

Anleitung zum Softwarepaket - Syswatcher

Vorwort:

in dieser Anleitung gehe ich nicht auf alle Kleinigkeiten ein, welche die Software unterstützt. Vielmehr geht es mir darum bestimmte Abläufe und Einstellmöglichkeiten zu erklären.

Folgende Punkte werden angesprochen:

1. Prinzipielle Arbeitsweise des Softwarepaketes
2. Erklärung der wesentlichen Elemente aller Masken
3. Aktivierung der Software
4. Erklärung der einzelnen Sensortypen
5. Spezielle Einstellungsmöglichkeiten
6. App-Schnittstelle
7. Prinzipieller Ablauf von Listenänderungen

1. Prinzipielle Arbeitsweise des Softwarepaketes

Das Softwarepaket besteht aus zwei Teilen, dem Hauptdienst und dem KonfigClient. Der Hauptdienst übernimmt die ganze Arbeit der Überwachung bzw. des Monitorings. Er lädt beim Starten die Konfiguration der Events aus einer Datenbank und prüft dieses zyklisch ab. Der Zeitraum dafür ist einstellbar. Gilt ein Sensor als ausgelöst (Fehlerfall), so erledigt dieser auch die entsprechenden Reaktionen, wie beispielsweise das Versenden einer Mail.

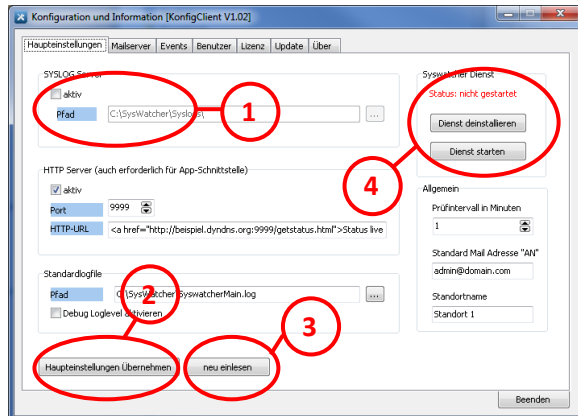
Der KonfigClient erstellt aus der Eingabe des Benutzers die Konfigurationsdatenbanken für den Hauptdienst. Dazu gehören:

1. Benutzerdatenbank
2. Eventsdatenbank
3. Grundeinstellungen

Die Datenbanken sind CFG-Dateien die auch von einem normalen Editor (Notepad) im Klartext bearbeitet werden könnten. Davon rate ich aber ab, weil der Syntax exakt eingehalten werden muss. Eine Abweichung vom korrekten Syntax kann unvorhergesehenen Folgen haben.

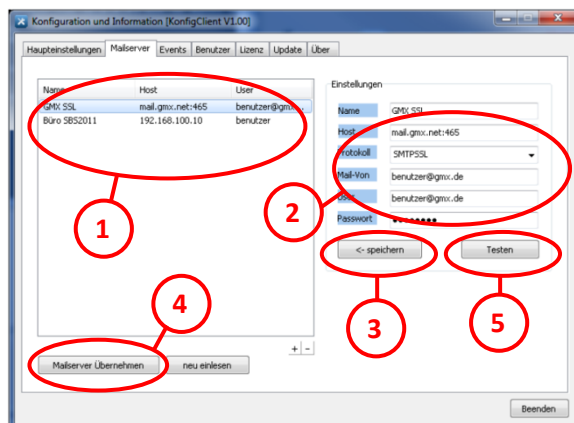
2. Erklärung der wesentlichen Elemente aller Masken

[Maske Haupteinstellungen]



1. Hier ist eine normale Einstellung zu finden, wie sie auf allen Masken sichtbar sind.
2. Mit Klick auf diesen Knopf werden alle aktuell sichtbaren Einstellungen in das entsprechende Datenbankfile auf die Festplatte geschrieben. Da der Hauptdienst seine Einstellungen nur beim Start lädt wird anschließend nach dessen Neustart gefragt.
3. Hier besteht die Möglichkeit die Daten aus der Datenbank für alle sichtbaren Eingabefelder neu in die Eingabemaske zu laden. Alle geänderten Einstellungen auf der aktuellen Seite gehen damit verloren und man hat wieder die Einstellungen die der Hauptdienst geladen hat.
4. Auf diesem Tab gibt es eine Spezialsektion, wo es möglich ist den Dienst manuell neu zu starten, zu stoppen, zu deinstallieren, oder zu installieren.

[Maske Mailserver]



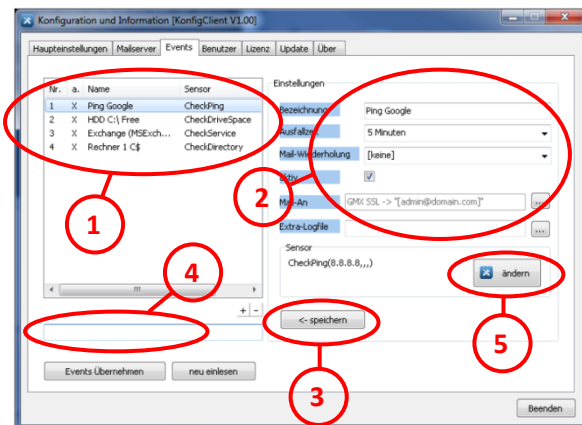
Wichtig ist, dass der erste Mailserver in der Liste immer der Standardmailserver ist. Wenn beispielsweise der Hauptdienst startet schickt er über diesen Server eine Infomail mit Informationen über den Start. Als Mail-Empfänger wird dabei wieder das in "[Maske Haupteinstellungen]" zu findende Feld "Standard Mail-Adresse AN" benutzt.

1. Dies ist eine Liste in welcher die aktuell eingerichteten Mailserver zu sehen sind. Mit einem einfachen Klick darauf wird der markierte Eintrag in Punkt 2 angezeigt und kann dort verändert werden. Ein Rechtsklick auf einen Listeneintrag gibt zusätzliche Möglichkeiten einer Veränderung.
2. Hier kann der aus Punkt 1 markierte Eintrag verändert werden. Dieser muss dann mit dem Knopf "<- speichern" (Punkt 3) wieder in die Liste übertragen werden. Damit sind die Einstellungen aber noch nicht in die Datenbank übernommen worden. Das passiert erst über den in Punkt 4 gezeigten Knopf.
3. Speichert die in Punkt 2 markierten Werte zurück in die Liste (Punkt 1). Besitzt dieser Knopf die Bezeichnung "<- hinzufügen" so wird ein Eintrag am Ende der Liste neu hinzugefügt.
4. Speichert alle sichtbaren Einträge aus der Liste zurück in die passende Datenbank und fragt nach dem Neustart des Hauptdienstes. Dieser übernimmt nach Bestätigung aktiv die neuen Einstellungen.
5. Hier wird eine Testmail generiert und mit den sichtbaren Einstellungen (Punkt 2) versendet. Die Daten müssen nicht vorher in die Liste übernommen werden. Als Mail-Empfänger der Testmail wird dabei das in "[Maske Haupteinstellungen]" zu findende Feld "Standard Mail-Adresse AN" benutzt.

[Maske Events]

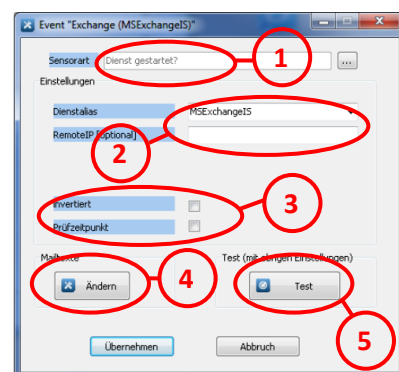
Diese Maske ist das Herzstück des Softwarepaketes. Hier werden alle Einstellungen erledigt was die Überwachung angeht. Jedes Gerät welches überwacht wird kann hier konfiguriert werden. Jedem Event ist ein Sensor zugeordnet welcher die Einstellungen beinhaltet was, wie überwacht wird. Über den Knopf "ändern" (Punkt 5) können diese individuellen Werte eingestellt werden.

Maske 1:



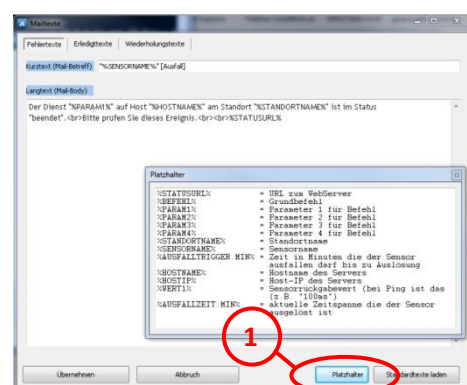
1. Dies ist eine Liste in welcher die aktuell eingerichteten Events zu sehen sind.
2. Hier kann der aus Punkt 1 markierte Eintrag verändert werden.
3. Übernimmt die in Punkt 2 markierten Werte in die Liste (Punkt 1).
4. Hier können die in der Liste angezeigten Events durch einen Suchbegriff gefiltert werden. Das ist besonders bei sehr vielen Events sehr hilfreich.
5. Die individuellen Einstellungen der Sensoren eines Eintrages werden hier konfiguriert. Auch eine Veränderung der Mailtexte ist in diesem Untermenü möglich. Der Klick auf diesen Knopf öffnet "Maske 2".

Maske 2:



1. Hier kann der Typ des Sensors ausgewählt werden. Siehe hierzu auch "[Erklärung der einzelnen Sensortypen](#)".
2. Das sind die individuellen Einstellungen zum aus "Punkt 1" gewählten Sensortyp.
3. Dies sind spezielle Einstellungen die es bei jedem Sensor gibt. Siehe hierzu auch "[spezielle Einstellungsmöglichkeiten](#)".
4. Hier kann man die Mailtexte die bei ausgelösten Sensor verschickt werden ändern. Auch der Text der Erledigt- und Wiederholungsmeldungen ist einstellbar. Der Klick auf diesen Knopf öffnet "Maske 3".
5. Hier können die Einstellungen des Sensors geprüft werden. Auch eventuelle Fehleinstellungen und Schwellwerte sind dabei zu erkennen.

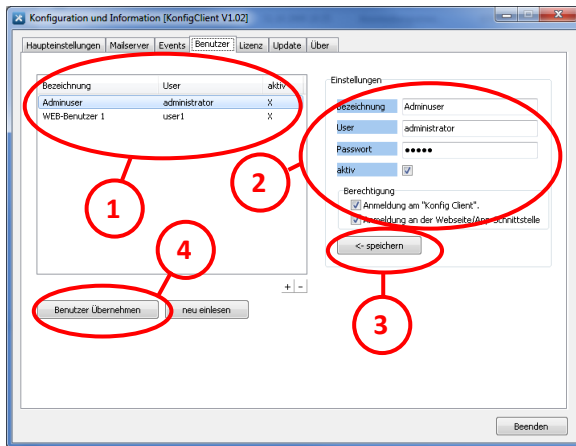
Maske 3:



Diese Maske ist selbsterklärend. Es gibt 3 verschiedene Textarten.

1. Fehlertext (ein Sensor ist ausgelöst)
2. Erledigttext (ein Sensor ist nicht mehr ausgelöst)
3. Wiederholungstext (Text für Mailwiederholungen - Maske 1->Punkt 2->Mail-Wiederholung)

Das Format ist HTML, damit kann also jede Wunschmail frei definiert werden. Die Platzhalter werden direkt durch die entsprechenden Werte ersetzt. Die Großschreibung ist dabei wichtig. Das Platzhaltermenü kann über "Punkt 1" geöffnet werden.

[Maske Benutzer]

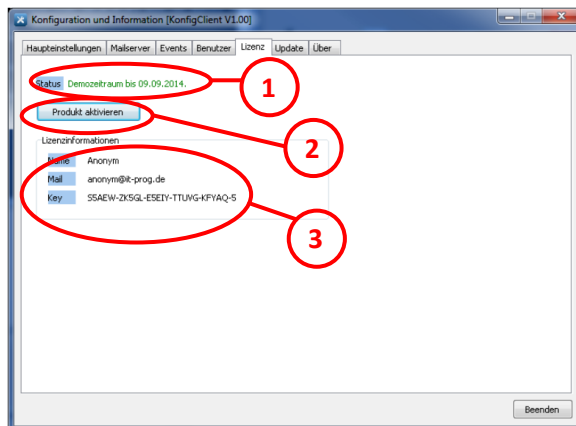
1. Dies ist eine Liste in welcher die aktuell eingerichteten Benutzer zu sehen sind.

2. Hier kann der aus "Punkt 1" markierte Eintrag verändert werden. Interessant sind ebenfalls die beiden Optionen.

1. Anmeldung am "Konfig Client"
2. Anmeldung an der Webseite

3. Übernimmt die in "Punkt 2" geänderten Einstellungen in die Liste (Punkt 1).

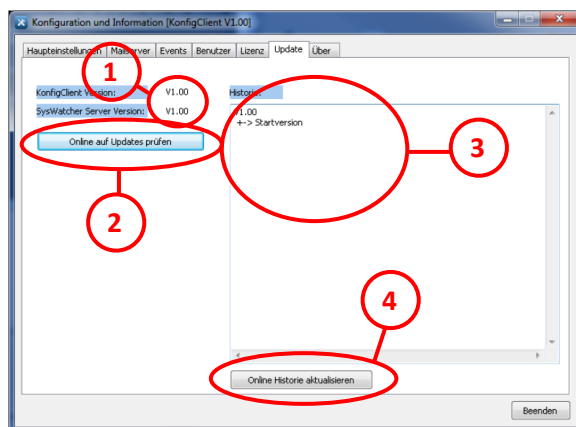
4. Speichert alle sichtbaren Einträge aus der Liste zurück in die passende Datenbank und fragt nach dem Neustart des Hauptdienstes. Dieser übernimmt nach Bestätigung aktiv die neuen Einstellungen.

[Maske Lizenz]

1. Zeigt den aktuellen Lizenzstatus an.

2. Mit diesem Knopf wird der Aktivierungsassistent gestartet. Dabei kann eine Lizenz erstellt oder gewandelt werden. Diese Funktion ist nicht verfügbar wenn eine Vollversion aktiviert ist.

3. Zeigt bei einer aktiven Lizenzierung die Lizenzierungsdaten an.

[Maske Update]

1. Zeigt die aktuellen Versionen der Module "KonfigClient" und "Hauptdienst".

2. Mit Klick auf diesen Knopf wird online abgefragt ob es für diese Programmhauptversion (V1.XX) ein Update gibt. Unter Umständen kann es vorkommen, dass ein Update für exakt die selbe Version (auch Unterversion) abrufbar ist.

3. Ansicht der Programmhistorie. Diese kann Online über den Knopf "Online Historie aktualisieren" mit dem Server neu abgeglichen werden.

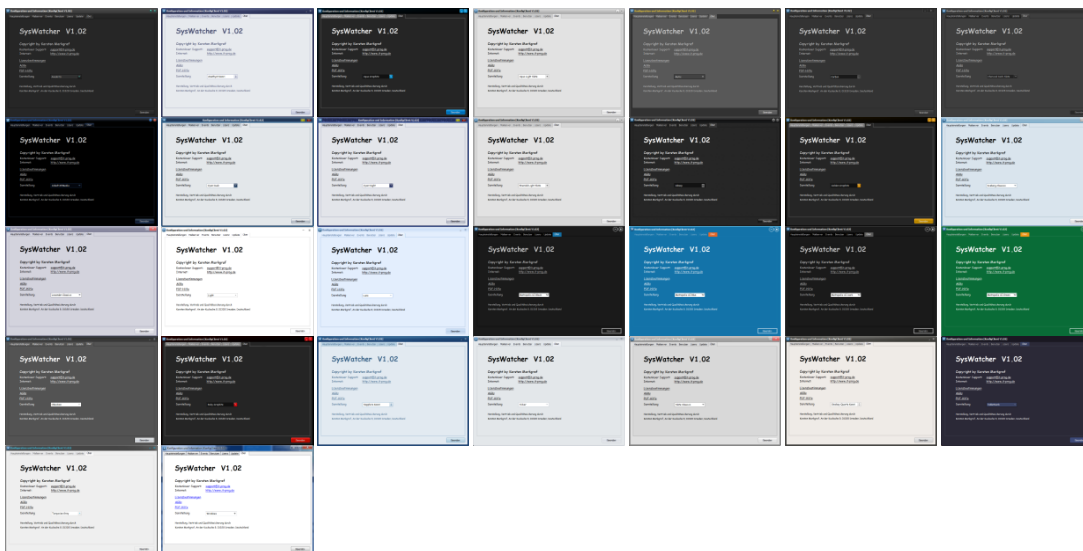
4. Aktualisiert die Programmhistorie mit den IT-Prog Onlineserver.

[Maske Über]

1. Hier kann die Art der Darstellung des Konfigclients geändert werden. Bei einigen Auswahlen kann es vorkommen das einige Elemente leicht verschoben dargestellt werden, was aber die Funktionalität keineswegs beeinflusst. Will man das Standard Windowsdesign haben muss hier "Windows" eingestellt werden. Die Standardeinstellung ist "Iceberg Classico". Die Einstellungen sind betriebssystemunabhängig.

Hilfe und die AGB'S können hier direkt geöffnet werden. Eine Hilfe ist aber auch über die Taste F1 von überall aus aufrufbar. Voraussetzung ist hier ein installierter Acrobat Reader.

Hier werden alle Darstellungsmöglichkeiten noch einmal als kleiner Screenshot gezeigt:



3. Aktivierung der Software

Der Ablauf der Aktivierung ist Dank des Assistenten selbsterklärend. Diese wird online über einen Aktivierungsserver durchgeführt. Ist vom System aus kein Zugang zum IT-Prog Aktivierungsserver möglich, so kann eine externe Aktivierung durchgeführt werden. Bitte folgen Sie den Anweisungen während der Aktivierung.

Es gibt 2 Arten der Lizenzen:

60 Tage Demo: Während des Demozeitraums kann das Produkt voll genutzt werden. Auch Updates sind dabei möglich. Nach diesen 60 Tagen verfällt die Demolizenz und der Hauptdienst wird nicht mehr starten. Nach dieser Zeit kann auf diesem System nur noch eine Vollversion des SysWatcher genutzt werden.

Vollversion: Wenn Sie einen Lizenzschlüssel erworben haben kann dieser zur dauerhaften Aktivierung des Produktes genutzt werden. Durch die Aktivierung wird der erworbene Key dem aktuellen System dauerhaft zugeordnet. Danach ist eine Aktivierung nur noch auf dem gleichen System, für das selbe

Softwareprodukt in derselben Hauptversion möglich (also SysWatcher V1.XX). Eine De- und Neuinstallation ist damit problemlos möglich. Die Umschlüsselung der Lizenz auf ein anderes System ist ausdrücklich nicht erlaubt.

4. Erklärung der einzelnen Sensortypen

Ping:

Erklärung: Es wird ein ICMP Paket zum Ziel geschickt (Ping). Kommt innerhalb von 5 Sekunden keine Antwort, so gilt der Sensor als ausgelöst. Die Wartezeit von 5 Sekunden ist über dem Parameter „Timeout MS (optional)“ einstellbar.

Parameter „Ziel“: Hier kann der Hostname bzw. die IP-Adresse des Zieles eingegeben werden welches der Hauptdienst versucht zu erreichen.

Parameter „Timeout MS (optional)“: Wartezeit in Millisekunden in welcher das Ziel antworten muss. Wird diese Zeit überschritten gilt der Sensor als ausgelöst.

TCP-Verbindungstest:

Erklärung: Ähnlich wie beim "Ping" wird hier eine TCP Verbindung zu einem bestimmten Ziel aufgebaut. Dabei wird nur ein "Connect" versucht. Es werden keinerlei Daten über diese Verbindung übertragen oder gar geprüft. Kommt keine Verbindung innerhalb von 5 Sekunden zu Stande gilt der Sensor als ausgelöst. Die Wartezeit von 5 Sekunden ist über dem Parameter „Timeout MS (optional)“ einstellbar.

Parameter "Host:Port": Hier kann der Hostname bzw. die IP des Zieles angegeben werden. Nach dem ":" folgt noch der Port. Dieser darf nicht vergessen werden, da sonst die Antwortzeit immer "-1" beträgt, was auf eine Nichterreichbarkeit hinweist und damit als "ausgelöster Sensor" bewertet wird.

Parameter „Timeout MS (optional)“: Wartezeit in Millisekunden in welcher der Connect zu Stande kommen muss. Wird diese Zeit überschritten gilt der Sensor als ausgelöst.

Kapazität Laufwerk (frei):

Erklärung: Es wird ein bestimmter Laufwerksbuchstabe auf seine freie Kapazität geprüft. Fällt diese unter den eingestellten Wert fällt, so gilt der Sensor als ausgelöst.

Parameter "Laufwerk": Auswahl des Laufwerks welches geprüft werden soll. Auch Netzlaufwerke sind hier denkbar. Existiert das Laufwerk nicht wird mit einer freien Speicherkapazität von "-0.00 MB" gerechnet, wodurch der Sensor immer als ausgelöst gilt. Durch dieses Verhalten kann man auch ein Verschwinden eines Laufwerkes (z.B. Backup USB Platte) ermitteln. Besser ist hier aber der Sensor „Verzeichnis erreichbar“.

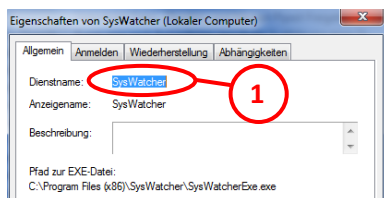
Parameter "min. Kapazität frei (MB)": Hier wird die Schwelle in Megabyte eingegeben. Wird die freie Laufwerkskapazität an dieser Schwelle unterschritten, so gilt der Sensor als ausgelöst. Ist kein Wert eingetragen, gilt der Sensor immer als ausgelöst.

Rückgabewert: Der Sensor gibt die aktuelle freie Speicherkapazität in Megabyte zurück und kann mit %WERT1% in die Mailtexte eingebunden werden. Im Rückgabewert ist die Einheit schon enthalten. Existiert das Laufwerk nicht, so wird auch hier ein Wert von "-0.00 MB" zurückgegeben.

Dienst gestartet:

Erklärung: Hier können Dienste überwacht werden. Interessant ist die Möglichkeit einen Dienst abzufragen der sich nicht auf dem eigenen System befindet. Dazu ist der Parameter "RemoteIP [optional]" gedacht, der auf das andere System zeigt. Entsprechende Rechte sind natürlich vorausgesetzt. Ist ein anderer Benutzer dafür notwendig kann das nur über die Anmeldeeinstellungen des Hauptdienstes realisiert werden. Das gilt dann aber für alle Aktionen des SysWatcher.

Parameter "Dienstalias": Hier wird die Bezeichnung des Dienstes angegeben. Dieser ist über die Dienstverwaltung eines Windows-Systems ermittelbar, siehe dazu Punkt 1 aus der Grafik.



Parameter "RemoteIP [optional]": Hier kann das Zielsystem angegeben werden. Dieses wird über RPC angesprochen und der Dienststatus abgefragt. Ist der Wert leer so werden alle Abfragen lokal ausgeführt.

Verzeichnis erreichbar:

Erklärung: Hier wird die Erreichbarkeit eines Verzeichnisses geprüft. Möglich sind alle Arten von Pfaden, also auch eine Angabe wie "\\192.168.0.1\C\$\Windows\".

Parameter "Pfad": Eingabe des zu prüfenden Pfades. Die Eingabe des Pfades muss nicht zwingend mit einem „\“ enden. Der SysWatcher kann mit beiden Pfaden umgehen.

Registrywert:

Erklärung: Hier ist es möglich einen Registryeintrag auf einen bestimmten Wert zu überprüfen. Hat der Eintrag den gewünschten Wert "Prüfwert", so gilt dieser Sensor als ausgelöst. Das Verhalten kann mit der Einstellung "invertiert" auch gedreht werden, siehe dazu „[Spezielle Einstellungsmöglichkeiten](#)“.

Parameter "Zweig": Die Eingabe des Zweiges besteht aus 2 Teilen (Root und Pfad). Root kann folgende Werte annehmen:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_USERS
- HKEY_PERFORMANCE_DATA
- HKEY_CURRENT_CONFIG

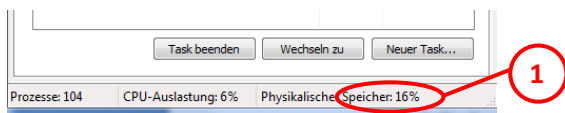
- HKEY_DYN_DATA
- HKEY_LOCAL_MACHINE

Damit wäre eine gültige Eingabe: "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ITProg\SysWatcher\ClientVersion". Hier wird der Wert des Schlüssels "ClientVersion" aus dem Pfad "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ITProg\SysWatcher\" zur Prüfung herangezogen.

Parameter "Prüfwert": Hier wird der zu prüfende Wert eingetragen. Dabei ist es egal, welches Format der Schlüsselt in der Registry hat.

RAM Belegung (Prozent):

Erklärung: Hier wird der systemweite Wert "dwMemoryLoad" ermittelt der aussagt, wie viel des physischen Speichers in Prozent belegt ist. Dies entspricht dem gleichen Wert der im Taskmanager zu sehen ist (Punkt 1).



Parameter "Schwelle": Ist der Wert höher als diese Schwelle, so gilt der Sensor als ausgelöst.

Rückgabewert: Der Sensor gibt den aktuellen Prozentwert des Systems zurück und kann mit %WERT1% in die Mailtexte eingebunden werden. Im Rückgabewert ist die Einheit % schon enthalten.

CMD Prüfung:

Erklärung: Hier wird das entsprechende Kommando ausgeführt und dessen Konsolenausgabe ermittelt. Diese wird dann mit einem Suchfilter verglichen. Passen diese nicht zusammen gilt der Sensor als ausgelöst. Ist ein Programm nicht innerhalb von 10 Sekunden beendet wird es automatisch geschlossen und alle bis dahin entstandenen Ausgaben werden zur weiteren Verarbeitung herangezogen.

Parameter "Kommando": Ist das zu startende Kommando mit Parametern. Beispiel „ipconfig /all“.

Parameter "Suchfilter": Wird in diesem Parameter kein „*“ oder „?“ verwendet, so wird die gesamte Zeichenkette in der Ausgabe gesucht. Groß- und Kleinschreibung ist dabei relevant. Sind diese Wildchars aber enthalten wird exakt wie beim Suchen von Dateien vorgegangen, also „*“ bedeutet alles und „?“ ersetzt nur ein beliebiges Zeichen. Eine passender Filter wäre „*192.???.*“.

Rückgabewert: Der Sensor gibt die aktuelle Ausgabe des Kommandos in %WERT1% zurück. Diese kann dadurch in die Mailtexte eingebunden werden.

5. Spezielle Einstellungsmöglichkeiten:

Invertiert: Ist diese Einstellung gesetzt, so wird der Sensorzustand vor der Auswertung noch einmal invertiert. Das heißt, wenn der Zustand vorher ausgelöst war ist er jetzt nicht mehr ausgelöst. Beim „Testen“ Knopf wird diese Einstellung schon mit berücksichtigt.

Prüfzeitpunkt: Diese Funktion wird eher selten genutzt. Entstanden ist diese aus folgender Problematik: Mein eigener Server ist so konzipiert, dass die Festplatten immer herunterfahren wenn diese nicht genutzt werden. Dadurch erhöht sich die Laufzeit der Platten enorm. Würde nun ein Sensor jede Minuten die freie Festplattenkapazität prüfen, wären diese nie im Spindown Zustand und würden permanent laufen. Ist ein Prüfzeitpunkt eingestellt, z.B. 22:00:00 Uhr, so würde der Sensorzustand nur um 22:00:00 Uhr, oder nach einem Dienstneustart nach 22:00:00 Uhr geprüft werden. Ist der Zustand bei dieser Prüfung ausgelöst, wird sofort die Fehlermail gesendet. Die Einstellung „Ausfallzeit“ hat dann keine Bewandnis mehr. Allerdings wird auch die nächste Prüfung erst durchgeführt wenn wieder die 22:00:00 Uhr Marke überschritten wird. Deshalb kommt auch die „Erledigtmeldung“ erst am nächsten Tag, oder wenn der Dienst nach 22:00:00 Uhr neu gestartet wird.

HTTP-URL in den Haupteinstellungen: In den Mailtexten gibt es den Platzhalter %STATUSURL%, welcher durch diese Zeichenkette ersetzt wird. Damit hat man die Möglichkeit den Zugriff auf den WebServer direkt in die Mails zu integrieren. Mit ein bisschen Ahnung von HTML kann man dort leicht seine eigenen Modifikationen durchführen, also beispielsweise den Ausgabertext ändern, oder auch das Ziel. Im normalen Betrieb muss man daran denken das der Port für die HTTP-Anfragen im URL mit eingetragen ist. Im Standard ist das die 9999. Eine korrekte Funktionsweise setzt dabei voraus, dass der TCP-Port 9999 von außen auch auf den internen Port 9999 des Hauptdienstes am Router umgesetzt wird. Auch die Firewall muss den Port durchlassen. Der lokale Port des Hauptdienstes wird im darüber liegenden Feld „Port“ eingetragen und darf natürlich von keiner anderen Anwendung verwendet werden.

Prüfintervall in Minuten: Der Hauptdienst ist so aufgebaut, dass die Prüfung der Events nur aller einer bestimmten Zeit durchgeführt wird (Standard „1 Minute“). Dabei werden alle Events nacheinander abgefragt. Wenn der Durchlauf beendet ist wird genau diese Zeit gewartet die hier eingetragen ist.

Extra-Logfile: Dies ist eine Einstellung in der man bestimmte Events in einem „Extra-Logfile“ mitprotokolieren kann. Das Logfile ist sehr einfach aufgebaut und zeigt jeden Zustandswechsel an:

- „0“ : Sensor ist nicht ausgelöst
- „1“ : Sensor ist ausgelöst
- „W“ : Wiederholungsmeldung wurde ausgelöst

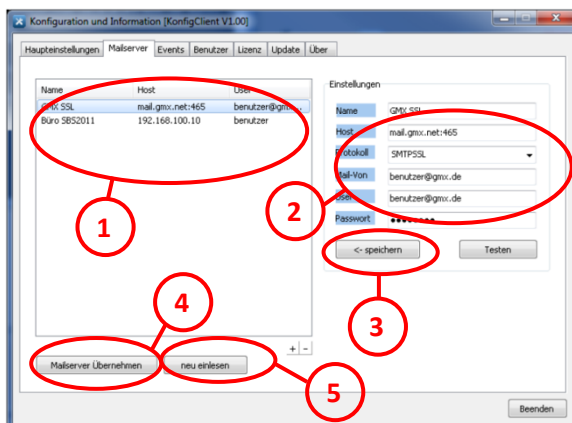
Das Verzeichnis des Logfiles wird automatisch erzeugt.

6. App-Schnittstelle:

Ab Version V1.02 ist der SysWatcher mit einer Schnittstelle ausgestattet die es ermöglicht die Daten auch von einem App (SysWatcher ClientApp) auslesen zu lassen. Dieser Zugang ist über den HTTP-Server realisiert. Will man das App nutzen muss man also auch den HTTP-Server aktivieren. Der Zugriff auf die Daten ist gesichert und kann über die Benutzerverwaltung gesteuert werden. Alle User die Zugriff auf die Web-Schnittstelle haben, können auch das App nutzen.

7. Prinzipieller Ablauf von Listenänderungen:

Der Ablauf von Änderungen in Listen ist auf jeder Maske gleich. Zuerst sucht man sich den entsprechenden Eintrag in der Liste raus und klickt diesen an (Punkt 1). Dadurch werden alle Einstellungen in „Punkt 2“ angezeigt und können dort verändert werden. Durch einen Klick auf „<-speichern“ (Punkt 3) werden diese wieder in die Liste übernommen. Erst wenn man beispielsweise „Mailserver Übernehmen“ (Punkt 4) klickt werden die Daten in die Datenbank auf der Festplatte geschrieben. Der Hauptdienst übernimmt die Einstellungen erst nach einem Neustart, weshalb bei Betätigung des Knopfes danach gefragt wird. „Punkt 5“ ist schließlich dazu da, dass man die Einstellungen aus der Datenbank erneut auslesen kann. Dadurch gehen aber alle Seiteneinstellungen verloren und es werden wieder die Daten vom letzten Speichervorgang angezeigt. Die Daten auf allen anderen Tabs (Haupteinstellungen, Events, Benutzer usw.) bleiben von allen Aktionen unberührt. Die Funktionsweise auf diesen Tabs ist aber äquivalent zu den hier beschriebenen.



[Rechtsklick auf Listeneintrag]



Mit einem Rechtsklick auf einen Eintrag sind weitere Funktionen verfügbar, wie löschen, duplizieren usw. Die Daten aus der Liste werden erst in die aktive Datenbank übernommen, wenn der Knopf „Punkt 4“ gedrückt wird.

Wird ein neuer Eintrag hinzugefügt, werden im „Punkt 2“ die Standard bzw. duplizierten Werte angezeigt und der Knopf (Punkt 3) ändert sich auf „<-hinzufügen“. Bei Betätigung wird nun der neue Eintrag am Ende der Liste hinzugefügt.