PA File Sight

Version 3.7 Pro

Last Update: July 14, 2009

Power Admin LLC
support@poweradmin.com
www.poweradmin.com

Prepared in the USA

Getting Started with PA File Sight

Thank you for choosing PA File Sight. The following topics offer some help in installing, configuring and using PA File Sight. These topics are also shown in the help menu at the left of the screen.

Installation

- Getting Started
- Quick Installation Guide

Configuration

Below are some instructions for core procedures that are used in setting up and using PA File Sight.

- Concepts
- Console
- Global Settings
- Database Settings
- HTTP Settings
- Report Settings
- Adding Monitors
- Adding Actions
- Error Auditing
- Maintenance Schedule
- Import & Export Configurations
- External API

Monitors

Monitors are the "building blocks" of PA File Sight. The following help topics explain the functionality of each monitor.

- File Sight Monitor

Actions

Monitors use Actions to notify you of error conditions or to run automated fixes in response to error conditions. The following help topics explain how each of the actions works.

- Dial-Up Connection
- E-mail Alert
- Execute Script
- Message Box
- Network Message (Net Send)
- Pager Alert via SNPP
- Phone Dialer (DTMF/SMS)
- Play Sound

- Reboot Server
- SMS Text Message
- Start Application
- Start Service
- Write to Event Log
- Write to Log File

Reports

Reports are summaries of conditions observed by PA File Sight on your network. The entries in this section explain the types of reports that are supported and how to view them.

- Server Status
- Ad Hoc Reports
- Scheduled Reports
- Publish Reports
- System Activity Log

Contents

Quick Installation Guide for PA File Sight

You will find that PA File Sight is very easy to set up and use. You just choose a directory to install into, press Next a few times, and you're done.

The product installs completely within it's own directory, with the exception of the optional Microsoft SQL Server Native Client, which is a system component and uses a Microsoft installer. The SQL Native Client is not required, and can be installed later.

Installation Considerations

PA File Sight doesn't take up much disk space. However, it records information to databases that can grow large depending on how many monitors you have and how long you keep the data. By default, the directory structure will look like this:

```
C:\Program Files
        PA File Sight
                Databases
                Reports
```

PA File Sight uses an embedded database by default. You can choose to store the bulk of your data in an MS SQL Server database if you wish.

For the embedded database's performance and integrity, it's recommended to keep the Database directory on a local NTFS drive. Putting the Database directory on a remote server via a network share is not recommended.

You can choose to move the Databases and Reports directory at a later time via the Database Settings dialog.

After the product is installed, a Startup Wizard for PA File Sight will guide you in setting up your first few monitors and actions. It will be helpful to have the following available:

- Your SMTP server information (such as SMTP server name, port (if non standard), SMTP username and password if needed) for sending alerts

Configuration

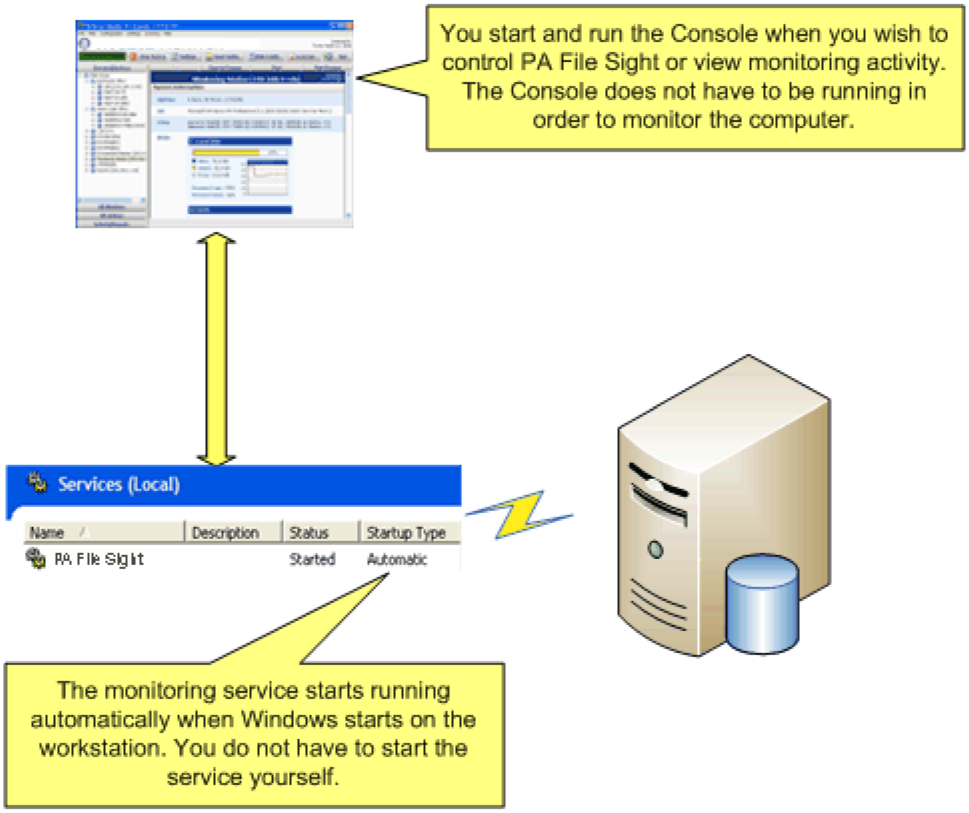
Contents

Terminology and Concepts of PA File Sight

PA File Sight runs on a Windows computer and monitors the file activity on that computer.

The PA File Sight product itself is composed of three parts: a graphical user interface that we call the Console, a background process called the monitoring service, and a file system driver that watches all file I/O on the machine. You see the Console when you launch PA File Sight from the desktop. The service is invisible and has no user interface of its own. The role of the Console program is to provide you with a convenient and effective way to work with PA File Sight.

The following diagram will give you a better idea of how the parts of PA File Sight work together.



You start and run the Console when you wish to control PA File Sight or view monitoring activity. The Console does not have to be running in order to monitor the computer.

The monitoring service starts running automatically when Windows starts on the workstation. You do not have to start the service yourself.

The service is the part of the product that performs the file monitoring. The Console does not need to be running in order for monitoring to take place. When you start the workstation that has PA File Sight installed to it, monitoring will start.

The Console, service and driver are installed at the same time when you install PA File Sight from the setup application. The service is set up so that it runs automatically when Windows starts.

Product Terminology

PA File Sight is based on the concepts of Monitors and Actions.

The PA File Sight product contains File Sight monitors that watch file I/O activity. You can create multiple File Sight monitors to watch different directories and drives on a machine. These monitors trigger Actions (such as notifications or server operations) as well as record monitored data to a database for report generation.

Monitor

A File Sight monitor continously scans file I/O activity and watches for activity that you have defined an interest in.

You can create a new Monitor by right-clicking on the computer and choosing Add New Monitor, and then filling in the required parameters.

Error Condition

An Error Condition happens when a file activity that you've specified an interest in happens. For example, if you're watching for file deletes, the deletion of a file would trigger an Error Condition.

Action

An Action is an activity that PA File Sight performs as part of its response to an Error Condition. All Actions are created from any of the available Action Types.

Examples of Action Types are sending e-mail, execution of a script, or writing text to a log file.

How Monitors And Actions Work Together

Monitors and Actions are always defined within PA File Sight as follows.

- A Monitor must be defined first.
- Actions are attached to the Monitor.

When an Error Condition occurs, the list of Actions that is attached to the Monitor is executed. Each Action in the list is executed, in the order in which it appears in the list. This list is called the Error Actions for the Monitor.

How Monitors and Actions are Created

Monitors and Actions may be created in two ways:

- Manually: you can right-click the server and choose Add New Monitor. See the help page Adding Monitors.
- Imported Server Configuration: PA File Sight provides a way to duplicate Monitors and Actions across several servers by saving the settings in a file. Refer to the help page Importing and Exporting Configurations for complete instructions.

In addition, you can manually edit any of the existing Monitors, and you can manually edit the Actions that are attached to the Monitors. You can add Actions to existing Monitors or delete them, and you can delete unneeded Monitors (and their Actions) as necessary.

[Contents](#)

PA File Sight Console

The Console is the administrative interface to PA File Sight.

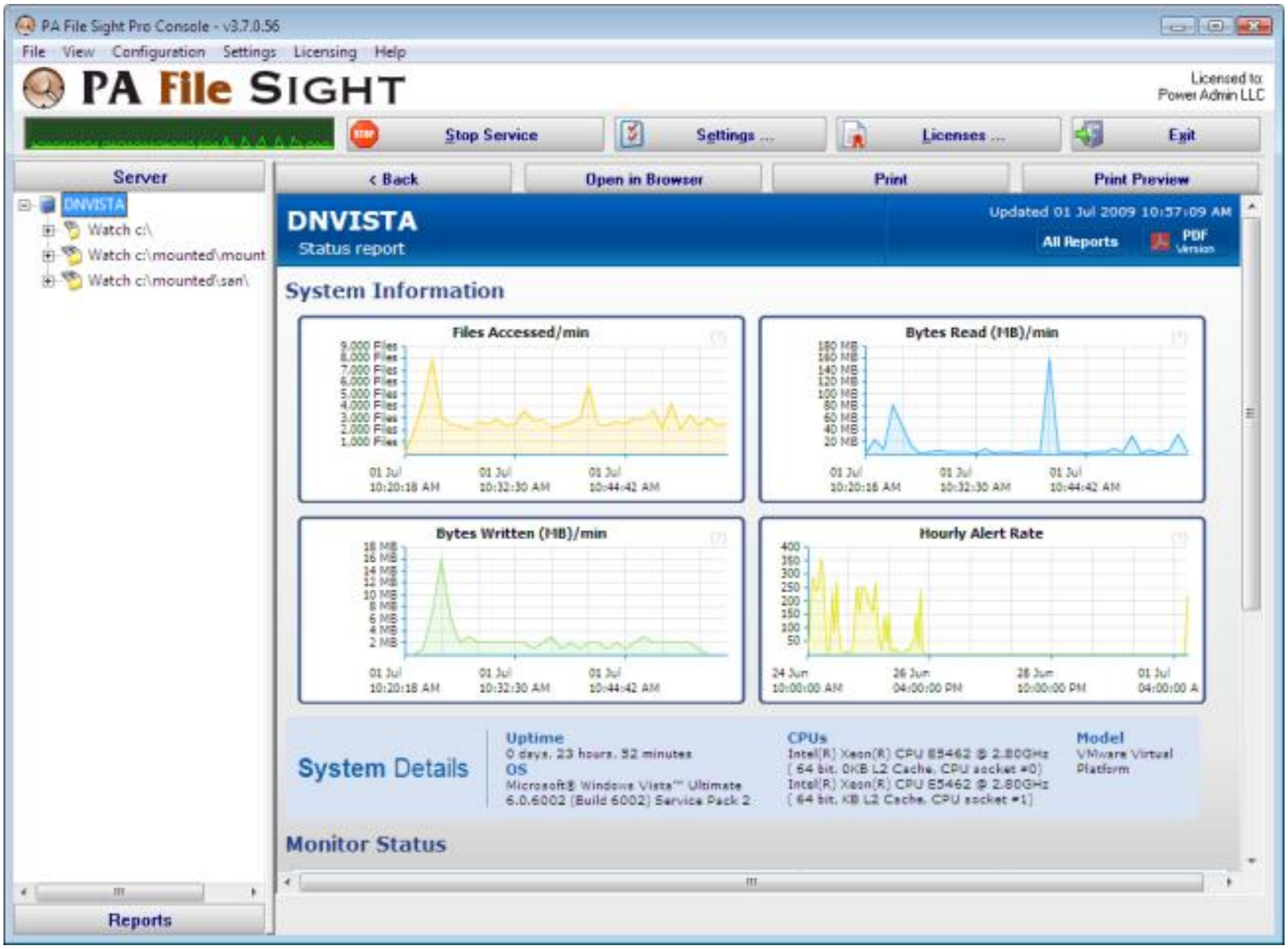
On the left side is the navigation pane. Similar to many other Windows products, this navigation pane displays items that you can interact with. Right clicking most items will give you a menu of choices. Selecting an item will cause the large right panel to change to your current selection.

In addition, you'll note that there are buttons in the navigation pane. These buttons group different items together that you can interact with.

The buttons across the top let you interact with PA File Sight as well as give you feedback.

Activity Graph The Activity Graph at the far left is an indication of system activity. The green line indicates the number of monitors that are running or scheduled to run, and the yellow line indicates the number of actions that have run.

Start/Stop Service The first button on the left lets you start and stop the PA File Sight service. When the Console first starts, it will be grey as the Console queries the operating system to determine if the service is running or not.



Uptime
0 days, 23 hours, 52 minutes

OS
Microsoft® Windows Vista™ Ultimate 6.0.6002 (Build 6002) Service Pack 2

CPUs
Intel(R) Xeon(R) CPU E5462 @ 2.80GHz (64 bit, 0KB L2 Cache, CPU socket #0)
Intel(R) Xeon(R) CPU E5462 @ 2.80GHz (64 bit, KB L2 Cache, CPU socket #1)

Model
VMware Virtual Platform

Settings The Settings button takes you to the global Settings dialog. Here you configure many aspects of the program. More information is available in the [Settings topic](#).

Licenses Licenses are installed by copying them into the PA File Sight directory. The Licenses button will display the License Manager dialog to let you see your current licensing status.

Exit This closes the PA File Sight Console. Since the actual monitoring is done by a service, exiting the Console does NOT stop the monitoring of your system.

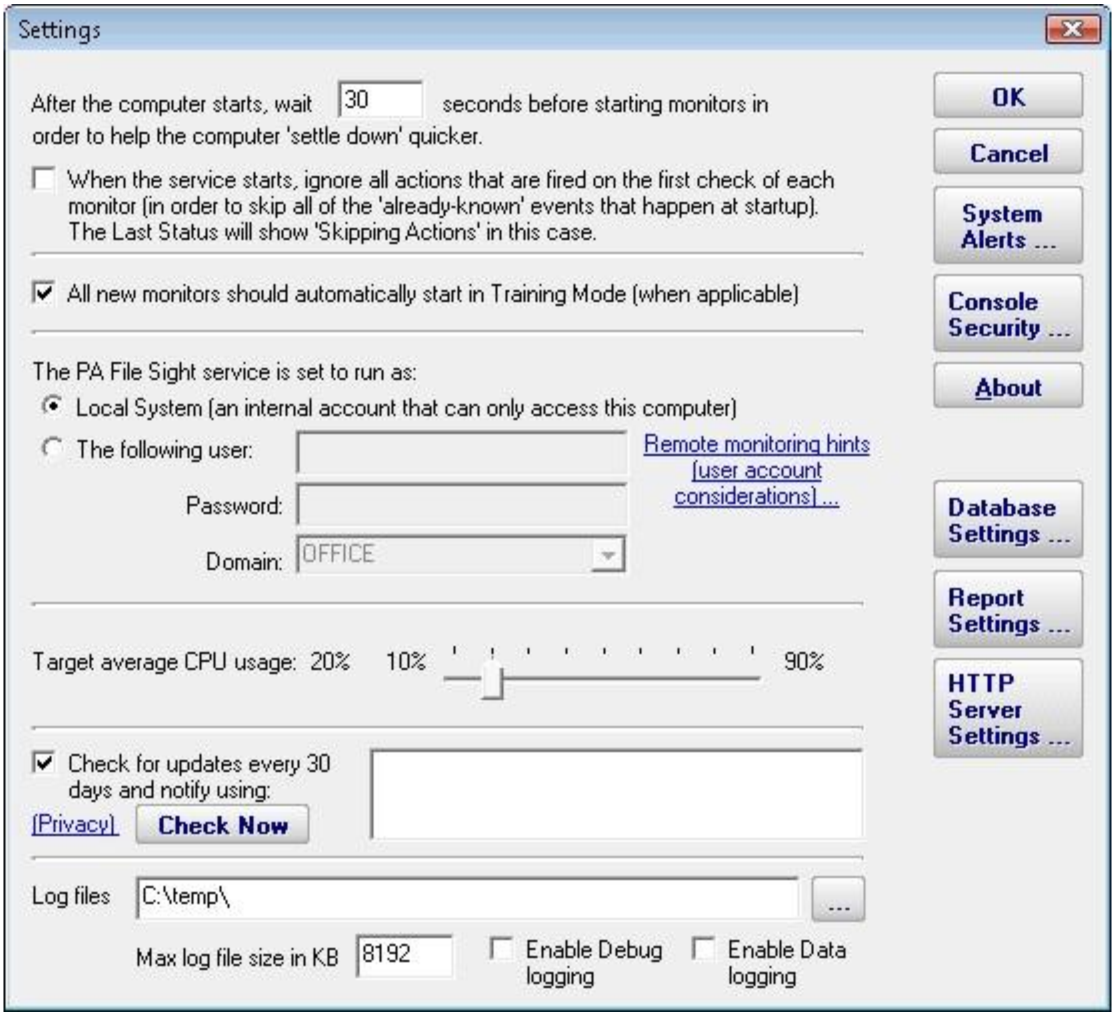
Contents

Global Settings

The Settings dialog lets you configure global aspects of the monitoring service.

There are several dialogs that are reached by the buttons on the right side of this dialog and which are also accessible via the Settings menu.

- System Alerts - Some alerts are sent to you from the monitoring system itself, and not in response to particular monitors. These alerts include security warnings (change of configuration, etc), license issues, internal problems, unaccessible computer warnings, etc. You can control which of these internal alerts are enabled, and which notification method each one should use.
- Console Security allows you to set a password that the Console will request when it is launched. This setting allows you to limit access to PA File Sight to authorized users.
- Database Settings dialog allows you to set up PA File Sight to use the embedded SQLite database or Microsoft SQL Server as the storage for PA File Sight data.
- Report Settings affect the storage of archived reports and the behavior of the reporting features of PA File Sight.
- HTTP Server Settings allows you to change details of the way the built-in web server in PA File Sight operates.



Settings

After the computer starts, wait 30 seconds before starting monitors in order to help the computer 'settle down' quicker.

□ When the service starts, ignore all actions that are fired on the first check of each monitor (in order to skip all of the 'already-known' events that happen at startup). The Last Status will show 'Skipping Actions' in this case.

☑ All new monitors should automatically start in Training Mode (when applicable)

The PA File Sight service is set to run as:

● Local System (an internal account that can only access this computer)

○ The following user:

Password:

Domain: OFFICE

Remote monitoring hints (user account considerations) ...

Target average CPU usage: 20% 10% 90%

☑ Check for updates every 30 days and notify using:

Log files C:\temp\

Max log file size in KB 8192 □ Enable Debug logging □ Enable Data logging

Startup Wait Time - When the monitoring service starts, you can instruct it to wait a number of seconds before active monitoring begins. This places less load on the system while it is starting, and also reduces false alarms that occur from the system not being completely started.

Ignore First Actions - To further reduce false alarms, the monitor service can ignore problems found on the very first run of each monitor. After the first run, all monitors will run normally.

Start in Training Mode - Most monitors support Automatic Training (see Advanced Monitor Options). When monitors are first created, they can automatically enter Training Mode. That is convenient in most cases, but it means the monitor might be a little harder to test initially since it won't fire actions until the training period has finished.

Logon As User - This is a *very* important setting. This setting lets you control which user account is used to run the monitoring service (this is the same setting you can set on each service in the Administrative Tools -> Services applet). This account is the account that the monitoring service will use when monitoring all resources.

CPU Throttling - The monitoring service has advanced CPU throttling built in which works to keep the average CPU usage at or around the value you set. Note that during report creation, the CPU usage will sometimes go above the throttle level, but it won't stay there for long.

Update Check - The monitoring service can periodically check if a newer version of the software is available and notify you via an alert email Action. We take privacy seriously: Please see the privacy considerations built in to the update check.

Log Files - The monitoring service writes diagnostic log files as it runs. You can control the maximum size for the log file. When the maximum is reached, a portion of the beginning of the log file is removed and then new information continues to get written to the end of the file. Debug logging writes a very large volume of data to the log in a short time--it shouldn't normally be enabled unless needed by Power Admin Support to diagnose an issue.

Contents

Database Settings

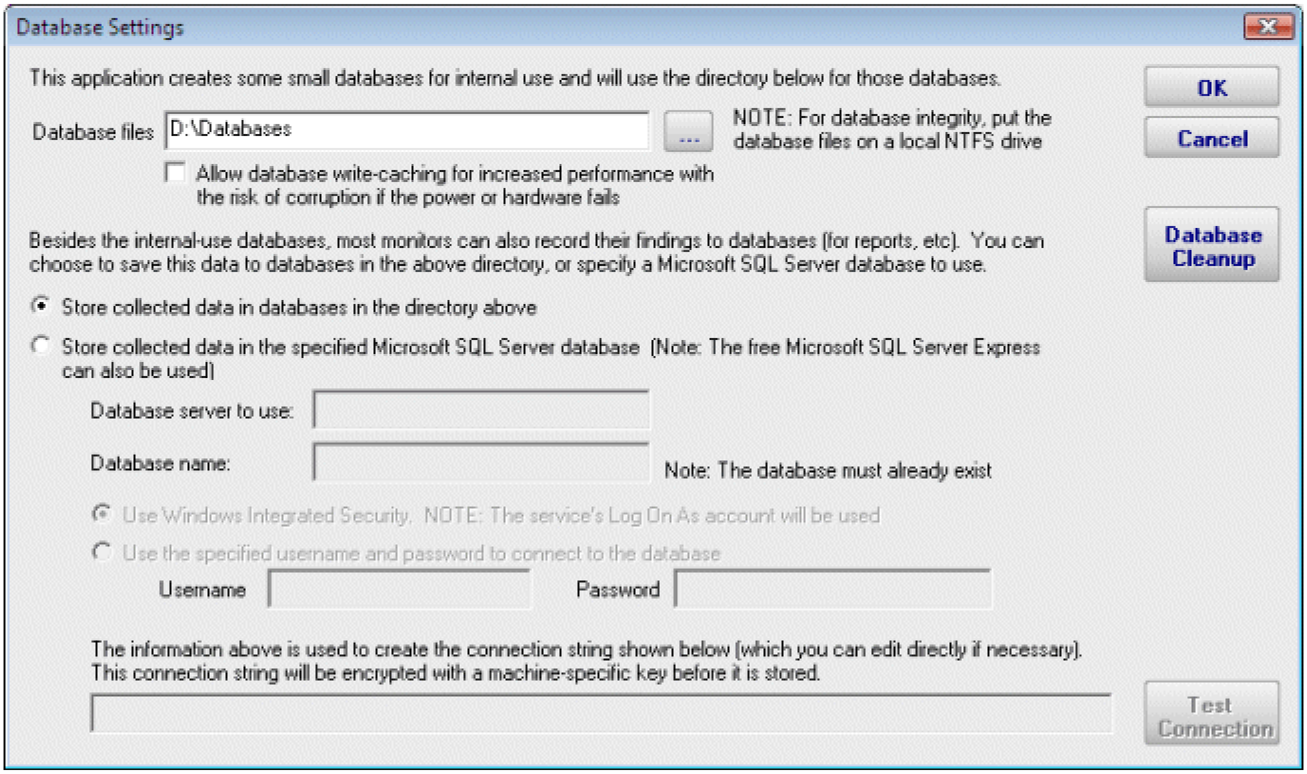
PA File Sight needs a place to store the data that it collects during operation. There are two choices available for data storage.

- **SQLite**
  By default, PA File Sight stores all of its data in compact, highly reliable SQLite databases. This is the choice that you make by selecting the radio button titled "Store collected data in databases in the directory above." This is the simplest choice available and is the one that most users make when using PA File Sight.
- **Microsoft SQL Server**
  The alternative choice is made with the other radio button whose label indicates Microsoft SQL Server. The SQL Server Express databases are fine for most installations, but do be aware that they limit the total database size to 4GB.

If you change the database settings, you will be prompted whether you want to copy your existing data from the current database to the new database. Depending on the size of your current databases, this can take a while (a large installation with 6GB of databases takes over a day for the transfer).

Database Cleanup

No maintenance is required for the databases. All monitors automatically remove old data from the databases automatically to help control database growth. You can control how many days of data is kept for the monitors via the Database Cleanup button.



This application creates some small databases for internal use and will use the directory below for those databases.

Database files: D:\Databases

NOTE: For database integrity, put the database files on a local NTFS drive

□ Allow database write-caching for increased performance with the risk of corruption if the power or hardware fails

Besides the internal-use databases, most monitors can also record their findings to databases (for reports, etc). You can choose to save this data to databases in the above directory, or specify a Microsoft SQL Server database to use.

● Store collected data in databases in the directory above

○ Store collected data in the specified Microsoft SQL Server database (Note: The free Microsoft SQL Server Express can also be used)

Database server to use:

Database name: Note: The database must already exist

● Use Windows Integrated Security. NOTE: The service's Log On As account will be used

○ Use the specified username and password to connect to the database

Username Password

The information above is used to create the connection string shown below (which you can edit directly if necessary). This connection string will be encrypted with a machine-specific key before it is stored.

More about Microsoft SQL Server and PA File Sight

To use SQL Server for storage, you need to install the SQL Server Native Client library, which is Microsoft's latest database connection technology.

If you did not install the Native Client Library at installation time, you can now by launching the installation file named `sqlncli.msi`, which will be located in the home directory of PA File Sight (normally `C:\Program Files\PA File Sight`.)

The following configuration data needs to be specified to use SQL Server:

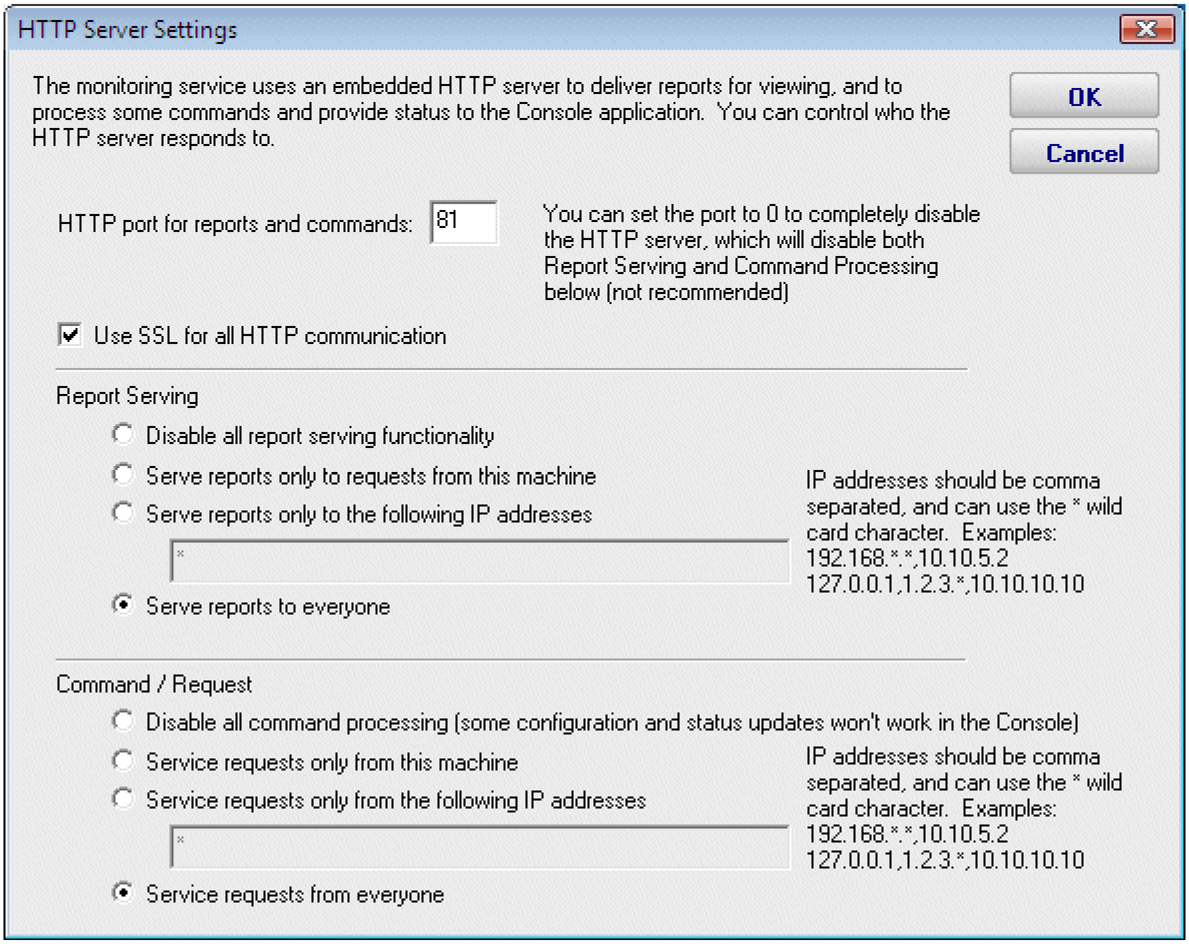
- Server name - name of server on which SQL Server instance is located. (Note that with SQL Express, this is often {server_name}\SQLEXPRESS)
- Database name - the name of a SQL Server database which will be used for PA File Sight storage. The database must exist prior to use.
- User name and password - as required by the SQL Server instance.
- Connection String - the connection string is automatically created by PA File Sight when you enter the configuration information above. You can hand edit the created connection string if you wish.

If you do not need or wish to use SQL Server as the database for PA File Sight, the SQL Server Native Client Library does not need to be installed.

Contents

HTTP (Web Server) Configuration

The PA File Sight service contains an embedded web server for serving HTML reports to the Console and to browsers, as well has handling some configuration requests from the Console. This embedded web server does NOT use or require IIS, and it can run on the same server as IIS or other web servers since it uses a different port than IIS generally uses.



HTTP Server Settings

The monitoring service uses an embedded HTTP server to deliver reports for viewing, and to process some commands and provide status to the Console application. You can control who the HTTP server responds to.

HTTP port for reports and commands: 81

You can set the port to 0 to completely disable the HTTP server, which will disable both Report Serving and Command Processing below (not recommended)

☑ Use SSL for all HTTP communication

Report Serving

○ Disable all report serving functionality
○ Serve reports only to requests from this machine
○ Serve reports only to the following IP addresses
*
● Serve reports to everyone

IP addresses should be comma separated, and can use the * wild card character. Examples:
192.168.*.*,10.10.5.2
127.0.0.1,1.2.3.*,10.10.10.10

Command / Request

○ Disable all command processing (some configuration and status updates won't work in the Console)
○ Service requests only from this machine
○ Service requests only from the following IP addresses
*
● Service requests from everyone

IP addresses should be comma separated, and can use the * wild card character. Examples:
192.168.*.*,10.10.5.2
127.0.0.1,1.2.3.*,10.10.10.10

The options available for controlling the built in web server are as follows.

- **HTTP Port for Reports and Commands**
  This setting lets you set the port which the embedded web server uses to listen for requests. Port 80 is generally used by IIS and Apache as the standard HTTP port for a web server. PA File Sight chooses a different port so it doesn't conflict. If you have another application that is already using this different port, you can easily change the port to another number.
- **Use SSL**
  PA File Sight supports using HTTPS for all communication to the service, which includes viewing reports, and Console-to-service communication. Self-signed digital certificates are used. This means most browsers will display a warning even though the HTTPS network traffic is encrypted. To fix the warning in the browser, follow the instructions on SSL Certificate Hints.

- **Report Serving**
  You can determine how PA File Sight serves reports. There are four options. You can disable all report serving. You can enable serving of reports but only to the same machine on which PA File Sight is installed. You can serve reports only to a set of other users, identified by the IP addresses of their computers. Or, you can serve reports to any other computer that requests reports. The default setting is "Serve reports to everyone".
- **Command Processing**
  This setting determines whether PA File Sight responds to commands that are issued by the Console part of PA File Sight. You may disable command processing entirely. Or, you may enable command processing, but only from the machine on which PA File Sight is installed. The default setting is "Process commands only from this machine."

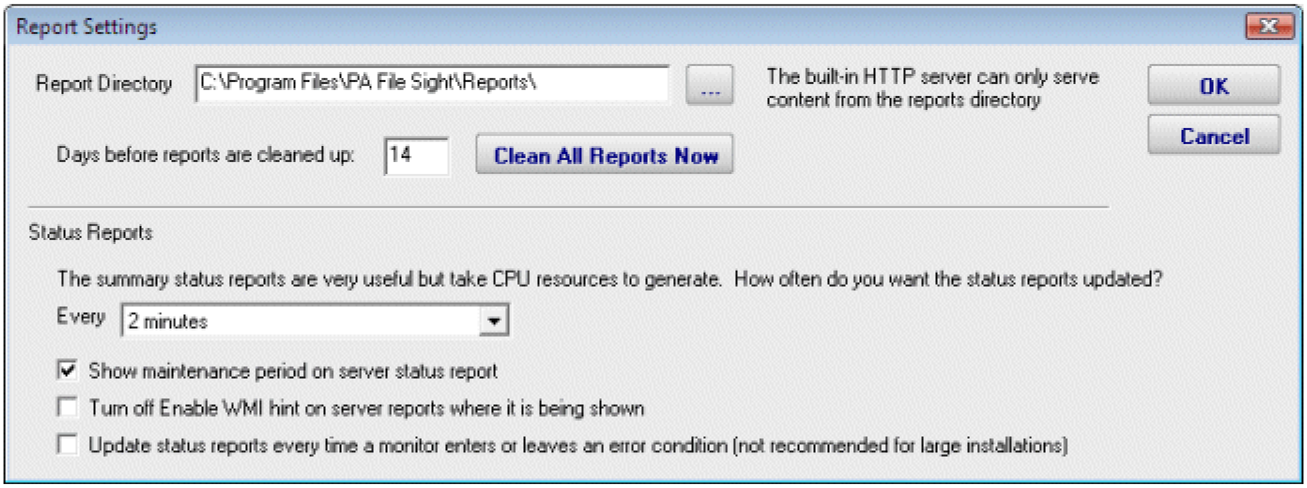
  Currently, the only case where commands are sent from a remote machine is if a user is viewing the Visual Status Map report in a browser on a separate machine.

Report Settings

The Report Settings dialog allows you to customize aspects of the way PA File Sight performs reporting.

The available settings and controls in this dialog are:

- Report Directory - This directory is where the HTML report files are created and stored by PA File Sight.
- Days before Reports are Cleaned Up - This value is the number of days reports (HTML files) will be available. After the given number of days, PA File Sight will delete the report. Note that reports that are always being updated (system summary reports and Scheduled Reports) will not be aged out.
- Clean All Reports Now - Pressing this button will purge all reports. Reports that are constantly refreshed (like the status reports for example) will be re-created on their normal reporting cycle.
- Status Reports Interval - This drop down list allows you to select the interval at which report files are generated.
- Show Maintenance Period on server status report - Self explanatory.
- Turn off "Enable WMI Hint" on Server Reports Where it is Being Shown - If PA File Sight is configured to poll a server via WMI for richer status reports, but that WMI polling fails, an error/hint message is shown at the top of the report. This check box disables this warning.
- Update Status Reports every time a Monitor enters or leaves an error condition - This option gives very small installations the ability to always have up to date reports.



Report Settings

Report Directory: C:\Program Files\PA File Sight\Reports\

The built-in HTTP server can only serve content from the reports directory

Days before reports are cleaned up: 14

Status Reports

The summary status reports are very useful but take CPU resources to generate. How often do you want the status reports updated?

Every 2 minutes

☑ Show maintenance period on server status report

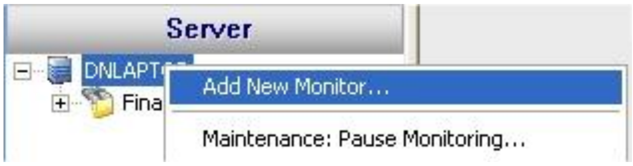
☐ Turn off Enable WMI hint on server reports where it is being shown

☐ Update status reports every time a monitor enters or leaves an error condition (not recommended for large installations)

Contents

Adding Monitors

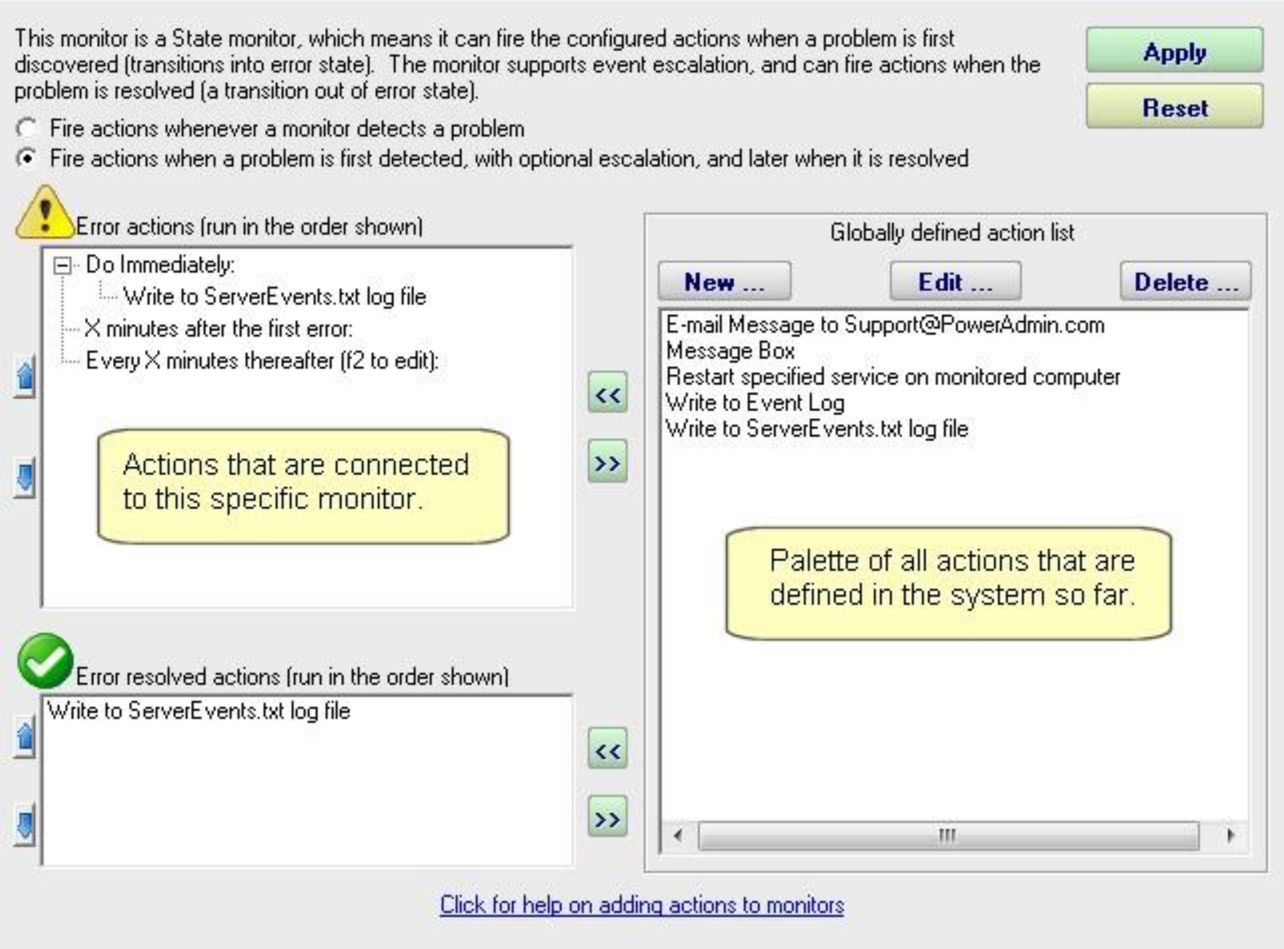
Adding monitors to an existing computer is very easy. Select the computer in the navigation pane and right click. Select the "Add New Monitor..." menu item.



A new instance of the monitor will be shown to the right of the navigation pane where you can configure that monitor to your particular environment.

Adding Actions

The Actions dialog is pictured below. (Depending on the features of the monitor being configured, the dialog may look slightly different than the one pictured below).



This monitor is a State monitor, which means it can fire the configured actions when a problem is first discovered (transitions into error state). The monitor supports event escalation, and can fire actions when the problem is resolved (a transition out of error state).

○ Fire actions whenever a monitor detects a problem
● Fire actions when a problem is first detected, with optional escalation, and later when it is resolved

Error actions (run in the order shown)

- Do Immediately:
  - Write to ServerEvents.txt log file
- X minutes after the first error:
- Every X minutes thereafter (f2 to edit):

Actions that are connected to this specific monitor.

E-mail Message to Support@PowerAdmin.com
Message Box
Restart specified service on monitored computer
Write to Event Log
Write to ServerEvents.txt log file

Palette of all actions that are defined in the system so far.

Error resolved actions (run in the order shown)

Write to ServerEvents.txt log file

Click for help on adding actions to monitors

On the left are shown all of the actions that are attached to this specific monitor. When the monitor 'fires actions' it will run that list of actions in the order shown. You can change the order with the blue up and down arrow buttons.

On the right is a list of all actions that are defined so far. These actions could be used by any monitor.

If you need an action that isn't listed (for example another email action, or a Start Application action), click the "New ..." button above the list of global actions.

You can edit actions in this list, and changes made will be reflected in every monitor that is using that action.

To add (or attach) an action to a monitor, simply select the action in the global list on the right, and press the green << button to move the action to the left monitor-specific list, to the Do Immediately node. (Other nodes may be shown for monitors that support event escalation)

State vs Event Monitors

Some monitors see discrete events -- a file is accessed, an event is written to the Event Log, etc. Others see conditions -- disk space is low, ping response is too slow, etc.

The following describes how State and Event monitors differ.

- *State* monitors keep track of whether the monitor is in a healthy state or an error state. For *State* monitors, you can choose to have actions run when a problem is detected, and then not again until it is fixed. State Monitors also support *event escalation* and *error resolved actions*.
- *Event* monitors run actions every time they see something wrong. You can control what actions are run and when.

State monitors can be configured to act like Event monitors, meaning you can choose to be notified every time an error state is detected. This is what the radio buttons near the top do.

With these differences in mind, the dialog above shows the action configuration dialog for a *State* monitor. Only state monitors support event escalation.

Contents

Error Auditing

Service Level Agreements (SLAs) and regulatory compliance with GLBA, HIPPA, PCI and SOX among other standards often requires auditing errors that occur on servers and devices. In addition, many IT organizations choose to use error auditing to ensure a high quality of service to the rest of the business.

Even if you don't have compliance requirements, the Error Audit report can be a good way to get a quick summary of a certain type of error that is occurring. See Not Just For Auditing below if this is you.

Three Pieces

PA Server Monitor, PA Storage Monitor and PA File Sight all have Error Auditing built-in to the product. Auditing can be enabled or disabled, and used however it works best for your organization.

There are three parts to Error Auditing:

1. Product monitors run and detect issues. Alerts are optionally fired and details are written to the database. The error details, source device, time, etc are all recorded to an error database.
2. Server administrators view server status reports and note recent errors. They check the Ack box next to the error indicating that they have reviewed and acknowledged the error. Their acknowledgement is recorded in the database along with the error details.
3. Administrators, management or compliance officers can run high-level Error Audit reports to make sure errors are being reviewed and acknowledged by server administrators. The Error Audit reports can be broken down by:

   - source computer or device
   - computer group
   - resource type (disk space, services, ping response, etc)
   - acknowledgement state (acknowledged or not yet acknowledged)
   - error type

   Multiple reports can be created which gives each manager/compliance officer the view of the network that they are responsible for.

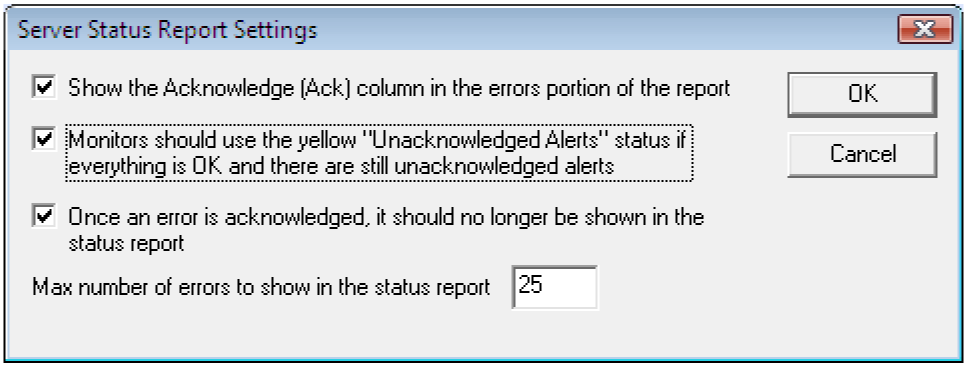
More Details

1. - Product monitors detect and record issues

The products have always monitored resources, fired alerts when over thresholds and recorded resource values in the database for later reporting and charting. In addtion, the different monitors would change color based on whether everything was OK (green) or alerts were fired (yellow). Red (internal or serious error) and grey (disabled or maintenance) are also possible colors.

When a monitor turns yellow, the yellow color shows up on summary screens for the whole server indicating that there is an alert on a monitor on that server. The server will show green when all monitors are green.

Some problems are transitory (a new event in the Event Log, a change to a file, etc). Alerts would be fired, but the monitor wouldn't stay yellow since on the next run everything looked OK, so the it would go back to green (OK). If the administrator was not watching the server closely, that yellow alert status could come and go without being seen. A new option that can be set on a per-server level is to force monitors to remain yellow while they have unacknowledged alerts. This is available by right-clicking the server and going to Report & Delivery Settings -> Report Settings.



Server Status Report Settings

☑ Show the Acknowledge (Ack) column in the errors portion of the report

☑ Monitors should use the yellow "Unacknowledged Alerts" status if everything is OK and there are still unacknowledged alerts

☑ Once an error is acknowledged, it should no longer be shown in the status report

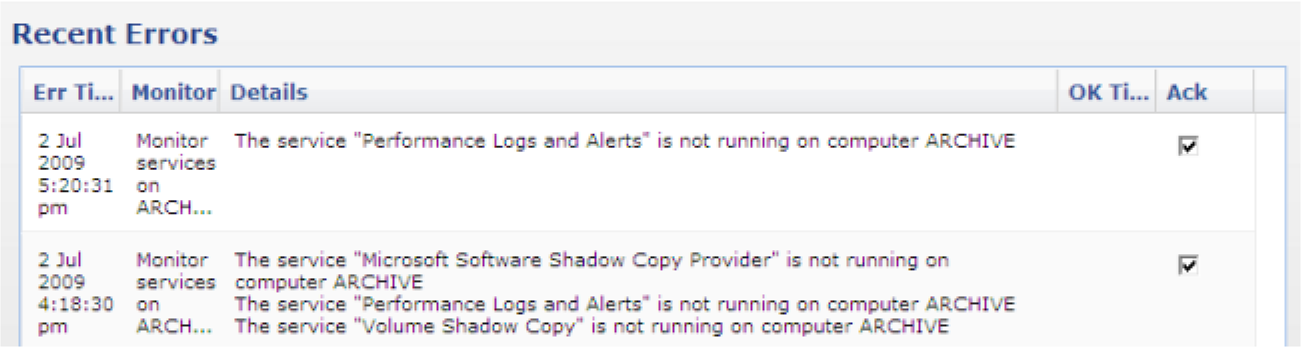
Max number of errors to show in the status report: 25

Additional options in this dialog control what is displayed in the Recent Errors section at the bottom of the server status report

2. - Server administrators acknowledge errors

The next piece of the auditing system is the server administrators. At the bottom of the server status report is the Recent Errors section. This shows issues that the monitors have recently discovered. What is shown there depends on the Report Settings dialog discussed above. Most often, there will be an Ack column.

When the Ack column is clicked, an request is sent to the service indicating that the error has been acknowledged. The acknowledgement time as well as the IP address of the user is recorded. [A future version will user logins to view reports -- at that time the username will be recorded instead of the IP address]. If an administrator accidentally acknowledges an error, they can click the Ack box again to clear the acknowledgement.



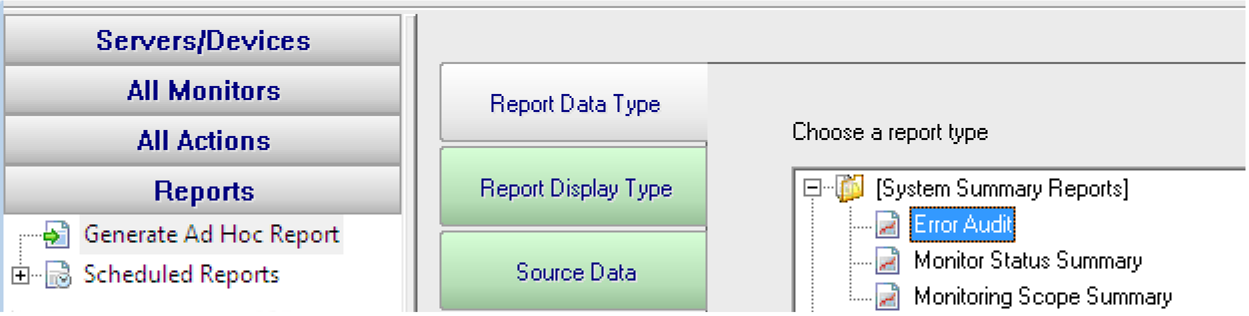
Recent Errors

Err Ti...	Monitor	Details	OK Ti...	Ack
2 Jul 2009 5:20:31 pm	Monitor services on ARCH...	The service "Performance Logs and Alerts" is not running on computer ARCHIVE		☑
2 Jul 2009 4:18:30 pm	Monitor services on ARCH...	The service "Microsoft Software Shadow Copy Provider" is not running on computer ARCHIVE The service "Performance Logs and Alerts" is not running on computer ARCHIVE The service "Volume Shadow Copy" is not running on computer ARCHIVE		☑

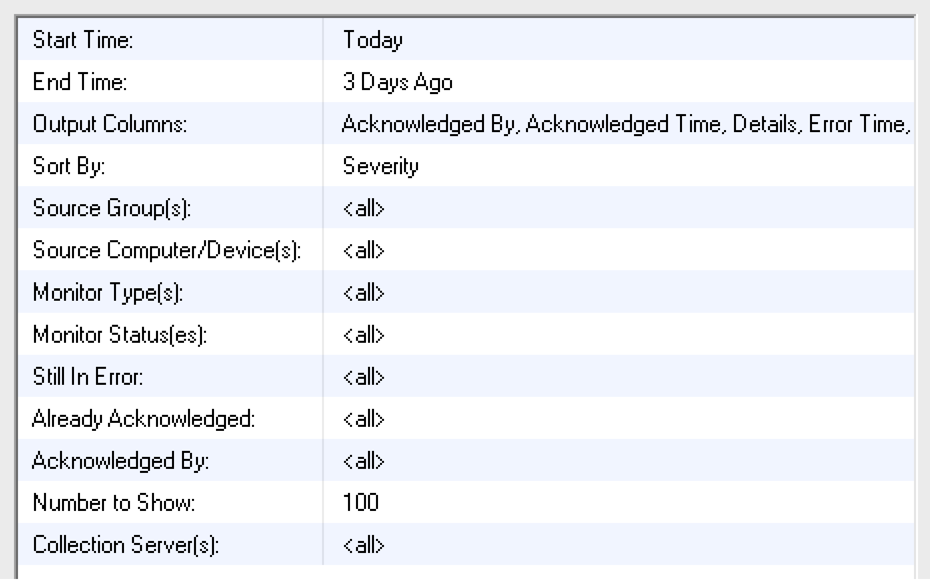
Administrators will often not want to see the error again once they've acknowledged it. This can be controlled via the Report Settings dialog mentioned above.

3. - Error auditing reports for compliance

The Error Audit report is available under the [System Summary Reports] section.



Once you've selected the report, go to the Filters and Parameters tab. This is where you specify exactly what you want to look at. There are a variety of different ways to filter the errors that you want to see. If your primary responsibility is disk space, just look at the Disk Space monitors under Monitor Type(s). If you have grouped the servers by geographic region, you could specify you only want to see errors in the Northern Europe Source Group for example.



Start Time:	Today
End Time:	3 Days Ago
Output Columns:	Acknowledged By, Acknowledged Time, Details, Error Time,
Sort By:	Severity
Source Group(s):	<all>
Source Computer/Device(s):	<all>
Monitor Type(s):	<all>
Monitor Status(es):	<all>
Still In Error:	<all>
Already Acknowledged:	<all>
Acknowledged By:	<all>
Number to Show:	100
Collection Server(s):	<all>

There is a lot of data available and it might seem a little overwhelming at first. We recommend using the Output Columns filter and only show the data that you're interested in. You can see when a problem happened, when it was fixed, when it was acknowledged, what computer/devices it was on, etc.

Once you user the report a few times and have decided what you want to watch, we recommend creating a Scheduled Report. That way the report that you want will always be available (Scheduled Reports always use the same URL, so you can save it in your favorites and quickly see the latest report.

Not Just For Auditing

Large organizations often have multiple people that are responsible for different parts of the IT infrastructure. Creating Error Audit reports is a good way to view all errors that are happening to a group of servers, or to a class of resources (ie errors related to Ping response for example).

We recommended that each person with a large responsibility have their own Error Audit report so they can quickly see all errors within their area of responsibility. Errors can even be acknowledged on the Error Audit report itself, just like on the server status reports.

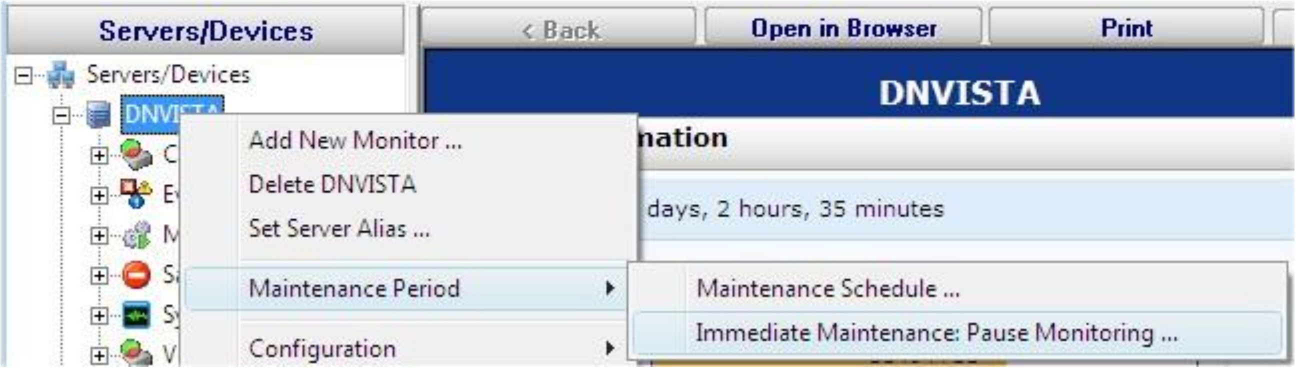
Contents

Maintenance Mode

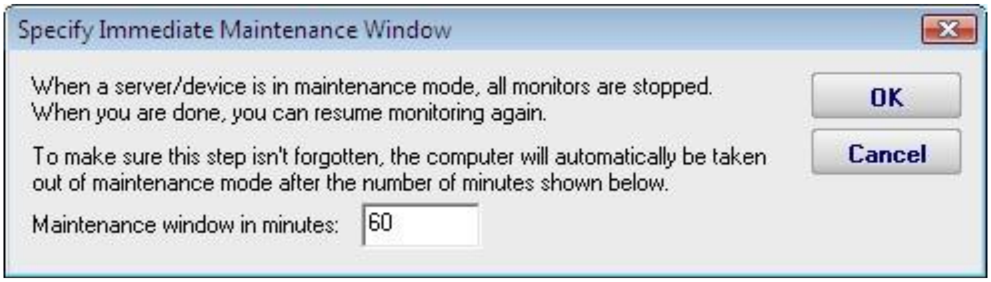
Maintenance Mode is very useful when you'll be working on a computer that is being monitored. Naturally you don't want to receive alerts or have the monitoring service try to correct things that you are working on. Instead of stopping the monitoring service (and potentially forgetting to start it again), you can indicated the monitored computer is being worked on with Maintenance Mode.

Manual Maintenance

You manually put a server into maintenance mode immediately by right clicking on the computer and choosing Maintenance Period -> Immediate Maintenance: Pause Monitoring.



When you enter Maintenance Mode, you specify how long you expect to be working on the server. No further monitoring of the server will take place until that amount of time has past. Then active monitoring of the server begins again automatically.



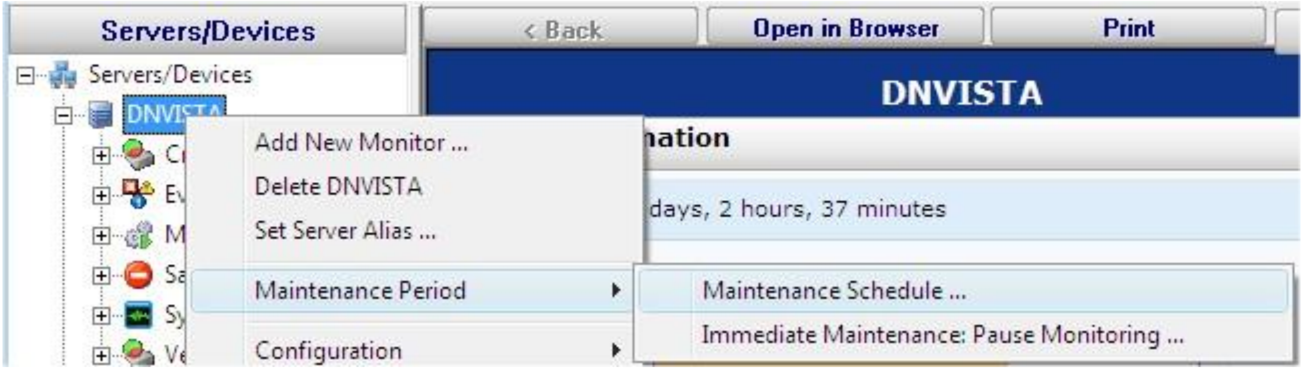
Specify Immediate Maintenance Window

When a server/device is in maintenance mode, all monitors are stopped. When you are done, you can resume monitoring again.

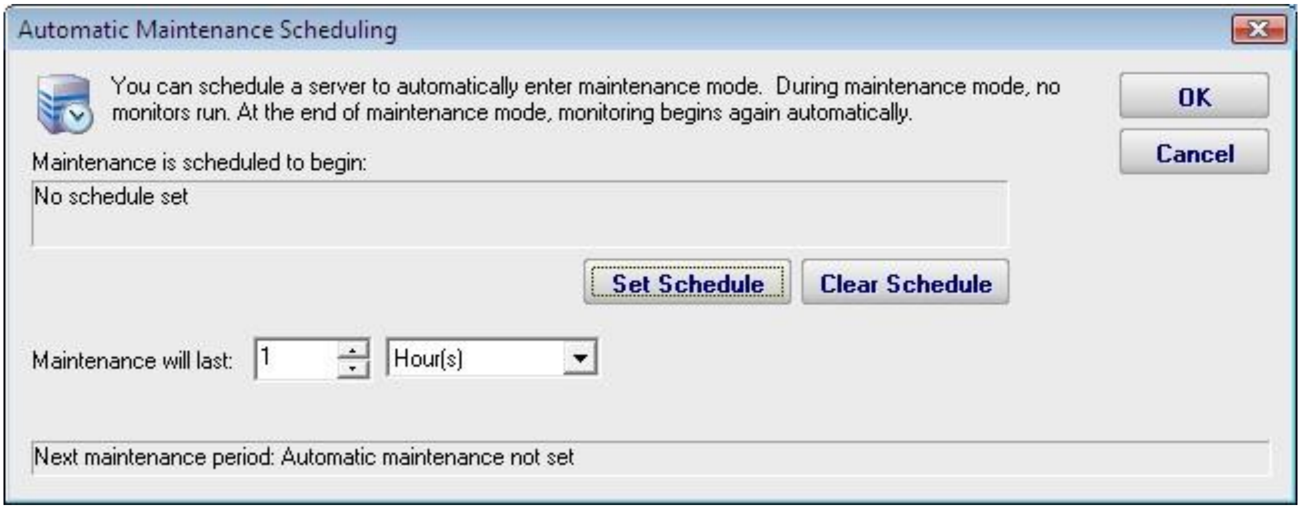
To make sure this step isn't forgotten, the computer will automatically be taken out of maintenance mode after the number of minutes shown below.

Maintenance window in minutes: 60

Scheduled Maintenance



In addition to the manual maintenance mode mentioned above, scheduled maintenance is also available. With this feature you can have the monitoring service automatically place a server into maintenance mode based on your schedule. This is often useful when some normal process (a nightly backup process for example) might exceed some of the monitors' normal thresholds.



You can schedule a server to automatically enter maintenance mode. During maintenance mode, no monitors run. At the end of maintenance mode, monitoring begins again automatically.

Maintenance is scheduled to begin: No schedule set

Maintenance will last: 1 Hour(s)

Next maintenance period: Automatic maintenance not set

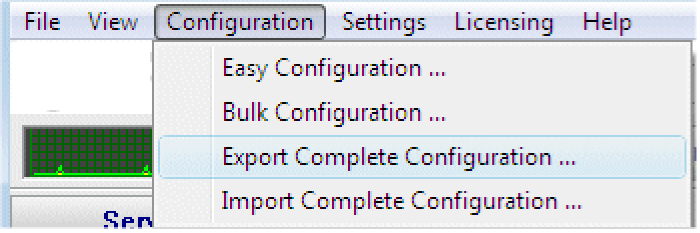
Importing and Exporting Configurations

PA File Sight supports a very easy and effective way to transfer your complex monitoring setups from one installation of the product to another. This is what exporting and importing configurations allows you to do.

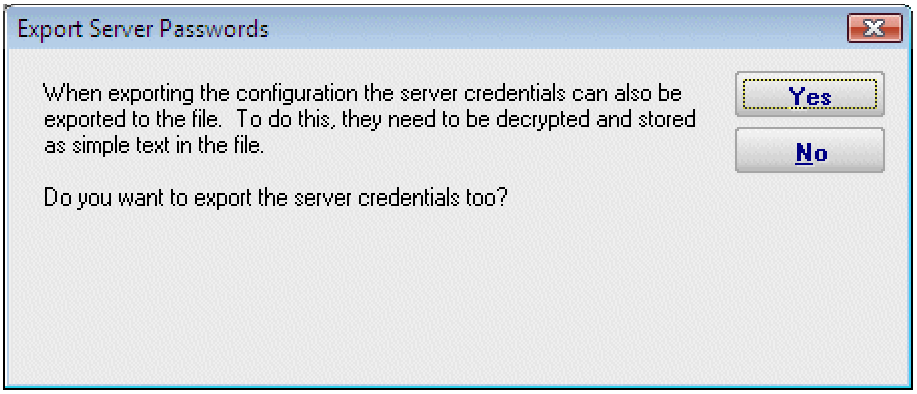
Exporting is a process by which you make PA File Sight save configuration data to a special XML format file. Importing is the process that allows PA File Sight to read in saved values from the same type of file and to restore the settings.

Exporting Complete Configuration

Exporting the complete configuration is an easy way to preserve all of the settings that are contained in an instance of PA File Sight. To get started, select the following menu setting:



The next dialog that you will see will ask you if you would like to export any server passwords that were entered previously:



When exporting the configuration the server credentials can also be exported to the file. To do this, they need to be decrypted and stored as simple text in the file.

Do you want to export the server credentials too?

If you work in an environment in which password and credential data must be handled in a specific manner due to legal or internal company restrictions, you may wish to answer "No" to this prompt. Otherwise, you may wish to allow PA File Sight to save all security credentials to the file by answering "Yes". The credentials will be decrypted and will be visible as plain text in the output file.

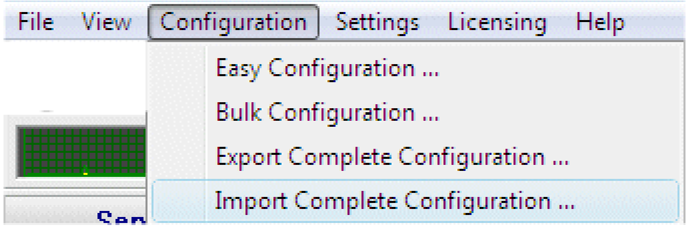
The next dialog to appear after you answer the question above will be a standard "File Save" Windows dialog that allows you to select a file name, and a location at which to save the configuration file. When you export a Complete Configuration, the default file name that is selected will be `PA File Sight App Configuration.axml`. The file extension `.axml` should always be used when you save the complete configuration because it indicates this type of exported configuration.

At the completion of the export of the configuration data, PA File Sight will display a message box but only if you chose to save the credential information.

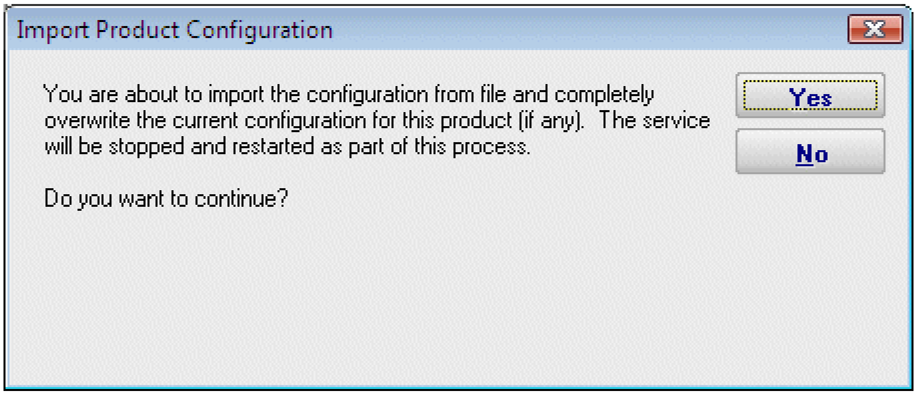
Importing Complete Configuration

Just as easily as you can export a PA File Sight configuration to a file, you can also import that file into a new installation of PA File Sight on another machine.

You use the following menu selection to choose Import Complete Configuration.



The first prompt that you will see will be a message box indicating that you are about to erase any configured settings in the current instance of PA File Sight and replace them with the contents of a configuration archive file.


Import Product Configuration

You are about to import the configuration from file and completely overwrite the current configuration for this product (if any). The service will be stopped and restarted as part of this process.

Do you want to continue?

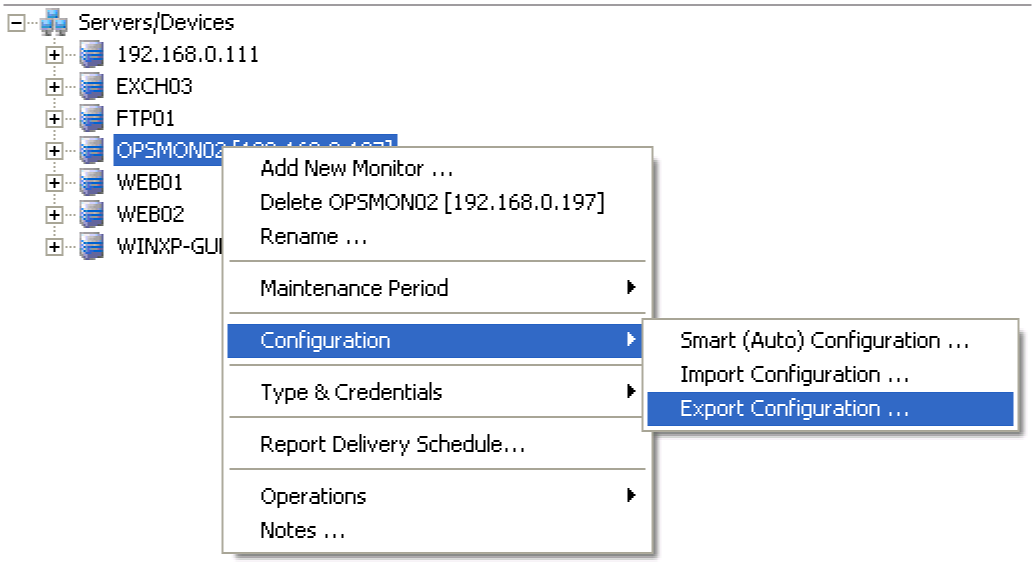
If you answered "Yes" to the question above you will see the standard File Open dialog to select a .axml file that you saved to previously.

Note that this dialog box indicates a file of the extension `.axml`, as saved by the Export procedure. At the end of the import, you should see the list of servers restored to the Navigation Pane. A message box will appear at the end of the import process indicating the success of the operation, as well as any monitors or actions that could not be restored.

Exporting Individual Server Configuration

You may export the settings (monitors and actions) that are associated with an individual computer. This operation is very similar to that of exporting the complete configuration of this product as shown above.

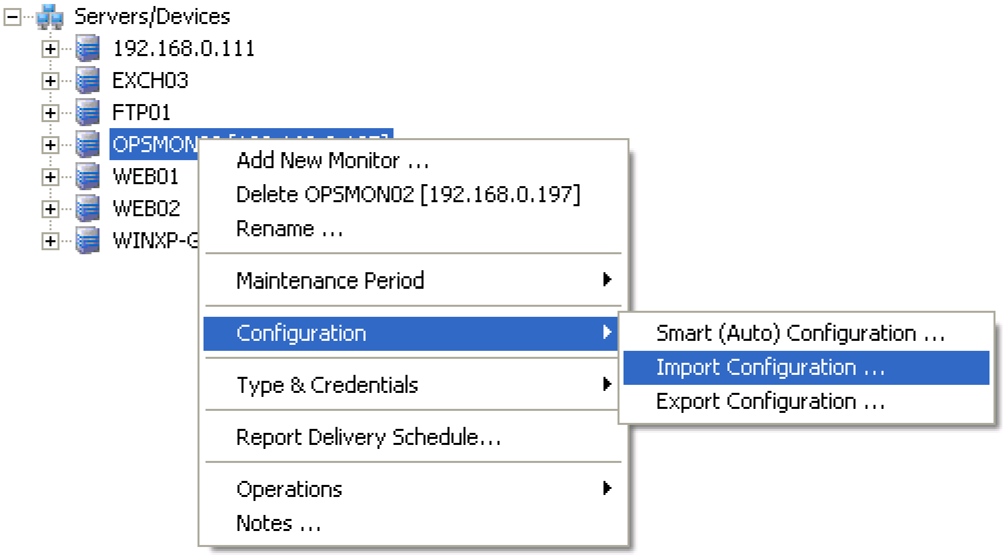
The menu item that selects the export server operation is accessed by right clicking a server or device whose configuration you wish to export. The menu appears as follows.



The series of dialog boxes and the options that appear is identical to that shown above for exporting a complete PA File Sight configuration, with the following exception. The file name will be `(Server_name) Configuration.cxml`. (Server_Name) represents the name of the server you are exporting.
Example for the illustration above: `192.168.0.197 Configuration.cxml`

Importing Individual Server Configuration

You may import the settings (monitors and actions) that are associated with an individual computer. The Import Server operation assumes that they exist already in a `.cxml` file.



This operation is identical to that of importing the complete configuration of this product as shown above, with the following exception. An import of a server configuration must be applied to a computer object that you have already created in PA File Sight. The IP address or name must be set by you explicitly, and will not be transferred from the previously exported computer. The monitors and the actions that are created will be associated with the IP or computer network name that the target computer had contained.

Contents

External API

PA File Sight has a simple API for basic operations.

Security

To protect the system from un-authorized requests, there are two security precautions that are required:

- **SSL** - SSL must be enabled for the embedded HTTP server. This can be done on the HTTP Settings dialog.
- **API Key** - The API Key registry setting must be set. This is analogous to a username/password. Create a value named API_KEY and set it to a long string value of random characters. The value goes under a product-specific key:

  PA File Sight - HKEY_LOCAL_MACHINE/software/PAFileSight
  PA Server Monitor - HKEY_LOCAL_MACHINE/software/PowerAdminServerMonitor
  PA Storage Monitor - HKEY_LOCAL_MACHINE/software/PAStorageMonitor

Requests are made via HTTPS. The format of the requests is:

```
HTTPS://{server}:{port}?API={command}&KEY={API Key}
```

Additional optional parameters can be appended to the URL using the pattern:

```
&{param_name}={value}
```

Return Values

All API commands return data as simple text. All successful commands return data as:

```
:START:
{returned data
can be multiple lines}
:END:
```

Errors are returned as:

```
:ERROR:{error text}
```

API Commands

Below are the supported commands. The command name should be insert where {command} is shown in the example above.

GET_SERVER_LIST	Returns a list of servers and the group that the server is in. Parameters: none Example: `https://server:81?API=GET_SERVER_LIST&KEY=921msa8gbk4j78dbglaj` Output (server|group{tab}group where {tab} is the ASCII tab

	(\t) character:
	`:START:`
	`DNVISTA|Servers/Devices`
	`192.168.2.5|Servers/Devices`
	`POWERADMIN.COM|Servers/Devices{tab}Boston`
	`NEBPUTER|Servers/Devices{tab}Servers{tab}Office`
	`DOMAIN|Servers/Devices`
	`MANY|Servers/Devices`
	`DNLAPTOP|Servers/Devices`
	`OPSMON02|Servers/Devices{tab}Servers{tab}Office`
	`ARCHIVE|Servers/Devices`
	`192.168.1.1|Servers/Devices`
	`192.168.2.111|Servers/Devices{tab}Linux`
	`192.168.2.113|Servers/Devices`
	`192.168.2.104|Servers/Devices{tab}Linux`
	`RFMAC|Servers/Devices Linux`
	`TEST|Servers/Devices`
	`:END:`

START_MAINTENANCE	Put the server into immediate maintenance mode.
	Parameters:
	SERVER - name of the server that should be put into maintenance mode
	MINUTES - time in minutes that the server should remain in maintenance mode before it automatically reverts to normal monitoring
	Example:
	`https://server:81?API=START_MAINTENANCE&KEY=921msa8gbk4j78dbglaj &SERVER=MAILSRV&MINUTES=15`
	Output:
	`:OK:`

END_MAINTENANCE	Put the server back into normal monitoring mode.
	Parameters:
	SERVER - name of the server that should be put into normal monitoring mode
	Example:
	`https://server:81?API=END_MAINTENANCE&KEY=921msa8gbk4j78dbglaj&SERVER=MAILSRV`
	Output:
	`:OK:`

ADD_SERVER	Add and optionally configure the named server Parameters: SERVER - name of the server that should be added WIN (optional) - defaults to 0. Set to 1 if this is a Windows server. WMI (optional) - defaults to 0. Set to 1 if WMI polling should happen to collect System Details information for the server status

	report
	CONFIG_PATH (optional) - defaults to none. Full path to a .cxml config file that specifies a configuration that should be applied to the new server. .cxml files are created by exporting a computer's configuration. The file must be on the same computer as PA File Sight is running on.
	Example:
	`https://server:81?API=ADD_SERVER&KEY=921msa8gbk4j78dbglaj&SERVER=MAILSRV2&WIN=1&WMI=1&CONFIG_PATH=C:\Configs\MailConfig.cxml`
	Output:
	`:OK:`

DELETE_SERVER	Delete the named server, along with all of its monitors
	Parameters:
	SERVER - name of the server that should be deleted
	Example:
	`https://server:81?API=DELETE_SERVER&KEY=921msa8gbk4j78dbglaj&SERVER=MAILSRV2`
	Output:
	`:OK:`

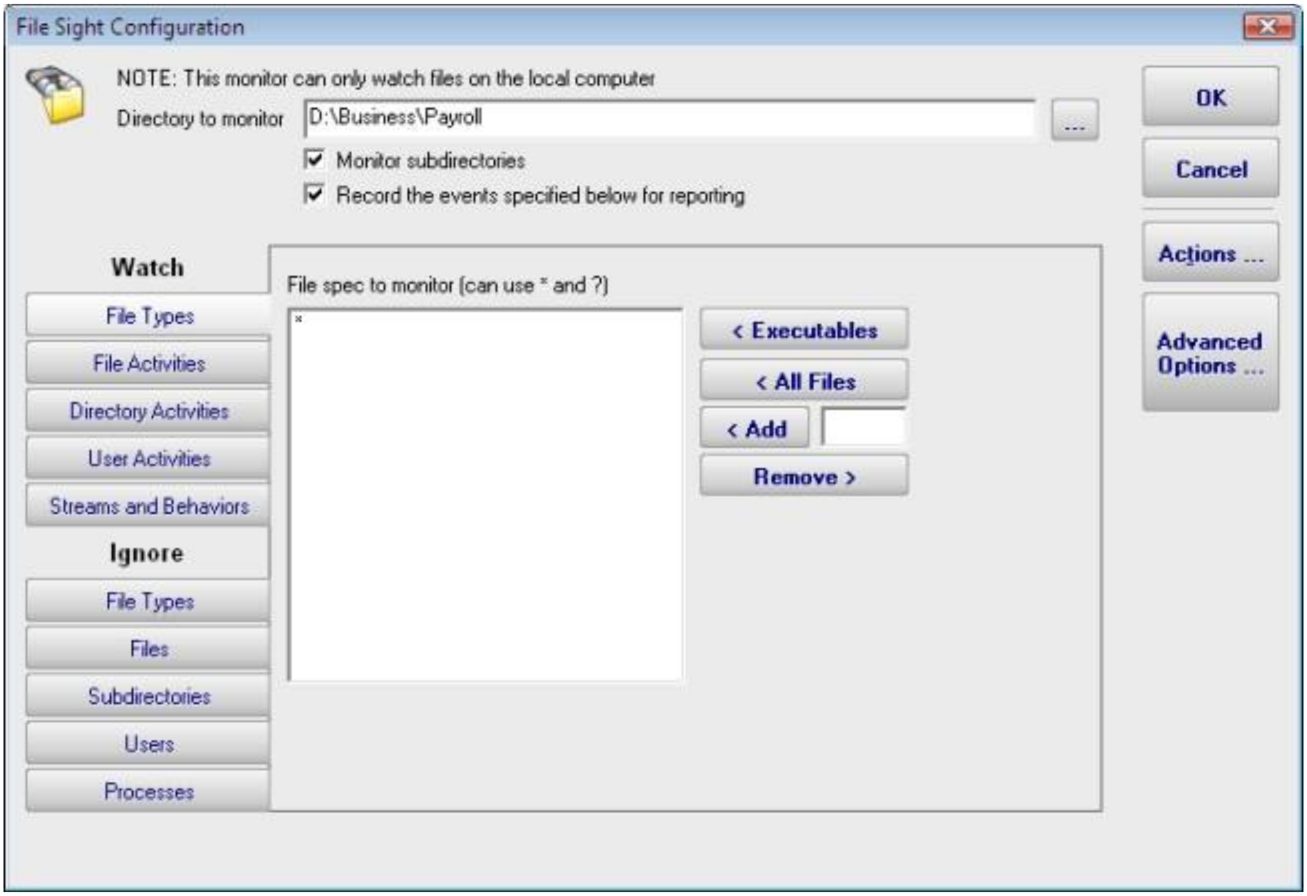
Monitors

Contents

File Sight - File Access Monitor

The File Sight monitor watches file and directory I/O take place and can record and alert you on many different conditions. When configuring the monitor, the first thing to decide is where to monitor. Generally there will be a directory that you're interested in. It is more efficient to monitor just that directory rather than an entire drive. You can create multiple File Sight monitors to watch various drives / directories in a computer.

In the dialog below you'll see there are many options. After specifying the root directory to monitor you can specify whether all subdirectories should also be monitored. You'll also need to decide whether you want to record the information to a database for reporting later. Recording to a database uses some extra resources, depending on how much information needs to be recorded (which you can control via settings that will be discussed below). Database recording is only available in the Pro product version -- it is not available in the Lite edition.



File Sight Configuration

NOTE: This monitor can only watch files on the local computer

Directory to monitor: D:\Business\Payroll

☑ Monitor subdirectories

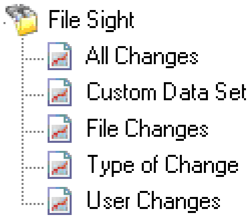
☑ Record the events specified below for reporting

File spec to monitor (can use * and ?): *

Standard Configuration Options

This monitor has standard buttons on the right for Adding Actions and setting Advanced Options.

Supported Reports

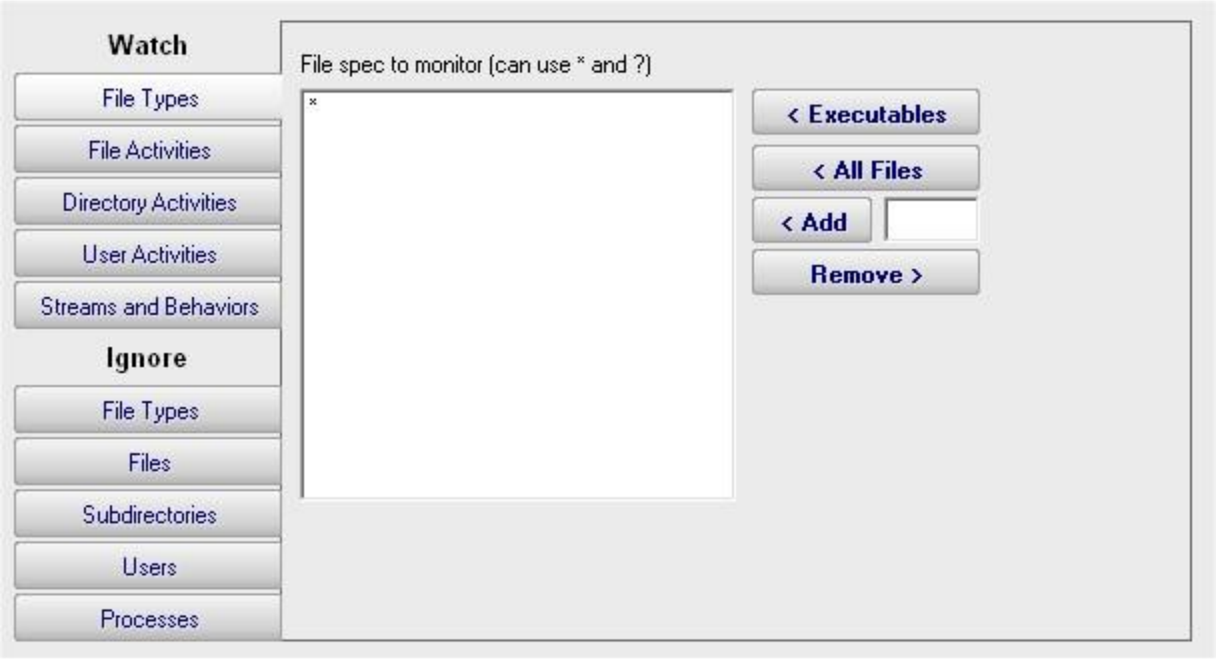


The **Pro** version of PA File Sight supports reports which can tell you about file and directory activities that have taken place in the past while PA File Sight was monitoring the server. You can report on changes to particular files or directories, changes made by a particular user, or types of changes (all deletes for example).

Configuration Tabs

Watch: File Types

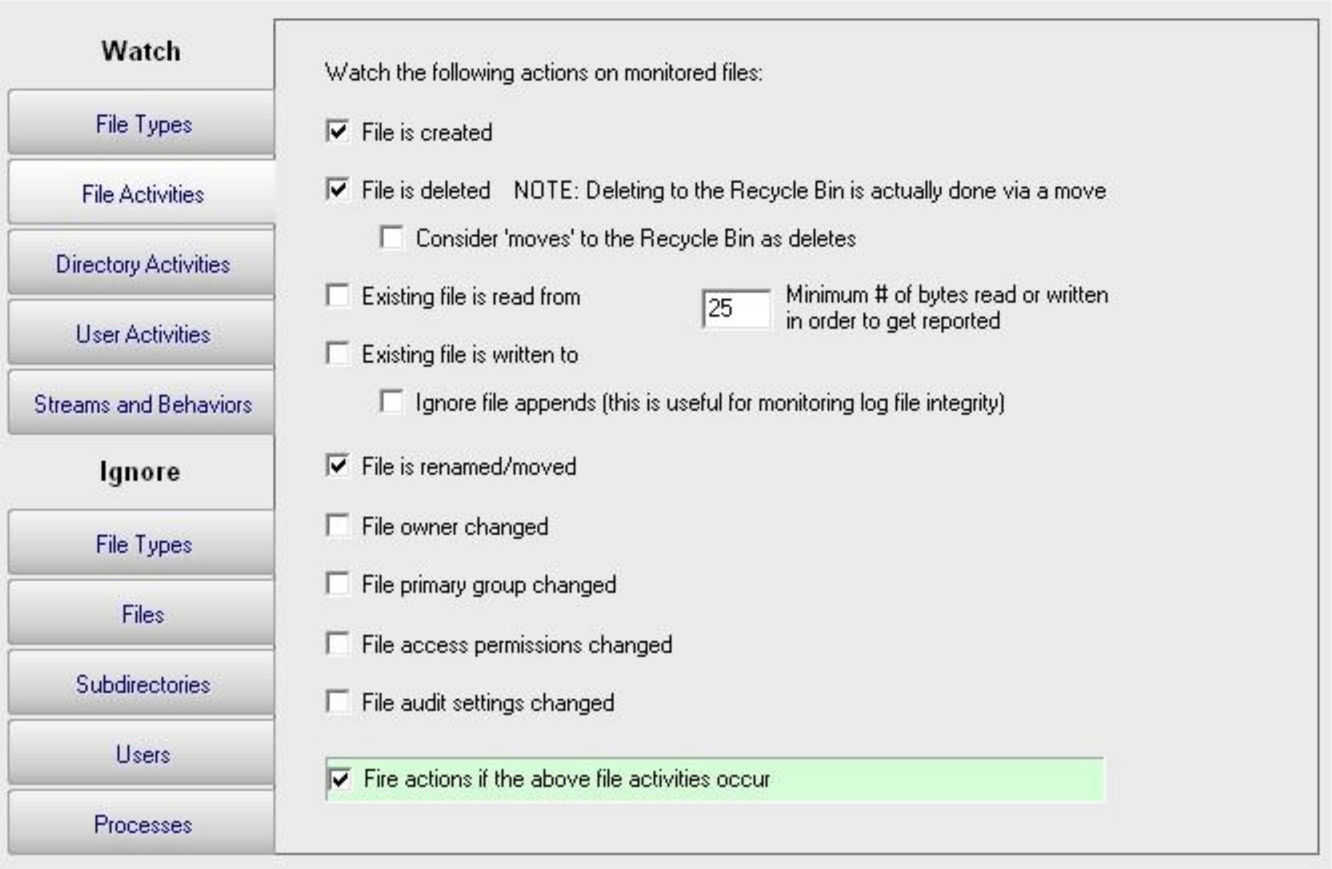
File Types tab lets you specify which files to consider. You can use typical * and ? wild card in specifying file types. Don't include paths here -- this is just for file types (for example *.doc would consider only file I/O that was on *.doc files).



Watch: File Activities

The File Activities tab is where you specify exactly what types of file I/O that you're interested in. File reads, writes, creates, deletes and moves can all be filtered on. For reads or writes you can further filter out very small reads which might happen if Explorer displays a directory.

The green box on the File Activities panel specifies whether actions should be fired when a matching file I/O activity happens. Sometimes this is unchecked because actions/alerts aren't needed, but the matching activities can still be written to the database.



Watch the following actions on monitored files:

☑ File is created

☑ File is deleted NOTE: Deleting to the Recycle Bin is actually done via a move

□ Consider 'moves' to the Recycle Bin as deletes

□ Existing file is read from

25 Minimum # of bytes read or written in order to get reported

□ Existing file is written to

□ Ignore file appends (this is useful for monitoring log file integrity)

☑ File is renamed/moved

□ File owner changed

□ File primary group changed

□ File access permissions changed

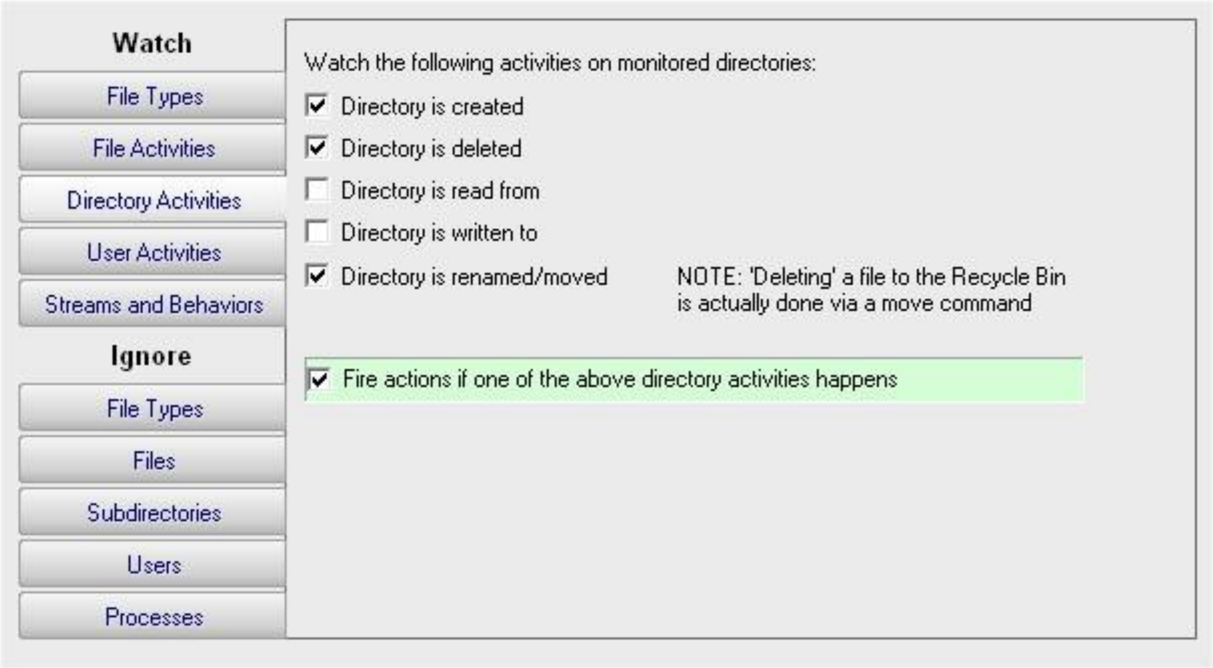
□ File audit settings changed

☑ Fire actions if the above file activities occur

NOTE: Only the Pro version of the product supports a database and reporting, so the "Fire actions if the above file activities occur" check box is almost always checked for a Lite installation that only does alerting.

Watch: Directory Activities

If you are interested in specifically directory actions, the Directory Activities tab is where you can specify them. This panel works just like the File Activities panel did, except it is focused on directories instead of files.



Watch the following activities on monitored directories:

☑ Directory is created

☑ Directory is deleted

☐ Directory is read from

☐ Directory is written to

☑ Directory is renamed/moved

NOTE: 'Deleting' a file to the Recycle Bin is actually done via a move command

☑ Fire actions if one of the above directory activities happens

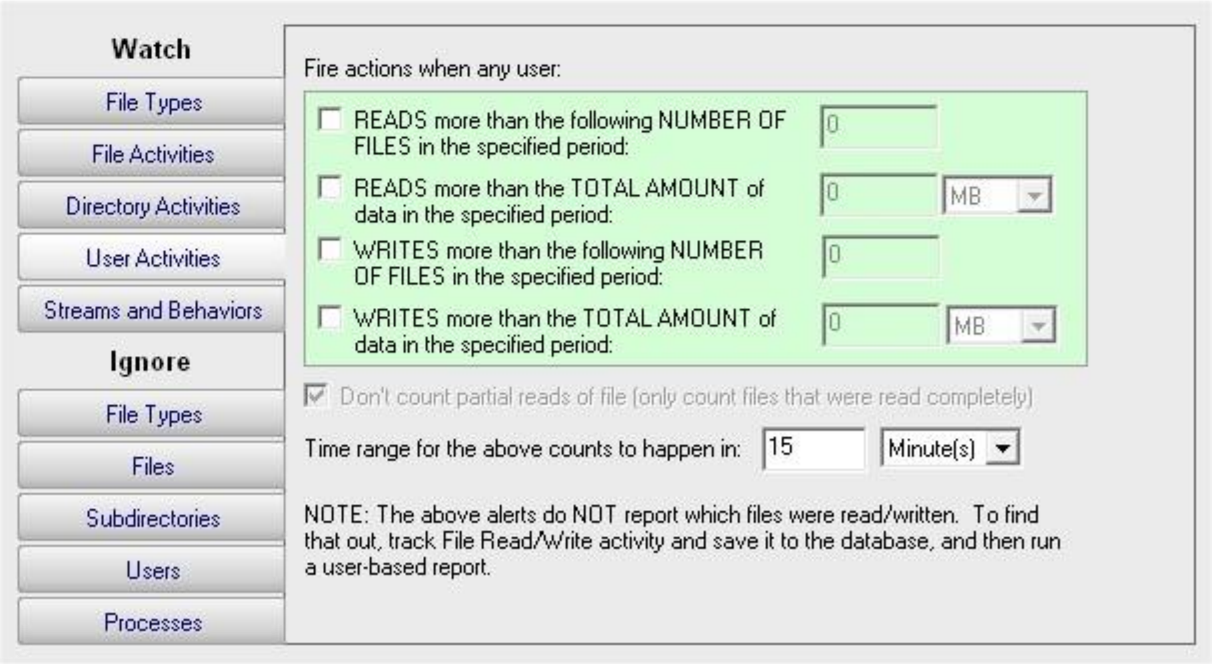
NOTE: Only the Pro version of the product supports a database and reporting, so the "Fire actions if one of the above directory activities happens" check box is almost always checked for a Lite installation that only does alerting.

Watch: User Activities

NOTE: This panel is only available in the Pro version of the product.

The User Activities panel is very powerful. It lets you specify alert conditions which are based on the number or amount of files that a user interacts with. These settings are all in a green box, which means they run actions (alerts) when the thresholds are met. These settings do not however cause anything to be written to the database. Be sure and set the corresponding settings in the File Activities panel if you'll want to run reports later and find out what was read or written to.

In addition, for file reads you can check the box indicating you only want to count complete file reads. Some administrators use this to try and detect a user copying a directory of files. At the file system level where this monitoring is taking place, it is impossible to detect where a file ends up once it is read (it could go straight to memory, to paper via a printer, out via an email, or copied to a different location on a disk). However, if many files are read completely in a very short time, that matches the heuristics of a file copy process.



Fire actions when any user:

- ☐ READS more than the following NUMBER OF FILES in the specified period: 0
- ☐ READS more than the TOTAL AMOUNT of data in the specified period: 0 MB
- ☐ WRITES more than the following NUMBER OF FILES in the specified period: 0
- ☐ WRITES more than the TOTAL AMOUNT of data in the specified period: 0 MB

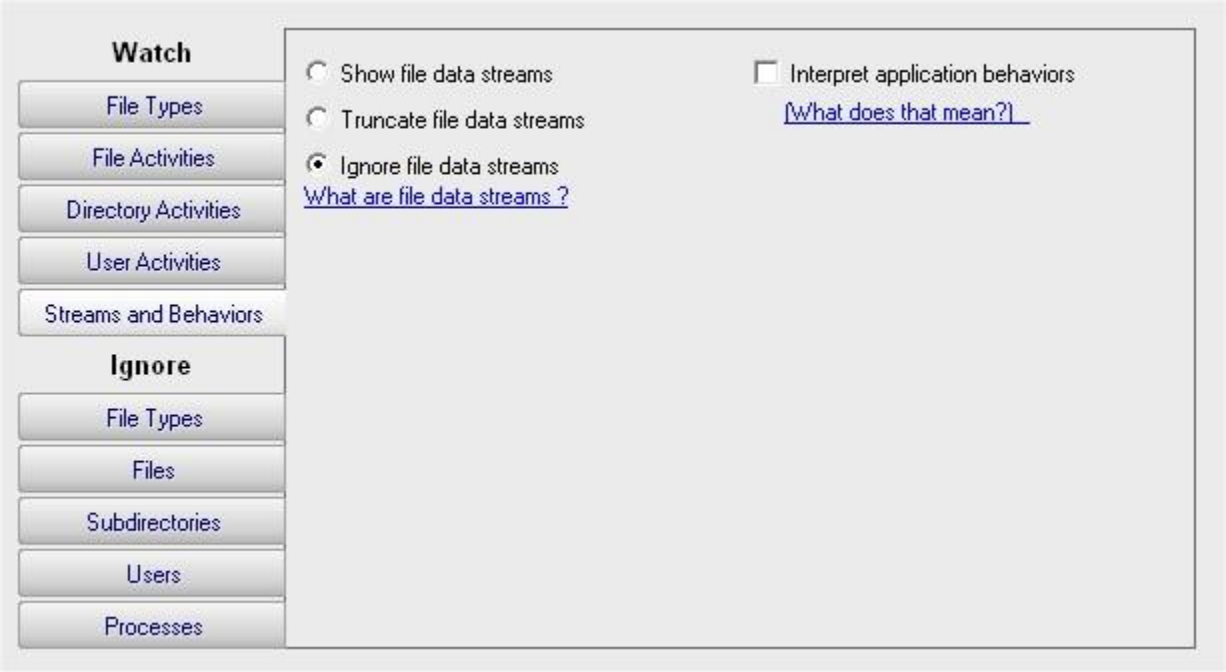
☑ Don't count partial reads of file (only count files that were read completely)

Time range for the above counts to happen in: 15 Minute(s)

NOTE: The above alerts do NOT report which files were read/written. To find that out, track File Read/Write activity and save it to the database, and then run a user-based report.

Watch: Streams and Behaviors

This panel lets you specify how to handle file streams that encountered, as well as whether File Sight should try and interpret typical application behaviors.



○ Show file data streams

○ Truncate file data streams

● Ignore file data streams

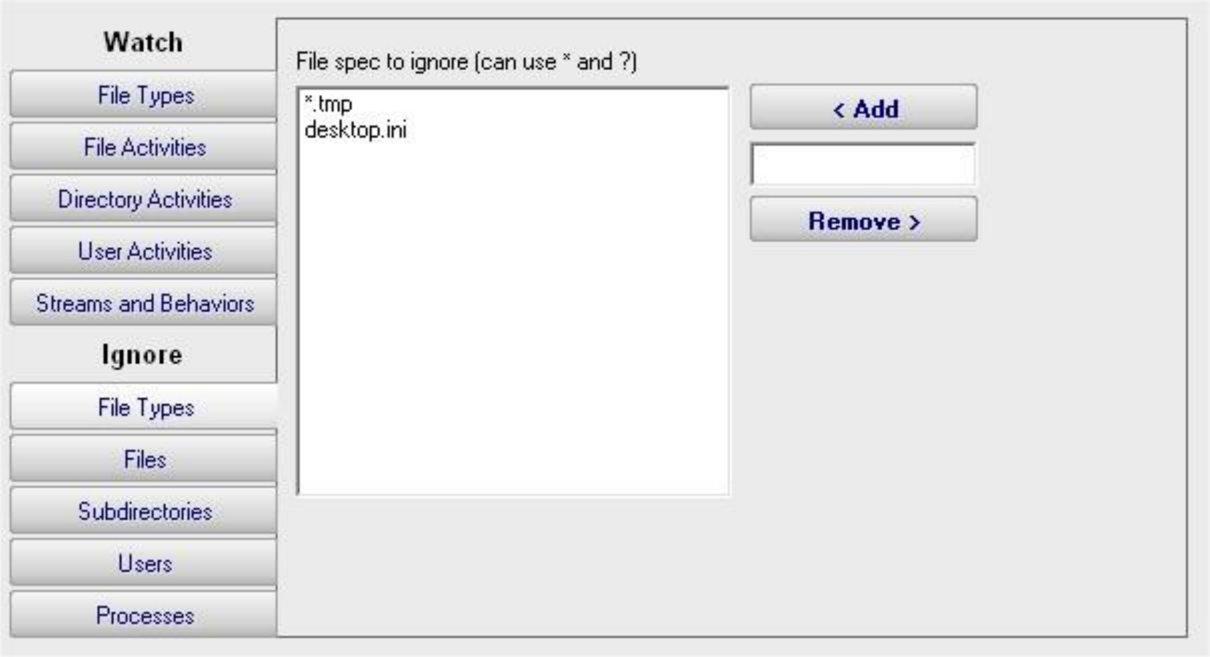
What are file data streams ?

☐ Interpret application behaviors

[What does that mean?]

Ignore: File Types

Similar to the Watch: File Types tab above, this tab lets you specify files using wild cards. In this case however, files that are seen that match the specification are ignored and not alerted on nor written to the database.



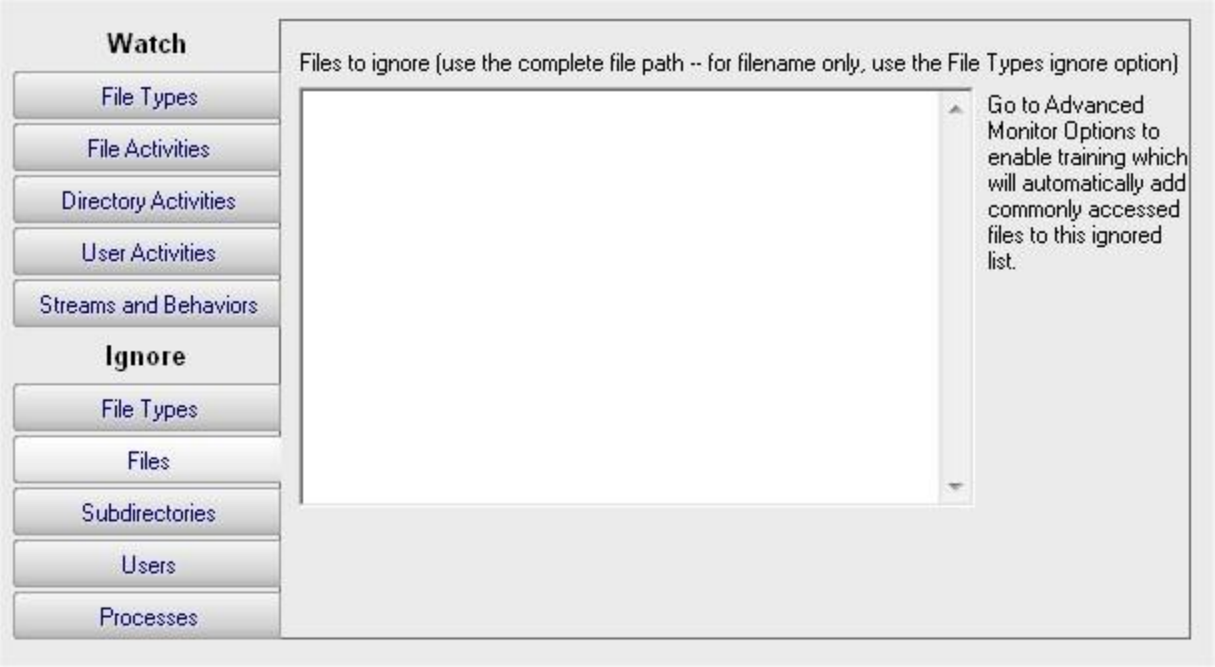
File spec to ignore (can use * and ?)

*.tmp
desktop.ini

Ignore: Files

The Ignore: Files panel lets you specifically ignore files, perhaps because they are just work files, temp files or otherwise unimportant. In this dialog you specify the file using the full path to the file.

If you enable Training via the Advanced Monitor Options, the monitor will watch all matching file I/O and automatically add all ignored files that are accessed during the training period to this list.



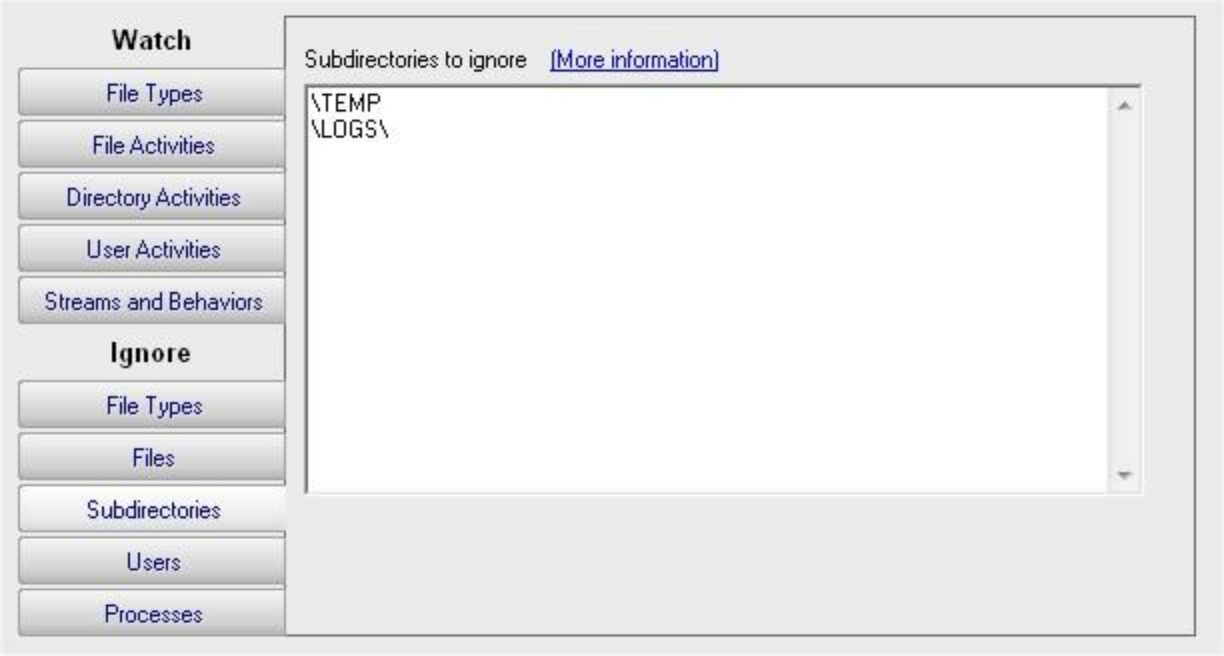
Files to ignore (use the complete file path -- for filename only, use the File Types ignore option)

Go to Advanced Monitor Options to enable training which will automatically add commonly accessed files to this ignored list.

Ignore: Subdirectories

If you need to ignore specific directories below the main directory that you're watching (perhaps a temp directory or a queue directory), you can specify the directory to ignore here. In this case wild cards do not work, but sub-path matching does. That means you can specify the entire directory path to ignore, or you can ignore just a part.

For example, if you enter \TEMP, that would match on C:\TEMP\, C:\TEMPORARY and C:\DOCS\TEMP\ because the characters "\TEMP" were found in each of those paths. If you didn't want to match on C:\TEMPORARY for example, you could filter on "\TEMP\".

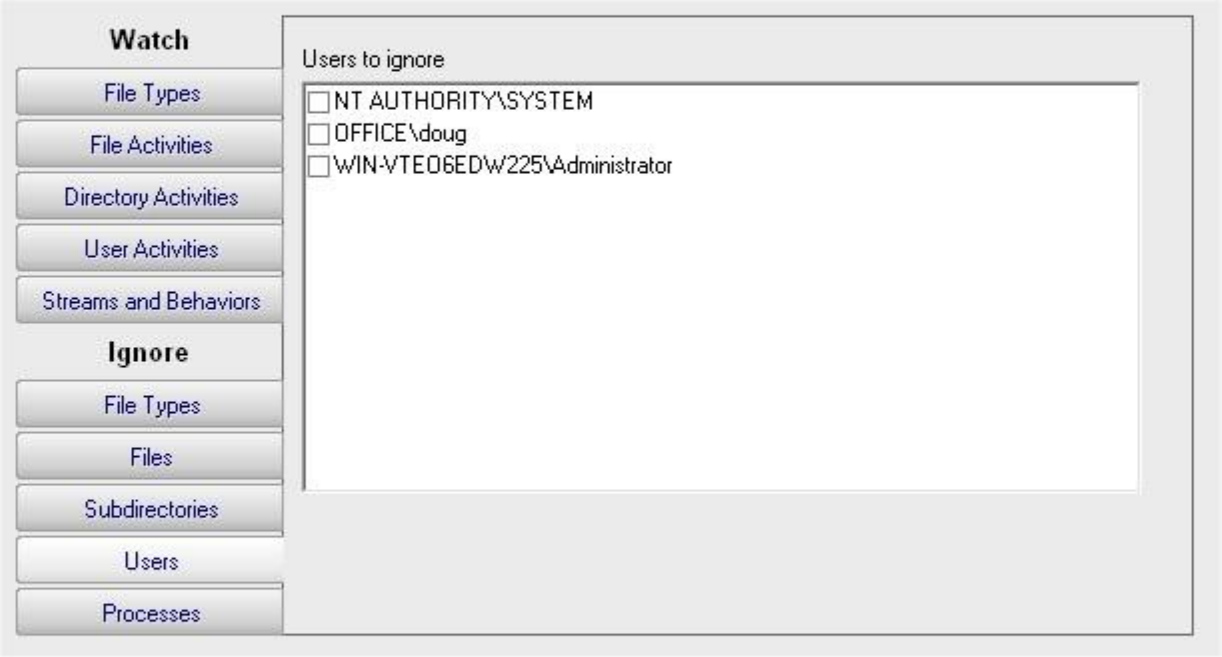


Subdirectories to ignore

```
\TEMP
\LOGS\
```

Ignore: Users

Often there are particular user accounts, particularly accounts that do automated processing like virus scanning, that should not be logged (if for no other reason than to keep the reports easier to review). You can select those user accounts to ignore on this tab.

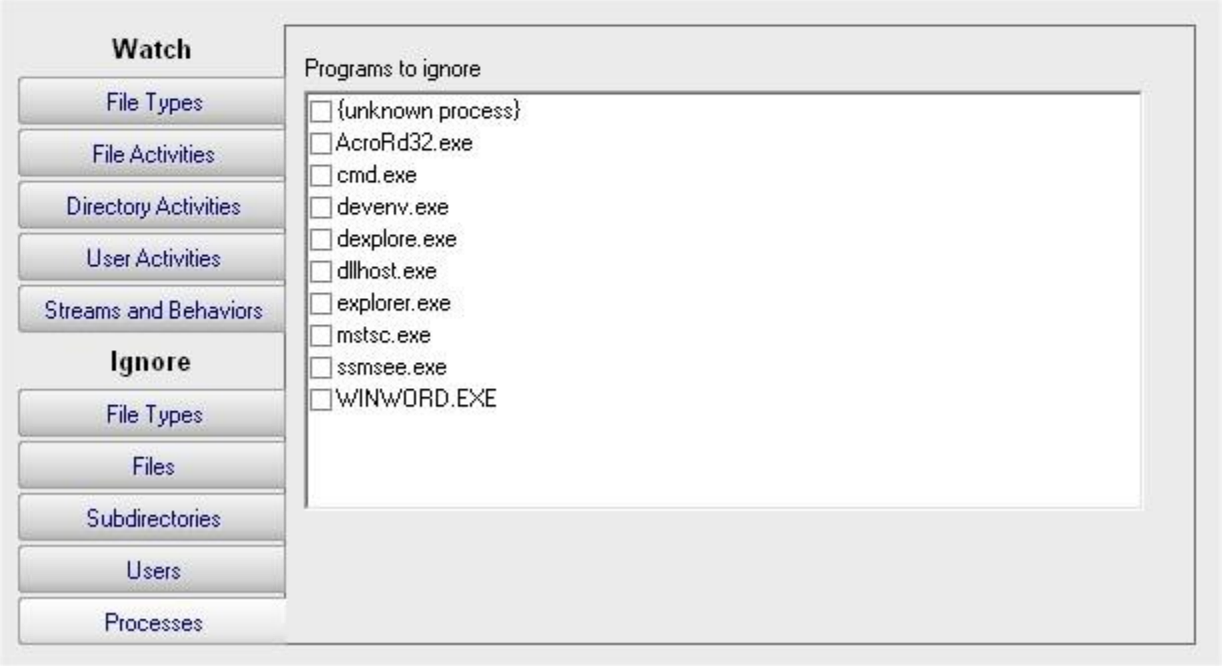


Users to ignore

- □ NT AUTHORITY\SYSTEM
- □ OFFICE\doug
- □ WIN-VTEO6EDW225\Administrator

Ignore: Processes

Similar to the Ignore: Users tab above, there are often reasons to ignore specific processes (perhaps that do automated processing of files) from alerting and being written to the database. These processes can be specified here. Note that only processes that have already been seen are listed.



Programs to ignore

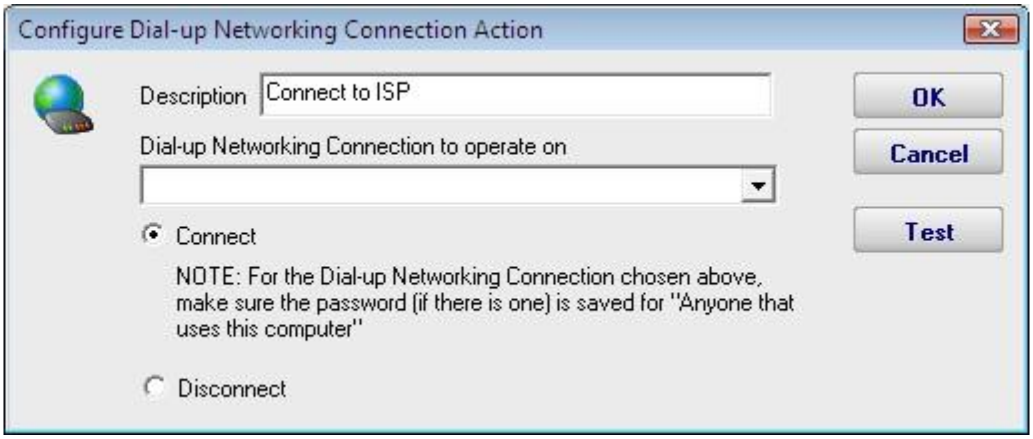
- □ {unknown process}
- □ AcroRd32.exe
- □ cmd.exe
- □ devenv.exe
- □ dexplore.exe
- □ dllhost.exe
- □ explorer.exe
- □ mstsc.exe
- □ ssmsee.exe
- □ WINWORD.EXE

Actions

Contents

Dial-up Connection Action

The Dial-up Connection action dials and connects a Windows Dial-up Networking Connection.


Configure Dial-up Networking Connection Action
Description
Dial-up Networking Connection to operate on
OK
Cancel
Test

Description: Connect to ISP

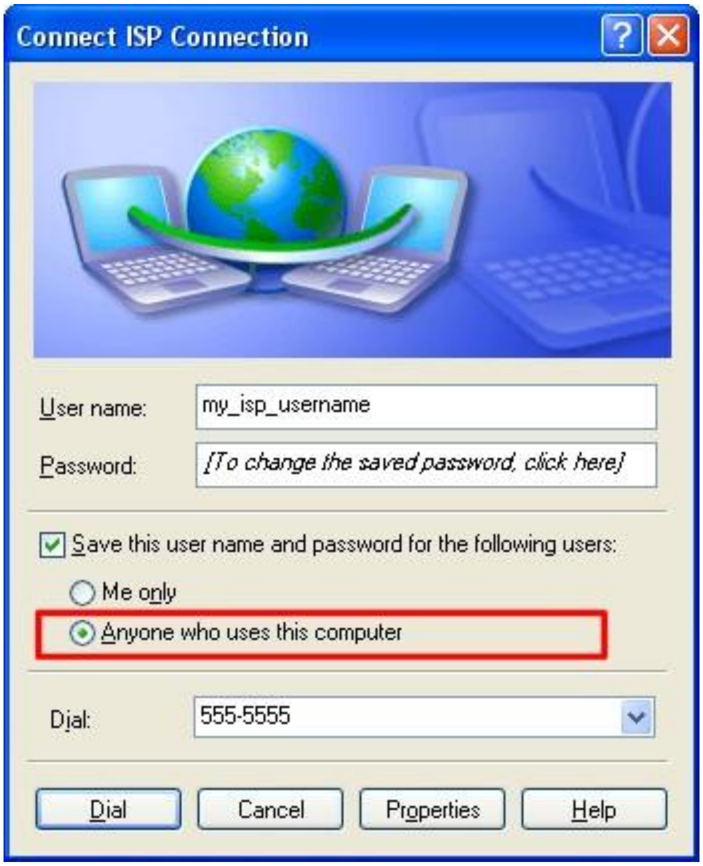
● Connect

NOTE: For the Dial-up Networking Connection chosen above, make sure the password (if there is one) is saved for "Anyone that uses this computer"

○ Disconnect

Previous to configuring this action, you need to create and configure the Dial-up Networking Connection in Windows. This typically involves specifying a phone number to dial, a modem to use, and a username and password to send to the ISP.

When you create the Dial-up Networking Connection, it is important that you save the username and password, and save it for "Anyone who uses this computer" since the account used to run the monitoring service will very often not be the same account that is used when the Dial-up Networking Connection is created.



Connect ISP Connection

User name: my_isp_username

Password: [To change the saved password, click here]

☑ Save this user name and password for the following users:

○ Me only

● Anyone who uses this computer

Dial: 555-5555

Contents

E-mail Message Action

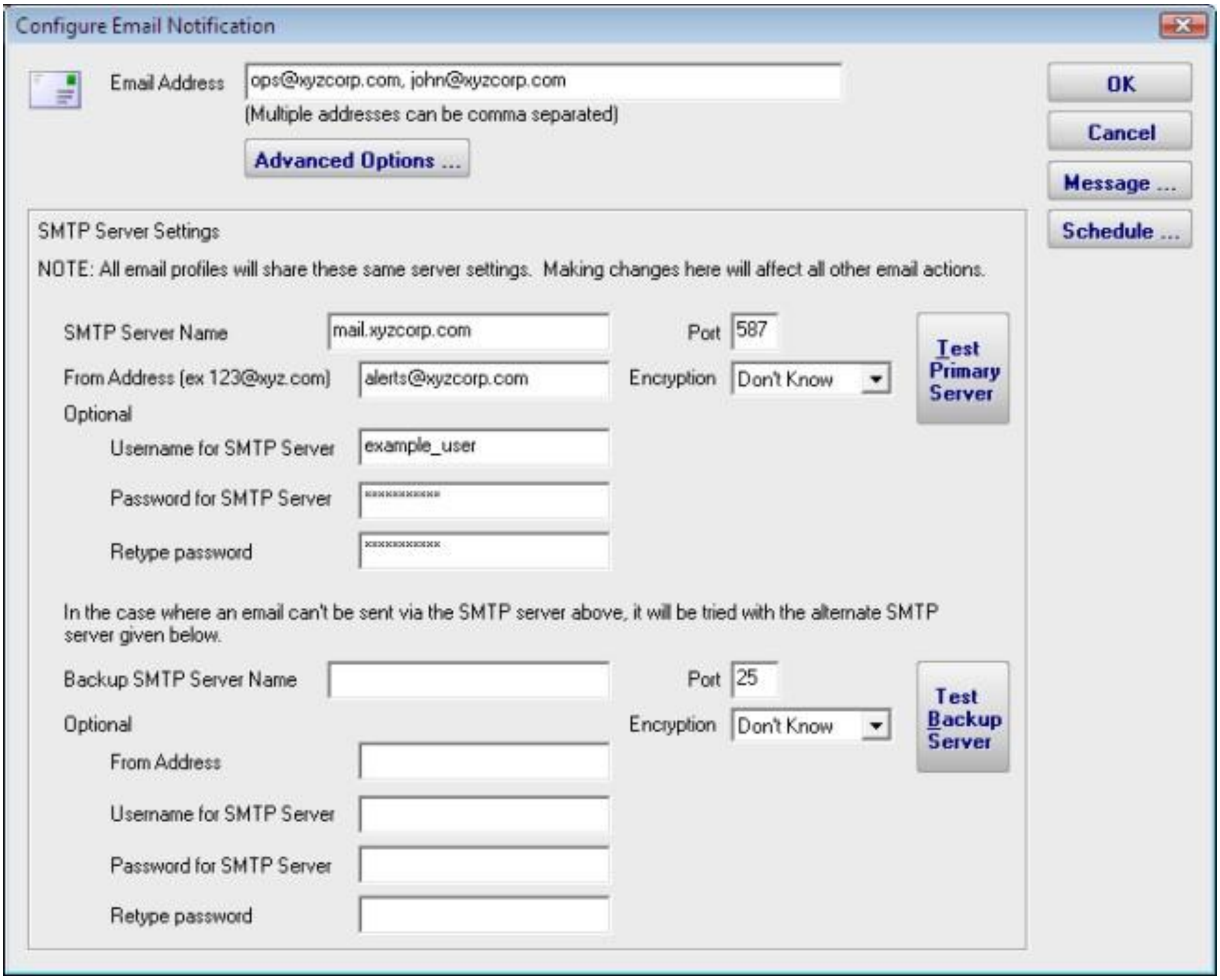
The E-mail Message Action is the standard way for monitors to notify you via SMTP email messages. This allows for typical email messages as well as messages sent to cell phones and pagers if you cell/pager provider has an SMTP gateway (many providers do). We have some hints on that in our SMS FAQ.

To configure this action, give the target SMTP email address. You can add multiple email addresses (comma separate them), and/or create multiple E-mail Message Actions -- whatever is easier for you.

SMTP server settings are shared among all E-mail Message Actions. You can specify a primary SMTP server and a backup which will be used if sending to the primary fails. Naturally a primary SMTP server must be specified; the backup is optional.

The settings for each SMTP server (primary and secondary) can be validated by by the program. You may do this by pressing the "Test Primary Server" and "Test Backup Server" button, respectively. This test causes PA File Sight to send a brief email message as a test to the email address that has been entered into the "Email address" text box at the top of the form. If the sending of the email succeeds and if you successfully receive the message at the same email address as that specified, then the SMTP server settings that you have entered are correct.

The E-mail Message Action supports using SSL for logging into the SMTP server. If you don't know which SSL option to use, leave the setting on Don't Know -- the Test button will figure it out for you.



Email Address: ops@xyzcorp.com, john@xyzcorp.com

(Multiple addresses can be comma separated)

SMTP Server Settings

NOTE: All email profiles will share these same server settings. Making changes here will affect all other email actions.

SMTP Server Name: mail.xyzcorp.com

Port: 587

From Address (ex 123@xyz.com): alerts@xyzcorp.com

Encryption: Don't Know

Optional

Username for SMTP Server: example_user

Password for SMTP Server: ***********

Retype password: ***********

In the case where an email can't be sent via the SMTP server above, it will be tried with the alternate SMTP server given below.

Backup SMTP Server Name:

Port: 25

Encryption: Don't Know

Optional

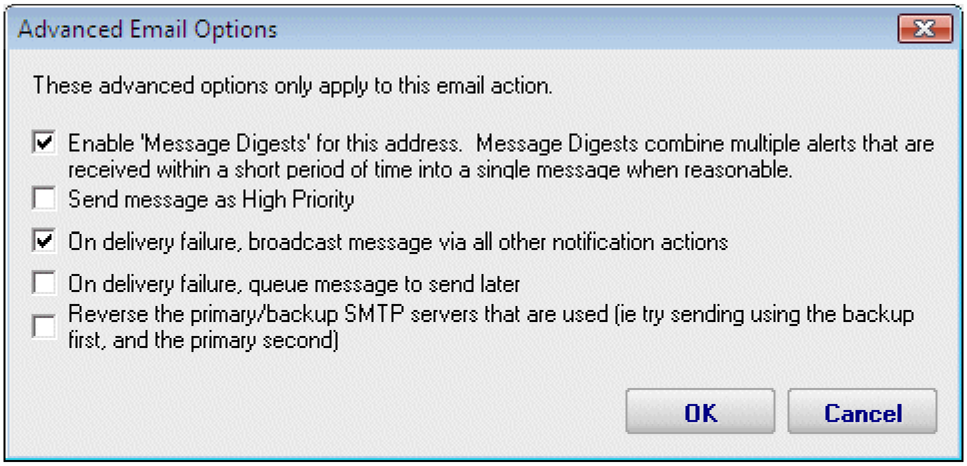
From Address:

Username for SMTP Server:

Password for SMTP Server:

Retype password:

The Advanced Options button will display the dialog below. Each of these options is specific to the E-mail Message Action that you are currently configuring.



These advanced options only apply to this email action.

☑ Enable 'Message Digests' for this address. Message Digests combine multiple alerts that are received within a short period of time into a single message when reasonable.

☐ Send message as High Priority

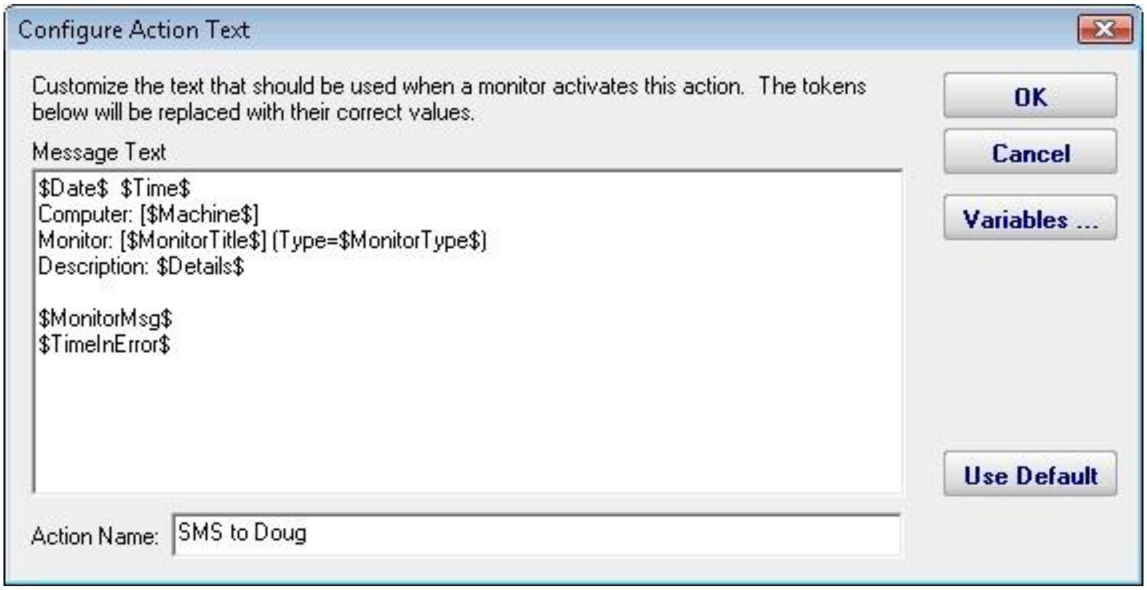
☑ On delivery failure, broadcast message via all other notification actions

☐ On delivery failure, queue message to send later

☐ Reverse the primary/backup SMTP servers that are used (ie try sending using the backup first, and the primary second)

- Messages Digests - To reduce possible message overload, you can specify that multiple messages that are going to be sent within a short time (about 1 minute) combine into a single message.
- Send as High Priority - Self explanatory
- Broadcast on Delivery Failure - If an alert can't be sent via the Primary or Secondary SMTP servers, this option instructs PA File Sight to send the message out using all other configured notification mechanisms. Only notification actions (like SMS, Pager, etc) will tried in this fallback scenario.
- Queue for Later - If a message can't be sent (perhaps because there is no connection to the server), you can specify that the message be queued for later delivery. Periodically PA File Sight will try to send any messages that are in the queue.
- Reverse Primary/Secondary - For testing purposes it is sometimes desirable to send via the Secondary SMTP server just to make sure it is working as expected.

Pressing the Message button displays the configuration dialog below. This lets you customize the message text that is sent to you. This is most useful when sending alerts to devices like pagers and cell phones which might only accept the first sentence or two of a message. You can also rename the action as it shows up in the various action lists (for example to give the email action a group name). You can reset the action to its original/default name by simply clearing the name field.



Customize the text that should be used when a monitor activates this action. The tokens below will be replaced with their correct values.

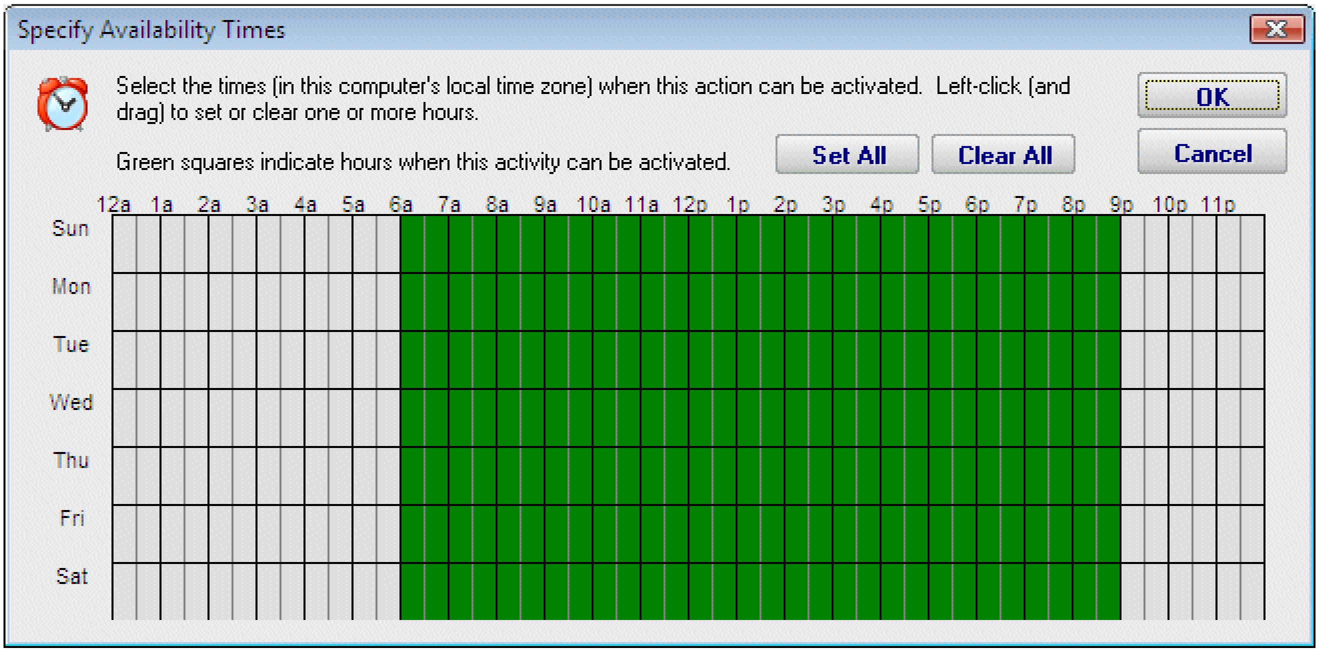
Message Text

```
$Date$  $Time$
Computer: [$Machine$]
Monitor: [$MonitorTitle$] (Type=$MonitorType$)
Description: $Details$

$MonitorMsg$
$TimeInError$
```

Action Name: SMS to Doug

If you're lucky enough to not be on call 24/7 you can use the Schedule button to specify when notifications should be sent through the given email address. On off hours the action acts as though it isn't configured at all. The dark green below indicates 'on hours' and the lighter grey specifies 'off hours'.



Specify Availability Times

Select the times (in this computer's local time zone) when this action can be activated. Left-click (and drag) to set or clear one or more hours.

Green squares indicate hours when this activity can be activated.

	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p
Sun	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜
Mon	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜
Tue	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜
Wed	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜
Thu	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜
Fri	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜
Sat	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜

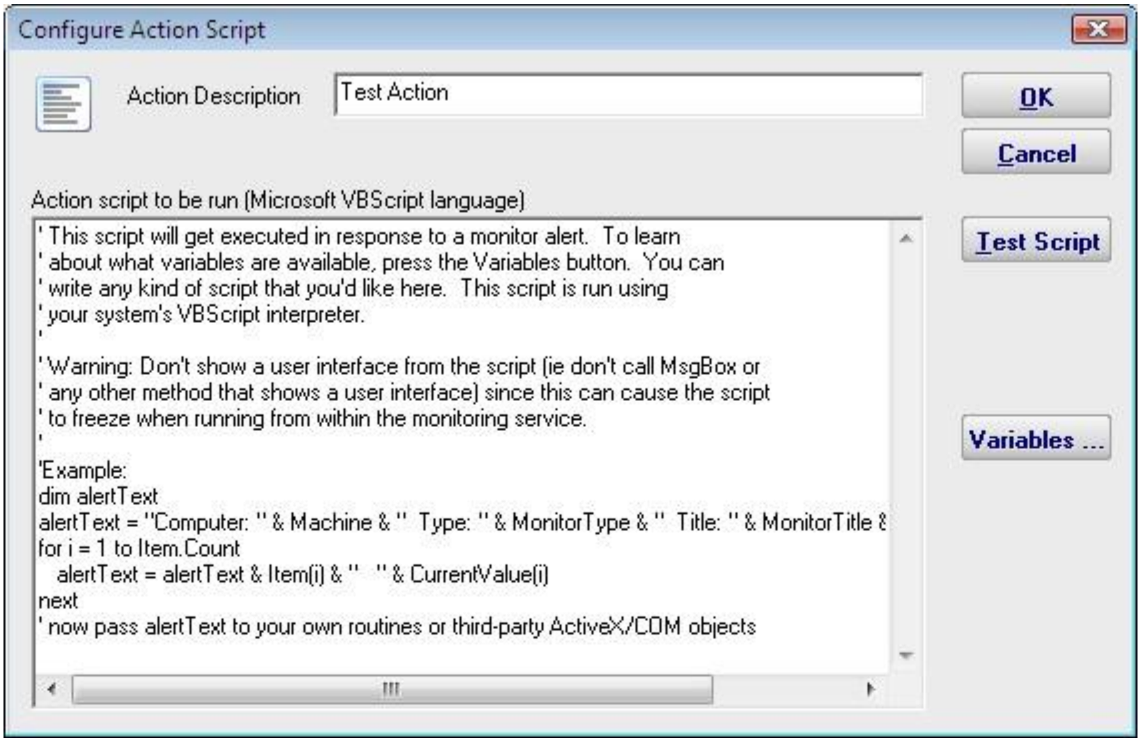
Execute Script Action

The Execute Script Action allows you to receive action parameters that were sent from a monitor and handle them in your own specific way.

The script is run using the computer's built-in VBScript interpreter. This means you can make use of the full VBScript language as well as any installed ActiveX/COM objects which are installed on the system.

Pressing the Test button will cause the script to execute immediately so you can test how it runs. One thing to keep in mind is which user the monitoring service is running as. If it isn't running as the same user that is currently logged in (which is seldom the case) it will have a different HKEY_CURRENT_USER registry hive, different drive mappings, different Internet Explorer settings, etc.

Since the monitoring service is not interactive, it is highly recommended that you **not** display any user interface (MsgBox, etc) from within the script since no users will be able to close the user interface (which will cause the thread running the script to never finish).



Action Description: Test Action

Action script to be run (Microsoft VBScript language)

```
' This script will get executed in response to a monitor alert.  To learn
' about what variables are available, press the Variables button.  You can
' write any kind of script that you'd like here.  This script is run using
' your system's VBScript interpreter.
'
' Warning: Don't show a user interface from the script (ie don't call MsgBox or
' any other method that shows a user interface) since this can cause the script
' to freeze when running from within the monitoring service.
'
'Example:
dim alertText
alertText = "Computer: " & Machine & "  Type: " & MonitorType & "  Title: " & MonitorTitle &
for i = 1 to Item.Count
   alertText = alertText & Item(i) & "   " & CurrentValue(i)
next
' now pass alertText to your own routines or third-party ActiveX/COM objects
```

An example script that connects to a database is shown below

```
Option Explicit
Dim objconnection
Dim objrecordset
Dim strDetails

Const adOpenStatic = 3
Const adLockOptimistic = 3

Set objconnection = CreateObject("ADODB.Connection")
Set objrecordset = CreateObject("ADODB.Recordset")
```

```
objconnection.Open _
"Provider=SQLOLEDB;Data Source=;" & _
"Initial Catalog=;" & _
"User ID=;Password=;"

objrecordset.Open "", objconnection, adOpenStatic, adLockOptimistic
```

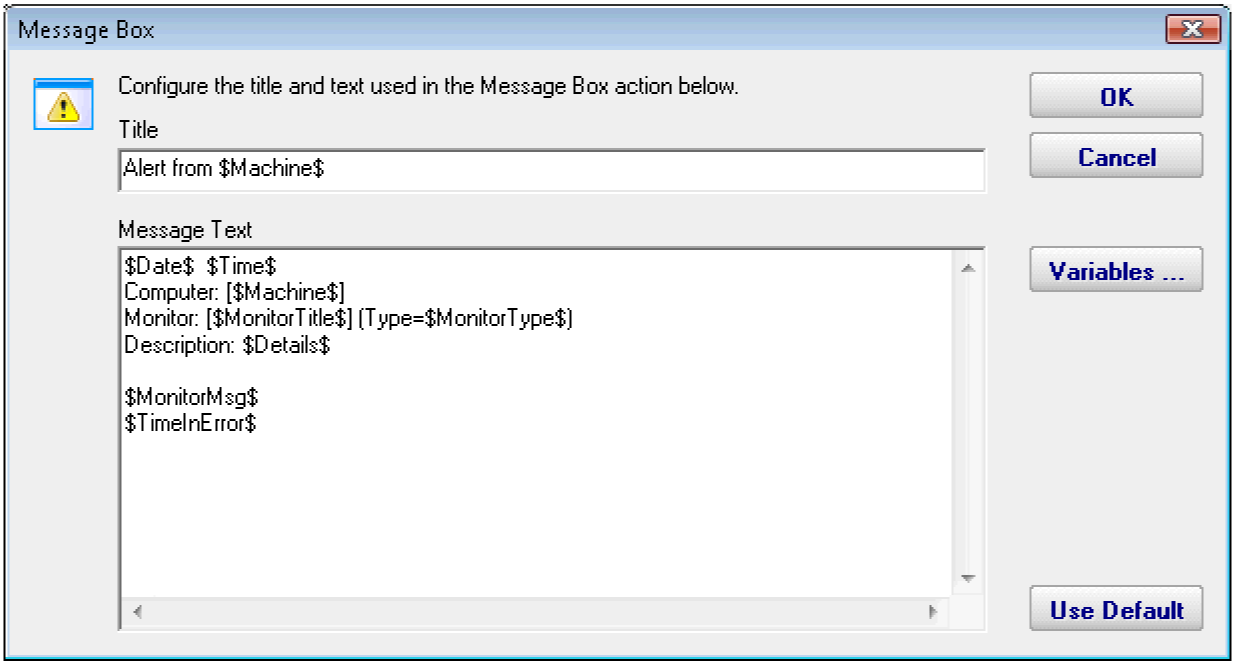
Contents

Message Box Action

This action can be used when you want a message box to pop-up on the machine that is running the monitoring service with details about a recent anomaly. The Message Box Action keeps track of how many more message boxes are waiting to be shown, and lets you cancel them all at once if you choose to.

The dialog shown below is displayed when you add or edit a message box action. PA File Sight fills this dialog with a standard message box title and message. You may customize the message box that is displayed when this action is taken when the error occurs by editing the Title or Message Text.

The button titled "Variables" will open a screen that displays the Replacement Variables that are available for use.



Configure the title and text used in the Message Box action below.

Title: Alert from $Machine$

Message Text:

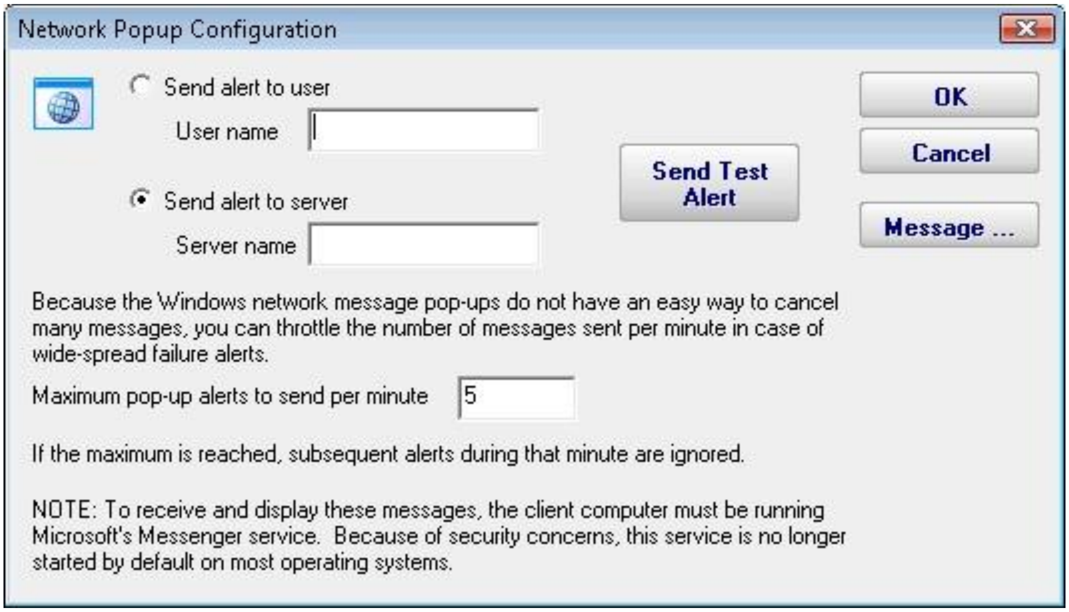
```
$Date$  $Time$
Computer: [$Machine$]
Monitor: [$MonitorTitle$] (Type=$MonitorType$)
Description: $Details$

$MonitorMsg$
$TimeInError$
```

Network Message Action

The Network Message Action is equivalent to doing a "net send" from the command line. It allows you to direct a message box pop-up to any particular user or computer on the network.

The client machine must be running Microsoft's Messenger service to receive and display these messages. Because of spam and security concerns, the Messenger service is not started by default on most systems.



○ Send alert to user

User name

● Send alert to server

Server name

Because the Windows network message pop-ups do not have an easy way to cancel many messages, you can throttle the number of messages sent per minute in case of wide-spread failure alerts.

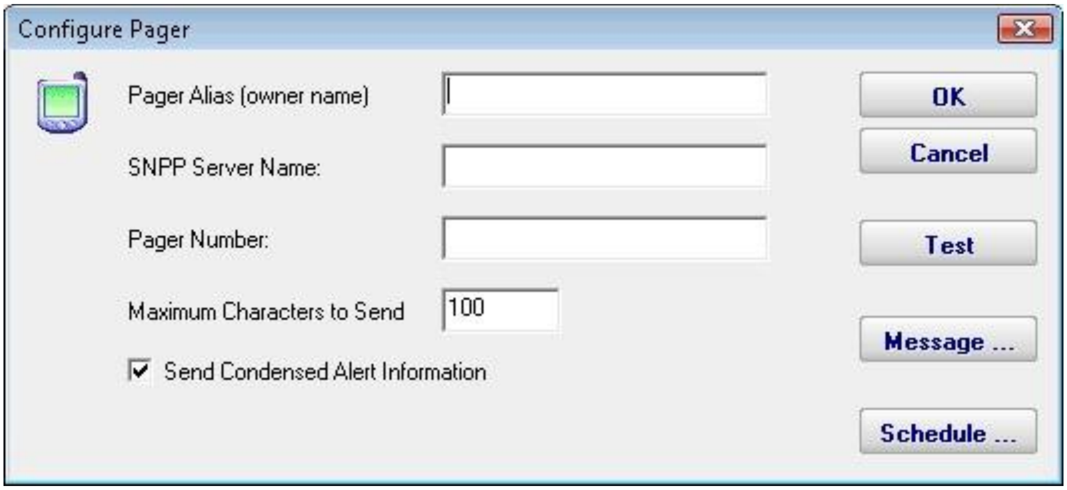
Maximum pop-up alerts to send per minute 5

If the maximum is reached, subsequent alerts during that minute are ignored.

NOTE: To receive and display these messages, the client computer must be running Microsoft's Messenger service. Because of security concerns, this service is no longer started by default on most operating systems.

Send Pager Alert Action

The Send Pager Alert action can send monitor details to an SNPP pager.



Pager Alias (owner name)

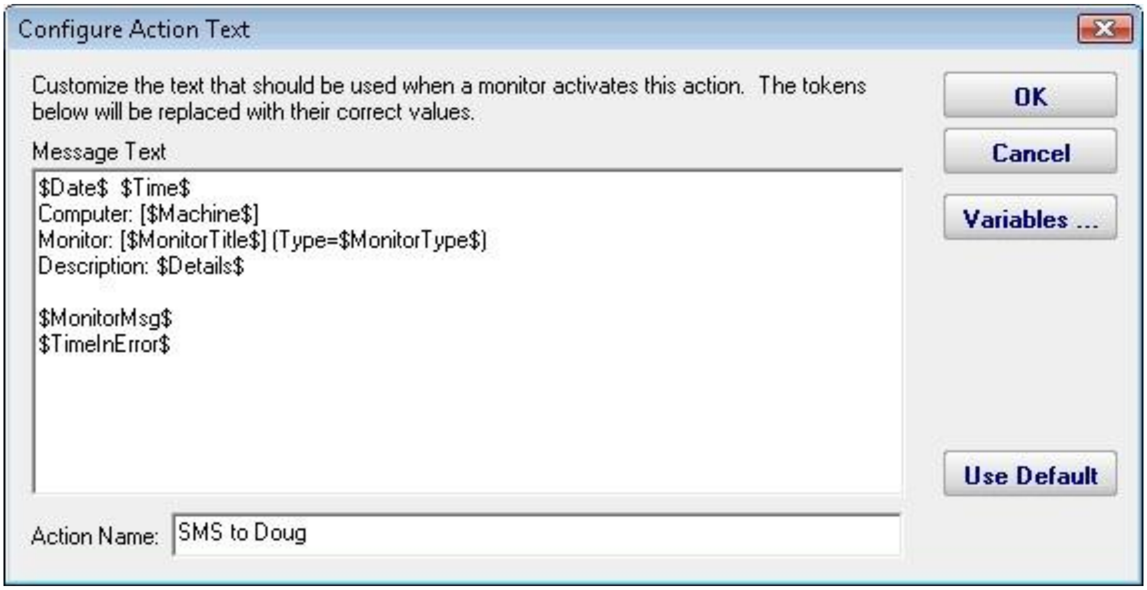
SNPP Server Name:

Pager Number:

Maximum Characters to Send: 100

☑ Send Condensed Alert Information

Pressing the Message button displays the configuration dialog below. This lets you customize the message text that is sent to you. This is most useful for trimming the size of the message that is sent to your pager. You can also rename the action as it shows up in the various action lists. You can reset the action to its original/default name by simply clearing the name field.



Customize the text that should be used when a monitor activates this action. The tokens below will be replaced with their correct values.

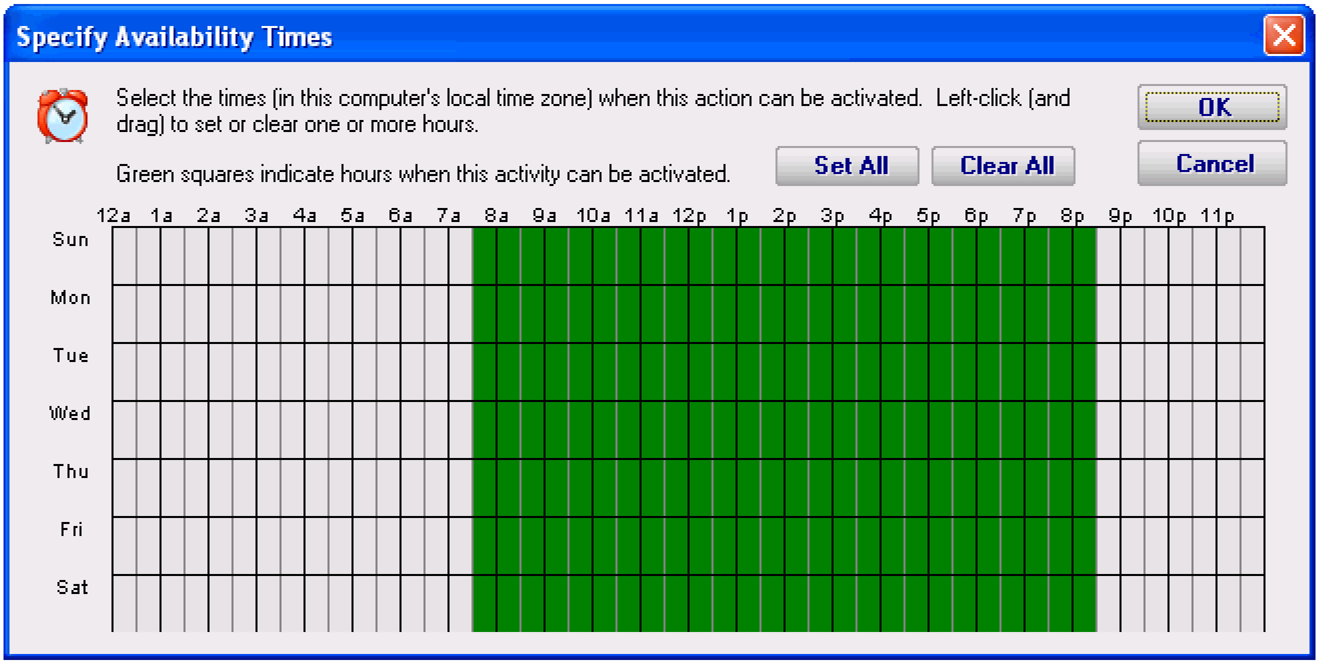
Message Text

```
$Date$ $Time$
Computer: [$Machine$]
Monitor: [$MonitorTitle$] (Type=$MonitorType$)
Description: $Details$

$MonitorMsg$
$TimeInError$
```

Action Name: SMS to Doug

If you're lucky enough to not be on call 24/7 you can use the Schedule button to specify when notifications should be sent to the given pager. On off hours the action acts as though it isn't configured at all. The dark green below indicates 'on hours' and the lighter grey specifies 'off hours'.



Select the times (in this computer's local time zone) when this action can be activated. Left-click (and drag) to set or clear one or more hours.

Green squares indicate hours when this activity can be activated.

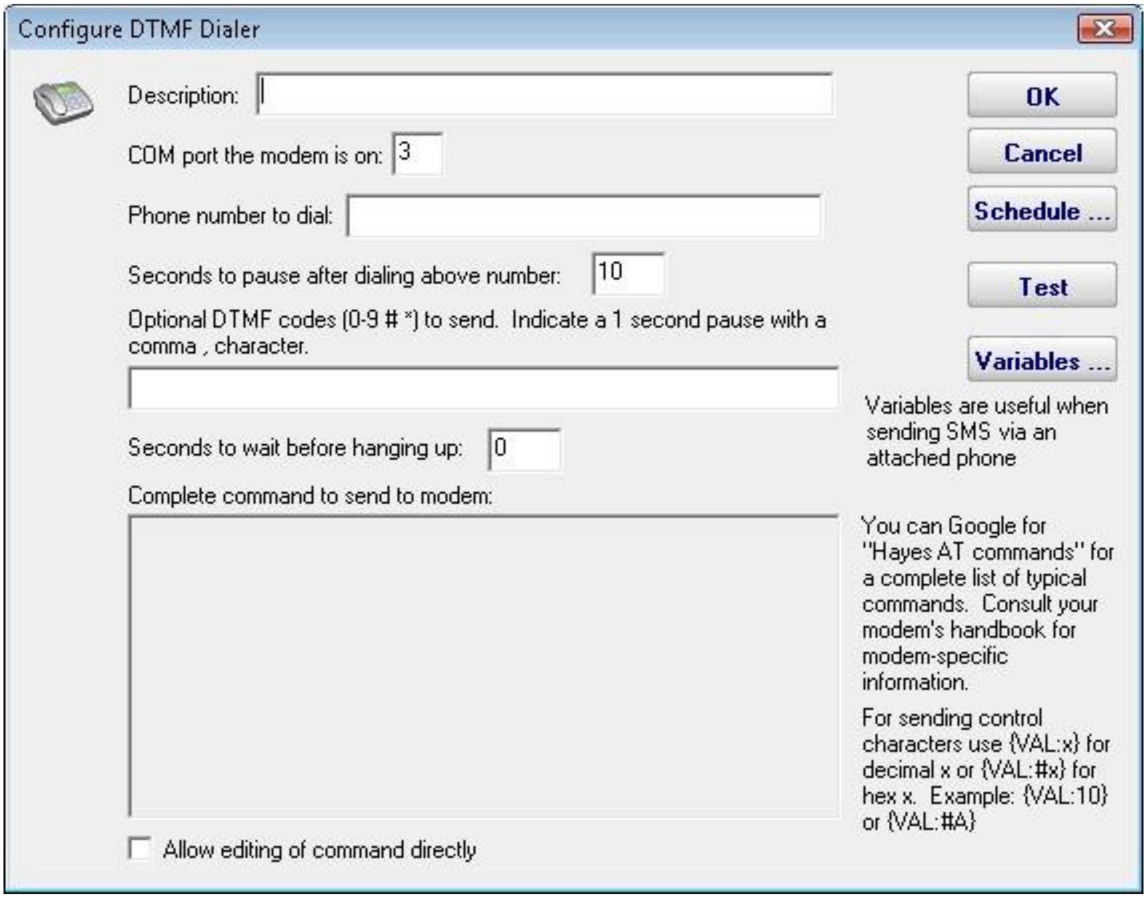
	12a		1a		2a		3a		4a		5a		6a		7a		8a		9a		10a		11a		12p		1p		2p		3p		4p		5p		6p		7p		8p		9p		10p		11p	
Sun																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩							
Mon																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩							
Tue																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩							
Wed																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩							
Thu																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩							
Fri																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩							
Sat																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩							

Phone Dialer (DTMF/SMS)

The Phone Dialer action is used to make calls over a normal phone line via a modem. This action doesn't need an ISP, but rather calls a phone (a human who would recognize the Caller ID), perhaps an automated system, or an attached cell phone through which SMS messages can be sent.

The Phone Dialer can also optionally send DTMF tones (touch-tones) which could be useful for automatically navigating a phone menu system, and any other characters such as SMS message text.

The timeout values are important. Since there isn't a well defined audio protocol with humans and/or phone systems on the other end, you'll need to build in delays. This includes delays for the other party to answer. Be sure to specify enough pause after dialing the number for the number to go through, the other phone to ring and be answered.



Configure DTMF Dialer

Description:

COM port the modem is on: 3

Phone number to dial:

Seconds to pause after dialing above number: 10

Optional DTMF codes (0-9 # *) to send. Indicate a 1 second pause with a comma , character.

Seconds to wait before hanging up: 0

Complete command to send to modem:

□ Allow editing of command directly

Variables are useful when sending SMS via an attached phone

You can Google for "Hayes AT commands" for a complete list of typical commands. Consult your modem's handbook for modem-specific information.

For sending control characters use {VAL:x} for decimal x or {VAL:#x} for hex x. Example: {VAL:10} or {VAL:#A}

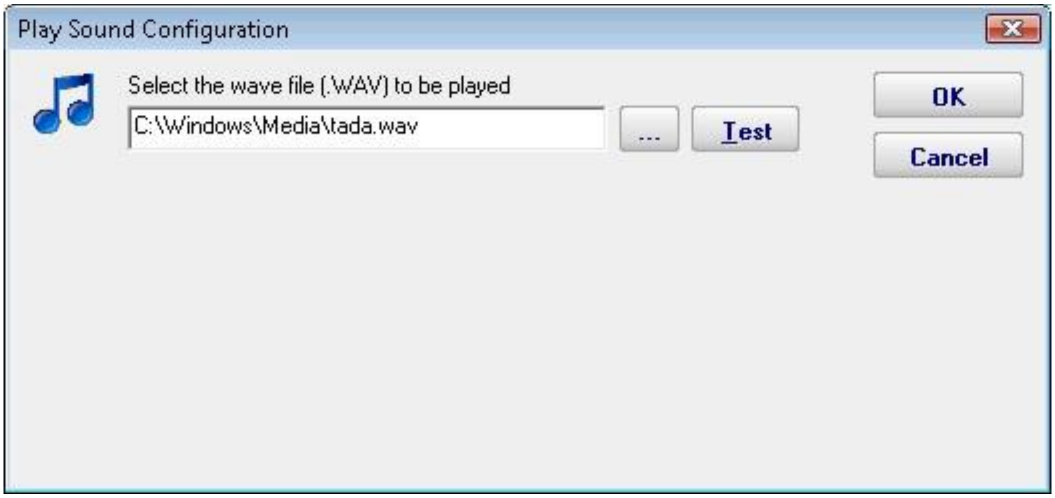
The modem script is shown at the bottom of the dialog, and will work with most modems since it is built on the basic Hayes AT command set. Your modem may have other features and/or require other commands. Your modem documentation will list the commands it accepts. If you need to modify the script to work with your specific modem, check "Allow editing of command directly".

For sending SMS messages via a directly connected cell phone, you'll need to modify the script directly. Look in your phone manual for the commands for sending messages. In general you'll be using some form of the AT+CMGS command. There is a sample script in our FAQ at SMS Hints.

Contents

Play Sound File Action

The Play Sound File action will play the specified .wav file when the action is triggered.



Play Sound Configuration

Select the wave file (.WAV) to be played

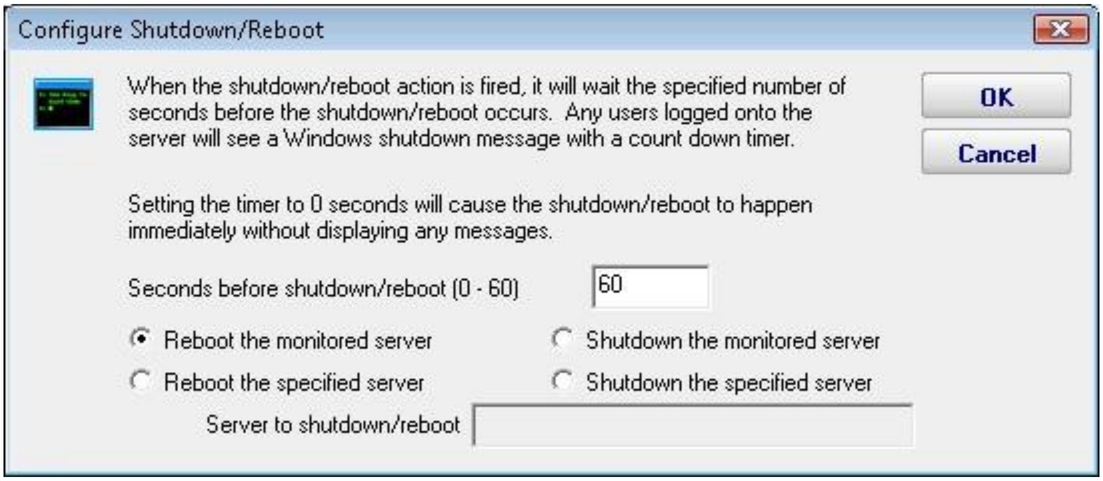
C:\Windows\Media\tada.wav

Contents

Reboot Computer Action

The Reboot Computer action causes a computer to reboot or shutdown when it is run. You can specify which computer using the radio button options. By default the **monitored computer** will be rebooted when this action is run.

To shut down the local computer, the user that is running the service must have the SE_SHUTDOWN_NAME privilege (also known as the "Shut down the system" policy). To shut down a remote computer, the user must have the SE_REMOTE_SHUTDOWN_NAME privilege on the remote computer.



Configure Shutdown/Reboot

When the shutdown/reboot action is fired, it will wait the specified number of seconds before the shutdown/reboot occurs. Any users logged onto the server will see a Windows shutdown message with a count down timer.

Setting the timer to 0 seconds will cause the shutdown/reboot to happen immediately without displaying any messages.

Seconds before shutdown/reboot (0 - 60) 60

● Reboot the monitored server ○ Shutdown the monitored server

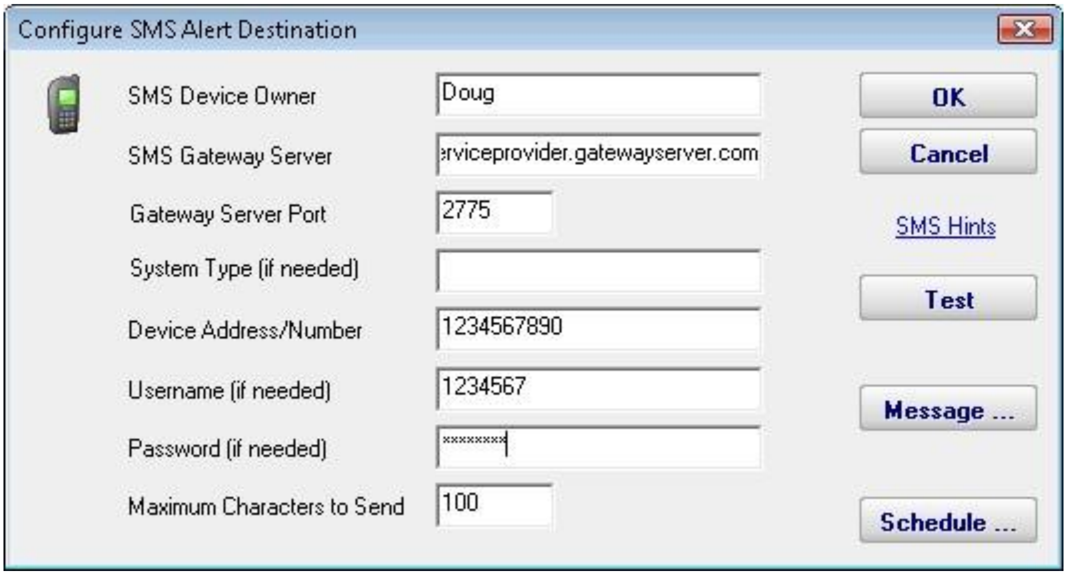
○ Reboot the specified server ○ Shutdown the specified server

Server to shutdown/reboot

Contents

SMS Text Message Action

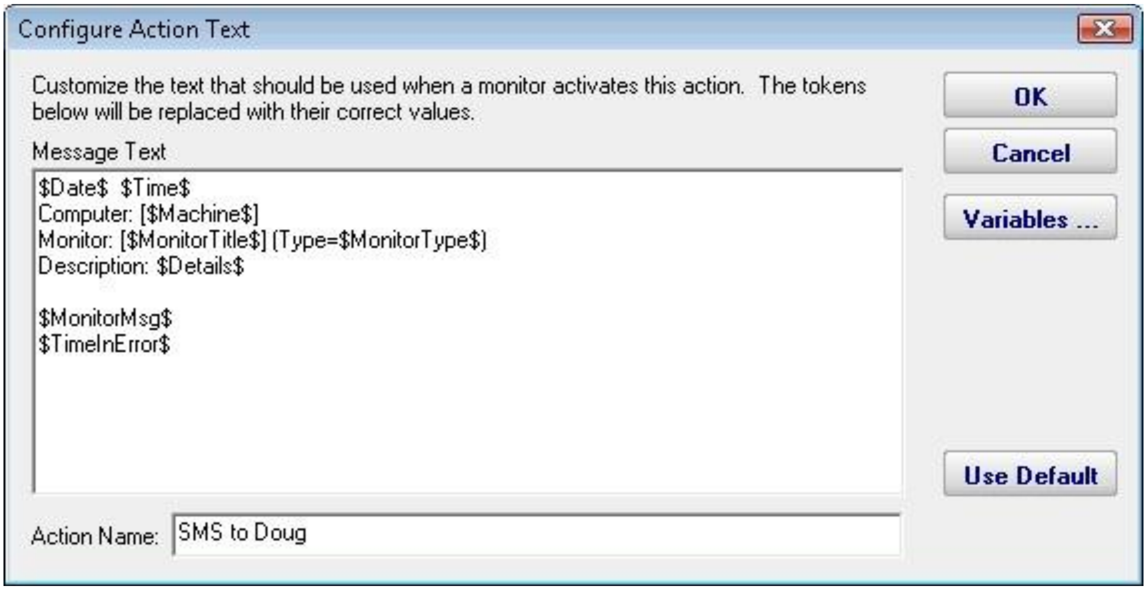
This action can send alert messages via SMS to your phone or mobile device. The message is sent through an SMS Gateway via the SMPP protol.



Configure SMS Alert Destination

SMS Device Owner: Doug
SMS Gateway Server: ərviceprovider.gatewayserver.com
Gateway Server Port: 2775
System Type (if needed):
Device Address/Number: 1234567890
Username (if needed): 1234567
Password (if needed): ********
Maximum Characters to Send: 100

Pressing the Message button displays the configuration dialog below. This lets you customize the message text that is sent to you. This is most useful for trimming the size of the message that is sent to your device. You can also rename the action as it shows up in the various action lists. You can reset the action to its original/default name by simply clearing the name field.



Configure Action Text

Customize the text that should be used when a monitor activates this action. The tokens below will be replaced with their correct values.

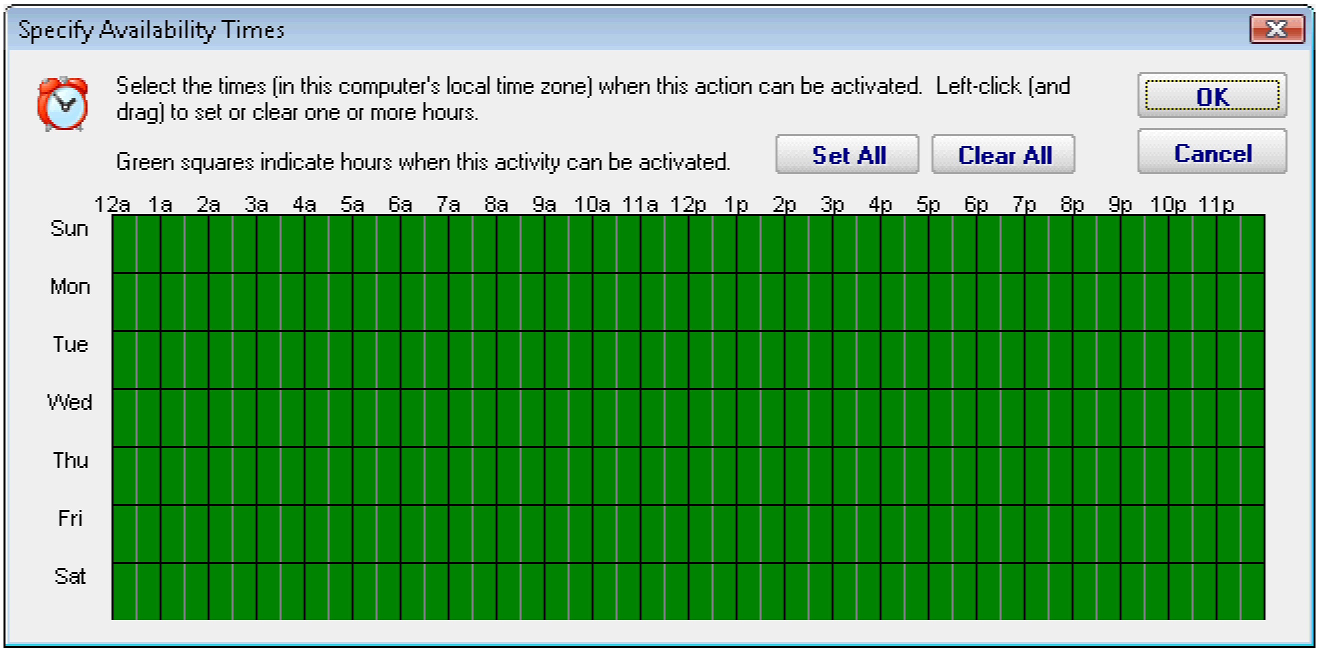
Message Text

```
$Date$  $Time$
Computer: [$Machine$]
Monitor: [$MonitorTitle$] (Type=$MonitorType$)
Description: $Details$

$MonitorMsg$
$TimeInError$
```

Action Name: SMS to Doug

If you're lucky enough to not be on call 24/7 you can use the Schedule button to specify when notifications should be sent to the given device. On off hours the action acts as though it isn't configured at all. The dark green below indicates 'on hours' and the lighter grey specifies 'off hours'.



Select the times (in this computer's local time zone) when this action can be activated. Left-click (and drag) to set or clear one or more hours.

Green squares indicate hours when this activity can be activated.

	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p
Sun	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Mon	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Tue	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Wed	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Thu	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Fri	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Sat	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Also note that we have an FAQ on other ways to send alerts to phones and pagers at: SMS Hints

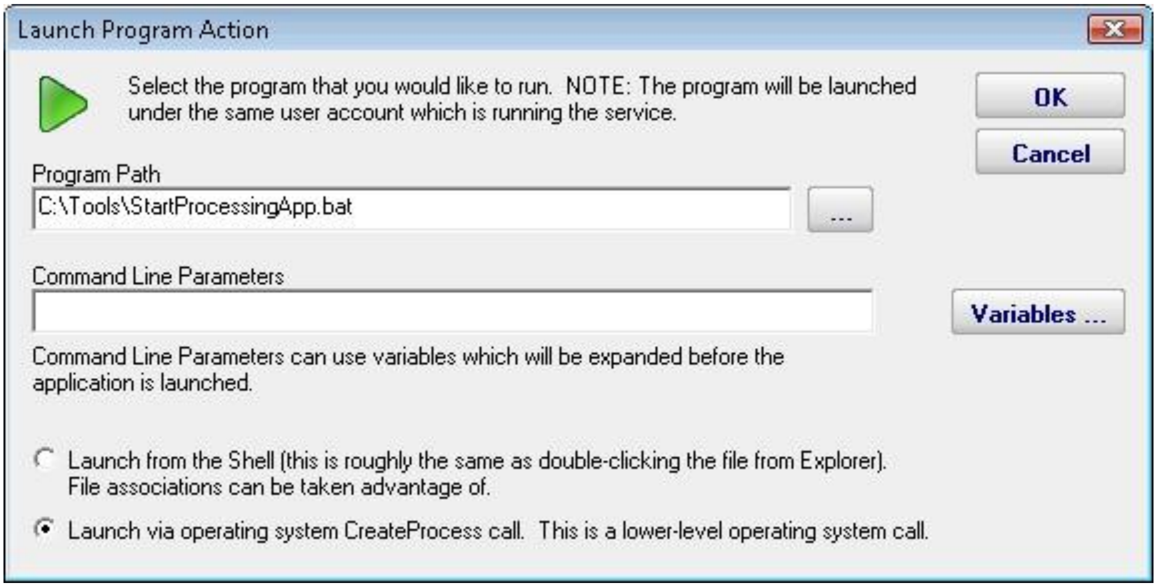
Contents

Start Application Action

This action will launch any local application that you specify when it is triggered by a monitor.

It is important to remember that the application is being launched by the monitoring service, which quite often runs as a restricted user (like Local System) which might not have the same HKEY_CURRENT_USER registry hive, mapped drives, printers, etc as you do. You can always configure who the service runs as from Preferences in the console application, or even configure which user is used to monitor a particular computer by right clicking on that computer in the navigation panel in the Console.

One final note: The application is started on the local computer (where the monitoring service is being run), not on any remote computer that might be monitored at that time. To launch an application on a remote machine, we recommend having the Start Application Action run Microsoft's PsExec, and direct it to launch your target application remotely. More information on PsExec


Launch Program Action

Select the program that you would like to run. NOTE: The program will be launched under the same user account which is running the service.

Program Path: C:\Tools\StartProcessingApp.bat

Command Line Parameters:

Command Line Parameters can use variables which will be expanded before the application is launched.

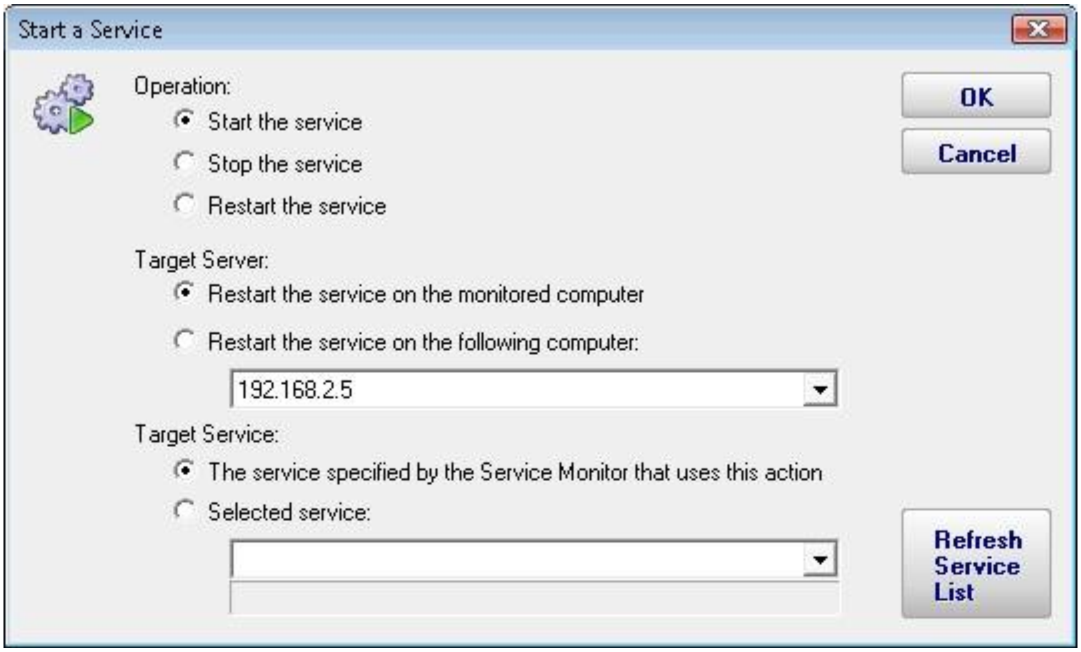
○ Launch from the Shell (this is roughly the same as double-clicking the file from Explorer). File associations can be taken advantage of.

● Launch via operating system CreateProcess call. This is a lower-level operating system call.

Start, Stop or Restart a Service Action

As the name implies, the Start, Stop or Restart a Service action can control the running state of a Windows service. It controls the specified service on the computer which is being monitored. For example, if computer OPS is running the monitoring service, and it is running a monitor which is watching the web server on computer WEB1, the web server on WEB1 could be restarted if needed.

The action can be configured to restart a specific service on a specific computer, or if attached to a Server Monitor, it can restart which ever service has stopped as reported by that monitor.



Start a Service

Operation:

● Start the service

○ Stop the service

○ Restart the service

Target Server:

● Restart the service on the monitored computer

○ Restart the service on the following computer:

192.168.2.5

Target Service:

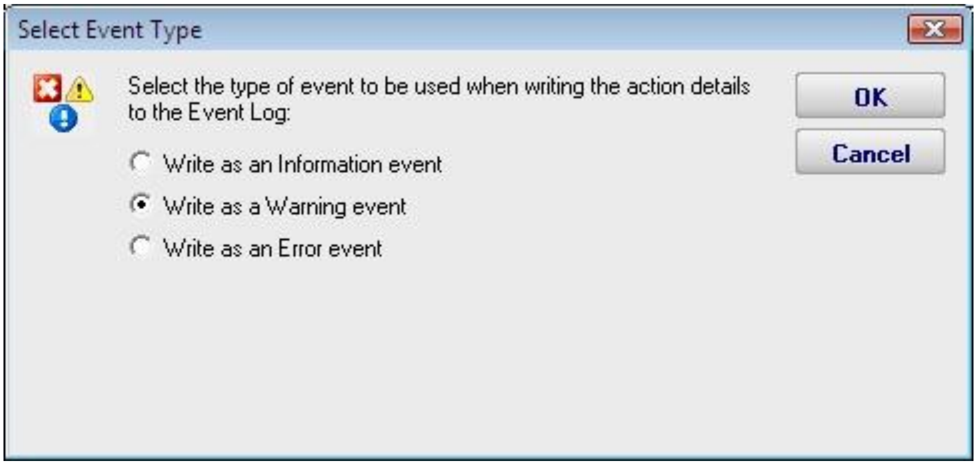
● The service specified by the Service Monitor that uses this action

○ Selected service:

Contents

Write to Event Log Action

The Write to Event Log Action writes details of a monitor's findings to the Windows Application Event Log. You can specify whether to write the event as an Error, Warning or Information event.



Select the type of event to be used when writing the action details to the Event Log:

○ Write as an Information event

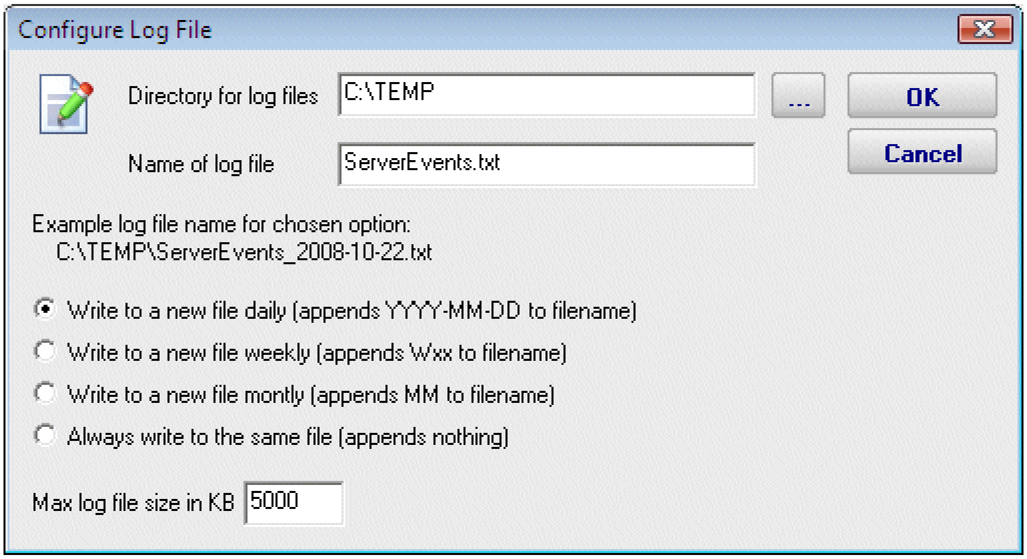
● Write as a Warning event

○ Write as an Error event

Contents

Write to a Text Log File Action

The text logging action writes to a text log file the details of a problem found by a monitor. You specify where the log file goes, and how often a new file is started.



Directory for log files: C:\TEMP

Name of log file: ServerEvents.txt

Example log file name for chosen option:
C:\TEMP\ServerEvents_2008-10-22.txt

● Write to a new file daily (appends YYYY-MM-DD to filename)
○ Write to a new file weekly (appends Wxx to filename)
○ Write to a new file montly (appends MM to filename)
○ Always write to the same file (appends nothing)

Max log file size in KB: 5000

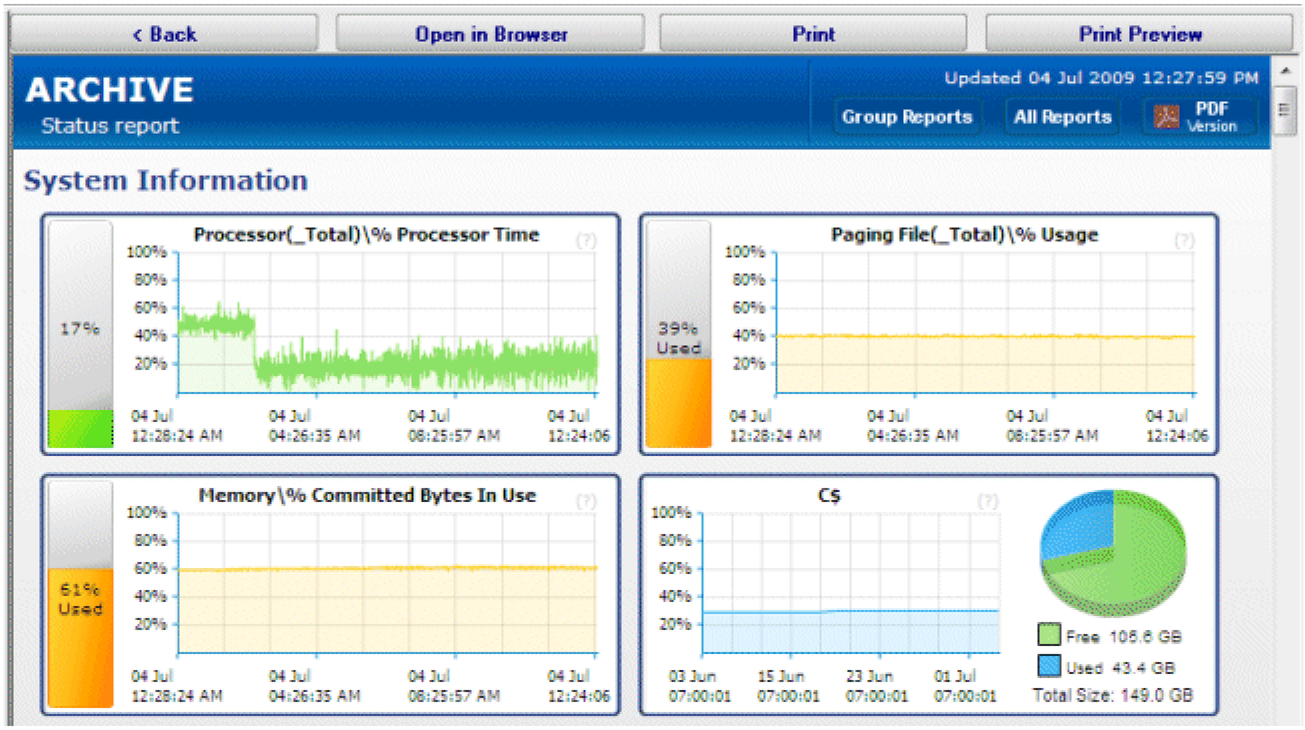
Reports

Contents

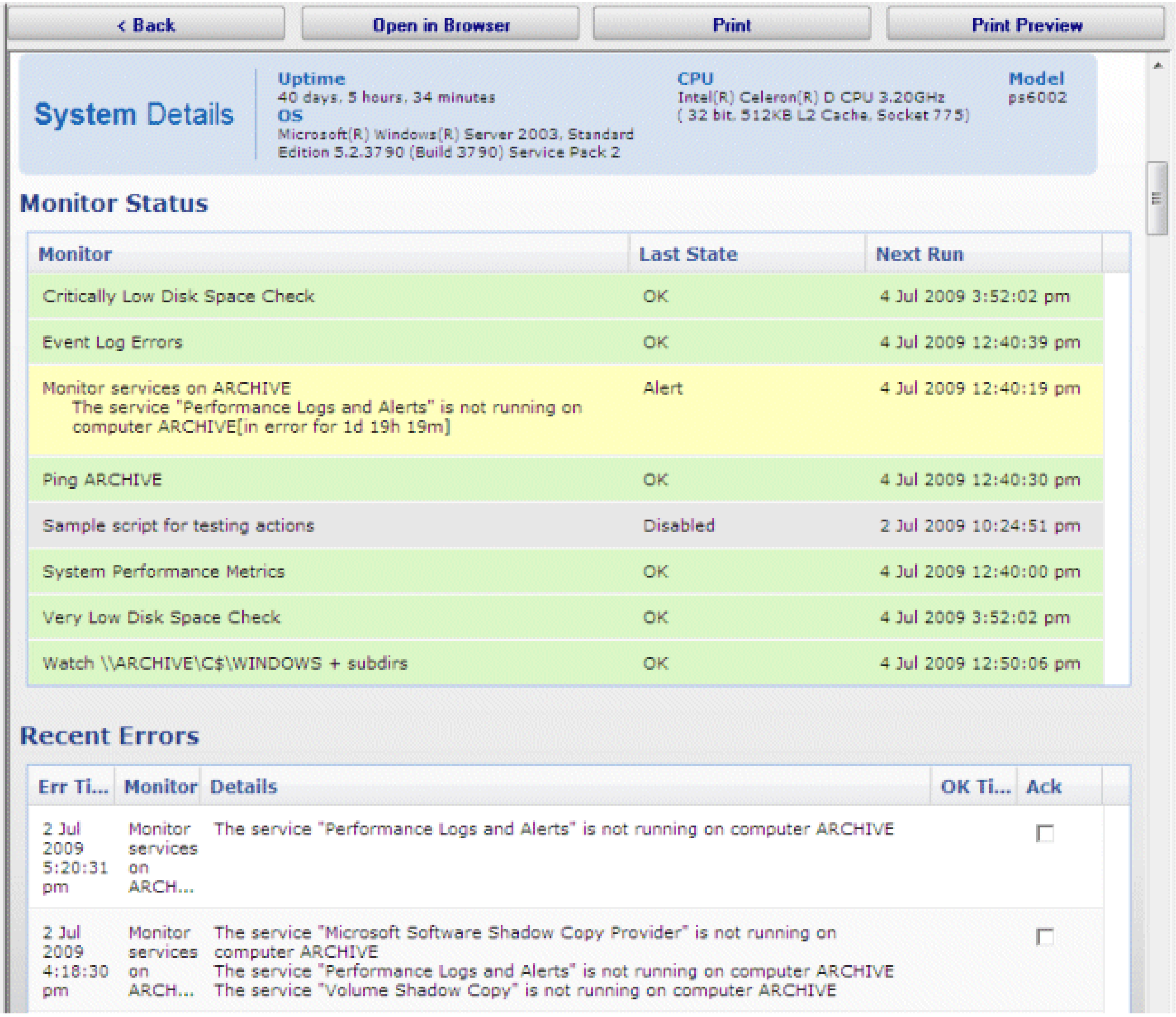
Server Status Report

The Server Status Report is a quick way to check basic stats on your server.

At the top right of the report are buttons to show you the reports for the group the server is part of, the index of all reports, and a button to get a PDF version of the report.



In the System Information area are some optional graphs. The graphs will probably be different than the ones shown above. The graphs are automatically created based on data collected by the running monitors.



System Details

Uptime
40 days, 5 hours, 34 minutes
OS
Microsoft(R) Windows(R) Server 2003, Standard Edition 5.2.3790 (Build 3790) Service Pack 2

CPU
Intel(R) Celeron(R) D CPU 3.20GHz
(32 bit, 512KB L2 Cache, Socket 775)

Model
ps6002

Monitor Status

Monitor	Last State	Next Run
Critically Low Disk Space Check	OK	4 Jul 2009 3:52:02 pm
Event Log Errors	OK	4 Jul 2009 12:40:39 pm
Monitor services on ARCHIVE The service "Performance Logs and Alerts" is not running on computer ARCHIVE[in error for 1d 19h 19m]	Alert	4 Jul 2009 12:40:19 pm
Ping ARCHIVE	OK	4 Jul 2009 12:40:30 pm
Sample script for testing actions	Disabled	2 Jul 2009 10:24:51 pm
System Performance Metrics	OK	4 Jul 2009 12:40:00 pm
Very Low Disk Space Check	OK	4 Jul 2009 3:52:02 pm
Watch \\ARCHIVE\C$\WINDOWS + subdirs	OK	4 Jul 2009 12:50:06 pm

Recent Errors

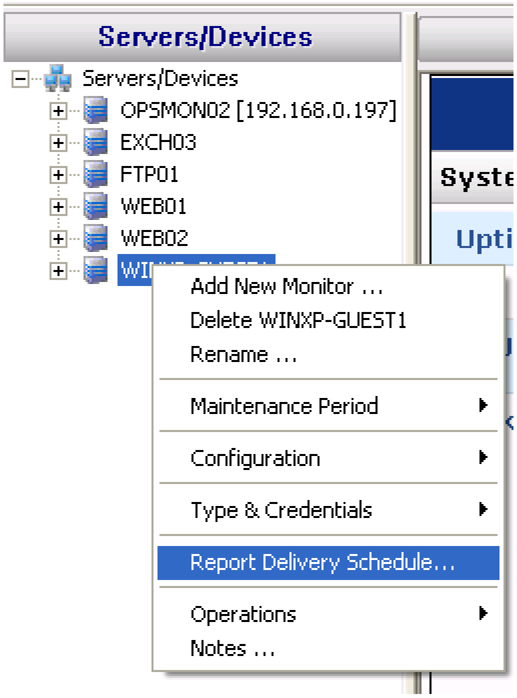
Err Ti...	Monitor	Details	OK Ti...	Ack
2 Jul 2009 5:20:31 pm	Monitor services on ARCH...	The service "Performance Logs and Alerts" is not running on computer ARCHIVE		□
2 Jul 2009 4:18:30 pm	Monitor services on ARCH...	The service "Microsoft Software Shadow Copy Provider" is not running on computer ARCHIVE The service "Performance Logs and Alerts" is not running on computer ARCHIVE The service "Volume Shadow Copy" is not running on computer ARCHIVE		□

When you scroll down past the charts, there maybe be a System Details section. The data for System Details is collected via WMI on Windows servers. If that section is missing, look at the very bottom of the report for WMI hints..

The next section is Monitor Status. All monitors on the server are shown here, along with the most recent status and the next run time for the monitor. If you want to see the Last Run Time, right-click on the monitor in the navigation panel on the left side of the application.

The Recent Errors section shows alerts that have recently been fired. On the right side is an optional columns labeled Ack, short for Acknowledge. The Ack column is part of the Error Auditing system. You can hide or show the column and make other adjustments to the Error Auditing settings by right-clicking the computer and going to Report & Delivery Settings -> Report Settings.

If you are using a Pro or Lite license, you can also schedule the status reports to be emailed to you. Simply right-click on the server and choose Report Delivery Schedule.

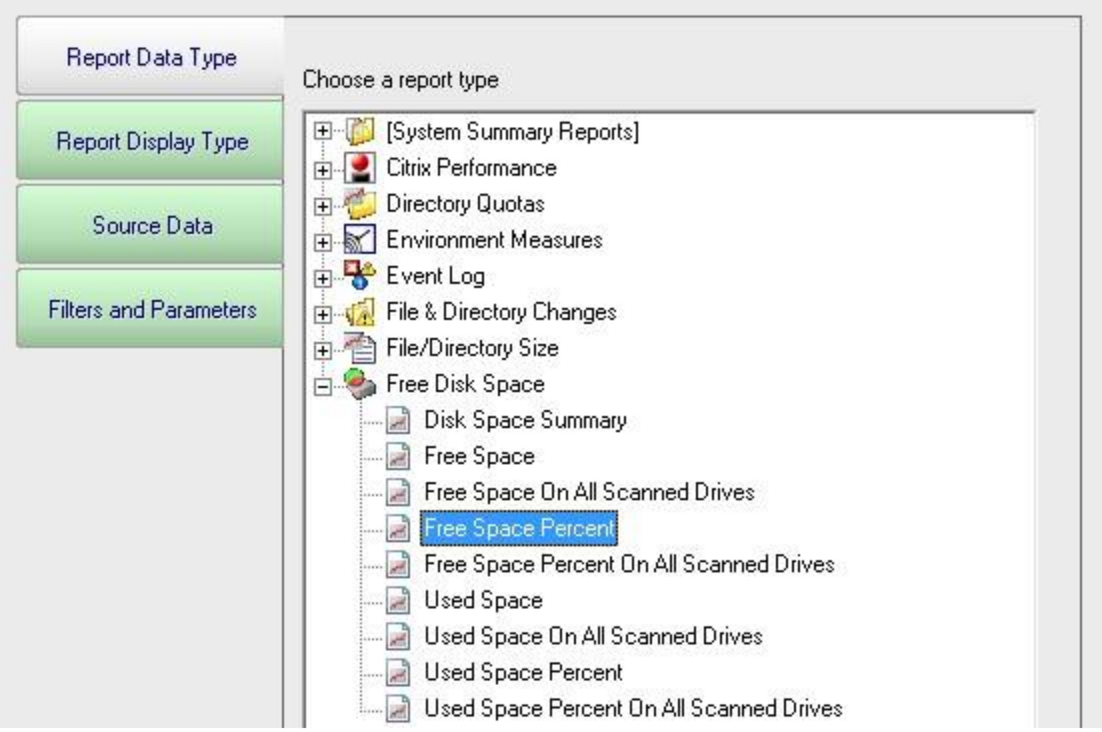

Servers/Devices
Servers/Devices
OPSMON02 [192.168.0.197]
EXCH03
FTP01
WEB01
WEB02
WI
Syste
Upti
Add New Monitor ...
Delete WINXP-GUEST1
Rename ...
Maintenance Period
Configuration
Type & Credentials
Report Delivery Schedule...
Operations
Notes ...

Contents

Ad Hoc Reports

Ad hoc reports can be generated at any time to quickly gather data on your systems. Simply click through each tab and make the selection that is presented on tha tab. Note that the reports present in your application may differ from those shown in the image below.

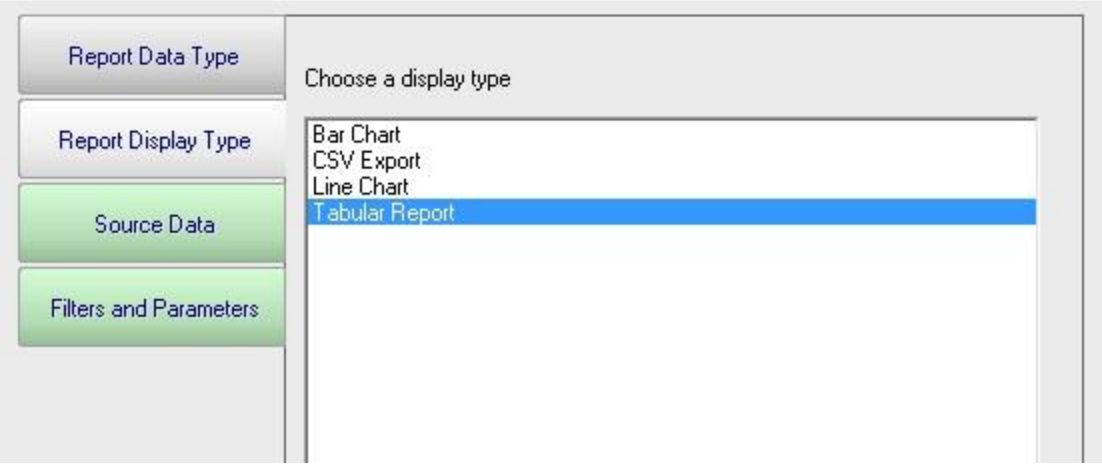
In the example below, the user is on the top Report Data Type tab. Report Types are defined by the monitors installed on the system (the monitors are what store the data, and they also create the reports). In this case, the user has selected the Free Disk Space report type, and specifically the Free Space Percent report. The remaining tabs have turned green to indicate that they still need to be visited.



Choose a report type

- [System Summary Reports]
- Citrix Performance
- Directory Quotas
- Environment Measures
- Event Log
- File & Directory Changes
- File/Directory Size
- Free Disk Space
  - Disk Space Summary
  - Free Space
  - Free Space On All Scanned Drives
  - Free Space Percent
  - Free Space Percent On All Scanned Drives
  - Used Space
  - Used Space On All Scanned Drives
  - Used Space Percent
  - Used Space Percent On All Scanned Drives

On the Report Display Type we see that this particular report can be represented as a Bar Chart, CSV Export, Line Chart or Tabular Report. The Tabular Report will display as a dynamic HTML table with sortable column headers. The CSV Export is a .csv file which can easily be imported into Excel and other applications. Some report display types won't make sense for some data types -- in that case, the display type will not be shown.



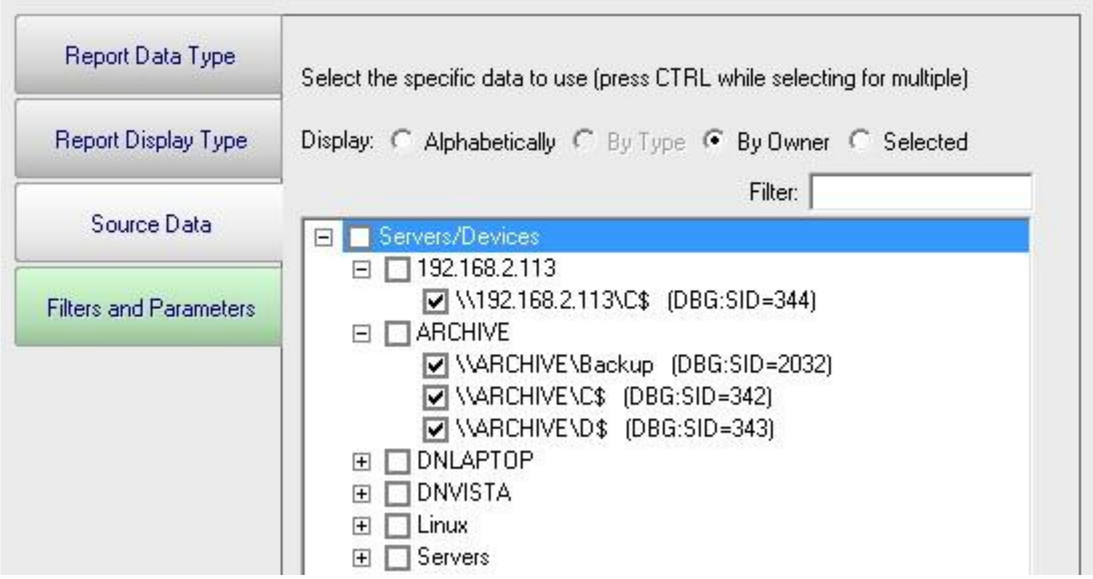
Choose a display type

Bar Chart
CSV Export
Line Chart
Tabular Report

After having selected the report type and the display format, it's time to choose which data to report on. This is done on the Source Data tab. This tab will display all of the data that is available for the chosen report type. In this case we are shown drives that can be reported on. The radio buttons at the top display the available data sets in different ways. In addition, the Filter box will filter the displayed items down to entries that contain text that you enter. This makes finding a particular data set from a very large list quick and easy.

Check the box next to the data set(s) that you want to report on. You can also place the check at a higher level in the data set tree and all data sets below it will also get checked.

NOTE: Most data sets can be deleted. Although not shown in this screenshot, there is a "Delete selected data sets" button near the bottom of this dialog. Clicking that button will delete the data for the checked data sets from the database.



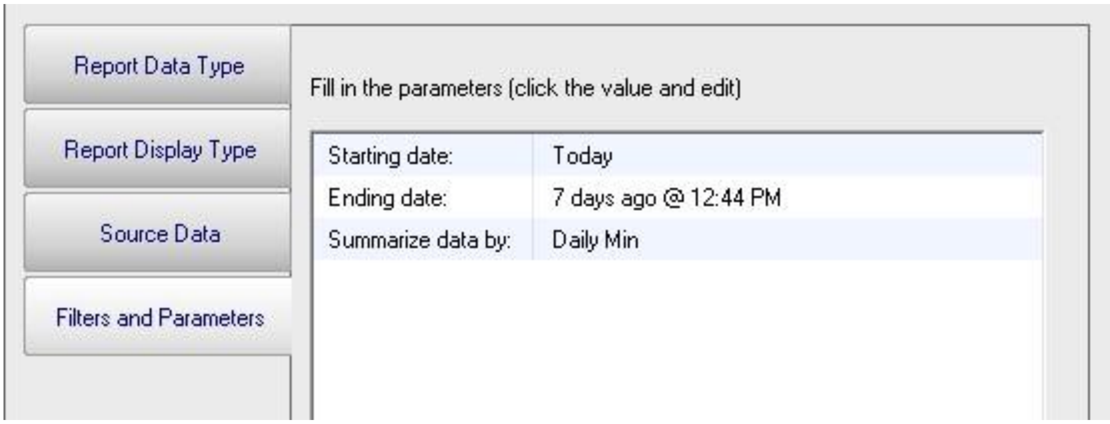
Select the specific data to use (press CTRL while selecting for multiple)

Display: ○ Alphabetically ○ By Type ● By Owner ○ Selected

Filter:

```
⊟ □ Servers/Devices
    ⊟ □ 192.168.2.113
          ☑ \\192.168.2.113\C$  (DBG:SID=344)
    ⊟ □ ARCHIVE
          ☑ \\ARCHIVE\Backup  (DBG:SID=2032)
          ☑ \\ARCHIVE\C$  (DBG:SID=342)
          ☑ \\ARCHIVE\D$  (DBG:SID=343)
    ⊞ □ DNLAPTOP
    ⊞ □ DNVISTA
    ⊞ □ Linux
    ⊞ □ Servers
```

The final tab is Filters and Parameters. The filters and parameters shown depend on which report type you are creating the report for. Most data sets have the ability to specify a time span for the report. Many report types also have summarization abilities like the example below. Summarizing allows you to take a large data set and summarize it into a smaller amount of data. That is done by taking a set of values (an hour, day, week or month's worth) and computing the minimum, maximum or average value for that period.



Fill in the parameters (click the value and edit)

Starting date:	Today
Ending date:	7 days ago @ 12:44 PM
Summarize data by:	Daily Min

When you press the Generate Report button you will be taken to a "Report Generation in Progress" page, and then automatically forwarded to the finished report.

Since the reports are HTML pages, you can open a report in a regular browser, print the report, generate a PDF, etc.

Report Troubleshooting

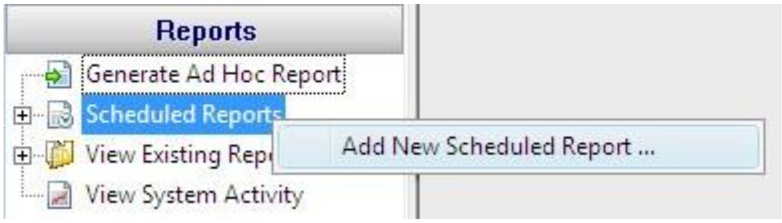
If a report doesn't show the data that you expect, check the following:

- Check the time frame the report is using (bottom tab in the graphic above). Often the time frame excludes available data.
- Consider when the report is run and when data collection happens. If you run a report at 1am, but the monitor first collects data at 2am, a report for Today won't have anything to display.

Contents

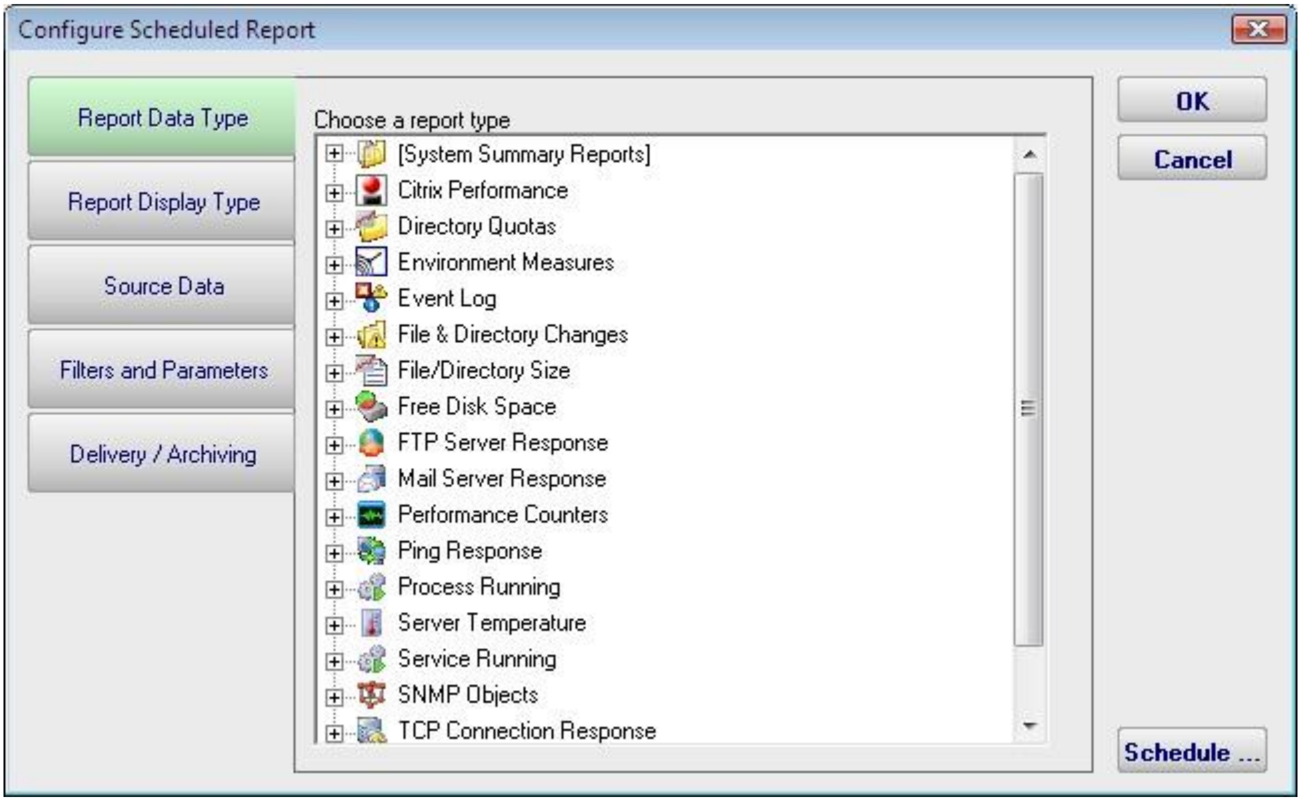
Scheduled Reports

Scheduling the automatic generation of reports is similar to creating ad hoc reports. To create a Scheduled Report, go to Reports and right-click on the Scheduled Reports item.



Creating a new Scheduled Report or editing an existing one will show the dialog below. (Note: The displayed Report Types may be different depending on which product you are using)

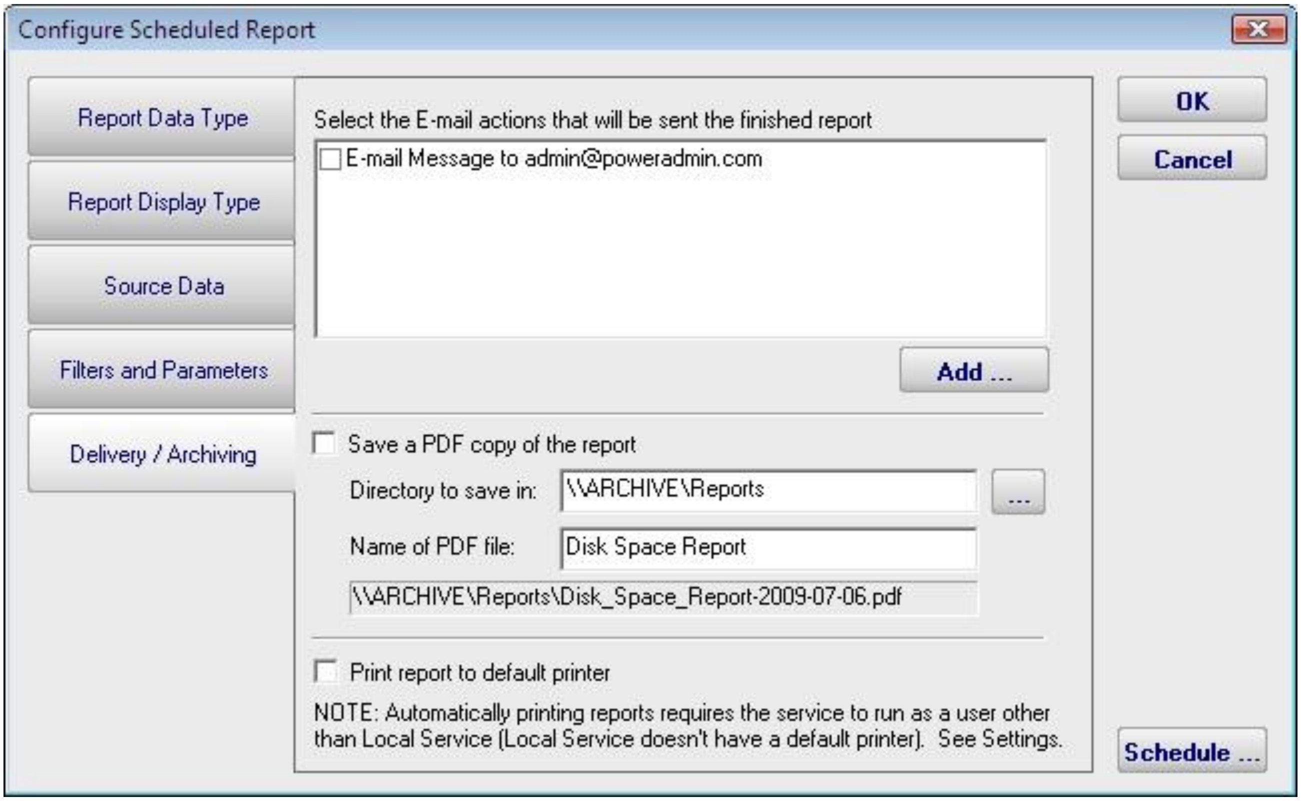
Just like with ad-hoc reports, you choose a monitor-type that sourced the data you want to report on, a report type (chart, tabular, CSV). You also choose a specific dataset to report on. Near the bottom of the dialog you specify reporting parameters that are unique to that report. More detail is given in the Ad Hoc Reports section which is exactly the same. In fact the only difference between the two is fifth Delivery/Archiving tab, and the Schedule button.



The new Delivery / Archiving tab lets you specify whether to email the report when it has run. The report email will contain a PDF as well as an image of the report (raw HTML isn't sent because of varying support in email clients).

You can also specify that a PDF copy of the report get saved in a location that you specify. If specifying a remote path, use UNC paths since mapped drives often aren't available to services. When the report is archived, a unique name containing the date and time will be created if there is already a report with the same name.

At the bottom of the report you'll see the familiar Schedule button. It works the same way as the Schedule buttons in the monitors. You can easily specify how often the report is run.



Configure Scheduled Report

Select the E-mail actions that will be sent the finished report

□ E-mail Message to admin@poweradmin.com

□ Save a PDF copy of the report

Directory to save in: \\ARCHIVE\Reports

Name of PDF file: Disk Space Report

\\ARCHIVE\Reports\Disk_Space_Report-2009-07-06.pdf

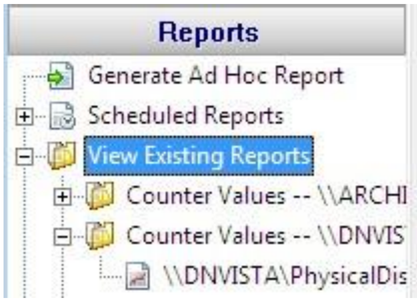
□ Print report to default printer

NOTE: Automatically printing reports requires the service to run as a user other than Local Service (Local Service doesn't have a default printer). See Settings.

Scheduled reports always write to the same location on disk, so the URL to the report is always the same, and viewing the report in the browser will show the latest generated version of that report. This makes it easy to save the URL in your browser's Favorites list.

Reports that have already run are available in two locations:

- In the Console. Click the Reports button on the right side of the navigation pane. Expand the View Existing Reports node to see all report types. Expand a report type to see existing reports of that type.



- The top right of every report contains a button labeled All Reports. This button will take you to a table of contents page showing all available reports.

Report Troubleshooting

If a report doesn't show the data that you expect, check the following:

- Check the time frame the report is using ("Filters and Parameters" tab in the graphic above). Often the time frame excludes available data.
- Consider when the report is run and when data collection happens. If you run a report at 1am, but the monitor first collects data at 2am, a report for Today won't have anything to display.
- Double-check the Filter and Parameters tab for other settings. Some times the parameters end up excluding data that you want.

Contents

Using Alternate Web Servers to Publish Reports

NOTE: The following still works as described, but should not be needed with version 3.6 and newer since the file references within the reports are all relative

By default, the links within the reports will be in the form http://<server>:<port>/... where

- server - the name of the server where the monitoring service is installed
- port - the HTTP port specified in Settings
- the root directory in the URL is the Reporting directory as specified in Settings

If you wish to have the reports available via a different means (perhaps you want to publish them on your intranet), you can configure them to use a different root URL that will work with your other web server, be it IIS, Apache or otherwise.

To use a different root URL, follow the steps below:

- Either go to Settings and point the Reporting directory to a different place, or point your WWW server at the Reporting directory. For example, with IIS you would create a Virtual Directory (named ServerReports for example) that points at C:\Program Files\PA Server Monitor\Reports
- Go to the main registry key for the product:

  For PA File Sight: HKEY_LOCAL_MACHINE\Software\PAFileSight
  For PA Server Monitor: HKEY_LOCAL_MACHINE\Software\PowerAdminServerMonitor
  For PA Storage Monitor: HKEY_LOCAL_MACHINE\Software\PAStorageMonitor

  and add a String value named:

  HTTP_URL_OVERRIDE

  IMPORTANT: Make SURE there are no spaces in the name of that value

  The value that you place there will replace the "http://<server>:<port>/" root that is used on internal report URLs.

  For instance, if you created the Virtual Directory above, you would set the value to HTTP_URL_OVERRIDE = "http://web_server_name/ServerReports/"

Contents

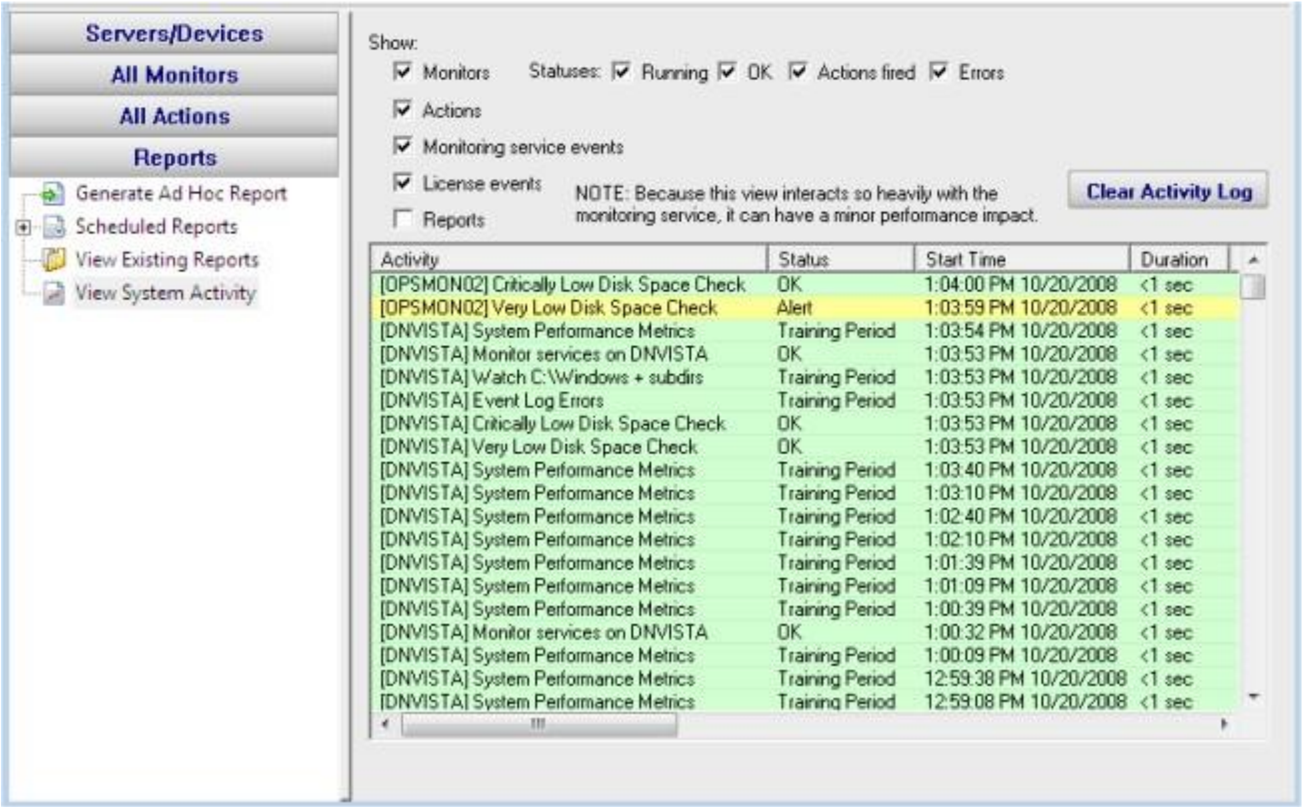
Viewing System Activity

The View System Activity item is the place to go if you ever want to see what the monitoring service is currently working on. You can choose to show or hide the following activity types:

- Monitors, with the ability to filter on monitor state (running, completed OK, fired actions, or internal error)
- Actions that have been fired
- Monitoring service start and stop events
- License events (new licenses found, license mode being used, etc)
- Reports generated (automatic or ad hoc)

When you view the running system, you'll notice that running monitors have a start time, but no duration since it hasn't finished yet.

The activity log is purely for your information and can be cleared at any time. When it grows to a length of 5000 items it begins to automatically remove the oldest items.



Show:

☑ Monitors Statuses: ☑ Running ☑ OK ☑ Actions fired ☑ Errors

☑ Actions

☑ Monitoring service events

☑ License events

□ Reports

NOTE: Because this view interacts so heavily with the monitoring service, it can have a minor performance impact.

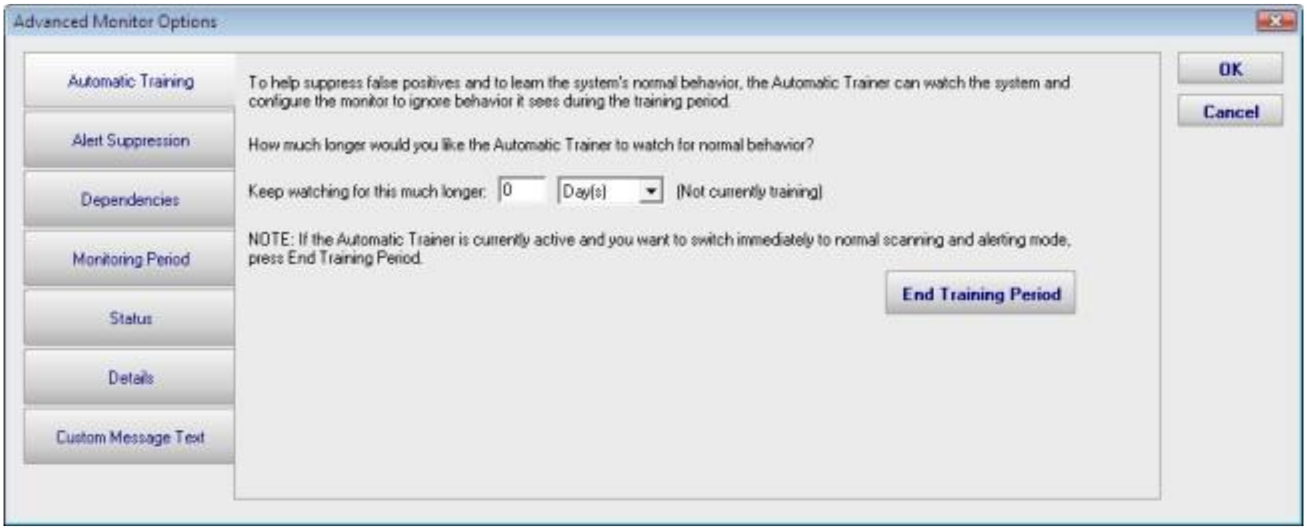
Activity	Status	Start Time	Duration
[OPSMON02] Critically Low Disk Space Check	OK	1:04:00 PM 10/20/2008	<1 sec
[OPSMON02] Very Low Disk Space Check	Alert	1:03:59 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:03:54 PM 10/20/2008	<1 sec
[DNVISTA] Monitor services on DNVISTA	OK	1:03:53 PM 10/20/2008	<1 sec
[DNVISTA] Watch C:\Windows + subdirs	Training Period	1:03:53 PM 10/20/2008	<1 sec
[DNVISTA] Event Log Errors	Training Period	1:03:53 PM 10/20/2008	<1 sec
[DNVISTA] Critically Low Disk Space Check	OK	1:03:53 PM 10/20/2008	<1 sec
[DNVISTA] Very Low Disk Space Check	OK	1:03:53 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:03:40 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:03:10 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:02:40 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:02:10 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:01:39 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:01:09 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:00:39 PM 10/20/2008	<1 sec
[DNVISTA] Monitor services on DNVISTA	OK	1:00:32 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:00:09 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	12:59:38 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	12:59:08 PM 10/20/2008	<1 sec

Additional Help Documents

Contents

Advanced Monitor Options

All monitors have an Advanced Monitor Options button on their right side. When you press that button you'll see the dialog below. This dialog is shown for a monitor that supports all advanced options. Others might not have all tabs when a particular feature is not relevant to that monitor.



To help suppress false positives and to learn the system's normal behavior, the Automatic Trainer can watch the system and configure the monitor to ignore behavior it sees during the training period.

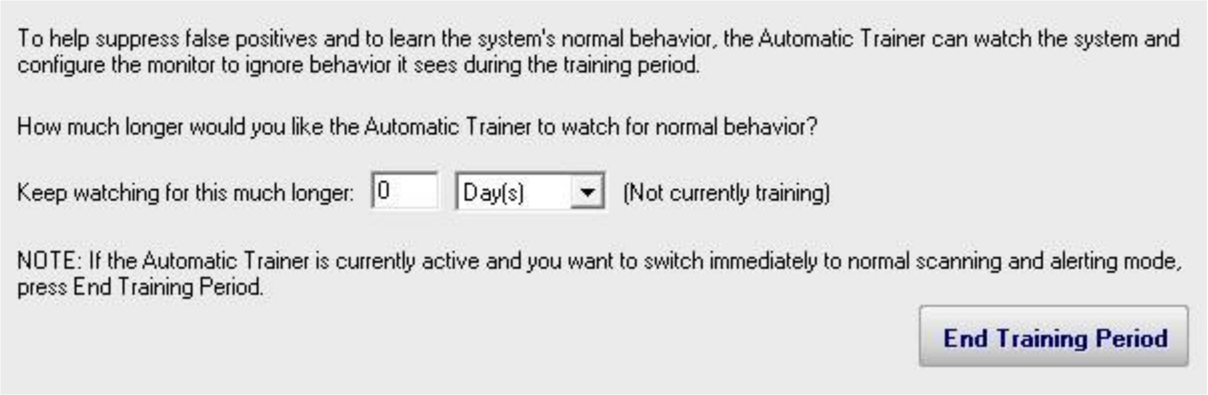
How much longer would you like the Automatic Trainer to watch for normal behavior?

Keep watching for this much longer: 0 Day(s) (Not currently training)

NOTE: If the Automatic Trainer is currently active and you want to switch immediately to normal scanning and alerting mode, press End Training Period.

Each of the different option tabs is discussed below.

Automatic Training



To help suppress false positives and to learn the system's normal behavior, the Automatic Trainer can watch the system and configure the monitor to ignore behavior it sees during the training period.

How much longer would you like the Automatic Trainer to watch for normal behavior?

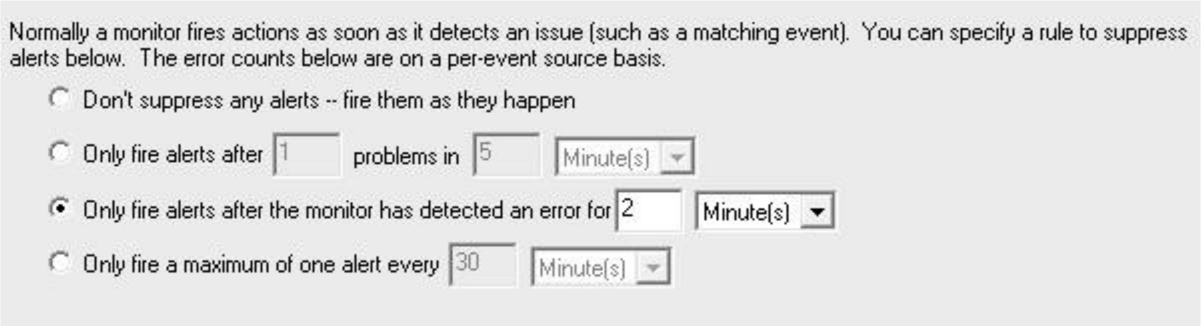
Keep watching for this much longer: 0 Day(s) (Not currently training)

NOTE: If the Automatic Trainer is currently active and you want to switch immediately to normal scanning and alerting mode, press End Training Period.

PA File Sight can have a monitor train itself. What that means is it will monitor like normal during the training period, but not fire any alerts. Anytime something 'abnormal' (or outside the normal thresholds) is seen, the thresholds are adjusted such that it won't alert on that activity if it is seen again.

At the end of the training period, the monitor will automatically switch back to normal monitoring mode. If you want to force it to switch back immediately, press the End Training Period button.

Alert Suppression



Normally a monitor fires actions as soon as it detects an issue (such as a matching event). You can specify a rule to suppress alerts below. The error counts below are on a per-event source basis.

○ Don't suppress any alerts -- fire them as they happen

○ Only fire alerts after 1 problems in 5 Minute(s)

● Only fire alerts after the monitor has detected an error for 2 Minute(s)

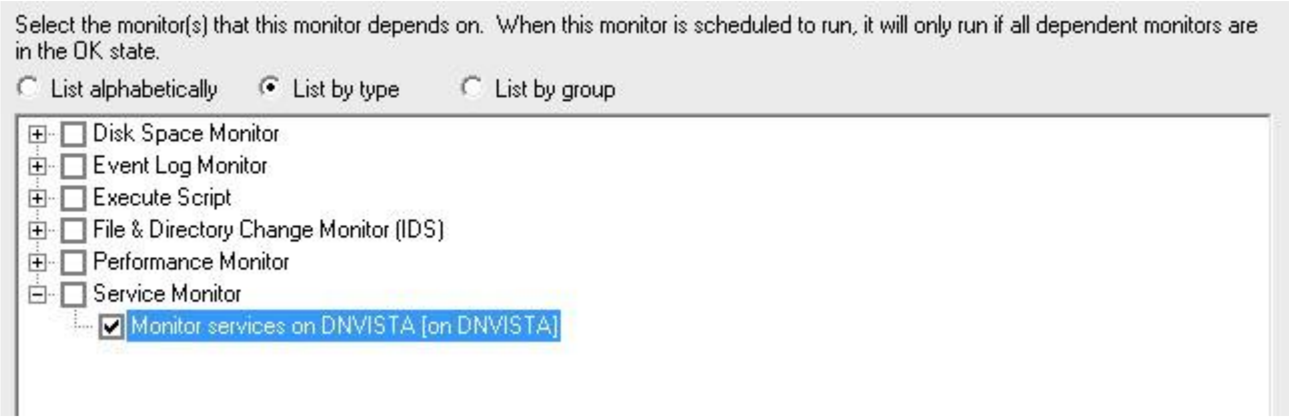
○ Only fire a maximum of one alert every 30 Minute(s)

With the Alert Suppression settings, you can instruct the monitor how often and how soon you want to be alerted about a specific issue. This lets enables the monitor to skip the first few failures on a specific device if you wish and only warn after an error has happened a few times or for a particular amount of time.

Alert Suppression settings can be set on many monitors at once using Bulk Config, as can the other advanced options.

Dependencies

Monitors can be dependent on other monitors. That means when the monitor you are currently editing is supposed to run, it will first check its dependent monitors. They need to all be in the OK state for the current monitor to run. This is useful for suppressing errors. For example, the monitor that checks disk space on a remote server might be dependent on a Ping monitor that is making sure connectivity to the server is possible.

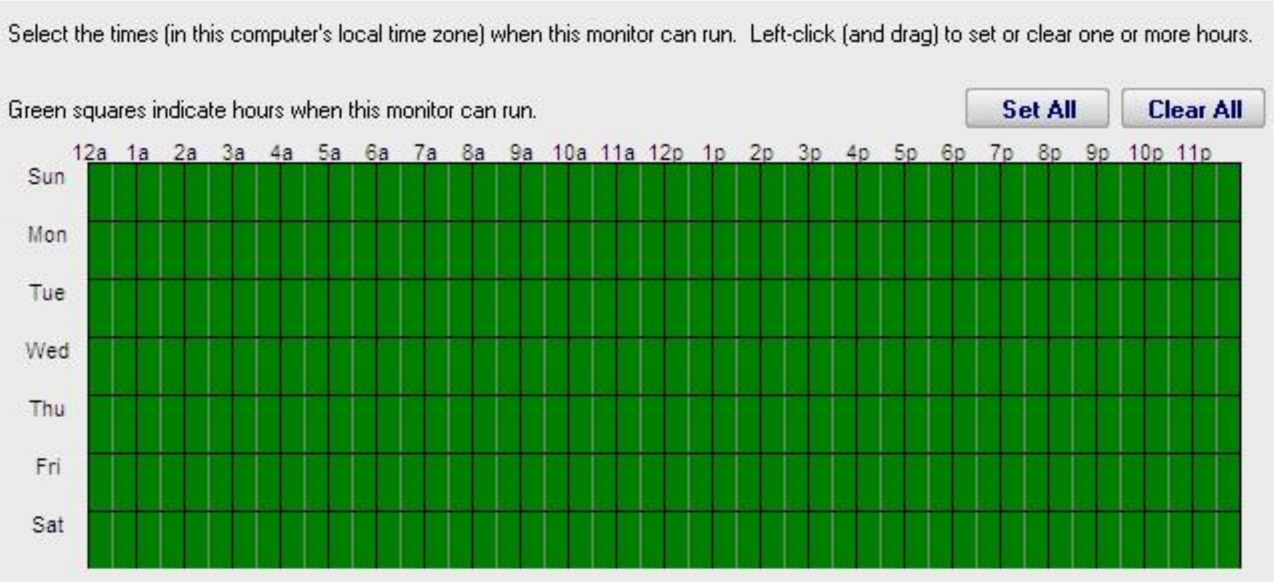


Select the monitor(s) that this monitor depends on. When this monitor is scheduled to run, it will only run if all dependent monitors are in the OK state.

○ List alphabetically ● List by type ○ List by group

- ⊞ □ Disk Space Monitor
- ⊞ □ Event Log Monitor
- ⊞ □ Execute Script
- ⊞ □ File & Directory Change Monitor (IDS)
- ⊞ □ Performance Monitor
- ⊟ □ Service Monitor
  - ☑ Monitor services on DNVISTA [on DNVISTA]

Monitoring Period



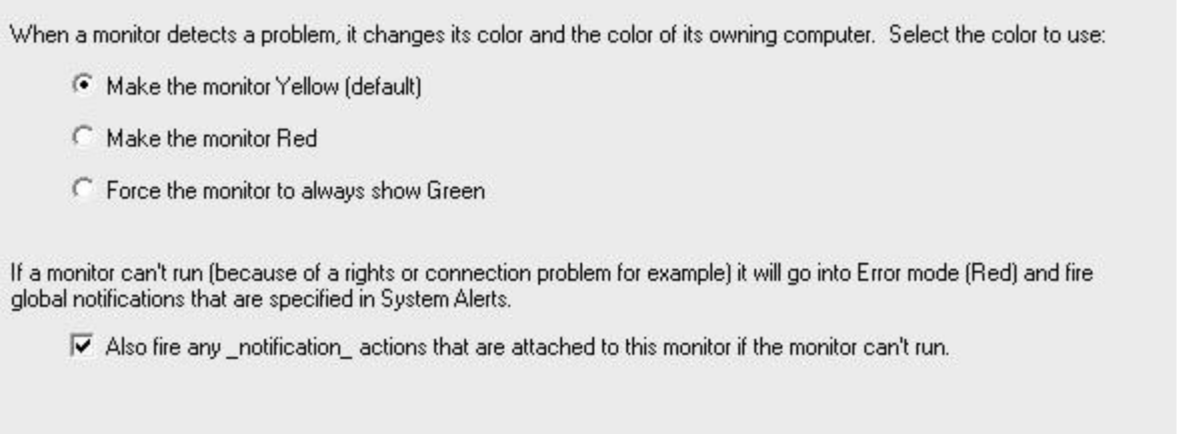
Select the times (in this computer's local time zone) when this monitor can run. Left-click (and drag) to set or clear one or more hours.

Green squares indicate hours when this monitor can run.

	12a	1a	2a	3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p
Sun	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Mon	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Tue	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Wed	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Thu	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Fri	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Sat	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Most monitors run all day, every day, on the specified schedule. Some times though you might have a need for a monitor to not during a certain time. If you don't want any monitors to run at a certain time, put the server in maintenance mode. But sometimes that isn't granular enough -- you just want a single monitor to not running during a specific period of time. That is where the Monitoring Period option is useful.

Status



When a monitor detects a problem, it changes its color and the color of its owning computer. Select the color to use:

● Make the monitor Yellow (default)

○ Make the monitor Red

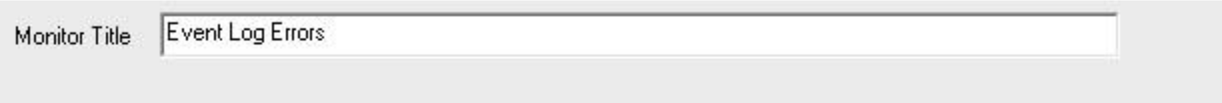
○ Force the monitor to always show Green

If a monitor can't run (because of a rights or connection problem for example) it will go into Error mode (Red) and fire global notifications that are specified in System Alerts.

☑ Also fire any _notification_ actions that are attached to this monitor if the monitor can't run.

The Status panel lets you configure how some monitors appear when they are in an alert state. Sometimes a monitor is not important (informational only) and it going into alert mode should not make the server status and group status turn Yellow. The Status panel lets you override those behaviors.

Details

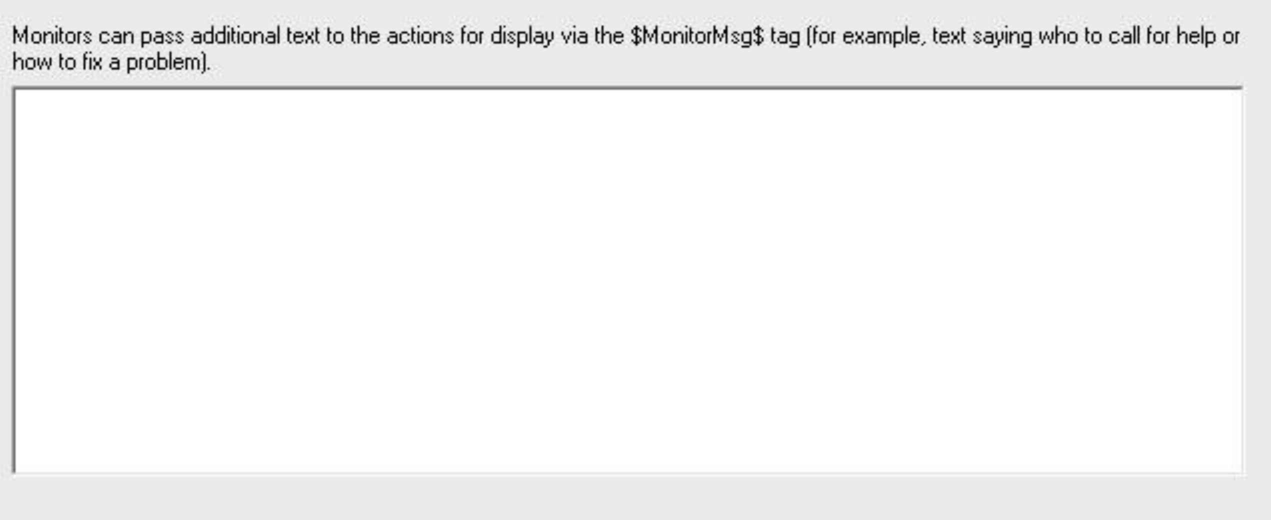


Monitor Title: Event Log Errors

This panel lets you set the monitor's name as it is displayed through the system. If you want to go back to the default name that was generated, just delete the name text completely.

Custom Message Text

Many of the actions (E-mail, Pager, Message Box, etc) let you customize the message that is sent out when actions are fired. You customize the message by using pre-defined variables. One of the variables is $MonitorMsg$. This is a value that can be defined on a per-monitor basis. Some uses would include a hint to the receiver about how to fix the error, or directions to call various support phone numbers.



Monitors can pass additional text to the actions for display via the $MonitorMsg$ tag (for example, text saying who to call for help or how to fix a problem).

Contents

Event Escalation

NOTE: Event Escalation is only available in the Pro edition.

State monitors (like the one shown below) support **event escalation**. This means that after a specified amount of time, additional actions will be run if the monitor is still in an error state.

When you attach the first action to an escalation item, a new escalation item will be added below the current escalation item, which you are free to use or ignore (that is, leave empty). The delay time that is preset for this action is automatically guessed -- you are free to change it.

You may configure a particular escalation group by first clicking on the Escalation node to select it. This configuration may consist of changing the time at which the escalation group's actions are activated. You can configure an escalation period by hand editing the time shown in it. To do so, press the F2 key or click on the node a second time after selecting it, to "open" the node for renaming (exactly as you would with a file or folder name in Windows Explorer.) You can then enter a time value, which consists of a whole decimal number (no decimal point) followed by one of these time units: minutes, hours, or days. You do not need to type the "after the first error" portion.

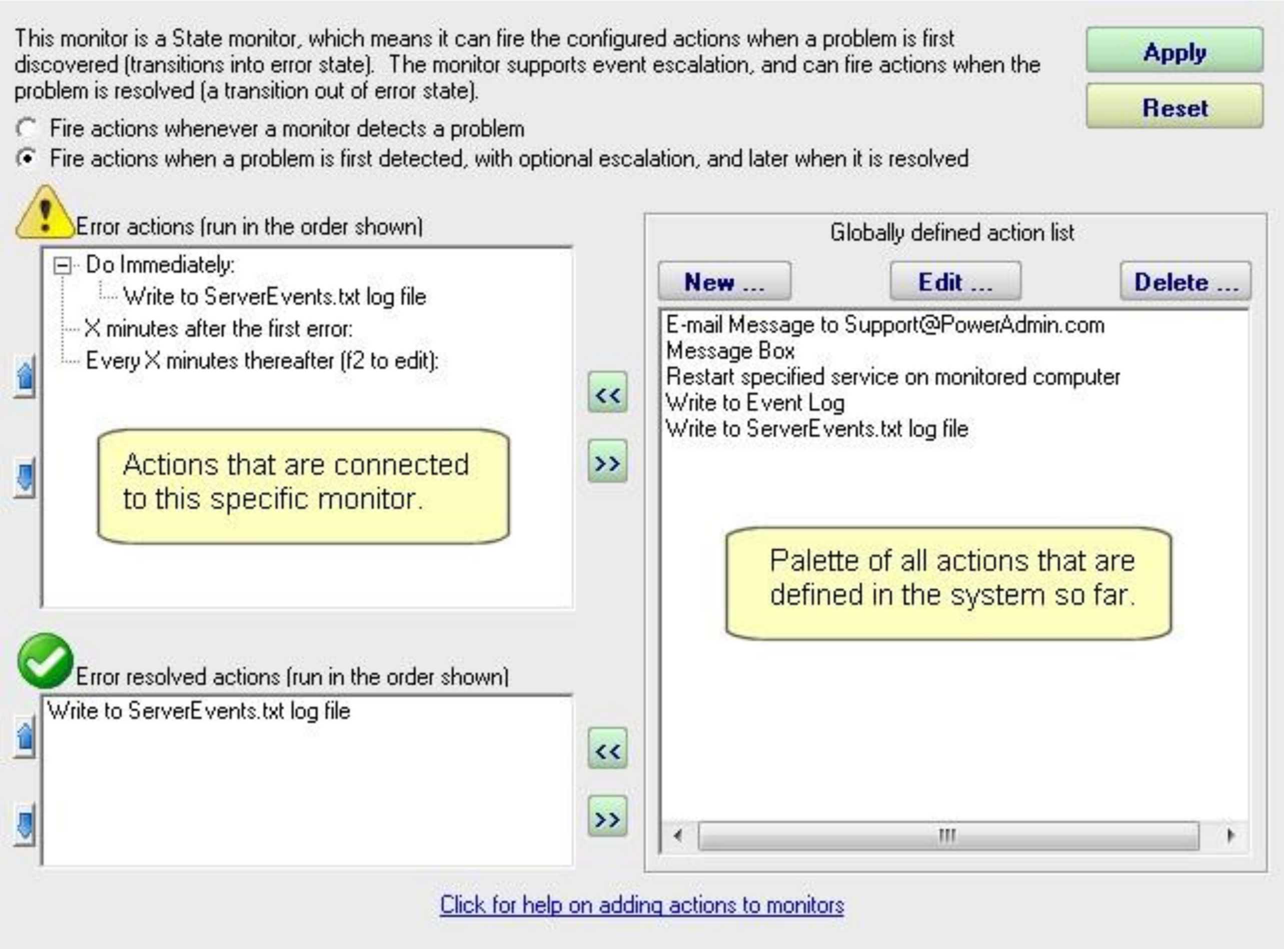
Examples of correct escalation time setting text:

- 12 minutes
- 2 hours
- 1 day

PA File Sight will always revise the text to read "XX minutes after the first error:" once you close the editing of the node. A non-minutes value will be normalized to the correct number of minutes (for instance, "1 hour" becomes "60 minutes after the first error.") The escalation groups will be visually re-sorted in the order of the times that they contain when you complete your editing.

Any escalation groups that are created, but left empty, will automatically be removed when you leave the Actions dialog.

See Adding Actions for additional information.



This monitor is a State monitor, which means it can fire the configured actions when a problem is first discovered (transitions into error state). The monitor supports event escalation, and can fire actions when the problem is resolved (a transition out of error state).

○ Fire actions whenever a monitor detects a problem

● Fire actions when a problem is first detected, with optional escalation, and later when it is resolved

Error actions (run in the order shown)

- Do Immediately:
  - Write to ServerEvents.txt log file
- X minutes after the first error:
- Every X minutes thereafter (f2 to edit):

Actions that are connected to this specific monitor.

Error resolved actions (run in the order shown)

Write to ServerEvents.txt log file

Globally defined action list

E-mail Message to Support@PowerAdmin.com
Message Box
Restart specified service on monitored computer
Write to Event Log
Write to ServerEvents.txt log file

Palette of all actions that are defined in the system so far.

Click for help on adding actions to monitors

Contents

File Sight - Alternate Data Streams

Alternate Data Streams are a feature of Microsoft's NTFS file system. Basically they are files within a file, with specially formatted information at the end of the file name to indicate which 'file' within the file is being specified. Some applications (including the operating system) uses these data streams, and some do not.

You can read more about them at:

- File Streams (Microsoft.com)
- Streams utility (Microsoft.com)
- Google Search

Data streams often look like the following example:

C:\Documents\Financial Data\Payroll.xls:38FJLK2KA81FJLA:$DATA

The data that is saved in a data stream is completely dependent on the operating system and/or the application. Sometimes it it meta data (such as author information), sometimes it might be tracking data, etc. The data in the streams may or may not be visible to the end user (meaning they might not know the alternate stream data is being changed by what they are doing).

PA File Sight sees these file streams being accessed just like any other normal file. For your alerting and reporting purposes PA File Sight lets you specify how you want to treat file stream data. The options are:

- Show stream access - This is the default, so for the example above you could see accesses happening to the shown stream as well as separate actions on the base Payroll.xls file
- Truncate stream - Instead of showing the complete file stream name in the example above, PA File Sight can truncate the name to the base file (C:\Documents\Financial Data\Payroll.xls in the example)
- Ignored streams - When a file stream is detected, it is completely ignored

Contents

File Sight - Interpreting Application Behavior

Many applications that work with documents (word processors, spreadsheet programs, graphic programs, etc) open your document and then work with it in a temporary file. For example, imagine you have the following file:

C:\Docs\My Story.doc

When you open the file, your word processor will often create the following file to track your edits:

C:\Docs\~My Story.tmp

When you are finished editing the document, the temporary file has all of your changes. In order to minimize data loss and be as safe as possible, many programs will do the following:

WRITE to C:\Docs\~My Story.tmp *(to save all of your edits)*
DELETE C:\Docs\My Story.doc
RENAME C:\Docs\~My Story.tmp to C:\Docs\My Story.doc

PA File Sight sees all of this activity and reports it. You might be concerned to receive alerts about files being deleted since people should only be editing, not deleting important documents. However, as shown above, the file really was deleted.

In order tell you what is really happening, PA File Sight will try to interpret the stream of activity above. It will match the DELETE and RENAME and turn it into a write event for alerting and reporting purposes.

So, if PA File Sight sees:

WRITE to C:\Docs\~My Story.tmp
DELETE C:\Docs\My Story.doc
RENAME C:\Docs\~My Story.tmp to C:\Docs\My Story.doc

it will turn it into

WRITE C:\Docs\My Story.doc

This will help you understand what is really happening as far as the end users are concerned.

Caveats:

- Doing the above processing requires extra memory--more events have to be held in memory now so they can be compared. (For example, all DELETEs have to be held in case a RENAME comes along a short while later).
- Some additional CPU processing power is also required to search through and match up related events.
- Alerting is delayed a few seconds (a DELETE alert should not be sent if it will ultimately get turned into a WRITE).
- Several saves within a few (5 - 10) seconds will not always be interpretted correctly, so some of the underlying RENAME and DELETE operations may show through.

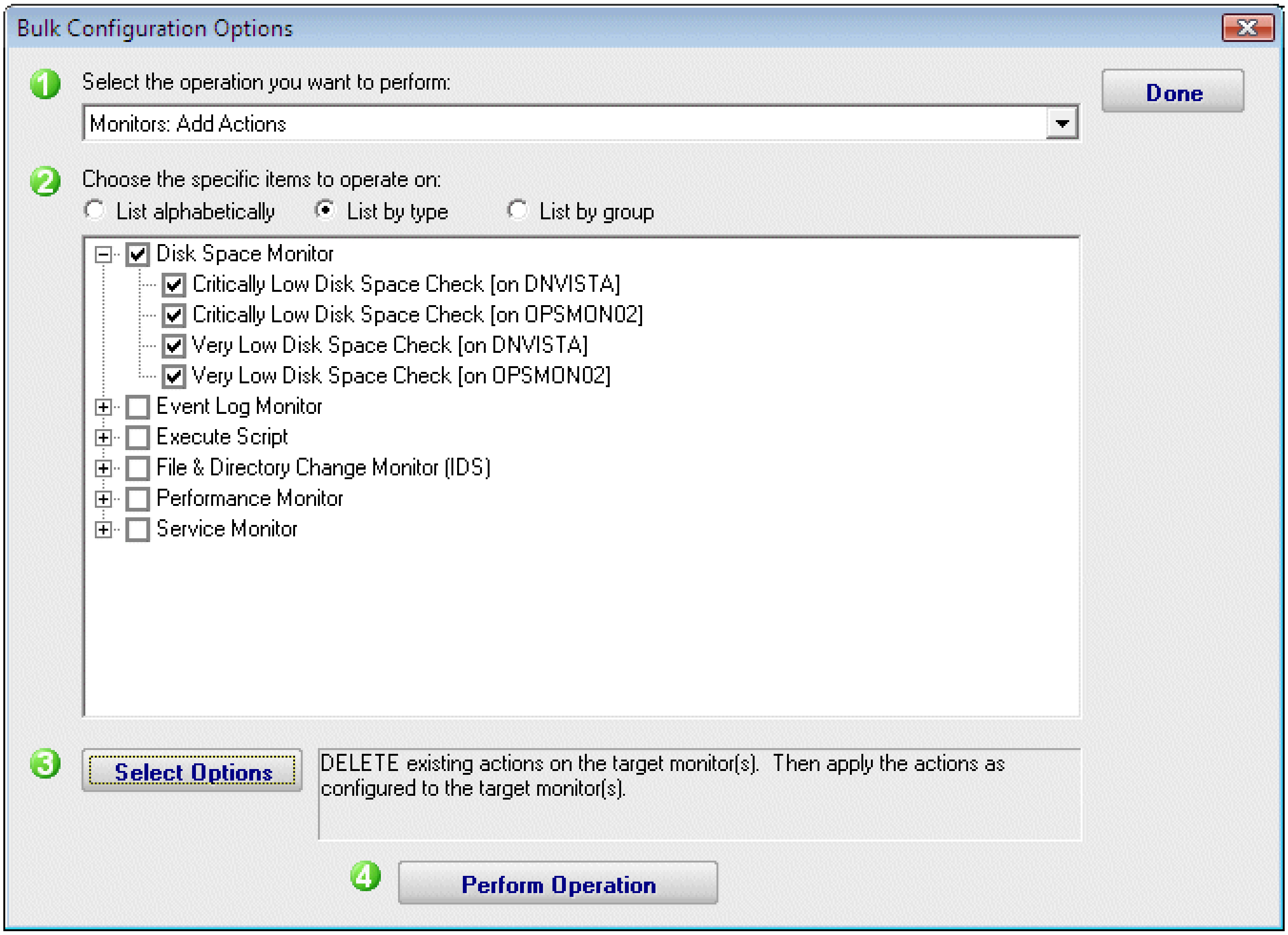
Contents

Bulk Configuration

The Bulk Configuration feature of PA File Sight will help you quickly configure large numbers of monitors, computers, actions, etc.

The Bulk Configuration dialog consists of two main areas:

- Operation: A drop-down control that lets you choose what type of operation to perform, and the types of objects it will be performed on.
- Target Objects: A list of objects that the operation will be performed on. You can use the radio buttons to choose different ways of grouping the objects to make object selection easier.



1 Select the operation you want to perform:
Monitors: Add Actions

2 Choose the specific items to operate on:
○ List alphabetically ● List by type ○ List by group

☑ Disk Space Monitor
- ☑ Critically Low Disk Space Check [on DNVISTA]
- ☑ Critically Low Disk Space Check [on OPSMON02]
- ☑ Very Low Disk Space Check [on DNVISTA]
- ☑ Very Low Disk Space Check [on OPSMON02]

☐ Event Log Monitor
☐ Execute Script
☐ File & Directory Change Monitor (IDS)
☐ Performance Monitor
☐ Service Monitor

3 DELETE existing actions on the target monitor(s). Then apply the actions as configured to the target monitor(s).

4

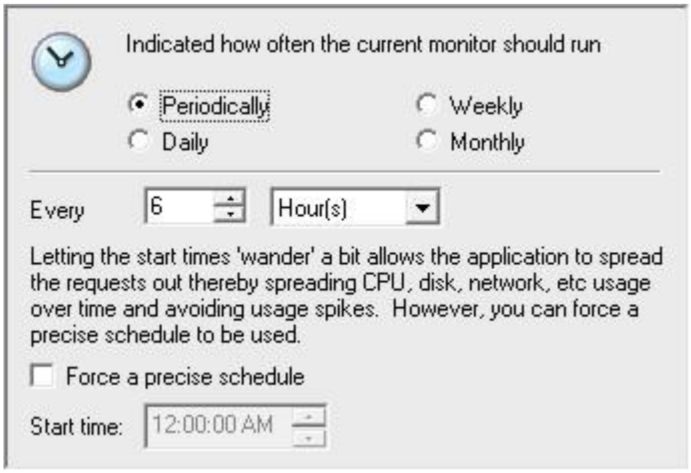
Once you've chosen the operation, and checked the boxes next to the objects that you want to operate on, press the Select Options button. This lets you specify details for the operation to be performed. When you're done, the text box next to the Select Options button will display a summary of what will happen.

After reviewing the summary of the operation to be performed, press the Perform Operation button. This will send your configuration request to the service for processing. Most operations are handled very quickly, but a few could take a minute or so. When the operation completes you will be shown a success message, or an error message with a reason for the failure.

NOTE: The Bulk Configuration option only works when the Console and the monitoring service are both running -- it doesn't work if the service has not been started.

Monitor Schedule

Most monitors have a Schedule button in the lower right corner of their configuration dialog. When your mouse hovers over the Schedule button, the Schedule window is shown below:



Indicated how often the current monitor should run

● Periodically ○ Weekly
○ Daily ○ Monthly

Every 6 Hour(s)

Letting the start times 'wander' a bit allows the application to spread the requests out thereby spreading CPU, disk, network, etc usage over time and avoiding usage spikes. However, you can force a precise schedule to be used.

□ Force a precise schedule

Start time: 12:00:00 AM

You can schedule the monitor to run using a time-based period, on a daily, weekly or monthly schedule.

Enable WMI (Windows Management Instrumentation)

WMI comes installed on all of Microsoft's modern operating systems (Windows 2000, Windows XP, Windows 2003, Windows Vista and Windows 2008[1]). What this page will describe (and the reason you were directed here from the server status view) is how to enable *remote access* to WMI. The following steps should only take a minute or two of your time.

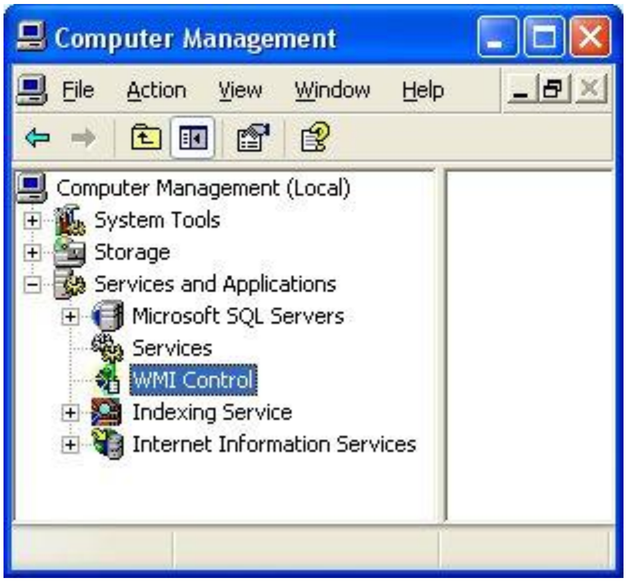
1. Enable remote WMI requests

This setting is usually all that needs to be changed to get WMI working. (Steps 2 and 3 are typically not needed, but they might be in some circumstances)

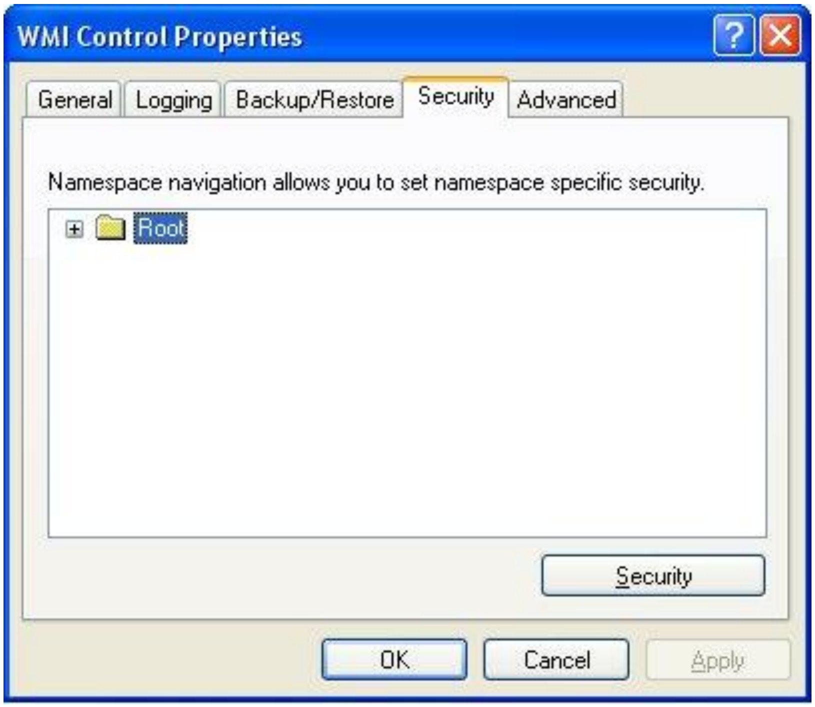
1. On the target server, go to Administrative Tools -> Computer Management.

2. Expand 'Services and Applications'

3. Right click for Properties on 'WMI Control'.

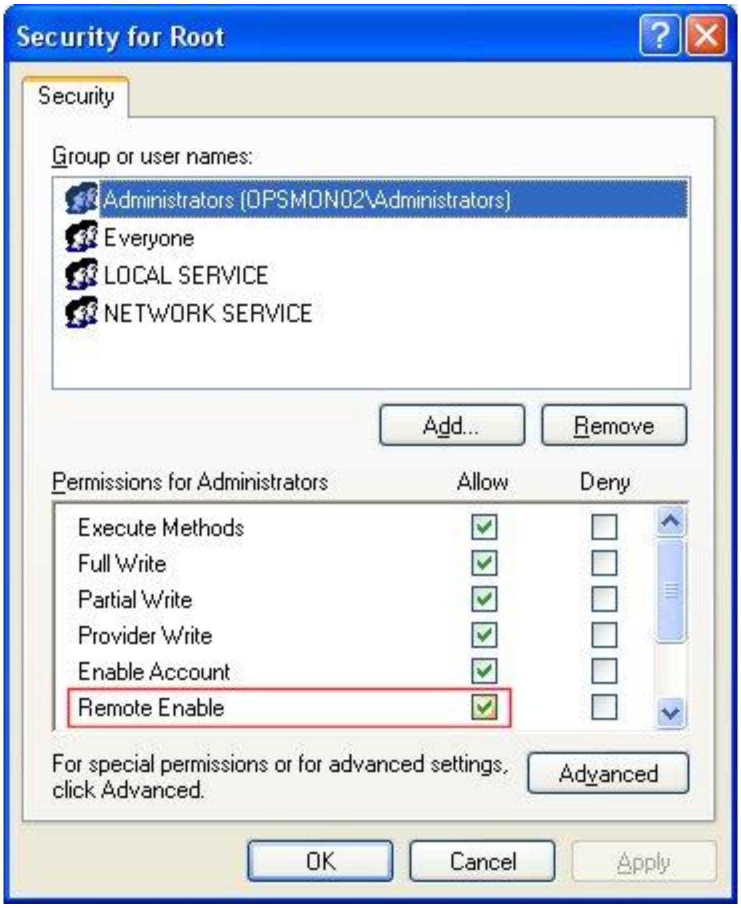


4. Select the Security tab
5. Press the Security button



Namespace navigation allows you to set namespace specific security.

6. Add the monitoring user (if needed), and then be sure to check Remote Enable for the user/group that will be requesting WMI data.



Group or user names:

- Administrators (OPSMON02\Administrators)
- Everyone
- LOCAL SERVICE
- NETWORK SERVICE

Permissions for Administrators	Allow	Deny
Execute Methods	☑	□
Full Write	☑	□
Partial Write	☑	□
Provider Write	☑	□
Enable Account	☑	□
Remote Enable	☑	□

For special permissions or for advanced settings, click Advanced.

At this point go back and see if this fixes the problem. It might take a couple of minutes for the reports to re-generate.

2. Allow WMI through Windows firewall

All users (including non-administrators) are able to query/read WMI data on the local computer.

For reading WMI data on a remote server, a connection needs to be made from your management computer (where our monitoring software is installed) to the server that you're monitoring (the target server). If the target server is running Windows Firewall (aka Internet Connection Firewall) like what is shipped with Windows XP and Windows 2003, then you need to tell it to let remote WMI requests through[2]. This can only be done at the command prompt. Run the following on the target computer if it is running a Windows firewall:

```
netsh firewall set service RemoteAdmin enable
```

3. Enable DCOM calls on the remote machine

If the account you are using to monitor the target server is NOT an administrator on the target server, you need to enable the non-administrator to interact with DCOM by following the simple steps listed here. Follow the steps for:

- To grant DCOM remote launch and activation permissions for a user or group
- To grant DCOM remote access permissions

Further Investigation

If the above steps didn't help, we recommend installing the WMI Administrative Tools from Microsoft. This includes a WMI browser that will let you connect to a remote machine and browse through the WMI information. That will help to isolate any connectivity/rights issues in a more direct and simple environment. Once the WMI browser can access a remote machine, our products should be able to as well.

WMI Administrative Tools:
http://www.microsoft.com/downloads/details.aspx?FamilyId=6430F853-1120-48DB-8CC5-F2ABDC3ED314&displaylang=en

References

[1] See http://www.microsoft.com/technet/scriptcenter/resources/wmifaq.mspx#ENAA

[2] See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/connecting_through_windows_firewall.asp -- "To Configure Connection 1". Our software doesn't use or need Connection 2.

Setting Up SMS Alert Messages

One of our most popular features is the ability to alert you when something isn't quite right. Many users want those alerts to go to their mobile phones via SMS message. There are three ways to accomplish this:

Send SMS Text Message (SMPP) Action

This action sends SMS messages from a monitoring program to a mobile phone via an SMPP gateway server on the Internet. Typically your mobile phone provider will have an SMPP gateway and will give you the parameters to fill in for this action. You can also contract with some 3rd party companies to let you use their gateways. However, there is often an easier way to get SMS messages to your cell phone:

SMTP Email Message Action

Many mobile phone providers provide an SMTP gateway for sending messages directly to a mobile phone.

For example:
T-Mobile supports sending an email message to <phonenumber>@TMoMail.com
Sprint supports sending email messages to <phonenumber>@messaging.sprintpcs.com

The messages get forwarded straight to the phone. Check with your phone provider to see if they provide this service, or check this Wikipedia article which lists many SMS-email gateways at the bottom of the page.

Phone Dialer (DTMF/SMS)

If you have a server that is not connected to the Internet, you can often hook up a modem/cell phone to the computer via a COM port. The Phone Dialer action lets you create scripts to dial the phone and send DTMF tones, or if a mobile phone is attached, you can send SMS messages directly.

Sending SMS messages directly from a mobile phone will require you to look in your mobile phone's manual and find out what commands it supports. Generally you'll be looking for the CMGS command. The following sample script gives you an idea of the commands that you are looking for:

```
ATZ
AT+CMGF=1
AT+CMGS=<number_to_dial>
<message text>
{VAL:26}
```

Note that the {VAL:26} is how you send a Ctrl-Z (End of Message character). Also, newer versions of our products support replacement variables in the message text so you can send the title or description of an error message.

Update Checks and Privacy

Many customers asked us for a simple way to be notified of product updates. We responded by building it into the application via the Settings dialog. You can control whether you check for updates, and how you are notified.

When an update check happens, an HTTP request is made to a page on our webserver. Appended to the URL we send the current version that is running (so the web server can decide whether a newer version is available or not, as well as whether any version-specific message needs to be sent back).

The product also sends three additional pieces of information for statistical purposes:

- Whether the product is in demo mode or not
- The number of servers being monitored
- How often the update check will happen (every 30 days if enabled)

Nothing in the list above identifies you, your company or the computer (no license information, no machine names, no expiration dates, no email addresses, etc). While it's true that all HTTP requests send an IP address, we do not and will not be tracking that.

Basically we'd like to eventually be able to report (well, brag) that X number of servers are being monitored by our products. We hope this update check mechanism will be viewed as a win-win.