigate to the "File types" tab;

A list of available file types will be presented, together with the necessary management options.



Other settings

Other TEMASOFT FileMonitor settings.

For more information on how to define users who are allowed to use the web application, how to configure "work hours" for your infrastructure, how to define and use file, application and context type associations, how to use the auto-update settings and how to configure Syslog settings in TEMASOFT FileMonitor Server, please refer to sections starting with *Configuring the product. Role-based access settings.*

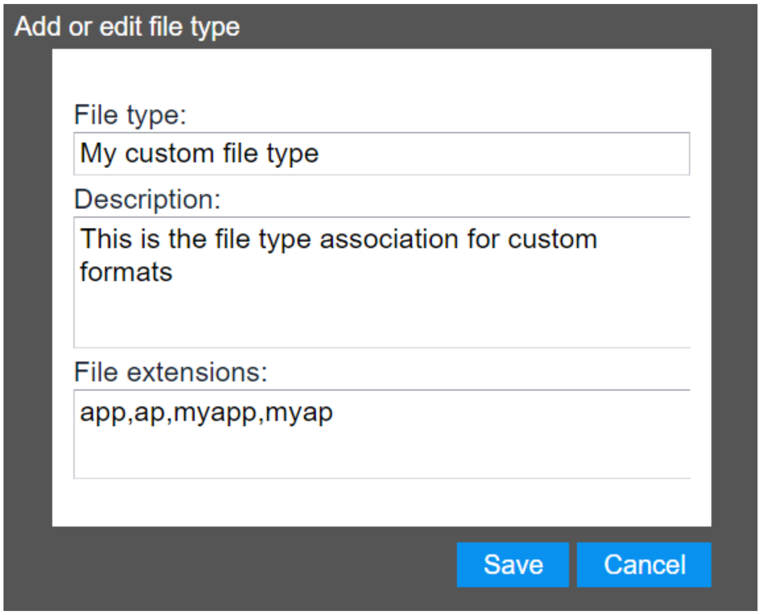
Manage file types.

	File type	Description	File extensions	
□	Archive	File type for common archives	zip,gzip,7z,tar,rar,cab,gz,iso,ace,arj,jar	⚙
□	Binary	Binary file types	exe,dll	⚙
□	Document	Document file types	doc,docx,ppt,pptx,xls,xlsx,pdf,odt,ods,odp,rtf	⚙
□	Info	Files containing application-related information	ini,inf	⚙
□	Video	File type for video files	avi,mp4,flw,svf,vob,mkv,asf,ogg,mpg,mpeg,vob	⚙

Figure 28: Configuring file types

Adding file types

- Next, to add new file type associations, click the “Plus” button, icon ⊕; a new dialog will appear;
  - Enter the name of the file type: This is important because this name will be used to create reports, actions or filtered views, based on this file type.
  - Optional: enter a description for this file type association;
  - File extensions: enter the file extensions that you wish to be associated with this file type, without the dot, separated by commas, as it can be seen in figure 29;
  - Click “Save” to save your configuration.



File type: My custom file type

Description: This is the file type association for custom formats

File extensions: app,ap,myapp,myap

Figure 29: Adding or editing a file type

Editing a file type

To edit an existing file type, hover over the corresponding “Gear” button, icon ⚙ and select the “Edit” option. The dialog in figure 29 will appear. Alternately, you can edit several entries at the same time, by selecting them using their associated tick boxes, and clicking the “Gear” button of any of them.

Deleting a file type

To delete an existing file type, hover over the corresponding “Gear” button, icon ⚙ and select the “Delete” option. Alternately, select the item using its corresponding tick box, and click the “Delete” button, icon ✖. You can delete several entries at the same time, by selecting them using their associated tick boxes, and clicking the “Delete” button.

Exporting the list of file types

To export the list of file types, please click on the “Export” button, icon 💾. This will create a zip archive containing the exported file profiles, each in xml format. The archive will be downloaded by the browser in the default downloads folder.

Importing file types

To import file types, please click the “Import” button, icon ⤒. This will prompt for the path to a file that contains the information, in XML format. Unzip the exported list of file types and select the file type that you wish to import.

Sorting the list of file types

To sort the list of file types, simply click the column that you want to sort by. Clicking again will reverse the sort order.

3.9 Application types settings

This section describes how to define and use application type associations. Application type associations are made based on lists of partial or full program names related to file operations. Defining such associations allow you to configure TEMASOFT FileMonitor to take action differently or present the information in the reports or data viewer differently, depending on the application. For example, you might want to see files being handled by browsers.

TEMASOFT FileMonitor comes with a predefined list of application type associations, as follows:

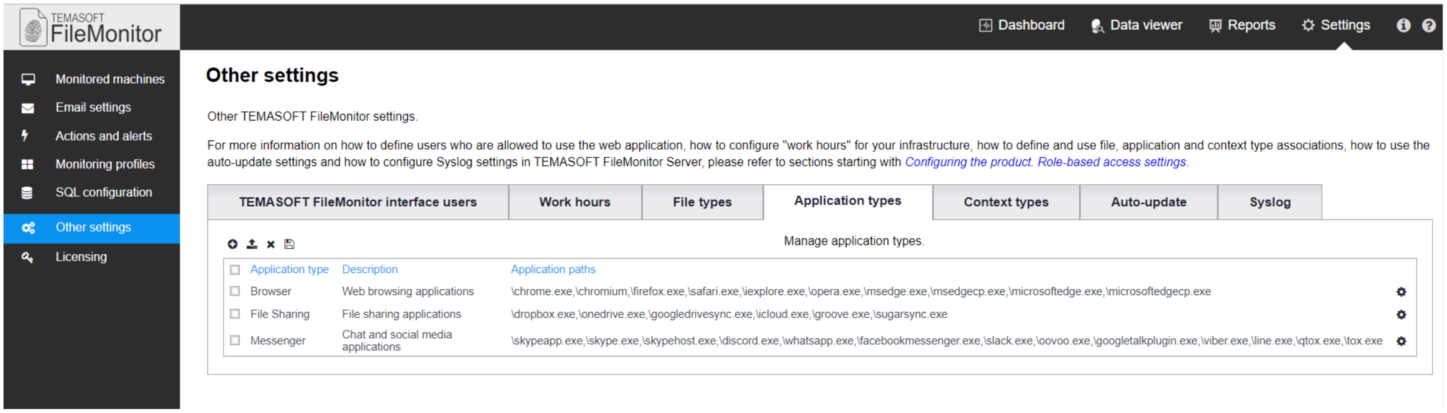
Application type	**Application paths**
Browser	\chrome.exe,\chromium,\firefox.exe,\safari.exe,\iexplore.exe,\opera.exe,\msedge.exe,\msedgecp.exe,\microsoftedge.exe,\microsoftedgecp.exe
File Sharing	\dropbox.exe,\onedrive.exe,\googledrivesync.exe,\icloud.exe,\groove.exe,\sugarsync.exe
Messenger	\skypeapp.exe,\skype.exe,\skypehost.exe,\discord.exe,\whatsapp.exe,\facebookmessenger.exe,\slack.exe,\oovoo.exe,\googletalkplugin.exe,\viber.exe,\line.exe,\qtox.exe,\tox.exe

Figure 30: List of default application types

You can add more file type associations, or edit the currently available ones by following these steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the “Settings” page;
- Click on “Other settings” in the left menu; A new view will load;
- Navigate to the “Application types” tab;

A list of available application types will be presented, together with the necessary management options.



Other settings

Other TEMASOFT FileMonitor settings.

For more information on how to define users who are allowed to use the web application, how to configure "work hours" for your infrastructure, how to define and use file, application and context type associations, how to use the auto-update settings and how to configure Syslog settings in TEMASOFT FileMonitor Server, please refer to sections starting with *Configuring the product. Role-based access settings*.

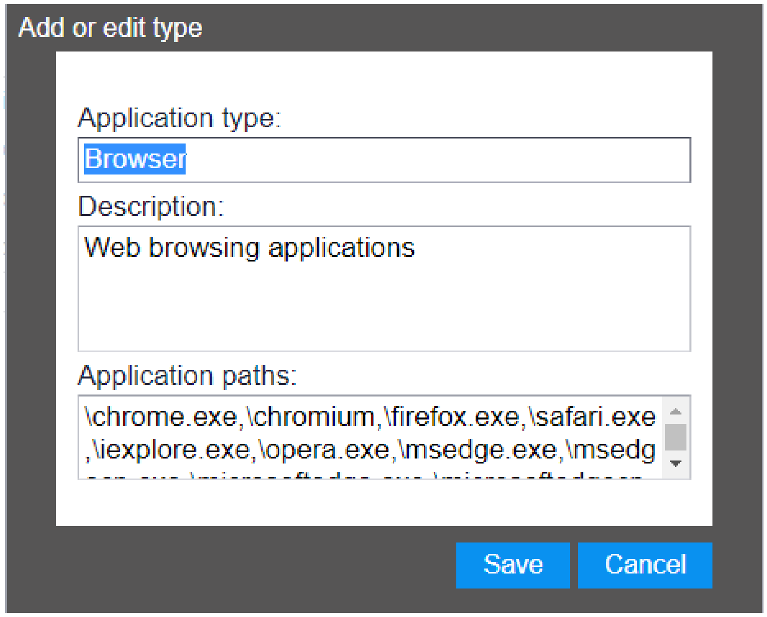
Manage application types.

□	Application type	Description	Application paths
□	Browser	Web browsing applications	\chrome.exe,\chromium,\firefox.exe,\safari.exe,\iexplore.exe,\opera.exe,\msedge.exe,\msedgecp.exe,\microsoftedge.exe,\microsoftedgecp.exe
□	File Sharing	File sharing applications	\dropbox.exe,\onedrive.exe,\googledrivesync.exe,\icloud.exe,\groove.exe,\sugarsync.exe
□	Messenger	Chat and social media applications	\skypeapp.exe,\skype.exe,\skypehost.exe,\discord.exe,\whatsapp.exe,\facebookmessenger.exe,\slack.exe,\oovoo.exe,\googletalkplugin.exe,\viber.exe,\line.exe,\qtox.exe,\tox.exe

Figure 31: Configuring application types

Adding application types

- Next, to add new file type associations, click the “Plus” button, icon ⊕; a new dialog will appear;
  - Enter the name of the application type: This is important because this name will be used to create reports, actions or filtered views, based on this type;
  - Optional: enter a description for this type association;
  - Application paths: enter the application partial or complete paths that you wish to be associated with this file type, separated by commas, as it can be seen in figure 31. For each file operation performed by a program, the full path of the application will be checked to see if it contains any of the application paths associated with the application type. If there is at least a match, the name of the application type will be written in the “Application Type” field of the event;
  - Click “Save” to save your configuration.



Add or edit type

Application type: Browser

Description: Web browsing applications

Application paths: \chrome.exe,\chromium,\firefox.exe,\safari.exe,\iexplore.exe,\opera.exe,\msedge.exe,\msedg

Figure 32: Adding or editing an application type

Editing an application type

To edit an existing application type, hover over the corresponding “Gear” button, icon ⚙ and select the “Edit” option. The dialog in figure 32 will appear. Alternately, you can edit several entries at the same time, by selecting them using their associated tick boxes, and clicking the “Gear” button of any of them.

Deleting an application type

To delete an existing application type, hover over the corresponding “Gear” button, icon ⚙ and select the “Delete” option. Alternately, select the item using its corresponding tick box, and click the “Delete” button, icon ✖. You can delete several entries at the same time, by selecting them using their associated tick boxes, and clicking the “Delete” button. The “Browser” application type cannot be deleted.

Exporting the list of application types

To export the list of application types, please click on the “Export” button, icon 💾. This will create a zip archive containing the exported types, each in xml format. The archive will be downloaded by the browser in the default downloads folder.

Importing application types

To import application types, please click the “Import” button, icon ⬆. This will prompt for the path to a file that contains the information, in XML format. Unzip the exported list of application types and select the type that you wish to import.

Sorting the list of application types

To sort the list of application types, simply click the column that you want to sort by. Clicking again will reverse the sort order.

3.10 Context types settings

This section describes how to define and use context type associations. Context type associations are made based on lists of keywords related to file operations. Defining such associations allow you to configure TEMASOFT FileMonitor to take action differently or present the information in the reports or data viewer differently, depending on certain keywords that might show up in the “Details” field of the event, for file read and write operations. For example, you might want to see files being uploaded to web file transfer sites.

TEMASOFT FileMonitor comes with a predefined list of context type associations, as follows:

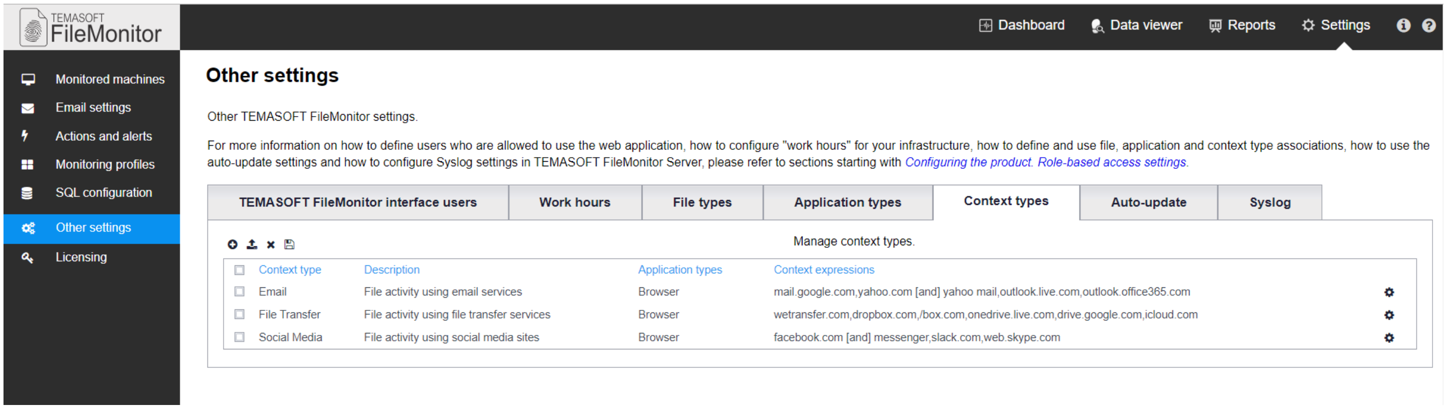
Context type	**Application paths**
Email	mail.google.com,yahoo.com [and] yahoo mail,outlook.live.com,outlook.office365.com
File Transfer	wetransfer.com,dropbox.com,/box.com,onedrive.live.com,drive.google.com,icloud.com
Social Media	facebook.com [and] messenger,slack.com,web.skype.com

Figure 33: List of default context types

You can add more context type associations, or edit the currently available ones by following these steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the “Settings” page;
- Click on “Other settings” in the left menu; A new view will load;
- Navigate to the “Context types” tab;

A list of available context types will be presented, together with the necessary management options.



Other settings

Other TEMASOFT FileMonitor settings.

For more information on how to define users who are allowed to use the web application, how to configure "work hours" for your infrastructure, how to define and use file, application and context type associations, how to use the auto-update settings and how to configure Syslog settings in TEMASOFT FileMonitor Server, please refer to sections starting with *Configuring the product. Role-based access settings*.

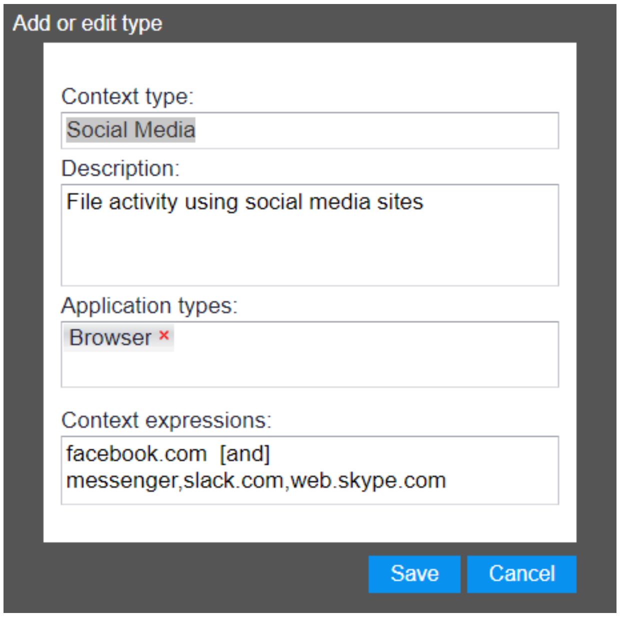
Manage context types.

□	Context type	Description	Application types	Context expressions
□	Email	File activity using email services	Browser	mail.google.com,yahoo.com [and] yahoo mail,outlook.live.com,outlook.office365.com
□	File Transfer	File activity using file transfer services	Browser	wetransfer.com,dropbox.com,/box.com,onedrive.live.com,drive.google.com,icloud.com
□	Social Media	File activity using social media sites	Browser	facebook.com [and] messenger,slack.com,web.skype.com

Figure 34: Configuring application types

Adding context types

- Next, to add new file context associations, click the "Plus" button, icon ⊕; a new dialog will appear;
  - Enter the name of the context type: This is important because this name will be used to create reports, actions or filtered views, based on this type;
  - Optional: enter a description for this type association;
  - Application types: optionally, choose to which application types this context applies;
  - Context expressions: enter a list of keyword expressions that you wish to be associated with this file type, separated by commas, as it can be seen in figure 34. A keyword expression can contain a single, or multiple keywords joined by the [and] operator. If the context type specifies application types, they will be matched first when a new file read or write operation event is processed. Then the "Details" field of the event will be checked to see if it contains any of the keyword expressions associated with the application type (if [and] is used, all the joined keywords must be present in the "Details" field to be considered a match). If there is at least a match, the name of the application type will be written in the "Context Type" field of the event;
  - Click "Save" to save your configuration.



Context type:
Social Media

Description:
File activity using social media sites

Application types:
Browser ×

Context expressions:
facebook.com [and] messenger,slack.com,web.skype.com

Figure 35: Adding or editing an application type

Editing a context type

To edit an existing context type, hover over the corresponding “Gear” button, icon ⚙ and select the “Edit” option. The dialog in figure 35 will appear. Alternately, you can edit several entries at the same time, by selecting them using their associated tick boxes, and clicking the “Gear” button of any of them.

Deleting a context type

To delete an existing context type, hover over the corresponding “Gear” button, icon ⚙ and select the “Delete” option. Alternately, select the item using its corresponding tick box, and click the “Delete” button, icon ✖. You can delete several entries at the same time, by selecting them using their associated tick boxes, and clicking the “Delete” button.

Exporting the list of context types

To export the list of context types, please click on the “Export” button, icon 💾. This will create a zip archive containing the exported types, each in xml format. The archive will be downloaded by the browser in the default downloads folder.

Importing context types

To import context types, please click the “Import” button, icon ⭱ . This will prompt for the path to a file that contains the information, in XML format. Unzip the exported list of context types and select the type that you wish to import.

Sorting the list of context types

To sort the list of application types, simply click the column that you want to sort by. Clicking again will reverse the sort order.

3.11 Auto-update settings

This section describes how to use the auto-update settings of TEMASOFT FileMonitor. Auto-updates enable the product to automatically download and install updates such as patches or improvements. It is recommended that the auto-update is enabled, and it is so by default. If you wish to change this setting, please follow the below procedure:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the “Settings” page;
- Click on “Other settings” in the left menu; A new view will load;
- Navigate to the “Auto-update” tab;

A page showing the status of auto-update will be presented. If you wish to change the status, press the “enable” / “disable” button (label and function depends on the present setting)

3.12 Syslog settings

This section contains the port settings for the Syslog receiver included in the TEMASOFT FileMonitor Server Service component. By default, the listener can receive messages on UDP port 514, but the value and the protocol can be customized. If the listener only uses one protocol, then the port for the other protocol should be set to 0. If Syslog messages are not needed at all, one should disable the receiver by setting both the TCP and UDP ports to 0.

3.13 Licensing

License file and license units

TEMASOFT FileMonitor can be used to scan different types of devices, each such device being licensed depending on the type and the operating system. These devices can be monitored using licensing units. A license file contains license units that can be assigned to the systems that need to be tracked. Clients purchase one or more license units which are typically bundled in a single license file that can be loaded in TEMASOFT FileMonitor.

Types of license keys

There are two types of license files that can be used by TEMASOFT FileMonitor:

- Commercial license file: this requires activation as per the steps in the paragraph below. The product will function for a period and thus allow the activation process to take place after the key has been entered and the product has been used. However, if the license is not activated in time, the product will cease to function. Customers who do not activate their license cannot receive support.
- Evaluation license file: this does not require activation and can be used to monitor a certain number of machines for a specified period of time.

Types of nodes

There are two types of nodes that are subject to the TEMASOFT FileMonitor licensing:

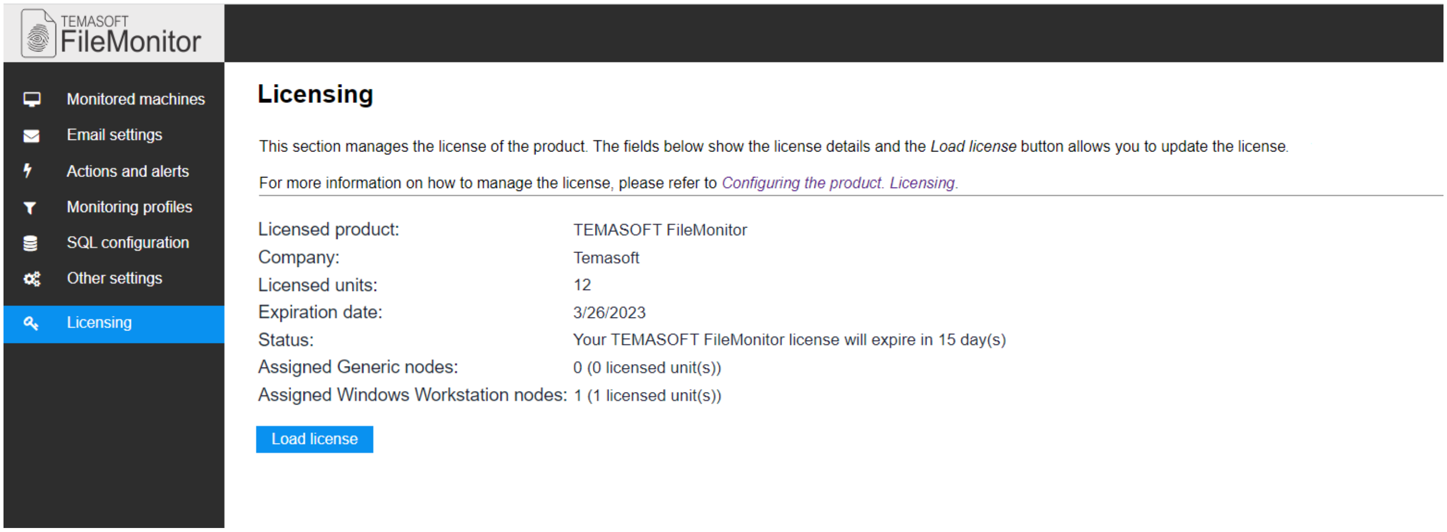
- Windows workstation nodes: nodes that refer to Windows workstations ONLY. One license unit can cover several such nodes;
- Generic nodes (or machines): they refer to devices that are not Windows workstations (i.e. supported Windows servers and NAS machines). In general, each such node consumes a license unit.

How to carry out the licensing process

TEMASOFT FileMonitor requires a license file and an internet connection to register and activate the license. This license file is received from TEMASOFT via email, either as part of the download registration process (for evaluating users) or as part of the sales process (for customers). To see the licensing status and manage the license, please follow these steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the “Settings” page;
- Click on “Licensing” in the left menu; A new page will load;

This window contains the license details such as licensed product version, the number of license units, the company name, license expiration date, license status (expired or not) and the number of generic and Windows workstation nodes in use and the assigned license units. To change the license, you need to click on the “load license file” button. To complete the process, you will be required a license file that is provided to you by TEMASOFT or its partners.



Licensing

This section manages the license of the product. The fields below show the license details and the *Load license* button allows you to update the license.

For more information on how to manage the license, please refer to *Configuring the product. Licensing*.

Licensed product:	TEMASOFT FileMonitor
Company:	Temasoft
Licensed units:	12
Expiration date:	3/26/2023
Status:	Your TEMASOFT FileMonitor license will expire in 15 day(s)
Assigned Generic nodes:	0 (0 licensed unit(s))
Assigned Windows Workstation nodes:	1 (1 licensed unit(s))

Figure 36: TEMASOFT FileMonitor licensing

4 Collecting File Operation Data

4.1 Collecting process and file operations information from Windows machines

TEMASOFT FileMonitor uses agents to record the file activity on remote Windows computers. The TEMASOFT FileMonitor agent relies on a kernel mode driver to capture the changes as they occur and collect all the necessary information relevant to each operation. It can record the following type of information:

- Basic file and folder operations: read, write, delete, attributes changes, security attributes changes (changes to the file ACL);
- Advanced file operations: file copy and file content duplication, irrespective of the application responsible for copying the file and how it performs the actual copy (via a file copy API, or via read / write sequences), as well as irrespective of the destination of the new file (network, USB / removable storage device, etc.) as well as file renamed, file archived, file uploaded by browser and file attached to an email (via Outlook);
- Applications and process activity: process created, and process stopped;
- User activity related to files and applications;
- The activity of users with administrative privileges;
- The files being changed;
- File integrity through file content hashing;

The difference between file copy and file content duplicated

TEMASOFT FileMonitor can detect most copy operations, involving normal activities and normally used files. However, if the file being copied is intensively used by multiple processes at the same time, (as is the case with log files, for example), the file copy operation may not be detected. In addition to that, there are some situations where TEMASOFT FileMonitor detects a file copy operation, but because of the data and processes in the memory, it cannot tell for sure where the source file of the file copy operation is. In this case, a “file content duplicated” event will be logged. The destination file name will contain the path and file name of the file to which the content was copied, and the “details” field will contain a list of possible file sources for the file copy operation. Although the product cannot pinpoint which one of the possible sources is the actual source, for sure one of them is the source file.

For each operation, TEMASOFT FileMonitor provides information about the timestamp, user, application (including executable path, PID) and other operation specific details such as determine if an operation was performed by a user with administrative privileges or if the operation resulted in a change of the file.

To be able to collect this information, the following flow is required:

- Install TEMASOFT FileMonitor Server – for details, please see chapter 2 of this manual;
- Configure TEMASOFT FileMonitor Server and deploy TEMASOFT FileMonitor Agents – for details, please see chapter 3 of this manual;
- At this point, the TEMASOFT FileMonitor Agent will collect the following information:
    - System-wide process / application activity on the target machines;
    - System-wide file copy operations on the target machines;
    - System-wide folder delete / rename operations;
    - If monitoring profile is assigned: All the file operations in the paths included in the associated monitoring profile (if any) with the "monitoring type" set to "monitor everything";
    - If monitoring profile is assigned: All the changes to files in the paths included in the associated monitoring profile (if any) with the "monitoring type" set to "monitor changes only"
- The information is sent back to the TEMASOFT FileMonitor Server in real time, if the server is available; if the server is not available, the agent will cache the data and send it to the server when the server becomes available again;
- The TEMASOFT FileMonitor Server will process the information it receives from the TEMASOFT FileMonitor agents;
- Based on the processing, it will act (if so configured) like tag, ignore or alert via email; Please see chapter 3, subchapter "Actions and alerting" for more details;
- Next, if the information is not ignored by an action, TEMASOFT FileMonitor Server will archive this information to the SQL Server database; Please see chapter 3, subchapter "Database Settings" for more information;
- Statistics on the information in the database can be utilized on the TEMASOFT FileMonitor Server dashboards; Please see chapter 5 for more details.
- The information can be analyzed in the Data viewer, where a wide variety of filters and sorting options are available; Please see chapter 6 for more information;
- The information can be reported on, using a comprehensive list of default reports as well as the a

4.2 Collecting file operations information from NAS machines

TEMASOFT FileMonitor can monitor file activity from NAS machines (QNAP and Synology). This is done via Syslog messages sent by those devices to the TEMASOFT FileMonitor Server. To record that information, one needs to configure the logging system on the NAS machines to enable the collection of file activity data and to send it to the TEMASOFT FileMonitor Server machine. For more details please review chapter 2.3, Monitoring file activity on Network Attached Storage (NAS) or Storage Area Networks (SAN).

4.3 File Permissions Auditing

TEMASOFT FileMonitor helps administrators keep track of file access permissions. This is implemented using a dual approach:

1. Taking on-demand snapshots of the current permissions set on different files and folders and through
2. Real-time detection of any changes in the file permissions

To perform on-demand auditing, one needs to:

1. Designate the foders (and files) that need to be audited. This is done from the monitoring profiles (see 3.2 Monitoring profiles). You can specify the folders and files to be audited or the ones that you want to exclude from auditing. Last, but not least, you need to make sure that the auditing profile is assigned to the machines you want to check.

2. From the Monitored machines section, for each machine or group you want to inspect, you have the option to trigger an auditing process, by clicking the “Run Permissions Audit” link.

The manual file permissions auditing process can take several minutes, depending on the number of files to be processed.

The real-time permissions change detection is already included in FileMonitor, since the first version, and does not use the “Audit permissions” and “Do not audit permissions” settings in the monitoring profiles. You only need to make sure the files are monitored by using one of the values “Monitor changes only” or “Monitor everything” in the monitored proifiles.

Note: “Monitor everything” refers only to real-time operations and does not include “Audit permissions”, which is used for on-demand (manual) file auditing permissions.

The results of the auditing process can be analyzed in the “Data viewer” section. There is a dedicated action (“Access rights audit”) that you can use to filter the data. Also, the details of the current permissions are shown in the “Details” field.

4.4 File Integrity Monitoring

TEMASOFT FileMonitor helps administrators monitor the integrity of the critical files related to server settings, software configuration, and other files and documents that must change only under strict conditions. This is process is ensured by the real-time file monitoring engine that can track different operations on files and also calculates hashes based on the file conten, that can be used as baselines to detect if the files are compromised.

To benefit from this feature, you only need to make sure the files are monitored by using one of the values “Monitor changes only” or “Monitor everything” in the monitored proifiles assigned to the computers you want to check.

Data can be analyzed in the “Data viewer” section, using the “Content hash” field. The hash value is a numeric value calculated based on the file content and its size.

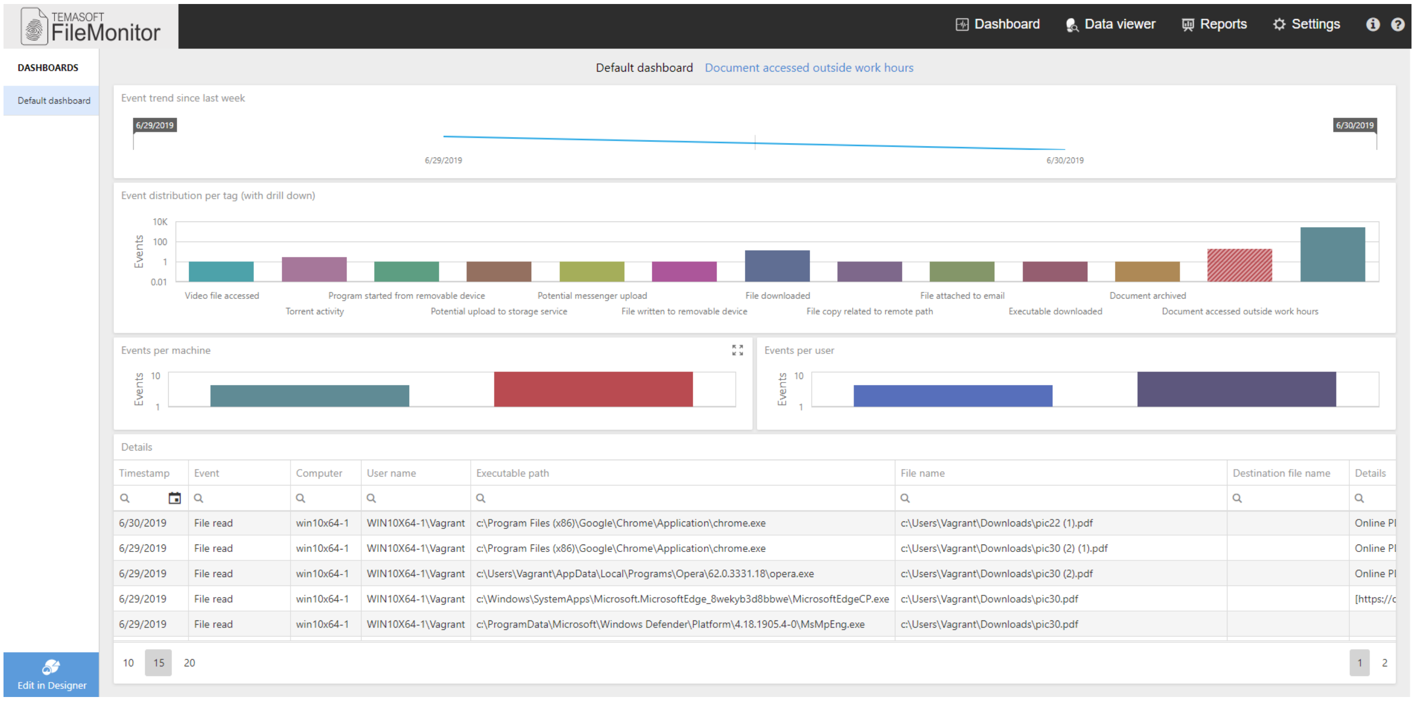
5 Activity Monitoring

This section describes how to use TEMASOFT FileMonitor to perform file and process activity monitoring based on data collected by the TEMASOFT FileMonitor Agents. This chapter focuses on how to use the TEMASOFT FileMonitor Server default dashboards and how to create custom dashboards for more specific activity monitoring.

5.1 Dashboard section

To access the TEMASOFT FileMonitor Server Dashboard Section, please perform the following steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace “localhost” with the appropriate TEMASOFT FileMonitor Server IP);
- Select the “Dashboard” tab at the right of the main navigation bar; a new page will be displayed.


TEMASOFT
FileMonitor
Dashboard
Data viewer
Reports
Settings
DASHBOARDS
Default dashboard
Default dashboard
Document accessed outside work hours
Event trend since last week
6/29/2019
6/30/2019
Event distribution per tag (with drill down)
10K
100
1
0.01
Events
Video file accessed
Program started from removable device
Potential messenger upload
File downloaded
File attached to email
Document archived
Torrent activity
Potential upload to storage service
File written to removable device
File copy related to remote path
Executable downloaded
Document accessed outside work hours
Events per machine
Events per user
10
1
Edit in Designer

Details

Timestamp	Event	Computer	User name	Executable path	File name	Destination file name	Details
6/30/2019	File read	win10x64-1	WIN10X64-1\Vagrant	c:\Program Files (x86)\Google\Chrome\Application\chrome.exe	c:\Users\Vagrant\Downloads\pic22 (1).pdf		Online Pl
6/29/2019	File read	win10x64-1	WIN10X64-1\Vagrant	c:\Program Files (x86)\Google\Chrome\Application\chrome.exe	c:\Users\Vagrant\Downloads\pic30 (2) (1).pdf		Online Pl
6/29/2019	File read	win10x64-1	WIN10X64-1\Vagrant	c:\Users\Vagrant\AppData\Local\Programs\Opera\62.0.3331.18\opera.exe	c:\Users\Vagrant\Downloads\pic30 (2).pdf		Online Pl
6/29/2019	File read	win10x64-1	WIN10X64-1\Vagrant	c:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe	c:\Users\Vagrant\Downloads\pic30.pdf		[https://c
6/29/2019	File read	win10x64-1	WIN10X64-1\Vagrant	c:\ProgramData\Microsoft\Windows Defender\Platform\4.18.1905.4-0\MsMpEng.exe	c:\Users\Vagrant\Downloads\pic30.pdf		

10 15 20 1 2

Figure 37: TEMASOFT FileMonitor Dashboard

The dashboard section presents the collected data filtered and aggregated on different criteria. Each dashboard item is highly configurable, and one can select different visualization styles, colors, aggregation and even details. The data presented by each item can be correlated if the drill-down option is enabled for the related items.

Each FileMonitor user can have multiple “dashboards”. The list of available dashboards is on the left pane. Each “dashboard” can contain different dashboard items. The layout is very flexible, and one can arrange the items in the most convenient way.

To edit or add dashboards and dashboard items, one need to switch to Edit mode, by pressing the “Edit in Designer” button from the bottom-left of the page. After editing a dashboard, one can switch back by pressing the “Viewer” button.

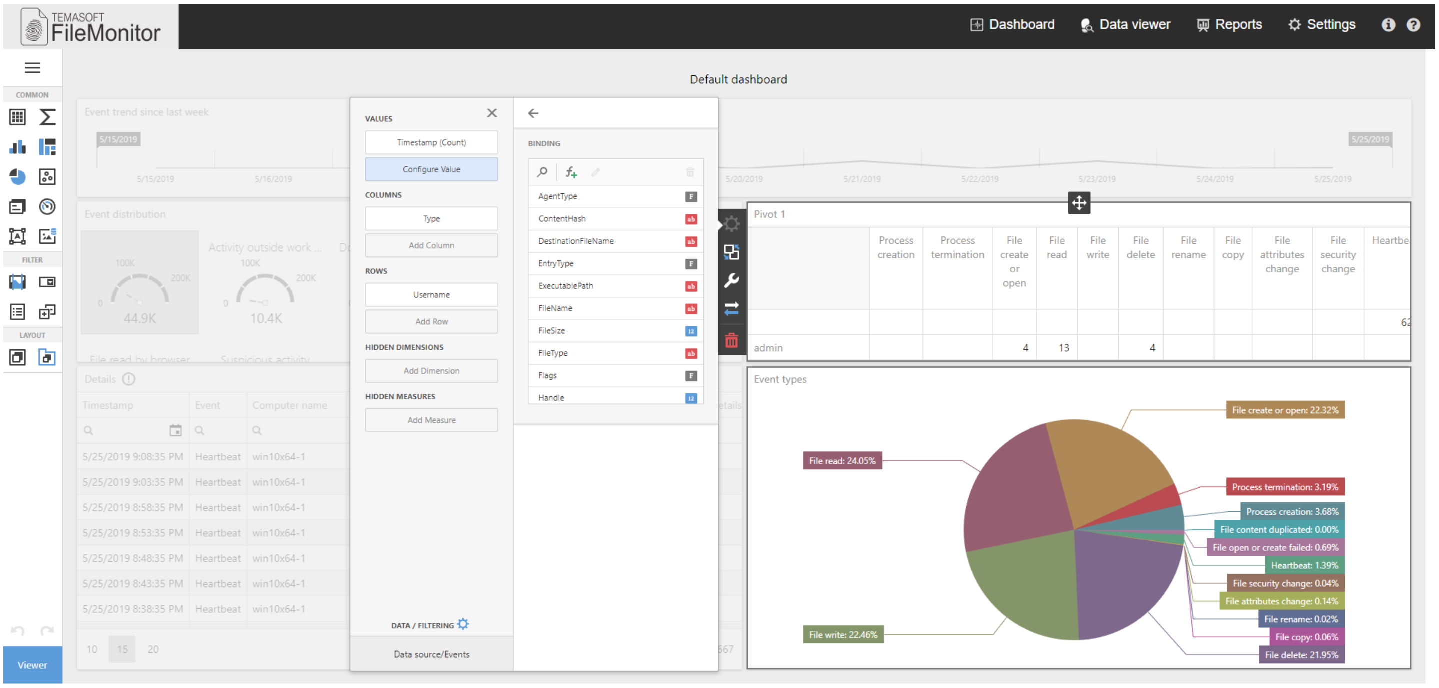


Figure 38: TEMASOFT FileMonitor Dashboard Editor

The dashboard section uses the data in the active TEMASOFT FileMonitor database configured in the Settings section of the product configuration – the database where the data from the TEMASOFT FileMonitor agents is being saved. Please see chapter 3, subchapter "Database settings" for more information on how to configure the active product database. Unlike the data analysis tool provided in TEMASOFT FileMonitor, the Data viewer and the Reports, the dashboard section does not support loading data from other TEMASOFT FileMonitor databases because its purpose is to deliver monitoring information of what is happening in real time.

5.2 Dashboard items

The dashboard items make up the TEMASOFT FileMonitor Dashboard and represent statistical representations, either graphs texts, or grids, of the data collected by TEMASOFT FileMonitor agents. There are several dashboard items you can configure. The data items can be connected and filtered through a drill-down approach. Each item has its own set of properties grouped by data binding, appearance, and custom properties. To group multiple items, you can use the layout dashboard items. Each item can be positioned or sized as needed, by dragging and resizing its layout box on the design page. The next grid presents the dashboard item types that are available when editing a dashboard:

Dashboard item type	**Description**
Grid	Shows data in a tabular format. Accepts aggregated and calculated fields.
Pivot	Useful to show data distributions in tabular format.
Chart	Useful to show trends in a graphical format.
Tree Map	Useful to show distributions as a heat map.
Pie	Useful to show distributions in circular graphical elements.
Scatter Chart	Useful to show distributions using more complex criteria to calculate and represent data.
Card	Useful to partition data on various field values and view relevant data in text boxes.
Gauge	Useful to partition and aggregate data and view the relevant values in a suggestive graphical representation.
Text box	Useful to represent data values in text format.
Bound Image	Advanced feature which displays images associated with different values.
Range filter	Range filter that can serve as master data set. The filter is represented graphically as a line graph with sliders.
Combo Box	Range filter that can serve as master data set. Values can be chosen from the combo box list.
List Box	Range filter that can serve as master data set. Values can be chosen from a list.
Tree View	Range filter that can serve as master data set. Values can be chosen from a tree list.
Group	Layout element that can group together multiple dashboard items.
Tab Container	Layout element that can group together multiple dashboard items, under a tab page.

Figure 39: List of available types of dashboard items

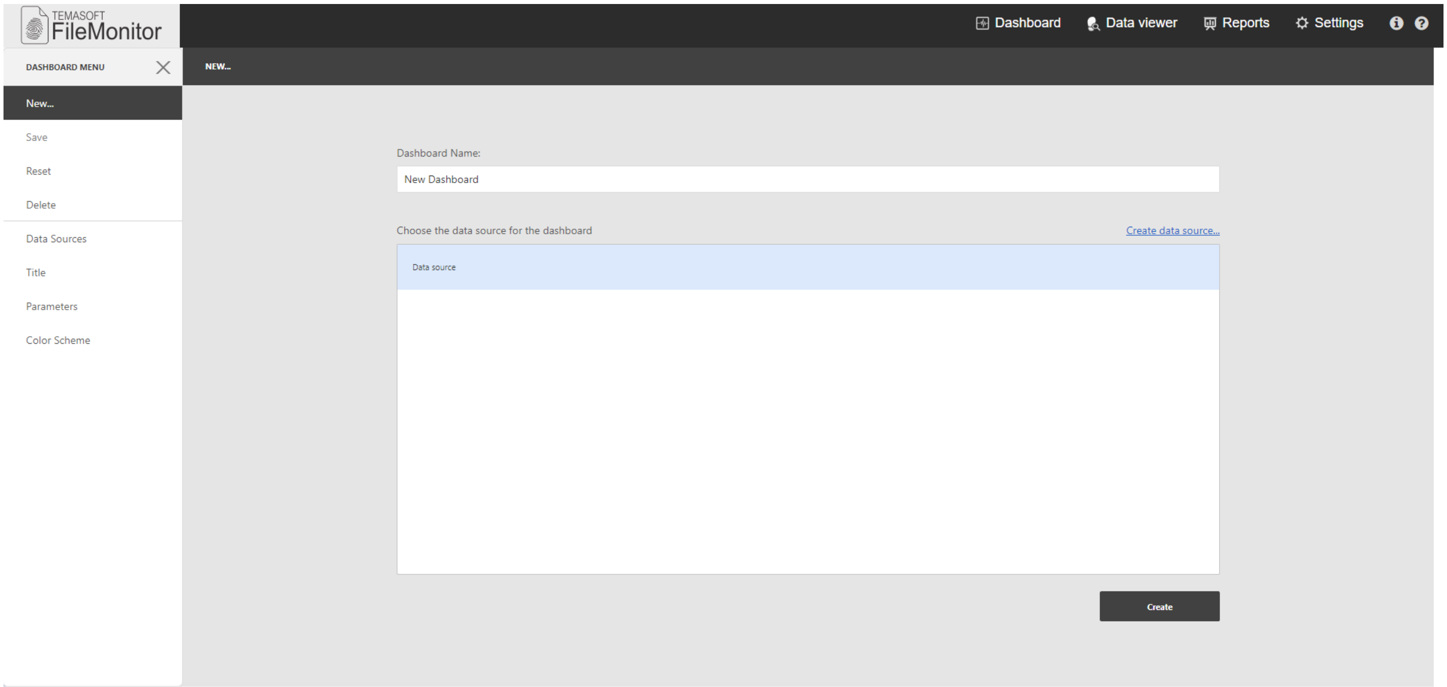
5.3 Managing dashboards

Each user can define multiple dashboards. There is also a predefined dashboard that is loaded by default for each user.

Creating a dashboard

To create a dashboard, switch to the designer mode by pressing “Edit in Designer” and open the dashboard menu by pressing the ☰ button from the top of the editor pane, then follow the next steps:

- Choose “New” from the menu;
- Enter a name of the new dashboard; You can change the title later from the dashboard menu, “Title” entry;
- Press “Create”;
- Add the dashboard items that you need;
- Open the dashboard menu again and click “Save” to save the dashboard.



Dashboard Name: New Dashboard

Choose the data source for the dashboard

Figure 40: Create dashboard

Removing a dashboard

To remove a dashboard item, please click the menu button, icon ☰, and select “Delete”. The dashboard will be removed. The default dashboard cannot be removed.

Resetting the default dashboard

If you change the default dashboard, and later you want to revert to the original design, open the dashboard menu and select “Reset”.

6 Data analysis

This chapter focuses on data analysis and how to work with the main data presentation tool of TEMASOFT FileMonitor, the Data viewer. The first two subchapters will cover the available event fields and how to use filtering, because to be able to manipulate the data and extract specific pieces of information for various use cases, it is needed to understand how the data is structured and what do the fields appearing in individual events mean.

6.1 Event fields

Each event, or file / process operation collected by TEMASOFT FileMonitor contains several pieces of information about the time when it occurred, the user who caused it, the processes and files involved, etc. These values are organized and stored in what we call event fields. The names of the fields are chosen to be intuitive for the values they host, so that it is easier to use them. The content of some fields changes slightly depending on the operation / action. Please see a table below, showing the existing event fields, their meaning and potential values:

Event field	**Meaning**	**Possible values**
Action	The type of the operation that led to the generation of the event.	Process related: Process creation, Process termination File related: File created or opened (when logged on a Windows machine, this indicates that a file has been created); File read, File write, File delete, File rename File copy, File attributes change, File security change, Access rights audit, File archived, File attached to Outlook, File moved to recycle bin, File restored from recycle bin, File open or create failed, File content duplicated, file probably archived (when several levels of nesting are used, it is not always possible to detect exactly which file was archived) Internal: Heartbeat
Application type	Custom value that represents the type of an executable (e.g. Browser, Messenger, etc.)	Editable value that has an associated list of program names that are matched against the Executable Path field using the “Contains” operator.
Computer	The computer where the event was generated	String values – computer names or IPs
Content hash	The value of the hash computed for the files to ensure file integrity	Hexadecimal values if calculated, or 0 if calculation is not possible, i.e. because of lack of access to the file content
Context type	A custom value that can be associated with read and write operations (e.g. Web email service, Transfer service, Social media site, etc.)	Editable value that has an associated list of keywords that are matched against the Details field using the “Contains” operator. Applicable only for read and write operations. Optionally, entries in the list can also use the [AND] operator to try to match all the keywords in the entry.

Event field	**Meaning**	**Possible values**
Destination file name	For copy, rename and move operations, this represents the destination file name, including the full path to it, on the network, on the computer or a removable device.	String value containing full path and file name of the files being copied, moved or renamed.
Details	In case of file copy operations where we cannot tell exactly the source file, this field contains the list of possible source files of the operation. For other operations, this field can show the URL or the title of the active window when a certain file operation occurred. It is also used to show file access permissions.	String value containing a list of full paths and file names of potential sources for a copy operation, or URLs or tiles of the active window when a file operation occurred. It can also contain the access permissions for files and folders, and other relevant information.
Entry type	The type of event being generated	Internal: agent, Web UI, server; File activity Process activity
Executable path	The path (including the executable name) of the process that caused the event	String value containing full file path and file name. For actions generated by the system (PID 4) this value will be <SYSTEM>
File name	The name of the file which makes the scope of the operation. In case of copy operations, this is the source file	String value containing full file path and file name
File size	The size of the file which makes the scope of the operation	Positive integer value in bytes
File type	The type of the file as defined in the product configuration -> file types. If the file type is not defined, this column lists the file extension.	String value containing a name, or an extension, including the dot
Flags	This holds a list of flags that TEMASOFT FileMonitor assigns to the event. None or more values may be present	File read by browser: if set, in conjunction with “File read to end” flag, it signals a potential file upload via browser; File renamed by browser: if set for files with particular extensions, it means a potential file download via browser; File read to end: if set, it means that most probably the entire file was read. User was impersonated: if set, it means that the process that generated the event impersonated the user listed under the field user name. For further forensics, please see all the available user names: process, handle, thread, etc. File is located on removable device: if set, it means that at the time when the action occurred, the file resides on a removable device. This is useful to identify file copy operations when the destination is a removable device.

Event field	Meaning	Possible values
		File is a directory: if set, it means that the file is a folder – used for easy monitoring of folders; User is administrator: if set, it means that the user who caused the event has administrative privileges; The file was changed by this operation: if set, it means that the operation resulted in a change to the file – used for easy monitoring of file changes without complex filters on the action type
Handle user name	The user who requested the handle to the file that makes the scope of the file operation that caused the event to be generated	String value – user name
In work hours	Specifies if the event took place in or outside (if false) the work hours, as they are defined in the product configuration	Boolean
IP address	IP of the source computer	String value
Parent ID	The PID of the parent process of the thread that caused the event to be generated. This value is populated if the action was performed in a thread, and this is the PID of the parent process	Positive integer
Process ID	The PID of the process that caused the event to be generated	Positive integer
Process user name	The user name to whom the security context of the process that caused the event to occur belongs to	String value
Status	If the operation succeeded or failed	Success or Failure. Note only file open operations may fail
Status code	The return code for some operations	Currently it is 0. In the future versions, for certain operations which fail, this field will hold the NT STATUS value, as returned by the operating system
Tag	The events that match an action that implies tagging the event, as configured in the "Actions and alerts" section, will have this field populated with the value configured as tag in the triggering action	String value
Thread Id	The Id of the thread that caused the event to be generated. This value is populated only if the action that led to the event generation was performed in a thread, rather than a process	Positive integer
Timestamp	The date and time of the event. In the database it is stored as UTC time. In reports and data viewer it is converter to the time zone of the TEMASOFT FileMonitor Server	Date time value
Computer local time	The local date and time of the event on the originating machine	Date time value

Event field	Meaning	Possible values
User Name	This value may be any of the user name fields (handle user name, process user name on Windows. For process activity events, this value is the process user name. For file activity events, this value is the most relevant between process user name and handle user name	String value

Figure 41: List of available event fields

The timestamp field

The timestamp indicates when an event has occurred on the agent machine. Its value is the time at which the event occurred with millisecond precision, converted to UTC. The timestamp is a value that records both the date and the time. This is how the timestamp value is saved in the database. The timestamp field is displayed in reports and data viewer as the timestamp of the event converted to the time zone of the TEMASOFT FileMonitor Server. For example, if a file operation occurred at 1 Mar 2015 13:00:00 UTC and the TEMASOFT FileMonitor Server is on a time zone corresponding to UTC+02 hours, then this timestamp will be displayed in reports and data viewer as 1 Mar 2015 15:00:00.

Using filters with the timestamp field: it is possible to use filters with the timestamp field, but you cannot use the “equals” operator. That is because timestamp is recorded with millisecond precision, it is very unlikely to specify a value that matches an event in the database using milliseconds. Hence the timestamp field is used with operators such as “is between”, “greater than” or “smaller than”. When specifying the matching values for the filtering conditions using such operators, you can specify dates (“01/02/2016”), times (“10:10:00”) or dates and times (“01/02/2016 12:00:01”). For example, to create a filter that returns results on the 15th of January until 13 hours, the filter would look like:

Timestamp is between “15/01/2016 00:00:00” and “15/01/2016 13:00:00”

Each event TEMASOFT FileMonitor collects is a collection of such fields and values. Hence, the event fields can be used for a variety of monitoring or data analysis purposes, on the product dashboard, in the Data viewer and in the Reports.

The computer local time field

In addition to the timestamp field, the TEMASOFT FileMonitor Agent also records and stores in the database the time difference in minutes between the time zone of the computer on which the event occurred and UTC at that moment. By combining the UTC timestamp of the event and the time zone shift, TEMASOFT FileMonitor can also display in the data viewer and reports the local date and time observed on the computer on which the event occurred, at that moment. This field is called "computer local time". As it is a calculated field, you will be able to inspect it, but you won't be able to use it for filtering and sorting operations.

6.2 Using filters

The Filter Builder dialog can be reached by clicking the “Filter” button, icon ▼, or by clicking a “Create filter” link, depending on the group that is filterable (filter data in Data viewer, filter monitoring profiles, create filters for reports or actions). Filtering is available both for data analysis and for those configuration views that can become large (such as list of monitored computers). Wherever filtering is available, this dialog will be presented to build a filter.

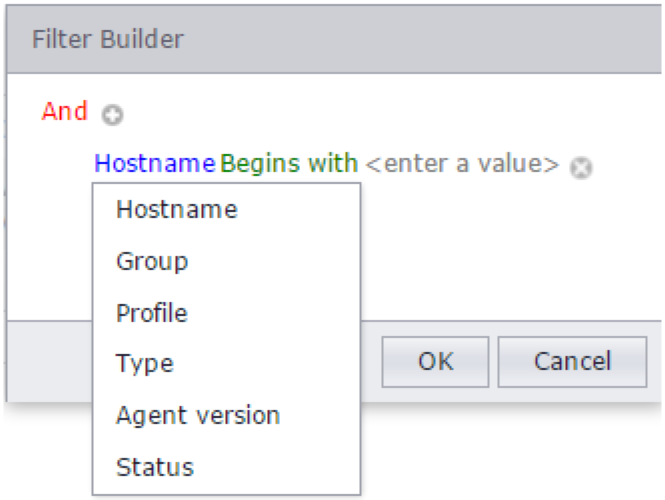


Figure 42: Filtering dialog

- Adding simple filtering condition:
  - First logical operator is “And” and it is the operator for the first level of conditions; You can change it to other operators: OR, NOT AND, NOT OR by clicking on it;

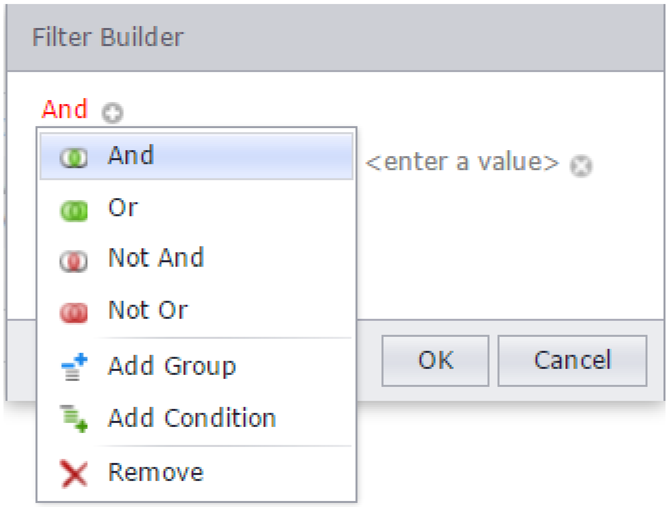
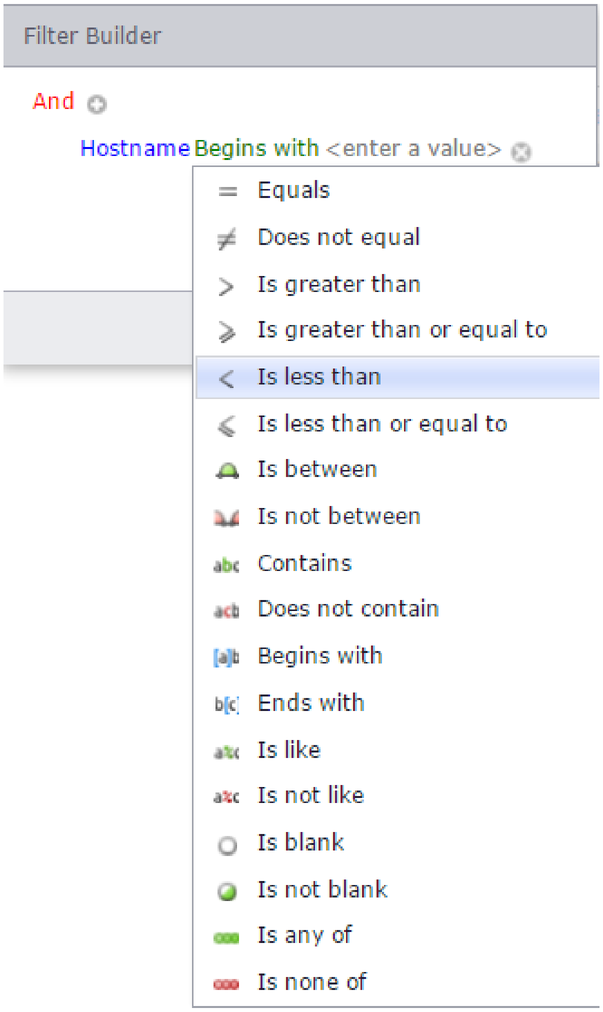


Figure 43: Editing top level logical operator

  - Click on the “Plus” button ⊕ ;
  - Select the field for your first condition from the list of available parameters described above (Figure 42);
  - Next, click on the operator hyperlink. For string parameters, default operator is “Begins with”;
  - A list of available operators will appear



And

Hostname Begins with <enter a value>

Figure 44: Available filtering operators

- Select the desired operator;
- Click on the <enter value> field to add your expected value for this condition;
- Repeat the process, if you want to add another condition; Note that the logical operator between the two conditions is the one at the top (defaults to “And”).

- Multiple conditions with different operators

If you want to have more than two conditions, and different operators between the two, you will need to use groups of conditions. Please follow these steps:

- Enter two conditions that you want to have the top-level operator between then, as per the above procedure
- Click on the default top operator and select “Add group”

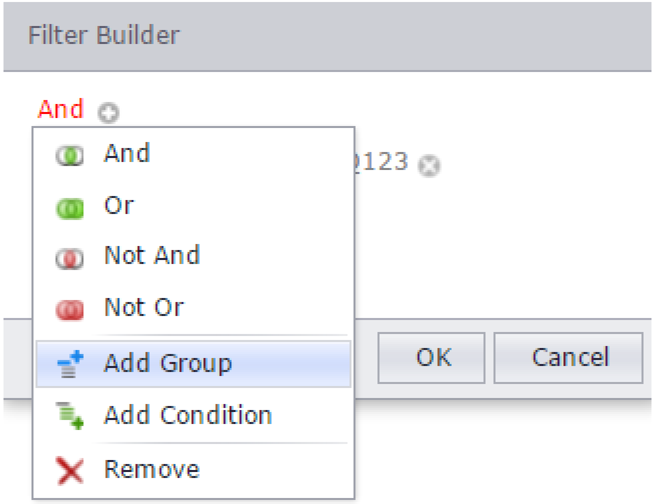
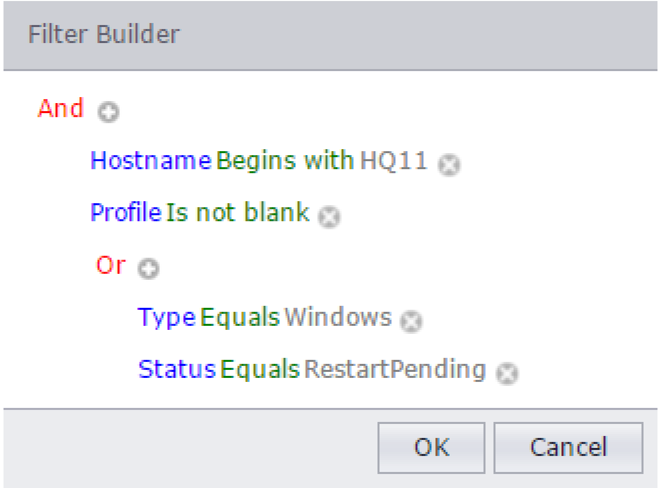


Figure 45: Adding a group of conditions

- The dialog will create a group of conditions with a new top-level operator (by default "And") which you can change as needed;
- Add subsequent conditions as needed;



And

Hostname Begins with HQ11

Profile Is not blank

Or

Type Equals Windows

Status Equals RestartPending

Figure 46: Example of conditions with different logical operators

- In the above example, the filter is the following:

(Hostname Begins with HQ11) AND (Profile is not blank) AND ((Type Equals Windows) OR (Status Equals RestartPending))

Note: to improve the performance of the reporting engine when using complex queries, please build the filter in such a way that it includes the conditions based on string operations involving string fields (i.e. user name ends with, or file name contains) last, and other conditions (like Action, or Flags) first.

6.3 Data viewer

The Data viewer is the most important tool for data analysis because it can show information in real time, and enables various layout, filtering and sorting options. The Data viewer is a grid control that is connected to a TEMASOFT FileMonitor Database. The central elements of the Data viewer are the views. There are several predefined views which can be customized, and you can also create new views. In addition, the top of the page contains a toolbar with buttons used for managing the views or exporting the information.

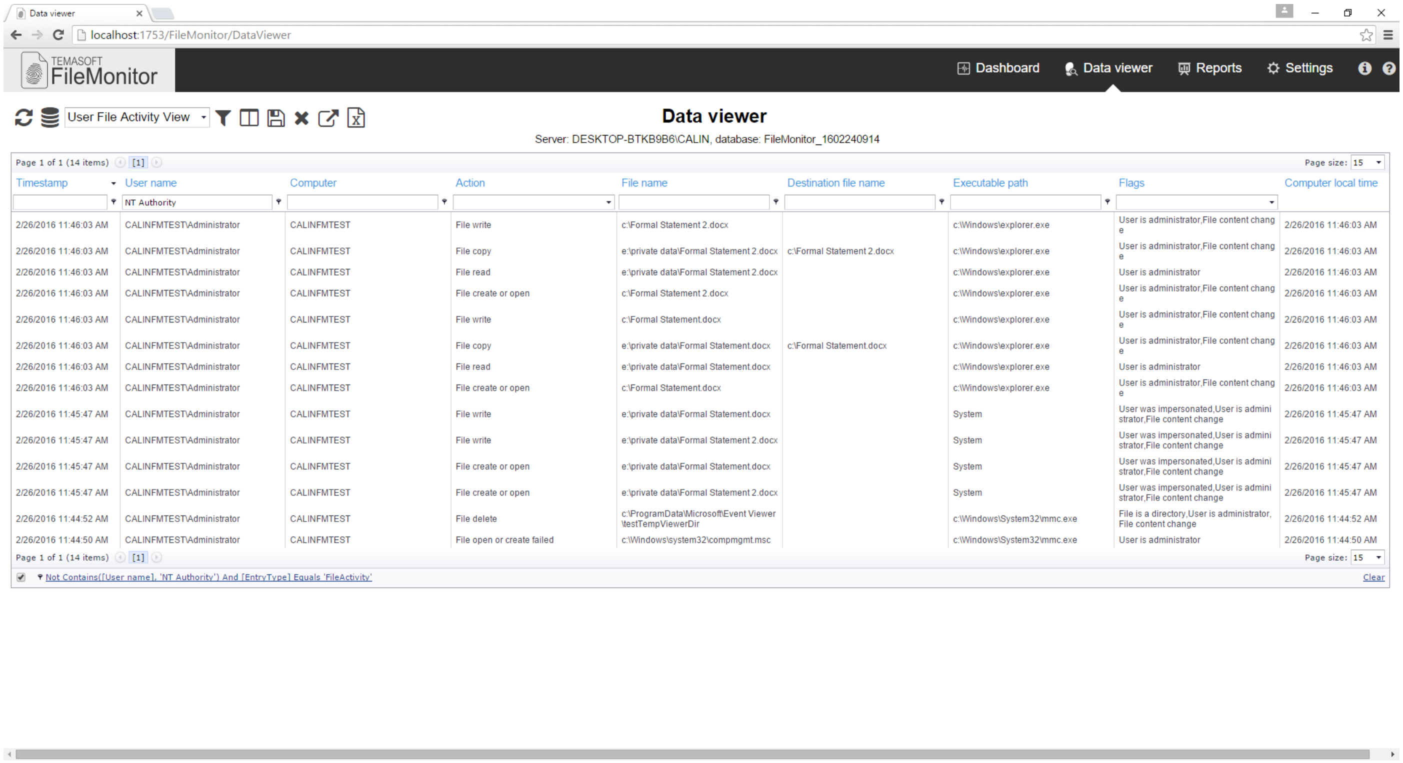
What is a view?

A view is a collection of columns that form the grid's layout, together with filters and sort options. The default views are displayed in a combo box at the top of the page.

Opening the Data viewer

To open the Data viewer, please follow the below procedure:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace "localhost" with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the "Data viewer" page;



Data viewer

Server: DESKTOP-BTKB9B6\CALIN, database: FileMonitor_1602240914

Page 1 of 1 (14 items) [1] Page size: 15

Timestamp	User name	Computer	Action	File name	Destination file name	Executable path	Flags	Computer local time
	NT Authority							
2/26/2016 11:46:03 AM	CALINFMTEST\Administrator	CALINFMTEST	File write	c:\Formal Statement 2.docx		c:\Windows\explorer.exe	User is administrator,File content change	2/26/2016 11:46:03 AM
2/26/2016 11:46:03 AM	CALINFMTEST\Administrator	CALINFMTEST	File copy	e:\private data\Formal Statement 2.docx	c:\Formal Statement 2.docx	c:\Windows\explorer.exe	User is administrator,File content change	2/26/2016 11:46:03 AM
2/26/2016 11:46:03 AM	CALINFMTEST\Administrator	CALINFMTEST	File read	e:\private data\Formal Statement 2.docx		c:\Windows\explorer.exe	User is administrator	2/26/2016 11:46:03 AM
2/26/2016 11:46:03 AM	CALINFMTEST\Administrator	CALINFMTEST	File create or open	c:\Formal Statement 2.docx		c:\Windows\explorer.exe	User is administrator,File content change	2/26/2016 11:46:03 AM
2/26/2016 11:46:03 AM	CALINFMTEST\Administrator	CALINFMTEST	File write	c:\Formal Statement.docx		c:\Windows\explorer.exe	User is administrator,File content change	2/26/2016 11:46:03 AM
2/26/2016 11:46:03 AM	CALINFMTEST\Administrator	CALINFMTEST	File copy	e:\private data\Formal Statement.docx	c:\Formal Statement.docx	c:\Windows\explorer.exe	User is administrator,File content change	2/26/2016 11:46:03 AM
2/26/2016 11:46:03 AM	CALINFMTEST\Administrator	CALINFMTEST	File read	e:\private data\Formal Statement.docx		c:\Windows\explorer.exe	User is administrator	2/26/2016 11:46:03 AM
2/26/2016 11:46:03 AM	CALINFMTEST\Administrator	CALINFMTEST	File create or open	c:\Formal Statement.docx		c:\Windows\explorer.exe	User is administrator,File content change	2/26/2016 11:46:03 AM
2/26/2016 11:45:47 AM	CALINFMTEST\Administrator	CALINFMTEST	File write	e:\private data\Formal Statement.docx		System	User was impersonated,User is administrator,File content change	2/26/2016 11:45:47 AM
2/26/2016 11:45:47 AM	CALINFMTEST\Administrator	CALINFMTEST	File write	e:\private data\Formal Statement 2.docx		System	User was impersonated,User is administrator,File content change	2/26/2016 11:45:47 AM
2/26/2016 11:45:47 AM	CALINFMTEST\Administrator	CALINFMTEST	File create or open	e:\private data\Formal Statement.docx		System	User was impersonated,User is administrator,File content change	2/26/2016 11:45:47 AM
2/26/2016 11:45:47 AM	CALINFMTEST\Administrator	CALINFMTEST	File create or open	e:\private data\Formal Statement 2.docx		System	User was impersonated,User is administrator,File content change	2/26/2016 11:45:47 AM
2/26/2016 11:44:52 AM	CALINFMTEST\Administrator	CALINFMTEST	File delete	c:\ProgramData\Microsoft\Event Viewer \testTempViewerDir		c:\Windows\System32\mmc.exe	File is a directory,User is administrator, File content change	2/26/2016 11:44:52 AM
2/26/2016 11:44:50 AM	CALINFMTEST\Administrator	CALINFMTEST	File open or create failed	c:\Windows\system32\compmgmt.msc		c:\Windows\System32\mmc.exe	User is administrator	2/26/2016 11:44:50 AM

Page 1 of 1 (14 items) [1] Page size: 15

☑ Not Contains([User name], 'NT Authority') And [EntryType] Equals 'FileActivity' Clear

Figure 47: Data viewer main page with Default View

Selecting a view and the list of default views available

The list of available views is presented in the combo box at the top left of the page. This list contains the views available by default, as well as custom views created by the user. The views available by default are not sorted, so the order is chronological (the default order). The columns are event fields. For more information on what each column means and its possible values, please see "Event fields". For more information on filters, please see "Using filters"

Views available by default

Name of default view	Columns	Filters
Default View	Timestamp, User name, Computer, Action, File name, Destination file name, Executable path, Details, Flags, Tag	All events stored in the database are shown
Access Rights Activity View	Timestamp, User name, Computer, Action, File name, Executable path, Details, Flags	User name does not contain “NT Authority” and action is ”Access rights audit”
File Change Activity View	Timestamp, User name, Computer, Action, File name, Destination file name, Executable path, Details, Flags, Tag	User name does not contain “NT Authority” and refers to a file modification or file read by browser or attached to an email
Admin Activity View	Timestamp, Computer, Action, File name, Destination file name, Executable path, Details, Flags	Flags equals “User is administrator”
Default Compliance View	Timestamp, User name, Computer, Action, File name, Destination file name, Executable path, User name, Flags	User name does not contain “NT Authority” AND Entry Type equals “File Activity”
Process Monitoring View	Timestamp, User name, Computer, Action, Executable path, Flags	User name does not contain “NT Authority” AND Entry Type equals “Process Activity”
File Activity View	Timestamp, User name, Computer, Action, File name, Destination file name, Executable path, Details, Flags, Flags	User name does not contain “NT Authority” AND Entry Type equals “File Activity”

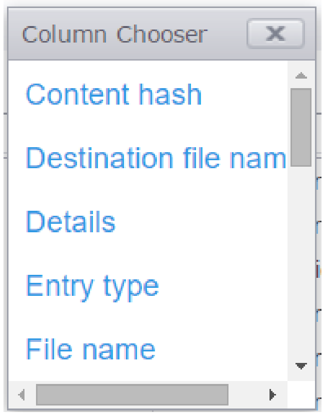
Figure 48: List of views available by default

Adding / editing a view

Adding or editing views is done by changing the columns or the filters of the current view and using the “Save” or “Save as” buttons. To create a custom view, simply change columns, add filters and sort data in the current view, and then click “Save as” and give the view a new name. The new view will get listed in the top left combo box. Using “Save” would overwrite the current view with the new configuration, and thus, the old view will be lost and replaced by the new view. To use these options, hoover over the “Save” button, icon 💾 and click “Save” or “Save as”, as desired, in the menu that will appear.

Editing columns

To edit the columns of the view, please click the “Columns” button, icon ◫ in the toolbar present on the top left of the page. This will bring up the “Column chooser” dialog presented below:



Column Chooser

Content hash

Destination file nam

Details

Entry type

File name

Figure 49: Column chooser dialog

This dialog lists all the available columns that are not already part of the current view. The columns correspond to the event fields. For a full list, please see “Event Fields”.

- Removing existing columns from the view: Drag the column you wish to remove over the “Column Chooser” dialog. An “x” sign will appear with your cursor signaling a “delete” operation. Drop the column over the “Column Chooser” dialog. It will be removed from the view and added to the “Column Chooser” list. If you wish to clear all the columns from the view, simply repeat the operation until all the columns are moved from the view, to the “Column Chooser” dialog;
- Changing the column order: Drag the column horizontally, from its current position, to left or right, keeping inside the header of the grid control, and drop it to the desired position. When the column reaches a spot where it can be dropped for repositioning, two arrows pointing to each other will appear with your cursor, indicating you can reposition the column there;
- Inserting new columns: Drag a column from the “Column Chooser” dialog and drop it in the desired location in the header of the grid;

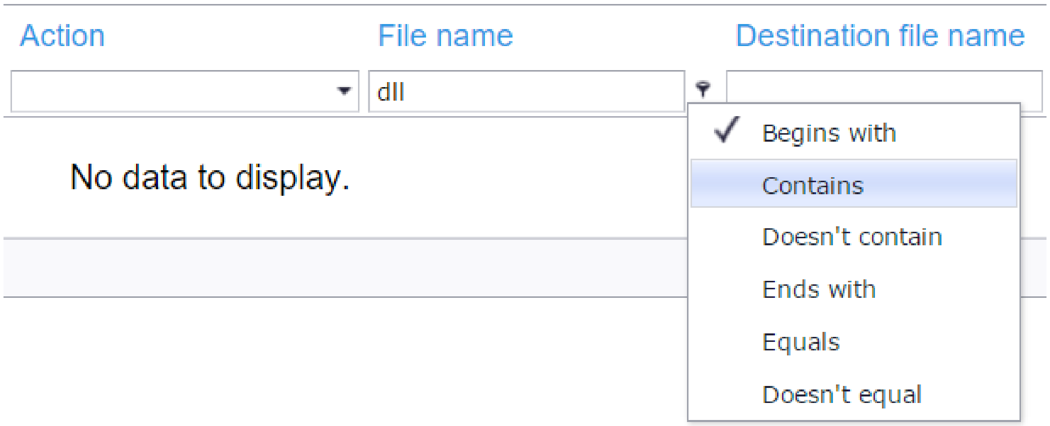
Filtering the view

The currently active filter for the view is displayed at the bottom of the grid control. You can also see the currently active filter by clicking the “filter” button, icon ▼ in the top left toolbar. This will bring up the filter builder dialog and list the currently active filtering condition(s). You can use the filter builder as described in subchapter “Using filters” to change the currently active filter or add more conditions to it.

Quick filtering

Alternately, you can quick filter by entering values in the edit boxes that are present in the header of the grid right under the name of the columns. Editing such an edit box, will create a filtering condition based on the column under which the edit box resides, and will use the default operator for the condition. Default operators are different depending on the type of column (or event field). To edit the operator of the quick filtering condition described above, click the “pin” button, icon ▼. A list of available operators will appear. The currently set operator will be signaled by a check mark. To change it, simply click the desired operator. The filtering condition will be added with the “AND” operator, to any currently active filter. If you would like to change that, you need to make use of the filter builder dialog by clicking the “Filter” button.

Figure 45 below shows how to quick filter based on the “File name” field. The intention is to filter in all DLL files (see all operations involving such files), so we have typed DLL in the corresponding edit box. However, because the default operator in this case is “Begins with”, the list of results is empty because there are no files that start with “dll” involved in operations saved in the database. Hence, the “Pin” button was clicked to bring up the list of operators, and then the “contains” or “ends with” operator can be selected to achieve the goal of the quick filtering operation.



✓ Begins with

dll

No data to display.

Figure 50: Quick filter - change operator

Unlike the filtering operation that makes use of the “Filter builder” dialog described in “Using filters”, the quick filtering only allows simple filters to be built. If you want to use different logical operators between conditions or more complex grouping of conditions, please use the “Filter builder”.

Sorting the view

To sort the view, simply click on the column based on which you wish to sort. A black triangle pointing upwards or downwards, depending if the sort order is ascending or descending, will appear at the right end of the column that is currently being used as sorting criteria. One click will sort ascending, a second click will sort descending. Any subsequent click on the name of the column will change the sort order.

Analyzing the results of the view

To analyze the results of a view, take note of the information displayed as rows in the view. That information meets the filtering criteria and will display the chosen event fields. Note that the information is paginated, so if there are more rows than fit the page, a list of numbers will be displayed at the top of the grid control, under the header. These numbers represent the number of the pages that contain data. You can navigate by clicking on the desired page number, or by clicking the left /right arrow buttons bordering the list of available page numbers.

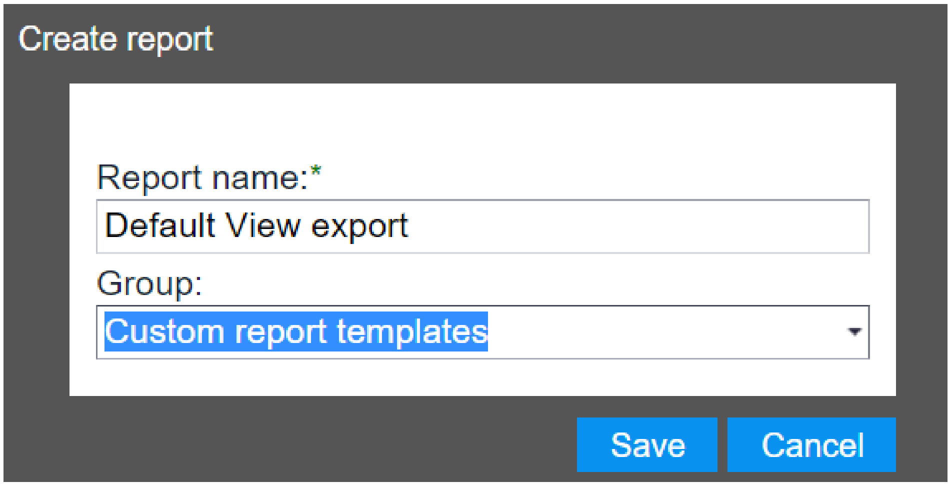
The data coming from TEMASOFT FileMonitor agents is saved in the database in real time, but the Data viewer does not show the data in real time automatically. You need to click the “Refresh” button, icon ⟳ to re-query the database and refresh the view.

Exporting a view

It is possible to export the results of the view to csv format for later analysis. To do that, simply click the “export to csv” button, icon x . The results will be written to a csv file which will be downloaded by the browser to the default download location.

Reporting from view

It is possible to create a report based on the current view in the “Data viewer”. To do that, please click on the “report from view” button, icon ↗ . A new dialog will appear that will prompt for a name for the report and will enable selection of a report group (optional) where the report will belong to. Clicking “Save” on this dialog will determine the creation of the report according to the settings of the current view (in terms of columns / layout and filtering condition (rows)). For more information on reports please see chapter 7, “Reporting”.



Create report

Report name:* Default View export

Group: Custom report templates

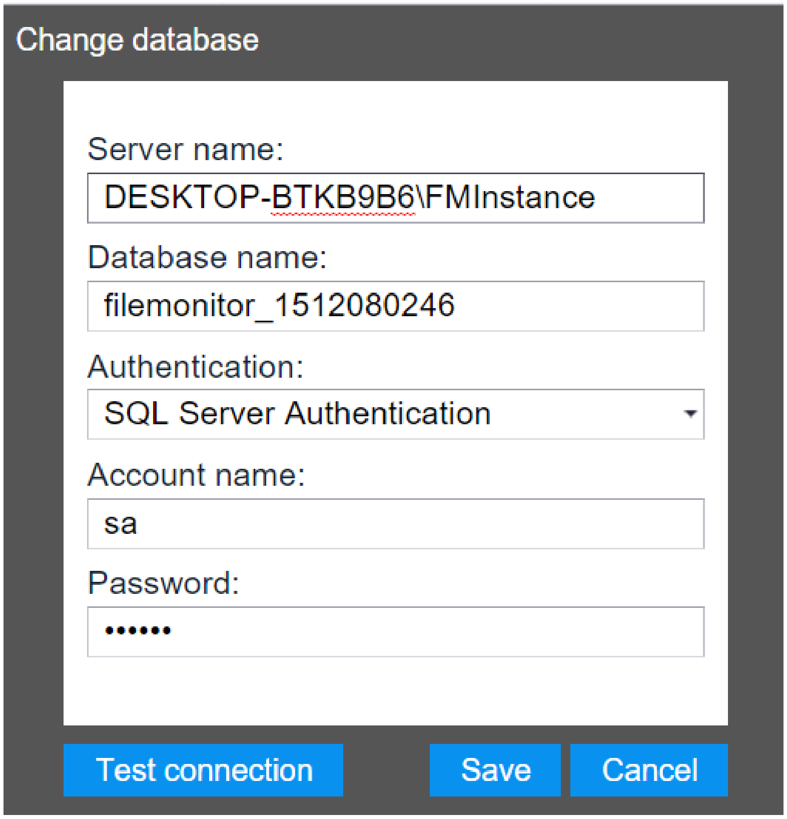
Figure 51: Create report from view

Change the source database for the view

By default, the Data viewer uses the currently configured database (Settings -> SQL Configuration – see “Database settings” for details) and will display its configuration (server: database name) at the top of the page, right beneath the title.

For advanced data analysis and forensic use cases, it is also possible to load data from a database different than the current database configured in Settings -> “Database settings” – the database where the information is currently being archived to. To do that, please click the “Change database” button, icon 🛢. A menu will be displayed enabling the selection of two options:

- Switch to main database: this option will switch the data source of the Data viewer to the database configured in Settings -> SQL configuration;
- Switch to another database: this option enables you to select another database as a data source for the Data viewer as follows:
  - SQL Server instance name you want to use;
  - The name of the database you want to use;
  - Select the type of authentication. If SQL Authentication, enter SQL credentials.
  - Optional (recommended): use the “Test connection” button to verify that the details entered are accurate.
  - Click “Save” to save the new configuration.



Change database

Server name: DESKTOP-BTKB9B6\FMInstance

Database name: filemonitor_1512080246

Authentication: SQL Server Authentication

Account name: sa

Password: ••••••

Figure 52: Change database for Data viewer

Deleting a view

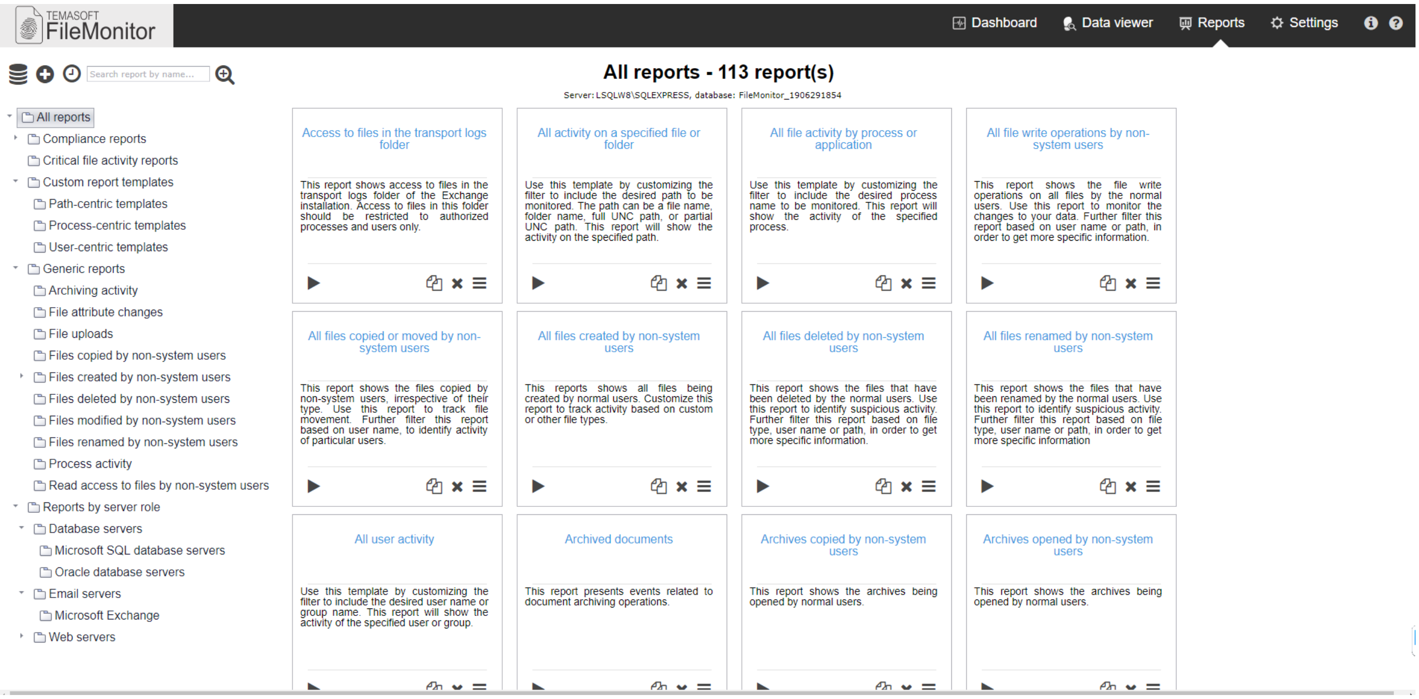
To delete a view, select it from the comb box containing the list of available views, so that it becomes the current view. Use the "Delete" button, icon ✖ in the toolbar at the top left of the page and the view will be deleted. The next view in the list will become the current view. Alternately you can edit the view and use "Save" which will overwrite this view with the new configuration.

7 Reporting

This chapter describes how to use the reporting section in the TEMASOFT FileMonitor Server Console to make use of the data that TEMASOFT FileMonitor agents collect.

To reach the reporting section please follow these steps:

- Open the TEMASOFT FileMonitor web console by accessing http://[MACHINE NAME]:1753 (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace "localhost" with the appropriate TEMASOFT FileMonitor Server IP)
- Navigate to the "Reports" page;



All reports - 113 report(s)

Server: LSQLW8\SQLEXPRESS, database: FileMonitor_1906291854

Access to files in the transport logs folder

This report shows access to files in the transport logs folder of the Exchange installation. Access to files in this folder should be restricted to authorized processes and users only.

All activity on a specified file or folder

Use this template by customizing the filter to include the desired path to be monitored. The path can be a file name, folder name, full UNC path, or partial UNC path. This report will show the activity on the specified path.

All file activity by process or application

Use this template by customizing the filter to include the desired process name to be monitored. This report will show the activity of the specified process.

All file write operations by non-system users

This report shows the file write operations on all files by the normal users. Use this report to monitor the changes to your data. Further filter this report based on user name or path, in order to get more specific information.

All files copied or moved by non-system users

This report shows the files copied by non-system users, irrespective of their type. Use this report to track file movement. Further filter this report based on user name, to identify activity of particular users.

All files created by non-system users

This reports shows all files being created by normal users. Customize this report to track activity based on custom or other file types.

All files deleted by non-system users

This report shows the files that have been deleted by the normal users. Use this report to identify suspicious activity. Further filter this report based on file type, user name or path, in order to get more specific information.

All files renamed by non-system users

This report shows the files that have been renamed by the normal users. Use this report to identify suspicious activity. Further filter this report based on file type, user name or path, in order to get more specific information

All user activity

Use this template by customizing the filter to include the desired user name or group name. This report will show the activity of the specified user or group.

Archived documents

This report presents events related to document archiving operations.

Archives copied by non-system users

This report shows the archives being opened by normal users.

Archives opened by non-system users

This report shows the archives being opened by normal users.

Figure 53: TEMASOFT FileMonitor Reports

The "Reports" page consists of the following items:

- A toolbar with main buttons at the top left of the page;
- A tree view displaying the list of available report groups, which are used for better organizing the reports. Each report group may have one or more reports or report groups. You can add report groups at any level in the tree.
- A list view displaying the reports in the currently selected report group on three columns. You can add reports to any report group. The title of the list view is the name of the currently selected report group. The title also displays the number of reports in the selected report group.

Default reports and report groups

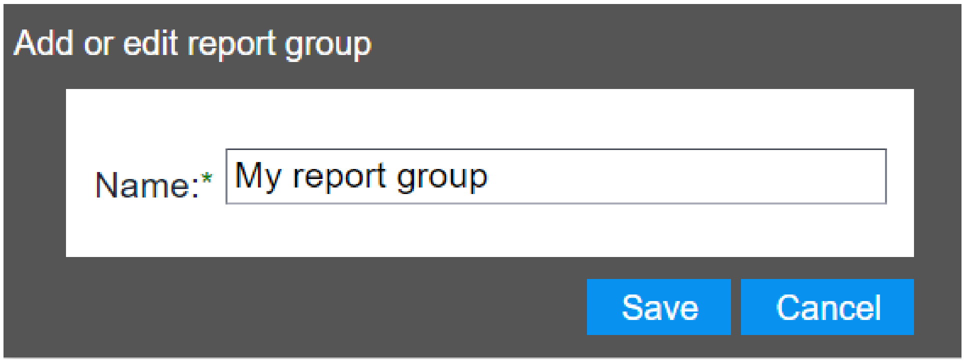
TEMASOFT FileMonitor offers more than 100 reports out of the box, organized in about 30 report groups.

Managing report groups

Report groups are managed using the buttons in the toolbar at the top left of the page.

Adding a report group

To add a report group, first select the parent group. If you want to create a top-level group, please select the "All reports" node in the tree view. Next, please click on the "plus" button, icon ⊕. A new dialog will be displayed. Enter a name for the group and click "Save". The group will be created.



Add or edit report group

Name:* My report group

Figure 54: Add report group

Renaming a report group

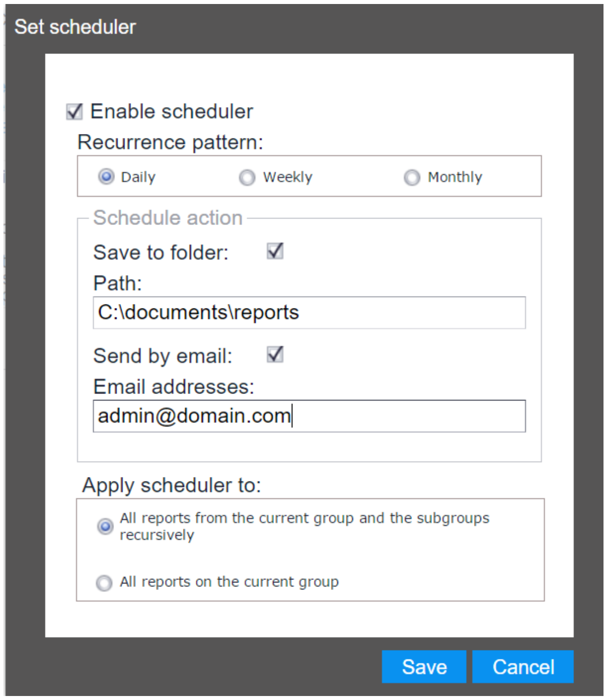
To rename a report group, please select it from the tree view and click the "Rename group button", icon ✎. The dialog in Figure 54 will appear and the "Name" edit box will be populated with the current name of the report. Make the necessary edits and click on "Save".

Deleting report groups

To delete a report group, please select it from the tree view and click the "Delete report group" button in the toolbar at the top left of the page, icon ✖. A confirmation dialog will be displayed and if "Yes" is clicked, the report group will be deleted. Please note that if the report group contains other report groups or reports, they will be deleted. Hence express caution when using this function to avoid losing reports or report groups.

Scheduling reports in a group

It is possible to schedule reports in a report group. To do so, please select the report group containing the reports that you want to schedule, and click the "Schedule" button, icon 🕘. A new dialog will appear.



Set scheduler

☑ Enable scheduler

Recurrence pattern:

● Daily ○ Weekly ○ Monthly

Schedule action

Save to folder: ☑

Path:

C:\documents\reports

Send by email: ☑

Email addresses:

admin@domain.com

Apply scheduler to:

● All reports from the current group and the subgroups recursively

○ All reports on the current group

Figure 55: Schedule reports

Please configure the scheduling options:

- Select a recurrence pattern: daily, weekly or monthly;
- Configure the folder repository where the reports will be saved
- Choose if to also send report by email; If so, configure the email address(es) where the report will be sent to;
- Choose if to apply the schedule to the reports in the group, or also to the reports in all the report groups in this group, recursively.
- Click “Save” to finish configuring the schedule.

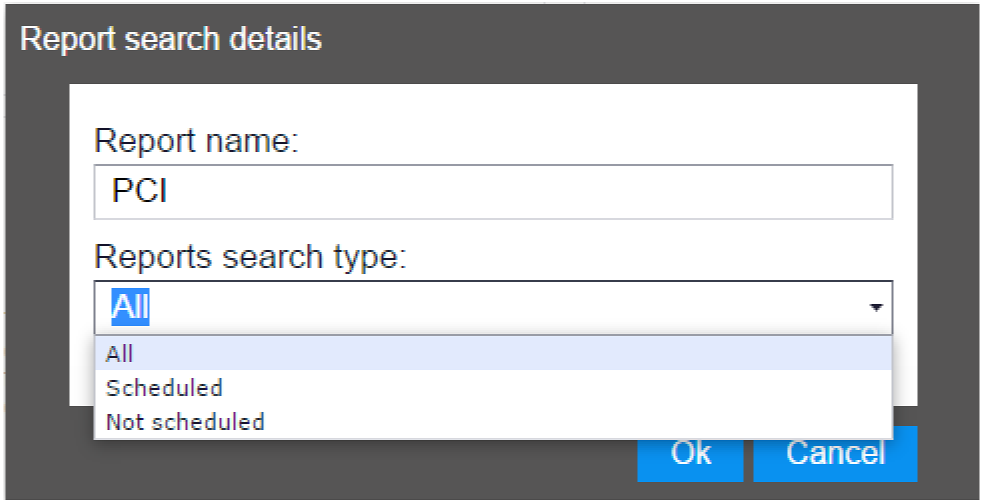
The reports will be sent in PDF format to the configured email addresses.

Searching reports

As the number of reports and report groups can become large, there is a “search for reports” function available. The function searches for reports by name. To use it, please enter text in the edit box “Search for reports” located in the toolbar at the top left of the page. The search function works on the fly and populate the list view with the results, as you type. The search function works on report groups and will only look in the report group that is currently selected in the tree view. If you wish to search through all reports, please select the “All reports” node in the tree view.

Advanced search

Please use the advanced search, button 🔍 to be able to search reports based on their scheduling settings. When clicking the button, a new dialog will appear. Enter your search criteria and click “Ok”.


Report search details

Report name: PCI

Reports search type: All

Figure 56: Reports - Advanced search

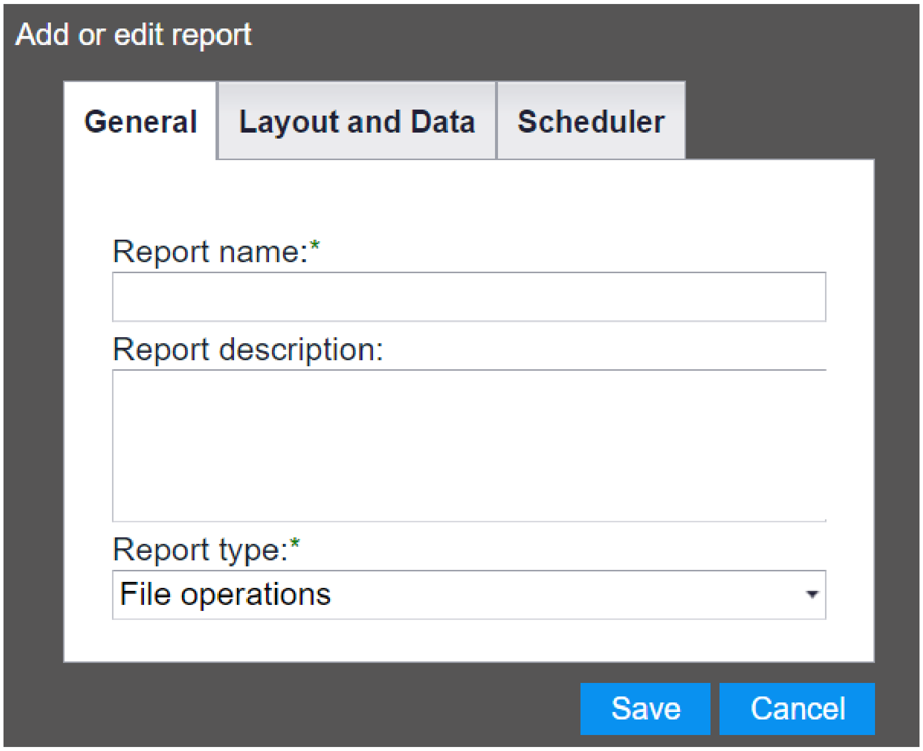
Managing reports

The existing reports are managed using the buttons at the bottom of the report panel belonging to each report in the list view, except adding reports, which is a report group function and is accessible through a button in the main toolbar at the top left of the page.

Adding reports

To add reports to a report group, please select the group first. Then click the “Add report” button, icon ⊞ in the toolbar at the top left of the page. A new dialog containing three tabs will be displayed.

The “General” tab


Add or edit report

Report name:*

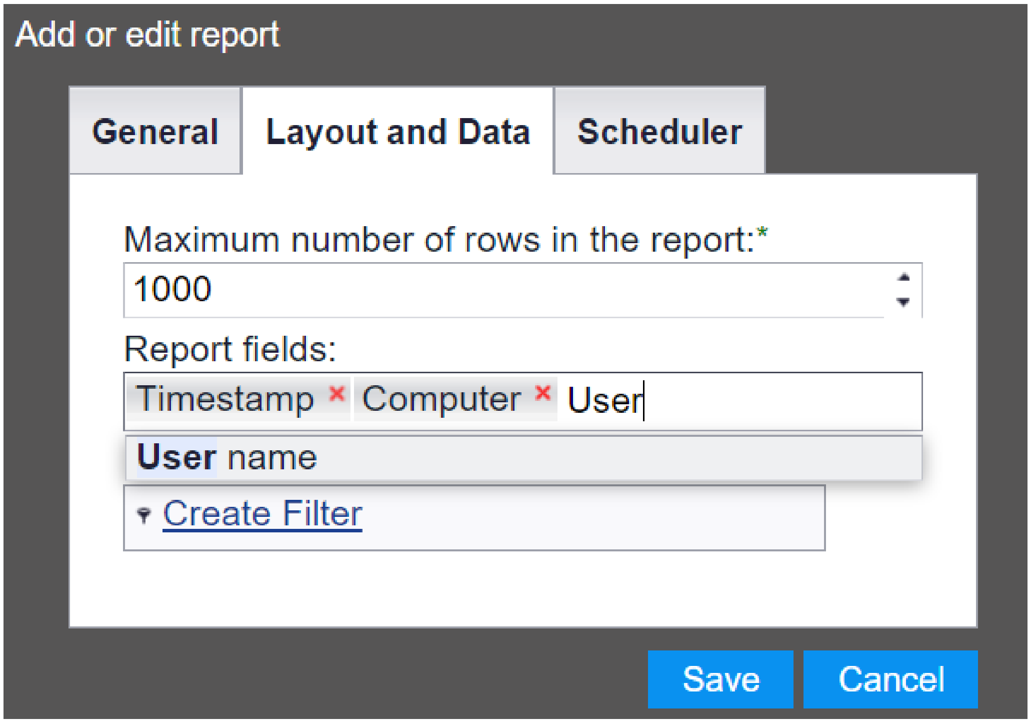
Report description:

Report type:* File operations

Figure 57: Add or edit report - the "General" tab

On this tab, you need to configure the report name, report description (optional) and the report type. The report type can be one of the following: “File operations” – if you want to show file operations in the report, “agent status” – if you want to report on the status of the TEMASOFT FileMonitor agents and “User interface operations” – if you want to report on the activity which takes place on the TEMASOFT FileMonitor Server Console.

The “Layout and Data” tab



Maximum number of rows in the report:*
1000

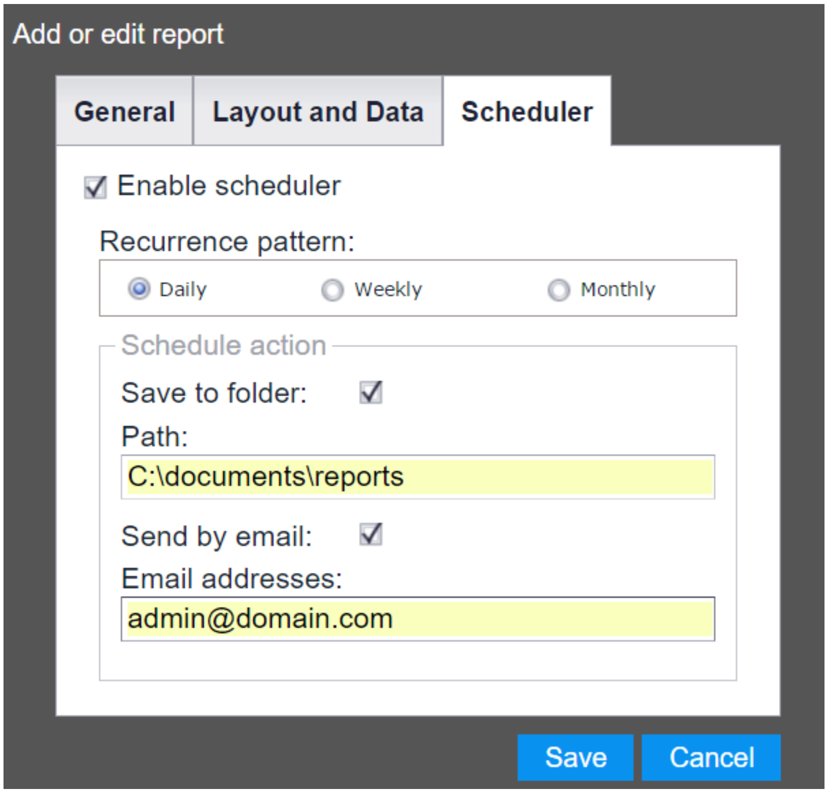
Report fields:
Timestamp × Computer × User
User name

Figure 58: Add or edit report - the "Layout and data" tab

On this tab, you need to configure the following:

- The maximum number of records in the report – defaults to 1000. This means that the top 1000 records that match the report filter will be inserted into the report. The events are inserted in the database chronologically, so this means that the latest 1000 records will be inserted in the report. You can change this number by editing the edit box or by using the up /down arrow buttons at the left side of the edit box;
- The report fields. These are the fields that get listed as the columns of the reports. For a list of available event fields, please see “Event fields”. The list of event fields is populated with all fields by default. You can remove them by pressing backspace with the focus on this list, or by clicking the red “x” button corresponding to each field that you want to remove. You can add such fields by typing in their name. There is an auto-complete function available, making it easier to find the fields that you need (as in Figure 58);
- The report filter: this is the criteria which establishes which records are listed in the report. For example, if you would like to see all the file copy operations, you would use a filer like “Action” equals “File copy”. To create a filter, please click on the “Create filter” link. This will bring up the Filter Builder dialog. Please see “Using filters” for information on how to build a filter.

The “Scheduler” tab



☑ Enable scheduler

Recurrence pattern:

● Daily ○ Weekly ○ Monthly

Schedule action

Save to folder: ☑

Path:

C:\documents\reports

Send by email: ☑

Email addresses:

admin@domain.com

Figure 59: Add or edit report - the Scheduler tab

On this tab you need to configure the scheduling options, if you want to schedule this report individually.

- First, set the recurrence interval: daily, weekly or monthly;
- Choose if to save report, send it by email or both;
- Optional: configure a folder where the report will be saved to;
- Optional: configure the email address(es) where the report will be sent to;
- Click "Save" to save the report.

The scheduled report will be saved and emailed in PDF format. The new report will appear as a new report panel in the list view when the focus is on the parent group in the tree view.

Editing reports

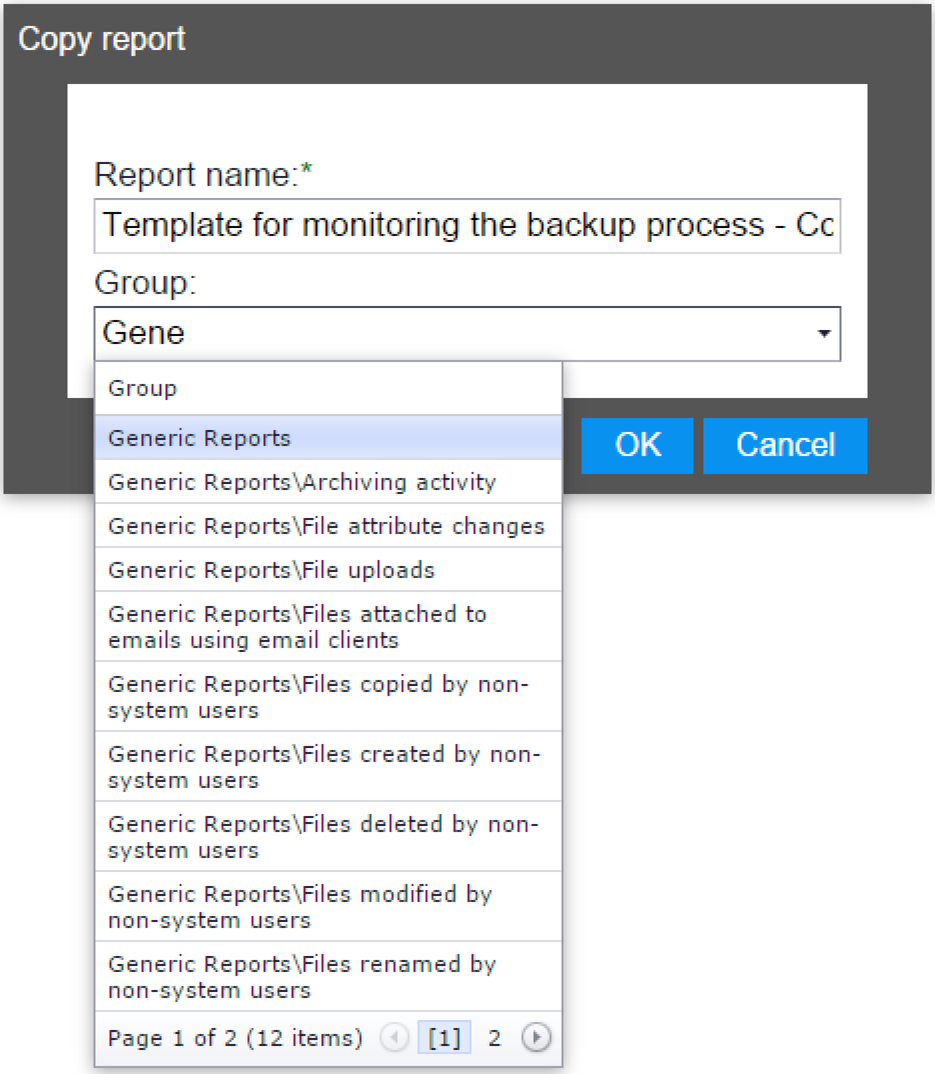
To edit a report, please click the "Edit" button, icon ≡ at the bottom right of the report panel, in the list view. This will bring up the "Add or edit" dialog having three tabs, presented in figures 58 through 62. The information is configured in a similar manner as when adding the report.

Deleting reports

To delete a report, please click the "Delete" button, icon ✖ at the bottom right of the report panel, in the list view. A confirmation dialog will be presented, and if "yes" is clicked, the report will be deleted.

Copying reports

Sometimes it may be easier to create new reports by copying existing ones and making slight modifications to the settings of the copy. Hence, the "copy report' function is available. To use it, click the "Copy" button at the bottom left of the report panel in the list view. A new dialog will appear.



Copy report

Report name:*

Template for monitoring the backup process - Cc

Group:

Gene

Group

Generic Reports

Generic Reports\Archiving activity

Generic Reports\File attribute changes

Generic Reports\File uploads

Generic Reports\Files attached to emails using email clients

Generic Reports\Files copied by non-system users

Generic Reports\Files created by non-system users

Generic Reports\Files deleted by non-system users

Generic Reports\Files modified by non-system users

Generic Reports\Files renamed by non-system users

Page 1 of 2 (12 items) [1] 2

Figure 60: Copy report

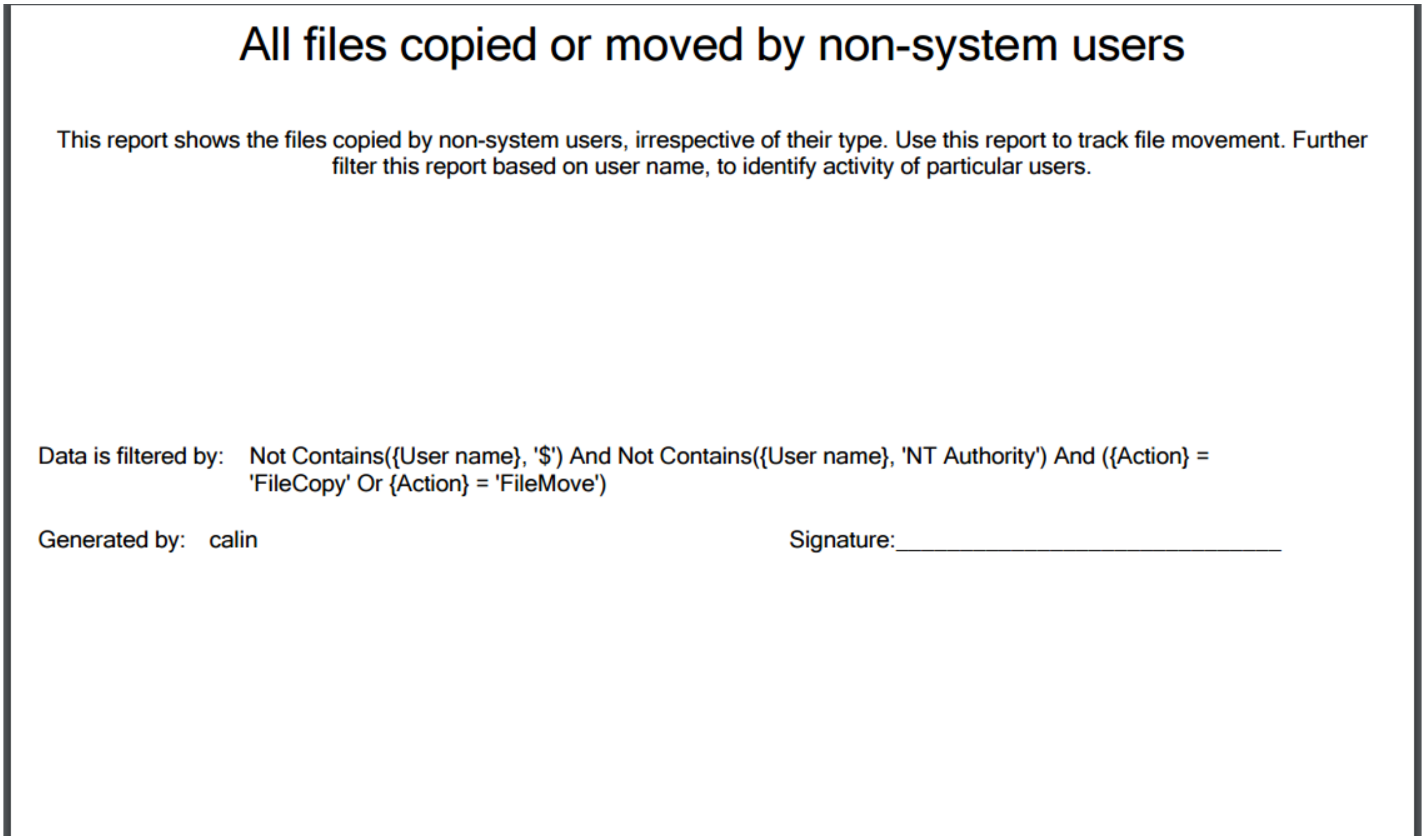
Next, edit the name of the report, if needed. Then, select the destination group, where the report will be copied to. There is a combo box containing the report groups available, but there is also a search function that searches as you type and populates a mini list of results as can be seen in Figure 60, in order to make it easier to find the target report group that you want to copy to. Select it from the list and click “Ok” to complete the copy operation.

Generating reports

To generate a report, please click the “Generate” button, icon ▶ at the bottom left of the report panel. This will result in the report being generated and opened in a new tab in your browser, in HTML format. The resulting report will have a cover page as can be seen in the image below, followed by the pages populated with data.

The report cover page

The cover page contains the title of the report (name), its description, date when the report was generated, the user who generated it as well as the filtering condition.



All files copied or moved by non-system users

This report shows the files copied by non-system users, irrespective of their type. Use this report to track file movement. Further filter this report based on user name, to identify activity of particular users.

Data is filtered by: Not Contains({User name}, '$') And Not Contains({User name}, 'NT Authority') And ({Action} = 'FileCopy' Or {Action} = 'FileMove')

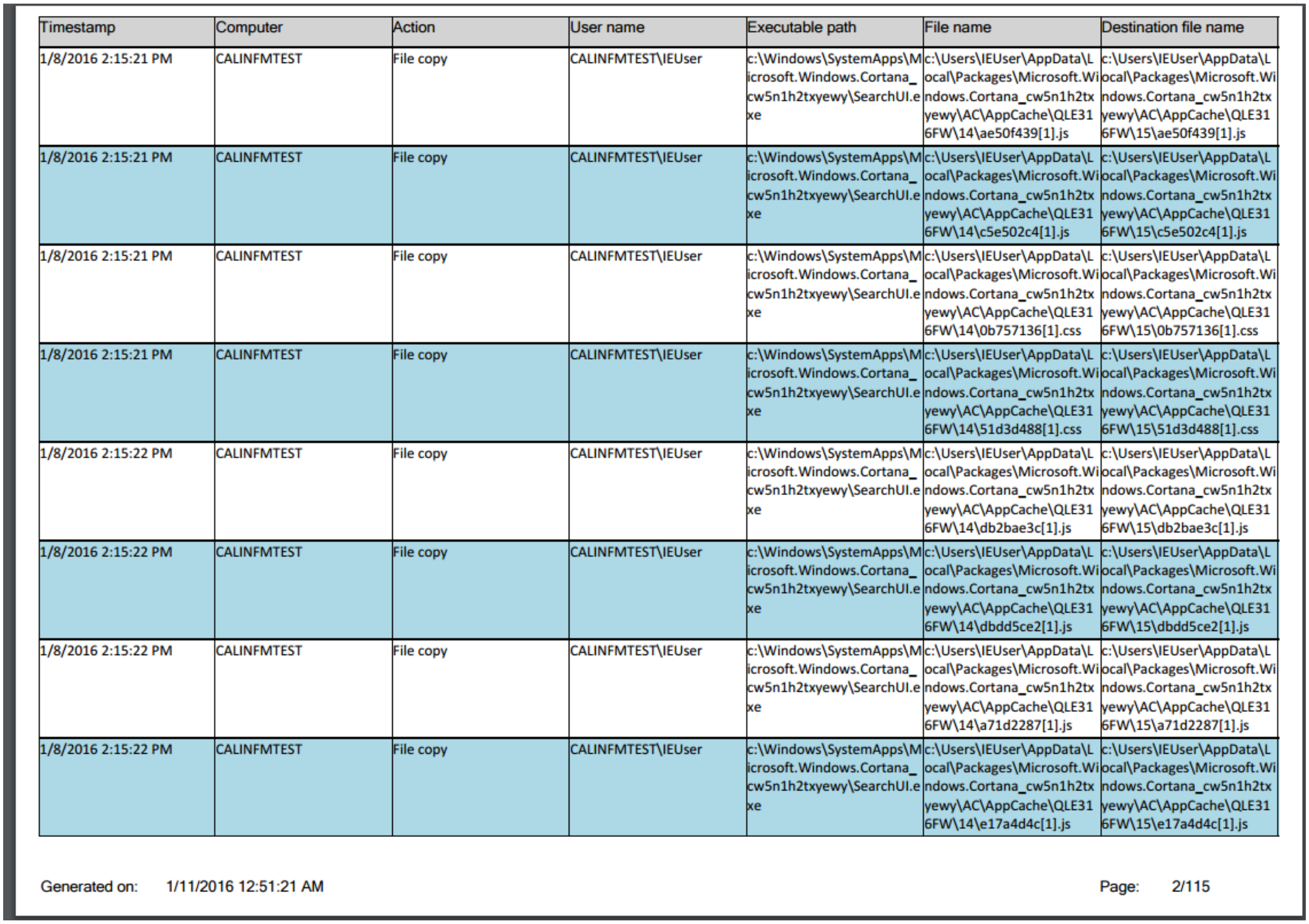
Generated by: calin

Signature:________________________________

Figure 61: Report cover page

The report contents

The report contents are presented in a tabular format and will contain the data that meets the filtering criteria. The data is listed using the columns (event fields) configured in the report.



Timestamp	Computer	Action	User name	Executable path	File name	Destination file name
1/8/2016 2:15:21 PM	CALINFMTEST	File copy	CALINFMTEST\IEUser	c:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\14\ae50f439[1].js	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\15\ae50f439[1].js
1/8/2016 2:15:21 PM	CALINFMTEST	File copy	CALINFMTEST\IEUser	c:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\14\c5e502c4[1].js	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\15\c5e502c4[1].js
1/8/2016 2:15:21 PM	CALINFMTEST	File copy	CALINFMTEST\IEUser	c:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\14\0b757136[1].css	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\15\0b757136[1].css
1/8/2016 2:15:21 PM	CALINFMTEST	File copy	CALINFMTEST\IEUser	c:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\14\51d3d488[1].css	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\15\51d3d488[1].css
1/8/2016 2:15:22 PM	CALINFMTEST	File copy	CALINFMTEST\IEUser	c:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\14\db2bae3c[1].js	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\15\db2bae3c[1].js
1/8/2016 2:15:22 PM	CALINFMTEST	File copy	CALINFMTEST\IEUser	c:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\14\dbdd5ce2[1].js	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\15\dbdd5ce2[1].js
1/8/2016 2:15:22 PM	CALINFMTEST	File copy	CALINFMTEST\IEUser	c:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\14\a71d2287[1].js	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\15\a71d2287[1].js
1/8/2016 2:15:22 PM	CALINFMTEST	File copy	CALINFMTEST\IEUser	c:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\14\e17a4d4c[1].js	c:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\QLE316FW\15\e17a4d4c[1].js

Generated on: 1/11/2016 12:51:21 AM

Page: 2/115

Figure 62: Report contents

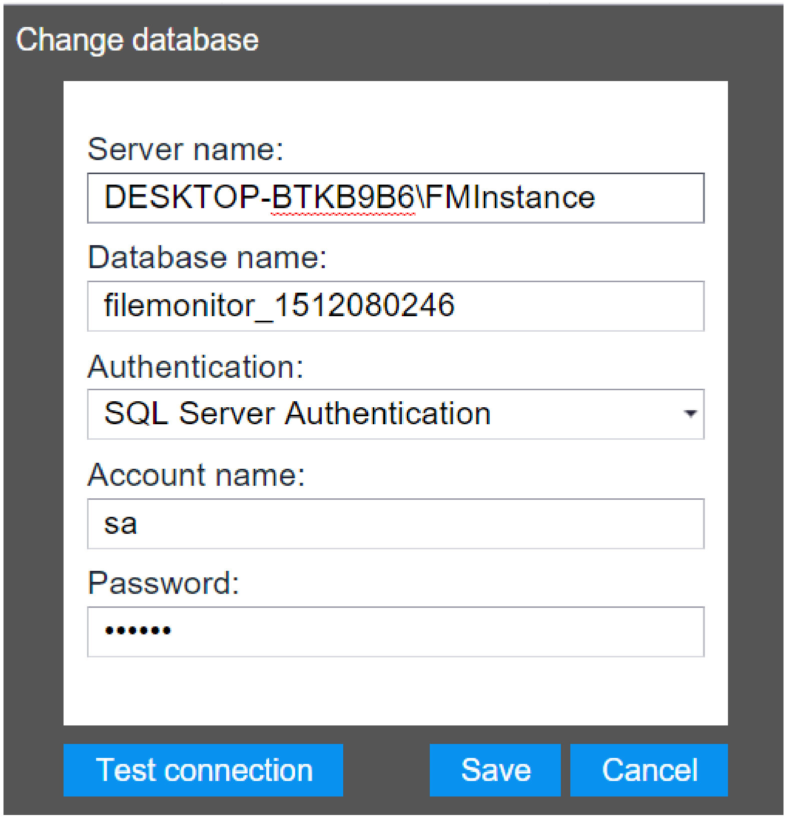
Changing the data source

By default, the reports run on the database configured in Settings -> SQL configuration. Please see "Database settings" for details. However, it is possible to change the data source for the report, without changing the main database where the TEMASOFT FileMonitor agents are saving data to. To do that, click the "Change database" button, icon 🛢. A new menu will be displayed presenting two options:

- Switch to main database: this option will switch the data source of the reports to the database configured in Settings -> SQL configuration;
- Switch to another database: this option enables you to select another database as a data source for the reports as follows:

A new dialog will be displayed, containing the settings of the currently configured database. To change the database used by the reports, please enter the necessary information in this dialog:

- SQL Server instance name you want to use;
- The name of the database you want to use;
- Select the type of authentication. If SQL Authentication, enter SQL credentials.
- Optional (recommended): use the "Test connection" button to verify that the details entered are accurate.
- Click "Save" to save the new configuration.



Server name: DESKTOP-BTKB9B6\FMInstance

Database name: filemonitor_1512080246

Authentication: SQL Server Authentication

Account name: sa

Password: ••••••

Figure 63: Change database

The currently active SQL Server and database are listed below the title of the main page.

8 Troubleshooting

8.1 Known limitations

Limitations regarding copying files

When monitoring a Windows machine, the copy operations from the Windows machine to a network destination which does not have a TEMASOFT FileMonitor Agent is detected and logged accordingly. However, a file copy operation from a network machine to a monitored machine is not detected in all the cases because sometimes (especially on slower networks) not all information can be retrieved in a timely fashion from the network driver. On the other hand, the product does log a "file create" and a "file write" event for each such file if the path is monitored.

TEMASOFT FileMonitor can detect most copy operations, involving normal activities and normally used files. However, if the file being copied is intensively changed (as is the case with log files, for example), the file copy operation may not be detected. In addition to that, there are some situations where TEMASOFT FileMonitor detects a file copy operation, but because of the data and processes in the memory, it cannot tell for sure where the source file of the file copy operation is. In this case, a "file content duplicated" event will be logged. The destination file name will contain the path and file name of the file to which the content was copied, and the "details" field will contain a list of possible file sources or destinations for the file copy operation. Although the product cannot pinpoint which one of the possible sources is the actual source, for sure one of them is the source file.

Limitations regarding detecting file archiving operations

TEMASOFT FileMonitor detects when a process archives a file and signals a "file archived" event. This is useful to detect attempts to evade protective measures when moving data around the company or uploading it to the internet. To be able to detect when files are archived make sure the monitoring profile associated to those files is set to monitor everything. There are also some circumstances under which file archived operations are not accurately detected in all cases:

- In rare cases, if the process performing the archiving does not end, we cannot detect the archiving operation. Also, if the process deletes the archive before it exits, the "file archived" operation will not be detected;
- "File archived" detection uses the file name, file size and timestamp of the file being archived as a correlation field. Hence, in certain conditions with multiple levels of nesting within the archive and multiple files, it is difficult to detect which files are archived. We point out these cases through a special action called "File probably archived".

Limitations regarding detecting file upload through browsers and file attached to Outlook operations

TEMASOFT FileMonitor detects when a file is read by a browser and it marks the action as a file upload through browsers. This operation however makes sense for documents and not for all files (e.g. dlls or other files which are used internally by browsers) so only when documents are read by browsers it usually happens when the documents are uploaded to various web sites. This operation is detected for most of the browsers, however for Microsoft Edge, not all file uploads are detected because sometimes various other Windows applications are used to read the files and then their content is sent directly to Edge by those apps.

"File attached to Outlook" operations are marked for those files which are attached to an email in Microsoft Outlook. This usually happens when users send emails with attachments, but it can also happen when users read documents attached to emails directly from Outlook. The name of this operation may change in the future to better reflect this situation.

Note: if you want to monitor files being attached to other type of desktop email clients, you need to identify the temporary folder where the attachment is copied as part of the process of attaching a file to an email. Usually such folders are in the “\ProgramData\” folder of the system partition, or in the temporary files of the user profile. When the folder is identified, you need to create an action that would flag any file being copied there, as attached to the email by the email client you want to monitor.

8.2 Troubleshooting agent deployment (Windows)

When testing the agent deployment settings in the user interface and the outcome is a failure message, please follow the below procedure to troubleshoot further:

- First make sure that the computer name of the machine that needs to be monitored is correct;
    - Run a ping command to the computer name or IP and see if it responds;
- Then make sure that the credentials you are supplying are correct:
    - Run a command console and type “net use \\computername” where “computername” is the name or IP of the target computer;
    - Enter the user named when prompted and then the password;
    - If the connection is successful, the credentials are correct;
    - If the connection is not successful, check the error message received. If “invalid user name or password” is received, the credentials are not correct;
- Troubleshooting access denied errors
    - When performing the above procedure, you may receive an “access denied” error;
    - To troubleshoot this, please verify the following:
        - Check if the credentials, although correct, have enough rights to connect to the machine;
        - Check the “sharing and security model” policy on the agent computer and make sure it is set to “Classic – local users authenticate as themselves”
        - Make sure file and printing sharing is enabled on the target machine;
        - Make sure network discover is enabled on the target machine;
        - The TEMASOFT FileMonitor Server uses \\computername\share$ to deploy the agents so make sure that administrative shares are enabled;
        - Make sure that the UAC remote restrictions do not apply. Please visit https://support.microsoft.com/en-us/kb/951016 in order to understand how UAC remote restrictions work, and what to do in order to allow access to administrative shares.

If none of the above help, please contact TEMASOFT support.

8.3 Enabling Debug mode

Enabling debug mode on TEMASOFT FileMonitor Server:

- Go to the installation directory of TEMASOFT FileMonitor Server – default folder is “C:\Program Files (x86)\Temasoft\FileMonitor Server”;
- Locate the logger.config.xml file and open it;
- Locate the <Level> </Level> tag;
- Replace the default value “Error” with “Info” ;
- Save the file and restart the product components:
    - Web console;
    - TEMASOFT FileMonitor Server Service (FileMonitor Server);
- Verbose logging is enabled for the server;

This procedure enables verbose logging for the TEMASOFT FileMonitor Server. This may be required to troubleshoot user interface issues, database related issues, reporting and alerting issues and communication issues.

To enable debug for the web UI, please change the same value in the "logger.config.xml" file from the C:\inetpub\wwwroot\FileMonitor\FileMonitor\ folder (assuming C: is the system partition).

Enabling debug mode on TEMASOFT FileMonitor Agent:

- Go to the installation directory of TEMASOFT FileMonitor Agent – default folder is "C:\Program Files (x86)\Temasoft\FileMonitor Agent";
- Locate the logger.config.xml file and open it;
- Locate the <Level> </Level> tag;
- Replace the default value "Error" with "Info" ;
- Save the file and restart the product components:
    - TEMASOFT FileMonitor Agent Service (FileMonitor Agent);
- Verbose logging is enabled for the agent;

This procedure enables verbose logging for the TEMASOFT FileMonitor Agent. This may be required to troubleshoot agent functionality such as file operations not being properly recorded.

8.4 Troubleshooting the web console

The TEMASOFT FileMonitor Server web console is using the locally installed IIS. Assuming installation was successful but the web console does not start, please go through the check list below:

- Make sure that the TEMASOFT FileMonitor Service ("FileMonitor Server") is running;
- Make sure that the "World Wide Web Publishing Service" is running;
    - Start -> Run -> type services.msc, sort the list by name, find the above services and check their status
    - If any of them are stopped, please start it.
- If both services are running fine, please verify if the port used by TEMASOFT FileMonitor Server web console in IIS is available for use. If the port is in use by another application, then the web console will not start
    - Default port for TEMASOFT FileMonitor Server web console is 1753;
    - Start-> Run -> type cmd.exe
        - Run "netstat –an|more", press a key to scroll the view;
        - Check if the port 1753 appears in the list and note the process ID using it;
        - If the process is different than "System" you have two options
            - Free the port and restart the "World Wide Web Publishing Service" and the TEMASOFT "FileMonitor Server" service;
            - In case you cannot free the port, change the default port for the TEMASOFT FileMonitor Server web console (note, this will change the port for other web applications too, if any):
                - Open IIS Manager and in the tree vie at the left, expand Sites and click the "Default site"
                - In the action pane at the top right, click on "Bindings"
                - Edit the binding for "http" (defaults to 80) and select another port number.
                - Save and restart the "World Wide Web Publishing Service";
                - Load the TEMASOFT FileMonitor Server console by running by accessing http://[MACHINE NAME]:%yourportnumber% (assuming you are on the same machine where the TEMASOFT FileMonitor server has been installed – otherwise, please replace "localhost" with the appropriate TEMASOFT FileMonitor Server IP). Replace %yourportnumber% with the value you have set in IIS. For example if you set 88 as the Binding for

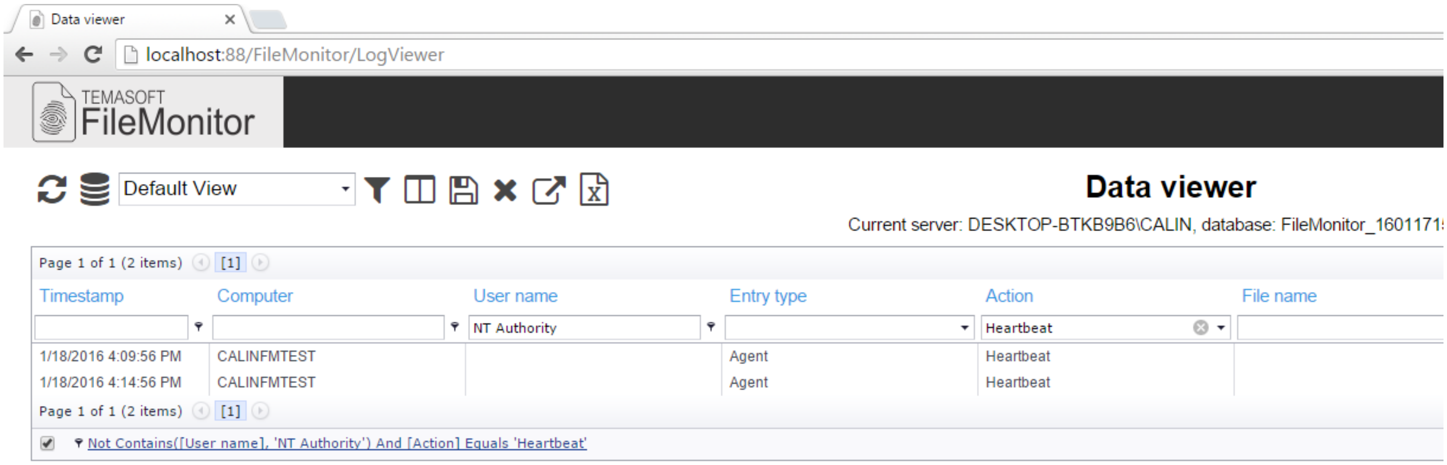
http in IIS, use [http://[MACHINE NAME]:88](http://[MACHINE NAME]:88) to launch the TEMASOFT FileMonitor Server Console.

- If none of the above works, please enable debug mode as per [“Enabling debug mode”]() and contact TEMASOFT support.

8.5 Some file activity does not show up in the TEMASOFT FileMonitor Server Console

This exercise assumes you have a running installation of TEMASOFT FileMonitor Server, with at least one agent deployed, and that you have configured the agent to scan a “custom” location by creating a monitoring profile that includes that location (see [“Monitoring profiles”]() for “how to”) and assigning this monitoring profile to the deployed agent. However, even though you have performed file activity there, you do not see it in the main console -> Data viewer (See [“Data Analysis”]() for “how to”).

- First make sure you create the correct filter in Data viewer- this ensures you are not missing the information. For more information on filters, please see [“Using filters”](). To troubleshoot this, you need a single filter similar to “File name contains PATH” where PATH is the repository you want to monitor (and you have configured in your monitoring profile).
- If this filter does not return results, continue troubleshooting:
    - Verify if the computer you are monitoring is live by sending a ping request;
    - If the computer is live, verify if the TEMASOFT FileMonitor Agent service is running (”FileMonitor Agent”);
    - If the agent is running fine, and the connectivity between the computer you are monitoring and the TEMASOFT FileMonitor Server is sound, please check the status of this in the TEMASOFT FileMonitor Server Console:
        - Go to the Data viewer(See [“Data Analysis”]() for more info);
        - Load the default view;
        - Locate the “Action” column;
        - Select “Heartbeat” in the combo box that appears when you click the edit box under the column label;
        - In the list that appears verify when is the last time when connectivity between TEMASOFT FileMonitor Server and the computer you want to monitor took place:



Data viewer

Current server: DESKTOP-BTKB9B6\CALIN, database: FileMonitor_1601171

Page 1 of 1 (2 items) [1]

Timestamp	Computer	User name	Entry type	Action	File name
		NT Authority		Heartbeat	
1/18/2016 4:09:56 PM	CALINFMTEST		Agent	Heartbeat	
1/18/2016 4:14:56 PM	CALINFMTEST		Agent	Heartbeat	

Page 1 of 1 (2 items) [1]

☑ Not Contains([User name], 'NT Authority') And [Action] Equals 'Heartbeat'

Figure 64: Troubleshooting agent connectivity

- If you cannot see the computer you want to monitor in this list, please enable debug as per “Enabling debug mode” and contact TEMASOFT support.
- If you can see the computer you want to monitor in the list, please troubleshoot further:
  - Re-verify configuration: Check if the monitoring profile is correct and that the correct path is configured and included for monitoring;
  - Re-verify configuration: Check if the monitoring profile is correctly assigned to the computer you want to monitor;
  - Look for any “ignore” actions (see “Actions and alerting”): Verify the list of configured actions and see if any is enabled. If so, please check the filtering conditions of the action, and see if they match any parameter related to the activity you have performed, or to the path you have configured. (For example if there is an action that ignores activity of system users, or computer accounts (username contains $), and you have performed file activity on the computer from the network (via a network share), depending on your security settings, the actual file activity might have been performed by the computer account of the machine you have used to connect there. Hence, this activity may be ignored;
  - If you cannot find an ignore action that should affect this exercise, please enable debug as per “Enabling debug mode” and contact TEMASOFT support.

8.6 Database connection issues

If SQL Server connection relies on Windows Authentication and more than one user accesses the database, the additional users might get the following error when opening the web interface:

“Database check failed. Make sure FileMonitor Server service is running and both Web Interface User and FileMonitor Service User have access to the specified database”.

This usually means that even if the user has been added to the list of authorized users in the FileMonitor interface, that user doesn’t have enough rights to connect to the FileMonitor database on the SQL Server. To fix this issue, one must configure SQL Server to add the required rights for that users. This can be easily achieved by using the SQL Server Management Studio interface, and following the next steps:

- Open Security->Logins and select New Login;
- From the General section select the user;
- From the User Mapping section select the FileMonitor databases and assign the proper access rights (e.g. DB_ACCESSADMIN, DB_OWNER);
- Apply the changes;
- Close the browser and open the FileMonitor web interface.

Another issue related to the database backend might occur when one opens the web interface of FileMonitor using Edge, from the same machine as the one hosting the FileMonitor Server and SQL Server. The following error will be displayed:

“Database check failed. Edge is not supported for local browsing. Please use a different browser or connect from a remote machine.”

This situation happens because of the sandbox security constraints in the Edge browser, which limits the capabilities of the authenticated users to access certain resources on the local machine. This affects the connection to a local SQL Server database. To overcome the situation, one needs to use a different browser or use Edge, but from a remote machine.