

# PA Storage Monitor

Version 3.7 Pro

Last Update: July 14, 2009

**Power Admin LLC**

support@poweradmin.com

[www.poweradmin.com](http://www.poweradmin.com)

Prepared in the USA

Power Admin and the PowerAdmin.com web site are  
© 2002-2009 Power Admin LLC. All Rights Reserved.

## Getting Started with PA Storage Monitor

---

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

### Installation

---

- › [Getting Started](#)
- › [Quick Installation Guide](#)
- › [Startup Wizard](#)

### Configuration

---

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

- › [Concepts](#)
- › [Console](#)
- › [Global Settings](#)
- › [Database Settings](#)
- › [HTTP Settings](#)
- › [Report Settings](#)
- › [Smart Configuration](#)
- › [Adding Computers](#)
- › [Adding Monitors](#)
- › [Adding Actions](#)
- › [Event Escalation](#)
- › [Error Auditing](#)
- › [Bulk Configuration](#)
- › [Maintenance Schedule](#)
- › [Import & Export Configurations](#)
- › [External API](#)

### Monitors

---

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

- › [Calculated Status Monitor](#)
- › [Directory Quota Monitor](#)
- › [Disk Space Monitor](#)
- › [Execute Scripts](#)
- › [File Age Monitor](#)
- › [File/Directory Size Monitor](#)
- › [File & Directory Monitor](#)
- › [File System Analyzer](#)
- › [User Quota 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](#)
- [Monitor-Directed Email](#)
- [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 Storage Monitor on your network. The entries in this section explain the types of reports that are supported and how to view them.

- [Server Status](#)
- [Group Summary](#)
- [All Errors Report](#)
- [All Servers Report](#)
- [Visual Status Map](#)
- [Group Settings](#)
- [Ad Hoc Reports](#)
- [Scheduled Reports](#)
- [Publish Reports](#)
- [System Activity Log](#)

## Quick Installation Guide for PA Storage Monitor

---

You will find that PA Storage Monitor 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 its 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 Storage Monitor 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 Storage Monitor

        Databases

        Reports

PA Storage Monitor 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 Storage Monitor will guide you in setting up your first few monitors and actions. It will be helpful to have the following available:

- The names of a few servers/devices to monitor
- The usernames and passwords needed to access the above servers/devices (a domain account works well for Windows servers, but is not required)
- Your SMTP server information (such as SMTP server name, port (if non standard), SMTP username and password if needed) for sending alerts

## PA Storage Monitor Startup Wizard

The instructions that are provided here apply to the process that you can follow when you run PA Storage Monitor for the first time.

Most of the screens that you will encounter in the Startup Wizard are standard configuration dialogs that are available to you from PA Storage Monitor, so you can always change the configuration for your setup later.

When you see the Welcome dialog, press Yes to enter the Wizard. Press No to return to PA Storage Monitor (you will have nothing configured if you do this and you will have to set up servers and other monitored devices manually.) If you press Yes you will see the next screen shown, Settings.

The screenshot shows the 'Settings' dialog box for PA Storage Monitor. It contains the following elements:

- Title Bar:** 'Settings' with a close button (X).
- Startup Delay:** A text box with '30' and the label 'After the computer starts, wait 30 seconds before starting monitors in order to help the computer 'settle down' quicker.'
- Service Start Options:**
  - 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)
- Service Account:**
  - Local System (an internal account that can only access this computer)
  - The following user: [text box], Password: [text box], Domain: OFFICE [dropdown]. Includes a link for 'Remote monitoring hints [user account considerations]...'.
- CPU Usage:** A slider for 'Target average CPU usage' ranging from 20% to 90%, with a marker at 10%.
- Updates:**
  - Check for updates every 30 days and notify using: [text box]. Includes a 'Check Now' button and a '[Privacy]' link.
- Logging:**
  - Log files: C:\Temp\ [text box] with a browse button (...).
  - Max log file size in KB: 8192 [text box].
  - Enable Debug logging
  - Enable Data logging
- Buttons:** A vertical column of buttons on the right: OK, Cancel, System Alerts ..., Console Security ..., About, Database Settings ..., Report Settings ..., HTTP Server Settings ...

Refer to the help page [Global Settings](#) for information on these entries.

Select OK when you are finished with this screen.

The next screen is Configure Email Notification.

**Configure Email Notification**

Email Address: ops@xyzcorp.com, john@xyzcorp.com  
 (Multiple addresses can be comma separated)

**Advanced Options ...**

**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 **Test Primary Server**

From Address (ex 123@xyz.com): alerts@xyzcorp.com Encryption: Don't Know

Optional

Username for SMTP Server: example\_user

Password for SMTP Server: [REDACTED]

Retype password: [REDACTED]

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: [REDACTED] Port: 25 **Test Backup Server**

Optional

From Address: [REDACTED]

Username for SMTP Server: [REDACTED]

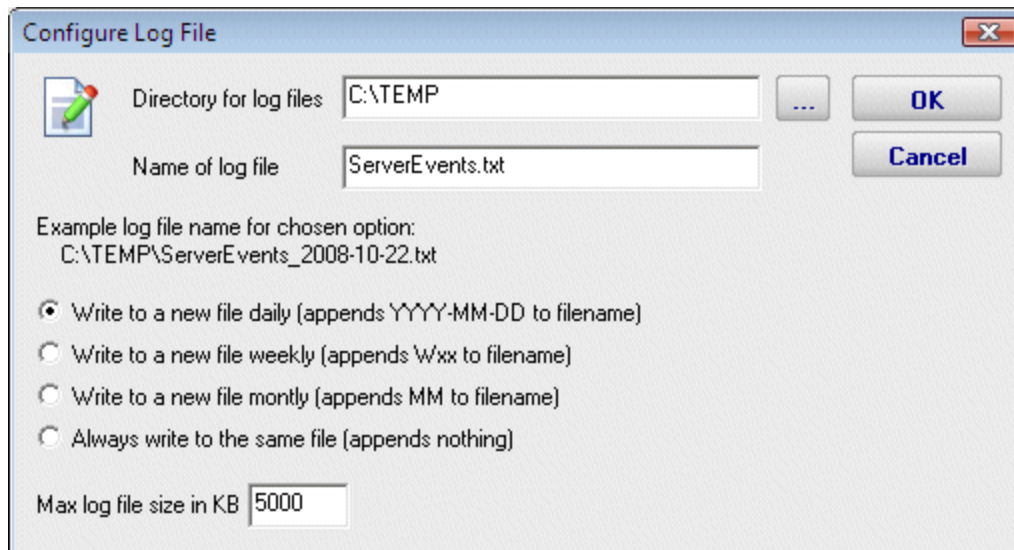
Password for SMTP Server: [REDACTED]

Retype password: [REDACTED]

Buttons: OK, Cancel, Message ..., Schedule ...

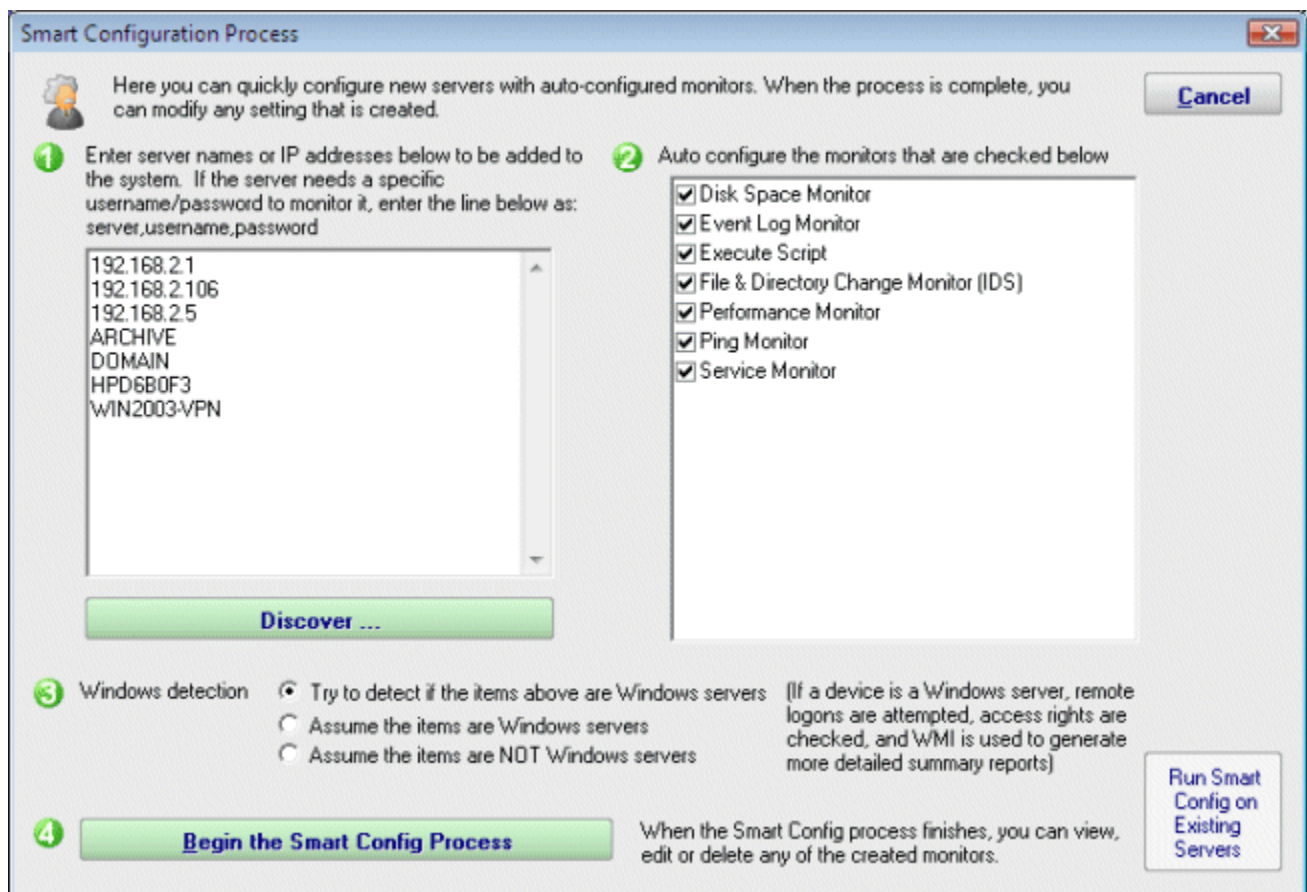
Refer to the help page [Send SMTP E-Mail](#) for directions. Select OK when you are finished with the Configure Email Notification screen.

The next screen helps you configure a [Write To Text Log File](#) action which the monitors can use to record human readable events that happen.



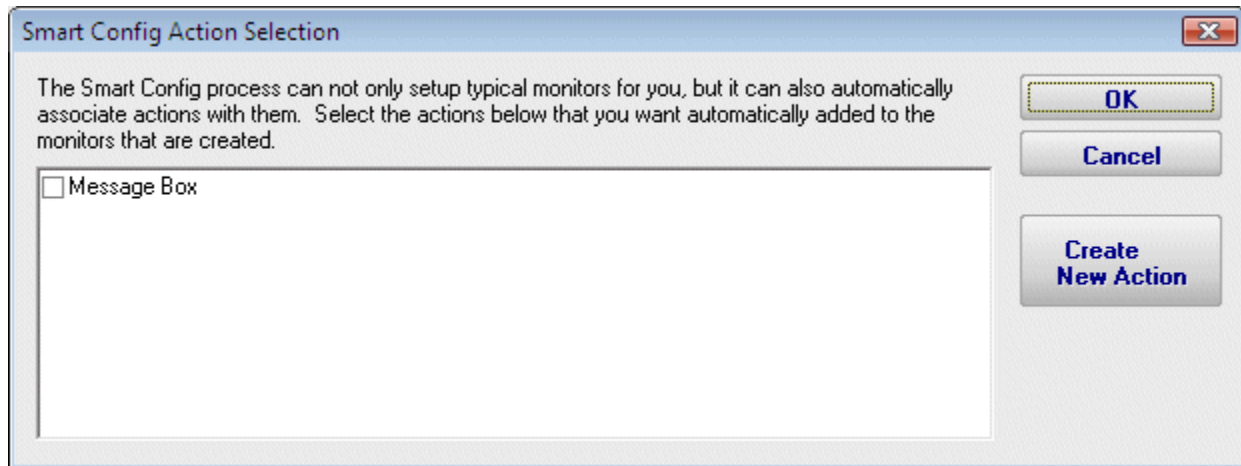
Select OK when you are finished with this screen.

The Smart Configuration screen help you set up many servers and devices in for monitoring. The program will create the some commonly used monitors and actions for each server or device that you enter. You can simply paste a list of machine names or IP addresses into the box for configuration to target those servers/devices. Optionally, you can press the Discover button to have the product do a Ping sweep to try and find servers and devices within a subnet.



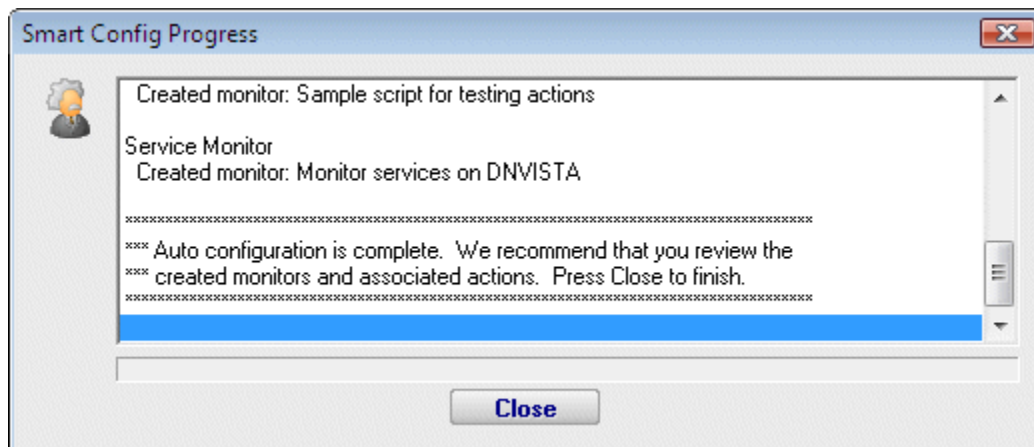
Refer to the help file entry labeled [Smart Configuration](#) for specific instructions for this screen.

After you have entered the necessary parameters, select the button labeled "Begin the Smart Config Process". You will then see the next screen.



The "Smart Config Action Selection" lets you customize the Actions that the Smart Configuration process will create for you for every Monitor that is created for a server or device.

When you have completed your selections, select OK. You will see a progress dialog as each server or device is checked and default monitors created.



The screen labeled "Smart Config Process" shows you what PA Storage Monitor is doing to set up the initial set of Monitors for your systems. When it is in process the centered button is labeled Cancel and you can stop the process by selecting it. When the process completes, you will see text as shown in the screen shot and the label on the button changes to Close. Select Close at this time in order to progress to the end of the Startup Wizard.

The final screen will display helpful information for you, and confirms the end of the Startup Wizard.

Press OK to continue. At this time, the [Console](#) of PA Storage Monitor will be displayed, configured with the Monitors and Actions that were automatically configured for the servers that you selected. These monitors are just defaults -- feel free to change or delete them.



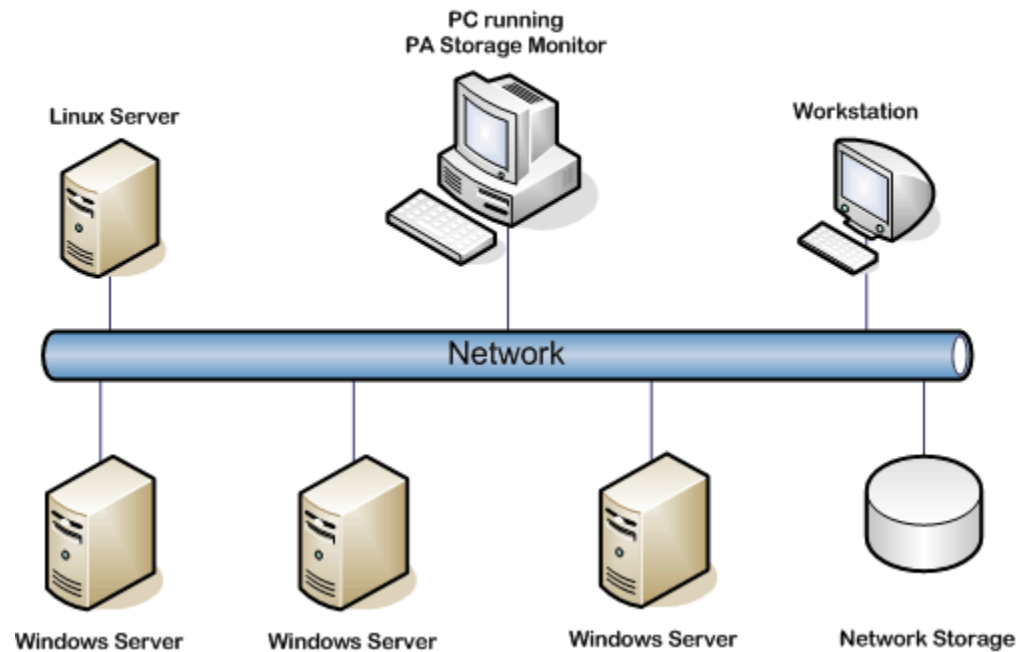
## Configuration

[Contents](#)

### Terminology and Concepts of PA Storage Monitor

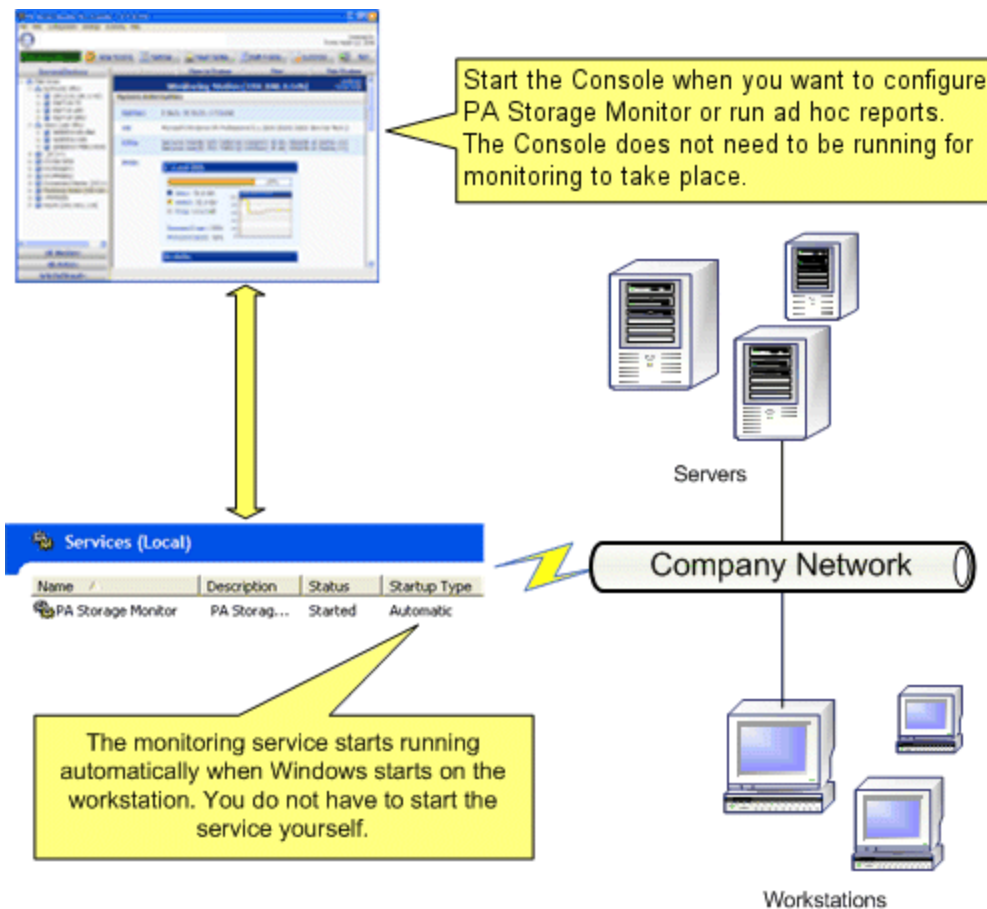
PA Storage Monitor runs on a Windows computer and monitors the condition of storage space on servers. The following graphic shows the basic structure of a network that is using PA Storage Monitor.

#### PA Storage Monitor In Operation in a Typical Network



The PA Storage Monitor product is composed of two parts: a graphical user interface which we call the Console, and a background process called the monitoring service. You see the Console when you launch PA Storage Monitor from the desktop. The service is invisible and has no user interface of its own.

The following diagram will give you a better idea of how the two parts of PA Storage Monitor work together.



The service is the part of the product that performs the monitoring of the servers. The service is set up so that it runs automatically when Windows starts. The Console does not need to be running in order for monitoring to take place.

The Console and the service are installed at the same time when you install PA Storage Monitor from the setup application.

## Product Terminology

PA Storage Monitor is based on the concepts of Monitors and Actions.

The PA Storage Monitor product contains different types of Monitors that watch server resources. These monitors trigger Actions (such as notifications or server operations) as well as record monitored data to a database for report generation.

### Monitor

A Monitor periodically checks a computer resource and optionally compares the measurement to a threshold value that you set.

You can create a new Monitor by selecting its type and filling in the required parameters.

### Error Condition

An Error Condition happens when a value of a resource that is checked by a Monitor is outside the acceptable range for that value.

One example of an Error Condition is space on a particular disk volume falling beneath a defined threshold.

## Action

An Action is an activity that PA Storage Monitor 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 Storage Monitor 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.

When the Error Condition stops occurring, another list of Actions that is attached to the monitor may be executed. This list is called the Fixed Actions for the Monitor. Each Action in the list is executed, in the order in which it appears in the list. Its entries are executed when the Error Condition has been fixed. Not all monitors have Fixed Actions.

## How Monitors and Actions are Created

Monitors and Actions may be created in any of three ways:

- Automatically: the [Smart Configuration](#) screen allows you to set check boxes that show the types of Monitors that you want the program to create for you. PA Storage Monitor will use these settings to create a set of Monitors that are typical and recommended. It will also create the accompanying Actions for each Monitor. PA Storage Monitor will do this for every server that you are configuring.
- Manually: you may use the tree view labeled Servers/Devices to add new monitors. See the help page [Adding Monitors](#).
- Imported Server Configuration: PA Storage Monitor 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.

## PA Storage Monitor Console

The Console is the administrative interface to PA Storage Monitor.

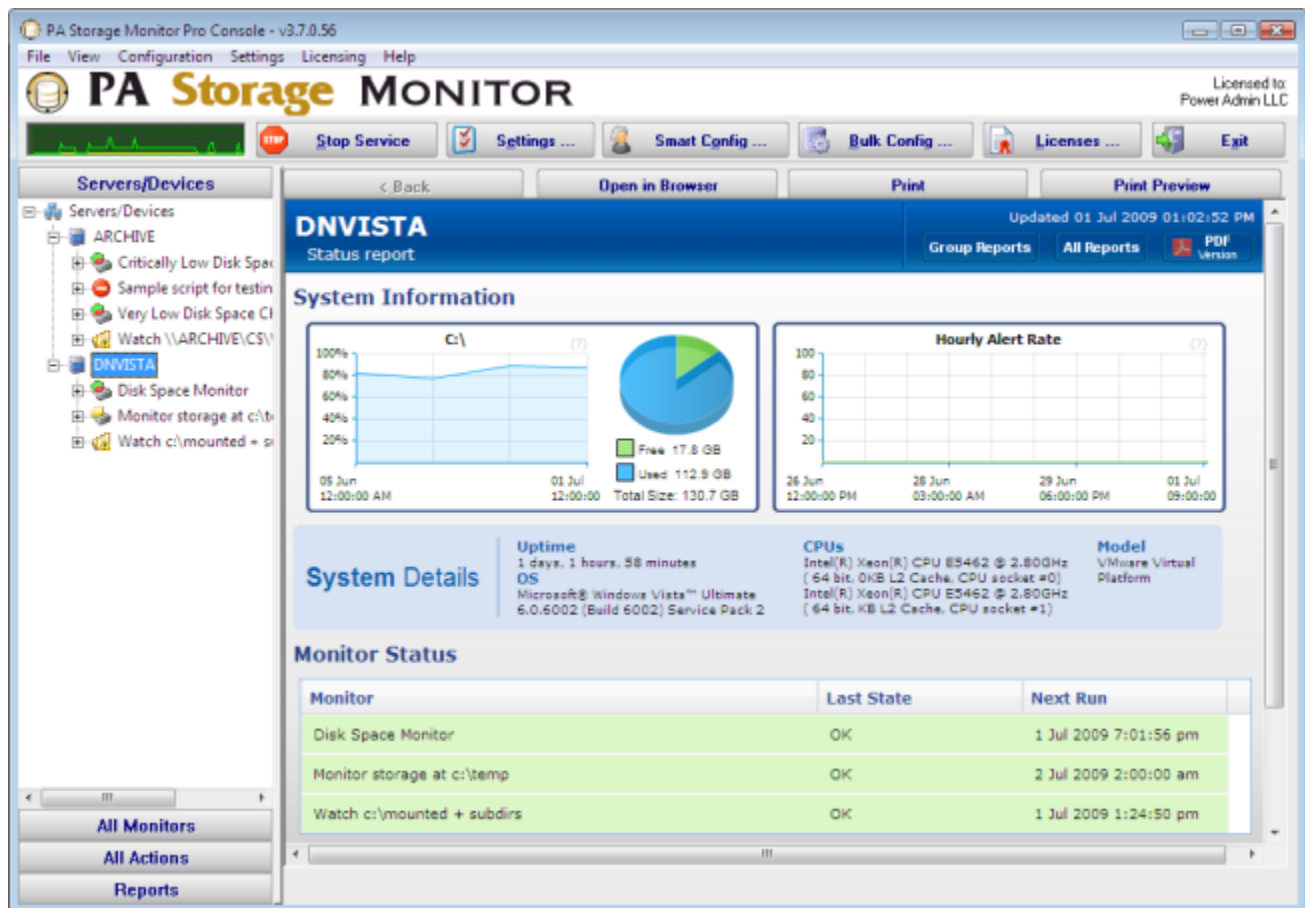
On the left side is the navigation pane. Similar to many other Windows products, this navigation pane displays items that you can interact with. Right clicking most items will give you a menu of choices. Selecting an item will cause the large right panel to change to your current selection.

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 Storage Monitor 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 Storage Monitor 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.



**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](#).

**Smart Configuration** This is the place to go any time you need to add additional computers to the system to be monitored. There is more information in the [Smart Config](#) help topic.

**Bulk Configuration** This feature allows you to perform changes to many computers, monitors, actions or reports at once. [More info...](#)

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

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

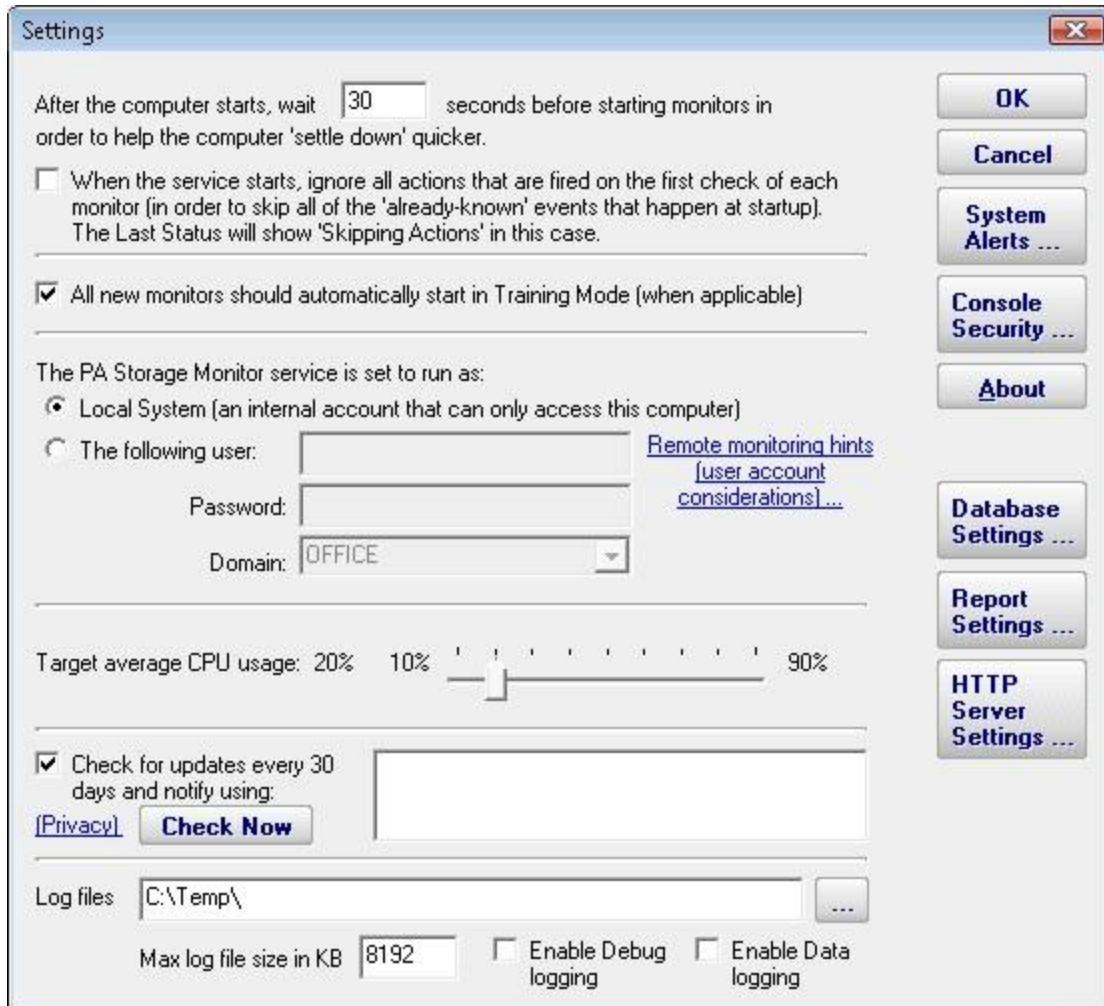
## Global Settings

---

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 Storage Monitor to authorized users.
- [Database Settings](#) dialog allows you to set up PA Storage Monitor to use the embedded SQLite database or Microsoft SQL Server as the storage for PA Storage Monitor data.
- [Report Settings](#) affect the storage of archived reports and the behavior of the reporting features of PA Storage Monitor.
- [HTTP Server Settings](#) allows you to change details of the way the built-in web server in PA Storage Monitor operates.



**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.

Note:

- The default Local System user can access all local resources, but can't access any remote Windows resources (it can however access non-Windows remote resources such as ping, web pages, etc).

- If you will be monitoring remote systems, select "The following user" radio button and set the user name and password to a domain account or to a local account which has the same user name and password as an account on the remote system ([see Remote Monitoring Hints](#)). Another alternative is to right-click the computer in the monitoring Console and select Type & Credentials -> Set Login Credentials for server-specific credentials.

**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.



## Database Settings

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

➤ **SQLite**

By default, PA Storage Monitor 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 Storage Monitor.

➤ **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.

**Database Settings**

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

Database files:  ... 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.

Test Connection

OK  
Cancel  
Database Cleanup

## More about Microsoft SQL Server and PA Storage Monitor

---

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 Storage Monitor (normally `C:\Program Files\PA Storage Monitor.`)

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 Storage Monitor 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 Storage Monitor 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 Storage Monitor, the SQL Server Native Client Library does not need to be installed.

## HTTP (Web Server) Configuration

The PA Storage Monitor service contains an embedded web server for serving HTML reports to the Console and to browsers, as well as 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.

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:  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

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 Storage Monitor 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 Storage Monitor 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 Storage Monitor 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 Storage Monitor 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 Storage Monitor responds to commands that are issued by the Console part of PA Storage Monitor. You may disable command processing entirely. Or, you may enable command processing, but only from the machine on which PA Storage Monitor is installed. The default setting is "Process commands only from this machine."

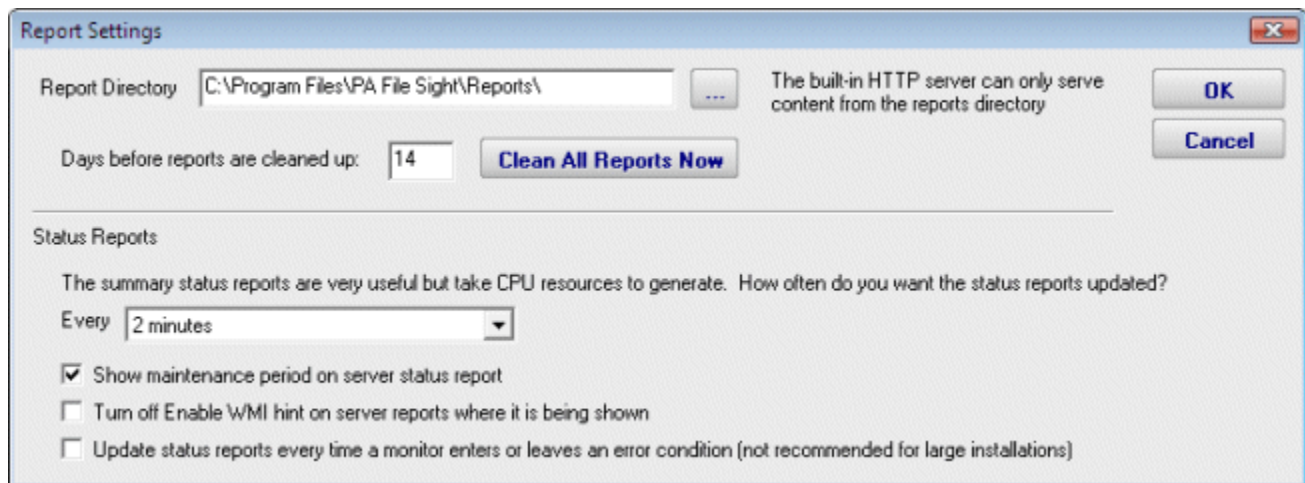
Currently, the only case where commands are sent from a remote machine is if a user is viewing the Visual Status Map report in a browser on a separate machine.

## Report Settings

The Report Settings dialog allows you to customize aspects of the way PA Storage Monitor 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 Storage Monitor.
- 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 Storage Monitor 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. In a small installation (less than 50 servers) regenerating the reports every minute is not a problem, but in a bigger installation choosing a larger interval would be more efficient.
- Show Maintenance Period on server status report - Self explanatory.
- Turn off "Enable WMI Hint" on Server Reports Where it is Being Shown - If PA Storage Monitor 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.



## Smart Configuration

The Smart Configuration feature is a very useful tool for quickly adding servers or devices to be monitored. You specify one or more servers, and the monitor modules inspect the server(s) and create appropriate monitors for each server based on default settings.

You can access the feature by clicking the Smart Config button at the top of the Console.

You can paste a list of server names or IP addresses into an edit box. You can specify a username and password to use when accessing the server by entering any line in the form:

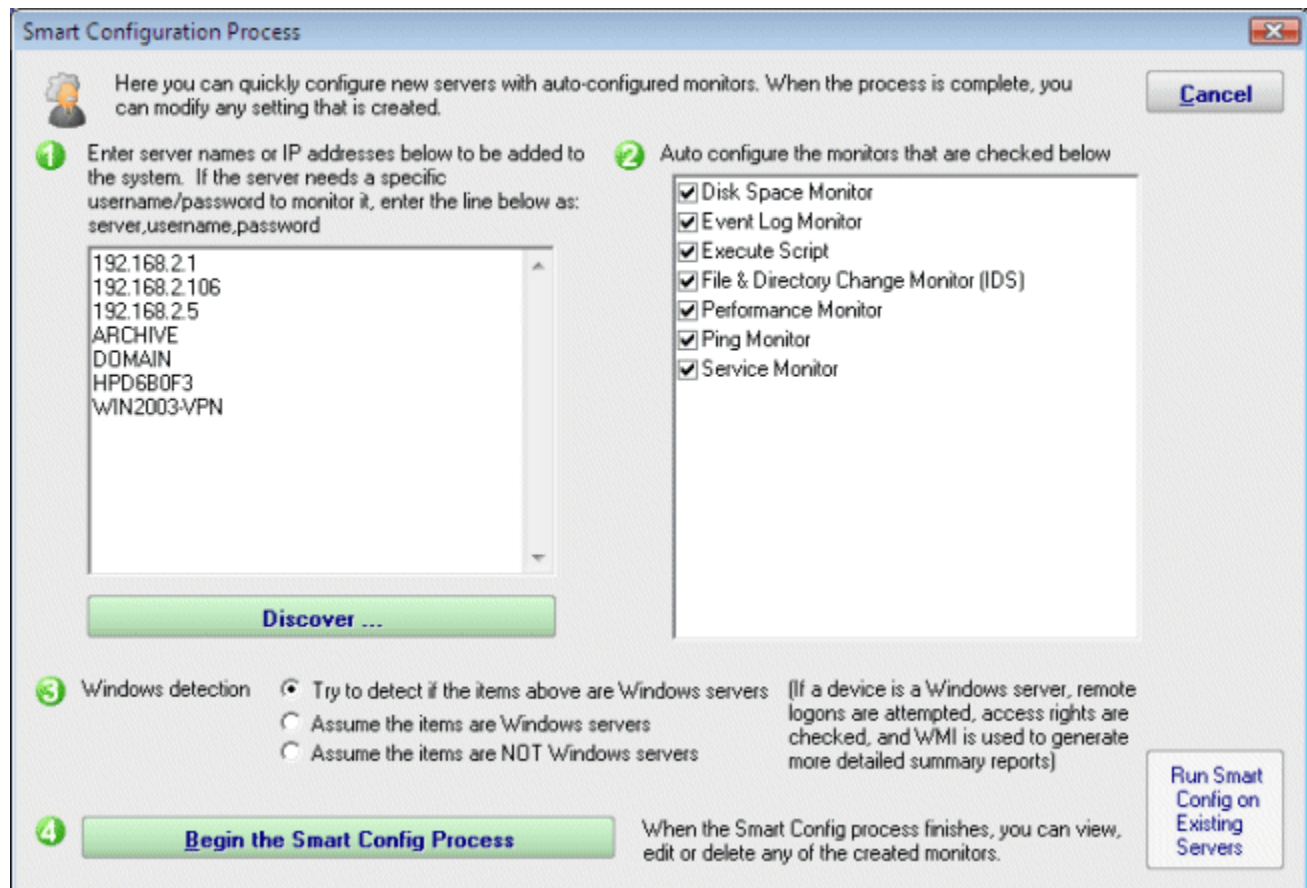
```
server_name,username,password
```

(for another example, open the dialog below in the Console, and let your mouse hover over the server list window for a helpful hint).

If no username/password is given, the configuration procedure will try any already entered credentials to see if they will work. Otherwise the service's Login As user will be used.

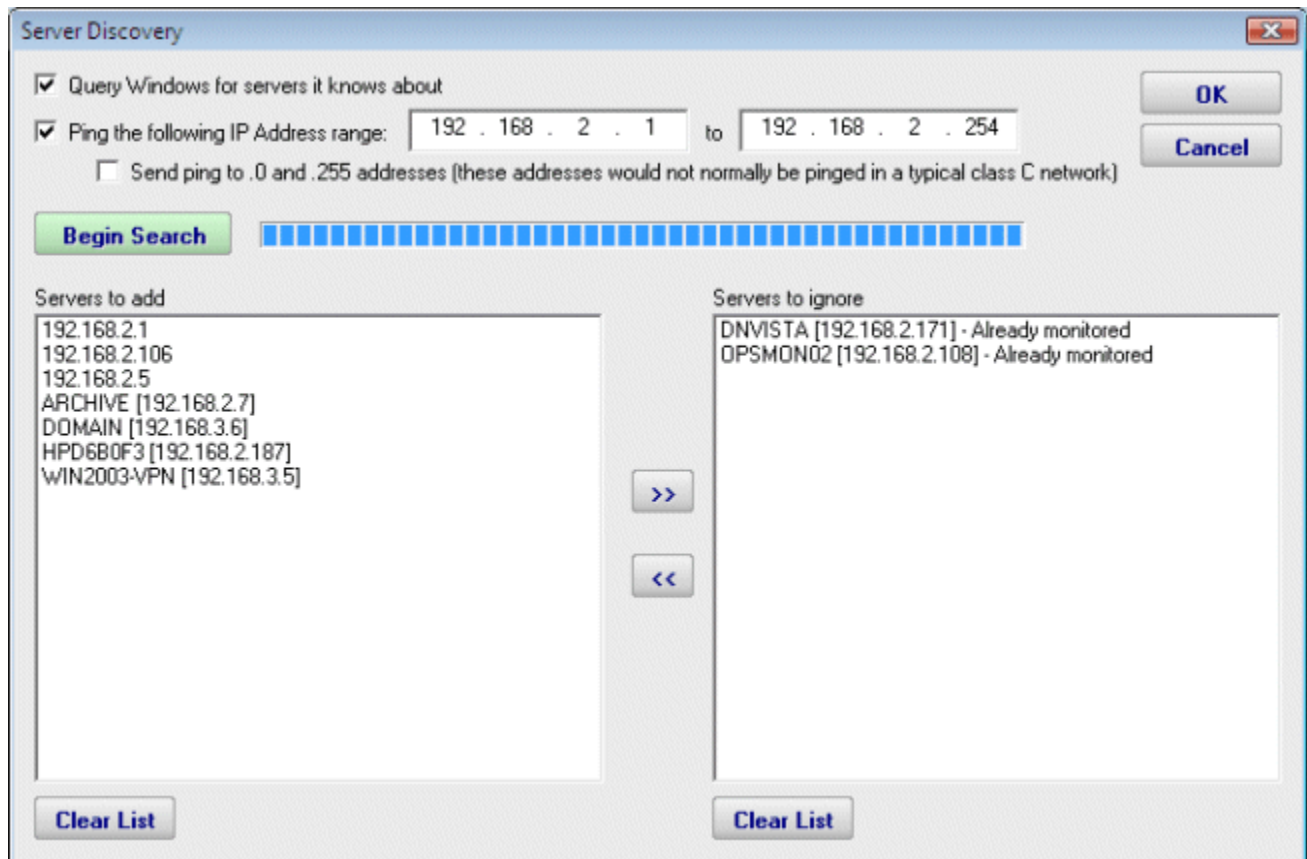
The next step is to select which monitor modules should inspect the server(s)/device(s) and press "Begin the Smart Config Process". In a few moments you'll have monitors automatically configured for your specific environment. Naturally the auto-created monitors can be changed or deleted just like any other monitor in the system.

Existing monitors and actions are not modified--new monitors and new actions are created while leaving the existing monitors and actions alone.





Pressing the green button labeled "Discover" in section 1 of this dialog allows PA Storage Monitor to scan the network for servers and devices without having to manually gather this information. To use this feature, press the "Discover" button. The following dialog will appear on top of the Smart Configuration dialog.



The following options are available to you for Server Discovery:

- Query Windows for servers it knows about: Windows has its own network discovery process that is used by Windows networking, and PA Storage Monitor will inquire it to determine any servers currently unknown to the program.
- Ping the following IP Address range: A TCP/IP message will be sent to each address that can exist in the range of IP addresses that are entered into the text boxes. Note that entering different numeric values for the third octet values (the ones shown as zeroes in the screen shot above) may dramatically increase the time required to complete the scan.
- Send ping to .0 and .255 addresses: these address values have special use in the TCP/IP protocol. The program will set this checkbox to disabled. You may enable this feature if you have reason to believe that these addresses are in use by computers of interest for monitoring.
- Servers to add: these are the IP addresses (or computer names if they could be resolved) where servers/devices were detected, and which are not currently being monitored.
- Servers to ignore: These are servers/devices that were discovered, but which are already being monitored.

Pressing the Ok button at the completion of the scan will close this dialog and will cause the servers that are listed in the "servers to add" list to be transferred to the list of servers in section 1 of the Smart Configuration Process dialog.

Back in the Smart Configuration Process dialog, you'll also notice in the dialog a subtle button on the right which lets you run Smart Config on existing servers. This will open up the Bulk Config feature and guide you through the rest of the process.

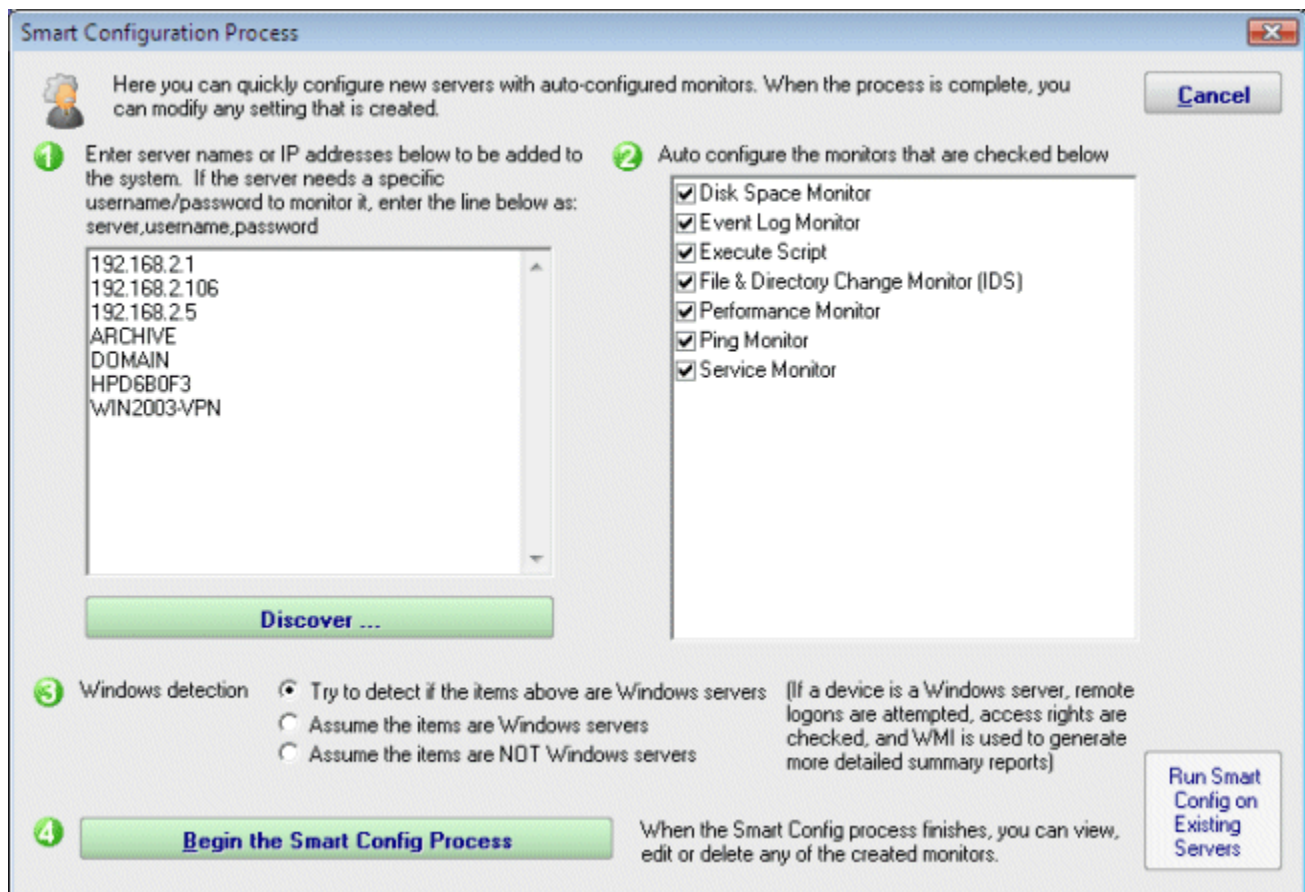


## Adding Computers

There are two ways to add computers/devices to the system to be monitored: individually and many at once. Both options are described below.

### Many at Once

The easiest way to add many computers/devices to the system at once is to use the Smart Config process. This will let you paste in a list of server names, device names or IP addresses that you want to monitor. You can also press the Discover button to help get that list. You'll also be able to choose a list of monitors to auto-configure for the new entities.



The Smart Config process will add the new computers to the top Servers/Devices group. You can use [Bulk Config](#) to easily move many servers at once to different groups.

[See Smart Configuration](#) for more detailed information.

### Adding Individual Computers

You can manually add a single computer to the list of computers to be monitored by right-clicking on any group in the left navigation pane in the Console. Doing so will first show the dialog below to collect the server name.

The "This is a Windows computer" gives the system hints about how it might need to authenticate with the remote computer. "Use WMI..." tells the system whether to attempt to query the new computer with WMI (Windows Management Instrumentation) in order to create a more detailed status report. Unchecking this value, even for a Windows server, will have no other effect other than a slightly less detailed status report. You can change these two settings later by right clicking on the computer and selecting Type & Credentials -> Set Server Type.



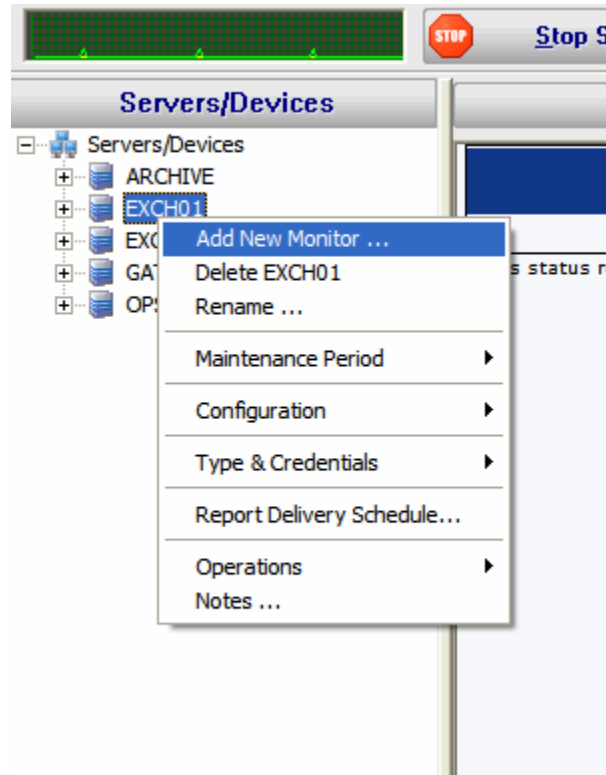
After the server name is entered, the credentials used to monitor the server are requested using the dialog below. You can enter credentials, or just monitor the server using the login that the monitoring service is already using. You can change these credentials later by right clicking the computer in the navigation pane and selecting the Type & Credentials -> Set Login Credentials menu item. The help page [Remote Monitoring Hints](#) has some advice and information about user accounts when monitoring Windows servers.



If you've already entered credentials for another server that should also work for this server, choose the middle radio button -- that will be easier than re-typing the credentials.

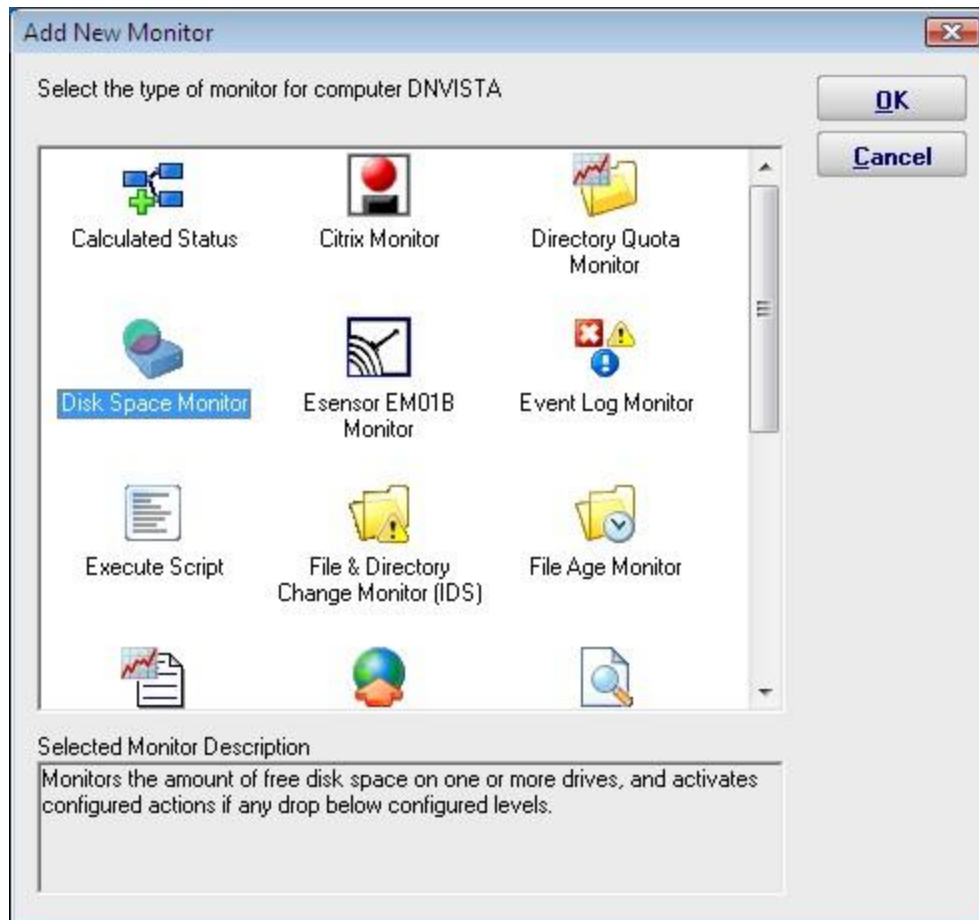
## Adding Monitors

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.



You will be shown the dialog below with all available monitors for your product and license (note that they may not be the same ones pictured).

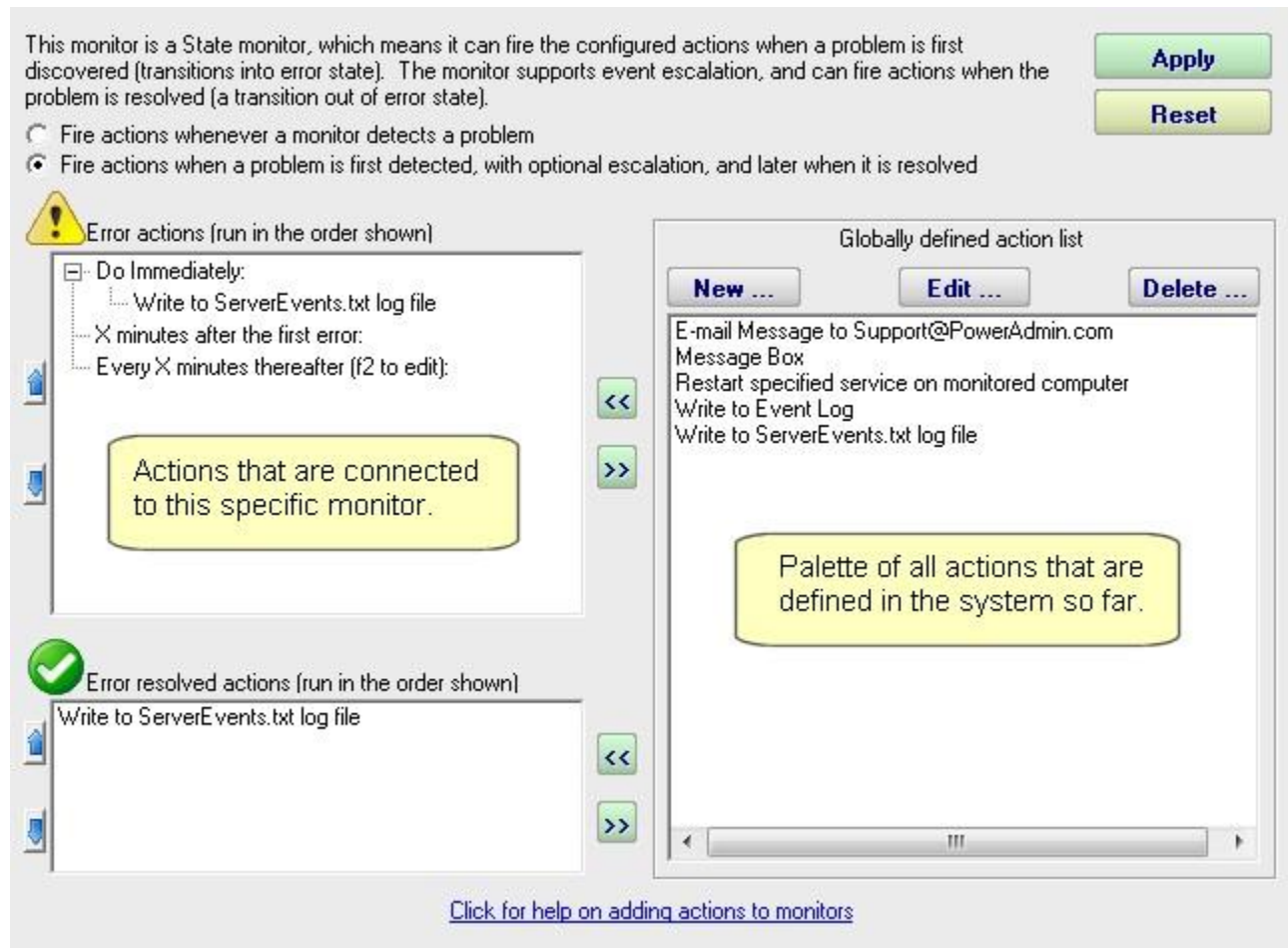
Once you select a monitor, you will be shown that monitor's configuration dialog.



Choose the type of monitor that you want and press OK. The monitor's configuration dialog will then be shown.

## 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).



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](#).

## 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 Storage Monitor 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).

Apply

Reset

- 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

New ... Edit ... Delete ...

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](#)



## 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

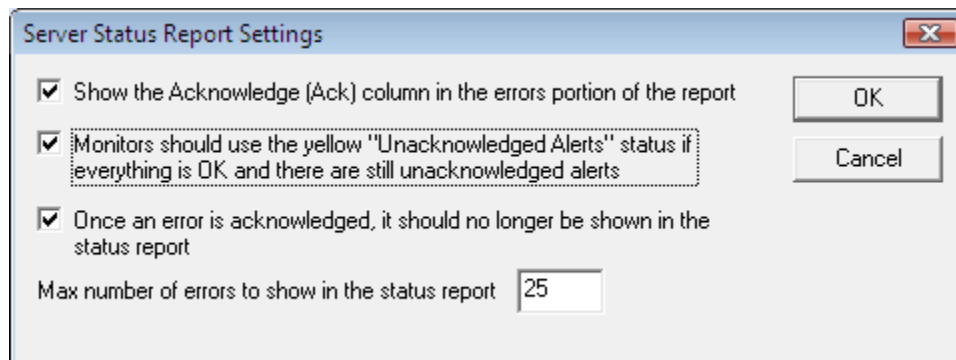
---

#### 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 addition, 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.



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.

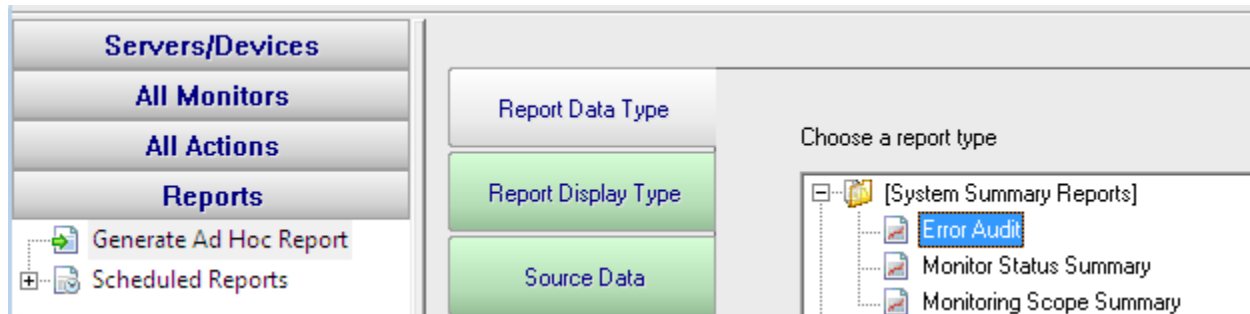
When the Ack column is clicked, an request is sent to the service indicating that the error has been acknowledged. The acknowledgement time as well as the IP address of the user is recorded. [A future version will user logins to view reports -- at that time the username will be recorded instead of the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

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		<input checked="" type="checkbox"/>
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		<input checked="" type="checkbox"/>

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 use 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).

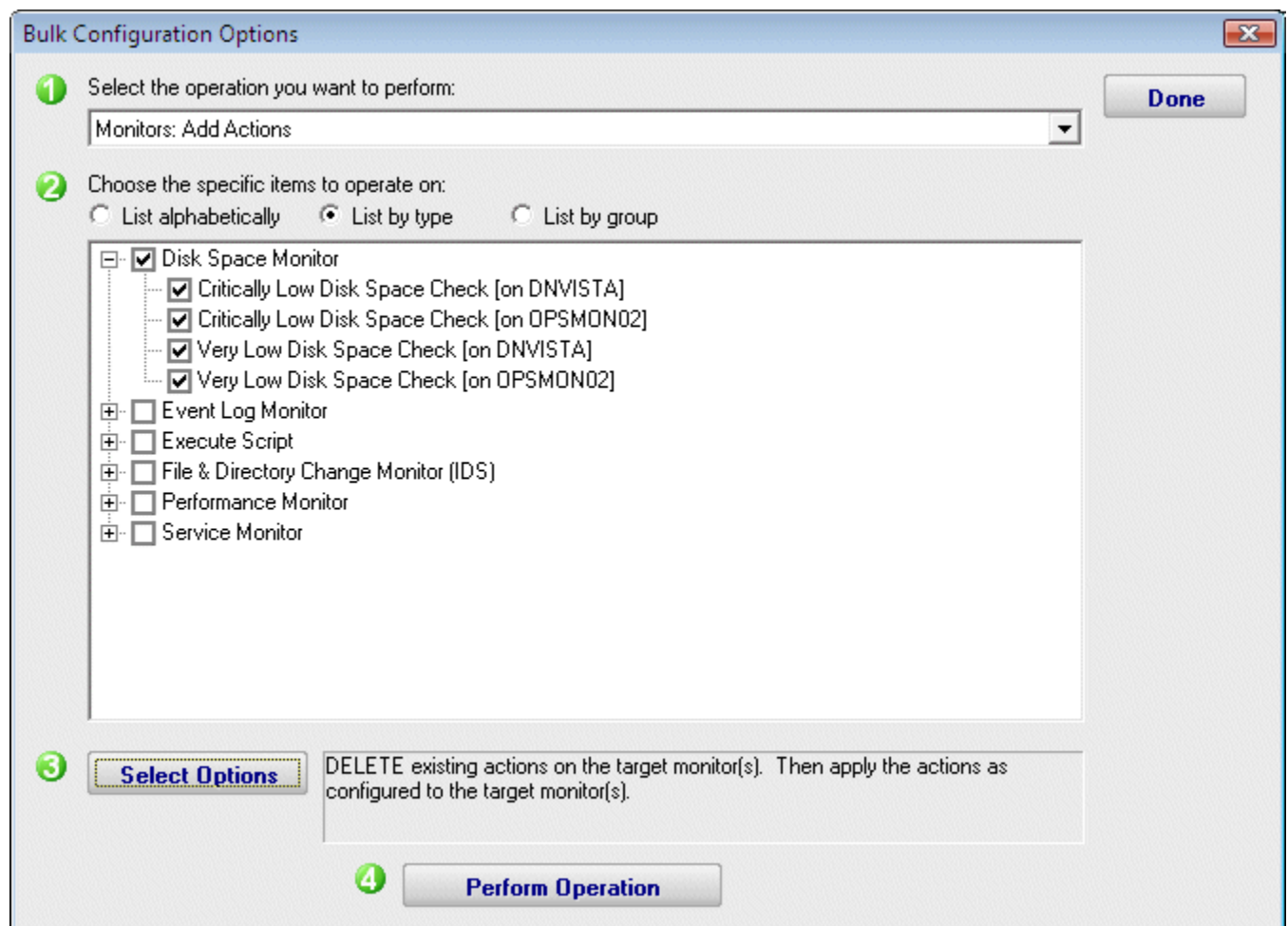
We recommended that each person with a large responsibility have their own Error Audit report so they can quickly see all errors within their area of responsibility. Errors can even be acknowledged on the Error Audit report itself, just like on the server status reports.

## Bulk Configuration

The Bulk Configuration feature of PA Storage Monitor 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.



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.

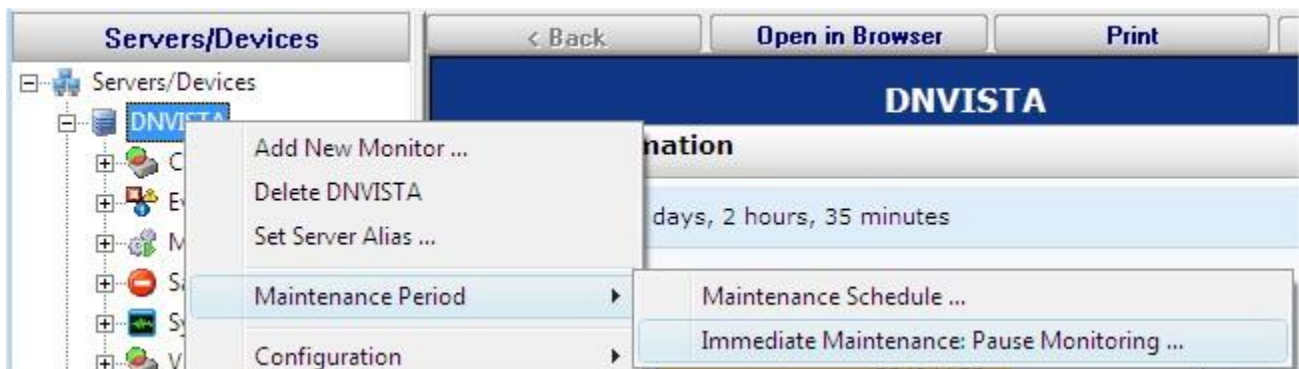
NOTE: The Bulk Configuration option only works when the Console and the monitoring service are both running -- it doesn't work if the service has not been started.

## Maintenance Mode

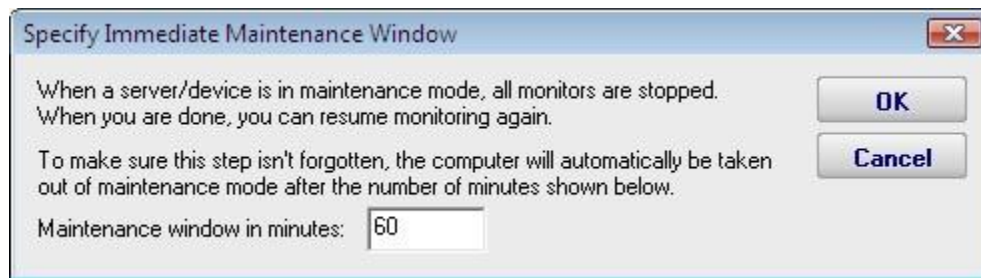
Maintenance Mode is very useful when you'll be working on a computer that is being monitored. Naturally you don't want to receive alerts or have the monitoring service try to correct things that you are working on. Instead of stopping the monitoring service (and potentially forgetting to start it again),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

## Manual Maintenance

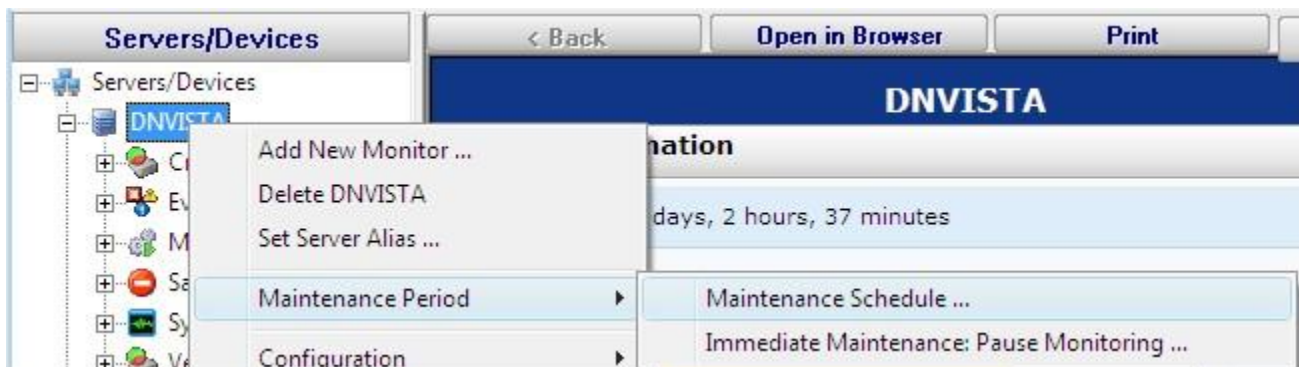
You manually put a server into maintenance mode immediately by right clicking on the computer and choosing Maintenance Period -> Immediate Maintenance: Pause Monitoring.



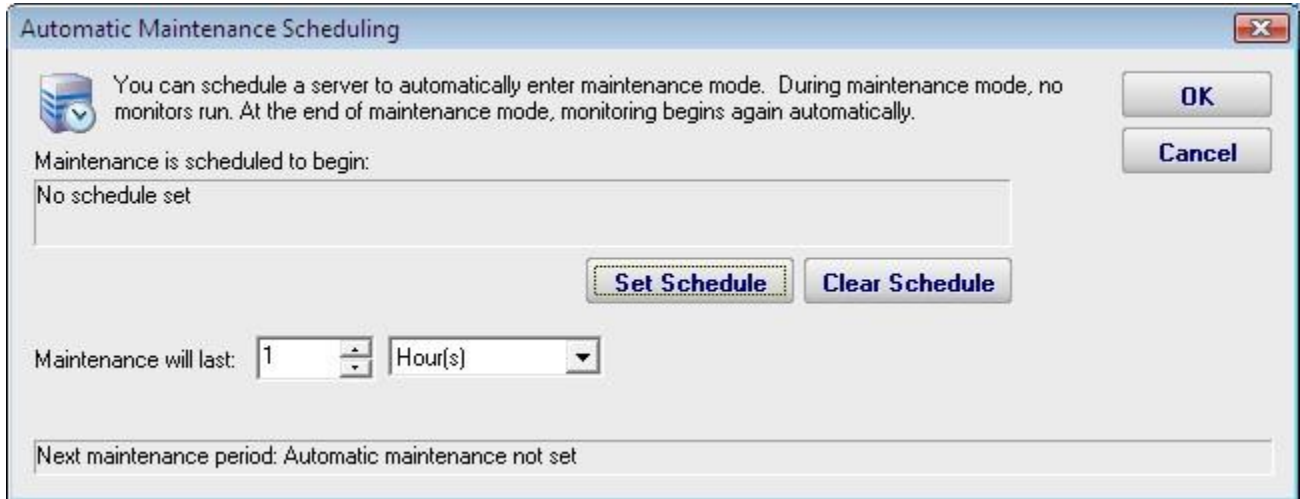
When you enter Maintenance Mode, you specify how long you expect to be working on the server. No further monitoring of the server will take place until that amount of time has past. Then active monitoring of the server begins again automatically.



## 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.





## Importing and Exporting Configurations

---

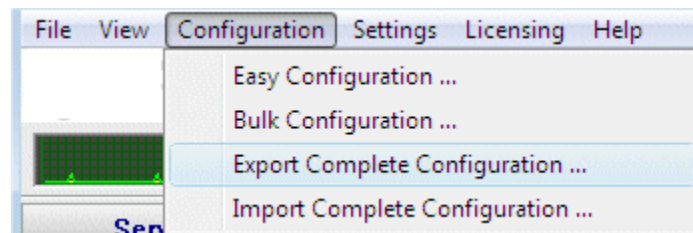
PA Storage Monitor supports a very easy and effective way to transfer your complex monitoring setups from one installation of the product to another. This is what exporting and importing configurations allows you to do.

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

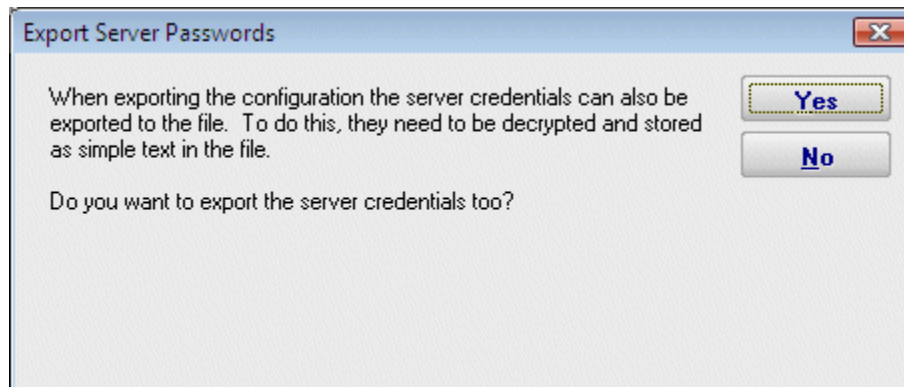
### Exporting Complete Configuration

---

Exporting the complete configuration is an easy way to preserve all of the settings that are contained in an instance of PA Storage Monitor. 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:



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 Storage Monitor 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 Storage Monitor 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.

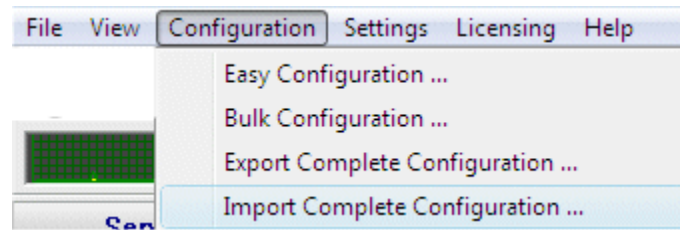
At the completion of the export of the configuration data, PA Storage Monitor will display a message box but only if you chose to save the credential information.

## Importing Complete Configuration

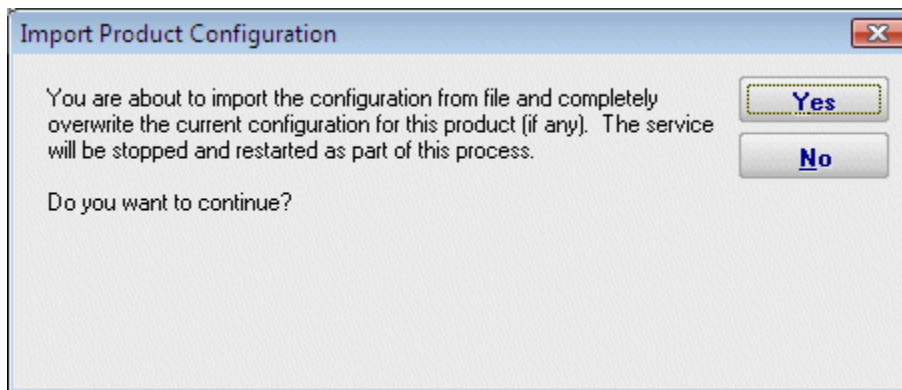
---

Just as easily as you can export a PA Storage Monitor configuration to a file, you can also import that file into a new installation of PA Storage Monitor 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 Storage Monitor and replace them with the contents of a configuration archive file.



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.

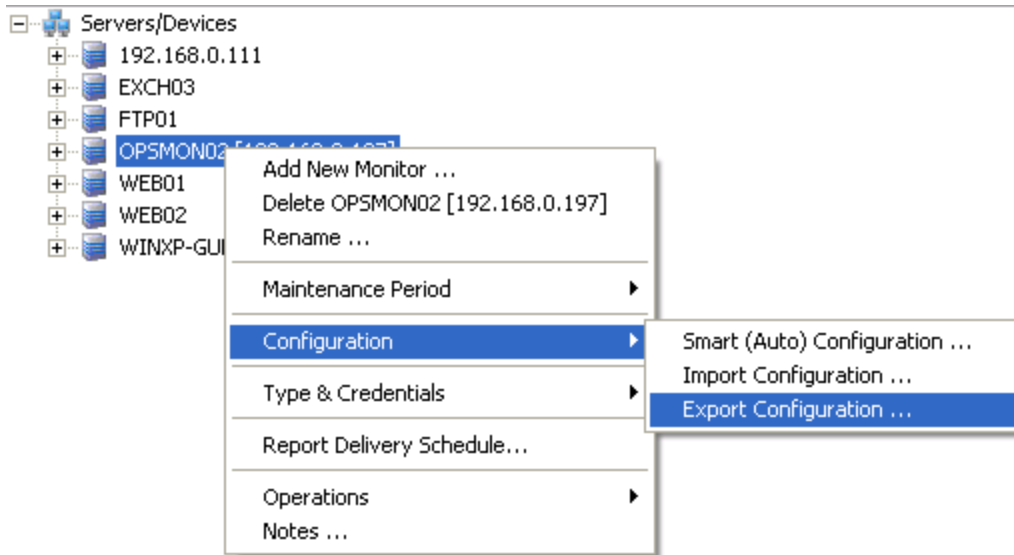
Note that this dialog box indicates a file of the extension .axml, as saved by the Export procedure. At the end of the import, you should see the list of servers restored to the Navigation Pane. A message box will appear at the end of the import process indicating the success of the operation, as well 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.

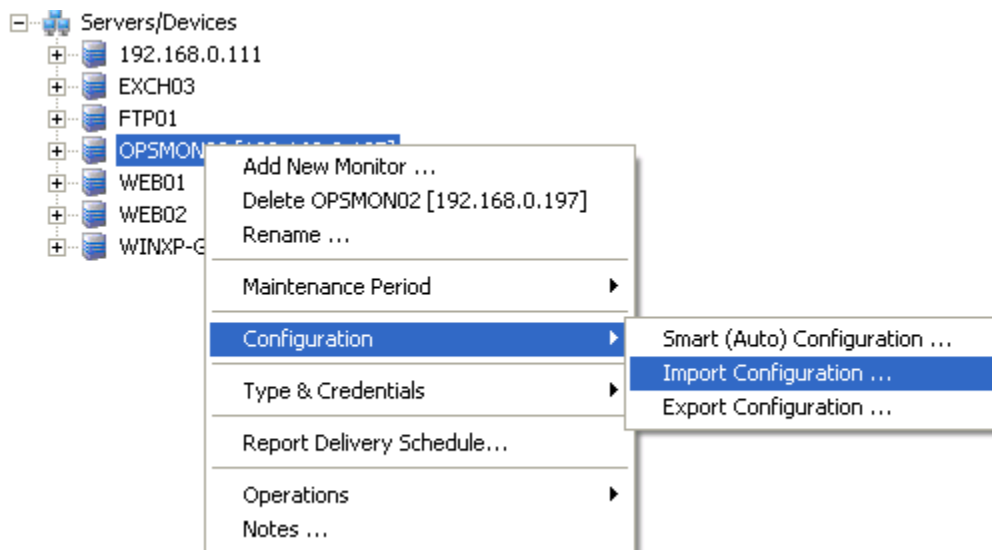
The menu item that selects the export server operation is accessed by right clicking a server or device whose configuration you wish to export. The menu appears as follows.



The series of dialog boxes and the options that appear is identical to that shown above for exporting a complete PA Storage Monitor 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 Storage Monitor. 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.

## External API

---

PA Storage Monitor 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/PASFileSight

PA Server Monitor - HKEY\_LOCAL\_MACHINE/software/PowerAdminServerMonitor

PA Storage Monitor - HKEY\_LOCAL\_MACHINE/software/PASStorageMonitor

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.

<b>GET_SERVER_LIST</b>	Returns a list of servers and the group that the server is in. Parameters: none Example: <pre>https://server:81?API=GET_SERVER_LIST&amp;KEY=921msa8gbk4j78dbglaj</pre> Output (server group{tab}group where {tab} is the ASCII tab
------------------------	--

	<p>(\t) character:</p> <pre> : 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 :</pre>
<b>START_MAINTENANCE</b>	<p>Put the server into immediate maintenance mode.</p> <p>Parameters:</p> <p>SERVER - name of the server that should be put into maintenance mode</p> <p>MINUTES - time in minutes that the server should remain in maintenance mode before it automatically reverts to normal monitoring</p> <p>Example:</p> <pre>https://server:81?API=START_MAINTENANCE&amp;KEY=921msa8gbk4j78dbglaj &amp;SERVER=MAILSRV&amp;MINUTES=15</pre> <p>Output:</p> <pre>:OK:</pre>
<b>END_MAINTENANCE</b>	<p>Put the server back into normal monitoring mode.</p> <p>Parameters:</p> <p>SERVER - name of the server that should be put into normal monitoring mode</p> <p>Example:</p> <pre>https://server:81?API=END_MAINTENANCE&amp;KEY=921msa8gbk4j78dbglaj&amp;SERVER=MAILSRV</pre> <p>Output:</p> <pre>:OK:</pre>
<b>ADD_SERVER</b>	<p>Add and optionally configure the named server</p> <p>Parameters:</p> <p>SERVER - name of the server that should be added</p> <p>WIN (optional) - defaults to 0. Set to 1 if this is a Windows server.</p> <p>WMI (optional) - defaults to 0. Set to 1 if WMI polling should happen to collect System Details information for the server status</p>

	<p>report</p> <p>CONFIG_PATH (optional) - defaults to none. Full path to a .xml config file that specifies a configuration that should be applied to the new server. .xml files are created by <a href="#">exporting a computer's configuration</a>. The file must be on the same computer as PA Storage Monitor is running on.</p> <p>Example:</p> <pre>https://server:81?API=ADD_SERVER&amp;KEY=921msa8gbk4j78dbglaj&amp;SERVER=MAILSRV2&amp;WIN=1&amp;WMI=1&amp;CONFIG_PATH=C:\Configs\MailConfig.xml</pre> <p>Output:</p> <pre>:OK:</pre>
<p><b>DELETE_SERVER</b></p>	<p>Delete the named server, along with all of its monitors</p> <p>Parameters:</p> <p>SERVER - name of the server that should be deleted</p> <p>Example:</p> <pre>https://server:81?API=DELETE_SERVER&amp;KEY=921msa8gbk4j78dbglaj&amp;SERVER=MAILSRV2</pre> <p>Output:</p> <pre>:OK:</pre>

## Monitors

---

[Contents](#)

### Calculated Status Monitor

---

There are sometimes situations where you want a monitor to report on the combined status of a few different monitors. Or perhaps you need the exact opposite of a monitor (for example, to be alerted when a Ping is successful on a back-up line that ought to be down most of the time). The Calculated Status monitor was created for these situations.

The Calculated Status Monitor is a script that uses the statuses of one or more input monitors. Once you have those input statuses, you can combine, compare or do any other operation that you like using the VBScript language. The final output is the status for the monitor. For example, look at the example script below (a somewhat similar default script is created for you automatically):

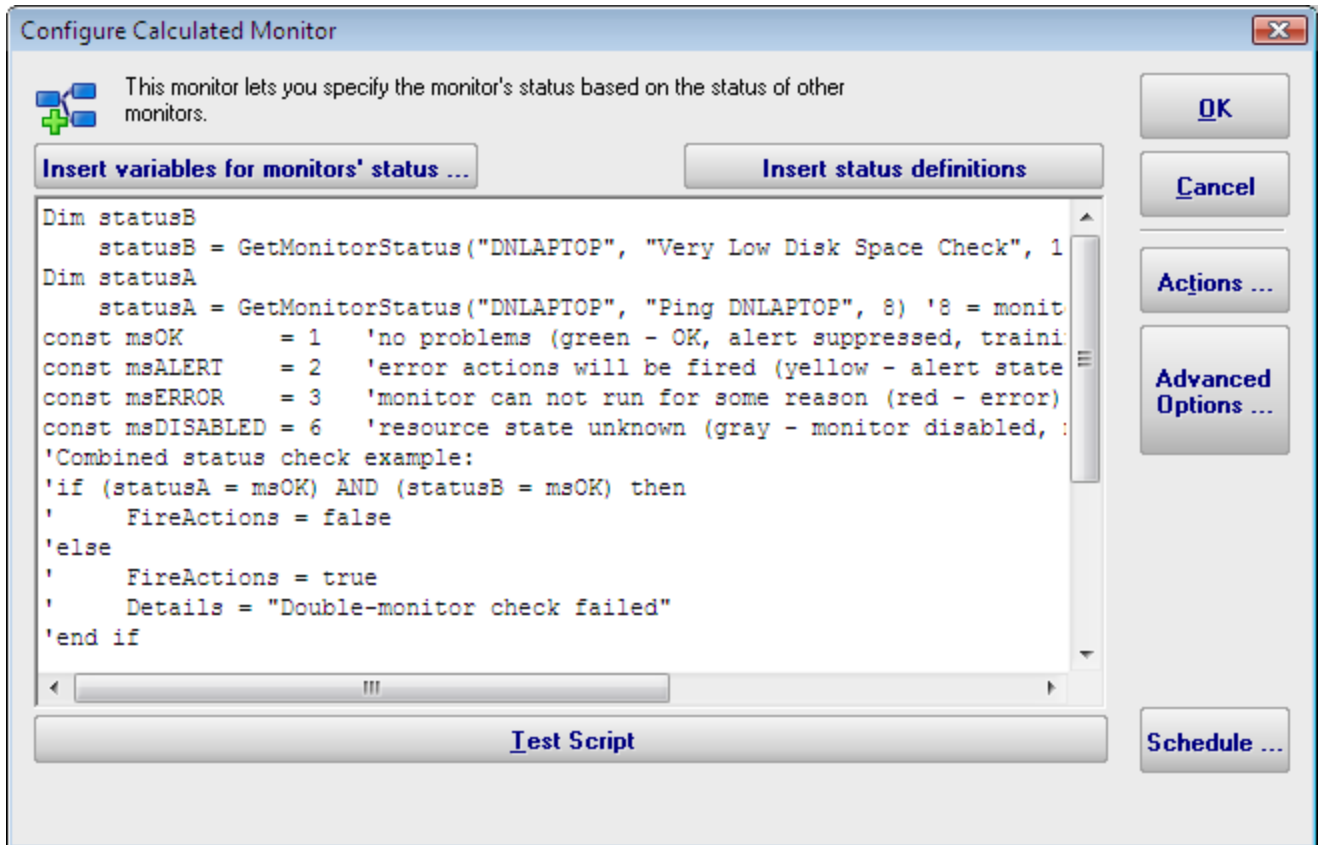
```
Dim statusB
statusB = GetMonitorStatus("DNVISTA", "Ping Backup Link", 7)
Dim statusA
statusA = GetMonitorStatus("DNVISTA", "Backup Failed Event Log Check", 2)

const msOK = 1 'no problems (green - OK, alert suppressed, training, etc)
const msALERT = 2 'error actions will be fired (yellow - alert state)
const msERROR = 3 'monitor can not run for some reason (red - error)
const msDISABLED = 6 'resource state unknown (gray - disabled, maintenance, etc)

'Combined status check example:
'if (statusA = msOK) AND (statusB = msOK) then
' FireActions = false
'else
' FireActions = true
' Details = "Double-monitor check failed"
'end if

'Opposite status example:
'if (statusA = msALERT) then
' FireActions = false
'else
' FireActions = true
' Details = "Put a detailed error message here"
'end if
```

In the example above, the GetMonitorStatus function gets the current status of the monitor listed in the parameters. The numbers 7 and 2 in the example are monitor types that are used internally. You don't need to guess what those values are -- if you want to operate on the status of a monitor, click the **Insert variables for monitors' status...** button. That will present a user interface where you can choose the monitor status to insert.



In the example script above, you'll also see definitions for msOK, msALERT, etc. If you accidentally delete those and need to get them back, press **Insert status definitions** and the code will be added back to your script.

In the example above, the "Ping Backup Link" is checking a backup link that should always be down, except when the primary link is down (in that case the backup should be up). That means we normally want the "Ping Backup Link" to be down (which would make it yellow in the status reports). Since this monitor is really just an input value, and we don't want it's normal yellow state to show yellow on all the status charts, it would make sense to go to that monitor, press Advanced Monitor Options, go to the Status tab, and indicate the monitor should always remain green.

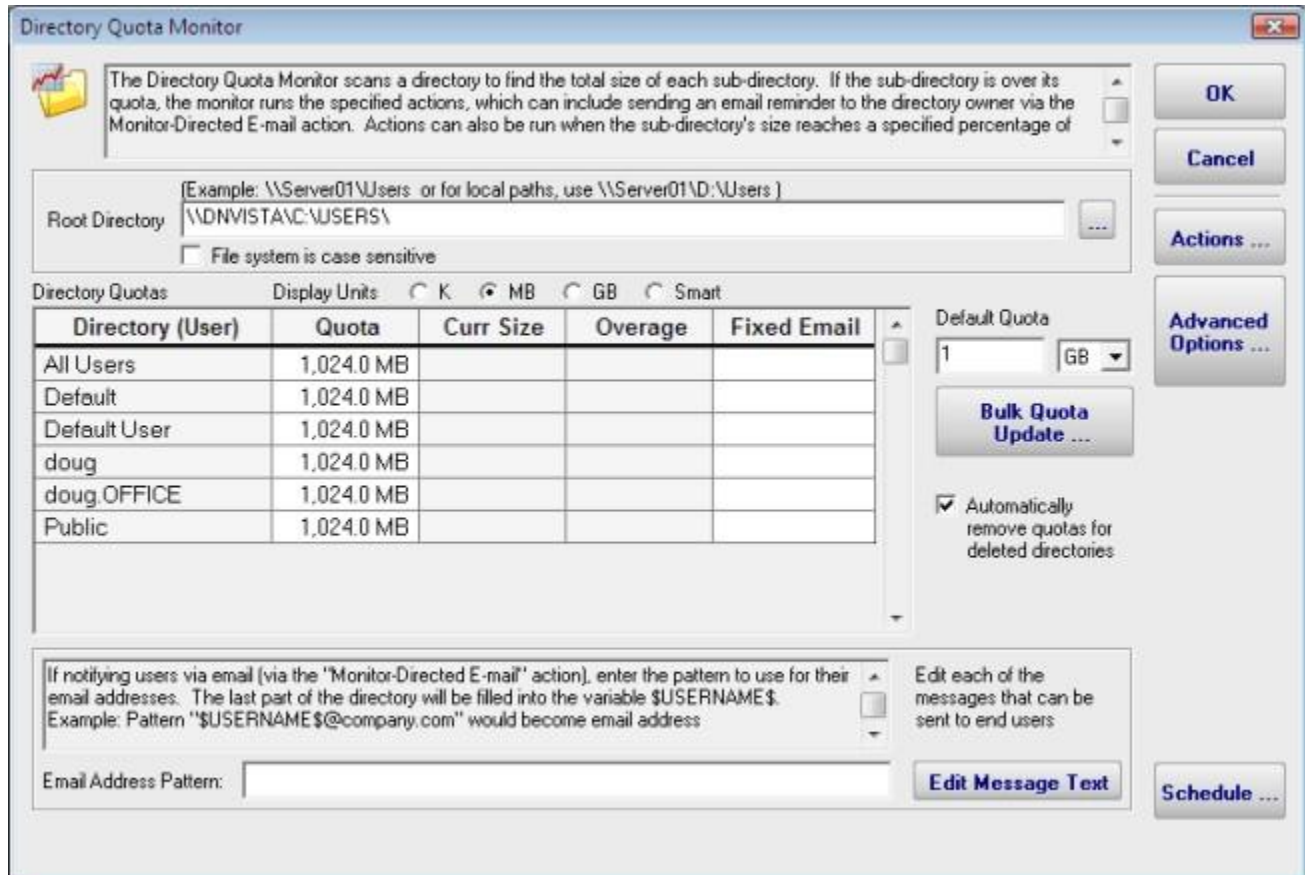
### Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for [Adding Actions](#), setting [Advanced Options](#) and setting the [Monitor Schedule](#).



## Directory Quota Monitor

The Directory Quota Monitor watches a the set of directories directly below a starting directory. Each sub-directory's total size is calculated (by summing up the sizes of all files in all sub-directories) and is then compared against the configured quota.



There are three ways to set the quota for each directory:




- Set the default quota which will be used for any directory that doesn't have a quota already specified (including new directories discovered during a scan)
- Manually enter quota values in the Quota column for any individual directory (specify units of K, MB or GB)
- Use the Bulk Quota Update mechanism which makes it easy to set many directories to quotas in a flexible way.

If you want end users (directory owners) to receive email quota reminders, be sure to add the Monitor Directed-Email action. The Directory Quota Monitor will need to determine an email address for each user to notify. You can either enter an email address for each directory in the Fixed Email column or create an Email Address Pattern for combining the directory name with some text to come up with an SMTP email address (this scenario assumes the directory name is closely related to a username). You can also edit the message that is sent to the user which can include simple replacement variables indicating quota sizes, directories, etc.

## Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for [Adding Actions](#), setting [Advanced Options](#) and setting the [Monitor Schedule](#).

## Supported Reports

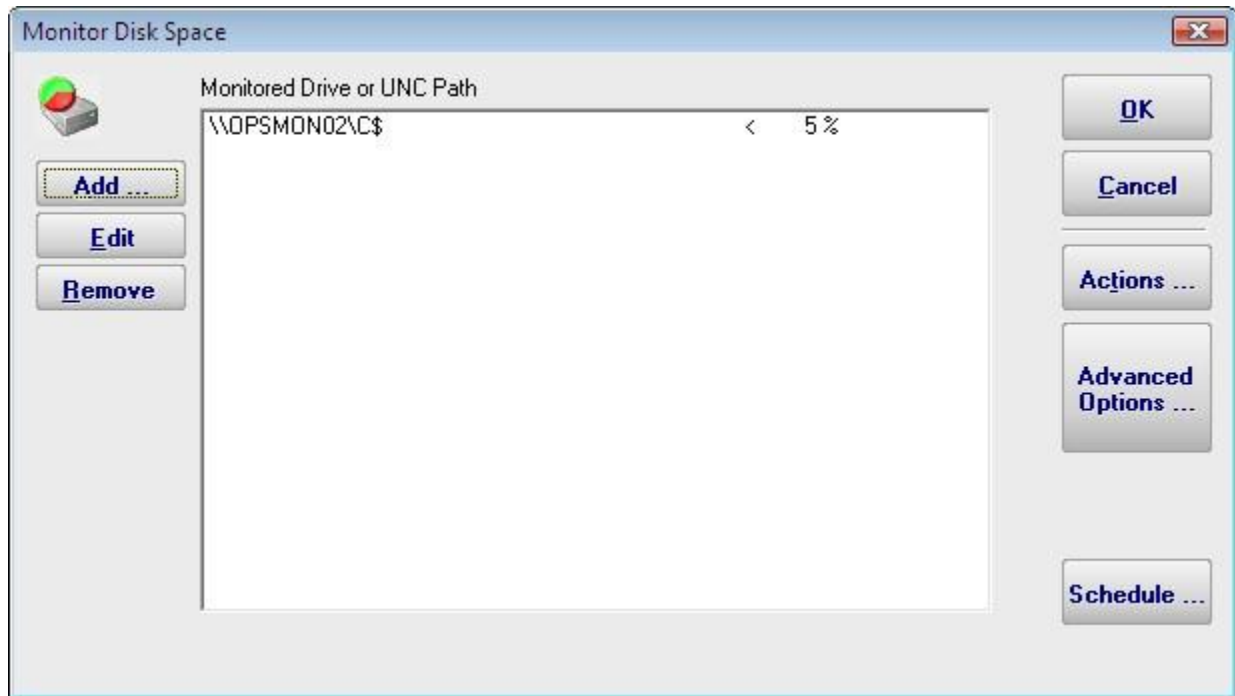
-  Directory Quotas
  -  Largest Directories
  -  Over Quota Directories

The monitor supports reports that detail which directories are over their quota, as well as the largest directories.

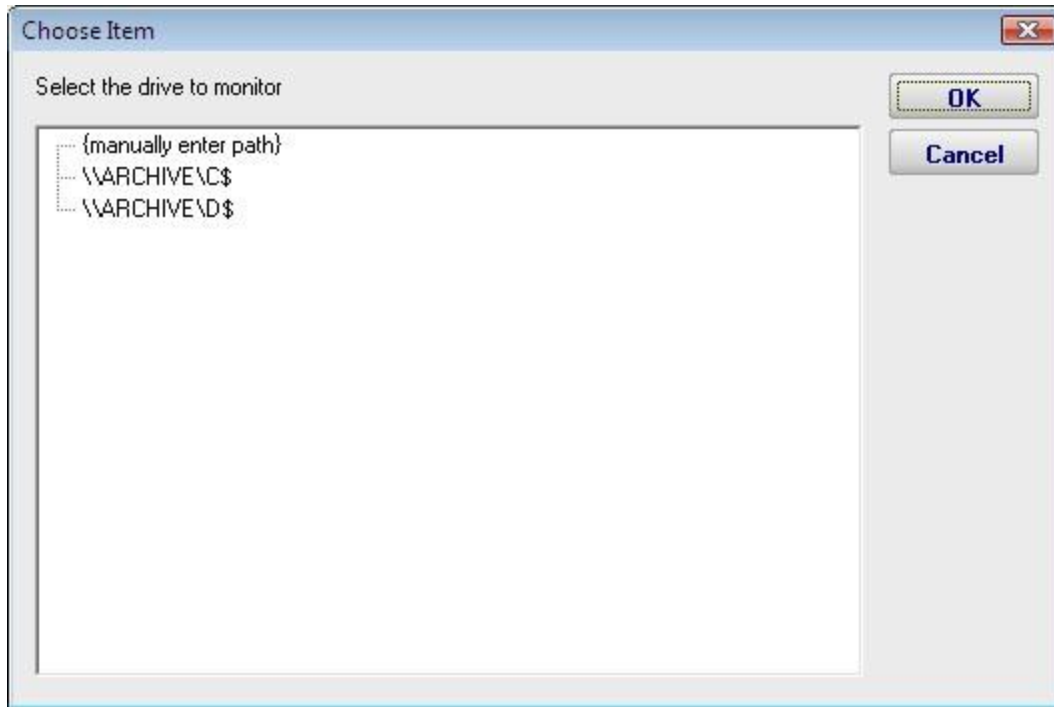
## Disk Space Monitor

The Disk Space monitor is simple to setup. You just add the drives that you want to monitor and the alert threshold (as an absolute size or as a percentage of the total disk size). You can also monitor specific folders if they are a volume mounted from another server / device.

The Add, Edit and Remove buttons on the left will let you change the disks that are being monitored.



Drives (volumes) on non-Windows machines are shown in the Add dialog as well. PA Storage Monitor uses SNMP behind the scenes to get drive information from the hrStorage table. If drive/volume information is not showing up, make sure that the correct [SNMP credentials](#) have been specified.



If a drive\share\volume that you want to monitor does not show up, choose {manually enter path}, and then enter the UNC path to be monitored on the next dialog.

When monitoring remote drives it is important to remember that the monitoring service will probably run as a different user than you are currently logged in with, and will most likely not have network drives mapped. The best way to specify a disk in this case is via UNC paths.

## Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for [Adding Actions](#), setting [Advanced Options](#) and setting the [Monitor Schedule](#).

## Supported Reports



The Disk Space monitor supports a number of disk space related reports. The Disk Space Summary is a good way to keep an eye on all disk space -- by default it shows a list of all servers with those with the least amount of free space at the top. Most of the reports can create bar and line charts, as well as tabular HTML and .CSV output.

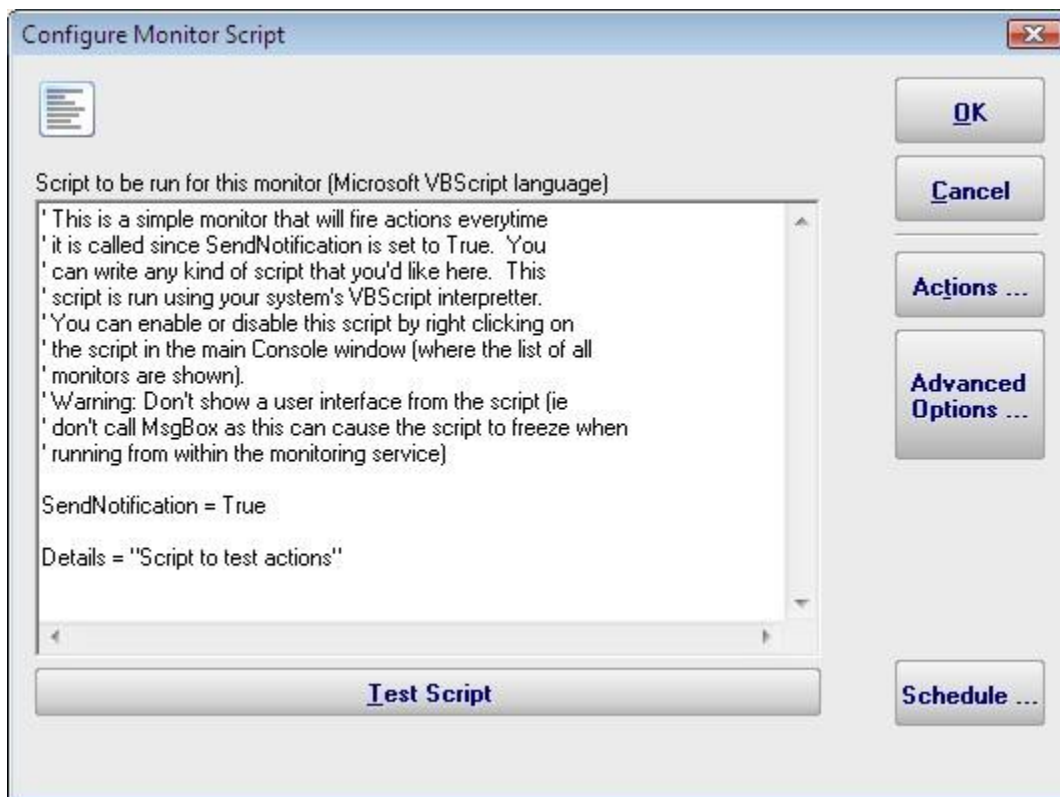
## Execute Script Monitor

The Execute Script Monitor allows you to write your own custom scripts in the VBScript language to check anything that your script can access. This monitor makes use of the VBScript engine that is already installed on nearly all Windows computers.

The script window is where you enter your VBScript. The script can do anything that can be done in VBScript (including creating external ActiveX/COM components) with all the standard restrictions.

The script has two global variables: *SendNotification* and *Details*. The script signals to the monitoring service that the configured actions should be fired by setting **SendNotification = True**. The **Details** variable can be set to any text, and that text will get passed to all configured actions.

Pressing the Test Script button will cause the script to be launched and run from the Console, and will report on the final state of the SendNotification variable. Note that the script will run as the currently logged on user when this button is clicked, but while running from within the monitoring service it will execute as the "run as" user for the service. This may or may not have an effect on the resources that the script can access.



### Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for [Adding Actions](#), setting [Advanced Options](#) and setting the [Monitor Schedule](#).

## Example Scripts

---

Below is an example script that checks a database connection:

```
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 "SELECT COUNT(*) FROM ", _
    objconnection, adOpenStatic, adLockOptimistic

If objrecordset.RecordCount <> 0 Then
    SendNotification = False
Else
    objrecordset.MoveFirst
    strDetails = "CODE RED !!!! No rows found!"
    SendNotification = True
End If

Details = strDetails
```

This next example checks to see if there are a certain number of files in a directory:

```
dim highCount
highCount = 1000
Set fso = CreateObject("Scripting.FileSystemObject")
Set oSrcFolder = fso.GetFolder("\\server\dir\tocheck")
fileCount = oSrcFolder.Files.Count

if fileCount > highCount then
    SendNotification = True
else
    SendNotification = False
end if
```

The last example script checks the size of a specific file:

```
FileToCheck = "C:\Files\Backup\dump.db"

Set objFSO = CreateObject("Scripting.FileSystemObject")

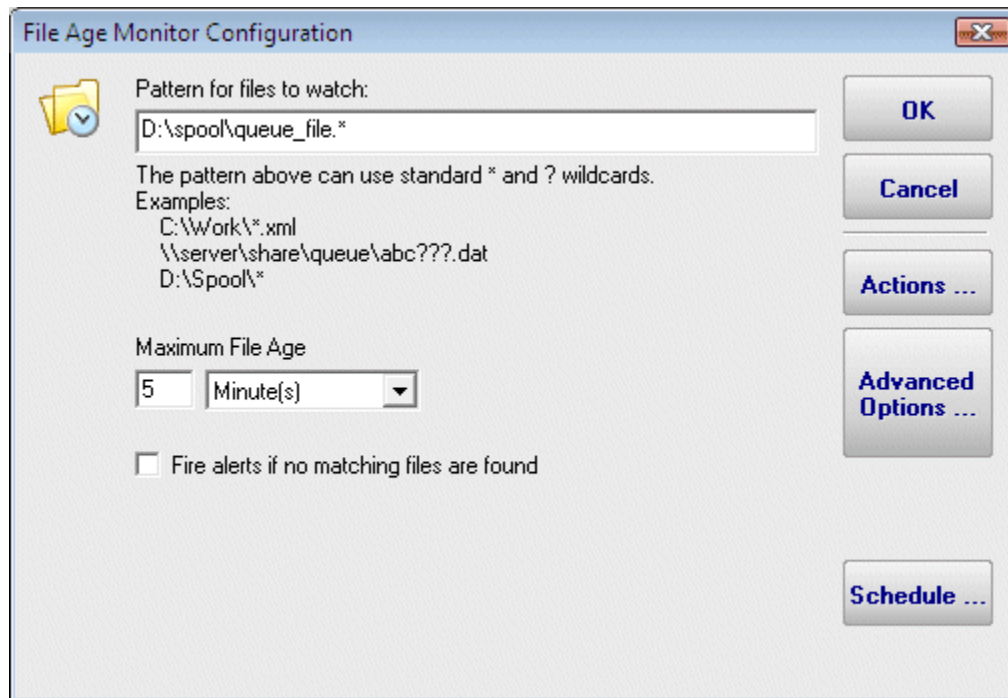
If objFSO.FileExists(FileToCheck) Then
    Set objFile = objFSO.GetFile(FileToCheck)
    If objFile.Size < 1000 Then
        SendNotification = True
        Details = FileToCheck & " is too small!"
    End If
End If
```

```
Else
    SendNotification = False
End If
Else
    SendNotification = True
    Details = FileToCheck & " does not exist!"
End If
```

## File Age Monitor

Configuring the File Age monitor consists of the following simple steps:

- Specify a pattern that defines which set of files will be watched. You may use wildcards in the file specification.
- Specify a maximum file age. The error state will be triggered if any files that match the pattern are older than the maximum file age.
- Indicate whether you want to be alerted if no matching files can be found.



### Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for [Adding Actions](#), setting [Advanced Options](#) and setting the [Monitor Schedule](#).



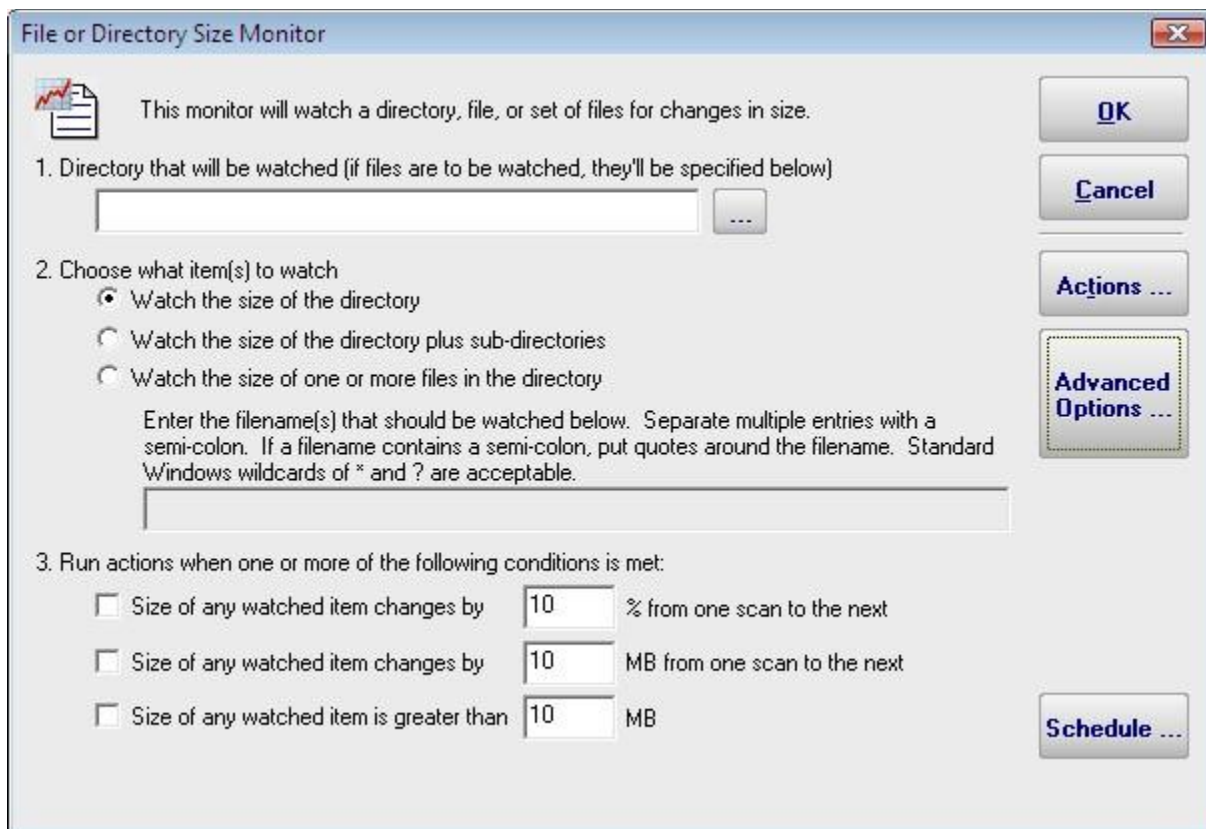
## File/Directory Size Monitor

The File/Directory Size Monitor is designed to watch an individual file, a set of files, or an individual directory and execute actions (such as notifying you) if it grows too large.

To specify what should be watched, first choose a starting directory. If you are watching remote files/directories, it is important to remember that the monitoring service will most likely not have access to shared drives, so use UNC paths.

Next you select whether a directory, directory with its child sub-directories, or a one or more files should be watched. To watch multiple files, use standard wild cards (ex: \*.db for instance).

Last you choose the growth conditions that should trigger the configured actions. They can include growth beyond a pre-set limit, or growth of a certain amount from one scan to the next.



The screenshot shows the 'File or Directory Size Monitor' dialog box. It has a title bar with a close button. The main area contains the following sections:

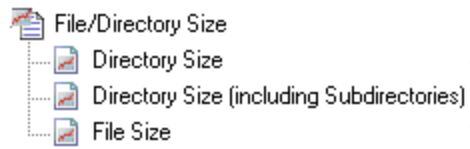
- 1. Directory that will be watched (if files are to be watched, they'll be specified below)**: A text input field with a browse button (...).
- 2. Choose what item(s) to watch**: Three radio button options:
  - Watch the size of the directory
  - Watch the size of the directory plus sub-directories
  - Watch the size of one or more files in the directoryA text input field below with instructions: "Enter the filename(s) that should be watched below. Separate multiple entries with a semi-colon. If a filename contains a semi-colon, put quotes around the filename. Standard Windows wildcards of \* and ? are acceptable."
- 3. Run actions when one or more of the following conditions is met:**: Three checkbox options, each with a numeric input field:
  - Size of any watched item changes by  % from one scan to the next
  - Size of any watched item changes by  MB from one scan to the next
  - Size of any watched item is greater than  MB

On the right side, there are four buttons: 'OK', 'Cancel', 'Actions ...', and 'Advanced Options ...'. At the bottom right, there is a 'Schedule ...' button.

### Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for [Adding Actions](#), setting [Advanced Options](#) and setting the [Monitor Schedule](#).

## Supported Reports

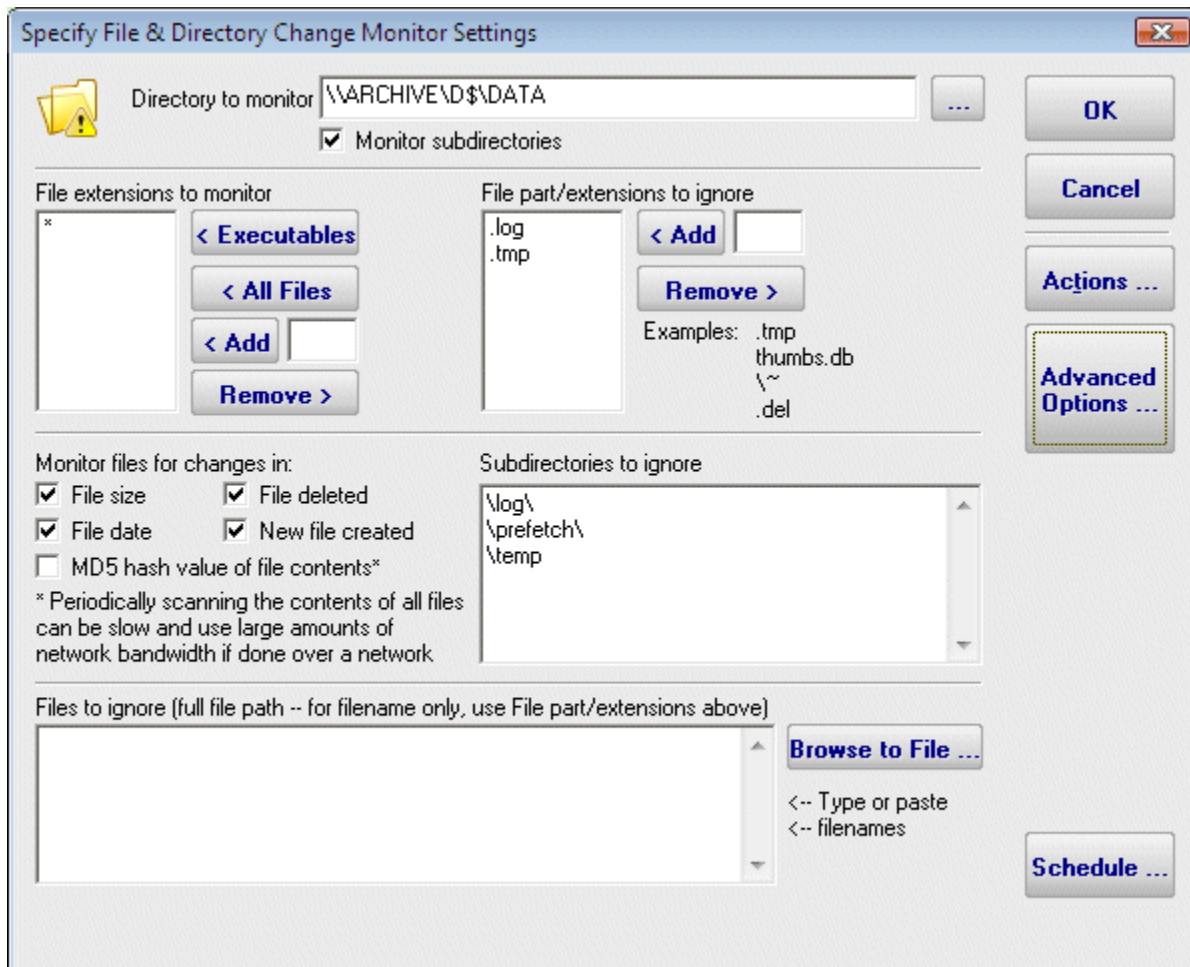


When this monitor runs, it records the measured value (directory size, directory size plus subdirectories, or file size) into a database. Those values can be charted or output to a .CSV file or tabular HTML report. You can specify the date range as well as summarization level (hourly, daily, weekly, monthly).

## File & Directory Change Monitor

The File & Directory Change Monitor is a very powerful monitor that can watch changes to files and directories on a server including file and directory creation and deletion. It can aid you in keeping track of changes to your systems, and even act as an intrusion detection system. In particular, this monitor can help fulfill the requirements of several mandated security practices, such as the ["Payment Card Industry Data Security Standard"](#) (part 11.5).

When configuring the File & Directory Change Monitor, specify the starting directory and whether the subdirectories should also be checked. If the directory is not local to the computer, using UNC paths is required since mapped drives are usually not available to the service when it runs.



You can specify which file types (by file extension) should be monitored. There are buttons that let you quickly add common executable file types, all files, or you can manually add individual file types that you care about.

If you select All Files in above, you can then filter out certain file types by extension. For example, knowing that temporary (.tmp) files have changed is often not helpful.

The Monitor Files For Changes area of the dialog is where you specify what aspects of the files and directories you'd like to monitor. If you select File Contents the file is opened and its entire contents are read and a checksum is generated for later comparison. This can be

resource intensive, and should generally only be done for the smallest subset of files that will accomplish your needs.

If you indicate that subdirectories should be monitored, you have the ability to filter out some of the subdirectories. The pattern-matching algorithm is very simple: Before a path is scanned, a backslash "\" is appended to the end of the path. Then the list of ignored directories is scanned and if the text of any ignored directory can be completely found within the path to be scanned, that directory (and all of its subdirectories) is skipped. The check is not case sensitive.

Some files are always changing (some system files for example), but not enough that you can ignore all files of that extension. You can specify individual files to ignore during the scan.

### About "Files to ignore" and Training

"Files to ignore" is a text box in which you can enter the names of files that are to be ignored by the File and Directory Change Monitor. This feature operates in conjunction with the Training feature in order to customize the behavior of PA Storage Monitor easily.

Training is a powerful feature available on many monitors. With the File & Directory Change monitor, the monitor will watch for changes over a period of time. Everything that changes within that period of time is automatically added to the Files to Ignore list.





After the training period ends, the monitor automatically switches into its normal scanning pattern.

Because "Files to ignore" is a text box, you can remove any files or add new files as you require by editing the list of files by hand.

### Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for [Adding Actions](#), setting [Advanced Options](#) and setting the [Monitor Schedule](#).

### Supported Reports

 File & Directory Changes	All file and directory changes that can be alerted on are also recorded to a database. This database allows you to run reports on types of changes, changes to particular files or directories, etc.
 Change Type	
 Changed Files	
 Changes to File	

## File System Analyzer

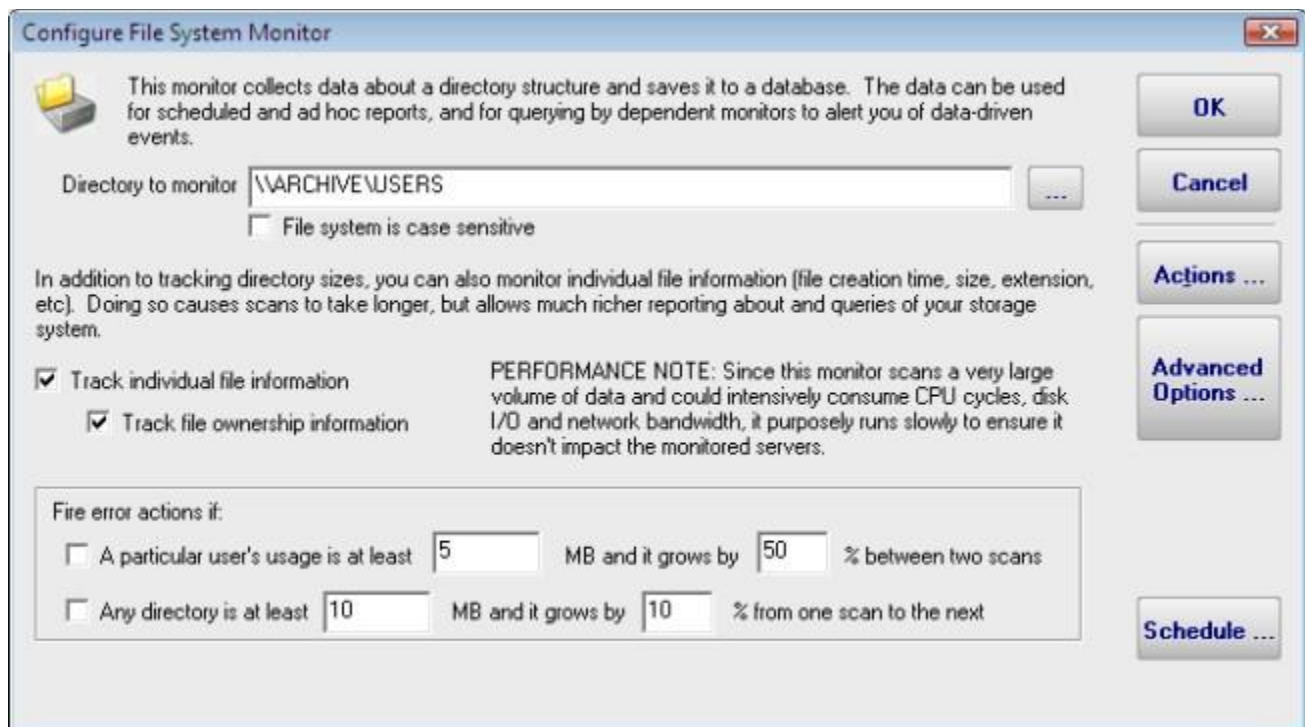
The File System Analyzer is a very powerful monitor that inspects a volume (local drive, network drive, etc) and records information about each directory, and optionally each file and file owner. Very rich reports are possible including:

- Directory growth over time
- Duplicate files on the file system
- File age, size and type distribution
- Largest files
- Largest storage users
- Custom file searches by name, type, age, size, owner, etc
- and more...

The data sets generated by the File System Analyzer can also be consumed by the User Quota monitor.

Configuring the File System Analyzer is as easy as selecting a starting directory and deciding how much information you would like to store in the local database. You can keep multiple data sets.

Scanning an entire file system, especially a large file system over a network can take a considerable amount of CPU, network bandwidth and disk I/O. In order to not impact the performance of the monitored file system server, the File System Analyzer throttles its scans. The trade off is that scans of a very large file system can take a few hours. Typically this isn't a problem because you can create automated reports, and optionally have the report URL emailed to you when the report is ready.

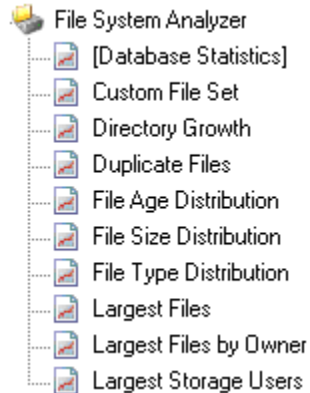


The File System Analyzer has some basic alerting on usage growth, but most users tend to use this monitor almost exclusively for its reporting power.

## Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for [Adding Actions](#), setting [Advanced Options](#) and setting the [Monitor Schedule](#).

## Supported Reports



The power in the File System Analyzer is in its reports. As you can see to the left, there are a wide variety of report types available.

- Database Statistics - general information about how much data and what type is stored in the database
- Custom File Set - a powerful report that will let you specify the types of files that you want to find base on age, file type, file owner, size, etc.
- Directory Growth - a popular report that shows the size of directories over time, with an optional percent change column between them
- Duplicate Files - useful for finding files that have the exact same name, size and date across a volume
- File Age Distribution - breaks down the ages of files into days, months and years old. Age is based on Last Accessed, Last Modified or Create Date
- File Size Distribution - breaks files into different size categories to help you understand what is being stored
- File Type Distribution - useful for finding out what types of files are using the most space on your servers
- Largest Files - finds the largest files that have been scanned
- Largest Files by Owner - displays the largest files that each person owns (based on file owner property)
- Largest Storage Users - shows you who is using the most space on the storage volume (based on file owner property)

## User Quota Monitor

User Quota Monitor is built to look at how much space each user is taking up on a volume and comparing that against their quota. If they are over the quota, actions get fired. The Directed-Email Action is especially useful in this case since it can send clean up reminders to the end users.

The User Quota Monitor inspects data sets collected by the File System Analyzer. This will make sense when you notice that you specify where you want the quotas to be checked by selecting an existing File System Analyzer data set. By doing this, the User Quota Monitor becomes dependent on the File System Analyzer, and is automatically run when at the end of the analysis (note that this monitor does not have the means to select its scan period--it runs after each run of the selected File System Analyzer).

Configuration of this monitor works best by letting the File System Analyzer complete one scan first. That way the User and Curr Size columns will be filled in automatically.

The User Quota Monitor scans data collected by the File System Analyzer and monitor individual users' disk usage as compared to their quota. If a user is over quota, the monitor runs the specified actions, which can include sending an email reminder to the user via the Monitor-Directed E-mail action.

Select the File System Analyzer data set to monitor (it must have File Owner tracking on)

Default Quota: 1 GB

Bulk Quota Update ...

User Quotas

Display Units:  K  MB  GB  Smart

User	Quota	Curr Size	Overage	Fixed Email
ARCHIVE\BACKUP	1,024.0 MB	12,496.7 MB	11,472.7 MB	
BUILTIN\ADMINISTRATOR	1,024.0 MB	103,635.1 MB	102,611.1 MB	
OFFICE\CHELSEA	1,024.0 MB	28.4 MB		
OFFICE\DANA	1,024.0 MB	1.6 MB		
OFFICE\JOSH	1,024.0 MB	6.2 MB		
OFFICE\TRAVIS	1,024.0 MB	10.0 MB		

If notifying users via email (via the 'Monitor-Directed E-mail' action), enter the pattern to use for their email addresses. The variable \$USERNAME\$ can be used in the pattern.

Edit each of the messages that can be sent to end users

Email Address Pattern:

Edit Message Text

OK

Cancel

Actions ...

Advanced Options ...

This monitor will run directly after the target File System Analyzer runs.

There are three ways to set the quota for each user:

1. Set the default quota which will be used for any user that doesn't have a quota already specified
2. Manually enter quota values in the Quota column for any individual user (specify units of K, MB or GB)
3. Use the Bulk Quota Update mechanism which makes it easy to set many users to quotas in a flexible way.

If you want the users to receive email quota reminders, be sure to add the Monitor Directed-Email action. The User Quota Monitor will need to determine an email address for each user to notify. You can either enter an email address for each user in the Fixed Email column or create an Email Address Pattern for combining the username with some text to come up with an SMTP email address. You can also edit the message that is sent to the user which can include simple replacement variables indicating quota sizes, directories, etc.

### Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for [Adding Actions](#) and setting [Advanced Options](#).



## Actions

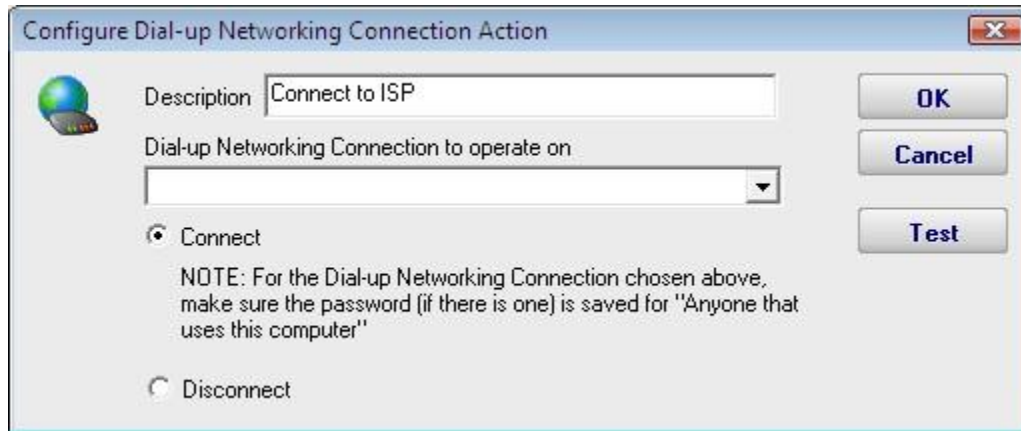
---

[Contents](#)

### Dial-up Connection Action

---

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



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

Dial Cancel Properties Help

## 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 Storage Monitor 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.

**Configure Email Notification**

Email Address: ops@xyzcorp.com, john@xyzcorp.com  
 (Multiple addresses can be comma separated)

**Advanced Options ...**

---

**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      **Test Primary Server**

From Address (ex 123@xyz.com): alerts@xyzcorp.com      Encryption: Don't Know

Optional

Username for SMTP Server: example\_user

Password for SMTP Server: [REDACTED]

Retype password: [REDACTED]

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: [REDACTED]      Port: 25      **Test Backup Server**

Optional

From Address: [REDACTED]

Username for SMTP Server: [REDACTED]

Password for SMTP Server: [REDACTED]

Retype password: [REDACTED]

Buttons: OK, Cancel, Message ..., Schedule ...

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.

**Advanced Email Options**

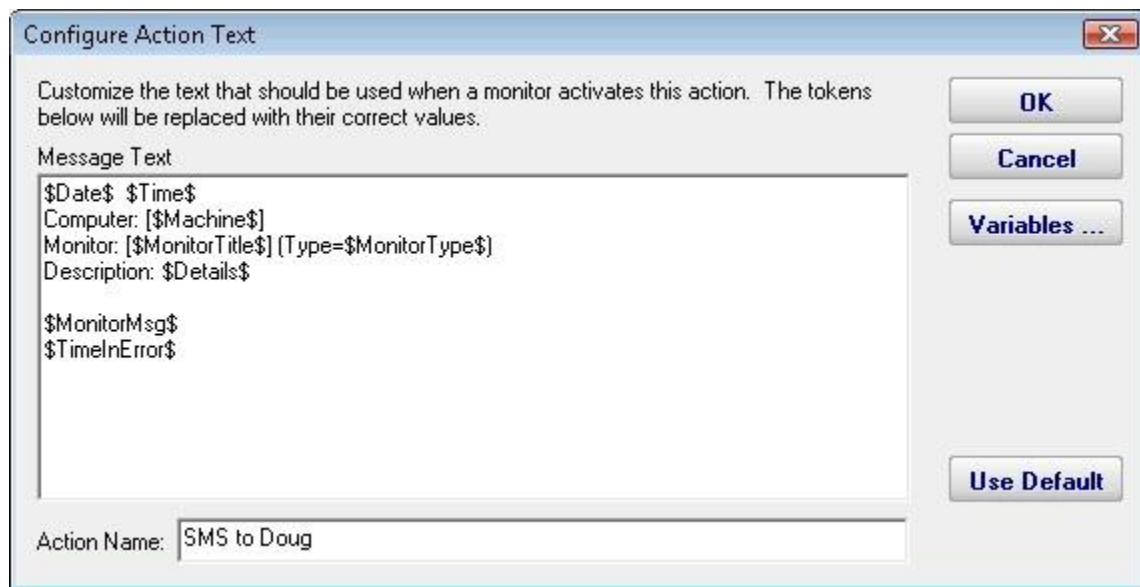
These advanced options only apply to this email action.

- 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)

Buttons: OK, Cancel

- 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 Storage Monitor to send the message out using all other configured notification mechanisms. Only notification actions (like SMS, Pager, etc) will be 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 Storage Monitor 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.



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.

OK

Green squares indicate hours when this activity can be activated.

Set All

Clear All

Cancel

	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																								

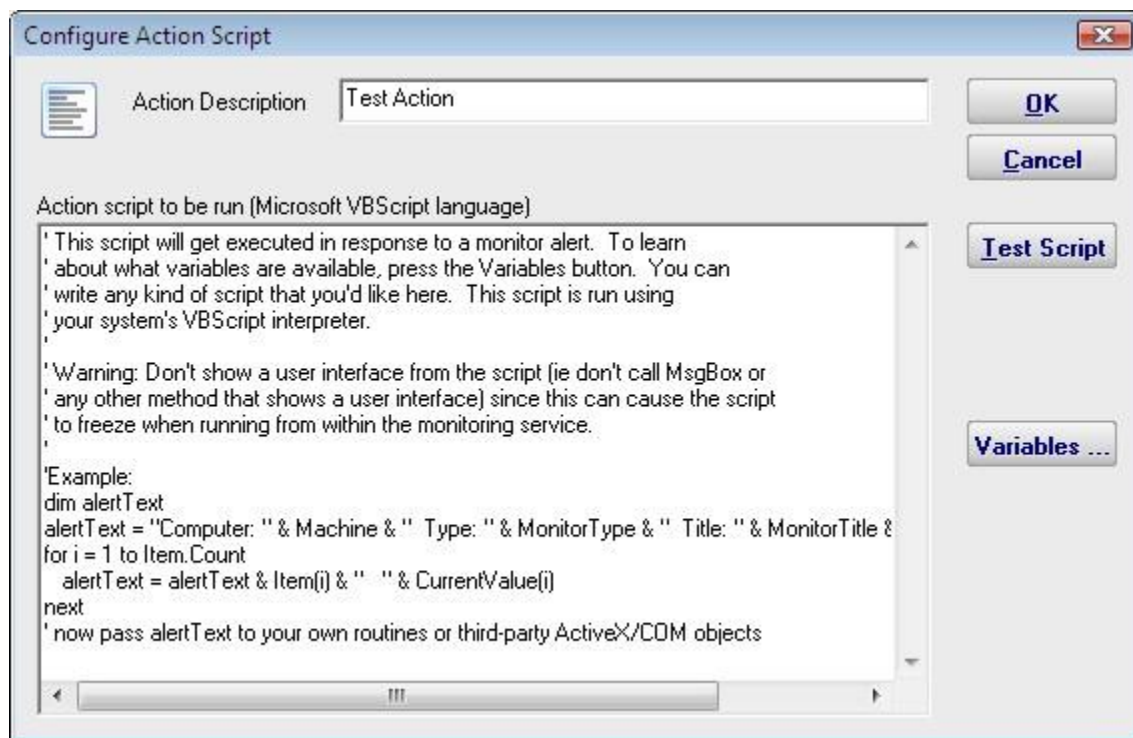
## Execute Script Action

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).



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
```

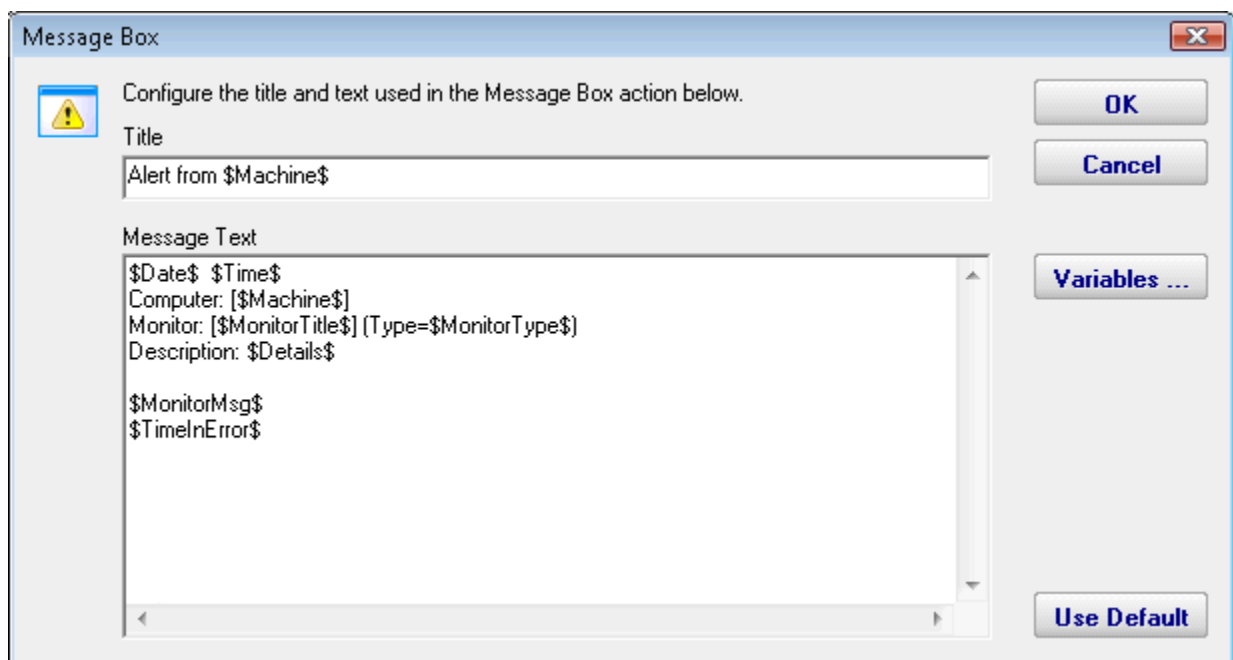


## Message Box Action

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 Storage Monitor 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.



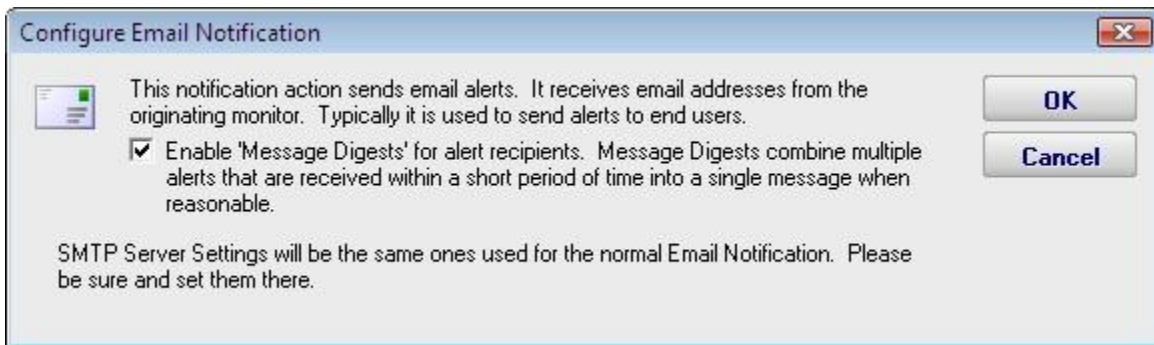
## Directed-Email Action

The Directed-Email Action is similar to the E-mail Message Action in that it sends SMTP email messages with the alert text in the message body. What makes it different is that the monitor that calls this action specifies who the emails should be sent to (instead of the email address being set at configuration time).

This action is typically used with monitors where end users might need to receive alerts (like the various Quota monitors for example).

Like the E-mail Message Action, the Directed-Email Action also supports Message Digests. Message Digests combine all messages that arrive within a short amount of time for a email address into a single message.

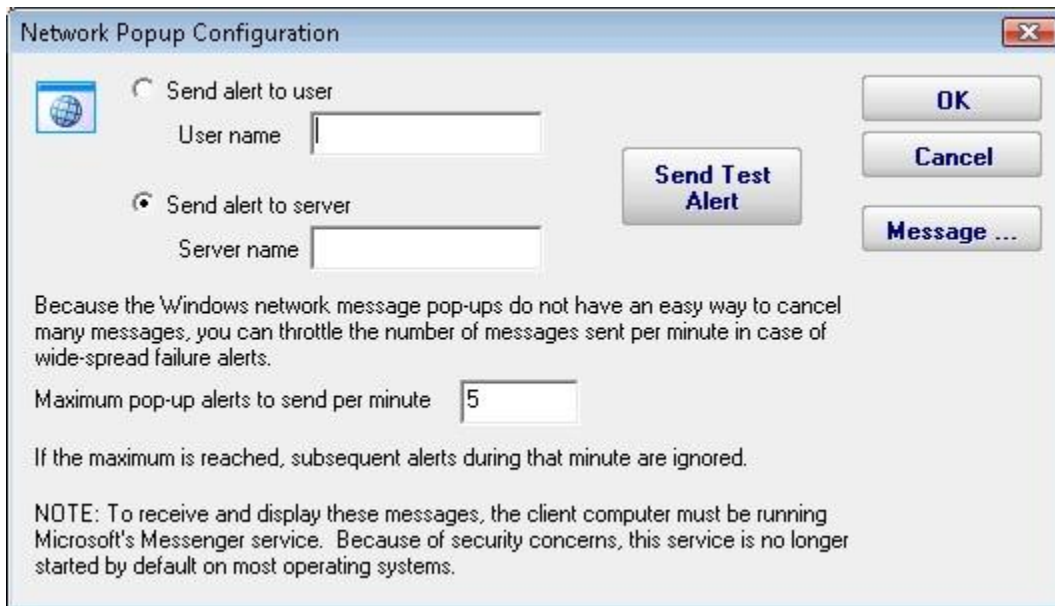
A primary and backup SMTP server can be specified to help ensure the message gets through. The main SMTP server (the first one listed) is required. The backup SMTP server is optional. One final note: The SMTP servers entered here are shared among all Directed-Email and E-mail Message actions.



## Network Message Action

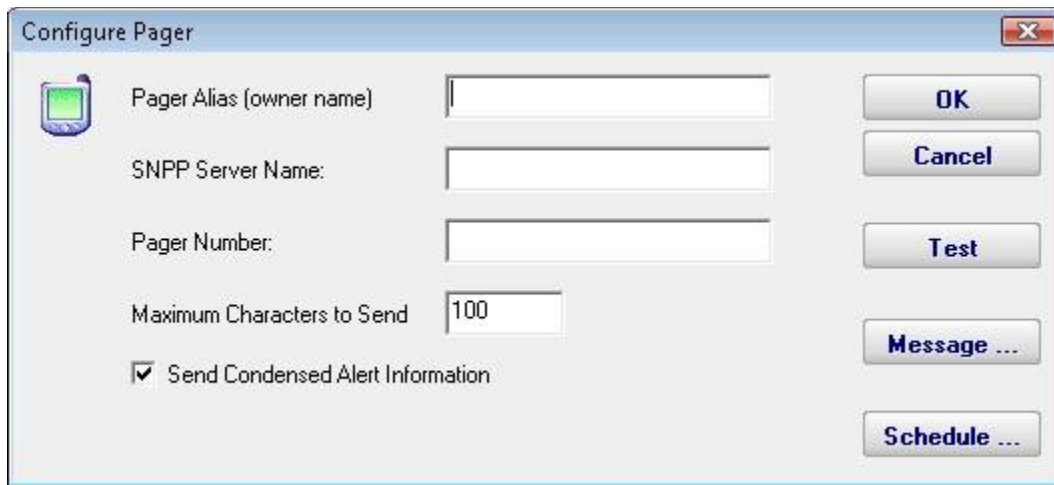
The Network Message Action is equivalent to doing a "net send" from the command line. It allows you to direct a message box pop-up to any particular user or computer on the network.

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 Pager Alert Action

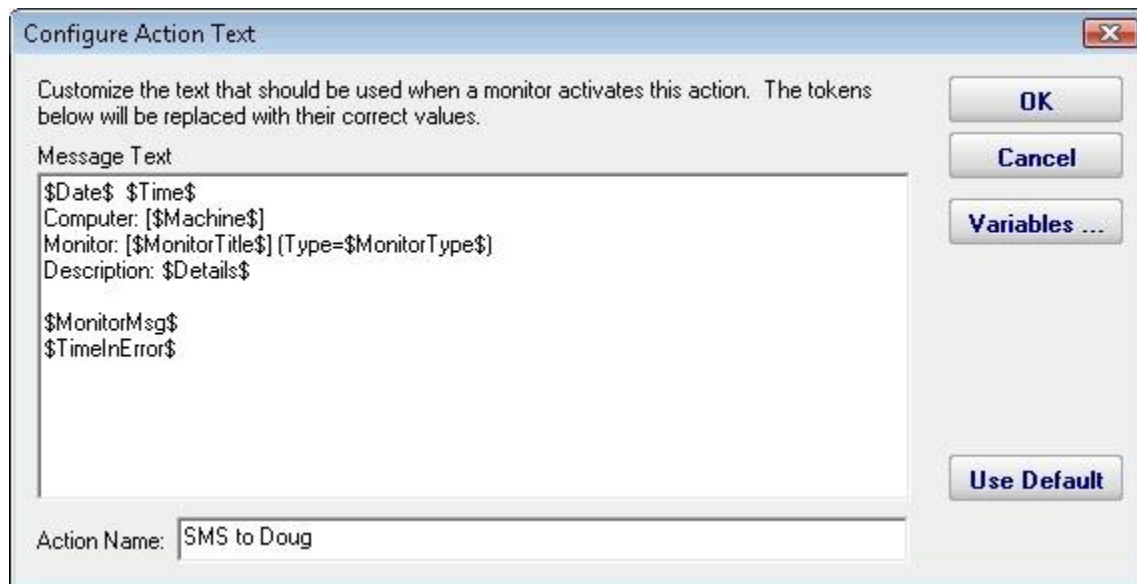
The Send Pager Alert action can send monitor details to an SNPP pager.



The 'Configure Pager' dialog box contains the following fields and buttons:

- Pager Alias (owner name):** A text input field.
- SNPP Server Name:** A text input field.
- Pager Number:** A text input field.
- Maximum Characters to Send:** A text input field with the value '100'.
- Send Condensed Alert Information**
- Buttons:** OK, Cancel, Test, Message ..., and Schedule ...

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.



The 'Configure Action Text' dialog box contains the following elements:

- Instruction:** 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:** A text area containing the following tokens:
  - \$Date\$ \$Time\$
  - Computer: [\$Machine\$]
  - Monitor: [\$MonitorTitle\$] (Type=\$MonitorType\$)
  - Description: \$Details\$
  
  - \$MonitorMsg\$
  - \$TimeInError\$
- Buttons:** OK, Cancel, Variables ..., and Use Default
- Action Name:** A text input field with the value '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'.

### 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.

OK

Green squares indicate hours when this activity can be activated.

Set All

Clear All

Cancel

	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:

Phone number to dial:

Seconds to pause after dialing above number:

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

Seconds to wait before hanging up:

Complete command to send to modem:

Allow editing of command directly

OK  
Cancel  
Schedule ...  
Test  
Variables ...

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}

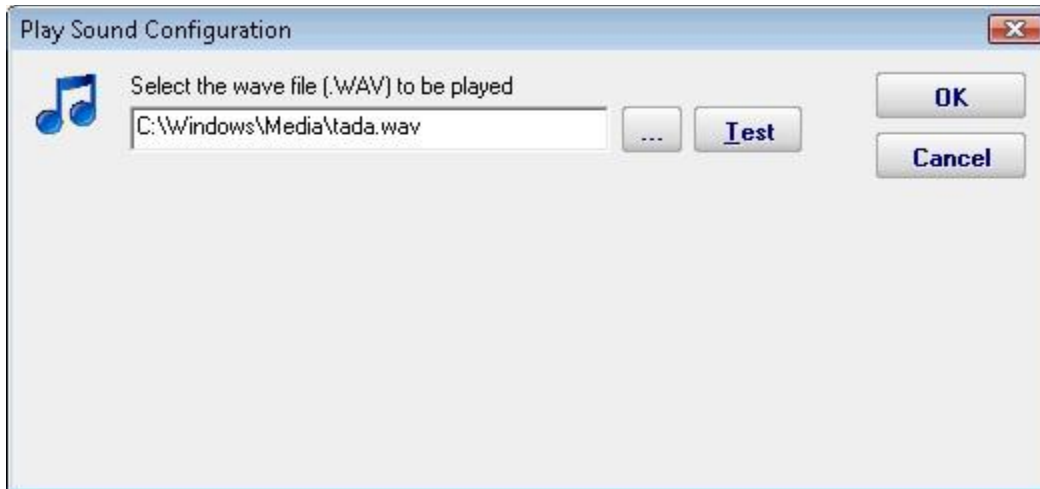
The modem script is shown at the bottom of the dialog, and will work with most modems since it is built on the basic Hayes AT command set. Your modem may have other features and/or require other commands. Your modem documentation will list the commands it accepts. If you need to modify the script to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

## Play Sound File Action

---

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

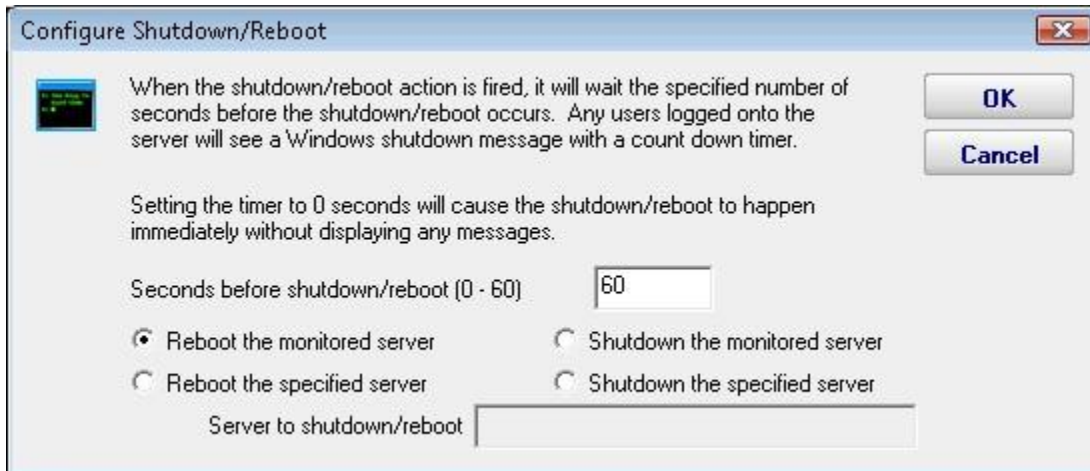




## Reboot Computer Action

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.



## SMS Text Message Action

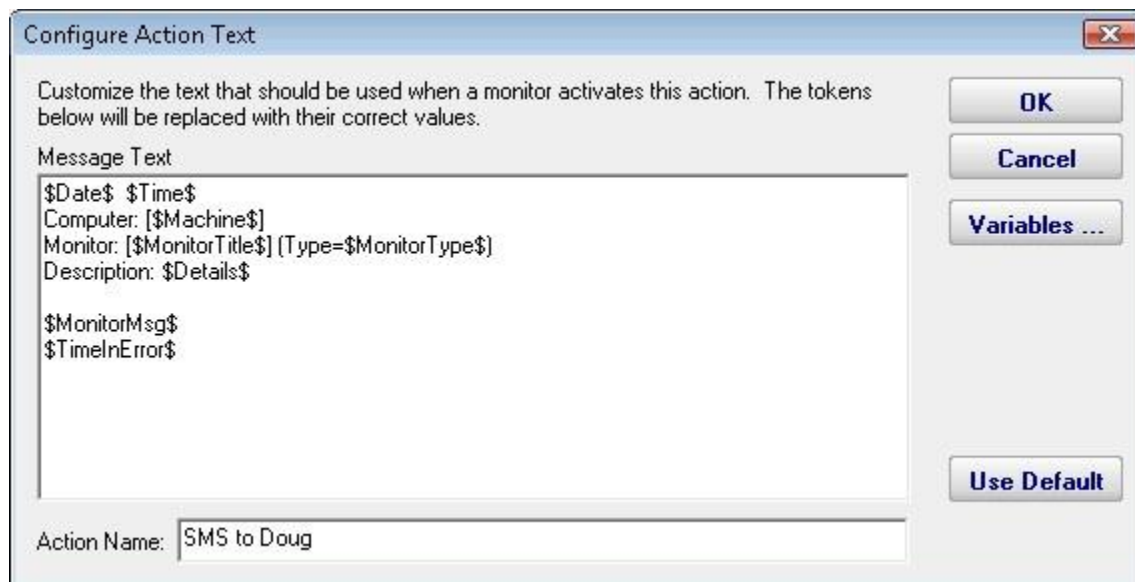
This action can send alert messages via SMS to your phone or mobile device. The message is sent through an SMS Gateway via the SMPP protocol.



The 'Configure SMS Alert Destination' dialog box contains the following fields and buttons:

SMS Device Owner	Doug	OK
SMS Gateway Server	serviceprovider.gatewayserver.com	Cancel
Gateway Server Port	2775	SMS Hints
System Type (if needed)		Test
Device Address/Number	1234567890	Message ...
Username (if needed)	1234567	Schedule ...
Password (if needed)	xxxxxxxx	
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.



The 'Configure Action Text' dialog box contains the following fields and buttons:

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

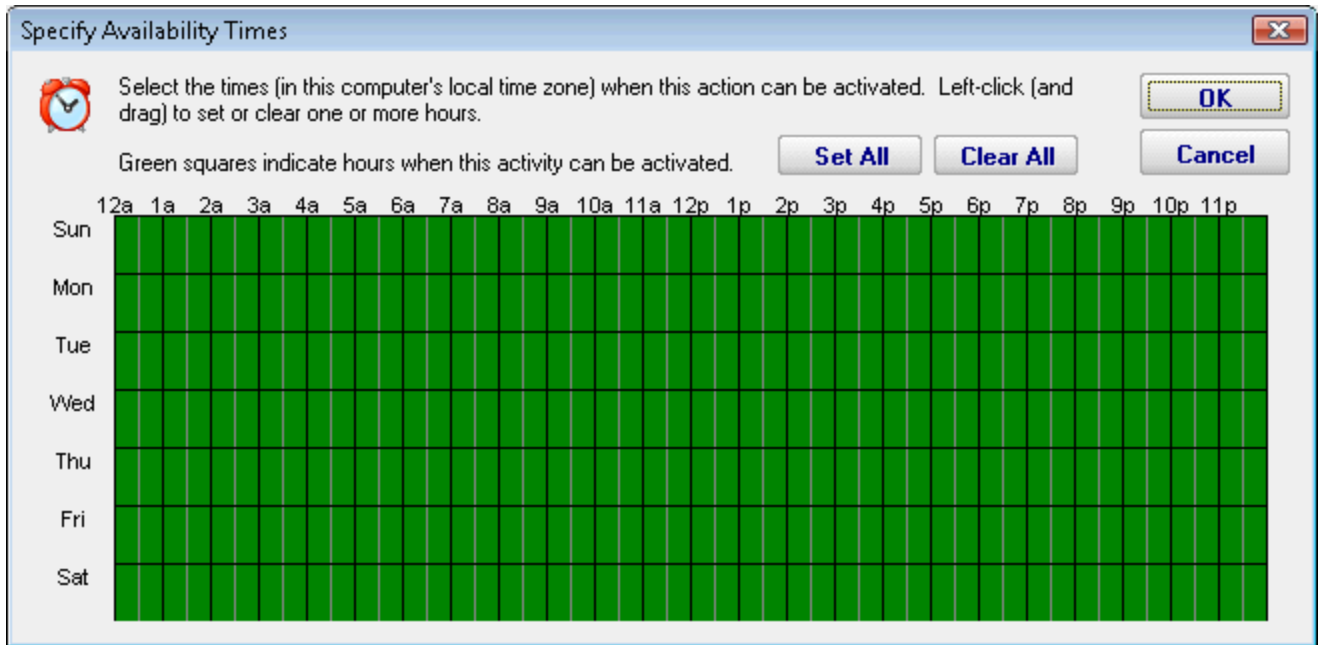
Message Text

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

Action Name: SMS to Doug

Buttons: OK, Cancel, Variables ..., Use Default

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'.



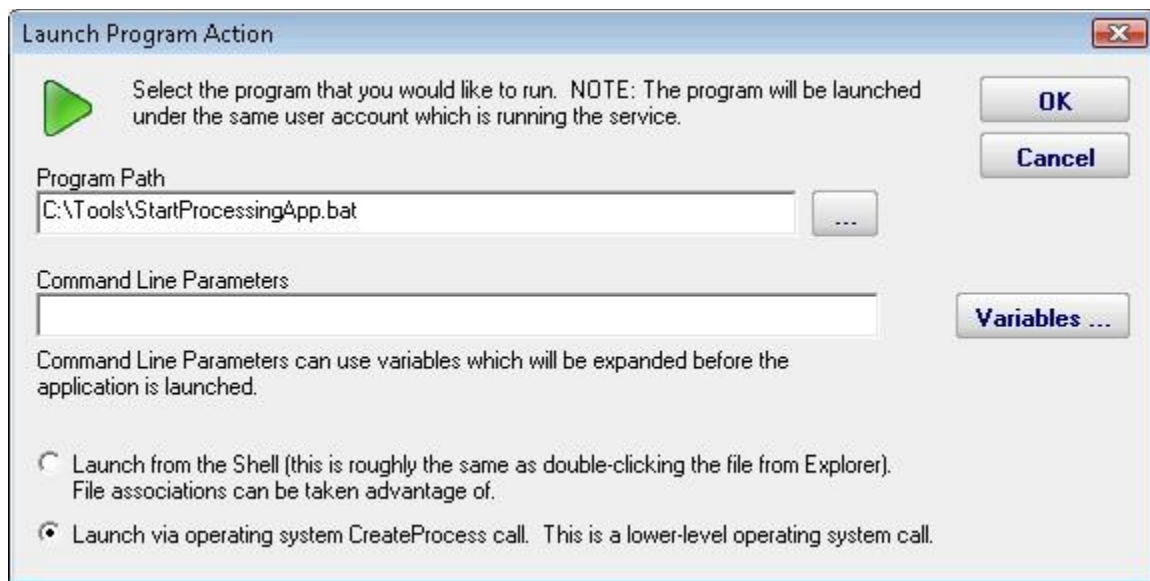
Also note that we have an FAQ on other ways to send alerts to phones and pagers at: [SMS Hints](#)

## 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.

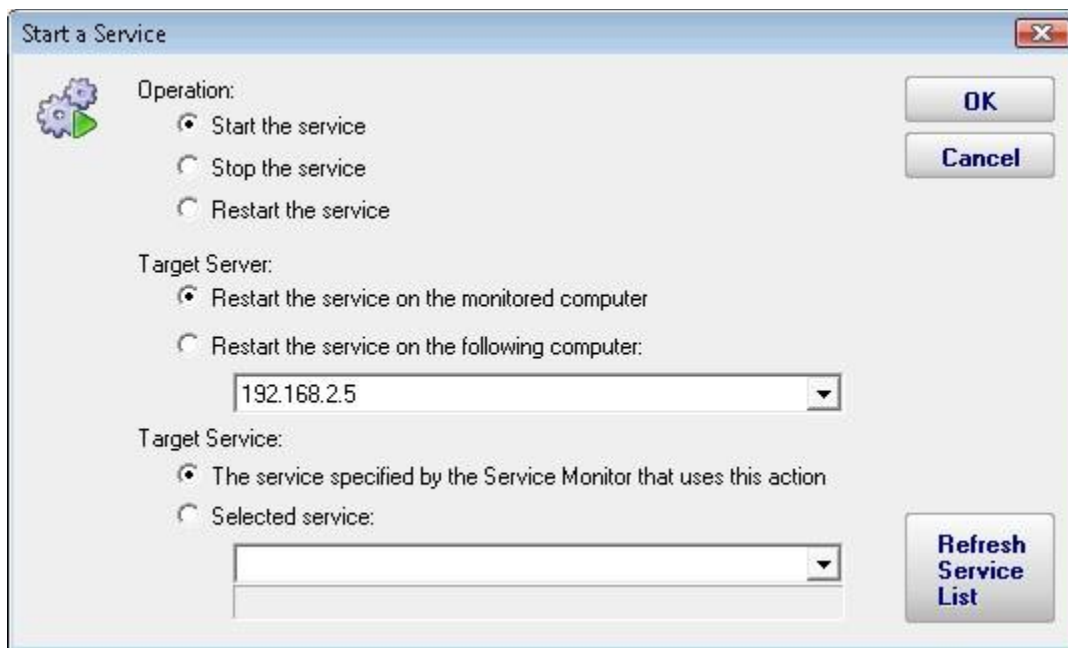
One final note: The application is started on the local computer (where the monitoring service is being run), not on any remote computer that might be monitored at that time. To launch an application on a remote machine, we recommend having the Start Application Action run Microsoft's PsExec, and direct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



## 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.

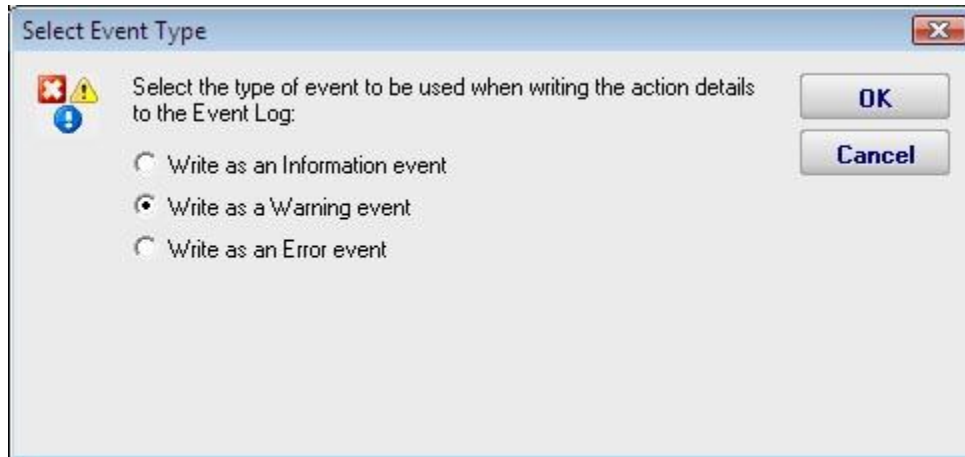
The action can be configured to restart a specific service on a specific computer, or if attached to a Server Monitor, it can restart which ever service has stopped as reported by that monitor.



## Write to Event Log Action

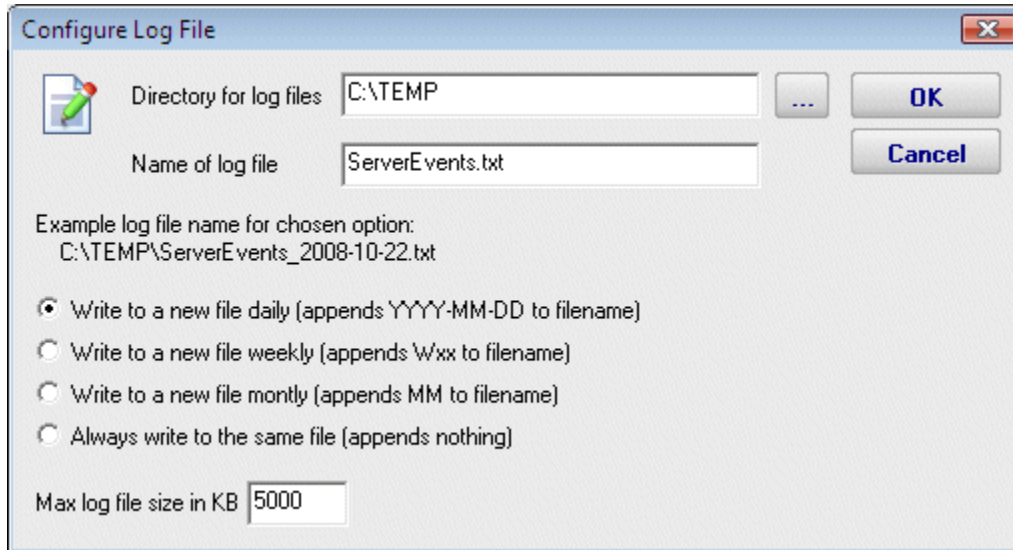
---

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.



## 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.



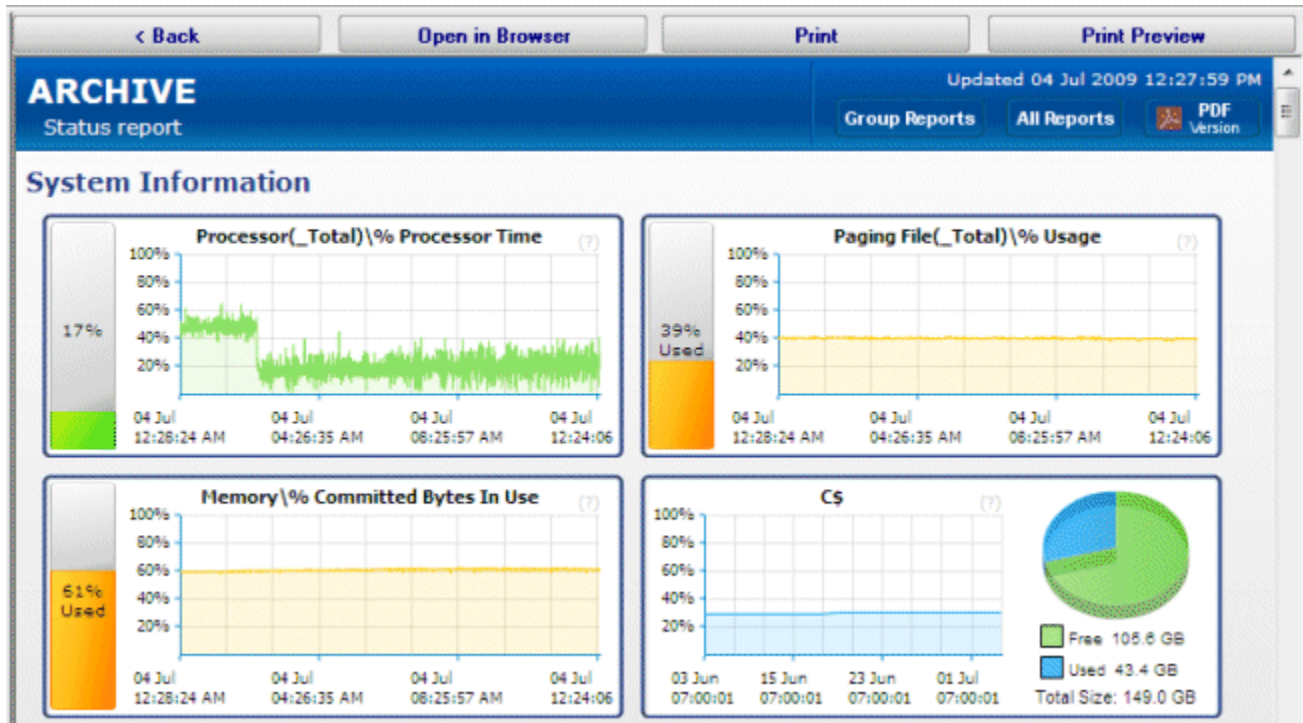
# Reports

[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.



[< Back](#)    [Open in Browser](#)    [Print](#)    [Print Preview](#)

---

### 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

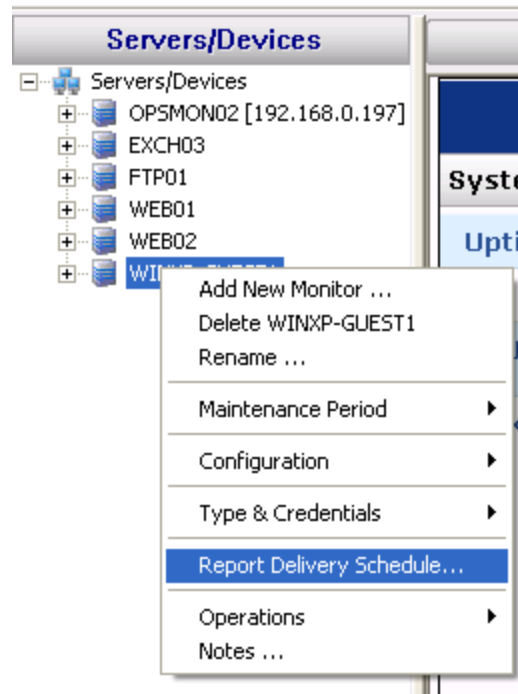
Err Ti...	Monitor	Details	OK Ti...	Ack
2 Jul 2009 5:20:31 pm	Monitor services on ARCH...	The service "Performance Logs and Alerts" is not running on computer ARCHIVE		<input type="checkbox"/>
2 Jul 2009 4:18:30 pm	Monitor services on ARCH...	The service "Microsoft Software Shadow Copy Provider" is not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

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.



## Group Summary Report

The Group Summary Report is a great way to get a detailed view of many servers at once. Like all group-based reports, there is a grey menu bar at the top that will take you to the other reports for the current group. Below and to the right is a button to go to an index of all reports, and a button to get a PDF of the report as it looks currently.

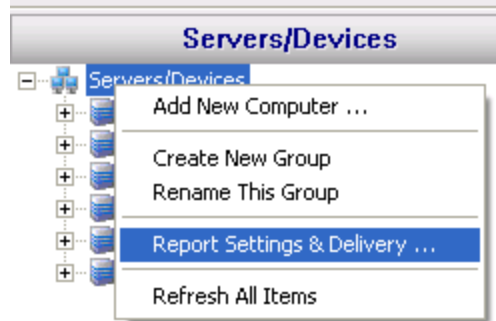
Next are two small tables indicating the number of servers and monitors that are OK (green), in Alert state (yellow), in error (red), or disabled/maintenance/etc (grey). A server is red if there is at least one monitor that is red, or yellow if there is at least one monitor that is yellow.

Moving downward you come to the group title bar for the current group. Within the group are the individual servers within the group, and optionally child groups will also be shown if there are any. Each server is represented as a line, with individual monitors on that server represented by boxes. The box color indicates the monitor's status. Green is OK, yellow is a warning, red is an error and grey means not monitoring (disabled, maintenance period, monitor dependencies not met).

You can click on any server name to be taken to that server's [server status report](#).

The screenshot shows the 'Group Summary for Servers/Devices' interface. At the top, there are navigation buttons: '< Back', 'Open in Browser', 'Print', and 'Print Preview'. Below these is a breadcrumb trail: 'Group Summary | Map | Servers Summary | Error Summary'. The main title is 'Group Summary for Servers/Devices' with a timestamp 'Updated 06 Jul 2009 02:09:49 PM' and buttons for 'All Reports' and 'PDF Version'. Two summary tables are present: 'Server Status Counts' (7 OK, 7 Alert, 0 Error, 3 Other) and 'Monitor Status Counts' (27 OK, 16 Alert, 0 Error, 18 Other). The main section, 'Servers/Devices', lists servers and their monitors. Servers listed include 127.0.0.1, 192.168.1.1, 192.168.2.5, and an 'ARCHIVE' group. Monitors shown include 'Event Log Monitor', 'Ping 192.168.1.1', 'Esensor EM01b Moni...', 'Ping 192.168.2.5', 'Critically Low Disk Sp...', 'Event Log Errors', 'Monitor services on ...', 'Ping ARCHIVE', 'Sample script for tes...', 'System Performance ...', 'Very Low Disk Space...', and 'Watch \\ARCHIVE\C\$...'.

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 group and choose [Report & Delivery Settings](#).



To see an even higher level view of the servers within the group, try the [All Servers Report](#) or customize the [Visual Status Map](#) report.

## All Errors Report

The All Error Report shows you all errors that have recently happened on all monitors, on all computers/devices, within a group. The report columns can be clicked to sort the errors for better understanding of what is happening on your network. This report can be enabled or disabled in [Report & Delivery Settings](#).

< BackOpen in BrowserPrintPrint Preview

Group Summary | Map | Servers Summary | Error SummaryUpdated 06 Jul 2009 03:40:43 PM

### Current Errors Summary

All Reports PDF version

#### Current Issues

Last Check	Server/Device	Monitor	Last Error
6 Jul 2009 3:38:45 pm	DNVISTA	Event Log Stuff	* Event Time: 06 Jul 2009 03:00:39 PM * Source: Interactive Services detection * Event Log: Application * Type: Information Event * * Event ID: 1000 * A device or program has requested attention. Dev [Truncated]
6 Jul 2009 3:40:20 pm	DNVISTA	Calculated Status	Double-monitor check failed [in error for 1m 41s]
6 Jul 2009 3:40:08 pm	192.168.2.113	Ping 192.168.2.113	192.168.2.113 is not responding to ping requests within 309 ms. [in error for 3d 22h 19m]

For a more detailed error report, with the ability to control what errors are shown and which columns are displayed, see [Error Auditing](#).

## All Servers Report

The All Servers Report is suitable for display in a Network Operations Center. The report shows each server in a group as a colored box, with the color of the box representing the 'worst' state of all the monitors on that server. The servers with the 'worst' state float to the top, so keeping an eye on the state of your data center can be done at a glance.

The display will add additional columns as the browser window gets wider in order to show as many servers as possible. At the very bottom of the report is a URL that can be used for displaying the report in browsers or on different computers.

The screenshot displays the 'All Servers Report' interface. At the top, there are navigation buttons: '< Back', 'Open in Browser', 'Print', and 'Print Preview'. Below these are links for 'Group Summary', 'Map', 'Servers Summary', and 'Error Summary'. The main title 'All Servers Report' is prominently displayed, along with the update time 'Updated 06 Jul 2009 02:39:26 PM' and buttons for 'All Reports' and 'PDF Version'.

Two summary tables are shown:

Server Status Counts			
11 OK	3 Alert	0 Error	7 Other

Monitor Status Counts			
48 OK	5 Alert	0 Error	8 Other

The main content area is a grid of server boxes. Each box contains a status icon (yellow or green) and the server name. The top row of boxes includes 'ARCHIVE' (yellow), 'DNVISTA' (yellow, with a note: 'This is a VM on the Mac Pro. Talk to Doug before rebooting.'), and 'MANY' (yellow). The remaining boxes are grey, indicating a better status: 'EXCHANGE1', 'EXCHANGE2', 'FREDS-MACHINE-GOOD.OFFICE-', 'FTP1', 'Printer', 'UPLINK', 'test', '127.0.0.1', '192.168.1.1', '192.168.2.5', 'DNLAPTOP.office-', 'DNMAC', 'DOMAIN', 'NEBPUTER', 'OPSMON02', 'POWERADMIN.COM', 'Server2008', and 'Ubuntu'.

Clicking on any computer will take you to that server's [server status report](#).



## Visual Status Map

The Visual Status Map is one of the available group level reports. The map display allows you to easily see the status of servers and server groups that you have placed on a map or other graphic. This type of display can be beneficial in determining network problems that are geographically significant due to server locations.

To see the Visual Status Map, select a group in the Navigation Window and click the "Map" link in the gray menu bar at the top of the report.

The following report is what a typical Visual Status Map might look like:



The map appearance and the positions and style of the status indicators can be configured in the [Status Map Editor Dialog](#). There are several maps of different areas around the world, and you can also add your own map graphic.

The map graphic and the server icons will stretch to fit the available browser window space.

The colors displayed by the status indicators correspond to the "worst" monitor state of all monitors on the computer (or for all monitors within the computer group). In other words, the presence of one monitor in an alert state for a given computer will cause its indicator to display in yellow. A "green" status indicates that the computer has no detected problems.

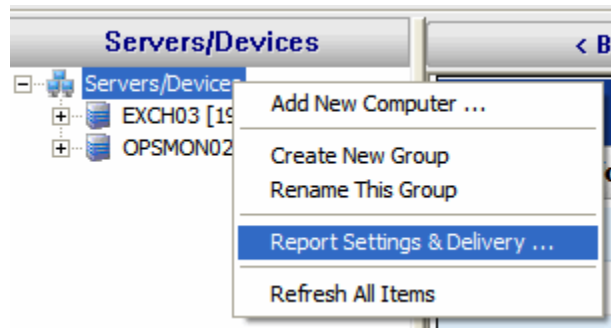


## Group Report Settings and Delivery

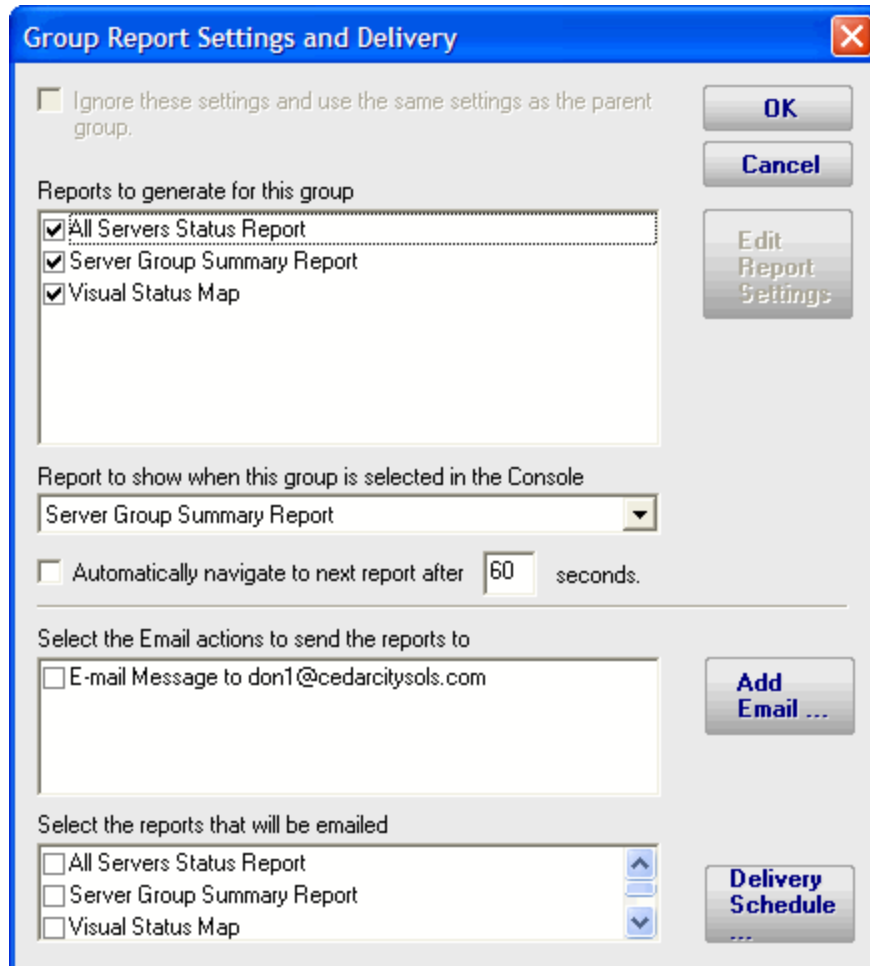
---

The Group Report Settings and Delivery dialog allows you to change some attributes of Group Reports. The Group Report is the display that is shown when you select a group item in the navigation pane. (The group item labeled "Servers/Devices" is the default group and always exists.)

To display the Group Report Settings and Delivery dialog, select the "Report Settings and Delivery" command item for the group whose group report options that you wish to work with, as shown.



Next, you will see the Group Report Settings and Delivery dialog displayed, as shown.



You may now change the appearance and some characteristics of the Group Reports displays.

- To change characteristics of the Visual Status Map, select the report in the list box at the top of the display and press the Edit Report Settings button.
- To change the report that is initially displayed when the group is selected by the user, select the report in the dropdown list labeled "Report to show when...".
- The check box labeled "Automatically navigate..." allows you to enable the feature that rotates the Server Group display through the three types of Server Group reports. When this check box is selected, the display will show each of the three report types in succession, and will pause at each report type for the number of seconds that have been specified in the text box to the right of the check box.
- "Select the Email Actions to send the reports to" allows you to specify which email addresses will be destinations where these reports will be emailed at intervals. You may add new email addresses, in addition to the pre-configured email addresses that are always available.
- "Select the reports that will be emailed" allows you to select which of the three types of group reports that will be emailed at intervals by the program.

## Status Map Editor Dialog

The Status Map Editor dialog is displayed when you choose the Visual Status Map item in the list and press the Edit Report Settings button. It is shown below.



You should understand the following in order to make the best use of the Status Map feature.

- The Status Map Editor allows you to select one of a number of included graphical maps of the world and of world regions that can be used as a background for the server status lights.
- The Visual Status Map is provided only as a passive visualization assistance for monitoring. It is not currently provided as part of any mapping, GIS, or GPS facility.

The functions provided by the Status Map editor are as follows.

- You may select a background map for this group's Visual Status Map display from one of a number of public domain and government provided maps that are installed with PA Storage Monitor.
- Alternatively, you may use the "Add" button next to the background map selection dropdown list in order to provide your own map graphic file. Your map file must be in one of the common graphical image file formats: BMP, GIF, JPEG, PNG, and TIF are supported.
- The "Zoom" Slider allows you to set the zoom of the background map.
- You may move the map image using the mouse, by left clicking and dragging the image.

- The "Use Status Lights" and "Use Status Icons" selection allows you to customize the way PA Storage Monitor displays the status indicators. Status lights are simple light images that may appear green, grey, yellow or red. Status icons are round images that have the same color coding as the status light but add an icon symbol inside each image: green contains a check, yellow is a triangle and contains an exclamation, and red is round with an exclamation. The status icon selection may be preferable for color blind users.
- The list of Servers/Devices allows you to select a computer in the group whose status indicator should be added to the map.
- Pressing the "Add Status Icon" button with a computer selected in the Servers/Devices list will cause a status indicator for the computer to be added to the map.
- To remove a status indicator from the map, drag it using your mouse cursor back to the Servers/Devices list.
- The three radio button selections: "Label on left", "Label on right", and "No Label", allows you to select the text labeling style that is to be applied to each status indicator. You should set these radio buttons to choose the style for the indicator that you place next. You may wish to "flop" the label in a certain direction so that a city name or feature on the underlying map is clearer. You may also wish to not apply a label to certain indicators, in case the server identity is obvious from appearance.

When viewing the status map with a browser or in the Console, the map graphic will be stretched or shrunk as needed to fill the browser window that holds it. The icons will be moved appropriately so they remain in the same relative location on the map.

The following report display for a properly configured Status Map is typical. In this example, the map indicator and background map display was configured using the settings shown in the Status Map Editor figure above.

< Back

Open in Browser

Print

Print Preview

Group Summary | Map | Servers Summary | Error Summary

## Visual Status Map

Updated 06 Jul 2009 09:25:59 PM

All Reports

PDF  
Version

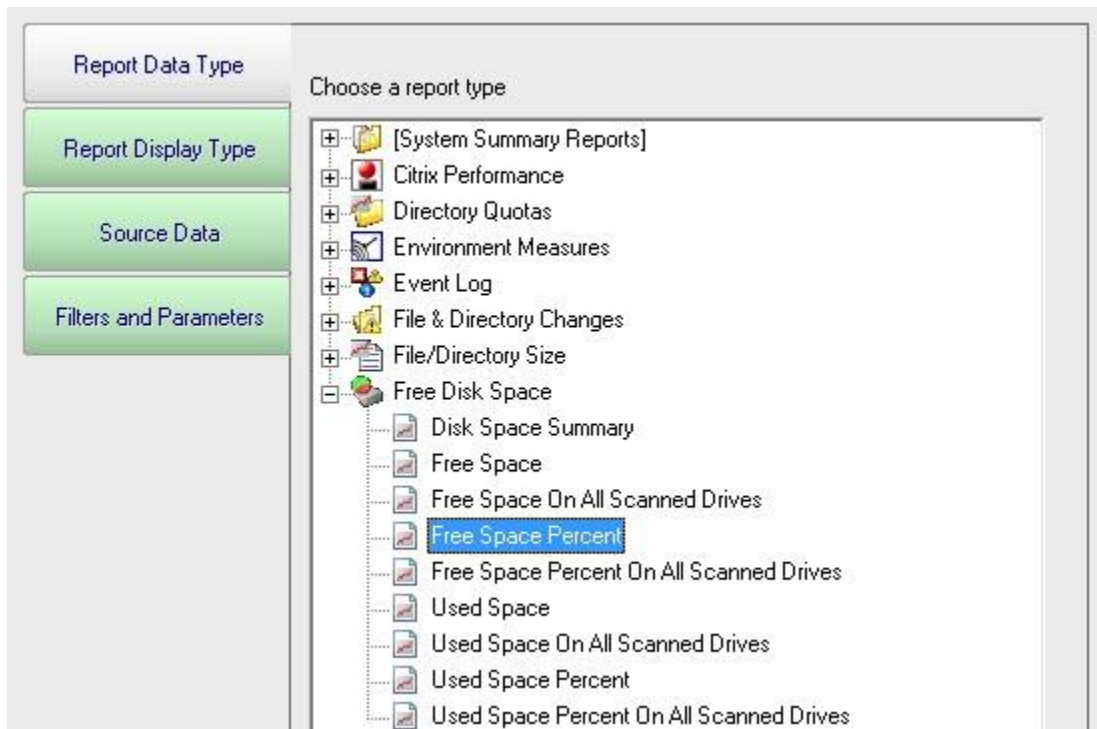


Indicator status: OK at 9:25:59 PM

## Ad Hoc Reports

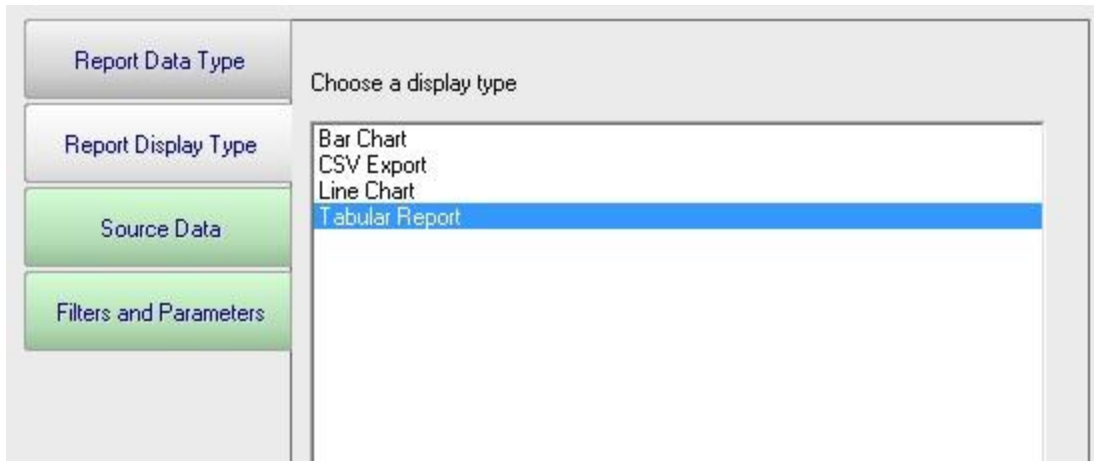
Ad hoc reports can be generated at any time to quickly gather data on your systems. Simply click through each tab and make the selection that is presented on the tab. Note that the reports present in your application may differ from those shown in the image below.

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.



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.

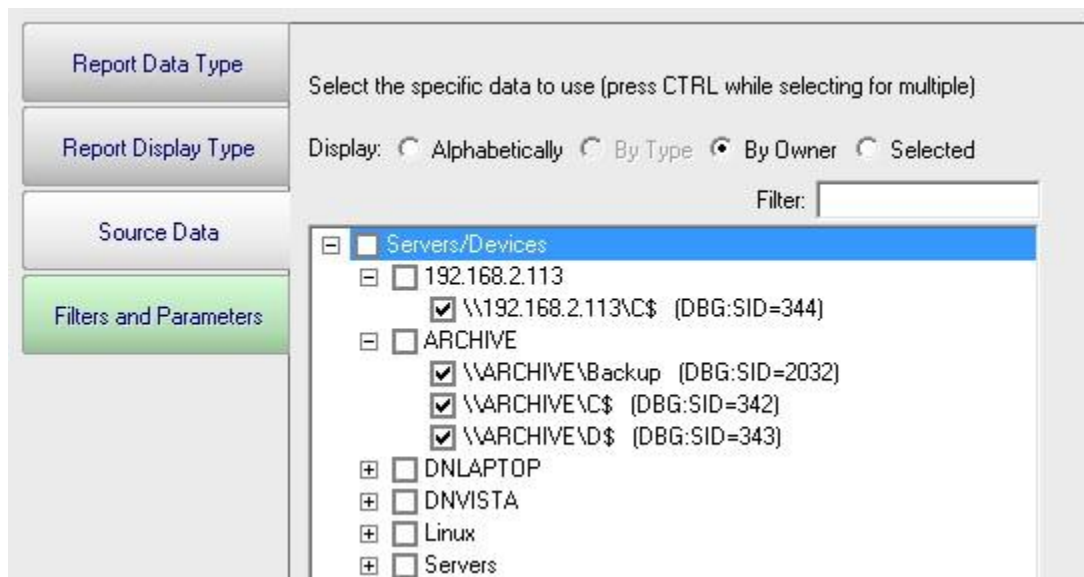




After having selected the report type and the display format, it's time to choose which data to report on. This is done on the Source Data tab. This tab will display all of the data that is available for the chosen report type. In this case we are shown drives that can be reported on. The radio buttons 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.



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

---

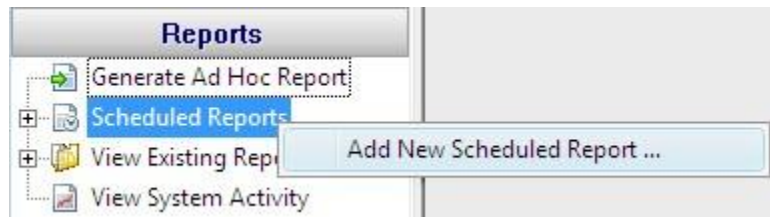
If a report doesn't show the data that you expect, check the following:

- 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.



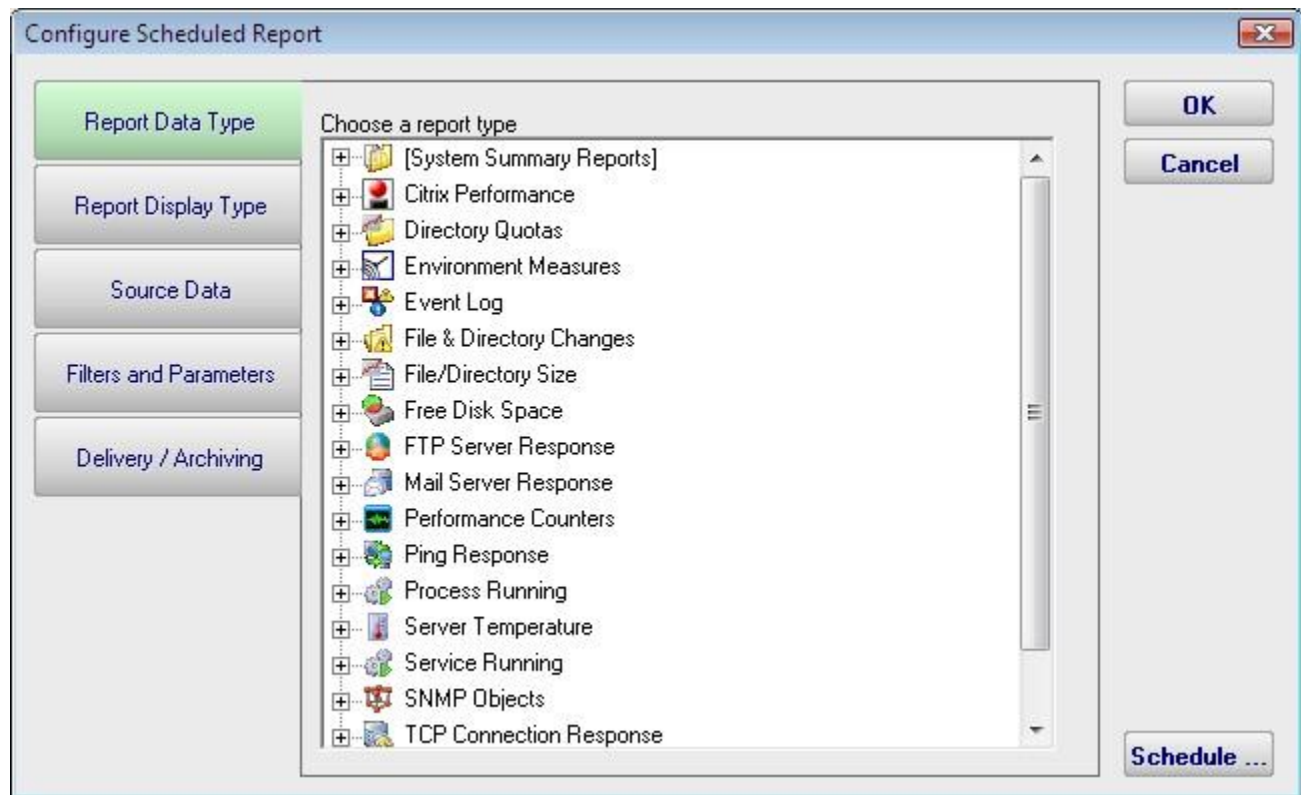
## Scheduled Reports

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.

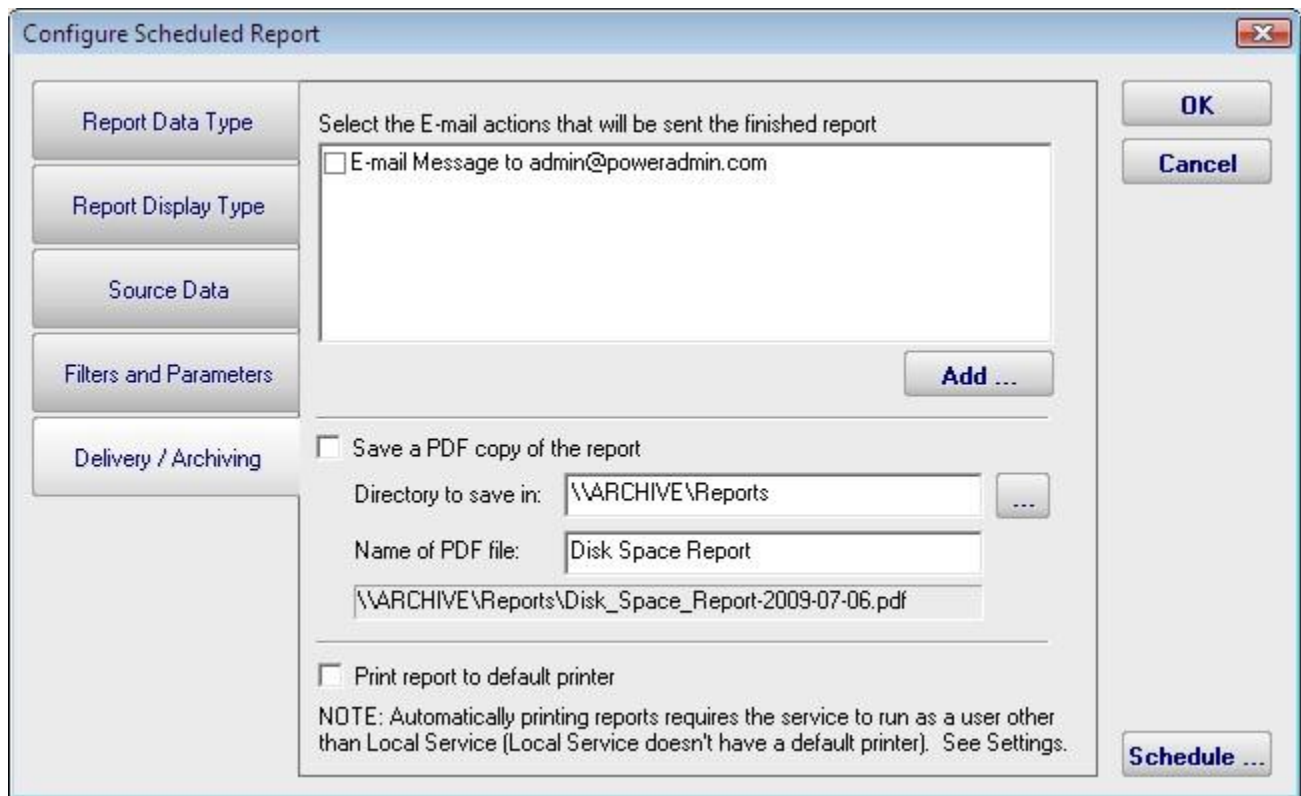


The new Delivery / Archiving tab lets you specify whether to email the report when it has run. The report email will contain a PDF as well as an image of the report (raw HTML isn't sent because of varying support in email clients).

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.

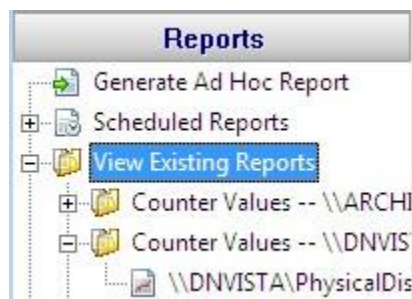
At the bottom of the report you'll see the familiar Schedule button. It works the same way as the Schedule buttons in the monitors. You can easily specify how often the report is run.



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.

## 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/"`

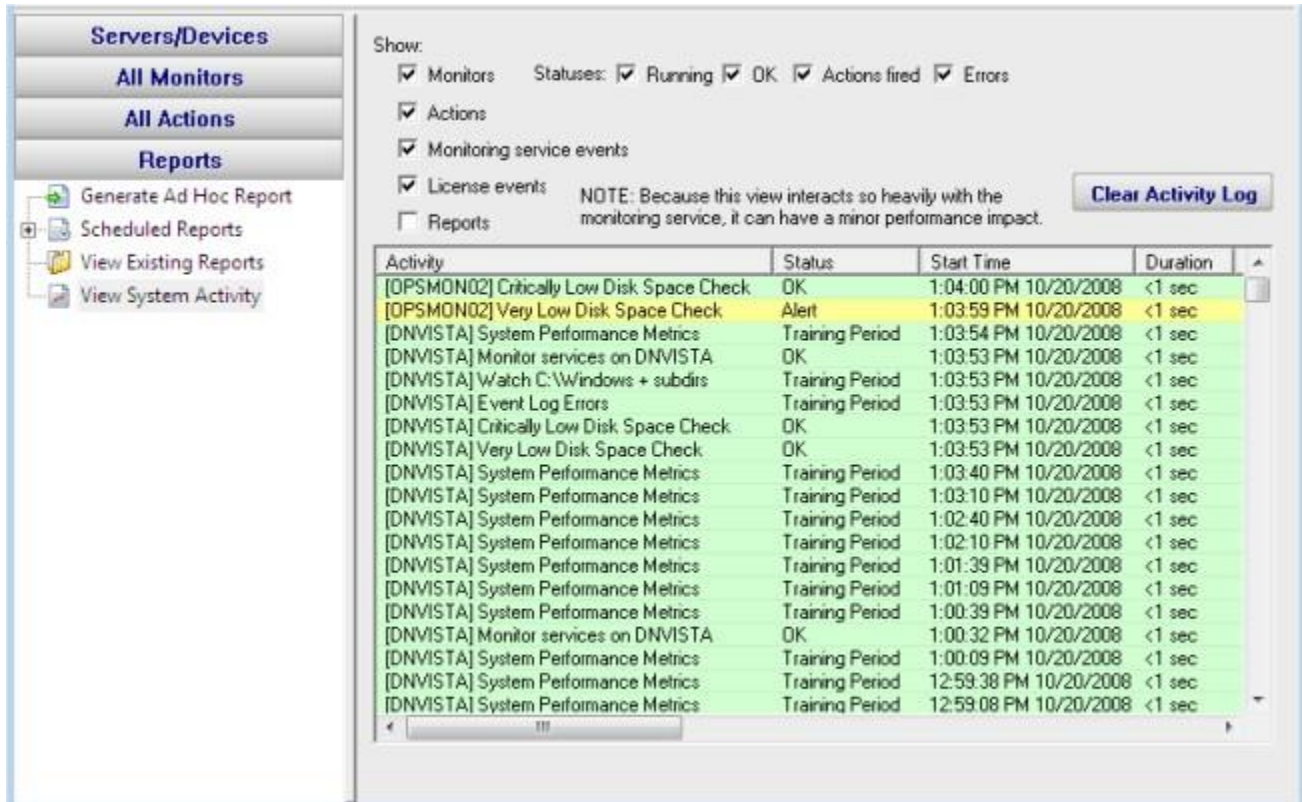
## Viewing System Activity

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.



The screenshot shows the 'View System Activity' window. On the left is a navigation pane with 'Servers/Devices' selected, containing 'All Monitors', 'All Actions', and 'Reports'. Under 'Reports', there are options: 'Generate Ad Hoc Report', 'Scheduled Reports', 'View Existing Reports', and 'View System Activity'. The main area shows a 'Show:' section with checkboxes for 'Monitors', 'Actions', 'Monitoring service events', 'License events', and 'Reports'. The 'Monitors' section is expanded to show 'Running', 'OK', 'Actions fired', and 'Errors'. A 'Clear Activity Log' button is visible. Below is a table of activity logs.

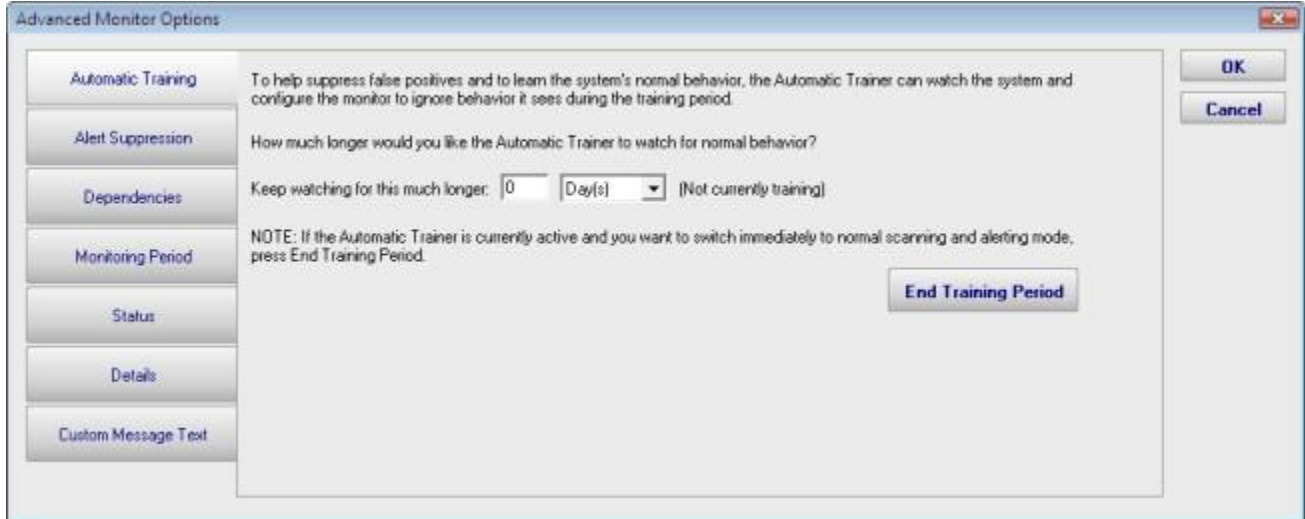
Activity	Status	Start Time	Duration
[OPSMON02] Critically Low Disk Space Check	OK	1:04:00 PM 10/20/2008	<1 sec
[OPSMON02] Very Low Disk Space Check	Alert	1:03:59 PM 10/20/2008	<1 sec
[DNVISTA] System Performance Metrics	Training Period	1:03:54 PM 10/20/2008	<1 sec
[DNVISTA] Monitor services on DNVISTA	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](#)

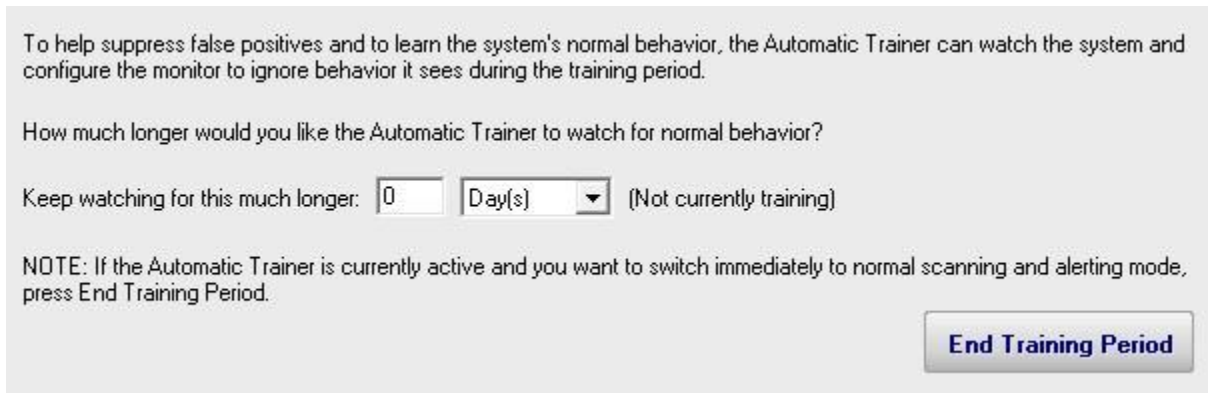
### Advanced Monitor Options

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.



Each of the different option tabs is discussed below.

#### Automatic Training



PA Storage Monitor 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  problems in  Minute(s) ▾
- Only fire alerts after the monitor has detected an error for  Minute(s) ▾
- Only fire a maximum of one alert every  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	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Mon	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Tue	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Wed	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Thu	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Fri	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Sat	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green

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

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.

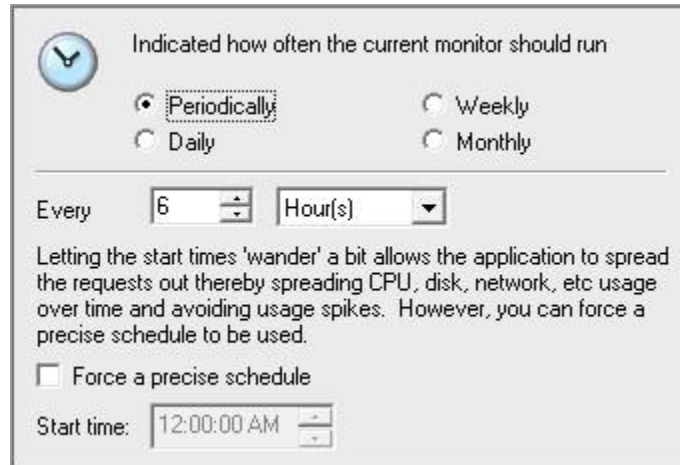
### Custom Message Text

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).

## 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:



The screenshot shows a dialog box titled "Indicated how often the current monitor should run". It features a clock icon in the top left. There are four radio buttons for scheduling: "Periodically" (selected), "Daily", "Weekly", and "Monthly". Below these is a section for "Every" with a numeric input field containing "6" and a dropdown menu set to "Hour(s)". A paragraph of text explains that letting start times "wander" helps spread CPU, disk, and network usage. Below this text is a checkbox labeled "Force a precise schedule" which is currently unchecked. At the bottom, there is a "Start time:" label followed by a time input field showing "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<sup>1</sup>). 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)

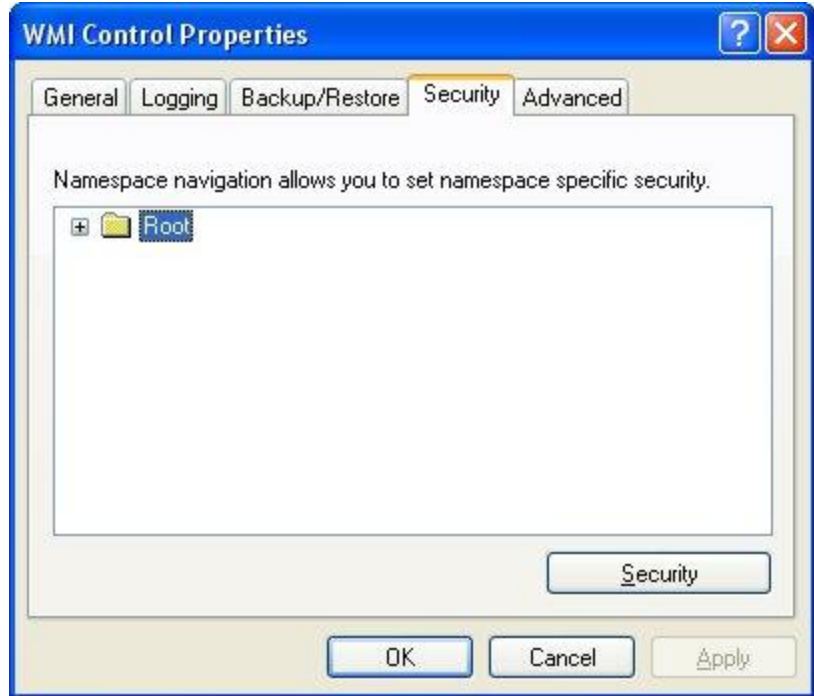
1. On the target server, go to Administrative Tools -> Computer Management.

2. Expand 'Services and Applications'

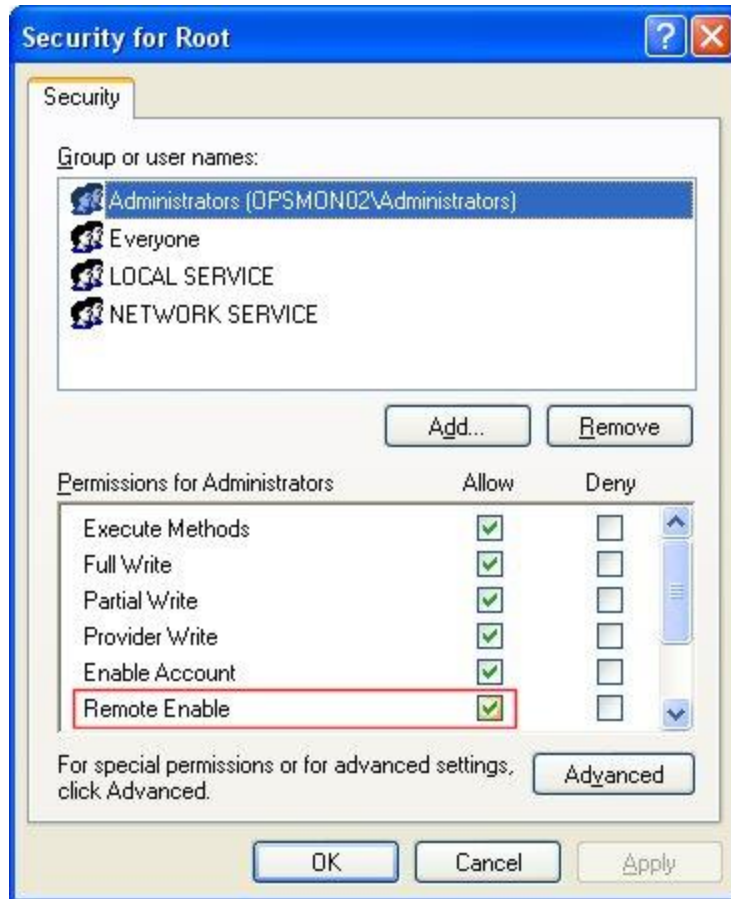
3. Right click for Properties on 'WMI Control'.



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



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.



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<sup>2</sup>. 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.msp#ENAA>

2. See [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/connecting\\_through\\_windows\\_firewall.asp](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.

## Remote Monitoring Account Hints

---

The most common problem when trying to monitor remote server resources (disks, PerfMon counters, running services, Event Log, etc.) is getting the remote server to allow access to the resources. Windows security won't simply fulfill any requested access issued by any random machine on the network (imagine the chaos!). A token representing the user making the request is sent along with the request. The remote server checks the token against an access control list which protects the target resource and determines whether to allow access or not.

## Troubleshooting

---

Skip forward to your particular scenario:

- [Connecting to computers in a domain](#)
- [Connecting to computers NOT in a domain](#)
- [Connecting to Vista and Windows 2008 computers](#)

## Background

---

So which user is making the request?

Go to the Services control panel applet (under Administrative Tools), and open the properties for any service. You will see a Log On tab. This tab controls which user account is used to launch the service. All services run as some user. A special user account named Local System is often used which has full access to the local machine, but no access outside the machine. In addition, you can right-click on a computer in the Console and select "Set Login Credentials" to set computer-specific credentials to use when monitoring that computer.

If no computer-specific credentials are entered, then all requests are made as the user which is listed on the Log On tab (also shown in Settings). In the examples below, we assume that there are no computer-specific credentials.

Consider the scenario where machine "OPS" is running a service (like the Power Admin monitoring service) and wants to look at the Event Log on machine "SERVER". If the service is running as Local System, the Event Log request would contain a token referring to user "OPS\Local System". The problem is, machine SERVER doesn't know anything about "OPS\Local System". For all it knows, that account might be a simple guest account. Access will be denied.



### What solutions exist?

There are two basic ways to get around this problem, and they both involve getting the request on OPS to run as a user which SERVER will recognize.

### Solution 1

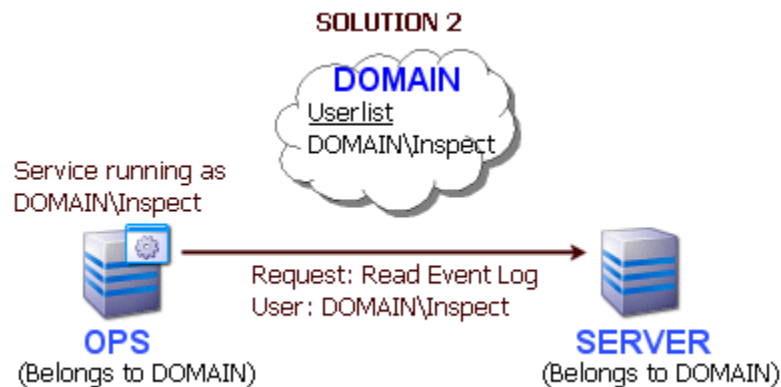
The first solution is to use synchronized username and passwords on the two machines. You can create a user account named "Inspect" on OPS with password "baseball". Then go to SERVER and create a user account named "Inspect" with password "baseball". When user "Inspect" runs the service on OPS, and sends a request to SERVER, the token turns out to contain not just the username, but a hashed form of the password as well. When SERVER receives the request, it checks its local user database and finds a matching user, hashes the local password and finds that they match. It then allows the request as though it had originated from the local user "Inspect". Any access to resources granted to the local user "Inspect" on SERVER can be accessed remotely from the similar user "Inspect" on machine OPS. The downside to this solution is it requires all monitored machines to have synchronized usernames and passwords. This doesn't work for "Local System" because Local System is a special operating system account tied to the local computer (and you can't set Local System's password).



NOTE: Starting with Windows XP a security policy was introduced that causes incoming local credentials (from a remote host) to be assigned Guest user rights. That won't help. You'll need to set the policy back to Classic mode. Microsoft documents this here: [\[1\]](#) and [\[2\]](#). This can be corrected by switching to Classic file sharing, or by going to Administrative Tools -> Local Security Policy -> Security Settings -> Local Policies -> Security Options. Look for "Network Access:Sharing and Security model for local accounts" and set it to "Classic".

## Solution 2

The second solution requires using domain accounts. Imagine that the machines OPS and SERVER are both in a domain named DOMAIN. The domain could then have a user created named "Inspect" for example. The service on OPS should then have its Log On user set to DOMAIN\Inspect. On SERVER, you would grant access to any resources that should be monitored to user DOMAIN\Inspect (or as a shortcut, make DOMAIN\Inspect part of the local Administrators group). When Server Monitor tries to monitor the Event Log on SERVER for example, a token representing DOMAIN\Inspect will be passed with the request. SERVER will recognize the token and allow access according to the rights granted to DOMAIN\Inspect.



**IMPORTANT NOTE:** Both solutions above discuss changing which user the monitoring service runs as. You can also set the login credentials on each individual server from within the Console. Right click the server and you'll see the Set Login Credentials option. You can choose to communicate with the server as the user running the service, or pick a specific username/password for that server. When choosing a username/password for that server, the username still has to satisfy what is discussed above (i.e. it needs to be a locally synchronized username or a domain username).

*Is there any other way?*

There is a third alternative: Install the monitoring product on the remote server. It can then run as Local System and look just at the server itself. Power Admin monitoring products install quickly, and the Easy Configuration feature makes it simple to copy a monitoring configuration from one machine to another.

## Connecting to Servers in a Domain

When monitoring machines that are in the same domain as the monitoring server, it's easiest to use a domain account to gain access to the remote servers. If one domain account will work for all servers, you can set the service to run as that account -- that is the easiest scenario.

If you can't run the service as a domain account (perhaps because multiple domains are involved), you might need to specify separate credentials for each server. You can do many at once via Bulk Config, or right-click on an individual server and choose Type & Credentials -> Set Login Credentials.

**Troubleshooting:** If you get an error indicating the credentials don't grant access to the remote machine, that very often implies some sort of firewall (a network firewall and/or a firewall running on the remote machine) is blocking access. In that case, try to remove as



many variables as possible and see if a connection can be made. We recommend using the Windows Event Log Viewer. Start it, and using it, try to connect to the remote machine and view its Event Log. If you can not connect (perhaps with RPC errors) that very often indicates a firewall is blocking Windows RPC calls.

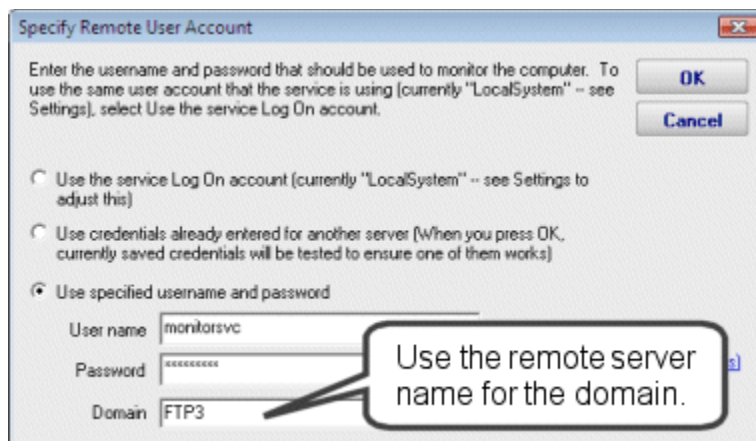
[More info on Windows RPC ports](#)

Also make sure the Remote Registry service is started on the target server.

## Connecting to Servers NOT in a Domain

When either the monitoring server or the target server are not in a domain, local accounts have to be used. In this case there are two options:

- Use [synchronized local accounts](#) (Solution 1) as discussed above. Use the local server name for the domain field.
- Use an account that only exists on the remote machine. In this case, make sure to use the remote server name for the domain field.



**Troubleshooting:** If the above doesn't work and you get an error indicating the credentials don't grant access to the remote machine, that very often implies some sort of firewall (a network firewall and/or a firewall running on the remote machine) is blocking access. In that case, try to remove as many variables as possible and see if a connection can be made. We recommend using the Windows Event Log Viewer. Start it, and using it, try to connect to the remote machine and view its Event Log. If you can not connect (perhaps with RPC errors) that very often indicates a firewall is blocking Windows RPC calls.

[More info on Windows RPC ports](#)

Also make sure the Remote Registry service is started on the target server.

If you can connect with the Event Log Viewer, but you are still told the credentials aren't working, you can force the monitoring product to create a connection to the server via the \\server\IPC\$ share. To do this, go to:

PA Server Monitor

HKEY\_LOCAL\_MACHINE\Software\PowerAdminServerMonitor

PA Storage Monitor

HKEY\_LOCAL\_MACHINE\Software\PAStorageMonitor

and set/create the DWORD value ImpForNetConnect = 1

## Connecting to Vista and Windows 2008 computers

---

The information above for [Connecting to Servers in a Domain](#) and [Connecting to Servers NOT in a Domain](#) still applies to Windows 2008 Servers and Vista. However, Windows 2008 and Vista comes with a powerful and strict firewall that is turned on by default. This firewall will almost certainly block remote monitoring requests.

To change the firewall configuration, go to Administrative Tools -> Windows Firewall with Advanced Security. Microsoft has a good [Getting Started Guide](#) to help you become familiar with the interface.

There are firewall rules to control fine-grained access to the server. If you want to monitor the server's Event Log, you'll need to enable those rules. For monitoring services, you'll need to enable the service-related rules. If you want the rich server status report (which is built by polling the server via WMI), you'll need to enable the WMI rules.

## 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.