MICROSENS

Benutzerhandbuch

Netzwerk Management Plattform - Server

NMP Server Version	NMP Server 1.010.x
Dokument Version	2.7
Datum	2013-11-06

MICROSENS
GmbH & Co. KG

Küferstraße 16
59067 Hamm/Germany

Tel. +49 2381 9452-0
FAX +49 2381 9452-100
Email info@microsens.com
Web www.microsens.com

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Lizenzvereinbarung

Die Lizenzvereinbarung regelt die Verwendung der MICROSENS Netzwerk Management Software („NMP") durch den Kunden („Lizenznehmer").

Durch die Installation, die Kopie oder eine anderweitige Verwendung der NMP Software stimmt der Lizenznehmer den Bestimmungen der Lizenzvereinbarung zu und ist an diese gebunden. Falls Sie diesen Bestimmungen nicht zustimmen, dürfen Sie die NMP Software weder installieren noch kopieren oder verwenden.

1.1 Lizenz

MICROSENS gewährt dem Lizenznehmer hiermit unter Maßgabe der nachstehenden Einschränkungen das folgende nicht-exklusive, nicht-übertragbare Recht zur Verwendung der NMP Software:

1. Die NMP Software wird lizensiert und nicht verkauft. Der Lizenznehmer darf eine Kopie der NMP Software auf einem einzigen Computer installieren und verwenden und außer zum Zweck einer Backup-Kopie der NMP Software keine weitere Kopie anfertigen. Diese NMP Softwarelizenz darf nicht mehrfach genutzt oder auf mehreren unterschiedlichen Computern gleichzeitig verwandt werden.
2. Die NMP Software wird als einzelnes Produkt lizensiert. Die einzelnen Bestand-teile dürfen weder getrennt voneinander auf mehr als einem Computer noch getrennt von den anderen Bestandteilen genutzt werden.
3. Der Lizenznehmer darf die NMP Software nicht an Dritte vermieten oder verleasen.

1.2 Gewährleistung

Die NMP Software und jedwede zugehörige Dokumentation werden ohne jegliche Mängelgewähr, weder ausdrücklich noch impliziert, bereitgestellt. Dies umfasst, ist jedoch nicht darauf beschränkt, die implizierte Gewährleistung der allgemeinen Gebrauchsfähigkeit oder der Eignung für einen speziellen Zweck.

Dem Lizenznehmer obliegt das gesamte Risiko, das aus der Verwendung oder den Funktionen der NMP Software erwächst, einschließlich, jedoch nicht darauf beschränkt, von Schäden oder dem Verlust von Geschäftsgewinnen, Datenverlust, Unterbrechung der Geschäftsabläufe, Verlust geschäftlicher Informationen oder materiellem Verlust.

1.3 Reverse-Engineering, Decompilation und Disassemblierung

Sie dürfen die Netzwerk Management Plattform Software keinem Reverse-Engineering unterziehen und sie nicht dekompilieren oder disassemblieren mit Ausnahme von und nur in dem Maß wie diese Aktivität — abweichend von dieser Beschränkung — ausdrücklich von geltendem Recht erlaubt ist.

1.4 Urheberrecht

2 Einführung

Das Management von Geräten umfasst deren ferngesteuerte Überwachung, Konfiguration und Administration. Die Netzwerk Management Plattform Software ist ein sehr leistungsfähiges Werkzeug, das den Netzwerkadministrator bei diesen Aufgaben unterstützt.

Die Netzwerk Management Plattform Software stellt eine einfach zu benutzende grafische Schnittstelle für die Verwaltung aller verwaltbaren Geräte bereit.

Eine Liste der gegenwärtig unterstützten Geräte ist in der gemeinsam mit der Software gelieferten Datei „devices.txt" enthalten.

2.1 Netzwerkadministration

Die Netzwerk Management Plattform Software implementiert Funktionen zur automatischen Erkennung aller verwaltbaren Geräte in diesem Netzwerk. Diese Konfiguration ist in einer Datenbank gespeichert und wird für die Überwachung des Netzwerkstatus' verwandt.

2.2 Netzwerküberwachung

Der aktuelle Status aller aktiven verwaltbaren Geräte im Netzwerk kann automatisch mittels der Geräteliste erfasst werden. Der Status wird über eine grafische Schnittstelle angezeigt

2.3 Netzwerkkonfiguration

Die Hardwarekonfiguration eines verwaltbaren Geräts, wie beispielsweise die Portkonfiguration der Verkehrspriorisierung, kann für einzelne Geräte oder für alle ähnlichen Geräte im Netzwerk gleichzeitig angezeigt und verändert werden.

3 Installation

3.1 Systemanforderungen

Der Netzwerk Management Plattform Server wurde für den Betrieb auf Personal Computern oder dedizierten Servermaschinen mit beliebigen Microsoft Windows oder Linux Betriebssystemen, 1GB RAM, 1GB freiem Speicherplatz entwickelt.

Für den Netzwerkzugang muss eine Netzwerkschnittstelle mit TCP/IP-Stack installiert und konfiguriert sein.

Die Client-Seite bezieht sich auf Abläufe, die vom Client im Rahmen einer Client-Server Beziehung in einem Computernetzwerk auftreten.

Als Client dient ein standard Web Browser, der auf einem lokalen Computer oder einer lokalen Workstation des Benutzers betrieben wird. Es können alle Betriebssysteme (Windows, Linux, Mac OS) genutzt werden. Der Client verbindet sich mit dem Server, die empfohlene Bildschirmauflösung beträgt mindestens 1280*1024 Punkte.

3.1.1 Unterstützte Web Browser

- Internet Explorer Releases 6, 7, 8 oder neuer
- Mozilla Firefox 3 oder neuer
- Safari 3, 4 oder neuer
- Opera 9.6 oder neuer

Java Script muss im Web Browser aktiviert sein. Es müssen keine weiteren Plug-Ins installiert werden.

3.2 Software Installation

Zur Installation der NMP Software starten Sie die mitgelieferte Installationsdatei und folgen den Anweisungen des Installationsprogramms. Für die Installation der NMP Software benötigen Sie Administratorrechte.

Für die Benutzung der Netzwerk Management Plattform sollten Sie eine gültige Lizenzdatei besitzen.

NMP Server verwendet zur Speicherung aller Daten (z.B. der Geräteliste, der Geräteparameter, der Protokolle sowie der Konfigurationsdateien etc.) die Apache Derby Datenbank. Für die NMP Server Applikation wird weiterhin Jetty als Web Applikationsserver genutzt.

3.2.1 Willkommen beim MICROSENS NMP Server Setup

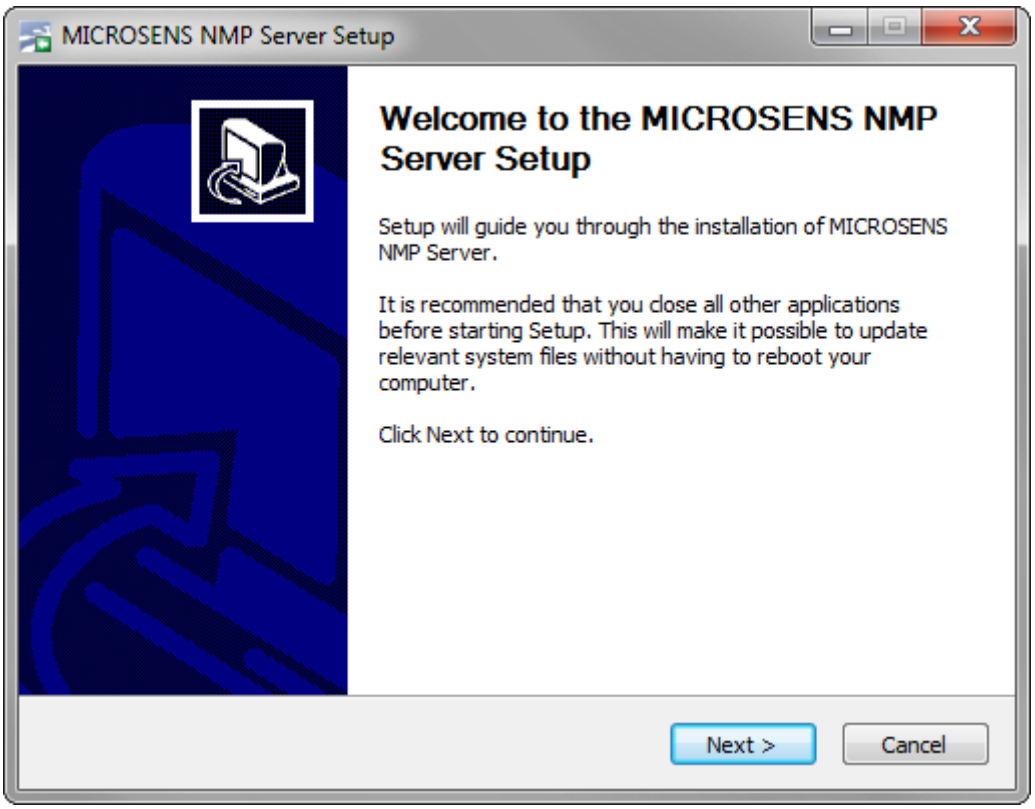

Abbildung 1: Setup Willkommensanzeige

Klicken Sie zur Anzeige der Lizenzvereinbarung auf die Schaltfläche „Weiter”.

3.2.2 Lizenzvereinbarung

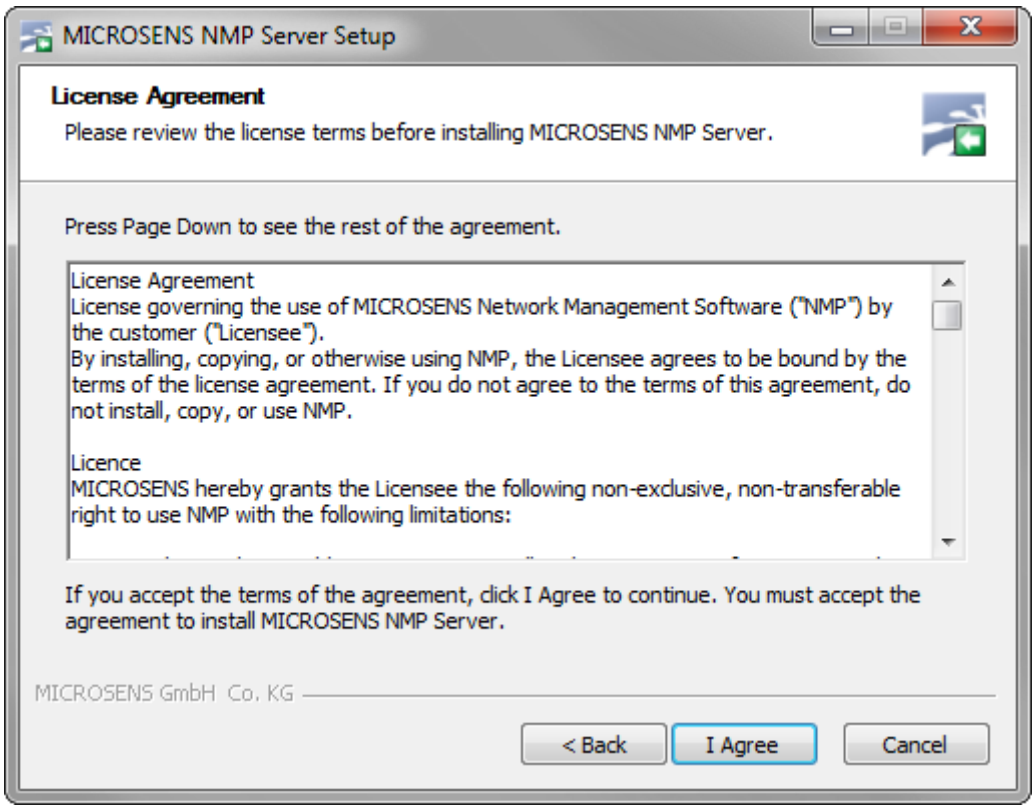

Abbildung 2: Lizenzvereinbarung

Nachdem Sie die Lizenzvereinbarung gelesen haben klicken Sie auf die Schaltfläche „I Agree". Anschließend gelangen Sie zur Auswahl des Installationsordners.

3.2.3 Auswahl des Installationsordners

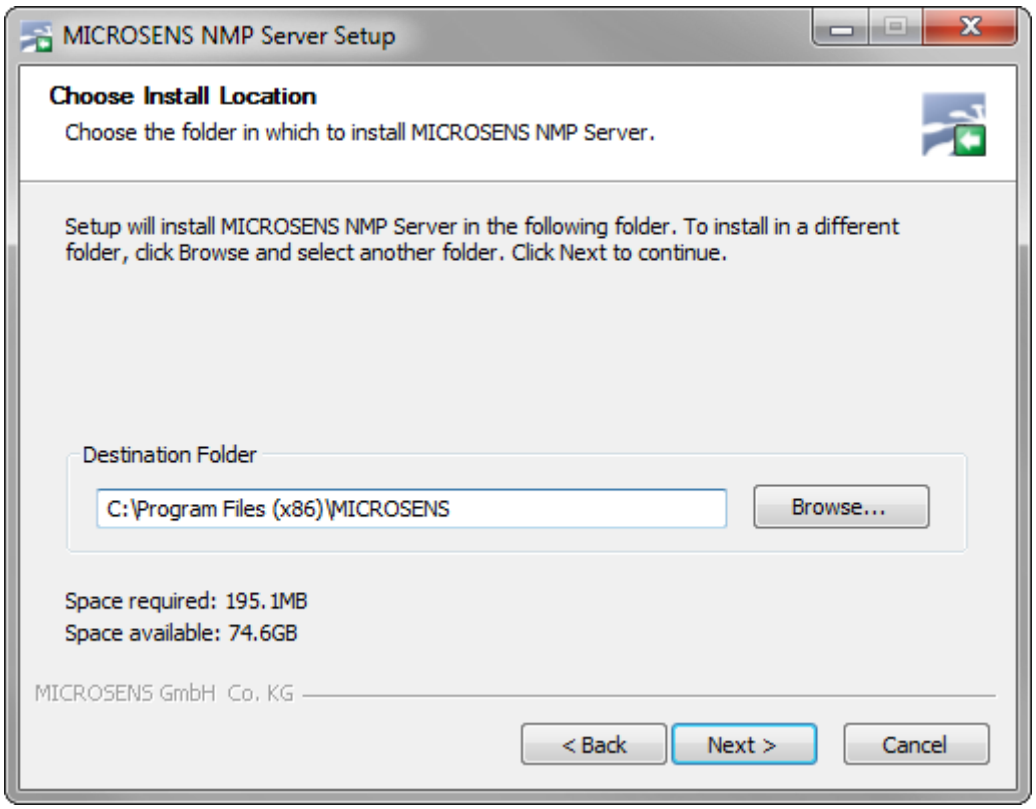

Abbildung 3: Dialog „Auswahl des Installationsordners"

Hier können Sie den Installationsordner der NMP Server Software auswählen. Mit einem Klick auf die Schaltfläche „Next" gelangen Sie zur Auswahl der einzelnen Installationsoptionen.

3.2.4 Installationsoptionen

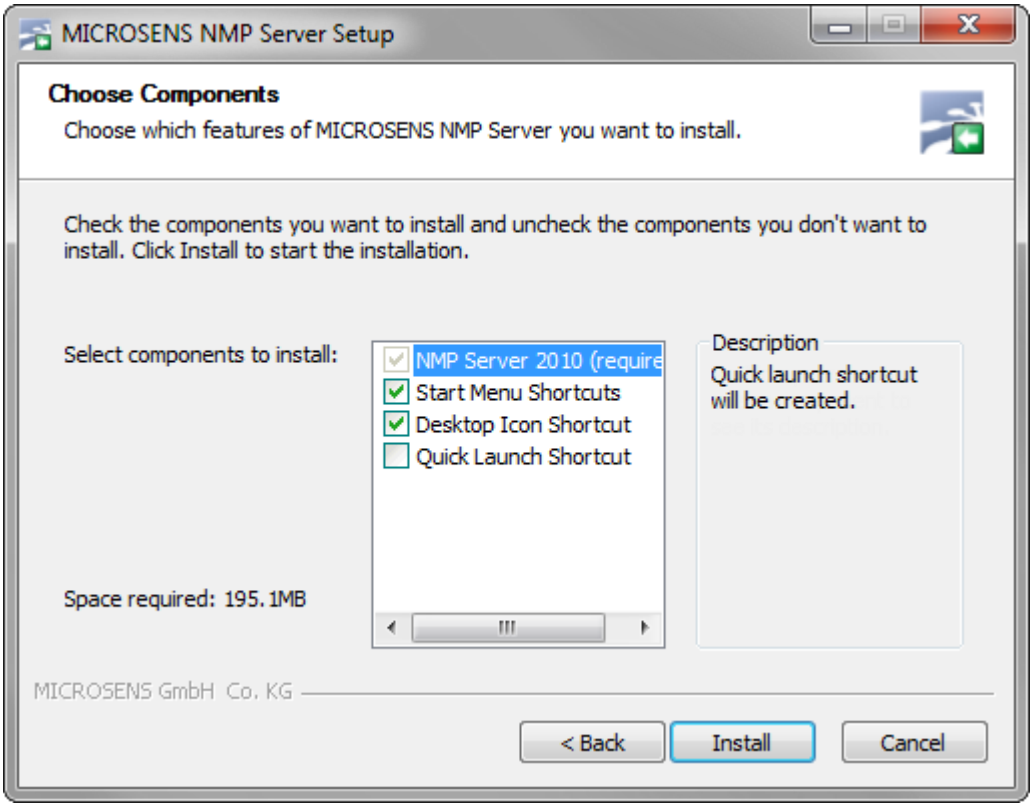

Abbildung 4: Dialog „Produktauswahl”

Entsprechend Ihrer Anforderungen können Sie die Installationsoptionen aus- bzw. abwählen. Die verfügbaren Optionen sind: Installation einer Verknüpfung im Startmenü, Installation eines Desktop-Icons, Installation eines Icons in der Schnellstartleiste. Zum Start der Installation auf Ihrem System klicken Sie auf die Schaltfläche „Install”.

Nach dem erfolgreichen Abschluss der Installation ist die Netzwerk Management Plattform Software zum Start bereit.

3.3 Erste Schritte

3.3.1 Auswahl der Lizenzdatei

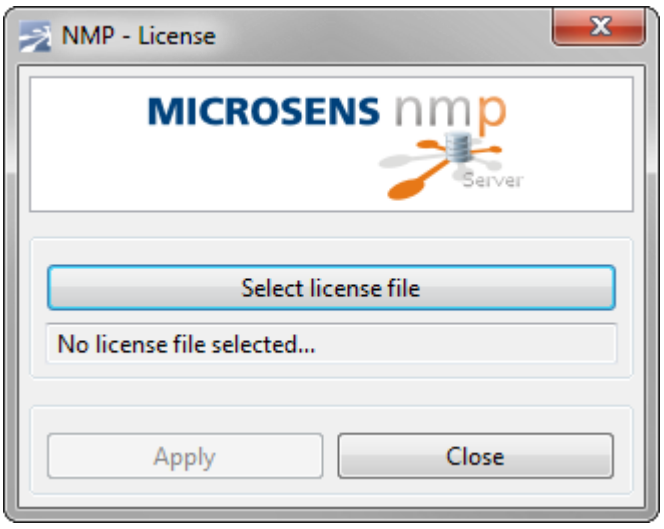

Abbildung 5: Dialog „Auswahl der Lizenzdatei"

Zur Nutzung der Netzwerk Management Plattform ist eine gültige Lizenzdatei erforderlich. Falls keine Lizenz ausgewählt ist (insbesondere nach der Installation der Software) werden Sie zur Auswahl einer Lizenzdatei aufgefordert.

Die standard NMP Server Lizenz ermöglicht die Konfiguration einer unbegrenzten Anzahl unterschiedlicher Benutzerkonten. Gleichzeitig können maximal 5 verschiedene Benutzer auf den Server zugreifen. Für die Erhöhung der maximalen Anzahl von Benutzern, die gleichzeitig auf den Server zugreifen können, ist der Erwerb zusätzlicher Lizenzen erforderlich.

Verfügbare Lizenzen sind:

- **MS200164-E** – Trial, Evaluationsversion
- **MS200164-n** – Basislizenz, bis zu 5 gleichzeitige Benutzer, n Jahre Wartungszeitraum
- **MS200164-U** – Basislizenz, bis zu 5 gleichzeitige Benutzer, unbegrenzter Wartungszeitraum
- **MS200165-n** – Wartungsupgrade (weitere n Jahre Wartung)
- **MS200166-Cn** – zusätzliche n Benutzerkonten (erhöht die Anzahl der möglichen gleichzeitig zugreifenden Benutzer)

Der Begriff „Wartungszeitraum" bezeichnet den Zeitraum, für den der Lizenznehmer kostenfreie Updates in Anspruch nehmen kann. Im Anschluss an diesen Zeitraum stehen keine kostenfreien Updates mehr zur Verfügung und der Lizenznehmer sollte eine **MS200165-n** Lizenz zur Verlängerung des Wartungszeitraums erwerben.

3.3.2 NMP Server Manager

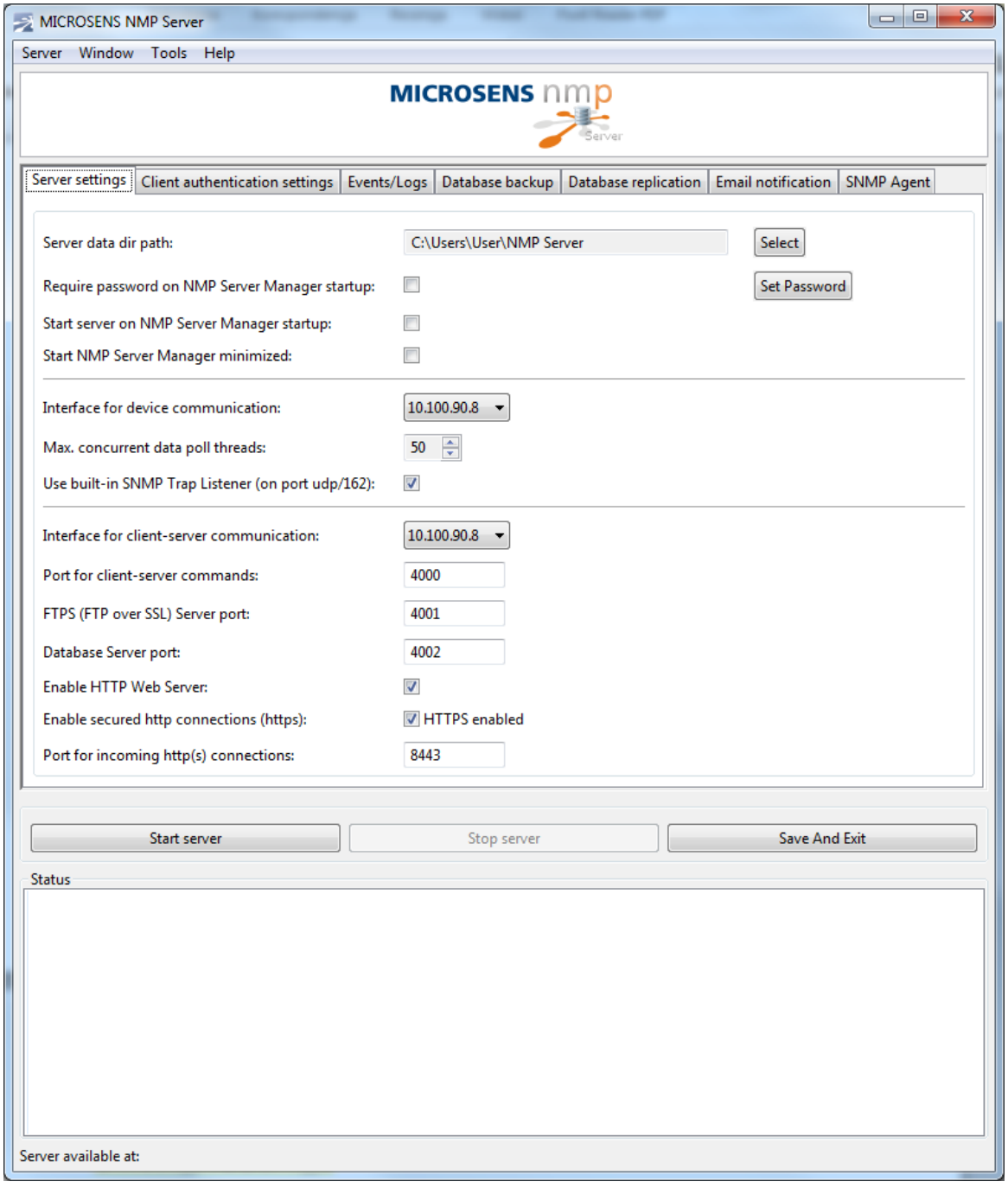

Abbildung 6: Dialog „Server Manager"

Das Hauptfenster der Netzwerk Management Plattform Server Manager besteht aus vier Hauptelementen:

- *Hauptmenü* (1)
- *Registerkarten* (2)
- *Server Schaltflächen* (3)
- *Nachrichtenfenster* (4)

Die folgenden Abschnitte enthalten detaillierte Beschreibungen dieser Elemente.

3.3.3 Basiskonfiguration

Beim erstmaligen Start sollte der Server Administrator alle Einstellungen der Applikation konfigurieren. Eine detaillierte Beschreibung ist im Abschnitt *Registerkartenansicht der Server Konfiguration* enthalten.

3.3.4 Software-Aktualisierung

Für ein Software Update muss der NMP Server gestoppt und das Fenster „NMP Server Manager" geschlossen werden. Alternativ muss der NMP Server Dienst gestoppt werden, falls NMPS als Windows Dienst gestartet wurde. Anschließend wird die neue Version installiert. Während der Installation wird derselbe Installationspfad wie für die vorherige Version ausgewählt. Alle Applikationsdateien werden daraufhin aktualisiert.

NMP Server bietet die Möglichkeit einer Überprüfung auf verfügbare Updates. Siehe hierzu auch den Befehl „NMP Server Updater" im Menü „Tools".

4 NMP Server Manager

Das NMP Server Manager Applikationsfenster beinhaltet Elemente zur Konfiguration des Servers und zur Statusüberwachung der Applikation.

4.1 Hauptmenü

Über das NMP Hauptmenü erhalten Sie Zugang zu Funktionen wie Starten und Stoppen des Servers, Interaktion mit einer Applikation oder Hilfe.

4.1.1 Server

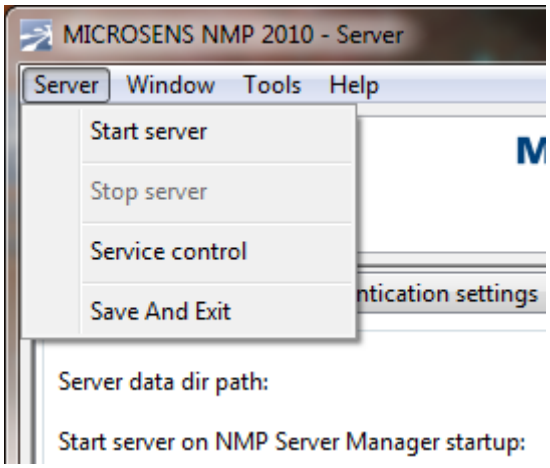

Abbildung 7: Menü „Server"

Start server: Startet den NMP Server, der Server Manager startet den konfigurierten http-Server (falls aktiviert) und die Datenbank

Stop server: Stoppt den NMP Server

Service control: Installiert bzw. deinstalliert den NMP Server als Windows Dienst. Detaillierte Informationen befinden sich im Abschnitt *NMP Server als Windows Dienst*.

Save And Exit: Speichert die aktuelle Konfiguration und schließt das NMP Server Manager Fenster

4.1.2 Fenster (Window)

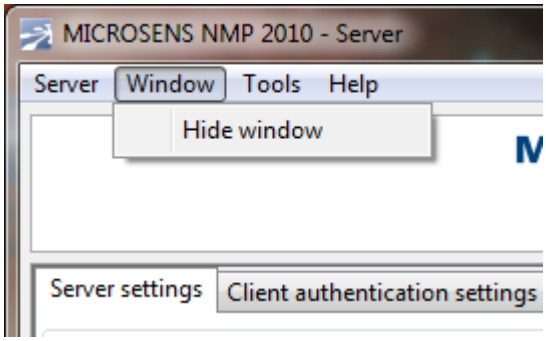

Abbildung 8: Menü „Window”

Hide window (Fenster ausblenden): Schließt das NMP Server Manager Fenster. Über das Symbol im Infobereich kann weiterhin auf die Applikation zugegriffen werden.

4.1.3 Extras (Tools)

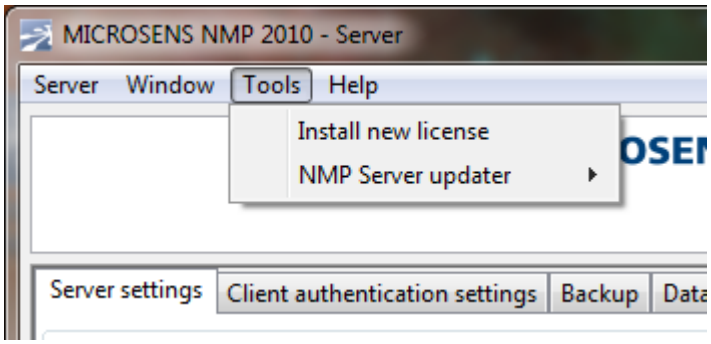

Abbildung 9: Menü „Tools”

Install new licence: Zur Nutzung der Network Management Platform ist eine gültige Lizenzdatei erforderlich.

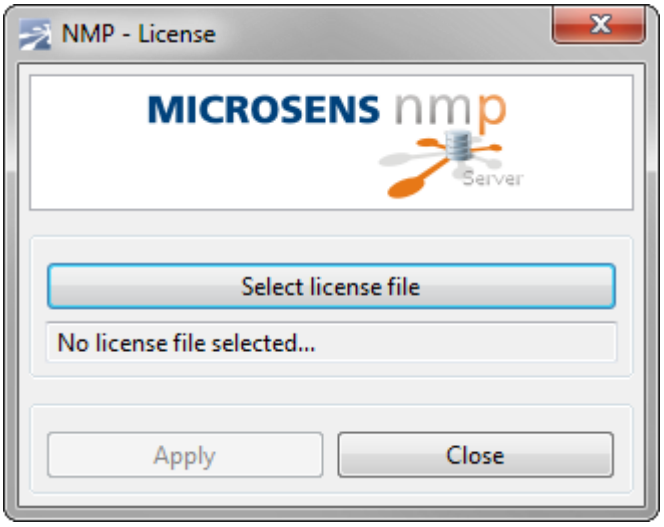

Abbildung 10: Fenster „Install New Licence"

Verwenden Sie zur Aktualisierung Ihrer Lizenz den Befehl "Install new licence". Dies ist beispielsweise nach Ablauf der Evaluierungsfrist erforderlich. Wählen Sie die Lizenzdatei aus und klicken Sie auf die Schaltfläche „Apply". Nach erfolgreicher Validierung der neuen Lizenzdatei wird die gegenwärtige Lizenzdatei aktualisiert. Bitte kontaktieren Sie zum Erhalt einer NMP Server Lizenzdatei MICROSENS.

Das "NMP Server updater – Check for Update" Werkzeug (Update-Prüfung) überprüft den MICROSENS Server auf neuere Versionen der Applikation. Sollte ein Update verfügbar sein, wird eine Release-Information in Verbindung mit einer Option zum Download des neuesten Installers angezeigt.

Nach dem erfolgreichen Download sollte der neue Installer entpackt und installiert werden. Die aktuelle NMP Server Instanz sollte vor der Installation einer neuen Version geschlossen werden.

Bitte bedenken Sie, dass eine neuere Version des NMP Servers nur dann installiert werden kann, wenn die installierte Lizenz gültig und die Wartungsperiode aktiv ist. Das "Check for Update" Werkzeug zeigt eine Warnung an, falls die Wartungsperiode abgelaufen sein sollte.

NMP Server updater – Proxy settings: Konfiguriert den vom NMPS Updater genutzten Proxy Server („Check for Update").

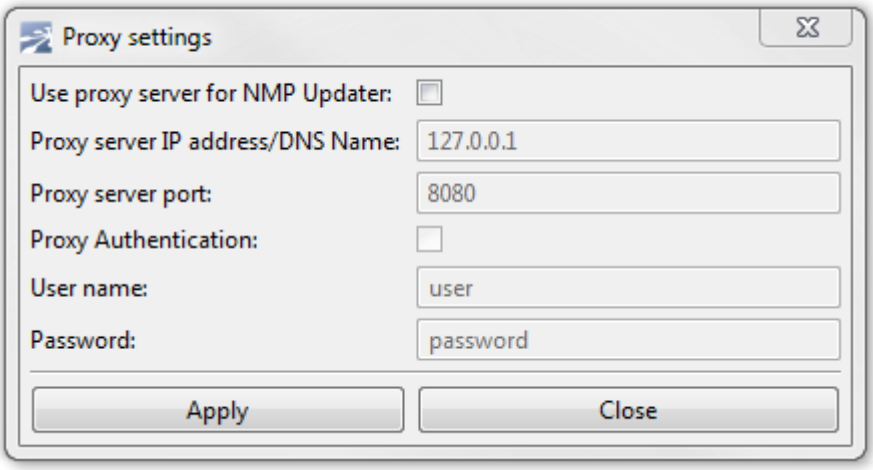

Abbildung 11: Dialog „Proxy Settings”

4.1.4 Hilfe (Help)

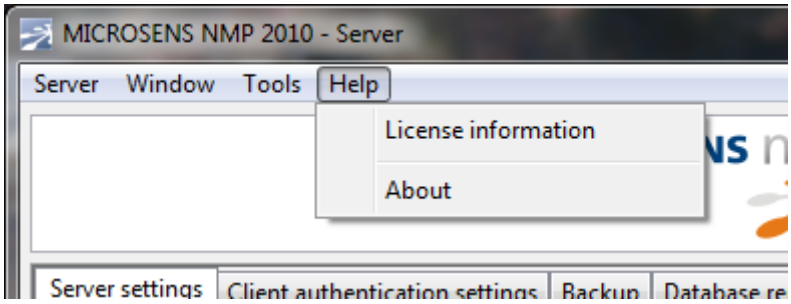

Abbildung 12: Fenster „Help”

NMP Server – help: Dieser Befehl zeigt die NMP Server Hilfedatei an. Die Handbücher werden im PDF-Format bereitgestellt. Zum korrekten Öffnen der Datei sollte auf dem System ein PDF-Reader installiert sein.

Licence information: Dieser Befehl zeigt Informationen über die gegenwärtig installierte Lizenzdatei an. Zusätzlich kann der NMP Lizenztext angezeigt werden.

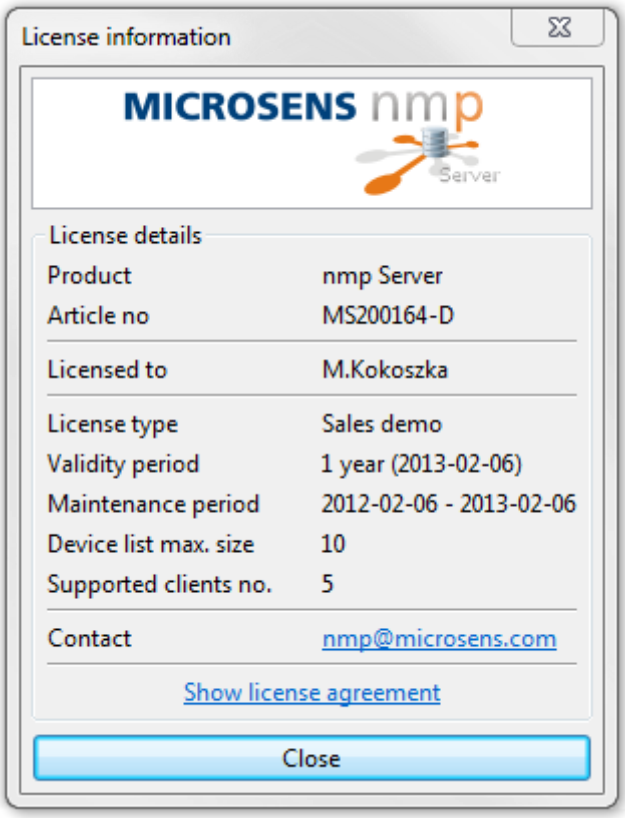

Abbildung 13: Fenster „Licence Information"

About: Zeigt Informationen über die NMP Server Release-Version an.

Abbildung 14: Fenster „About"

4.2 Registerkartenansicht der Server-Konfiguration

Die NMP Server Manager Registerkartenansicht ermöglicht die Konfiguration aller Applikationsparameter.

4.2.1 Servereinstellungen (Server Settings)

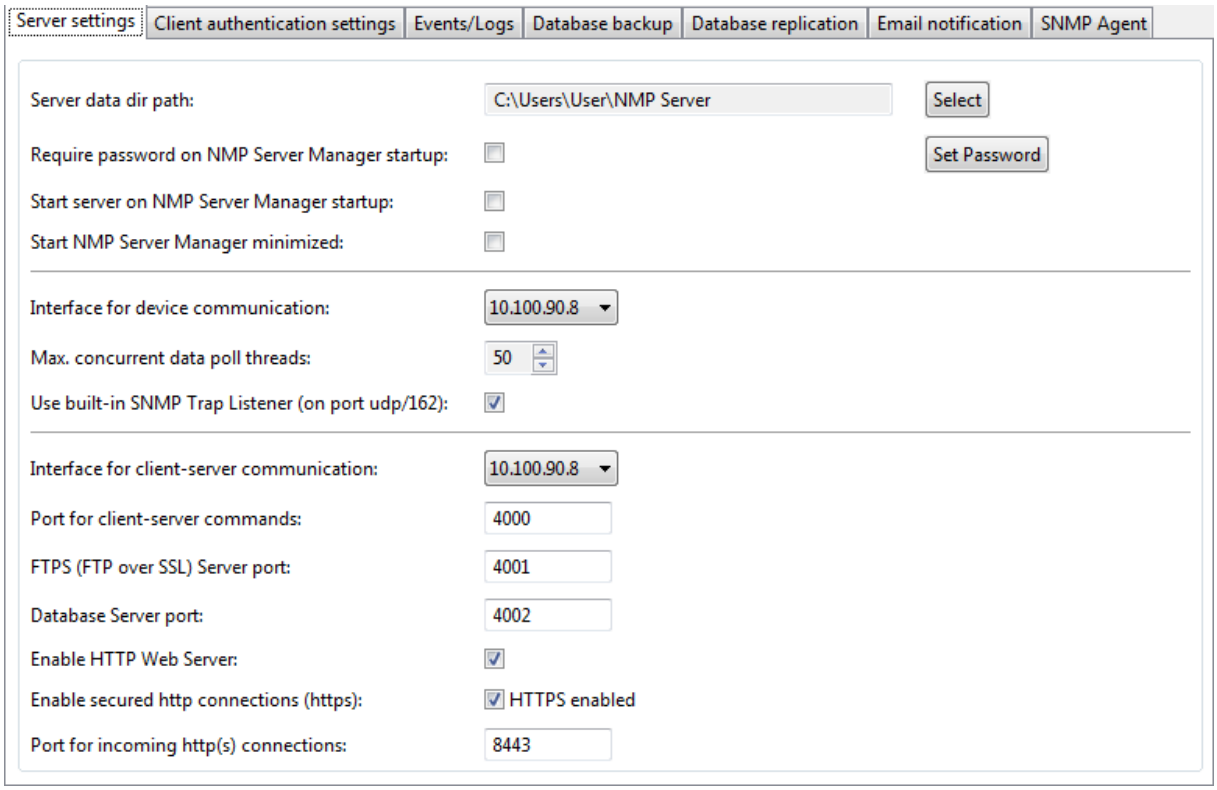

Abbildung 15: Dialog „Server Settings”

Server data dir path: An dieser Stelle wird das Verzeichnis eingestellt, in dem NMP Server alle erforderlichen Konfigurationsdateien und Datenbanken speichert. Der Standardordner ist „$USER_HOME\NMP Server”. An dem ausgewählten Ort wird ein Verzeichnis „NMP Server” erstellt.

Require password on NMP Server Manager starting: Bei Aktivierung dieser Option wird vor dem Öffnen des NMP Server Managers eine Passwortanfrage angezeigt. Das Passwort kann durch Auswahl der Schaltfläche „Set Password” eingestellt werden. Diese Funktion ermöglicht den Schutz des Servers vor einer Umkonfiguration.

Start server on NMP Server Manager startup: Startet beim Start des NMP Server Managers automatisch den Server (HTTP, Datenbank und Gerätedaten Collector). Wenn der NMP Server Manager den Startup Applikationen des Betriebssystems hinzugefügt wurde, startet der NMP Server automatisch und steht nach einem Neustart des Betriebssystems zur Verfügung.

Start NMP Server Manager minimized: Startet ein minimiertes NMP Server Manager Fenster. Das Applikationsfenster ist über das Icon im Infobereich verfügbar.

Interface for device communication: Die für die Kommunikation mit den verwalteten Geräten zu verwendende Netzwerkschnittstelle. In komplexeren Fällen, bei denen die Server-Hardware (PC) mehr als eine NIC aufweist, kann eine Schnittstelle (vom sicheren lokalen Netzwerk aus zugänglich) für die Gerätekommunikation genutzt werden. Eine andere Schnittstelle (vom externen Netzwerk aus zugänglich) kann für den Client-Zugang genutzt werden. Hierdurch haben Clients keinen direkten Zugriff auf die verwalteten Geräte. Auf die Geräte kann nur über die NMP Server Applikation zugegriffen werden.

Max. concurrent data poll threads: Dieser Parameter wird zur Definition der Anzahl der Geräte genutzt, die zu einem beliebigen Zeitpunkt gleichzeitig abgefragt werden können. Bei langsameren PCs, hochbelasteten Netzwerken oder langsamen Netzwerkverbindungen (z.B. langsamen VPN-Verbindungen) wird eine Reduzierung der Zahl gleichzeitiger Abfragen empfohlen.

Use built-in SNMP Trap Listener (on port udp/162): NMP Server beinhaltet einen integrierten SNMP Trap-Empfänger zum Empfang der von Netzwerkgeräten ausgesandten Traps. Der Trap-Empfänger ist in der Standardeinstellung deaktiviert, kann aber auch aktiviert werden, falls kein alternativer Trap-Empfänger verwandt wird.

Interface for client-server communication: Die Netzwerkschnittstelle, die für den Client-Zugang genutzt wird (NMP-Client). Falls der HTTP-Server für den Web Client-Zugang aktiviert ist, wird diese Schnittstelle auch für den integrierten HTTP-Server verwandt.

Port for client-server commands: Der von der NMP Client-Applikation für die Kommunikation mit dem NMP Server genutzte Port (standardmäßig 4000).

FTPS (FTP over SSL) Server port: Der integrierte FTPS-Server wird von der NMP Client-Applikation für die Synchronisierung der Gerätelisten und der Firmware-Aktualisierungen genutzt (standardmäßig 4001).

Database Server port: Vom integrierten Datenbank-Server für den NMP Client Zugang genutzter Port (standardmäßig 4002).

Enable HTTP Web Server: Aktiviert oder deaktiviert den für den Web Client Zugang genutzten integrierten HTTP-Server

Enable secure HTTP connections (https): NMP Server kann sichere HTTP-Verbindungen für den Web-Zugang aktivieren. Die HTTPS-Verbindungen sind verschlüsselt und gestalten die Kommunikation zwischen den Clients und dem Server hierdurch sicherer.

Port for incoming HTTP(s) connections: Für den HTTP(s)-Server zu verwendender Port. Standardmäßig verwendet NMP Server den Port 8080 für standard HTTP- und 8443 für HTTPS-Verbindungen.

Für die Verwendung durch den NMP Server konfigurierte Portnummern müssen in den installierten Firewalls freigegeben sein.

4.2.2 Einstellungen für die Client-Authentifizierung

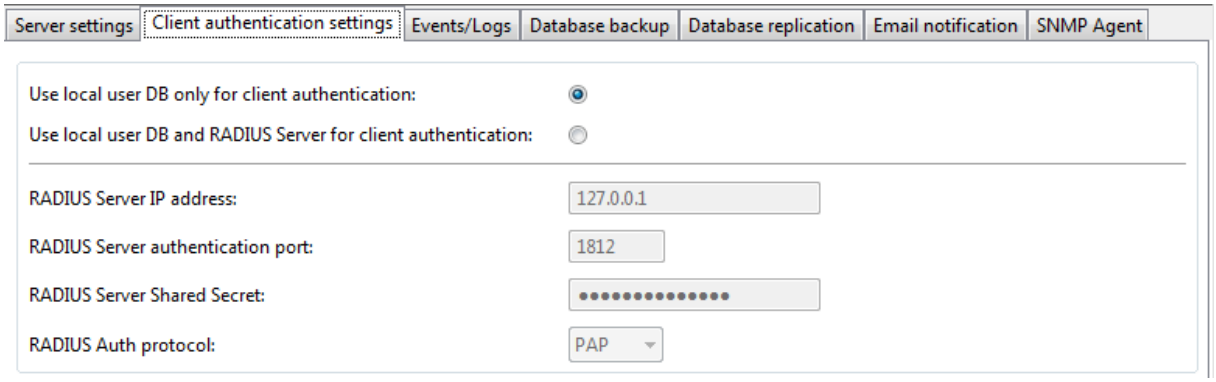

Abbildung 16: Dialog „Client Authentication Settings”

Use local user database only for client authentication: NMP Server verwendet für die Benutzer-Authentifizierung ausschließlich die in der lokalen Datenbank enthaltenen Informationen.

Use local user database and RADIUS-Server for client authentication: NMP Server verwendet den definierten RADIUS-Server zur Authentifizierung des Benutzers. Das lokale Benutzerkonto (in der lokalen NMP Server-Datenbank) wird automatisch angelegt, falls das Konto nicht bereits existiert. NMP Server kann einen neuen Benutzer nur dann authentifizieren und eine lokales Konto erzeugen, wenn die Anzahl der vorhandenen Konten geringer ist als die Anzahl der durch die NMP Server-Lizenz erlaubten Benutzerkonten. Der Zugang zum NMP Server wird nur dann gewährt, wenn der RADIUS-Server die „ACCESS ACCEPT” Nachricht retourniert und ein lokales Benutzerkonto mit dem richtigen Login und Passwort vorhanden ist.

RADIUS-NMP Server -> Zuordnung der Benutzerrechte:

RADIUS Benutzerstufe (Service Typ)	NMP Server Benutzerstufe
Login User (1)	User
NAS Prompt User (7)	Manager
Administrative User (6)	Administrator
Callback Administrative (11)	System Administrator

Beispiel für FreeRADIUS („Benutzer” Datei):

admin Cleartext password := "admin"
Service type = Administrative user

sysadmin Cleartext password := "sysadmin"
Service type = Login user

manager Cleartext password := "manager"
Service type = NAS prompt user

user Cleartext password := "user"
Service type = Login user

Bei diesem Authentifizierungsverfahren wird der RADIUS-Server als Master-Authentifizierungsserver betrachtet. Bei einer Änderung der Benutzerstufe (Servicetyp) oder des Benutzerpassworts auf dem RADIUS-Server aktualisiert NMP Server automatisch das lokale Benutzerkonto. WICHTIG: In der lokalen NMPS-Datenbank muss wenigstens ein Benutzer mit „sysadmin” Rechten angelegt sein. NMP Server wird die Änderung einer Benutzerstufe eines lokalen Kontos nicht erlauben, falls anschließend kein Benutzer mit „sysadmin” Rechten mehr in der lokalen Datenbank vorhanden wäre (es muss wenigstens ein „sysadmin” existieren).

Nach der Löschung eines Benutzerkontos vom RADIUS-Server wird das lokale NMPS-Konto nicht automatisch gelöscht. Der Systemadministrator sollte das Benutzerkonto manuell in der lokalen NMP Server-Datenbank löschen.

Bitte bedenken Sie, daß die Anzahl der auf einem RADIUS-Server definierten Benutzer des NMP Servers der Anzahl der über die Lizenzdatei definierten Benutzerkonten des NMP Servers entsprechen sollte.

RADIUS-Server IP address: Die IP-Adresse des RADIUS-Servers

RADIUS-Server authentication port: Der vom RADIUS-Server für die Authentifizierung genutzte Port. Die Standardeinstellung ist 1812.

RADIUS-Server Shared Secret: Das während des Authentifizierungsvorgangs genutzte RADIUS-Server Shared Secret (Passwort). Die Standardeinstellung lautet „default_secret”

RADIUS Auth protocol: Das vom RADIUS-Server verwandte Authentifizierungsverfahren (PAP oder CHAP).

4.2.3 Datenbank-Einstellungen

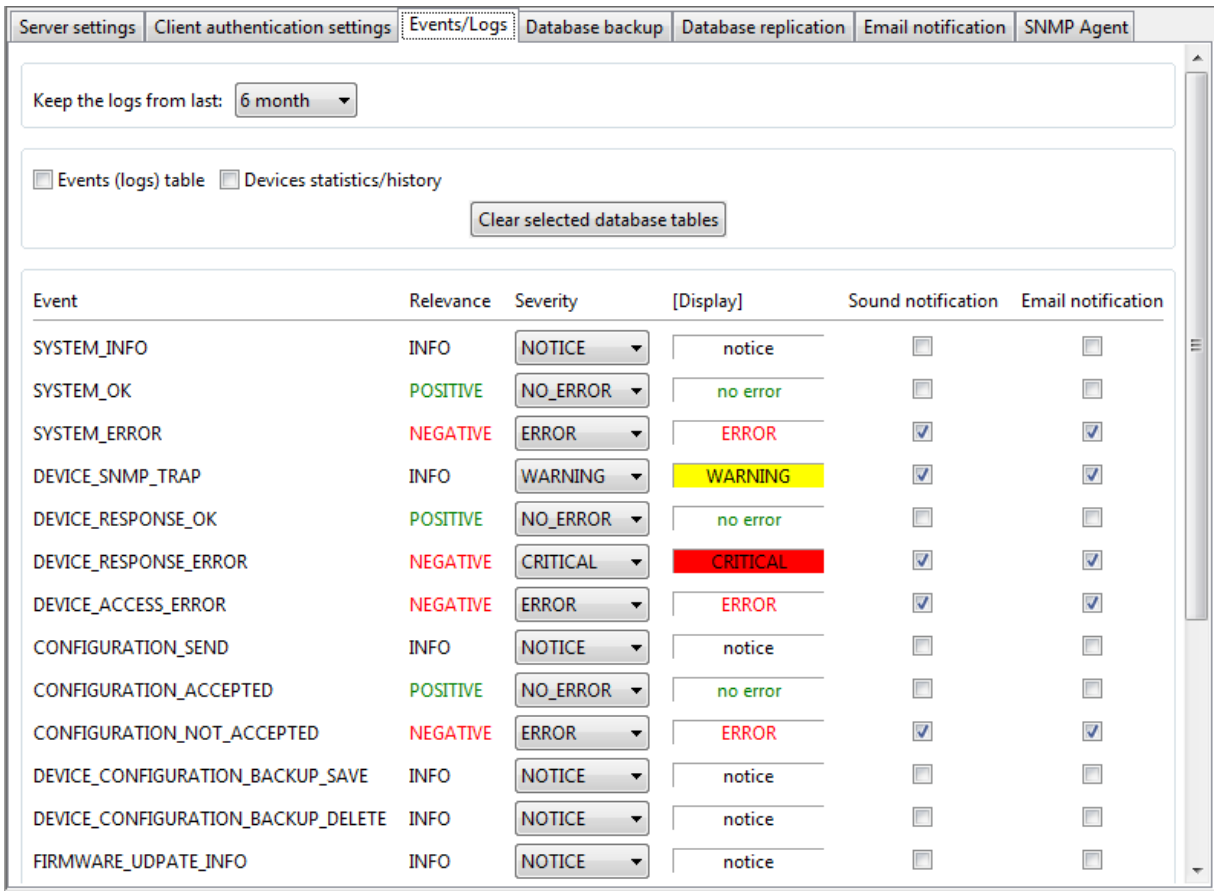

Abbildung 17: Dialog „Database Settings”

Keep the logs from last n months: Zur Beschränkung der Datenbankgröße löscht NMP Server die ältesten Protokolleinträge aus der Datenbank (Geräte-protokolle, Benutzerprotokolle, Gerätestatistiken). In der Standardeinstellung löscht NMP Server alle Protokolle, die älter als ein Monat sind. Die Protokolle können für einen maximalen Zeitraum von 12 Monaten gespeichert werden. NMP Server bereinigt die Datenbank jeden Tag um 02:00 Uhr (AM).

Dieses Register ermöglicht auch die manuelle Bereinigung der Datenbank-tabellen. Hierzu werden die zu bereinigenden Tabellen manuell ausgewählt und die Schaltfläche „Clear selected database tables” betätigt. Bei diesem Vorgang werden alle Protokolleinträge der ausgewählten Tabellen gelöscht.

Events configuration: Hier können aller NMP Server-Events konfiguriert werden. Es existieren viele unterschiedliche Arten von Protokollnachrichten mit unterschiedlicher Relevanz:

- INFO – informatives Ereignis
- POSITIVE – positive Nachricht (kein Fehler)
- NEGATIVE – negative Nachricht (Warnung, Fehler, kritisch)

Jedem Ereignis wird automatisch eine Prioritätsstufe entsprechend seiner Relevanz zugewiesen. Der Benutzer kann die Relevanzstufe nicht verändern. Weiterhin wird jedem Ereignis ein modifizierbarer Schweregrad zugewiesen. Es gibt sechs verschiedene Stufen:

- DISABLED – das Ereignis wird keine Protokolleintrag verursachen (nicht angezeigt oder nicht gespeichert)
- NOTICE – informatives Ereignis, das keine besondere Aufmerksamkeit des Benutzers erfordert (z.B. Systemnachrichten)
- NO_ERROR – Benachrichtigung über eine erfolgreiche Aktion (z.B. eine erfolgreich angewandte Konfiguration)
- WARNING – Warnmeldung mit niedriger Warnstufe
- ERROR – Fehlermeldung, die Aufmerksamkeit des Benutzers ist erforderlich
- CRITICAL – kritischer Fehler, die unmittelbare Aufmerksamkeit des Benutzers ist erforderlich

Die Nachrichten werden in der Protokolltabelle des NMP Clients unterschiedlich dargestellt. Dies erleichtert die Zuwendung der Aufmerksamkeit auf die wichtigen Ereignisse. Die Art der Darstellung der Nachrichten wird von der definierten Stufe bestimmt.

Für jeden Ereignistyp kann der Systemdministrator eine akustische oder E-Mail-Benachrichtigung ein- bzw. ausschalten. Wenn diese aktiviert sind spielt der NMP Client beim Auftreten des Ereignisses einen Ton ab und der NMP Server versendet eine E-Mail an alle definierten Empfänger. Bitte vergessen Sie nicht, hierfür die E-Mail Benachrichtigung im Fenster „ Email notification” zu konfigurieren und aktivieren.

4.2.4 Backup und Wiederherstellung der Datenbank

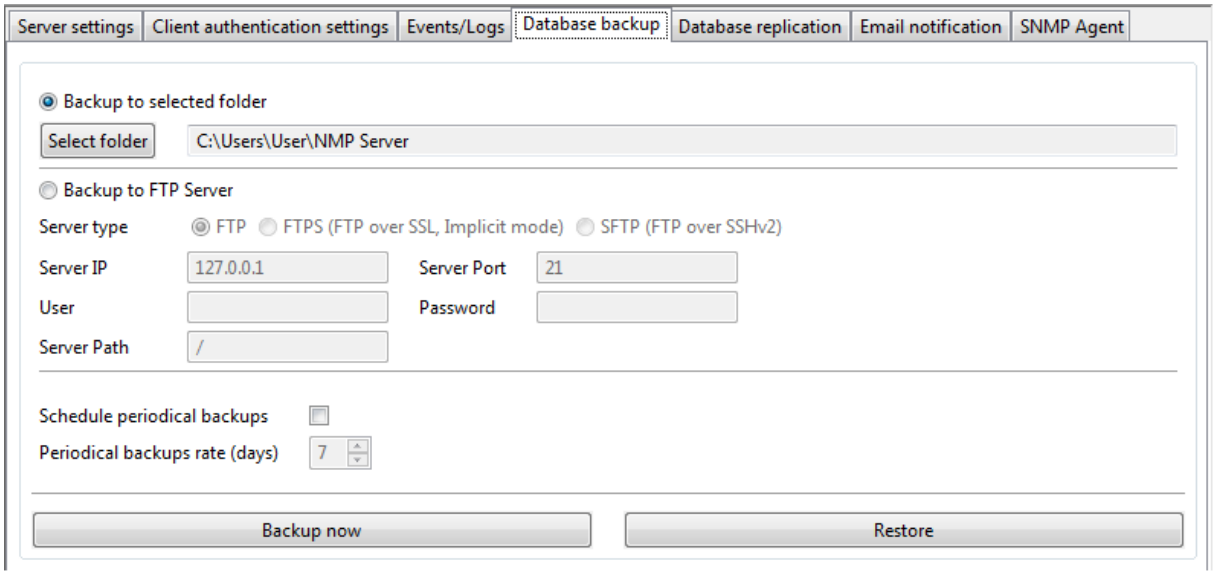

Abbildung 18: Dialog „Database Backup”

NMP Server kann eine Backup-Kopie der aktuell genutzten Datenbank anlegen. Der Systemadministrator kann die Datenbank manuell durch einen Klick auf die Schaltfläche „Backup now” sichern. Je nach der ausgewählten Option kann die Kopie der Datenbank:

- im ausgewählten Ordner gesichert werden
- an den konfigurierten FTP-Server gesandt werden.

Bei Verwendung der Option „Backup to FTP-Server” sollte auch der Pfad zum Backup-Verzeichnis eingegeben werden (beispielsweise „/Some Folder/Backup”). Eine leere Zeichenkette oder „/” ist erforderlich, wenn die Backup Datei im Root Verzeichnis gespeichert werden soll.

Die Backups werden als ZIP Archive gesichert. Der Name jeder Datei enthält das aktuelle Datum (beispielsweise „NMPS_DB_BACKUP_2011-06-15.zip”). Sollte in diesem Backup Verzeichnis bereits eine Datei gleichen Namens vorhanden sein, wird dem aktuellen Datum die aktuelle Zeit in Millisekunden angehängt. Auf diese Weise können die Dateien unterschieden werden.

Die Aktivierung geplanter Backups ist ebenfalls möglich. In einem solchen Fall erzeugt NMP Server automatisch alle x Tage (1 ... 30 Tage) eine Kopie der Datenbank. Der Scheduler wird bei der Erzeugung des Backups die aktuelle ausgewählte Option (Backup im ausgewählten Verzeichnis oder Backup zu einem FTP-Server) verwenden.

Zur Wiederherstellung der Datenbank aus einer Backup Datei betätigen Sie die Schaltfläche „Restore” und wählen die Datei aus, aus der die Datenbank wiederhergestellt werden soll. NMP Server muss vor dem Beginn der Wiederherstellungsprozedur gestoppt werden.

Die Datenbank kann nur aus einer lokalen Backup Datei heraus wiederhergestellt werden. Bei FTP-Backups sollte ein FTP-Client zum Download der Backup-Kopie vom Server verwandt werden.

4.2.5 Server Replikation – Einstellungen

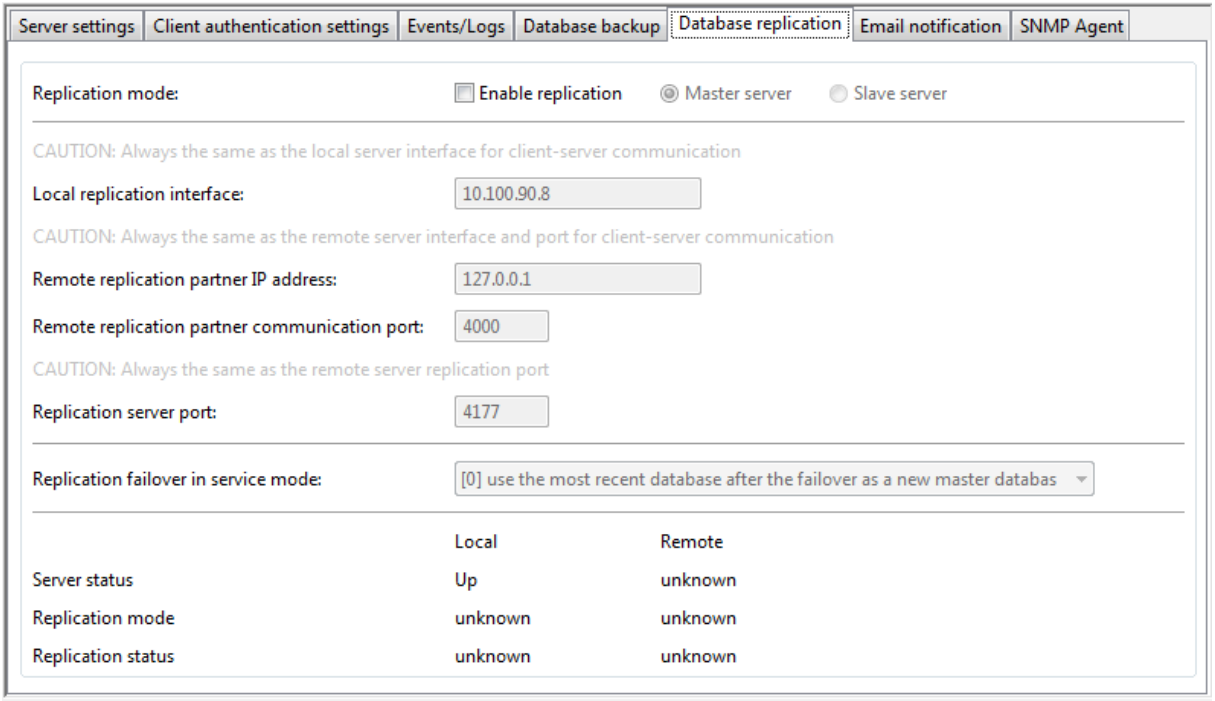

Abbildung 19: Dialog „Server Replication Settings”

Hier können zwei NMP Server-Instanzen in einem Master – Slave Replikations-modus konfiguriert werden. Weitere Details sind im Kapitel *NMP Server Replikation* enthalten.

4.2.6 E-Mail Benachrichtigungen

NMP Server kann beim Erhalt von SNMP-Traps oder Fehlermeldungen E-Mail Benachrichtigungen versenden. Der konfigurierte SMTP-Server wird als E-Mail Relay-Server verwandt. E-Mail Benachrichtigungen werden an alle definierten Benutzer des NMP Servers versandt. Der NMP Server-Systemadministrator und alle Benutzer sollten ihre korrekten E-Mail Adressen konfigurieren.

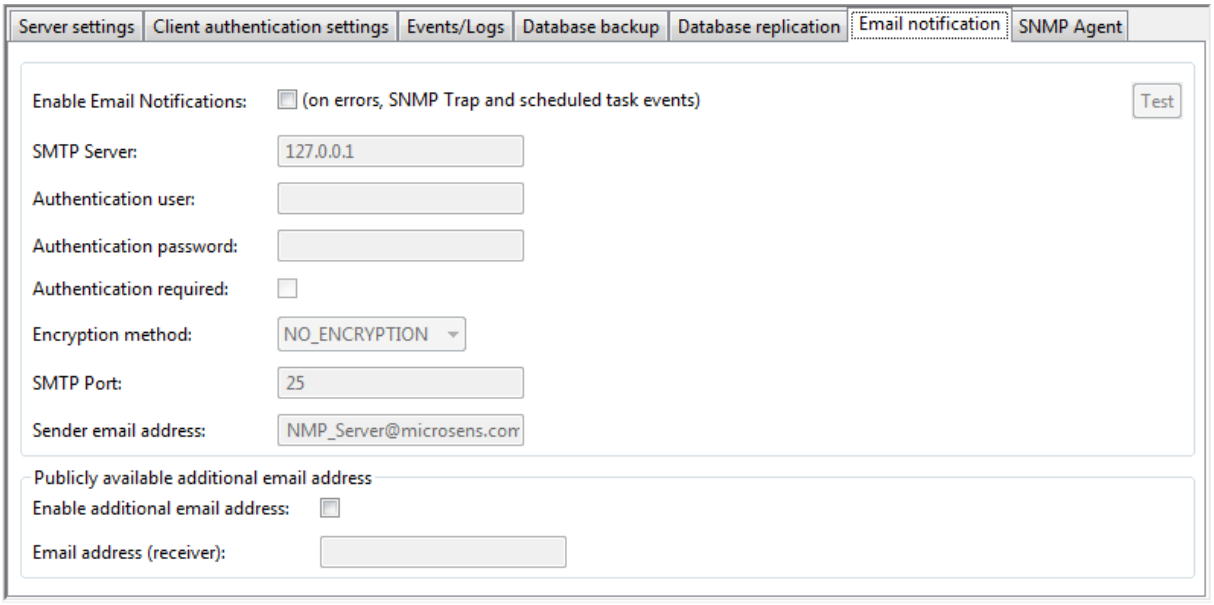

Abbildung 20: Dialog „E-Mail Notification”

Enable Email Notifications: Bei aktivierter Option werden Fehler- und SNMP Trap-Informationen per E-Mail an die weiter unten benannten Empfänger versandt. Ein existierendes E-Mail Konto mit SMTP-Zugang ist ebenfalls erforderlich.
SMTP-Server: Die Adresse des SMTP-Servers für abgehende E-Mails. Zum Beispiel „smtp.gmail.com”
Authentication user: Der Benutzername für dieses E-Mail Konto
Authentication password: Das Passwort für dieses E-Mail Konto
Authentication required: Prüfung, ob der SMTP-Server eine Benutzerauthentifizierung erfordert
Encryption method: Vom SMTP-Server benutztes Verschlüsselungsverfahren (NO_ENCRYPTION/SSL/TLS)
SMTP Port: SMTP-Server Port
Sender email address: Die im „Von” Feld der gesandten Nachricht verwandte E-Mail Adresse

Enable additional email address: Der NMP Server sendet E-Mail Benachrichtigungen an weitere (öffentlich verfügbare) E-Mail Adressen, die nicht mit irgendeinem Benutzerkonto des NMP Servers in Verbindung stehen

Email address (receiver): Weitere Empfänger der E-Mail Benachrichtigung

4.2.7 SNMP-Agent (Northbound Interface)

Eine Northbound-Schnittstelle ist eine Schnittstelle, die einer bestimmten Komponente des Netzwerks die Kommunikation mit einer Komponente einer höheren Stufe ermöglicht. Der NMP Server stellt eine Northbound-Schnittstelle in Form eines SNMP-Agenten bereit. Das SNMP-Protokoll kann dazu verwandt werden, Managementdaten für andere Managementsysteme zur Verfügung zu stellen.

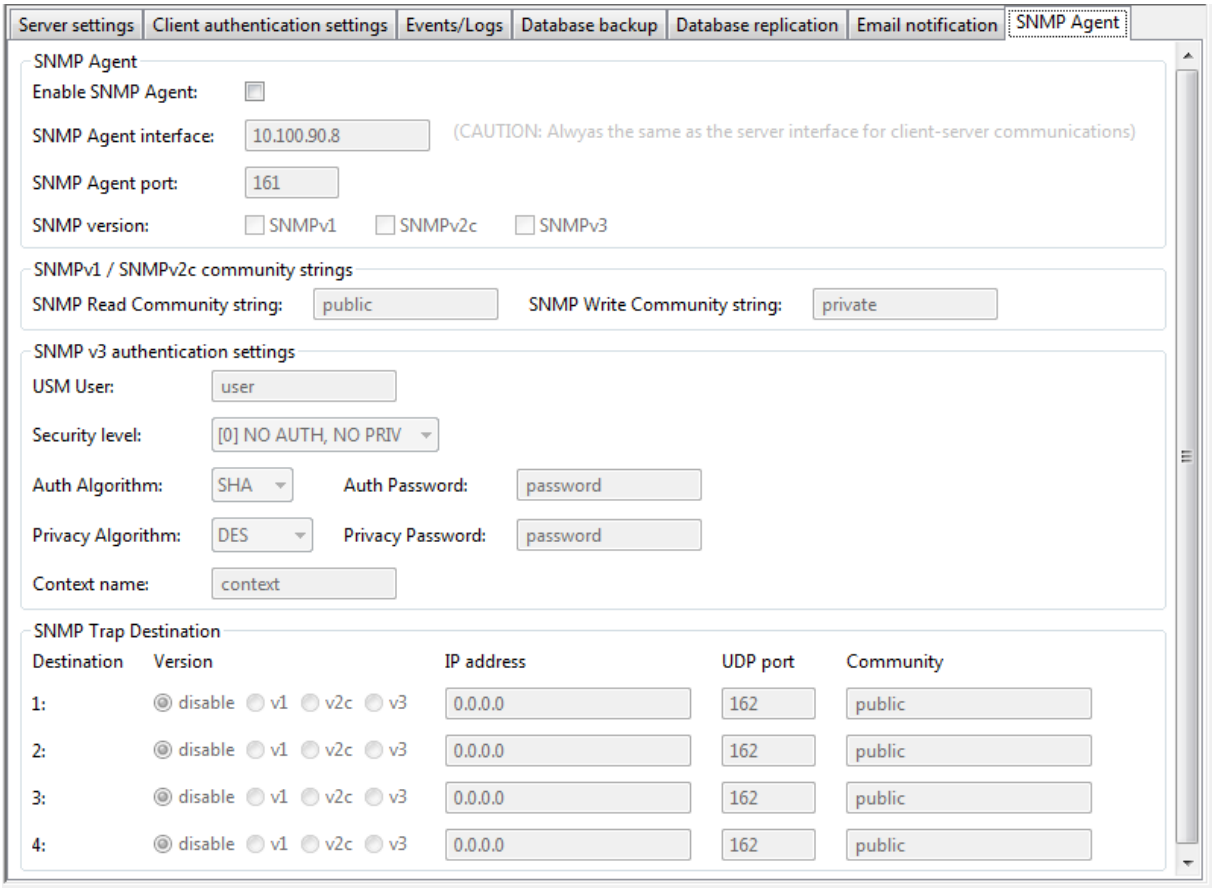

Abbildung 21: Fenster „SNMP-Agent"

SNMP-Agent

Enable SNMP Agent: Die Aktivierung des SNMP-Agenten ermöglicht die Bereitstellung der vom NMP Server gesammelten Managementdaten für die anderen SNMP-Manager.

SNMP Agent interface: Die vom SNMP-Agenten genutzte Netzwerkschnittstelle. Hier können die anderen SNMP-Manager Daten abfragen. Die Schnittstelle wird über das Register „Server settings" konfiguriert und ist immer mit der Schnittstelle für die Client-Server Kommunikation identisch.

SNMP Agent port: Der vom SNMP-Agenten genutzte Port

SNMP version: Wählen Sie hier die vom SNMP-Agenten zu unterstützende SNMP-Version aus. Es sollte wenigstens eine Version aktiviert sein.

SNMPv1/SNMPv2c community strings

SNMP Read Community string: Der Read-only Community-String ermöglicht dem Benutzer das Auslesen von Datenwerten.

SNMP Write Community string: Der Read-Write Community-String ermöglicht dem Benutzer das Auslesen und Schreiben von Datenwerten.

SNMPv3 authentication settings

USM User: Der Sicherheitsname des Benutzers (üblicherweise der Benutzername)

Security level: Der SNMPv3-Agent unterstützt die folgenden Sicherheitsstufen (wie im USM MIB RFC 2574 definiert):

- **noAuthnoPriv:** Kommunikation ohne Authentifizierung und Verschlüsselung
- **authNoPriv:** Kommunikation mit Authentifizierung jedoch ohne Verschlüsselung. Für die Authentifizierung werden wie Protokolle MD5 und SHA (Secure Hash Algorithm) genutzt.
- **authPriv:** Kommunikation mit Authentifizierung und Verschlüsselung. Für die Authentifizierung werden wie Protokolle MD5 und SHA genutzt. Für die Verschlüsselung werden die Protokolle DES (Data Encryption Standard) und AES (Advanced Encryption Standard) genutzt.

Auth Algorithm: Die dem Benutzer zugeordnete Authentifizierungsprotokoll-ID

Auth Password: Das Authentifizierungspasswort

Privacy Algorithm: Die dem Benutzer zugeordnete Verschlüsselungsprotokoll-ID

Privacy Password: Das Verschlüsselungspasswort

Context name: Ein SNMP-Context ist eine Sammlung von Managementinformationen, die für eine SNMP-Entity zugänglich ist.

SNMP Trap Destination

Der SNMP-Agent kann SNMP-Traps versenden wenn der NMP Server verschiedene Ereignisse generiert. Von anderen Geräten empfangene Traps können auch weitergeleitet werden. Es können bis zu vier unterschiedliche Trap-Ziele definiert werden. Für jedes Ziel kann eine Trap-Version gewählt werden (SNMP v1, v2c oder v3).

4.2.7.1 Management Information Base (MIB)

Eine Management Information Base (MIB) ist eine Datenbank, die für die Verwaltung von Entities in einem Kommunikationsnetzwerk genutzt wird. Die Datenbank ist hierarchisch strukturiert (Baumstruktur), jede Entity wird über einen Object Identifier (OID) adressiert.

Die MIB-Datei des NMP Server SNMP-Agenten wird immer gemeinsam mit dem NMP Server installiert. Die NMP Server MIB-Datei (*NMP_SERVER_MIB.mib*) befindet sich im Ordner „NMP_SERVER_INSTALLATION_PATH\mib\".

Die NMP Server-MIB enthält mehrere Gruppen, die Informationen über die verwalteten Geräte sowie den Status des NMP Servers bereitstellen:

- serverInfo – Information über Version und Status des NMP Servers
- deviceList – Information über alle vom NMP Server verwalteten Geräte (Module, Ports, verfügbar in der Geräteliste des NMP Servers)
- servicesList – Information über die konfigurierten Geräte (definierte Port-zu-Port Verbindungen, Links)
- nmpServerTrap – Vom NMP Server versandte Traps

OID	Name	Zugang	Beschreibung
.1.3.6.1.4.1.3181	**microsens**		
.1.3.6.1.4.1.3181.5909	**nmpServer**		
.1.3.6.1.4.1.3181.5909.1	**serverInfo**		
.1.3.6.1.4.1.3181.5909.1.1.0	serverName	R	Der Name des NMP Servers
.1.3.6.1.4.1.3181.5909.1.2.0	serverManufacturer	R	Der Hersteller des NMP Servers
.1.3.6.1.4.1.3181.5909.1.3.0	serverVersion	R	Die Version des NMP Servers
.1.3.6.1.4.1.3181.5909.1.4.0	serverLicenseArticleNumber	R	Die Lizenzartikel-nummer des NMP Servers
.1.3.6.1.4.1.3181.5909.1.5.0	serverLicenseHolder	R	Der Lizenzhalter
.1.3.6.1.4.1.3181.5909.1.6.0	serverMaintenancePeriod	R	Der Wartungszeitraum des NMP Servers
.1.3.6.1.4.1.3181.5909.1.7.0	serverMaxActiveUsers	R	Die Anzahl der maximal gleichzeitig unterstützten aktiven Benutzer
.1.3.6.1.4.1.3181.5909.1.8.0	serverCurrentActiveUsers	R	Die Anzahl der momentan aktiven Benutzer
.1.3.6.1.4.1.3181.5909.1.9.0	serverStartTime	R	Die Startzeit des NMP Servers
.1.3.6.1.4.1.3181.5909.1.10.0	serverUptime	R	Die Betriebszeit des

OID	Name	Zugang	Beschreibung
			NMP Servers
.1.3.6.1.4.1.3181.5909.1.11.0	serverReplicationMode	R	Der Replizierungsmodus des NMP Servers
.1.3.6.1.4.1.3181.5909.1.12.0	serverReplicationStatus	R	Der Replizierungsstatus des NMP Servers
.1.3.6.1.4.1.3181.5909.2	**deviceList**	R	
.1.3.6.1.4.1.3181.5909.2.1.0	deviceListSize	R	Die Größe der Geräteliste des NMP Servers
.1.3.6.1.4.1.3181.5909.2.2	deviceListTable	NA	Diese Tabelle enthält die Geräte-liste des NMP Servers
.1.3.6.1.4.1.3181.5909.2.2.1	deviceListTableEntry	NA	Eintrag in der Geräliste
.1.3.6.1.4.1.3181.5909.2.2.1.1	deviceIp	NA	Tabellenindex Die IP-Adresse des Geräts
.1.3.6.1.4.1.3181.5909.2.2.1.2	deviceSubnetMask	R	Die Subnetzmaske des Geräts
.1.3.6.1.4.1.3181.5909.2.2.1.3	deviceGateway	R	Das Gateway des Geräts
.1.3.6.1.4.1.3181.5909.2.2.1.4	deviceDhcpMode	R	Der DHCP-Modus des Geräts
.1.3.6.1.4.1.3181.5909.2.2.1.5	deviceMac	R	Die MAC-Adresse des Geräts
.1.3.6.1.4.1.3181.5909.2.2.1.6	deviceName	R	Der Gerätename
.1.3.6.1.4.1.3181.5909.2.2.1.7	deviceLocation	R	Der Standort des Geräts
.1.3.6.1.4.1.3181.5909.2.2.1.8	deviceContact	R	Der Name der für dieses Gerät verantwortlichen Person
.1.3.6.1.4.1.3181.5909.2.2.1.9	deviceGroup	R	Der Name der Gerätelistegruppe
.1.3.6.1.4.1.3181.5909.2.2.1.10	deviceInventoryString	R	Der Inventory-String des Geräts
.1.3.6.1.4.1.3181.5909.2.2.1.11	deviceStatus	R	Der Gerätestatus: - kein Status(1) - Download von Daten (2) - nicht verfügbar (3) - verfügbar(4) Zurücksetzen(5) - Firmware-Aktualisierung

OID	Name	Zugang	Beschreibung
			(6) - Überprüfung(7) - Benutzerdefinierter Alarm (8)
.1.3.6.1.4.1.3181.5909.2.3	deviceModulesTable	NA	Tabelle mit der Gerätemodulliste
.1.3.6.1.4.1.3181.5909.2.3.1	deviceModulesTableEntry	NA	Eintrag in der Gerätemodul-Tabelle
.1.3.6.1.4.1.3181.5909.2.3.1.1	moduleDeviceIp	NA	Tabellenindex Die IP-Adresse des Geräts
.1.3.6.1.4.1.3181.5909.2.3.1.2	moduleId	NA	Tabellenindex Die Position des Moduls in der folgenden Syntax: nodeId:unitId:slotId
.1.3.6.1.4.1.3181.5909.2.3.1.3	moduleArticleNumber	R	Die Artikelnummer des Moduls
.1.3.6.1.4.1.3181.5909.2.3.1.4	moduleSerialNumber	R	Die Seriennummer des Moduls
.1.3.6.1.4.1.3181.5909.2.3.1.5	moduleFirmwareVersion	R	Die Firmware-Version des Moduls
.1.3.6.1.4.1.3181.5909.2.3.1.6	moduleHardwareVersion	R	Die Hardware-Version des Moduls
.1.3.6.1.4.1.3181.5909.2.3.1.7	moduleTemperature	R	Die Modultemperatur
.1.3.6.1.4.1.3181.5909.2.3.1.8	moduleStatus	R	Der Modulstatus: – ok (1), – SpareModus (2), – inaktiv (3), – Warnung (4), – Alarm (5), – unbekannt (255)
.1.3.6.1.4.1.3181.5909.2.4	deviceModulePortsTable	NA	Die Liste der Modulports des Geräts
.1.3.6.1.4.1.3181.5909.2.4.1	deviceModulePortsTableEntry	NA	Eintrag in der Modulport-Tabelle des Geräts
.1.3.6.1.4.1.3181.5909.2.4.1.1	portModuleDeviceIp	NA	Tabellenindex Die IP-Adresse des Geräts
.1.3.6.1.4.1.3181.5909.2.4.1.2	portModuleId	NA	Tabellenindex Die Modulposition in der folgenden Syntax: nodeId/unitId/slotId

OID	Name	Zugang	Beschreibung
.1.3.6.1.4.1.3181.5909.2.4.1.3	portId	NA	Tabellenindex Die Port-ID des Moduls
.1.3.6.1.4.1.3181.5909.2.4.1.4	portAlias	R	Alias des Modulports
.1.3.6.1.4.1.3181.5909.2.4.1.5	portStatus	R	Der Portstatus des Moduls
.1.3.6.1.4.1.3181.5909.3	**servicesList**	R	
.1.3.6.1.4.1.3181.5909.3.1.0	servicesListSize	R	Die Anzahl der definierten Services
.1.3.6.1.4.1.3181.5909.3.2.0	servicesOk	R	Anzahl der Services mit Status "OK"
.1.3.6.1.4.1.3181.5909.3.3.0	servicesError	R	Anzahl der Services mit Status "Fehler"
.1.3.6.1.4.1.3181.5909.3.4	servicesListTable	NA	Die Liste der definierten Services
.1.3.6.1.4.1.3181.5909.3.4.1	servicesListTableEntry	NA	Eintrag in der Service-Tabelle
.1.3.6.1.4.1.3181.5909.3.4.1.1	serviceId	NA	Tabellenindex Die Service-ID
.1.3.6.1.4.1.3181.5909.3.4.1.2	serviceName	R	Der Service-Name
.1.3.6.1.4.1.3181.5909.3.4.1.3	serviceDescription	R	Detaillierte Service-Beschreibung
.1.3.6.1.4.1.3181.5909.3.4.1.4	serviceStatus	R	Der Service-Status
.1.3.6.1.4.1.3181.5909.100	**nmpServerTrap**		
.1.3.6.1.4.1.3181.5909.100.0	**nmpServerNotifications**		
.1.3.6.1.4.1.3181.5909.100.0.100	nmpServerShutdownTrap		Dieser Trap zeigt an, dass der NMP Server ausgeschaltet ist.
.1.3.6.1.4.1.3181.5909.100.1	**trapSourceDevice**		
.1.3.6.1.4.1.3181.5909.100.1.1.0	trapSourceDeviceIpAddress		Die IP-Adresse der
.1.3.6.1.4.1.3181.5909.100.1.2.0	trapSourceDeviceSysUpTime		Die sysUpTime des Trap-Source-Geräts
.1.3.6.1.4.1.3181.5909.100.1.3.0	trapSourceDeviceTrapOid		Der snmpTrapOID-Wert des Trap-Source-Geräts
.1.3.6.1.4.1.3181.5909.100.1.4.0	trapSourceDeviceEnterpriseOid		Der snmpTrapEnterprise-Wert des Trap-Source-Geräts

4.3 Server-Schaltflächen

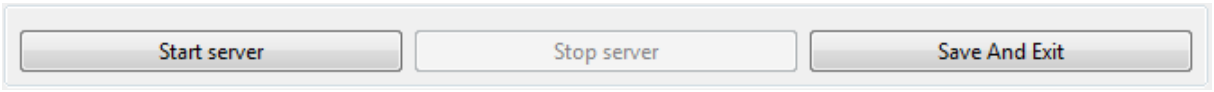

Abbildung 22: Server-Schaltflächen

Start Server: *S*tartet die NMP Server-Dienste (http-Server, Datenbank, Gerätedaten-Kollektor und Trap-Listener, sofern konfiguriert). Nach dem Start steht der Server unter der konfigurierten IP-Adresse und dem Port für die Ausführung von Client-Applikationen bereit. Alle Nachrichten des Startvorgangs sind im „Nachrichtenfenster" verfügbar. NMP Server zeigt bei einem fehlerhaften Start mehrere Nachrichten an (beispielsweise wenn ein konfigurierter Port nicht verfügbar ist).

Stop server: Stoppt den NMP Server

Save And Exit: Sichert die aktuellen Einstellungen und schließt das NMP Server-Applikationsfenster. Die Schaltfläche „Exit" steht nur bei gestopptem Server zur Verfügung.

4.4 Nachrichtenfenster

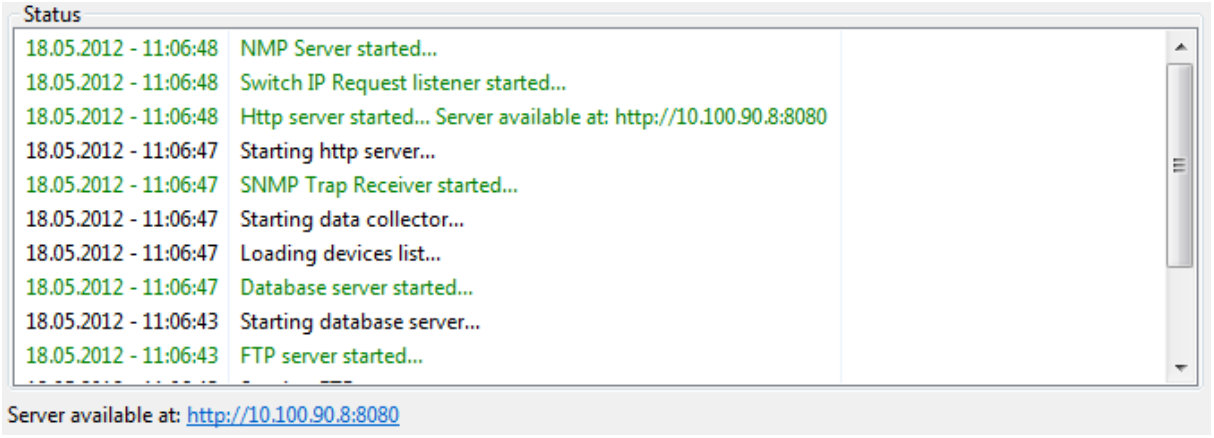

Abbildung 23: Nachrichtenfenster

Das Nachrichtenfenster stellt nützliche Informationen über den aktuellen Status des NMP Servers bereit. Alle Informationen bezüglich Start und Stopp von Diensten sind hier verfügbar. Der Link zum NMP Web Server befindet sich im unteren Bereich des Nachrichtenfensters, er kann für den Test der korrekten Funktion des Web Servers genutzt werden. Nach Auswahl des Links wird der standard Web Browser des Betriebssystems automatisch mit der NMP Web Client-Applikation geöffnet.

4.5 System Infobereich (Tray Icon)

Das NMP Server-Fenster kann zu einem Icon im Infobereich des Systems minimiert werden.

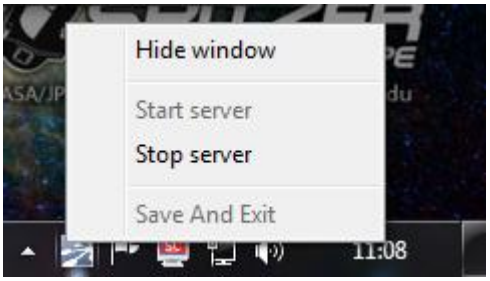

Abbildung 24: Fenster „System Tray Icon"

Zur Minimierung des NMP Server-Fensters zu einem Icon im Infobereich des Systems wird der Befehl „Window\Hide window" in der Menüzeile verwandt. Alternativ kann das Fenster durch einen Klick auf das Schließkreuz „X" in der rechten oberen Ecke geschlossen werden. Das Fenster kann durch einen Klick mit der linken Maustaste auf das Icon im Infobereich des Systems wiederhergestellt werden.

Ein Klick mit der rechten Maustaste auf das Icon im Infobereich des Systems öffnet ein kurzes Kontextmenü. Dieses Menü stellt die folgenden Optionen bereit:

- Fenster anzeigen (Show Window, stellt das NMP Server-Fenster wieder her)
- Server starten (Start server, startet den NMP Server)
- Server stoppen (Stop server, stoppt den NMP Server)
- Speichern und Beenden (Save And Exit, speichert die aktuelle Konfiguration und schließt die NMP Server-Applikation; ist nur bei gestopptem NMP Server verfügbar)

5 NMP Server als Windows Dienst

NMP Server kann als Windows-Dienst installiert werden. In Microsoft Windows Betriebssystemen ist ein Windows-Dienst ein dauerhaft ausgeführtes Programm, das spezifische Funktionen ausführt und für den Betrieb ohne Benutzerinterventionen entwickelt wurde. Windows-Dienste können so konfiguriert werden, dass sie beim Start des Betriebssystems gestartet werden und im Hintergrund laufen, solange Windows aktiv ist. Dienste können auch manuell gesteuert werden.

Zur Installation bzw. Deinstallation des NMP Server-Dienstes muss die Applikation mit Administrator-Rechten gestartet werden. Weiterhin muss das für die Installation des NMP Server Dienstes genutzte Windows Benutzerkonto das Recht „Log on as a service" aufweisen.

Zum Hinzufügen des „log on as a service"-Rechts zu einem Konto:

- Öffnen Sie „Local Security Policy" (Windows Control Panel/Administrative Tools).
- Doppelklicken Sie im Konsolenbaum auf „Local Policies" und klicken anschließend auf „User Rights Assignments".
- Doppelklicken Sie in der Detailansicht auf „Log on as a service".

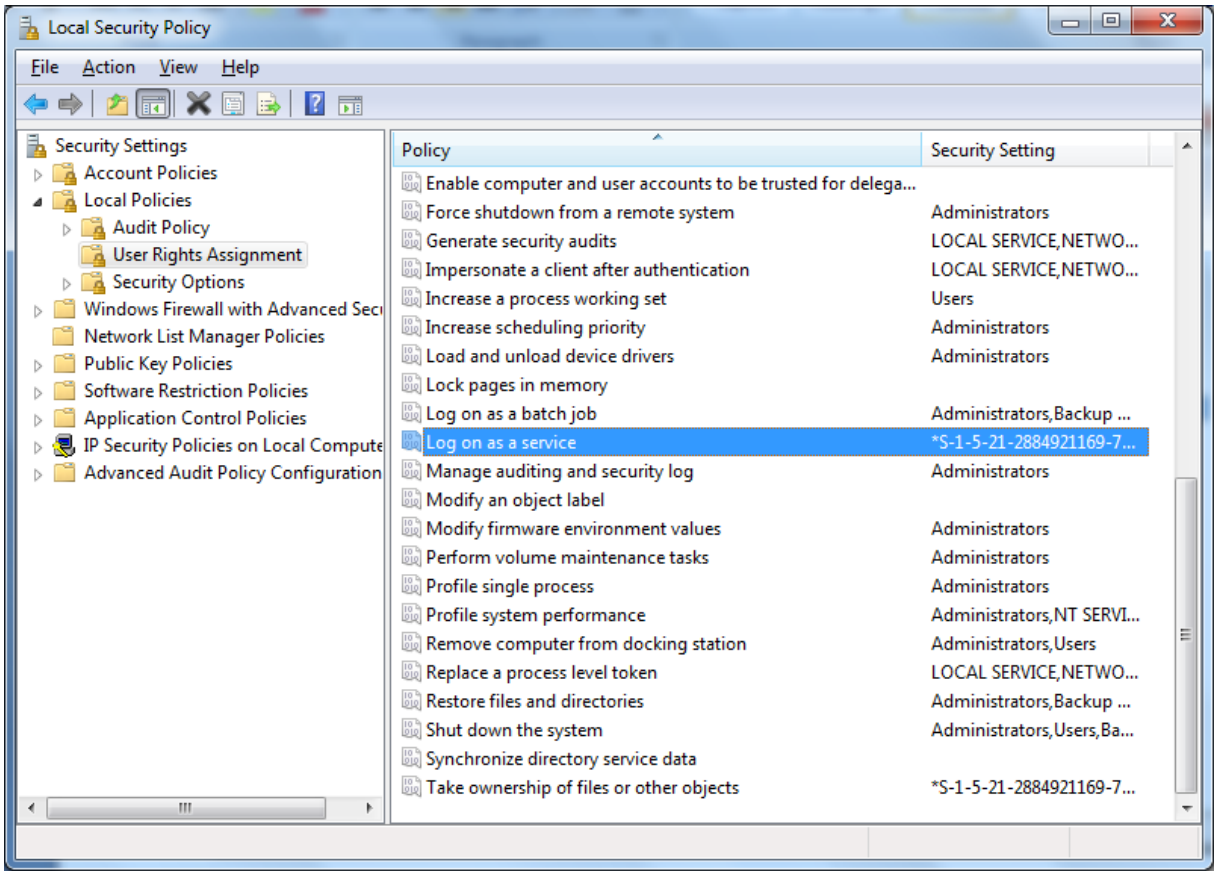

Abbildung 25: Fenster „Local Security Policy"

- Klicken Sie auf „Add User or Group” und fügen Sie anschließend das entsprechende Konto der Liste der Konten mit dem Recht „Log on as service” hinzu.

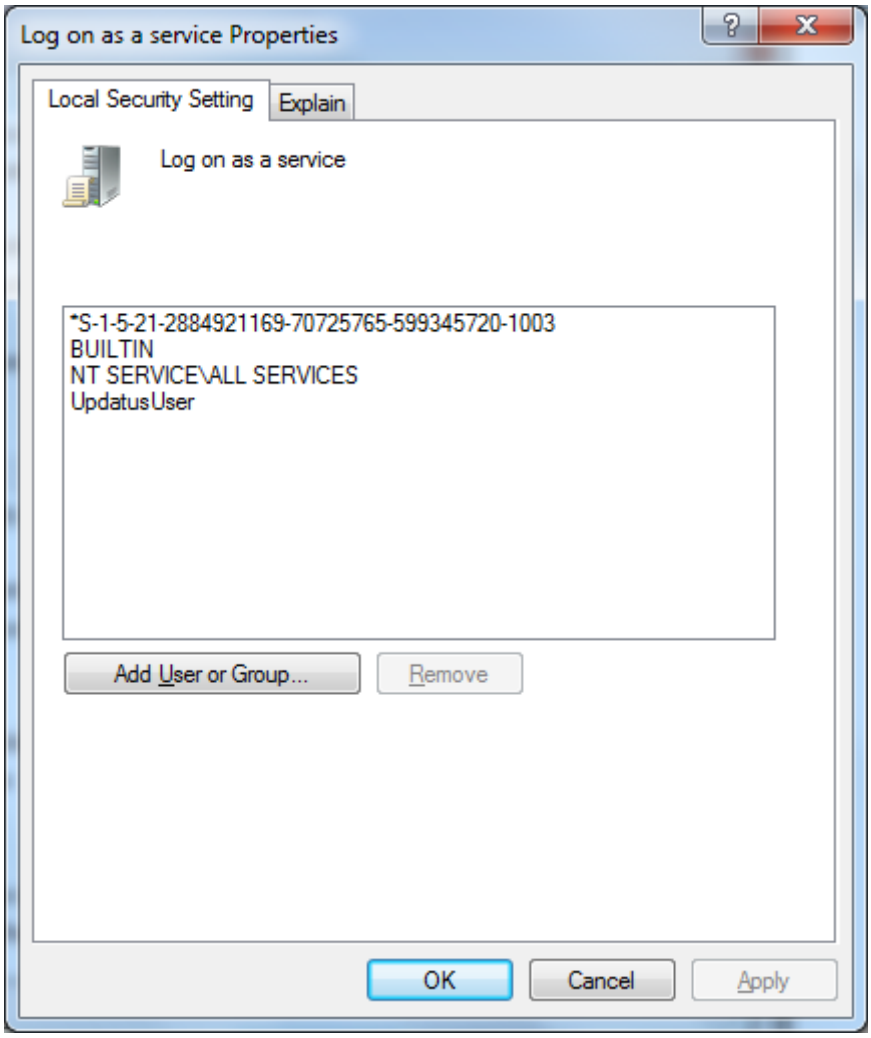

Abbildung 26: Fenster „Log on as a Service Properties”

Wenn das zum Start der NMP Server-Applikation genutzte Benutzerkonto alle erforderlichen Rechte aufweist, kann der NMP Server-Dienst korrekt installiert werden.

Vor der Installation des NMP Server-Dienstes sollte die Applikation im GUI-Modus konfiguriert werden (Schnittstellen, Ports, Backups). Öffnen Sie das NMP Server Manager-Fenster über das Windows Startmenü oder die Desktop-Verknüpfung. Konfigurieren Sie alle erforderlichen NMP Server-Optionen und betätigen Sie anschließend die Schaltfläche „Save and Exit”. Hierdurch wird die Konfigurations-datei („Settings.properties”) im Verzeichnis „$USER_HOME\NMP Server” gespeichert.

Diese Konfigurationsdatei wird von NMP Server im Servicemodus benötigt. Während der Konfiguration des NMP Servers sollte dasselbe Windows-Konto verwandt werden, das auch für den Start des NMP Servers genutzt wird. NMP Server speichert bzw. lädt seine Konfigurationsdatei immer im bzw. vom Verzeichnis „$USER_HOME\NMP Server". Falls während der Konfiguration des Servers ein anderes Windows-Konto als später beim Start des Dienstes verwandt wurde, wird NMP Server seine Konfigurationsdatei in einem falschen Verzeichnis suchen. In einem solchen Fall wird eine Standardkonfiguration verwandt.

Zur Installation des NMP Servers als Dienst sollte der Benutzer den Befehl „Service control" verwenden, der in der Menüzeile des NMP Servers im Menü „Server" verfügbar ist (Server\Service control).

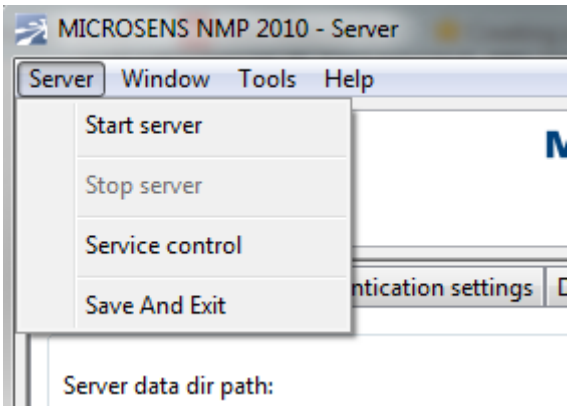

Abbildung 27: Menü „NMP Server/Service Control"

Zur Installation des Dienstes muss der Benutzer das für das Windows-Konto gültige Passwort angeben und (falls ein Domänenkonto verwandt wird) den Domänennamen.

NMP Server sollte immer konfiguriert werden (Schnittstellen, Ports, Backups), bevor die Installation als Dienst ausgeführt wird.

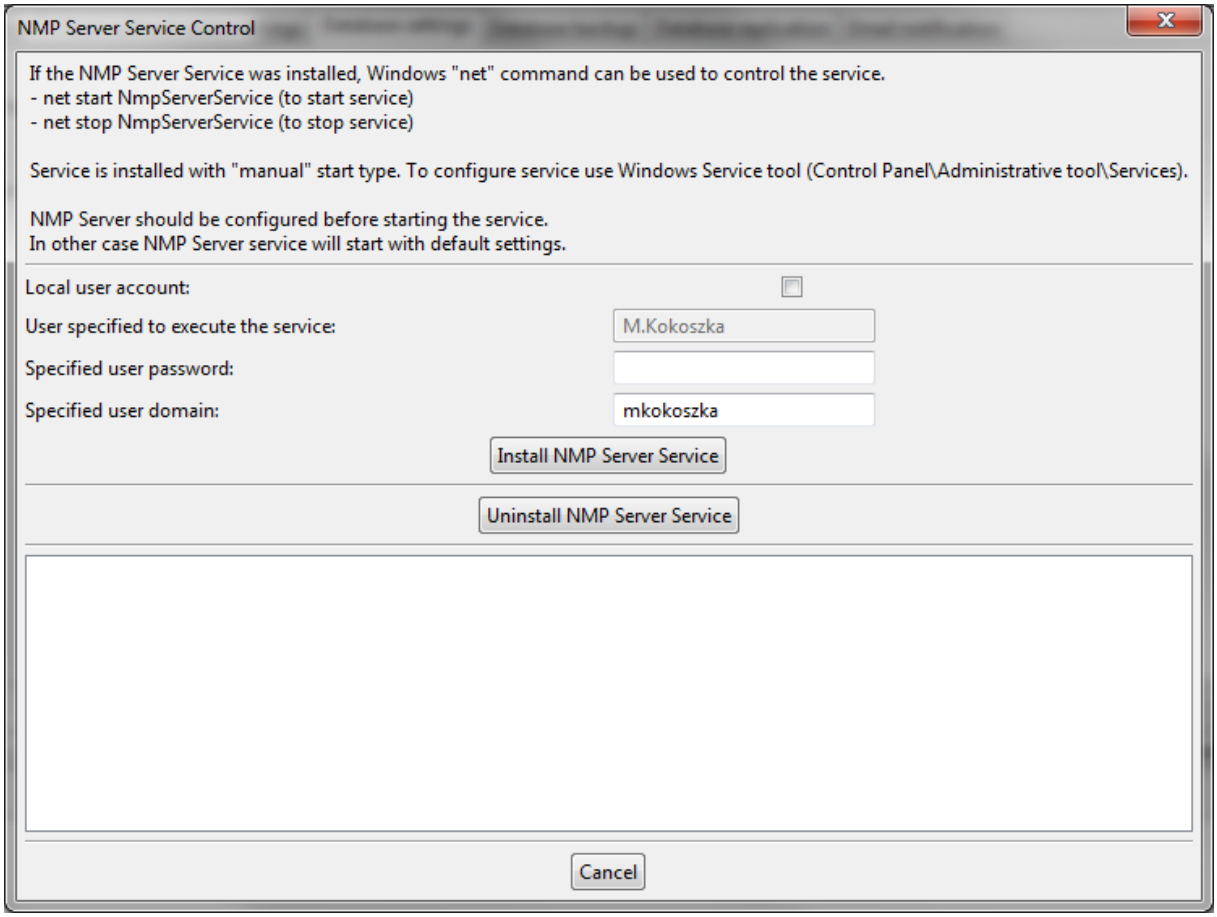

Abbildung 28: Dialog „Service Control”

Nach Auswahl von „Install NMP Server Service” wird das Tool den Dienst installieren. Das Protokollfenster sollte zur Überprüfung der Installationsergebnisse beobachtet werden. Nach Eingabe des richtigen Benutzernamens und des richtigen Passworts (und gegebenenfalls des Domänennamens) wird das Tool den Dienst installieren. Der Dienst wird jedoch nicht installiert, falls dies bereits in der Vergangenheit geschehen ist.

Nach Auswahl von „Uninstall NMP Server Service” wird das Tool den Dienst im System deinstallieren.

Der NMP Server-Dienst wird als Typ „Auto” Start installiert, der Name lautet „NmpServerService”. Damit wird der Dienst automatisch beim Start des Systems mitgestartet. Ein Login des Benutzers in das System ist nicht erforderlich. Der NMP Server-Dienst weist keine Interaktion mit dem Desktop auf (er wird als Non-GUI Hintergrundprozess gestartet). Zur Änderung einer NMPS-Konfiguration muss der Dienst gestoppt werden. Anschließend muss der normale GUI NMPS-Manager gestartet und die Änderungen durchgeführt werden. Nach Beenden des NMPS-Managers kann der Dienst dann neu gestartet werden (entweder manuell oder durch einen Neustart des Systems). Eine Aktualisierung des NMP Servers auf die neueste Version erfordert ebenfalls einen Stopp des Dienstes.

Nach der Installation des Dienstes kann dieser über die Ausführung von „Services" in der Windows Systemsteuerung → Verwaltung oder durch Eingabe von „Services.msc" im Befehl „Ausführen" im Startmenü (Zubehör) verwaltet werden. In Windows Vista (oder später) kann der Dienst im Register „Dienste" des Windows Task Managers (wo auch der entsprechende Prozess gefunden werden kann) gestartet und gestoppt werden. Die Verwaltungskonsole für „Dienste" stellt eine kurze Beschreibung der Funktionen des Dienstes bereit und zeigt den Pfad zu der ausführbaren Datei, ihren aktuellen Status, den Starttyp, die Abhängigkeiten und das Konto an, unter dem der Dienst betrieben wird.

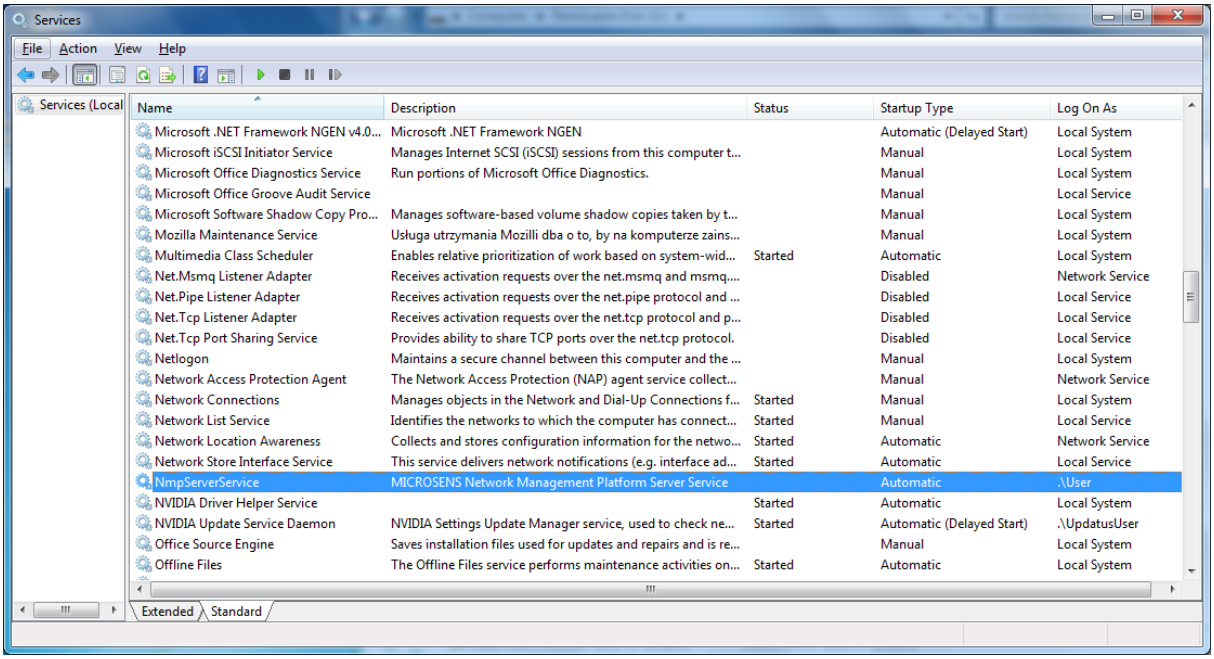

Abbildung 29: Fenster „Windows Services"

Dies ermöglicht dem Benutzer:

- Den Start, Stopp, die Pause oder den Neustart von Diensten
- Die Spezifikation von Dienstparametern
- Die Änderung des Startup-Typs (automatisch, manuell oder deaktiviert):
  - **Automatisch:** Der Dienst wird beim Systemstart mitgestartet.
  - **Manuell:** Der Dienst wird bedarfsorientiert gestartet oder wenn eine Applikation ihn aufruft (entsprechend der Definition. Dies ist jedoch nur zu einem Teil der Zeit richtig und hängt von dem aktuellen betroffenen Dienst ab).
  - **Deaktiviert:** Der Dienst ist vollständig deaktiviert, sein Betrieb und der Betrieb der Abhängigkeiten wird verhindert.
  - **Automatisch (verzögert):** Dies ist ein neuer Starttyp, der in Windows Vista eingeführt wurde. Der Dienst wird eine kurze Zeit nach dem Abschluss des Systemstarts und dem Durchlaufen der initialen Prozeduren gestartet. Dies ermöglicht einen schnelleren Systemstart.

- Änderung des Kontos, mit dem der Dienst angemeldet ist (es ist zu beachten, dass der NMP Server nach einer Änderung des Kontos des NMP Servers-Dienstes in dem neuen Verzeichnis ($USER_HOME\NMP Server) nach seiner Konfigurationsdatei suchen wird. Es wird eine Standard-konfiguration benutzt, falls die Konfigurationsdatei nicht verfügbar sein sollte.).
- Konfiguration von Wiederherstellungsoptionen nach einem Fehler des Dienstes

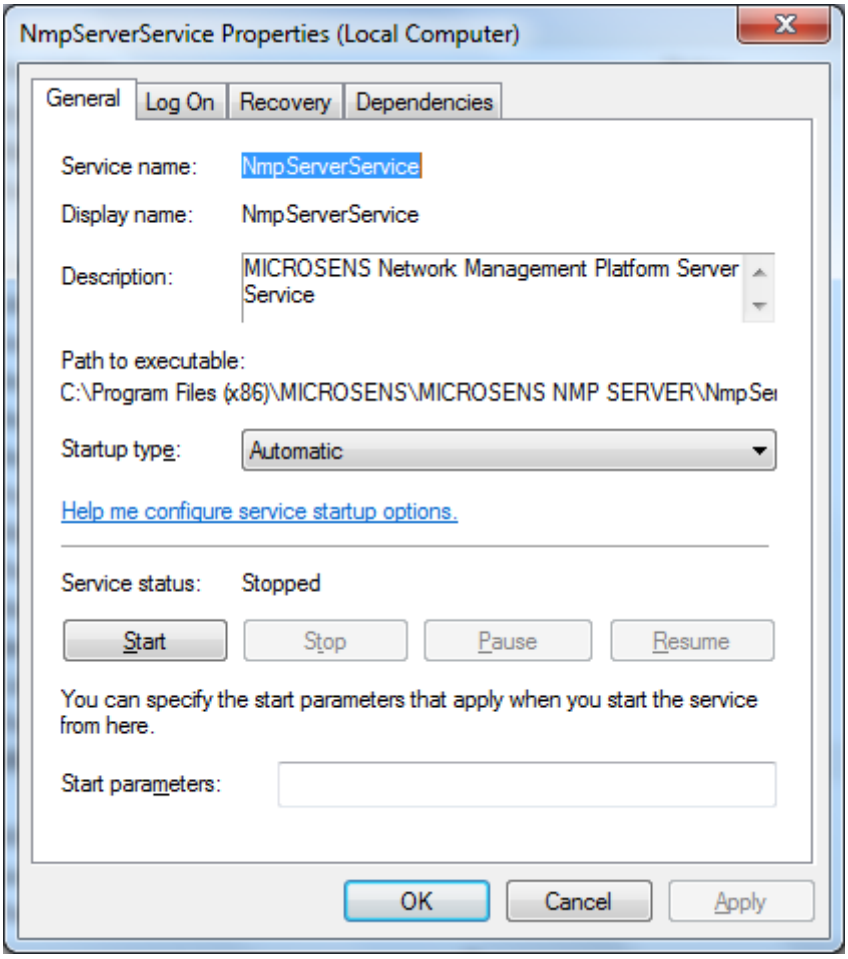

Abbildung 30: Dialog „Service General Properties”

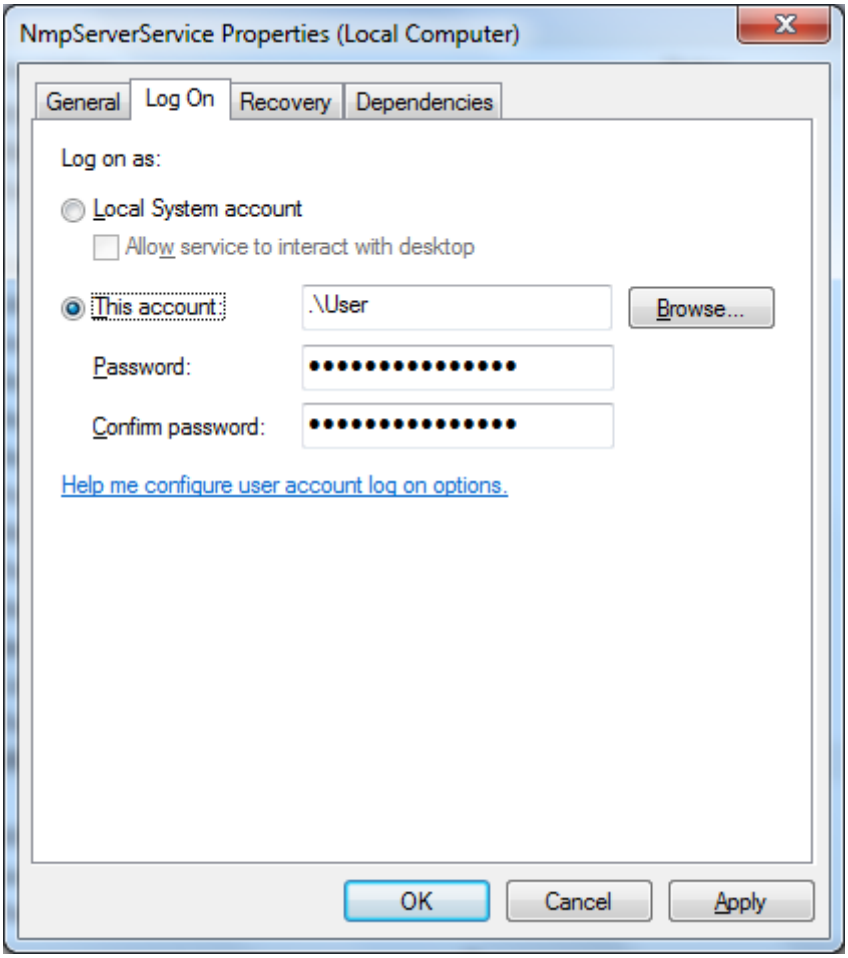

Abbildung 31: Dialog „Service Log On Properties"

Zum Stopp bzw. Start des NMP Server-Dienstes kann der Benutzer auch den Windows Befehl „net" verwenden. Um den Dienst mit diesem Befehl zu starten oder stoppen muss das Windows Kommandozeilenfenster geöffnet werden (cmd.exe).

- Zum Start des Dienstes lautet der Befehl: net start NmpServerService
- Zum Stopp des Dienstes lautet der Befehl: net stop NmpServerService

Bei aktivierter Firewall sollte die Applikation „NmpServerServcie.exe", die im NMPS-Installationsverzeichnis verfügbar ist, der Ausnahmeliste der Firewall hinzugefügt werden. Anderenfalls kann nicht auf den NMP Server-Dienst zugegriffen werden.

6 Switch DHCP-Autokonfiguration

Die Funktion DHCP-Autokonfiguration des Switches wird für die Aktualisierung der Firmware und die Konfiguration der MICROSENS Micro Switch (FTTO) und Industrial Profi Line Switche genutzt.

Bei aktivierter DHCP-Option (in den IP-Einstellungen) und aktiviertem DHCP Konfigurations-Request kann ein Gerät vom Server zusammen mit seinen IP-Einstellungen weitere Informationen erhalten. Der DHCP-Server kann die IP-Adresse des NMP Servers sowie den Namen der für die Rekonfiguration des Geräts zu verwendenden Konfigurationsdatei übermitteln. Nach Erhalt dieser Informationen vom DHCP-Server sendet der Switch den „Reconfiguration Request" an den NMP Server. Dieser wiederum aktualisiert nach Erhalt des „Reconfiguration Request" vom Switch die Firmware des Geräts (sofern erforderlich) und sendet eine neue Konfiguration an das Gerät. Das folgende Diagramm zeigt das Anwendungsprinzip:

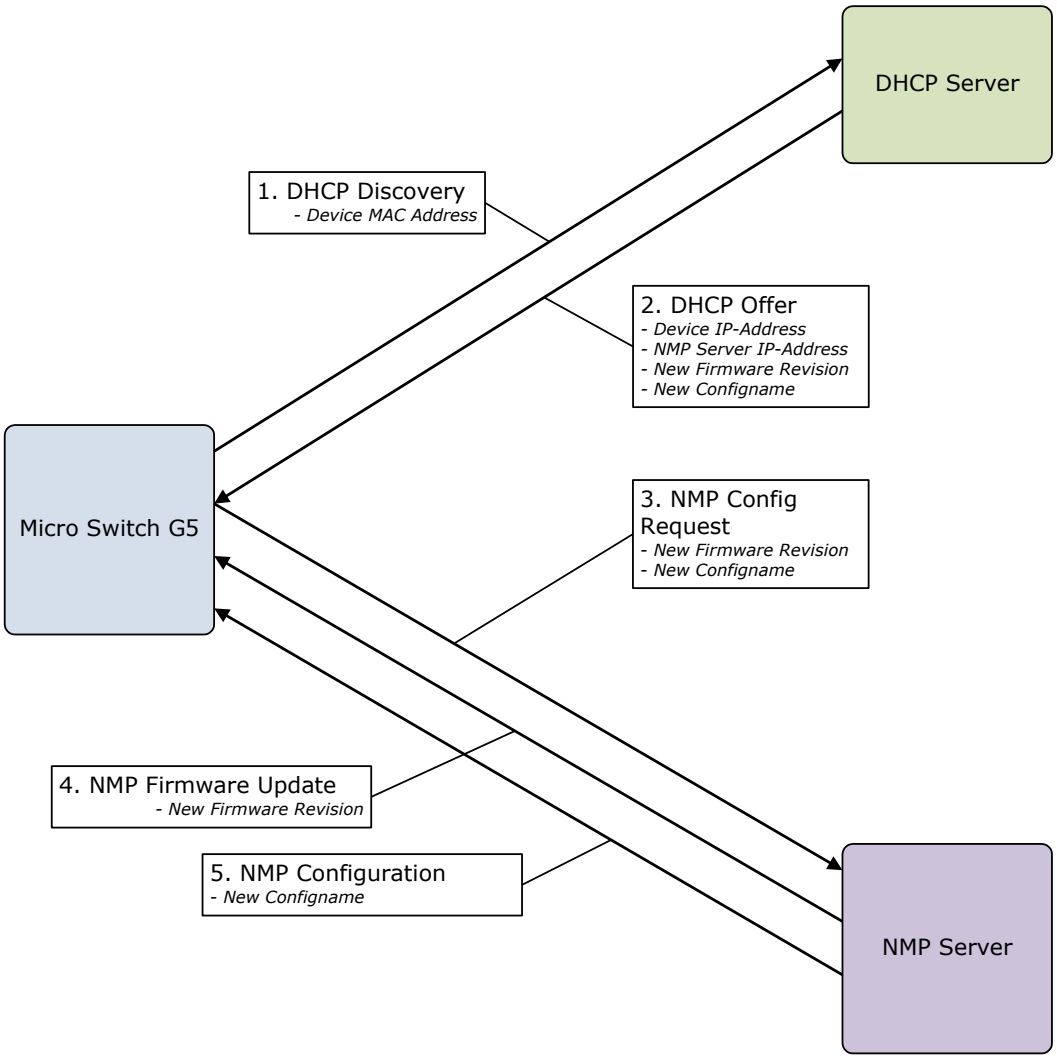

Abbildung 32: DHCP-Autokonfiguration

6.1 DHCP-Server Konfiguration

Der DHCP-Server muss zur Bereitstellung von zwei zusätzlichen DHCP Optionen im DHCP Offer Frame entsprechend konfiguriert werden.

Option 66: Server Name (TFTP-Server Name [RFC2132])

Diese Option enthält die IP-Adresse des NMP Servers, da DNS vom Switch nicht unterstützt wird.

Option 67: Bootfile Name (boot file name [RFC2132])

Diese Option muss den Dateinamen der Master Konfigurationsdatei (*.nmpmc), die vom NMP Server auf den Switch angewandt wird, enthalten.

6.2 NMP Server-Konfiguration

NMP Server wartet am UDP Port 8340 auf Anforderungen. Zwei Dateien werden verwandt, um den vom Switch gesandten „Reconfiguration Request" zu verarbeiten:

- Die Master-Konfigurationsdatei (*.nmpmc, required) – von der NMP Client-Applikation erzeugt. Diese beinhaltet die Konfiguration des Switches und den Namen der Firmware-Datei.
- Die Firmware-Datei (*.bin, optional) – neue Firmware für Switche

Die Konfigurationsdatei ist erforderlich. Ohne diese Datei startet NMPS die Prozesse zur Rekonfiguration und Firmware-Aktualisierung nicht.

Die Firmware-Datei ist optional (NMPS wird die Firmware des Geräts nicht aktualisieren, falls diese Datei nicht verfügbar sein sollte).

Beide Dateien sollten sich im Verzeichnis
„NMP Server data directory/FTP/DHCPAutoconfigFiles" befinden.

Der Benutzer kann die Dateien manuell oder unter Verwendung der NMP Client-Applikation in dem Verzeichnis „DHCPAutoconfigFiles" hinterlegen.

6.3 Erzeugen/Editieren der Master-Konfigurationsdatei für die DHCP-Autokonfiguration

Die Befehle zur DHCP-Autokonfiguration befinden sich im Menü „Tools” (Extras):

- ”Create configuration file” — erzeugt eine neue Konfigurationsdatei
- “Edit configuration file” — editiert eine vorhandene Konfigurationsdatei

Zur Erzeugung einer Master-Konfigurationsdatei zur Verwendung durch den NMP Server für das DHCP-Autokonfigurationsverfahren öffnen Sie die NMP Client-Applikation, verbinden sich mit dem NMP Server und wählen den Befehl „Create configuration file” aus. Das Fenster mit dem Gerätelistenbaum öffnet sich.

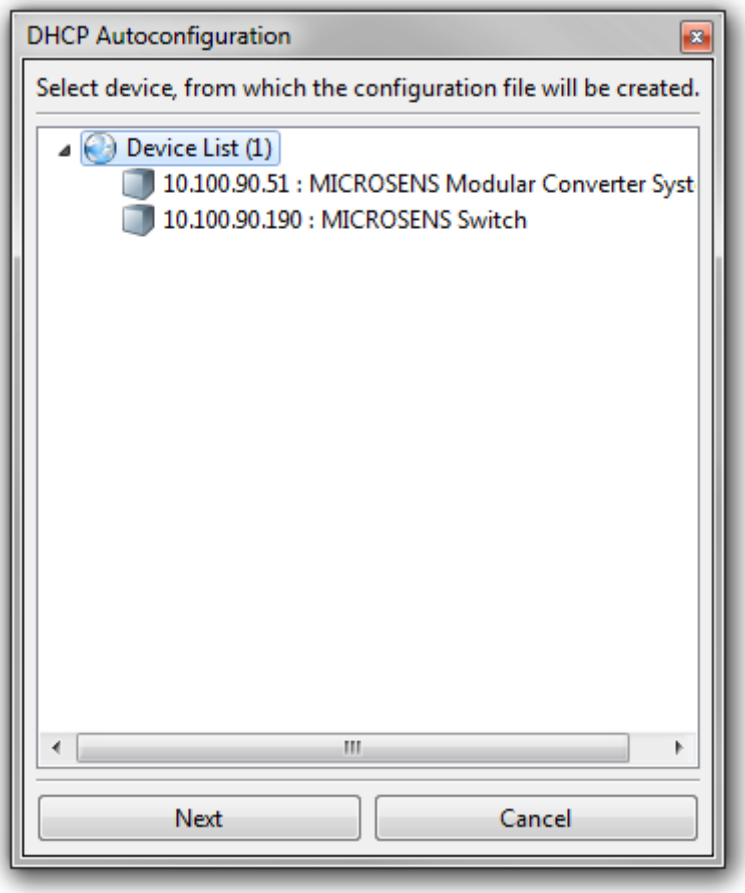

Abbildung 33: Fenster „DHCP Autoconfiguration – Geräteauswahl”

Wählen Sie das für die Erzeugung der Master-Konfigurationsdatei zu verwendende Gerät aus (Konfigurationsvorlage). Nach einem Klick auf die Schaltfläche „Next” erscheint das folgende Fenster „Master Configuration Editor”:

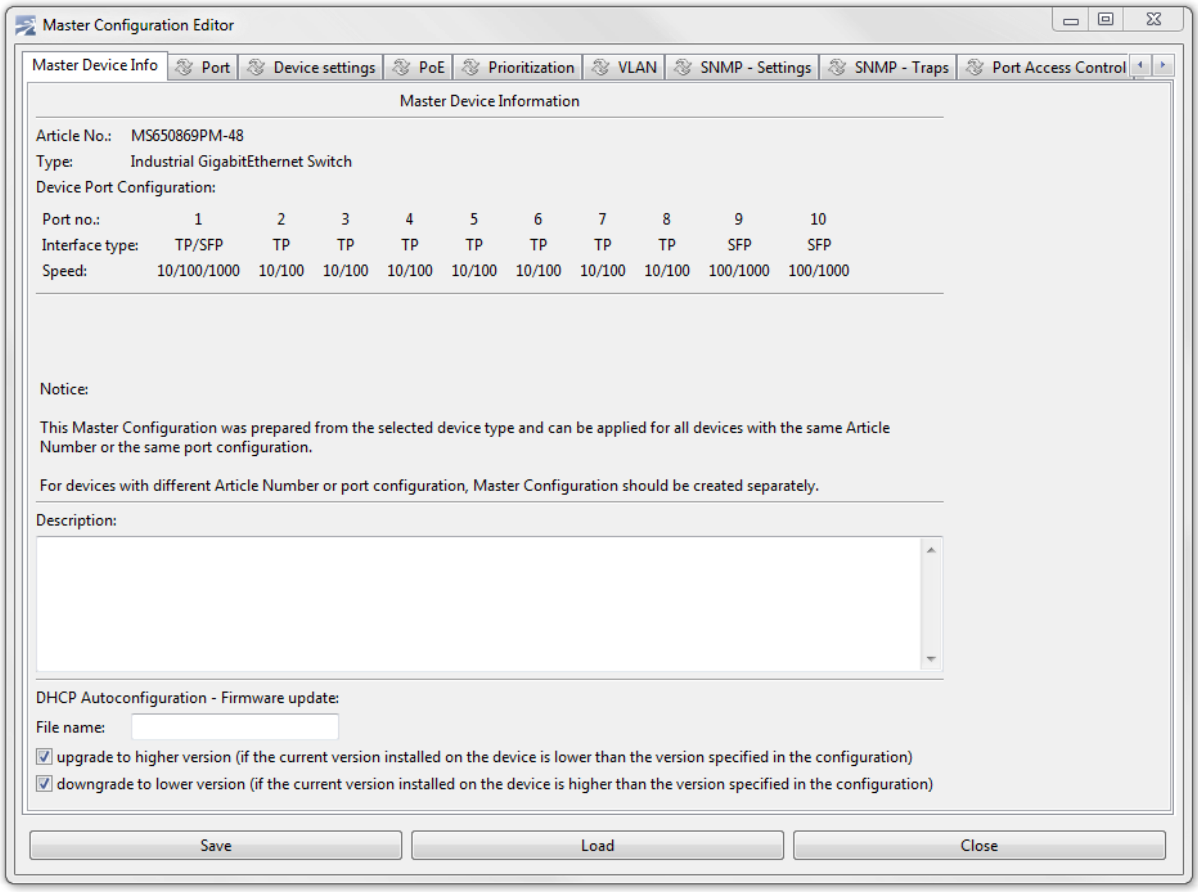

Abbildung 34: Erzeugen einer Konfigurationsdatei für die DHCP-Autokonfiguration

In diesem Fenster kann der Benutzer die Gerätekonfiguration editieren und die zu ändernden Konfigurationsoptionen auswählen (durch Auswahl der „change" Markierungsfelder neben den Konfigurationsoptionen).

Optional kann der Benutzer auch den Namen der für die Aktualisierung des Geräts zu verwendenden Firmware-Datei eingeben und entscheiden, welche Aktion während der Aktualisierungsprozedur stattfinden soll:

- Aktualisierung der Firmware auf eine höhere Version (falls die gegenwärtig auf dem Gerät installierte Version niedriger ist als die in der Konfigurationsdatei angegebene Version)
- Downgrade der Firmware auf eine niedrigere Version (falls die gegenwärtig auf dem Gerät installierte Version höher ist als die in der Konfigurationsdatei angegebene Version)

Die Firmware Upload-Prozedur startet nicht, falls beide Aktionen deaktiviert sein sollten oder die aktuelle Version der Firmware dieselbe ist wie in der Konfigurationsdatei angegeben.

Der in der Konfigurationsdatei angegebene Dateiname der Firmware muss das richtige Namensformat aufweisen. Anderenfalls kann NMP Server die Version der Firmware nicht erkennen und die Update-Prozedur wird nicht gestartet. Die richtige Syntax ist: some_text_ppppvxyyzzq.bin, wobei:

- pppp – Projektnummer (5313, 5324, 5331, 7018, 7014, 9135) (**erforderlich**)
- v – für Version (**erforderlich**)
- x – eine Ziffer (0...9), Hauptversionsnummer (**erforderlich**)
- yy – zwei Ziffern (00... 99), Unterversionsnummer (e.g. 08) (**erforderlich**)
- zz – zwei Ziffern (00... 99), Projekt-Releasenummer (z.B. 04) (**erforderlich**)
- q – ein Buchstabe (a...z), Projekt-Unterreleasebuchstabe (optional)
- .bin – Firmware-Dateiendung

Die folgenden Dateinamen-Beispiele sind gültig:

- mf5324v80301.bin,
- new_firmware_mf7014v80300d.bin
- 10.01.2012_5331v80805a.bin

Die folgenden Dateinamen sind ungültig:

- mf5324v8031.bin, (Projekt-Releasenummer zu kurz, zz ist „1”, sollte „01” sein)
- new_firmware_mf7014v80300d_some_text.bin (zusätzlicher Text zwischen der Projekt-Unterreleasenummer und der „.bin”-Dateiendung)
- 10.01.2012_v80805a.bin (keine Projektnummer vor dem „v”)

6.4 Versenden der Dateien zum NMP Server

Wählen Sie den Befehl „DHCP Autoconfiguration files", um die Konfigurations- und Firmware-Dateien an den NMP Server zu senden. Das folgende „File Transfer"-Fenster sollte erscheinen:

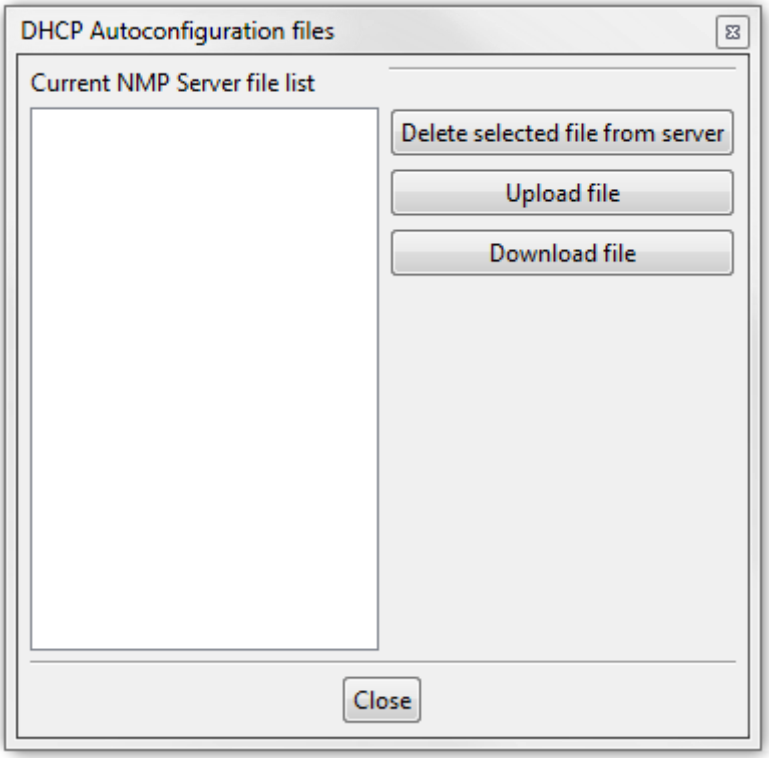

Abbildung 35: Versenden der Dateien an den NMP Server

Verwenden Sie dieses Fenster, um:

- die Konfigurationsdateien vom Server zu löschen,
- neue Konfigurationsdateien hochzuladen und
- vorhandene Konfigurationsdateien herunterzuladen.

Wenn Sie nicht den Client zum Hochladen der Dateien zum NMP Server verwenden, müssen die erforderlichen Dateien in dem Verzeichnis „NMP Server Data Directory/FTP/DHCPAutoconfigFiles" abgelegt werden.

7 NMP Server Replikation

Replikation ist ein wichtiges Element eines stabilen Datenbank-Verwaltungssystems. In NMP Server können Sie die Replikation der Datenbank auf einfache Art und Weise über die NMP Server-Manager GUI starten.

Die Replikationseigenschaften des NMP Servers umfassen die folgenden Funktionen:

One Master, One Slave: Eine replizierte Datenbank befindet sich an zwei Orten und wird von zwei verschiedenen NMP Server-Instanzen verwaltet. Eine dieser NMP Server-Instanzen nimmt für die Datenbank die *Master*-Rolle ein, die andere Instanz nimmt die *Slave*-Rolle ein. Gemeinsam repräsentieren der Master und der assoziierte Slave ein „Replikationspaar".

Roll-forward shipped log*:* Die Replikation beruht auf der Übertragung des Transaktionsprotokolls der NMP Server Datenbank vom Master an den Slave. Anschließend werden die im Protokoll beschriebenen Abläufe auf der Slave-Datenbank nachvollzogen.

Asymmetry*:* Nur der Master verarbeitet Transaktionen. Der Slave verarbeitet keine Transaktionen, auch keine reinen Lese-Operationen. Nur der Master kann Verbindungen mit dem Client akzeptieren. Der Slave leitet alle Verbindungen mit Clients an den Master-Server weiter.

Asynchronicity*:* Transaktionen werden an den Master übermittelt ohne dabei auf den Slave zu warten. Das Transaktionsprotokoll wird regelmäßig an den Slave übermittelt, es ist vollständig von der Ausführung der Transaktionen durch den Master entkoppelt. Dies kann zu einigen wenigen verlorenen Transaktionen führen, falls der Master ausfallen sollte.

Shared nothing*:* Mit Ausnahme der Netzwerkverbindung wird angenommenerweise keine Hardware gemeinsam genutzt.

Replikation beruht auf der Fähigkeit des NMP Servers zur Wiederherstellung nach einem Ausfall. Hierbei wird mit einem Backup gestartet und anschließend werden die NMP Server-Transaktionsdateien verarbeitet. Der Master sendet Protokollaufzeichnungen an den Slave, hierzu wird eine Netzwerkverbindung genutzt. Der Slave schreibt diese Protokollaufzeichnungen in seine lokale Protokolldatei und führt diese erneut aus.

Beim Ausfall des Masters vervollständigt der Slave die Wiederherstellung durch die Verarbeitung der noch nicht prozessierten Protokolle. Der Slave hat im Anschluss daran einen Status, der dem Status des Masters im Moment des Ausfalls sehr ähnlich ist. Einige der zuletzt ausgeführten Transaktionen des Masters sind möglicherweise noch nicht zum Slave gesandt worden und werden aus diesem Grund möglicherweise nicht dargestellt. Nach Abschluss der Wiederherstellungsarbeiten durch den Slave wird dieser in eine normale NMP Server-Instanz umgewandelt (ohne Replikationsmodus), die normale Transaktionen verarbeiten kann. Von nun an kann der Slave Verbindungen von Clients akzeptieren und wartet darauf, dass der Master-Server nach dessen Reparatur wieder verfügbar ist.

7.1 Start und Ausführen der Replikation

Vor dem Start der Replikation müssen auf zwei Servern (PCs) zwei NMP Server-Instanzen konfiguriert werden.

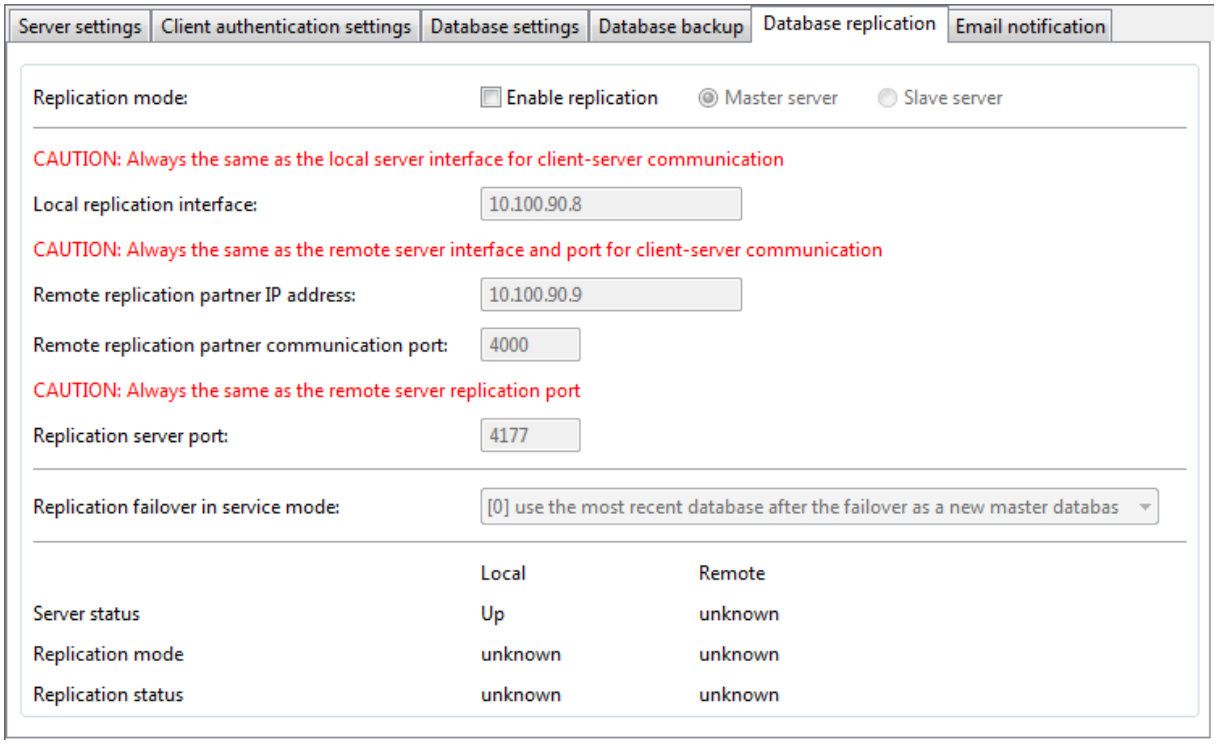

Abbildung 36: Fenster „Database Replication”

Replication mode: Aktiviert/deaktiviert die Replikation, definiert die Rolle der Server (Master oder Slave). Als Voreinstellung ist die Replikation deaktiviert.

Local replication interface: Die vom lokalen Server genutzte Netzwerkschnittstelle. Diese Schnittstelle ist immer dieselbe wie die für die Client-Server Kommunikation genutzte Schnittstelle (im Register „Server settings” konfiguriert).

Remote replication partner IP address: Die IP-Adresse des Partnerservers der Remote-Replikation. Diese Schnittstelle muss immer dieselbe sein, die auch der Remove-Server für die Client-Server Konfiguration nutzt (im Register „Server settings” konfiguriert).

Remote replication partner communication port: Die Portnummer des Remote Replikation-Partnerservers für die Client-Server Kommunikation
Replication server port: Die Portnummer, die für die Replikation der Datenbank genutzt werden wird. Der Port auf dem lokalen Server muss derselbe Port sein, der auf dem Partnerserver für die Remote-Replikation konfiguriert wurde (Standardeinstellung = 4177).

Replication failover in service mode: Auswahl der Datenbank, die nach einer fehlerbedingten Umschaltung (Failover) als neue Master-Datenbank genutzt werden wird. Verfügbare Optionen sind:

1. Verwendung der aktuellen Datenbank als neue Master-Datenbank (nach einem Failover). Bei der Wiederherstellung der Replikation nach einem Fehler des Masters oder des Slaves wird die aktuelle Datenbank benutzt.
2. Verwendung der Master-Datenbank als neue Master-Datenbank (nach einem Failover). Bei der Wiederherstellung der Replikation nach einem Fehler des Masters oder des Slaves wird immer die Datenbank des Master-Servers genutzt.
3. Verwendung der Slave-Datenbank als neue Master-Datenbank (nach einem Failover). Bei der Wiederherstellung der Replikation nach einem Fehler des Masters oder des Slaves wird immer die Datenbank des Slave-Servers genutzt.

Zum Start der Replikation sollte der Benutzer beide Server konfigurieren. Beide Server müssen sich im Netzwerk sehen. Der Replikationsport sollte auf beiden Servern exakt gleich sein. Die NMP Server arbeiten paarweise. Einer der Server sollte als Master-Server konfiguriert sein, der andere Server als Slave-Server. Die Replikation wird nicht initialisert, wenn zwei Server als Master (oder Slave) konfiguriert sind. Die Replikation wird ebenfalls nicht gestartet, wenn die Replikation auf einem der beiden Server deaktiviert ist.

Beide Server müssen Zugriff auf die verwalteten Geräte haben. Sollte der erste Server ausfallen (Master oder Slave), wird der zweite Server sich selbst im Nicht-Replikationsmodus neu starten und die Geräteüberwachung fortsetzen.

Nach Abschluss der Konfiguration der Replikationsoptionen sollten beide Server durch Betätigen der Schaltfläche „Start server" neu gestartet werden. Von nun an werden die Server die Replikation automatisch initialisieren. Der Benutzer sollte das Protokollfenster des NMP Server Managers überwachen, dort sind alle Abläufe dargestellt.

Nach dem Start der Replikation der existierenden Datenbanken zeigt der Master-Server (der als Replikations-Controller agiert) ein Dialogfeld mit der Abfrage an, welche Datenbank als Master-Datenbank gewählt werden sollte. Beide Datenbanken müssen synchronisiert sein.

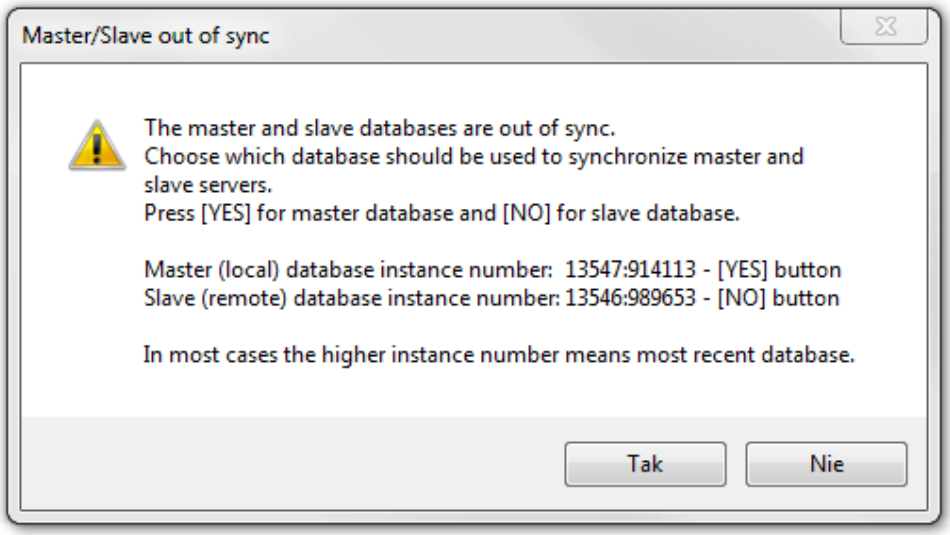

Abbildung 37: Nachricht „Master/Slave out of Sync"

Die Datenbank mit der höheren Ordnungsnummer ist die neueste Datenbank. Der Benutzer kann entscheiden, welche Datenbank als neue Master-Datenbank für die Replikation verwandt werden sollte. Das oben dargestellte Fenster wird nicht angezeigt, wenn die Datenbank noch nicht existiert (Erstinstallation des NMP Servers). Die nicht als Master-Datenbank für die Replikation ausgewählte Datenbank wird durch die neue Master-Datenbank ersetzt.

Wenn die Replikation gestartet wird, während die NMP Server als Windows-Dienste laufen, sollte der Benutzer beide Server mithilfe des NMP Server Manager-Fensters konfigurieren. Nach Abschluss der Konfiguration sollten beide NMP Server Manager durch einen Klick auf die Schaltfläche „Exit" geschlossen werden. Beim Start von „NmpServerServices" wird die Replikation automatisch initialisiert. Bei einem Start der Replikation im NMP Server-Dienstmodus wählt der Master-Server automatisch die neue Master-Datenbank für die Synchronisierung der Datenbank aus. Der Master-Server verwendet die vom Administrator konfigurierten Optionen (siehe hierzu auch *NMP Server Replikations-Failover*).

Nach dem Start der Replikation können Sie die Client-Applikation (NMP Client oder Web Client) verwenden, um sich mit dem Master-Server zu verbinden. Der Slave-Server kann keine Verbindungen von Clients akzeptieren. Falls der Benutzer versucht, sich mit dem Slave-Server zu verbinden:

- wird der Web Client automatisch zum Master-Server umgeleitet (nur dann, wenn Web Server auf beiden NMP Servern aktiviert sind).
- zeigt der NMP Client eine Warnmeldung an, dass der Slave-Server keine Verbindungen von Clients akzeptieren kann.

Zum Stopp der NMP Server-Replikation sollte zuerst der Master-Server und anschließend der Slave-Server gestoppt werden. Der Slave-Server kann bei noch laufendem Master-Server und noch ausgeführter Replikation nicht gestoppt werden.

7.2 NMP Server Replikations-Failover

Die NMP Server-Replikation kann nach einem Ausfall eines der beiden NMP Server automatisch wiederhergestellt werden. Beim Ausfall eines der beiden Replikations-Partnerserver startet der zweite Server automatisch neu im Nicht-Replikationsmodus und setzt die Überwachung der Geräte fort. Dieser Server kann dann auch Verbindungen von Clients akzeptieren (es ist dabei unerheblich, ob der Server zuvor als Master oder Slave definiert war). Nach der Reparatur des Replikationspartners und dessen Neustart sprechen beide Server miteinander, die Replikation wird automatisch neu initialisiert.

Während der Replikations-Failover-Prozedur müssen beide Server ihre Datenbanken synchronisieren. Sofern die Server im GUI-Modus gestartet werden, muss der Administrator die als neue Master-Datenbank für die Replikation zu verwendende Datenbank manuell auswählen. Bei einem Start der Server im Windows-Dienstmodus entscheidet der Master-Server automatisch darüber, welche Datenbank als neue Master-Datenbank genutzt wird. Die nicht ausgewählte Datenbank wird durch die neue Master-Datenbank ersetzt.

7.2.1 Redundanter NMP Serverbetrieb

1. NMP Server A ist der Replikations-Master
2. Neue Daten werden in der Master-Datenbank gespeichert
3. NMP Server A repliziert die Daten zur Slave-Datenbank auf NMP B

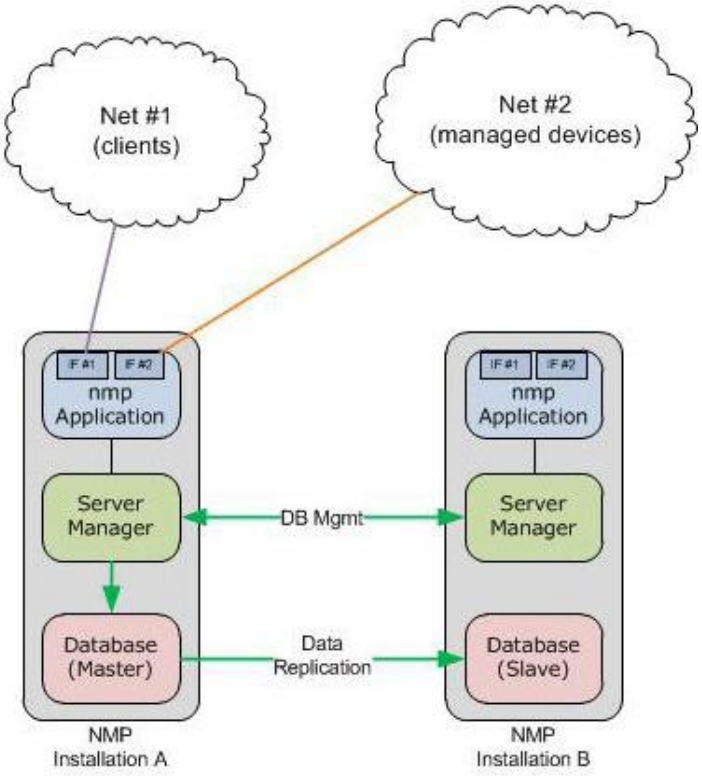

Abbildung 38: Redundanter Betrieb

7.2.2 Fehler des Master-Servers

1. NMP Server A (Master) ist nicht verfügbar
2. NMP Server B (Slave) schaltet auf Einzelbetrieb um
3. NMP Server B übernimmt die Aufgaben des NMP Servers A
4. NMP Server B speichert Daten in seiner eigenen Datenbank
5. NMP Server B wartet auf den Neustart von NMP Server A

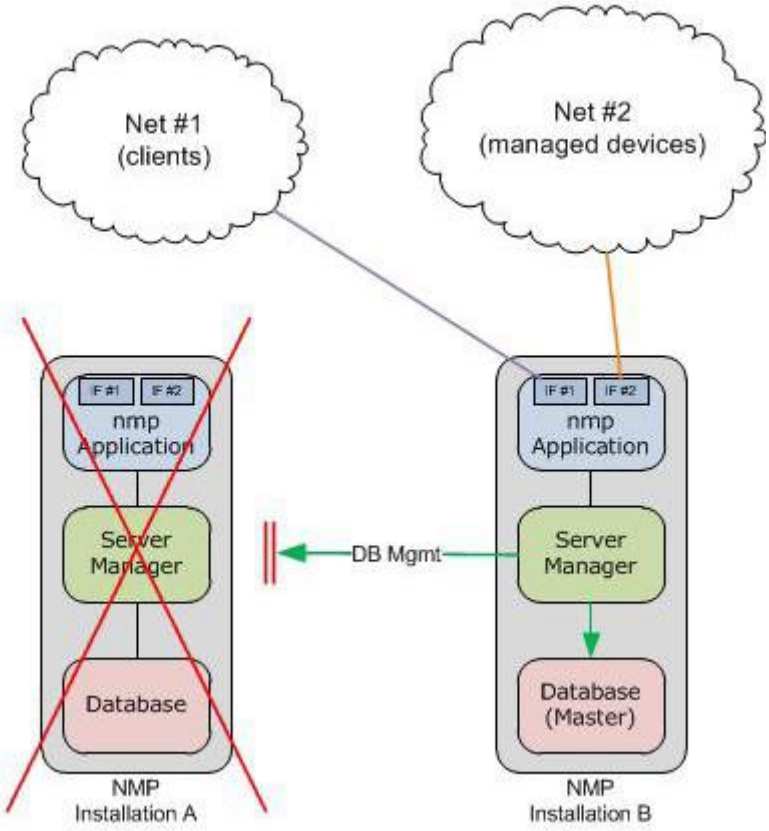

Abbildung 39: Fehler des Master-Servers

7.2.3 Der Master-Server startet nach einem Fehler neu

1. NMP Server B (Slave) weist die aktuelle Datenbank auf
2. NMP Server B speichert die Daten in seiner eigenen Datenbank
3. NMP Server A (Master) startet neu
4. NMP Server A initialisiert die Replikationsprozedur und wartet auf seinen Partnerserver
5. NMP Server B bemerkt, dass sein Replikationspartner wieder verfügbar ist und startet neu im Replikationsmodus
6. Beide Server synchronisieren ihre Datenbanken
7. Die Replikation wird neu initialisiert, beide Server arbeiten in ihren zuvor definierten Betriebszuständen (Master und Slave)

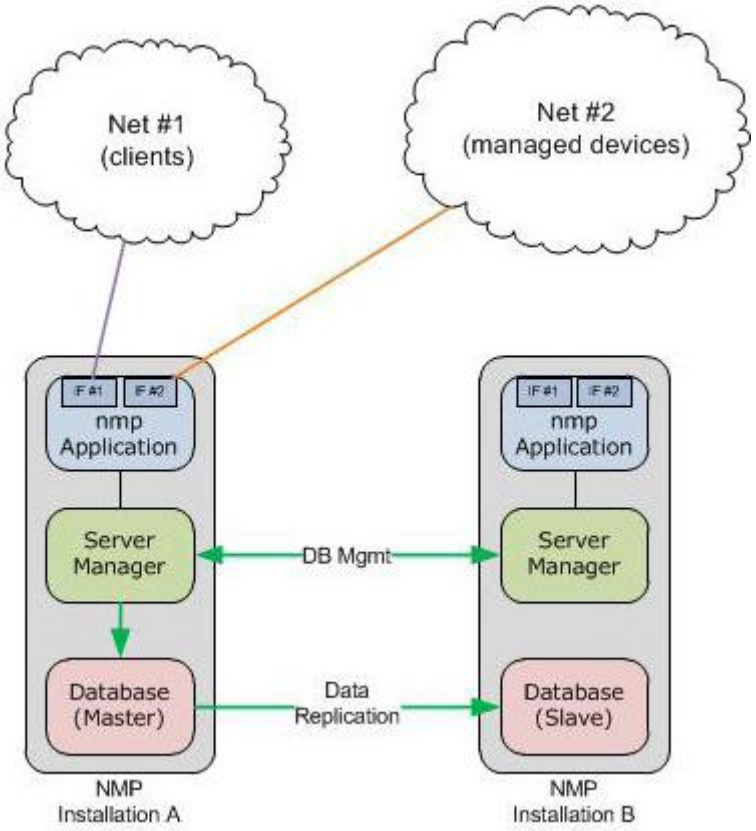

Abbildung 40: Der Master-Server startet neu

7.2.4 Fehler des Slave-Servers

1. NMP Server B (Slave) ist nicht verfügbar
2. NMP Server A (Master) schaltet auf Einzelbetrieb um
3. NMP Server A arbeitet weiterhin normal
4. NMP Server A wartet darauf, dass sein Replikationspartner wieder verfügbar ist

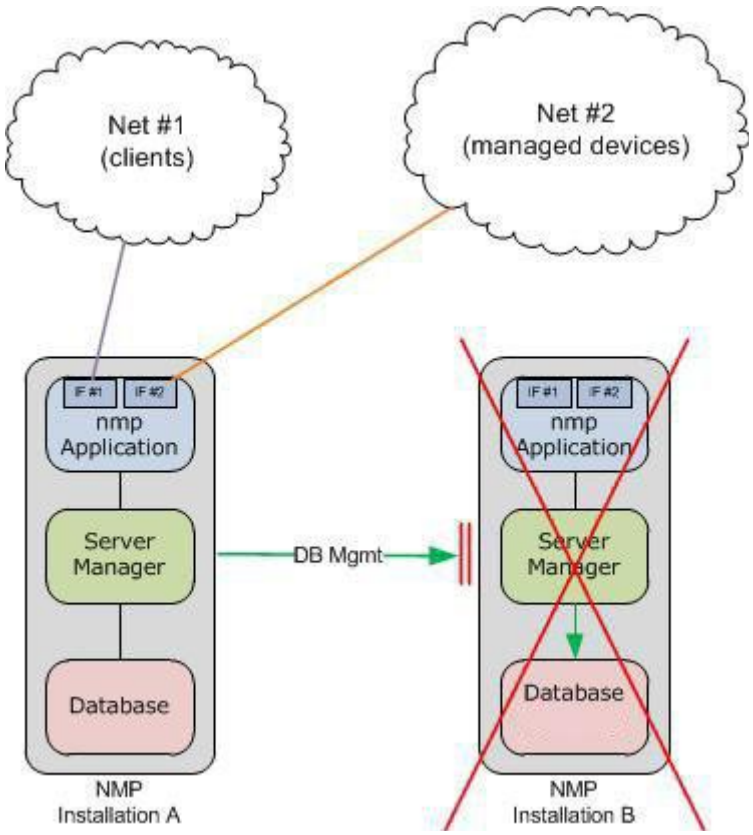

Abbildung 41: Fehler des Slave-Servers

7.2.5 Slave-Server startet nach einem Fehler neu

1. NMP Server A (Master) weist die aktuelle Datenbank auf
2. NMP Server A speichert die Daten in seiner eigenen Datenbank
3. NMP Server B (Slave) startet neu
4. NMP Server B initialisiert die Replikationsprozedur und wartet auf seinen Partnerserver
5. NMP Server A bemerkt, dass sein Replikationspartner wieder verfügbar ist und startet neu im Replikationsmodus
6. Beide Server synchronisieren ihre Datenbanken
7. Die Replikation wird neu initialisiert, beide Server arbeiten in ihren zuvor definierten Betriebszuständen (Master und Slave)

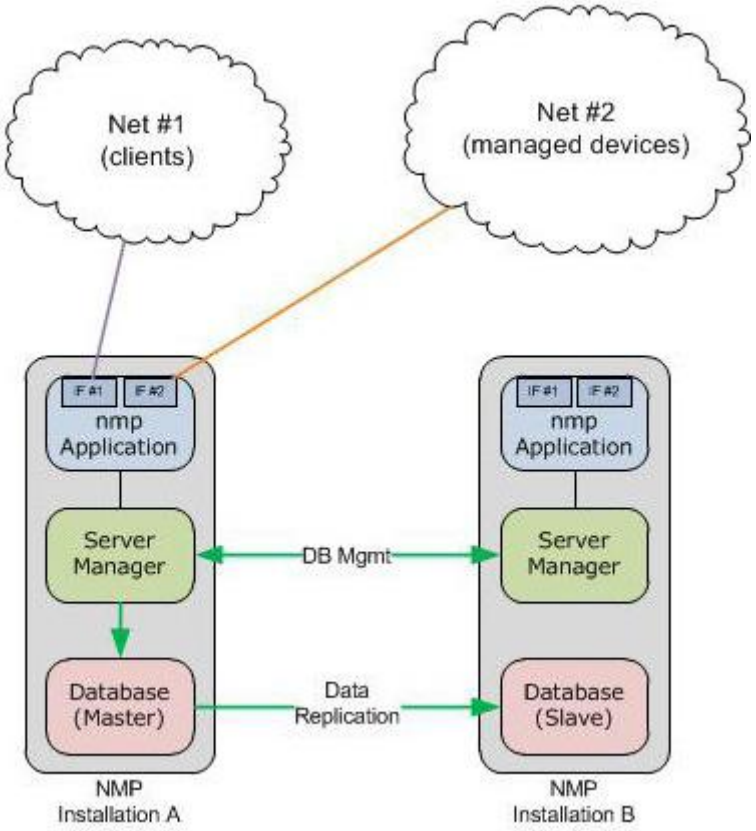

Abbildung 42: Der Slave-Server startet neu

7.2.6 Verbindungsfehler zwischen Master und Slave

1. Die Server sehen sich nicht mehr
2. Beide Server starten neu im Einzelbetriebsmodus
3. Beide Server können Verbindungen von Clients akzeptieren und überwachen verwaltete Geräte
4. Eine Replikation ist nicht möglich
5. Beide Server warten darauf, dass ihre Remote Replikations-Partnerserver wieder verfügbar sind

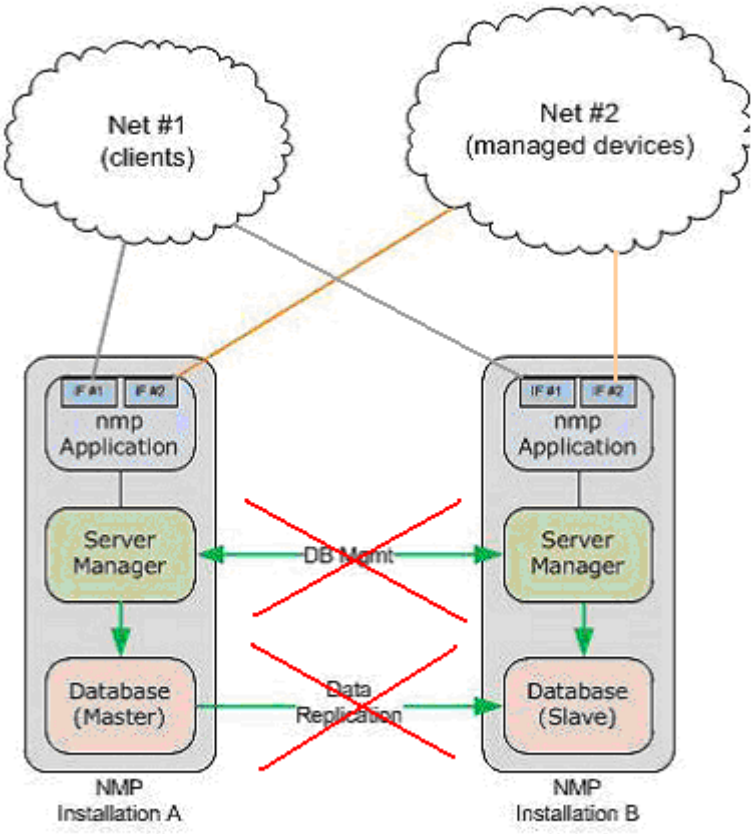

Abbildung 43: Verbindungsfehler zwischen Master und Slave

7.2.7 Wiederherstellung der Verbindung zwischen Master und Slave

1. Beide Server bemerken, dass ihre Replikationspartner wieder verfügbar sind
2. Beide Server starten neu im Replikationsmodus
3. Die Replikation wird neu initialisiert, beide Server synchronisieren ihre Datenbanken
4. NMP Server A agiert als Master-Replikationsserver
5. NMP Server B agiert als Slave-Replikationsserver

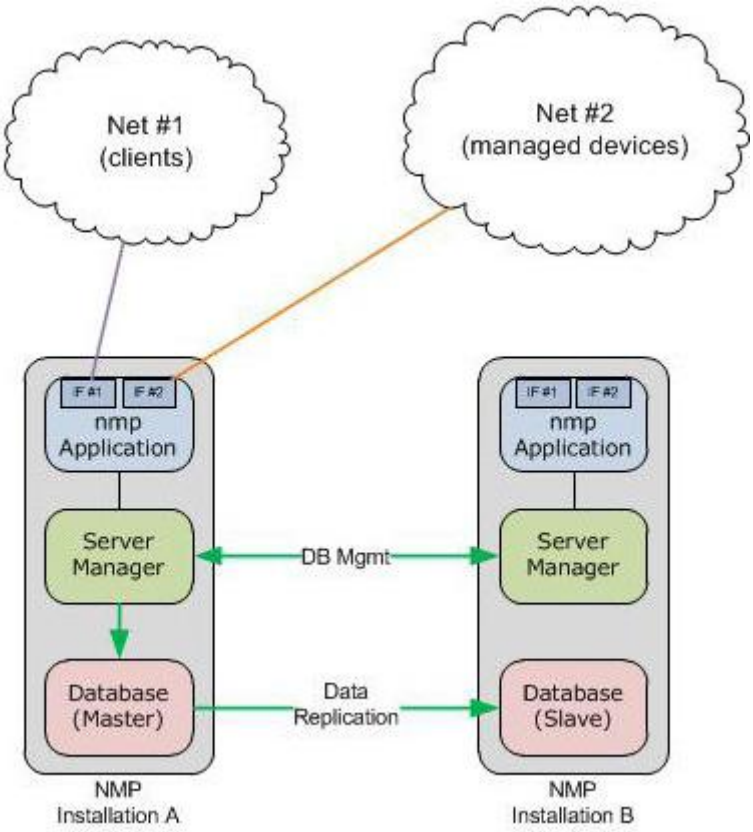

Abbildung 44: Wiederherstellung der Verbindung zwischen Master- und Slave-Servern

8 Client-Applikationen

Client-seitig bezieht sich auf Vorgänge, die von einem Client in einer Client-Server Beziehung in einem Computernetzwerk ausgeführt werden.

Seit NMP Server Version 1.5.8 ist die Verwendung einer standard NMP Applikation (mindestens Version v1.6.5) als Client möglich. Hierfür wurde ein besonderes Protokoll für den Datenaustausch entwickelt und implementiert. NMP Client steht für alle Benutzer mit installierter standard NMP Applikation zur Verfügung.

Alternativ kann auch ein standard Web Browser, der auf dem lokalen Computer des Benutzers mit einem beliebigen Betriebssystem (Windows, Linux, Mac OS, Opera) betrieben wird, als Client-Applikation genutzt werden. Der Web Client stellt nicht alle Funktionen bereit, die mit der NMP Client-Applikation verfügbar sind.

Die empfohlene Bildschirmauflösung für den Web Client beträgt mindestens 1280*1024.

Unterstützte Web Browser:

- Internet Explorer Releases 6, 7, 8 oder neuer
- Mozilla Firefox 3 oder neuer
- Safari 3, 4 oder neuer
- Opera 9.6 oder neuer

Der Web Browser muss Java Script unterstützen. Es müssen keine weiteren Plugins installiert werden.

8.1 NMP Client-Applikation

Dieses Dokument beschreibt die Befehle und besonderen Funktionen der NMP Client-Applikation. Die meisten der NMP Funktionen entsprechen den Funktionen der eigenständigen NMP und NMP Clients. Einige dieser Funktionen sind nur im NMP Client verfügbar, andere sind nur in der eigenständigen NMP Applikation verfügbar. Das NMP Benutzerhandbuch enthält detaillierte Beschreibungen der NMP Befehle und Funktionen.

Zur Verwendung der NMP Applikation als Client für NMP Server benötigt der Benutzer keine weiteren Lizenzdateien. Der NMP Client überprüft die NMP Server Lizenz während des Anmeldevorgangs.

8.1.1 Start des NMP Clients

Bitte verwenden Sie zum Start von NMP im Client-Modus eine der im Windows Startmenü verfügbaren Verknüpfungen („Start/Programs/MICROSENS/MICROSENS NMP Client" oder „MICROSENS NMP Client (Debug mode)").

Beim Start des NMP Clients im Debug-Modus öffnet sich ein weiteres Windows Kommandozeilenfenster (cmd), in dem alle Protokolle und Fehler angezeigt werden.

8.1.2 Anmeldung am Server

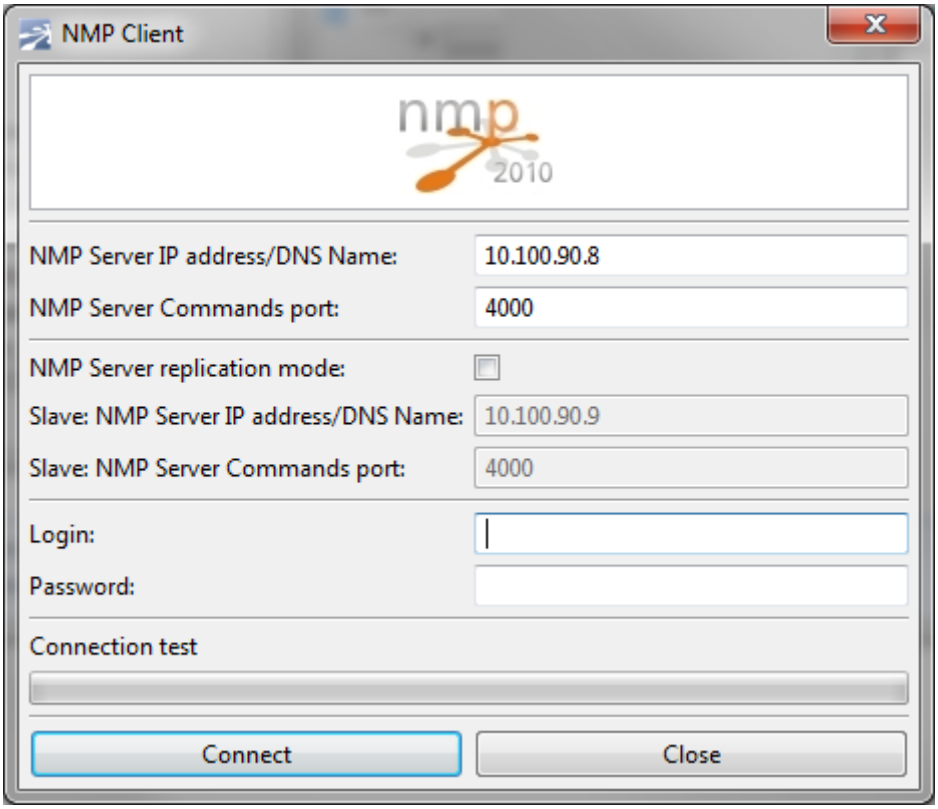

Abbildung 45: Dialog „NMP Client-Login"

Zur Kommunikation des NMP Clients mit der Server-Applikation muss der Benutzer die NMP Server IP-Adresse und die Befehls-Portnummer angeben. Alle weiteren Konfigurationsparameter (FTP-Port, Datenbank-Serverport) werden automatisch vom Server bezogen. Ein gültiger Benutzername und ein gültiges Passwort sind ebenfalls erforderlich.

Wenn NMP Server im Master-Slave Replikationsmodus betrieben wird, kann der Benutzer auch die IP-Adresse und die Befehls-Portnummer des Slave-Servers angeben. Der NMP Client wird immer versuchen, sich zuerst mit dem Master-Server zu verbinden. Im Fehlerfall (der Master-Server ist nicht verfügbar) wird er jedoch versuchen, eine Verbindung mit dem Slave-Server aufzubauen. Hierzu wird NMP Client die angegebene Slave-Server IP-Adresse und den spezifizierten Befehlsport verwenden.

Die Standardeinstellungen sind:

- Systemadministrator
  - Berechtigungsebene: sysadmin
  - Passwort: sysadmin
- Administrator
  - Berechtigungsebene: admin
  - Passwort: admin
- Manager
  - Berechtigungsebene: manager
  - Passwort: manager
- Benutzer
  - Berechtigungsebene: user
  - Passwort: user

Die Applikation stellt einen „User Manager" bereit, mit dessen Hilfe Benutzer-konten hinzugefügt, gelöscht oder geändert werden können. MICROSENS empfiehlt die Zuweisung Ihres eigenen Passworts nach der ersten Verwendung. Auf diese Weise wird eine unauthorisierte Verwendung der Software vermieden.

Bitte bedenken Sie, dass mindestens ein Benutzer mit „Systemadministrator" Rechten existieren muss. Die Applikation wird Sie daran hindern, das letzte Konto mit „Systemadministrator" Rechten zu löschen oder dessen Rechte zu ändern.

Benutzerstufen

Zugang	unauth.	Benutzer	Manager	Admin	System Admin
Gerätedaten	–	RO	RW (RO für IP Einstel-lungen)	RW	RW
Geräteliste	–	RO	RO	RW	RW
Benutzerdaten	–	–	–	–	RW
Applikationsdaten	–	–	–	–	RW

RO – Read Only (Nur Lesen); RW – Read/Write (Lesen/Schreiben)

Sollte die NMP Client-Applikation bzw. das Betriebssystem abstürzen und ein Benutzer die Client-Applikation nicht mehr korrekt schließen können, meldet NMP Server den Benutzer automatisch nach einem Zeitraum von 5 Minuten ohne Benutzeraktivität ab.

Bei einem normalen Schließen der NMP Client-Applikation wird der Benutzer automatisch vom NMP Server abgemeldet.

8.1.3 Synchronisierung der Geräteliste

Nach einer erfolgreichen Anmeldung synchronisiert NMP Client automatisch die lokale Geräteliste mit der Geräteliste des NMP Servers.

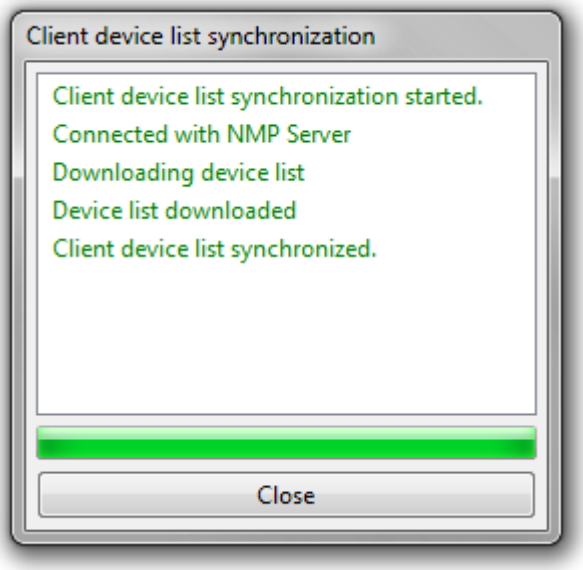

Abbildung 46: Synchronisierung der Geräteliste

Jeder NMP Client hat dieselbe Gerätelistenversion wie der NMP Server.

Zur Editierung der Geräteliste muss der Benutzer die lokale Kopie der Geräteliste entsperren. Damit wird die Geräteliste des Servers automatisch gesperrt. Dies ist möglich solange die Geräteliste des Servers nicht bereits von einem anderen Benutzer gesperrt wurde. In einem solchen Fall wird ein Nachrichtenfenster angezeigt, dieses enthält den Namen des Benutzers, der die Geräteliste des Servers gesperrt hat.

Zum Sperren bzw. Entsperren der lokalen Geräteliste kann der Befehl „Unlock/lock device list" in der Menüzeile des NMP Clients („Edit") genutzt werden. Sie können auch das Schloß-Symbol in der NMP Client-Baumansicht verwenden.

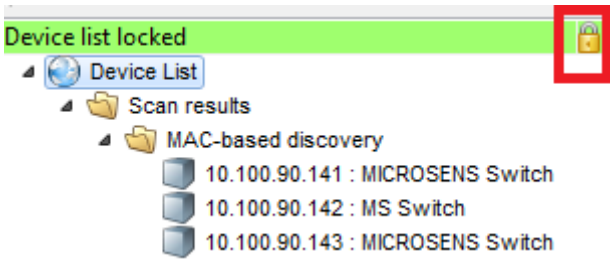

Abbildung 47: Sperren/Entsperren der Geräteliste

Im Anschluss an die Durchführung der Änderungen der Geräteliste muss der Benutzer seine lokale Kopie der Geräteliste sperren. In diesem Fall wird ein Dialogfeld angezeigt. Der Benutzer muss entscheiden, ob die Geräteliste des Servers synchronisiert wird oder nicht. Sollte die Geräteliste des Servers nicht synchronisiert werden, wird der NMP Client die Geräteliste des Servers laden und alle lokalen Änderungen gehen verloren. Bei einer Synchronisierung der Geräteliste wird die modifizierte Geräteliste zum Server gesandt. Alle verbundenen Clients (NMP Clients und Web Clients) erhalten die aktualisierte Geräteliste binnen einer Minute. Die Geräteliste des Servers wird entsperrt.

Nur Benutzer mit admin- oder sysadmin-Rechten können die Geräteliste editieren.

Der Prozess der Synchronisierung der Geräteliste ist automatisiert. Eine manuelle Synchronisierung der lokalen Geräteliste mit der des Servers ist jedoch ebenfalls möglich. Zur Durchführung der manuellen Synchronisierung sollten Befehle aus dem Menü „Edit" genutzt werden:

Synchronize local client device list: Die neue Liste wird vom Server geladen.

Synchronize remote sever device list: Die lokale Geräteliste wird zum Server gesandt.

Die Geräteliste der standard NMP Applikation kann ebenfalls genutzt werden. Hierzu wird die NMP Client-Geräteliste entsperrt und mithilfe des Befehls „Open" importiert. Anschließend wird die Liste des lokalen NMP Clients gesperrt.

8.1.4 Besondere Befehle des NMP Clients

In diesem Abschnitt werden spezifische Befehle des NMP Clients beschrieben. Alle hier nicht beschriebenen Befehle sind im NMP Benutzerhandbuch beschrieben.

8.1.4.1 Benutzer ändern

Dieser Befehl ist Bestandteil des Menüs „File\Change User".

Der Befehl ermöglicht die erneute Anmeldung mit einem neuen Benutzernamen und Passwort. Der Benutzer kann sich auf einfache Art und Weise ohne Neustart des NMP Clients mit einem anderen Konto bei NMP Server anmelden (z.B. mit anderen Zugriffsrechten). Nach Auswahl dieses Befehls öffnet sich das NMP Client-Anmeldefenster.

8.1.4.2 Geräteliste Sperren/Entsperren

Dieser Befehl ist Bestandteil des Menüs „Edit\Lock\Unlock device list".

Entsperrt die Geräteliste zum Zweck der Editierung. Die Geräteliste des Servers wird gesperrt und kein anderer Benutzer kann die Geräteliste zu diesem Zeitpunkt editieren. Nach erfolgreicher Durchführung der Änderungen muss die lokale Geräteliste gesperrt werden. Die lokale Kopie wird anschließend mit der Geräteliste des Servers synchronisiert und diese dann entsperrt. Nach Beendigung dieser Aktion werden alle verbundenen Clients binnen einer Minute mit der aktualisierten Geräteliste synchronisiert.

8.1.4.3 Synchronisiere die lokale Geräteliste

Dieser Befehl ist Bestandteil des Menüs „Edit\Synchronize local client device list".

Nach jeder Aktualisierung synchronisiert der NMP Client die lokale Geräteliste automatisch mit der auf dem Server befindlichen Kopie. Mithilfe dieses Befehls kann die Synchronisierung der lokalen Geräteliste auch manuell ausgelöst werden.

8.1.4.4 Synchronisiere die Remote Server-Geräteliste

Dieser Befehl ist Bestandteil des Menüs „Edit\Synchronize remote server device list".

Führt eine manuelle Synchronisierung der Geräteliste des Servers mit der lokalen Kopie durch.

8.1.4.5 RMA IP-Bereich Scanner

Dieser Befehl ist Bestandteil des Menüs „Tools\RMA IP Range scanner".

Der RMA-Scanner wird für den Scan eines definierten IP-Adressbereichs von neuen Geräten genutzt (verbunden, um defekte Geräte zu ersetzen). Falls in dem definierten IP-Bereich ein neues Gerät gefunden wird, wird eine neue Gruppe mit dem Namen „RMA-Liste" und eine Untergruppe mit einem Bereichs-Alias automatisch in der Baumliste erzeugt. Alle gefundenen Geräte sind Bestandteil dieser Gruppe.

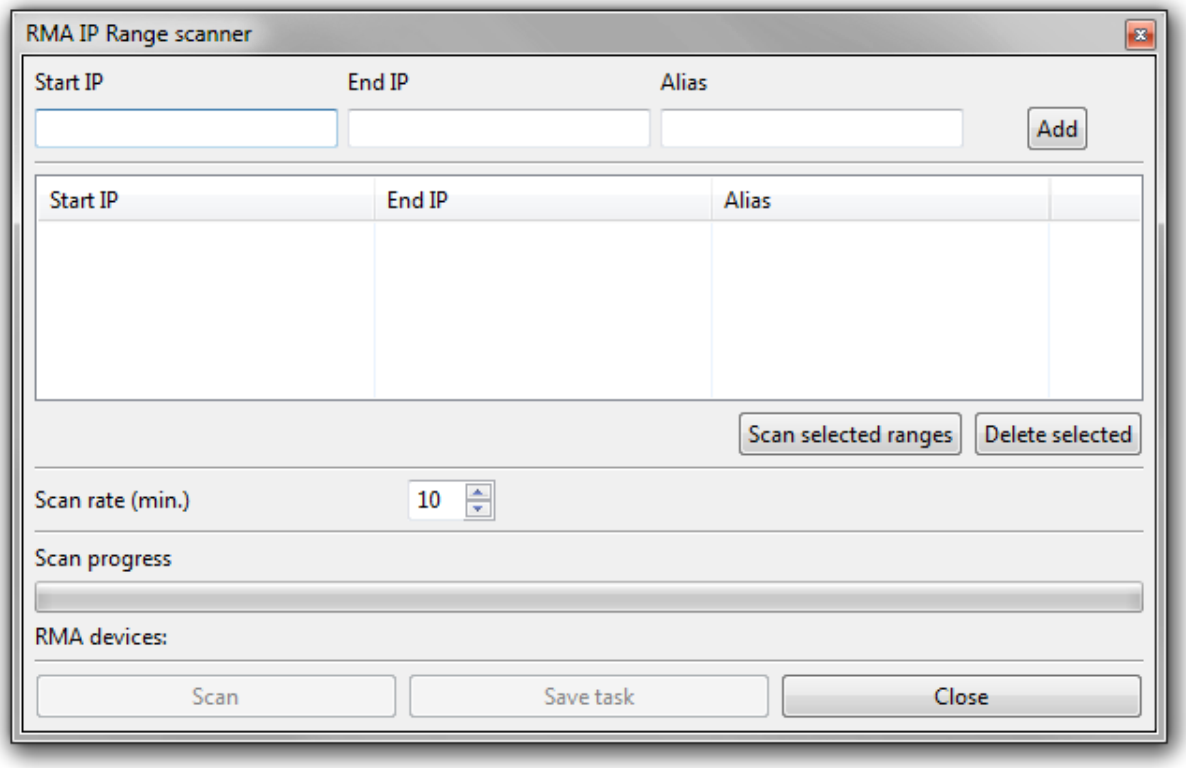

Abbildung 48: Dialog RMA IP-Bereich Scanner

Es kann eine Anzahl kleinerer Bereiche anstelle eines großen Bereichs definiert werden. Der Scan einer Anzahl kleinerer Bereiche beschleunigt den Scanvorgang. Der Scanvorgang kann auch für einen einzelnen in der Tabelle ausgewählten Bereich gestartet werden.

Der RMA IP-Bereich Scanner bietet die Option einer geplanten Ausführung der „Scanaufgabe". Die Aufgabe wird alle x Minuten gestartet (Scanrate: 10…120) und kann aus der „Übersicht geplanter Aufgaben" gelöscht oder dort editiert werden (Befehl: „Tools\Scheduled tasks viewer").

8.1.4.6 RMA-Gerätekonfigurator

Dieser Befehl ist Bestandteil des Menüs „Tools\RMA Device configurator".

Der „RMA Device Configurator" wird zur Rekonfiguration der neuen Geräte (verbunden, um defekte Geräte zu ersetzen) in der vom „RMA IP-Bereich Scanner" erzeugten „RMA-Liste" genutzt.

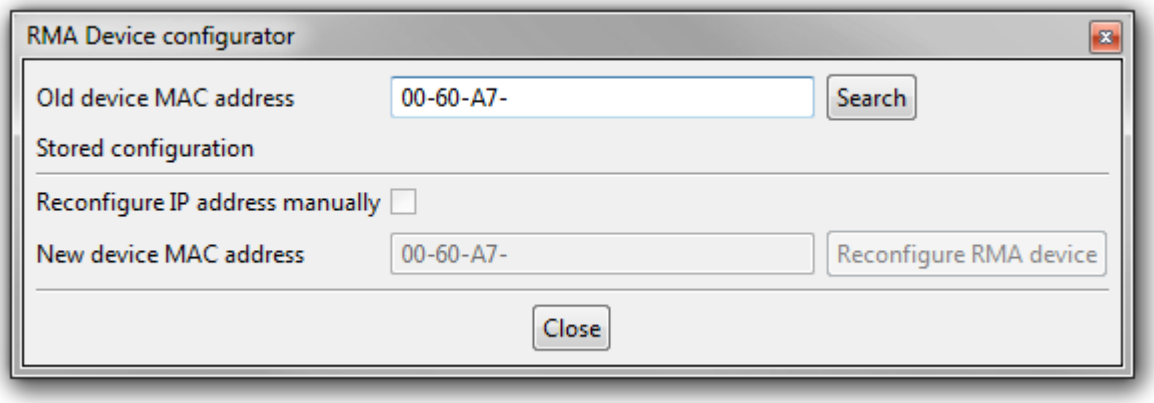

Abbildung 49: Dialog „RMA Device Configurator"

Zur Rekonfiguration eines neuen Geräts wählen Sie den Ordner mit den gespeicherten Konfigurationsdateien aus, geben die IP-Adresse des alten (defekten) Geräts ein und betätigen die Schaltfläche „Suche". Die gespeicherte Konfigurationsdatei des defekten Geräts wird gesucht. Die Schaltfläche „IP-Adresse manuell konfigurieren" und das Textfeld „MAC-Adresse des neuen Geräts" werden aktiviert, sobald die Konfiguration gefunden wurde.

Geben Sie die MAC-Adresse des neuen Geräts ein und betätigen Sie die Schaltfläche „Rekonfiguration starten". Falls das Gerät in der „RMA-Liste" verfügbar ist, wird die alte Gerätekonfiguration (einschließlich der IP-Einstellungen) automatisch auf das neue Gerät übertragen. Erfolgs- oder Fehlermeldungen werden in einem Nachrichtenfenster aufgeführt.

Der NMP Server-Administrator sollte eine geplante Aufgabe zur Durchführung eines Backups der Gerätekonfiguration erzeugen oder eine manuelle Datensicherung der Konfigurationen ausführen. Die automatische Rekonfiguration eines RMA-Geräts ist nur dann möglich, wenn in der NMP Server-Datenbank eine alte Gerätekonfiguration verfügbar ist.

8.1.4.7 Stored Device Configurations Viewer

Dieser Befehl ist Bestandteil des Menüs „Tools\Stored device configurations viewer".

Das Werkzeug ermöglicht die Betrachtung und Löschung der gespeicherten Gerätekonfigurationen.

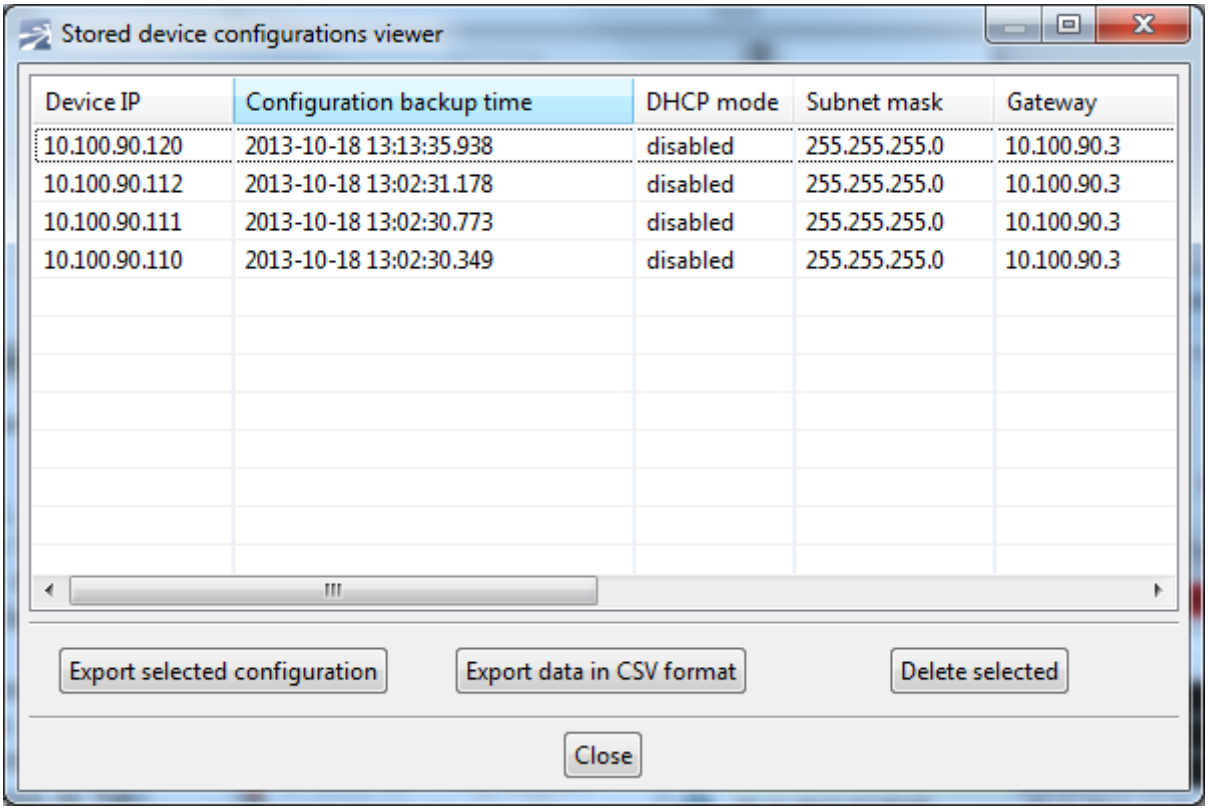

Abbildung 50: Fenster „Stored Device Configurations Viewer"

Gerätekonfigurationen können manuell gespeichert werden. Hierzu dient der Befehl „Device configuration load/save" im Kontextmenü der Baumansicht oder die automatische Definition der „Scheduled configuration backup"-Aufgabe (geplantes Backup der Konfiguration).

Durch Betätigen der Schaltfläche „Export selected configuration" kann der Benutzer die Konfigurationsdatei für eine spätere Verwendung aus der Datenbank exportieren (z.B. Senden der Konfiguration an ein Gerät mit einer eigenständigen NMP Applikation).

8.1.4.8 Benutzer Manager

Dieser Befehl ist Bestandteil des Menüs „Tools\User manager".

Mithilfe des Benutzermanager-Werkzeugs können Benutzerkonten hinzugefügt, gelöscht oder editiert werden. Zum Hinzufügen eines neuen Benutzerkontos werden alle Felder benötigt (Vorname, Nachname, E-Mail, Anmeldename und Passwort). Der Anmeldename muss eindeutig sein; NMP warnt, falls der eingegebene Anmeldename in der Datenbank bereits existiert. Achtung: es muss mindestens ein Benutzerkonto mit „Systemadministrator"-Rechten existieren (da nur ein Systemadministrator Benutzerkonten editieren kann). Die Applikation warnt, falls versucht wird, die Rechte des letzten „Systemadministrator" Kontos zu löschen oder zu verändern.

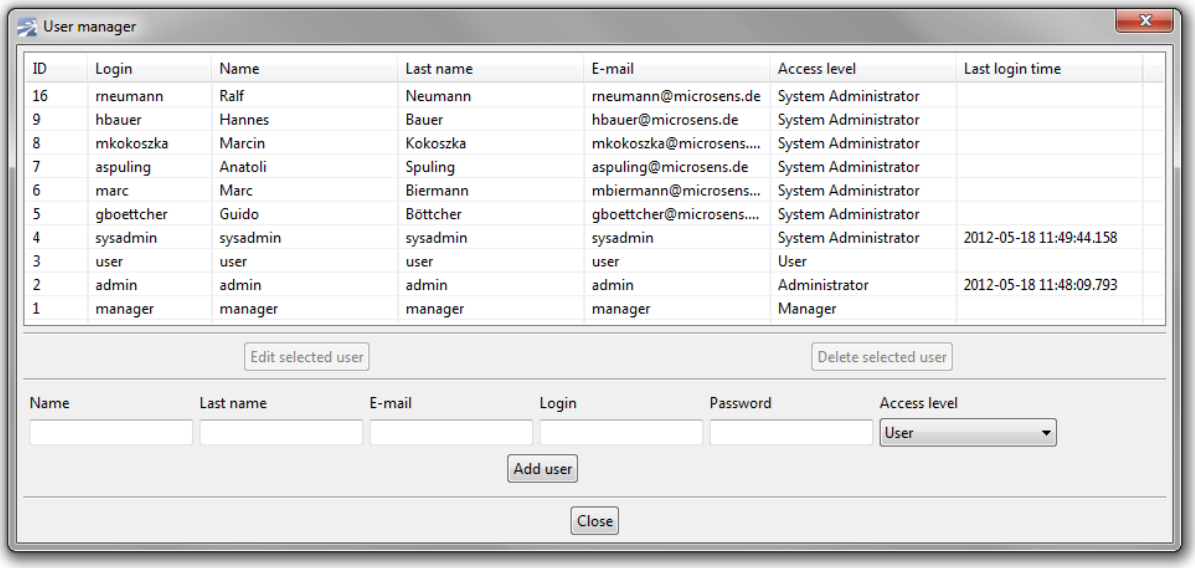

Abbildung 51: Fenster „User Manager"

Die Anzahl der möglichen Benutzerkonten-IDs wird durch die NMP Server-Lizenzdatei definiert.

8.1.4.9 Eigenes Konto editieren

Dieser Befehl ist Bestandteil des Menüs „Tools\Edit my account".

Dieses Werkzeug ermöglicht die Änderung des eigenen Passworts. Die Option ist für alle Benutzertypen verfügbar.

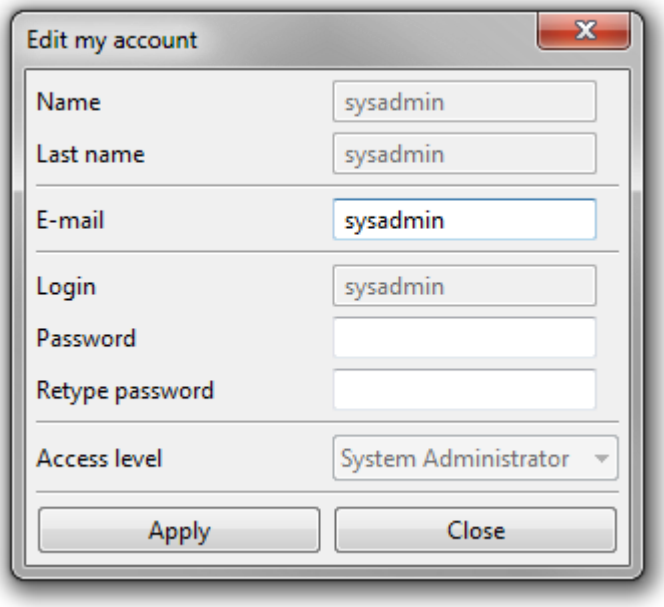

Abbildung 52: Dialog „Edit my Account"

8.1.4.10 DHCP-Autokonfiguration / Erzeuge Konfigurationsdatei

Erzeugt eine Konfigurationsdatei für die DHCP-Autokonfiguration. Weitere Details sind im Abschnitt *Switch DHCP-Autokonfiguration* enthalten.

8.1.4.11 DHCP-Autokonfiguration / Editiere Konfigurationsdatei

Editiert eine Konfigurationsdatei für die DHCP-Autokonfiguration. Weitere Details sind im Abschnitt *Switch DHCP-Autokonfiguration* enthalten.

8.1.4.12 DHCP-Autokonfiguration/DHCP-Autokonfigurationsdateien

Hier kann der Client für den einfachen Versand, den Download oder die Löschung von Konfigurations- und Firmware Dateien genutzt werden, die von NMP Server im Rahmen der Prozeduren zur DHCP-Autokonfiguration benötigt werden. Weitere Details sind im Abschnitt *Switch DHCP-Autokonfiguration* enthalten.

8.1.4.13 NMP Server – Status

Dieser Befehl ist Bestandteil des Menüs „Tools\NMP Server – Status".

Hiermit kann der aktuelle NMP Server-Status geprüft werden. Es stehen drei separate Register für die folgenden Informationen bereit:

- Server-Betriebszeit
- Datenbankgröße
- Verbundene Clients
- Replikationsstatus und Konfiguration
- NMP Server-Konfiguration

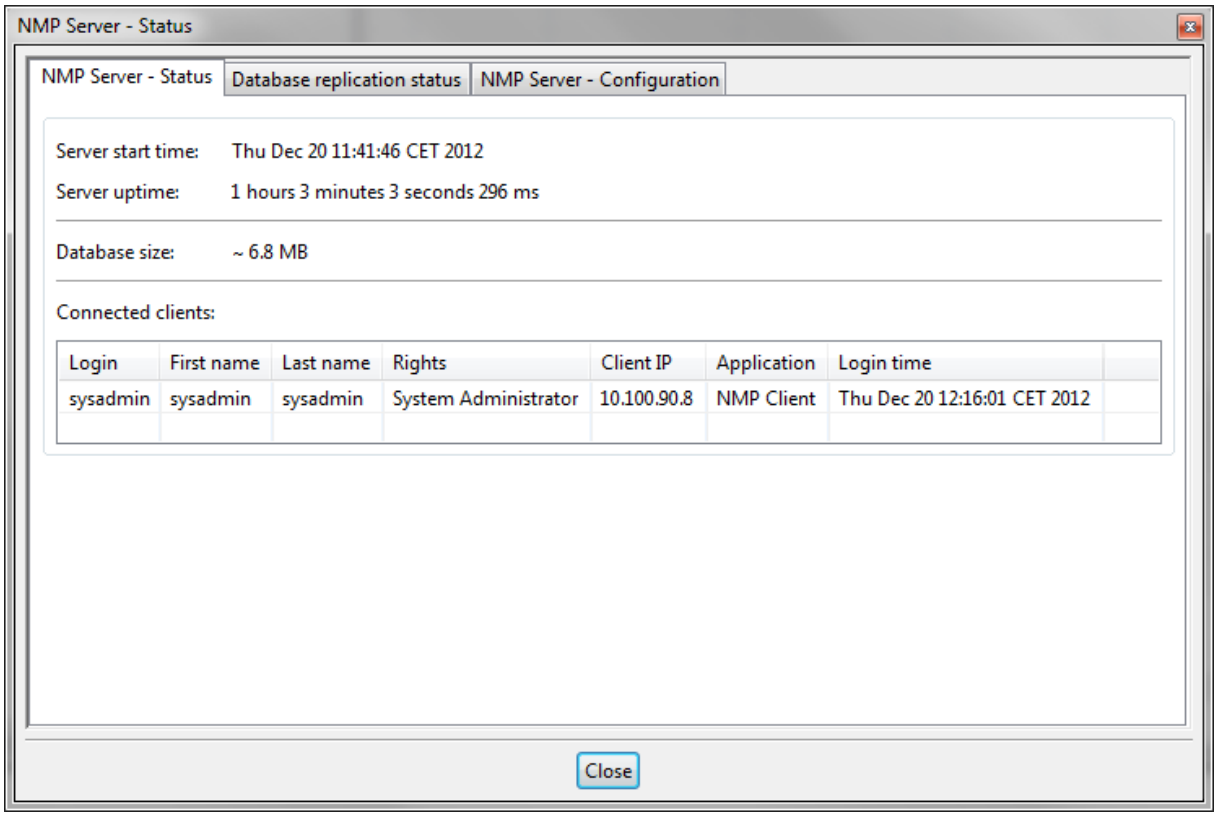

Abbildung 53: Fenster „NMP Server – Status"

Dieser Befehl steht nur Benutzern mit „sysadmin"-Rechten zur Verfügung.

8.1.4.14 Server-Lizenzinformation

Dieser Befehl ist Bestandteil des Menüs „Tools\Server licence information”.

In diesem Fenster werden Informationen zur gegenwärtig installierten Server Lizenzdatei dargestellt.

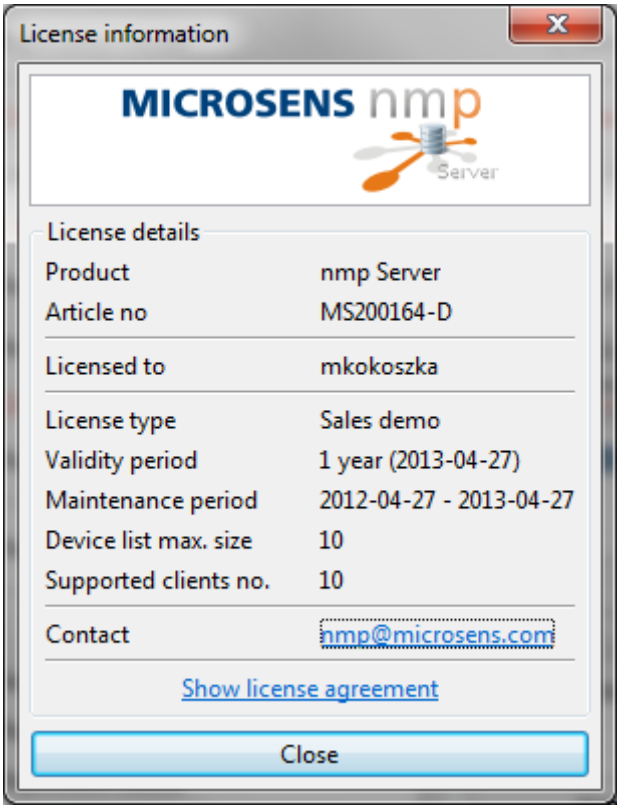

Abbildung 54: Fenster „Licence Information”

8.1.4.15 Gerätehistorie

Dieser Befehl ist Bestandteil des Gerätebaum Kontextmenüs „Device history”.

NMP Server protokolliert die Geräteverfügbarkeit und Temperatur. Zusätzlich werden Informationen über die eingesteckten SFP-Module (Temperatur, Spannung, Bias, TX/RX Leistung) gespeichert. Alle gespeicherten Daten werden in einer Historienübersicht dargestellt. Zum Öffnen der Historiensicht wird der Befehl „Device history\Device history charts” verwandt.

Das Werkzeugt erlaubt die Sicht auf die kürzliche Historie (vordefinierte Zeiträume):

- 30 Minuten
- 1 Stunde
- 12 Stunden
- 24 Stunden
- 1 Woche
- 1 Monat
- 6 Monate
- 1 Jahr
- Alles

Alternativ kann ein Zeitraum manuell eingegeben werden (um mehr Details des gewählten Zeitraums sehen zu können).

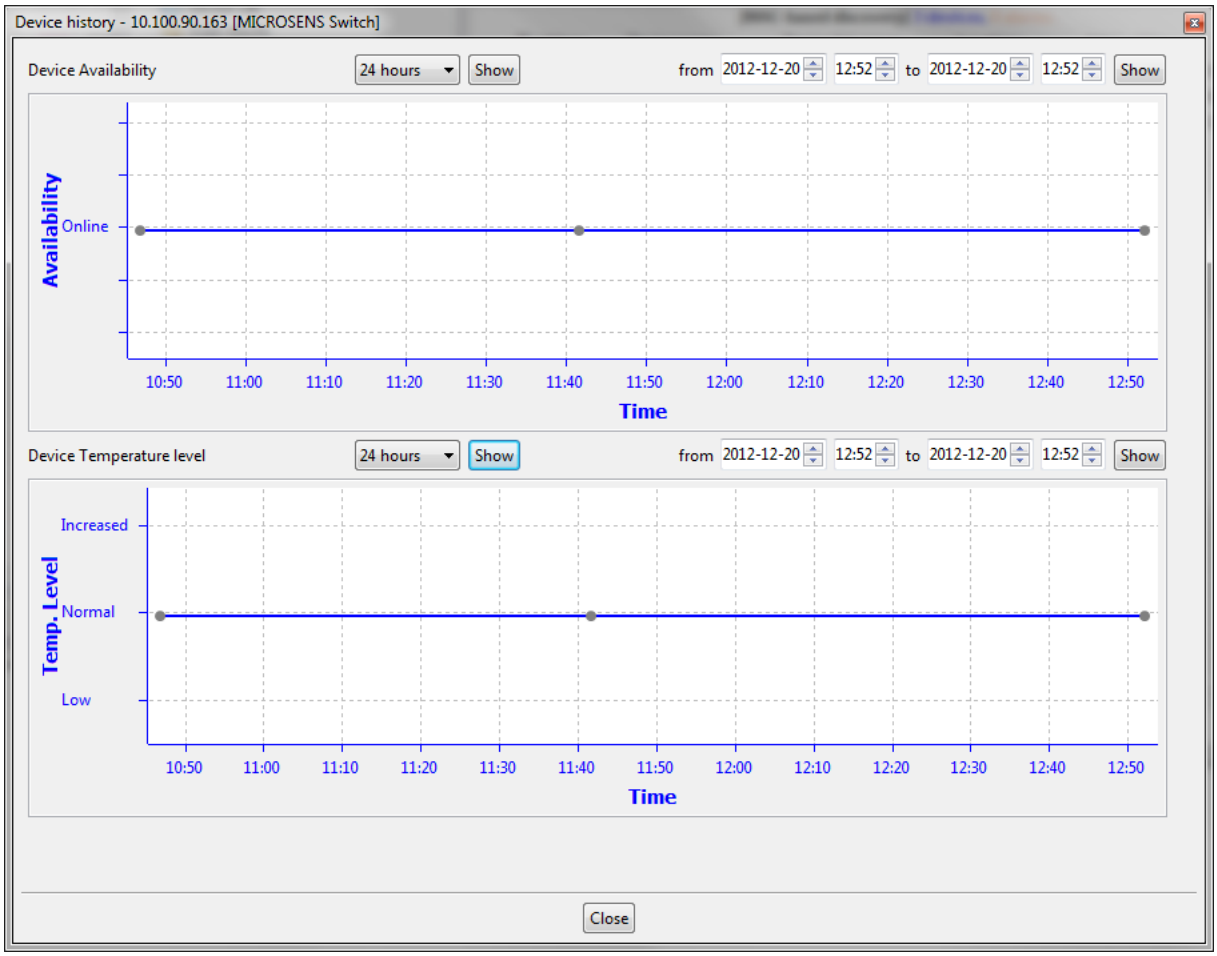

Abbildung 55: Diagramm „Device History"

Ein Benutzer mit „admin”- oder „sysadmin”-Rechten kann die Gerätehistorie über den Befehl „Device history\Clear history” löschen.

Gegenwärtig ist die Darstellung der Gerätehistorie nur für MICROSENS Switche verfügbar.

8.1.4.16 Unbenutzte Geräte finden

Dieser Befehl ist Bestandteil des Gerätebaum Kontextmenüs „Find unused devices”.

Dieses Werkzeug ermöglicht das Auffinden ungenutzter Geräte (nur MICROSENS Switche). Es werden Geräte identifiziert, die seit einem definierten Datum nicht aktiv über den Client-Port verbunden wurden (kein Uplink/Downlink Port).

Die Ergebnisse werden in einer Tabelle dargestellt und können als *.csv Datei exportiert werden. Die Suchergebnisse können auch der Geräteliste hinzugefügt werden. Hierzu wird im Gerätebaum eine zusätzliche Gruppe „Unused devices” angelegt.

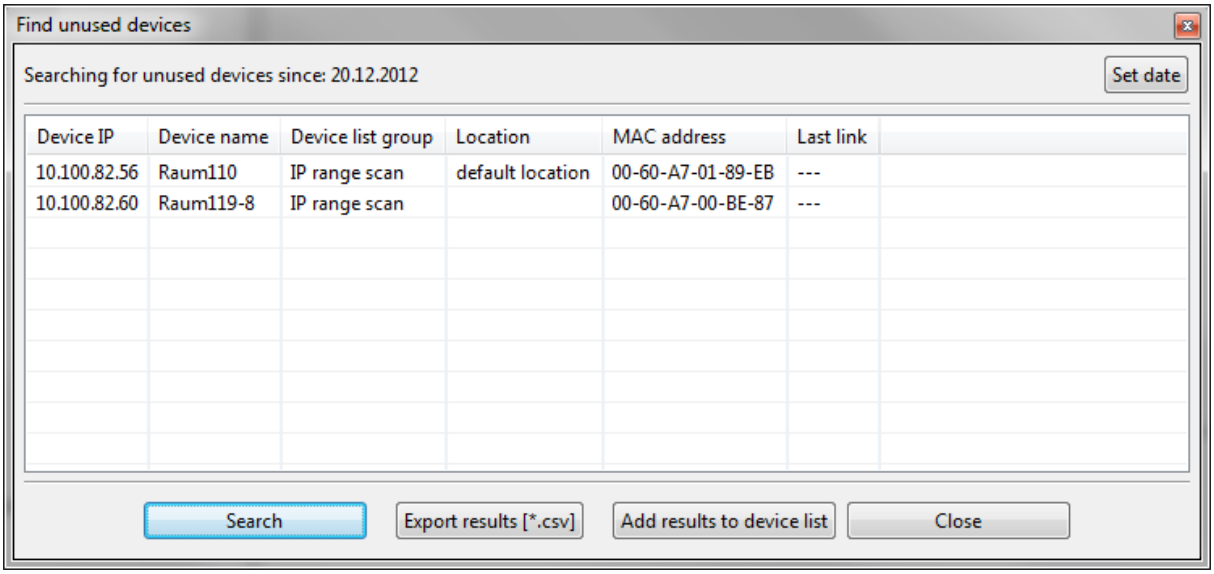

Abbildung 56: Fenster „Unused Device Finder“

8.2 Web Client-Applikation

Nach dem Start von Network Management Platform Server kann – sofern der NMPS HTTP-Server aktiviert ist – jeder Web Browser für den Zugang zum Server genutzt werden. Der Zugriff auf den Server erfolgt über eine der folgenden URL-Adressen:

- http://server_ip_address:http_server_port
  – für standard HTTP-Verbindungen oder
- https://server_ip_address:https_server_port
  – für sichere HTTP-Verbindungen (falls sicheres HTTP konfiguriert wurde)

8.2.1 Anmeldung

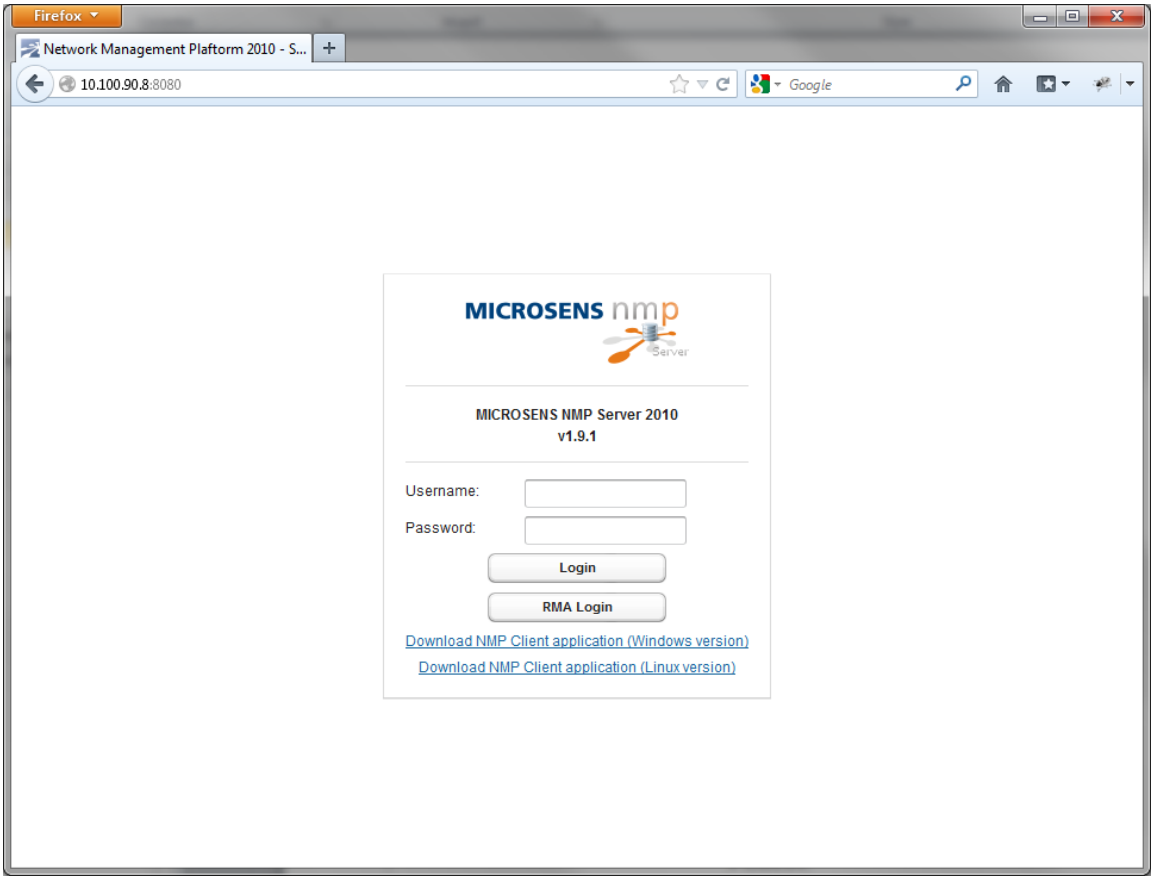

Abbildung 57: Web Client-Anmeldedialog

Geben Sie für den Zugriff auf die NMP Server Web-Applikation einen Benutzernamen und ein Passwort ein. Die Standard-Benutzerkonten und Benutzer-Zugriffsstufen sind im Abschnitt „*Anmeldung zum Server*" beschrieben.

Die Anmeldeseite stellt auch eine „RMA-Login”-Schaltfläche zur Verfügung, die das „RMA Device Configurator” Werkzeug öffnet. Dieses Werkzeug steht auch nach einer normalen Anmeldung zur Verfügung (Befehl in der Menüzeile „Tools\RMA Device configurator”). Weitere Informationen über das RMA-Werkzeug sind im Abschnitt *RMA-Gerätekonfigurator* enthalten.

Für den Download der NMP Client-Applikation werden zwei Links bereitgestellt (für die Windows- bzw. die Linux-Version).

8.2.2 Hauptfenster

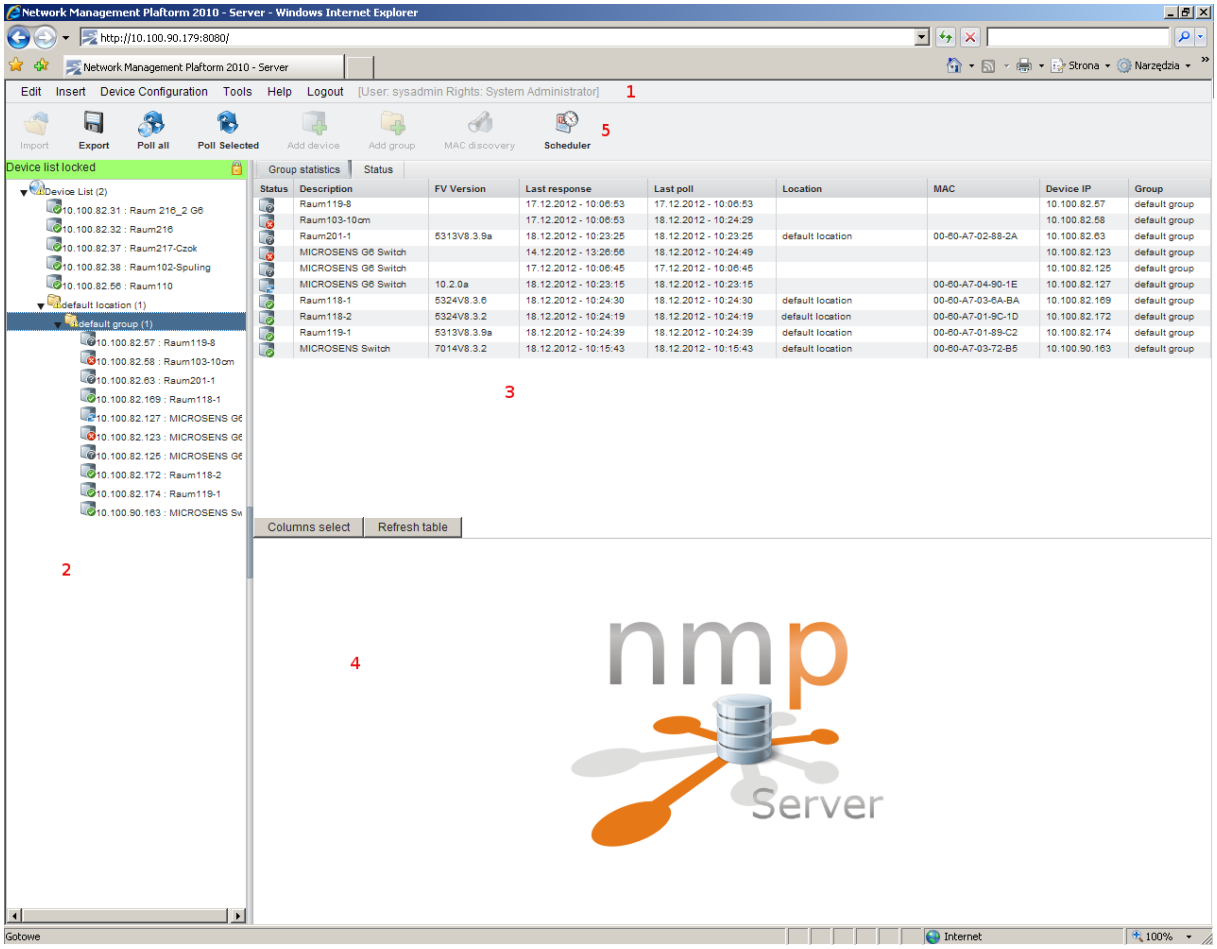

Abbildung 58: Fenster „Web Client Main Window”

Das Hauptfenster der Netzwerk Management Plattform Software besteht aus den folgenden Hauptelementen:

- Hauptmenü (1)
- Baumdarstellung der Geräteliste (2)
- Geräteliste/Gerätestatus-Informationsfenster (3)
- Fenster grafische Gerätedarstellung (4)
- Hauptmenü-Symbolleiste *(5)*

Das NMP Benutzerhandbuch enthält detaillierte Beschreibungen dieser Elemente.

9 Disclaimer

Alle in diesem Dokument enthaltenen Informationen werden als „wie gesehen" bereitgestellt und können jederzeit ohne vorherige Ankündigung geändert werden.

MICROSENS GmbH & Co. KG übernimmt keine Verantwortung für die Richtigkeit, Vollständigkeit oder Qualität der bereitgestellten Informationen, der Tauglichkeit für eine besondere Anforderung oder für Folgeschäden.

Alle hierin erwähnten Produktnamen können Warenzeichen und/oder eingetragene Warenzeichen der jeweiligen Unternehmen sein.

MK/aku MS20016x_NMP_SRV_MAN_DE_V1.0.0.Doc