PA File Sight

Version 9.3 Ultra

Last Update: January 08, 2024

PA File Sight Documentation Table of Contents

Welcome & Install

Getting Started

Adv. Configuration

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

Automatic Fail Over
>   Setup a second instance of PA File Sight to monitor the primary monitoring service, and take over if it fails

Blocked Users List
>   Blocks access to all drives monitored by PA File Sight to any account added to the Blocked List.

Command Line
>   Different options that can be used to help automate PA File Sight.

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

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

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

Endpoints
>   Detect file copying using the File Sight Endpoint agent.

Endpoint Alerts
>   Configure alerts for cases where the Endpoint goes offline

Endpoint Operations
>   Apply configuration options to many Endpoints at once

Endpoint USB Blocking
>   Configure the File Sight Endpoint to block unauthorized external/USB drives and CD/DVDs.

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.

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 File Sight 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 File Sight 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.

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

Adv. Configuration

Concepts
Trusted Applications concepts

Trusted Lists
Trusted Applications - Trusted Lists

Statements
Trusted Applications - Statements

Rules
Trusted Applications - Rules

Getting Started
Trusted Applications - Getting Started

Day to Day Ops
Trusted Applications - Day to Day Operations

Monitors

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

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.

Drive Sight
Protects servers and workstations by preventing CD/DVDs and/or external drives, including USB drives, from being attached. Any specified devices that are attached are immediately detached by the operating system so they cannot be accessed.

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.

File Sight
The File Sight monitor watches real time file access by users and programs. You can configure which files it watches, and how you are notified when a particular operation (file read, write, delete, etc) occurs.

*The **Ultra** version also lets you:*
* Record the file access operations to a database for reporting (by user, by file, by operation, etc)
* Alert on user usage patterns (i.e. user reads X amount of data in Y time, useful for ransomware protection and detecting file copying)

NOTE: This monitor can ONLY monitor drives on the local computer. Watching files on remote computers requires that the PA File Sight service (or a Satellite) be installed on the remote computers.

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.

Trusted Applications
Checks all file access on a server against a set of rules (application whitelisting) to determine if the application should start and whether file access is allowed.

Actions

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

Add to Blocked List
>   Adds all users reported on by a File Sight monitor to the Global Blocked Users List.

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.

Password Protection
Password protect web reports in PA File Sight

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.

FS: All Changes
Get a quick report to see everything PA File Sight has recorded in a specified time frame.

FS: Custom Data Set
Create a report that filters on many different File Sight criteria.

FS: File Changes
Quickly see all changes that happened to specific file or set of files.

FS: Type of Change
See all file operations of a specific type. For example, all files that were deleted in the past two days could be quickly shown.

FS: User Activity

Find all users who have done more than a specified number of specific operations. For example, anyone that has deleted more than 50 files in the past week.

FS: User Block List
Quick way to see which users are on the File Sight User Block List, and which are on the white list.

FS: User Changes
Select a specific user and a time frame to see all recorded file activities they have performed.

FS: User R/W Amt
Find all users who have read and/or written a specified amount of data in a given time frame.

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 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: 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 File Sight

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 File Sight

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

Deploy Satellites
Information on deploying Satellites remotely.

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

Integration
How to integrate with other enterprise systems and usage scenarios

NIST 800-53
How to fulfill NIST 800-53 requirements to protect and audit data access

NIST 800-171
How to fulfill NIST 800-171 requirements to audit data access

Office365 and OAuth
Authenticating to Office365 with OAuth 2.0

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

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.

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

Product Overview for PA File Sight

Thank you for choosing PA File Sight. The following documentation offers help in installing, configuring and using PA File Sight. These topics are also shown in the help menu at the left of the screen.
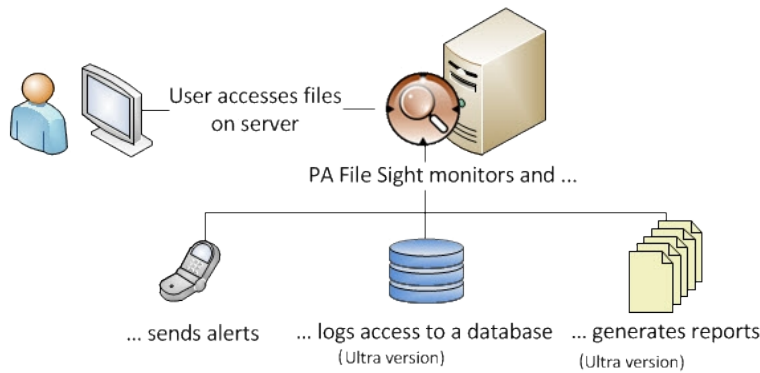
> 💡
>
> If you are looking for something specific, try the Search box at the top of the page.

Product Architecture and Layout

Typical Installation (Main Install)

Every installation has a monitoring service installed on a Windows Server or Workstation. This monitoring service will monitor the drives in the server it is installed on.


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

Centralized Capabilities

In addition to monitoring drives on the local server, Ultra editions of PA File Sight can also manage the monitoring of remote servers, including across the Internet without needing a VPN. This is accomplished by installing a Satellite Monitoring Service on additional servers or workstations. The Satellite will monitor itself (the server it is installed on). Alerts and monitoring data will be sent back to the Central Monitoring Service via SSL-encrypted HTTP.

The Ultra version can manage all configuration from a central console.
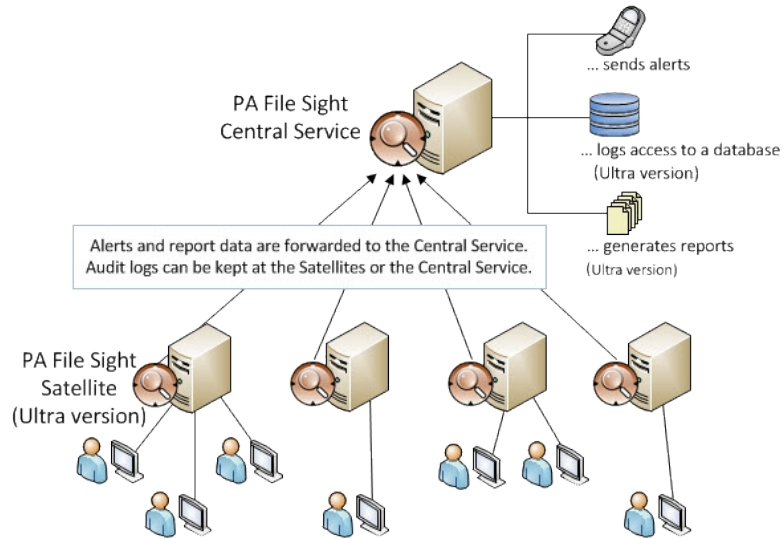
Installation Help

The first step to using PA File Sight is to install the Central Monitoring Service.

Terminology and Concepts of PA File Sight

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

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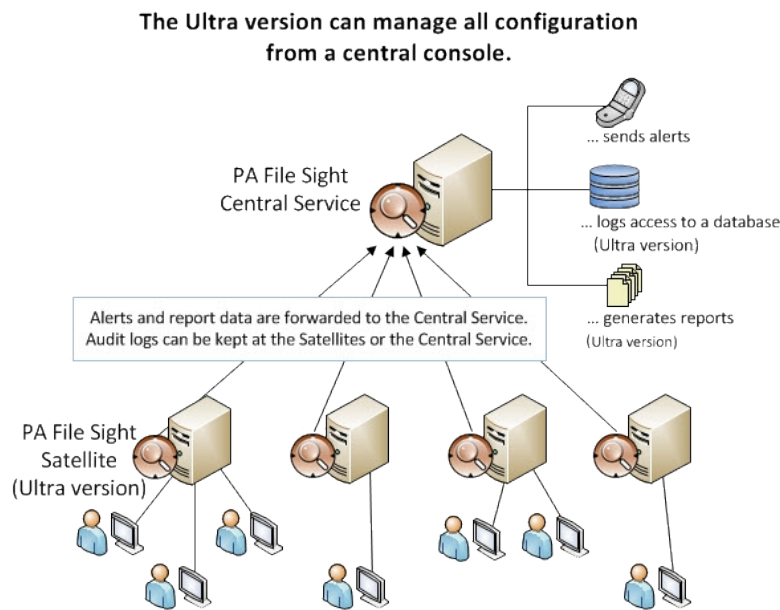
(Central) Monitoring Service

The Central Monitoring Service is the part of the product that performs the monitoring of the file activity on the local computer. 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.

If only a single server is being monitored, this will be the only Monitoring Service. If additional servers are being monitored and they are reporting to this service, this service is then referred to as the Central Monitoring Service. Note that the Lite Edition does not have centralized capabilities, and thus does not communicate with other Monitoring Services.

Satellite Monitoring Service (Ultra Edition)

The Satellite Monitoring Service (or just Satellite for short) is an optional additional monitoring engine. It can run monitors on additional computers just like the Central Monitoring Service. If you want central monitoring, configuration and reporting for many servers, Satellites are typically installed on additional servers and they are then pointed back to the Central Monitoring Service.

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

Product Terminology

PA File Sight 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.

Globally defined list of actions
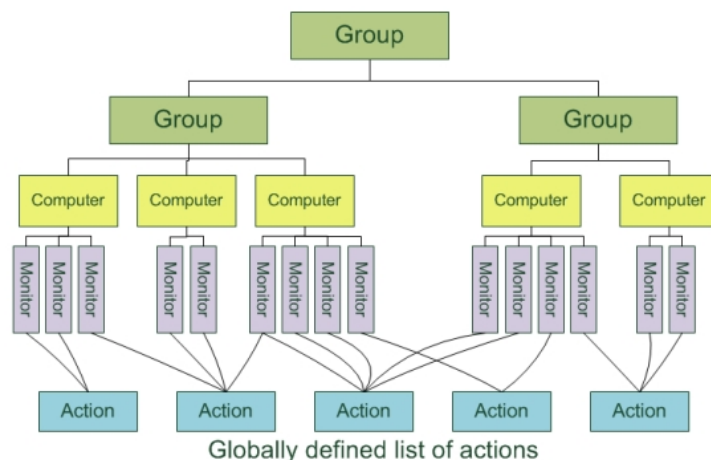
Group (Ultra Edition)

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. Note that Groups only exist and make sense with the Ultra Edition, since the other editions can only configure and monitor a single computer.

Adding new computers is best done with Easy Deploy.

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

Computer

Computers represent a server with drives that are monitored. Monitors are created and attached to computers.

Server status reports are generated automatically and show the status of the monitors on the server.

Monitor

A Monitor continuously monitors file and directory activity on monitored drives and compares that activity to settings you specify. Detected changes that meet your criteria can be alerted on, and with the Ultra version are written to a database so historical reports can be run.

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 (only the Ultra version has the database, the Lite version does not). 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 File Sight 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.
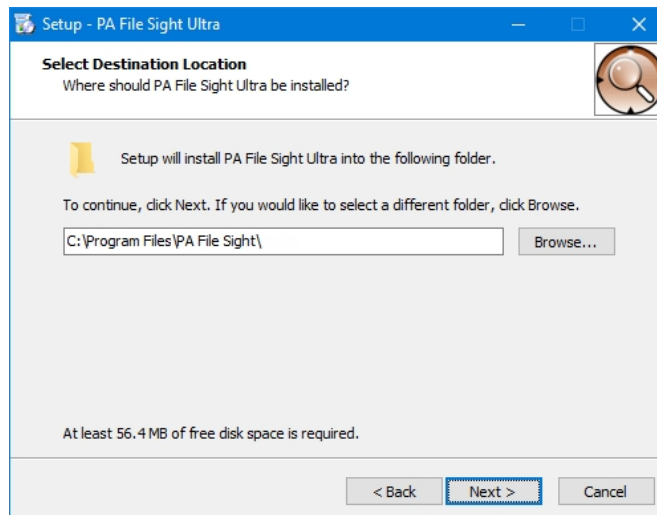
3. Do one of the following:
   - Accept the default folder path.

   - 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.
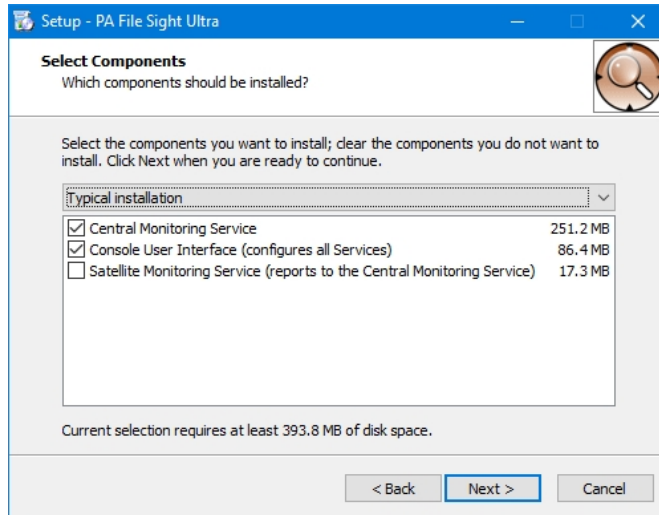
5. Accept the defaults for a typical installation. You can select the components individually, or you can click the **arrow**, and then select an installation from the list. For a first installation, choose the default "Typical installation" with a monitoring service and console.

6. Click **Next**. The Select Additional Tasks page appears.
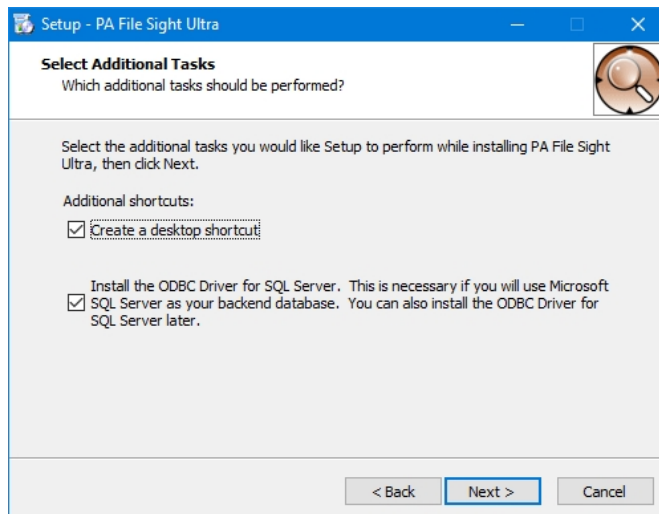

7. Select the **Create a desktop icon** option if you want the installation to place an icon on your desktop.

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.
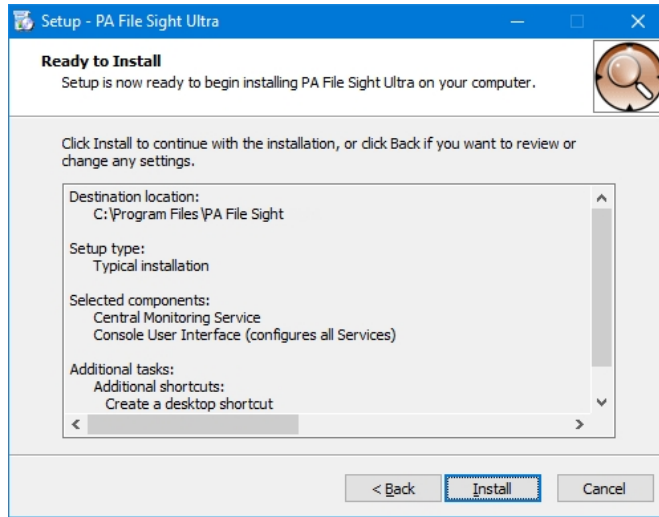
10. Click **Install**. The Installing page appears. When the installation has finished, the Completing the PA File Sight Setup Wizard page appears.
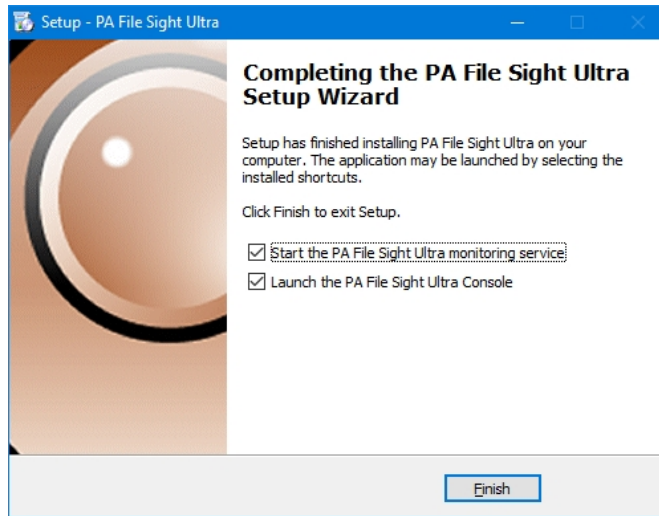
11. Specify whether you want to start the PA File Sight Service or launch the PA File Sight Console by selecting its option, and then click **Finish**. If you have selected the option to launch the console, the PA File Sight Console window appears.
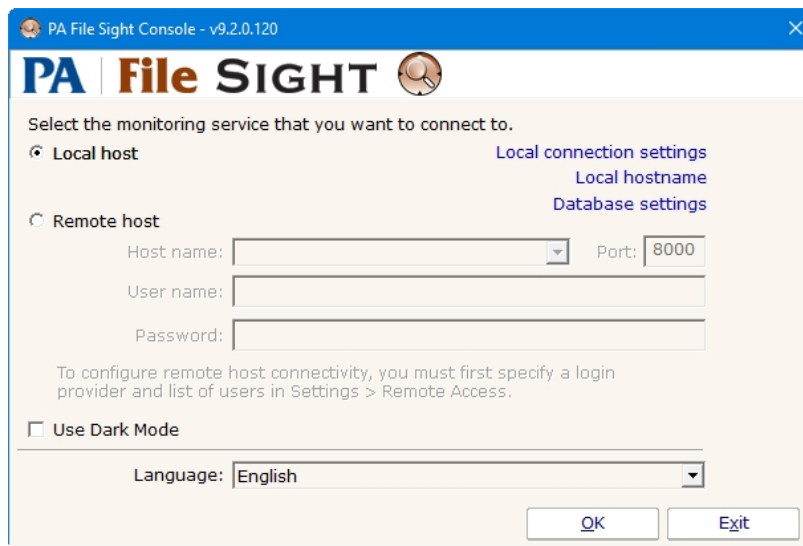
Next steps:

Start the Console GUI

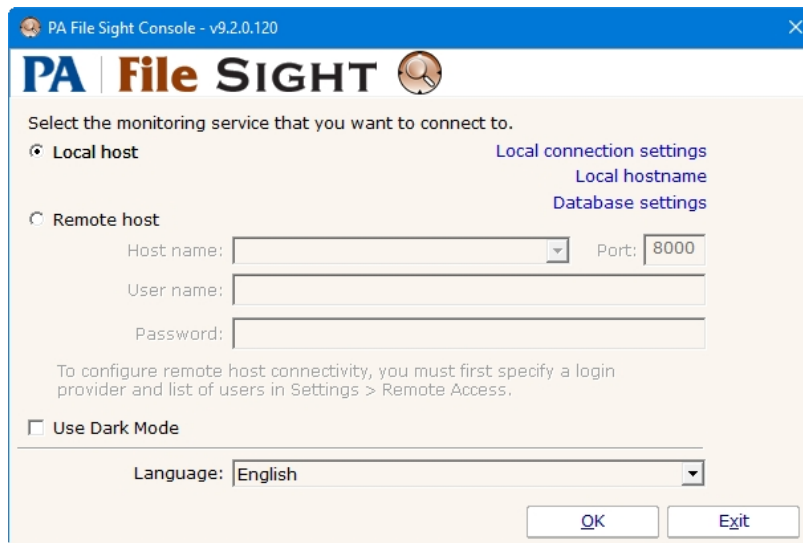Prerequisites for installing a remote Console or Remote Satellite

Install the Console GUI on additional computers

Install the Remote Satellite on remote servers

Starting the PA File Sight Console

To start the PA File Sight Console

1. Double-click the PA File Sight 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 File Sight Console

The Console is the administrative interface to PA File Sight. 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
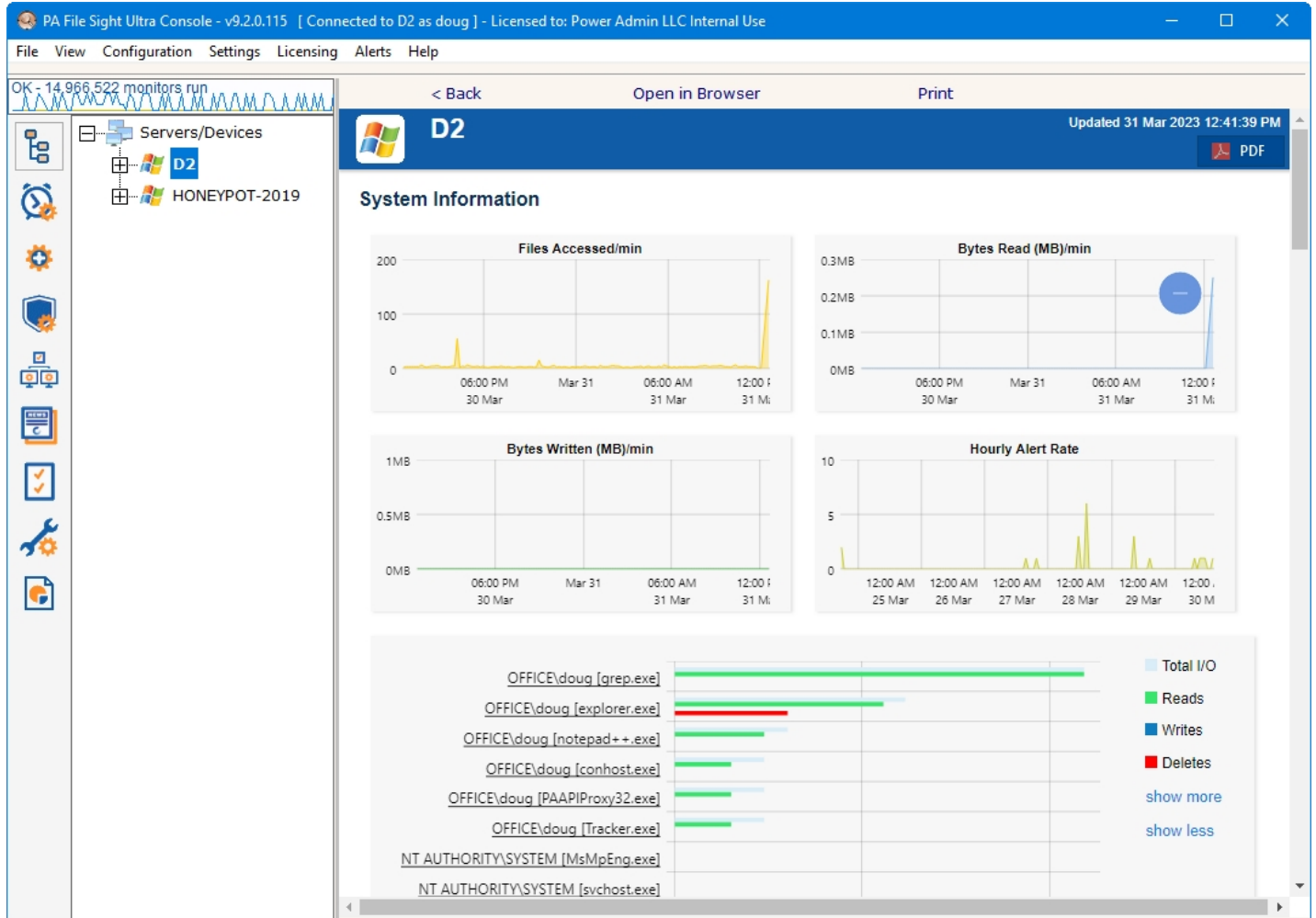
Activity Graph The Activity Graph at the far left is an indication of system activity. The green line indicates the number of monitors that are running or scheduled to run, and the yellow line indicates the number of actions that have run. Monitors running on remote Satellites are not represented. Double 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.

Trusted Applications takes you to the rules, lists and warnings that make up the Trusted Applications feature.

Endpoints shows all of the options work viewing, configuring and reporting on Endpoints

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 File Sight Startup Wizard

The instructions that are provided here apply to the process that you can follow when you run PA File Sight 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 File Sight, 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 File Sight (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.
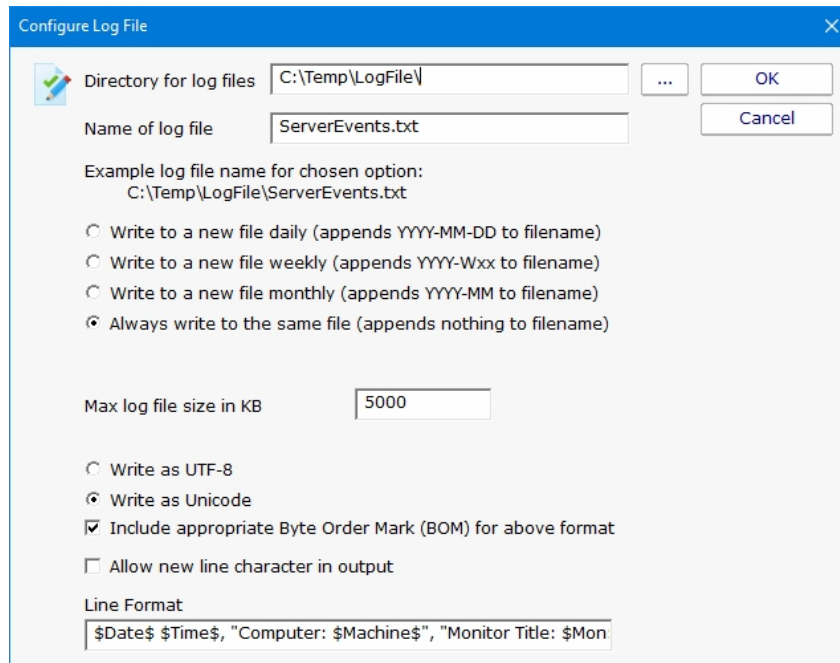
Select OK when you are finished with this screen.

Press OK to continue. At this time, you will be prompted for an initial path to be monitored. A File Sight monitor will then be created and this path filled in. That completes the Startup Wizard.

Global Settings

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

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

System Alerts - Some alerts are sent to you from the monitoring system itself, and not in response to particular monitors. These alerts include security warnings (change of configuration, etc), license issues, internal problems, unaccessible computer warnings, etc. You can control which of these internal alerts are enabled, and which notification method each one should use.

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

Database Settings dialog allows you to set up PA File Sight to use the embedded SQLite database or Microsoft SQL Server as the storage for PA File Sight data.

Report Settings affect the storage of archived reports and the behavior of the reporting features of PA File Sight.

HTTP Server Settings allows you to change details of the way the built-in web server in PA File Sight operates.

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 File Sight.
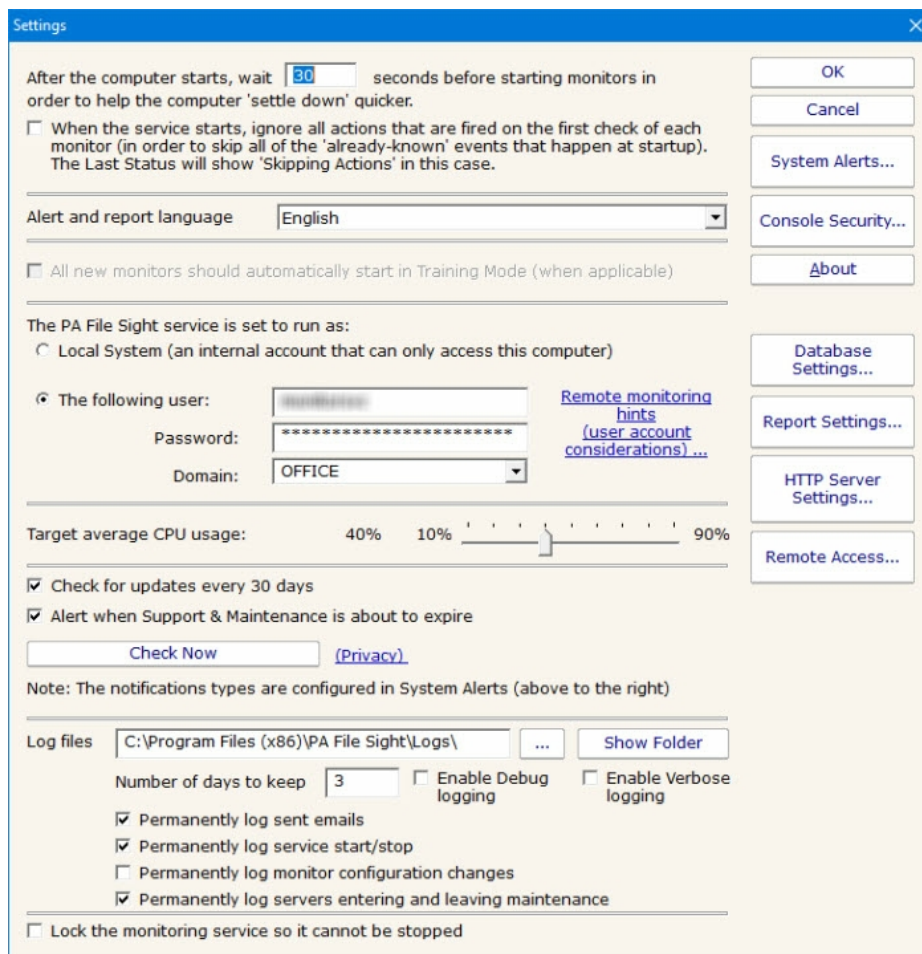
Startup Wait Time - When the monitoring service starts, you can instruct it to wait a number of seconds before active monitoring begins.

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 File Sight 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 File Sight 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 File Sight.

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 File Sight (normally `C:\Program Files\PA File Sight`.)

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

Server name - name of server on which SQL Server instance is located. (Note that with SQL Express, this is often {server_name}\SQLEXPRESS)

Database name - the name of a SQL Server database which will be used for PA File Sight storage. The database must exist prior to use 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 File Sight 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 File Sight, 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.
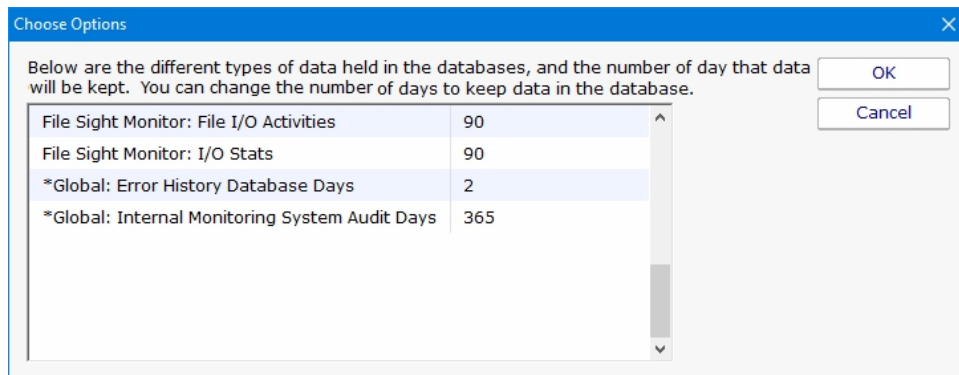
Data Location

With Satellites in use, the question of where to keep audit data arises. By default, each Satellite uses its own database settings (which means each Satellite will store data in its own local SQLite database by default). You can specify that each Satellite connect to a MS SQL Server database and store its data there. The check box at the bottom gives another option: centralized database storage.

Centralized Database Storage

By underlining the check box at the bottom of the Database Settings dialog, you instruct the Satellites to forward all of their file I/O audit findings to the Central Monitoring Service. The Central Monitoring Service will then store that data in the database that it is configured to use (local SQLite or MS SQL Server as defined above). The Satellites will cache the file I/O records in memory, and then deliver the records to the Central Monitoring Service every few minutes. If the connection to the Central Monitoring Service is not available, the records will be cached in memory until the connection becomes available.

Performance Considerations

Naturally the Centralized Storage setting will put a little more load on the Central Monitoring Service, the network connection to it, and the database connection. In our testing with 500 Satellites connected to a Central Monitoring Service, we found that MS SQL Server could easily keep up. The embedded SQLite kept up with the write requests until around 100 to 200 servers. The network bandwidth used is surprisingly light. Each minute, each Satellite will make approximately 4 HTTPS connections. Approximately 4KB will be sent to the Central Monitoring Service, and approximately 2KB being sent back to the Satellite during each minute. These values can vary widely based on monitor configuration. The **[System Summary Reports] -> System Statistics** report shows bandwidth usage from each Satellite and is a good way to check this for your particular configuration.

Reporting is not affected by the Centralized Database Storage setting. If data is kept in a central database, reports will query that database. If data is stored out at the Satellite locations, the Satellites will be queried when a report is generated for their part of the report.

Note that when Centralized Database Storage settings are changed, existing data in the database(s) is <u>not</u> moved to the new location, and will in some cases become invisible to queries.

Report Settings

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

Days before Reports are Cleaned Up - This value is the number of days reports (HTML files) will be available. After the given number of days, PA File Sight will delete the report. Note that reports that are always being updated (system summary reports and Scheduled Reports) will not be aged out.

Clean All Reports Now - Pressing this button will purge all reports. Reports that are constantly refreshed (like the status reports for example) will be re-created on their normal reporting cycle.

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.

Show Maintenance Period on server status report - Self explanatory.

Turn off "Enable WMI Hint"... - If PA File Sight is configured to poll a server via WMI for richer status reports, but that WMI polling fails, an error/hint message is shown at the top of the report. This check box disables this warning.

HTTP (Web Server) Configuration

The PA File Sight service contains an embedded web server for serving HTML reports to the Console and to browsers, as well 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.
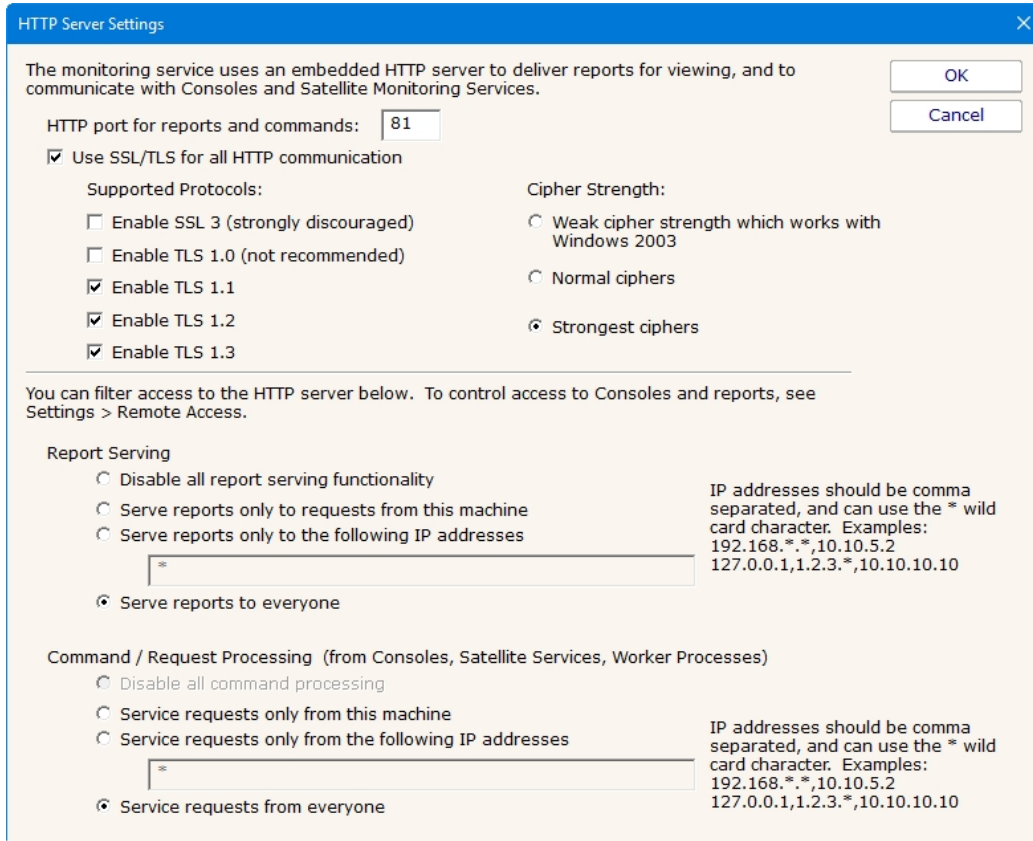
The options available for controlling the built in web server are as follows.

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 File Sight chooses a different port so it doesn't conflict. If you have another application that is already using this different port, you can easily change the port to another number.

Use SSL
PA File Sight supports using HTTPS for all communication to the service, which includes viewing reports, and Console-to-service communication. Self-signed digital certificates are used. This means most browsers will display a warning even though the HTTPS network traffic is encrypted. To fix the warning in the browser, follow the instructions on SSL Certificate Hints.

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 File Sight serves reports. There are four options. You can disable all report serving. You can enable serving of reports but only to the same machine on which PA File Sight is installed. You can serve reports only to a set of other users, identified by the IP addresses of their computers. Or, you can serve reports to any other computer that requests reports. The default setting is

"Serve reports to everyone".

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.

Easy Deploy

Easy Deploy is meant to help push out Satellite Monitoring Service software to servers that should be monitored.
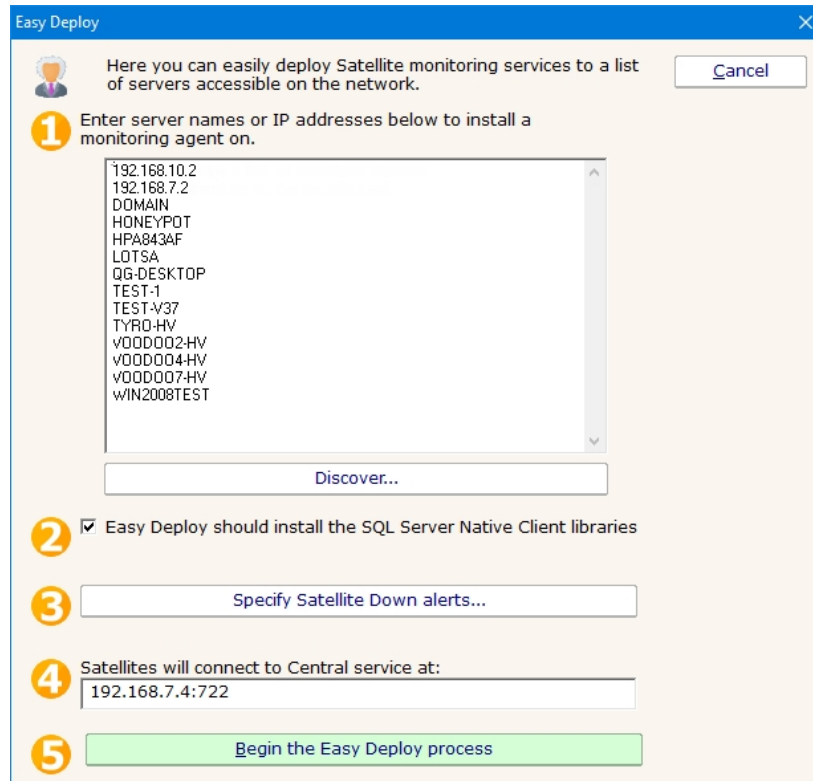
Simply follow the steps outlined with the orange numbers:

1. Enter a list of servers to receive the Satellite software. The Discover button can be used to do a ping sweep and find servers on your local network for you. Connections will be made to these servers using their administrator share. That means you'll want the PA File Sight service to be running as a domain account that will grant access to these servers, or add a username and password to each line next to the server name, like:
192.168.10.2,administrator,p@assW0RD

2. When Satellites are not connecting to the Central Monitoring Service, you can receive an optional alert. This button controls that. It can be changed later on an individual Satellite basis, or many can be changed at once via Bulk Config.

3. The Satellites have to know the server name and port to connect to the Central Monitoring Service. The default value will work in most circumstances, but if a different machine name (perhaps an IP address) needs to be used, you can change this here. Once the value is sent out, you can change it on each individual Satellite if needed.

4. Begin! When the process starts, you will be taken to a report that updates every 30 seconds showing the progress being made.

Deployment Process

The following steps are automatically followed by the deployment process:

1. PA File Sight's Setup.exe (copied from the product's Install folder) is sent to the remote server via an administrator share.

2. PA File Sight's Setup.exe program is launched via RemCom, an open source package similar to Microsoft's PsExec program.

3. Setup.exe will run silently installing the Satellite component on the target server. Setup is instructed to never reboot the

computer.

4. The Satellite service will be started and told to connect to the Central Monitoring Service using the server name and port specified above.

5. The Satellite will connect, and the Easy Deploy process will automatically accept it, and then add a computer (the Satellite itself) to be monitored by the Satellite.

At this point, you can add monitors to the target servers.

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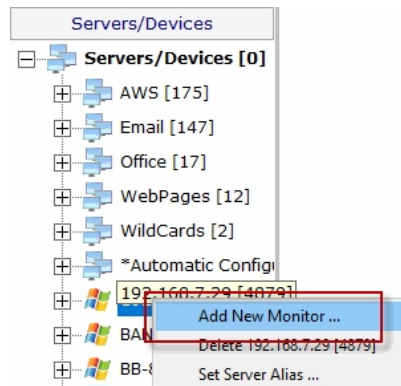
You will be shown the dialog below with all available monitors for your product and license (note that they may not be the same ones pictured).

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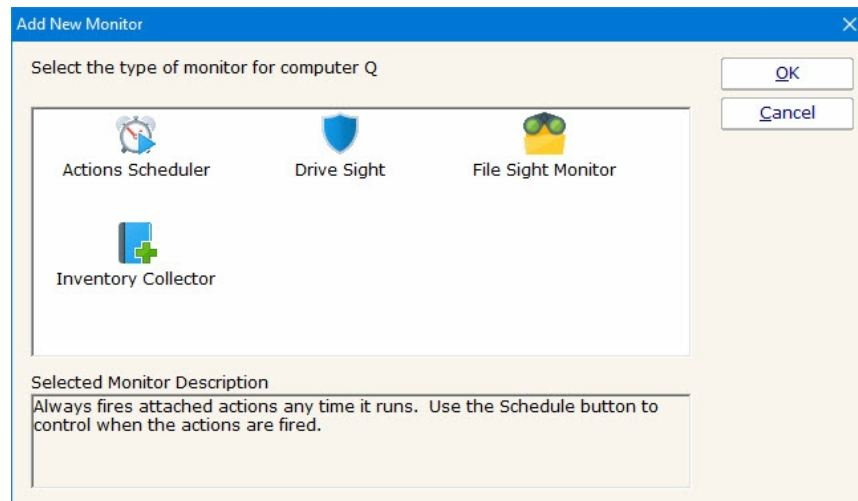
Choose the type of monitor that you want and press OK. The monitor's configuration dialog will then be shown.

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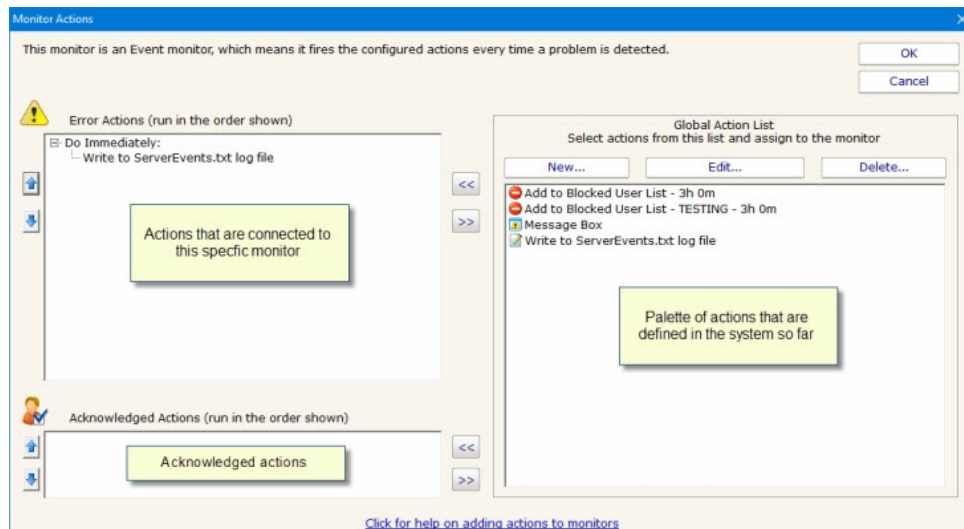
On the left are shown all of the actions that are attached to this specific monitor. When the monitor 'fires actions' it will run that list of actions in the order shown. You can change the order with the blue up and down arrow buttons.

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)

Bulk Config

Bulk Config is one of the most powerful configuration feature in PA File Sight. 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.
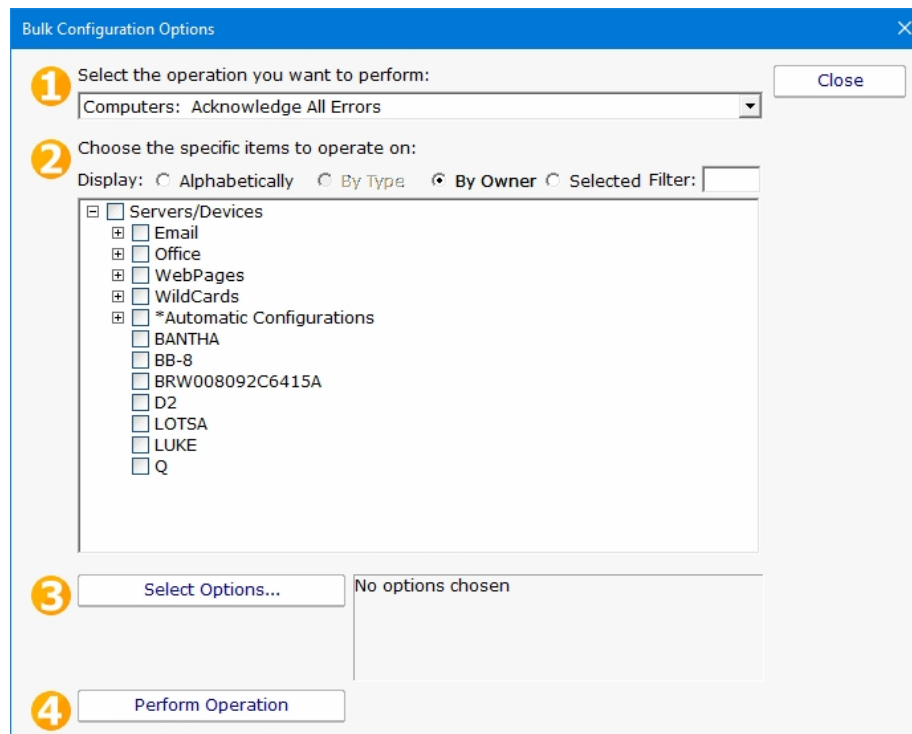
Once you've chosen the operation, and checked the boxes next to the objects that you want to operate on, press the Select Options button. This lets you specify details for the operation to be performed. When you're done, the text box next to the Select Options button will display a summary of what will 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.

ErrID ▼	Error Time ▼	OK Time ▼	Monitor Title	▼	Details	▼	Acknowledged By ▼
1679...	3/25/2020 1:54:19 PM		Event Log Monitor		* Event Time: 25 Mar 2020 01:51:56 PM * Source: Microsoft-Windows-DistributedCOM * Event Log: System * Type: Error * Event ID: 10006 * Event User: OFFICE\\monitorsvc * DCOM got error "2147944122" from the computer		☐

○ 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.

☑ Enable error acknowledgement feature

    Email alerts can be acknowledged by replying to the email alert. For this to work, the reply message needs to go to a mailbox that you specify below. You will need to create this mailbox and a login.

    ☑ Enable email acknowledgement

        Use the following Reply-To: address for email alerts (to make replying easier):

        [   ]@gmail.com

        ● Access mailbox via POP3
        ○ Access mailbox via IMAP4

Mail Server Name	pop.gmail.com	Port	995
Username (email address)	[ ]@gmail.com	Encryption	Implicit (SSL)
Password	****************		
	Test Connection		

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.
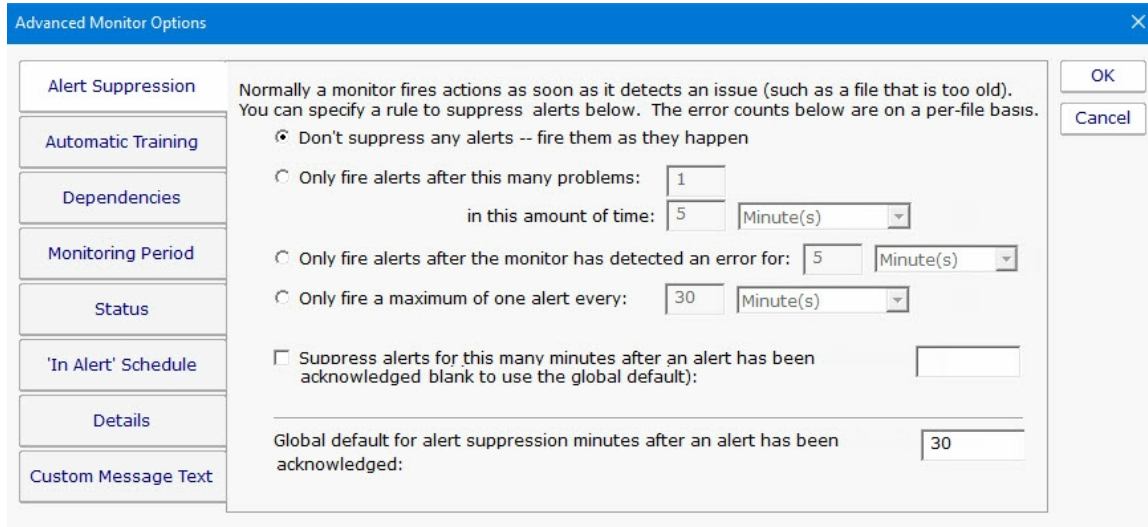
Each of the different option tabs is discussed below.

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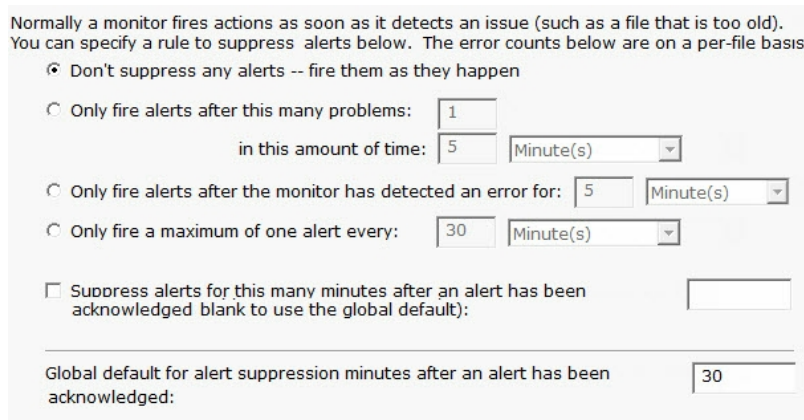
With the Alert Suppression settings, you can instruct the monitor how often and how soon you want to be alerted about a specific issue. This enables the monitor to skip the first few failures on a specific device if you wish and only warn after an error has happened a few times or for a particular amount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

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

Automatic Training

> To help suppress false positives and to learn the system's normal behavior, the Automatic Trainer can watch the system and configure the monitor to ignore behavior it sees during the training period.
>
> How much longer would you like the Automatic Trainer to watch for normal behavior?
>
> Keep watching for this much longer: [0] [Day(s) ▾] (Not currently training)
>
> NOTE: If the Automatic Trainer is currently active and you want to switch immediately to normal scanning and alerting mode, press End Training Period.
>
> [End Training Period]

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

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

Dependencies

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

> Select the monitor(s) that this monitor depends on. When this monitor is scheduled to run, it will only run if all dependent monitors are in the OK state.
>
> Display: ○ Alphabetically ○ By Type ◉ By Owner ○ Selected   Filter: [   ]
>
> ⊞ ☐ Office
> ⊞ ☐ WebPages
> ⊞ ☐ WildCards
> ⊟ ◪ DOMAIN2
>   ☐ Bandwidth monitor
>   ☐ Critically Low Disk Space Check
>   ☑ Event Log Monitor
>   ☐ Inventory Collector
>   ☐ Monitor services on DOMAIN2
>   ☐ Ping DOMAIN2
>   ☐ System Performance Metrics
>   ☐ Very Low Disk Space Check
>   ☐ Watch \\DOMAIN2\C$\Windows + subdirs
> ⊞ ☐ LOTSA

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.

Monitors can pass additional alert information, or override the default alert message that would normally be sent.

Alert Subject Override [   ] (leave blank for default subject)

⦿ Set the text below in the $MonitorMsg$ tag to be used in alert text templates
○ Override the alert text template and use what is below instead

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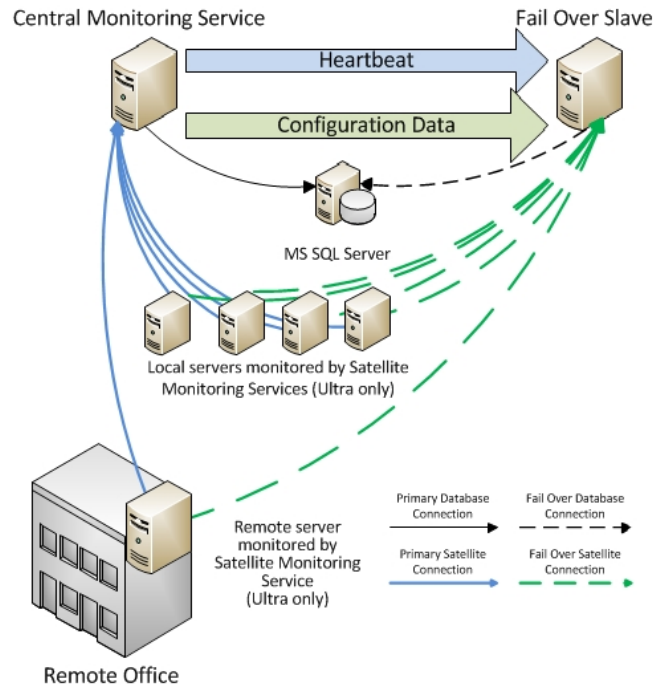
Data that is automatically mirrored to the Fail Over Slave are:

- 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 File Sight service on both servers need to be using the same MS SQL Server. This can be changed in Database Settings.

2. PA File Sight on both servers should use the same service account.

3. Use the same version of PA File Sight on both servers. You can get the installer from the Central Server at C:\Program Files\PA File Sight\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\PAFileSight   [DWORD]FO_IsSlave = 1

3. Restart the PA File Sight 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.
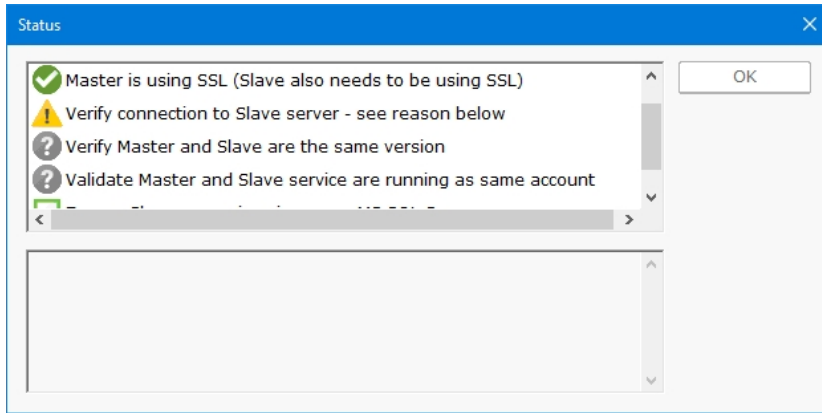
Once all items are green, press OK and the Master and Slave will begin synchronizing configuration information.

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.

Blocked Users List

The Blocked Users List is a global list of accounts shared among all File Sight monitors within a PA File Sight installation, including those on Satellite Monitoring Services. Its purpose is to protect the servers from accounts performing malicious activities.

There are two parts to the list:

Global Blocked User List

All accounts listed here will have be blocked from all file access to all monitored drives (at all sites covered by the installation). That means file access via network share will be blocked, and if the user is logged into a protected server (either directly or via Remote Desktop) they will not be able to access files, which usually means any programs they are running will fail.

When an account is added to the Blocked list, it is with a time duration. After the time expires, the account is automatically unblocked. However, if the account keeps trying to access files while being blocked, the blocked time is reset. This means the account needs to stop trying to access files for the duration of the blocked period.

Global User Account White List

Any account on the White List will not be blocked under any circumstance. Be careful which accounts are added to the White List. Accounts that you might want to add are those that specific services run as, such as a database service or an anti-virus service.

Unblocking Users

When a user is removed from the Blocked User List, they are automatically added to the White List for 3 minutes (a configurable time). This gives them time to complete whatever activity initially triggered putting them on the Blocked User List.

View the Lists

You can view the lists from the File Sight > User Block List report, as shown below.

The Blocked list will normally be empty. Note that you can see how an account ended up on the list (from an action, or manually).

You can also view the lists by opening a Add to Blocked Users List action. This is also where you can add and remove accounts from

the lists.
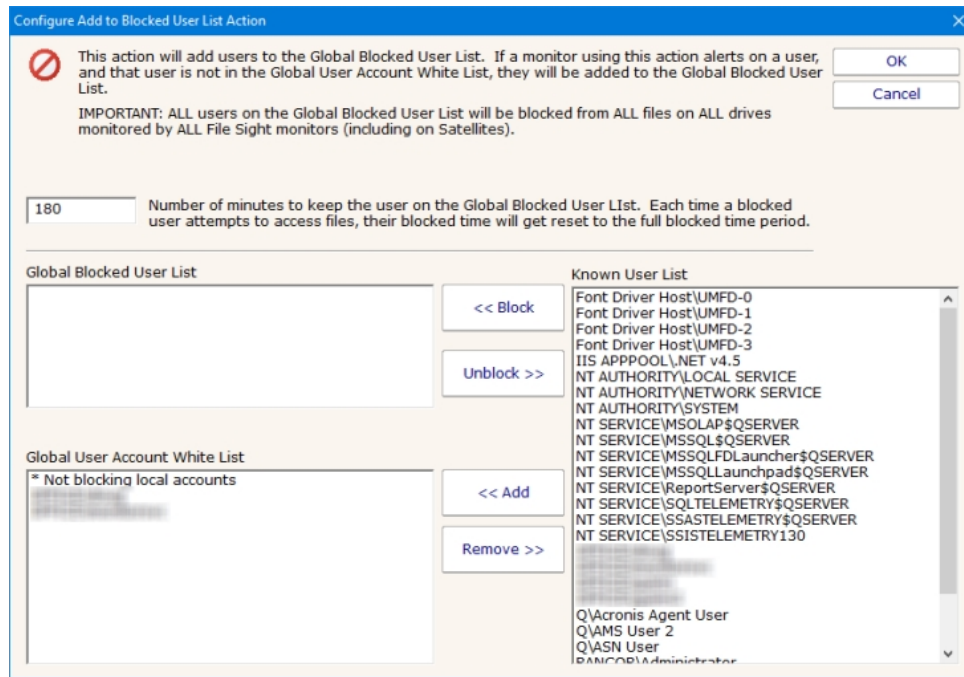
Blocking Effects

When a user that is being blocked tries to access a file, the file access will fail with error STATUS_DATA_ERROR (0xC000003E) "An error in reading or writing data occurred". This is an existing error code used by Windows, but it is uncommon to see it so it was selected. This can be changed to a different error code if needed. The application that the user is using may or may not show this error message.

Precautions

By default, and shown as the first entry in the White List above, local (non-domain) accounts are automatically added to the White List. This is to help prevent important services from being blocked.

Local accounts are *not* blocked if the server is a domain server (all accounts are domain accounts in this case), or if the server is not part of a domain (domain accounts don't apply in this case).

Testing

You might see accounts in the Blocked list with TEST added to the name. This account won't actually be blocked and was added with a Testing version of the Add to Blocked Users List.

Synchronization

The lists are automatically synchronized by the Central Monitoring Service and any Satellite Monitoring Services that are part of the installation. If a Satellite can't contact the Central Monitoring Service, it will keep using the last copy of the Global Blocked User List and Global User Account White List that it received.

Recovery

In an emergency situation where a critical account has been blocked, it is best to remove it from the Blocked list and add it to the White list. If the list can not be synchronized to a Satellite, you can clear the blocking by stopping the PA File Sight (Satellite) service. This will disable blocking.

Command Line Options

Starting PA File Sight 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.

FileSightSvc.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 FileSightSvc.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 FileSightSvc.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: FileSightSvc.exe /COMPRESS_DATABASES

3. After it finishes, restart the monitoring service

/U

Uninstall the PA File Sight service. -S can be appended to hide the confirmation dialog.

/I

Install the PA File Sight service. -S can be appended to hide the confirmation dialog.

/C

To launch FileSightSvc.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 <u>not</u> 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 <u>not</u> 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 File Sight configured, you probably don't want anyone making unauthorized changes. There are a few ways PA File Sight 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 File Sight 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 File Sight 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 File Sight\Config\Backup.

System Alerts

The Settings dialog also has a System Alerts button which will display the dialog below.
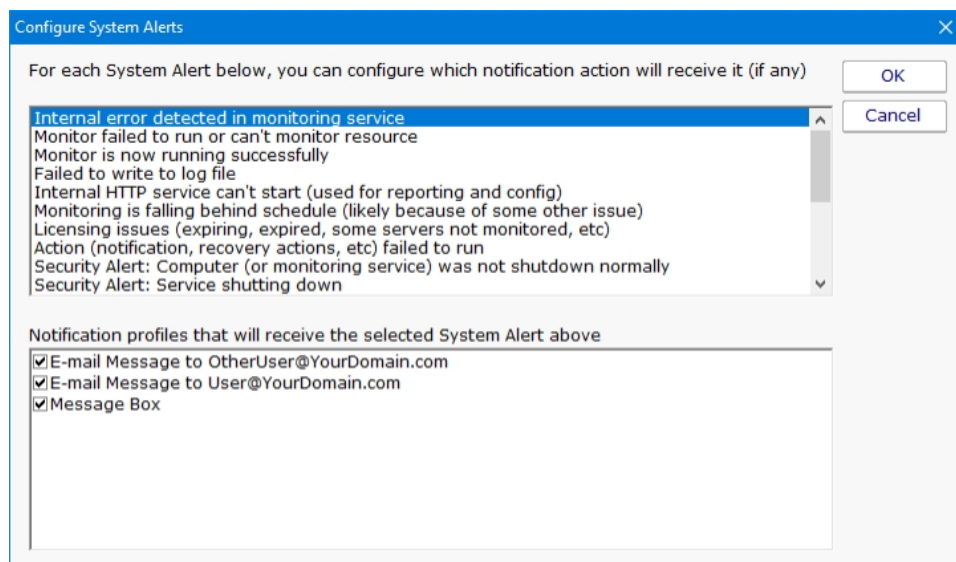
Here you can indicate ways of being notified for a variety of security-related events including:

○ 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.

Setting Windows Credentials

PA File Sight 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.
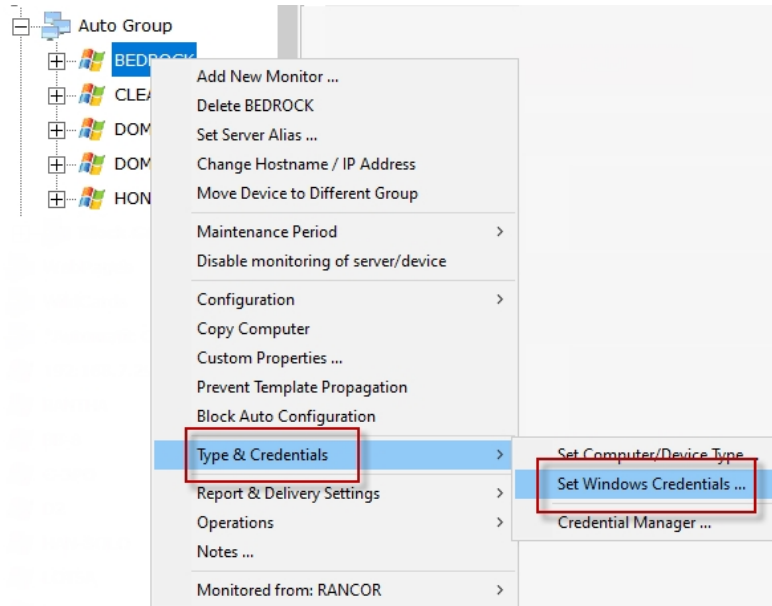
You can enter credentials, or just monitor the server using the login that the monitoring service is already using. The middle radio button is a convenience feature -- it lets the system try already-entered passwords to find one that works.
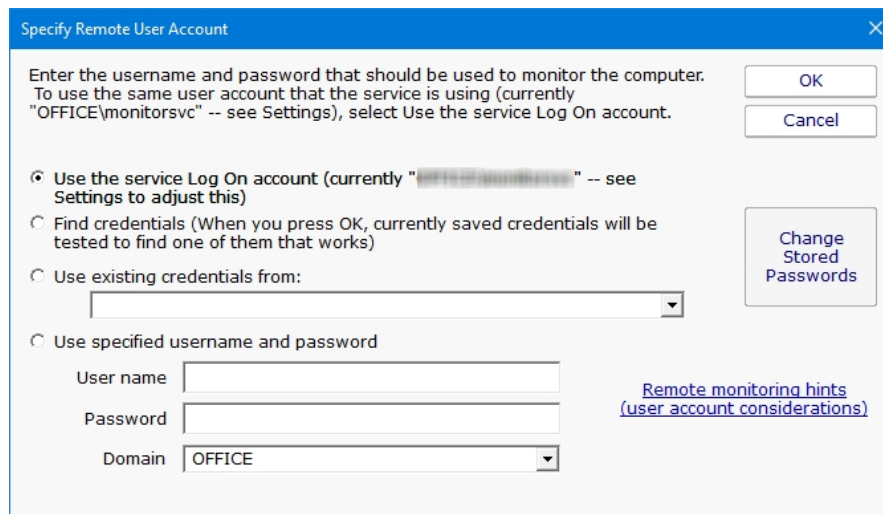
When you press OK, the credentials are checked by trying to access the target server's Event Log and the list of running services. If this succeeds, the credentials are saved.

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 File Sight Console can show custom icons for servers/devices and groups.
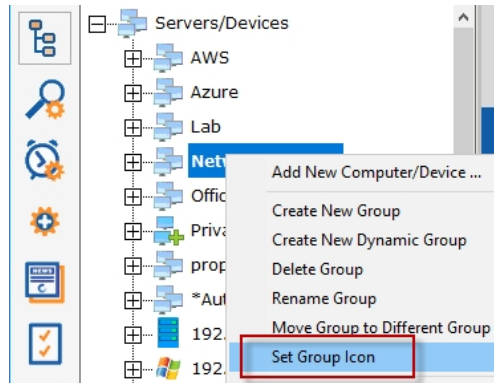
To set the icon on a group, right-click the group and choose Set Group Icon.
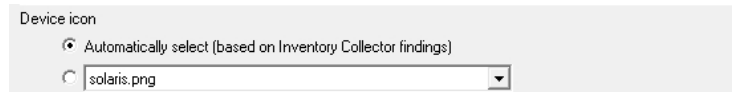
To set the icon on a server/device, right click the server/device and go to Type & Credentials. At the bottom of the dialog is a setting for the device icon. By default the icon will be chosen based on rules applied to what the Inventory Collector monitor finds.

Icon Files

You can add your own icon images by copying a .PNG file to C:\Program Files\PA File Sight\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 File Sight\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 File Sight\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.
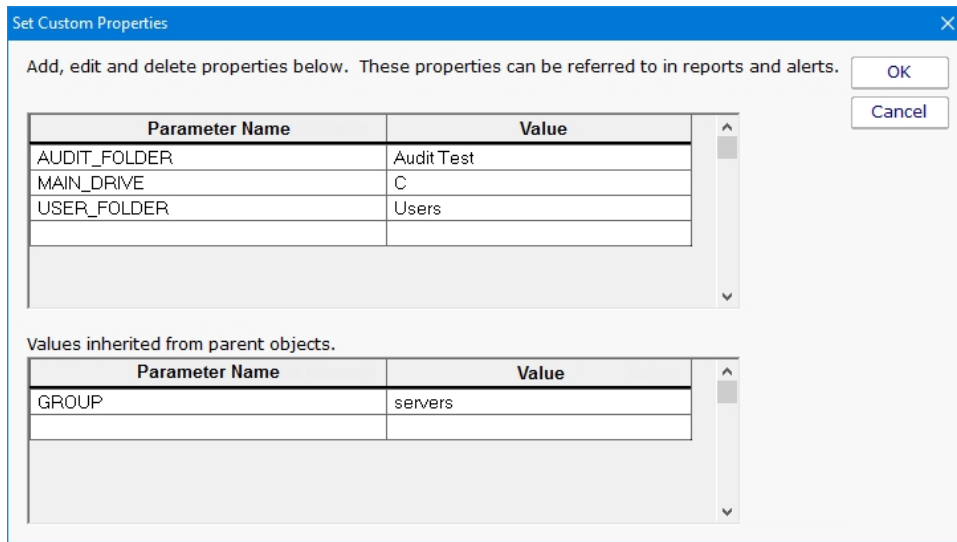
The above example shows Custom Properties on a Computer. AUDIT_FOLDER, MAIN_DRIVE and USER_FOLDER are all defined on the Computer. GROUP is defined at a higher level and is inherited by this Computer. If this Computer also had a value named GROUP defined, the Computer's value would be used (in other 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.

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.

OK - 44,725,701 monitors run

- Servers/Devices
  - AWS
  - Azure
  - Lab

< Back   Open in Browser

Test banner message

NETWORK MAP   OVERVIEW   GROUP SUMMARY

CURRENT ERRORS   STATUS OVERVIEW

Servers/Devices

Set Custom Properties

Add, edit and delete properties below. These properties can be referred to in reports and a

Parameter Name	
GLOBAL_ERROR_BANNER	Test banner message

Customize the Console's Operations Menu

When you right-click a server in the PA File Sight Console, there is an Operations menu which can do various things to the selected device.
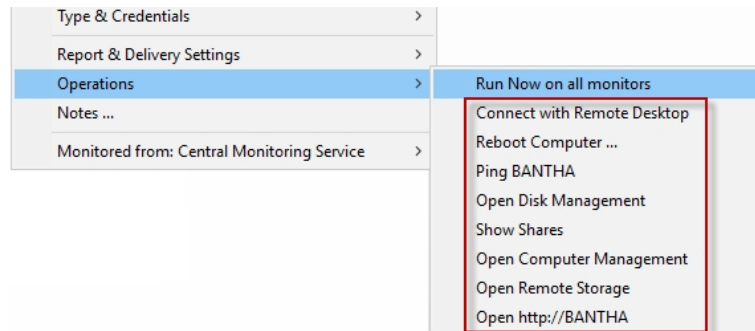
The list of commands can be changed, including adding commands for your own specific situation.

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

```
C:\Program Files\PA File Sight\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.

File Sight Endpoint

The File Sight Endpoint can perform Trusted Application checking, as well as help audit files that are accessed on a server from a client computer. The Endpoint is meant to run on user workstations. It does not do the full monitoring of the File Sight monitor which is used on servers.

Trusted Applications

Trusted Application rules can be used by the Endpoint to protect the end user computer from many kinds of malware.

In addition, the rules can control file access, such as denying writes to a local cloud folder (DropBox, OneDrive, etc).

Once the Endpoints are installed (more information on that below) the Endpoint Operations page can be used to enable Trusted Application Rule checking to provide protection. It can also be used to tempoarilty disable protection for software upgrades, etc.

File Access Auditing

By itself, the File Sight monitor sees activity on a file server, which includes which users are accessing files, what actions (reading, writing, deleting, etc) they are doing, their IP address, etc. However, once a file arrives on the client's computer, the server-based File Sight monitor can't see what is happening. Is the file being copied to a thumb drive? Opened in Word? Sent via Email? The File Sight Endpoint helps answer those questions.

The File Sight Endpoint is a small agent that gets installed on end-user Windows computers. It uses very little resources and shouldn't be noticed. It has no user interface.

By detecting a file being read from the server by Explorer.exe and then that same filename being written to the local computer, you can be fairly certain that a file copy is taking place. On the other hand, if you find the file was read into a process named Word.exe, and no local saves took place, this would appear to be a user just editing a document.

The File Sight Endpoint will add additional information to file I/O records that are saved by the File Sight Monitor. These extra fields will be in alerts and available in reports.

> 💡
>
> The client and server both need to be Windows 7 / Windows 2008 R2 or newer for the server to know which Endpoint to communicate with. If either is older, an older version of the SMB protocol is used which did not provide the client IP address.

> 💡
>
> The File Sight Endpoint should not be installed on a server where the PA File Sight Central Monitoring Service, or a Satellite Monitoring Service are installed.

Normal Client	**Client with the File Sight Endpoint***
○ File Name ○ File Name	

○ Time	○ Time
○ File Operation	○ File Operation
○ User Account	○ User Account
○ User IP Address[*]	○ User IP Address[*]
○ User Computer[*]	○ User Computer[*]
○ Server Process	○ Server Process
	○ Client Process (Explorer.exe, Word.exe, etc)
	○ Logged In User (usually same as User Account above)
	○ List of files written by the Client Process
	○ Probable Copy (meaning the file is probably being copied)

* Requires that the server and client are both Windows 7 / 2008 R2 or newer

The File Sight Endpoint performs the following functions:

○ Connects to the PA File Sight central service, or to a Satellite service

○ Watches files that area accessed from the network, and notes the process that accesses them

○ Notes which other files are written by that process

○ If a file is read from the network, and then written to disk, it is tagged as a *probable copy*

We use the term "probable copy" because the actual file contents are not compared between all files read and all files written. This would have a large performance impact on the client computer. Instead, the File Sight Endpoint notes that a file (Finance.xls for example) is read from the network, and then a file also named Finance.xml is saved to disk by the same process (Explorer.exe for example). This looks very much like a copy.

Configuration

No changes to the File Sight monitor are required. If files are accessed from a computer running the File Sight Endpoint, the extra data will automatically be recorded and added to any alerts that are sent.

The only configuration needed for the File Sight Endpoint is to give a host name/IP address and port for the central service/Satellite that will be used for communication. This is done via the command line.

Only one connection to a central service/Satellite is needed. If the client computer will use files from multiple files servers that are all being watched by PA File Sight, and they are all part of the same Ultra installation, they will communicate amongst themselves to find the File Sight Endpoint if needed.

Installing the File Sight Endpoint

The actual File Sight Endpoint is found at:

C:\Program Files\PA File Sight\Install\pafsendp.exe

The File Sight Endpoint executable program (pafsendp.exe) just needs to be copied to a client computer and run with some command line options to direct it to the server it should connect to. It does not require any additional files. The copy and execution steps can be done using any techniques or infrastructure that you already use, such as executing a script, using a software distribution program, or Microsoft's Group Policy. So the steps are simply:

1. Copy pafsendp.exe to the client computer

2. Run pafsendp.exe with configuration command-line options given below

3. Start the pafsendp service on the client computer

The endpoint supports a few command line options. The command line options are not case sensitive.

-S	Don't show a pop-up when installing or uninstalling the service
-I	Install the endpoint as a service named pafsendp
-U	Uninstall the endpoint as a service
-HOST=*host:port* -HOST2=*host:port* -HOST3=*host:port* -HOST4=*host:port*	Give the hostname or IP address, and port, of the PA File Sight Central Service, or a Satellite that should be connected to. Because Satellites might be unavailable at times, or just for added robustness, additional hostnames can be given which the Endpoint will connect to if the current target host is not available. Example: -HOST=myserver:8000
-LOCK	Set the endpoint service so it cannot be stopped. Unlocking happens via the Console in the Endpoint Operations view.

Installation Examples

Here are links to three examples of how to install the File Sight Endpoint.

- Typical Install Command

- Example Install Script

- Example Group Policy

File Sight Endpoint Status

You can check to see which computers have the File Sight Endpoint installed and running by looking in the Console at Advanced Services > File Sight Endpoints.

If you have some File Sight Endpoints that are not up to the latest version, you can right click the File Sight Endpoint node and choose to have an update command sent to them.
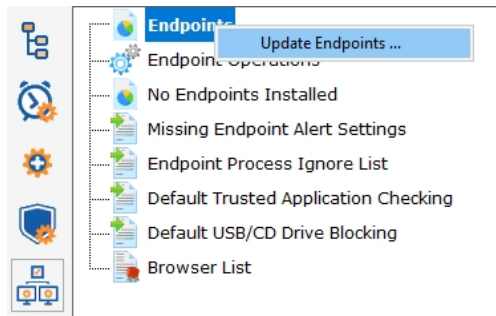
Typical Install Command

Most often you would run pafsendp *on the target computer* with a command such as:

```
pafsendp.exe -s -i -host={central server IP}:{central port}
```

This could be run using any software distribution mechanism you already have in place. If you don't have something in place see the Example Install Script or Example Group Policy below.

A few notes:

○ The File Sight Endpoint uses the same file system driver as PA File Sight to watch file I/O. That means the agent needs to run as an account that has rights to start a driver. A local administrator account or Local System will work.

○ All of the command line operations change registry values that normal user accounts typically don't have access to, so those operations will need to be run with an administrator account.

> 💡
>
> **IMPORTANT**
>
> If you are monitoring servers at multiple sites (separate local networks), be sure the Endpoint is connected to and communicating with a Satellite or the Central Service that is on the same local network as the Endpoint.

Example Install Script

If you don't already have a way to deploy software to workstations, this example installation script could be used to get the File Sight Endpoint installed on an end-user's computer. This example uses Microsoft's PsExec program. It also uses Sleep.exe which is in the same folder as pafsendp.exe.

```
REM Install the File Sight Endpoint service. PsExec will copy
REM pafsendp.exe to the client computer's Windows folder.
REM Run this from the C:\Program Files (x86)\PA File Sight\Install folder
REM so pafsendp.exe can be found by PsExec

psexec \\{target server} -u {username} -p {password} -c -d -h -v
    pafsendp.exe "-s -i
    -host={central service/Satellite IP address:port} -host2={failover     service/second Satellite IP
address:port} -lock"

REM wait just a bit for installation to finish

Sleep.exe 15000
```

```
REM start the remote service

psexec \\{target server} -u {username} -p {password} -s net start pafsendp
```

In the example below, our target client computer is 192.168.7.6. We'll be using an administrator account, with password s3cr3t. The central service is at 192.168.7.22, running on port 8000, with a Satellite at 192.168.10.4 that we'll use as a secondary connection.

```
CD "C:\Program Files (x86)\PA File Sight\Install"

c:\tools\psexec \\192.168.7.6 -u administrator -p s3cr3t -c -d -h -v pafsendp.exe "-s -i -
host=192.168.7.22:8000 -host2=192.168.10.4:8000 -lock"

sleep.exe 15000

c:\tools\psexec \\192.168.7.6 -u administrator -p s3cr3t -s net start pafsendp
```

Example Group Policy

This example will show how to use Group Policy to run a Batch file that will install the File Sight Endpoint on many workstations and then start the Endpoints services.

1. Save the pafsendp.exe file to a shared drive that all workstations will have access to. You will need to use that location in the script.

2. Create a script that will copy the pafsendp.exe file to the workstations, and run the installer, and start the service. Here is an example.

```
@REM Deploys the PA File Sight Endpoints using this script and
@REM Group Policy Object (GPO) to push them to remote clients.

@ECHO OFF

@REM Check to see if the Endpoint has already been installed
SC QUERY | FIND "pafsendp"

@REM If not installed run the following else if installed exit
IF %ERRORLEVEL% EQU 1 (
    @REM ******* Need to change the Shared Location of the executable file *******
    @REM ******* Example \\yourServer\MySharedFolder\pafsendp.exe *******
    COPY "\\server\MySharedFolder\pafsendp.exe" "C:\Windows\"

    @REM ******* Change the Host name and port number for the Endpoints to report to. *******
    START "" "C:\Windows\pafsendp.exe" -s -i -host=192.168.7.4:722 -LOCK

    TIMEOUT 5 > nul
    NET START pafsendp
)

EXIT 0
```

3. Create a new Group Policy Object in Active Directory:

○ **Open Server Manager** using the icon on the desktop taskbar or from the Start screen.

○ In the Tools menu, **select Group Policy Management**.

○ In the Group Policy Management Console (GPMC), expand your Active Directory (AD) forest, domain and **click the Group Policy Objects container**.

- Right-click the Group Policy Objects container and New from the menu.
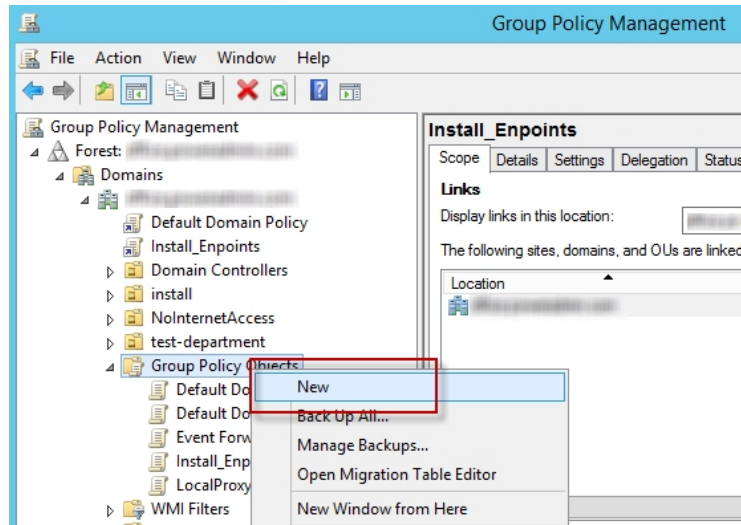
- In the New GPO dialog box, give the new Group Policy Object (GPO) a name and press OK.
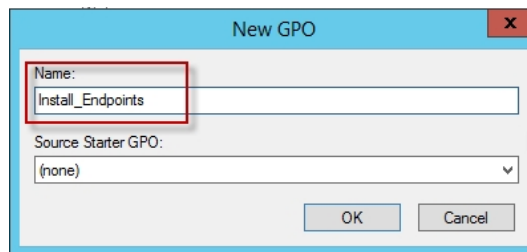
- Now right-click the new GPO in the left pane and select Edit from the menu.
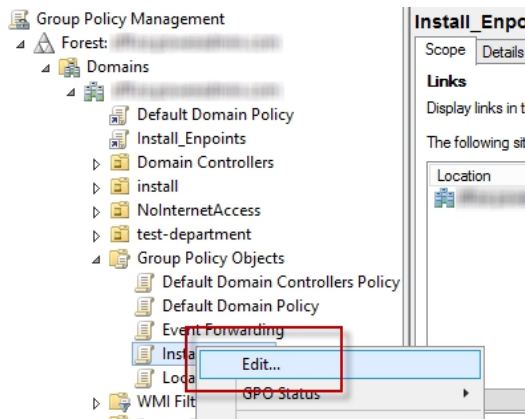
4. Add the startup script settings to the GPO:

- In the left pane of the Group Policy Management Editor window, expand Computer Configuration, Policies, Windows Settings and click Scripts.

- In the right pane, double-click Startup.
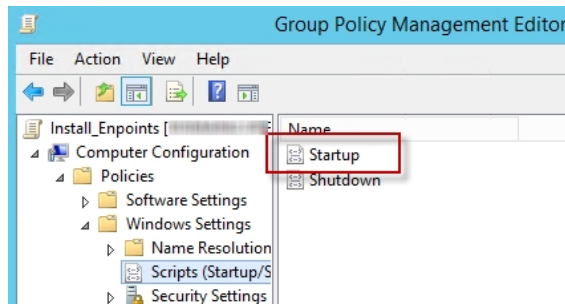
- On the Scripts tab of the Startup Properties dialog, **click the Add button**.

- On the Add a Script menu, **click the Browse** button.

- **Copy and paste your script file into this menu**. Then **select the script** and **click on the Open** button.
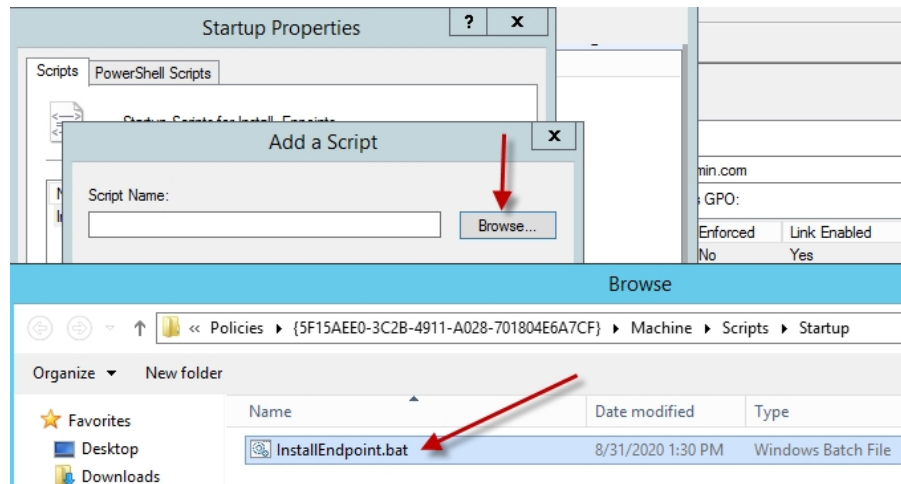
- Click **OK** to continue.

- Close the Group Policy Management Editor window.

  5. Edit the Security Filtering of the new Group Policy Object:

- **Select the new Group Policy Object** on the left.

- On the Scope tab under **Security Filtering**, you will need to **add the accounts you want to use or the workstations** where you want this new script to run. This example will use workstations, but you could select the default Authenticated Users Group or other accounts from the AD. Use the Add, Remove, and Properties buttons to select the AD objects to this filtering.
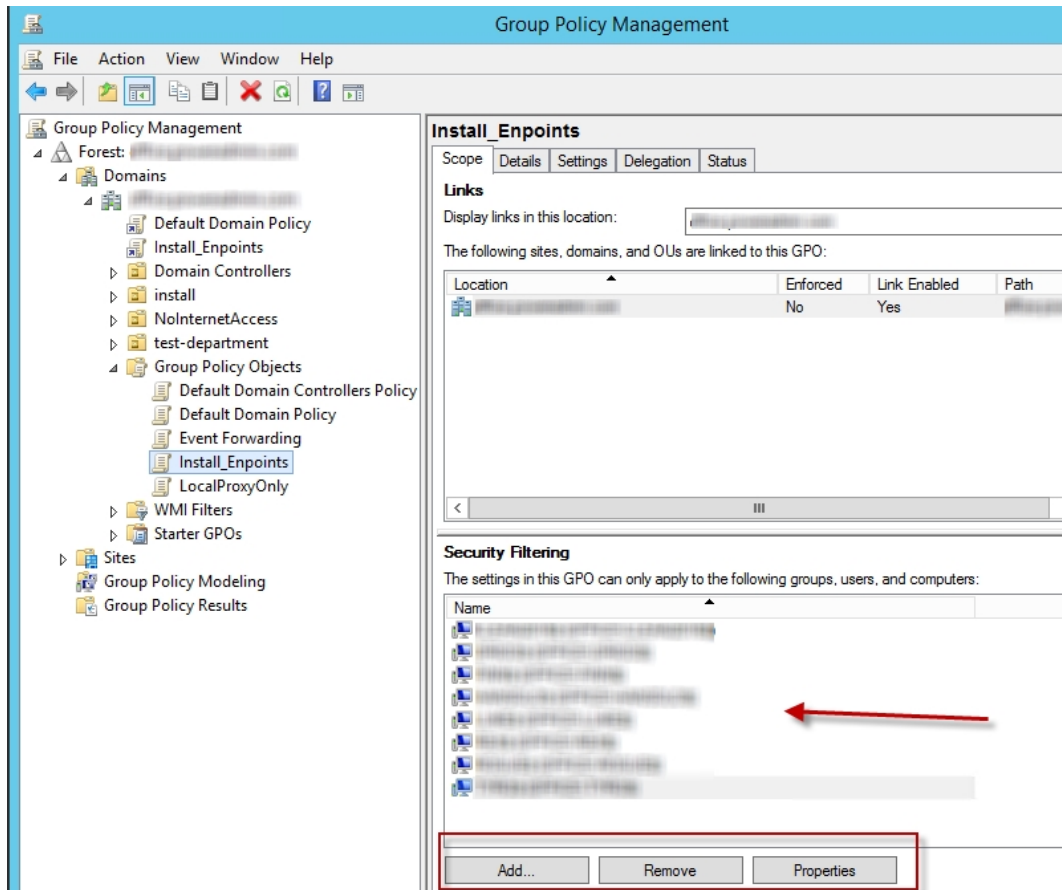
Once you have these steps completed, the new Group Policy will be added to the workstations within one to two hours. When the workstation is rebooted, the script will run and install and start up the PA File Sight Endpoint.

Testing: If you need to test how this group policy works. You can force the workstation to update its Group Policy using the following command on the remote workstation. Open an Elevated Command Prompt. Then type in the command and run it.

```
gpupdate /force
```
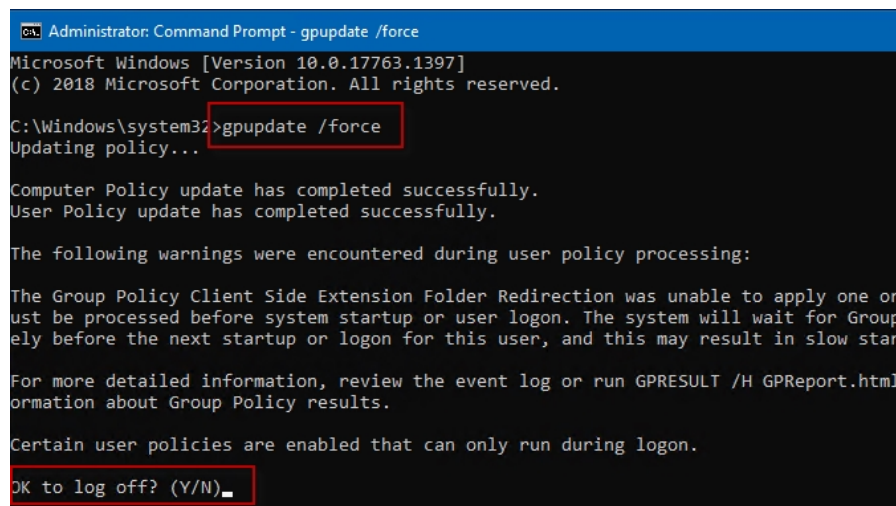
You will be asked to log off to complete the updating of the GPO at this time. The logging off will not run the batch file, you will need to reboot the workstation for this to occur.

File Sight Endpoint Security Alerts

The File Sight Endpoint helps detect files being copied from a server. However, it can't help with this assignment if it isn't running. The Endpoint Alerts help you ensure the Endpoint service is up and running properly.

These settings are accessed in the Endpoint Alert Settings node in the Console.
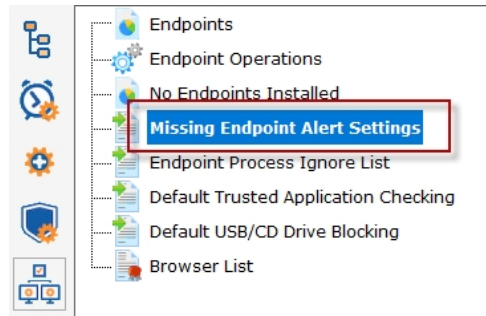
The first decision is how you want to be alerted if an Endpoint is not communicating with the PA File Sight installation. A list of notification actions that you've already defined is shown. Simply check or uncheck any entry that is available to you.
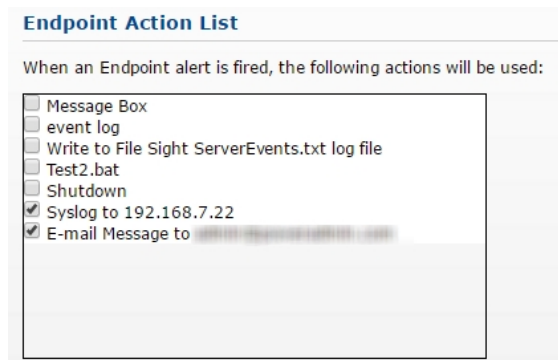
Endpoints don't have specific alert settings initially. So they will use the Global Default Setting that is shown. The third option prevent receiving alerts if an Endpoint isn't communicating because the client computer has been turned off.
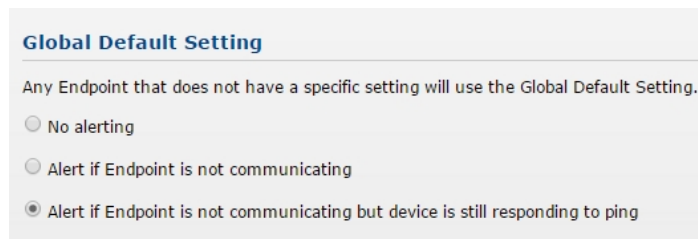
To specify different settings for specific Endpoints, use the Endpoint Operations page.

72

File Sight Endpoint Operations

Endpoint Selection

The Endpoint Operations page is designed to let you quickly apply configuration changes to many Endpoints at once. The key to this is Endpoint Information filter box at the top. Using this you can filter on many different fields (hostname, ip address, username, software version, etc) on the Endpoint. In the example below, "83.5" was entered, and any Endpoint that has that in the name, IP address or other information is shown. In this case, the filter found a few Endpoints that contain that in their IP address.
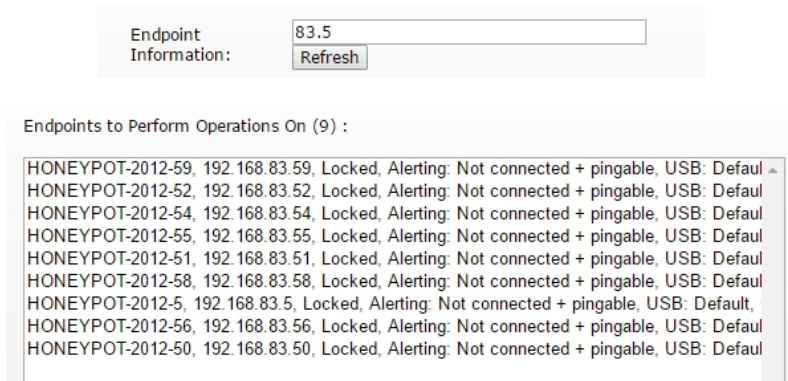
The number of selected Endpoints is shown in parenthesis (9 in the example above).

There are also some short-cut links that let you quickly filter on additional settings and configuration data.

Making Changes

Once the target set of Endpoints has been selected, there are a number of different operations that can be performed by using the options on the right side of the selected Endpoint list.

Endpoint Service Locking

When an Endpoint Service is locked, it cannot be stopped from the Windows Service Control Manager (services.msc) or the net stop command. This prevents end-users from preventing file copy tracking.

Software Updates

This is a simple way to tell Endpoints to update to the same software version as the Central Monitoring Service or Satellite that the Endpoint is connected to. Note that there is a shortcut filter "Running older versions" to easily select those Endpoints that need to be updated.

Endpoint Security Alerts

The Endpoint Alerts page lets you set the Global Default alert setting. This option lets you set a specific alert setting to the filtered list of Endpoints. You can change them to use the Global Default, or to a specific alert setting. Please see the Endpoint Alert settings page for more information.

USB Drive Blocking

USB Drive Blocking lets you optionally block external USB drives from computers where the Endpoint is installed and running. The options are to only allow white listed external drives (that are defined on the USB/CD Drive Blocking page) and block everything else, block everything, or to block nothing.

CD/DVD Drive Blocking

This option is very similar to the USB Drive Blocking option, except it operates on CDs/DVDs that are inserted into the Endpoint computer. The white listed discs can be specified on the same USB/CD Drive Blocking page as above.

Endpoint Host Lists

This option will allow you to change where the Endpoints (listed on the left) will report back to, including upto 3 backup services. You could change them to report to a satellite and then to the central service as a backup, or any combination you need. Once you enter the hostname or IP address with the port number select the Update button to push the changes to the Endpoints.

Trusted Application Checking

A variety of Trusted Application settings can be set on the Endpoints. When the Update Trusted App Settings Above button is pressed, the three shown settings (Enable/Disable, Test/Blocking Mode AND Alert Settings) will all be sent to the selected Endpoints.

Request Trusted Publishers Scan

Clicking this button will request that the selected Endpoints scan all .exe and .dll files on the system and collect the digital signatures from each, and then merge them into the Trusted Publishers list. This can take a while to complete.

Pause Trusted Application Checking

Clicking this button will send a command to the selected Endpoints to pause all Trusted Application checks for 15 minutes. This is useful when temporary unsigned files need to run, as is often the case when software is installed. Each click of the button will restart the 15 minute pause time.

USB/CD Drive Blocking

File Sight Endpoints can be told to automatically eject any USB drive or CDs/DVDs that are not on the Global Media White List.

If an Endpoint doesn't have a setting, it will use the Global Default Setting as shown below.

Global Default Setting

Any Endpoint that does not have a specific setting will use the Global Default Setting.

USB Drive Blocking

◯ Block external drives that aren't on the Global Media White List

◉ Do not block any external drives

CD/DVD Drive Blocking

◯ Block CDs/DVDs that aren't on the Global Media White List

◉ Do not block any CDs/DVDs

To change the setting for individual Endpoints, use the Endpoint Operations page.

Global Media White List

If blocking is to be done, the USB drives/CDs/DVDs are checked against the Global Media White List. This is a list of Volume Serial Numbers from drives/discs that are allowed.

Volume Serial Numbers for drives can most easily be seen from a command prompt with the `dir` or `vol` commands.

```
I:\>dir
Volume in drive I is HD GDU3
Volume Serial Number is D265-ABAD
```

```
L:\>vol
Volume in drive L is USB DISK
Volume Serial Number is 621F-2A19
```

Enter the Volume Serial Number in the Global Media White List. Since that number doesn't help identify the drive/disc, you can add a comment after it with the # symbol.

Global Media White List

Enter Volume Serial Numbers for drives/devices that will be allowed on Endpoint protected systems.
You can give comments following the ID by placing a # and then the comment.

Allowed Volume Serial Numbers

```
D265-ABAD # Marketing's pass-around assets USB drive
621f-2a19 # IT's DBAN boot DVD
```

Update Global Media White List

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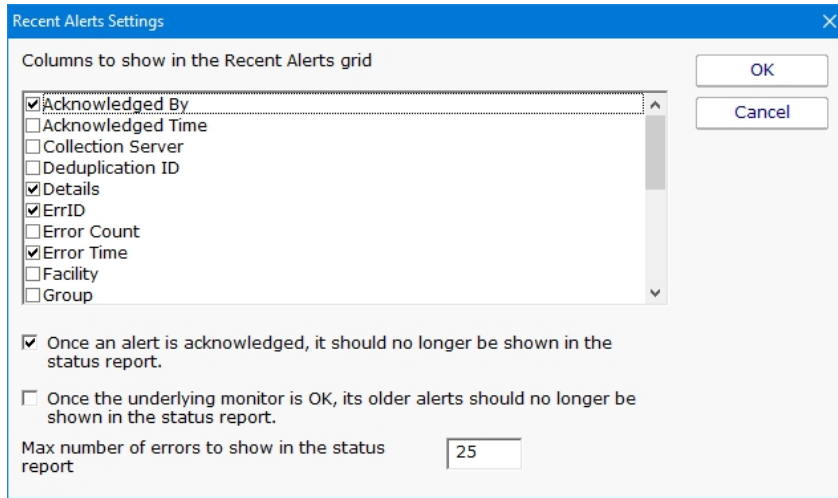
Additional options in this dialog control what is displayed in the Recent Errors section at the bottom of the server status report

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.
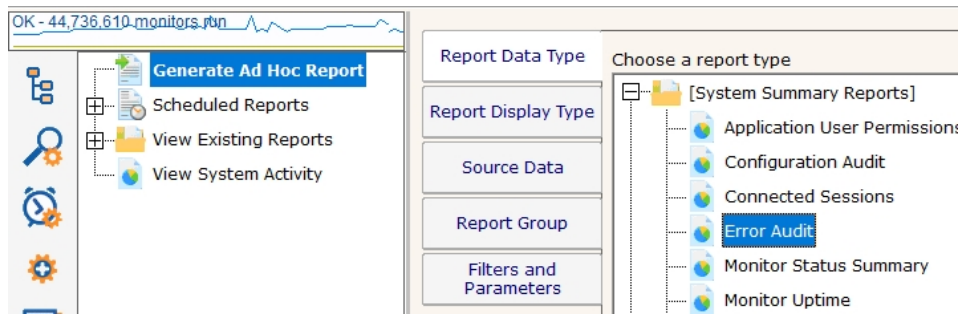
Once you've selected the report, go to the Filters and Parameters tab. This is where you specify exactly what you want to look at. There are a variety of different ways to filter the errors that you want to see. If your primary responsibility is disk space, just look at the Disk Space monitors under 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.
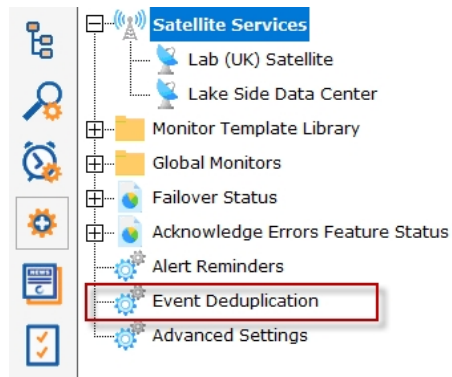
Here you can select between the default Simple event deduplication (which doesn't do very much deduplication), or advanced event deduplication. Advanced Event Deduplication is what this page will describe further.

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).

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	*$Item(x)$* - Unused
Scheduler	*$State(x)$* - OK or PROBLEM
Drive	*$CurrentValue(x)$* - Always set to 'LOADED'
Sight	*$Item(x)$* - Drive Letter
	$ItemType(x)$ - CDROM or DRIVE
	$State(x)$ - OK or PROBLEM
Dynamic	*$CurrentValue(x)$* - "ADDED" or "REMOVED"
Server	*$Item(x)$* - IP address of the computer/device
List	*$ItemType(x)$* - Constant value of "DEVICE"
	$LimitValue(x)$ - DNS name if it can be determined
	$State(x)$ - OK or PROBLEM
File Sight	*$CurrentValue(x)$* - Type of change that occurred. Possible values: 'Created', 'Wrote', 'Read', 'Deleted', 'Moved', 'Renamed', 'Audit
Monitor	Changed', 'Permissions Changed', 'Owner Changed', 'Group Changed', 'Failed to Create', 'Failed to Write', 'Failed to Read', 'Failed to Delete', 'Failed to Move', 'Failed to Rename', 'Failed to Change Audit', 'Failed to Change Permissions', 'Failed to Change Owner', 'Failed to Change Group' 'OVERLIMIT_READ' 'OVERLIMIT_WRITE' 'OVERLIMIT_DELETE' 'OVERLIMIT_RENAME'
	$Extra1(x)$ - Name of the user that triggered the alert
	$Extra2(x)$ - Name of the application (if available) used to make the change, or empty if a User Activity Alert
	$Item(x)$ - File or directory path that was accessed, or the User that is being alerted on for User Activity Alerts
	$ItemType(x)$ - Constant value always equal to 'File', 'Directory' or 'User'
	$LimitValue(x)$ - The IP address of the requesting user, or N/A if it cannot be determined
	$State(x)$ - OK or PROBLEM
Inventory	*$CurrentValue(x)$* - Not Set
Collector	*$Item(x)$* - Not Set
	$ItemType(x)$ - Not Set
	$LimitValue(x)$ - Not Set
	$State(x)$ - OK or PROBLEM

External API

PA File Sight 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\PAFileSight, 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
Server/Device Commands
Monitor Commands
Action Commands
Miscellaneous Commands

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
```

```
: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.

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 File Sight 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 File Sight\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 File Sight\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 File Sight\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\PAFileSight\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 File Sight\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 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 File Sight stores a variety of files under the product directory. This will explain what and where they are.

C:\Program Files\PA File Sight
    Product executable and DLL files
C:\Program Files\PA File Sight\CA
    Self-signed SSL certificate files
C:\Program Files\PA File Sight\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 <u>not</u> contain password information.
C:\Program Files\PA File Sight\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 File Sight\Install
    The PA File Sight 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 File Sight\Logs
    Default location for internal product log files. This can be changed in Global Settings.
C:\Program Files\PA File Sight\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 File Sight\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 File Sight\Config
C:\Program Files\PA File Sight\Databases
C:\Program Files\PA File Sight\Logs
C:\Program Files\PA File Sight\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 File Sight 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 File Sight configuration data to a XML formatted file. Importing is loading the PA File Sight XML file in and restoring the configuration.

Exporting Complete Configuration

To get started, select the following menu setting:
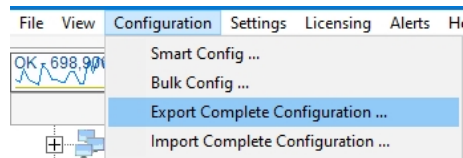
The next dialog that you will see will ask you if you would like to export any server passwords that were entered previously:
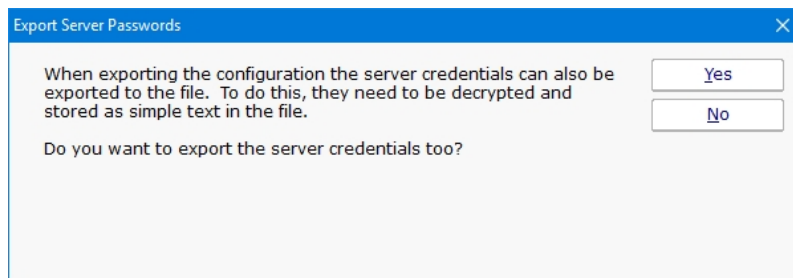
The credentials will be decrypted and visible as plain text in the output file, so you may wish to answer "No" to this prompt.

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 File Sight App Configuration.axml`.

Importing Complete Configuration

Importing a saved PA File Sight 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:
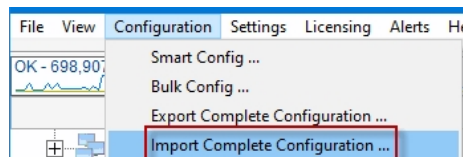
The first prompt that you will see will be a message box indicating that you are about to erase all configured settings in the current instance of PA File Sight and replace them with the contents of the configuration file.
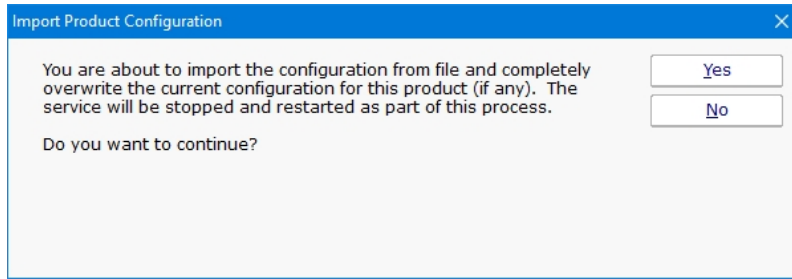
If you answered "Yes" to the question above you will see the standard File Open dialog to select a .axml file that you saved to previously.

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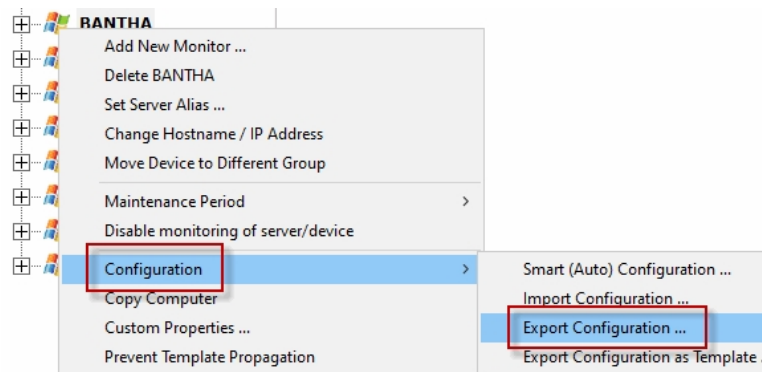
The series of dialog boxes and the options that appear is similar to that shown above for exporting a complete PA File Sight configuration.

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.
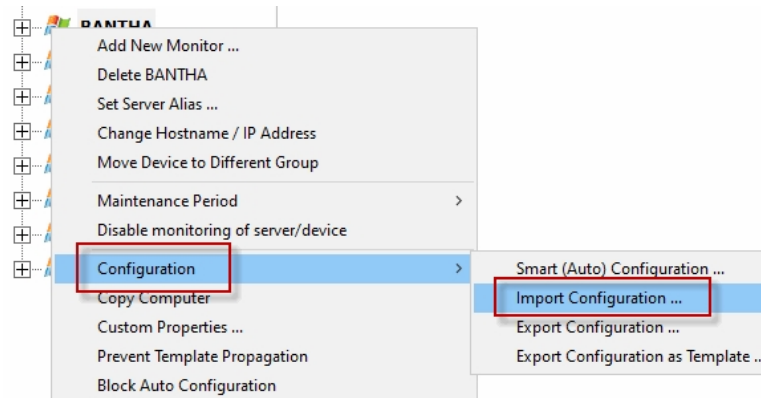
This operation is identical to that of importing the complete configuration of this product as shown above, with the following exception. An import of a server configuration must be applied to an existing computer object that you have already created in PA File Sight.

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.
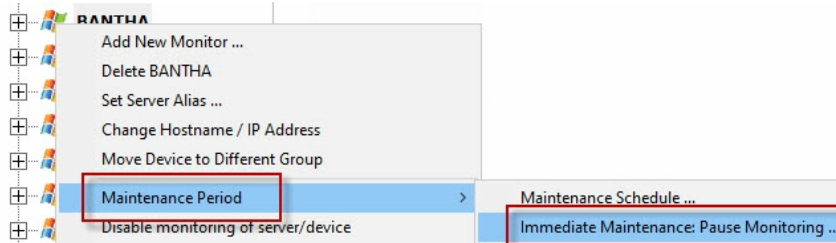
When you enter Maintenance Mode, you specify how long you expect to be working on the server. No further monitoring of the server will take place until that amount of time has past. Then active monitoring of the server begins again automatically.
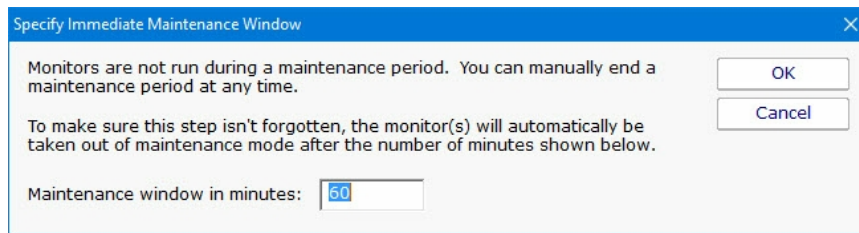
Scheduled Maintenance
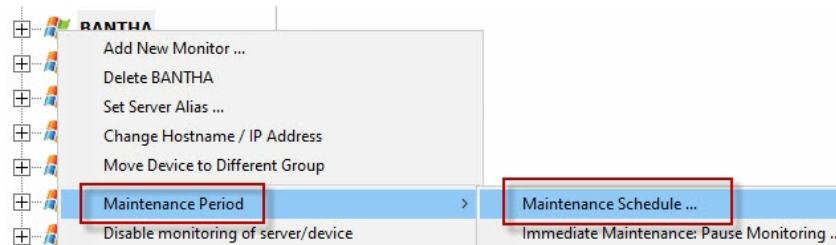
In addition to the manual maintenance mode mentioned above, scheduled maintenance is also available. With this feature you can have the monitoring service automatically place a server into maintenance mode based on your schedule. This is often useful when some normal process (a nightly backup process 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, no monitors 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

Monitor Templates

PA File Sight 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.
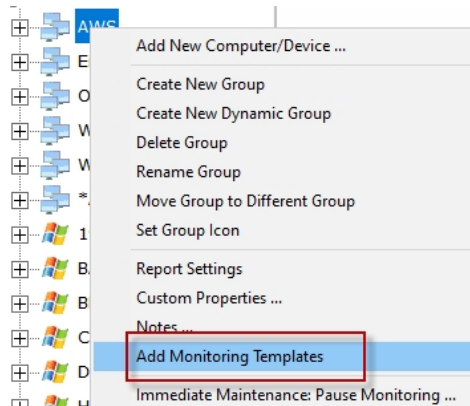
Once that is done, a new Power Templates folder will exist in the group.
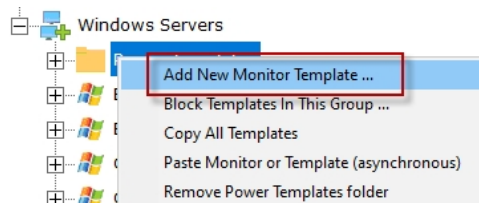
Right-clicking the Power Templates folder reveals a few options:

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.
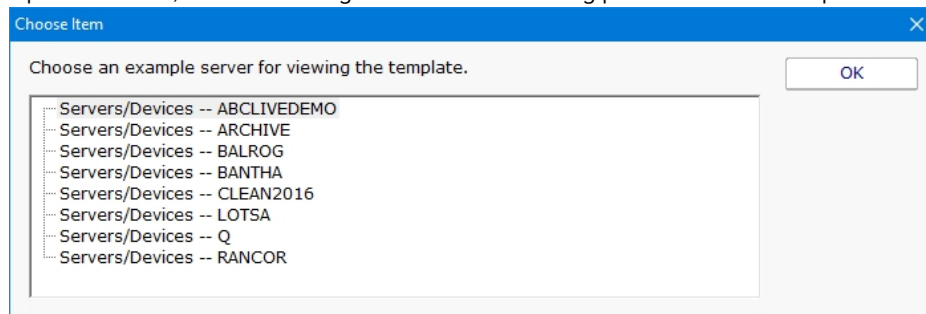
      2. Configuring the monitor normally

Once a template is configured, you'll notice there is one of two symbols before the monitor name. These symbols mean:
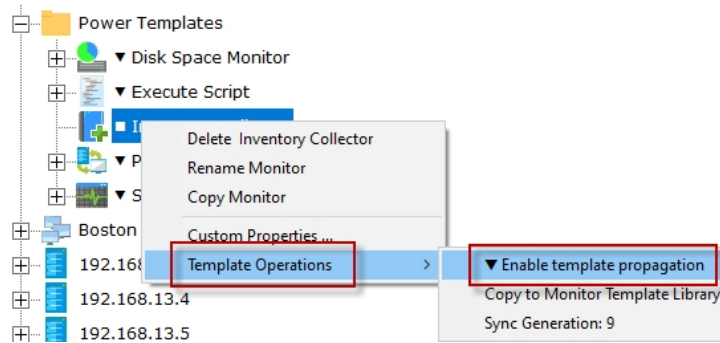
■ - The template is not currently propagating down to servers in this group. This is the default state of a new template.

▼ - 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.

- Satellite Services
  - Lab (UK) Satellite
  - Lake Side Data Center
- **Monitor Template Library**
  - Active Directory Login Monitor
  - Bandwidth Monitor
  - Core - Disk Space Monitor
  - Core - Windows Event Log Errors
  - Core - Windows File Changes
  - Core - Hardware Monitor
  - Core - Anti-Virus Up to Date
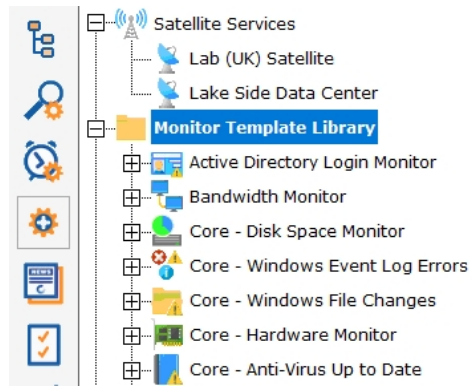
Security Protected Settings

There are many settings for PA File Sight which are available under:

```
HKEY_LOCAL_MACHINE\software\PAFileSight
```

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\PAFileSight\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 File Sight 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.

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.
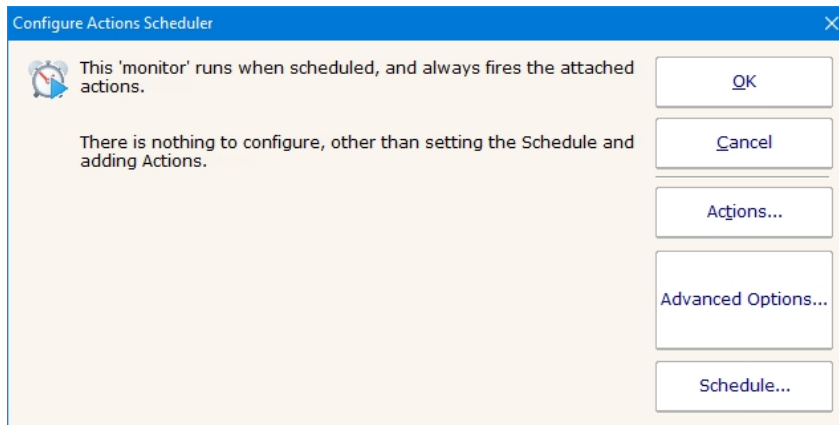
Standard Configuration Options

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

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.
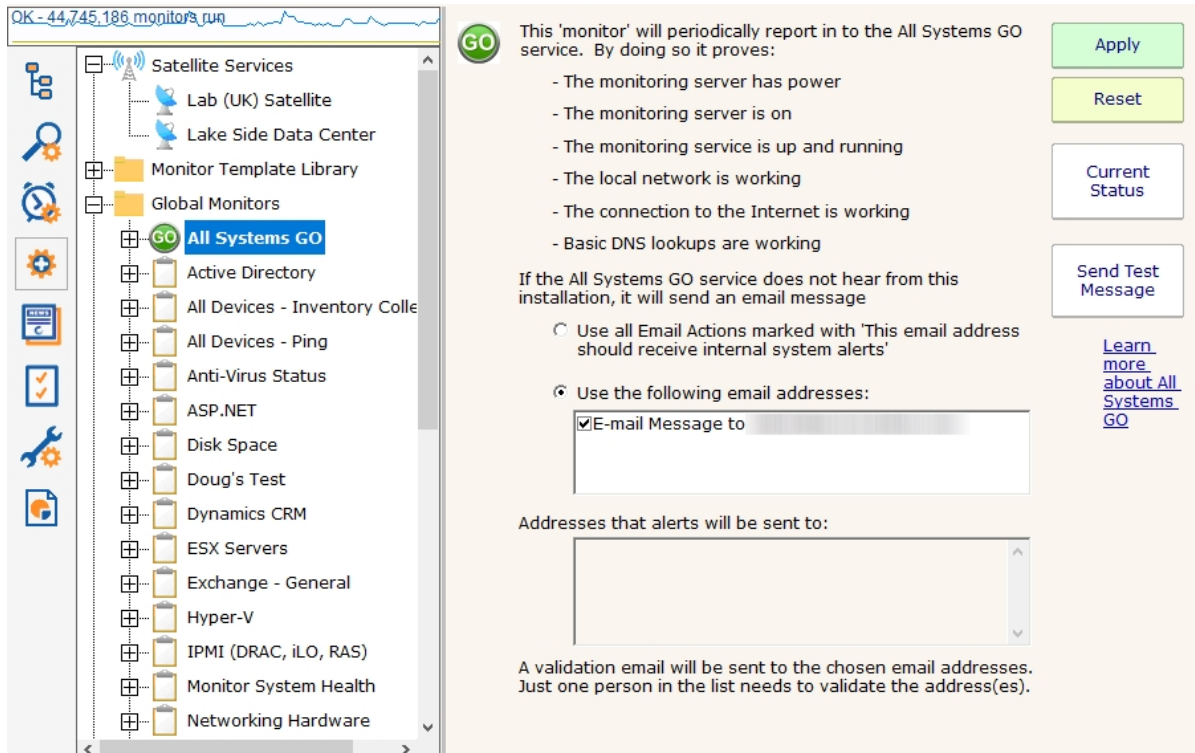
The only thing to configure in the monitor are which email addresses (from email actions) should be emailed if the monitoring service does not check in with the All-Systems-GO service.

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.

Drive Sight

The Drive Sight monitor is a simple monitor with one job: make sure external drives, including USB drives, and/or CD/DVD discs are not added to the system. If a specified disk is added, it is immediately disconnected.
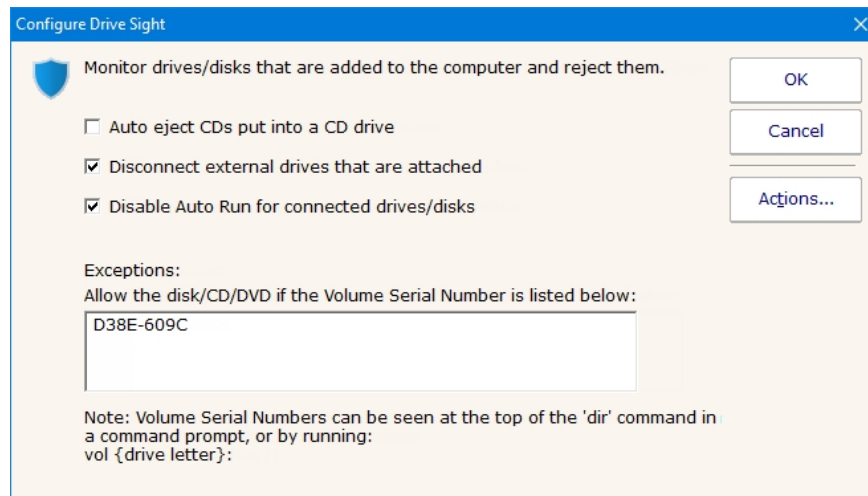
If you have specific drives/disks that you want to make an exception for, get the disk's volume serial number as shown below:

These disks for which an exception has been added will be able to connect and stay connected.

Standard Configuration Options

Like all monitors, this monitor has standard button on the right for Adding Actions. These actions would be fired when the Drive Sight monitor detects a new disk/drive and disconnects it. The action would typically be used to notify you.

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
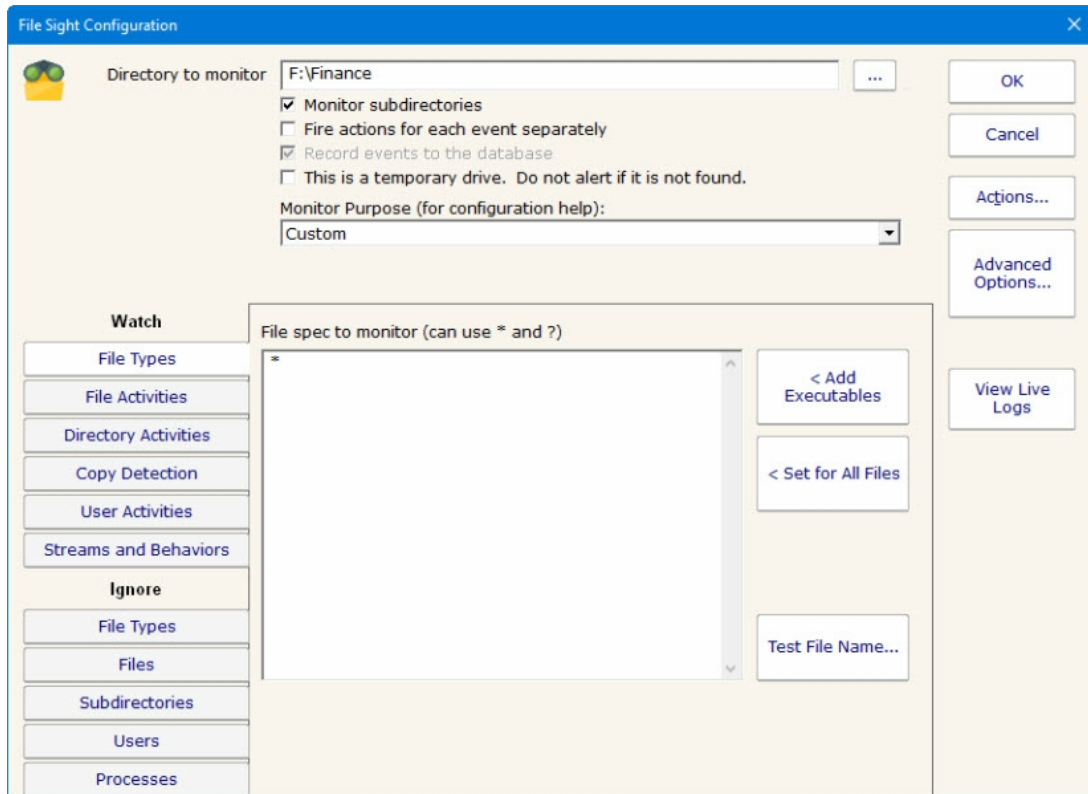
- Grant access to servers in the group

Standard Configuration Options

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

File Sight - File Access Monitor

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

In the dialog below you'll see there are many options. After specifying the root directory to monitor you can specify whether all subdirectories should also be monitored. Database recording is only available in the Ultra product version -- it is not available in the Lite edition.

Standard Configuration Options

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

Supported Reports

A variety of reports are available for PA File Sight, including:

All Changes
Custom Data Set
File Changes
Type of Change
User Activity
User Block List
User Changes
User Read/Write Amount

The **Ultra** version of PA File Sight supports reports which can tell you about file and directory activities that have taken place in the

past while PA File Sight was monitoring the server. You can report on changes to particular files or directories, changes made by a particular user, types of changes (all deletes for example), and any of this during a specific time frame.

💡

Having issues with File Sight? Take a look at the [troubleshooting guide](#).

Optional File Tracker Endpoint

Reports and alerts can contain even more information if the client Windows computer that accesses files on the server is running the [File Sight Endpoint](#).

Top Settings

Monitor Subdirectories

This check box indicates whether just the target folder should be monitored, or all child folders as well.

Fire Actions For Each Event Separately

By default everything that a monitor sees on a single scan will all be reported together. You can have each individual reportable event (each file Delete, Write, etc) reported on separately. This is useful when sending File Sight alerts to a SIEM or other 3rd party application.

Record Events to the Database

This is checked for Ultra installations, and unchecked for Lite installations.

Temporary Drive

Normally if a drive can't be found an alert will be fired. If the drive is removable, or part of a cluster that might not be available sometimes, this setting will prevent the 'drive not found' type of alerts.

Monitor Purpose

The Monitor Purpose allows the monitor to audit its own settings and give configuration hints to ensure the monitor can meet the stated purpose. For example, if you want to be alerted about file copying but don't have any alerts attached, this monitor will highlight that using a red banner. Set to Custom to disable all configuration hints.

Configuration Tabs

Watch: File Types

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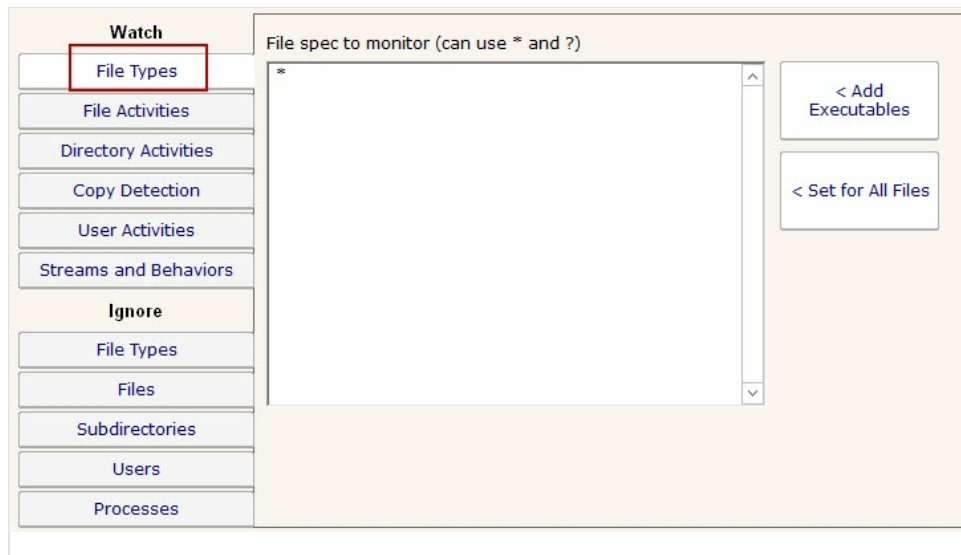
Watch: File Activities

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

The green box on the File Activities panel specifies whether actions should be fired when a matching file I/O activity happens. Sometimes this is unchecked because actions/alerts aren't needed, but the matching activities can still be written to the database.
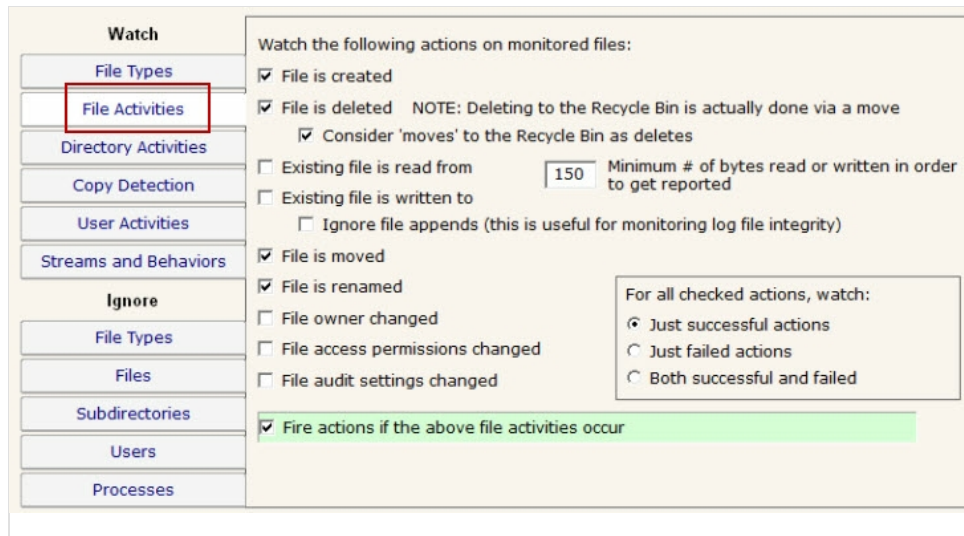
NOTE: Only the Ultra version of the product supports a database and reporting, so the "Fire actions if the above file activities occur" check box is almost always checked for a Lite installation that only does alerting.

Watch: Directory Activities

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

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

Watch: Copy Detection

NOTE: Only the Ultra version of the product supports Endpoints.

File Sight Endpoints allow directly detecting when file copying happens. You can choose to receive alerts when a file copy operation is detected by an Endpoint by checking the box and indicating how many copies have to be seen. If there are clients that are not running the Endpoint, you can indicate you want to be alerted after they read X number of files in some amount of time. Note that reads don't necessarily indicate copies, but without the Endpoint, the server has no way of knowing where the read file ends up.
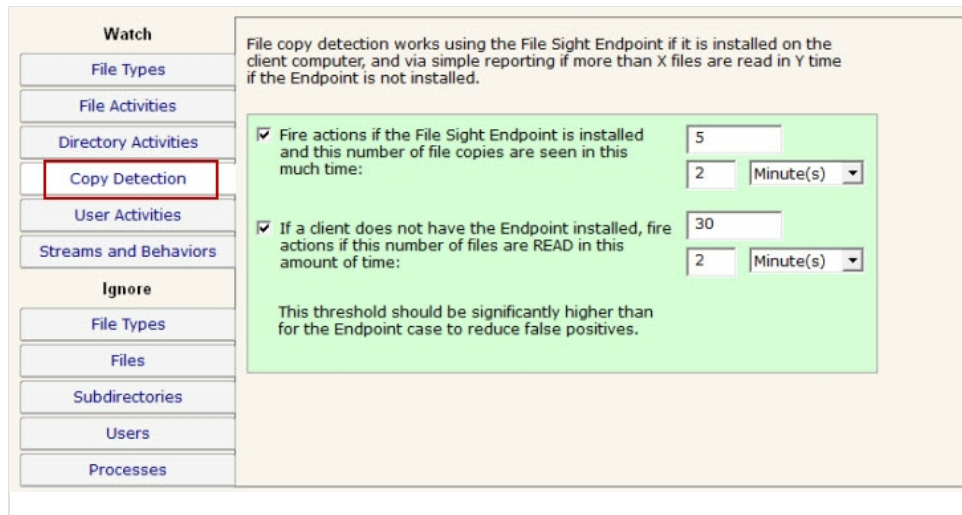
Watch: User Activities

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

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

When one of the conditions is met, the fired alerts will list the files that caused the condition to be triggered.

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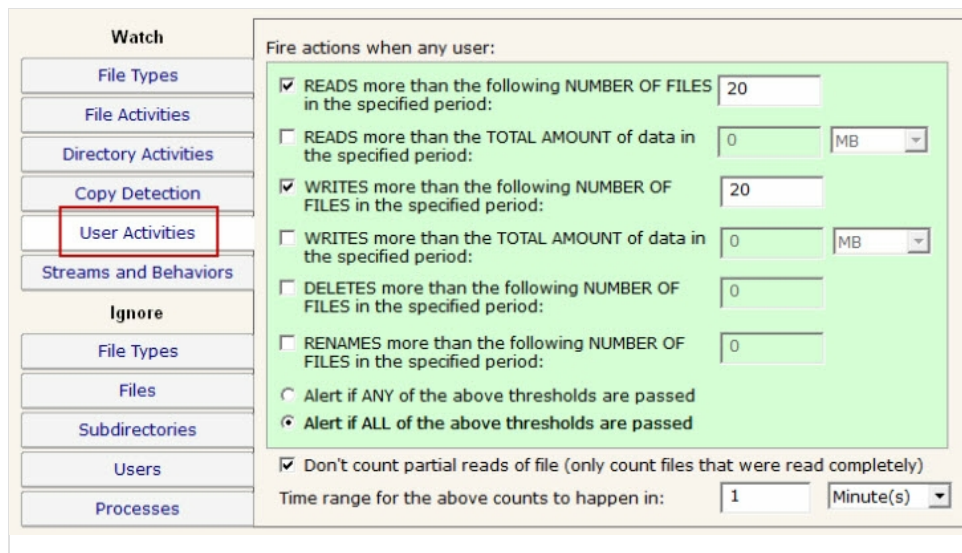
Watch: Streams and Behaviors

This panel lets you specify how to handle <u>file streams</u> that encountered, as well as whether File Sight should try and interpret typical <u>application behaviors</u>.
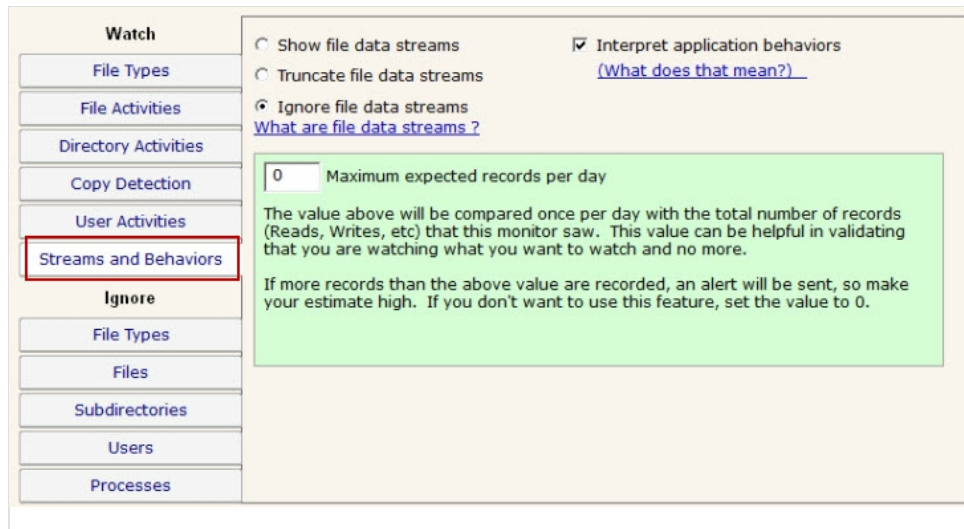
The "Maximum expected records per day" option is really just to help you verify that you are collecting roughly the number of file activity records that you expect to be recording.

Ignore: File Types

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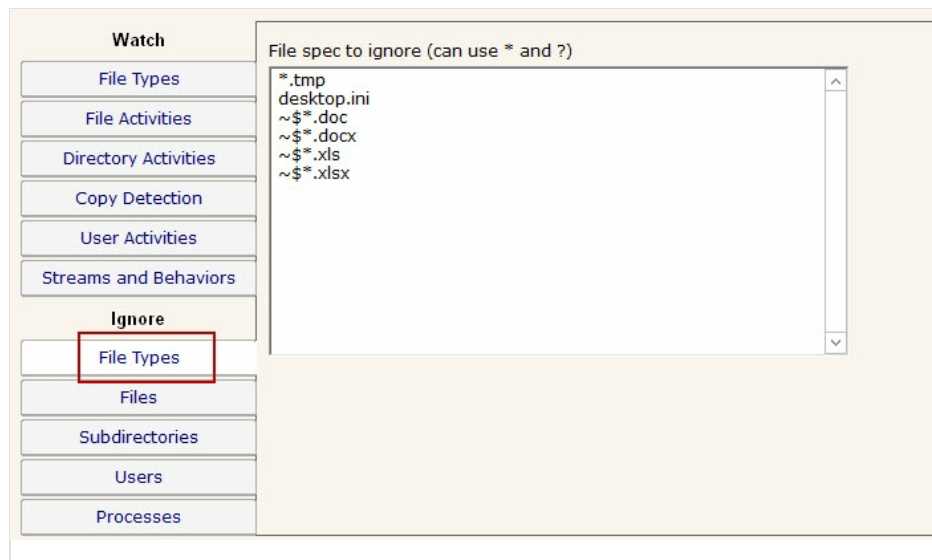
Ignore: Files

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

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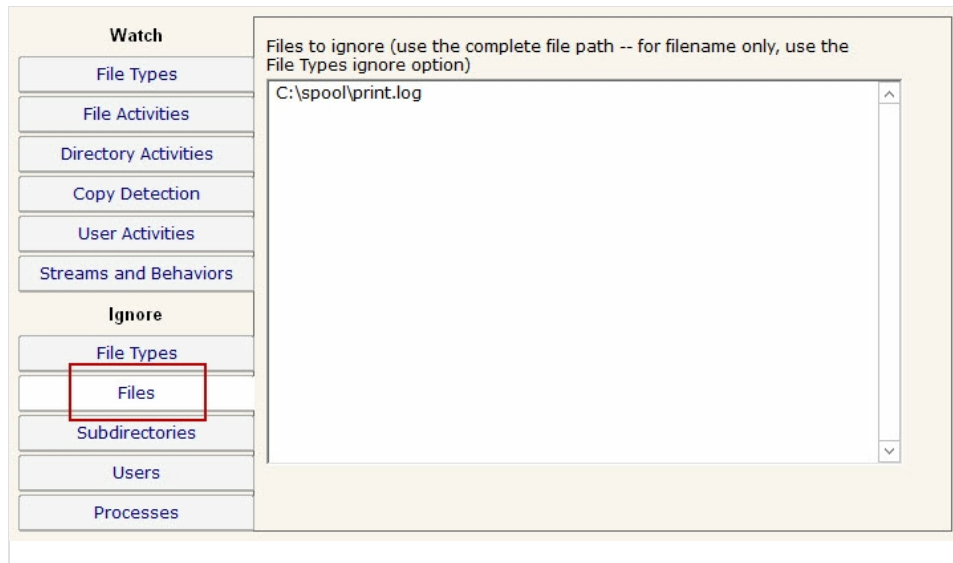
Ignore: Subdirectories

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

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

Ignore: Users

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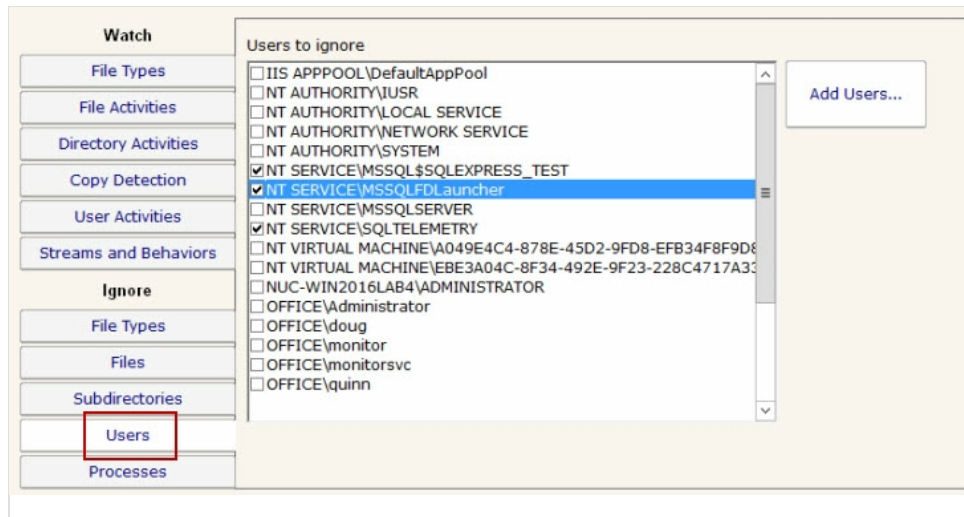
Ignore: Processes

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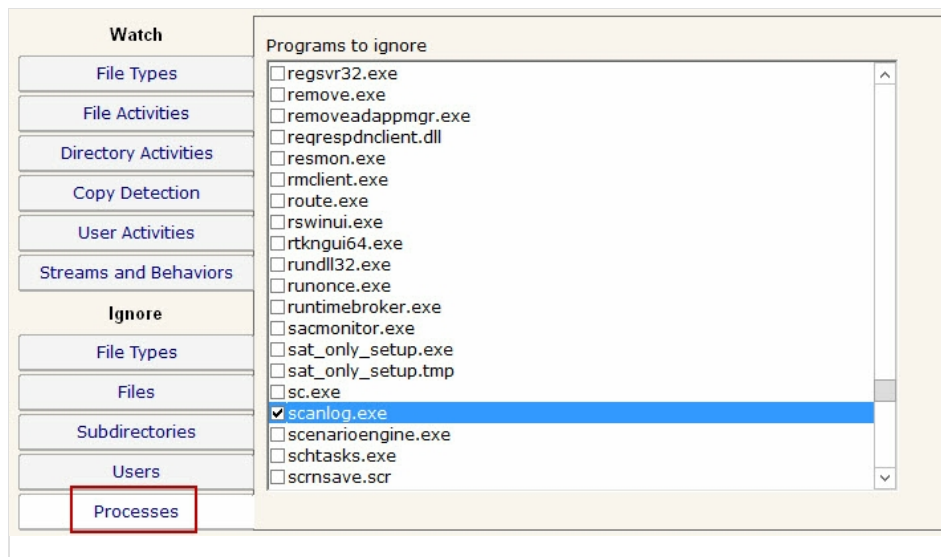
Reported Values

When a file or directory access takes place that meets the filter criteria described above, PA File Sight can alert on that event. By default, it uses the following format:

Op: Created
File: C:\example\file.txt
User: domain\dave
Source: dave-pc [192.168.10.12]
App: explorer.exe

This format is configurable via the FS_LineFormat registry value.

The Op line (short for Operation) can be one of the following list of values:

Operation	Notes
Created	A new file that didn't exist before exists now

Deleted	The file was deleted. Note: The Save routine for some applications (Microsoft Office for example) happens by saving to a temporary file, deleting the original file, and then renaming the temporary to the original file name. File Sight sees this and properly reports the file deletion. If you don't want this behavior, see the Interpret Application Behavior option.
Read	Some or all of an existing file was read from disk. Note that clicking a file in Explorer often causes a part of the file to be read (author information, icon is extracted, etc). In addition, clicking a file might cause an anti-virus app to scan the file. PA File Sigth sees and can report on all of this. To avoid some Read reports, you can indicate that at least 200 bytes of the file must be read (that would filter out icon extraction by Explorer).
Renamed	A files was renamed, or moved to the same drive (the operating system calls moves 'renames')
Wrote	An existing file was written to (ie changed)
Audit Changed	Audit settings on the file were changed
Permissions Changed	File access permissions on the file were changed
Owner Changed	The file's owner was changed
Group Changed	This is not usually seen, but is listed in this table for completeness' sake
Failed to Create	
Failed to Delete	
Failed to Read	
Failed to Rename	
Failed to Write	
Failed to Change Audit	
Failed to Change Permissions	
Failed to Change Owner	
Failed to Change Group	

The values above can be translated into a local language.

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)
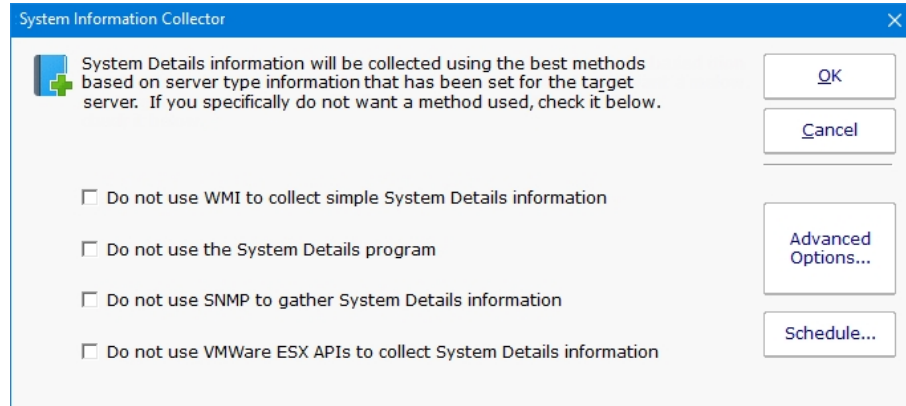
System Details and Inventory Probe

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.

Trusted Applications Monitor

The Trusted Applications Monitor enabled the applicationn whitelisting/trusted application feature for the given server. Read more about:

- Concepts

- Trusted Lists

- Statements

- Rules

- Getting Started

- Day to Day Operations

When the monitor is enabled, the Trusted Application functionality will be active on the server. Disable or delete the monitor to stop the Trusted Application functionality. There is an approximate 30 second delay from disabling/deleting the monitor until the Trusted Application functionality is completely disabled.

The monitor allows specifying **Test Mode (where file activity is not actually blocked) or Block Mode which is the production setting.**

Alerting for blocked files can also be enabled.
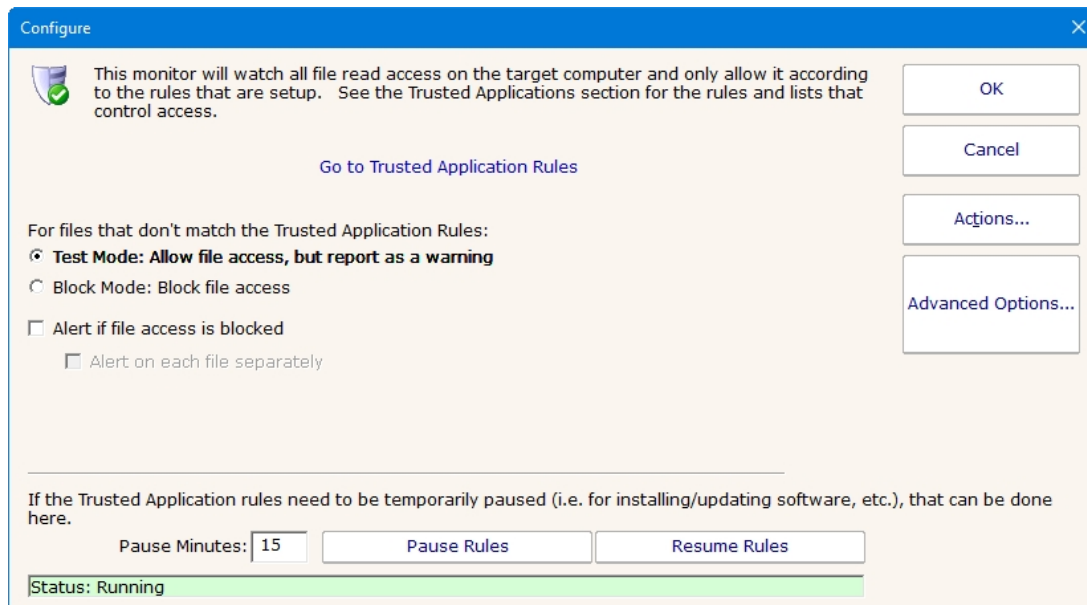
If you need to temporarily disable the monitoring and checking of a Trusted Application monitor, click the Pause Rules button. This is useful in situations where new software needs to be installed (sometimes installer components are not signed).

> 💡
>
> If you need to temporarily disable Trusted Applications on an Endpoint, go to Endpoint Services > Endpoint Operations. There you can filter the Endpoint list to just those you want to disable the checking on, and then click the "Pause Trusted Application Checking" button on the right. This will disable checking for 15 minutes.

Standard Configuration Options

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

Supported Reports

When this monitor runs, it will record any files that are blocked for which reports can be run. There is also an interactive Trusted Applications Warning viewer that can be used to help fine tune the system.

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.
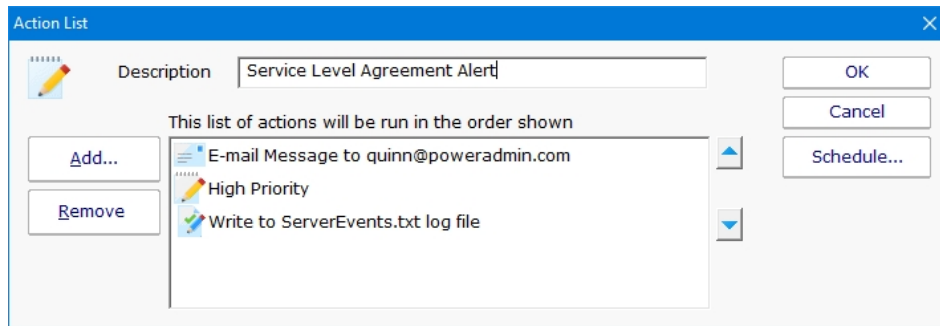
For an example monitor below, the action list shown above is assigned to this monitor and many others like it. When any of these monitors detects a problem, they will run all of the actions defined in the "Service Level Agreement Alert" action list.

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'.

Add to Blocked Users List Action

Part of the protection aspect of PA File Sight is the Blocked Users List. Any account added to the Blocked Users List will not be able to read, write or delete files on any drive that is monitored by the PA File Sight installation (including drives monitored by Satellite Monitoring Services).

This action can only be added to a File Sight monitor. It is not supported with any other monitor type.

This action can automatically add accounts to the Blocked Users List when a monitor triggers on some particular action. This might be useful in the following scenarios:

User Deletes X files in Y time*
    If a user is deleting many files, it might be malware, or a user trying to cause damage. The user could automatically be blocked from all monitored servers when this is triggered.
User Reads X files in Y time*
    This might happen if a user is copying files, or a malware out break is reading files in order to encrypt them.
Honeypot file is touched
    You could setup a special directory that users shouldn't access. It would act as a honeypot, and any account that accesses files in that folder could be automatically blocked.

These options are available in the Ultra edition of PA File Sight.

> 💡
>
> This action is very powerful, and caution should be taken when using it so valid accounts are not blocked.

Configuration

The action is very easy to configure: you just specify how long an account should be blocked when the monitor it is attached to fires this action.

Any time a File Sight monitor has one of these actions attached, it will show a red warning banner reminding you that any account that the monitor triggers on will have file access blocked.
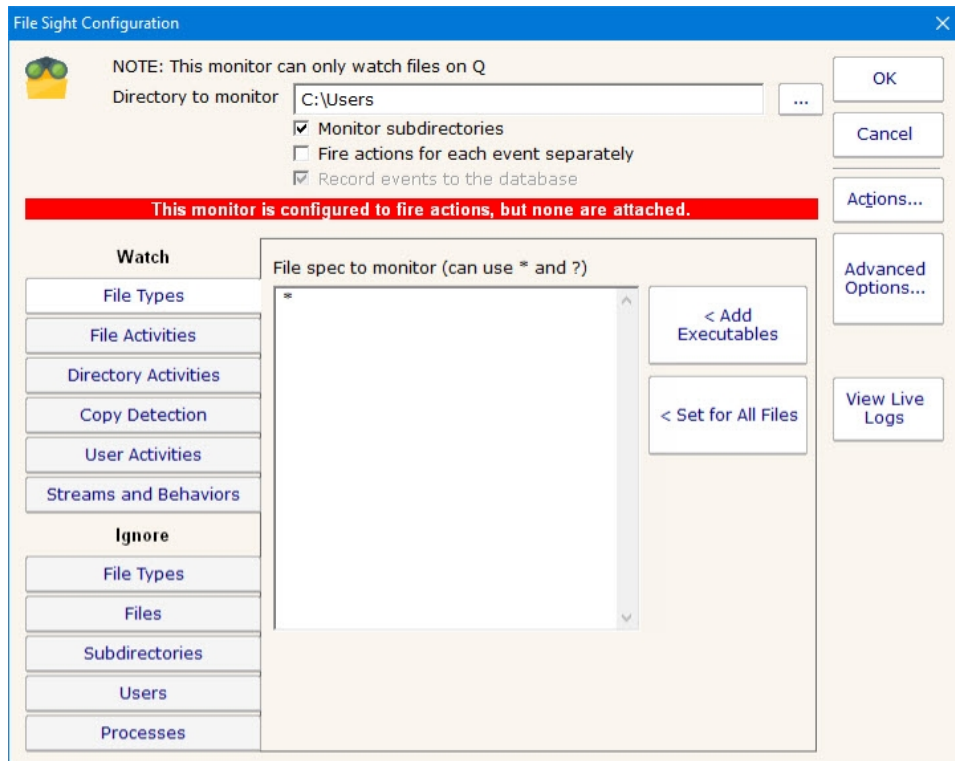
Testing

Because blocking access to the wrong accounts could cause trouble, there is always a TESTING version of the Add to Blocked Users List action. This action does the exact same thing as the normal action, except it adds "TEST" to the wrong of all accounts on the blocked list. Because of this, they are not actually blocked.
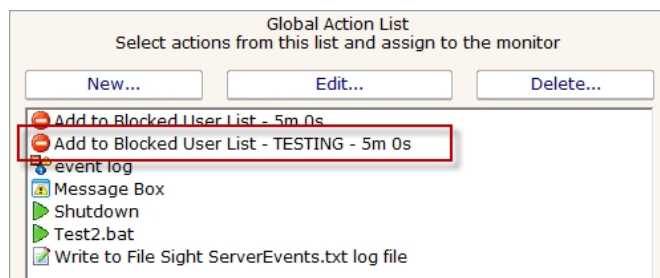
It is recommended to use this TESTING action while you are getting your monitor configured, and let it run that way for a little while. When you are convinced that no false positives are occurring, remove the TESTING action from the monitor and attach the real action.

Precautions

It is expected that having an account on the Blocked Users List should be a rare event. Therefore, when a user is added to the list:

- A System Alert is fired so administrators know who was added

- A red banner will be shown in the Console and at the top of group-level reports

  Adding this action to a File Sight monitor without also adding an Email Action will cause a warning.

The List

The bottom half of the action is a convenient place to see the current Blocked List and the White List of unblockable accounts. It's also where you can add and remove users from the lists.

[Read more about the Blocked Users List here](#).

Call URL Action

This action will call a URL that you specify, possibly passing additional information about the alert via GET or POST variables.
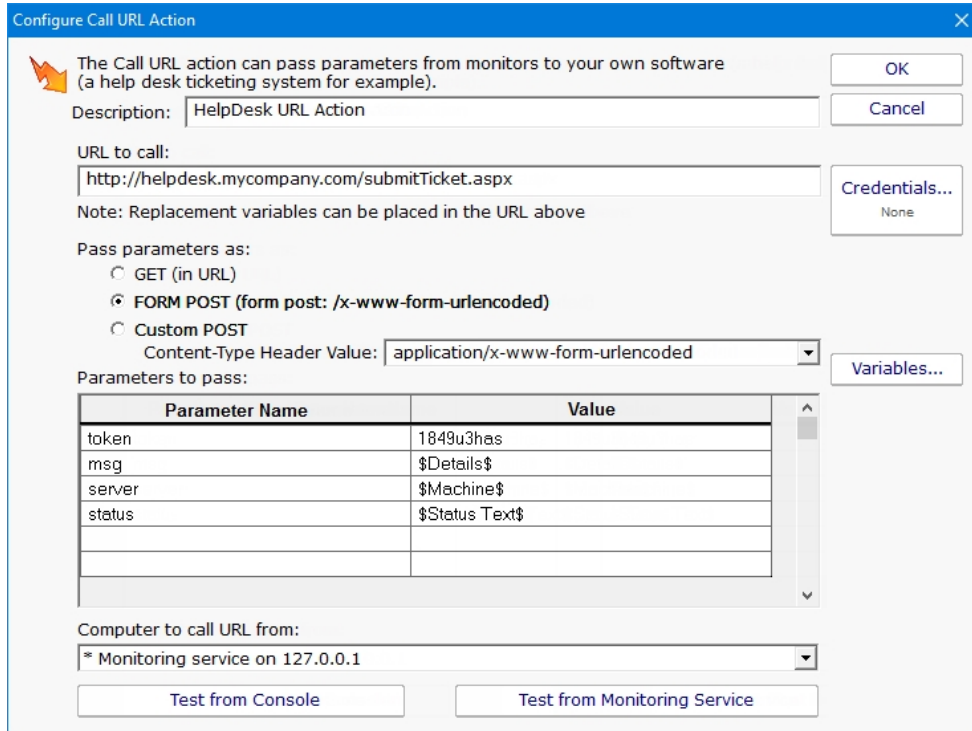
Specify the URL to call, and whether it should be called with GET (with parameters added to the URL), or with POST (with parameters being form posted).

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.
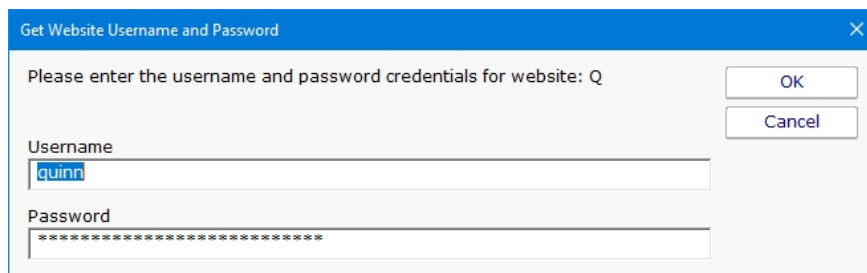
Click on the Credentials button to enter the username and password credentials for the website.

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.
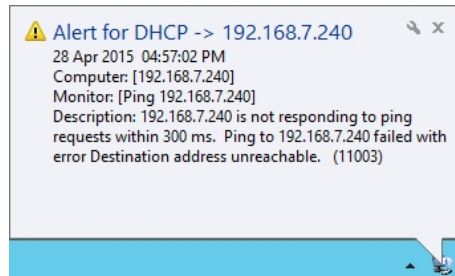

Installation

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 File Sight\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.
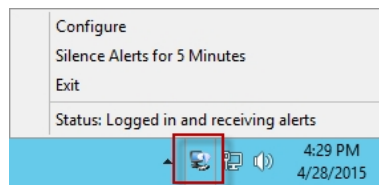
Specify the Central Monitoring Server's hostname/IP address and the port it uses for HTTPS communication. This can be determined by looking in the Console at the HTTP Settings.

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.
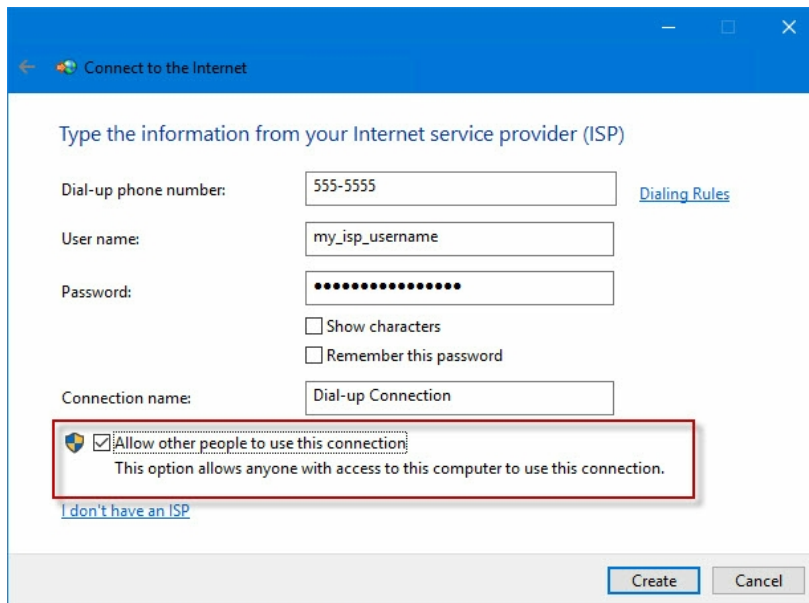
Dial-up Connection Action

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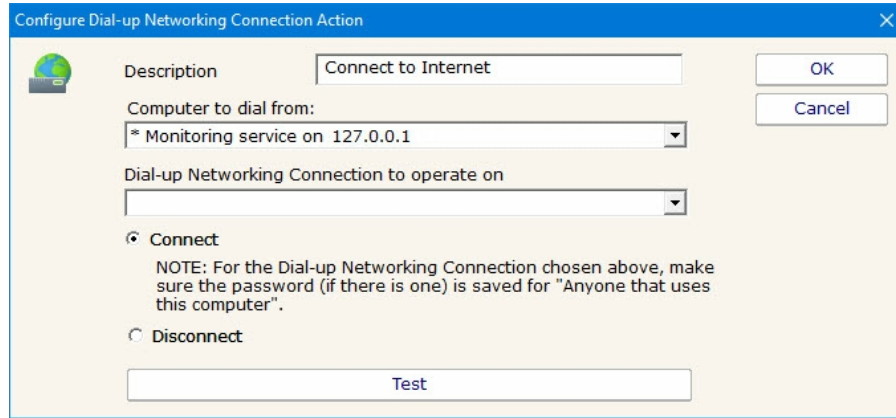
Previous to configuring this action, you need to manually create and configure the Dial-up Networking Connection in Windows. This typically involves specifying a phone number to dial, a modem to use, and a username and password to send to the ISP.

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.
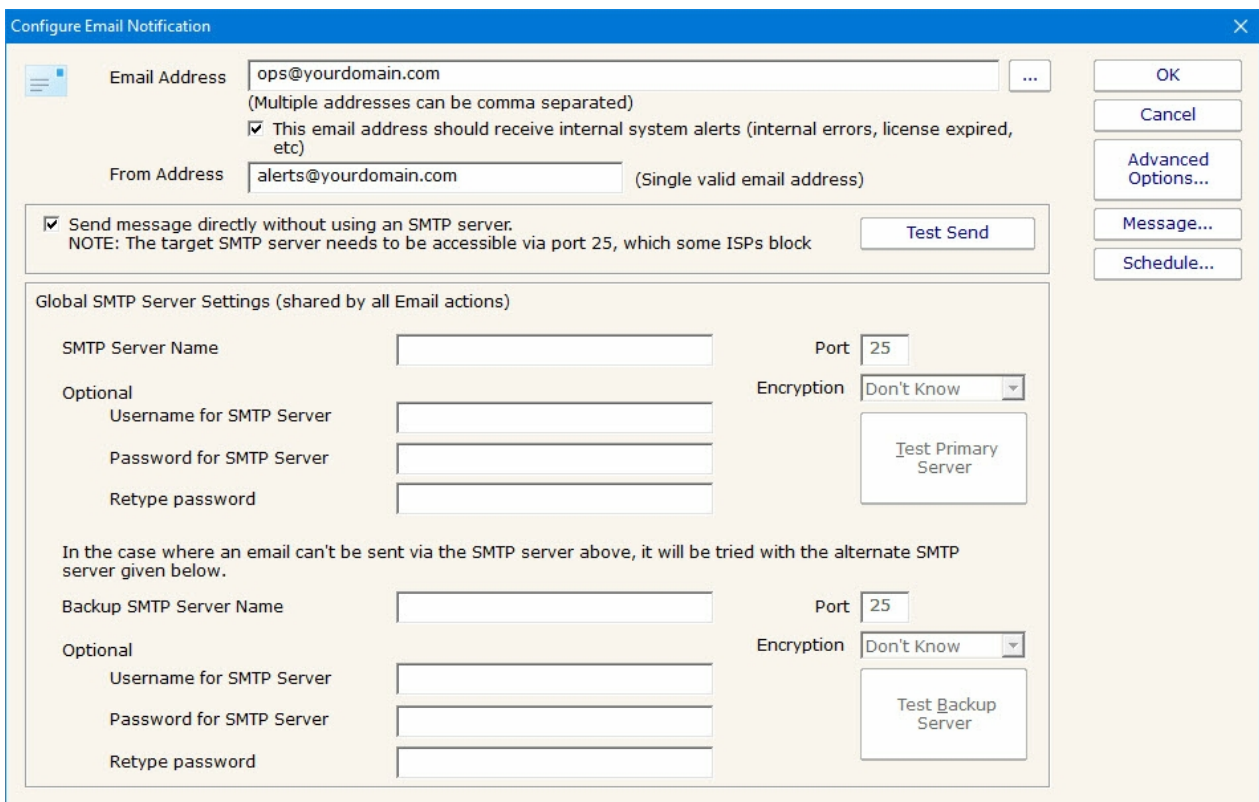
Direct Send

PA File Sight 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 File Sight 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 File Sight.

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 File Sight to send the message out using all other configured notification mechanisms. Only notification actions (like SMS, Pager, etc) will tried in this fallback scenario.

- Queue for Later - If a message can't be sent (perhaps because there is no connection to the server), you can specify that the message be queued for later delivery. Periodically PA File Sight will try to send any messages that are in the queue.

- Reverse Primary/Secondary - For testing purposes it is sometimes desirable to send via the Secondary SMTP server just to make sure it is working as expected.

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.
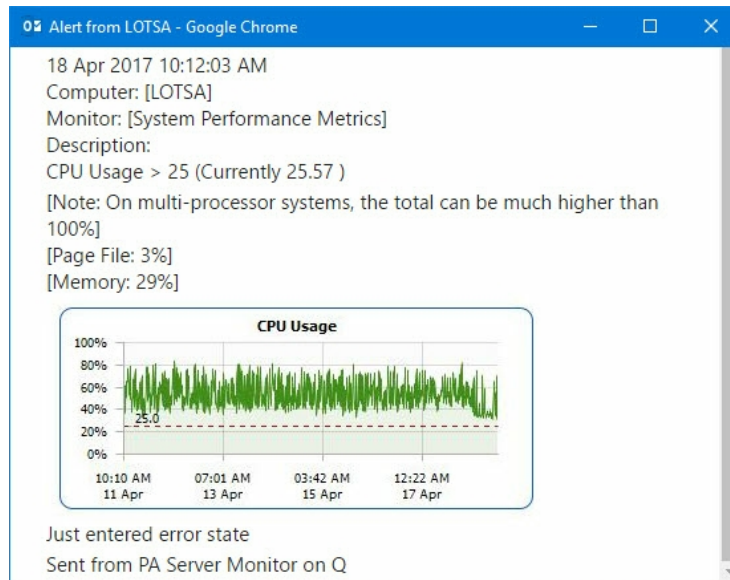
> 💡
>
> Some good hints and tips about HTML email are available here:
> http://www.mailchimp.com/resources/guides/email-marketing-field-guide/

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.
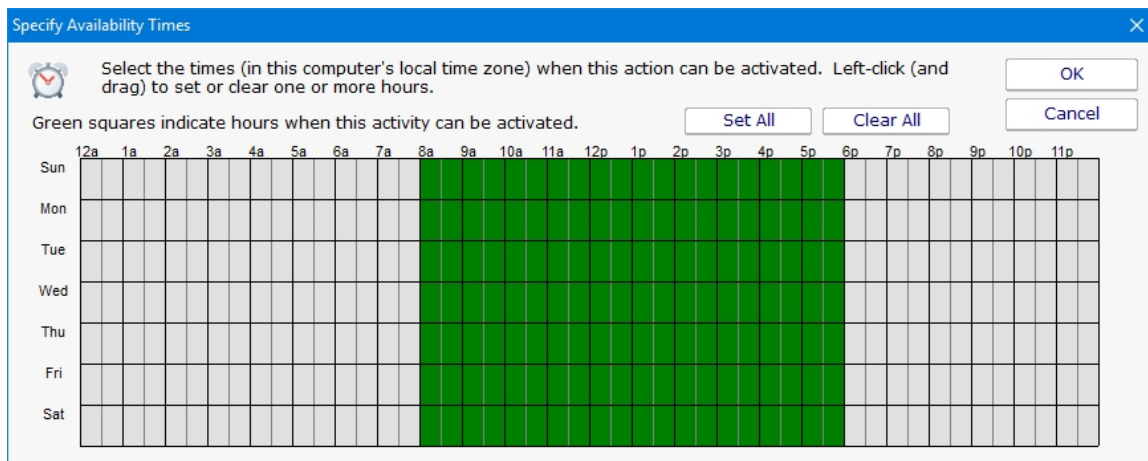
A typical alert email could look something like this:

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
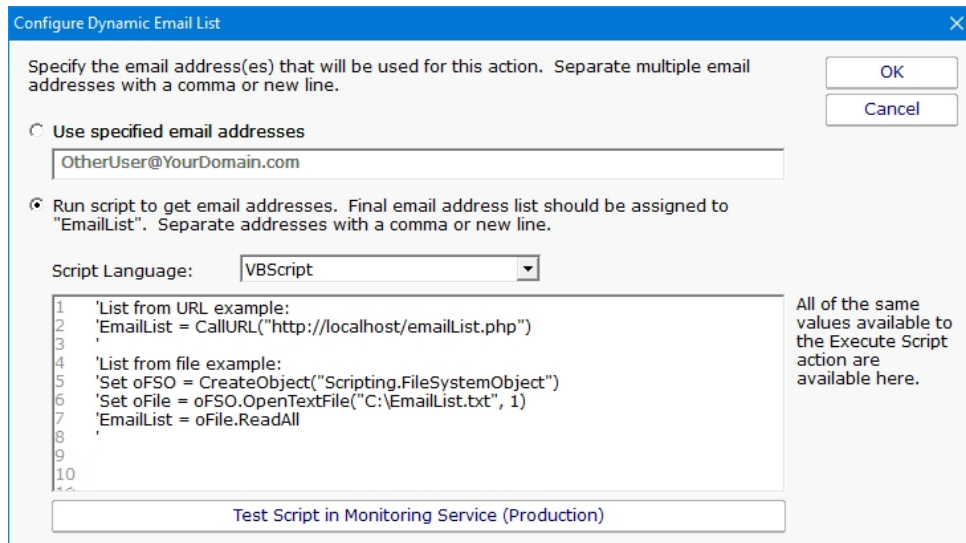
Scripting the Recipients

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".

Configure Dynamic Email List ✕

Specify the email address(es) that will be used for this action. Separate multiple email addresses with a comma or new line.

OK | Cancel

○ Use specified email addresses

    OtherUser@YourDomain.com

◉ Run script to get email addresses. Final email address list should be assigned to "EmailList". Separate addresses with a comma or new line.

Script Language: VBScript ▾

```
1   'List from URL example:
2   'EmailList = CallURL("http://localhost/emailList.php")
3   '
4   'List from file example:
5   'Set oFSO = CreateObject("Scripting.FileSystemObject")
6   'Set oFile = oFSO.OpenTextFile("C:\EmailList.txt", 1)
7   'EmailList = oFile.ReadAll
8   '
9
10
```

All of the same values available to the Execute Script action are available here.
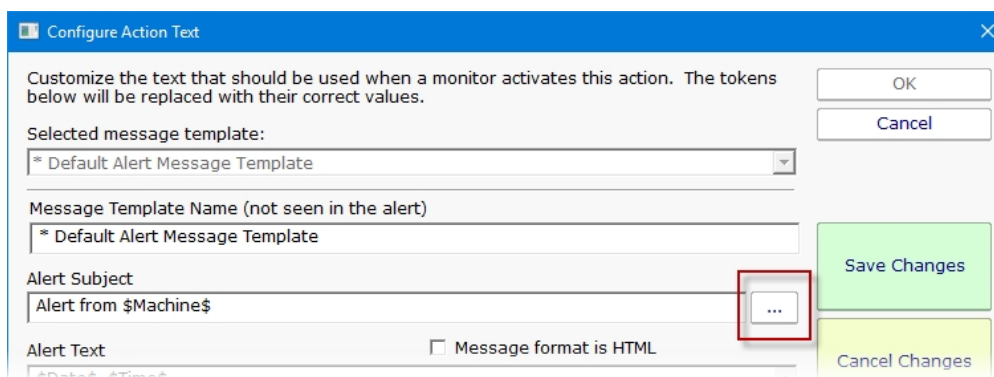
Test Script in Monitoring Service (Production)

## 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.
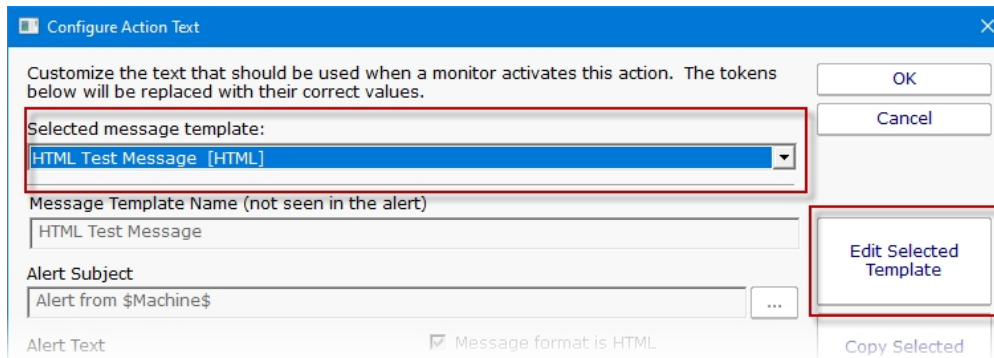
Then to access this script click the ... button on the Message dialog.

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.
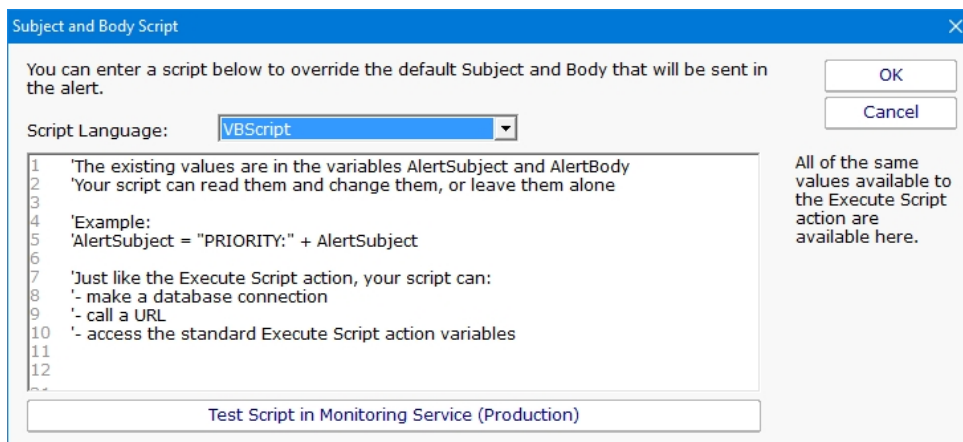
Execute Script Action

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")
```

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

- Delete log files

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 File Sight fills this dialog with a standard message box title and message. You may customize the message box that is displayed when this action is taken when the error occurs by editing the Title or Message Text.
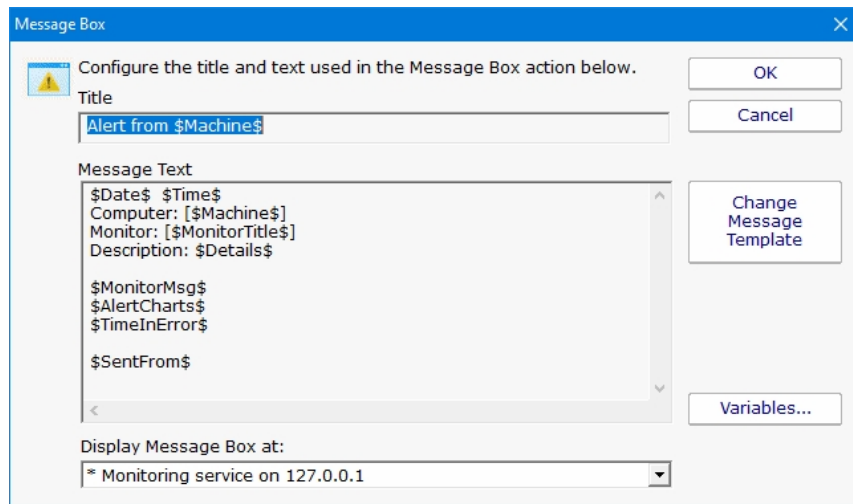
The button titled "Variables" will open a screen that displays the replacement variables that are available for use.

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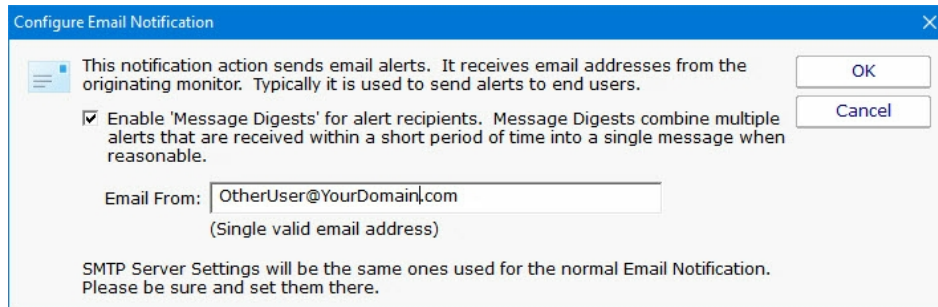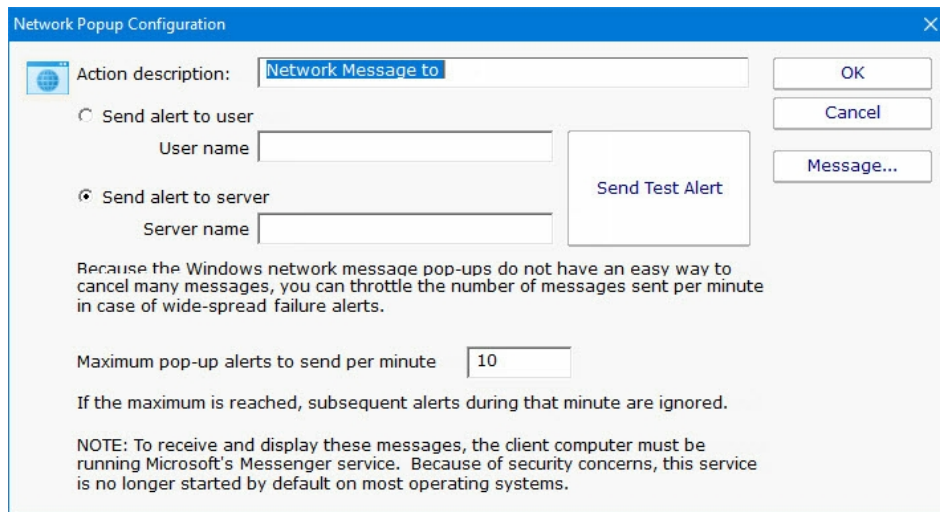
Like the E-mail Message Action, the Directed-Email Action also supports Message Digests. Message Digests combine all messages that arrive within a short amount of time for a email address into a single message.

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.
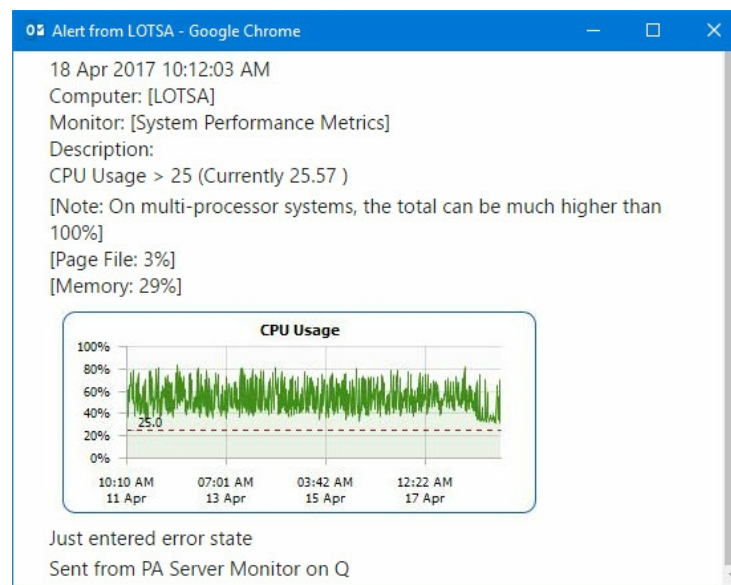
  Some good hints and tips about HTML email are available here:
  http://www.mailchimp.com/resources/guides/email-marketing-field-guide/

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.
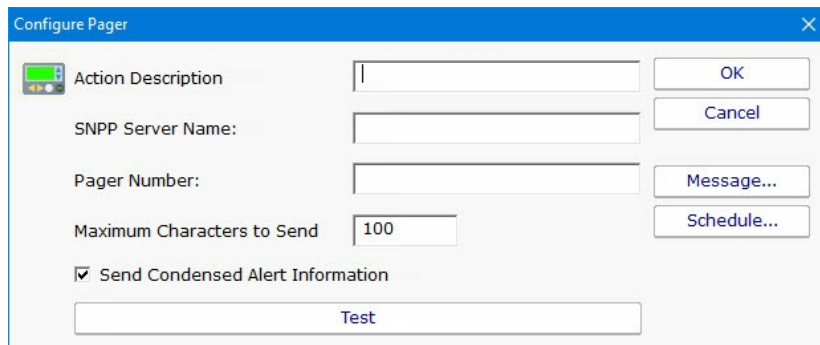
Some pager providers have an SMTP gateway. It is often easier to configure an E-Mail Action to send to a pager than the Send Pager Alert action. See the related FAQ about sending SMS alerts.

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'.

Specify Availability Times   ✕

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

Green squares indicate hours when this activity can be activated.

| Set All | Clear All |

| OK |
| Cancel |

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 File Sight can be sent to PagerDuty for handling.
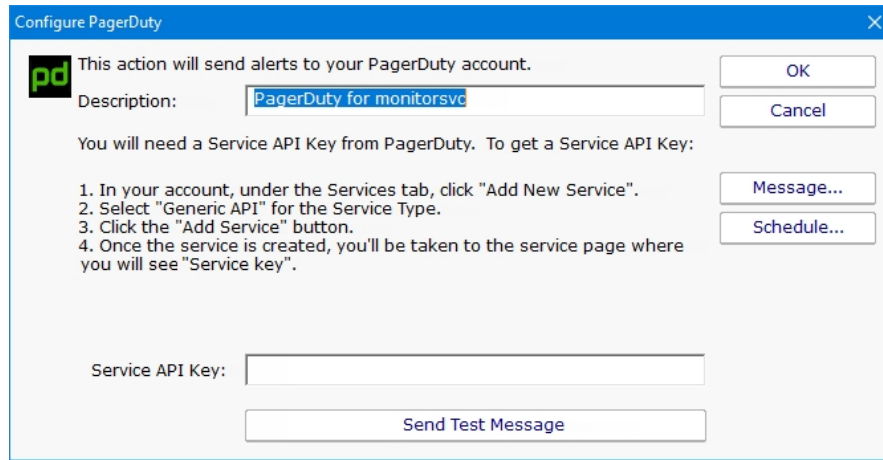
As is shown in the screenshot above, you just need to get a Service API Key from your PagerDuty account and paste it into the action. The action will then be able to send alerts directory to PagerDuty. Use this action like you would an email action or any other notification action.

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 ability 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'.

185

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

187

(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'.
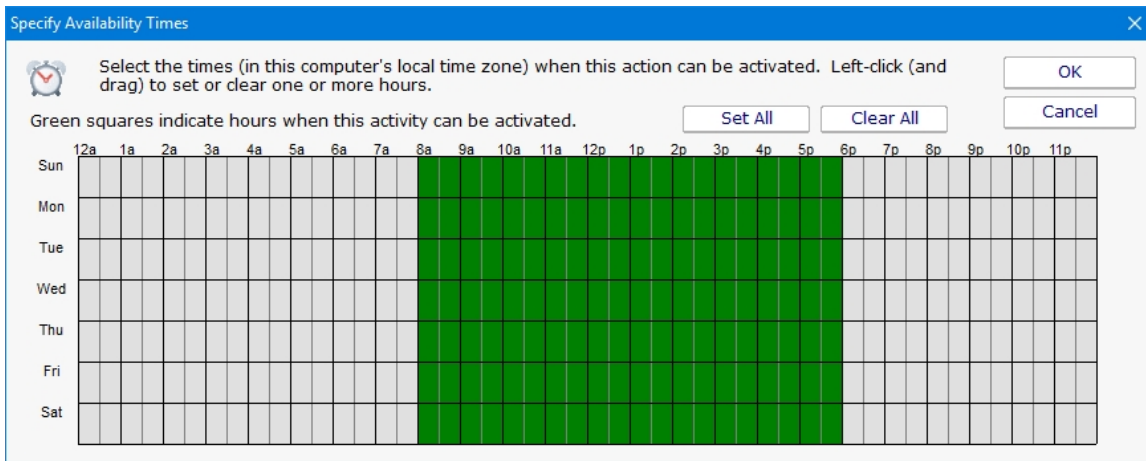
Experience from the field

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.
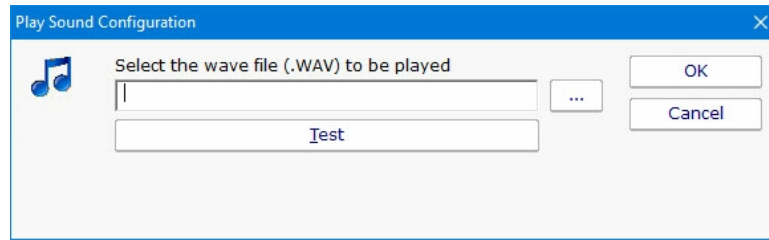
The sound is played on the Central Monitoring Service computer.

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.
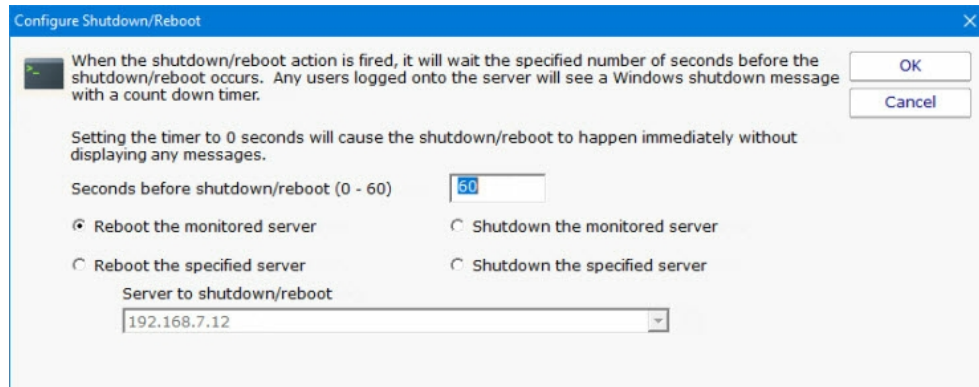
Run Report Action

Building on PA File Sight's incredible flexibility, now you can have a monitor trigger the generation of a Scheduled Report with the Run Report Action.
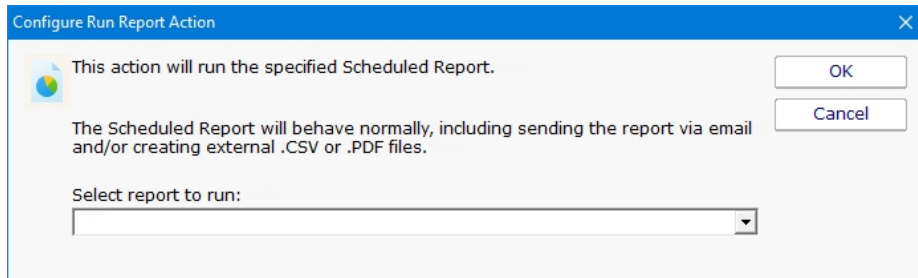
As is shown in the screenshot above, you just select an existing Scheduled Report. When this action is triggered, the Scheduled Report will run, including sending any specified emails and saving external PDF or CSV files.

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).
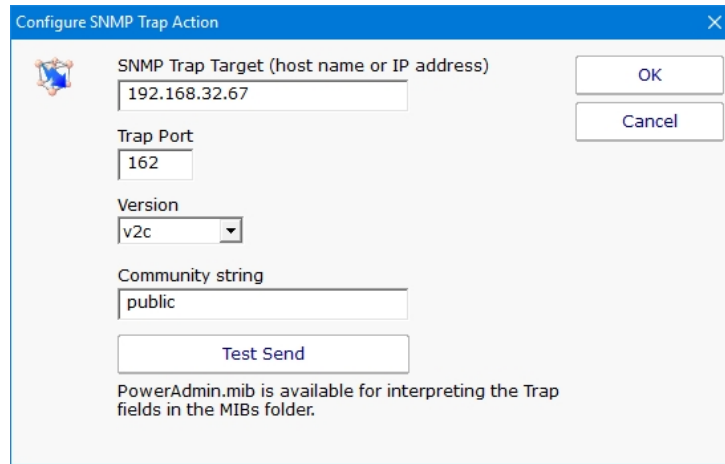
Traps will have the following fields:

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\PAFileSight, [DWORD] xShowIDs = 1

A MIB file exists in the C:\Program Files\PA File Sight\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
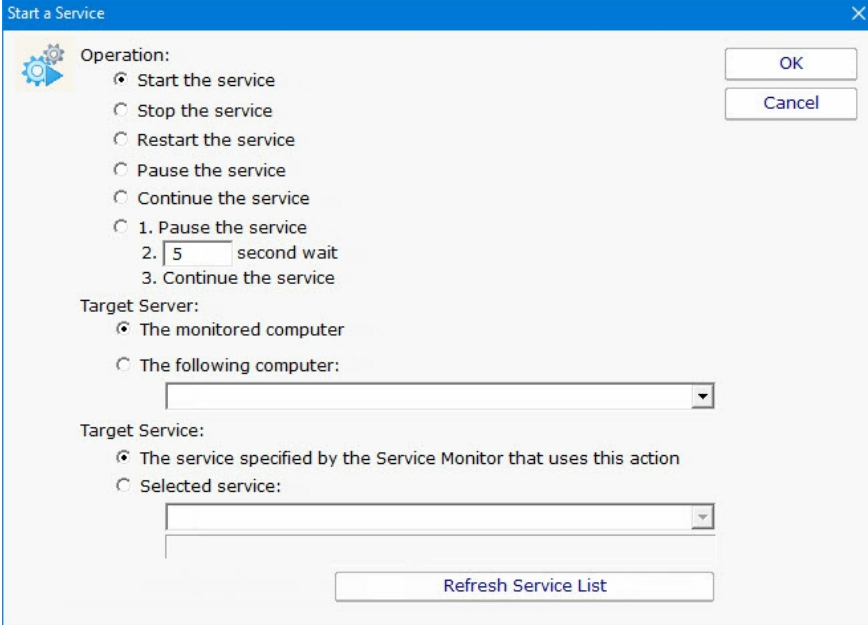
Replacement variables can optionally be passed on the command line to the program that is being launched.

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:$ItemType(x)$CV:$CurrVal(x)$LM:$LimitVal(x)$X1:$Extra1(x)$X2:$Extra2(x)$ID:$ID(x)$F:$Facility(x)$S:$Severity(x)$

> 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.
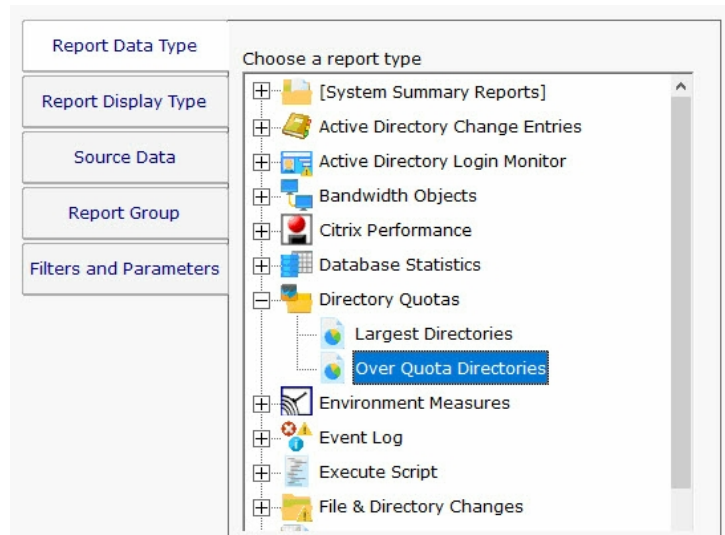
On the Report Display Type we see that this particular report can be represented as a Bar Chart, CSV Export, Line Chart or Tabular Report. The Tabular Report will create a dynamic HTML table with sortable column headers. The CSV Export is a .csv file which can easily be imported into Excel and other applications. Some report display types won't make sense for some data types -- in that case, the display type will not be shown.
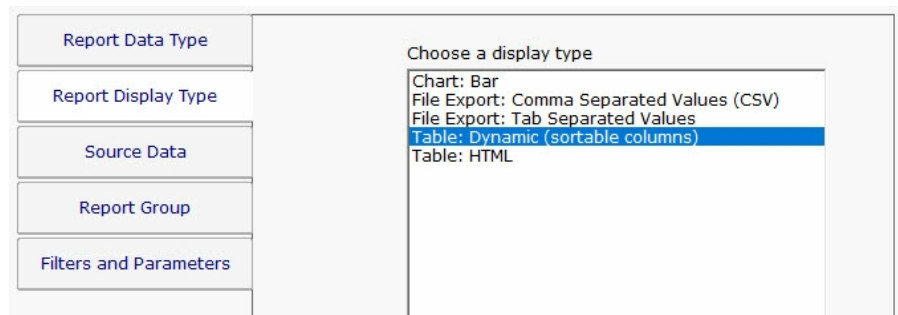
After having selected the report type and the display format, it's time to choose which data to report on. This is done on the Source Data tab. This tab will display all of the data that is available for the chosen report type. In this case we are shown drives that can be reported on. The radio buttons 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.
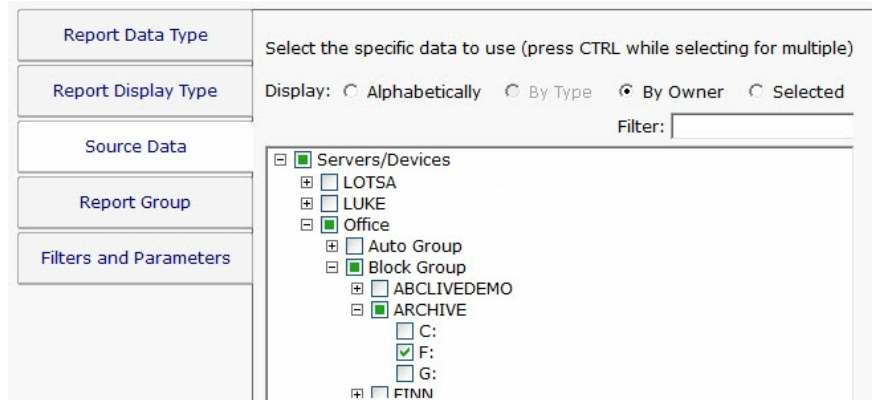
Select the Group where the Ad Hoc report will be saved to under View Existing Reports.
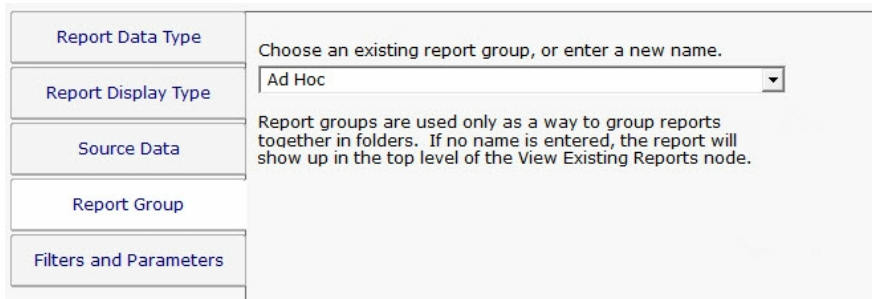
The final tab is Filters and Parameters. The filters and parameters shown depend on which report type you are creating. Most data sets have the ability to specify a time span for the report. Many report types also have summarization abilities like the example below. Summarizing allows you to take a large 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.
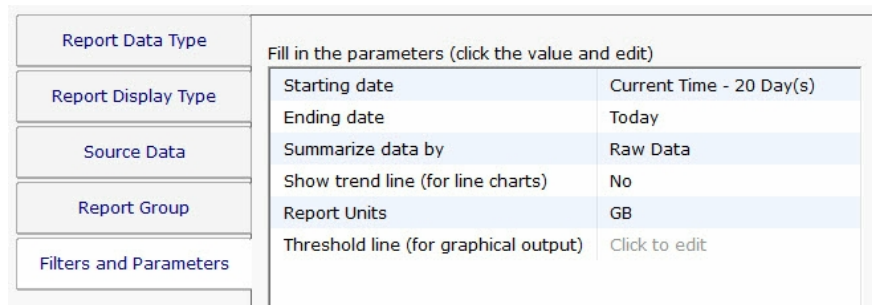
When you press the Generate Report button you will be taken to a "Report Generation in Progress" page, and then automatically forwarded to the finished report.

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 File Sight 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 File Sight\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

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.
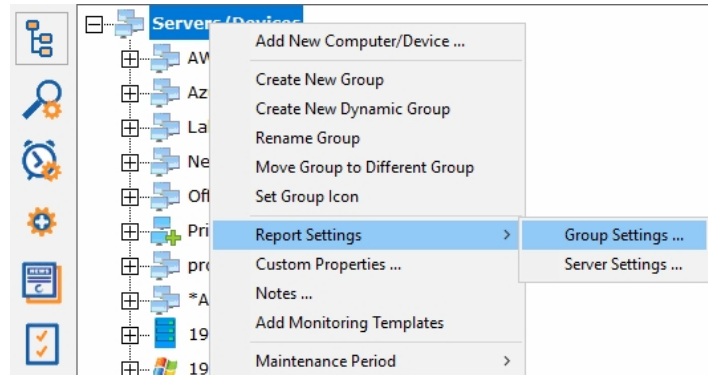
Next, you will see the Group Report Settings and Delivery dialog displayed, as shown.
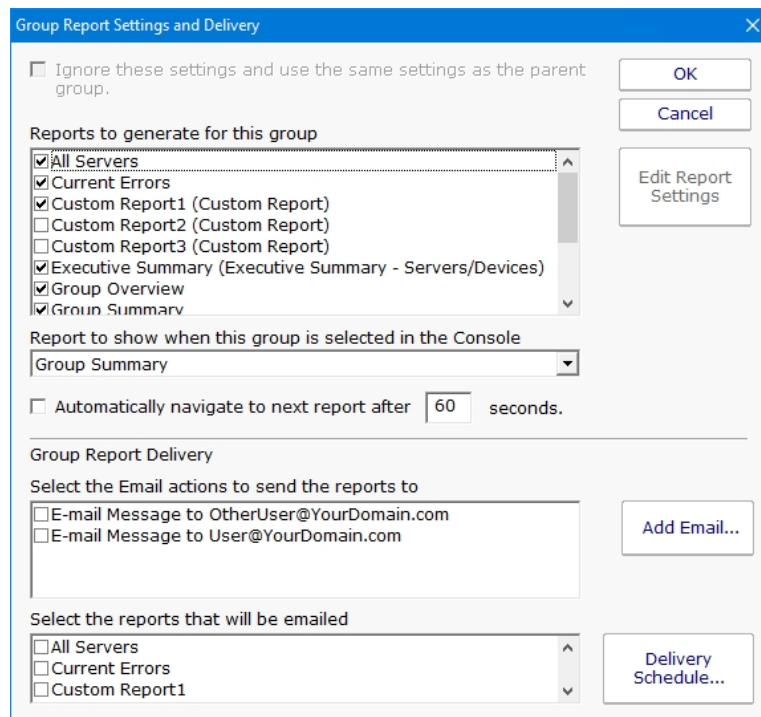
Here you can change the appearance and some characteristics of the Group Reports displays.

- 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\PAFileSight
> [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.
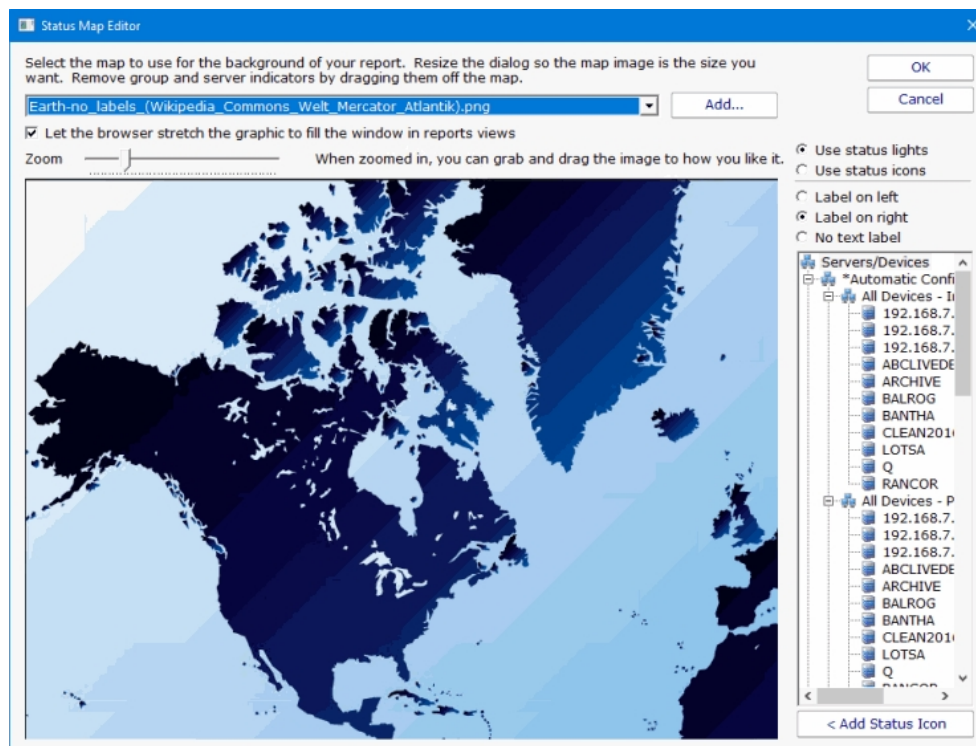
○ The Status Map Editor allows you to select one of a number of included graphical maps of the world and of world regions that can be used as a background for the server status lights.

○ 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 File Sight.

○ 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 File Sight 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 Servers

Servers/Devices
Visual Status Map

Web Report Access

PA File Sight 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\PAFileSight
[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

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
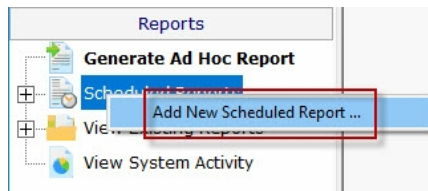Connected
Last Contact: 27 Mar 05:20 PM

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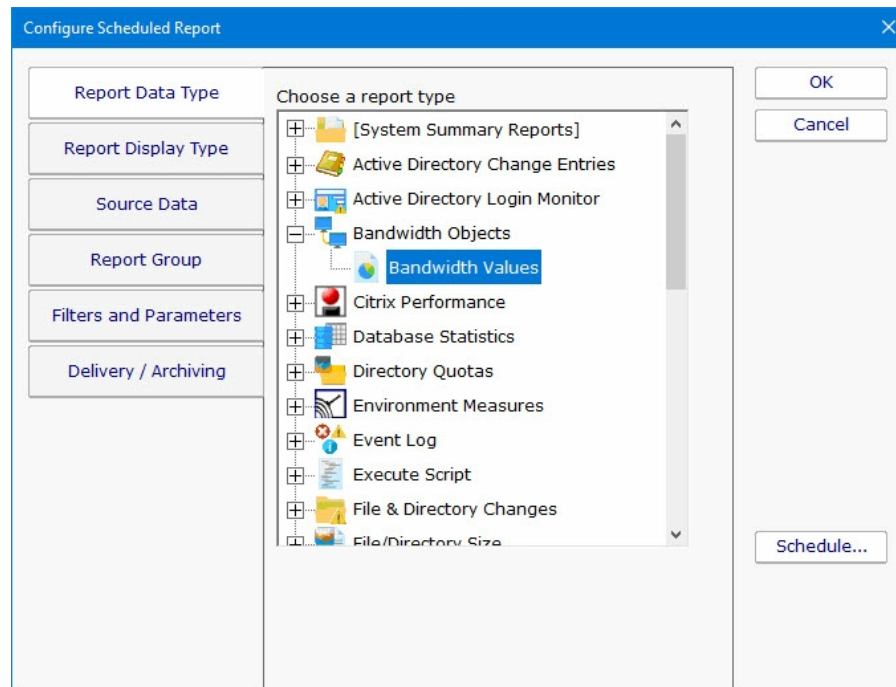
The Delivery / Archiving tab lets you specify whether to email the report when it has run. The report email will contain a PDF as well as an image of the report (raw HTML isn't sent because of varying support in email clients).

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.
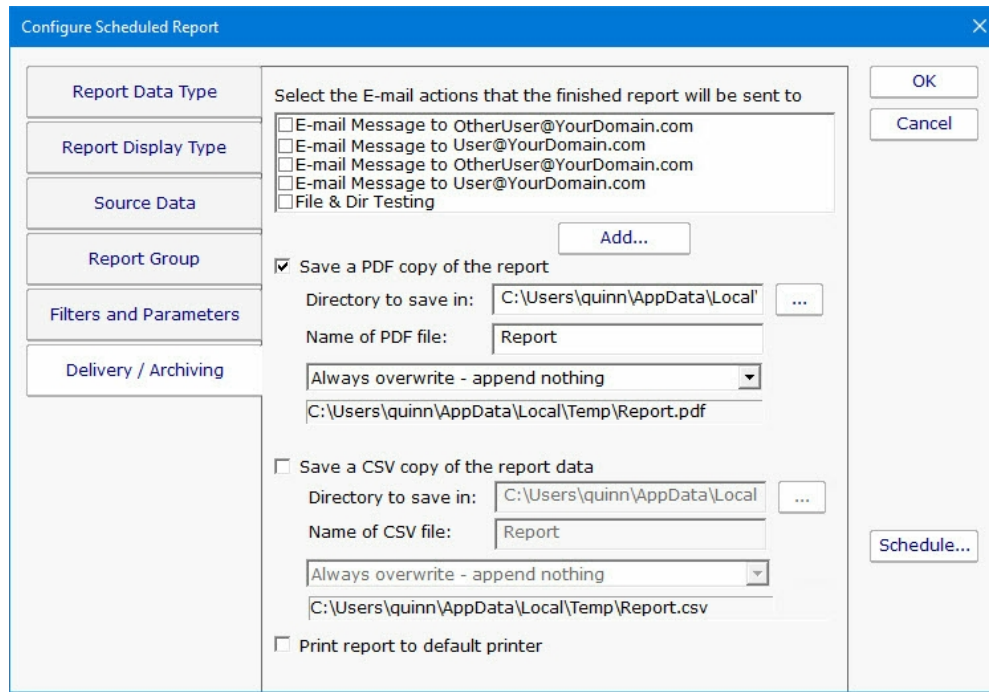
Scheduled reports always write to the same location on disk, so the URL to the report is always the same, and viewing the report in the browser will show the latest generated version of that report. This makes it easy to save the URL in your browser's Favorites list. If you want to change this behavior, 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.
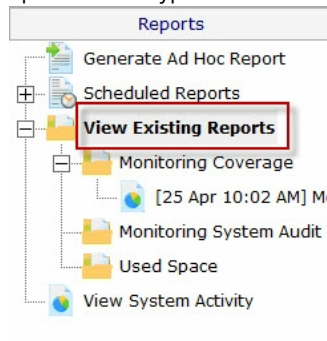
○ The top right of every report contains a button labeled All Reports. This button will take you to a table of contents page showing all available reports.

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.
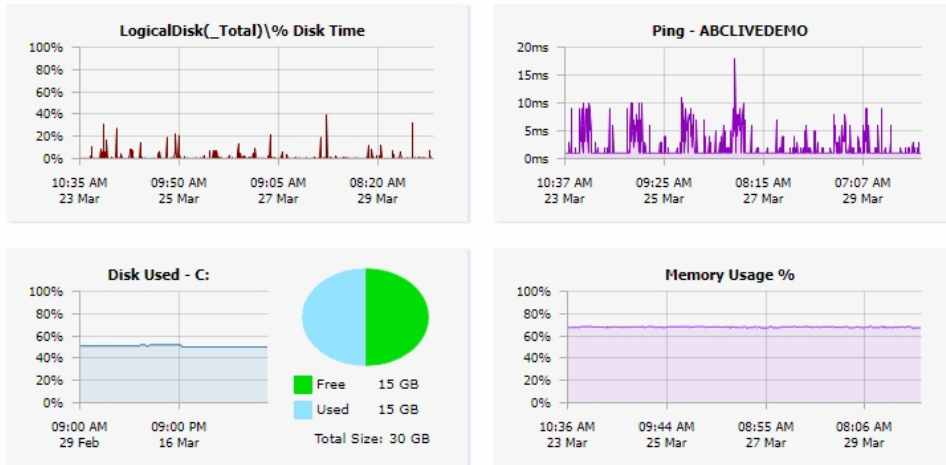
Server Status Report

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.
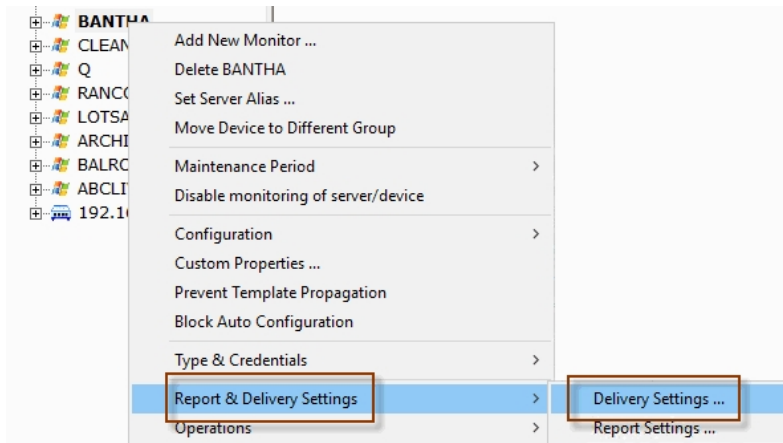
> 💡 If you are a Managed Service Provider, use Filter User Access at Settings -> Remote Access to control which servers and devices your customers can see.

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...
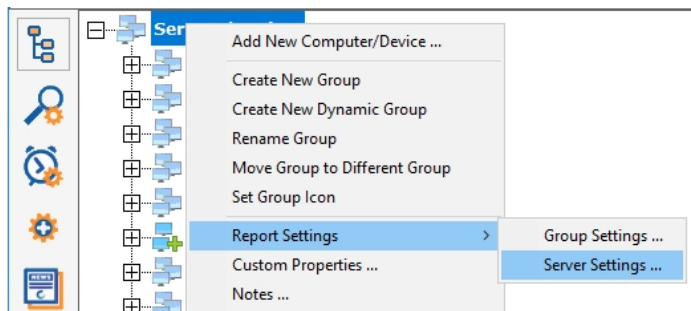
... or select a specific computer and choose Report & Delivery Settings -> Report Settings.
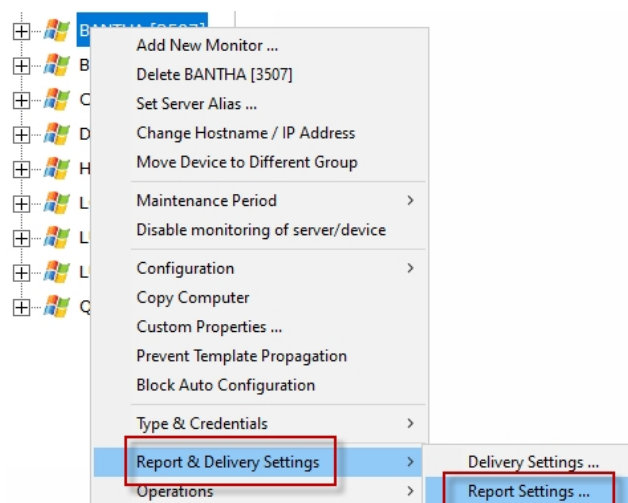
Report Parts

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.
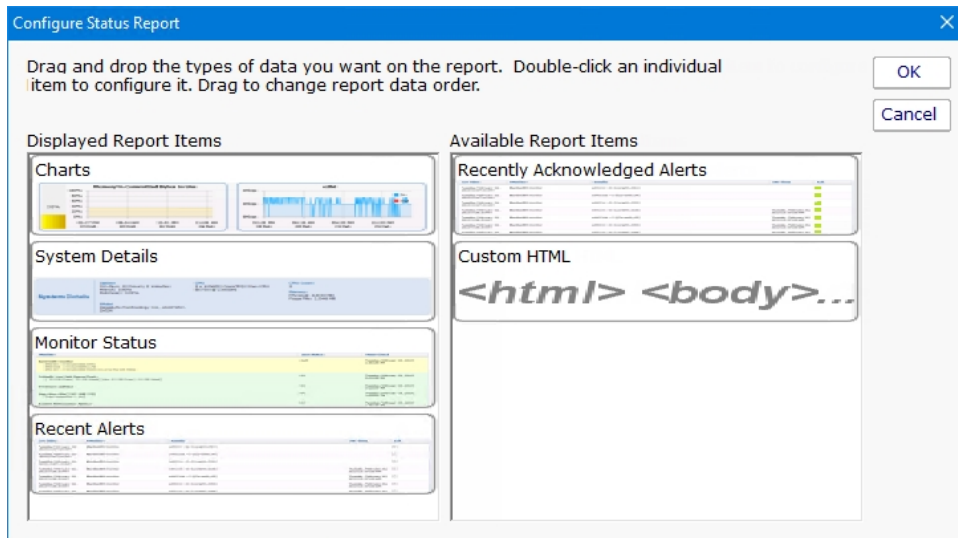
Double-click on a report item to configure settings for that report item.

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)
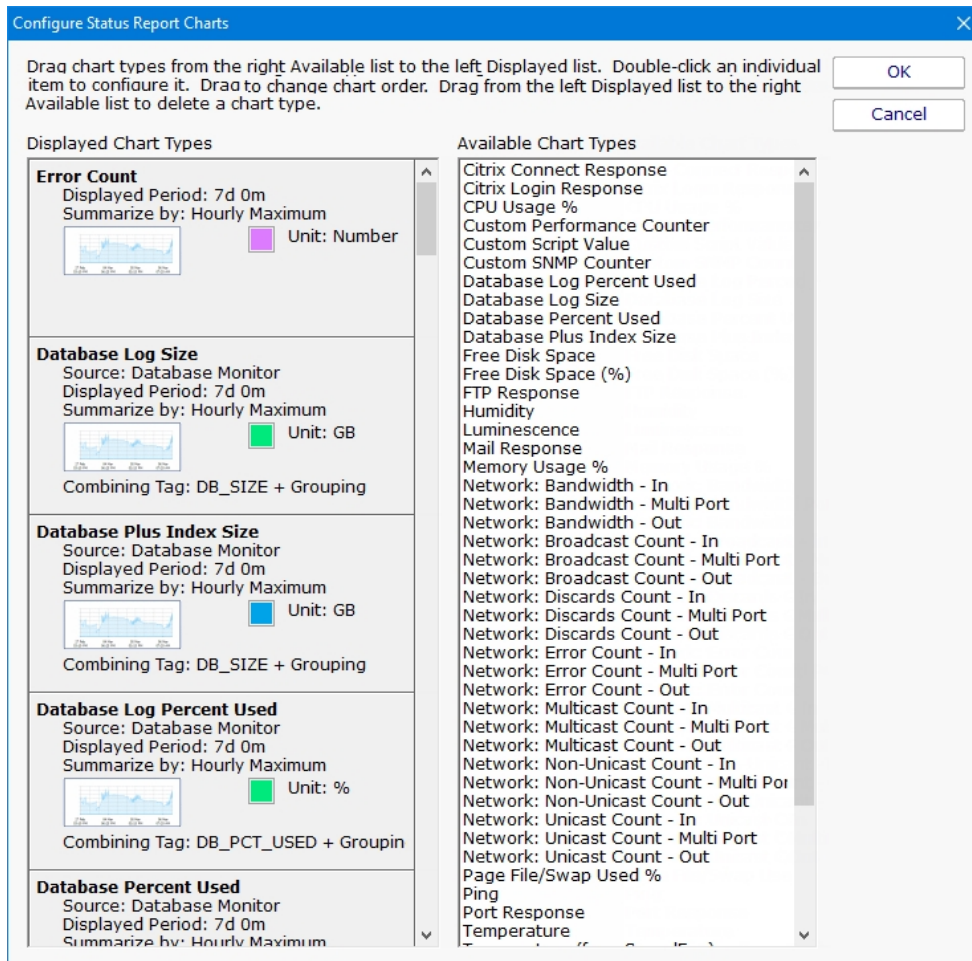
The above Configured Status Report Charts menu is an example of how the menu will appear when you select the menu from the Servers/Devices node. All of the chart types listed at this level are available to all servers/devices under this node.
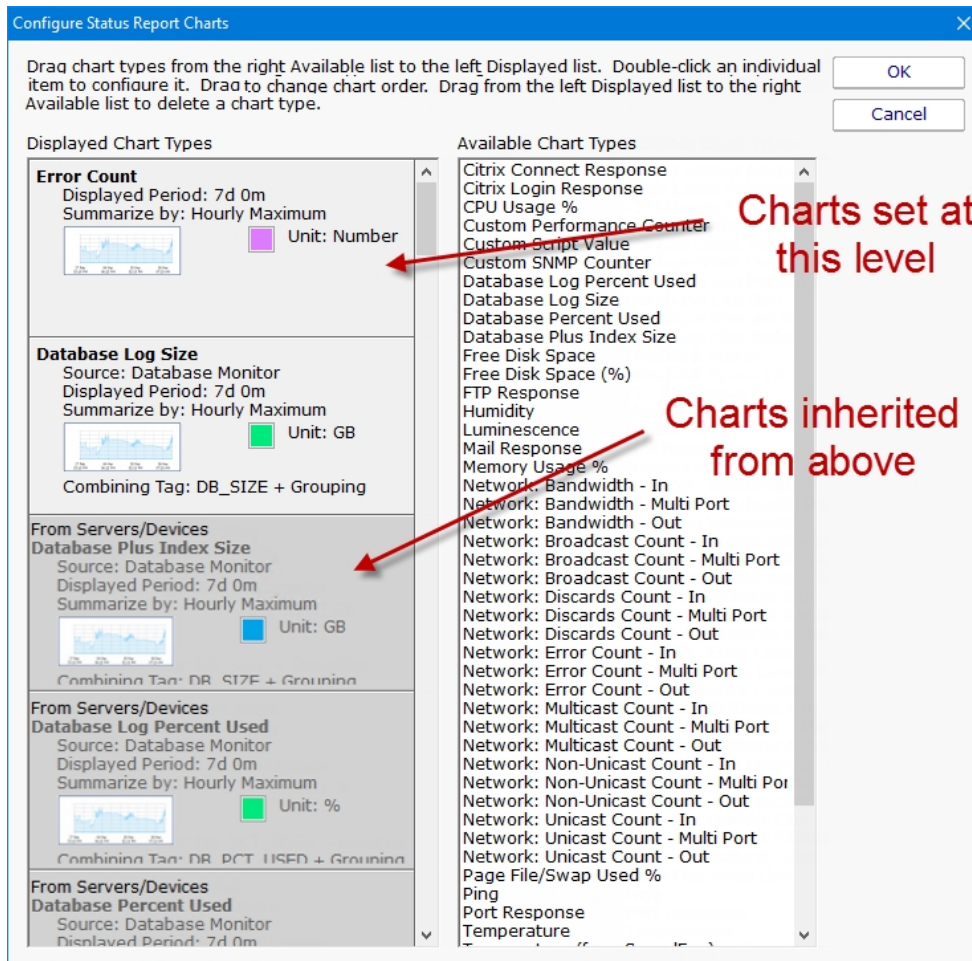
The above Configured Status Report Charts menu is an example of how the menu will appear if you select the Configured Status Report Charts menu at a group or server/device level. Note the different shaded chart types. The darker shaded charts are inherited from a group above. The lighter shaded charts 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.
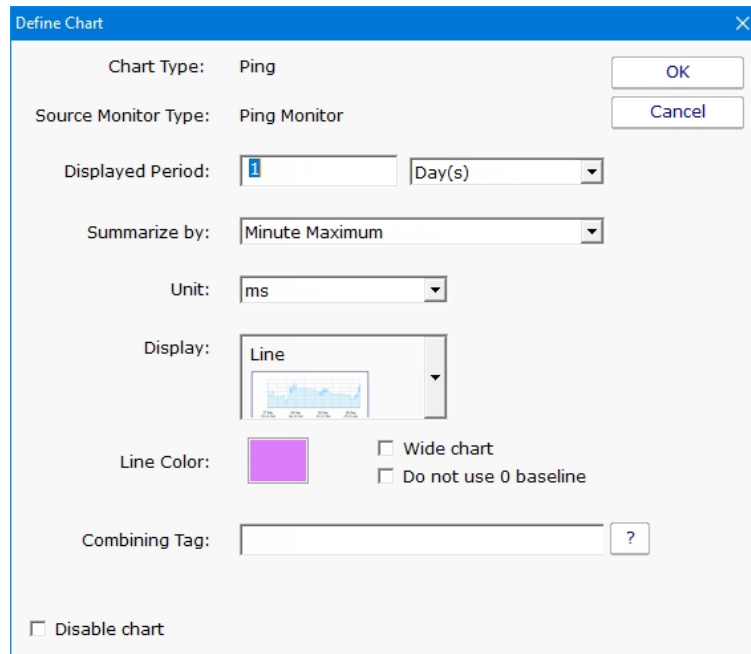
Configuring System Details

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.
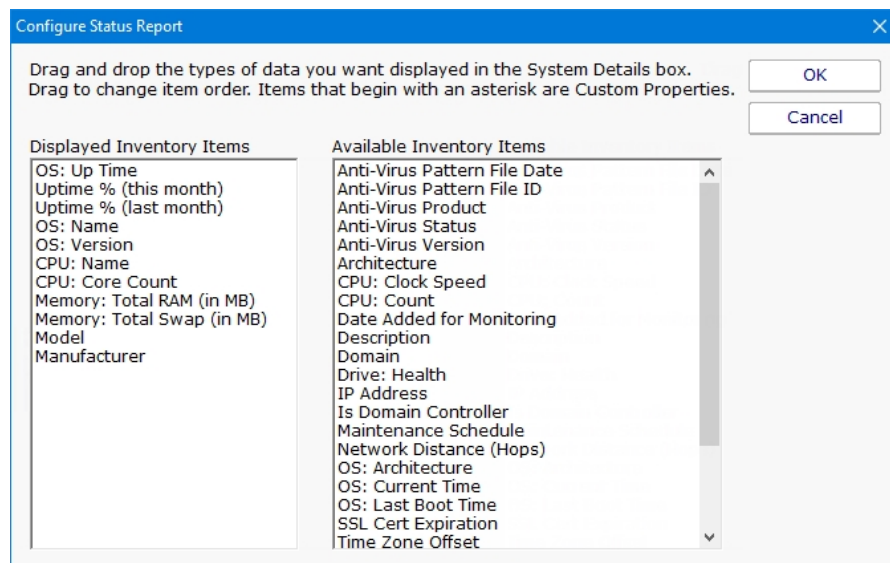
Configure Monitor Status

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.
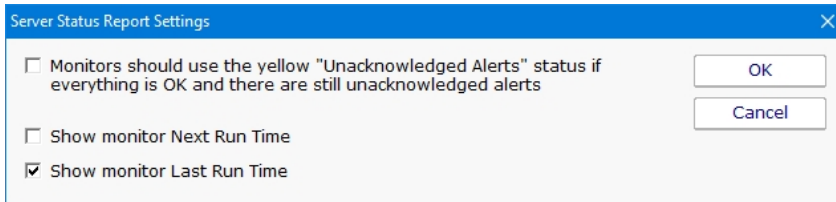
Configure Recent Alerts

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.
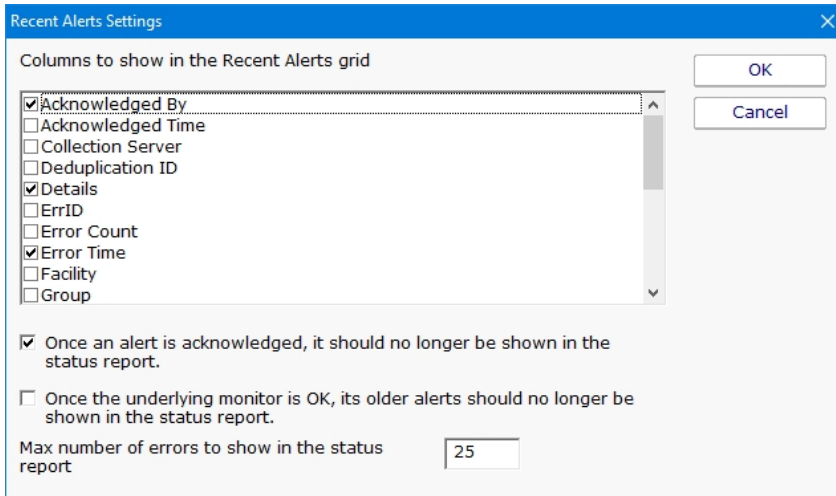
Configure Recently Acknowledged Alerts

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.
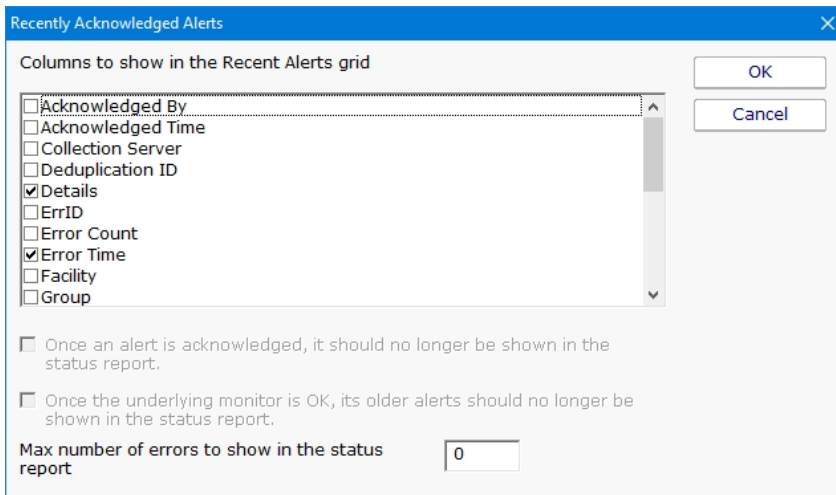
Configure Custom HTML

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.
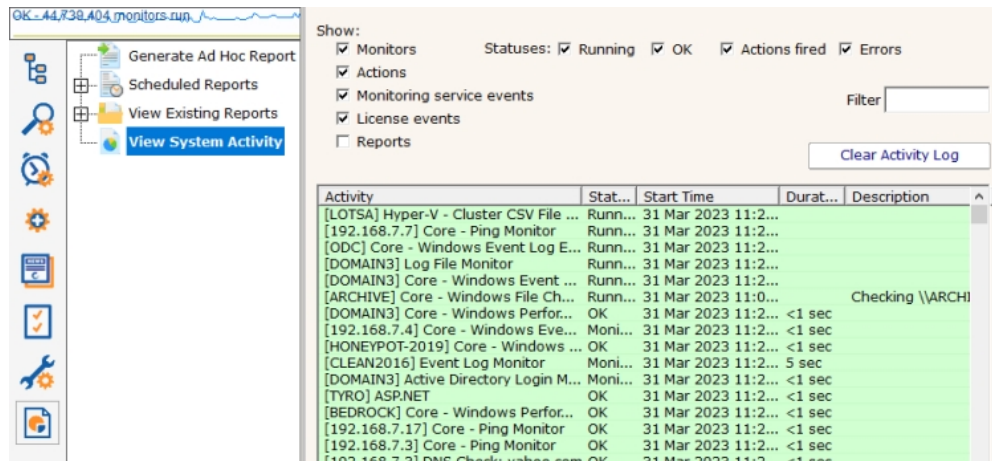
Standard Report Tabs

Running a report in PA File Sight 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.
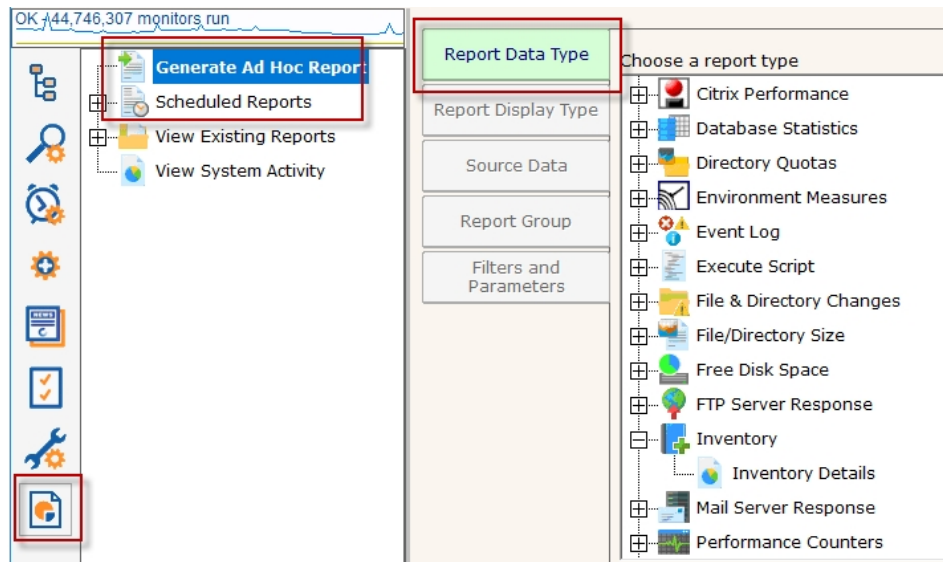
On the right side are all of the different report types. In general you would want to go to the monitor that is collecting the data that you want to run a report on. In this example we'll select the Active Directory Login Monitor. You might have different monitor/report types listed based on your product and license.
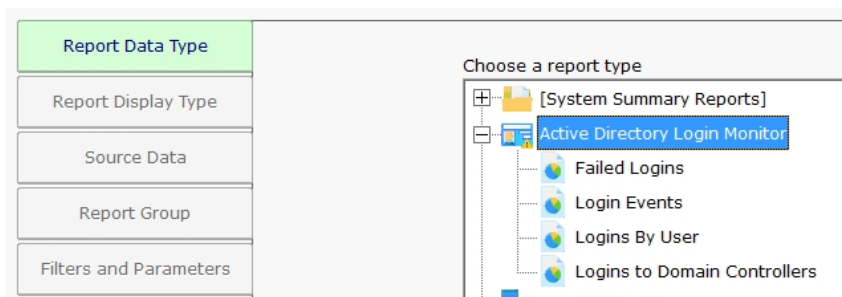
Once you've selected the report type, visit each of the tabs on the left to make selections.

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.
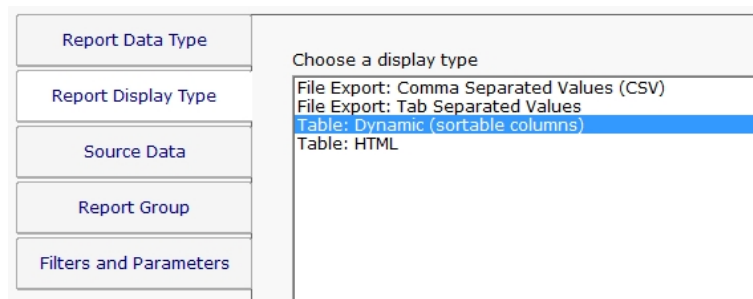
Source Data

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.
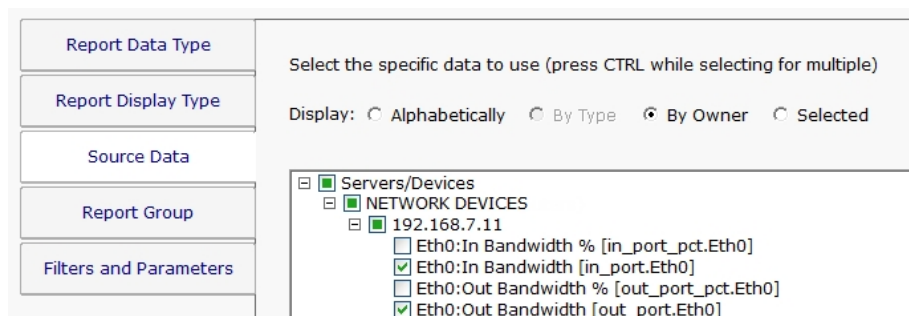
Report Group

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.
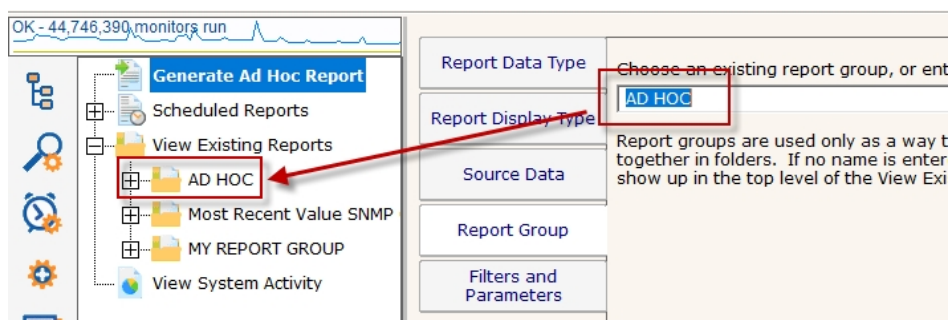
Filters and Parameters

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.

Report Data Type	Select the E-mail actions that the finished report will be sent to
Report Display Type	☐ Email
Source Data	☐ E-mail
Report Group	
Filters and Parameters	Add...
Delivery / Archiving	

☐ Save a PDF copy of the report

Directory to save in: H:\TEMP   ...

Name of PDF file: Report

Always overwrite - append nothing

H:\TEMP\Report.pdf

☐ Save a CSV copy of the report data

Directory to save in: H:\TEMP   ...

Name of CSV file: Report

Always overwrite - append nothing

H:\TEMP\Report.csv

☐ Print report to default printer

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.

PA File Sight - All Changes Report

The All Changes report is a quick way to see everything PA File Sight has recorded in an environment during a specified time frame. Because it uses few filters it is most often useful in testing, or in environment where only a few activities are being monitored.
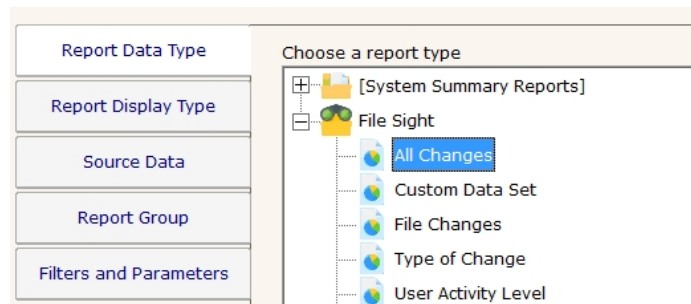
This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.
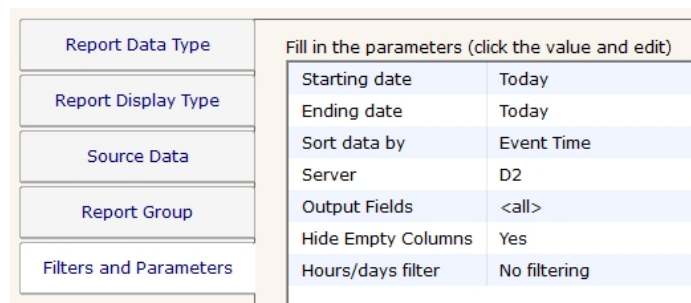
You can control which fields are shown in the output via the **Output Fields** column. Data from only a specific server can be selected using the **Server** field.

PA File Sight - Custom Data Set Report

The Custom Data Set Report is a very flexible report which offers the most filtering options to see exactly what you are searching for.
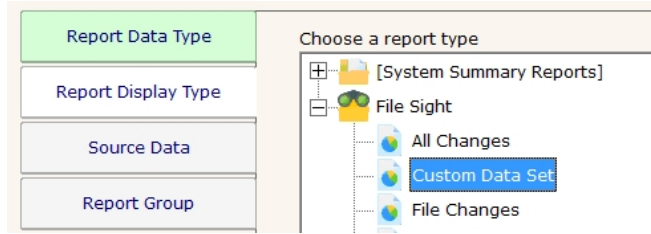
This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.
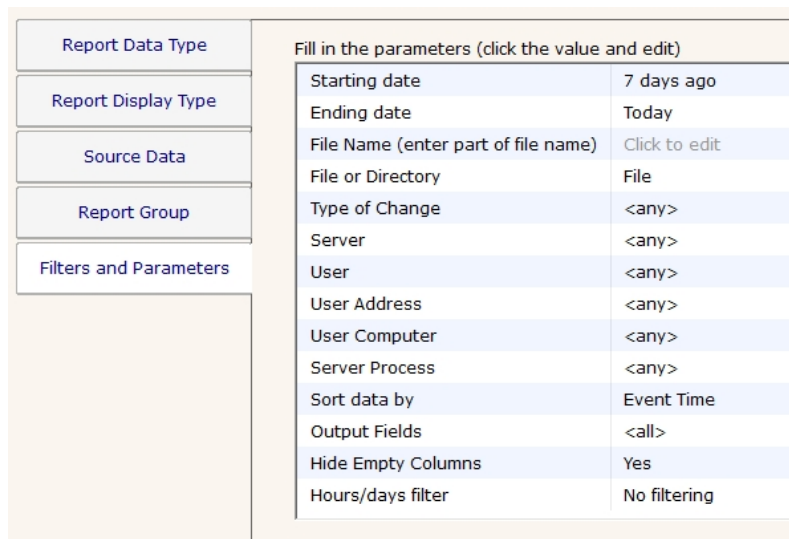
The fields that can be set include:

Starting date:
Ending date:
Hours/days filter
    See the standard report tabs **for information**
File Name
    This field will be used to match against the full path of files and directories in the database. It accepts the * wild-card. You do not have to specify the full path for matching files - if the text you enter is found anywhere in the path, that is a match.

You can use a comma to separate multiple file names. You can put an exclamation mark (!) in front of a file to indicate NOT that file.

Some examples:

.mp3 - return any file that contains .mp3 anywhere in the full path of the file

*.mp3 - the same as above

.docx, .xlsx, .pdf - return any files that contain .docx, .xlsx or .pdf anywhere in the full path

\DOCS\ - return any files that contain \docs\ anywhere in the filepath (checks are not case sensitive)

!authorized - return any files that do NOT contain 'authorized' in the full path

.docx,!authorized - return all .docx files unless 'authorized' is in the full path

File or Directory
Indicate whether the search should work on just files, just directories, or both.

Type of Change
Filter the files by the operation that was performed on them. The change can be one or more of:
Audit Changed (file security setting)
Copy (detected by the PA File Sight Endpoint)
Created
Deleted
Failed to Change Audit
Failed to Change Group
Failed to Change Owner
Failed to Change Permission
Failed to Create
Failed to Delete
Failed to Move
Failed to Read
Failed to Rename
Failed to Write
Group Changed (file security setting)
Moved
Owner Changed
Permission Changed
Read
Renamed
Wrote
Server
Select the server from which file activity is being reported on
User
Select a specific user for which file activity is being reported. A list of users seen will be loaded from the database.
User Address
Select a specific user IP address for which file activity is being reported. A list of user IP addresses that have been seen will be loaded from the database.
User Computer
Select a specific user's computer name for which file activity is being reported. A list of user computer names that have been seen will be loaded from the database.
Server Process
A list of all server processes will be loaded and shown from the database. Specify those that you want to report on. The special System or Network entry is used when the server operating system was the source of a file operation, OR when the operation came from a remote computer (a request from the network).
Output Fields
Control the size of the report by only showing the columns you are interested in
Hide Empty Columns
Depending on the report settings and the information available, some fields might be empty. This setting can automatically hide columns where all values within the column are empty.

Custom Data Set
Summarized Data

All Reports **PDF Version**

Data shown for 20 Mar 2020 12:00 AM to 31 Mar 2020 11:59 PM, 98 records

Event T..	Operat..	File Name	File S..	User ..	Server Pr..
3/20/2020 1:06:35 PM	Created	K:\Customer Files\Unconfirmed 503287.crdownload	Q	127.0....	chrome.exe
3/20/2020 1:06:35 PM	Permiss... Changed	K:\Customer Files\Unconfirmed 503287.crdownload	Q	127.0....	chrome.exe
3/20/2020 1:06:35 PM	Read	K:\Customer Files\Unconfirmed 503287.crdownload	Q	127.0....	chrome.exe
3/20/2020 1:06:35 PM	Renamed	K:\Customer Files\Unconfirmed 503287.crdownload -to-> K:\Customer Files\Paycor, Inc. - 03132020Q160 - Invoice.pdf	Q	127.0....	chrome.exe
3/20/2020 1:08:24 PM	Read	K:\Customer Files\Paycor, Inc. - 03132020Q160 - Invoice.pdf	Q	127.0....	acrord32.exe
3/20/2020 1:09:00 PM	Permiss... Changed	K:\Customer Files\Unconfirmed 770209.crdownload	Q	127.0....	chrome.exe

PA File Sight - File Changes Report

This report is useful to quickly find out what activities happened to a specific file. In the example below, everything that happened to the budget.xls file will be shown.
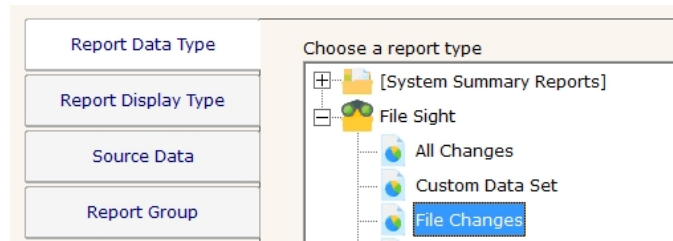
This report is a subset of the more powerful Custom Data Set Report.

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.
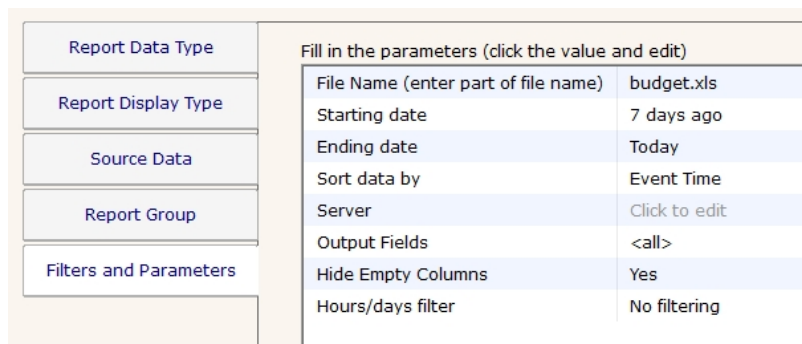
The fields that can be set include:

File Name

This field will be used to match against the full path of files and directories in the database. It accepts the * wild-card. You do not have to specify the full path for matching files - if the text you enter is found anywhere in the path, that is a match.

You can use a comma to separate multiple file names. You can put an exclamation mark (!) in front of a file to indicate NOT that file.

Some examples:

.mp3 - return any file that contains .mp3 anywhere in the full path of the file

*.mp3 - the same as above

.docx, .xlsx, .pdf - return any files that contain .docx, .xlsx or .pdf anywhere in the full path

\DOCS\ - return any files that contain \docs\ anywhere in the filepath (checks are not case sensitive)

!authorized - return any files that do NOT contain 'authorized' in the full path

.docx,!authorized - return all .docx files unless 'authorized' is in the full path

Starting date:

Ending date:

Hours/days filter

    See the standard report tabs **for information**

Server

    Select the server from which file activity is being reported on

Output Fields

    Control the size of the report by only showing the columns you are interested in

Hide Empty Columns

    Depending on the report settings and the information available, some fields might be empty. This setting can automatically hide columns where all values within the column are empty.

PA File Sight - Type of Change Report

The Type of Change report is a good way to see all changes of a specific type within a time frame. For instance, this is a good way to quickly see all files that have been deleted within a time range.
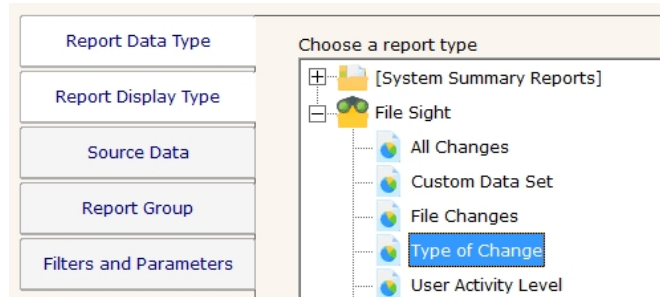
This report is a subset of the more powerful Custom Data Set Report.

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.
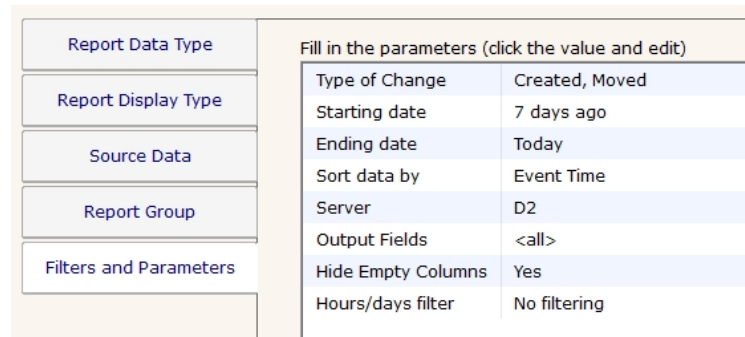
The fields that can be set include:

Type of Change
  Filter the files by the operation that was performed on them. The change can be one or more of:
    Audit Changed (file security setting)
    Copy (detected by the PA File Sight Endpoint)
    Created
    Deleted
    Failed to Change Audit
    Failed to Change Group
    Failed to Change Owner
    Failed to Change Permission
    Failed to Create
    Failed to Delete
    Failed to Move
    Failed to Read
    Failed to Rename
    Failed to Write
    Group Changed (file security setting)
    Moved
    Owner Changed
    Permission Changed
    Read

239

Renamed

Wrote

Starting date:

Ending date:

Hours/days filter

See the standard report tabs for information

Server

Select the server from which file activity is being reported on

Output Fields

Control the size of the report by only showing the columns you are interested in

Hide Empty Columns

Depending on the report settings and the information available, some fields might be empty. This setting can automatically hide columns where all values within the column are empty.

PA File Sight - User Activity Level Report

This report lets you search for any users that have done more than some number of specific operations. For example, you could search for users who have deleted for than 100 files in the past 7 days.
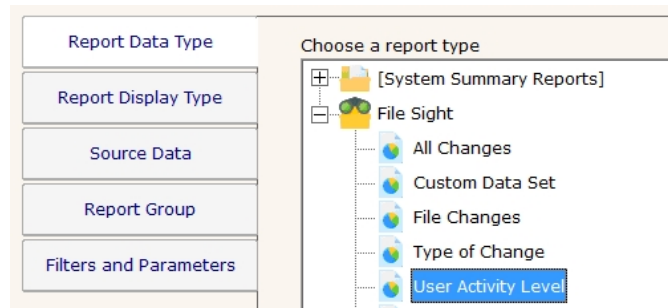
This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.
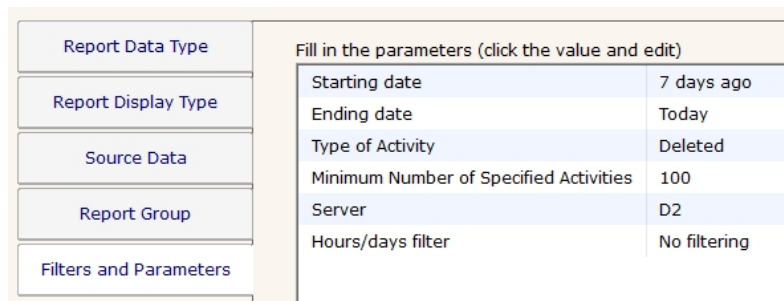
The fields that can be set include:

Starting date:
Ending date:
Hours/days filter
        See the standard report tabs **for information**
Type of Activity
        Filter the files by the operation that was performed on them. The change can be one or more of:
                Audit Changed (file security setting)
                Copy (detected by the PA File Sight Endpoint)
                Created
                Deleted
                Failed to Change Audit
                Failed to Change Group
                Failed to Change Owner
                Failed to Change Permission
                Failed to Create
                Failed to Delete
                Failed to Move
                Failed to Read
                Failed to Rename
                Failed to Write
                Group Changed (file security setting)
                Moved
                Owner Changed
                Permission Changed

> Read
> Renamed
> Wrote

Minimum Number of Specified Activities

> All activities of the specified types will be counted within the given time frame for each user. Any user that is over this limit will be listed in the report.

Server

> Select the server from which file activity is being reported on

Output Fields

> Control the size of the report by only showing the columns you are interested in

User Activity Level on Q, RANCOR [RANCOR]
Summarized Data

Created 31 Mar 2020 04:54 PM

All Reports | PDF Version

Data shown for 01 Jan 2020 12:00 AM to 31 Mar 2020 11:59 PM, 3 records

User	Activity Count
░░░░░░░░░░░	2193
OFFICE\quinn	129
NT AUTHORITY\SYSTEM	55

PA File Sight - User Block List Report

As part of the Blocked User List system, this report is a convenient way to see all users that are blocked or that are white-listed.
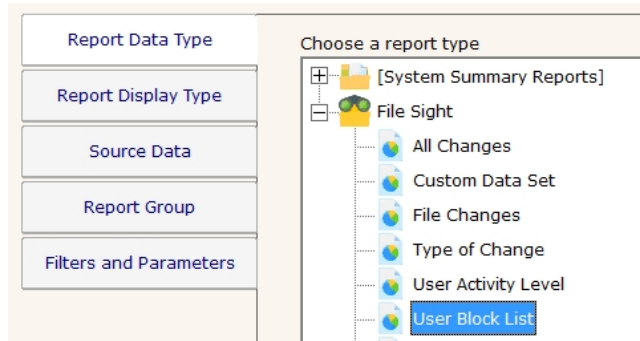
This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors.

Unlike most monitors, this report does not have any settings on the Filters & Parameters tab. Rather you select the data you want on the Source Data tab.

PA File Sight - User Changes Report

This report is best for quickly determining what file activities a particular user account has performed. For example it can answer "What files has George operated on in the past week?"
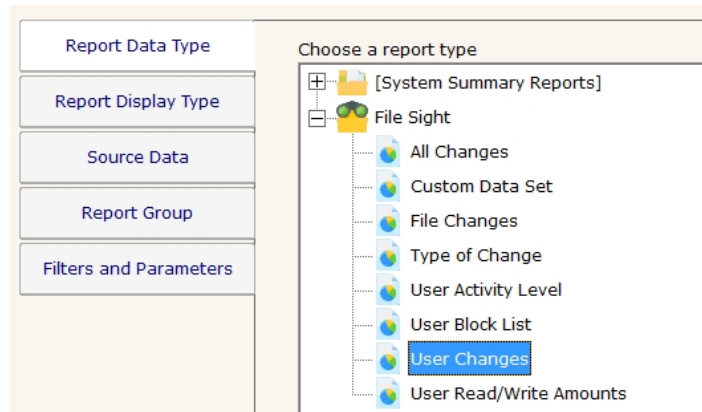
This report is a subset of the more powerful Custom Data Set Report.

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.
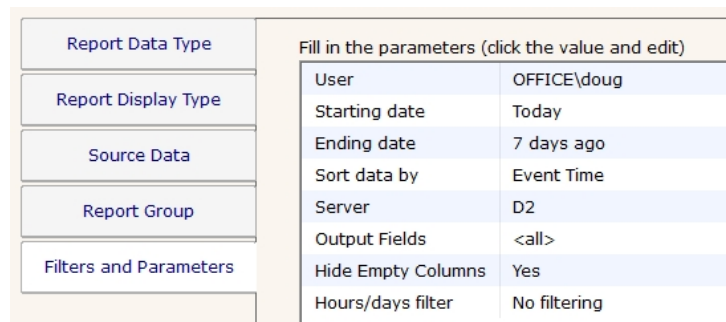
The fields that can be set include:

User
> **Select a specific user for which file activity is being reported. A list of users seen will be loaded from the database.**

Starting date:

Ending date:

Hours/days filter
> **See the** standard report tabs **for information**

Server
> **Select the server from which file activity is being reported on**

Output Fields
> **Control the size of the report by only showing the columns you are interested in**

Hide Empty Columns
> **Depending on the report settings and the information available, some fields might be empty. This setting can automatically hide columns where all values within the column are empty.**

Custom Data Set
Summarized Data

All Reports   PDF Version

Data shown for 20 Mar 2020 12:00 AM to 31 Mar 2020 11:59 PM, 98 records

Event T..	Operat..	File Name	File S..	User ..	Server Pr..
3/20/2020 1:06:35 PM	Created	K:\Customer Files\Unconfirmed 503287.crdownload	Q	127.0....	chrome.exe
3/20/2020 1:06:35 PM	Permiss... Changed	K:\Customer Files\Unconfirmed 503287.crdownload	Q	127.0....	chrome.exe
3/20/2020 1:06:35 PM	Read	K:\Customer Files\Unconfirmed 503287.crdownload	Q	127.0....	chrome.exe
3/20/2020 1:06:35 PM	Renamed	K:\Customer Files\Unconfirmed 503287.crdownload -to-> K:\Customer Files\Paycor, Inc. - 03132020Q160 - Invoice.pdf	Q	127.0....	chrome.exe
3/20/2020 1:08:24 PM	Read	K:\Customer Files\Paycor, Inc. - 03132020Q160 - Invoice.pdf	Q	127.0....	acrord32.exe
3/20/2020 1:09:00 PM	Permiss... Changed	K:\Customer Files\Unconfirmed 770209.crdownload	Q	127.0....	chrome.exe

PA File Sight - User Read/Write Amounts Report

Find user accounts that have read, written, or both more than a specified amount of data within a date range.
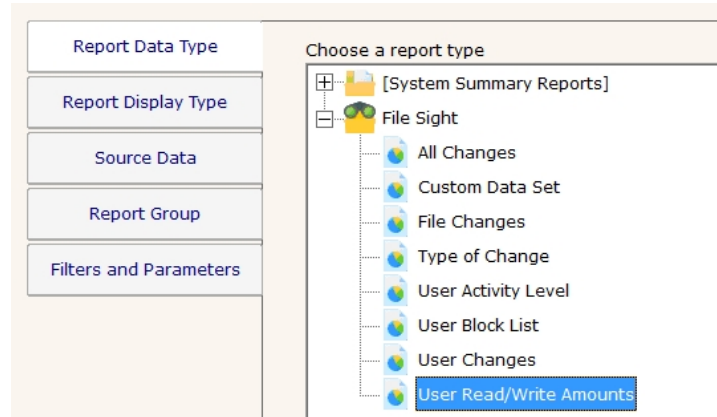
This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.
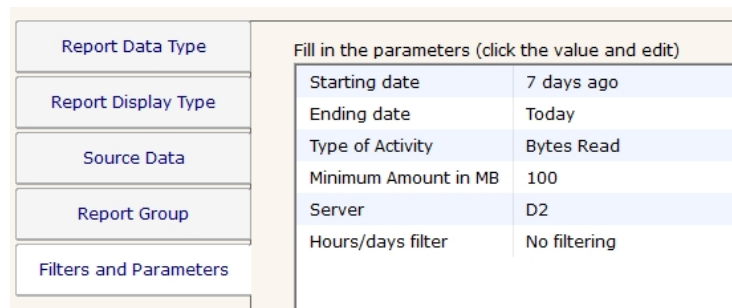
The fields that can be set include:

Starting date:
Ending date:
Hours/days filter
> See the standard report tabs for information
Type of Activity
> This field indicates whether to sum all reads, all writes, or reads and write.
Minimum Amount in MB
> The specified data transfer types (read/write) will be summed, and any user over this threshold will be displayed.
Server
> Select the server from which file activity is being reported on

Data shown for 01 Jan 2020 12:00 AM to 31 Mar 2020 11:59 PM, 3 records

User	Total ▼
▼	
████████████	634
NT AUTHORITY\SYSTEM	341
████████	313

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.
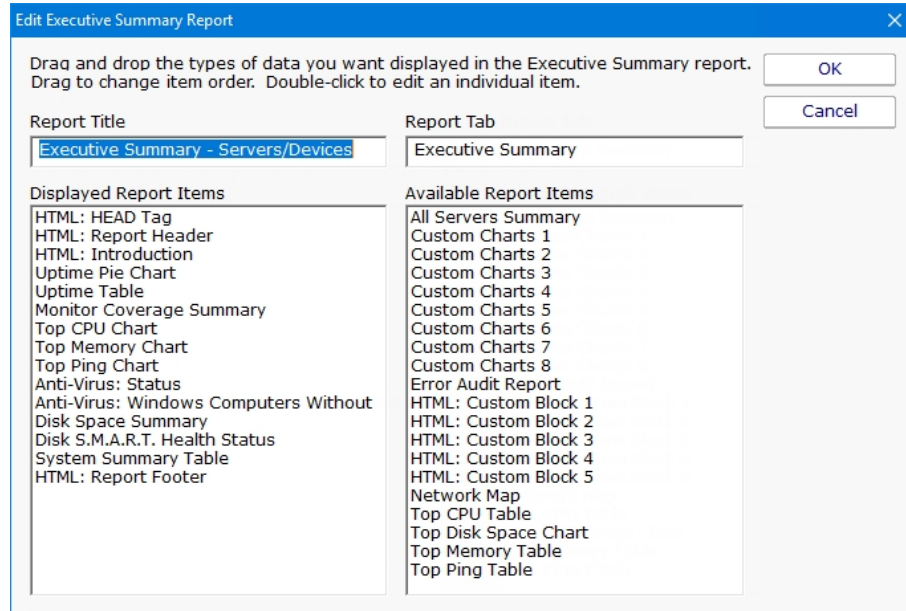
A variety of report parts can be chosen. Some are pre-built charts while others let you specify counters that should be charted. To add a report part, drag the part from the right side and drop it on the left side. Double-click the report part on the left side to set parameters for that part.

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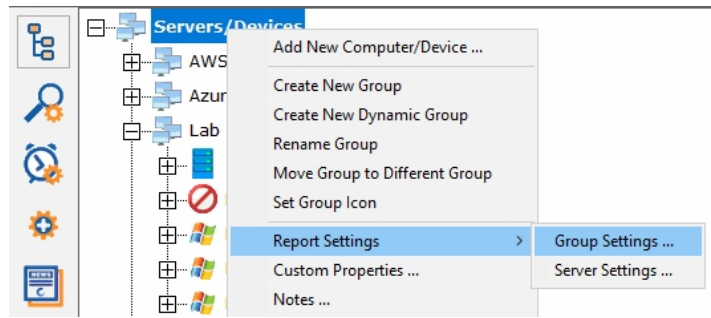
To see an even higher level view of the servers within the group, try the [All Servers Report](#) or customize the [Visual Status Map](#) report.

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.

💡
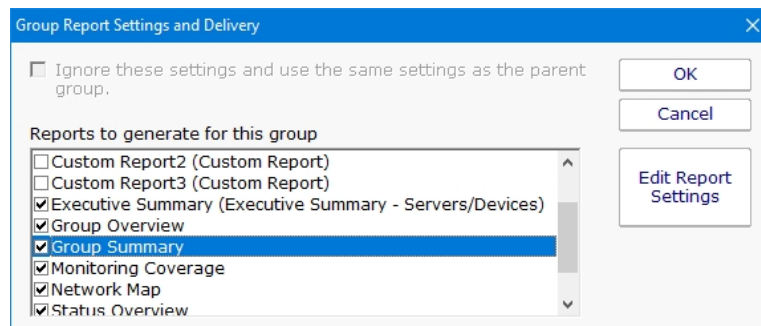
To see the most server statuses on the screen at once, use the [All Servers Report](#)

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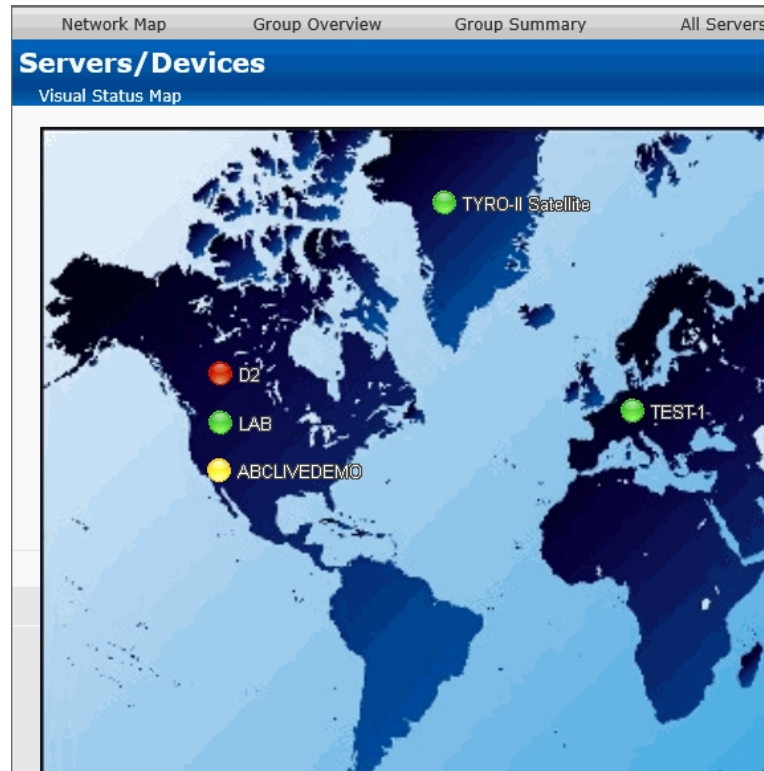
The map appearance and the positions and style of the status indicators can be configured in the Status Map Editor Dialog. There are several maps of different areas around the world, and you can also add your own map grapic.

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.

Configuration Audit Reports

This report shows PA File Sight'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.
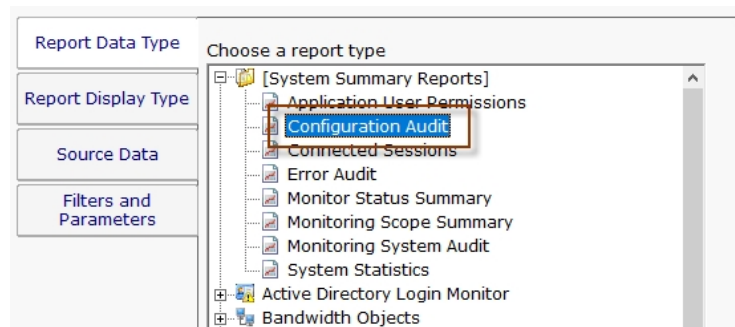
The Filters and Parameters tab is most important. A few options let you select what is included in the report; which monitor types, their actions, the monitor's configuration, and source group.
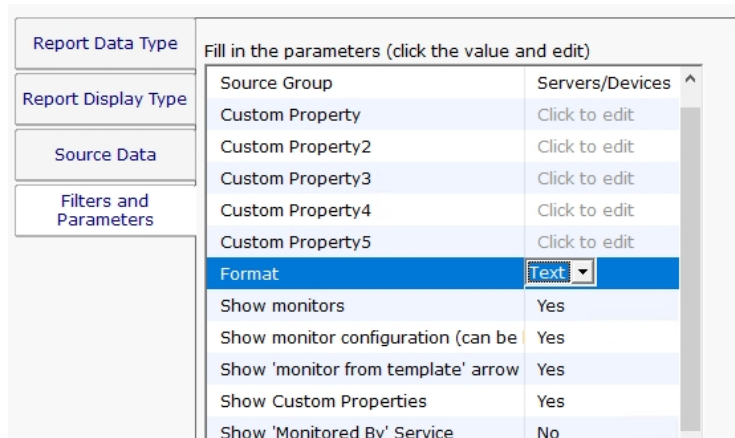
Pressing the Generate Report button will display a link indicating where the report was created. You can click the link to open the report in your browser.

```
Configuration Audit for Group Servers/Devices
04/18/17 14:28:48

[GROUP] Servers/Devices
    [DEVICE] DOMAIN2
      MONITORS:
      Critically Low Disk Space Check
        Every 3 Hour(s)
        ACTIONS:
            Do Immediately:
              Write to ServerEvents.txt log file
      Event Log Monitor
        Every 1 Hour(s)
        ACTIONS:
            Do Immediately:
              Write to ServerEvents.txt log file
      Inventory Collector
        Every 6 Hour(s)
        ACTIONS:
      Monitor services on DOMAIN2
        Every 5 Minute(s)
        ACTIONS:
```

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.
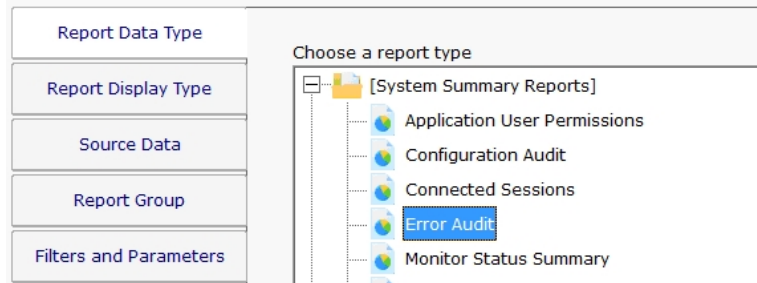
This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.

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	☐

259

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 Status Summary Report

This report lets you quickly see the current status of a set of monitors you define.
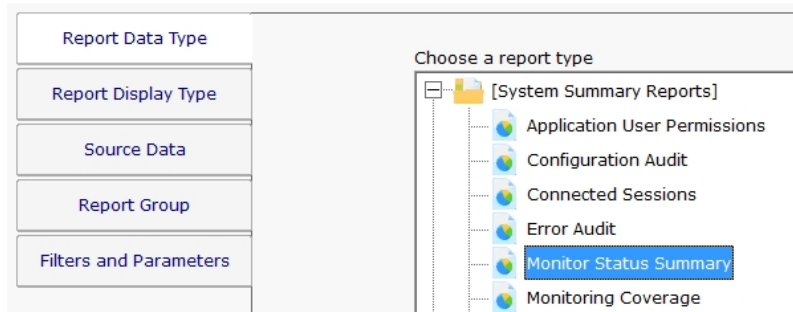
This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.

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.

261

System Statistics Report

System Statistics Report shows top level statistics about the monitoring system, including details about connections and HTTPS server information.
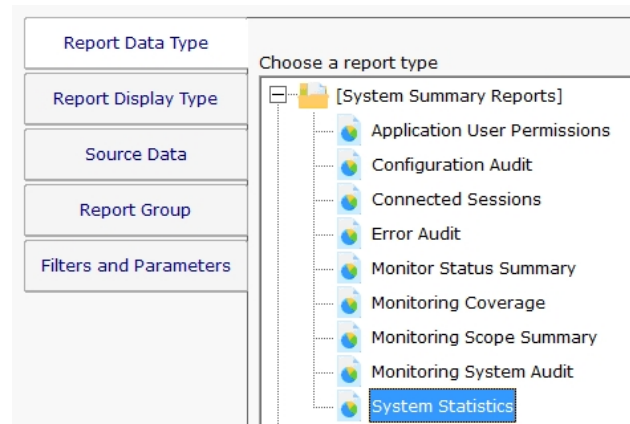
This monitor has the standard report tabs: Report Display Type, Source Data, and Report Group tabs as the rest of the monitors, and as usual, the most important settings are on the Filters and Parameters tab.

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), ...

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.
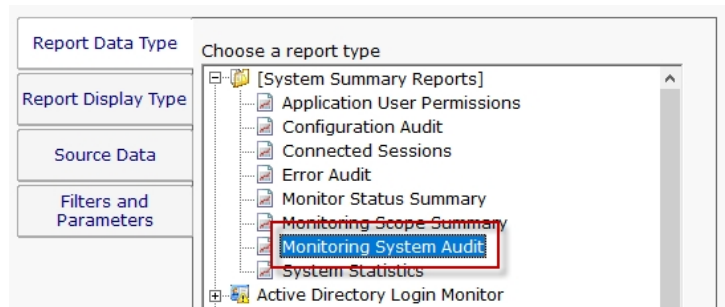
The report is located at [System Summary Reports] > Monitoring System Audit.

Configuring the report is as simple as choosing a date range, and the type of events you would like to see.

Item Selection

Select the parameters to use for the report

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

Filter: [   ]

- ☐■ Selections
  - ☑ Central Server OS Boot
  - ☐ Central Service Abnormal Stop
  - ☐ Central Service Start
  - ☐ Central Service Stop
  - ☐ Changed Auto Configuration Setting
  - ☐ Created Action
  - ☐ Created Computer
  - ☐ Created Group
  - ☐ Created Monitor
  - ☐ Created Monitor Template
  - ☐ Deleted Action
  - ☐ Deleted Computer
  - ☐ Deleted Group
  - ☐ Deleted Monitor
  - ☐ Deleted Monitor Template
  - ☐ Monitor Changed
  - ☐ Satellite Connect
  - ☑ Satellite Down

[Accept]   [Cancel]

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.

Remote Server Monitoring

PA File Sight can monitor the server it's installed on. It can also monitor other servers on the LAN by installing a Satellite Monitoring Service on them.

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 is normally installed on servers on the local LAN, but it can also be installed on servers across firewalls (including across the Internet) as long as a single incoming port is opened to the Central Monitioring Service (so the Satellite can make a secure HTTPS connection).

NOTE: The Satellite Monitoring Service is only available in Ultra product editions.
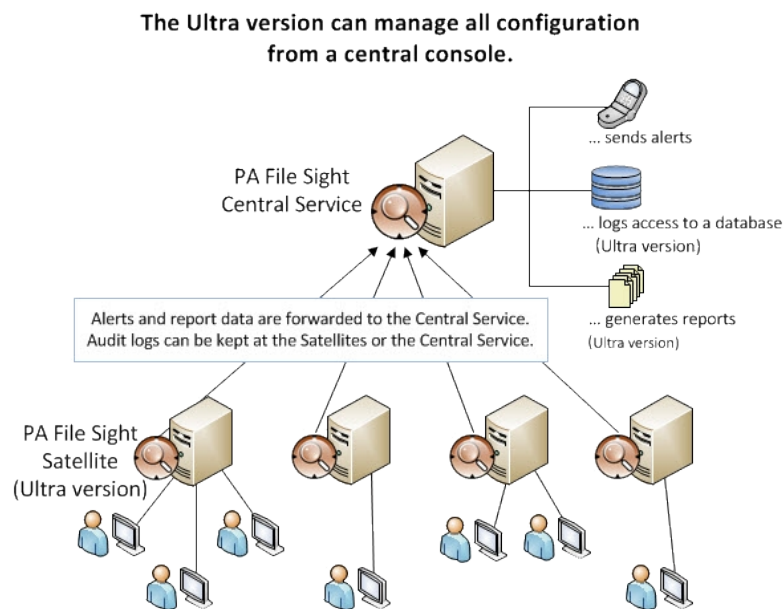
The steps to monitoring additional servers are:

1. Install a Satellite Monitoring Service on the additional servers. This is usually easiest done via Easy Deploy, though it can be installed manually as well.

2. Configure the Satellite Monitoring Service (not necessary if Easy Deploy was used)

3. Once the computers have been added, add new monitors to watch the servers. You will be able to add the new monitors as though the computers they belonged to were on the local LAN -- PA File Sight takes care of everything else.

Remote Installation Prerequisites

You must complete the following steps before installing either PA File Sight Consoles on a remote computer or Satellite Monitoring Services. These steps <u>not</u> 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 File Sight 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.
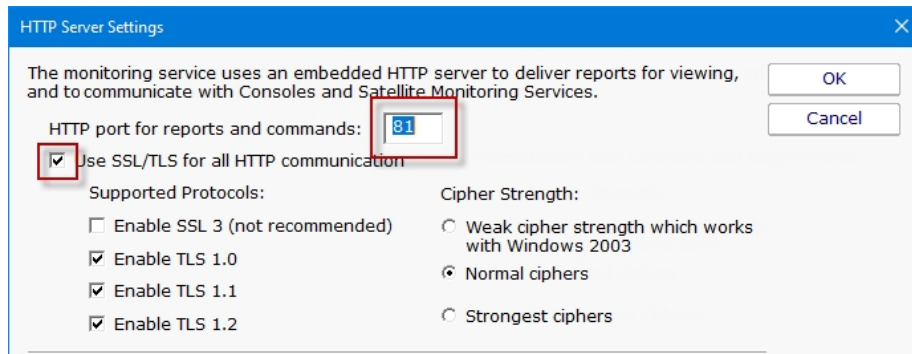
4. Select the **Use SSL for all HTTP communication** option and note the HTTP port number.

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.
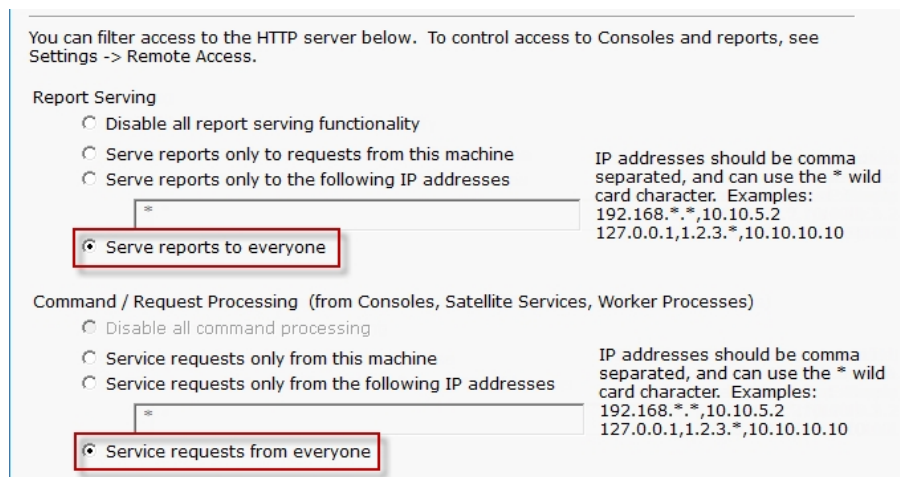
7. Click **OK** to restart the monitoring service.

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 File Sight Setup Wizard page, and then click **Finish**. The Configure Satellite Monitoring Service window will appear.

Next, Configuring a Satellite Monitoring Service.

270

Configuring the Satellite Monitoring Service

To configure the Satellite Monitoring Service
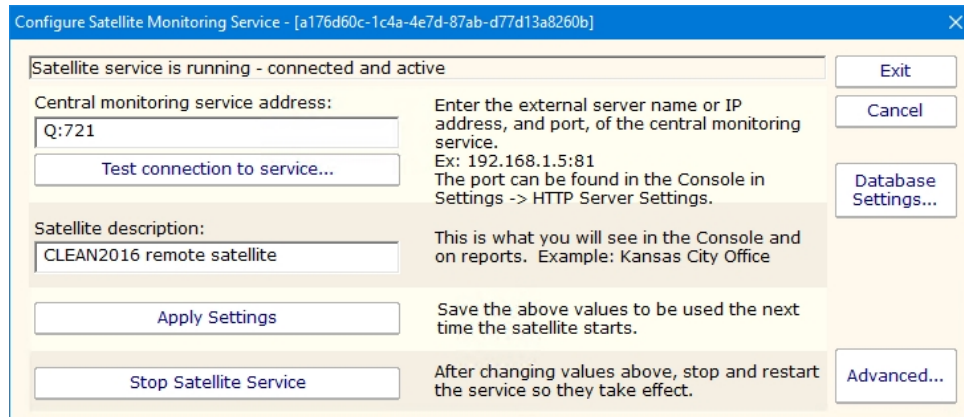
1. Enter the computer address and port of the Central Monitoring Service in the **Central monitoring service address** box. This was determined during the Installation Prerequisites.

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.

271
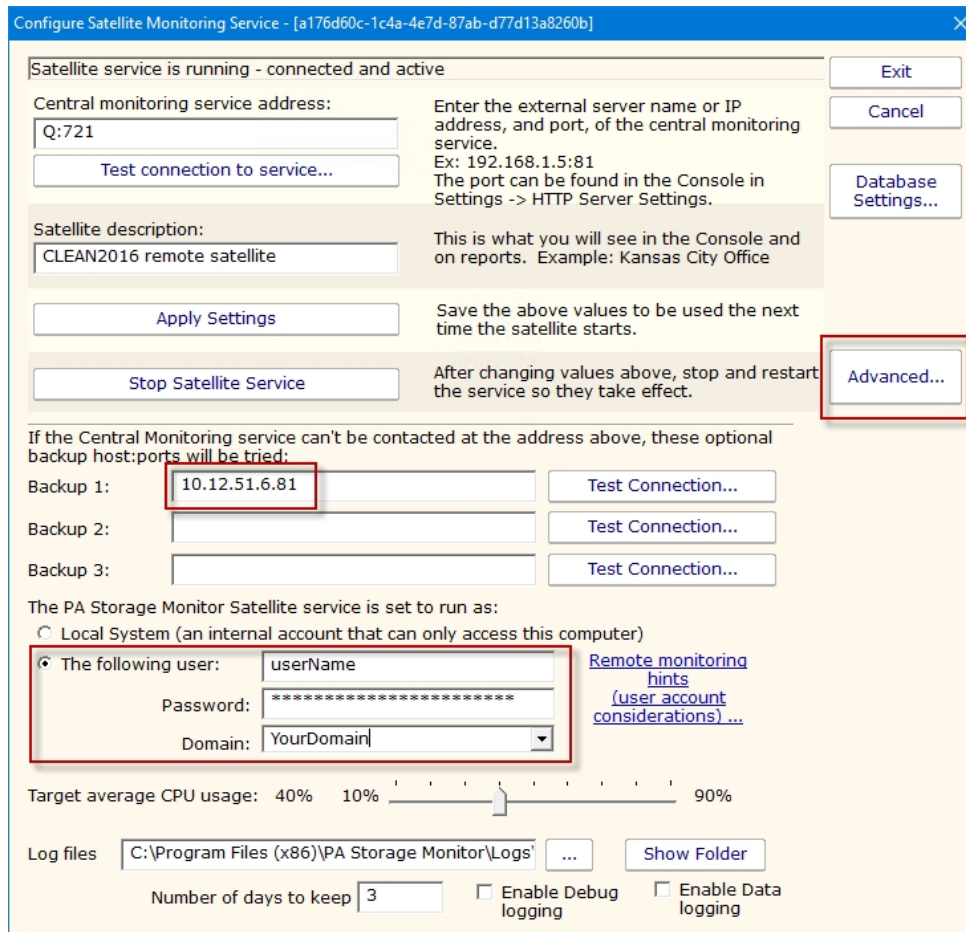
7. Click **Apply Settings** to save your changes.

8. Start a Console GUI, and then connect the console to the Central Monitoring Service. The main PA File Sight 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.
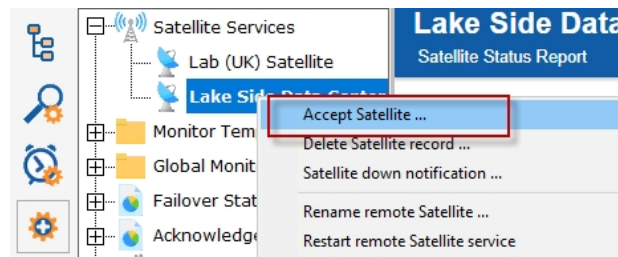
Now that the Satellite is connected to the Central Monitoring System, the system will add the computer to Servers/Devices in the Navigation Panel. You can now add and configure monitors on that computer via the Console just like you would add a monitor from the Central Monitoring System.

Satellite Operations

From within the Console, you can right-click a Satellite and see a variety of options that are described below.
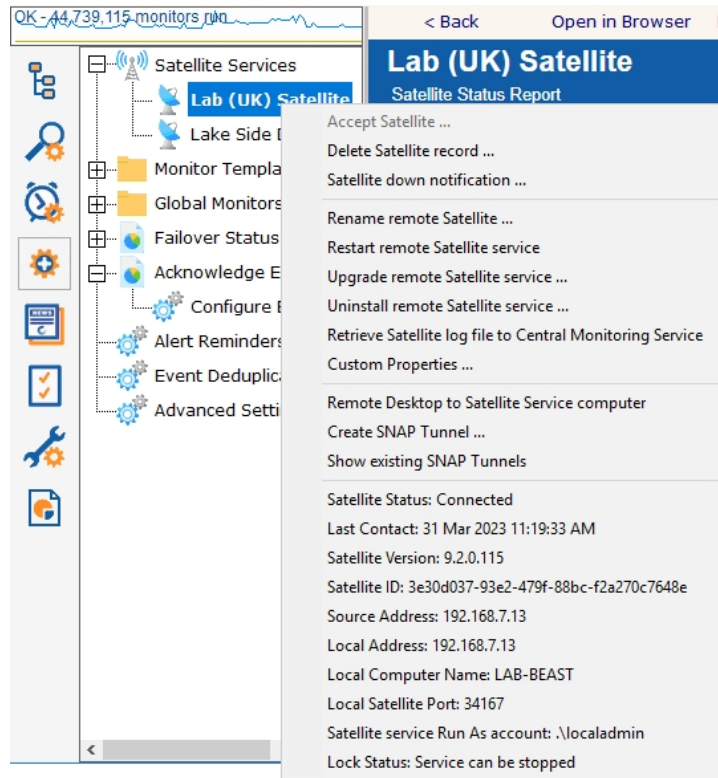
Accept Satellite - This allows a newly added Satellite to communicate with the Central Monitoring Service as mentioned in Configure Satellites.

Delete Satellite record - This removes the Satellite from the Central Monitoring Service. Computers that are monitored by the Satellite service will <u>not</u> 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.
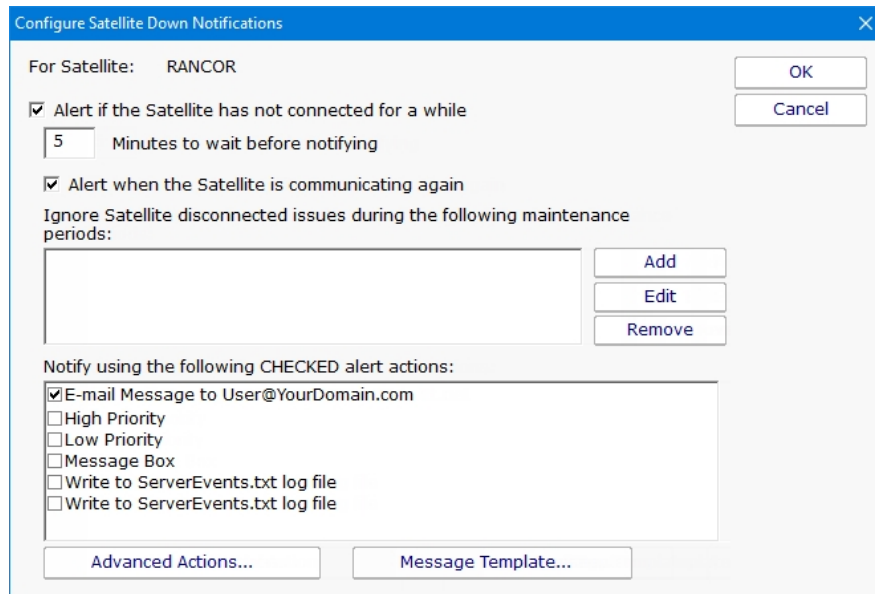
Rename remote Satellite - This option simply renames the Satellite as it appears in the Console GUI and in reports.

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 File Sight 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\PAFileSight\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\PAFileSight\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\PAFileSight\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 <u>not</u> 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 File Sight 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).
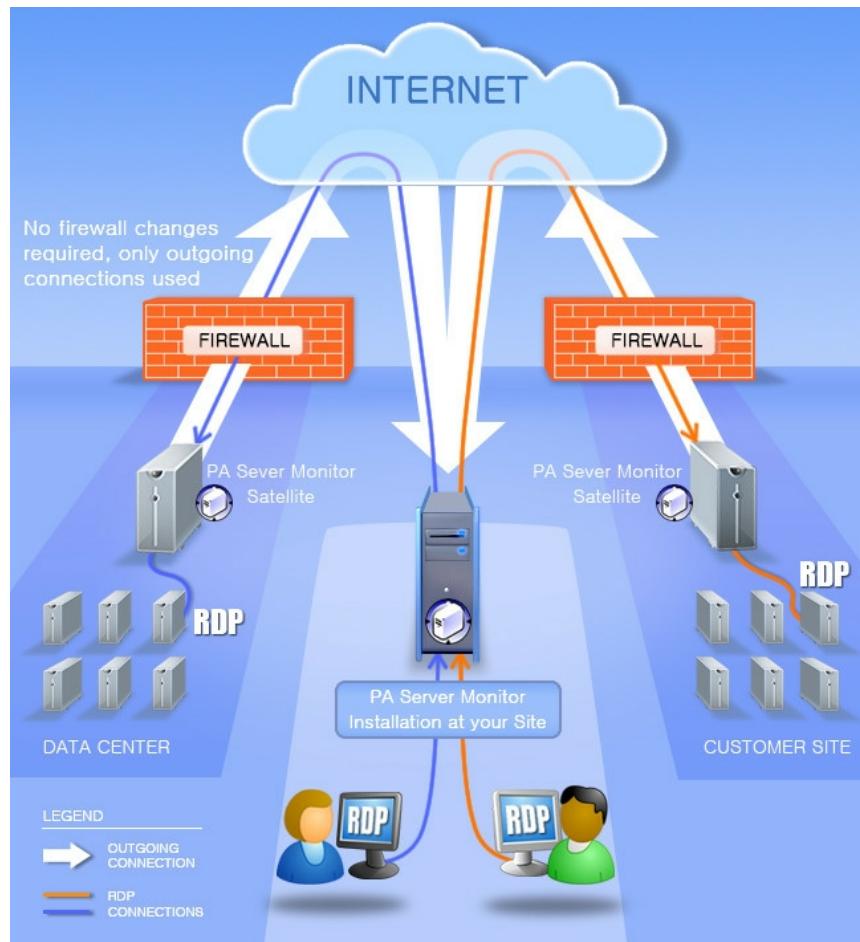
As usual, this is completely agentless -- you do not need an agent on the target server. It just has to be visible to a Satellite Monitoring Service.

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.
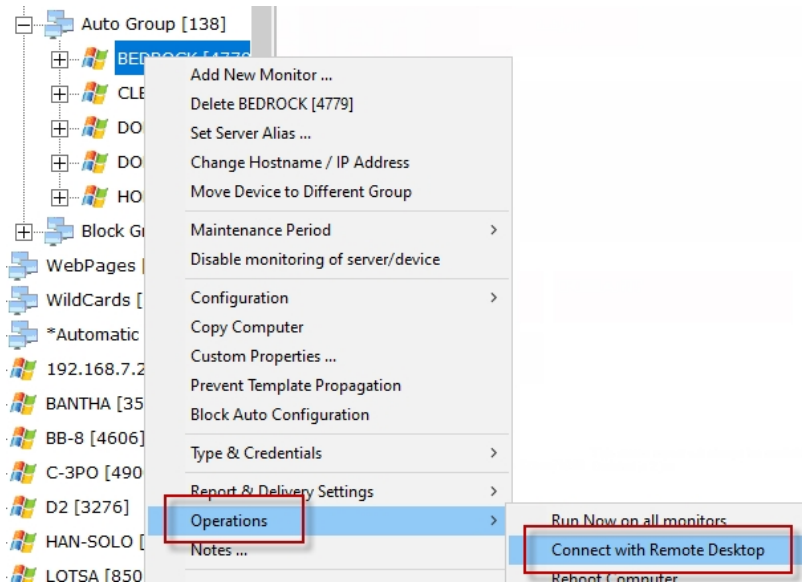
Connect to a Satellite Computer

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.
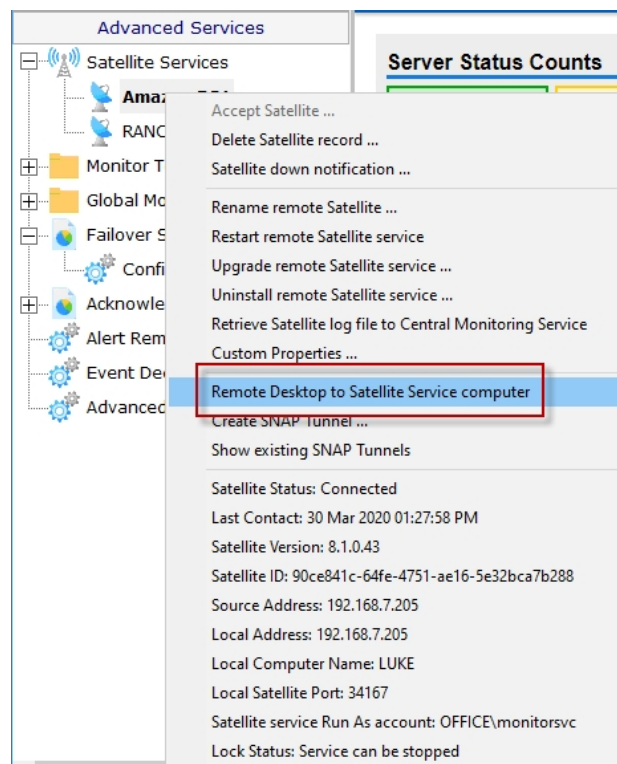
Installing Remote Consoles

The PA File Sight 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.
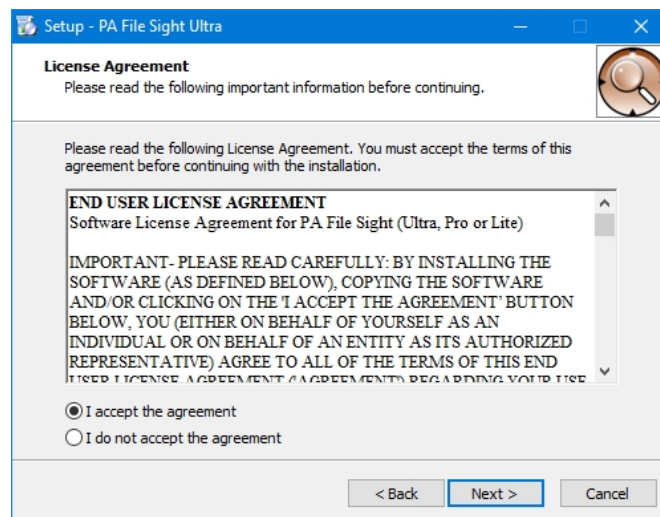
4. The License Agreement page will appear.

5. Click **Next** to advance through the wizard, accept the license agreement, select a destination location, and then display the Select Components page.
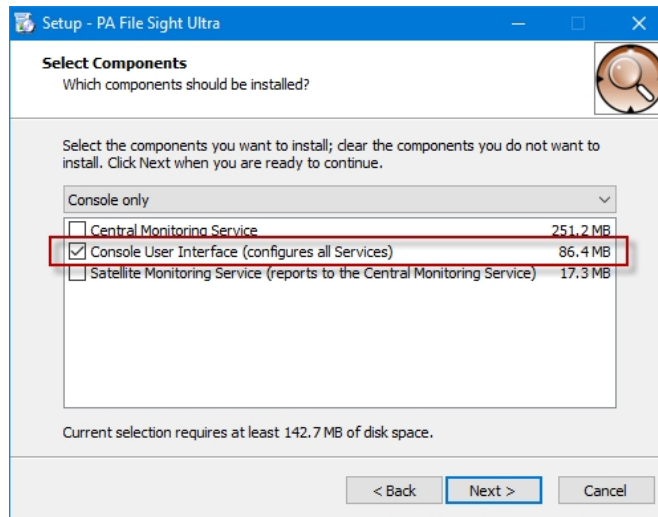
6. Select the **Console User Interface** option, and leave the other options unselected.

7. Click **Next** repeatedly while accepting all the defaults.

8. Click **Finish** to complete the installation. The PA File Sight Console connection window will appear.

Next, <u>Starting the Console</u>

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 File Sight 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.
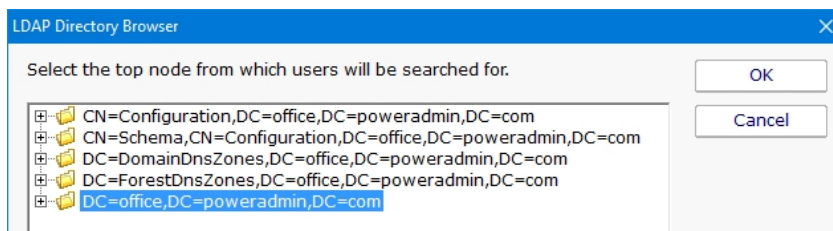
5. Choose three groups whose members will have Administrator, Run Report and View Report rights respectively. If a user is in multiple groups, they get the rights of the highest group they are in.
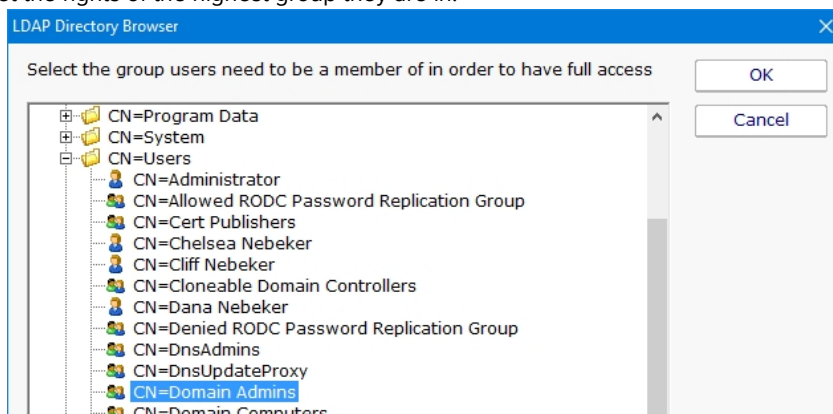
   Not all groups have to be specified as shown below.

6. Press OK to finish. The monitoring service does <u>not</u> 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 File Sight 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.

Remove users from the User Block List

Allows the specified user to remove users from the [User Block List](#).

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.
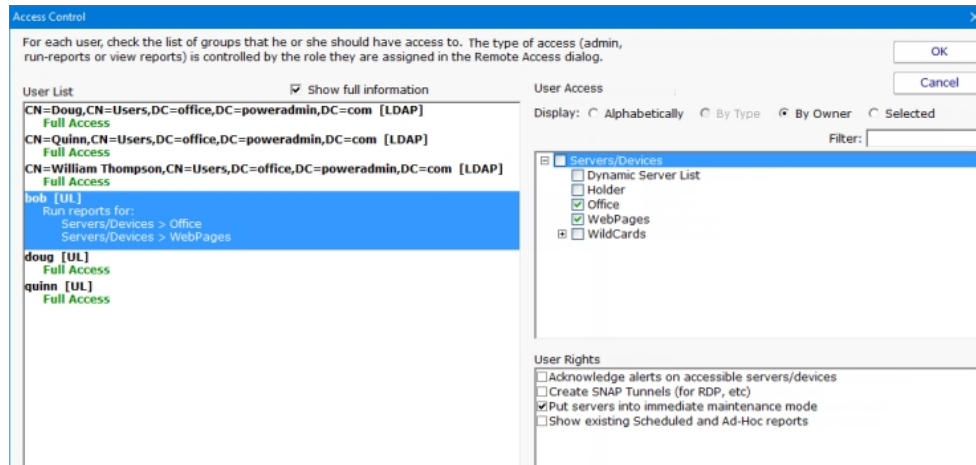
Editing

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.
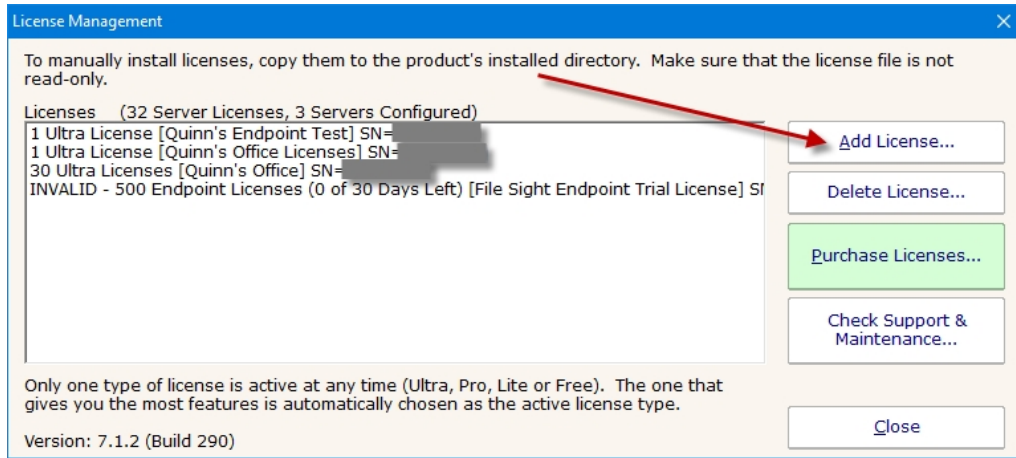
2. Then browse to where your license file is and select the file. Then select OK.
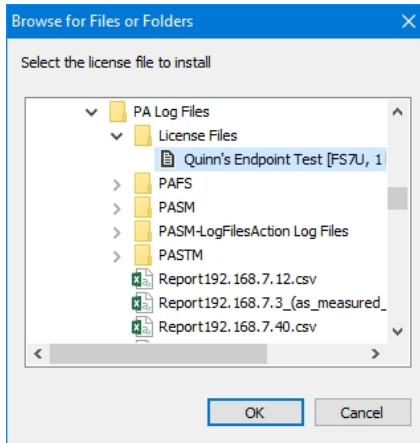
3. Select Yes to automatically upload and activate the license.
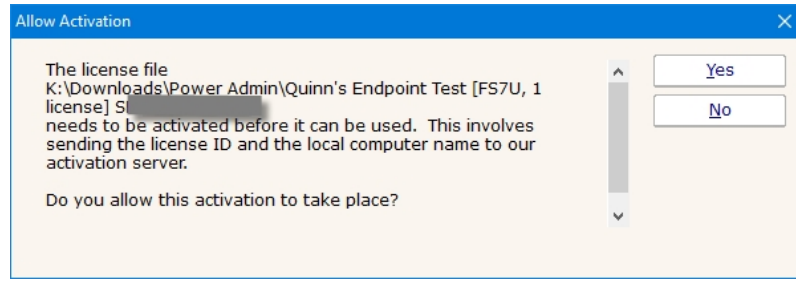
Adding License Files to the install Directory

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...
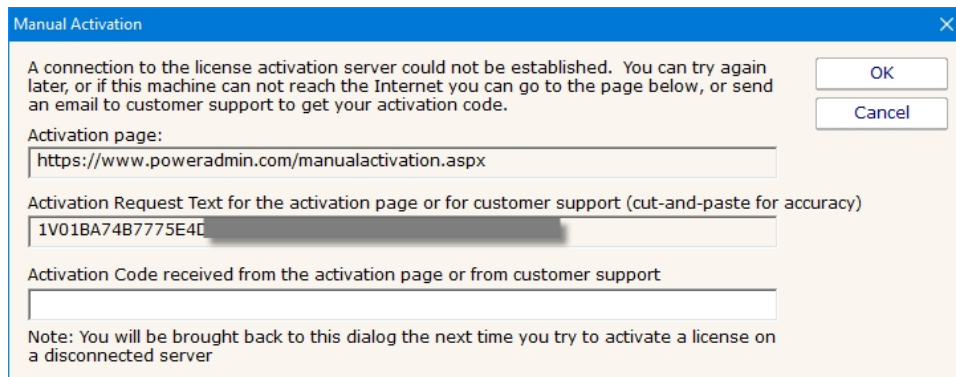
2. Follow the instructions in the Manual Activation menu to manually activate your license. Go to a machine that has Internet access and go to the URL address shown. You can highlight and copy the URL and Activation Request Text from this menu.
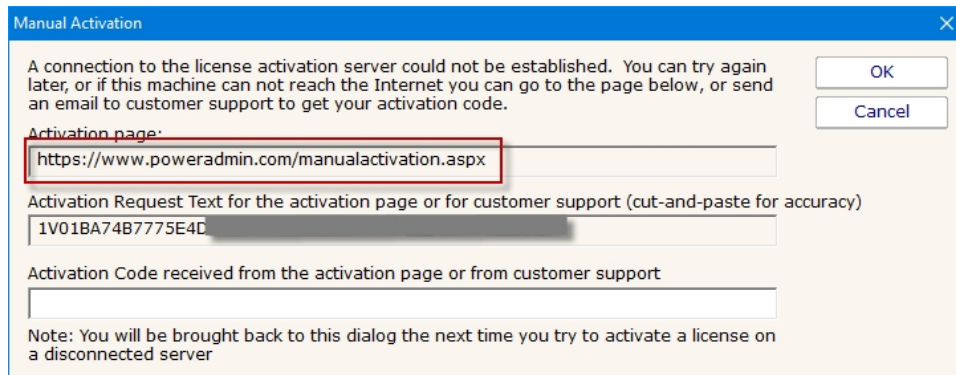
3. Copy the Activation Request Text from the menu and enter it on this webpage.

288

Manual License Activation

Thank you for activating your Power Admin product license. If you need any help please contact us.

Please enter your Activation Request Text below:

1V01BA74B7775E4D[_____] Submit

4. Then copy the Activation Code and enter it back in the Manual Activation menu and click on OK.

Manual License Activation

Thank you for activating your Power Admin product license. If you need any help please contact us.

Your activation text was:
1V01BA74B7775E[_____]

Your activation code is:
1V749[____]

Please enter another Activation Request Text below if needed:

[_____] Submit

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 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 File Sight\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\PAFileSight
```

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\PAFileSight]
"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:

```
FileSightSatellite.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 File Sight 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).

Once the Satellite is accepted the system will add the computer to Servers/Devices in the Navigation Panel. You will be able to add and configure monitors on the computer via the Console just like you would add a monitor from the Central Monitoring System.

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 File Sight

Data for PA File Sight 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.

File Access Records

The File Access Records are stored in a few key tables:

Table Name	Contains
FileSightFindings	The main table that lists file activity monitored by the File Sight monitor. IDs in this table will refer to the FileSightUsers, FileSightSourceComputerIPs, FileSightComputers and other tables.
FileSightFindingsExtra	If there was a File Sight Endpoint involved with the fiel I/O, this table lists the information available from the Endpoint. The ExtraInfoKey field will be used to link records from this table to the FileSightFindings table.
FSRCBlocked	This table lists activities that were blocked/alerted on by the Trusted Application Monitors, and any rules that were running on end-user computers that are using the File Sight Endpoint.
FSRCWarnings	This table lists warnings from the Trusted Application Monitors. These are mostly performance and configuration related.

💡

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:
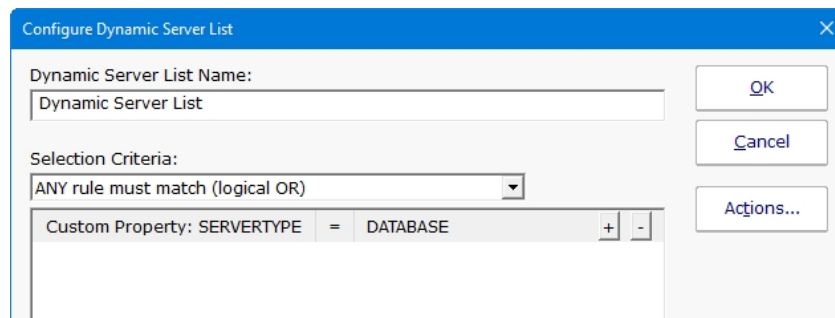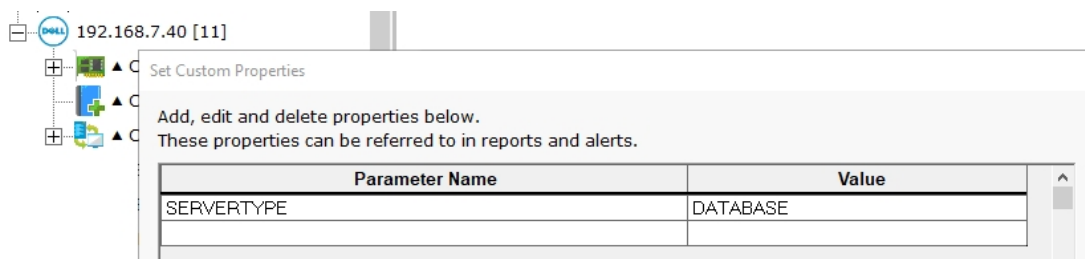
Once this Dynamic Server List is created, you can create a Dynamic Group which is based on the output of the list. Using this technique, you can arbitrarily assign any server/device to a group by setting a property on that server/device and have it automatically show up in your desired group.

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 Integrate with PA File Sight

PA File Sight 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.

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 File Sight databases for use in your own systems.

HOWTO - NIST 800-53 Compliance Solution

NIST 800-53, "Security and Privacy Controls for Information Systems and Organizations" is a recommendation from the National Institute of Standards and Technology for securing data. It is available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

PA File Sight offers powerful access and auditing capabilities for accessing files stored on Microsoft Windows file servers. See below how PA File Sight can help fulfill the requirements of NIST 800-53.

Executive Summary: PA File Sight can assist with requirements in NIST 800-53 section 3.1 (AC-2, AC-3), section 3.3 (AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11, AU-12), section 3.5 (CM-6, CM14), section 3.10 (MP-7), section 3.18 (SC-17, SC-43) and section 3.19 (SI-3, SI-4, SI-5).

3.1 ACCESS CONTROLS

AC-2 AWARENESS AND TRAINING, (g) Monitor the use of accounts
The Trusted Applications monitor can prevent access to files based on rules you create. The rules can inspect the application being used to access the files, the user account and group membership, etc.

AC-2 AWARENESS AND TRAINING, (l.12.a) Monitor system accounts for atypical usage
The File Sight monitor can alert if more than X files are accessed in Y amount of time. For example, a typical office worker might reasonably open 3-5 documents in 1 minute. If 20 documents aree read from the server within 1 minute this would signify an action that should be investigated (it could be exporting data or malware encrypting files).

AC-3 ACCESS ENFORCEMENT
AC-3 INFORMATION FLOW ENFORCEMENT
The Trusted Applications monitor can allow or prevent access to files based on rules you create. The rules are configureable and can inspect the application being used to access the files, the file itself, the location of the file, the user account and group membership, etc.

The Drive Sight monitor can block external USB drives, and the Blocked User List action can cut off access to server files completely for a specific user account when a monitor triggers a configured threshold for a user.

3.3 AUDIT AND ACCOUNTABILITY

AU-2 EVENT LOGGING
AU-3 CONTENT OF AUDIT RECORDS
AU-12 AUDIT RECORD GENERATION
When users access (read, write, move, delete) files on a server their file action is recorded in a database via the File Sight monitor. In addition, if they are denied access by Trusted Application rules, that is also recorded. The record will contain the user account, the computer/IP address where they made the request from, the target server and target file, time, full path to the file being accessed, and optionally (if the Endpoint is on the user computer) the process they used on their computer to do the file activity.

AU-4 AUDIT LOG STORAGE CAPACITY
AU-11 AUDIT RECORD RETENTION
File access records are stored in a database with a configurable time limit to control how long the records are kept. In addition, data from remote servers ("Satellites") is typically forwarded to the Central Server for storage. The optional Endpoints also forward their data to the Central Server to help protect it and keep it centralized for reporting purposes.

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES
PA File Sight has many built in measure to ensure auditing is proceeding correctly, including automatic perodic internal test procedures, various internal checking mechanisms, and configurable alerting for the occasion that a problem might be found. In addition, the monitoring is done by a Windows service which can be locked to prevent it from being stopped, even by administrator users.

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING
AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION
With the PA File Sight Ultra edition, all audit data is kept in a database. That database backs various configurable reports that can be run on demand, or which can be scheduled and automatically delivered at a specified time.

AU-8 TIME STAMPS

All timestamps are recorded in UTC (Coordinated Universal Time) and are converted to local time when displayed in reports.

AU-9 PROTECTION OF AUDIT INFORMATION

As mentioned above, audit information is forwarded to the Central Server for storage in the database. One database that can be used is MS SQL Server which had additional security and protection mechanisms. Audit records are never changed by the system, and are only deleted based on a maximum record-age setting.

3.5 CONFIGURATION MANAGEMENT

CM-6 CONFIGURATION SETTINGS

For configuration files that are stored on a Windows server, PA File Sight can monitor and alert when a configuration file is changed and record who, when and where the change was made by.

CM-14 SIGNED COMPONENTS

The Trusted Applications monitor can optionally use rules to prevent non-signed binary from being installed/saved to disk, thus preventing unvetted software from being installed.

3.10 MEDIA PROTECTION

MP-7 MEDIA USE

The Drive Sight monitor can "prohibit the use of portable storage devices" by preventing USB drives from attaching to a server.

3.18 SYSTEM AND COMMUNICATIONS PROTECTION

SC-17 BOUNDARY PROTECTION, (10, a) Prevent the exfiltration of information

The File Sight's copy detection settings, the Drive Sight monitor's ability to block USB drives, and Trusted Application monitor's ability to control which processes can read files, and to prevent writes to places such as cloud storage folders (OneDrive, Google Drive, DropBox, etc) or external drives are powerful ways to prevent information exfiltration.

SC-17 BOUNDARY PROTECTION, (24, b) PERSONALLY IDENTIFIABLE INFORMATION

The Trusted Applications feature can be configured to only allow specific executable programs from accessing protected files, which allows for monitoring and enforcing information protection.

SC-43 USAGE RESTRICTIONS

The Trusted Applications feature can be configured to only allow specific executable programs to run in an environment, also sometimes known as "application whitelisting".

3.19 SYSTEM AND INFORMATION INTEGRITY

SI-3 MALICIOUS CODE PROTECTION

The Trusted Applications feature allows for rules that defined what a 'good' program is (signed by a well known software company for example), and can prevent any programs that do not meet the rules from being able to start.

SI-4 SYSTEM MONITORING

The File Sight monitor has the ability to watch for a specified number of reads AND writes happening from any user account within a short amount of time. This activity is usually done my ransomware as it has to read a file into memory, encrypt it, and then write it back to disk. By detecting this behavior the user account can be immediately blocked from the server and alerts sent to the IT team to investigate.

SI-5 SECURITY ALERTS, ADVISORIES and DIRECTIVES

All of the monitors within the PA File Sight product have the ability to send alerts, including via email, SMS, web hook, scripts and pop-up messages.

HOWTO - NIST 800-171 Auditing and Accountability Software Solution

NIST 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" is a recommendation from the National Institute of Standards and Technology for securing data. It is available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

PA File Sight offers powerful access and auditing capabilities for accessing files stored on Microsoft Windows file servers. See below how PA File Sight can help fulfill the requirements of NIST 800-171.

Executive Summary: PA File Sight can assist with requirements in NIST 800-171 section 3.1 (3.1.1, 3.1.3, 3.1.11, 3.1.21) and section 3.3 (3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.3.6, 3.3.7, 3.3.8, 3.3.9)

3.1 ACCESS CONTROLS

Section 3.1 of the document discusses access controls. See below for how PA File Sight can help with specific requirements.

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)
...and...
3.1.3 Control the flow of CUI in accordance with approved authorizations
> The Trusted Applications monitor can prevent access to files based on rules you create. The rules can inspect the application being used to access the files, the user account and group membership, etc.

3.1.11 Terminate (automatically) a user session after a defined condition
> The Block User List action can be triggered by any monitor, and when a user is on that list, they are prevented from accessing any files on the Windows servers where PA File Sight is protecting file structures.

3.1.21 Limit use of portable storage devices on external systems
> The Drive Sight monitor can prevent USB drives from attaching to the system, thus preventing data getting copied to them. The Trusted Applications monitor can also prevent files from being written to USB drive as well as common cloud drives (OneDrive, Google Drive, DropBox, etc).

3.3 AUDIT AND ACCOUNTABILITY

3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity
> The File Sight monitor can record who accesses files (user account, from which computer/IP) on the server, and with the optional Endpoint you can also see which process was used on the user's computer, as well as if the file was then written out (a copy operation). Operations that can be recorded include file reads, writes, moves and deletes.
>
> In addition, the Trusted Applications rules can be triggered not only on failed access (when access is prevented) but can also be used to record access to the database for later reporting.
>
> When using the Ultra version of PA File Sight, the collected data is kept in a database which can be used for running reports later during audit investigations.

3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions
> When PA File Sight records a file I/O operation, it records the user account used and also includes the user's IP address from which they requested file data.

3.3.3 Review and update logged events
> As mentioned, PA File Sight's Ultra Edition records monitoring data to a database. Ad hoc reports can be run to view the data. It is also often helpful to schedule daily or weekly reports to be reviewed by personnel. These reports can be viewed via web browser or emailed in PDF form.

3.3.4 Alert in the event of an audit logging process failure
> PA File Sight has many built in measure to ensure auditing is proceeding correctly, including automatic perodic internal test procedures, various internal checking mechanisms, and configurable alerting for the occasion that a problem might be found. In addition, the monitoring is done by a Windows service which can be locked to prevent it from being stopped, even by administrator users.

3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity

Reports in PA File Sight make it simple to see who interacted with specific files, or to see all file activity performed my a specific user during a specific time period. This aids in analysis and correlation of unauthorized activity.

In addition, alert thresholds can be created to monitor for unusual activity levels, such as a high level of data file read activity, or a high number of file deletes.

3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting

Besides scheduled reports which can be scheduled for any timeframe, ad-hoc or one-off reports can be quickly run to support on-demand analysis.

3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records

PA File Sight relies on the Windows system clock for timestamps. Windows computers can be configured to use an NTP time source to provide accurate time. In addition, PA File Sight has a built in periodic check to detect if the system time is ever tampered with (moved forward or backwards).

3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion

Access to the PA File Sight software can be configured to require a login, even on the local host where it is installed. The monitoring service can be locked such that it cannot be stopped.

Audit data is stored by default in local database files, and it can also be configured to be stored in a Microsoft SQL Server database with all of the security protection that product provides. In addition, when remote "Satellite" servers are monitored, their auditing data is forwarded to the "Central" server for data storage, so the auditing data is not even necessarily on the target server.

3.3.9 Limit management of audit logging functionality to a subset of privileged users

PA File Sight supports multiple logins for multiple users, and each user can have different rights in the system (just view reports, run reports, and administrative access). In addition, if many servers are monitored, access to specific servers can be locked down to specific personnel.

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 File Sight installation for sending email alerts.

Note: The below steps are supported in PA File Sight version 8.5 or newer.

Register PA File Sight in Azure Active Directory

> 💡
>
> If you have multiple installations of PA File Sight, 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:
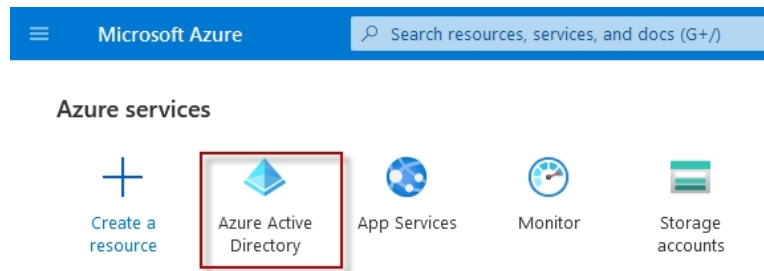
Once you are in Azure Active Directory, click on App Registrations found on the left side.
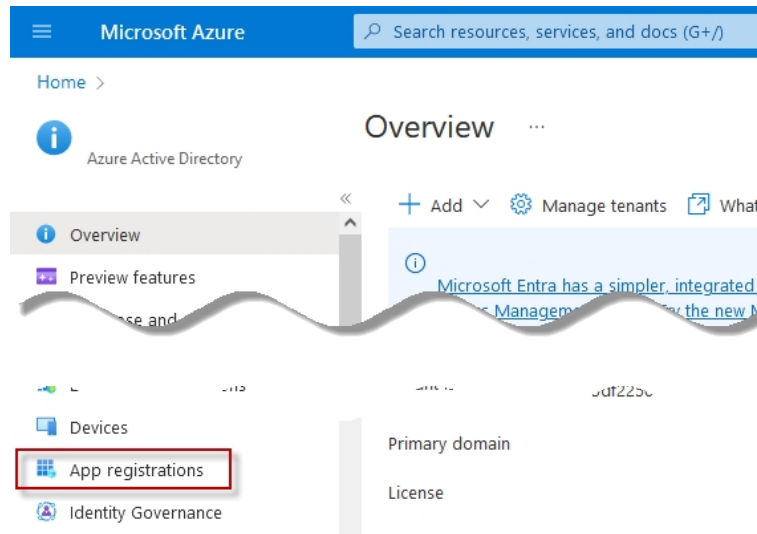
Click New Registrations near the top.

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 File Sight 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
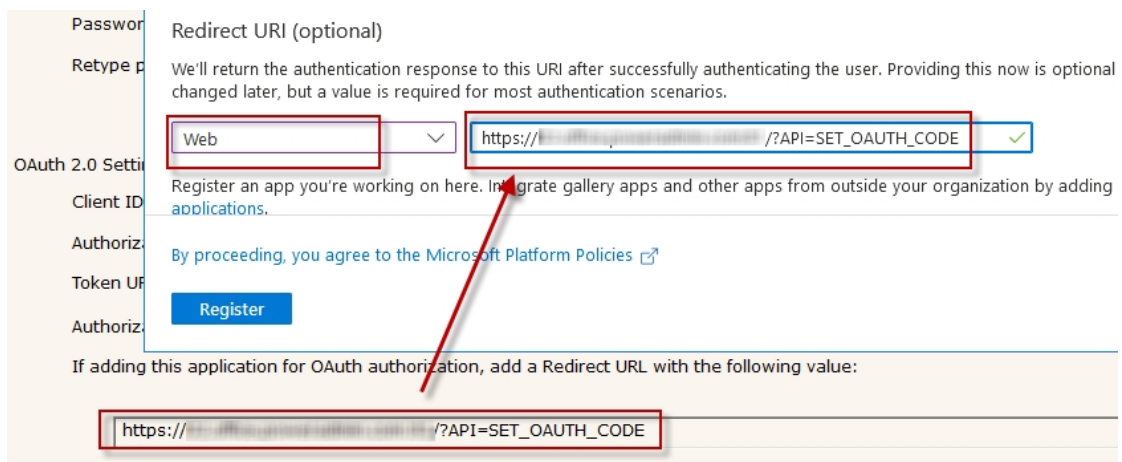
Application Values

Now copy the Azure Application (Client) ID to the Client ID field in the Email Action.
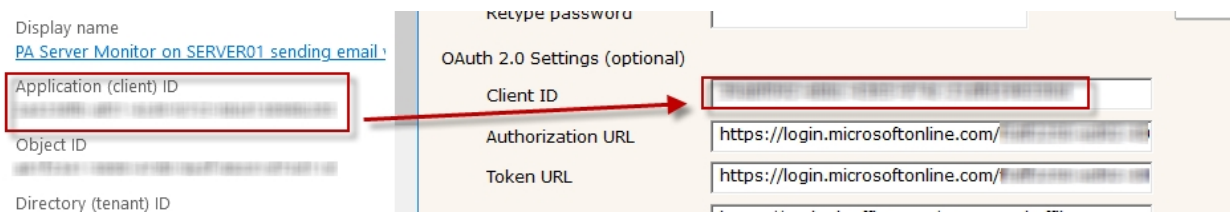
To get the Email Action's Authorization URL and Token URL values, click the Endpoints button in the Azure Application Registration, and copy the URLs on the right.
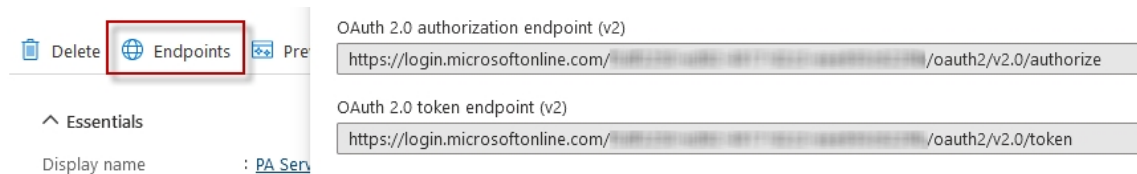
Application Scope

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.
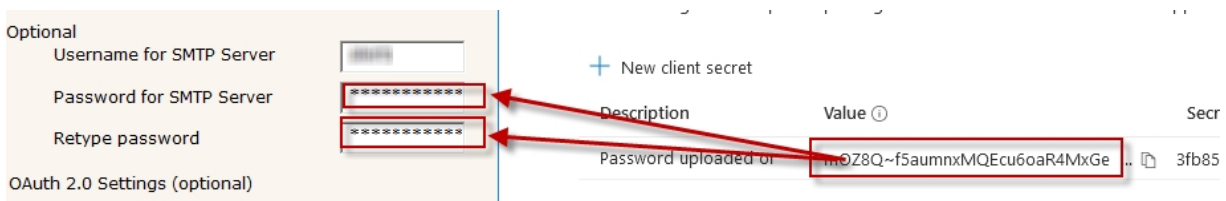
API Permissions (for POP3 or IMAP)

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.
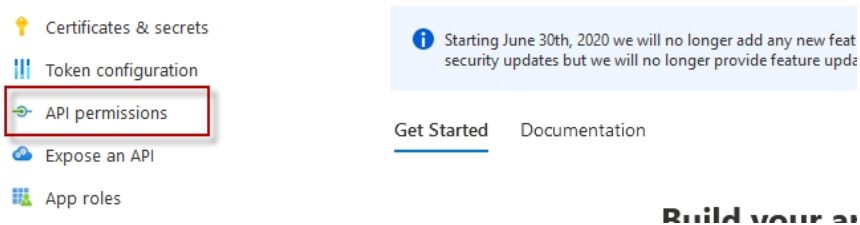
Click "Add a permission", and then on the left the "APIs my organization uses". Enter "office" in the search box and then select "Office 365 Exchange Online".
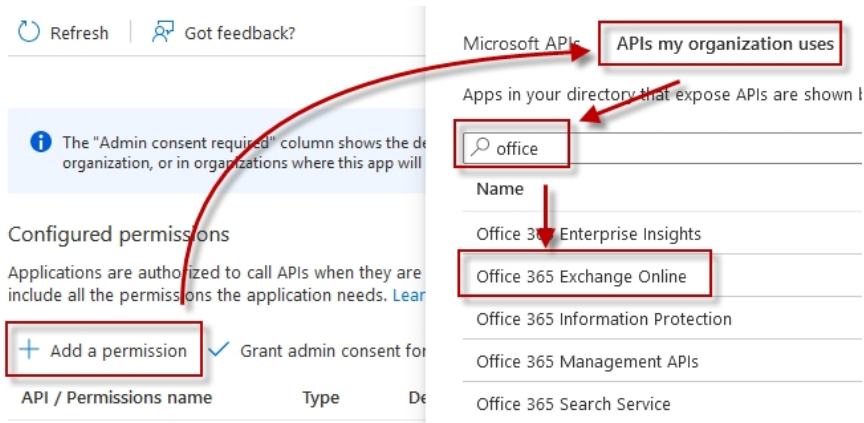
Select Applications Permissions on the left side.
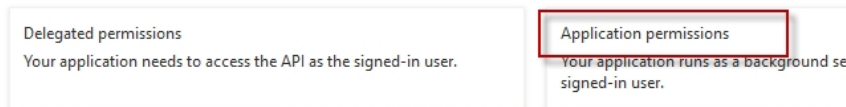
Scroll down and select "IMAP.AccessAsApp" and/or "POP.AccessAsApp" as required, and then click "Add Permissions" at the bottom.
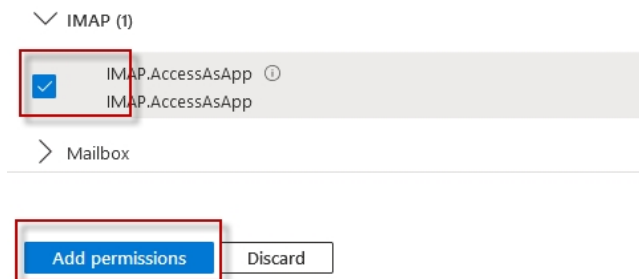
Authenticating with OAuth 2.0

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).
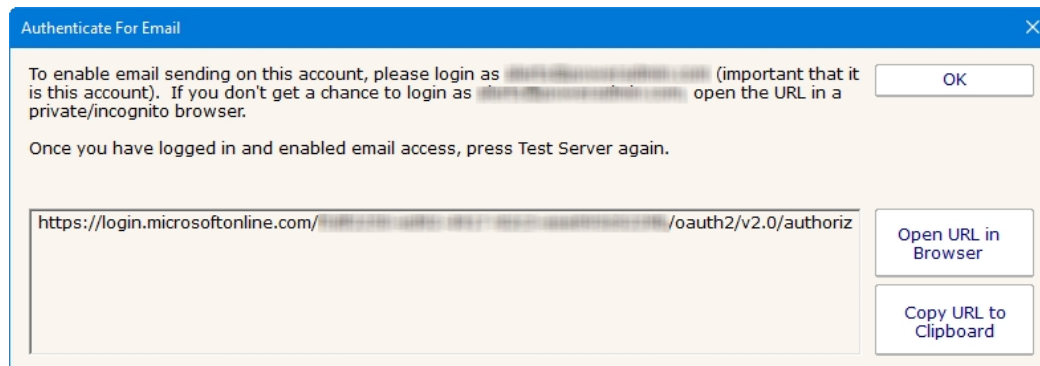
The shown authentication URL needs to be visited and logged into in a brower. You can either copy the URL and open a browser yourself, or press the Open Browser button. Be sure to login with the requested account (the account that will send emails).

> **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\PAFileSight
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 Shrink Database Files

PA File Sight 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 File Sight\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 File Sight service and run:

    C:\Program Files\PA File Sight\FileSightSvc.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:
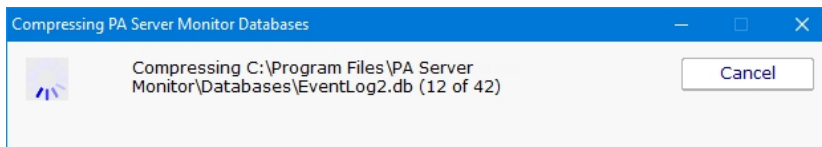
When the compressing step is finished, you should start the PA File Sight service.

How to Integrate with Slack

Integrating with Slack is very easy with PA File Sight. 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 File Sight",
"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 File Sight",
"text":"$Date$ $Time$\nComputer: [$Machine$]\nMonitor: [$MonitorTitle$]\nDescription: $Details['"',' ']
[80]$\n\n$MonitorMsg$\n$TimeInError$\n\n$SentFrom$",
"icon_emoji":":$Status["msOK","white_check_mark"]["msALERT_RED","no_entry"]["msALERT","warning"]$:"
}
```

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

PA File Sight 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 File Sight\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 File Sight\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 File Sight 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 File Sight\CA\openssl.cnf
   ```

   The conversion command:

   ```
   "C:\Program Files\PA File Sight\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 File Sight\CA\SSL_PRIVATE_KEY.pem

3. Save the SSL certificate to
   C:\Program Files\PA File Sight\CA\SSL_CERT.pem

4. PA File Sight will need to know the password for the private key. You can specify this by running the following command:
   ```
   "C:\Program Files\PA File Sight\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 File Sight\diag.exe" /SETCONFIG=SSLCertPKPW:
```

5. Restart the PA File Sight service and it will now be using your SSL certificate.

Create your own new certificate

1. Go to the C:\Program Files\PA File Sight\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 File Sight\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 File Sight\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 File Sight\openssl.exe" req -newkey rsa:2048 -keyout "C:\Program Files\PA File Sight\CA\NewCert\SSL_PRIVATE_KEY.pem" -keyform PEM -out "C:\Program Files\PA File Sight\CA\NewCert\SSL_CERT_CSR.csr" -outform PEM -rand "C:\Program Files\PA File Sight\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 File Sight\openssl.exe" req -in "C:\Program Files\PA File Sight\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 File Sight\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 File Sight\CA**NewCert**\SSL_PRIVATE_KEY.pem
    into the CA folder.

11. PA File Sight 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 File Sight the password by running the following command:

    ```
    "C:\Program Files\PA File Sight\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 File Sight service and it will now be using your SSL certificate.

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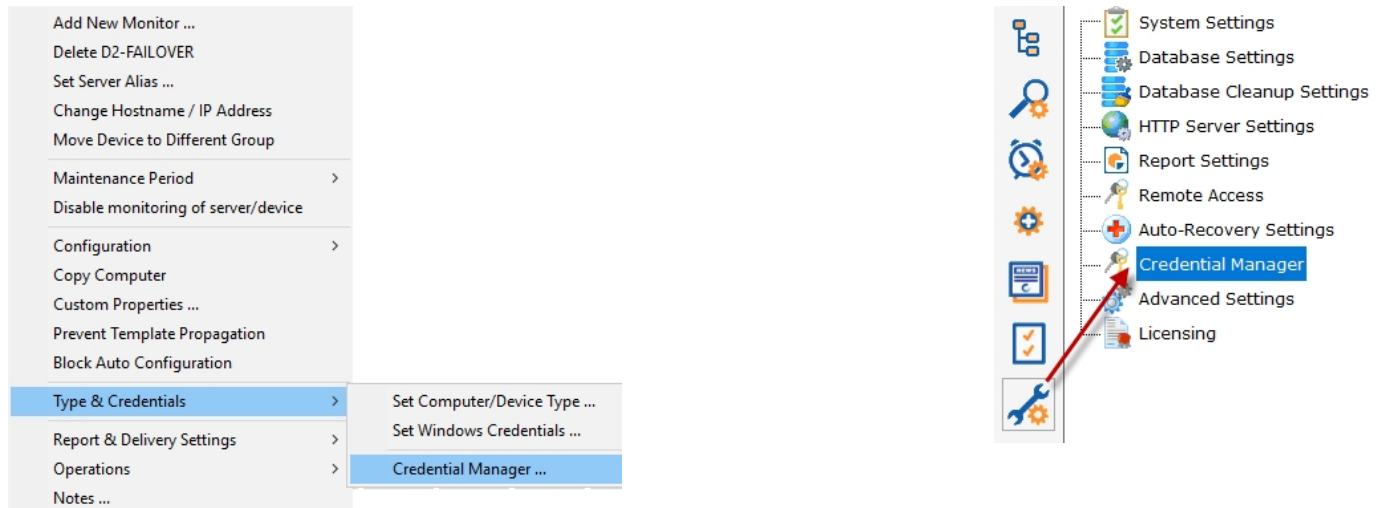
Credentials are groups into different types. Sometimes credentials are used by multiple devices. In this case the credential is attached to a single device, and the other devices point to that single device. The check box at the top toggles between viewing these two scenarios.

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.

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.

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.
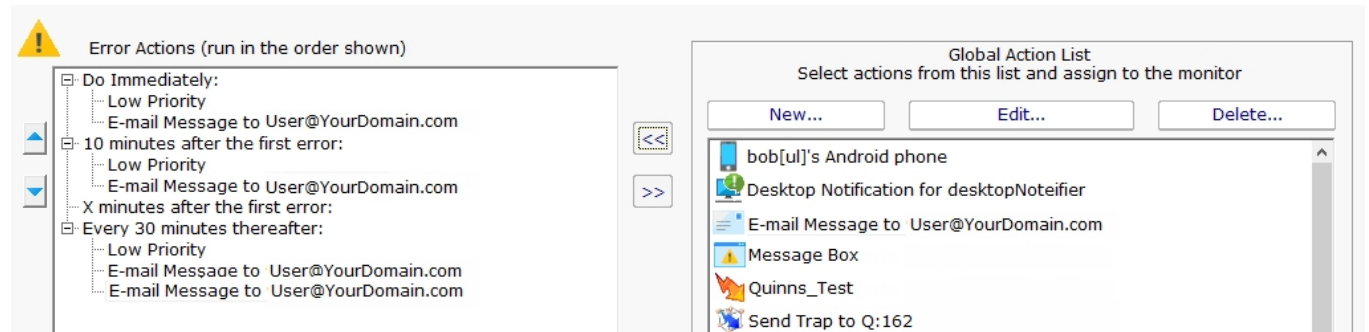
You may configure a particular escalation group by first clicking on the Escalation node to select it. This configuration may consist of changing the time at which the escalation group's actions are activated. You can configure an escalation period by hand editing the time shown in it. To do so, press 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 File Sight will always revise the text to read "XX minutes after the first error:" once you close the editing of the node. A non-minutes value will be normalized to the correct number of minutes (for instance, "1 hour" becomes "60 minutes after the first error.") The escalation groups will be visually re-sorted in the order of the times that they contain when you complete your editing.

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

See Adding Actions for additional information.

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

Trusted Applications (Application Whitelisting) Concepts

Trying to prevent malware attacks is difficult because the malware is always changing. Anti-virus and other security products attempt to keep up with changing file signatures and behaviors, but this means they are always slightly behind because they have to analyze a new malware before they can protect against it.

An alternate approach is to use Application Whitelisting, which is a way of specifying which applications should be able to run and access files. Any process which is not on the list doesn't get to run. This will be a smaller, and most importantly, a finite set for any given computer.

PA File Sight does Application Whitelisting with a Trusted Applications approach. The system administrator defines rules that define which applications can run, and which files they can access. The second point, defining which files can be accessed, is critical as there are many applications that are perfectly safe and valid when used properly, but can also be used in nefarious ways such as Powershell, the command shell, etc. By controlling which files these trusted applications can read (to read a script file as input for example), system security can be greatly enhanced.

The Trusted Application feature of PA File Sight looks at every file access (read, write, delete, move/rename) that takes place on a computer and looks at data about:

○ Attributes of the file being accessed

○ Attributes of the process that is accessing the file

○ The user account running the process

With these sets of information, rules can very quickly be run to determine whether the file access should succeed or not. If the rules are not met, the access is blocked, with optional alerting and logging.

An important concept to understand is that before a process starts, it is initially read into memory as a file (by whatever process is staring the new process). So the FILE_xxx statements will first be applied to it, and then once it is running, the PROCESS_xxx statements will apply as the process reads in additional files.

For example, double-clicking Notepad.exe from Explorer.exe will cause:

Explorer.exe (process) to read Notepad.exe (file) as part of loading and starting the Notepad.exe process
... then ...
Notepad.exe (process) will read additional files

Stopping a process before it starts is usually done by blocking Reads of the process file with FILE_xxx rules.

PA File Sight Ultra can protect servers (both where the Central Monitoring Service and Satellites are installed) as well as client computers where the optional Endpoint is installed.

Next, read about the Trusted Lists.

Day to Day Operations with Trusted Applications (Application Whitelisting)

Once you have the Trusted Applications feature up and running, and blocking access when it is not allowed, the day to day operations become fairly simple.

Watch Alerts

It is important to receive alerts when file access is blocked. Ideally, only malware would be blocked so file access alerts should be rare. If you get alerts that aren't malware, it might be a user trying to run a legitimate application that hasn't been allowed yet.

Allowing Legitimate Applications

Typically you'll see an alert about a blocked (or test-blocked) application in the Access Warnings dialog. Since typical rules will allow access to files from the Trusted Applications list, the easiest thing to do is add the blocked application to the list. This can be done by clicking the green button as shown in the image below:
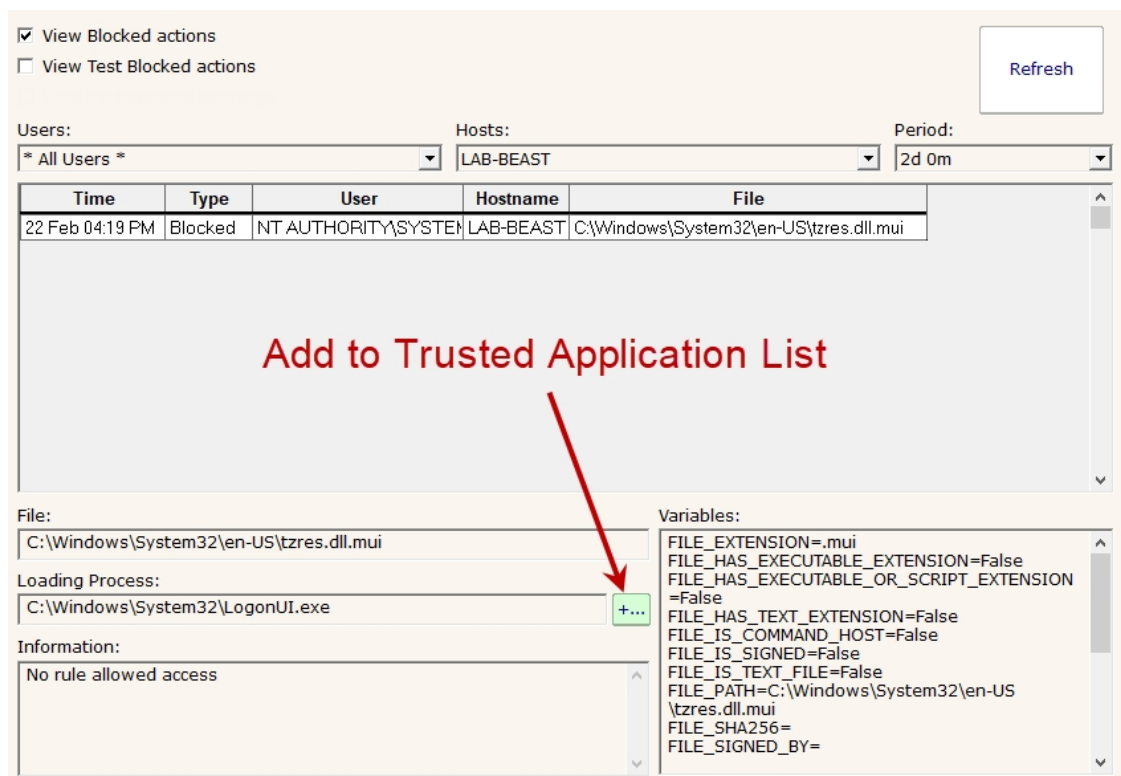
Clicking this button will send a query to the Central Service, Satellites, and Endpoints to get a list of signers, file sizes and file dates for that particular file. If the next attempt to launch matches those criteria, the application will be trusted and allowed to run.

To make warnings easier to look at, other warnings coming from the same application will be cleared since they probably wouldn't have happened now that the application is in the Trusted Application List.

Other Ways to Allow Legitimate Applications

Besides clicking the green button on the Access Warnings dialog as shown above, there are three other ways to allow legitimate applications to run:

320

Use the Trusted Publishers List

Any application that is digitally signed by a company in the Trusted Publisher's list can run based on one of the default rules. So adding to the Trusted Publishers list is an easy way to allow many legitimate applications. The <blue>Getting Started</blue> page suggested sending a command to the Central Server, Satellites and Endpoints to automatically scan and load the Trusted Publishers list with all digital signers for software currently installed.

Add a Rule for the Application

It is possible to add a specific rule for an application, such as:

```
(FILE_PATH = "C:\Program Files\MyApplication\*") OR (PROCESS_PATH = "C:\Program
Files\MyApplication\*")
```

This can become hard to manage, so the next idea is a better suggestion.

Use Custom Lists

Use one of the Custom Lists to keep track of applications or application folders that need to be able to run (often because they are not digitally signed), and then create a rule that allows software in the Custom List to run. For example, this custom list:

and this associated rule would allow applications in the above folders to run:

Note that the title of the rule can be anything - just the rule itself needs to refer to the Custom List name.

Pausing Rules

There might be times when the Trusted Application Rules need to be temporarily turned off such as when new software is installed or upgraded. To do this:

- For the Central Server or Satellites: Go to the Trusted Applications monitor, and specify how long rules should be paused and then press the Pause Rules button.

- For Endpoints: Go to the Endpoint Operations page, select/filter to those Endpoints that need to be operated on, and click the Paused Trusted Application Checking button at the lower right corner. This will pause checks for 15 minutes. Each time the button is clicked, the 15 minutes for the selected Endpoints is reset.

Getting Started with Trusted Applications (Application Whitelisting)

There are a few steps to take in preparing for monitoring for and using Trusted Applications. Follow the guide below to get everything configured correctly. These steps will probably be spread out over a total of a few days.

Security Applications

Go to the Security Applications list and you'll see some entries for Microsoft Defender. Security Applications are special in that they are not monitored or restricted in any way. If you have additional security applications, such as a third party anti-virus application, add it here in the form of:

```
{program exectuable path}={digital signature company}
```

For example, if you use ESET you would enter:

```
C:\Program Files\ESET\ESET Endpoint Antivirus\ekrn.exe=ESET, spol. s r.o.
```

If a program in the Security Applications list is not signed by the given signer, it will be monitored like any other executable program.

If your company has a variety of anti-virus versions, vendors, etc, it is OK to add them all here. Just the ones that are running on any particular computer will be given the special status.

Trusted Publishers

Some of the rules that you will use to determine whether an application should run or not will depend on the Trusted Publishers list. This is a list of the digital signers of the executable files (.exe, .dll, .sys, .ocx) that are installed on the systems that will be protected.

Rather than gathering these values manually, you can issue a command to the Satellites and optional Endpoints to scan local drives and collect all the digital signers, and add them to the Trusted Publishers list.

Scanning all of the executables on a server or workstation can take some time. The scan process purposely runs slowly so it doesn't impact the performance of the computer. Expect it to take a couple of hours. You can easily send a scan command using the following methods:

- Central Server and Satellites: Use Bulk Config's "Computers: Scan for Trusted Publishers". This will issue the command. After a short time the Satellite's status report will show it is scanning.

- Endpoints: Go to Endpoint Operations and select the Endpoints you want to scan (all of them is recommended) and use the "Request Trusted Publishers Scan" button. Nothing visual happens when you click the button, but commands will get sent to the Endpoints to start scanning.

After a few hours, you can check the Trusted Publishers list and you'll probably see entries. A comment will show what computer the

entry came from and what file just to help you understand what the application is which is connected to that digital signer. It's quite likely that many of the scans found any particular list entry, but only the first one that reports in adds the entry to the list.

Trusted Application Rules

The individual rules get run when a file access is attempted. The rule looks at attributes of the file being accessed, and the process that is accessing the file, and compares information to Trusted List values (such as the Trusted Publishers) using expression statements

Look at the Trusted Application Rules to see that they are setup to protect your systems how you want. For example, you might want to deny access to Command Host files, or allow them but only for administrators. There are some default rules that you can use, change or delete, as well as adding your own rules. The rules will get synchronized to the Central Server, Satellites and Endpoints automatically. None of the rules will be used until they are enabled.

Enabling Rule Checking

Once rules are in place it's time to enable checks so the rules can do their work. There are two modes for the rules:

- **Testing Mode**: This is where all file access is still allowed as normal, but warnings are issued for file access that would have been blocked by the rules. It is recommended to start out with Testing Mode until the rules are all working exactly as expected.

- **Blocking Mode**: This mode is what provides protection. Once the rules are working correctly, this mode will block file access to anything that doesn't match rules.

  Enabling scanning is done in two ways:

- Central Server and/or Satellites: Create a Trusted Applications Monitor on the server. You'll note there is a setting for Testing/Blocking Mode as well as alerting. If you ever need to disable the scanning (perhaps to do an installation of a new application) you can disable the monitor.

- Endpoints: Go to Endpoint Operations and choose the Endpoints to operate on. Near the bottom right are settings under the Trusted Application Checking title. This lets you set the Test/Block mode, enable/disable scanning and enable/disable alerting. By default, all Endpoints use a global default. With Endpoint Operations you can give specific Endpoints specfic settings for testing. Once everything is working well, you can use the Endpoints > Endpoint Trusted Application Checking node in the Console to change the defaults.

Check Warnings

Once scanning is enabled, warnings will probably start getting queued up for review. In the Console go to Trusted App Services > Access Warnings. Here you can see warnings filtered by user, by host and/or by time. Click on each warning to review the details about that file access.

If you need to change the Trusted Application Rules to handle a situation, all of the properties that could be operated on are shown on the right side of the display.

One thing that will often happen is you will need to white list a particular executable (perhaps because it isn't digitally signed for example). Next to the process name is a green +... button. Use that button to easily add the process to the Trusted Applications List. When you add it to the list, all warnings from that process are removed since it is now a handled situation.

Performance Warnings

One type of warning you can check on are performance warnings. This will let you know if any particular rule is slowing down file access. The goal is for normal file processing to proceed at full speed, and illegal file access to be stopped completely.

Enable Blocking

Once you are not getting blocking warnings for typical file access for a few days, it is time to start enabling Blocking Mode on the Central Server/Satellites and on Endpoints. It is a good idea to proceed slowly - enable it on a couple of servers or Endpoints at a time and see if any problems happen (which would indicate something happened that didn't happen while warnings were being watched).

Blocking Mode is enable with the Central Server/Satellites with each server's Trusted Applications Monitor, and for Endpoints it is via the Endpoint Operations, or via the Endpoint Services > Endpoint Trusted Application Checking page to change the default for Endpoints that are still using the defaults.

> 💡
>
> An easy way to prevent files being copied or moved to a cloud folder is to create a Deny rule which applies to Write and Move/Rename operations and is set to:
>
> ```
> (FILE_PATH_IN_CLOUD_FOLDER = True)
> ```
>
> If you want the cloud service to still be able to put files into the cloud folder (for read-only access) you will need to allow it with something like the following which allows the rule to not apply to the DropBox service:
>
> ```
> (FILE_PATH_IN_CLOUD_FOLDER = True) AND (PROCESS_PATH != "*\DbxSvc.exe")
> ```

Trusted Lists

To make admininstration of the [Trusted Application Rules](#) easier, attributes of files and the processes accessing them can be compared against lists of trusted values, rather than needing to specify each situation explicitly. Many of the built-in [Statements](#) refer to these lists implicitly. See below to learn about each list.
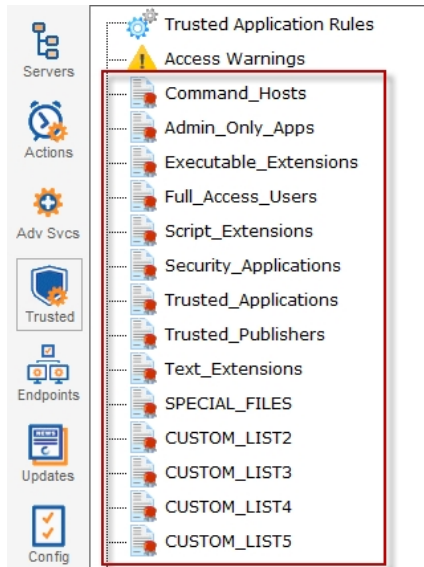
> 💡
>
> Your own rules can refer to these lists using the IN operator.
> Example:
> (FILE_PATH IN Admin_Only_Apps)

Admin_Only_Apps
    This is a list of applications that are typically only used by administrators. They are also often used by hackers to do reconnaissance once they have a foot hold in a network. It is uncommon for end users to use these applications, so seeing them run on an Endpoint could be cause for suspicion. If an admin is doing some work on an end-user's computer and needs to use these applications, they could use temporarily disable Trusted Application Checking on that particular Endpoint using the Endpoint Operations node in the Console.

Command_Hosts
    Applications in this list need to be checked more carefully because they can generally be scripted, and some scripts might cause problems. Files being accessed by applications in this list should be checked more thoroughly, such as making sure (script) files can only be read from protected/trusted locations. This list is used by the FILE_IS_COMMAND_HOST and PROCESS_IS_COMMAND_HOST statements. It is recommended to NOT add files in this list to the Trusted Applications list, otherwise they will run with fewer checks.

Custom Lists
    These lists are to make your rules simpler. For example, instead of a rule referring to 3 or 4 usernames, you can put those usernames in a custom list, and then have the rule check to see if the USER_NAME variable is IN the list. This could also be used for hostnames, file paths, etc. The Custom Lists can be renamed to make them easier to understand when looking at them in a rule. So for example CUSTOM_LIST2 might be renamed to EXECUTIVE_USERS for example, or CUSTOM_LIST3 might be SQL_SERVERS.

    The following characters cannot be used in a Custom List name: (space) (tab) (new line) , = ! < > ( ) " \

    Example: (USER_NAME IN CUSTOM_LIST2)
    Example: (HOST_NAME IN SQL_SERVERS)

Executable_Extensions

This is a simple list of file extensions that can be used with the **FILE_HAS_EXECUTABLE_EXTENSION** or **FILE_HAS_EXECUTABLE_OR_SCRIPT_EXTENSION** statements.

💡

Trusting file extensions can be a shortcut but it may not be safe. It is important to realize many files can use the wrong extension but still retain their full functionality.

Full_Access_Users
This list is for user accounts that should not be blocked. Typically it would be for operating system accounts such as NT AUTHORITY\SYSTEM. This list is used by the statement USER_IS_FULL_ACCESS.

Script_Extensions
This is a simple list of file extensions that are often seen with script files. This list is used with the FILE_HAS_EXECUTABLE_OR_SCRIPT_EXTENSION statement.

Security_Applications
Processes in this list are considered completely safe and they won't be monitored at all. This means these applications can't be misused to cause problems. Typically anti-virus and other security applications such as Windows Defender would be in this list. Backup programs could also be added to this list if they can't be used in a destructive manner (no destructive command line or scripting options).

Text_Extensions
This is a list of file extensions that are usually text files. This list is use with the FILE_HAS_TEXT_EXTENSION statement.

Trusted_Applications
This set of processes are considered safe. They will be reflected in the PROCESS_IS_TRUSTED statement. If a process in this list changes (size, digital signature, etc) it will need to be added to the list again. It is recommended to NOT add Command Host files to this list since they may not be safe depending on what script they are given.

Trusted_Publishers
This is a list of digital signers of executable programs, DLLs, OCXs, drivers, etc. Applications and even files can be checked to see if they are signed by a known application publisher. If a file or process is not digitally signed, it should be checked more thoroughly. This list of Trusted Publishers can be built up by requesting monitored servers and optionally client endpoints to scan all currently installed executable files and add digitally signers to the Trusted Publishers list. This list is used by the FILE_SIGNED_BY_TRUSTED and PROCESS_SIGNED_BY_TRUSTED statements.

Read about [Statements](#) next.

Trusted Application (Application Whitelisting) Rules

Each time a file is accessed, Trusted Application Rules are run to determine whether the file accessed should be allowed or blocked.

Rules have a type of file I/O that they can apply to: Read, Write, Delete and/or Rename/Move. A Rename/Move is a file rename, or a move of a file on the same drive. It is possible for a rule to only allow or block Reads or Writes for example. Rules are only run if they match the requested file I/O activity. In other words, if a rule only applies to Reads, but the current file I/O activity is a Write, that particular rule will not be run.

If a rule evaluates to True, the rule's type (Allow or Disallow) is activated. If the rule evaluates to False, the next rule is run. If all rules are run and none ever grant access to a file, the file access is denied.

> There are **Allow** and **Disallow** rules. As soon as any rule evaluates to true, rule processing stops and the type of rule (Allow or Disallow) determines whether access is allowed or not. Rules are run in order from top to bottom, so rule order is important. If no rule Allows access to a file, access will be blocked.

Rule List

The Trusted Application Rules can be found in the Trusted Applications section of the Console.

There are a list of Rules shown in the Rules List. The Rules will be run in the order shown, from top to bottom. Clicking a rule will show the rule description and a preview of the expression. Any rule can be edited, deleted and new rules can be created.

To the right of each rule is whether it allows **+** or disallows **-** I/O, and what types of I/O are impacted (**R**ead, **W**rite, **D**elete, **r**ename/Move). In addition, an approximate relative cost of running the rule is shown.

Optimizations

Since rules are run in order, you will get better performance by running the faster rules first since they might allow or disallow file access, and then the remaining rules won't need to be run. You can order the rules manually using the up and down arrow buttons on the Rules List.

> It is safe to reorder a small set of Allow rules amongst themselves, or a small list of Disallow rules amongst themselves, but since rules run in order, moving an Allow rule past a Disallow rule or vice versa could impact the desitred functioning of the rules.

Individual Statements with rules have differing compute needs, so sorting the statements within an individual rule can make rule execution faster. For example, imagine a rule that indicates a file must be in the Trusted Applications List AND the user must be an administrator. If the rule determines the file is not in the Trusted Applications List, there is no reason to check whether the user is an administrator because we already know that rule will evaluate to false. The **Optimize** button in the rule editor will re-order the statements to best performance while ensuring the meaning of the rule is not changed.

Rule Editor

The Rule Editor is where you can create the actual rules that will be evaluated when a file access is attempted. Statements evaluate to information for a file access request, and that can be compared with = or != boolean operators to values you specify. AND, OR and NOT boolean operators can also be used to make more complete expressions. Paranthesis can be used for logical grouping/ordering of statements.

> 💡
>
> The wildcard * character can be used when comparing string values using the = and != operator. Also, comparisons with the = and != operator are case-insensitive.
> Example:
> (FILE_PATH = "F:\Documents\Chapter*\Notes.txt") OR (PROCESS_PATH = "C:\Windows\System32*.exe")

Rule Syntax

Rules are boolean expressions that ultimately evaluate to either True or False. The operators AND, OR, NOT, = and != can be used, as well as parentheses to ensure correct order of operations. The IN operator can be used to see if a Statement value is found in a list.

Let's look at an example:

```
(FILE_IS_COMMAND_HOST = true) AND NOT ((PROCESS_IS_TRUSTED = true) OR ((USER_NAME = "NT
AUTHORITY\SYSTEM") OR ((USER_GROUPS = "*,Administrators,*") OR (USER_GROUPS = "*,Domain
Administrators,*"))))
```

FILE_IS_COMMAND_HOST and PROCESS_IS_TRUSTED both evaluate to a boolean True or False, so they are compared against those values. Note that comparisons are case-insensitive. USER_NAME evaluates to a string value, so it is compared to a string value.

In the case of the USER_GROUPS statement, we see the * wild card being used in the comparison. This will match on "Users,Administrators,Printer Operators", but it will not match on "Domain Administrators,Printer Operators,Everyone" because the literal value ",Administrators," is not found in the USER_GROUPS string value.

💡

If your rules start getting long because of many exceptions, it is often easiest to put the exceptions into a Custom List and have the rule refer to the list with the IN operator. For example, imagine the following list of frequently changing programs used by Finance are not digitally signed. They could be added to a Custom List named "CHANGING_HR_FILES":

```
C:\Finance\MonthlyWrapUp.exe
C:\Finance\Daily*Probe.exe
D:\Data\SalesImport\*.csv
```

This list could be checked with a simple rule such as:

```
(FILE_PATH IN CHANGING_HR_FILES) OR (PROCESS_PATH IN
CHANGING_HR_FILES)
```

To easily insert a statement into the Expression, use the Insert dropdown box. The selected Statement will be inserted into the expression editor wherever the cursor is currently at. The expression editor is a simple text editor so you can copy/paste and edit as expected.

💡

You can refer to environment variables using the standard Windows % syntax. For example, %WINDIR% will be expanded to C:\WINDOWS.
Example:
(FILE_PATH = "%WINDIR%*\ARP.EXE")

That rule would match C:\Windows\System32\arp.exe, or C:\Windows\SysWow64\arp.exe, or even C:\Windows\Servicing\LCU\Package_for_RollupFix~31bf385\wow64_microsoft\r\arp.exe.

The **Validate** button can be used to ensure the expression is properly formatted. If there is a problem, it will indicate the first position in the expression where there is an error.

The **Optimize** button will reorder the rule so the fastest statements are executed first.

The **Format Text** button can be helpful to format the text of a rule to help see the logic more easily.

💡

Many other application whitelisting products on the market can only block executable file execution, and don't check other accessed files (such as script files).

If you want the Trusted Applications feature to work in this simpler (and less safe) way, you can create the following Allow rule:

(FILE_HAS_EXECUTABLE_EXTENSION = False)

This will have the effect of allow access to all non-executable files.

Testing

Testing expressions is recommended. At the bottom of the Rule Editor are a set of fields. Fill these in to simulate a file access request that might happen. The expression will run, with the [Statements](#) being evaluated for the given test field values.

Use a full path to an existing file for the target of the test, and a full path to an executable file (ideally to an executable that is running). These need to be paths to existing files because the Statements will be extracting information about the file and process. For this reason, wild-cards cannot be used for the tests fields.

When the test runs, the expression will be evaluated as though the request for the access to the file was actually taking place. The final result of the evaluation will be a True or a False. If the rule is an Allow rule, a True will allow access. If the rule is a Deny rule, a True result will deny access.

Trusted Application (Application Whitelisting) Statements

Each time a file is accessed, data about the file and also about the process accessing the file is made available to Trusted Application Rules. The rules are evaluated and access to the file is either allowed or denied based on the outcome of the evaluation. Rules are made up of logical checks against Statements.

Each statement below evaluates to True or False, or to a string value for the file access that is being checked. Comparisons (such as comparing a value to a string) are case insensitive. You can read more about each statement below.

Note that file extensions don't guarantee the type of file but serve as a hint in most cases. Trusting them is not always safe.

FILE_COPY_SOURCE
    If IS_PROBABLE_COPY is True, then this is the path of the source file of the copy.
FILE_EXTENSION
    Evaluates to a string containing the file extension including dot. Example: (FILE_EXTENSION = ".exe")
FILE_HAS_EXECUTABLE_EXTENSION
    Evaluates to True or False. The file's extension is checked against the Executable Extensions list, and if found, the statement evaluates to True, otherwise to False. FILE_IS_EXECUTABLE or FILE_IS_DLL are more reliable checks, though they takes longer to check. Example: (FILE_HAS_EXECUTABLE_EXTENSION = True)
FILE_HAS_EXECUTABLE_OR_SCRIPT_EXTENSION
    Evaluates to True or False. The file's extension is checked against the Executable Extensions list and the Script Extensions list, and if found in either, the statement evaluates to True, otherwise to False. Note that trusting file extensions is not always safe. Example: (FILE_HAS_EXECUTABLE_OR_SCRIPT_EXTENSION = False)
FILE_HAS_TEXT_EXTENSION
    Evaluates to True or False, based on whether the file's extension is found in the Text Extensions list. Example: (FILE_HAS_TEXT_EXTENSION = True)
FILE_IS_COMMAND_HOST
    Evaluates to True or False, depending on whether the file name (excluding path) is found in the Command Hosts list. If CMD.EXE was in the Command Hosts list, both C:\cmd.exe and C:\Windows\System\cmd.exe would evaluate to True. Example: (FILE_IS_COMMAND_HOST = False)
FILE_IS_DLL
    Evaluates to True or False, depending on whether the file is an DLL file based on a check of the file header. This is slower, but more trustworthy than the FILE_HAS_EXECUTABLE_EXTENSION check because the file header is checked. Typically .DLL, .CPL, .OCX, etc files will meet the criteria. Example: (FILE_IS_DLL = True)
FILE_IS_EXECUTABLE
    Evaluates to True or False, depending on whether the file is an executable file based on a check of the file header. This is slower, but more trustworthy than the FILE_HAS_EXECUTABLE_EXTENSION check. Typically only .EXE files will meet the criteria. Example: (FILE_IS_EXECUTABLE = True)
FILE_PATH_IS_REMOTE
    Boolean indicating if the file path is on a remote computer, such as with a mapped drive or UNC path. Example: (FILE_PATH_IS_REMOTE = False)
FILE_IS_SIGNED
    Evaluates to True or False. The file is checked for a digital signature, and if found, the result is True. Example: (FILE_IS_SIGNED = True)
FILE_IS_TEXT_FILE
    Evaluates to True or False. The file is opened and inspected using heuristics on the first 64KB to determine whether it appears to be a text file or not. Example: (FILE_IS_TEXT_FILE = True)
FILE_PATH
    Evaluates to a string containing the full path of the file being accessed. Example: (FILE_PATH = "C:\Users\Bob\Documents\Bob's Updates.docx")
FILE_PATH_IN_CLOUD_FOLDER
    Evaluates to True or False indicating if the file is located within a local cloud product folder. OneDrive, Google Drive and DropBox are currently detected and supported. Example: (FILE_PATH_IN_CLOUD_FOLDER = True)
FILE_PATH_IN_EXTERNAL_DRIVE
    Evaluates to True or False indicating if the file is located on an external drive, such as a USB thumb drive. Example: (FILE_PATH_IN_EXTERNAL_DRIVE = True)

For the FILE_RENAME_DEST_xxx statements below, IF the file operation is a Move/Rename, then these statements are filled in

with the new filename. If the file operation is not a Move/Rename, then they will have the same value as the FILE_PATH_xxx statements above.

FILE_RENAME_DEST_EXTENSION

File extension of the rename/move destination file, including the dot, such as .TXT. If not a rename/move operation, this will be the same value as FILE_EXTENSION. Example: (FILE_RENAME_DEST_EXTENSION = ".docx")

FILE_RENAME_DEST_PATH

In the case of a rename/move operation, this is the full path to the destination file. If not a rename/move operation, it is the same as FILE_PATH. Example: (FILE_RENAME_DEST_PATH = "D:\My-Backup-Files\Secret.docx")

FILE_RENAME_DEST_PATH_IN_CLOUD_FOLDER

In the case of a rename/move operation, boolean indicating if the rename/move destination path is in a cloud synchronization folder, such as OneDrive, DropBox or GoogleDrive. If not a move/rename operation it is the same as FILE_PATH_IN_CLOUD_FOLDER. Example: (FILE_RENAME_DEST_PATH_IN_CLOUD_FOLDER = True)

FILE_RENAME_DEST_PATH_IN_EXTERNAL_DRIVE

Evaluates to True or False, and will be True if FILE_RENAME_DEST_PATH is on an external drive, such as a USB thumb drive. If not a move/rename operation it is the same as FILE_PATH_IN_EXTERNAL_DRIVE. Example: (FILE_RENAME_DEST_PATH_IN_EXTERNAL_DRIVE = False)

FILE_SHA256

Evaluates to a string consisting of the SHA256 hash of the file. This can potentially be an expensive operation as it requires opening and reading the entire file to compute the hash. Example: (FILE_SHA256 = "588A31053B19A3E8F5B4E7EF16AC9C45862EB097E9403739B59E0FD437D623EA")

FILE_SIGNED_BY

Evaluates to a value extracted from the file's digital signature. If there is no digital signature the value will be an empty string. Example: (FILE_SIGNED_BY = "Power Admin LLC") OR (FILE_SIGNED_BY = "")
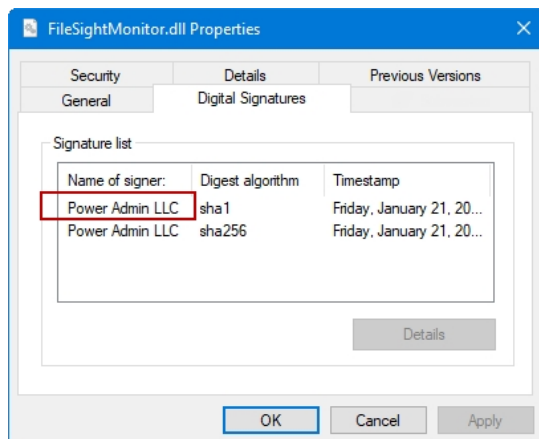
FILE_SIGNED_BY_TRUSTED

Evaluates to True or False. The file's digital signature signer is extracted (see FILE_SIGNED_BY) and that value is searched for in the Trusted Publishers list. If found, the statement evalutes to True. Example: (FILE_SIGNED_BY_TRUSTED = True)

HOST_NAME

Evaluates to a string containing the hostname where the rule is being run. This can be the Central Server, a Satellite Server or an Endpoint. Example: (HOSTNAME = "MSDC1")

PROCESS_IS_COMMAND_HOST

Evaluates to True or False. The current process name (without the path) that is reading the file being checked is compared to the Command Host list. If it is found in the list, the statement evaluates to True. Example: (PROCESS_IS_COMMAND_HOST = True)

PROCESS_IS_SIGNED

Evaluates to True or False. Indicates whether the executable file, of the process that is accessing the file, contains a digital signature. Example: (PROCESS_IS_SIGNED = False)

PROCESS_IS_TRUSTED_APP

Evaluates to True or False. The process' path is compared against entries in the Trusted Applications list and evaluates to True if a match is found, and details about the file (signer, date, size) also match what was added to the list. Example: (PROCESS_IS_TRUSTED = True)

PROCESS_PATH

Evaluates to a string consisting of the process' executable file path, without any command line arguments. Example: (PROCESS_PATH = "C:\Windows\Notepad.exe")

PROCESS_PATH_IN_CLOUD_FOLDER

Evaluates to True or False, and is True if the process is running from within a local cloud folder (OneDrive, Google Drive or DropBox). Example: (PROCESS_PATH_IN_CLOUD_FOLDER = false)

PROCESS_SHA256

Evaluates to a string containing the SHA256 hash of the process' executable file. This can be expensive to compute as it requires opening and reading the entire process executable file. Example: (PROCESS_SHA256 = "A9E8AD0792B546A4A8CE49EDA82B327AD9581141312EFEC3AC6F2D3AD5A05F17")

PROCESS_SIGNED_BY

Evaluates to a string containing the process executable file's digital signature signer, or an empty string if there is no digital signature. Example: (PROCESS_SIGNED_BY = "Microsoft Windows")

PROCESS_SIGNED_BY_TRUSTED

Evaluates to True or False. The process file's digital signature signer is extracted and then checked against the Trusted Publishers list. If found the statement evaluates to True. Be cautious with this since most Command Host processes (like cmd.exe and powershell.exe) are signed by a trusted company. Example: (PROCESS_SIGNED_BY_TRUSTED = True)

REQUESTOR_HAS_ENDPOINT

Boolean value indicating whether the file being requested is from a system with one of the following running: the Endpoint, the Central Server or a Satellite server. This statement is only evaluated on the Central Server or a Satellite - it always True when checked on the Endpoint. Example: (REQUESTOR_HAS_ENDPOINT = True)

REQUEST_FROM_NETWORK

Boolean value indicating if the file is being requested from something on the network (i.e. not a local file access). This value is meant to be processed on the server, so the Endpoint always sets it to True. Example: (REQUEST_FROM_NETWORK = True)

REQUEST_IPADDRESS

String value indicating the IP address of the requestor if the request comes from the network. It could potentially hold a local address for requests from the local system. It is mostly used for logging and diagnostics.

USER_GROUPS

Evalulates to a comma separated list of all the groups (local and Active Directory) that the user requesting the file read is a member of. Because some group names might contain other group names ("Administrators" could be a substring of "Domain Administrators") it is best to do comparisons with a comma at the start and end of the target group being checked for. Also, wildcards will be needed to ignore the rest of the string in a comparison. In this example, the user is being checked to see if they are part of the local Administrators group: (USER_GROUPS = "*,Administrators,*")

Comparing against "*Administrators*" could match against Administrators, Domain Administrators, Print Administrators or even HRAdministrators.

USER_IS_FULL_ACCESS

This evaluates to True or False depending on if the user (USER_NAME value) is found in the Full Access Users list. Example: (USER_IS_FULL_ACCESS = True)

USER_NAME

Evaluates to a string of the logged in user, using domain\username format. Example: (USER_NAME = "OFFICE\Bob")

Learn about Trusted Application [Rules](#) next.

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.

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.
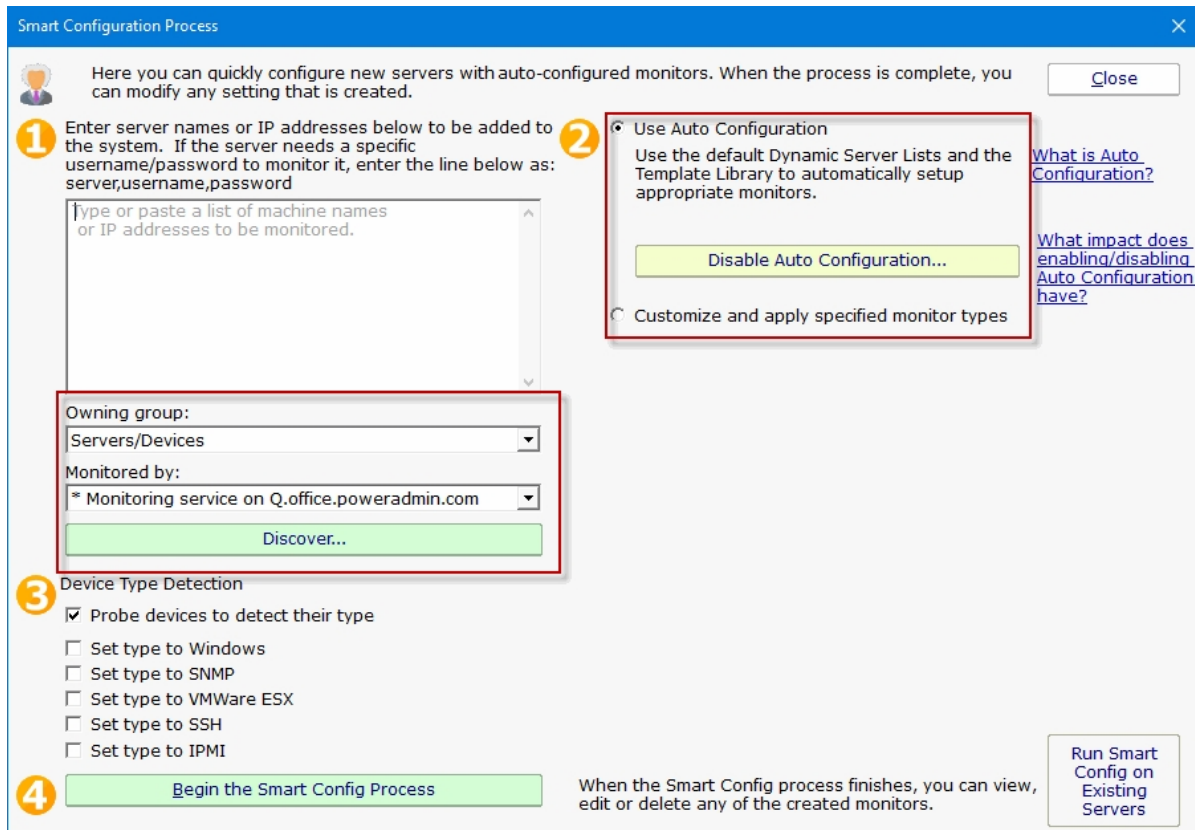
The next step is to select how the service will inspect the server(s)/device(s) to add monitor modules, either by Automatic Configuration or Customize and apply specified monitor types. Then select the Device Type for your servers/devices and press "Begin the Smart Config Process". In a few moments you'll 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 File Sight 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.
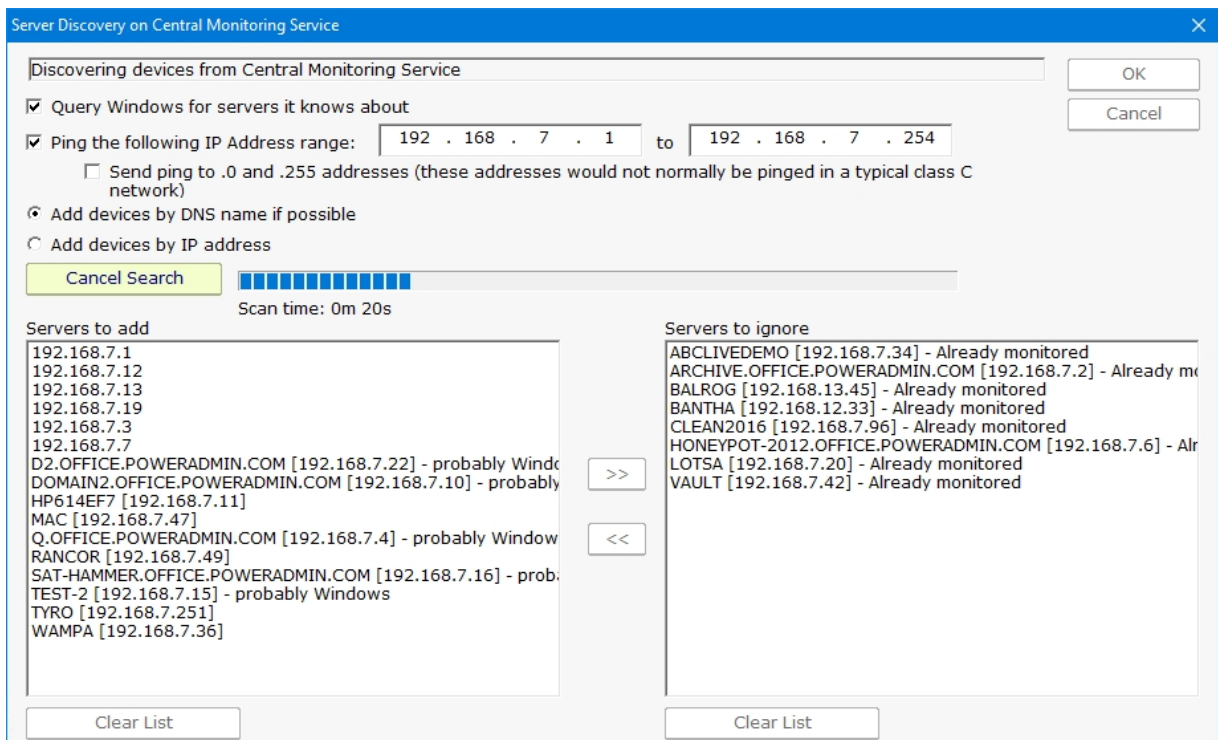
The following options are available for Server Discovery:

○ Query Windows for servers it knows about: Windows has its own network discovery process that PA File Sight 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.

Smart Config Status

Smart Config for 2 servers/devices - In Progress

Created 25 Mar 2020 11:33 AM

All Reports   PDF Version

1 records

Server/Device	Status	Details
In Progress ...	.	.

Report URL:
This automatically generated report will always be created in the same location
Created in 2 ms

Generated by PA Server Monitor
v8.1.0

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.

Global Monitors

Global Monitors are very similar to normal monitors with the exception that they are not attached to a server or group.
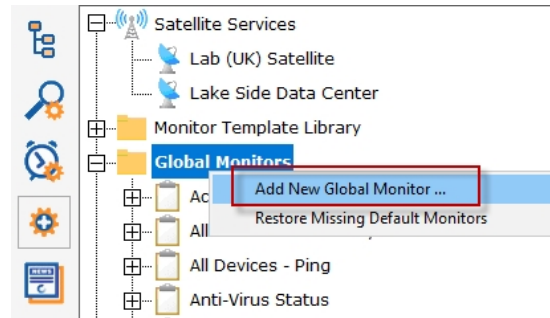
Global Monitors are found under the Advanced Services section of the Console application.

Like regular monitors, these monitors have the standard options for Adding Actions, setting Advanced Options and setting the Monitor Schedule.

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
Error	$mon.msError
Disabled	$mon.msDISABLED
Alert Show as Green	$mon.msALERT_GREEN
Alert Show as Red	$mon.msALERT_RED

$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\PAFileSight\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_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). 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

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

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

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
```

```
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
```

```
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

```
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
- Launch a PS program and record results
- Monitor AD Sysvol
- Monitor AD Replication
- Monitor Window's License Activations

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})"
```

5. Monitor memory of service

Your Script

If you would like to share your script, please contact us.

File Sight - Interpreting Application Behavior

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

C:\Docs\My Story.doc

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

C:\Docs\~My Story.tmp

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

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

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

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

So, if PA File Sight sees:

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

it will turn it into

WRITE C:\Docs\My Story.doc

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

Caveats:

○ Doing the above processing requires extra memory--more events have to be held in memory now so they can be compared. (For example, all DELETEs have to be held in case a RENAME comes along a short while later).

○ Some additional CPU processing power is also required to search through and match up related events.

○ Alerting is delayed a few seconds (a DELETE alert should not be sent if it will ultimately get turned into a WRITE).

○ Several saves within a few (5 - 10) seconds will not always be interpretted correctly, so some of the underlying RENAME and DELETE operations may show through.

File Sight - Alternate Data Streams

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

You can read more about them at:

○ File Streams (Microsoft.com)

○ Streams utility (Microsoft.com)

○ Google Search

Data streams often look like the following example:

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

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

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

○ Show stream access - This is the default, so for the example above you could see accesses happening to the shown stream as well as separate actions on the base Payroll.xls file

○ Truncate stream - Instead of showing the complete file stream name in the example above, PA File Sight can truncate the name to the base file (C:\Documents\Financial Data\Payroll.xls in the example)

○ Ignored streams - When a file stream is detected, it is completely ignored

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.
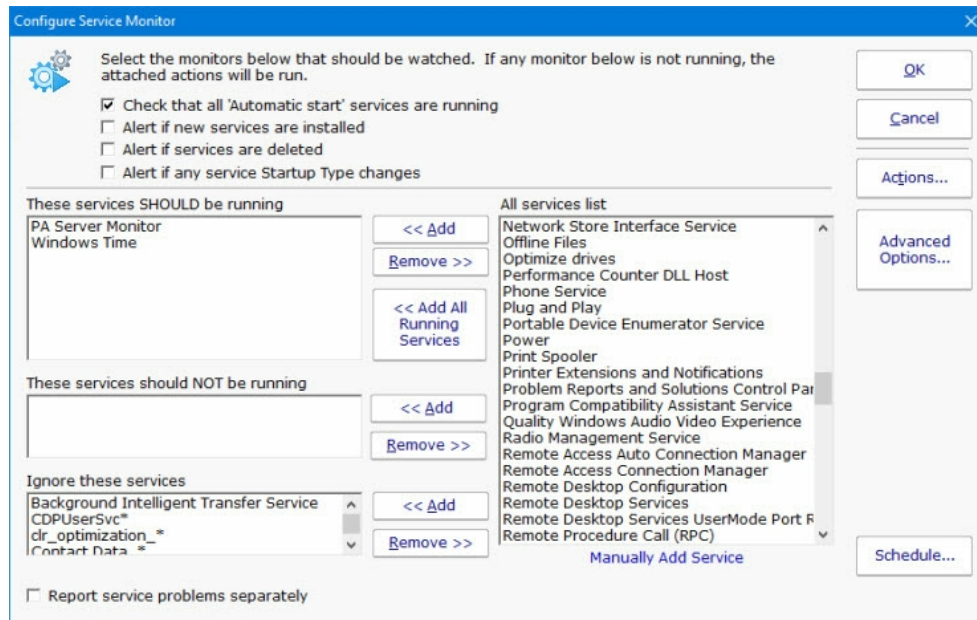
There are a lot of different parts to this monitor, so we'll take them one at a time.

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.

All services list

Manually Add Service
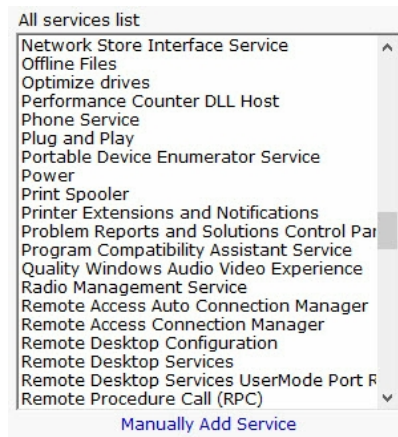
This box lists all of the service that are currently listed on the target server. It will match the list you see in services.msc. If you can see this list, the monitor is able to actively communicate with the target server (even if you are monitoring a server at a remote site via a Satellite Monitoring 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.
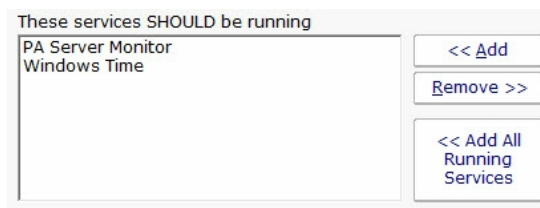
If you have services that need to be running (perhaps they aren't "Automatic Start", or you don't want to monitor all "Automatic Start" services with the check box above), you can list them here.
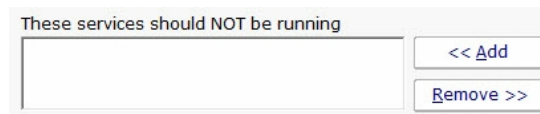
Indicate any service that should NOT be running here. For example, some organizations will disable a service because of a security policy. If that service is ever running, it would need to be brought to someone's attention.
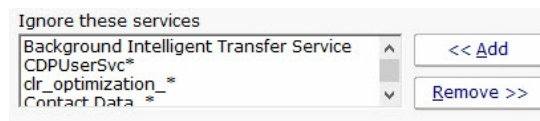
A number of services start and stop on their own during normal usage. You probably don't want to be notified about those services, so you can indicate they should be ignored. Ignoring a service means it will be ignored from all other checks specified above. PA File Sight automatically adds a few common 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
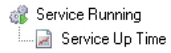
Service up or down data is recorded every time the monitor runs. You can define a time period, and optionally a summarization (hourly, daily, weekly, monthly) to create an uptime report for the service.

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.

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.
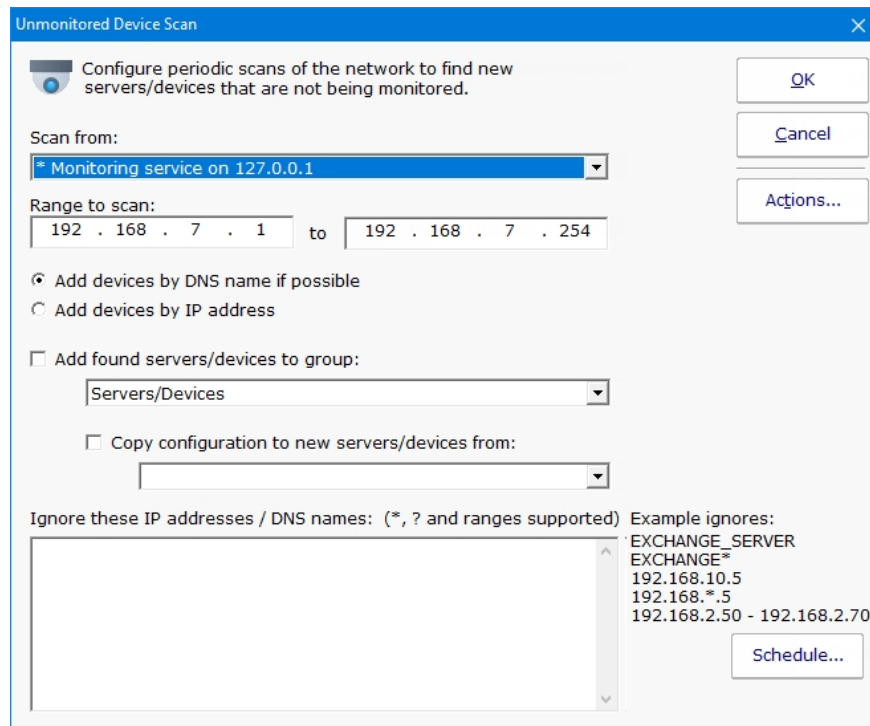
When new devices are found on the network, you can have them automatically added to PA File Sight to a specific group. You can also have a configuration copied from an existing server/device.

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.

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 |

PA File Sight 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 File Sight\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 File Sight\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 File Sight 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 File Sight\CA\openssl.cnf
   ```

   The conversion command:

   ```
   "C:\Program Files\PA File Sight\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 File Sight\CA\CLIENT_PRIVATE.pem

3. Save the SSL certificate to
   C:\Program Files\PA File Sight\CA\SIGNED_CLIENT_CERT.pem

4. PA File Sight will need to know the password for the private key. You can specify this by running the following command:
   ```
   "C:\Program Files\PA File Sight\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 File Sight\diag.exe" /SETCONFIG=SSLCertPKPW:
```

5. Restart the PA File Sight service and it will now be using your SSL certificate.

Create your own new certificate

1. Go to the C:\Program Files\PA File Sight\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 File Sight\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 File Sight\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 File Sight\openssl.exe" req -newkey rsa:2048 -keyout "C:\Program Files\PA File
Sight\CA\NewCert\CLIENT_PRIVATE.pem" -keyform PEM -out "C:\Program Files\PA File
Sight\CA\NewCert\SSL_CERT_CSR.csr" -outform PEM -rand "C:\Program Files\PA File Sight\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 File Sight\openssl.exe" req -in "C:\Program Files\PA File
Sight\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 File Sight\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 File Sight\CA**NewCert**\CLIENT_PRIVATE.pem
    into the CA folder.

11. PA File Sight 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 File Sight the password by running the following command:

    ```
    "C:\Program Files\PA File Sight\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 File Sight service and it will now be using your SSL certificate.
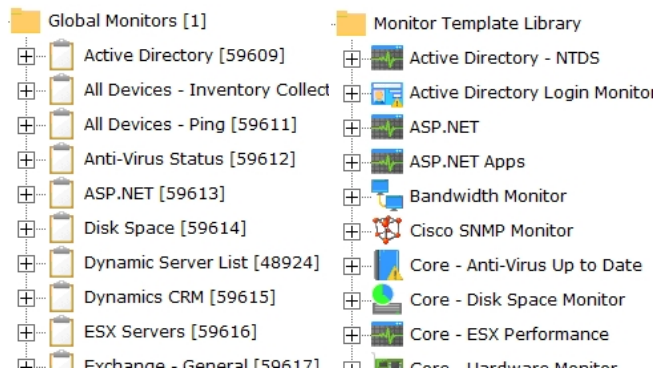
Automatic Configuration

PA File Sight 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.
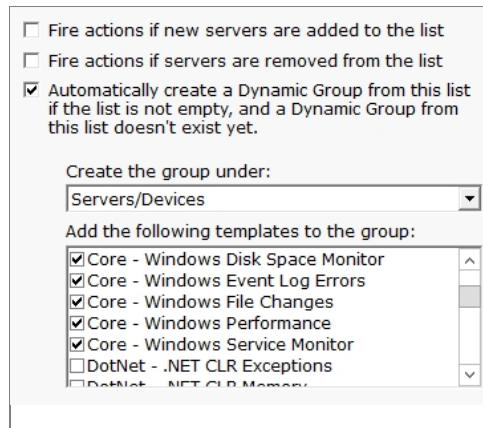
Automatic Configuration Group

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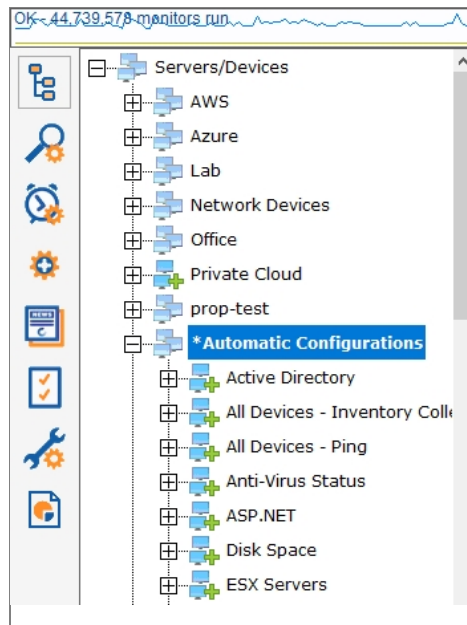
As servers/devices are added to these groups, the normal operation of copying Power Templates to the servers/devices will take place. That is automatic configuration.

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](#).

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 File Sight\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.