PA Server Monitor

Version 9.4 Ultra

Last Update: March 25, 2024

Power Admin LLC

support@poweradmin.com

www.poweradmin.com

Prepared in the USA

PA Server Monitor Documentation Table of Contents

Welcome & Install

Getting Started

Adv. Configuration

Acknowledging Alerts
: Acknowledge alerts to indicate they have been seen, are owned, and being worked on.

Adv. Monitor Options
: Many advanced options that exist on every monitor can help PA Server Monitor work the way you want it to.

Alert Reminders
: Configure reminders to get sent for previous alerts that might not have been handled yet

Automatic Config
: Automatic rules-based detection and configuration of monitors.

Automatic Fail Over
: Setup a second instance of PA Server Monitor to monitor the primary monitoring service, and take over if it fails

Command Line
: Different options that can be used to help automate PA Server Monitor.

Config Email Ack
: Acknowledge alerts by replying to an email.

Config Security
: Password protect the Console, and alert on changes that could affect monitoring.

Credential Manager
: View and change existing credentials in the Credential Manager.

Credentials: AWS
: Edit AWS settings centrally to control the credentials used when monitoring a server via the AWS (Amazon Web Services) CloudWatch API.

Credentials: ESX
: Edit ESX settings centrally to control the credentials used when monitoring a server via the VMWare ESX API.

Credentials: IPMI
: Edit IPMI settings centrally to control the credentials used when monitoring a server via IPMI.

Credentials: SNMP
: Edit SNMP settings centrally to control the credentials used when monitoring a server via SNMP.

Credentials: SSH
: Edit SSH settings centrally to control the credentials used when monitoring a server via SSH.

Credentials: Windows
: Edit Windows credentials to control the credentials used when monitoring a server via Windows RPC.

Custom Icons
: Servers/devices and groups can have custom icons manually or automatically assigned based on what the Inventory Collector monitor finds.

Custom Properties
: Set cascading iCustomer Properties on Groups, Computers/Devices and Monitors which can be used in monitor, scripts and message templates.

Customize Menus
: Customize the Operations right-click pop-up menu in the Console to add your own commands, or change or remove existing commands

Error Auditing
: Keep track of which errors have been reviewed and acknowledged. Also a great way for administrators to have an overview of any errors within their area of responsibility.

Event Deduplication
: Detects errors which are very similar or identical to existing outstanding alerts and suppresses them.

Event Escalation
: Many monitors are capable of sending escalating events. For example, low disk space alerts could first go to a first-tier Ops team. If the aren't handled in a specified time frame, they could be forwarded to a second-tier Ops team.

Expansion Variables
: Variables with details about alerts can be used to change the output of custom messages.

External API
: Send basic configuration requests to the product via an HTTPS URL.

File Locations
: Locations of files used in the product

Import & Export
: Paste a list of servers or IP address into a list and let PA Server Monitor inspect and self-configure for each server/device. Or easily copy the configuration from one configured server to one or more other servers.

Locking Configuration
: Lock monitors or actions to prevent their configuration from being changed.

Maintenance Mode
: While a computer is in maintenance mode, PA Server Monitor won't run monitors. It will turn itself back on automatically after the maintenance window expires if you manually entered maintenance mode, or it can automatically enter and leave maintenance mode on a schedule.

Mobile: Android
: PA Server Monitor for Android lets you stay up to date even if you're away

Mobile: iPhone
: PA Server Monitor for iPhone lets you stay up to date even if you're away

Monitor Schedule
: You can configure how often every single monitor runs -- put them on a custom poll cycle or let them run with the default schedule.

Monitor Templates
: Create monitors at a group level that are automatically deployed to all servers/devices within the group.

Secure Settings
: Controls various security related functions in the application

VMWare ESX
: Monitor aspects of a VMWare ESX host server.

Adv. Configuration

Monitors

Action Scheduler
: Automate common IT tasks with the Action Scheduler. It will run your defined Actions when you specify.

Active Dir. Change
: Monitor creation, deletion, and changes of the Active Directory objects.

Active Directory Login
: Monitor login and other security-related activity in Active Directory, Domain servers, and even for local logins.

All-Systems-GO
: Reports to the All-Systems-GO service which can notify you if the monitoring installation is affected in any way that would prevent its from alerting.

Bandwidth
: Monitor bandwidth, network error counts, broadcasts and other values from SNMP-based devices as well as from Windows Performance Counters.

Calculated Status
: This monitor lets you calculate its status by running a script on the statuses of other monitors.

Citrix Server
: Monitor and alert on Citrix XenApp (Presentation Server) client connect and login response times. Alert if too slow, and record times for historical charts.

Database
: The Database Monitor can watch that individual databases are up and running, keep an eye on the transaction log size, and alert if databases are added or deleted from a server.

Directory Quota
: The Directory Quota Monitor keeps track of directory sizes, and executes actions if the directory sizes are over the quota. End users (directory owners) can be notified via email with the Monitor-Directed E-mail action. Includes reports.

Disk Space
: Monitor the free disk space on server drives. You can set the warning threshold in absolute size, or percentage of disk space. Includes reports and auto-configuration.

DNS
: Monitor the results of a DNS lookup, or a reverse DNS lookup. You can specify which DNS server the request should be sent to. If an unexpected result is returned, actions are fired.

Dynamic Server List
: Dynamic Server Lists are groups of serves that meet your criteria. Once the list is known, you can define Dynamic Groups based on the list, and use that group everywhere else groups are used.

Email
: Monitor email messages in a POP3 or IMAP4 mail box for messages that contain specific text. When a match is found, alerts are fired.

Environment
: Connects to an Esensors EM01b Websensor on the LAN and monitors the current temperature, humidity and luminescence, and notifies you if the values go above thresholds that you set. Historical reports as well.

Event Log
: Checks any specified Windows Event Logs (Application, System, Security plus custom event logs) and executes actions you specify if a source you're interested in adds an event to the log.

Event Validator
: Verifies that specific events, such as backup succeeded or anti-virus pattern file updated events are in the event log. If they are missing, fire alerts.

Execute Scripts
: Execute your custom written scripts written in the Visual Basic Scripting Edition language. You can use custom or 3rd party ActiveX controls. The script determines whether to trigger actions using your own logic.

File Age
: Monitor file ages and alert if the files become too old (good for watching server queues, spool directories, etc).

File/Directory Size
: Track the size of a directory or a set of specific files within a directory. Includes reports.

File & Directory (CIFS)
: This monitor is a host-based IDS (Intrusion Detection System) that will notify you when the date, size or even content of a file changes on local files, or files on any CIFS share. File creation and deletion is also monitored. A good tool to help with configuration management as well. Auto-configuration functionality is available.

FTP Server
: The FTP Server monitor can login to FTP servers (including SSL-enabled FTP servers) to make sure they are up and running.

Hardware
: Monitor the hardware status of ESX, Dell DRAC/iDRAC, HP iLO, IBM RAS and other IPMI-based devices.

Inventory Alerter
: Alerts on inventory data collected by the Inventory Collector monitor.

Inventory Collector
: Collects inventory information (hardware information, pending Windows Update, anti-virus status, etc) from a variety of sources including WMI, SNMP and an optional System Details application.

Log File
: Periodically checks the content of one or more log files for target text. Target text and be a simple text phrase or a regular expression.

Mail Server
: Monitor your mail servers (POP3, IMAP & SMTP) and validate that they are running and accepting incoming connections.

Network Scan
: The Network Scan monitor will periodically perform a ping scan of a specified IP address range looking for new devices that are not already being monitored. They can automatically get added to the system and configured for monitoring.

Performance
: The entire breadth of the system Performance Counters can be monitored allowing you to set actionable thresholds on CPU usage, memory usage, NIC traffic, etc. Performance counter values are stored in a database so you can view historical counter reports and understand trends.

Ping
: Tests a connection/device by periodically testing it with a ping. No response or too great a delay triggers actions. Ping response times are recorded in a database for reporting and graphing.

Plugin
: Runs an executable or external script launched via Windows, or via SSH, and parses the output to determine whether alerts should be fired. Plugins can also return values that are recorded to the database and can be charted.

Process
: Monitor that specified processes are running on Windows or Linux servers.

RD Gateway
: Monitor Remote Desktop Gateways and show currently connected sessions on a dashboard

Server Temperature
: Using the free SpeedFan utility, the Server Temperature Monitor will watch the values from the various temperature probes on your server and notify you if they go above the thresholds you set.

Service
: Watches system services and runs customized actions (including restarting the service) if they are not running.

SNMP
: Connects to local or remote SNMP agents and queries SNMP object values. Custom MIBs are supported. The value is compared to a threshold that you set and actions are fired as specified. SNMP values are also recorded to a local database for reporting purposes. Supports SNMP v1, v2c and v3.

SNMP Trap
: Receives SNMP Traps and optionally filters on trap text before running attached actions.

Syslog
: Receives Syslog log events and optionally filters on incoming log text before running attached actions.

Task Scheduler
: Monitors the enable/disable status and the Last Run Result value of Windows Task Scheduler tasks.

TCP Port
: Makes a TCP connection on a specified port. Optionally send command text and check response text. Timing data is recorded for reporting purposes.

Web Page
: Monitor one or many pages on a web site. Checks for positive cases (text that must be found), negative cases (alerts if error text found) and if the page has changed at all. Response times are checked and recorded, and reports can be generated to understand trends.

Actions

Action List
: Groups of actions for common notifications, group notifications, etc.

Call URL
: This action will call a URL you specify, optionally posting information about the current alert. This makes it easy to connect to a helpdesk/ticketing system.

Desktop Notifier
: Delivers alerts to Windows desktops via a pop-up message box or a slider in the lower right corner of the screen.

Dial-Up Connection
: Connects or disconnects a Windows Dial-up Connection. Typically this is for servers that are not on the Internet, but need to connect to send alerts.

E-mail Alert
: Sends SMTP email messages to mail boxes, cell phones, mobile devices, etc. The E-mail action has *Alert Digests* which are a powerful/friendly feature that combines multiple alerts that happen within a short time into a single email notification. This can be very helpful when something goes *really* wrong. You can easily specify when messages should be sent or suppressed.

Execute Script
: Similar to the Execute Script monitor, this Action lets you extend the list of available actions via your own script written in VBScript. Many variables from the source monitor are also available for creating rich, situation-specific responses.

Message Box
: A simple message box that displays monitor findings. These message boxes are smart: if there are many pending alerts you can easily dismiss them all at once.

Directed-Email
: The monitor which detects a problem specifies the email address to use for each alert. This is very useful when sending reminders and alerts to end users such as with the User Quota Monitor and the Directory Quota Monitor.

Network Message
: Sends a message box containing the critical monitor details to every place that you are logged in.

Pager Alert via SNPP
: Send monitor results to pagers via standard Simple Network Paging Protocol (SNPP). You can easily specify when messages should be sent or suppressed, and the content of the message.

PagerDuty Integration
: Send alerts directly to your PagerDuty account and track them using the full power of the PagerDuty platform.

Phone Dialer
: Dials a modem/phone and optionally sends DTMF commands or other commands (to send SMS messages for example). This is typically used by a disconnected server to send an alert over a normal phone line (where the CallerID identifies the server)

Play Sound
: Audible alert when monitors detect a problem with the server.

Reboot Server
: Reboots the server if a monitor has detected a critical system failure.

Run Report
: When this action is triggered, it will run the specified Scheduled Report including sending any emails or saving PDF or CSV files that report requires.

SMS Text Message
: Send SMS text messages to your mobile device via your service providers SMS Internet gateway (SMPP server). You can control which information gets sent, as well as when messages are allowed.

Server Maintenance
: Set or remove the Immediate Maintenance period for a server or servers

SNMP Trap
: Sends an SNMP Trap with details from the monitor firing the action

Start Application
: Starts a specified application when the monitor triggers actions

Start Service
: Sends control messages to the Windows Service Control Manager to start, stop or restart a specified service.

Syslog
: Sends monitor alerts to a Syslog server on the network

Write to Event Log
: Writes monitor details to the Windows Event Log.

Write to Log File
: Log the findings of any triggered monitor to a file. Separate files can be created for each day, week, month, etc.

Reports

Ad Hoc Reports
: Generate reports on the fly to quickly see graphical trends

Branding Reports
: Easily brand reports with your company logo at the top

Group Settings
: Group summary reports can be specified and controlled in a per-group way. In addition, group reports can be automatically emailed to anyone that needs to keep track of the servers.

Inventory
: Collect and report on hardware and system inventory of the monitored servers and devices.

Multi-Port Chart
: Combines and shows multiple bandwidth charts on an efficient set of one or more graphs.

Password Protection
: Password protect web reports in PA Server Monitor

Satellite Status
: Quickly see the current status of an individual Satellite Monitoring Service.

Satellite Summaries
: Two reports that let you see the status of all of the Satellites at once.

Scheduled Reports
: You can create scheduled reports which will get created when you want them, and optionally email the report to a list of recipients. Scheduled report URLs are stable so you can add them to your Favorites list to quickly and easily see the latest results.

Server Status
: Easily see at a glance the state of your server along with system statistics

System Activity Log
: Quickly see which monitors are running, how long they are taking, which actions are being fired and more.

Standard Report Tabs
: View the tabs and information that is common among most report types.

Uptime Reports
: Uptime Reports can be run on many different types of data, with summarization at the raw, hourly, daily, weekly and monthly level.

Grp: All Errors Report
: The All Errors report show all recent errors on all monitors on all servers/devices within a group. This is a good place to quickly get a detailed

view of any problems happening on the network.

Grp: All Servers Report
: This report shows all of your servers in a group in a single page. Each server is a small box that is color coded according to the status of the monitors on that server.

Grp: Custom Group
: Create custom reports at a group level to show custom HTML, charts, and other status values for the contained servers.

Grp: Group Overview
: A compact report that shows high-level server health with detailed monitor types in a column layout.

Grp: Group Summary
: See a one line status indicator per server to see at a glance how the servers in your data center are doing. Per-group status reports are also supported.

Grp: Network Map
: View all of the servers/devices within a group in a single report, grouping all computers and showing their status.

Grp: Status Map
: See a graphical map that contains status indicators that show you at a glance how servers in different geographic regions are doing.

Sys: Config Audit
: This report shows you what your current configuration is with your Groups, Servers, Monitors, and Actions.

Sys: Conn. Sessions
: See all sessions (Console, Satellite, mobile apps) currently connected to the Central Service.

Sys: Error Audit
: Powerful report to look at current and past alert conditions that have been detected by the system.

Sys: Monitor Scope
: Displays a summary of what is being monitored on a per-group basis. This would be appropriate to show stake holders to indicate the level of monitoring work being done.

Sys: Monitor Status
: A quick table-based overview of current monitor statuses. You can specify a specific monitor type, only monitors in error, etc.

Sys: Statistics
: View system statistics such as HTTPS connections and data transferred, numbers of monitors and connected Satellites, etc.

Sys: System Audit
: Find out about activities within the monitoring system, such as alert emails sent, user logins, Satellite disconnects, etc.

Sys: User Permissions
: This report will display all users defined in the system, what they have access to, and their permissions.

Remote Sites

Remote Monitoring
: Monitoring remote servers and devices with PA Server Monitor

Install Prerequisites
: Pre-requisites for installing a remote Console or Agent

Install Satellites
: Installing a monitoring agent at a remote location

Configure Satellites
: Configuring a monitoring agent at a remote location

Satellite Operations
: Operations on a Satellite Monitoring Service

Remote Support

SNAP Tunnels
: Safely send data to remote networks using SNAP Tunnels

Remote Desktop
: Securely connect to Remote Desktop even through firewalls with PA Server Monitor

Remote Users

Install Consoles
: Installing a Console GUI

Remote Access Users
: Managing remote user access

Filter User Access
: Control which users can see which groups and servers

HOWTO

Ack and Silence Alerts
: How to acknowledge alerts such that they stop coming for known problems.

Add Licenses
: How to add licenses.

Alternate Sat Upgrade
: Discover how to make Satellite upgrades download the installer file from an alternate location

Audit Logons
: Information on auditing Windows account logon and logon failures.

Deploy Satellites
: Information on deploying Satellites remotely.

Disable Remote UAC
: Steps to disable remote UAC so remote administrator rights work.

Embed Child Reports
: Steps to embed child Custom Reports within parent Custom Reports

Extract Data
: Extract data from the databases for use in your own systems

Group Devices
: How to dynamically group servers and devices based on arbitrary device selection

Ignore Google Update
: How to ignore the changing Google Update services

Integration
: How to integrate with other enterprise systems and usage scenarios

Monitor ASP.NET
: How to monitor ASP.NET Counters

Monitor Backups
: How to monitor backup software

Monitor Databases

Techniques for monitoring databases

Monitor Exchange
How to monitor Microsoft Exchange server

Monitor IIS
How to monitor Internet Information Services (IIS)

Monitor MySQL
How to monitor MySQL

Monitor RADIUS
How to monitor RADIUS servers

Monitor SQL Server
How to monitor SQL Server

Monitor SSL Certs
How to monitor SSL certificate expiration

Monitor via SNMP
How to monitor devices via SNMP

Monitor Voice SIP
How to monitor voice SIP

Monitor Win. Firewall
How to monitor if Windows Firewall is completely on

Office365 and OAuth
Authenticating to Office365 with OAuth 2.0

Prepare for Imaging
How to prepare a Satellite installation for disk imaging and duplication

Predict Full Disks
How to predict when the disk will be full.

Shrink Databases
How to shrink the embedded database files in the Databases folder

Slack Integration
How to integrate with Slack by sending alerts to Slack channels.

Uptime Summary
Learn how to generate an uptime report showing the summarized uptime for a number of servers on the same report.

Use Other SSL Cert
Explains how to use your own SSL certificate in place of the default.

Using Dependencies
Explains how to add Dependencies to monitors and templates.

Product Overview for PA Server Monitor

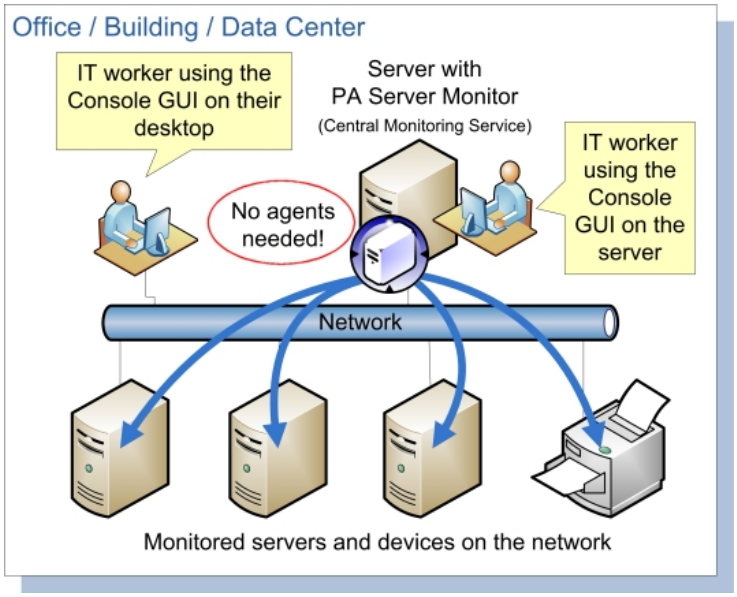
Thank you for choosing PA Server Monitor. The following documentation offers help in installing, configuring and using PA Server Monitor. These topics are also shown in the help menu at the left of the screen.

If you are looking for something specific, try the Search box at the top of the page.

Product Architecture and Layout

Typical Installation (Main Install)

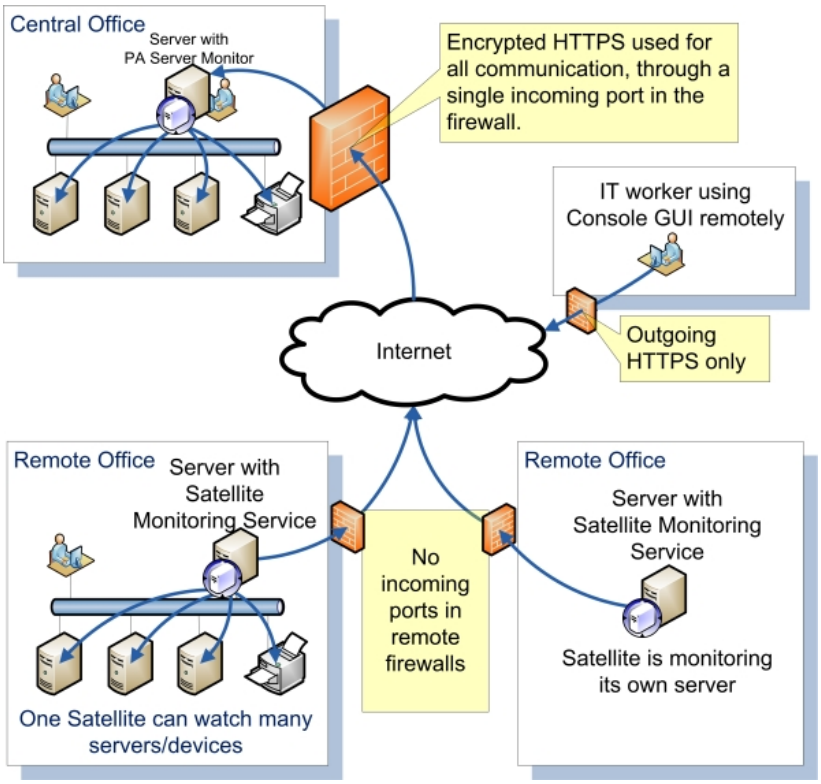
Every installation has a central monitoring service installed on a Windows Server or Workstation. This monitoring service can monitor computers and devices (including itself) on the local network.



The first installation will also include a Console GUI application for working with and configuring the central monitoring service.

Remote Capabilities

In addition to monitoring servers and devices on the local network, Ultra editions of PA Server Monitor can also monitor remote servers and devices corporate firewalls, and across the Internet without needing a VPN. This is accomplished by installing a Satellite Monitoring Service on a single server or workstation at the remote site. The Satellite will then monitor itself (the computer it is installed on) and/or other servers and devices on the local network at the remote site. Alerts and monitoring data will be sent back to the Central Monitoring Service via SSL-encrypted HTTP.

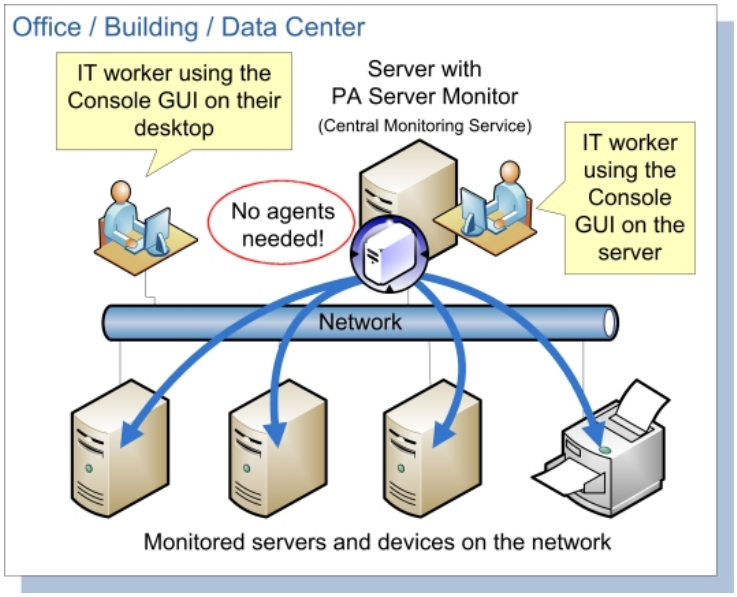


Installation Help

The first step to using PA Server Monitor is to install the Central Monitoring Service.

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 is composed of two parts: a graphical user interface that called the Console, and a background process called the Central Monitoring Service. You see the Console when you launch PA Server Monitor from the desktop. The Central Monitoring Service is invisible and has no user interface of its own.

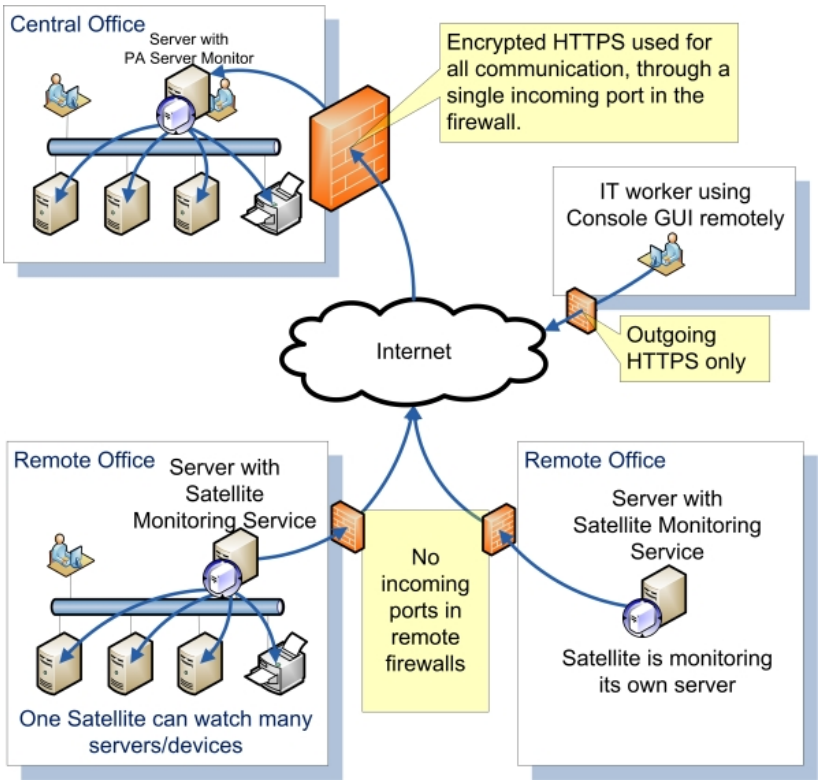
Central Monitoring Service

The Central Monitoring Service is the part of the product that performs the monitoring of the local network. It is the hub that Remote Consoles and Satellite Monitoring Services connect to. The service is set up to run automatically when Windows starts. The Console does not need to be running in order for monitoring to take place.

Satellite Monitoring Service

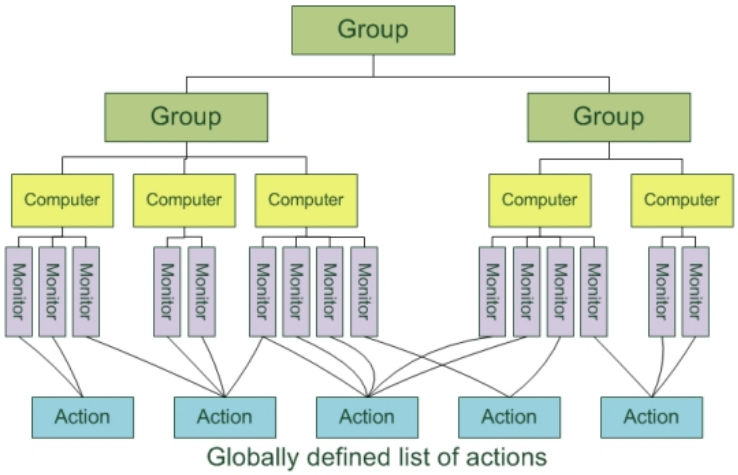
The Satellite Monitoring Service (or just Satellite for short) is an optional additional monitoring engine. It can run monitors just like the Central Monitoring Service. Satellites are typically installed where the Central Monitoring Service doesn't have access (on the other side of a firewall in a corporate environment, or at a remote location across the Internet.

NOTE: The Satellite Monitoring Service is only available in Ultra product editions.



Product Terminology

PA Server Monitor is based on the concepts of Groups, Computers, Monitors, Actions and Reports. These run on the Central Monitoring Service and/or a Satellite Monitoring Service.



Group

Groups hold computers and optionally other groups. They are for your use to organize the computers that you monitor. You can drag and drop computers and groups into groups using the Console.

Adding new computers consists of right-clicking on a Group and choosing Add New.., or using Smart Config.

Group status reports show the overall status of computers within the group.

Computer

Computers represent a server or device on the network -- something that has an IP address. A Computer specified which credentials should be used when monitoring the device, whether it is running Windows or not and other settings. Monitors are created and attached to computers.

Server status reports are generated automatically and show the overall status of the server/device.

Monitor

A Monitor periodically checks a computer resource and optionally compares the measurement to a threshold value that you set. Most monitors also write the measurement to a database so live and historical reports can be run.

When a measurement is outside the threshold (low disk space for example), or an event happens that you have indicated interest in (a file is accessed), Actions are fired.

Monitors are defined to check the computer that they are attached to. If you want to monitor a different server/device, create that new server/device (Computer), and create a new monitor to watch it. Multiple monitors of the same type can optionally be created for the same computer.

If you have remote computers being monitored by a Satellite Monitoring Service, configuring monitors for those remote servers will be as easy as if they were on the local LAN.

Action

An Action is run in response to monitor findings. Examples of Actions are sending e-mail, execution of a script, or writing text to a log file.

Actions are defined once, and can be referenced by many monitors in the system. Multiple actions of the same type can also be created (ie different e-mail actions to notify different people).

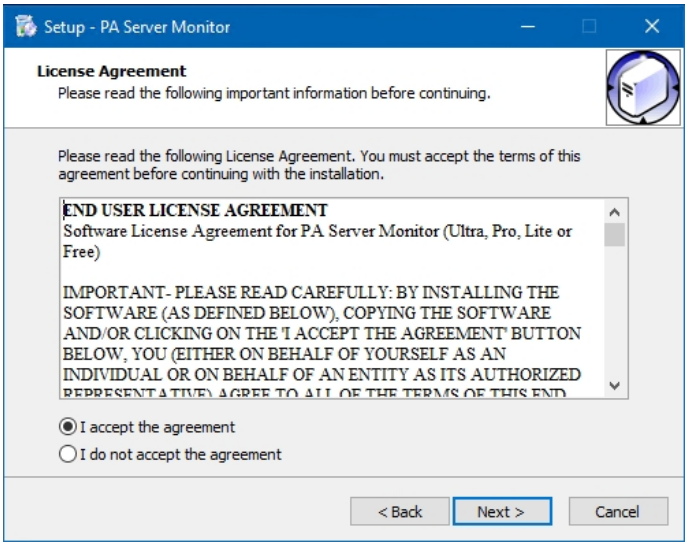
Reports

Data from the databases is shown via reports. There are pre-defined status reports for servers, and summaries for groups of servers. In addition, you can create ad hoc reports to view historical data. If a report is used on a regular basis, you can create a Scheduled Report.

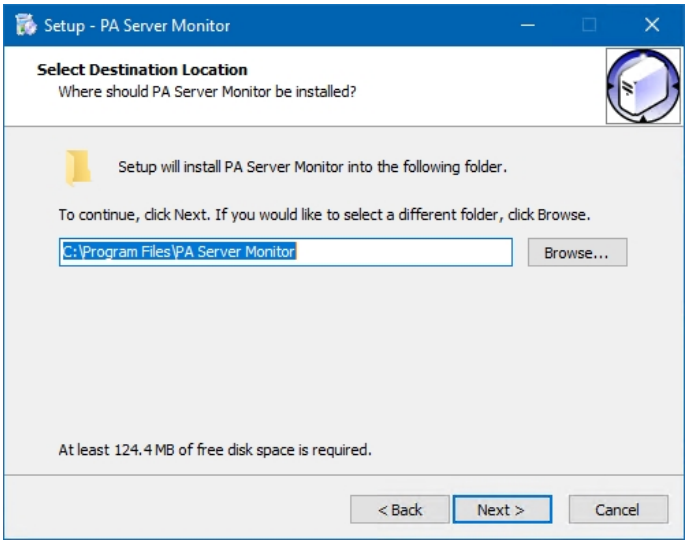
Installing the Central Monitoring Service

To install the Central Monitoring Service

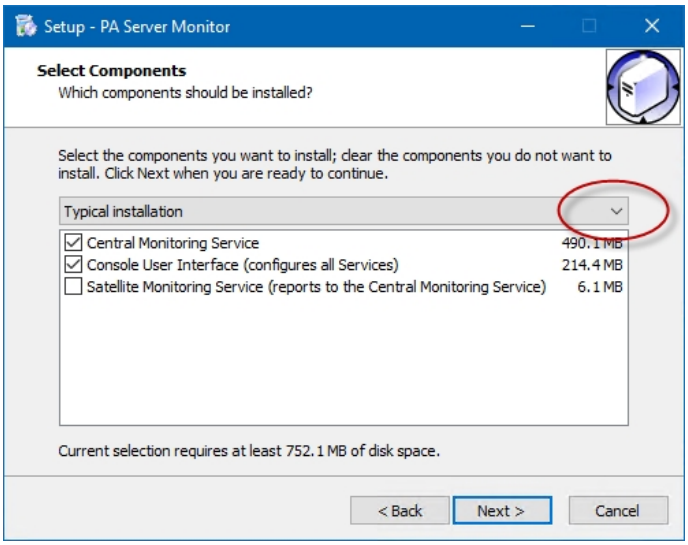
1. Run the PA Server Monitor setup program. The License Agreement page appears.
   Note: If this is an update from a previous version, the installation stops the existing service.



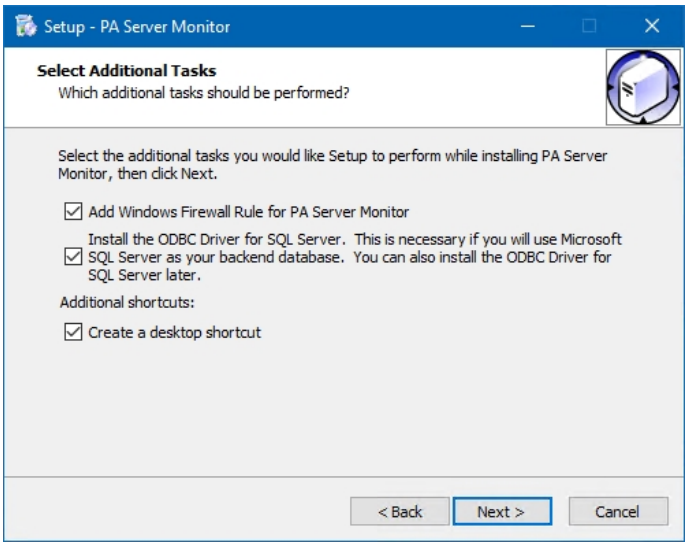
2. Select the **I accept the agreement** option, and then click **Next**. The Select Destination Location page appears.



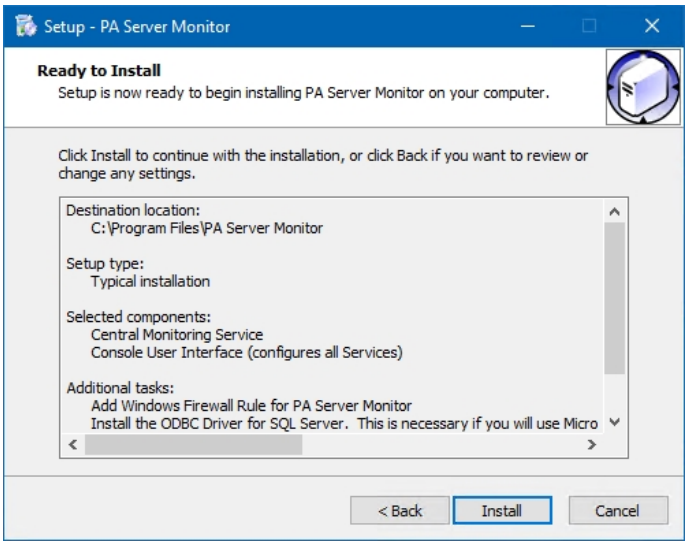
3. Do one of the following:
   - Accept the default folder path.
   - Enter a new folder path in the box. You can click **Browse** to display a standard Windows browse window, and then navigate to your destination folder.
4. Click **Next**. The Select Components page appears.



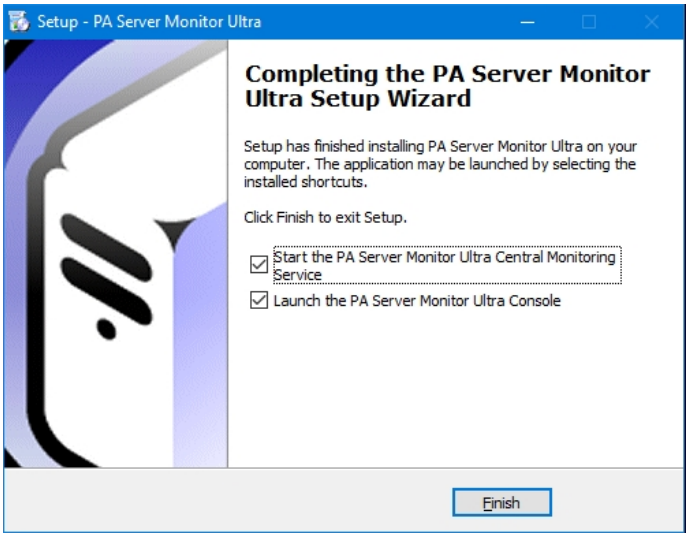
5. Accept the defaults for a typical installation. You can select the components individually, or you can click the **arrow**, and then select an installation from the list. For a first installation, choose the default "Typical installation" with a monitoring service and console.
6. Click **Next**. The Select Additional Tasks page appears.



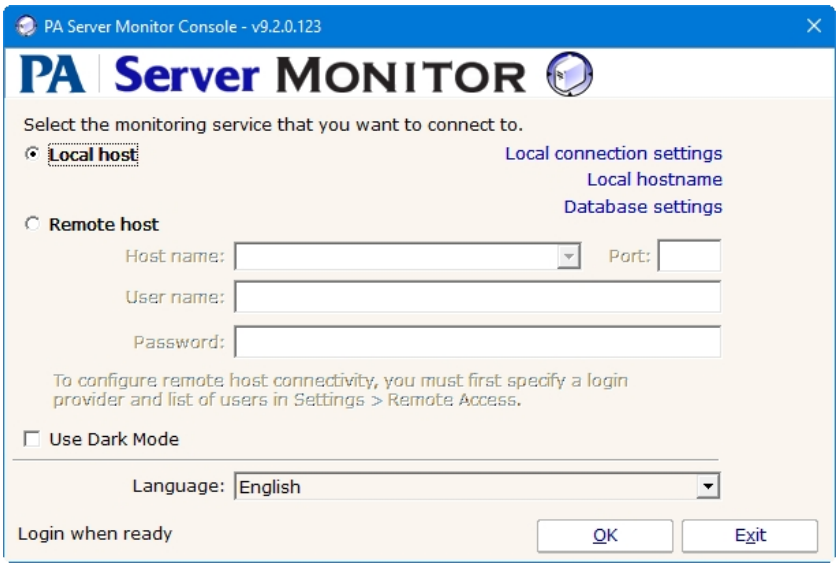
7. Select the **Create a desktop icon** option if you want the installation to place an icon on your desktop.
8. Select the **SQL Server Native Client** library option if you want to use Microsoft SQL Server as your backend database. You can leave this unchecked if you are not sure at this point -- this can be added later.
9. Click **Next**. The Ready to Install page appears.



10. Click **Install**. The Installing page appears. When the installation has finished, the Completing the PA Server Monitor Setup Wizard page appears.



11. Specify whether you want to start the PA Server Monitor Service or launch the PA Server Monitor Console by selecting its option, and then click **Finish**. If you have selected the option to launch the console, the PA Server Monitor Console window appears.



Next steps:

Start the Console GUI

Prerequisites for installing a remote Console or Remote Satellite

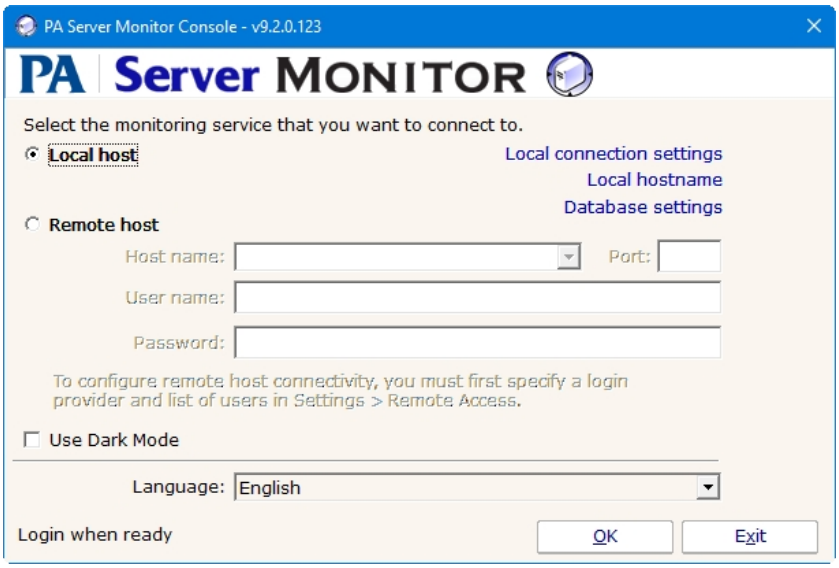
Install the Console GUI on additional computers

Install the Remote Satellite on remote servers

Starting the PA Server Monitor Console

To start the PA Server Monitor Console

1. Double-click the PA Server Monitor Console icon on your desktop. The Console connection window appears:



2. Do one of the following:
   - Select the **Local Host** option to connect to the monitoring service on the same computer.
   - Select the **Remote Host** option to connect to the host on a remote computer. Enter the remote host name, port number, user name, and password.

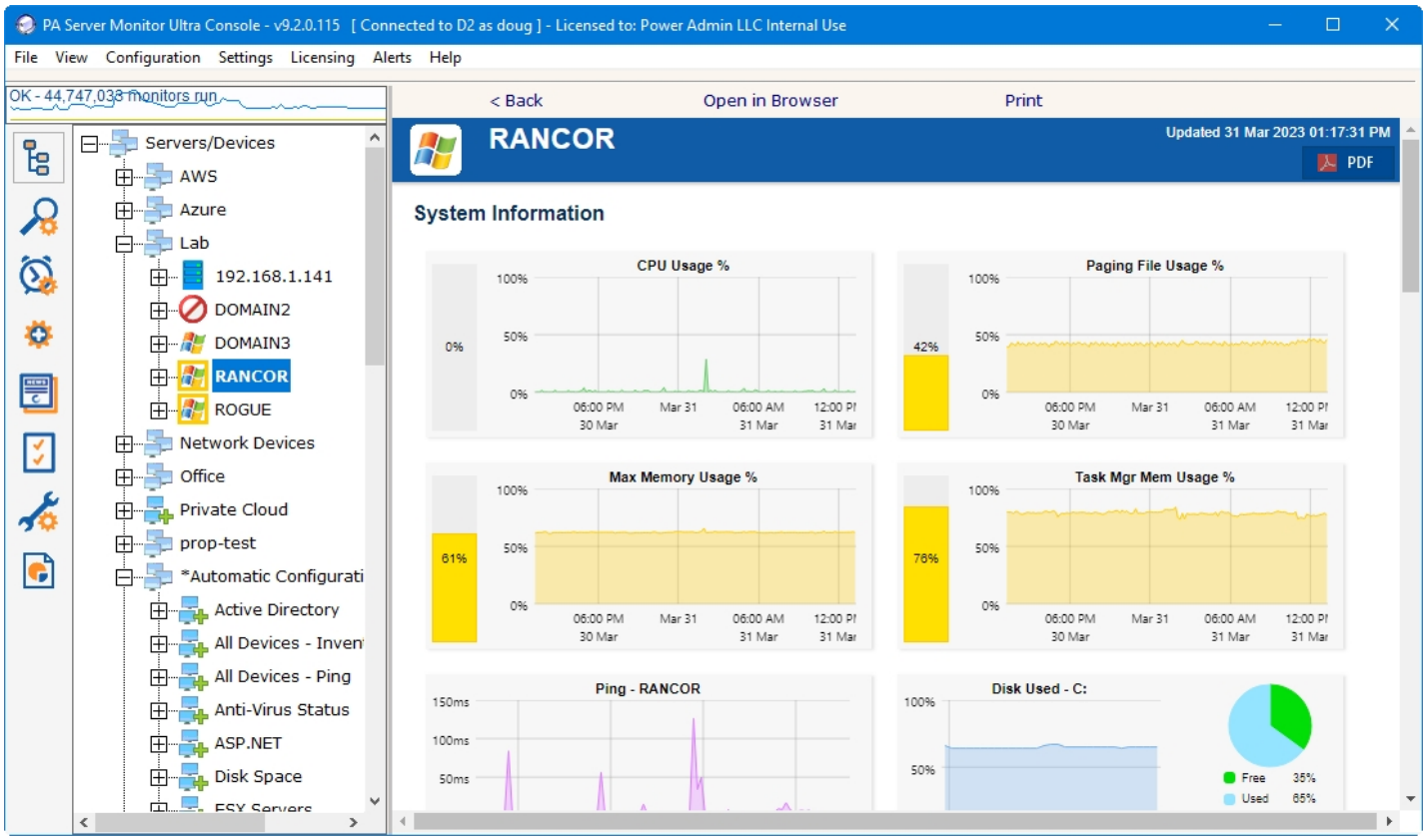
     Note: Remote access must previously have been configured in Settings > Remote Access.
3. "Use Dark Mode" can optionally be checked to put the Console into dark mode for this session.
4. A language option can be chosen for the Console. A language option can be set separately in System Settings for content that is created in the server.
5. Click **OK** to connect and open the Console GUI. If there are any errors, an error message will offer hints on how to resolve them.
6. The Console GUI will appear.

Note that there are also a few other options. You can make changes to the Database Settings, the Server HTTP/S Settings and the name used when connecting to the local server (localhost by default).

PA Server Monitor Console

The Console is the administrative interface to PA Server Monitor. Some buttons that appear in the column at the left are only available if you run the Console on the same machine where the Central Monitoring Service is installed.

Left Button Bar



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. Monitors running on remote Satellites are not represented. Double click on the Activity Graph and a larger version with more details will appear, and to view activity on Satellites.

The **Server/Device tree** shows the groups and devices that are being monitored, as well as individual monitiors.

The **All Monitors** button shows all monitors grouped by type. This button can be added or removed from the View menu.

All Actions shows all actions grouped by type. This button can be added or removed from the View menu.

Advanced Services is where Satellite Services, Monitor Template Library, Global Monitors, Failover Status, Acknowledge Errors, Alert Reminder, and Event Deduplication settings can be viewed and changed.

News and Updates is where you can view "Updates, Tips and News" which is a great way to get information on new features and view articles that are posted on our Network Wrangler - Tech Blog site. You can also check for product updates, manage local upgrades to satellites and check for license updates.

Configuration Settings holds options for Smart Config, Bulk Config and importing and exporting the configuration.

Settings (not available in Remote Consoles) will show you options for System Settings, Database Settings, HTTP Server Settings, etc.

Reports is where you can create your own reports, create scheduled reports, view existing reports and view current system activity.

Navigation Tree

Next to the button column 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. Clicking a button in the column will control what is shown in the navigation tree.

The right panel displays details about the item selected in the navigation pane. Some times that information being viewed is a report, or monitor or action configuration details.

All reports that can be viewed within the Console can also be viewed in any web browser. Scroll to the bottom of the report to see the link for that report, or hit the Open in Browser button above the report.

Command Line Options

Normally the Console is started without any command line parameters, but occasionally a command line option may be useful.

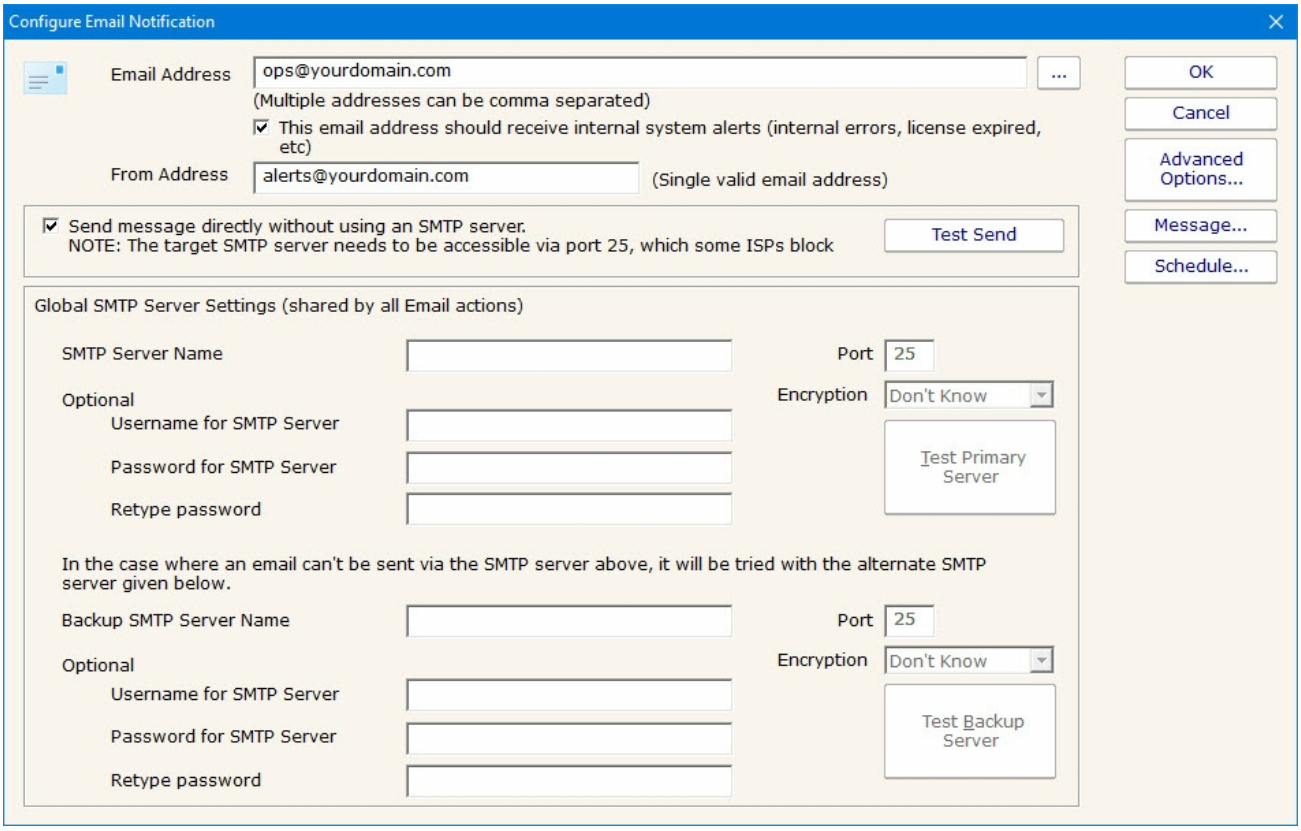
See Command Line Options for details.

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.

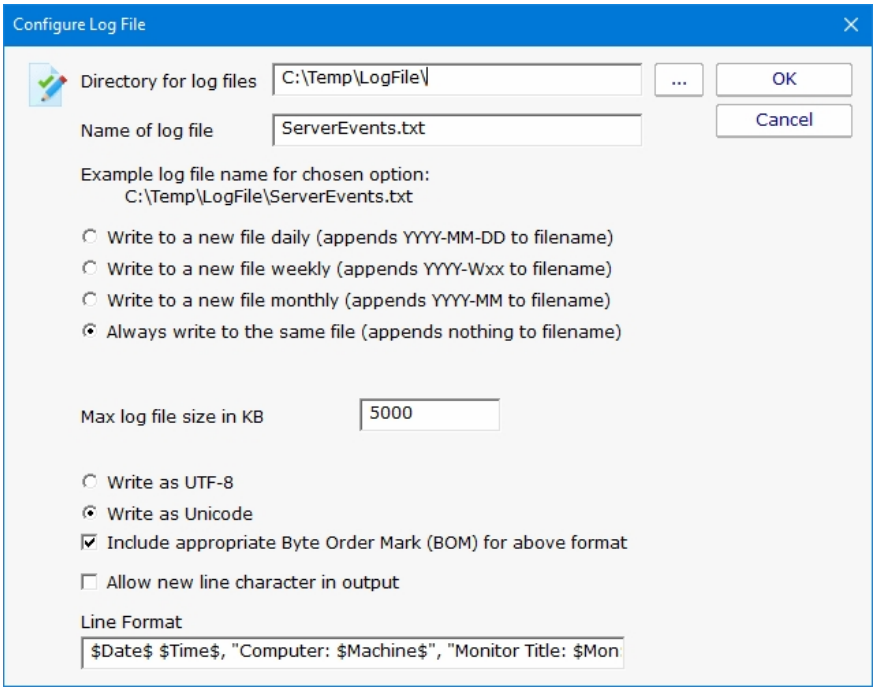
Most of the screens that you will encounter in the Startup Wizard are standard configuration dialogs that are available to you from PA Server Monitor, so you can always change the configuration for your setup later.

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, Configure Email Notification.



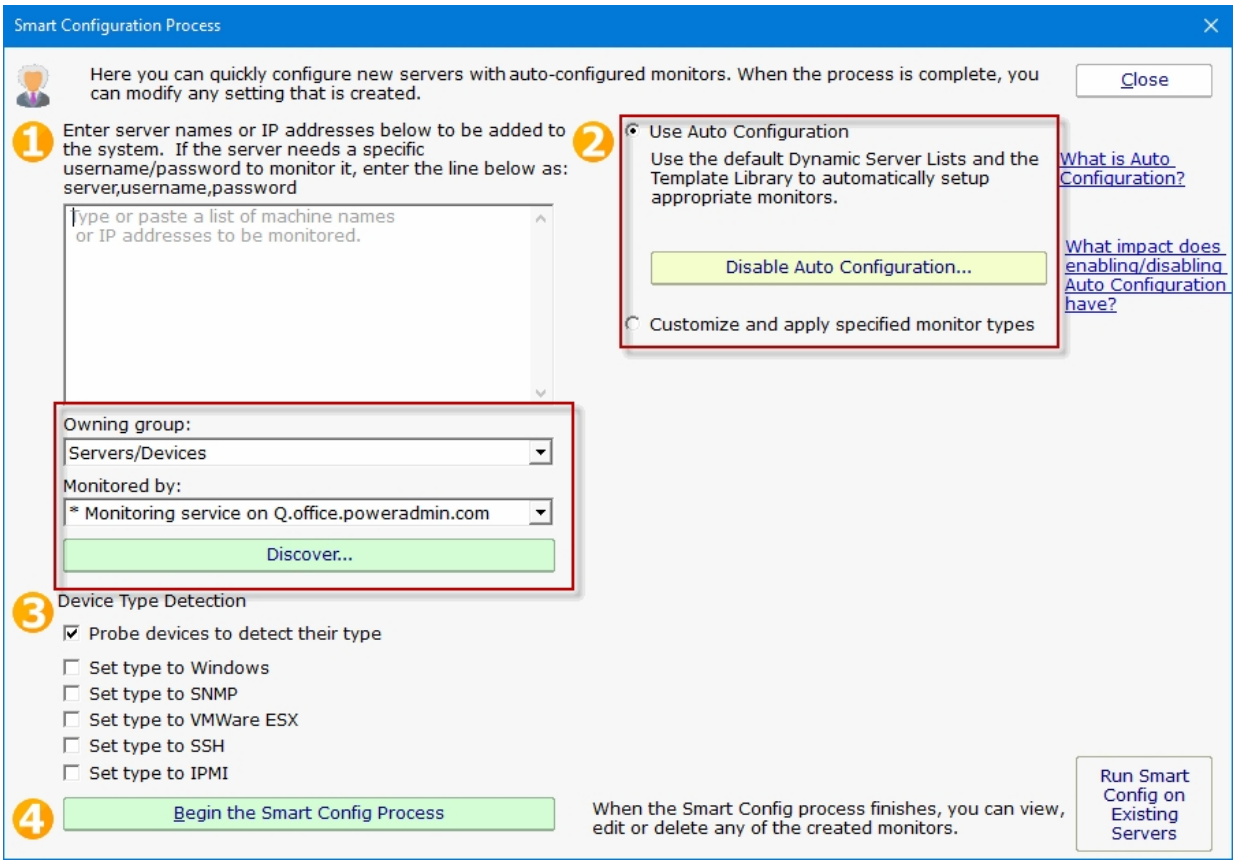
Refer to the help page Send SMTP E-Mail for directions. Select OK when you are finished with the Configure Email Notification screen.

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



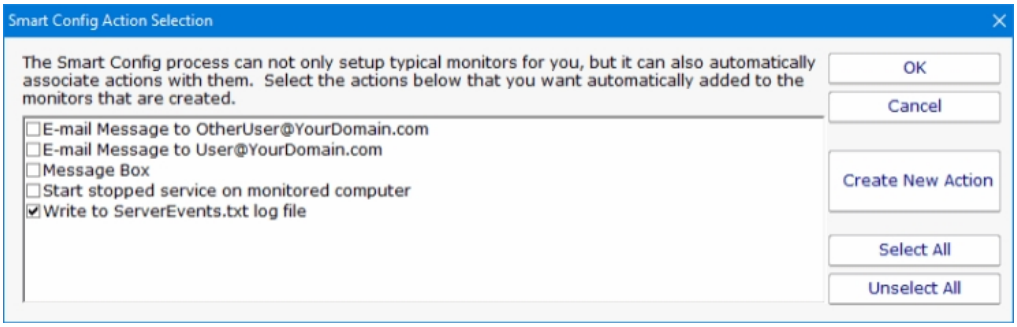
Select OK when you are finished with this screen.

The Smart Configuration screen will help you set up many servers and devices for monitoring. 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. The program will allow you to use the Automatic Configuration or the Customize and apply specified monitors options to configure your monitors. More information on Automatic Configuration.



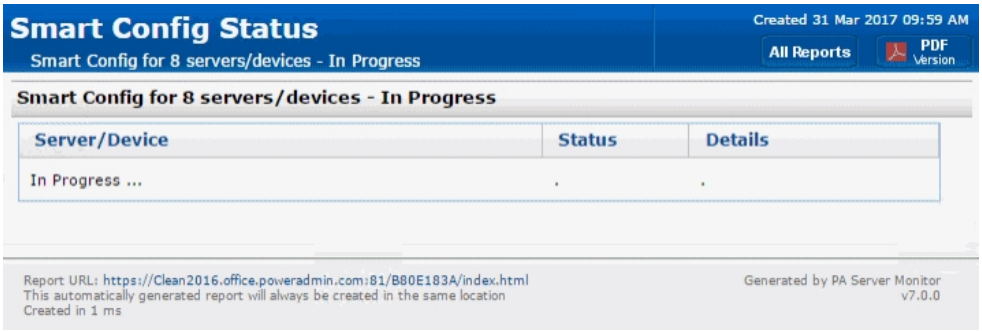
Refer to the help file entry labeled Smart Configuration for specific instructions for this screen.

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



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

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



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

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.

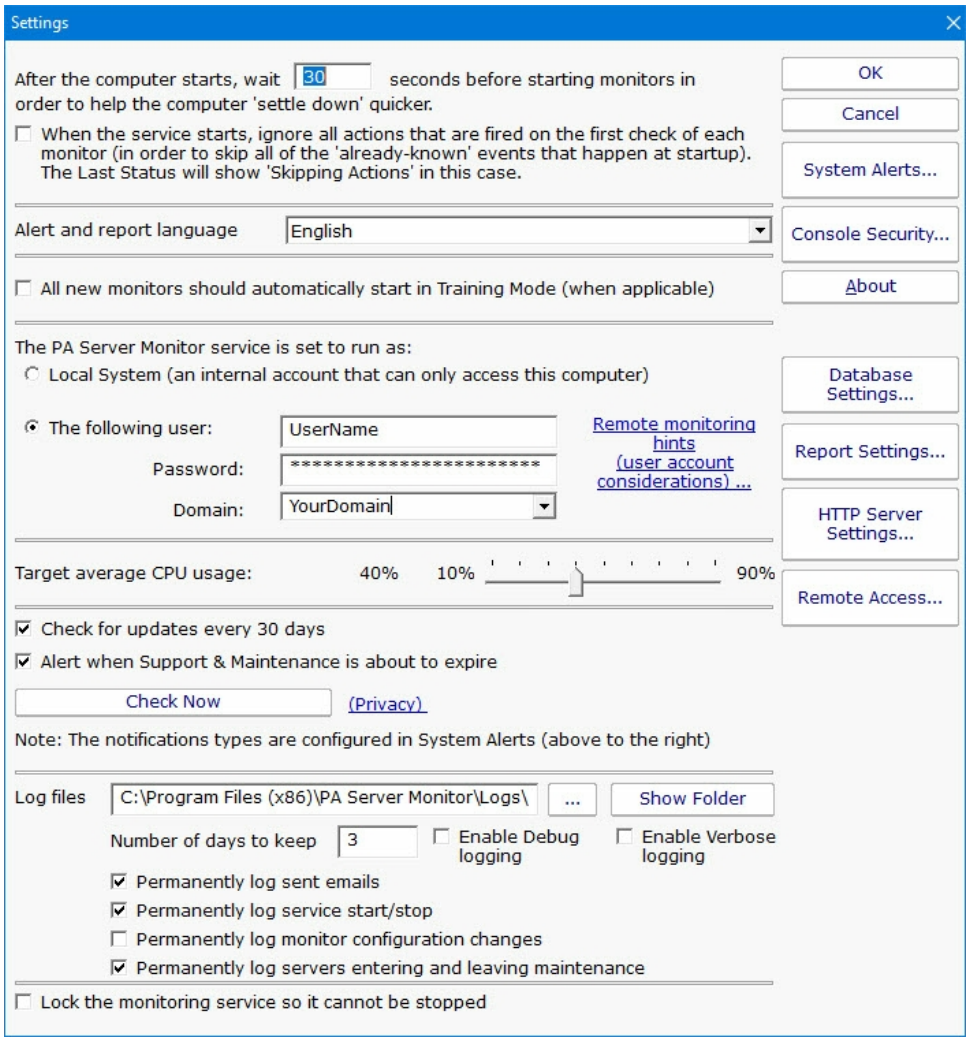
Console Security allows you to set a password that the Console will request when it is launched. This setting allows you to limit access to PA Server Monitor to authorized users.

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.

Remote Access allows you to specify which users can use a Remote Console to connect to the Central Monitoring Service and/or access reports in PA Server Monitor.



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.

Alert and Report Language - Change the display language for all of the reports and alerts.

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.

Service Account - 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.

Location where the service log files are stored. This location can be changed by entering the new location.

Number of days that you want to keep log information.

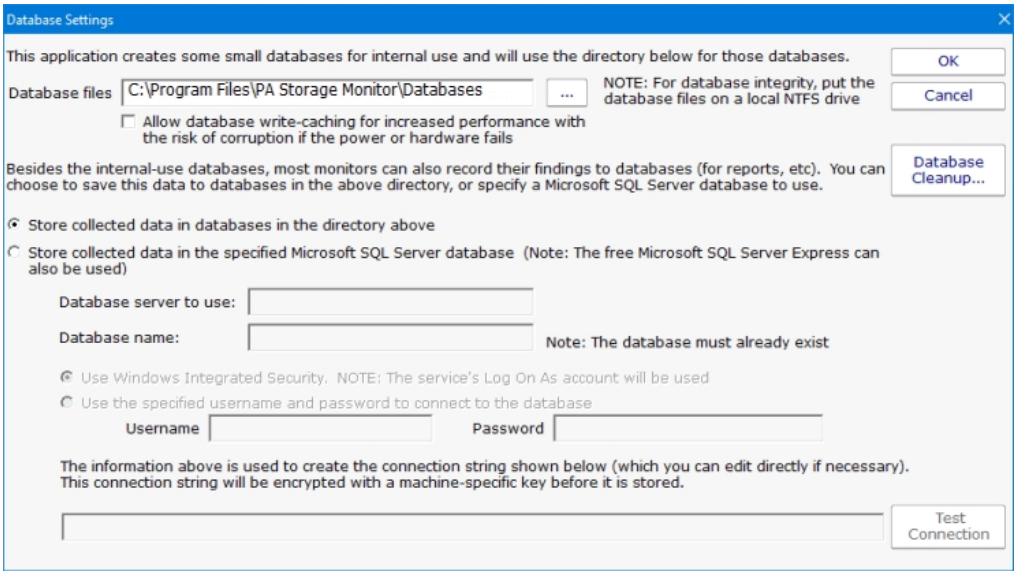
There are two Debug options allow you to collect more information for the purposes of debugging monitoring issues. This is NOT something that you normally leave turned on as the amount of data recorded in the log files will grow fast and create large log files.

There are four options to record certain events to a permanent log file (log files where data doesn't roll off after time). These log file are not affected by the number of days that you have entered to retain log information. The events that is kept in these log files are sent emails, service start & stop, monitor configuration changes, and entering and leaving maintenance.

Lock Monitoring Service - The monitoring service can be locked so it cannot be stopped. This prevents the service from being stopped using services.msc or the NET STOP command. It is still possible to uninstall the product. It is also still possible to upgrade and restart the service from the Console. To lock a Satellite Monitoring Service use the "Satellites: Lock Service (so service can't be stopped)" option in Bulk Config.

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

SQLite is a highly reliable open-source database. By default, PA Server Monitor stores all of its data in 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.

Database files will be created and stored in the directory specified. Even if MS SQL Server is chosen for the database, a small amount of data will still be stored in the specified database directory.

Microsoft SQL Server

To use SQL Server for storage, you need to install the SQL Server Native Client library, which is Microsoft's latest database connection technology. The SQL Server Express databases are fine for most installations, but do be aware that they limit the total database size to 10GB (for SQL Server 2008 R2 Express).

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 and can be empty.

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.

Note: If you are using database mirroring, you can manually add the Failover_Partner parameter to specify the alternate database to connect to.

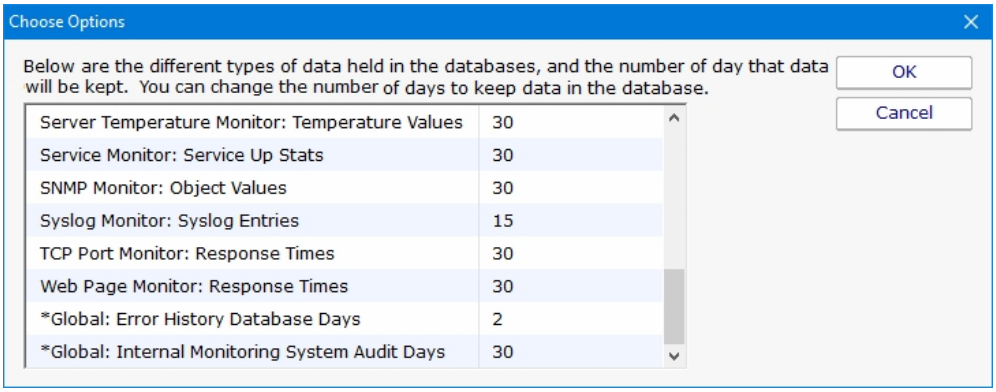
If you do not need or wish to use SQL Server as the database for PA Server Monitor, the SQL Server Native Client Library does not need to be installed.

Changing Databases

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 can take a day for the transfer).

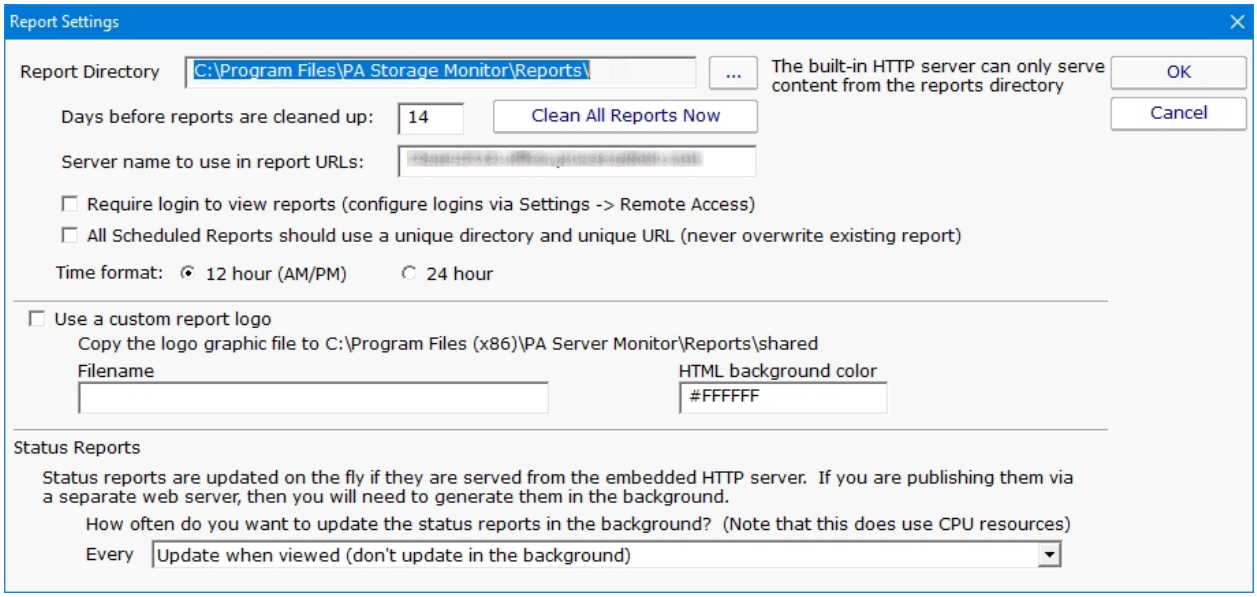
Database Cleanup

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.



Report Settings

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



The available settings 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.

Server name to use in report URLs - By default the report URLs are http(s)://{servername}:{port}/ If you need to change {servername} (such as using an IP address, or perhaps to use an externally accessible server name) you can do it here.

Require login to view reports - By default, anyone that can access the product's built in HTTP server can view the reports. You can lock this down by IP address in HTTP Settings. Or you can require that users login before they can view reports by checking this box.

Since usernames and passwords will be sent across the network, SSL must also be enabled in HTTP Settings. See Remote Access Users for how to specify users.

Use unique directory - By default, Scheduled Reports always get written to the same directory, so the URL they use is always the same. If you want to keep reports around for a while, you can check this box and Scheduled Reports will always write to a different directory. The downside is the URL changes each time the report runs so you can't save the URL in a browser. Another option for archiving reports in to archive a PDF of the report available in the Scheduled Report configuration.

Time format - Choose whether the reports display times in 12 hour AM/PM format or 24 hour format

Report Branding - See Report Branding for details

Status Reports Interval - This drop down list allows you to select the interval at which report files are generated. By default, reports are generated when they are accessed.

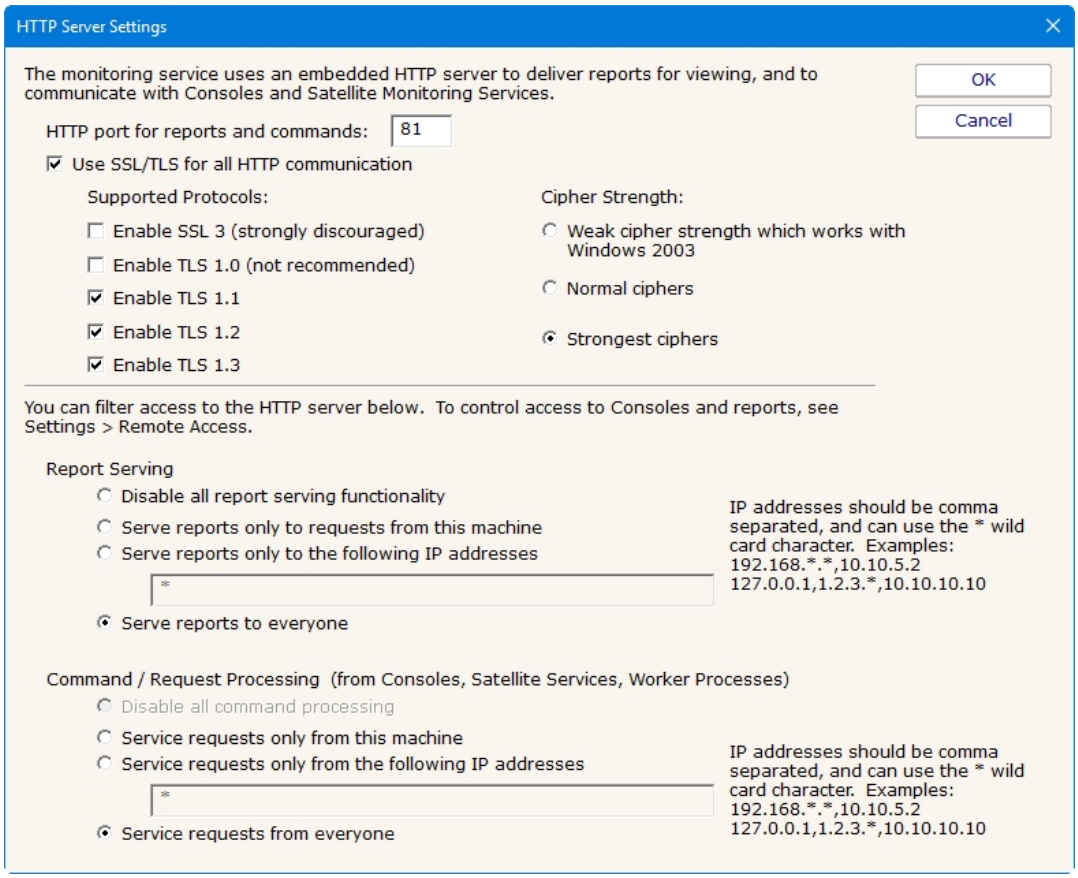
If you are serving reports via a different web server, you should specify that the reports are generated on a regular schedule. In a small installation (less than 50 servers) regenerating the reports every minute is not a problem, but in a bigger installation choosing a larger interval would be more efficient.

Show Maintenance Period on server status report - Self explanatory.

Turn off "Enable WMI Hint"... - 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.

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 as communicating with the Console and Satellite Monitoring Services. 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 can use any port specified.



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.

You can also get a signed SSL certificate which will remove the warnings.

NOTE: For security reasons, usage of remote Satellites and/or Remote Consoles requires SSL to be enabled.

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".

You can optionally require a user login to access reports. See Report Settings.

Command Processing
Commands are sent from a variety of sources, including the Console, worker processes, optional remote Satellites and some dynamically updating reports. This setting determines where command requests can come from. Generally it is best to leave it at "Service requests from everyone" since all sensitive data is protected by username/password and/or SSL (if enabled) when in transit.

Smart Config

The Smart Config feature is a very useful tool for quickly adding servers or devices to be monitored. You specify one or more servers, and the monitors inspect the servers/devices and create appropriate monitors for each one based on default settings.

Watch the training video How to Use Smart Config in PA Server Monitor.

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 also press the Discover button to find a list of servers for you (more on that below).

You can optionally specify a username and password to use when accessing the server by entering any line in the form:

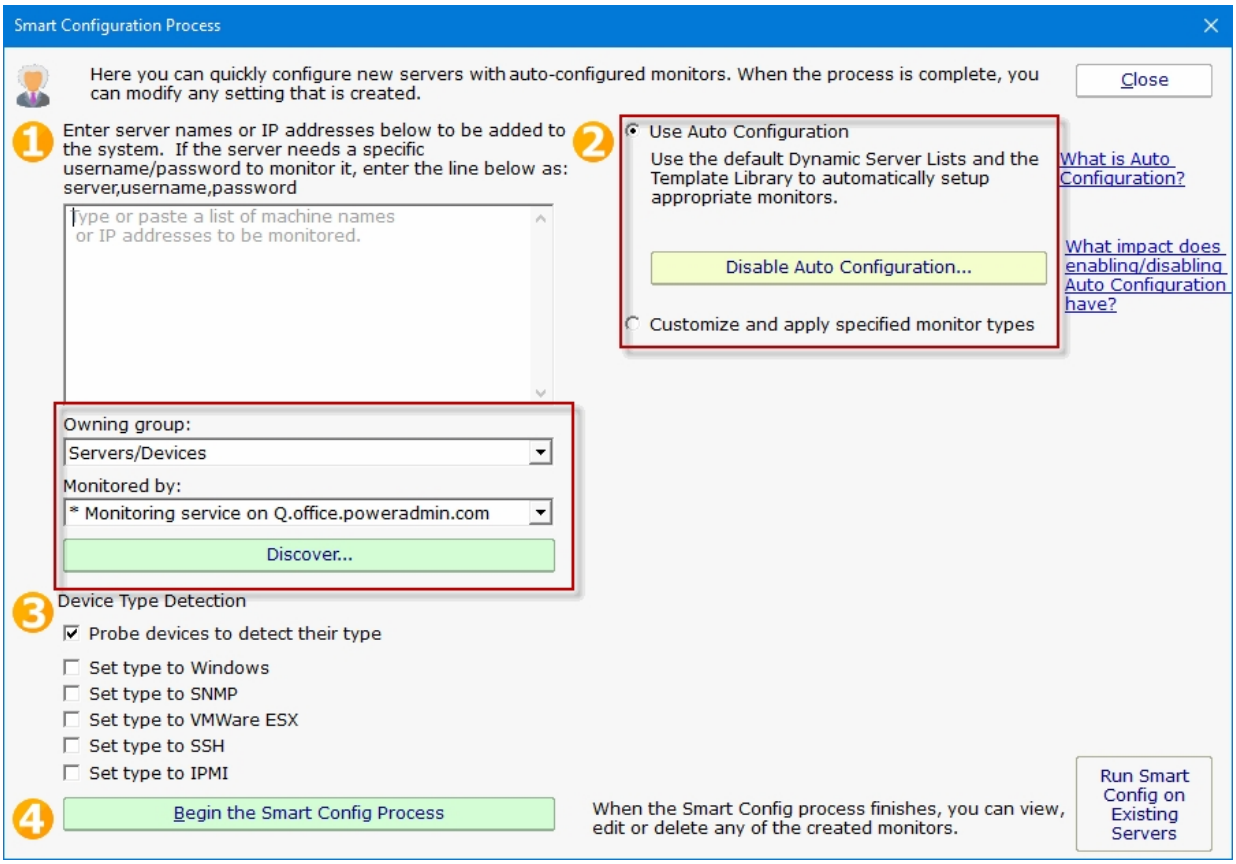
```
server_name,username,password,alias
```

(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 already entered credentials to see if they will work. Otherwise the service's Login As user will be used.

Owning Group
When adding new servicers or devices to be monitored, this option will give you the ability to add them to a group. By default the Servers/Devicese root group is chosen.

Monitored By
If you have remote Satellite monitoring sites, you can indicate that the remote Satellite should monitor the list of servers. By default the Central Monitoring Service is chosen. That means newly created servers/devices in the system will be assigned to the monitoring system chosen from this list.



The next step is to select how the service will inspect the server(s)/device(s) to add monitor modules, either by Automatic Configuration or Customize and apply specified monitor types. Then select the Device Type for your servers/devices 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.

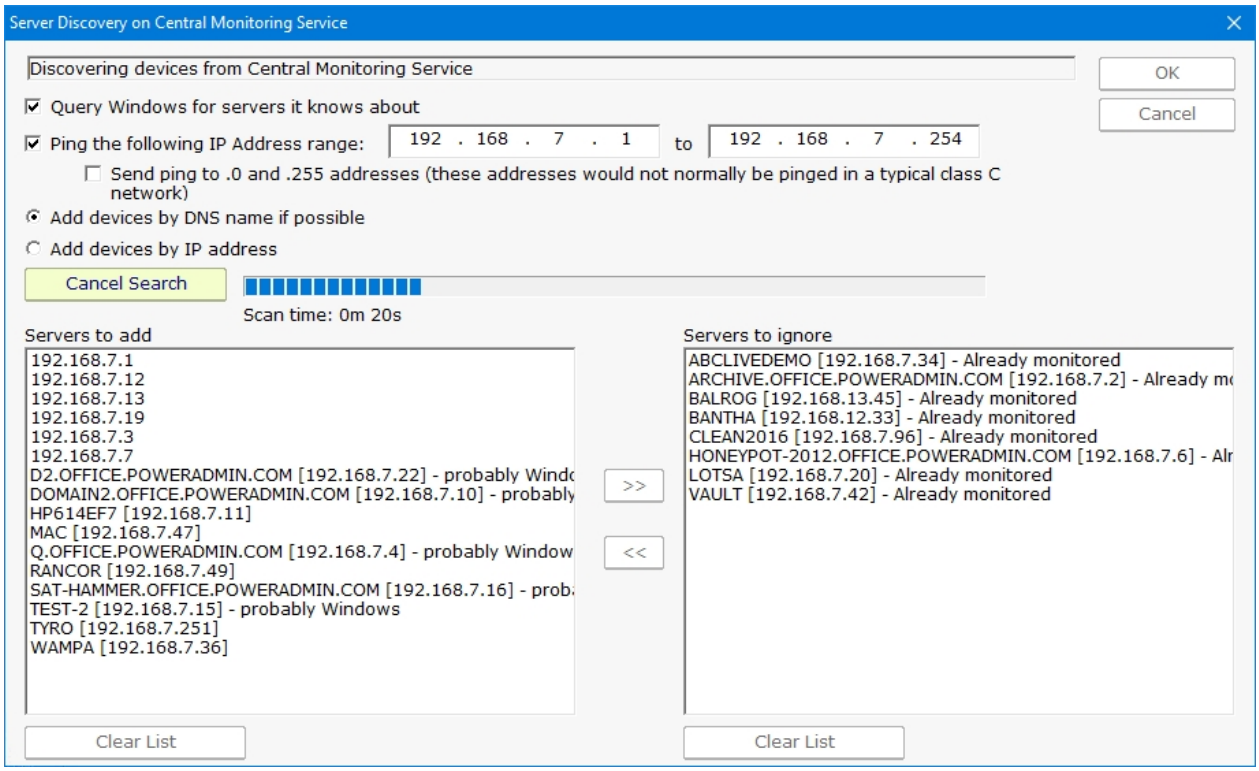
A subtle button at the bottom right lets you run Smart Config on existing servers/devices. This will open up the Bulk Config feature and guide you through the rest of the process.

Existing monitors and actions are not modified -- new monitors and new actions are created while leaving the existing monitors and actions alone. If an existing monitor of a particular type already exists, Smart Config will not add a duplicate.

Server Discovery

Pressing the green button labeled "Discover" allows PA Server Monitor to scan the network for servers and devices without having to manually gather this information. The following dialog will appear on top of the Smart Configuration dialog.

If you selected a Satellite service in the "Monitored by" box mentioned above, the discovery scan will be sent to the remote Satellite to be performed. That means you can discover servers/devices at remote sites to be monitored even if you are not on the remote network.



The following options are available for Server Discovery:

Query Windows for servers it knows about: Windows has its own network discovery process that PA Server Monitor will query to find servers that Windows knows about.

Ping the following IP Address range: A Ping message will be sent to each address that exist in the range of IP addresses given.

Send ping to .0 and .255 addresses: these address values have special use in the TCP/IP protocol. By default this box is unchecked. You may enable this feature if you have reason to believe that these addresses are in use by computers of interest for monitoring.

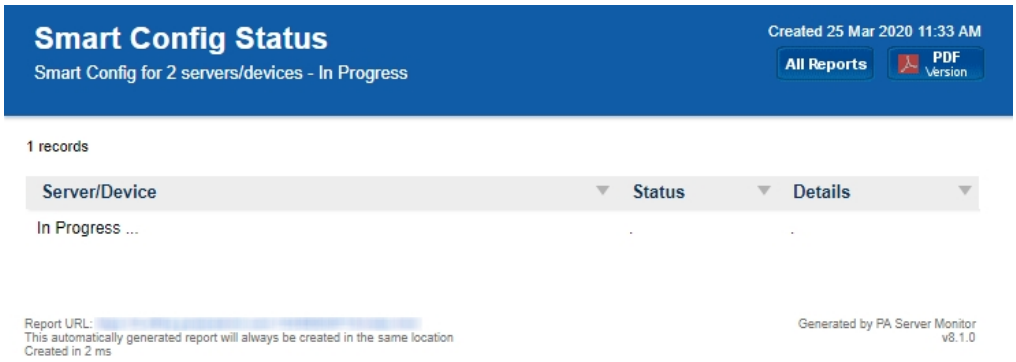
Servers to add: these are the IP addresses (or computer names if they could be resolved) where servers/devices were detected, and which are not currently being monitored.

Servers to ignore: These are servers/devices that were discovered, but which are already being monitored.

Pressing the OK button will append the list of servers on the left ("Servers to add") to the list of servers to run Smart Config on shown above.

Starting the process...

Pressing the green "Begin the Smart Config Process" button will send the server list and settings to the specified monitoring service (the Central Monitoring Service or a remote Satellite) for execution. When that happens, the following dialog is shown.



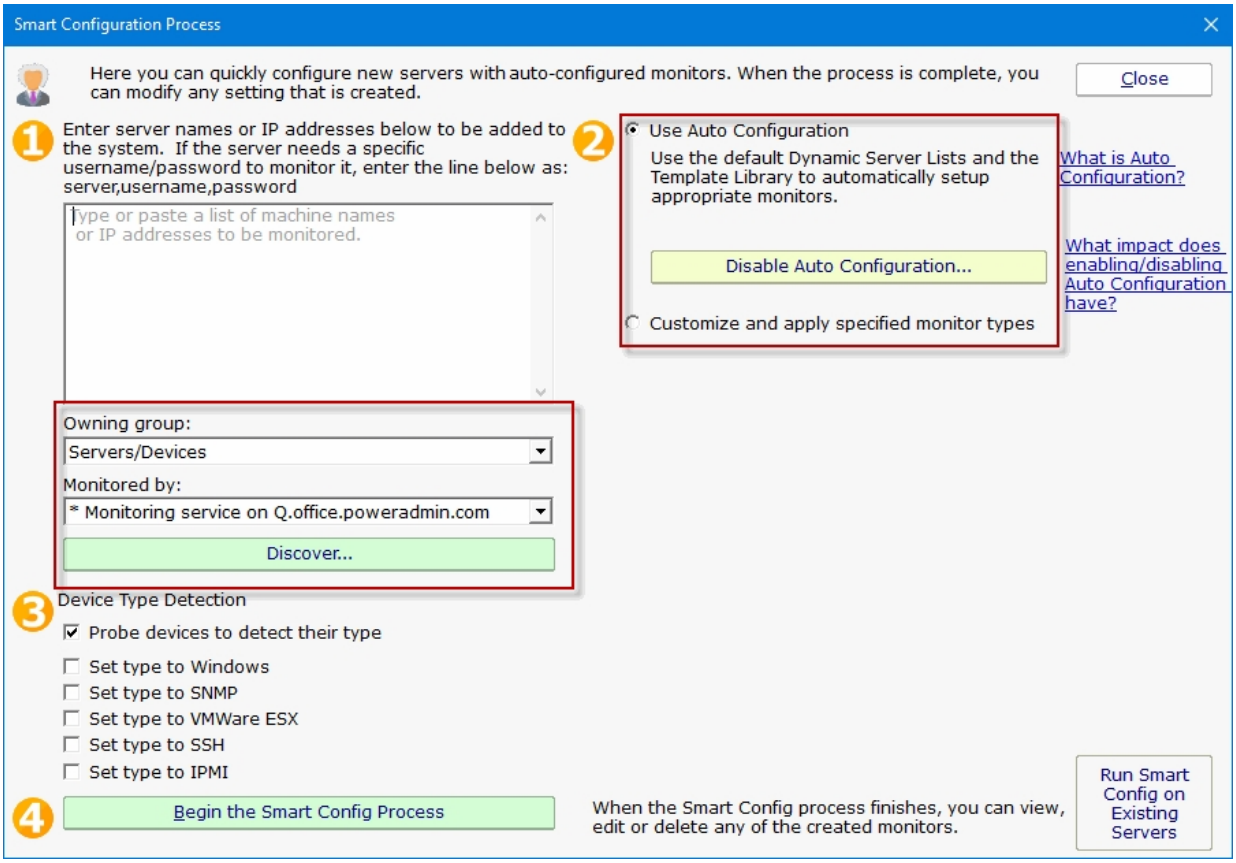
The dialog will display the progress of the Smart Config process. You can leave it open and watch or close it -- the process will continue in the background. The newly created server(s) and monitor(s) will automatically appear in the Console navigation panel a few moments after each one is created.

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 a list of machine names or IP addresses that you want to monitor. You can also press the Discover button to help get that list. The program will allow you to use the Automatic Configuration or the Customize and apply specified monitors options to configure your monitors. More information on Automatic Configuration.



When adding new servicers or devices to be monitored make sure to add them to a group using the Owning Group option.

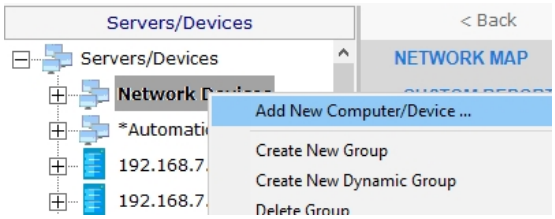
If you are using Satellites it's very important to make sure that the Satellite you want to monitor the new servers is selected in the "Monitored by". If not using Satellites, this box will select the Central Monitoring Service.

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.

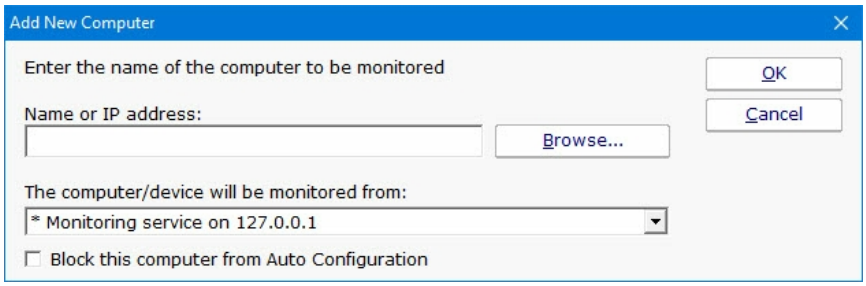
See Smart Config for more detailed information.

Adding Individual Computers

You can manually add a single computer to be monitored by right-clicking on any group in the left navigation pane in the Console.



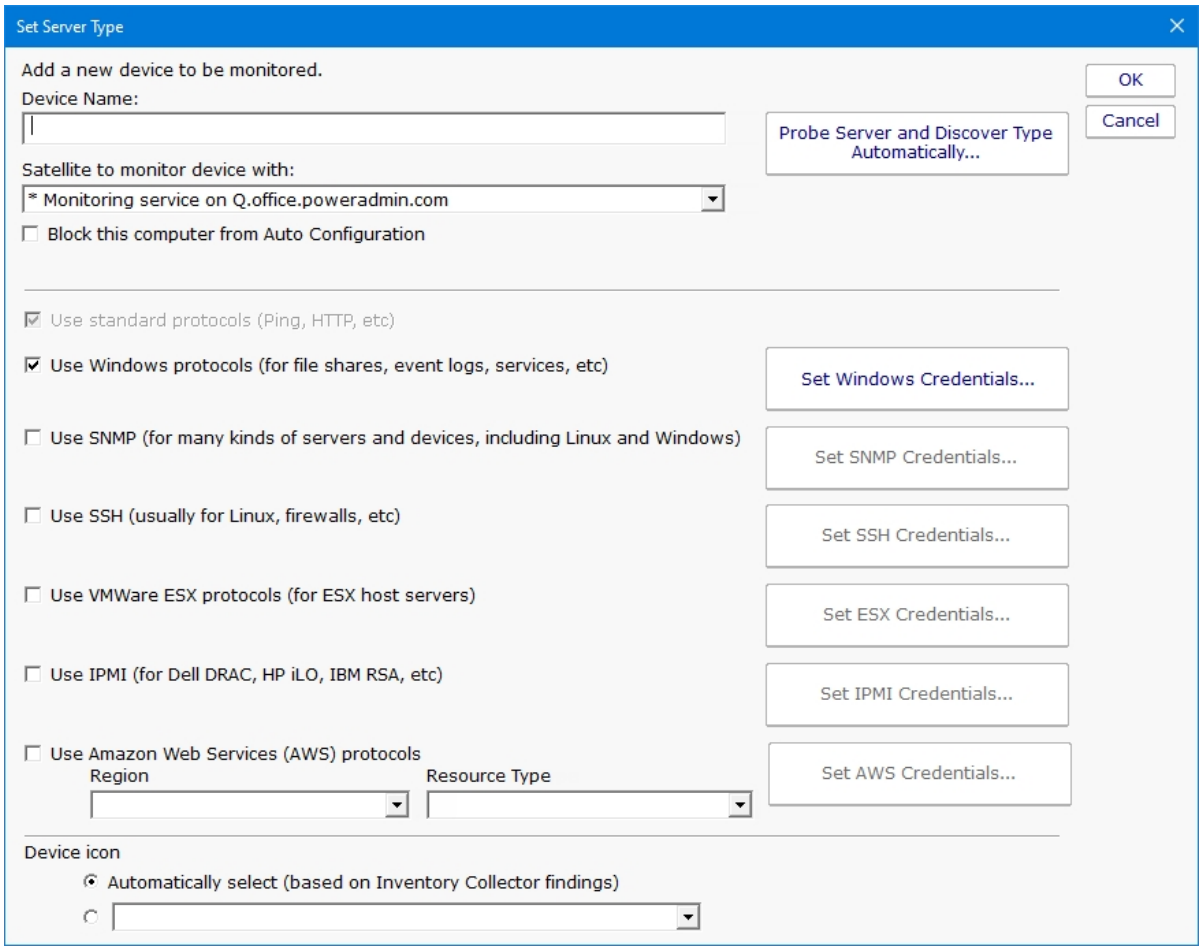
Doing so will first show the dialog below to collect the server name.



"The computer/device will be monitored from" lets you specify whether the Central Monitoring System or a remote Satellite will be monitoring the device. Naturally the monitoring system that has access to the device should be chosen.

Set Server Type

The next step is to tell PA Server Monitor what type of server/device is being added. This helps the product know which protocols to use when communicating with the server/device. The dialog below is how you indicate this. The buttons on the right let you give device-type credentials (ie Windows username/password, SNMP community string, etc). The button also indicates the credentials currently being used.



You can click the "Probe Server and Discover Automatically" to have PA Server Monitor determine which protocols the server/device responds to. You may still need to specify credentials though.

If you want to get back to this dialog later, it's always available by right-clicking on the server/device and going to Type & Credentials > Set Server Type.

For more information on setting individual credential types, see the links below.

Setting Windows Credentials

Setting SNMP Credentials

Setting AWS Credentials

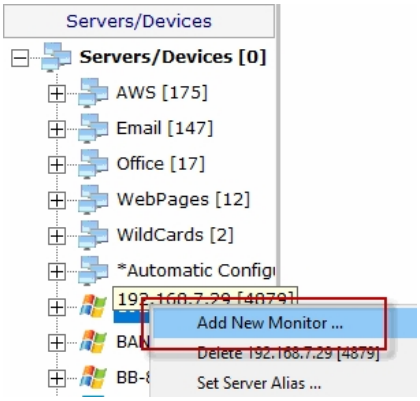
Setting VMWare ESX Credentials

Setting SSH Credentials

Setting IPMI Credentials

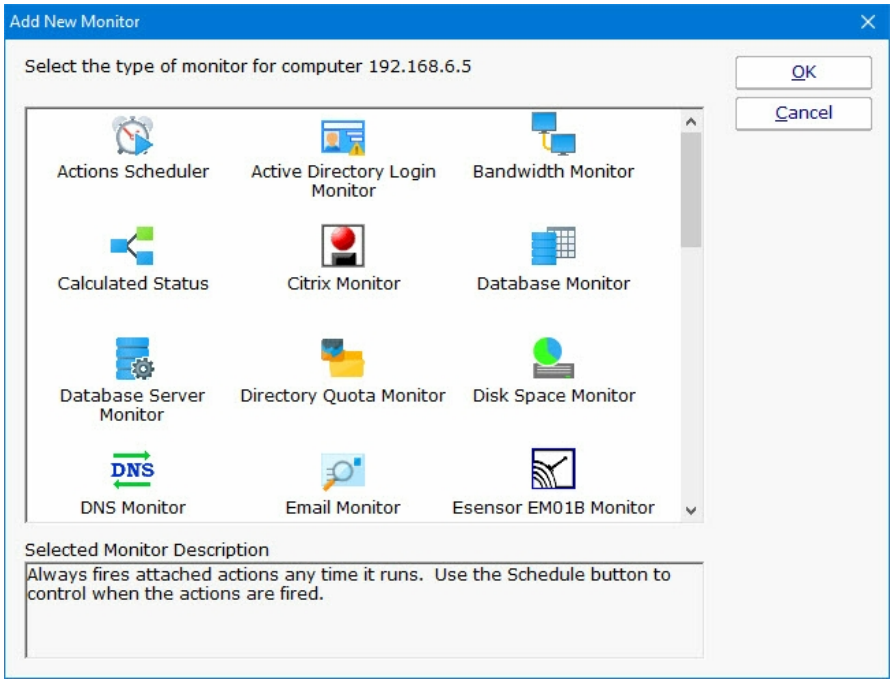
Adding Monitors

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



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

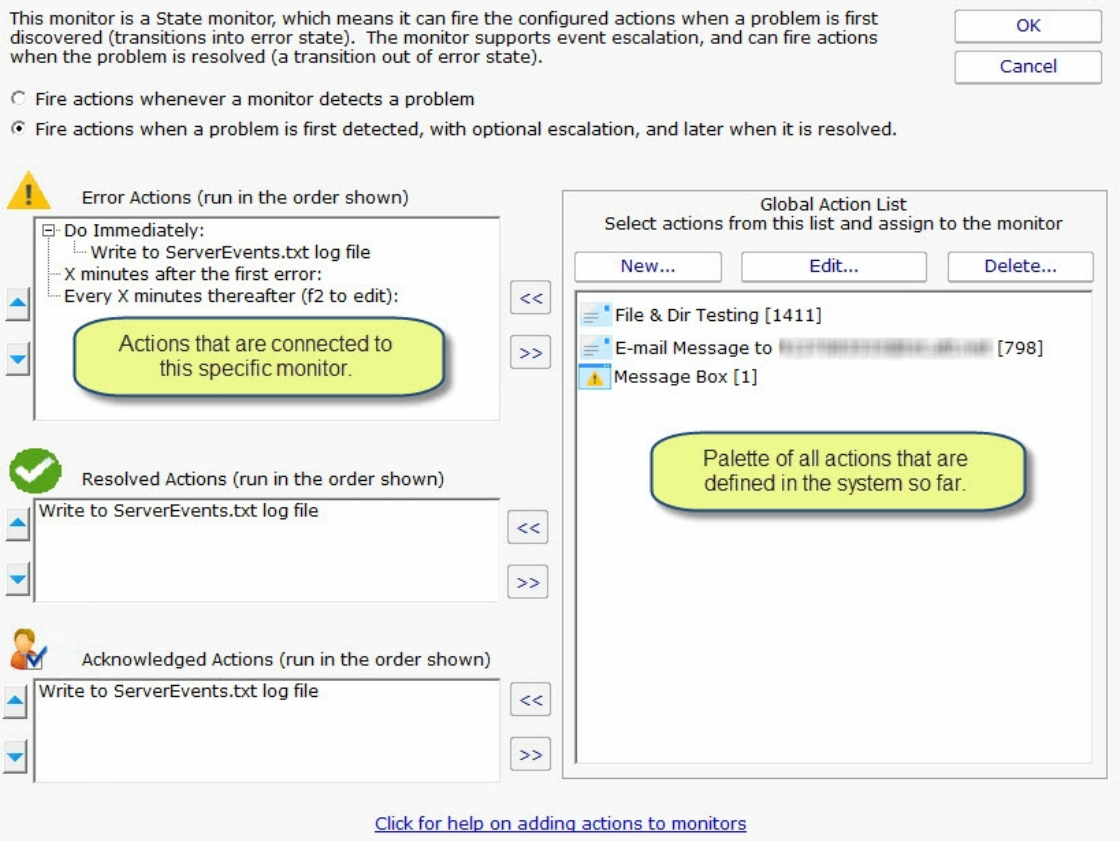
Once you select a monitor, you will be shown that monitor's configuration dialog.



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

Adding Actions

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



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

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

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

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

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

State vs Event Monitors

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

is low, ping response is too slow, etc.

The following describes how State and Event monitors differ.

State monitors keep track of whether the monitor is in a healthy state or an error state. For *State* monitors, you can choose to have actions run when a problem is detected, and then not again until it is fixed. State Monitors also support *event escalation* and *error resolved actions*.

Event monitors run actions every time they see something wrong. You can control what actions are run and when.

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

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

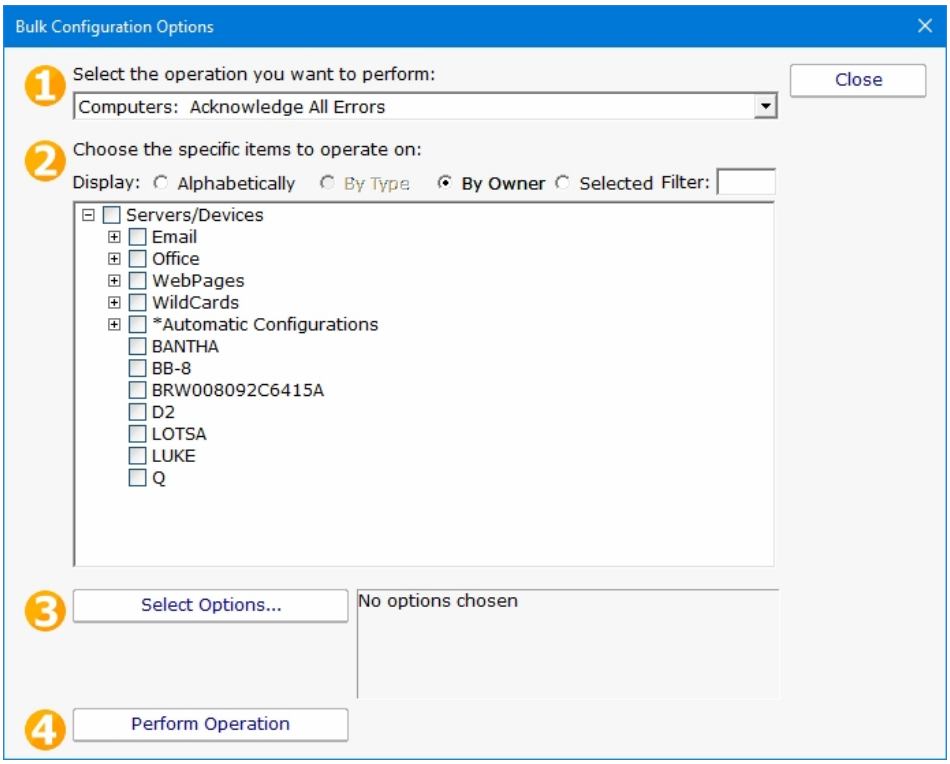
Bulk Config

Bulk Config is one of the most powerful configuration feature in PA Server Monitor. It will help you quickly configure large numbers of monitors, computers, actions, etc.

The Bulk Config dialog consists of two main areas:

(1) 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.

(2) Target Objects: A list of objects that the operation will be performed on. You can use the radio buttons to choose different ways of grouping the objects to make object selection easier.



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

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

Acknowledging Alerts

Alerts can be sent out using a variety of actions such as email, SMS, calling an external URL, etc. All of these are methods to notify you about a problem. You can also choose to acknowledge alerts if that feature has been enabled in Advanced Services > Acknowledge Errors Feature Status > Configure Error Acknowledgement.

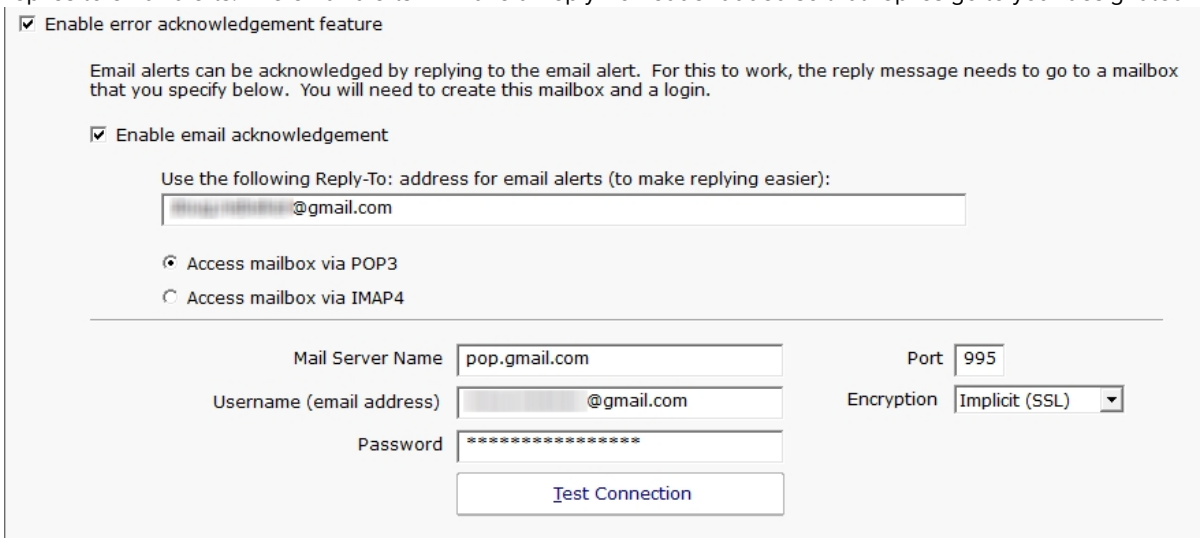
Acknowledgement Methods

There are a few different ways to acknowledge alerts:

Add an Acknowledgement check the box in the Server Status Report, or in the Error Audit Report. Then clicking that box in the report will acknowledge the alert.

The External API has a command for acknowledging alert programmatically via an HTTPS call.

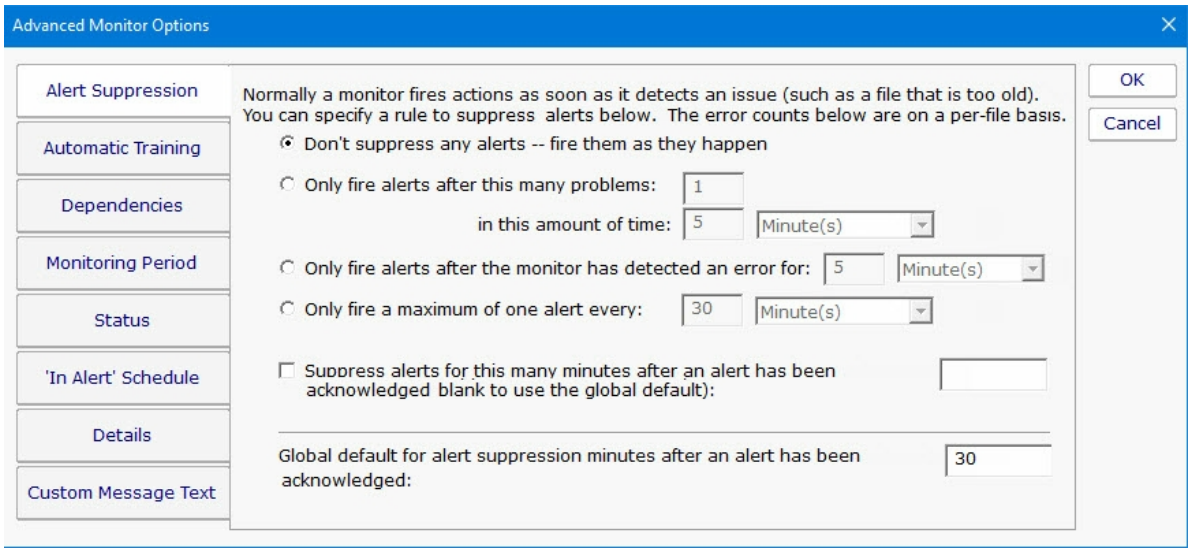
You can reply to alerts via email and acknowledge them that way. Simply designate an email address that will be monitored for replies to email alerts. The email alerts will have a Reply-To header added so that replies go to your designated mail box.



Additional details on Configuring Email Alert Acknowledgement.

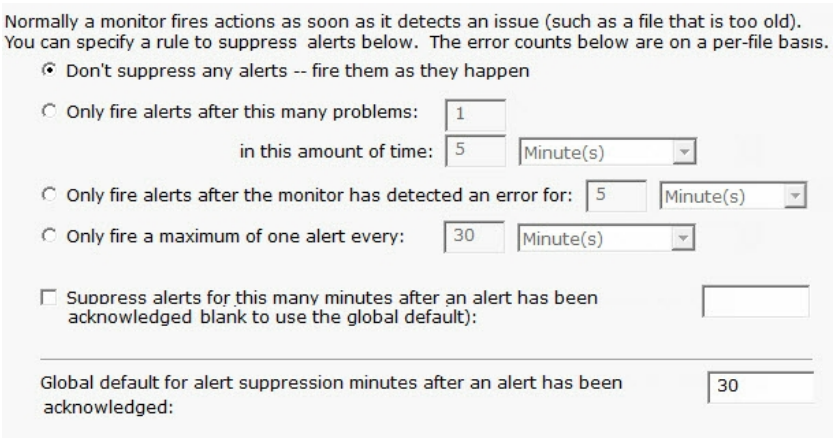
Advanced Monitor Options

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



Each of the different option tabs is discussed below.

Alert Suppression

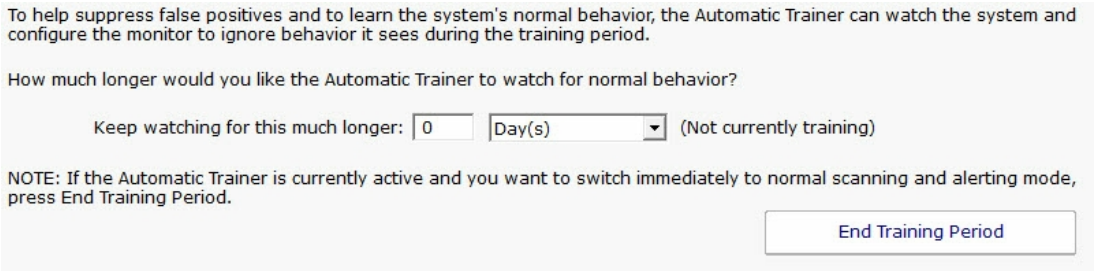


With the Alert Suppression settings, you can instruct the monitor how often and how soon you want to be alerted about a specific issue. This enables the monitor to skip the first few failures on a specific device if you wish and only warn after an error has happened a few times or for a particular amount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

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

See Alert Suppressing, Event Escalation and Event Deduplication to see how these features can be used together for suppressing alerts.

Automatic Training

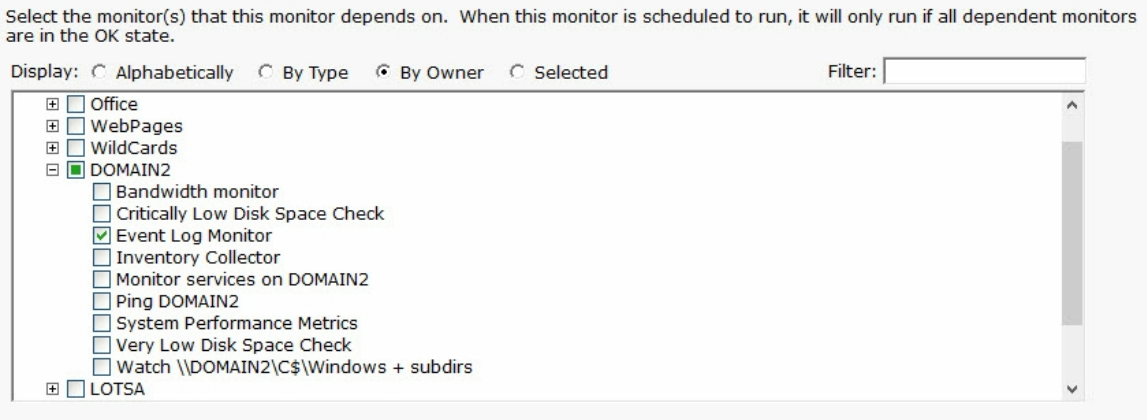


PA Server Monitor can have a monitor train itself. What that means is it will monitor like normal during the training period, but not fire any alerts. Anytime something 'abnormal' (or outside the normal thresholds) is seen, the thresholds are adjusted such that it won't alert on that activity if it is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

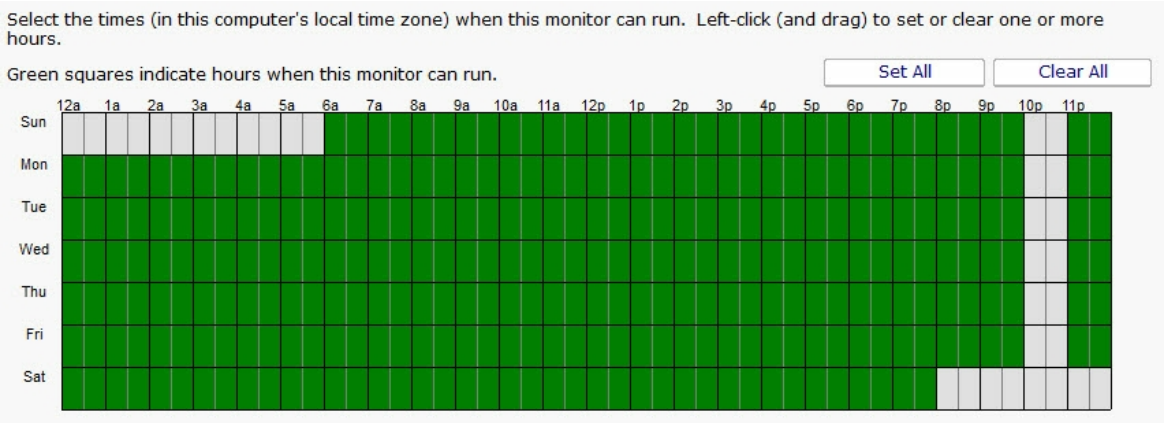
At the end of the training period, the monitor will automatically switch back to normal monitoring mode. If you want to force it to switch back immediately, press the End Training Period button.

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.



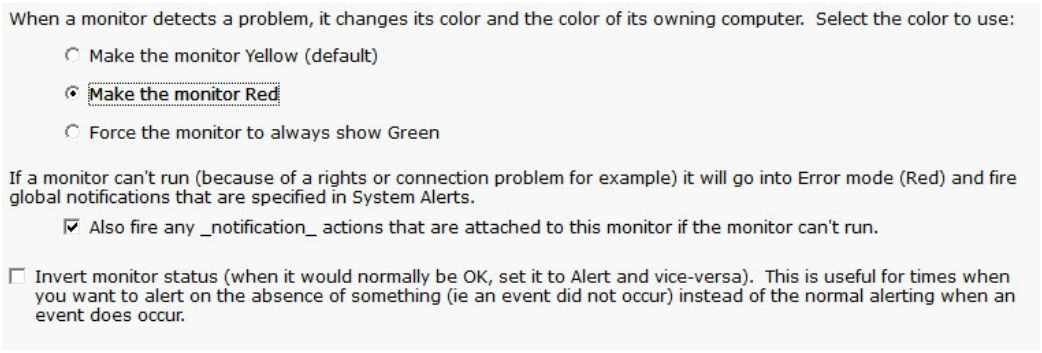
Monitoring Period



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.

The dark green boxes indicate times the monitor can run, and the light gray boxes are times when the monitor will not run.

Status



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.

'In Alert' Schedule

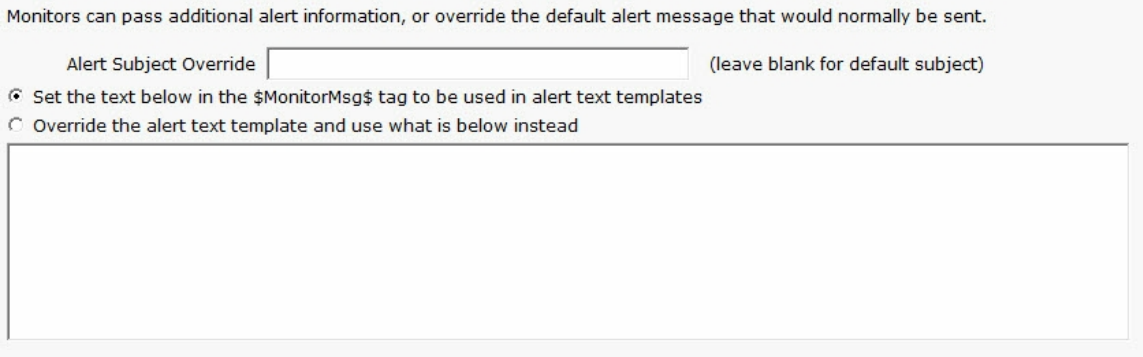
This panel will allow you to change the scheduling of the monitor when it is in alert mode. The schedule of the monitor can be escalated by selecting on of several option in the dropdown box.

Details

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

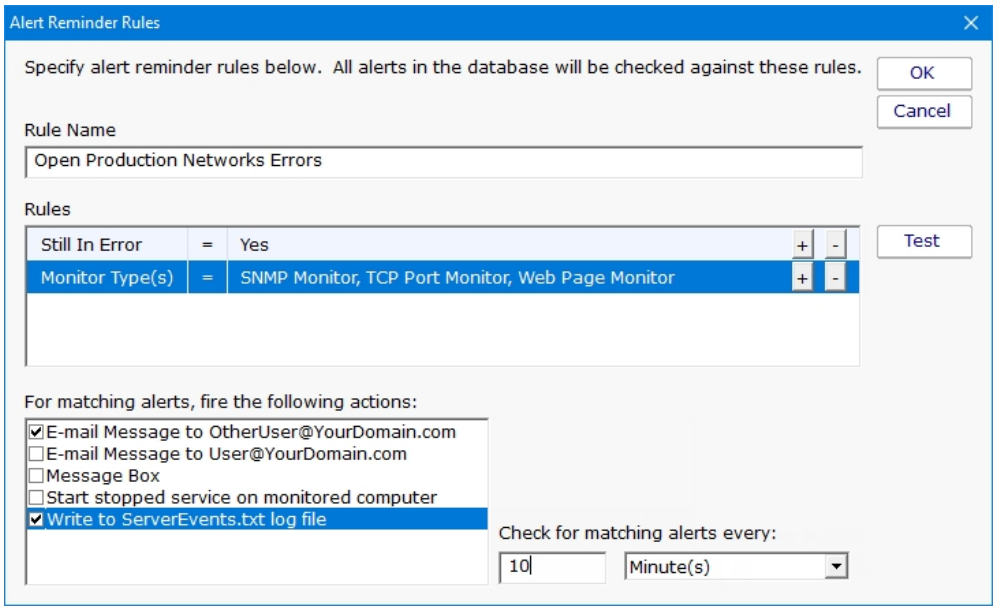
Many of the actions (E-mail, Pager, Message Box, etc) let you customize the message that is sent out when actions are fired. You customize the message by using pre-defined variables. One of the variables is $MonitorMsg$. This is a value that can be defined on a per-monitor basis. Some uses would include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



Alert Reminders

Some times a customer will have alerts or problems that happen which aren't handled immediately, usually because something else of higher priority is being taken care of. But the alerts were defined because they were important so they need to get looked at.

Humans forget, but PA Server Monitor doesn't, so it can be configured to occasionally send reminders. This is especially useful if you are using Event Deduplication and want to be reminded of duplicate events that are being suppressed.



Defining reminder rules is very simple. Just select the fields that describe the set of alerts you want to be reminded on. For example, the field "Still in Error" is something you would probably want to set to Yes. You can alert on acknowledged or not, time when the error first occurred, or the most recent time that it occurred.

The image above just shows a single reminder rule being created, but you can create as many as you need.

Part of the reminder rule is who should receive the reminder. Just check the boxes and you're done.

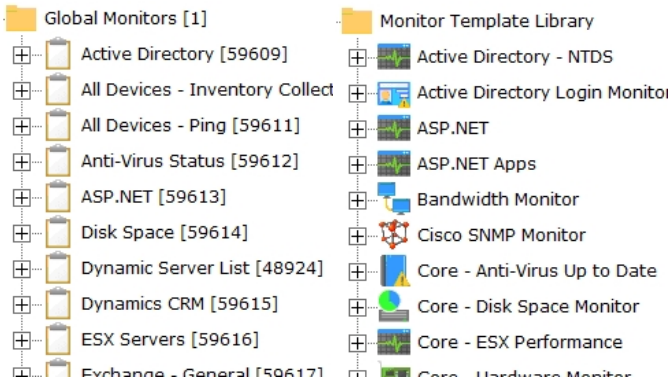
Automatic Configuration

PA Server Monitor can use rule-based automatic monitor configuration, which makes configuring monitors for your environment almost effortless.

Enabling or disabling Automatic Configuration has some big effects. Read more here...

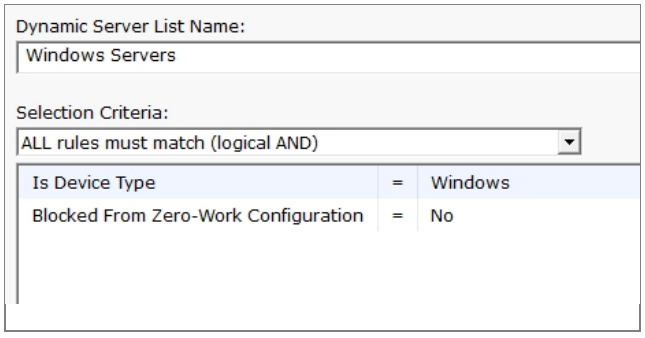
How It Works

A list of Dynamic Server List monitors are created automatically in the Global Monitors list. A list of monitor templates are also created in the Template Library.

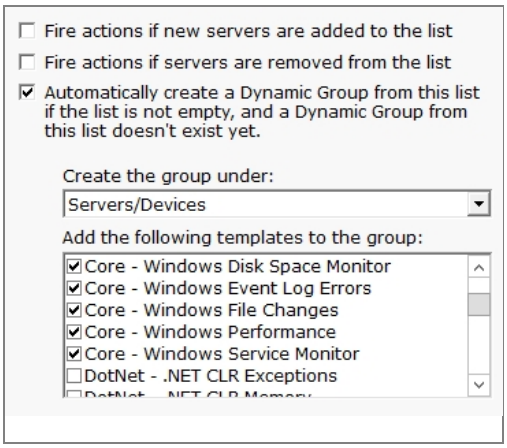


The Dynamic Server List monitors are setup to detect specific server types. In addition, they ignore any servers that are tagged as being blocked from Automatic Configuration (more on that below).

The Windows Server rule which will be applied to all computers that are marked as being Windows is shown below.

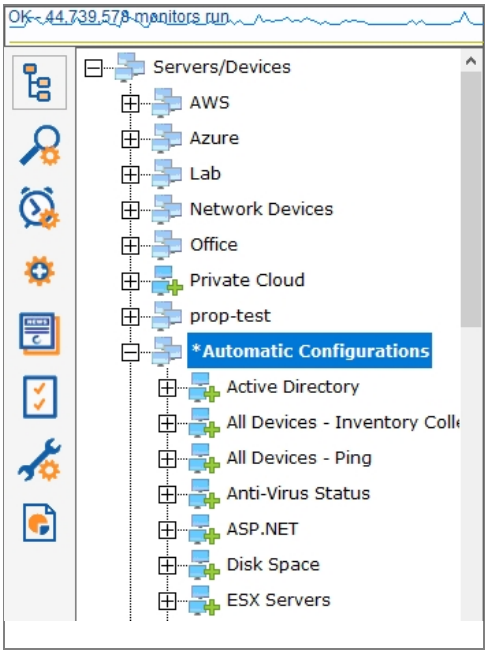


If there are any servers that match this rule, the Dynamic Server List is configured to create a new Dynamic Group that contains the matching servers. In addition, a list of templates will be added as Power Templates to the new dynamic group.



Automatic Configuration Group

The dynamic groups that are created will all be placed in a group named "*Automatic Configurations" (the asterisk in the name causes the group to get sorted to the bottom). This group will be created at the top level under Servers/Devices. The group can be renamed and moved under other groups if desired. The dynamic groups inside it (based on the Dynamic Server Lists) should not be moved out of the Automatic Configuration group.



As servers/devices are added to these groups, the normal operation of copying Power Templates to the servers/devices will take place. That is automatic configuration.

Note that monitor templates are copied from the Template Library to the Dynamic Groups. You can make changes to the templates in the Dynamic Groups and the changes will propagate to the servers/devices. Changes made to the templates in the Template Library will not propagate anywhere.

Over time as servers are added to the monitor system or installed software changes, the global Dynamic Server Lists will automatically update, which will cause the Dynamic Groups to update, which leads to monitor templates being added or removed as needed.

Blocking Automatic Configuration

You may have one or more servers that you don't want automatic configuration to apply to. You can set a "Block Automatic

Configuration" flag on individual servers via:

Bulk Config's "Computers: Set/Reset Block From Automatic Configuration" operation

Right-click a server/device and choose the "Block Automatic Configuration" menu option

The same options above can also be used to unblock Automatic Configuration.

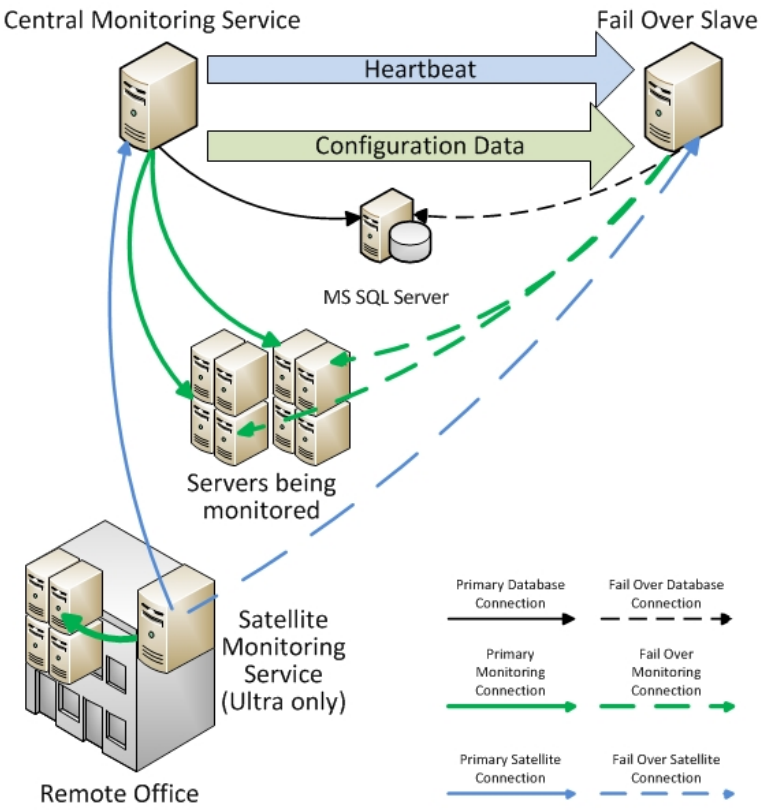
Customize For Your Needs

Automatic Configuration is a concept that you can use as well. All it requires is adding some monitor templates to the global Template Library, and then adding a Dynamic Server List that will decide which servers/devices those templates should be applied to.

Watch the training video How to Configure a Dynamic Server List Monitor.

Automatic Fail Over

The Automatic Fail Over feature lets you create a second monitoring server which will automatically mirror your primary Central Monitoring Service. This Fail Over Slave server will sit quietly and listen for heart beats from the primary monitoring service. If a heart beat isn't received for 5 minutes, it will take over monitoring, alerting and reporting.



Data that is automatically mirrored to the Fail Over Slave are:

configuration database (groups, computers, servers, monitors, actions, reports)

Satellite registration database

application registry settings

System Alert definitions

UserList.txt and LDAP/Active Directory settings for remote access

license file(s)

shared report files (report templates, graphics, maps, etc)

MIB files

language translation files

oemconfig.ini (optional file)

Because all configuration is 'owned' by the Central Monitoring Service, you can connect to the Fail Over Slave with the Console, but won't be able to change much.

Setup

To use the Automatic Fail Over feature, install a second Central Monitoring Service on a second server, just like you installed the original. Don't worry about adding licenses or importing configuration, etc.

Prerequisites

1. The PA Server Monitor service on both servers need to be using the same MS SQL Server. This can be changed in Database Settings.
2. PA Server Monitor on both servers should use the same service account.
3. Use the same version of PA Server Monitor on both servers. You can get the installer from the Central Server at C:\Program Files\PA Server Monitor\Install\Setup.exe.

On the Fail Over Slave

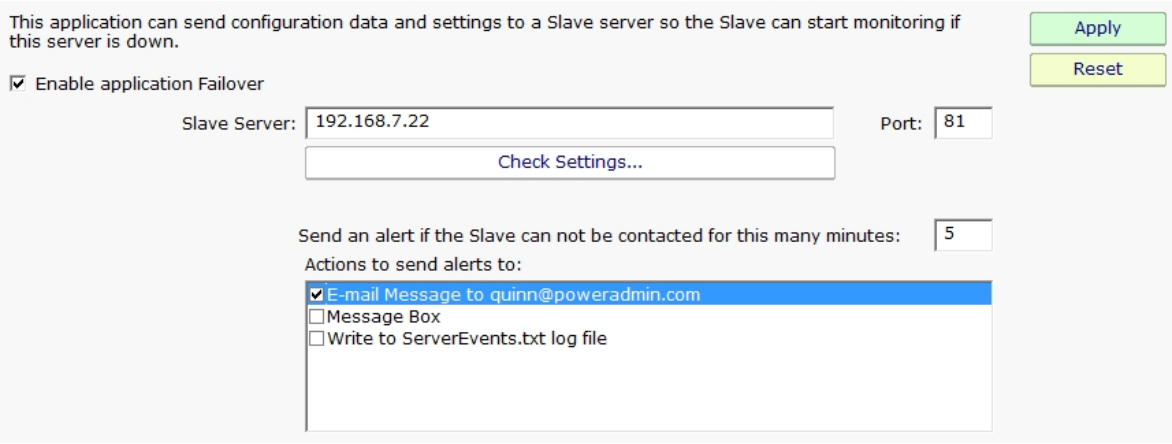
This second installation will be referred to as the Fail Over Slave. On the Fail Over Slave:

1. Start the Console on the Fail Over Slave and connect. Go to Settings and check or change the port if needed.
2. Set HKEY_LOCAL_MACHINE\software\PAServerMonitor [DWORD]FO_IsSlave = 1
3. Restart the PA Server Monitor service
4. Open a browser and point it to https://127.0.0.1:{port}/ to ensure the Windows Firewall is not blocking access

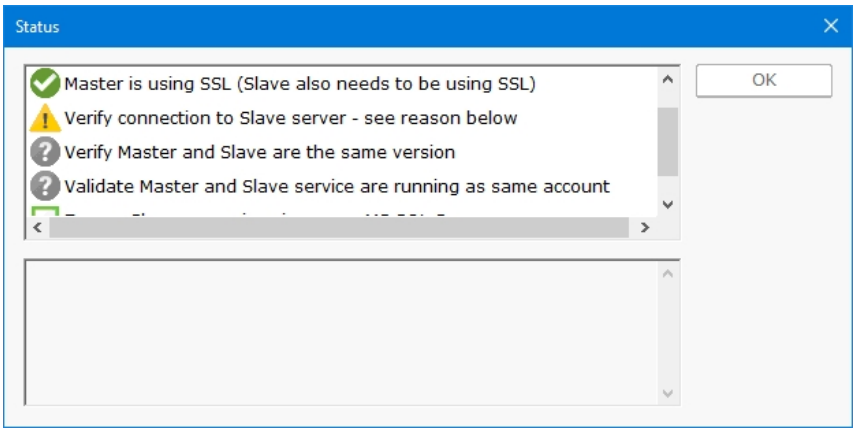
On the Central Server (Master)

Next, get on the main Central Monitoring Service (the Master in the Master-Slave configuration). Start the Console and go to Advanced Services > Failover Status > Configure Fail Over.

You will see the dialog below. Enter the Slave's host name and port.



Press the Check Settings button. This will test the settings on both the Master and Slave. If any items are not green check boxes, select that item to get additional information.



Once all items are green, press OK and the Master and Slave will begin synchronizing configuration information.

Using Satellites?

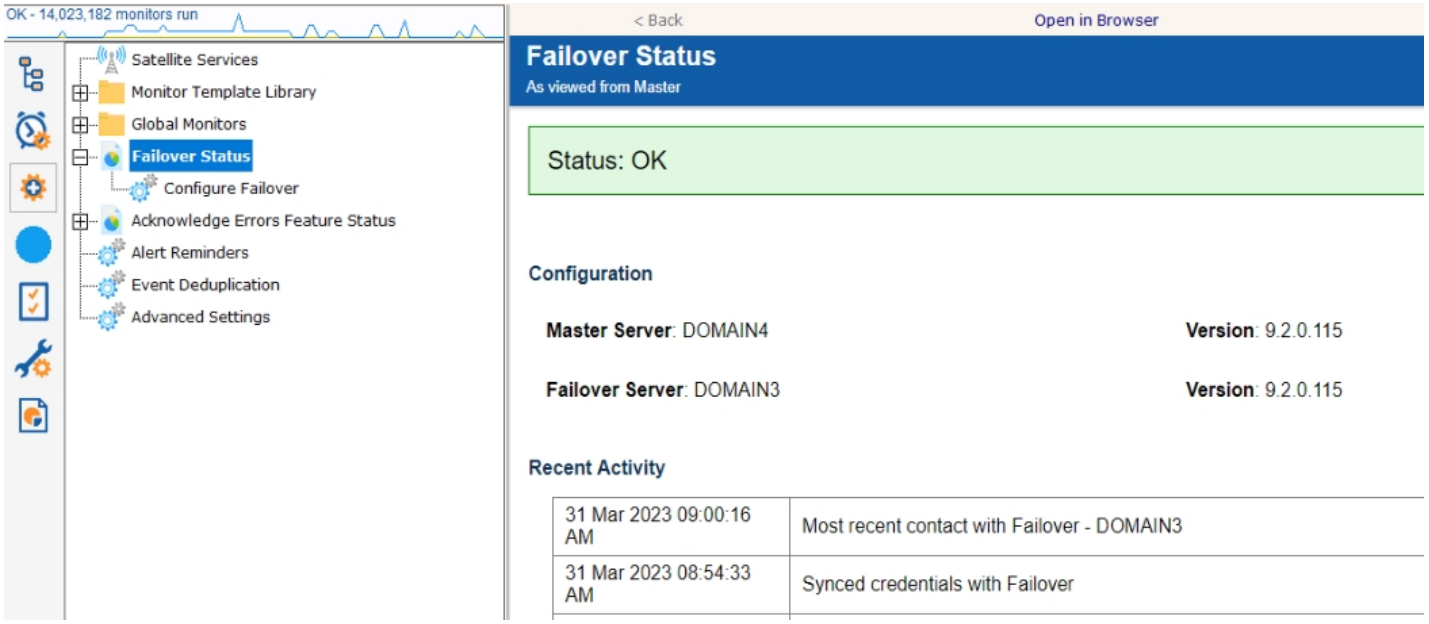
If you are using the Satellite Monitoring Service on other servers, you need to give those other servers the hostname or IP address of the Fail Over Server so the Satellites can switch to the Fail Over Server in the event that the Central Monitoring Service goes down. This can be done in two ways:

Visit every Satellite - you can manually add an additional host:port to each Satellite's configuration application via the Advanced button.

Bulk Config - you can send the Fail Over Server's host:port to all the Satellites using the Bulk Config operation **Satellites: Set Central Server Hosts**. The main host:port is probably already configured on the Satellites, so you'll most likely be setting the Backup 1 host:port entry to point to the Fail Over Slave. Note that Satellite will test the host:port given, and if it can't connect, it will not set the value.

Check Status

The Fail Over Status report will show the Automatic Fail Over system's health and readiness, as well as recent communications between the Master and Slave.



You can click the (Slave's status report) link to see the Slave's view of the fail over system's health.

Failing Over

When the Fail Over Slave hasn't heard from the Central Server for 5 minutes, it will take over monitoring. If there are Satellites, they will automatically switch to the Fail Over Slave within a few minutes after that.

When the Central Server comes back up, the Fail Over Slave will automatically stop monitoring, and any Satellites that were connected to it will automatically switch back to the Central Server after a minute or two.

Command Line Options

Starting PA Server Monitor applications with command line options is not typically needed. They are however useful for automating certain configuration changes.

Console.exe Command Line Options

/AUTO_LOGIN
This option essentially presses the OK button automatically on the login dialog, using whatever settings were previously used.
/PASSWORD={password}
Not recommended, but this can be used to automate logging in to the Console. If PASSWORD, SERVER and USER are all given on the command line, the Console will login automatically without needing to press OK at the login prompt.
/SERVER={hostname}:{port}
Pre-fill the Host name and Port fields in the initial Console connection dialog. This would be useful for creating shortcuts to different installations, or for connection from different locations (such as a laptop connecting from work or from home where the hostname might be different).
/USER={username}
Pre-fill the User name field in the initial Console connection dialog. This would be useful for creating shortcuts to different installations, or for connection from different locations (such as a laptop connecting from work or from home where the hostname might be different).
/FORCE_DEBUG_DUMP
Occasionally Support will request that you obtain a crash dump to send for diagnostic purposes. This command line option will force the monitoring service to crash and create the crash dump file. After the service self-crashes, it will automatically restart and begin monitoring again. The crash dump file will be in the same directory as the product's internal log files -- the directory is shown at the bottom of the Settings dialog.

ServerMonSvc.exe Command Line Options

/ADDSERVER={servername} /WMI={0|1} /WIN={0|1} /CONFIG={full path to exported server config file}
This option allows you to use ServerMonSvc.exe in batch scripts that can add servers to the system to be monitored. This works very similar to the ADD_SERVER command in the External API. WIN and WMI are both optional values that default to 0. If set to 1, it indicates the server is a Windows server and should be polled with WMI respectively.

CONFIGFILE is a required parameter. The configuration file must have been exported from an individual server as explained here.. The configuration in that file will be applied to the named server. If the server does not exist yet, it will be created first.

/DELSERVER={servername}

This option allows you to use ServerMonSvc.exe in batch scripts that might need to delete a server and it's associated monitors. This works very similar to the DELETE_SERVER command in the External API.

/CONFIGFILE={full path to exported server config file}

The same as running: /ADDSERVER={local_computer_name} /CONFIG={full path to exported server config file}

This option is useful for use in installing a configuration from a build script for custom/OEM hardware installations.

/COMPRESS_DATABASES

If you are using the embedded database (see Database Settings), the database is stored as a collection of files. To shrink the database files after having freed up space:

1. Stop the monitoring service
2. Run: ServerMonSvc.exe /COMPRESS_DATABASES
3. After it finishes, restart the monitoring service

/U

Uninstall the PA Server Monitor service. -S can be appended to hide the confirmation dialog.

/I

Install the PA Server Monitor service. -S can be appended to hide the confirmation dialog.

/C

To launch ServerMonSvc.exe directly from the command line (ie, do not run as a service). -S can be appended to hide the confirmation dialog.

/DIAGNOSTICS

Rarely used, this option display a diagnostic dialog for getting some internal system state.

Acknowledge Alerts via Email

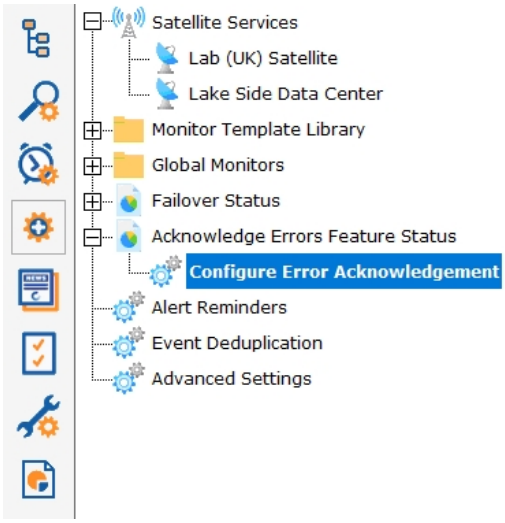
If your organization tracks alerts via Error Auditing, then being able to acknowledge an alert by simply replying to an email is a useful feature. When this feature is enabled:

1. Each alert is assigned a unique ID
2. Emails have the alert ID appended to the subject like this: "Server is down {id:431}"
3. The alert email will come from a special email address that you specify
4. When support staff receive the email alert, they can simply reply to the mail, indicating they acknowledge it. Nothing special needs to be in the message body.
5. The mail box where the replied-to alert goes is scanned for incoming messages
6. Arriving messages are checked for the special ID in the subject
7. If the message has the ID, that alert is acknowledged using the From: field of the message, and the acknowledgement email is deleted to keep the mail box clean.

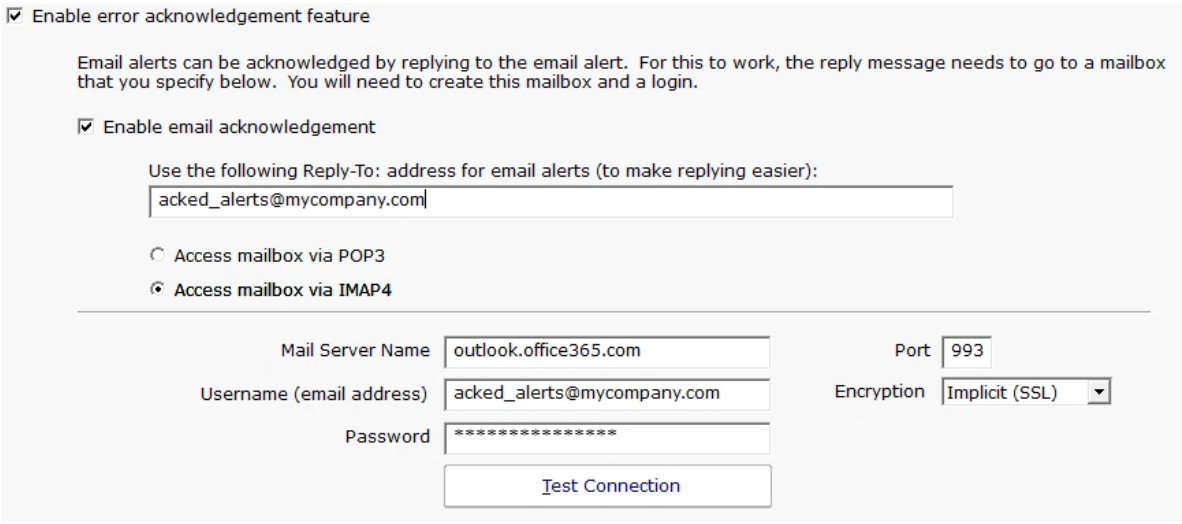
Configuration

Configuring this is very easy. First, you need to create or choose an existing email mail box that will receive the alert acknowledgement emails.

The configuration is available under the Advanced Services group as shown below.



The configuration dialog asks for typical email account information that will allow it to look at the received email messages.



Once Email Acknowledgement is enabled, email alerts will have the ID appended to the subject.

Additional Control

Alerts will not be acknowledged if the reply is an "Auto-Submitted" message, such as a vacation notice. These are detected by the AUTO-SUBMITTED email header that should be present according to RFC 3834.

You can futher control which emails count or don't count as an acknowledgement by changing the following registry values:

Mail_Ack_Keyword - A comma delimited list of keywords to search for. If a keyword contains a * character, the word can be a partial match. So GO* could match GONE or GOING for example. If these keywords are seen, the email is acknowledged. If no keywords are defined (the default case), simply replying to the alert email will acknowledge it.

Mail_Ack_Skip_Keyword - Also a comma delimited list of keywords. If a keyword in this list is found, the reply email does not trigger an alert acknowledgement.

Mail_AckAll_Keyword - A comma delimited list of keywords that defaults to ACKALL. If a keyword from this list is seen, all errors from the computer that sent the alert will be acknowledged.

Two additional registry settings that can be changed:

Mail_Ack_LinesChecked - Defaults to 4. Only this many lines at the top of the email will be checked for Ack commands.

Mail_Ack_Maint_Cmd - Empty by default (so disabled by default). You can give a keyword, such as MAINT, and if MAINT is seen, the next value will be considered a number of minutes to put the servers into maintenance for (example: MAINT 15)

Examples:

Mail_Ack_Keyword: {blank}
Any email received will cause the alert to be acknowledged.

Mail_Ack_Keyword: ACK
Received emails must contain 'ACK' in the first {Mail_Ack_LinesChecked} lines for the alert to be acknowledged. If that is not seen, the alert is not acknowledged.

Mail_Ack_Skip_Keyword: vacation

An auto-responder email is received that contains "I'm out of the office on vacation". It will not cause an acknowledgement.

Mail_Ack_Keyword: {blank}
Mail_Ack_Maint_Cmd: MAINT
An email is received that contains in the first few lines: MAINT 10
The server will be put into Immediate Maintenance for 10 minutes, and the alerts will be acknowledged since no keyword is required by Mail_Ack_Keyword.

Mail_Ack_Keyword: ACK
Mail_Ack_Maint_Cmd: MAINT
An email is received that contains in the first few lines: MAINT 10
The server will be put into Immediate Maintenance for 10 minutes, but the alert will NOT be acknowledged because the required ACK keyword was not seen.

Mail_Ack_Keyword: ACK
Mail_Ack_Maint_Cmd: MAINT
An email is received that contains in the first few lines:
ACK MAINT 15
- or -
ACK
MAINT 15
The server will be put into Immediate Maintenance for 15 minutes, and the alert will be acknowledged.

Mail_Ack_Keyword: ACK*
If an email is received that contains ACKNOWLEDGED, ACK, ACK'D, or ACKNOWLEDGING, the alert will be acknowledged.

Configuration Security

After getting PA Server Monitor configured, you probably don't want anyone making unauthorized changes. There are a few ways PA Server Monitor can help.

Console Password for Local Logins

In the global Settings dialog there is a button labeled Console Security. Using that feature you can assign a password that must be entered everytime the PA Server Monitor Console is started. To clear an existing password, simply get into the Console again and enter an empty password.

This is useful for locking down access to the local Console installed on the Central Monitoring System.

Console Rights for Remote Logins

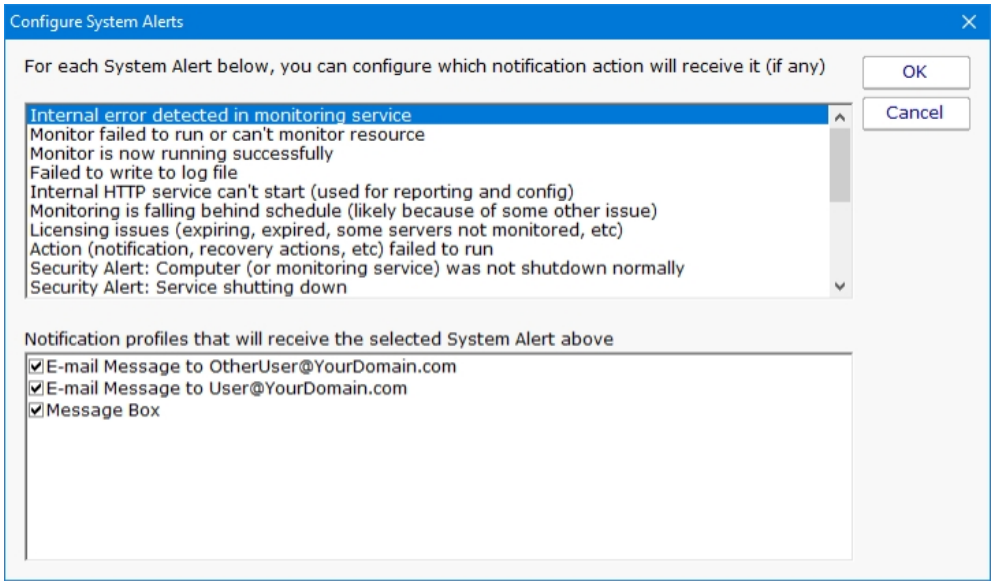
For users logging in with a Console from any where other than the Central Monitoring Service, they will login using a username configured in Remote User Access. Use the "Run Reports" and "View Reports" rights rather than granting everyone "Administrator" rights.

Automatic Configuration Backup

Every time PA Server Monitor starts, and about once a day after that, the entire configuration (except saved credentials) is backed up and saved. By default the back ups are stored in C:\Program Files\PA Server Monitor\Config\Backup.

System Alerts

The Settings dialog also has a System Alerts button which will display the dialog below.



Here you can indicate ways of being notified for a variety of security-related events including:

Configuration changes

Monitoring service shutting down

Computer or service shutdown abnormally (power outage, etc)

Service starting back up

A server entering or leaving maintenance mode (during which no monitoring happens)

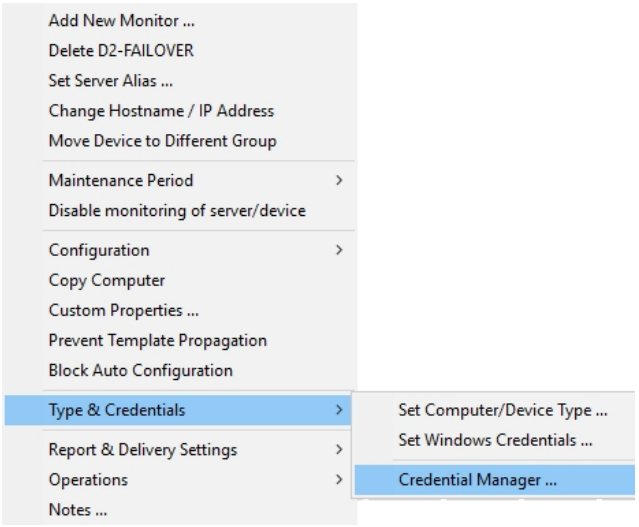
Besides the security related events, there are additional events related to system stability, monitoring integrity and licensing.

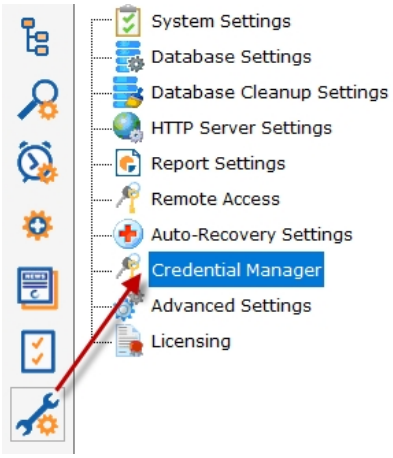
To control the means of notification for the different events, simply choose an event, and then check the appropriate notification means for that event.

Credential Manager

The Credential Manager lets you see in one place the credentials in the system, and allows you to update passwords that have changed, or delete stored credentials.

The Credential Manager is accessed by right-clicking on any device and going to Type & Credentials > Credential Manager, or from the Settings navigation button.





Credentials are groups into different types. Sometimes credentials are used by multiple devices. In this case the credential is attached to a single device, and the other devices point to that single device. The check box at the top toggles between viewing these two scenarios.

To change a credential, select it at the top, make the change on the lower part of the dialog and press the Save Changes button.

A special category of **Custom Credentials** exists for you to enter credentials that aren't being used internally by the monitoring system. This lets you store arbitrary credentials which can be accessed via the Execute Script monitors and actions via the $mon.GetCredentials or $act.GetCredentials methods. See the Protected Settings page for how to enable this.

Credential Security

All credentials are protected using the Microsoft best practice of encrypting them with a machine-specific key, which means they can only be decrypted on the same computer they were encrypted on.

Setting AWS Credentials

Setting AWS Credentials in PA Server Monitor is a slightly different than with other credential types. With AWS, you need to specify a Region and a Device Type, which is discussed below.

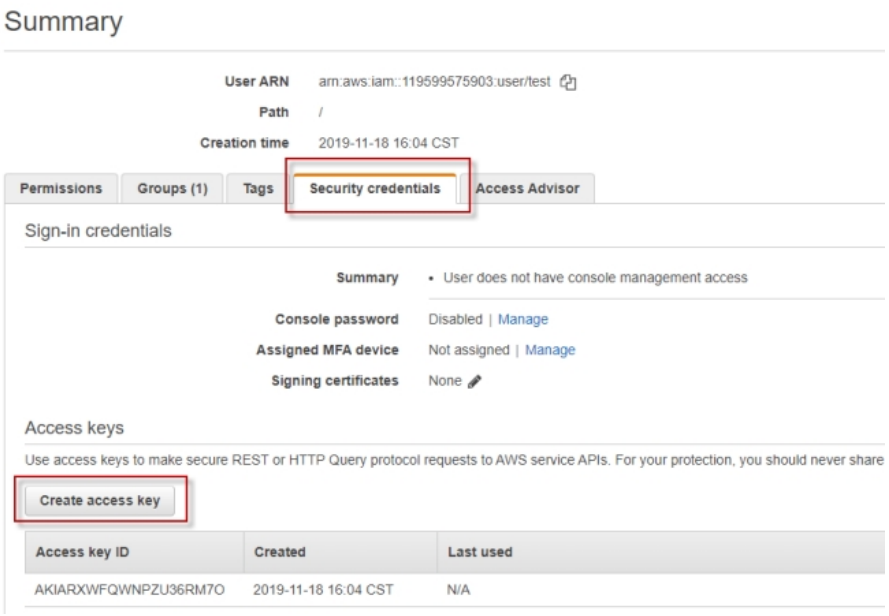
Credentials

Credentials for all AWS devices are a CloudWatch Access Key ID and a Secret Access Key. These are created in the IAM service on a particular user on the Security Credentials tab. The user should belong to an IAM Group with **CloudWatchReadOnlyAccess** permissions. Creating IAM users and groups is not discussed in this document.

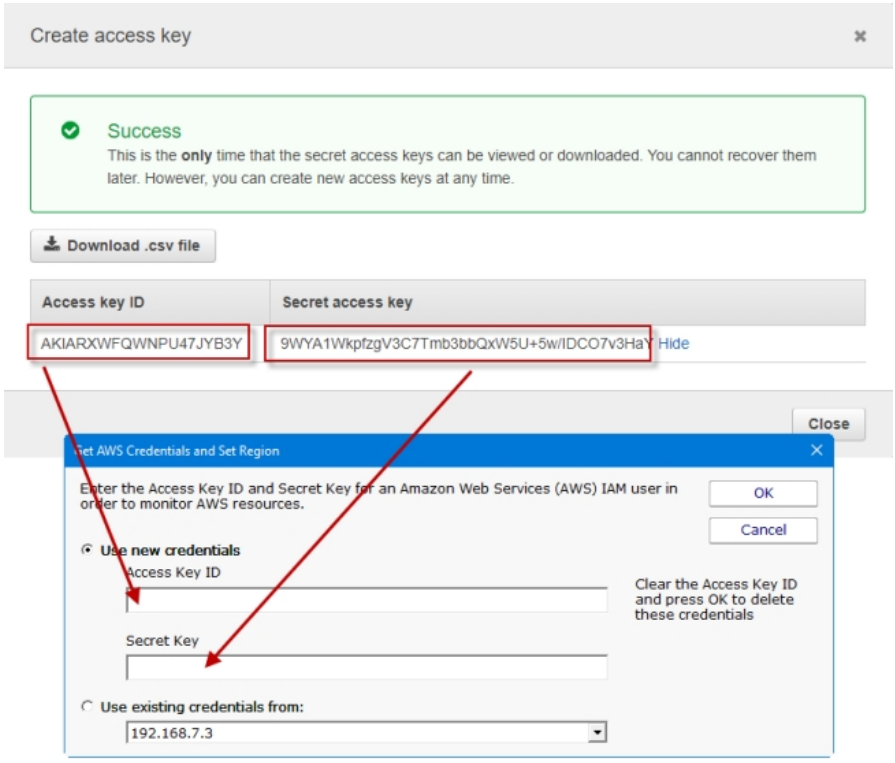
It is recommended to use a separate user account for monitoring. In addition, a single Access Key ID and Secret Access Key can be used to monitor all AWS resources from PA Server Monitor.

Once you have an IAM user account for monitoring, create a new Access Key. Note that each account can only ever have two Access Keys. If you ever want to create a new one you will need to first delete an existing Access Key.

Creating an Access Key is very simple - press the "Create access key" button.

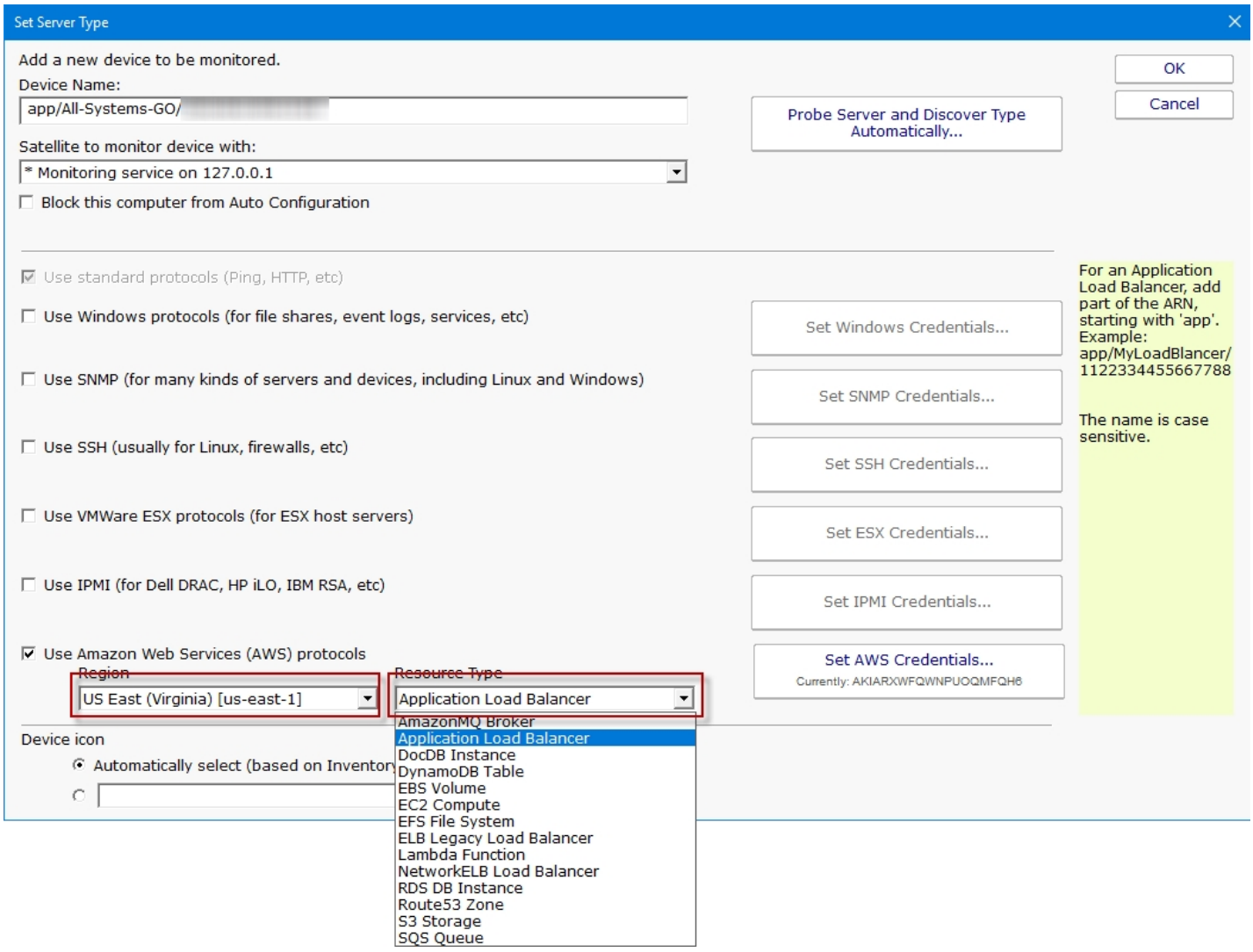


You will be shown the Access key ID and the Secret Access Key. Although you can retrieve the Access Key ID at any time, this is the ONLY time the Secret Access Key is shown, so it must be copied and input into PA Server Monitor at this time.



Region and Device Type

Unlike other monitored resources, with an AWS resource the AWS Region and it's type need to be set. This is done by selecting the appropriate selections from the drop down boxes.



When adding an AWS resource for monitoring, you don't add an IP Address or Hostname but instead add the resource's AWS name. A hint box is shown in yellow to help you know what name to add for the currently selected Resource Type.

Once an AWS resource is added for monitoring, and it has credentials, a Region and Resource Type, you can create a Performance Counter to monitor the AWS CloudWatch counters that are available for that resource type.

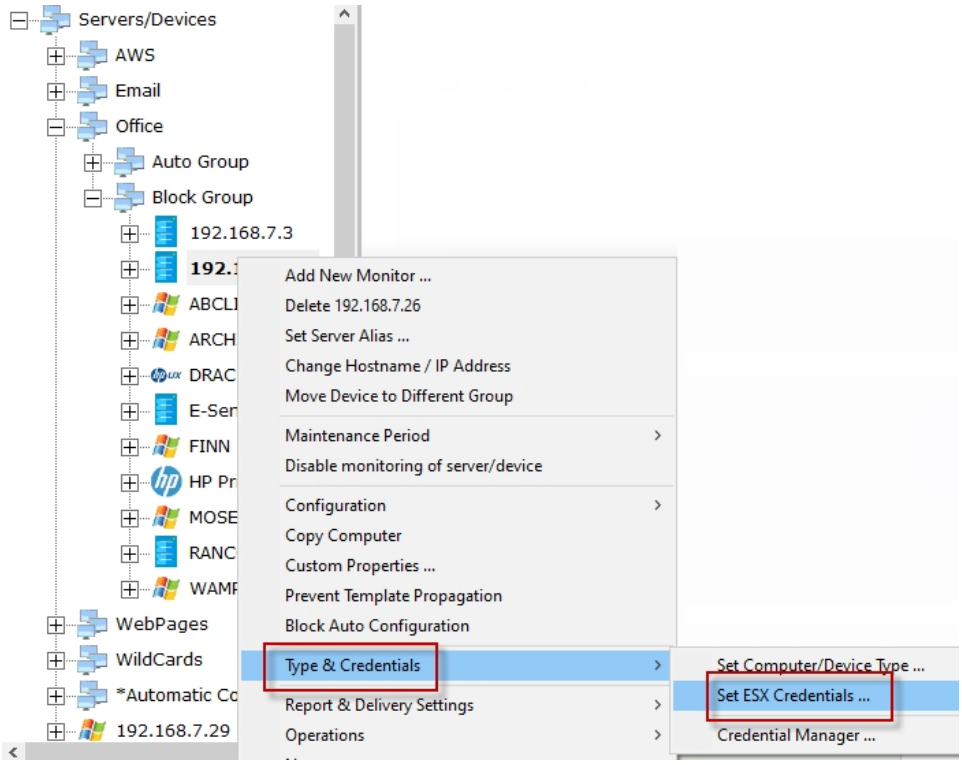
Credential Manager

You can see and update current credentials in the system via the Credential Manager.

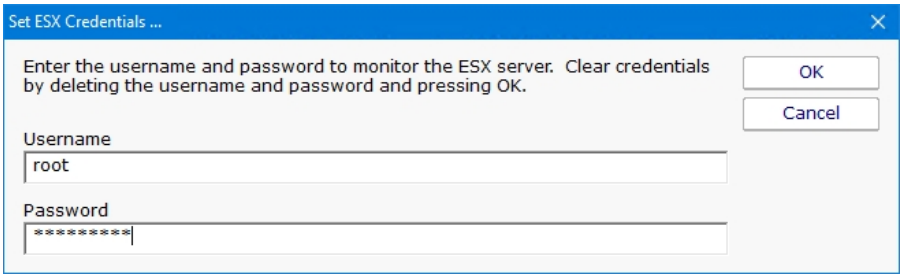
Setting ESX Credentials

PA Server Monitor can associate a set of VMWare ESX credentials with a monitored computer.

The following context menu choice allows you to access the Set ESX Credentials dialog. If you don't see the ESX menu, you need to set the Server Type.



The Set ESX Credentials dialog lets you set ESX credentials that will be used when accessing an ESX server.



When you press OK, the credentials are validated and saved. If you want to clear the credentials, clear both values and press OK.

Credential Security

All credentials are protected using the Microsoft best practice of encrypting them with a machine-specific key, which means they can only be decrypted on the same computer they were encrypted on.

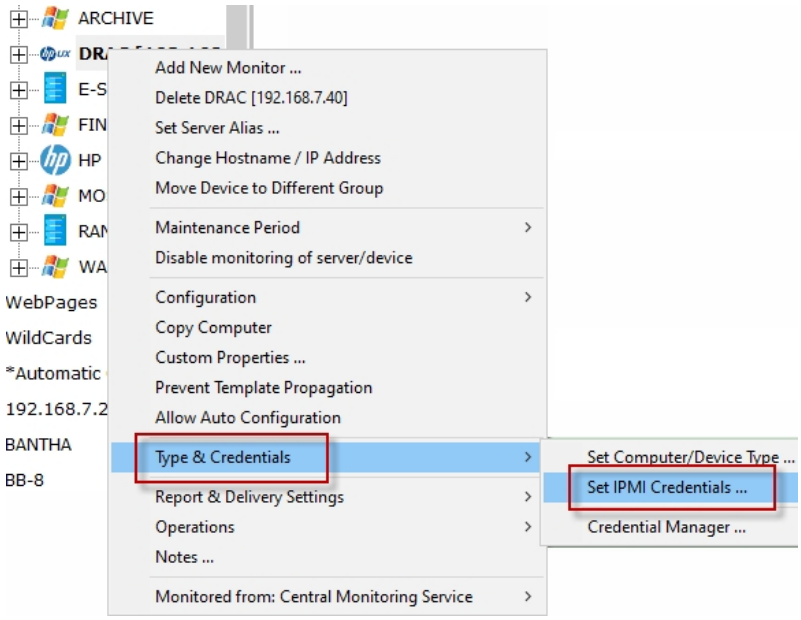
Credential Manager

You can see and update current credentials in the system via the Credential Manager.

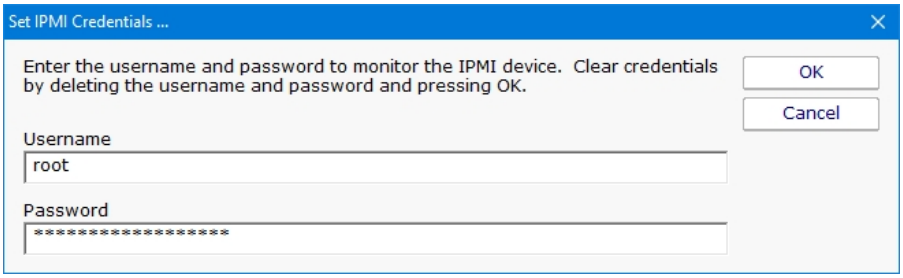
Setting IPMI Credentials

PA Server Monitor can associate a set of IPMI credentials with a monitored computer.

The following context menu choice allows you to access the Set IPMI Credentials dialog. If you don't see the IPMI menu, you need to set the Server Type.



The Set IPMI Credentials dialog lets you set IPMI credentials that will be used when accessing an IPMI device.



When you press OK, the credentials are validated and saved. If you want to clear the credentials, clear both values and press OK.

Credential Security

All credentials are protected using the Microsoft best practice of encrypting them with a machine-specific key, which means they can only be decrypted on the same computer they were encrypted on.

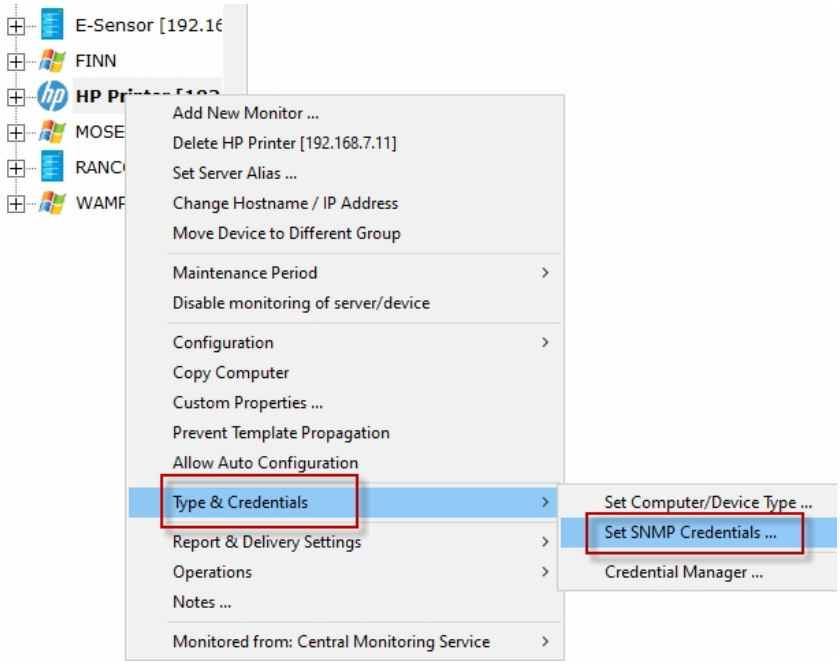
Credential Manager

You can see and update current credentials in the system via the Credential Manager.

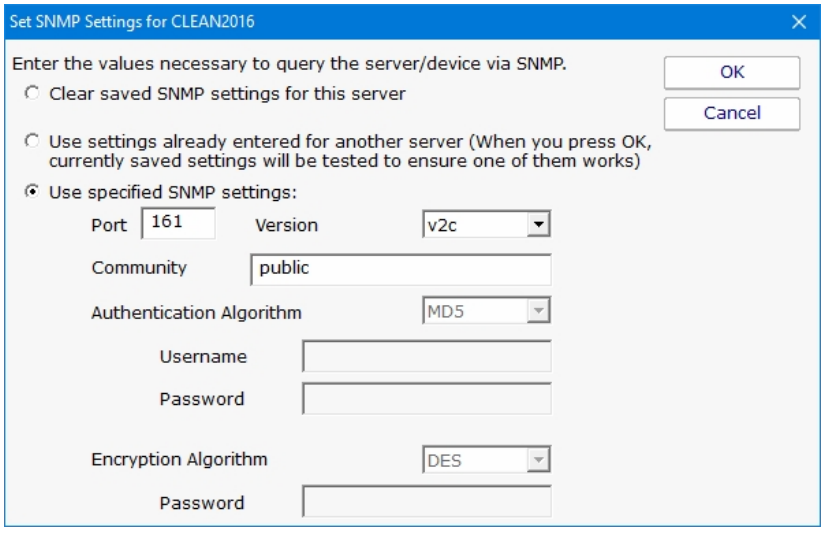
SNMP Credentials

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

The following context menu choice allows you to see the Set SNMP Credentials dialog. If you don't see the SSH menu, you need to set the Server Type.



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



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 credentials are used any time SNMP is used to access the target computer or device on the network.

Credential Security

All credentials are protected using the Microsoft best practice of encrypting them with a machine-specific key, which means they can only be decrypted on the same computer they were encrypted on.

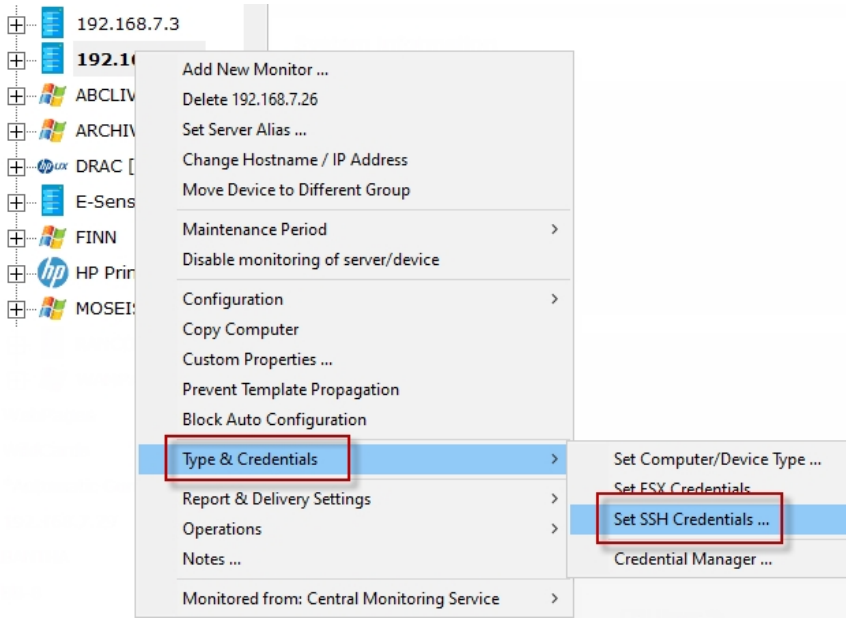
Credential Manager

You can see and update current credentials in the system via the Credential Manager.

Setting SSH Credentials

PA Server Monitor can associate a set of SSH (Secure Shell) credentials with a monitored computer or device.

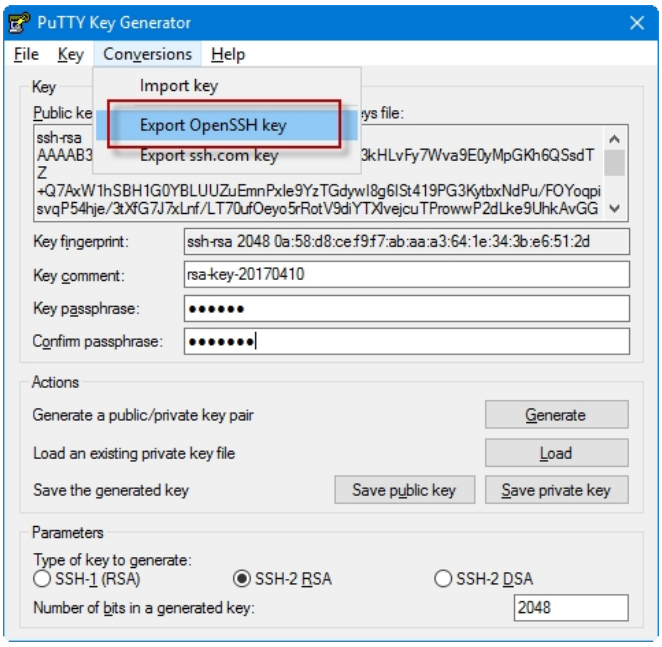
The following context menu choice allows you to see the Set SSH Credentials dialog. If you don't see the SSH menu, you need to set the Server Type.



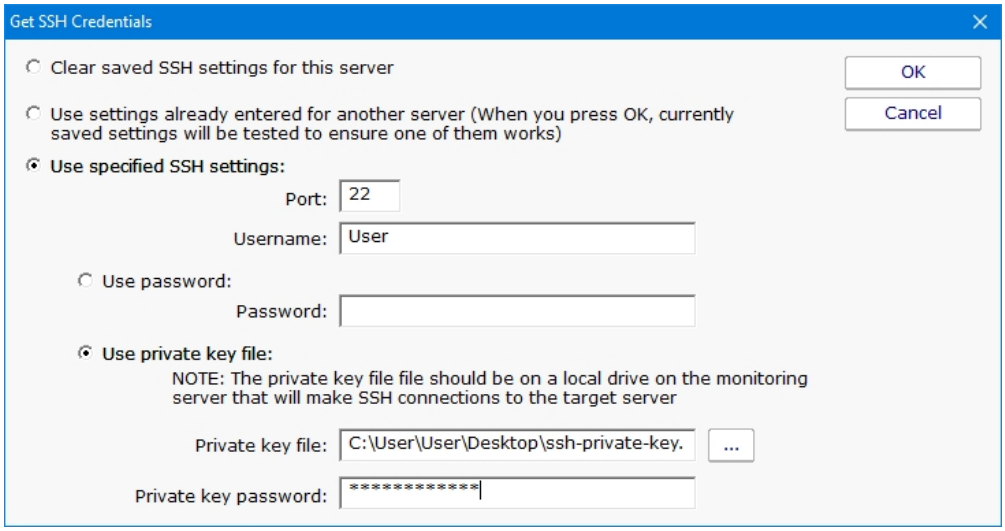
With SSH, you can connect using a username & password, or a username & public/private key. The "keyboard-interactive" login type is not supported.

Public/Private Key File Authentication

If using the public/private key method, the private key needs to be in **OpenSSH format**, and stored on the local machine (the Central Monitoring Service or the Satellite Monitoring Service) that will monitor the target computer. Make sure and give a password for the private key. Public/private keys can be easily created on Windows with the free **PuTTYgen** utility pictured below. Click the Generate button to get started.



The public key needs to be put on the target server. Where and how to do that for any particular server/device is beyond the scope of this document, though there is an example on our blog for enabling SSH logins with public/private keys [on our blog.]



Credential Security

All credentials are protected using the Microsoft best practice of encrypting them with a machine-specific key, which means they can only be decrypted on the same computer they were encrypted on.

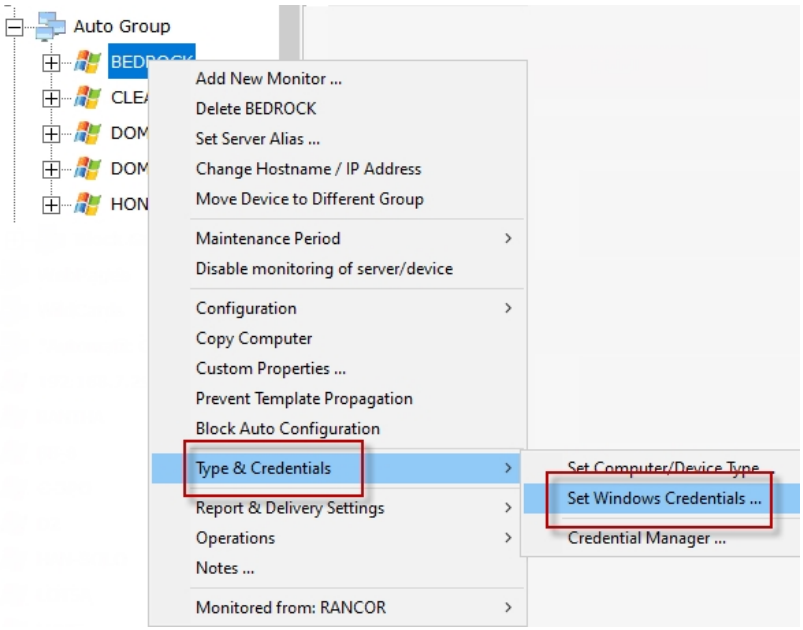
Credential Manager

You can see and update current credentials in the system via the Credential Manager.

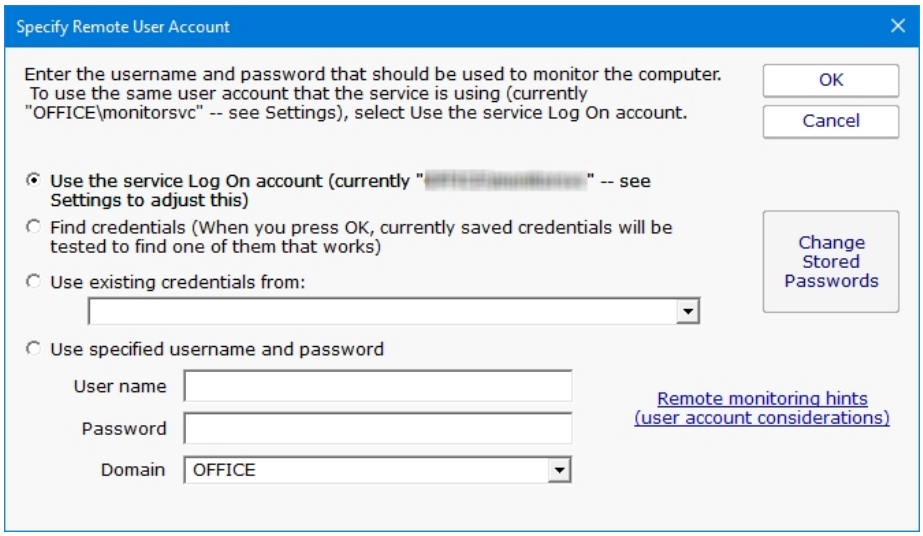
Setting Windows Credentials

PA Server Monitor can associate a set of Windows credentials with a monitored computer.

The following context menu let you access the Set Windows Credentials dialog. If you don't see the SSH menu, you need to set the Server Type.



You can enter credentials, or just monitor the server using the login that the monitoring service is already using. The middle radio button is a convenience feature -- it lets the system try already-entered passwords to find one that works.



When you press OK, the credentials are checked by trying to access the target server's Event Log and the list of running services. If this succeeds, the credentials are saved.

The help page Remote Monitoring Hints has some advice and information about user accounts when monitoring Windows servers.

Credential Security

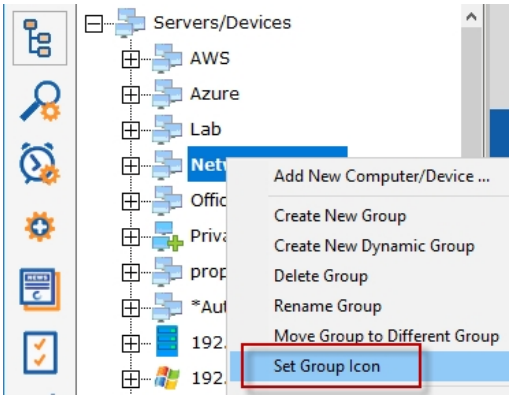
All credentials are protected using the Microsoft best practice of encrypting them with a machine-specific key, which means they can only be decrypted on the same computer they were encrypted on.

Credential Manager

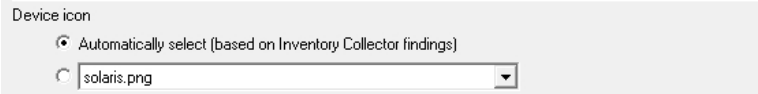
You can see and update current credentials in the system via the Credential Manager.

Custom Icons

The PA Server Monitor Console can show custom icons for servers/devices and groups.



To set the icon on a group, right-click the group and choose Set Group Icon.



To set the icon on a server/device, right click the server/device and go to Type & Credentials. At the bottom of the dialog is a setting for the device icon. By default the icon will be chosen based on rules applied to what the Inventory Collector monitor finds.

Icon Files

You can add your own icon images by copying a .PNG file to C:\Program Files\PA Server Monitor\Icons. The images should be 40 pixels wide by 40 pixels tall.

When you add an icon file, be sure to add an entry to the C:\Program Files\PA Server Monitor\Icons.INI file. The file contains instructions on the simple format.

Icon Rules

To control which icons are automatically chosen for a server/device, edit C:\Program Files\PA Server Monitor\Icons.INI

You can look in that file, and Icons_Default.ini to see the format. Only edit Icons.ini since Icons_Default.ini will get overwritten with future updates.

Syncing

About once an hour remote Consoles will automatically sync the Icons.INI file and any new images in the Icons folder. This synchronization also happens shortly after the remote Console logs in.

Custom Properties

Custom Properties are name-value pairs that can be set on a Satellite, Group, Computer/Device or Monitor. Custom properties can be used in:

Many Monitors
: An Execute Script monitor can read a Custom Property and make decisions based on it's value. See below for more examples.

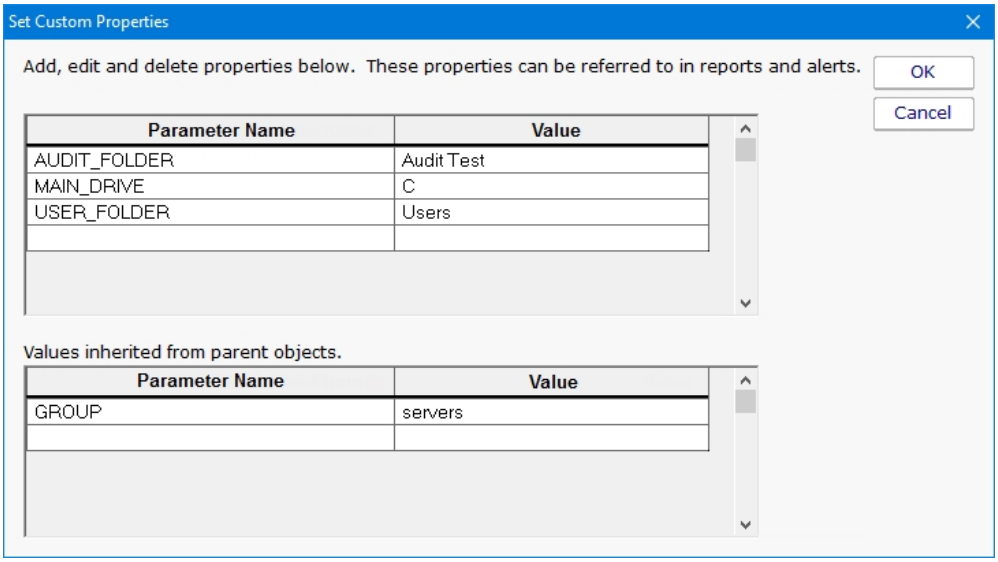
Some Actions
: Custom Properties can be used in email templates.

Dynamic Groups
: Dynamic Groups, based on Dynamic Server Lists can be based on Custom Properties.

Reports
: Some reports, such as the Error Audit Report, can use Custom Properties as a way to select which items to report on.

External API
: The External API can get and set Customer Properties on servers/devices (see the SET_SERVER_PROP and GET_SERVER_PROP functions).

Custom Properties are set in the Console by right-clicking a Group, Computer or Monitor and choosing Custom Properties.



The above example shows Custom Properties on a Computer. AUDIT_FOLDER, MAIN_DRIVE and USER_FOLDER are all defined on the Computer. GROUP is defined at a higher level and is inherited by this Computer. If this Computer also had a value named GROUP defined, the Computer's value would be used (in other words, the closest definition of Property value is used).

Custom Properties can be accessed via the CustomProperty and SetComputerCustomProp in Execute Script monitors and Execute Script actions. They can also be set via the External API via the **SET_SERVER_PROP** and **GET_SERVER_PROP** functions.

Custom Properties can be used in message templates via the $CustomProp(*property_name*)$ replacement variable.

Directory paths in the following monitors can contain the $CustomProp(*property_name*)$ replacement variable:

Disk Space Monitor

Log File Monitor

File Age Monitor

File & Directory Change Monitor

File/Directory Size Monitor

Directory Quota Monitor

An example of the above would be to have a monitor check this folder:

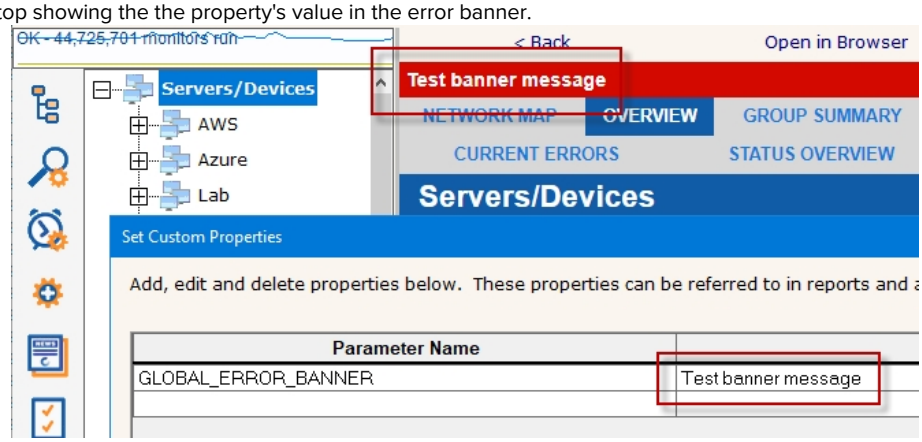
```
\\SERVER\FILE_SHARE\$CustomProp(AUDIT_FOLDER)$
```

Pre-Defined Custom Properties

The below list of Custom Properties have specific meaning to the system, which you can take advantage of.

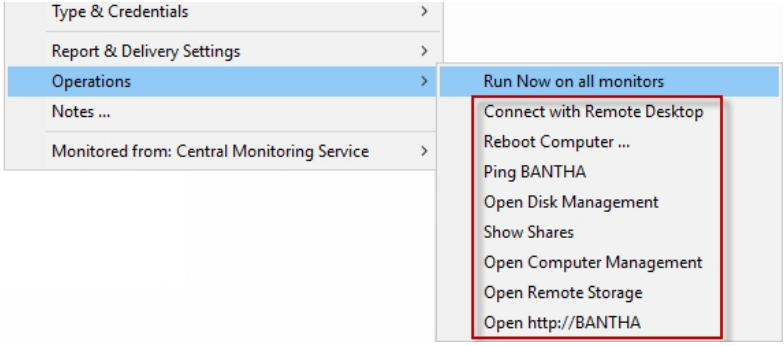
GLOBAL_ERROR_BANNER

When a global error happens, such as a database error, a red error banner is shown across the top of group-level reports. If this property is set, the value of the property will be shown in the red error banner. Note that real error messages will preempt the showing of this property's value. Clear the property to stop showing the the property's value in the error banner.



Customize the Console's Operations Menu

When you right-click a server in the PA Server Monitor Console, there is an Operations menu which can do various things to the selected device.



The list of commands can be changed, including adding commands for your own specific situation.

To edit the commands, use a text editor and open:

```
C:\Program Files\PA Server Monitor\Console_Operations.ini
```

The file contains complete information on how to make changes.

Distributing Changes

The Console_Operations.ini file gets synchronized from the central monitoring service out to remote Consoles about every hour or so, and immediately after the Console logs in. So be sure to make changes to this file on the central monitoring service.

Error Auditing

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

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

Three Pieces

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

There are three parts to Error Auditing:

1. Product monitors run and detect issues. Alerts are optionally fired and details are written to the database. The error details, source device, time, etc are all recorded to an error database.

2. Server administrators view server status reports and note recent errors. They check the Ack box next to the error indicating that they have reviewed and acknowledged the error. Their acknowledgement is recorded in the database along with the error details.

3. Administrators, management or compliance officers can run high-level Error Audit reports to make sure errors are being reviewed and acknowledged by server administrators. The Error Audit reports can be broken down by:
   - source computer or device
   - computer group
   - resource type (disk space, services, ping response, etc)
   - acknowledgement state (acknowledged or not yet acknowledged)
   - error type

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

More Details

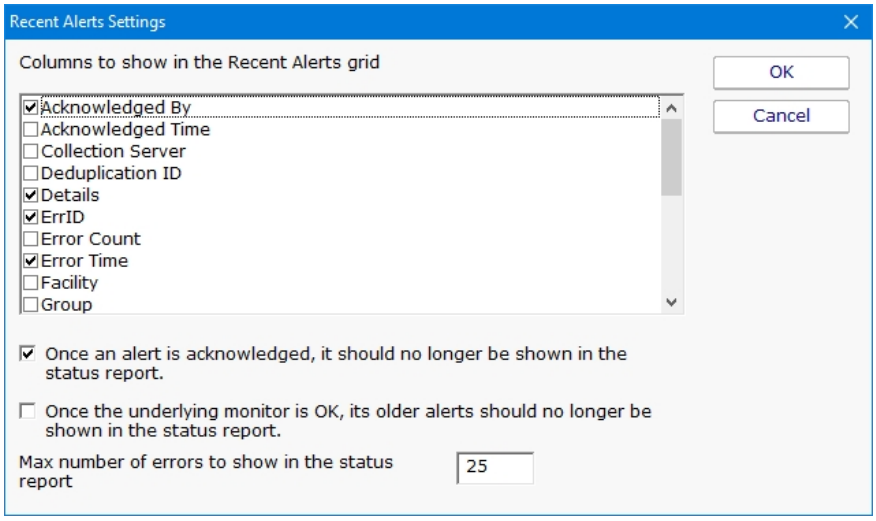
1. Product monitors detect and record issues

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

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

Some problems are transitory (a new event in the Event Log, a change to a file, etc). Alerts would be fired, but the monitor wouldn't stay yellow since on the next run everything looked OK, so 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. Then double click on the Recent Alerts in the Displayed Report Items column.



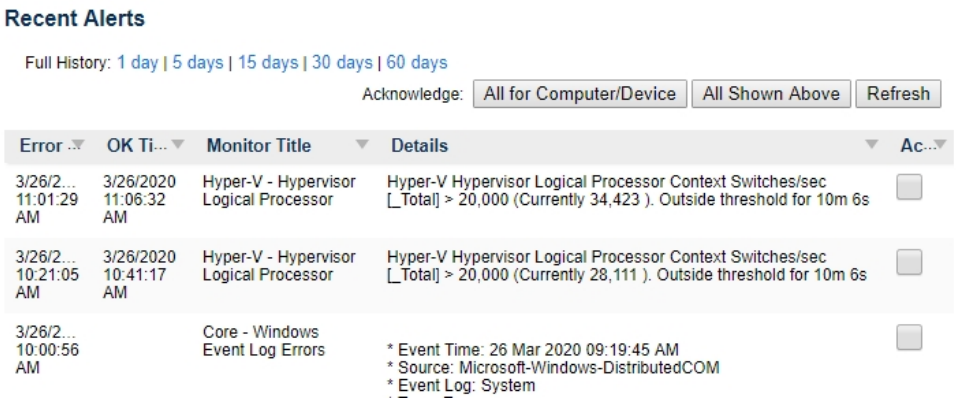
Additional options in this dialog control what is displayed in the Recent Errors section at the bottom of the server status report

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 Alerts 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, a 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.

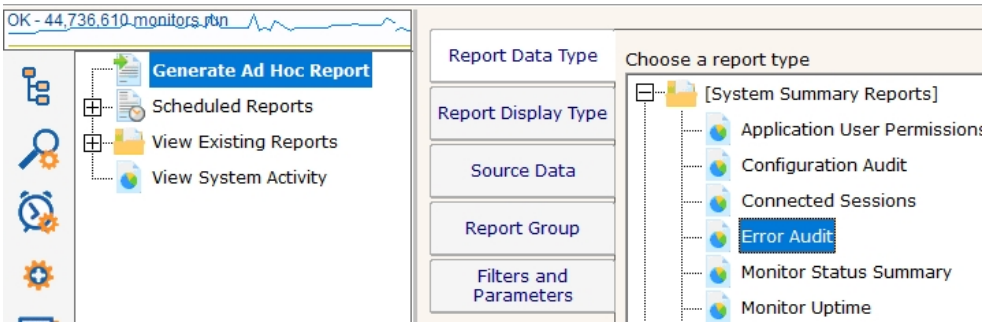
There are additional methods to acknowledge alerts.



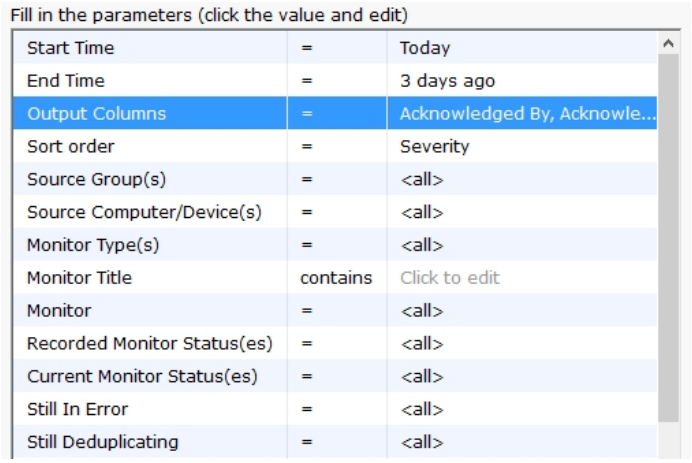
Administrators will often not want to see the error again once they've acknowledged it. This can be controlled via the Report Settings dialog mentioned above.

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.



More information about the Error Audit Report

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.

Create a scheduled Error Audit report for different team members that have responsibility for different areas of your network. They can save the URL in their browser's Favorites and quickly check and see if anything needs to be done.

Event Deduplication / Aggregation

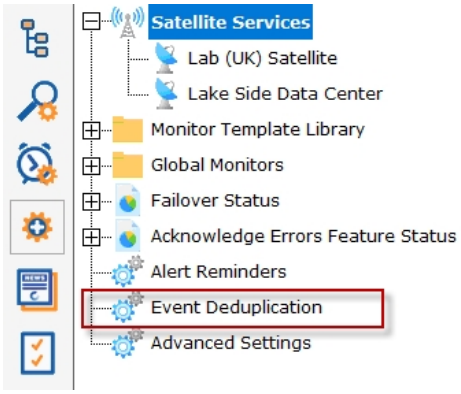
Event Deduplication (also known as Event Aggregation) is a technique for detecting that a new incoming alert (event):

1. is similar to an existing event that has already been reported
2. suppressing the duplicate alert

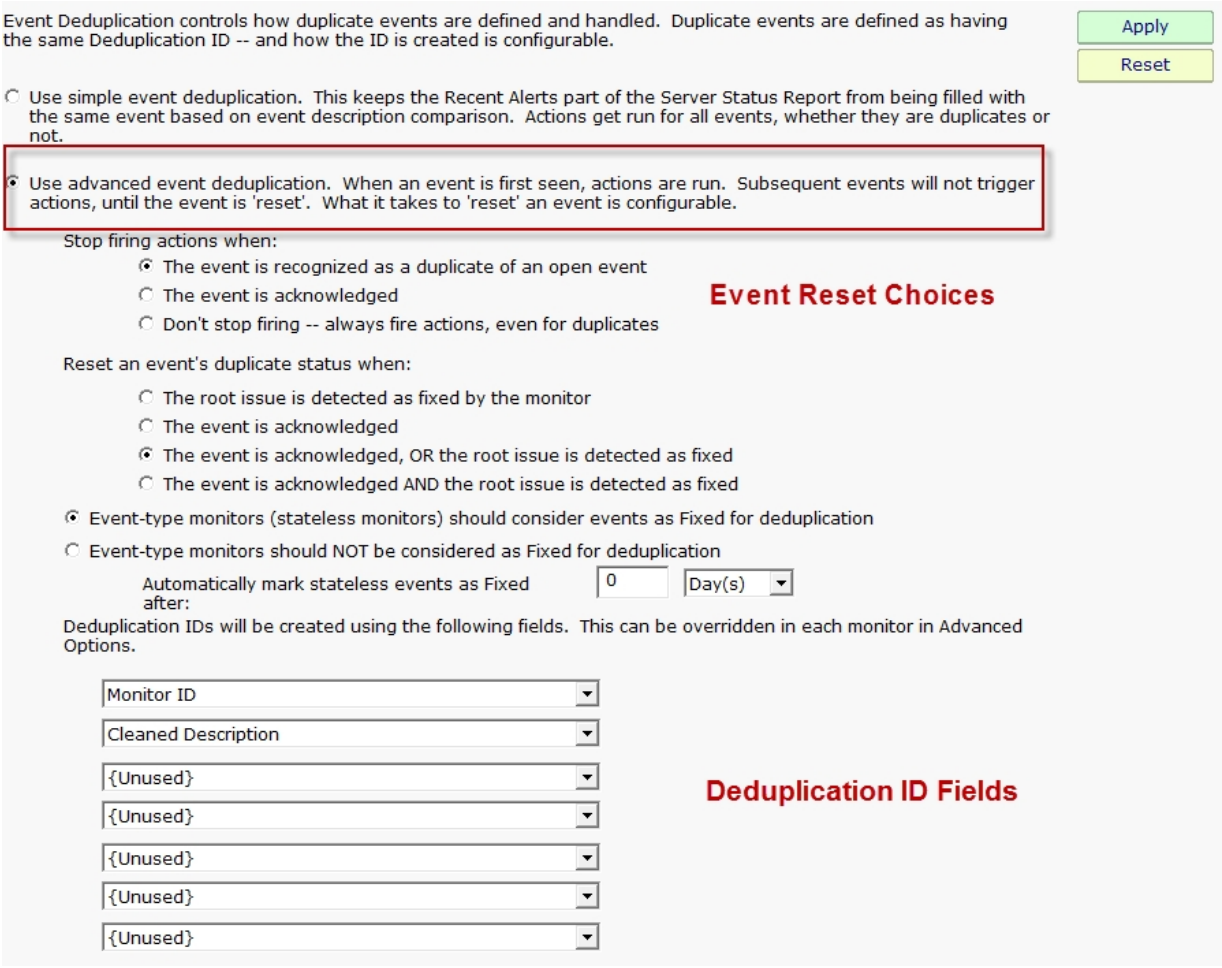
This is somewhat related to Alert Suppression and Event Escalation, but allows finer and configurable control over when to suppress an alert.

See Alert Suppressing, Event Escalation and Event Deduplication to see how these features can be used together for suppressing alerts.

Event Deduplication can be configured in the Advanced Services part of the Console.



Here you can select between the default Simple event deduplication (which doesn't do very much deduplication), or advanced event deduplication. Advanced Event Deduplication is what this page will describe further.



Event Reset

The first thing to decide is whether or not to alert when a duplicate event arrives. Usually the new event would be shown if the previous event situation has been 'reset', meaning the system will no longer consider new events duplicates of the previous event because something has changed. Usually this means the previous event was acknowledged, or the underlying error was fixed. If this is the case, and a new event arrives, it should not be considered a duplication but rather a new situation that should be alerted on again.

State vs Event-type events

Some events are 'state' events, meaning they are in a good or bad state (responding to ping or not responding to ping, low disk space or OK disk space, etc). Those are easy to define as 'Fixed' or not.

Other event types are stateless, or Event-type events, meaning they happened, but don't represent a good or bad state. An error listed in the event log, an error received via SNMP Trap or syslog, or a change detected in a file are such situations. These are not good or bad states, they simply occurred.

For Event-type events, you decide how to consider them 'fixed' for use in Deduplication resetting. You can consider them immediately fixed, or fixed after a certain amount of time.

Deduplication ID

The key principle to understand is the Deduplication ID. The Deduplication ID is a text string that represents the essence of the event. If two events have the same Deduplication ID, they are considered the same event for Event Deduplication purposes. You will therefore want to define the Deduplication ID so it combines events that you want considered the same.

For example, the default fields used are:

Computer ID - an internal unique ID assigned to each monitored computer

Monitor ID - an internal unique ID assigned to each monitor

Cleaned Description - the event description text with user names, paths, dates, amounts, etc removed

With these default settings, the two events below would be considered identical, and thus the second event would not fire alerts when using Advanced Event Deduplication:

```
21 Feb 2014 09:05:56 PM
Computer: [3271187]
Monitor: [Low Disk Space]
Description:

Free disk space on F: is below the threshold of 5% (Currently 4%, 11.6 GB)
```

```
21 Feb 2014 11:05:53 PM
Computer: [3271187]
Monitor: [Low Disk Space]
Description:

Free disk space on F: is below the threshold of 5% (Currently 3%, 8.7 GB)
```

These are identical because the events are for the same computer and from the same monitor, and the Cleaned Description field (after removing dates, times amounts, etc) is the same too -- they are about low disk space on the same drive on the same computer.

Peeking at the database...

ErrID	Src...	MonitorTitle	MonitorID	ActionDescription	ErrCount	DedupeID
1355785	130	Execute Script	1518	Testing Execute Script monitor	653	C130-M1518-CD3404619332
1430360	31	Inventory Collector	79	Failed to retrieve system details vi...	31	C31-M79-CD2925635685
1473765	130	Monitor services on...	1006	The service "Performance Logs ...	6520	C130-M1006-CD2994397729
1483278	129	Very Low Disk Spa...	992	\\TEST-1\C$ < 10 % (Currently 0...	773	C129-M992-CD1844245446
1483280	130	Very Low Disk Spa...	1000	C:\ < 10 % (Currently 4 %, 344.7 ...	767	C130-M1000-CD2011771327
1499354	120	Inventory Collector	592	Failed to retrieve system details vi...	14	C120-M592-CD3826456382
1499637	129	Critically Low Disk ...	993	\\TEST-1\C$ < 3 % (Currently 0 ...	287	C129-M993-CD1844245446
1499639	130	Critically Low Disk ...	1001	C:\ < 5 % (Currently 4 %, 371.4 MB)	268	C130-M1001-CD1844245446

The image above shows some of the fields in the Error History table. Deduplication IDs are shown at the right side. Notice the ErrCount column -- that shows how many incoming alerts were considered duplicates of the shown alert. Instead of alerting on that incoming event, the ErrCount column was incremented and no alerts were fired. If you think you might want a reminder about events that have not reset and thus are suppressing new incoming alerts, look at the Alert Reminders feature.

Global with Override

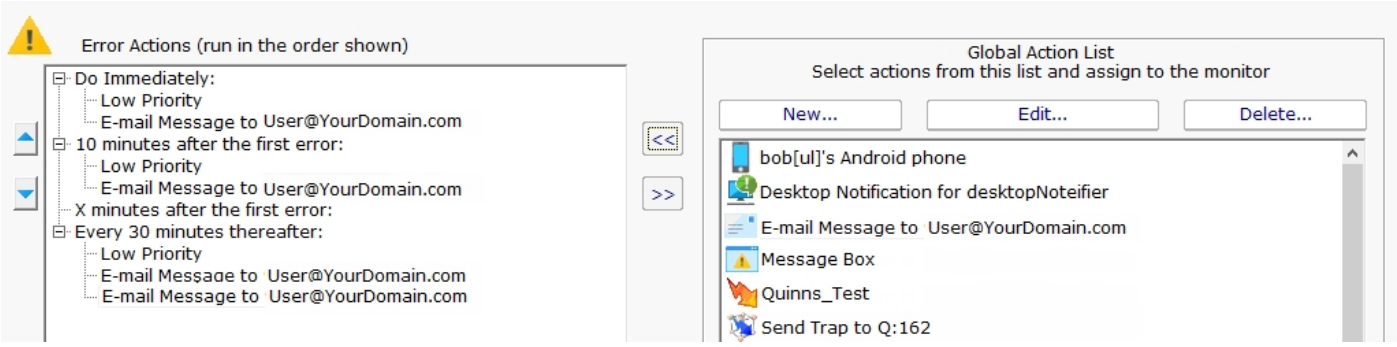
This setting is a global setting that applies to all monitors. Individual monitors can define their Deduplication ID in a unique way to give added flexibility. This is done in Advanced Monitor Options (bottom of the page).

Event Escalation

NOTE: Event Escalation is only available in the Pro and Ultra editions.

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.

See Alert Suppressing, Event Escalation and Event Deduplication to see how these features can be used together for suppressing alerts.

Variables

A number of the actions accept variables to alter their output. The messaging actions (E-mail, Message Box, Network Message, Pager Alert, and SMS Message) can all accept variables in their message template. In addition, the executable actions (Execute Script and Start Application) can also accept variables to change the action at run time.

Replacement Variables

The variables below can be inserted into the action or the message template as shown. The one exception is the Execute Script action -- in that case, the starting and ending $ are not used.

Variable Modifications

Most variables support replacement and truncation using this format:

`$Details['a','b']$`	replace character 'a' with character 'b' in the value of Details before using it as a replacement value.
`$Details["abc","xyz"]$`	replace string "abc" with "xyz" in the Details's value before using it as a replacement value.
`$Details[50]$`	Truncate the value to 50 characters before the replacement

Note that these can also be combined such as:

`$Details['"',' '][60]$>`	Replace quote characters with a single space, and truncate to 60 characters
`$Details['!','~']["\r\n",""][70]$>`	Replace pipe characters with tilde characters, remove newline combinations, and truncate to 70 characters

General Variables

The following variables are always available. Please note that variables are case sensitive.

Variable	Meaning
$AlertCharts$	This value will be replaced with charts if any are available for the alert. This variable only works with Email Actions.
$AlertID$	A unique integer that represents this particular alert.
$CustomProp(propName)$	The value for a custom property for the target monitor, computer or containing group. Empty if the property is not defined. See below for more details.
$Date$	Current date in string format
$Details$	Text describing the result of the monitor. This is what most other actions display/report. If you want the Details value to be on a single line, use $Details_Single_Line$
$Details_Single_Line$	The Details variable with everything on one line (line breaks removed)
$Details_Single_Line(x)$	The first X characters of the Details variable. Useful for trimming the value to a specific length.
$Group$	The group that contains the computer where the monitor detected the issue
$GroupPath$	The full group path (ie Group1\Group2\Group3) that contains the computer where the monitor detected the issue
$Machine$	The computer where the monitor detected the issue
$MachineIP$	The IP address of the computer where the monitor detected the issue. Defaults to 0.0.0.0 if the value can't be determined.
$MachineID$	ID of the computer involved. Defaults to 0 if the value can't be determined.
$MachineAlias$	The aliased computer name (if an alias was entered, otherwise the same as Machine above)
$MonitorTitle$	Title of the reporting monitor

$MonitorMsg$	Custom message text from the originating monitor. This can be set in the monitor's Advanced Monitor Options
NL	New Line character
$ProdVer$	Current version of this program
$MonitorType$	The type of monitor that detected the issue. This is the same text as you see in the list when choosing to create a new monitor.
$Status$	Status of the monitor. *(See table below for possible values.)*
$StatusText$	A cleaner version of Status. See table below for possible values (note that some values are rarely seen).
$Time$	Current time in string format
$TimeInError$	Amount of time that a monitor is or was in error. Ex: "Was in error for 1h 2m 3s"
$WinDir$	WINDOWS directory for the target computer

Status	Status Text	Meaning
msOK	OK	Monitor is OK
msALERT	Alert	Monitor is in alert state because of what it found
msALERT_GREEN	Alert (Green)	The monitor is in Alert state, but has been configured to remain green anyway.
msALERT_RED	Alert (Red)	The monitor is in Alert state, but has been configured to turn red.
msSUPPRESSED_ALERT	Suppressed Alert	The monitor is in Alert state, but actions are being suppressed via Alert Suppression settings.
msUNACKNOWLEDGED	Unacknowledged Alerts	OK state, except there are unacknowledged errors and Error Acknowledgement is enabled
msERROR	Internal Error	The product is not functioning correctly. This is not usually a monitor status, but used for global problem broadcasts.
msSUPPRESSED_ERROR	Suppressed Error	The monitor is in ERROR state, but Alert Suppression settings are keeping it from firing actions.
msCANTMONITOR	Can't Run!	The monitor is unable to perform its function, possibly because of lack of rights or access.
msDISABLED	Disabled	The monitor is currently disabled
msRUNNING	Running	Monitor is currently running.
msINIT	Scheduled	All monitors are set to this status when the service first starts
msPAUSING	Initial Pause	If the monitoring service is set to wait at startup (via Settings), the monitors will use this status
msUNLICENSED	Not Enough Licenses	Set if more servers are being monitored than licenses allow
msSKIPPINGACTIONS	Skipping Actions	If alerts should not be fired at startup, as specified in Settings
msCANTMONITORNOW	Monitor Busy	Usually happens if a monitor is contrained and has to wait a little longer before it can run. Not an error.
msTRAINING	Training Period	The monitor is collecting data for automatic training purposes, and will not alert.
msMAINTENANCE	Server Maintenance	The server is in maintenance mode, so the monitor will not run
msWRONG_EDITION	Wrong Product Edition	This monitor is not supported with the installed license.
msEXCLUSION_PERIOD	Exclusion Period	The monitor is configured not allowed to run at this time.
msDEPENDENCY_NOT_MET	Dependency Not Met	Monitor dependencies are not met, so this monitor will not run.
msSERVER_DISABLED	Server Disabled	The server is disabled, so the monitors will not run.
msOWNING_SATELLITE_DISCONNECTED	Satellite Disconnected	The satellite that runs this monitor has not reported in, so the monitor status is unknown

Custom Properties

Custom Properties can be used as expansion variables by using them in this form:

$CustomProp(*propertyName*)$

Row Variables

In addition to the values that are always available, the following values are available depending on which monitor type is sending the alert. The additional information is reported in rows for those monitors that can report information on a number of items (such as a list of changed files and directories). The number in parenthesis (the x) should therefore be replaced with a 1 for the first row of results, 2 for the second, etc. (Example: $Item(1)$, $Item(2)$, $State(1)$...).

NOTE: Is is possible to not have any extra row data, especially in the emergency alert cases shown above.

Monitors	Row Variables
Actions Scheduler	*$Item(x)$* - Unused *$State(x)$* - OK or PROBLEM
Active Directory Login Monitor	*$CurrentValue(x)$* - User involved with the event (if applicable) *$ID(x)$* - ID of the Event *$Item(x)$* - The category for the event *$ItemType(x)$* - A constant value always equal to 'Category' *$State(x)$* - OK or PROBLEM
Bandwidth Monitor	*$CurrentValue(x)$* - The current bandwidth usage value *$Facility(x)$* - Port description *$Item(x)$* - Port alias *$ItemType(x)$* - One of: 'Bytes', 'Errors', 'Discards', 'Multicasts', 'Broadcasts', 'Unicasts', or 'NotUnicasts' *$LimitValue(x)$* - Configured bandwidth threshold for the port *$State(x)$* - OK or PROBLEM
Calculated Status	*$Item(x)$* - Unused *$State(x)$* - OK or PROBLEM
Citrix Monitor	*$CurrentValue(x)$* - Number of ms for the the Connection or Login to happen. Equals -1 on error *$Item(x)$* - The server being probe *$ItemType(x)$* - Constant value always equal to 'Connection' or 'Login' *$LimitValue(x)$* - Configured threshold seconds for login to complete *$State(x)$* - OK or PROBLEM
Database Monitor	*$CurrentValue(x)$* - Current value *$Item(x)$* - The database being checked *$ItemType(x)$* - Statistic being checked. One of: DBINDEX_SIZE, LOGSIZE, TOTALSIZE, FILEOVERLIMIT, LOGOVERLIMIT, RECOVERYCHANGED *$LimitValue(x)$* - Configured threshold *$State(x)$* - OK or PROBLEM
Database Server Monitor	*$CurrentValue(x)$* - N/A *$Description(x)$* - Constant value equal to 'CREATED', 'DELETED', 'CHANGED' or 'DOWN'. *$Item(x)$* - Database name *$ItemType(x)$* - Constant value equal to 'DATABASE' *$LimitValue(x)$* - N/A *$State(x)$* - OK or PROBLEM
Directory Quota Monitor	*$CurrentValue(x)$* - Directory size in MB *$Item(x)$* - Directory being checked *$ItemType(x)$* - Constant value always equal to 'Directory' *$LimitValue(x)$* - Configured threshold directory size in MB *$State(x)$* - OK or PROBLEM
Disk Space Monitor	*$CurrentValue(x)$* - Number of free MB on the drive *$Item(x)$* - The drive whose free disk space is being checked *$ItemType(x)$* - Constant value equal to 'Disk', or 'Error' *$LimitValue(x)$* - Configured threshold (could be in % or an absolute size and unit) *$State(x)$* - OK or PROBLEM
DNS Monitor	*$CurrentValue(x)$* - The resolved result *$Item(x)$* - The hostname or IP address being resolved *$ItemType(x)$* - Constant value always equal to 'Host' *$State(x)$* - OK or PROBLEM
Dynamic Server List	*$CurrentValue(x)$* - "ADDED" or "REMOVED" *$Item(x)$* - IP address of the computer/device *$ItemType(x)$* - Constant value of "DEVICE"

	$LimitValue(x)$ - DNS name if it can be determined
	$State(x)$ - OK or PROBLEM
Email Monitor	*$ID(x)$* - Email message-ID field
	$Item(x)$ - Email address being monitored
	$ItemType(x)$ - 'BODY' or 'SUBJECT' depending on what was matched
	$State(x)$ - OK or PROBLEM
Esensor EM01B Monitor	*$CurrentValue(x)$* - The value of the measured item
	$Item(x)$ - Constant value always equal to 'EM01b Temperature', 'EM01b Humidity', or 'EM01b Luminescence'.
	$ItemType(x)$ - Constant value always equal to 'EM01b Temperature', 'EM01b Humidity', or 'EM01b Luminescence'.
	$LimitValue(x)$ - Configured threshold for the item
	$State(x)$ - OK or PROBLEM
Event Log Monitor	*$CurrentValue(x)$* - Time of the log item in the Event Log, as a string
	$Extra1(x)$ - Content of the log item
	$Extra2(x)$ - Event ID of the log item
	$Item(x)$ - The Event Log Source that produced the log item
	$ItemType(x)$ - Constant value always equal to 'Source'
	$State(x)$ - OK or PROBLEM
Event Validator	*$CurrentValue(x)$* - Time of the log item in the Event Log, as a string
	$Extra1(x)$ - Content of the log item
	$Extra2(x)$ - Event ID of the log item
	$Item(x)$ - The Event Log Source that produced the log item
	$ItemType(x)$ - Constant value always equal to 'Source'
	$State(x)$ - OK or PROBLEM
Execute Script	*$Item(x)$* - Unused
	$State(x)$ - OK or PROBLEM
File & Directory Change Monitor (CIFS)	*$CurrentValue(x)$* - Type of change that occurred. One of: 'Created', 'Deleted', or 'Changed'.
	$Item(x)$ - File or directory path that changed
	$ItemType(x)$ - Constant value always equal to 'File' or 'Directory'
	$State(x)$ - OK or PROBLEM
File Age Monitor	*$CurrentValue(x)$* - Age of the file in minutes
	$Extra1(x)$ - File path (file & directory) that is too old
	$Item(x)$ - File name (not path) that is too old
	$ItemType(x)$ - Constant value always equal to 'File'
	$State(x)$ - OK or PROBLEM
File/Directory Size Monitor	*$CurrentValue(x)$* - Current size of the file/directory
	$Item(x)$ - The directory or file that has grown beyond the threshold
	$ItemType(x)$ - Constant value always equal to 'Directory' or 'File'
	$LimitValue(x)$ - Threshold for the file/directory before firing actions
	$State(x)$ - OK or PROBLEM
FTP Server Monitor	*$Item(x)$* - The ftp server being monitored
	$ItemType(x)$ - Constant value always equal to 'Server'
	$State(x)$ - OK or PROBLEM
Hardware Monitor	*$CurrentValue(x)$* - Current status value
	$Item(x)$ - The sensor name that is in error, or change, or was added or removed
	$ItemType(x)$ - Constant value always equal to 'Added', 'Removed', 'Changed' or 'Sensor'
	$State(x)$ - OK or PROBLEM
Inventory Alerter	*$CurrentValue(x)$* - Current property value
	$Extra1(x)$ - Comparison operation
	$Item(x)$ - Property name
	$ItemType(x)$ - Constant value always set to 'Property'
	$LimitValue(x)$ - Value the property is compared against
	$State(x)$ - OK or PROBLEM
Inventory Collector	*$CurrentValue(x)$* - Not Set
	$Item(x)$ - Not Set
	$ItemType(x)$ - Not Set
	$LimitValue(x)$ - Not Set
	$State(x)$ - OK or PROBLEM
Log File Monitor	*$Extra1(x)$* - Content of the matching log line(s)

	$Item(x)$ - The Log File that produced the log item *$ItemType(x)$* - Constant value always equal to 'File' *$State(x)$* - OK or PROBLEM
Mail Server Monitor	*$Item(x)$* - The mail server being monitored *$ItemType(x)$* - Constant value always equal to 'Server' *$State(x)$* - OK or PROBLEM
Network Scanner	*$CurrentValue(x)$* - IP address *$Item(x)$* - IP address of the new computer/device that was found *$ItemType(x)$* - Constant value of "DEVICE" *$LimitValue(x)$* - DNS name if it can be determined *$State(x)$* - OK or PROBLEM
Performance Monitor	*$CurrentValue(x)$* - Current value of the counter, or the process % CPU usage *$Extra1(x)$* - PID if item is 'Process' *$Item(x)$* - The complete path of the performance counter, or the process name as seen in Perfmon *$ItemType(x)$* - Constant value always equal to 'Counter' or 'Process' *$LimitValue(x)$* - Configured counter threshold value as specified in the monitor *$State(x)$* - OK or PROBLEM
Ping Monitor	*$CurrentValue(x)$* - Time the ping took to return (could possibly be empty depending on settings) *$Item(x)$* - The host name/IP address of the server/device being pinged *$ItemType(x)$* - Constant value always equal to 'Server' *$LimitValue(x)$* - Maximum time the ping is allowed to take before alerting *$State(x)$* - OK or PROBLEM
Plugin Monitor	*$CurrentValue(x)$* - Return code from the plugin, or a performance value *$Item(x)$* - "Command", or a performance value's name returned from the plugin *$ItemType(x)$* - Constant set to "ReturnCode" or "PerformanceValue" *$LimitValue(x)$* - Warning threshold for a PerformanceValue if specified *$State(x)$* - OK or PROBLEM
Process Monitor	*$CurrentValue(x)$* - Either 'Up' or 'Down' *$Item(x)$* - The process name being checked *$ItemType(x)$* - Constant value always equal to 'Process' *$LimitValue(x)$* - Configured threshold value as specified in the monitor *$State(x)$* - OK or PROBLEM
Server Temperature Monitor	*$CurrentValue(x)$* - Current temperature *$Item(x)$* - Probe Number *$ItemType(x)$* - Constant value always equal to 'Temperature' *$LimitValue(x)$* - Threshold temperature *$State(x)$* - OK or PROBLEM
Service Monitor	*$CurrentValue(x)$* - One of three values: 'Up', 'Down', or '?' if the status can't be determined *$Extra1(x)$* - The display name of the service being checked *$Extra2(x)$* - Reason for the alert. Can be 'Status', 'Start-type-changed', 'Added' or 'Deleted' *$Item(x)$* - The system name for the service being checked *$ItemType(x)$* - Constant value always equal to 'Service' *$State(x)$* - OK or PROBLEM
SNMP Monitor	*$CurrentValue(x)$* - The current value of the object *$Item(x)$* - The name of the SNMP object being queried *$ItemType(x)$* - Constant value always equal to 'Object' *$LimitValue(x)$* - Configured threshold for the object *$State(x)$* - OK or PROBLEM
SNMP Trap Monitor	*$CurrentValue(x)$* - The current value of the object *$Extra1(x)$* - Trap OID or the ErrorIndex.ErrorStatus values for an Inform (this value will be the same for all rows) *$Item(x)$* - The name of the SNMP object being reported on *$ItemType(x)$* - Constant value always equal to 'Trap' or 'Inform' *$State(x)$* - OK or PROBLEM
Syslog Monitor	*$CurrentValue(x)$* - Message content of the log item *$Extra1(x)$* - Severity numeric constant *$Extra2(x)$* - Facility numeric constant *$Item(x)$* - Hostname that the event came from *$ItemType(x)$* - Constant always equal to 'Log'

	$State(x)$ - OK or PROBLEM
Task Scheduler	*$CurrentValue(x)$* - /The current Last Run Result value, or ENABLED or DISABLED *$Item(x)$* - The name of the Scheduled Task, including path *$ItemType(x)$* - Constant value equal to one of: ENABLE-CHANGE, LAST-RUN-RESULT-CHANGE, LAST-RUN-RESULT, or MISSING *$LimitValue(x)$* - The task's previous Last Run Result value for the STATUS-CHANGE state *$State(x)$* - OK or PROBLEM
TCP Port Monitor	*$Extra1(x)$* - Port that is being monitored *$Item(x)$* - The server being monitored *$ItemType(x)$* - Constant value always equal to 'Server' *$State(x)$* - OK or PROBLEM
Web Page Monitor	*$CurrentValue(x)$* - Time the page took to return *$Item(x)$* - The URL being monitored *$ItemType(x)$* - Constant value always equal to 'URL' *$LimitValue(x)$* - Maximum time the page was allowed to take before alerting *$State(x)$* - OK or PROBLEM

External API

PA Server Monitor has a simple API for automating some 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. Under HKEY_LOCAL_MACHINE\software\PAServerMonitor, create a value named API_KEY. Set it to a long string value of random characters.

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

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

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. Successful commands return as XML, or in the following format:

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

All errors are returned as:

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

IDs: Some of the requests below take a Group ID, Computer ID and/or Monitor ID. You can get IDs via:

In the Console by enabling View > Show Object IDs in Navigation Tree

Get them programatically by using the following requests:
Group IDs : GET_GROUP_LIST

Computer IDs: GET_SERVER_LIST

Monitor IDs: GET_MONITOR_INFO

Querying the ConfigComputerInfo or ConfigGroupInfo tables in the database. Monitor IDs are not available this way.

API Commands

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

Group Commands

GET_GROUP_LIST

Returns a list of groups, with their name, full path name, group ID, and group ID for the group's parent.

Optional Parameters
XML = {0|1} - defaults to 0

Example

```
https://server:81?KEY=mysecretkey&API=GET_GROUP_LIST
```

Output (name|full path|id|parentID)

```
:START:
Servers/Devices|Servers/Devices|0|-1
Boston|Servers/Devices^Boston|1|0
Office|Servers/Devices^Office|2|0
Dev|Servers/Devices^Office^Dev|3|2
:END:
```

XML Example

```
https://server:81?KEY=mysecretkey&API=GET_GROUP_LIST&XML=1
```

XML Output

```
<?xml version="1.0" ?>
<groups>
  <group name="Servers/Devices" path="Servers/Devices" id="0" parentID="-1" />
  <group name="Boston" group="Servers/Devices^Boston" id="1" parentID="0" />
  <group name="Office" group="Servers/Devices^Office" id="2" parentID="0" />
  <group name="Dev" group="Servers/Devices^Office^Dev" id="3" parentID="2" />
</groups>
```

ADD_GROUP

Add the given group if it doesn't already exist

Required Parameters

NAME - Full of the group name. For example, a group named "Exchange Servers" under the top "Servers\Devices" would set NAME to Servers\Devices^Exchange%20Servers (delimit groups with ^, URL encode, so a space becomes %20)

Example

```
https://server:81?KEY=mysecretkey&API=ADD_GROUP&NAME=Servers\Devices^New%20York^Web
```

Output

```
:OK:
123
```

The 123 above is the new Group ID (referred to as GID in some other functions)

DELETE_GROUP

Delete the named group. If it contains child groups or servers, they will become orphaned and moved to the top Servers\Devices group the next time the monitoring service is restarted.

Required Parameters

NAME - Full of the group name. For example, a group named "Exchange Servers" under the top "Servers\Devices" would set NAME to Servers\Devices^Exchange%20Servers (delimit groups with ^, URL encode, so a space becomes %20)

Example

```
https://server:81?KEY=mysecretkey&API=DELETE_GROUP
&NAME=Servers\Devices^New%20York^Web
```

Output

```
:OK:
```

GET_GROUP_PROP

Retrieves a custom property on a group. If the property is not defined, an empty value is returned.

Required Parameters

GID - Group ID for the group to target for the operation.

PROPNAME - Name of the property to retrieve

Example

```
https://server:81?KEY=mysecretkey&API=GET_GROUP_PROP&GID=0&PROPNAME=ONCALL
```

Output

```
:START:
555-555-1234
:END:
```

SET_GROUP_PROP

Sets a custom property on a group. If the property value is empty, the custom property is removed.

Required Parameters

GID - Group ID for the group to target for the operation.

PROPNAME - Name of the property to set
PROPVAL - Value of the property to set

Example

```
https://server:81?KEY=mysecretkey&API=SET_GROUP_PROP&GID=0
&PROPNAME=ONCALL&PROPVAL=555-555-1234
```

Output

```
:OK:
```

GET_NOTES

Gets the Notes from a Server/Device or from a Group

Required Parameters

CID - Computer ID for the computer to retrieve notes from.
- or -
GID - Group ID for the group to retrieve notes from.
PATH - File that the notes will be saved into. This needs to be accessible to the Central Monitoring Service (a local file).

Example

```
https://server:81?KEY=mysecretkey&API=GET_NOTES&CID=125&PATH=C:\Notes\Comp125Notes.txt
```

Output

```
:OK:
```

SET_NOTES

Sets the Notes for a Server/Device or for a Group

Required Parameters

CID - Computer ID for the computer to retrieve notes from.
- or -
GID - Group ID for the group to retrieve notes from.
PATH - File that the notes will be read from. This needs to be accessible to the Central Monitoring Service (a local file).

Example

```
https://server:81?KEY=mysecretkey&API=SET_NOTES&CID=125&PATH=C:\Notes\Comp125Notes.txt
```

Output

```
:OK:
```

START_MAINTENANCE

Put server(s) or a monitor into immediate maintenance mode.

Required Parameters

CID - Computer ID for the computer to target for the operation.
- or -
GID - Group ID for the group that contains target computers (including those in child-groups).
- or -
MID - Monitor ID for the specific monitor that should be affected.

MINUTES - time in minutes that the server should remain in maintenance mode before it automatically reverts to normal monitoring

Optional Parameters

FORCE - 1 to allow the maintenance window to be shortened. Defaults to 0

Example

```
https://server:81?KEY=mysecretkey&API=START_MAINTENANCE&CID=37&MINUTES=15&FORCE=1
```

Output

```
:OK:
```

END_MAINTENANCE

Put server(s) or a monitor back into normal monitoring mode.

Required Parameters

CID - Computer ID for the computer to target for the operation.
- or -
GID - Group ID for the group that contains target computers (including those in child-groups).

- or -
MID - Monitor ID for the specific monitor that should be affected.

Example

```
https://server:81?KEY=mysecretkey&API=END_MAINTENANCE&CID=37
```

Output

```
:OK:
```

Server/Device Commands

GET_SERVER_LIST
Returns a list of servers and the group that the server is in. The XML version also shows the computer's internal ID.

Optional Parameters
XML = {0|1} - defaults to 0
GID = {group ID}, defaults to 0 (top Servers/Devices group).
ALL = {0|1} - 0 means just return the servers directly in the group, 1 returns all servers in all sub-groups as well

Example

```
https://server:81?KEY=mysecretkey&API=GET_SERVER_LIST
```

Output (server|group^group)

```
:START:
DNVISTA|Servers/Devices
192.168.2.5|Servers/Devices
POWERADMIN.COM|Servers/Devices^Boston
OPSMON02|Servers/Devices^Servers^Office
ARCHIVE|Servers/Devices
:END:
```

XML Example

```
https://server:81?KEY=mysecretkey&API=GET_SERVER_LIST&XML=1
```

XML Output

```
<?xml version="1.0" ?>
<servers>
  <server name="DNVISTA" group="Servers/Devices^Boston^Servers" id="1" groupID="1" alias="DNVISTA"
status="ok" />
  <server name="192.168.2.5" group="Servers/Devices^Kansas City" id="2" groupID="2"
alias="EXCHANGE" status="maintenance" />
  <server name="POWERADMIN.COM" group="Servers/Devices^External" id="4" groupID="3"
alias="POWERADMIN.COM" status="disabled" />
  <server name="OPSMON02" group="Servers/Devices^Boston^Servers" id="5" groupID="1" alias="OPS"
status="unlicensed" />
  <server name="ARCHIVE" group="Servers/Devices^Boston^Servers" id="8" groupID="1" alias="ARCHIVE"
```

```
status="sat_disconnected" />
</servers>

Note that all possible values of 'status' are shown above
```

LOOKUP_CID

Given a device hostname or IP address, looks up the device and returns the Computer ID (CID) which is used in many other API calls.

Required Parameters

NAME - Host name or IP address of the target server.

Example

```
https://server:81?KEY=mysecretkey&API=LOOKUP_CID&NAME=FS01
```

Output

```
:OK:
42
```

ADD_SERVER

Add and optionally configure the named server

Required Parameters

SERVER - name of the server that should be added. If the server already exists, it will be operated on (WIN, WMI and GROUP will not have an effect in that case).

Optional Parameters

ALIAS={new alias|CLEAR_ALIAS} - If set to CLEAR_ALIAS, deletes the alias. Otherwise sets the alias to the new value. If the value is blank or ALIAS is not sent, no changes to the alias are made.

WIN={0|1} - defaults to 0. Set to 1 if this is a Windows server.

WMI={0|1} - defaults to 0. Set to 1 if WMI polling should happen to collect System Details information for the server status report

CONFIG_PATH - 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, or by using the EXPORT_SERVER API below. The file must be on the same computer as PA Server Monitor is running on.

GROUP - defaults to none (which implies the top level group). The full path to the group that the server should be placed in, for example: Servers/Devices^Seattle^Exchange Servers (where the ^ delimits group names).

SATID - Satellite ID. Defaults to the Central Service. Satellite IDs can be obtained in the Console by looking at the Satellite's status report. They generally look something like: 51fa284a-58d6-41a0-870e-1cbd7db6c12a

GETID={0|1} - defaults to 0. If set to 1, this function will wait (possibly a long time) until the new device is added so the Computer ID (CID) value can be returned.

Example

```
https://server:81?KEY=mysecretkey&API=ADD_SERVER&SERVER=MAILSRV2&WIN=1&WMI=1&GETID=1
&CONFIG_PATH=C:\Configs\Mail+Config.cxml
```

Output

```
:OK:
471
```

The 471 above is the newly created Computer ID (CID) that is returned because GETID=1. Without GETID=1, the Output would simply be :OK:

DELETE_SERVER

Delete the named server, along with all of its monitors

Required Parameters

CID - Computer ID for the computer to target for the operation.
{deprecated} SERVER - name of the server that should be deleted

Example

```
https://server:81?KEY=mysecretkey&API=DELETE_SERVER&CID=125
```

Output

```
:OK:
```

EXPORT_SERVER

Exports the configuration of the specified server in a .cxml file. Per-server passwords (if any) are NOT exported.

Required Parameters

CID - Computer ID for the computer to target for the operation.
- or -
SERVER - Name of the computer to target. If there are multiple computers with the same name (perhaps at different locations), which one is returned is not defined.

Optional Parameters

PATH - Full path to the output file. If this is not given, the file will be saved to C:\Program Files\PA Server Monitor\Config\Backup\Export_Computer_{CID}.cxml

Note: Be careful where these files are saved as some monitor configurations might contain sensitive information.

Example

```
https://server:81?KEY=mysecretkey&API=EXPORT_SERVER&CID=125
```

Output

```
:OK:
```

GET_SERVER_PROP

Retrieves a custom property on a server. If the property is not defined, an empty value is returned.

Required Parameters

CID - Computer ID for the computer to target for the operation.
- or -
SERVER - Name of the computer to target. If there are multiple computers with the same name (perhaps at different locations), which one is returned is not defined.
PROPNAME - Name of the property to retrieve Multiple properties can be passed in a comma separated list.

Example (single property)

```
https://server:81?KEY=mysecretkey&API=GET_SERVER_PROP&CID=125&PROPNAME=Customer
```

Example (multiple properties)

```
https://server:81?KEY=mysecretkey&API=GET_SERVER_PROP&CID=125&PROPNAME=Customer,ID,Phone
```

Output

```
:START:
IBM
51434
555-555-1234
:END:
```

Example (ID property not defined on target)

```
https://server:81?KEY=mysecretkey&API=GET_SERVER_PROP&CID=125&PROPNAME=Customer,ID,Phone
```

Output

```
:START:
IBM

555-555-1234
:END:
```

Output

```
:START:
IBM
:END:
```

SET_SERVER_PROP

Sets a custom property on a server. If the property value is empty, the custom property is removed.

Required Parameters

CID - Computer ID for the computer to target for the operation.

- or -
SERVER - Name of the computer to target. If there are multiple computers with the same name (perhaps at different locations), which one is returned is not defined.
PROPNAME - Name of the property to set
PROPVAL - Value of the property to set

Example

```
https://server:81?KEY=mysecretkey&API=SET_SERVER_PROP&CID=125
&PROPNAME=Customer&PROPVAL=IBM
```

Output

```
:OK:
```

The Custom Property DISPLAYED_NOTES is the value you can set by right-clicking a computer and selecting Notes. Notes show up at the top of a Server Status Report.

GET_NOTES

Gets the Notes from a Server/Device or from a Group

Required Parameters
CID - Computer ID for the computer to retrieve notes from.
- or -
GID - Group ID for the group to retrieve notes from.
PATH - File that the notes will be saved into. This needs to be accessible to the Central Monitoring Service (a local file).

Example

```
https://server:81?KEY=mysecretkey&API=GET_NOTES&CID=125&PATH=C:\Notes\Comp125Notes.txt
```

Output

```
:OK:
```

SET_NOTES

Sets the Notes for a Server/Device or for a Group

Required Parameters
CID - Computer ID for the computer to retrieve notes from.
- or -
GID - Group ID for the group to retrieve notes from.
PATH - File that the notes will be read from. This needs to be accessible to the Central Monitoring Service (a local file).

Example

```
https://server:81?KEY=mysecretkey&API=SET_NOTES&CID=125&PATH=C:\Notes\Comp125Notes.txt
```

Output

```
:OK:
```

START_MAINTENANCE

Put server(s) or a monitor into immediate maintenance mode.

Required Parameters

CID - Computer ID for the computer to target for the operation.
- or -
GID - Group ID for the group that contains target computers (including those in child-groups).
- or -
MID - Monitor ID for the specific monitor that should be affected.

MINUTES - time in minutes that the server should remain in maintenance mode before it automatically reverts to normal monitoring

Optional Parameters

FORCE - 1 to allow the maintenance window to be shortened. Defaults to 0

Example

```
https://server:81?KEY=mysecretkey&API=START_MAINTENANCE&CID=37&MINUTES=15&FORCE=1
```

Output

```
:OK:
```

END_MAINTENANCE

Put server(s) or a monitor back into normal monitoring mode.

Required Parameters

CID - Computer ID for the computer to target for the operation.
- or -
GID - Group ID for the group that contains target computers (including those in child-groups).
- or -
MID - Monitor ID for the specific monitor that should be affected.

Example

```
https://server:81?KEY=mysecretkey&API=END_MAINTENANCE&CID=37
```

Output

```
:OK:
```

SERVER_ENABLE

Enables or disables the server (disabling a server disables all monitors for that device)

Required Parameters

CID - Computer ID for the computer to target for the operation.
ENABLE - Set to 1 to enable monitoring, or 0 to disable monitoring

Example

```
https://server:81?KEY=mysecretkey&API=SERVER_ENABLE&CID=42&ENABLE=0
```

Output

```
:OK:
```

GOTO_SERVER_REPORT

Pass a server name and get forwarded to that server's status report

Required Parameters

CID - Computer ID for the computer to target for the operation.
{deprecated} SERVER - name of the server

Example

```
https://server:81?KEY=mysecretkey&API=GOTO_SERVER_REPORT&CID=362
```

Output

Browser gets redirected to the given server's status report page

Monitor Commands

GET_MONITOR_INFO

Returns information about all monitors owned by a particular computer.

Required Parameters

CID - Computer ID for the computer to target for the operation. **ALL** can be used to return information all monitors

Optional Parameters

FORMAT_DATE - 0 to always output as dd-mm-yyyy hh:mm:ss (24 hour hh), or 1 to use the same format that the existing reports use (which can be customized). Defaults to 0.
STATUS - a comma separated list of monitor statuses. Only monitors that are currently the specified status will be returned. See status values in the table at the bottom of the page.

Example

```
https://server:81?KEY=mysecretkey&API=GET_MONITOR_INFO&CID=371
&FORMAT_DATE=1
```

```
https://server:81?KEY=mysecretkey&API=GET_MONITOR_INFO&CID=ALL
&STATUS=2,10,17,18,19
```

Output (XML)

```
<?xml version="1.0" ?>
<monitors>
   <monitor id="105047" status="OK" depends_on="" title="DNS Check: Yahoo" lastRun="24-02-2023
11:22:45" nextRun="24-02-2023 11:23:45" errText="[yahoo.com resolving to 74.6.143.26] "
errActionIDs="12" fixedActionIDs="12" inErrSeconds="0" monitorType="DNS Monitor" monitorKind="M"
owningCompID="31" owningGroupID="0"/>    <monitor id="111981" status="OK" depends_on=""
title="Check directory size at E:\Hyper-V" lastRun="24-02-2023 11:19:06" nextRun="24-02-2023
11:24:06" errText="[Last size: 112 GB] " errActionIDs="" fixedActionIDs="" inErrSeconds="0"
monitorType="File/Dir Size" monitorKind="M" owningCompID="31" owningGroupID="0"/>    <monitor
id="118722" status="OK" depends_on="" title="Core - Ping Monitor" lastRun="" nextRun="" errText=""
errActionIDs="" fixedActionIDs="" inErrSeconds="0" monitorType="Ping" monitorKind="T"
owningCompID="0" owningGroupID="98"/>
</monitors>
```

Notes:
* monitorKind can be "M" for a typical monitor, "T" for a monitor template, "MT" for a monitor that derives from a template, or "G" for a global monitor.
* owningComputerID will be 0 for templates (T) and global monitors (G)
* owningGroupID will only be non-zero for monitor templates (T)

GET_MONITOR_CONFIG

Retrieves a monitor's XML configuration. This can also be retrieve manually in the Console by first enabling the Console_ShowExportMonitor option in Advanced Services > Advanced Settings. Once that is done, you can right-click a monitor and click the new Export Monitor Configuration menu option.

Required Parameters

MID - Monitor ID for the target monitor

Example

```
https://server:81?KEY=mysecretkey&API=GET_MONITOR_CONFIG&MID=198709
```

Output

The XML configuration data is returned which will look similar to:

```
<?xml version="1.0"?><checksum value="3272823308">
<Obj-Monitor2 ver="3">
...
```

SET_MONITOR_CONFIG

Set the configuration of a monitor to new values. Often this XML would have been retrieved using GET_MONITOR_CONFIG or from the Console.

Required Parameters

MID - Monitor ID for the target monitor
CONFIG - The monitor configuration XML

Important: If the XML is not valid, there is a chance the monitoring service will crash when loading the monitor. Great care should be used in manipulating the XML. If the service crashes, you may need to restore from the configuration backup which is stored in the Config\Backup folder.

In addition, because of the format and size of the typical monitor XML, this API usually needs to be called via a POST rather than a GET.

Example

```
wget.exe --no-check-certificate --post-file=C:\Data\SetMonitor.txt https://localhost:81
```

See the contents of SetMonitor.txt to see the URL-encoded content that is sent as a form post.

Note that at the top you'll see the familiar

```
KEY=mysecretkey&API=SET_MONITOR_CONFIG&MID=198709&CONFIG={encoded XML}
```

Output

```
:OK:
```

ADD_MONITOR

Adds a new monitor to a server. Often this XML would have been retrieved using GET_MONITOR_CONFIG or from the Console.

Required Parameters
CID - Target Computer ID for the computer that the monitor will be added to
CONFIG - The monitor configuration XML

Important: If the XML is not valid, there is a chance the monitoring service will crash when loading the monitor. Great care should be used in manipulating the XML. If the service crashes, you may need to restore from the configuration backup which is stored in the Config\Backup folder.

In addition, because of the format and size of the typical monitor XML, this API usually needs to be called via a POST rather than a GET.

Example

```
wget.exe --no-check-certificate --post-file=C:\Data\AddMonitor.txt https://localhost:81
```

See the contents of AddMonitor.txt to see the URL-encoded content that is sent as a form post.

Note that at the top you'll see the familiar

```
KEY=mysecretkey&API=ADD_MONITOR&CID=3579&CONFIG={encoded XML}
```

Output

```
:OK:
456
```

The 456 above is the newly added Monitor ID (referred to as MID in other functions)

MONITOR_ENABLE

Enables or disables the monitor

Required Parameters

MID - Monitor ID for the monitor to target for the operation.
ENABLE - Set to 1 to enable monitoring, or 0 to disable monitoring

Example

```
https://server:81?KEY=mysecretkey&API=MONITOR_ENABLE&MID=1312&ENABLE=0
```

Output

```
:OK:
```

START_MAINTENANCE

Put server(s) or a monitor into immediate maintenance mode.

Required Parameters

CID - Computer ID for the computer to target for the operation.
- or -
GID - Group ID for the group that contains target computers (including those in child-groups).
- or -
MID - Monitor ID for the specific monitor that should be affected.

MINUTES - time in minutes that the server should remain in maintenance mode before it automatically reverts to normal monitoring

Optional Parameters

FORCE - 1 to allow the maintenance window to be shortened. Defaults to 0

Example

```
https://server:81?KEY=mysecretkey&API=START_MAINTENANCE&CID=37&MINUTES=15&FORCE=1
```

Output

```
:OK:
```

END_MAINTENANCE

Put server(s) or a monitor back into normal monitoring mode.

Required Parameters

CID - Computer ID for the computer to target for the operation.
- or -
GID - Group ID for the group that contains target computers (including those in child-groups).
- or -
MID - Monitor ID for the specific monitor that should be affected.

Example

```
https://server:81?KEY=mysecretkey&API=END_MAINTENANCE&CID=37
```

Output

```
:OK:
```

RUN_NOW

Request the specified monitor be run immediately

Required Parameters

MID - Monitor ID for the monitor to run immediately.

Optional Parameters

FORCE - 1 to run the monitor even if it's disabled or the server is in maintenance. Defaults to 0

Example

```
https://server:81?KEY=mysecretkey&API=RUN_NOW&MID=4721&FORCE=1
```

Output

```
:OK:
```

Action Commands

GET_ACTION_INFO

Returns a list describing all the actions in the system (these IDs are used in the errorActionIDs and fixedActionIDs attributes returned from GET_MONITOR_INFO

Example

```
https://server:81?KEY=mysecretkey&API=GET_ACTION_INFO
```

Output (XML)

```
<?xml version="1.0" ?>
<actions>
  <action id="1" type="Message Box" typeID="3" title="Message Box" />
  <action id="2" type="Write to a Text Log File" typeID="6" title="Write to ServerEvents.txt log
file" />
  <action id="6" type="Start, Stop or Restart a Service" typeID="5" title="Restart stopped service
on monitored computer" />
</actions>
```

Miscellaneous Commands

ACK_ALERT

Acknowledge an alert

Required Parameters

ERRID - The Error ID for the alert. This can be shown in Error Audit reports, or shown on the Server Status report

Optional Parameters

ACKALERTS - 1 to send any Acknowledge alerts attached to the monitor, or 0 to suppress sending them. Defaults to 0.
ACKBY - Name to list as the person doing the acknowledgement. By default it will show "External API". The IP address of the caller will be appended.

Example

```
https://server:81?KEY=mysecretkey&API=ACK_ALERT&ERRID=4172&ACKBY=Robert
```

Output

```
:OK:
```

CREATE_CHART

Creates a chart jpeg file similar to those shown in the server status reports. The chart image will be in the Reports\Temp folder. The caller is responsible for deleting the file when done using it.

Required Parameters

STATID - statistic ID to be charted. The StatID value can be found in the Statistic table, StatID column.
MONTYPE - Monitor type. This is the value from the OwnerType column in the Statistic table.

Optional Parameters

NONZEROBASE - The y-axis of most charts starts at 0. Set this to 1 to indicate the chart should pick a better axis starting point. Defaults to 0
MINUTES - The number of minutes back to chart. Defaults to 1440 (one day)
SUMMARIZATION - Control how the data is summarized, using a value from the below chart. Defaults to 25 (5-minute maximum)

Chart raw values	0
Minute minimum	15
Minute average	14
Minute maximum	16

5-Minute minimum	24
5-Minute average	23
5-Minute maximum	25
Hourly minimum	5
Hourly average	1
Hourly maximum	6
Daily minimum	7
Daily average	2
Daily maximum	8
Weekly minimum	9
Weekly average	3
Weekly maximum	10
Monthly minimum	11
Monthly average	4
Monthly maximum	12
Yearly minimum	18
Yearly average	17
Yearly maximum	19

UNIT - The unit from the table below. Used for display and scaling if needed. Defaults to 15 (generic number)

Generic number	15
Bytes	1
KB	2
MB	3
GB	4
TB	12
PB	13
EB	14
Bps	11
Kbps	17
Mbps	18
Gbps	19
Tbps	20
Scale dynamically	5
Percentage	6
milliseconds	7
Temperature in C	9
Lux	10

COLOR - HTML color for the line. Defaults to #000080
TITLE - Override the title for the chart. Uses the statistic's name by default
FILENAME - Filename only (no path). All files are stored in the Reports\Temp folder. A default name will be chosen if one is not given.
WIDTH - width in pixels. Defaults to 345 wide x 175 high. Either both WIDTH and HEIGHT need to be given, or neither should be given.
HEIGHT - height in pixels.

Example

```
https://server:81?KEY=mysecretkey&API=CREATE_CHART&STATID=4812&MONTYPE=8
&MINUTES=180&COLOR=008000&WIDTH=1000&HEIGHT=500&TITLE=My+Chart+Title
```

Output

```
:OK:
C:\Program Files\PA Server Monitor\Reports\Temp\SingleChart_48127.jpg
```

GET_PERF_STATS

Returns *internal* monitoring system performance metrics.

Note that these can also be enabled and retrieved as Windows performance counters. For the list of values returned, the first column is the performance ID, the second column is the name, and the third column is the performance value.

To see what statistics are available, call the API without an IDS parameter.

Required Parameters
NONE

Optional Parameters
IDS - comma separated list of performance IDs to return. If IDS is not give, all performance values are returned.

Example

```
https://server:81?KEY=mysecretkey&API=GET_PERF_STATS&IDS=68,69
```

Output

```
:OK:
68 FileSightRecsHandled 3289
69 TotalMonitorsRun 1070110
```

DISCOVERY_CONFIG

Scan an IP address range for new servers that aren't being monitored, and run Smart Config for the new servers. The Discovery and Smart Config procedures can take some time, so an OK result means that the process has been started.

Required Parameters
START - Start of IP address range
END - End of IP address range

Example

```
https://server:81?KEY=mysecretkey&API=DISCOVERY_CONFIG&START=192.168.0.1
&END=192.168.0.254
```

Output

```
:OK:
```

DO_BACKUP

Once a day and any time the monitoring service starts, the configuration is backed up to C:\Program Files\PA Server Monitor\Config\Backup. Using this API command, you can force the backup to happen on demand.

Optional Parameters
EXPORTCREDS - Backups normally do NOT contain all of the credentials that a system might have (credentials for accessing other servers, SMTP mail account credentials, database connection string, etc). If you must backup the credentials, you can

append &EXPORTCREDS=1 to the end of the URL below and credentials will be saved in plain text in the backup file.

Note: Be VERY careful about using this option. Exporting credentials can be globally disabled by setting

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor\Protected
[DWORD] DisablePasswordExport = 1
```

Example

```
https://server:81?KEY=mysecretkey&API=DO_BACKUP
```

Output

A new backup file named Backup1.axml is created in C:\Program Files\PA Server Monitor\Config\Backup

TUNNEL_CREATE

Creates a SNAP Tunnel based on configuration properties that are passed.

Required Parameters

LPORT - Listen side port (port that you will connect to).
SATID - Satellite where the tunnel will be created to/from. Satellite IDs can be seen in the Console on the Satellite's status report page.
DADDR - Destination hostname/IP address. This is where data will be sent/read from at the Satellite side. It can be the Satellite itself (127.0.0.1 for example) or a host on the remote Satellite's network.
DPORT - Destination port - this is the port where data will be sent to on the destination host.
USERNAME - The user whose credentials will be used to create the tunnel. This user's access will be used to confirm they have access to the destination address. See Remote User Access. To use the legacy mode of not requiring a login, see SNAP_AllowTunnelFromAnonAPI on this page.
PASSWORD - The password for the user specified by the USERNAME credential

Optional Parameters

SVC_LISTENS - 1 or 0 (defaults to 1). If 1 indicates whether the Central Server will listen on the port specified by LPORT. If 0, the Satellite will listen on the LPORT port.

Example

This will create a listening port on port 9000 on the Central Service which forwards to the RDP port (3389) on 192.168.7.4 on the Satellite's remote network. You could then launch the Remote Desktop application using: mstsc.exe /v:{IP of central service}:9000

```
https://server:81?KEY=mysecretkey&API=TUNNEL_CREATE&LPORT=9000&SATID=f7edb5fe-3aa6-4687-b686-9ecaa9094893&DADDR=192.168.7.4&DPORT=3389
```

Output

```
:OK:
Listening Port: 9000
```

TUNNEL_CLOSE

Closes a SNAP Tunnel based on configuration properties that are passed. These are the same parameters that would have been passed when the tunnel was created.

Required Parameters

LPORT - Listen side port (port that you will connect to).
SATID - Satellite where the tunnel will be created to/from. Satellite IDs can be seen in the Console on the Satellite's status report page.
DADDR - Destination hostname/IP address. This is where data will be sent/read from at the Satellite side.
DPORT - Destination port - this is the port where data will be sent to on the destination host.

Optional Parameters

SVC_LISTENS - 1 or 0 (defaults to 1). If 1 indicates whether the Central Server will listen on the port specified by LPORT. If 0, the Satellite will listen on the LPORT port.

Example

This will close the tunnel that was created in the TUNNEL_CREATE example above.

```
https://server:81?KEY=mysecretkey&API=TUNNEL_CLOSE&LPORT=9000&SATID=f7edb5fe-3aa6-4687-b686-9ecaa9094893&DADDR=192.168.7.4&DPORT=3389
```

Output

```
:OK:
```

TUNNELS_LIST

Lists SNAP Tunnels that exist to the target Satellite.

Required Parameters

SATID - Satellite for which the tunnel list is requested.

Example

```
https://server:81?KEY=mysecretkey&API=TUNNELS_LIST&SATID=f7edb5fe-3aa6-4687-b686-9ecaa9094893
```

Output

```
<?xml version="1.0"?>
<tunnels count="1">
 <tunnel>
  <listen>9000</listen>
  <destPort>3389</destPort>
  <destAddr>192.168.7.4</destAddr>
  <bServiceIsListener>1</bServiceIsListener>
  <satelliteID>f7edb5fe-3aa6-4687-b686-9ecaa9094893</satelliteID>
 </tunnel>
</tunnels>
```

Monitor-Specific Commands

GET_EVENTLOG_MONITOR_FILTER

Retrieves the filter that is set for the given monitor and event source.

Required Parameters

MID - The Monitor ID for the Event Log monitor
SOURCE - Source (left side of the Event Grid) to check in the montior. Note that spaces have to be URL escaped by changing them to a +
FTYPE - Indicates whether the Include or the Exclude filter should be returned. Valid values are INCLUDE and EXCLUDE.

Example

```
https://server:81?
KEY=mysecretkey&API=GET_EVENTLOG_MONITOR_FILTER&MID=123&SOURCE=.NET+Runtime&FTYPE=EXCLUDE
```

Output

```
:OK:
(1,4,5) OR "Bob"
```

SET_EVENTLOG_MONITOR_FILTER

Sets the filter for the given monitor and event source.

Required Parameters

MID - The Monitor ID for the Event Log monitor
SOURCE - Source (left side of the Event Grid) to check in the montior. Note that spaces have to be URL escaped by changing them to a +
FILTER - Filter to set on the source. Note that spaces have to be escaped.
FTYPE - Indicates whether the Include or the Exclude filter should be set. Valid values are INCLUDE and EXCLUDE.

Example

```
https://server:81?
KEY=mysecretkey&API=SET_EVENTLOG_MONITOR_FILTER&MID=123&SOURCE=.NET+Runtime&FTYPE=INCLUDE&FILTER=
(1,4,5)+OR+"George"
```

Output

```
:OK:
```

GET_EVENTLOG_MONITOR_LEVEL

Returns whether a specific event source's Level (Info, Error, Critical, etc) box is checked or not

Required Parameters

MID - The Monitor ID for the Event Log monitor
SOURCE - Source (left side of the Event Grid) to check in the montior. Note that spaces have to be URL escaped by changing them to a +
LEVEL - One of the following values: INFO, WARNING, ERROR, CRITICAL, AUDITSUCCESS, AUDITFAILURE

A return value of 1 means the level is checked, and 0 means it is unchecked.

Example

```
https://server:81?
KEY=mysecretkey&API=GET_EVENTLOG_MONITOR_LEVEL&MID=123&SOURCE=.NET+Runtime&LEVEL=CRITICAL
```

Output

```
:OK:
1
```

SET_EVENTLOG_MONITOR_LEVEL

Sets or clears a specific event source's Level (Info, Error, Critical, etc) check box

Required Parameters

MID - The Monitor ID for the Event Log monitor
SOURCE - Source (left side of the Event Grid) to check in the montior. Note that spaces have to be URL escaped by changing them to a +
LEVEL - One of the following values: INFO, WARNING, ERROR, CRITICAL, AUDITSUCCESS, AUDITFAILURE
VALUE - 1 to check the box, 0 to clear the box

Example

```
https://server:81?
KEY=mysecretkey&API=SET_EVENTLOG_MONITOR_LEVEL&MID=123&SOURCE=.NET+Runtime&LEVEL=CRITICAL&VALUE=1
```

Output

```
:OK:
```

Monitor Statuses

Alert	2
Alert - Skipping Actions	10
Alert - Green	17
Alert - Red	18
Alert - Suppressing	19
Bad License	14
Can't Run	4
Dependency Not Met	16
Disabled	6
Error	3
Error - Suppressed	21
OK	1
OK - Unacknowledged Alerts - Yellow	20
OK - Unacknowledged Alerts - Red	24
OK - Unacknowledged Alerts - Green	25
Monitor Busy	11
Monitor Maintenance Mode	13
Satellite Disconnected	23
Scheduled	7

Server Disabled	22
Server Maintenance Mode	26
Startup Pause	8
Training	12
Unlicensed	9

File Locations

PA Server Monitor stores a variety of files under the product directory. This will explain what and where they are.

C:\Program Files\PA Server Monitor
: Product executable and DLL files

C:\Program Files\PA Server Monitor\CA
: Self-signed SSL certificate files

C:\Program Files\PA Server Monitor\Config
: Database containing computer, monitor, action, and report configuration. A Backup directory below this contains periodic exports of the configuration which you can use to go back to a previous point if needed. The backups do not contain password information.

C:\Program Files\PA Server Monitor\Databases
: Database files which hold monitor findings as well as some system management data. If you choose to use MS SQL Server instead of the embedded database, only a few system management database files will exist here. This directory is configurable via Database Settings.

C:\Program Files\PA Server Monitor\Install
: The PA Server Monitor installer will copy itself here, along with a few files to help Satellites upgrade themselves. When you download the Console installer from the product's main report page, it comes from this directory.

C:\Program Files\PA Server Monitor\Logs
: Default location for internal product log files. This can be changed in Global Settings.

C:\Program Files\PA Server Monitor\Maps
: The Visual Status Map report pulls initial maps graphics during configuration from this folder. You can add your own map graphics here if you wish.

C:\Program Files\PA Server Monitor\Reports
: All reports are generated and stored in this directory. The Shared directory contains files used by all reports. You can delete this directory and everything will be recreated as needed. This directory is configurable via Report Settings.

Ignore Folders

It is highly recommended to add exceptions to file scanning application such as anti-virus, backup and search indexers to ignore the following folders:

C:\Program Files\PA Server Monitor\Config
C:\Program Files\PA Server Monitor\Databases
C:\Program Files\PA Server Monitor\Logs
C:\Program Files\PA Server Monitor\Reports

That will protect these folders from any possible file corruption that might happen from files accessed simultaneously from multiple processes.

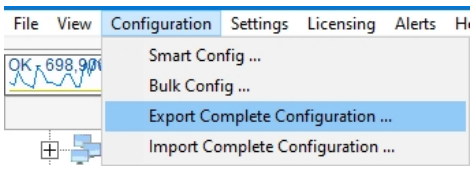
Importing and Exporting Configurations

PA Server Monitor supports a simple and effective way to transfer your complex monitoring configuration from one installation of the product to another. This is what exporting and importing configurations does.

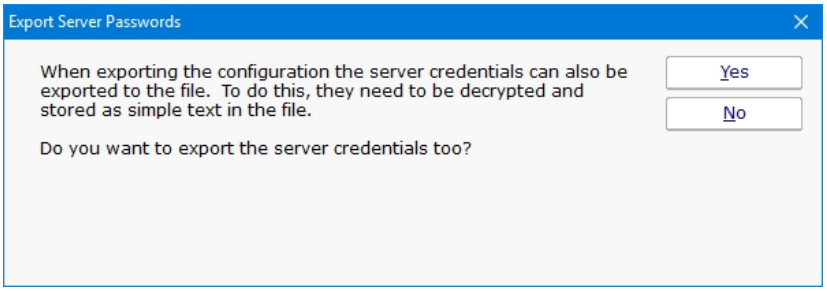
Exporting saves PA Server Monitor configuration data to a XML formatted file. Importing is loading the PA Server Monitor XML file in and restoring the configuration.

Exporting Complete Configuration

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:



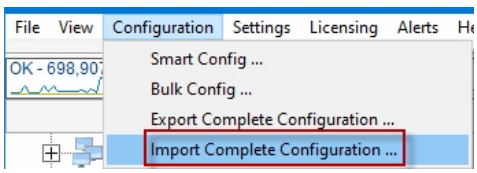
The credentials will be decrypted and visible as plain text in the output file, so you may wish to answer "No" to this prompt.

A standard "File Save" Windows dialog will let you choose a file name, and a location to save the configuration file at. When you export a Complete Configuration, the default file name will be `PA Server Monitor App Configuration.axml`.

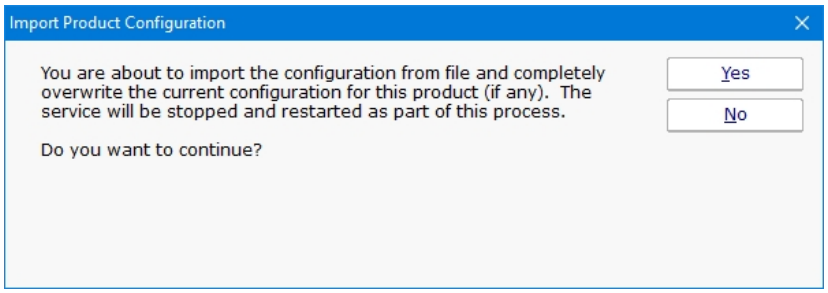
Importing Complete Configuration

Importing a saved PA Server Monitor configuration from file is a simple process. Note: Importing a complete configuration will erase all existing settings. This is an overwrite operation, not a merge.

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 all configured settings in the current instance of PA Server Monitor and replace them with the contents of the configuration file.



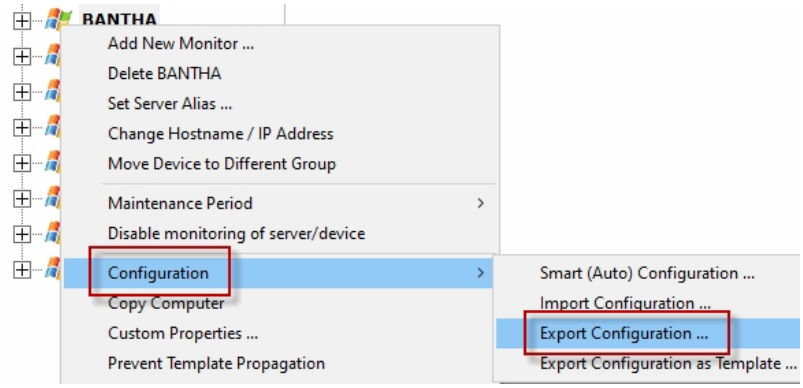
If you answered "Yes" to the question above you will see the standard File Open dialog to select a .axml file that you saved to previously.

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.

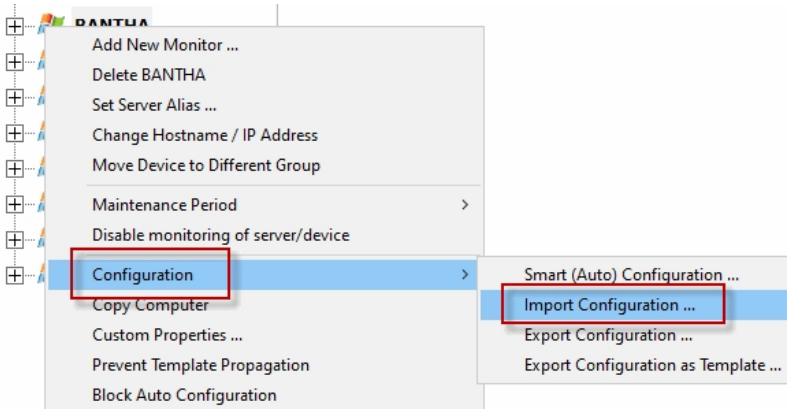
The menu item that selects the export server operation is accessed by right clicking a server or device whose configuration you wish to export. The menu appears as follows.



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

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 from a previous export operation.



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 an existing computer object that you have already created in PA Server Monitor.

Locking Monitors and Actions

There might be cases where a monitor or action is critical in its functionality and should not be changed in any way, even by users with administrator rights. This is when locking is useful.

Locking a monitor or action will prevent changes to that monitor or action's configuration. Monitors can still be disabled or be put into maintenance mode, but the configuration cannot be changed.

When a monitor or action is locked, the Apply button will be disabled and show a lock icon, such as this:

The Configuration Audit report can also show which monitors and actions are locked.

How to Lock

A monitor can be locked via Bulk Config's "Monitors: Lock Monitors" operation. It can also be locked in the monitor's Advanced Options > Miscellaneous tab.

An action can be locked via Bulk Config's "Actions: Lock Actions" operation.

Unlocking!

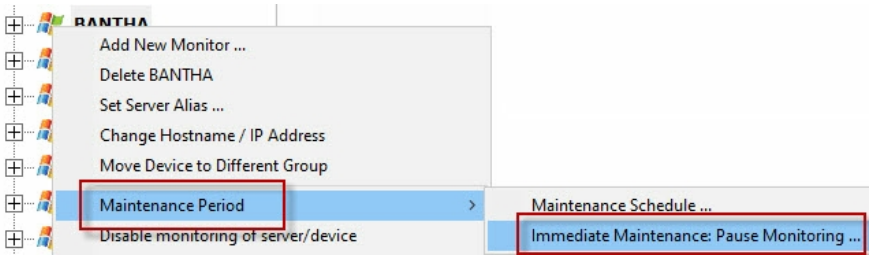
Because locking a monitor or action is meant to prevent even administrators from making changes, the only way to unlock it is to login to the Console on the Central Monitoring server, and from there run Bulk Config's "Monitors: Unlock Monitors" or "Actions: Unlock Actions" operation.

Maintenance Mode

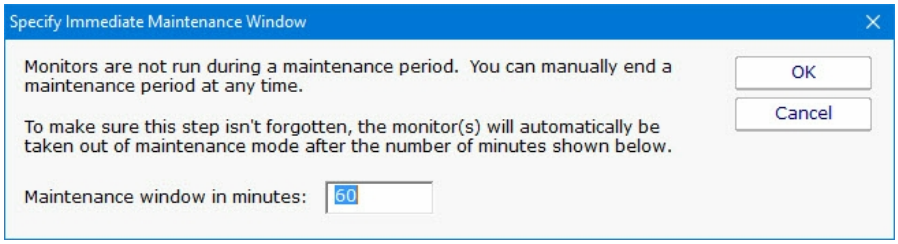
Maintenance Mode is very useful when you'll be working on a computer that is being monitored. Naturally you don't want to receive alerts or have the monitoring service try to correct things that you are working on. Instead of stopping the monitoring service (and potentially forgetting to start it again),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

Manual Maintenance

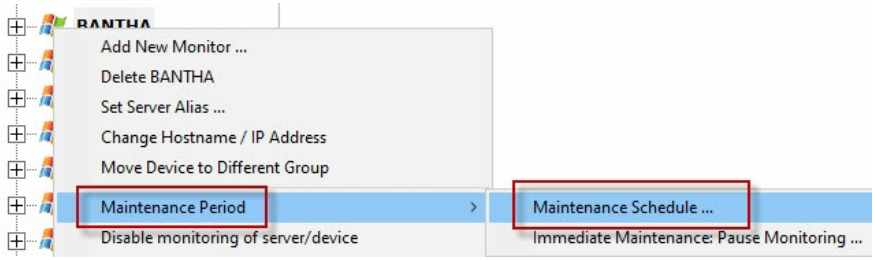
You manually put a server into maintenance mode immediately by right clicking on the computer and choosing Maintenance Period -> Immediate Maintenance: Pause Monitoring.



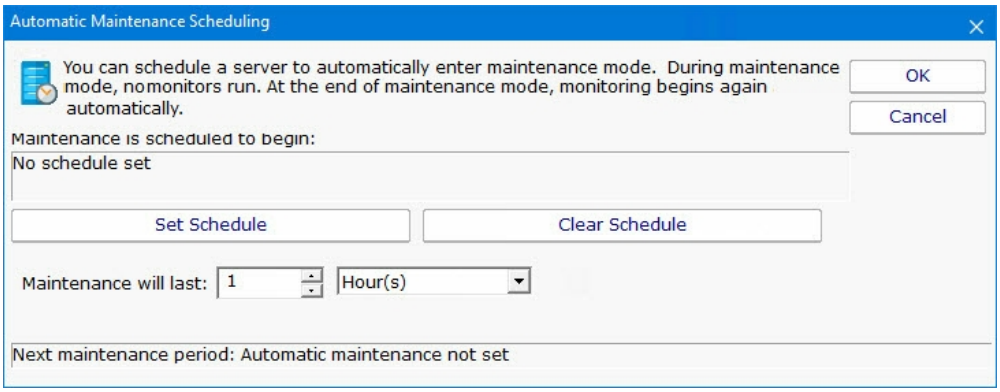
When you enter Maintenance Mode, you specify how long you expect to be working on the server. No further monitoring of the server will take place until that amount of time has past. Then active monitoring of the server begins again automatically.



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.


Automatic Maintenance Scheduling
You can schedule a server to automatically enter maintenance mode. During maintenance mode, nomonitors run. At the end of maintenance mode, monitoring begins again automatically.
OK
Cancel
Maintenance is scheduled to begin:
No schedule set
Set Schedule
Clear Schedule
Maintenance will last:
1
Hour(s)
Next maintenance period: Automatic maintenance not set

PA Server Monitor for Android

A free Android application is available for PA Server Monitor to help you keep track of your servers and network while on the go.

Download from Google Play:
https://play.google.com/store/apps/details?id=com.poweradmin.android.servermonitor

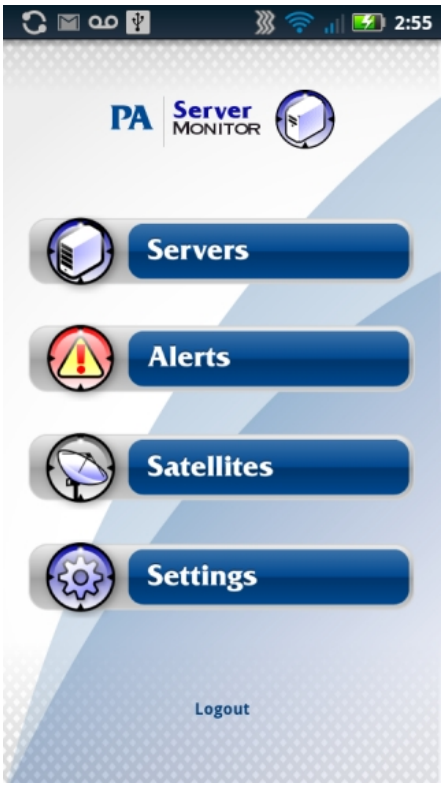
App Prerequisites

To use the Android application, you need to do the same steps that are required before you can launch a Remote Console, namely:

1. Enable SSL for the embedded HTTP server
2. Specify login usernames and passwords

Application Startup

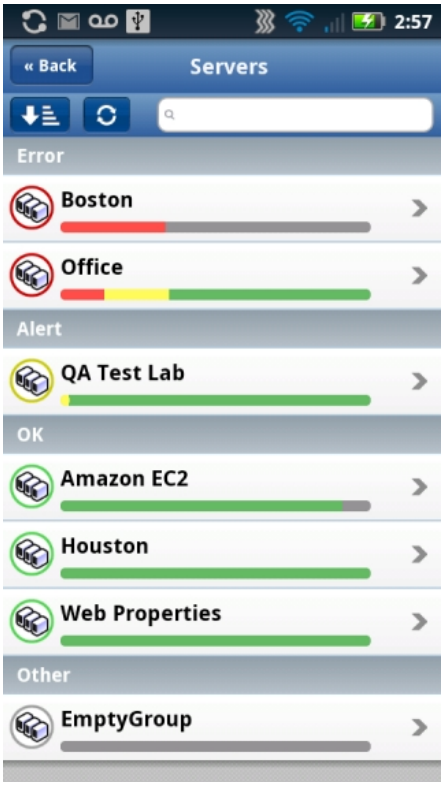
Log in to the application using the same server settings and credentials as you would use when running a Remote Console.



Server Groups

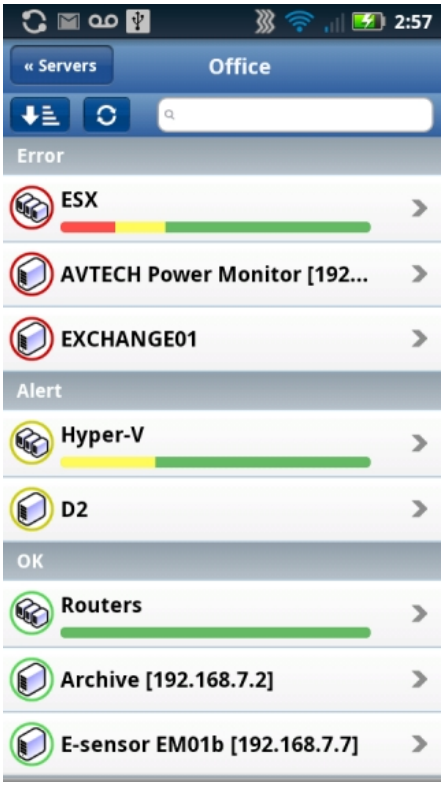
Click the Servers button to navigate through your servers and groups.

The group health bar gives you a rough idea of the health of the servers within that group. The more red or yellow you see, the more servers that have one or monitors that are in the error or alert state.



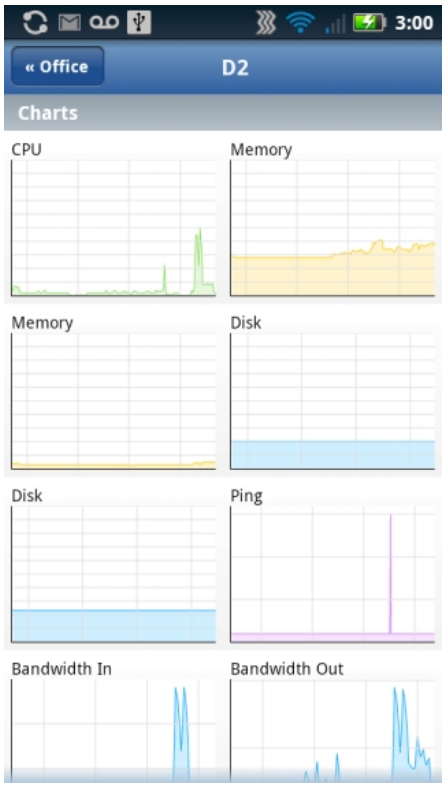
Clicking the sort/group button in the upper left brings groups with problems to your attention by listing them first. In the image above,

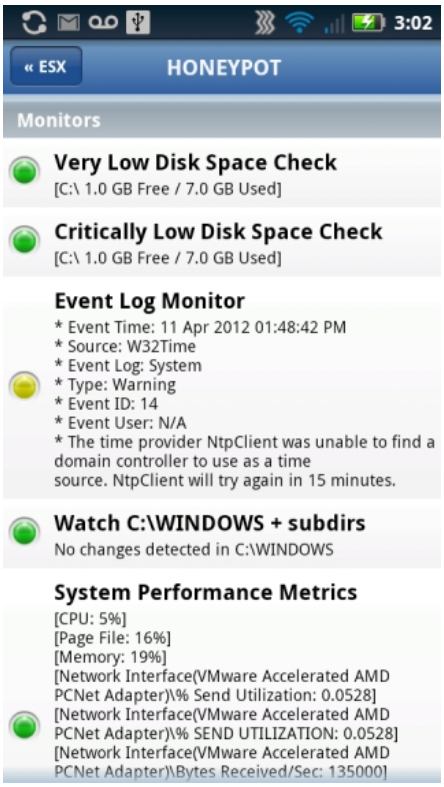
the Office group has some some error and a few more alert monitors somewhere. Clicking that group will drill down to the Office group.



Drilling down to the Office group shows the EXCHANGE01 server is red, which means one or more monitors on that server are red. You can click the server to drill down further. A couple of other groups within the Office group have some yellow -- they will need to be investigated as well.

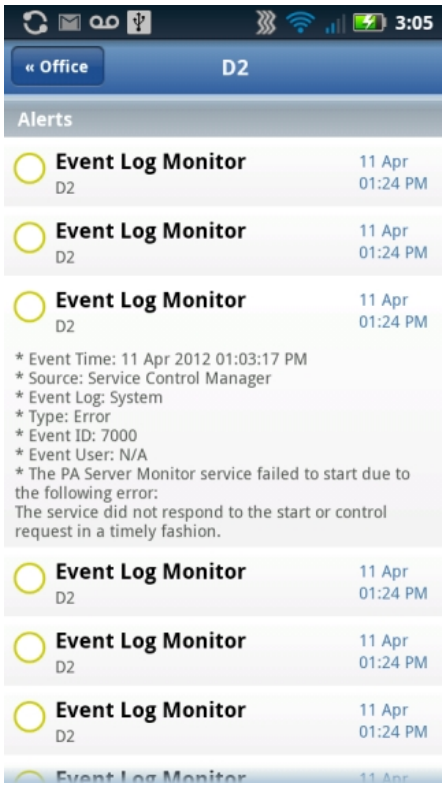
Servers

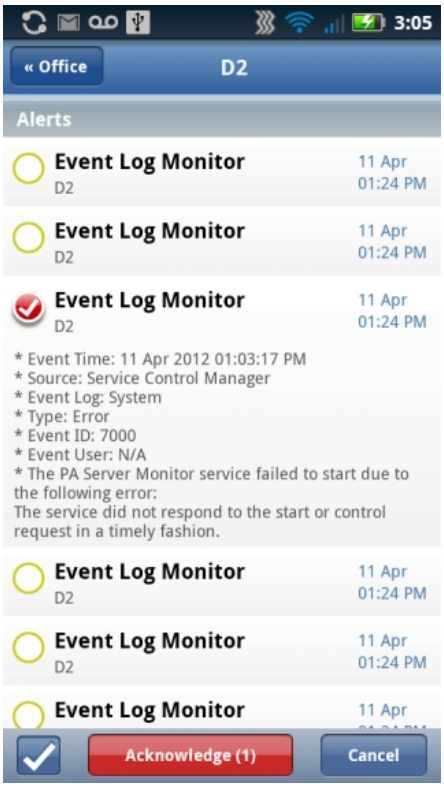




Clicking an individual server will show charts for that server (if any), monitors with their current status, and recent alerts at the bottom. Individual charts can be clicked to zoom in.

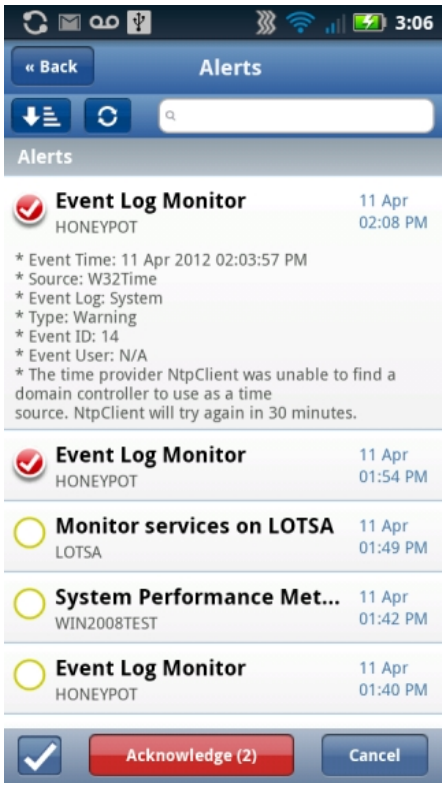
Acknowledge Server Alerts

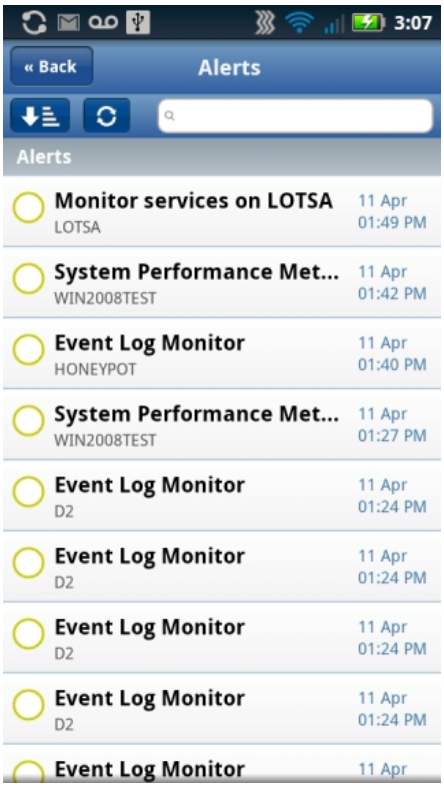




Scroll down to the bottom of a server view to see recent alerts. Click individual alerts to expand them and see more details about the alert. Click the circle at the left to select the alert to be acknowledged.

Global Alert List





You can also press the Alerts button on the home screen to see a global list of recent alerts. These alerts can be sorted/grouped just like servers. They can also be acknowledged. And, using the search bar, you can filter for entries that contain the specified text.

PA Server Monitor for iPhone

A free iPhone application is available for PA Server Monitor to help you keep track of your servers and network while on the go. Receiving iPhone Notifications is also possible by installing the application.

Download from iTunes:
http://itunes.apple.com/us/app/pa-server-monitor-for-iphone/id492253481?ls=1&mt=8

App Prerequisites

To use the iPhone application, you need to do the same steps that are required before you can launch a Remote Console, namely:

1. Enable SSL for the embedded HTTP server
2. Specify login usernames and passwords

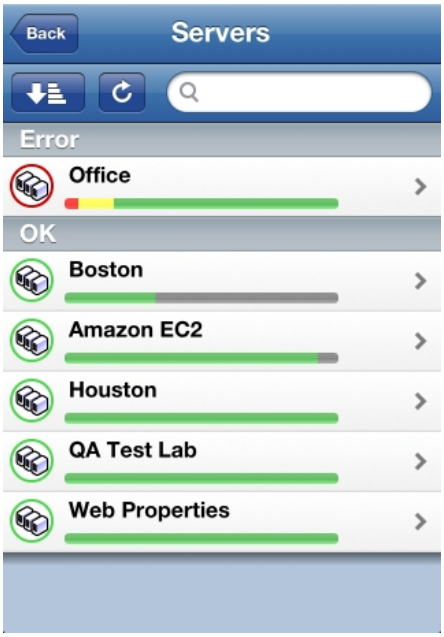
Application Startup

Log in to the application using the same server settings and credentials as you would use when running a Remote Console.

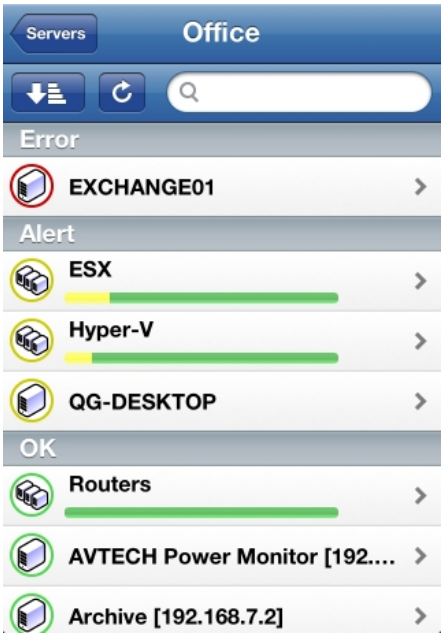
Server Groups

Click the Servers button to navigate through your servers and groups.

The group health bar gives you a rough idea of the health of the servers within that group. The more red or yellow you see, the more servers that have one or monitors that are in the error or alert state.

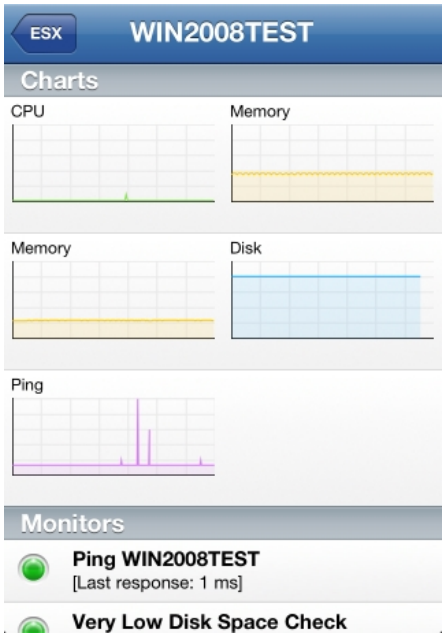


Clicking the sort/group button in the upper left brings groups with problems to your attention by listing them first. In the image above, the Office group has some some error and a few more alert monitors somewhere. Clicking that group will drill down to the Office group.



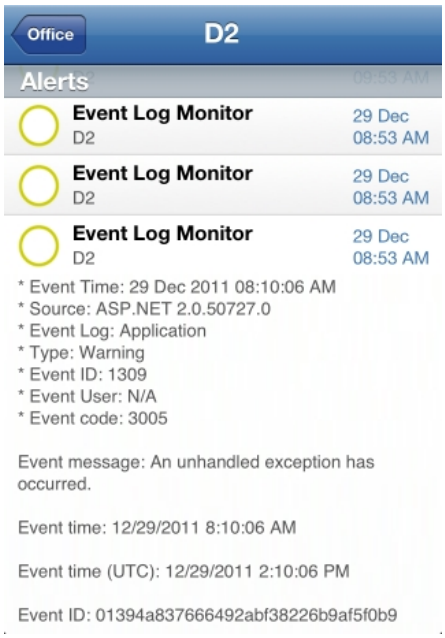
Drilling down to the Office group shows the EXCHANGE01 server is red, which means one or more monitors on that server are red. You can click the server to drill down further. A couple of other groups within the Office group have some yellow -- they will need to be investigated as well.

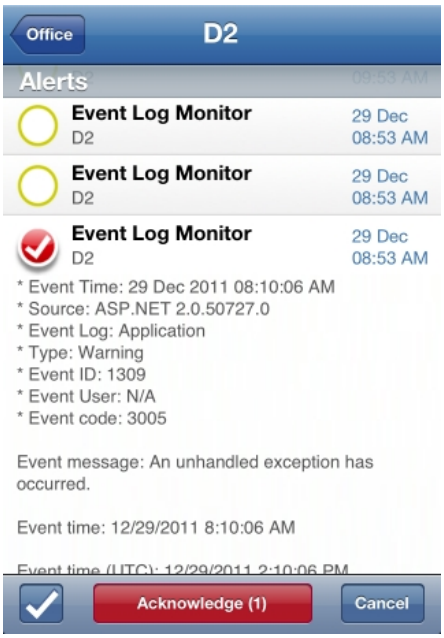
Servers



Clicking an individual server will show charts for that server (if any), monitors with their current status, and recent alerts at the bottom. Individual charts can be clicked to zoom in.

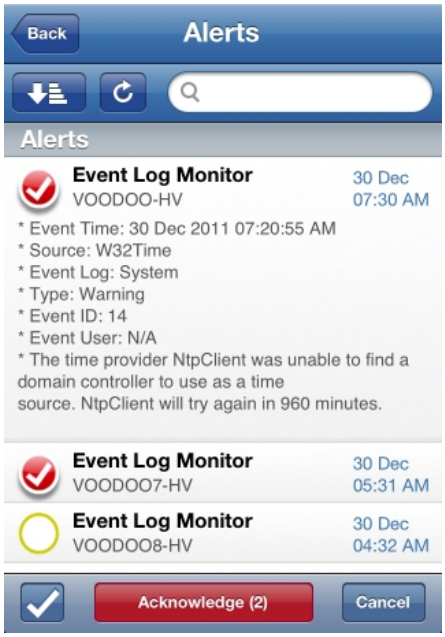
Acknowledge Server Alerts

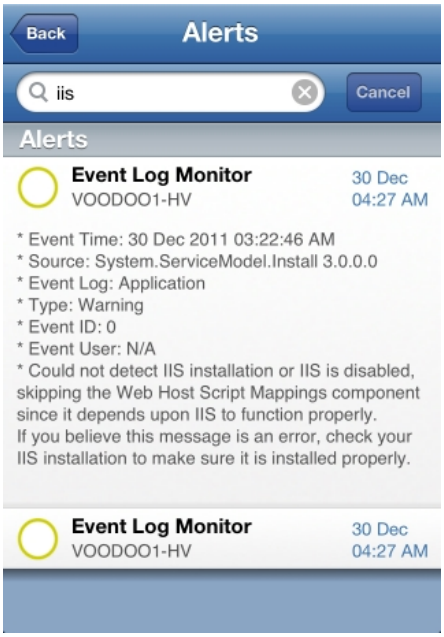




Scroll down to the bottom of a server view to see recent alerts. Click individual alerts to expand them and see more details about the alert. Click the circle at the left to select the alert to be acknowledged.

Global Alert List

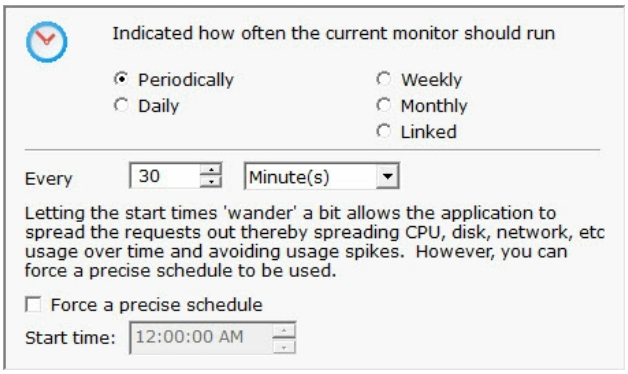




You can also press the Alerts button on the home screen to see a global list of recent alerts. These alerts can be sorted/grouped just like servers. They can also be acknowledged. And, using the search bar, you can filter for entries that contain the specified text.

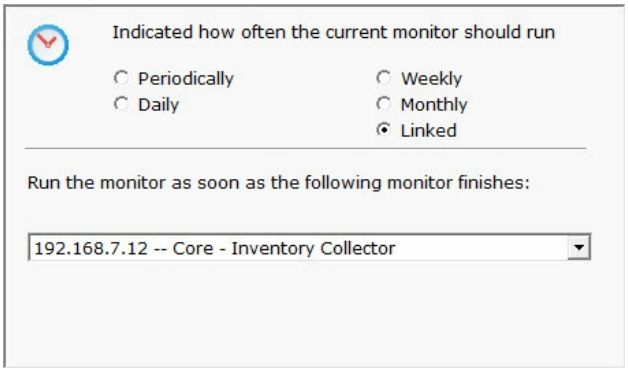
Monitor Schedule

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



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

An additional option, Linked, lets you specify that a monitor should run immediately after another monitor finishes. This is useful in cases where two monitors need to work together, or perhaps see the same underlying system state.



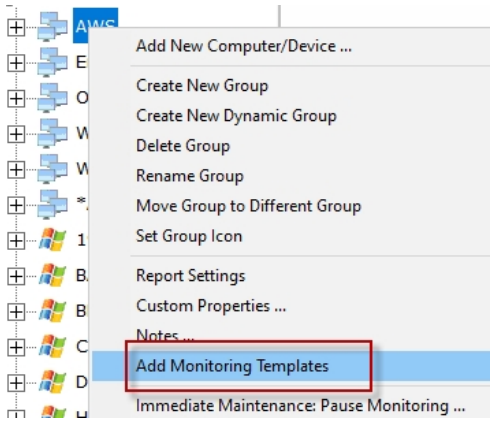
Advanced Options for most monitors will also let you specify a time during the week (in 30 minute increments) when a specific monitor should not be run. This might be useful during system backup for example.

Monitor Templates

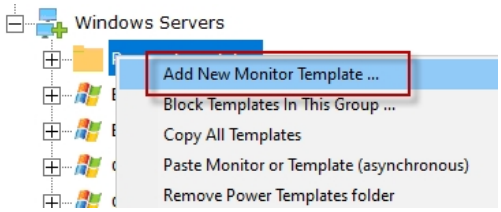
PA Server Monitor has a powerful templating system which can be used in a few ways, and which has features that show up in a couple of different places in the Console application.

Power Templates

Power Templates are templates that can be configured at a group level, and which are then inherited by monitors contained within that group or sub-groups. The first step is to add a Power Templates folder to the group by selecting Add Monitoring Templates from the group's right-click menu.



Once that is done, a new Power Templates folder will exist in the group.

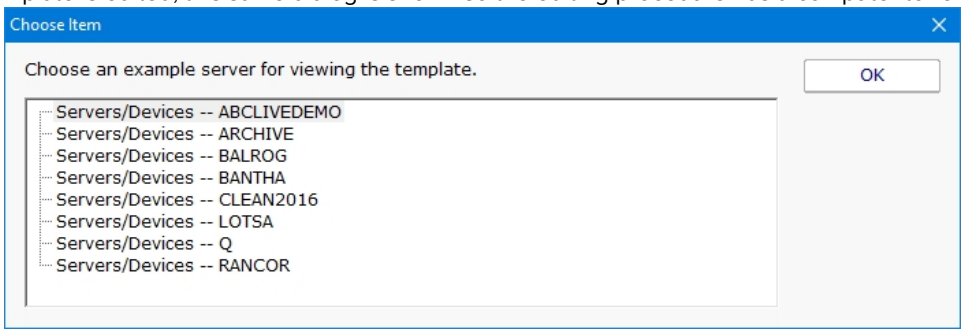


Right-clicking the Power Templates folder reveals a few options:

Add New Power Template

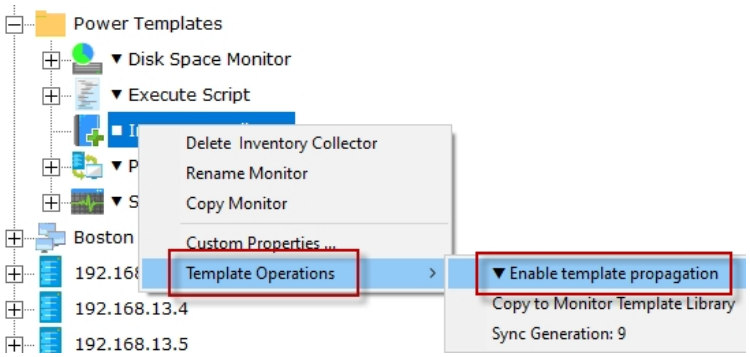
Adding new monitor templates consists of:

1. Choosing an initial computer for the monitor to refer to. This computer is only referred to during monitor configuration. Any time a monitor template is edited, this same dialog is shown so the editing procedure has a computer to refer to if needed.



2. Configuring the monitor normally

Once a template is configured, you'll notice there is one of two symbols before the monitor name. These symbols mean:



■ - The template is not currently propagating down to servers in this group. This is the default state of a new template.

▼ - The template is actively being propagated down to all servers in this group, or within sub-groups. Changes made to the template will also be propagated down.

▲ - This isn't on the template itself, but if you look at a server and see a monitor with this symbol, it indicates this monitor is from a template defined above and cannot be modified directly.

Template Propagation

Monitors that are derived from templates can not be edited -- the monitor configuration is defined by the template. If a template-derived monitor needs to be changed, it can be disconnected from the template, and then edited directly. Changes in the template will no longer change the disconnected monitor. If the disconnected monitor is ever deleted, the template will propagate down to the server again and create a new monitor.

Copying new templates or template updates down to computers within the group happens approximately every minute. If there are many computers within a group the propagation process can take a little while as the template is checked for each computer before it is added.

If a template is deleted, monitors that are derived from it will automatically get deleted within a few minutes.

Remove Power Templates Folder
: This option simply removes the Power Templates folder. The folder must be empty before it can be deleted.

Copy All Templates
: This command will copy all of the templates in the folder into the clipboard. You can then go to a server or the Template Library and paste all of them at once.

Paste Monitor or Template (asynchronous)
: Pasting a monitor to a Power Template folder will create a new template from the source monitor. Anything specific to the original source computer is removed so that the template can work with any server it is propagated to. It's also possible to paste templates that were copied from other Power Template folders, or from the Template Library.

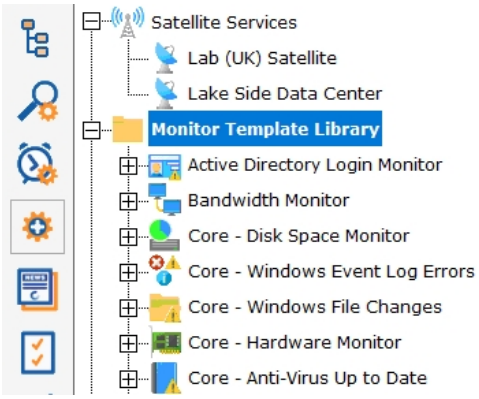
Template Library

Besides the Power Templates that can exist at a group level, there is a Template Library under Advanced Services in the Console. This list of templates is useful for:

A convenient place to store monitor templates that you can copy/paste from

When Smart Config is run, besides showing the normal default monitor options, templates in the Template Library are also listed and

can be used for the Smart Config process.



Security Protected Settings

There are many settings for PA Server Monitor which are available under:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor
```

There are a few settings that are important enough that some customers don't even want administrators to be able to make changes to them. For these cases, there are a few settings in:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor\Protected
```

A separate registry key is used so you can set additional access protections using the operating system to control who can change these settings. Be sure that the PA Server Monitor service can read these settings.

Settings

All settings below can be set to 1 or 0.

AllowExpiredHTTPSCertsInClient
: Any time an internal HTTPS request is made (Console to the Central Server, Satellite to the Central Server, Web Page monitor, etc) a decision has to be made whether to accept a connection to an endpoint that has an expired SSL/TLS certificate. Even if it is expired, the connection is still encrypted. Setting this to 1 allows connections using expired certificates, and 0 blocks those connections. Defaults to 0.

AllowLegacyMobileAppSkip2FA
: Older versions of the mobile application didn't support requesting a 2FA PIN. Set this to 1 to allow them to login without the PIN. Setting to 0 will require a PIN if 2FA is enabled for the user (see User Access). Defaults to 1.

DisableBlankLocalLogin
: When the Console on the Central Monitoring Service is run, if the user is a local administrator they are able to login without a username/password. To disable this, set this value to 1. See Remote Users for defining logins. Defaults to 0.

DisablePasswordExport
: When exporting configuration data, sometimes passwords can be exported as well. Setting this value to 1 will disable exporting passwords. Defaults to 0.

EnableScriptCredentialAccess
: The Execute Script monitor can request configured passwords for the device the script is running for via the $mon.TargetUserName, $mon.TargetUserDomain and $mon.TargetUserPassword properties.

  This can be disabled by setting this value to 0, or enabled by setting to 1. Defaults to 0.

  Because of the concern of scripts exfiltrating credentials, we recommend locking monitors or actions that use the TargetUserName, TargetUserDomain or TargetUserPassword properties.

EnableScriptCredentialAccess_Custom
: If this value is set to 1, the Execute Script monitor or action can request configured Custom credentials for arbitrary devices via the $mon.GetCredentials or $act.GetCredentials function. The functions will fail if this value is set to 0.

  This can be disabled by setting this value to 0, or enabled by setting to 1. Defaults to 0.

  Because of the concern of scripts exfiltrating credentials, we recommend locking monitors or actions that use the GetCredentials function.

EnableScriptCredentialAccess_All
: If this value is set to 1, the Execute Script monitor or action can request any configured credentials for arbitrary devices via the $mon.GetCredentials or $act.GetCredentials function. The functions will fail if this value is set to 0.

This can be disabled by setting this value to 0, or enabled by setting to 1. Defaults to 0.

Because of the concern of scripts exfiltrating credentials, we recommend locking monitors or actions that use the GetCredentials function.

SNAP_AllowTunnel2

SNAP Tunnels allow tunneling a connection to a remote device across the communication link between the Central Monitoring Service and a Satellite Monitoring Service. This is useful for getting to an RDP session on a remote device. Tunnels can be disabled completely by setting this value to 0 on the Central Monitoring Service, or set it to 0 on a Satellite to disable tunnels to that specific Satellite. Defaults to 1.

SNAP_AccessUnmonDevices

When a SNAP Tunnel is created, the creating user's access is checked to confirm they have access to the device. If connecting to an unmonitored device (perhaps by creating a tunnel from the External API) set this value to 1 to disable access checks. Defaults to 0.

SNAP_AllowTunnelFromAnonAPI

The External API can create SNAP Tunnels and requires a username and password. To enable the legacy mode of not requiring credentials, set this value to 1. Defaults to 0.

Monitoring VMWare ESX Hosts

PA Server Monitor monitors virtual machines (guest operating systems) as though they were physical machines.

With VMWare ESX and ESXi *hosts*, ESX specific credentials need to be given. And PA Server Monitor needs to know the server is ESX/ESXi so it knows to use those credentials. This is done by setting the server type.

Once the target server is marked as an ESX host, the standard Performance monitor will retrieve and monitor counters for the host's CPU and memory usage. In addition, installed and running VM counts can be monitored.

Further, SNMP can be enabled on the ESX/ESXi host so additional counters can be watched, both natively via the SNMP monitor and via the simulated counters in the Performance monitor.

To enable SNMP you need to use the vSphere Command Line interface and run the following commands:

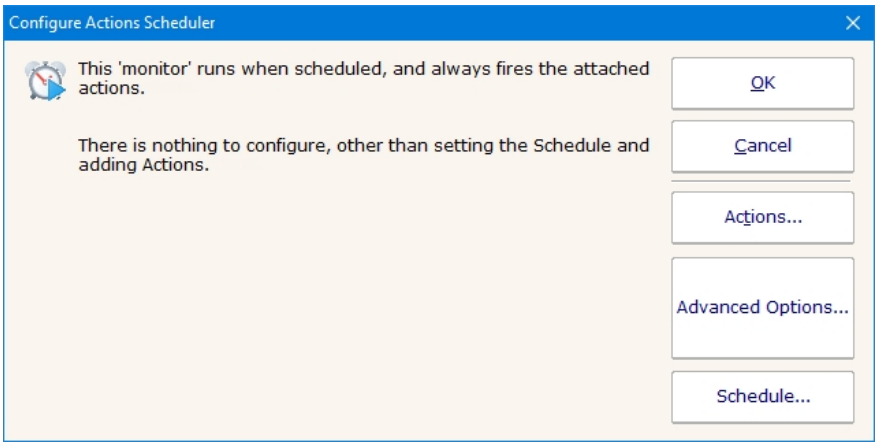
```
#enable SNMP
vicfg-snmp.pl --server {server_name} --username root --password xxxxxxx -c readcommunity

#enable SNMP Trap
vicfg-snmp.pl --server {server_name} --username root --password xxxxxx -t
{trap_target_server}@162/trapcommunity

#enable SNMP daemon
vicfg-snmp.pl --server {server_name} --username root --password xxxxxxxx --E
```

(Thanks to Mikael in Sweden for passing on this tip)

Actions Scheduler 'Monitor'

The Actions Scheduler 'monitor' is not really a monitor like all others. It does not check for a condition and alert if that condition is found. Instead, every time the monitor runs, it executes all actions that are attached.

This 'monitor' makes it very easy to schedule IT automation tasks by simply setting the schedule for when the tasks should run, and adding the Actions that you want to run.



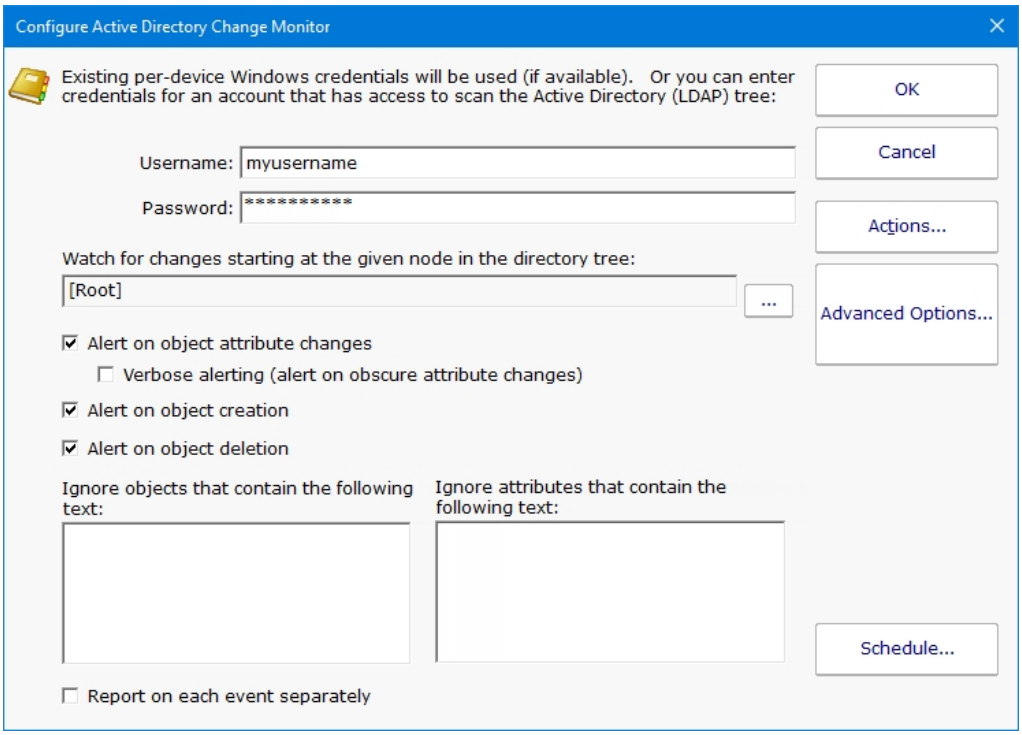
Standard Configuration Options

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

Active Directory Change Monitor

The Active Directory Change Monitor watches the Active Directory and records object changes to a database. It can alert on an object or attribute change, object creations or deletions, and run reports later to see a history of changes.

All object changes get written to the database, for full historical reporting capability. To alert on specific types of changes, check the appropriate box.



The username and password are used to connect to Active Directory and scan the directory tree. The domain should not be given in the username field.

In the above example, the node of the Active Directory tree is selected to be monitored. Alerting is set up to alert on attribute changes and object creation and deletion.

Alerting on Attributes

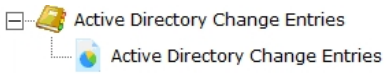
Each object in Active Directory has many attributes, some of them are more common than others. If the "Alert on object attribute changes" option is selected, the most common attributes are monitored. If the "Verbose Alerting" option is selected, the more obscure attributes are also monitored.

Objects or attributes that contain specific text phrases can be ignored by entering the text in one of the Ignore entry boxes.

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

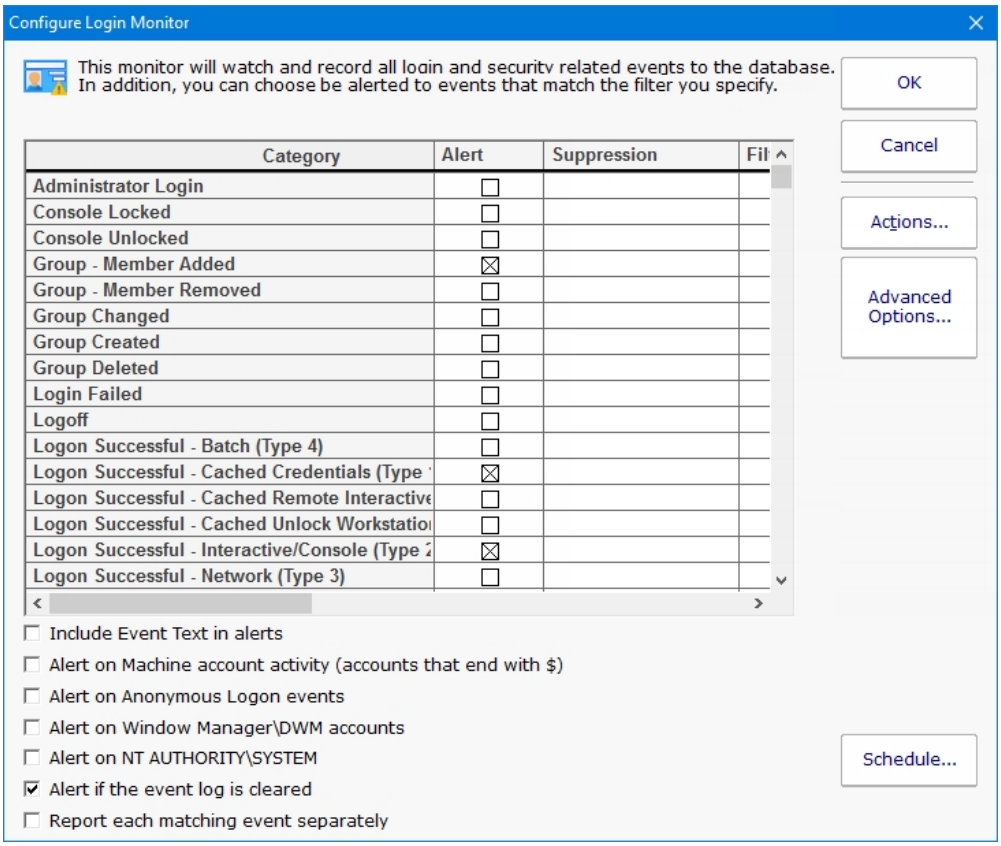


You can run reports that list the differnt types of changes to the Active Directory in HTML or .CSV files for importing into Excel, etc.

Active Directory Login Monitor

The Active Directory Login Monitor watches the Security Event Log and records logins to a database. It can also alert for certain login events, and run reports later to see a history of logins.

The monitor is powerful, yet simple to setup. All events get written to the database so you have full reporting capability later. To alert on specific events, check the box next to the category.



Login Event Categories

There are many types of logins and similar events that the monitor will watch. These events are grouped into the following categories:

> Note: 3-digit Event IDs are generally for Windows 2003 and earlier. In addition, some Event IDs are listed in multiple categories. In that case, information within the event is checked to determine which category the event should be assigned to.

Category	Included Event IDs
Logoff	538, 551, 683, 4634, 4647, 4779
Logon Failed	529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 675, 4625, 4768, 4771, 4772, 4825
Administrator Logon	576, 4672

Logon Suceeded - Interactive (Logon Type 2 - Console)	528, 540, 4624
Logon Suceeded - Interactive - Cached Credentials (Logon Type 11)	528, 540, 4624
Logon Suceeded - Remote Interactive (Logon Type 10 - RDP, etc)	528, 540, 4624
Logon Suceeded - Remote Interactive - Cached Credentials (Logon Type 12 - RDP, etc)	528, 540, 4624
Logon Suceeded - Unlock Workstation (Logon Type 7)	528, 540, 4624
Logon Suceeded - Unlock Workstation - Cached Credentials (Logon Type 31)	528, 540, 4624
Logon Suceeded - Network (Logon Type 3)	528, 540, 4624
Logon Suceeded - Batch (Logon Type 4)	528, 540, 4624
Logon Suceeded - Service (Logon Type 5)	528, 540, 4624
Logon Suceeded - Network Clear Text (Logon Type 8)	528, 540, 4624
Logon Successful - Different Credentials	528, 540, 4624

Other Security Categories

In addition to login tracking, there are other events that are tracked that involve security, such as user and group changes, accounts and consoles locked, etc.

Category	Included Event IDs
Console Locked	4800, 4802
Console Unlocked	4801, 4803
Group Created	631, 635, 658, 694, 4727, 4731, 4754, 4783, 4790
Group Deleted	634, 638, 662, 693, 696, 4730, 4734, 4758, 4789, 4792
Group Changed	639, 641, 659, 668, 695, 4735, 4737, 4755, 4764, 4784, 4791
Member Added To Group	632, 636, 660, 689, 4728, 4732, 4756, 4785
Member Removed From Group	633, 637, 661, 690, 4729, 4733, 4757, 4786
Security Alert (DoS, replay, and IPsec events)	4646, 4649, 4976, 4977, 4978
User Account Created	624, 4720
User Account Deleted	630, 4726
User Account Changed	608, 609, 642, 685, 4704, 4705, 4738, 4781
User Account Enabled	626, 4722
User Account Disabled	629, 4725
User Account Locked Out	644, 4740, 6279
User Account Unlocked	671, 4767, 6280
User Credentials Change Succeeded	627, 628, 4723, 4724, 5377
User Credentials Change Failed	627, 4723, 4724

Configuration Options

Suppression

There are some events, such as failed login attempts, that you only care about if there are a lot of them in a short amount of time (indicating some sort of break in attempt). The Suppression setting lets you configure a threshold for how many have to happen before an alert is fired.

Filtering

If there are specific accounts, workstations, etc, that you don't want to be alerted about, you can exclude them, or only include specific targets. The filter text is checked against the entire Event Log Event text, so it can target any part of the event.

Definitions

To see specifically which Event IDs are included in each category, scroll to the right and there is Definition column. Hover the mouse

over any row to see the Event IDs in that category.

Non-Human Accounts

Windows has many types of logins, including:

Normal - typical user logins

Machine Accounts - this is when Windows itself performs a login to a different computer

Windows Manager/DWM - newer versions of Windows have Desktop Windows Manager that logs in along side each user

Anonymous Logons - usually to access publicly available resources

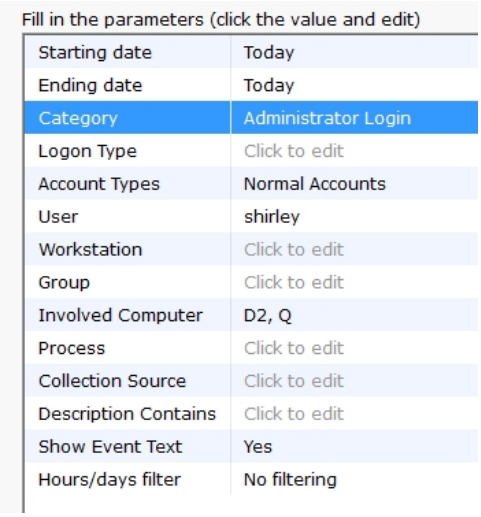
NT AUTHORITY\SYSTEM - these usually represent the operating system requesting access to local resources

By default, the non-normal login types are ignored, but you can choose to alert on them if they are of a category that is being monitored.

Reporting

There are a few different types of reports available that make it easy to find out what login activity happened.

The Login Events report is especially flexible with many options for selecting the events you want to see, as shown below.



Not all fields make sense for all event types. So you would just fill in the details you care about and let the report find the appropriate events for you.

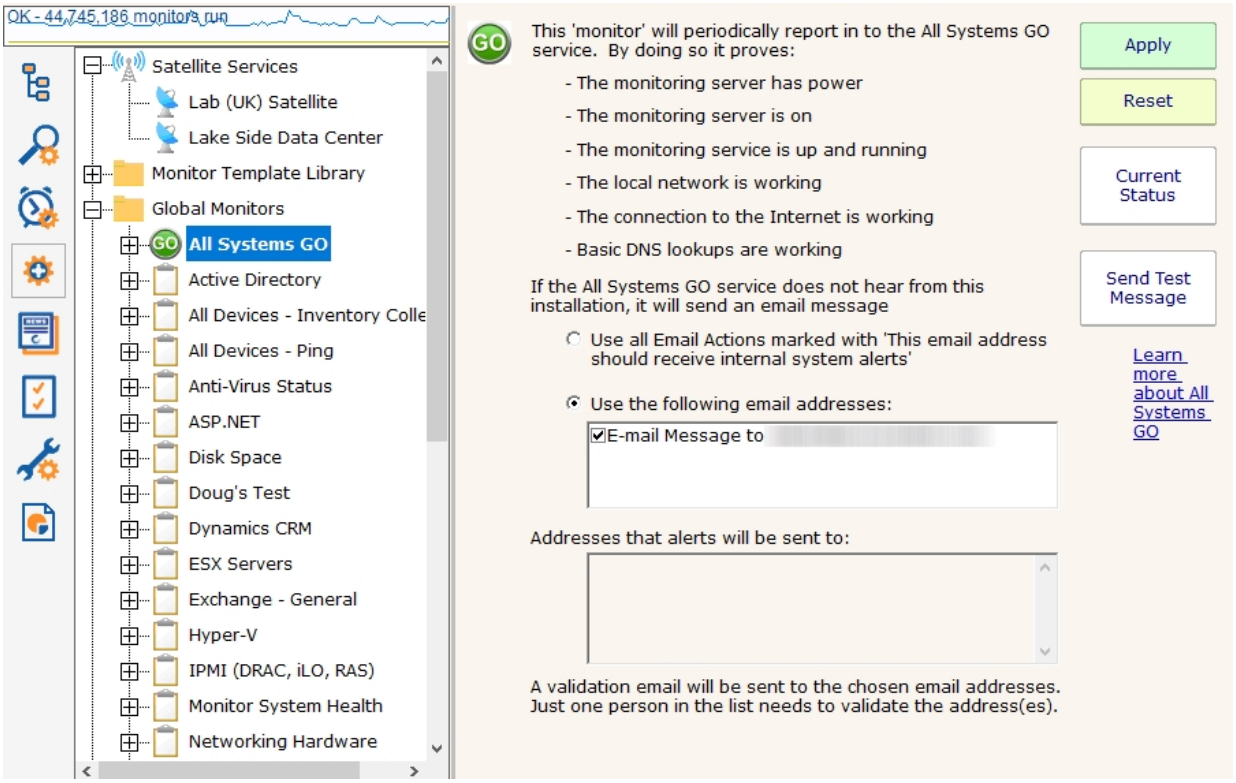
Standard Configuration Options

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

All-Systems-GO Monitor

The All-Systems-GO 'monitor' is a monitor in name only. It is actually a way to get your monitoring installation to check in to the All-Systems-GO service (a free service) to make sure if anything happens with your monitoring server, or the infrastructure/environment that it uses, you find out about it. It's a monitor for the monitor.

The All-Systems-GO Monitor is a Global Monitor, and only one ever needs to be created.



The only thing to configure in the monitor are which email addresses (from email actions) should be emailed if the monitoring service does not check in with the All-Systems-GO service.

When the monitor is setup, an activation email will get sent to the email addresses that were specified. Just one of those addresses needs to click the link in the activation email to indicate this installation is particating in All-Systems-GO. Email actions can be added or removed from this configuration screen to control which email addresses would receive notifications should the installation not check in.

The **Current Status** button indicates if this installation is successfully connecting to the All-Systems-GO service.

The button colors indicate the connection status with the All-System-GO service:

Green - everything is OK

Yellow - the email addresses have probably not been validated. Click the button to see more information.

Red - the All-Systems-GO service doesn't know anything about this installation. ***The button will be red when the monitor is first created***, and will turn yellow or green once the monitor has run.

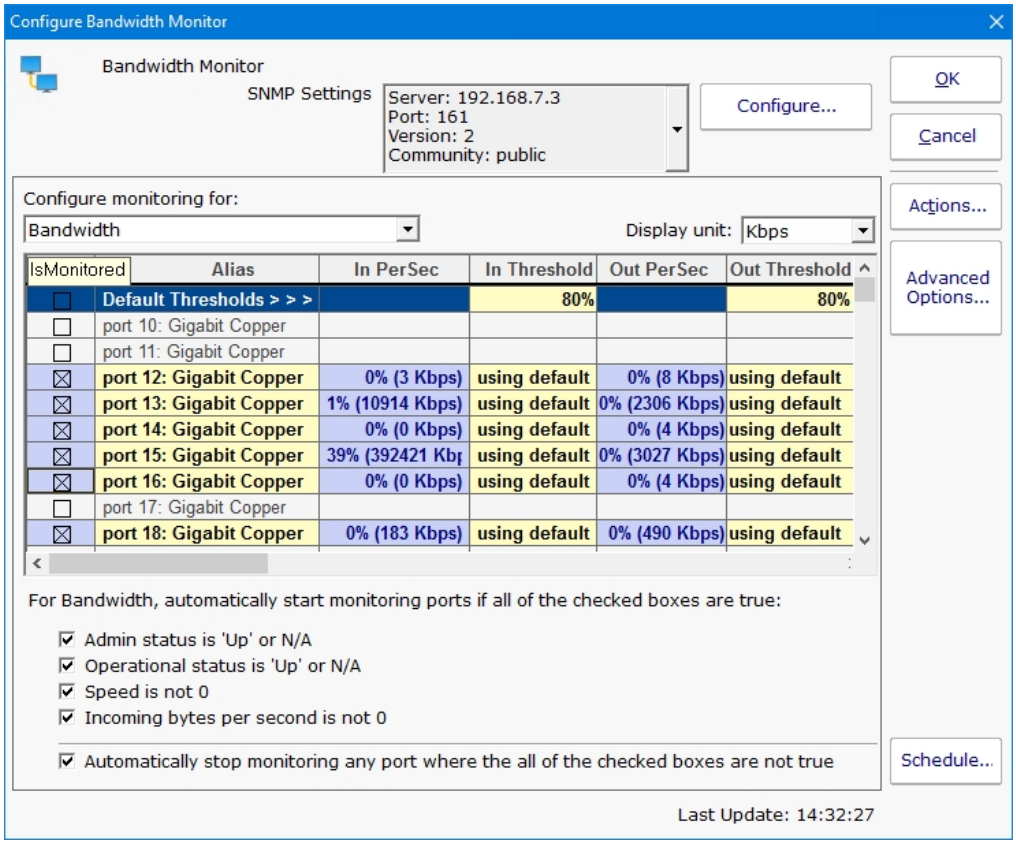
Pressing the Current Status button will display more details, as well as the most recent times and email addresses where alerts were

sent.

If the link in the activation email mentioned above was never clicked, pressing the Current Status button will trigger another email to get sent out.

Bandwidth Monitor

The Bandwidth Monitor can retrieve data from SNMP counters (ifTable and ifXTable) and from Windows (Network Interface counters). Different types of data (data rates, error counts, etc) can be monitored, recorded, and alerted on.



The configuration dialog above shows the Bandwidth Monitor. Notice the drop drop-down menu has selected Bandwidth as the values that are being shown. It can be set to one of the following values:

Bandwidth

Error Count

Discard Count

Multicast Count

Broadcast Count

Unicast Count

Non-Unicast Count

Each Bandwidth Monitor can watch one of the value types above. If you wanted to watch Bandwidth and Error Counts for example, create two Bandwidth Monitors.

The Bandwidth value needs a unit (Bps, MBps, etc) which can be specified. The other counter types are simply a counter value.

In the discussion below, *ports* will be referred to as switches are often monitored. If a Windows computer is being monitored, *ports*

would refer to *network interfaces*.

The grid shows the different ports that were found when inspecting the device. You can change the port name to an alias that is more meaningful.

The first port, IsMonitored, indicates whether a port is being monitored. Ports that are monitored get a different color. Cells that are yellow can be edited. That means the Alias, and In Threshold and Out Threshold columns can be changed for monitored ports.

For each port, the current incoming and outgoing value are shown, and an optional threshold value that you can set.

By scrolling to the right, there are more columns as shown below.

Alert After	Speed	Op Status	Admin Stat	Description
using default	100000 Kbps	up [1]	up [1]	port 16: Gigabit Copper
using default		down [2]	up [1]	port 17: Gigabit Copper

Name	Type	Connected	In CurrVal	Out CurrVal
port 16: Gigabit Copper	ethernet-csmacd [6]		752	177
port 17: Gigabit Copper	ethernet-csmacd [6]		0	0

The Alert After column lets you indicate how long a port has to be over its threshold before alerting. Values are set in minutes and should be specified like "1 Minute" or "15 Minutes".

In addition, values such as the port's speed, operational and admin status are shown. Description and Name are retrieved and cannot be changed. Since Windows does not support these values, N/A will be shown for Op Status, Admin Status, Type and Connected.

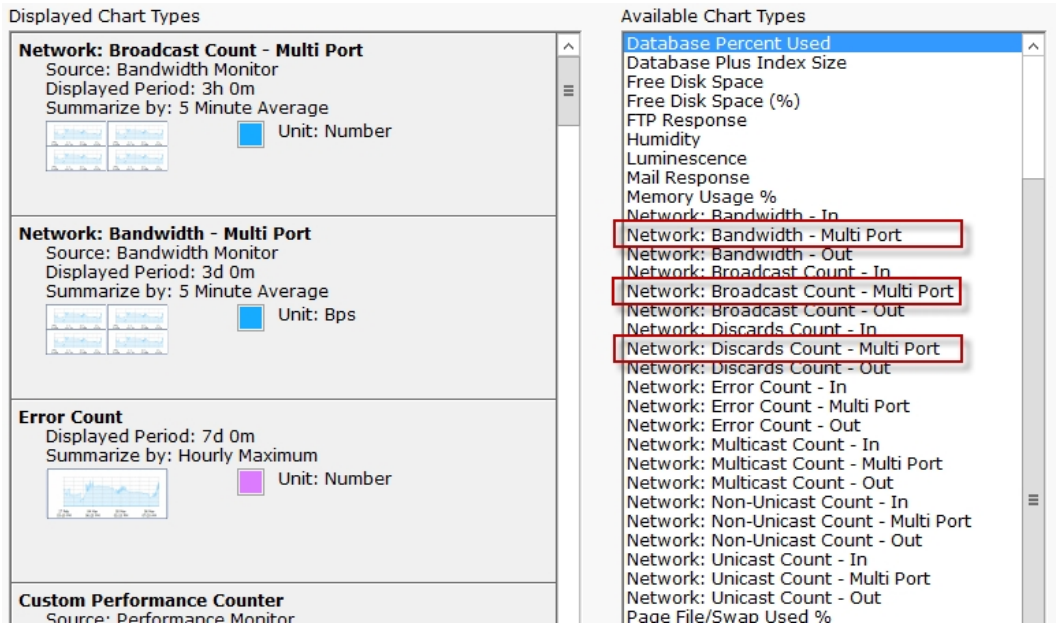
The last two columns are just for diagnostic purposes - they show the raw per-second value coming from the counter, without any units being applied.

Automatically Adding and Removing Ports for Monitoring

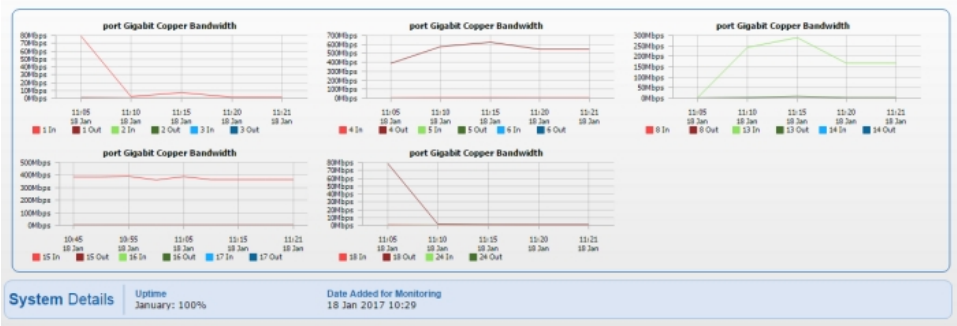
For a large switch, or for counters coming from a computer where network hardware is changed, the available ports be added or removed, or their status might change (from being used to no longer in use, etc). The check boxes at the bottom of the monitor enable automatic monitoring of newly added/active ports, or to stop monitoring removed/disabled ports.

Multi-Port Chart

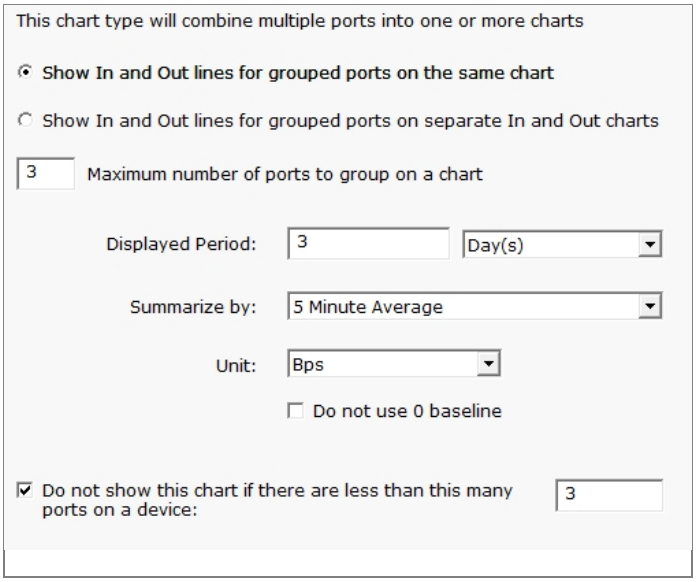
Most monitors can show configurable charts for data that is retrieved. The Bandwidth Monitor can show charts for each kind of data that is retrieved (Bandwidth, Error Count, etc). Because the Bandwidth monitor can track so many ports, and this data is frequently charted, a special Multi-Port chart is available to show the bandwidth data together. Examples are shown below (this image comes from the chart configuration screen).



The Multi-Port chart creates a large chart area with multiple charts within it. Ports, and their input/output values can be grouped together in a variety of ways.



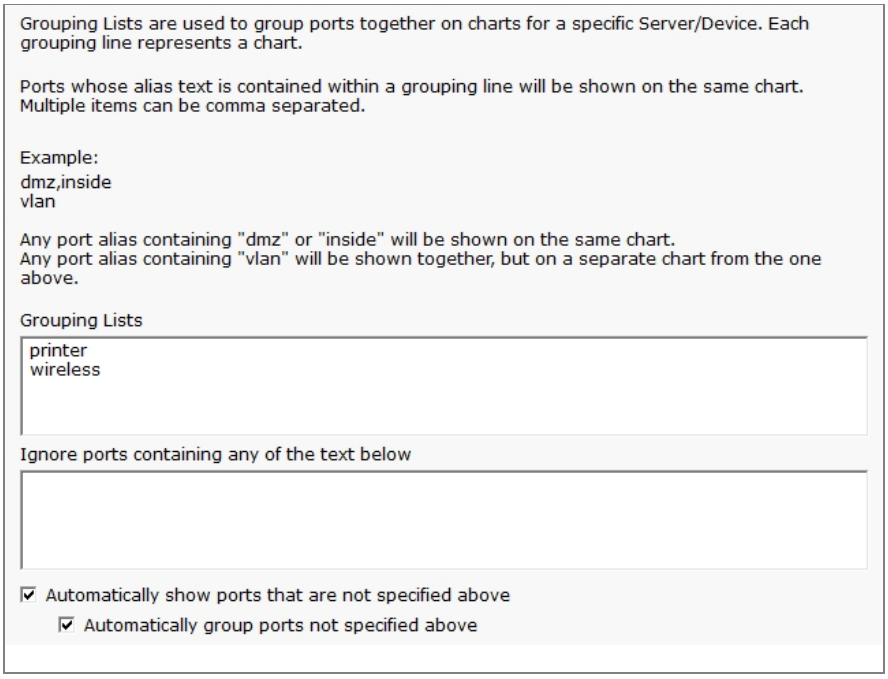
The configuration dialog for the Multi-Port chart is larger than most, so we'll split it in half and look at each half separately.



The first half of the dialog controls grouping. Each port has an input and an output value. Some customers want to see all inputs on

one chart, and all outputs on a separate chart. Both options are possible. In addition, because showing a large number of ports on each chart would make it hard to read, you can indicate only a certain number should be shown. Additional charts will be created as needed to handle all of the ports.

Also note that if a device has fewer than a specified number of ports (3 in this example), the Multi-Port chart won't be used. This allows you to specify a Multi-Port chart at a high level (at Servers/Devices) and if the chart is not appropriate (perhaps for computers where only a single NIC is being monitored) it won't be shown. In addition, if a port is shown in the Multi-Port chart, it won't also be shown in a separate single-port chart (like Network: Bandwidth In).



The second half of the dialog lets us control how the ports are grouped together. By default they are grouped together numerically (i.e. the first X ports are together, and then the next X ports, etc). You can group the charts based on their alias. In the example above, any ports that have 'printer' in their alias will get grouped together into a chart, and any that have 'wireless' in their alias will get grouped together in a separate chart.

In addition, ports can be ignored and not charted at all, again based on the alias.

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.

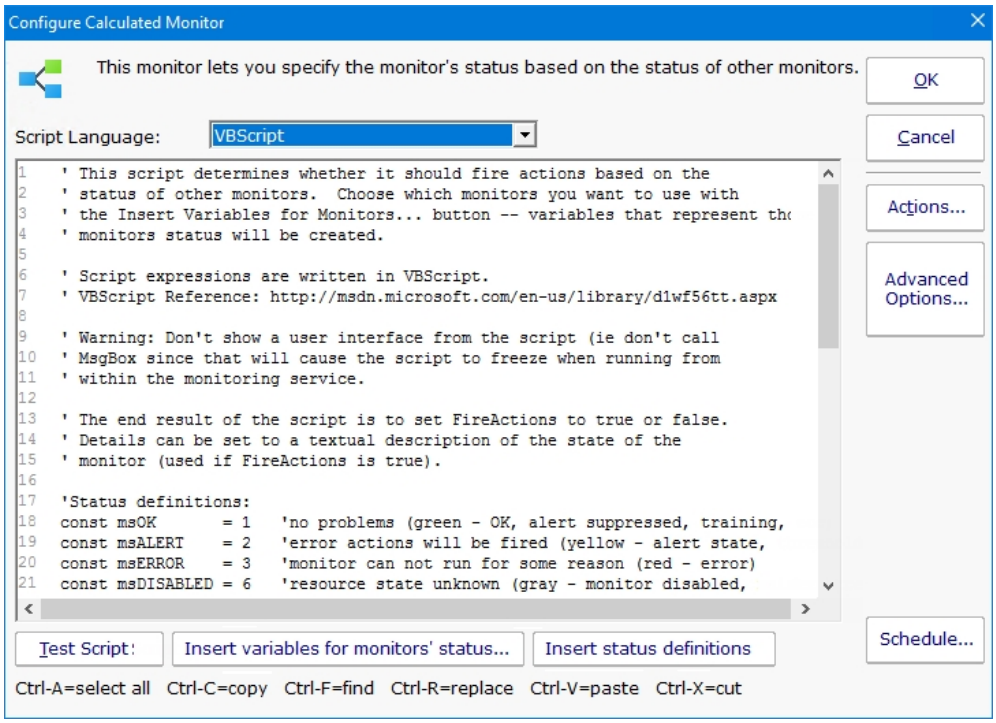
Calculated Status Monitor

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 either the VBScript or Javascript language. You can select the language to use in the **Script Language** dropdown box. The final output is the status for the monitor. For example, look at the example script below (a somewhat similar default script is created for you automatically):

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

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

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

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

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



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

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

Standard Configuration Options

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

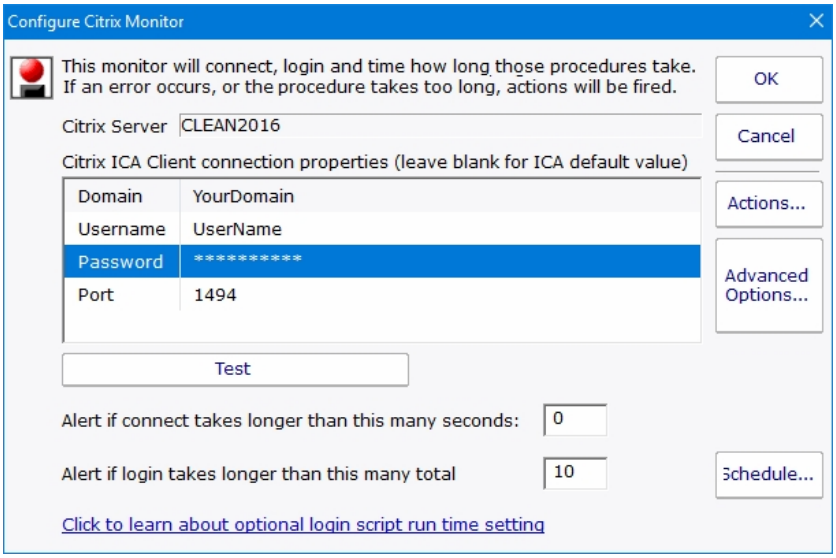
Citrix Monitor

The Citrix monitor is a simple "health check" of a Citrix Virtual Apps and Desktops server (formerly XenApp and XenDesktop). 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.



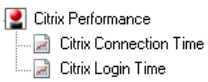
You need to enter the domain name, user name, and password into the dialog. If the Citrix server is configured for a non standard port, you need to enter that port value too.

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:

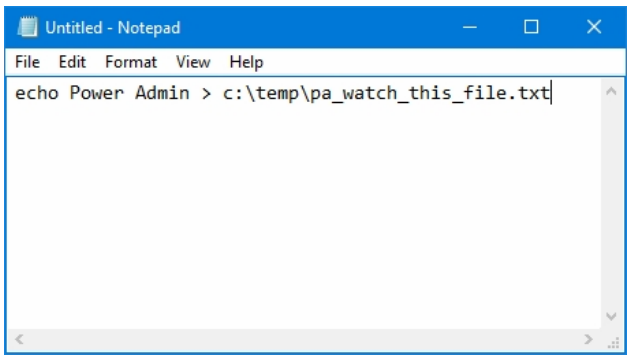
```
HKEY_LOCAL_MACHINE\SOFTWARE\PowerAdminServerMonitor  [DWORD]Citrix_LoginScriptRunSeconds
```

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
```

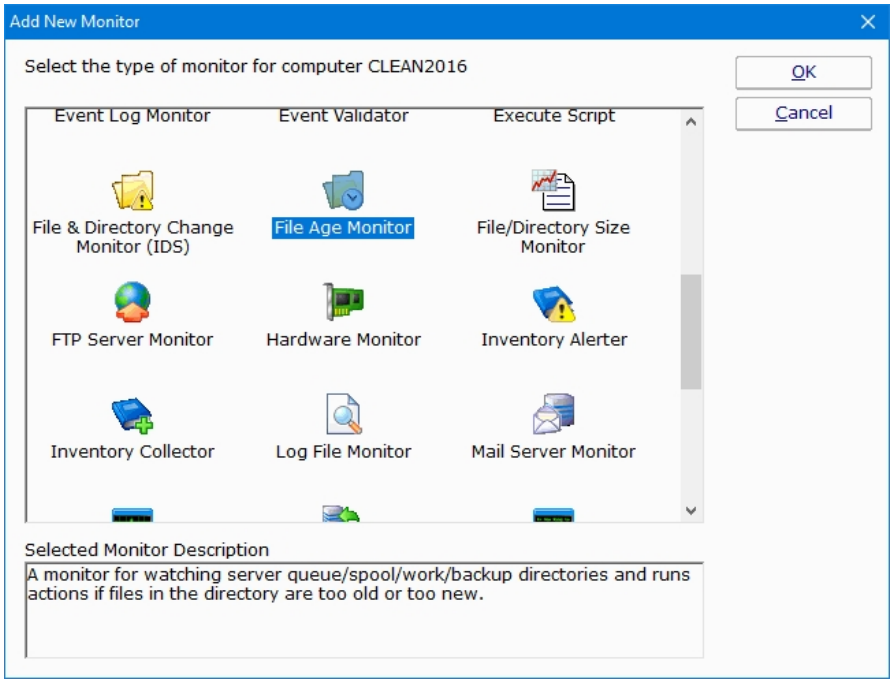


What this does is it overwrites the text file called "pa_watch_this_file.txt" every time the user logs in.

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.

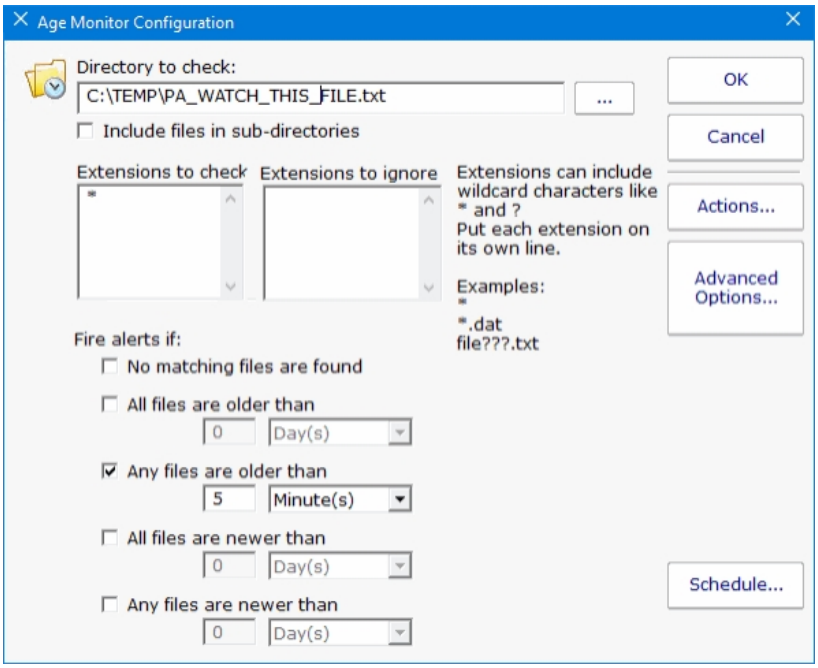
3. Monitor for a stale file.

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:



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).


Age Monitor Configuration
Directory to check:
C:\TEMP\PA_WATCH_THIS_FILE.txt
...
Include files in sub-directories
Extensions to check
*
Extensions to ignore
Extensions can include wildcard characters like * and ?
Put each extension on its own line.
Examples:
*
*.dat
file???.txt
Fire alerts if:
No matching files are found
All files are older than
0
Day(s)
Any files are older than
5
Minute(s)
All files are newer than
0
Day(s)
Any files are newer than
0
Day(s)
OK
Cancel
Actions...
Advanced Options...
Schedule...

Database Monitor

The Database Monitor is really two monitors - the Database Server Monitor, and one or more Database Monitors. Currently Microsoft's SQL Server is the only database supported.

Database Server Monitor

The Database Server Monitor is always created first, and it is used to create individual Database Monitors. After a valid connection string is entered, the list of databases on the database server are displayed.

For help coming up with the proper connection string, please see:

https://www.connectionstrings.com/sql-server/

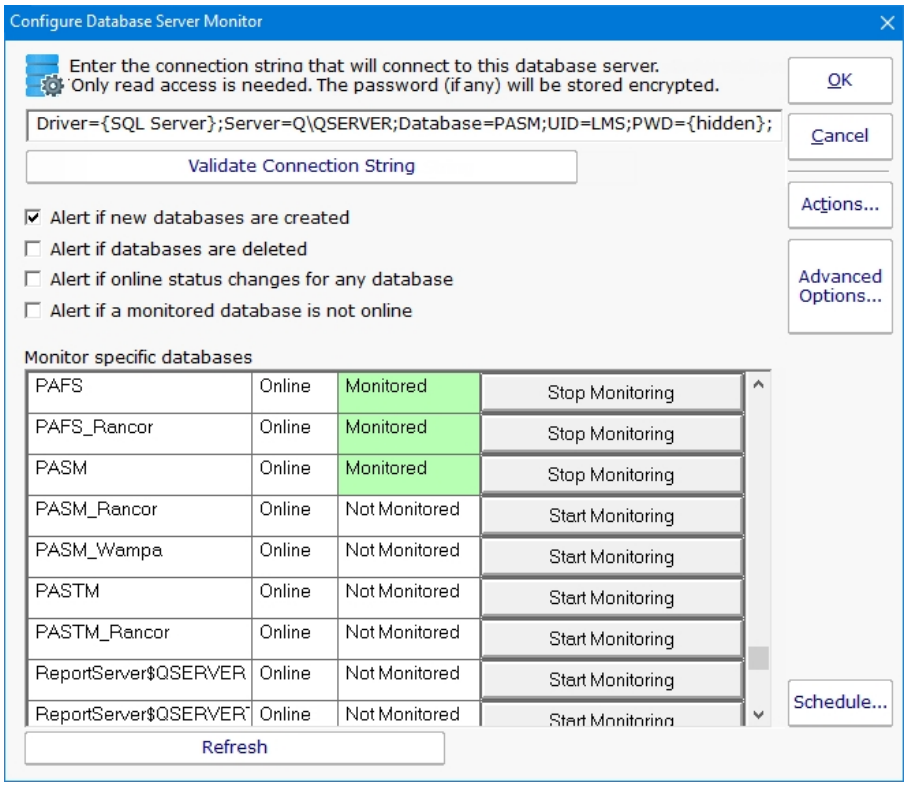
In this step, you do NOT need to specify a Database parameter yet. So one of the two connection strings below will probably work:

Using Trusted_Connection

```
Driver={SQL Server Native Client 10.0}; Server=<your_servername_here>;
Trusted_Connection=yes;
```

Using Username/Password

```
Driver={SQL Server Native Client 10.0}; Server=<your_servername_here>; UID=
<your_username>; PWD=<your_password>;
```



The check boxes on the monitor control what it will alert on, specifically it can alert when:

databases are created

databases are deleted

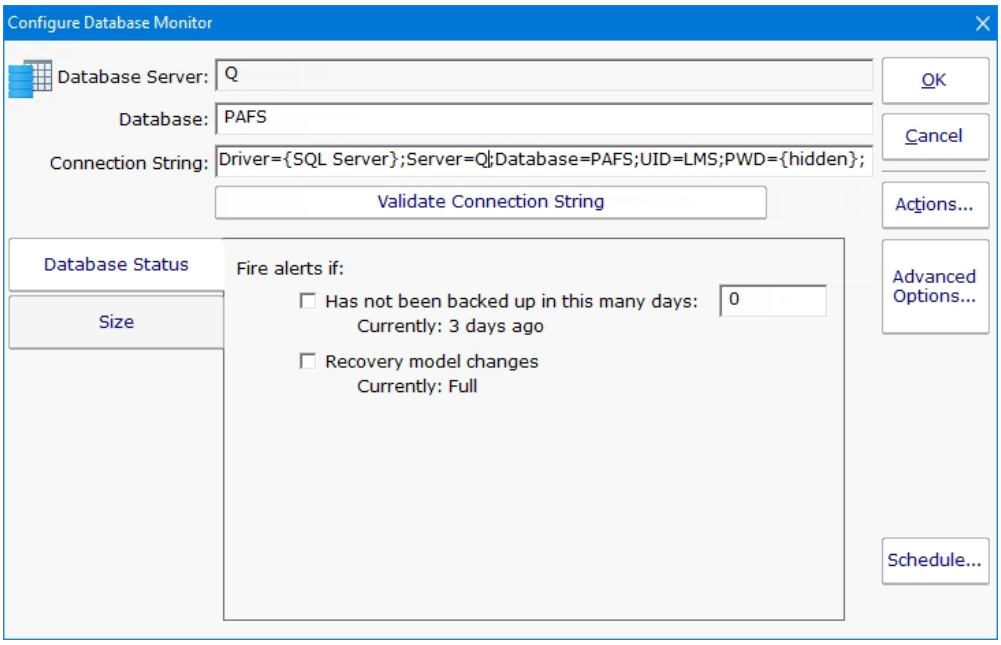
database online status changes

a monitored database goes offline

This monitor also shows which individual databases are being monitored, and lets you start or stop monitoring those databases via a Database Monitor.

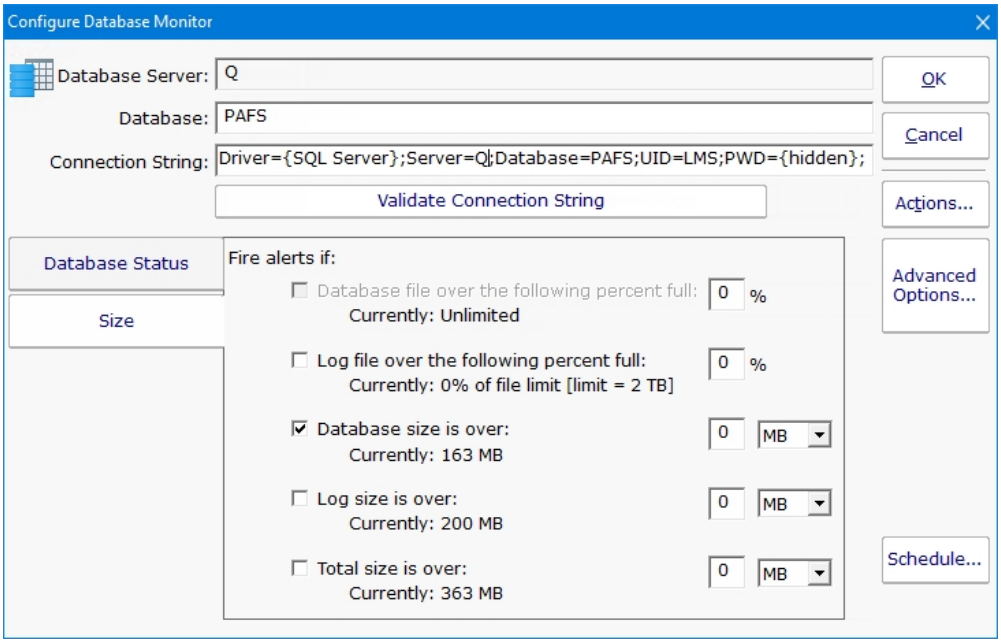
Database Monitor

When you start monitoring a new database, a Database Monitor is automatically created. After it is created, you can go straight to the Database Monitor to edit the configuration or even delete the monitor.



The connection string is automatically generated for you based on the connection string used in the Database Server Monitor above. You can edit it as needed.

The Database Monitor has two tabs that control what it will watch. It can watch and alert on the status which involves the database's backup and recovery model. To watch that the database itself is up, use the Database Server Monitor above.



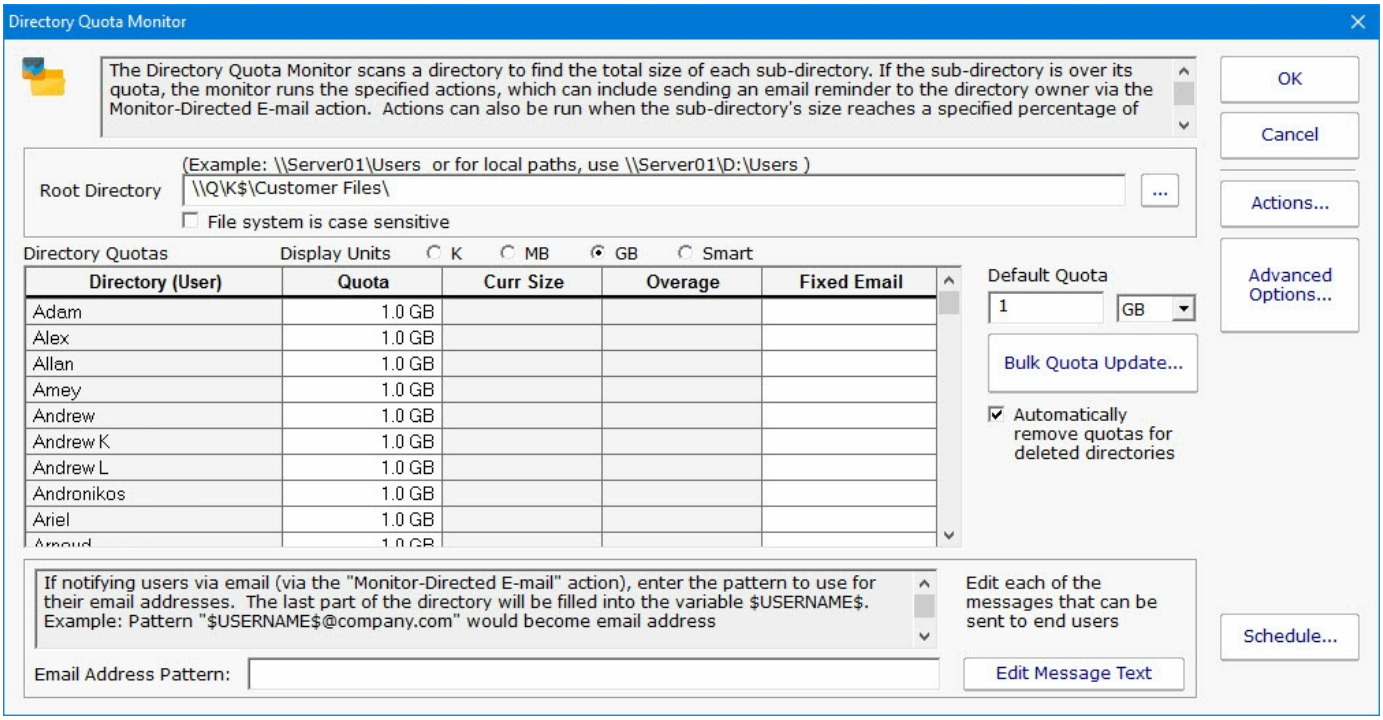
The other tab lets you monitor the size of the database and its transaction log.

Standard Configuration Options

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

Directory Quota Monitor

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



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

Set the default quota which will be used for any directory that doesn't have a quota already specified (including new directories discovered during a scan)

Manually enter quota values in the Quota column for any individual directory (specify units of K, MB or GB)

Use the Bulk Quota Update mechanism which makes it easy to set many directories to quotas in a flexible way.

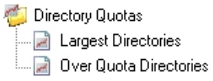
If you want end users (directory owners) to receive email quota reminders, be sure to add the Monitor Directed-Email action. The Directory Quota Monitor will need to determine an email address for each user to notify. You can either enter an email address for each directory in the Fixed Email column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

Note: If the specified directory is monitored by a Satellite, the true directory names will be retrieved from the Satellite during the configuration step.

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



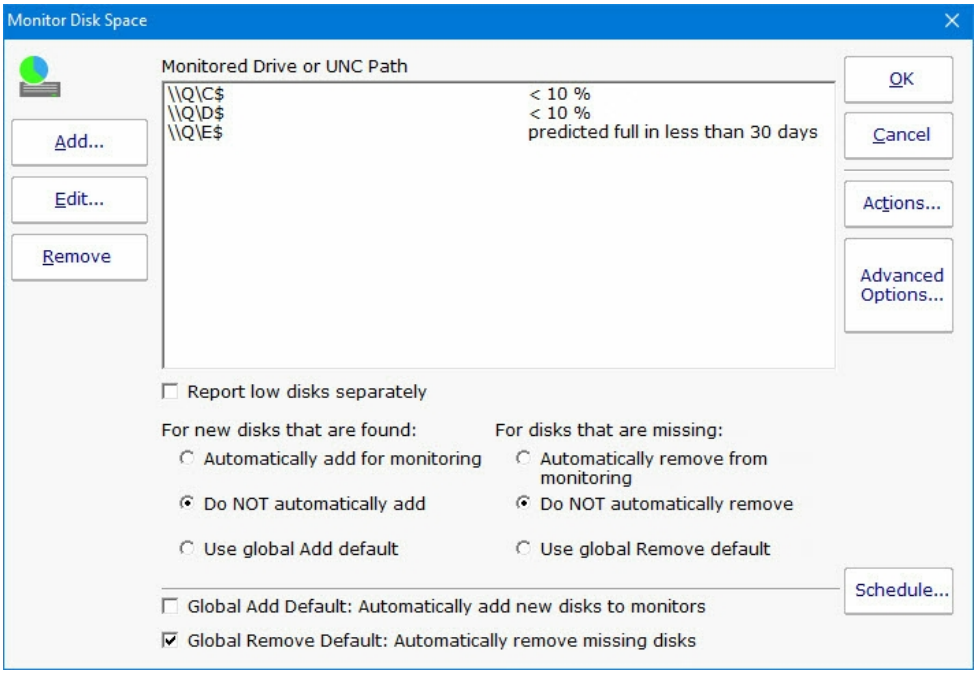
The monitor supports reports that detail which directories are over their quota, as well as the largest directories.

Disk Space Monitor

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

Watch the training video How to Monitor Disk Space.

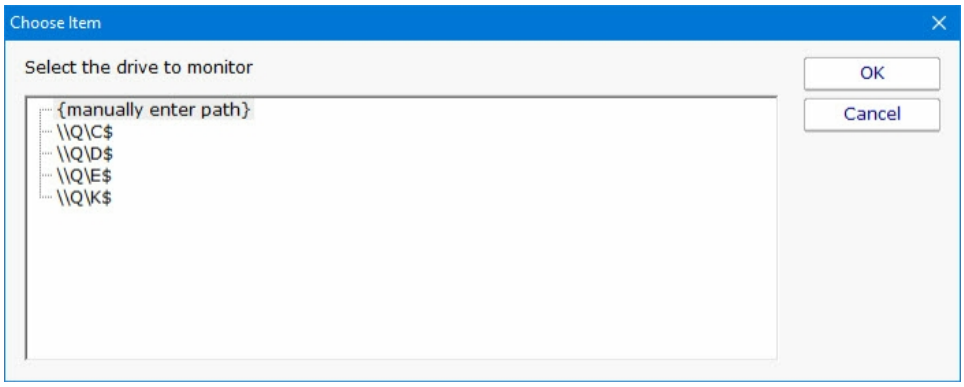
The Add, Edit and Remove buttons on the left will let you change the disks that are being monitored.



The radio buttons at the bottom of the dialog let you indicate what should happen if new unmonitored drives are detected during a scan. You can automatically add them, not add them, or do whatever the global (shared among all Disk Space monitors) default is. The default is shown and changed with the check box below the radio buttons.

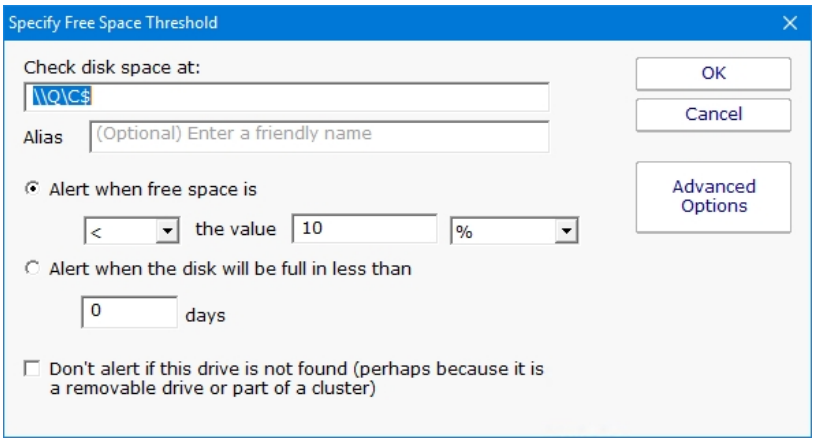
If a new drive is found and added to the monitor, the average threshold for existing disks will be used for the new disk.

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.

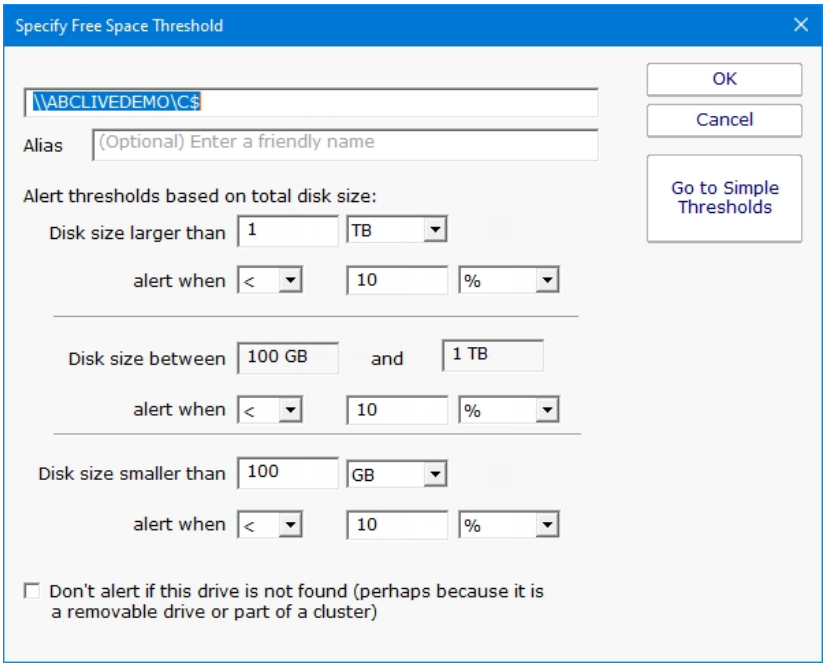


Note: If the target server is monitored by a Satellite, the drive names will be retrieved from the Satellite during the configuration step.

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.



The Advanced Options button will let you give separate thresholds based on disk size. This is helpful when creating Monitor Templates that can be applied to multiple servers.



Once the drive to monitor is selected, specify the free space threshold.

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 be able to access mapped drives. The best way to specify a disk in this case is via UNC paths.

Disk Full Predictions

Note that one of the alert threshold options is to be alerted when a disk is predicted to be X days away from being full. This uses historical disk readings and trend analysis to predict when the disk will be full. This is very helpful for capacity planning.

Standard Configuration Options

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

Supported Reports

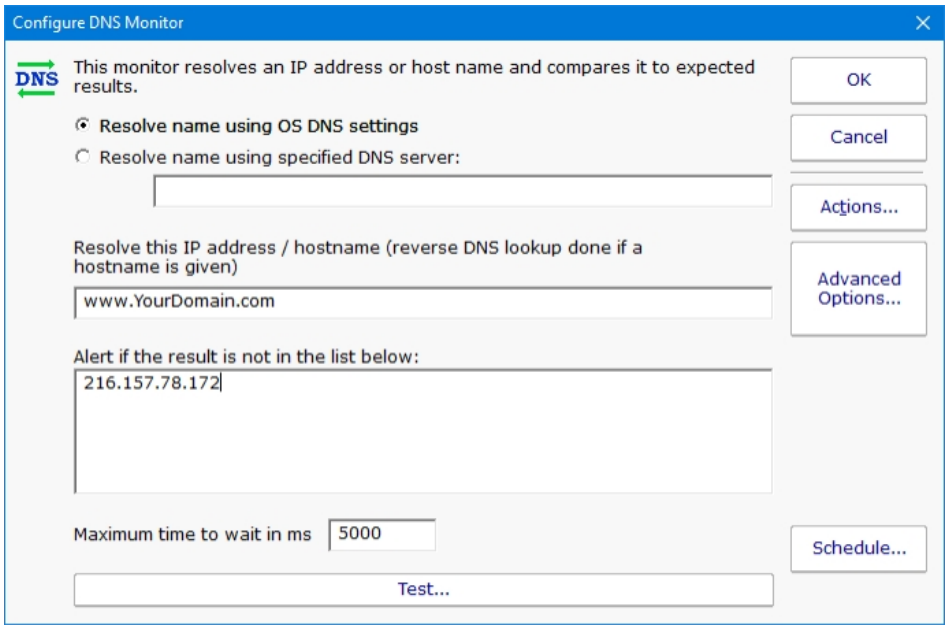
The Disk Space monitor supports a number of disk space related reports. The Disk Space Summary is a good way to keep an eye on all disk space -- by default it shows a list of all servers with those with the least amount of free space at the top. Most of the reports can create bar and line charts, as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

See how to predict when disks will fill up

DNS Monitor

The DNS monitor will resolve a hostname, or do a reverse DNS lookup on an IP address and return the hostname. The result is compared to a list and if the result is in the list, the lookup is considered successful. If the lookup returns something not in the list, or the lookup fails, the monitor fires actions.

You can specify the local computer's DNS server settings should be used, or you can indicate a specific DNS server to send the request to. If the specific DNS server can not be reached or returns an error, the monitor will fire actions.



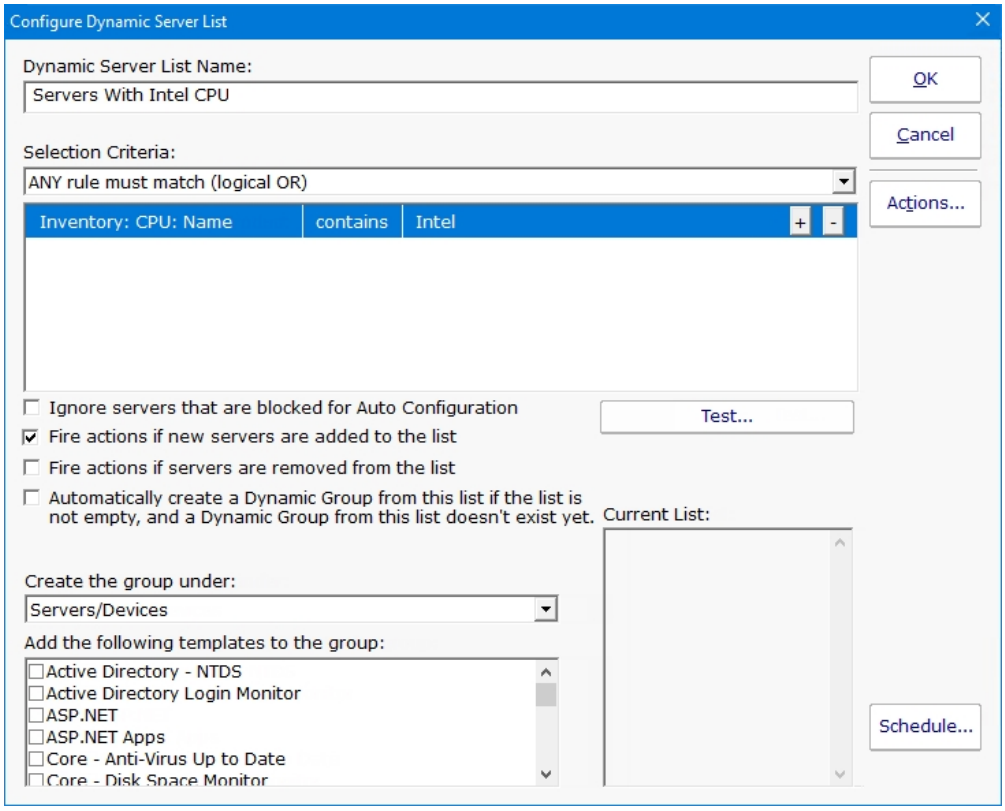
If you are resolving hostnames, and a CNAME record is returned (something like www.poweradmin.com -> poweradmin.com) the resulting hostname will be looked up so that the final result is an IP address. Though it's uncommon, chained CNAME records can be followed.

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.

Dynamic Server List

The Dynamic Server List monitor is a Global Monitor that runs outside of any server. It periodically checks servers to see which ones belong in a list determined by your criteria.



This monitor is very powerful and lets you select servers by:

Calculated status values (disk space, CPU usage, SNMP values, etc.)

Event Log entries

Group membership

Installed Windows services

Inventory values

Monitor types assigned

Monitored by Satellite

Name matching

Running processes

For example, you could define a list of:

Servers with average CPU usage over 10%

Servers with no anti-virus protection

Servers running IIS

You can receive alerts when servers enter and/or leave the list.

Rule Information

Each of the rules available gather information from different places and have specific behaviors, which will be documented below.

Blocked From Auto Configuration
: This is a setting that is applied to Servers/Devices when they are first created. It can be updated via the Bulk Config operation Computers: Set/Reset Block From Auto Configuration.

Contained in Group
: This rule will return all computer that are in the specified group, or within a sub-group of the specified group.

Contained Monitor Names
: This rule is a string search, that will check the names of monitors within a server/device, and if the name search matches, the server/device is added to the list.

Contains Monitor Type
: Checks the server for all monitors it contains and if any are of the specified monitor type, the server is added to the list.

Custom Property
: Custom Properties on the server/device are checked for a match. Note that Customer Properties are inherited from groups 'above' the server/device in the group hierarchy, so Custom Properties set directly on the server/device as well as inherited properties are checked.

Has Process
: Checks the database for a list of Processes on servers/devices that were monitored by a Process Monitor.

Has Windows Service
: Checks the database for any services that were monitored by a Service Monitor on the target server. Removing a Service Monitor from a server does not automatically remove the database entries for that server. This is a powerful way to make Dynamic Groups based on the software installed on a server.

Inventory
: This will check values collected and stored in the database by the Inventory Collection monitor. Things such as Anti-Virus product, IP Address, OS version, installed CPU and memory, etc can be queried. Note that not all inventory fields are found/collected for all devices.

Is Device Type
: This works on the property that can be set on servers/devices via Type & Credentials > Set Computer/Device Type in the Console. This can also be set by the Bulk Config operation Computers: Set Credentials (Windows, SNMP, ESX, IPMI).

Monitored By
: This allows you to create a list of devices that are monitored by the Central Monitoring Service, or by particular Satellites. This can be useful for creating lists of servers owned by a particular customer or in a specific geography if your other groups are arranged this way.

Monitoring Software is Installed
: This property is true for servers where the Central Monitoring Service or a Satellite Monitoring Service is installed and running.

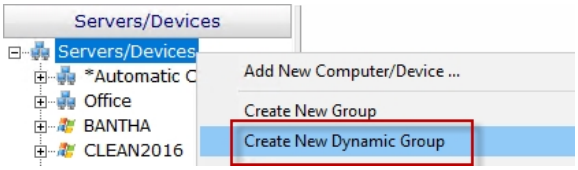
Registry
: This rule reads a particular registry value and compares it to the criteria you set. If the criteria match, the server is added to the list.

Server/Device Name
: The name (including any alias that is set) is compared to the given rule to determine servers/devices that match.

Statistic
: Statistics from most monitor types can be targeted with this rule. Once a specific statistic is chosen, values from that statistic are checked, and servers for which the statistic meets the checks are added to the list.

Dynamic Groups

Once you've defined a server list and how often it should update, you can use it further by defining a Dynamic Group.



The Dynamic Group is defined by choosing an existing Dynamic Server List. Any server/device that shows up in the Dynamic Server List will belong to the group.

Because the Dynamic Group is defined by the server list, servers/devices can not be manually added or removed from the group. Other than that, these groups behave similar to other groups. That means you can:

Define status reports for the group, showing specific information for your chosen servers

Use Dynamic Groups in Bulk Config as a selection criteria for servers to operate on (for example, a group with all Windows 2012 R2 servers)

Run Ad-Hoc or Scheduled Reports for the servers in the group

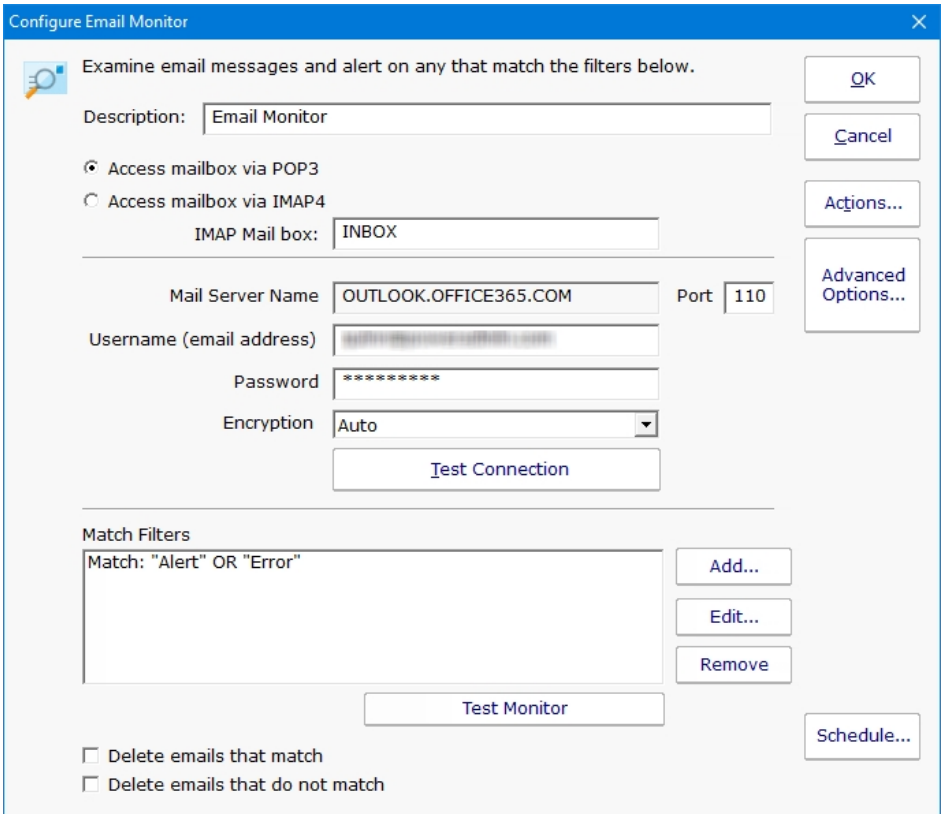
Grant access to servers in the group

Standard Configuration Options

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

Email Monitor

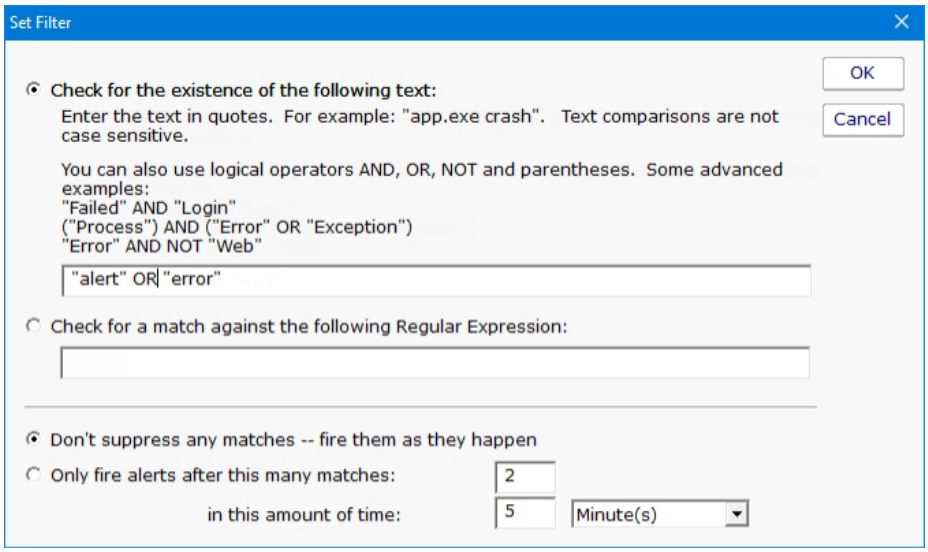
The Email Monitor can connect to a POP3 or IMAP4 mailbox and scan for messages that match criteria you choose. This could be used to monitor devices that can only send email alerts, or as part of an email loop monitor verify email sending is working.



Above you can see the configuration dialog for configuring the Email Monitor. The Mail Server Name is taken from the server that the monitor is attached to. Mail server type (POP3 or IMAP4), username, password, port and encryption settings can be set.

To be able to monitor Gmail accounts a security setting change is needed.
How To Enable Gmail Access

The most powerful part are the filters. Here you can specify what needs to match in order for the actions on monitor to fire. The matching text should be placed in quotes. You can use parentheses, and AND, OR and NOT logical operators. In addition, a regular expression can be used.



The filter is run against the email message body, and also the subject. If a filter matches either one, actions are fired.

At the bottom of the main configuration dialog are instructions about what should be done with messages after they are scanned. They can be deleted if they match, and/or deleted if they don't match.

We recommend using a special mailbox for this monitor, and then delete all messages whether they match or not to keep the mailbox size small, and to prevent messages from being scanned multiple times.

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.

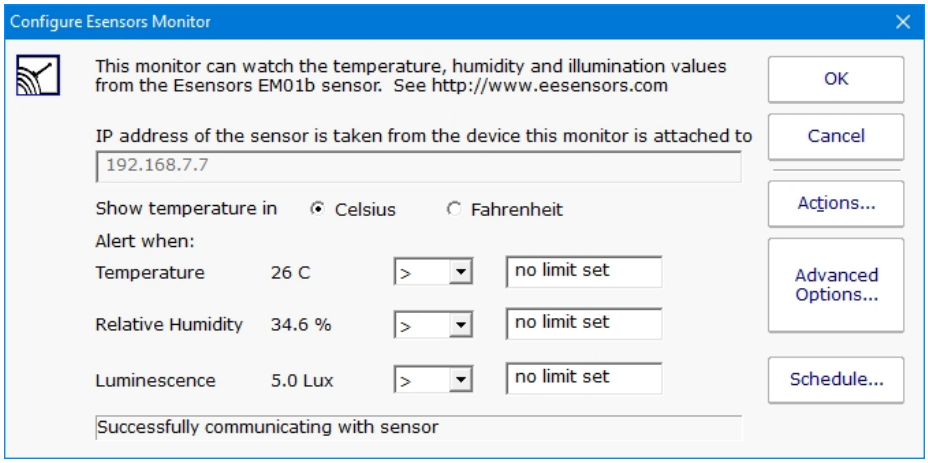
Esensor Environment Monitor

This monitor will check the temperature, humidity and light level readings from environmental sensors manufactured by Esensors, Inc. This monitor will work with the EM01B Websensor model.

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.



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

Note: If the target probe is monitored by a Satellite, the environmental values will be retrieved from the Satellite during the configuration step.

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)

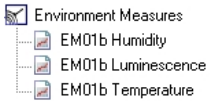
Luminescence (in Lux)

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 enter the Alert 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

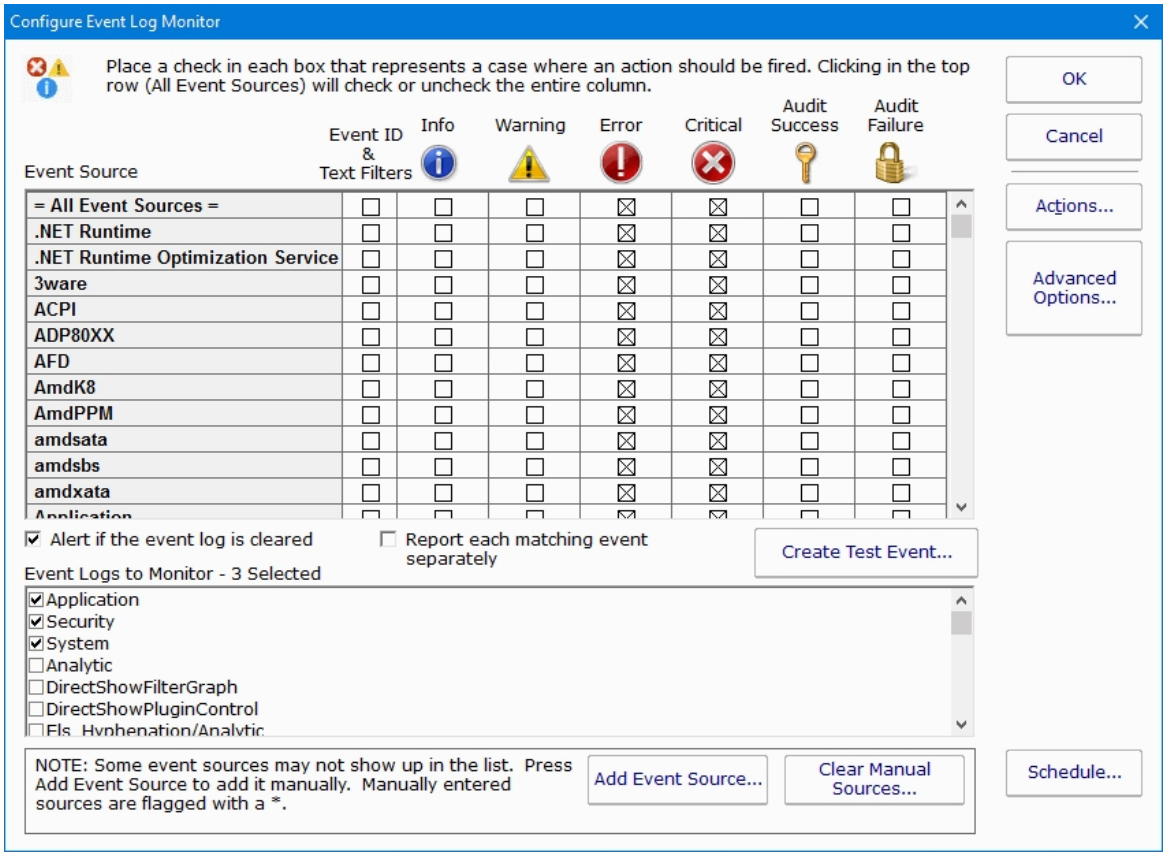


The monitored values of temperature, relative humidity and luminescence can all be charted or output to .CSV file or tabular HTML. The data can be summarized into hourly, daily, weekly or monthly minimum, maximum or average values.

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).

Watch the training video How to Monitor Event Logs for Errors.

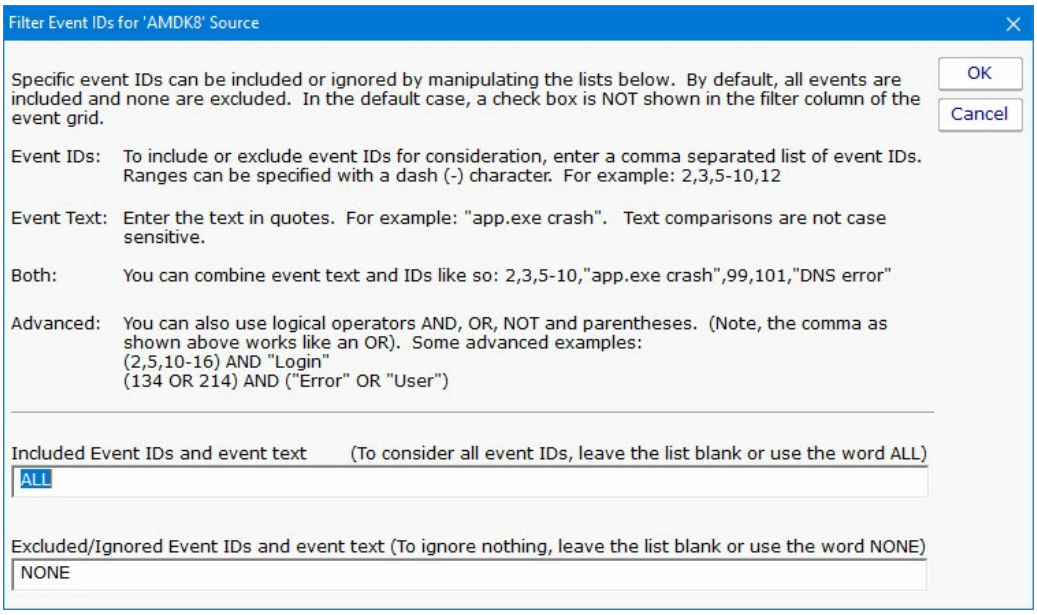


The large Event Source grid shows all currently registered Event Log sources. Next to each source are six columns: a special filter column, and the five different event types. Place a check next to the event source of the event type that you want to watch for.

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

Note: If the target server is monitored by a Satellite, the Event Log sources will be retrieved from the Satellite during the configuration step.

Additional Filtering



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.

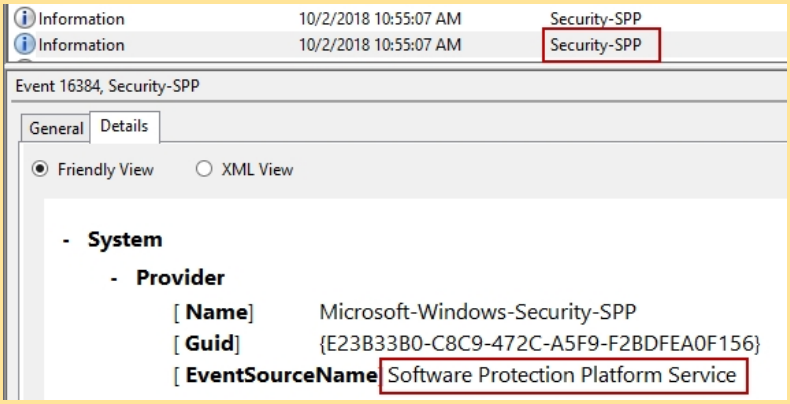
To learn how to audit for logons and logon failures using additional filtering read our HOWTO page Audit Logons

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.

Some Event Sources aren't what they appear to be. To see the true Event Source name, look at the Event's details. When adding a custom Event Source, you need to add the real name. After seeing what the real name is, you might find it is already in the list.



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.

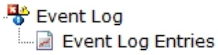
Customized Alerting

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



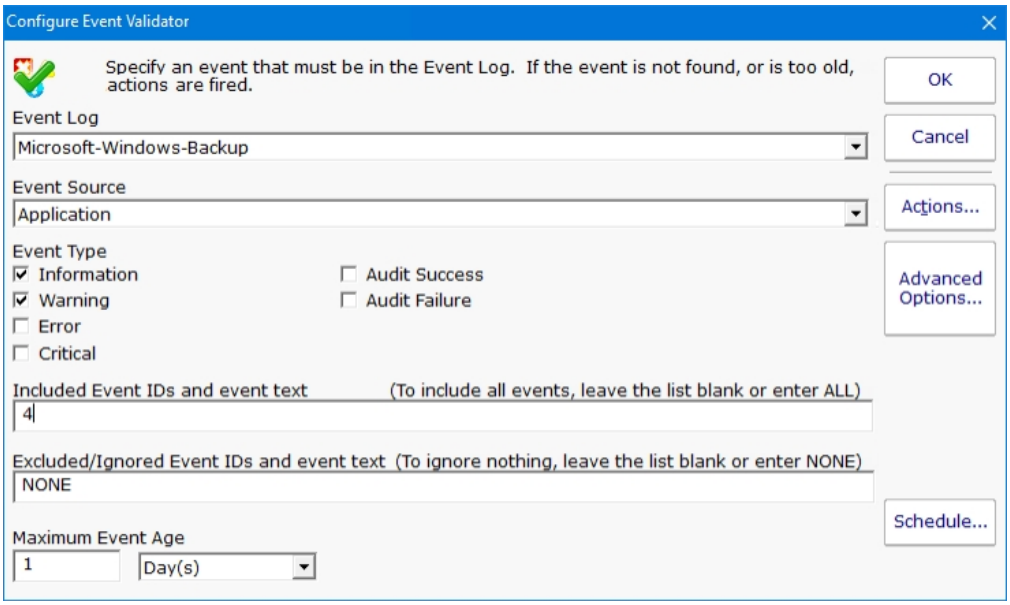
The Event Log monitor supports running reports on all of the matching events that have happened. You can filter the reported events on event source, type, date range, etc.

If you want to watch for a specific event, like a backup succeeded event, and be alerted if the event does NOT occur, create an Event Validator monitor.

Event Validator (for Backup Monitoring, etc)

The Event Log Monitor is great for watching for errors and alerting you when they happen. But in common cases like Backup monitoring, or monitoring anti-virus pattern file updates, you want to be notified if a specified event does NOT happen. That is what the Event Validator monitor is for.

The screenshot below is from a backup monitor. It is watching for a successful Windows Backup event.



In this example, the backup should happen once per day, so the monitor is checking to ensure there is an event with Event ID 4 from the Microsoft-Windows-Backup source. If the event is not found from within the past day, it would indicate the backup either failed, or didn't run at all. In this case, the monitor will fire alerts.

The monitor can run as often as you like. By default it checks once per day. That can be changed with the Schedule button in the lower right corner.

To learn how to audit for software backups read our HOWTO page Monitor Backup Success

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.

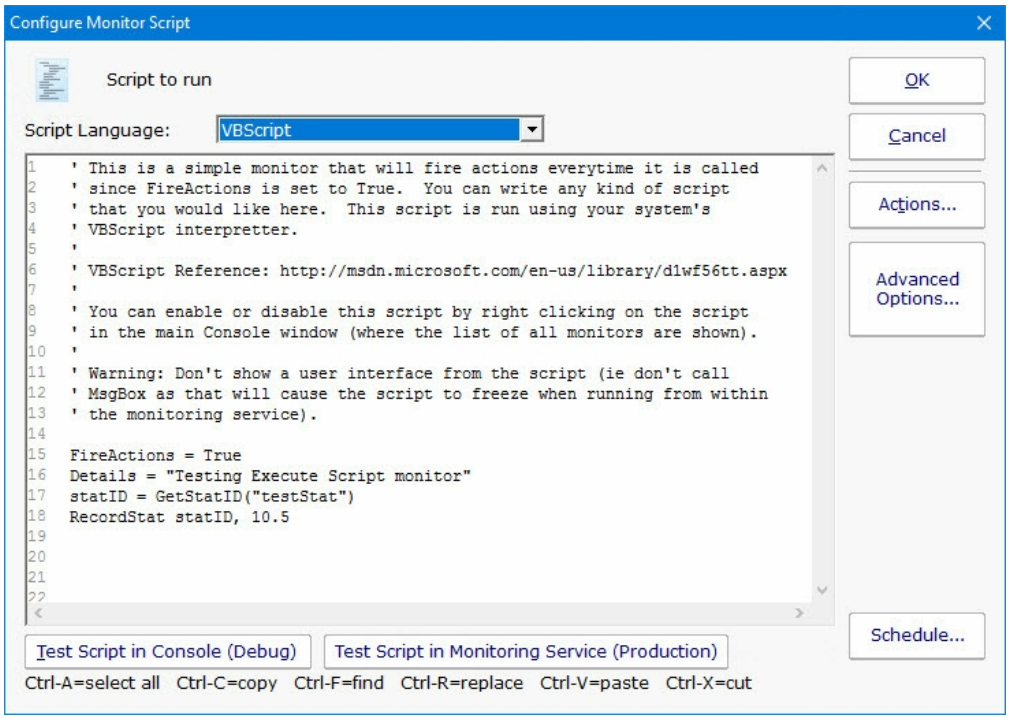
Supported Reports

The Event Validator monitor stores events in the same database as the Event Log monitor. That means the Event Log monitor's report is where you can find out about events that the Event Validator sees.

Execute Script Monitor

The Execute Script Monitor allows you to write your own custom scripts in the VBScript, JavaScript, PowerShell languages, or via an SSH connection to a host. You can check anything that your script can access. For VBScript, JavaScript and PowerShell, this monitor makes use of the applicable scripting engine that is already installed on nearly all Windows computers.

The script window is where you enter your script. The script can do anything that can be done in the selected language (including creating external components if available) with all the standard restrictions.



There are two Test buttons. One will run the script within the Console. The other will send the script to the monitoring service that is monitoring the target computer (Central Monitoring Service or a Satellite) and run the script there. This helps find any problems that might come up from the script possibly running on a different machine, or running as a different user (the service Log As user).

Keep in mind that when the script runs, it might run on a different computer than where you are editing it. That means drive mappings, HKEY_CURRENT_USER registry hive, Internet Explorer settings and the currently running user will often be different.

IMPORTANT: Do not show any user interface elements in the script -- they will not be visible in the monitoring service and will block the script from ever completing.

Topics

VBScript
- Documentation - Examples

Javascript
Documentation - Examples
PowerShell
Documentation - Examples
SSH
Documentation - Examples

Additional Script Elements

Besides the scripting language's own objects and elements, the following additional global variables and methods are available within each scripting environment:

VBScript

A good VBScript reference is available at: http://msdn.microsoft.com/en-us/library/d1wf56tt.aspx

ComputerName

This read-only string variable is the name of the computer that the monitor is attached to.

Example:

```
myStr = ComputerName
```

CustomProp

This function retrieves the named value of a custom property. It checks the Monitor first, and if not found, checks the monitor's owning computer, and then the computer's group, and then the group's parent group, etc. Custom properties can be set on Groups, Computers and Monitors by right-clicking on the item and choosing the Custom Properties menu.

Example:

```
myStr = CustomProp("NotifyGroupID")
```

Details

This is a string value. This value is passed to any attached actions as the details for the action (ie the content of an email notification for example).

Example:

```
Details = "Alert! Can't contact remote system"
```

FireActions

This is a boolean value. If the value is set to True, actions attached to the monitor will fire. If it is False, they will not fire. The value defaults to False.

Example:

```
FireActions = true
```

GetStatID

RecordStat

GetStatID and RecordStat are used together to record numeric data values to the database for reports.

GetStatID is a function that takes a single string value and returns an integer statID. The string value should be a useful name to you, such as the name of the thing you're probing with the script. Including the server/device name in the string would be a good idea if a similar script will run on multiple computers -- it will make it easier to choose the specific data that you want when you create reports.

Example:

```
statID = GetStatID("ftpSvr1-myObject")
```

RecordStat is a method that takes two inputs -- the statID obtained from GetStatID above, and the numeric value to record to the database. The time the value is recorded also gets saved to the database for use in line charts, etc.

Example:

```
RecordStat statID, objectValue
```

GetValue
StoreValue

GetValue method takes a text name and returns the value that was stored earlier via the StoreValue call described below. If nothing was ever stored with that name, an empty string is returned.

Example:

```
prevState = GetValue("LastState")
```

The StoreValue method takes a text name, and a text value and stores it. This named value can be retrieved later (even when the script runs next) via GetValue. Note that these values will be persisted in the configuration database and kept in memory with the monitor, so they should be kept relatively small (a few hundred characters long or less).

Example:

```
StoreValue "LastState", "1|15|OK"
```

InventoryValue

Request an inventory value for the current computer, or a different one. An inventory propertyID must be used to specify which inventory value to retrieve. An optional ComputerID value can be used to get the inventory value from a computer other than the current computer. If a property can have multiple values (CPU Names for example), each one will have a newline character appended.

Example:

```
'returns the Operating System (18) for the current computer myStr = InventoryValue(18)
'returns the Operating System (18) for the current computer (0 means use default) myStr =
InventoryValue(18, 0)
'returns the Operating System (18) for computerID 238 myStr = InventoryValue(18, 238)
```

The inventoryID values are given below. Note that not all computers/devices will have all inventory values, and some may have none (especially if an Inventory Collector monitor is not added to the computer).

Anti-virus Version	38
Anti-virus Pattern File	39
Anti-virus Pattern File Date	40
Anti-virus Status	41
Operating System	18
OS Architecture	19
OS Version	20
OS Last Boot Time (_time_t UTC value)	21
OS Current Time (_time_t UTC value)	22
CPU Count	13
CPU Name (multi value)	15
CPU Number of Cores (multi value)	16
CPU Clock Speed (multi value)	17
Display Name	6
Drive Status (multi value)	23
Domain	9
Manufacturer	10
Page File size in MB	24
RAM in MB	14
System Architecture	12
System Model	11
Time Zone Offset	8
Uptime % this month	28
Uptime % last month	29

MachineID

Returns the numeric value that uniquely identifies this computer (Computer ID - CID) within the application. Useful in conjunction with the External API.

Example:

```
myID = MachineID
```

GroupPath

The name of the group that the computer the monitor is attached to belongs in, with child groups delimited with a > (ie, Servers/Devices > Austin > Lab)

Example:

```
myStr = GroupPath
```

ReportResults

This method will take the current value of FireActions and Details and report the result as though the monitor had finished. This is a way for a monitor to report multiple individual errors, similarly to how some other monitors have a "report each event separately" check box.

Example:

```
ReportResults
```

SendMail

This method sends an email message to the recipient that you choose. This method can also send the email in HTML format if it sees the <!DOCTYPE in the body of the message.

Example:

```
SendMail "to_address@host.com", "from_address@host.com", "Subject of message", "Body of email message"
```

SetComputerCustomPropByID

Custom Properties can be used in directory paths, email messages, scripts and other places. Your script can set a Custom Property on a computer by giving it's ID (first parameter). If the ID is 0, the computer the monitor is running on will be targeted.

Example:

```
SetComputerCustomPropByID 0, "DEVICEID", "BSQL"
```

The Custom Property DISPLAYED_NOTES is the value you can set by right-clicking a computer and selecting Notes. Notes show up at the top of a Server Status Report.

Sleep

This VBScript method takes a single integer value, which is the number of milliseconds that the script should stop and sleep. Be careful about using this: causing too many monitors to sleep for very long means other monitors may not get run.

Example:

```
Sleep 1500
```

ToLog

This method takes a string value and appends it to the service's log file (useful for debugging scripts). The line will start with MONITOR_SCRIPT_LOG.

Example:

```
ToLog "Arrived at first loop"
```

ToLog resultVal

JavaScript

ComputerName

This read-only string variable is the name of the computer that the monitor is attached to.

Example:

```
myStr = ComputerName;
```

CustomProp

This function retrieves the named value of a custom property. It checks the Monitor first, and if not found, checks the monitor's owning computer, and then the computer's group, and then the group's parent group, etc. Custom properties can be set on Groups, Computers and Monitors by right-clicking on the item and choosing the Custom Properties menu.

Example:

```
myStr = CustomProp("NotifyGroupID");
```

Details

This is a string value. This value is passed to any attached actions as the details for the action (ie the content of an email notification for example).

Example:

```
Details = "Alert! Can't contact remote system";
```

FireActions

This is a boolean value. If the value is set to True, actions attached to the monitor will fire. If it is False, they will not fire. The value defaults to False.

Example:

```
FireActions = true;
```

GetStatID
RecordStat

GetStatID and RecordStat are used together to record numeric data values to the database for reports.

GetStatID is a function that takes a single string value and returns an integer statID. The string value should be a useful name to you, such as the name of the thing you're probing with the script. Including the server/device name in the string would be a good idea if a similar script will run on multiple computers -- it will make it easier to choose the specific data that you want when you create reports.

Example:

```
statID = GetStatID("ftpSvr1-myObject");
```

RecordStat is a method that takes two inputs -- the statID obtained from GetStatID above, and the numeric value to record to the database. The time the value is recorded also gets saved to the database for use in line charts, etc.

Example:

```
RecordStat(statID, objectValue);
```

GetValue
StoreValue

GetValue method takes a text name and returns the value that was stored earlier via the StoreValue call described below. If nothing was ever stored with that name, an empty string is returned.

Example:

```
prevState = GetValue("LastState");
```

The StoreValue method takes a text name, and a text value and stores it. This named value can be retrieved later (even when the script runs next) via GetValue. Note that these values will be persisted in the configuration database and kept in memory with the monitor, so they should be kept relatively small (a few hundred characters long or less).

Example:

```
StoreValue("LastState", "1|15|OK");
```

InventoryValue

Request an inventory value for the current computer, or a different one. An inventory propertyID must be used to specify which inventory value to retrieve. An optional ComputerID value can be used to get the inventory value from a computer other than the current computer. If a property can have multiple values (CPU Names for example), each one will have a newline character appended.

Example:

```
//returns the Operating System (18) for the current computer myStr = InventoryValue(18);
//returns the Operating System (18) for the current computer (0 means use default) myStr =
InventoryValue(18, 0);
//returns the Operating System (18) for computerID 238 myStr = InventoryValue(18, 238);
```

The inventoryID values are given below. Note that not all computers/devices will have all inventory values, and some may have none (especially if an Inventory Collector monitor is not added to the computer).

Anti-virus Version	38
Anti-virus Pattern File	39
Anti-virus Pattern File Date	40
Anti-virus Status	41
Operating System	18
OS Architecture	19
OS Version	20
OS Last Boot Time (_time_t UTC value)	21
OS Current Time (_time_t UTC value)	22
CPU Count	13
CPU Name (multi value)	15
CPU Number of Cores (multi value)	16
CPU Clock Speed (multi value)	17
Display Name	6
Drive Status (multi value)	23
Domain	9
Manufacturer	10
Page File size in MB	24

RAM in MB	14
System Architecture	12
System Model	11
Time Zone Offset	8
Uptime % this month	28
Uptime % last month	29

MachineID

Returns the numeric value that uniquely identifies this computer (Computer ID - CID) within the application. Useful in conjunction with the External API.

Example:

```
myID = MachineID;
```

GroupPath

The name of the group that the computer the monitor is attached to belongs in, with child groups delimited with a > (ie, Servers/Devices > Austin > Lab)

Example:

```
myStr = GroupPath
```

ReportResults

This method will take the current value of FireActions and Details and report the result as though the monitor had finished. This is a way for a monitor to report multiple individual errors, similarly to how some other monitors have a "report each event separately" check box.

Example:

```
ReportResults();
```

SendMail

This method sends an email message to the recipient that you choose. This method can also send the email in HTML format if it sees the <!DOCTYPE in the body of the message.

Example:

```
SendMail("to_address@host.com", "from_address@host.com", "Subject of message", "Body of email
message");
```

SetComputerCustomPropByID

Custom Properties can be used in directory paths, email messages, scripts and other places. Your script can set a Custom Property on the computer whose ID is given (first parameter), or use 0 to indicate the computer the monitor is running on should be targeted.

Example:

```
SetComputerCustomPropByID(0, "DEVICEID", "BSQL");
```

The Custom Property DISPLAYED_NOTES is the value you can set by right-clicking a computer and selecting Notes. Notes show up at the top of a Server Status Report.

Sleep

This method takes a single integer value, which is the number of milliseconds that the script should stop and sleep. Be careful about using this: causing too many monitors to sleep for very long means other monitors may not get run.

Example:

```
Sleep(1500);
```

ToLog

This method takes a string value and appends it to the service's log file (useful for debugging scripts). The line will start with MONITOR_SCRIPT_LOG.

Example:

```
ToLog "Arrived at first loop"
```

ToLog resultVal

PowerShell

PowerShell interaction happens via the $mon object.

$mon.ChangeMonitorStatus

SetMonitorStatus is a function that sets the status of any monitor. This function takes three values: Monitor ID, Monitor Status, and Status Text. The Monitor ID is assigned in the monitoring service and you can find the ID value by showing the IDs from the View menu and then looking in the navigation colunm. If you use 0 for the Monitor ID the function will change the staus of the monitor the action is attached to. There are four statuses that are available: msOK, msAlert, msError, and msDISABLED. The Status Text is the message that you can supply that is listed for the monitor and will be shown in reports.

Example:

```
$mon.ChangeMonitorStatus(43, $mon.msAlert, "Status changed for monitor")
```

Possible values:

Monitor Status	Values
OK	$mon.msOK
Alert	$mon.msAlert
Alert Show as Green	$mon.msALERT_GREEN
Alert Show as Red	$mon.msALERT_RED
Error	$mon.msError
Disabled	$mon.msDISABLED

$mon.ComputerName

This read-only string variable is the name of the computer that the monitor is attached to.

Example:

```
$myStr = $mon.ComputerName
```

$mon.CustomProp

This function retrieves the named value of a custom property. It checks the Monitor first, and if not found, checks the monitor's owning computer, and then the computer's group, and then the group's parent group, etc. Custom properties can be set on Groups, Computers and Monitors by right-clicking on the item and choosing the Custom Properties menu.

Example:

```
$myStr = $mon.CustomProp("NotifyGroupID")
```

$mon.Details

This is a string value. This value is passed to any attached actions as the details for the action (ie the content of an email notification for example).

Example:

```
$mon.Details = "Alert! Can't contact remote system"
```

$mon.FireActions

This is a boolean value. If the value is set to True, actions attached to the monitor will fire. If it is False, they will not fire. The value defaults to False.

Example:

```
$mon.FireActions = $true
```

$mon.GetCredentials

The GetCredentials function lets your script request credentials for use within the script. The relevent setting must be enabled (disabled by default) in the Security Protected Settings. This function takes two parameters: A server name/key value, and a credential type.

Credential types can be one of: ctWIN, ctESX, ctSSH, ctAWS, ctCUSTOM

Example:

```
$user = ""
$info = ""
$pass = ""
if ($mon.GetCredentials("TEST-ENV-DB", [PALowPriorityHelper_Net4.CredType]::ctCUSTOM, [ref]$user,
[ref]$info, [ref]$pass))
{
   #use credentials
}
else
{
   #failed to get credentials
```

```
}
```

Because of the concern of scripts exfiltrating credentials, we recommend locking monitors or actions that use the GetCredentials function.

$mon.GetMonitorList

GetMonitorList is a function that uses the Server ID to return a list of monitors assigned to the server and the monitor's attributes. The server ID can be for any server and if no server is given the default will be the current server that this monitor is assigned to. The returned value is a Hashtable that can be iterated through to find the value needed.

Example:

```
$myTable = $mon.GetMonitorList(1)
```

The monitor's attributes values:

Status	status
Error Text	errText
Dependency	depends_on
Title	title
Error Action IDs	errActionIDs
Scheduled Next Run Time	nextRun
Time in Error (seconds)	inErrSeconds
Fixed Action ID	fixedActionIDs
Last Run Time	lastRun

$mon.GetServerList

GetServerList is a function that returns a list of servers assigned to a group and the server's attributes. Two parameter are needed for this function; GroupID and include Child Groups. If no GroupID is used the default 0 is used, which is the entire list of servers at the root level. The second parameter is a switch used to return or not return servers that are in child groups under the starting group. Use to 0 to return all servers and 1 to return servers at the parent level only. The returned value is a Hashtable that can be iterated through to find the value needed.

Example:

```
$myTable = $mon.GetServerList(2, 1)
```

The server's attributes values:

Server Name	name
Group Level	group
Group ID	groupID
Status	status
Alias for Server	alias

$mon.GetStatID

$mon.RecordStat

GetStatID and RecordStat are used together to record numeric data values to the database for reports.

GetStatID is a function that takes a single string value and returns an integer statID. The string value should be a useful name to you, such as the name of the thing you're probing with the script. Including the server/device name in the string would be a good idea if a similar script will run on multiple computers -- it will make it easier to choose the specific data that you want when you create reports.

Example:

```
$statID = $mon.GetStatID("ftpSvr1-myObject")
```

RecordStat is a method that takes two inputs -- the statID obtained from GetStatID above, and the numeric value to record to the database. The time the value is recorded also gets saved to the database for use in line charts, etc.

Example:

```
$mon.RecordStat($statID, $objectValue)
```

$mon.GetValue
$mon.StoreValue

The GetValue method takes a text name and returns the value that was stored earlier via the StoreValue call described below. If nothing was ever stored with that name, an empty string is returned.

Example:

```
$prevState = $mon.GetValue("LastState")
```

The StoreValue method takes a text name, and a text value and stores it. This named value can be retrieved later (even when the script runs next) via GetValue. Note that these values will be persisted in the configuration database and kept in memory with the monitor, so they should be kept relatively small (a few hundred characters long or less).

Example:

```
$mon.StoreValue("LastState", "1|15|OK")
```

$mon.GroupPath

The name of the group that the computer the monitor is attached to belongs in, with child groups delimited with a > (ie, Servers/Devices > Austin > Lab)

Example:

```
myStr = $mon.GroupPath
```

$mon.InventoryValue

Request an inventory value for the current computer, or a different one. An inventory propertyID must be used to specify which inventory value to retrieve. An optional ComputerID value can be used to get the inventory value from a computer other than the current computer. If a property can have multiple values (CPU Names for example), each one will have a newline character appended.

Example:

```
//returns the Operating System (18) for the current computer myStr = $mon.InventoryValue(18);
//returns the Operating System (18) for the current computer (0 means use default) myStr =
$mon.InventoryValue(18, 0);
//returns the Operating System (18) for computerID 238 myStr = $mon.InventoryValue(18, 238);
```

The inventoryID values are given below. Note that not all computers/devices will have all inventory values, and some may have none (especially if an Inventory Collector monitor is not added to the computer).

Anti-virus Version	38
Anti-virus Pattern File	39
Anti-virus Pattern File Date	40
Anti-virus Status	41
Operating System	18
OS Architecture	19
OS Version	20
OS Last Boot Time (_time_t UTC value)	21
OS Current Time (_time_t UTC value)	22
CPU Count	13
CPU Name (multi value)	15
CPU Number of Cores (multi value)	16
CPU Clock Speed (multi value)	17
Display Name	6
Drive Status (multi value)	23
Domain	9
Manufacturer	10
Page File size in MB	24
RAM in MB	14
System Architecture	12
System Model	11
Time Zone Offset	8
Uptime % this month	28
Uptime % last month	29

$mon.MachineID

Returns the numeric value that uniquely identifies this computer (Computer ID - CID) within the application. Useful in conjunction with the External API.

Example:

```
$myID = $mon.MachineID
```

$mon.ReportResults

This method will take the current value of FireActions and Details and report the result as though the monitor had finished. This is a way for a monitor to report multiple individual errors, similarly to how some other monitors have a "report each event separately" check box.

Example:

```
$mon.ReportResults()
```

$mon.SendMail

This method sends an email message to the recipient that you choose.

Example:

```
$mon.SendMail("to_address@host.com", "from_address@host.com", "Subject of message", "Body of email
```

```
message")
```

$mon.SetComputerCustomPropByID

Custom Properties exist on groups, computers and monitors. This function lets you set the custom property on a computer. You can specify the computer ID in the first parameter, or set it to 0 to indicate the computer the monitor is running on should be targeted.

Example:

```
$mon.SetComputerCustomPropByID(0, "DEVICEID", "BSQL")
```

The Custom Property DISPLAYED_NOTES is the value you can set by right-clicking a computer and selecting Notes. Notes show up at the top of a Server Status Report.

$mon.SetMonitorStatus

SetMonitorStatus is a function that sets the status of the Excute Script monitor if FireActions is set to true (this function is ignored if FireActions is false). There are three statuses that are available: msOK, msAlert, and msError. The default is msAlert.

Example:

```
$mon.SetMonitorStatus($mon.msAlert)
```

Possible values:

Monitor Status	Value
OK	$mon.msOK
Alert	$mon.msAlert
Error	$mon.msError

$mon.TargetUsername
$mon.TargetDomain
$mon.TargetPassword

These values return username, domain and password for the target server if BOTH of the below conditions are met:

- Per-server credentials have been added for the server
- The EnableScriptCredentialAccess value at HKEY_LOCAL_MACHINE\software\PAServerMonitor\Protected must be set to 1

Example:

```
MyLoginFunc($mon.TargetDomain, $mon.TargetUsername, $mon.TargetPassword)
```

$mon.ToLog

This method takes a string value and appends it to the service's log file (useful for debugging scripts). The line will start with MONITOR_SCRIPT_LOG.

Example:

```
$mon.ToLog "Arrived at first loop"
$mon.ToLog $resultVal
```

Start-Sleep

The PowerShell cmdlet takes two parameters. The first parameter specifies timer in seconds (-s) or milliseconds (-m) and the second is an integer that specifies period of time.

Example:

```
Start-Sleep -s 10
```

SSH

SSH is a little different than the others. In this case, your script will be sent to the remote computer/device to run. The resulting terminal output is scanned for the special keywords below, and they will be 'executed' in the monitoring service when the script finishes. The keywords must start in the very first column to be recognized. One way to achieve this is to output the line with a new line character right before the keyword, as in this example below:

```
\nPA_Details("There is a problem")
```

PA_ChangeMonitorStatus(monitorID, status, description)

This is function that lets you pass the monitor ID, a status value, and a test description to set as the new status for the monitor given by the id. The monitor IDs can be obtains in the Console by setting View > Show Object IDs, or from the GET_MONITOR_INFO External API command.

Possible values for status:

Monitor Status	Values
OK	1
Alert	2
Alert Show as Green	17
Alert Show as Red	18
Error	3
Disabled	6

Example:

```
PA_ChangeMonitorStatus(12, 2, "Alert! Can't contact remote system")
```

PA_Details(string)

This is a string value. This value is passed to any attached actions as the details for the action (ie the content of an email notification for example). This particular value can span multiple lines. The value is terminated when a ") is seen.

Example:

```
PA_Details("Alert! Can't contact remote system")
```

PA_FireActions(boolean)

This is a boolean value. If the value is set to true, actions attached to the monitor will fire. If it is false, they will not fire. The value defaults to false.

Example:

```
PA_FireActions(true)
```

PA_RecordStat(stat_name, value)

This 'function' will record a statistic returned from the script to the database. It is equivalent to GetStatID and RecordStat in the other languages above.

The first parameter is a string value. The string value should be a useful name to you, such as the name of the thing you're probing with the script. The second value is a numeric value that will be stored.

Example:

```
PA_RecordStat("Scans_Per_Second", 45.6)
```

PA_SendMail(to, from, subject, body)

This method sends an email message to the recipient that you choose.

Example:

```
PA_SendMail("to_address@host.com", "from_address@host.com", "Subject of message", "Body of email
message")
```

The SSH script can also use replacement variables that are replaced before the script is sent to the host. These include the following:

$CustomProp(propName)$

$CustomProp(*propertyName*)$ will be replaced with the value of propertyName which came from from the source monitor, source computer or a parent group. It will be blank if the property is not defined.

$Date$

Date in a human-readable format

$Group$

Name of the group that the owning monitor is in (i.e. could be a value like "Routers").

$GroupPath$

Full path name of the group that the owning monitor is in (i.e. could be a value like "Servers/Devices > Boston > Routers")

$Machine$

Name of the target server

$MachineAlias$

Alias of the target server if one has been set. There will be no value (meaning an empty string) if no alias has been set.

$MachineID$

Internal ID representing the target server. These IDs can be obtained using the External API.

$MachineIP$

IP address of the target server

$MonitorType$

Textual name of the monitor type (i.e. "Event Log Monitor")

NL

Value that gets turned into a carriage return-newline pair.

$Time$

Human readable time on the monitoring server.

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.

VBScript Examples

Check a database value

Check files in a directory

Check the size of a specific file and record to a database

Check if the newest file is older than 6 hours old

Launch a program and check the result code

Check for text in a file

Check a database value

```
Option Explicit
Dim objconnection
Dim objrecordset
Dim strDetails
Dim valToCheck

Const adOpenStatic = 3
Const adLockOptimistic = 3

FireActions = False

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

objconnection.Open _
 "Provider=SQLOLEDB;Data Source=<data_base_server>;" & _
 "Initial Catalog=<database_name>;" & _
 "User ID=<username>;Password=<password>;"

'ensure there are at least 1000 rows
objrecordset.Open "SELECT COUNT(*) FROM <database_name>", _
 objconnection, adOpenStatic, adLockOptimistic

If objrecordset.RecordCount <> 0 Then
   objrecordset.MoveFirst
   valToCheck = objrecordset.Fields(0)

   If valToCheck < 1000 Then
      strDetails = "There are only " & valToCheck & " rows in the table!"
      FireActions = True
   End If
Else
   strDetails = "CODE RED !!!! Failed to get result!"
   FireActions = True
End If

Details = strDetails
```

Check 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
   FireActions = True
else
   FireActions = False
end if
```

Check the size of a specific file and record to a database

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

Set objFSO = CreateObject("Scripting.FileSystemObject")

If objFSO.FileExists(FileToCheck) Then
   Set objFile = objFSO.GetFile(FileToCheck)

   statID = GetStatID(FileToCheck)
   RecordStat statID, objFile.Size

   If objFile.Size < 1000 Then
      FireActions = True
      Details = FileToCheck & " is too small!"
   Else
      FireActions = False
   End If
Else
   FireActions = True
   Details = FileToCheck & " does not exist!"
End If
```

Check if the newest file is older than 6 hours old (to ensure new files are being created)

```
DirToCheck = "C:\Logs"
Dim fNewest
set oFolder=createobject("scripting.filesystemobject").getfolder(DirToCheck)
For Each aFile In oFolder.Files
   If fNewest = "" Then
      Set fNewest = aFile
   Else
      If fNewest.DateCreated < aFile.DateCreated Then
         Set fNewest = aFile
      End If
   End If
Next

if fNewest.DateCreated < (DateAdd("h",-6,Now())) then
   FireActions = True
   Details = "NEWEST LOG FILE older than 6 hours (latest file " & fNewest.DateCreated & ")"
else
   FireActions = False
end if
```

Launch a program and check the result code

```
Dim objShell
Set objShell = CreateObject("WScript.Shell")
'Spaces in the path below can cause trouble for the Run method
exitCode = objShell.Run("C:\Test\App.exe", 1, True)
Set objShell = Nothing
```

```
if (exitCode = 0) then 'assuming 0 means OK in this case
    FireActions = false
    Details = "Everything is OK"
Else
    FireActions = true
    Details = "Test app returned " + exitCode
End If
```

Check for text in a file

```
Option Explicit
Dim oFSO, sFile, oFile, sText
Set oFSO = CreateObject("Scripting.FileSystemObject")
sFile = "\\machine\share\textfile.txt"
If oFSO.FileExists(sFile) Then
    Set oFile = oFSO.OpenTextFile(sFile, 1)
    Do While Not oFile.AtEndOfStream
        sText = oFile.ReadLine
        If Trim(sText) = "ERROR" Then
            FireActions = True
        Else
            FireActions = False
        End If
    Loop
    oFile.Close
Else
    FireActions = True
End If
```

Thanks goes out to Seth Johnson at Williams for this

Monitor UDP ports using Microsoft PortQry

```
Set p = CreateObject("WScript.Shell").Exec("%COMSPEC% /c c:\portqry.exe -n <server_name> -e 443 -p
udp")
Do While p.Status = 0
Sleep "100"
Loop
Details = p.StdOut.ReadAll
if inStr(Details, "NOT LISTENING") then
    FireActions = True
else
    FireActions = false
end if
```

Thanks goes out to Darrell Swafford at Hardee County Schools for this

Javascript Examples

The Javascript and VBScript scripting engines are identical, other than the syntax of the language. That means you can look at all of the VBScript examples and make simple changes so it uses Javascript syntax. For example:

```
VBScript:
 Set p = CreateObject("WScript.Shell")
 FireActions = True
 Sleep "100"

Javascript:
 object p = CreateObject("WScript.Shell");
 FireActions = True;
 Sleep(100);
```

With that in mind, go to the VBScript examples.

PowerShell Examples

Check files in a directory

```
$mon.FireActions = $false
$mon.Details = ""
$highCount = 1000
$folder = "C:\Temp"
$files = Get-ChildItem $folder -Force

if ($files.Count -gt $highCount)
{
   $mon.FireActions = $true
   $mon.Details = "File Count is " + $files.Count
}
```

Launch a PS program and record results

```
$mon.FireActions = $false
$statID = $mon.GetStatID("VMGUEST1_5z_free")
$mon.Details= &powershell.exe "c:\skripte\VM_LUN_Freeperc.ps1 VC1 vmguest1_5z"
$mon.RecordStat($statID, $mon.Details)
```

Thanks goes out to Peter Strauss at KELAG-KÃƒÂ¯Ã‚Â¿Ã‚Â½rntner for this

Monitor AD Sysvol

```
$Mon.FireActions = $False
$Name = $Mon.ComputerName
$Mon.Details = ""
$Folder = "\\" + $Name + "\Sysvol"

If ((Test-Path $Folder) -eq $False)
{
$Mon.FireActions = $true
$Mon.Details = "SYSVOL is not accessible on " + $Name
}
Else
{
$Mon.Details = "SYSVOL is accessible on " + $Name
$Mon.FireActions = $False
}
```

Thanks goes out to Joel Ashman at Progeny Systems Corporation for this

Monitor AD Replication

```
#Note: Requires AD RSAT tools on PA Server for RepAdmin.exe

$Mon.FireActions = $False
$Mon.Details = ""

$Name = $Mon.ComputerName

$Replication = Repadmin /ShowRepl $Name /CSV | ConvertFrom-CSV | Where {$_.'Number of Failures' -gt 0 }
| Select -Unique 'Source DSA' | Sort 'Source DSA'

If ($Replication)
{
$String = ""
$String += "The Domain Controller $($Name.ToUpper()) is having difficulty replicating The following
servers:`n`n"
$String += " Server`n"
$String += " --------`n"

ForEach ($ReplError in ($Replication ))
{
$Source = $ReplError.'Source DSA'
$String += " " + $Source + "`n"
}
$Mon.FireActions = $True
$Mon.Details = $String
}
Else
{
$Mon.FireActions = $False
$Mon.Details = "Replication is now functioning for Domain Controller " + $Name
}
```

Thanks goes out to Joel Ashman at Progeny Systems Corporation for this

Monitor Window's License Activations

```
$mon.FireActions = $true
$mon.Details = "Windows OS is NOT activated"

$DNSHostName = $mon.ComputerName
try {
$wpa = Get-WmiObject SoftwareLicensingProduct -ComputerName $DNSHostName `
-Filter "ApplicationID = '55c92734-d682-4d71-983e-d6ec3f16059f'" `
-Property LicenseStatus -ErrorAction Stop
}
catch {
$status = New-Object ComponentModel.Win32Exception ($_.Exception.ErrorCode)
$wpa = $null
}

$out = New-Object psobject -Property @{
ComputerName = $DNSHostName;
Status = [string]::Empty;
}

[bool] $fireAction = $true

if ($wpa) {
:outer foreach($item in $wpa) {
switch ($item.LicenseStatus) {
0 {$out.Status = "Unlicensed"}
1 {$out.Status = "Licensed"; $fireAction = $false; break outer}
2 {$out.Status = "Out-Of-Box Grace Period"; break outer}
3 {$out.Status = "Out-Of-Tolerance Grace Period"; break outer}
4 {$out.Status = "Non-Genuine Grace Period"; break outer}
```

```
5 {$out.Status = "Notification"; break outer}
6 {$out.Status = "Extended Grace"; break outer}
default {$out.Status = "Unknown value"}
}
}
}
else {$out.Status = $status.Message}

if(!$fireAction)
{
$mon.FireActions = $fireAction
$mon.Details = $DNSHostName + ": Windows OS is activated"
}
```

Thanks goes out to Joel Ashman at Progeny Systems Corporation for this

SSH Examples

Monitor process memory usage

```
# The lines highlighted in red are where the SSH script returns information back to the monitor

#--- Set variables here ---

PROCESS_NAME="???" # Run ps -eo comm,pmem to find this
THRESHOLD="30.0" # The percentage memory usage to start firing actions

#--------------------------
AWK_SCRIPT="\$2 ~ /${PROCESS_NAME}/ {memoryusage += \$1} END {print memoryusage}"
MEMUSAGE=`/bin/ps -eo pmem,comm | /usr/bin/awk "${AWK_SCRIPT}"`
TEST_RESULT=`echo "${MEMUSAGE} > ${THRESHOLD}" | /usr/bin/bc -q`
PREPOSITION="below"
if [ ${TEST_RESULT} == "1" ]; then
  echo "PA_FireActions(true)"
    PREPOSITION="above";
fi

echo "PA_Details(\"Memory usage of ${PROCESS_NAME} is ${PREPOSITION} ${THRESHOLD}% (${MEMUSAGE}%)\")"
echo "PA_RecordStat(\"Memory Usage/${PROCESS_NAME}\", ${MEMUSAGE})"
```

- Monitor memory of service

Your Script

```
If you would like to share your script, please contact us.
```

File Age Monitor

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

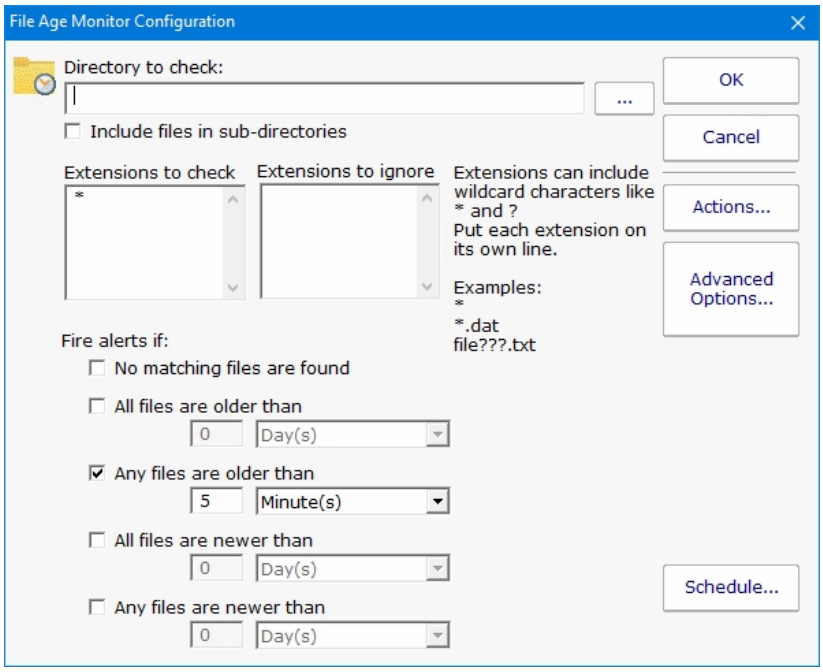
Specify a pattern that defines which set of files will be watched. You may use wildcards in the file specification.

As shown below, indicate the condition when you want to be notified. This can include:
Indicating the extension(s) to check for or to ignore

No files of the specified type found

Any or all files are too old

Any or all files are too new



Standard Configuration Options

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

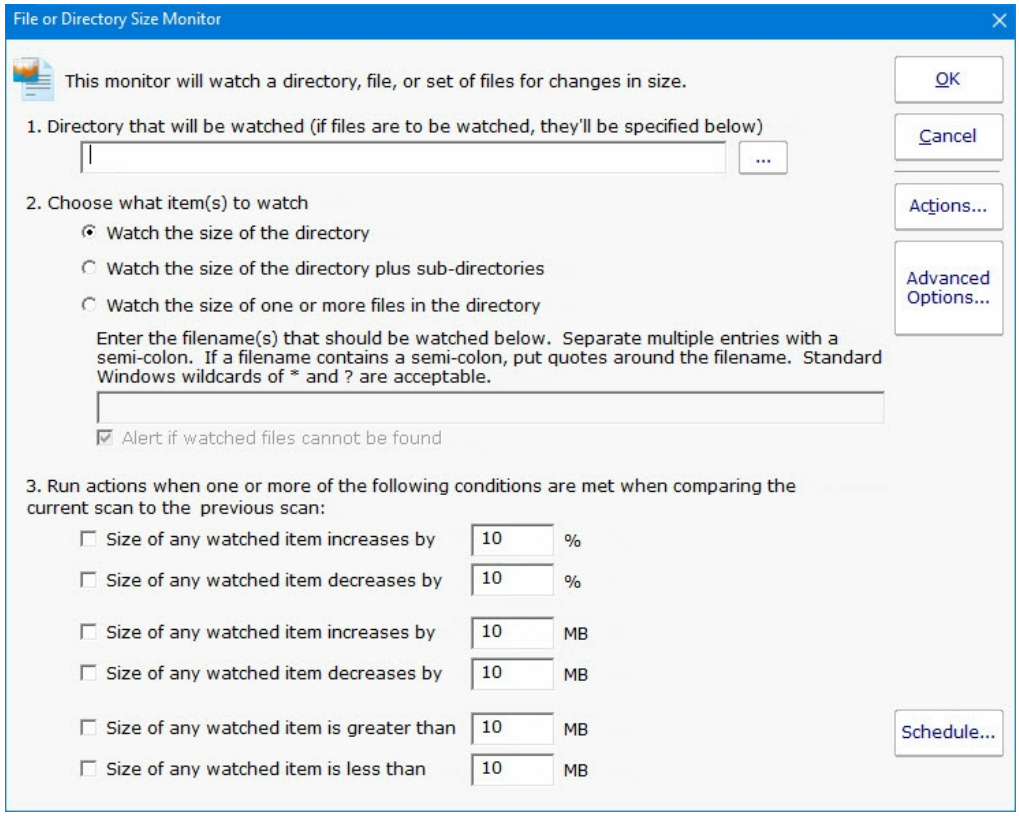
File/Directory Size Monitor

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

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

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

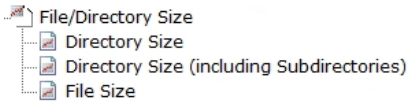
Last choose the growth conditions that should trigger the configured actions. They can include growth beyond a pre-set limit, or growth of a certain amount from one scan to the next.



Standard Configuration Options

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

Supported Reports



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

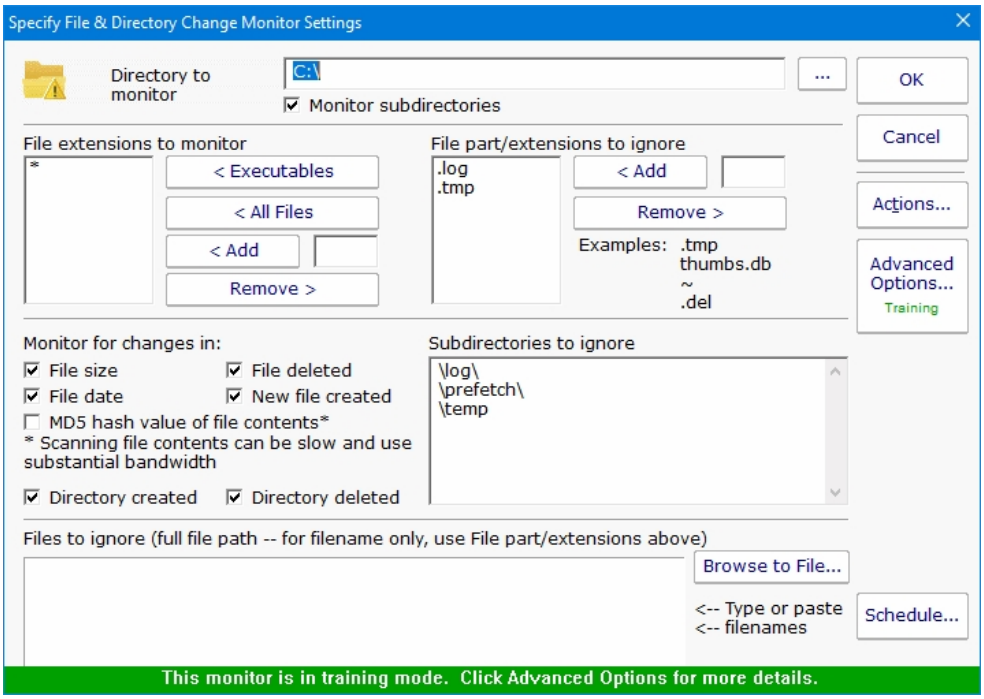
File & Directory Change Monitor

(aka CIFS Monitoring, File Integrity Monitoring, FIM)

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 file integrity monitoring (FIM) as described in the "Payment Card Industry Data Security Standard" (PCI DSS) (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.

The File & Directory Change Monitor can watch any CIFS share, which includes Windows shares, shares on a NAS device, and shares on Linux/Unix computer that were shared with the Samba daemon.



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, 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...** 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 where 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

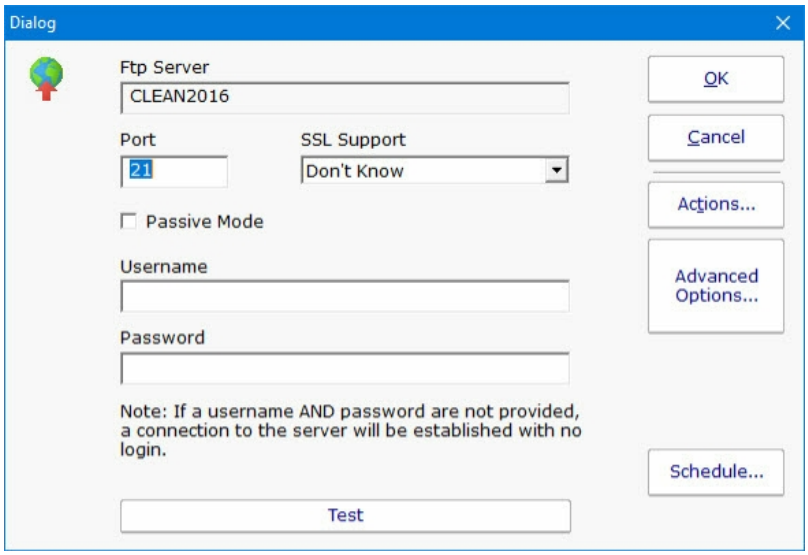
Like all monitors, this monitor has standard buttons on the right for Adding Actions, setting Advanced Options and setting the Monitor Schedule.

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.



Above you can see the configuration dialog for configuring the FTP Server monitor. The FTP server name is taken from the server that the monitor is attached to. An optional username and password can be entered.

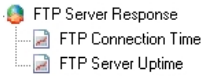
SSL connections (FTPS) are supported. If you don't know which setting to use, select "Don't Know" and press the Test button. Each option will be tried and the one that works will be selected for you automatically.

When you press the Test button, the FTP settings are sent to the monitoring service (Central Monitoring Service or Satellite) and are tried there. The test results will be sent back and displayed.

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.

Hardware Monitor

The Hardware Monitor can query hardware status from the following devices:

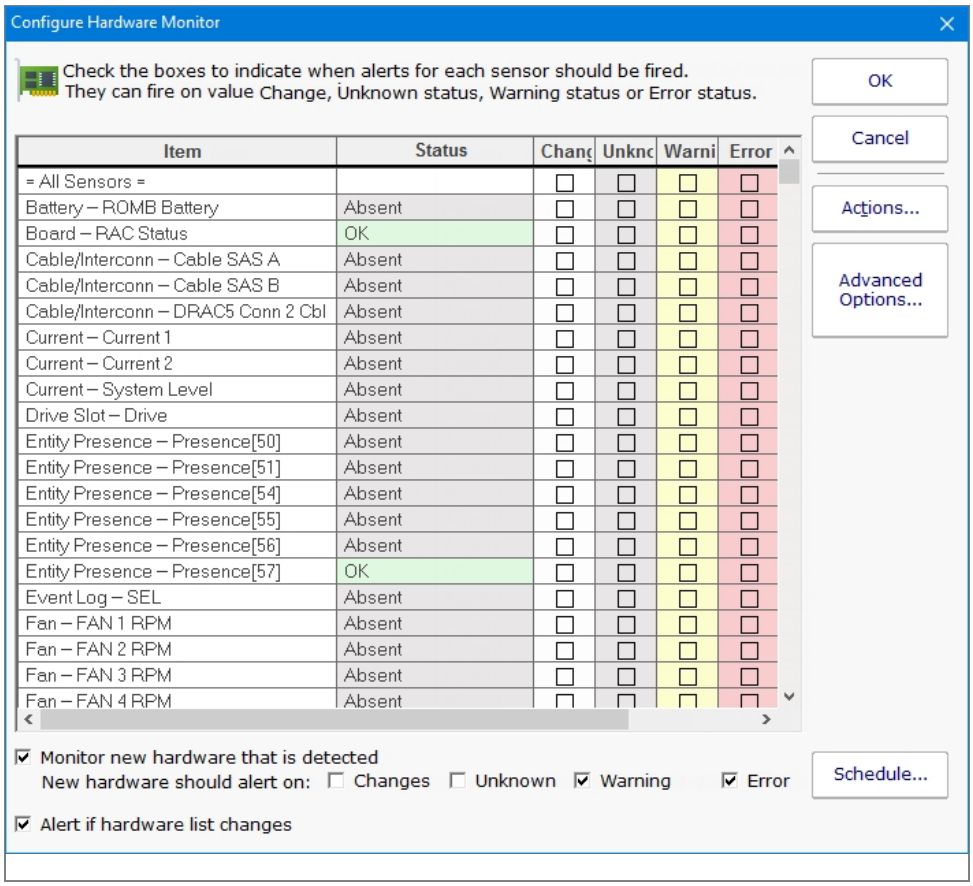
VMWare ESX (via ESX APIs)

Dell DRAC/iDRAC (via IPMI)

HP iLO (via IPMI)

IBM RAS (via IPMI)

Other IPMI devices



Configuration

Configuration is very simple. Make sure the device has IPMI or ESX credentials set. After that, the device will be queried and the status of all hardware components will be shown.

Place a check box next to any component for the value you want to be alerted on. You can be alerted if the status is OK, Warning or Error. You can also be alerted if the status value changes.

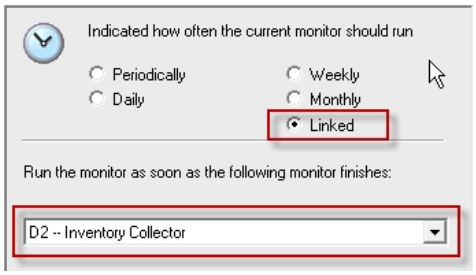
At the bottom of the monitor you can indicate what should happen if the list of hardware components changes. This might indicate hardware is being added or removed from a system.

Standard Configuration Options

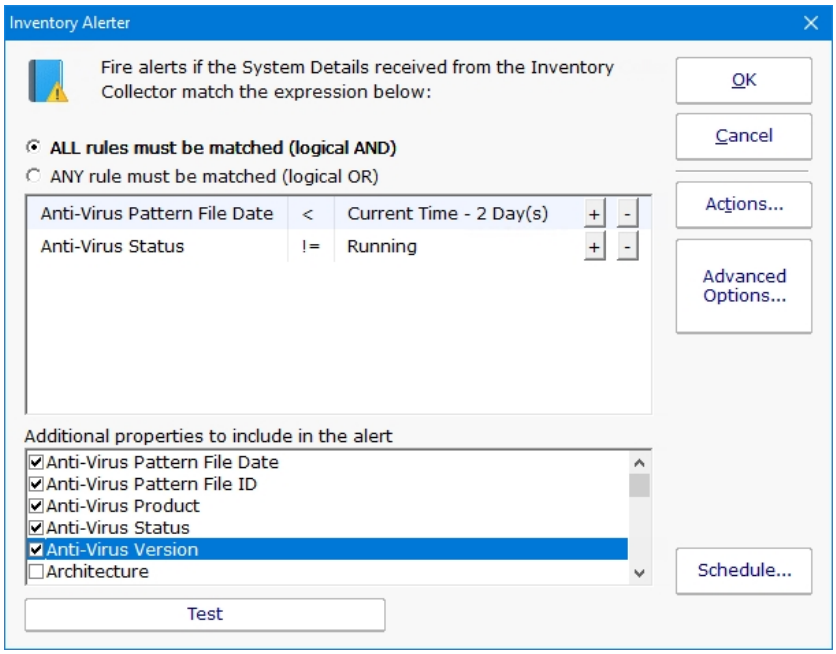
Like all monitors, this monitor has standard buttons on the right for Adding Actions, setting Advanced Options and setting the Monitor Schedule.

Inventory Alerter

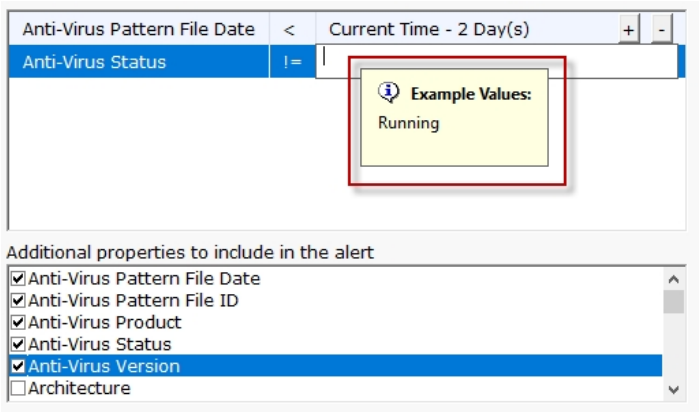
The Inventory Alerter monitor runs checks against the inventory database which was filled by the Inventory Collector monitor. Because they work so closely, the Inventory Alerter's schedule is usually linked to the Inventory Collector, so it runs as soon as the Collector finishes.



The Inventory Alerter is basically an expression builder that lets you specify a list of rules to check for the target server. If the rules match, the monitor's actions are fired. The example below shows a possible check of the anti-virus software running on the target server.

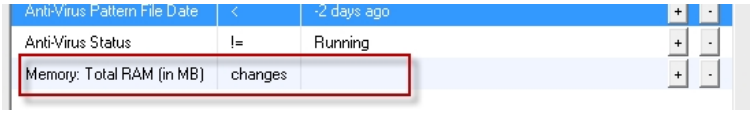


Many of the possible values for an inventory property would be hard to guess, so you can hover over the field to see a list of example values in the database for that value.



Besides specifying property match values, you can also indicate which additional properties should be shown in alert messages. This often helps give context to what is wrong with the present value of the property. For example, by including the Last Boot field when there are pending updates, you might discover a computer isn't rebooting as expected.

You can also detect and be alerted to hardware changes in a target computer. For example, you could detect if RAM was added or removed.

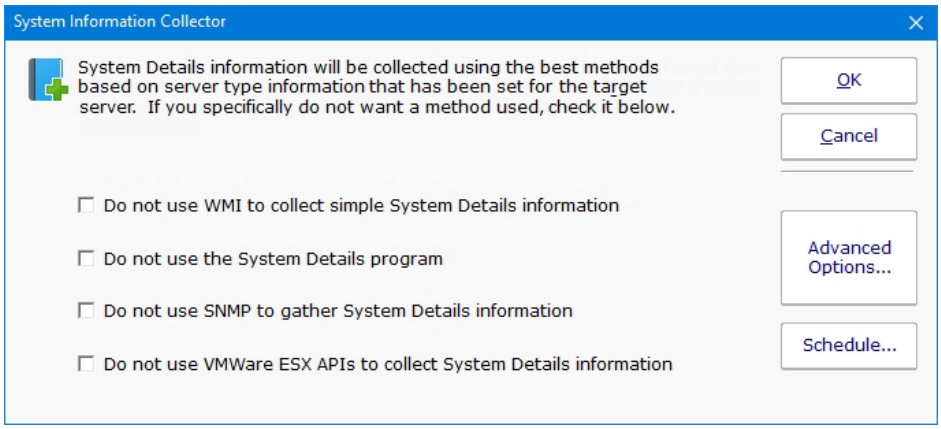


Watch the training video How to Monitor Anti-Virus and alert when Pattern File Date is out of date.

Inventory Collector

The Inventory Collector monitor collects the basic machine information that is shown in the System Details box on the Server Status Report. Most of the collected information does not change often, so the monitor defaults to running every few hours.

To configure the monitor, indicate what techniques should be used to collect inventory information. The available techniques are based on the server type of the target device. Selecting the inventory technique is as simple as checking the available box(es). (Note that some products will have different sets of check boxes available)



System Details and Inventory Probe

The System Details and Inventory probe has a few extra system requirements to allow the probe to be able to scan the server. If you are you are receiving error messages about installing .NET or Powershell, you can resolve the error by installing the necessary items or by unchecking the second option, "Collecting System Details and Inventory data with the System Details program".

System Details Probe Requirements	
Powershell Version	1.0 or 2.0
.NET	2.0/3.5

Anti-Virus Detection

The System Details program (second check box from the top) can collect information about anti-virus applications installed on Windows computers. Supported applications and versions are listed below.

Product	Tested Version
ESET NOD32	4.0
McAfee Virusscan Enterprise	2013
Microsoft Security Essentials	4.1
Norton Internet Security	
Symantec Endpoint Protection	12.0
Trend Micro	7.0

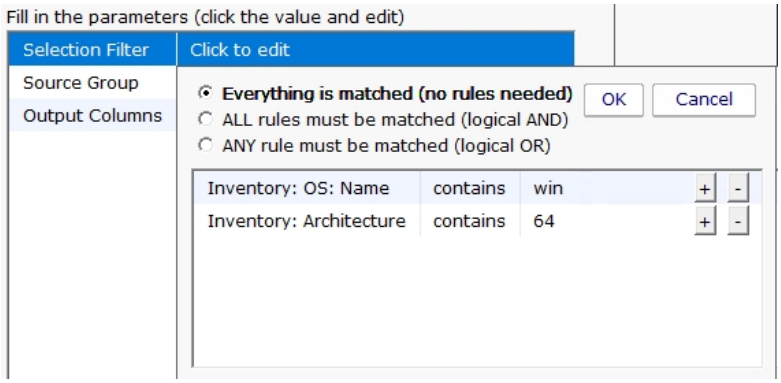
Depending on how the anti-virus manufacturers change or don't change their settings, other versions might also be successfully detected.

Custom Inventory Items

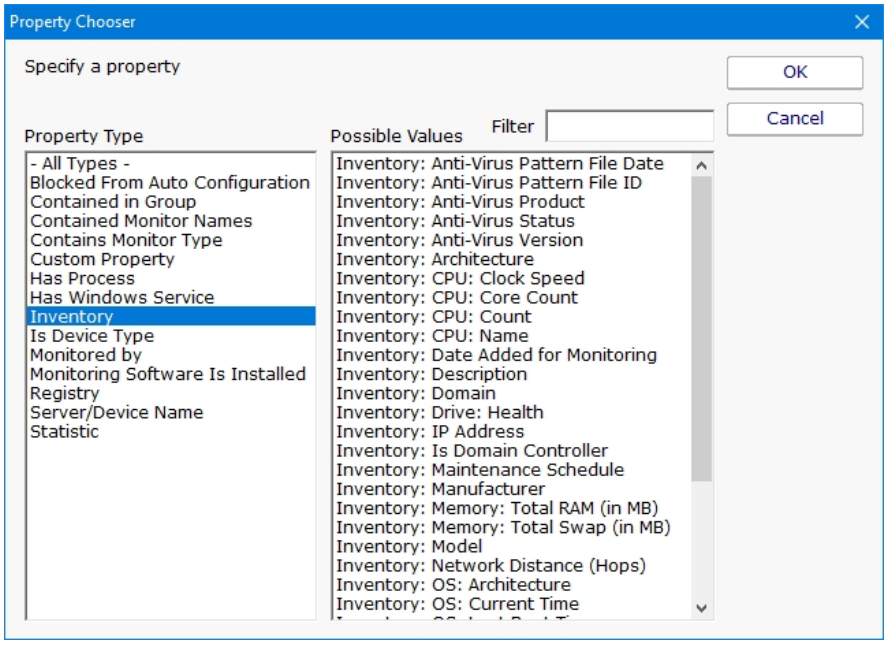
You can add additional items to be collected via SNMP using the InventoryList.txt file that is in the product directory. The file contains instructions on using the simple file format.

Inventory Reports

The information collected by the Inventory Collector will populate the Inventory Database. You can run reports against this database and use a simple expression builder to specify exactly which servers you'd like to show up in the report.



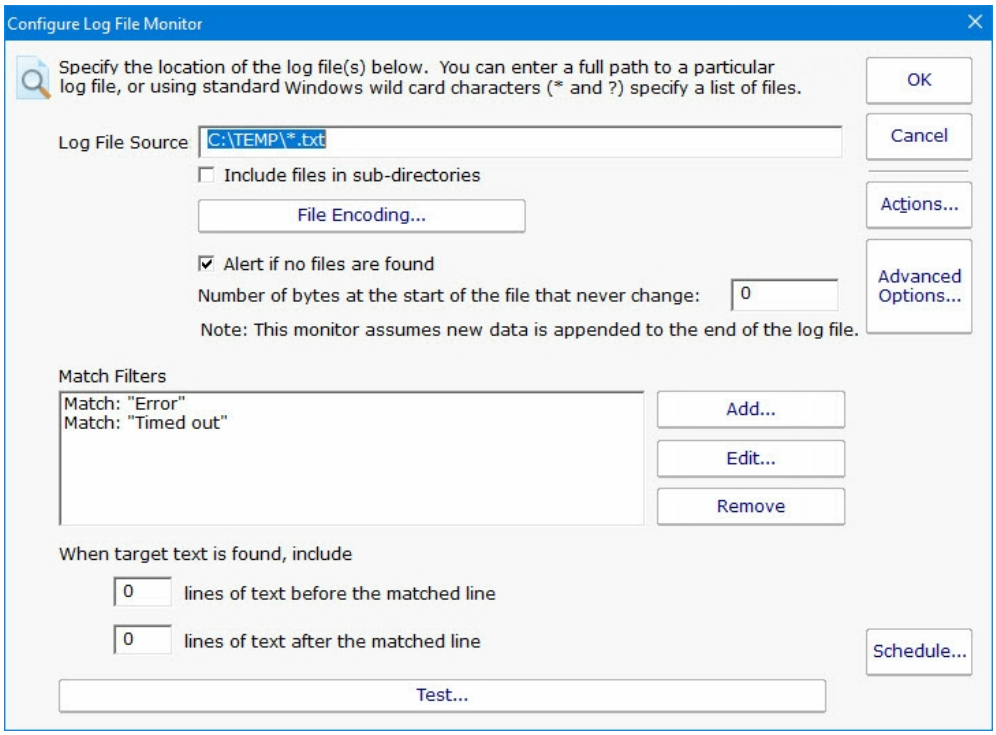
Once the target servers are specified, you can select the output columns that should be shown. Additional inventory property values are being added all the time.



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.

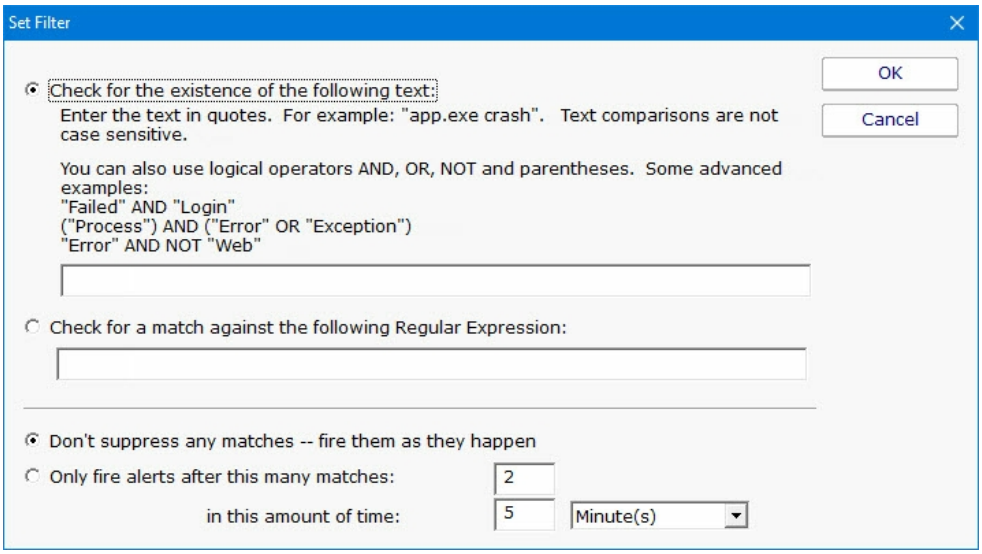
The Log File Monitor employs an efficient mechanism to only read changed parts of the file(s). That means it starts reading only text that is added after the first run of the monitor. The search text can be specified as a simple phrase, or you can use the power of regular expressions for more complex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



Multiple filters can be specified as in the example above. If any filter matches, the monitor will alert on the matched line of text.

Filters

Filters can be specified in two ways: text matching or Regular Expression.



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**

Testing

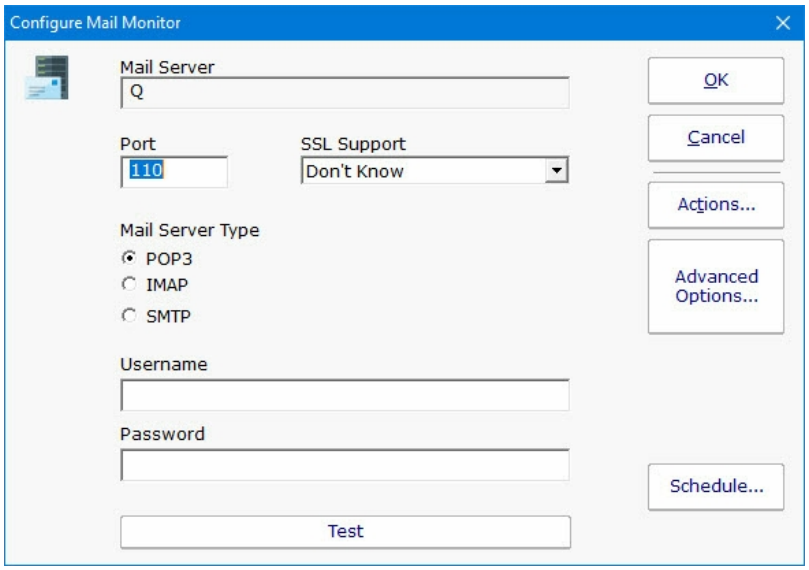
You can test your filters with the Test button. This will send your filters and file specification to the monitoring service to make a quick check. **One Caveat:** When testing, the check will run from the beginning of the file. When the monitor is running normally though, it's only going to check what has been recently added to the file (so it doesn't keep alerting on the same text over and over).

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.

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.



Above you can see the configuration dialog 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.

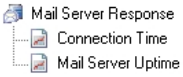
SSL connections (POPS, IMAPS and SMTPS) are supported. If you don't know which setting to use, select "Don't Know" and press the Test button. Each option will be tried and the one that works will be selected for you automatically.

When you press the Test button, the mail settings are sent to the monitoring service (Central Monitoring Service or Satellite) and are tried there. The test results will be sent back and displayed.

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.

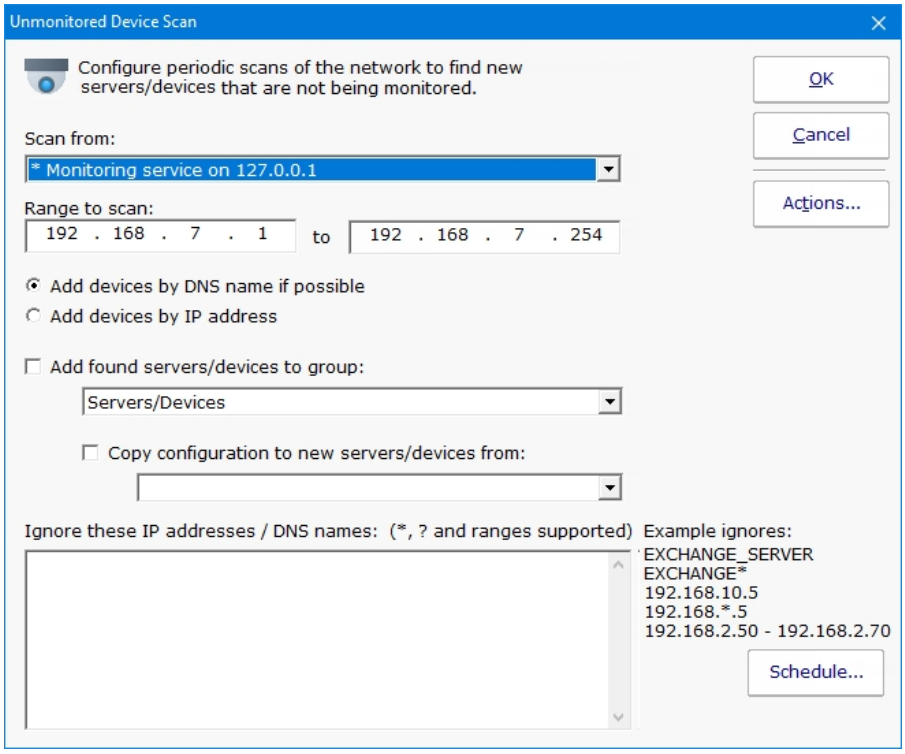
Supported Reports



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.

Network Scanner

The Network Scanner monitor is a Global Monitor that runs outside of any server. It does an IP address ping scan looking for servers that are not already being monitored.



When new devices are found on the network, you can have them automatically added to PA Server Monitor to a specific group. You can also have a configuration copied from an existing server/device.

If you configure actions for this monitor and new devices are found on the network, you will receive a list of those devices in the fired 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.

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 simulated for Linux/Unix machines via SNMP, and via VMWare interfaces for ESX servers, and via IPMI for those devices such as the Dell DRAC/iDRAC and HP iLO. Monitoring and charting those values is now as easy as with a Windows server.

Watch the training video How to Monitor Memory or How to Monitor CPU.

Supported Server/Device Types

This monitor supports retrieving and monitoring counter values for:

All Windows versions

Linux and other devices that support SNMP

VMWare ESX

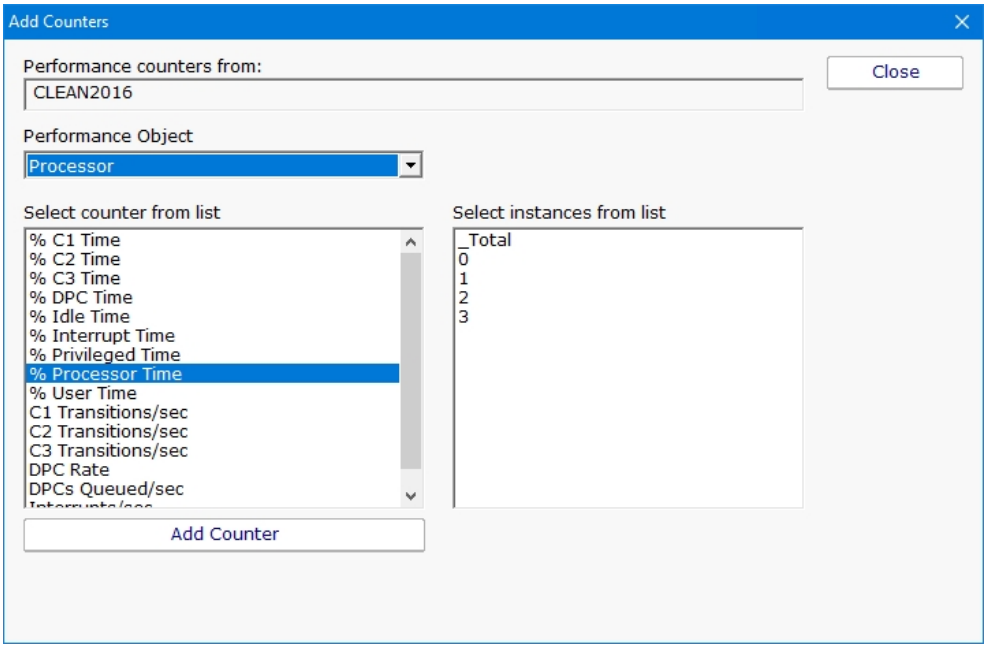
IPMI devices such as the Dell DRAC/iDRAC and HP iLO, and others

Amazon Web Services (AWS) CloudWatch based counters

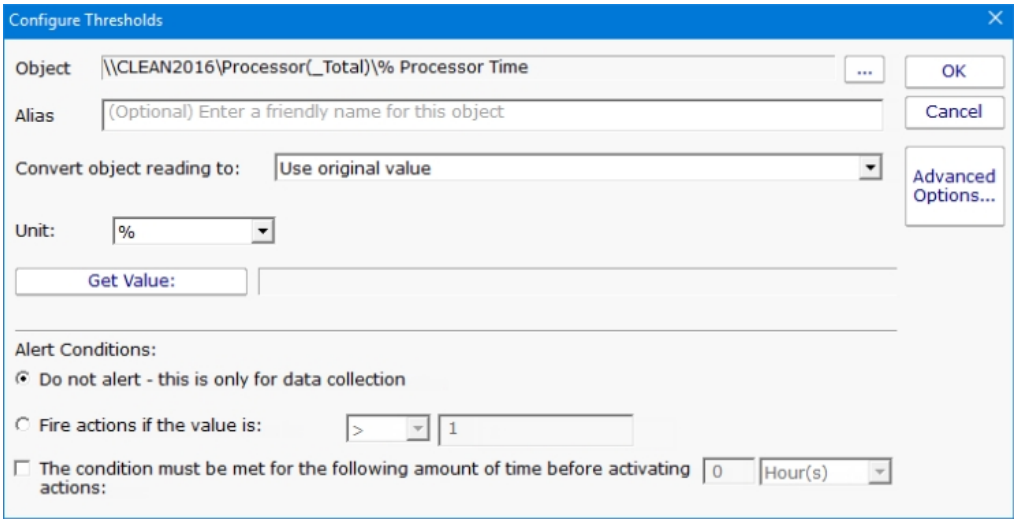
Make sure the computer's Server Type is set correctly, and that the appropriate credentials (Windows, SNMP, ESX, IPMI, AWS) exist to allow the monitor to access the performance counters.

Configuration

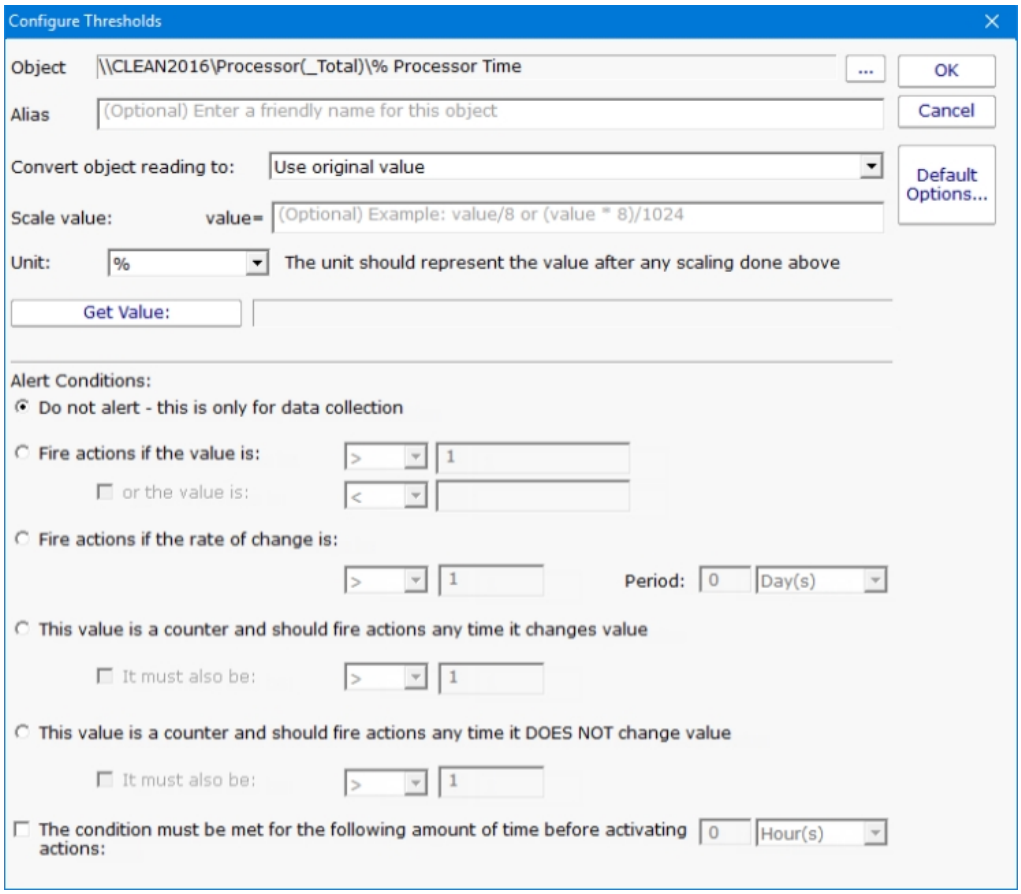
When adding a counter to be monitored, the target server is queried for counters it supports, and a dialog similar to the Windows Perfmon dialog is shown where you can select the counter that you want to monitor. Servers monitored by Satellites will also be queried immediately for their counter lists.



Once a counter has been chosen, alerting criteria are specified. A threshold (low or high) and the amount of time the threshold has to be exceeded before actions are fired can be given. If the theshold is passed, the offending counter and its current value will be part of the action description.



If you choose the Advanced Options button, the dialog changes and you are given richer threshold options, which include rate of change, checking for values within a range, or not alerting at all and just collecting data.



Each time a performance counter is measured and checked, it is also recorded in a database in order to generate historical reports.

Units

For the charting to work correctly, it's important to specify the correct unit of the counter. The monitor will correctly correctly guess the unit for some common counters, but you will need to set it for others.

Scaling

If the counter value cannot be represented by an existing unit, you might be able to scale it. For example, imagine the counter is MBps, but the available unit is Mbps. To correctly record the value, you should set the scale to:

```
value = value * 8
```

and then set the unit to Mbps

Instance Wildcards

Many counter paths have an *instance* value. Using the Network Interface counter as an example, these two counters might be on a computer:

```
\\SERVER\Network Interface(Intel[R] Ethernet Connection [2] I219-V)\Bytes Received/sec
\\SERVER\Network Interface(Intel[R] 82574L Gigabit Network Connection)\Bytes Received/sec
```

The *instance* is the part between the (and), so in this example, the instances would be:

```
Intel[R] Ethernet Connection [2] I219-V
Intel[R] 82574L Gigabit Network Connection
```

Sometimes you want to monitor an object, but don't know what the instance might be named (very common with the Network Interface scenario). This can happen if you're trying to copy the monitor, or setup a monitor template. In that case, click the "**...**" button next to the path, and change the instance to *

In our example, a monitor that could watch both example counters (or others found on other computers) could use the following path:

```
\\SERVER\Network Interface(*)\Bytes Received/sec
```

When the monitor runs, it will replace the * with each instance it finds of that counter type, and then monitor and record the instance-specific value.

The instance can be replaced with * and ? with other letters and numbers, where * means any characters and ? means any single character. So you could for example use:

```
\\SERVER\Network Interface(Giga*)\Bytes Received/sec
```

Regular Expressions

The instance can also use Regular Expressions besides just * and ?. To use them, the format needs to be

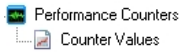
```
RegEx:{regular expression}
```

For example, the following example will watch all ASP.NET Application Pools, *except* for the _Total instance:

```
\\SERVER\APP_POOL_WAS(RegEx:^[A-Z,a-z,0-9].*$)\Current Application Pool State
```

The regular expression above will match any app pool name that starts with A-Z, a-z or 0-9. _Total does not match that.

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.

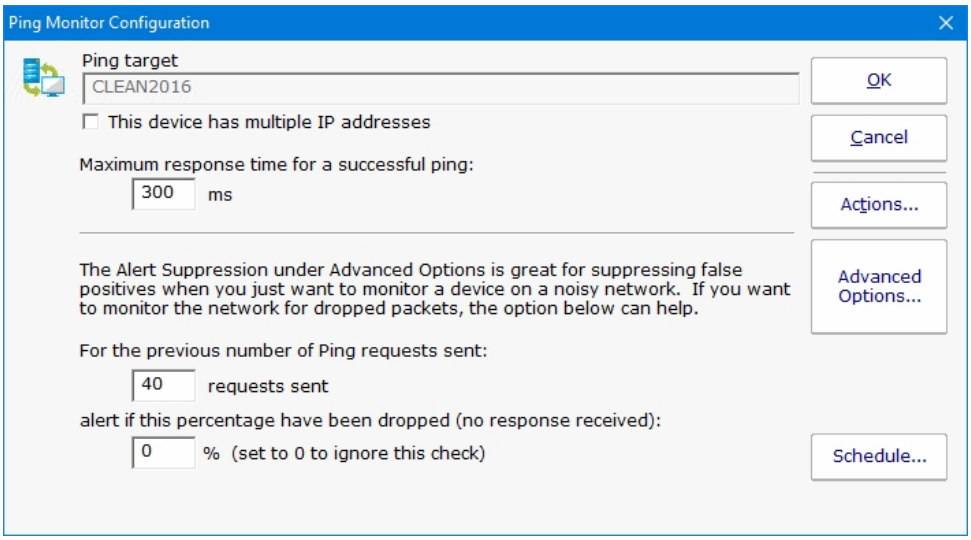
In addition, the Server Status Report can be configured to show charts for any value that is monitored.

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.

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.



DNS monitoring

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

Internal Pings

There are a variety of internal operations that can also cause ping requests to be sent (for example, a ping might be sent if a monitor has a dependency on a Ping monitor, but the Ping monitor hasn't run recently). The results of these internal pings are cached for a few seconds to keep from doing duplicate work.

Monitor Operation

When the ping monitor runs, it checks the cache to see if there was a successful ping recently (within the past 10 seconds by default). If there was, it reports success.

If you want to ping more often than once every 10 seconds, you should change the registry value:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor
[DWORD] Ping_Cache_Response_Sec
```

so the caching time is shorter.

If a fresh enough value is not found in the cache, a ping request is sent on the network. If a successful response is received within the specified time frame, all is well.

If no response is received, or a response is received but it took too long, up to two more ping requests are sent. If any are received successfully within the specified time frame, the monitor considers this a success.

Percent Dropped

The Ping monitor can also alert if the percent of dropped requests passed a defined threshold. This percentage is based on all ping requests sent to the host, whether sent because of retries or internal operations. Requests satisfied from cache are not counted since a ping request was not actually sent out on the network in this case. The calculation is based on the past 128 ping results.

Ping Data

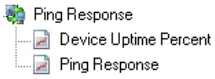
Ping result times are recorded for report generation. If a ping response is never returned, a time of 30,000 is used to indicate the failure in reports. The Uptime Report is very useful with Ping data.

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.

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 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.

Plugin Monitor

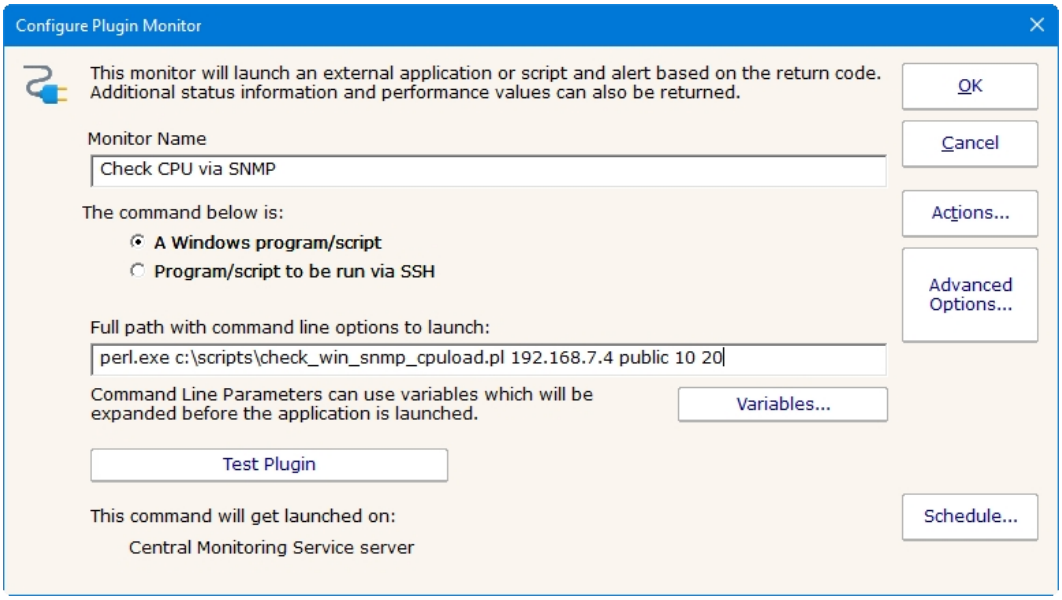
The Plugin Monitor makes it easier to add custom monitors to PA Server Monitor. To make plugin reuse as easy as possible, this monitor is compatible with the output from Nagios plugins, which means many plugins from the Nagios Exchange will work. Not all plugins at the exchange will work - some need extra dependencies, and some don't follow the plugin output format properly.

Plugin Types

Plugins are executable programs or scripts that can be run by the monitor. There are two types:

Windows programs/scripts - These are run on the Central Monitoring Service, or a Satellite Monitoring Service, that is monitoring the target server.

SSH - These are scripts or programs run via an SSH session. A terminal session will be created on the target device via SSH from the monitoring service (Central Service or Satellite Monitoring Service).



Plugin commands can use replacement variables in the command line which will be replaced before the command is run. For example, the following could be used as a monitor template:

```
perl.exe c:\scripts\check_win_snmp_cpuload.pl $DEVICENAME$ public 70 90
```

In this case $DEVICENAME$ could be replaced by the target device's hostname/IP as it is known to the system.

Output Format

Any program/script can be used as a plugin as long as it follows these rules:

Return/Exit Code
: The return code, also known as an exit code, for the program will be interpreted as follows:

- 0 - OK

- 1 - monitor should go into Alert state and run actions
- 2 - monitor should go into Alert (Red) state and run actions
- 3 - monitor should go into Can't Run Monitor Now, and try again soon

Any return code other than the above will put the monitor into the red Can't Run Monitor error state.

Returned Status

This monitor is compatible with Nagios plugins, which means the returned text (from stdout; stderr is ignored) as follows:

- Any text on the first line, up to a | (pipe) symbol is status text that will be used for the monitor status and for alerts. Everything after the | is considered performance data.
- Any text on the following lines will be appended to the first line as more status text.
- The next to the last line uses the same format as the first line (meaning it can have the optional | symbol with performance data following).
- All of the last line is considered performance data.

In all cases, the performance data must be formatted as:

```
{name}={value}{unit};{warning threshold};{everything here ignored up until a space}{space
character}{name}={value}{unit};{warning threshold};...
```

- {name} must be quoted with a single quote if the name contains spaces.
- {unit} is optional, and can be one of: %, ms, us, s, B, KB, MB, TB
- {warning threshold} is optional, but if it exists, is assumed to use the same unit as {value}
- Spaces are important - a space signifies the end of one performance value and the start of the next.

Some examples:

```
OK - everything running smoothly|CPU=1% 'Physical Memory'=1TB 'Free Disk Space'=57%;10;5;1; (this
is all on one line)
```

Note that the 5;1; above is ignored since it comes after the threshold.

```
Alert - temperatures are too high. CPU is 220F
Disk temperatures are 180F, 190F
```

This plugin did not return any performance data - it's all status text. Also note that the plugin MUST return an exit code of 1 or 2 if the monitor is supposed to fire actions - the status text does not affect the monitor status.

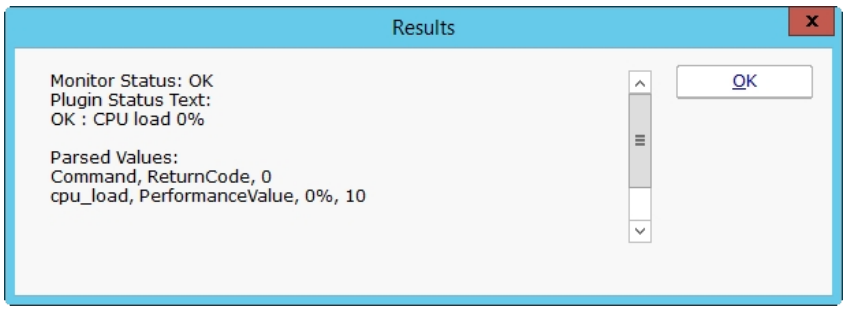
```
OK - Mail systems good | CPU=5%;90 Free-Disk:80%
Memory-Usage:45% Mail-Store-Usage:67%
```

The last line is performance data that will be parsed and stored in the database.

Testing

The **Test Plugin** button will run the plugin and show how the text was interpreted, and show the raw text that was received from the

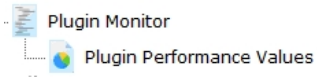
plugin. For SSH-run plugins, you will see a few lines of additional script code that are used to receive the output.



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 Plugin Monitor can create reports based on the performance values returned from the plugin progra/script. This data can be charted as well as output in .CSV or HTML tabular form.

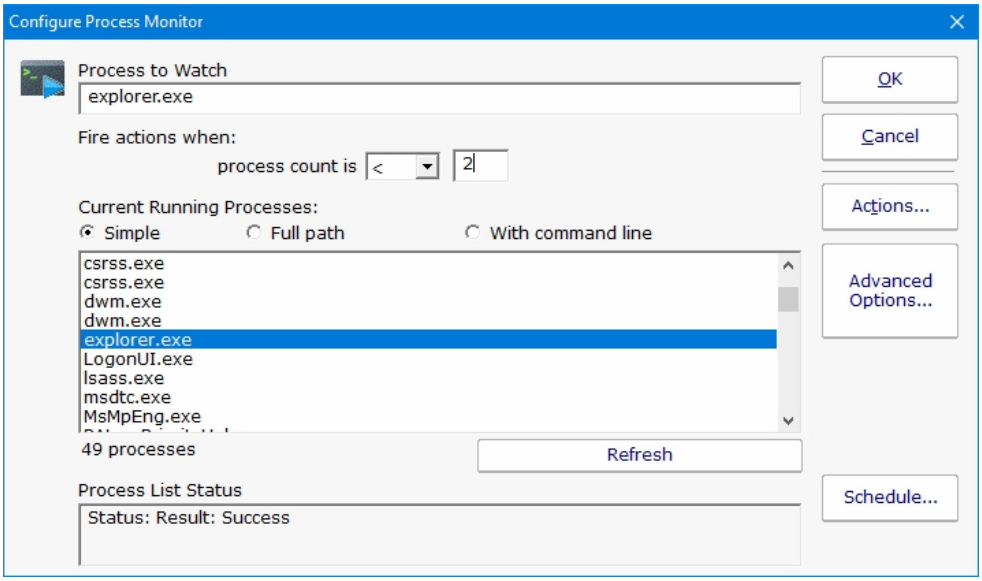
Process Monitor

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.

Watch the training video How to Monitor if a Process is Running.

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.



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.

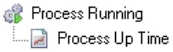
Note: If the target server is monitored by a Satellite, the available processes will be retrieved from the Satellite during the configuration step.

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.

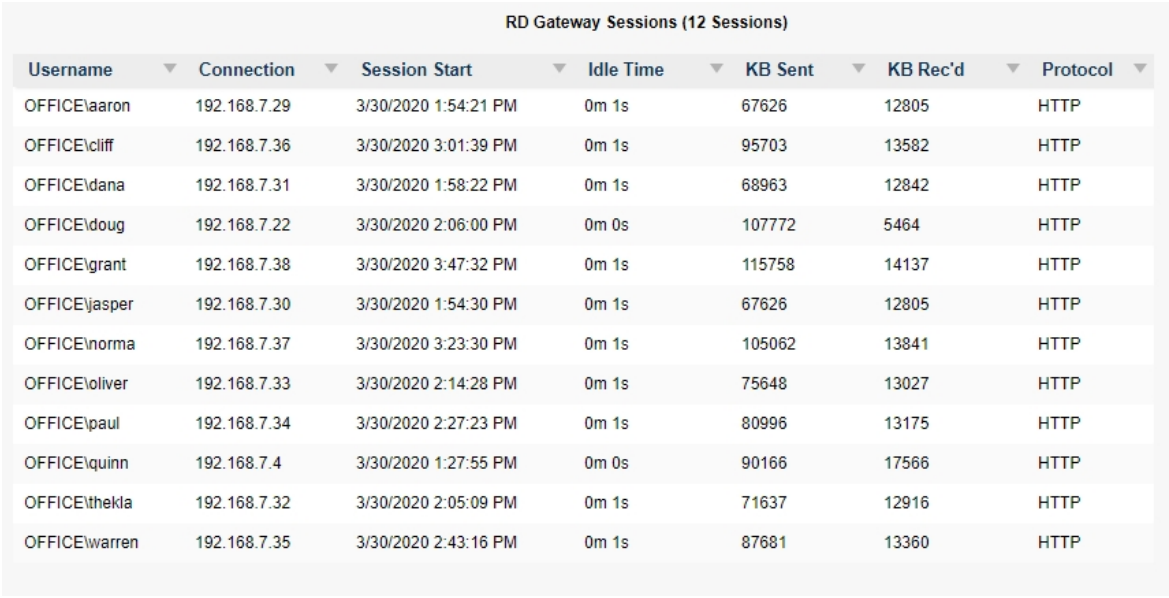
Supported Reports



Process 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.

Remote Desktop (RD) Gateway Monitor

The RD Gateway monitor is used to periodically retrieve a list of Remote Desktop sessions connected to the Gateway



RD Gateway Sessions (12 Sessions)

Username	Connection	Session Start	Idle Time	KB Sent	KB Rec'd	Protocol
OFFICE\aaron	192.168.7.29	3/30/2020 1:54:21 PM	0m 1s	67626	12805	HTTP
OFFICE\cliff	192.168.7.36	3/30/2020 3:01:39 PM	0m 1s	95703	13582	HTTP
OFFICE\dana	192.168.7.31	3/30/2020 1:58:22 PM	0m 1s	68963	12842	HTTP
OFFICE\doug	192.168.7.22	3/30/2020 2:06:00 PM	0m 0s	107772	5464	HTTP
OFFICE\grant	192.168.7.38	3/30/2020 3:47:32 PM	0m 1s	115758	14137	HTTP
OFFICE\jasper	192.168.7.30	3/30/2020 1:54:30 PM	0m 1s	67626	12805	HTTP
OFFICE\norma	192.168.7.37	3/30/2020 3:23:30 PM	0m 1s	105062	13841	HTTP
OFFICE\oliver	192.168.7.33	3/30/2020 2:14:28 PM	0m 1s	75648	13027	HTTP
OFFICE\paul	192.168.7.34	3/30/2020 2:27:23 PM	0m 1s	80996	13175	HTTP
OFFICE\quinn	192.168.7.4	3/30/2020 1:27:55 PM	0m 0s	90166	17566	HTTP
OFFICE\thekla	192.168.7.32	3/30/2020 2:05:09 PM	0m 1s	71637	12916	HTTP
OFFICE\warren	192.168.7.35	3/30/2020 2:43:16 PM	0m 1s	87681	13360	HTTP

There is no configuration for the monitor and it doesn't presently fire alerts. It is just used for reporting. The chart above would be shown on a Server Status Report.

Supported Reports

The RD Gateway Monitor can report on Remote Desktop sessions on a per-user, per-connected resource or per-gateway basis.

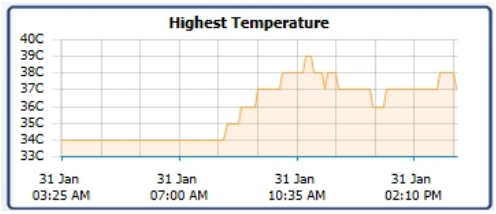
Server Temperature Monitor

The Server Temperature Monitor works with the free SpeedFan computer temperature measuring 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.*

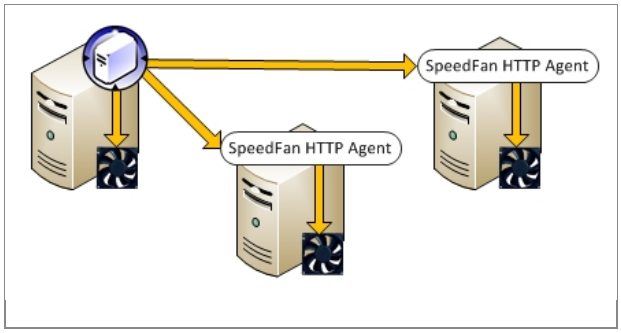
After SpeedFan is installed, the Server Temperature Monitor will query the SpeedFan app to extract current temperature values from the various temperature probes detected.

Server reports will soon show a temperature graph charting the highest measured temperature:



Server Temperatures Across the Network

The Server Temperature Monitor can automatically connect to SpeedFan that is installed on the same computer as the PA Server Monitor software. To retrieve temperatures from SpeedFan running on other computers on the network, you'll need to install the free SpeedFan HTTP Agent which makes the temperature data available on the network as shown below:

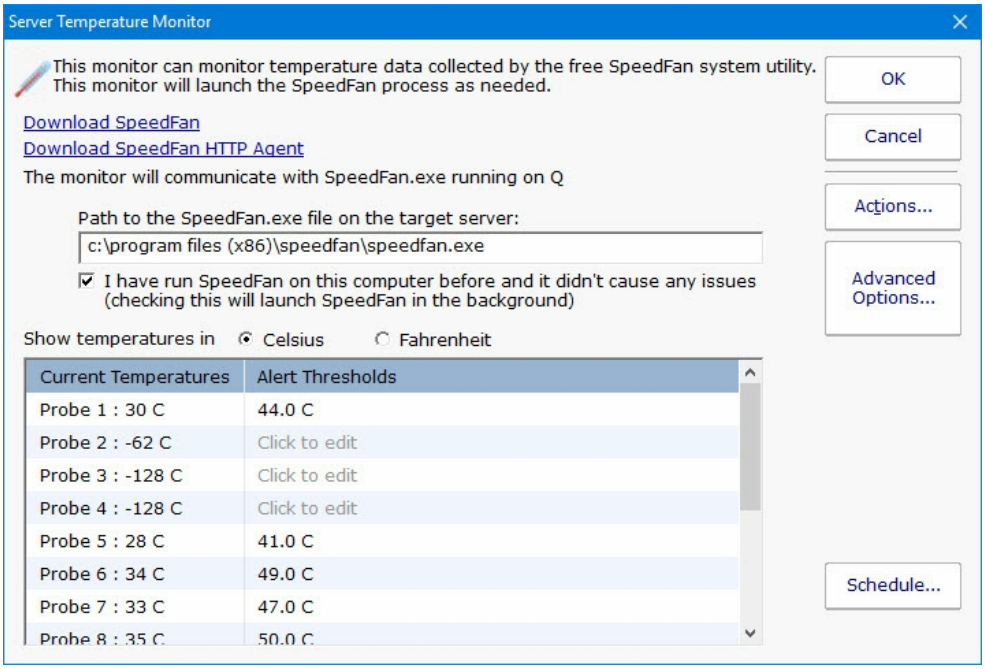


Configuration

To configure the Server Temperature Monitor:

If monitoring the local computer, simply specify the path to the SpeedFan.exe file (the default path given is typically correct). Then indicate that you have successfully run SpeedFan before (to allow PA Server Monitor to launch SpeedFan)

If monitoring temperatures on a remote computer, give the port that the SpeedFan HTTP Agent is using



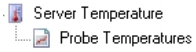
After a connection to SpeedFan has been established, live temperatures will then be collected and displayed.

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

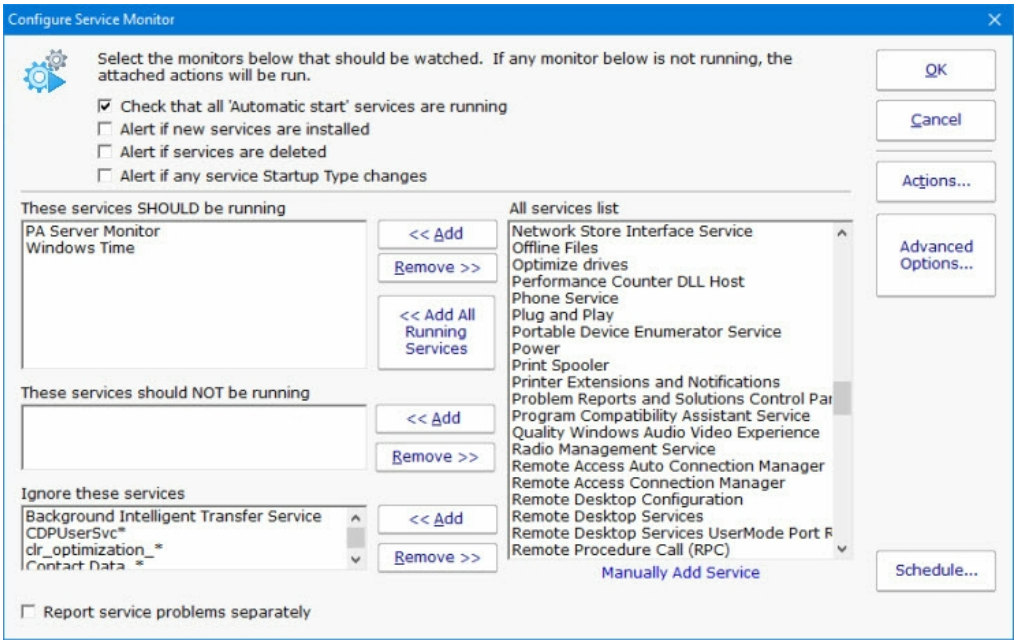


The various temperature values are all recorded to a database. You can run reports that chart these values or produce tabular output in HTML or .CSV files for importing into Excel, etc. The data can be optionally summarized into hourly, daily, weekly and monthly values.

Service Monitor

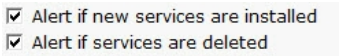
The Service Monitor watches the same system services that can be seen from the Administrator Tools Services applet (services.msc). If a service is not running, actions are fired (which could notify you and/or restart the service for example). The Restart Service action is typically attached to this monitor.

Watch the training video How to Add a Service Monitor in PA Server Monitor.

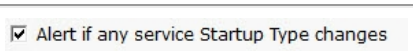


There are a lot of different parts to this monitor, so we'll take them one at a time.

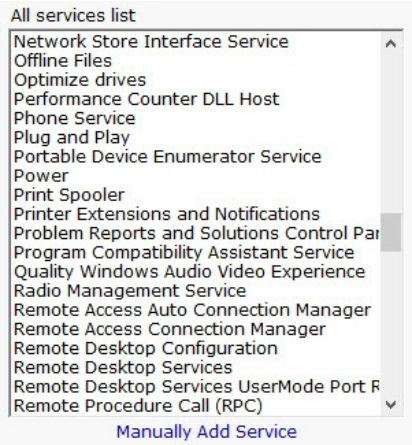
The easiest way to use this monitor is to check the "Check that all 'Automatic Start' services are running". Every time the monitor runs, the service list is fetched and if a service is set to Automatic start isn't running, alerts will fire.



This option simply fires alerts when a new service is first seen, or if a service that was once registered is no longer there.

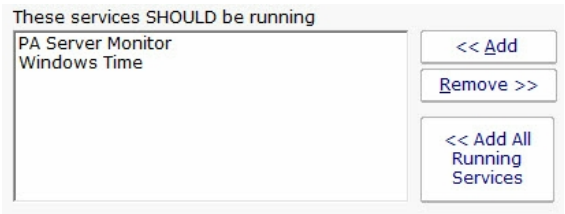


This option simply fires alerts when service's Startup Type changes.

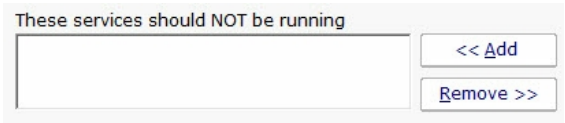


This box lists all of the service that are currently listed on the target server. It will match the list you see in services.msc. If you can see this list, the monitor is able to actively communicate with the target server (even if you are monitoring a server at a remote site via a Satellite Monitoring Service).

Occasionally you may come across a service that is added and removed during some procedure. If you want to ignore a service like that, you can click the "Manually Add Service" link at the bottom to temporarily add it to the "All services list". Once it's there, you can add it to the Ignored service list so it won't be alerted on.



If you have services that need to be running (perhaps they aren't "Automatic Start", or you don't want to monitor all "Automatic Start" services with the check box above), you can list them here.



Indicate any service that should NOT be running here. For example, some organizations will disable a service because of a security policy. If that service is ever running, it would need to be brought to someone's attention.

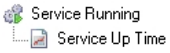
A number of services start and stop on their own during normal usage. You probably don't want to be notified about those services, so you can indicate they should be ignored. Ignoring a service means it will be ignored from all other checks specified above. PA Server Monitor automatically adds a few common auto-stop services to this list automatically.

This option will tell the service to send alerts for each service that gose into alert mode instead of grouping alerts together.

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.

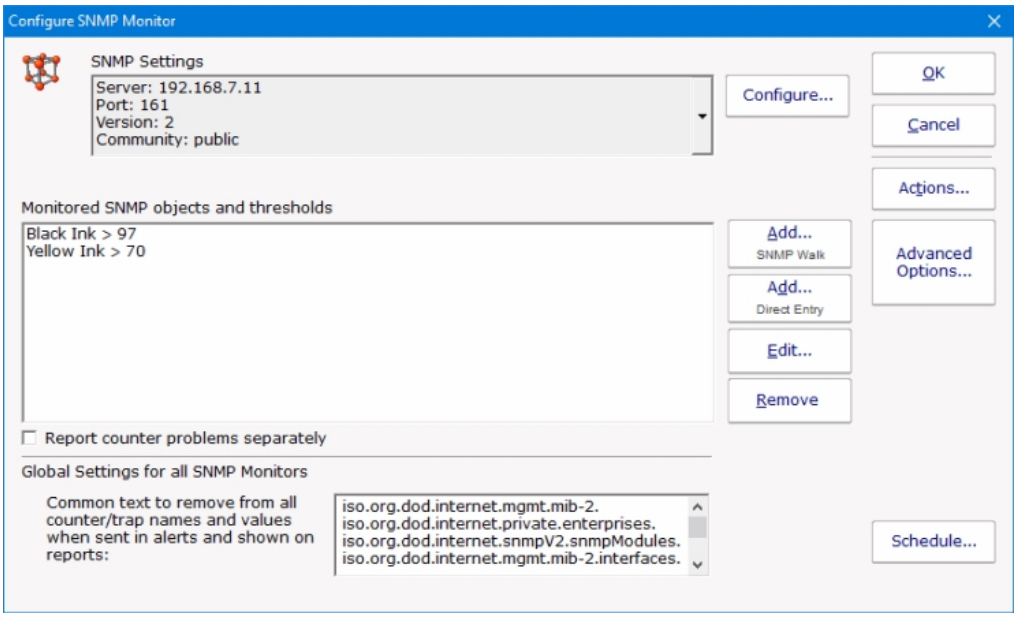
Supported Reports



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.

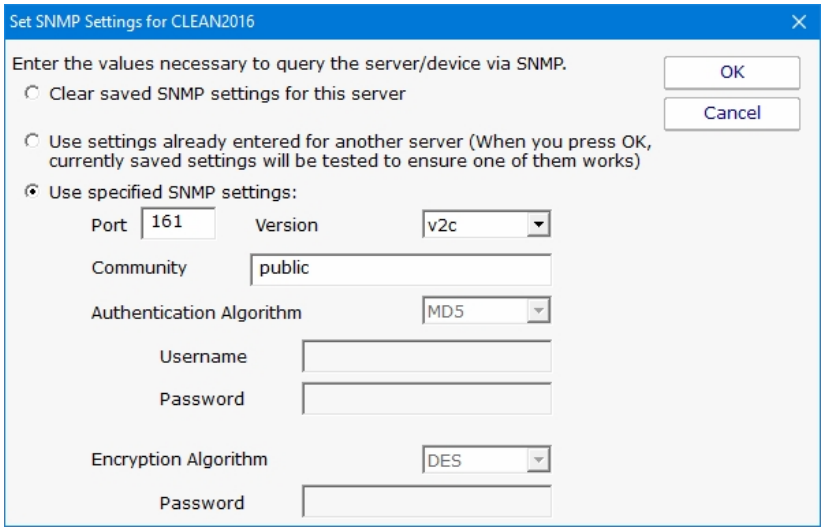
SNMP Monitor

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.



Configuring the SNMP Monitor requires SNMP credentials to be set, and 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.



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.

Monitoring a Linux server?

By default, Linux restricts SNMP access to queries from the local computer only. To enable network access, you'll need to edit:

```
/etc/snmp/snmpd.conf
```

Look for a line about agentAddress. It might look similar to the following:

```
agentAddress      udp:127.0.0.1:161
```

The above line might be commented out, or might not be in your file (not all snmpd.conf files are formatted the same). Instruct the SNMP daemon to respond to requests from the network is what is needed. Using the format from above, that line should look like this:

```
agentAddress      udp:161
```

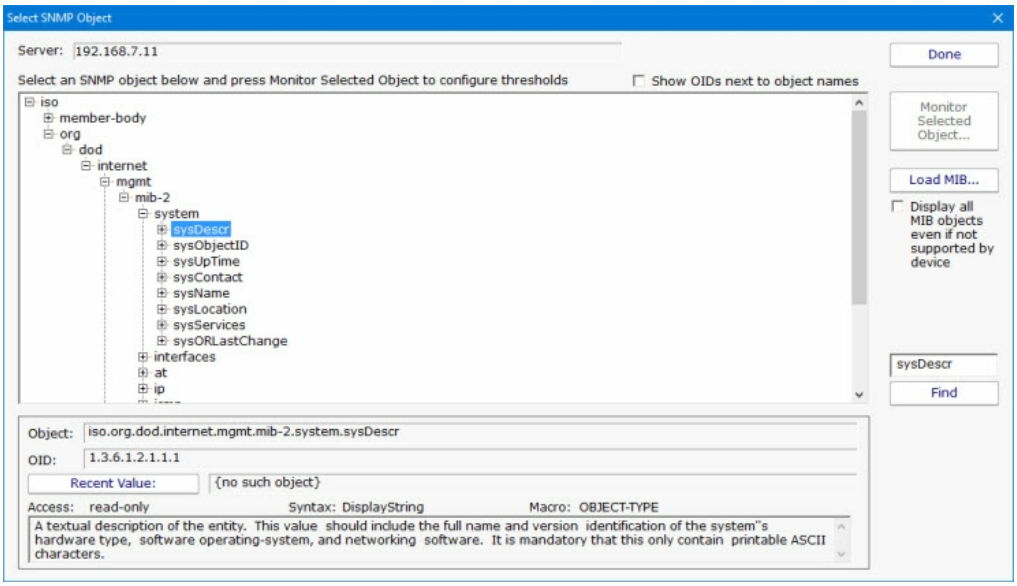
In addition, the default snmpd.conf file also restricts what you are able to see via SNMP. This is done by limiting which branches in the OID tree you can see. To enable more access, look for 'view' lines and add a line like the following:

```
view    systemonly    included    .1.3.6.1
```

After making these changes, you will need to restart the SNMP daemon (how you do that depends on your distribution of Linux)

Thank you to Timothy Stokes for researching and sharing this information.

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.



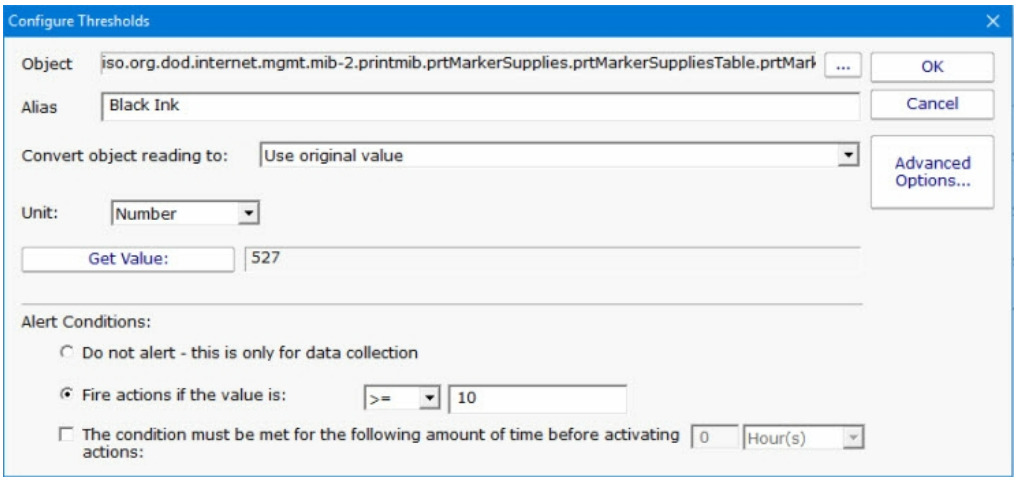
Note: If the target server is monitored by a Satellite, the available SNMP objects will be retrieved from the Satellite during the configuration step.

To monitor network bandwidth usage on a router or server, use the Find button to look for "ifInOctets" and "ifOutOctets" objects.

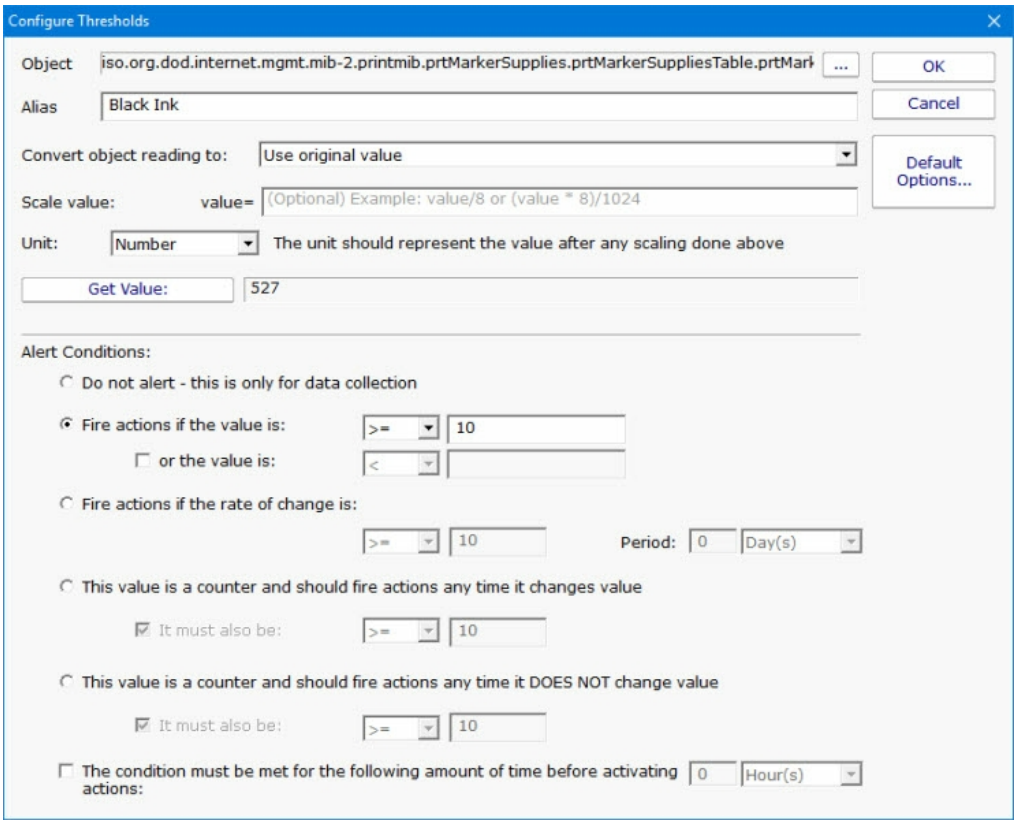
Unlike many SNMP browsers that only show objects for which you have MIBs loaded, this SNMP browser shows all objects that are available on the remote machine. Loading MIBs will add additional detail (like symbolic object names instead of just the numeric OID, and also textual descriptions for the fields).

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 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.



If you choose the Advanced Options button, the dialog changes and you are given richer threshold options, which include rate of change, checking for values within a range, or not alerting at all and just collecting data.



Each time a performance counter is measured and checked, it is also recorded in a database in order to generate historical reports.

Units

For the charting to work correctly, it's important to specify the correct unit of the counter. The monitor will correctly correctly guess the unit for some common counters, but you will need to set it for others.

Scaling

If the counter value cannot be represented by an existing unit, you might be able to scale it. For example, imagine the counter is MBps, but the available unit is Mbps. To correctly record the value, you should set the scale to:

```
value = value * 8
```

and then set the unit to Mbps

Using MIB Files

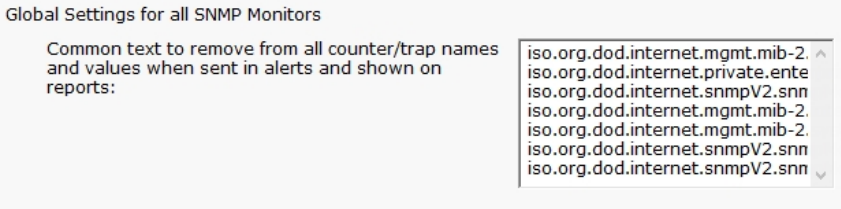
As mentioned above, MIB files are not required to monitor, but they make it easier to understand and find the different nodes available. You can load MIBs into the system by clicking the "Load MIB..." button shown above. In addition, one or MIB files can be copied into the following folder on the Central Monitoring Service:

C:\Program Files\PA Server Monitor\MIBs

Every few minutes, MIBs copied to that folder will get loaded and parsed, and shared among Consoles or Satellites that don't have them.

Shared Settings

Near the bottom of the dialog, you'll see this area where common SNMP removal text is shown:

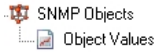


Removal text is shared among all SNMP monitors and Actions. Any time an SNMP object is reported on, the removal text is removed from the SNMP object's name. This helps cut down on clutter and makes reading the SNMP object names much easier.

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



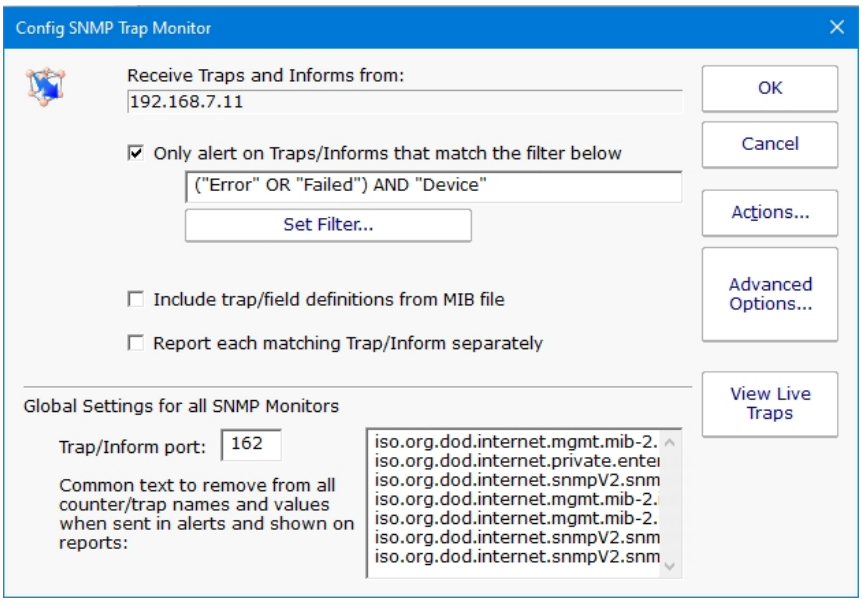
The SNMP monitor can create charts from any of the counter values that are being monitored. This includes bar and line charts. Tabular HTML and .CSV output for importing into other apps (Excel) are also possible.

SNMP Troubleshooting

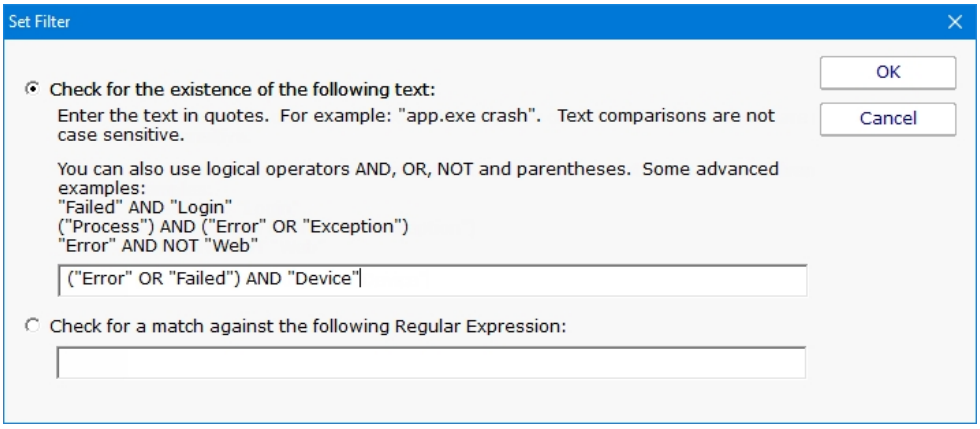
If you can't connect to a server/device via SNMP, make sure to double check the SNMP settings (version and community string in particular). Windows servers by default don't enable 'public' as a community string, and they don't accept SNMP requests from the network by default. These can both be changed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

SNMP Trap Monitor

The SNMP Trap Monitor receives SNMP Traps and Informs sent by networked devices. You configure those devices to forward Traps to PA Server Monitor, and configure the device trap thresholds, etc. So really, the SNMP Trap Monitor is an SNMP Trap receiver.



By default, all received traps will be alerted on. You can optionally create a filter that will only fire actions on specific traps that are received. Select the Set Filter button to enter your filter either using text or Regular Expression.



If you want to send some traps to one group of people, and other traps to a separate group, create two or more separate SNMP Trap monitors to watch for each group's specific traps.

If you will be forwarding traps via an E-mail Action, you can optionally specify that each individual trap be sent as a separate email.

Using MIB Files

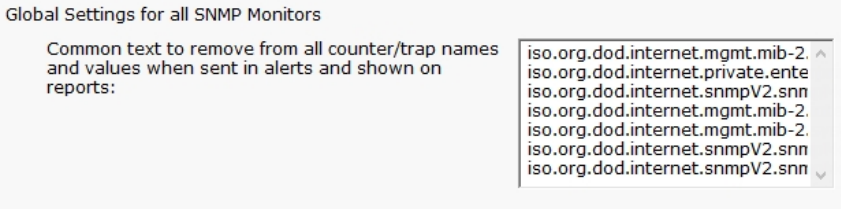
MIB files are not required to receive traps, but they usually make traps more human-readable. You can add MIBs to the system by copying them into the following folder on the Central Monitoring Service:

C:\Program Files\PA Server Monitor\MIBs

Every few minutes, MIBs copied to that folder will get loaded and parsed, and shared among Consoles or Satellites that don't have them.

Shared Settings

Near the bottom of the dialog, you'll see this area where common SNMP removal text is shown:



Removal text is shared among all SNMP monitors and Actions. Any time an SNMP object is reported on, the removal text is removed from the SNMP object's name. This helps cut down on clutter and makes reading the SNMP object names much easier.

Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for Adding Actions and setting Advanced Options. This monitor does not have a Schedule button since a schedule is not needed to receive traps.

Syslog Monitoring and Reporting

The Syslog Monitor receives logs from syslog agents on devices on your network. You configure those devices to forward their logs to PA Server Monitor. When a log line is received, the Syslog Monitor can store it in a database and optionally alert on it (send an email or write it to a log file for example).

Configuration - Port

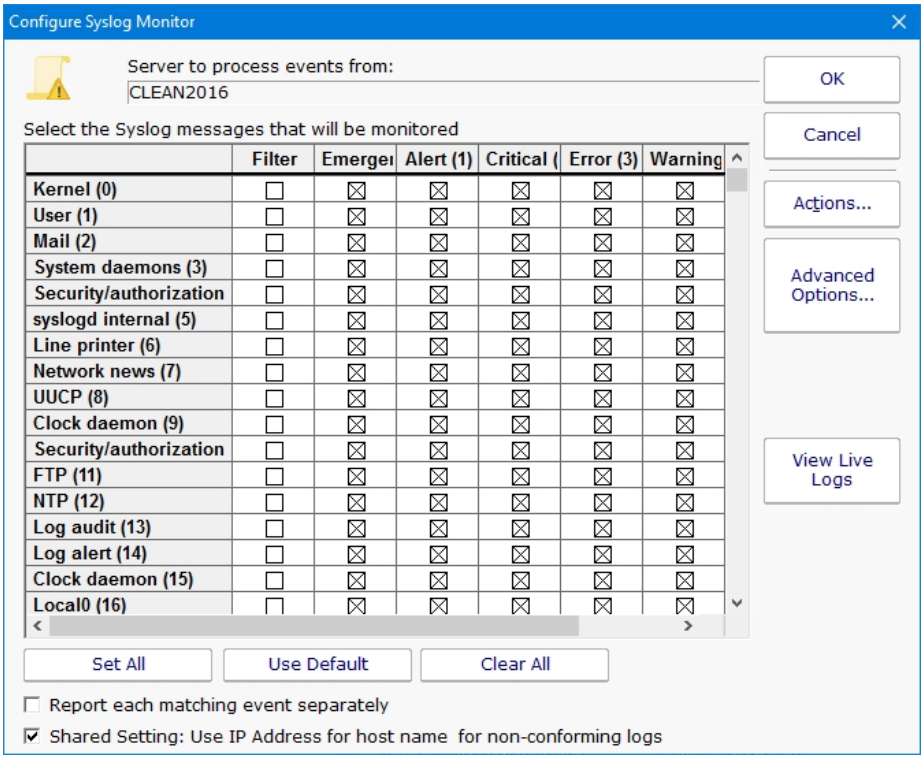
By default, the Syslog Monitor listens on the standard 514 syslog port. This can be changed in the registry at:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor
Syslog_Port = 514
```

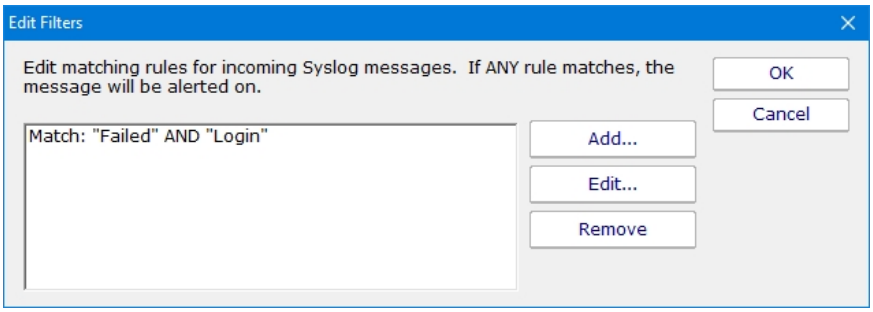
Note that this is a global value that affects all Syslog Monitors. The PA Server Monitor service needs to be restarted if this value is changed.

Configuration - Monitor Settings

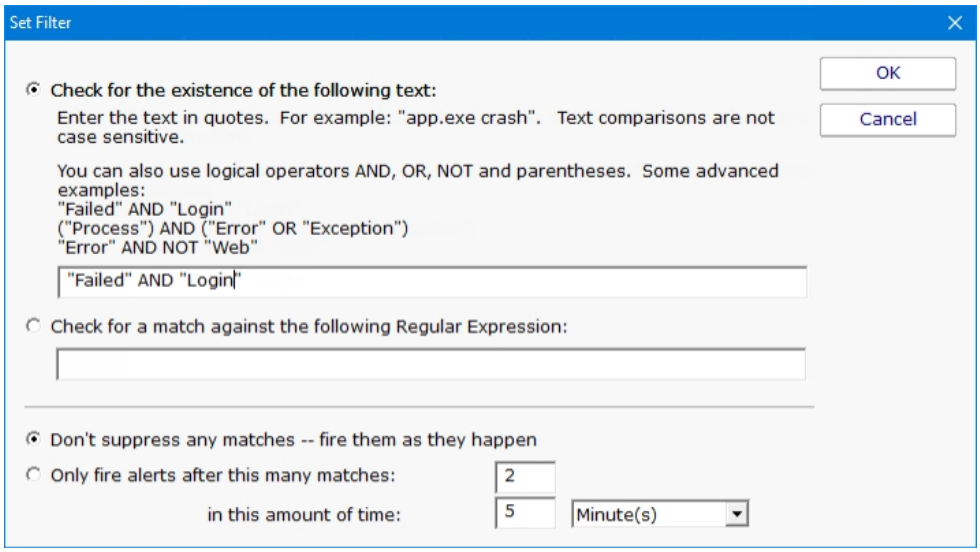
The monitor shows a grid of the standard syslog severities across the top, and standard facilities going down the left side. If you want the monitor to react to a syslog of a particular severity and facility, check that box. Syslogs that correspond to an unchecked box are ignored. All syslogs that match a checked box get written to a database for use in reports.



In addition to the severity/facility grid, you can also specify filters to further narrow which syslogs will cause alerts to fire and which you would like to ignore. Select the Filter Box in the column next to the Syslog.



Select the Add button to add a filter or Edit to edit a filter using text or a Regular Expression.



Syslogs that match the filter (which requires that they also match the severity/facility grid) will cause actions to fire. These actions can send email, write to log file, write to the Windows Event Log, etc.

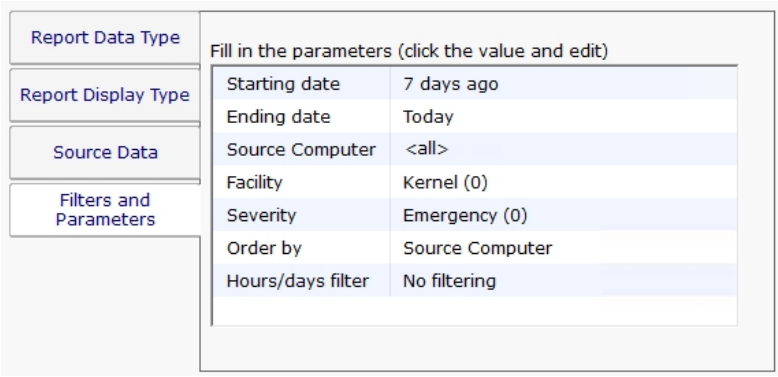
If you want different actions to run for different syslogs (perhaps some events going to one group and some events going to another group), you can create multiple Syslog Monitors with different filters, grid settings and attached actions.

Standard Configuration Options

Like all monitors, this monitor has standard buttons on the right for Adding Actions and setting Advanced Options. This monitor does not have a Schedule button since a schedule is not needed to receive syslogs.

Reports

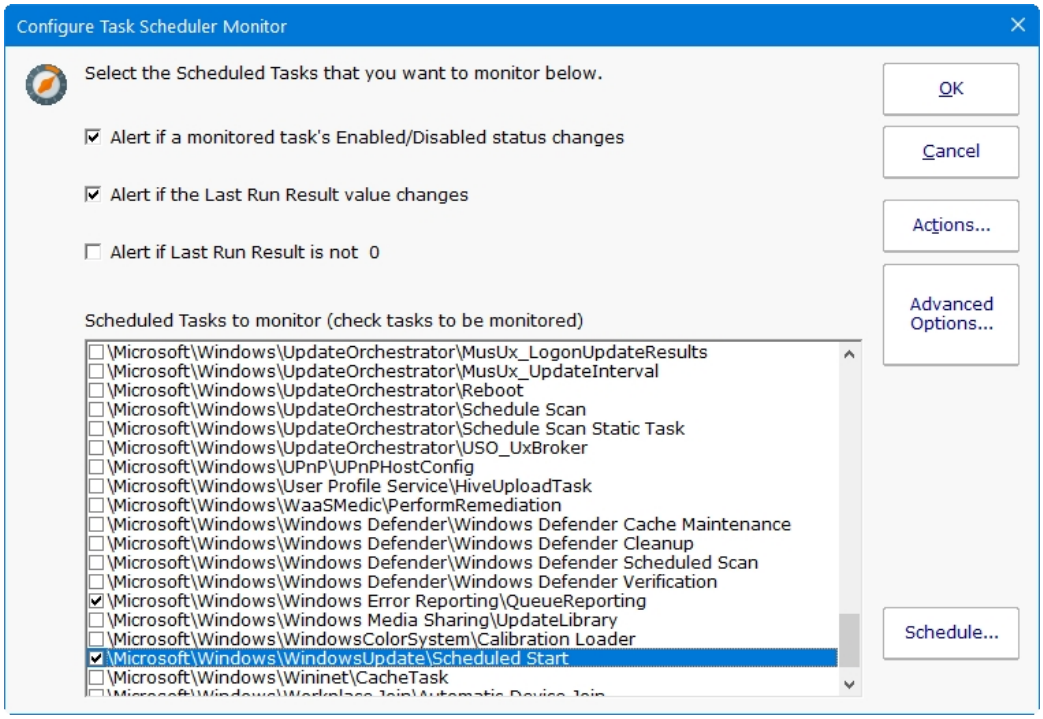
Besides live alerting on particular syslogs, you can also run reports to review syslogs that have been received and processed. You can filter on sending computer, severity, facility, and date range.



If you want to do your own processing or reporting on received syslog entries, they are stored in the SyslogEntries table (in the C:\Program Files\PA Server Monitor\Databases\SyslogMonitor.db file if using the embedded SQLite database).

Task Scheduler Monitor

The Task Scheduler Monitor works with the Windows Task Scheduler to alert you if any Scheduled Tasks fail, or change status.



This monitor is very easy to use. You can optionally have actions run when the following happen:

If a Scheduled Task's enabled status changes (from enabled to disabled, or from disabled to enabled)

If the Last Run Result changes. This is a useful option for Scheduled Tasks that typically don't return 0 after a run

If the Last Run Result is not 0. Most Scheduled Tasks return 0 after a successful run, so this could alert on failed runs

The alerting rules will be applied to the checked Scheduled Tasks. Many Scheduled Tasks are managed by the operating system or by 3rd party applications, so typically you would only monitor those which are specifically important to your business needs.

Standard Configuration Options

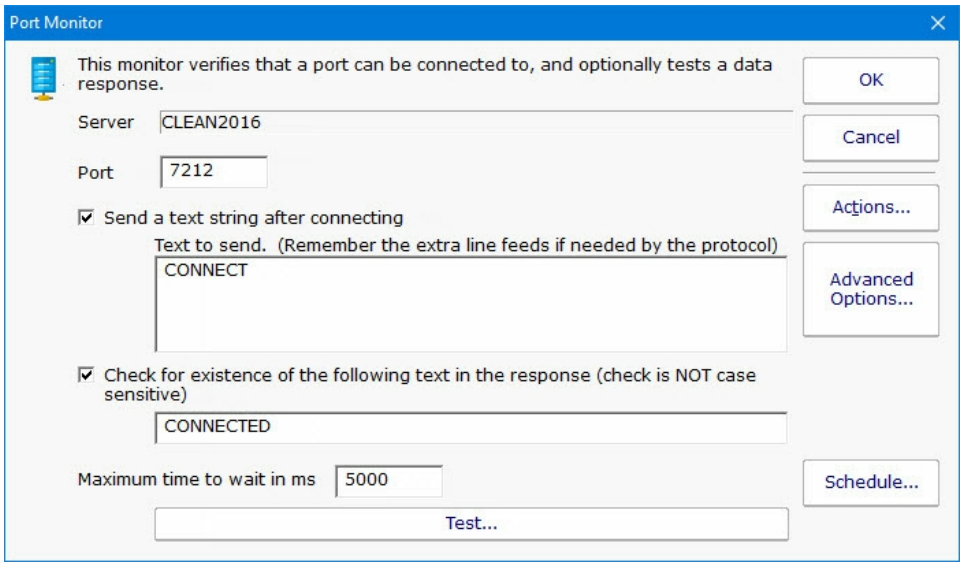
Like all monitors, this monitor has standard buttons on the right for Adding Actions, setting Advanced Options and setting the Monitor Schedule.

Supported Reports

The Task Scheduler Monitor will record the Last Run Result of the monitored tasks. A report can show the historical value of these Last Run Result values.

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).



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:

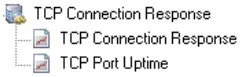
GET / HTTP/1.1<enter>
<enter>
<enter> (blank lines are important for this protocol!)

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



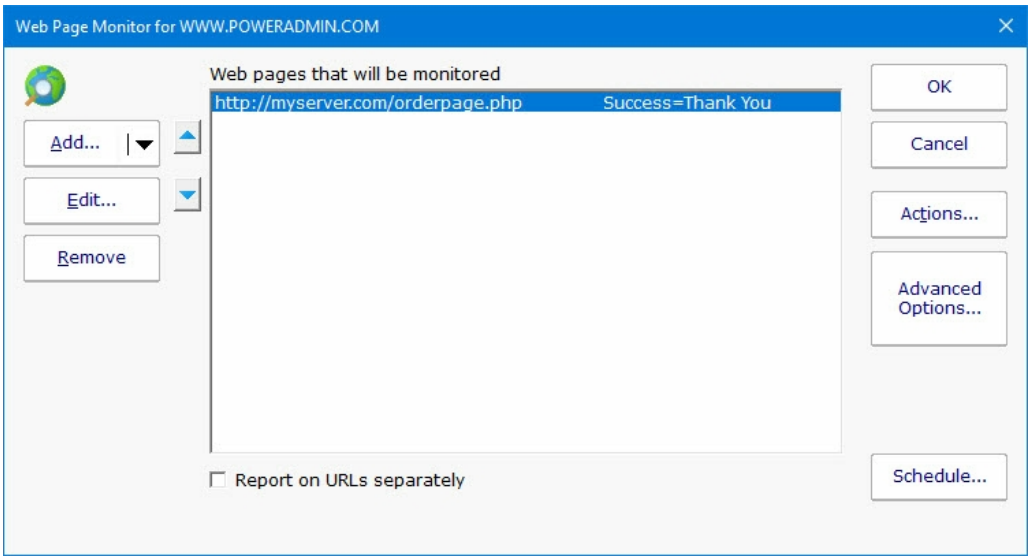
The TCP Port monitor can create reports based on the port response time from the target server/device. This data can be charted as well as output in .CSV or HTML tabular form. In addition, you can define what 'up' means and create an uptime report showing a percentage of uptime over a given time period.

Web Page Monitor

This is the most flexible and powerful Web Page monitor out there :)
The Web Page Monitor lets you define one or more web pages or web resources that should be checked. You can check return codes, data size, content on the page and/or changes in content size.

Data about load times are stored for charting and reporting.

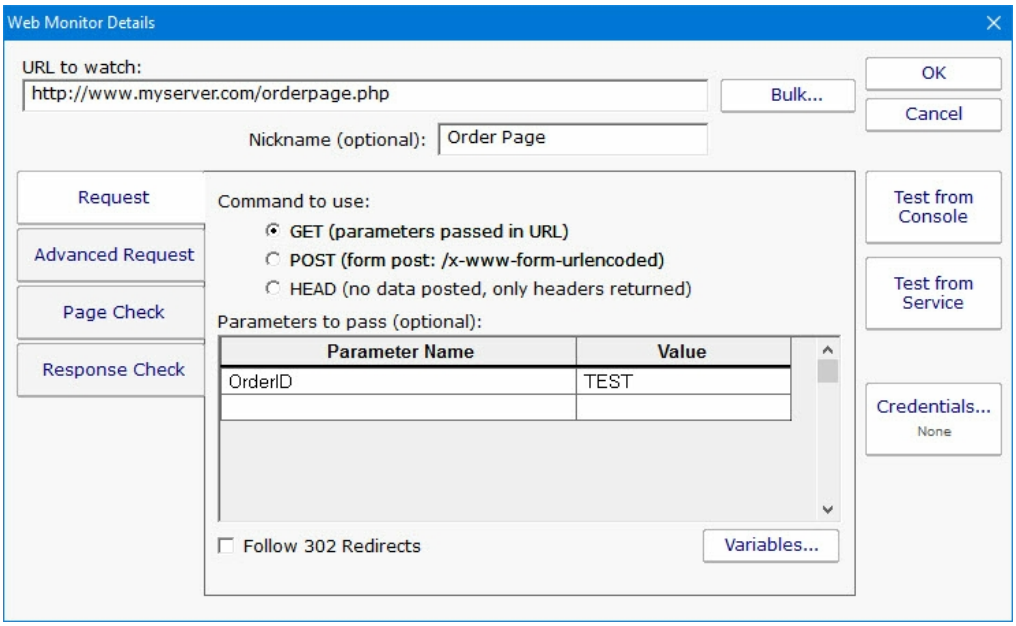
Watch the training video How to Monitor a Website.



One or more pages can be checked by each monitor. If any pages are not OK, the monitor will fire actions. You can also create multiple Web Page monitors to check different pages, or alert differently.

Individual Settings (Request Tab)

A number of parameters can be given to control what and how the web page is monitored. When you first create the monitor, you will see this first dialog.



URL to watch

The URL for the page is specified at the top. The protocol (http:// or https:// for example) should be included in the URL. Additional parameters can be passed in the URL if desired. For example:

```
http://www.myserver.com/pages/check.php?page=1&val=test
```

In addition, parameters can also be passed via the Parameters section below, which is especially useful if you want to POST data to a page.

Nickname (optional)

Reports will use the Nickname if available, otherwise the URL will be shown.

GET/POST/HEAD

Specify whether the URL should be called with an HTTP GET, POST or HEAD command. If fields and values are specified, they will be appended to the URL for a GET, or POSTed as a form post. If POST is used, the URL is not changed (even if you appended variables in the URL field at the top).

HEAD doesn't request the body of the page, so you can't check the content. However, it is a good light weight command for checking error codes, SSL certificate expiration, etc. And it usually doesn't count as a page hit if you don't want to affect page stats.

Parameters to pass

Here you can give field names and values for those fields. These values will be appended to the URL for a GET, or sent as a form post for a POST. The data will be UTF-8 encoded before sending.

Variables

Variables are values that are replaced when the monitor is run. They can appear in the parameter name or value, and also in the URL. For example:

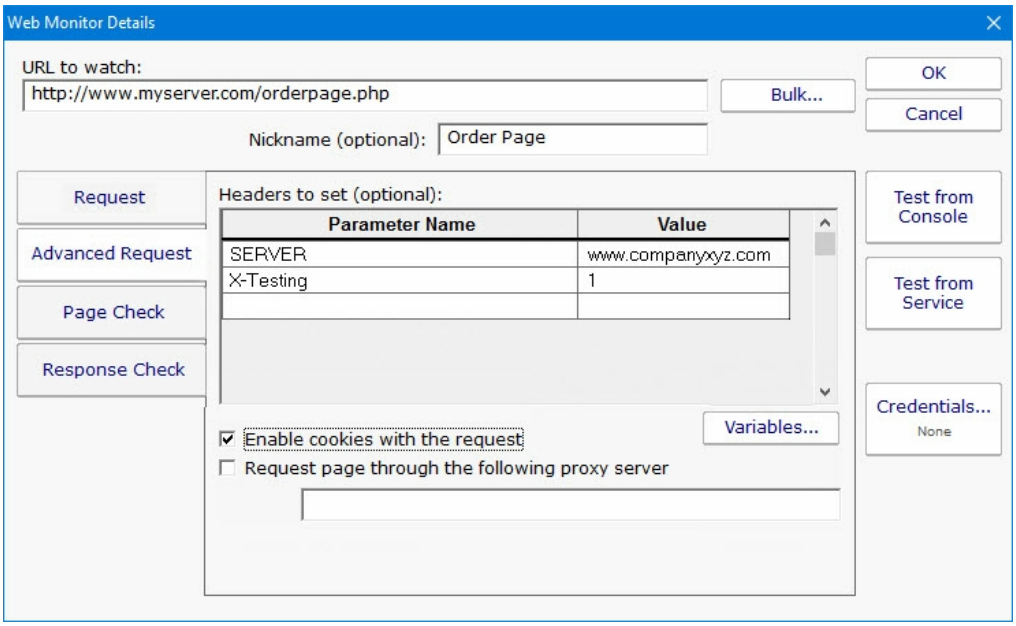
```
http://www.test.com/getpage.aspx?randomID=$CACHEBUSTER$
```

$CACHEBUSTER$ will be replaced when the HTTP request is made with a unique value each time the monitor runs.

Follow Redirects

If an HTTP redirect status code (301, 302, etc) is returned, it will be followed if this flag is checked. The followed page will then be checked for Success Text, Error Text, etc.

Advanced Request Tab



Headers

If you have a server that hosts many web sites, you probably need to set the SERVER header so the web server can differentiate which site to send the request to. Any headers can be added here, and they can use variables just like the GET/POST parameters can.

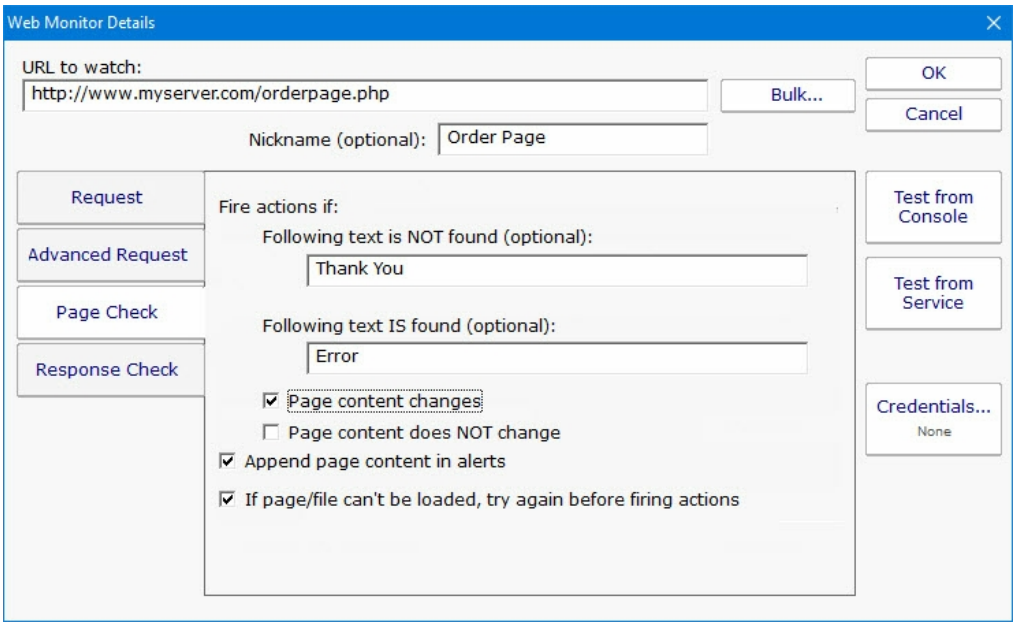
Enable Cookies

Cookies can be recorded and then used on subsequent requests if this is checked. This could be useful for pages that allocate new IDs (visitor IDs for example) or other values/resources for each new visitor.

Proxy Server

If the page must be retrieved through a specific proxy server, that proxy can be given in this field.

Page Check Tab (when to alert)



Success Text

If this value is given, the retrieved page will be searched. If the Success Text is not found, the monitor will fire alert actions.

Failure Text

If this value is given, the retrieved page is scanned. If this text is seen, the monitor fires alert actions.

Page Content Changes

If checked, the monitor will compare the retrieved page to the previously retrieved page and look for differences. If a difference is found, the monitor will fire alerts.

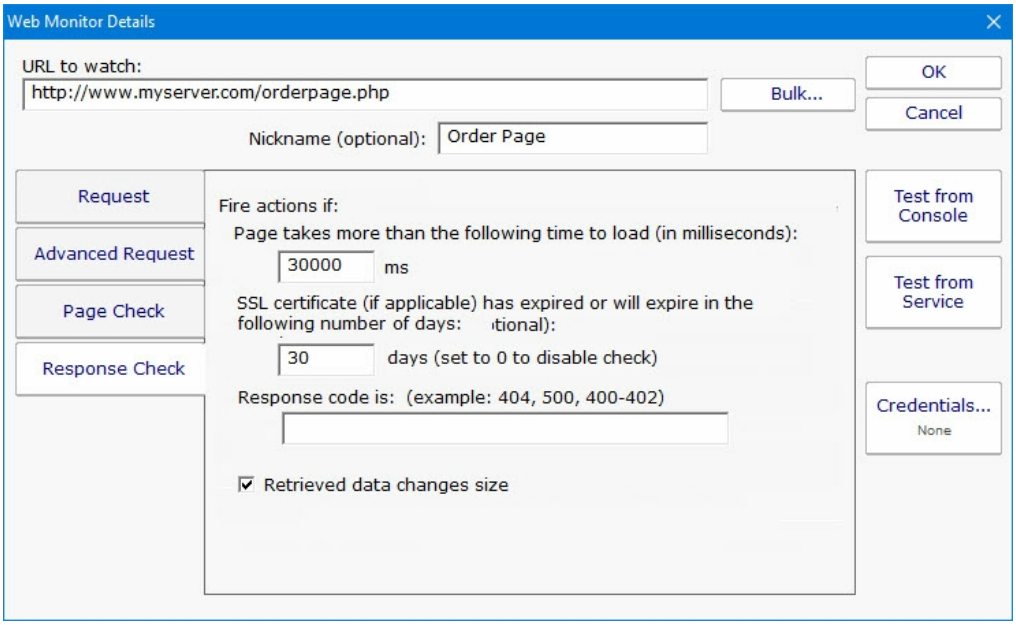
Append Page Content

If alert actions are fired, this check box indicates the retrieved page HTML should be appended to the alert. This often helps when troubleshooting a problem.

Try Again

If the page fails to load, or the target values can't be found, the monitor can make an additional try to load the page and will check again when this value is checked.

Response Check (when to alert)



Page Load ms

The page load time is compared against this value. If load time is greater than this value, alerts are fired.

SSL Certificate Expiration

If you check an HTTPS URL, the certificate's expiration date will be checked. If it will expire within the specified number of days, an alert is fired. You can set this value to 0 to ignore certificate expiration errors. If HTTPS is not used (ie, just HTTP), then this setting is ignored.

Response Code

The HTTP Response Code will be checked, and if it matches the value given, alerts will be fired. This is a good way to check a non-text resource, such as verifying a particular graphic or download file is accessible. This can be used with the HEAD request type to avoid actually downloading the target object.

Data Size Changes

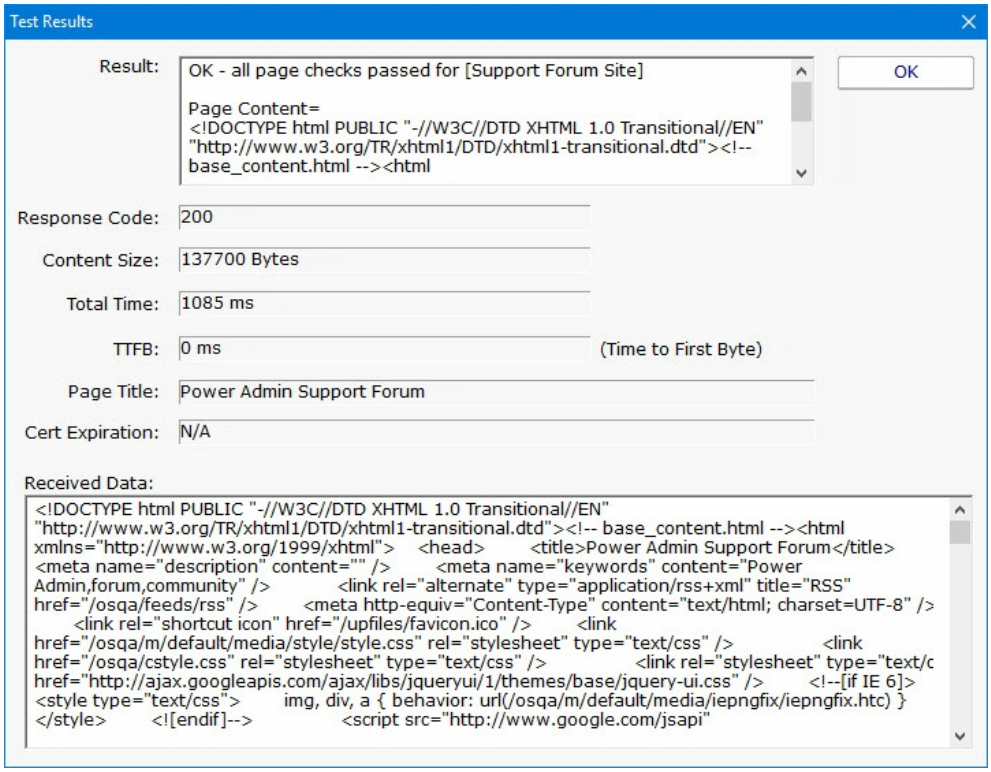
Alert if the size of the requested page/item changes. This works with the HEAD command so you can verify that a target file is available and the correct size.

Testing

There are two test buttons. "Test from Console" will make the web page request from the Console that you are using. "Test from Service" will send the URL and parameters to the Central Monitoring Service (which may or may not be on the same computer as the Console) and make the request from there. This tests the page request in a production setting.

If you are using the Data Size Changes or Page Content Changes settings, the page will be requested twice, with approximately a 5 second pause between requests, and then the two requests will be compared. During production runs, the size and content will be retrieved and compared to the values saved during the previous monitor run.

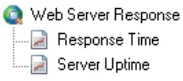
After running the test, you will see something similar to this:



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.

Action Lists

Action Lists are useful for creating a standard notification pattern for monitors. Possible ideas for actions lists:

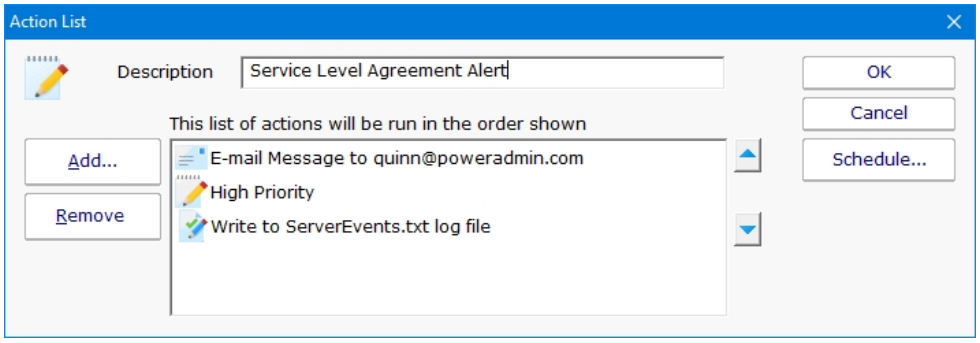
During hours, and after hours notification lists

On-call notification list (easily add or remove someone from one list rather than from many individual monitors)

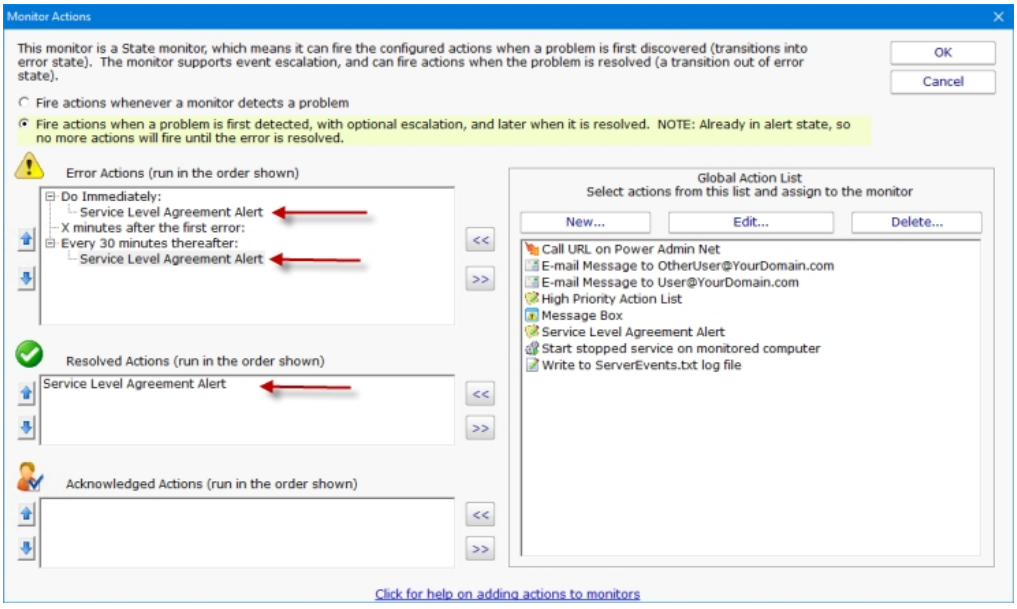
Procedures to run for high priority problems

Standard procedures for specific problems (IIS being down for example)

Action Lists are normal system actions that can be added to any monitor. The only configuration needed is to add the actions that will be called by this action when it is called.

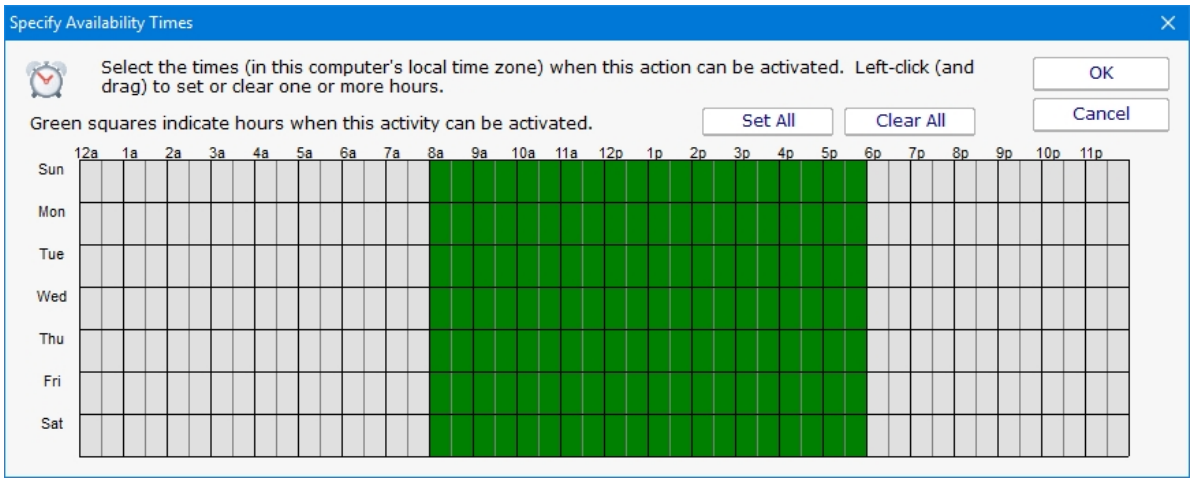


For an example monitor below, the action list shown above is assigned to this monitor and many others like it. When any of these monitors detects a problem, they will run all of the actions defined in the "Service Level Agreement Alert" action list.



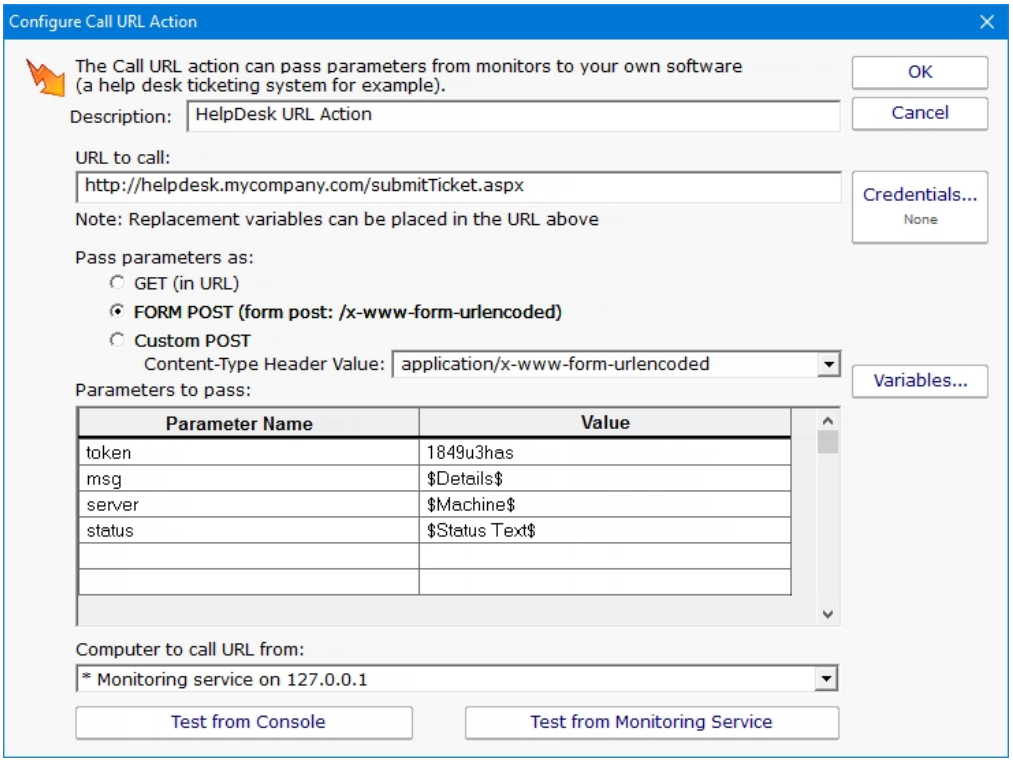
Scheduling

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


Specify Availability Times
Select the times (in this computer's local time zone) when this action can be activated. Left-click (and drag) to set or clear one or more hours.
OK
Cancel
Green squares indicate hours when this activity can be activated.
Set All
Clear All
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

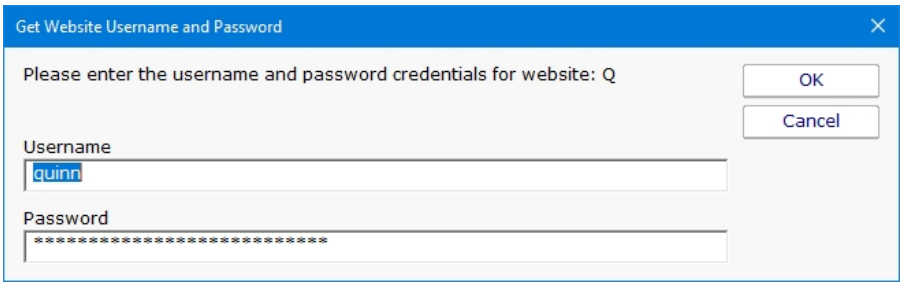
Call URL Action

This action will call a URL that you specify, possibly passing additional information about the alert via GET or POST variables.



Specify the URL to call, and whether it should be called with GET (with parameters added to the URL), or with POST (with parameters being form posted).

Specify any additional parameters that you want added in the field list below. The Parameter Name should be something the web page is looking for, and the parameter value can be whatever value you want. Click the Variables button to see a list of replacement variables that can be used for passing information about the alert to the web page.

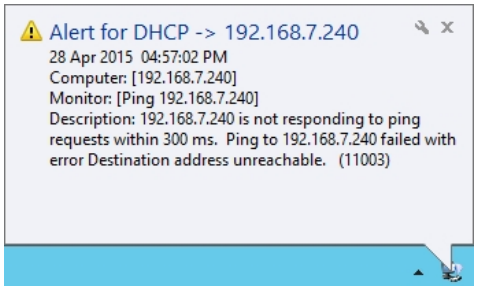


Click on the Credentials button to enter the username and password credentials for the website.

When you press one of the Test buttons, the appropriate HTTP request is built (with parameters appended to the URL, or built into a form post) and sent to the web page. One caution for the GET setting -- most web servers have a limit on the amount of data that can be sent via a GET request. A 2KB limit is not uncommon.

Desktop Notifier Action

The Desktop Notifier Action is small application that runs in the Windows task bar. It connects to your central server and listens for notifications to display.



Installation

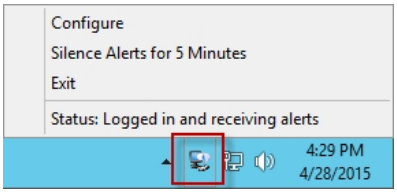
To install the Desktop Notifier to a computer, copy all of the files from the folder below to your target computer:

```
C:\Program Files\PA Server Monitor\DesktopNotifier
```

Once copied, run PADesktopNotifier.exe by double-clicking on it.

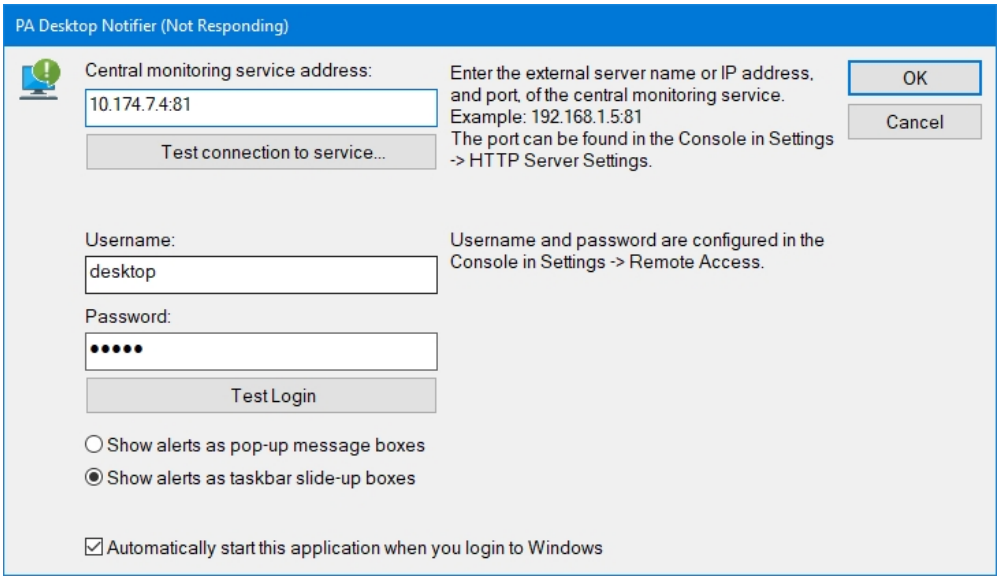
Configuration

The very first time the PA Desktop Notifier is run, the configuration dialog will be shown below. It is also shown if you right-click the application icon in the task bar and choose Configure.



Specify the Central Monitoring Server's hostname/IP address and the port it uses for HTTPS communication. This can be determined by looking in the Console at the HTTP Settings.

A username and password also need to be specified. This is the same username and password a user might use to login to the web-based reports or a remote Console. Click to see more information on managing user accounts.



The settings entered will be saved in:

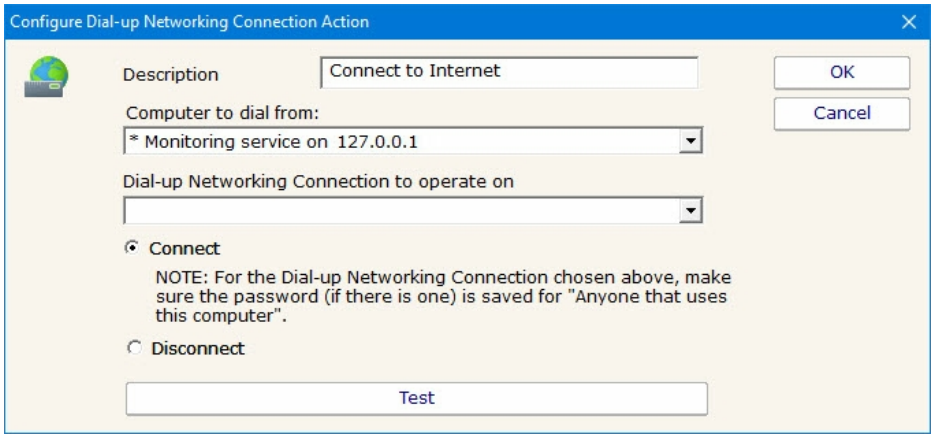
```
C:\Users\{user account}\AppData\Roaming\PADesktopNotifier.ini
```

The username and password are encrypted using the recommended Windows encryption functions. This file can be deleted if you want to reset the configuration.

Once the user has logged in, a new Desktop Notification action will appear in the Console application and can be assigned to monitors just like any other action.

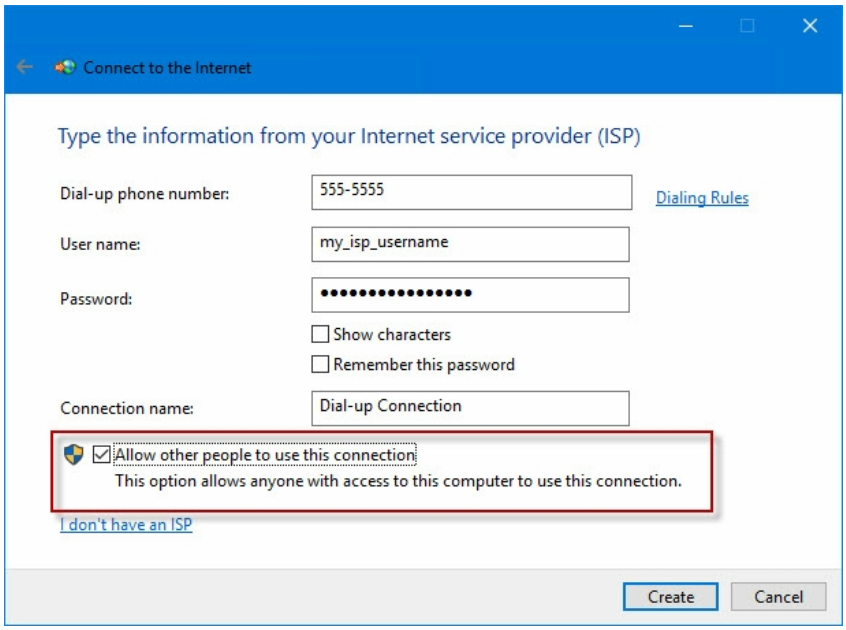
Dial-up Connection Action

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



Previous to configuring this action, you need to manually 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.

Also note that this action can dial a Dial-up Networking Connection that is created on the Central Monitoring Service, or on a remote Satellite. Naturally the Dial-up Network Connection must be created at the location that you want to dial it.



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.

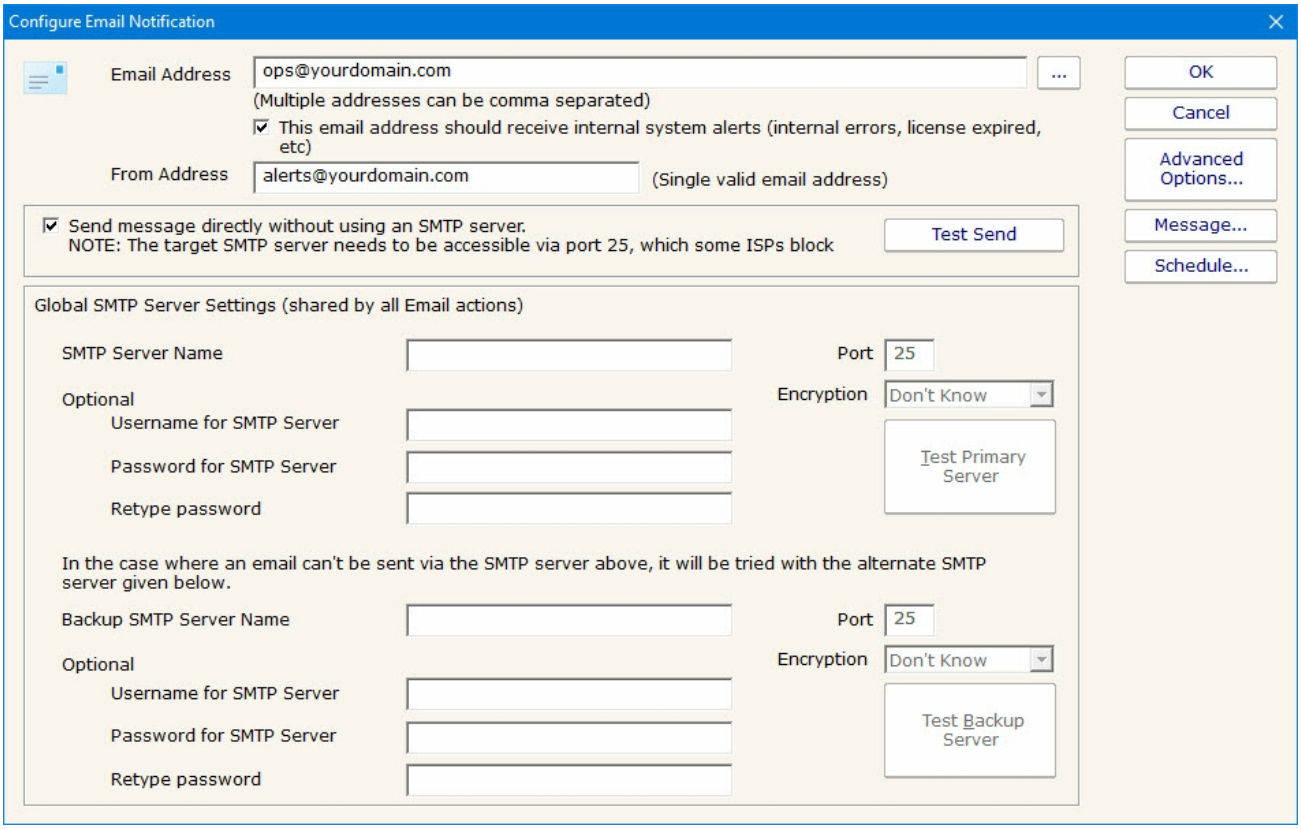
E-mail Message Action

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 your cell/pager provider has an SMTP gateway (most providers do). There are some hints about that in the SMS FAQ.

To configure this action, give the target SMTP email address. You can add multiple email addresses (comma separate them) for sending alerts to the same addresses, and/or create multiple E-mail Message Actions and attaching them to different monitors for more customized alerting.

E-mail alerts are always sent from the Central Monitoring Service. In the case where a monitor running on a remote Satellite detects an issue and runs an attached E-mail Message Action, the alert message will be sent to the Central Monitoring Service for ultimate delivery.

There are two ways to send a message: Direct, or via a standard SMTP server.



Direct Send

PA Server Monitor can act like a simple SMTP server and send messages directly to the recipient's receiving SMTP server. That means a connection to the destination server via port 25 needs to be possible (sometimes Internet Service Providers block outgoing port 25 to help limit spam, but if PA Server Monitor is on the same network as your mail server, it will probably work). The other requirement is that an MX DSN lookup returns a name for the target mail server that is resolvable from the machine hosting PA Server Monitor.

The easiest way to determine if all the above requirements are met is to just try it. Click the "Send message directly..." checkbox and then press the "Test Send" button. If the message is successfully sent, the configuration is complete. If it is not sent, uncheck the

checkbox and continue to configure the SMTP server settings.

Send via SMTP Server

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 via the primary fails. Unless using Direct Send, a primary SMTP server must be specified; the backup is optional.

The settings for each SMTP server (primary and secondary) can be validated by the program. You can do this by pressing the "Test Primary Server" and "Test Backup Server" buttons respectively. This test sends a short email message as a test to the email address(es) that were entered in the "Email address" field at the top of the form. If sending the email succeeds and you successfully receive the message, then the SMTP server settings that you have entered are correct. If the message is not received but you are sure the settings are correct, see the Troubleshooting Missing Email Alerts FAQ for help.

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.

Exchange

For sending via a Microsoft Exchange server, check the Exchange configuration to ensure SMTP relaying is allowed from the Central Monitoring Service computer.

Office365

For sending email with Office365 with "modern authentication" (OAuth 2.0) please see this help document.

GMail

To send alerts using a GMail account a security setting change is needed.
How To Enable Gmail Access

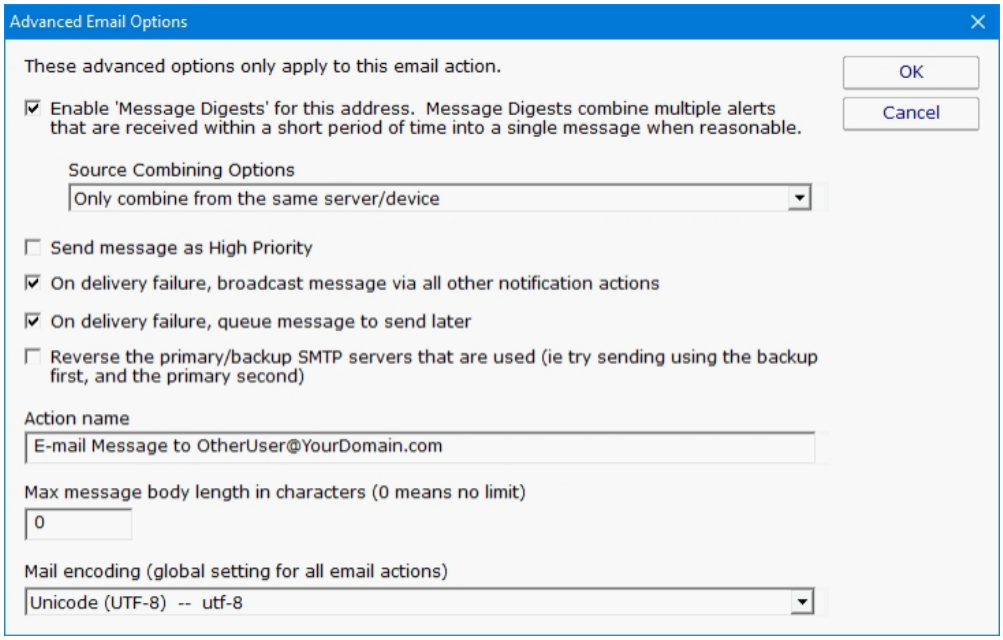
Troubleshooting

If email alerts are not showing up as expected, check out the Troubleshooting Missing Email Alerts FAQ for help.

Additional Configuration Options

Advanced Options

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.



Messages Digests - To reduce possible message overload, you can specify that multiple messages 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.

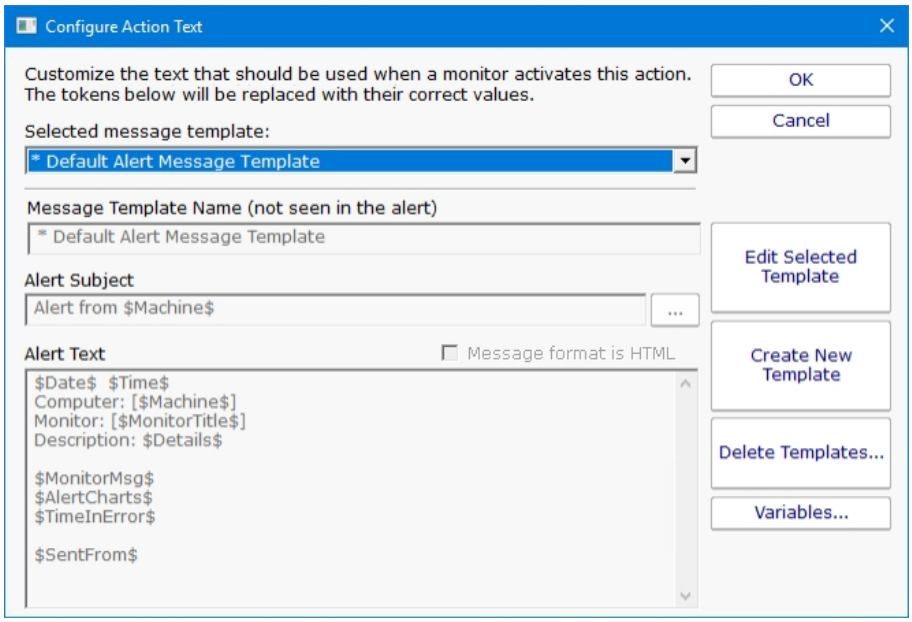
Queue for Later - If a message can't be sent (perhaps because there is no connection to the server), you can specify that the message be queued for later delivery. Periodically PA Server Monitor will try to send any messages that are in the queue.

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.

If the message will be going to a device with limited capabilities (perhaps a pager via SMS for example), you can specify that only the first 200 characters (for example) get sent.

Message Template

Pressing the Message button displays the configuration dialog below. This lets you customize message text, select different templates to use, and to create new templates. 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. Also, having the abillity to use different message templates will help you get the right information to the right groups.



Select message template dropdown - Allows the option to use different message templates for individual actions that use message templating.

Edit Selected Template - Select and then edit the message template that you wish to change.

Create New Template - Create a new template by supplying the new template with a template name, alert subject, and alert text.

Delete Templates - Delete templates that are no longer needed. Select the Delete Template button and then select the templates that you wish to delete.

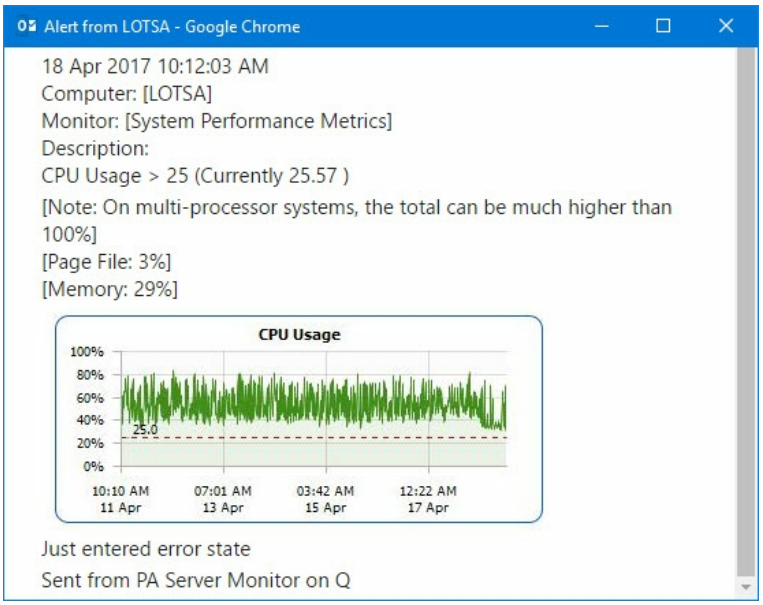
Variables - Using replacement variables allow you to insert details into your message templates.

You can also specify specify that the message is HTML, and enter an HTML message template. Enclose the template in an <html> tag. Don't bother with a <head> tag as most email clients will strip it out.

Some good hints and tips about HTML email are available here:
http://www.mailchimp.com/resources/guides/email-marketing-field-guide/

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.

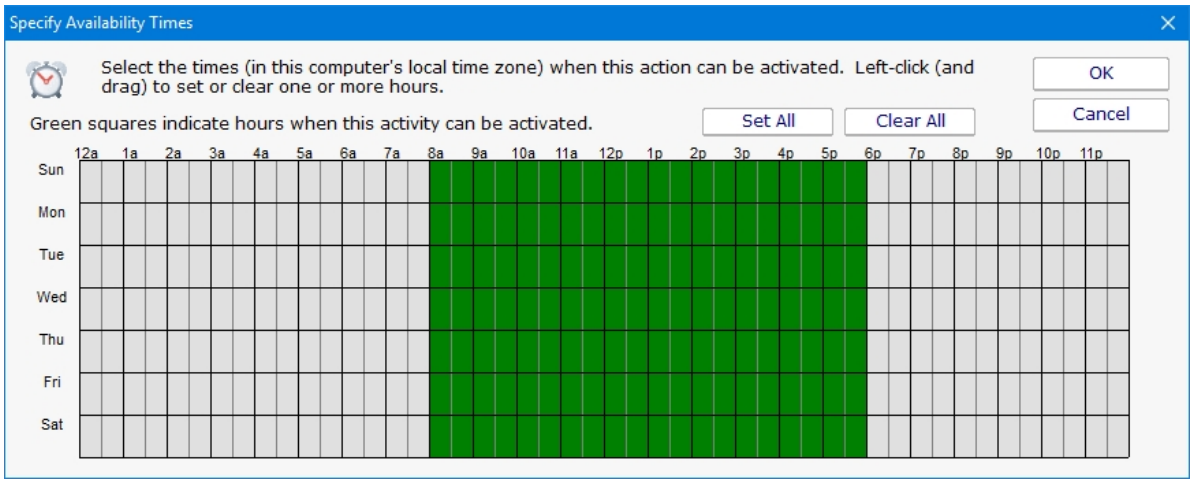
A typical alert email could look something like this:



Note: Actual message content will vary depending on the product being used, and the monitor which fires the actions.

Scheduling

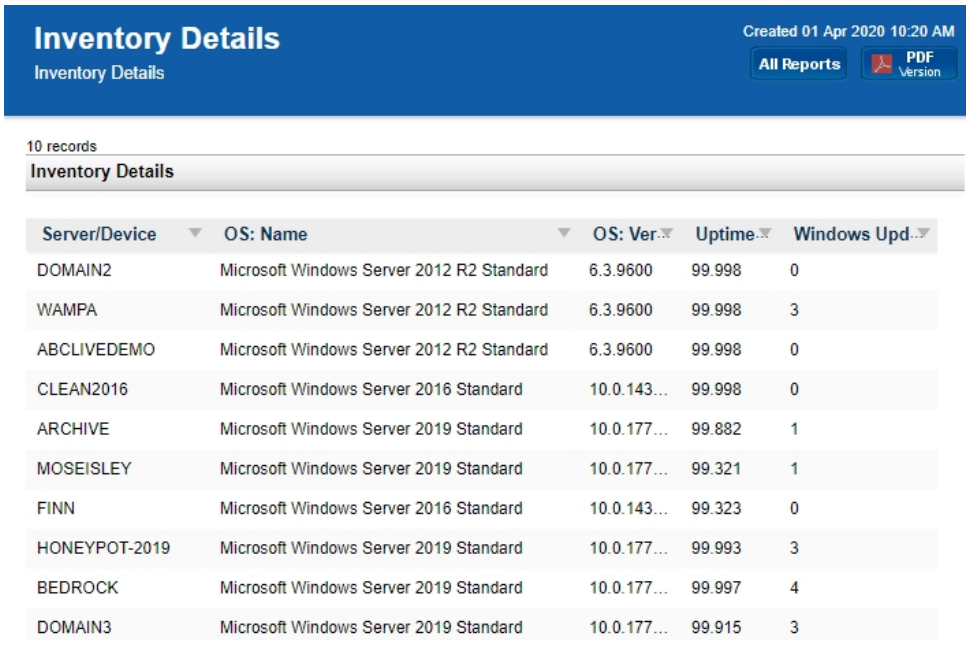
If the action should not be used 24/7 you can use the Schedule button to specify when notifications should be sent to the given pager. On off hours the action acts as though it isn't configured at all. The dark green below indicates 'on hours' and the lighter grey specifies 'off hours'.



Advanced: Scripting Options

Scripting the Recipients

The Email Action can determine who to send the email to on the fly by calling a script. To access that feature, click the ... button next to the Email Address field.



Inventory Details

Inventory Details

Created 01 Apr 2020 10:20 AM

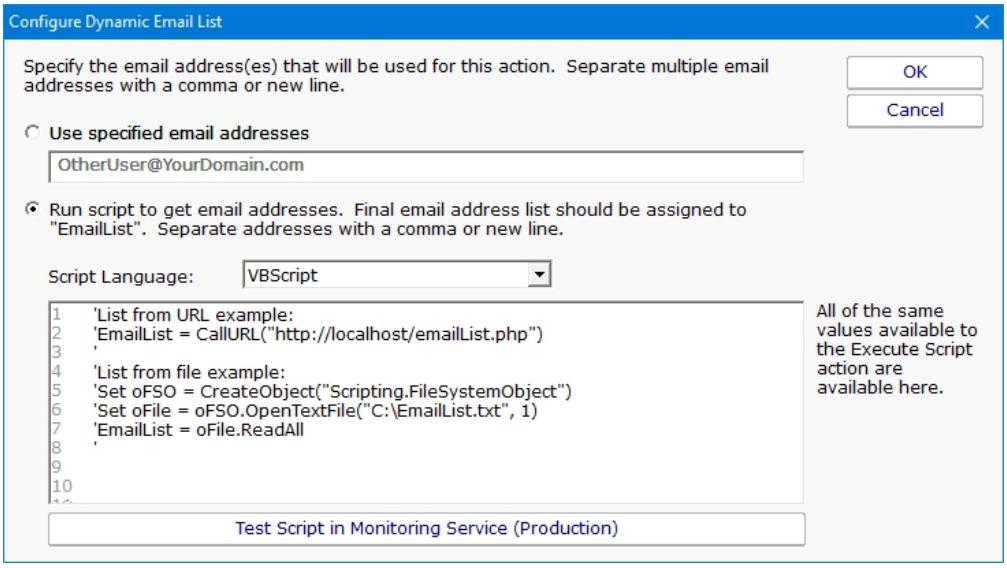
All Reports | PDF Version

10 records

Inventory Details

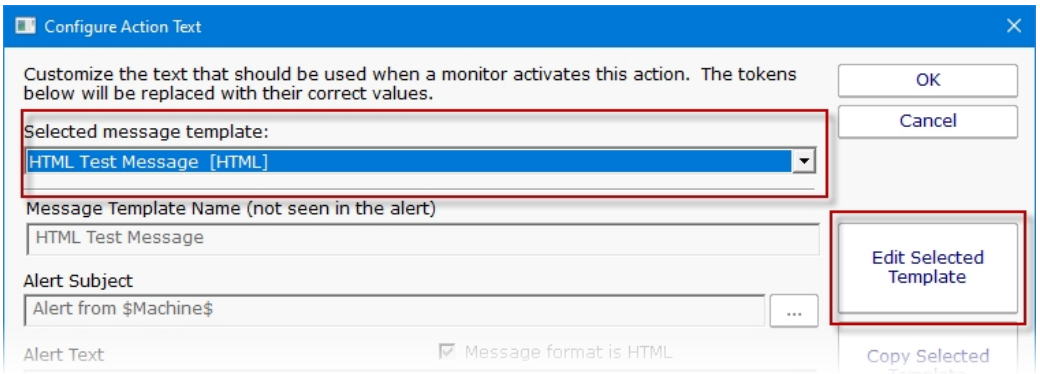
Server/Device	OS: Name	OS: Ver	Uptime	Windows Upd
DOMAIN2	Microsoft Windows Server 2012 R2 Standard	6.3.9600	99.998	0
WAMPA	Microsoft Windows Server 2012 R2 Standard	6.3.9600	99.998	3
ABCLIVEDEMO	Microsoft Windows Server 2012 R2 Standard	6.3.9600	99.998	0
CLEAN2016	Microsoft Windows Server 2016 Standard	10.0.143...	99.998	0
ARCHIVE	Microsoft Windows Server 2019 Standard	10.0.177...	99.882	1
MOSEISLEY	Microsoft Windows Server 2019 Standard	10.0.177...	99.321	1
FINN	Microsoft Windows Server 2016 Standard	10.0.143...	99.323	0
HONEYPOT-2019	Microsoft Windows Server 2019 Standard	10.0.177...	99.993	3
BEDROCK	Microsoft Windows Server 2019 Standard	10.0.177...	99.997	4
DOMAIN3	Microsoft Windows Server 2019 Standard	10.0.177...	99.915	3

Here you can specify a script that will run. The results of the script must be assigned to the variable EmailList, and should consist of a simple text string of one or more email addresses. Each email address should be on a separate line, or on the same line and separated by commas. The script can do anything you want to get the email list, like reading from a database, from a URL or from a text file. If the script determines that the email should not be sent, set the EmailList variable to the string "NO_SEND".

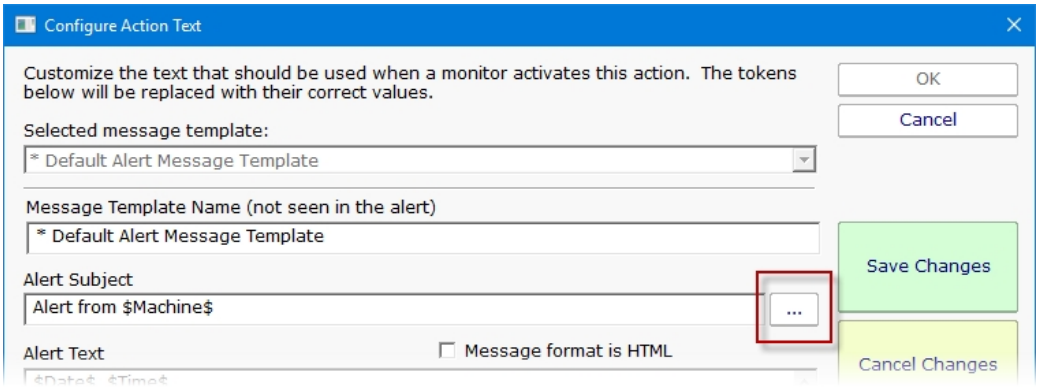


Overriding the Subject or Body via Script

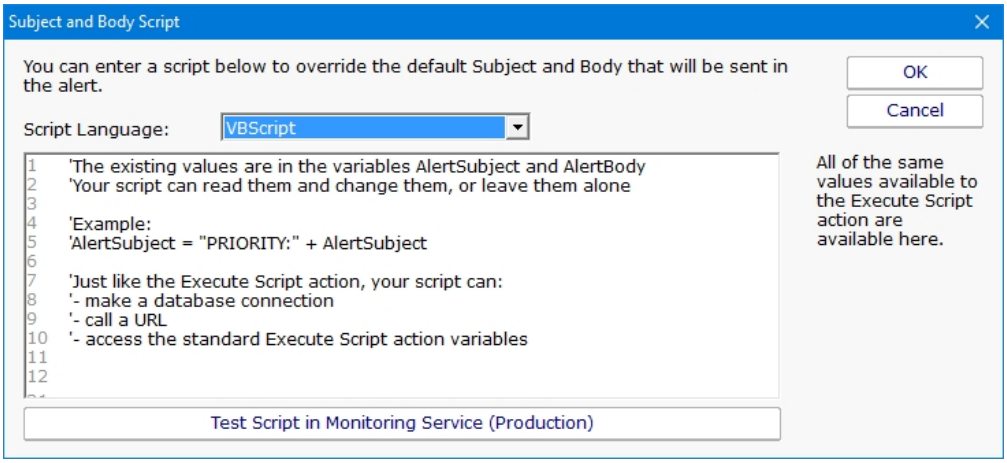
The Subject or Body of an email message can be changed on-the-fly as an alert email is going out. First select the templet to edit from the dropdown and then click on the Edit Selected Template button.



Then to access this script click the ... button on the Message dialog.



This script has access to all of the same values and functions as the Execute Script action has. Assign the final output to the variables Body and/or Subject. The variables are initialized with the current value to be used. You can change the value, replace it, or leave it alone.



Execute Script Action

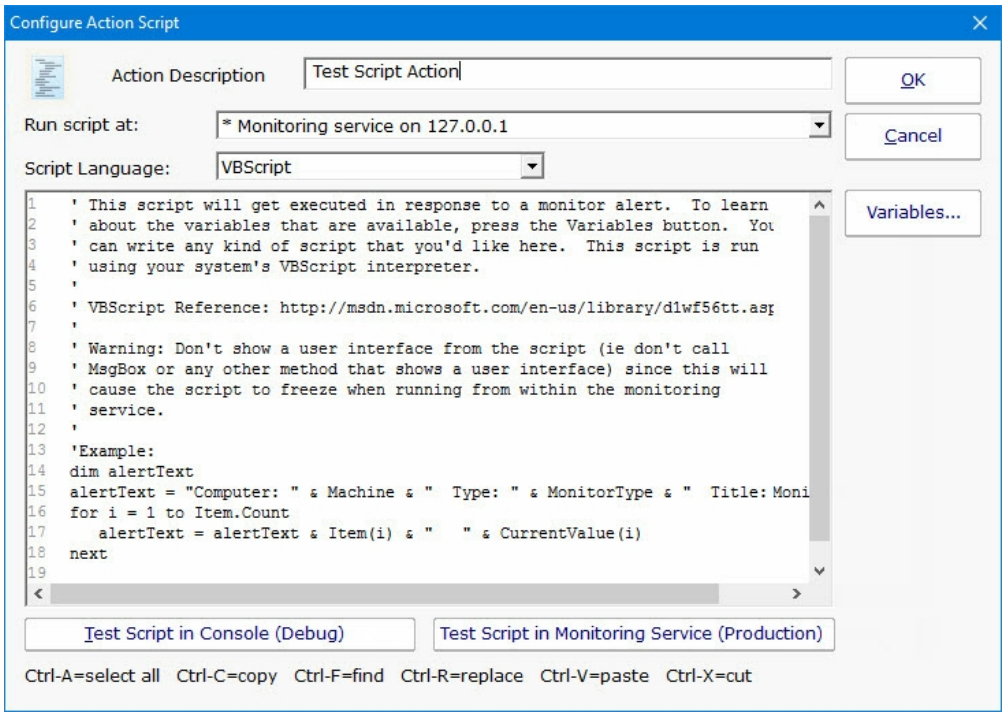
The Execute Script Action allows you to receive action parameters that were sent from a monitor and handle them in your own specific way.

The script is run using the computer's built-in VBScript, JavaScript or Powershell interpreter. This means you can make use of the full scripting language as well as any installed 3rd party components that are installed on the system.

Near the top of the action dialog is a "Run script at" selection box. Here you can specify where the script should be run if you have Satellite monitoring services. The default is to run the script on the Central Monitoring Service.

The next control simply allows you to select the language for your script. If the script window is empty or still showing the default script, changing the current language will show a new default script in the language you speciy.

The script window is where you enter your script. The script can do anything that can be done in the select language (including creating external components) with all the standard restrictions. A good VBScript reference is available at: http://msdn.microsoft.com/en-us/library/d1wf56tt.aspx



There are two Test buttons. One will run the script within the Console. The other will send the script to the monitoring service that is monitoring the target computer (Central Monitoring Service or a Satellite) and run the script there. This helps find any problems that might come up from the script possibly running on a different machine, or running as a different user (the service Log As user).

Keep in mind that when the script runs, it might run on a different computer than where you are editing it. That means drive mappings, HKEY_CURRENT_USER registry hive, Internet Explorer settings and the currently running user will often be different.

IMPORTANT: Do not show any user interface elements in the script -- they will not be visible in the monitoring service and will block the script from ever completing.

Topics

Example scripts

VBScript

JavaScript

PowerShell

SSH

Additional Script Elements

Besides the scripting language's own objects and elements, the following additional global variables and methods are available within each scripting environment:

VBScript

AlertType

This value indicates if the script is running because of an alert condition, a fixed condition, because an error was acknowledged, or for a reminder of a still open error.
Possible values are:
1 = Alert
2 = Fixed
3 = Acknowledged
4 = Reminder

Example:

```
if AlertType = 1 Then {do something ... }
```

CurrentValue

This is an array of string values, representing the current value (if any) for the item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = CurrentValue(1)
```

CustomProp

This function retrieves the named value of a custom property. It checks the Monitor first, and if not found, checks the monitor's owning computer, and then the computer's group, and then the group's parent group, etc. Custom properties can be set on Groups, Computers and Monitors by right-clicking on the item and choosing the Custom Properties menu.

Example:

```
myStr = CustomProp("NotifyGroupID")
```

.

Details

This is a string value. This value is the content of the action being fired. It is sent from the monitor and typically contains information about the alert.

Example:

```
myStr = Details
```

Description

This is an array of string values, representing a description of this particular item's status. The Details value (above) is usually all of the Description values appended together.

Example:

```
myStr = Description(1)
```

Extra1

This is an array of string values, representing extra information that may be available from a particular monitor. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = Extra1(1)
```

Extra2

This is an array of string values, representing extra information that may be available from a particular monitor. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = Extra2(1)
```

Group

The name of the group that the computer the monitor is attached to belongs in.

Example:

```
myStr = Group
```

GroupPath

The name of the group that the computer the monitor is attached to belongs in, with child groups delimited with a > (ie, Servers/Devices > Austin > Lab)

Example:

```
myStr = GroupPath
```

InventoryValue

Request an inventory value for the current computer, or a different one. An inventory propertyID must be used to specify which inventory value to retrieve. An optional ComputerID value can be used to get the inventory value from a computer other than the current computer. If a property can have multiple values (CPU Names for example), each one will have a newline character appended.

Example:

```
'returns the Operating System (18) for the current computer myStr = InventoryValue(18)
'returns the Operating System (18) for the current computer (0 means use default) myStr =
InventoryValue(18, 0)
'returns the Operating System (18) for computerID 238 myStr = InventoryValue(18, 238)
```

The inventoryID values are given below. Note that not all computers/devices will have all inventory values, and some may have none (especially if an Inventory Collector monitor is not added to the computer).

Anti-virus Version	38
Anti-virus Pattern File	39
Anti-virus Pattern File Date	40
Anti-virus Status	41
Operating System	18
OS Architecture	19
OS Version	20
OS Last Boot Time (_time_t UTC value)	21
OS Current Time (_time_t UTC value)	22
CPU Count	13
CPU Name (multi value)	15
CPU Number of Cores (multi value)	16
CPU Clock Speed (multi value)	17
Display Name	6
Drive Status (multi value)	23
Domain	9
Manufacturer	10
Page File size in MB	24
RAM in MB	14
System Architecture	12
System Model	11
Time Zone Offset	8
Uptime % this month	28
Uptime % last month	29

Item

This is an array of string values, representing the item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = Item(1)
```

ItemType

This is an array of string values, representing the type of item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = ItemType(1)
```

LimitValue

This is an array of string values, representing the limit/threshold (if any) for the item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = LimitValue(1)
```

Machine

This read-only string variable is the name of the computer that caused the script action to fire.

Example:

```
myStr = Machine
```

MachineAlias

This read-only string variable is the aliased name of the computer that caused the script action to fire.

Example:

```
myStr = MachineAlias
```

MachineIP

IP address text string of the computer that the firing monitor is attached to

Example:

```
myStr = MachineIP
```

MachineID

Returns the numeric value that uniquely identifies this computer (Computer ID - CID) within the application. Useful in conjunction with the External API.

Example:

```
myID = MachineID
```

MonitorTitle

This read-only string variable is the title of monitor that caused this script action to fire.

Example:

```
myStr = MonitorTitle
```

MonitorType

This read-only string variable is the type of monitor that caused this script action to fire.

Example:

```
myStr = MonitorType
```

RunAction

This method allows you to run other actions from within the script. The method takes an action ID to specify which action to run. Action IDs can be viewed in the Console by enabling the View > Show Object IDs in Navigation Tree menu item.

Example:

```
RunAction 12
```

SecondsInError

Number of seconds that the monitor has been in error.

Example:

```
inErrSeconds = SecondsInError
```

State

An array of string values that contain the OK or PROBLEM state for each item being reported on. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = State(1)
```

SendMail

This method sends an email message to the recipient that you choose. This would be useful for sending the incoming Details variable to a different email recipient based on some external factors (such as who is currently carrying the pager)

Example:

```
SendMail "to_address@host.com", "from_address@host.com", "Subject of message", "Body of email
```

```
message"
```

SetComputerCustomPropByID

Custom Properties can be used in directory paths, email messages, scripts and other places. Your script can set a Custom Property on a computer by specifying its ID (first parameter), or use 0 to indicate the computer that the action is running for should be targeted.

Example:

```
SetComputerCustomPropByID(0, "DEVICEID", "BSQL")
```

The Custom Property DISPLAYED_NOTES is the value you can set by right-clicking a computer and selecting Notes. Notes show up at the top of a Server Status Report.

Sleep

This method takes a single integer value, which is the number of milliseconds that the script should stop and sleep. Be careful about using this -- causing too many actions to sleep for very long means other actions may get delayed

Example:

```
Sleep 1500
```

Status

A read-only string indicating the current status of the monitor. To see all possible values, See Row Variables from the "Variables..." button for the action.

Example:

```
myStat = Status
```

StatusText

A read-only string indicating the current status of the monitor. This is a more human-friendly value than Status. To see all possible values, See Row Variables from the "Variables..." button for the action.

Example:

```
myStat = Status
```

TimeInErrorStr

A text string of how long the monitor has been in error

Example:

```
myStr = TimeInErrorStr
```

ToLog

This method takes a string value and appends it to the service's log file (useful for debugging scripts). The line will start with ACTION_SCRIPT_LOG.

Example:

```
ToLog "Arrived at first loop"
ToLog resultVal
```

JavaScript

AlertType

This value indicates if the script is running because of an alert condition, a fixed condition, because an error was acknowledged, or for a reminder of a still open error.
Possible values are:
1 = Alert
2 = Fixed
3 = Acknowledged
4 = Reminder

Example:

```
if(AlertType == 1) {do something ... }
```

CurrentValue

This is an array of string values, representing the current value (if any) for the item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = CurrentValue(1);
```

CustomProp

This function retrieves the named value of a custom property. It checks the Monitor first, and if not found, checks the monitor's owning computer, and then the computer's group, and then the group's parent group, etc. Custom properties can be set on Groups, Computers and Monitors by right-clicking on the item and choosing the Custom Properties menu.

Example:

```
myStr = CustomProp("NotifyGroupID");
```

Details

This is a string value. This value is the content of the action being fired. It is sent from the monitor and typically contains information about the alert.

Example:

```
myStr = Details;
```

Extra1

This is an array of string values, representing extra information that may be available from a particular monitor. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = Extra1(1);
```

Extra2

This is an array of string values, representing extra information that may be available from a particular monitor. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = Extra2(1);
```

Group

The name of the group that the computer the monitor is attached to belongs in.

Example:

```
myStr = Group;
```

GroupPath

The name of the group that the computer the monitor is attached to belongs in, with child groups delimited with a > (ie, Servers/Devices > Austin > Lab)

Example:

```
myStr = GroupPath;
```

InventoryValue

Request an inventory value for the current computer, or a different one. An inventory propertyID must be used to specify which inventory value to retrieve. An optional ComputerID value can be used to get the inventory value from a computer other than the current computer. If a property can have multiple values (CPU Names for example), each one will have a newline character appended.

Example:

```
//returns the Operating System (18) for the current computer myStr = InventoryValue(18);
//returns the Operating System (18) for the current computer (0 means use default) myStr =
InventoryValue(18, 0);
//returns the Operating System (18) for computerID 238 myStr = InventoryValue(18, 238);
```

The inventoryID values are given below. Note that not all computers/devices will have all inventory values, and some may have none (especially if an Inventory Collector monitor is not added to the computer).

Anti-virus Version	38
Anti-virus Pattern File	39
Anti-virus Pattern File Date	40
Anti-virus Status	41
Operating System	18
OS Architecture	19
OS Version	20
OS Last Boot Time (_time_t UTC value)	21
OS Current Time (_time_t UTC value)	22
CPU Count	13
CPU Name (multi value)	15
CPU Number of Cores (multi value)	16
CPU Clock Speed (multi value)	17
Display Name	6
Drive Status (multi value)	23
Domain	9
Manufacturer	10
Page File size in MB	24
RAM in MB	14
System Architecture	12
System Model	11
Time Zone Offset	8
Uptime % this month	28
Uptime % last month	29

Item

This is an array of string values, representing the item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = Item(1);
```

ItemType

This is an array of string values, representing the type of item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = ItemType(1);
```

LimitValue

This is an array of string values, representing the limit/threshold (if any) for the item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = LimitValue(1);
```

Machine

This read-only string variable is the name of the computer that caused the script action to fire.

Example:

```
myStr = Machine;
```

MachineAlias

This read-only string variable is the aliased name of the computer that caused the script action to fire.

Example:

```
myStr = MachineAlias;
```

MachineIP

IP address text string of the computer that the firing monitor is attached to

Example:

```
myStr = MachineIP;
```

MachineID

Returns the numeric value that uniquely identifies this computer (Computer ID - CID) within the application. Useful in conjunction with the External API.

Example:

```
myID = MachineID;
```

MonitorTitle

This read-only string variable is the title of monitor that caused this script action to fire.

Example:

```
myStr = MonitorTitle;
```

MonitorType

This read-only string variable is the type of monitor that caused this script action to fire.

Example:

```
myStr = MonitorType;
```

RunAction

This method allows you to run other actions from within the script. The method takes an action ID to specify which action to run. Action IDs can be viewed in the Console by enabling the View > Show Object IDs in Navigation Tree menu item.

Example:

```
RunAction(12);
```

SecondsInError

Number of seconds that the monitor has been in error.

Example:

```
inErrSeconds = SecondsInError;
```

State

An array of string values that contain the OK or PROBLEM state for each item being reported on. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = State(1);
```

SendMail

This method sends an email message to the recipient that you choose. This would be useful for sending the incoming Details variable to a different email recipient based on some external factors (such as who is currently carrying the pager)

Example:

```
SendMail("to_address@host.com", "from_address@host.com", "Subject of message", "Body of email
message");
```

SetComputerCustomPropByID

Custom Properties can be used in directory paths, email messages, scripts and other places. Your script can set a Custom Property on a computer by specifying it's computer ID, or use 0 to indicate the computer the action is bring run for should be targeted.

Example:

```
SetComputerCustomPropByID(0, "DEVICEID", "BSQL");
```

The Custom Property DISPLAYED_NOTES is the value you can set by right-clicking a computer and selecting Notes. Notes show up at the top of a Server Status Report.

Sleep

This method takes a single integer value, which is the number of milliseconds that the script should stop and sleep. Be careful about using this -- causing too many actions to sleep for very long means other actions may get delayed

Example:

```
Sleep 1500;
```

Status

A read-only string indicating the current status of the monitor. To see all possible values, See Row Variables from the "Variables..." button for the action.

Example:

```
myStat = Status;
```

StatusText

A read-only string indicating the current status of the monitor. This is a more human-friendly value than Status. To see all possible values, See Row Variables from the "Variables..." button for the action.

Example:

```
myStat = Status;
```

TimeInErrorStr

A text string of how long the monitor has been in error

Example:

```
myStr = TimeInErrorStr;
```

ToLog

This method takes a string value and appends it to the service's log file (useful for debugging scripts). The line will start with ACTION_SCRIPT_LOG.

Example:

```
ToLog("Arrived at first loop");
ToLog(resultVal);
```

PowerShell

PowerShell interaction happens via the $act object.

$act.AcknowledgeAlert

This Function will allow you to acknowledge the alert and to fire or not fire alerts. The three parameters are AlertID ($act.AlertID), AckAlerts, and Acknowledged By. AckAlerts needs to be set to either 0 (doesn't fire achnowledge alerts) or 1(fire achnowledge alerts), defaults is 1.

Example:

```
$act.AcknowledgeAlert($act.AlertID, 1, "Quinn")
```

$act.AlertType

This value indicates if the script is running because of an alert condition, a fixed condition, because an error was acknowledged, or for a reminder of a still open error.

Possible values are:
1 = Alert
2 = Fixed
3 = Acknowledged
4 = Reminder

Example:

```
if($act.AlertType)
```

$act.ChangeMonitorStatus

SetMonitorStatus is a function that sets the status of any monitor. This function takes three values: Monitor ID, Monitor Status, and Status Text. The Monitor ID is assigned in the monitoring service and you can find the ID value by showing the IDs from the View menu and then looking in the navigation colunm. If you use 0 for the Monitor ID the function will change the staus of the monitor the action is attached to. There are four statuses that are available: msOK, msAlert, msError, and msDISABLED. The Status Text is the message that you can supply that is listed for the monitor and will be shown in reports.

Example:

```
$act.ChangeMonitorStatus(43, $act.msAlert, "Status changed for monitor")
```

Possible values:

Monitor Status	Values
OK	$act.msOK
Alert	$act.msAlert
Error	$act.msError
Disabled	$act.msDISABLED
Alert Show as Green	$act.msALERT_GREEN
Alert Show as Red	$act.msALERT_RED

$act.CurrentValue

This is an array of string values, representing the current value (if any) for the item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = $act.CurrentValue[0]
```

$act.CustomProp

This function retrieves the named value of a custom property. It checks the Monitor first, and if not found, checks the monitor's owning computer, and then the computer's group, and then the group's parent group, etc. Custom properties can be set on Groups, Computers and Monitors by right-clicking on the item and choosing the Custom Properties menu.

Example:

```
myStr = $act.CustomProp("NotifyGroupID")
```

$act.Details

This is a string value. This value is the content of the action being fired. It is sent from the monitor and typically contains information about the alert.

Example:

```
myStr = $act.Details
```

$act.Extra1

This is an array of string values, representing extra information that may be available from a particular monitor. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = $act.Extra1[0]
```

$act.Extra2

This is an array of string values, representing extra information that may be available from a particular monitor. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = $act.Extra2[0]
```

$act.GetCredentials

The GetCredentials function lets your script request credentials for use within the script. The relevent setting must be enabled (disabled by default) in the Security Protected Settings. This function takes two parameters: A server name/key value, and a credential type.

Credential types can be one of: ctWIN, ctESX, ctSSH, ctAWS, ctCUSTOM

Example:

```
$user = ""
$info = ""
$pass = ""
if ($act.GetCredentials("TEST-ENV-DB", [PALowPriorityHelper_Net4.CredType]::ctCUSTOM, [ref]$user,
[ref]$info, [ref]$pass))
{
   #use credentials
}
else
{
   #failed to get credentials
}
```

Because of the concern of scripts exfiltrating credentials, we recommend locking monitors or actions that use the GetCredentials function.

$act.GetMonitorList

GetMonitorList is a function that uses the Server ID to return a list of monitors assigned to the server and the monitor's attributes. The server ID can be for any server and if no server is given the default will be the current server that this monitor is assigned to. The returned value is a Hashtable that can be iterated through to find the value needed.

Example:

```
$myTable = $act.GetMonitorList(1)
```

The monitor's attributes values:

Status	status
Error Text	errText
Dependency	depends_on
Title	title
Error Action IDs	errActionIDs
Scheduled Next Run Time	nextRun
Time in Error (seconds)	inErrSeconds
Fixed Action ID	fixedActionIDs
Last Run Time	lastRun

$act.GetServerList

GetServerList is a function that returns a list of servers assigned to a group and the server's attributes. Two parameter are needed for this function; GroupID and include Child Groups. If no GroupID is used the default 0 is used, which is the entire list of servers at the root level. The second parameter is a switch used to return or not return servers that are in child groups under the starting group. Use to 0 to return all servers and 1 to return servers at the parent level only. The returned value is a Hashtable that can be iterated through to find the value needed.

Example:

```
$myTable = $act.GetServerList(2, 1)
```

The server's attributes values:

Server Name	name
Group Level	group
Group ID	groupID
Status	status
Alias for Server	alias

$act.Group

The name of the group that the computer the monitor is attached to belongs in.

Example:

```
myStr = $act.Group
```

$act.GroupPath

The name of the group that the computer the monitor is attached to belongs in, with child groups delimited with a > (ie, Servers/Devices > Austin > Lab)

Example:

```
myStr = $act.GroupPath
```

$act.InventoryValue

Request an inventory value for the current computer, or a different one. An inventory propertyID must be used to specify which inventory value to retrieve. An optional ComputerID value can be used to get the inventory value from a computer other than the current computer. If a property can have multiple values (CPU Names for example), each one will have a newline character appended.

Example:

```
//returns the Operating System (18) for the current computer myStr = $act.InventoryValue(18)
//returns the Operating System (18) for the current computer (0 means use default) myStr =
$act.InventoryValue(18, 0)
//returns the Operating System (18) for computerID 238 myStr = $act.InventoryValue(18, 238)
```

The inventoryID values are given below. Note that not all computers/devices will have all inventory values, and some may have none (especially if an Inventory Collector monitor is not added to the computer).

Anti-virus Version	38
Anti-virus Pattern File	39
Anti-virus Pattern File Date	40
Anti-virus Status	41
Operating System	18
OS Architecture	19
OS Version	20
OS Last Boot Time (_time_t UTC value)	21
OS Current Time (_time_t UTC value)	22
CPU Count	13
CPU Name (multi value)	15
CPU Number of Cores (multi value)	16
CPU Clock Speed (multi value)	17
Display Name	6
Drive Status (multi value)	23
Domain	9
Manufacturer	10
Page File size in MB	24
RAM in MB	14
System Architecture	12
System Model	11
Time Zone Offset	8
Uptime % this month	28
Uptime % last month	29

$act.Item

This is an array of string values, representing the item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = $act.Item[0]
```

$act.ItemType

This is an array of string values, representing the type of item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = $act.ItemType[0]
```

$act.LimitValue

This is an array of string values, representing the limit/threshold (if any) for the item being tested. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = $act.LimitValue[0]
```

$act.Machine

This read-only string variable is the name of the computer that caused the script action to fire.

Example:

```
myStr = $act.Machine
```

$act.MachineAlias

This read-only string variable is the aliased name of the computer that caused the script action to fire.

Example:

```
myStr = $act.MachineAlias
```

$act.MachineID

Returns the numeric value that uniquely identifies this computer (Computer ID - CID) within the application. Useful in conjunction with the External API.

Example:

```
myID = $act.MachineID
```

$act.MachineIP

IP address text string of the computer that the firing monitor is attached to

Example:

```
myStr = $act.MachineIP
```

$act.MonitorTitle

This read-only string variable is the title of monitor that caused this script action to fire.

Example:

```
myStr = $act.MonitorTitle
```

$act.MonitorType

This read-only string variable is the type of monitor that caused this script action to fire.

Example:

```
myStr = $act.MonitorType
```

$act.RunAction

This method allows you to run other actions from within the script. The method takes an action ID to specify which action to run. Action IDs can be viewed in the Console by enabling the View > Show Object IDs in Navigation Tree menu item.

Example:

```
$act.RunAction(12)
```

$act.SecondsInError

Number of seconds that the monitor has been in error.

Example:

```
inErrSeconds = $act.SecondsInError
```

$act.SendMail

This method sends an email message to the recipient that you choose. This would be useful for sending the incoming Details variable to a different email recipient based on some external factors (such as who is currently carrying the pager)

Example:

```
$act.SendMail("to_address@host.com", "from_address@host.com", "Subject of message", "Body of email message")
```

NOTE: It works best if the From address is the same From address being used in your Email Actions.

$act.SetComputerCustomPropByID

Custom Properties exist on groups, computers and monitors. This function lets you set the custom property on a computer. You can specify the computer ID in the first parameter, or set it to 0 to indicate the computer the actions is running for should be targeted.

Example:

```
   $act.SetComputerCustomPropByID(0, "DEVICEID", "BSQL")
```

The Custom Property DISPLAYED_NOTES is the value you can set by right-clicking a computer and selecting Notes. Notes show up at the top of a Server Status Report.

$act.State

An array of string values that contain the OK or PROBLEM state for each item being reported on. See Row Variables from the "Variables..." button for the action.

Example:

```
myStr = $act.State[0]
```

$act.Status

A read-only string indicating the current status of the monitor. To see all possible values, See Row Variables from the "Variables..." button for the action.

Example:

```
myStat = $act.Status
```

$act.StatusText

A read-only string indicating the current status of the monitor. This is a more human-friendly value than Status. To see all possible values, See Row Variables from the "Variables..." button for the action.

Example:

```
myStat = $act.Status
```

$act.TimeInErrorStr

A text string of how long the monitor has been in error

Example:

```
myStr = $act.TimeInErrorStr
```

$act.ToLog

This method takes a string value and appends it to the service's log file (useful for debugging scripts). The line will start with ACTION_SCRIPT_LOG.

Example:

```
$act.ToLog "Arrived at first loop"
$act.ToLog $resultVal
```

Sleep

This is a PowerShell cmdlet that takes two parameters and is not part of the $act object. The first parameter specifies timer in seconds (-s) or milliseconds (-m) and the second is an integer that specifies period of time.

Example:

```
Start-Sleep -s 10
```

SSH

The SSH script works using replacement variables. You can use the variables below which will be replaced with the real values from the monitor. Then the finished script is set to the target computer to be executed.

$AlertID$
: A unique integer value representing this error. If Event Deduplication is enabled, this value will represent the latest error of this type.

$CustomProp(propName)$
: $CustomProp(*propertyName*)$ will be replaced with the value of propertyName which came from from the source monitor, source computer or a parent group. It will be blank if the property is not defined.

$Date$
: Date in a human-readable format

$Details$
: Details of the alert, meaning the text that is normally seen in an email alert for example.

$Details_Single_Line$
: Same as $Details$ above, but all new lines and carriage returns have been removed

$Group$
: Name of the group that the owning monitor is in (i.e. could be a value like "Routers").

$GroupPath$
: Full path name of the group that the owning monitor is in (i.e. could be a value like "Servers/Devices > Boston > Routers")

$Machine$
: Name of the target server

$MachineAlias$
: Alias of the target server if one has been set. There will be no value (meaning an empty string) if no alias has been set.

$MachineID$
: Internal ID representing the target server. These IDs can be obtained using the External API.

$MachineIP$
: IP address of the target server

$MonitorType$
: Textual name of the monitor type (i.e. "Event Log Monitor")

NL
: Value that gets turned into a carriage return-newline pair.

$Status$
: Text representing the monitor status. To see all possible values, See Row Variables from the "Variables..." button for the action.

$StatusText$
: A text value that is more human-friendly that $Status$ above. To see all possible values, See Row Variables from the "Variables..." button for the action.

$Time$
: Human readable time on the monitoring server.

$TimeInError$
: Human readable amount of time the monitor has been in an error/alert state.

Example VBScripts

Connect to a database

```
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
```

Delete Log Files

```
DirToCheck = "C:\Logs"
ExtensionToDelete = "txt"

set oFSO = CreateObject("Scripting.FileSystemObject")
set oFolder = oFSO.GetFolder(DirToCheck)
For Each aFile In oFolder.Files
   if(oFSO.GetExtensionName(aFile.Path) = ExtensionToDelete) then
      oFSO.DeleteFile(aFile.Path)
   end if
Next
```

Example PowerShell

Check files in a directory

Delete Log Files

```
$TargetFolder = "D:\Testing Dir\"
$strFileName = "*.txt"

get-childitem $TargetFolder -include $strFileName -recurse | foreach ($_) {remove-item $_.fullname}
```

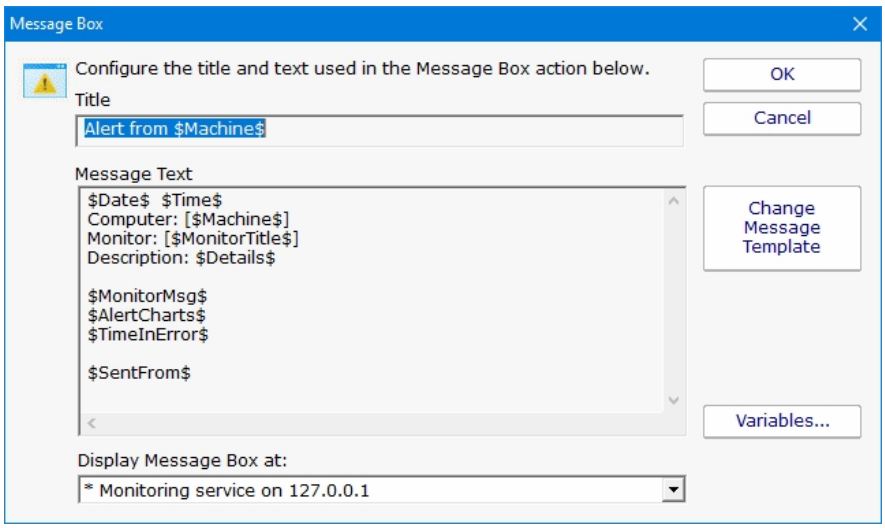
Your Script

```
If you would like to share your script, please contact us.
```

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.



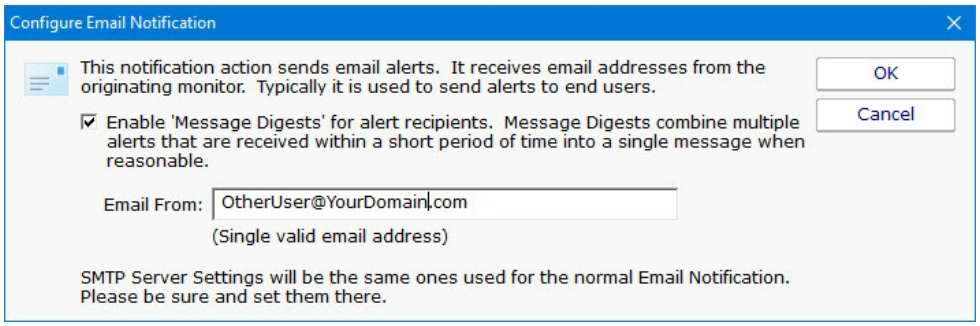
The button titled "Variables" will open a screen that displays the replacement variables that are available for use.

Note that you can choose where the Message Box is displayed. By default it will be displayed on the Central Monitoring Service computer, but you can choose to display it on a remote Satellite computer as well.

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.

The SMTP server settings (which are global to all email actions) are also used by this action to send the message. To change them, go to an E-Mail Message action and change them there.

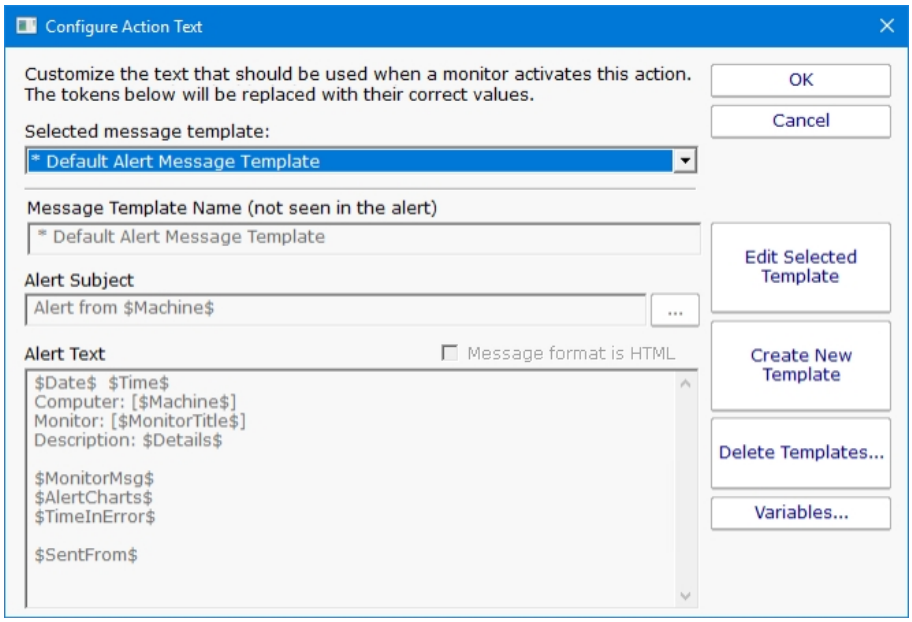
Network Message Action

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.

Message Template

Pressing the Message button displays the configuration dialog below. This lets you customize message text, select different templates to use, and to create new templates. 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. Also, having the abillity to use different message templates will help you get the right information to the right groups.



Select message template dropdown - Allows the option to use different message templates for individual actions that use message templating.

Edit Selected Template - Select and then edit the message template that you wish to change.

Create New Template - Create a new template by supplying the new template with a template name, alert subject, and alert text.

Delete Templates - Delete templates that are no longer needed. Select the Delete Template button and then select the templates that you wish to delete.

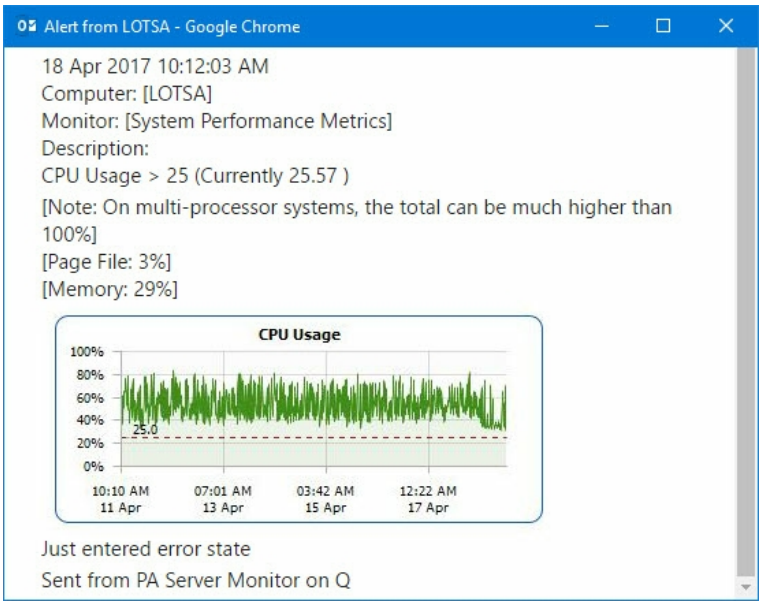
Variables - Using replacement variables allow you to insert details into your message templates.

You can also specify specify that the message is HTML, and enter an HTML message template. Enclose the template in an <html> tag. Don't bother with a <head> tag as most email clients will strip it out.

Some good hints and tips about HTML email are available here:
http://www.mailchimp.com/resources/guides/email-marketing-field-guide/

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.

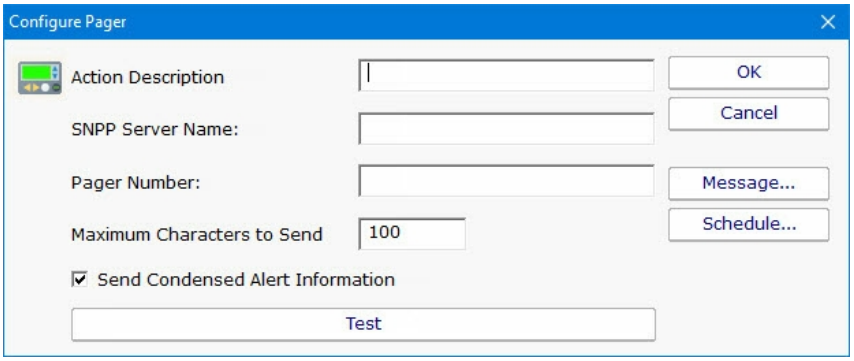
A typical alert email could look something like this:



Note: Actual message content will vary depending on the product being used, and the monitor which fires the actions.

Send Pager Alert Action

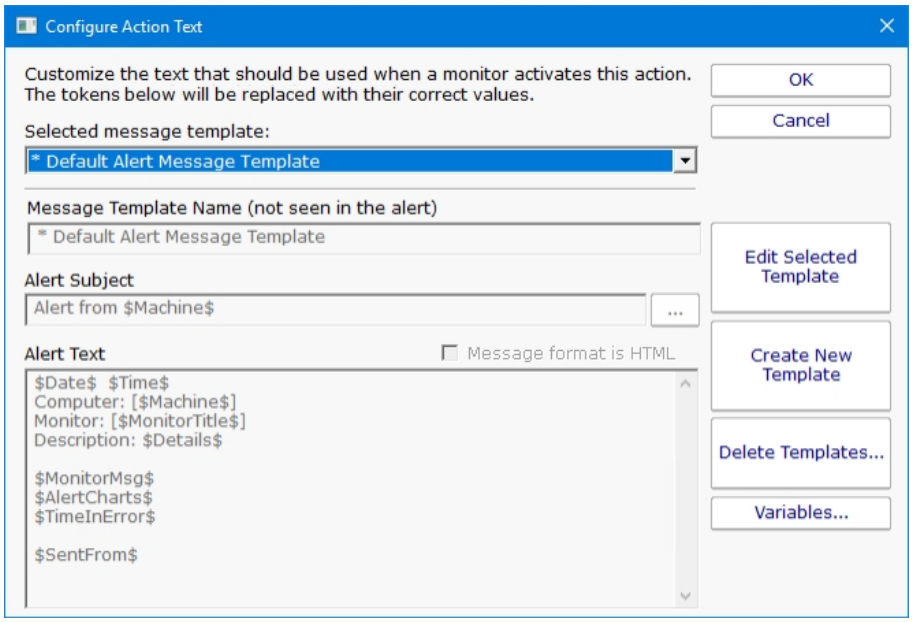
The Send Pager Alert action can send monitor details to an SNPP pager. You will need to get the SNPP server name from your SNPP provider.



Some pager providers have an SMTP gateway. It is often easier to configure an E-Mail Action to send to a pager than the Send Pager Alert action. See the related FAQ about sending SMS alerts.

Message Template

Pressing the Message button displays the configuration dialog below. This lets you customize message text, select different templates to use, and to create new templates. 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. Also, having the abillity to use different message templates will help you get the right information to the right groups.



Select message template dropdown - Allows the option to use different message templates for individual actions that use message templating.

Edit Selected Template - Select and then edit the message template that you wish to change.

Create New Template - Create a new template by supplying the new template with a template name, alert subject, and alert text.

Delete Templates - Delete templates that are no longer needed. Select the Delete Template button and then select the templates that you wish to delete.

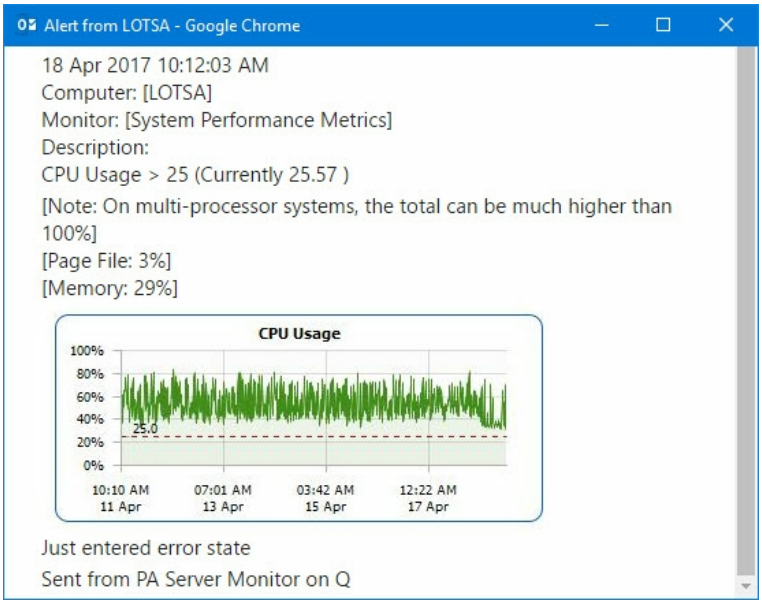
Variables - Using replacement variables allow you to insert details into your message templates.

You can also specify specify that the message is HTML, and enter an HTML message template. Enclose the template in an <html> tag. Don't bother with a <head> tag as most email clients will strip it out.

Some good hints and tips about HTML email are available here:
http://www.mailchimp.com/resources/guides/email-marketing-field-guide/

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.

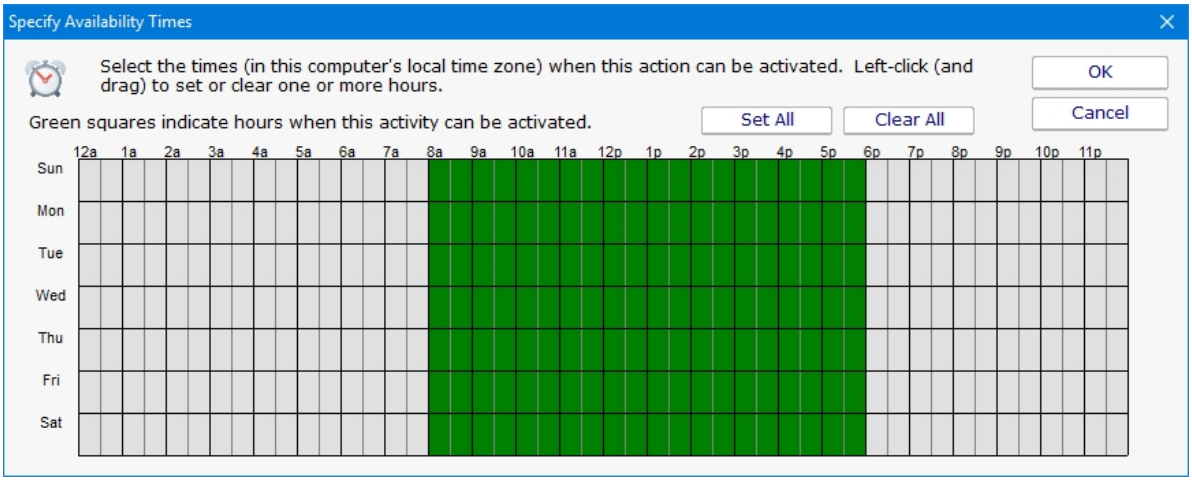
A typical alert email could look something like this:



Note: Actual message content will vary depending on the product being used, and the monitor which fires the actions.

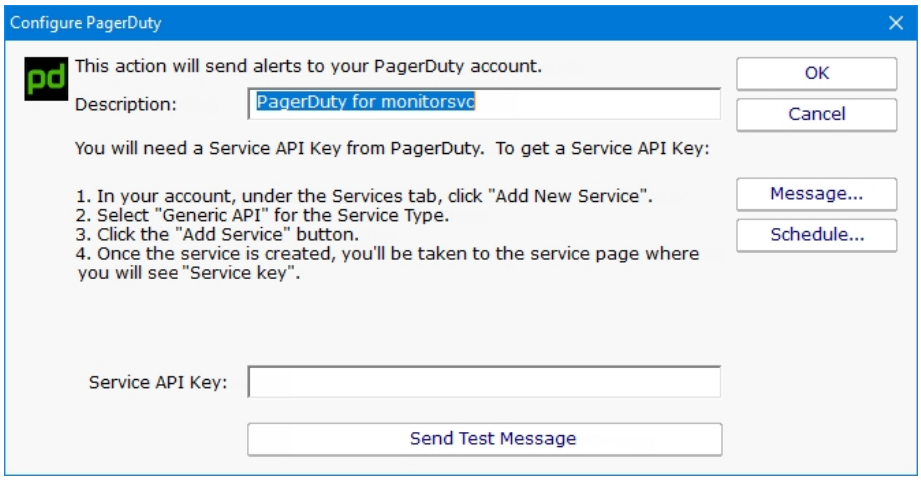
Scheduling

If the action should not be used 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'.



PagerDuty Action

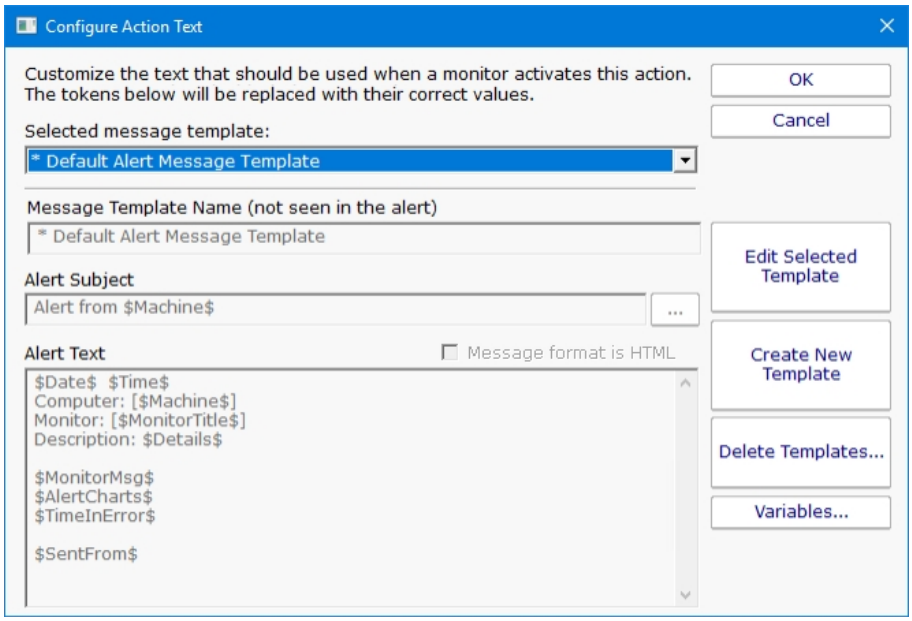
PagerDuty is a popular incident management platform that accepts alerts and helps your team handle them. With the PagerDuty Action, alerts from PA Server Monitor can be sent to PagerDuty for handling.



As is shown in the screenshot above, you just need to get a Service API Key from your PagerDuty account and paste it into the action. The action will then be able to send alerts directory to PagerDuty. Use this action like you would an email action or any other notification action.

Message Template

Pressing the Message button displays the configuration dialog below. This lets you customize message text, select different templates to use, and to create new templates. 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. Also, having the abillity to use different message templates will help you get the right information to the right groups.



Select message template dropdown - Allows the option to use different message templates for individual actions that use message templating.

Edit Selected Template - Select and then edit the message template that you wish to change.

Create New Template - Create a new template by supplying the new template with a template name, alert subject, and alert text.

Delete Templates - Delete templates that are no longer needed. Select the Delete Template button and then select the templates that you wish to delete.

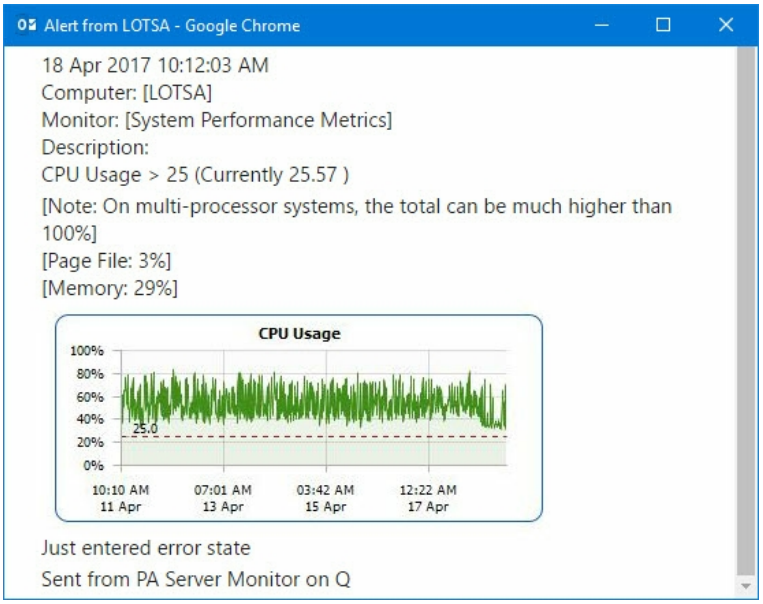
Variables - Using replacement variables allow you to insert details into your message templates.

You can also specify specify that the message is HTML, and enter an HTML message template. Enclose the template in an <html> tag. Don't bother with a <head> tag as most email clients will strip it out.

Some good hints and tips about HTML email are available here:
http://www.mailchimp.com/resources/guides/email-marketing-field-guide/

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.

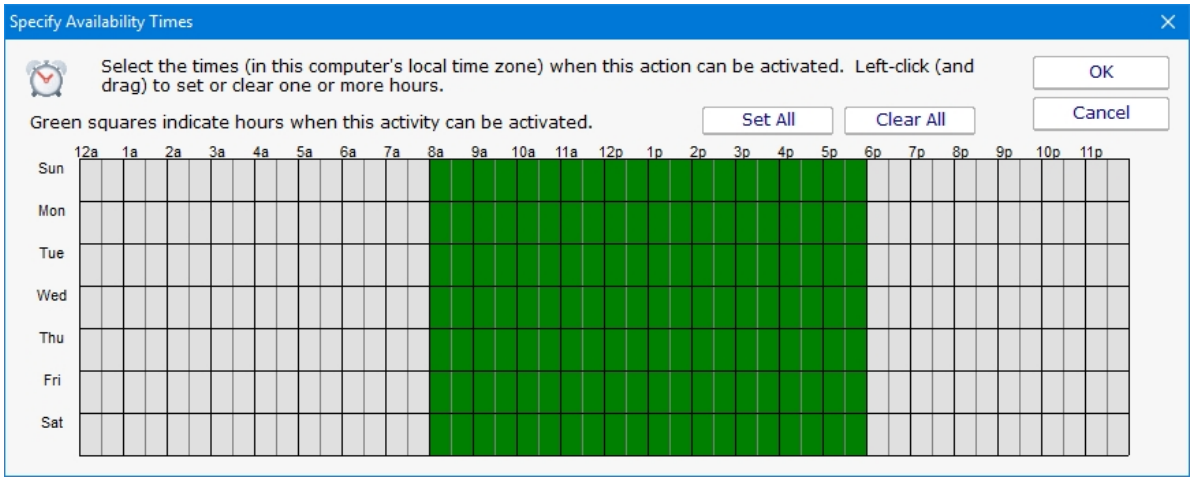
A typical alert email could look something like this:



Note: Actual message content will vary depending on the product being used, and the monitor which fires the actions.

Scheduling

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

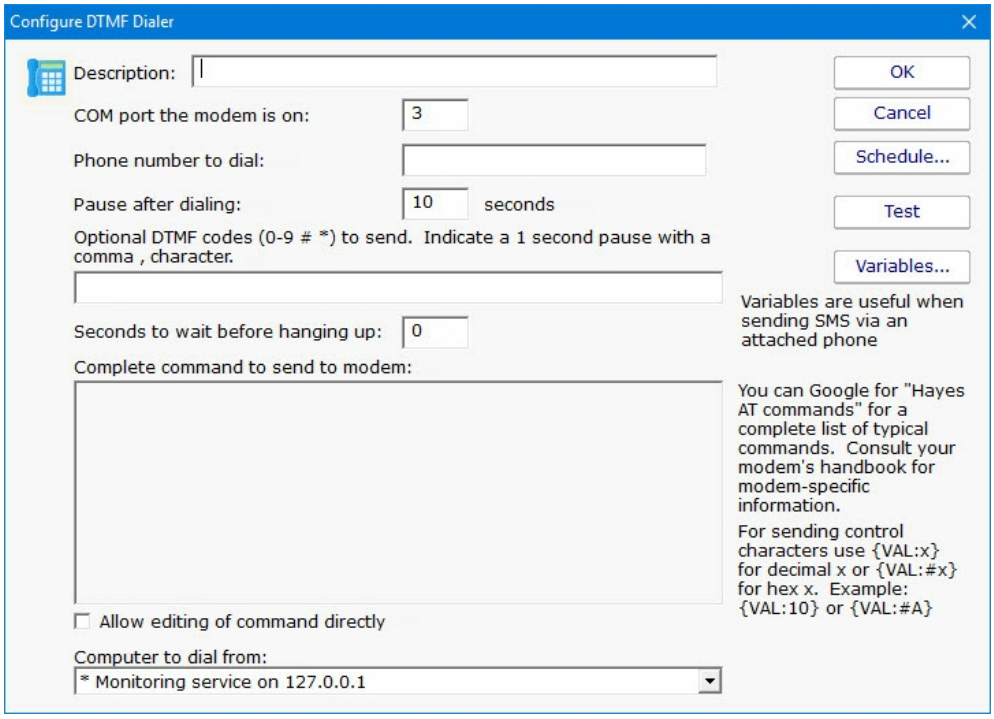

Specify Availability Times
Select the times (in this computer's local time zone) when this action can be activated. Left-click (and drag) to set or clear one or more hours.
OK
Cancel
Green squares indicate hours when this activity can be activated.
Set All
Clear All
12a 1a 2a 3a 4a 5a 6a 7a 8a 9a 10a 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.



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. Your script might look something like the following example:

```
AT
ATZ
ATE0
AT+CMGF=1
AT+CMGS="number_to_dial"
message text
{VAL:26}
```

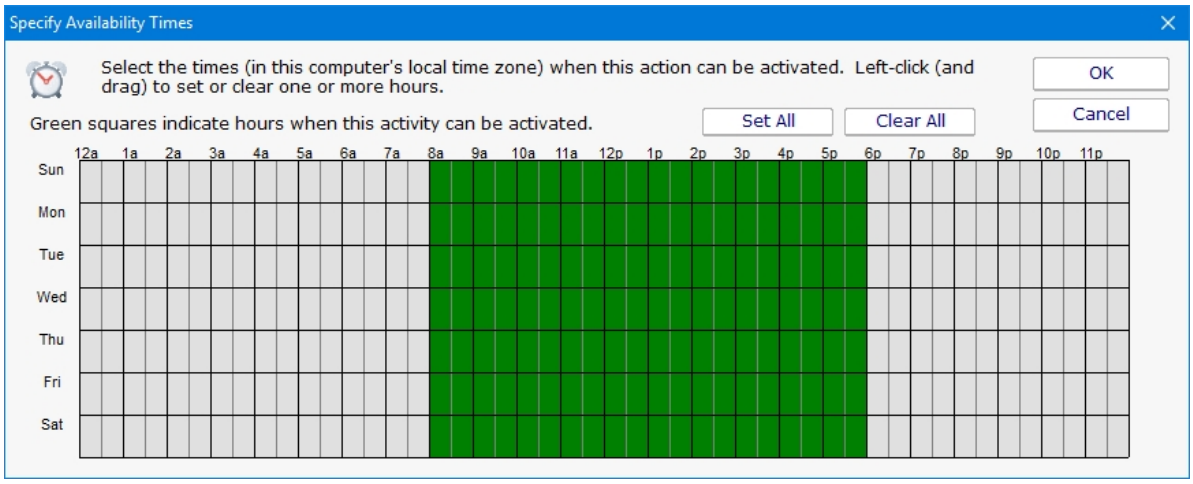
Note that the {VAL:26} is how you send a Ctrl-Z (End of Message character). The value 26 is an ASCII value that maps to Ctrl-Z. The {VAL:x} pattern is how you send arbitrary ASCII codes. There are many ASCII charts on the Internet. Wikipedia's shows Ctrl-Z as 26 (decimal) here. If you want to format the value as hex instead of decimal, use {VAL:#x}, ie {VAL:#1A} to send Ctrl-Z.

In addition, you can have the action send the text of replacement variables. The variable names and their values are shown in the action by pressing the Variables button. An example would be:
$Details$ which expands to the alert descriptive text. So your script might look like this:

```
AT
ATZ
ATE0
AT+CMGF=1
AT+CMGS="number_to_dial"
$Details$
{VAL:26}
```

Scheduling

If the action should not be used 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'.



Experience from the field

At least one customer found that having any extra lines (even blank lines) after the {VAL:26} would cause the message to not send (this is likely phone specific). Also, ATE0 turns off local echo, which will prevent the system from interpreting echoed outgoing text as response commands from the phone/modem.

We have a few customers in Europe that have connected a cell phone to their computer to send SMS messages without an Internet connection.

A customer in the U.S. did the same thing and gives some tips:

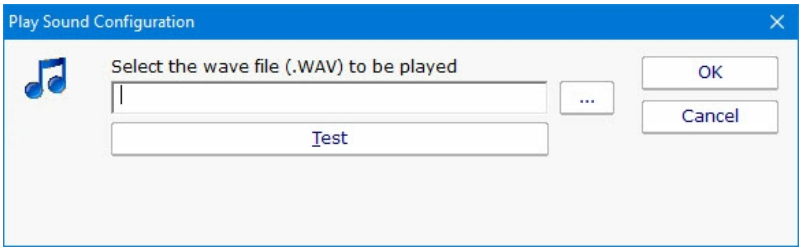
```
Phone used: AT&T Go Phone - Samsung SGH-a177
The phone powers/charges through the USB cable
```

```
Get the data cable. The box doesn't come with a CD so you have to go online at Samsung and
get the drivers at http://www.samsung.com/us/support/search/supportSearchModelResult.do

The drivers won't load the modem. You have to download the Samsung Studio (used for
transferring data and backing up your address book). After you download and install the 95 MB
program and connect to the phone, the drivers will load.

Check your COM port in Control Panel - Modems, and use that in the Phone Dialer action
settings.

ALSO, When I disconnect and reconnect the phone, the COM port used by the phone jumps from 4
to 5 and back. So be aware that if you have to cycle power on the box, check the COM port or
you won't get notified. One option around this is to setup two Phone Dialer actions -- one
goes to COM4 and another one to COM5 and just put up with the email on the failed alert.
```

Thanks Tim.

Play Sound File Action

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

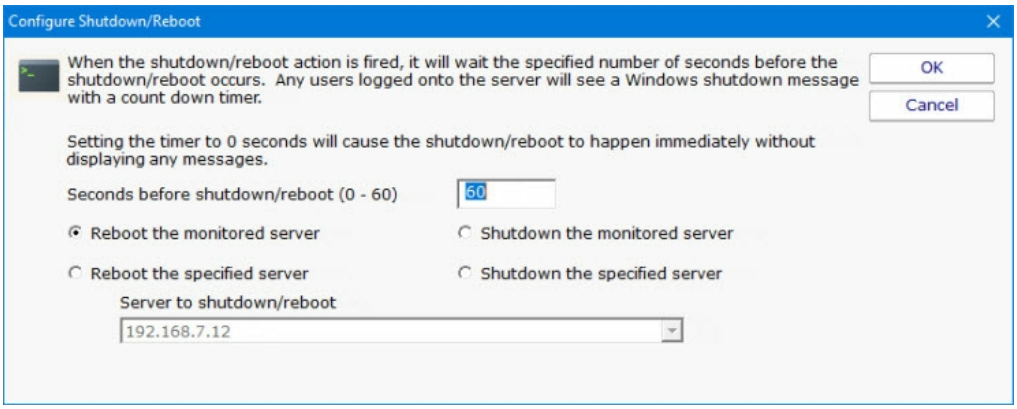


The sound is played on the Central Monitoring Service computer.

Reboot Computer Action

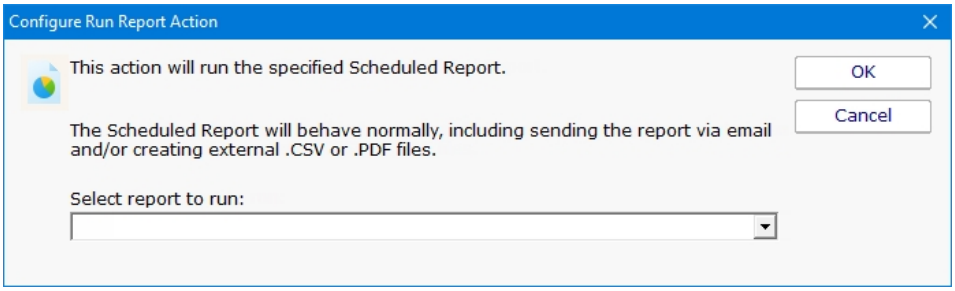
The Reboot Computer action causes a computer to reboot or shutdown when it is run. You can specify which computer using the radio button options. By default the **monitored computer** will be rebooted when this action is run.

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.



Run Report Action

Building on PA Server Monitor's incredible flexibility, now you can have a monitor trigger the generation of a Scheduled Report with the Run Report Action.



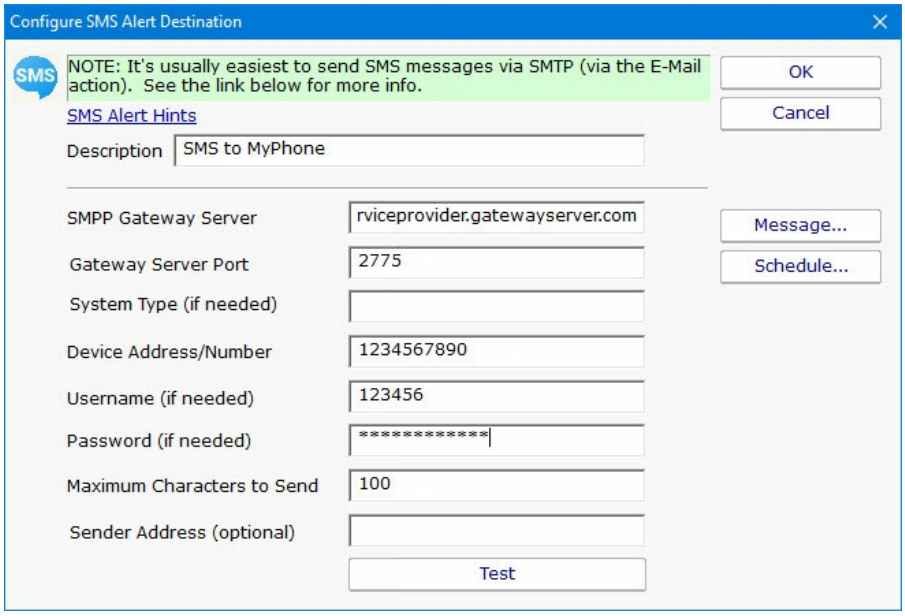
As is shown in the screenshot above, you just select an existing Scheduled Report. When this action is triggered, the Scheduled Report will run, including sending any specified emails and saving external PDF or CSV files.

SMS Text Message Action

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

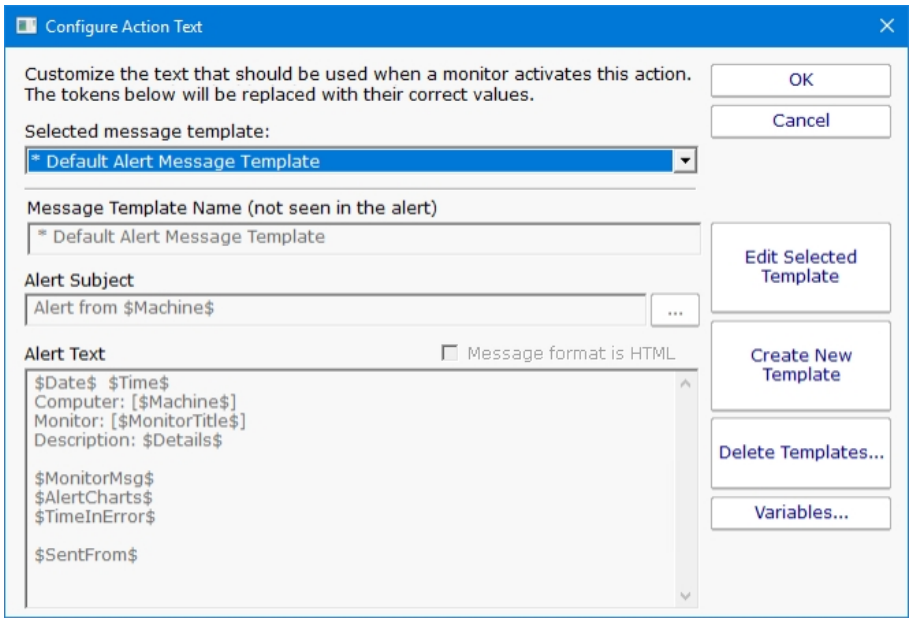
Finding out your phone company's SMPP server is often challenging. It's usually easier to send SMS messages to phones and mobile devices via SMTP with the E-mail Message action. (See the SMS FAQ for details).

If you want to send via SMPP, it might be necessary to get a third party SMS account if your service provider doesn't have a public SMPP server. One company offering this service is Clickatell.



Message Template

Pressing the Message button displays the configuration dialog below. This lets you customize message text, select different templates to use, and to create new templates. 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. Also, having the abillity to use different message templates will help you get the right information to the right groups.



Select message template dropdown - Allows the option to use different message templates for individual actions that use message templating.

Edit Selected Template - Select and then edit the message template that you wish to change.

Create New Template - Create a new template by supplying the new template with a template name, alert subject, and alert text.

Delete Templates - Delete templates that are no longer needed. Select the Delete Template button and then select the templates that you wish to delete.

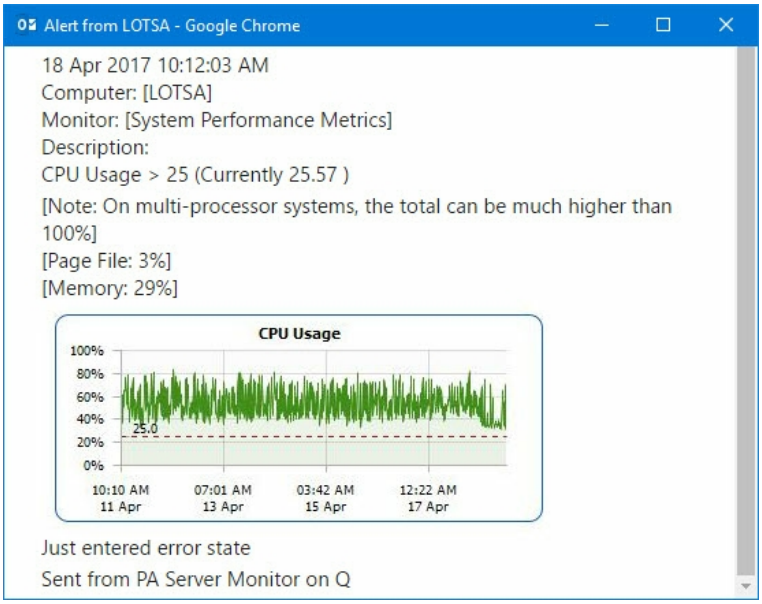
Variables - Using replacement variables allow you to insert details into your message templates.

You can also specify specify that the message is HTML, and enter an HTML message template. Enclose the template in an <html> tag. Don't bother with a <head> tag as most email clients will strip it out.

Some good hints and tips about HTML email are available here:
http://www.mailchimp.com/resources/guides/email-marketing-field-guide/

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.

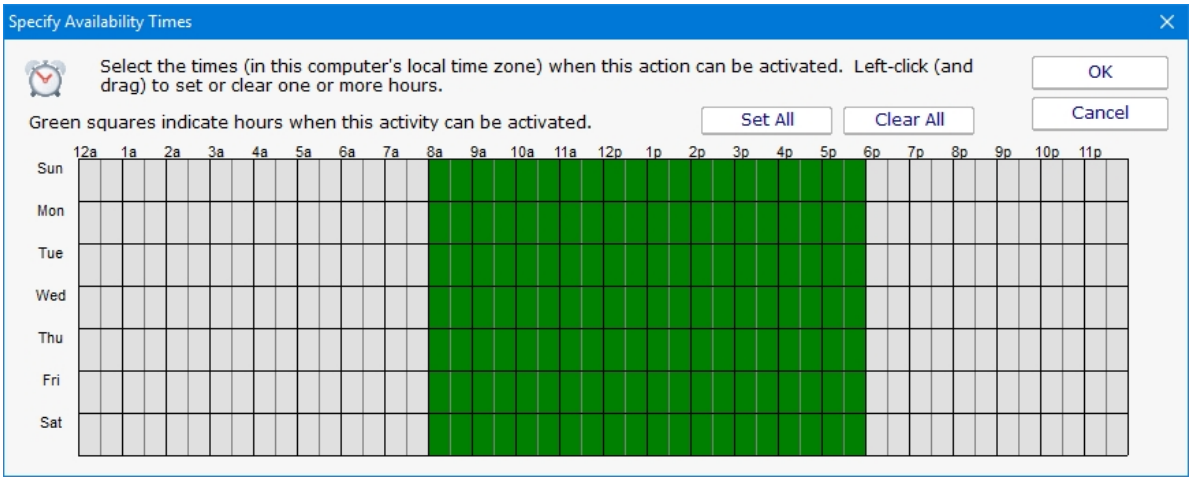
A typical alert email could look something like this:



Note: Actual message content will vary depending on the product being used, and the monitor which fires the actions.

Scheduling

If the action should not be used 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'.

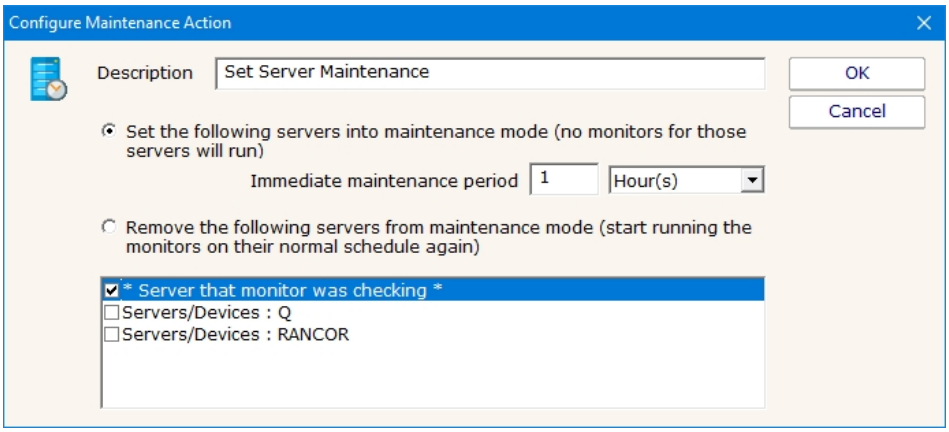


See the FAQ on other ways to send alerts to phones and pagers at: SMS Hints

Set Server Maintenance Mode Action

This action can be used to put a server or a group of servers into immediate maintenance mode. It can also be set to remove server(s) from immediate maintenance.

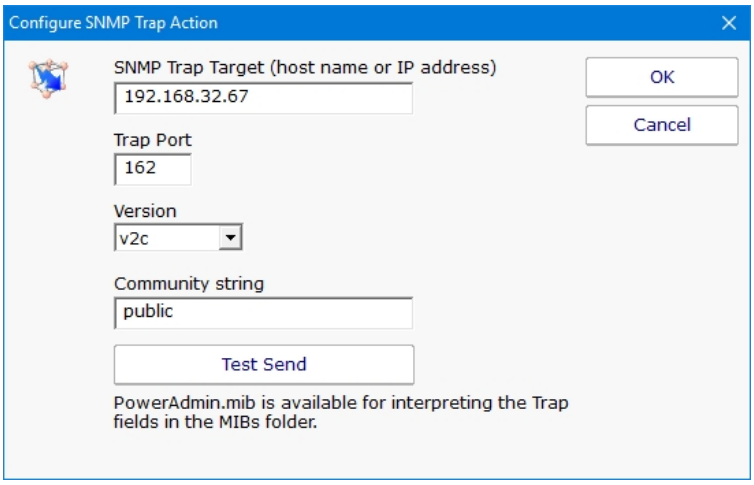
The dialog shown below is displayed when you add or edit a set server maintenance mode action. You may select either to put servers into maintenance or remove them but not both in the same action.



Enter the name of the action making it something that will be meaningful to you. Then select the option to set how the maintenance will occur and then select the servers to include. The top server option can be used to select the server that is currently being monitored.

SNMP Trap Action

The SNMP Trap action will take values, descriptions, etc from a monitor and fire them off as an SNMP Trap. You can configure the action to send the Trap to any server/device on the network, using any port (port 162 is the default SNMP Trap port).



Traps will have the following fields:

alertSummary	A human readable summary of the alert condition.
computerName	Source Computer Name
monitorName	Source monitor name.
monitorStatus	Monitor status.
monitorMessage	A custom message from the monitor. This field is often empty.
alertTimestamp	A string representing the time of the error in YYYYMMDDHHMMSS format. This is in the local time of the reporting agent.
monitorType	Source monitor type.
monitorStatusID	Monitor status ID.
computerID	*Source computer ID within the Power Admin monitoring product.
monitorID	*Source monitor ID.
monitorTypeID	Source monitor type ID.
monitorIDasOID	*Source monitor ID as an OID
computerIDasOID	*Source computer ID as an OID

* You can view the IDs in the Console by setting HKEY_LOCAL_MACHINE\software\PAServerMonitor, [DWORD] xShowIDs = 1

A MIB file exists in the C:\Program Files\PA Server Monitor\MIBs folder which describes the format of the Traps that will be sent.

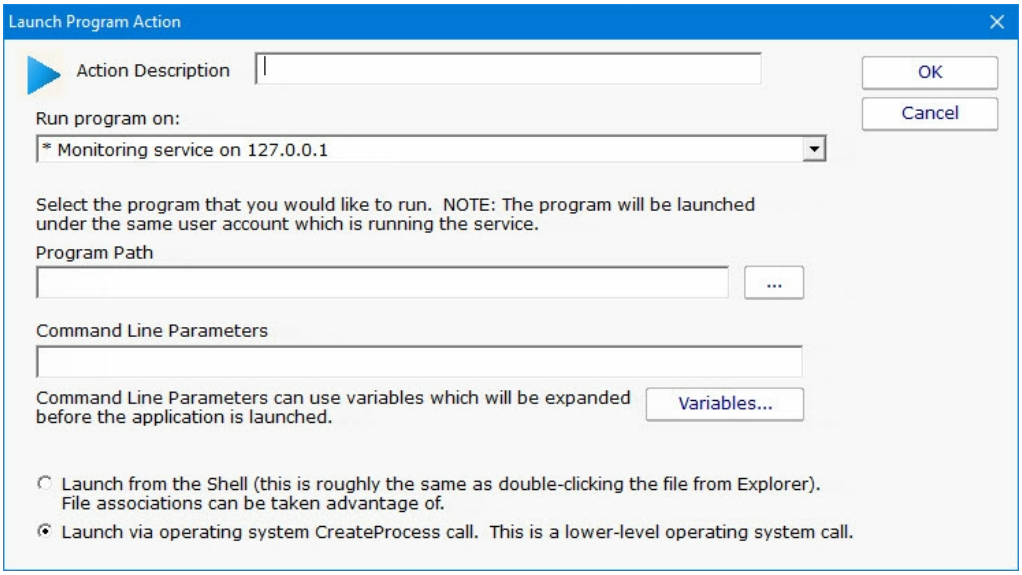
You can download that same MIB file here.

Start Application Action

This action will start a program and run it on the Central Monitoring Service, or on a remote Satellite computer.

The application is started on the specified monitoring computer (where the monitoring service is being run), not on the target computer that is being monitored.

To launch an application on a remote computer, we recommend having the Start Application Action run Microsoft's PsExec, and direct it to launch your target application remotely. More information on PsExec



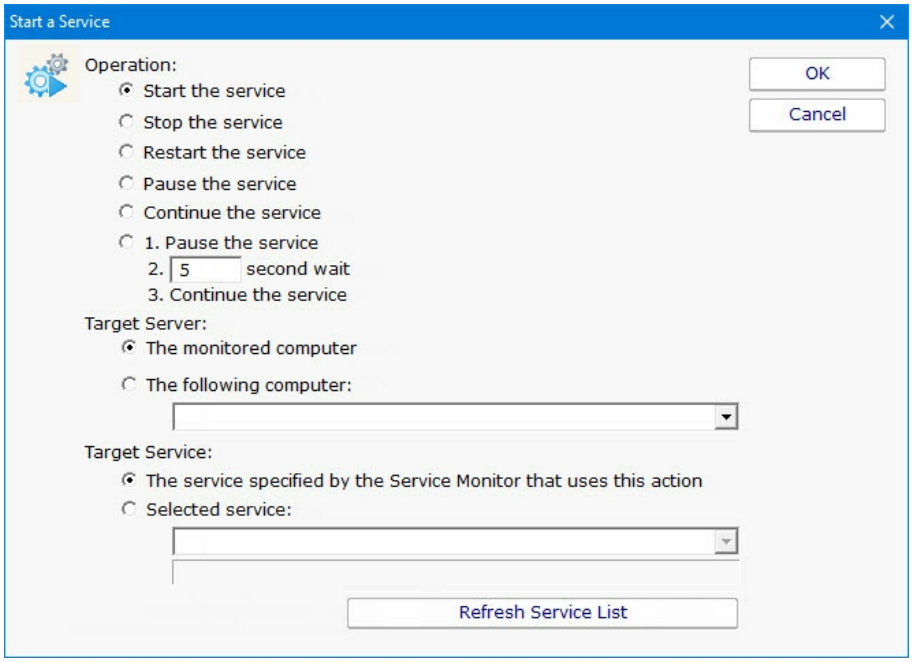
Replacement variables can optionally be passed on the command line to the program that is being launched.

It is important to remember that the application is being launched by the monitoring service, which quite often runs as a different user account than you. It which might not have the same HKEY_CURRENT_USER registry hive, mapped drives, Internet settings, etc as you do. You can configure the account that the service runs as from Preferences in the Console application, or configure which user is used to monitor a particular computer by right clicking on that computer in the navigation panel and choosing Type & Credentials -> Set Login Credentials.

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.

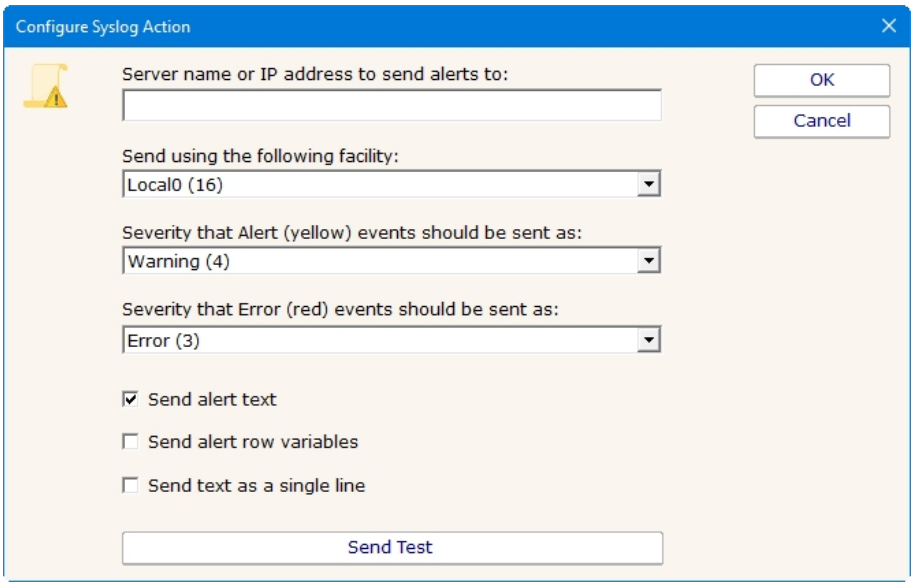
This action can operate on a specified serivce on a specified server, or it can default to operating on the service and server that is passed in by a monitor (the Service Monitor passes this information when it finds a service is down).



Syslog Action

The Syslog action will send a summary description of a monitor's findings as a Syslog event. You can configure the action to send the log event to any server/device on the network that is listening for syslog events.

You can indicate just a hostname or IP address, in which case port 514 will be used. Or you can use a hostname:port or IP address:port format to target a different port.



You configure which syslog facility should be used when sending the log event, as well as the severity that should be used.

Multiple Syslog Actions could be set up to send different logs to different Syslog servers. Some monitors could then use one Syslog Action, and other monitors could send alerts through a different Syslog Action.

Message Format

The Syslog Action has a few options to control the output of the message, and the message content will also be affected by the source monitor sending the message. In some cases it will be easiest to try it and see what the message looks like in your particular scenario.

Send alert text
: With this option chosen the alert text is sent, the same as you might see in an email message.

Send alert row variables
: Row variables depend on which monitor is sending the alert. The bottom of the Expansion Variables page lists the possible variables and their meaning. Row variables will be concatenated together, with each field separated by a pipe | character.

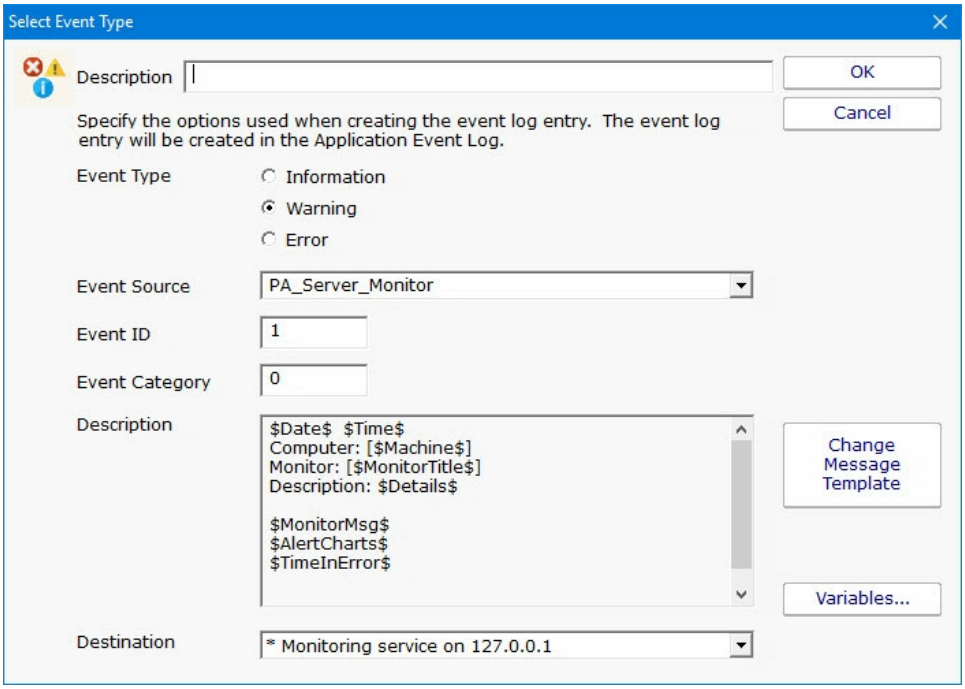
I:*$Item(x)$*IT:*$ItemType(x)$*ICV:*$CurrVal(x)$*LM:$LimitVal(x)$IX1:*$Extra1(x)$*X2:*$Extra2(x)$*ID:*$ID(x)$*F:$Facility(x)$IS:*$Severity(x)$*

Each of the fields will be emitted even if there is no value in the field. Each row variable line ends with a newline (\r\n).

Send text as a single line
: With this option checked, all new lines (\n and \r characters) are stripped from the output.

Write to Event Log Action

The Write to Event Log Action writes details of a monitor's findings to the Windows Application Event Log.

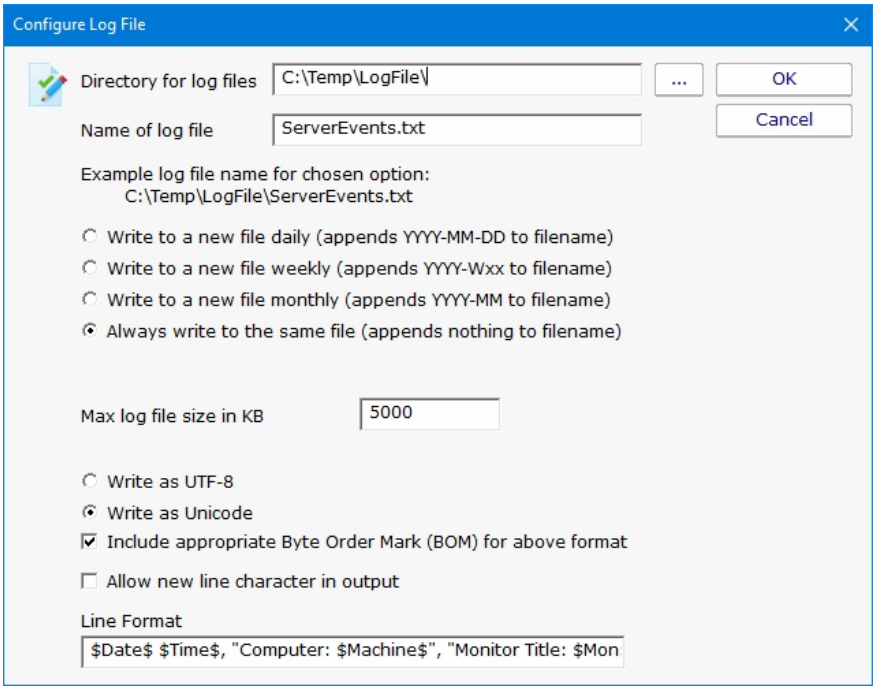


You can specify whether to write the event as an Error, Warning or Information event, the Source, ID and Category to use, and specify the event description.

The event will be written to the specified monitoring service's Application Event Log.

Write to a Text Log File Action

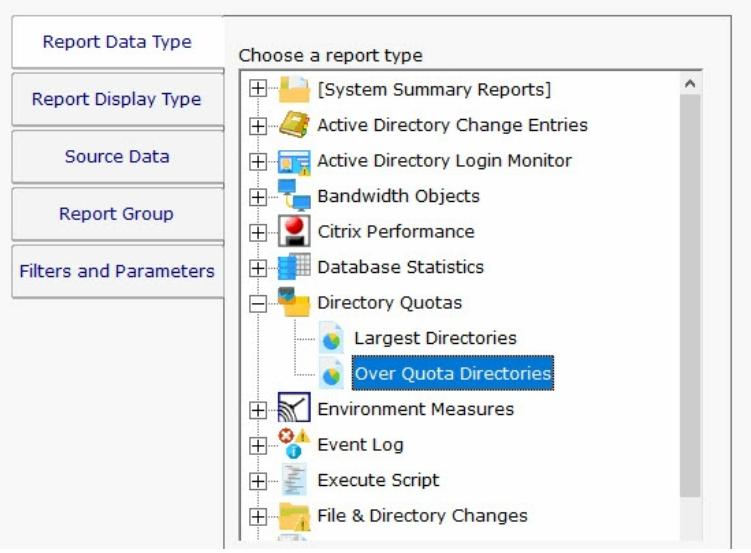
The text logging action writes to a text log file the details of a problem found by a monitor. You specify where the log file goes, and how often a new file is started.



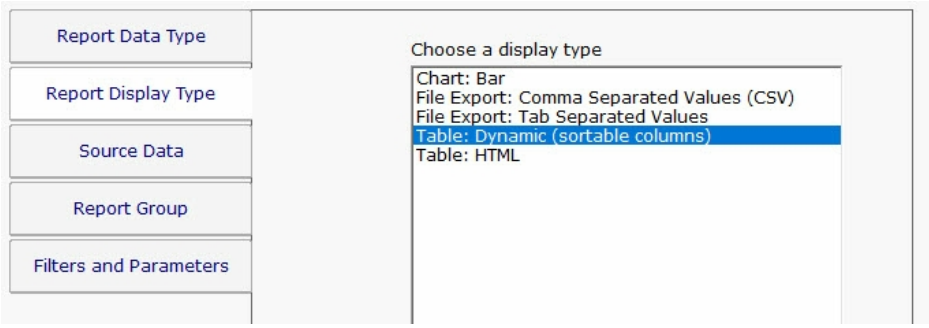
Ad Hoc Reports

Ad hoc reports can be generated at any time to quickly gather historical and current data on your systems. Simply click through each tab and make the selection that is presented on that 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 create a dynamic HTML table with sortable column headers. The CSV Export is a .csv file which can easily be imported into Excel and other applications. Some report display types won't make sense for some data types -- in that case, the display type will not be shown.

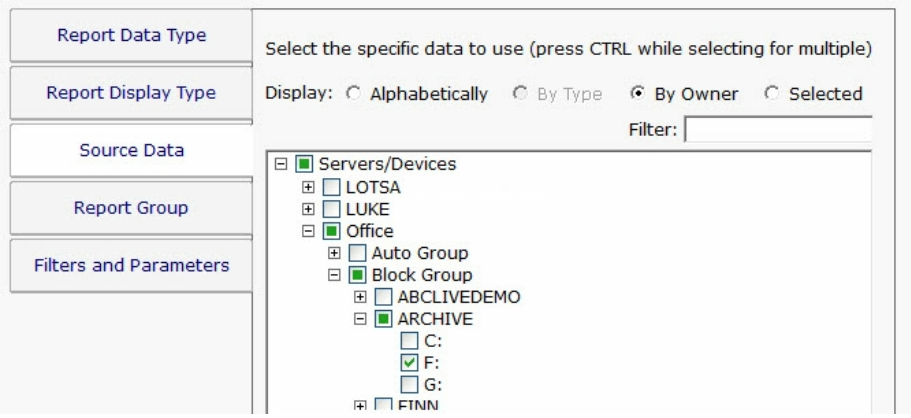


After having selected the report type and the display format, it's time to choose which data to report on. This is done on the Source Data tab. This tab will display all of the data that is available for the chosen report type. In this case we are shown drives that can be reported on. The radio buttons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

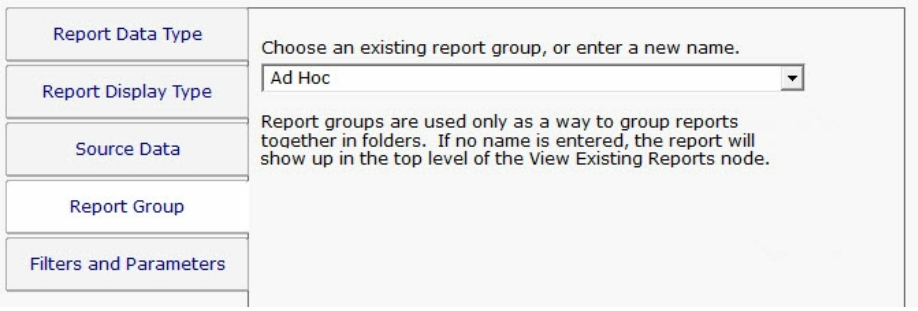
Check the box next to the data set(s) that you want to report on. You can also place the check at a higher level in the data set tree

and all data sets below it will also get checked.

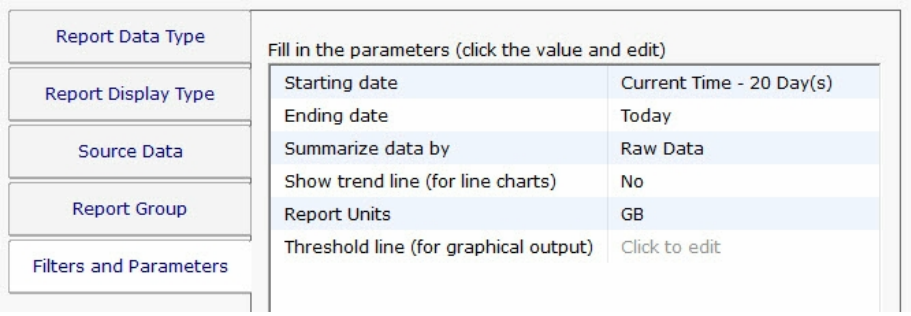
NOTE: Most data sets can be deleted. Although not shown in this screenshot, there is a "Delete selected data sets" button near the bottom of this dialog. Clicking that button will delete the data for the checked data sets from the database.



Select the Group where the Ad Hoc report will be saved to under View Existing Reports.



The final tab is Filters and Parameters. The filters and parameters shown depend on which report type you are creating. 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.



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. To see the URL for the finished report, scroll all the way to the bottom.

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.

Double-check the Filter and Parameters tab for other settings. Some times the parameters end up excluding data that you want.

Make sure the data set selected in the Source Data tab is what you expect.

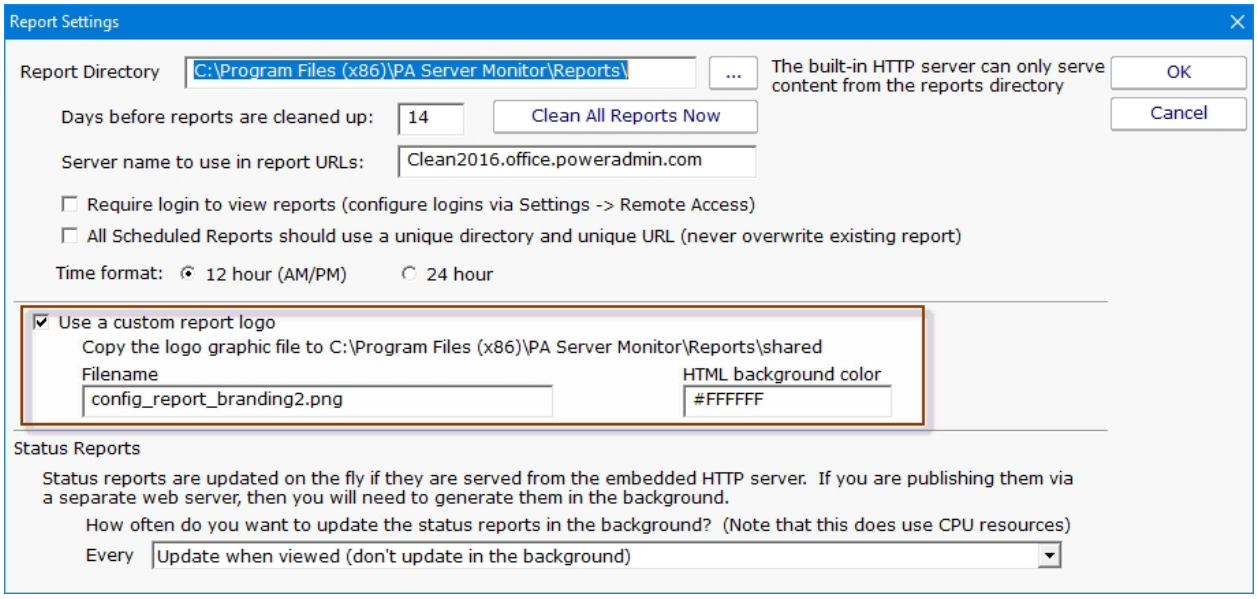
Report Branding

Managed Service Providers are always looking for ways to add value for their customers and build their brand. PA Server Monitor can help by making it easy to brand reports that you give customers.

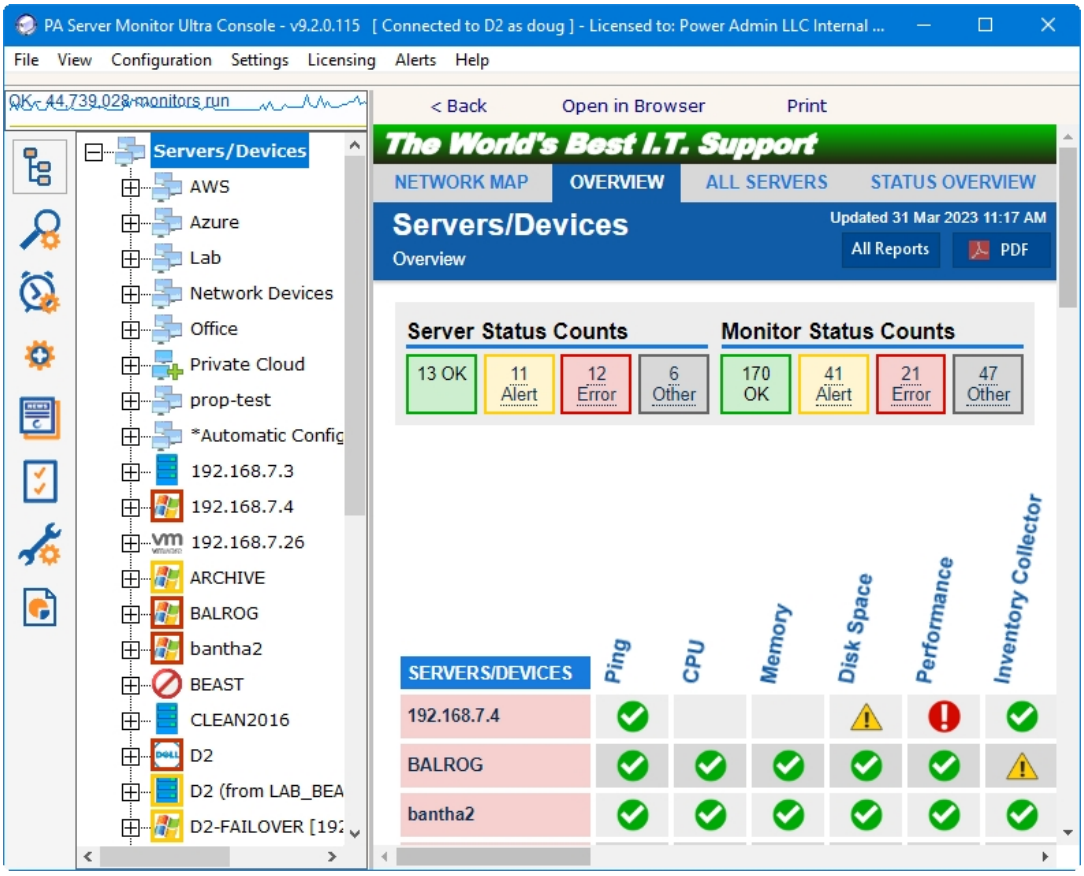
Create a graphic file (any image format that can be displayed by a browser will work). Copy that graphic file to:
C:\Program Files\PA Server Monitor\Reports\Shared

Example "my_logo.png"

Next, go to Settings -> Report Settings and indicate the graphic file name (just the file name, not the full path). The graphic file will be shown in a band at the top of the report. If the graphic doesn't fill the whole space, you can choose what background color to show in the rest of the band (use HTML colors like #FFFFFF for white for example).



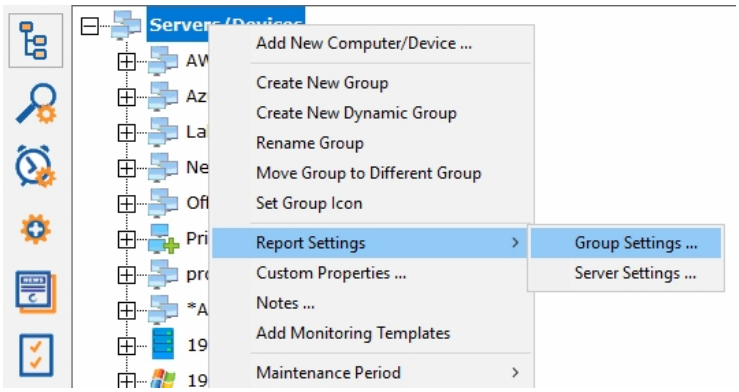
Reports will then appear like the example below


PA Server Monitor Ultra Console - v9.2.0.115 [Connected to D2 as doug] - Licensed to: Power Admin LLC Internal ...
File View Configuration Settings Licensing Alerts Help
OK - 44,739,028 monitors run
Servers/Devices
AWS
Azure
Lab
Network Devices
Office
Private Cloud
prop-test
*Automatic Config
192.168.7.3
192.168.7.4
192.168.7.26
ARCHIVE
BALROG
bantha2
BEAST
CLEAN2016
D2
D2 (from LAB_BEA
D2-FAILOVER [192
< Back
Open in Browser
Print
The World's Best I.T. Support
NETWORK MAP
OVERVIEW
ALL SERVERS
STATUS OVERVIEW
Servers/Devices
Overview
Updated 31 Mar 2023 11:17 AM
All Reports
PDF
Server Status Counts
13 OK
11 Alert
12 Error
6 Other
Monitor Status Counts
170 OK
41 Alert
21 Error
47 Other
SERVERS/DEVICES
Ping
CPU
Memory
Disk Space
Performance
Inventory Collector
192.168.7.4
BALROG
bantha2

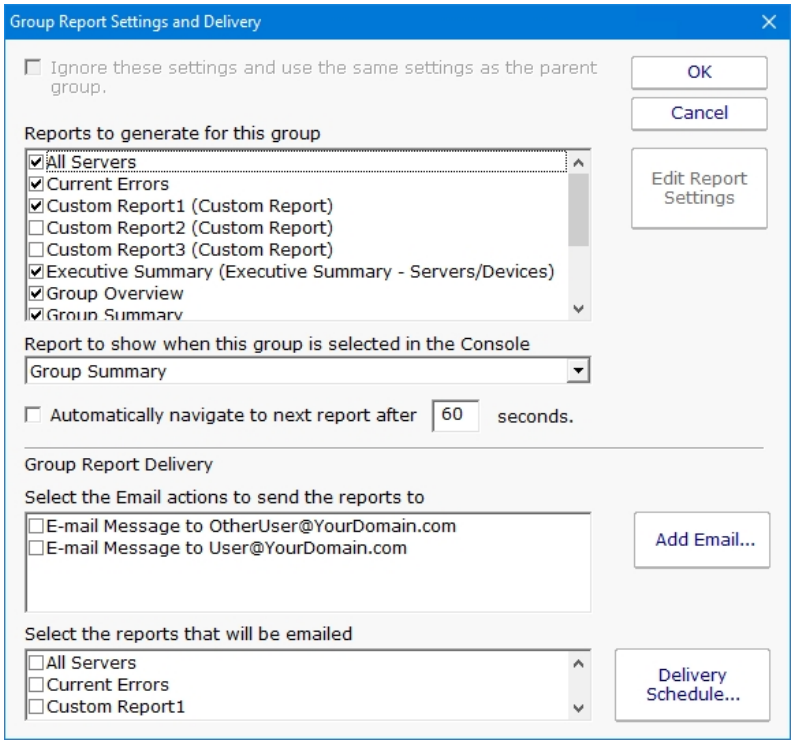
Group Report Settings and Delivery

The Group Report Settings and Delivery dialog allows you to change some attributes of Group Reports. Group Report are shown when you select a group in the navigation pane. They can also be shown in a browser.

To display the Group Report Settings and Delivery dialog, go to "Report Settings" and select the "Group Settings" 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.



Here you can 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 various types of Server Group reports. When this check box is selected, the display will show each of the report types in succession, and will pause at each report type for the number of seconds that have been specified in the box to the right.

"Select the Email Actions to send the reports to" allows you to specify which email addresses that the reports will periodically get sent to. You can add new email addresses, in addition to the pre-configured email addresses that are already 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.

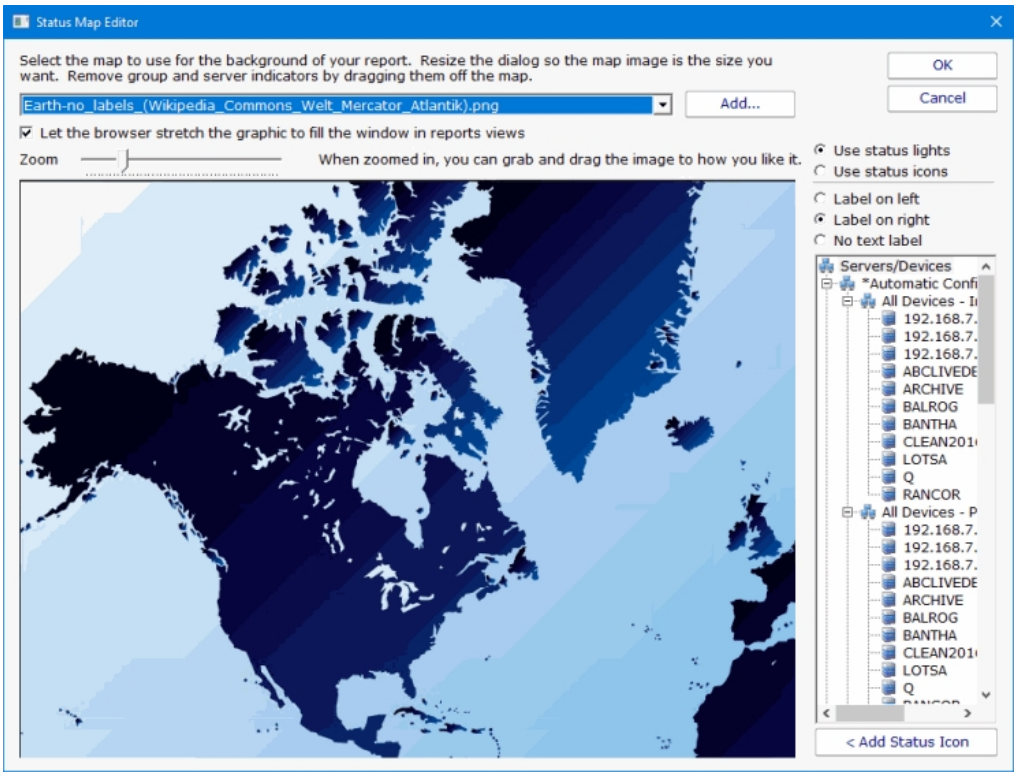
If you are an IT service provider and want to mail reports to your clients, be sure and set:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor
[DWORD]Reports_DisableNavButtons = 1
```

This will remove navigation links from the reports so clients won't be able to browse to other clients' reports. Naturally navigation within the Console will be unaffected.

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. A variety of map graphics are available by default, and you can add your own.



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.

You need to manually place the groups or servers that you want on the map graphic. They do not show up automatically.

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

You can 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 can use the "Add" button next to the background map selection 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 can move the map image 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 can 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 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 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 can "flip" the label in a certain direction so that a city name or feature on the underlying map is clearer. You can also not apply a label to certain indicators.

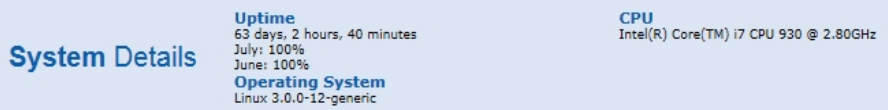
When viewing the status map with a browser or in the Console, the map graphic will be stretched or shrunk as needed to fill the browser window that holds it. The icons will be moved appropriately so they remain in the same relative location on the map.

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.

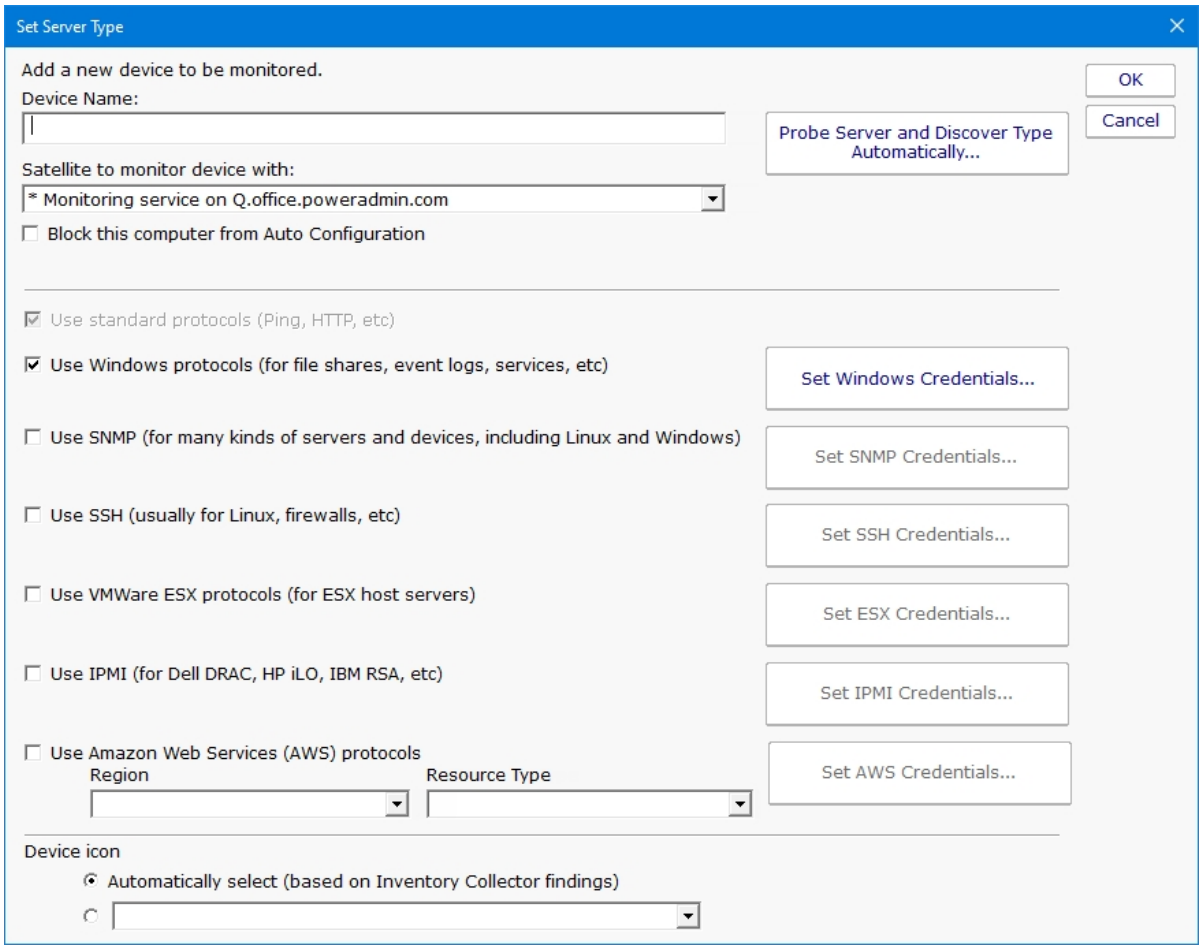

Network Map
Group Overview
Group Summary
All Server
Servers/Devices
Visual Status Map
TYRO-II Satellite
D2
LAB
ABCLIVEDEMO
TEST-1

Server Inventory

By default, PA Server Monitor will gather basic hardware and system inventory from monitored servers and devices. This inventory information is shown in the System Details box on the Server Status Report.



The method for gathering inventory data depends on the settings on the Set Server Type dialog which is accessible by right-clicking the server/device and going to Type & Credentials -> Set Server Type.



The following methods can be used to try and get inventory information:

WMI
: Used for Windows servers

System Details Agent
: A small executable file (PASystemDetails.exe) is copied to the target Windows computer and launched. It collects system information, reports back to PA Server Monitor, and then shuts down. The executable file is then removed from the system. PAExec is used for the remote launch.

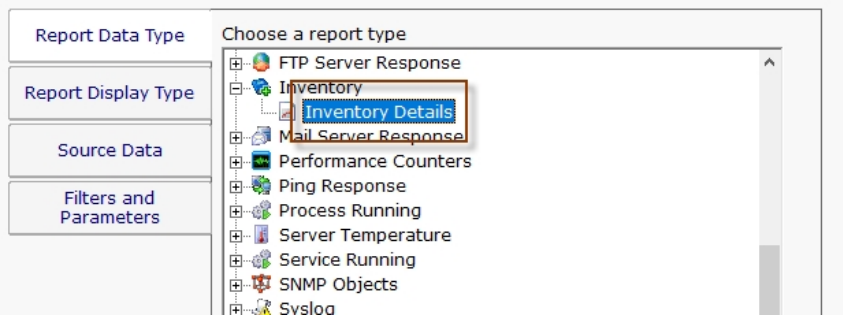
SNMP
: Useful for Windows and non-Windows devices

ESX API
: VMWare's ESX host servers can be queried as well

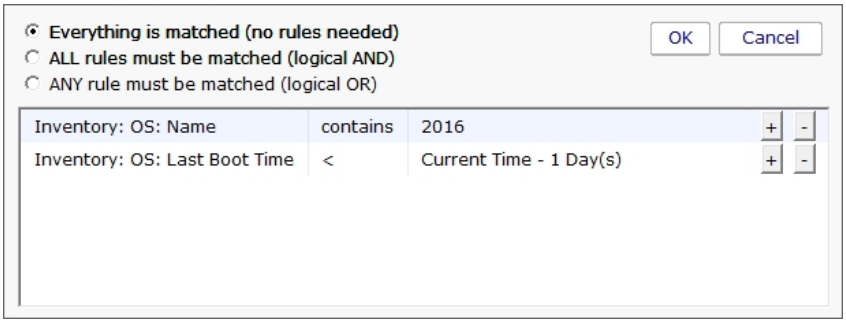
IMPORTANT: Inventory collection is done independent of monitoring. Specifically, WMI and the System Details agent are NOT used for monitoring or alerting.

Inventory Report

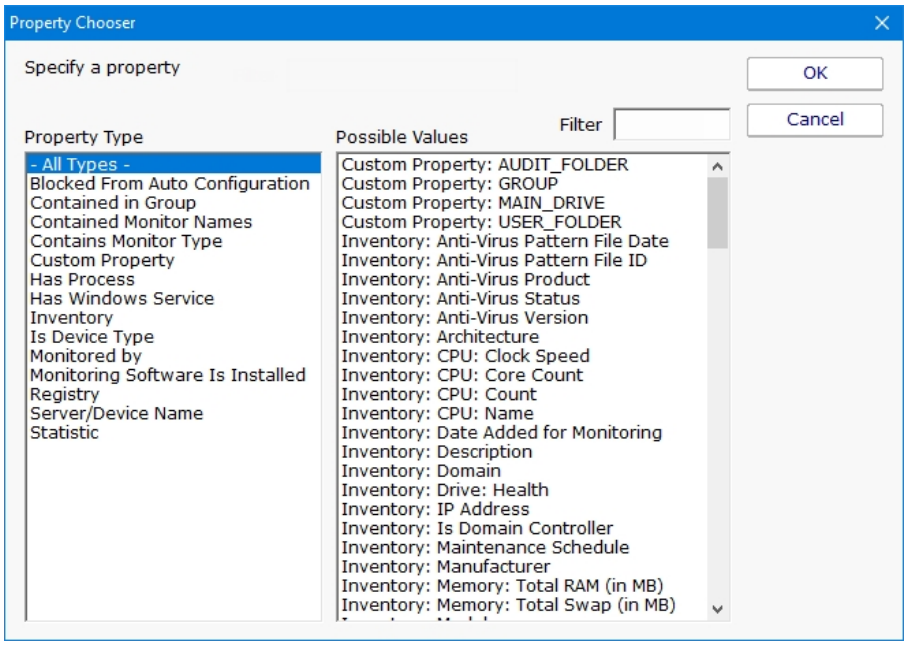
Along with inventory collection and display on the Server Status Report, the Inventory Details report can also display inventory data.



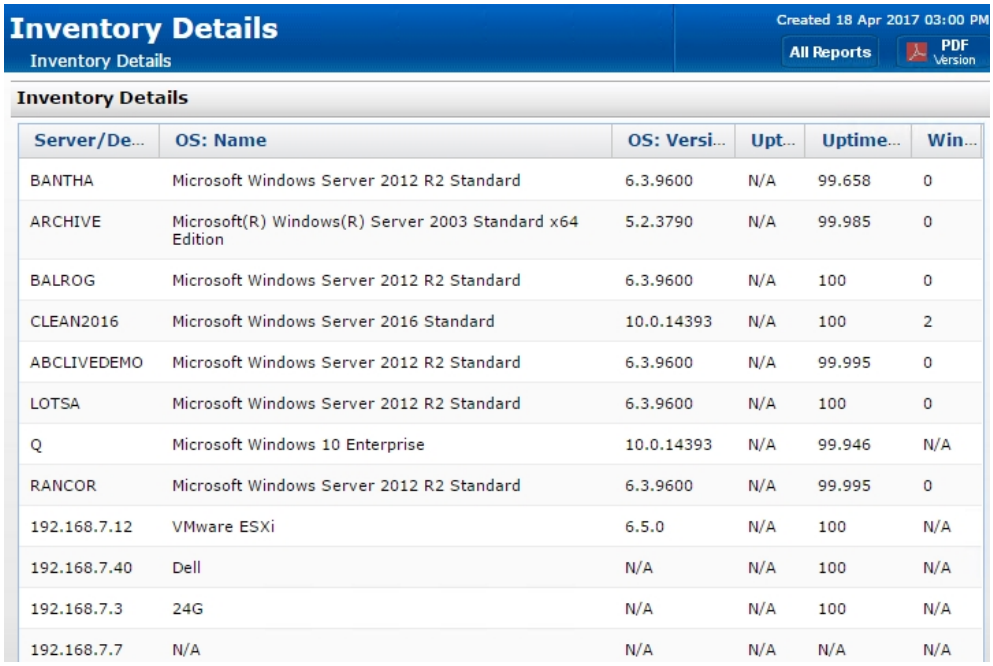
The computers/devices to report on are selected via their inventory properties. All or just some of the selections can be met depending on your radio buttons at the top.



Output columns can also be chosen from a list of gathered inventory details.



Like all reports, this report can output in a sortable table, a flat HTML table, or a comma-separated text file (CSV) for import into another program like Excel.



Inventory Details

Inventory Details

Created 18 Apr 2017 03:00 PM

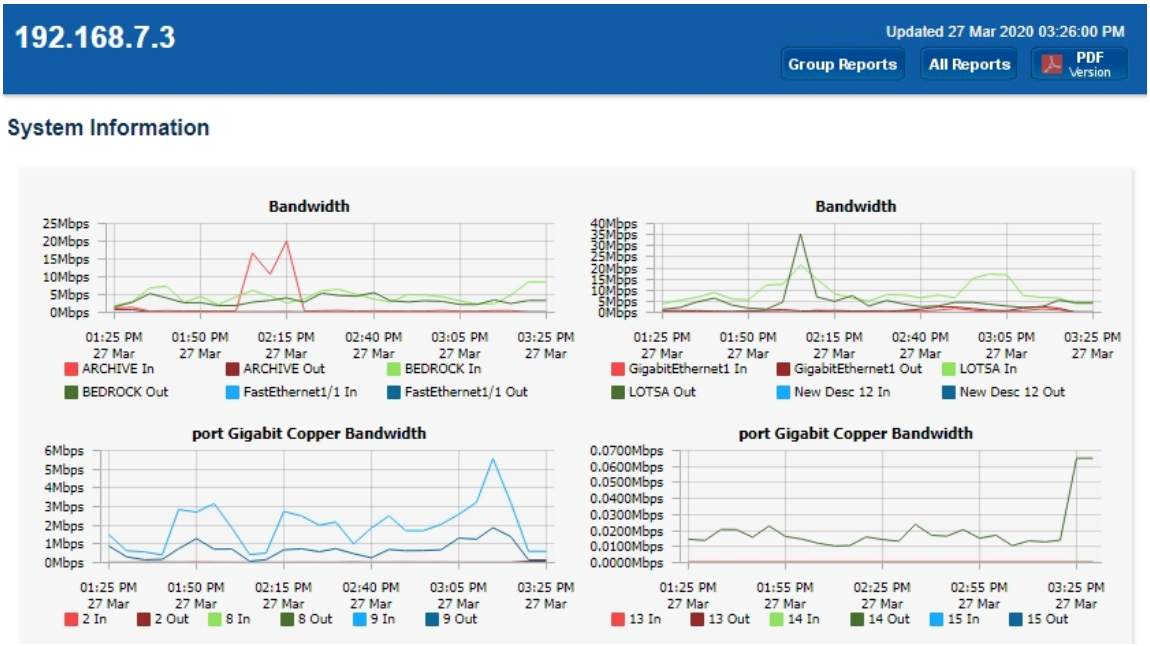
All Reports | PDF Version

Inventory Details

Server/De...	OS: Name	OS: Versi...	Upt...	Uptime...	Win...
BANTHA	Microsoft Windows Server 2012 R2 Standard	6.3.9600	N/A	99.658	0
ARCHIVE	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition	5.2.3790	N/A	99.985	0
BALROG	Microsoft Windows Server 2012 R2 Standard	6.3.9600	N/A	100	0
CLEAN2016	Microsoft Windows Server 2016 Standard	10.0.14393	N/A	100	2
ABCLIVEDEMO	Microsoft Windows Server 2012 R2 Standard	6.3.9600	N/A	99.995	0
LOTSA	Microsoft Windows Server 2012 R2 Standard	6.3.9600	N/A	100	0
Q	Microsoft Windows 10 Enterprise	10.0.14393	N/A	99.946	N/A
RANCOR	Microsoft Windows Server 2012 R2 Standard	6.3.9600	N/A	99.995	0
192.168.7.12	VMware ESXi	6.5.0	N/A	100	N/A
192.168.7.40	Dell	N/A	N/A	100	N/A
192.168.7.3	24G	N/A	N/A	100	N/A
192.168.7.7	N/A	N/A	N/A	N/A	N/A

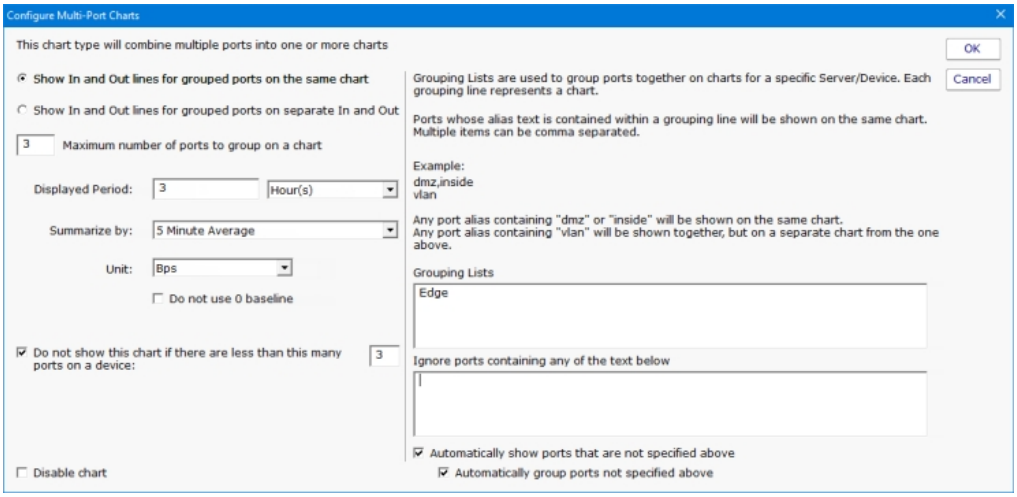
Multi-Port Charts

For devices that have many ports (routers, switches, etc.) the Multi-Port Chart can display in and out bandwidth charts in an efficient way to get as many ports on the screen as possible.



In the image above, In lines are on one chart, and Out lines are on a different chart. The background color of the charts visually tie the In and Out port lines together.

The chart is configured by adding a custom chart to the server as described in configuring Server Status Reports. When you are ready to configure the Multi-Port chart, you will see a dialog like the one below:



Web Report Access

PA Server Monitor can optionally require a user login in order to view reports via HTTPS. This is configured in Report Settings.

Once reports are password protected and SSL is enabled, you manage who can view reports via Remote Access Users. This is the same place where remote Console access is configured as well.

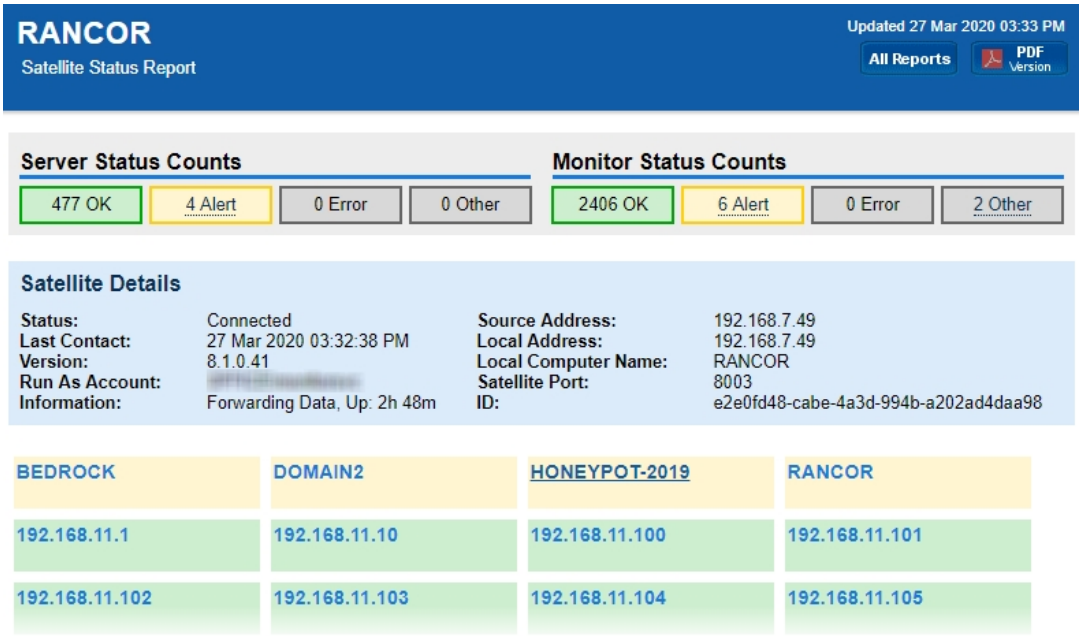
If you are an IT service provider and want to give your clients web access to their reports, set:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor
[DWORD]Reports_DisableNavButtons = 1
```

This will remove navigation links from the reports so clients won't be able to browse to other clients' reports. Naturally navigation within the Console will be unaffected.

Satellite Status Report

The Satellite Status Report is a quick way to check basic stats on a remote Satellite Monitoring Service.



Like many reports, there is a timestamp showing the report generation time in the upper right, along with buttons to take you to the table of contents, and to generate a PDF of the report.

Below the report header is a row of boxes giving quick counts of servers and monitors that are run by that particular Satellite Monitoring Service, and their status.

The blue Satellite Details box gives information about the Satellite, it's status, remote (at the remote site) computer name and IP address, etc.

Below the Satellite Details box will be a group of colored boxes, where each colored box represents a computer being monitored by this Satellite. This group of boxes is show the individual servers' status and operates just like the All Servers Report.

If the Satellite still needs to be accepted, a large yellow box will indicate that status and give instruction on how to accomplish that task.

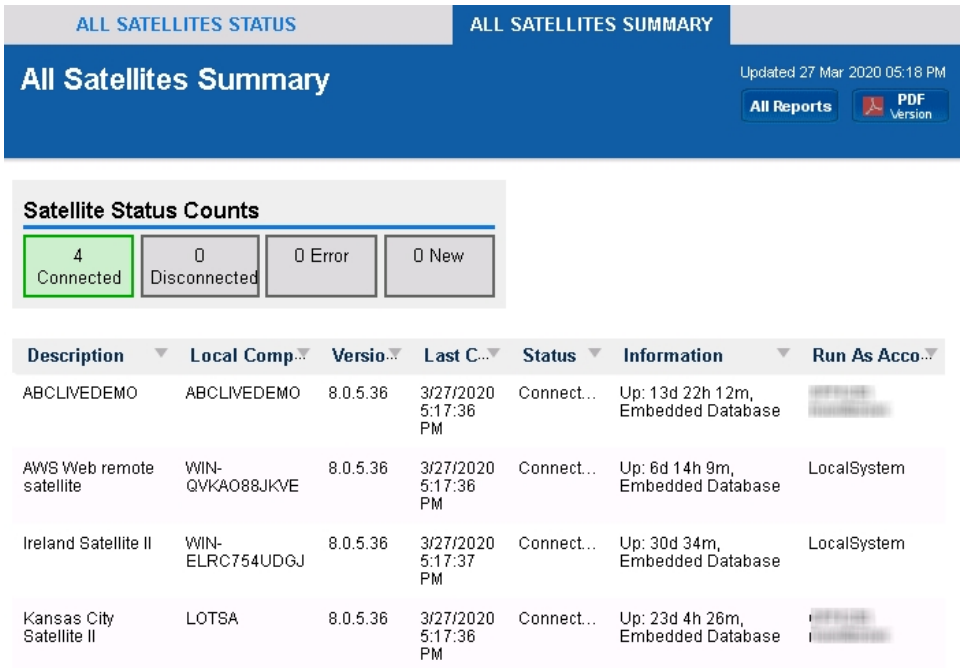
Satellite Status Report

There are two reports to show the status of multiple Satellites at once: The All Satellites Summary, and the All Satellites Status. You can switch between these two reports via the two links in the grey bar above the blue title bar.

These reports are accessed by clicking on the SATELLITE SERVERS node in the Satellite Services category on the left of the Console.

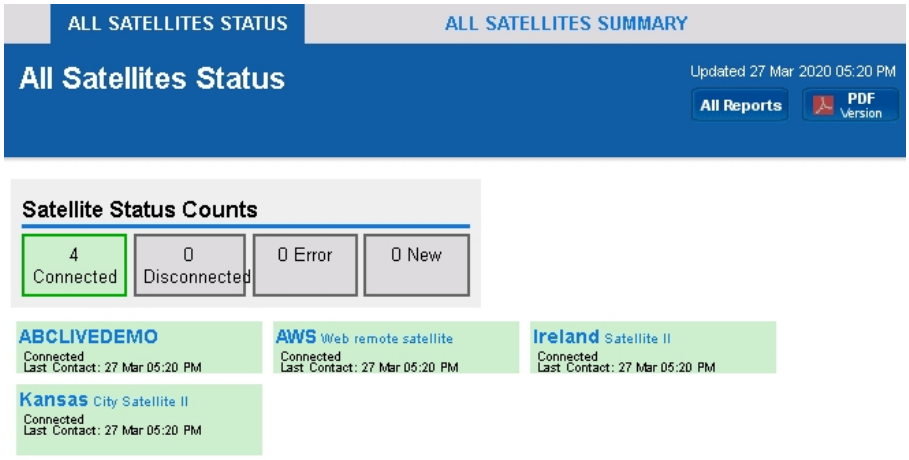
All Satellites Summary

This report lets you quickly see the status of all of your remote Satellite Monitoring Services, and easily shows if they are all on the same software version (sort by the Version column to quickly find Satellites with different versions).



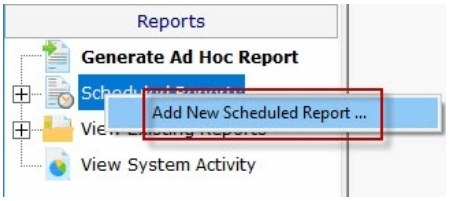
All Satellites Status

This report uses the familiar metaphor of showing each Satellite as a separate box. The color of the box indicates the Satellite's connection status (green = connected, yellow = disconnected). Disconnected Satellites will automatically float to the top to draw your attention to them.


ALL SATELLITES STATUS
ALL SATELLITES SUMMARY
All Satellites Status
Updated 27 Mar 2020 05:20 PM
All Reports
PDF Version
Satellite Status Counts
4 Connected
0 Disconnected
0 Error
0 New
ABCLIVEDEMO
Connected
Last Contact: 27 Mar 05:20 PM
AWS Web remote satellite
Connected
Last Contact: 27 Mar 05:20 PM
Ireland Satellite II
Connected
Last Contact: 27 Mar 05:20 PM
Kansas City Satellite II
Connected
Last Contact: 27 Mar 05:20 PM

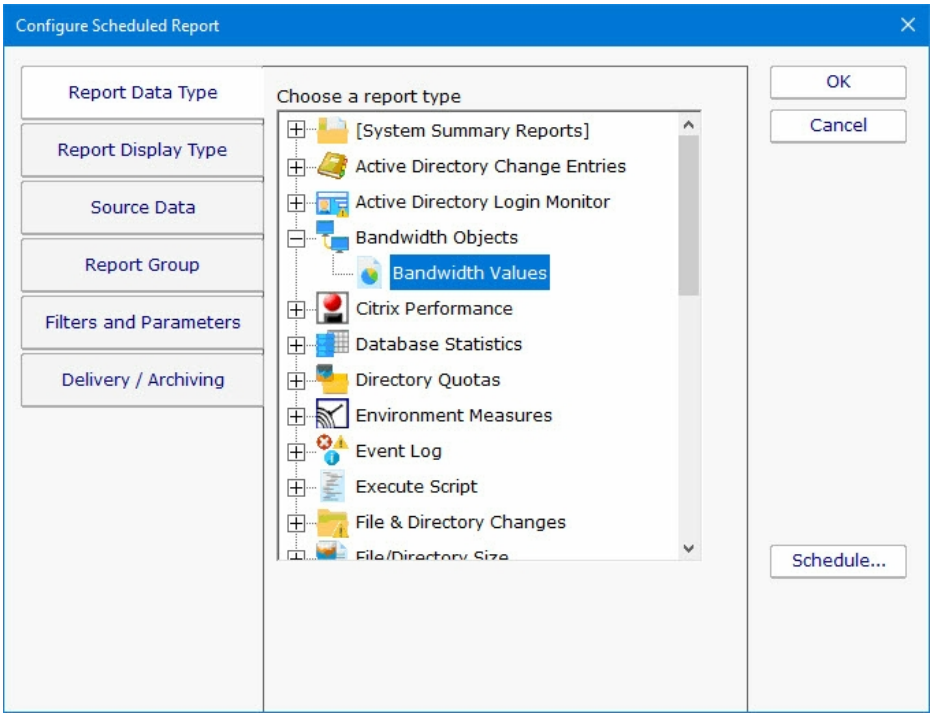
Scheduled Reports

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)

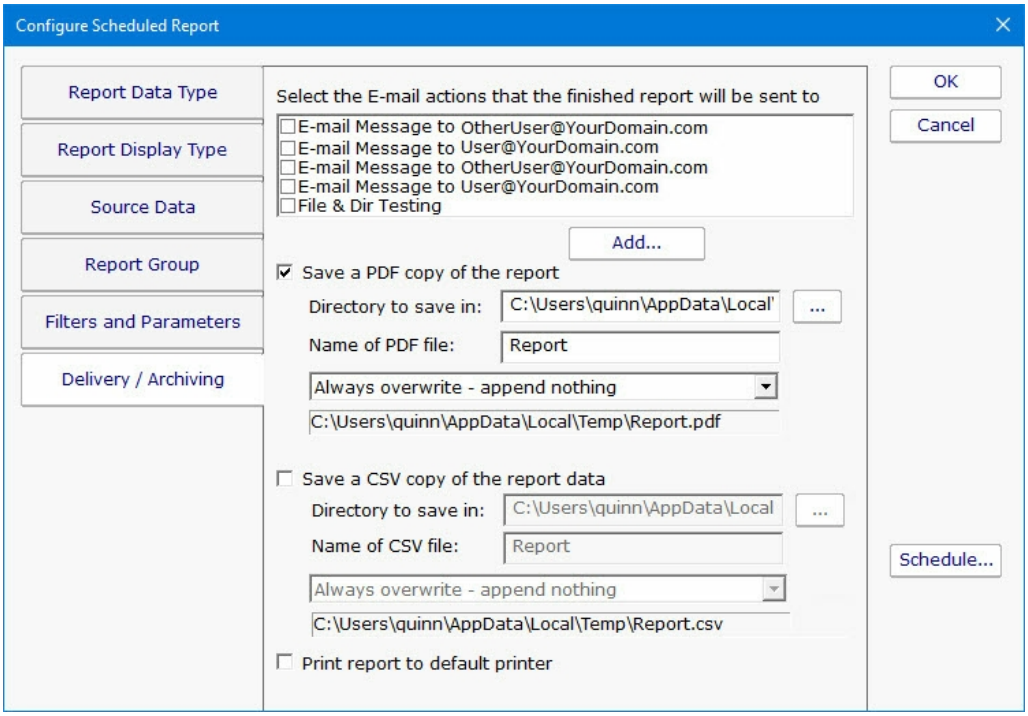
Just like with ad-hoc reports, you choose a monitor-type that sourced the data you want to report on, a report type (chart, tabular, CSV). You also choose a specific dataset to report on. Near the bottom of the dialog you specify reporting parameters that are unique to that report. More detail is given 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 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.

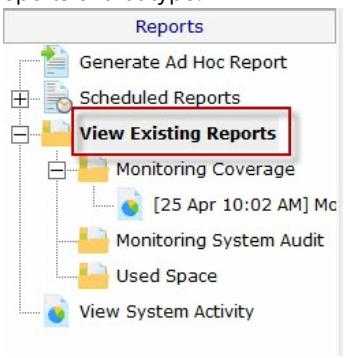
At the bottom of the dialog you will see the familiar Schedule button. It works the same way as the Schedule buttons in the monitors. You can easily specify how often the report is run.



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

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.

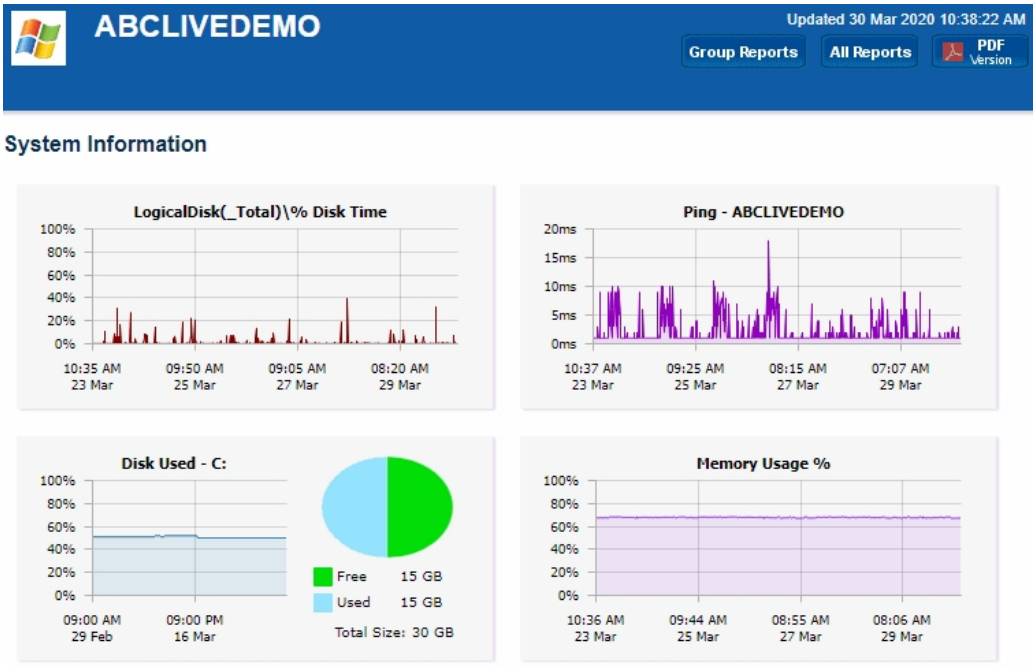
Double-check the Filter and Parameters tab for other settings. Some times the parameters end up excluding data that you want.

Make sure the data set selected in the Source Data tab is what you expect.

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.



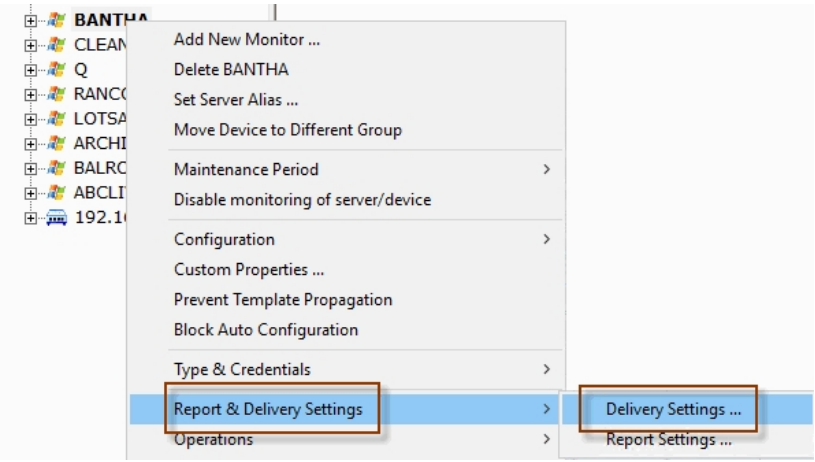
In the System Information area are some optional charts. The graphs will probably be different than the ones shown above. The charts are automatically created based on data collected by the running monitors. That means if you want to see a Disk Space chart for example, a Disk Space monitor needs to be added to the server to collect the data for the chart.

When you scroll down past the charts, there may 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. (Note: Getting WMI working can be tricky. Many customers opt to disable WMI polling completely, with the only side-effect being that the blue System Details block above is not shown. Monitoring and alerting does NOT depend on WMI at all).

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 column 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 an Ultra, 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 Settings -> Delivery Settings.

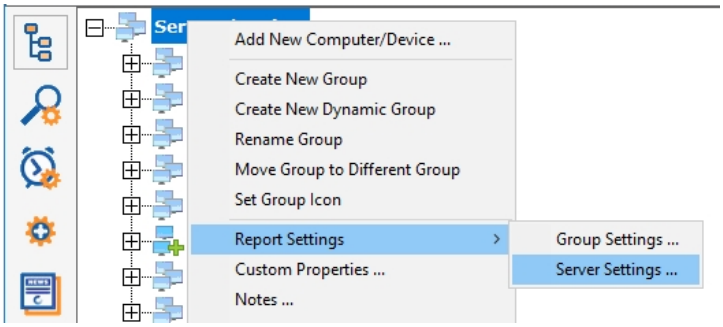


If you are a Managed Service Provider, use Filter User Access at Settings -> Remote Access to control which servers and devices your customers can see.

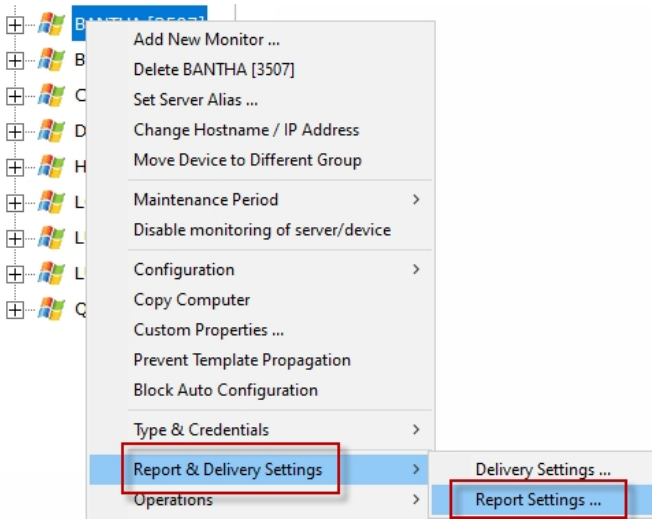
Configuring Server Reports

In this menu you can select the sections of the server report that you want to appear, and configure aspects of each section (i.e. which charts show up.)

To start, you select the Group for which all contained servers reports will be edited, and right-click to choose Report Settings -> Server Settings...

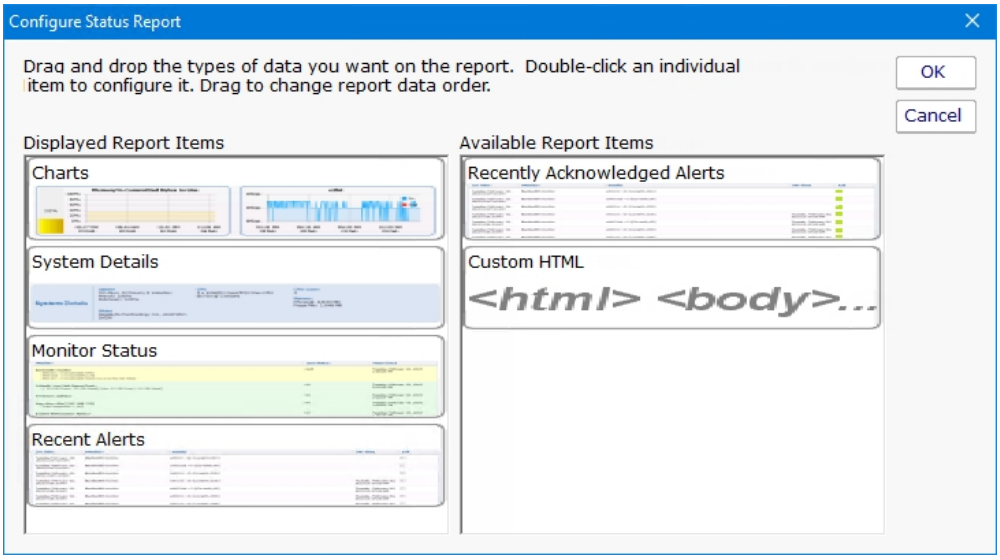


... or select a specific computer and choose Report & Delivery Settings -> Report Settings.



Report Parts

Opening either menu entry will show you the dialogue below. Here you can drag and drop the different report sections to control whether they are displayed or not, as well as their displayed order. In this example, the Custom HTML part of the chart will not be displayed.



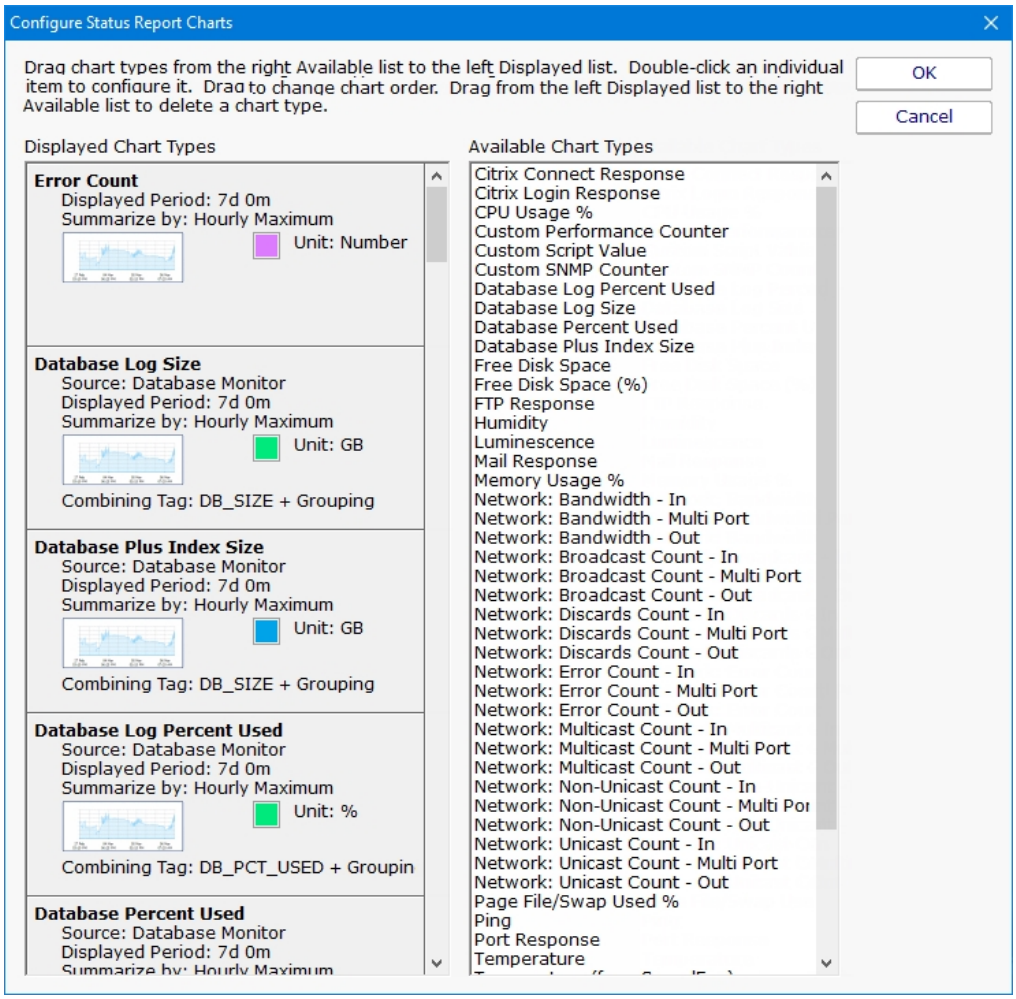
Double-click on a report item to configure settings for that report item.

Configuring Charts

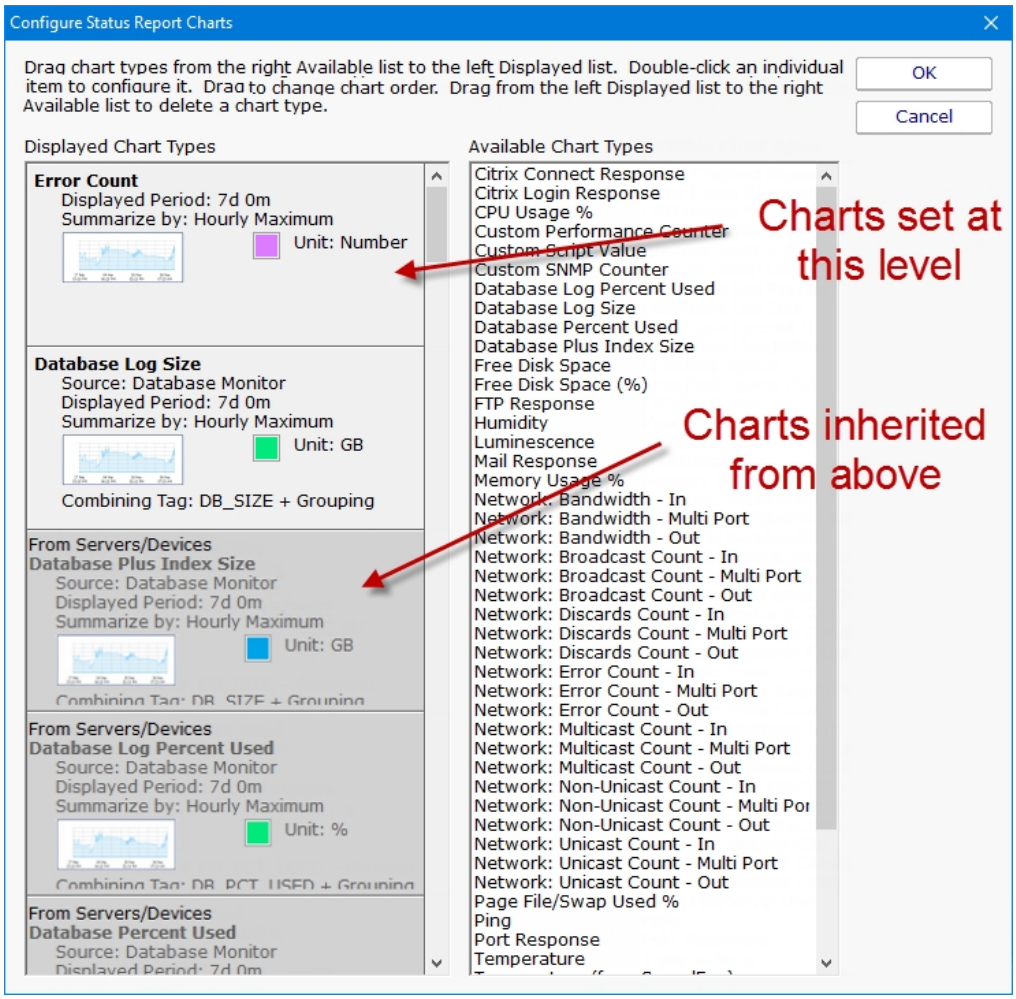
Double-clicking the Charts report type will show the dialogue below. This is where you have great flexibility in defining the charts that are displayed for a server/device. Similar to the Report Parts dialog, you can drag and drop items back and forth between the right and left lists. You can also change the order of the items on the left side by dragging and dropping them.

Note: If a chart is defined, but that particular type of data is not available for a server/device, the chart will not be displayed. It's OK to define charts that some servers will and wonÃƒÂ¯Ã‚Â¿Ã‚Â½t have.

(Available chart types will vary based on the product and license you are using)



The above Configured Status Report Charts menu is an example of how the menu will appear when you select the menu from the Servers/Devices node. All of the chart types listed at this level are available to all servers/devices under this node.



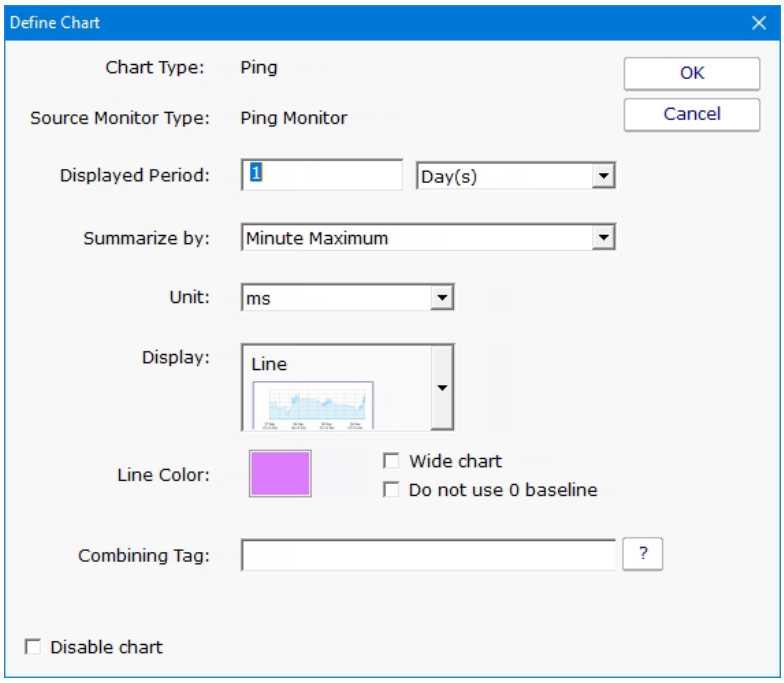
The above Configured Status Report Charts menu is an example of how the menu will appear if you select the Configured Status Report Charts menu at a group or server/device level. Note the different shaded chart types. The darker shaded charts are inherited from a group above. The lighter shaded charts are charts set at this level and will be available to servers/devices below this level.

Adding Charts - To add charts to the server status report, choose one of the chart types from the Available Chart Types and drag it to the left side. Remember that if you add a chart, there needs to be a monitor that collects the data to be able to display the chart. Edit the parameters as needed.

Editing Charts - Double-click on any individual chart type to change its properties, including the number of days to display, the granularity of individual data points, line color and more.

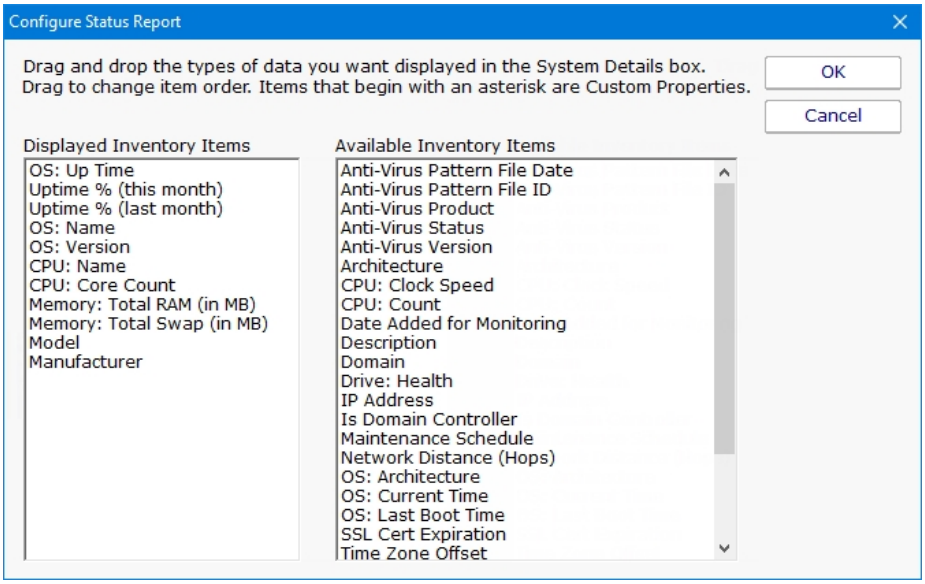
Inherited Charts - If you want to change an inherited chart type you should navigate to a higher node where it was created. If you want to disable this chart for this node and below, double click on it and check the Disable Chart check box. If you find later that you want this chart to be shown again, simply drag it off to the right side and it will be inherited again.

Custom Charts - To create custom charts, choose one of the Custom chart types (depending on which monitor is collecting the data that you want) and drag it to the left side. Be sure to fill in the Filter parameter -- this is a simple piece of text that will be matched to all statistics being monitored on the target server, and if it matches, that statistic will be charted.



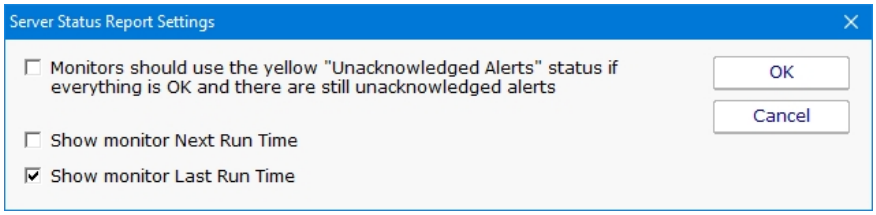
Configuring System Details

The blue System Details box can be customized to show any fields that the Inventory Collector monitor puts into the database. Drag and drop to show or hide, and to change the order of displayed fields.



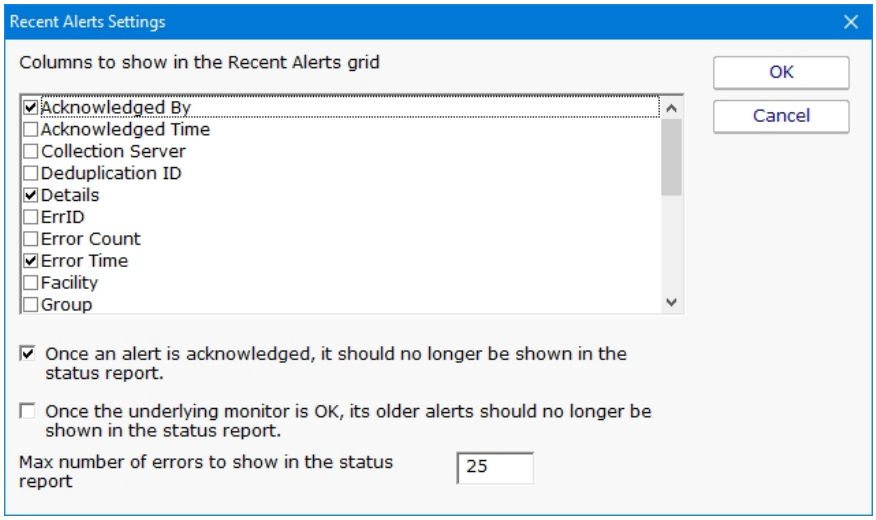
Configure Monitor Status

The Monitor Status grid displays monitors for a server and their current status. You can configure whether a monitor's errors have to be acknowledged before it is allowed to show green after having been yellow. Also, you can select to either show the monitor's "Next Run Time" or "Last Run Time". This is part of the Error Auditing system.



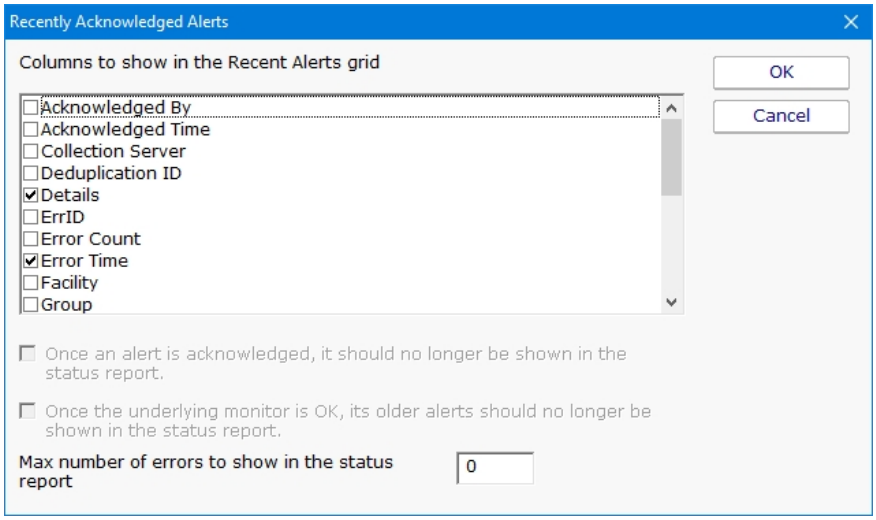
Configure Recent Alerts

Here you specify what columns appear in the alert grid, how many recent errors to show, and whether the errors should be acknowledged or not as part of an Error Auditing procedure you might use at your location.



Configure Recently Acknowledged Alerts

This menu works the same as the Recent Alerts menu with the exception that you can't select either of the two options on the bottom of the menu.



Configure Custom HTML

When this menu is double clicked a text file will open. This text will allow you to enter HTML code that will be placed on the server status page in the position listed on the left side of the Configure Status Report. To save the file, select the save option in your text editor and the page will be saved to the correct location.

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

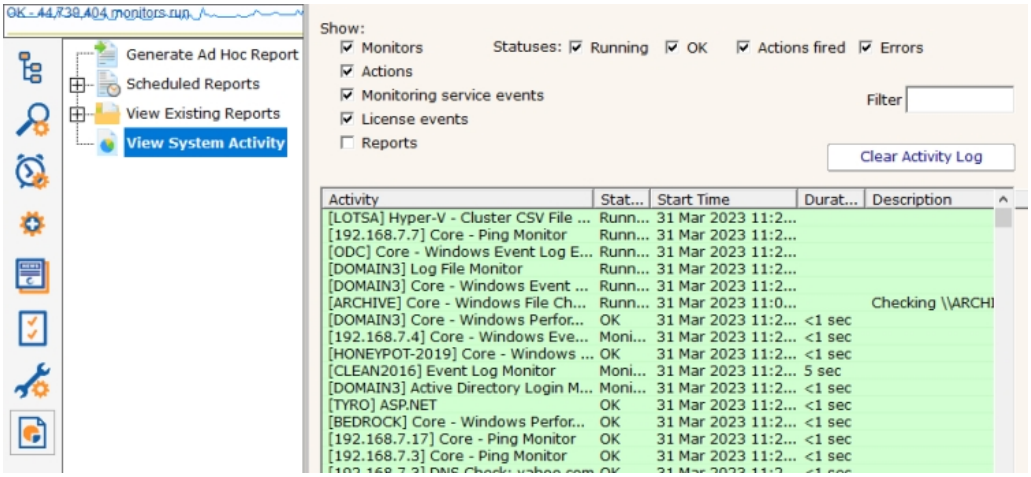
Monitoring service start and stop events

License events (new licenses found, license mode being used, etc)

Reports generated (automatic or ad hoc)

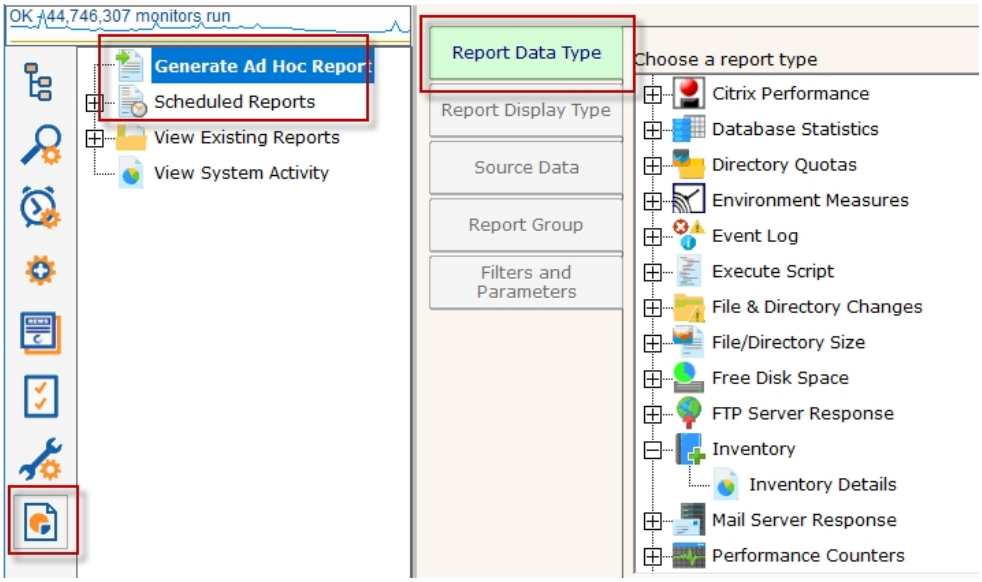
When you view the running system, you'll notice that running monitors have a start time, but no duration since it hasn't finished yet.

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.

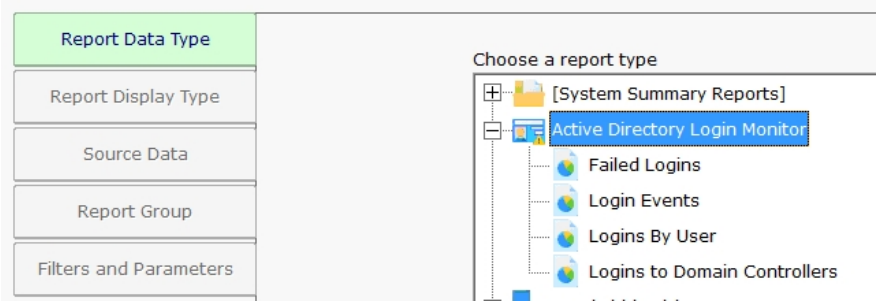


Standard Report Tabs

Running a report in PA Server Monitor is very easy. You start by going to the Reports node, and then to either Generate Ad Hoc Report, or right-click on Scheduled Reports.



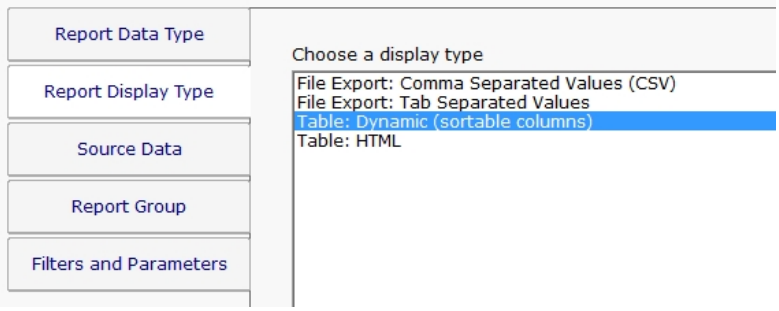
On the right side are all of the different report types. In general you would want to go to the monitor that is collecting the data that you want to run a report on. In this example we'll select the Active Directory Login Monitor. You might have different monitor/report types listed based on your product and license.



Once you've selected the report type, visit each of the tabs on the left to make selections.

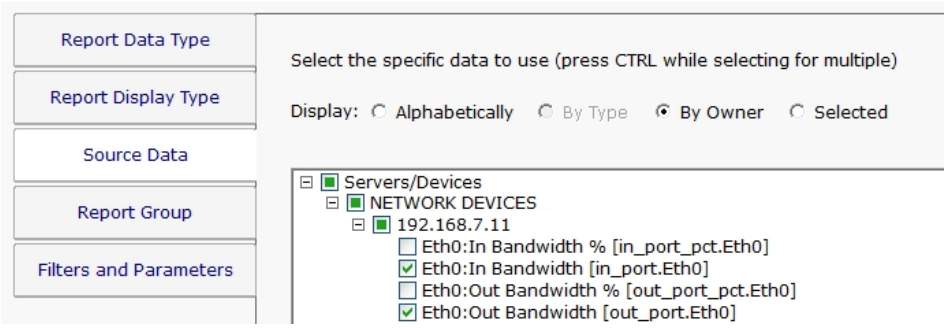
Report Display Type

The Report Display Type tab lets you select the output format for the report. The "Table: Dynamic" is a popular report format that shows a dynamic table in the output. For very large reports (thousands of lines of output), the CSV report might be preferred as Excel usually handles large amounts of database better than a browser.



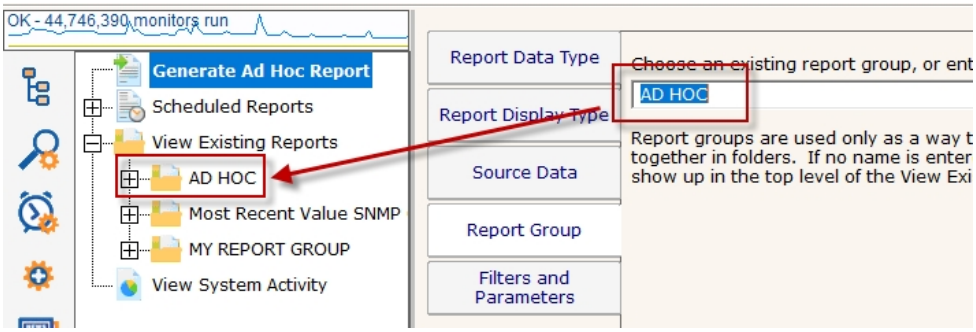
Source Data

The Source Data tab is where you select which data set to use. For some report types there might only be a single selection. For the image below we chose the Bandwidth monitor report type in order to show how this looks when there are multiple data sets to choose from.



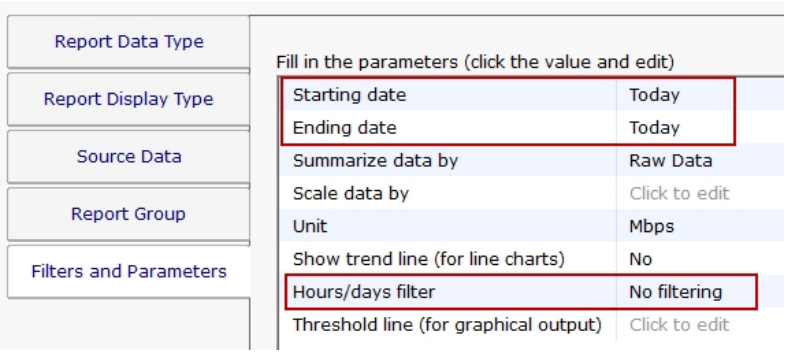
Report Group

Report Groups are an easy way to get similar reports grouped together. This is purely for your organizational use. If the value is left blank the reports will get added to the Ad Hoc group. This is most useful for cases where there are many Scheduled Reports that a group of people will refer to often.



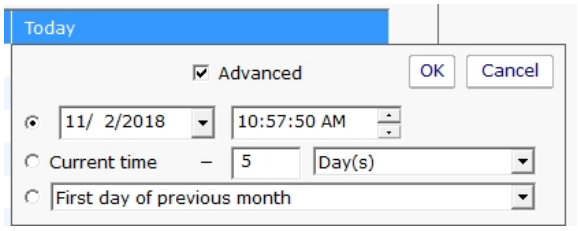
Filters and Parameters

The most important tab for most reports is Filters and Parameters. This is where you really define what the report should show. The list of fields shown will be different for each report type. Most reports have a few fields in common:

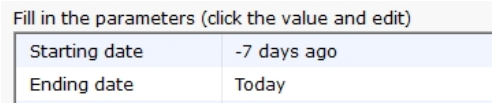


Starting Date
Ending Date

These two fields specify the time frame for the report. The order of the times doesn't matter - they will automatically be re-ordered if needed. Clicking the date gives the typical date selector control, and clicking the Advanced box expands the selection so also specify specific times, or relative times from today.

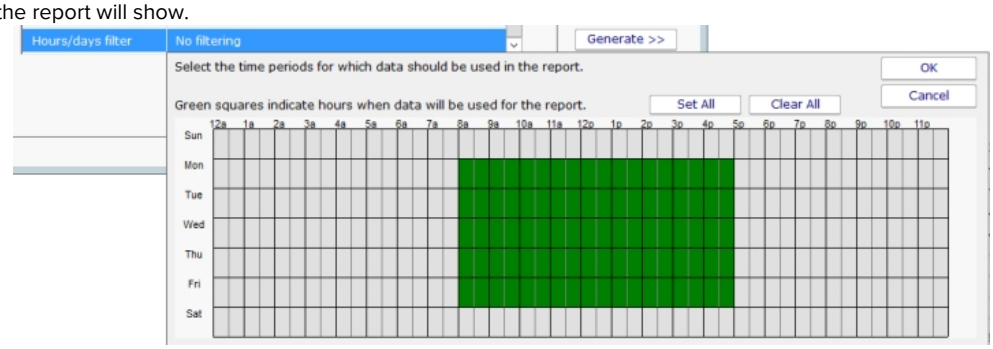


Once you've made your selection, the date is converted into a relative date from today so the report can be run on any date to give the desired results.



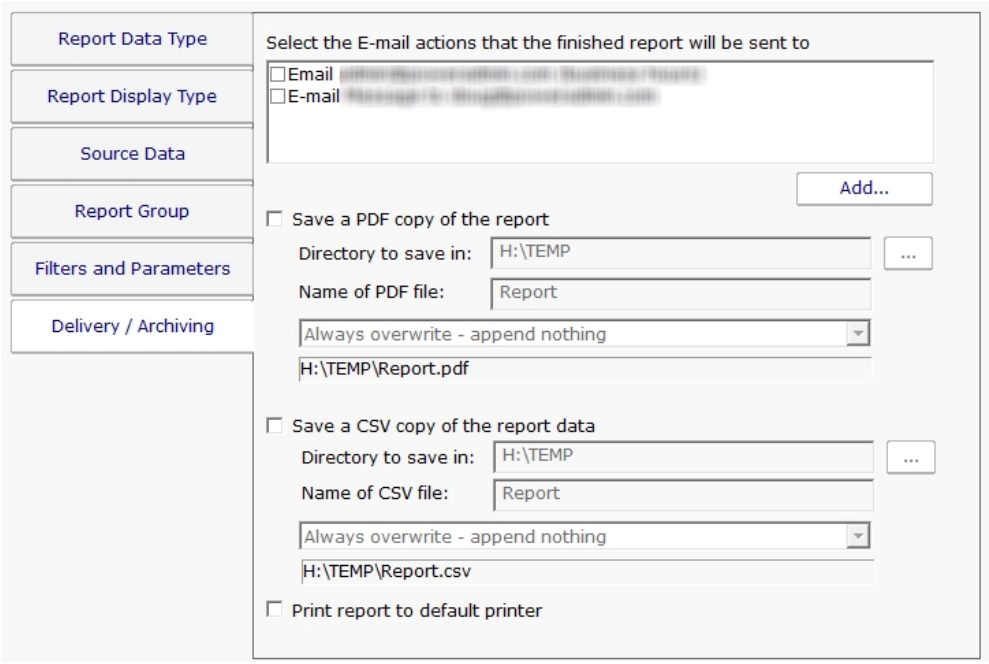
Hours/days filter

If you need a report to only a specific part of the week (only work hours for example), you can do that with this field. The green/dark cells are the period of time the report will show.



Delivery / Archiving

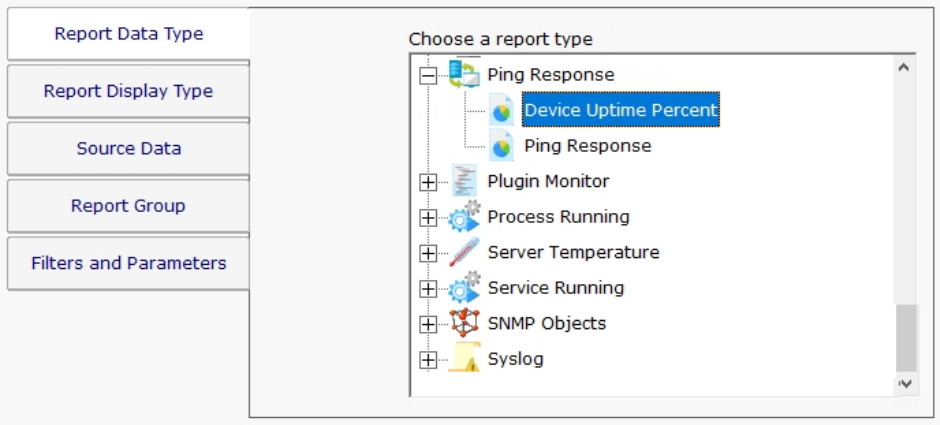
If you choose to create a Scheduled Report ran than running an Ad Hoc Report, there is an additional tab for emailing the report and/or saving the report data.



If saving a CSV or PDF file, it is recommended to save it to a local drive. If it must be a remote drive, specify the folder using a UNC path as mapped drive letters are not available to service processes.

Uptime Reports

Many of the monitors (Ping monitor, Web Page monitor, Service and Process monitors, etc) support an Uptime Report.



What is Up?

Most of the Uptime Reports let you define what 'up' means. In the case of monitors that collect timing data like the Ping monitor and the Web page monitor, you define up in terms of response time. For example, you might define 'up' as being a response within 500ms.

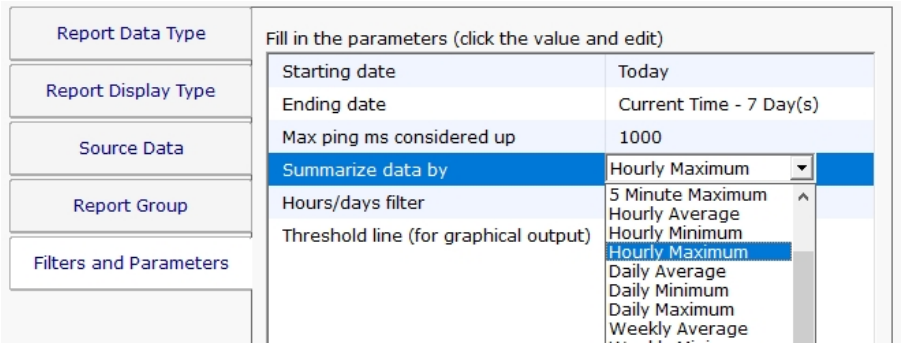
Data Summarization

When running an Uptime Report, it is important to understand the data summarization choice. Basically the data that you choose is grouped into periods that you choose, and a value is derived from each group. Periods can be Hourly, Daily, Weekly and Monthly, and the grouping operation can be Minimum, Maximum and Average. So for example:

Daily Average: Take the average value for each day

Hourly Minimum: Take the minimum value for each hour

Monthly Maximum: Take the maximum value for each month

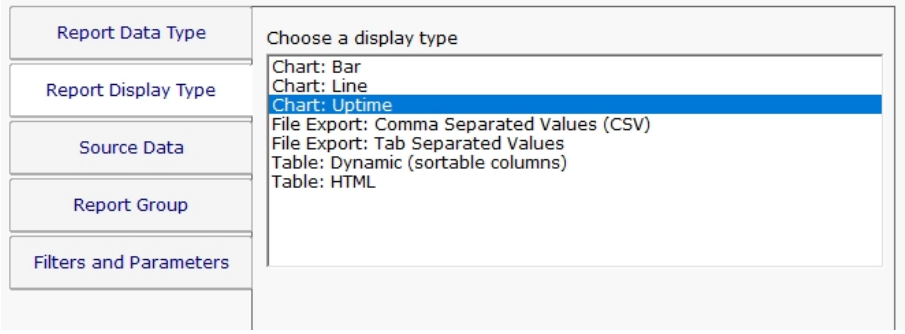


With Ping for example, a lower value is typically better, so you would typically want to see the Maximum value (ie, run a report to see the worst performance in a period). Looking at the Minimum might be hiding a lot of bad values that occurred. So if there was a single value of 1 ms in the time period, the Minimum would return that value, making the time period look good. On the other hand, if there was a single value of 800 ms in the period, that value would be returned with the Maximum selection, indicating a problem in the time period.

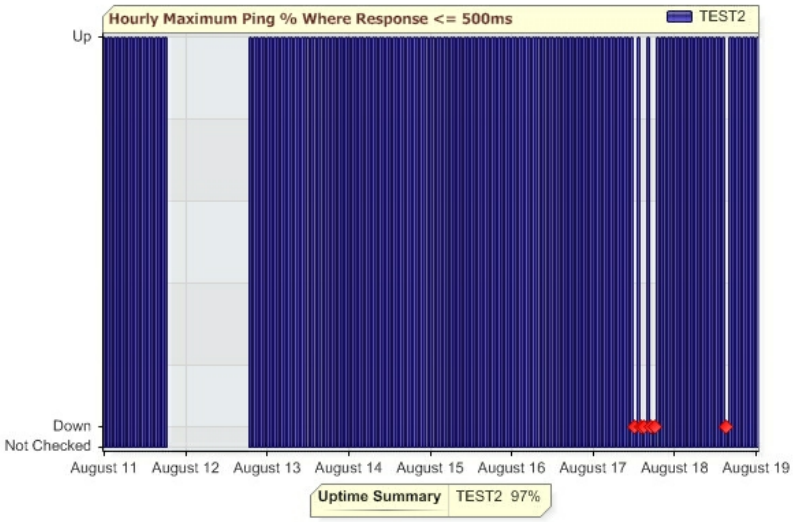
One thing to keep in mind a very high sentinal value used by some monitors (Ping and Web Page monitor specifically) that is used to indicate a failure to get any response at all. For Ping, this value defaults to 30,000 ms. For Web Page, it is 90,000 ms.

Visual Output

When you run an uptime report, you can output the data in tabular form, bar chart or line chart. In these cases, 'up' is the value 100, and 'down' is the value 0.



You can also choose to output the report as an Uptime Chart. This is a bar chart that shows 100% up with a bar going all the way to the top. If there was a down even, a red diamond is shown. If the monitor didn't run at all during a period of time, there will be no bar for that period.



The report above indicates monitoring was stopped around August 12th for about a day, and a few down events that occurred on August 17th and August 18th.

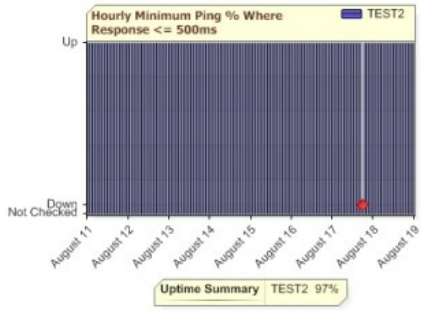
Uptime Summary

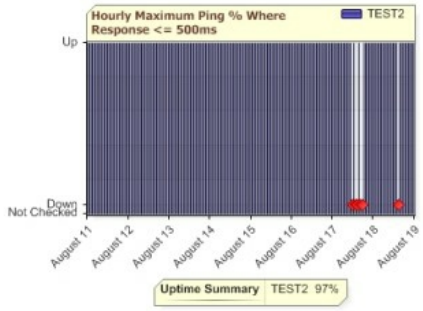
The Uptime Summary statistic is shown at the bottom of the Uptime Report. The value is calculated by tallying up each measurement one minute at a time across the entire time range. If there are multiple values for a minute, those values are averaged. If there is a minute with no data, the value for the previous minute is used (this can take place for multiple minutes with no data). Each minute's value is compared to the 'up' definition and assigned a value of 100 (100% up for that minute) or 0 (completely down for the minute). Then the average across the whole time range is computed and displayed.

Note that the Uptime Summary DOES use the definition of 'up' (ie < 500ms in our example), but it does NOT depend on the Hourly/Daily/Weekly/Monthly or the Minimum/Maximum/Average charting choices -- it attempts to give the true uptime over the

specified period.

For example, look at the two charts below. The chart on the left uses Hourly Minimum, which means if there is a good ping response in the hour, the whole hour is recorded as 'up'. The chart on the right uses Hourly Maximum -- if any ping is over the threshold, that hour is shown as 'down'. Although the charts look different, the Uptime Summary statistic is the same in both.

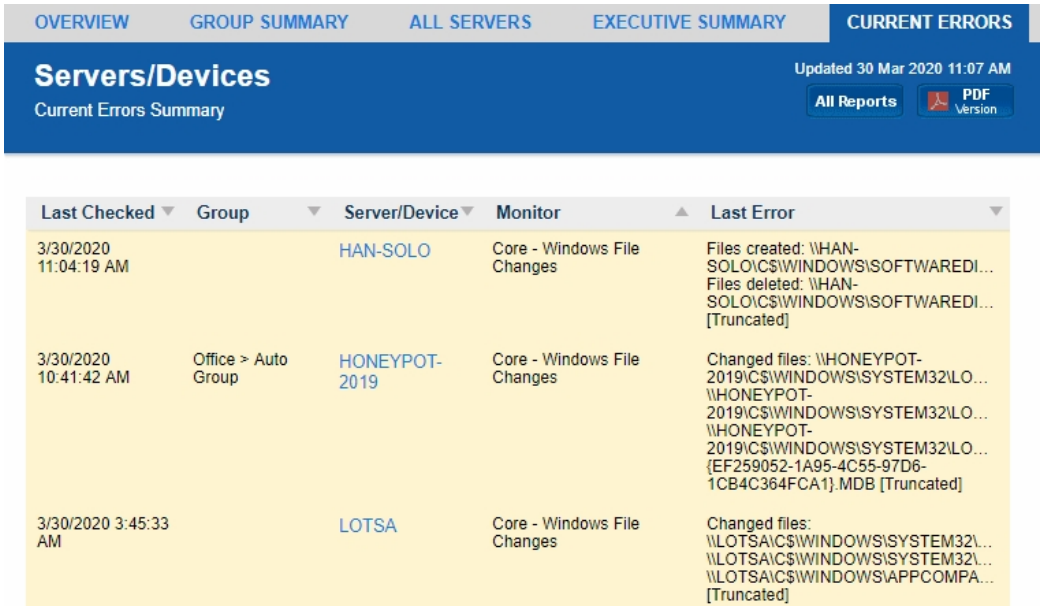




CAVEAT: Note that the Uptime Summary assumes that the monitor was running for the entire time. If monitoring was stopped, that can show up in the chart, but the statistic will use values from the previous minutes in the calculation.

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.



Group status reports can be configured to auto-rotate among reports. See Group Report Settings.

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

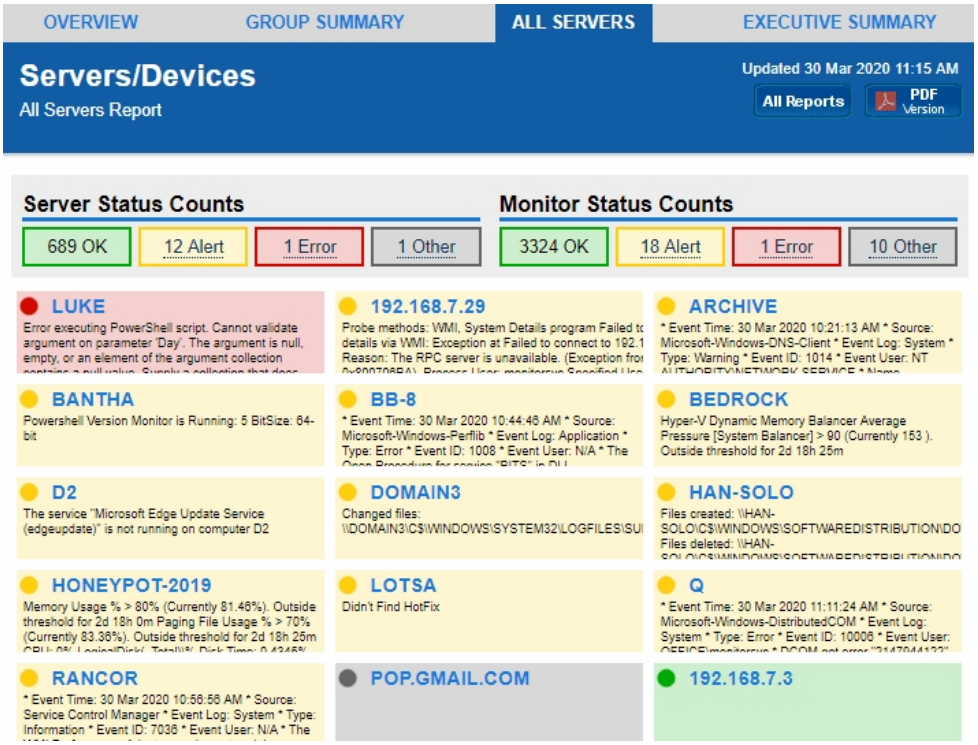
All Servers Report

This 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.

For IT departments that mount a large screen on the wall for everyone to keep track of server status, this report is the most popular for display.

Group status reports can also be configured to auto-rotate among reports. See Group Report Settings.

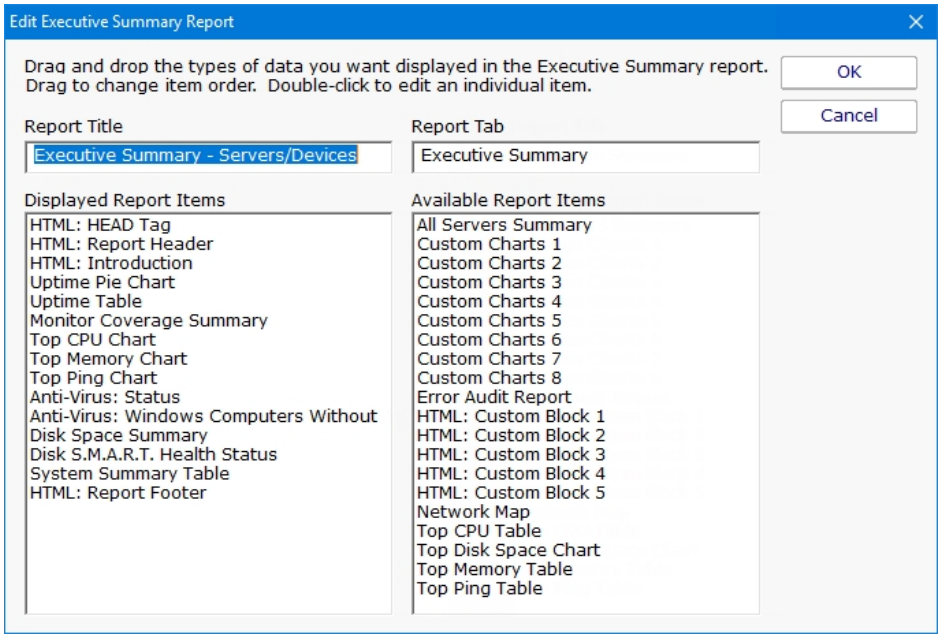
The display will add additional columns as the browser window gets wider in order to show as many servers as possible. At the very bottom of the report is a URL that can be used for displaying the report in browsers or on different computers.



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

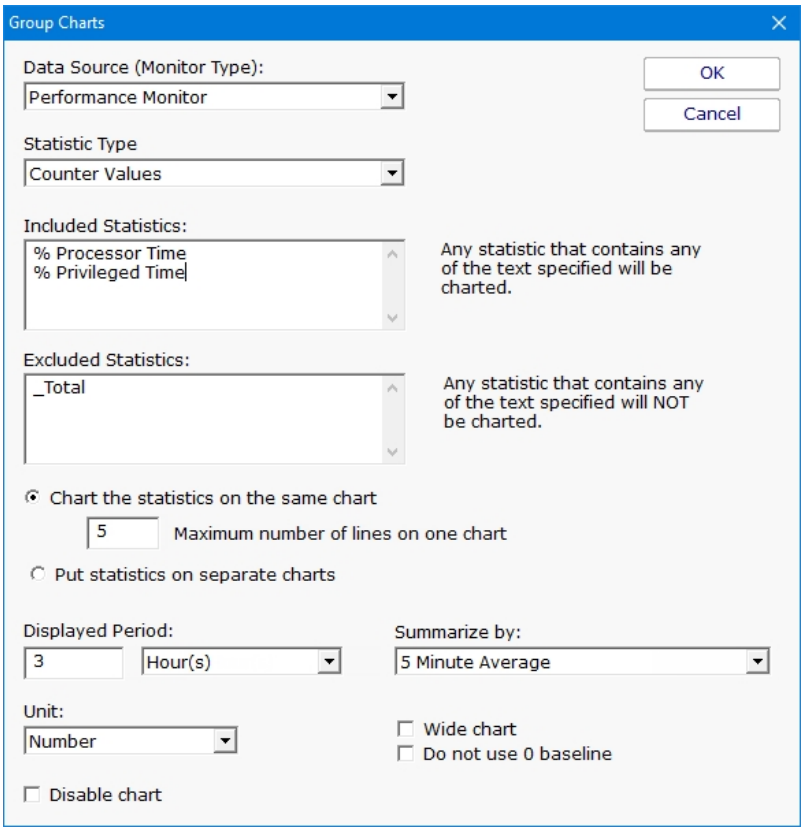
Custom Group Report

By right clicking a group and going to Report Settings -> Group Settings you will see three Custom Group reports and an Executive Summary report. They both allow you to add your own fields, charts and custom HTML blocks to the report to customize it to your needs.



A variety of report parts can be chosen. Some are pre-built charts while others let you specify counters that should be charted. To add a report part, drag the part from the right side and drop it on the left side. Double-click the report part on the left side to set parameters for that part.

Most of the report parts are self-explanatory. The Custom Charts parts are more complex and powerful and deserve some explanation.



The top box labeled Included Counters is where you will specify which counters should be charted. Any counter that contains text from any line in that box will be selected for charting. Since this is a group-level report, the statistic also has to come from a server within the group or sub-groups.

If you need to exclude a particular counter, you can enter some text and if that text is found in the counter name, that counter will be excluded.

For example, imagine you have the following counters:

```
\\SERVER\Processor(_Total)\% Processor Time
\\SERVER\Processor(0)\% Processor Time
\\SERVER\Processor(1)\% Processor Time
```

To show processor time for CPUs 0 and 1, but not for _Total, you would use:
Included Counters: % Processor Time
Excluded Counters: _Total

Once counters are specified, you need to choose how they should be displayed. If there are many servers in the group, the number of matching counters might be large, so there are simple settings to help you control the layout, how many charts are created, how many statistics are combined onto one chart, etc.

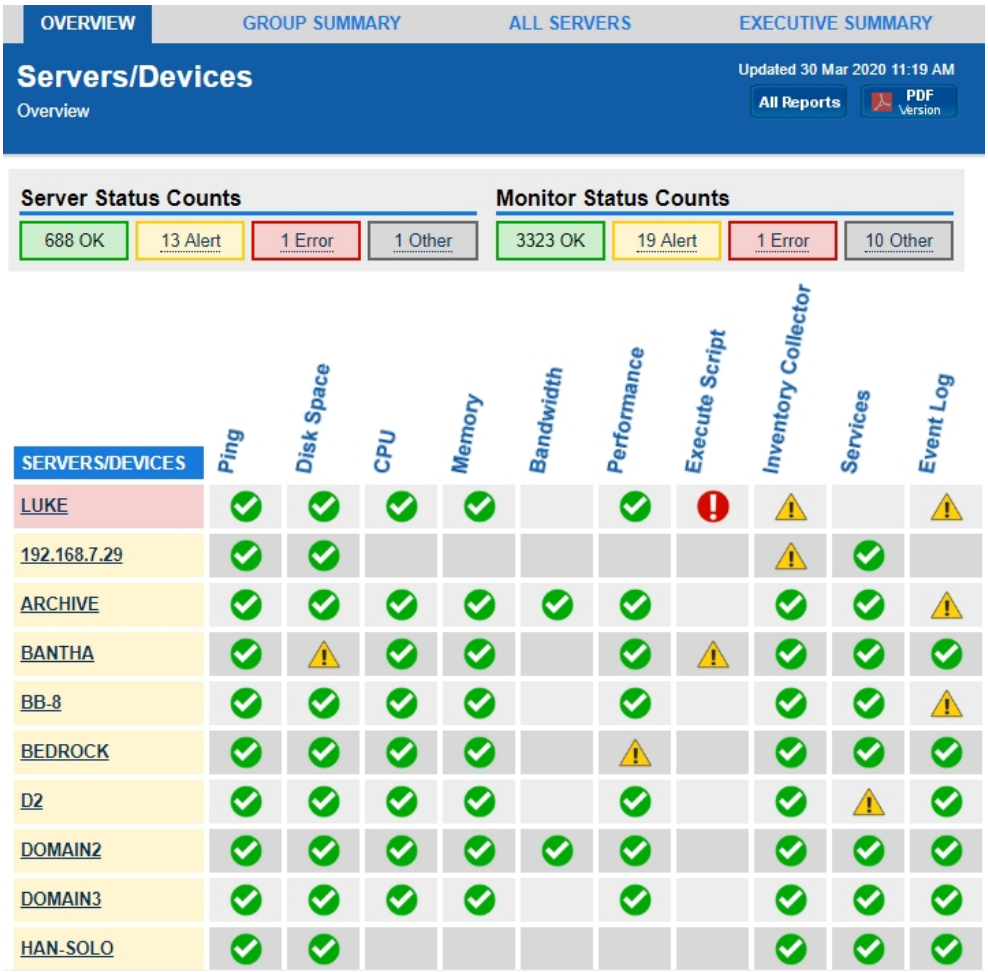
The Wide Chart setting will create a chart that is the full width of the report, instead of the smaller default chart size.

The y-axis on most charts starts at 0, but you can indicate the y-axis minimum value should be dynamically computed based on the data to be displayed. Sometimes this makes changes in large values easier to see.

If the chart is disabled, it won't be shown, but will be left as part of the report for future editing.

Group Overview Report

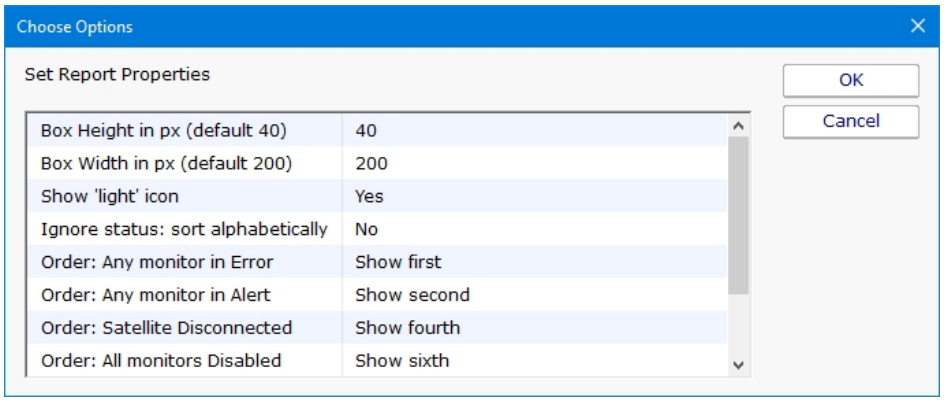
The Group Overview Report is a great mix of high level and detailed view. Here you can see servers and specific server health metrics along with monitor types. Problem servers are always floated to the top, so if a server isn't on the screen, you don't need to worry about it.



Green arrows represent a monitor with a healthy status. Yellow and red indicate a monitor has detected a problem. A grey clock means the server or monitor is disabled or in a maintenance period. If a cell is empty, it indicates that particular server/device doesn't have a monitor of the type specified in the column header.

Customizing the Report

You can configure the size of the the monitor box by right-clicking the group and going to Report & Delivery Settings. Select the Group Overview Report and click Edit Report Settings. While there you can also choose the order of the servers or change the sorting.


Choose Options
Set Report Properties
OK
Cancel
Box Height in px (default 40)
40
Box Width in px (default 200)
200
Show 'light' icon
Yes
Ignore status: sort alphabetically
No
Order: Any monitor in Error
Show first
Order: Any monitor in Alert
Show second
Order: Satellite Disconnected
Show fourth
Order: All monitors Disabled
Show sixth

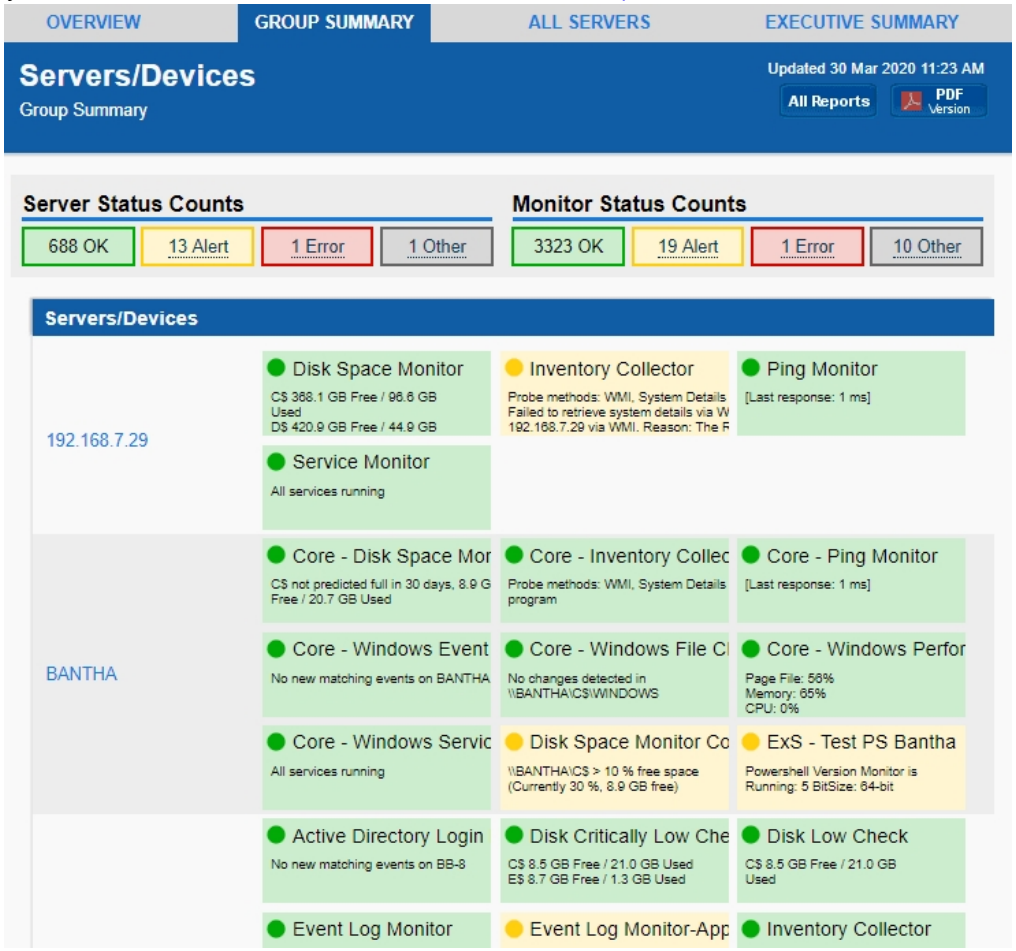
Group Summary Report

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.

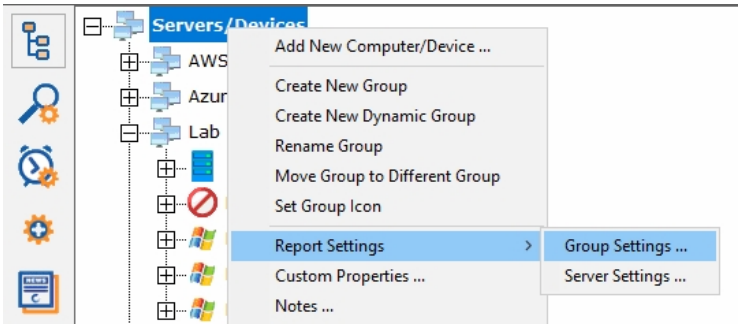
Moving downward you come to the group title bar for the current group. Within the group are the individual servers within the group, and optionally child groups will also be shown if there are any. Each server is represented as a line, with individual monitors on that server represented by boxes. The 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). See below for changing the box size.

You can click on any server name to be taken to that server's server status report.



Group status reports can be configured to auto-rotate among reports. See Group Report Settings.

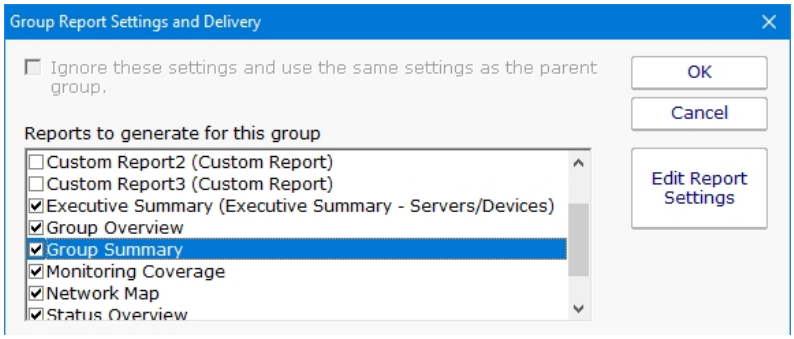
If you are using a Ultra, Pro or Lite license, you can also schedule the status reports to be emailed to you. Simply right-click on the group and choose Report & Delivery Settings.



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.

Customizing the Report

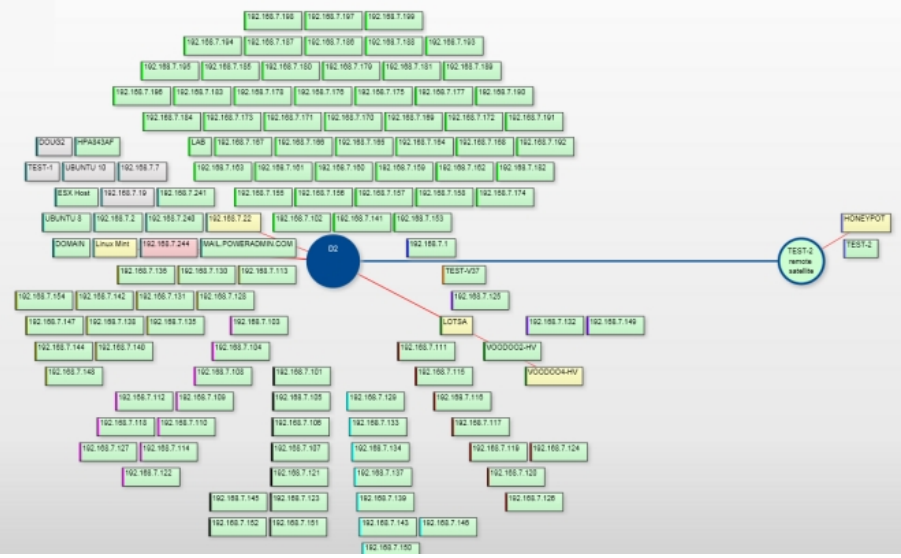
Some people like the level of detail available with a larger monitor box. Others want to get status about more servers on the screen. You can configure the size of the monitor box by right-clicking the group and going to Report & Delivery Settings. Select the Group Summary Report and click Edit Report Settings. You will be able to choose whether to show the title and additional details as shown above, or just the title, and how wide the title should be.



To see the most server statuses on the screen at once, use the All Servers Report

Network Map Report

The Network Map gives you a quick overview of the health of the network in a single view. All of the servers, including those at remote sites, will be shown on the report, and the report will automatically be resized to fit the report window.



In the image above, each box represents a server or device. The blue circles are monitoring stations. In this example, the solid blue Central Monitoring Service is D2. There is also a Satellite Monitoring Service (blue circle, fill green) named TEST-2.

The left edge of each box is colored. This helps to visually group the server boxes, which are also laid out according to group.

If a server is red or yellow, there will be a red line from the monitoring node to the box -- this helps identify which node is monitoring that particular server/device which may not always be as obvious as the example image.

If a Satellite is not connected, the Satellite circle will be blue, but filled yellow. All servers/devices monitored by that Satellite will also be yellow.

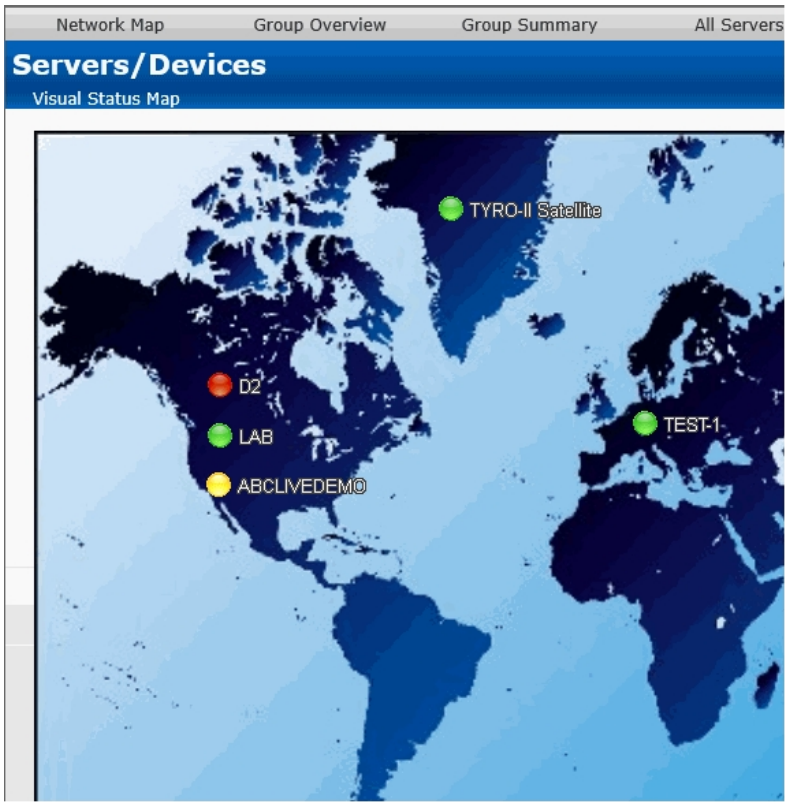
Clicking a box will take you to the Server Status Report for that server. In addition, you can view a Network Map for any group, and just that group's servers/devices will be shown.

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 beneficial in determining network problems that are geographically significant due to server locations.

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

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



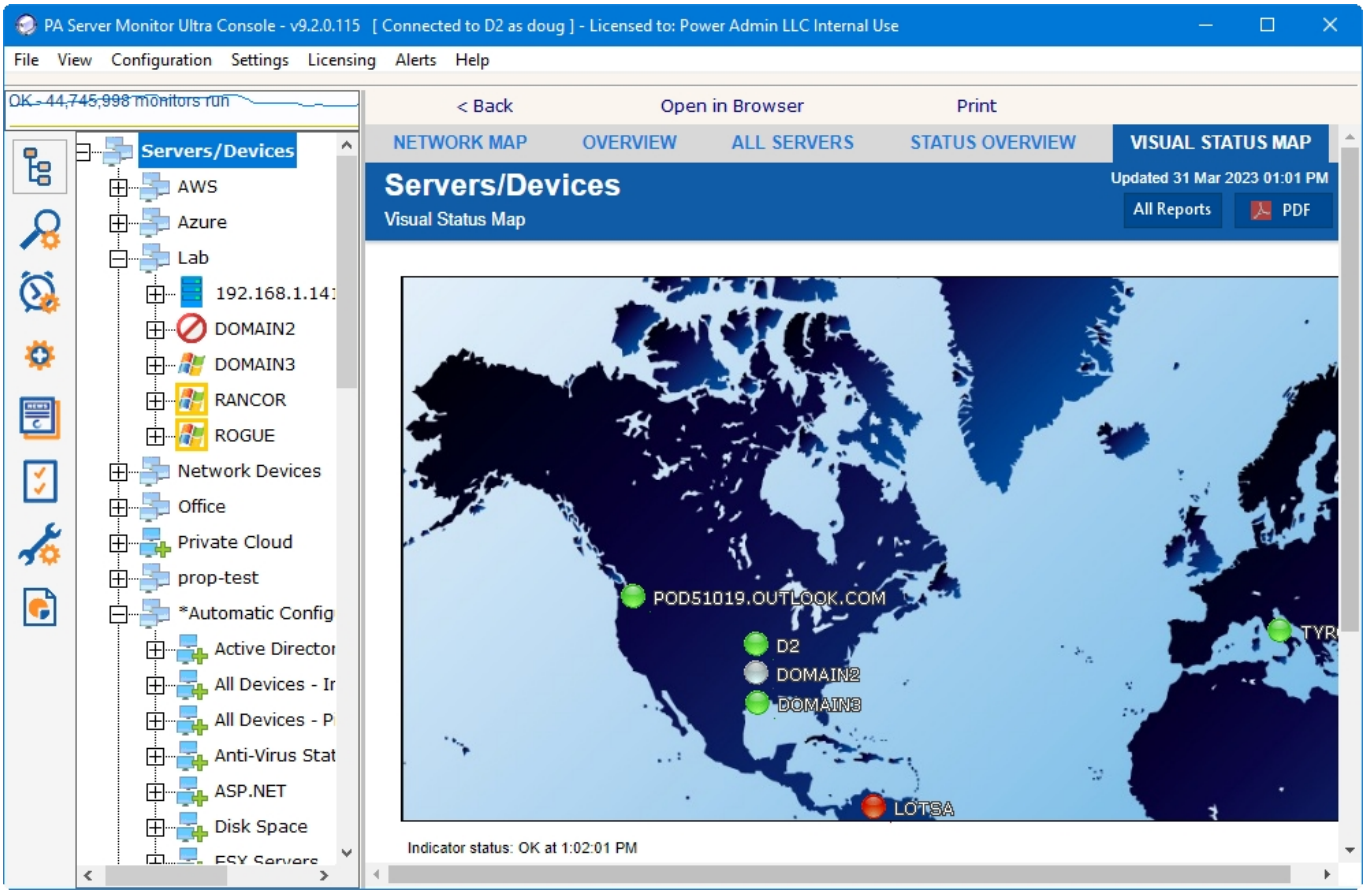
The map appearance and the positions and style of the status indicators can be configured in the Status Map Editor Dialog. There are several maps of different areas around the world, and you can also add your own map grapic.

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.

Group status reports can be configured to auto-rotate among reports. See Group Report Settings.

Note that you can add custom background images :)

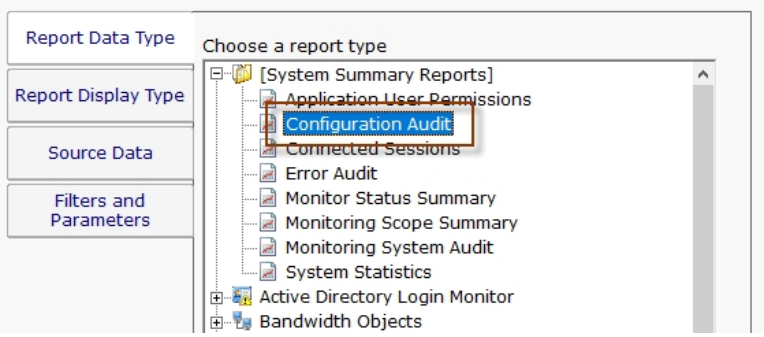

PA Server Monitor Ultra Console - v9.2.0.115 [Connected to D2 as doug] - Licensed to: Power Admin LLC Internal Use
File View Configuration Settings Licensing Alerts Help
OK - 44,745,998 monitors run
Servers/Devices
AWS
Azure
Lab
192.168.1.141
DOMAIN2
DOMAIN3
RANCOR
ROGUE
Network Devices
Office
Private Cloud
prop-test
*Automatic Config
Active Director
All Devices - Ir
All Devices - P
Anti-Virus Stat
ASP.NET
Disk Space
< Back
Open in Browser
Print
NETWORK MAP
OVERVIEW
ALL SERVERS
STATUS OVERVIEW
VISUAL STATUS MAP
Servers/Devices
Visual Status Map
Updated 31 Mar 2023 01:01 PM
All Reports
PDF
POD51019.OUTLOOK.COM
D2
DOMAIN2
DOMAIN3
LOTSA
TYR
Indicator status: OK at 1:02:01 PM

Configuration Audit Reports

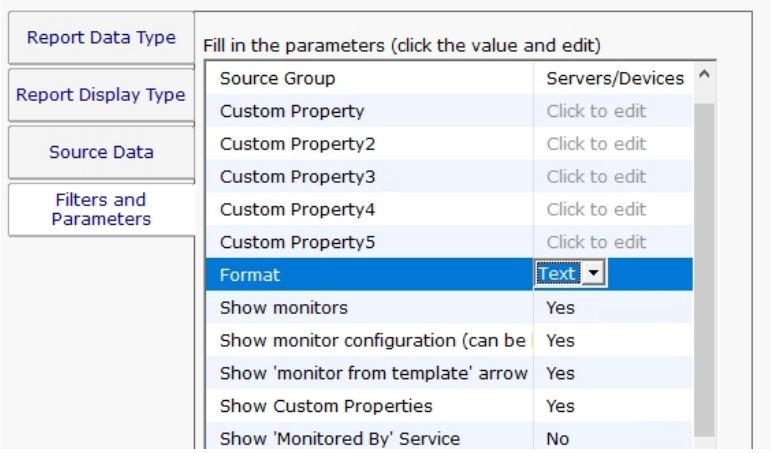
This report shows PA Server Monitor's current configuration, including Groups, Servers, Monitors, and Actions. The report generates a text file listing the Groups with their server and devices. Each server/device will have a list of monitors assigned to them. You can optionally add the monitor's configuration and/or the actions that are attached to the monitors.

Watch the training video on how to create a Configuration Audit Report.

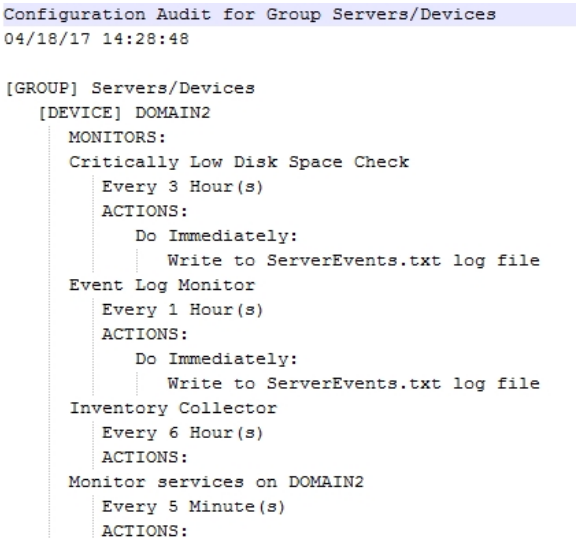
In the example below, the user selects the Configuration Audit report on the top Report Data Type tab. The Configuration Audit report can be found under the System Summary Reports node.



The Filters and Parameters tab is most important. A few options let you select what is included in the report; which monitor types, their actions, the monitor's configuration, and source group.



Pressing the Generate Report button will display a link indicating where the report was created. You can click the link to open the report in your browser.



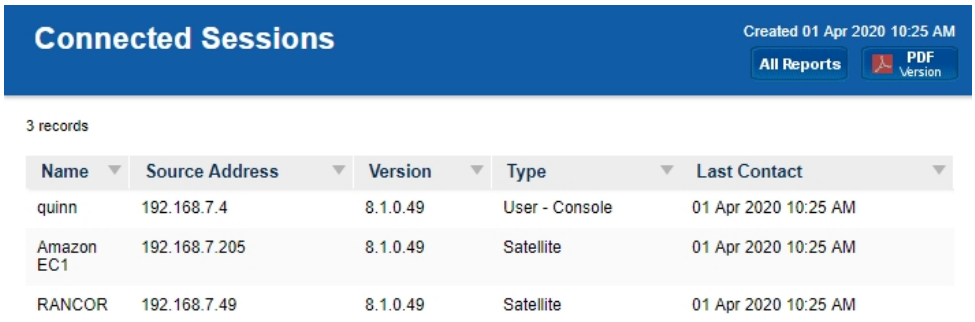
Data Summarization

The Configuration Audit report is organized in the same order as Servers/Devices in the Console:

Groups
  Servers/Devices
    Monitors
      Settings
      Actions

Connected Sessions

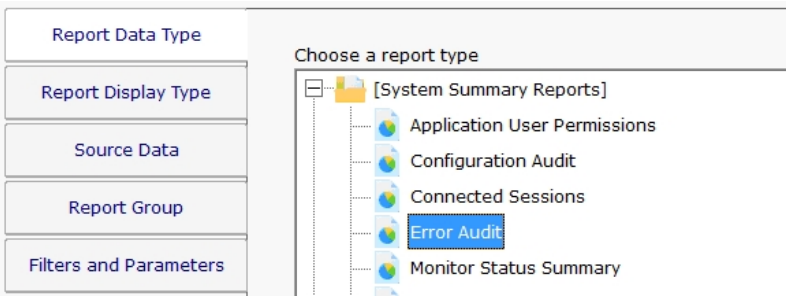
The Connected Sessions report is a simple report that takes no parameters. It shows all currently connected sessions, including Console, mobile applications and Satellites.



Error Audit Report

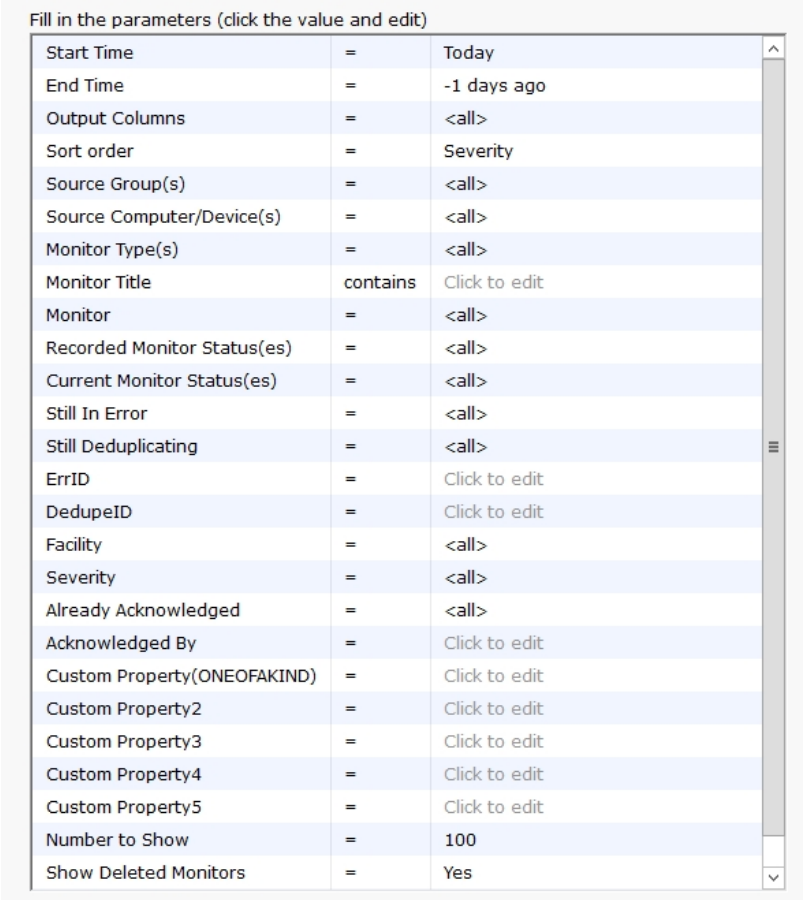
The Error Audit report is a powerful report that lets you view current and past events that have been detected by the monitoring service. There are a large number of parameters that can be used for filtering.

This report is part of the Error Auditing system.



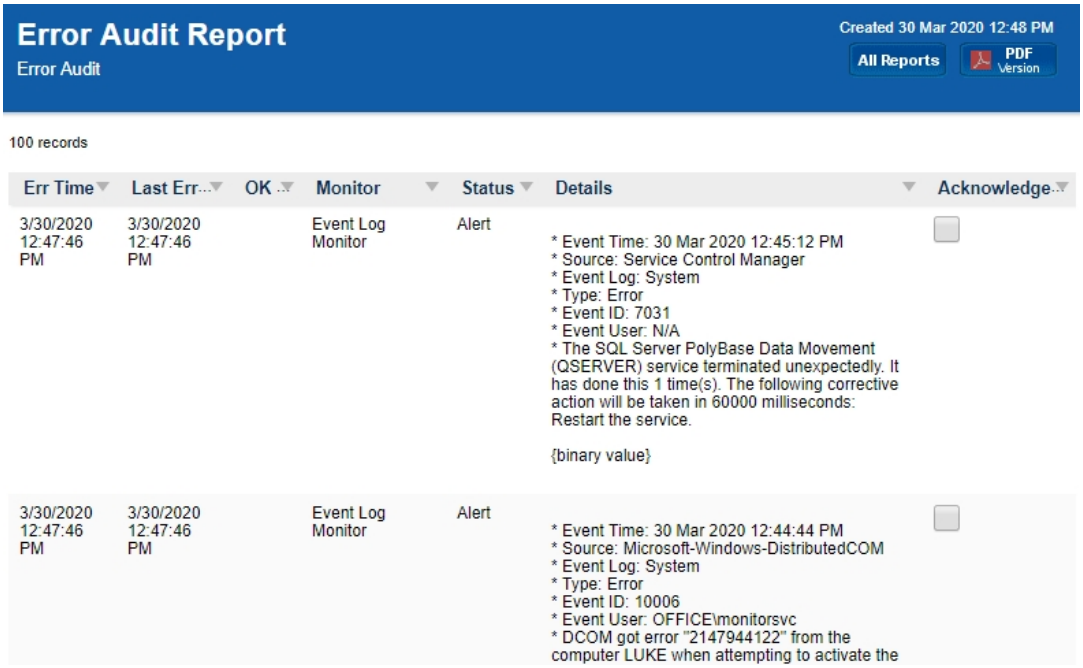
This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.

Any field can be set, or leave it blank or set to <any> to indicate that field should not be filtered on.



An example report is shown below. Note it can show who acknowledged an issue, as well as show a check box for the viewer to

click to indicate they are acknowledging the issue.



Error Audit Report

Error Audit

Created 30 Mar 2020 12:48 PM

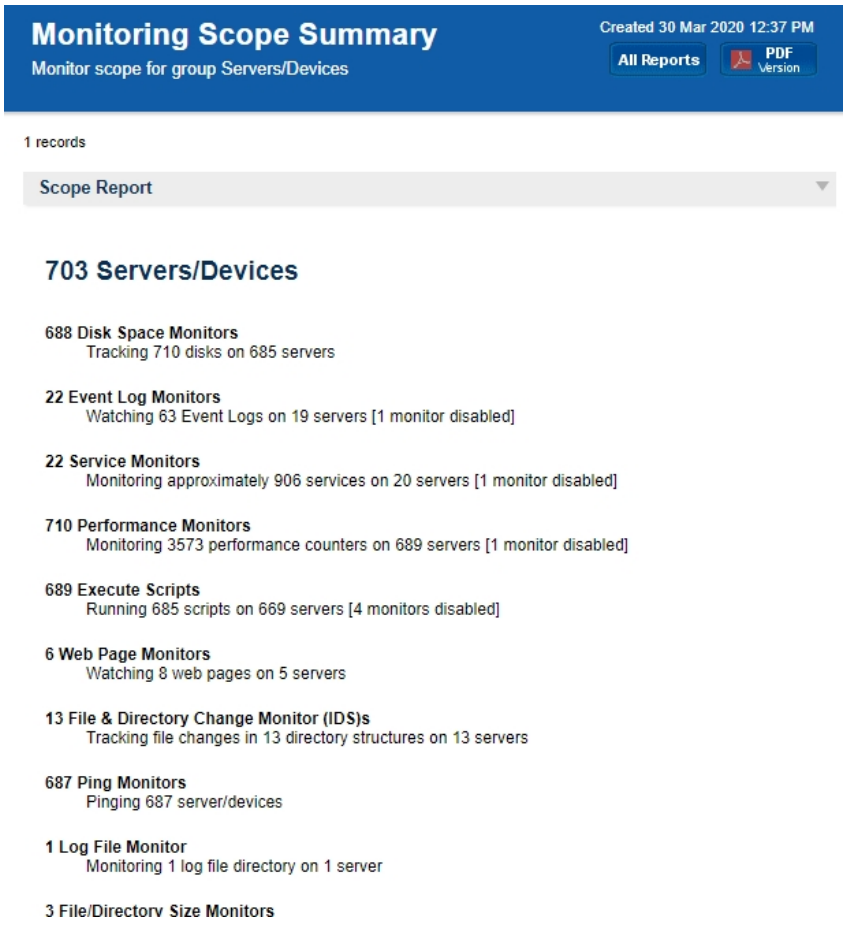
All Reports | PDF Version

100 records

Err Time	Last Err...	OK	Monitor	Status	Details	Acknowledge
3/30/2020 12:47:46 PM	3/30/2020 12:47:46 PM		Event Log Monitor	Alert	* Event Time: 30 Mar 2020 12:45:12 PM * Source: Service Control Manager * Event Log: System * Type: Error * Event ID: 7031 * Event User: N/A * The SQL Server PolyBase Data Movement (QSERVER) service terminated unexpectedly. It has done this 1 time(s). The following corrective action will be taken in 60000 milliseconds: Restart the service. {binary value}	☐
3/30/2020 12:47:46 PM	3/30/2020 12:47:46 PM		Event Log Monitor	Alert	* Event Time: 30 Mar 2020 12:44:44 PM * Source: Microsoft-Windows-DistributedCOM * Event Log: System * Type: Error * Event ID: 10006 * Event User: OFFICE\monitorsvc * DCOM got error "2147944122" from the computer LUKE when attempting to activate the	☐

Monitoring Scope Summary Report

The Monitoring Scope Summary Report is a report that shows all the monitoring work being done from a particular group (which includes all child groups and devices). This report is useful for showing stakeholders the a high level overview of the monitoring being done.



Monitoring Scope Summary

Monitor scope for group Servers/Devices

Created 30 Mar 2020 12:37 PM

All Reports | PDF Version

1 records

Scope Report

703 Servers/Devices

688 Disk Space Monitors
Tracking 710 disks on 685 servers

22 Event Log Monitors
Watching 63 Event Logs on 19 servers [1 monitor disabled]

22 Service Monitors
Monitoring approximately 906 services on 20 servers [1 monitor disabled]

710 Performance Monitors
Monitoring 3573 performance counters on 689 servers [1 monitor disabled]

689 Execute Scripts
Running 685 scripts on 669 servers [4 monitors disabled]

6 Web Page Monitors
Watching 8 web pages on 5 servers

13 File & Directory Change Monitor (IDS)s
Tracking file changes in 13 directory structures on 13 servers

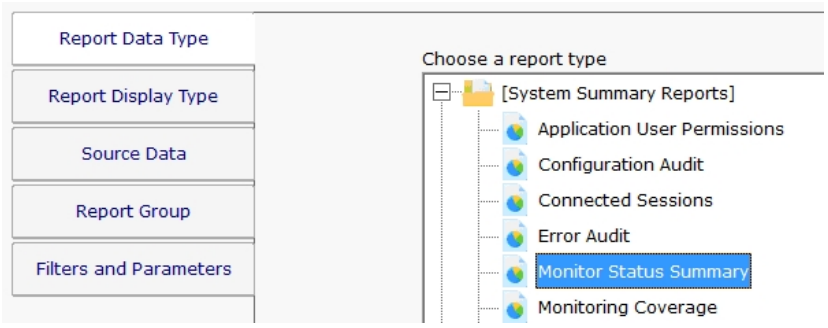
687 Ping Monitors
Pinging 687 server/devices

1 Log File Monitor
Monitoring 1 log file directory on 1 server

3 File/Directory Size Monitors

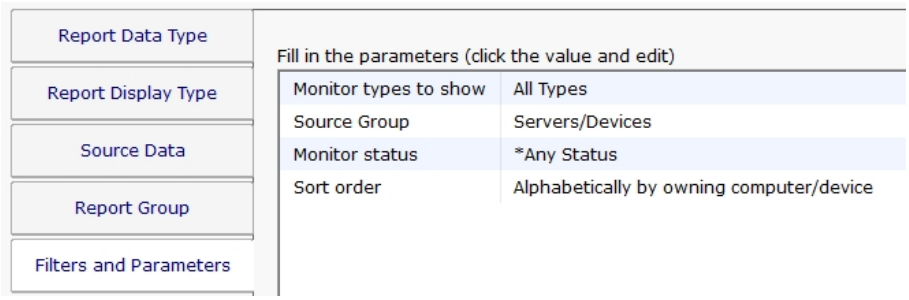
Monitoring Status Summary Report

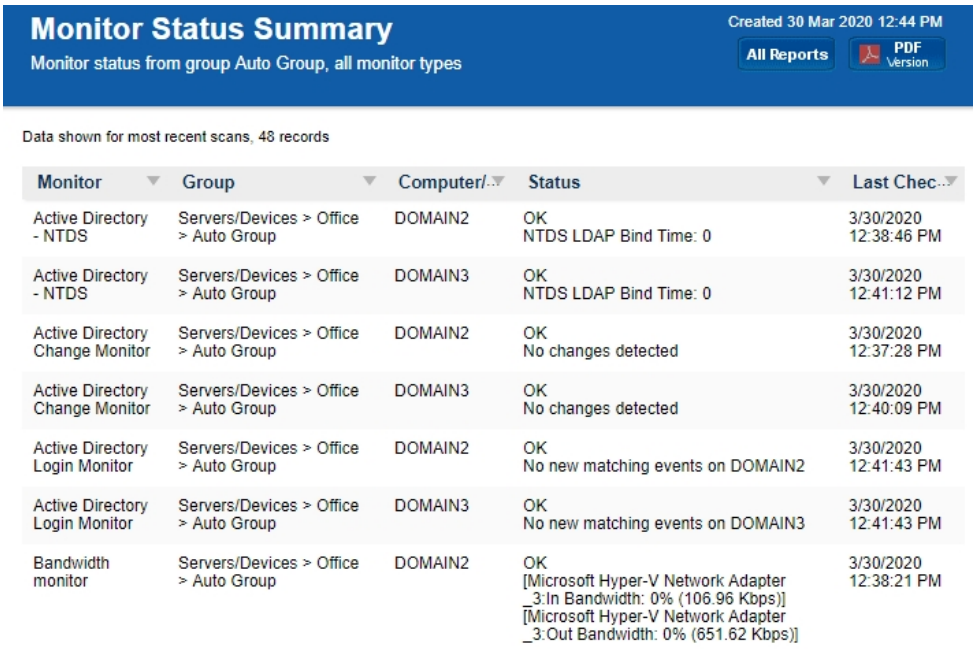
This report lets you quickly see the current status of a set of monitors you define.



This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.

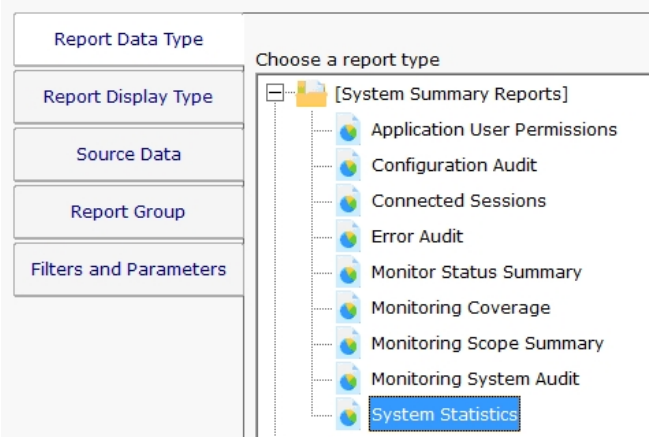
You can choose to see all monitors that are in error, or that have a specific status (those in Dependency Not Met for example), or even a specific monitor type. The filters will work based on monitors that are within a specific group that you select.





System Statistics Report

System Statistics Report shows top level statistics about the monitoring system, including details about connections and HTTPS server information.



This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.

Unlike most reports, this report does not have any fields to fill in on the Filters & Parameters tab.

System Statistics

HTTP Bandwidth per Minute (averaged over last 15 minutes), ...

Created 30 Mar 2020 02:54 PM

All Reports | PDF Version

35 total records

System Statistics

Statistic	Value
Number of Servers/Devices	704
Number of Connected Satellites	2
Number of Monitors	3492
Number of Actions	25
Number of Sessions	5
Number of Held HTTP Connections	2
Process Memory (KB)	429736
Process Handles	2791
Number of Queued Stats to Write	57

HTTP Bandwidth per Minute (averaged over last 15 minutes)

Client	Number of Requests	KB Received from Client	KB Sent to Client
127.0.0.1	16.6	52.1	14.2
192.168.7.4	46.9	28.2	817.2
192.168.7.49	19.5	20.1	16.4
192.168.7.205	12.5	21.3	7.4
[Total]	95.5	121.6	855.2

HTTP Server Statistics

Statistic	Value
Collection Period (secs)	901
Number of Idle HTTP Threads	6

System Audit Report

The System Audit Report is a pulled from a database of activities that have happened in the monitoring system.

System Activity Types

Email Alert Sent

User Logged In

User Logged Out

User Login Failed

Server Start Maintenance

Server End Maintenance

Central Service OS Boot

Central Service Start

Central Service Stop

Central Service Abnormal Stop

Satellite Service OS Boot

Satellite Service Start

Satellite Service Stop

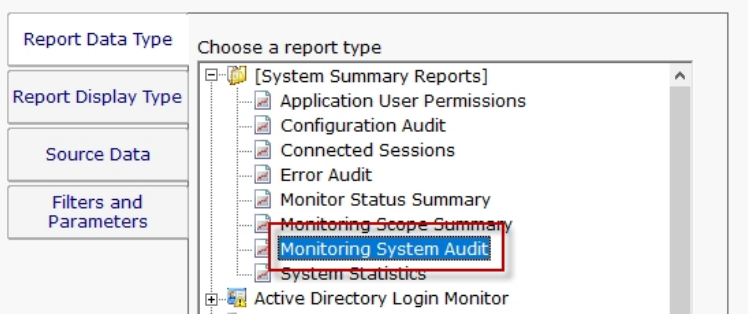
Satellite Service Abnormal Stop

Satellite Connect to Central

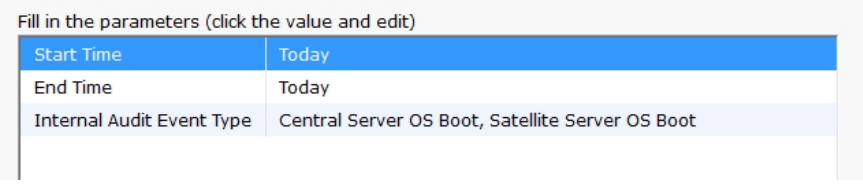
Satellite Down

- Group Created
- Group Deleted
- Computer Created
- Computer Deleted
- Monitor Created
- Monitor Changed
- Monitor Deleted
- Monitor Template Created
- Monitor Template Deleted
- Action Created
- Action Deleted

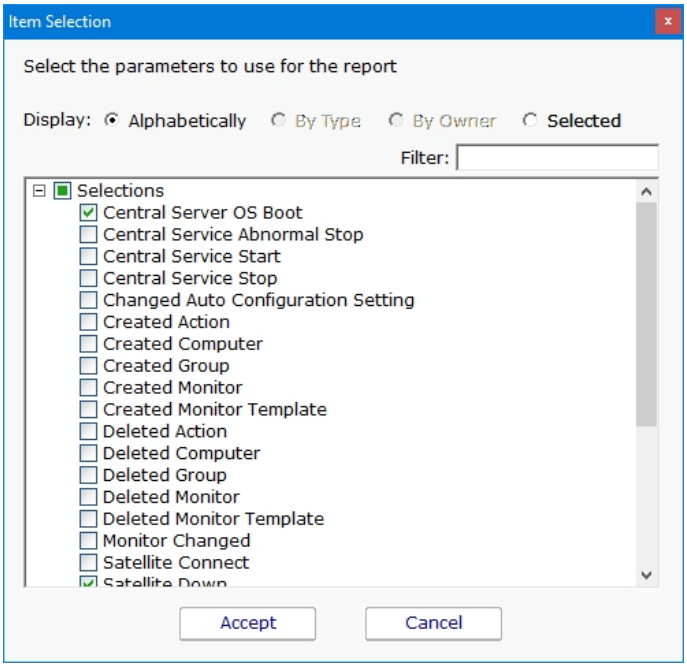
This data is collected and stored automatically - nothing needs to be configured.



The report is located at [System Summary Reports] > Monitoring System Audit.

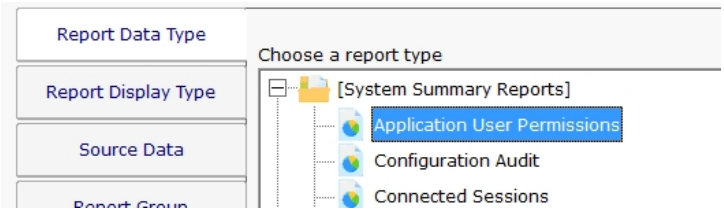


Configuring the report is as simple as choosing a date range, and the type of events you would like to see.



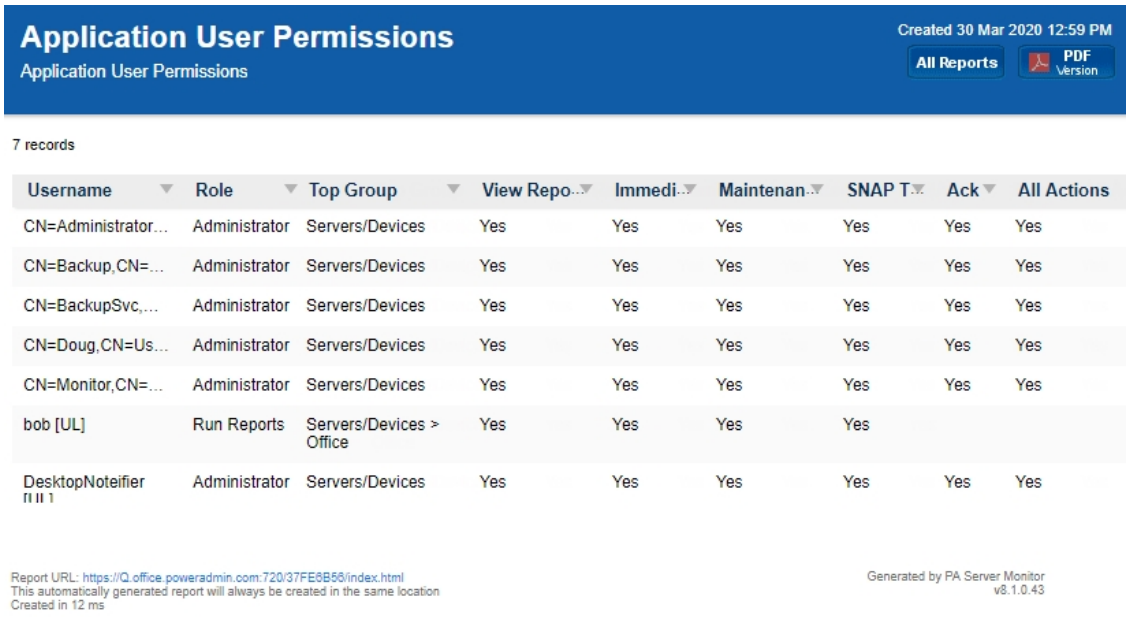
Application User Permissions Report

This report shows all defined users within the monitoring application, what they have access to, and what permissions they have.



This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.

Unlike most reports, this report does not have any fields to fill in on the Filters & Parameters tab.



Application User Permissions

Application User Permissions

Created 30 Mar 2020 12:59 PM

All Reports | PDF Version

7 records

Username	Role	Top Group	View Repo...	Immedi...	Maintenan...	SNAP T...	Ack	All Actions
CN=Administrator...	Administrator	Servers/Devices	Yes	Yes	Yes	Yes	Yes	Yes
CN=Backup,CN=...	Administrator	Servers/Devices	Yes	Yes	Yes	Yes	Yes	Yes
CN=BackupSvc,...	Administrator	Servers/Devices	Yes	Yes	Yes	Yes	Yes	Yes
CN=Doug,CN=Us...	Administrator	Servers/Devices	Yes	Yes	Yes	Yes	Yes	Yes
CN=Monitor,CN=...	Administrator	Servers/Devices	Yes	Yes	Yes	Yes	Yes	Yes
bob [UL]	Run Reports	Servers/Devices > Office	Yes	Yes	Yes	Yes		
DesktopNoteifier	Administrator	Servers/Devices	Yes	Yes	Yes	Yes	Yes	Yes

Report URL: https://Q.office.poweradmin.com:720/37FE8B56/index.html
This automatically generated report will always be created in the same location
Created in 12 ms

Generated by PA Server Monitor v8.1.0.43

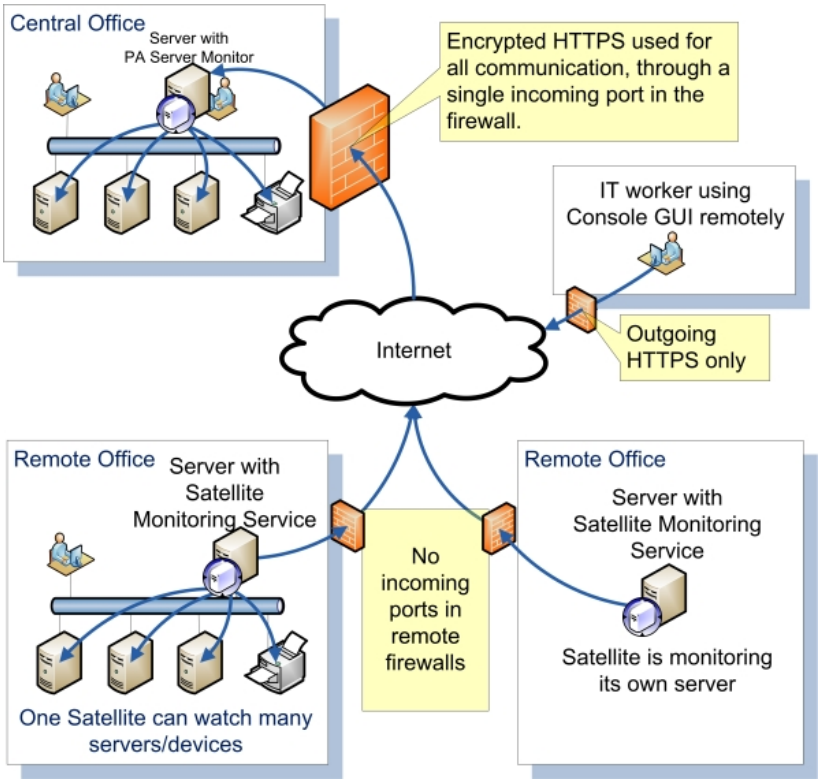
Remote and Distributed Server Monitoring

PA Server Monitor can monitor servers within the local LAN with just the Central Monitoring Service. No additional software is needed.

If you want to monitor servers and devices that are on the other side of a firewall from the Central Monitoring Service (either within a corporate network, or across the Internet) then a Satellite Monitoring Service needs to be installed. The Satellite will do the monitoring at the remote location and report statistics and status information back to the Central Monitoring Service as shown in the image below. The Satellite Monitoring Service typically **only needs to be installed on a single server** at the remote site.

Pro Tip: **Do not** install a Satellite on each monitored server. Just install one at each remote location and let it monitor the local network. This works great for monitoring a DMZ as well.

NOTE: The Satellite Monitoring Service is only available in Ultra product editions.



The steps to monitoring remote computers and devices are:

1. Install a Satellite Monitoring Service at the remote location
2. Configure the Satellite Monitoring Service
3. Using the PA Server Monitor Console, add new computers and devices to be monitored. The trick is to make sure and indicate that the newly added computers/devices will be monitored using the Satellite, and not the Central Monitoring Service.

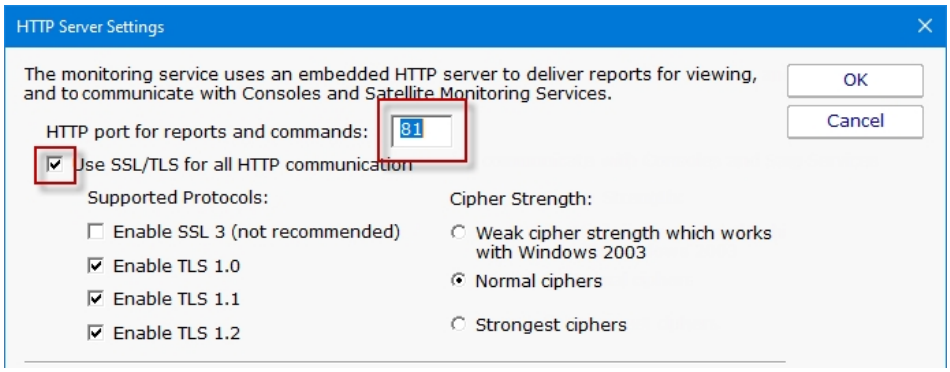
4. Once the computers have been added, add new monitors to watch the computers/devices added above. You will be able to add the new monitors as though the computers they belonged to were on the local LAN -- PA Server Monitor takes care of everything else.

Remote Installation Prerequisites

You must complete the following steps before installing either PA Server Monitor Consoles on a remote computer or Satellite Monitoring Services. These steps not needed for the initial installation.

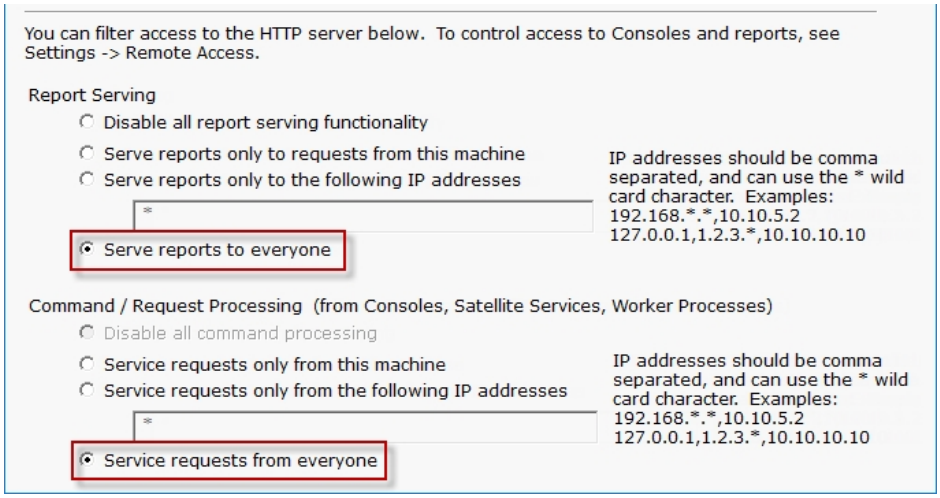
Note: You only need to complete these steps one time. You do not need to repeat them if you install additional Consoles or Satellite Monitoring Services.

1. Open the PA Server Monitor Console that was installed on the same computer as the Central Monitoring Service.
2. Connect to the local host.
3. Select the **HTTP Server Settings** command on the **Settings** menu. The HTTP Server Settings window appears.



4. Select the **Use SSL for all HTTP communication** option and note the HTTP port number.
5. Ensure the port is accessible from the remote servers. A firewall exception might need to be created if Consoles or Satellite Monitoring Services will be installed across the Internet from the Central Monitoring Service. This is the only incoming port that might need to be opened.
6. Filter Settings

- **Report Serving** - for remote console use select "Serve reports to everyone" or enter the IP addresses needed.
- **Command/Request Processing** - for ALL remote requests select "Service requests from everyone" or enter the IP addresses needed.



7. Click **OK** to restart the monitoring service.

   Note: If you are using SSL for all HTTP communication, and browser certificate alerts appear, click the SSL Certificate Hints link for information about how to resolve the alerts for your browser.

Installing a Satellite Monitoring Service

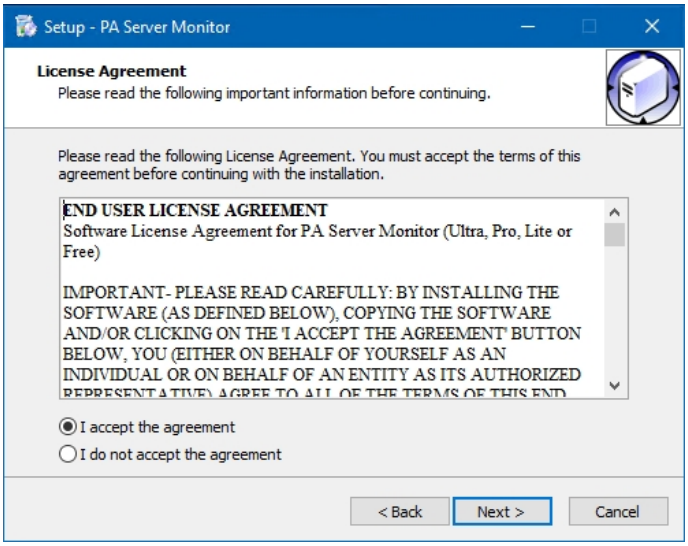
To install a Satellite Monitoring Service

1. Be sure that you have completed the Installation Prerequisites before installing your first Satellite Monitoring Service.
2. On the computer on which you want to install a Satellite Monitoring Service, open a browser, and connect to your Central Monitoring Service using the following URL:

   https://[*computername*]:[*port number*]

   where *computername* is the name of the computer where the Central Monitoring Service is installed, and *port number* is the HTTPS port that the service exposes (See Installation Prerequisites).

3. On the login page there is a small link below the credential window with a link for "Satellite Installer". Download and run the setup program.
4. The License Agreement page will appear.

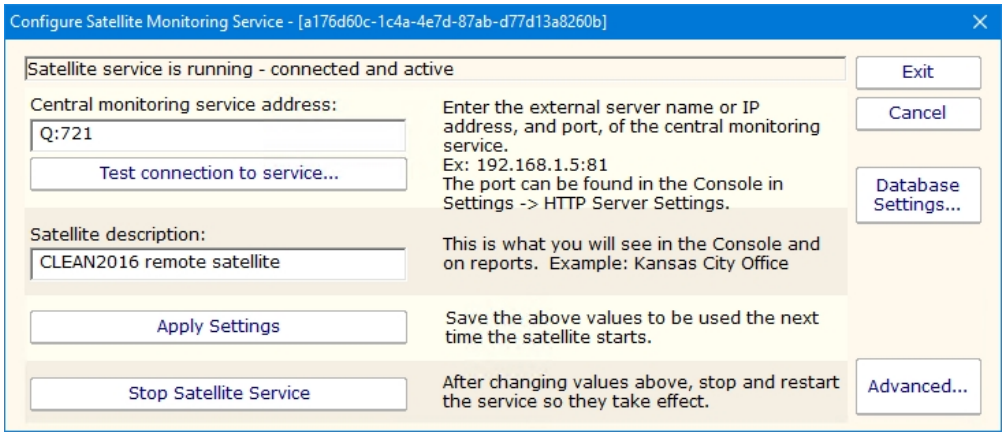


5. Click **Next** to advance through the wizard, accept the license agreement, select a destination location, and then display the Select Components page.
6. Select the **Satellite Monitoring Service** option.
   Note: If you don't have access to a remote Console, select the **Console User Interface** option as well.
7. Click **Next** repeatedly while accepting all the defaults.
8. Ensure all options are selected on the Completing the PA Server Monitor Setup Wizard page, and then click **Finish**. The Configure Satellite Monitoring Service window will appear.

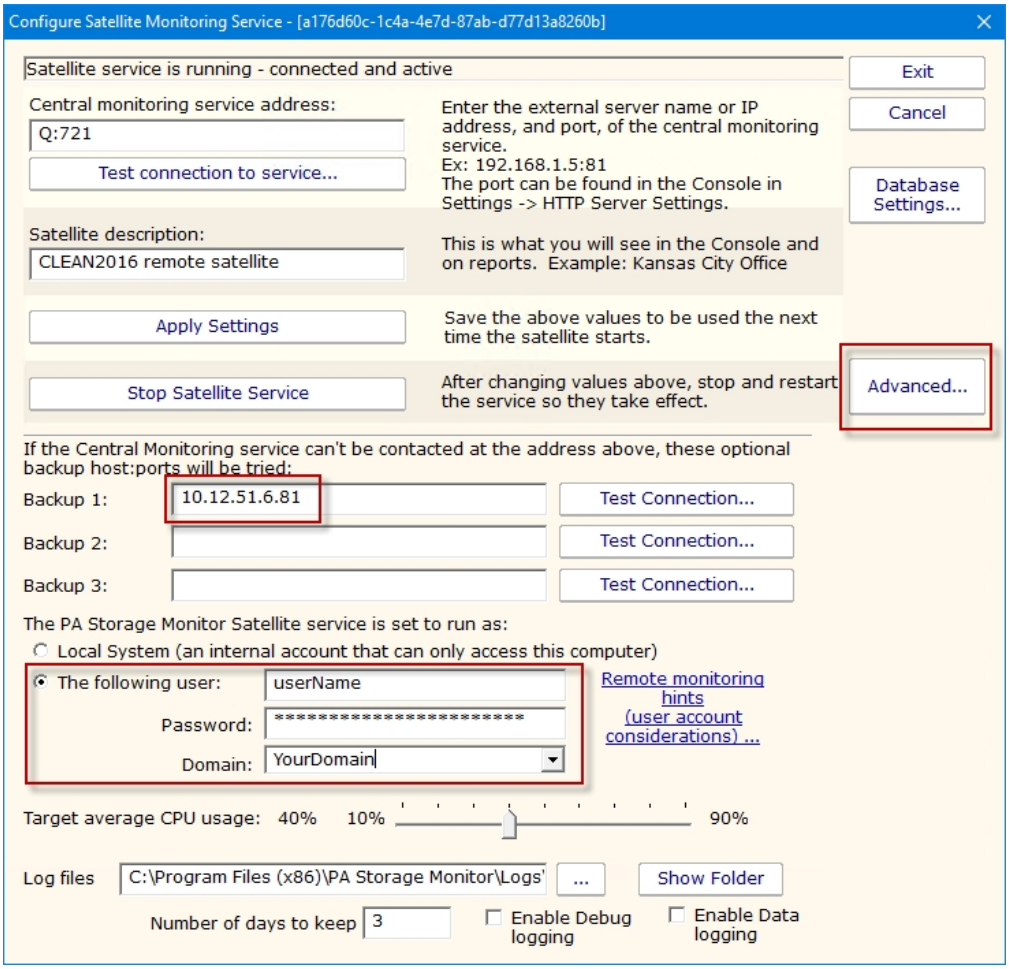
Next, Configuring a Satellite Monitoring Service.

Configuring the Satellite Monitoring Service

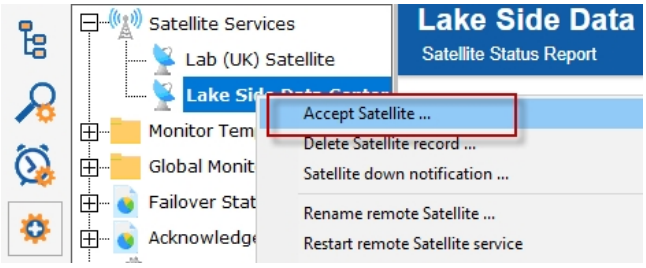
To configure the Satellite Monitoring Service



1. Enter the computer address and port of the Central Monitoring Service in the **Central monitoring service address** box. This was determined during the Installation Prerequisites.
2. Click **Test connection to service**. The Success window appears if the the connection is successful. If there is a problem, several troubleshooting tips will be shown to help fix the problem.
3. Click **OK** to close the Success window.
4. Enter a name in the **Satellite description** box.
5. If there are multiple network paths to the Central Monitoring service, you can give additional addresses for the server. Click the **Advanced ...** button which will display three additional places for host:port settings. Any time the Central Monitoring service can't be accessed using the primary host:port settings above, each of the Backup host:port settings will be tried to try and find a connection to a Central Monitoring service. This is useful if you are using Automatic Fail Over as it allows the Satellites to find the Fail Over Slave server if the main Central Monitoring Service is down.
6. Click the **Advanced ...** button which will display settings for the Satellite Monitoring Service. It is recommended to have the service use an account that has access to the computers that it will be monitoring. The default Local System account cannot access remote computers. See Remote Monitoring Account Hints for more information.



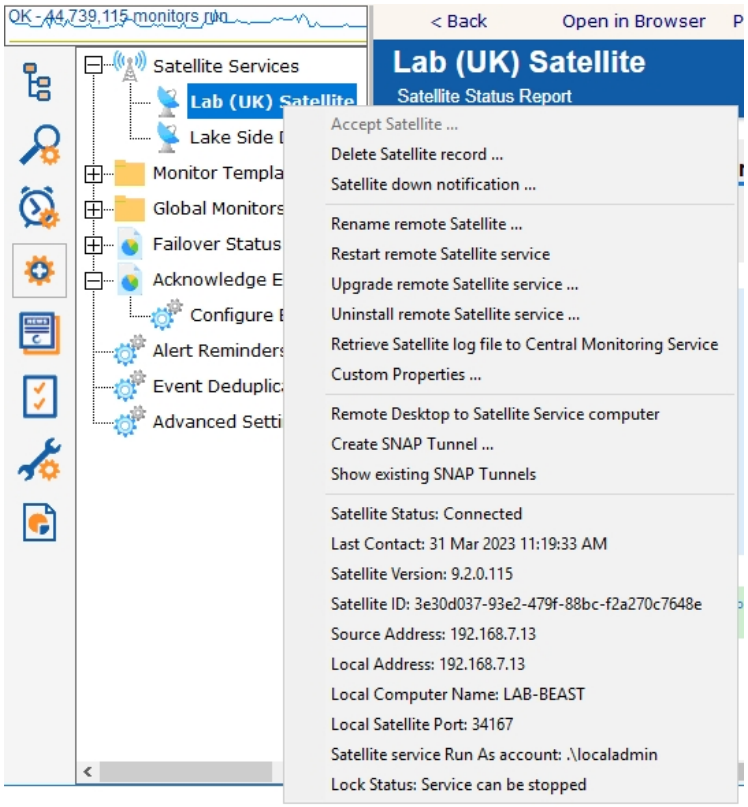
7. Click **Apply Settings** to save your changes.
8. Start a Console GUI, and then connect the console to the Central Monitoring Service. The main PA Server Monitor Console window will appear:
9. Click **Satellites Services** in the left navigation panel, and then select the Satellite you just installed. If it is not displayed, wait a few moments and then click the Satellite Services node to refresh the list.
10. Right-click the Satellite that was just installed, and select **Accept Satellite...**. This will allow the Satellite to connect to the Central Monitoring Service.



Now that the Satellite is connected to the Central Monitoring System, you can add computers to the Satellite via the Console just like you would add computers to be monitored from the Central Monitoring System. Just be sure to indicate which Satellite should monitor the newly added computers.

Satellite Operations

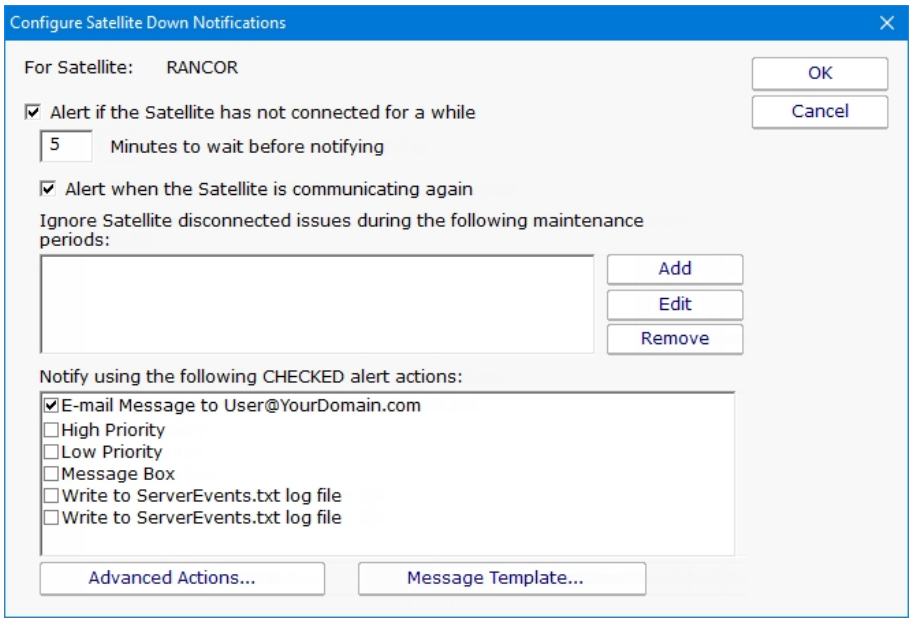
From within the Console, you can right-click a Satellite and see a variety of options that are described below.



Accept Satellite - This allows a newly added Satellite to communicate with the Central Monitoring Service as mentioned in Configure Satellites.

Delete Satellite record - This removes the Satellite from the Central Monitoring Service. Computers that are monitored by the Satellite service will not be automatically removed. If the Satellite service is still installed and running on a remote computer, it will need to be accepted again before it is able to communicate with the Central Monitoring Service.

Satellite down notification - When a Satellite is created, you can specify if you want to be notified if the Satellite stops reporting in to the Central Monitoring Service. This menu item lets you change that notification setting at a later time as well.



Rename remote Satellite - This option simply renames the Satellite as it appears in the Console GUI and in reports.

Restart remote Satellite service - This command will instruct the remote Satellite service to stop and restart itself. The computer hosting the Satellite service will NOT be rebooted.

Upgrade remote Satellite service - Using the Satellite Status Report you can see which software version each Satellite is running (this is also available at the bottom of the Satellite's pop-up menu in the status area). This option will upgrade the Satellite to the current PA Server Monitor software version that the Central Monitoring Service is using (the setup file is downloaded from the Central Monitoring Service). The remote Satellite service will stop and restart as part of the process, but the remote computer hosting the Satellite service will NOT be rebooted.

Retrieve Satellite log file ... - A request is sent to the remote Satellite to send its internal log file to the Central Monitoring Service. The file will be saved along with the other product log files as specified at the bottom of the Settings dialog. The request is sent immediately, but it could take a minute or two (especially if the log file is large) before it shows up in the Log directory.

Custom Properties - Custom Properties are name-value pairs that can be set on a Satellite, Group, Computer/Device or Monitor.

Remote Desktop to Satellite Service computer - A SNAP Tunnel will be created to the remote Satellite using a dynamically chosen source port. The Remote Desktop client application will be launched and connected to the remote Satellite computer automatically.

Create SNAP Tunnel - See SNAP Tunnels.

Show existing SNAP Tunnels - All existing SNAP Tunnels are displayed. You can select an existing SNAP Tunnel and close/delete it. Any application that might have been using the SNAP Tunnel will see its connection terminated.

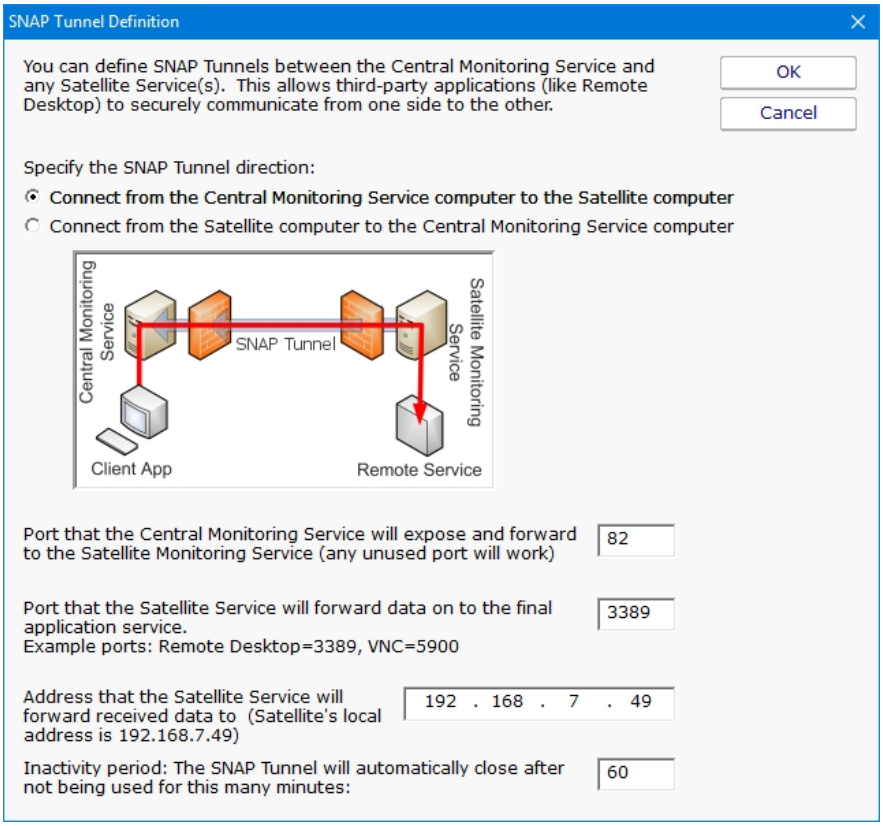
Satellite Status - Various Satellite status values are shown here.

SNAP Tunnels

NOTE: The features described below require a Satellite Monitoring Service, and thus are only available in Ultra product editions.

Secure Network Access Portal Tunnels, or "SNAP Tunnel" for short, are a means of securely tunneling arbitrary TCP/IP data from the Central Monitoring Service to a remote Satellite Monitoring Service, and vice versa. This enables point to point network connections among LANs, even if separated by firewalls or the Internet.

SNAP Tunnels are defined by choosing a direction (from Central Monitoring Service to Satellite, or the reverse), a destination IP address, and source and destination ports. Once defined, data arriving at the source port will be securely forwarded to the destination port. A timeout value can also be specified to automatically close the SNAP Tunnel after the given amount of inactivity time expires.



In the diagram above, the red arrow indicates the direction that connections take place. The destination port is 3389 which is the typical Remote Desktop port. So a client that connects to the computer where the Central Monitoring Service is running, on port 82 as shown above, will actually get forwarded to and connect to the remote network's 192.168.2.200 on port 3389. That means the Remote Desktop client can connect to port 82 on the local computer and actually have an RDP session with a remote computer, even though the remote computer has not opened any ports in the firewall.

Existing SNAP Tunnels can be seen by right clicking a Satellite and choosing Show Existing SNAP Tunnels as described in Satellite Operations.

Security

SNAP Tunnels have a couple of factors that make them very safe:

All data going through a tunnel is SSL encrypted. This is a requirement for using remote Satellites and can not be circumvented.

The remote Satellite contacts the Central Monitoring Service via a single HTTPS port. No ports are opened to the remote Satellite computer (see remote scenario image). No ports in remote firewalls need to be created. This means there is no way for an outsider to access the tunnel. Only computers on the local network on the source side of the SNAP Tunnel can access the tunnel.

Inactivity timeouts automatically close the SNAP Tunnel when not being used

When the SNAP Tunnel is created, the creating user's access is checked to verify they can access the target device.

Additional Security Settings

If you don't ever want to use SNAP Tunnels, they can be disabled completely by setting the following registry value on the Central Monitoring Service:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor\Protected
SNAP_AllowTunnel2 = 0
```

With this value set, all SNAP Tunnels will be blocked. You can also set the value on individual Satellites to disable SNAP Tunnels to that Satellite.

To access devices which are not monitored (and thus access can't be check), set the following on the Central Monitoring Service:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor\Protected
SNAP_AccessUnmonDevices = 1
```

The TUNNEL_CREATE external API call now requires a login. To go back to the legacy setting where a login is not needed, set:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor\Protected
SNAP_AllowTunnelFromAnonAPI = 1
```

Usage

The most common usage for SNAP Tunnels is for remote support, via Remote Desktop, VNC or another remote control client. Other applications can be used as well -- just point the destination port at the remote service's listen port and IP address. Then connect the client application to the local side of the tunnel.

For example, if you want to connect using VNC to a computer at a client's office, and the client's computer IP address is 192.168.5.12, set up the SNAP Tunnel as follows:

Direction: Connect from Central Monitoring Service to Satellite computer (top radio button)

Source port can be any unused port: 9000 (for this example)

Destination port: 5900 since that is VNC's default listen port (this assumes the VNC listener is installed on the client computer and using the default port)

Address: 192.168.5.12. Note that this address does not need to be accessible from the Central Monitoring Service -- it just needs to be accessible from the Satellite.

Timeout: 5 minutes (to close the port when finished

Launch the VNC client at point it at: {Central Monitoring Service IP address}, port 9000. VNC will connect and be forwarded to the client's computer.

Note that the above example used VNC and requires the VNC listener to be running. Remote Desktop is typically running and

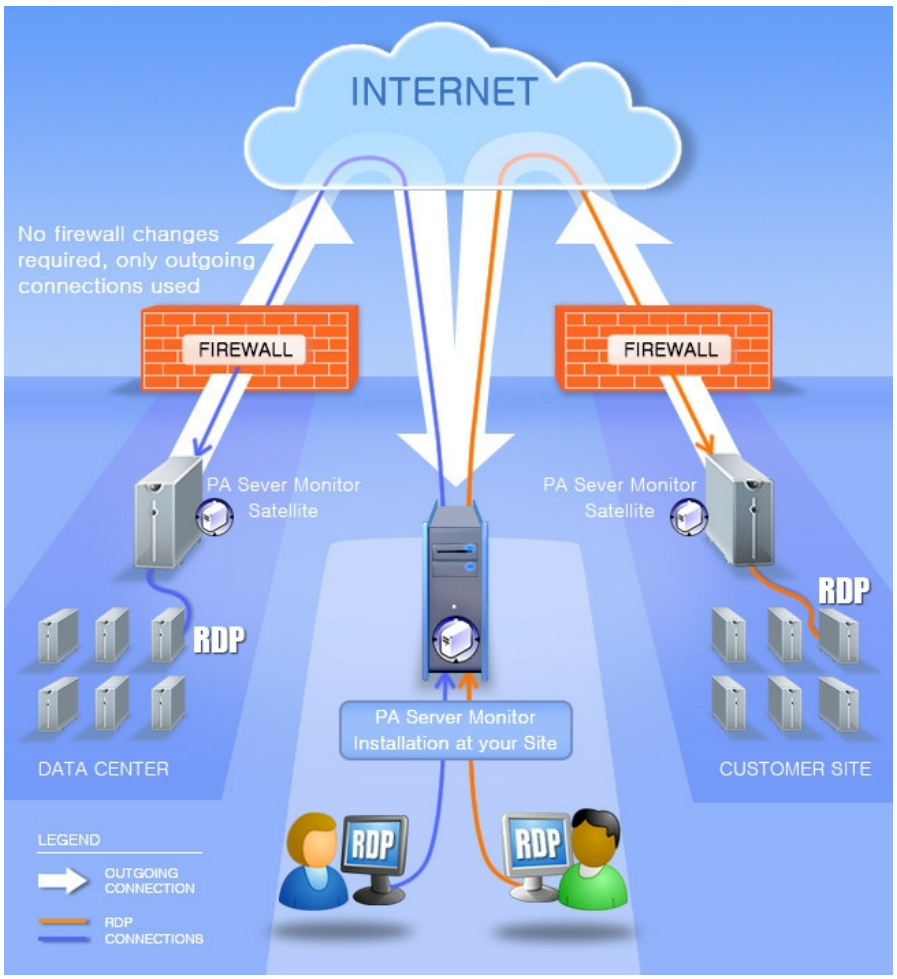
available on most Windows servers and is therefore often an easier option.

Remote Desktop (Remote Support)

NOTE: The features described below require a Satellite Monitoring Service, and thus are only available in Ultra product editions.

PA Server Monitor enables Microsoft's Remote Desktop (and VNC, etc) to connect to computers across firewalls that otherwise would not be accessible.

Access to remote servers is made available using the same outgoing-only, SSL-encrypted HTTP connection that the Satellite uses when connecting to your Central server. (See SNAP Tunnels for more information).

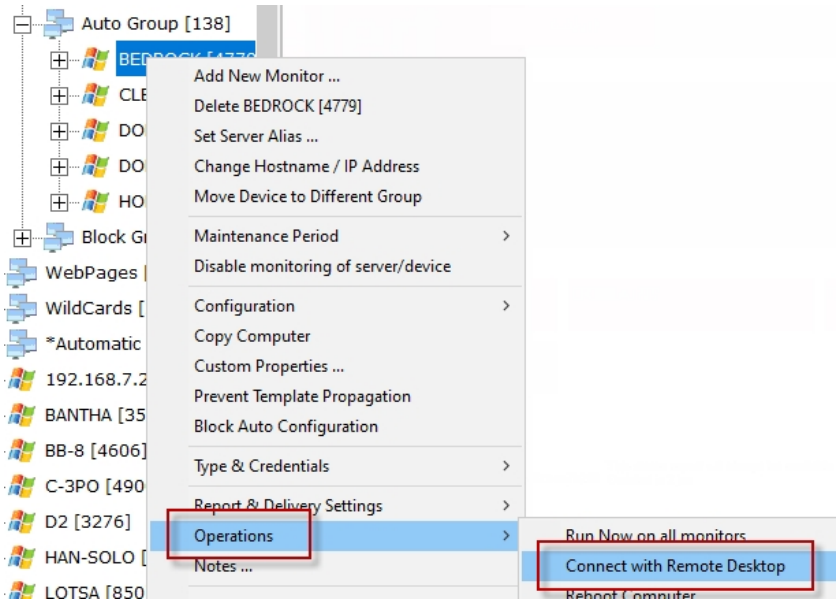


As usual, this is completely agentless -- you do not need an agent on the target server. It just has to be visible to a Satellite Monitoring Service.

There are two easy ways to quickly start a Remote Desktop session with a remote computer.

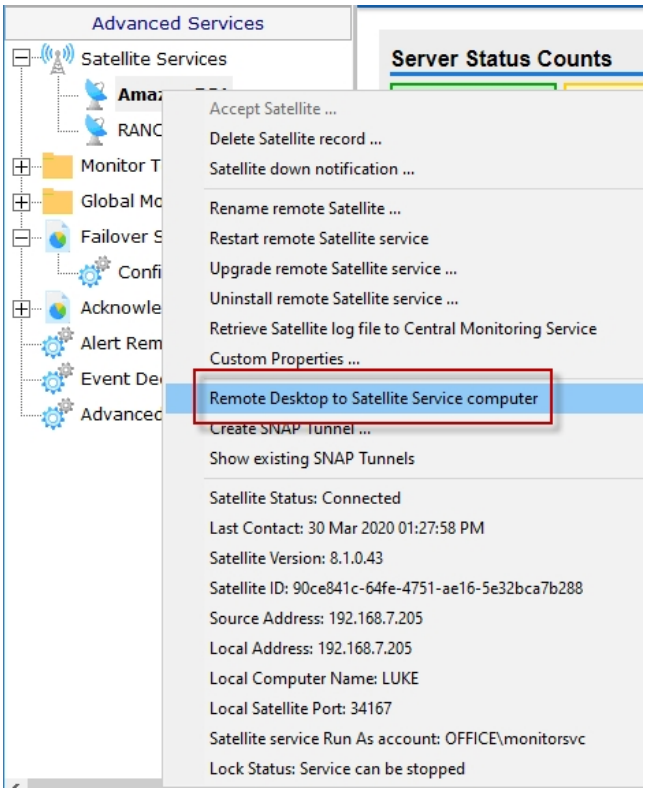
Connect to a Monitored Server

Right-click the computer and choose **Operations** -> **Connect with Remote Desktop**. This will create a SNAP Tunnel and then launch Remote Desktop with the appropriate commands for it to connect using the SNAP Tunnel.



Connect to a Satellite Computer

Right-click on a Satellite and choose **Remote Desktop to Satellite Service computer**. This will create a SNAP Tunnel and then launch Remote Desktop with the appropriate commands for it to connect using the SNAP Tunnel.



Installing Remote Consoles

The PA Server Monitor Console can be installed and run on any computer that can reach the Central Monitoring Service. If the service's HTTPS port is available through the company firewall, the Console can be installed and run on any computer that has Internet access.

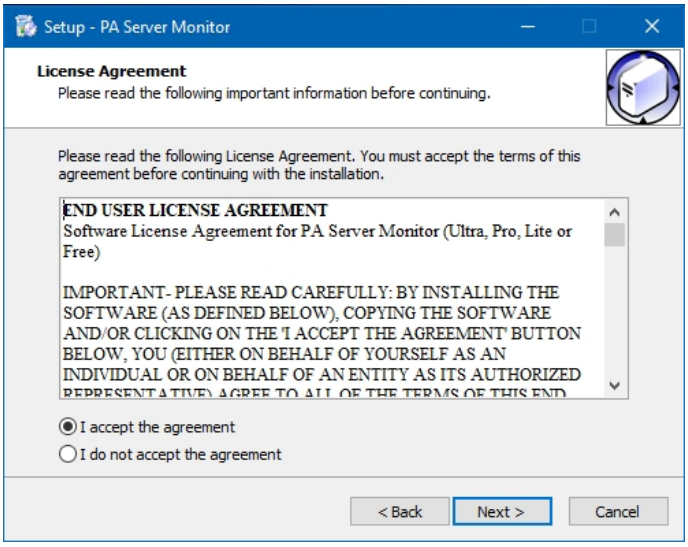
To install a Remote Console

1. Be sure that you have completed the Installation Prerequisites before installing your first Remote Console.
2. On the computer on which you want to install the Remote Console, open a browser, and connect to your Central Monitoring Service using the following URL:

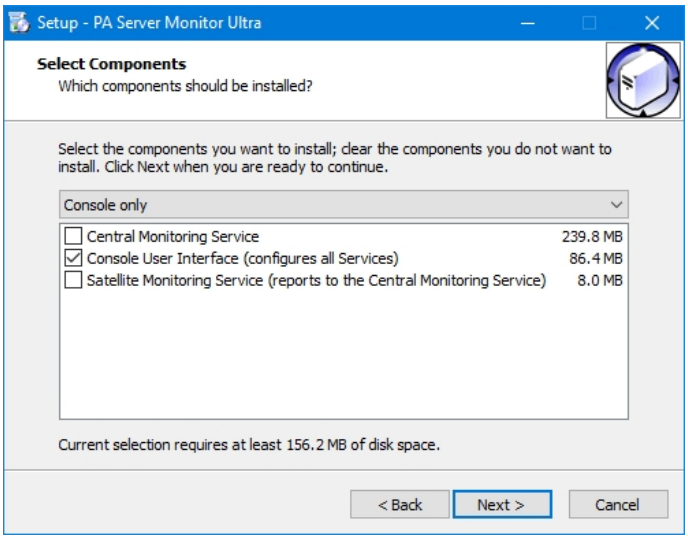
   https://[*computername*]:[*port number*]

   where *computername* is the name of the computer where the Central Monitoring Service is installed, and *port number* is the HTTPS port that the service exposes (See Installation Prerequisites).

3. On the main reports page, near the bottom, is a "Product Installer" link for the Setup program. Download and run the setup program.
4. The License Agreement page will appear.



5. Click **Next** to advance through the wizard, accept the license agreement, select a destination location, and then display the Select Components page.



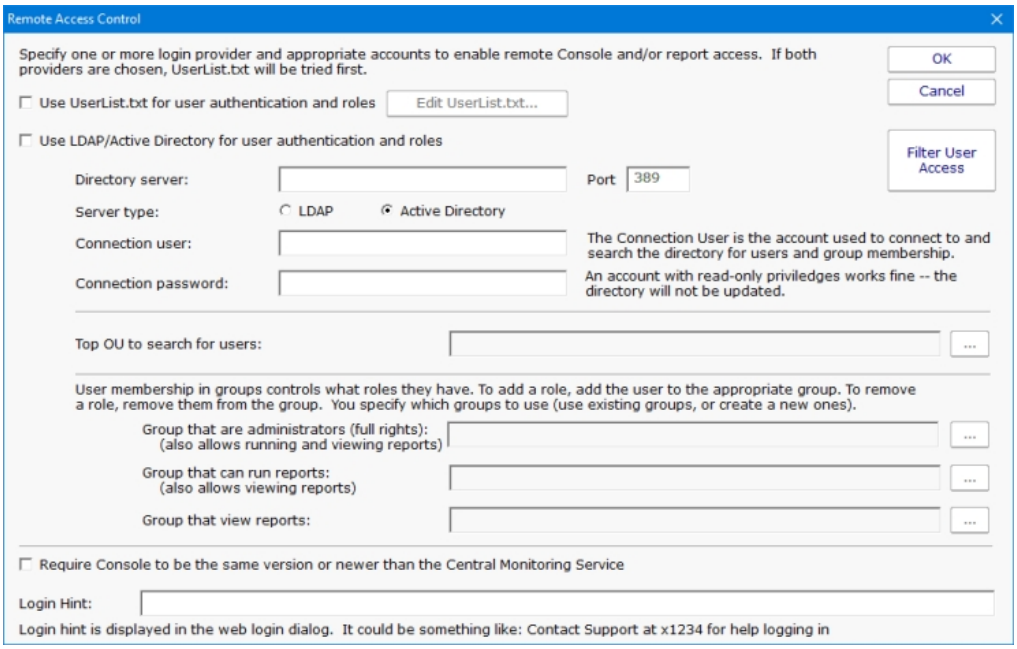
6. Select the **Console User Interface** option, and leave the other options unselected.
7. Click **Next** repeatedly while accepting all the defaults.
8. Click **Finish** to complete the installation. The PA Server Monitor Console connection window will appear.

Next, Starting the Console

Controlling Remote Access

To control which users can use a Remote Console to connect to the Central Monitoring Service, go to **Settings** -> **Remote Access**. This must be done from the Console installed on the Central Monitoring Service.

When you initially open the Remote Access Control window, it looks like the image below.



Remote Access allows you to specify lists of users that can run Remote Consoles, and also which users can login and view reports if they are protected. You can specify a user list via simple text file, or via Active Directory or LDAP groups. When logins are checked, the UserList.txt file is checked first, and then the LDAP or Active Directory server.

Once you have specified which users can login here, you can go to Filter User Access to further restrict some logins to just particular groups of servers. This is particularly useful in a Managed Service Provider setting where you want to give customers access to see their own server status reports.

UserList.txt Users

The easiest way to specify users is via the UserList.txt file. This is a simple text file which contains comments on how to enter new users. It's quite easy:

```
# This is the default UserList.txt file
# Users are specified using the format shown below:
# [Users]
# {username}={password},{role}
#
# Passwords ARE case sensitive, username is not. Don't use a comma in
# the password itself.
# Role is a value shown below:
# A - administrator - full rights to configure the system (implies R and V)
# R - run reports (implies V)
# V - view existing reports (via Console or web browser)
#
# So an example file might look like:
#
# [Users]
```

```
# dan=S3cr3tP@assw0rd,A
# jon=m1ghym0us3,R
# philip=w@tch,V
#
# Extra space or tab characters will be removed when the file is processed


[Users]
doug=test16,A
quinn=h@ryp077er,A
john=l33tr,A
henry=5891sda,A
bob=239ska,R
```

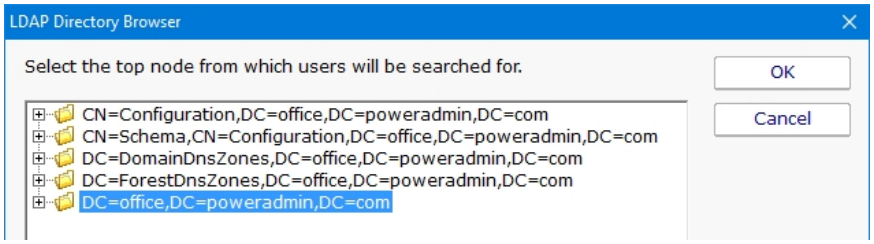
In the example above, user Quinn would be able to login to a Remote Console or a password protected report page using password h@ryp077er.

Active Directory Users

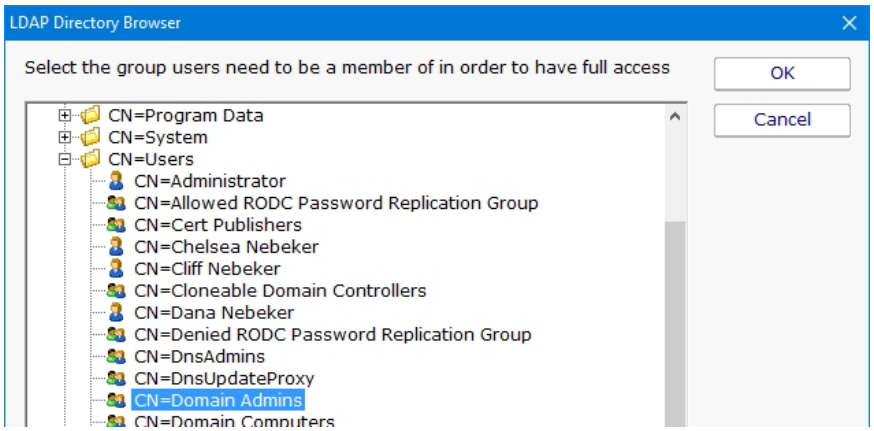
PA Server Monitor can also refer to Active Directory groups to specify user logins.

1. First, specify an Active Directory or LDAP server and its port. The default LDAP port is 389.
2. Indicate whether the server is LDAP or Active Directory.
3. Specify a username and password for an account that can connect to and search the directory. This will be used to check group membership. This account does not need any write rights to the directory.

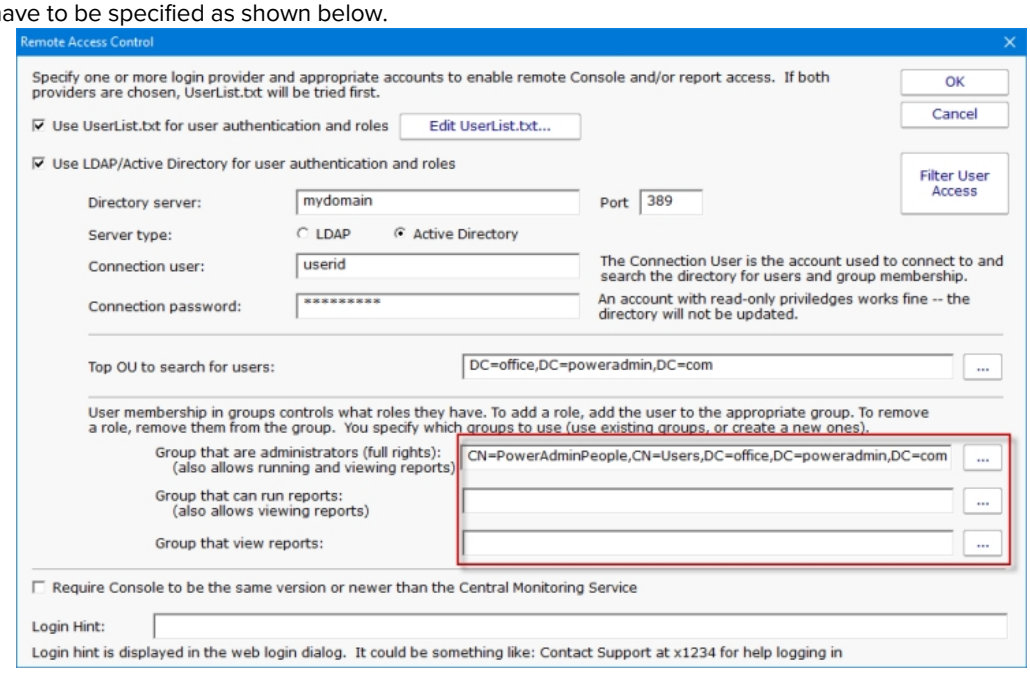
   Every few seconds the server settings and account credentials are checked. Once good credentials have been entered, the rest of the dialog will be enabled automatically.
4. Click the ... button next to **Top OU to search for users**. If nothing happens, the credentials are not allowing access to the LDAP or Active Directory server. If the credentials are good, an LDAP Browser dialog will appear. Choose the top OU where the user accounts exist.



5. Choose three groups whose members will have Administrator, Run Report and View Report rights respectively. If a user is in multiple groups, they get the rights of the highest group they are in.



Not all groups have to be specified as shown below.



6. Press OK to finish. The monitoring service does not need to be restarted for these changes to take effect.

Access Control

Access Control allows different remote users to have different access to the monitored servers. For example, system administrators usually need to see everything, but particular groups or customers might only need to see their own servers.

Reports for servers or groups that a user can't access will be hidden from them. If they some how find a URL to a report that they aren't allowed to see, the report will be blocked.

To change the Access Control settings, launch the Console on the server where PA Server Monitor is installed. Go to Settings -> Remote Access -> Filter User Access.

Layout

User List

The Access Control dialog is a simple one. On the left is a list of users. Names that have [UL] after them are defined in the UserList.txt file. All other users shown were found in the specified Active Directory OU (specified in the Remote Access dialog).

Below each name is a summary of their current access. "Full Access" is shown for users that can see all servers/devices being monitored.

Group List

On the right side is a list of all of the groups defined. Access is controlled on a group by group basis. The groups can be sorted alphabetically, or in their normal hierarchical layout.

User Rights

User Rights are extra rights that are typically given to users that have limited rights. Top-level administrators (administrators that have access to the top Servers/Devices group) automatically have all User Rights. Administrators that have restricted access do not necessarily have the rights below unless explicitly granted.

Access all actions

By default users have access to actions that are attached to a monitor that they already have access to. This User Right will give the selected user access to all actions defined in the system.

Acknowledge alerts on accessible servers/devices

This right allows the specified user to acknowledge alerts on all servers/devices that they already have access to.

Create SNAP Tunnels (for RDP, etc)

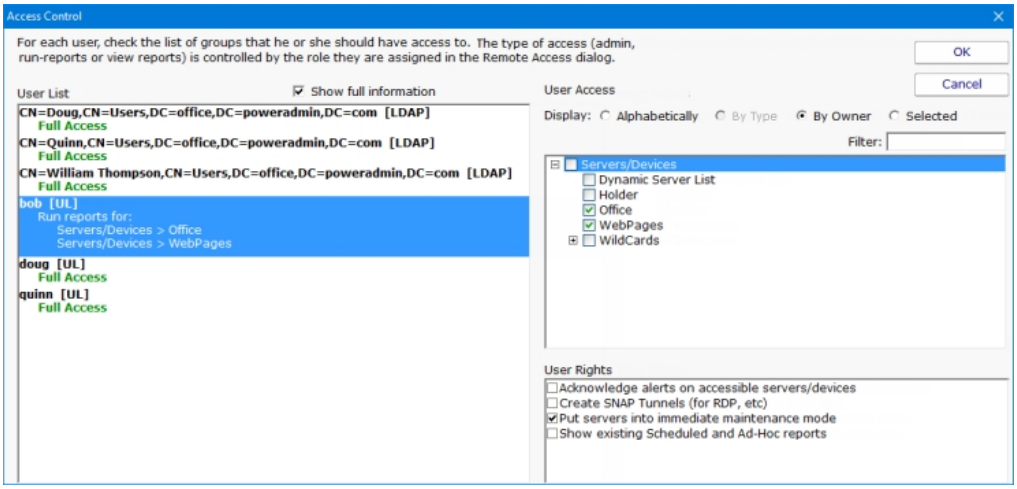
This allows the specified user to create SNAP Tunnels which are use for remote access among other things.

Put servers into immediate maintenance mode

Administrator users automatically have the right to put servers into maintenance. This User Right allows you to grant this right to non-administrator users.

Show existing Scheduled and Ad-Hoc reports

This user option will allow a user to view the Scheduled and Ad-Hoc reports. When a user is selected in the User List and this check box is checked the user will be able to view the reports section in the console and in the web interface.



Editing

To change what a user can access, select the user account on the left. The right side will display a check box in each group that the user can access. Simply select the groups that the user will have access to. Switching to a new user or pressing the OK button will save the changes to that user's access control.

Type of Access

This dialog controls what a user can access. To control what type of access they have (administrator, run-reports or view reports) to the servers, go to Remote Access where each user's role is specified.

How to Acknowledge and Stop Alerts

A common desire is to be notified when there is a problem, possibly with event escalation, and then to quiet the alerts while the problem is being worked on. This can be enabled using Event Deduplication.

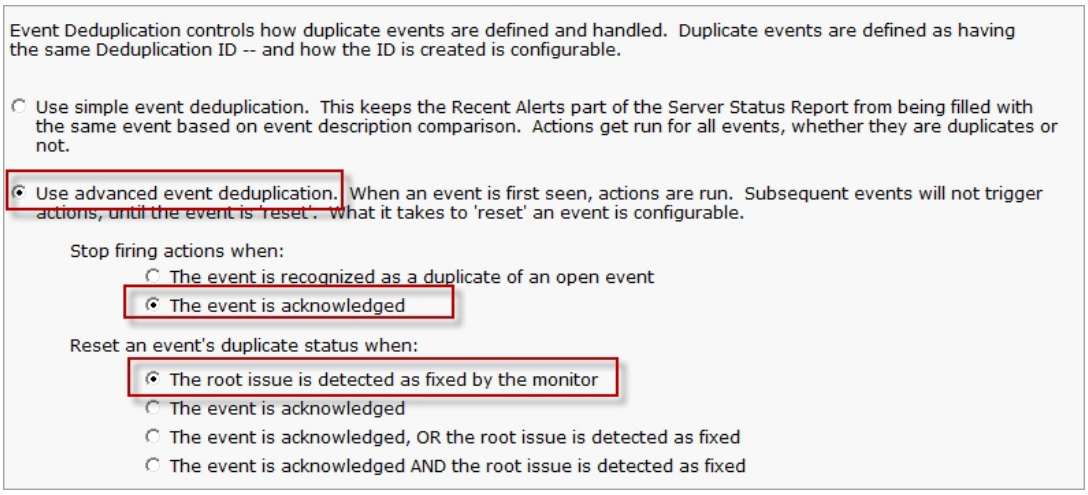
Escalate Alerts

First, decide what sort of event escalation steps you'd like. Perhaps if disk space is low you would like to get an initial alert, again 30 minutes later, and then again every 6 hours until the problem is fixed. This is Event Escalation, and can be configured in the monitor's Action settings.

Event Deduplication

The Event Deduplication engine is responsible for figuring out that two events are the same. Once an event is recognized as a duplicate, some rules kick in. By default, duplicate alerts are suppressed. However, you can instead choose to keep sending alerts until the event is acknowledged.

With the setting to stop sending alerts when an event is acknowledged, you should also change the deduplication 'reset' step to only use the monitor's state, specifically the monitor has to transition back to an OK state before incoming events are considered new events and alerted on again. See the settings below:



How to Add and Activate Licenses

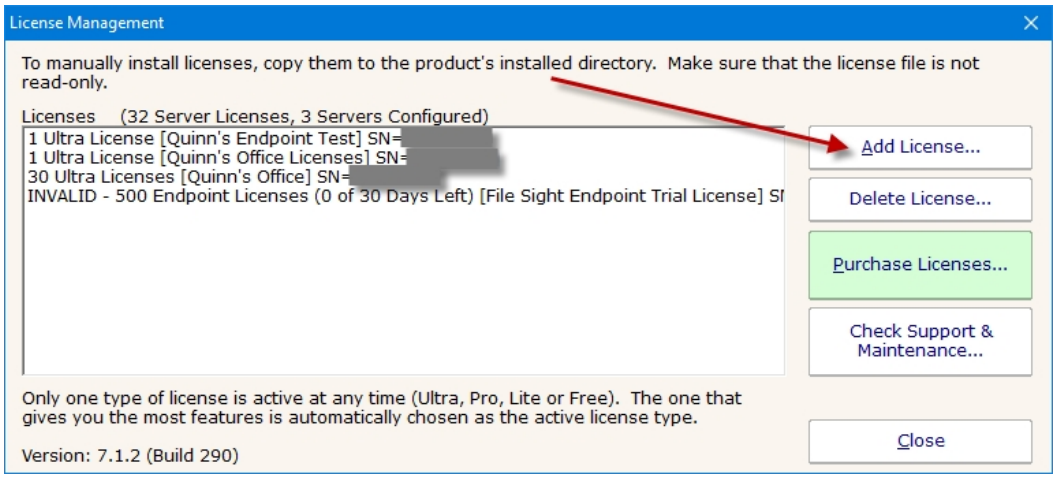
Most of the time your licenses will be automaticly activated using the first steps listed below but there are times when you may have to manually activte your license.

Automatic License Activation

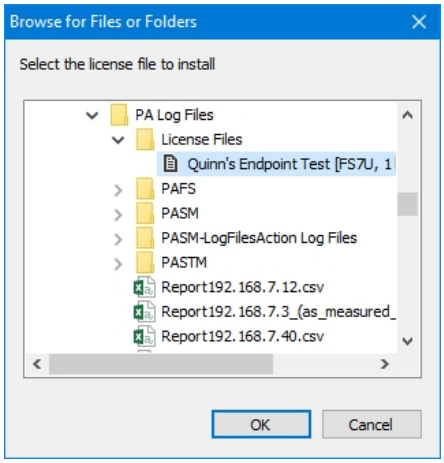
There are two ways to add licenses to your installation, using the Console or add the license files to the installation's root directory.

Adding License Files Using the Console

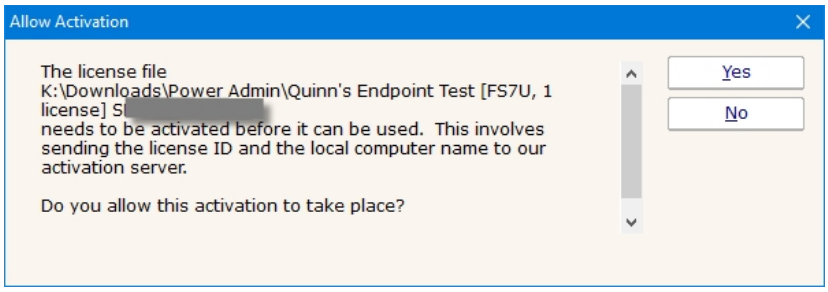
1. You can upload you license files within the Console. In the top menu of the Console go to Licensing. In the License Management menu select the Add License button.



2. Then browse to where your license file is and select the file. Then select OK.



3. Select Yes to automatically upload and activate the license.

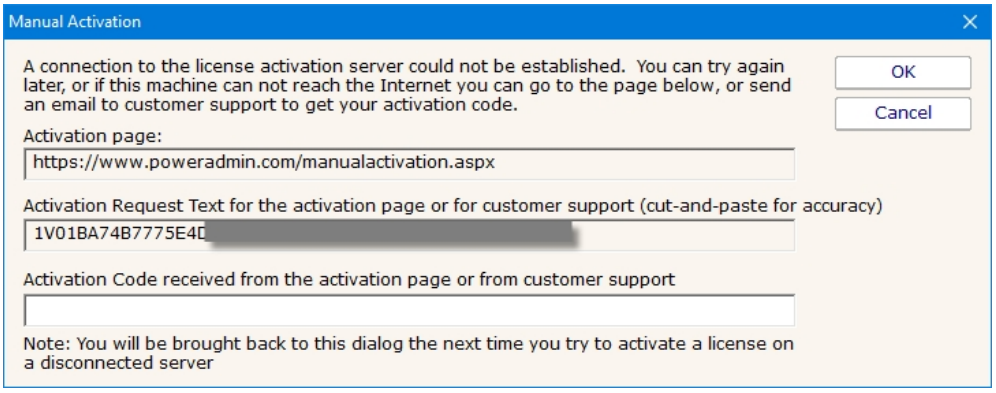


Adding License Files to the install Directory

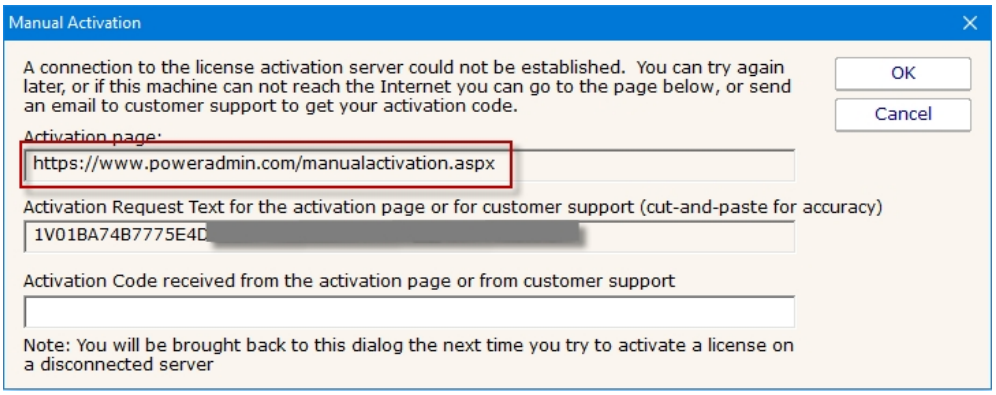
Copy the license file to the root install directory. When you restart your Console, you will be given the "Allow Activation" pop-up, select Yes to activate your license.

Manual License Activation

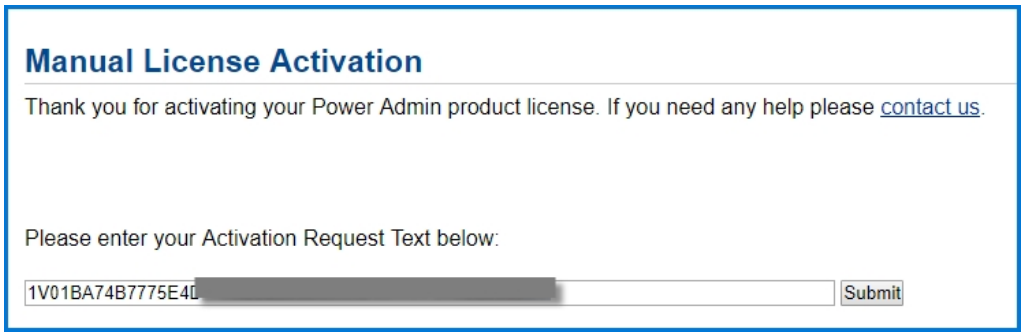
1. When the server where your monitoring service is running has no Internet access you will need to manually activate your license. Follow the steps above to add your license in the service and when the service gets to the point where it tries to activate your license you will be given a menu like this...



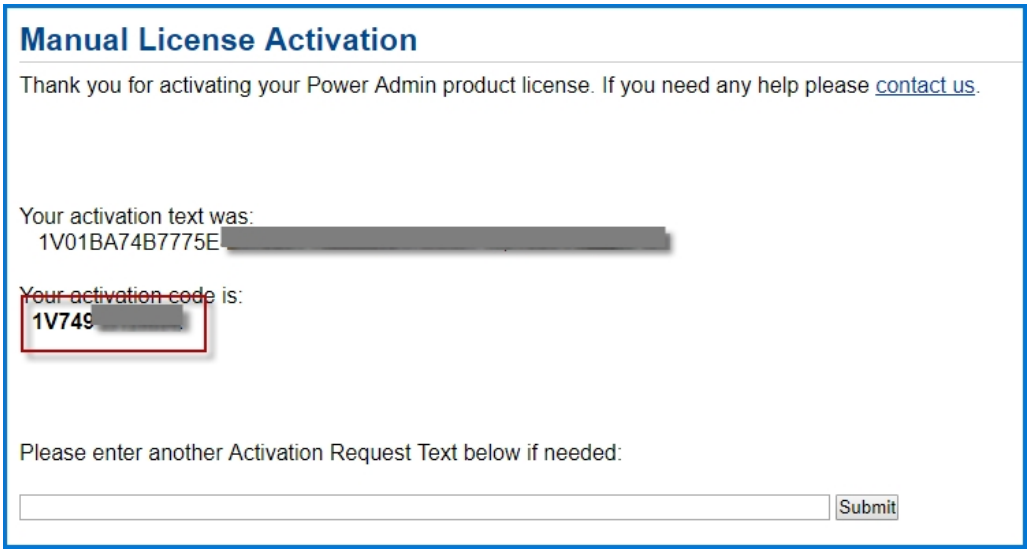
2. Follow the instructions in the Manual Activation menu to manually activate your license. Go to a machine that has Internet access and go to the URL address shown. You can highlight and copy the URL and Activation Request Text from this menu.



3. Copy the Activation Request Text from the menu and enter it on this webpage.



4. Then copy the Activation Code and enter it back in the Manual Activation menu and click on OK.



How to Update Satellites from an Alternate Source

When the Central Monitoring Service sends an update command to the Satellites, the Satellites download three files from the Central Service's Install folder:

Sleep.exe

Upgrade_Satellite.bat

Sat_Only_Setup.exe

The last file, Sat_Only_Setup.exe, is usually in the 30-40MB range. If you have a very slow network connection to the Central Service, or you have many Satellites (some customers have many hundreds), the bandwidth used might cause a problem.

By editing the Upgrade_Satellite.bat file, AND replacing the Sat_Only_Setup.exe with a smaller file (which will be ignored and overwritten), you can direct the Satellite to download from a different location. And since Sat_Only_Setup.exe is a small file, bandwidth to the Central Service server will be greatly reduced.

If you look in Upgrade_Satellite.bat, you'll see it does the following steps:

1. logs the time
2. stops the service
3. sleeps for 60 seconds
4. launches setup
5. waits 30 seconds
6. starts the service

You can edit the file (in the Central Service's Install folder) and add a step 3.5 which will use wget to download the Sat_Only_Setup.exe from a different location.

For example, right before Sat_Only_Setup.exe is launched, insert this code:

```
REM Download from custom URL
IF EXIST "%PROGRAMFILES(X86)%" (GOTO 64BIT) ELSE (GOTO 32BIT)

:64BIT
"%ProgramFiles(x86)%\PA Server Monitor\wget.exe" --no-check-certificate --output-document
"%ProgramFiles(x86)%\PA Server Monitor\Install\Sat_Only_Setup.exe" https://{URL where you have placed
Sat_Only_Install.exe}
Goto CONTINUE_INSTALL

:32BIT
"%ProgramFiles%\PA server monitor\wget.exe" --no-check-certificate --output-document "%ProgramFiles%\PA
Server Monitor\Install\Sat_Only_Setup.exe" https://{URL where you have placed Sat_Only_Install.exe}
Goto CONTINUE_INSTALL

:CONTINUE_INSTALL
```

Thank you to Russell at Sheffield Business Systems for helping us work this out!

The above code will download Sat_Only_Setup.exe from a location you choose. You should upload the Sat_Only_Setup.exe file from your Central Service's Install folder -- that way the Satellite is guaranteed to be the same version as the Central Service.

One note: Every time the Central Service is upgraded, the Upgrade_Satellite.bat will get overwritten with the original file. That turns

out to be helpful as it will be a good reminder to upload a recent Sat_Only_Setup.exe to your preferred download location.

Summary

1. Upgrade_Satellite.bat in the Central Service's Install folder according to the above example
2. Upload the valid Sat_Only_Setup.exe in the Central Service's Install folder to a website of your choosing
3. Replace Sat_Only_Setup.exe in the Central Service's Install folder with any small file (it will be ignored)
4. Tell the Satellites to upgrade themselves via the Console

How to Audit Windows Logons and Logon Failures

When a user logs into a Windows computer, or fails to logon, an event can be written to the Windows Event Log. This feature is built in to Windows.

The Event Log monitor in PA Server Monitor can tell you when one of these events occurs, thus alerting you to a server logon, or a failed server logon. And because the Event Log monitor has a configurable monitoring cycle (the Schedule button in the lower right corner), you can find out about the logon in nearly real time.

Watch the training video Add Event ID and Text Filter to Event Log Monitor.

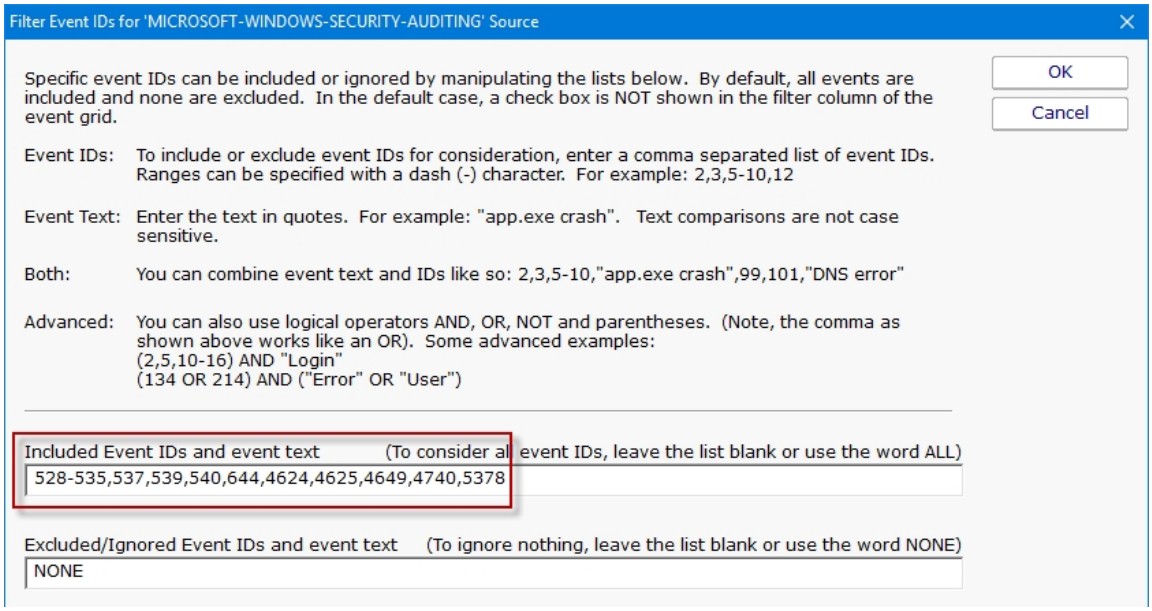
Create the Event Log monitor

1. Create an Event Log monitor on the server that you want to check. It's OK if there is already an existing Event Log monitor on the server -- you can have multiple monitors of any type on a server, or you can combine the steps below into your existing Event Log monitor.
2. Ensure the "Security" Event Log in the lower left corner is checked
3. In the large grid, go to the "Security" source (for Windows 2003 servers) or the "Microsoft Windows security auditing" source (for Windows 2008 or newer) and check the Audit Success and Audit Failure boxes. If both sources are available, check both (that way you'll be able to copy this monitor to other computers and it will work for both 2003 and 2008 servers).
4. In the source line(s) above, click the box in the first column labeled Filters. We're going to set a filter for the following Event IDs:
   - 528 - Successful Logon
   - 529 - Logon Failure: Unknown user name or bad password
   - 530 - Logon Failure: Account logon time restriction violation
   - 531 - Logon Failure: Account currently disabled
   - 532 - Logon Failure: The specified user account has expired
   - 533 - Logon Failure: User not allowed to logon at this computer
   - 534 - Logon Failure: The user has not been granted the requested logon type at this machine
   - 535 - Logon Failure: The specified account's password has expired
   - 537 - Logon Failure: An unexpected error occurred during logon
   - 539 - Logon Failure: Account locked out
   - 540 - Successful network logon
   - 644 - User Account Locked Out
   - 4624 - An account was successfully logged on
   - 4625 - An account failed to log on
   - 4649 - A replay attack was detected

- 4740 - A user account was locked out
- 5378 - The requested credentials delegation was disallowed by policy

  See http://support.microsoft.com/default.aspx?scid=kb;en-us;Q174073
  See http://support.microsoft.com/kb/947226

  To add the filter, add the following to the "Included Event IDs and event text" field:
  528-535,537,539,540,644,4624,4625,4649,4740,5378



You can adjust the list of Event IDs that are being filtered, and add additional filters for watching for particular text (like a specific username for example). To do that, just add more to the filter line.

Example Filters

Windows 2008 R2 Server Example:
If you are monitoring a Windows 2008 R2 Server and you want to alert on a logon success or failure, set the filter line to:
(4624,4625,5461) AND ("Logon Type: 10" OR "Logon Type: 2")

Windows 2003 Server Example:
If you are monitoring a Windows 2003 Server and you want to alert on a logon success or failure, set the filter line to:
(528-535,537,539,540,644) AND ("Logon Type: 9" OR "Logon Type: 3")

***Note:** The Event IDs list in the above examples are **not** all inclusive and you should verify the Event IDs that you need to monitor for.

Now this Event Log monitor will alert on logons and failed logons to the server that it's monitoring. Add actions (the Email Action for example) to specify how you want to be alerted.

References:

http://blogs.msdn.com/b/ericfitz/archive/2004/12/09/279282.aspx

http://blogs.msdn.com/b/ericfitz/archive/2007/05/08/the-trouble-with-logoff-events.aspx

http://blogs.msdn.com/b/ericfitz/archive/2008/08/20/tracking-user-logon-activity-using-logon-events.aspx

http://blogs.msdn.com/b/ericfitz/archive/2009/06/10/mapping-pre-vista-security-event-ids-to-security-event-ids-in-vista.aspx

http://support.microsoft.com/default.aspx?scid=kb;EN-US;947226

http://www.microsoft.com/download/en/details.aspx?DisplayLang=en&id=17871

http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=21561

http://www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx

How to Automate Satellite Deployment

Deploying the Satellite service to remote computers can be done with a few operations. Essentially the Satellite has to be installed and then told where the Central Monitoring Service is.

Get Files to Remote Server

The installer comes with the Central Monitoring Service, the Satellite and the Console. You need to get the installer onto the target computer. This can be done via your own copy/delivery operation. You have the option of fetching the Setup.exe from the Central Monitoring Service via an HTTPS call. At installation time, the installer copies itself to C:\Program Files\PA Server Monitor\Install\Setup.exe, which is available from:
https://{central server name}:{configured port}/$INSTALL_PATH$/Setup.exe (including the $ characters).

A registry file will also be needed (discussed below). You could copy that to the Install directory above, and reference the file via URL using $INSTALL_PATH$/{your registry file}

Install Satellite

Once the Setup.exe program is on the target server, start it with the following command line:

```
Setup.exe /SP- /VERYSILENT /SUPPRESSMSGBOXES /NORESTART /TYPE=satellite /TASKS="!desktopicon,!nacli"
```

Documentation about these parameters and their meaning is available at
http://unattended.sourceforge.net/InnoSetup_Switches_ExitCodes.html

Directing the Satellite

The Satellite will connect to the Central Monitoring Service indicated by a registry setting. The registry key is:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor
```

Note: On 64-bit operating systems, the key is actually under HKEY_LOCAL_MACHINE\Software\Wow6432Node

The registry settings to set are:

ServiceHostName - The hostname or IP address of the Central Monitoring Service

ReportHTTPPort - The port that the Central Monitoring Service is listening on. This is configurable.

Agent_Name (optional) - The name of the Satellite that should show up in Consoles and reports. The local computer name will be used if this is left blank.

An example registry file is shown below.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\software\PAServerMonitor]
"Agent_Name"="Dr. Johnson's Dentist Office"
"ReportHTTPPort"=dword:00000051
"ServiceHostName"="MYPUBLIC.HOST.NAME"
```

Note: The ReportHTTPPort dword value above must be in hexidecimal

You can run RegEdit and point it at a registry file like the example above, or launch the Satellite with the /HOST command line to set the ReportHTTPPort and ServiceHostName registry values:

```
ServerMonitorSatellite.exe /HOST=MYPUBLIC.HOST.NAME:81 /END
```

The /END option tells the Satellite process to stop after it processes the command line (it's not running as a service if you've launched it this way, so no reason to keep running).

Start Satellite

Once the above steps are complete, you can start the Satellite service using:

```
net start "PA Server Monitor Satellite"
```

The Satellite will now connect to the Central Monitoring Service and wait to be accepted (see Configuring the Satellite Monitoring Service, the last few steps).

You can now add servers and monitors to be monitored by the Satellite just like you would for monitoring from the Central Monitoring Service -- just indicate that the Satellite will monitor the server when adding it (see Adding Computers).

How to Disable Remote UAC

If you are getting Access Denied errors when trying to connect to a server, even though you are using administrator credentials, your problem may be UAC-related.

UAC Policy

The UAC policy "**User Account Control: Run all administrators in Admin Approval Mode**" sometimes makes remote requests fail to run as a true admin since there is no way to show the UAC permission dialog.

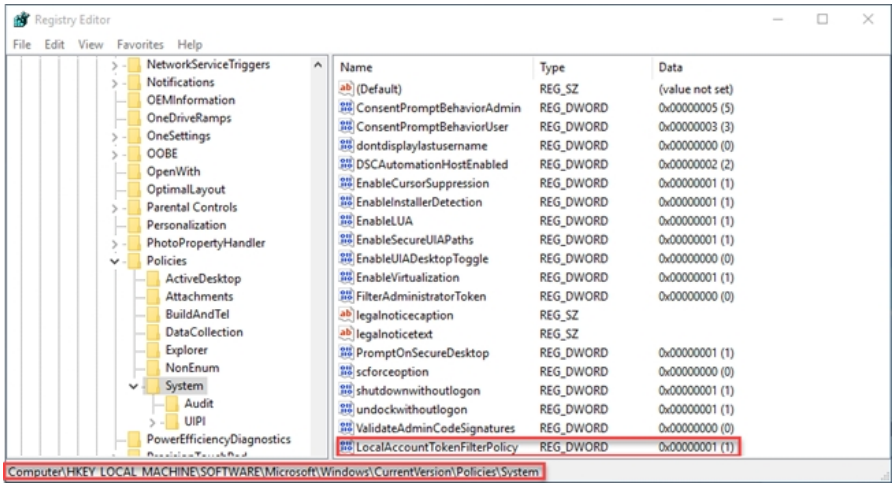
Remote UAC

If you are trying to access the server, you may get a message that says "**Access Denied- Failed to connect to the ADMIN$ share**" even if you have already given the server admin status. The target system likely has **Remote UAC** running, which blocks local servers from operating in an elevated mode while connected to the network. To disable Remote UAC, you can edit the registry by following these steps:

1. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**.

2. Create a DWORD value named **LocalAccountTokenFilterPolicy** and set it to **1**.

3. Reboot, or restart the server service.



How to Embed Child Reports in Parent Reports

Customers often want to show custom reports for child groups in parent groups. This can be done by showing an IFRAME in the parent group using the child group's URL. The technique below will show how to automatically determine the child URLs to use from a parent group.

Implementation

For this approach, you will define two Custom Report/Executive Summary reports. We recommend doing this on the Servers/Devices group so all groups below will inherit these definitions.

One custom report will be for the Parent level, and another will be for all the Child (sub-group) reports.

Create and define the Child Custom Report first with whatever content you want in it.

In the Child Custom Report, set the Report Title field to "NONE" (without the quotes). That will make it look a little better (this will promote the group names to bigger headers in the report).

In the Parent report, add an HTML: Custom Block and put the code below in it:

```
<script>

  function resizeIframe(obj) {
 obj.style.height = obj.contentWindow.document.body.scrollHeight + 'px';
  }

</script>

$for{childID in paGetGroupChildIDs(objID)}
   <iframe  src="https://127.0.0.1:81/STATUS_CUSTOM_(16_${childID})/index.html?
  CMD=REFRESH_REPORT&RTYPE=16&ROBJ=${childID}&hideMenu=1"
    frameborder="0" scrolling="no" style="width:100%;"
    onload="resizeIframe(this);" > </iframe>
$rof
```

Ths above code will add an IFRAME pointing to each of the Child group Custom Reports. This way you can open the top level company report, and it will also show the child reports within the report.

You will need to change the red values. Figuring out what to replace the **16** with is a tiny bit tricky, but it can be done:

View one of the child Custom Reports (for any group, it doesn't matter which one).

Click the Open in Browser button so the report is opened in a browser. It might take you to the login screen, and that is OK.

Look at the URL. There is an RTYPE value there. It will be one of 14, 15, 16 or 17. Whatever is there is what you put in place of the 16's in the code example above.

Now you can go to the Parent Custom Report and you should see each Child Custom Report embedded within it.

How to Extract Data from PA Server Monitor

Data for PA Server Monitor is stored in a database, and some customers want to access that data for additional uses. This is fairly easy to do. Reading data is fine. **We recommend NOT writing** to the databases.

SQLite or MS SSQL?

Before you go much further, you need to know if you are using the embedded SQLite databases, or a MS SQL Server database. This can be seen in the Database Settings dialog. Your application will either use the same or a similar connection string to connect to the MS SQL Server database, or one of the many available connectors for the SQLite databases.

Statistics

The most common case requested is access to the numeric data such as comes from performance counters, disk space measurements, ping and web page response times, etc.

To find the data you want, look in the Statistics table. The rows in this table define each individual statistic for which data is kept. The **CompID column** is the ID for the device. You can see these IDs in the Console by choosing the View > Show Object IDs in Navigation Tree menu option. You can also look in the ConfigCompInfo table to map computer names to CompIDs.

SQLite vs MS SQL Server: Unlike MS SQL Server which keeps all the data in a single database, with SQLite data is split up among separate databases in separate database files. These are kept in a folder shown in the Database Settings page.

There will be a separate database file per monitor type. For example, Ping response data is kept in PingResponse.db and Disk Space data is kept in FreeDiskSpace.db. The ConfigCompInfo table is in the ConfigInfo.db file.

Each SQLite database file will contain the Statistics table, and the StatData table. With MS SQL Server, there is a single Statitics table for all monitor types. There may be a single StatData table, or that table might have been split into multiple tables for large installations.

When searching the Statistics table for the data you want, look at the **OwnerType column** - this indicates the type of monitor that the data came from. The values for Owner Type are:

Monitor Type	Owner Type
Bandwidth Monitor	38
Citrix Monitor	21
Disk Space	1
Environment Monitor	20
Execute Script (custom values)	5
FTP Monitor	24
Performance Monitor	4
Ping Monitor	8
Server Temperature	15
Service Monitor (up/down state)	3

SNMP Monitor	18
Web Page Monitor	6
Plugin Monitor	42

SQLite Locking: When doing reads or writes to an SQLite database, the entire database file is locked for everyone. So make sure your queries run as quickly as possible so the database locking doesn't affect the monitoring process.

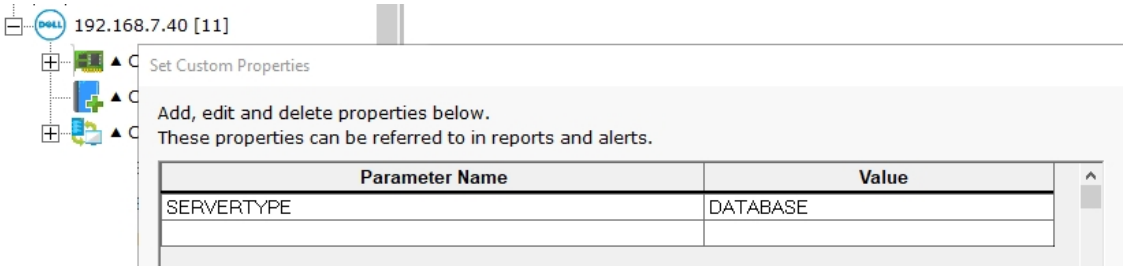
How to Dynamically Group Devices

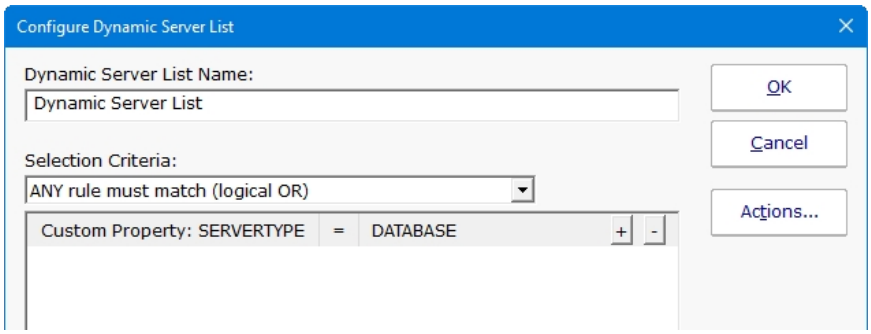
Servers/devices 'live' in one group at a time. You can drag (move) servers/devices into a different group by dragging it in the Console. However, sometimes you want the server or device to show up in more than one group. This is one method to accomplish this.

Rules Based Grouping

Using the Dynamic Server List, you can define rules that will create a list of servers. One powerful way to create a list of your choosing is to base the list on which servers have a specific custom property that you specify. Then you can create a list of all servers that have that property.

For example, you might add a custom property of "SERVERTYPE" and set it equal to "DATABASE". Then you could create a Dynamic Server List that finds all servers where USAGE=DATABASE as shown below:





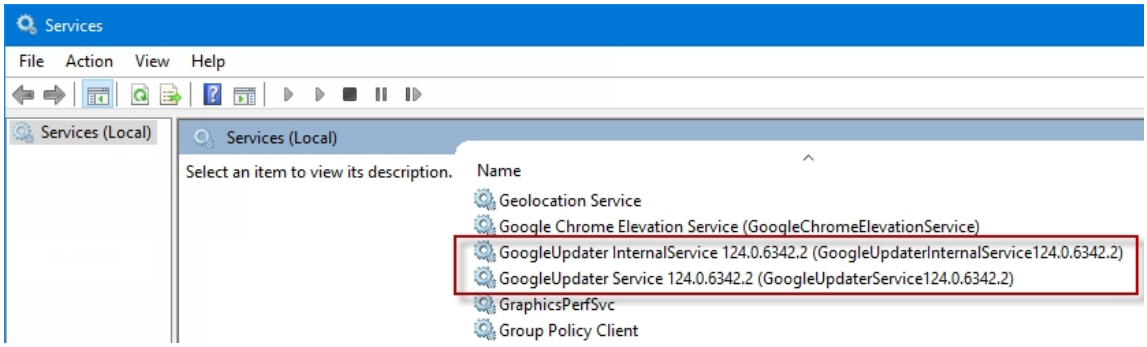
Once this Dynamic Server List is created, you can create a Dynamic Group which is based on the output of the list. Using this technique, you can arbitrarily assign any server/device to a group by setting a property on that server/device and have it automatically show up in your desired group.

Creating a Dynamic Group is as easy as right-clicking on Servers/Devices and choosing Create New Dyanmic Group, and then selecting the server list that will populate that group. As the Dynamic Server List monitor runs and updates the server list, the group will also update to match the server list.

To automate monitoring configuration, you can use this tip and add monitor templates to the dynamic group to automatically apply monitors to specific types of servers/devices.

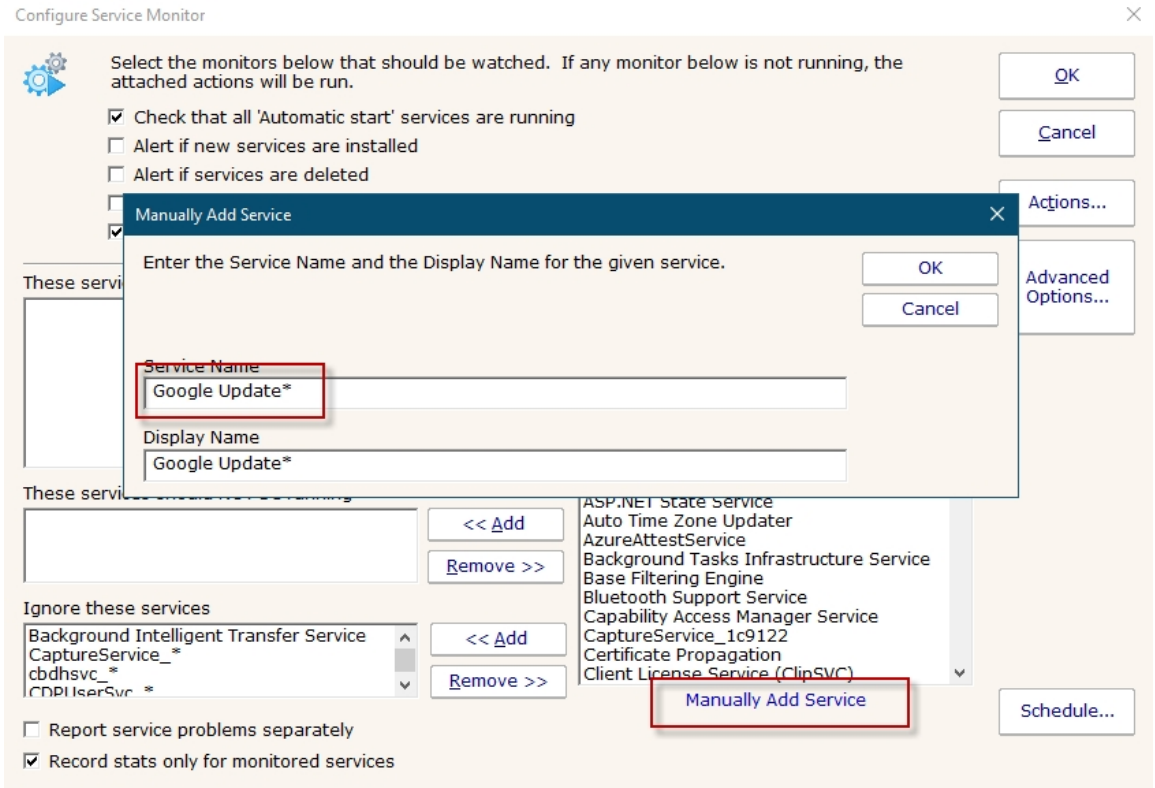
How to Ignore Google Update Services

The Google Chrome browser comes with a service that keeps the browser up to date. Sometimes this service has a version attached, which means the service name keep changing over time.



In that past you could just ignore the Google Update service, but since the name keeps changing that no longer works.

The solution is to add a custom service named Google Update* and ignore it. This way you ignore all service names that begin with Google. If you want to be less precise, you could ignore Google*



Once this new service is added, you can select it in the list on the right side and press the << Add button to add it to the Ignore these services list.

Now when a new Google Update service is installed, it will continue to be ignored.

How to Integrate with PA Server Monitor

PA Server Monitor has a variety of ways to integrate into your business to help support business needs. A few integration points and ideas are listed below.

Sending Alerts to External Systems

PagerDuty
: Use the built-in PagerDuty Action to forward notifications and fixed events.

SIEM Systems
: Security Information and Event Management systems often accept incoming data via Syslog or SNMP Trap.

Slack
: This HOWTO page shows how to use the Call URL action to forward alerts to Slack

Ticketing System
: Many customers use the Call URL action to put tickets into their helpdesk/trouble ticket system.

Execute Script
: The Execute Script action can be used to run VBScript, Javascript and Powershell scripts to send alerts to your existing systems.

Run Program
: Some customers use the Start Application action to pass alert details to other programs.

Enterprise Configuration Syncing

A number of customers need to keep their configuration management (often home-grown systems) in sync with their monitoring so nothing slips through the cracks.

Sync Current System Lists
: Most of the External API is useful for keeping track of what is monitored.

Sync Current Network Devices
: The `ConfigComputerInfo` and `ConfigGroupInfo` tables are specifically for external application usage to see what computers are being monitored.

Automatically Monitor New Devices
: The Network Scanner can run periodically and discover new devices on the network and start monitoring them.

Custom Monitors

Plugins
: The Plugin Monitor can use custom built plugins, including those compatible with Nagios.

Execute Script
: The Execute Script monitor can do customized checks via VBScript, Javascript, Powershell and SSH scripts.

Watch Custom Windows Applications and Services
: The Performance Monitor will watch performance counter from any application that provides them, and the Service Monitor can watch any service, whether originally part of Windows or not.

Watch Any SNMP Counter
: The SNMP Monitor can watch virtually any counter provided by any device that can expose its counters to the network.

Extending Report Usage

Show Reports
: Besides showing some reports on large screens in the IT department, some people show reports in an IFRAME on their own report page.

Generate Chart Images
: The External API's `CREATE_CHART` command can generate chart images like those on the server status reports.

Use Existing Charts

Some customers will show charts in existing Scheduled Report from their own web-based report via simple HTTPS link to the image .

Import Raw Monitored Data

Some customers have their Scheduled Reports write out CSV files that are imported into their other systems for processing.

Direct Data Usage

Extract Data

You can extract data from the PA Server Monitor databases for use in your own systems.

How to Monitor ASP.NET

Below are recommendations for monitoring ASP.NET performance counters. There are many counters that can be used to monitor ASP.NET; the list below are some of the most suggested counters to monitor. Although these are suggested counters there isn't much on suggested thresholds for them because the number of applications running will vary too widely to get an accurate thresholds. The best practice would be to start monitoring and collecting data for the counters and then set the threshold values at a later date.

ASP.NET Counters

.NET Counters

Counter Path
.NET CLR Exceptions(*)\# of Exceps Thrown / sec
.NET CLR Loading(*)\Current Assemblies
.NET CLR Loading(*)\Bytes in Loader Heap
.NET CLR Memory(*)\Allocated Bytes/sec
.NET CLR Memory(*)\% Time in GC
.NET CLR Memory(*)\# Bytes in all Heaps
.NET CLR Memory(*)\% Time in GC
.NET CLR Memory(*)\# Gen 0 Collections
.NET CLR Memory(*)\# Gen 1 Collections
.NET CLR Memory(*)\# Gen 2 Collections

ASP.NET Counters

Counter Path
\Application Restarts
\Applications Running
\Request Execution Time
\Request Wait Time
\Requests Current
\Requests Queued
\Requests Rejected
\Worker Process Restarts

ASP.NET Application Counters

Counter Path
\Anonymous Request/Sec
\Cache API Hit Ratio
\Cache Total Hit Ratio
\Errors During Execution
\Errors Total
\Errors Total/sec
\Errors Unhandled During Execution
\Requests Executing
\Requests Failed
\Requests In Application Queue
\Requests Timed Out
\Request Wait Time

\Requests Total
\Requests/Sec

Other Counters to Monitor

Most technical sources suggest the following performance counters should be monitored with all ASP.NET applications.

Counter Path
Processor Counter\% Processor Time
Memory Counter\Available Mbytes
System Counter\Context Switches/sec
Web Service Counters\Current Connections
Web Service Counters\Total Method Requests/sec
Web Service Counters\ISAPI Extension Requests/sec

References

http://msdn.microsoft.com/en-us/library/ms972959.aspx

How to - Monitor Backup Success

Everyone knows that backing up data is absolutely critical. Most of us have processes in place for backup software to run periodically and perform backups. But if those backups silently fail, they don't have any value. So monitoring to make sure that backups are succeeding is important.

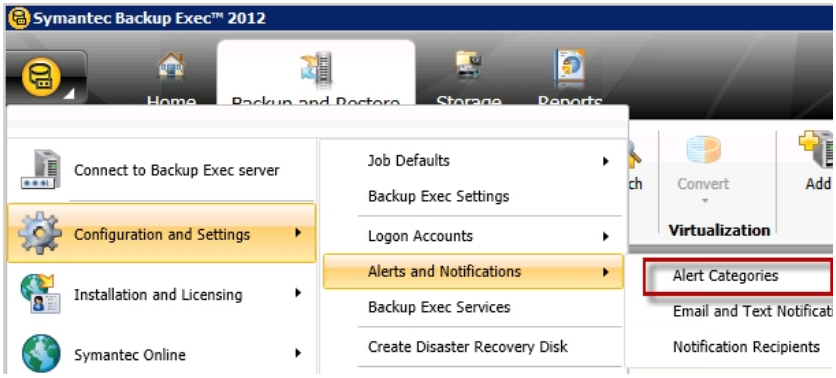
Most backup software reports success or failure by writing to an Event Log. This HOWTO will describe how to use the Event Validator monitor in PA Server Monitor to monitor scheduled backups of a few popular backup products.

We've done some research to find common backup products and their success events which are shown below. Check your server's Event Log to find the exact values to use. If you have additions (or corrections) for this list, please contact us.

Product	Event Log	Source	Event ID	Message
Backup Exec	Application	Backup Exec	34112	Backup job completed successfully.
Windows Backup	Microsoft-Windows-Backup	Microsoft-Windows-Backup	4	Backup finished successfully.
Acronis Backup & Recovery 11.5	Application	Acronis Backup & Recovery 11.5 Agent Core	1	Running backup plan [Name of Backup] has completed successfully.
Veeam Backup & Replication	Veeam Backup	Veeam Backup Events	150	VM [VM Name] task has finished with [Status] state. VM task details: [reason of the warning/failure].

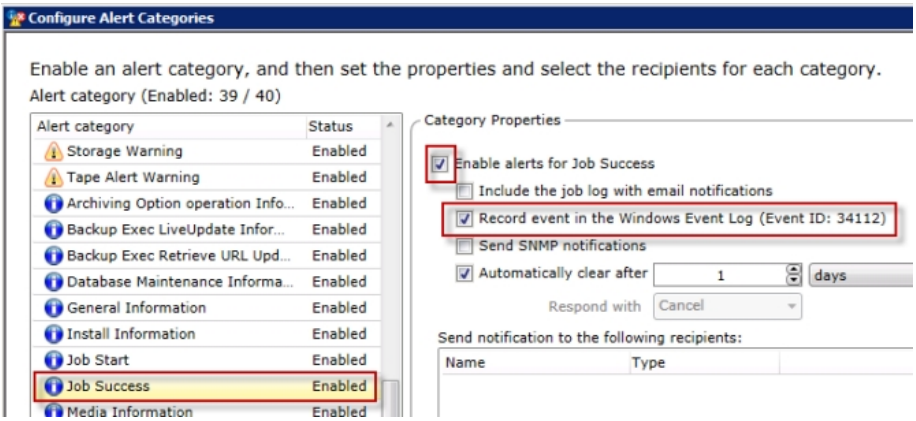
Symantec Backup Exec 2012

Symantec allows you to select the Event IDs that are recorded in the Windows Application Event Log. To view, select, or edit the event IDs that are recorded in the Application Event Log, open Symantec Backup Exec and go to Configuration and Settings -> Alerts and Notifications -> Alert Categories.

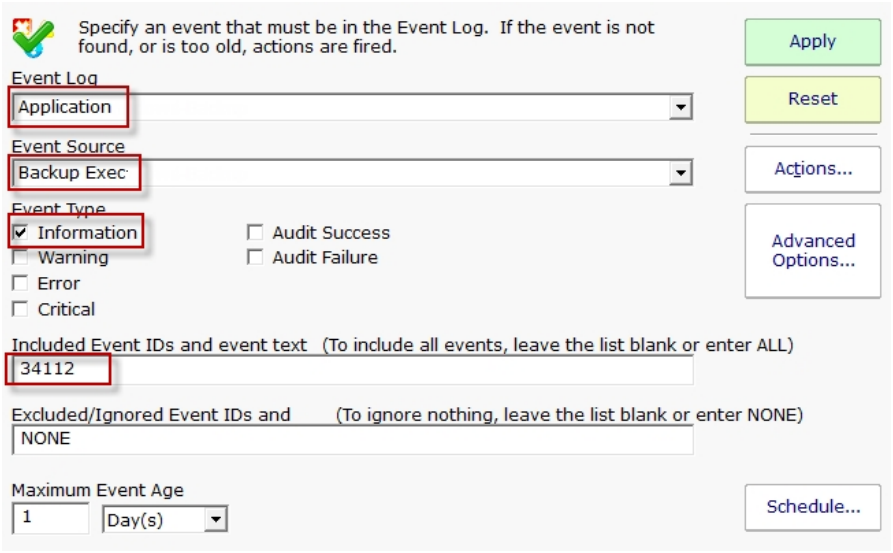


By default Symantec **dose not** record the "Job Success" (event ID 34112) in the log file. In the Configure Alert Categories menu scroll

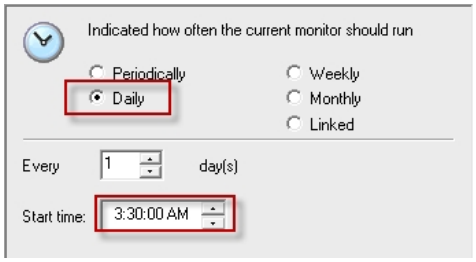
to find "Job Success" and select it. On the right, in Category Properties, enable the alert and check the "Record event in the Windows Event Log (Event ID: 34112)" option.



Add an Event Validator monitor to the server where Symantec Backup Exec is installed and running. To monitor for backup "Job Success" edit the monitor to include the following setting. Edit the Maximum Event Age as needed

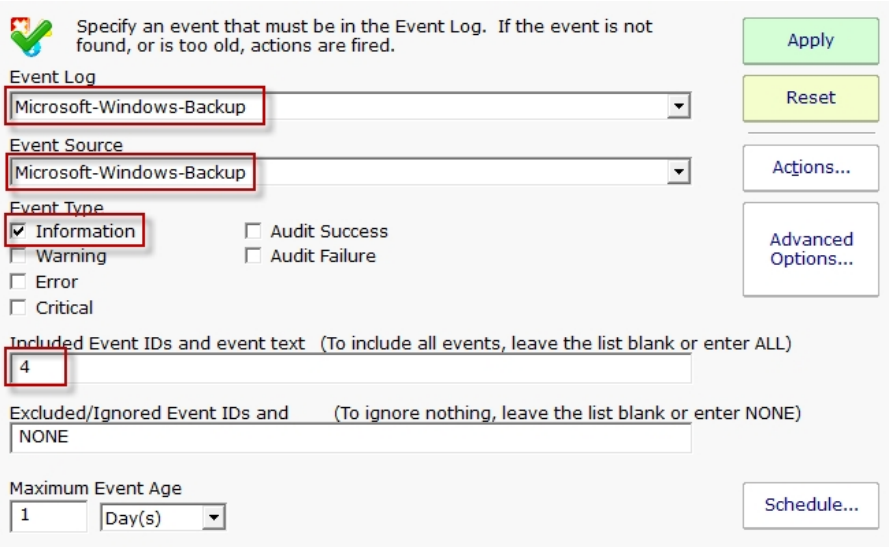


Now any time the monitor runs and does NOT see the 34112 Event ID, it will fire actions. The last trick is to make sure the monitor only runs after a backup should have completed. So if your backups normally run daily from 1:00am to 3:00am for example, set the monitor to run daily at 3:30am. If you don't want to be alerted at 3:30am in the morning, perhaps daily at 8:00am would better :)

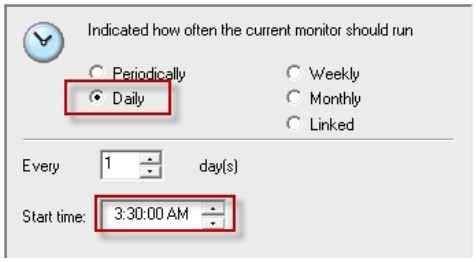


Microsoft Server Backup

Add an Event Validator monitor to the server where Microsoft Server Backup is installed and running. To monitor for backup "Job Success" edit the monitor to include the following setting. Edit the Maximum Event Age as needed



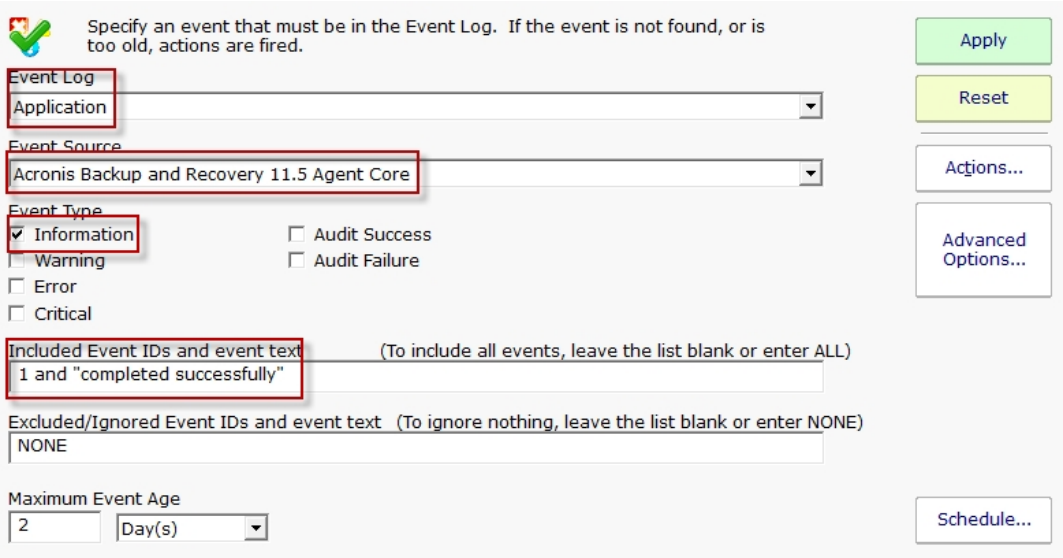
Now any time the monitor runs and does NOT see the 4 Event ID, it will fire actions. The last trick is to make sure the monitor only runs after a backup should have completed. So if your backups normally run daily from 1:00am to 3:00am for example, set the monitor to run daily at 3:30am. If you don't want to be alerted at 3:30am in the morning, perhaps daily at 8:00am would better :)



Here is a link to find other Microsoft Server Backup Event IDs. :)

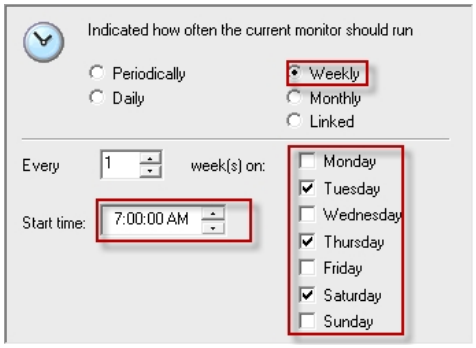
Acronis Backup & Recovery 11.5

Add an Event Validator monitor to the server where Acronis Backup & Recovery is installed and running. To monitor for backup "Job Success" edit the monitor to include the following setting. Edit the Maximum Event Age as needed



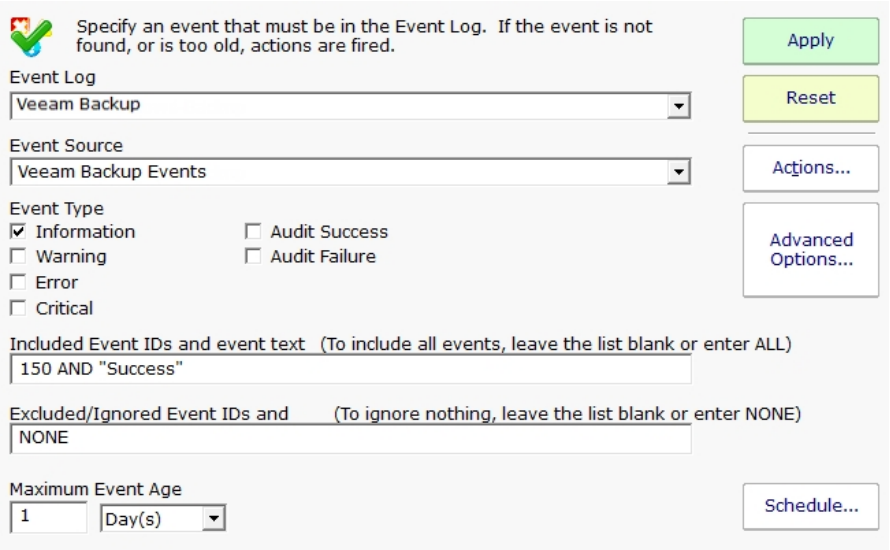
Note: Acronis records all of their events under the Event ID of 1. To be able to monitor for the a successful backup you will need to monitor for some Event Text. In the example above you will see that we are looking for Event ID of 1 and for the text "Quinn's Backup" and "completed successfully". Acronis will put into the event text the name of Acronis's "Backup Plan" and the words "completed successfully" when the backup plan has completed successfully.

Now any time the monitor runs and does NOT see the items listed in the Include Event ID's and Event Text text box, it will fire actions. The last trick is to make sure the monitor only runs after a backup should have completed. So if your backups normally run on Tuesday, Thursday, and Saturday from 1:00am to 6:00am for example, set the monitor to run Weekly on those same days at 7:00am.



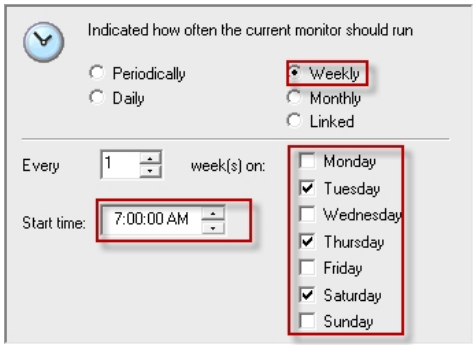
Veeam Backup & Replication

Add an Event Validator monitor to the server where Veeam Backup & Replication is installed and running. To monitor for backup "Job Success" edit the monitor to include the following setting. Edit the Maximum Event Age as needed



Note: Veeam Backup & Replication records their backup status events under the Event ID of 150 and uses text such as "Warning", "Error", or "Success" to report the status of the backup. In the example above you will see that we are looking for Event ID 150 and for the text "Success".

Now any time the monitor runs and does NOT see the items listed in the Include Event ID's and Event Text text box, it will fire actions. The last trick is to make sure the monitor only runs after a backup should have completed. So if your backups normally run on Tuesday, Thursday, and Saturday from 1:00am to 6:00am for example, set the monitor to run Weekly on those same days at 7:00am.



Here is a link to find other Veeam Backup Event IDs that you may need to know. :)

How to Monitor Databases

There are a few simple approaches that work for easily monitoring databases.

Performance Counters

The Microsoft SQL Server database publishes many performance counters. The Performance Monitor can monitor any of them. MSDN has a recommended list of counters that can be monitored.

In addition, other database servers like MySQL can also be monitored via SNMP. Other databases likely have similar functionality.

Poll Database

The Execute Script monitor can periodically connect to a database and perform a check. The first example script shows how to do that. This method even lets you easily check on a database value (table size for example).

Web Page Check

Create a web page that connects to the database and then returns something like "OK" or "Problem". The Web Page monitor could then check that page and alert if it didn't see "OK". That web page could of course perform any sorts of checks that you need.

How to Monitor Microsoft Exchange

Below are some recommendations for monitoring a Microsoft Exchange installation. These steps generally refer to Exchange 2010, but most of the details also apply to other versions as well.

PA Server Monitor's Smart Config procedure will create default monitors to check the overall health of the server that Exchange is installed on.

To automatically create monitors that watch for Exchange-specific details, download the Exchange Monitoring Template and import it to each server that is running an Exchange role. The template will automatically get tailored to the specific roles running on a server.

Exchange 2010 Template.txml

Note: We are always trying to improve. If you have suggestions for this template, please contact us.

Exchange Roles

Exchange 2010 is split up into a variety of roles. These roles consist of different software, services and performance counters. The roles can be installed on the same server or separate servers. Shown below are services and counters to be monitored regardless of where it is installed.

Service Note: Services marked with a * are optional or not automatically started. If the service isn't set to Automatic start when the template is imported, it will not be monitored.

Performance Counter Note: Counters that are marked with (c) are increasing counters (usually error counters). Any time they change value should be looked into. Also, many of the performance counter thresholds depend on the size of the Exchange installation (ie how many mail boxes, servers, etc). The imported template monitors will be in Automatic Training mode for a few days so the thresholds can be monitored and automatically adjusted to fit the specific servers being monitored.

Mailbox Role

Services

Service Name	Short Name
Microsoft Exchange Active Directory Topology	MSExchangeADTopology
Microsoft Exchange Information Store	MSExchangeIS
Microsoft Exchange Mail Submission	MSExchangeMailSubmission
Microsoft Exchange Mailbox Assistants	MSExchangeMailboxAssistants
Microsoft Exchange Monitoring*	MSExchangeMonitoring
Microsoft Exchange Replication Service*	MSExchangeRepl
Microsoft Exchange RPC Client Access*	MSExchangeRPC
Microsoft Exchange Search Indexer	MSExchangeSearch
Microsoft Exchange Search Indexer*	MSExchangeSearch
Microsoft Exchange Server Extension for Windows Server Backup	WSBExchange
Microsoft Exchange Service Host	MSExchangeServiceHost
Microsoft Exchange System Attendant	MSExchangeSA
Microsoft Exchange Throttling	MSExchangeThrottling
Microsoft Exchange Transport Log Search*	MSExchangeTransportLogSearch
Microsoft Search (Exchange Server)*	msftesql-Exchange

Counter Path	Default Threshold
Database\Database Page Fault Stalls/sec	=0
Database\Log Record Stalls/sec	<100
Database\Log Threads Waiting	<10
MSExchange ADAccess Domain Controllers(*)\LDAP Read Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Search Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Searches timed out per minute	<10
MSExchange ADAccess Domain Controllers(*)\Long running LDAP operations/Min	<50
MSExchange ADAccess Processes(*)\LDAP Read Time	<100
MSExchange ADAccess Processes(*)\LDAP Search Time	<100
MSExchange Assistants - Per Assistant(*)\Average Event Processing Time in Seconds	<2
MSExchange Calendar Attendant\Requests Failed	=0 (c)
MSExchange Database ==> Instances(*)\Log Generation Checkpoint Depth	<500
MSExchange Database Instances(*)\I/O Database Reads Average Latency	<50
MSExchange Database Instances(*)\I/O Database Writes Average Latency	<50
MSExchange Database(Information Store)\Database Cache % Hit	>= 90
MSExchange Database(Information Store)\Log Record Stalls/sec	<100
MSExchange Database(Information Store)\Log Threads Waiting	<10
MSExchange Database(Information Store)\Version buckets allocated	<12000
MSExchange Database\I/O Database Reads (Attached) Average Latency	<1000
MSExchange Database\IO Log Read Average Latency	<1000
MSExchange Database\IO Log Writes Average Latency	<10
MSExchange Database\Log Bytes Write/sec	<10000000
MSExchange Replication(*)\CopyQueueLength	=0
MSExchange Resource Booking\Requests Failed	=0 (c)
MSExchange Search Indices(*)\ Average Document Indexing Time	<30000
MSExchange Store Interface(*)\RPC Requests failed (%)	=0
MSExchange Store Interface(*)\RPC Slow Requests (%)	=0
MSExchange Store Interface(_Total)\RPC Latency average (msec)	<100
MSExchange Store Interface(_Total)\RPC Requests outstanding	=0
MSExchangeIS Client (*)\RPC Average Latency	<50
MSExchangeIS Mailbox(*)\Search Task Rate	<10
MSExchangeIS Mailbox(*)\Slow Findrow Rate	<10
MSExchangeIS Mailbox(_Total)\Messages Queued for Submission	<50
MSExchangeIS Mailbox\RPC Averaged Latency	<11
MSExchangeIS Public(_Total)\Messages Queued for Submission	<20
MSExchangeIS Public(_Total)\Replication Receive Queue Size	<100
MSExchangeIS\Client: RPCs Failed:Server Too Busy/sec	=0
MSExchangeIS\RPC Averaged Latency	<11

MSExchangeIS\RPC Requests	<70
MSExchangeIS\Slow QP Threads	<10
MSExchangeIS\Slow Search Threads	<10
MSExchangeMailSubmission(*)\Failed Submissions Per Second	=0
MSExchangeMailSubmission(*)\Hub Servers In Retry	=0
MSExchangeMailSubmission(*)\Temporary Submission Failures/sec	=0
Process(Microsoft.Exchange.Search.ExSearch)\% Processor time	<5
Process(MSExchangeMailboxAssistants)\% Processor Time	<5

Client Access Role

Services

Service Name	Short Name
Internet Information Services Admin Service	IISAdmin
Microsoft Exchange Active Directory Topology Service	MSExchangeADTopology
Microsoft Exchange Address Book	MSExchangeAB
Microsoft Exchange File Distribution Service	MSExchangeFDS
Microsoft Exchange Forms-Based Authentication	MSExchangeFBA
Microsoft Exchange IMAP4*	MSExchangeIMAP4
Microsoft Exchange Mailbox Replication Service*	MSExchangeMailboxReplication
Microsoft Exchange Monitoring*	MSExchangeMonitoring
Microsoft Exchange POP3*	MSExchangePOP3
Microsoft Exchange Protected Service Host	MSExchangeProtectedServiceHost
Microsoft Exchange RPC Client Access	MSExchangeRPC
Microsoft Exchange Service Host	MSExchangeServiceHost
World Wide Web Publishing Service	W3SVC

Performance Counters

Counter Path	Default Threshold
ASP.NET Applications(*)\Requests In Application Queue	>0
ASP.NET\Application Restarts	=0 (c)
ASP.NET\Request Wait Time	=0
ASP.NET\Worker Process Restarts	=0 (c)
MSExchange ActiveSync\Requests Queued	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Read Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Search Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Searches timed out per minute	<10
MSExchange ADAccess Domain Controllers(*)\Long running LDAP operations/Min	<50
MSExchange ADAccess Processes(*)\LDAP Read Time	<100
MSExchange ADAccess Processes(*)\LDAP Search Time	<100
MSExchange Availability Service\Average Time to Process a Free Busy Request	<5
MSExchange Control Panel\Outbound Proxy Requests - Average Response Time	<6000
MSExchange Control Panel\Requests - Average Response Time	<6000
MSExchange OWA\Average Search Time	<5000
MSExchange RpcClientAccess\RPC Averaged Latency	<250

MSExchange RpcClientAccess\RPC Requests	<40
MSExchangeAB\NSPI RPC Browse Requests Average Latency	<1000
MSExchangeAB\NSPI RPC Requests Average Latency	<1000
MSExchangeAB\Referral RPC Requests Average Latency	<1000
MSExchangeFDS:OAB(*)\Download Task Queued	=0 (c)
RPC/HTTP Proxy\Number of Failed Back-End Connection attempts per Second	=0

Hub Transport Role

Services

Service Name	Short Name
Microsoft Exchange Active Directory Topology Service	MSExchangeADTopology
Microsoft Exchange Anti-spam Update*	MSExchangeAntispamUpdate
Microsoft Exchange EdgeSync*	MSExchangeEdgeSync
Microsoft Exchange Monitoring*	MSExchangeMonitoring
Microsoft Exchange Protected Service Host	MSExchangeProtectedServiceHost
Microsoft Exchange Service Host	MSExchangeServiceHost
Microsoft Exchange Transport Log Search*	MSExchangeTransportLogSearch
Microsoft Exchange Transport	MSExchangeTransport
Microsoft Search (Exchange Server)*	msftesql-Exchange

Performance Counters

Counter Path	Default Threshold
\MSExchangeTransport Queues(_total)\Active Mailbox Delivery Queue Length	<250
\MSExchangeTransport Queues(_total)\Active Non-Smtp Delivery Queue Length	<250
\MSExchangeTransport Queues(_total)\Active Remote Delivery Queue Length	<250
\MSExchangeTransport Queues(_total)\Aggregate Delivery Queue Length (All Queues)	<5000
\MSExchangeTransport Queues(_total)\Largest Delivery Queue Length	<200
\MSExchangeTransport Queues(_total)\Poison Queue Length	=0
\MSExchangeTransport Queues(_total)\Retry Mailbox Delivery Queue Length	<100
\MSExchangeTransport Queues(_total)\Retry Non-Smtp Delivery Queue Length	<100
\MSExchangeTransport Queues(_total)\Retry Remote Delivery Queue Length	<100
\MSExchangeTransport Queues(_total)\Submission Queue Length	<100
\MSExchangeTransport Queues(_total)\Unreachable Queue Length	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Read Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Search Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Searches timed out per minute	<10
MSExchange ADAccess Domain Controllers(*)\Long running LDAP operations/Min	<50

MSExchange ADAccess Processes(*)\LDAP Read Time	<100
MSExchange ADAccess Processes(*)\LDAP Search Time	<100
MSExchange Database ==> Instances(edgetransport/Transport Mail Database)\Version buckets allocated	<200
MSExchange Database ==> Instances(edgetransport/Transport Mail Database)\Log Record Stalls/sec	<10
MSExchange Database ==> Instances(edgetransport/Transport Mail Database)\Log Threads Waiting	<10
MSExchange Extensibility Agents(*)\Average Agent Processing Time (sec)	<20

Edge Transport Role

Services

Service Name	Short Name
Microsoft Exchange ADAM	ADAM_MSExchange
Microsoft Exchange Anti-spam Update*	MSExchangeAntispamUpdate
Microsoft Exchange Credential Service	MSExchangeEdgeCredential
Microsoft Exchange Monitoring*	MSExchangeMonitoring
Microsoft Exchange Service Host	MSExchangeServiceHost
Microsoft Exchange Transport Log Search*	MSExchangeTransportLogSearch
Microsoft Exchange Transport	MSExchangeTransport

Performance Counters

Counter Path	Default Threshold
\MSExchangeTransport Queues(_total)\Active Mailbox Delivery Queue Length	<250
\MSExchangeTransport Queues(_total)\Active Non-Smtp Delivery Queue Length	<250
\MSExchangeTransport Queues(_total)\Active Remote Delivery Queue Length	<250
\MSExchangeTransport Queues(_total)\Aggregate Delivery Queue Length (All Queues)	<5000
\MSExchangeTransport Queues(_total)\Largest Delivery Queue Length	<200
\MSExchangeTransport Queues(_total)\Poison Queue Length	=0
\MSExchangeTransport Queues(_total)\Retry Mailbox Delivery Queue Length	<100
\MSExchangeTransport Queues(_total)\Retry Non-Smtp Delivery Queue Length	<100
\MSExchangeTransport Queues(_total)\Retry Remote Delivery Queue Length	<100
\MSExchangeTransport Queues(_total)\Submission Queue Length	<100
\MSExchangeTransport Queues(_total)\Unreachable Queue Length	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Read Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Search Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Searches timed out per minute	<10
MSExchange ADAccess Domain Controllers(*)\Long running LDAP operations/Min	<50

MSExchange ADAccess Processes(*)\LDAP Read Time	<100
MSExchange ADAccess Processes(*)\LDAP Search Time	<100
MSExchange Database ==> Instances(edgetransport/Transport Mail Database)\Version buckets allocated	<200
MSExchange Database ==> Instances(edgetransport/Transport Mail Database)\Log Record Stalls/sec	<10
MSExchange Database ==> Instances(edgetransport/Transport Mail Database)\Log Threads Waiting	<10
MSExchange Extensibility Agents(*)\Average Agent Processing Time (sec)	<20

Unified Messaging Role (Optional)

Services

Service Name	Short Name
Microsoft Exchange Active Directory Topology Service	MSExchangeADTopology
Microsoft Exchange File Distribution	MSExchangeFDS
Microsoft Exchange Monitoring*	MSExchangeMonitoring
Microsoft Exchange Service Host	MSExchangeServiceHost
Microsoft Exchange Speech Engine	MSSpeechService
Microsoft Exchange Unified Messaging	MSExchangeUM

Performance Counters

Counter Path	Default Threshold
MSExchange ADAccess Domain Controllers(*)\LDAP Read Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Search Time	<100
MSExchange ADAccess Domain Controllers(*)\LDAP Searches timed out per minute	<10
MSExchange ADAccess Domain Controllers(*)\Long running LDAP operations/Min	<50
MSExchange ADAccess Processes(*)\LDAP Read Time	<100
MSExchange ADAccess Processes(*)\LDAP Search Time	<100
MSExchangeUMAvailability\% of Failed Mailbox Connection Attempts Over the Last Hour	<5
MSExchangeUMAvailability\% of Inbound Calls Rejected by the UM Service Over the Last Hour	<5
MSExchangeUMAvailability\% of Inbound Calls Rejected by the UM Worker Process Over the Last Hour	<5
MSExchangeUMAvailability\% of Messages Successfully Processed Over the Last Hour	>= 95
MSExchangeUMAvailability\% of Partner Voice Message Transcription Failures Over the Last Hour	<5
MSExchangeUMAvailability\Calls Disconnected on Irrecoverable Internal Error	=0 (c)
MSExchangeUMAvailability\Directory Access Failures	=0 (c)
MSExchangeUMAvailability\Total Inbound Calls Rejected by the UM Service	=0 (c)
MSExchangeUMAvailability\Total Inbound Calls Rejected by the UM Worker Process	=0 (c)
MSExchangeUMCallAnswer\\Calls Disconnected by Callers During UM Audio Hourglass	=0 (c)
MSExchangeUMPerformance\Operations over Six Seconds	=0 (c)

References

http://technet.microsoft.com/en-us/library/dd335215.aspx
http://technet.microsoft.com/en-us/library/ff367923.aspx
http://technet.microsoft.com/en-us/library/ee423542.aspx
http://technet.microsoft.com/en-us/library/bb124699.aspx#SA
http://technet.microsoft.com/en-us/library/bb331967.aspx

How to monitor Internet Information Services (IIS)

Listed below are some of the recommendations for monitoring the Internet Information Services (IIS) counters and services.

Watch the training video How to monitor Internet Information Services (IIS).

IIS Services to Monitor

Services	Service Name
Application Host Helper Service	AppHostSvc
Windows Process Activation Service*	WAS
World Wide Web Publishing Service	W3SVC

Events to Monitor

The Windows Process Activation Service also has some Event IDs that should be monitored as well. The Event Source for the following Event IDs is the Microsoft-Windows-WAS log file. The Event Log Monitor is ideal for this task.

5144 - (Error): WAS is not able to enable application pool.

5002 - (Error): Application pool is being automatically disabled.

5059 - (Error): WAS encountered a failure when it started a worker process to save the application pool. The application pool has been disabled.

5117 - (Warning): A worker process serving application pool has requested a recycle because it reached its private bytes memory limit.

5077 - (Warning): A worker process serving application pool has requested a recycle because it reached its virtual memory limit.

5009 - (Warning): A process serving application pool terminated unexpectedly.

IIS Performance Counters to Watch

Object\Counter	Default Threshold
Memory\Pages/sec	0 - 20
Memory\Available Bytes	10% of physical memory
Memory\Committed Bytes	75% of physical memory
Memory\Pool	Nonpaged Bytes A steady value. (A slow rise might indicate a memory leak.)
Processor\% Processor Time	< 75%
Processor\System Processor Queue Length	< 2
LogicalDisk\% Disk Time	As low as possible
LogicalDisk\Avg. Disk Queue Length	< 2
LogicalDisk\Avg. Disk Bytes/Transfer	As high as possible
Web Service\Bytes Total/sec	As high as possible

Monitor IIS Application Pools

There are performance counters on the APP_POOL_WAS object that you can monitor using the Performance Monitor. One counter in particular, Current Application Pool State that has the following definition (pulled from Windows Perfmon description)

Current Status of the Application Pool from APP_POOL_WAS\Current Application Pool State

1 - Uninitialized

2 - Initialized

3 - Running

4 - Disabling

5 - Disabled

6 - Shutdown Pending

7 - Delete Pending

References

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/7898b860-462c-4846-a3a8-1179f287ad88.mspx?mfr=true
http://technet.microsoft.com/en-us/library/bb727100.aspx
http://letitknow.wordpress.com/2012/07/27/what-services-should-be-monitored-in-case-of-iis/

How to Monitor MySQL

MySQL can be monitored via SNMP with the free Mysql-snmp module by Brice Figureau. There are many counters available under:

```
.1.3.6.1.4.1.20267.200.1
iso.org.dod.internet.private.enterprises.(??).mySQL.myStatus
```

But did you notice that (??) node in the counter path? That's because of how the MySQL MIB file is defined. Depending on what application you use for SNMP monitoring (it should be PA Server Monitor!!) it may have problems getting from the enterprises node to the mySQL node. This might be considered a MYSQL-SERVER.mib error.

This can be easily fixed with a small change to the MYSQL-SERVER.mib file.

Change this line:

```
::= { enterprises 20267 200 }
```

to this:

```
::= { enterprises mySQLRoot(20267) 200 }
```

Now that unnamed node has a name (mySQLRoot) most SNMP applications will be able to parse and traverse the MIB without problems.

Make sure the changed MIB file is in:

C:\Program Files\PA Server Monitor\MIBs

and restart the monitoring service so the changed MIB file is reparsed.

How to Monitor RADIUS Servers

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides Authentication, Authorization, and Accounting. A server is used to implement the service side of the client-server protocol, and this HOWTO article will describe how the server can be monitored.

radauth for Windows

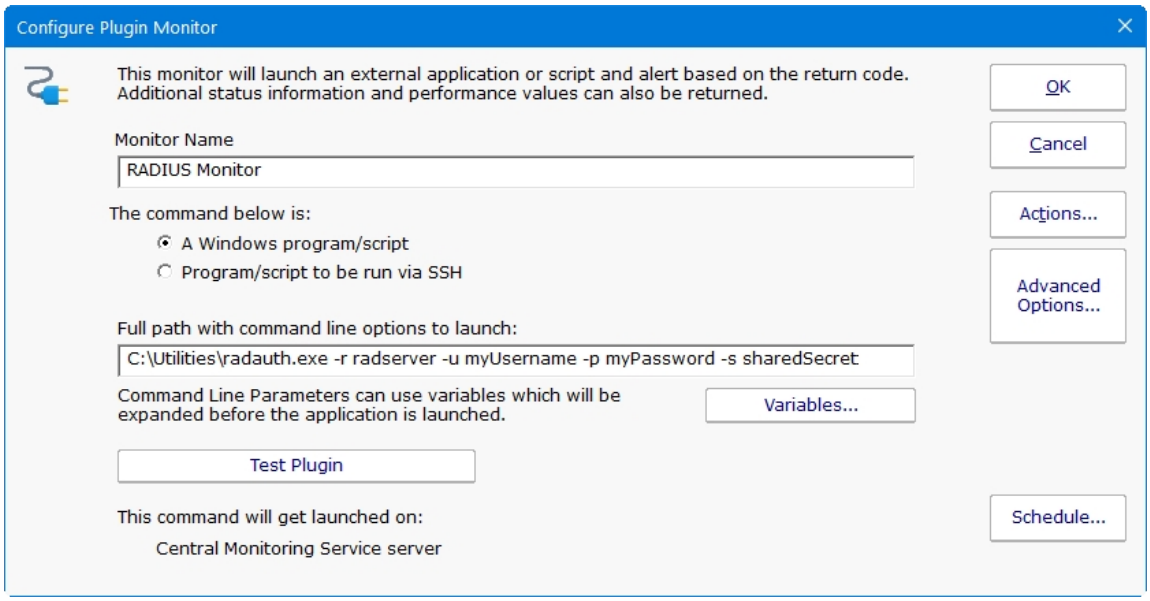
radauth is an open source command line application used for testing authentication against a RADIUS server. Typically available for unix/Linux operating systems, Power Admin has recompiled the utility for Windows systems. The binary executable as well as the source code and project files are available here.

Running radauth with the -h command line argument shows the options available.

radauth will show its success or failure in the console, but it's primary means of communicating success or failure to monitoring systems is via its exit code. An exit code of 0 indicates a successful authentication against the RADIUS server. An exit code of 0 for success means radauth is compatible with the Plugin Monitor.

Configuring RADIUS Server Monitoring

Add the RADIUS server for monitoring, and then add a Plugin Monitor to the device.



The example above will attempt a login of username *myUsername* against RADIUS server *radserver* with password *myPassword* and RADIUS shared secret *sharedSecret*. If radauth succeeds and returns 0, the monitor will be in an OK status, otherwise it will enter the Alert status.

How to Monitor Microsoft SQL Server

Listed below are some of the recommendations for monitoring a Microsoft SQL Server Database counters and services. These generally refer to SQL Server 2012, but most of the details also apply to other versions as well.

SQL Server Services

Microsoft SQL Server consists of three core services for the database engine. They are the SQL Server service itself (or MSSQLSERVER), the SQL Server Agent (SQLSERVERAGENT), and the SQL Server SQL Browser. Then there are many add-on or supplemental products, tools and reporting services that Microsoft offers that you can monitor but again they are optional.

The core services, the services that should be monitored is the MSSQLSERVER & SQLSERVERAGENT service. The SQL Server Agent (SQLSERVERAGENT) is the job scheduler for SQL Server and handles other maintenance tasks. All applications and communication with the relational database engine happens with the SQL Server Service (MSSQLSERVER).

Services to Monitor

Services	Service Name
SQL Server Service	MSSQLSERVER
SQL Server Agent	SQLSERVERAGENT

SQL Server Counters

Microsoft SQL Server provides many objects and counters that can be used to monitor the health and activity of an SQL Server instance running on a server. An object in an SQL Server instance can have one or many counters depending on the resources that are available and each can be monitored. Each of the following counters below are counters that are recommended to be monitored for the performance of your SQL server instances.

Performance Counters to Watch

Object\Counter	Default Threshold
System\Processor Queue Length	< 4 per CPU
SQL Server: Buffer Manager\Page Life Expectancy	> 300
SQLServer:General Statistics\User Connections	Watch counter over time to get a high and low count, then set your threshold to meet your requirements.
SQLServer:SQL Statistics\Batch Requests/sec	The higher the better. Watch counter to find a low threshold that meets requirements.
SQLServer:SQL Statistics\Compilations/sec	10% of Batch Requests
SQLServer:SQL Statistics\Recompilations/sec	10% of Compilations
SQLServer:Locks\Lock Waits/sec	0
SQLServer:Access Methods\Page Splits/sec	< 20 per 100 Batch Requests/Sec

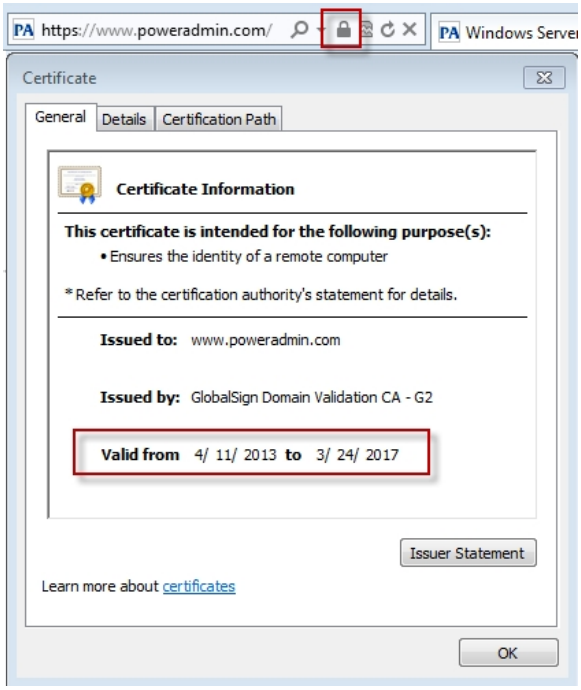
References

http://msdn.microsoft.com/en-us/library/ms190382.aspx
http://www.quest.com/techbrief/sql-server-perfmon-counters-poster811635.aspx

How to Monitor SSL Certificate Expiration

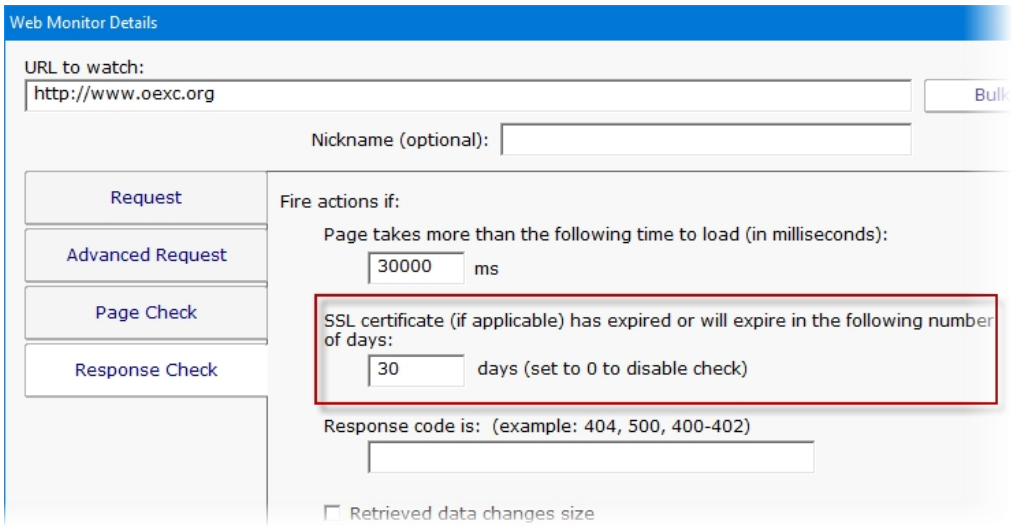
SSL Certificates used on a web server always have an expiration date. After that date, visitors to the site will see a warning about an expired certificate, which does not inspire confidence.

You can normally view the certificate for a site by clicking the lock icon in the browser. In this example, you can see the listed expiration date of certificate along with other information. You can manually check any certificate this way, and as long as you remember, that is enough. But humans forget -- so better to automate it!



Being notified of an expired certificate, or better yet, an SSL certificate that is about to expire is very simple: Use our Web Page Monitor. One of the default things it checks is the page's SSL certificate (if one exists). It can be set to warn you if it is expired or about to expire.

(See the SSL certificate setting about 3/4 of the way down the dialog). In this example, a warning will be sent once the certificate is going to expire within the next 30 days.

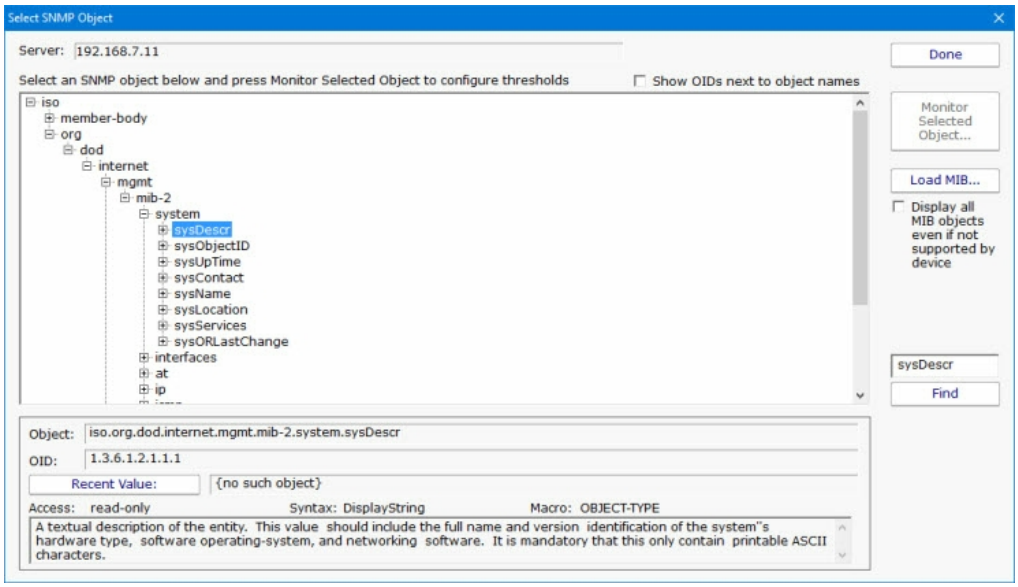

Web Monitor Details
URL to watch:
http://www.oexc.org
Bul
Nickname (optional):
Request
Advanced Request
Page Check
Response Check
Fire actions if:
Page takes more than the following time to load (in milliseconds):
30000
ms
SSL certificate (if applicable) has expired or will expire in the following number of days:
30
days (set to 0 to disable check)
Response code is: (example: 404, 500, 400-402)
Retrieved data changes size

How to Monitor via SNMP

Many devices such as routers, printers, servers, etc. support SNMP, which is a protocol for getting status information from a device. If you have a device that supports SNMP, PA Server Monitor can gather information from it and monitor it.

To monitor an SNMP-capable device, follow these steps:

1. Add the device to PA Server Monitor for monitoring.
2. While adding the device, indicate SNMP should be used to monitor it. If this wasn't done earlier, you can right-click the device and go to Type & Credentials -> Set Computer/Device Type.
3. When you mark it as an SNMP device, you can also specify the credentials to use when communicating with the device. By default, SNMP version 2c is used, with a community string of 'public'.
4. You will need to ensure your device will accept SNMP requests from the network. For example, most default Linux installations do not accept SNMP requests from the network, so the snmpd.conf file has to be edited on the Linux host.
5. Add a new monitor to the device, specifically an SNMP Monitor.
6. On the SNMP Monitor click the Add button. This will show an object tree of all values that can be monitored on the device.



7. *(Optional)* If you have a device-specific MIB file from the manufacturer, add it to the monitor with the Load MIB button. This will turn some of the numbers into human-readable values which makes finding your target value easier.
8. Now you can go to the value that you want to monitor, either by navigating or using the Find button, and press the Monitor Selected Object button.

At this point, you have an SNMP monitor that can monitor any counter value that is supported by your specific device. Setting up alerts is done the same as with other monitors.

How to Monitor Voice SIP

We offer a free utility named SIP-Ping which can be used from the command line to ping a SIP endpoint.

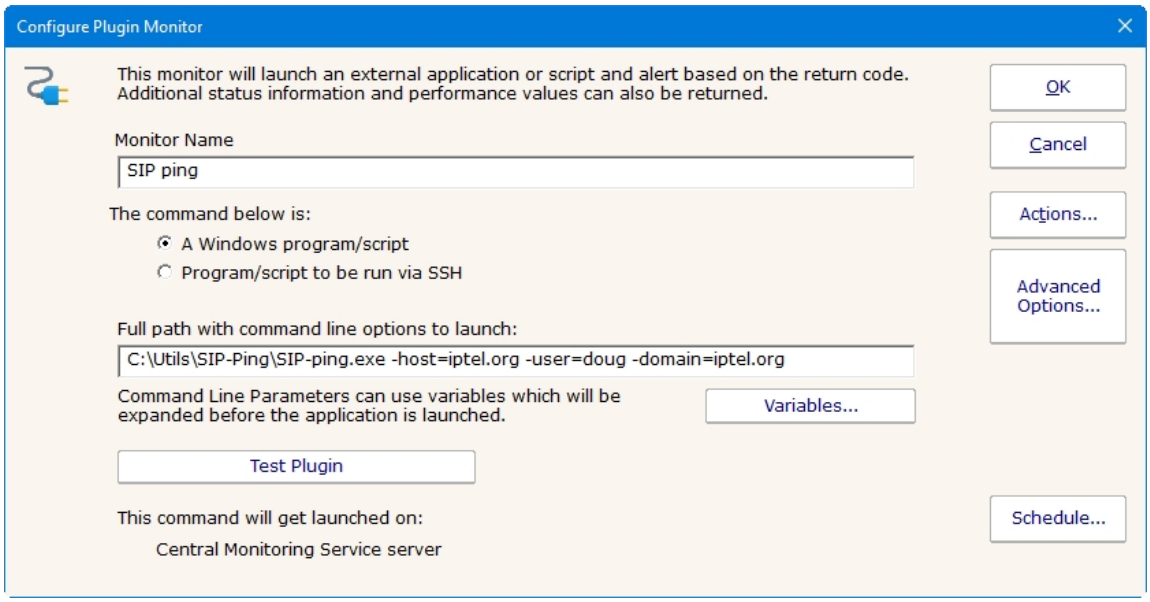
You can use a Plugin Monitor along with this utility to do a SIP protocol ping to your SIP server and endpoints.

Create the Plugin Monitor, and set the top value to "A Windows program/script".

The full path will be something like this:

```
"C:\YourPath\SIP-Ping.exe" -host=$DEVICE_NAME$ -user=test_user -domain=your_domain
```

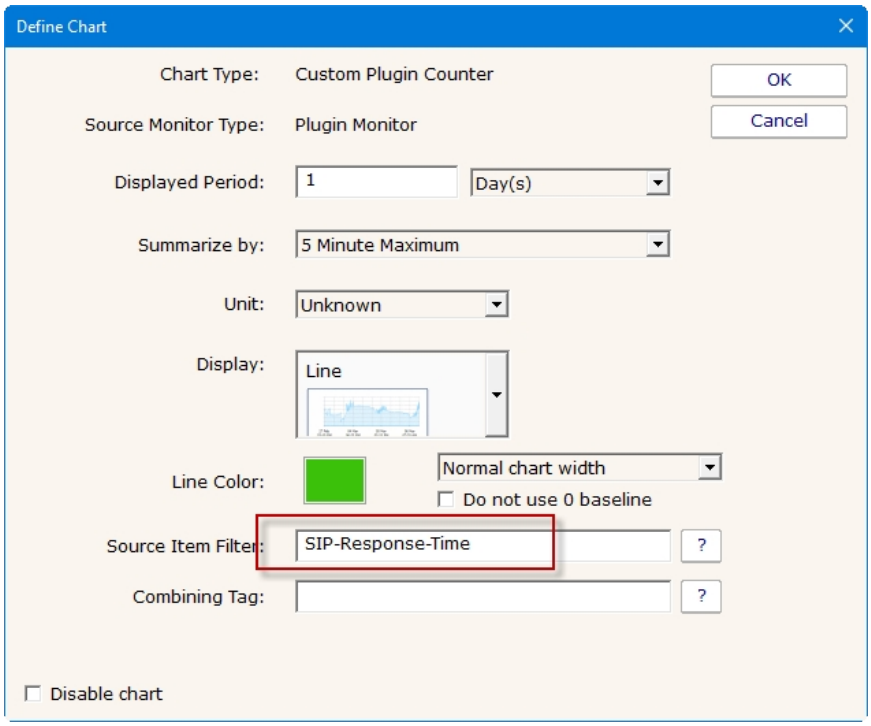
Note that $DEVICE_NAME$ will be replaced with the name of the device that the monitor is attached to.



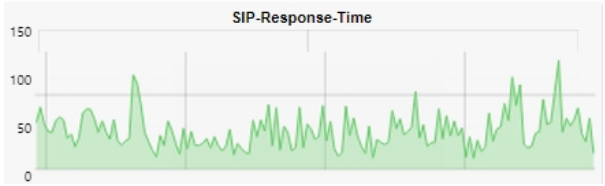
You should NOT use the -verbose option as that outputs in a format that is incompatible with the plugin reader.

You CAN use the other optional parameters to fit your needs (-UseTCP, -port, -strict, -threshold, etc).

With this monitor in place, you can add a custom chart for the SIP ping response time. When you go into the charts area, add a "Custom Plugin Counter" and use "SIP-Response-Time" for the Source Item Filter.



After the monitor has been running for a while, you'll start seeing a chart like the one below.



How to Monitor Windows Firewall

Windows Firewall can be monitored via a COM object or the netsh command. This example will use the Execute Script monitor to run a netsh command line and parse the results to ensure all firewall profiles are on.

Create an Execute Script monitor. Set the language to VBScript and paste the following into the code window.

```
Dim WshShell, oExec
Set WshShell = CreateObject("WScript.Shell")
Set oExec = WshShell.Exec("c:\windows\system32\netsh -r "
+ ComputerName + " advfirewall monitor show firewall")

strOut = ""

 Do While Not oExec.StdOut.AtEndOfStream
  strOut = strOut & oExec.StdOut.ReadLine()
  strOut = strOut & vbNewLine
 Loop

listLines = Split(strOut, vbNewline)

For Each line In listLines
 If InStr(line, "State ") > 0 Then
    If InStr(line, "ON") = 0 Then
       FireActions = true
     Details = Details & "A Firewall Profile is OFF - " & line & vbNewLine
      End If
  End If
Next
```

In the VBScript above, the netsh is run with commands to show the current status of the firewall on the remote server specified with the -r command. Note that the firewall rule **"Windows Firewall Remote Management"** has to be enabled for this to work.

Each line is parsed looking for a the text "State ". The space at the end is to prevent lines like "StatefulFTP" from being included. If "State " is seen, then the script checks for the word "ON".

This script *might* need to be customized for non-English systems.

This monitor could be used as a Monitor Template and applied to many servers at once for a quick check of your Windows servers.

How to Setup OAuth 2.0 with Office365

Starting in October 2022, Microsoft is expected to disable legacy (username/password) logins for Office365 and only allow "modern" authentication mechanisms, specifically OAuth 2.0.

Although POP and IMAP access will require OAuth, Microsoft is allowing SMTP to continue using 'legacy' authentication (username/password). The legacy option is easier to use and less of a security risk for SMTP than with POP and IMAP (since it is send-only).

OAuth 2.0 requires an application to be registered in an authentication directory, and for Office365 that is Azure Active Directory. This document will walk you through the required steps so you can use Office365 in your PA Server Monitor installation for sending email alerts.

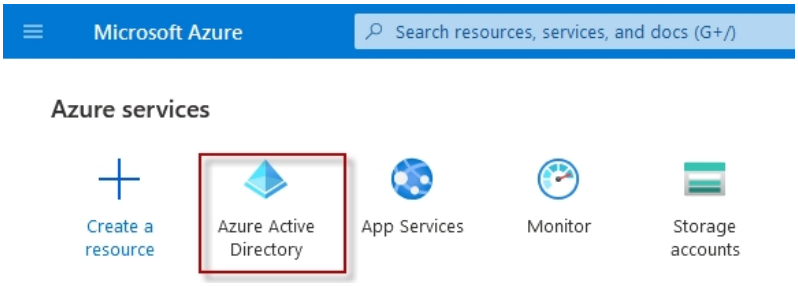
Note: The below steps are supported in PA Server Monitor version 8.5 or newer.

Register PA Server Monitor in Azure Active Directory

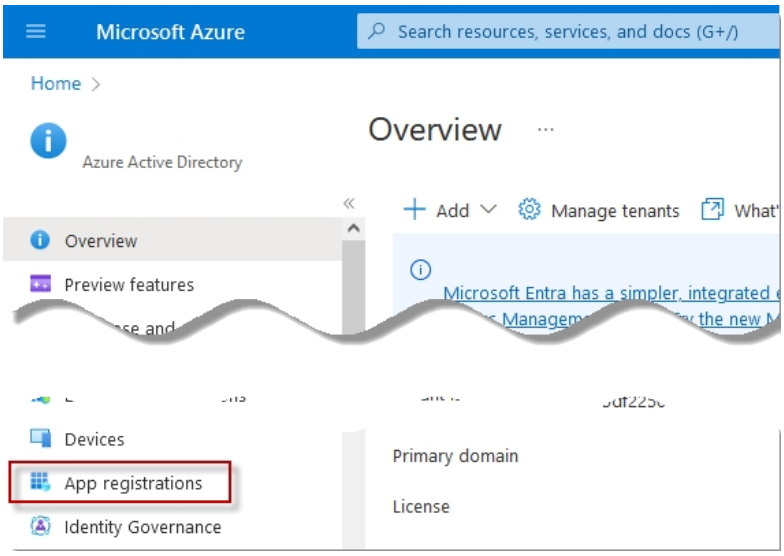
If you have multiple installations of PA Server Monitor, these steps (application registration) must be done for each installation. Installations can NOT share the IDs and secrets that will be granted through this process. If the IDs and secrets are shared among multiple applications or installations, they will log each other out every time the credentials are used (every time an email is sent).

However, you CAN have multiple applications all send through the same Office365 account/email address.

If you have an Office365 account, you also have an Azure Active Directory account. Login to Azure at https://portal.azure.com/. If you don't go directly to your Active Directory, you might need to select it at the top:



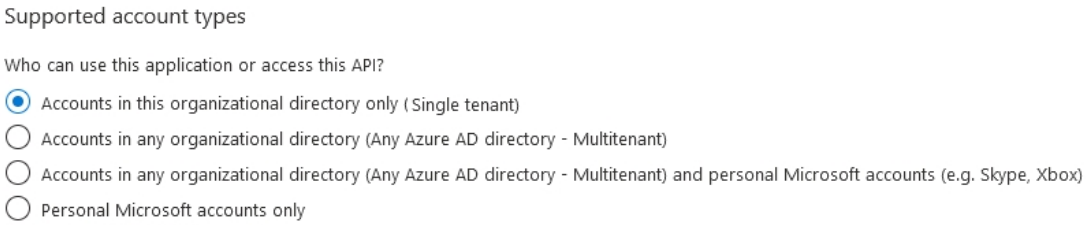
Once you are in Azure Active Directory, click on App Registrations found on the left side.



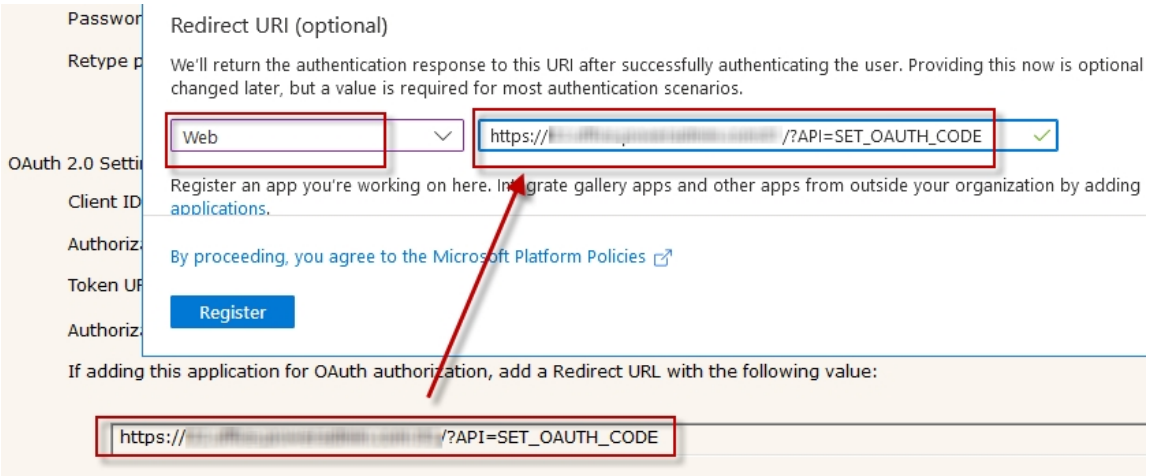
Click New Registrations near the top.

Give your application registration a name. We recommend including the application name and the server it is installed and what access is being granted. Something like "PA Server Monitor on SERVER01 for emailing via Office365".

The default Supported Account Type (single tenant) is the correct value for most situations.

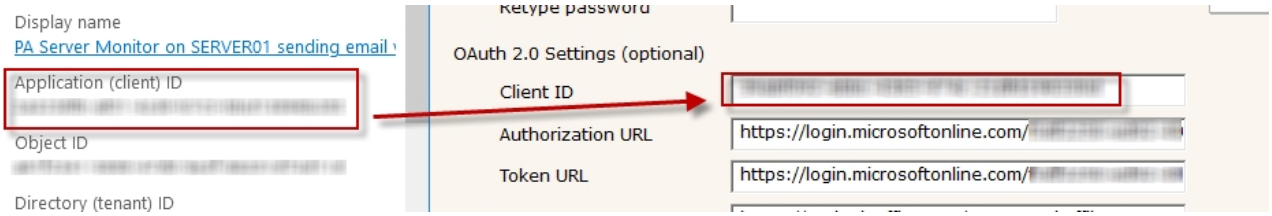


For the Redirect URI, choose Web, and specify the URL found at the bottom of your Email Action

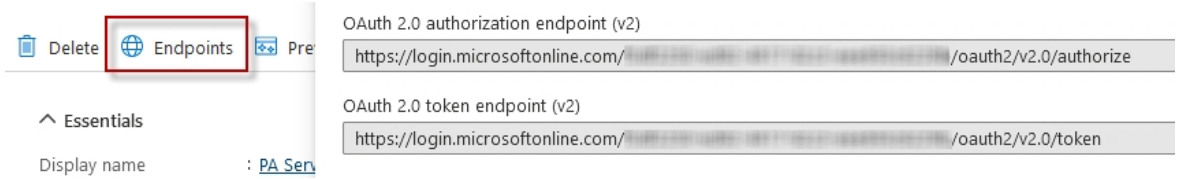


Application Values

Now copy the Azure Application (Client) ID to the Client ID field in the Email Action.



To get the Email Action's Authorization URL and Token URL values, click the Endpoints button in the Azure Application Registration, and copy the URLs on the right.



Application Scope

The Authorization Scope requests specific access to Office365 resources. Depending on what type of connection you're setting up, use one of these Scope strings. For the Email Action use the SMTP setting. Other scenarios, such as the Email Acknowledgement feature, might use POP3 or IMAP.

For SMTP:

```
https://outlook.office.com/SMTP.Send offline_access
```

For POP3:

```
https://outlook.office.com/POP.AccessAsUser.All offline_access
```

For IMAP:

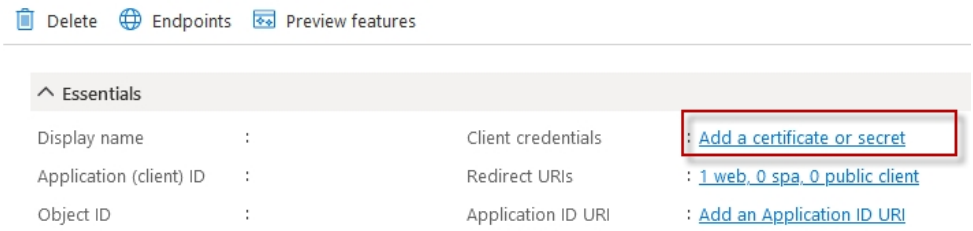
```
https://outlook.office.com/IMAP.AccessAsUser.All offline_access
```

Mail Server

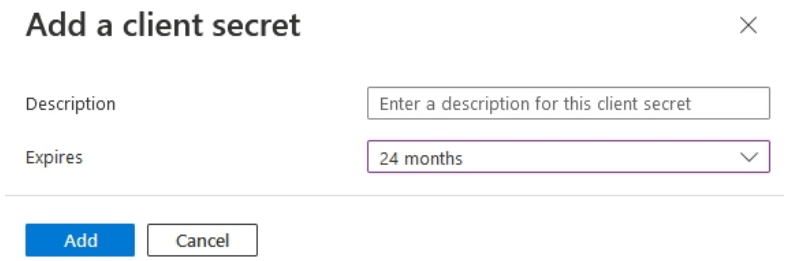
The Email Action's SMTP Server Name, Port, and Username for SMTP Server will be the same whether you use OAuth 2.0 or not, and will be available from your Office365 account. Typically these are values such as smtp.outlook.com, port 587, and Explicit SSL/TLS respectively.

Client Secret (instead of Password)

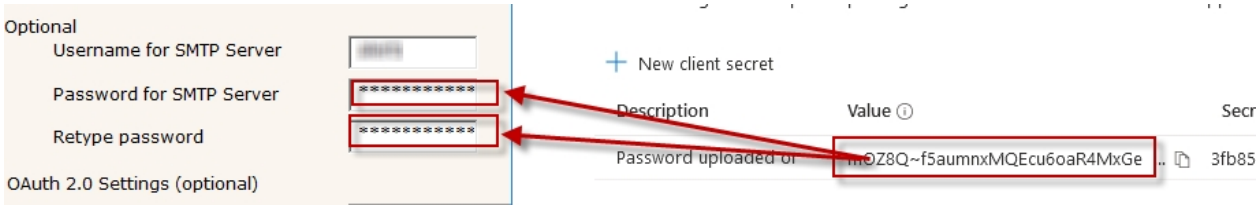
The Password field is NOT the email account password, but rather a Client Secret for this specific Application Registration. Click the Add a Certificate or Secret link.



Click the +New Client Secret button and give the secret a name. We recommend making the expiration as long as possible so you will not need to revisit this soon. Currently 24 months is the maximum allowed.

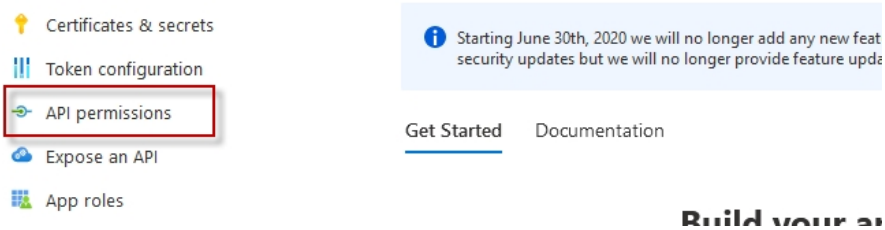


Once you press the Add button, the Client Secret's value is displayed. Copy the value immediately. Once you leave this page, the value will never be displayed again. This Client Secret is used in the Email Action's Password field.

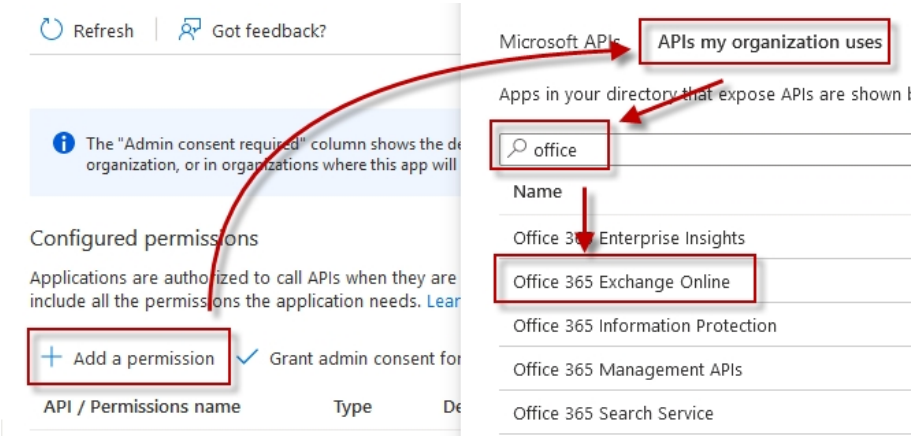


API Permissions (for POP3 or IMAP)

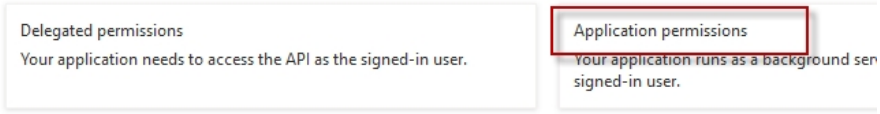
API permissions may need to be granted, for example if using IMAP or POP access for example. To do that, select the API permissions link on the left.



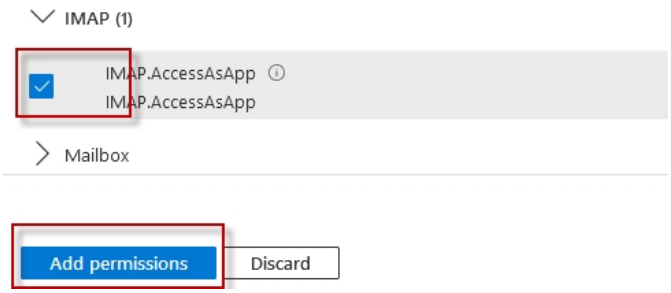
Click "Add a permission", and then on the left the "APIs my organization uses". Enter "office" in the search box and then select "Office 365 Exchange Online".



Select Applications Permissions on the left side.

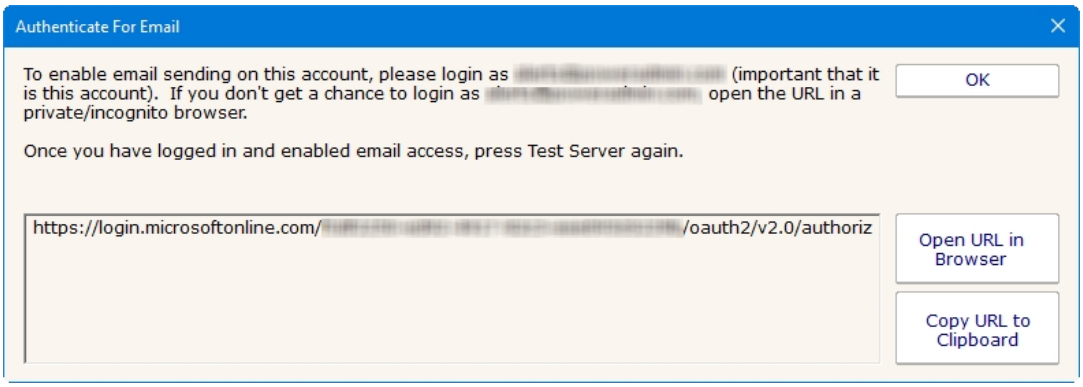


Scroll down and select "IMAP.AccessAsApp" and/or "POP.AccessAsApp" as required, and then click "Add Permissions" at the bottom.



Authenticating with OAuth 2.0

Now that all of the pieces are in place, you can click the Email Action's Test Server button (or the Test button in the other area in the application where you are working). This will probably display the dialog below. This dialog can also potentially be shown at other times if tokens expire and Office365 requires a new authentication (more on this below).



The shown authentication URL needs to be visited and logged into in a brower. You can either copy the URL and open a browser yourself, or press the Open Browser button. Be sure to login with the requested account (the account that will send emails).

CAVEAT: Office365/Azure uses cookies to keep track of logged in sessions. If you go to this URL and it immediately forwards you to the OAuth Authentication Complete page, you will have authenticated using whatever account the cookies are tied to, and not necessarily the account that the Email Action will use. If this happens, copy the URL to a private/incognito browser and login there. This will ensure you authenticate the proper account.

Once you have authenticated, press the Test Server button again to do a final and complete email send test.

Periodic Reauthentication

Office365 (Azure) now controls how long the authentication is valid. Every time an email is sent the authentication is checked and refreshed. According to Microsoft documentation, if the internal authentication tokens aren't used for 90 days (i.e. no emails are sent for 90 days) the authentication will timeout. If the Office365 user account's password is changed this can also cancel the current authentication. In addition, we saw above that the Client Secret is only valid for up to 24 months.

If/when the authentication becomes invalid, that is considered a System Error and the new required authentication URL will be shown at the top of reports, and sent out via other notification Actions. This would be a good reason to have a Backup SMTP server configured. Until the newest authentication URL is used to login, email will fail to send.

How to Prepare Satellite Installations for Imaging

Satellite Monitoring Services have a unique ID that helps the Central Monitoring Service know which Satellite is communicating, which one should receive which monitors, etc.

When a Satellite server is imaged and that image is then duplicated to multiple servers, the multiple Satellites will have the same ID (no longer unique) which will cause problems.

To get around this, set the following registry values on the Satellite server before imaging it:

```
HKEY_LOCAL_MACHINE\software\PAServerMonitor
Agent_ID = "$MacAddress$"
Agent_Name = "$Machine$"
```

When the Satellite is run, it will use the computer's network card MAC Address, and/or the computer's fully qualified domain name for the given parameter. Note that you can combine these values and add additional values. That means the above values can be any combination of:

$MacAddress$

$Machine$

Any letters from A-Z and any digits from 0-9

Any number of dash - characters

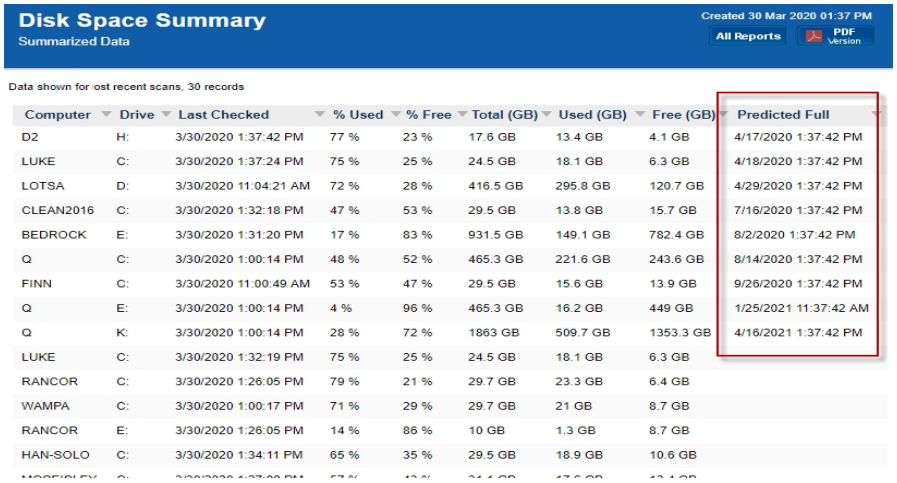
These are all valid examples:

```
Agent_ID = "$MacAddress$"
Agent_ID = "$Machine$"
Agent_ID = "$MacAddress$-$Machine$"
Agent_ID = "CONTROL-428-A-$MacAddress$"
```

How to Predict Full Server Disks

With PA Server Monitor, you can run reports and see mathematical predictions of when server disk drives will run out of room. Follow the steps below.

Watch the training video Using Disk Space Trends to Predict Low Disk Space.



Disk Space Summary
Summarized Data

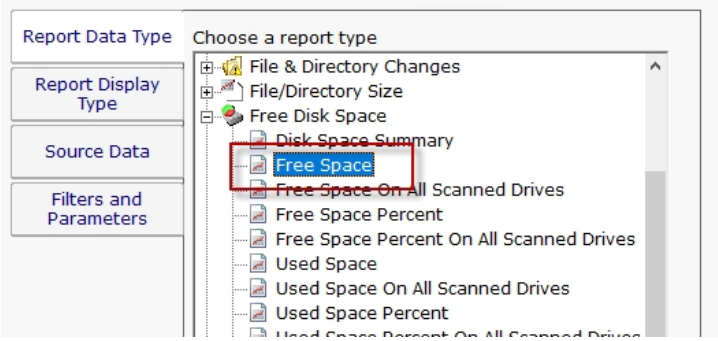
Created 30 Mar 2020 01:37 PM
All Reports | PDF Version

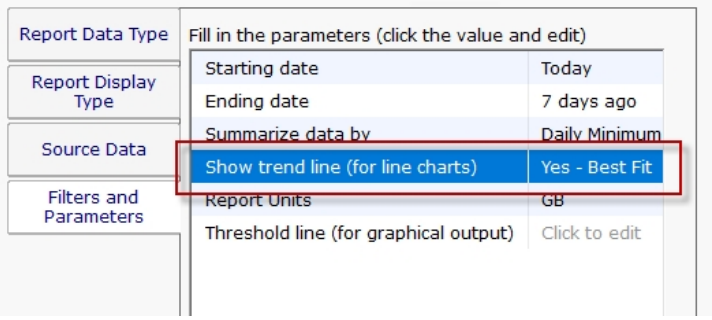
Data shown for ost recent scans, 30 records

Computer	Drive	Last Checked	% Used	% Free	Total (GB)	Used (GB)	Free (GB)	Predicted Full
D2	H:	3/30/2020 1:37:42 PM	77 %	23 %	17.6 GB	13.4 GB	4.1 GB	4/17/2020 1:37:42 PM
LUKE	C:	3/30/2020 1:37:24 PM	75 %	25 %	24.5 GB	18.1 GB	6.3 GB	4/18/2020 1:37:42 PM
LOTSA	D:	3/30/2020 11:04:21 AM	72 %	28 %	416.5 GB	295.8 GB	120.7 GB	4/29/2020 1:37:42 PM
CLEAN2016	C:	3/30/2020 1:32:18 PM	47 %	53 %	29.5 GB	13.8 GB	15.7 GB	7/16/2020 1:37:42 PM
BEDROCK	E:	3/30/2020 1:31:20 PM	17 %	83 %	931.5 GB	149.1 GB	782.4 GB	8/2/2020 1:37:42 PM
Q	C:	3/30/2020 1:00:14 PM	48 %	52 %	465.3 GB	221.6 GB	243.6 GB	8/14/2020 1:37:42 PM
FINN	C:	3/30/2020 11:00:49 AM	53 %	47 %	29.5 GB	15.6 GB	13.9 GB	9/26/2020 1:37:42 PM
Q	E:	3/30/2020 1:00:14 PM	4 %	96 %	465.3 GB	16.2 GB	449 GB	1/25/2021 11:37:42 AM
Q	K:	3/30/2020 1:00:14 PM	28 %	72 %	1863 GB	509.7 GB	1353.3 GB	4/16/2021 1:37:42 PM
LUKE	C:	3/30/2020 1:32:19 PM	75 %	25 %	24.5 GB	18.1 GB	6.3 GB	
RANCOR	C:	3/30/2020 1:26:05 PM	79 %	21 %	29.7 GB	23.3 GB	6.4 GB	
WAMPA	C:	3/30/2020 1:00:17 PM	71 %	29 %	29.7 GB	21 GB	8.7 GB	
RANCOR	E:	3/30/2020 1:26:05 PM	14 %	86 %	10 GB	1.3 GB	8.7 GB	
HAN-SOLO	C:	3/30/2020 1:34:11 PM	65 %	35 %	29.5 GB	18.9 GB	10.6 GB	

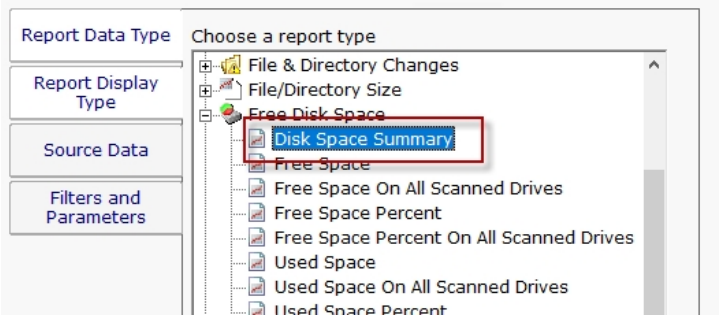
Click to enlarge

1. Install PA Server Monitor and add the computers that you want to monitor.
2. Add a Disk Space monitor to each computer (if there isn't one already) and have it monitor the disk space on the server's drives
3. By default, the Disk Space monitor will check and record the free and used disk space once every 6 hours. This is configurable.
4. After a few days, there will be enough data to start creating trend lines in the Free Disk Space report.





5. **To get a Predicted Full Date**, run the Free Disk Space -> Disk Space Summary report.
   - You can easily select all the drives on all the servers that you are monitoring, or any subset.
   - On the Filters and Parameters tab, make sure the 'Predicted Full' column is selected in the 'Columns to Show' parameter.
   - When the report finishes, click the Predicted Full column header to sort by that column.



Note that if a drive's disk usage isn't trending up, it won't have a Predicted Full date. This is normal and expected.

How to Shrink Database Files

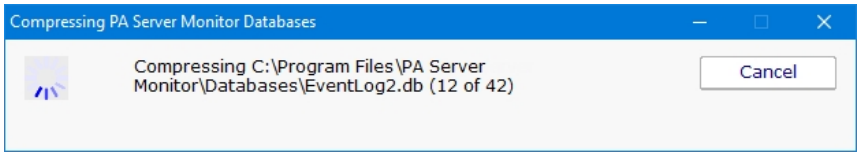
PA Server Monitor can use MS SQL Server or an embedded SQLite database to store it's data. This can be changed in Database Settings. You can control how much data is kept by adjusting the Database Cleanup Settings in the Database Settings dialog.

If you find the embedded SQLite database is using too much space (the files are stored in C:\Program Files\PA Server Monitor\Databases) you can do the following to shrink the database files:

1. Change the Database Cleanup Settings so that data is kept for a shorter amount of time.
2. Because the databases get cleaned up about once per day, wait a day for the databases to get cleaned up.
3. After the database files have been cleaned up, they will not be smaller, but there will be empty space in the database files. To reclaim the empty space, stop the PA Server Monitor service and run:

   C:\Program Files\PA Server Monitor\ServerMonSvc.exe /COMPRESS_DATABASES

   Extra disk space is needed for this operation as a copy of each database is made during the cleanup step. You will see the following dialog:



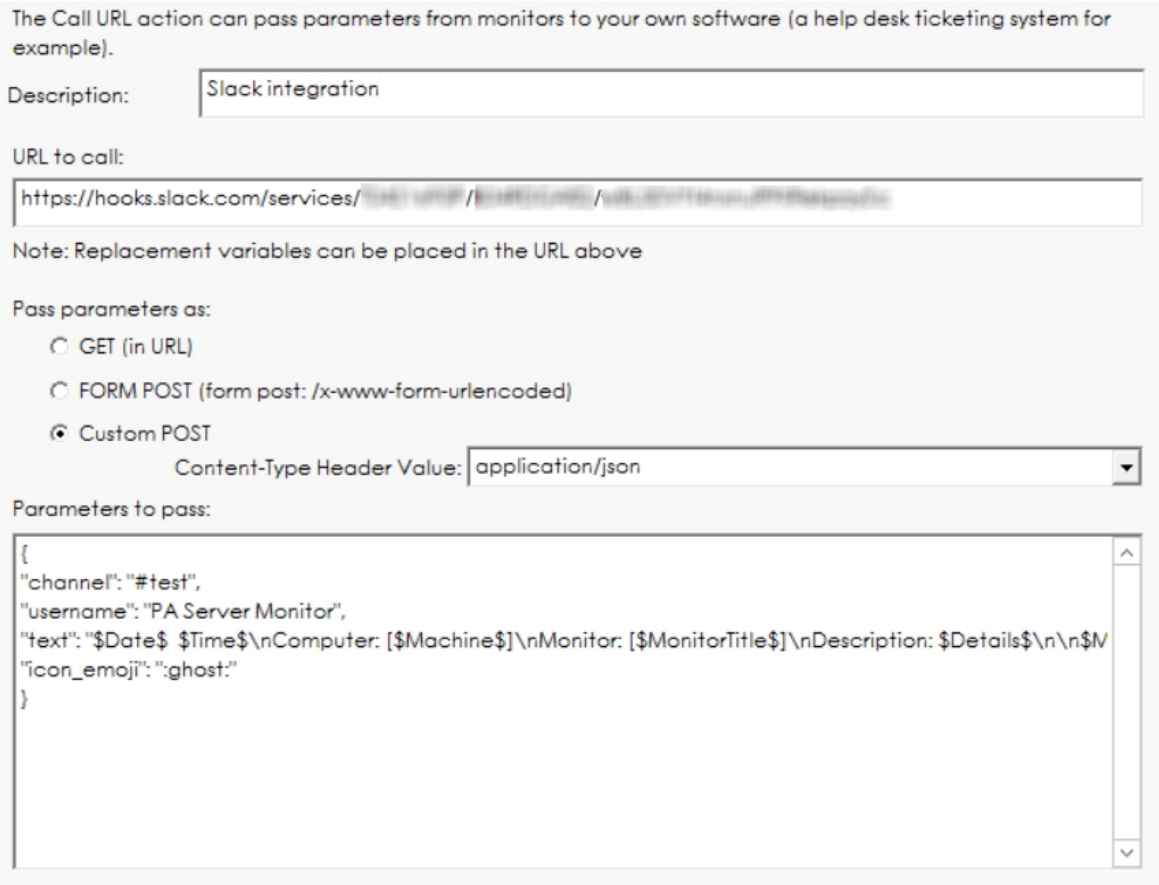
When the compressing step is finished, you should start the PA Server Monitor service.

How to Integrate with Slack

Integrating with Slack is very easy with PA Server Monitor. The Call URL action can be used to post alerts to a Slack channel.

Before creating the Call URL action, you need to get an "**Incoming WebHook**" integration URL from within your slack account. This will be the URL that is called from the Call URL action.

Once you have the **Incoming WebHook** URL from Slack, create the Call URL action and set it up like the image below, where the "URL to call" field is your **Incoming WebHook**.



The Custom POST option needs to be selected, with application/json as the encoding.

The format of the Parameters section is controlled by Slack. They have additional fields that can be used. We have shown some typical fields in the example above.

You can copy/paste from here:

```
{
"channel":"#test",
"username":"PA Server Monitor",
"text":"$Date$ $Time$\nComputer: [$Machine$]\nMonitor: [$MonitorTitle$]\nDescription: $Details['"',' ']
[80]$\n\n$MonitorMsg$\n$TimeInError$\n\n$SentFrom$",
"icon_emoji":":ghost:"
}
```

In the fields, you can use the standard replacement variables that are enclosed in $ such as $Details$ which will contain the body of the alert. Press the Variables button to see a full list of replacement variables. Note that in this example, any quote marks in the $Details$ variable are being turned into spaces, and the variable is being truncated to 80 characters.

One advanced user came up with this clever way of attaching a different icon based on the Status variable (thanks Jonathan!)

```
{
"channel":"#test",
"username":"PA Server Monitor",
"text":"$Date$ $Time$\nComputer: [$Machine$]\nMonitor: [$MonitorTitle$]\nDescription: $Details['"',' ']
[80]$\n\n$MonitorMsg$\n$TimeInError$\n\n$SentFrom$",
"icon_emoji":":$Status["msOK","white_check_mark"]["msALERT_RED","no_entry"]["msALERT","warning"]$:"
}
```

How to Create a Consolidated Uptime Report

Many monitors have Uptime reports which show graphically any down time reported by that monitor (for the Ping and Service monitors for example). You can also create a summary uptime report like the one shown below.

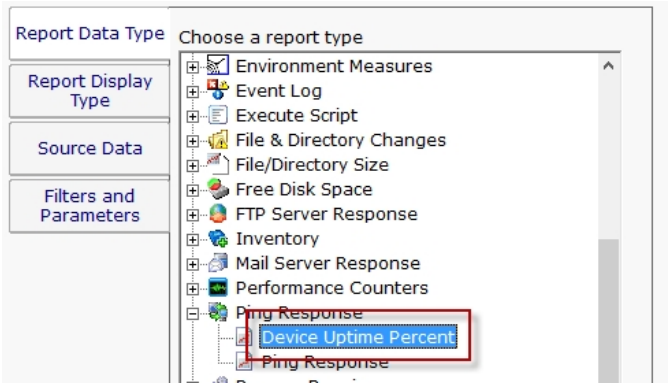
Complete Range Avg Ping %
Summarized Data
Created 30 Mar 2020 01:47 PM
All Reports | PDF Version

Data shown for 01 Mar 2020 12:00 AM to 30 Mar 2020 11:59 PM, 6 records

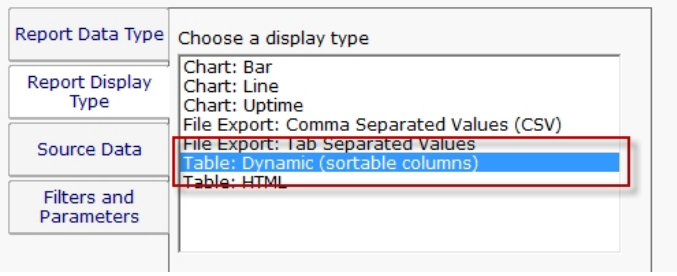
Source	Date	Up Percent
BANTHA	2/29/2020 8:00:00 PM	99.9 %
BB-8	3/4/2020 12:56:00 PM	99.3 %
D2	2/29/2020 8:00:00 PM	99.99 %
HAN-SOLO	3/25/2020 11:34:00 AM	99.9 %
LOTSA	2/29/2020 8:00:00 PM	99.99 %
LUKE	3/27/2020 3:59:00 PM	100 %

The basic solution is to create an Uptime report, with a tabular output, for multiple data sets. The secret is to summarize the data using the "Complete Range" summarization rule -- that is what gives you one line per monitor. Details shown below.

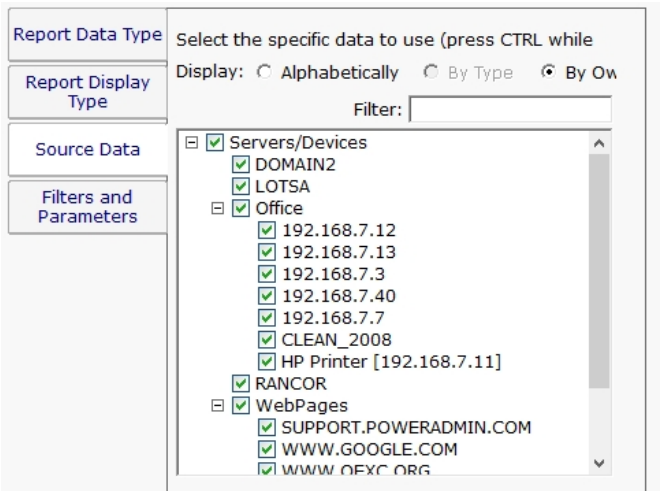
First, select the Uptime report for the data that you want to report on. In this case, we'll choose the Ping Uptime report.



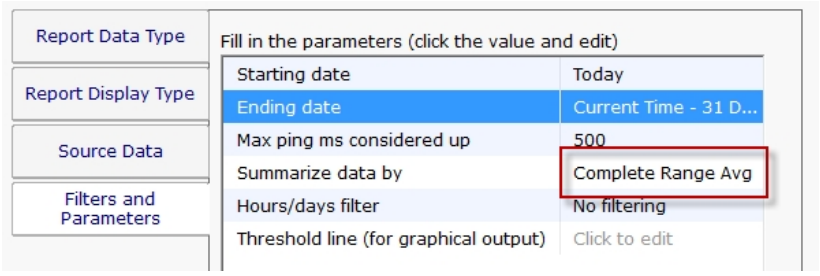
Next, choose a display type. The Tabular Report, HTML Table Report or CSV Export types will work fine.



Choose the server/devices that you want to report on. You can select the top group node to select all servers/devices. NOTE: Each selected server/device has to be queried separately in the database, so a large selection can make the report take a while. Once you get the report how you like it, create a Scheduled Report so the report is run and ready before you need it.



The report parameters are the key step here. Choose the time period for the report, and then chose **Complete Range** for the summarization period. This will average all the data between the two dates and come up with an overall Uptime percent.



Custom SSL Certificate

IMPORTANT:

To try and make the filenames below a little easier to work with, they were changed in version 8.5. If you are using version 8.4 or older, click the Show Older Names button below to show the filenames that apply to your software version.

Show Newer Names Show Older Names

Documentation currently showing: Showing v8.5 and newer filenames

File Type	New Name	Old Name
Private Key	SSL_PRIVATE_KEY.pem	CLIENT_PRIVATE.pem
SSL Certificate	SSL_CERT.pem	SIGNED_CLIENT_CERT.pem

Starting with version 9.4, you can optionally rename the two files above to something else to fit your process better. Set the new file names in the registry at:
HKEY_LOCAL_MACHINE\software\PAServerMonitor
values SSL_CERT_NAME and SSL_PRIVATE_KEY_NAME

Those registry entries will need to be created, and they should only be set to the new filename, not the full path. For example:
SSL_CERT_NAME = myCert.pem
SSL_PRIVATE_KEY_NAME = myCert.key

To revert back to the old filenames, just delete those two registry entries. Any time these registry entries are changed, the monitoring service needs to be restarted.

PA Server Monitor can use your own SSL certificate instead of the default self-signed certificate.

If at any time there are any problems with certificates, you can run the C:\Program Files\PA Server Monitor\CA\000_RESET_CERTIFICATES.cmd file (run as an administrator), and then restart the service. New certificates will be created. If things are really messed up, you can delete the C:\Program Files\PA Server Monitor\CA folder completely and restart the service to create a new CA folder.

Note that although the commands are shown on multiple lines, this is simply because there isn't space to show the full command one on line. But the text in the command boxes below should be run as a single command.

Use your own existing certificate

1. You will need to get your certificate into PEM format if it isn't already. There are a number of utilities that can do this that you can find on the Internet. Try searching for something like 'convert {your cert type} to PEM'. Note that .pem, .crt, .cer, and .key are often used interchangably. If you look at the file with a text editor and see readable text, you have a .pem file.

For example, to convert a .PFX file using OpenSSL (which is in the C:\Program Files\PA Server Monitor folder) run the following:

Tell OpenSSL where to find its configuration file (do NOT use quotes, even if there are spaces in the path):

```
set OPENSSL_CONF=C:\Program Files\PA Server Monitor\CA\openssl.cnf
```

The conversion command:

```
"C:\Program Files\PA Server Monitor\openssl.exe" pkcs12 -in "C:\My Files\myCert.pfx" -passin
pass:current-pfx-password -out "C:\My Files\myNewCert.pem" -passout pass:new-pem-password
```

current-pfx-password above is the current private key password for the .pfx file, and *new-pem-password* is the private key password for the output pem file.

Look at the resulting .pem file in a text editor -- you'll see there are two sections. Split this into two separate files, like below:

SSL_PRIVATE_KEY.pem file contents:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkfhkiG9w0BBQgwMzAbBgkqh1iG9w0BBQwwDgQIvSKYYbDSkPICAggA
... many more lines like those above ...
4pvqu3DGh93oIV7YlC1Gn4BY/2jVd2F1NxRjIxvDsllhDvvFFMUWC41Xc5pZ6d9U
pyY=
-----END ENCRYPTED PRIVATE KEY-----
```

SSL_CERT.pem file contents:

```
-----BEGIN CERTIFICATE-----
MIIFPzCCBCFgAwIBAgIS3SGXUxVkgYN9r5PZvhFNF148MA0GCSqGSIb3DQ5BBQUA
... many more lines like those above ...
ITywFF+LW4hdG5TYw2smJmbBgkfbW7nusufXAzg7I0E5z2HyxRmLm+Eees4J00mo
f6jn
-----END CERTIFICATE-----
```

You don't need the other lines that are in the file.

IMPORTANT: if your .pem file does not have a PRIVATE KEY section, then you must already have the private key in another file somewhere else - you must find that file and get it into pem format. The private key is created when the CSR (Certificate Signing Request) was initially sent to the certificate vendor (Verisign, GlobalSign, etc). It CANNOT be generated later - the private key and the certificate are a matched set.

If you want to include a full certificate chain in SSL_CERT.pem, make sure that:

- The certifcates are listed in the order of Application Certificate, Intermediate Certificate(s), Root Certificate (possibly the reverse of what is in the original .pem file)
- There needs to be a blank line between each --END CERTIFICATE-- and --BEGIN CERTIFICATE-- section

Thank you Martin for these tips :)

2. Save the certificate's private key file to
   C:\Program Files\PA Server Monitor\CA\SSL_PRIVATE_KEY.pem
3. Save the SSL certificate to
   C:\Program Files\PA Server Monitor\CA\SSL_CERT.pem
4. PA Server Monitor will need to know the password for the private key. You can specify this by running the following command:

```
"C:\Program Files\PA Server Monitor\diag.exe" /SETCONFIG=SSLCertPKPW:your-certificate-password
```

   The above command will encrypt and store the password with a machine-specific key in the registry.

   If you ever need to erase the password (such as if you delete the CA folder and go back to the self-signed certificate), run:

```
"C:\Program Files\PA Server Monitor\diag.exe" /SETCONFIG=SSLCertPKPW:
```

5. Restart the PA Server Monitor service and it will now be using your SSL certificate.

Create your own new certificate

1. Go to the C:\Program Files\PA Server Monitor\CA folder
2. Create a folder inside CA named **NewCert**.
3. Copy Client.cnf from CA into **NewCert**
4. Open **NewCert**\Client.cnf in a text editor. Go to the PACA_dn section near the bottom and edit the values as you like (C=Country, ST=State/Province, L=City).

   If you want to change the private key file's password, change the entries on the lines for input_password and output_password.

   Change the CN value to the hostname of your server. Some SSL certificate providers expect to see a dot in the name, so the public name of your server would best (something like monitor.mydomain.com).

   Note that depending on the SSL provider that you use, the subjectAltName field might be ignored which is where additional machine names are mentioned.
5. Open a command prompt and change directory to
   C:\Program Files\PA Server Monitor\CA**NewCert**
6. Run the following to tell OpenSSL where to find your configuration file (do NOT use quotes, even if there are spaces in the path):

```
set OPENSSL_CONF=C:\Program Files\PA Server Monitor\CA\NewCert\client.cnf
```

Then run the following to actually create the Certificate Signing Request file (also known as a CSR file). DO use quotes if there are spaces in the path: (note the below is all on one line)

```
"C:\Program Files\PA Server Monitor\openssl.exe" req -newkey rsa:2048 -keyout "C:\Program Files\PA Server Monitor\CA\NewCert\SSL_PRIVATE_KEY.pem" -keyform PEM -out "C:\Program Files\PA Server Monitor\CA\NewCert\SSL_CERT_CSR.csr" -outform PEM -rand "C:\Program Files\PA Server Monitor\openssl.exe"
```

7. This will create two new files:
   SSL_CERT_CSR.csr -- this is the Certificate Signing Request file that you will send/copy to the SSL certificate vendor (like Verisign, GlobalSign, etc)
   SSL_PRIVATE_KEY.pem -- this is the private key file for this certificate. This file will need to remain on the server, but should be kept private.
8. To see what you are sending to the SSL provider, run:

```
"C:\Program Files\PA Server Monitor\openssl.exe" req -in "C:\Program Files\PA Server Monitor\CA\NewCert\SSL_CERT_CSR.csr" -noout -text
```

9. After sending SSL_CERT_CSR.csr to a certificate provider, you will get back a certificate file. Save the file (in PEM format) to:
   C:\Program Files\PA Server Monitor\CA\SSL_CERT.pem

   If you want to include a full certificate chain in SSL_CERT.pem, make sure that:
   - The certifcates are listed in the order of Application Certificate, Intermediate Certificate(s), Root Certificate
   - There needs to be a blank line between each --END CERTIFICATE-- and --BEGIN CERTIFICATE-- section

   Thank you Martin for these tips :)

10. When the above file is copied, also copy
    C:\Program Files\PA Server Monitor\CA\NewCert\SSL_PRIVATE_KEY.pem
    into the CA folder.
11. PA Server Monitor will need to know the password for the private key. This password can be found in the client.cnf file on the line with input_password. You can give PA Server Monitor the password by running the following command:

```
"C:\Program Files\PA Server Monitor\diag.exe" /SETCONFIG=SSLCertPKPW:private-key-pass-phrase
```

    The above command will encrypt and store the password with a machine-specific key in the registry.
12. You can optionally delete the NewCert folder at this point.
13. Restart the PA Server Monitor service and it will now be using your SSL certificate.

How to Use Monitor 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. The monitor(s) set as the dependency need to all be in the OK state for the current monitor to run. This is useful for suppressing errors. As one customer stated "Trust me, it really helps prevent 'Death By Alerts'".

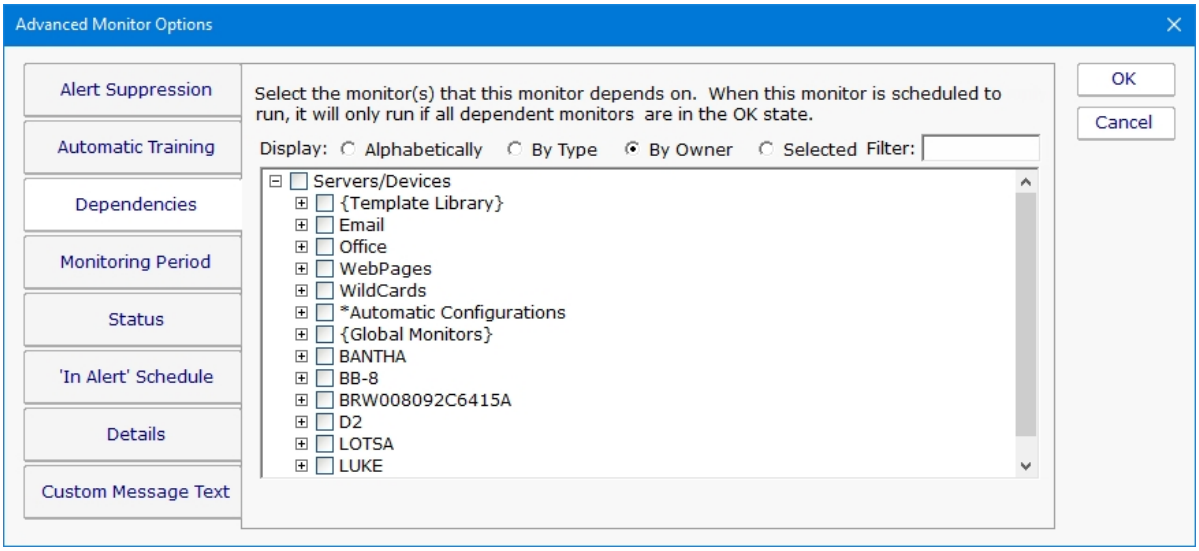
Setting Dependency on Monitors

To add a Dependency to a monitor simply open the Advanced Options menu for your monitor and then select the Dependencies tab. You can select any monitor on any server for the monitor to be dependent on. For example, you are editing the Disk Space monitor on Server1. Open the Advanced Options menu for the Disk Space monitor and locate the Ping monitor for Server1 and select it. Save your changes. When that Disk Space monitor runs it will check the Ping monitor first, if the status is OK then the Disk Space monitor will run, if not the Disk Space monitor will not run. The message Dependency Not meet will be given but no alerts will be fired.

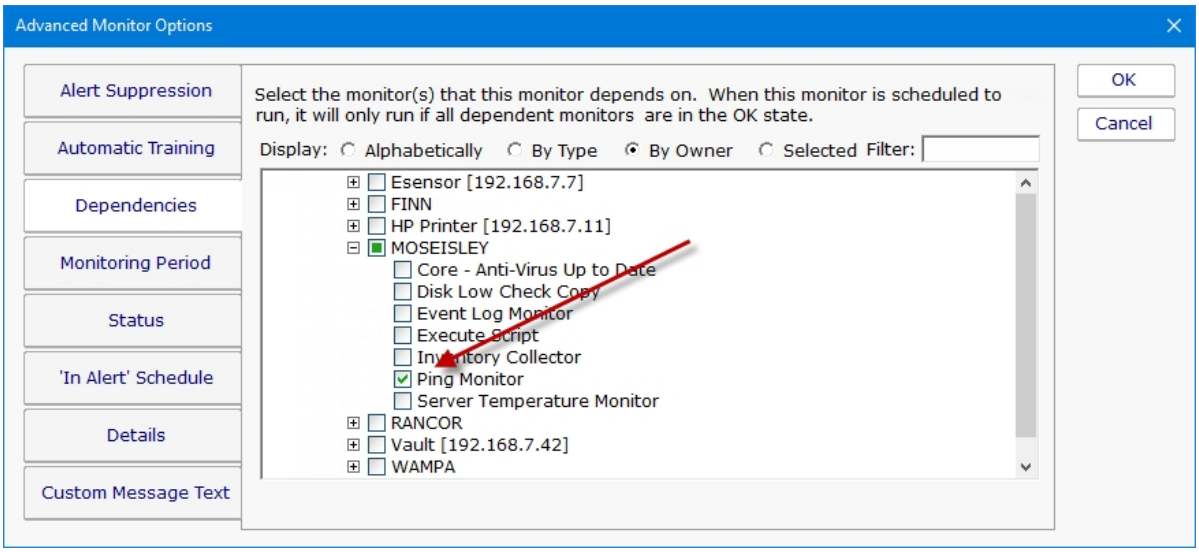
Another example: You want to set the dependency of a Performance monitor on Server2 on the Ping monitor for the Router called Rout1. Open the Advanced Options menu and find the Ping monitor for Rout1. Select it and save changes. When Server2's Performance monitor runs it will check Ping monitor for Rout1 first. If the status is OK it will run, if the status is anything else the Performance monitor will not run.

Setting Dependency for Standard Monitors

1. Select a monitor you want to add a Dependency to and click on the Advanced Options button



2. Then browse to find the monitor that you want this monitor to be dependent on. Check the box and click OK. When you are done editing the monitor make save the changes by clicking Apply.

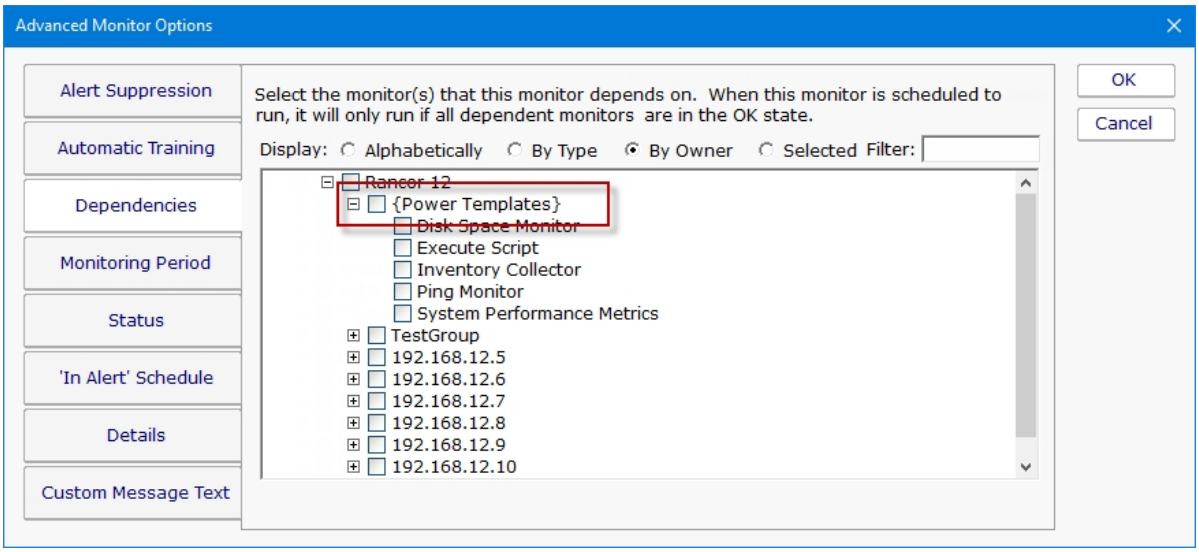


Setting Dependency for Power Templates

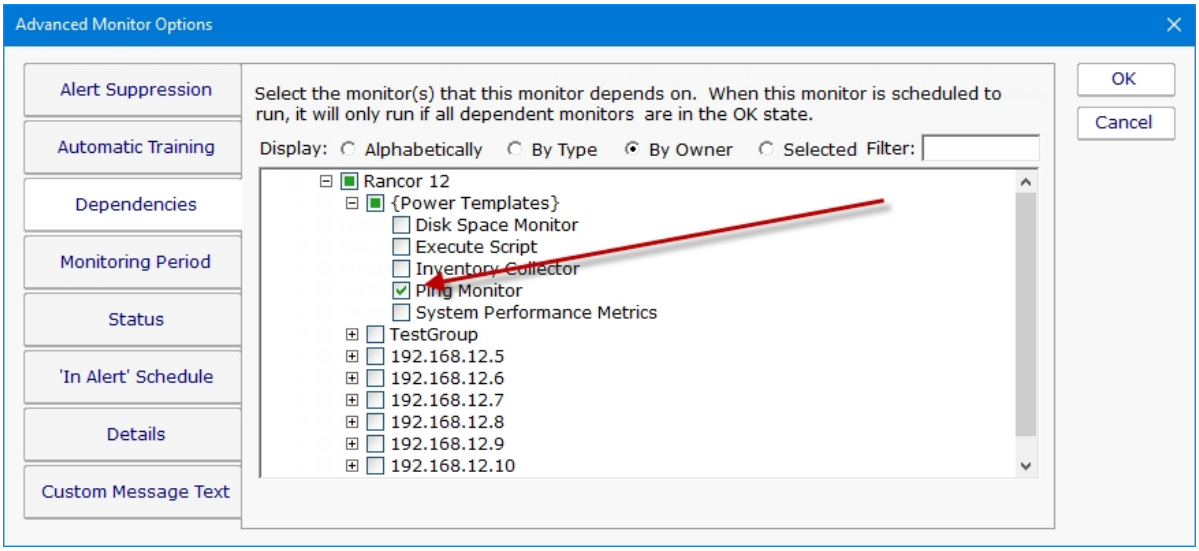
You can set dependencies on Power Templates but be careful about which monitor you set the dependency on. When you edit a template monitor to add a dependency, and you set the dependency to another template monitor, the changes will be propagated down to the servers/devices and adjusted to the monitors on each device. However, if you set the dependency to a standard monitor then propagation will use that target monitor as the dependency and not adjust it to fit the server.

For example: if you set a Disk Space Template Monitor to have the dependency set to the Ping Monitor on XYZ server, then all of the Disk Space Monitors that were added to the servers in that group will all be dependent on the Ping Monitor on XYZ server, not on the Ping monitor of the server where the edits took place

1. Select a Power Template that you want to add a Dependency to and click on the Advanced Options button and go to the Dependencies tab.
2. Locate the Power Template folder were the Power Template you are editing is located.



3. Then select the Monitor Template for the dependency for your monitor.



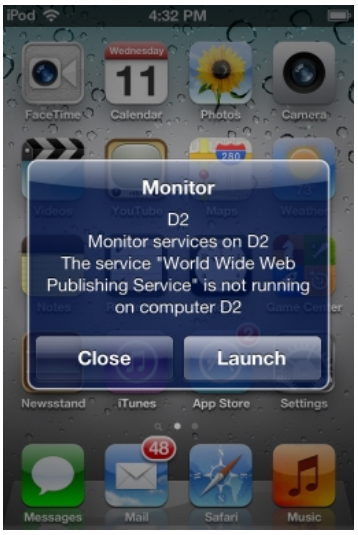
Note: Bulk Config will allow you make many dependency changes at the same time.

iPhone Notification

The iPhone Notification action is automatically added to your system when you first login with the iPhone app.

Once the action has been added, you'll be able to assign it to monitors just like you would add actions to any other monitor.

When a monitor fires the action, you will see a message box notification on your iPhone with details about the alert. The PA Server Monitor for iPhone application does not need to be running in order to receive these alerts.



You can configure and control the display of these notifications the same way you would with any other iPhone application. Go to Settings -> Notifications, and then scroll down to Monitor (the app's short name).

Alert Suppression, Event Escalation, Event Deduplication

Understanding how Alert Suppression, Event Escalation, and Event Deduplication work together can give you the tools to have fine grained control over your alerting environment.

Alert Suppression

When a monitor first detects a problem, it consults with its Alert Suppression rules to determine whether the monitor should go into Alert state or not. So this is the first filter in the alert path. If the alert is suppressed, the monitor is not in Alert state and no further alerting is considered.

Action List - Event Escalation

If a monitor is in Alert state at the end of it's check, it consults it's list of actions that might contain a list of Event Escalation alerts. This step is where the set of actions to run is determined. Event Escalation can be enabled and configured on a monitor-by-monitor basis.

Event Deduplication

There are two kinds of Event Deduplication -- Simple and Advanced. Below we'll discuss Advanced, as Simple doesn't have any affect on actions that are run.

After getting a list of possible actions to fire during the Event Escalation step, the alert is check to see if it is a 'new' alert. If it is new, the actions are fired as normal. But, if the event is not 'new', that means it's a duplicate. 'New' and 'duplicate' are determined by looking at fields in the event.

If an event is a duplicate:

By default, actions are not fired on duplicate events

You can indicate actions should continue to be fired, until the alert is acknowledged.

Enabling Automatic Configuration

Things to expect:

The most important point is many new monitors will get created for all of your servers/devices. If you have an existing installation, these will probably be duplicate monitors.
Because of the above, you might want to delete any standard monitors that you haven't made special customizations to. You can do that via Bulk Config > Monitors: Delete Monitors. Sorting "By Type" might make it easier to delete all of one type of monitor (all Ping monitors for example) at once.

Most of the new monitors don't have any actions assigned to them yet. You'll need to go to the Automatic Configuration group, and visit each contained group to add notification actions to the Power Templates in that group.

By default, all servers/devices inherit from the same (applicable) Power Templates. If you need different servers to send alerts to different groups, you'll need to have your own Dynamic Groups with templates that alert according to your needs, and rules that apply these templates to some servers but not others (Custom Properties is an easy way to do this).

Summary: If you have an existing installation that is working well, it's probably better to NOT enable Automatic Configuration

Learn more about Automatic Configuration

Disabling Automatic Configuration

Things to expect:

When Automatic Configuration is disabled, the Automatic Configuration group, with its child groups, will be deleted.
Because of the above, the Power Templates will get deleted, which means all monitors that inherit from those templates will be deleted.

You can always re-enable Automatic Configuration, but the new Power Templates that are created will not have the actions attached the way you have it now.

Summary: If your configuration was originally created by Auto Configuration, it might be best to leave it rather than lose your configuration and need to start over.

Making the Change

After reading the above, if you would like to make the change anyway, you will need to enter this keyword:

```
UNDERSTAND
```

Undo the Change

When Auto Configuration is enabled or disabled, a configuration backup is created at:

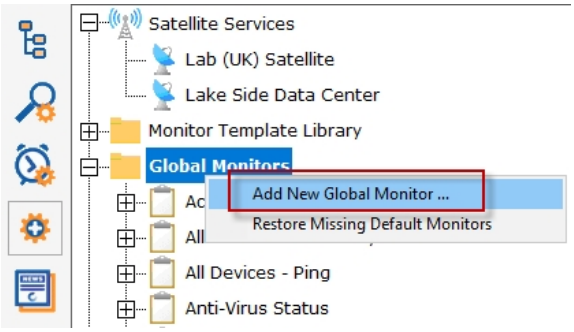
```
C:\Program Files\PA Server Monitor\Config\Backup
```

The backup is made before the Auto Configuration change is made.

If you need to restore this backup, you'll need to use the Console on the Central Monitoring Service, and go to the following menu: Configuration > Import Complete Configuration.

Global Monitors

Global Monitors are very similar to normal monitors with the exception that they are not attached to a server or group.

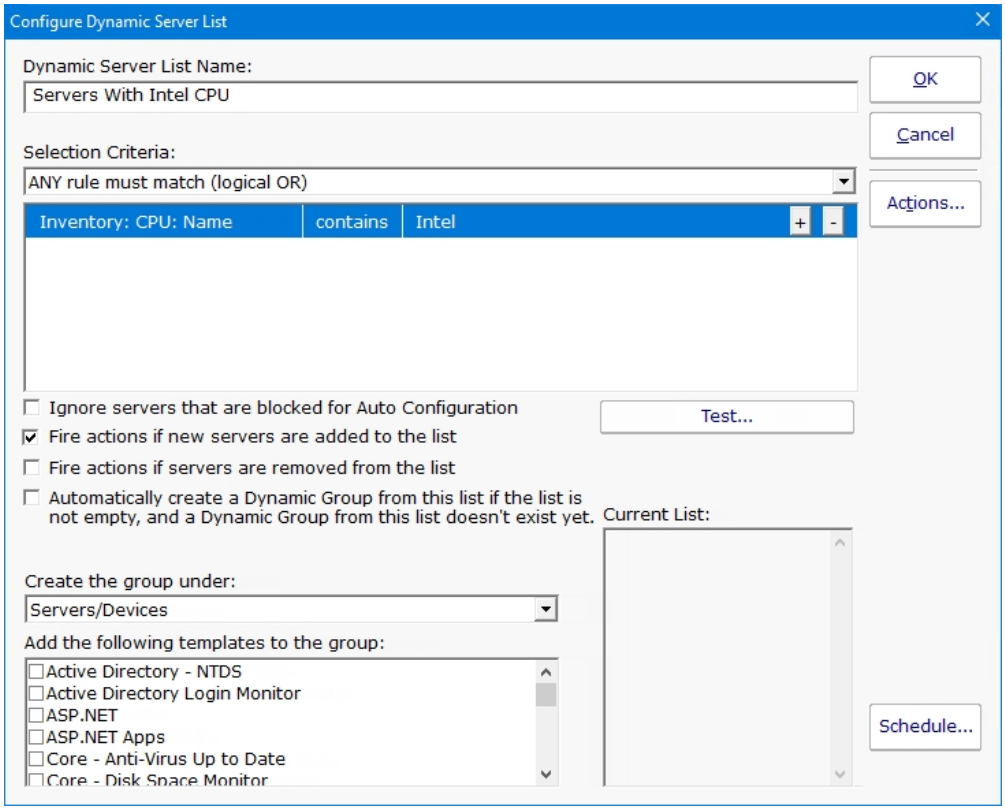


Global Monitors are found under the Advanced Services section of the Console application.

Like regular monitors, these monitors have the standard options for Adding Actions, setting Advanced Options and setting the Monitor Schedule.

Dynamic Server List

The Dynamic Server List monitor is a Global Monitor that runs outside of any server. It periodically checks servers to see which ones belong in a list determined by your criteria.



This monitor is very powerful and lets you select servers by:

Calculated status values (disk space, CPU usage, SNMP values, etc.)

Event Log entries

Group membership

Installed Windows services

Inventory values

Monitor types assigned

Monitored by Satellite

Name matching

Running processes

For example, you could define a list of:

Servers with average CPU usage over 10%

Servers with no anti-virus protection

Servers running IIS

You can receive alerts when servers enter and/or leave the list.

Rule Information

Each of the rules available gather information from different places and have specific behaviors, which will be documented below.

Blocked From Auto Configuration
: This is a setting that is applied to Servers/Devices when they are first created. It can be updated via the Bulk Config operation Computers: Set/Reset Block From Auto Configuration.

Contained in Group
: This rule will return all computer that are in the specified group, or within a sub-group of the specified group.

Contained Monitor Names
: This rule is a string search, that will check the names of monitors within a server/device, and if the name search matches, the server/device is added to the list.

Contains Monitor Type
: Checks the server for all monitors it contains and if any are of the specified monitor type, the server is added to the list.

Custom Property
: Custom Properties on the server/device are checked for a match. Note that Customer Properties are inherited from groups 'above' the server/device in the group hierarchy, so Custom Properties set directly on the server/device as well as inherited properties are checked.

Has Process
: Checks the database for a list of Processes on servers/devices that were monitored by a Process Monitor.

Has Windows Service
: Checks the database for any services that were monitored by a Service Monitor on the target server. Removing a Service Monitor from a server does not automatically remove the database entries for that server. This is a powerful way to make Dynamic Groups based on the software installed on a server.

Inventory
: This will check values collected and stored in the database by the Inventory Collection monitor. Things such as Anti-Virus product, IP Address, OS version, installed CPU and memory, etc can be queried. Note that not all inventory fields are found/collected for all devices.

Is Device Type
: This works on the property that can be set on servers/devices via Type & Credentials > Set Computer/Device Type in the Console. This can also be set by the Bulk Config operation Computers: Set Credentials (Windows, SNMP, ESX, IPMI).

Monitored By
: This allows you to create a list of devices that are monitored by the Central Monitoring Service, or by particular Satellites. This can be useful for creating lists of servers owned by a particular customer or in a specific geography if your other groups are arranged this way.

Monitoring Software is Installed
: This property is true for servers where the Central Monitoring Service or a Satellite Monitoring Service is installed and running.

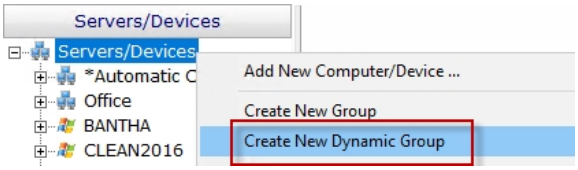
Registry
: This rule reads a particular registry value and compares it to the criteria you set. If the criteria match, the server is added to the list.

Server/Device Name
: The name (including any alias that is set) is compared to the given rule to determine servers/devices that match.

Statistic
: Statistics from most monitor types can be targeted with this rule. Once a specific statistic is chosen, values from that statistic are checked, and servers for which the statistic meets the checks are added to the list.

Dynamic Groups

Once you've defined a server list and how often it should update, you can use it further by defining a Dynamic Group.



The Dynamic Group is defined by choosing an existing Dynamic Server List. Any server/device that shows up in the Dynamic Server List will belong to the group.

Because the Dynamic Group is defined by the server list, servers/devices can not be manually added or removed from the group. Other than that, these groups behave similar to other groups. That means you can:

Define status reports for the group, showing specific information for your chosen servers

Use Dynamic Groups in Bulk Config as a selection criteria for servers to operate on (for example, a group with all Windows 2012 R2 servers)

Run Ad-Hoc or Scheduled Reports for the servers in the group

Grant access to servers in the group

Standard Configuration Options

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

Custom SSL Certificate

IMPORTANT:

To try and make the filenames below a little easier to work with, they were changed in version 8.5. If you are using version 8.4 or older, click the Show Older Names button below to show the filenames that apply to your software version.

Show Newer Names Show Older Names

Documentation currently showing: Showing v8.4 and older filenames

File Type	New Name	Old Name
Private Key	SSL_PRIVATE_KEY.pem	CLIENT_PRIVATE.pem
SSL Certificate	SSL_CERT.pem	SIGNED_CLIENT_CERT.pem

Starting with version 9.4, you can optionally rename the two files above to something else to fit your process better. Set the new file names in the registry at:
HKEY_LOCAL_MACHINE\software\PAServerMonitor
values SSL_CERT_NAME and SSL_PRIVATE_KEY_NAME

Those registry entries will need to be created, and they should only be set to the new filename, not the full path. For example:
SSL_CERT_NAME = myCert.pem
SSL_PRIVATE_KEY_NAME = myCert.key

To revert back to the old filenames, just delete those two registry entries. Any time these registry entries are changed, the monitoring service needs to be restarted.

PA Server Monitor can use your own SSL certificate instead of the default self-signed certificate.

If at any time there are any problems with certificates, you can run the C:\Program Files\PA Server Monitor\CA\000_RESET_CERTIFICATES.cmd file (run as an administrator), and then restart the service. New certificates will be created. If things are really messed up, you can delete the C:\Program Files\PA Server Monitor\CA folder completely and restart the service to create a new CA folder.

Note that although the commands are shown on multiple lines, this is simply because there isn't space to show the full command one on line. But the text in the command boxes below should be run as a single command.

Use your own existing certificate

1. You will need to get your certificate into PEM format if it isn't already. There are a number of utilities that can do this that you can find on the Internet. Try searching for something like 'convert {your cert type} to PEM'. Note that .pem, .crt, .cer, and .key are often used interchangably. If you look at the file with a text editor and see readable text, you have a .pem file.

For example, to convert a .PFX file using OpenSSL (which is in the C:\Program Files\PA Server Monitor folder) run the following:

Tell OpenSSL where to find its configuration file (do NOT use quotes, even if there are spaces in the path):

```
set OPENSSL_CONF=C:\Program Files\PA Server Monitor\CA\openssl.cnf
```

The conversion command:

```
"C:\Program Files\PA Server Monitor\openssl.exe" pkcs12 -in "C:\My Files\myCert.pfx" -passin
pass:current-pfx-password -out "C:\My Files\myNewCert.pem" -passout pass:new-pem-password
```

current-pfx-password above is the current private key password for the .pfx file, and *new-pem-password* is the private key password for the output pem file.

Look at the resulting .pem file in a text editor -- you'll see there are two sections. Split this into two separate files, like below:

CLIENT_PRIVATE.pem file contents:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkfhkiG9w0BBQgwMzAbBgkqh1iG9w0BBQwwDgQIvSKYYbDSkPICAggA
... many more lines like those above ...
4pvqu3DGh93oIV7YlC1Gn4BY/2jVd2F1NxRjIxvDsllhDvvFFMUWC41Xc5pZ6d9U
pyY=
-----END ENCRYPTED PRIVATE KEY-----
```

SIGNED_CLIENT_CERT.pem file contents:

```
-----BEGIN CERTIFICATE-----
MIIFPzCCBCFgAwIBAgIS3SGXUxVkgYN9r5PZvhFNF148MA0GCSqGSIb3DQ5BBQUA
... many more lines like those above ...
ITywFF+LW4hdG5TYw2smJmbBgkfbW7nusufXAzg7I0E5z2HyxRmLm+Eees4J00mo
f6jn
-----END CERTIFICATE-----
```

You don't need the other lines that are in the file.

IMPORTANT: if your .pem file does not have a PRIVATE KEY section, then you must already have the private key in another file somewhere else - you must find that file and get it into pem format. The private key is created when the CSR (Certificate Signing Request) was initially sent to the certificate vendor (Verisign, GlobalSign, etc). It CANNOT be generated later - the private key and the certificate are a matched set.

If you want to include a full certificate chain in SIGNED_CLIENT_CERT.pem, make sure that:

- The certifcates are listed in the order of Application Certificate, Intermediate Certificate(s), Root Certificate (possibly the reverse of what is in the original .pem file)
- There needs to be a blank line between each --END CERTIFICATE-- and --BEGIN CERTIFICATE-- section

Thank you Martin for these tips :)

2. Save the certificate's private key file to
   C:\Program Files\PA Server Monitor\CA\CLIENT_PRIVATE.pem
3. Save the SSL certificate to
   C:\Program Files\PA Server Monitor\CA\SIGNED_CLIENT_CERT.pem
4. PA Server Monitor will need to know the password for the private key. You can specify this by running the following command:

   ```
   "C:\Program Files\PA Server Monitor\diag.exe" /SETCONFIG=SSLCertPKPW:your-certificate-password
   ```

   The above command will encrypt and store the password with a machine-specific key in the registry.

   If you ever need to erase the password (such as if you delete the CA folder and go back to the self-signed certificate), run:

   ```
   "C:\Program Files\PA Server Monitor\diag.exe" /SETCONFIG=SSLCertPKPW:
   ```

5. Restart the PA Server Monitor service and it will now be using your SSL certificate.

Create your own new certificate

1. Go to the C:\Program Files\PA Server Monitor\CA folder
2. Create a folder inside CA named **NewCert**.
3. Copy Client.cnf from CA into **NewCert**
4. Open **NewCert**\Client.cnf in a text editor. Go to the PACA_dn section near the bottom and edit the values as you like (C=Country, ST=State/Province, L=City).

   If you want to change the private key file's password, change the entries on the lines for input_password and output_password.

   Change the CN value to the hostname of your server. Some SSL certificate providers expect to see a dot in the name, so the public name of your server would best (something like monitor.mydomain.com).

   Note that depending on the SSL provider that you use, the subjectAltName field might be ignored which is where additional machine names are mentioned.
5. Open a command prompt and change directory to
   C:\Program Files\PA Server Monitor\CA**NewCert**
6. Run the following to tell OpenSSL where to find your configuration file (do NOT use quotes, even if there are spaces in the path):

   ```
   set OPENSSL_CONF=C:\Program Files\PA Server Monitor\CA\NewCert\client.cnf
   ```

Then run the following to actually create the Certificate Signing Request file (also known as a CSR file). DO use quotes if there are spaces in the path: (note the below is all on one line)

```
"C:\Program Files\PA Server Monitor\openssl.exe" req -newkey rsa:2048 -keyout "C:\Program Files\PA Server Monitor\CA\NewCert\CLIENT_PRIVATE.pem" -keyform PEM -out "C:\Program Files\PA Server Monitor\CA\NewCert\SSL_CERT_CSR.csr" -outform PEM -rand "C:\Program Files\PA Server Monitor\openssl.exe"
```

7. This will create two new files:
   SSL_CERT_CSR.csr -- this is the Certificate Signing Request file that you will send/copy to the SSL certificate vendor (like Verisign, GlobalSign, etc)
   CLIENT_PRIVATE.pem -- this is the private key file for this certificate. This file will need to remain on the server, but should be kept private.
8. To see what you are sending to the SSL provider, run:

```
"C:\Program Files\PA Server Monitor\openssl.exe" req -in "C:\Program Files\PA Server Monitor\CA\NewCert\SSL_CERT_CSR.csr" -noout -text
```

9. After sending SSL_CERT_CSR.csr to a certificate provider, you will get back a certificate file. Save the file (in PEM format) to:
   C:\Program Files\PA Server Monitor\CA\SIGNED_CLIENT_CERT.pem

   If you want to include a full certificate chain in SIGNED_CLIENT_CERT.pem, make sure that:
   - The certifcates are listed in the order of Application Certificate, Intermediate Certificate(s), Root Certificate
   - There needs to be a blank line between each --END CERTIFICATE-- and --BEGIN CERTIFICATE-- section

   Thank you Martin for these tips :)

10. When the above file is copied, also copy
    C:\Program Files\PA Server Monitor\CA\NewCert\CLIENT_PRIVATE.pem
    into the CA folder.
11. PA Server Monitor will need to know the password for the private key. This password can be found in the client.cnf file on the line with input_password. You can give PA Server Monitor the password by running the following command:

```
"C:\Program Files\PA Server Monitor\diag.exe" /SETCONFIG=SSLCertPKPW:private-key-pass-phrase
```

    The above command will encrypt and store the password with a machine-specific key in the registry.
12. You can optionally delete the NewCert folder at this point.
13. Restart the PA Server Monitor service and it will now be using your SSL certificate.