Benutzerhandbuch

© Michael Rothofer

Inhalt

Diese Dokumentation erhebt keinen Anspruch auf Vollständigkeit.

node***WATCH***
wurde entwickelt um die täglichen Überwachungsaufgaben eines Administrators zu erleichtern.

Bei der Entwicklung standen und stehen folgende Punkte im Vordergrund. Die Software sollte
einfach bedienbar,
schnell erlernbar und konfigurierbar
und **universell** einsetzbar sein.

einfach – schnell - universell

Installation

Die Installation von node***WATCH*** erfordert folgende Mindestvoraussetztungen:

Betriebssystem: Microsoft Windwos 7, Windwos 10, Windows Server 2012, Windows Server 2016

Arbeitsspeicher: 4 GB

Festplattenspeicher: 50 GB

Datenbank: MS SQL-Server Express ab Version 2016

Nennen Sie für die Installation ggf. die Datei Setup.bak in Setup.exe um und führen sie die Datei aus.

Setup

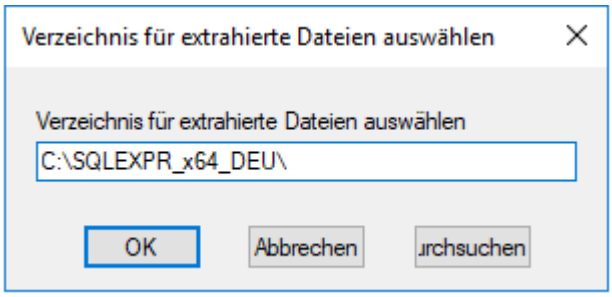
Bevor Sie mit der Installation von node***WATCH*** beginnen, sollten sie zuvor SQL-Server Express ab Version 2016 installieren.

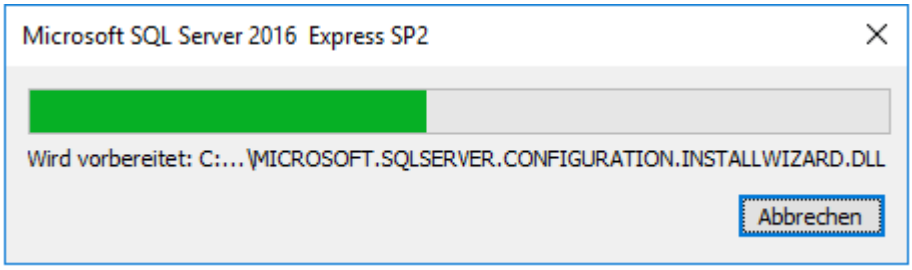
SQL Express Installation

Laden Sie MS SQL-Server Express 2016 oder später von folgender Seite herunter:

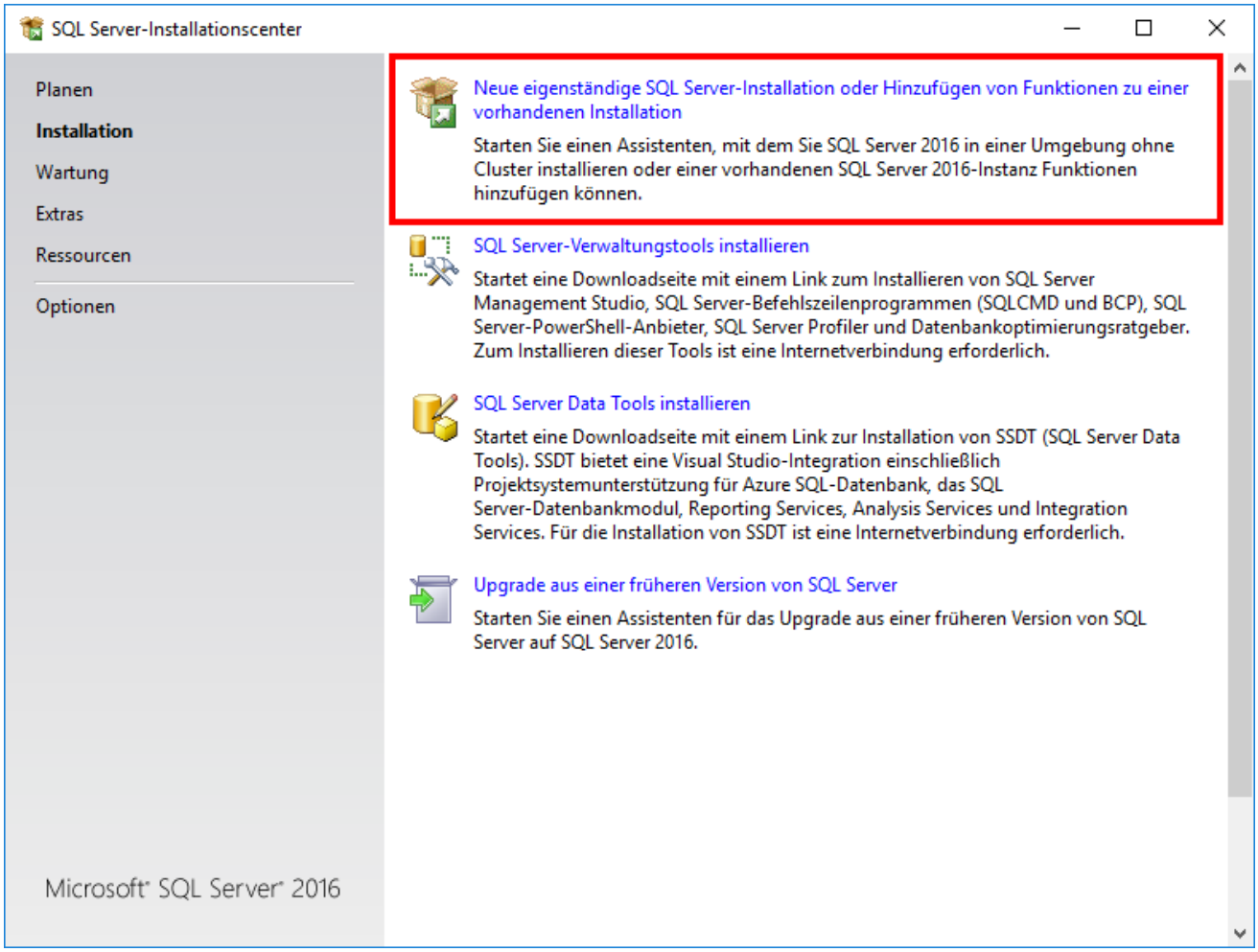
https://www.microsoft.com/de-DE/download/details.aspx?id=56840

Starten Sie das Setup und folgen Sie den Anweisungen. Nach dem Start des Setups müssen Sie zuerst ein Verzeichnis angeben, in dem die extrahierten Dateien abgelegt werden können.

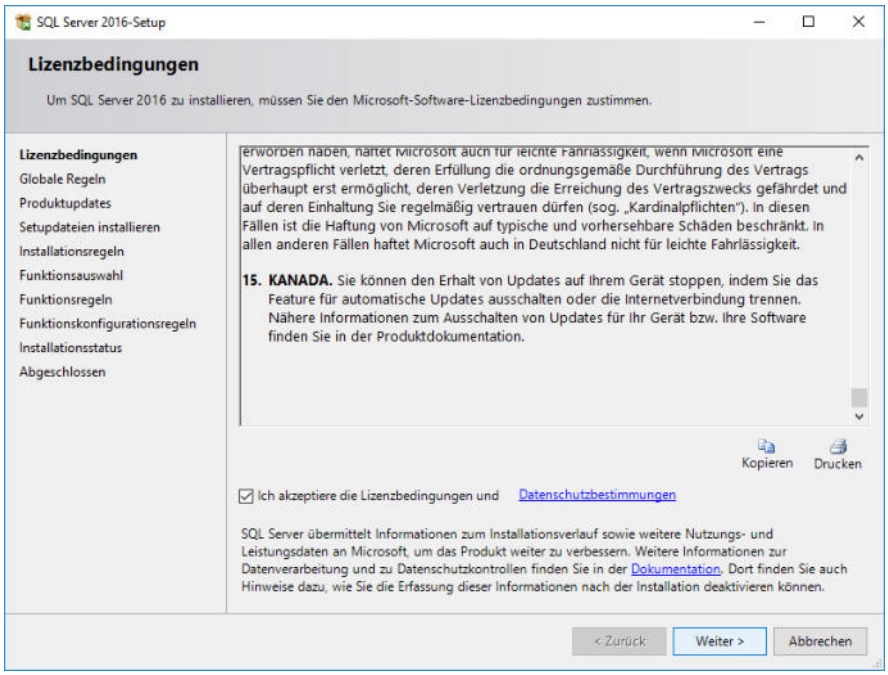


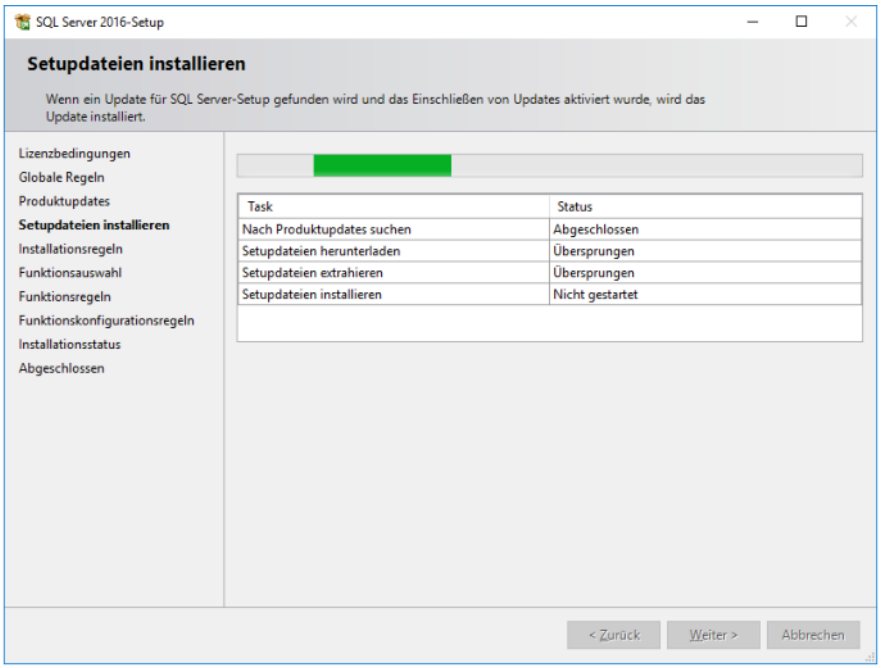


Nach dem entpacken der Dateien öffnet sich das Installationscenter, Wählen Sie hie den obersten Punkt **Neue eigenständige SQL Server-Installation oder Hinzufügen von Funktionen zu einer vorhandenen Installation**.

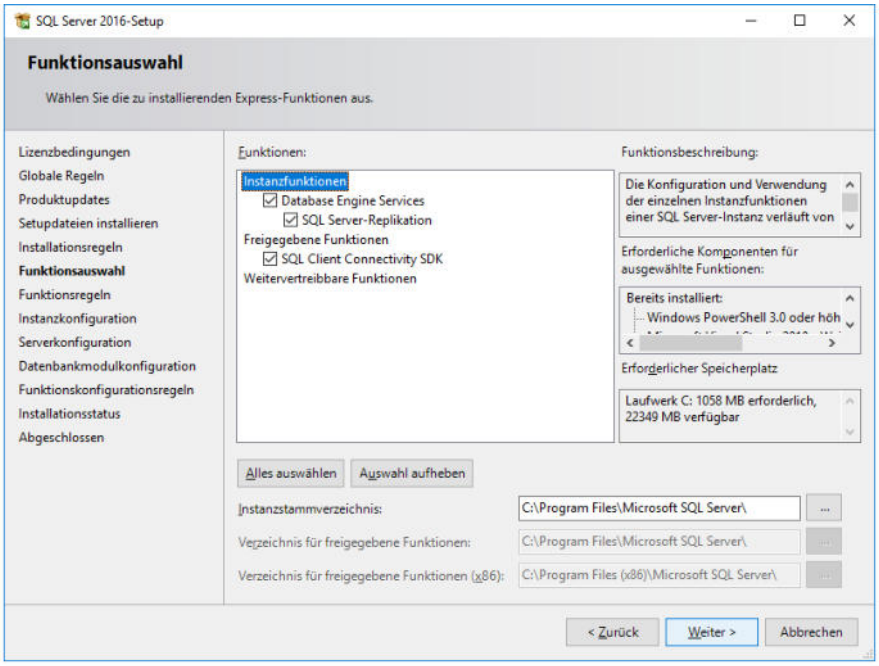


Gehen Sie schrittweise durch die Installation und folgen Sie den Anweisungen.

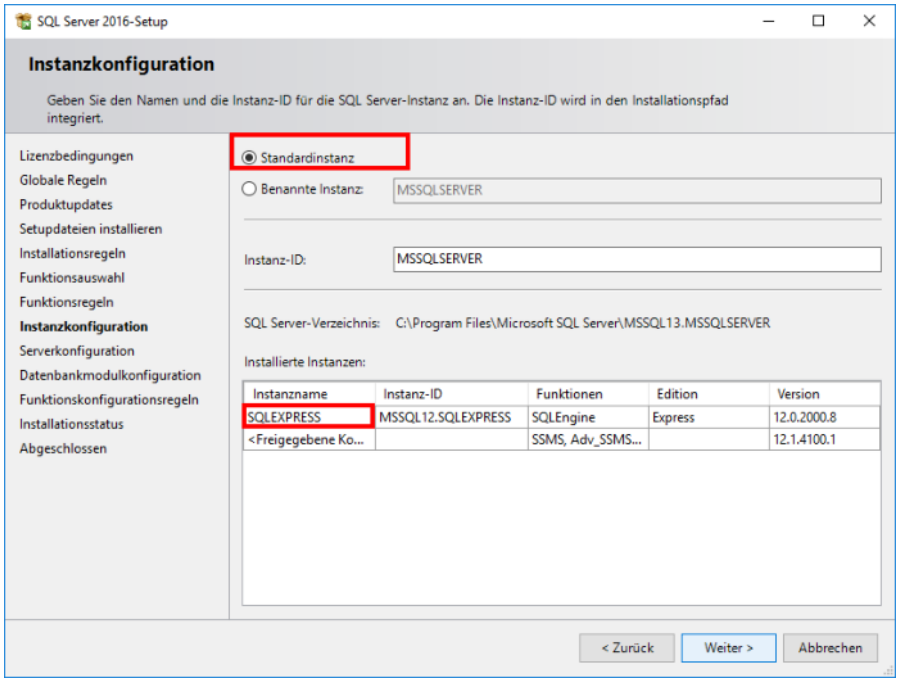




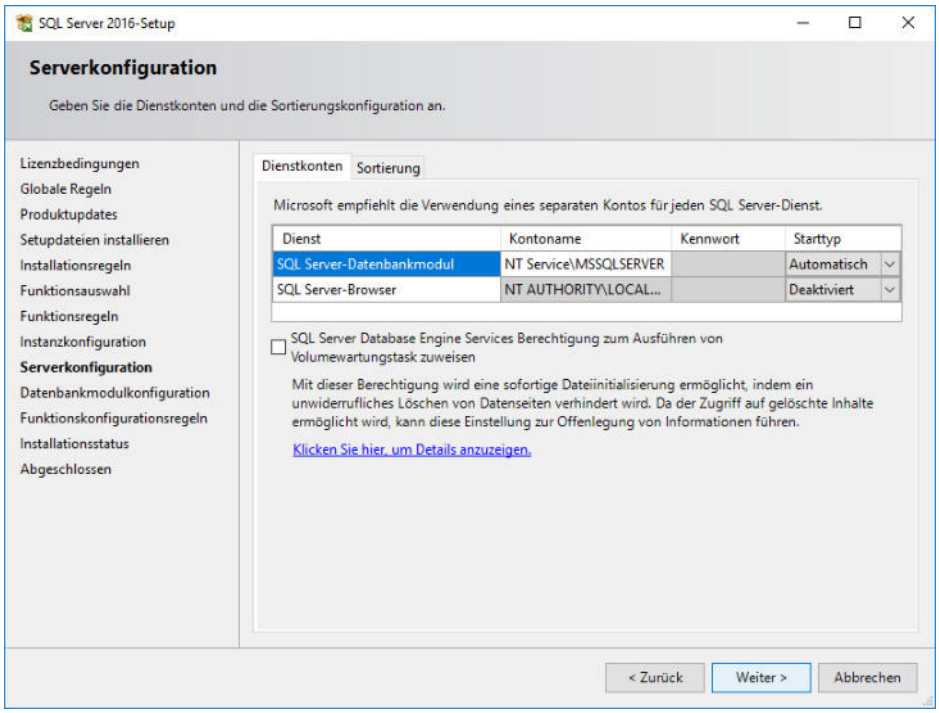
Wählen Sie die mindestens die Funktion **Database Engine Service** und **SDK Client Connektivity, SDK** aus.



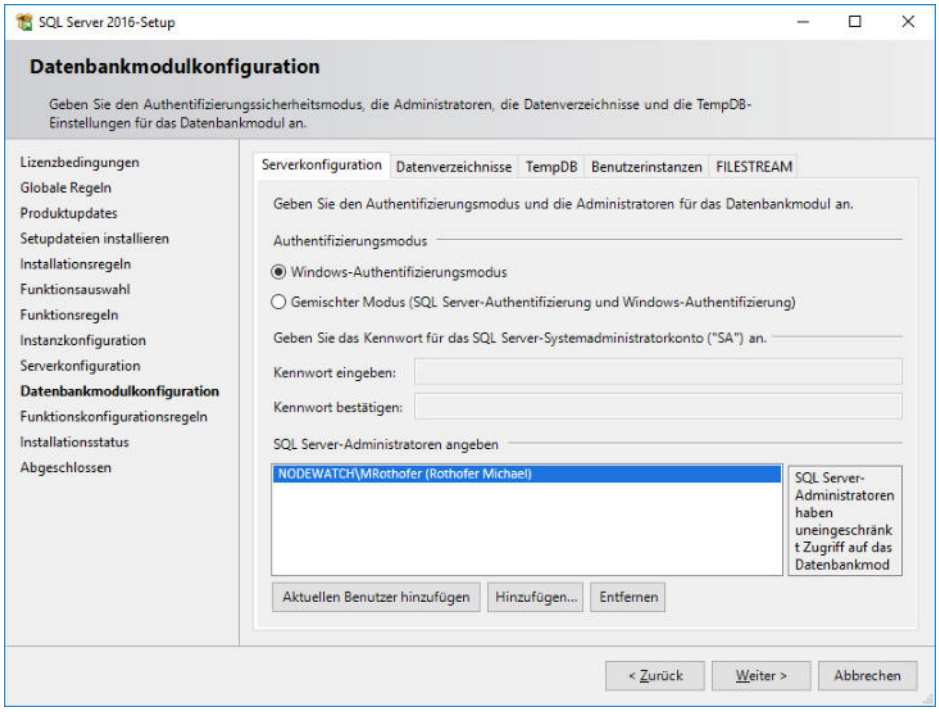
Als Instanz sollte **Standardinstanz** ausgewählt und als Instanz Name **SQLEXPRESS** eingetragen werden.

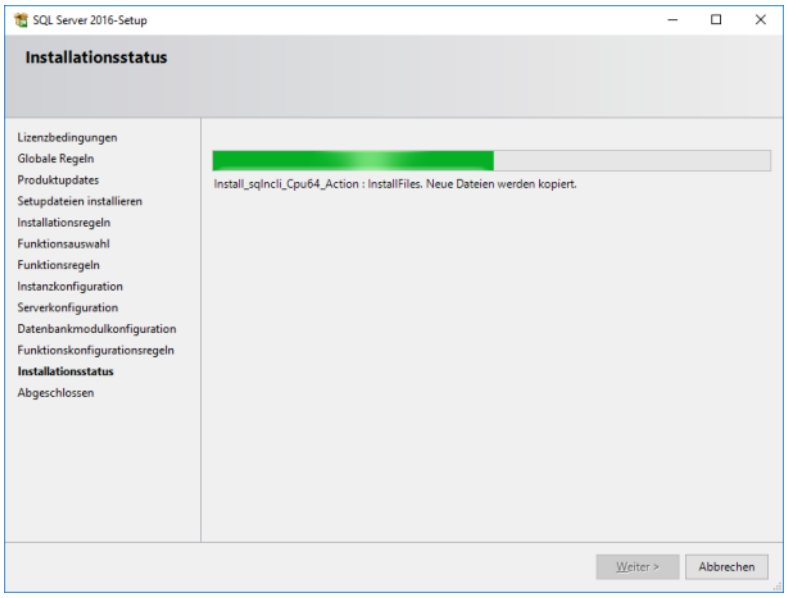


Bestätigen Sie die Serverkonfiguration mit Weiter.

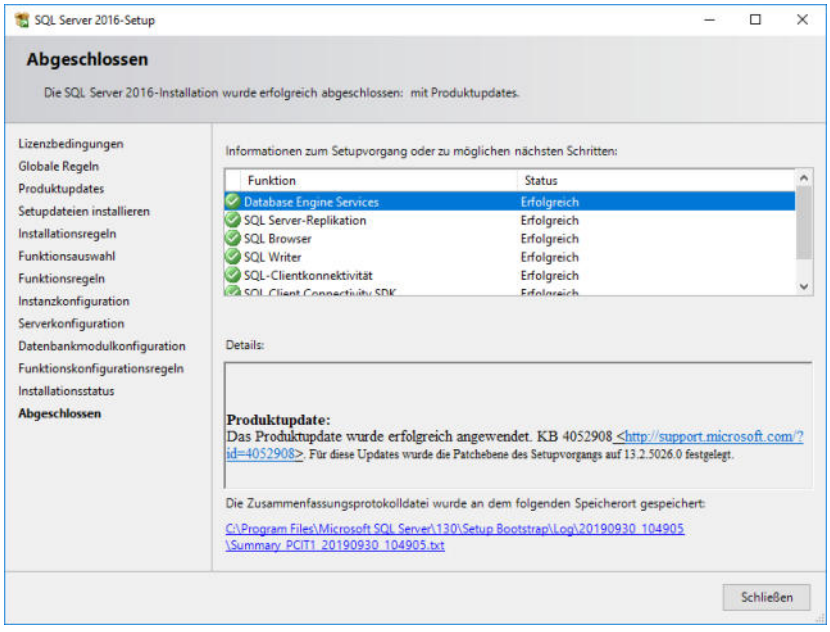


Wählen Sie bei Datenbankkonfiguration **Windows-Authentifizierungsmodus.**

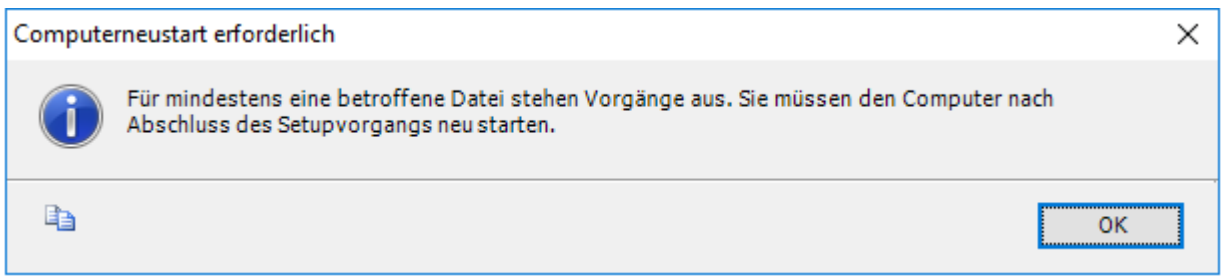




Wenn alles geklappt hat, dann sollte am Ende der Installation folgendes Bild erscheinen:

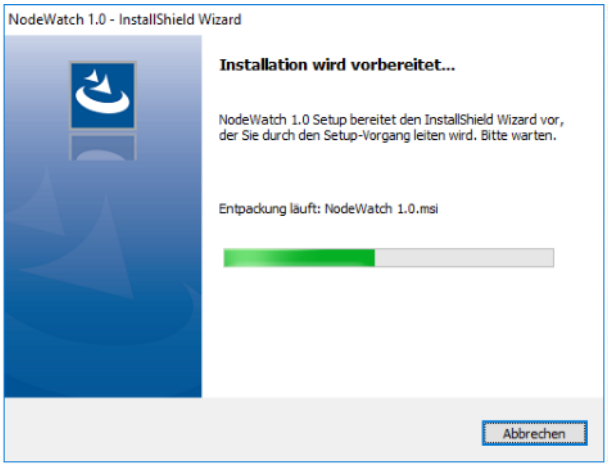


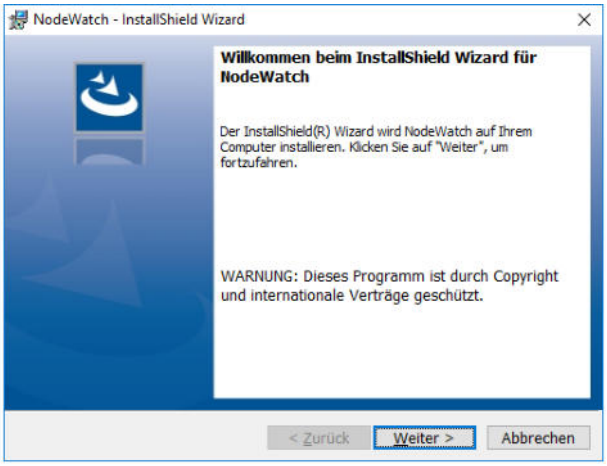
Eventuell müssen Sie den Computer neu starten um die Installation abzuschließen.

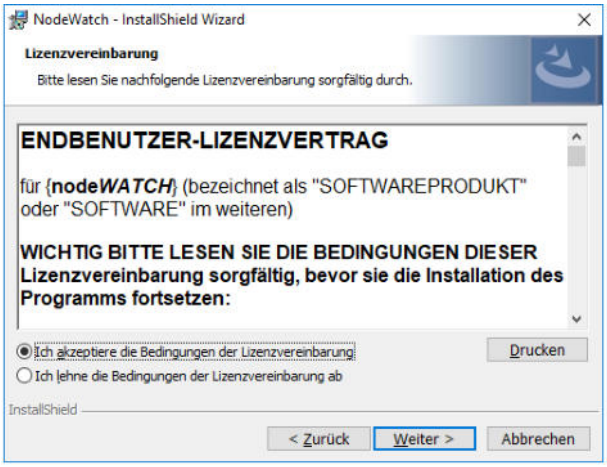


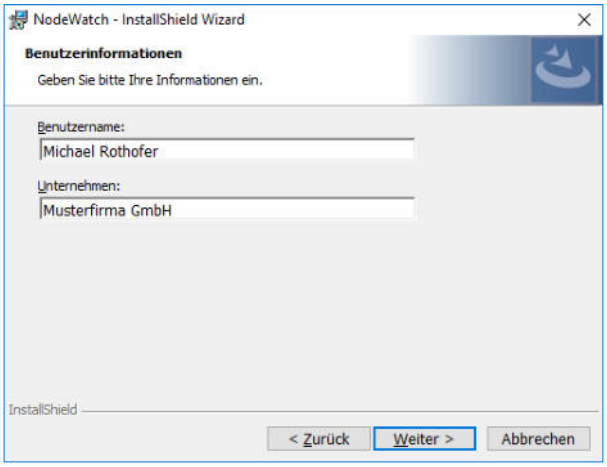
nodeWATCH Installation

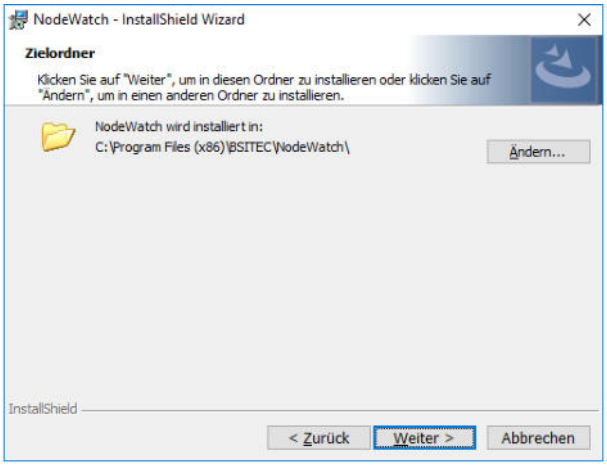
Nach der Installation von SQL Server-Express kann mit der Installation von nodeWATCH begonnen werden. Führen Sie hierzu die Setup.exe aus. Der Assistent führt Sie schrittweise durch die Installation.

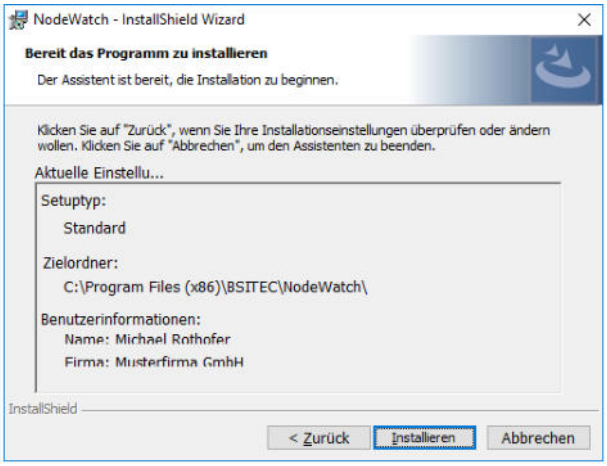


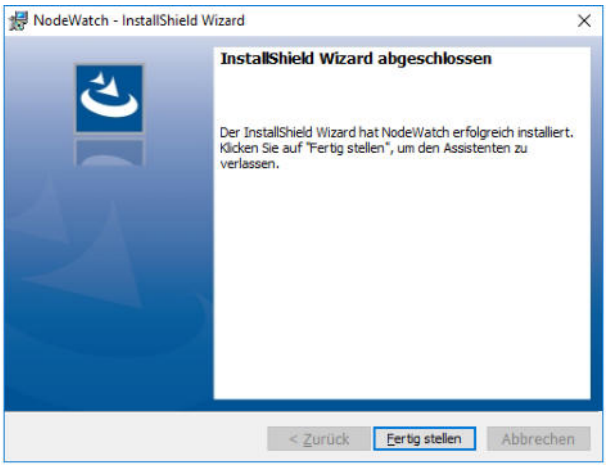






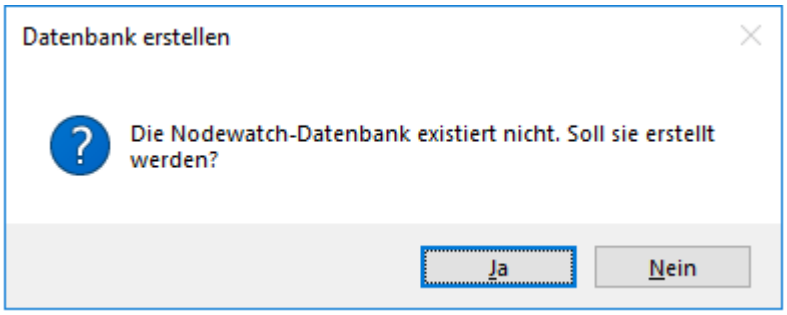




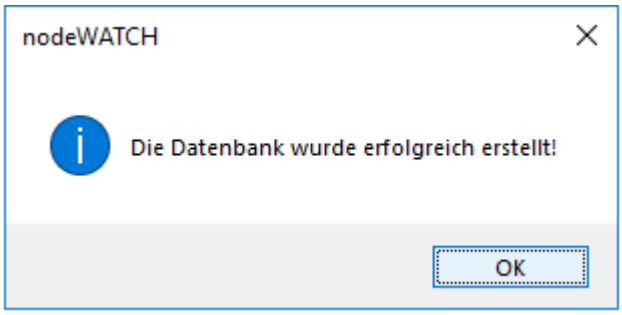

NodeWatch - InstallShield Wizard
InstallShield Wizard abgeschlossen
Der InstallShield Wizard hat NodeWatch erfolgreich installiert. Klicken Sie auf "Fertig stellen", um den Assistenten zu verlassen.
< Zurück
Fertig stellen
Abbrechen

Erste Schritte

Nach dem erstmaligen Start von node***WATCH*** wird die Datenbank eingerichtet. Das System sucht nach der lokalen MS SQL-Express Datenbank und verbindet sich damit. Nach erfolgreicher Verbindung werden Sie gefragt, ob die node***WATCH*** Datenbank erstellt werden soll.

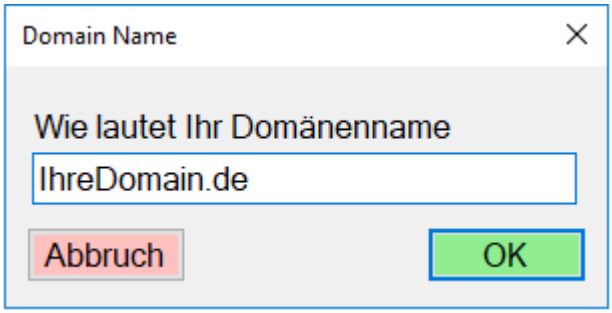


Beantworten Sie diese Frage mit **Ja**.
Nach erfolgreicher Erstellung erscheint eine Bestätigungsmeldung.



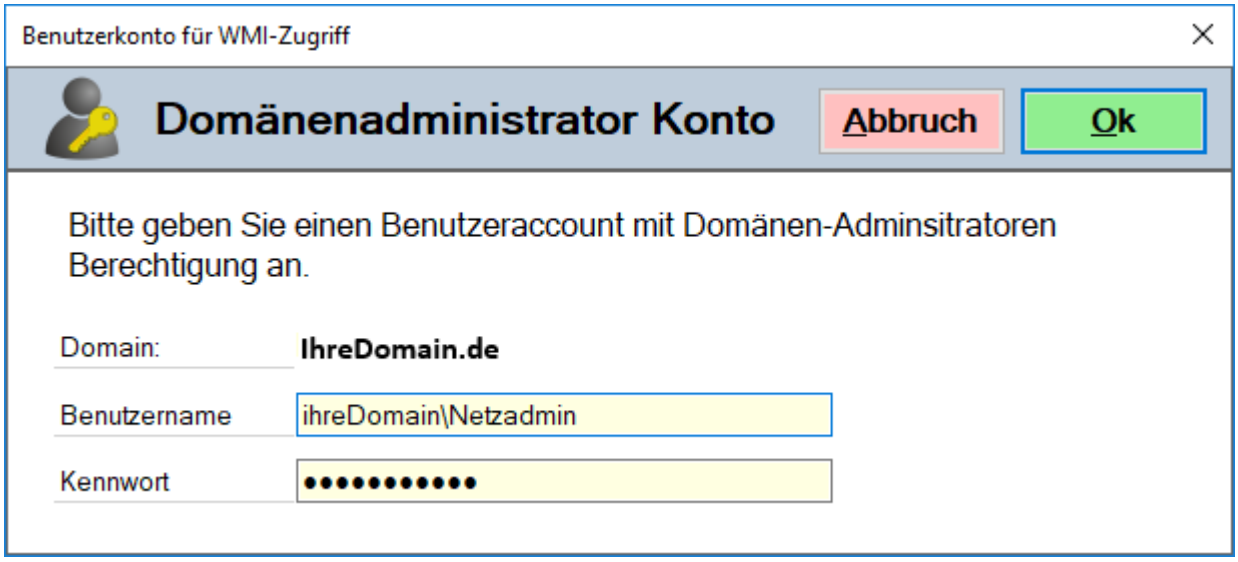
Nun, wo die Datenbank erfolgreich angelegt werden konnte, werden als nächstes die Tabellen generiert und Standardwerde eingefügt.

Ein zentraler Bestandteil von node***WATCH*** ist die Überwachung von Active-Directory, weshalb im nächsten Schritt der Name der internen Domäne abgefragt wird. Dieser ist ebenfalls für die Lizenzierung von zentraler Bedeutung. Sind Sie mit einem Domänenkonto angemeldet, dann wird die Domäne bereits vorgeschlagen.



Bestätigen Sie Ihren Domänennamen mit OK.

Für die Überwachung der Netzwerkgeräte ist ein Benutzerkonto mit Domänenadministratoren Berechtigungen erforderlich. Geben Sie deshalb im nachfolgenden Fenster ein Benutzerkonto mit entsprechenden Berechtigungen an.



Nun wird die node***WATCH-***Oberfläche das erste Mal gestartet und im Hintergrund folgende Aufgaben durchgeführt. Zuerst werden die im Active-Directory Standorte und Dienste hinterlegten Standorte samt Netzadressen ausgelesen und in den Stammdaten hinterlegt. Dieser werden für die Standortzuordnung der zu überwachenden Geräte herangezogen.

Im Anschluss wird versucht die Windows Server zu ermitteln und für die Überwachung einzurichten. Der Fortschritt wird in der Mitte des node***WATCH***-Logos angezeigt. Während des Scanvorgangs sind die Schaltflächen **Überwachung starten** und **Überwachung konfigurieren** deaktiviert.

Wenn das System über eine Internetverbindung verfügt und der Port 3113 ausgehend geöffnet ist, dann wird parallel zum Scan eine Lizenzanforderung gesendet und bei Erstinstallation eine entsprechende Testlizenz für einen begrenzten Zeitraum freigeschaltet.

Nachdem die Lizenzanforderung und der Systemscan abgeschlossen sind, werden die Schaltflächen **Überwachung starten** und **Überwachung konfigurieren** wieder aktiviert.

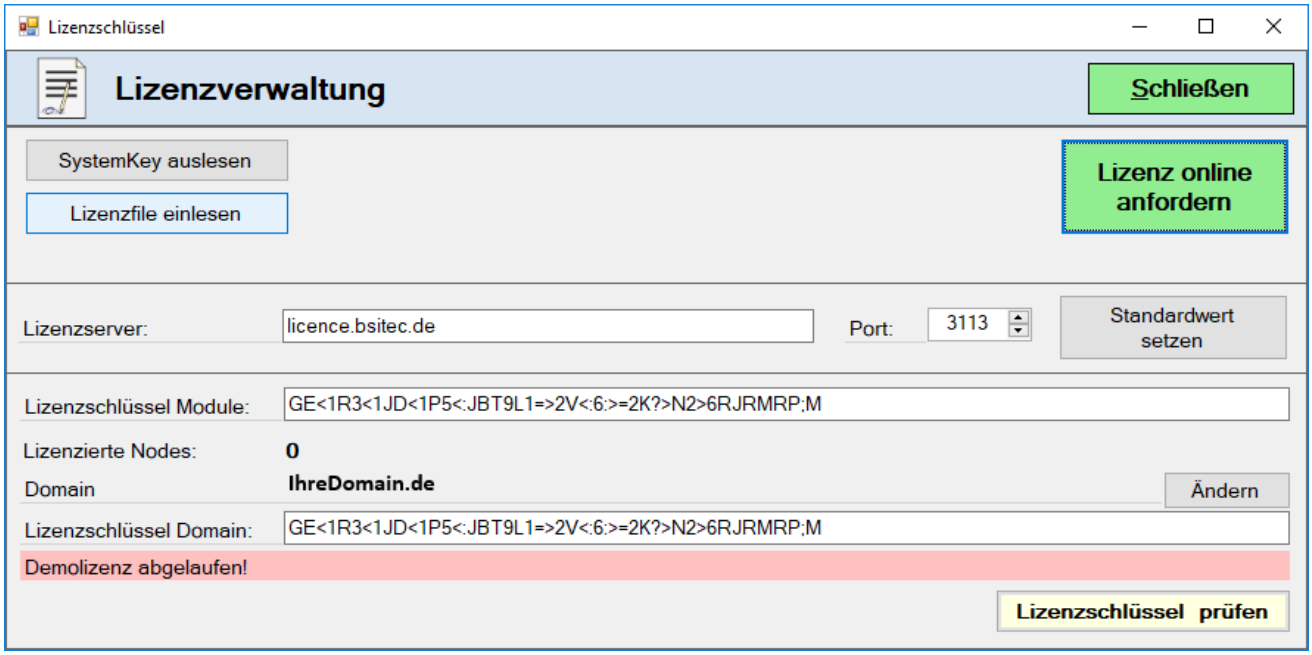
Dieser Vorgang wird nur beim allerersten Start von node***WATCH*** ausgeführt.

Ist die automatische Lizenzanforderung fehlgeschlagen, dann können Sie das nun über den Button **Lizenzverwaltung** erneut versuchen.

Lizenzverwaltung

Um node***WATCH*** verwenden zu können, müssen Sie zuerst einen gültigen Lizenzschlüssel eintragen. Die Verwendung der Software ist an einen eindeutigen SystemKey gebunden. Zur Generierung eines gültigen Lizenzschlüssels ist es erforderlich, diesen eindeutigen SystemKey an den Lizenzgeber zu senden.

Klicken Sie in der Lizenzverwaltung auf die Schaltfläche **Lizenz online anfordern**. Das System verbindet sich daraufhin mit dem Lizenzserver und erhält bei erstmaliger Installation einen Lizenzschlüssel zum Testen der Software.



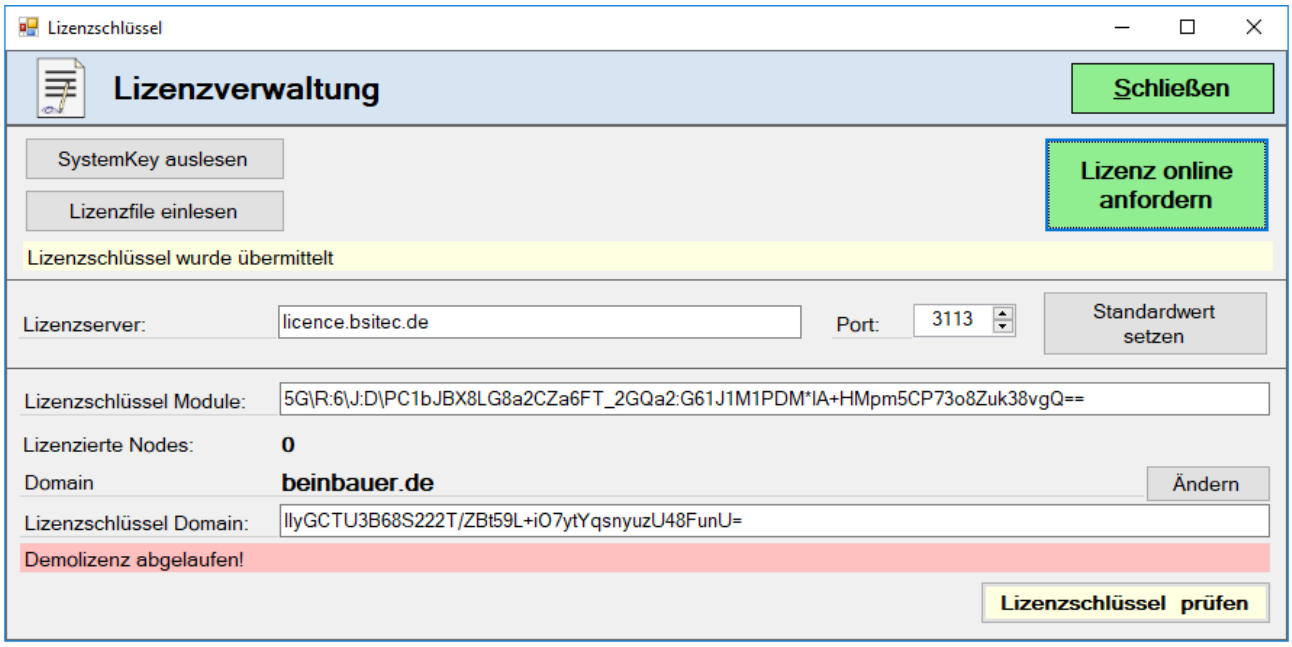
Bei Problemen kann das Lizenzfile auch manuell angefordert werden. Klicken Sie hierfür im Hauptmenü auf die Schaltfläche Lizenzverwaltung, dann auf **[SystemKey auslesen]**.

Speichern Sie den Key auf Festplatte und senden sie ihn an licence@nodewatch.de.

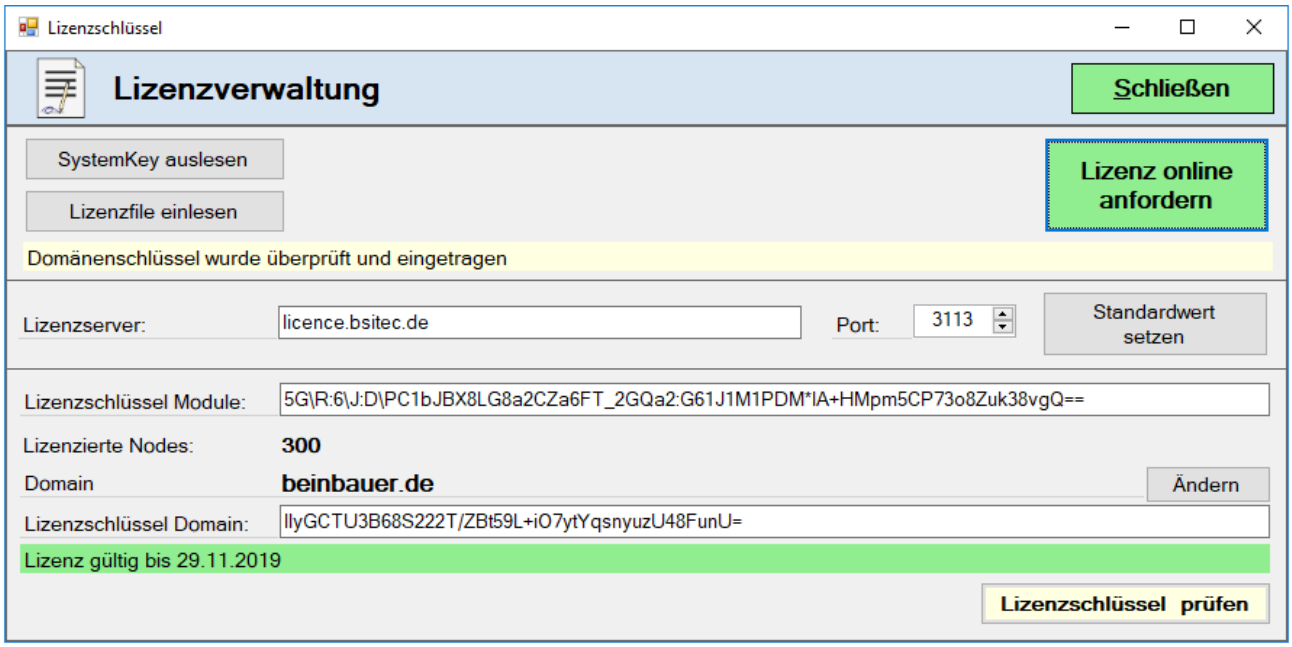
Der Systemkey enthält eindeutige Hardwareinformationen, so dass der Lizenzschlüssel dem System exakt zugeordnet werden kann.

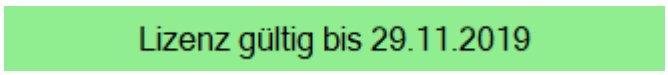
Nach Eingang Ihrer Anfrage wird ein Freischaltcode für Ihr System generiert, der Ihnen ebenfalls via Email zugesandt wird.

Sie können dann das Lizenzfile über die Schaltfläche **Lizenzfile einlesen** zuordnen.



Durch drücken auf den Button „**Lizenzschlüssel prüfen**“ können wird die Gültigkeitsdauer des Schlüssels angezeigt.





Nach Ablauf der Lizenz sind Sie nicht mehr berechtigt, die Software zu verwenden und die Module werden deaktiviert!

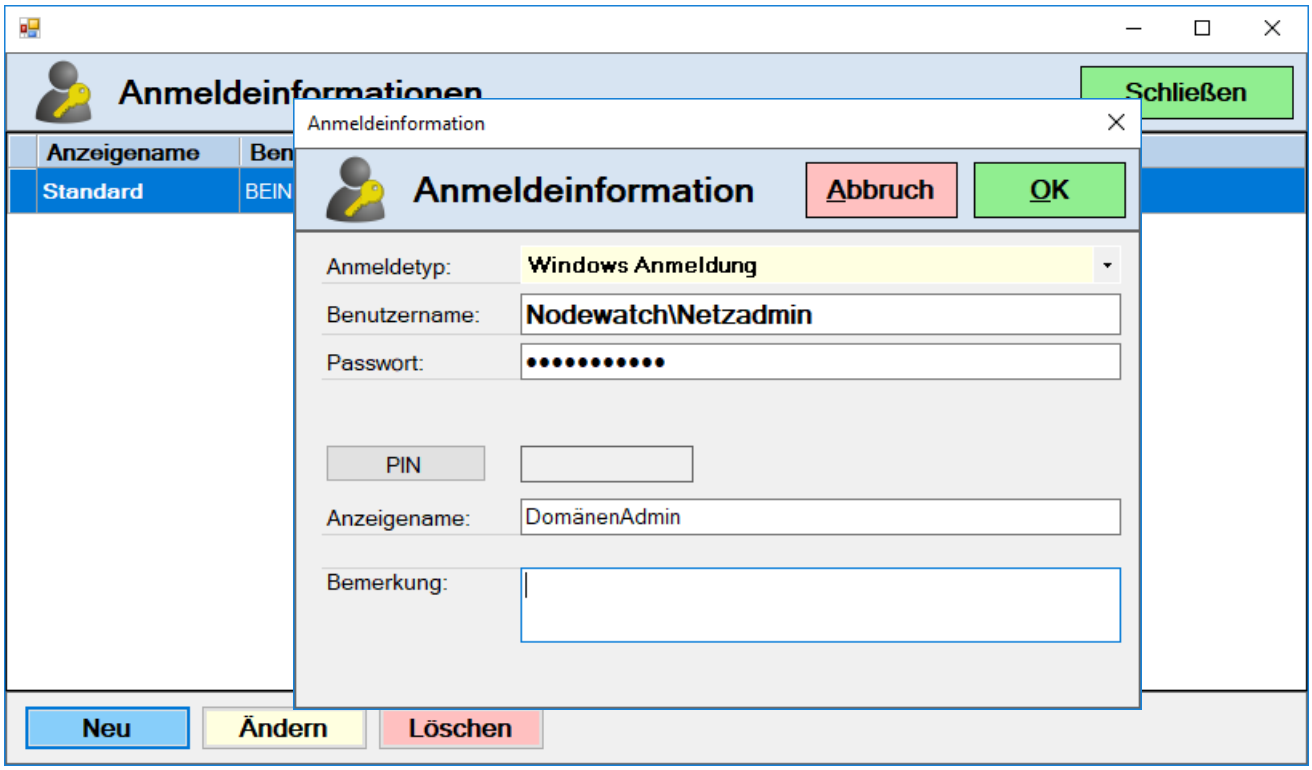
Basis Konfiguration

Vor der ersten Verwendung sollten zuerst einige Stammdaten gepflegt werden. Der Benutzer, unter dem node***WATCH*** ausgeführt wird benötigt nicht zwingend administrative Berechtigungen. Mittels des Menüpunkts Authentifizierung können verschiedene Benutzerkonten hinterlegt werden.

Authentifizierung

Im Fenster zur Verwaltung der Authentifizierung wird an erster Stelle immer die lokale Anmeldung angezeigt. Dieser Eintrag kann nicht gelöscht, oder geändert werden.

Durch betätigen der Schaltfläche Neu können beliebig viele Accounts hinzugefügt werden.



Als Anmeldetyp kann entweder Windows Anmeldung oder SQL-Server Anmeldung verwendet werden.

Lokale Anmeldung macht keinen Sinn, da bereits ein Standardeintrag mit Lokale Anmeldung vorhanden ist.

Windows-Anmeldung

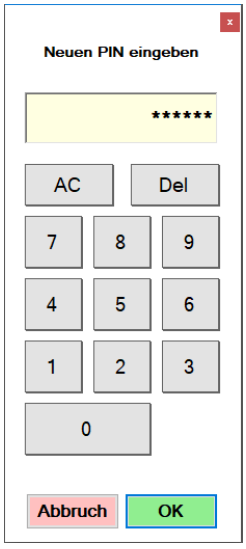
Bei Windows-Anmeldung können sowohl Domänenkonten, als auch lokale Konten angegeben werden. entspricht die Schreibweise Domäne\Benutzername oder Computername\Benutzername.

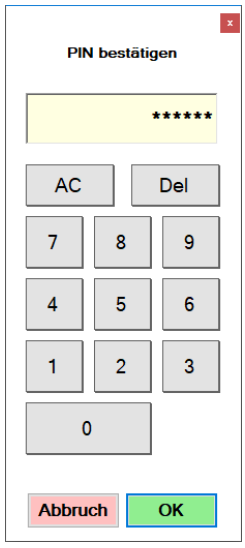
Bei Auswahl von Windows-Anmeldung wird eine zusätzliche Schaltfläche zur Eingabe eines PINs angezeigt. Der PIN ist erforderlich um Aktivitäten im Active Directory durchführen zu können. Ohne PIN stehen bestimmte Funktionen wie z.B.

- Benutzerkonto entsperren
- Kennwort zurücksetzen
- Konto aktivieren /deaktivieren
- Ablaufdatum setzen/entfernen
- Remote Neustart von Windows-Systemen

nicht zur Verfügung.

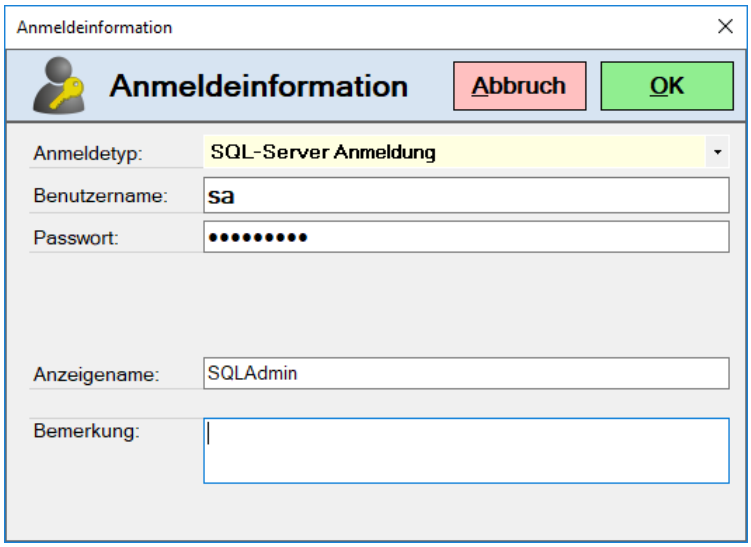
Nach Eingabe eines PINs muss dieser noch einmal bestätigt werden.





SQL-Server Anmeldung

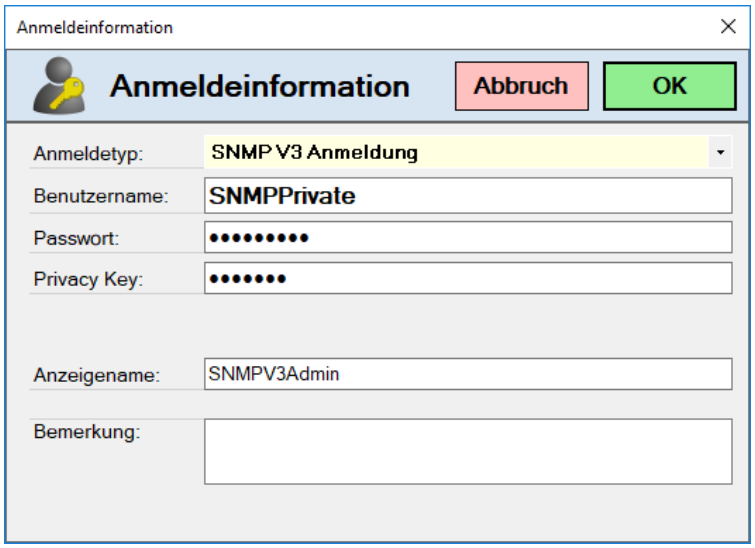
Für die Überwachung von MS SQL-Server Aktivitäten können lokale Anmeldeinformationen eines SQL-Servers hinterlegt werden.



Diese stehen dann bei der Konfiguration von SQL-Server Überwachungen als Auswahl zur Verfügung.

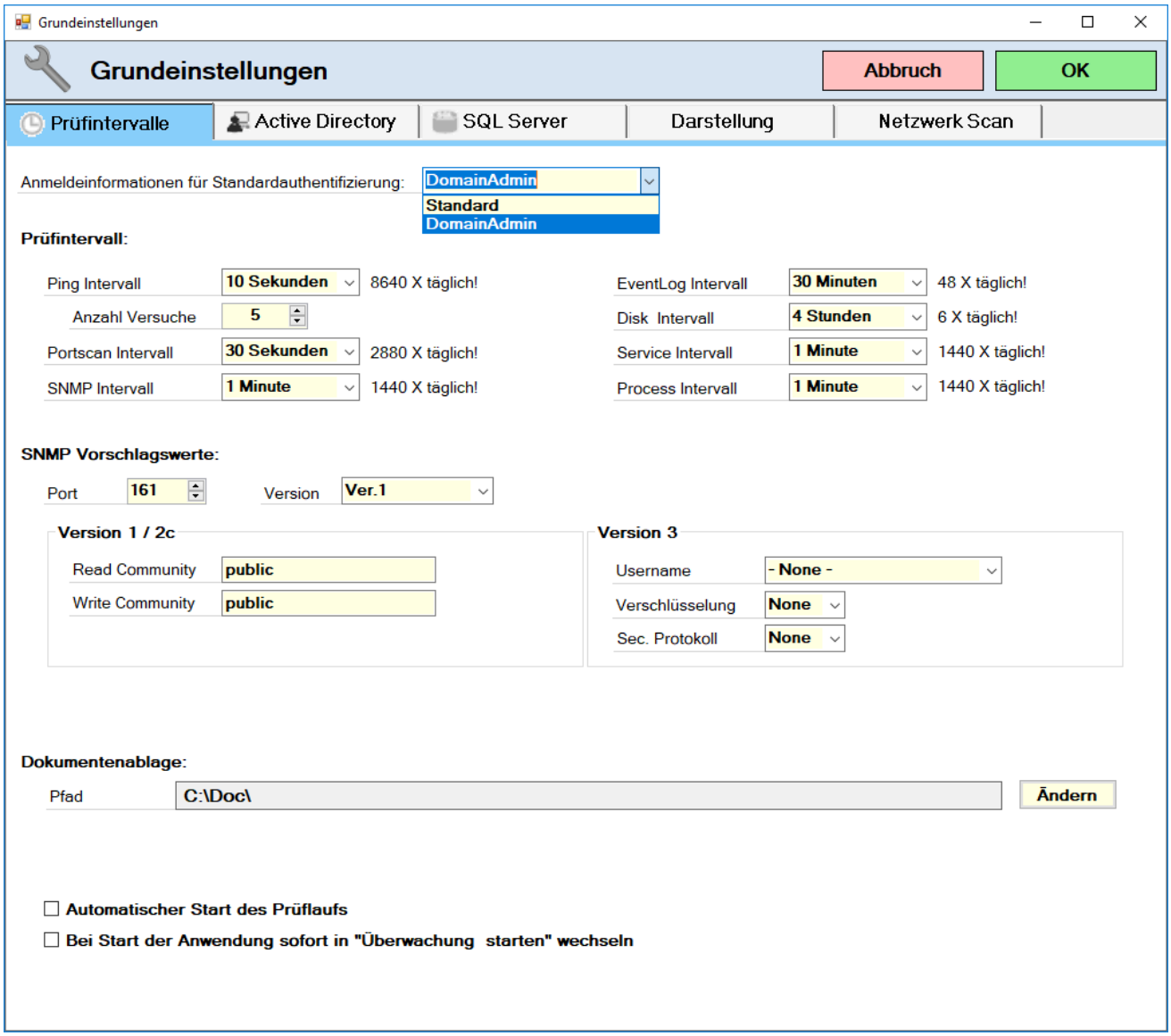
SNMP V3 Anmeldung

Für Geräteüberwachungen auf SNMP V3 Basis können hier die Zugangsdaten hinterlegt werden. Hash Funktionen (MD5 / SHA1) und Verschlüsselung DES / AES werden in der zu überwachenden Node hinterlegt.



Grundeinstellungen

In den Grundeinstellungen werden die zentralen Anmeldeinformationen hinterlegt, die bei der Prüfung der Systeme verwendet werden sollen. Hier können alle zuvor unter Anmeldeinformationen angelegten Windows-Benutzer ausgewählt werden. Das hier hinterlegte Benutzerkonto sollte ausreichend berechtigt sein, um die jeweiligen WMI-Abfragen auf den zu überwachenden Systemen durchführen zu können.



Prüfintervalle

Im Register Prüfintervalle wird der Zeitintervall eingestellt, in dem die Systeme überprüft werden sollen.

Folgende Prüfungen stehen zur Verfügung:

- **Ping Inervall** Führt im angegebenen Intervall einen Ping auf das System aus. Schlägt der Ping fehl, dann wird wie unter Anzahl PING Versuche angegeben, das System erneut angepingt. Schlagen alle Versuche fehl, dann wird für das überwachte System ein Alarm ausgelöst.
- **Portscan Intervall** Prüft, ob bestimmte Ports offen sind. Reagiert das zu überwachende System nicht auf die Portanfrage, dann wird ein Alarm ausgelöst.
- **SNMP Intervall** Zeitabstand, in dem SNMP-Abfragen auf die zu überwachenden Systeme durchgeführt werden sollen.

Für Windows-Systeme stehen zusätzlich folgende Überwachungsfunktionen zur Verfügung:

- **EventLog Intervall** Stellt den Zeitintervall dar, in dem definierte Ereignisprotokolle der zu überwachenden Systeme ausgelesen werden sollen. Hierbei werden lediglich die Einträge der letzten 24h ausgelesen.
- **Disk Intervall** Zeitabstand, in dem der freie Speicher der zu überwachenden Systeme überprüft werden soll.
- **Service Intervall** Zeitabstand, in dem die für ein System zu überwachenden Dienste überprüft werden sollen.
- **Process Intervall** Zeitabstand, in dem die ausgeführten Prozesse eines zu überwachenden Systems geprüft werden sollen.

SNMP Vorschlagswerte

In den Feldern **Port** und **Version** werden die Vorschlagswerte hinterlegt, die im SNMP Vorlageneditor (SNMP-Button) beim Öffnen voreingestellt werden.

Für Version 1 und Version 2c können die **Read-** und **Write Community** und für die Version 3 der **Benutzername**, der Hash für die **Verschlüsselung** und das **Security Protokoll** voreingestellt werden.

Dokumentenablage

Hier kann durch Angabe eines Speicherorts die Dokumentenverwaltung aktiviert werden. Alle verwalteten Dokumente werden unter dem hinterlegten Pfad abgelegt.

☑ Automatische Start des Prüflaufs

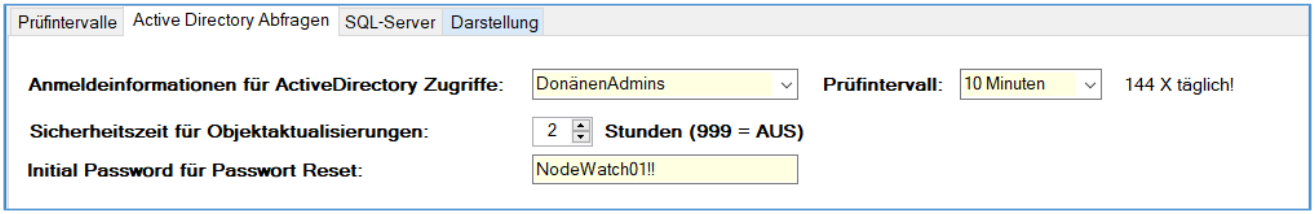
Ist diese Option aktiviert, dann startet die Überwachung der Nodes unmittelbar nach Aufruf der Schaltfläche **Überwachung starten** im Hauptmenü, ansonsten werden die Nodes lediglich am Bildschirm visualisiert und der Start der Überwachung muss manuell angestoßen werden.

☐ Bei Start der Anwendung sofort in „Überwachung starten“ wechseln

Bei aktivierter Option wird nach Start der Anwendung automatisch der Überwachungsmodus gestartet. Diese Option macht z.B. sinn, wenn das System auf dem node***WATCH*** läuft, von Zeit zu Zeit automatisch neu gestartet wird, z.B. nach einem automatischen Systemupdate.

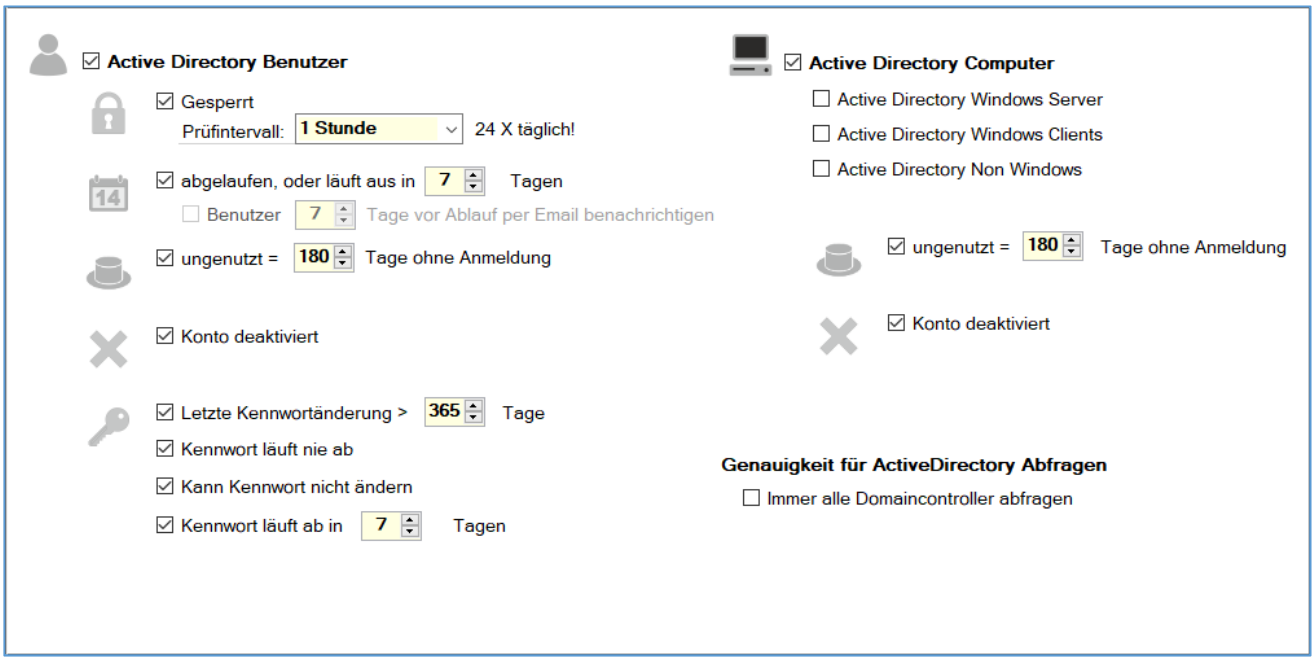
Active Directory Abfragen

In diesem Register werden die Abfrageintervalle und der Umfang der Active Directory Überprüfungen hinterlegt. Als Anmeldeinformation sollte hier wieder ein Benutzer mit ausreichend Berechtigungen im Active Directory hinterlegt werden. Um das Active Directory nicht zu sehr zu belasten sollte der Prüfintervall nicht zu kurz sein. Bei Active Directory Überwachungen liest das System einmal täglich alle Active Directory Objekte ein, in den restlichen Prüfungen werden nur noch geänderte Objekte neu eingelesen.



Die Option **Sicherheitszeit für Objektaktualisierungen** stellt sicher, dass bei Zeitumstellungen (Sommer-Winterzeit), oder Zeitabweichungen zwischen den Systemen keine geänderten Objekte ausgelassen werden.

Im Feld **Initial Passwort für Passwort Reset** kann ein Vorschlagswert für Kennwortrücksetzungen über node***WATCH*** hinterlegt werden.



Benutzerkonten Überwachung

Für AD-Benutzerkonten können in diesem Abschnitt folgende Überwachungen eingerichtet werden:

- **Gesperrt** Prüft Benutzerkonten, die aufgrund von falscher Kennworteingabe gesperrt wurden. Für diese Prüfung kann abweichender Prüfintervall eingestellt werden.
- **abgelaufen …** Überprüft Konten auf ein hinterlegtes Ablaufdatum. Über die Anzahl Tage kann eingestellt werden, dass z.B. X Tage vor Erreichen des Ablaufdatums eine Warnung ausgegeben wird. So kann z.B. sichergestellt werden, dass noch eventuelle Formalitäten mit dem Benutzer geklärt werden können, bevor er das Unternehmen verlässt.
- **Benutzer Email** Wenn die Benachrichtigungseinstellungen ordnungsgemäß konfiguriert wurden, dann kann hier eine automatische Erinnerung über den baldigen Kennwortablauf an die Domänenbenutzer versandt werden.
- **ungenutzt** Listet Alle Benutzerkonten auf, die sich seit der Anzahl der definierten Tage nicht mehr an einem System angemeldet haben. Diese Funktion eignet sich hervorragend zum Bereinigen von Active Directory.
- **Konto deaktiviert** Listet alle deaktivierten Benutzerkonten auf.
- **Kennwortthemen** Hier können Einstellungen die als kennwortkritisch betrachtet werden in den AD-Warnhinweis mit aufgenommen werden. So kann es z.B. als kritisch betrachtet werden, wenn ein Kennwort länger als 180 Tage nicht geändert wurde. Auch Einstellungen wie „Kennwort läuft nie ab“, oder „Kann Kennwort nicht ändern“ sind meist zurecht unerwünscht und können in die Warnhinweise mit aufgenommen werden. Ebenso verhält es sich mit abgelaufenen Kennwörtern, oder Kennwörter die in x Tagen ablaufen.

Die Active Directory Hinweise werden im Überwachungsmodus am unteren Bildschrimrand entsprechend angezeigt:

Computerkonten Überwachung

Für AD-Computerkonten stehen nur folgende zwei Überwachungsfunktionen zur Verfügung:

- **Konto deaktiviert** Listet alle deaktivierten Computerkonten auf. Diese Funktion kann für Aufräumzwecke verwendet werden.

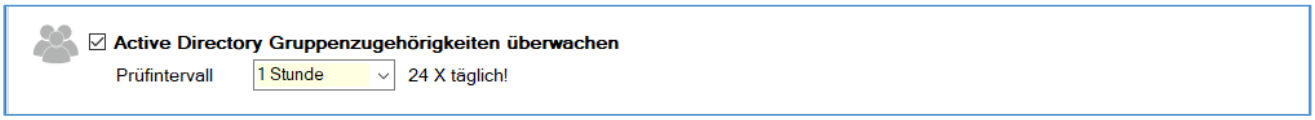
- **ungenutzt** Listet Alle Benutzerkonten auf, die sich seit der Anzahl der definierten Tage nicht mehr an einem System angemeldet haben. Wie auch bei den Benutzerkonten eignet sich diese Funktion ebenfalls hervorragend zum Bereinigen von Active Directory.

Die Hinweise werden im Überwachungsmodus ebenfalls am unteren Bildschirmrand wie folgt angezeigt:

Die Option **Immer alle Domänencontroller abfragen** hat nur eine Auswirkung bei ungenutzte Benutzer- und Computerkonten-Überwachung. Da das Attribut LastLogonTime nicht synchronisiert und LastLogonTimeStamp nur zwischen 11 und 16 Tagen repliziert wird, kommt es bei deaktivierter Option zu einer Unschärfe von bis zu 16 Tagen im Hinblick auf die letzte Verwendung des AD-Objekts. Es wird empfohlen diese Option nicht zu aktivieren, da bei aktivierter Option bei jeder Prüfung immer alle Domänencontroller abgefragt werden.

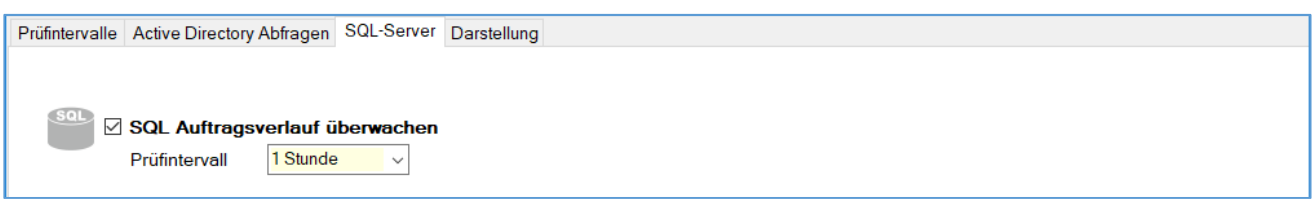
Active Directory Gruppenüberwachung

In diesem Abschnitt legen Sie fest, dass Gruppenmitgliedschaften von Active Directory überwacht werden sollen. Der Prüfintervall sollte hierbei ebenfalls nicht zu hoch eingestellt werden.



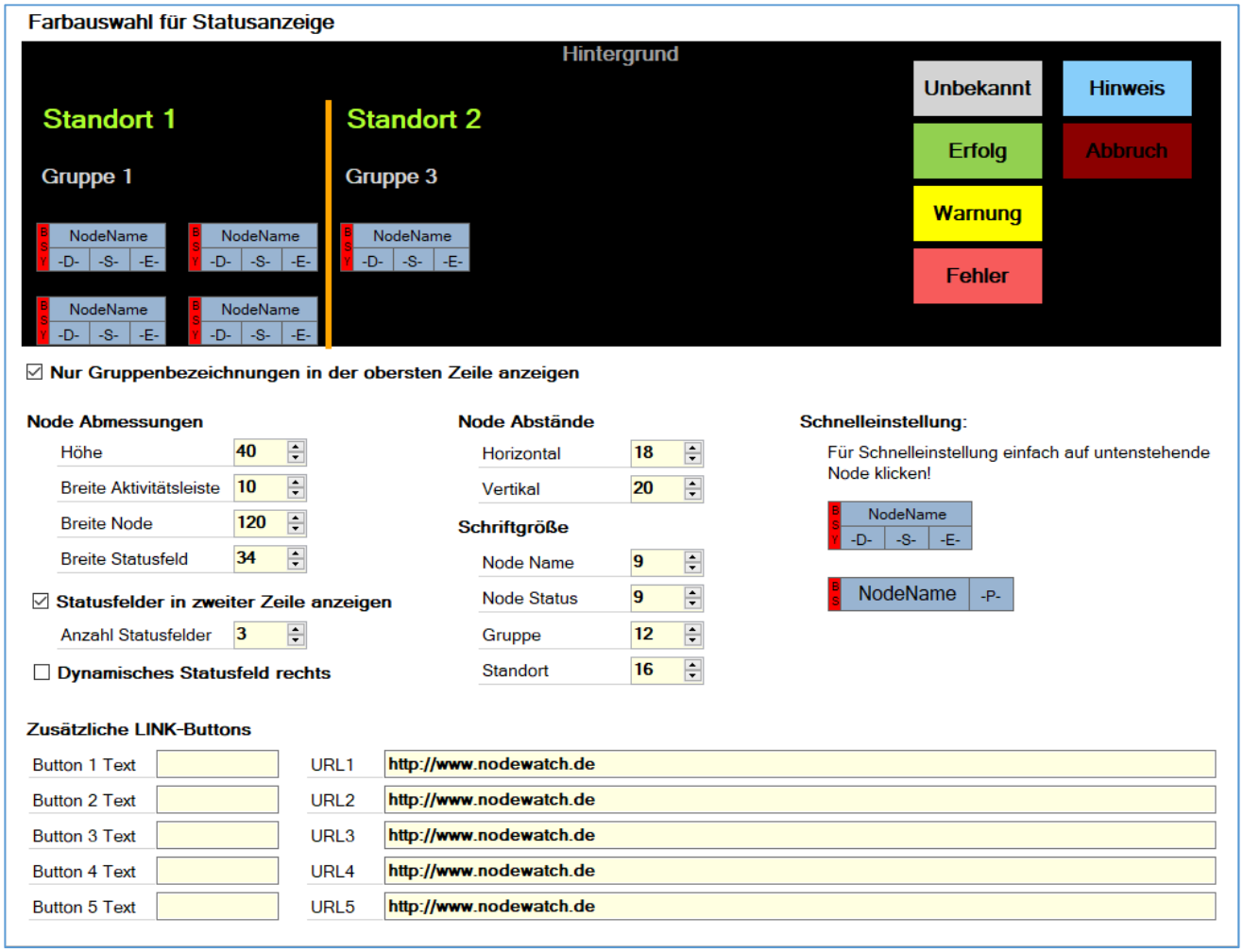
SQL-Server

Hier kann die Überwachung des MS SQL-Server Auftragsverlaufs aktiviert werden. Hier sollte ein stündlicher Abruf mehr als ausreichend sein. Welche MS SQL-Server überwacht werden sollen, ist in einem separaten Menüpunkt einstellbar.



Darstellung

Im Register Darstellung können die Farben, Höhe und Breite und Inhalt der Nodes eingestellt werden. Zum Ändern der Farben einfach auf eine Farbe Rechts am Rand klicken und die neue Farbe auswählen.



Die Anzahl der Statusfelder (maximal 4) haben folgende Bedeutung:

Feld Nr.

1 –D– zeigt an, dass in dieser Node die Überwachung des freien Speichers erfolgt

2 –S– zeigt an, dass für diese Node eine Dienstüberwachung eingerichtet wurde

3 –E– zeigt an, dass für diese Node Event Log Protokolleinträge überwacht werden

4 –P– zeigt an, dass für diese Node aktive Prozesse überwacht werden

Schnelleinstellung

Durch Klick auf eine Node-Symbol unterhalb der Schnelleinstellung werden die Einstellungen für die Darstellung der ausgewählten Node gesetzt.

Zusätzliche Link-Buttons

Wird der Button Text ausgefüllt, dann wird in der Überwachungsansicht auf der rechten Seite ein Link-Button eingeblendet, der auf den entsprechenden Hyperlink verweist.

Es können bis zu fünf Schnellzugriffe konfiguriert werden.

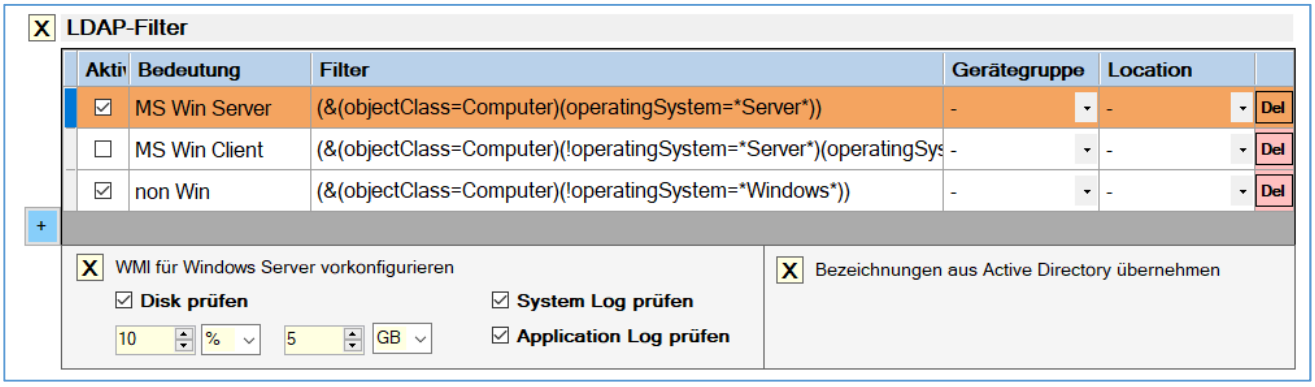
Netzwerk Scan

Neue Netzwerkgeräte können auf unterschiedliche Weise erkannt werden. Im Register Netzwerk Scan können hierfür verschiedene Verfahren aktiviert und entsprechende Filter hinterlegt werden.

Durch Aktivierung der Option **Täglich automatisch nach neuen Geräten suchen** wird mit den nachfolgenden Filtereinstellungen täglich nach neuen Geräten im Netzwerk gesucht. Alle neu hinzugefügten Geräte werden entsprechend als NEU gekennzeichnet.

LDAP-Filter

Der LDAP-Filter ist bei Auslieferung bereits vordefiniert. Über Gerätegruppe kann und Location kann bereits eine Vorkonfiguration für neu gefundene Geräte vorgenommen werden. Wird bei Location nichts eingetragen, dann versucht das System den Standort automatisch anhand der in den Stammdaten hinterlegten Standortdaten zuzuordnen.



WMI-Einstellungen

Im unteren Abscnitt können Voreinstellungen für WMI-Abfragen durchgeführt werden. Diese werden allerdings nur auf Windows Server Betriebssysteme angewandt.

Bezeichnungen aktualisieren

Bei aktivierung dieser Option werden beim Scanvorgang für alle im Suchbereich befindlichen Geräte die Active-Directory Beschreibung übernommen.

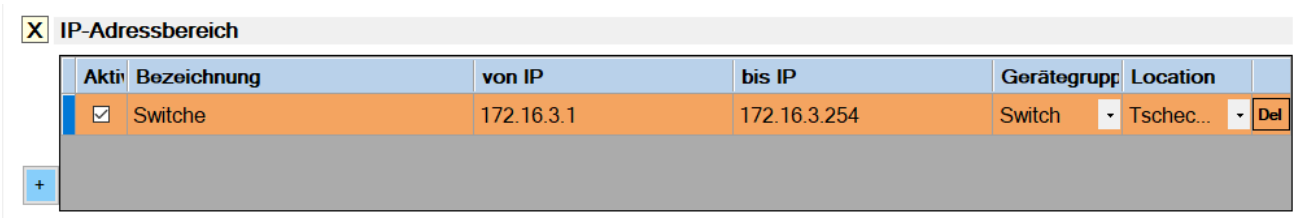
DNS-Filter

Über den DNS-Filter kann der Active-Directory integrierte DNS-Server nach neuen Geräten durchsucht werden. Über die Zone wird der Suchbereich auf eine Domain eingeschränkt. Hostnamen können mit * maskiert werden. So wird mit dem Eintrag SRV* täglich nach Hostnamen die mit SRV* beginnen gesucht und mit den bereits vorhandenen Geräten verglichen. Wird kein Eintrag zu diesem Gerät in der aktuellen Netzwerkliste gefunden, dann wird der gefundene Eintrag hinzugefügt.

Zusätzlich kann der Filter auch noch auf einen IP-Adressbereich eingeschränkt werden. Einfach Start- und End-IP-Bereich eingeben um den Suchbereich weiter einzuschränken.

IP-Adressbereich

In diesem Abschnitt besteht die Möglichkeit einen klassischen IP-Scan durchzuführen. Gefundene Geräte können wieder entsprechend vorkonfiguriert werden. Gefundene Geräte werden wieder mit der aktuellen Geräteliste verglichen. Wird ein Eintrag nicht gefunden, dann wird er der Liste hinzugefügt.

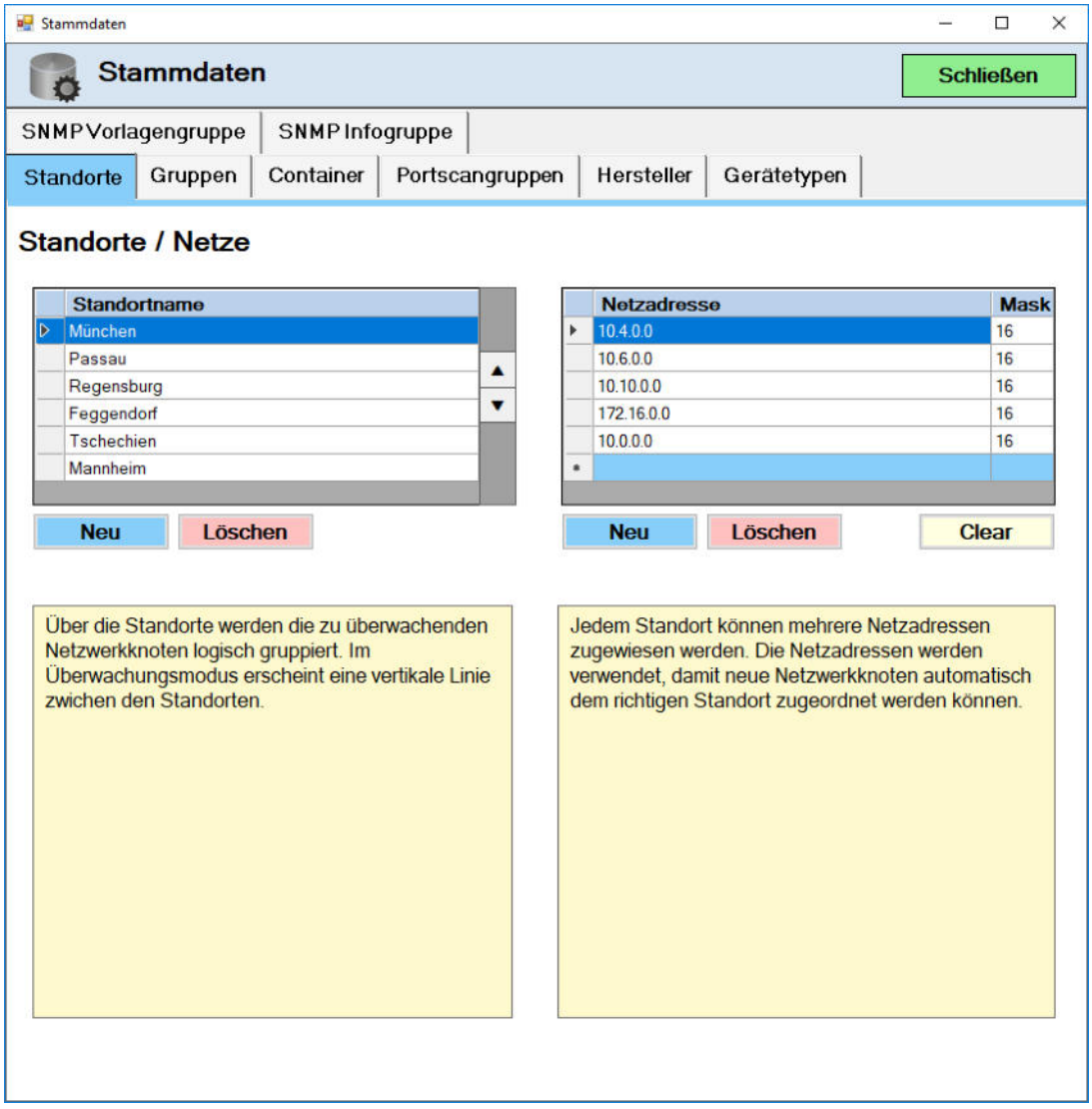


Stammdaten Bearbeiten

Unter dem Menüpunkt Stammdaten können Listen für Unternehmensstandorte, Hardwaregruppen, Vorlagen für Portscans, Herstellerangaben und Gerätetypen hinterlegt werden.

Standorte

Beim ersten öffnen des Stammdatendialogs erscheint eine Abfrage, ob das System die Standorte automatisch ermitteln soll. Wenn Sie die Frage mit Ja beantworten, dann werden die Einstellungen aus Active Directory Standorte und Dienste ausgelesen. Jedem Standort werden die zugewiesenen Netzwerkadressen zugeordnet. Die Einträge können jederzeit manuell ergänzt werden. Das System verwendet diese Informationen, um die einzelnen Nodes dem jeweiligen Standort zuordnen zu können. Die Zuordnung kann für jede Node auch manuell erfolgen.

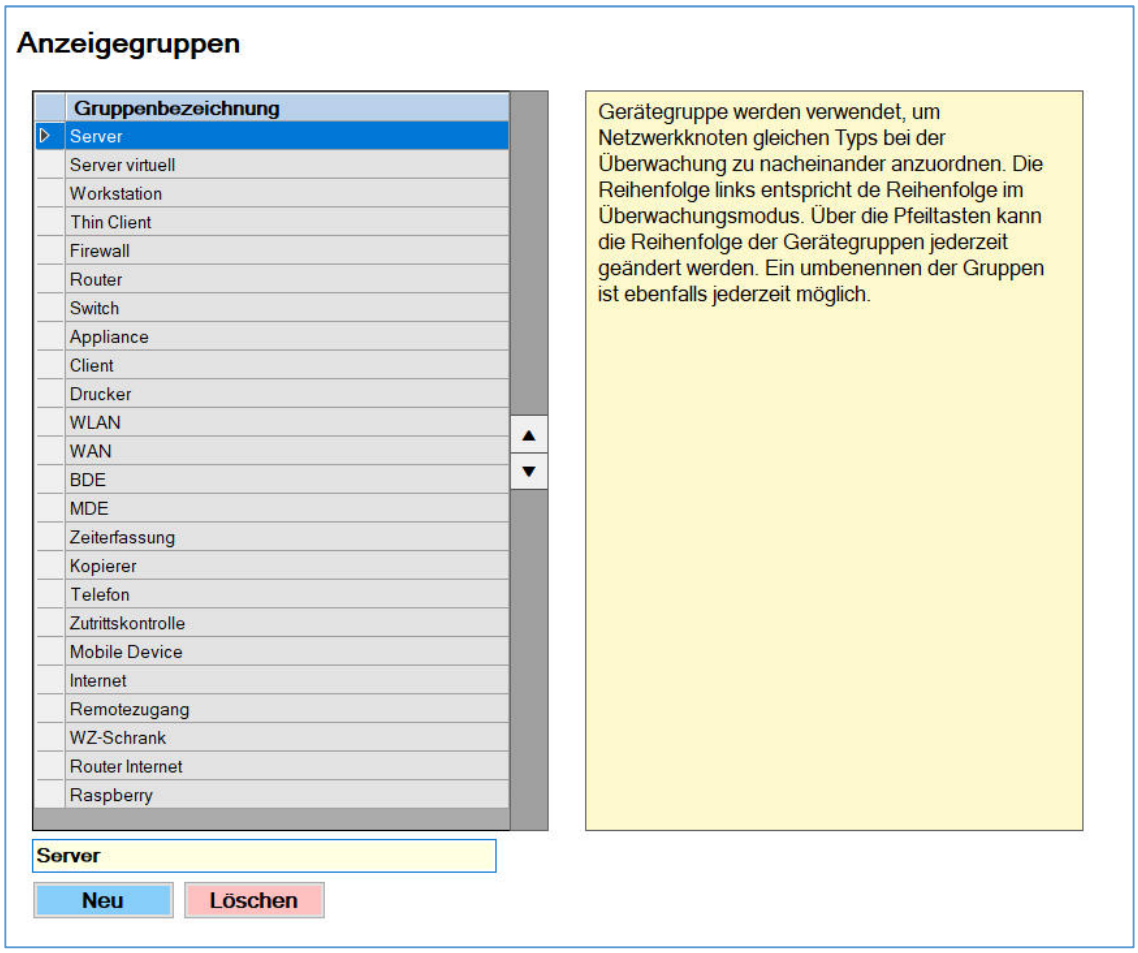


Es muss sich in dieser Kategorie aber nicht zwingend um Standorte handeln, sonder es können auch eigene Bezeichnungen verwendet werden. Die hier gemachten Angaben dienen Stellen das oberste Gruppierungsmerkmal dar. Genausogut könnte man hier als Standortname Bezeichnungen wie Server, Storage, Client, Drucker, WLAN… verwenden.

Anzeigegruppen

Im Register Anzeigegruppen können für die spätere Gruppierung der Geräte Gruppierungsmerkmale angelegt werden, z.B.:

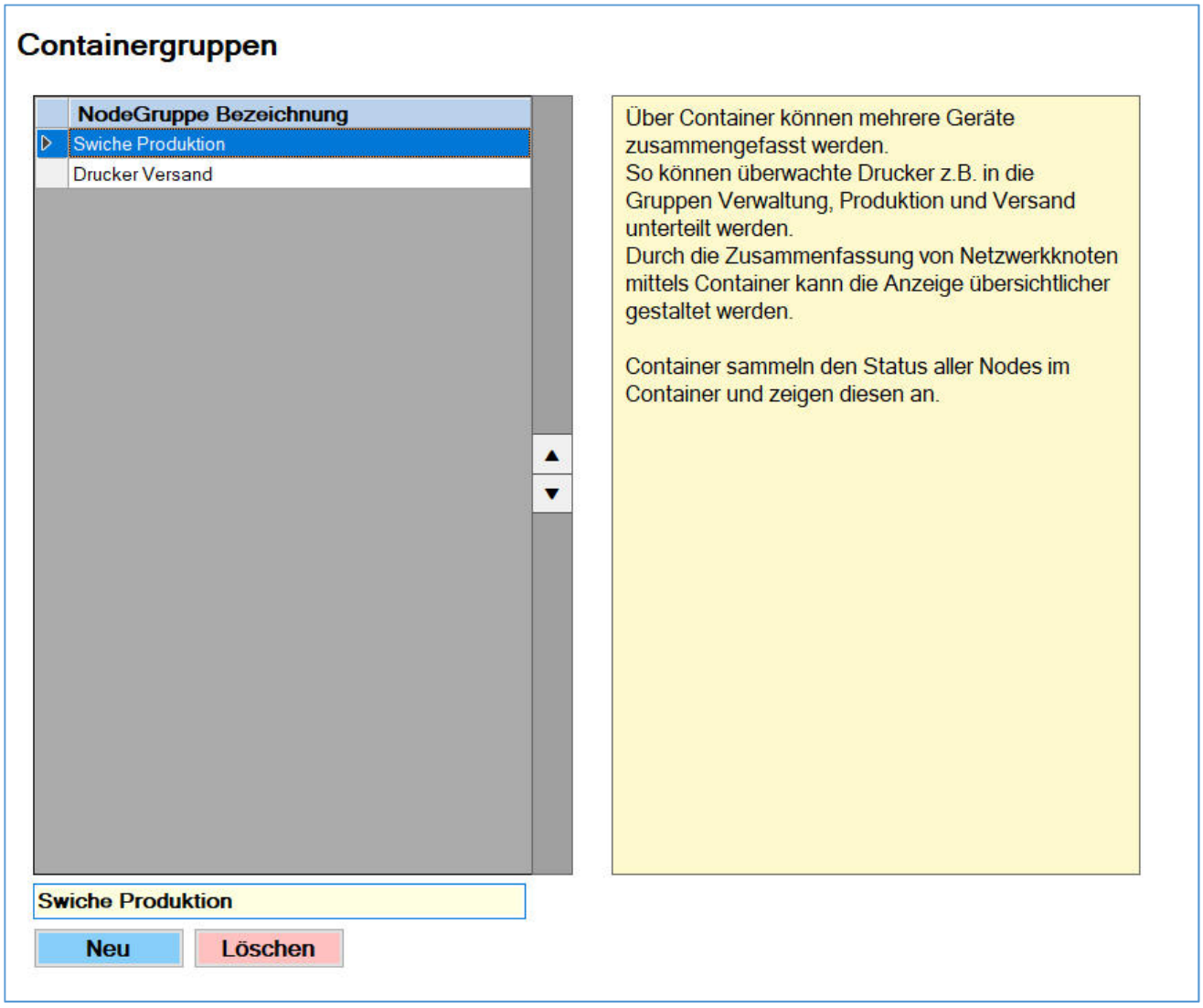
Server, Storage, Clients, Drucker, Firewall, Router, Switch …



Im Überwachungsmodus werden die Gruppen in der hier angezeigten Reihenfolge sortiert. Die Reihenfolge kann über die beiden Pfeiltasten ▼ ▲ geändert werden.

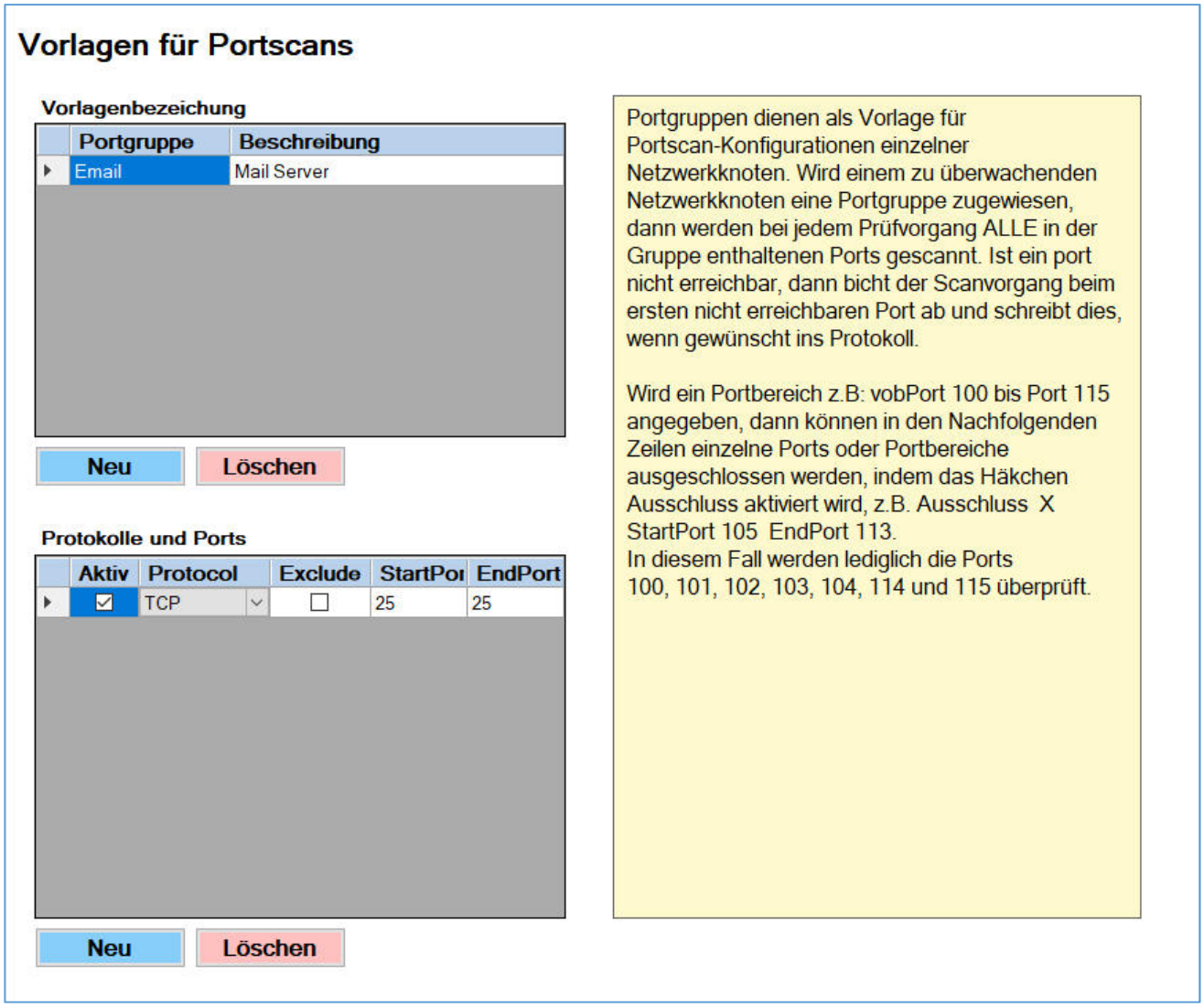
Container

Im Register Container werden Überbegriffe für die spätere Zusammenfassung von Geräten in einem Container hinterlegt. Durch bilden von Containern kann in großen Netzwerken die Überwachungsansicht übersichtlicher gestaltet werden.



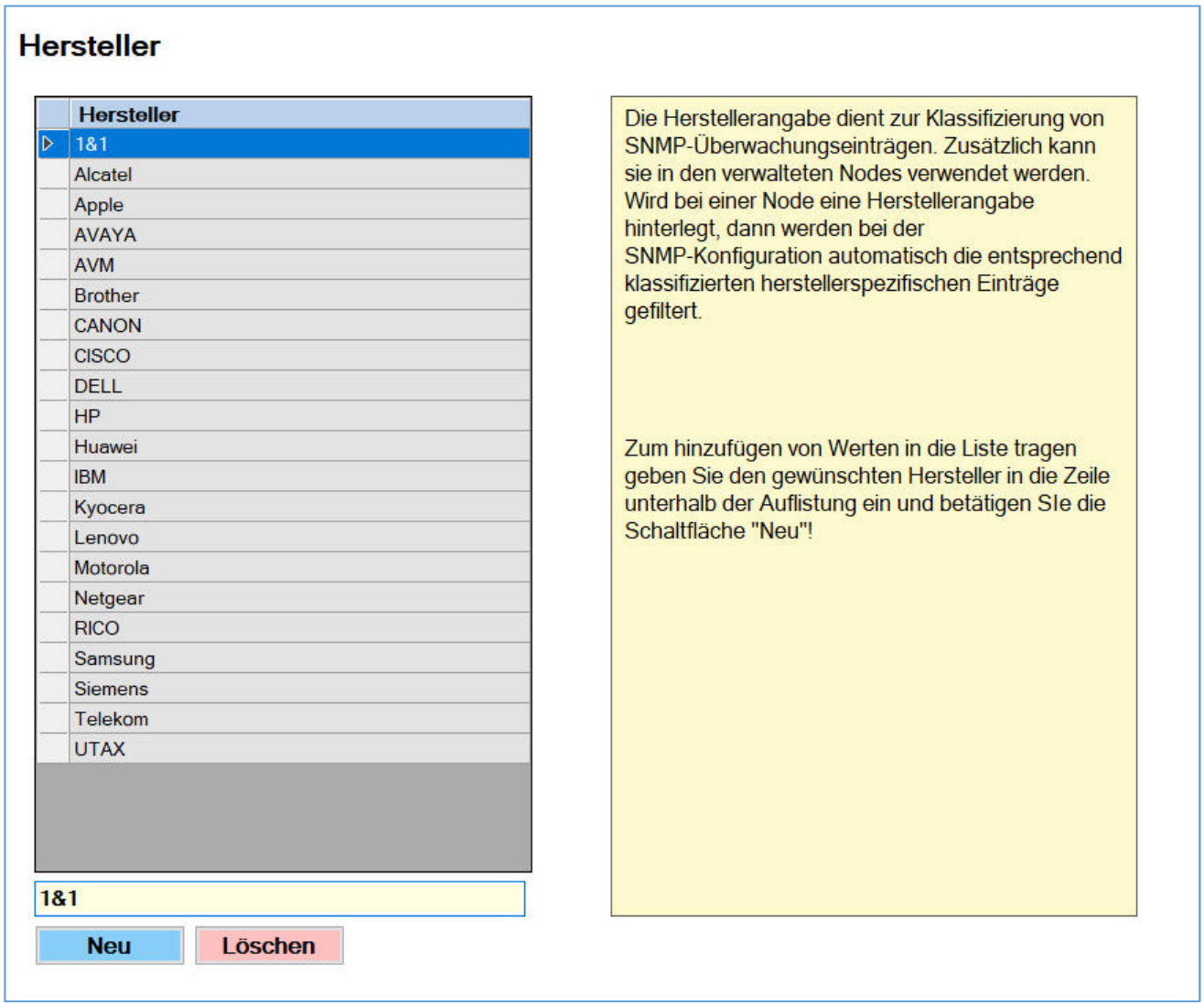
Port Definitionen

Vordefinierte Vorlagen für Portscans können im Register Port Definitionen erstellt werden. Unter Vorlagenbezeichnung muss zuerst eine neue Vorlagengruppe hinzugefügt werden. Im Anschluss kann man für die Vorlagengruppe im Abschnitt Protokolle und Ports beliebig viele Ports hinterlegen, die unter Verwendung dieser Vorlage gescannt werden sollen.



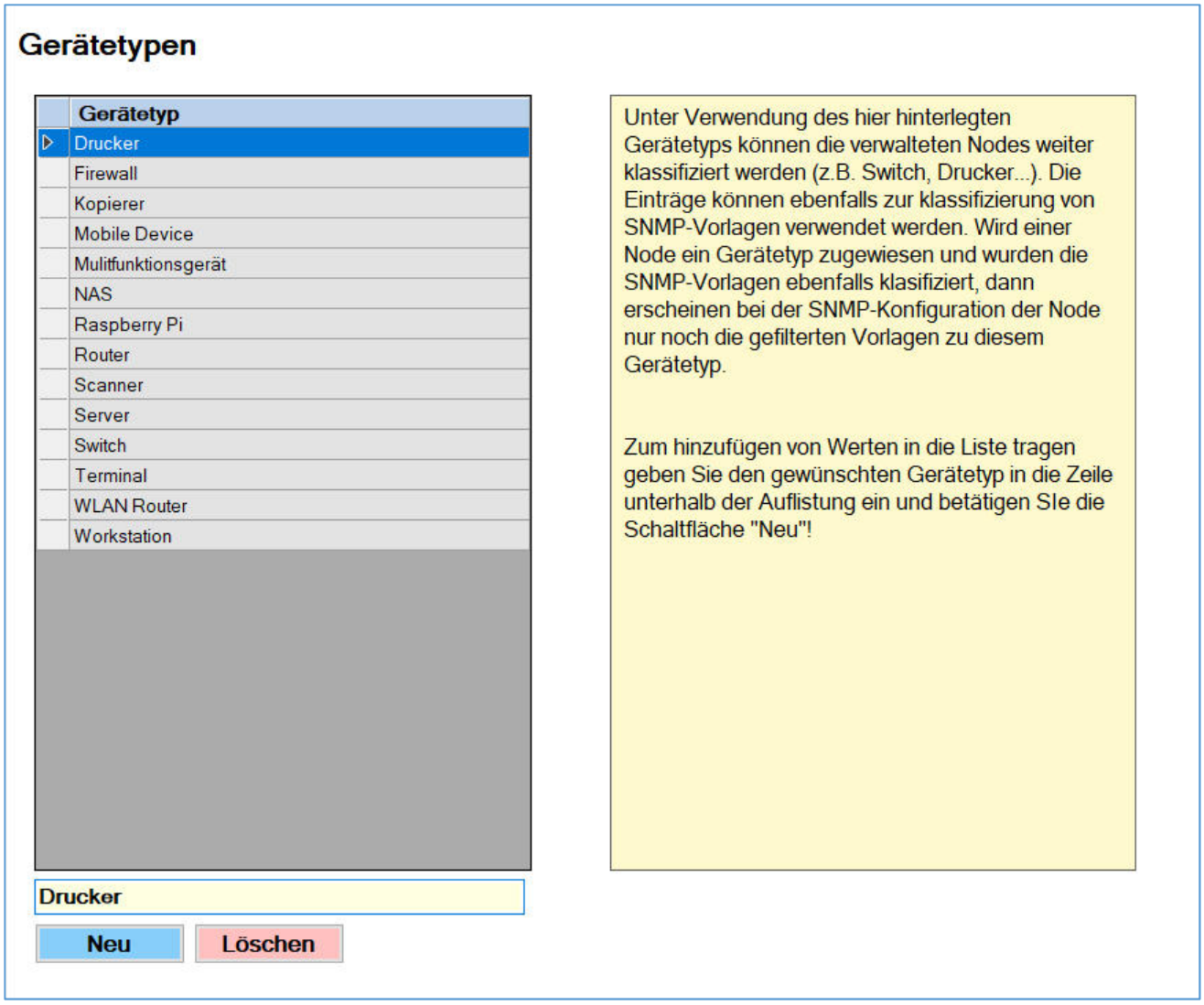
Hersteller

Im Register Hersteller können Hardwarehersteller erfasst werden. Diese stehen dann zur Klassifizierung der Nodes und SNMP-Vorlagen zur Verfügung.



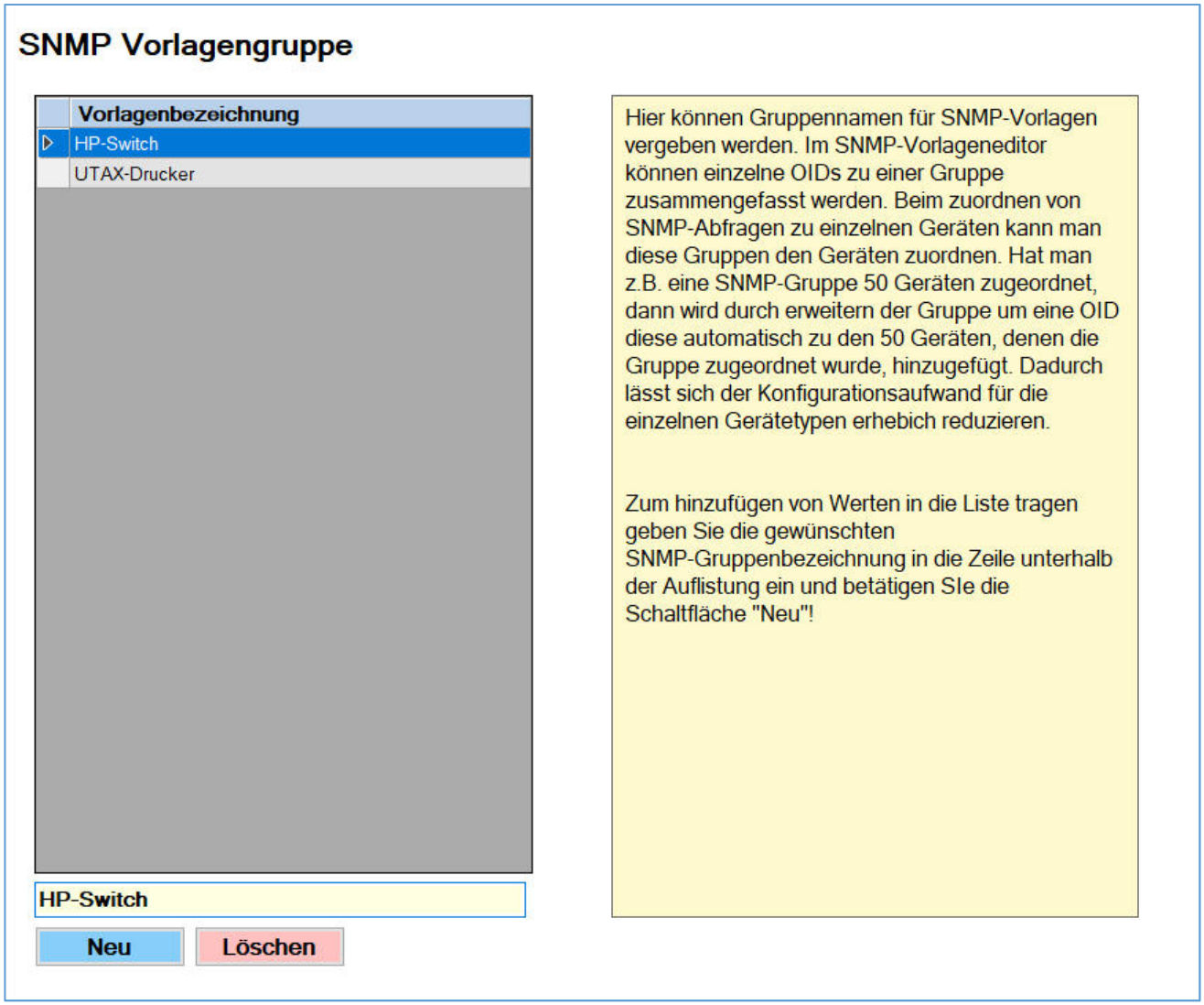
Gerätetypen

Unter Gerätetypen sind die verschiedenen Arten von Netzwerkgeräten aufgelistet. Diese können jederzeit nach Belieben erweitert werden. Die hier angegebenen Gerätetypen können einer Node und den SNMP Templates zugewiesen werden.



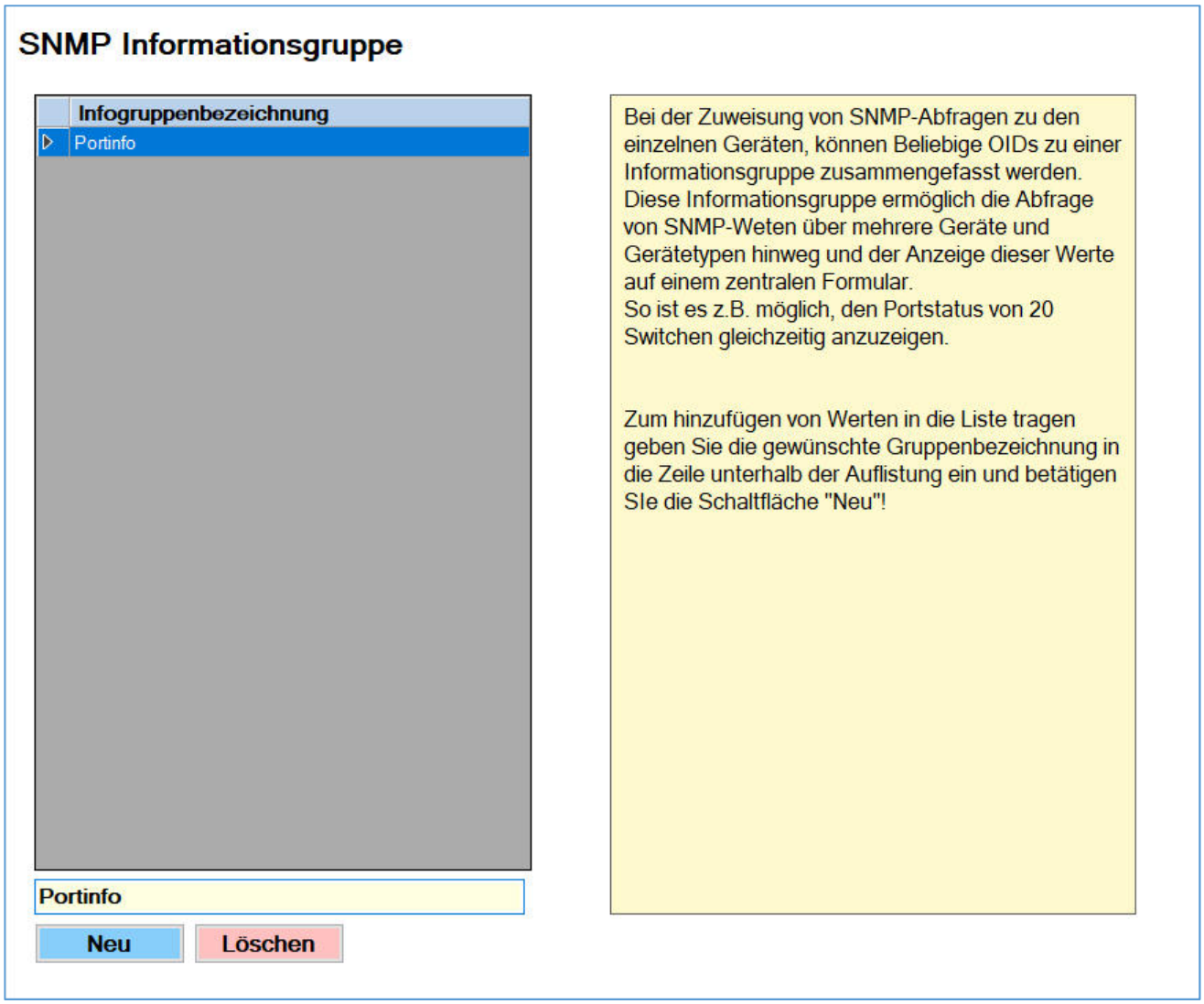
SNMP Vorlagengruppe

Vorlagengruppen dienen der Zusammenfassung von SNMP-OID zu einer Gruppe. Dadurch lassen sich Hersteller und Gerätespezifische SNMP-Filter zu einer logischen Einheit zusammenfassen. Diese können dann als Gruppe einem Gerät zugeordnet werden. Ist eine Gruppe z.B. 50 identischen Netzwerkgeräten zugeordnet, dann werden Änderungen an der Gruppe für alle Geräte wirksam, denen die Gruppe zugeordnet ist.



SNMP Infogruppe

Eine Infogruppe ermöglicht die Darstellung von SNMP-Informationen über mehrere verschiedene Geräte hinweg. Wird eine Infogruppe aufgerufen, dann wird werden auf allen Geräten, denen SNMP-Abfragen mit dieser Infogruppe zugeordnet sind, die Abfragen ausgeführt und entsprechend übersichtlich dargestellt.



Benachrichtigung

Die Schaltfläche Benachrichtigungen im Hauptmenü ermöglicht die Konfiguration von Email Benachrichtigungsgruppen. Um Benachrichtigungen verwenden zu können, muss die Option **Benachrichtigungen aktivieren** angekreuzt werden.

Serverangaben

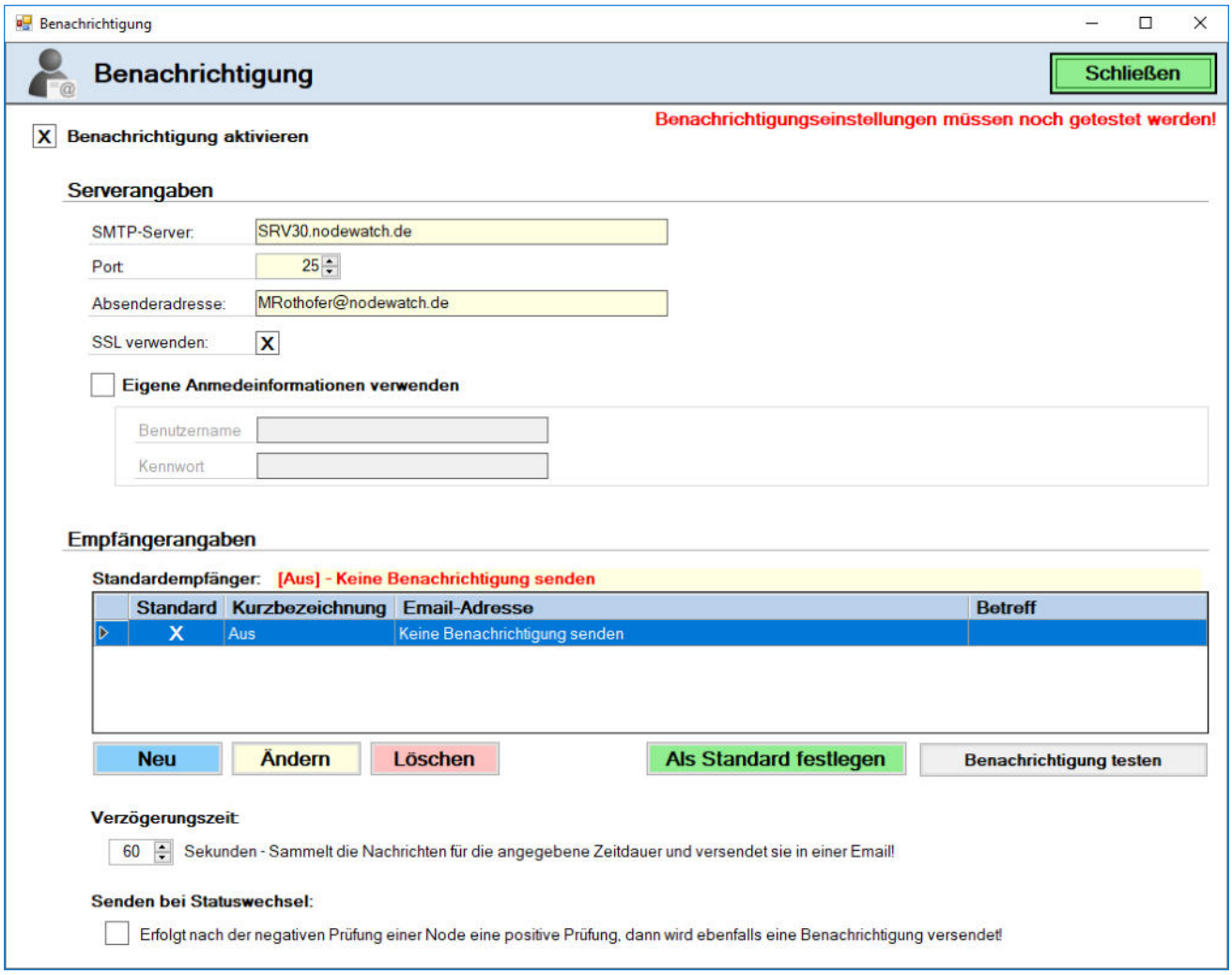
Damit node***WATCH*** Benachrichtigungen versenden kann, müssen unter Serverangaben folgende Einträge gepflegt werden:

SMTP-Server: Name eines internen oder externen Mailservers

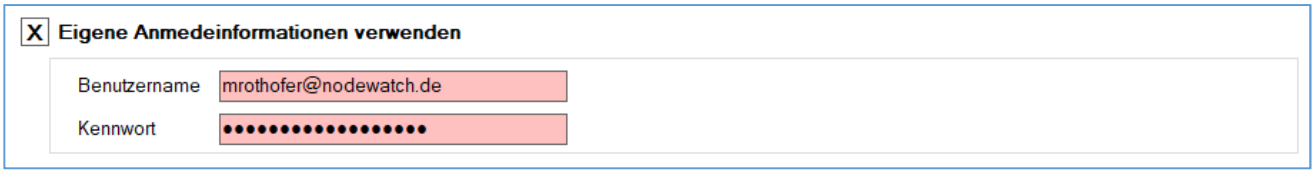
Port: Empfänger Port des unter SMTP-Server eingetragenen Mailservers.

Absenderadresse: Beliebige Absenderadresse die als Absender für die von node***WATCH*** versendeten Mails verwendet wird.

SSL verwenden: Kann angekreuzt werden, wenn der Server SSL-Verschlüsselung unterstützt.



Zum Versenden von Emails verwendet node***WATCH*** die Anmeldeinformationen mit denen die Software gestartet wurde. Verfügt der aktuelle Benutzer nicht über Berechtigung zum Versenden von Emails, oder sollte ein externer Mailserver für den Versand von Benachrichtigungsmails verwendet werden, dann kann über die Option **Eigene Anmeldeinformationen verwenden** ein alternativer Benutzername und ein alternatives Kennwort zur Authentifizierung am Mailserver angegeben werden.



Empfängerangaben

Nachdem die Serverparameter eingegeben wurden, muss man zum Abschluss der Konfiguration nur noch einen Empfänger für die Benachrichtigungen hinterlegen. Über die Schaltfläche Neu wird ein neuer Nachrichtenempfänger angelegt.

Wird später für eine Node eine Benachrichtigung eingerichtet, dann erscheint die Kurzbezeichnung in der auswahlliste für die Empfängerangabe. Unter Email-Adresse können nun ein oder mehrere durch Semikolon getrennte Email Empfänger eingetragen werden.
Abschließend ist noch die Angabe eines Betreffs erforderlich. Die Nodes können unterschiedliche Empfänger zugeordnet werden, z.B. ERP-Systemen erhalten als Benachrichtigungsgruppe ERPAdmins und SQL-Server als Benachrichtigungsgruppe SQLAdmins. Die restlichen Systeme erhalten BasisAdmins.

Nachdem ein Empfänger hinzugefügt wurde, muss noch ein Eintrag als Standard ausgewählt werden. Hierfür ist lediglich die Empfängerzeile zu markieren und die Schaltfläche „Als Standard festlegen“ zu betätigen.

Nachdem nun Absender- und Empfängerinformationen eingerichtet wurden, kann die Konfiguration über die Schaltfläche **Benachrichtigung testen** überprüft werden.

Weitere Optionen

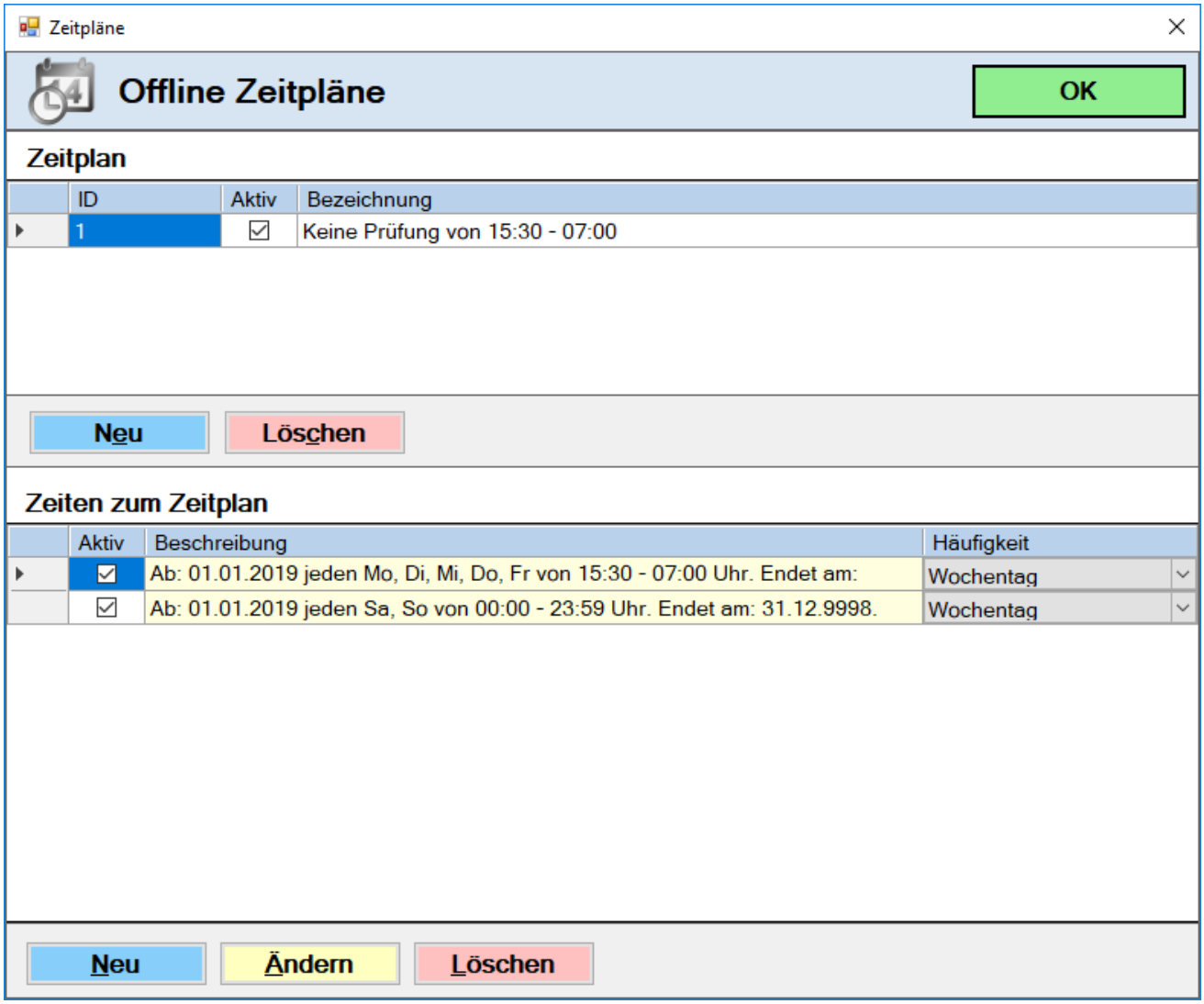
Eine wichtige Einstellung ist die Option **Verzögerungszeit**. Hier kann eingestellt werden, wie lange node***WATCH*** die Alarme sammelt, bevor eine Email-Benachrichtigung versendet wird. Wird hier 0 eingetragen, dann versendet node***WATCH*** für jeden einzelnen Fehler eine Nachricht.

Die Option **Senden bei Statuswechsel** bedeutet, dass falls nach einer fehlerhaften Prüfung wieder eine Erfolgsprüfung durchgeführt wird, dann wird ebenfalls eine Benachrichtigungsmail versendet.

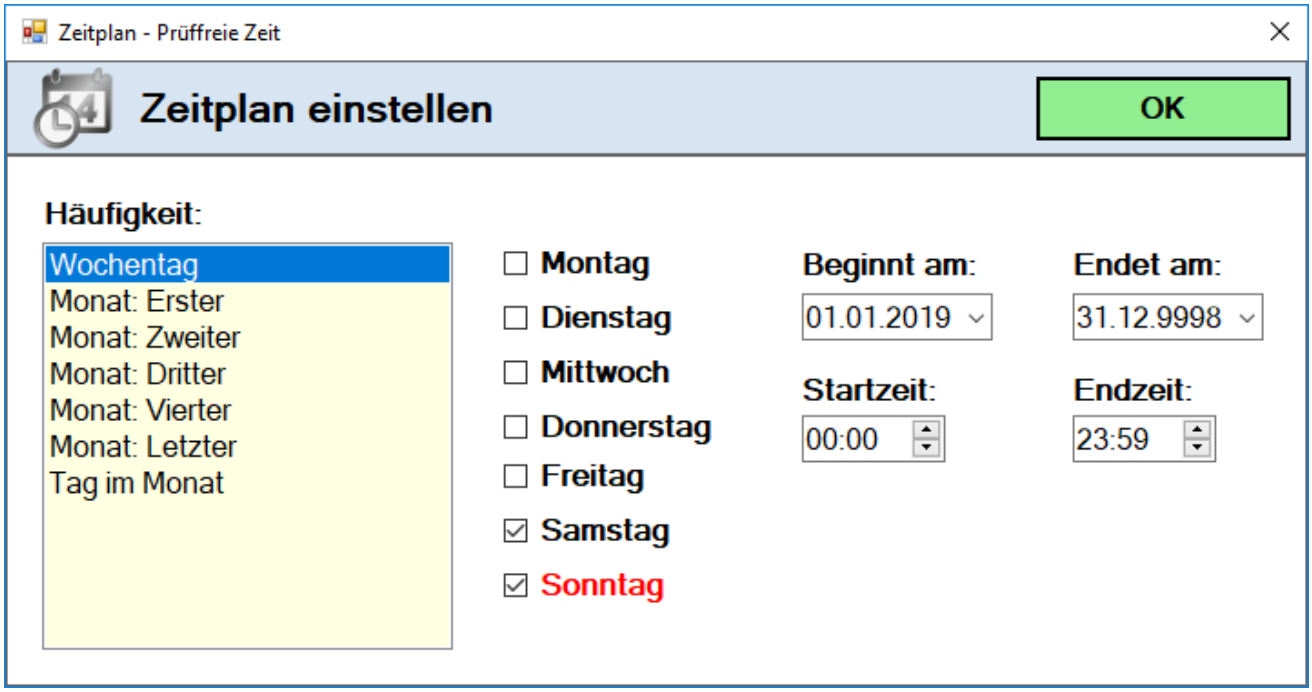
Um eine unnötige Benachrichtigungsflut zu verhindern, wird im Fehlerfall eine Mail versendet. Besteht bei der nächsten Prüfung immer noch derselbe Fehler, dann wird keine neue Mail versende. Ist jedoch eine Prüfung fehlerhaft, dann wieder erfolgreich und anschließend wieder fehlerhaft, dann wird für den zweiten Fehler wieder eine Benachrichtigungsmail versendet. Die Benachrichtigungsfunktion kann aber über Zeitpläne individuell ausgesetzt werden.

Zeitpläne

Im Hauptmenü gelangt man über die Schaltfläche Zeitpläne zu der Verwaltungsoberfläche für Erstellung und Änderung von Zeitplänen. Im Abschnitt Zeitplan muss zuerst ein neuer Eintrag hinzugefügt werden. Das System vergibt hierbei eine neue Zeitplan-ID. Über das Kontrollkästchen **[Aktiv]** kann der Zeitplan aktiviert bzw. deaktiviert werden. Im Feld Bezeichnung sollte beschrieben werden, welche Zeiten der Plan ausgrenzt.



Im Abschnitt **Zeiten zum Zeitplan** können dann beliebig viele Offlinezeiten definiert werden. Über die Option **[Aktiv]** können die einzelnen Definitionen wieder aktiv bzw. inaktiv gesetzt werden. Alle definierten Zeiten zu einem Zeitplan wirken kumulativ.

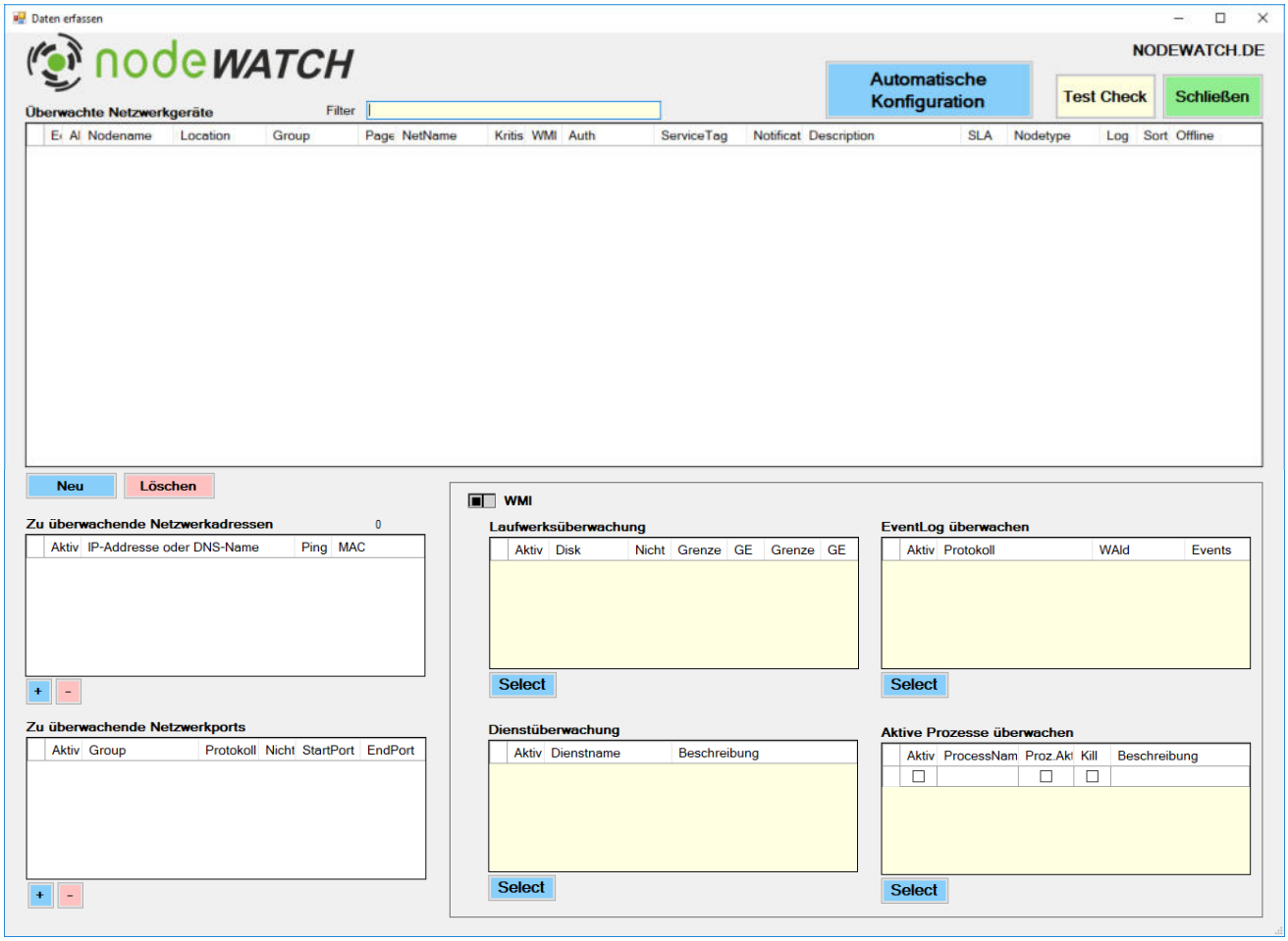


Unter Häufigkeit können Sie einstellen, dass z.B. immer am ersten Samstag im Monat keine Prüfung stattfinden soll, da hier z.B. immer Wartungsarbeiten stattfinden.

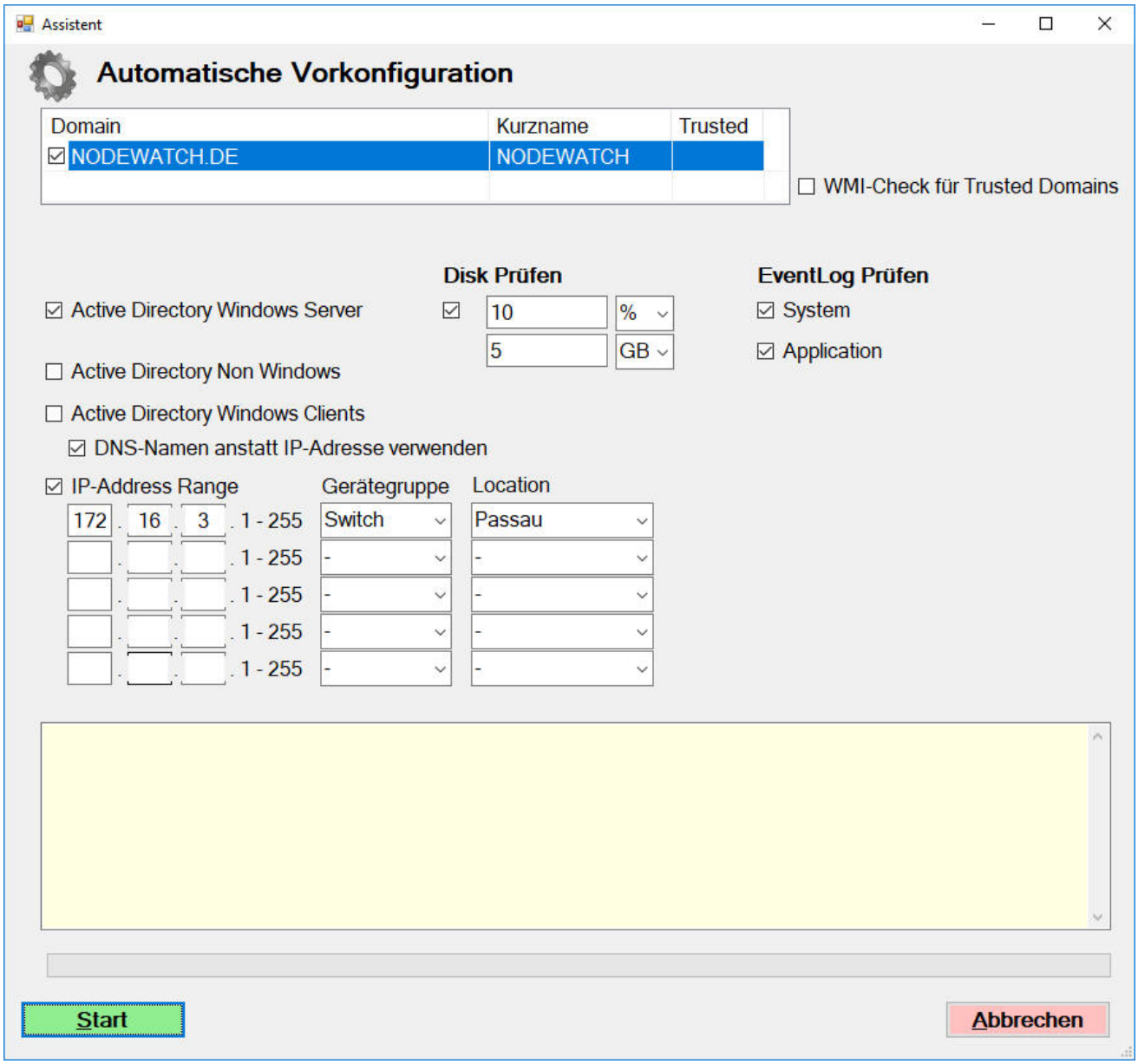
Ist für eine Node ein Zeitplan aktiv, dann werden innerhalb des definierten Zeitraums die Prüfungen für die Node ausgesetzt. Die Node wird dann ab dem ersten Prüfversuch innerhalb der Prüffreien Zeit grau (= Offline) dargestellt.

Überwachung konfigurieren

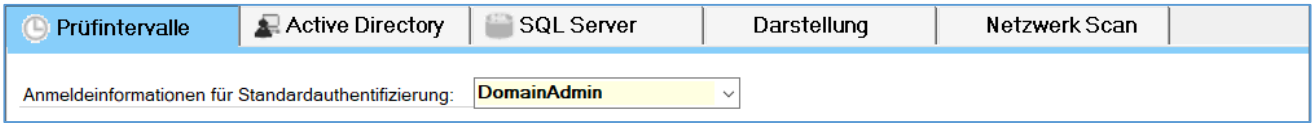
Nachdem nun die ersten Tätigkeiten durchgeführt wurden, kann über die Schaltfläche „**Überwachung konfigurieren**“ im Hauptmenü, mit der eigentlichen Konfiguration begonnen werden.



Um den Aufwand der manuellen Konfiguration zu reduzieren kann über die Schaltfläche **Automatische Konfiguration** ein Assistent gestartet werden. Dieser ermöglicht das einlesen der Nodes über Active Directory und den Scan des Netzwerks für nicht Active Directory Komponenten.



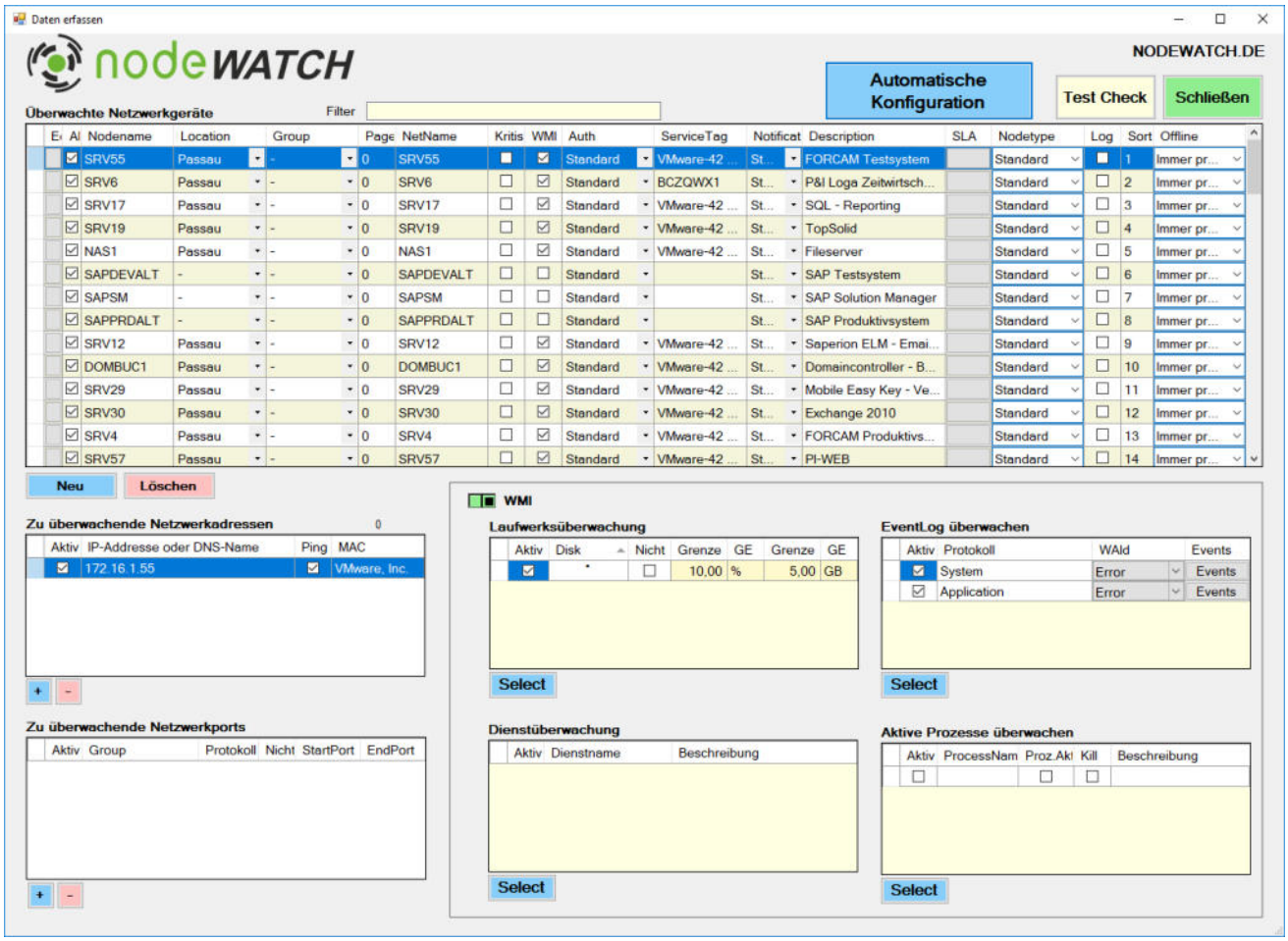
Wenn die Optionen **Disk prüfen** und **Even Log prüfen** angewählt sind, dann sollte in den Basiseinstellungen im Register **Prüfintervalle** bei Anmeldeinformationen für Standardauthentifizierung ein Benutzer mit Domänenadmin-Rechten hinterlegt sein. Beim Scannen der Systeme prüft das System den WMI-Zugriff zum Auslesen von Disk und Event Logs. Schlägt der Zugriff fehl, dann wird die Überwachung nicht automatisch eingerichtet, sondern muss im Nachgang manuell konfiguriert werden.



Netzwerkscan

Unter der Option **IP-Addres -Range** kann ein Netzwerkscan durchgeführt werden. Wenn Sie Ihr Netzwerk strukturiert haben, dann können Sie die den verschiedenen Bereichen gleich eine Gerätegruppe und eine Location zuweisen.

Nach Ausführen der automatischen Konfiguration sollte die Konfigurationsoberfläche erst einmal ordentlich gefüllt sein. Die gängigsten Überwachungseinstellungen können für jede Node direkt in dieser Anzeige durchgeführt werden.



Die Filterfunktion ermöglicht bei einer Vielzahl von Nodes das schnelle Auffinden bestimmter Nodes. Der Filter sucht über den Nodename und über die Beschreibung (Description).

Für jede Node kann nun die Überwachung über die Spalte **Aktiv** aktiviert oder deaktiviert werden. Nachfolgend die Beschreibung der einzelnen Spalten:

Edit-Button Springt in die Detailkonfiguration der Node

Aktiv Aktiviert oder deaktiviert die Überwachung für die Node.

Nodename	ist die Beschriftung der Node im Überwachungsmodus.
Location	Bezeichnet den Unternehmensstandort dem die Node zugeordnet wurde. Standorte werden durch vertikale Linien getrennt in der Überwachung dargestellt.
Group	Bezeichnet die Gerätegruppe, die der Node zugeordnet wurde. Innerhalb der Standorte erfolgt die Gruppierung der Nodes nach der Group. Die Reihenfolge innerhalb einer Gruppe wird durch die Spalte Sort bestimmt.
NetName	Eindeutiger Systemname wie z.B.: Computername
Kritisch	Mit dieser Option können wichtige Systeme gekennzeichnet werden, die für den Unternehmenserfolg unerlässlich sin.
WMI	zeigt WMI-Überwachung eingerichtet wurde.
Auth	hier können Benutzeranmeldeinformationen ausgewählt werden, mit denen eine Überwachung des Systems durchgeführt wird.
ServiceTag	Service Tag der Hardware. Bei Windows-Systemen und automatischer Konfiguration wird versucht diese automatisch zu ermitteln.
Notification	Hier kann der Empfänger für die Benachrichtigung ausgewählt werden.
Description	Hier kann die Funktion der Node beschrieben werden.
Log	noch nicht in Verwendung
Sort	Bestimmt die Anzeigereihenfolge innerhalb der Gruppierung
Offline	Hier kann ein Zeitplan für Offlinezeiten hinterlegt werden.

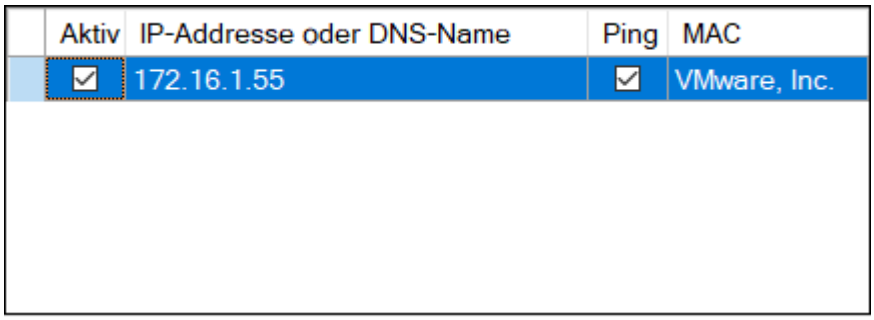
In dieser Hauptansicht können die meisten Überwachungsfunktionen schnell eingerichtet werden. Weitere Möglichkeiten stehen durch betätigen des vorderen Edit-Buttons der Node zur Verfügung. Diese werden weiter hinten beschrieben.

Zuerst sehen wir uns auf den nächsten Seiten die Konfigurationsmöglichkeiten des Hauptfensters an.

Für jede Node muss im „**Zu überwachende Netzwerkadressen**“ mindestens eine IP-Adresse oder DNS-Name angegeben werden. Damit die Überwachung funktioniert muss mindestens ein Eintrag aktiv gekennzeichnet sein.

Zu überwachende Netzwerkadressen

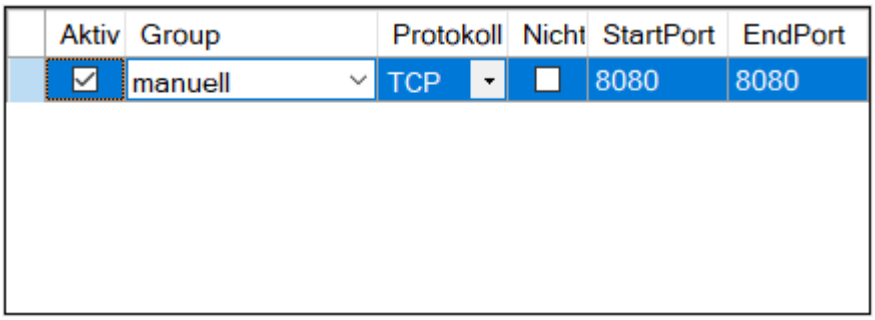
Die Einfachste Prüfung ist der Ping auf die hier hinterlegten Adressen. Dieser wird aktiviert, wenn das Kontrollkästchen Ping angekreuzt ist.



Es können beliebig viele IP-Adressen hinterlegt werden. Für die weiteren Prüfungen wie z.B. WMI oder SNMP wird die erste Adresseintrag verwendet. Die Konfiguration unter **Zu überwachende Netzwerkports** ist jedoch adressspezifisch, d.h. sie wird nur für den markierten Adresseintrag durchgeführt.

Zu überwachende Netzwerkports

Das nachfolgende Bild zeigt einen exemplarischen Eintrag für einen Portscan. Ist das Kontrollkästchen **[Aktiv]** aktiviert, dann wird der Portscan bei der Prüfung für die zugewiesene Adresse durchgeführt.



In der Spalte **Group** kann eine zuvor unter „**Stammdaten** bearbeiten“ / Register **Portdefinitionen** definierte Gruppe ausgewählt werden.

WMI – Windows Management Instrumentation

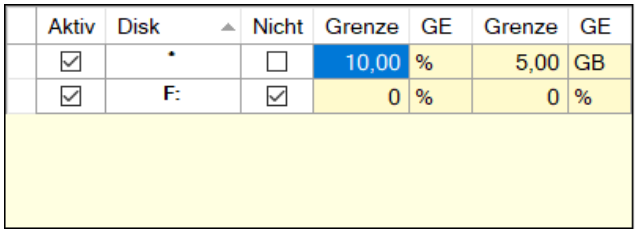
Durch Auswahl einer Node mit Microsoft Windows OS und betätigen einer der vier Select-Schaltflächen im WMI-Abschnitt kann sehr bequem eine Überwachung für die selektierte Node eingerichtet werden. Voraussetzung ist hierfür, dass auf der zu überwachenden Node die WMI-Dienste aktiv sind.

Über die Spalte **Auth** der ausgewählten Node lassen sich alternative Anmeldeinformationen für die WMI-Abfragen zuordnen. Der Wert Standard in dieser Spalte bedeutet, dass die Prüfung der Node mit den in der Basiskonfiguration angegeben Anmeldeinformationen erfolgt.

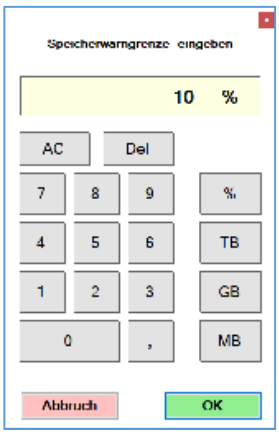
Für WMI-Prüfungen stehen folgende vier Überwachungsmöglichkeiten zur Verfügung:

Laufwerksüberwachung

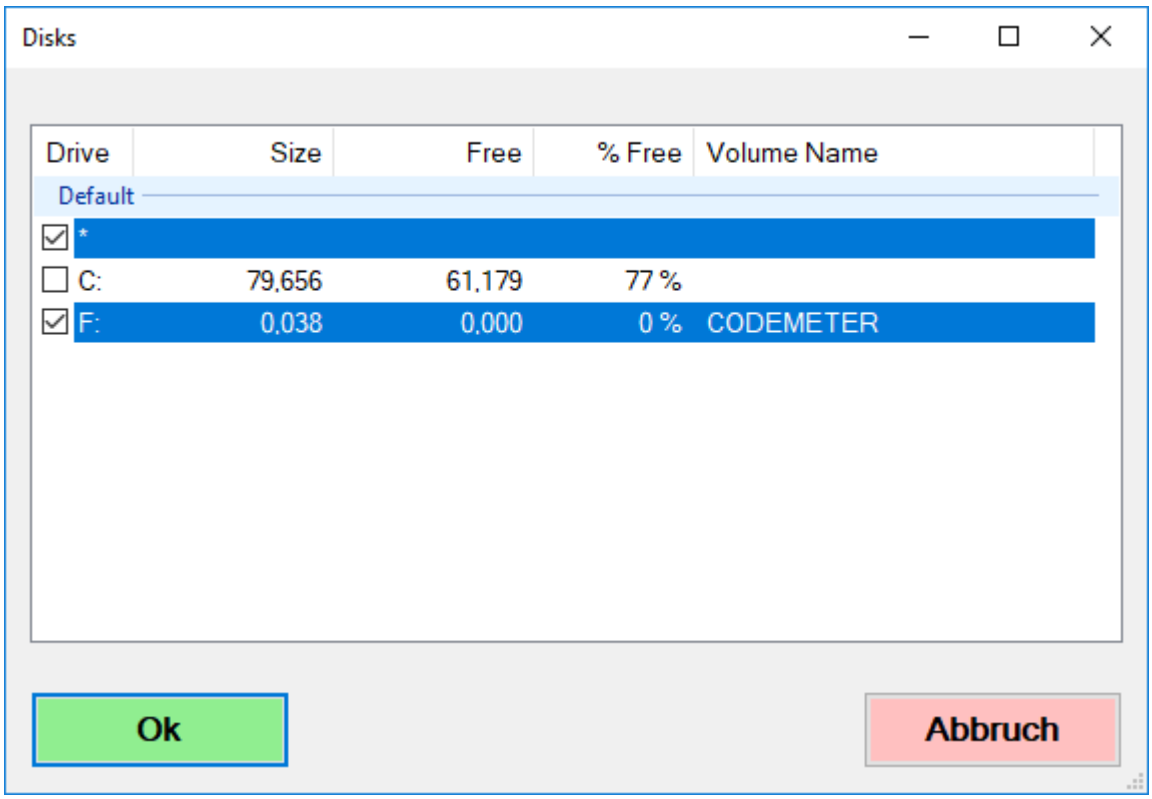
Im Bereich Laufwerksüberwachung werden die zu überwachenden Laufwerke der selektierten Node angezeigt. Ein * bedeutet, dass alle Laufwerke überwacht werden und für alle Laufwerke die gleichen Speichergrenzen gelten. Wird zum Stern ein zusätzliches Laufwerk ausgewählt, dann wird dies von der Überwachung ausgeschlossen und die Option **Nicht** ist angekreuzt.



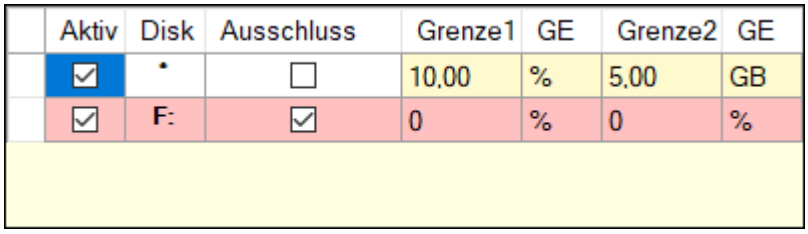
Klickt man auf die gelb markierten Felder in den Spalten **Grenze** und **GE**, dann erscheint folgender Eingabedialog zur Festlegung neuer Überwachungsgrenzen.



Möchte man unterschiedliche Speichergrenzwerte je Laufwerk festlegen, dann kann man dies einfach durch betätigen des Select-Buttons bewerkstelligen. Es erscheint ein Fenster mit der Auflistung aller Laufwerke für diese Node. Jetzt muss man nur noch die Auswahl mit dem * entmarkieren, die gewünschten Laufwerke markieren und mit **Set** bestätigen.



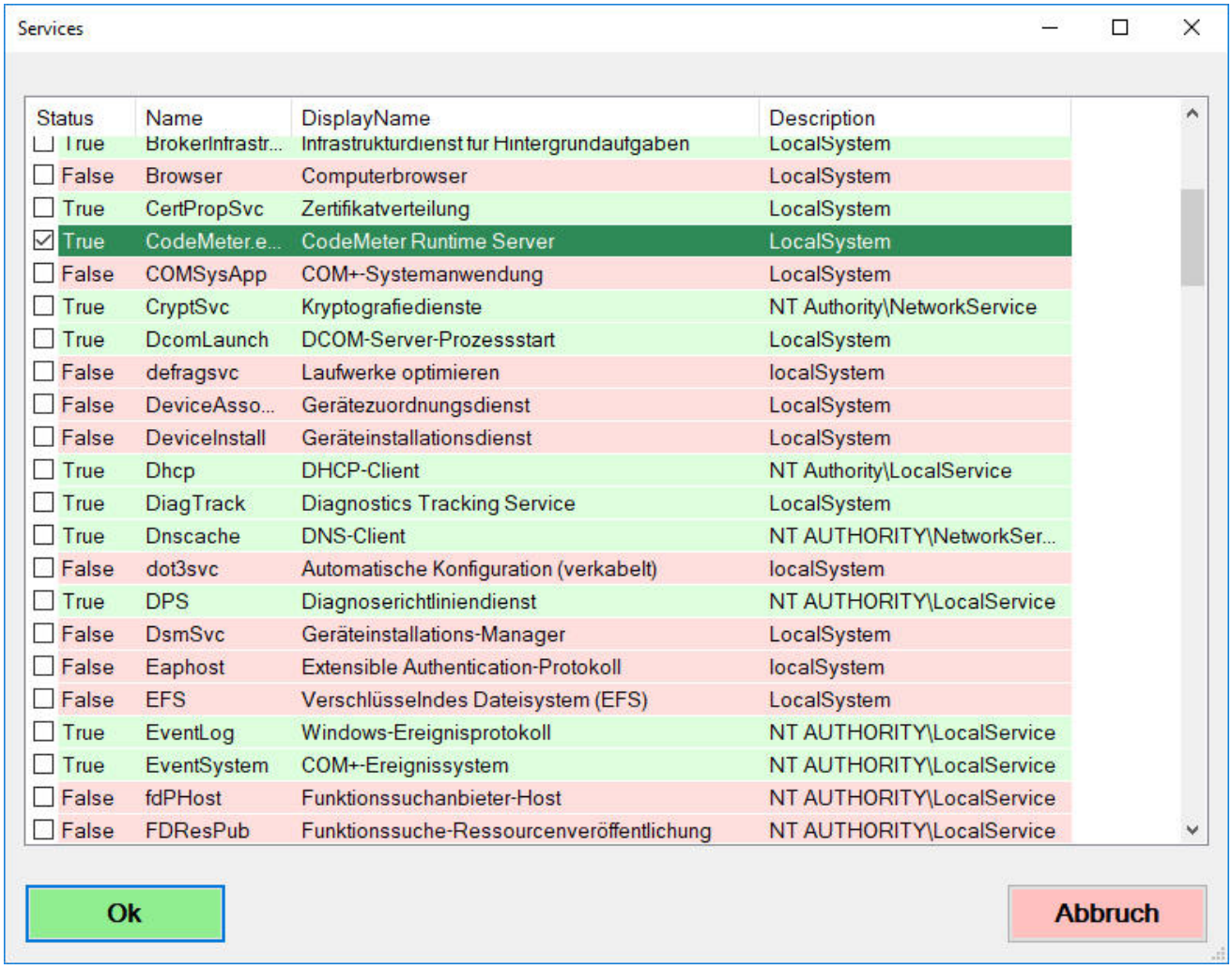
Nun werden ALLE zuvor markierten Laufwerke einzeln aufgelistet. Wird Stern mit ausgewählt, dann werden die selektierten Laufwerke von der Überwachung ausgeschlossen.



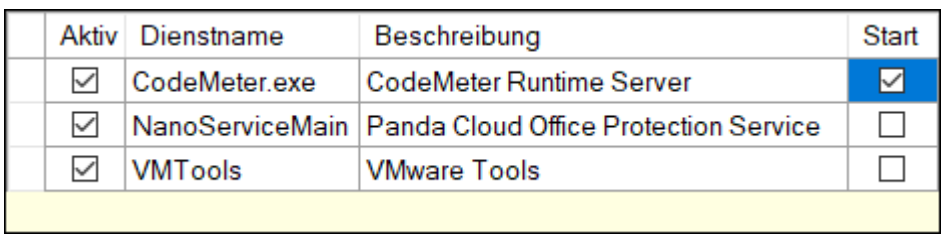
Durch klicken auf die Spalte **Grenze** des jeweiligen Laufwerks können nun individuelle Speichergrenzwerte festgelegt werden.

Dienstüberwachung

Genauso einfach wie die Laufwerksüberwachung gestaltet sich die Überwachung von Diensten. Zur Einrichtung einer Überwachung einfach auf die **Select** Schaltfläche klicken und es öffnet sich ein Fenster mit allen aktiven Diensten der selektierten Node.



Jetzt müssen die zu überwachenden Dienste nur noch selektiert und mit **Set** bestätigt werden.

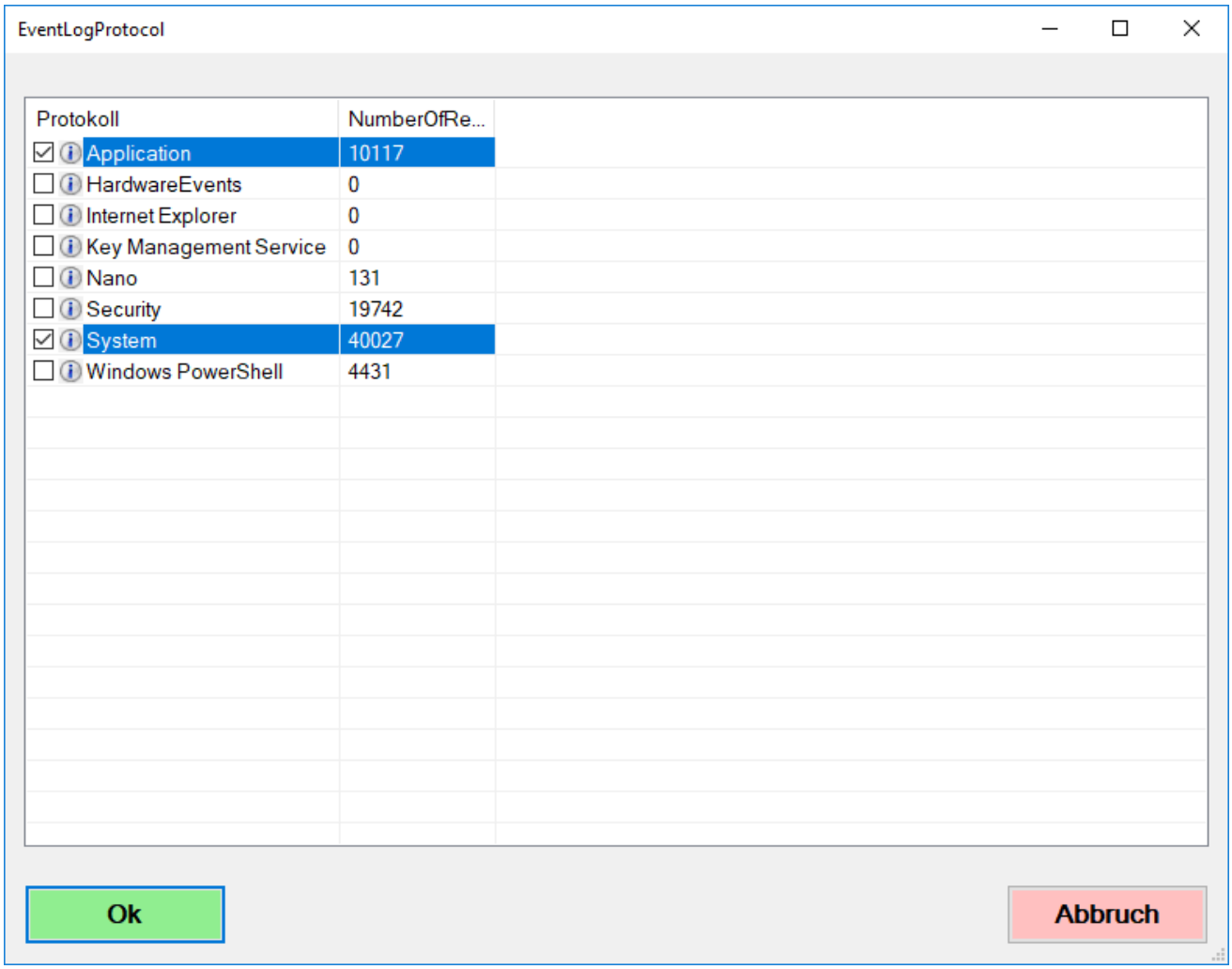


Über die Option **Start** kann eingestellt werden, dass beim Ausfall eines Dienstes versucht werden soll, den Dienst wieder zu starten.

Nach erfolgter Auswahl werden die zu überwachenden Dienste wie oben dargestellt in der Konfigurationsübersicht angezeigt.

EventLog Überwachung

Eine Besonderheit ist die Überwachung der Log-Einträge eines beliebigen Windows EventLog Protokolls. Nach Betätigung der **Select**-Schaltfläche erscheinen die auf dem selektierten System zur Verfügung stehenden Protokolle. Die Spalte NumberOfRecords zeigt die Anzahl der Einträge im EventLog Protokoll. Die Überwachung der Protokolle kann wie auch bei den Überwachungen zuvor durch einfaches anklicken eingerichtet werden.

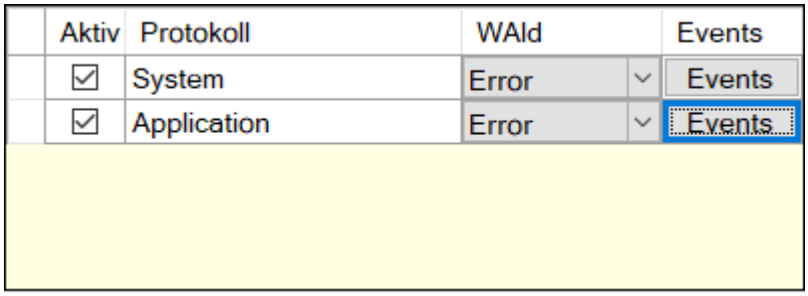


Im Unterschied zu den anderen Überwachungen werden bei Event Log Einträgen lediglich die als Fehler oder kritisch aufgeführten Einträge der letzten 24 Stunden gelesen. Diese werden in der

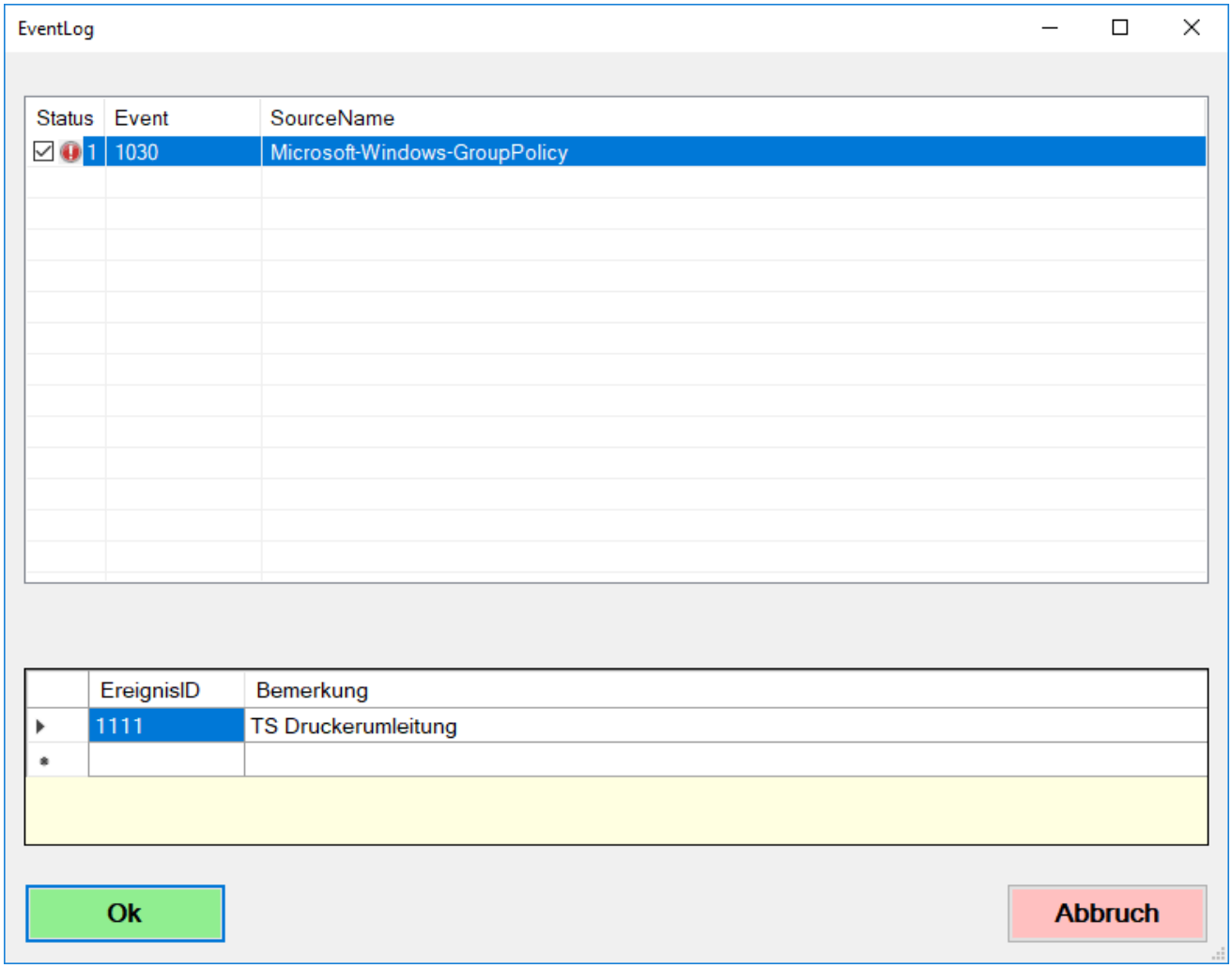
Überwachung auch nicht als Fehler, sondern als Warnung angezeigt. Zusätzlich erscheint in der Node die Anzahl der gefundenen Fehler-Einträge. Diese können in der täglichen Arbeit sehr hilfreich sein, wenn z.B. Programme, die im Hintergrund aktualisiert werden sollten Fehler verursachen, die man so nicht mitbekommt. Die Erfahrung hat gezeigt, dass dies z.B. bei Aktualisierungen von Vieren Scannern manchmal der Fall ist. In so einem Fall wären die Systeme nicht mehr richtig geschützt. In der Überwachung würden aber die Zähler in den Nodes erhöht und möglicherweise erscheint der Fehler auf mehreren Systemen gleichzeitig.

Genau so kann es sein, dass nach konfigurationsarbeiten oder Installationsarbeiten plötzlich mehrere Fehler im Protokoll auftauchen. Diese werden oft zu spät bemerkt. In der aktiven Überwachung wäre dies sehr zeitnah auffällig.

Das nachfolgende Fenster zeigt die Einrichtung für die Überwachung von zwei Event Log-Protokollen:



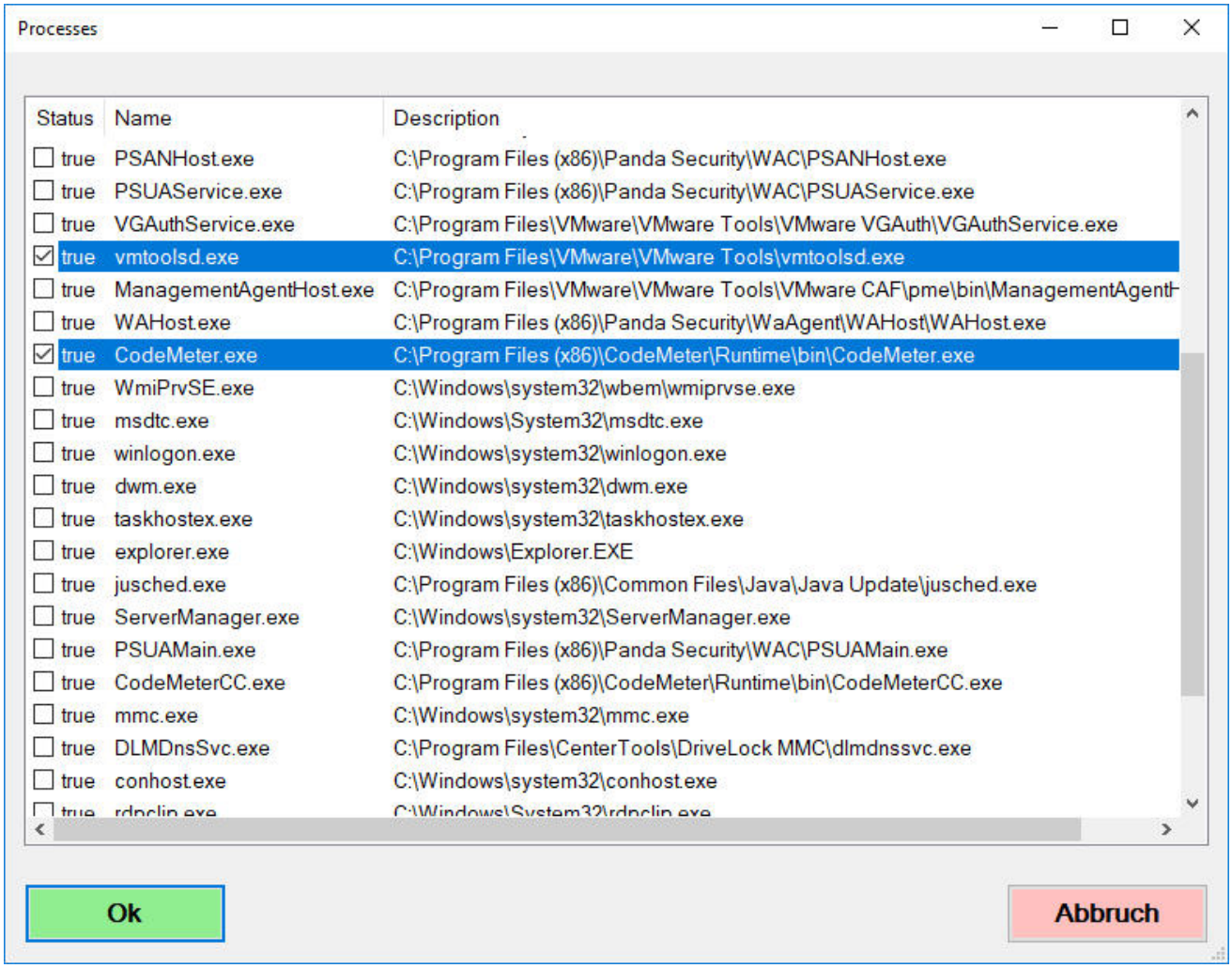
Jetzt kann es natürlich vorkommen, dass auf den Systemen immer wieder Fehler erscheinen, die sich nicht abstellen lassen, aber keine wichtige Funktion beeinträchtigen, so zum Beispiel die Fehler-ID 1111 auf einem Terminalserver, die aussagt, dass es Probleme mit dem Remote Drucker gibt. Solche nervigen für die Überwachung irrelevanten Fehlermeldungen kann man ignorieren.



Nach Betätigung des Buttons **Events** erscheinen alle Fehlercodes der letzten 24 Stunden in einem Auswahlfenster. Durch Markierung dieser Codes werden die Fehler zukünftig ignoriert. Ist der Fehler nicht in der Liste vorhanden, dann kann er im unteren Abschnitt auch manuell eingetragen werden.

Aktive Prozesse überwachen

Als weitere Möglichkeit können auch aktive Prozesse einer Windows Node überwacht werden. Wie auch schon bei der Dienstüberwachung beschrieben erscheint nach Betätigung des Select-Buttons ein Fenster mit allen zurzeit auf dieser Node aktiven Prozessen. Diese können wieder durch einfaches anklicken selektiert und mittels Betätigung des **Set**-Buttons in die Überwachung übernommen werden.



Bei der Überwachung von Prozessen können als Besonderheit auch manuelle Einträge hinzugefügt und die Überwachung umgekehrt werden.

Will man beispielsweise verhindern, dass TeamViewer auf einem System ausgeführt wird, und man kennt nicht den vollständigen Prozessnamen dann kann man den Prozessnamen wie im nächsten Bild gezeigt, zwischen zwei Sterne setzen. Zusätzlich muss die Option **Proz.Akt** aktiviert sein.

Aktiv	ProcessName	Proz.Aktiv	Kill	Bechreibung
☑	vmtoolsd.exe	☐	☐	
☑	CodeMeter.exe	☐	☐	
☑	*TeamView*	☑	☑	Teamviewer killen
☐		☐	☐	

Dieser Eintrag erzeugt nun einen Alarm, wenn ein Prozess mit der Bezeichnung TeamView im Prozessnamen gestartet wird. Ist zusätzlich die Option **Kill** mit aktiviert, dann wird der Prozess mit dieser Bezeichnung auf dem Überwachten System beendet.

Die Beendigungsfunktion **Kill** hat nur eine Auswirkung auf Prozesse, bei denen die Option **Proz.Akt.** mit angekreuzt ist.

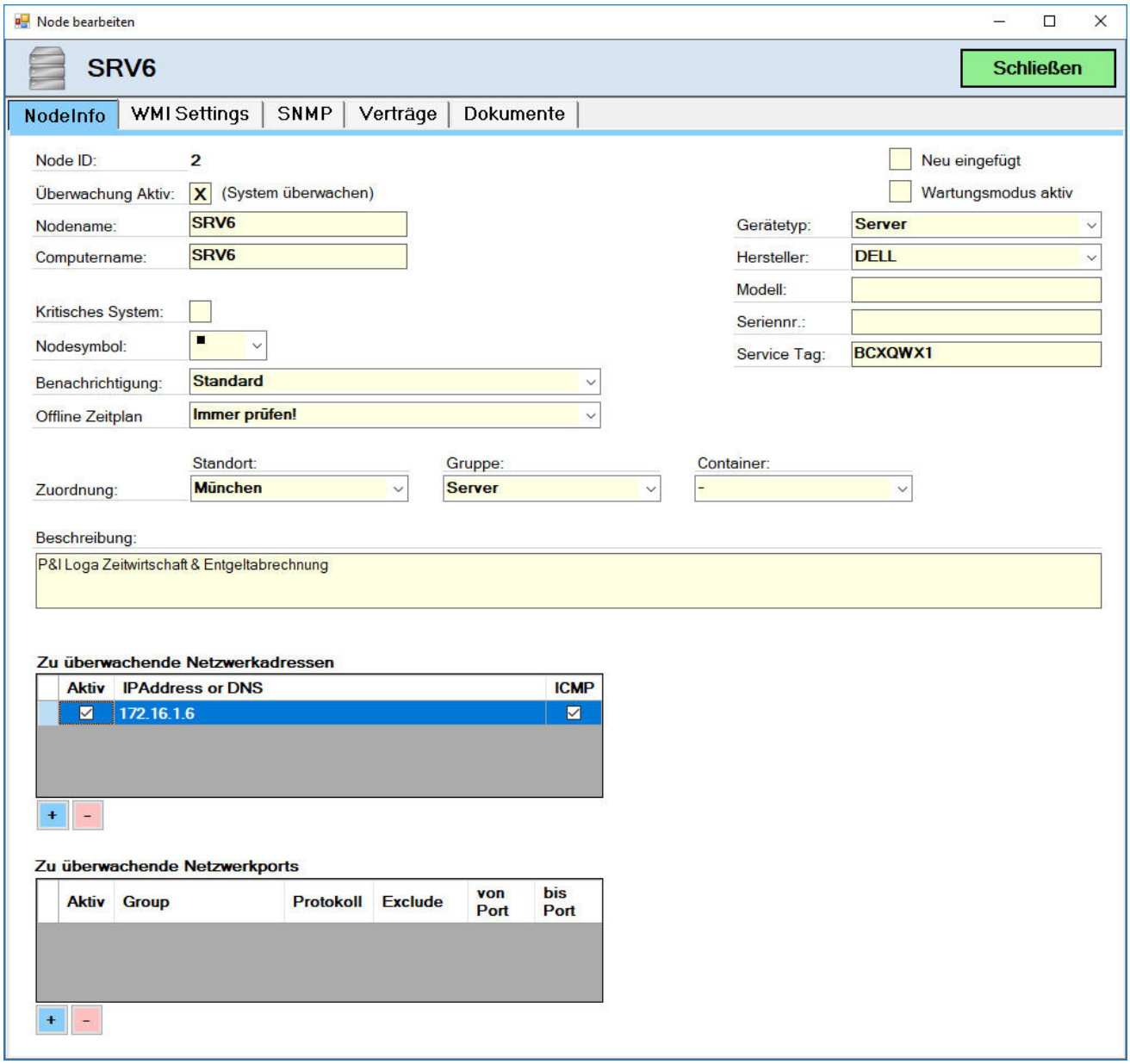
Detail-Konfiguration

Durch Betätigung des vordersten Edit-Buttons in der Node-Liste gelangt man in die Detailkonfiguration der Node.

E	Al	Nodename	Location	Group	Page	NetName	Kritis	WMI	Auth	ServiceTag	Notificat	Description	SLA	Nodetype	Log	Sort	Offline
	☑	SRV6	Obernzell	Server	0	SRV6	☐	☑	Admin	BCZQWX1	St...	P&I Loga Zeitwirtsch...	1	Standard	☐	2	Immer pr...

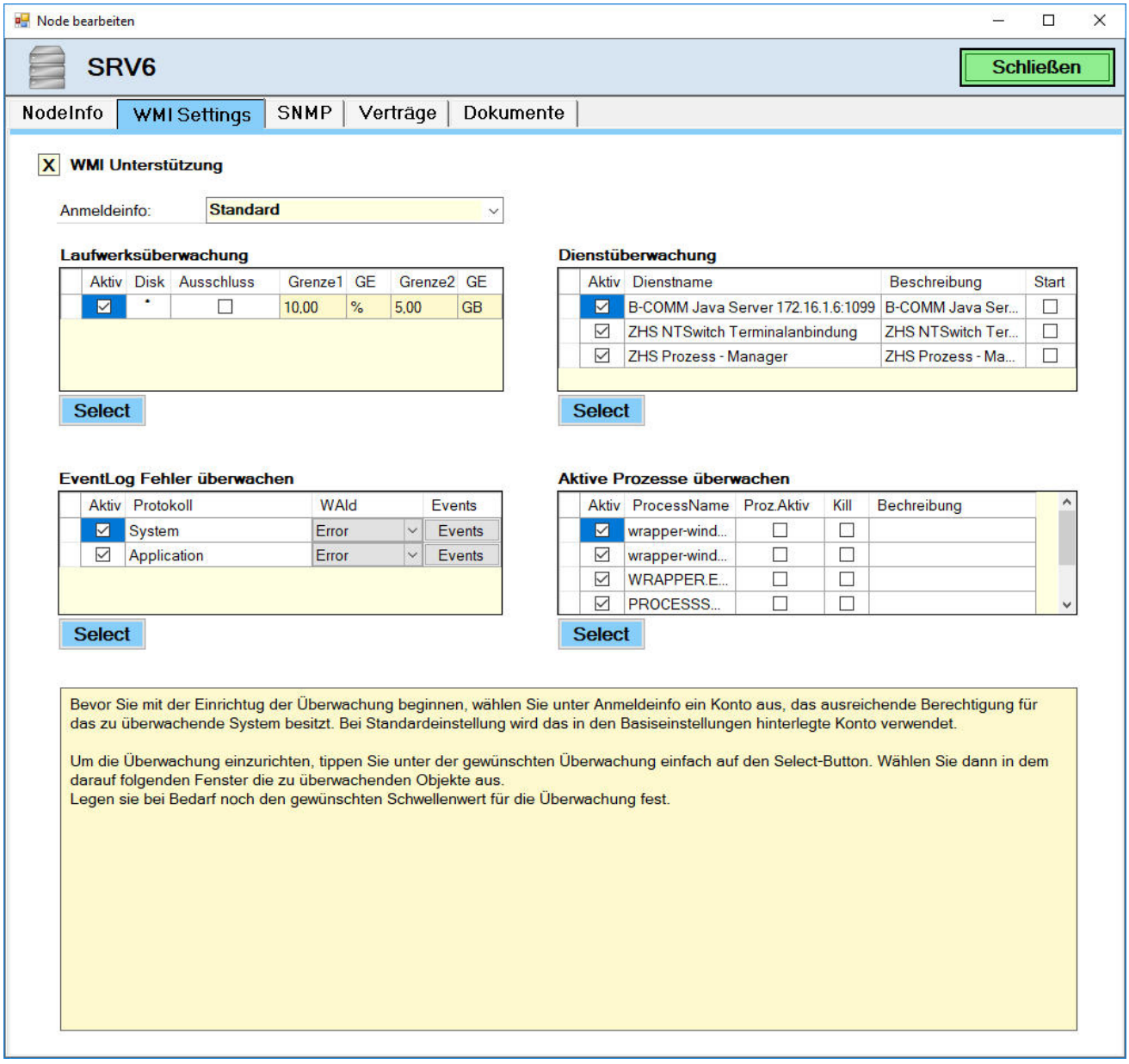
NodeInfo

Im oberen Bereich wird der Name der Node angezeigt. Im Register | NodeInfo | werden allgemeine Informationen wie Beschreibung, Standortdaten, Gerätetyp, Hersteller, Seriennummer, Benachrichtigungseinstellungen, Zeitpläne und IP-Adressinformationen.



WMI Settings

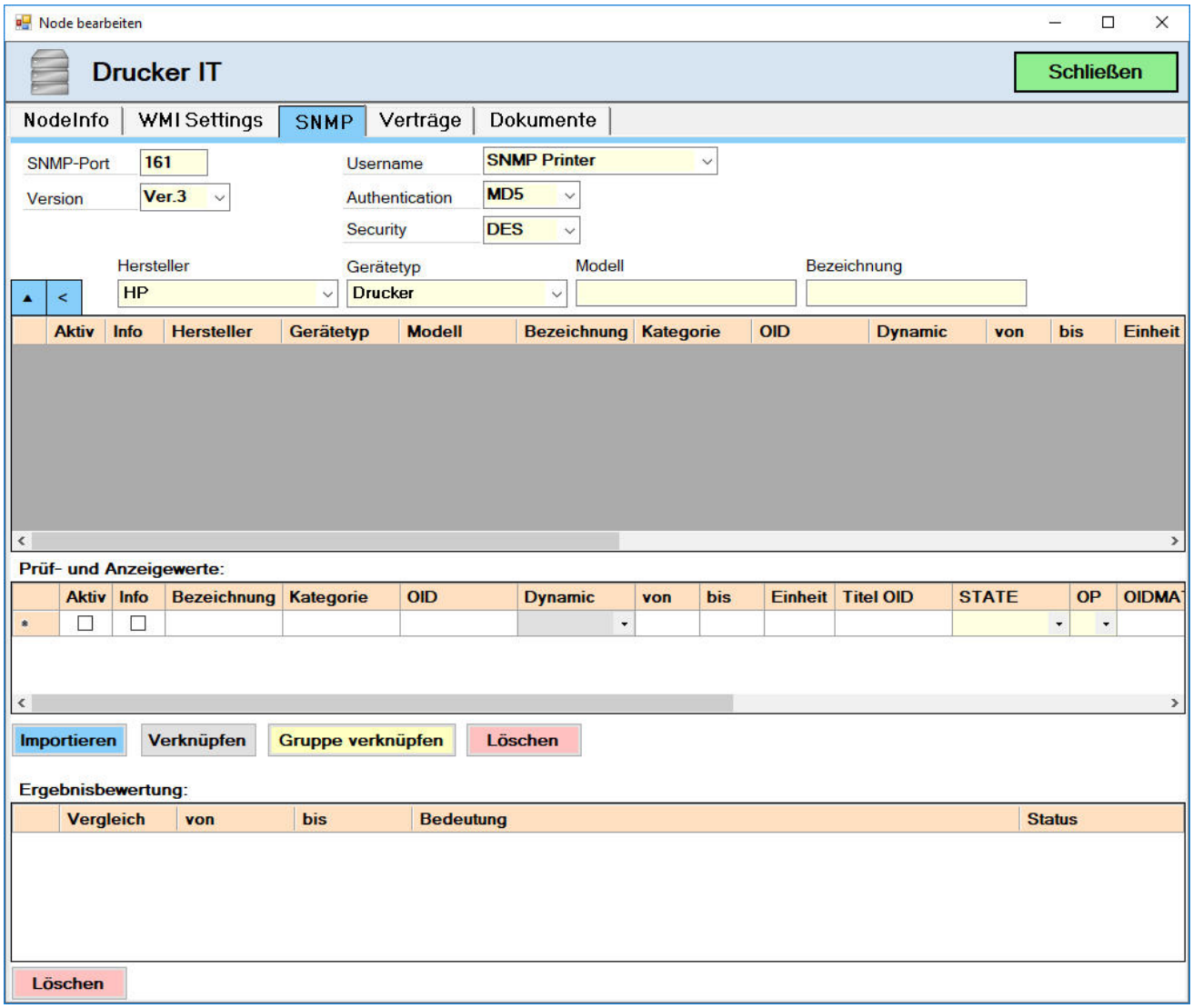
Im Register | WMI Settings | können für Windows Endgeräte Überwachungen für Freien Plattenspeicher, laufende Dienste, aktive Prozesse und Event Log Fehlereinträge eingerichtet werden. Die Einrichtung funktioniert wie unter **WMI – Windows Management Instrumentation** beschrieben.



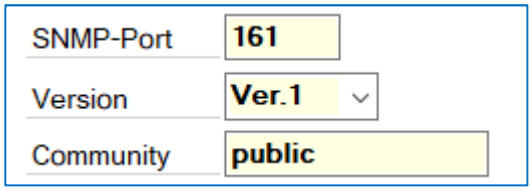
SNMP

Für nicht Windows Nodes gibt es die Möglichkeit Überwachungen via SNMP durchzuführen, soweit dies vom Endgeräte unterstützt wird.

Nachfolgendes Fenster zeigt den Arbeitsbereich zum Zuordnen von SNMP-Vorlagen zur Node.

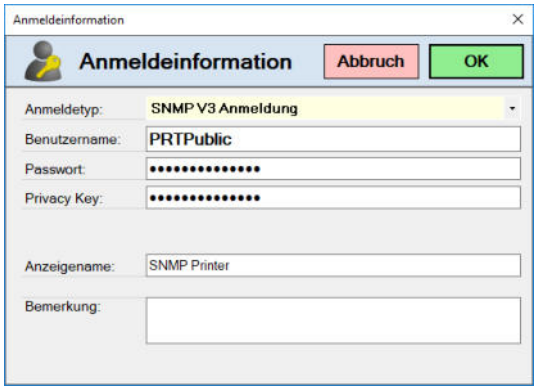


Für die Einrichtung von SNMP-Abfragen für das Gerät müssen zuerst die zu verwendende SNMP-Version und die zugehörigen Parameter wie Community (für Version 1 und 2c),

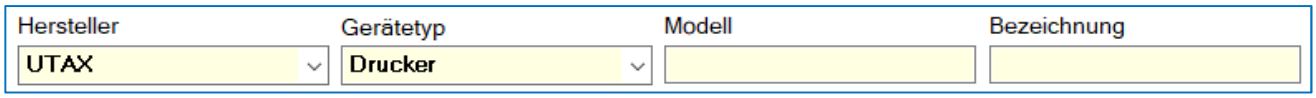


oder Username, Authentication und Security für Version 3.

Der eigentliche Name und die Schlüssel für Authentication und Security sind in der Benutzerverwaltung (Authentifizierung) hinterlegt.



Die darunterliegende Zeile mit Hersteller, Gerätetyp Modell und Bezeichnung dienen zur Filterung der Vorlagentabelle. Dadurch lässt sich die Ergebnismenge stark einschränken.



Im oberen Tabellenbereich werden die Vorhandenen SNMP-Vorlagen angezeigt.

Durch Betätigung von  werden die vorderen Spalten Hersteller, Gerätetyp und Modell ausgeblendet, dadurch wird der Bereich etwas übersichtlicher.

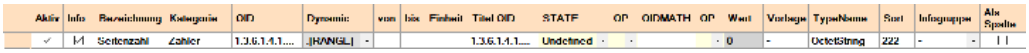
A	I	Bezeichnung	Kategorie	OID	Dynamic	von	bis	Einhei	Titel OID	Status	OP	OIDMATH	OP	Wert	Kon	TypeName	Sort	Infogruppe	Vorlagengruppe
☑	☑	Seitenzahl	Zähler	1.3.6.1.4.1....	.[RANGE]				1.3.6.1.4.1....	Undefin...				0		OctetString	222	-	UTAX-Drucker
☑	☑	Tonerstand	Zähler	1.3.6.1.2.1....	.[RANGE]	1	1	%		Good	/	1.3.6.1.2.1....	*	100		Integer32	1	Druckerinfo	UTAX-Drucker
☑	☑	Displaytext	Gerätestatus	1.3.6.1.4.1....	[OFF]					Undefin...				0		OctetString	0	-	UTAX-Drucker
☑	☑	Seriennum...	Modellinfo	1.3.6.1.2.1....	[OFF]					Undefin...				0		OctetString	0	-	UTAX-Drucker
☑	☑	IP-Adresse	Netzwerk	1.3.6.1.4.1....	[OFF]					Undefin...				0		IPAddress	0	-	-
☑	☑	Modell	Modellinfo	1.3.6.1.4.1....	[OFF]					Undefin...				0		OctetString	0	-	-

Mit der Schaltfläche  kann der Vorlagenbereich ausgeblendet werden, dadurch steht dem Überwachungsbereich mehr Platz zur Verfügung.

Sie können Vorlagen auf verschiedene Weise dem Gerät zuweisen. Entweder durch …

Importieren

Fügt die markierte Vorlage zum Überwachungsbereich hinzu und ermöglicht die individuelle Anpassung der Tabellenfelder im Überwachungsbereich.

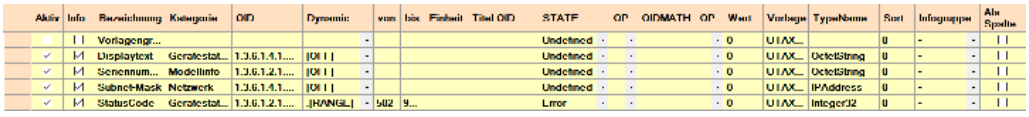


Verknüpfen

Fügt die markierte Vorlage als Verknüpfung zur Überwachung hinzu. Eine Anpassung der Werte in der Überwachung ist nicht möglich. Durch Anpassung der Vorlage wird automatisch der Wert in der Überwachung angepasst. Somit können Überwachungseinstellungen für einheitliche Geräte zentral über die Templates verwaltet werden. Verknüpfte Einträge werden grau dargestellt.

Gruppe verknüpfen

Ist einer Vorlage in der Spalte Vorlagengruppe ein Wert zugewiesen, dann kann dieser als Gruppe verknüpft werden. Hierbei werden ALLE Vorlagenzeilen, die die selbe Zuweisung in der Gruppe besitzen der Überwachung hinzugefügt. Einträge aus verknüpften Gruppen werden im Überwachungsbereich gelb angezeigt.



Diese Einträge können in der Überwachung ebenfalls nicht bearbeitet werden, sondern muss wieder im Vorlageneditor erfolgen. Der Vorteil von verknüpften Gruppen liegt darin, dass beim zuweisen neuer Werte zu einer Vorlagengruppe diese auch allen Geräten, denen diese Gruppe zugeordnet wurde, hinzugefügt wird.

Löschen

Entfernt einen Überwachungseintrag. Ist die Zeile einer Vorlagengruppe markiert, dann werden alle Zeilen der Gruppe aus der Überwachung entfernt.

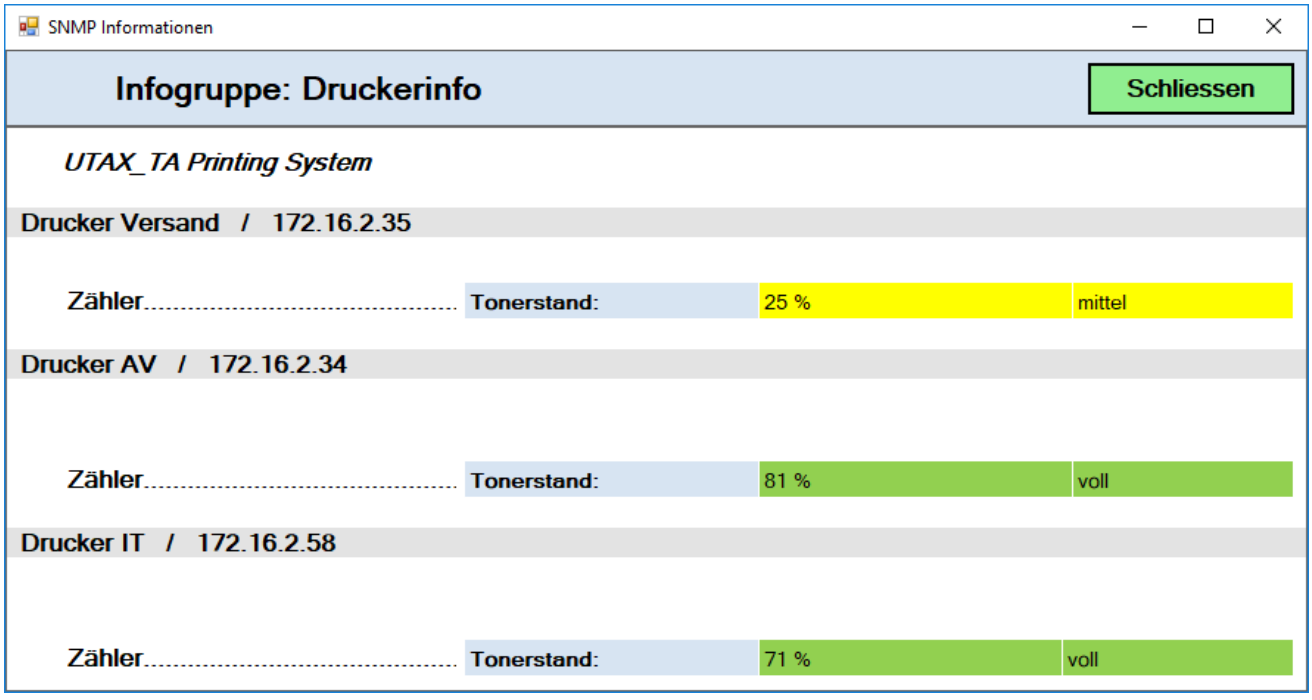
Ergebnisbedeutung

Im unteren Bereich befindet sich der Abschnitt für die Ergebnisbedeutung. Hier kann die Bedeutung des ermittelten SNMP-Werts eingestellt werden. Für unser Tonerstand Beispiel haben wir eingestellt, dass Werte Größer 30 % (wir haben in der OID den Prozentwert berechnet) als Gut dargestellt werden, zwischen 10 und 30 % wird eine Warnung ausgegeben und unter 10 Prozent ein Fehler.

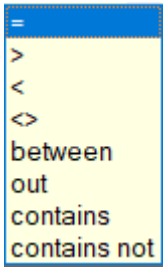
	Vergleich	von	bis	Bedeutung	Status
▶	>	30		voll	Good
	betwe...	10	30	mittel	Warning
	<	10		Toner wechseln!	Error
*					

Der Bedeutungstext wird bei Anzeige von SNMP-Informationen zusätzlich zum Wert dargestellt. Der Status nimmt Einfluss auf die Farbe sowohl in der Überwachung als auch in der Informationsübersicht der ermittelten Werte.

Nachfolgendes Fenster zeigt, die Auswirkung der Werte auf die Anzeige:



In der Spalte Vergleichswert stehen folgende Möglichkeiten zur Verfügung:

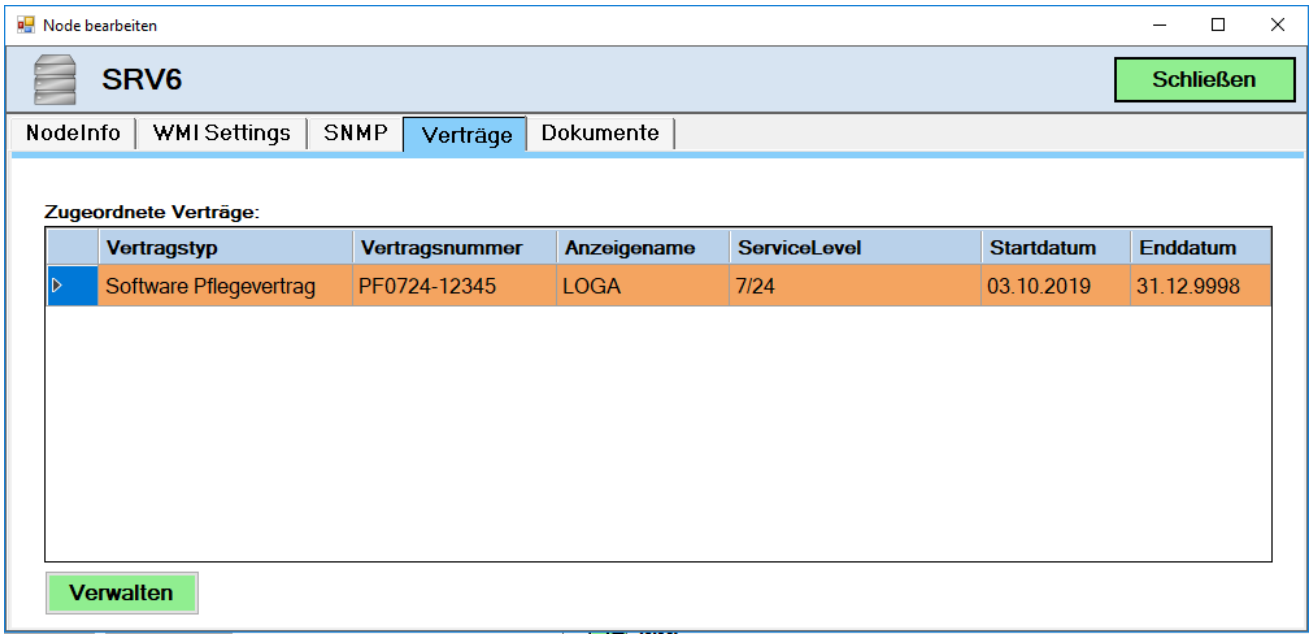


=	Der ermittelte Wert muss genau der Eingabe entsprechen
>	Der ermittelte Wert muss größer als die Eingabe sein
<	Der ermittelte Wert muss keiner als die Eingabe sein
<>	Der ermittelte Wert muss ungleich als die Eingabe sein
between	Der ermittelte Wert muss zwischen den Eingabewerten liegen
out	Der ermittelte Wert muss sich außerhalb der Eingabewerte befinden
contains	Der ermittelte Wert muss die eingegebene Zeichenfolge beinhalten
contains not	Der ermittelte Wert muss die eingegebene Zeichenfolge NICHT beinhalten

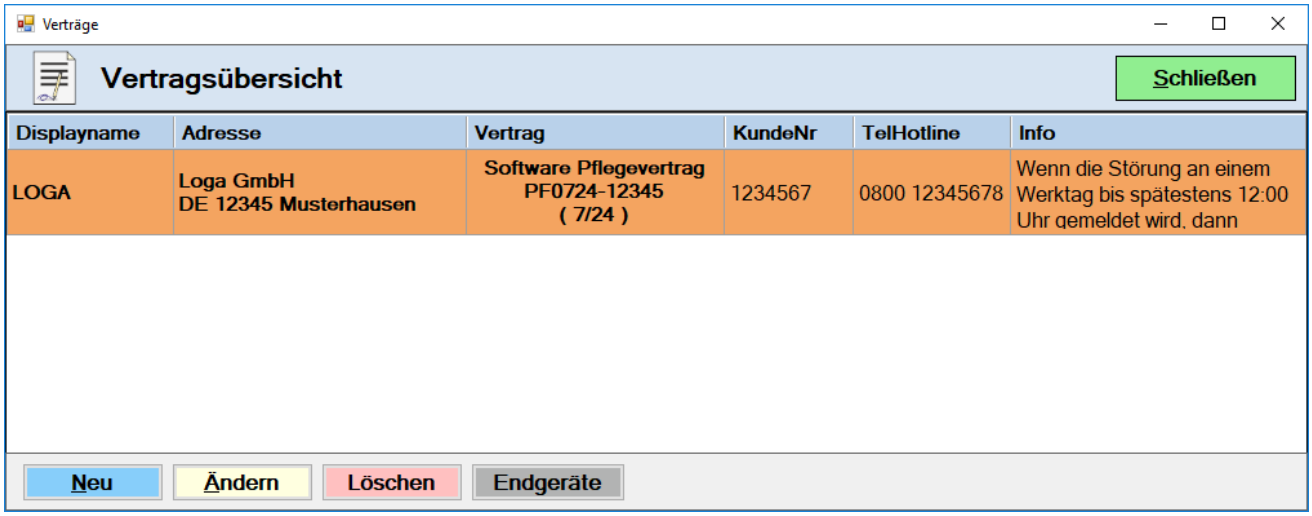
Die genaue Vorgehensweise zum Erstellen von Templates wird im Kapitel SNMP Vorlagen beschrieben.

Verträge

Wartungsverträge können im Register | Verträge | verwaltet und zugeordnet werden. Hier werden alle dem System zugeordneten Wartungsverträge angezeigt.



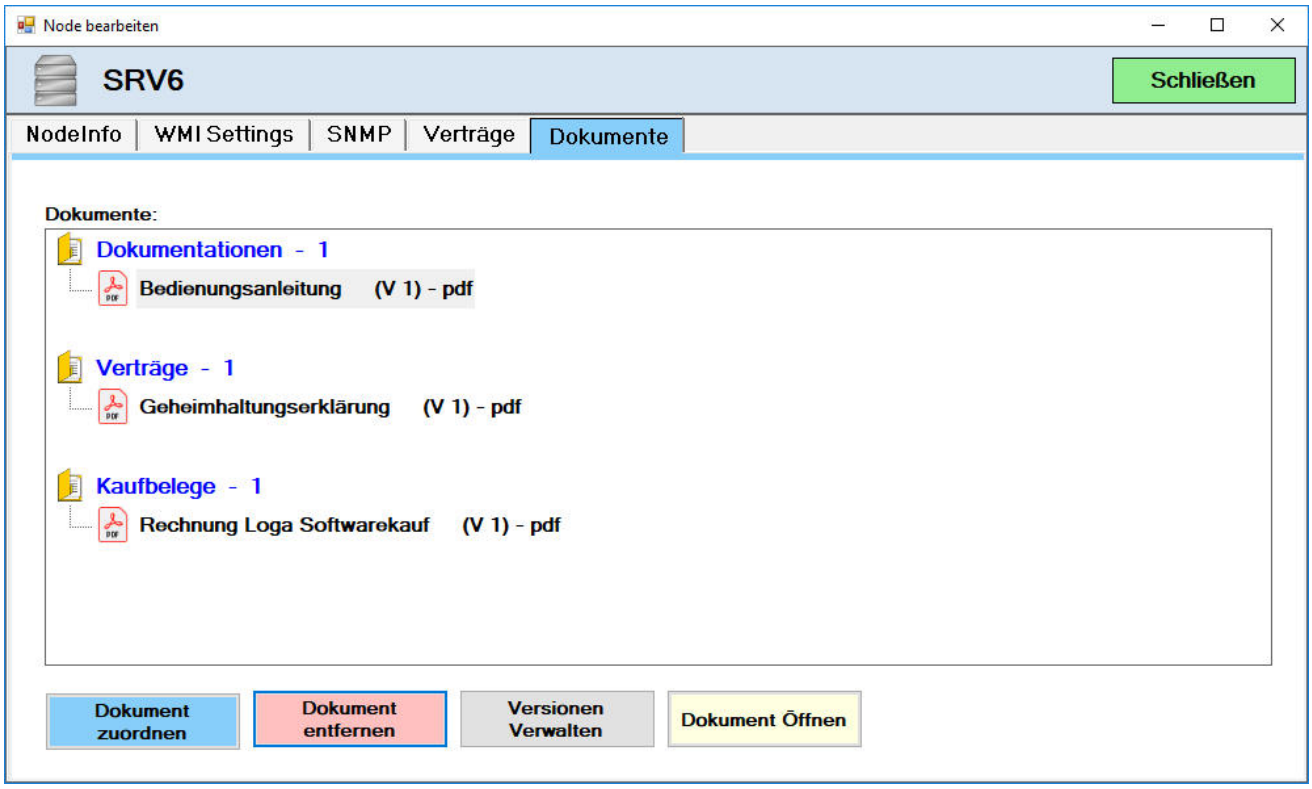
Durch Klick auf [Verwalten] gelangt man in den gelangt man zur Liste mit den Verträgen.



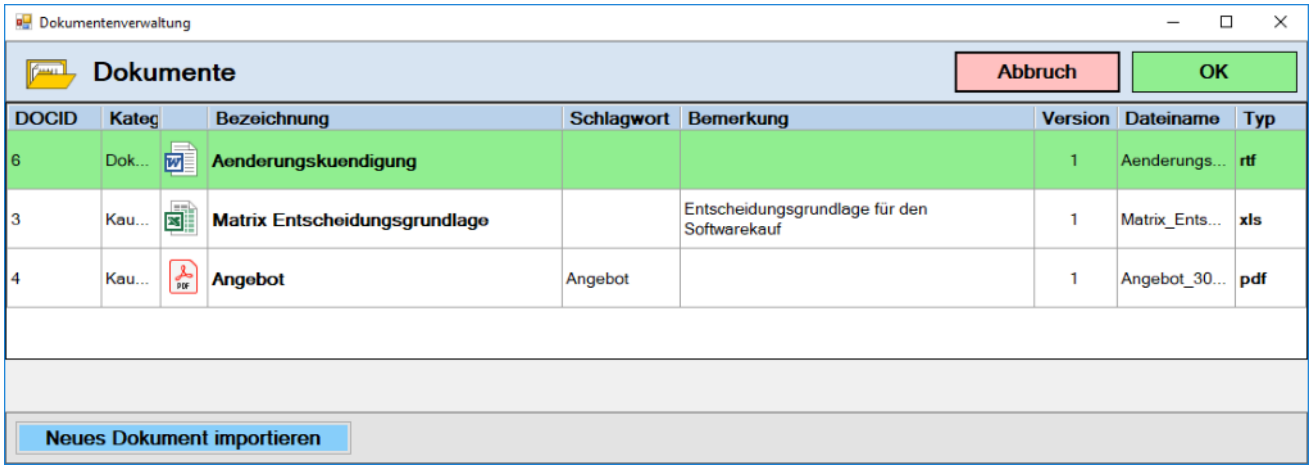
Der weitere Ablauf funktioniert wie unter Abschnitt **Wartungsverträge** beschrieben.

Dokumente

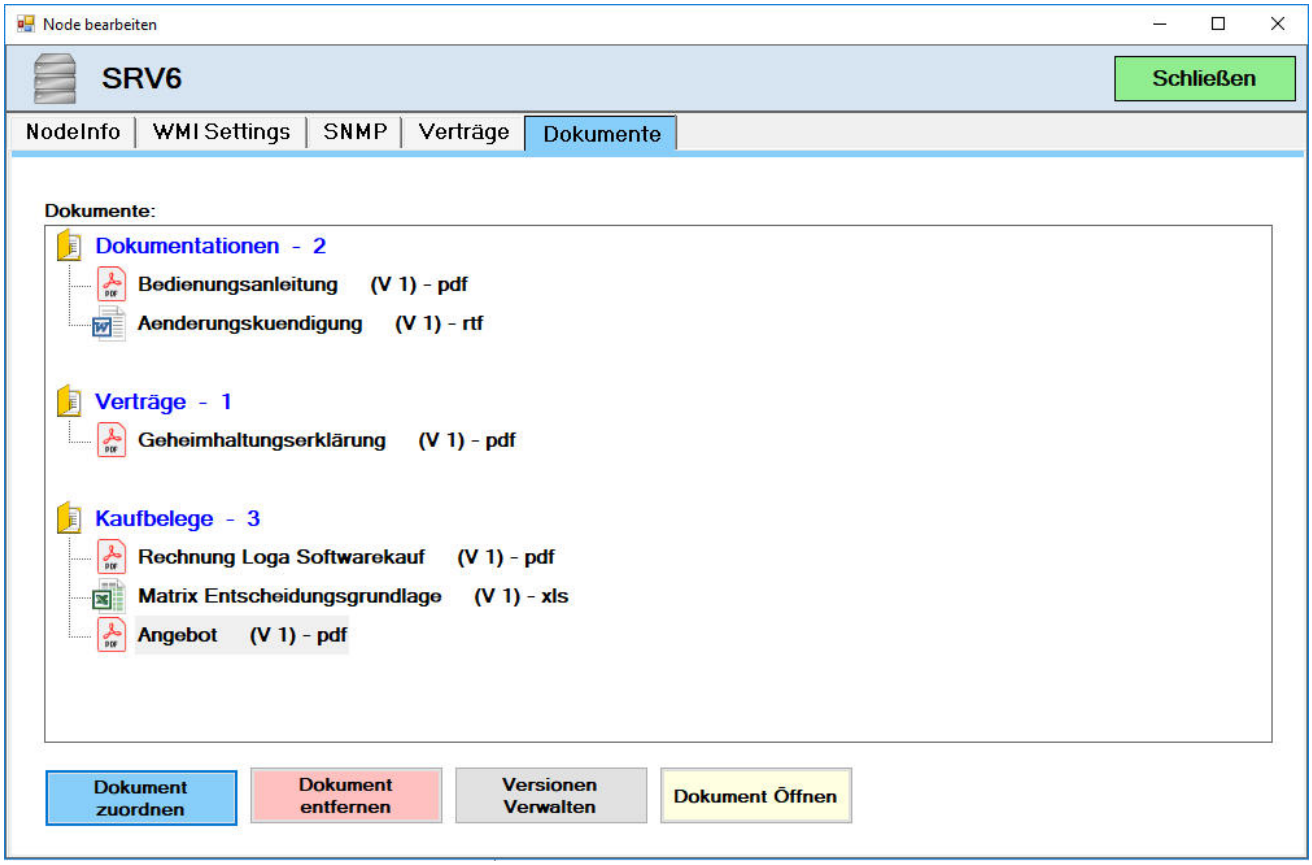
Im Register Dokumente können Einem Geräte Dokumente aus der Dokumentenverwaltung zugeordnet werden.



Über die Schaltfläche [Dokument zuordnen] gelangen Sie zum Dokumentenvorrat der Dokumentenverwaltung. Sind noch keine Dokumente in der Dokumentenverwaltung hinterlegt, dann kann man auch direkt ein Dokument aus dem Dateisystem über die Schaltfläche [Neues Dokument importieren] auswählen.



Im Fenster der Dokumentenverwaltung kann man nun einen aber auch mehrere Verträge auswählen. Nach Betätigung von [OK] werden die Dokumente dem Gerät zugeordnet.



Für markierte Dokumente können folgende Aktivitäten ausgeführt werden:

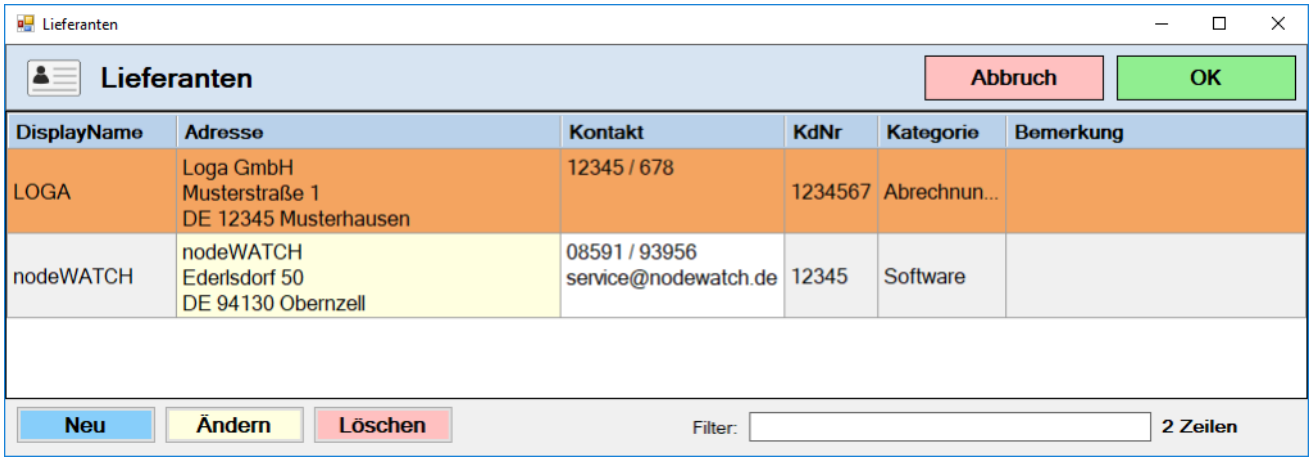
[Dokument entfernen] Löscht die Zuordnung des Dokuments. Das Dokument bleibt in der Dokumentenverwaltung erhalten.

[Versionen Verwalten] Springt in die Versionsverwaltung des Dokuments. Hier können neue Versionen erstellt, oder alte Versionen eingesehen werden. Die Beschreibung finden Sie im Kapitel Dokumentenverwaltung

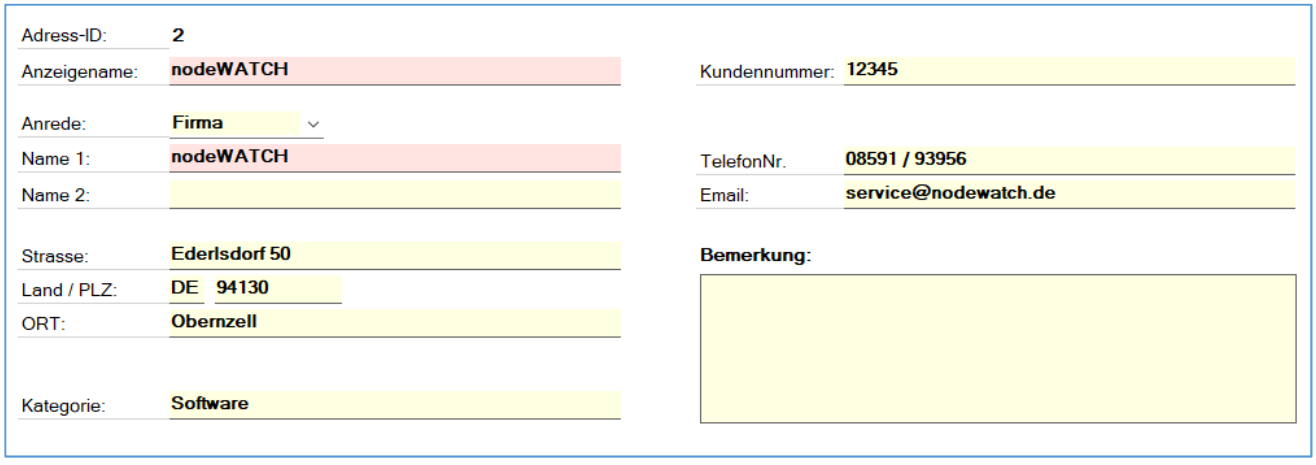
[Dokument öffnen] Durch markieren eines Dokuments und betätigen der Schaltfläche [Dokument öffnen] werden die Dokumente angezeigt. Voraussetzung hierfür ist, dass die entsprechende Software installiert ist, mit dem das Dokument geöffnet werden kann.

Kontaktdaten

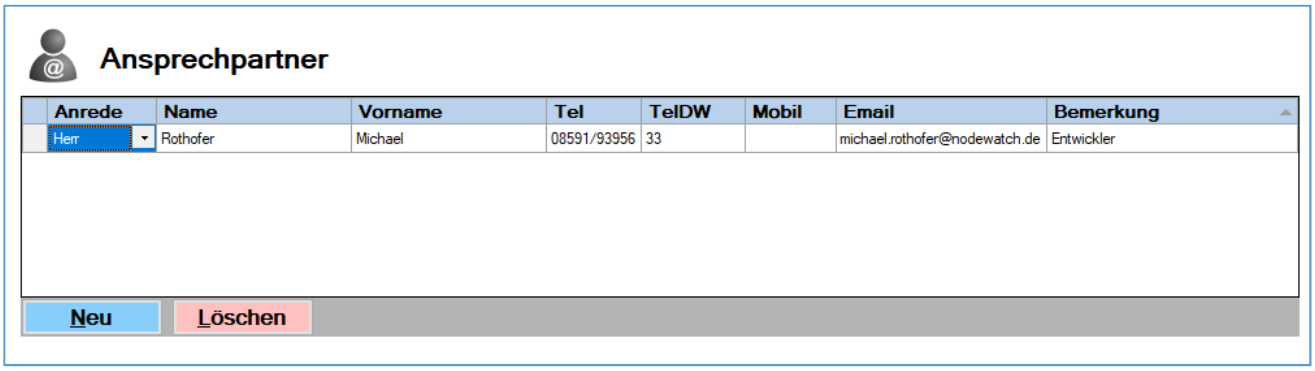
Neben der Überwachung von Systemen ist auch die Verwaltung von Notfallansprechpartner eine wichtige Funktion, deshalb wurde sie in node***WATCH*** implementiert. Gelangt man in die Übersicht der Lieferantenkontaktdaten. Von hier aus können neue Kontaktdaten erfasst, bestehende geändert und gelöscht werden.



Über die Schaltflächen **Neu** und **Ändern** gelangt man in die Erfassungs- bzw. Änderungsformular. Im oberen Teil können die Adressdaten des Lieferanten erfasst werden. Die hier erfassten Adressen werden. Die Felder **Anzeigename** und **Name 1** sind Pflichtfelder.



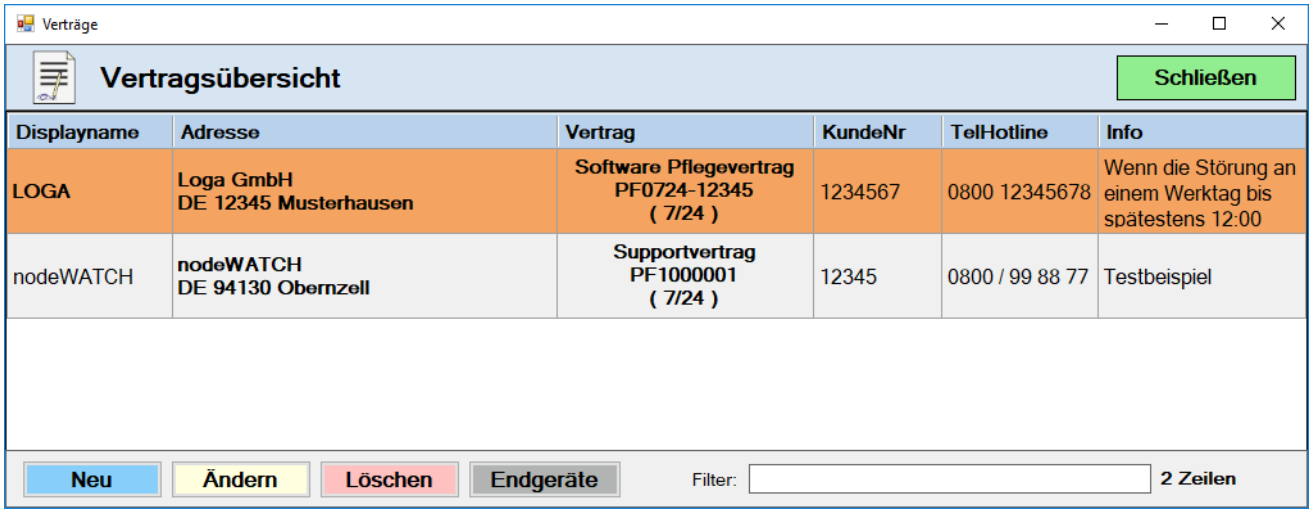
Im unteren Abschnitt lassen sich dann noch Ansprechpartner zum Lieferanten erfassen.



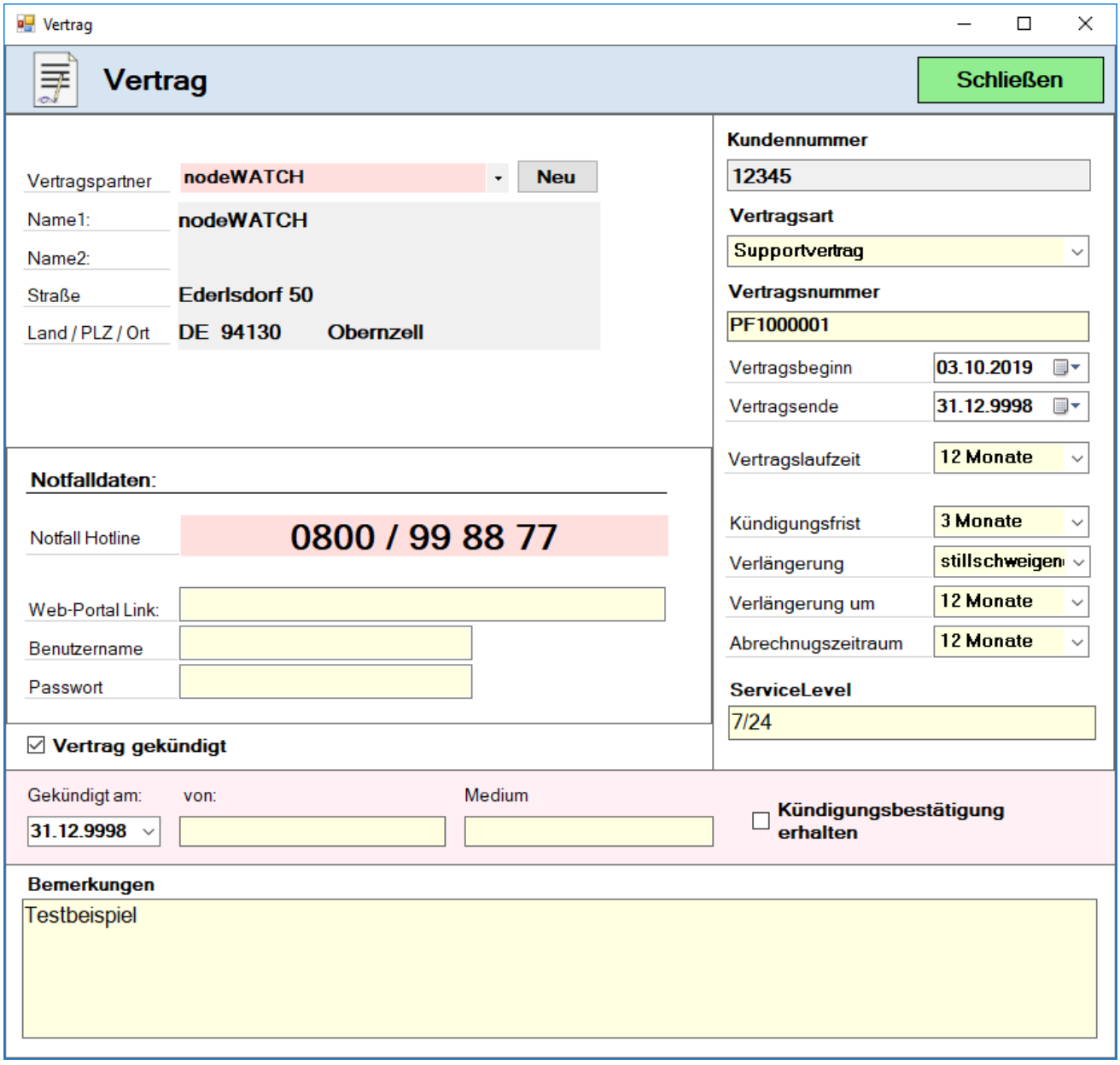
Die Erfassung von neuen Lieferanten kann auch direkt bei der Anlage von neuen Wartungsverträgen erfolgen und muss nicht zwingend vorab geschehen. Die Vorgehensweise wird im Kapitel Wartungsverträge beschrieben.

Wartungsverträge

Neben der Überwachung von Systemen ist es im Notfall auch wichtig, Relevante Daten wie Wartungsvertragsnummern, Telefonnummer für die Notfallhotline uns Ansprechpartner schnell griffbereit zu haben. Zu diesem Zweck wurde in node***WATCH*** die Möglichkeit zur Verwaltung von Vertragsdaten implementiert. Unter dem Menüpunkt **Wartungsverträge** im Hauptmenü, können die wichtigsten Vertragsinformationen erfasst werden. Der Klick auf Wartungsverträge zeigt eine Übersicht über alle erfassten Verträge.



Durch Klick auf die Schaltfläche Neu gelangt man in die Vertragserfassung. Bei der Anlage eines neuen Wartungsvertrages muss zuerst der Vertragspartner im Adressfeld ausgewählt werden. Wurde dieser noch nicht erfasst, dann kann dies an dieser Stelle über die Schaltfläche **Neu** neben dem Auswahlfeld für den Vertragspartner erfolgen.

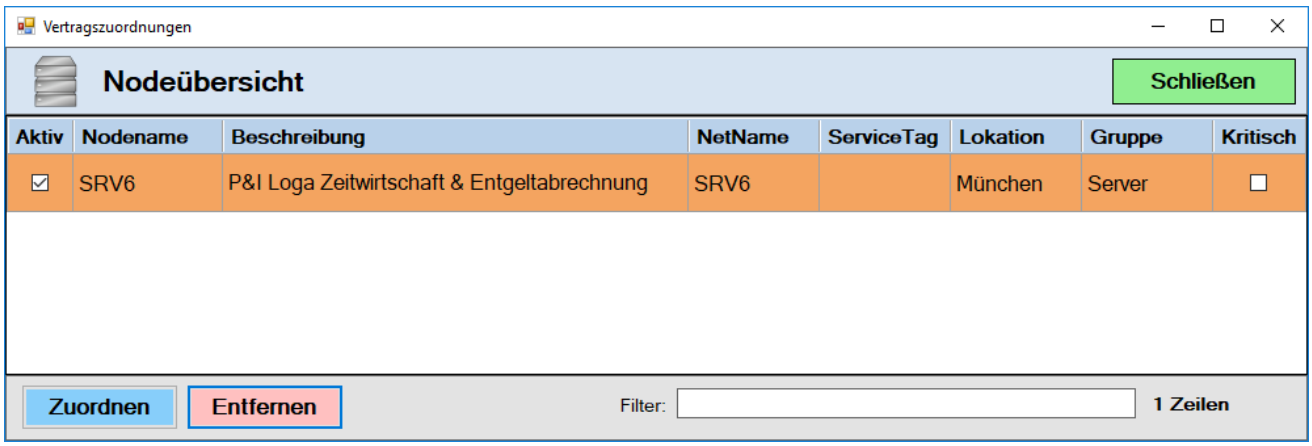


Die hier erfassten Vertragsdaten sind im Überwachungsmodus bei einem Notfall mit wenigen Klicks zu erreichen. Damit der Schnelle Zugriff auf die zugehörigen Verträge ermöglicht wird, muss man die hier erfassten Verträge natürlich auch den zugehörigen Endgeräten zuordnen.

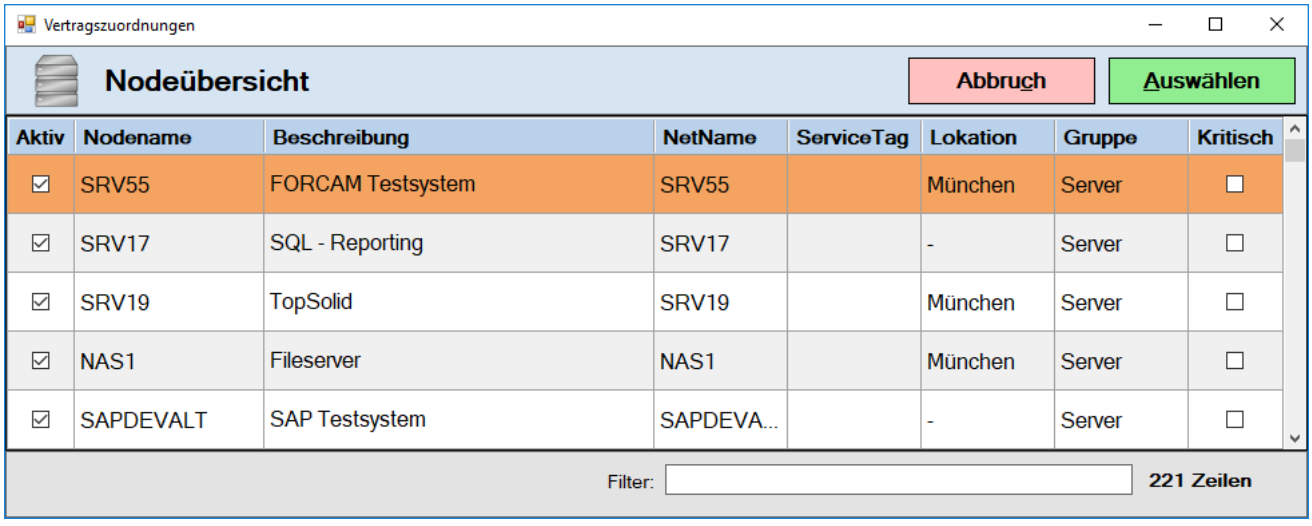
Verträge Endgeräten zuordnen

Die Zuordnung der Verträge zu den jeweiligen Endgeräten erfolgt in der Vertragsübersicht. Hierfür muss der zuzuordnende Vertrag selektiert und dann die Schaltfläche Endgeräte betätigt werden.

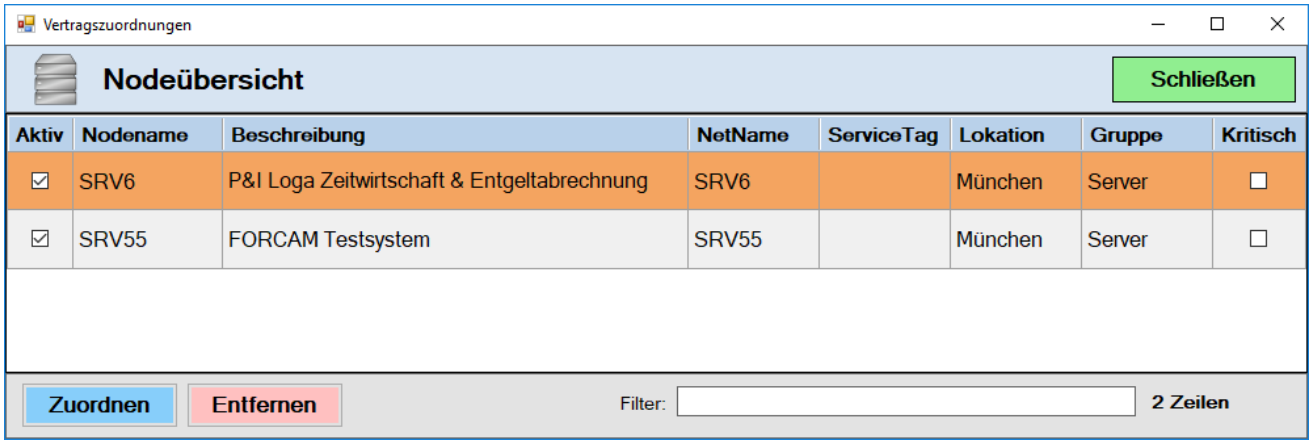
Daraufhin wird eine Liste aller Endgeräte angezeigt, denen der Vertrag zugeordnet wurde.



Durch Klick auf Zuordnen wird eine Liste aller Nodes angezeigt, denen man den Vertrag noch zuordnen kann. Bereits zugeordnete Nodes werden nicht mehr mit aufgelistet.



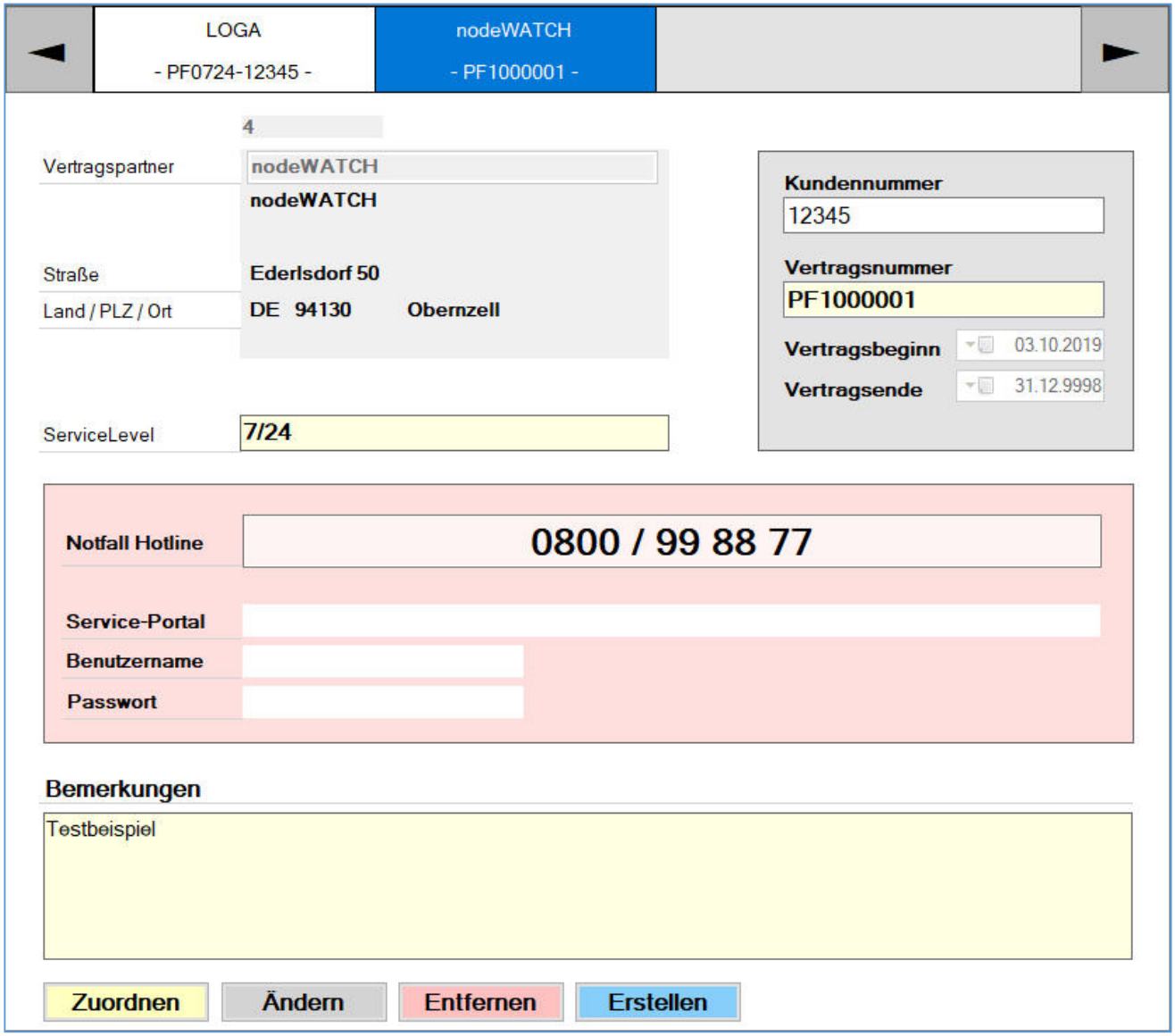
Über das Feld Filter kann man die Auswahl schnell und unkompliziert einschränken. Hat man die Node gefunden, der der Vertrag zugeordnet werden soll, dann muss diese lediglich markieren und die Schaltfläche **Auswählen** betätigen.



Nach Auswahl der neuen Node wird diese ebenfalls in den Vertragszuordnungen angezeigt. Jetzt kann der Vertrag zukünftig im Überwachungsmodus über zugeordnete Node mit wenigen Klicks aufgerufen werden. Über den **Zuordnen**-Button können beliebige weitere Zuordnungen erfolgen. Es ist auch möglich mehrere Verträge einer Node zuzuordnen. Hierfür muss man nur einen neuen Vertrag auswählen oder anlegen und über die Schaltfläche **Endgeräte** und **Zuordnungen** eine neue Gerätezuordnung durchführen.

Beim Aufruf der Vertragsübersicht im Überwachungsmodus werden selbstverständlich ALLE zugeordneten Verträge zur Node angezeigt.

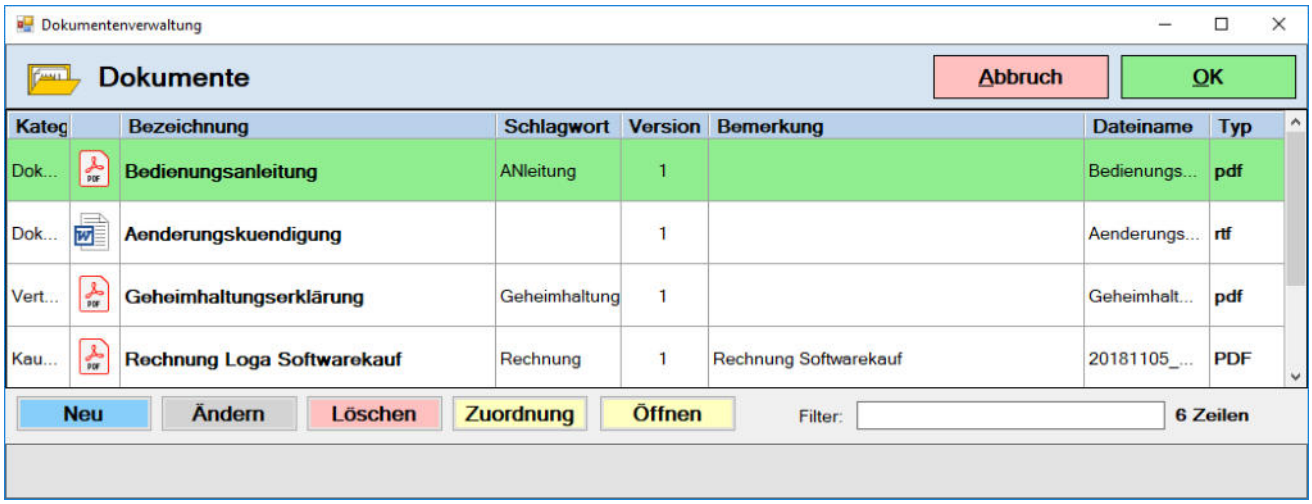
Das nachfolgende Bild zeigt die Darstellung der Vertragsdaten aus dem Überwachungsmodus heraus:



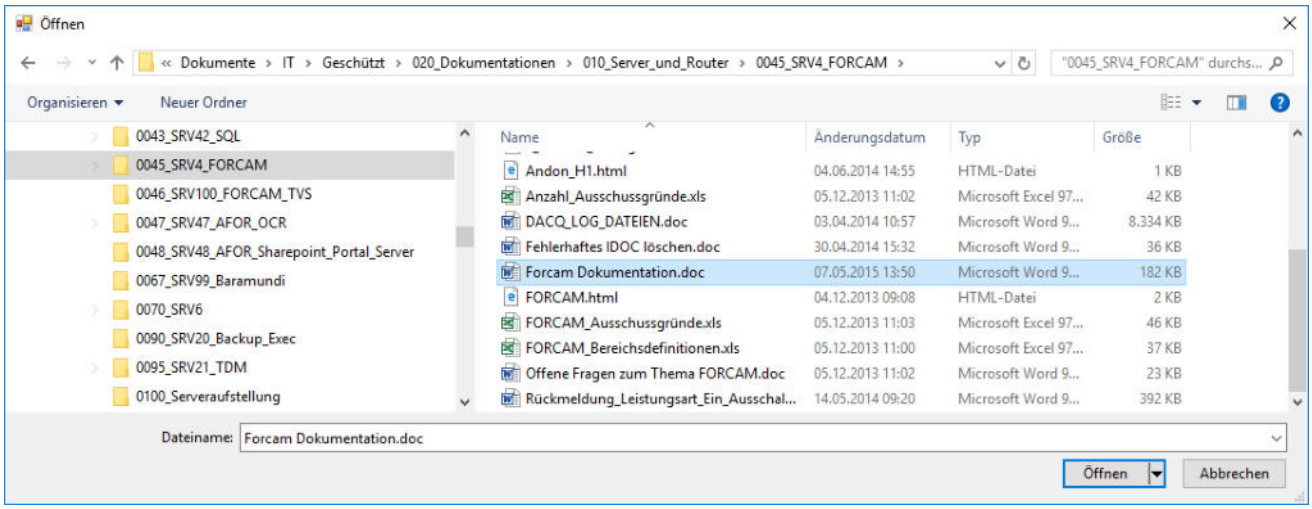
Der Slider im oberen Bereich zeigt alle zur Node zugeordneten Verträge. Durch klicken auf die Vertragsnummer wenden die Vertragsdaten angezeigt.

Dokumentenverwaltung

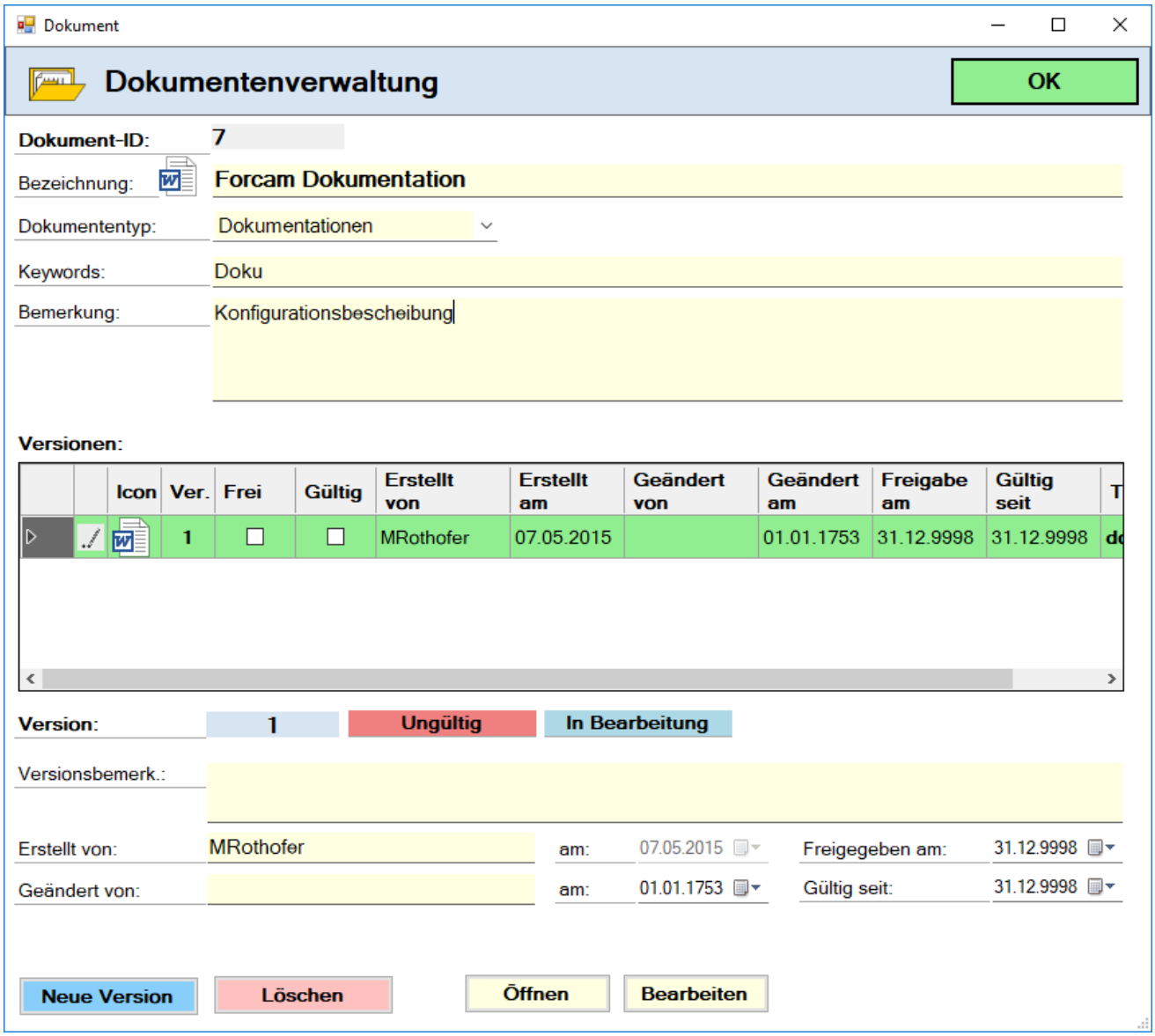
Neben der Überwachung von Systemen ist auch die Verwaltung von zugehörigen Dokumentationen ein wichtiger Bestandteil beim Ausfall von Systemen. Das schnelle Auffinden von wichtigen Dokumenten wie Notfallwiederherstellung, Supportverträge, Notfallansprechpartner etc. kann den Stress und die Ausfalldauer möglicherweise etwas reduzieren. Für diese Fälle wurde in node***WATCH*** eine mini Dokumentenverwaltung implementiert.



Um ein neues Dokument hinzuzufügen klicken Sie auf die Schaltfläche **[Neu]** und es erscheint der Datei öffnen Dialog.



Wählen Sie ein Dokument aus und bestätigen Sie es mit öffnen.



Die Felder haben folgende Bedeutung:

Dokumenten-ID: Eindeutige Nummer des Dokuments

Bezeichnung: Aussagekräftiger Name für das Dokument

Keywords Suchbegriffe

Bemerkung Anmerkungen zum Dokument

Versionen

Im Abschnitt Versionen wird der Lebenszyklus eines Dokuments angezeigt. Sind mehrere Versionen eines Dokuments vorhanden, dann können diese durch selektieren und betätigen des Buttons öffnen jederzeit angezeigt werden.

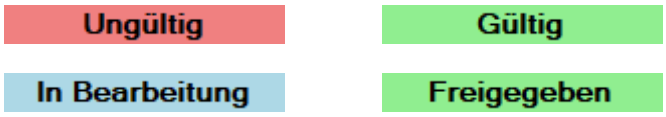
Die erste Spalte in der Versionstabelle zeigt den Freigabestatus des Dokuments. Die Symbole haben folgende Bedeutung:

 Das Dokument im Bearbeitungsmodus

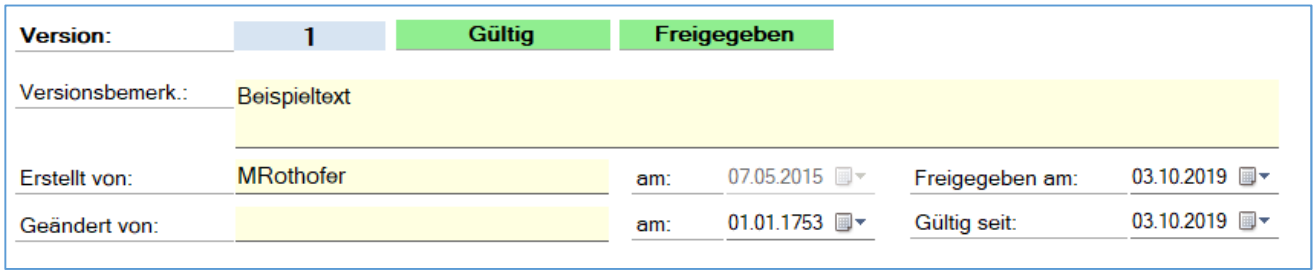
 Das Dokument ist aktuell freigegeben und auch gültig

 Das Dokument ist freigegeben, aber nicht gültig

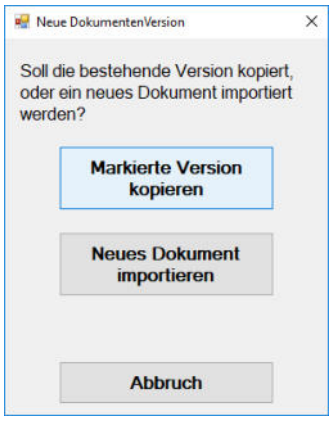
Es kann immer nur jeweils eine Version gültig sein. Durch Klick auf die folgenden Symbole kann zwischen den Statis gewechselt werden.



Unterhalb der Versionstabelle werden die Details zur selektierten Version angezeigt.

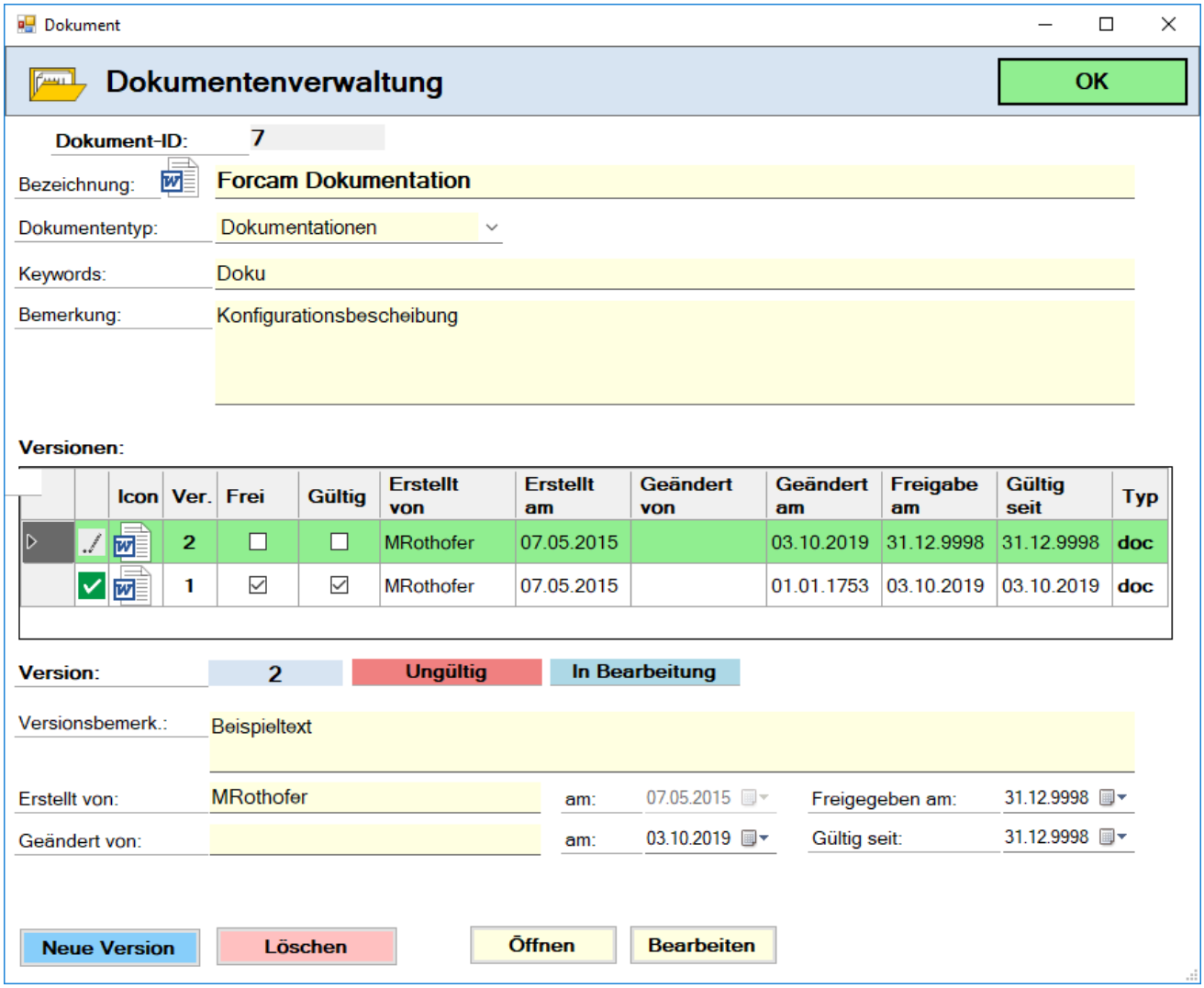


Über die Schaltfläche **[Neue Version]** kann eine neue Dokumentenversion eingefügt bzw. auch erstellt werden. Es erscheint folgende Meldung:



[Markierte Version kopieren] Erstellt eine Kopie von der zuvor ausgewählten Version und setzt diese in den Bearbeitungsmodus und den erklärt sie als ungültig.

[Neues Dokument importieren] Öffnet den Datei öffnen Dialog zum Hinzufügen eines neuen Dokuments. Die neue Version wird auch herbei wieder in den Bearbeitungsmodus versetz und als ungültig erklärt.



Nachfolgend die Schaltflächenbeschreibung:

[Löschen] Löscht die letzte Version. Achtung: Es kann immer nur die letzte Version gelöscht werden. Sollen alle Versionen entfernt werden, dann müssen Sie diese von der jüngsten zur ältesten Version der Reihe nach löschen.

[Öffnen] Öffnet die markierte Version im Lesemodus

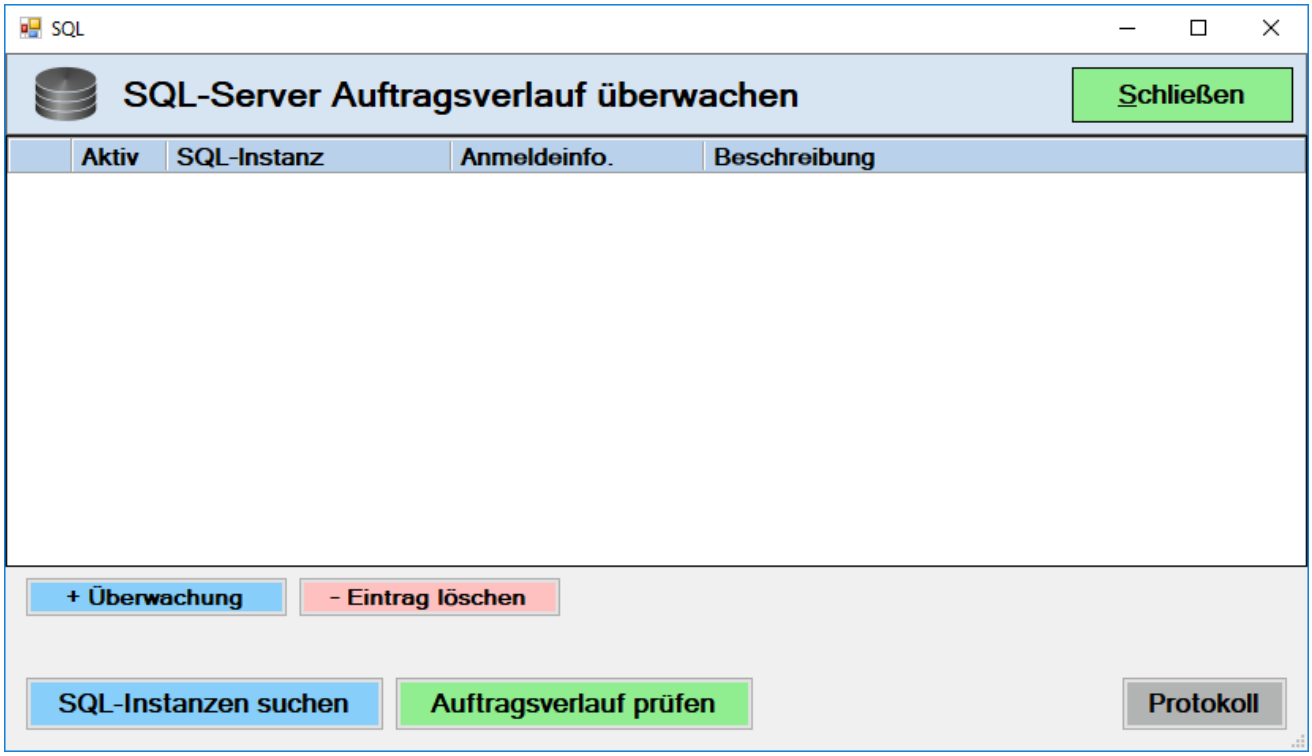
[Bearbeiten] Öffnet die markierte Version im Änderungsmodus

SQL-Auftragsverlauf

Als weitere Überwachungsmöglichkeit kann die Überwachung des MS-SQL-Server Auftragsverlaufs eingerichtet werden. Der Aufruf erfolgt wie immer über das Hauptmenü. Durch Klick auf die Schaltfläche **SQL-Server Auftragsverlauf** gelangt man in die Konfigurationsoberfläche. Die Konfiguration der Überwachung setzt ausreichend Zugriffsrechte auf die zu überwachenden SQL-Server voraus. Die Benutzer benötigen Lesezugriff auf die **msdb**-Datenbank des SQL-Servers. Spezifische Anmeldeinformationen können wie unter **Authentifizierung** beschrieben entsprechend vor der Konfiguration angelegt werden. Da bei der Einrichtung bereits ein Verbindungsversuch durchgeführt wird, ist es erforderlich, dass der bei Einrichtung der Überwachung hinterlegte Benutzer ausreichende Berechtigung besitz, ansonsten kann der Einrichtungsvorgang nicht durchgeführt werden.

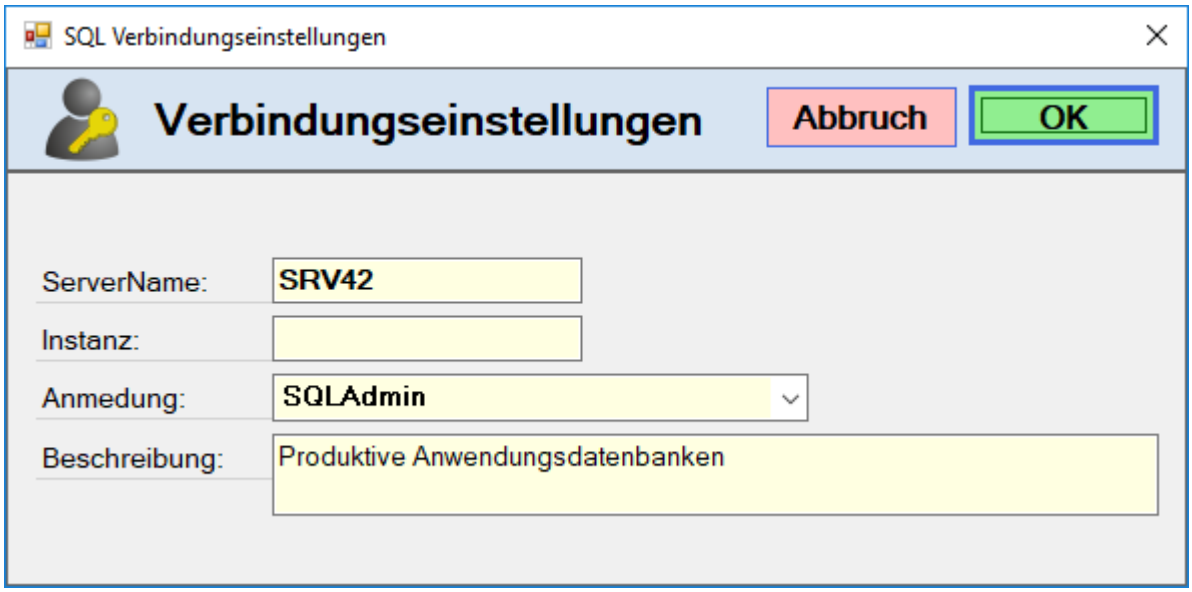
Manuelle Einrichtung von SQL-Überwachung

Die Einrichtung der Überwachung kann entweder durch Betätigung der Schaltfläche **[SQL-Instanzen suchen]** erfolgen, oder einzeln, durch Betätigung des Buttons **[+ Überwachung]**.

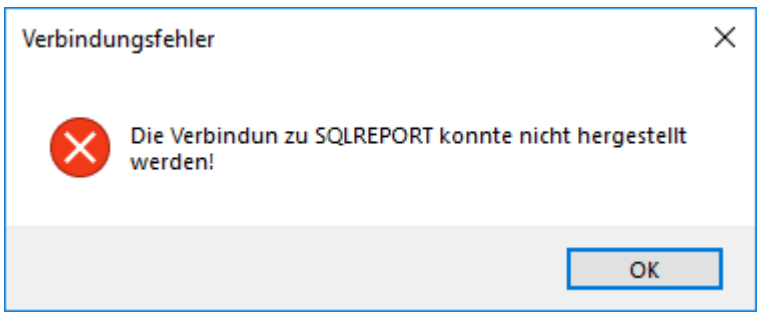


Die manuelle Einrichtung einer MS SQL-Server Überwachung erfolgt über die Schaltfläche **[+ Überwachung]**.

Es öffnet sich ein Fenster zur Eingabe der Verbindungseinstellungen.

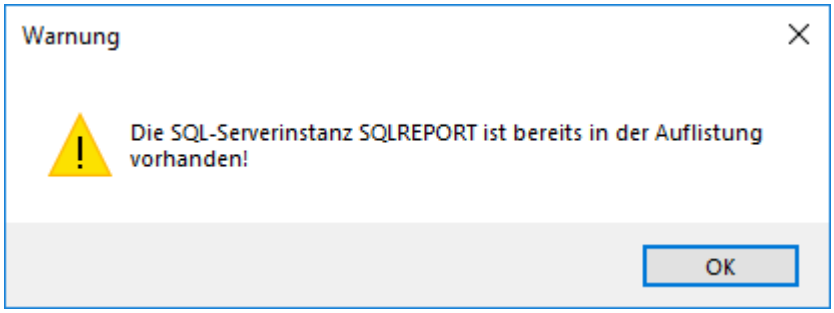


In das Feld **Servername** ist der Name Name oder die IP-Adresse des zu überwachenden SQL-Servers einzutragen. Bei instanzierten Installationen ist im Feld **Instanz** zusätzlich der Instanzname der SQL-Installation erforderlich, ansonsten bleibt das Feld leer. Unter **Anmeldung** werden die Anmeldeinformationen zugeordnet, mit denen die Überwachung durchgeführt werden soll.
Nach Betätigung von **[OK]** wird mit den eingegebenen Daten ein Verbindungsaufbau durchgeführt. Schlägt dieser fehl, dann erscheint folgende Meldung:

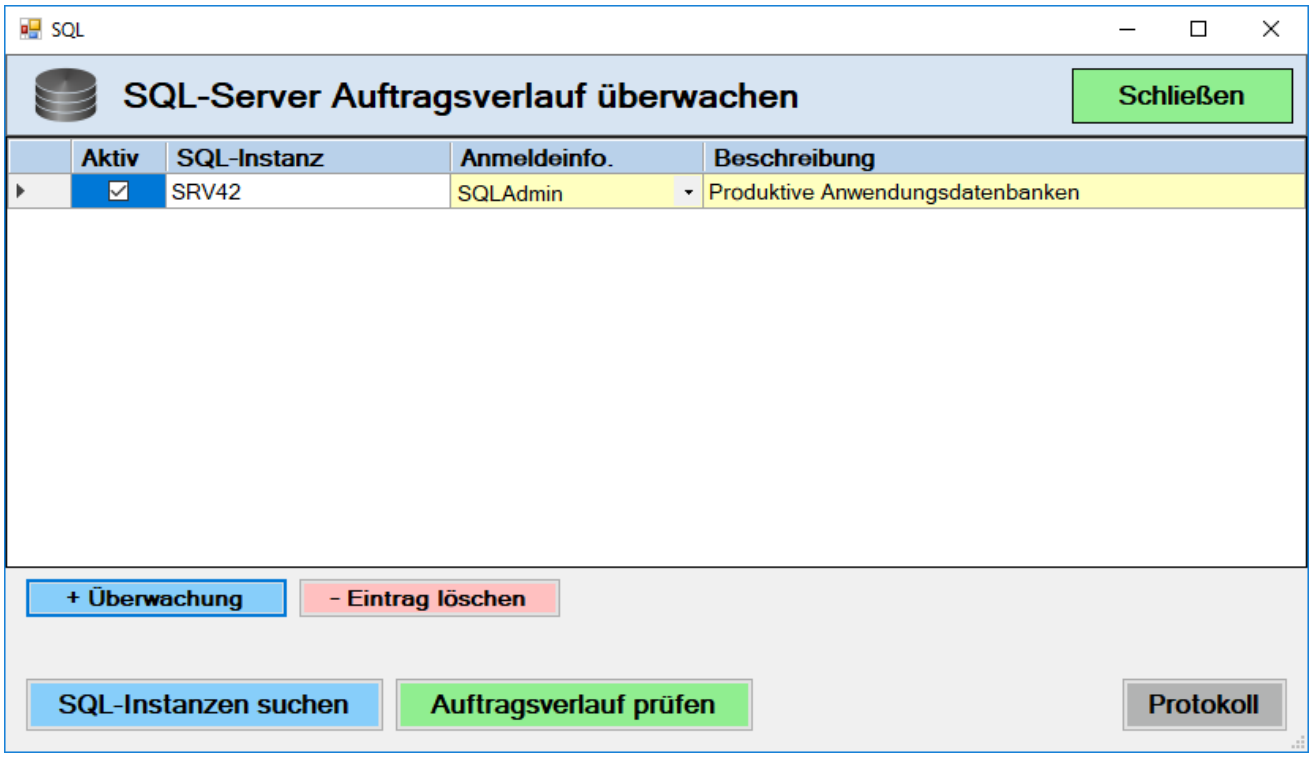


Nach Bestätigung des Fensters mit **[OK]** Erscheint wieder das Fenster mit den Verbindungseinstellungen. Hat man vergessen zuvor im Bereich Authentifizierung gültige Anmeldeinformationen zu hinterlegen, dann muss man den Vorgang abbrechen und zuerst die Anmeldeinformationen, wie unter **Authentifizierung** beschrieben, hinterlegen.

Sind die eingegebenen Informationen gültig, aber es befindet sich bereits ein Eintrag mit derselben Instanz in der Auflistung, dann erscheint folgende Fehlermeldung:



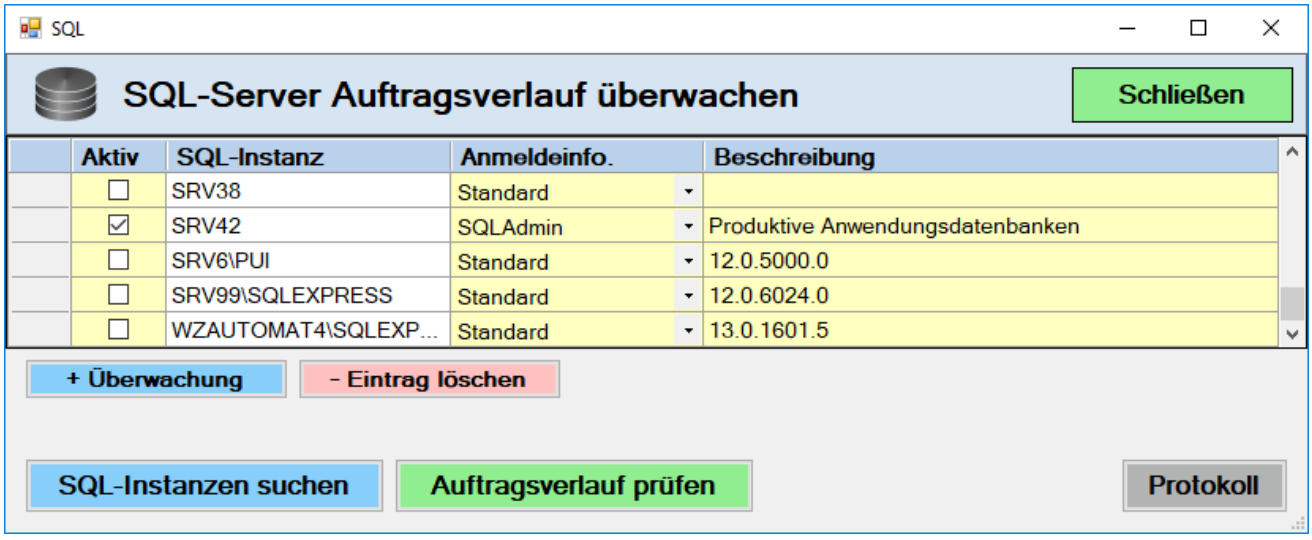
Die Übernahme der Daten ist in diesem Fall ebenfalls nicht möglich!
Ist ein Verbindungsaufbau mit den eingegebenen Daten möglich und befindet sich der Eintrag noch nicht in der Liste, dann werden die neuen Überwachungseinstellungen übernommen.



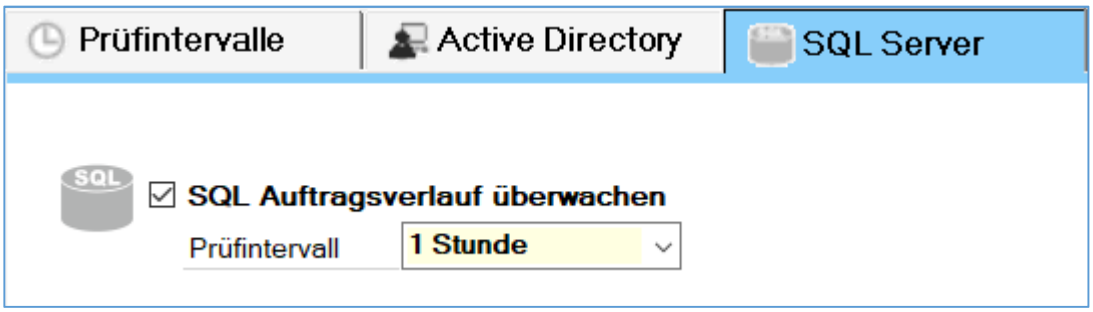
Automatische Suche von SQL-Instanzen

Wird **[SQL-Instanzen suchen]** betätigt, dann durchsucht node***WATCH*** das Netzwerk nach *MS SQL-Server* Installationen und listet alle gefundenen Instanzen auf. Bei allen über **[SQL-Instanzen suchen]** gefnundene Einträgen ist das Feld **Aktiv** deaktiviert. Die gewünschten Einträge können nun bei Bedarf auf Aktiv gesetzt werden. Da bei der Suche auch keine Überprüfung der Anmeldeinfomationen erfolgt, müssen diese noch überprüft und ggf. angepasst werden. Nicht benötigte Instanzen können entweder wieder aus der Liste gelöscht, oder durch deaktivieren über die Spalte **Aktiv** von der Überwachung ausgeschlossen werden.

Nachfolgendes Bild zeigt eine Darstellung nach einer automatischen Suche von SQL-Instanzen:



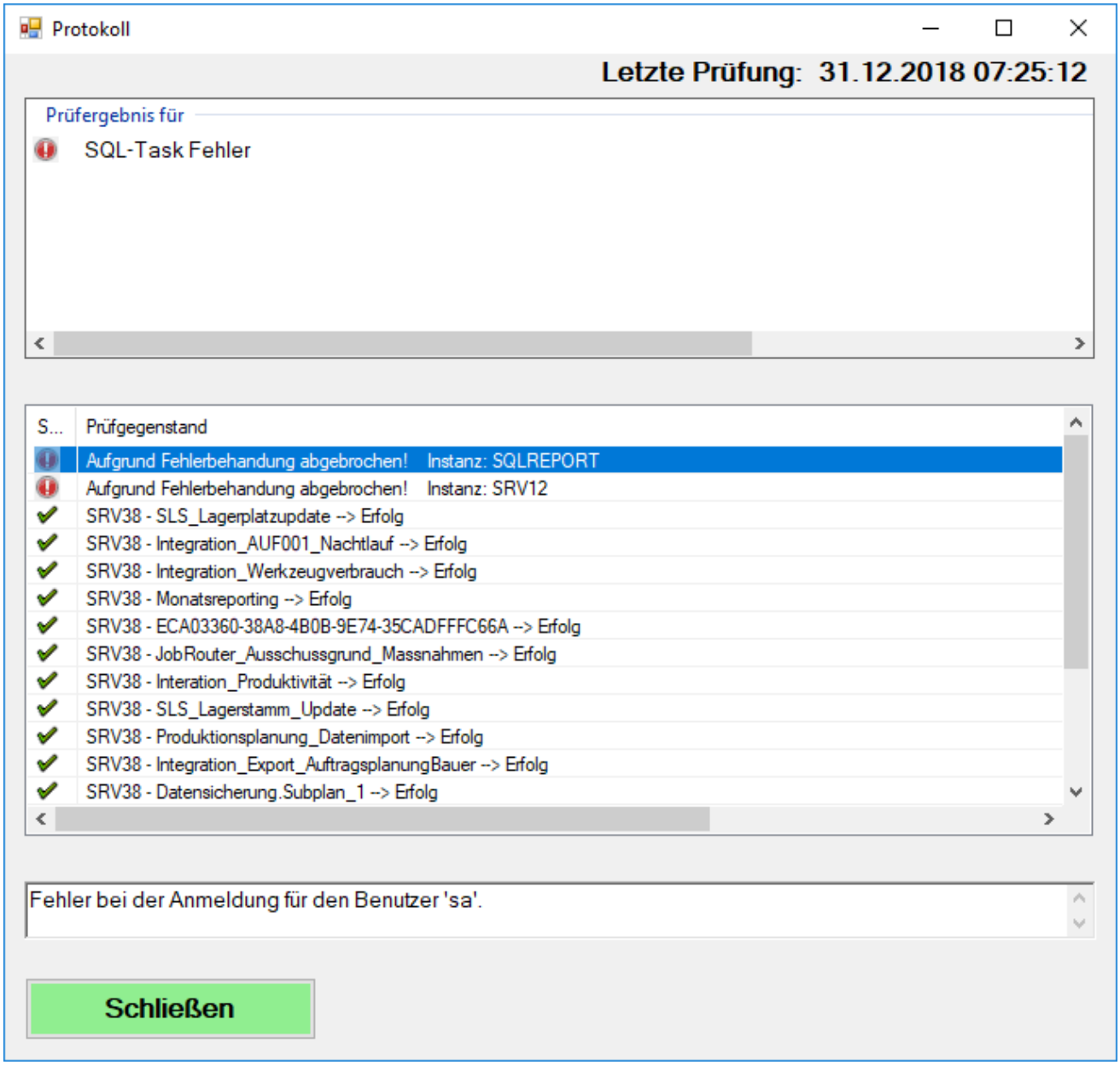
Die zentrale Aktivierung der Überwachung erfolgt über die Grundseinstellungen im Register **|SQL-Server|**



Der Prüfintervall sollte hierbei nicht zu kurz eingestellt werden!

Manuelle Überprüfung des Auftragsverlaufs

Für alle in der Auflistung als **Aktiv** gekennzeichneten Instanzen kann durch Betätigung von **[Auftragsverlauf pürfen]** ein Überwachungstest durchgeführt werden. Nach Betätigung der Schaltfläche **[Protokoll]** wird das Ergebnis der Prüfung angezeigt.

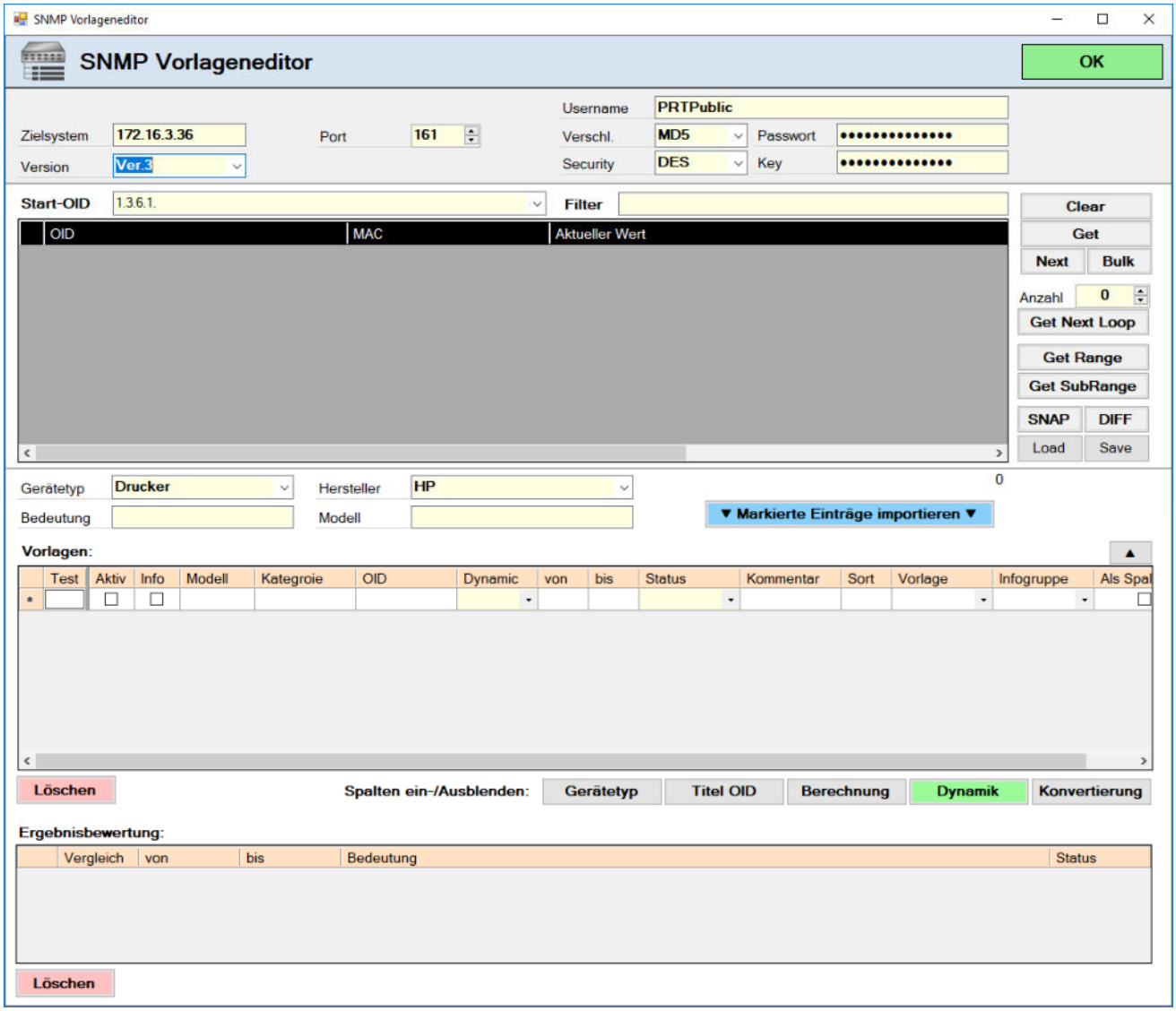


Durch Klick auf die Fehlerzeile erhält man im unteren Bereich detaillierte Fehlerinformationen. Im Überwachungsmodus wird je Fehlerzeile im Bereich Prüfgegestand der Fehlerzähler um eins erhöht und die Anzahl der Fehler im SQL-Icon angezeigt.

SNMP Vorlageneditor

Der SNMP Vorlageneditor ermöglicht das Auslesen von SNMP Endgeräten und recherchieren des Inhalts mittels eines Suchfilters. Es ist auch möglich Differenzabbilder der SNMP-Werte zu erstellen. Hierfür liest man zuerst einen gewünschten OID-Zweig ein und sichert, wenn gewünscht das Abbild für die spätere Verwendung. Tritt nun ein bestimmtes Ereignis auf dem Endgerät auf, dann kann man die zuvor gespeicherten Werte wieder von der Datei laden und ein Differenzabbild zum Endgerät erstellen. Hat man nun die gesuchten Werte gefunden, können Sie einfach als Vorlage importiert werden.

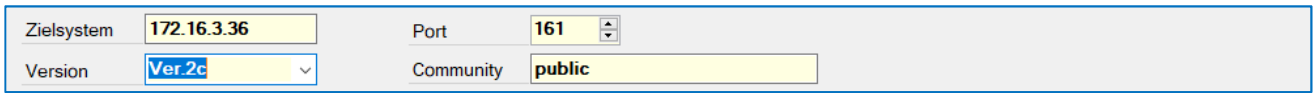
Das nachfolgende Bild zeigt den Vorlageneditor:



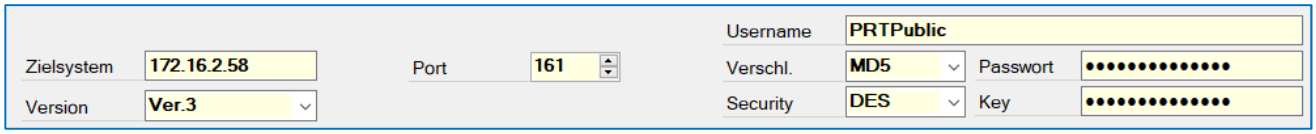
Zum Erstellen einer Vorlage müssen im oberen Bereich zuerst die Verbindungseinstellungen eingetragen werden. Hierzu zählen Endgerät, Portnummer, SNMP Version und abhängig von der Version die Community bzw. Benutzername und Verschlüsselungseinstellungen.

Abhängig von der Version wird neben dem Zielsystem für Version 1 und Version 2c die Community mit angezeigt. Wählt man Version 3, dann wird die Community ausgeblendet und stattdessen der Username und die Verschlüsselungseinstellungen eingeblendet. Die erforderlichen Einstellungen sind von der Konfiguration des Endgerätes abhängig.

Anzeige der Version 1 und 2c



Anzeige der Version 3:



Nachdem die Verbindungseinstellungen gesetzt worden sind, kann mit der Suche nach Werten begonnen werden. Im Feld Start-OID kann entweder eine komplette OID eingegeben werden, soweit diese bekannt ist, aber auch nur ein Teilbereich. Der Voreingestellte OID Teilbereich stellt quasi den Startbereich für unsere Analyse dar.

Die Rechts angeordneten Bottons haben folgende Bedeutung:

[Clear] Entfernt alle Einträge aus dem Ergebnisfenster und leert den Speicher mit der zuletzt gemerkten OID (wird für **[Next]** benötigt).

[Get] Sucht nach der im Feld Start-OID eingetragenen OID. Achtung. Die OID muss im vorhanden sein und exakt übereinstummen.

[Next]

Sucht die OID, die der im Start-OID eingegebenen Wert folgt. Somit kann auch nach OIDs gesucht werden, wenn nur die Startsequenz der OID bekannt ist. Nach Betätigung von Next merkt sich das System den die zuletzt gefundene OID und setzt nach erneuter Betätigung von Next die Suche ab der letzten OID fort. Clear entfernt auch die gemerkte OID, so dass mit der Suche wieder von vorne begonnen werden kann.

[Bulk]

Wenn es sich bei der OID um einen Tabellenbereich handelt, dann wird die gesamte Tabelle eingelesen

[Get Next Loop]

Die Im Feld Anzahl kann eingetragen werden wie viele Werte nacheinander mit Next ausgelesen werden sollen. Die hier voreingestellte Anzahl an OIDs wird dann nacheinander ausgelesen und im Ergebnisbereich angezeigt. Bei Anzahl 10 würde das in etwa so aussehen:

OID	MAC	Aktueller Wert	Dezimalstring	Datentyp	TypID	isHex
1.3.6.1.2.1.1.1.0	01 02 01 01 01 00	UTAX_TA Printing System		OctetString	4	☐
1.3.6.1.2.1.1.2.0	01 02 01 01 02 00	1.3.6.1.4.1.1347.41		ObjectId	6	☐
1.3.6.1.2.1.1.3.0	01 02 01 01 03 00	129d 23h 1m 25s 630ms		TimeTicks	67	☐
1.3.6.1.2.1.1.4.0	01 02 01 01 04 00			OctetString	4	☐
1.3.6.1.2.1.1.5.0	01 02 01 01 05 00			OctetString	4	☐
1.3.6.1.2.1.1.6.0	01 02 01 01 06 00	Buero IT		OctetString	4	☐
1.3.6.1.2.1.1.7.0	01 02 01 01 07 00	12		Integer32	2	☐
1.3.6.1.2.1.2.1.0	01 02 01 02 01 00	1		Integer32	2	☐
1.3.6.1.2.1.2.2.1.1.1	01 02 02 01 01 01	1		Integer32	2	☐

Wird als Anzahl 0 eingetragen, dann wird bis zum Ende der eingegebenen Startsequenz gelesen, also solange bis die Start-OID nicht mehr mit dem vorderen Teil der ausgelesenen OID übereinstimmt.

[Get Range]

Hier muss eine exakte OID eingegeben werden. In unserem Beispiel wollen wir den Seitenzählerstand eines Druckers ermitteln. Die Zugehörige OID startet bei **1.3.6.1.4.1.1347.42.2.1.1.1.6.1** und endet bei 1.3.6.1.4.1.1347.42.2.1.1.1.6.9
Als Start-OID wird 1.3.6.1.4.1.1347.42.2.1.1.1.6.1 eingetragen als Ergebnis werden alle OIDs eingelesen, die mit **1.3.6.1.4.1.1347.42.2.1.1.1.6.** beginnen. Lediglich die letzte Stelle der OID darf sich ändern. In unserm Beispiel wird folgendes Ergebnis angezeigt:

OID △	MAC	Aktueller Wert	Dezimalstring	Datentyp	TypID	isHex
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.1	01 01 01 06 01 01	4465		Integer32	2	☐
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.2	01 01 01 06 01 02	0		Integer32	2	☐
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.3	01 01 01 06 01 03	8		Integer32	2	☐
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.4	01 01 01 06 01 04	0		Integer32	2	☐
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.5	01 01 01 06 01 05	0		Integer32	2	☐
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.6	01 01 01 06 01 06	0		Integer32	2	☐
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.7	01 01 01 06 01 07	0		Integer32	2	☐
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.8	01 01 01 06 01 08	0		Integer32	2	☐
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.9	01 01 01 06 01 09	0		Integer32	2	☐

[Get Subrange] Im Gegensatz zu Range ermittelt Subrange auch weitere Unterstrukturen. Es werden also zur Teil-OID alle mit der Teil-OID übereinstimmenden OIDs ausgelesen. Im Falle unseres zuvor eingelesenen Seitenzählerstands ist das sinnvoll, da wir zwar den Zählerstand wissen, nicht aber welches Papierformat der Zähler repräsentiert. Wir verwenden also die zuvor eingegebene OID und kürzen sie um die letzte Stelle und tragen somit **1.3.6.1.4.1.1347.42.2.1.1.1**. als Start-OID ein. Das Ergebnis sieht dann folgendermaßen aus:

OID	MAC	Aktueller Wert	Dezimalstring	Datentyp	TypID	isHex
1.3.6.1.4.1.1347.42.2.1.1.1.2.1.1	01 01 01 02 01 01	A4		OctetString	4	☐
1.3.6.1.4.1.1347.42.2.1.1.1.2.1.2	01 01 01 02 01 02	B5		OctetString	4	☐
1.3.6.1.4.1.1347.42.2.1.1.1.2.1.3	01 01 01 02 01 03	A5		OctetString	4	☐
1.3.6.1.4.1.1347.42.2.1.1.1.2.1.4	01 01 01 02 01 04	Folio		OctetString	4	☐
1.3.6.1.4.1.1347.42.2.1.1.1.2.1.5	01 01 01 02 01 05	Legal		OctetString	4	☐
1.3.6.1.4.1.1347.42.2.1.1.1.2.1.6	01 01 01 02 01 06	Letter		OctetString	4	☐
1.3.6.1.4.1.1347.42.2.1.1.1.2.1.7	01 01 01 02 01 07	Statement		OctetString	4	☐
1.3.6.1.4.1.1347.42.2.1.1.1.2.1.8	01 01 01 02 01 08	Other1		OctetString	4	☐
1.3.6.1.4.1.1347.42.2.1.1.1.2.1.9	01 01 01 02 01 09	Other2		OctetString	4	☐
1.3.6.1.4.1.1347.42.2.1.1.1.3.1.1	01 01 01 03 01 01	3		Integer32	2	☐

1.3.6.1.4.1.1347.42.2.1.1.1.**2**.1.1 ist also das Seitenformat A4
1.3.6.1.4.1.1347.42.2.1.1.1.**6**.1.1 der zugehörige Zählerstand A4
Es fällt auf, dass sich in unserem Fall zusammengehörige Werte unterhalb einer gemeinsamen OID Startsequenz befinden in unserem Fall
1.3.6.1.4.1.1347.42.2.1.1.1.
Der Seitenzähler für A5 ist analog in den nachfolgenden OIDs vorhanden
1.3.6.1.4.1.1347.42.2.1.1.1.**2**.1.3 ist also das Seitenformat A4
1.3.6.1.4.1.1347.42.2.1.1.1.**6**.1.3 der zugehörige Zählerstand A4
2 enthält also die Überschriften, **6** den Zählerstand.
Wie Sie sehen kann man mit dem Werkzeug einfach in die SNMP-Werte eines Gerätes auslesen und analysieren.

[Snap] Arbeitet wie SubRange, aber merkt sich die eingelesenen Daten um später mit DIFF einen Differenzabgleich machen zu können.

[Diff] Erstellt zum zuvor gemachten Schnappschuss eine Differenztabelle und zeigt die Unterschiede um Ergebnisbereich an.

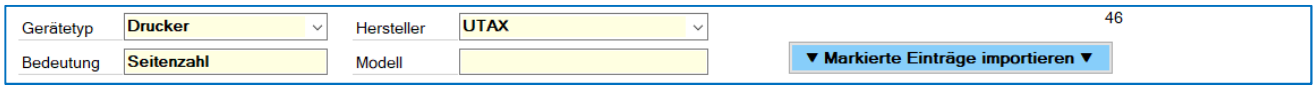
[Load] Sichert den zuvor über SNAP erstellten Schnappschuss in einer Datei für die spätere Erstellung eines Differenzabgleichs.

[Save] Lädt einen gespeicherten Schnappschuss in den SNAP-Puffer um anschließend einen Differenzabgleich erstellen zu können

Über das Filterfeld kann der Ergebnisbereich bequem nach Werten durchsucht werden. Die Spalte MAC im Ergebnisbereich stellt die letzten 6 Werte der OID im Hexadezimalformat dar. Switche verwenden oft OID-Sequenzen die mit der Dezimal codierten MAC-Adresse eines Endgerätes enden. Dadurch ist es auch möglich OIDs nach möglichen MAC-Address Sequenzen zu durchsuchen.

Vorlage erstellen

Um nun die gefundenen OID-Sequenzen wieder verwenden zu können müssen diese im Ergebnisbereich lediglich markiert und über die Schaltfläche **[Markierte Einträge importieren]** in den Vorlagenbereich eingefügt werden. Zuvor sollten aber noch der Gerätetyp und Hersteller, sowie die Bedeutung des einzufügenden Wertes eingetragen werden. Man will ja später auch wissen, welchem Gerät die Vorlage zugewiesen werden kann und was da denn nun ausgelesen wird.



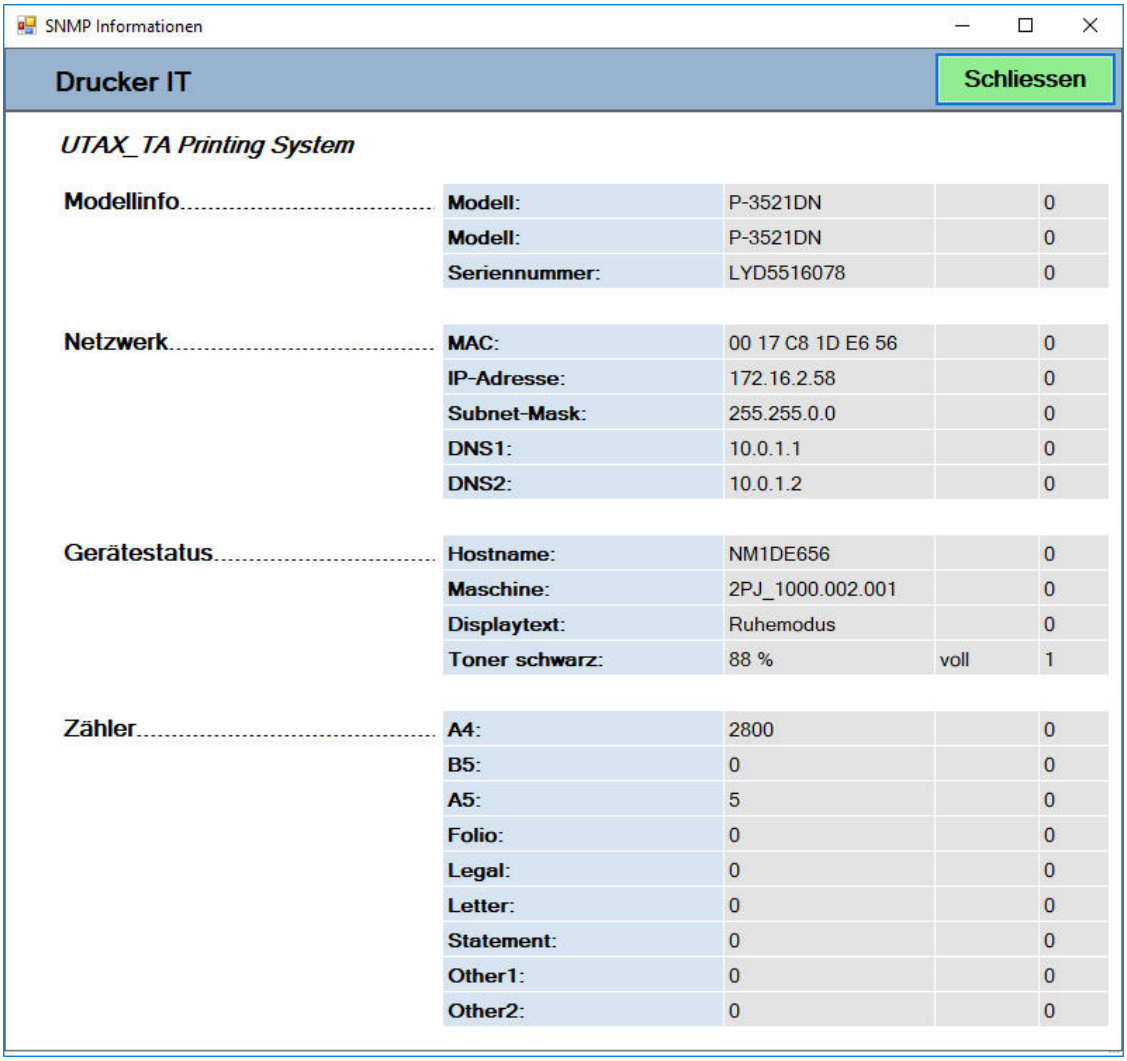
Im Vorlagenbereich stehen nun umfangreiche Möglichkeiten zur Optimierung der Abfragen zur Verfügung. Die einzelnen Felder haben folgende Bedeutung.

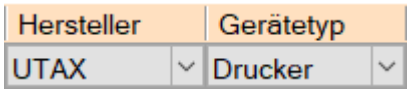
Test Über den Button in der **Test**-Spalte kann die Abfrage getestet werden. Bei Betätigung werden die Ergebnisse des Tests angezeigt und die Schaltfläche färbt sich grün.

Aktiv Bedeutet, dass die Abfrage aktiviert ist, wenn Sie einem Gerät zugeordnet wird. Es ist möglich, mehrere Vorlagen einem Gerät zuzuordnen und später einfach einzelne Werte wieder zu deaktivieren, ohne dass die Einträge gelöscht werden müssen

Info Im Überwachungsmodus werden nur kritische Einträge beobachtet. Will man zusätzliche Informationen wie Standort, Gerätebezeichnung … beim Abrufen der Geräteinformationen, gibt es die Möglichkeit diese SNMP-Einträge als Info-Einträge zu kennzeichnen. Es werden dann neben den Kritischen Werten auch diese zusätzlichen Werte mit abgefragt und angezeigt.
Es wird z.B. der Tonerstand eines Gerätes überwacht in der Infoanzeige soll aber zusätzlich das Gerätemodell, Standort und Firmware Release Stand mit angezeigt werden.

So könnte z.B. eine Abfrage aussehen:





Hersteller Hier wird der Hersteller, wie unter **Markierte Einträge importieren** voreingestellt, übernommen. Der Eintrag kann jederzeit geändert werden. Er wird lediglich zu Informationszwecken herangezogen und für die Vorlagenfilterung verwendet.

Gerätetyp Der Gerätetyp wird wie auch der Hersteller aus den Voreinstellungen **Markierte Einträge importieren** übernommen. Vorlagen können nach dem Gerätetyp gefiltert werden. Das erleichtert die Suche bei der Zuweisung der Überwachung zu einzelnen Geräten.

Modell	Bezeichnung	Kategroie
	Seitenzahl A4	Zähler

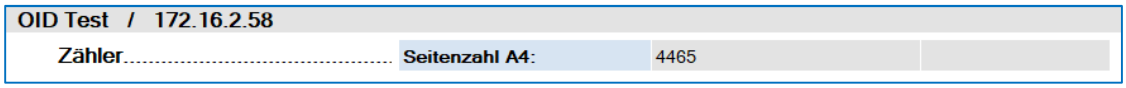
Modell Wenn es sich um einen Gerätemodellspezifischen SNMP-Wert handelt, kann hier die Modellbezeichnung des zu überwachenden Gerätes eingetragen werden.

Bezeichnung Sollte einen aussagekräftigen Begriff enthalten, was denn mit diesem SNMP-Eintrag ausgelesen wird. In unserm Beispiel ist es die Seitenzahl DIN A4. Der Wert wird bei Gruppierung entweder als Spaltenüberschrift, oder als Zeilenüberschrift angezeigt.

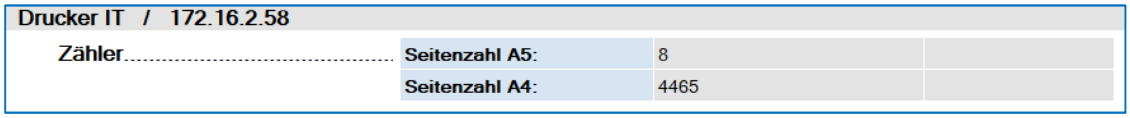
Kategorie Dieses Feld steht im Zusammenhang mit der Anzeige. Die Kategorie wird in der Anzeige links als Gruppenüberschrift aufgeführt.

OID
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.1

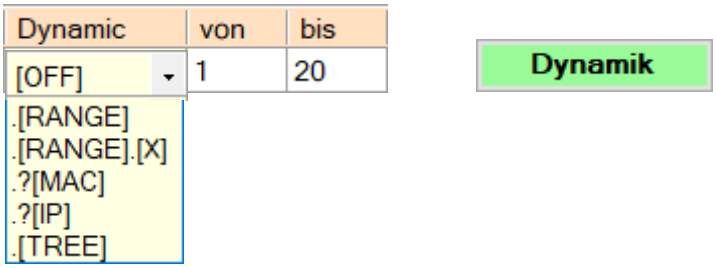
OID Ist nun der SNMP-Wert der abgefragt werden soll. Bei Dynamic = OFF muss dieser immer vollständig sein.



Hier sieht man schon, wo die Werte Kategorie und Bezeichnung angezeigt werden. Konfiguriert man nun einen zweiten Eintrag für DIN A5, dann sieht die Anzeige so aus:



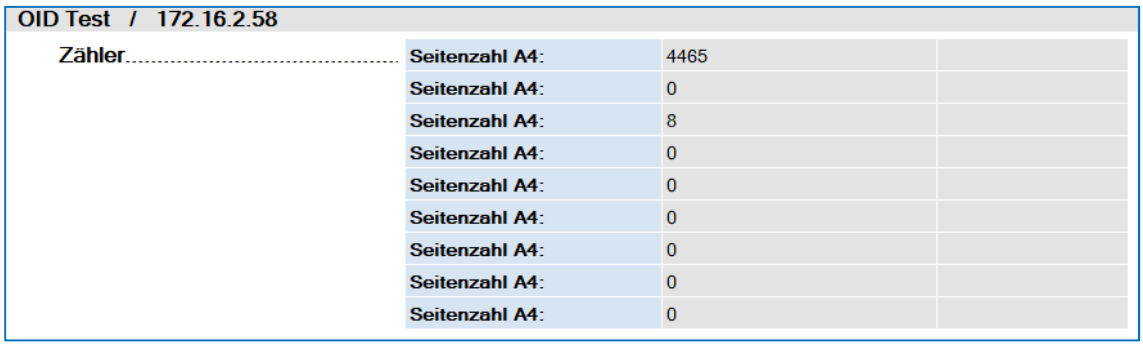
Hier sieht man, dass die Werte nach Kategorie zusammengefasst werden.



Dynamic Hier beginnt nun die Stärke dieses Tools. Da wir ja nicht wissen, wie viele Seitenformate ein Gerät unterstützt und wir die Vorlage für mehrere Gerätetypen verwenden wollen, stellen wir hier im Feld Dynamic den Wert einfach auf **[.RANGE]** um. Dadurch wird die letzte Stelle der OID durch eine Automatik ersetzt. Wir entfernen also die letzte 1 von unserer Seitenzähler OID, so dass der Automatismus diese stellen füllen kann. Der Bereich kann über die Felder von und bis weiter eingegrenzt werden, so dass die letzte Stelle maximal mit Werten von z.B. 1 bis 20 ersetzt wird.

OID	Dynamic	von	bis
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.	.[RANGE]	1	20

Das Ergebnis unserer Abfrage würde dann so aussehen:



Das nächste Problem, das nun sichtbar wird ist, dass nun jede Zeile mit Seitenzahl A4 beschriftet wurde. Wie wir weiter vorne gesehen haben, ist die Angabe des Seitenformats in einer anderen parallel verlaufenden OID abgelegt.
1.3.6.1.4.1.1347.42.2.1.1.1.**2**.1.1 ist also das Seitenformat A4
1.3.6.1.4.1.1347.42.2.1.1.1.**6**.1.1 der zugehörige Zählerstand A4
Da die OIDs am Ende parallel verlaufen, können wir die Beschriftung ebenfalls dynamisieren. Weitere Dynamisierungsfunktionen werden am Ende dieses Kapitels beschrieben.

Auswahl: .[Range].[X]
Während [Range] nur die letzte Zahl einer OID repräsentiert, also OID.X kann mit [Range].[X] eine größere Menge an Zahlen der OID automatisiert gelesen werden z.b.

OID.X.X oder OID.X.X.X. Der Lesevorgang endet, wenn sich der im Feld OID eingetragene Wert von der Startsequenz des gelesenen SMTP-Keys unterscheidet.

Auswahl: .[Tree]

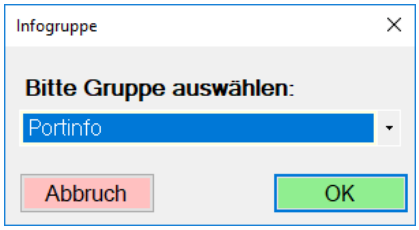
Bisher noch ohne Funktion.

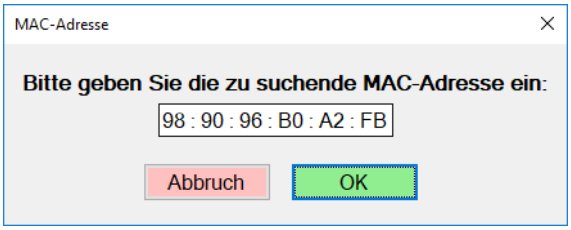
Auswahl: .?[MAC]

Diese Auswahl ist nur in Zusammenhang mit Infogruppen sinnvoll. .?[MAC] bedeutet, dass der im Feld OID eingetragene Objekt-Key um die Werte einer MAC-Adresse in Dezimal-Notation ergänzt wird. Will man dann diese OID lesen, erscheint zuerst ein Popup-Fenster, in dem eine MAC-Adresse eingetragen werden muss.
Diese MAC-Adresse wird dann in Dezimalschreibweise umgewandelt und an die eingetragene OID angehängt. Aus OID.?MAC wird bei Eingabe der MAC-Adresse 98 90 96 B0 A2 FB der Wert OID.152.144.150.176.162.251
Sinn und Zweck dieser Möglichkeit ist, dass im Bereich der Switche die OIDs dynamisch mit den MAC-Adressen der angeschlossenen Geräte generiert werden und hier z.B. Informationen abrufbar sind, an welchen Switch-Port eine bestimmte MAC-Adresse angeschlossen wurde.
Der Beispieleintrag würde folgendermaßen aussehen:

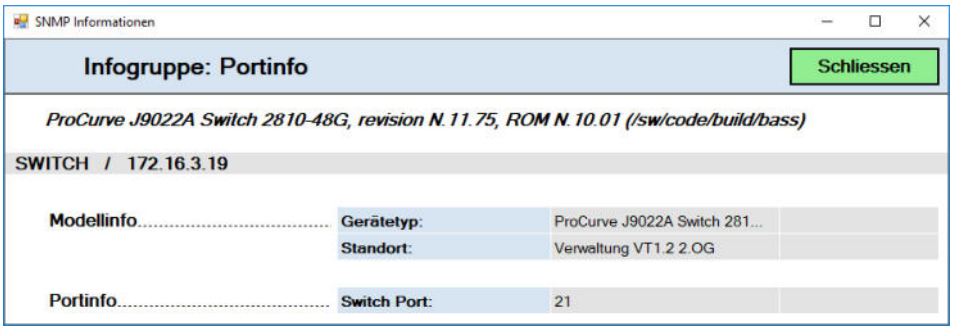
Kategroie	OID	Dynamic	Infogruppe
Portinfo	1.3.6.1.2.1.17.4.3.1.2	.?[MAC]	Portinfo

Beim Aufruf der Infogruppe aus der Überwachung heraus erscheinen folgende Fenster:





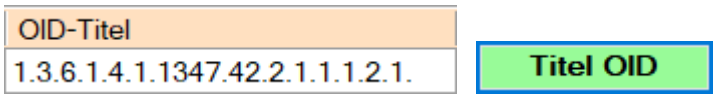
Es erscheint folgende Anzeige:



Das gesuchte Gerät steckt auf Port 21.

Auswahl: .?[IP]

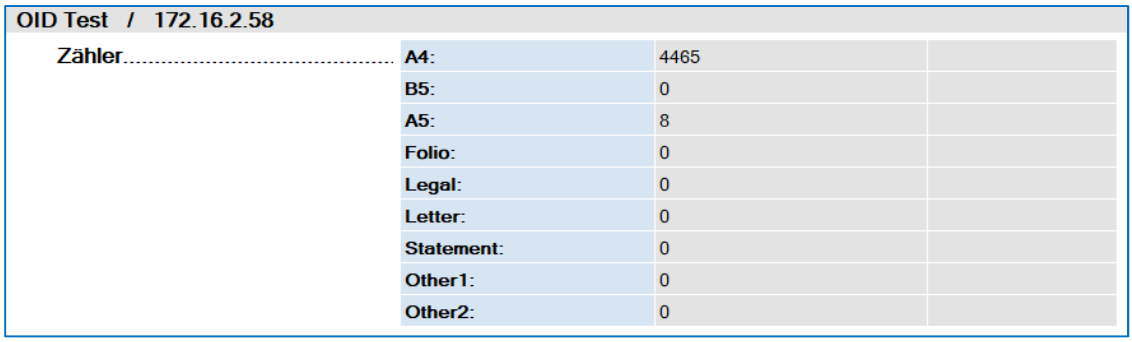
Funktioniert wie ?MAC, nur dass anstatt der MAC-Adresse die IP-Adresse an die IOD angehängt wird.



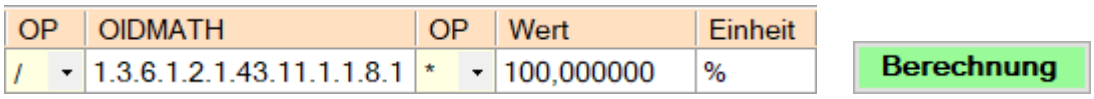
OID-Titel Im Titelfeld kann nun parallel zur Range eine OID eingetragen werden. In unserem Fall ist das die OID mit den Seitenformaten. Wir tragen also den Wert 1.3.6.1.4.1.1347.42.2.1.1.1.**2**.1 ein.

OID	Dynamic	von	bis	OID-Titel
1.3.6.1.4.1.1347.42.2.1.1.1.6.1.	.[RANGE]	1	20	1.3.6.1.4.1.1347.42.2.1.1.1.2.1.

Das Ergebnis für diese Zeile sieht nun folgendermaßen aus:



Ohne die Dynamik wären neun Einträge erforderlich gewesen, so war es nur einer.



OP Führt eine Operation mit dem ermittelten SNMP-Wert durch. Die Grundrechenarten stehen zur Verfügung.

OIDMATH Manchmal werden die gesuchten Werte nicht direkt als Ergebnis einer OID abgelegt. So speichert z.B. der Hersteller UTAX die Resttoneranzeige nicht in %, sondern legt hierzu zwei Werte ab.

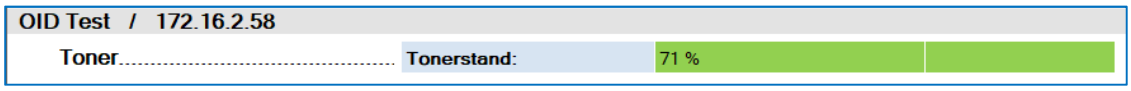
OID 1.3.6.1.2.1.43.11.1.1.**9**.1.1 enthält die Seitenanzahl, die noch gedruckt werden kann.

OID 1.3.6.1.2.1.43.11.1.1.**8**.1.1 enthält die Gesamtseitenzahl, die mit einem neuen Toner gedruckt werden kann

Um dieses Problem zu lösen, kann man nun sagen, dass der Wert aus OID 1.3.6.1.2.1.43.11.1.1.9.1.1 durch den Wert aus OID 1.3.6.1.2.1.43.11.1.1.8.1.1 dividiert werden soll. Über Operand 2 kann dann noch eine Multiplikation mit 100 durchgeführt.

OID	OP	OIDMATH	OP	Wert	Einheit
1.3.6.1.2.1.43.11.1.1.9.1.1	/	1.3.6.1.2.1.43.11.1.1.8.1.1	*	100,000000	%

Das Ergebnis würde dann so dargestellt:



Wert Ein Wert , mit dem aus dem Ergebnis der eingelesenen OID eine Grundrechenoperation durchgeführt wird.

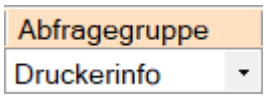
Einheit Die Einheit des ermittelten Wertes (Seiten, MBIT, % …)

Status
Good

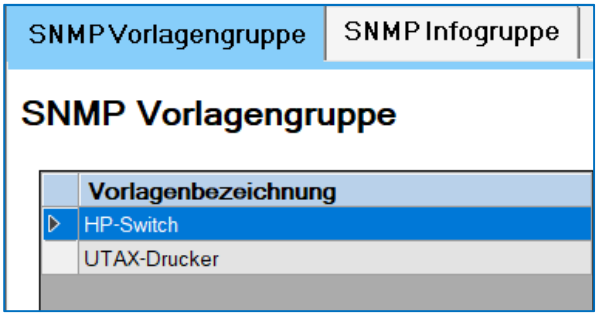
Status Hier kann der Überwachungsstatus eingestellt werden, das dem gefundenen Ergebnis vorab zugewiesen wird. Dieser Status kann durch die Tabelleneinträge in der Tabelle Ergebnisbedeutung überschrieben werden.
Nachfolgende Tabelle zeigt die Einträge der Ergebnisbedeutung:

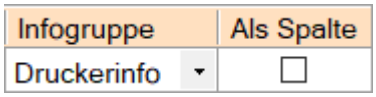
Vergleich	von	bis	Bedeutung	Status
>	30		voll	Good
between	10	30	mittel	Warning
<	10		Toner wechseln!	Error

Sind keine Ergebnisse definiert, dann zählt dann wird immer der übergeordnete Status ausgegeben.

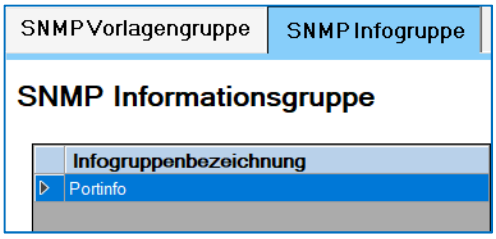


Vorlage SNMP-Abfragen können mittels Vorlagenbezeichnungen gruppiert werden. Später kann man dann durch markieren einer Vorlagenzeile die ganze Vorlagengruppe einem Gerät zuweisen. Der Vorteil liegt darin, dass vorlagen z.B. 20 Geräten zugeordnet werden können. Ändert man die zentrale Vorlage, dann ist diese Änderung in allen zugewiesenen Geräten aktiv.
Vorlagenbezeichnungen müssen zuvor in den Stammdaten hinterlegt werden.

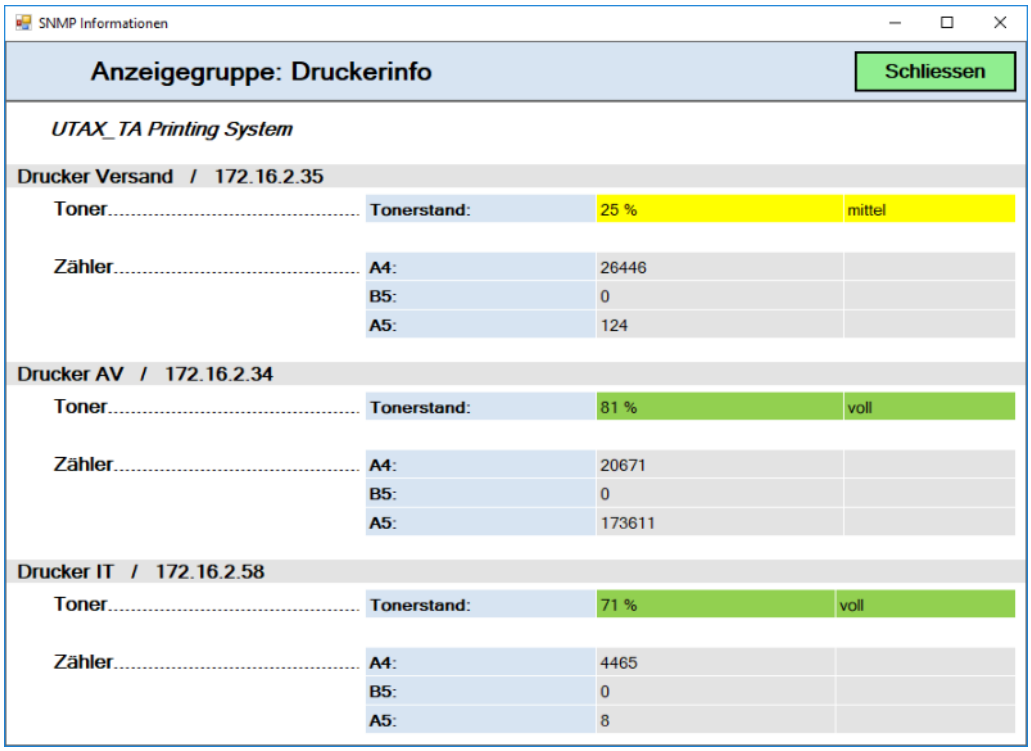




Infogruppe Ermöglicht im Überwachungsmodus Geräteübergreifende Informationen via SNMP abzufragen. Infogruppen müssen zuerst in den Stammdaten angelegt werden, damit Sie in der Auswahl Infogruppe zur Verfügung stehen.

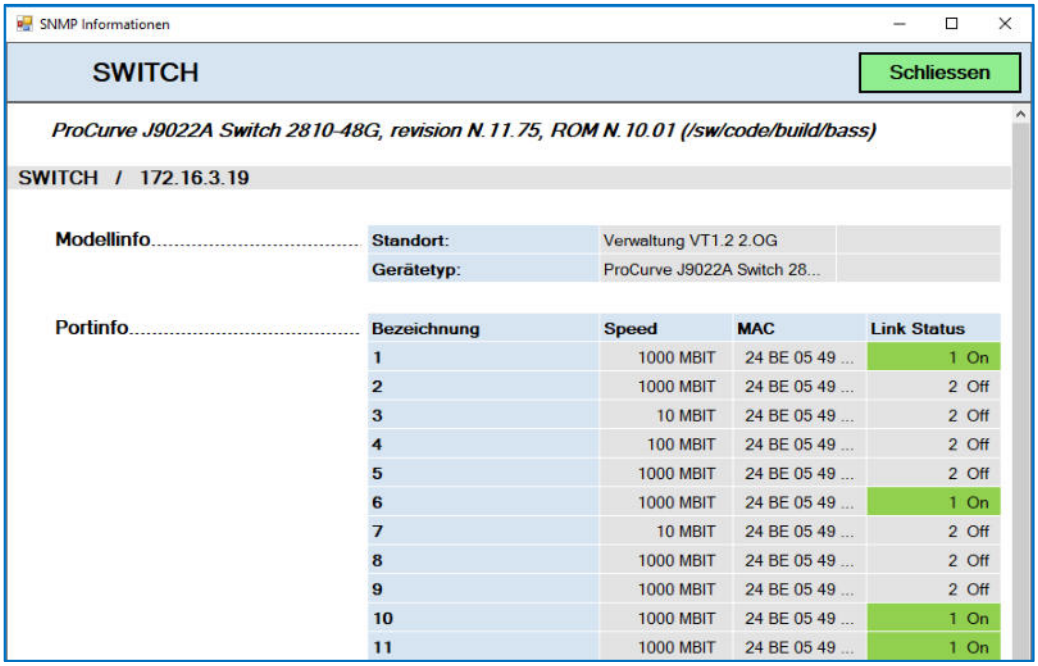


Wird z.B. der SNMP-Vorlage Tonerstand die Abfragegruppe Druckerinfo zugewiesen, dann wird im Überwachungsmodus beim Abruf der Abfragegruppe eine Übersicht aller Geräte und dessen Tonerstand angezeigt, denen dieser SNMP-Wert mit der klassifizierten Abfragegruppe Druckerinfo zugewiesen wurde. Diese Informationen werden auch Geräteübergreifend abgerufen. Fügen wir der zuvor für den Seitenzähler erstellten Regel ebenfalls die Infogruppe Druckerinfo zu und weisen diese drei Geräten zu, dann würde die Anzeige z.B. folgendermaßen aussehen:



Als Spalte

Über dieses Feld kann die Anzeige der Werte beeinflusst werden. Für Werte, die der gleichen Kategorie zugeordnet sind und die Als Spalte Option aktiviert haben, werden dann jeweils nebeneinander in einer eigenen Spalte angezeigt.



Sort
1

Sort Über das Sortierfeld kann die Reihenfolge der Dargestellten Werte in der Anzeige beeinflusst werden. Ist im vorherigen Beispiel in Modellinfo zuerst der Standort und dann die Gerätegruppe angezeigt worden, so kann durch vertauschen der Sortiernummer die Reihenfolge in der Anzeige getauscht werden.

Vorher

Modellinfo.....	Standort:	Verwaltung VT1.2 2.OG
	Gerätetyp:	ProCurve J9022A Switch 28...

Nachher

Modellinfo.....	Gerätetyp:	ProCurve J9022A Switch 281...
	Standort:	Verwaltung VT1.2 2.OG

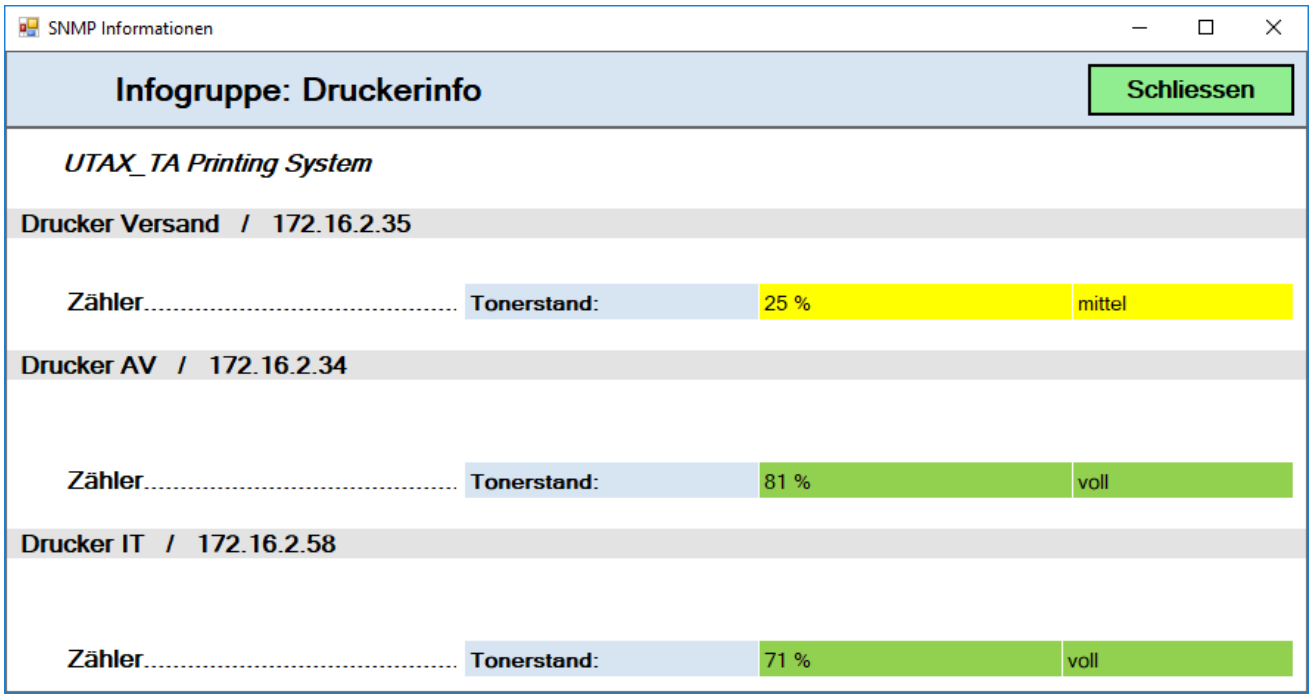
Ergebnisbewertung

Im unteren Bereich befindet sich der Abschnitt für die Ergebnisbewertung. Hier kann die Bedeutung des ermittelten SNMP-Werts eingestellt werden. Für unser Tonerstand Beispiel haben wir eingestellt, dass Werte Größer 30 % (wir haben in der OID den Prozentwert berechnet) als Gut dargestellt werden, zwischen 10 und 30 % wird eine Warnung ausgegeben und unter 10 Prozent ein Fehler.

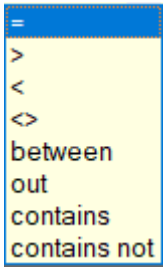
	Vergleich	von	bis	Bedeutung	Status
▶	>	30		voll	Good
	betwe...	10	30	mittel	Warning
	<	10		Toner wechseln!	Error
*					

Der Bedeutungstext wird bei Anzeige von SNMP-Informationen zusätzlich zum Wert dargestellt. Der Status nimmt Einfluss auf die Farbe sowohl in der Überwachung als auch in der Informationsübersicht der ermittelten Werte.

Nachfolgendes Fenster zeigt, die Auswirkung der Werte auf die Anzeige:



In der Spalte Vergleichswert stehen folgende Möglichkeiten zur Verfügung:

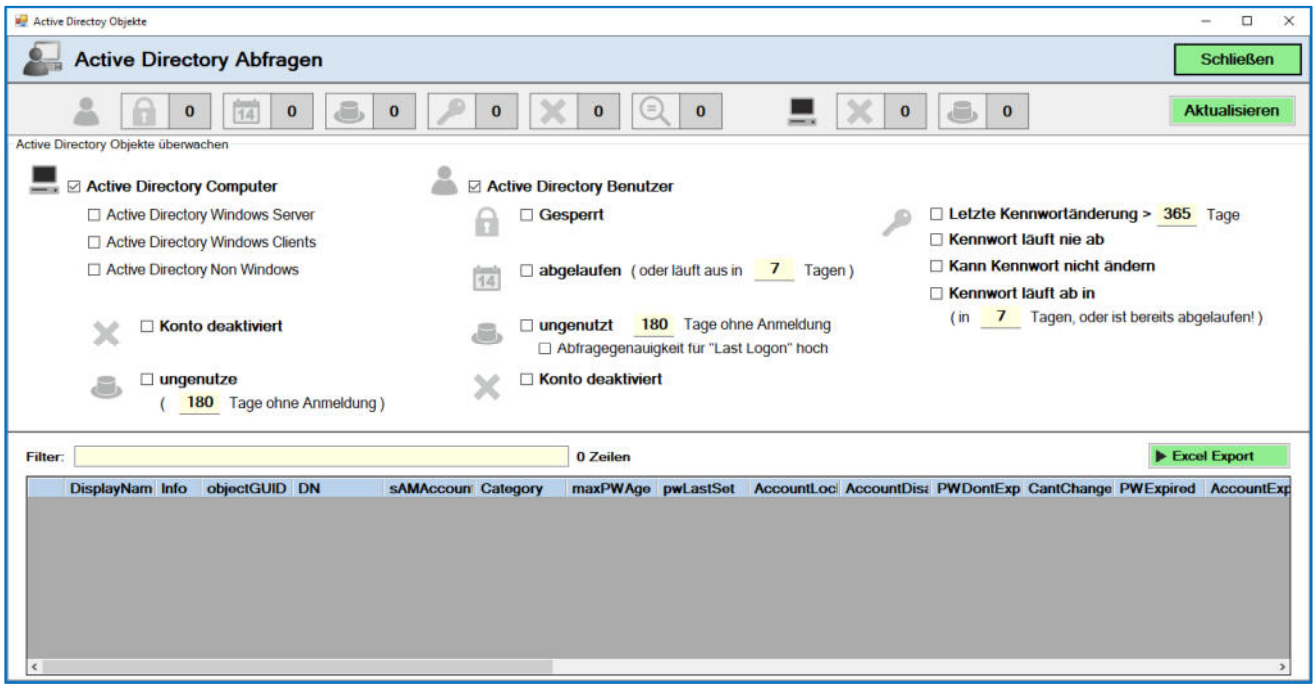


=	Der ermittelte Wert muss genau der Eingabe entsprechen
>	Der ermittelte Wert muss größer als die Eingabe sein
<	Der ermittelte Wert muss keiner als die Eingabe sein
<>	Der ermittelte Wert muss ungleich als die Eingabe sein
between	Der ermittelte Wert muss zwischen den Eingabewerten liegen
out	Der ermittelte Wert muss sich außerhalb der Eingabewerte befinden
contains	Der ermittelte Wert muss die eingegebene Zeichenfolge beinhalten
contains not	Der ermittelte Wert muss die eingegebene Zeichenfolge NICHT beinhalten

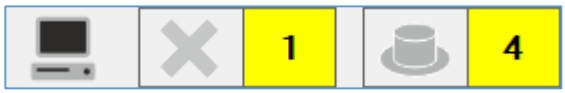
Active-Directory Benutzer & Computer

Die Überwachung von Netzwerkgeräten ist eine wichtige Aufgabe, die Überwachung von Active-Directory Einträgen aber ebenfalls. In node***WATCH*** wurde deshalb die Möglichkeit der Überwachung von Active-Directory Benutzer- Computer- und Gruppenobjekten integriert. Über die Jahre kann es oft vorkommen, dass im Active-Directory nicht mehr benötigte Benutzer- und Computerkonten vorhanden sind, da z.B. Computer getauscht, aber die Computerkonten nicht gelöscht wurden. Ebenso kann es sein, dass Administratoren nicht über das Ausscheiden von Mitarbeitern informiert werden und somit nicht mehr benötigte Benutzerkonten im Active-Directory verbleiben.

node***WATCH*** bietet hier Hilfestellung. Im Hauptmenü gelangt man über die Schaltfläche [Active Directory Benutzer & Computer] zur Verwaltungsoberfläche. Hier können durch setzen verschiedenster Filter Computer- und Benutzerkonten einfach analysiert und ggf. auch gesperrt werden.

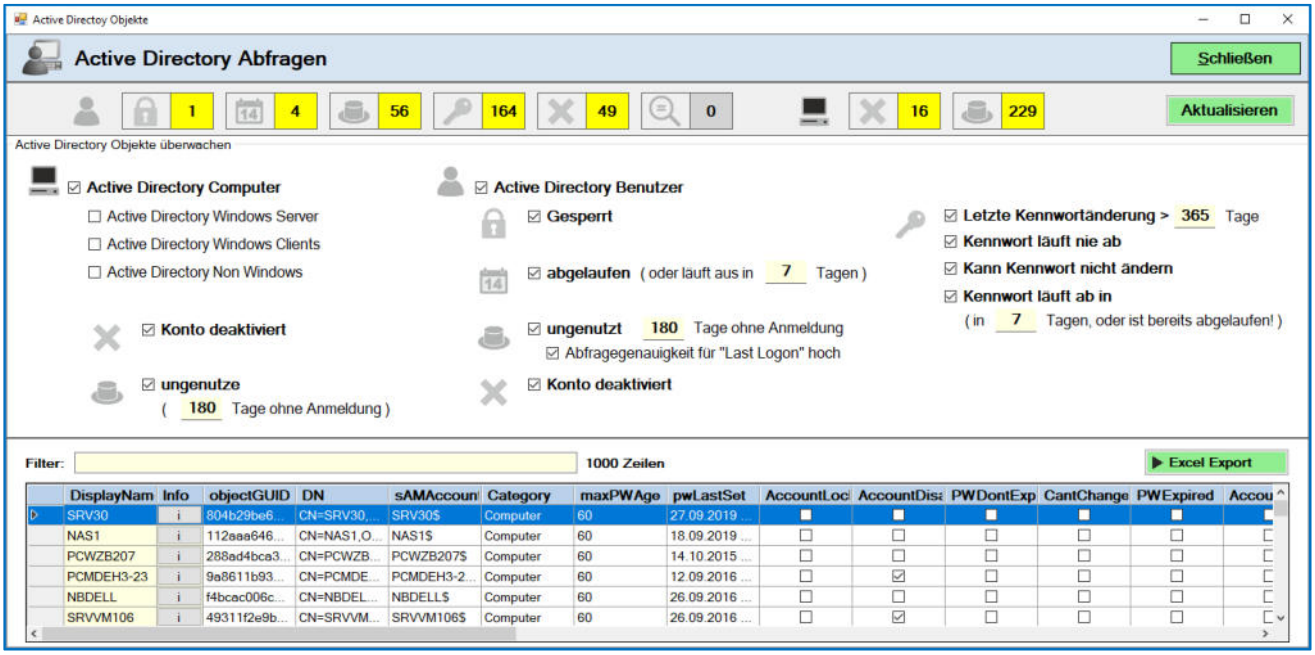


Die Optionen **[ ] Konto deaktiviert** und **[ ] ungenutzte** unter der Option **Active Directory Computer** stellen keine Filter dar, sondern bewirken lediglich, dass in den Symbolen die Anzahl der zutreffenden Ausnahmen angezeigt und durch klicken auf das Symbol aufgelistet werden.



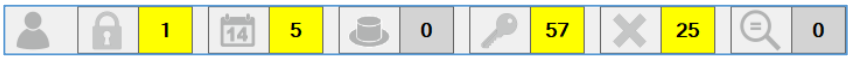
Betätigt man nachdem alle Filter gesetzt wurden die Schaltfläche [Aktualisieren], dann werden die ausgewählten Active Directory Konten entsprechend eingelesen und im Container angezeigt.

Über das Feld Filter kann man schnell die gewünschten Benutzer- und Computerkonten auffinden. Die Ergebnismenge entspricht dann nur noch den Einträgen, die im Feld DisplayName den Wert aus Filter aufweisen.



Active Directory Überwachungsleiste

Nach erfolgter Aktualisierung wird die Anzahl der gefundenen Abweichungen in der Überwachungsleiste angezeigt.



Die Symbole haben hierbei folgende Bedeutung:

 Es geht um Active Directory Benutzerkonten.

 Es geht um Active Directory Computerkonten.

 Es wurden gesperrte Benutzerkonten gefunden.

 Es wurden Benutzerkonten mit Ablaufdatum gefunden.

 Es wurden Konten gefunden, die lange keine Windows-Anmeldung mehr durchgeführt haben.

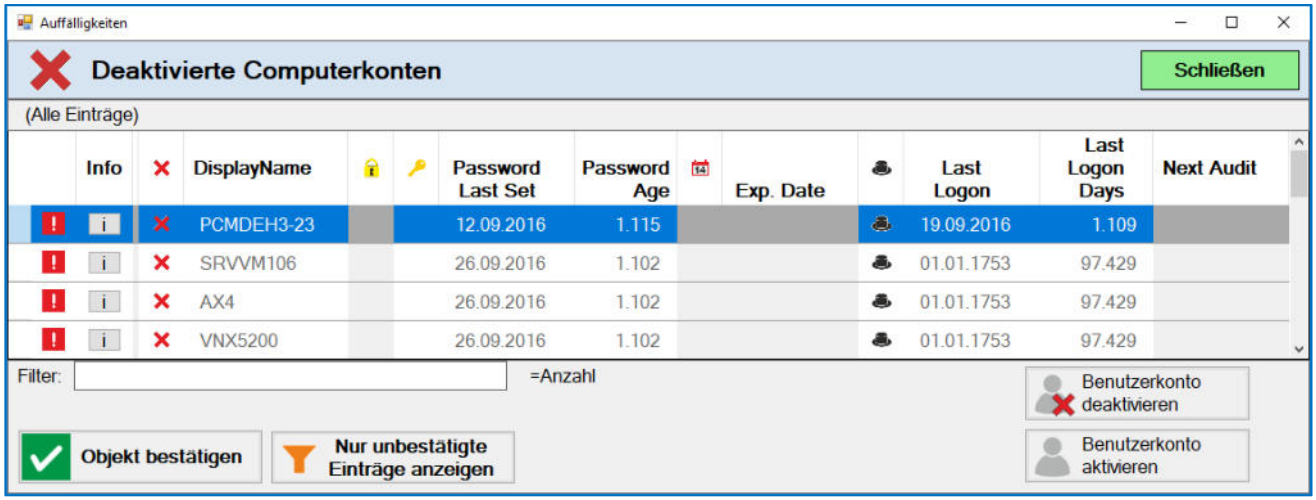
 Es wurden Konten gefunden, die kritische Kennworteinstellungen haben (Laut Konfigurationseinstellungen)

 Es wurden deaktivierte Konten gefunden.

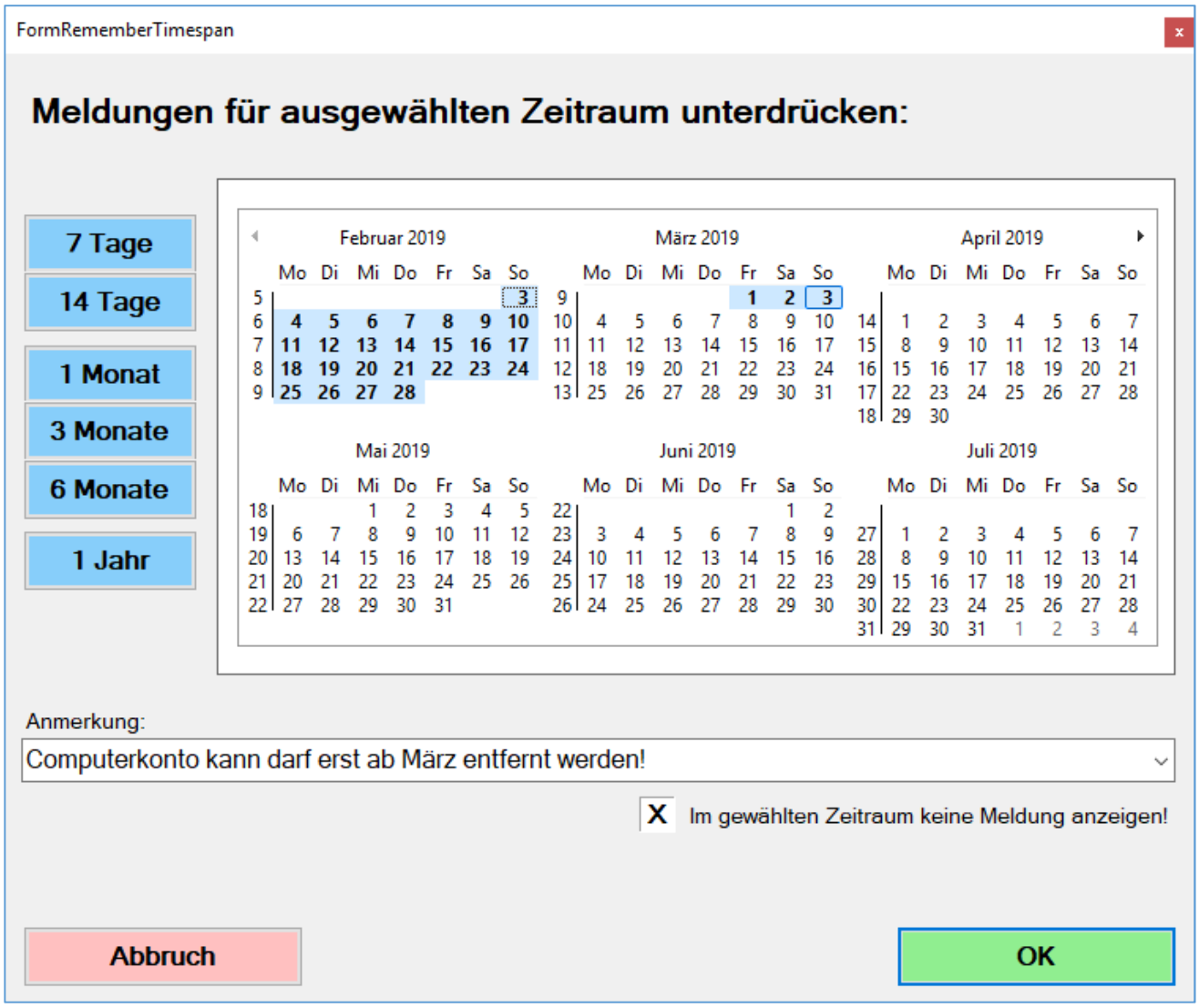
 Einstellungen von überwachten Konten wurden verändert.

Klickt man nun auf ein Symbol, dann werden die Konten angezeigt, bei denen eine Auffälligkeit gefunden wurde.

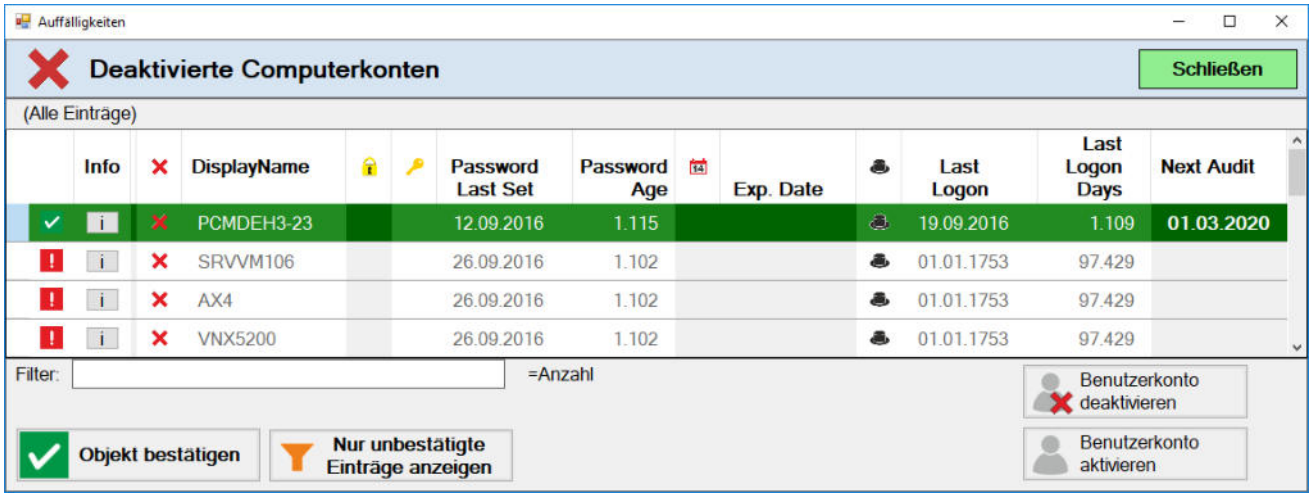
Klickt man auf ein Symbol oder eine Zahl in der Überwachungsleiste, dann öffnet dich das Fenster mit der Ausnahmeliste. Über die Symbolspalten kann man erkennen, ob es für dieses Objekt noch weitere Ausnahmen gibt, d.h. das Selbe Objekt kann in mehreren Ausnahmelisten erscheinen.



Manchmal sind Objekte bewusst nicht aus Active Directory entfernt worden und man möchte die Objekte erst ab einem bestimmten Zeitpunkt löschen. Dabei besteht die Gefahr, dass die Objektlöschung dann übersehen wird und als Leiche im System verbleibt. Um dies zu verhindern kann man mit node***WATCH*** die auffälligen Objekte für einen bestimmten Zeitraum bestätigen. Für den Zeitraum der Bestätigung werden dann keine Meldungen zu diesem Objekt mehr angezeigt.
Soll die gefundene Ausnahme als OK gekennzeichnet werden, dann kann man dies durch Klick auf das rote Ausrufezeichen in der vordersten Spalte. Im darauffolgenden Fenster kann dann eingestellt werden, wie lange die Ausnahmemeldung für dieses Objekt unterdrückt werden soll. Dort kann man den Zeitraum über die Schnellzugriff-Buttons oder durch klicken in den Kalender gezielt einstellen. Zur Bestätigung des Objekts ist dann noch eine Anmerkung, und die Aktivierung des Kontrollkästchens **[X] im gewählten Zeitraum keine Meldung anzeigen** erforderlich.



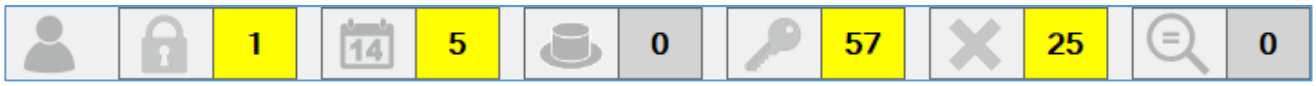
Nach Bestätigung der Unterdrückungseinstellungen wird das gewählte Objekt grün angezeigt und bis zum zuvor ausgewählten Termin nicht mehr als Ausnahme ausgeführt.



Ebenso können Computer-Objekte über diese Ansicht im Active Directory aktiviert bzw. deaktiviert werden. Voraussetzung hierfür ist, dass zuvor in der Benutzerverwaltung ein Domänenbenutzer mit ausreichenden Berechtigungen hinterlegt und diesem Benutzer eine PIN-Nummer zugewiesen wurde.

Wenn die Ausnahmeliste geschlossen wird, aktualisiert sich der Ausnamezähler, es werden also nur alle nicht bestätigten Objekte gezählt.

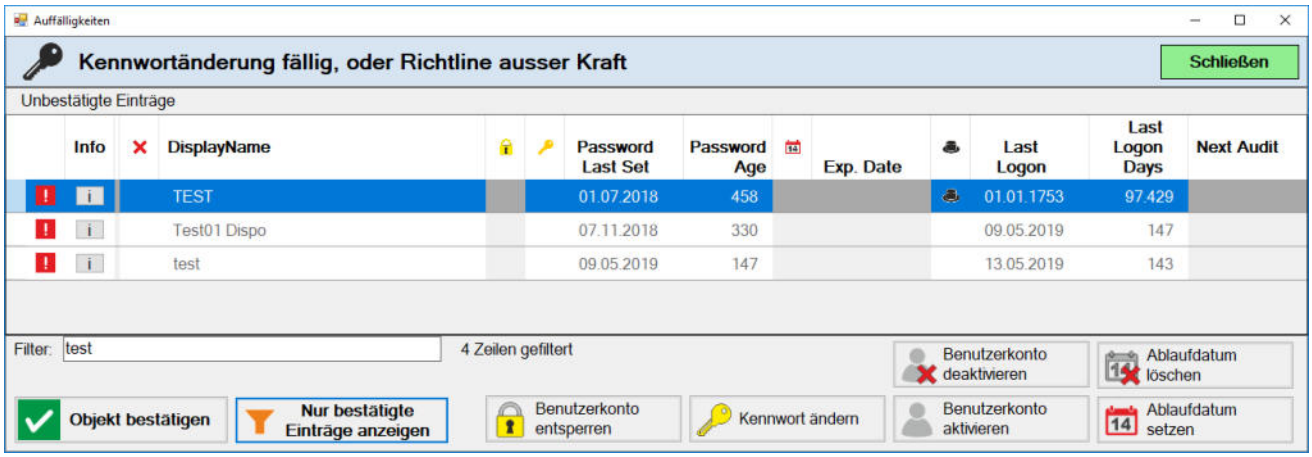
Bei der Überwachung von Benutzerkonten verhält es sich ebenso wie bei Computerkonten. Ist die Option **[ ] Active Directory Benutzer** aktiv, dann werden ALLE Benutzerkonten eingelesen. Die zusätzlichen Auswahlmöglichkeiten haben wieder lediglich eine Auswirkung auf die Ausnahmelisten (Zähler und Liste in den Symbolen der oben dargestellten Benutzerleiste.



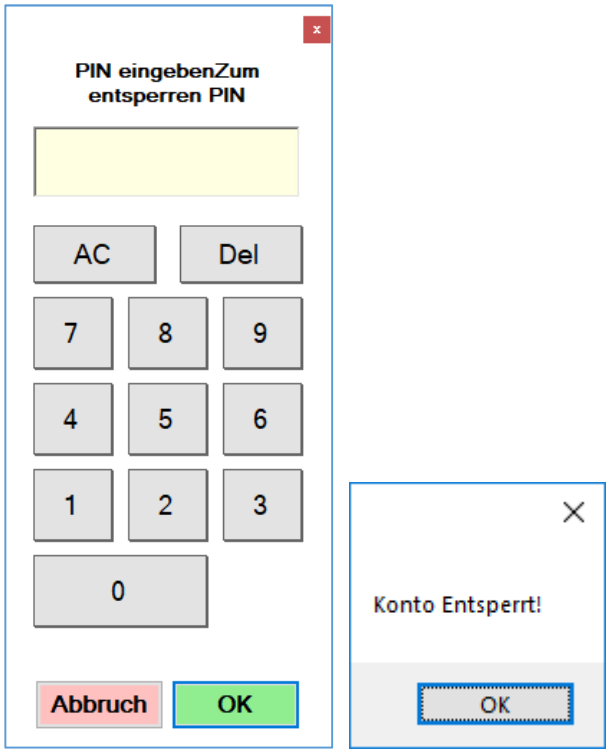
Nachfolgendes Fenster zeigt die Übersicht der gesperrten Benutzer an. Für Benutzerobjekte stehen zusätzliche Active-Directory Funktionen wie

- Benutzerkonto entsperren
- Kennwort ändern
- Benutzerkonto deaktivieren
- Benutzerkonto aktivieren
- Ablaufdatum löschen
- Ablaufdatum setzen

zur Verfügung.

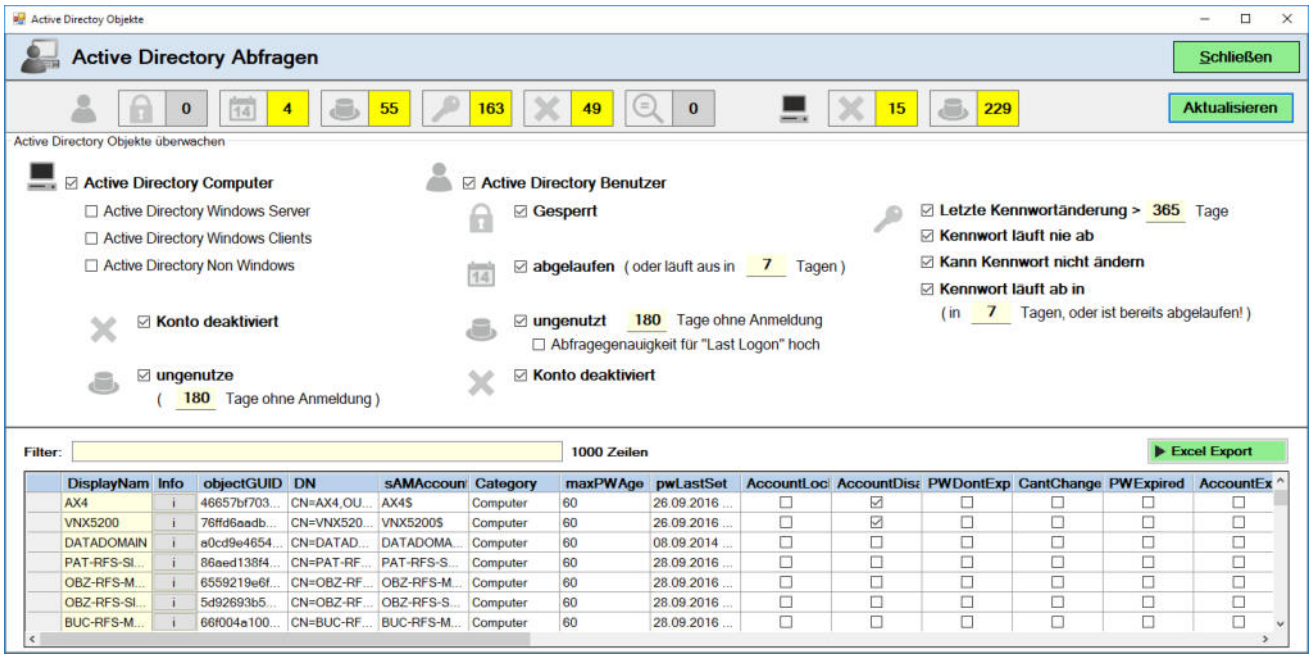


Zum Ausführen einer Active-Directory Funktion ist wie auch bei den Computerobjekten Voraussetzung, dass in der Benutzerverwaltung zuvor Domänenbenutzer mit ausreichenden Berechtigungen hinterlegt und dem Benutzer wiederum eine PIN-Nummer zugewiesen wurde.

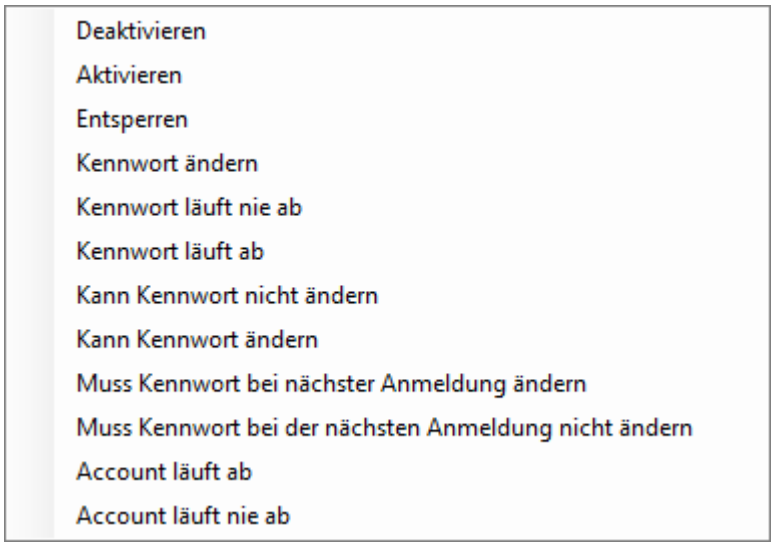


Nach Eingabe der PIN wird mit dem zugeordneten Konto die Aktivität ausgeführt.

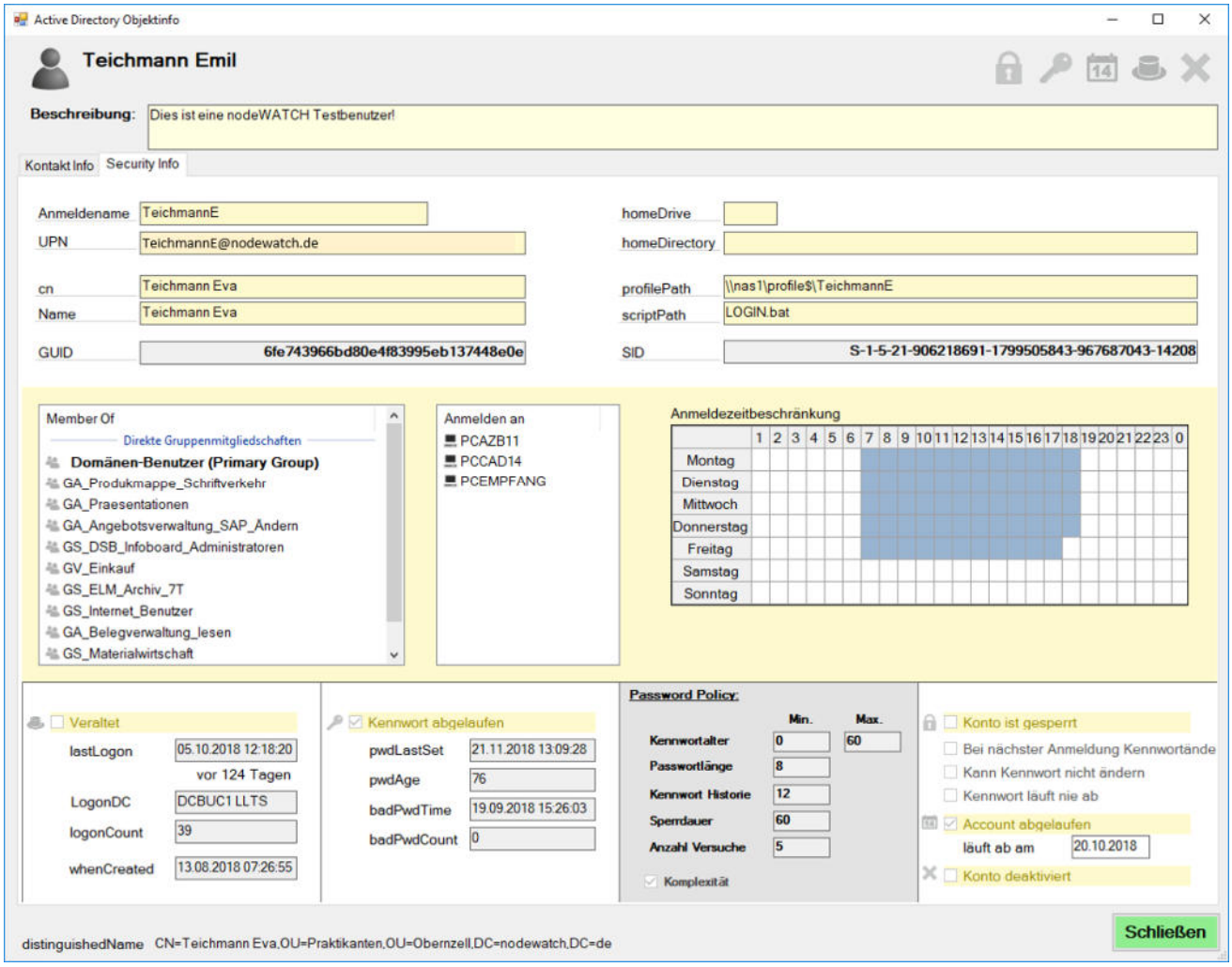
Wird ein gesperrtes Benutzerkonto wieder entsperrt, dann wird nach dem Schließen der Ausnahmeliste der Zähler für gesperrte Konten wieder aktualisiert.



Über das Kontextmenü können folgende Active-Directory-Funktionen für ein Objekt ausgeführt werden:



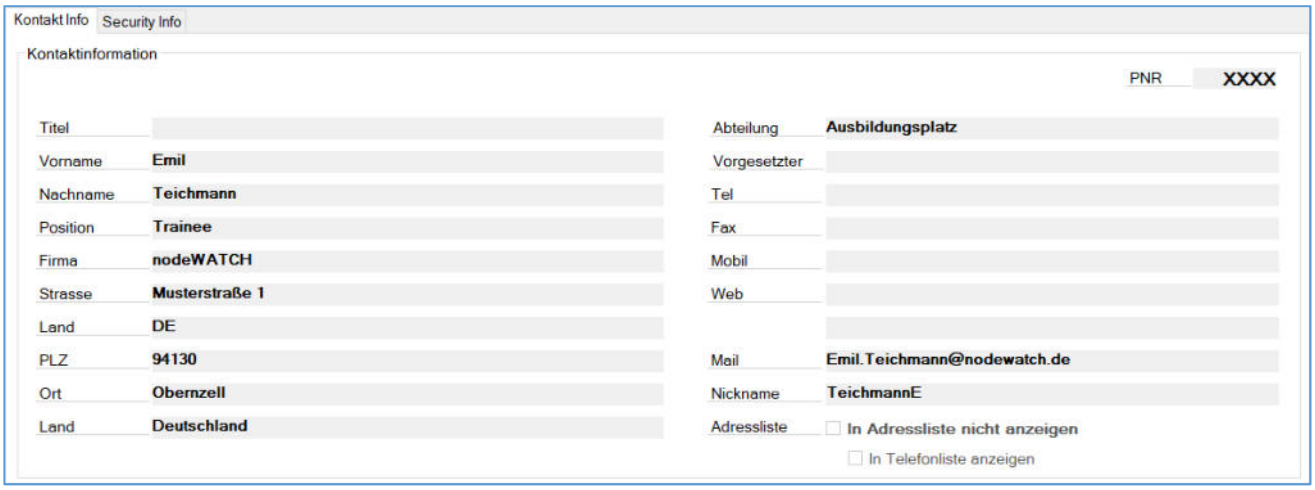
Durch Klick auf den Button **[i]** in der Info-Spalte gelangt man in die Objektübersicht. Hier werden wichtige Informationen des Objekts in einer Zusammenfassung angezeigt.



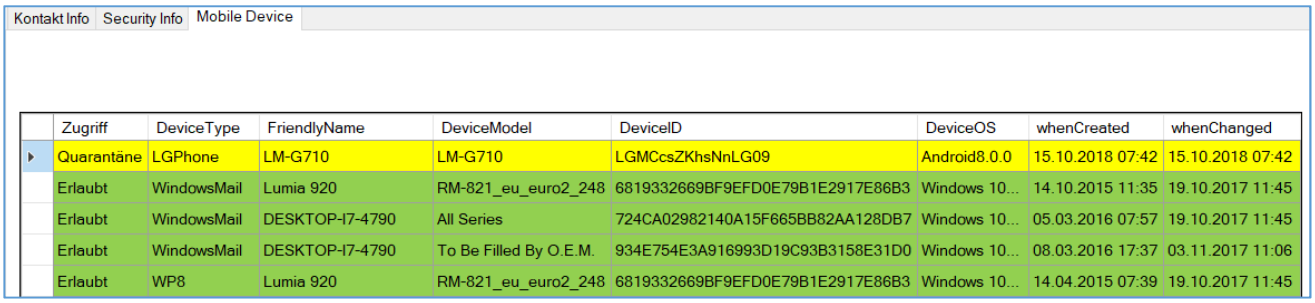
Der obere Abschnitt beinhaltet angaben zum Objektnamen, Anmeldenamen, Home-Laufwerk, Profilpfad und Anmeldeskript, GUID und SID.
Im mittleren Abschnitt werden Informationen zu Gruppenmitgliedschaften, Arbeitsstationsbeschränkungen und Anmeldeeiten angezeigt. Die besonderheit hierbei ist, dass auch indirekte Gruppenmitgliedschaften aufgelistet werden, d.h. Gruppenmitgliedschaften, die man durch Mitglidschaft einer anderen Gruppe erhält.

Im unteren Abschnitt befinden sich dann noch Informationen Kennwortrichtlinien, Kennworteinstellungen, Ablaufdatum und Informationen über die letzte Anmeldung mit diesem Benutzerkonto.

Im Register | Kontakt Info | werden Standort und Telefon, Fax- und Mailadressinformationen des Benutzers angezeigt.



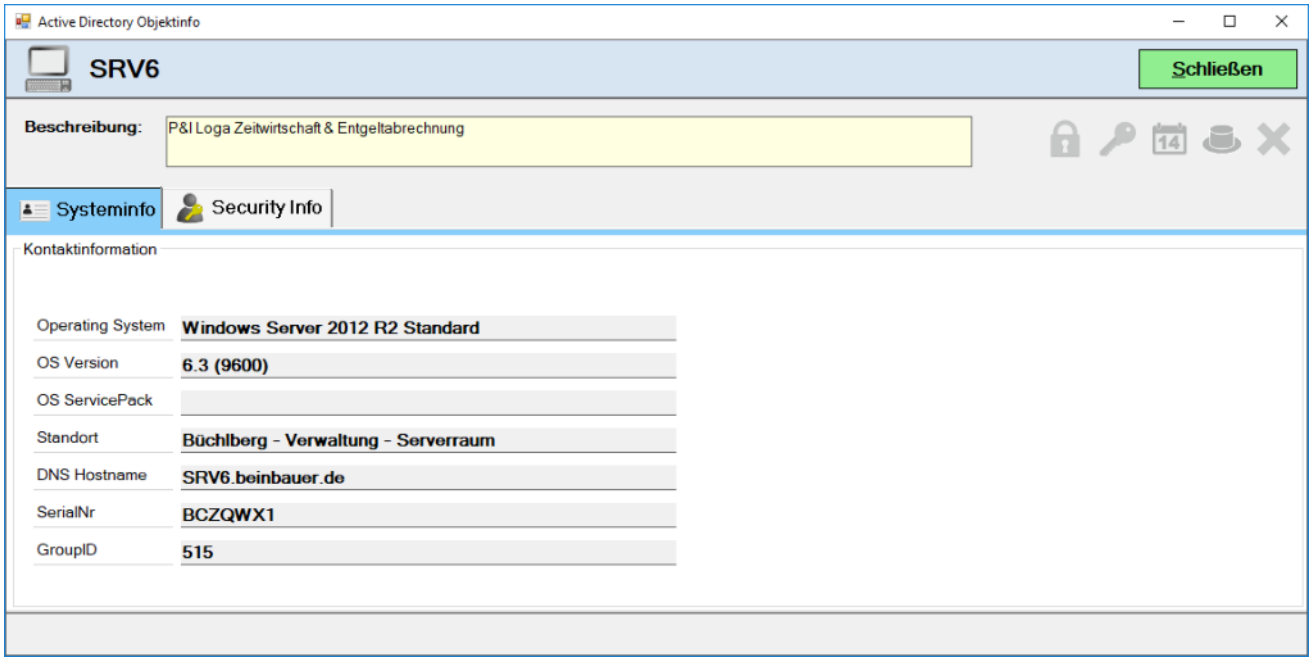
Und für den Fall, dass der Benutzer, der zum auslesen von ActiveDirectory hinterlegt ist, genügend Berechtigungen besitzt und Mobile Endgeräte über ActiveSync am Exchange-Server angebunden wurden, dann werden im Register | Mobile Device | die mobilen Endgeräte angezeigt, mit denen der Benutzer seine Emails synchronisiert.



Zugriff	DeviceType	FriendlyName	DeviceModel	DeviceID	DeviceOS	whenCreated	whenChanged
Quarantäne	LGPhone	LM-G710	LM-G710	LGMCcsZKhsNnLG09	Android8.0.0	15.10.2018 07:42	15.10.2018 07:42
Erlaubt	WindowsMail	Lumia 920	RM-821_eu_euro2_248	6819332669BF9EFD0E79B1E2917E86B3	Windows 10...	14.10.2015 11:35	19.10.2017 11:45
Erlaubt	WindowsMail	DESKTOP-I7-4790	All Series	724CA02982140A15F665BB82AA128DB7	Windows 10...	05.03.2016 07:57	19.10.2017 11:45
Erlaubt	WindowsMail	DESKTOP-I7-4790	To Be Filled By O.E.M.	934E754E3A916993D19C93B3158E31D0	Windows 10...	08.03.2016 17:37	03.11.2017 11:06
Erlaubt	WP8	Lumia 920	RM-821_eu_euro2_248	6819332669BF9EFD0E79B1E2917E86B3	Windows 10...	14.04.2015 07:39	19.10.2017 11:45

Grün zeigt freigegebene, gelb in Quarantäne befindliche und rot deaktivierte Geräte.

Bei Informationen über ein Computerobjekt werden im Register | Systeminformationen | entsprechend Informationen zum aktuell verwendeten Betriebssystem sowie die Standortdaten angezeigt.



Active Directory Gruppenmitglieder überwachen

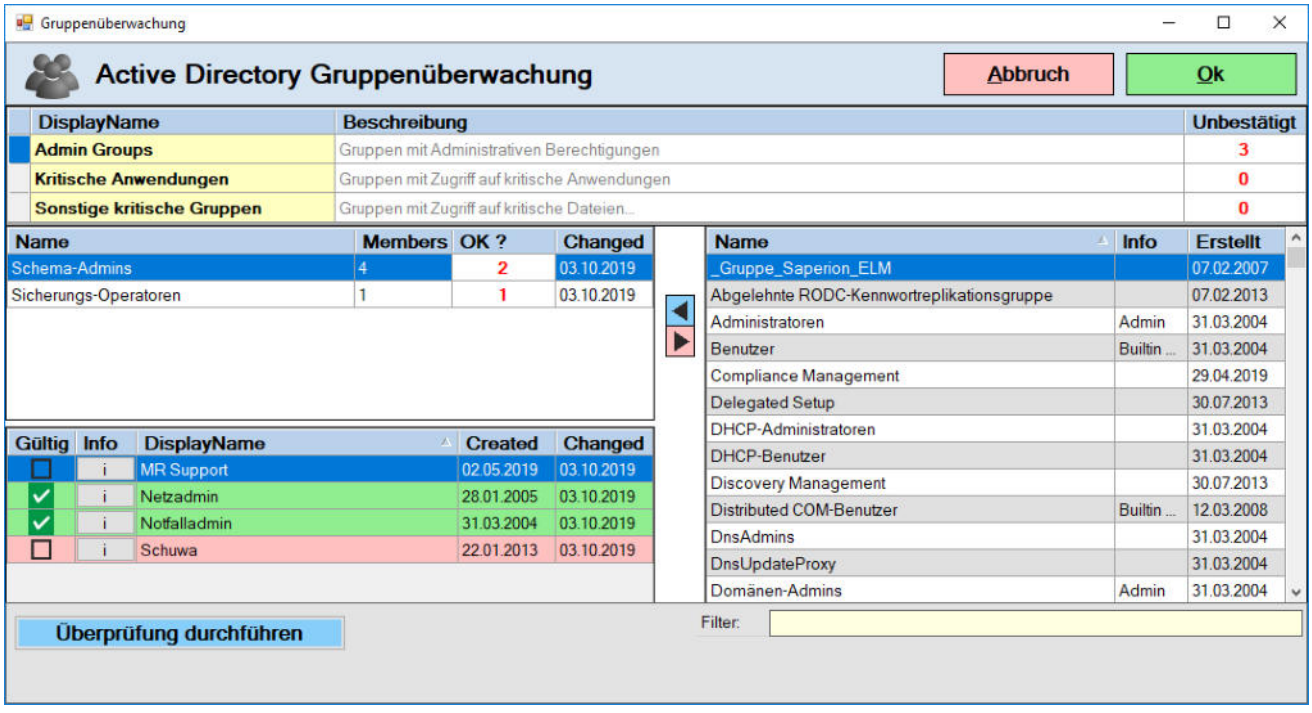
Die Überwachung von Active-Directory Gruppenmitgliedschaften ist ein weiteres Feature. Unerwünschte Änderungen von Gruppenmitgliedschaften wie z.B. den Domänen-Administratoren können hiermit überwacht werden.

Die Gruppenüberwachung unterteilt sich hierbei in drei Ebenen:

Admin Gruppen ist die Erste Ebene, hier sollten Gruppen mit Administrativen Berechtigungen zugeordnet werden.

Kritische Anwendungen stellt die zweite Ebene dar. Dieser Ebene sollten Gruppen mit Zugriffsberechtigungen auf kritische Anwendungen oder Verzeichnisse wie z.B. dies im Personalwesen der Fall ist, zugeordnet werden.

Sonstige kritische Gruppe ist die letzte Ebene und kann nach Belieben verwendet werden.



Um eine Gruppe zu überwachen, muss man zunächst in der oberen Tabelle eine Ebene auswählen, in der die Gruppe überwacht werden soll.

Die rechte Tabelle zeigt ALLE Active Directory Sicherheitsgruppen an. In der Spalte Info kann man erkennen, ob es sich um eine Builtin Gruppe handelt. Das System versucht Gruppen mit administrativen Berechtigungen automatisch zu erkennen und kennzeichnet diese in der Info-Spalte mit Admin.

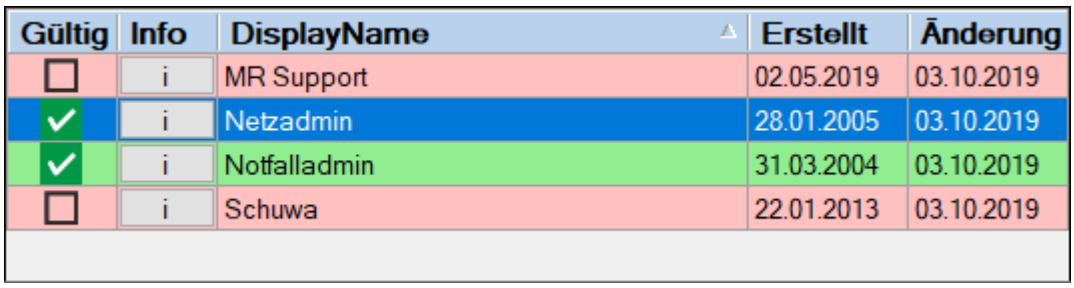
Name	Info	Erstellt
Benutzer	Builtin ...	31.03.2004
Compliance Management		29.04.2019
Delegated Setup		30.07.2013
DHCP-Administratoren		31.03.2004
DHCP-Benutzer		31.03.2004
Discovery Management		30.07.2013
Distributed COM-Benutzer	Builtin ...	12.03.2008
DnsAdmins		31.03.2004
DnsUpdateProxy		31.03.2004
Domänen-Admins	Admin	31.03.2004
Domänen-Benutzer		31.03.2004
Domänencomputer		31.03.2004
Domänencontroller		31.03.2004

Über die blaue Pfeiltaste  können ausgewählte Gruppen nun zur ausgewählten Überwachungsebene hinzugefügt werden. Diese werden dann der mittleren Tabelle auf der linken Seite des Formulars hinzugefügt.

Name	Mitglieder	OK ?	Änderung
Schema-Admins	4	2	03.10.2019
Sicherungs-Operatoren	1	1	03.10.2019

Die Spalte Members zeigt die Anzahl der Gruppenmitglieder in die Spalte OK ? die Anzahl der nicht bestätigten Mitglieder. In der letzten Spalte wird das Änderungsdatum der Gruppe angezeigt.

Unterhalb dieser Tabelle werden Gruppenmitglieder der selektierten Gruppe dargestellt. Wird eine neue Gruppe hinzugefügt sind erst einmal alle Einträge rot. Mit Klick auf die vorderste Spalte Gültig kann die Gruppenmitgliedschaft bestätigt werden und der Eintrag wird grün. Der Zähler oben neben der Gruppe und in der Überwachungsebene reduziert sich um jeweils eins.



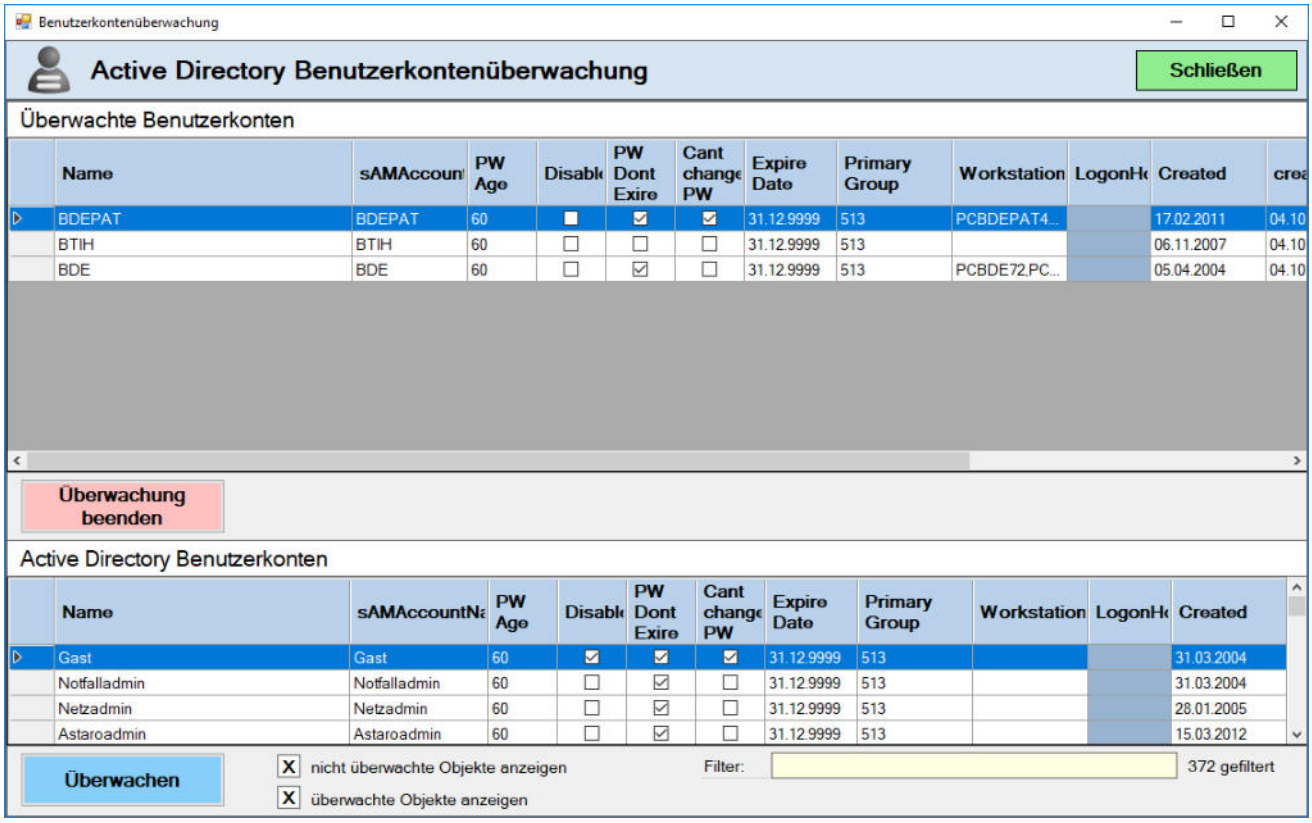
Gültig	Info	DisplayName	Erstellt	Änderung
☐	i	MR Support	02.05.2019	03.10.2019
☑	i	Netzadmin	28.01.2005	03.10.2019
☑	i	Notfalladmin	31.03.2004	03.10.2019
☐	i	Schuwa	22.01.2013	03.10.2019

Klickt man neben dem Benutzer auf das **[i]** (Info-Button) dann werden Detailinformationen zum Benutzerkonto angezeigt.

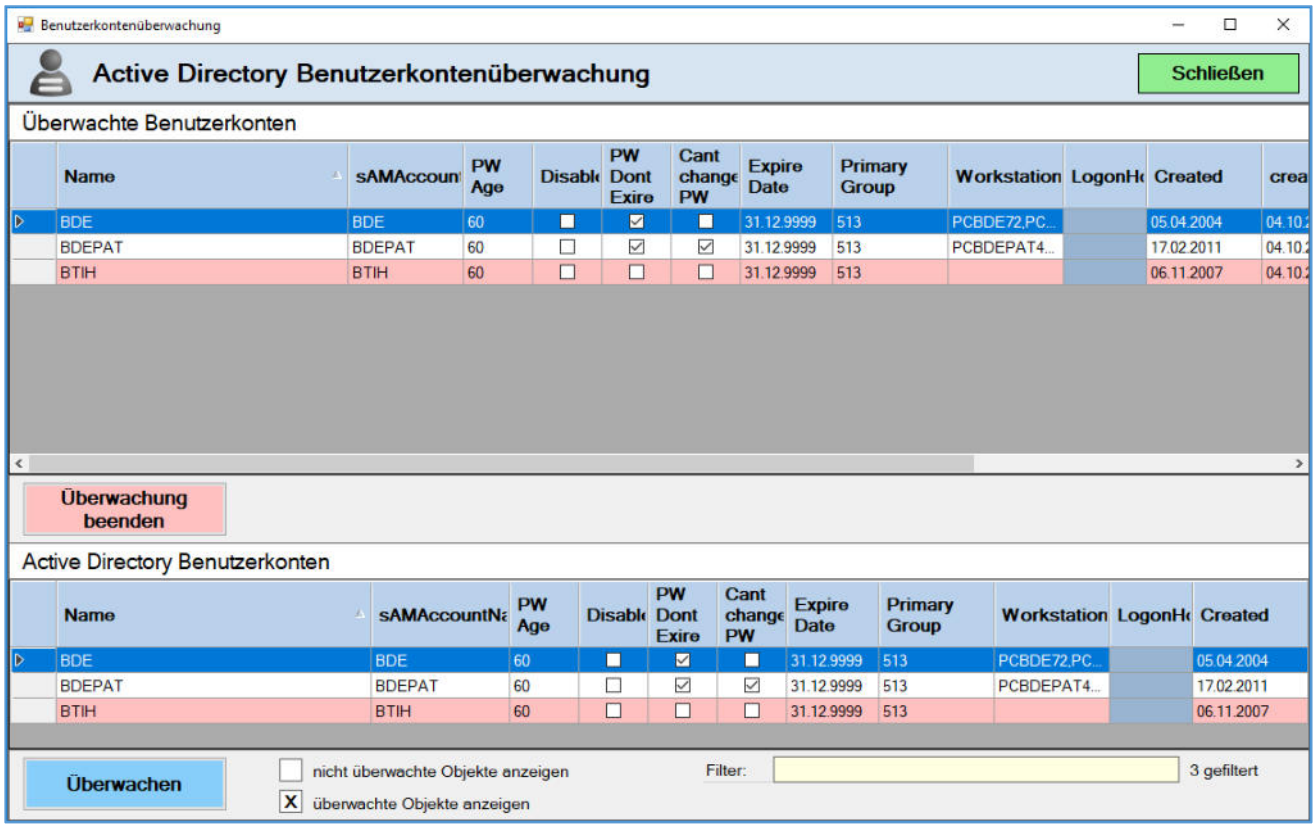
Erwähnt werden muss an dieser Stelle noch, dass hier nicht nur alle direkten Gruppenmitglieder, sondern auch alle indirekten Gruppenmitglieder angezeigt und überwacht werden. Somit werden auch Änderungen in verschachtelten Gruppen angezeigt.

Active Directory Benutzeränderungen

Benutzerkonten, die von mehreren Benutzern verwendet werden wie das z.B. bei Terminals zur Betriebsdatenerfassung oftmals der Fall ist, bedürfen der besonderen Aufmerksamkeit. Änderungen Gruppenmitgliedschaften haben hier gleich weitreichende Folgen, da die neuen Berechtigungen allen Benutzern dieses Gruppen-Accounts zur Verfügung stehen. Vor allem bei verschachtelten Gruppen werden Änderungen sehr schnell intransparent. Um es den Administratoren hier etwas zu erleichtern wurde das Modul zur Überwachung von Benutzeränderungen entwickelt.

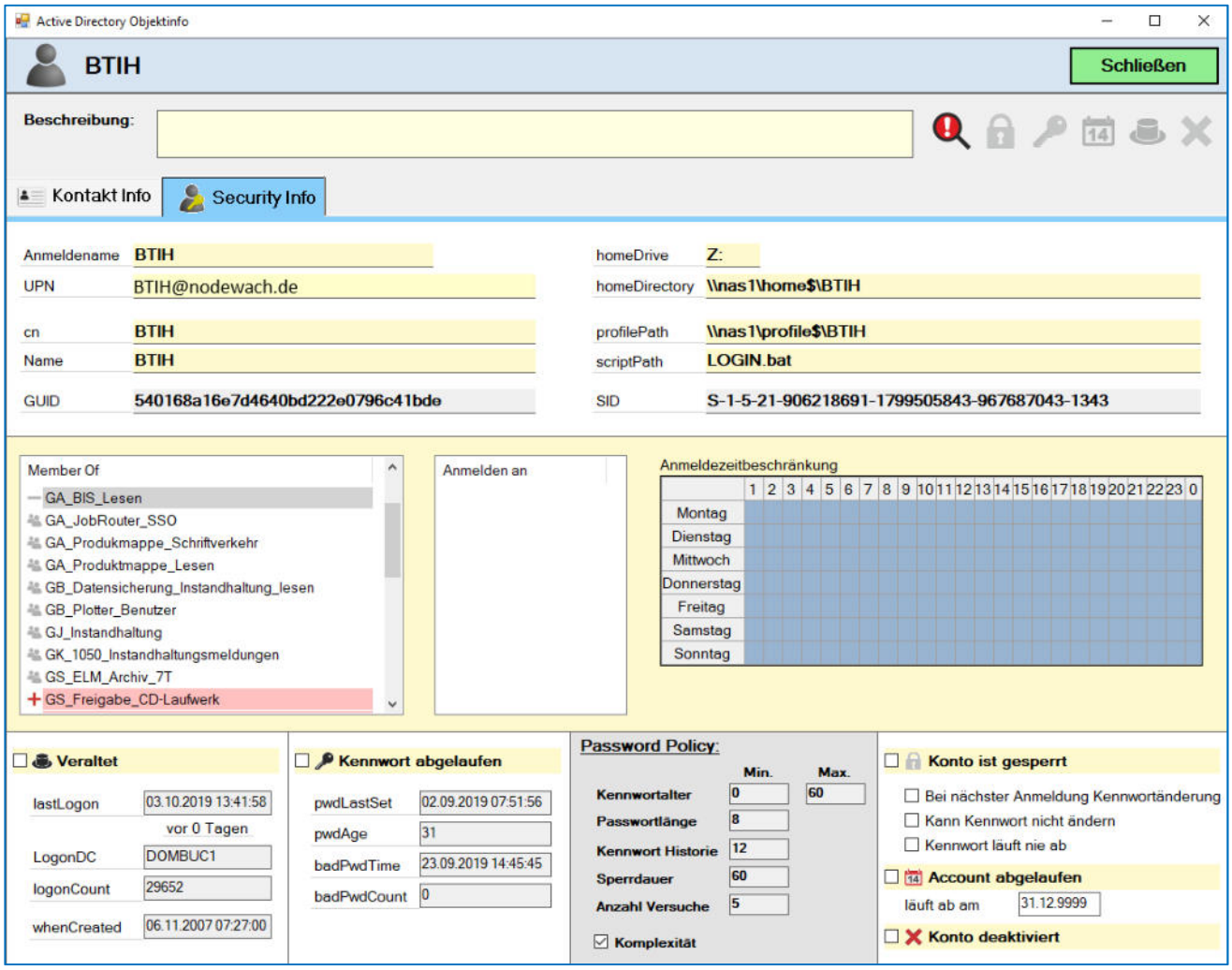


Im oberen Bereich werden die Benutzerkonten angezeigt, die überwacht werden sollen. In der unteren Tabelle werden alle für die Überwachung zur Verfügung stehenden Benutzerkonten angezeigt. Zur Überwachung des Benutzeraccounts muss man zuerst einen Benutzer im unteren Bereich markieren und anschließend auf Schaltfläche **[Überwachen]** klicken. Das Benutzerkonto wird nun im Container *Überwachte Benutzerkonten* mit angezeigt. Wird die Überwachung gestartet, dann zeigt ein Zähler im Überwachungssymbol die Anzahl der Benutzerkonten an, die von den ursprünglichen Einstellungen abweichen.



Eine Rote Zeile weist auf eine Abweichung der Einstellungen hin. Deaktiviert man die Option nicht überwachte Objekte anzeigen, dann werden in beiden Abschnitten nur noch die Benutzerkonten angezeigt, für die eine Überwachung eingerichtet wurde. Durch einen Doppelklick auf den rot markierten Eintrag gelangt man in die Detailansicht.

Die nachfolgende Abbildung zeigt Änderungen an den Gruppenmitgliedschaften.



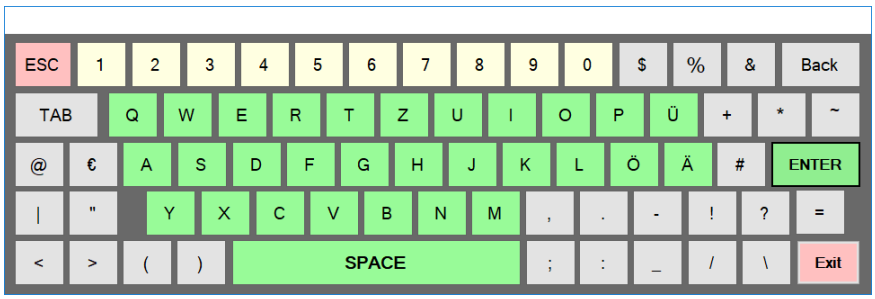
Grau hinterlegte Einträge wurden entfernt, rot hinterlegte Einträge wurden neu hinzugefügt. Änderungen an Passworteinstellungen werden rot hervorgehoben.

Überwachung starten

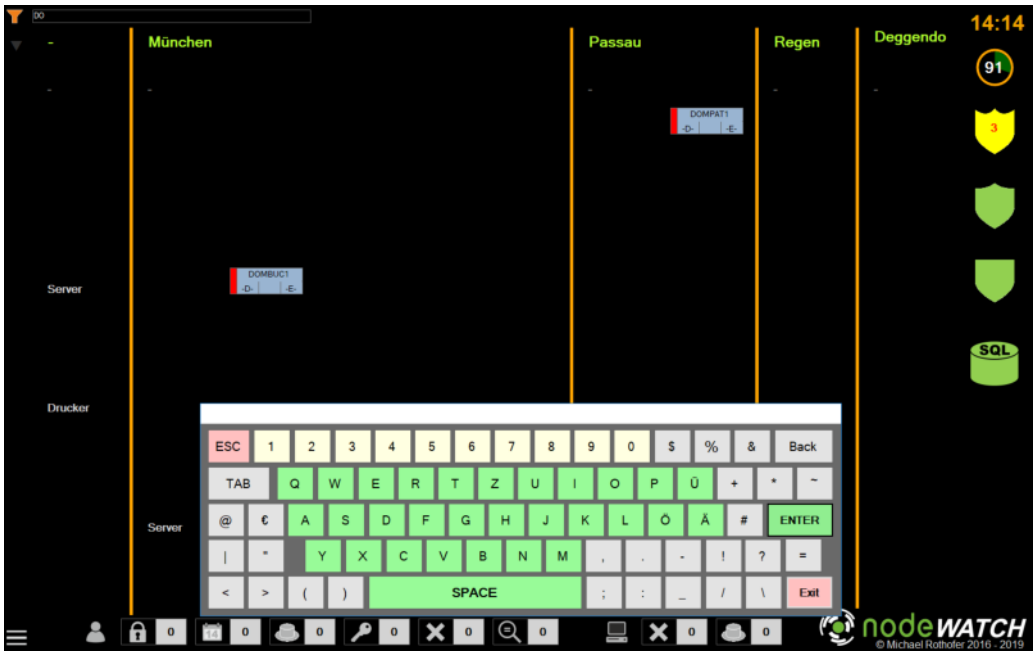
Wenn alles eingerichtet wurde, kann mit der Überwachung begonnen werden. Klicken Sie hierfür im Hauptmenü auf die Schaltfläche **[Überwachung starten]**.

Beim ersten Start wurden ja bereits im Hintergrund Serversysteme ermittelt und zugeordnet. In unserm Beispiel sieht der Überwachungsbereich folgendermaßen aus:

Das Filtersymbol oben links dient dazu, Nodes schneller zu finden, wenn schon sehr viele Geräte zur Überwachung angezeigt werden. Wenn man auf den Filter tippt, dann wird ein Eingabefeld eingeblendet und eine Bildschirmtastatur erscheint.



Wird nun ein Suchbegriff eingetragen, dann werden ALLE Nodes ausgeblendet, die nicht dem Suchbegriff entsprechen.



Durch erneutes tippen auf das Filtersymbol wird der Filter geschlossen und alle Nodes werden wieder angezeigt.

Über das dunkelgraue Dreieck ▾ auf der linken oberen Seite kann eine Schnellzugriffleise eingeblendet werden.


Uhrzeit ein- /ausblenden


Positioniermodus ein- /ausschalten

Neue Nodes einfügen

Sucht im Hintergrund nach neuen Geräten

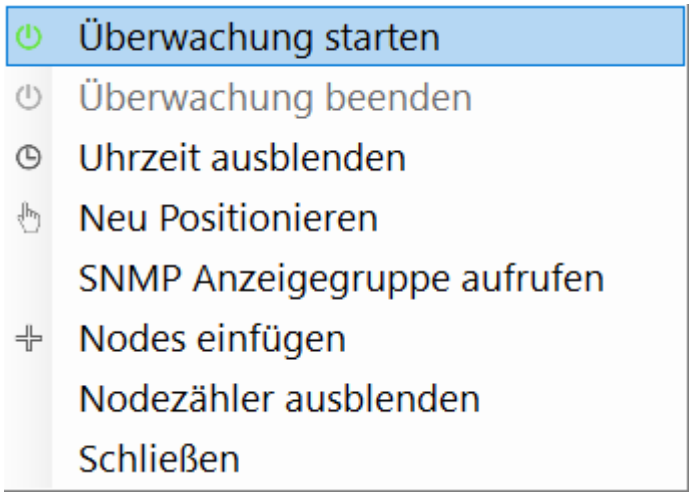
Node Zähler (oben rechts) ein-/ ausblenden


SNMP Infogruppe abrufen


Überwachung starten / stoppen

Alle Funktionen der Schnellzugriffsleiste sind auch über das Menü (unten links) abrufbar:

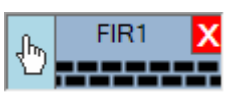
Menü



Neu positionieren

Wählt man im Menü das Hand-Symbol (= Node positionieren), dann erscheint über jeder Node dieses Symbol. Das deutet darauf hin, dass der Sortiermodus aktiv ist.

Klickt man nun mit der Maus auf das Hand-Symbol einer Node, dann wird diese Markiert und ist für die Umsortierung bereit.

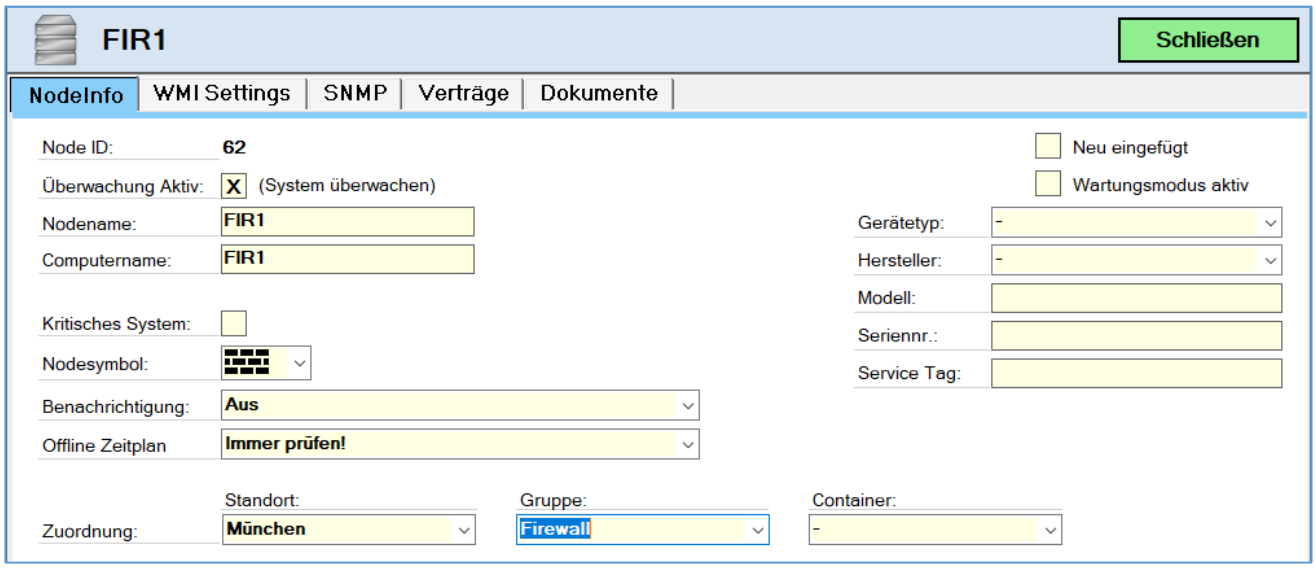


Nun kann man entweder direkt auf die Gruppe, einen Standort, oder eine andere Node klicken, um die markierte Node direkt dahinter einzusortieren.

Über das X kann die Node aus der Überwachung entfernt werden. Ein erneuter Klick auf das Hand-Symbol in der Schnellzugriffsleiste beendet den Sortiermodus.

Klickt man nun auf eine Node erscheint ein Schnellzugriffsmenü für diese Node, die unten folgende Schaltflächen aufweist:

Über das Schraubenschlüsselsymbol gelangt man zur Node Konfiguration ,wie schon unter Kapitel Überwachung konfigurieren / Detail-Konfiguration beschrieben.



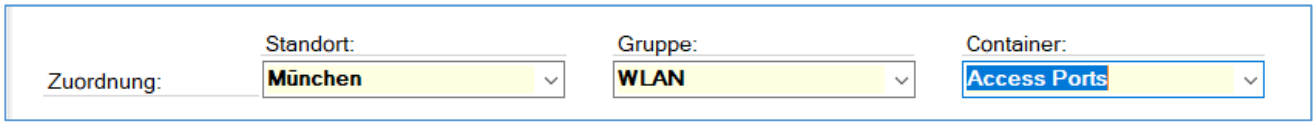
Unter Zuordnung kann nun die Umsortierung in eine Gruppe vorgenommen werden, die noch nicht in der Überwachung angezeigt wird. In unserm Beispiel ist das die Gruppe Switch. Ebenso kann noch ein Symbol für Nodes, die keine WMI-Überwachung konfiguriert haben, ausgewählt werden (Node Symbol). Nach dem Schließen des Fensters wird die Node umsortiert.

Nach der Umsortierung aller Nodes könnte der Überwachungsbildschirm so aussehen:

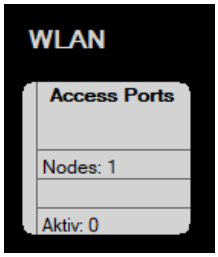

München
Passau
Regen
Deggendorf
15:11
Firewall
Server
Switch
Drucker
WLAN
SQL
nodeWATCH
© Michael Rothofer 2016 - 2019

Node-Container

Will man sich noch etwas Platz schaffen, dann kann man die Nodes innerhalb einer Gruppe in Containern zusammenfassen. Dies ist z.B. bei WLAN-Sendern oder Switchen sinnvoll. Wechseln wir hierzu wieder in die Einstellungen der Node und weisen einen Container zu.



Wir wählen für den WLAN-Sender als Container Access Ports und bestätigen unsere Wahl mit Schließen. In der Überwachung erscheint nun folgendes Symbol:



Jetzt wechseln wir wieder in den Sortiermodus (Schnellzugriffsleiste Hand-Symbol) und sortieren die verbliebenen WLAN-Nodes in den Container durch selektieren der Nodes und anschließendes Klicken auf die Container-Node. Danach beenden wir den Sortiermodus wieder.

Die Anzeige sieht nun folgendermaßen aus:

In der Container-Node wird angezeigt, wie viele Nodes sich im Container befinden. Die Zeile **Aktiv** zeigt an, für wie viele im Container enthaltenen Nodes gerade eine Überwachung durchgeführt wird. Der Container hat immer die Farbe des schlechtesten Status der Nodes im Container. Schlägt für eine Node im Container die Überwachung fehl, dann wird der gesamte Container rot.

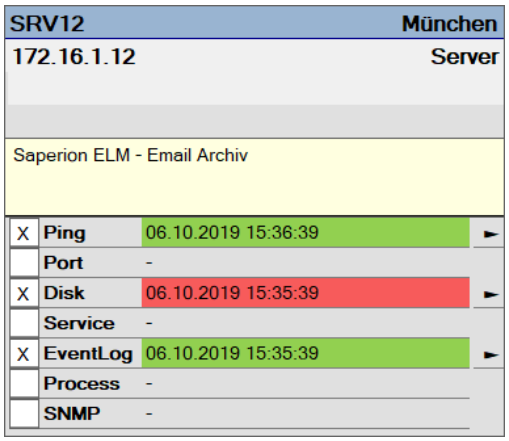
Klickt man auf die Überschrift der Container-Node, dann öffnet sie sich und die darin enthaltenen Nodes werden angezeigt. Die Titelleiste des Containers zeigt die aktuelle Position des Containers in der Überwachung.

Im Sortiermodus können die Nodes übe das X-Symbol oben rechts auf der Node wieder aus dem Container entfernt werden. Durch entfernen aller Nodes aus dem Container, löst sich der Container wieder auf.

Überwachung starten

Starten wir nun die Überwachung indem wir im Schnellzugriff-Menü das Einschaltsymbol auswählen. Das Symbol wird daraufhin grün und die Überwachung beginnt. Man erkennt eine aktive Überwachung an den braunen Balken.

Klickt man nun auf die Node Beschriftung, dann wird eine Schnellübersicht die Überwachungsergebnisse angezeigt.



Durch Klick auf den Pfeil erhält man genauere Details zum Fehler:

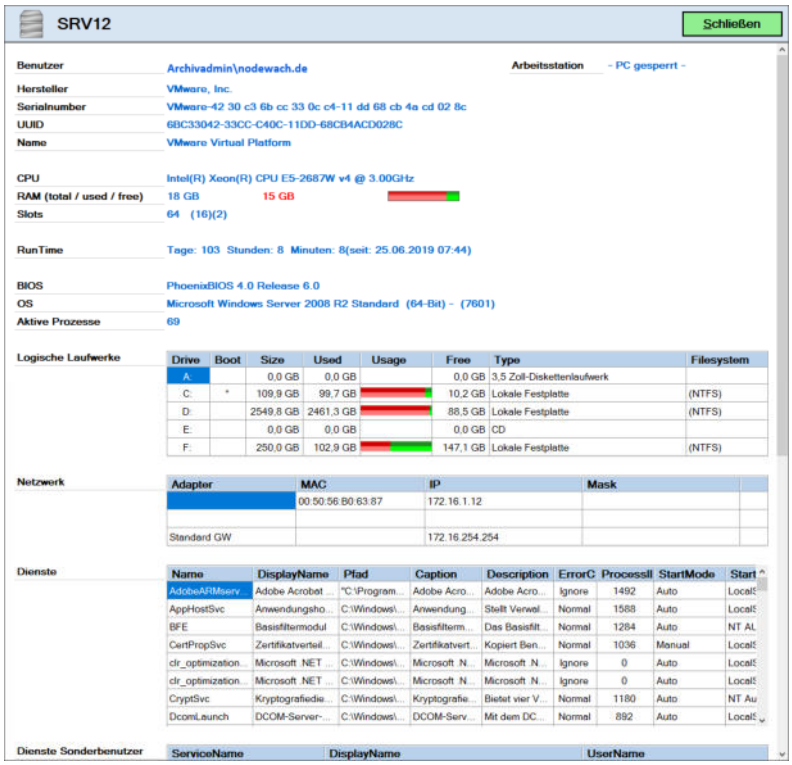
Disk	Größe	Belegt	Frei	Grenze1	Grenze2	DS
C:	110 GB	100 GB	10 GB (9,3 %)	10 %		NTFS
D:	2550 GB	2461 GB	89 GB (3,5 %)	10 %		NTFS
F:	250 GB	103 GB	147 GB (59 %)	10 %	5 GB	NTFS

Node-Buttons

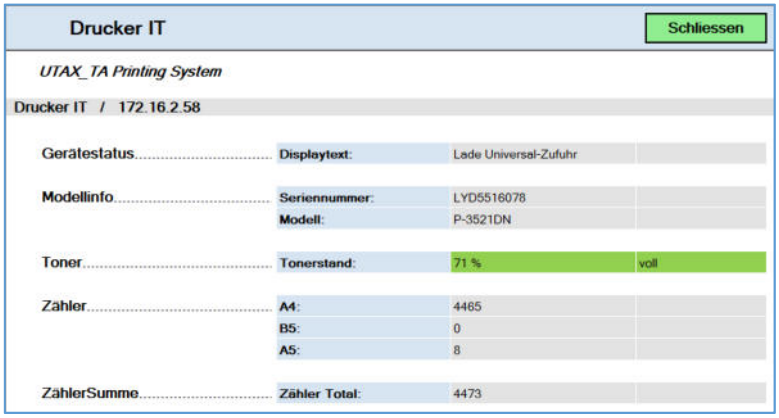
Über die Schnellzugriffsymbole der Node stehen außerdem folgende Funktionen zur Verfügung

Aktualisierung - Startet die Überwachung der Node neu.

Systeminfo - Zeigt Details zur Node. Bei WMI-überwachten Geräten zeigt das System folgendes:



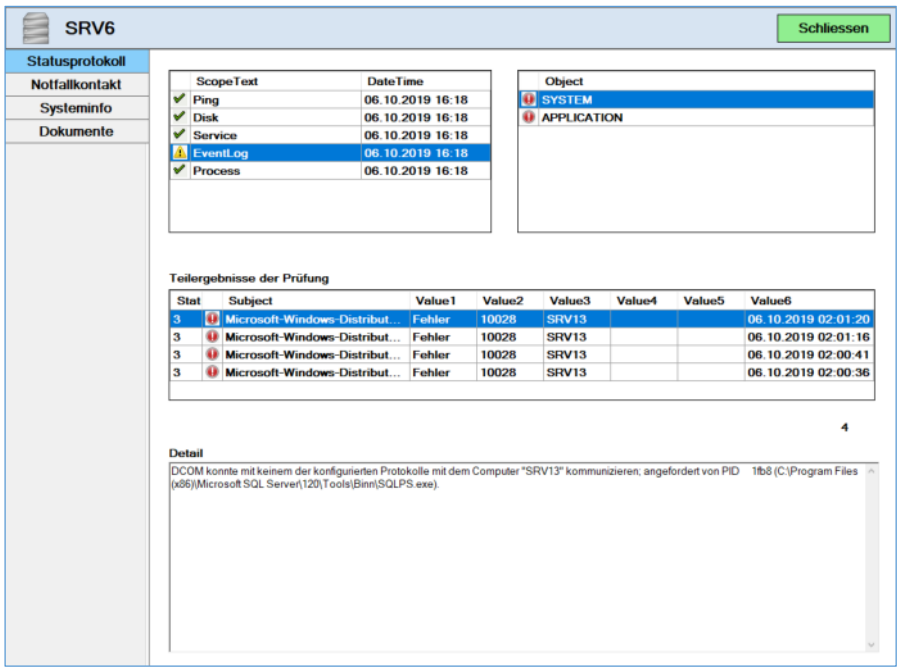
Bei Geräten mit eingerichteter SNMP-Überwachung die zugewiesenen SNMP-Werte und die Werte, die als Infofelder gekennzeichnet sind.



Überwachungsprotokoll - Zeigt die Detailergebnisse des Überwachungsprotokolls. Hier stehen folgende Möglichkeiten zur Verfügung:

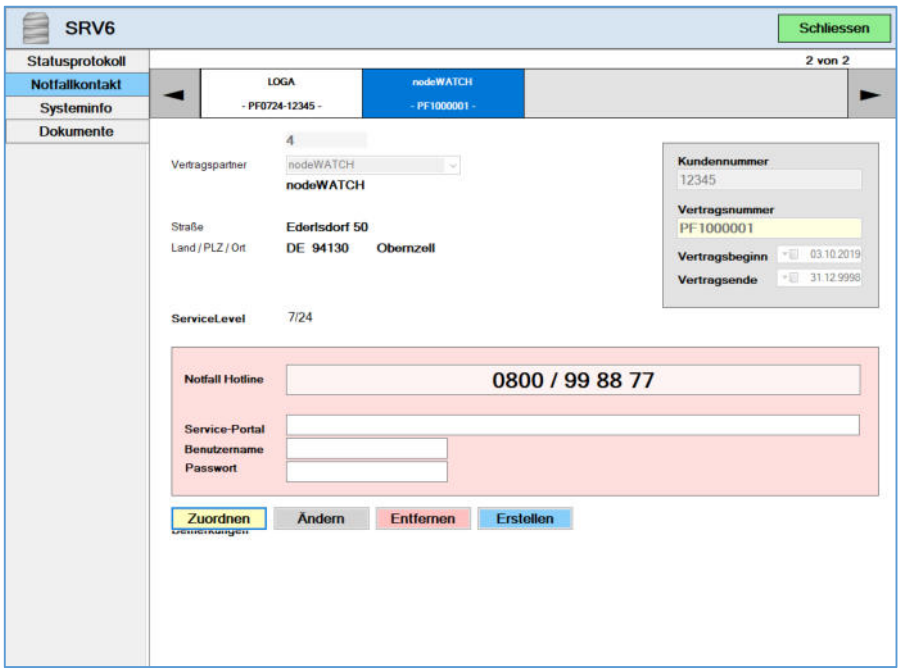
Statusprotoll:

Im Statusprotokoll können alle Details zur Überwachung eingesehen werden. Über die Symbolik kann man schnell feststellen, welche Überwachungsereignisse kritisch sind.



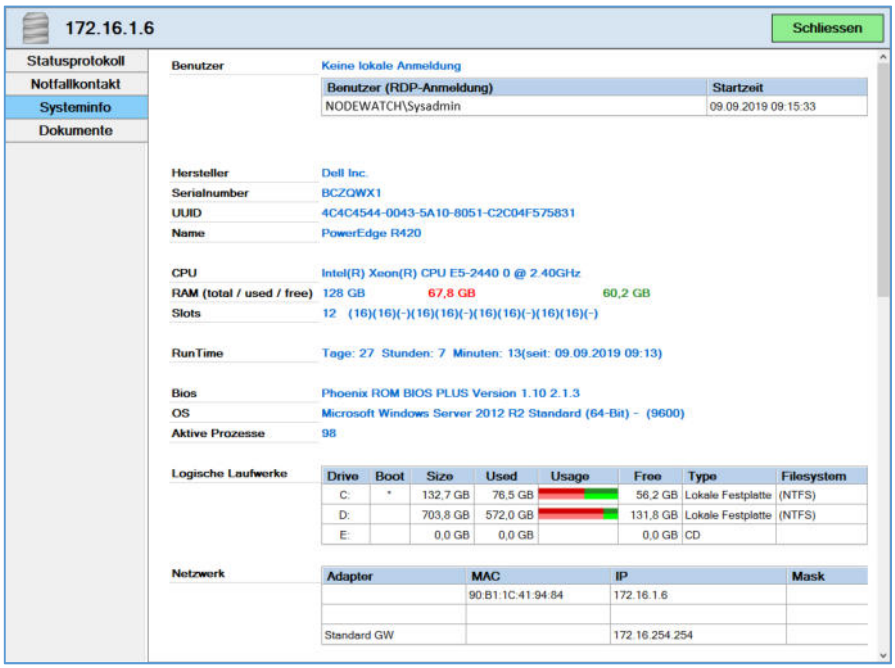
Notfallkontakt:

Ermöglicht den schnellen Zugriff auf wichtige Vertragsdaten und Ansprechpartner im Notfall.



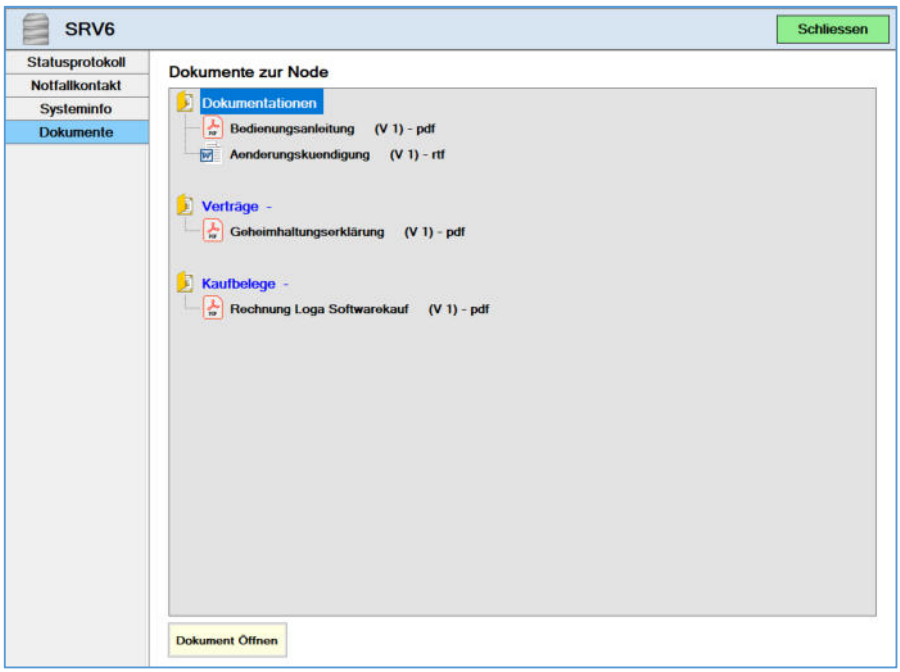
Systeminfo:

Zeigt eine Zusammenfassung von Systemparametern wie zuvor unter Systeminfo beschrieben.



Dokumente:

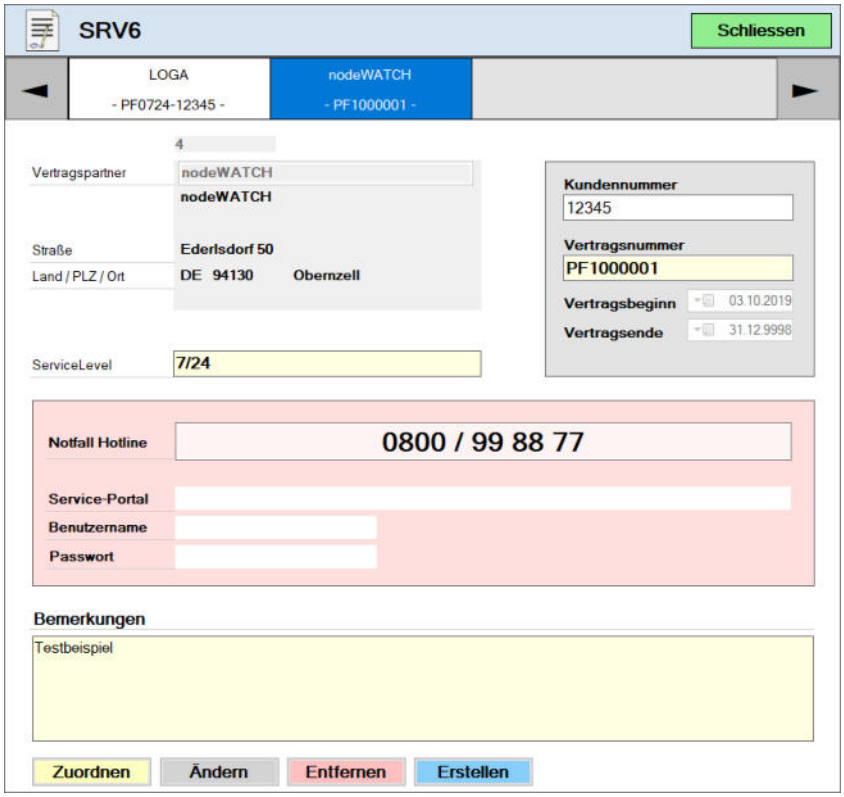
Zeigt eine Übersicht der Dokumente, die der Node zugewiesen wurden. Diese können von hier aus einfach geöffnet werden, soweit die erforderlichen Programme zum Öffnen der Dokumente auf dem System installiert sind.



Startet eine Windows Node neu. Der Benutzer muss die entsprechenden Berechtigungen für den Neustart besitzen.

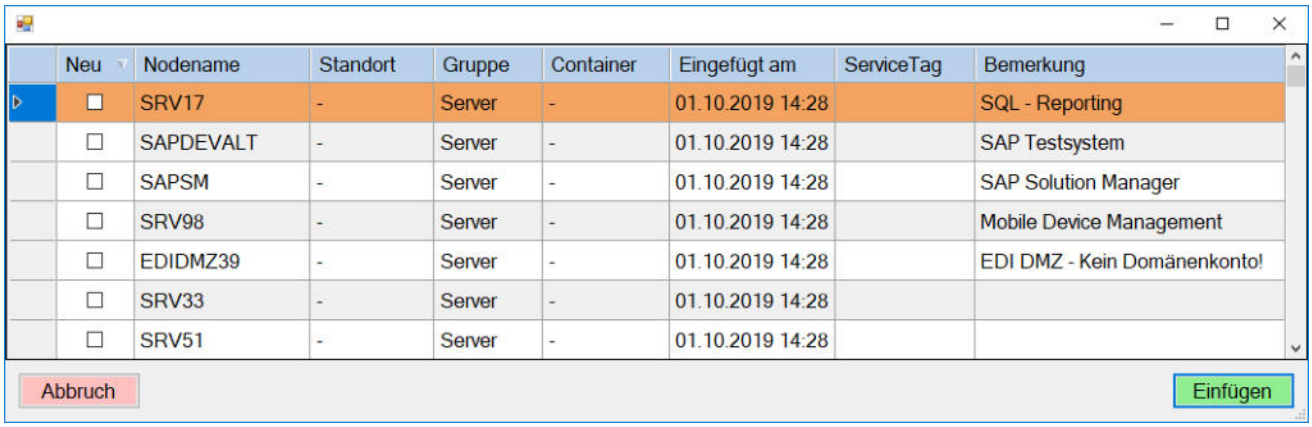
Öffnet die Node Konfiguration. Siehe Kapitel **Überwachung konfigurieren** / **Detail-Konfiguration**

Öffnet eine Schnellübersicht über die zugewiesenen Verträge und hebt Notfallkontaktnummern hervor.



Neue Nodes einfügen

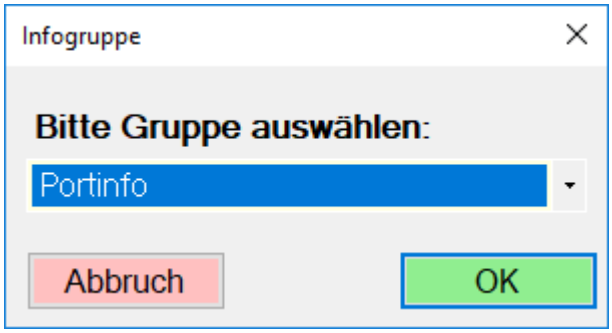
Klickt man im Schnellzugriff den Button , dann erscheint das Fenster zur Node Auswahl. Darin werden ALLE Nodes angezeigt, die nicht als aktiv gekennzeichnet sind. Führt man über Scan einen Netzwerkscan durch und werden dabei neue Geräte gefunden, dann werden diese mit dem Flag **Neu** gekennzeichnet. Für den Fall, dass eine automatische Suche für neue Geräte konfiguriert wurde, gilt dasselbe. Alle neu gefundenen Geräte werden entsprechend gekennzeichnet.



Hier kann man nun die gewünschten Systeme markieren und durch klicken von **Einfügen** der Überwachung hinzufügen.

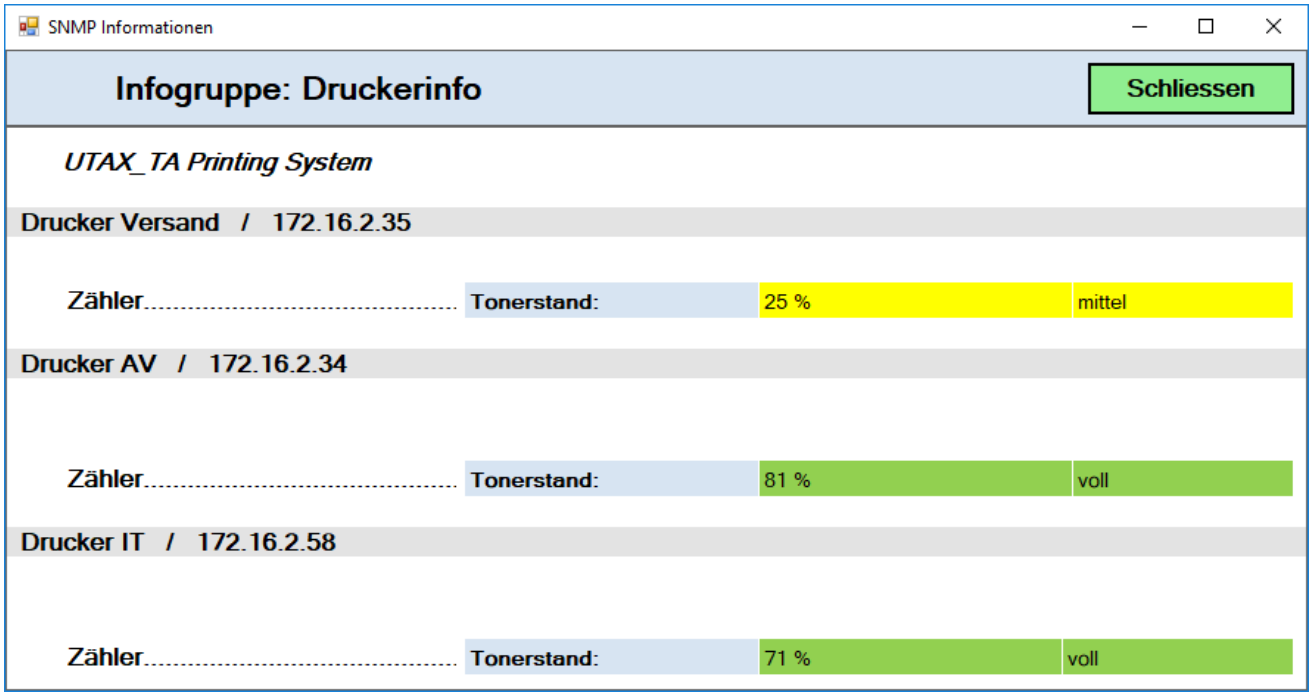
SNMP Infogruppe abrufen

Die im SNMP Kapitel beschriebenen Infogruppen können über den Schnellzugriff ? angerufen werden. Nach Betätigen der Schaltfläche erscheint folgende Anzeige:



Hier muss nun die konfigurierte Infogruppe ausgewählt werden.

Nach Bestätigung mit OK werden die Daten im Hintergrund abgerufen. Das kann je nach Anzahl der zugeordneten Geräte eine Weile dauern. Wenn alle Daten ermittelt sind, dann werden die Werte entsprechend angezeigt. Die nachfolgende Bild zeigt die Darstellung einer Infogruppe:



Die Active Directory Überwachungsleiste

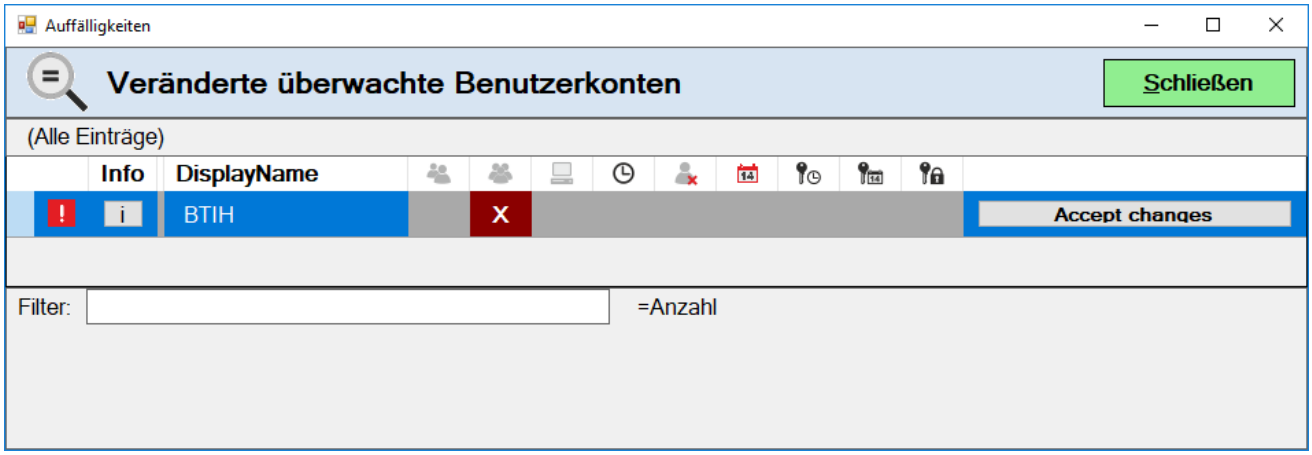
Im unteren Bereich der Überwachung befindet sich die Active-Directory Überwachungsleiste. Hier wird angezeigt, wie viele Ereignisse für eine Überwachungsgruppe aufgetreten sind

Die genaue Funktionsweise ist **unter Active Directory Überwachungsleiste** im Kapitel **Active-Directory Benutzer & Computer** beschrieben.

Benutzerüberwachung

Ist eine Überwachung für Active-Directory Benutzer eingerichtet worden und gibt es eine Abweichung des überwachten Objekts, dann werden die Änderungen in der Active-Directory Überwachungsleiste im Überwachungsmodus mit folgendem Symbol angezeigt.

Durch Klick auf Symbol öffnet sich die Detailanzeige.



Die Symbole zeigen an, in welchem Bereich sich die die Einstellungen seit Einrichtung der Überwachung geändert haben.

Die Symbole haben folgende Bedeutung:

- Änderung der **primären Gruppe**
- Änderung **Gruppenmitgliedschaft**

Änderung der **Anmeldestationen**

Änderung der **Anmeldezeit**

Account wurde **Deaktiviert / Aktiviert**

Änderung des **Ablaufdatums**

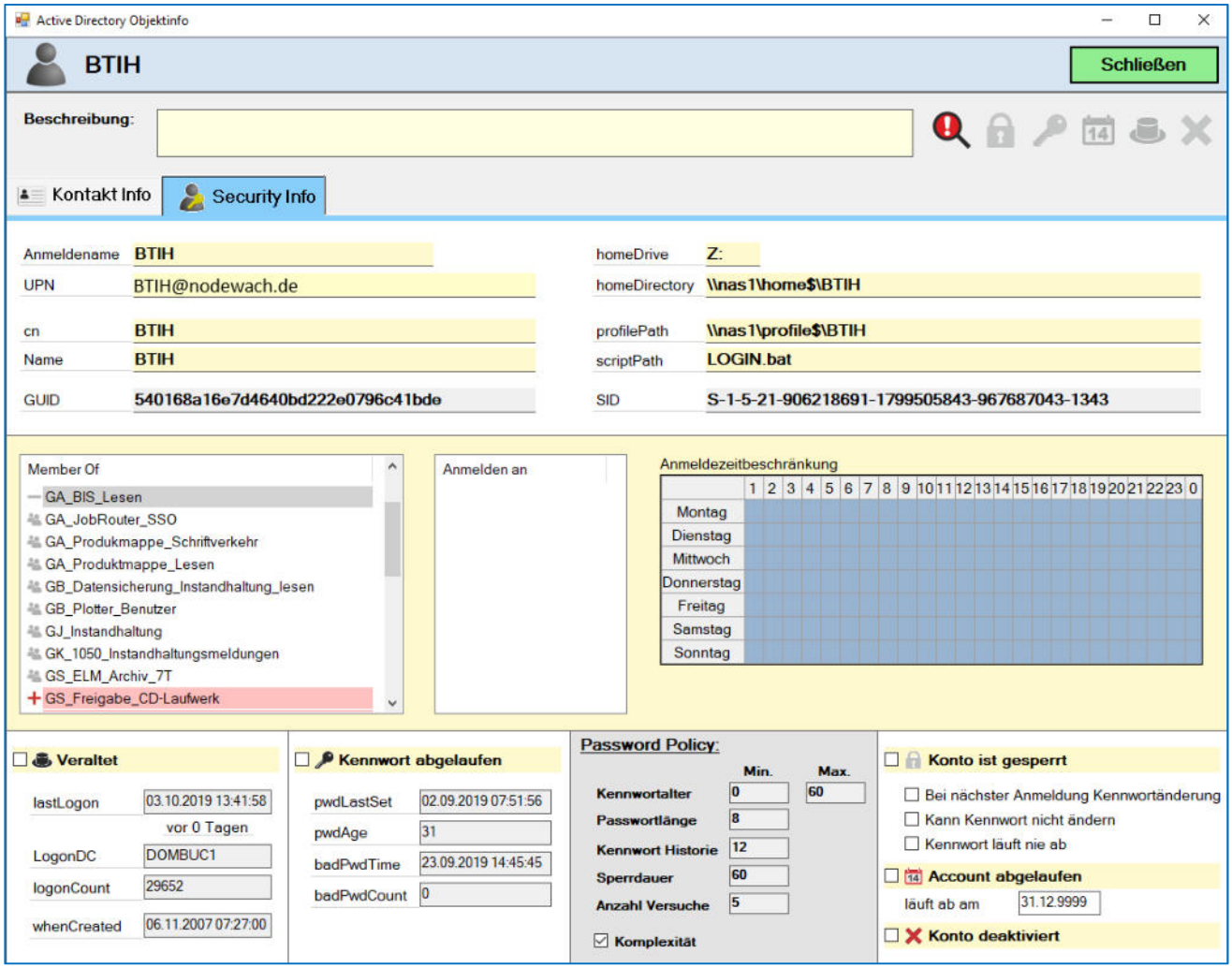
Änderung des **maximalen Kennwortalters**

Änderung an **Kennwort läuft nie ab**

Änderung der Einstellung **Kann Kennwort nicht ändern**

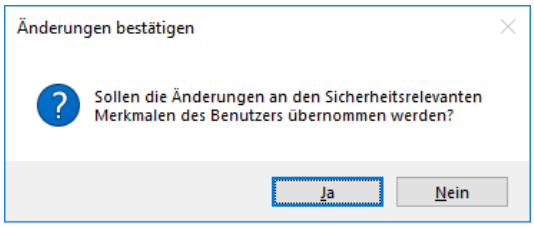
Klickt man auf den Info Button, dann werden die Änderungsdetails angezeigt.

Die nachfolgende Abbildung zeigt Änderungen an den Gruppenmitgliedschaften.



Grau hinterlegte Einträge wurden entfernt, rot hinterlegte Einträge wurden neu hinzugefügt. Änderungen an Passworteinstellungen werden rot hervorgehoben.

Um die Änderungen zu akzeptieren muss man in der vorangegangenen Anzeige lediglich die Schaltfläche **[Accept changes]** klicken. Es erscheint folgende Sicherheitsabfrage:



Wird die Frage mit Ja bestätigt, dann werden die aktuellen Änderungen akzeptiert und der Eintrag aus der Ausnahmeliste entfernt. Die Überwachung beginnt nun mit den neuen Einstellungen wieder von vorne.

Active Directory Gruppenüberwachung

Rechts im Überwachungsbereich befinden sich die Übersichten für die Active Directory Gruppenüberwachung. Die drei Überwachungsebenen werden als Schildsymbole angezeigt.

Die Symbole haben folgende Bedeutung:

Admingruppe

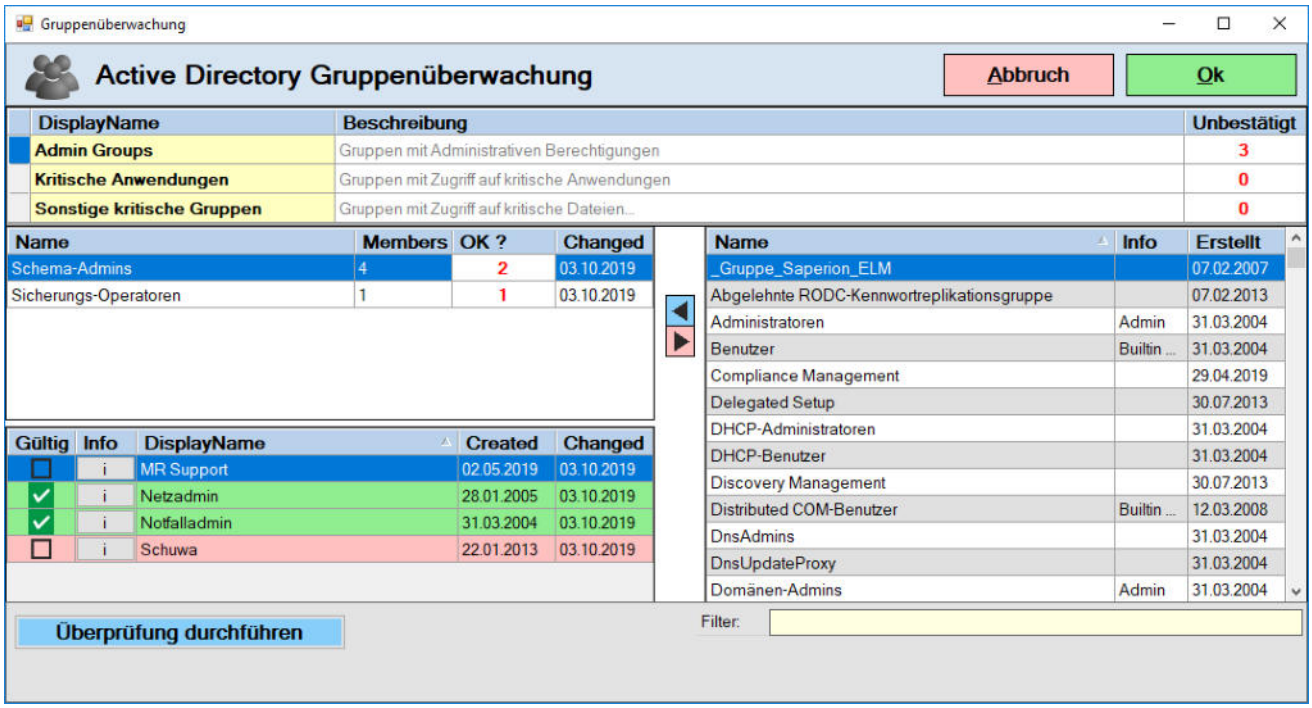
Anwendungsgruppen

Sonstige Gruppen

In der Konfiguration ist das folgender Bereich:

DisplayName	Beschreibung	Unbestätigt
Admin Groups	Gruppen mit Administrativen Berechtigungen	3
Kritische Anwendungen	Gruppen mit Zugriff auf kritische Anwendungen	0
Sonstige kritische Gruppen	Gruppen mit Zugriff auf kritische Dateien...	0

Durch Rechtsklick auf eines der Gruppensymbole kann über das Kontextmenü der Überwachungslauf über den Menüeintrag **Daten aktualisieren** manuell angestoßen werden. Mit einem Linksklick wird die Anzeige der Gruppenüberwachung wie im Kapitel **Active Directory Gruppenmitglieder überwachen** angezeigt.



SQL-Server Überwachung

Ist eine Überwachung für SQL-Server auftragsverlauf eingerichtet, dann wird folgendes Symbol im Überwachungsmodus angezeigt.

Die Zahl im Symbol zeigt die Anzahl der aufgetretenen Fehler. Klickt man auf das Symbol, dann werden die Überwachungsdetails angezeigt.