



**Beratung und Support**  
**Technische Plattform**  
**Support-Netz-Portal**

---

paedML® – stabil und zuverlässig vernetzen

# Installationsanleitung

Neu-Installation von paedML Novell-GMS 18.1.1

Stand 25.05.2019

## paedML® Novell

Version: Version → bitte eingeben

## **Impressum**

### **Herausgeber**

Landesmedienzentrum Baden-Württemberg (LMZ)  
Support-Netz  
Rotenbergstraße 111  
70190 Stuttgart

### **Autoren**

der Zentralen Expertengruppe Netze (ZEN),  
Support-Netz, LMZ

Holger Dzeik  
Stefan Falk  
Ulrich Frei  
Carl Heinz Gutjahr  
Stephan Kluge  
Uwe Labs  
Alfred Wackler

### **Endredaktion**

Alfred Wackler

### **Bildnachweis**

Symbole von "The Noun Project" ([www.thenounproject.com](http://www.thenounproject.com))

### **Weitere Informationen**

[www.support-netz.de](http://www.support-netz.de)  
[www.lmz-bw.de](http://www.lmz-bw.de)

**Änderungen und Irrtümer vorbehalten.**

Veröffentlicht: 2019

Die Nutzung dieses Handbuches ist ausschließlich für eigene Zwecke zulässig. Die Nutzung sowie die Weitergabe dieses Handbuches zu kommerziellen Zwecken wie z.B. Schulungen ist nur nach ausdrücklicher Einwilligung durch das LMZ erlaubt.

© Landesmedienzentrum Baden-Württemberg

## Inhaltsverzeichnis

<b>1</b>	<b>Voraussetzungen.....</b>	<b>4</b>
<b>2</b>	<b>Installation GMS-OVA .....</b>	<b>5</b>
2.1	LMZ-Paket .....	5
2.2	Einspielen der gms1811.ova.....	5
2.3	Firewallregel für den GMS-Server erstellen.....	8
<b>3</b>	<b>Anpassungen des GMS .....</b>	<b>11</b>
3.1	Vorbereitungen am GServer03 .....	11
3.2	Konfiguration des GMS.....	18
<b>4</b>	<b>SLES Patch .....</b>	<b>22</b>
4.1	Automatische Online Updates .....	22
4.2	Hintergrundbilder .....	23
<b>5</b>	<b>Schluss .....</b>	<b>23</b>
<b>Anhang A (Zertifikat).....</b>		<b>25</b>
Erzeugung des Zertifikats .....		25
Bereitstellung des Zertifikats .....		26
<b>Anhang B (Nat-Regeln).....</b>		<b>27</b>
<b>Anhang C (Tipps).....</b>		<b>29</b>
Tipp 1	.....	29
Tipp 2	.....	30

## Vorwort

Diese Anleitung beschreibt die Einrichtung des *GroupWise Mobility Server 18* in der Version 18.1.1.

Der GroupWise Mobility Service ermöglicht die Synchronisation zwischen GroupWise Email-Konten und mobilen Geräten. Die Synchronisation umfasst Email, Termine, Kontakte, Nachrichten und Telefon-Nachrichten.

Diese Anleitung beschreibt das Einspielen eines SLES 12 SP3-Servers, auf dem GMS installiert ist, das vor Ort noch schulspezifisch angepasst werden muss.

## 1 Voraussetzungen

Um den *paedML Novell GMS* Server einzusetzen, benötigen Sie einen Virtualisierungsserver, z.B. auf Basis von *VMware ESXi*, auf dem genügend Speicherplatz im DataStore für die **neue virtuelle Maschine** ist.

### Systemvoraussetzungen:

Um eine schulgerechte einfache Installation zu erhalten, haben wir uns für den Einsatz von GMS auf eine Ein-Server-Lösung beschränkt. Laut Angaben von Micro Focus (Novell) ist diese geeignet für 750 Benutzer / 1000 mobile Geräte.

Für den Server werden empfohlen:

4 CPUs  
4 GB RAM (für 300 mobile Geräte)  
8 GB RAM (für 750 Benutzer / 1000 mobile Geräte)

Prüfen Sie also, ob diese Ressourcen auf Ihren ESXi-Host zur Verfügung stehen (CPUs können „überbucht“ werden, RAM nicht).

Die Leistungsfähigkeit eines solchen Servers wird von Micro Focus (Novell) angegeben mit:

Im Mittel 181 GroupWise Events pro Minute  
Im Mittel 474 Events pro Benutzer pro 24 Stunden  
Im Mittel 165 Geräte-Anfragen pro Minute  
Im Mittel 427 Emails von Geräten innerhalb 24 Stunden  
usw...

Dies erscheint uns mehr als ausreichend, so dass Sie ggf. mit der CPU- und RAM-Anzahl auch nach unten experimentieren können.

Die Anforderung an Festplatten-Speicherplatz für eine solche Umgebung ist mit 200 GB angegeben. Daher haben wir dem zugrunde liegenden SLES12SP3-Server zwei virtuelle Festplatten spendiert, eine System-Platte mit 80 GB und eine Platte als */var*-Partition für die Datenspeicherung von GMS. Da wir für diese Platten i.d.R. den „Thin“-Modus von ESXi empfehlen, sind die Plattengrößen nach der Installation aber zunächst klein (ca. 5,5 GB und 0,5 GB), können dann aber „wachsen“.

Da GroupWise Mobility Service (GMS) in der Version 18 auch ein GroupWise 18 voraussetzt, müssen Sie auch schon Ihren GServer03 auf den Stand der paedML Novell 4.3, besser 4.4 gebracht haben, auf dem GW 18 läuft. (Oder Sie besitzen einen eigenständigen GW-18-Server.)



**Der *GMS-18-Server* setzt ein laufendes GroupWise 18 System voraus, also auch die paedML Novell 4.3, besser 4.4!**

Aus Sicherheitsgründen sollte der *GMS-Server* in der DMZ betrieben werden. Unser *GMS-Server* hat daher die IP-Adresse **192.168.1.37**. Für den Zugriff von außen, was ja oft die Regel beim Einsatz von mobilen Geräten ist, ist weiter ein vertrauenswürdigen Zertifikat nötig.

Beim Einsatz eines **einfachen Zertifikats** auf dem *GMS-Server* ist dazu erforderlich, dass eine Firewall (normalerweise die Sophos UTM/SG) oder wenigstens ein Router vorhanden ist, der zwischen der DMZ und dem GServer03 im internen Netz routen kann. In diesem Fall benötigen Sie vom Provider (z.B. Belwü) einen DNS-Eintrag, der auf eine für den *GMS-Server* festgelegte öffentliche IP-Adresse verweist, und entsprechende Einstellungen auf Ihrer Firewall. Haben Sie keine freie IP-Adresse, geht es auch über einen festgelegten Port einer bereits benutzten IP-Adresse, ebenfalls mit entsprechenden Einstellungen incl. Portweiterleitung auf Ihrer Firewall. Genaueres folgt in dieser Anleitung.

Beim Einsatz eines **Wildcard-Zertifikats** auf dem GServer03 ist dies nicht nötig. Dieses Verfahren wird im Dokument *paedML-Novell-meineschule.de-anpassen.pdf* (Gesicherter Zugriff von außen (meineschule.de anpassen)) (liegt bei; auch im Support-Portal im Bereich Novell/Erweiterungen) beschrieben.

Zu Zertifikaten, siehe auch Anhang A

## 2 Installation GMS-OVA

### 2.1 LMZ-Paket

Das vom LMZ ausgelieferte Installationspaket enthält einen lauffähigen *SLES12SP3-Server* incl. GMS, der als virtuelle Maschine auf dem ESXi Host installiert werden kann. Wegen der späteren Funktion haben wir ihm den Namen *GMSServer* gegeben.

#### Inhalt:

*gms1811.ova*

Zusätzliche Dokumente:

*OVA\_paedML-Novell.pdf*

*Online-Update\_paedML-Novell.pdf*

*paedML-Novell-meineschule.de-anpassen.pdf*

### 2.2 Einspielen der gms1811.ova

Kopieren Sie die vom LMZ erhaltene Datei *gms1811.ova* auf eine Arbeitsstation, die den *vSphere Client* installiert hat oder von der Sie den *vSphere WebClient* benutzen können.

Wie eine OVA mittels *vSphere Client* oder *vSphere-Webclient* auf dem ESXi Host eingespielt wird, steht im Dokument *OVA\_paedML-Novell.pdf*, das dem LMZ-Paket beiliegt. Daher beschränken wir uns hier auf eine (vollständige) Kurzform.



In neueren ESXi-(VCenter)-Versionen, die nicht mehr über den *vSphere Client* konfiguriert werden, sondern über ein Browser-Interface, kann es sein, dass eine OVA so wie bisher nicht mehr eingespielt werden kann.

Laden Sie sich in diesem Fall von VMware das *ovftool* (Version  $\geq 4.20$ ) herunter und installieren es auf Ihrem Admin-PC.

Wechseln Sie dann in einer Eingabeaufforderung (DOS-Box) in dasjenige Verzeichnis, in dem die *gms.ova* liegt.

Zum Hochladen der OVA auf den ESXi benötigen Sie den folgenden Befehl, den Sie natürlich für Ihre Verhältnisse anpassen müssen:

```
<Pfad>\ovftool --disableVerification --noSSLVerify --
datastore=<Datastore> --network="<Network>" gms1810.ova
vi://root@<IP des ESXi>
```

(alles eine Zeile)

Schauen Sie in Ihrem ESXi nach, wie Ihr DataStore und Ihr Network heißt. Wechseln Sie zuerst in das Verzeichnis, in dem die OVA liegt. Der Befehl könnte vielleicht so aussehen (abhängig von Ihren Bezeichnungen für *datastore* und *network*):

```
C:\Program Files\VMware\VMware OVF Tool\ovftool --
disableVerification --noSSLVerify -datastore=PAEDML-
DATASTORE --network="paedML_DMZ" gms1811.ova
vi://root@10.1.1.39
```

**Wichtig:** Bitte beachten Sie bei diesem Befehl die Groß- und Kleinschreibung .

Sie werden nach dem Abschicken dieses Kommandos nach dem Passwort ihres ESXi gefragt.

Nach dem Hochladen, dauert es einen Moment, bis in der Verwaltung des ESXi der neue Server angezeigt wird.

Starten Sie den *vSphere Client*.

Öffnen Sie den Menü-Eintrag „Datei I OVF-Vorlage bereitstellen“. Damit wird ein Dialog gestartet, in dem Quelle, Name und Speicherort konfiguriert werden können.

Quelle:

Navigieren Sie zu der vom LMZ erhaltenen Datei *gms1811.ova* und fahren Sie fort mit „Weiter“.

Klicken Sie auf „Weiter“ und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA). Drücken Sie erneut auf „Weiter“.

Name und Speicherort

Geben Sie als Namen der virtuellen Maschine *GMSServer* ein und fahren Sie fort mit „Weiter“.

Datenspeicher auswählen:

Hier geben Sie an, wo die Daten der virtuellen Maschine gespeichert werden sollen. Wählen Sie den *paedML\_DATASTORE* oder bei Bedarf (und falls vorhanden) einen anderen DataStore aus. Fahren Sie fort mit „Weiter“.

Festplattenformat:

Es gibt zwei Formate, die ESXi zur Verfügung stellt:

- „schnell bereitgestellt“, „thin provisioning“: Die Festplattengröße wächst nach Bedarf langsam an. Wenn keine Snapshots vorhanden sind, kann der Festplattenspeicher problemlos erweitert werden! Wir empfehlen dieses Festplattenformat.
- „thick provisioning“: Speicher wird sofort zugeteilt. Auch hier kann der Speicher noch erweitert werden, der Speicherplatz ist aber sofort „verbraucht“.

Wählen Sie das gewünschte Festplattenformat aus und fahren Sie fort mit „Weiter“.

Netzwerkzuordnung:

Die Konfiguration der Netzwerkkarten wird nach der Bereitstellung vorgenommen. Fahren Sie fort mit „Weiter“.

Klicken Sie auf „Bereit zum Abschließen“ und anschließend auf „Beenden“. Die virtuelle Maschine wird anschließend installiert.

Wenn die Bereitstellung abgeschlossen ist, ist der *GMSServer* als virtuelle Maschine konfigurierbar. Markieren Sie die VM mit einem Rechts-Klick und wählen Sie dann „Einstellungen bearbeiten...“. Nun können Sie die Netzwerkadapter des Gastes zuordnen:

Klicken Sie im Reiter Hardware auf „Netzwerkadapter 1“ und wählen Sie den Eintrag „*paedML\_DMZ*“.

Fügen Sie noch ein CD-/DVD-Laufwerk zum eventuellen späteren Einbinden einer ISOs hinzu.

### CPU / Arbeitsspeicher:

Unser GMSServer ist auf 1 CPU und 4 GB RAM gesetzt. Ändern Sie dies ggf. nach Ihren Gegebenheiten, wie weiter oben beschrieben.

Starten Sie den *GMS* und melden sich als *root* an. Das Passwort im Auslieferungszustand ist *54321*. Nach erfolgter Anmeldung sollten Sie das Passwort sofort(!) mit dem Befehl *passwd* an der Konsole ändern. Notieren Sie sich das vergebene Passwort: \_\_\_\_\_



SLES 12 bringt bereits installierte VMware-Tools mit. Bitte prüfen Sie im *VSphere Client* beim *GMSServer* / *Übersicht* nach, ob die VMware-Tools laufen und aktuell sind.

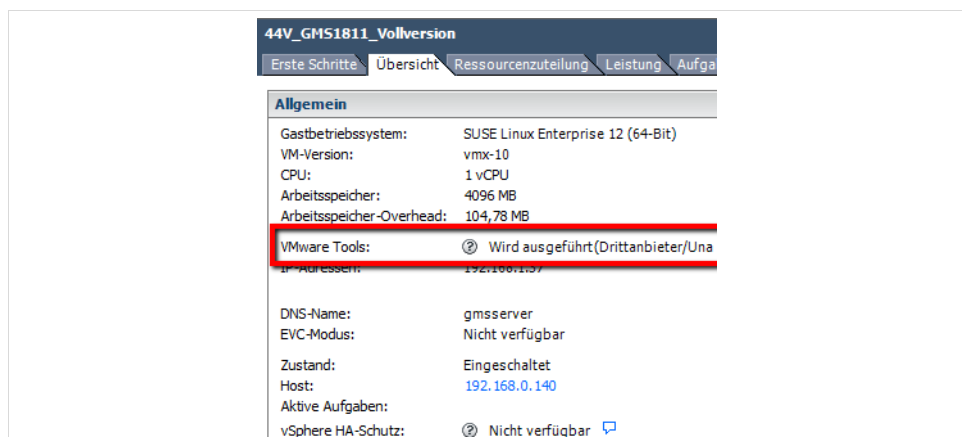


Abb. 1:

Ist dies nicht der Fall, können Sie selbst tätig werden. Die Vorgehensweise ist ebenfalls in den oben genannten Dokumenten *OVA\_paedML-Novell.pdf* beschrieben.

## 2.3 Firewallregel für den GMS-Server erstellen

Um ggf. Updates direkt auf dem *GMS* ausführen zu können, ist es sinnvoll dafür zu sorgen, dass der *GMS* Server eine Verbindung zum Internet herstellen kann. Sollten die weiter unten beschriebenen Regeln in Ihrem System schon vorhanden sein, überspringen Sie dieses Kapitel und machen mit der Installation weiter.

Wir gehen in dieser Beschreibung davon aus, dass sie als Firewall eine *Sophos UTM* einsetzen. Sie müssen dafür mittels Verwaltungskonsole auf die *Sophos UTM* zugreifen. Starten Sie in einem Browser die Adresse <https://10.1.1.30:4444> und melden Sie sich an der Verwaltungskonsole der *Sophos UTM* an. Erzeugen Sie einen Hosteintrag im Menü *Definitions & Users* unter dem Punkt *Network Definitions* mit dem Namen *DMZ GMS* mit der IP-Adresse **192.168.1.37**. Speichern Sie den Hosteintrag.

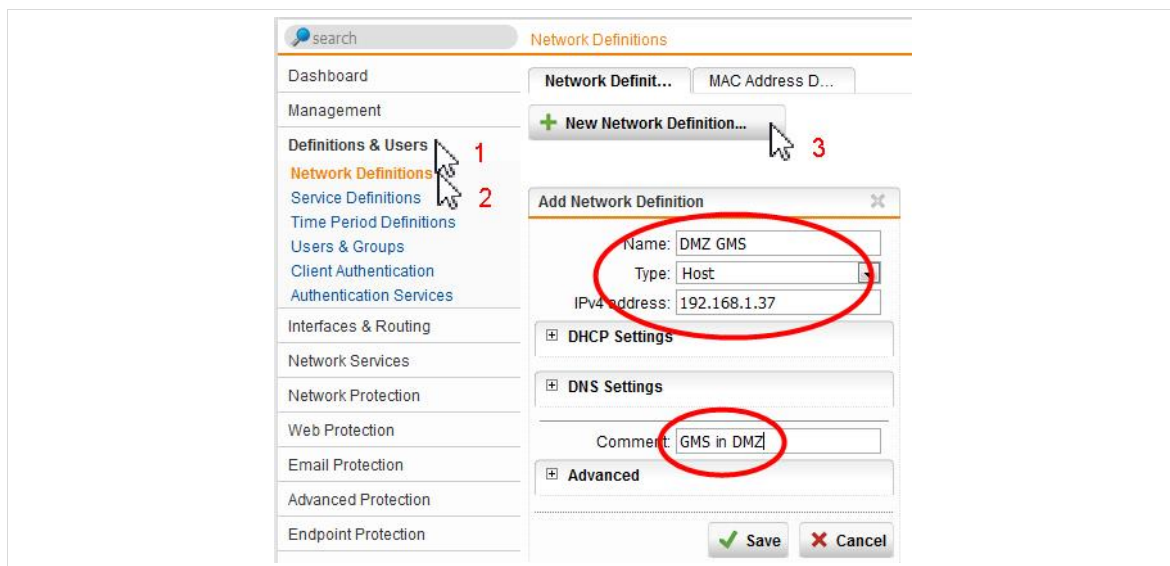


Abb. 2: Host-Eintrag

Als nächstes erzeugen Sie die Regel, die es dem *GMS* erlaubt die Internetverbindung herzustellen. Erzeugen Sie im Menü *Network Protection* unter *Firewall* eine neue Regel mit neuer Gruppe *DMZ-out GMS* mit der Quelle *DMZ GMS*, mit Service *https* und Ziel *Any over External*. Speichern Sie die Regel.



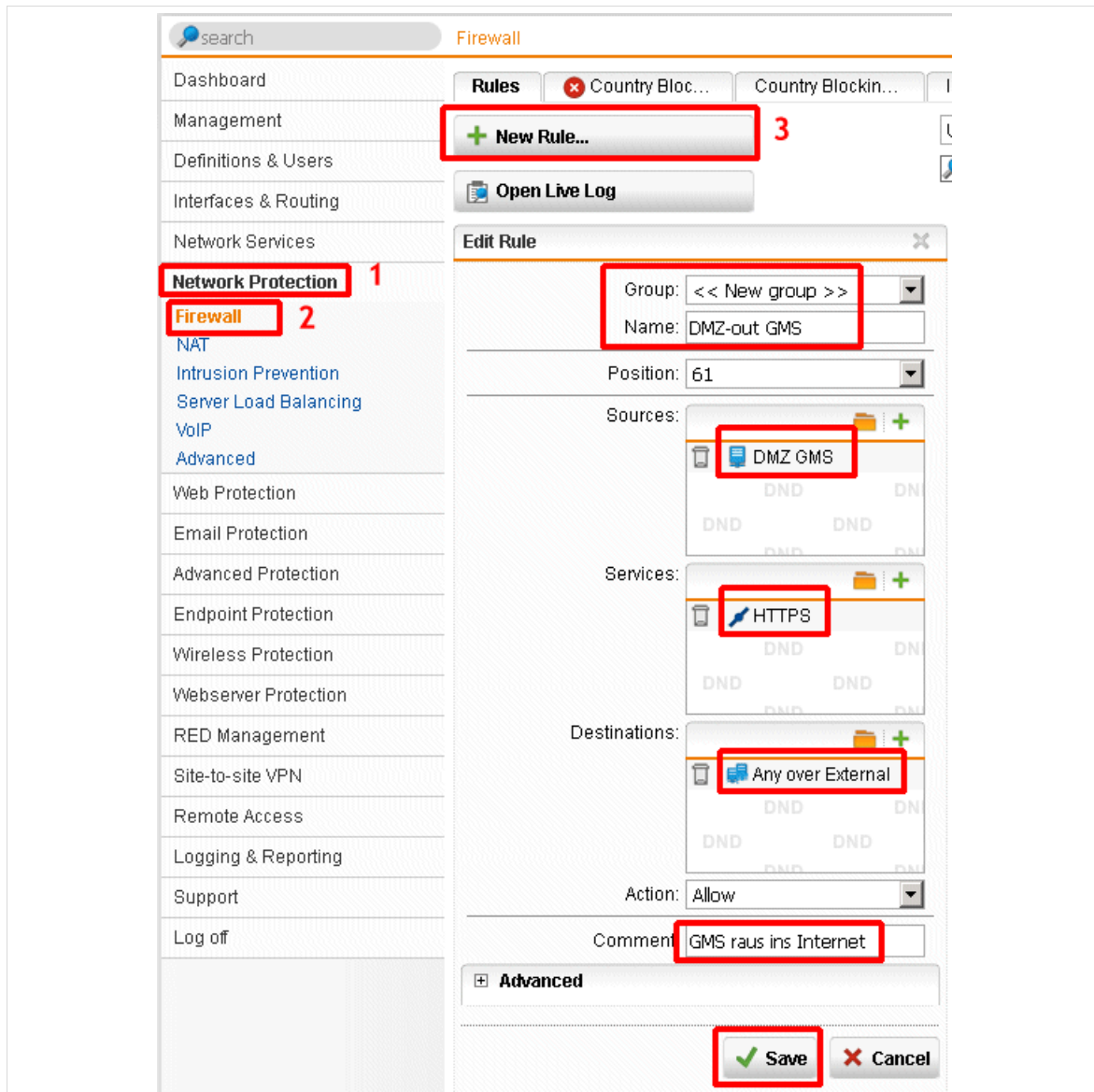


Abb. 3: Firewallregel

und

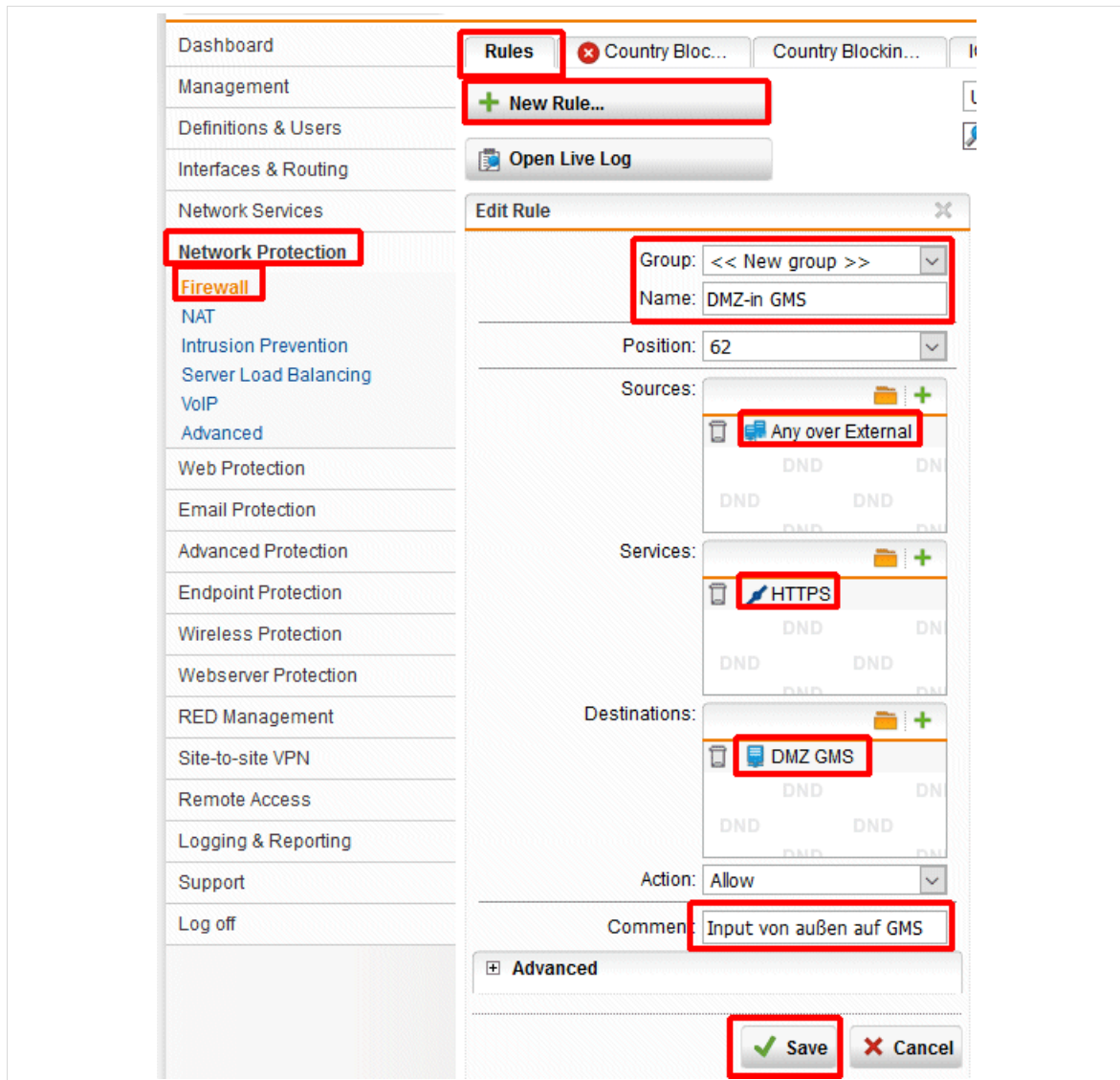


Abb. 4: Firewallregel

Die Regeln stehen ganz am Ende der Liste oder an einer von Ihnen gewählten Position. Damit die Regeln wirksam werden, müssen Sie die Regel aktivieren. Klicken Sie hierzu auf die kleine Ein/Aus-Schaltfläche der Regel.

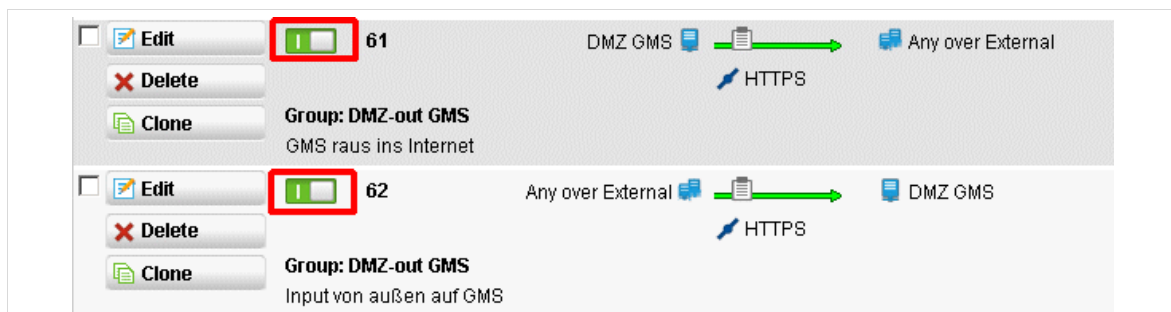


Abb. 5: Firewallregeln aktivieren

Bei Bedarf kann der Internetzugang des *GMSServers* an und abgeschaltet werden.

Wenn Sie Ihren GMS mit einer öffentlichen IP-Adresse (z.B. aus Ihrem Belwü-IP-Adress-Pool) betreiben wollen, benötigen Sie vom Provider (z.B. Belwü) einen DNS-Eintrag und die Öffnung mindestens des Ports 443 und außerdem weitere Firewall-einstellung (siehe hierzu Anhang B).

## 3 Anpassungen des GMS

### 3.1 Vorbereitungen am GServer03

Erzeugen Sie eine „verbürgte Anwendung“. Starten Sie dazu die GroupWise-Adminkonsole am besten über Browser von einer Arbeitsstation aus (<https://10.1.1.32:9710/gwadmin-console>) oder auch auf der grafischen Oberfläche des GServers und loggen sich als *gwadmin* ein.  
(Je nach Zugang haben Sie eine deutsche oder englische Oberfläche. (Im Anmeldefenster kann man allerdings auch die Sprache wählen.))

Wählen Sie dort in der Navigation *System* und dann rechts die Funktion *Verbürgte Anwendungen (Trusted Applications)*.

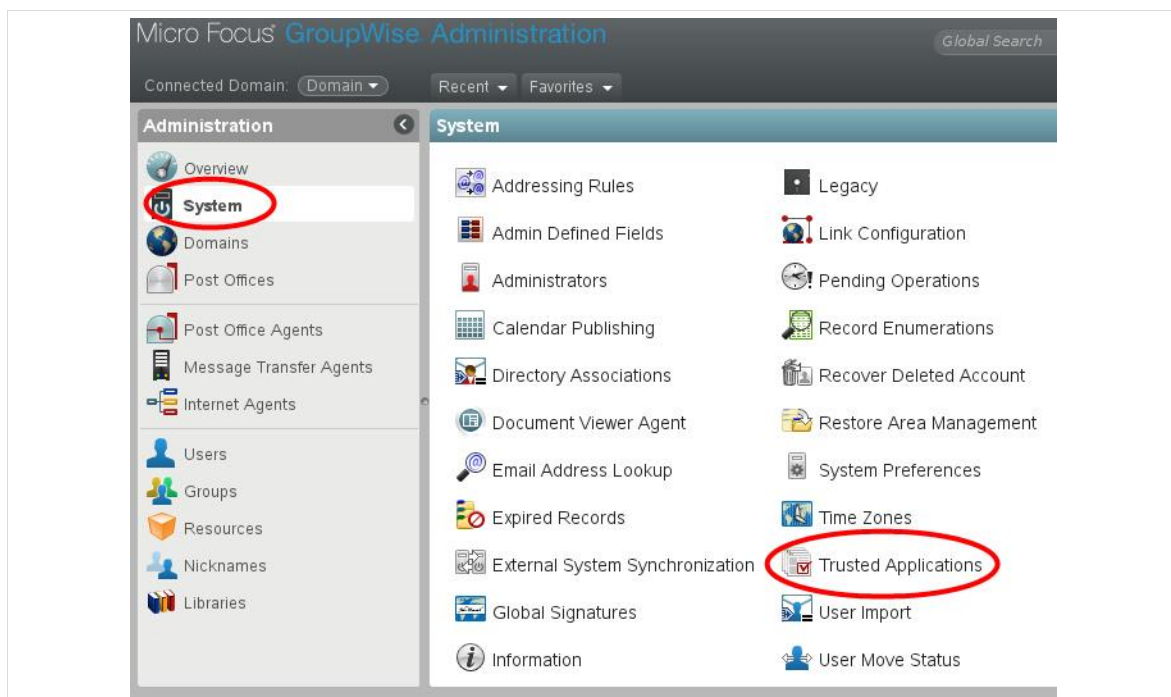


Abb. 6: verbürgte Anwendung 1

Wählen Sie *Neu (New)* und vergeben der verbürgten Anwendung den Namen *GMSServer*, weitere Einstellungen sind nicht erforderlich. Außer den hier gezeigten Eingaben darf nichts ausgefüllt werden!

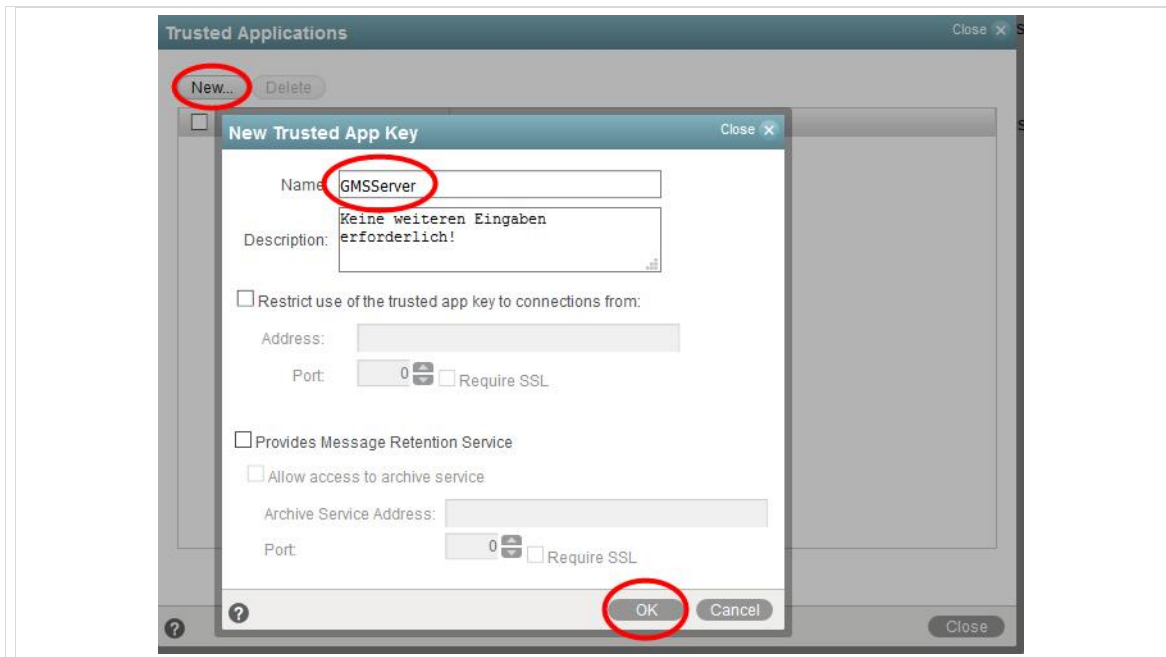


Abb. 7: verbürgte Anwendung 2

→ OK.

Nachdem der Schlüssel erzeugt wurde, öffnet sich der Dialog, um den Schlüssel zu exportieren.



Abb. 8: verbürgte Anwendung 3

Wählen Sie *Export* und speichern in die Datei unter dem Namen *GMSServer.txt*. Ein Klick auf *OK* speichert *GMSServer.txt* im konfigurierten Downloadordner des Browsers. Klicken Sie *OK* und dann *Schließen (Close)* um den Dialog zu schließen. **Je nachdem**, ob Sie diese Aktion auf einer Arbeitsstation oder auf dem GServer03 selbst ausgeführt haben, gehen Sie nun folgendermaßen vor:

**Arbeitsstation:** Kopieren Sie die eben gespeicherte Datei (z.B. mit WinSCP) auf den *GMSServer* nach */root/Downloads*.

**GServer03:** Vermutlich haben Sie die Datei auf dem GServer03 nach */root/Downloads* gesichert. Kopieren Sie nun diese Datei auf dem *GMSServer* mit folgendem Befehl (alles eine Zeile) an der Kommandoprompt, einem Terminalfenster oder einem PuTTY-Fenster:

```
scp /root/Downloads/GMSServer.txt root@192.168.1.37:/root/Downloads/GMSServer.txt
```

Geben Sie das Root-Passwort vom *GMS* ein und bestätigen Sie mit **Enter**.

Die Schlüsseldatei befindet sich nun auf dem *GMS* im Verzeichnis */root/Downloads*.

Weiter in der GroupWise-Adminkonsole gehen Sie zu *Post Office Agenten*, wählen rechts dasjenige POA, zu dem die Benutzer gehören, die den GMS nutzen sollen, klicken auf den Reiter *Agenteneinstellungen* (*Agent settings*) und entfernen Sie den Haken *Nur an TCP/IP-Adresse binden* (*Bind exclusively to TCP/IP Address*). Sollen Benutzer aus mehreren POs den GMS nutzen, entfernen Sie den Haken bei allen betroffenen POAs. (Stören Sie sich nicht an den in folgenden Bild gezeigten Portnummern. Behalten Sie Ihre Einstellungen bei!) Stoppen und starten Sie über den Reiter *General* das POA.

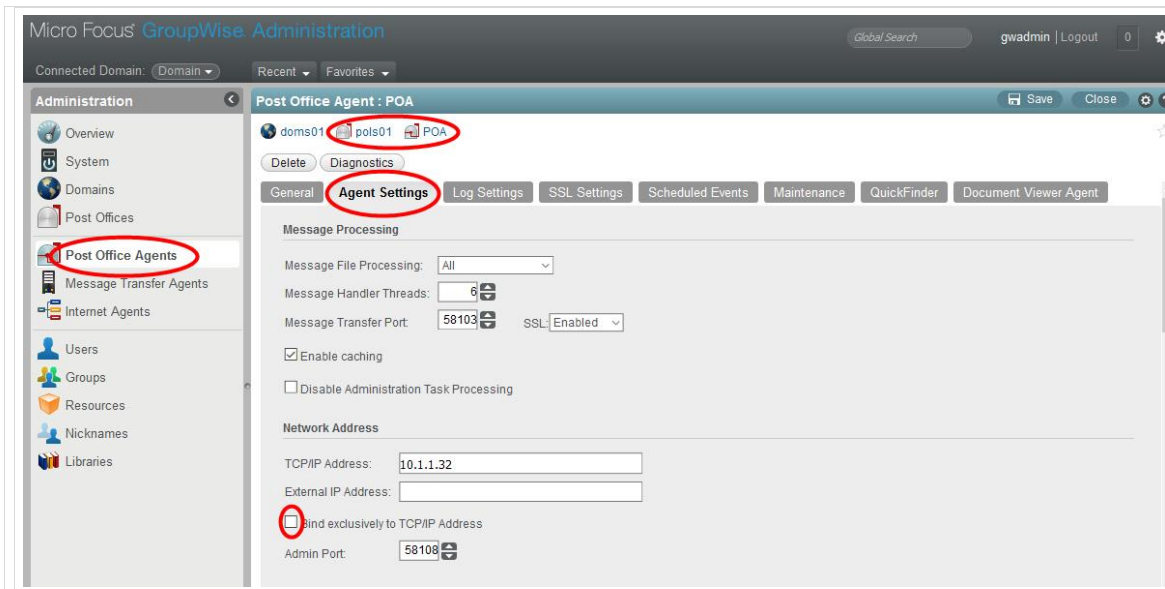


Abb. 9: Post Office Agent Settings

Erzeugen Sie den Benutzer *gwadressbuchuser* im GroupWise-System. Klicken Sie dazu in der Navigation auf *Benutzer* (*Users*) und rechts oben auf *Neu* (*New*) und legen den Benutzer im entsprechenden PO (*PostOffice*) an. Klicken sie auf *OK*.

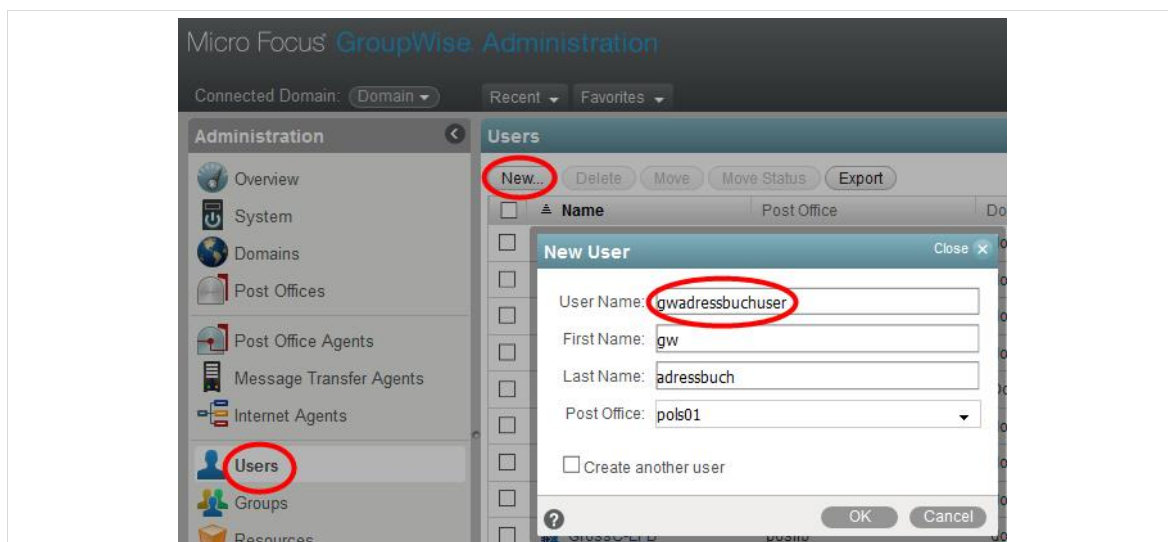


Abb. 10: Adressbuchbenutzer

→ OK.

Warten Sie bis der Benutzer erzeugt ist und vergeben dem Benutzer ein Passwort. Wählen Sie hierzu den gerade erzeugten Benutzer aus. Über die Funktion *Passwort ändern* (*Change Password*) vergeben Sie das Passwort.

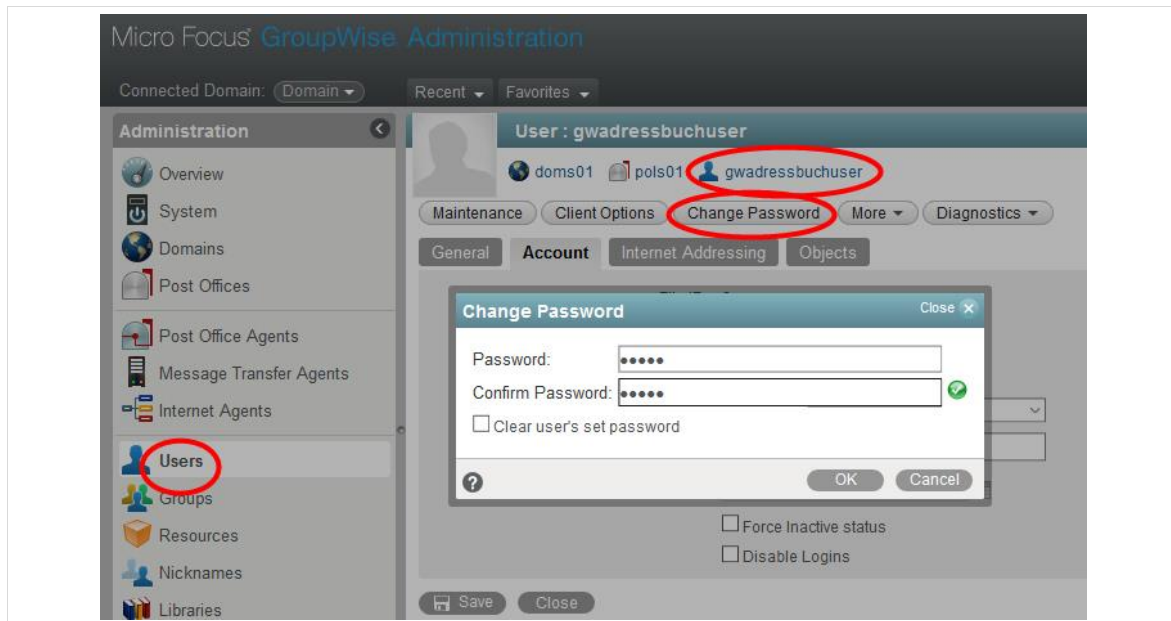


Abb. 11: Adressbuchbenutzer Passwort setzen

→ OK.

Notieren Sie das Passwort: \_\_\_\_\_

Hinweis: Dieser Benutzer wird benutzt, um das Adressbuch auszulesen. Wenn bei Ihnen nur Benutzer aus einem PO den GMS nutzen sollen, erzeugen Sie den Adressbuchbenutzer in diesem PO. Wenn Benutzer aus verschiedenen POs den GMS benutzen sollen, prüfen sie bei allen Benutzern die Sichtbarkeit (Visibility), diese muss ggf. angepasst werden. Weitere Informationen finden Sie in der [Dokumentation zu GroupWise](#). Loggen Sie sich aus der GW-Admin-Konsole aus.

Starten Sie den iManager durch Aufruf der Adresse <https://10.1.1.32/nps> und erzeugen Sie im Kontext *ml3/DIENSTE/Server* den Benutzer *ldapusergms* mit Passwort, falls noch nicht vorhanden. Falls vorhanden, ändern Sie das Passwort. Notieren Sie das Passwort: \_\_\_\_\_

Weiter gehen Sie zu den Eigenschaften des *ldapusergms* in der OU *Server.DIENSTE.ml3* auf den Reiter *Beschränkungen*, dann *Adressbeschränkung*, und geben dort die IP 192.168.1.37 ein. → Anwenden → OK. (Falls sich die IP nicht hinzufügen lässt, benutzen Sie statt iManager die ConsoleOne.)

Geben Sie diesem User nun die erforderlichen Rechte bzw. überprüfen Sie diese, falls der *ldapusergms* schon vorhanden war.:

Wählen Sie im iManager die Baumansicht und markieren *SCHULBAUM03* und *aktuelle Ebene*. Über *Aktion* gehen Sie zu *Trustees bearbeiten*.



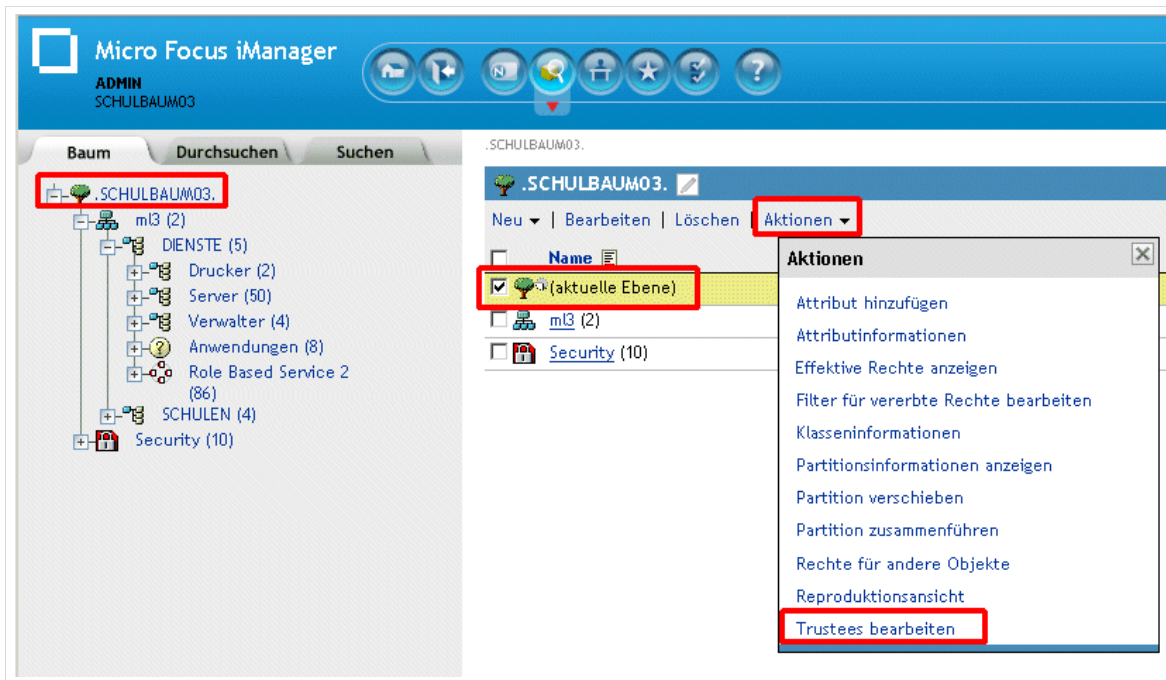


Abb. 12:

Fügen Sie nun den Trustee *ldapusergms* hinzu,

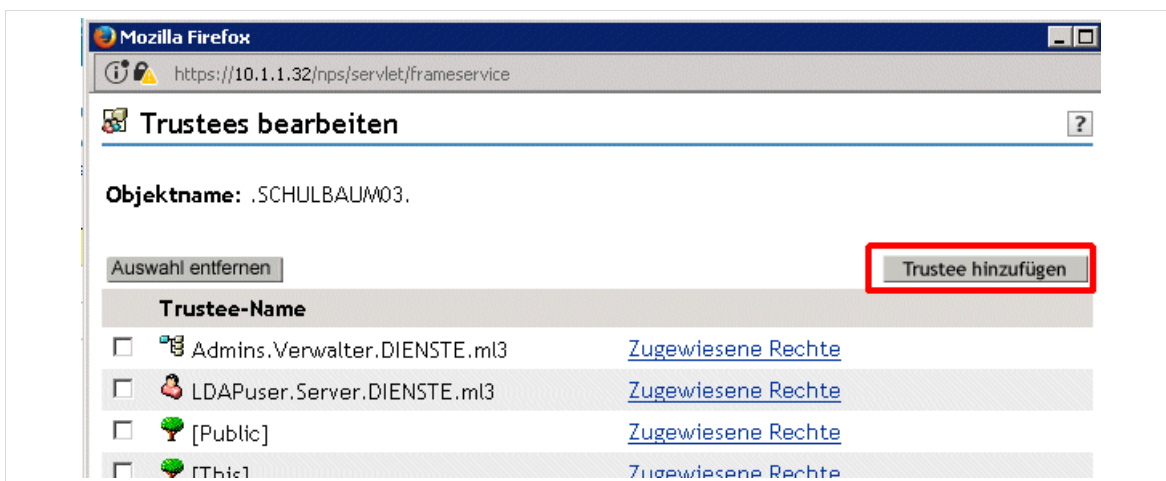


Abb. 13:

Scrollen nach unten und klicken bei *ldapusergms* auf *Zugewiesene Rechte*:

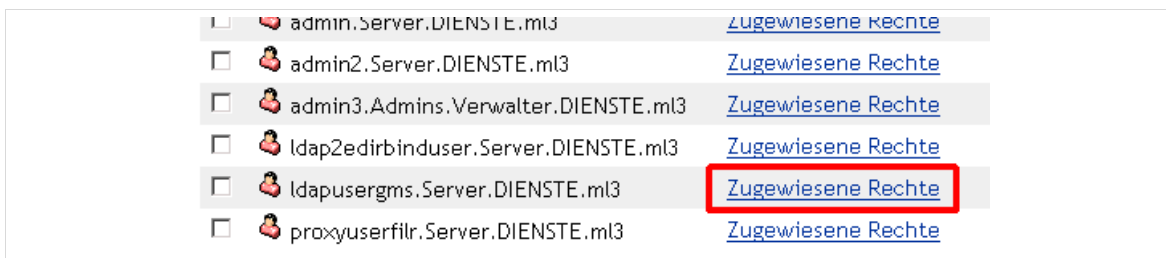


Abb. 14:

Löschen Sie dort den Eintrag *All Attribute Rights*,

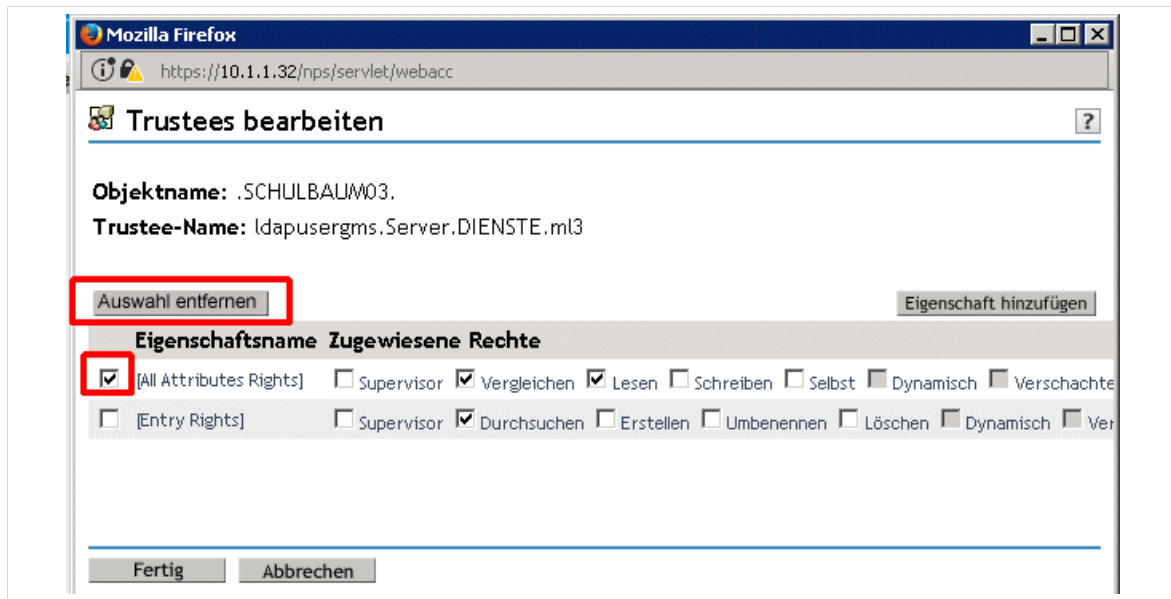


Abb. 15:

Setzen in *Entry Rights* die Häkchen bei *Durchsuchen* und *Vererben*

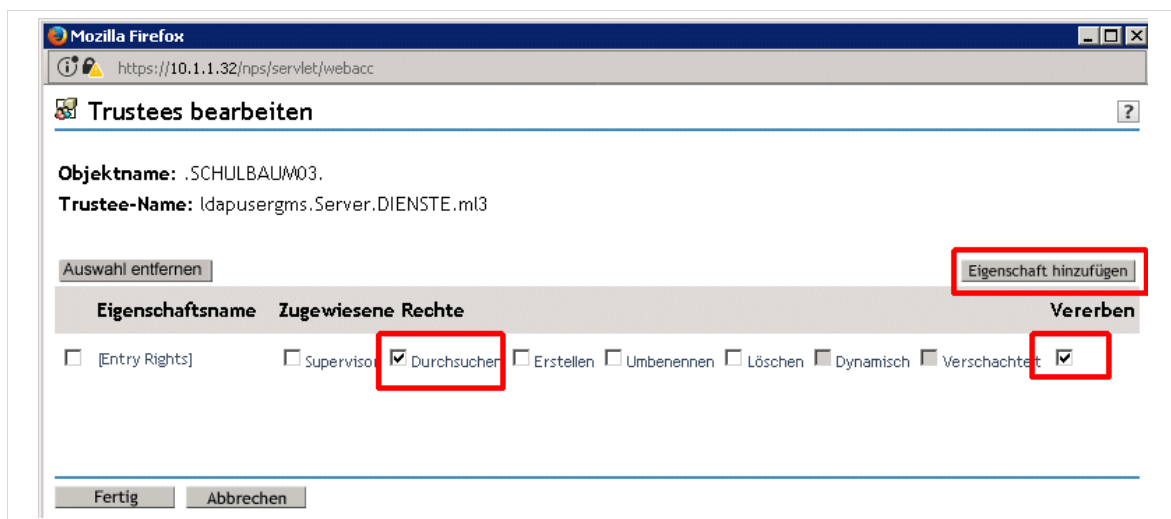


Abb. 16:

Und klicken auf *Eigenschaften hinzufügen*:



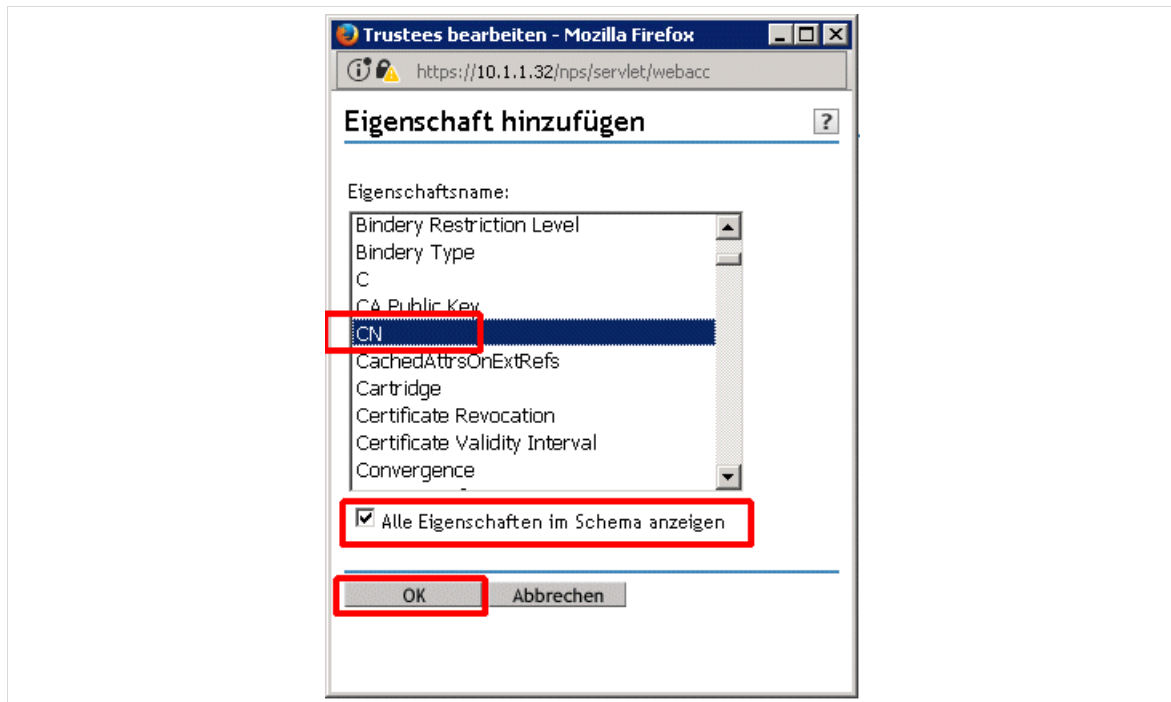


Abb. 17:

Setzen Sie das Häkchen bei *Alle Eigenschaften im Schema anzeigen* und fügen Sie die Eigenschaft *CN* ein → OK.

Wiederholen Sie dies für die Eigenschaften: *Given Name*, *Surname*, *dn*, *Member*, *Password Expiration Time*.

Danach setzen (bzw. löschen) Sie die Häkchen, wie folgt:

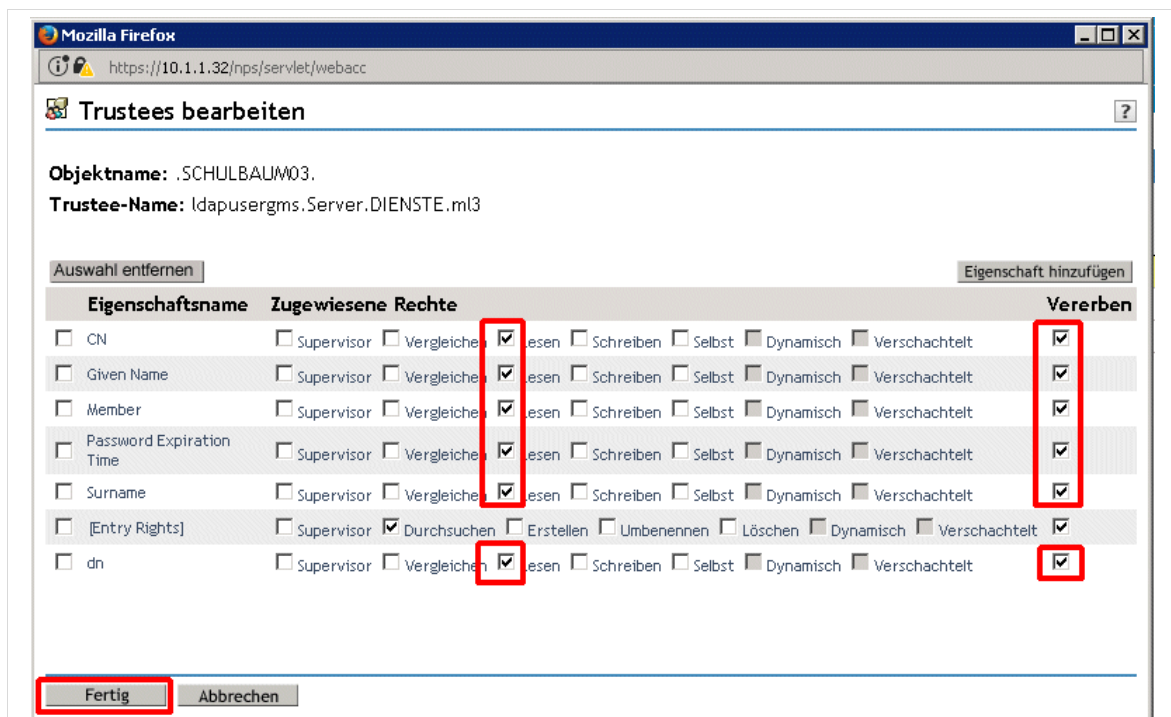


Abb. 18:

→ Fertig → Anwenden (ganz unten) → OK → OK.

Erzeugen Sie eine eDirectory-Gruppe *GMSGruppe* in dem Kontext, in dem die zugriffsberechtigten Benutzer liegen, z. B. im Kontext *Lehrer*. Nehmen Sie die Benutzer, die den *GMS* nutzen sollen, in diese Gruppe auf. Überlegenswert ist auch, die eDirectory-Gruppe *GMSGruppe* als dynamische Gruppe anzulegen.

### 3.2 Konfiguration des GMS

Weiter unten benötigen Sie die SOAP-Portnummer des Post-Office-Agents (POA) desjenigen Post-Office, das für die Verbindung von GMS zu GroupWise zuständig sein soll. Schauen Sie in der GroupWise-Adminkonsole unter *Post Office Agenten / POA / Agent Settings* diesen *SOAP-Port* nach.

(Für die Schule S01 ist dies **58106** (pols01), ansonsten **57093** (Ihr Lehrer-PO)). Eine Übersicht über die GW-Ports finden Sie im Anhang jeder GServer-Installationsanleitungen irgendeiner 4.x-Version.)

Das Datenbank-Passwort des GMS-Dienstes steht in der Auslieferung auf 12345. Dies sollten Sie in ein echtes und gutes Passwort ändern. Loggen Sie sich dazu an der Konsole oder per PuTTY auf dem GMS-Server als root ein und führen Sie folgende Schritte aus:

```
gmsserver:~ # dsapp -db
```



v249 FORCED

```
Change psql datasync_user password? [y/n] y
Enter new password: <Ihr Passwort>
Re-enter new password: <Noch einmal Ihr Passwort>
```

```
Changing database password..
```

```
Database password updated. Please restart mobility
```

```
Press Enter to continue
```

Starten Sie dem GMS-Dienst neu:

```
systemctl restart gms.service
```

Die restlichen Einstellungen werden am GMS unter <https://192.168.1.37:8120> durchgeführt.

Diese URL erreichen Sie problemlos mit dem Firefox auf der graphischen Oberfläche des *GMS*. Um die GMS-Konsole auch von einer Arbeitsstation aus zu erreichen, müssen in der SuSEfirewall2 auf dem *GMS* die Ports 4500 und 8120 geöffnet sein. Außerdem muss der Port 443 erreichbar sein. Dies ist in der vorliegenden virtuellen Maschine bereits eingestellt.

Um von einem Arbeitsstation aus auf den *GMS* zugreifen zu können, ändern Sie bitte am **GServer03** die *wpad.dat* im Verzeichnis */srv/www/htdocs* und fügen dort bitte unterhalb des Eintrags für den KServer einen Eintrag für den GMS-Server (IP 192.168.1.37) hinzu. Starten Sie danach den Webserver Apache2 neu:

```
function FindProxyForURL(url, host)
{
  if (isPlainHostName(host) || dnsDomainIs(host, ".oes.ml-bw.de"))
  return "DIRECT";
  else if
  (host=="127.0.0.1")
  return "DIRECT";
  else if
  (isInNet (host, "10.1.0.0", "255.255.0.0"))
  return "DIRECT";
  else if
  (host=="192.168.1.36") return "DIRECT";
  else if
  (host=="192.168.1.37") return "DIRECT";
  else
  return "PROXY 10.1.1.31:3128; DIRECT";
}
```

Abb. 19:

```
systemctl restart apache2.service
```

Starten Sie nun <https://192.168.1.37:8120> und melden sich als *root*-Benutzer des *GMS* an.

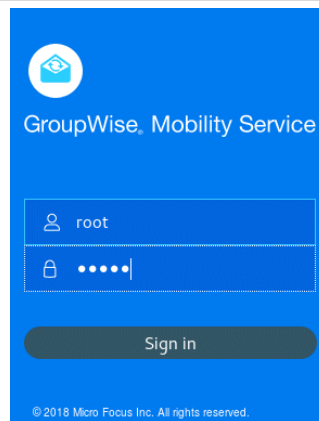


Abb. 20:

Wechseln Sie in den *Config*-Bereich. Unter *General* legen Sie die maximal zu übertragende Größe von Email-Anhängen fest

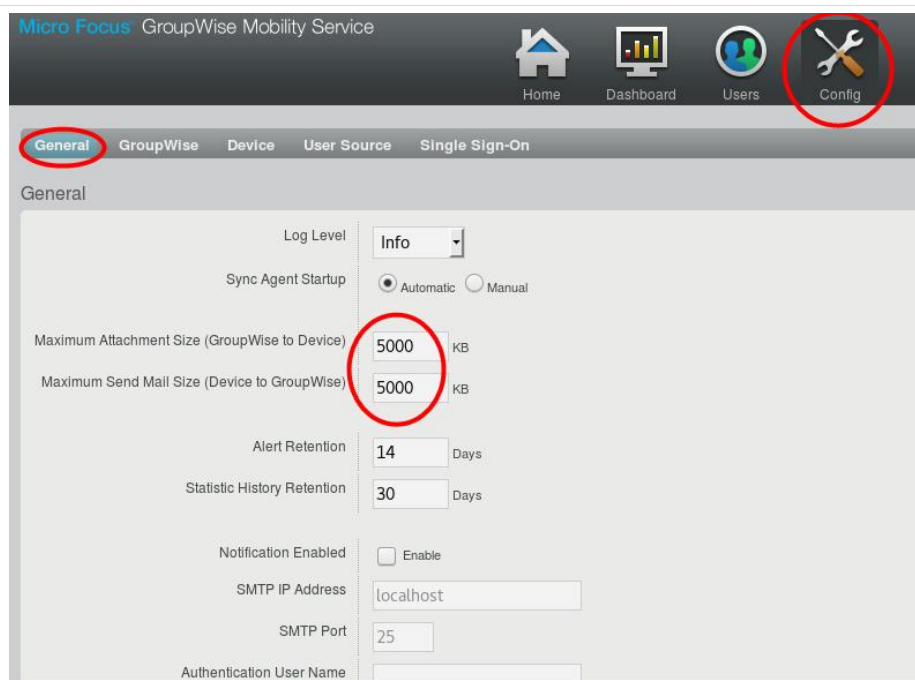


Abb. 21: GMS Config General

→ Save

Unter *GroupWise* sind die Synchronisationsdaten zusammengefasst, hier steht der SOAP-Port und an dieser Stelle kann global die Synchronisation eingeschränkt werden. Wenn Sie z. B. nur Emails und Termine zum Synchronisieren bereitstellen wollen, dann aktivieren Sie hier im unteren Bereich nur *Appointments* und *Mail*.

Bitte fügen Sie den „Schlüssel der verbürgten Anwendung“ bzw. den „Trusted Application Key“ ein (vgl. folgenden Screenshot).

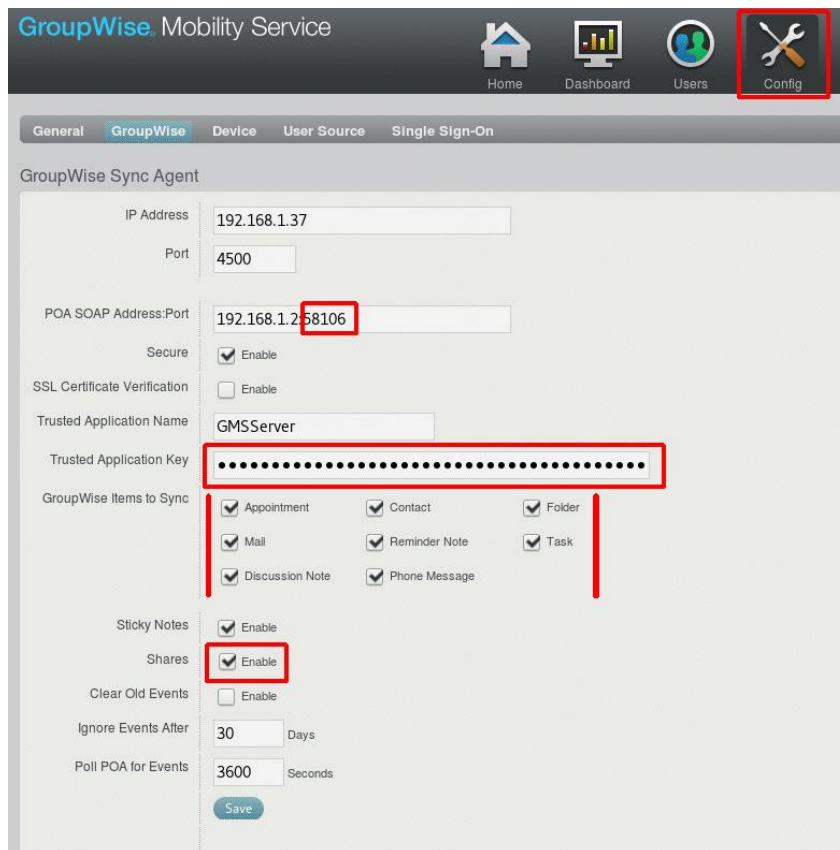


Abb. 22: GMS Config GroupWise

→ Save

Falls Sie auch freigegebene Kalender (z.B. für Schultermine) synchronisieren wollen, müssen Sie auch ein Häkchen bei *Shared (Geteilte Inhalte)* setzen.

Im Abschnitt *GroupWise Items to Sync* setzen Sie die Häkchen nach Ihren Wünschen.

Bei *User Source* konfigurieren Sie den LDAP-Zugriff auf den GServer03. Stellen Sie bei *User Source Provisioning* und *Authentication* auf *LDAP*. Bei der LDAP-Konfiguration nehmen Sie folgende Einstellungen vor:  
*IP Adresse:* 192.168.1.2; *Port* 389; *Admin Full DN:* cn=ldapusergms,ou=Server,ou=DIENSTE,o=ml3 und  
 Passwort unter *Admin Password*;  
*Base User/Group DNs:* ou=lehrer,ou=benutzer,ou=<Schule>,ou=schulen,o=ml3 (bzw. bei der Gruppe Ihren benutzen Gruppencontainer).

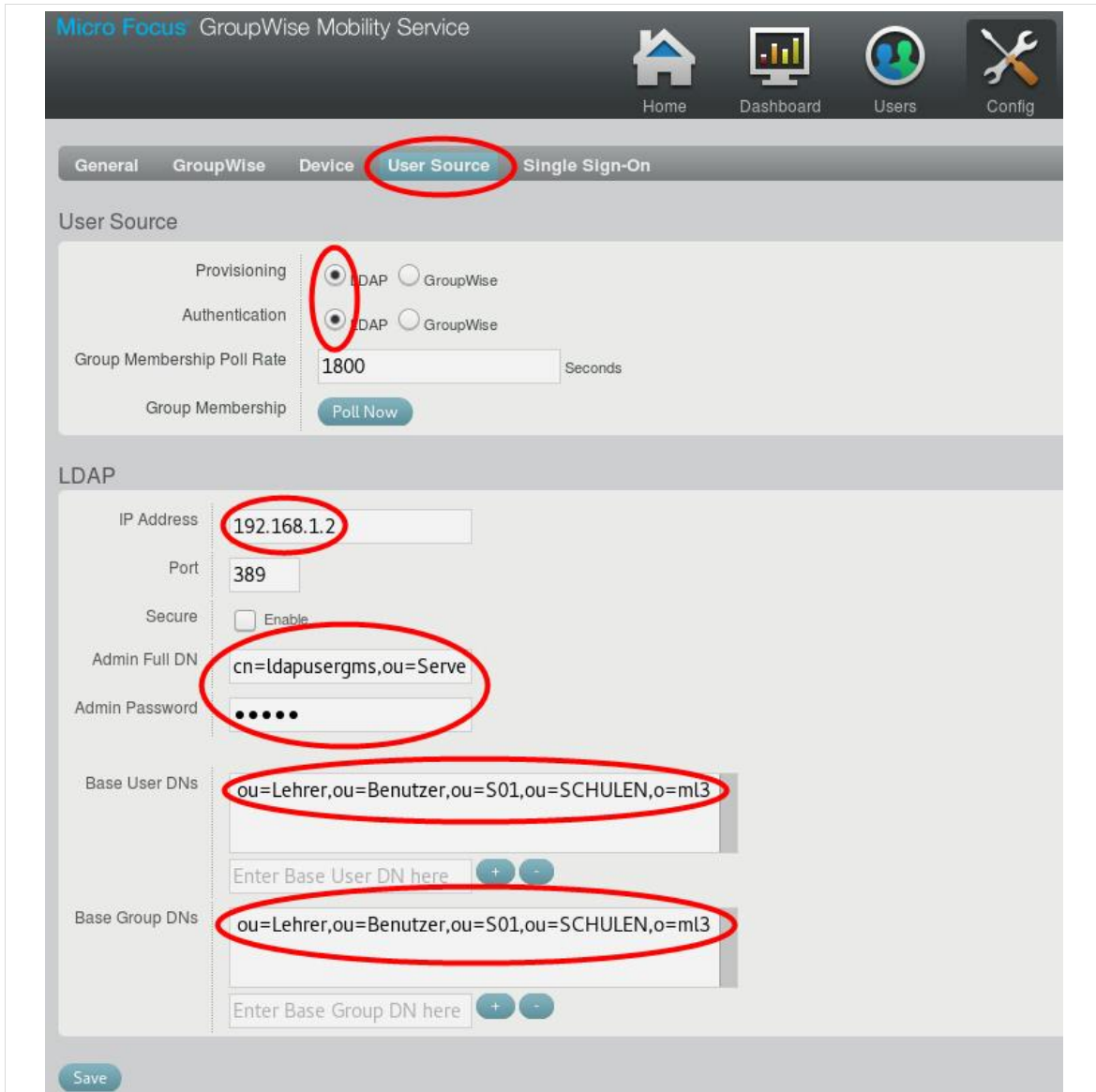


Abb. 23: GMS Config User Source

→ Save

**Diese Einstellungen werden erst nach einem Neustart des gms-service oder des GMSServer aktiv.** Speichern Sie ab und führen Sie

```
systemctl restart gms.service
```

oder einen Neustart durch. Loggen Sie sich anschließend wieder in die GMS-Konsole ein.

Nehmen Sie die GMSGruppe als Gruppe auf.

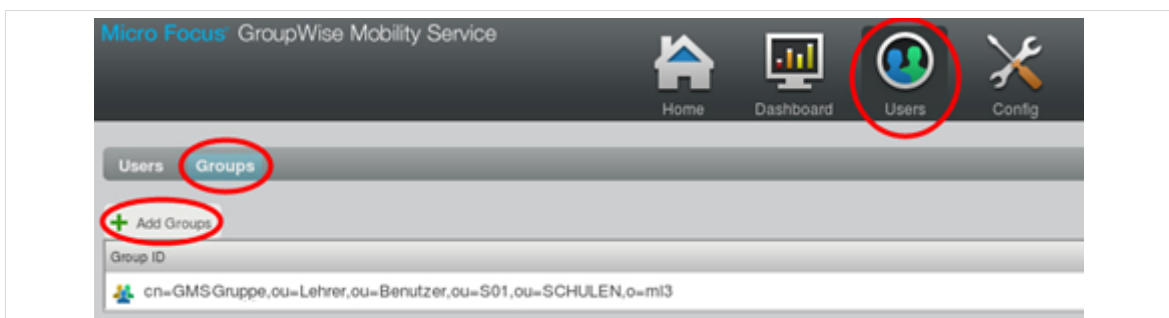


Abb. 24: GMS Users Groups

Wählen Sie dazu *LDAP* und geben in das Eingabefeld den Anfang des Gruppennamens ein (z.B. den Anfang von: gmsg...) und klicken auf den Button *Search*. Es erscheint dann eine Liste von Gruppen, die mit der Eingabe übereinstimmen, aus der Sie die gewünschte Gruppe auswählen können. (Man kann auch mehrere Gruppen einfügen.)

Nach Synchronisation bzw. Klick auf *Poll Now* unter *Config - UserSource - UserSource* erscheinen die Benutzer der Gruppe im *GMS Server*.

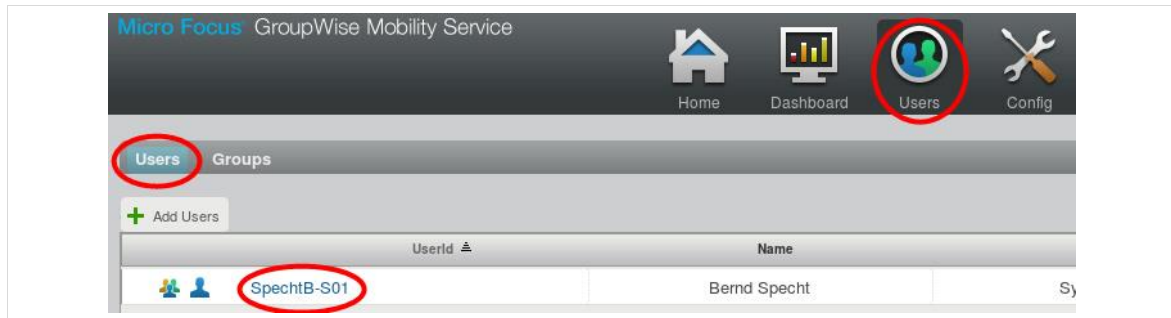


Abb. 25: GMS Users

Für einzelne Benutzer lassen sich auch Einstellungen vornehmen (Mobility Settings). Dies geht über den Aufruf <https://192.168.1.37:8120> und Anmeldung als Benutzer (z.B. SpechtB-S01).

## 4 SLES Patch

### 4.1 Automatische Online Updates

Bereits in YaST vorbereitet, aber nicht eingeschaltet, ist ein automatisches Online-Update mit Sicherheitspatches ohne Serverneustart für einen registrierten Server voreingerichtet.

Siehe unter YaST / *Software* / *Online Update Configuration*:

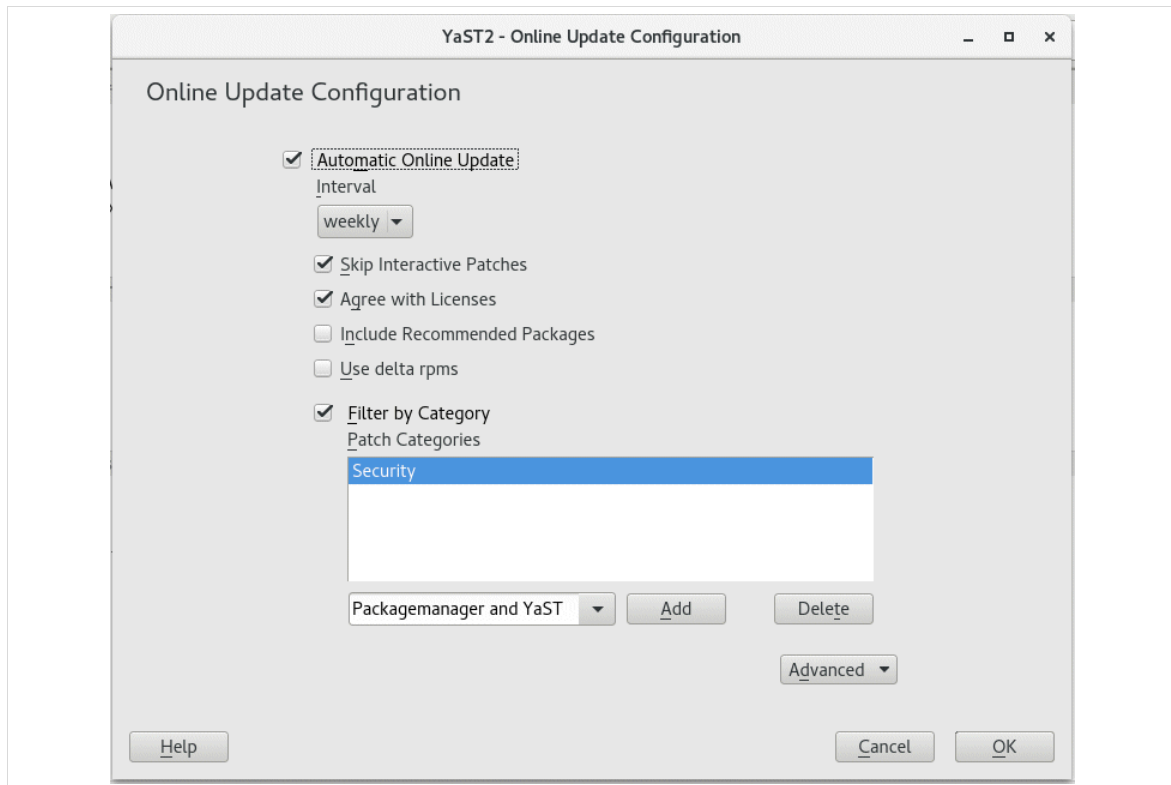


Abb. 26:

Über das Häkchen *Automatic Online Update* kann diese Funktion ein oder ausgeschaltet werden. Einzelheiten siehe Dokument *Online-Update\_paedML-Novell.pdf*.

## 4.2 Hintergrundbilder

Wenn Sie für den zugrunde liegenden SLES 12 SP3 online Patches einspielen, kann es sein, dass danach im graphischen Modus das Hintergrundbild verändert wird, das bei uns den zentrierte Streifen



Abb. 27:

enthält.

Für diesen Fall liegen im Verzeichnis `/root/wallpaper` unsere Hintergrundbilder und ein Skript, das unsere Originale wiederherstellt, mit

```
sh /root/wallpaper/restore-wallpaper.sh
```

Außerdem kann es sein, dass die Desktop-Icons plötzlich weiß und deaktiviert sind. Führen Sie dann jeweils einen Doppelklick auf jedes Icon aus und bestätigen Sie das „Trusted“-Fenster.

## 5 Schluss

Wir von der ZEN-Novell sind der Ansicht, dass *GMS* ein ausgesprochen nützliches Werkzeug ist, mit dem weitere Cloud-Features auf sicherem Wege in die *paedML Novell* gebracht werden können. *GMS*

ermöglicht uns ein sehr komfortables Arbeiten mit GroupWise, von überall aus und mit den verschiedensten Geräten. Wir hoffen, dass Ihnen der *GMS* gefällt und wünschen Ihnen viel Erfolg damit.

Ihre ZEN-Novell.



## Anhang A (Zertifikat)

In diesem Kapitel geht es um die Erzeugung und Bereitstellung eines Einzelzertifikats für den GMSServer.

Für ein Wildcard-Zertifikat auf dem GServer03 und dessen Nutzung siehe beiliegendes Dokument *paedML-Novell-meineschule.de-anpassen.pdf* (Gesicherter Zugriff von außen (meineschule.de anpassen)). Dies ist die von den Entwicklern empfohlene und einfache Möglichkeit. Wählen Sie diese Möglichkeit, ist das Weitere in diesem Anhang für Sie nicht mehr relevant.

Wenn Sie jedoch Ihren *GMSServer* mit einer öffentlichen IP-Adresse (z.B. aus Ihrem Belwü-IP-Adress-Pool) betreiben wollen, benötigen Sie vom Provider (z.B. Belwü) einen DNS-Eintrag und die Öffnung mindestens des Ports 443.

In diesem Fall benötigen Sie weitere Firewall Einstellungen. Diese beschreiben wir im Anhang B.

### Erzeugung des Zertifikats

Die folgende Vorgehensweise ist beschrieben in *gwmob18\_guide\_admin.pdf* und vor allem in der [TID 7006904](#).

Wir arbeiten an der Konsole des GMSServer oder in einem Terminalfenster (z.B. PuTTY). Wechseln Sie in das Verzeichnis */root* und legen Sie dort ein Unterverzeichnis namens *certs* und darin ein weiteres Unterverzeichnis *trusted* an:

```
cd /root
mkdir certs
cd certs
mkdir trusted
cd trusted
```

Zunächst wird ein Key- und ein CSR-File erzeugt:

```
openssl genrsa -des3 -out gmsserver.key 2048
```

Geben Sie ein Passwort für den Key-File ein und merken es sich gut.

```
openssl req -new -key gmsserver.key -out gmsserver.csr
```

Geben Sie das eben benutzte Passwort ein und weiter:

```
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Baden-Wuerttemberg
Locality Name (eg, city) []:<Meine Stadt>
Organization Name (eg, company) [Internet Widgits Pty Ltd]:<Meine Schule>
Organizational Unit Name (eg, section) []:z.B. EDV
Common Name (e.g. server FQDN or YOUR name) []:<Ihr GMS-Domain-Name>
Email Address []:<eine geeignete Email-Adresse>
A challenge password []:<leer lassen>
An optional company name []:<leer lassen>
```

Mit einem Texteditor müssen Sie nun den Inhalt dieser csr-Datei per Copy&Paste in das Online-Antrags-Formular des Zertifikatsanbieters übertragen. Als Typ wählen Sie *pem*-Format (fragen Sie ggf. beim Anbieter nach).

Füllen Sie alle vom Anbieter geforderten Angaben aus und senden dann den Antrag an den Anbieter. Von ihm bekommen Sie dann, an Ihre Email-Adresse, die Zertifikatsdateien.

**Bemerkung:** Falls Sie beim Antrag eine Bestätigungs-Email-Adresse aus einer vorgegebenen Liste auswählen müssen, die aber unpassend ist, kann es sein, dass der Anbieter Ihnen eine Text-Datei mit einem Hash schickt und Sie bitten diese Datei temporär in das „document root“ Ihres Servers zu kopieren, also nach `/srv/www/htdocs`. Der Anbieter möchte dann per `http(s)://server.meineschule.de/<Textdatei.txt>` darauf zugreifen können. **Dies funktioniert aber auf einem GMS-Server nicht!** Alternativ können Sie eventuell auch eine Email-Adresse aus der beantragten Domain angeben, z.B. `admin@meineschule.de`. Fragen Sie bei Problemen beim Anbieter nach.

## Bereitstellung des Zertifikats

Nach Erhalt der Zertifikatsdatei des Anbieters (z.B. `certificate.zip`) kopieren Sie dies auf den *GMSServer* nach `/root/certs/trusted` und packen sie aus: `unzip certificate.zip`. Die folgende Beschreibung ist als Beispiel zu verstehen, da dies je nach Zertifikat-Anbieter etwas unterschiedlich aussehen kann.

Es entsteht i.d.R. eine Verzeichnisstruktur. In einem dieser Verzeichnisse ist etwa enthalten: `certificate.crt`, `intermediate1.crt`, `intermediate2.crt`. Kopieren Sie diese Dateien am besten in das Verzeichnis `/root/certs/trusted`. Wechseln Sie in dieses Verzeichnis.

Beseitigung des Passworts aus `gmsserver.key`:

```
openssl rsa -in gmsserver.key -out gmsserver.ohnepw.key
```

Führen Sie zusammen (in dieser Reihenfolge!):

```
cat gmsserver.ohnepw.key certificate.crt intermediate1.crt intermediate2.crt > mobility.pem
```

Öffnen Sie die Datei `mobility.pem` mit einem Texteditor (z.B. `mcedit` oder `gedit`) und fügen Sie ggf. an **allen** Stellen der Form `-----END RSA PRIVATE KEY-----BEGIN CERTIFICATE-----` in der Mitte ein Return ein, so dass dies anschließend so aussieht:

```
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
...
```

Speichern Sie ab.

Führen Sie noch aus:

```
openssl x509 -in mobility.pem -inform PEM -out mobility.cer -outform DER
```

Sichern Sie die Original-Zertifikate,

```
cd /var/lib/datasync/device
cp -a mobility.pem mobility.pem.orig
cp -a mobility.cer mobility.cer.orig
```

kopieren die neuen Zertifikate:

```
cp -a /root/certs/trusted/mobility.pem /var/lib/datasync/device
cp -a /root/certs/trusted/mobility.cer /var/lib/datasync/device
```

und starten den GMS-Service neu:

```
systemctl restart gms.service
```

Wenn Sie auch den Aufruf der GMS-Konsole absichern wollen, so führen Sie noch aus:

```
cp -a /var/lib/datasync/webadmin/server.pem /var/lib/datasync/webadmin/server.pem.orig
cp -a /var/lib/datasync/device/mobility.pem /var/lib/datasync/webadmin/server.pem
```

und wieder

```
systemctl restart gms.service
```

Die oben erzeugte Datei *mobility.der* wird u.U. auch benötigt, um sie manchen mobilen Geräten manuell zuzuweisen. Diese Datei sollte deswegen auch außerhalb des *GMSServer* bereitgehalten werden.

## Anhang B (Nat-Regeln)

Wenn Sie Ihren *GMSServer* mit einer öffentlichen IP-Adresse (z.B. aus Ihrem Belwü-IP-Adress-Pool) betreiben wollen, benötigen Sie vom Provider (z.B. Belwü) einen DNS-Eintrag und die Öffnung mindestens des Ports 443.

In diesem Fall benötigen Sie weitere Firewall-Einstellungen:

Zunächst muss dazu eine Interface-Einstellung mit der öffentlichen IP-Adresse erzeugt werden. Die tatsächliche IP und die Netzmaske entnehmen Sie bitte Ihren Belwü-Unterlagen.

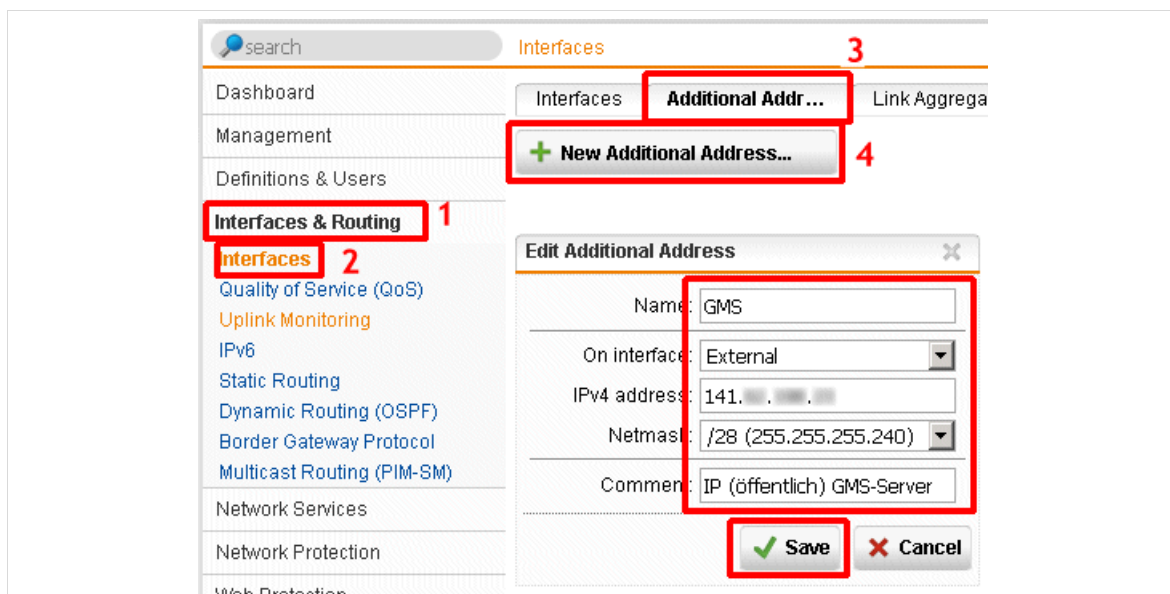


Abb. 28:

Dieser Eintrag muss danach eingeschaltet werden:

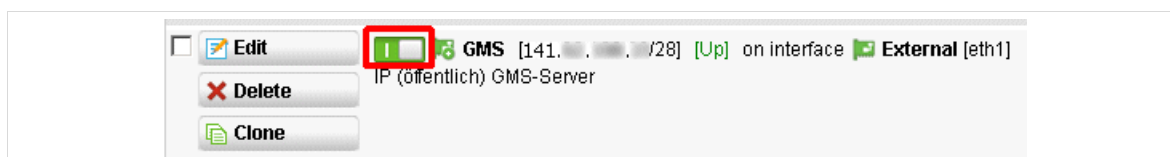


Abb. 29:

Zwei NAT-Regeln müssen erzeugt werden. Eine SNAT:

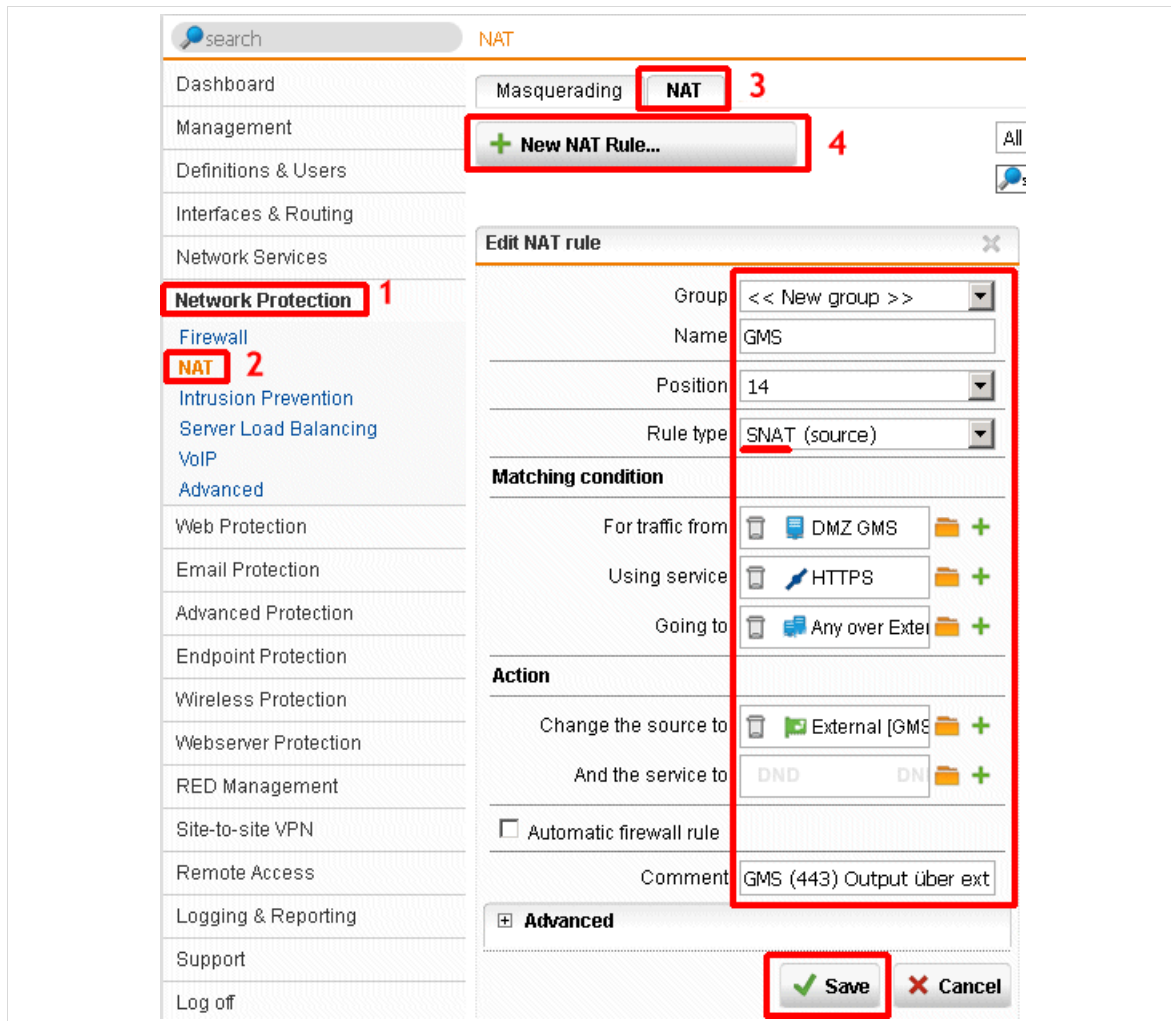


Abb. 30:

und eine DNAT:

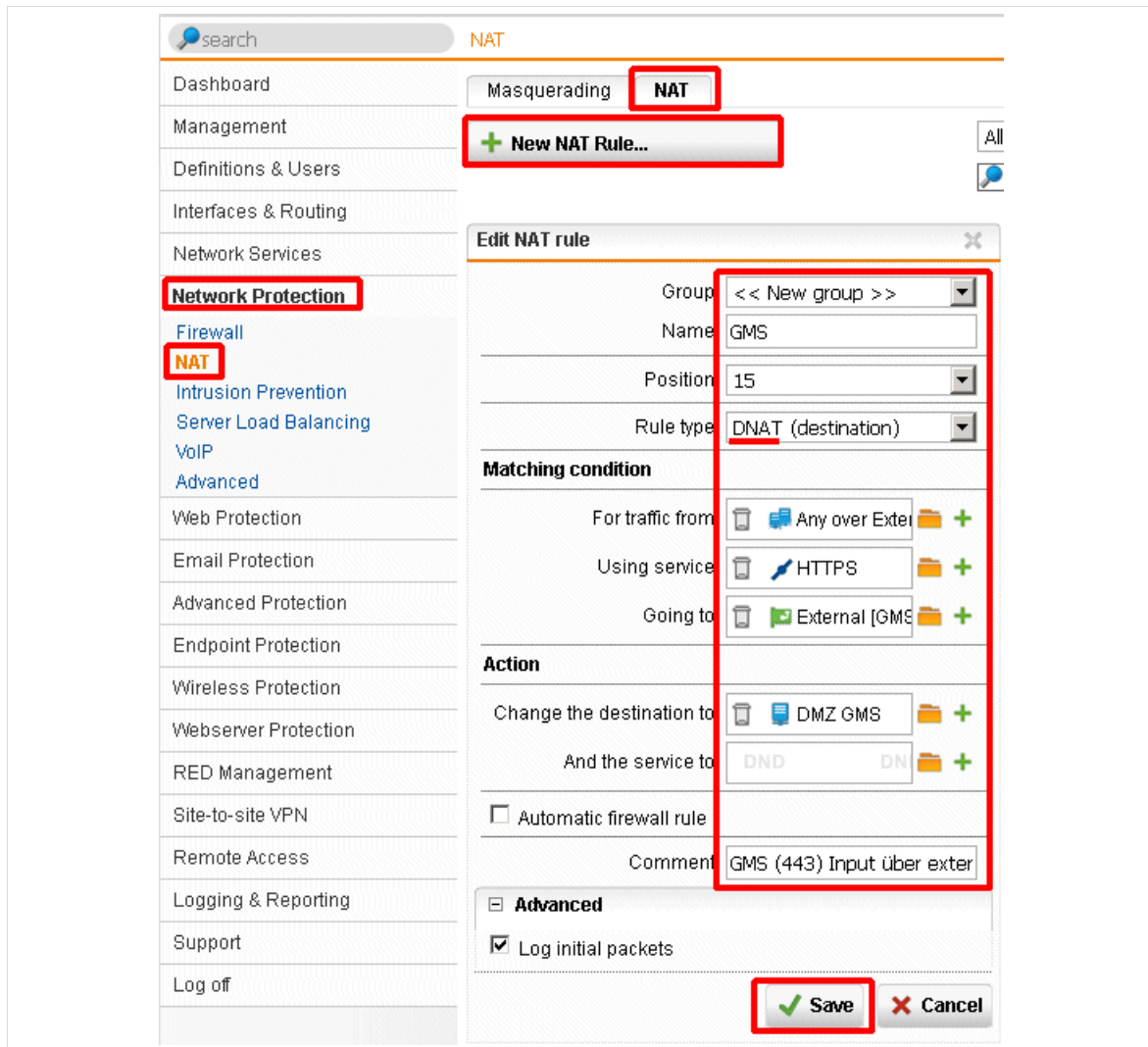


Abb. 31:

Einschalten:

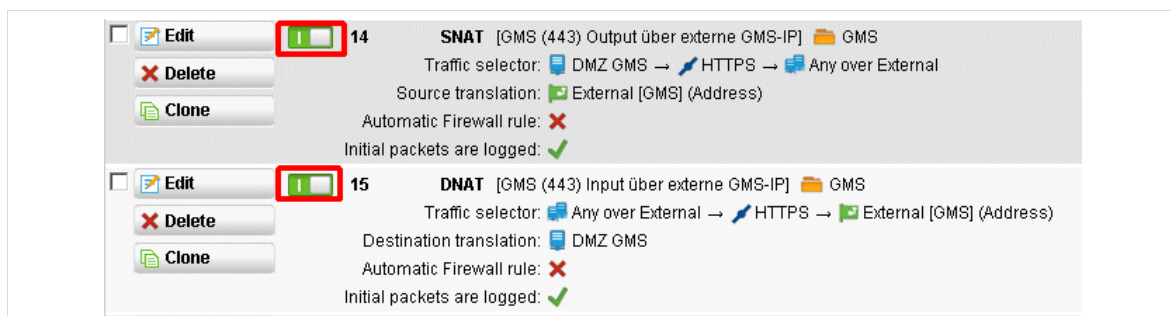


Abb. 32:

## Anhang C (Tipps)

### Tipp 1

Es gibt ein Cool-Solution-Tool namens *dsapp*, das für viele Service-Arbeiten am GMS nützlich sein kann. Siehe hierzu

[https://www.novell.com/communities/coolsolutions/cool\\_tools/dsapp/](https://www.novell.com/communities/coolsolutions/cool_tools/dsapp/)

Dies ist bereits auf dem vorliegenden Server installiert.

## Tipp 2

Die Dokumentation für GMS finden Sie unter

<https://www.novell.com/documentation/groupwise18/>

Für den normalen Benutzer siehe dort das Dokument [Quick Start for Mobile Device Users](#).

Auf dem Lehrerfortbildungsserver-BW gibt es eine Präsentation:

Siehe unter [https://lehrerfortbildung-bw.de/st\\_digital/netz/muster/novell/material/cloud/](https://lehrerfortbildung-bw.de/st_digital/netz/muster/novell/material/cloud/)

---

**Landesmedienzentrum Baden-Württemberg (LMZ)**  
**Support Netz**  
**Rotenbergstraße 111**  
**70190 Stuttgart**

© Landesmedienzentrum Baden-Württemberg, 2019