PA Server Monitor

Version 3.7 Pro

Last Update: July 13, 2009

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

Prepared in the USA

Getting Started with PA Server Monitor

Thank you for choosing PA Server Monitor. The following topics offer some help in installing, configuring and using PA Server 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 Server Monitor.

- Concepts
- Console
- Global Settings
- Database Settings
- HTTP Settings
- Report Settings
- SNMP 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 Server Monitor. The following help topics explain the functionality of each monitor.

- Calculated Status Monitor
- Citrix Presentation Server Monitor
- Directory Quota Monitor
- Disk Space Monitor
- Environment Monitor
- Event Log Monitor
- Execute Scripts
- File Age Monitor
- File & Directory Monitor
- FTP Server Monitor
- Log File Monitor

- Mail Server Monitor
- Performance Monitor
- Ping Monitor
- Process Monitor
- Server Temperature Monitor
- Service Monitor
- SNMP Monitor
- TCP Port Monitor
- Web Page 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 Server 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

Contents

Quick Installation Guide for PA Server Monitor

You will find that PA Server 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 it's own directory, with the exception of the optional Microsoft SQL Server Native Client, which is a system component and uses a Microsoft installer. The SQL Native Client is not required, and can be installed later.

Installation Considerations

PA Server 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 Server Monitor
                Databases
                Reports
```

PA Server 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 Server 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

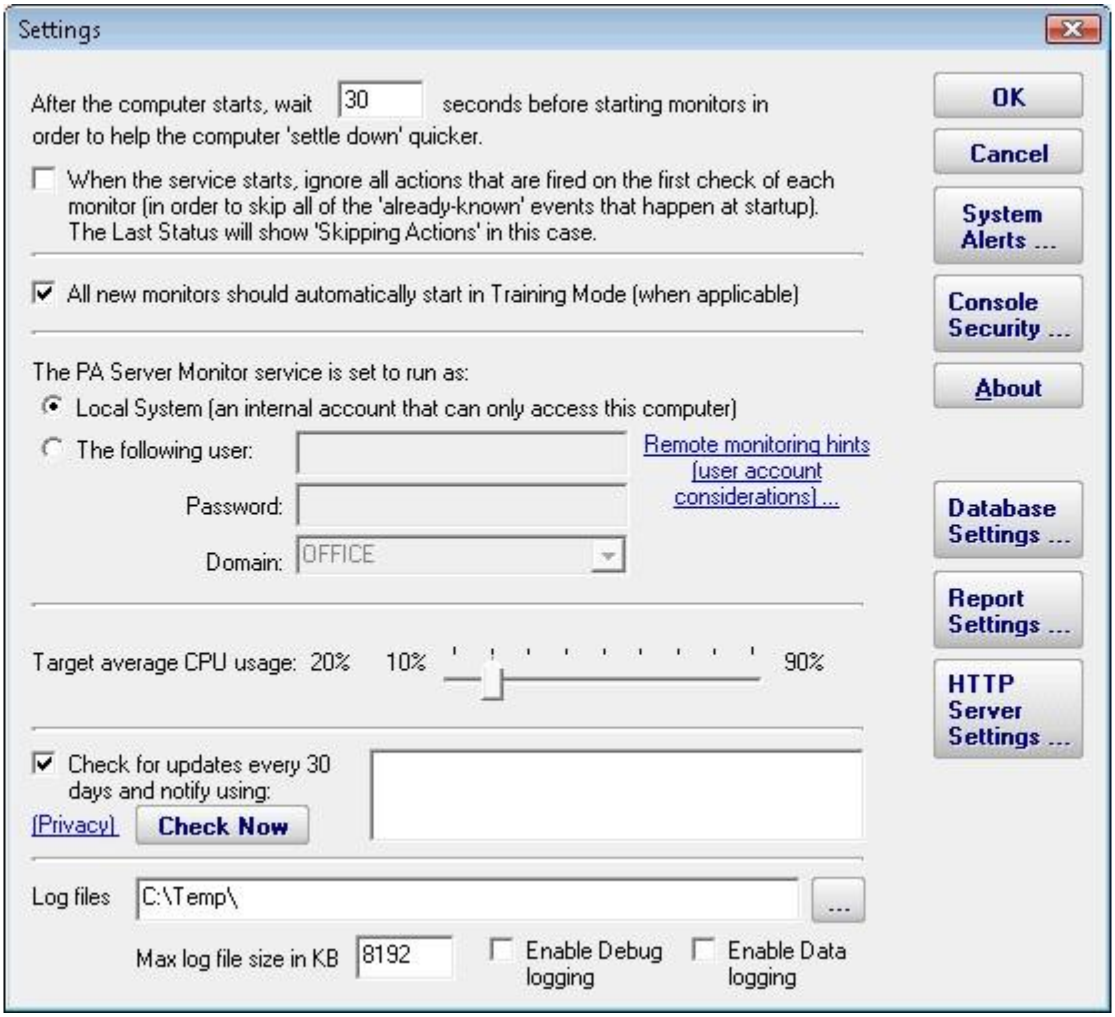
Contents

PA Server Monitor Startup Wizard

The instructions that are provided here apply to the process that you can follow when you run PA Server 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 Server 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 Server 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.



Settings

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

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

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

The PA Server Monitor service is set to run as:

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

○ The following user:

Password:

Domain: OFFICE

Target average CPU usage: 20%

☑ Check for updates every 30 days and notify using:

Log files: C:\Temp\

Max log file size in KB: 8192

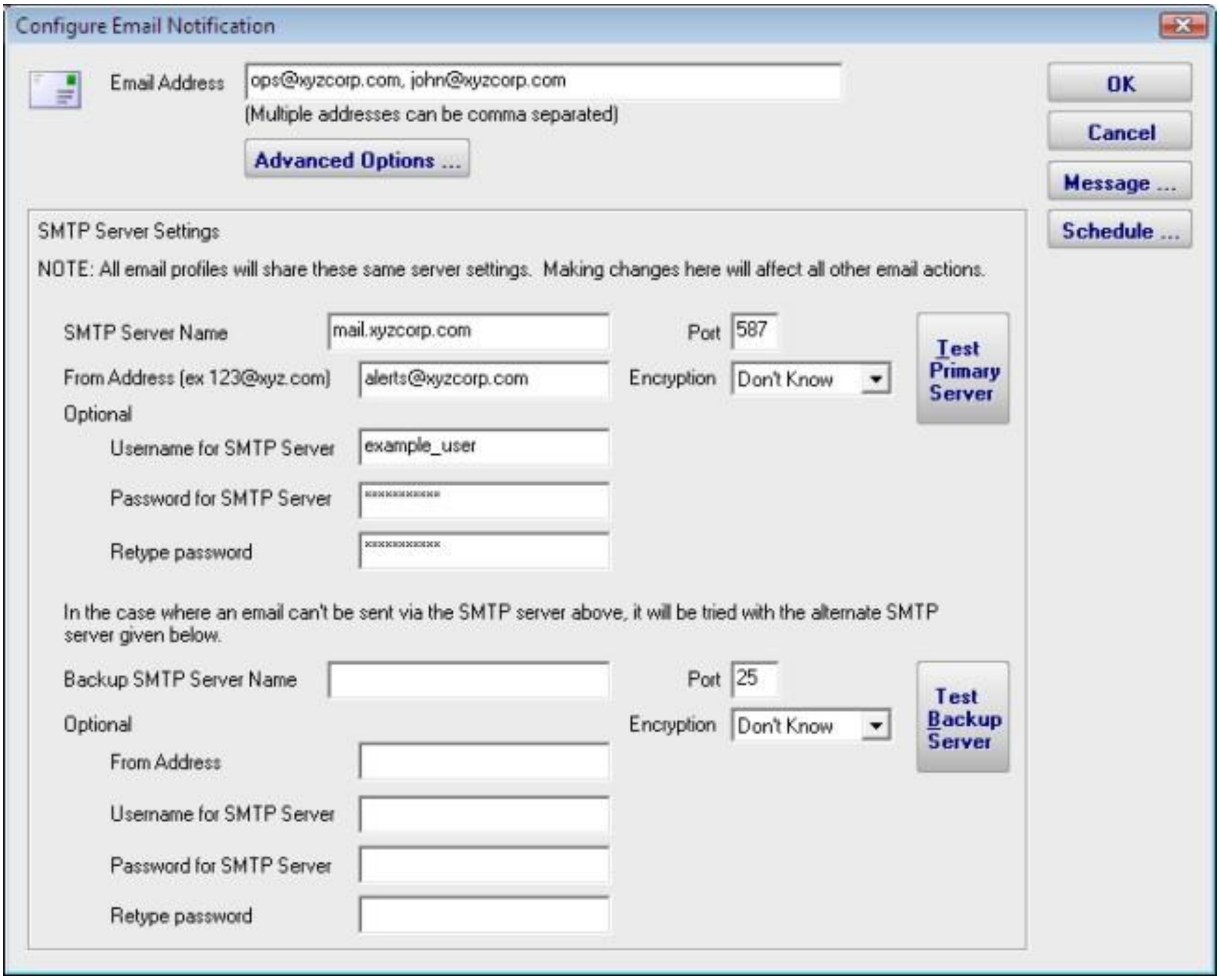
☐ Enable Debug logging

☐ Enable Data logging

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)

SMTP Server Settings

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

SMTP Server Name: mail.xyzcorp.com

Port: 587

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

Encryption: Don't Know

Optional

Username for SMTP Server: example_user

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

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

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

Backup SMTP Server Name:

Port: 25

Encryption: Don't Know

Optional

From Address:

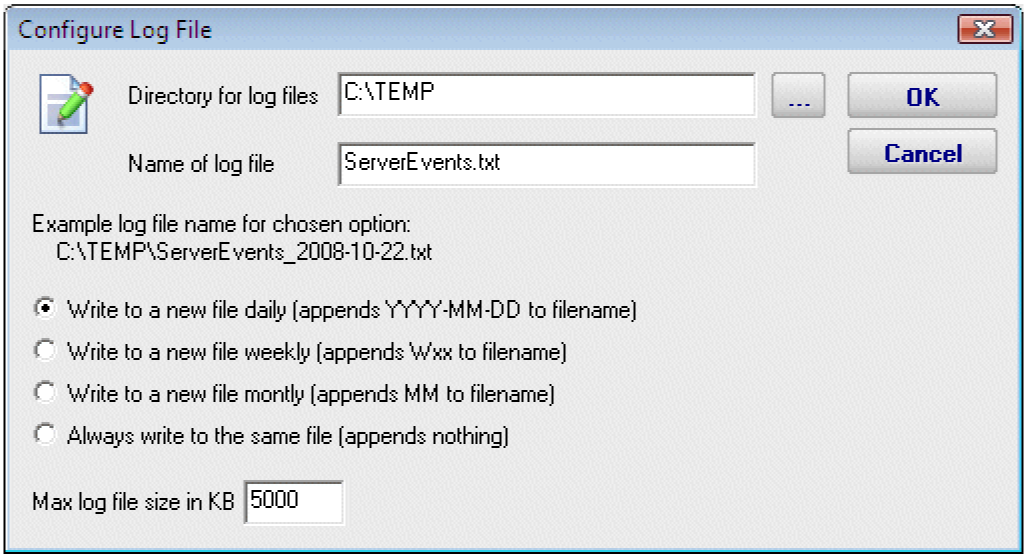
Username for SMTP Server:

Password for SMTP Server:

Retype password:

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.



Directory for log files: C:\TEMP

Name of log file: ServerEvents.txt

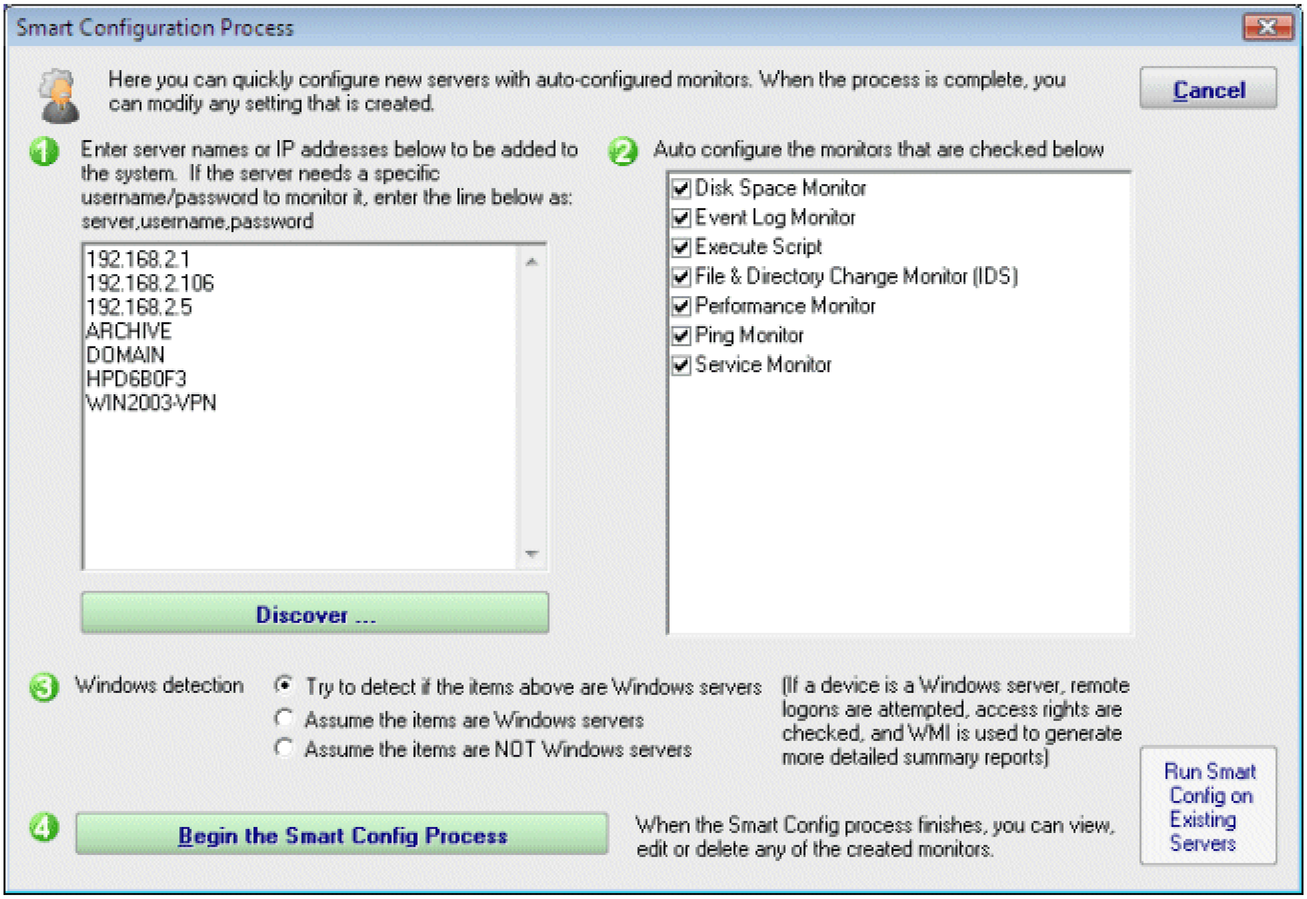
Example log file name for chosen option:
C:\TEMP\ServerEvents_2008-10-22.txt

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

Max log file size in KB: 5000

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.


Smart Configuration Process
Cancel
Discover ...
Begin the Smart Config Process
Run Smart Config on Existing Servers

Here you can quickly configure new servers with auto-configured monitors. When the process is complete, you can modify any setting that is created.

1 Enter server names or IP addresses below to be added to the system. If the server needs a specific username/password to monitor it, enter the line below as: server,username,password

```
192.168.2.1
192.168.2.106
192.168.2.5
ARCHIVE
DOMAIN
HPD6B0F3
WIN2003-VPN
```

2 Auto configure the monitors that are checked below

☑ Disk Space Monitor
☑ Event Log Monitor
☑ Execute Script
☑ File & Directory Change Monitor (IDS)
☑ Performance Monitor
☑ Ping Monitor
☑ Service Monitor

3 Windows detection

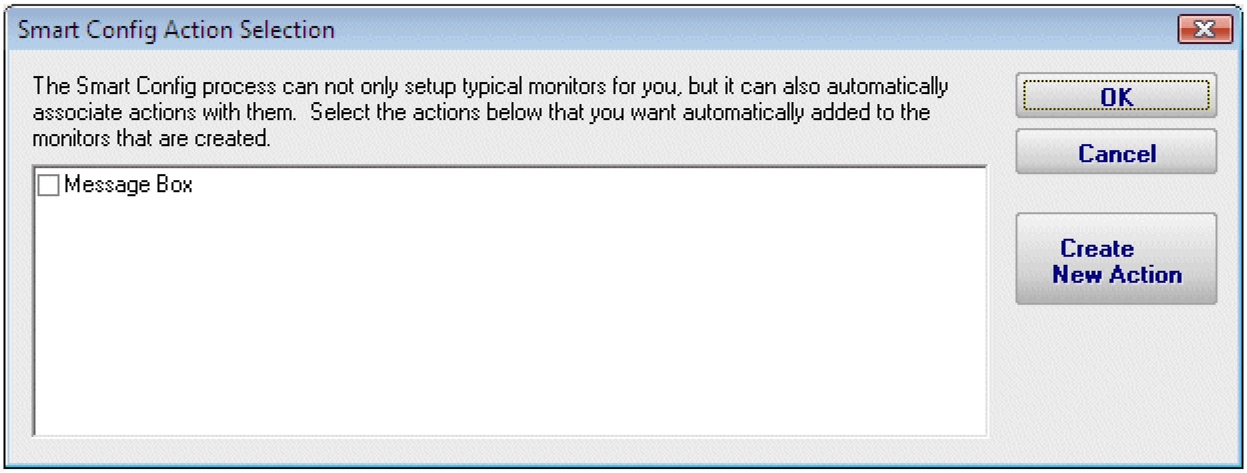
● Try to detect if the items above are Windows servers
○ Assume the items are Windows servers
○ Assume the items are NOT Windows servers

(If a device is a Windows server, remote logons are attempted, access rights are checked, and WMI is used to generate more detailed summary reports)

4 When the Smart Config process finishes, you can view, edit or delete any of the created monitors.

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.

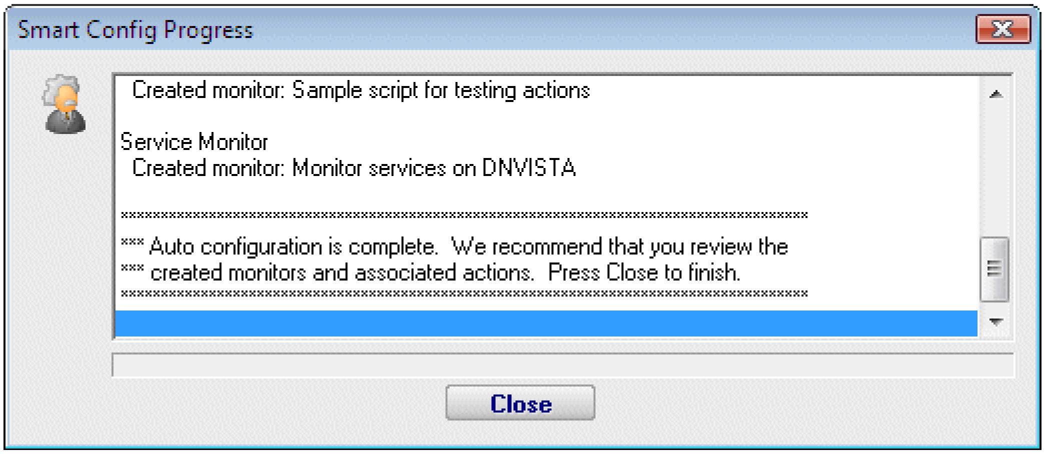

Smart Config Action Selection

The Smart Config process can not only setup typical monitors for you, but it can also automatically associate actions with them. Select the actions below that you want automatically added to the monitors that are created.

□ Message Box

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.


Smart Config Progress

```
  Created monitor: Sample script for testing actions

Service Monitor
  Created monitor: Monitor services on DNVISTA

*****************************************************************************
*** Auto configuration is complete.  We recommend that you review the
*** created monitors and associated actions.  Press Close to finish.
*****************************************************************************
```

The screen labeled "Smart Config Process" shows you what PA Server 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 Server 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.

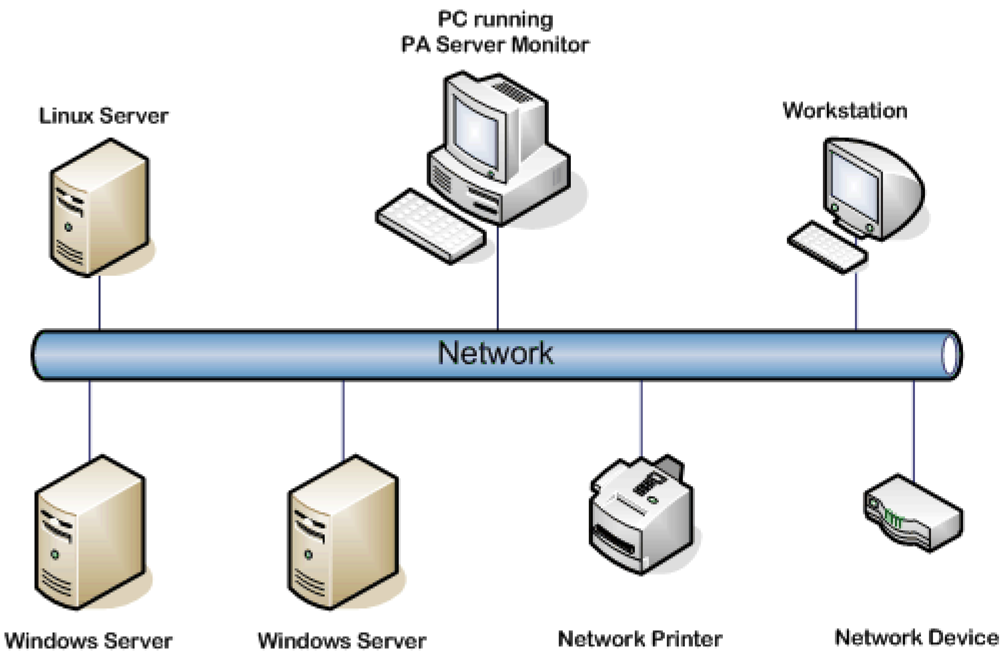
Configuration

Contents

Terminology and Concepts of PA Server Monitor

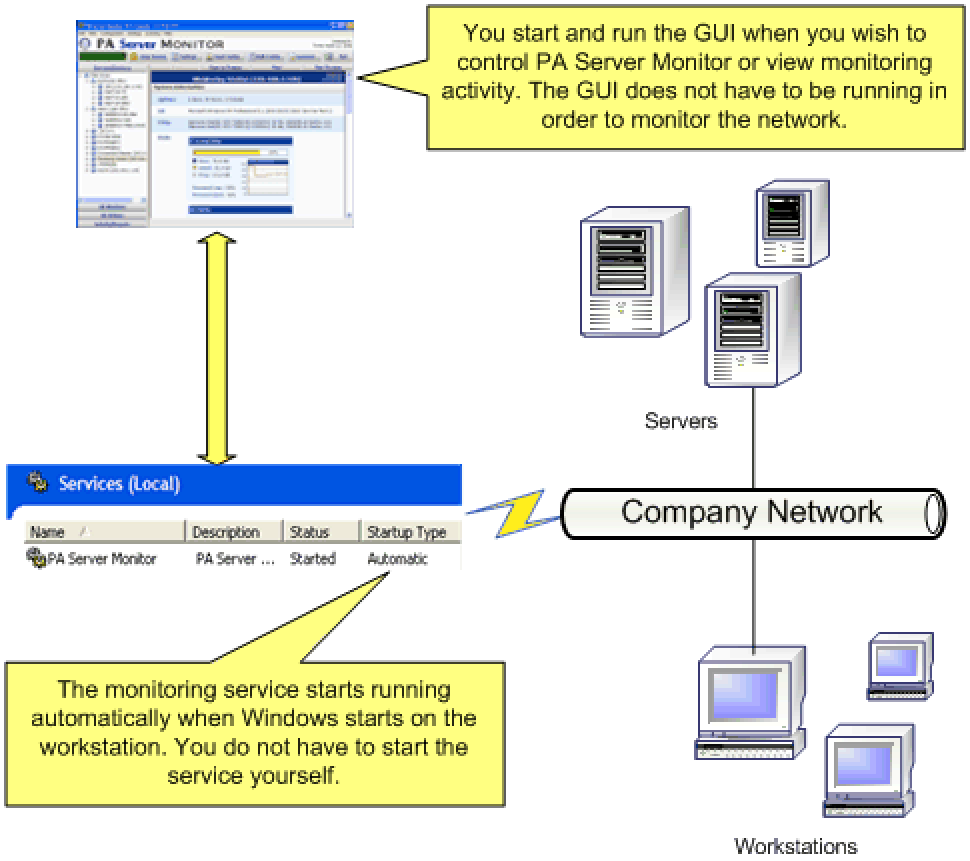
PA Server Monitor runs on a Windows computer and monitors the condition of servers and other equipment on your network. The following graphic shows the basic structure of a network that is using PA Server Monitor.

PA Server Monitor In Operation in a Typical Network



The PA Server Monitor product is composed of two parts: a graphical user interface that we call the Console, and a background process called the monitoring service. You see the Console when you launch PA Server 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 Server Monitor work together.



You start and run the GUI when you wish to control PA Server Monitor or view monitoring activity. The GUI does not have to be running in order to monitor the network.

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

The service is the part of the product that performs the monitoring of the network. 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 Server Monitor from the setup application.

Product Terminology

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

The PA Server 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. Another example of an Error Condition is lack of response to a "Ping".

Action

An Action is an activity that PA Server 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 Server 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 Server 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 Server 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 Server 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.

Contents

PA Server Monitor Console

The Console is the administrative interface to PA Server Monitor.

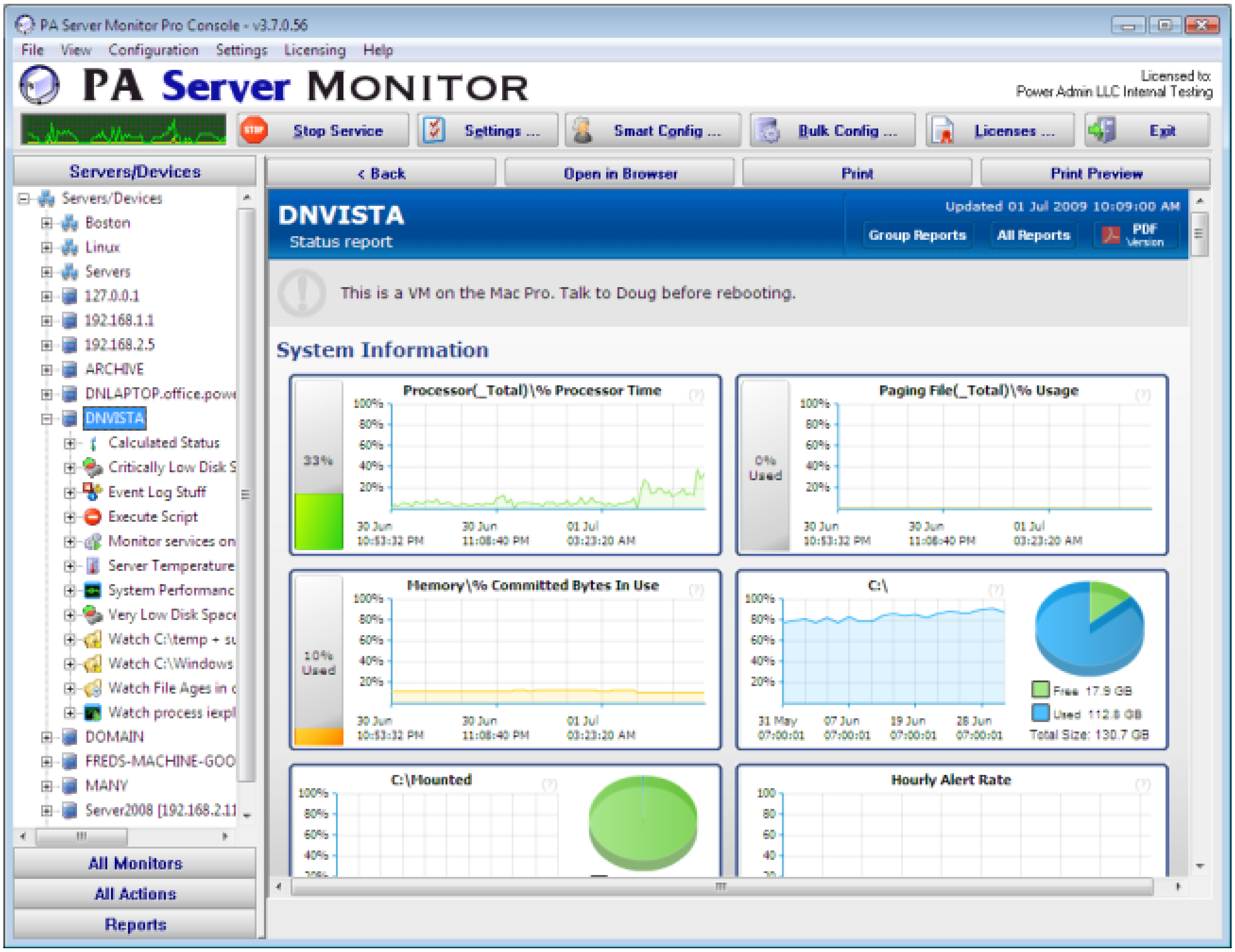
On the left side is the navigation pane. Similar to many other Windows products, this navigation pane displays items that you can interact with. Right clicking most items will give you a menu of choices. Selecting an item will cause the large right panel to change to your current selection.

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 Server 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 Server 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.



This is a VM on the Mac Pro. Talk to Doug before rebooting.

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 Server Monitor directory. The Licenses button will display the License Manager dialog to let you see your current licensing status.

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

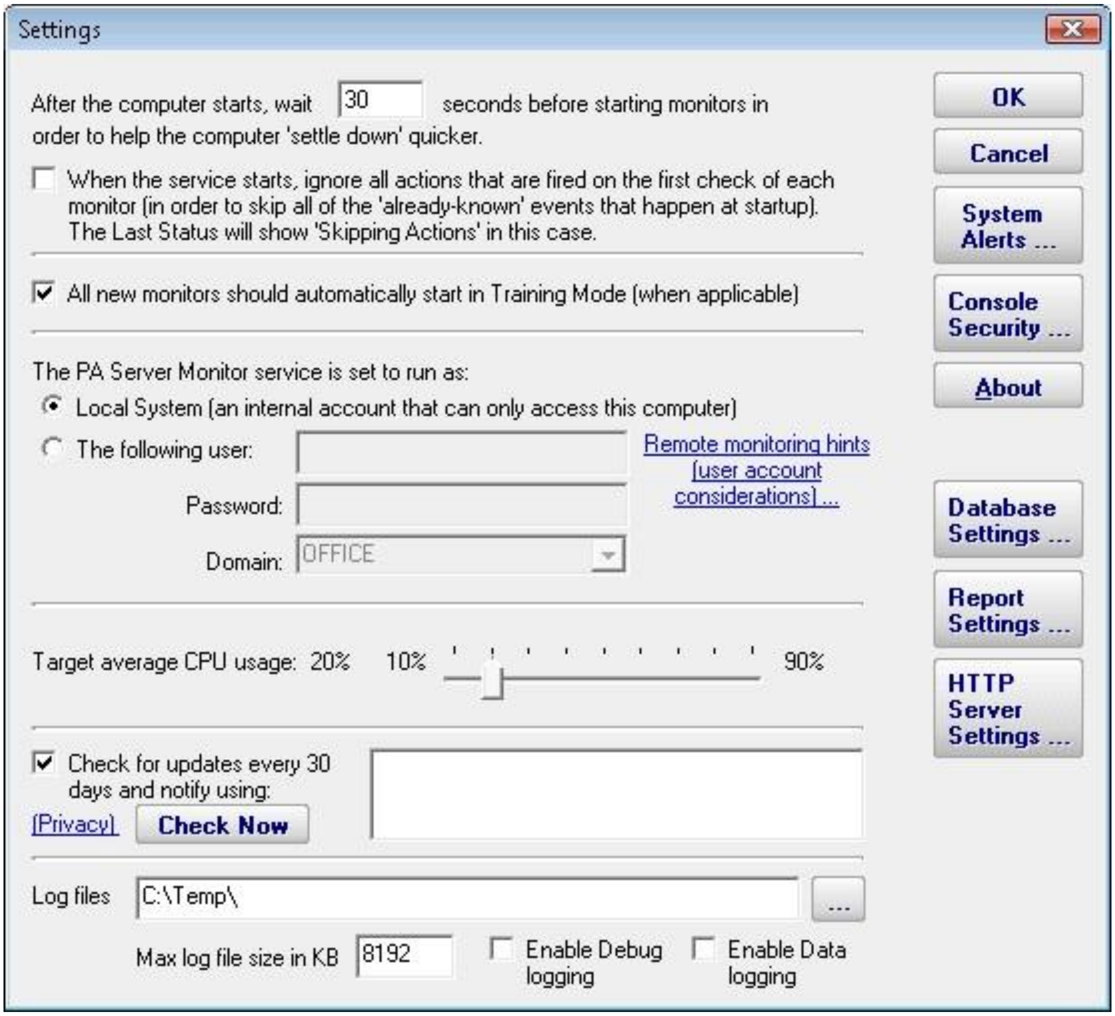
Contents

Global Settings

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

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

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



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

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

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

The PA Server Monitor service is set to run as:

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

○ The following user:

Password:

Domain: OFFICE

Target average CPU usage: 20% 10% 90%

☑ Check for updates every 30 days and notify using:

Log files C:\Temp\

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

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

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

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

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

Contents

Database Settings

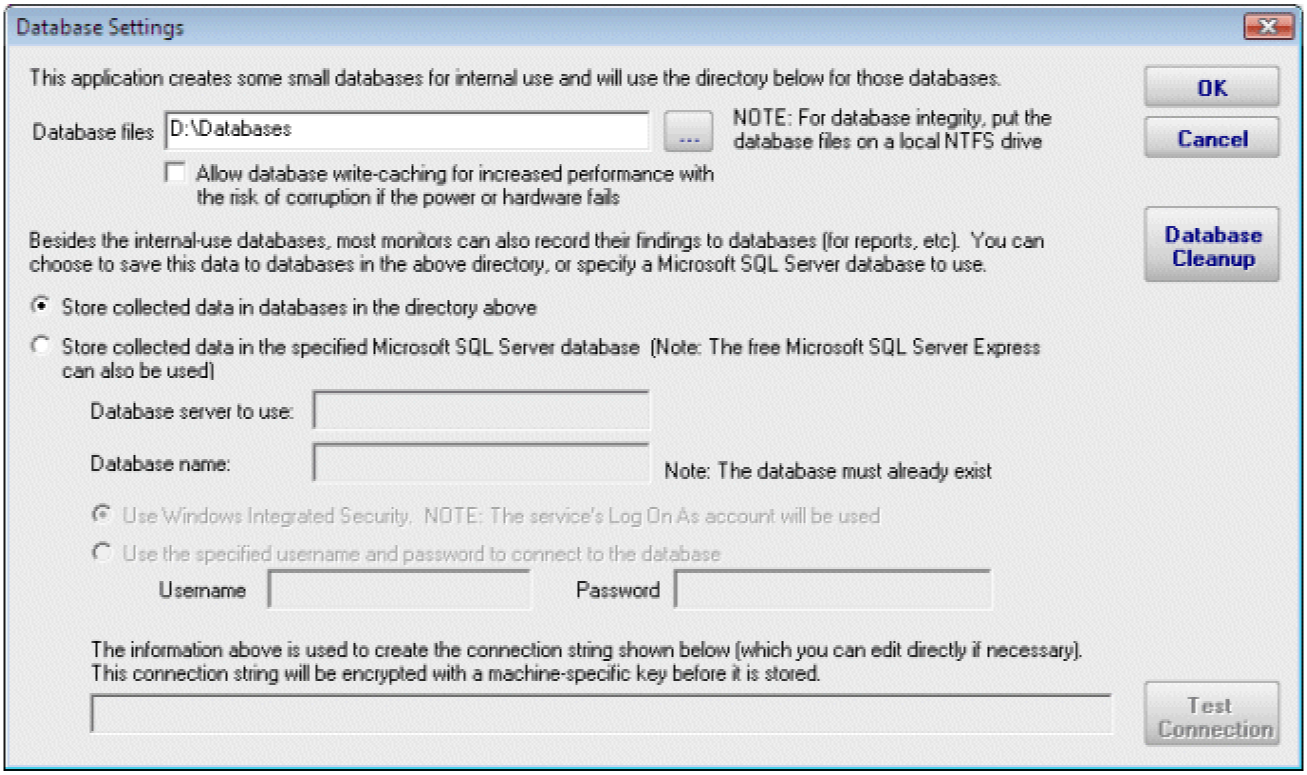
PA Server Monitor needs a place to store the data that it collects during operation. There are two choices available for data storage.

- **SQLite**
  By default, PA Server 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 Server 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.



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

Database files: D:\Databases

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

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

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

● Store collected data in databases in the directory above

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

Database server to use:

Database name:

Note: The database must already exist

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

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

Username: Password:

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

More about Microsoft SQL Server and PA Server 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 Server Monitor (normally `C:\Program Files\PA Server Monitor`.)

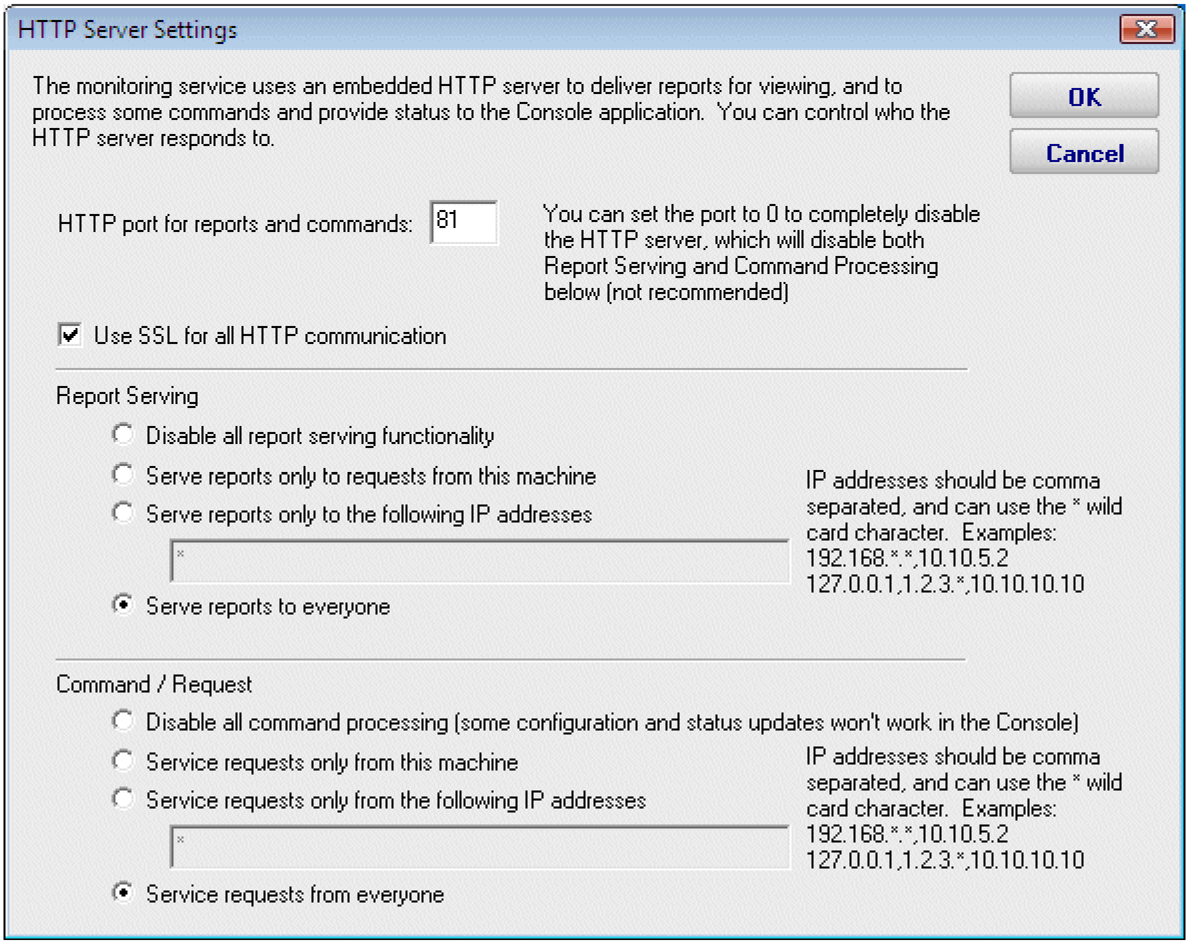
The following configuration data needs to be specified to use SQL Server:

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

HTTP (Web Server) Configuration

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



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

HTTP port for reports and commands: 81

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

☑ Use SSL for all HTTP communication

Report Serving

○ Disable all report serving functionality

○ Serve reports only to requests from this machine

○ Serve reports only to the following IP addresses

*

● Serve reports to everyone

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

Command / Request

○ Disable all command processing (some configuration and status updates won't work in the Console)

○ Service requests only from this machine

○ Service requests only from the following IP addresses

*

● Service requests from everyone

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

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

- **HTTP Port for Reports and Commands**
  This setting lets you set the port which the embedded web server uses to listen for requests. Port 80 is generally used by IIS and Apache as the standard HTTP port for a web server. PA Server 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 Server 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 Server 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 Server 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 Server Monitor responds to commands that are issued by the Console part of PA Server Monitor. You may disable command processing entirely. Or, you may enable command processing, but only from the machine on which PA Server 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.

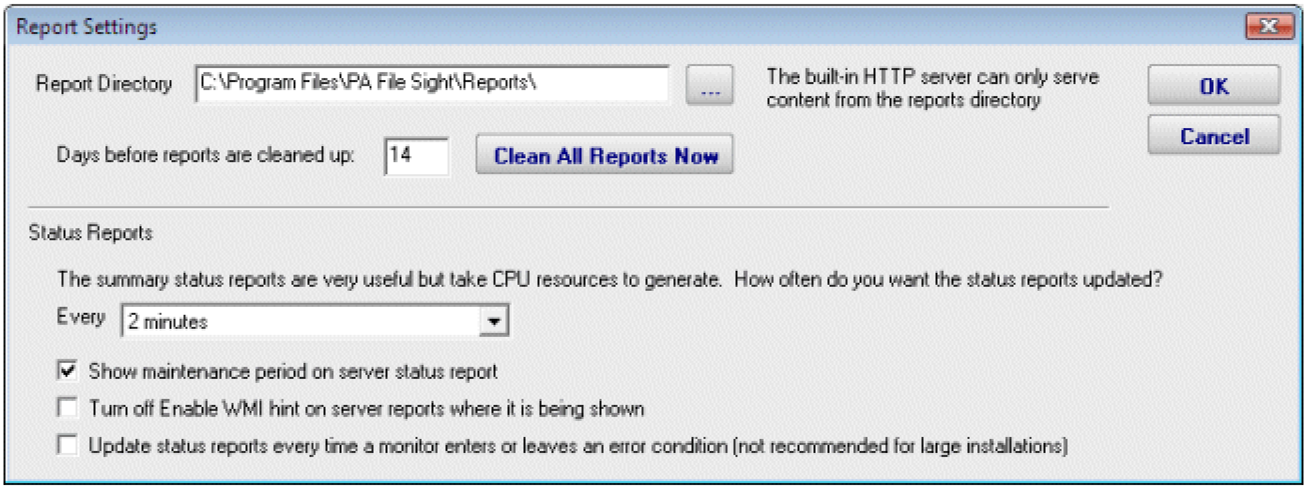
Contents

Report Settings

The Report Settings dialog allows you to customize aspects of the way PA Server 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 Server 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 Server 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 Server 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.



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

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

Days before reports are cleaned up: 14

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

Every 2 minutes

☑ Show maintenance period on server status report

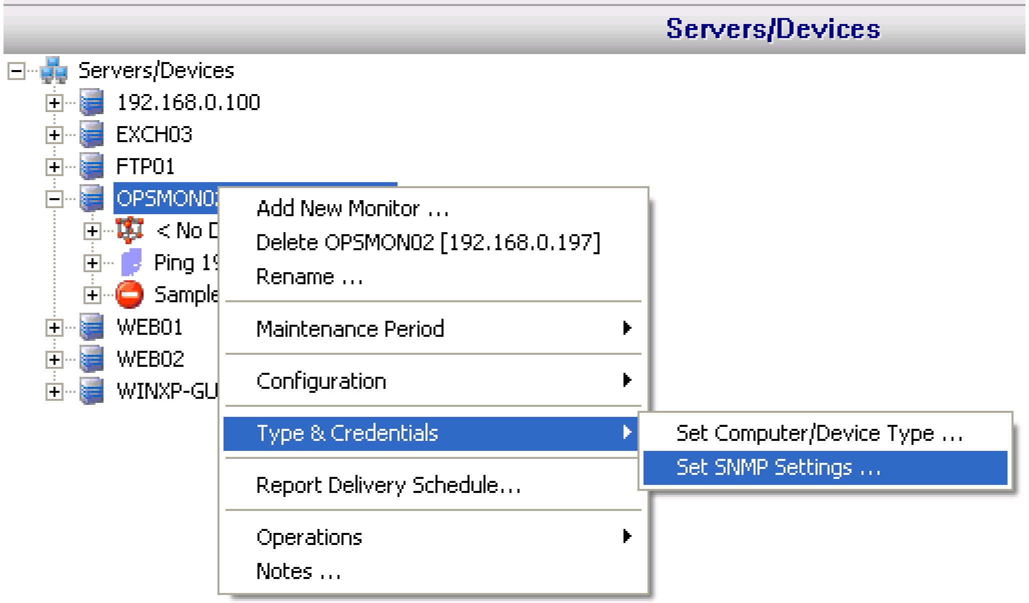
☐ Turn off Enable WMI hint on server reports where it is being shown

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

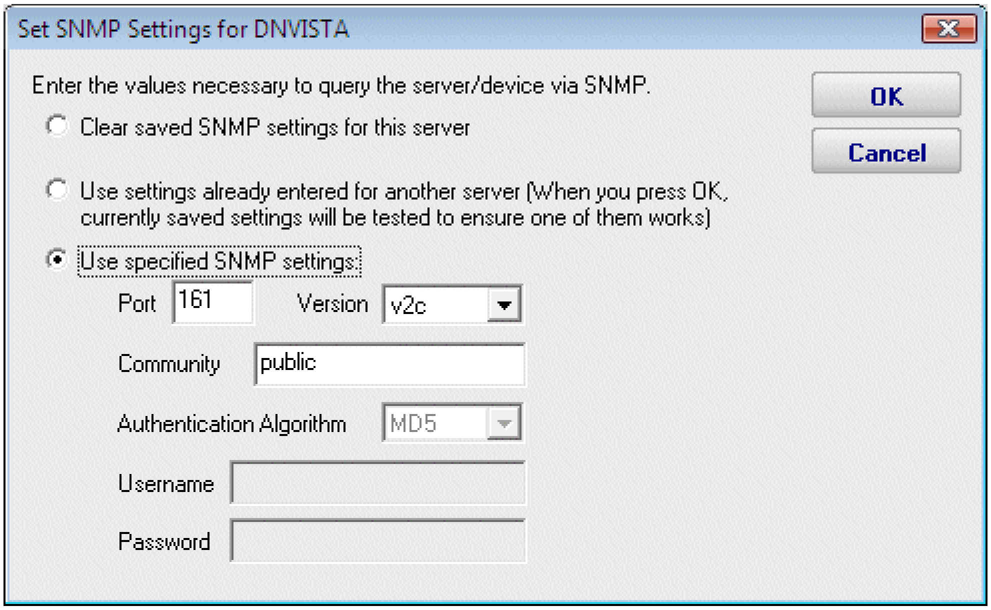
SNMP Settings

PA Server Monitor can associate a set of SNMP (Simple Network Management Protocol) credential with a monitored computer or device.

The following context menu choice allows you to see the Set SNMP Settings dialog.



The Set SNMP Settings dialog allows you to set SNMP credentials that are appropriate for the server being monitored.


Set SNMP Settings for DNVISTA

Enter the values necessary to query the server/device via SNMP.

○ Clear saved SNMP settings for this server

○ Use settings already entered for another server (When you press OK, currently saved settings will be tested to ensure one of them works)

● Use specified SNMP settings

Port: 161 Version: v2c

Community: public

Authentication Algorithm: MD5

Username:

Password:

This dialog allows you to set the following items:

- SNMP version of the remote agent - v1, v2c and v3 are supported. The SNMP version value v2c is the default setting.

- If using SNMP version v3, a username/password needs to be entered
- The community string value is set to 'public' by default

The SNMP settings are used for checking disk space and CPU usage on Linux/*nix machines, as well as by the SNMP Monitor for products that support it.

Contents

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:

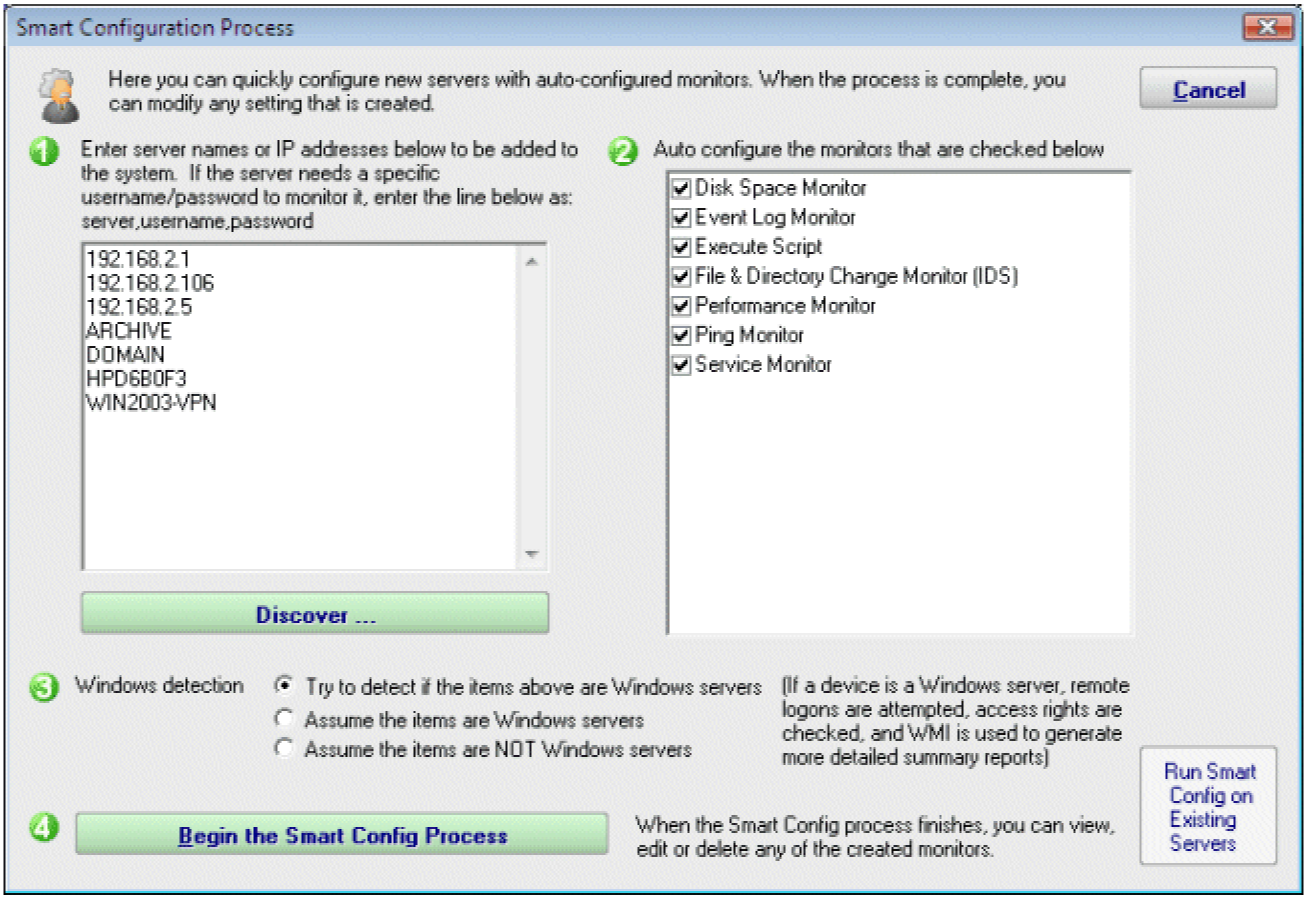
```
server_name,username,password
```

(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.


Smart Configuration Process
Cancel
Discover ...
Begin the Smart Config Process
Run Smart Config on Existing Servers

Here you can quickly configure new servers with auto-configured monitors. When the process is complete, you can modify any setting that is created.

1 Enter server names or IP addresses below to be added to the system. If the server needs a specific username/password to monitor it, enter the line below as: server,username,password

```
192.168.2.1
192.168.2.106
192.168.2.5
ARCHIVE
DOMAIN
HPD6B0F3
WIN2003-VPN
```

2 Auto configure the monitors that are checked below

☑ Disk Space Monitor
☑ Event Log Monitor
☑ Execute Script
☑ File & Directory Change Monitor (IDS)
☑ Performance Monitor
☑ Ping Monitor
☑ Service Monitor

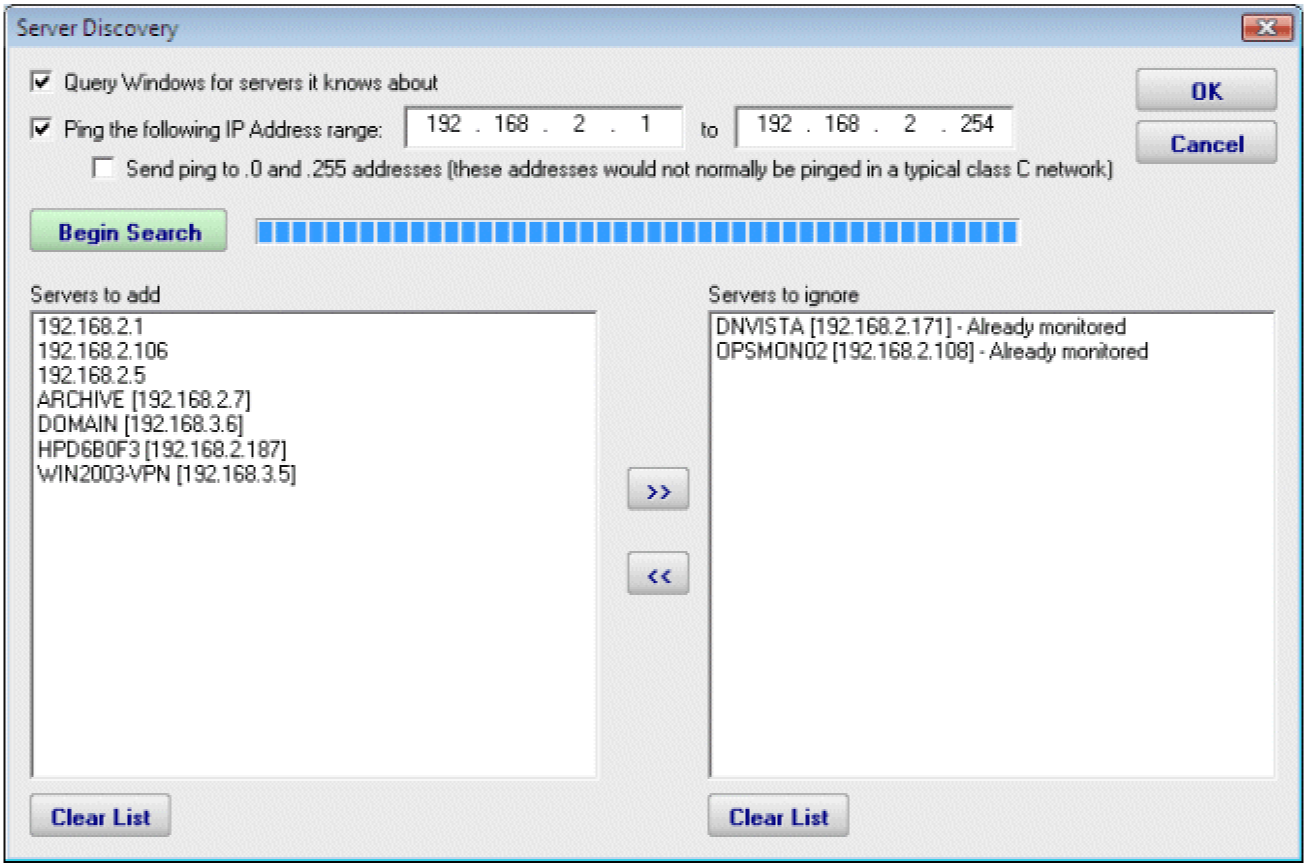
3 Windows detection

● Try to detect if the items above are Windows servers
○ Assume the items are Windows servers
○ Assume the items are NOT Windows servers

(If a device is a Windows server, remote logons are attempted, access rights are checked, and WMI is used to generate more detailed summary reports)

4 When the Smart Config process finishes, you can view, edit or delete any of the created monitors.

Pressing the green button labeled "Discover" in section 1 of this dialog allows PA Server 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.



Server Discovery

☑ Query Windows for servers it knows about

☑ Ping the following IP Address range: 192 . 168 . 2 . 1 to 192 . 168 . 2 . 254

□ Send ping to .0 and .255 addresses (these addresses would not normally be pinged in a typical class C network)

Servers to add

192.168.2.1
192.168.2.106
192.168.2.5
ARCHIVE [192.168.2.7]
DOMAIN [192.168.3.6]
HPD6B0F3 [192.168.2.187]
WIN2003-VPN [192.168.3.5]

Servers to ignore

DNVISTA [192.168.2.171] - Already monitored
OPSMON02 [192.168.2.108] - Already monitored

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 Server 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.

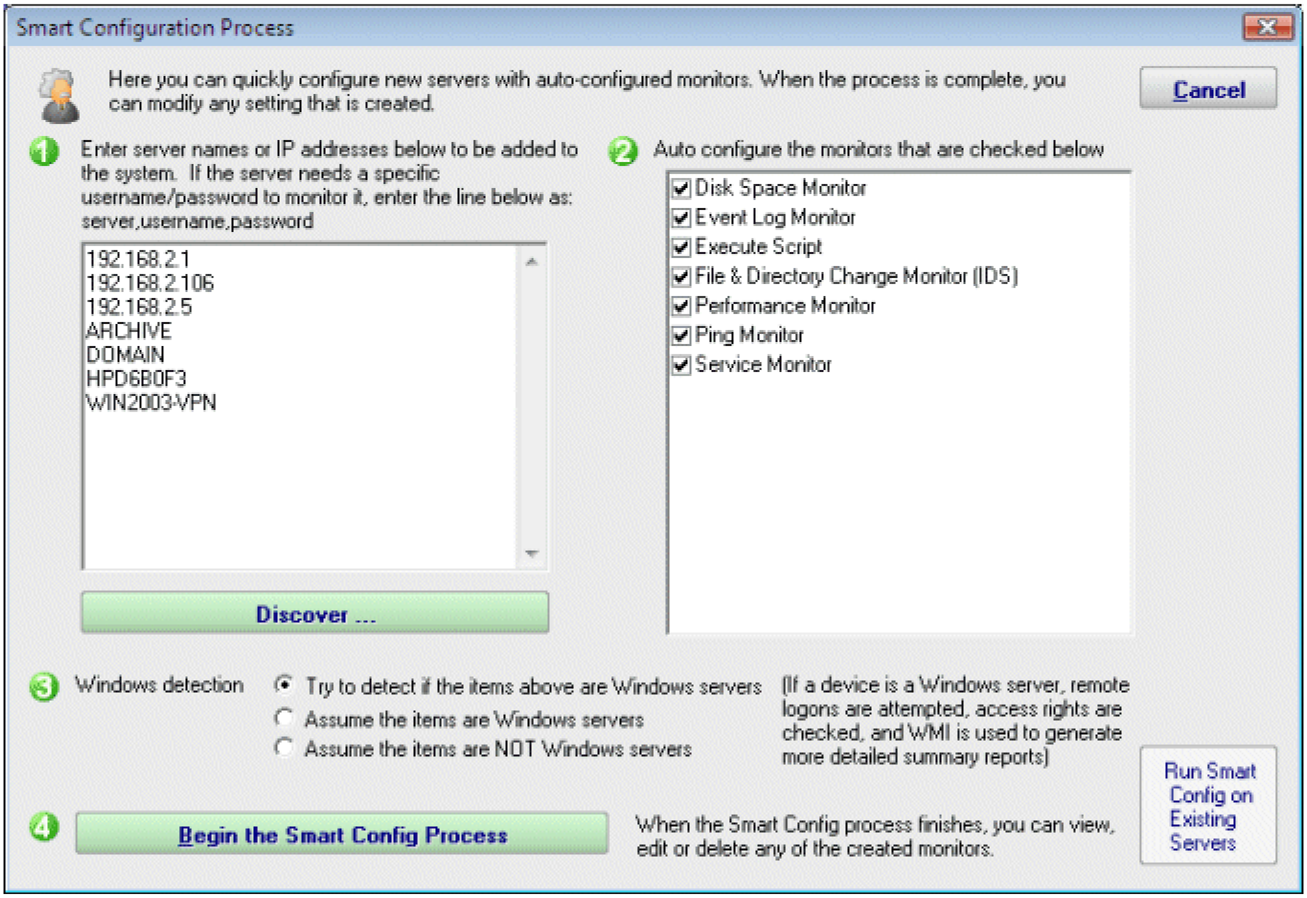
Contents

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.



Smart Configuration Process

Here you can quickly configure new servers with auto-configured monitors. When the process is complete, you can modify any setting that is created.

1 Enter server names or IP addresses below to be added to the system. If the server needs a specific username/password to monitor it, enter the line below as: server,username,password

```
192.168.2.1
192.168.2.106
192.168.2.5
ARCHIVE
DOMAIN
HPD6B0F3
WIN2003-VPN
```

2 Auto configure the monitors that are checked below

☑ Disk Space Monitor
☑ Event Log Monitor
☑ Execute Script
☑ File & Directory Change Monitor (IDS)
☑ Performance Monitor
☑ Ping Monitor
☑ Service Monitor

3 Windows detection

● Try to detect if the items above are Windows servers
○ Assume the items are Windows servers
○ Assume the items are NOT Windows servers

(If a device is a Windows server, remote logons are attempted, access rights are checked, and WMI is used to generate more detailed summary reports)

4 When the Smart Config process finishes, you can view, edit or delete any of the created monitors.

Cancel
Discover ...
Begin the Smart Config Process
Run Smart Config on Existing Servers

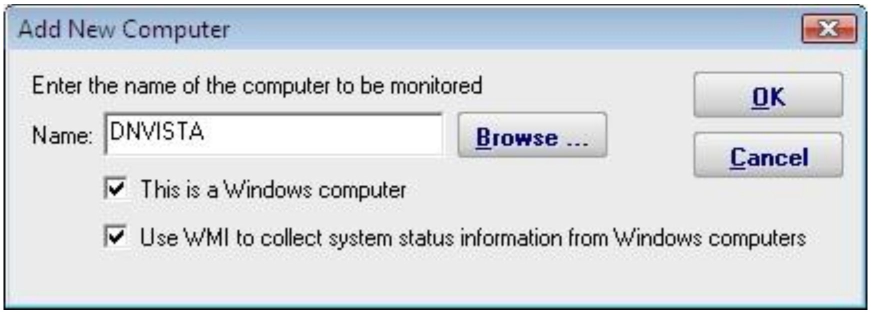
The Smart Config process will add the new computers to the top Servers/Devices group. You can use Bulk Config to easily move many servers at once to different groups.

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.



Add New Computer

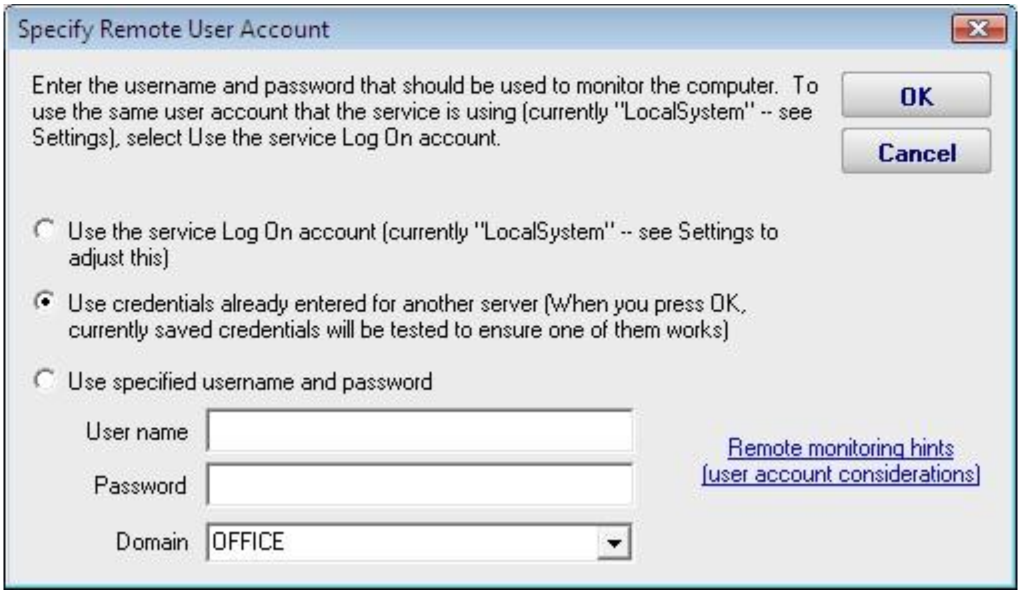
Enter the name of the computer to be monitored

Name: DNVISTA

☑ This is a Windows computer

☑ Use WMI to collect system status information from Windows computers

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.



Specify Remote User Account

Enter the username and password that should be used to monitor the computer. To use the same user account that the service is using (currently "LocalSystem" -- see Settings), select Use the service Log On account.

○ Use the service Log On account (currently "LocalSystem" -- see Settings to adjust this)

● Use credentials already entered for another server (When you press OK, currently saved credentials will be tested to ensure one of them works)

○ Use specified username and password

User name

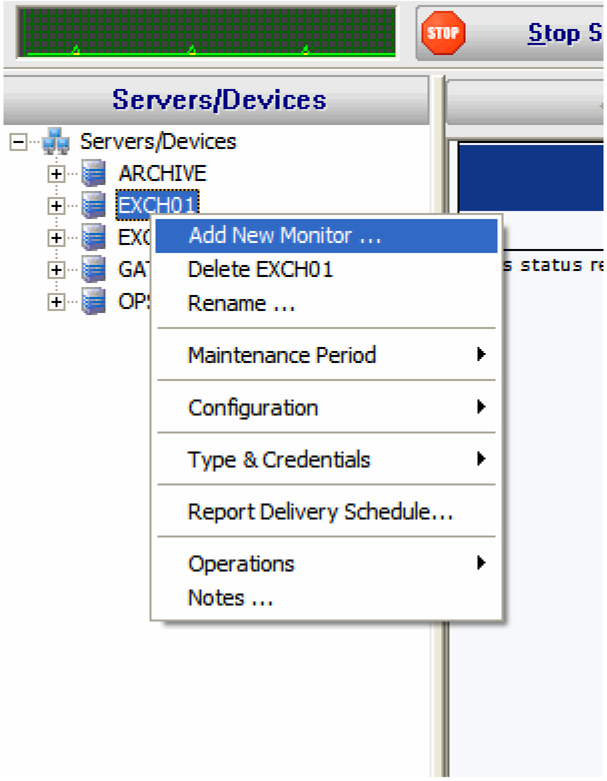
Password

Domain OFFICE

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.

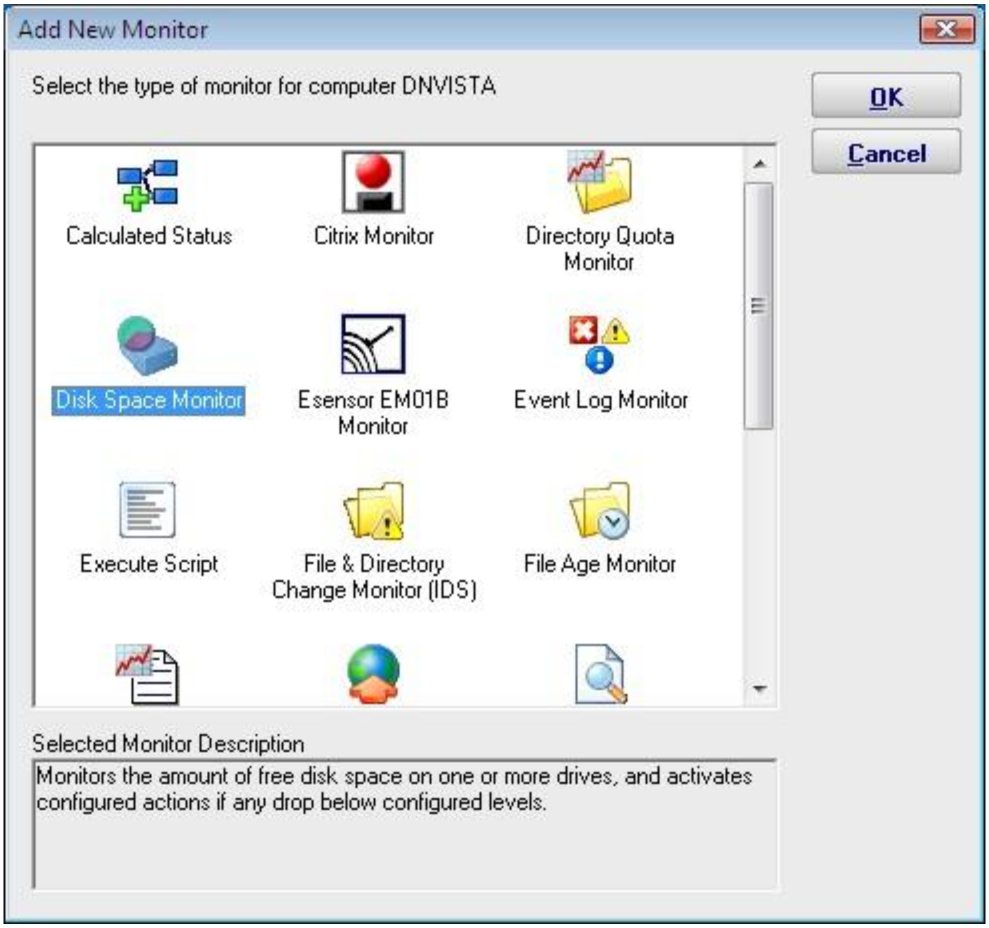
Adding Monitors

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.



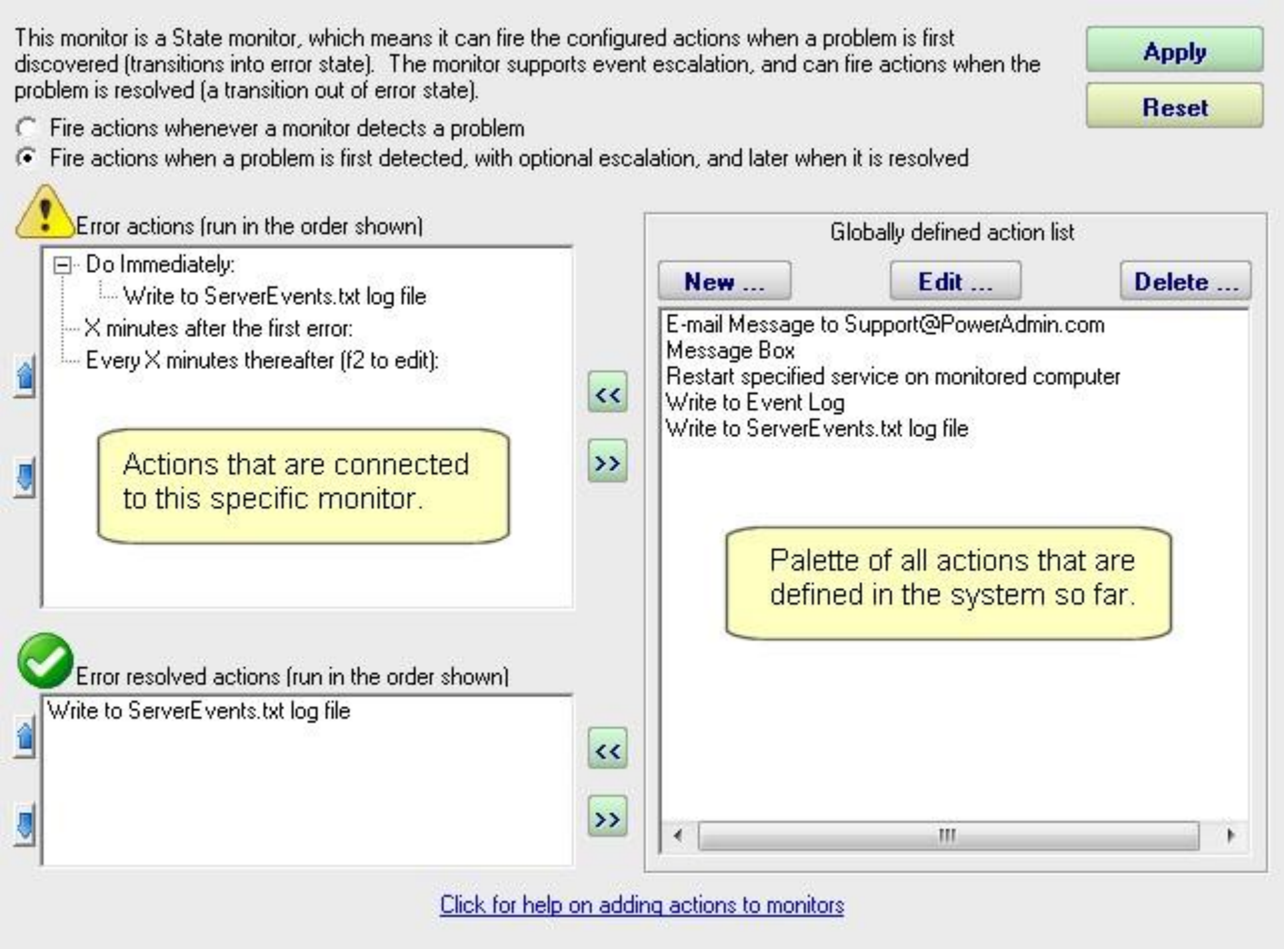
Select the type of monitor for computer DNVISTA

Monitors the amount of free disk space on one or more drives, and activates configured actions if any drop below configured levels.

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).



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

○ Fire actions whenever a monitor detects a problem

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

Error actions (run in the order shown)

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

Actions that are connected to this specific monitor.

Error resolved actions (run in the order shown)

- Write to ServerEvents.txt log file

Globally defined action list

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

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

Click for help on adding actions to monitors

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

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

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

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

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

State vs Event Monitors

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

The following describes how State and Event monitors differ.

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

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

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

Contents

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.

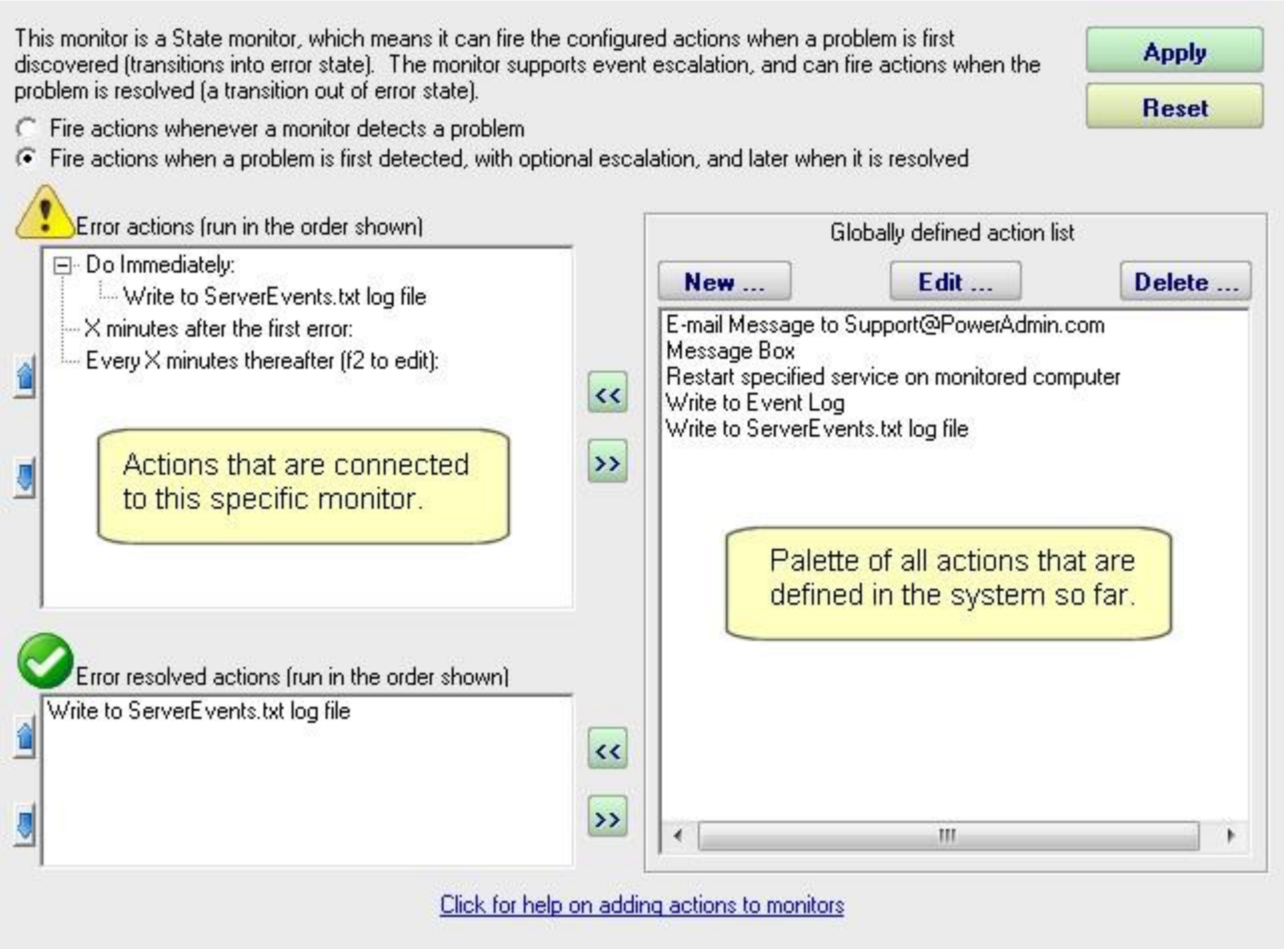
Examples of correct escalation time setting text:

- 12 minutes
- 2 hours
- 1 day

PA Server 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).

○ Fire actions whenever a monitor detects a problem

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

Error actions (run in the order shown)

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

Actions that are connected to this specific monitor.

Error resolved actions (run in the order shown)

Write to ServerEvents.txt log file

Globally defined action list

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

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

Click for help on adding actions to monitors

Contents

Error Auditing

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

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

Three Pieces

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

There are three parts to Error Auditing:

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

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

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

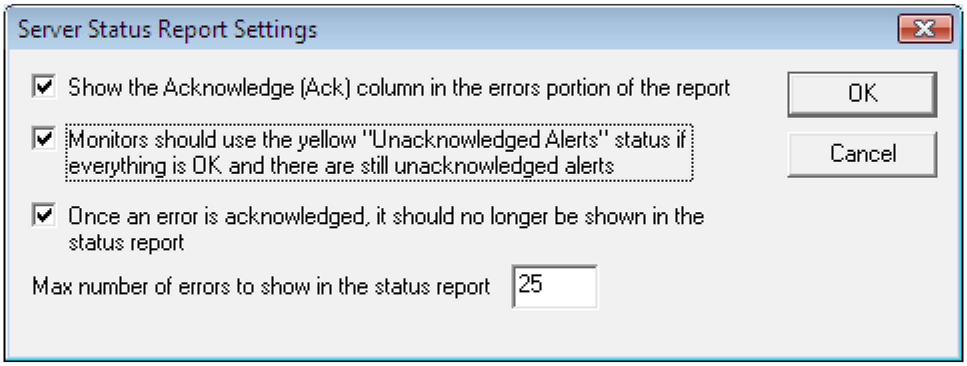
More Details

1. - Product monitors detect and record issues

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

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

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



Server Status Report Settings

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

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

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

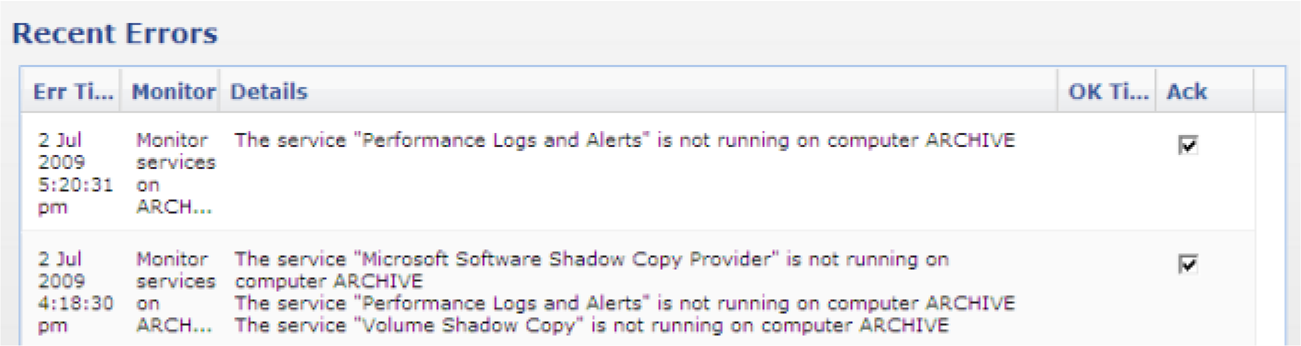
Max number of errors to show in the status report: 25

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

2. - Server administrators acknowledge errors

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

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



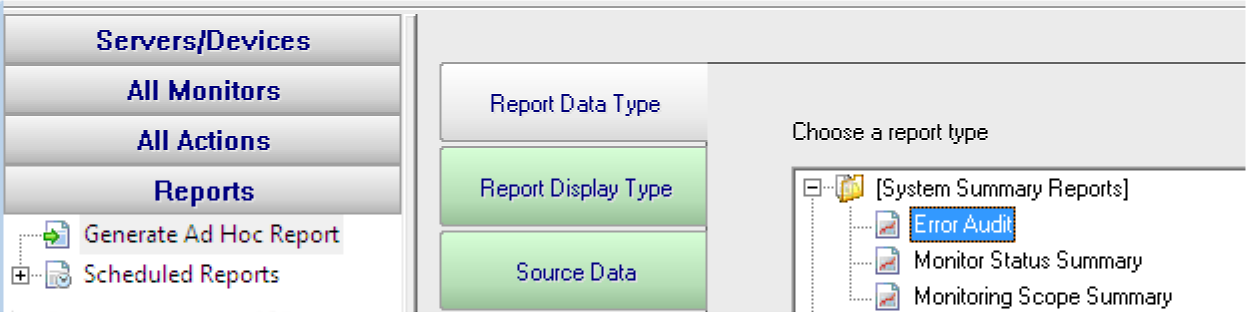
Recent Errors

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

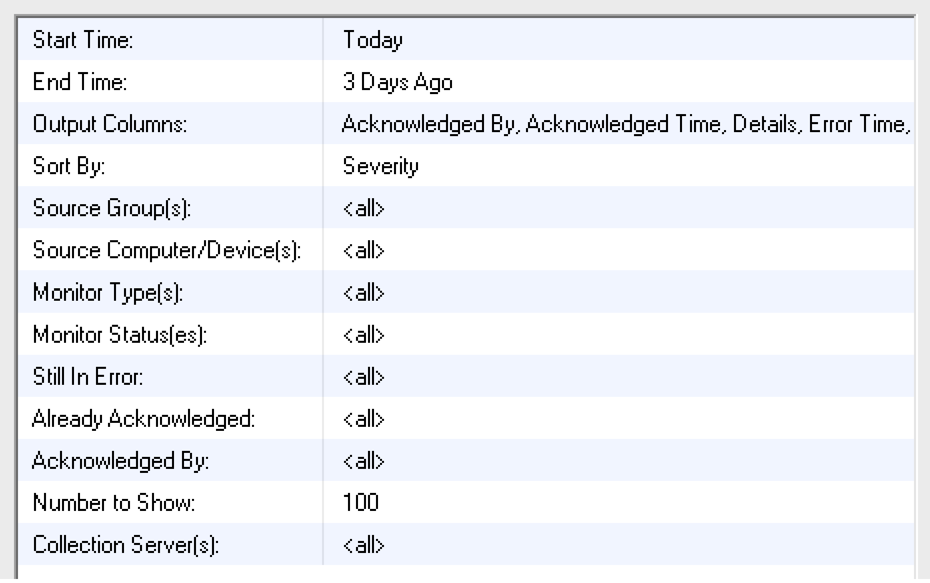
Administrators will often not want to see the error again once they've acknowledged it. This can be controlled via the Report Settings dialog mentioned above.

3. - Error auditing reports for compliance

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



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



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

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

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

Not Just For Auditing

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

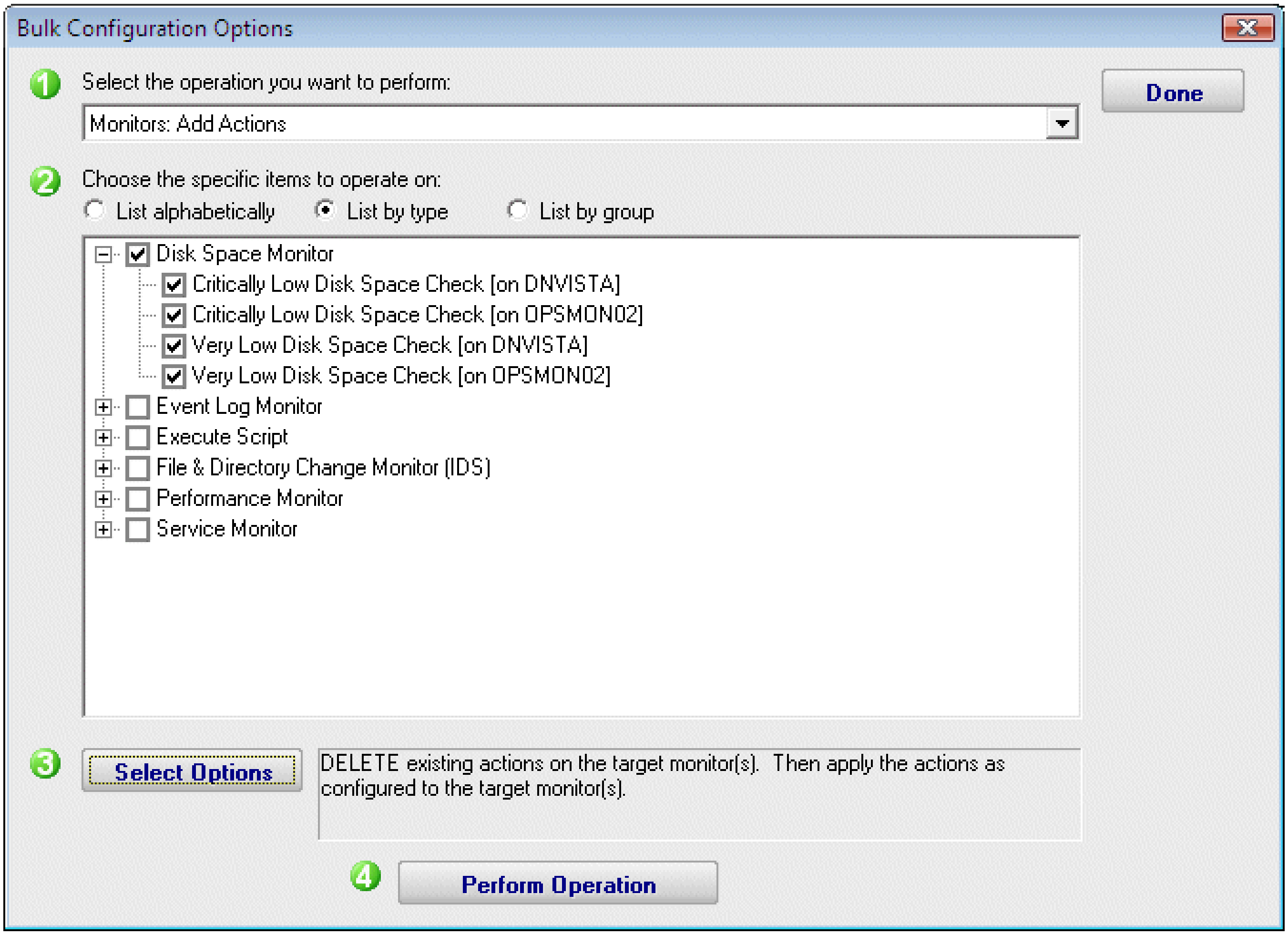
We recommended that each person with a large responsibility have their own Error Audit report so they can quickly see all errors within their area of responsibility. Errors can even be acknowledged on the Error Audit report itself, just like on the server status reports.

Bulk Configuration

The Bulk Configuration feature of PA Server 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.



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

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

- ☑ Disk Space Monitor
  - ☑ Critically Low Disk Space Check [on DNVISTA]
  - ☑ Critically Low Disk Space Check [on OPSMON02]
  - ☑ Very Low Disk Space Check [on DNVISTA]
  - ☑ Very Low Disk Space Check [on OPSMON02]
- □ Event Log Monitor
- □ Execute Script
- □ File & Directory Change Monitor (IDS)
- □ Performance Monitor
- □ Service Monitor

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

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.

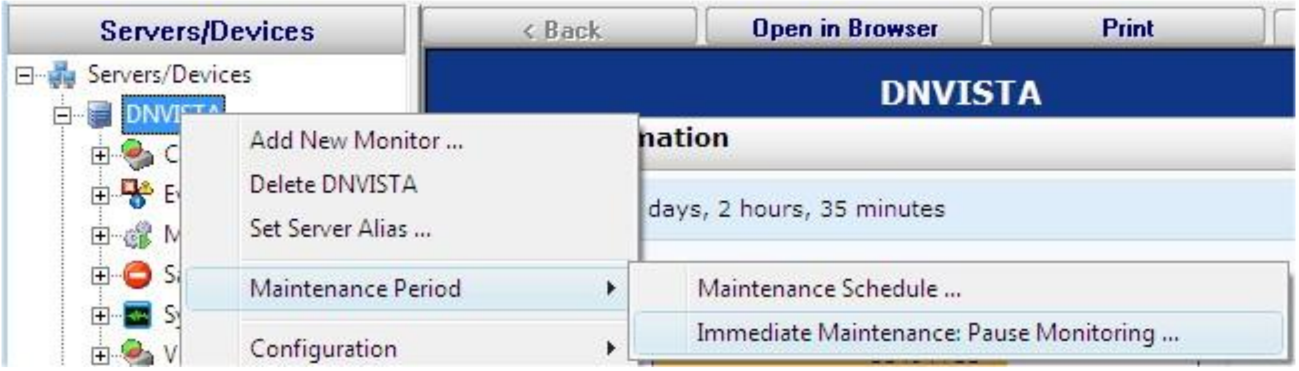
Contents

Maintenance Mode

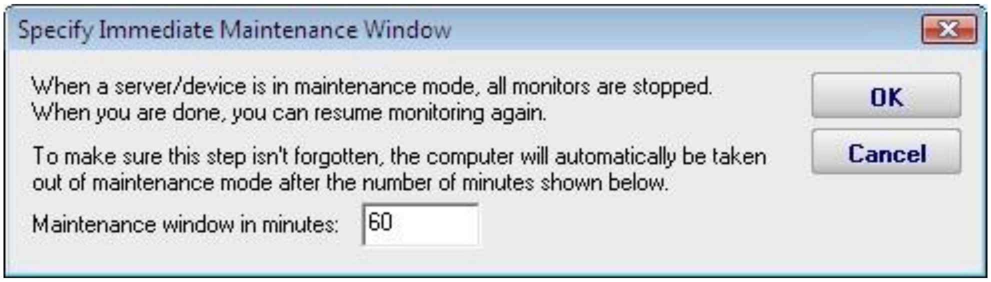
Maintenance Mode is very useful when you'll be working on a computer that is being monitored. Naturally you don't want to receive alerts or have the monitoring service try to correct things that you are working on. Instead of stopping the monitoring service (and potentially forgetting to start it again),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

Manual Maintenance

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



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

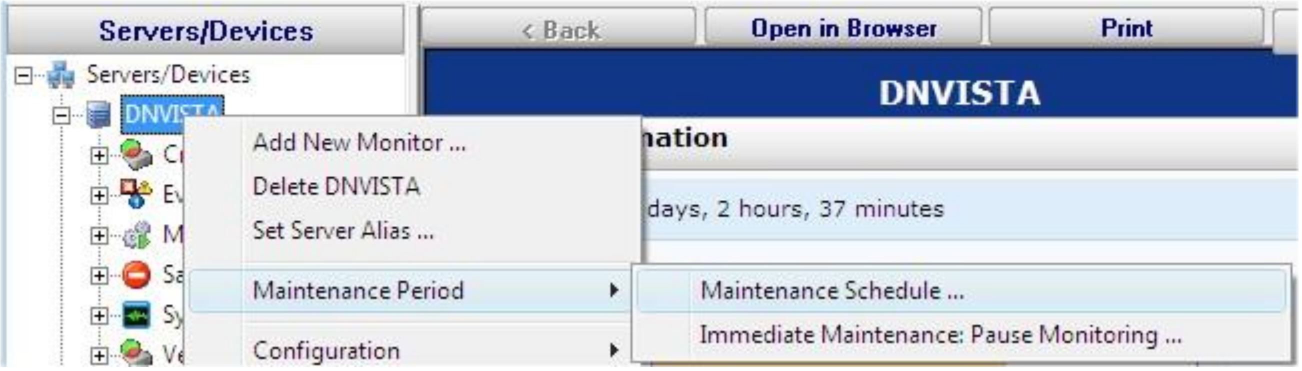


When a server/device is in maintenance mode, all monitors are stopped. When you are done, you can resume monitoring again.

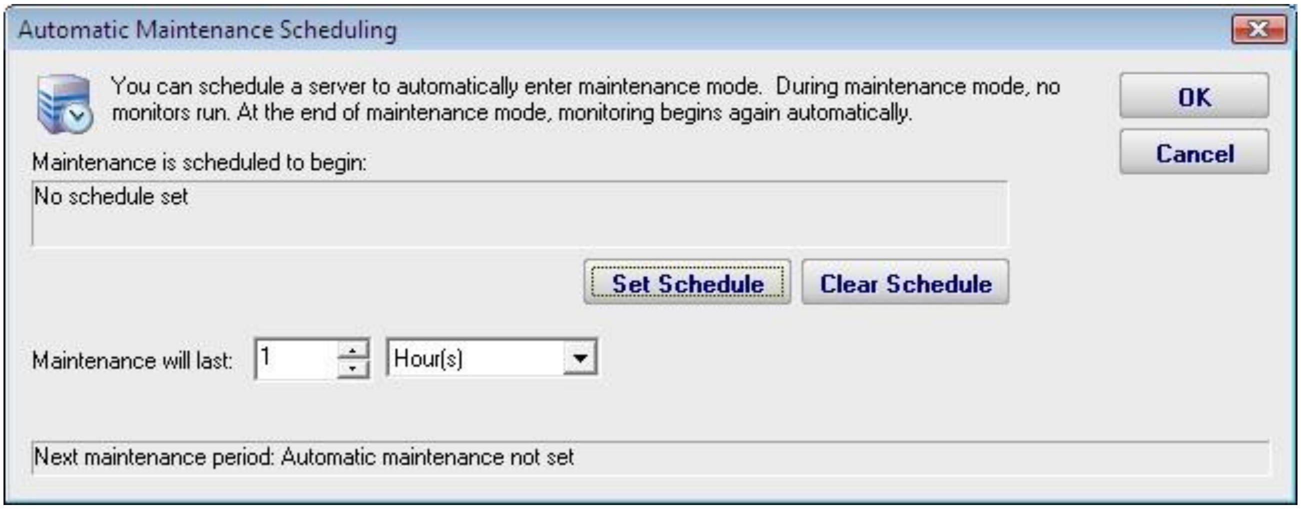
To make sure this step isn't forgotten, the computer will automatically be taken out of maintenance mode after the number of minutes shown below.

Maintenance window in minutes: 60

Scheduled Maintenance



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



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

Maintenance is scheduled to begin:
No schedule set

Maintenance will last: 1 Hour(s)

Next maintenance period: Automatic maintenance not set

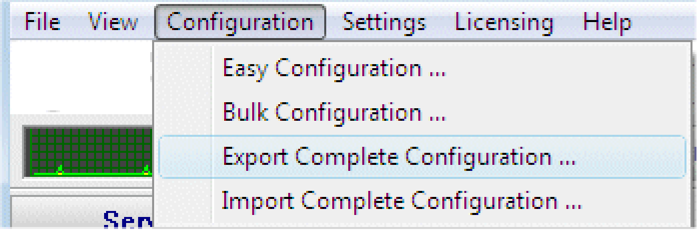
Importing and Exporting Configurations

PA Server 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.

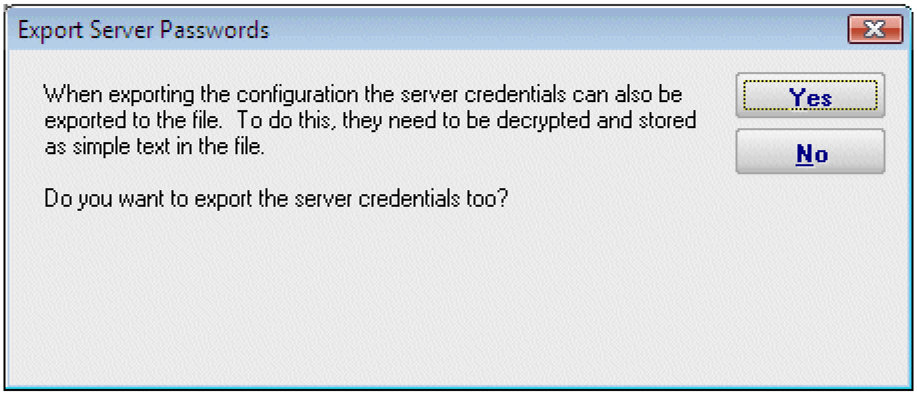
Exporting is a process by which you make PA Server Monitor save configuration data to a special XML format file. Importing is the process that allows PA Server Monitor to read in saved values from the same type of file and to restore the settings.

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 Server 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:


Export Server Passwords

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

Do you want to export the server credentials too?

If you work in an environment in which password and credential data must be handled in a specific manner due to legal or internal company restrictions, you may wish to answer "No" to this prompt. Otherwise, you may wish to allow PA Server 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.

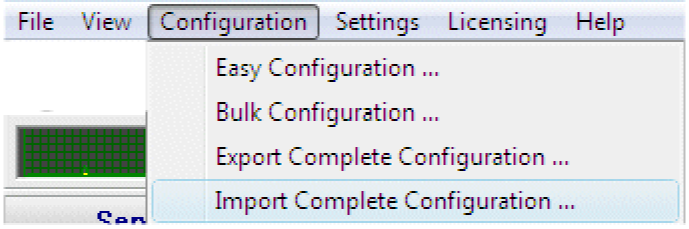
The next dialog to appear after you answer the question above will be a standard "File Save" Windows dialog that allows you to select a file name, and a location at which to save the configuration file. When you export a Complete Configuration, the default file name that is selected will be `PA Server 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 Server Monitor will display a message box but only if you chose to save the credential information.

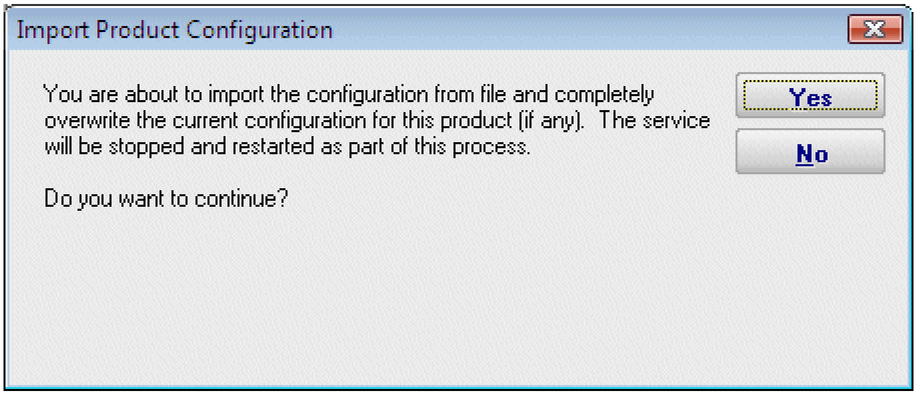
Importing Complete Configuration

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



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

Do you want to continue?

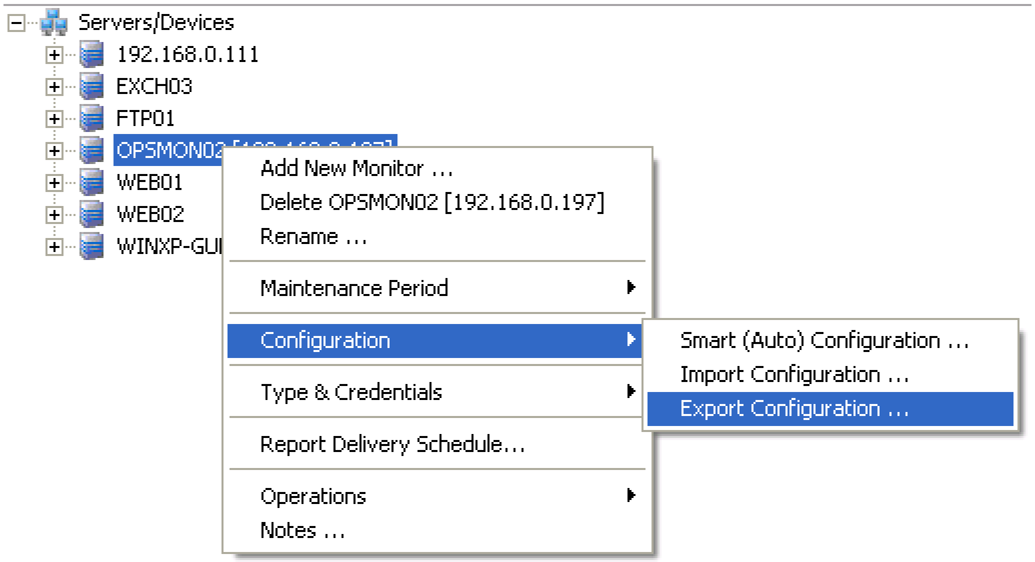
If you answered "Yes" to the question above you will see the standard File Open dialog to select a `.axml` file that you saved to previously.

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

Exporting Individual Server Configuration

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

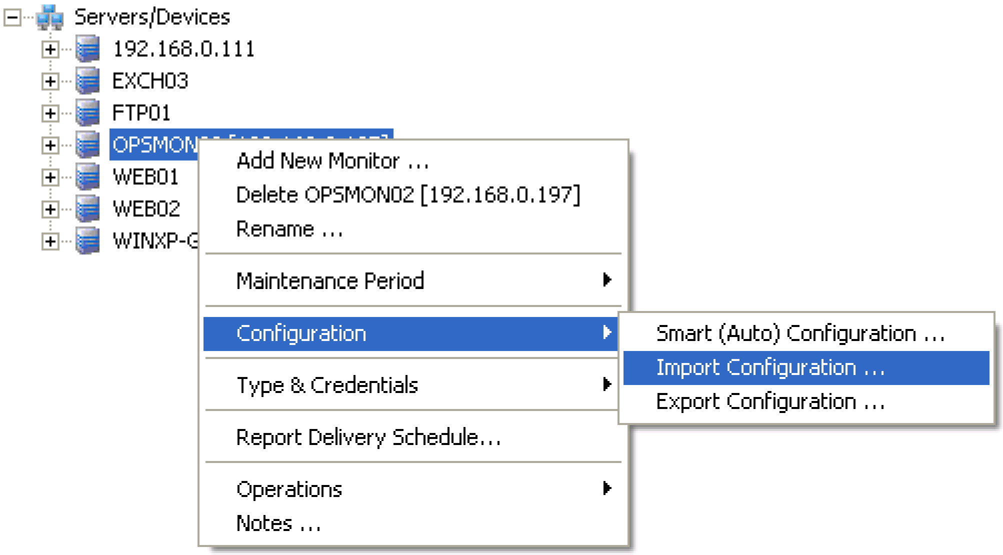
The menu item that selects the export server operation is accessed by right clicking a server or device whose configuration you wish to export. The menu appears as follows.



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

Contents

External API

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

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

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

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

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

Return Values

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

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

Errors are returned as:

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

API Commands

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

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

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

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

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

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

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

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

Monitors

Contents

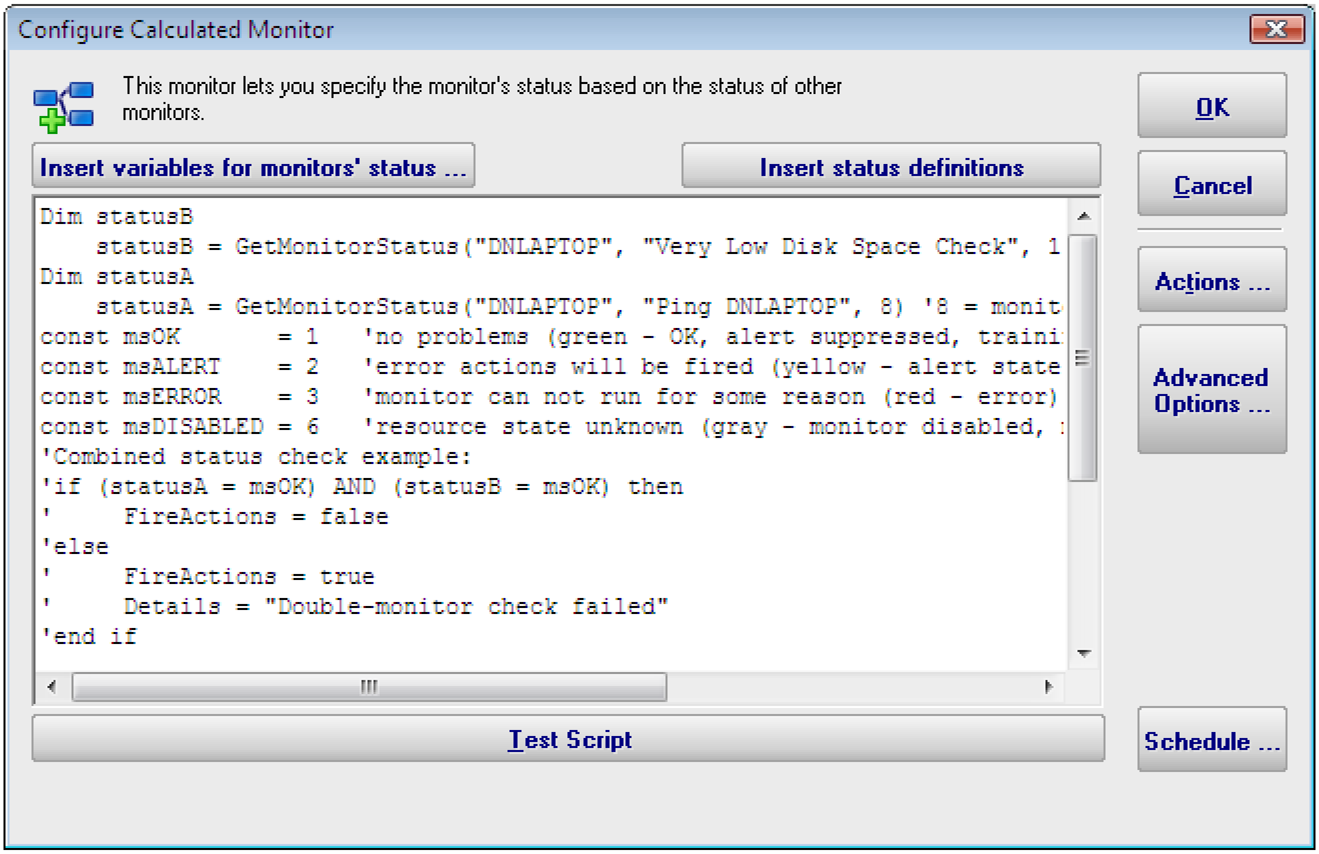
Calculated Status Monitor

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.



Configure Calculated Monitor
OK
Cancel
Actions ...
Advanced Options ...
Insert variables for monitors' status ...
Insert status definitions
Test Script
Schedule ...

This monitor lets you specify the monitor's status based on the status of other monitors.

```
Dim statusB
    statusB = GetMonitorStatus("DNLAPTOP", "Very Low Disk Space Check", 1
Dim statusA
    statusA = GetMonitorStatus("DNLAPTOP", "Ping DNLAPTOP", 8) '8 = monit
const msOK       = 1   'no problems (green - OK, alert suppressed, traini
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 - monitor disabled, :
'Combined status check example:
'if (statusA = msOK) AND (statusB = msOK) then
'     FireActions = false
'else
'     FireActions = true
'     Details = "Double-monitor check failed"
'end if
```

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.

Contents

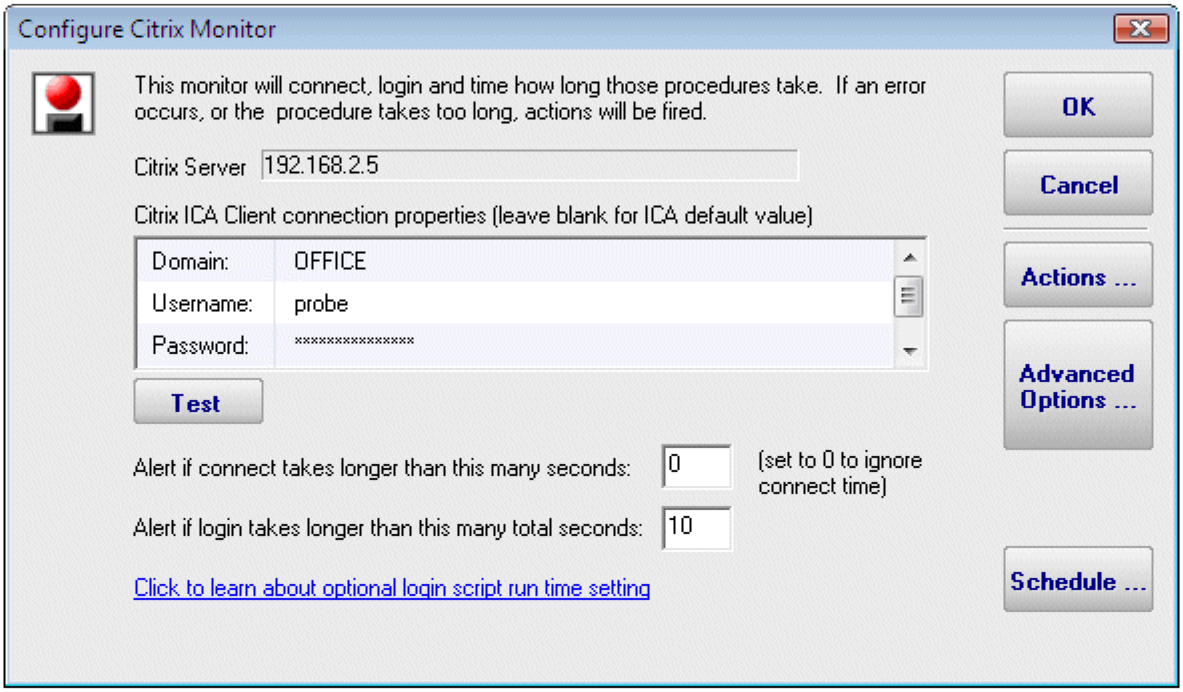
Citrix Monitor

The Citrix monitor is a simple "health check" of a Citrix XenServer (formerly Citrix Presentation Server). The monitor will periodically connect to and log in to the Citrix server, and will time that event. If the login fails to occur, or if it takes too long, the monitor will enter the alert state and fire actions.

The Citrix monitor expects to find a Citrix server at the address of the "computer" that the monitor is attached to. Normally, a Citrix server will require its own Computer entry in the Navigation Pane's list of computers and devices and that entry will indicate the network name or IP address of the Citrix server.

NOTE: The Citrix Monitor requires the Citrix ICA Client to be installed on the same machine as PA Server Monitor

The dialog below is used to configure the Citrix Monitor.



Configure Citrix Monitor

This monitor will connect, login and time how long those procedures take. If an error occurs, or the procedure takes too long, actions will be fired.

Citrix Server: 192.168.2.5

Citrix ICA Client connection properties (leave blank for ICA default value)

Domain:	OFFICE
Username:	probe
Password:	***************

Alert if connect takes longer than this many seconds: 0 (set to 0 to ignore connect time)

Alert if login takes longer than this many total seconds: 10

Click to learn about optional login script run time setting

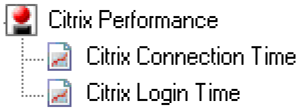
You need to enter the domain name, user name, and password into the dialog. If the Citrix server is configured for a non standard port, you need to enter that port value too.

The Schedule function specifies the interval at which the test of the Citrix monitor (the connection and test login sequence) will be applied.

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 Citrix monitor supports creating reports on the connect and login times that were recorded. You can create bar and line charts, as well as .CSV and tabular HTML reports.

Detecting Other Citrix Login Failures

Logging into a Citrix server involves various stages. The first two stages are **connect** then **login**. Successfully passing through these puts a client into a logged-in relationship with the server (the client's credentials have been accepted and a session is established). At this point, however, the session may not be fully functional from a user standpoint. For example, there may be Windows Startup programs expected to run (or other login actions that are launched). This means that the time to login (the time to establish valid credentials) may happen rather quickly while the time needed to get a fully running Windows may take longer. In this way, **login** can be subdivided as follows:

```
    1) Initial Citrix Login (Validating Credentials)
```

and

```
    2) Running Windows Startup Programs
```

The alert value supplied for "Alert if login takes longer than this many seconds" is associated with the first of those. Normally, this is not noteworthy, but there is a known "black hole" condition in Citrix Servers where the Initial Citrix Login works, but nothing happens after that. Users who experience this often describe it as a hung server. When a server enters such a state, it is difficult to detect because the Initial Citrix Login works.

If such a hung condition is suspected, then it can be detected by using advanced features within PA Server Monitor. Here is how:

1. Specify how long to it takes for the Windows Startup Programs to run.

In the registry on the machine running PA Server Monitor, specify the number of seconds that the Citrix monitor should stay logged in to allow the all Windows Startup Programs to run. That registry setting is:

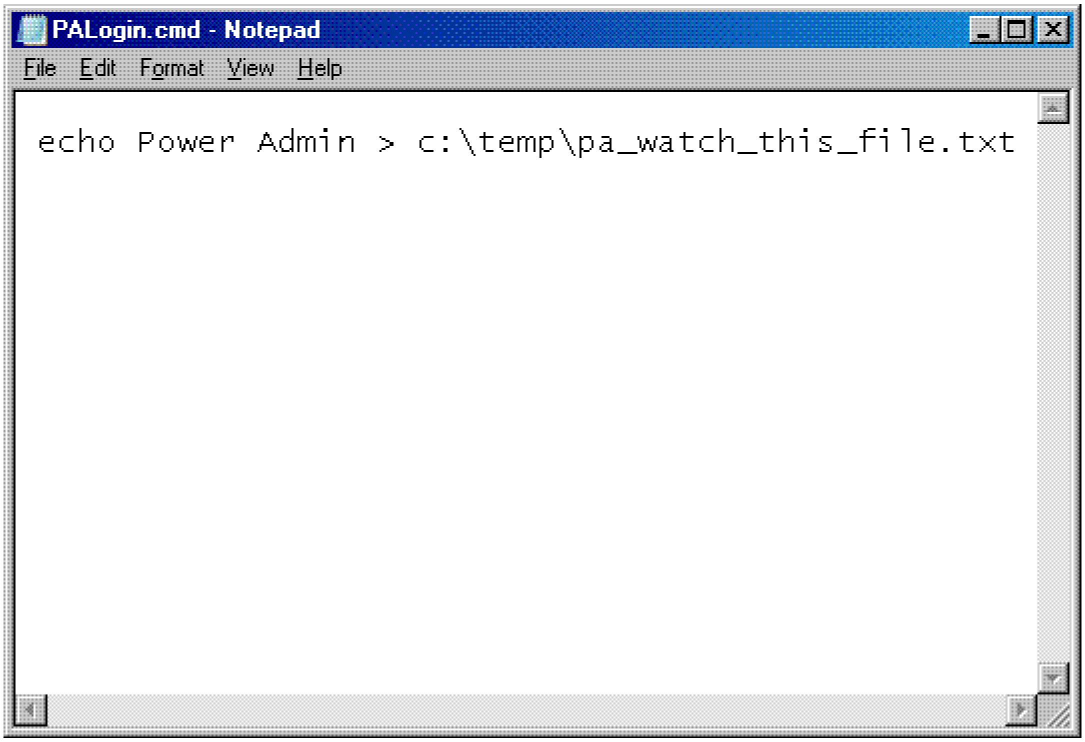
```
 HKEY_LOCAL_MACHINE\SOFTWARE\PowerAdminServerMonitor
[DWORD]Citrix_LoginScriptRunSeconds
```

You should set this value to match how long it takes for your startup programs to launch in your Citrix environment. For example, if after logging into Citrix it takes an additional 15 seconds for Windows to run the programs in the Startup folder, then you would set this value to 15.

2. Create a Citrix script.

Using the same Citrix user specified in PA Server Monitor, log onto the Citrix server and add a batch file to your Windows Startup folder. This batch file (or startup script) is a simple text file created with Notepad. You should save it as a .CMD file (for example, C:\TEMP\PALogin.CMD) and then add C:\TEMP\PALogin.CMD to your Windows Startup. The startup script (the .CMD file) should contain the following line:

```
    echo Power Admin > c:\temp\pa_watch_this_file.txt
```



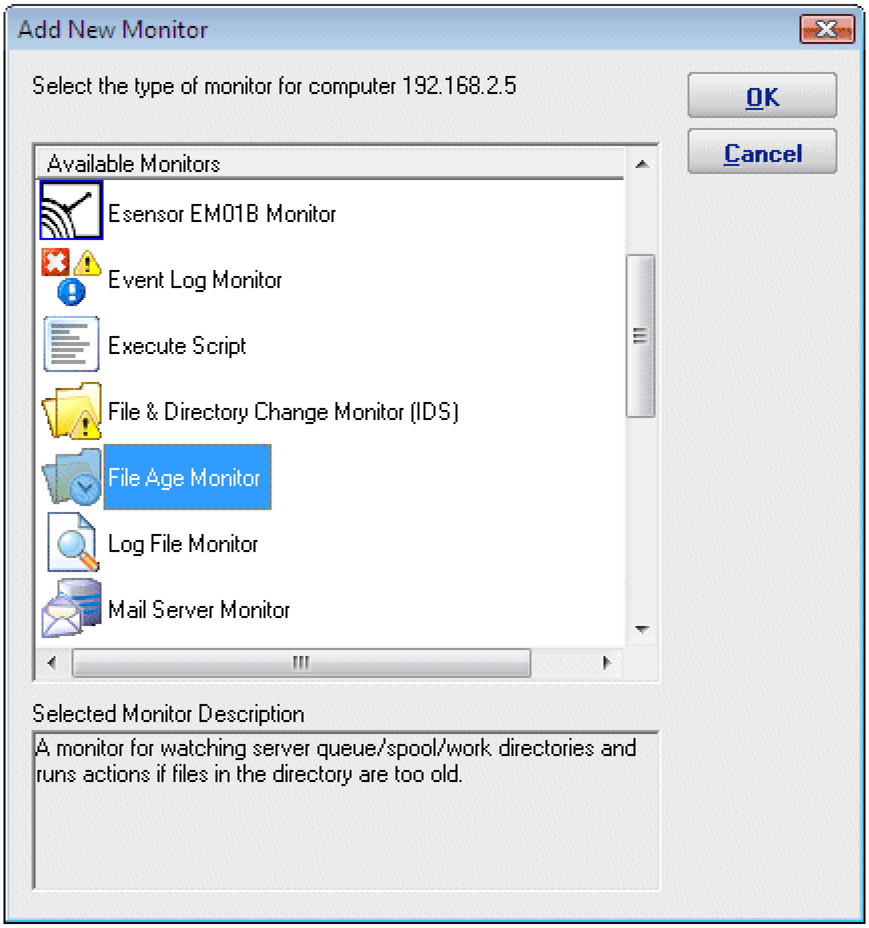
```
echo Power Admin > c:\temp\pa_watch_this_file.txt
```

What this does is it overwrites the text file called "pa_watch_this_file.txt" every time the user logs in.

The key here is this: if for some reason the Windows Startup Programs do not run, then the text file pa_watch_this_file.txt will not be refreshed (it will grow stale). We will then monitor that file (see the next step) and if it is ever older than expected, then we know that the Running of Windows Startup Programs is not taking place as expected. That is, we will know that we can log onto the Citrix server, but the server is acting as if it is in a hung state.

3. Monitor for a stale file.

If you followed the previous step, then you have configured a Citrix user such that a Windows Startup script will run every time that user logs in; in the example provided, it will create a file called c:\temp\pa_watch_this_file.txt. You now need to monitor the age of that file using PA Server Monitor. To do that, add a File Age Monitor as follows:

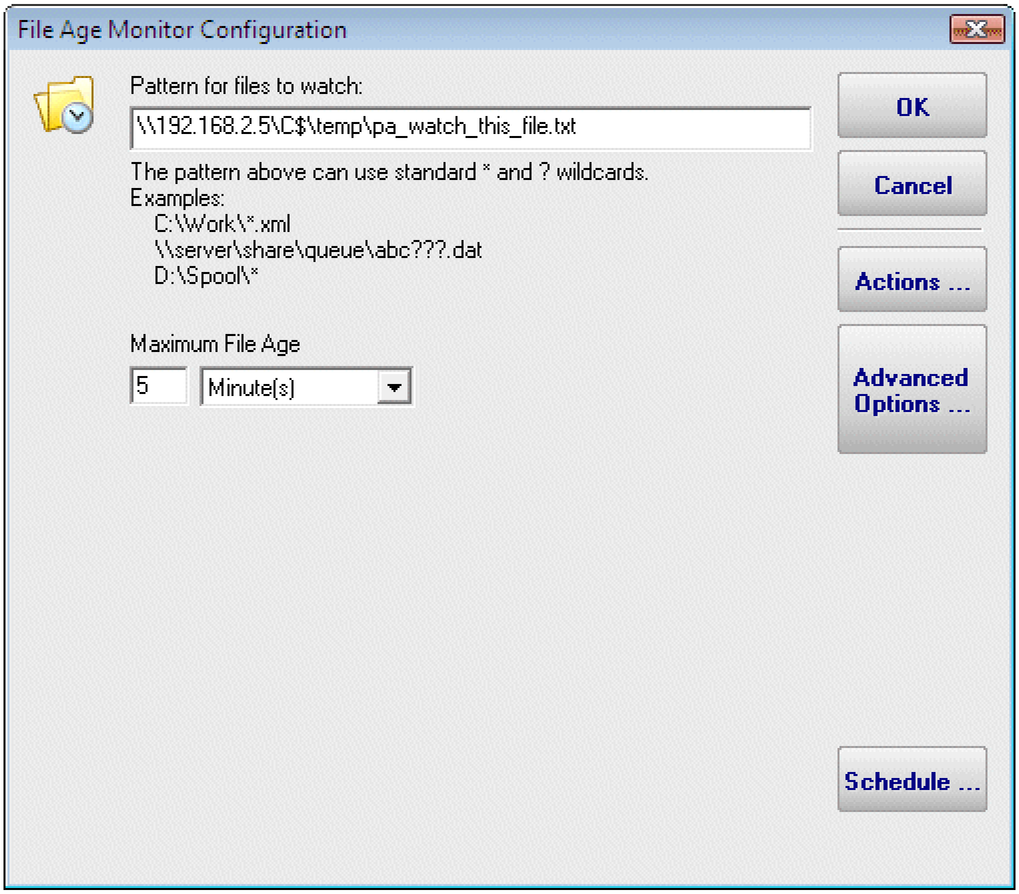


Select the type of monitor for computer 192.168.2.5

A monitor for watching server queue/spool/work directories and runs actions if files in the directory are too old.

If the Citrix Monitor is running every four minutes (as an example), then a full login should happen every four minutes and the file we are monitoring should never be older than five minutes. We will monitor that condition.

NOTE: If PA Server Monitor is not running on the Citrix server itself, then a UNC designator can be supplied for the file (pa_watch_this_file.txt).



File Age Monitor Configuration

Pattern for files to watch:

\\192.168.2.5\C$\temp\pa_watch_this_file.txt

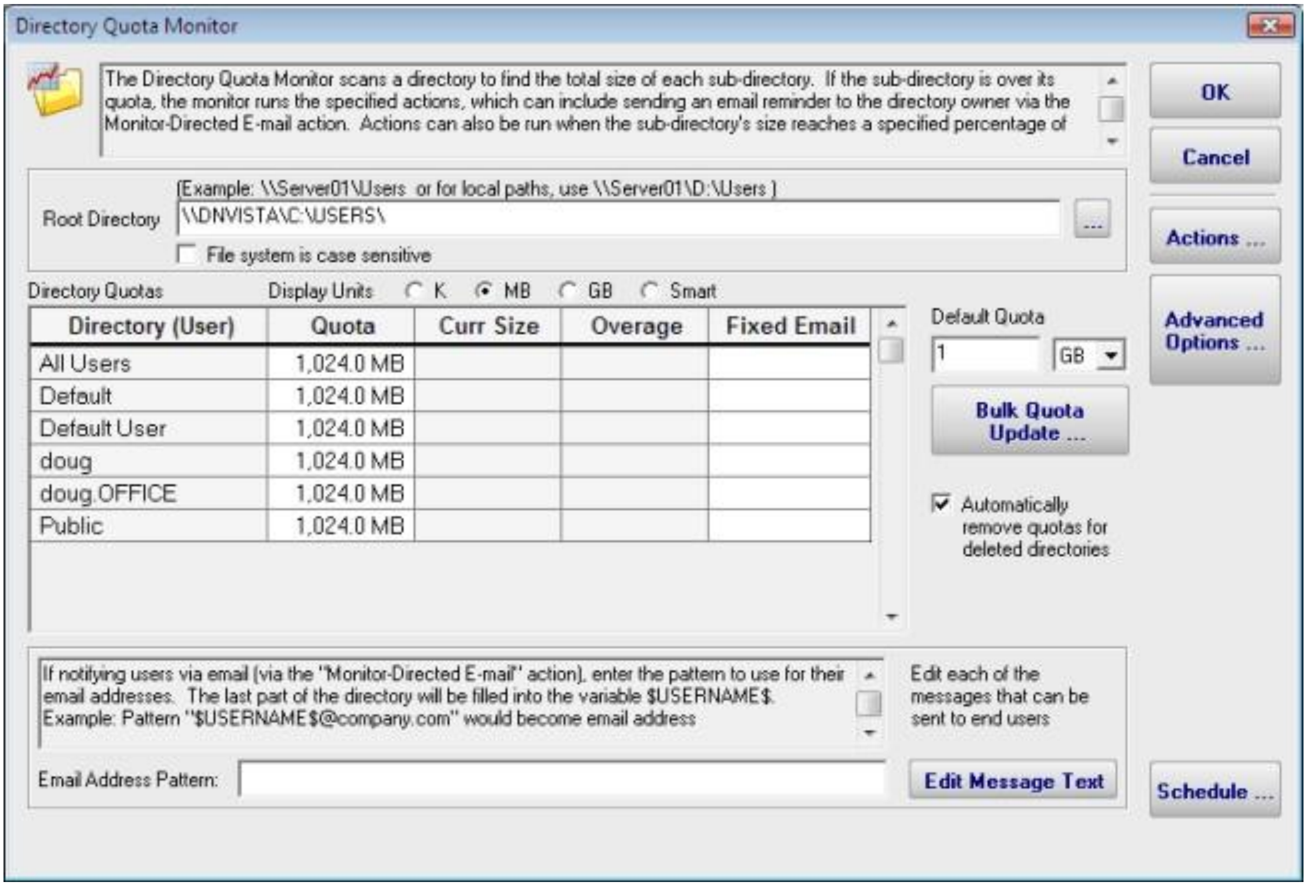
The pattern above can use standard * and ? wildcards.
Examples:
C:\Work\*.xml
\\server\share\queue\abc???.dat
D:\Spool\*

Maximum File Age

5 Minute(s)

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.



The Directory Quota Monitor scans a directory to find the total size of each sub-directory. If the sub-directory is over its quota, the monitor runs the specified actions, which can include sending an email reminder to the directory owner via the Monitor-Directed E-mail action. Actions can also be run when the sub-directory's size reaches a specified percentage of

(Example: \\Server01\Users or for local paths, use \\Server01\D:\Users)

Root Directory \\DNVISTA\C:\USERS\

☐ File system is case sensitive

Directory Quotas Display Units ○ K ● MB ○ GB ○ Smart

Directory (User)	Quota	Curr Size	Overage	Fixed Email
All Users	1,024.0 MB			
Default	1,024.0 MB			
Default User	1,024.0 MB			
doug	1,024.0 MB			
doug.OFFICE	1,024.0 MB			
Public	1,024.0 MB			

Default Quota 1 GB

☑ Automatically remove quotas for deleted directories

If notifying users via email (via the "Monitor-Directed E-mail" action), enter the pattern to use for their email addresses. The last part of the directory will be filled into the variable $USERNAME$. Example: Pattern "$USERNAME$@company.com" would become email address

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

Email Address Pattern:

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

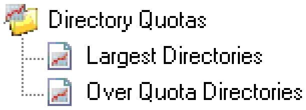
- Set the default quota which will be used for any directory that doesn't have a quota already specified (including new directories discovered during a scan)
- Manually enter quota values in the Quota column for any individual directory (specify units of K, MB or GB)
- Use the Bulk Quota Update mechanism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

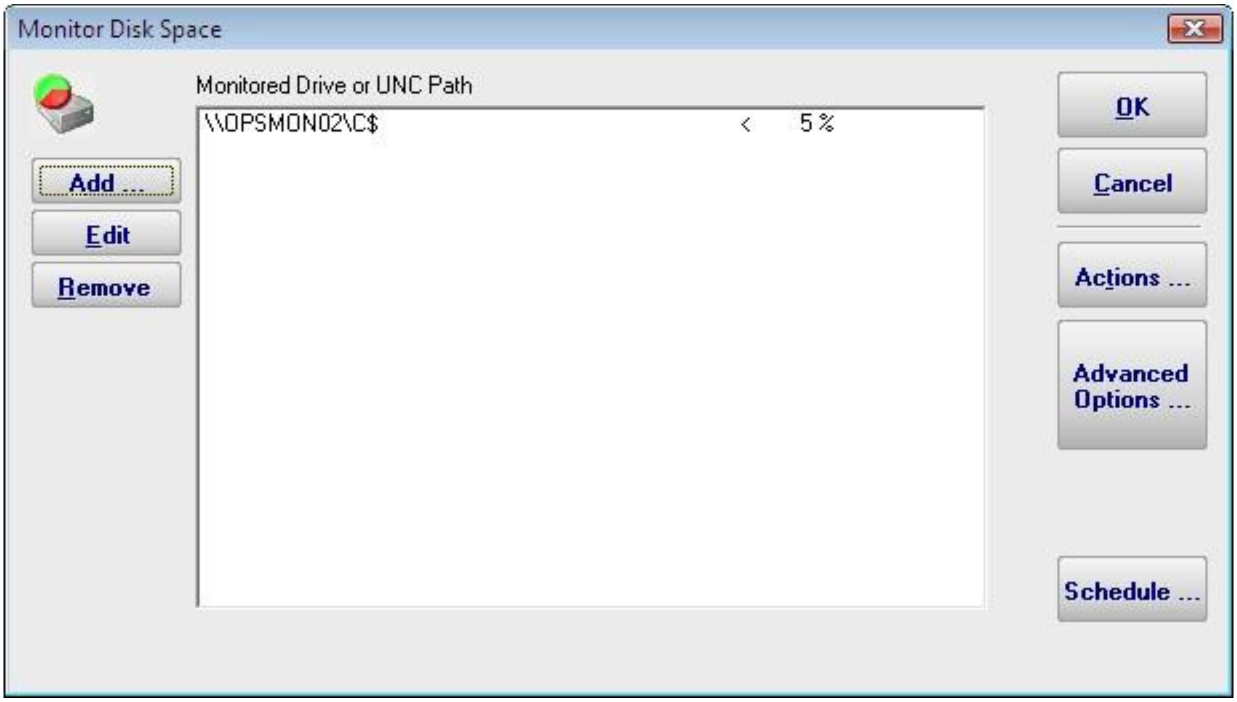
The monitor supports reports that detail which directories are over their quota, as well as the largest directories.

Contents

Disk Space Monitor

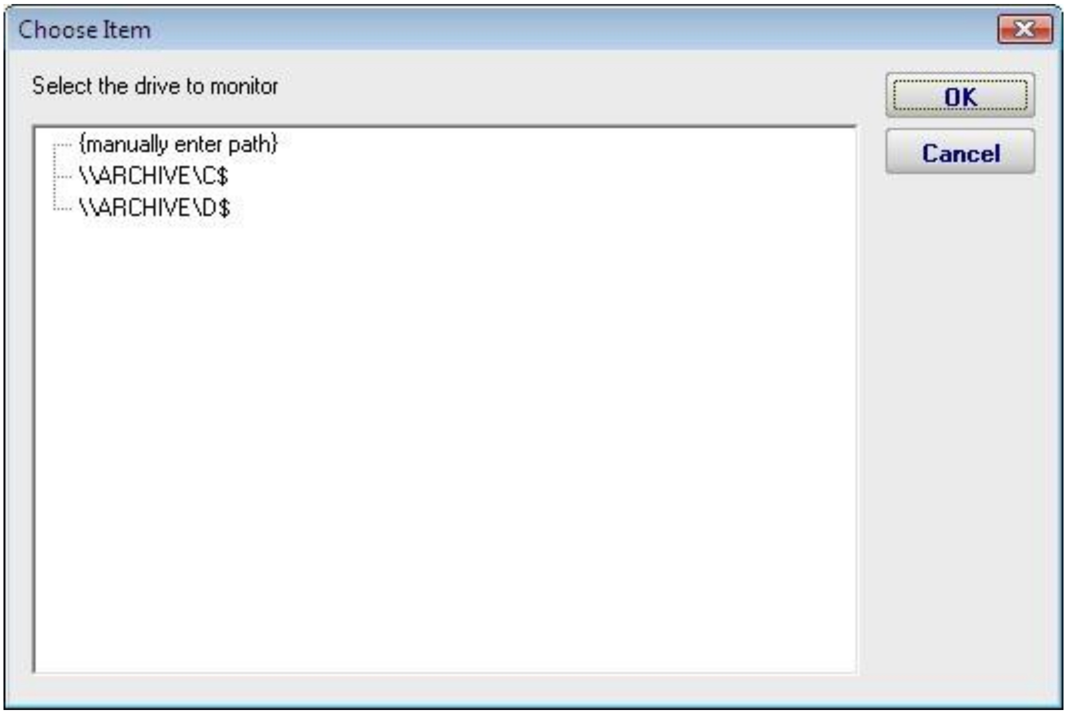
The Disk Space monitor is simple to setup. You just add the drives that you want to monitor and the alert threshold (as an absolute size or as a percentage of the total disk size). You can also monitor specific folders if they are a volume mounted from another server / device.

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



\\OPSMON02\C$ < 5 %

Drives (volumes) on non-Windows machines are shown in the Add dialog as well. PA Server 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.



Select the drive to monitor

- {manually enter path}
- \\ARCHIVE\C$
- \\ARCHIVE\D$

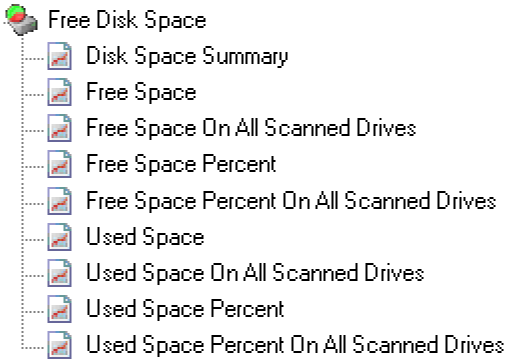
If a drive\share\volume that you want to monitor does not show up, choose {manually enter path}, and then enter the UNC path to be monitored on the next dialog.

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



- Free Disk Space
  - Disk Space Summary
  - Free Space
  - Free Space On All Scanned Drives
  - Free Space Percent
  - Free Space Percent On All Scanned Drives
  - Used Space
  - Used Space On All Scanned Drives
  - Used Space Percent
  - Used Space Percent On All Scanned Drives

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.

Contents

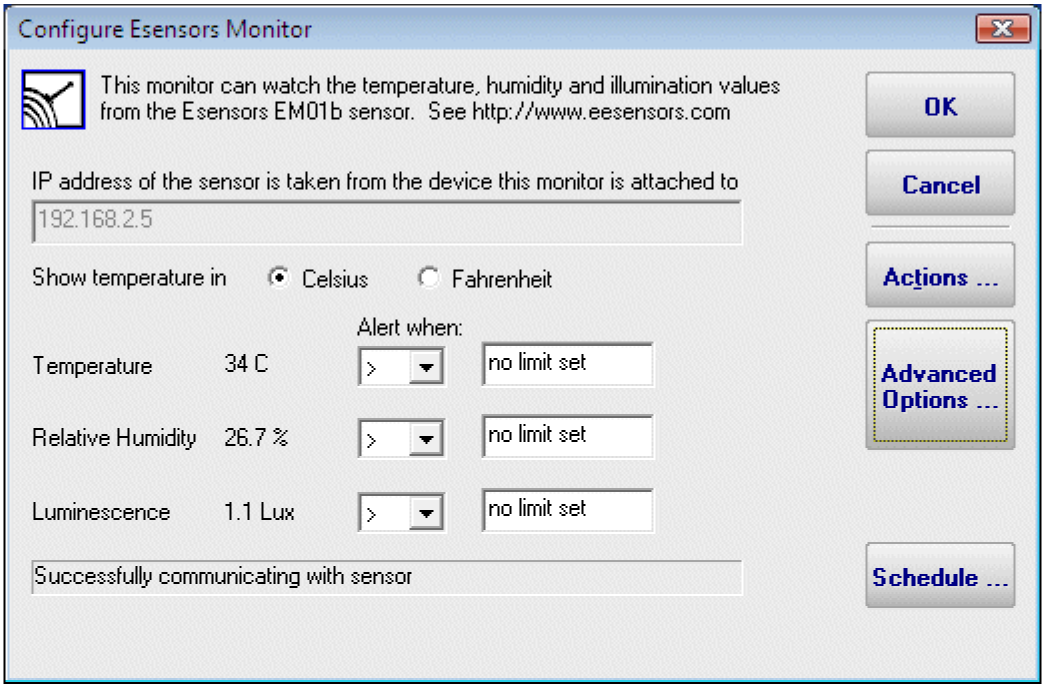
Esensor Environment Monitor

This monitor will perform checking of a model EM01B environmental sensor manufactured by Esensors, Inc. (http://www.eesensors.com). This monitor will work with the EM01B-STN, EM01B-VLT and EM01B-THM.

Please note that you must use the web configuration screen that is built into the EM01B in order to configure it for use on your network. PA Server Monitor does not support a way to configure the EM01B itself.

In order to monitor the EM01B sensor, you must first create a computer object in PA Server Monitor and assign it the IP address being used by the EM01B sensor. This will represent the EM01B for monitoring by PA Server Monitor. Refer to the page on Adding Computers.

Next, you can add a monitor of type "Esensor EM01B Monitor" You will then see the dialog below.



Configure Esensors Monitor

This monitor can watch the temperature, humidity and illumination values from the Esensors EM01b sensor. See http://www.eesensors.com

IP address of the sensor is taken from the device this monitor is attached to

192.168.2.5

Show temperature in ● Celsius ○ Fahrenheit

		Alert when:	
Temperature	34 C	>	no limit set
Relative Humidity	26.7 %	>	no limit set
Luminescence	1.1 Lux	>	no limit set

Successfully communicating with sensor

The status line at the bottom of the dialog (which above, reads "Initializing") will indicate if there is a problem detecting the sensor.

The sensor may be monitored for any or all of following three values that it detects:

- Temperature (in celsius or fahrenheit)
- Relative Humidity (in percent)
- Luminescence (in Lux)

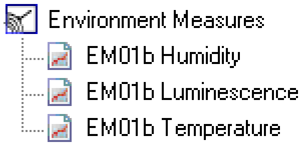
NOTE: The EM01B-VLT and EM01B-THM models support an additional measurement, but the Esensor Environment Monitor is not currently able to read that additional measurement.

If any of the value(s) that you set in the dialog above are reached and crossed by the values sent back by the EM01B, this monitor will reach an error state and fire actions. The error state may be reached by an "under" value or an "over" value, according to the "Alert when" setting for that sensor value.

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

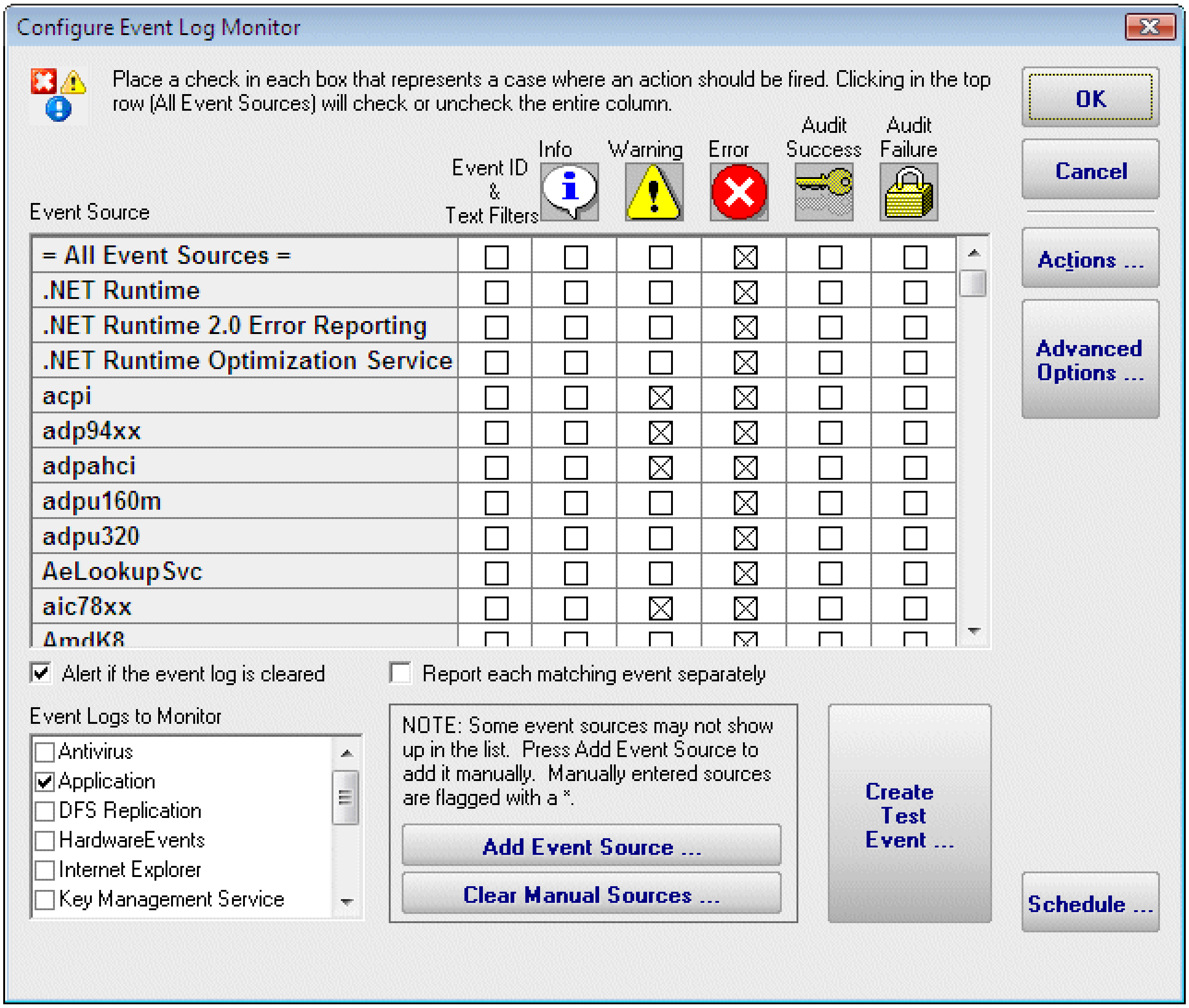


Environment Measures
- EM01b Humidity
- EM01b Luminescence
- EM01b Temperature

The monitored values of temperature, relative humidity and luminescence can all be charted or output to .CSV file or tabular HTML. The data can be summarized into hourly, daily, weekly or monthly minimum, maximum or average values.

Event Log Monitor

The Event Log Monitor can monitor one or more event logs on the system, including the standard Application, Security and System logs as well as custom event logs. You have complete flexibility in specifying which types of events are important to you and which types you'd like to ignore. In addition, you can manually add dynamic event sources (event sources that register themselves, add an event, and then unregister themselves).



Place a check in each box that represents a case where an action should be fired. Clicking in the top row (All Event Sources) will check or uncheck the entire column.

Event Source	Event ID & Text Filters	Info	Warning	Error	Audit Success	Audit Failure
= All Event Sources =	□	□	□	☒	□	□
.NET Runtime	□	□	□	☒	□	□
.NET Runtime 2.0 Error Reporting	□	□	□	☒	□	□
.NET Runtime Optimization Service	□	□	□	☒	□	□
acpi	□	□	☒	☒	□	□
adp94xx	□	□	☒	☒	□	□
adpahci	□	□	☒	☒	□	□
adpu160m	□	□	□	☒	□	□
adpu320	□	□	□	☒	□	□
AeLookupSvc	□	□	□	☒	□	□
aic78xx	□	□	☒	☒	□	□
AmdK8	□	□	□	☒	□	□

☑ Alert if the event log is cleared

□ Report each matching event separately

Event Logs to Monitor

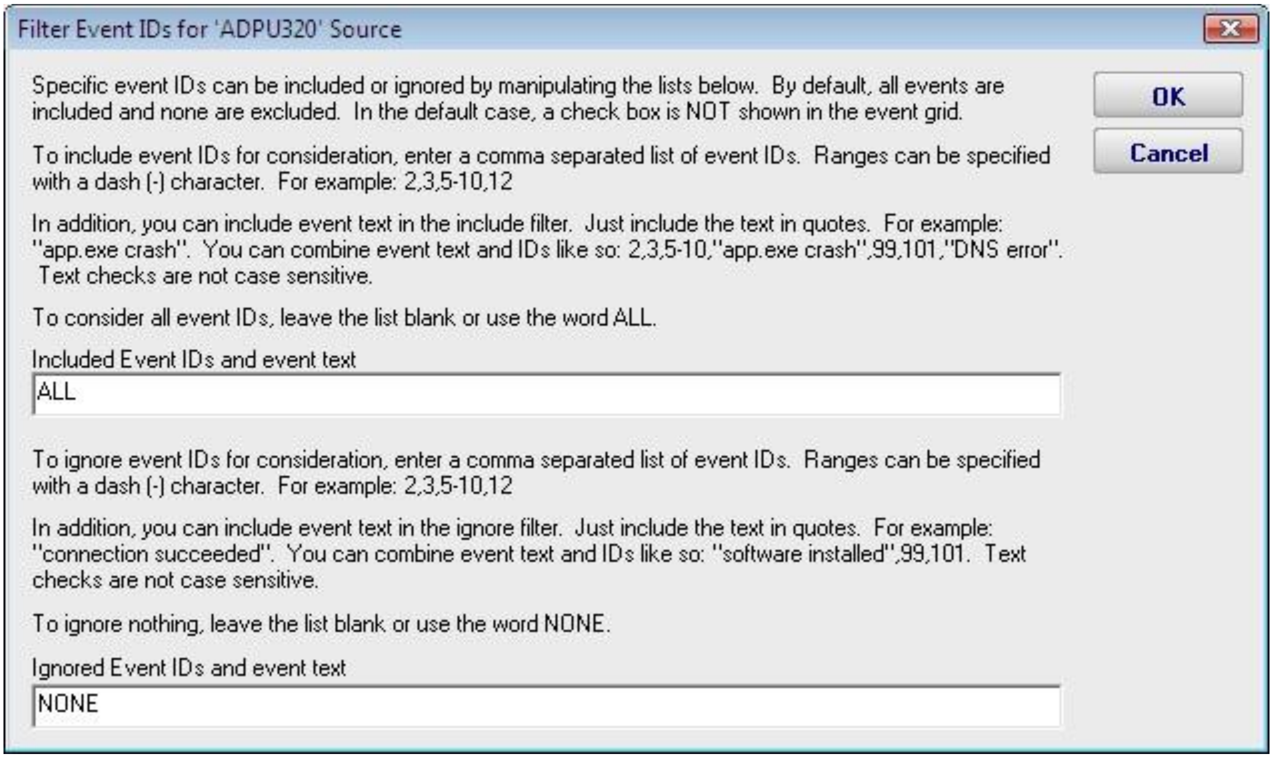
- □ Antivirus
- ☑ Application
- □ DFS Replication
- □ HardwareEvents
- □ Internet Explorer
- □ Key Management Service

NOTE: Some event sources may not show up in the list. Press Add Event Source to add it manually. Manually entered sources are flagged with a *.

The large Event Source grid shows all currently registered Event Log sources. Next to each source are six columns: a special filter column, and the five different event types. Place a check next to the event source of the event type that you want to watch for.

The special "=All Event Sources=" at the top of the list can be used to easily check events from all sources in a column.

Additional Filtering



Filter Event IDs for 'ADPU320' Source

Specific event IDs can be included or ignored by manipulating the lists below. By default, all events are included and none are excluded. In the default case, a check box is NOT shown in the event grid.

To include event IDs for consideration, enter a comma separated list of event IDs. Ranges can be specified with a dash (-) character. For example: 2,3,5-10,12

In addition, you can include event text in the include filter. Just include the text in quotes. For example: "app.exe crash". You can combine event text and IDs like so: 2,3,5-10,"app.exe crash",99,101,"DNS error". Text checks are not case sensitive.

To consider all event IDs, leave the list blank or use the word ALL.

Included Event IDs and event text

ALL

To ignore event IDs for consideration, enter a comma separated list of event IDs. Ranges can be specified with a dash (-) character. For example: 2,3,5-10,12

In addition, you can include event text in the ignore filter. Just include the text in quotes. For example: "connection succeeded". You can combine event text and IDs like so: "software installed",99,101. Text checks are not case sensitive.

To ignore nothing, leave the list blank or use the word NONE.

Ignored Event IDs and event text

NONE

If you want to filter the events by ID or by text (to either include or exclude events), check the box in the "Event ID & Text Filters" column. The dialog shown above will be displayed allowing you to enter event IDs or event text that should be filtered on.

Note: Even if you have an Event ID or text filter defined, you still need to have a check in at least one of the Event Type columns to control which types of events will have the filter applied.

Adding Event Sources

Some sources register themselves with the system just long enough to add an event, and then unregister themselves, which causes them to not show up in the Event Sources list. If you want to monitor such an event source, you can press Add Event Source and manually add the name of the event source. Events that are manually entered will be shown at the top of the list and have a * added to their name. You will then be able to select which event types you'd like to monitor against that source.

If you've entered manual sources but find that you no longer need them, you can press the Clear Manual Sources button to delete your manually entered sources.

Testing the Monitor

The Test Event button allows you to create an event in the event log (possibly mimicking one you're trying to target) to see if the current configuration will pick it up. After you create the event, wait a few moments for the running system to find the new event.

Note: Test events can only be created in the Application event log, and cannot be created with the Security source (only the operating system can create events with that source).

The Training option

in Advanced Monitor Options is particularly useful for this monitor type. You can tell the monitor to watch a computer for a few days and automatically ignore the events that occur within that time frame (this assumes the server is healthy and behaving normally during the monitoring period). You can always go back and remove any filters that are created.

Customized Alerting

Most monitors run periodically and report everything they find in a single alert/message at the end of the run. This monitor has the additional option of sending each matching event as a separate email alert (if an email action is attached to the monitor). This is done by checking "Report each matching event separately".

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 Event Log monitor supports running reports on all of the matching events that have happened. You can filter the reported events on event source, type, date range, etc.

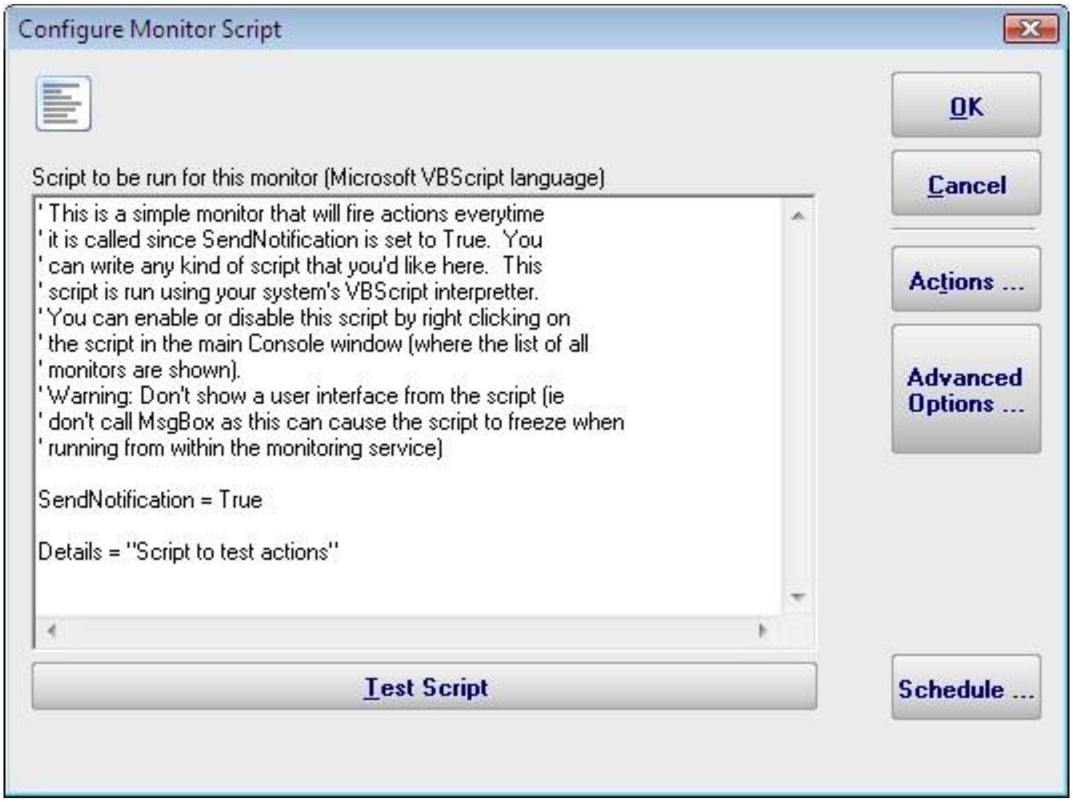
Execute Script Monitor

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: *SendNotication* 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.



Script to be run for this monitor (Microsoft VBScript language)

```
' This is a simple monitor that will fire actions everytime
' it is called since SendNotification is set to True.  You
' can write any kind of script that you'd like here.  This
' script is run using your system's VBScript interpretter.
' You can enable or disable this script by right clicking on
' the script in the main Console window (where the list of all
' monitors are shown).
' Warning: Don't show a user interface from the script (ie
' don't call MsgBox as this can cause the script to freeze when
' running from within the monitoring service)

SendNotification = True

Details = "Script to test actions"
```

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:

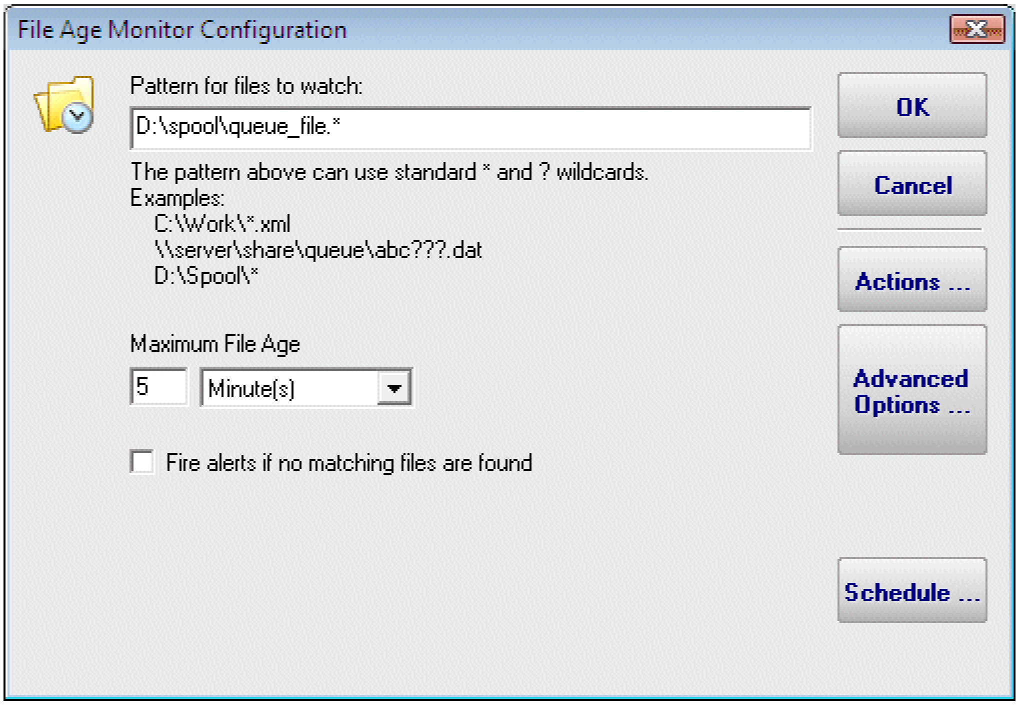
```
FileToCheck = "C:\Files\Backup\dump.db"

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

Contents

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.



File Age Monitor Configuration

Pattern for files to watch: D:\spool\queue_file.*

The pattern above can use standard * and ? wildcards.
Examples:
C:\Work\*.xml
\\server\share\queue\abc???.dat
D:\Spool\*

Maximum File Age: 5 Minute(s)

□ Fire alerts if no matching files are found

Standard Configuration Options

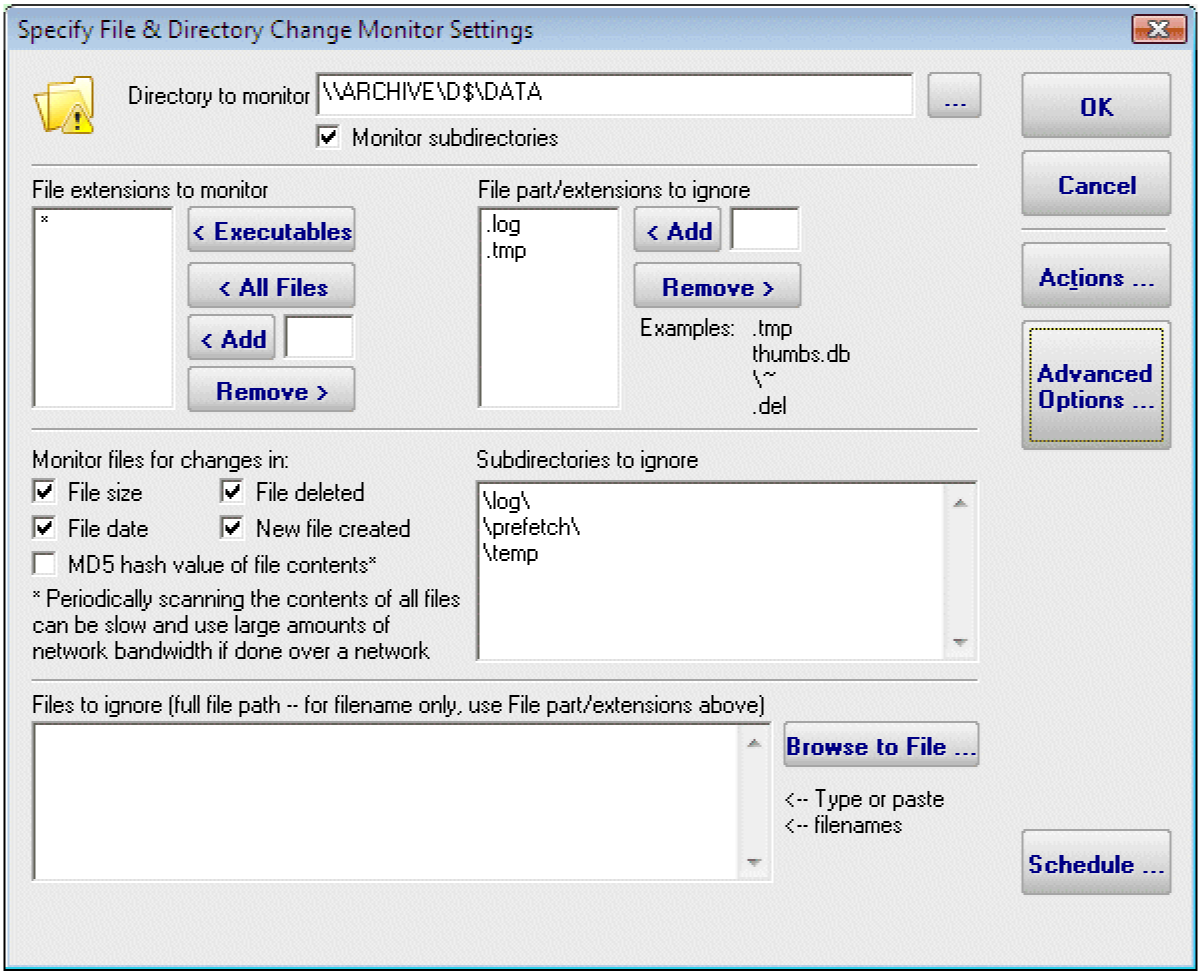
Like all monitors, this monitor has standard buttons on the right for Adding Actions, setting Advanced Options and setting the Monitor Schedule.

Contents

File & Directory Change Monitor

The File & Directory Change Monitor is a very powerful monitor that can for 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.



Directory to monitor: \\ARCHIVE\D$\DATA

☑ Monitor subdirectories

File extensions to monitor:
*

File part/extensions to ignore:
.log
.tmp

Examples: .tmp
thumbs.db
\~
.del

Monitor files for changes in:

☑ File size ☑ File deleted
☑ File date ☑ New file created
☐ MD5 hash value of file contents*

* Periodically scanning the contents of all files can be slow and use large amounts of network bandwidth if done over a network

Subdirectories to ignore:
\log\
\prefetch\
\temp

Files to ignore (full file path -- for filename only, use File part/extensions above)

<-- Type or paste
<-- filenames

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 Server 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.

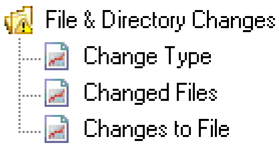
After the training period ends, the monitor automatically switches into its normal scanning pattern.

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.

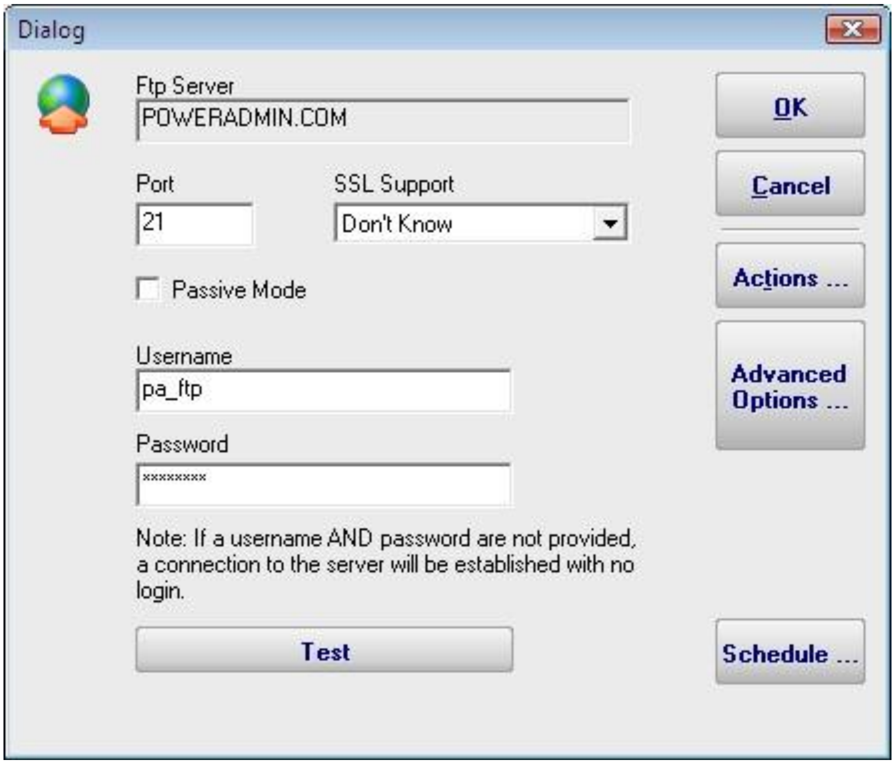
Supported Reports



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.

FTP Server Monitor

The FTP Server monitor can watch an FTP server on a monitored computer to ensure it is up and running. This is accomplished by connecting to the server, optionally using credentials that you supply.



Ftp Server: POWERADMIN.COM

Port: 21

SSL Support: Don't Know

☐ Passive Mode

Username: pa_ftp

Password: ********

Note: If a username AND password are not provided, a connection to the server will be established with no login.

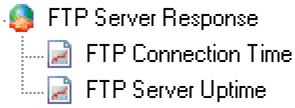
Above you can see the configuration dialog that for configuring the Mail Server monitor. The mail server name is taken from the server that the monitor is attached to. The mail server type and optional username and password need to be entered. When the server type is selected, the standard port is entered for you, but you can also change it for non-standard configurations.

SSL connections (POPS, IMAPS and SMTPS) are supported. If you don't know which setting to use, select "Don't Know" and press the Test button. Each option will be tried and the one that works will be selected for you automatically.

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

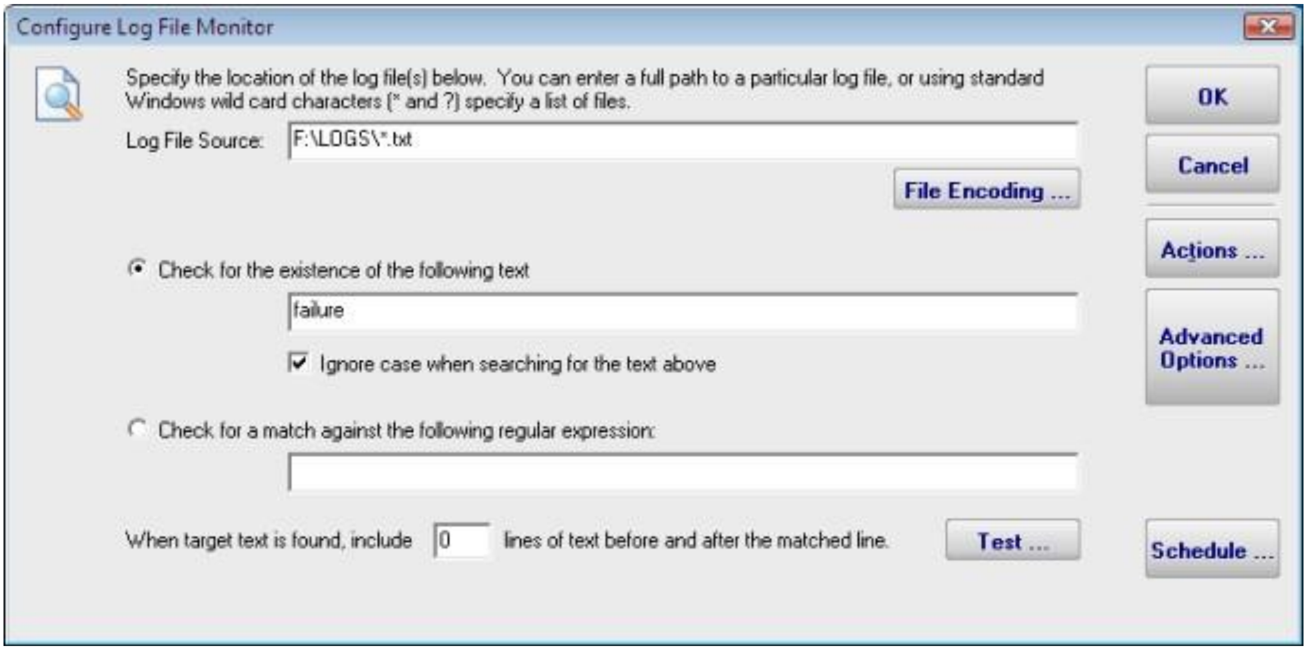


The FTP Server can create reports based on the time to connect to the FTP server. This data can be charted as well as output in .CSV or HTML tabular form. In addition, you can define what 'up' means and create an uptime report showing a percentage of uptime over a given time period.

Log File Monitor

The Log File Monitor watches text files and notifies you when specific text is seen. You can use standard Windows wildcard characters ? and * to specify more than one file to monitor.

The Log File Monitor employs an efficient mechanism to only read changed parts of the file(s). That means it starts reading only text that is added after the first run of the monitor. The search text can be specified as a simple phrase, or you can use the power of regular expressions for more complex text searches.



Configure Log File Monitor

Specify the location of the log file(s) below. You can enter a full path to a particular log file, or using standard Windows wild card characters (* and ?) specify a list of files.

Log File Source: F:\LOGS\*.txt

● Check for the existence of the following text

failure

☑ Ignore case when searching for the text above

○ Check for a match against the following regular expression:

When target text is found, include 0 lines of text before and after the matched line.

The first option is a simple text search. You enter exactly the text that you want found, and specify whether the case should match or not. This is good for searching for specific phrases or specific words or parts of words. An example would be: **database connection error**

The second option lets you specify the search text with Regular Expressions (a great refresher is available at RegExLib.com). For example, if you want to search for the word 'error' OR 'failure' you would enter: **error | failure**

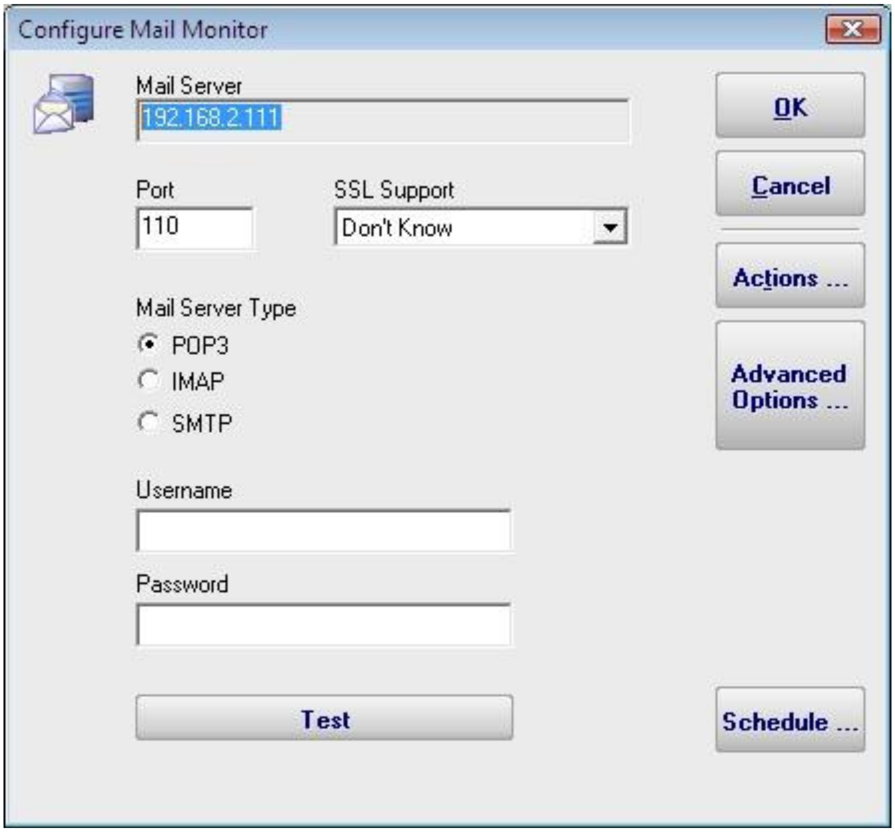
Standard Configuration Options

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

Contents

Mail Server Monitor

The Mail Server monitor can watch a POP3, IMAP4 or SMTP mail server on a monitored computer to ensure it is up and running. This is accomplished by logging into the server using one of the above protocols using credentials that you supply.


Configure Mail Monitor

Mail Server: 192.168.2.111

Port: 110

SSL Support: Don't Know

Mail Server Type

● POP3

○ IMAP

○ SMTP

Username:

Password:

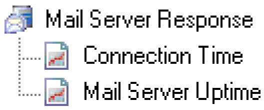
Above you can see the configuration dialog that for configuring the Mail Server monitor. The mail server name is taken from the server that the monitor is attached to. The mail server type and optional username and password need to be entered. When the server type is selected, the standard port is entered for you, but you can also change it for non-standard configurations.

SSL connections (POPS, IMAPS and SMTPS) are supported. If you don't know which setting to use, select "Don't Know" and press the Test button. Each option will be tried and the one that works will be selected for you automatically.

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 Mail Server monitor can create reports based on the time to connect to the mail server. This data can be charted as well as output in .CSV or HTML tabular form. In addition, you can define what 'up' means and create an uptime report showing a percentage of uptime over a given time period.

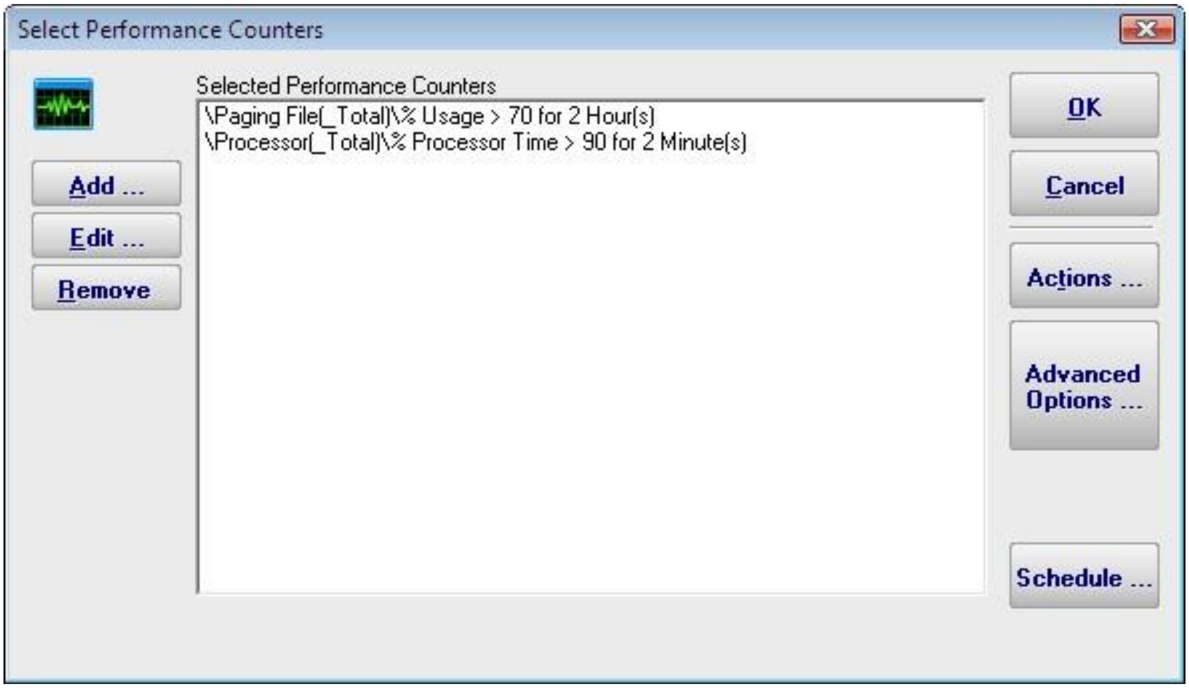
Performance Counter Monitor

The Performance Counter Monitor can watch any performance counter that the Windows Perfmon tool can display. This gives you great flexibility since many systems and drivers on the computer report statistics and their current state via the performance counters.

In addition, CPU and memory usage counters are simulate for Linux/Unix machines via SNMP, so monitoring and charting those values is now as easy as with a Windows server.

When adding counters to be monitored, you can select a counter, a threshold (low or high) and the amount of time the threshold has to be exceeded before actions are fired. The offending counter and its current value will be part of the action description.

The values of each performance counter are recorded in a local database in order to generate historical reports.


Select Performance Counters

Selected Performance Counters

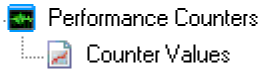
\Paging File(_Total)\% Usage > 70 for 2 Hour(s)
\Processor(_Total)\% Processor Time > 90 for 2 Minute(s)

When you click the Add button, the target server is queried for counters it supports, and a dialog similar to the Windows Perfmon dialog is shown where you can select the counter that you want to monitor. For this to work with Linux/Unix servers, SNMP is used. Make sure you have entered the SNMP credentials if the defaults of v2c and 'public' won't work.

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 Performance monitor can create charts from any of the counter values that are being monitored. This includes bar and line charts. Tabular HTML and .CSV output for importing into other apps (Excel) are also possible.

Simulated Network Counters

Windows doesn't have a performance counter for **% Network Utilization**, so PA Server Monitor has support for computed counters for Send and Receive Utilization percents. To get them, you need to add the two base counters that each is based on. The computed values are percentages from 0 to 100.

For each of the counters below, you can set the alert thresholds to anything you want. Current Bandwidth is supposed to be a constant value, so monitoring it for alerting purposes isn't important. In that case an alert threshold of = 0 would be a good default. For Bytes Sent and Received/sec you also might not care about alerting on it. Since it could realistically be 0 some times, you could set the alert threshold to < 0 so it never alerts.

To get **\Network Interface\(<network card>)\% Receive Utilization** [Ex: alert on > 95]

- Add: **\Network Interface\(<network card>)\Bytes Received/sec** [Ex: alert on < 0]
- Add: **\Network Interface\(<network card>)\Current Bandwidth** [Ex: alert on = 0]

To get **\Network Interface\(<network card>)\% Send Utilization** [Ex: alert on > 95]

- Add: **\Network Interface\(<network card>)\Bytes Sent/sec** [Ex: alert on < 0]
- Add: **\Network Interface\(<network card>)\Current Bandwidth** [Ex: alert on = 0]

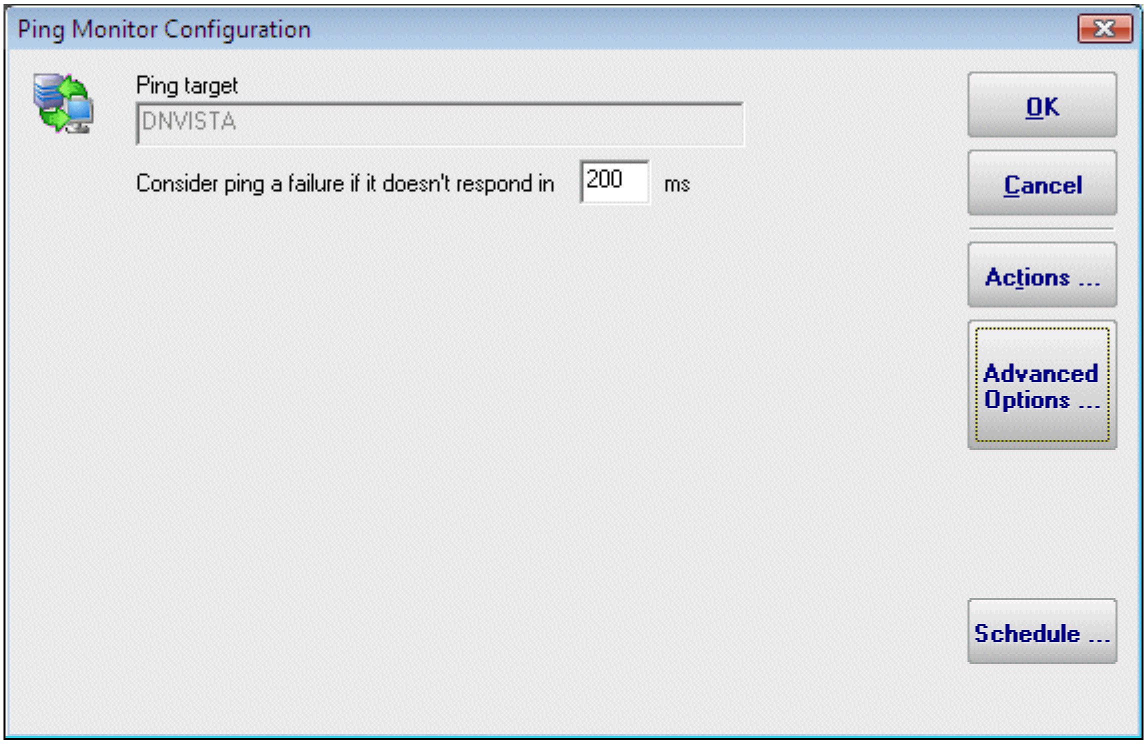
Ping Monitor

The Ping Monitor sends out a typical ICMP 'ping' message to the specified host as often as is specified by the Schedule button. If the host doesn't respond before the given timeout value, the configured actions are fired.

The host name is resolved each time the ping happens which allows this monitor to also watch DNS servers. The time to resolve an address is not counted towards the total ping timeout.

Many system administrators only want to be alerted after a few ping responses are missed. Configure that under the Alert Suppression setting in Advanced Options.

Ping result times are recorded for report generation. If a ping response is never returned, a time of 30,000 is used to indicate the failure in reports. The Uptime Report is very useful with Ping data.



Ping Monitor Configuration

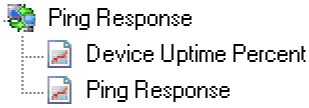
Ping target: DNVISTA

Consider ping a failure if it doesn't respond in 200 ms

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



- Ping Response
  - Device Uptime Percent
  - Ping Response

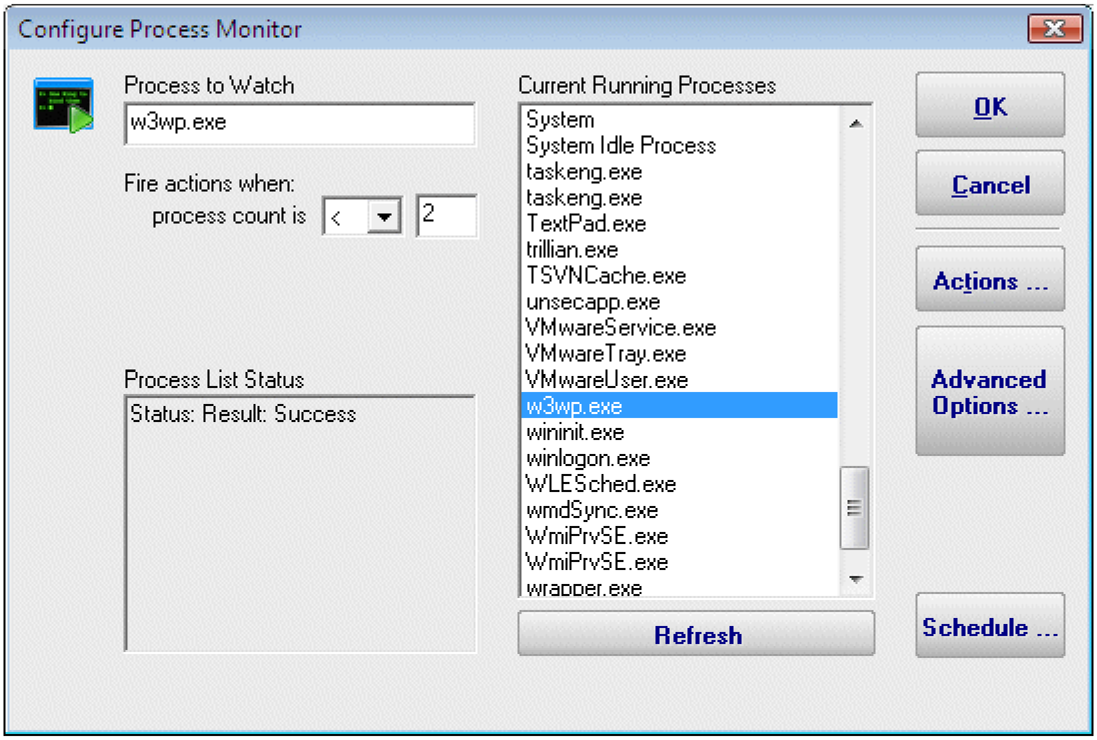
The Ping Server monitor can create reports based on the ping response from the target server/device. This data can be charted as well as output in .CSV or HTML tabular form. In addition, you can define what 'up' means and create an uptime report showing a percentage of uptime over a given time period.

Process Monitor

The Process monitor check how many instances of a target process are running. It then compares that to the threshold and fires actions as needed.

The process may be running locally, or remotely. PA Server Monitor can monitor remote processes on Windows servers via WMI or SNMP, as well as processes on remote Linux/Unix servers via SNMP.

To monitor a process, create a monitor of type Process Monitor on the computer that hosts the target process. You will see the dialog shown below.



Configure Process Monitor

Process to Watch: w3wp.exe

Fire actions when: process count is < 2

Current Running Processes:

System
System Idle Process
taskeng.exe
taskeng.exe
TextPad.exe
trillian.exe
TSVNCache.exe
unsecapp.exe
VMwareService.exe
VMwareTray.exe
VMwareUser.exe
w3wp.exe
wininit.exe
winlogon.exe
WLESched.exe
wmdSync.exe
WmiPrvSE.exe
WmiPrvSE.exe
wrapper.exe

Process List Status: Status: Result: Success

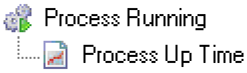
The list "Current Running Processes" should quickly fill with a list of processes that are now running on the target machine. Select the process from the list and specify the alert condition. If the process list doesn't fill, check the WMI and/or SNMP credentials for the server.

If the process name does not appear in the list, then you can type its name manually into the "Process to Watch" text box.

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



Process Running
Process Up Time

Process up or down data is recorded every time the monitor runs. You can define a time period, and optionally a summarization (hourly, daily, weekly, monthly) to create an uptime report for the process.

Contents

Server Temperature Monitor

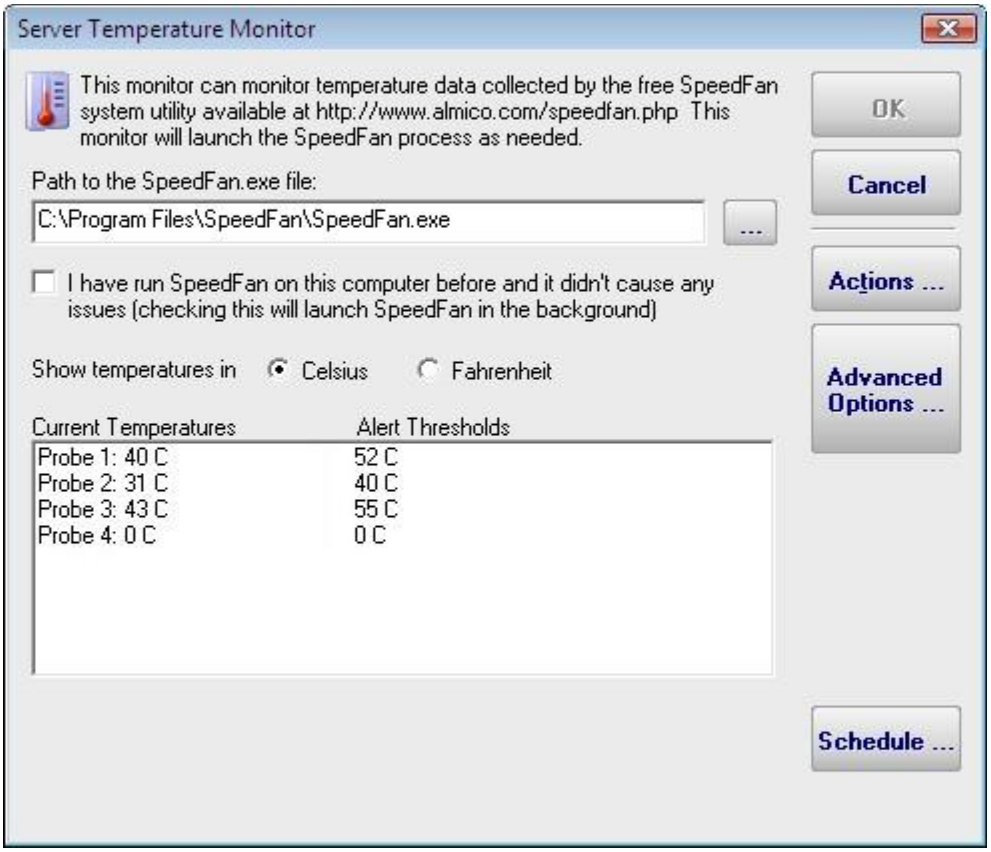
The Server Temperature Monitor works with the free SpeedFan utility program. You need to download it from http://www.almico.com/speedfan.php and install it (it can be downloaded and installed in under a minute).

NOTE: Because SpeedFan interacts with and probes very low-level hardware, the SpeedFan website suggests caution when first running it in case there are any issues. Running it on test hardware is recommended

After SpeedFan is installed, the Server Temperature Monitor will query the SpeedFan app to extract current temperature values from the various temperature probes detected.

NOTE: Because SpeedFan interacts with the local hardware, this monitor only works on the computer where the monitoring program is installed.

To configure the Server Temperature Monitor, simply specify the path to the SpeedFan.exe file (the default path given is typically correct). Then indicate whether you have successfully run SpeedFan before.



Server Temperature Monitor

This monitor can monitor temperature data collected by the free SpeedFan system utility available at http://www.almico.com/speedfan.php This monitor will launch the SpeedFan process as needed.

Path to the SpeedFan.exe file: C:\Program Files\SpeedFan\SpeedFan.exe

□ I have run SpeedFan on this computer before and it didn't cause any issues (checking this will launch SpeedFan in the background)

Show temperatures in ● Celsius ○ Fahrenheit

Current Temperatures	Alert Thresholds
Probe 1: 40 C	52 C
Probe 2: 31 C	40 C
Probe 3: 43 C	55 C
Probe 4: 0 C	0 C

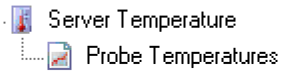
After the path has been specified and you've indicated SpeedFan runs OK on your computer, SpeedFan will be launched in the background. Live temperatures will then be collected and displayed.

Default temperature thresholds are shown to the right of the live temperatures. Simply click a temperature threshold and change it to whatever value you like.

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 various temperature values are all recorded to a database. You can run reports that chart these values or produce tabular output in HTML or .CSV files for importing into Excel, etc. The data can be optionally summarized into hourly, daily, weekly and monthly values.

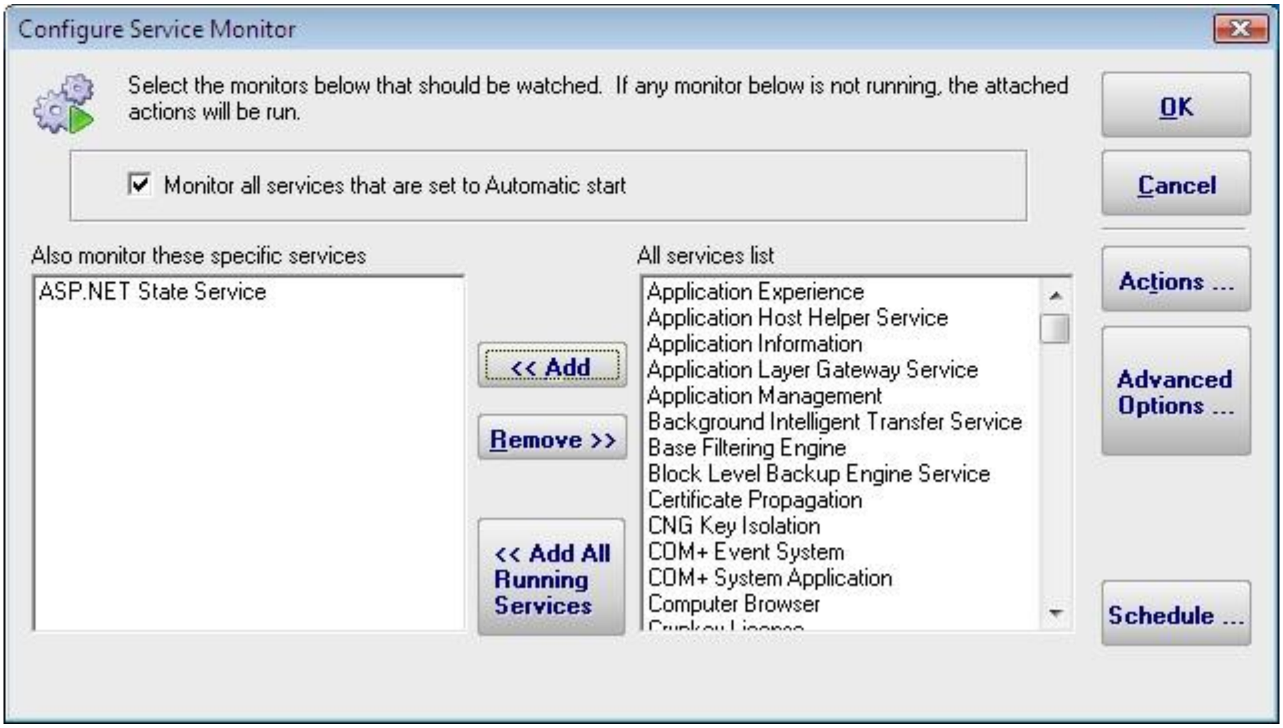
Service Monitor

The Service Monitor watches the same system services that can be seen from the Administrator Tools Services applet. If a service is not running, actions are fired (which could notify you and/or restart the service for example). The Restart Service action is typically attached to this monitor.

The services in the "All services list" come from the computer being monitored.

The easiest way to use this monitor is to check the "Monitor all services that are set to Automatic start". If a service is set to Automatic start isn't running, alerts will fire.

In addition to (or instead of) the above check box, you can also specify a specific list of services to monitor by moving them to the list on the left labeled "Also monitor these specific services". You can press Add All Running Services to automatically add the services which are BOTH currently running AND set to Automatic start type.



Configure Service Monitor

Select the monitors below that should be watched. If any monitor below is not running, the attached actions will be run.

☑ Monitor all services that are set to Automatic start

Also monitor these specific services

ASP.NET State Service

All services list

Application Experience
Application Host Helper Service
Application Information
Application Layer Gateway Service
Application Management
Background Intelligent Transfer Service
Base Filtering Engine
Block Level Backup Engine Service
Certificate Propagation
CNG Key Isolation
COM+ Event System
COM+ System Application
Computer Browser

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.

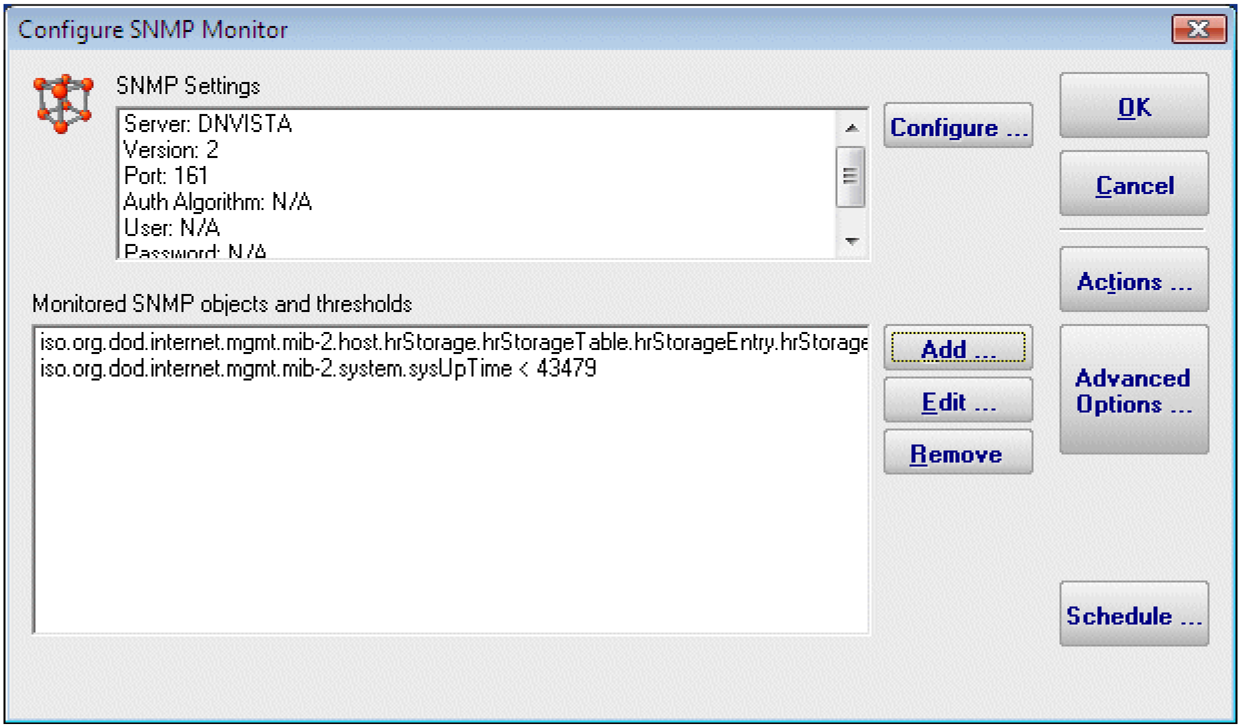
Supported Reports

Service up or down data is recorded every time the monitor runs. You can define a time period, and optionally a summarization (hourly, daily, weekly, monthly) to create an uptime report for the service.

Contents

SNMP Monitor

The SNMP Monitor works as an SNMP Manager--it can query local or remote SNMP agents for specific values, and then compare those values to thresholds. If the thresholds are passed, actions are fired. In addition, the retrieved values are also stored in the database for creating reports.

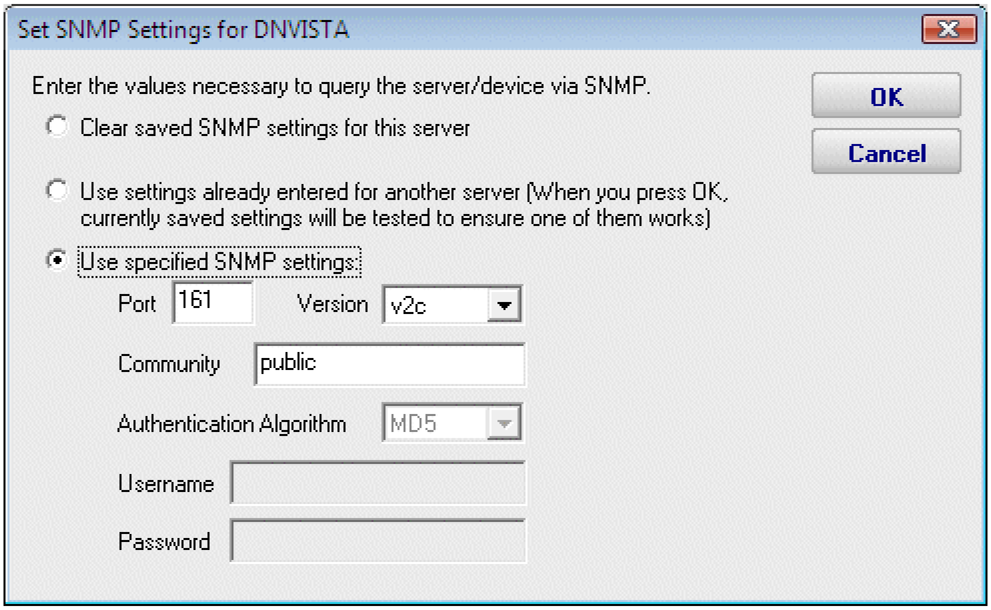


Server: DNVISTA
Version: 2
Port: 161
Auth Algorithm: N/A
User: N/A
Password: N/A

iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorage
iso.org.dod.internet.mgmt.mib-2.system.sysUpTime < 43479

Configuring the SNMP Monitor requires SNMP credentials to be set, and also specific SNMP objects and thresholds to be selected.

The default SNMP credentials are set to use v2c with community string set to 'public'. That will work in many cases, but you might need to make changes depending on your environment. The current settings are shown in the dialog above near the top, and pressing the Configure button will let you change those settings. You can also right-click the computer/device in the Console and choose Type & Credentials -> Set SNMP Settings.



Enter the values necessary to query the server/device via SNMP.

○ Clear saved SNMP settings for this server

○ Use settings already entered for another server (When you press OK, currently saved settings will be tested to ensure one of them works)

● Use specified SNMP settings:

Port 161 Version v2c

Community public

Authentication Algorithm MD5

Username

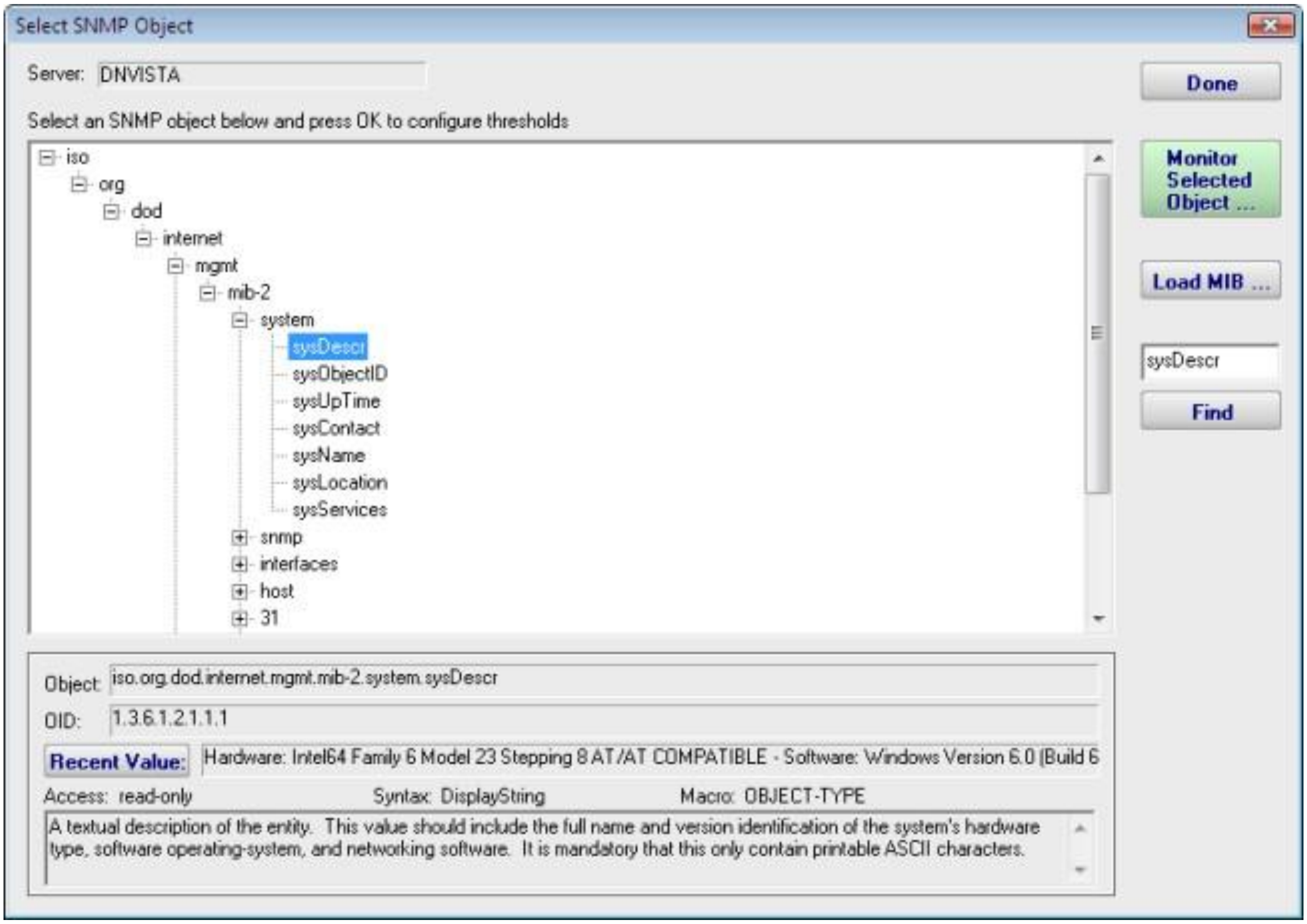
Password

This dialog allows you to set the following items:

- SNMP version of the remote agent - v1, v2c and v3 are supported. The SNMP version value v2c is the default setting.
- If using SNMP version v3, a username/password needs to be entered.
- Community string value which is to 'public' by default.

Once you have entered the information that will allow access to your SNMP agent, press OK in the "Set SNMP Settings" dialog to save the SNMP server settings and to return to the Configure SNMP Monitor dialog.

From the Configure SNMP Monitor dialog, press the Add button. That will display the dialog shown below. The SNMP monitor will query the remote agent and show you a list of all SNMP objects available from the agent. Those objects are also displayed using information from default MIBs that are on your system. If you have additional MIB files for objects that you want to view, press Load MIB button to select the MIB file. The display will update to include information from the newly loaded MIB file.



Server: DNVISTA

Select an SNMP object below and press OK to configure thresholds

Object: iso.org.dod.internet.mgmt.mib-2.system.sysDescr

OID: 1.3.6.1.2.1.1.1

Recent Value: Hardware: Intel64 Family 6 Model 23 Stepping 8 AT/AT COMPATIBLE - Software: Windows Version 6.0 (Build 6

Access: read-only Syntax: DisplayString Macro: OBJECT-TYPE

A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.

Unlike many SNMP browsers that only show objects for which you have MIBs loaded, this SNMP browser shows all objects that are available on the remote machine. Loading MIBs will add additional detail (like symbolic object names instead of just the numeric OID, and also textual descriptions for the fields).

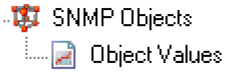
As you move through the SNMP object tree, you'll see that the information at the bottom of the dialog changes. This bottom part of the dialog gives you information about each object according to any applicable MIB that was loaded. In addition, you can press the Recent Value button to see what the value is at that moment. You can navigate to the object that you're interested in, or use the Find button to find an object. The Find button will search for OIDs, object names and object values. You can press the Find button again after a search to keep searching further for the same value.

Once your target object has been found, press the green Monitor Selected Object button. This will show you a small dialog where you can configure the thresholds for the value of that object. Once the threshold is set, you're brought back to the previous dialog so you can continue selecting addtional objects to monitor. When you're finished, press the Done button to return to the main SNMP Monitor configuration dialog.

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



SNMP Objects
Object Values

The SNMP monitor can create charts from any of the counter values that are being monitored. This includes bar and line charts. Tabular HTML and .CSV output for importing into other apps (Excel) are also possible.

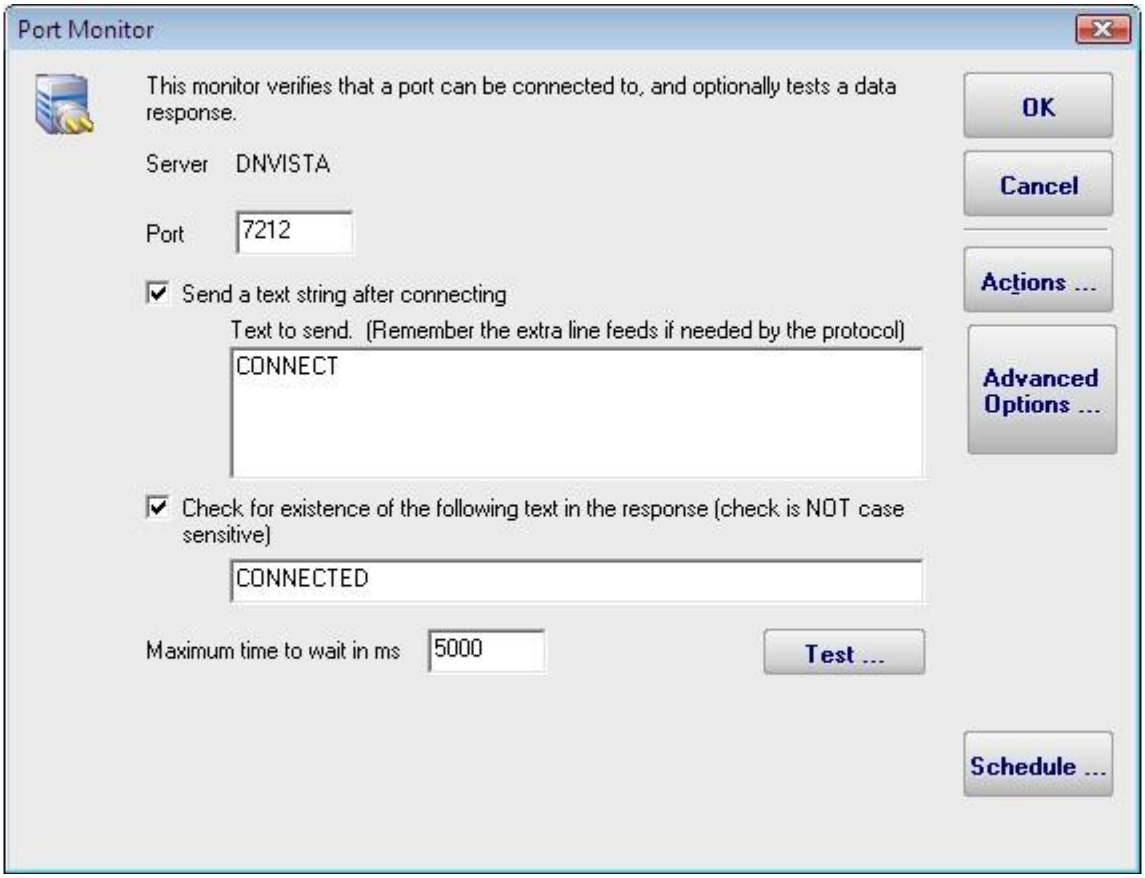
SNMP Troubleshooting

If you can't connect to a server/device via SNMP, make sure to double check the SNMP settings (version and community string in particular). Windows servers by default don't enable 'public' as a community string, and they don't accept SNMP requests from the network by default. These can both be changed by going to the SNMP server (in the Administrator Tools -> Services applet), to the Security tab.

Contents

TCP Port Monitor

The TCP Port Monitor will periodically connect to a port on the defined server and record how long the connection took. In addition, a text command can be sent, and a specific text response can be checked for (if no response is specified, the establishment of a connection is considered successful).



This monitor verifies that a port can be connected to, and optionally tests a data response.

Server DNVISTA

Port 7212

☑ Send a text string after connecting

Text to send. (Remember the extra line feeds if needed by the protocol)

CONNECT

☑ Check for existence of the following text in the response (check is NOT case sensitive)

CONNECTED

Maximum time to wait in ms 5000

Since connection times are recorded, you can create reports that show connection times to help you understand when the system is under load.

For example, you could use this monitor to test whether an HTTP server is accepting connections by specifying the following send text:

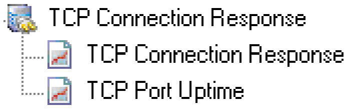
GET / HTTP/1.1<enter>
<enter>
<enter>   (blank lines are important for this protocol!)

and then check for response text of '200'. (This is just an example--in this particular case, it would be easier to just use the Web Page Monitor).

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



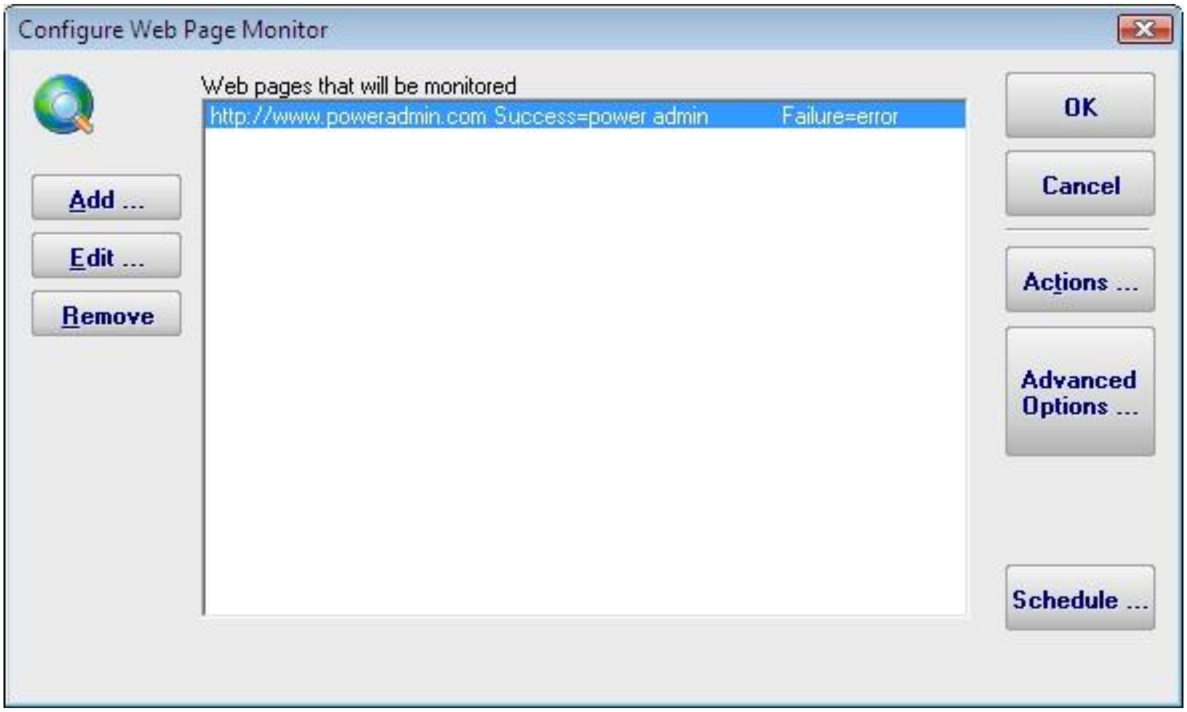
TCP Connection Response

- TCP Connection Response
- TCP Port Uptime

The TCP Port monitor can create reports based on the port response time from the target server/device. This data can be charted as well as output in .CSV or HTML tabular form. In addition, you can define what 'up' means and create an uptime report showing a percentage of uptime over a given time period.

Web Page Monitor

The Web Page Monitor lets you define one or more web pages and content on those pages that should be checked.

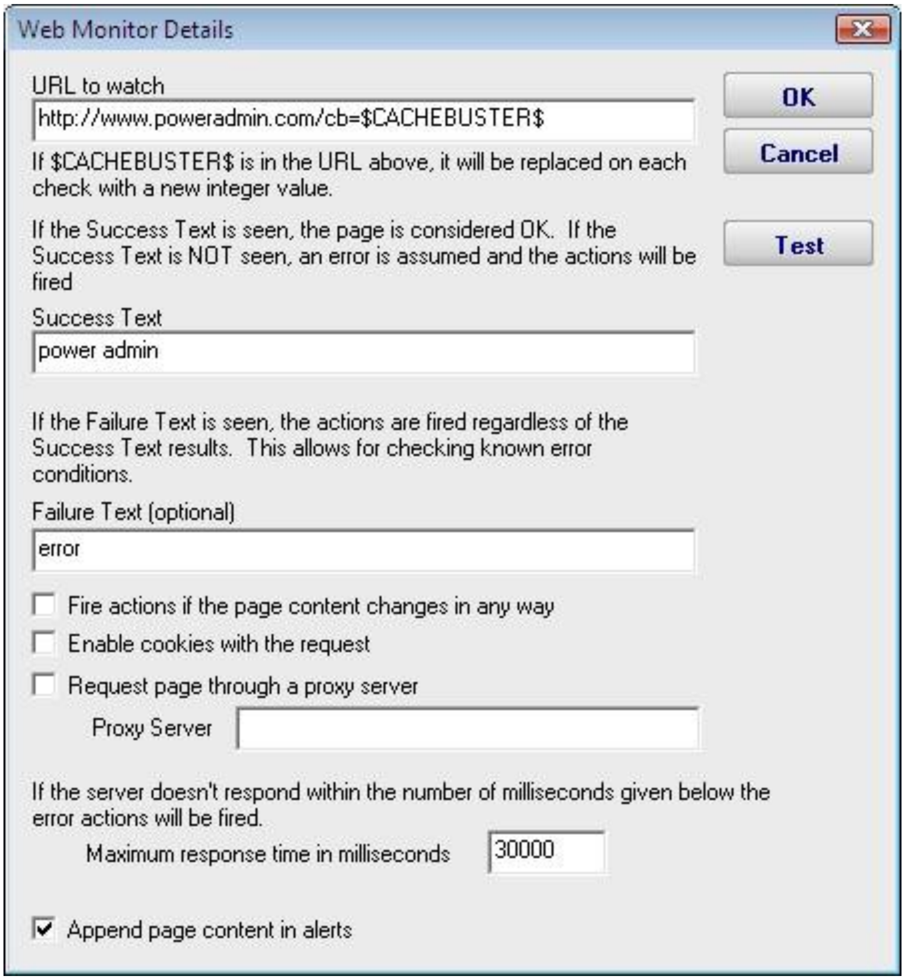


Configure Web Page Monitor

Web pages that will be monitored

http://www.poweradmin.com Success=power admin Failure=error

When you specify a web page to be watched, you give the URL to the page, a specific piece of text that must exist on the page to indicate success, and an optional piece of text on the page that would indicate an error. You can specify whether cookies are passed and whether a proxy-server needs to be used to get to the page. Finally, you can also specify the maximum amount of time that a page can take to respond--if it takes longer the configured actions are fired (just like the other failure cases of not finding the success text on the page or finding the optional error text on the page).



URL to watch

http://www.poweradmin.com/cb=$CACHEBUSTER$

If $CACHEBUSTER$ is in the URL above, it will be replaced on each check with a new integer value.

If the Success Text is seen, the page is considered OK. If the Success Text is NOT seen, an error is assumed and the actions will be fired

Success Text

power admin

If the Failure Text is seen, the actions are fired regardless of the Success Text results. This allows for checking known error conditions.

Failure Text (optional)

error

☐ Fire actions if the page content changes in any way

☐ Enable cookies with the request

☐ Request page through a proxy server

Proxy Server

If the server doesn't respond within the number of milliseconds given below the error actions will be fired.

Maximum response time in milliseconds 30000

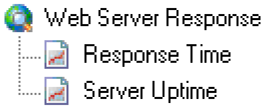
☑ Append page content in alerts

Web page response times are recorded so you can create tabular or graphical reports to show response history.

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

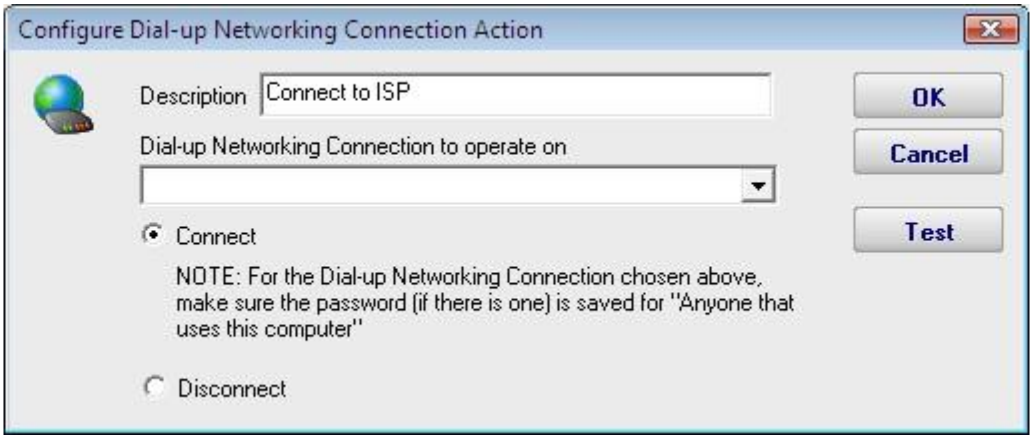


The Web Page monitor can create reports based on the page response time for the target URL. This data can be charted as well as output in .CSV or HTML tabular form. In addition, you can define what 'up' means and create an uptime report showing a percentage of uptime over a given time period.

Contents

Dial-up Connection Action

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



Configure Dial-up Networking Connection Action

Description: Connect to ISP

Dial-up Networking Connection to operate on

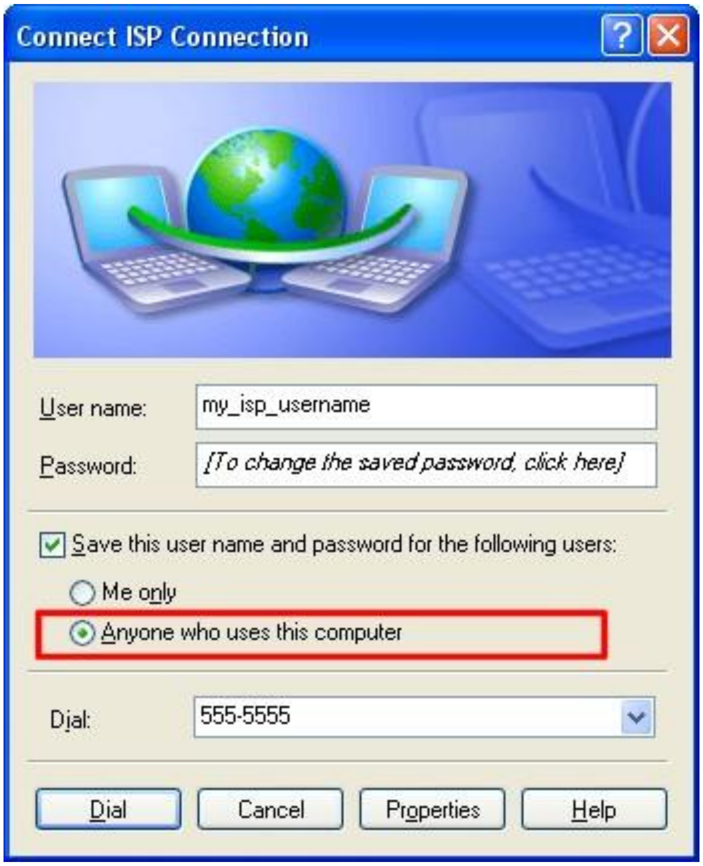
● Connect

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

○ Disconnect

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

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



User name: my_isp_username

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

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

○ Me only

● Anyone who uses this computer

Dial: 555-5555

Contents

E-mail Message Action

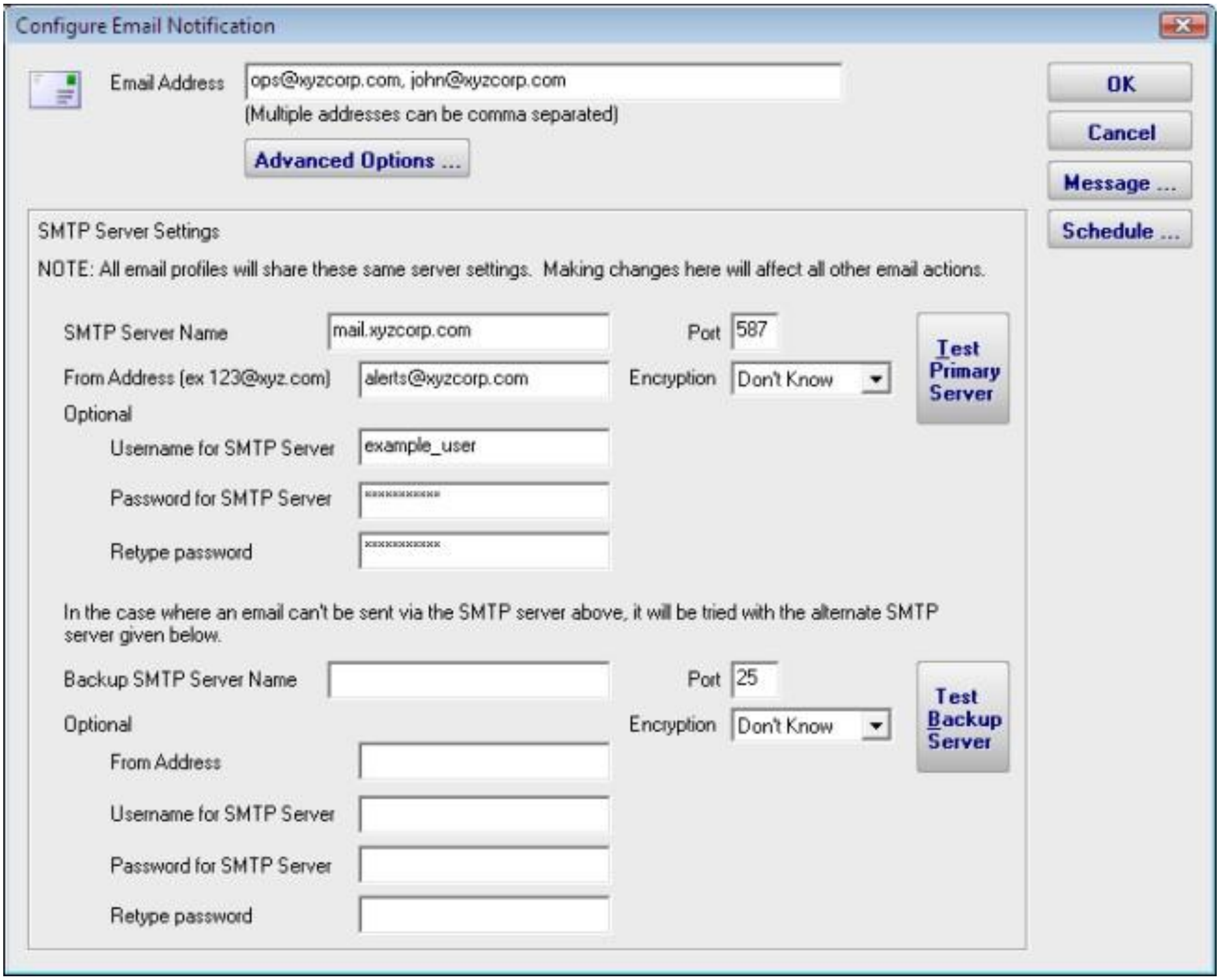
The E-mail Message Action is the standard way for monitors to notify you via SMTP email messages. This allows for typical email messages as well as messages sent to cell phones and pagers if you cell/pager provider has an SMTP gateway (many providers do). We have some hints on that in our SMS FAQ.

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

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

The settings for each SMTP server (primary and secondary) can be validated by by the program. You may do this by pressing the "Test Primary Server" and "Test Backup Server" button, respectively. This test causes PA Server 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.



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

(Multiple addresses can be comma separated)

SMTP Server Settings

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

SMTP Server Name: mail.xyzcorp.com

Port: 587

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

Encryption: Don't Know

Optional

Username for SMTP Server: example_user

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

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

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

Backup SMTP Server Name:

Port: 25

Optional

Encryption: Don't Know

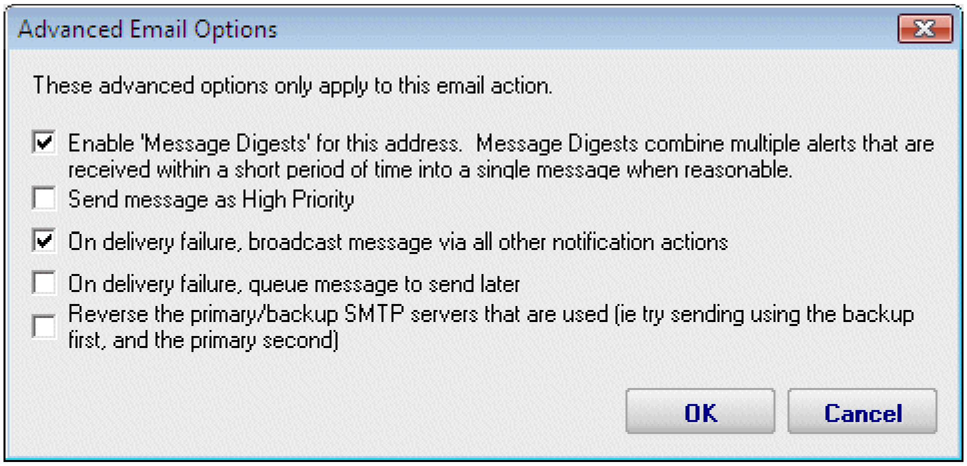
From Address:

Username for SMTP Server:

Password for SMTP Server:

Retype password:

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



These advanced options only apply to this email action.

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

☐ Send message as High Priority

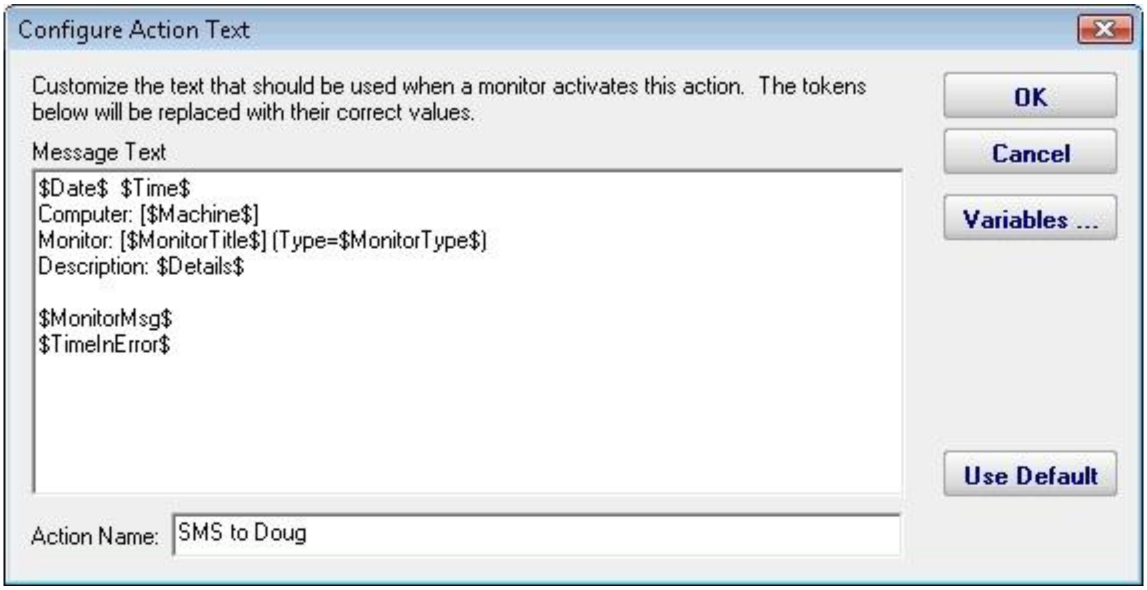
☑ On delivery failure, broadcast message via all other notification actions

☐ On delivery failure, queue message to send later

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

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



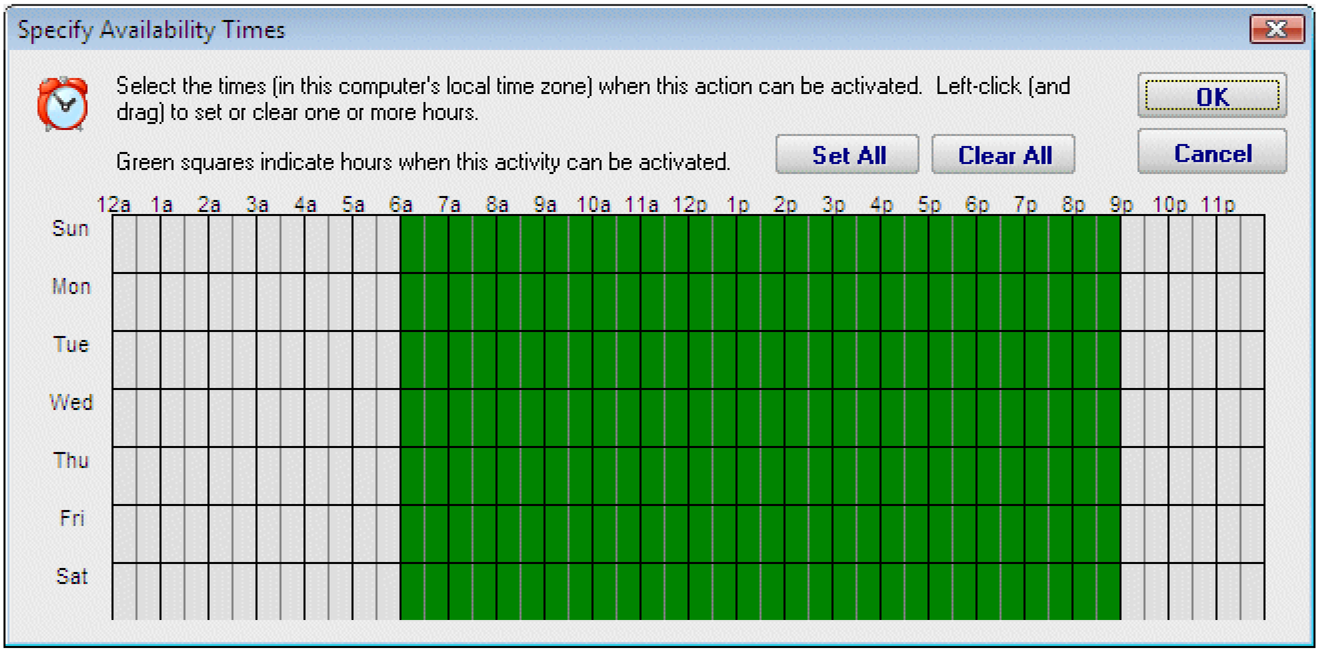
Customize the text that should be used when a monitor activates this action. The tokens below will be replaced with their correct values.

Message Text

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

$MonitorMsg$
$TimeInError$
```

Action Name: SMS to Doug

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



Specify Availability Times

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

Green squares indicate hours when this activity can be activated.

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

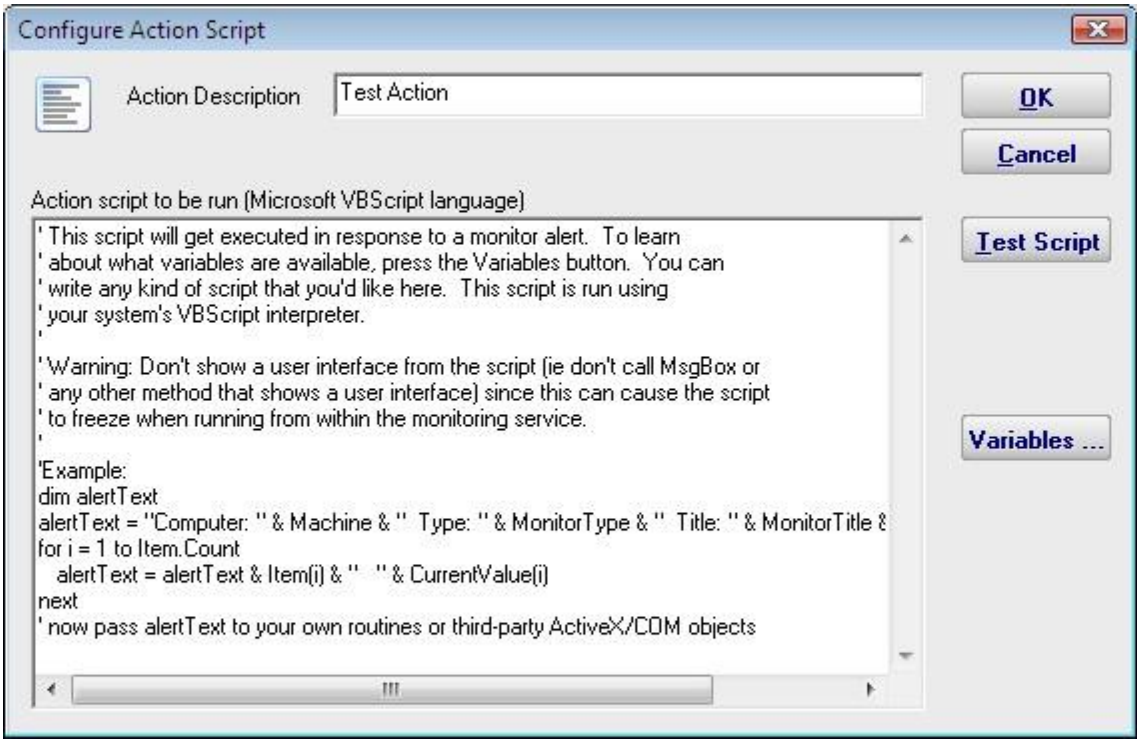
Execute Script Action

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

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

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

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



Action Description: Test Action

Action script to be run (Microsoft VBScript language)

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

An example script that connects to a database is shown below

```
Option Explicit
Dim objconnection
Dim objrecordset
Dim strDetails

Const adOpenStatic = 3
Const adLockOptimistic = 3

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

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

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

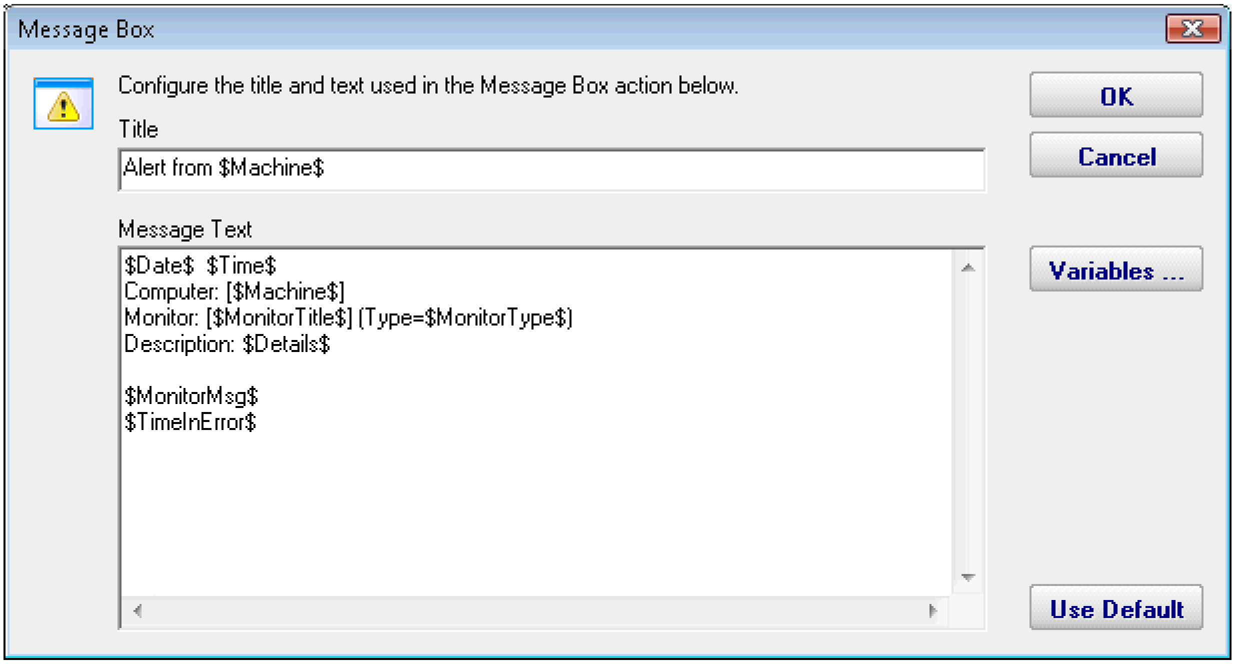
Contents

Message Box Action

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

The dialog shown below is displayed when you add or edit a message box action. PA Server 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.



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

Title

Alert from $Machine$

Message Text

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

$MonitorMsg$
$TimeInError$
```

Contents

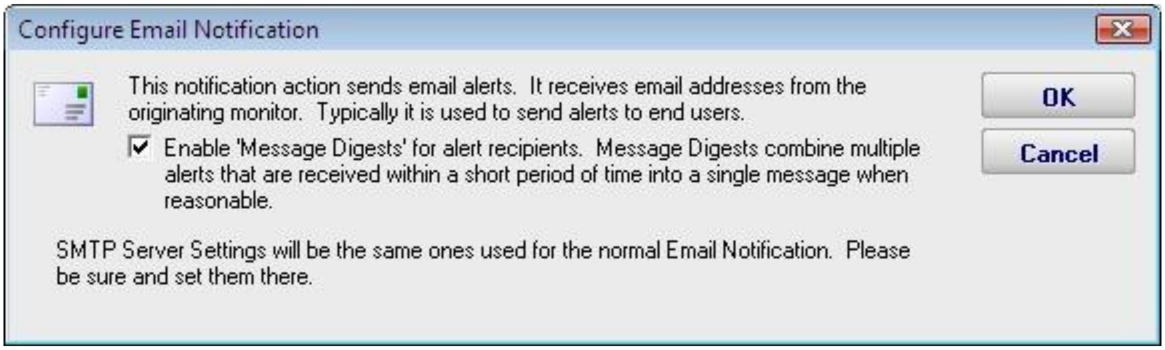
Directed-Email Action

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.



This notification action sends email alerts. It receives email addresses from the originating monitor. Typically it is used to send alerts to end users.

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

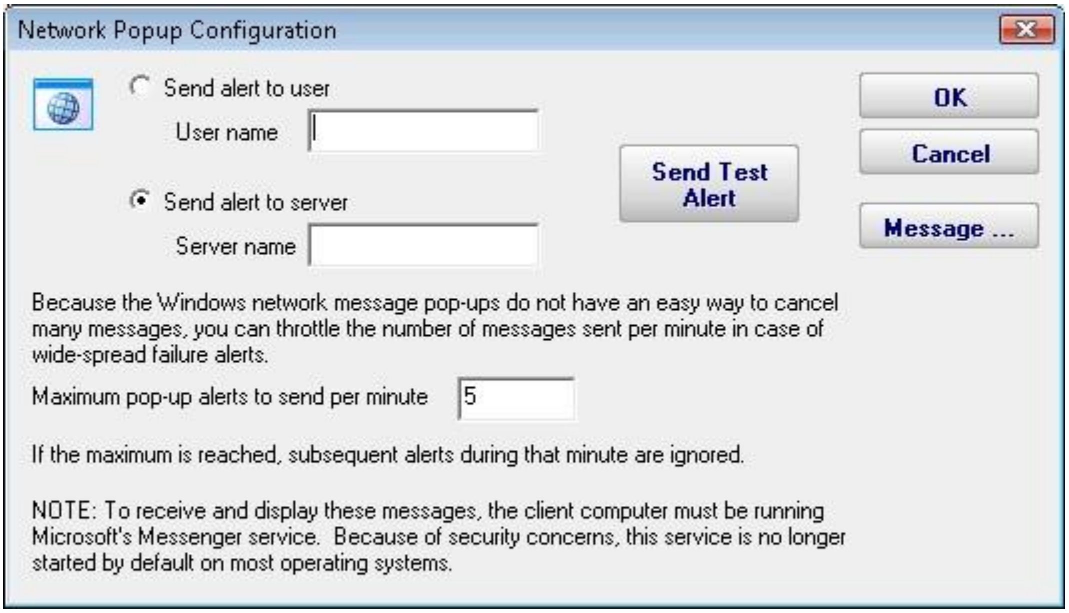
SMTP Server Settings will be the same ones used for the normal Email Notification. Please be sure and set them there.

Contents

Network Message Action

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

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



○ Send alert to user

User name

● Send alert to server

Server name

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

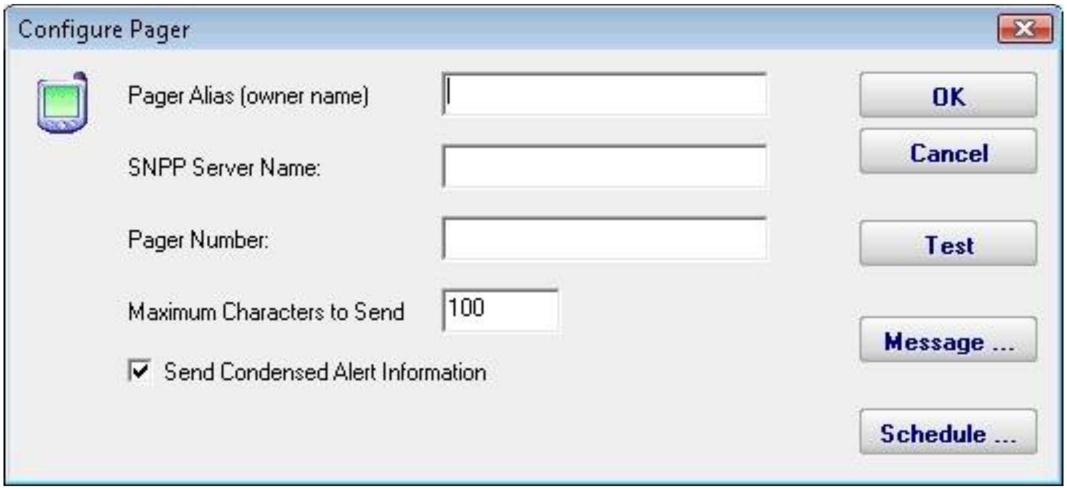
Maximum pop-up alerts to send per minute 5

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

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

Send Pager Alert Action

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



Pager Alias (owner name)

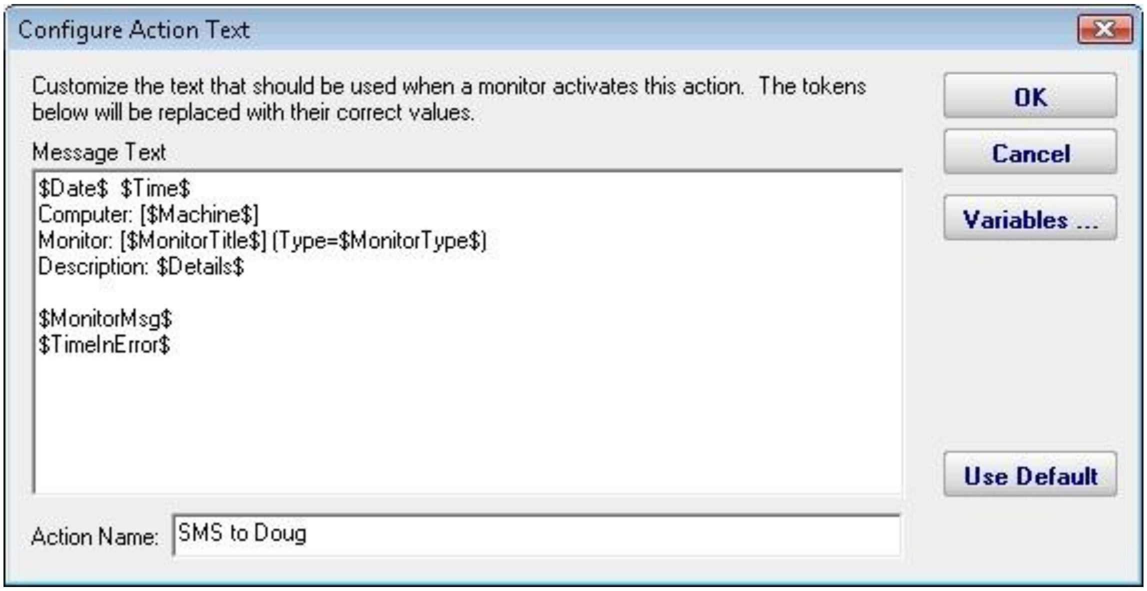
SNPP Server Name:

Pager Number:

Maximum Characters to Send 100

☑ Send Condensed Alert Information

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



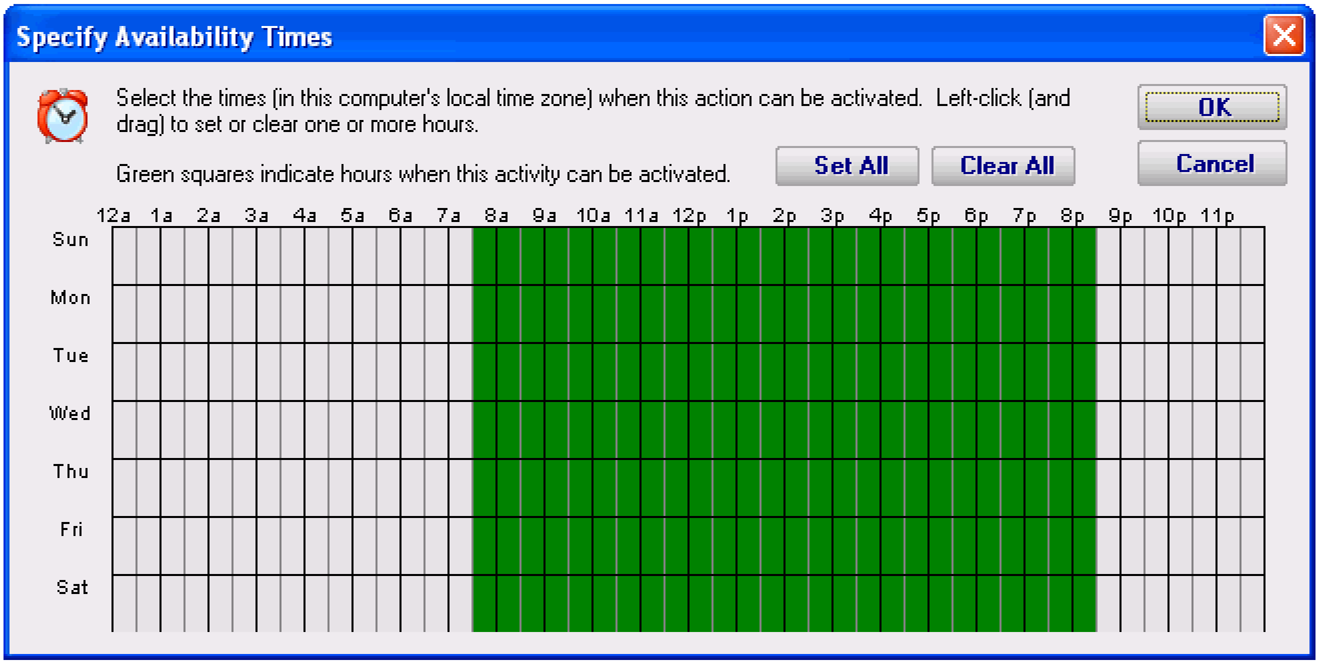
Customize the text that should be used when a monitor activates this action. The tokens below will be replaced with their correct values.

Message Text

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

$MonitorMsg$
$TimeInError$
```

Action Name: SMS to Doug

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



Specify Availability Times

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

Green squares indicate hours when this activity can be activated.

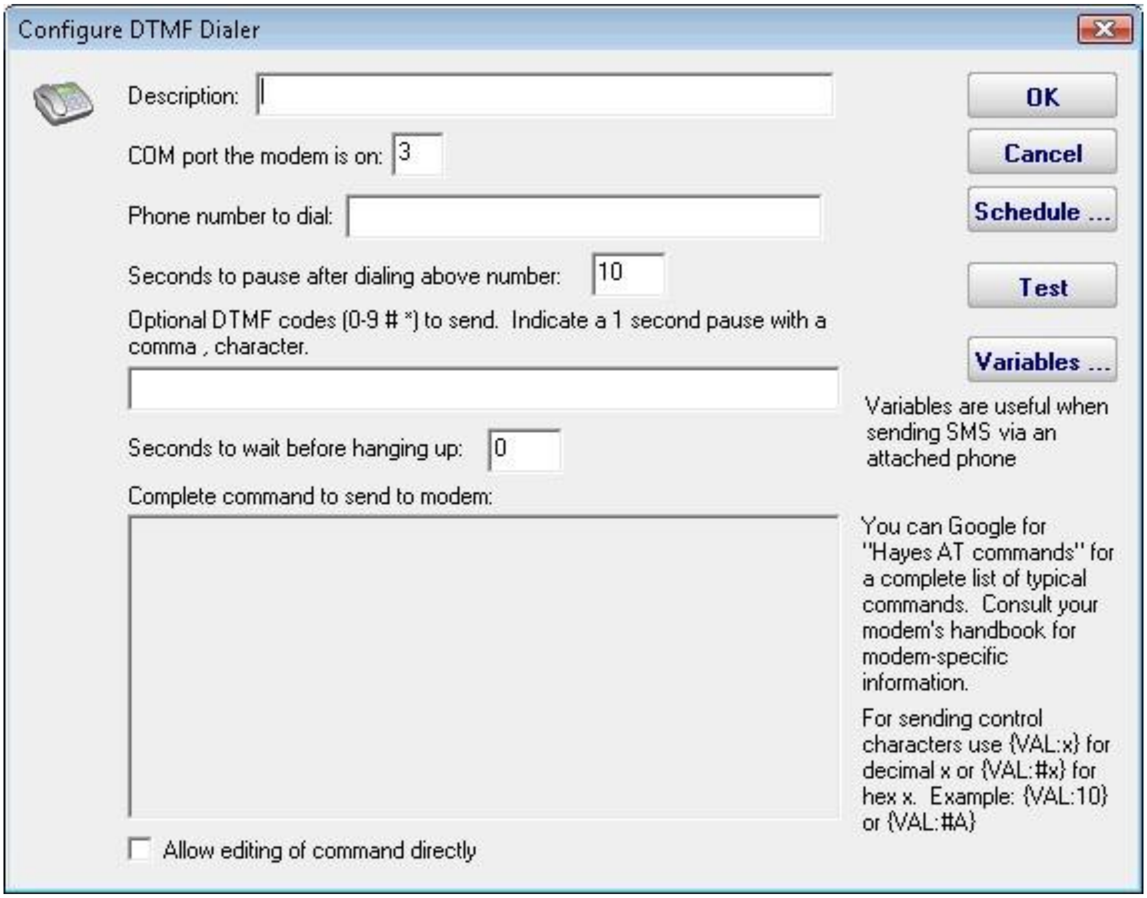
	12a		1a		2a		3a		4a		5a		6a		7a		8a		9a		10a		11a		12p		1p		2p		3p		4p		5p		6p		7p		8p		9p		10p		11p	
Sun																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩							
Mon																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩							
Tue																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩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

Phone Dialer (DTMF/SMS)

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

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

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



Configure DTMF Dialer

Description:

COM port the modem is on: 3

Phone number to dial:

Seconds to pause after dialing above number: 10

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

Seconds to wait before hanging up: 0

Complete command to send to modem:

☐ Allow editing of command directly

Variables are useful when sending SMS via an attached phone

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

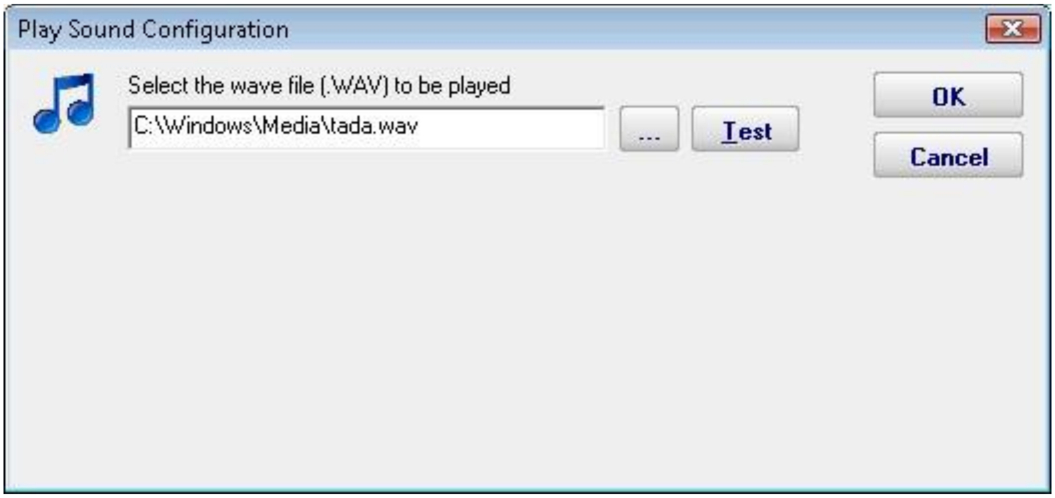
For sending control characters use {VAL:x} for decimal x or {VAL:#x} for hex x. Example: {VAL:10} or {VAL:#A}

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

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

Play Sound File Action

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



Play Sound Configuration

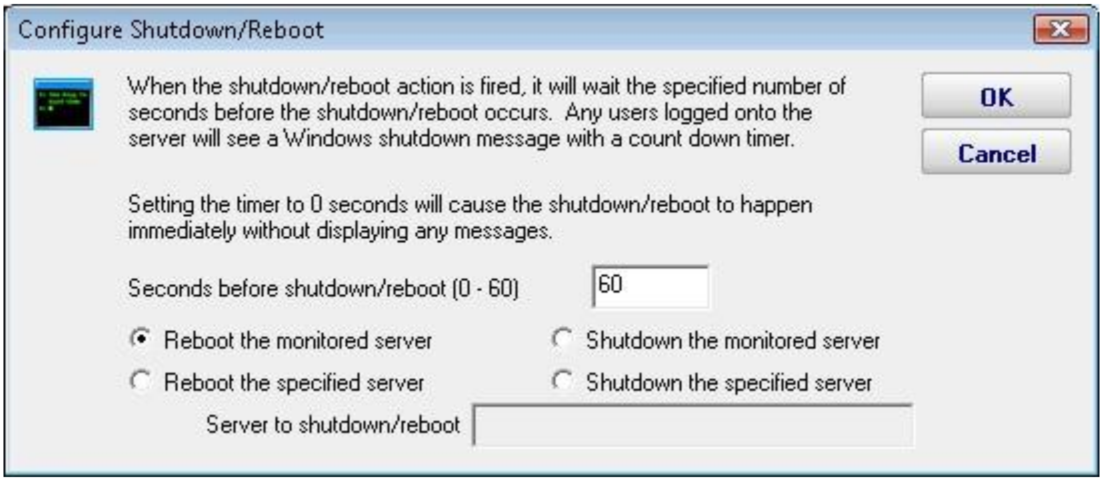
Select the wave file (.WAV) to be played

C:\Windows\Media\tada.wav

Reboot Computer Action

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

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



Configure Shutdown/Reboot

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

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

Seconds before shutdown/reboot (0 - 60): 60

● Reboot the monitored server

○ Shutdown the monitored server

○ Reboot the specified server

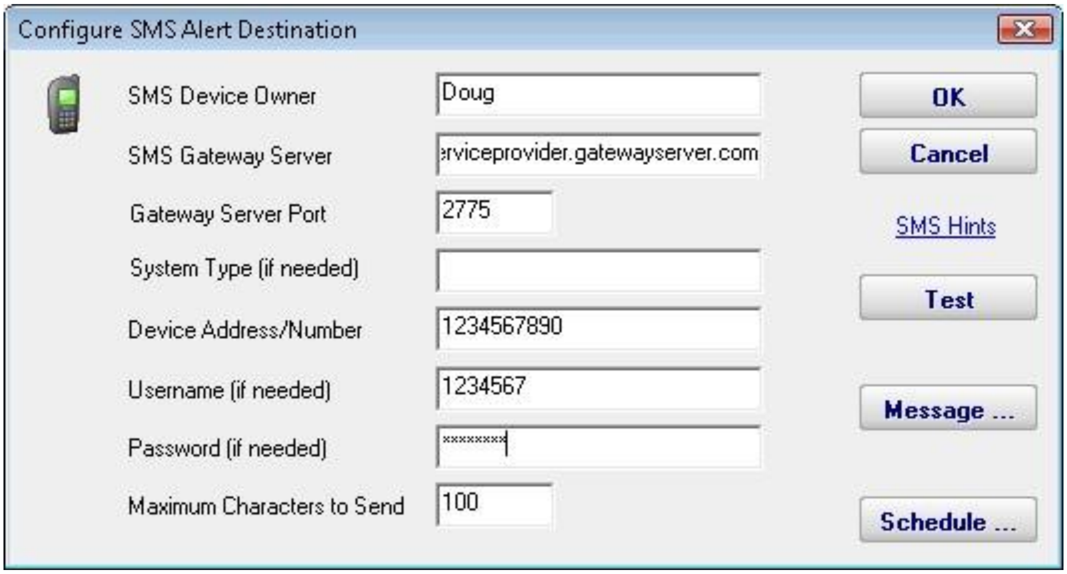
○ Shutdown the specified server

Server to shutdown/reboot:

Contents

SMS Text Message Action

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



Configure SMS Alert Destination

SMS Device Owner: Doug

SMS Gateway Server: erviceprovider.gatewayserver.com

Gateway Server Port: 2775

System Type (if needed):

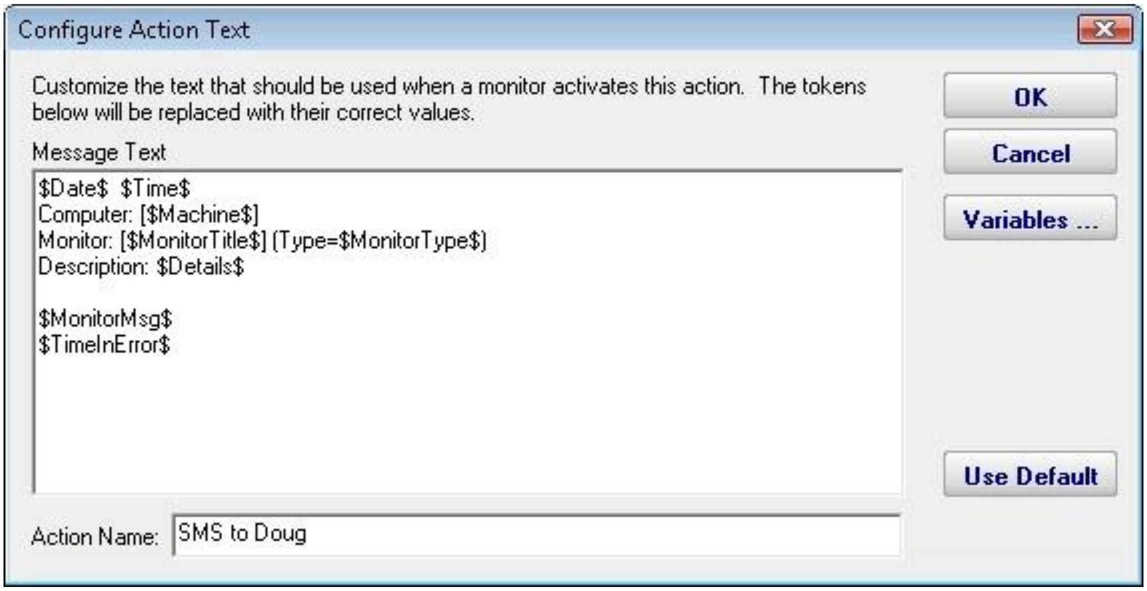
Device Address/Number: 1234567890

Username (if needed): 1234567

Password (if needed): ********

Maximum Characters to Send: 100

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



Configure Action Text

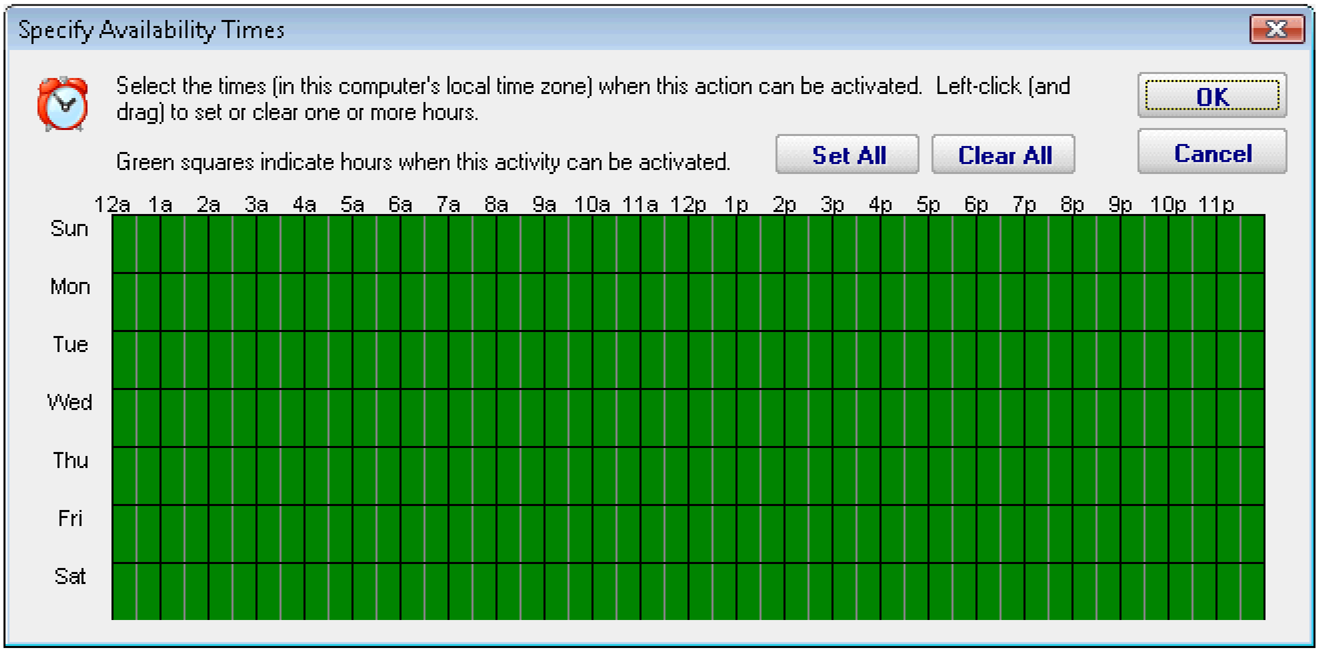
Customize the text that should be used when a monitor activates this action. The tokens below will be replaced with their correct values.

Message Text

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

$MonitorMsg$
$TimeInError$
```

Action Name: SMS to Doug

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



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

Green squares indicate hours when this activity can be activated.

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

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

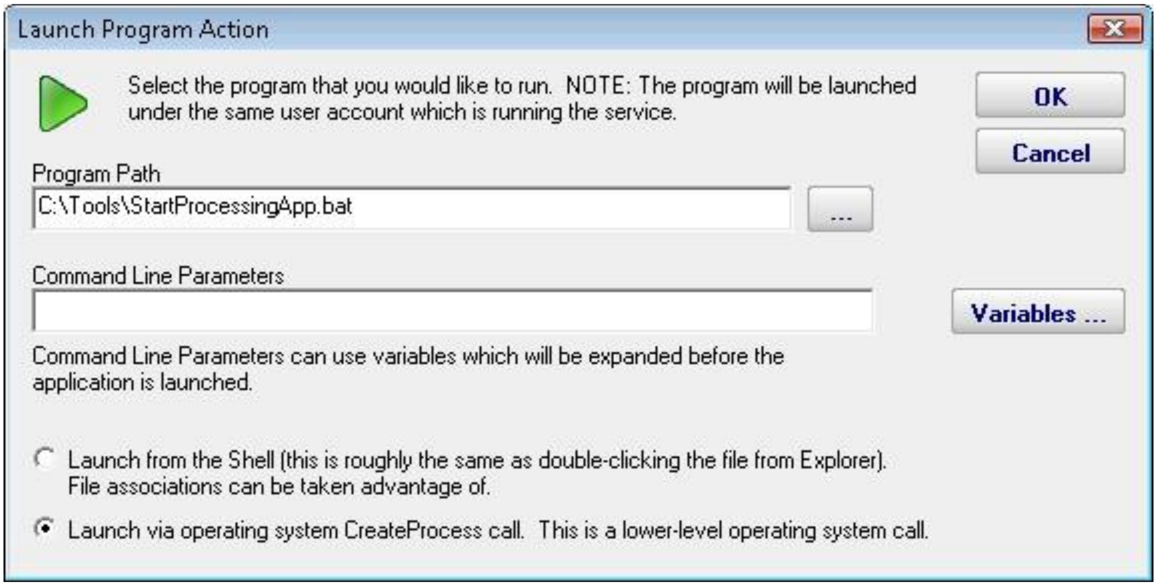
Contents

Start Application Action

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

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

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



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

Program Path: C:\Tools\StartProcessingApp.bat

Command Line Parameters:

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

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

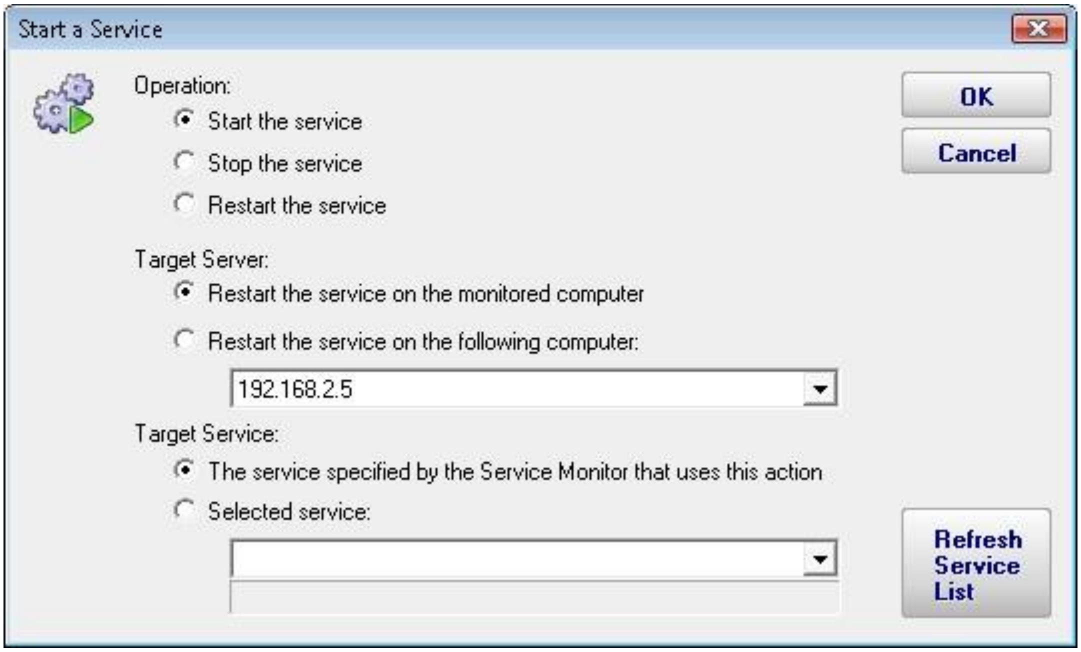
● Launch via operating system CreateProcess call. This is a lower-level operating system call.

Contents

Start, Stop or Restart a Service Action

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

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



Start a Service

Operation:
- ● Start the service
- ○ Stop the service
- ○ Restart the service

Target Server:
- ● Restart the service on the monitored computer
- ○ Restart the service on the following computer:

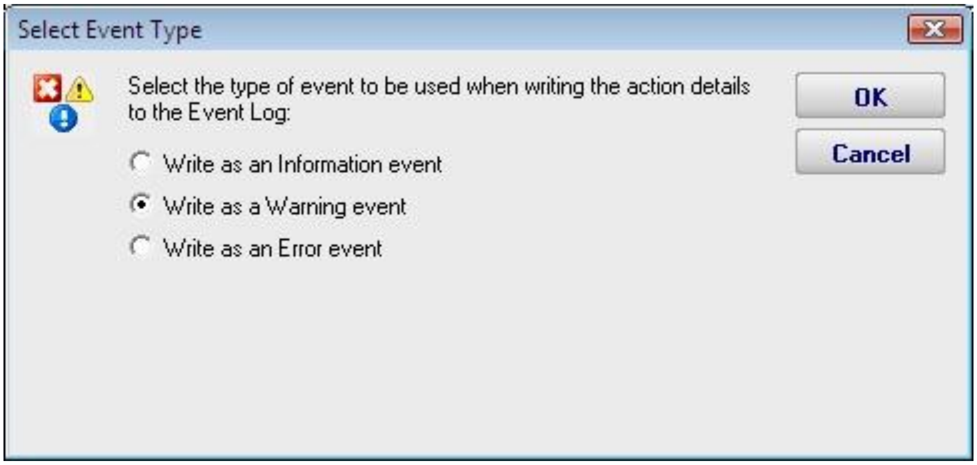
192.168.2.5

Target Service:
- ● The service specified by the Service Monitor that uses this action
- ○ Selected service:

Contents

Write to Event Log Action

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



Select Event Type

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

○ Write as an Information event

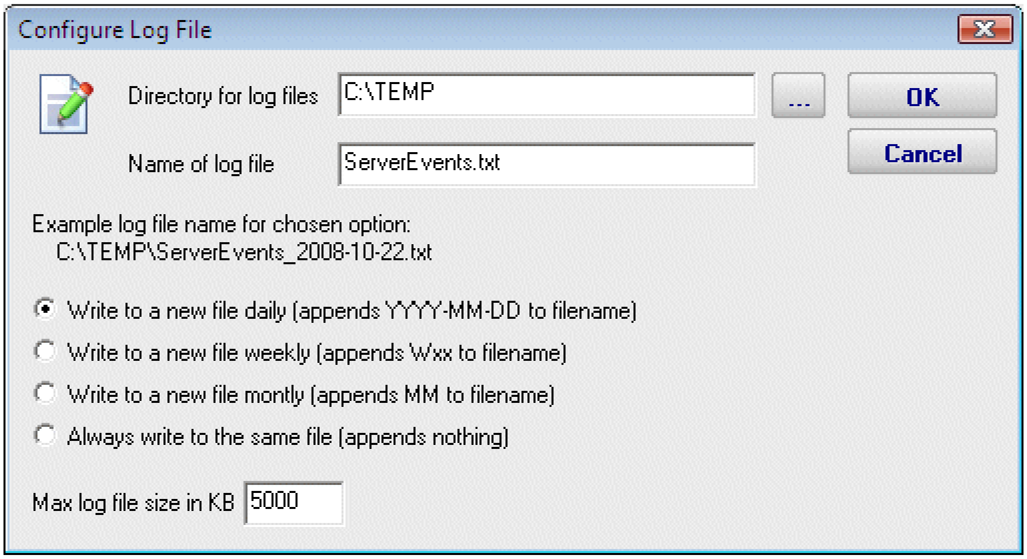
● Write as a Warning event

○ Write as an Error event

Contents

Write to a Text Log File Action

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



Configure Log File

Directory for log files: C:\TEMP

Name of log file: ServerEvents.txt

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

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

Max log file size in KB: 5000

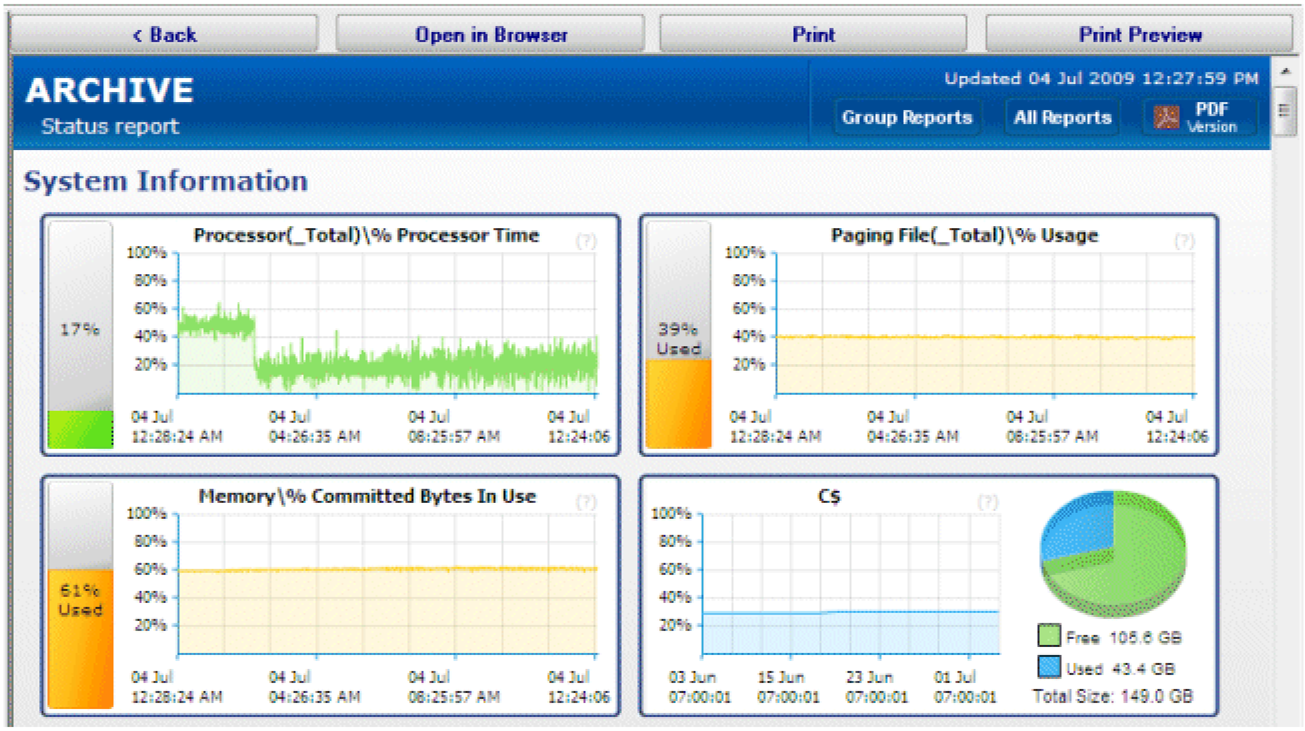
Reports

Contents

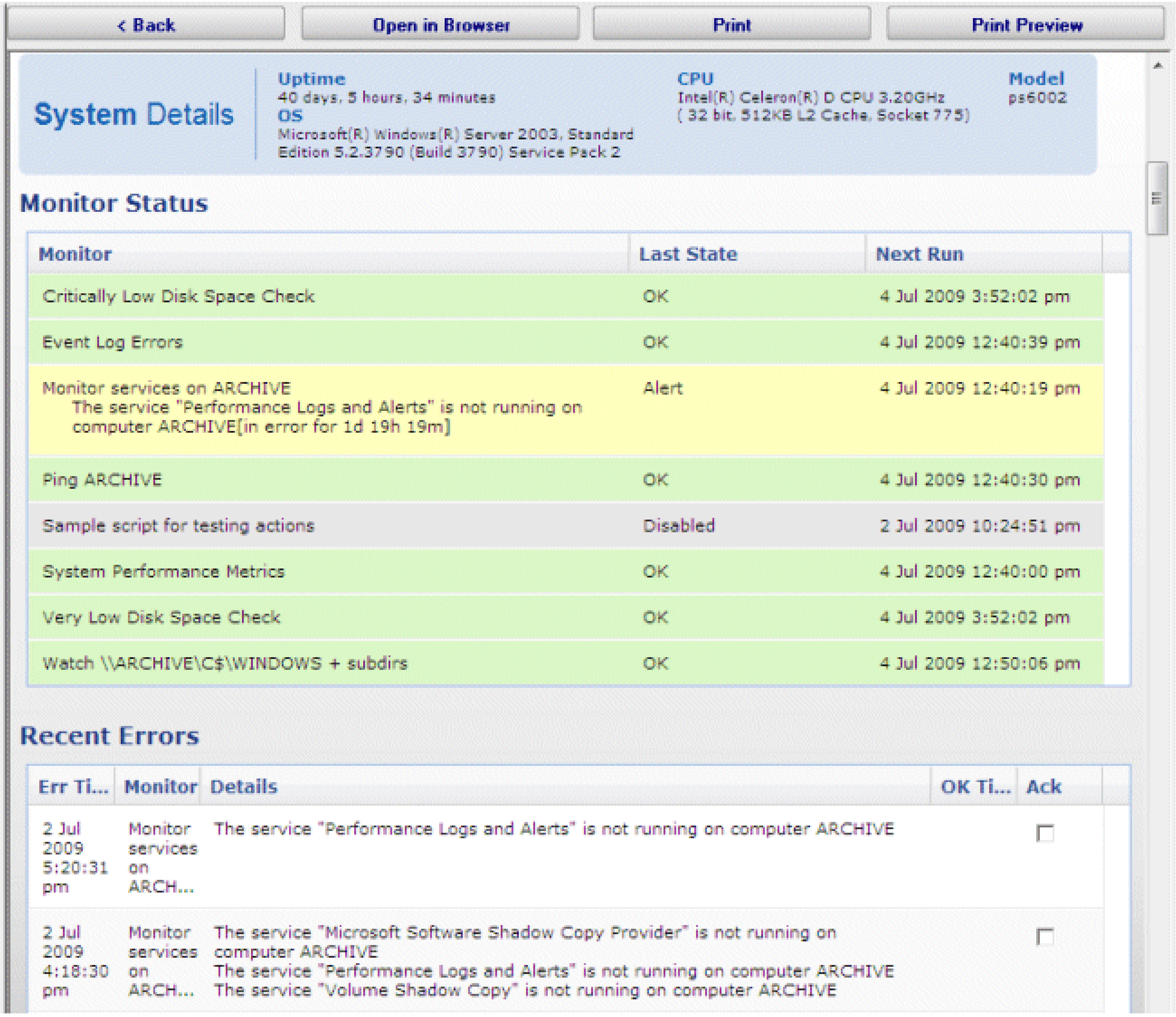
Server Status Report

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

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



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



System Details

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

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

Model
ps6002

Monitor Status

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

Recent Errors

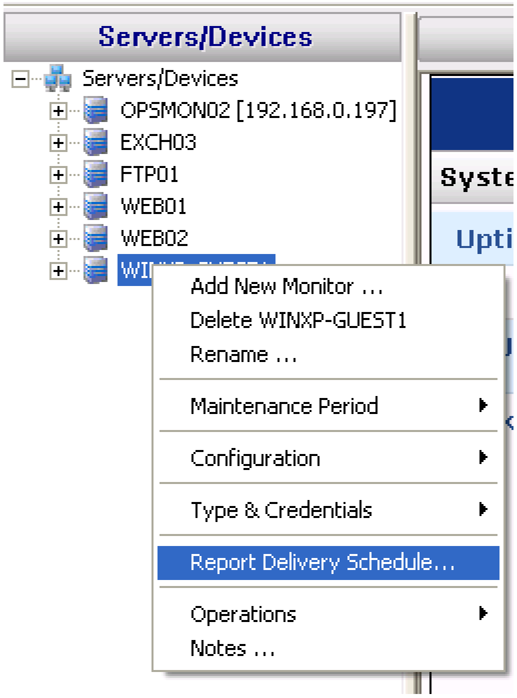
Err Ti...	Monitor	Details	OK Ti...	Ack
2 Jul 2009 5:20:31 pm	Monitor services on ARCH...	The service "Performance Logs and Alerts" is not running on computer ARCHIVE		□
2 Jul 2009 4:18:30 pm	Monitor services on ARCH...	The service "Microsoft Software Shadow Copy Provider" is not running on computer ARCHIVE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

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

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

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

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


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

Contents

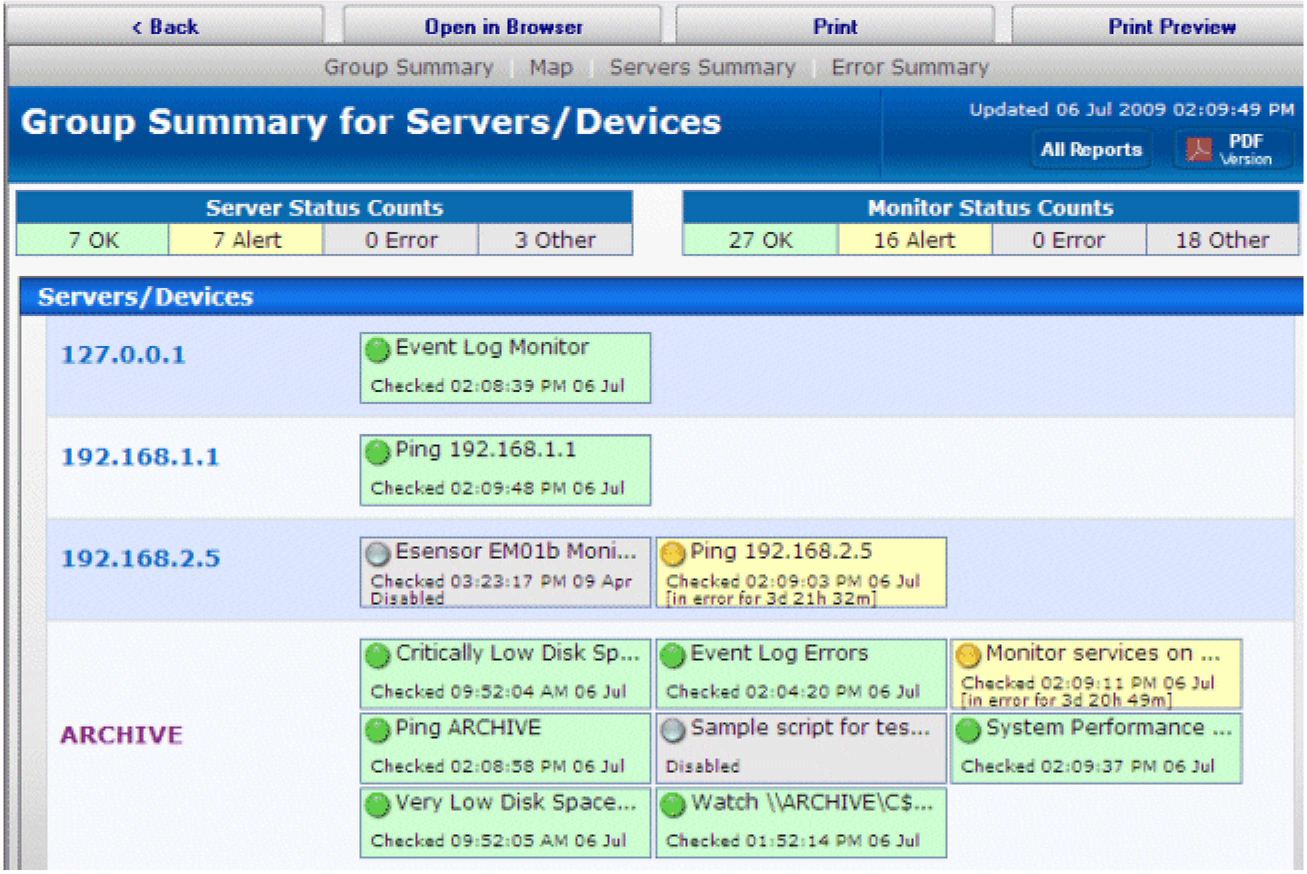
Group Summary Report

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.



Group Summary for Servers/Devices

Updated 06 Jul 2009 02:09:49 PM

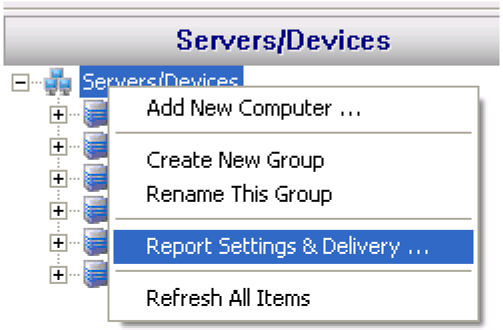
Server Status Counts			
7 OK	7 Alert	0 Error	3 Other

Monitor Status Counts			
27 OK	16 Alert	0 Error	18 Other

Servers/Devices

127.0.0.1	Event Log Monitor Checked 02:08:39 PM 06 Jul		
192.168.1.1	Ping 192.168.1.1 Checked 02:09:48 PM 06 Jul		
192.168.2.5	Esensor EM01b Moni... Checked 03:23:17 PM 09 Apr Disabled	Ping 192.168.2.5 Checked 02:09:03 PM 06 Jul [in error for 3d 21h 32m]	
ARCHIVE	Critically Low Disk Sp... Checked 09:52:04 AM 06 Jul	Event Log Errors Checked 02:04:20 PM 06 Jul	Monitor services on ... Checked 02:09:11 PM 06 Jul [in error for 3d 20h 49m]
	Ping ARCHIVE Checked 02:08:58 PM 06 Jul	Sample script for tes... Disabled	System Performance ... Checked 02:09:37 PM 06 Jul
	Very Low Disk Space... Checked 09:52:05 AM 06 Jul	Watch \\ARCHIVE\C$... Checked 01:52:14 PM 06 Jul	

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.

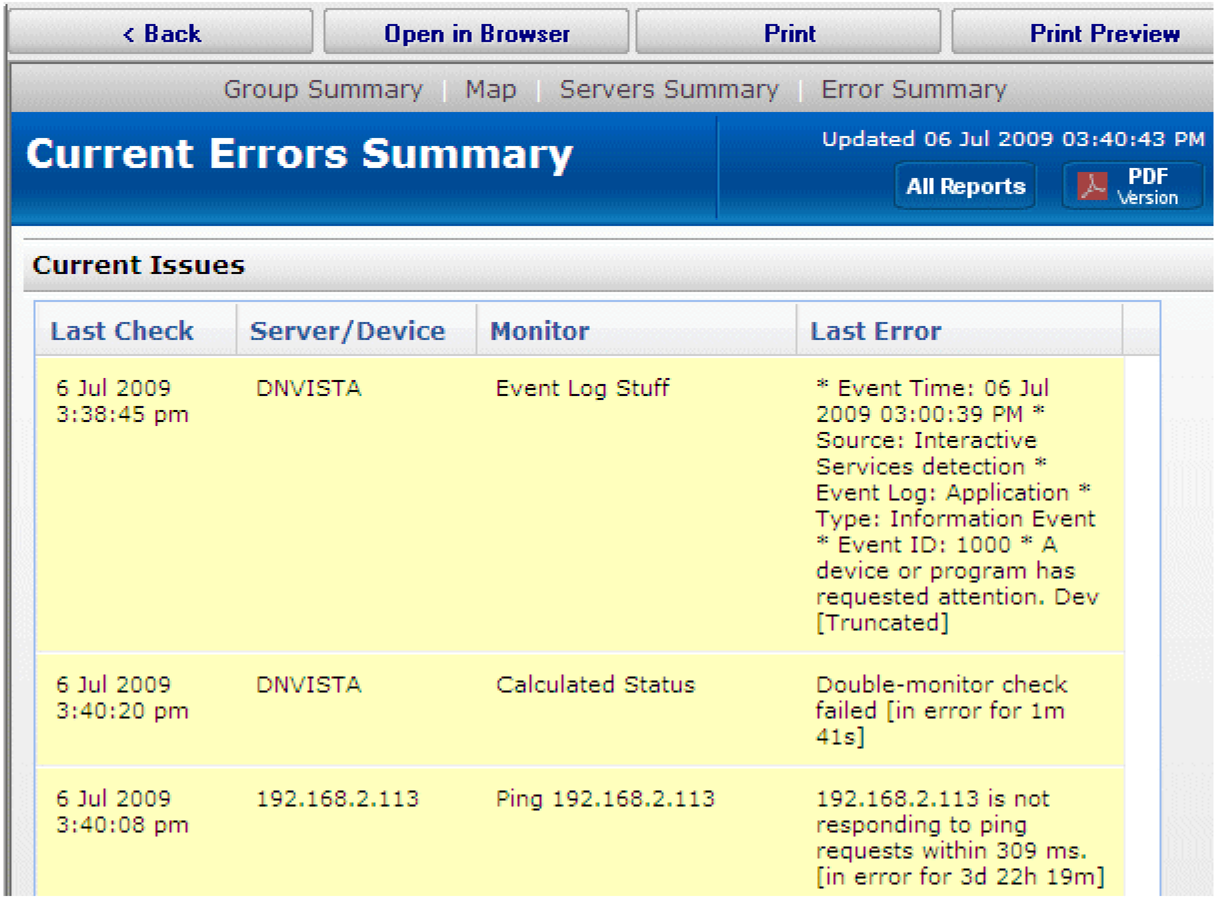


To see an even higher level view of the servers within the group, try the All Servers Report or customize the Visual Status Map report.

Contents

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.



Current Errors Summary

Updated 06 Jul 2009 03:40:43 PM

Current Issues

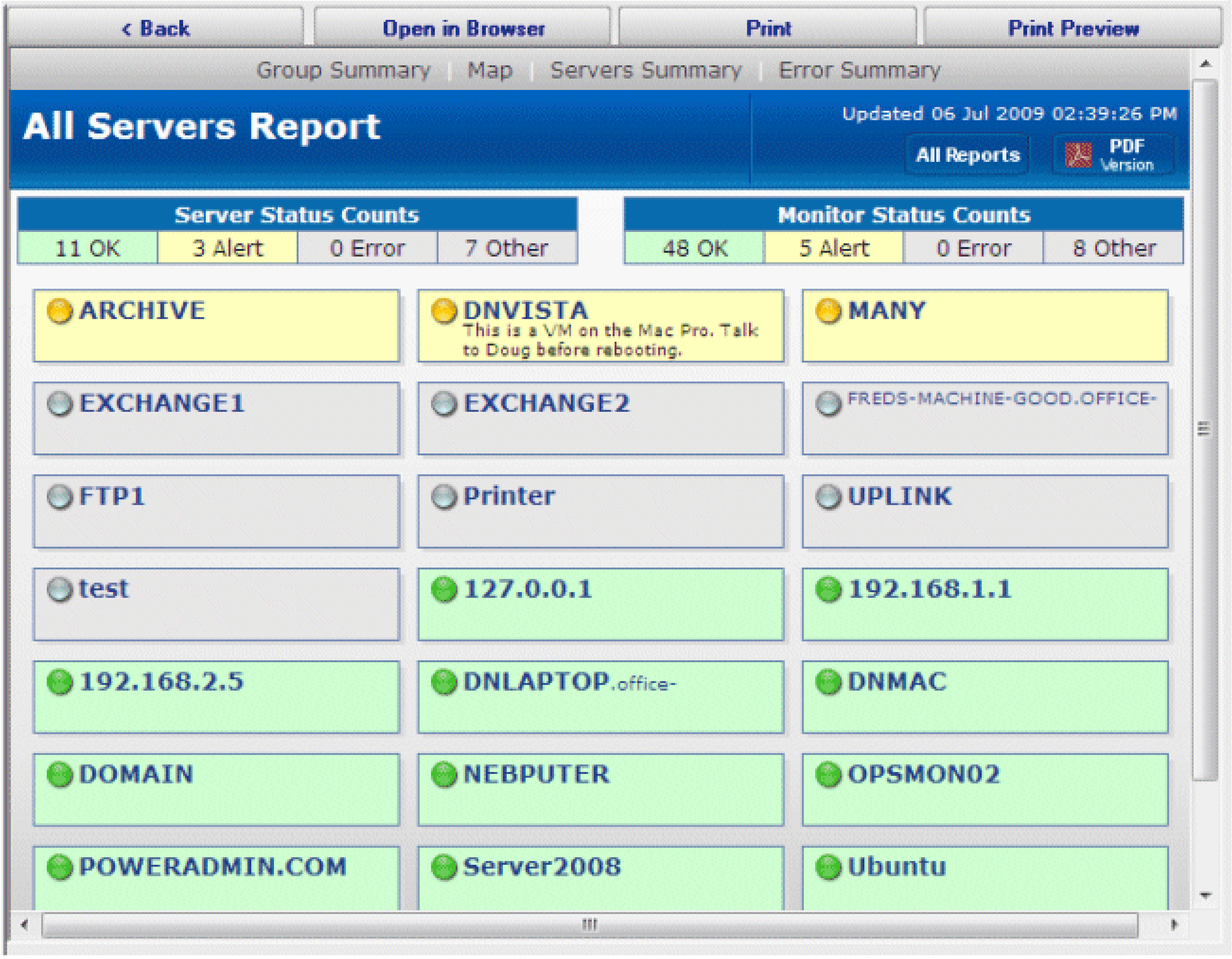
Last Check	Server/Device	Monitor	Last Error
6 Jul 2009 3:38:45 pm	DNVISTA	Event Log Stuff	* Event Time: 06 Jul 2009 03:00:39 PM * Source: Interactive Services detection * Event Log: Application * Type: Information Event * Event ID: 1000 * A device or program has requested attention. Dev [Truncated]
6 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.



All Servers Report

Updated 06 Jul 2009 02:39:26 PM

Server Status Counts			
11 OK	3 Alert	0 Error	7 Other

Monitor Status Counts			
48 OK	5 Alert	0 Error	8 Other

ARCHIVE	DNVISTA This is a VM on the Mac Pro. Talk to Doug before rebooting.	MANY
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	Ubuntu

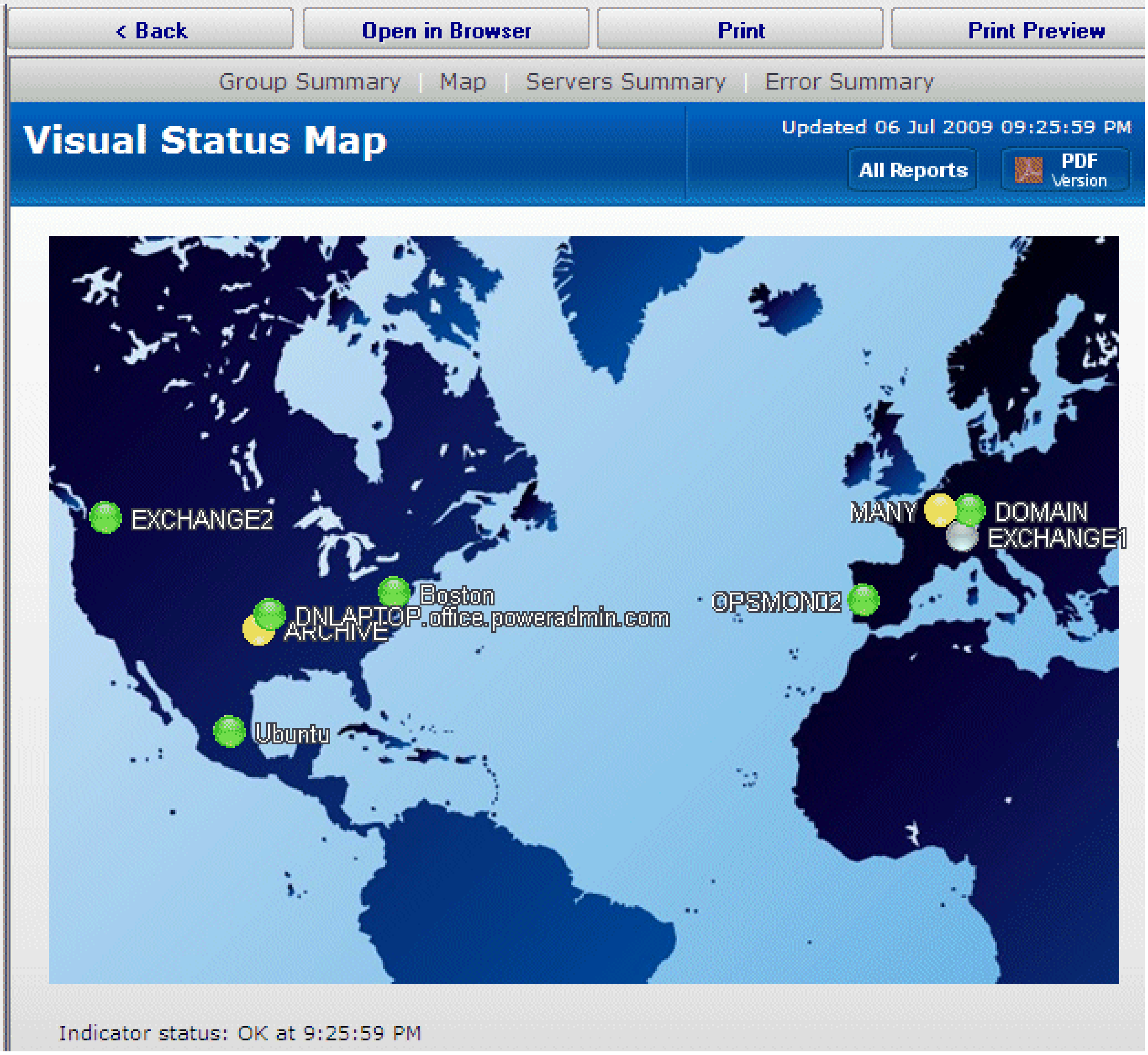
Clicking on any computer will take you to that server's server status report.

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:


< 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
EXCHANGE2
Boston
DNLAPTOP.office.poweradmin.com
ARCHIVE
Ubuntu
OPSMON02
MANY
DOMAIN
EXCHANGE1
Indicator status: OK at 9:25:59 PM

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 grapic.

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

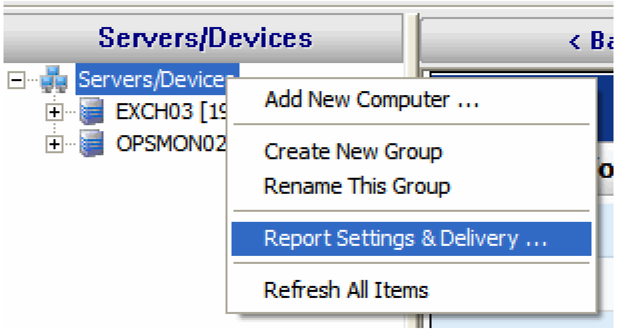
The colors displayed by the status indicators correspond to the "worst" monitor state of all monitors on the computer (or for all monitors within the computer group). In other words, the presence of one monitor in an alert state for a given computer will cause its indicator to display in yellow. A "green"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

Contents

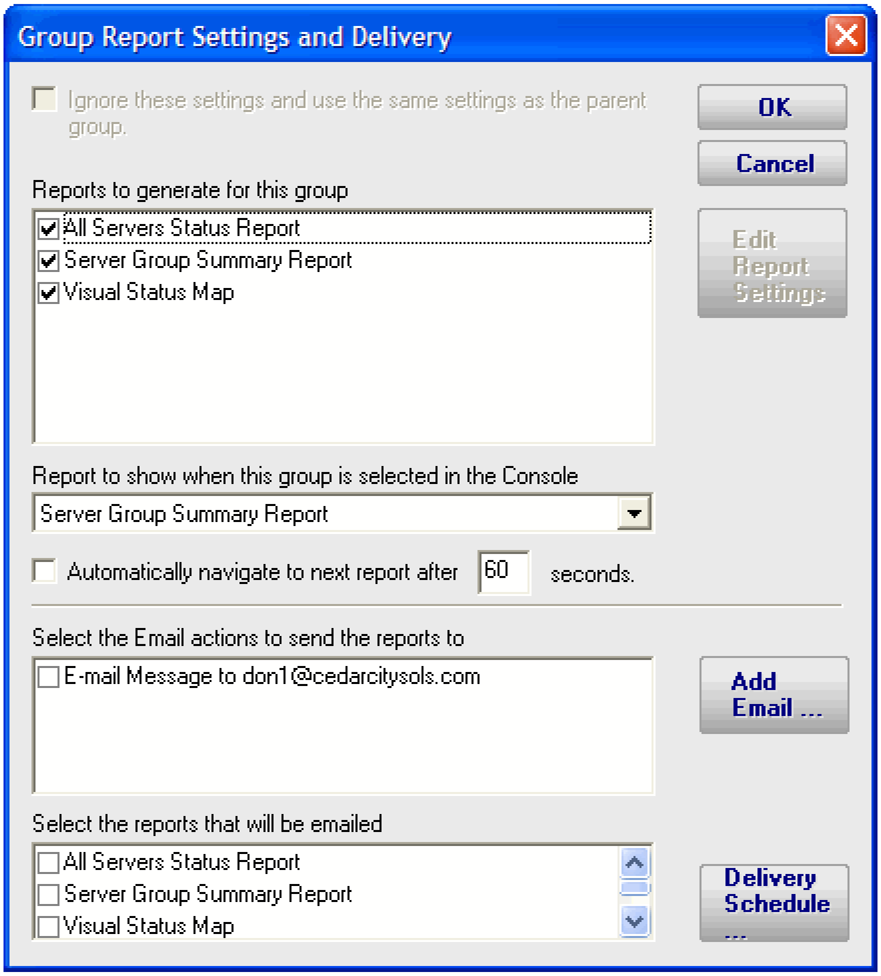
Group Report Settings and Delivery

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.



□ Ignore these settings and use the same settings as the parent group.

Reports to generate for this group

☑ All Servers Status Report
☑ Server Group Summary Report
☑ Visual Status Map

Report to show when this group is selected in the Console

Server Group Summary Report

□ Automatically navigate to next report after 60 seconds.

Select the Email actions to send the reports to

□ E-mail Message to don1@cedarcitysols.com

Select the reports that will be emailed

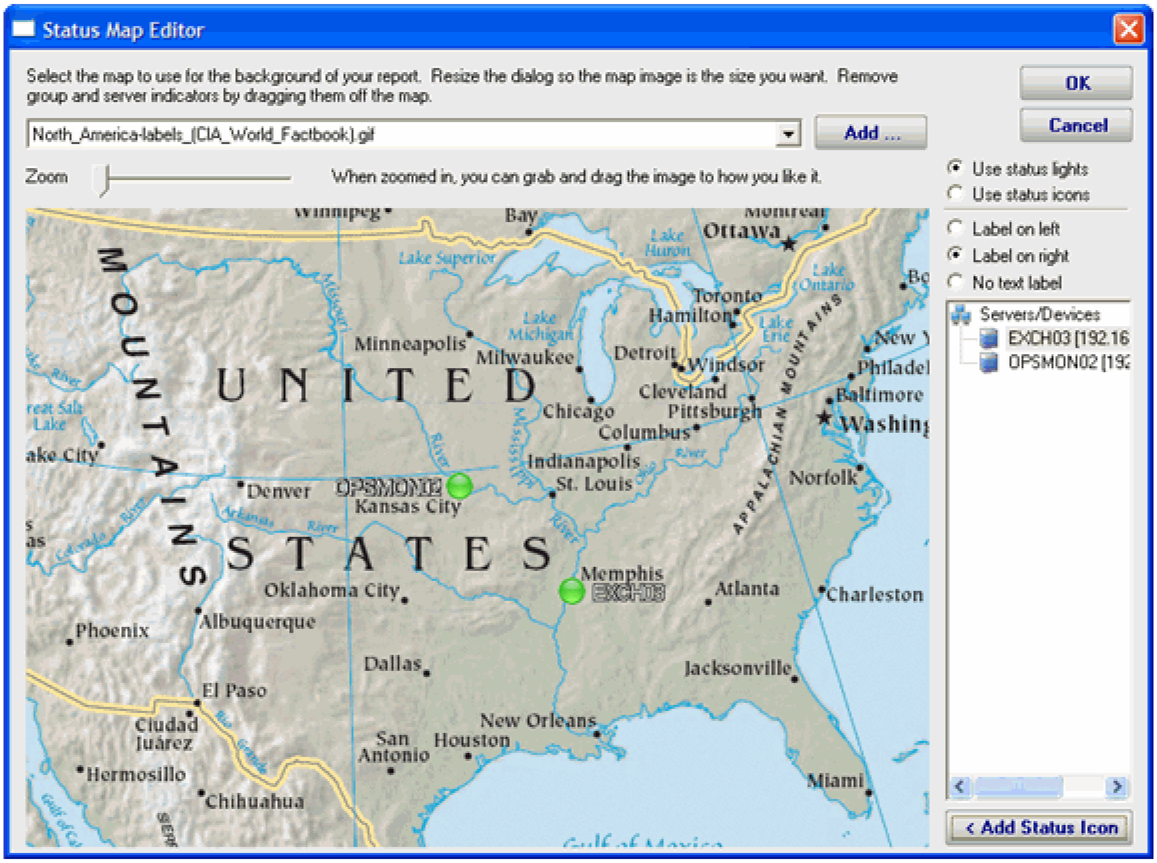
□ All Servers Status Report
□ Server Group Summary Report
□ Visual Status Map

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 specific 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.



Status Map Editor

Select the map to use for the background of your report. Resize the dialog so the map image is the size you want. Remove group and server indicators by dragging them off the map.

North_America-labels_(CIA_World_Factbook).gif

Zoom

When zoomed in, you can grab and drag the image to how you like it.

● Use status lights
○ Use status icons

○ Label on left
● Label on right
○ No text label

Servers/Devices
- EXCH03 [192.16
- OPSMON02 [19

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.

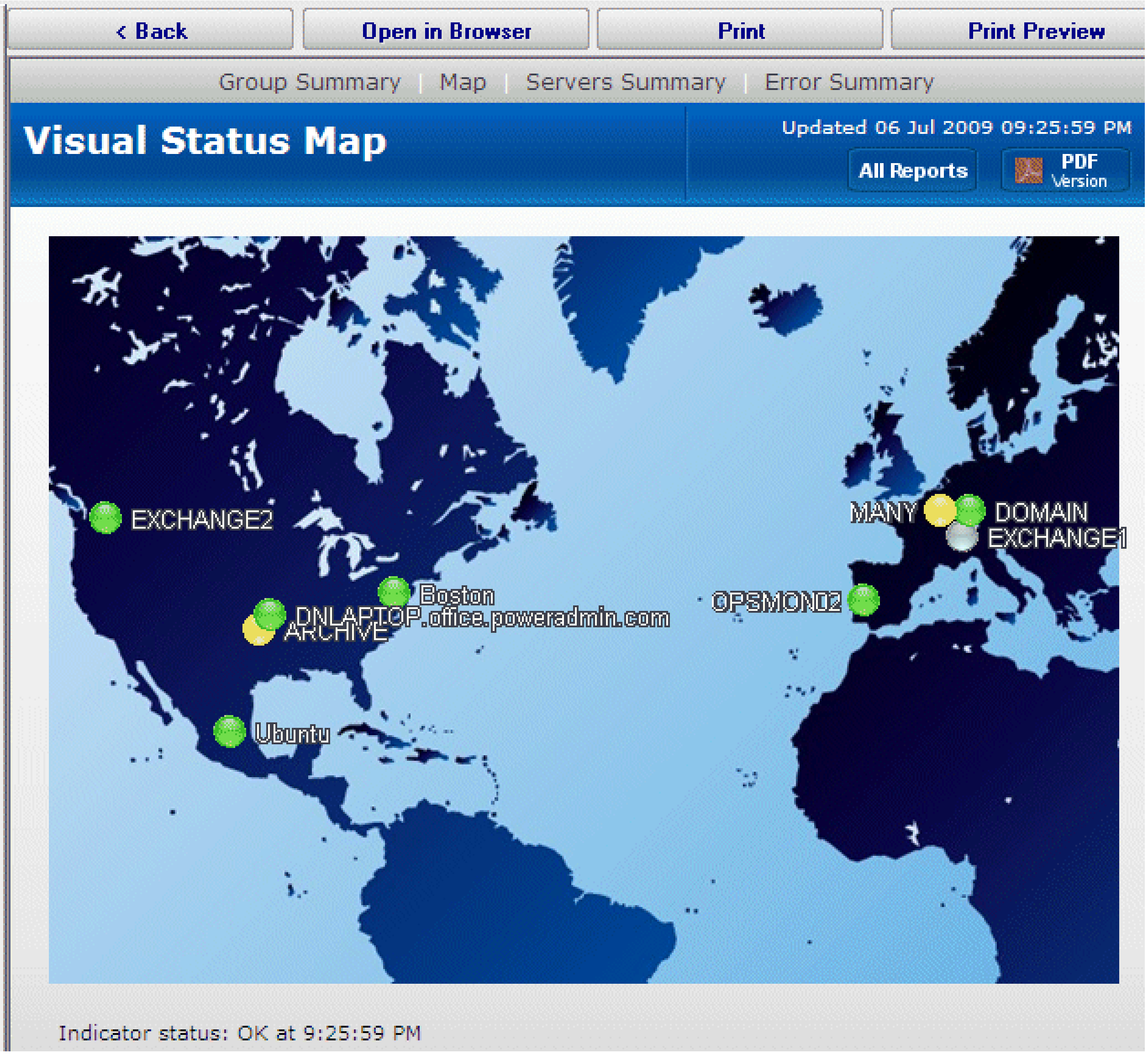
The functions provided by the Status Map editor are as follows.

- 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 Server 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 Server 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.



Visual Status Map

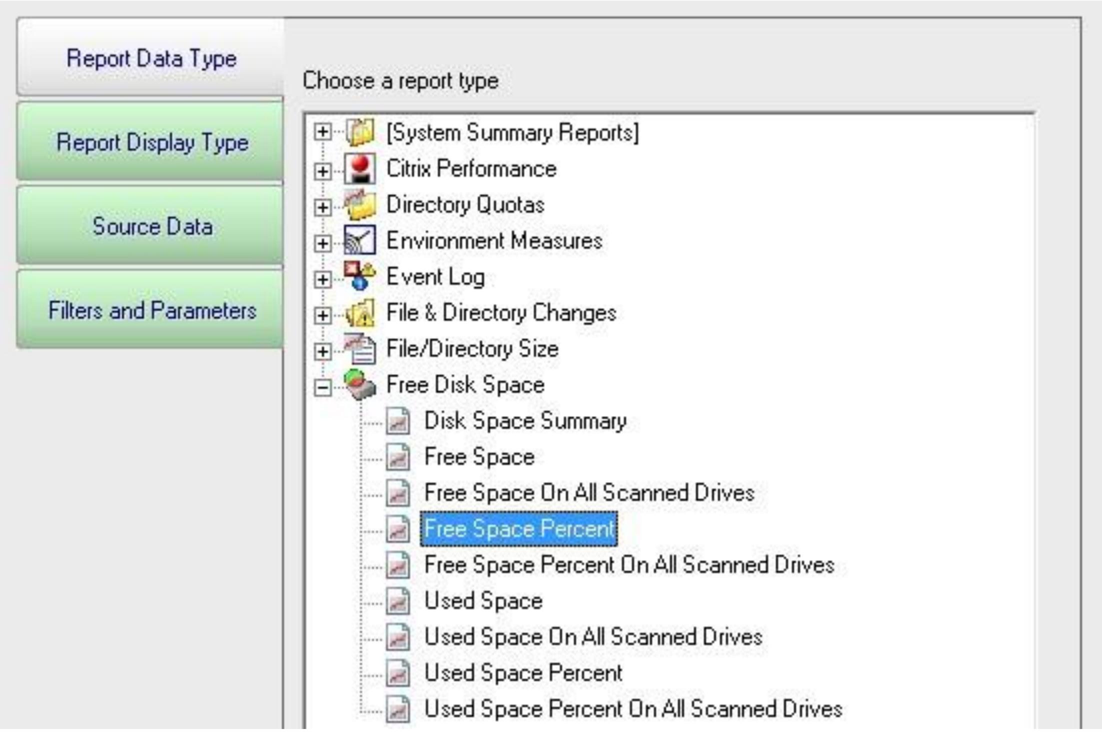
Updated 06 Jul 2009 09:25:59 PM

Indicator status: OK at 9:25:59 PM

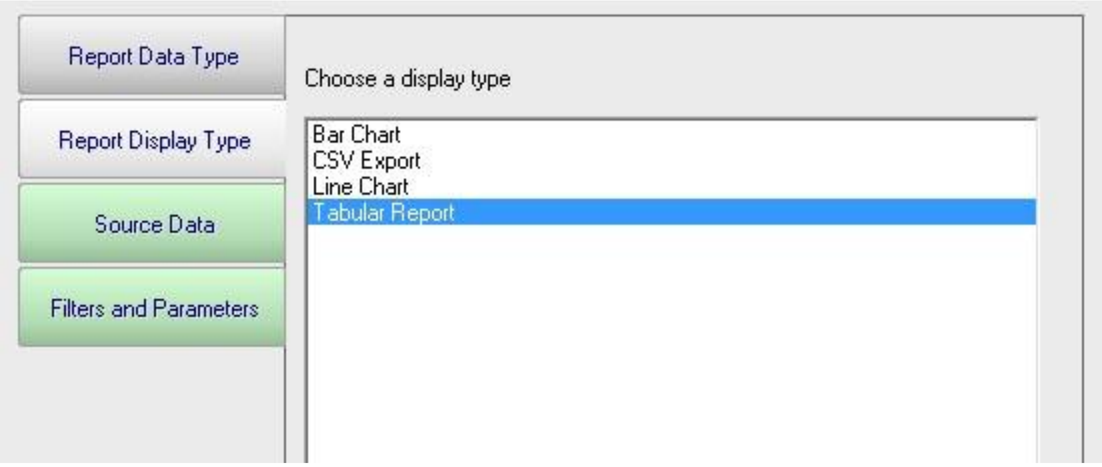
Ad Hoc Reports

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 tha tab. Note that the reports present in your application may differ from those shown in the image below.

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



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



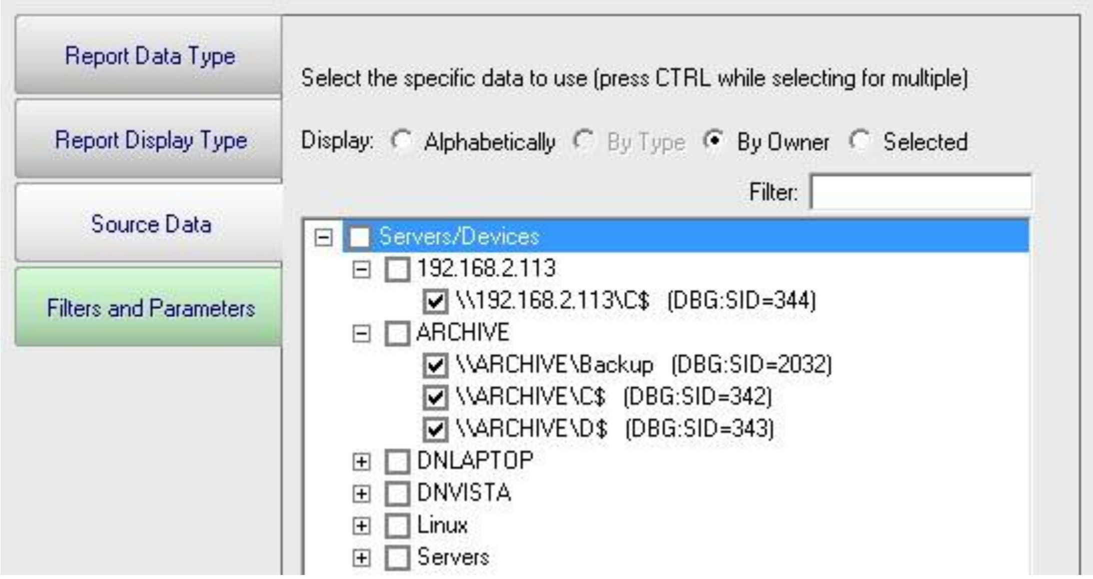
Choose a display type

Bar Chart
CSV Export
Line Chart
Tabular Report

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

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

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



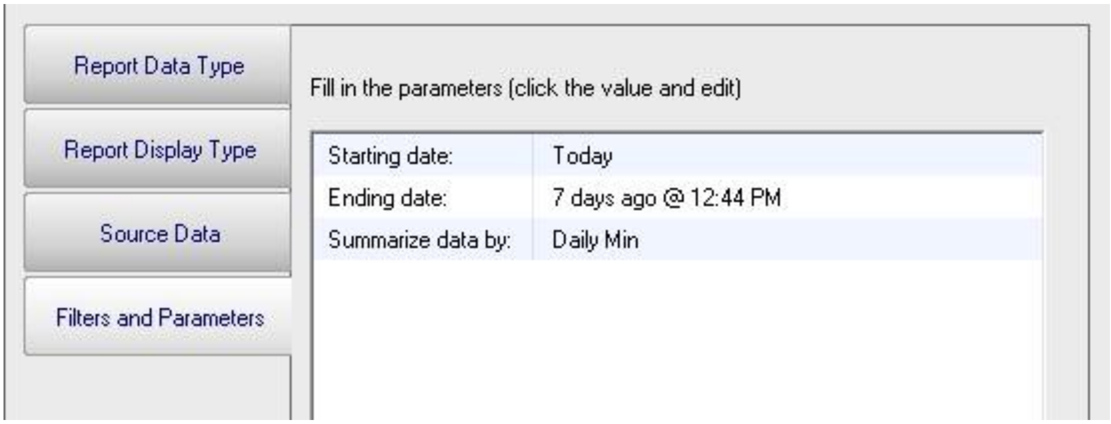
Select the specific data to use (press CTRL while selecting for multiple)

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

Filter:

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

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



Fill in the parameters (click the value and edit)

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

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

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

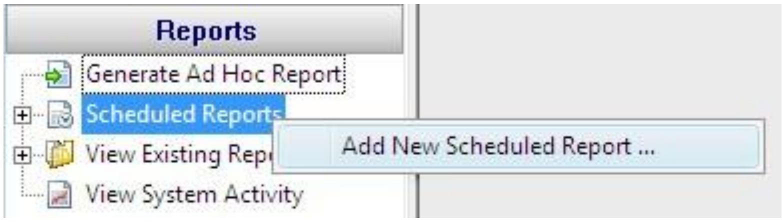
Report Troubleshooting

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

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

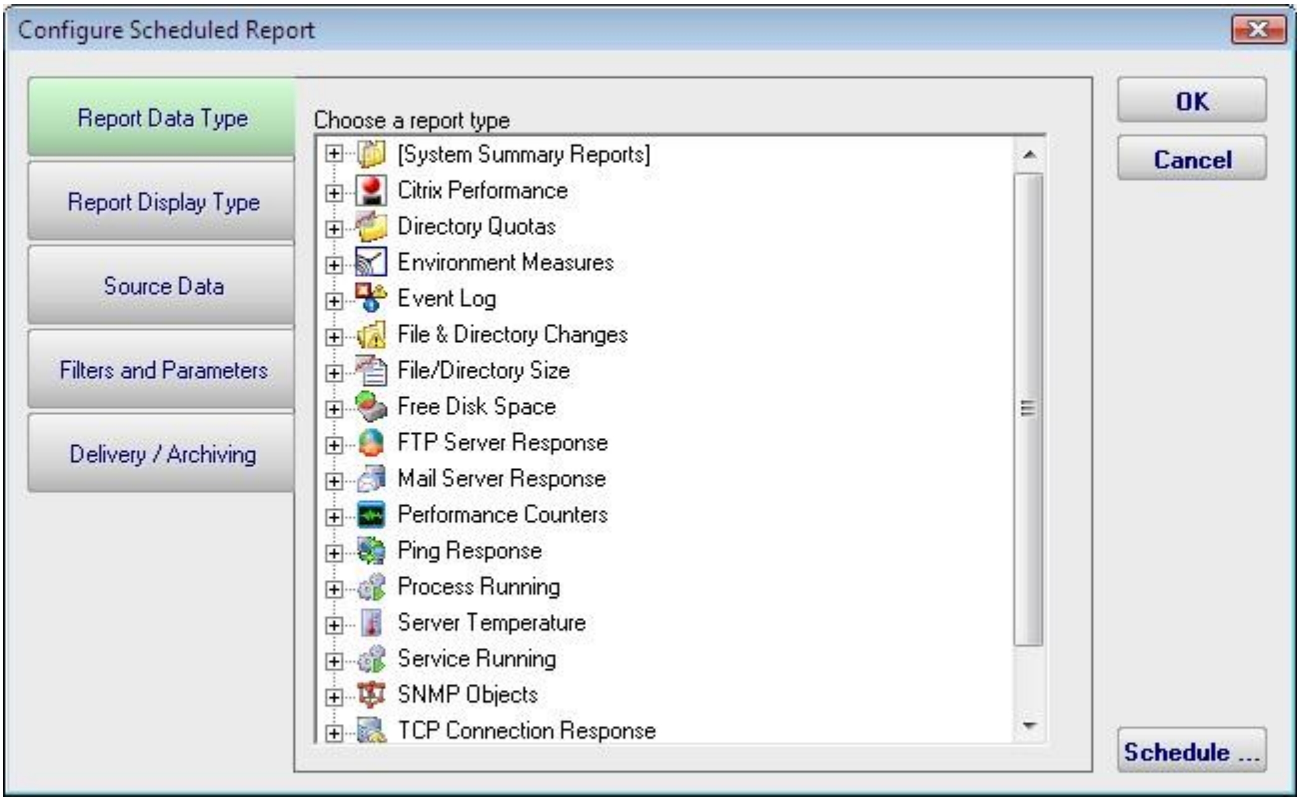
Scheduled Reports

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



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

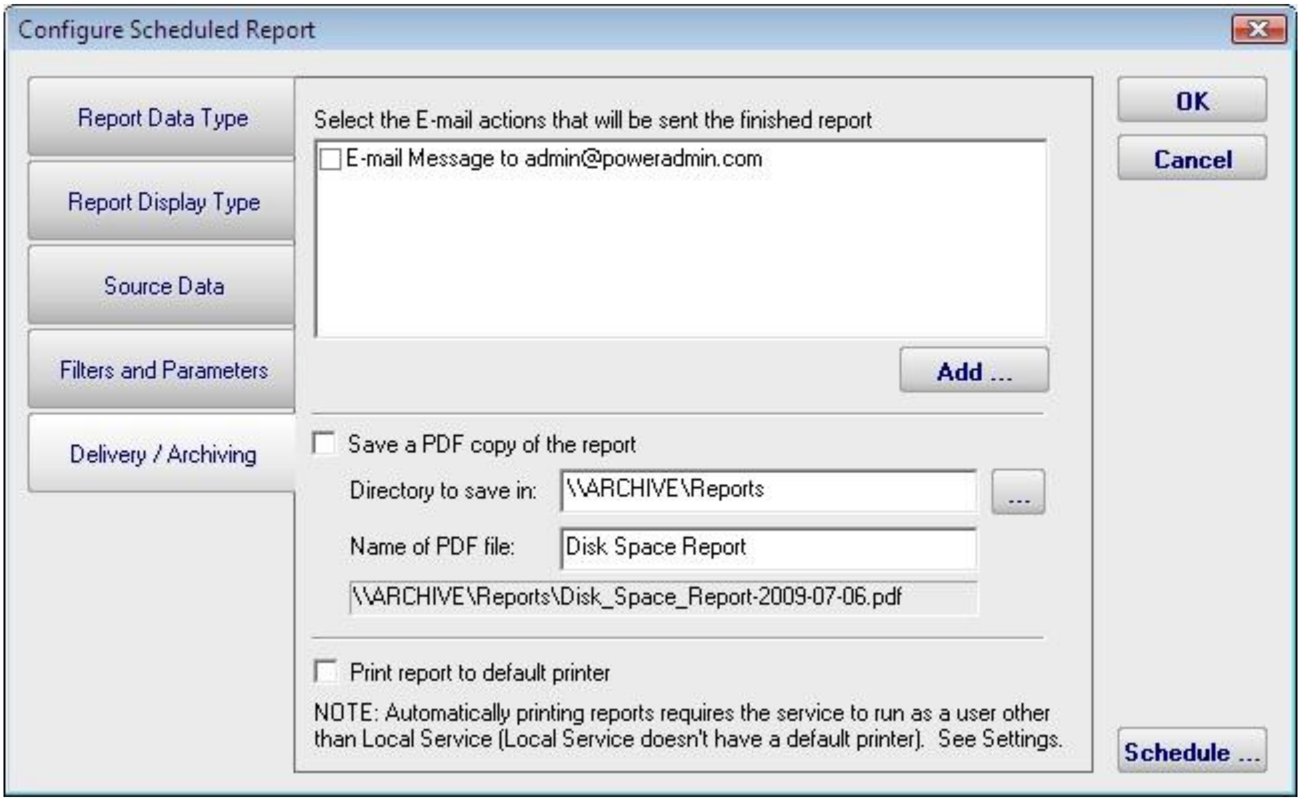
Just like with ad-hoc reports, you choose a monitor-type that sourced the data you want to report on, a report type (chart, tabular, CSV). You also choose a specific dataset to report on. Near the bottom of the dialog you specify reporting parameters that are unique to that report. More detail is given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



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

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

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



Configure Scheduled Report

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

□ E-mail Message to admin@poweradmin.com

□ Save a PDF copy of the report

Directory to save in: \\ARCHIVE\Reports

Name of PDF file: Disk Space Report

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

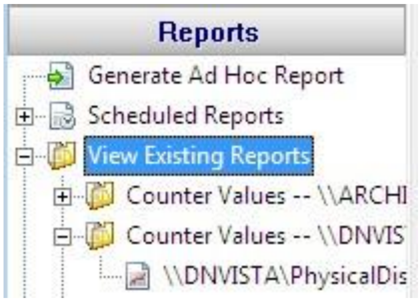
□ Print report to default printer

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

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

Reports that have already run are available in two locations:

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



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

Report Troubleshooting

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

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

Contents

Using Alternate Web Servers to Publish Reports

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

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

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

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

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

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

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

  and add a String value named:

  HTTP_URL_OVERRIDE

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

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

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

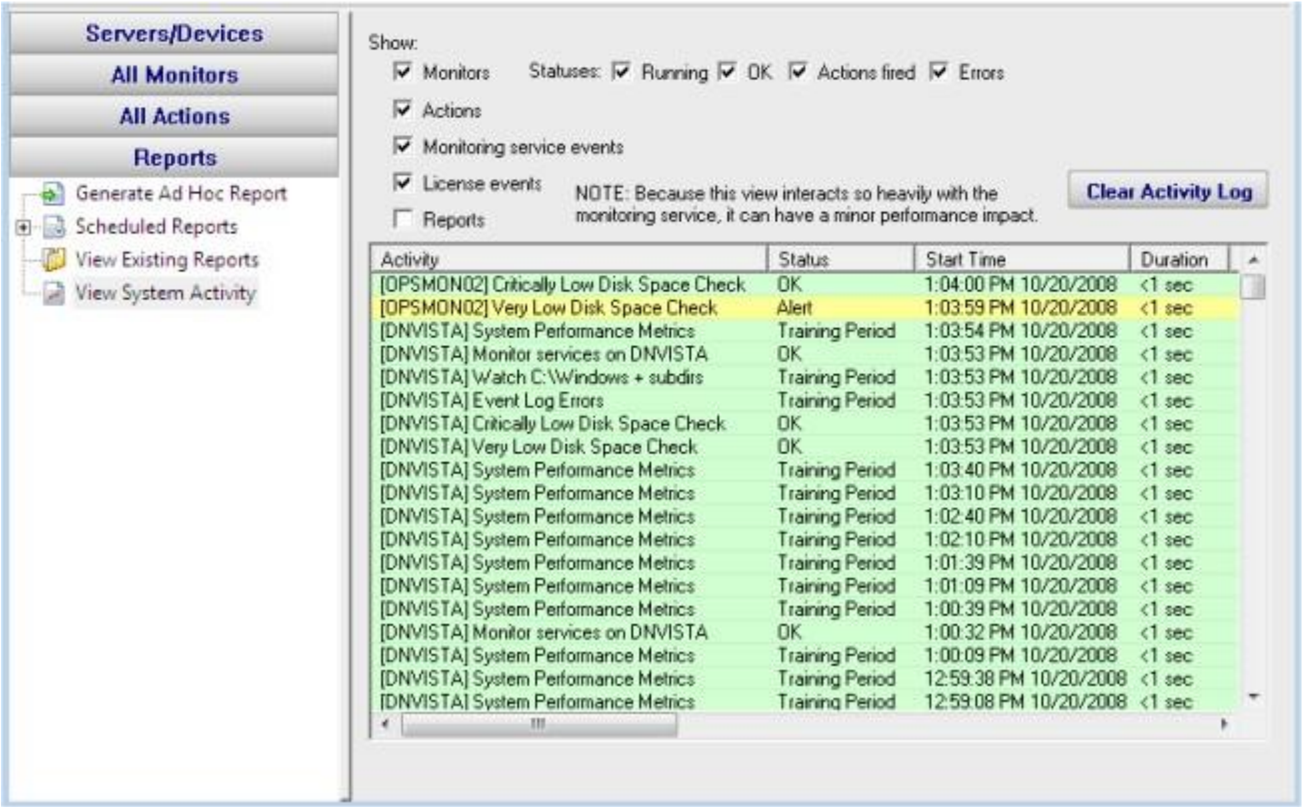
Viewing System Activity

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

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

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

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



Show:

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

☑ Actions

☑ Monitoring service events

☑ License events

□ Reports

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

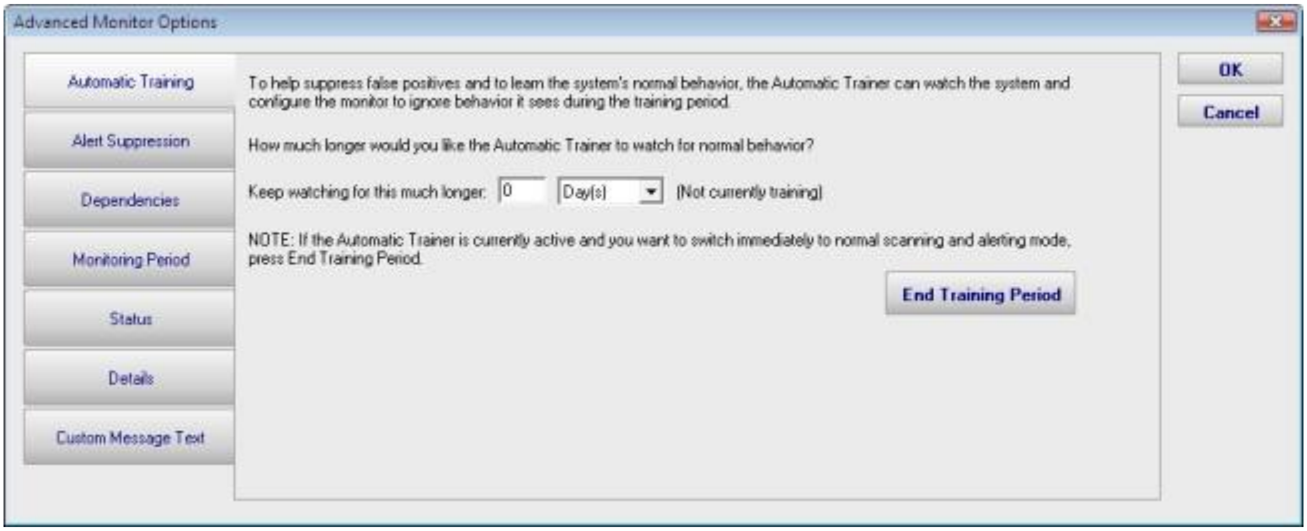
Activity	Status	Start Time	Duration
[OPSMON02] Critically Low Disk Space Check	OK	1:04:00 PM 10/20/2008	<1 sec
[OPSMON02] Very Low Disk Space Check	Alert	1:03:59 PM 10/20/2008	<1 sec
[DNVISTA] System Perfomance Metrics	Training Period	1:03:54 PM 10/20/2008	<1 sec
[DNVISTA] Monitor services on DNVISTA	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 Perfomance Metrics	Training Period	1:03:40 PM 10/20/2008	<1 sec
[DNVISTA] System Perfomance Metrics	Training Period	1:03:10 PM 10/20/2008	<1 sec
[DNVISTA] System Perfomance Metrics	Training Period	1:02:40 PM 10/20/2008	<1 sec
[DNVISTA] System Perfomance Metrics	Training Period	1:02:10 PM 10/20/2008	<1 sec
[DNVISTA] System Perfomance Metrics	Training Period	1:01:39 PM 10/20/2008	<1 sec
[DNVISTA] System Perfomance Metrics	Training Period	1:01:09 PM 10/20/2008	<1 sec
[DNVISTA] System Perfomance 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 Perfomance Metrics	Training Period	1:00:09 PM 10/20/2008	<1 sec
[DNVISTA] System Perfomance Metrics	Training Period	12:59:38 PM 10/20/2008	<1 sec
[DNVISTA] System Perfomance Metrics	Training Period	12:59:08 PM 10/20/2008	<1 sec

Additional Help Documents

Contents

Advanced Monitor Options

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



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

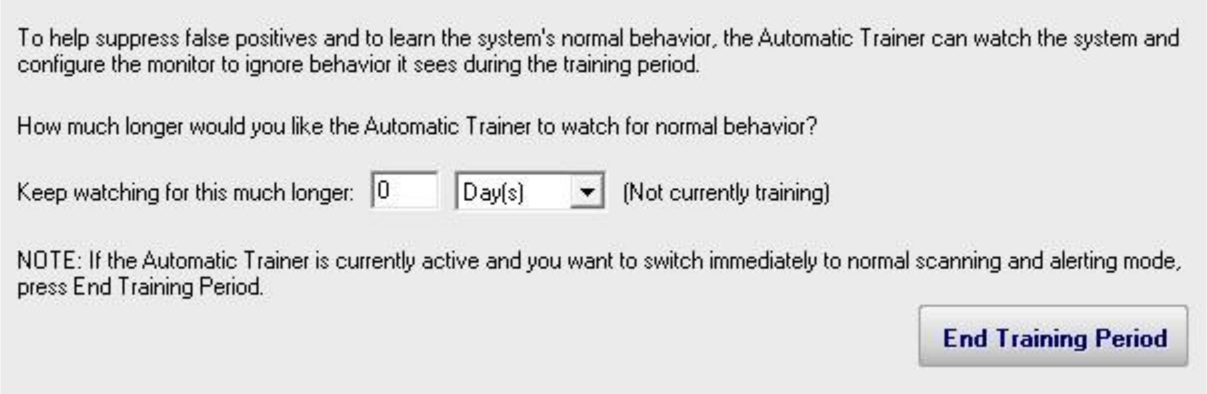
How much longer would you like the Automatic Trainer to watch for normal behavior?

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

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

Each of the different option tabs is discussed below.

Automatic Training



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

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

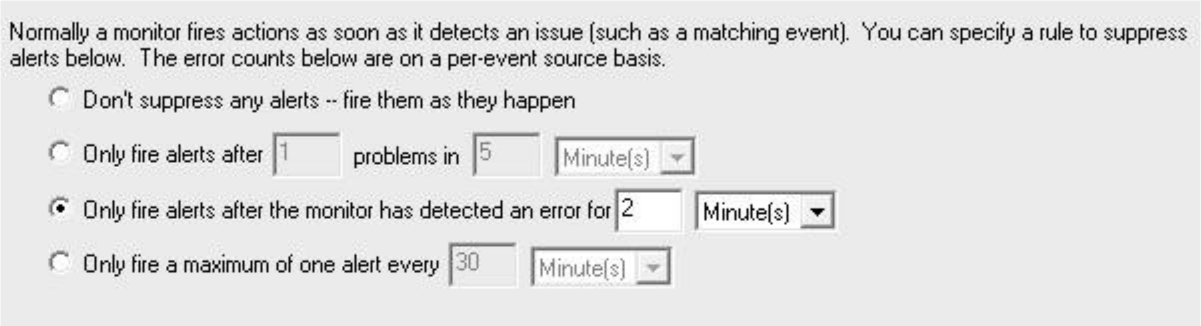
Keep watching for this much longer: 0 Day(s) (Not currently training)

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

PA Server 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 1 problems in 5 Minute(s)

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

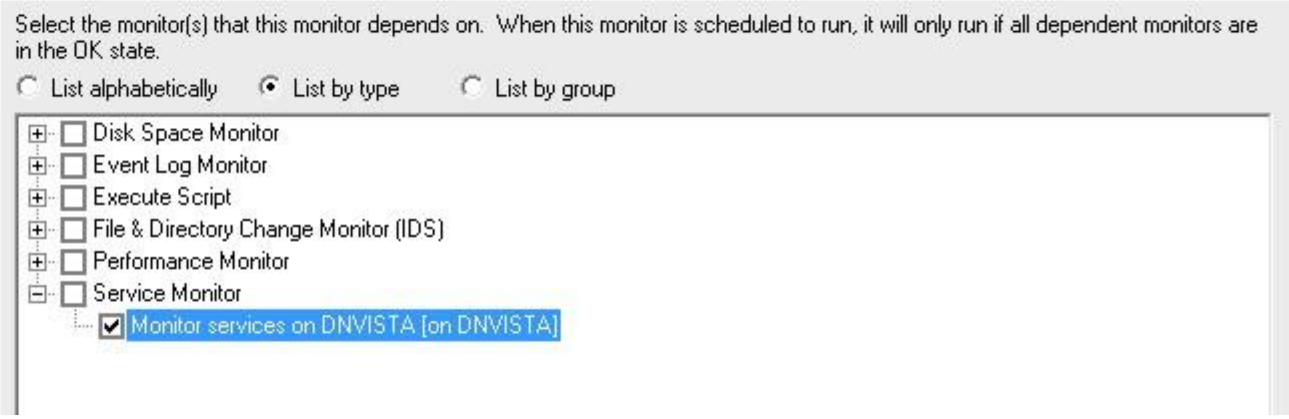
○ Only fire a maximum of one alert every 30 Minute(s)

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

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

Dependencies

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

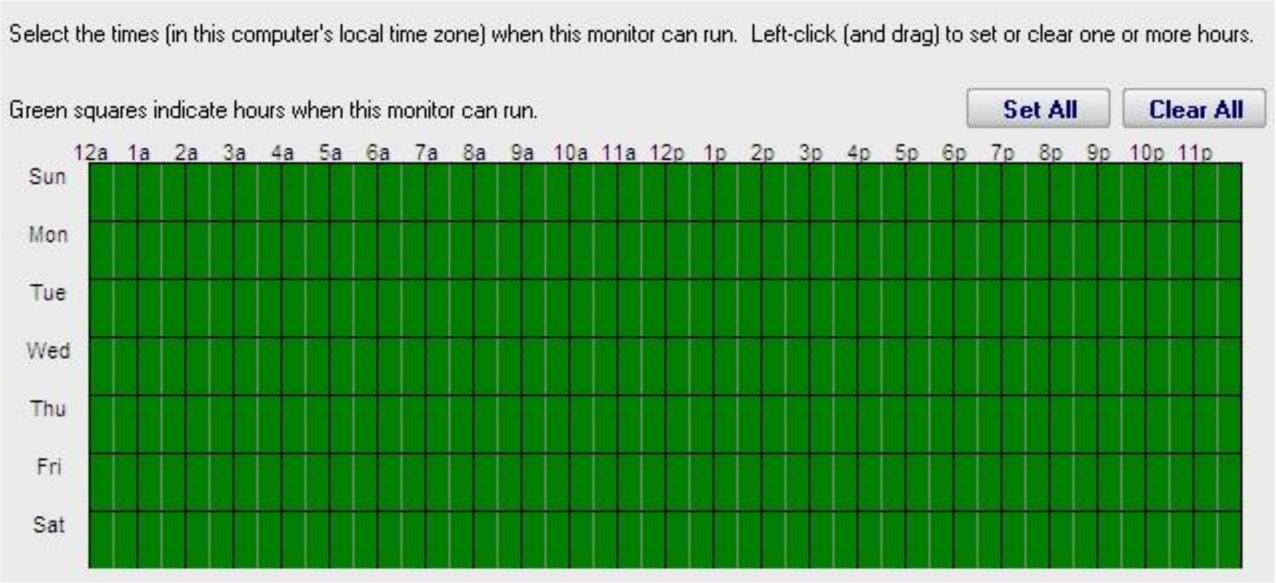


Select the monitor(s) that this monitor depends on. When this monitor is scheduled to run, it will only run if all dependent monitors are in the OK state.

○ List alphabetically ● List by type ○ List by group

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

Monitoring Period



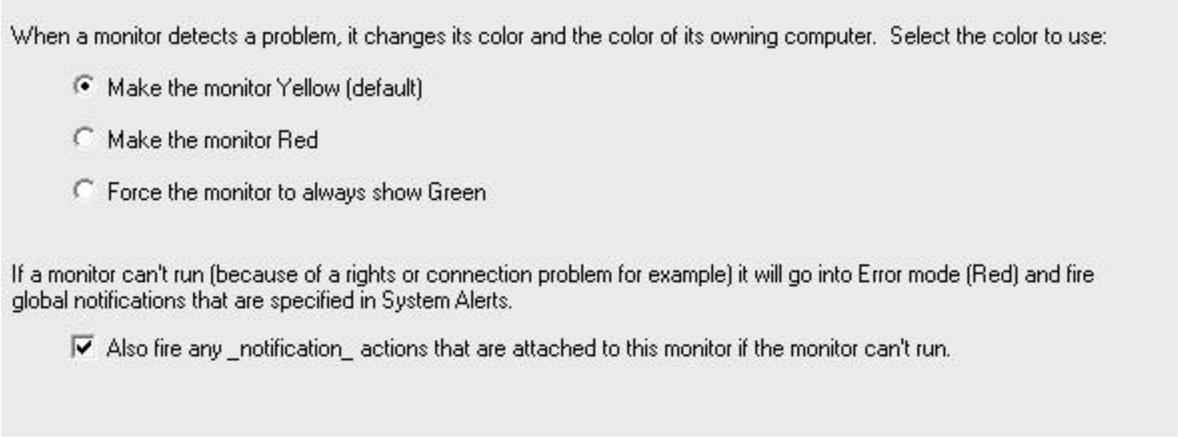
Select the times (in this computer's local time zone) when this monitor can run. Left-click (and drag) to set or clear one or more hours.

Green squares indicate hours when this monitor can run.

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

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

Status



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

● Make the monitor Yellow (default)

○ Make the monitor Red

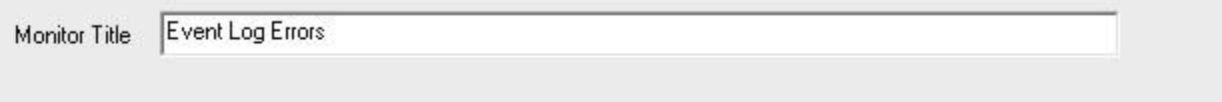
○ Force the monitor to always show Green

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

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

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

Details

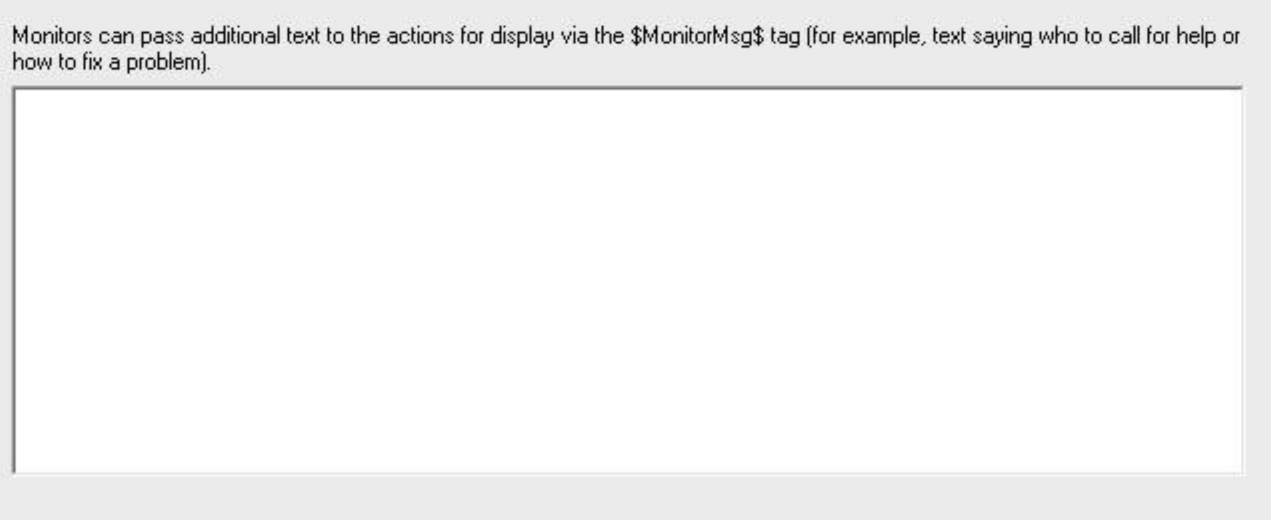


Monitor Title: Event Log Errors

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

Custom Message Text

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

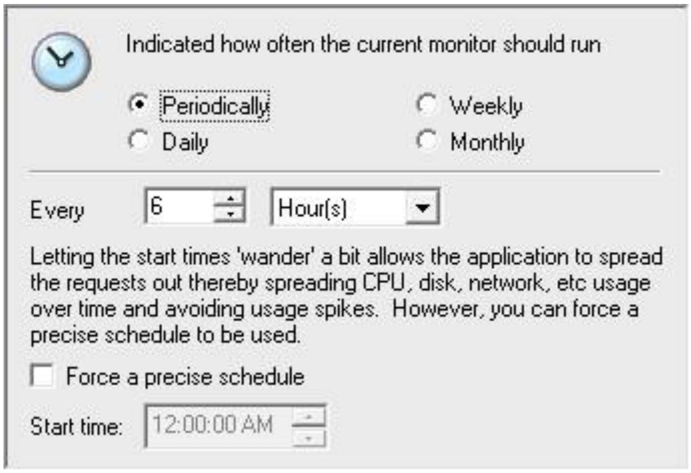


Monitors can pass additional text to the actions for display via the $MonitorMsg$ tag (for example, text saying who to call for help or how to fix a problem).

Contents

Monitor Schedule

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



Indicated how often the current monitor should run

● Periodically ○ Weekly
○ Daily ○ Monthly

Every 6 Hour(s)

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

□ Force a precise schedule

Start time: 12:00:00 AM

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

Contents

Enable WMI (Windows Management Instrumentation)

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

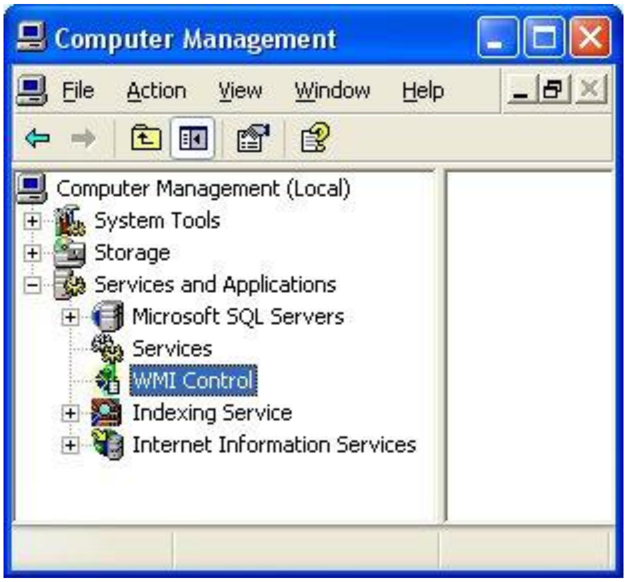
1. Enable remote WMI requests

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

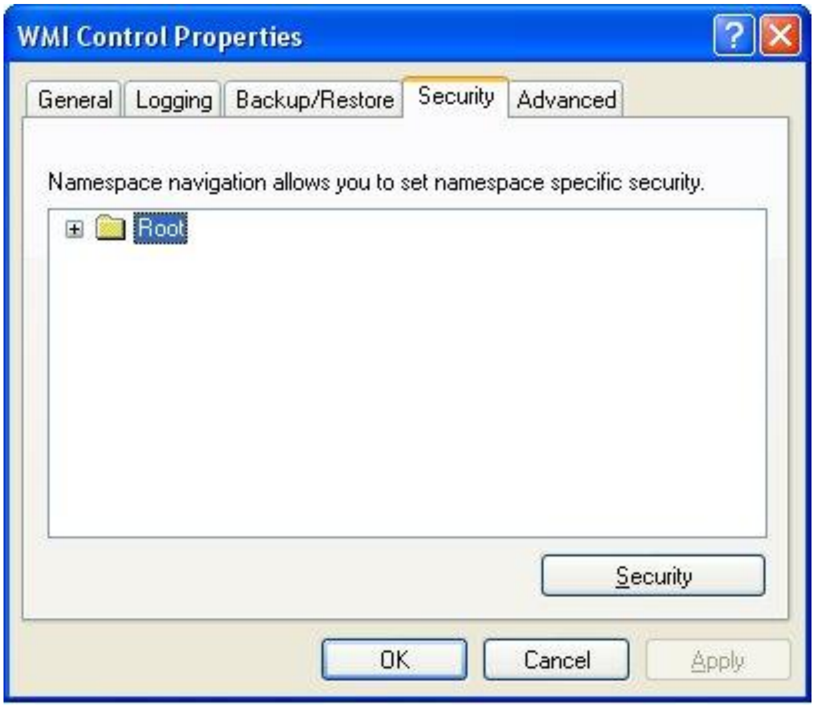
1. On the target server, go to Administrative Tools -> Computer Management.

2. Expand 'Services and Applications'

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

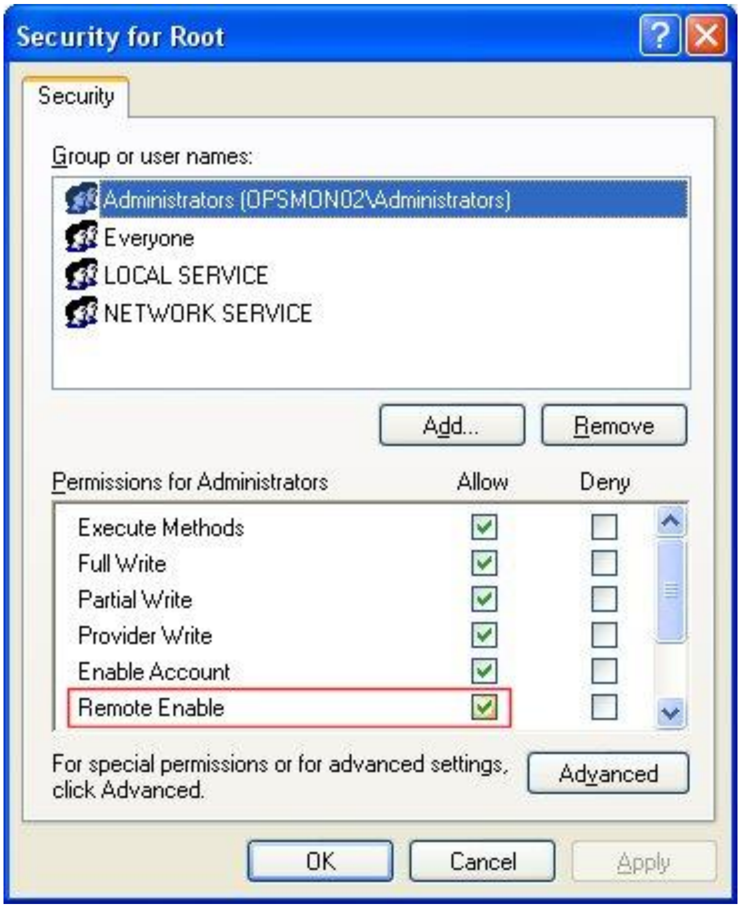


4. Select the Security tab
5. Press the Security button



Namespace navigation allows you to set namespace specific security.

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



Group or user names:

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

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

For special permissions or for advanced settings, click Advanced.

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

2. Allow WMI through Windows firewall

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

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

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

3. Enable DCOM calls on the remote machine

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

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

Further Investigation

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

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

References

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

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

Contents

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

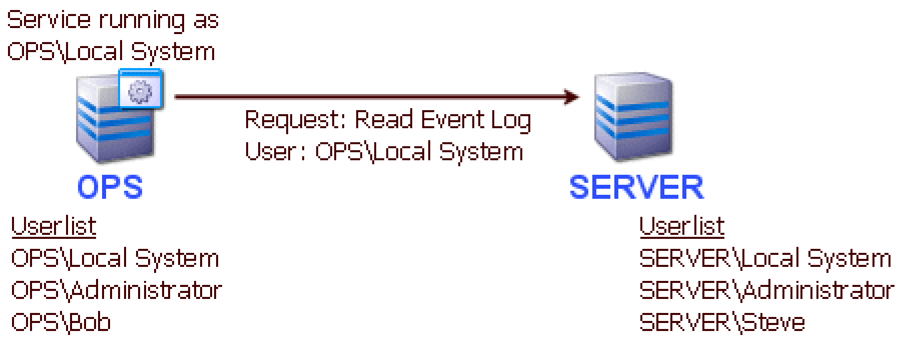
Background

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.

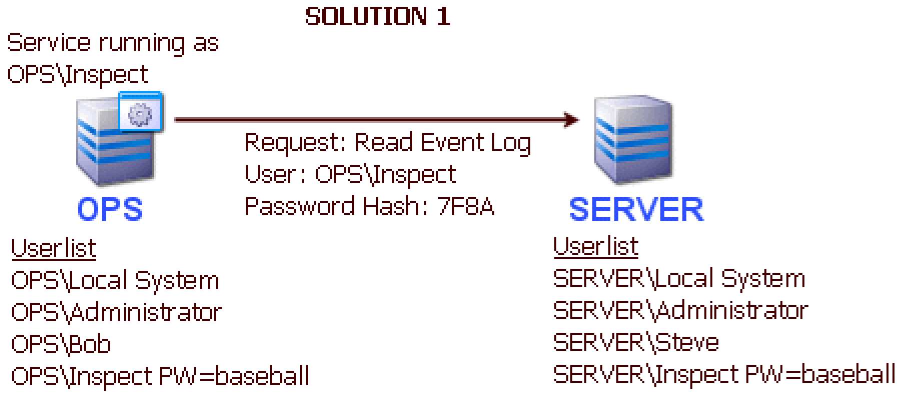
Consider the scenario where machine "OPS" is running a service (like the Power Admin monitoring service) and wants to look at the Event Log on machine "SERVER". If the service is running as Local System, the Event Log request would contain a token referring to user "OPS\Local System". The problem is, 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

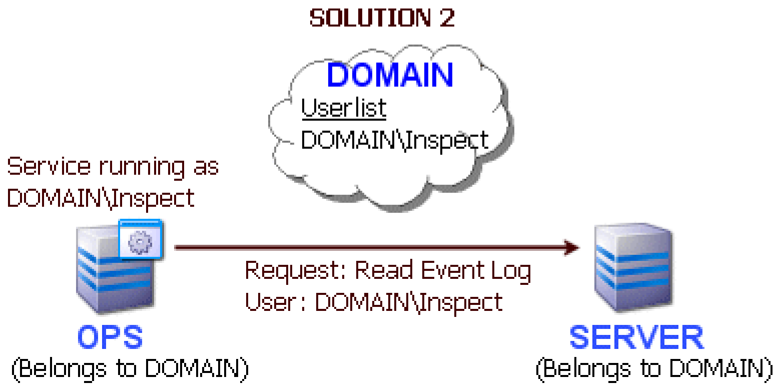
The first solution is to use synchronized username and passwords on the two machines. You can create a user account named "Inspect" on OPS with password "baseball". Then go to SERVER and create a user account named "Inspect" with password "baseball". When user "Inspect" runs the service on OPS, and sends 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 it's 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.

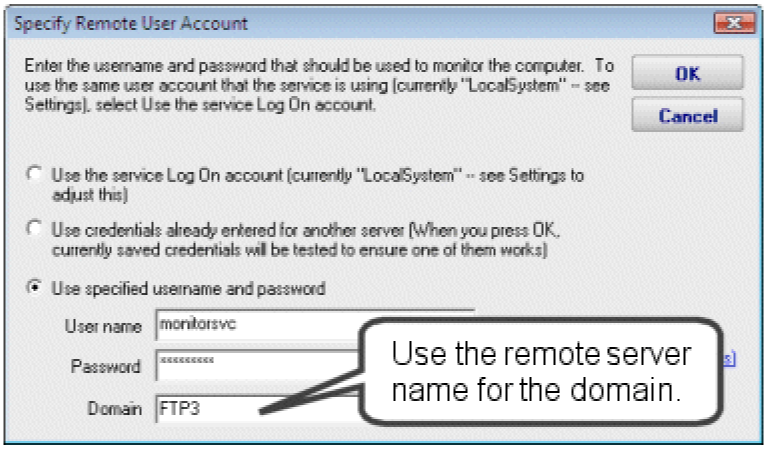
If you can't run the service as a domain account (perhaps because multiple domains are involved), you might need to specify separate credentials for each server. You can do many at once via Bulk Config, or right-click on an individual server and choose Type & Credentials -> Set Login Credentials.

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.



Specify Remote User Account

Enter the username and password that should be used to monitor the computer. To use the same user account that the service is using (currently "LocalSystem" -- see Settings), select Use the service Log On account.

○ Use the service Log On account (currently "LocalSystem" -- see Settings to adjust this)

○ Use credentials already entered for another server (When you press OK, currently saved credentials will be tested to ensure one of them works)

● Use specified username and password

User name: monitorsvc

Password: *********

Domain: FTP3

Use the remote server name for the domain.

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.

Contents

SSL Certificate Hints

Starting with version 3.7, Power Admin products (PA Server Monitor, PA Storage Monitor and PA File Sight) support using SSL-enabled HTTP (HTTPS) for serving reports, and for console to service communication. Self-signed certs are used by default to make this as convenient as possible for you the customer.

Certifying Authority

Most SSL certificates come from a well-known certifying authority like Verisign, Thawte, GeoTrust and others. These companies charge for their certificates, which enables them to do some level of check on the company requesting the certificate. Because of this, browsers recognize certificates signed by these Certificate Authorities.

Self-Signed Certs

With self-signed certs, a Certifying Authority was not involved. That means the product has to sign it's own SSL certificates, and therefore be its own Certifying Authority. Since the browser doesn't know about this new Certifying Authority, it shows warnings indicating it doesn't know whether to trust the SSL certificate or not.

To make the browser stop displaying the warnings, you have to install the new Certifying Authority certificate into the browser as a Root CA or Trusted CA. Be careful -- only install a new Certifying Authority when you know who it is because you are telling the browser to trust SSL certificates from that authority. In this case, the Power Admin product created the new Ceritfying Authority on your computer. No other computer has that Certifying Authority.

For instructions on installing a new Certifying Authority in popular browsers, choose your browser below:

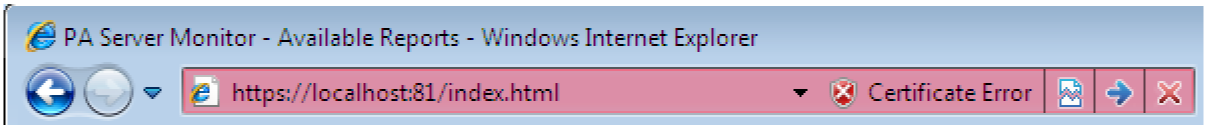
Instruction for installing in Internet Explorer

Instruction for installing in FireFox

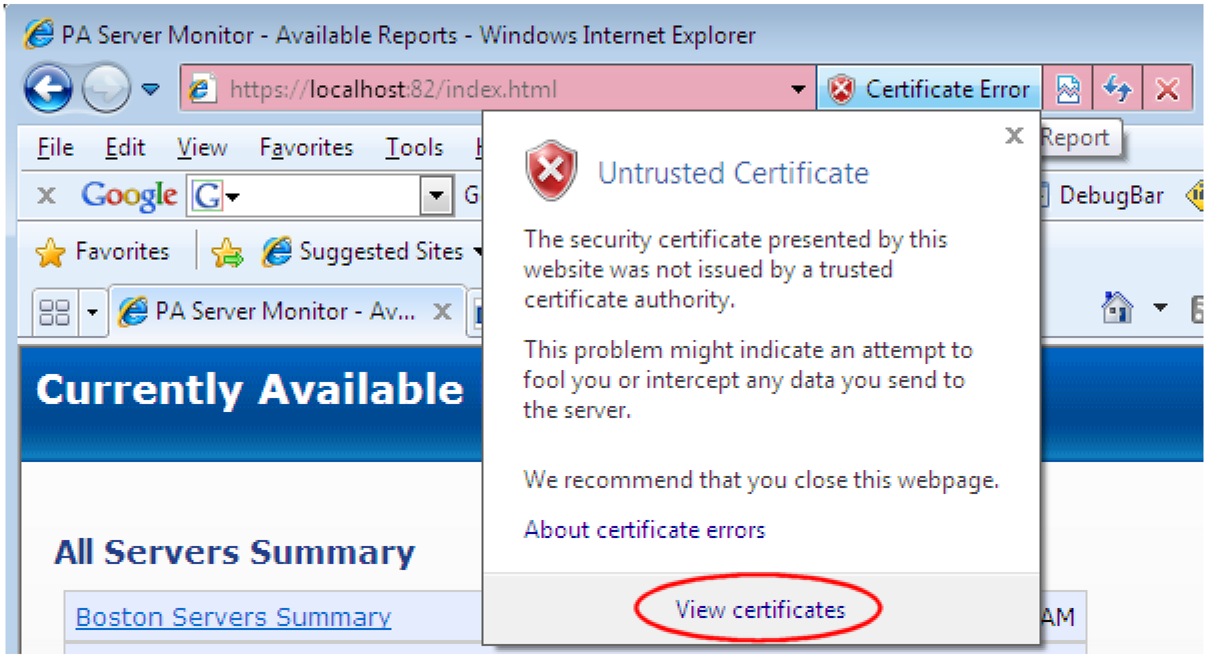
Instruction for installing in Google Chrome

Installing Certificates in Internet Explorer

When you first connect to a server using self-signed certs, Internet Explorer will display a warning. When you continue on, a certificate error is shown similar to the following:


PA Server Monitor - Available Reports - Windows Internet Explorer
https://localhost:81/index.html
Certificate Error

If you click the "Certificate Error" text in the address bar, you'll see an explanation with a "View certificates" link at the bottom. That's our goal -- to view the certificate.



Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

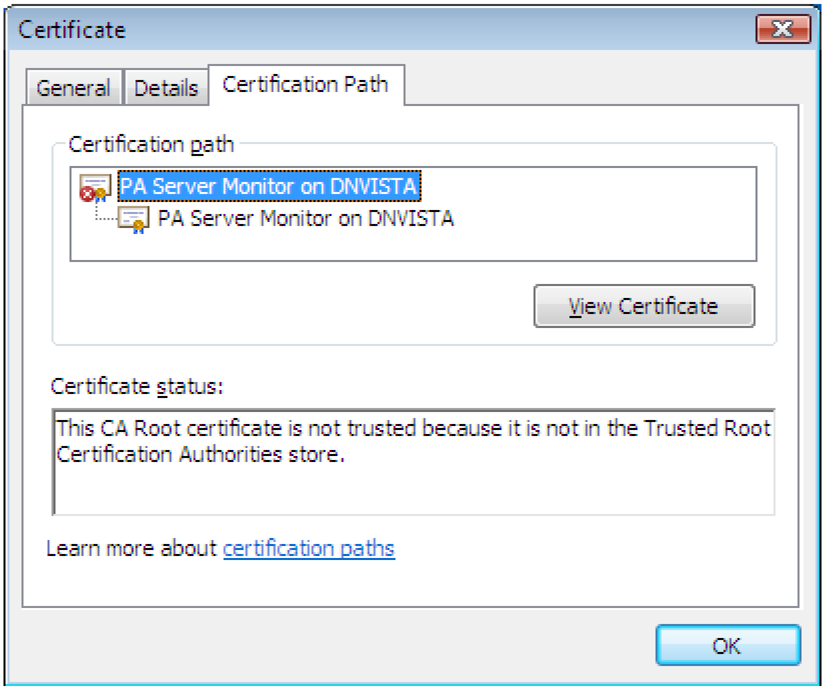
This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

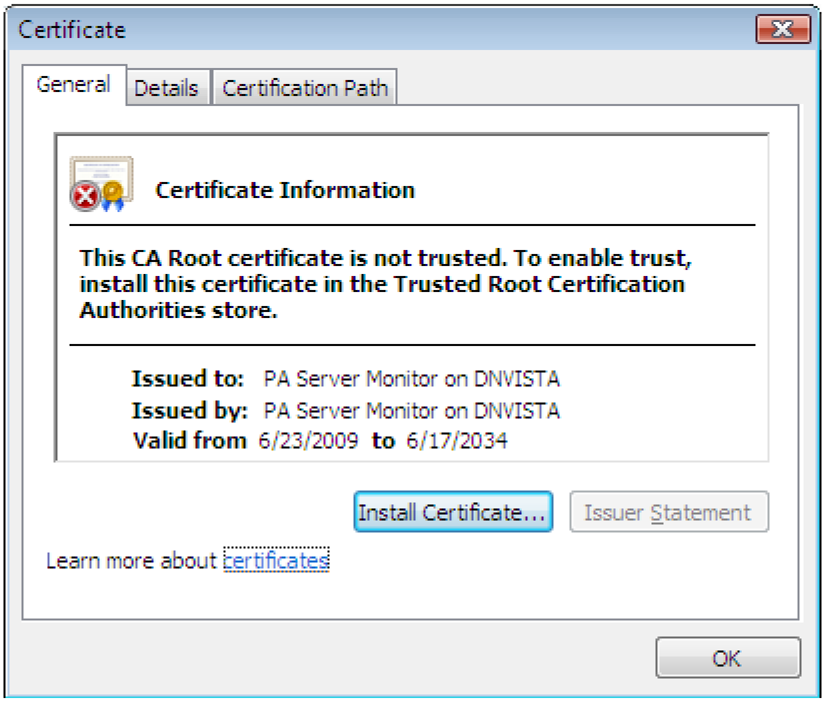
View certificates

When you click "View certificates", a dialog will display information about the SSL certificate. The Certifying Authority (also called a CA Root) certificate need to be installed. Click the "Certification Path" tab, and then select the top certificate shown. That is the CA Root. Note that the certificate names will be different on your machine than what is shown in the screenshot below.



This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

Click the "View Certificate" button near the middle of the dialog. A new dialog opens which shows the CA Root itself. This is the one we need to install. Near the bottom of the new dialog is a button to Install Certificate.



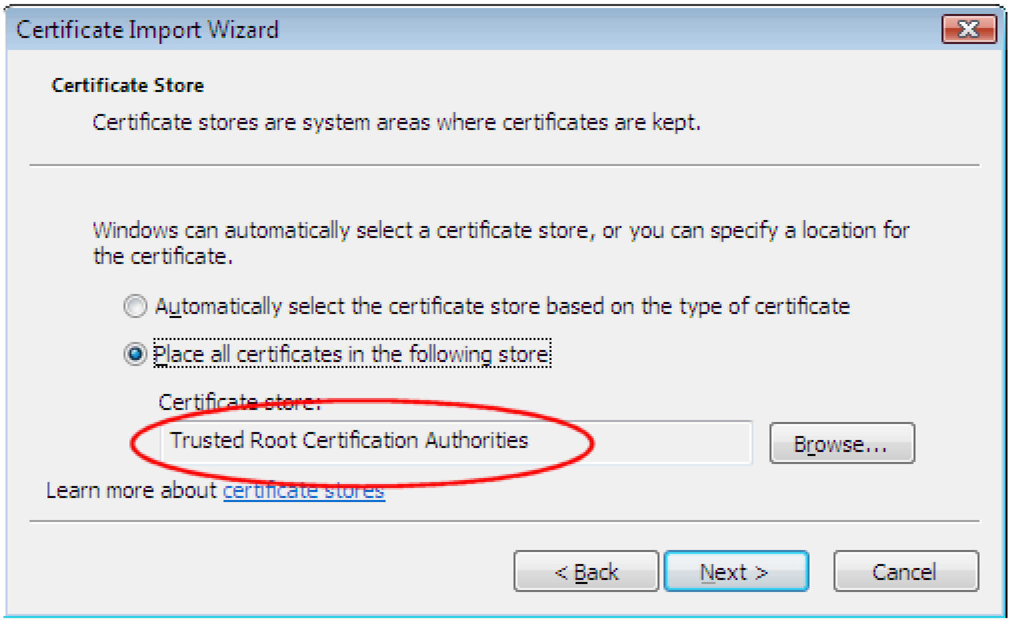
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: PA Server Monitor on DNVISTA

Issued by: PA Server Monitor on DNVISTA

Valid from 6/23/2009 **to** 6/17/2034

When you click "Install Certificate", a Certificate Import Wizard will start which will help you install the certificate. It's important to install the CA Root certificate into the "Trusted Root Certification Authorities".



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

Click Next until you get to the Finish button. Once you click Finish, a final confirmation dialog (Security Warning) is displayed to make sure you want to add the new cerificate (this dialog helps insure that a human is doing this action and not some malware).

Now that you've finished the steps above, Internet Explorer will accept the new SSL certificates without displaying an error.

SSL Domain Matching

When the SSL certificate was made, it was created using the computer's name, localhost and 127.0.0.1. In the examples above, that means we could go to https://dnvista or https://localhost or https://127.0.0.1 and the URL would match the server listed in the SSL certificate. If you will always access the web reports using one of the above server names, you can stop now.

Mismatched Address

If your server is accessible via different names or additional IP addresses (perhaps via an external and internal IP address) then the URL won't match the internal server name and the browser will give a Mismatched Address error. This is the same error that occurs if you take the SSL certificate from server and put it on a different server

One of the best ways to fix this would be to add an entry to your hosts file that maps the server's name to the IP address that you are using to access the server. That will enable the URL to match the certificate.

Contents

Adding a Security Exception

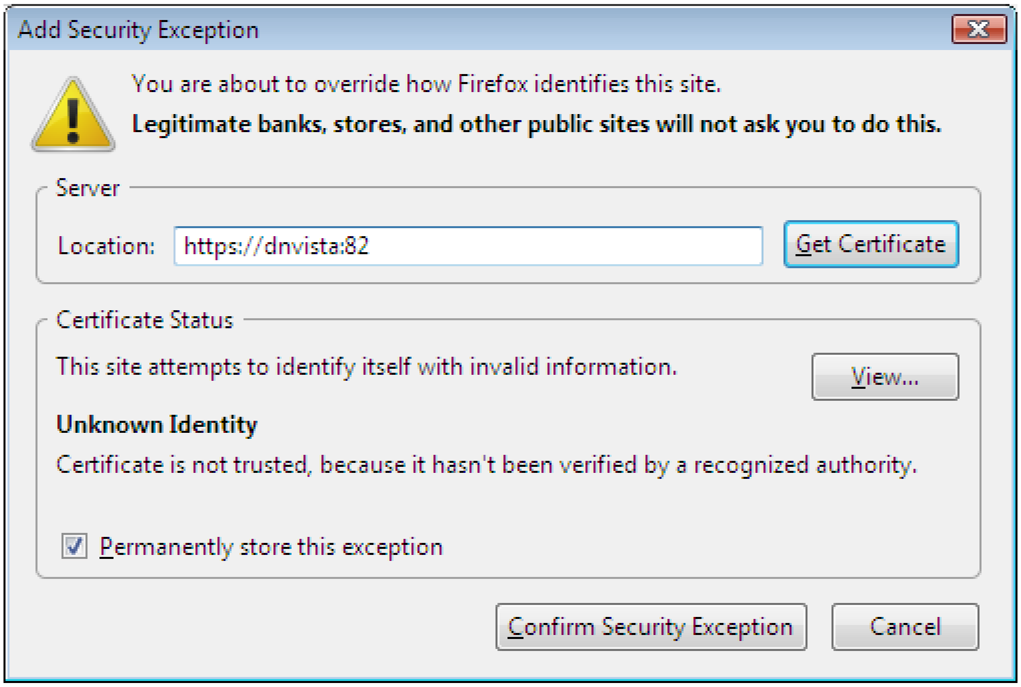
When FireFox encounters a self-signed cert, it won't load the page. The way to make it work is to add a Security Exception for that particular website.

- In FireFox, go to Tools -> Options
- Click the Advanced Tab, then the View Certificates button
- Go to the Servers tab and press the Add Exception button

The Add Security Exception dialog will be displayed. You need to enter the host and port used to access the web page you want. For example, if you want to access the following report:

https://dnvista:82/STATUS_MANY/index.html

you would enter https://dnvista:82



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Location: https://dnvista:82

This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

Once you've entered the URL, press Get Certificate. The cause of the problem (unrecognized authority) will be displayed.

Check the box near the bottom ("Permanently store this exception") and press "Confirm Security Exception".

From this point on, FireFox won't show SSL-related errors when visiting this URL.

Mismatched Address

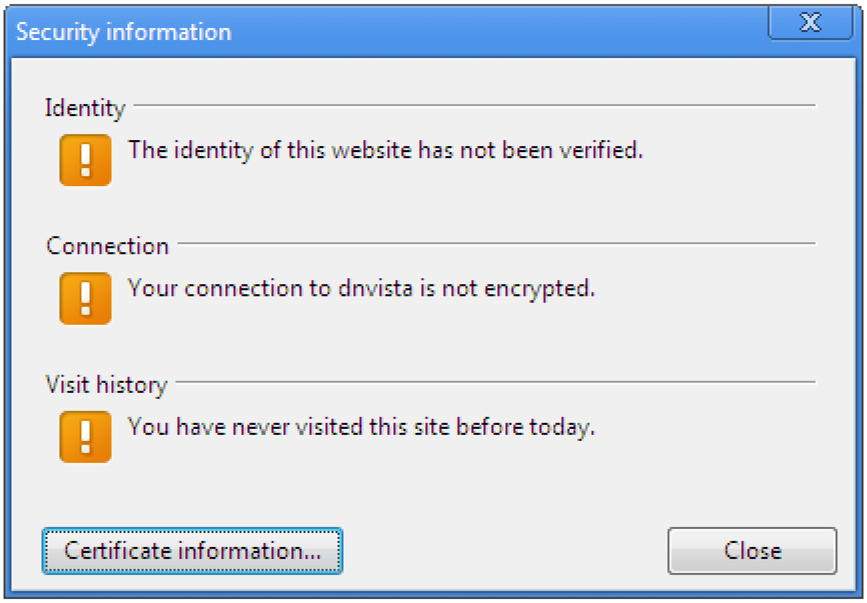
If your server is accessible via different names or additional IP addresses (perhaps via an external and internal IP address) then the URL won't match the internal server name and the browser will give a Mismatched Address error. This is the same error that occurs if you take the SSL certificate from server and put it on a different server

One fix would be to go back and add another Security Exception for additional URL. Optionally, you could also add an entry to your hosts file that maps the server's name to the IP address that you are using to access the server. That will enable the URL to match the certificate.

Contents

Installing Certificates in Google Chrome

When you first connect to a server using self-signed certs, Chrome will display a large "The site's security certificate is not trusted!" warning. In the address bar is an orange warning triangle. Clicking that triangle will display the following dialog:



Security information

Identity

The identity of this website has not been verified.

Connection

Your connection to dnvista is not encrypted.

Visit history

You have never visited this site before today.

Chrome relies on the Windows certificate store. Unfortunately, it does not (currently) give any way of installing a certificate from a URL. We recommend starting Internet Explorer and installing the Root Certificate Authority following those directions. When you're done, restart Chrome and it will recognize the SSL certificate as being properly signed.

SSL Domain Matching

When the SSL certificate was made, it was created using the computer's name, localhost and 127.0.0.1. In the example above, that means we could go to https://dnvista or https://localhost or https://127.0.0.1 and the URL would match the server listed in the SSL certificate. If you will always access the web reports using one of the above server names, you can stop now.

Mismatched Address

If your server is accessible via different names or additional IP addresses (perhaps via an external and internal IP address) then the URL may not match the internal server name and the browser will give a Mismatched Address error. This is the same error that occurs if you take the SSL certificate from server and put it on a different server

One of the easiest ways to fix this would be to add an entry to your hosts file that maps the server's name to the IP address that you are using to access the server. That will enable the URL to match the certificate.

Contents

Monitoring Remote Servers Through Firewalls

Power Admin monitoring products contain a variety of modules that monitor different server resources. In general, the server resources are accessed through one of two ways:

- Standard protocol ports
- Windows RPC

Standard Protocol Ports

Standard Protocol Ports would be those ports that are used by a protocol-specific monitor. For example, the Web Page monitor uses HTTP, and therefore (by default) port 80 to access the remote server. The SMTP server monitor uses a default port of 25, POP3 is a default of port 110, etc. These standard protocol monitors therefore use the port specified by the relevant standard.

Windows RPC

Windows-specific monitors (Event Log monitor, Disk Space monitor, Service monitor, etc) use standard Windows RPC to access the underlying resources. Windows RPC uses **TCP port 135** by default (although you can change this via tools on the Microsoft website). Because port 135 is targeted by much of the malware and worms on the Internet, we do not recommend opening that port on an Internet-facing firewall.