Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

HowTo

WLAN in der paedML Linux und GS

Stand 10.10.2023

paedML® Linux

Version: 7.2

paedML L

lmz Landesmedienzentrum Baden-Württemberg

Impressum

Herausgeber

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

70190 Stuttgart

Autoren

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

Johannes Albani, Alexander Vötterle

Endredaktion

Kay Höllwarth

Bildnachweis Symbole Titelseite

CC By 3.0 US von Gregor Cresnar, The Noun Project

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2023

Inhaltsverzeichnis

Vorwort

Es gibt mehrere Möglichkeiten Endgeräte per WLAN in das Schulnetz einzubinden. Dabei muss im Vorfeld entschieden werden, ob es sich zum Beispiel um Schüler- oder Lehrergeräte handelt, die eingebunden werden sollen. Auch die Frage, ob der Internetzugang dauerhaft oder nur zeitweilig bestehen soll, muss bedacht sein. Neben pädagogischen und didaktischen Aspekten hängt die jeweilige Entscheidung auch von der technischen Ausstattung der Schule ab. So sollte im Vorfeld klar sein, welche Anzahl an Zugriffen das schulische WLAN bedienen kann. Auch der Internetanschluss muss eine Vielzahl von Anfragen gleichzeitig bedienen können (Stichwort Flaschenhals), wenn das WLAN für viele Geräte genutzt werden soll.

Die Einrichtung des WLAN – ob innerhalb oder außerhalb der paedML Linux und GS – sollte von einem mit Netzwerktechnik vertrauten, versierten Dienstleister durchgeführt werden. Ein Support durch das Team der paedML Linux und GS ist hier über Einstellungen innerhalb der paedML Linux und GS hinaus nicht möglich.

Das folgende HowTo bezieht sich auf WLAN-Netze **innerhalb** der paedML Linux und GS.

Wir stellen Ihnen im folgenden HowTo drei verschiedene Möglichkeiten, deren technische Umsetzung innerhalb der paedML Linux und GS und entsprechende Anwendungsszenarien vor:
Die bekannte Einbindung über WPA2-Keys, die Radius-Authentifizierung und das Voucher-System Captive Portal.

Außerdem wird in 5. Kapitel auf die Integration von AirPrint-Druckern eingegangen, um sowohl mit herkömmlichen Windows-Clients, als auch mit iPads zu drucken.

Zielgruppe	Schwierigkeitsgrad
Händler, Administratoren	schwierig

1 Überlegungen zum Aufbau eines Schul-WLANs

Ein WLAN-Netz für die Schule muss vor Beginn der Arbeiten ausführlich konzipiert werden. Dabei muss die vorhandene Kabelstruktur analysiert und in vielen Fällen erheblich erweitert werden. Dies ist mit Kosten und häufig mit einem längerfristigen Planungsprozess verbunden. Die Umsetzung kann bauliche Maßnahmen erfordern. Die Access-Points sollten bereits ab einer geringen Stückzahl über eine zentrale Instanz verwaltbar sein und den Kriterien eines professionellen WLAN genügen. Bereits bei der Planung und spätestens vor Beschaffungsentscheidungen sollte dringend Beratung in Anspruch genommen werden.

Die eingesetzten Switche und der Internetanschluss müssen ausreichend dimensioniert sein und die nötigen Bandbreiten aufweisen. Insbesondere müssen die noch gängigen 100 Mbit-Switche ausgetauscht werden.

Für ein flächendeckendes und stabiles WLAN sollte das Schulhaus ausgeleuchtet werden.

Nicht zuletzt sollte bereits im Vorfeld entschieden werden, wie das WLAN an der Schule eingesetzt werden soll. Sollen etwa Schüler und Lehrer oder nur Lehrer Zugang bekommen? Soll der ganze Campus oder nur einzelne Bereiche des Schulhauses mit WLAN versorgt werden?

Relevant ist überdies die Frage, ob das WLAN nur schuleigene Geräte bedienen soll oder schülereigene Geräte (BYOD).

Nach diesen Fragestellungen richtet sich die eingesetzte Technik aber auch die netzwerktechnische Verortung des WLAN.

2 WPA2-Keys

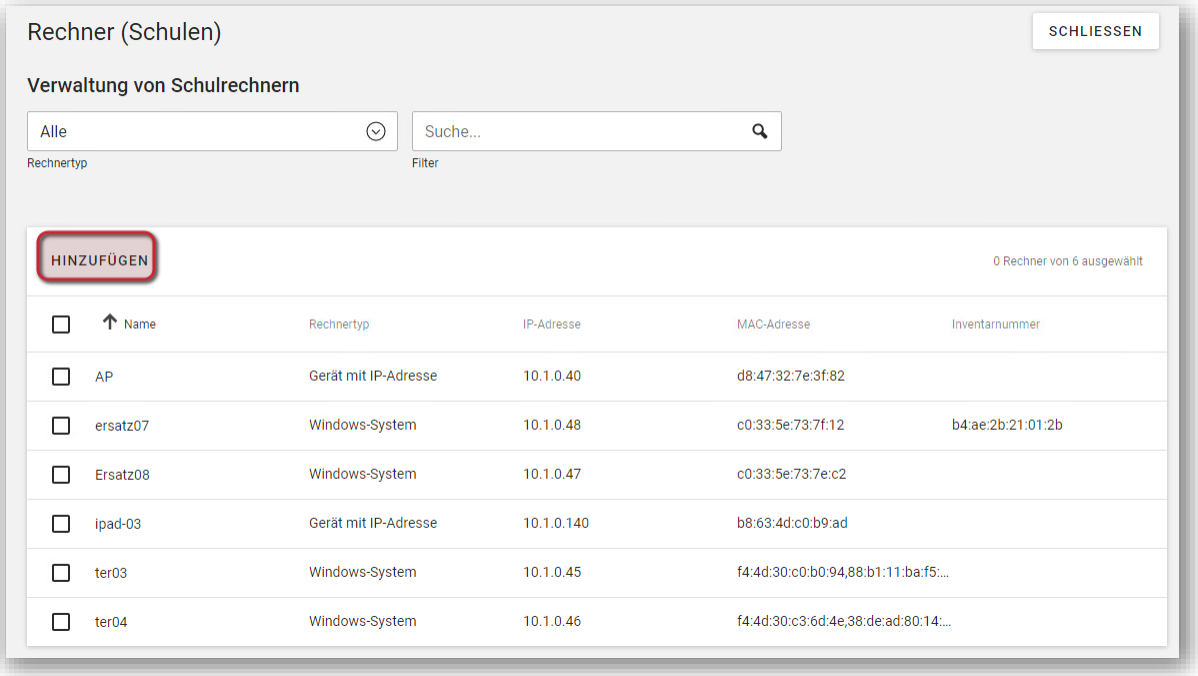
Die Anmeldung an einem WLAN mithilfe vorher bekannt gegebener Kennwörter (WPA2-Keys) ist unter Administratoren umstritten, da es möglich ist, solche Keys an manchen Geräten auszulesen. Da das Verfahren jedoch einfach und stabil ist, wird es trotzdem an vielen Schulen praktiziert. Eine Möglichkeit hier etwas mehr Sicherheit zu schaffen ist die Kennwörter in kurzen Abständen zu ändern und autorisierte Benutzer zur Geheimhaltung (evtl. schriftlich) zu verpflichten. Zusätzlich kann eine MAC-Adress-Filterung eingerichtet werden. Im pädagogischen Netz der paedML Linux und GS ist diese über die Aufnahme in der Schulkonsole umgesetzt.

Im Dokument **„Tablets in der paedML Linux und GS“** beschreiben wir in Kapitel 9 die Aufnahme eines Access-Points in das **MDM-Netz** und die Verteilung von WPA2-Keys an **iOS-Geräte**.

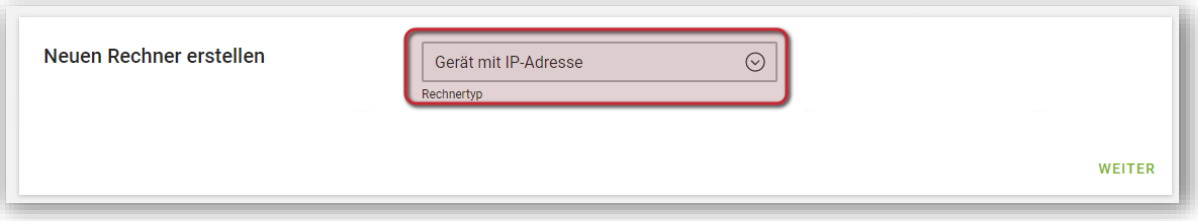
Im Folgenden wird die Aufnahme eines Access-Points in das **pädagogische Netz** und die Einrichtung eines per WPA2-Key gesicherten Netzes beschrieben. Die Verteilung der WPA2-Keys an **Windows-Geräte** erfolgt über ein opsi-Paket.

2.1 Aufnahme des Access-Points in der Schulkonsole

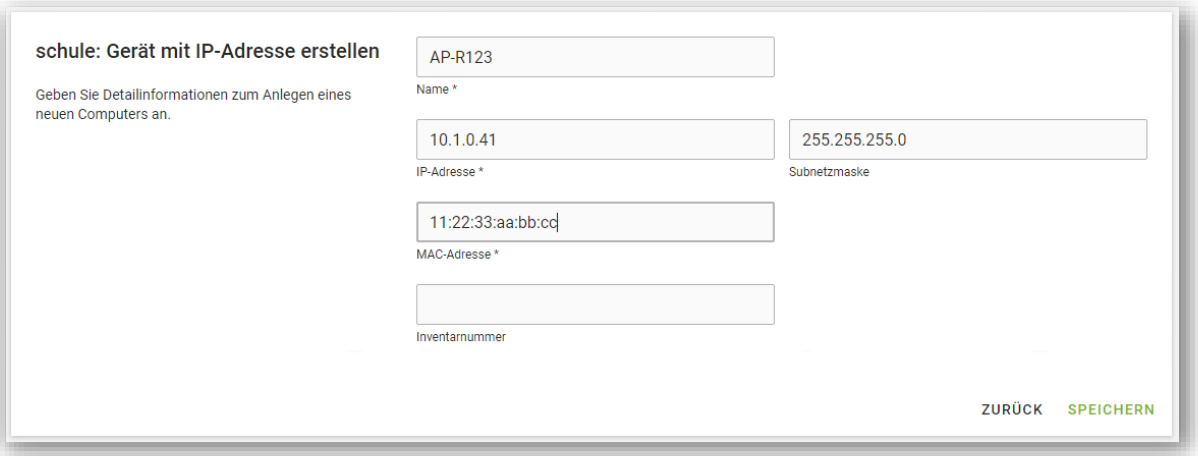
Öffnen Sie dazu in der Schulkonsole das Modul *Rechner* und klicken Sie auf *hinzufügen*.



Wählen Sie als *Rechnertyp „Gerät mit IP-Adresse*".



Wählen Sie einen aussagekräftigen Namen, vergeben Sie eine IP-Adresse und tragen Sie die MAC-Adresse ein.

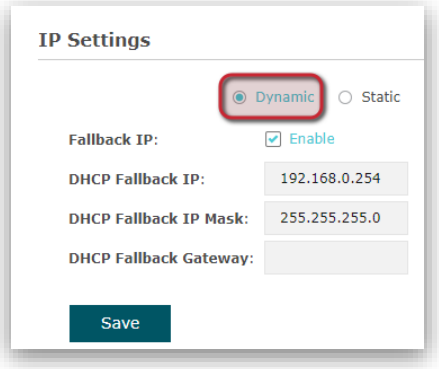


Der neu angelegt Access-Point erscheint nun in der Schulkonsole.

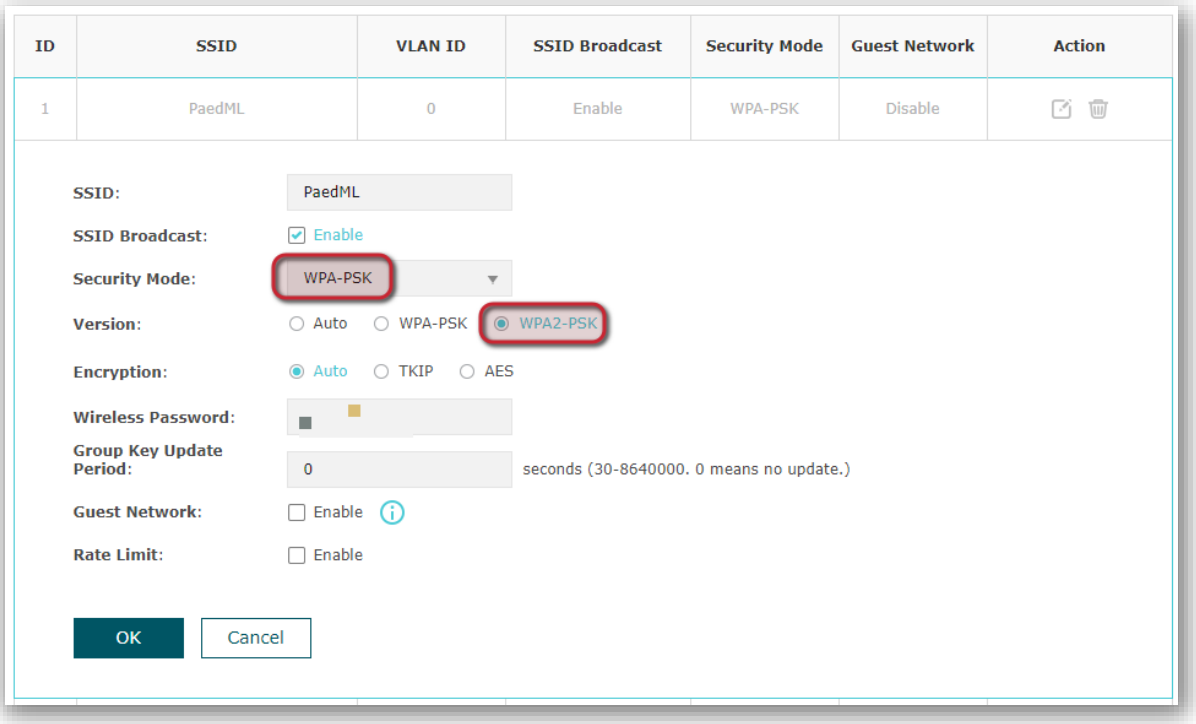
2.2 Konfiguration des Access-Points

Damit der Access-Point die korrekte IP-Adresse zugewiesen bekommt, muss dieser die IP-Konfiguration per DHCP erhalten.

Kontrollieren Sie dies in den Einstellungen des Access-Points. Hier wurde ein Access-Point mit der IP-Adresse 10.1.0.40 angelegt. In den IP-Setting ist zu erkennen, dass DHCP aktiviert ist.



Nun wird eine SSID *PaedML* mit einem WPA2-Key erzeugt. Das entsprechende Passwort wird im Access-Point eingetragen.



2.3 Verteilung der WPA2-Keys

2.3.1 Windows 10 / 11

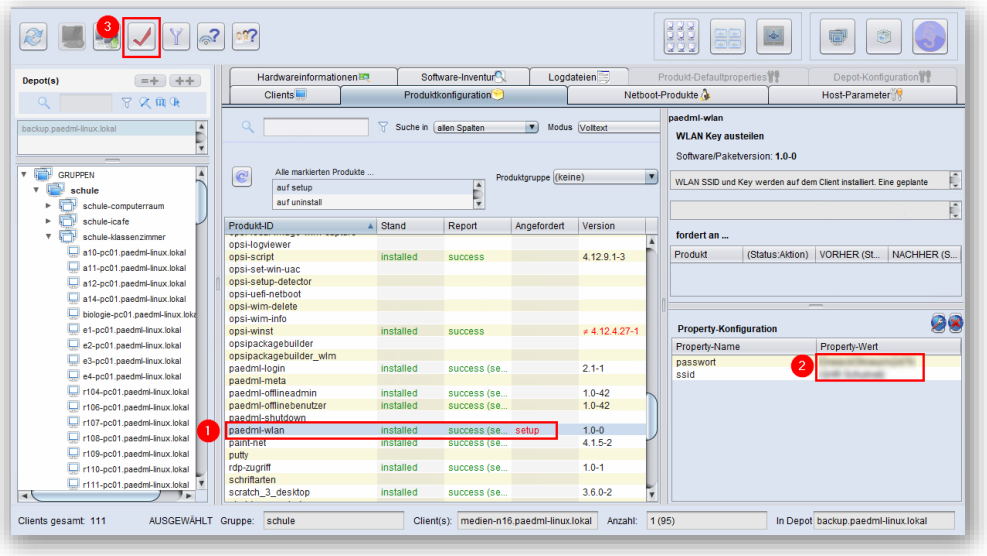
Für die Verteilung der WPA2-Keys kann das opsi-Paket „paedml-wlan“ verwendet werden. Voraussetzung hierbei ist, dass das Gerät über die LAN-Schnittstelle mit dem pädagogischen Netzwerk verbunden ist und über die Schulkonsole in die paedML aufgenommen wurde. Wie sie ein Windows-Gerät in das pädagogische Netzwerk aufnehmen, ist im Administratorhandbuch beschrieben.

Um das opsi-Paket „paedml-wlan“ auf dem opsi-Server zu installieren, melden Sie sich als „root“ am opsi-Server an und führen Sie diesen Befehl aus:

```
opsi-package-updater install paedml-wlan
```

Öffnen Sie dann den opsi-configed und markieren Sie den Client bzw. mehrere Clients, auf denen das WLAN ausgespielt werden soll.

1. Setzen Sie das opsi-Paket „paedml-wlan“ auf setup.
2. Geben Sie das Passwort und die SSID des WLAN ein.
3. Bestätigen Sie die Konfiguration mit einem Klick auf den roten Haken. Starten Sie den Client neu.

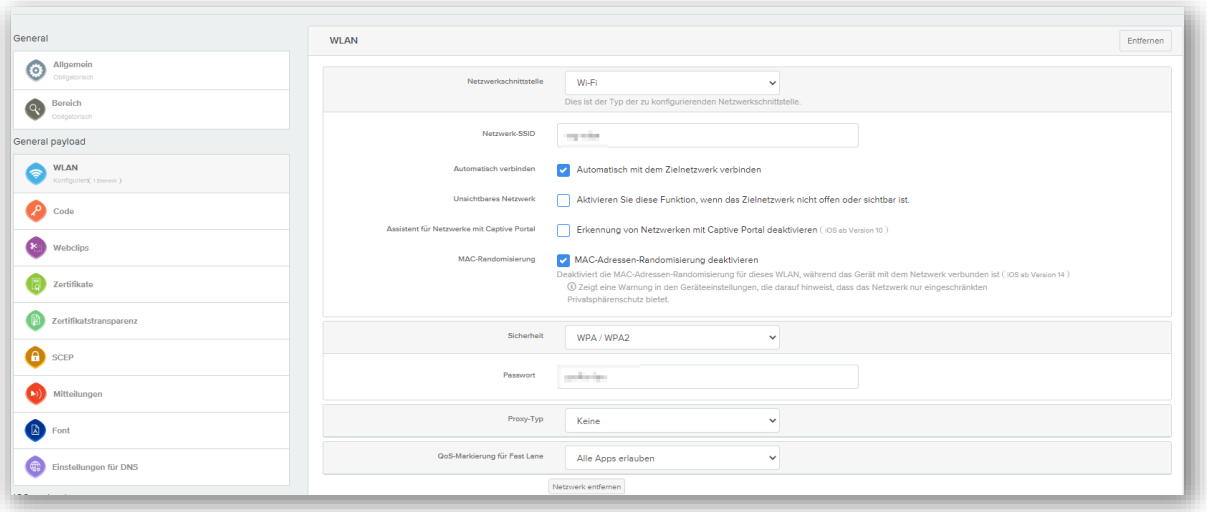


Das WLAN ist dem Rechner nun bekannt. Bitte beachten Sie, dass das WLAN als „paedML-WLAN“ angezeigt wird. Sollte der Client sich nicht automatisch mit dem WLAN verbinden, klicken Sie unten rechts auf das Netzwerksymbol und wählen Sie das WLAN „paedML-WLAN“ aus. Die Verbindung mit dem WLAN ist auch im Sperrbildschirm von Windows möglich. Auch hier klicken Sie unten rechts auf das Netzwerksymbol und wählen das WLAN aus.

2.3.2 iOS-Geräte

Auf iOS-Geräte können WLAN-Profile per MDM übertragen werden. Beachten Sie, dass die Geräte für die Übertragung des Profils bereits WLAN benötigen. Hier bietet sich ein offenes WLAN an, das nur für die Zeit der Installation der Tablets aktiviert wird.

Melden Sie sich an Ihrem MDM an und navigieren Sie zur entsprechenden Einstellung des Profils. Im Beispiel wird die Einstellung im MDM Jamf School gezeigt:



3 Radius

RADIUS wird in der paedML Linux und GS für die Authentifizierung von Rechnern und Benutzern im WLAN eingesetzt. Durch den Einsatz eines Radius-Servers melden sich die Benutzer mit den in der Benutzerdatenbank (Ldap) der *paedML Linux* gespeicherten Zugangsdaten (Benutzername und Passwort) an, anstatt einen einheitlichen WLAN-Schlüssel zu verwenden. Hierdurch erhält jeder Benutzer einen Zugang zum Netzwerk, abgesichert mit einem individuellen WLAN-Schlüssel. Diese Verschlüsselungsmethode wird zumeist *„WPA-Enterprise“* genannt, die der Accesspoint beherrschen muss.

Darüber hinaus kann die Radius-Authentifizierung auch für Windows-Clients eingerichtet werden.

Der *RADIUS-Server* muss auf den Access Points konfiguriert werden. Die vom Client übertragenen Benutzerkennungen werden dann durch den festgelegten *RADIUS-Server* geprüft, der wiederum für die Authentifizierung auf den UCS-Verzeichnisdienst zugreift.

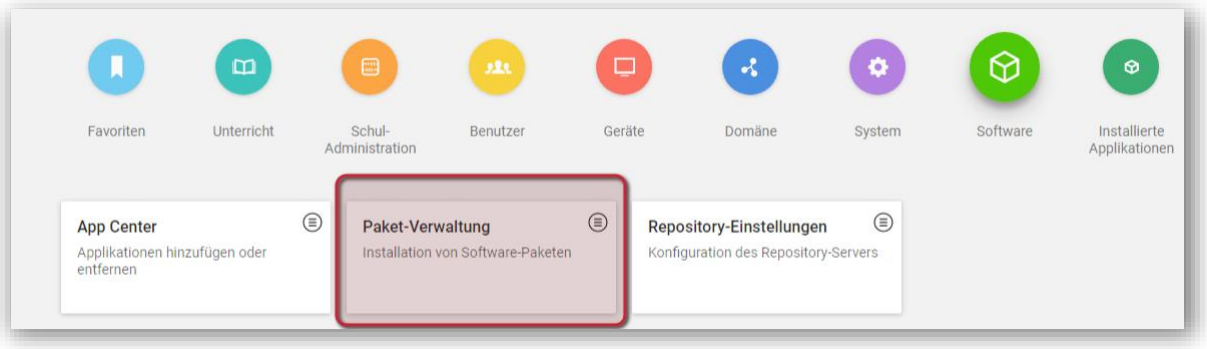
ACHTUNG für Bestandskunden:

In den Versionen 7.0 und 7.1 der paedML wurde Radius über die Datei „clients.conf" konfiguriert, eine Migration dieser Datei auf die paedML 7.2 und höher ist nicht möglich, da die Konfiguration nun über die Schulkonsole realisiert wird.

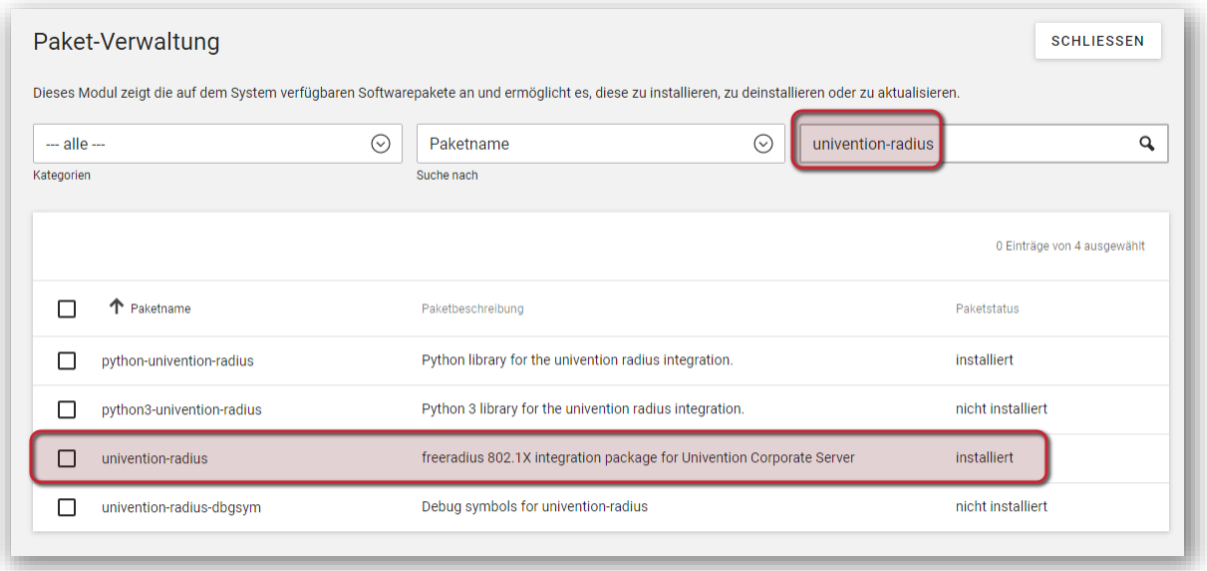
3.1 Installation des Radius-Servers

3.1.1 Installation von Univention-Radius

Überprüfen Sie, ob das Paket *„Univention-Radius"* installiert ist. Melden Sie sich dazu als *Administrator* an der Schulkonsole des Servers an und klicken Sie in der Kategorie *„Software"* auf *„Paket-Verwaltung"*.

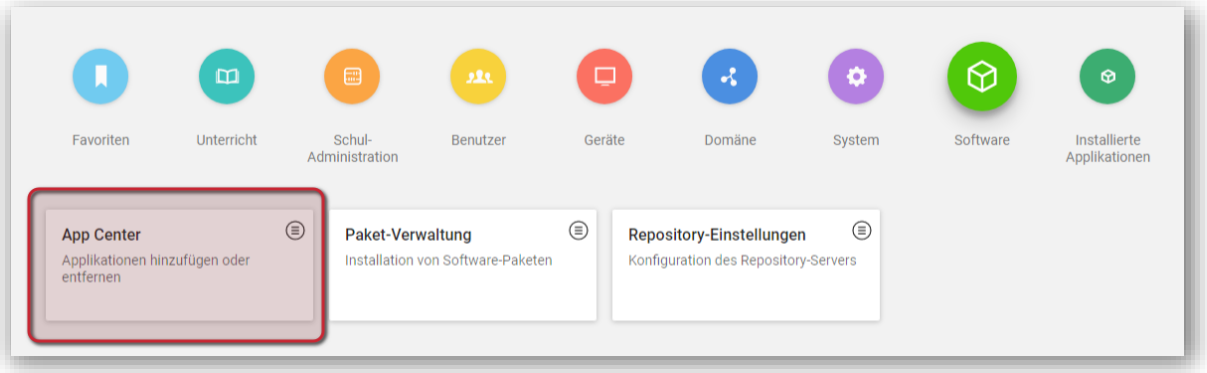


In der Paketverwaltung können Sie nach dem Paket suchen. In der Spalte *„Paketstatus"* wird angezeigt, ob das Paket installiert ist. Gegebenenfalls können Sie hier die Installation nachholen.

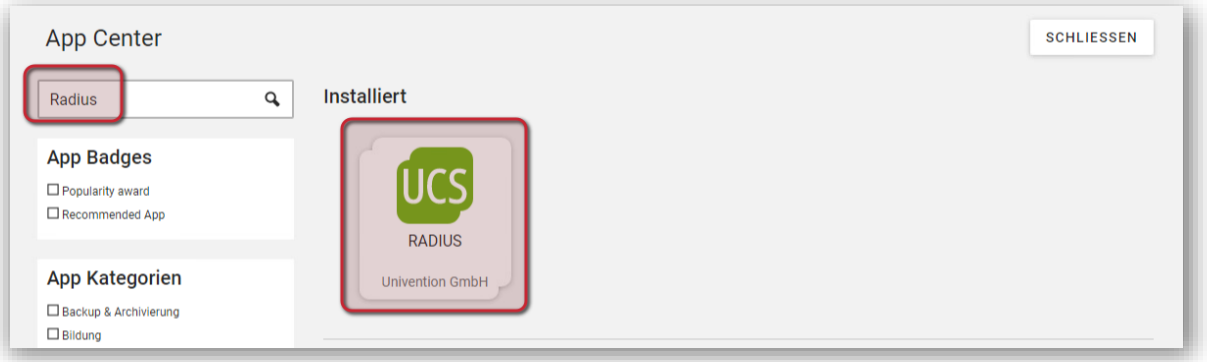


3.1.2 Installation der Univention-App Radius

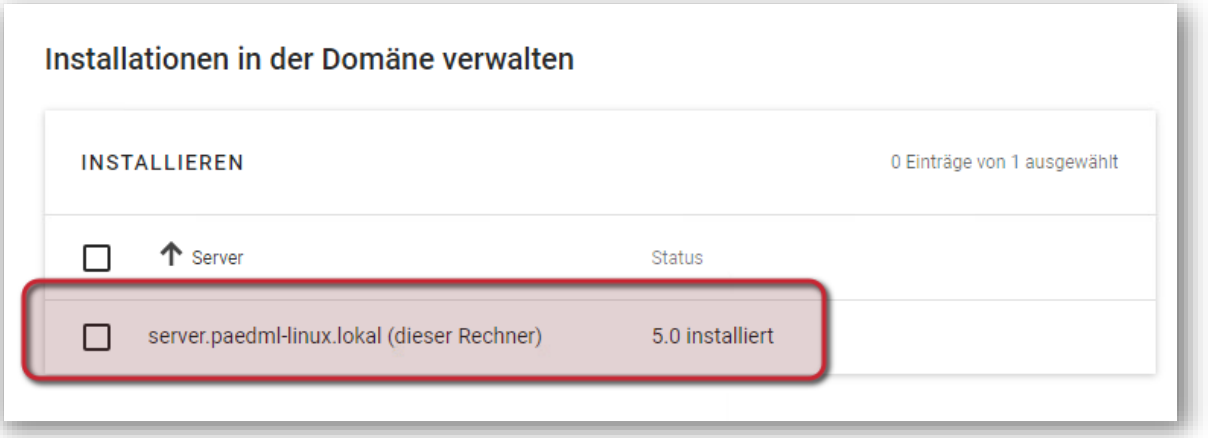
Klicken Sie im Bereich *Software* auf *App-Center*.



Suchen Sie die App *Radius* und klicken Sie auf deren Symbol.



Nach erfolgreicher Installation wir der Server als Installationsort aufgeführt.



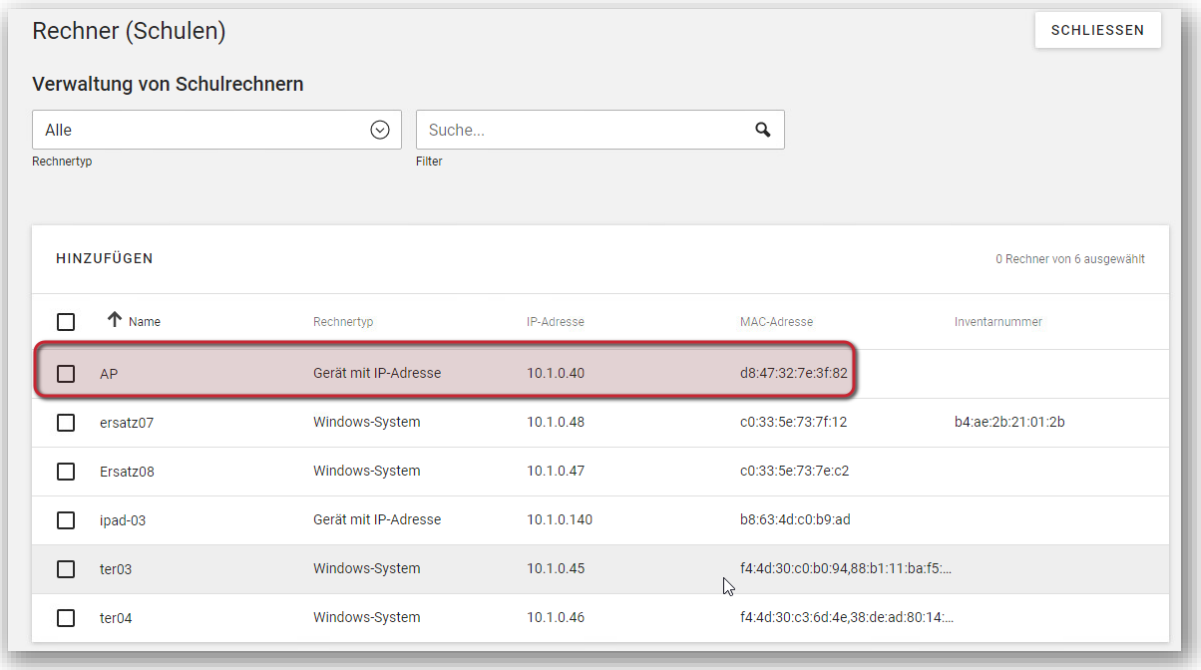
Nun kann Radius konfiguriert werden.

3.2 Konfiguration des RADIUS-Servers

3.2.1 Konfiguration der Access-Points in der Schulkonsole

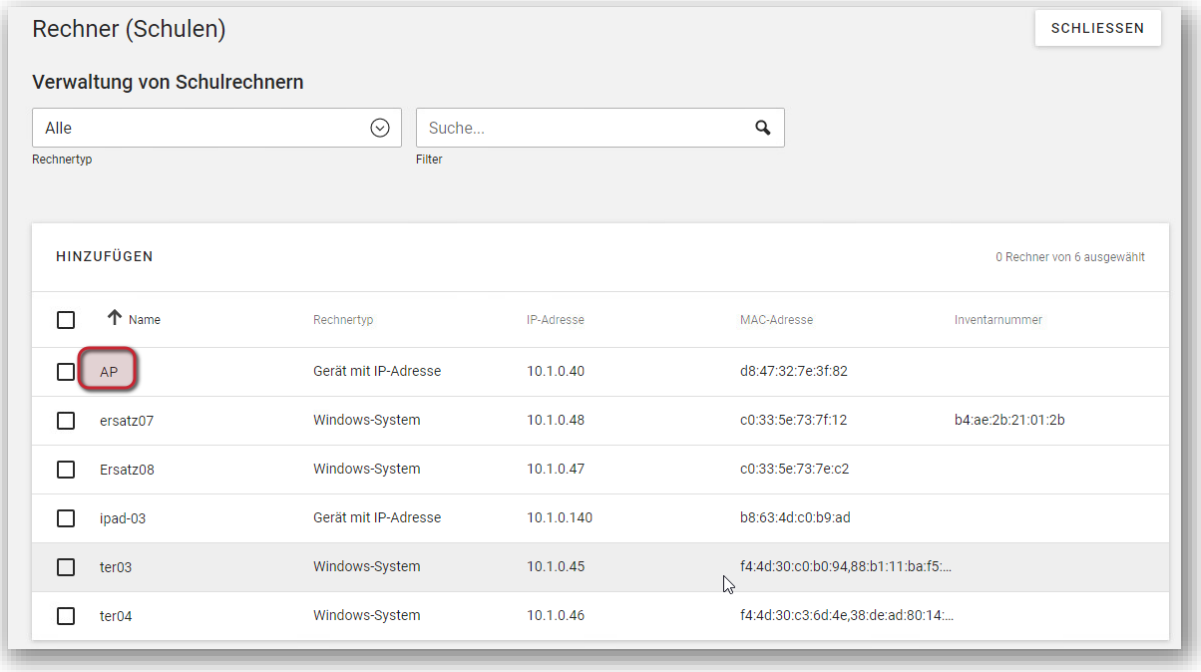
Die Aufnahme der Access-Points in der Schulkonsole wurde in Kapitel 1 beschrieben.

Das weitere Vorgehen wird anhand eines Accesspoints „AP“ im pädagogischen Netz beschrieben, der nach der Aufnahme in der Schulkonsole mit den folgenden Parametern erscheint:

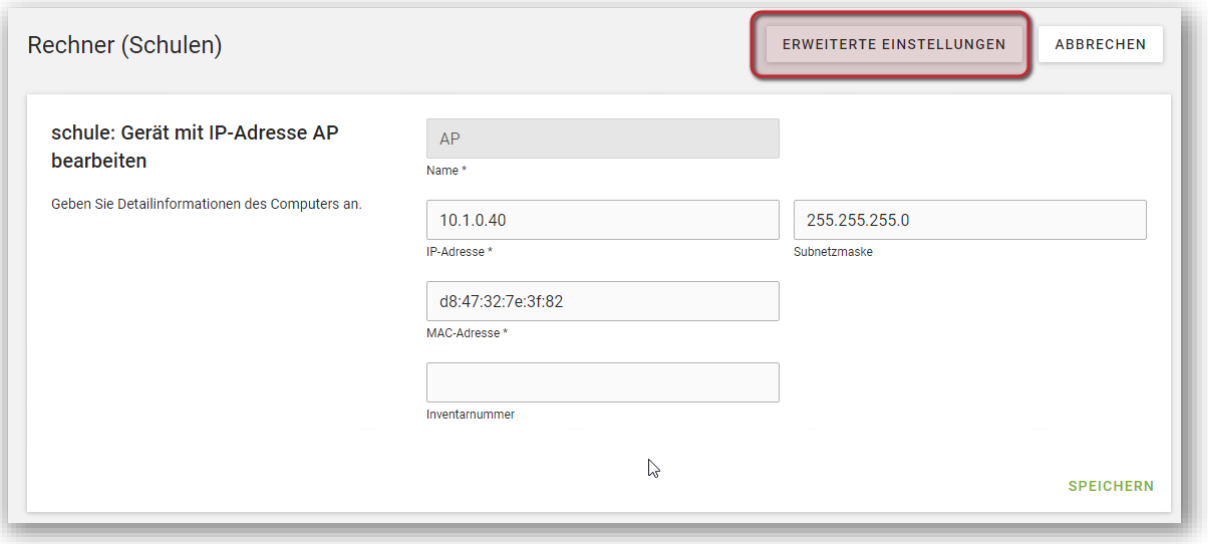


Für den Aufbau eines sicheren Tunnels zwischen Schulserver und den Accesspoints wird ein *„Secret“* zwischen dem RADIUS-Server und den Access Points ausgetauscht.

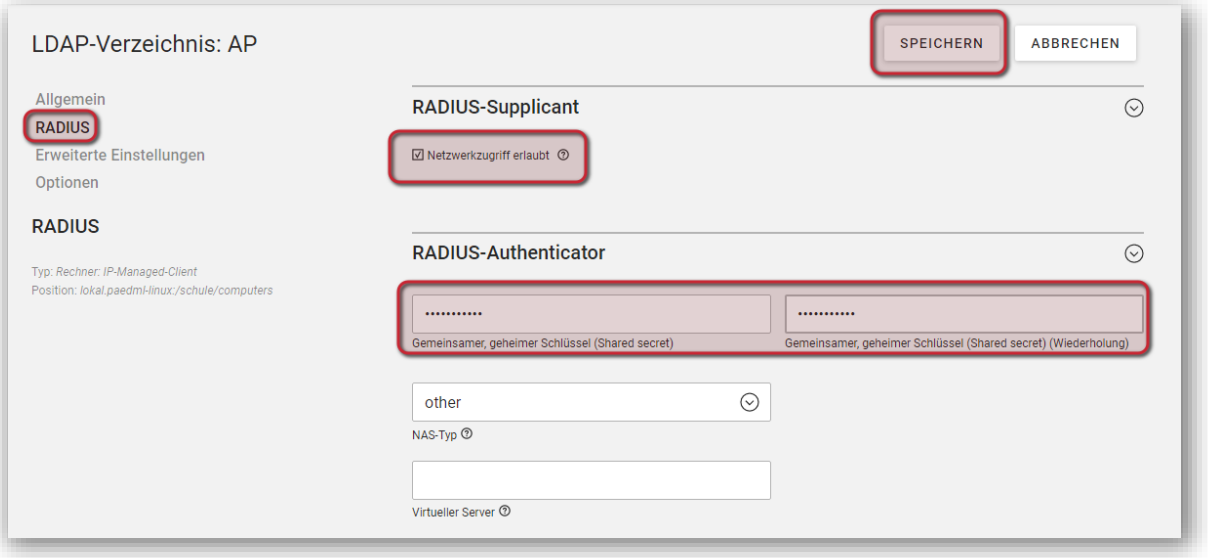
Klicken Sie dazu in der Rechnerliste auf den Accesspoint „AP“.



Klicken Sie auf *Erweiterte Einstellungen*.



Gehen Sie im folgenden Menü auf *RADIUS*, setzen Sie den Haken bei *Netzwerkzugriff erlauben*, geben Sie im Feld *Gemeinsamer geheimer Schlüssel* das Shared Secret ein und bestätigen Sie die Eingabe. Vergessen Sie nicht zu speichern.

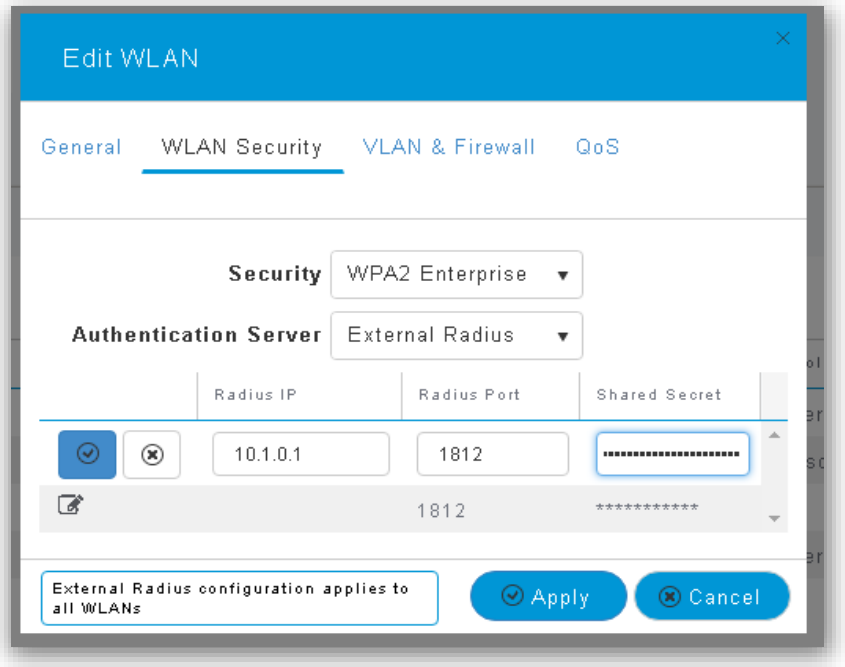


3.3 Aktivierung von Radius auf den Access-Points

Im Access Point muss die Authentifizierungsmethode auf *„WPA2 Enterprise“* mit externem Radiusserver eingestellt werden. Dies wird je nach Hersteller des Accesspoints unterschiedlich konfiguriert. Konsultieren Sie hierzu die Hinweise des Herstellers. Die folgende Abbildung zeigt die Konfiguration des Accesspoints am Beispiel des Modells *„Cisco AIR-AP1832I“.*

Die Adresse des Radiusservers ist *„10.1.0.1“*, der Radius Port *„1812“*.

Das *„Shared Secret“* muss dem der in der Schulkonsole hinterlegten *„Shared Secret“* entsprechen.

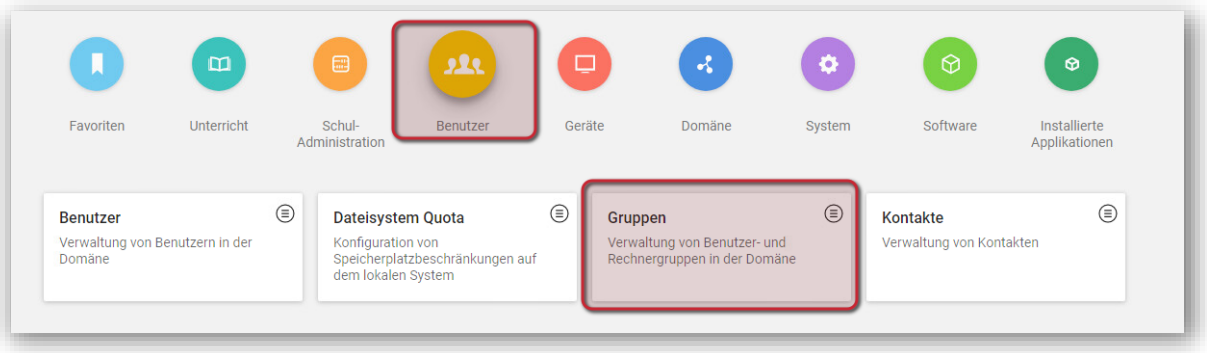


3.4 WLAN-Zugriff für Benutzer und Gruppen aktivieren

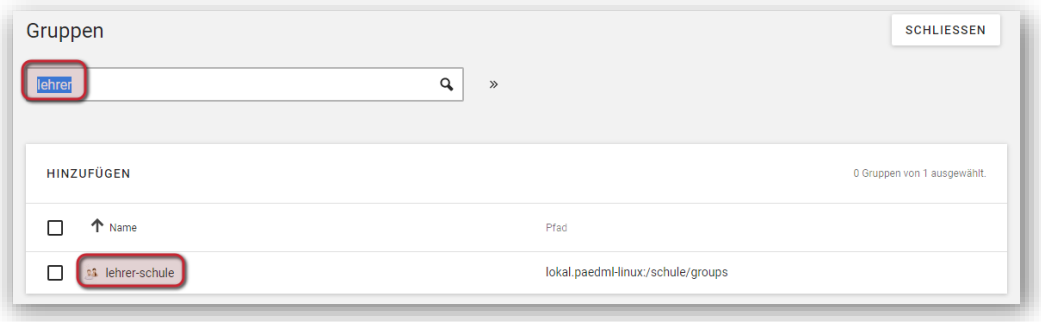
Eine Authentifizierung ist erst aus Sicherheitsgründen erst dann möglich, wenn dies dem Benutzer über die Schulkonsole erlaubt wird.

In der Regel wird die Erlaubnis auf Gruppen bezogen erteilt werden. Im Folgenden wird das Vorgehen am Beispiel der Gruppe der Lehrer beschrieben.

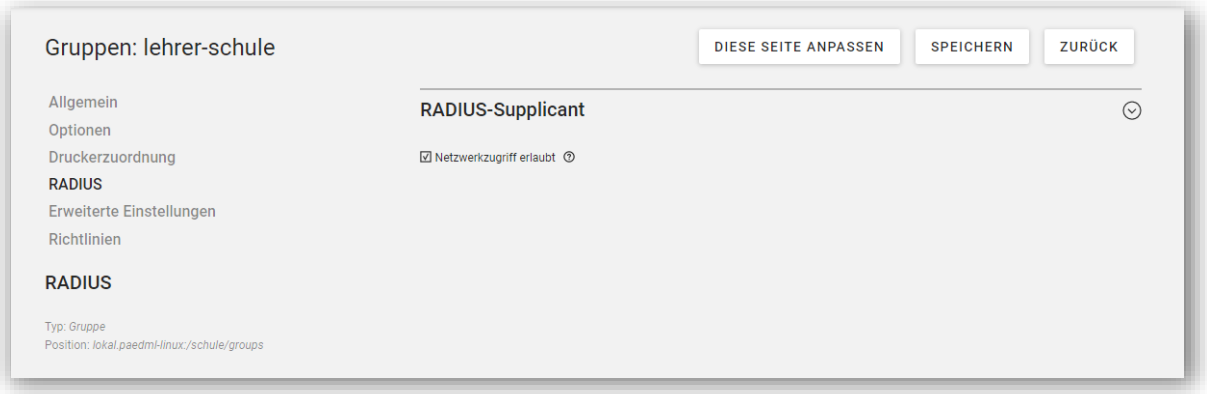
Dazu im Bereich Benutzer (gelb) Gruppen auswählen.



Im folgenden Dialog nach der Gruppe „*lehrer*“ suchen und diese auswählen.



Gehen Sie auf RADIUS, setzen Sie den Haken bei Netzwerkzugriff erlauben und speichern Sie die Einstellung.



Nun können sich alle Mitglieder der Gruppe lehrer-schule mithilfe von Radius authentifizieren.

Einzelnen Benutzern kann der Zugriff analog erlaubt werden. Dies wird jedoch nur in seltenen Fällen praktiziert werden.

3.5 Radius für Computerkonten einrichten

Für Computer, die im pädagogischen Netz über eine WLAN-Verbindung betrieben werden, bietet sich eine Radius-Authentifizierung über den Computernamen (das Computerkonto) an.

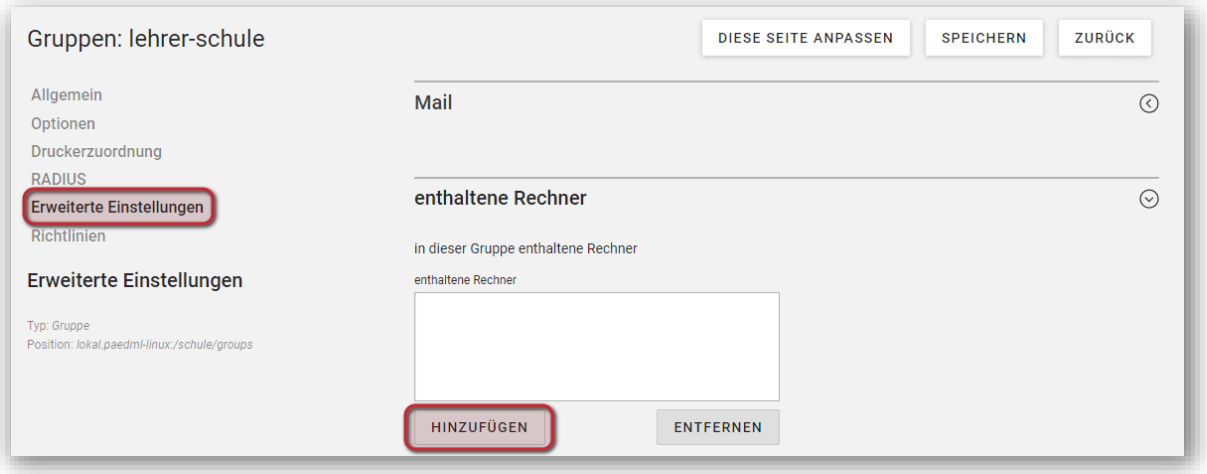
WICHTIG:

Die Radius Authentifizierung ist *„Case-Sensitive“,* das heißt, dass Groß- und Kleinschreibung beachtet werden. Dabei gilt die in Schulkonsole bzw. *Ldap* hinterlegte Schreibweise. Da Windows jedoch Groß- und Kleinschreibung weitgehend ignoriert, funktioniert eine Computerauthentifizierung **nur** wenn der Computername in der Schulkonsole bzw. Ldap keine Großbuchstaben enthält!

3.5.1 Aufnahme des Computers in Radius-berechtigte Gruppe

Der Computer muss einer Gruppe zugeordnet werden, für die Radius gemäß Kapitel 3 erlaubt wurde. Im Folgenden wird das Vorgehen wiederum am Beispiel der Gruppe *lehrer-schule* beschrieben.

Bearbeiten Sie dazu, wie in Kapitel 3 beschrieben die Gruppe *lehrer-schule*. Gehen Sie auf *Erweiterte Einstellungen* und öffnen Sie den Reiter „*enthaltene Rechner*“. Fügen Sie die Rechner hinzu, für die Sie die Radius-Authentifizierung erlauben möchten. Speichern Sie die Einstellungen.



3.5.2 Anpassungen am Computer

Für das Authentifizieren mit Hilfe des Computerkontos muss auf dem Computer noch das Wurzelzertifikat des *paedML* Servers installiert werden und die Verbindung per Computerkonto aktiviert werden.

Vorgehensweise für Windows 10 Clients:
Die nachfolgend beschriebenen Dialoge unter Windows 10 sind über

Netzwerk- und Interneteinstellungen | Ethernet | Adapteroptionen ändern | WLAN | Status | Drahtloseigenschaften

zu erreichen.

http://wiki.univention.de/index.php?title=Einrichtung_des_WLAN-Zugriffs_%C3%BCber_RADIUS_f%C3%BCr_Windows_10

Das Zertifikat wird automatisch durch das Opsi-Paket „zertifikat“ auf allen Clients ausgerollt, daher kann der erste Teil der Univention-Anleitung übersprungen werden.

3.6 Fehlersuche

Im Fehlerfall sollte die Logdatei *„/var/log/freeradius/radius.log“* geprüft werden. Erfolgreiche Logins führen zu einem Logeintrag *„Auth: Login OK“* und eine fehlgeschlagene Authentifizierung beispielsweise zu *„Auth: Login incorrect“.*

Weitere Informationen zu *„Freeradius“* ist unter http://freeradius.org/doc/ zu finden.

Mit dem Befehl

univention-radius-check-access -- username *Benutzername*

kann überprüft werden, ob für einen bestimmten Benutzernamen die Radius-Authentifizierung erlaubt ist.

```
Last login: Tue Mar 30 14:56:15 2021 from 10.1.0.15
root@server:~# univention-radius-check-access --username anna.na
```

4 Captive Portal

Im Unterrichtsgeschehen wird es zunehmend wünschenswert, den Schülerinnen und Schülern die Möglichkeit zu geben, das Internet zu nutzen. So können etwa Recherchen gemacht oder bestimmte Apps sinnvoll eingesetzt werden. Da in der Regel fast alle Schülerinnen und Schüler ab einem bestimmten Alter ein Smartphone in der Schule ohnehin dabeihaben, macht es gegebenenfalls Sinn, dieses zu nutzen.

Leider könnten die Schülerinnen und Schüler zum einen das WLAN außerhalb dieser Phasen missbrauchen, zum anderen könnten Nutzer – auch Lehrerinnen und Lehrer – mit ihren Privatgeräten das Netzwerk der Schule belasten.

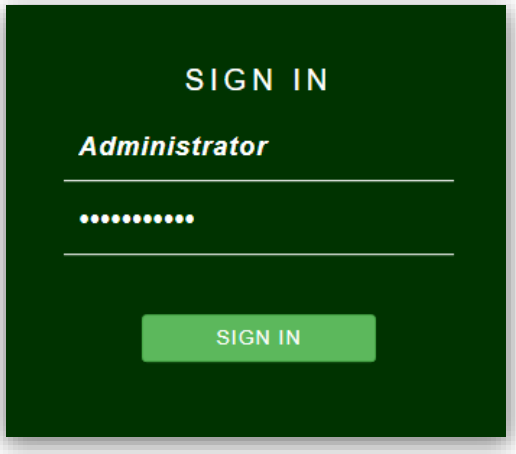
Eine Lösung stellt die Vergabe von zeitbeschränkten WLAN-Zugangscodes, sogenannten Vouchers, dar. Dabei erhalten Nutzer einen Code, der im Browser eingegeben werden muss. Sie können dann nach einer vorgegebenen Zeit im Internet surfen. Diese Zugangscodes verlieren nach Ablauf der Zeit ihre Gültigkeit.

Die folgende Anleitung beschreibt die Einrichtung des Dienstes *Captive Portal* auf der Firewall *pfsense*. Mit Hilfe dieses Dienstes können Vouchers erzeugt werden, die ein zeitlich beschränktes Surfen im Internet ermöglichen.

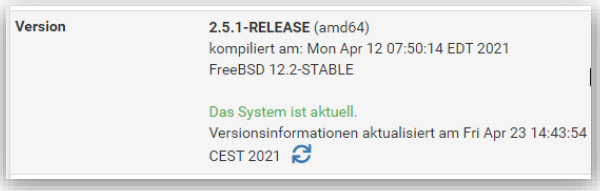
Die Beschreibung bezieht sich auf die Verwendung von Captive Portal beim Gästenetz der paedML Linux, da sich in diesem die schulfremden Geräte bewegen sollten.

4.1 Captive-Portal aktivieren

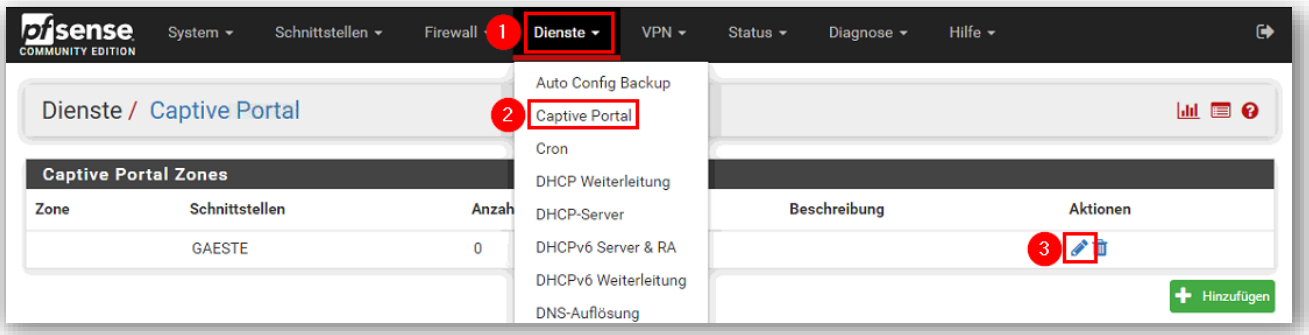
Das Captive Portal wird komplett auf der Firewall (pfSense) umgesetzt. Öffnen Sie die Weboberfläche der Firewall. Öffnen Sie im Browser dazu „https://firewall.paedml-linux.lokal/“ . Geben Sie als Benutzernamen *Administrator* und das Firewall-Passwort ein und klicken Sie auf *SIGN IN*.



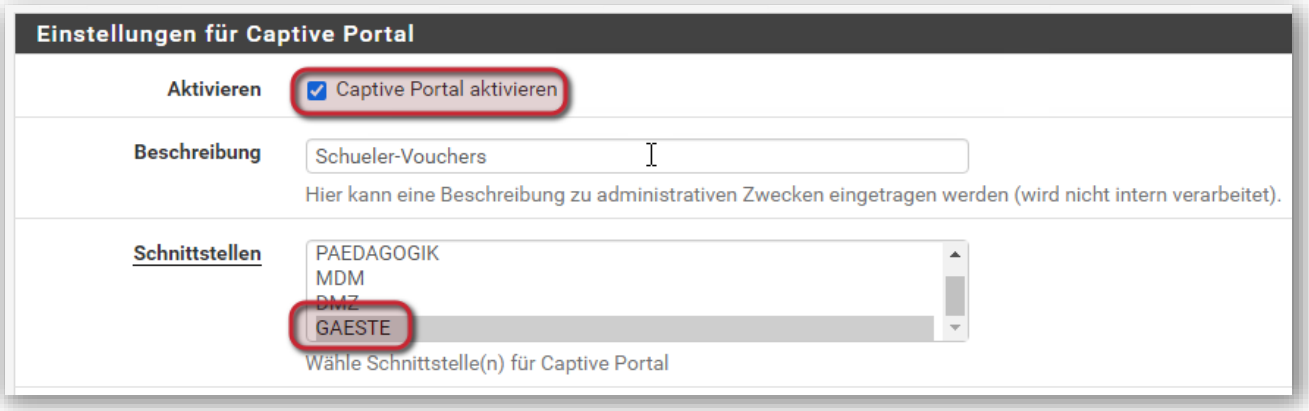
Bitte kontrollieren Sie in der Übersichtsseite ob Ihre Firewall aktuell ist, führen Sie gegebenenfalls ein Update durch.



Öffnen Sie im *Menü Dienste* | *Captive Portal*. Klicken Sie in der Zeile *GAESTE* bei *Aktionen* auf das Bleistiftsymbol. Sollte dieser Eintrag bei ihnen fehlen fügen Sie zunächst eine Captive-Portal-Zone hinzu.

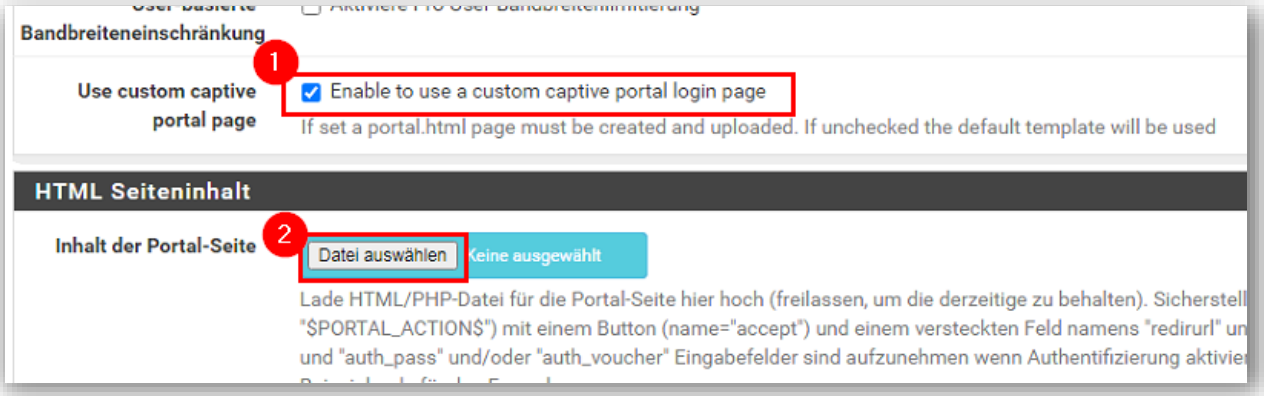


Als erstes setzen Sie den Haken bei *Captive Portal aktivieren*. Die Seite blendet dadurch neue Einstellungen ein.

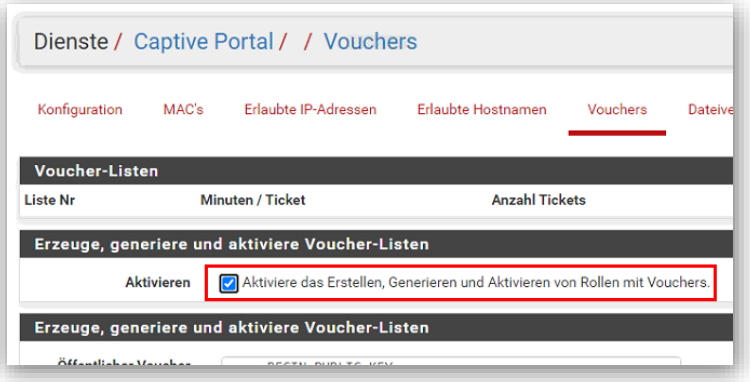


Die Einstellungen können auf den Standardeinstellungen belassen werden, suchen Sie jedoch den Abschnitt *Use custom captive portal page* und klicken Sie auf *Enable to use a custom portal login page*. Dadurch können Sie eine eigene Portalseite verwenden. Benutzen Sie hierzu die Vorlage *portal.html*. Diese können Sie von der Homepage des LMZ im Bereich paedML Linux unter Downloads herunterladen. Sie ist in der zip-Datei „Captive-Portal-Dateien“ enthalten. Klicken Sie auf „Datei auswählen“ und wählen die Datei *„portal.html“* aus. Klicken Sie dann ganz unten auf der Seite auf *Speichern*.

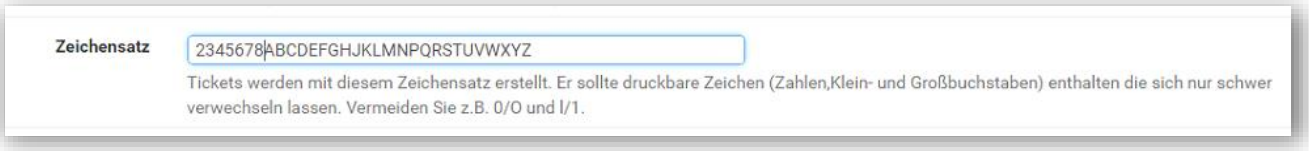
Sie gelangen durch das Speichern zurück zur Captive Portal Übersichtsseite. Klicken Sie erneut auf das



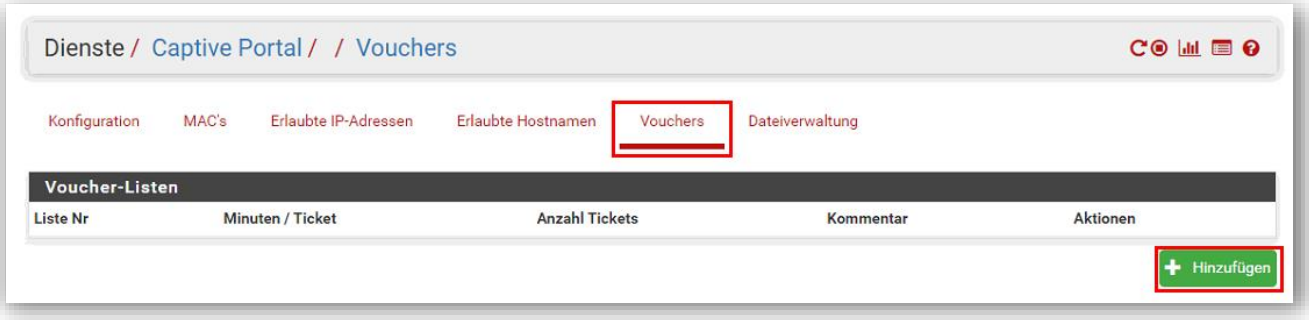
Bleistiftsymbol und wählen Sie „Vouchers“. Klicken Sie auf *„Aktiviere das Erstellen, Generieren und Aktivieren von Rollen mit Vouchers“.*



Um den Schülerinnen und Schülern das Eingeben der Voucher zu erleichtern können Sie den Zeichensatz anpassen, z.B. alle Kleinbuchstaben entfernen. Dadurch können zwar weniger Voucher pro Vorgang erzeugt werden, erleichtern aber den Umgang damit. Klicken Sie wieder auf „Speichern“ am unteren Seitenende.

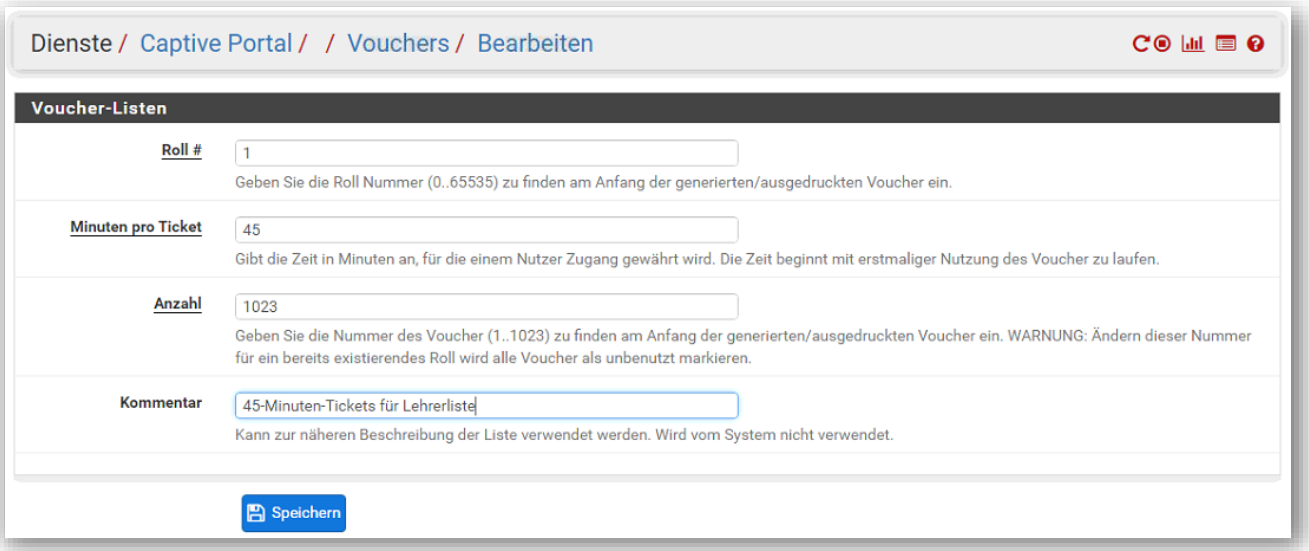


Nun müssen Voucher erzeugt werden. Klicken Sie im Menü *Vouchers* bei *Voucher-Listen* auf *+Hinzufügen*.



Im Voucher Rolls Menü legen Sie die *Roll #* fest. Dies ist die Eindeutige Voucher Nummer. Da noch keine Voucher bestehen wählen sie die 1, später die 2, 3 usw. Sie können die Rolls später auch wieder entfernen und die Roll Nummer dann erneut verwenden.

Bei *Minuten pro Ticket* wählen Sie, für wie viele Minuten nach der ersten Aktivierung der Voucher abläuft. Bei *Anzahl* legen Sie fest, wie viele verschiedene Voucher sie benötigen. Bei *Kommentar* tragen Sie den Verwendungszweck der Voucher ein. Klicken Sie im Anschluss auf *Speichern*.



Um die Excel-Vorlage *„Schluessel.xlsx“* für das Erstellen von Voucher-Listen benutzen zu können erstellen Sie bitte die folgenden vier Voucher-Rolls, wobei die Roll-Nummer gegebenenfalls angepasst werden kann:

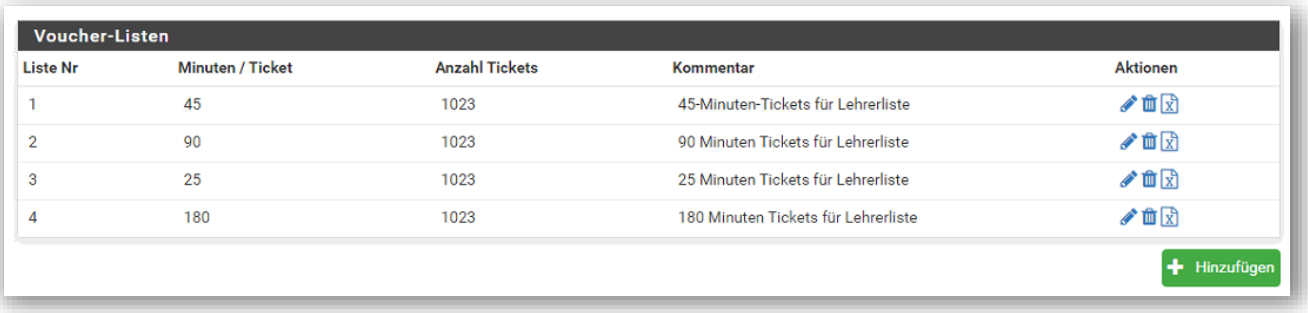
Liste Nr 1, Minuten/Ticket: 45, Anzahl Tickets 1023, Kommentar: 45 Minuten Tickets für Lehrerliste

Liste Nr 2, Minuten/Ticket: 90, Anzahl Tickets 1023, Kommentar: 90 Minuten Tickets für Lehrerliste

Liste Nr 3, Minuten/Ticket: 25, Anzahl Tickets 1023, Kommentar: 25 Minuten Tickets für Lehrerliste

Liste Nr 4, Minuten/Ticket: 180, Anzahl Tickets 1023, Kommentar: 180 Minuten Tickets für Lehrerliste

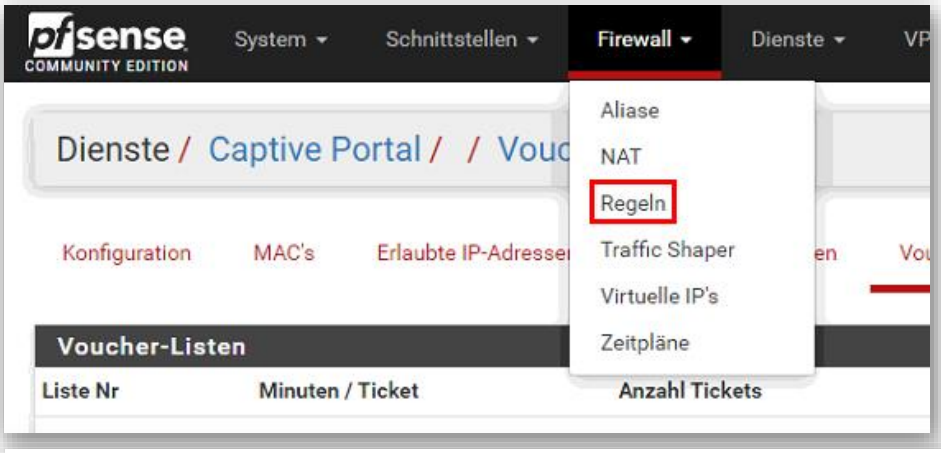
Laden Sie sich nun die erstellten Voucher Listen herunter. Klicken Sie dazu auf das Blattsymbol mit dem „x“. Mit dem Mülleimer Symbol können Sie gegebenenfalls nicht mehr benötigte Voucher wieder löschen und die Liste dadurch wieder freigeben. Die heruntergeladenen Voucher-Listen können nun mit einem Tabellenkalkulationsprogramm oder Notepad++ geöffnet werden und die Voucher verwendet werden.

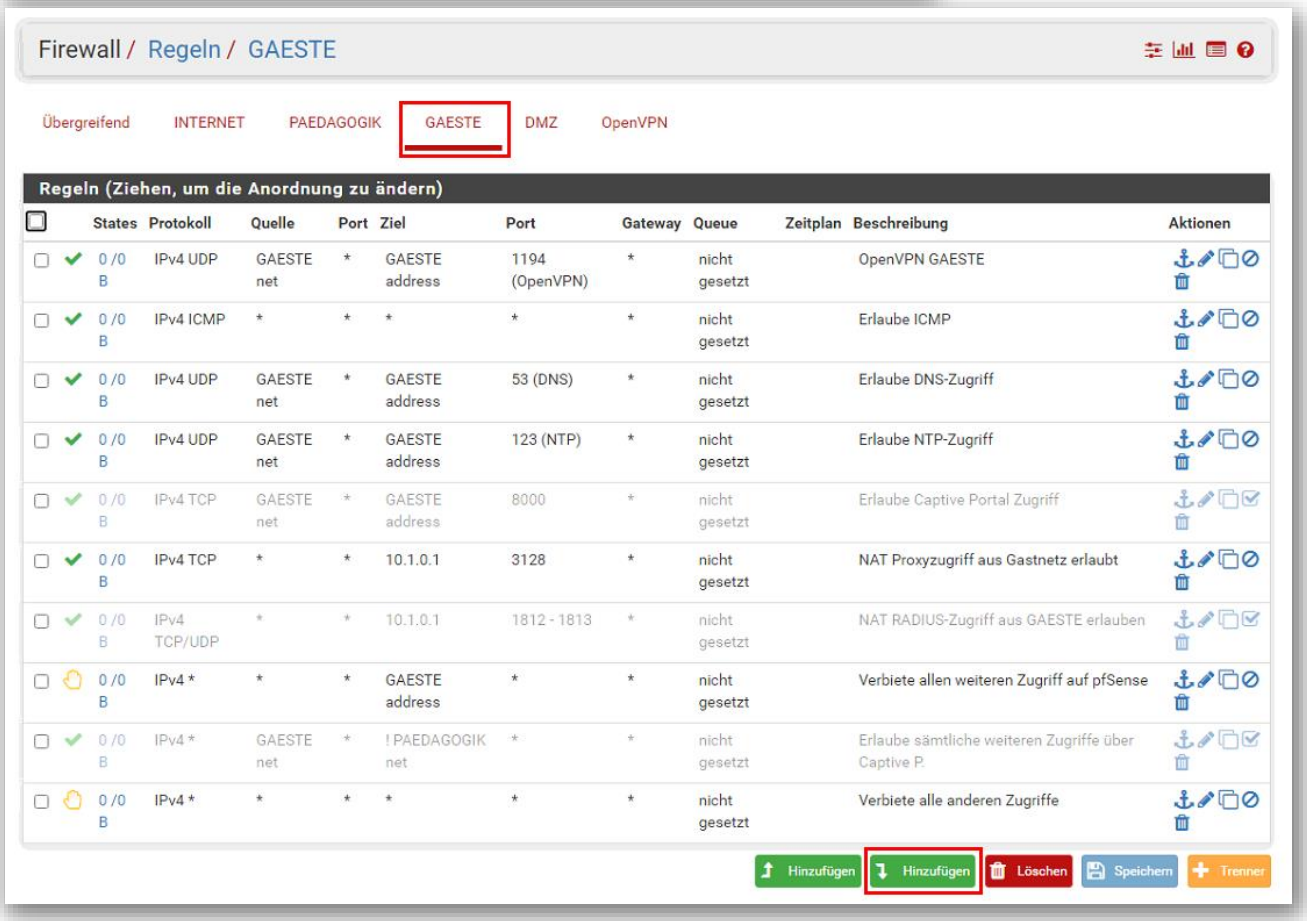


4.2 Internetzugriff freischalten

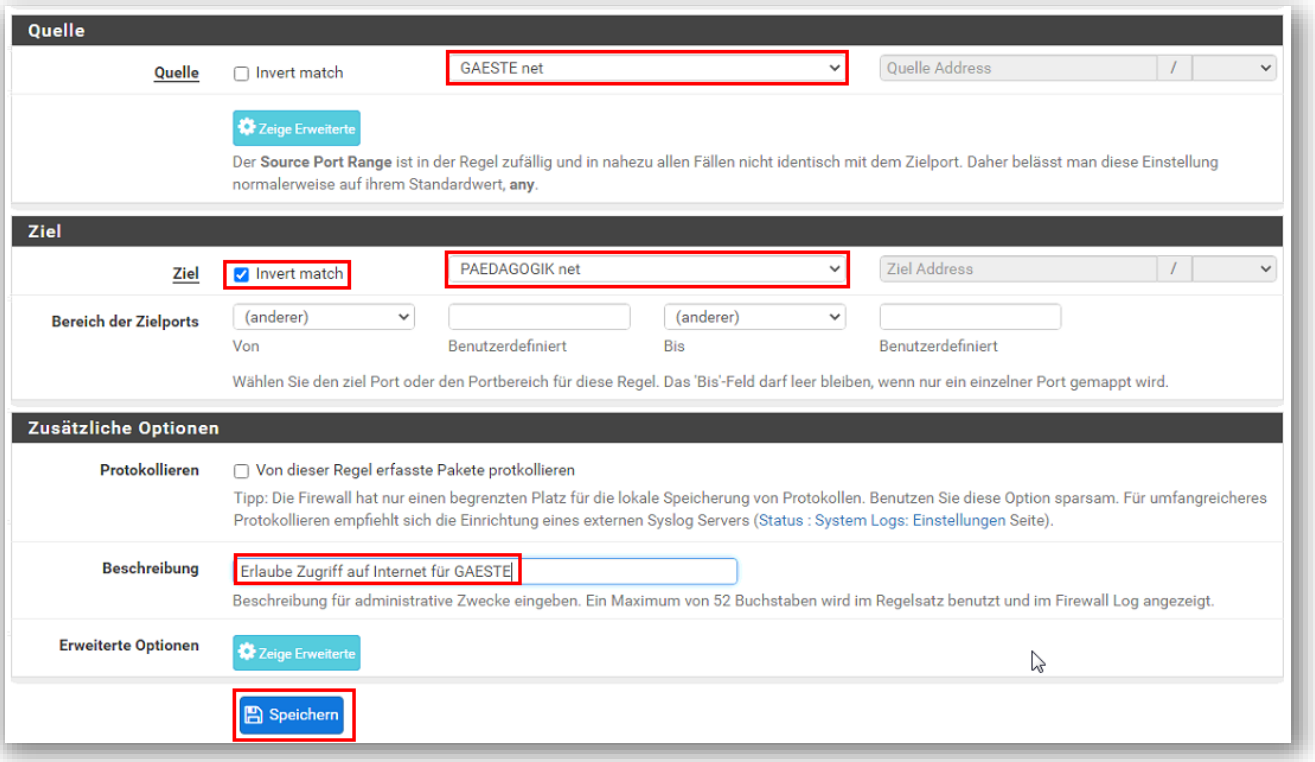
Die Voucher lassen nun Benutzer in das Gästenetz. Damit man aus dem Gästenetz jedoch auch eine Internetverbindung herstellen kann muss dies in der Firewall noch erlaubt werden.

Klicken Sie auf *Firewall* | *Regeln* und wählen Sie *GAESTE* aus.





Klicken Sie auf den linken „Hinzufügen“-Knopf, um eine Regel „oben“ einzufügen. Stellen Sie bei Quelle *GAESTE net* ein, bei *Ziel* klicken Sie auf *Invert match*. und wählen Sie *PAEDAGOGIK net* aus, damit WLAN-Nutzer keinen Zugriff auf das pädagogische Netz, aber ansonsten keine Einschränkungen haben. Geben Sie bei *Beschreibung* eine Erklärung der Regel an, z.B. „Erlaube Zugriff auf Internet für GAESTE“ und klicken Sie auf *Save*.



Vergessen Sie nicht die Änderungen durch *Speichern* zu übernehmen.

Manchmal öffnen Endgeräte nicht direkt die Captive Portal Seite. Man kann in diesem Fall einen Browser und dort eine Webseite öffnen. Wenn die Seite per **http** angesprochen wird, wird das Captive Portal angezeigt. Achten Sie darauf, dass moderne Browser jedoch in der Regel versuchen mit **https** ins Internet zu gehen. D.h. man muss die Adresse manuell anpassen und das **s** löschen.

Aus https://www.heise.de muss http://www.heise.de werden, um das Captive Portal verlässlich anzeigen zu lassen.

Dieses Verhalten hat jedoch jedes Captive Portal, z.B. auch jeder Hotspot in Fast-Food Restaurants.

4.3 Voucher verteilen

Um während des Unterrichts den Schülerinnen und Schülern WLAN zur Verfügung zu stellen, brauchen Lehrende gültige Voucher. Dazu können Sie die Datei *„Schluessel.xlsx“* verwenden. Diese können Sie von der Homepage des LMZ im Downloadbereich der paedML Linux herunterladen. Die Datei ist im zip-Archiv „Captive-Portal-Dateien“ enthalten.

Die Datei hat 6 Datenblätter, *VoucherDruck, Lehrende, 45, 90, 25* und *180*. Jede Voucher-Schlüssel Seite ist einmalig und sollte nur von einer Person verwendet werden, da einmal benutzte Voucher nicht mehr von anderen verwendet werden können.

Um die Datei einsetzen zu können brauchen Sie die Voucher-Listen, die Sie in der Firewall erzeugt und heruntergeladen haben. Öffnen Sie die Datei mit den 45 Minuten Vouchern in Excel oder LibreOffice und kopieren Sie deren Inhalt (Strg+c). Öffnen Sie nun in der Schluessel.xlsx das Blatt 45 und überschreiben den Inhalt mit den kopierten Inhalten. Verfahren Sie entsprechend mit den Vouchern für 90, 25 und 180 Minuten.

Wenn Sie Ihre aktuellen Voucher alle in die Tabellen eingefügt haben, tragen Sie bitte noch bei *„Lehrende“* jeweils ein, welche Nummer welchem Lehrenden zugeordnet werden soll.

Nun können Sie auf der Seite *VoucherDruck* rechts oben die Nummer anpassen, der Name der/des Lehrenden und neue Voucher werden auf der Seite dargestellt. Diese können Sie nun ausdrucken. Ändern Sie für die nächste Liste wieder die Nummer rechts oben, drucken, usw.

Achten Sie darauf, dass bei den ca. 1000 erstellten Vouchern bei nach 38 gedruckten Listen die verfügbaren Voucher ausgehen. Erstellen Sie bei Bedarf weitere Voucher und hängen Sie diese an die Listen (45, 90…) an. Sie können natürlich auch die Rolls 1 bis 4 wieder löschen und die Voucher-Listen neu erzeugen, z.B. beim Schuljahreswechsel.

5 AirPrint-Drucker

Damit iPads Drucker verwenden können muss der Drucker den AirPrint Standard unterstützen und über das Bonjour-Protokoll auffindbar sein. In der Regel funktioniert dieses Protokoll nur, wenn die Drucker im gleichen (Sub-)Netz sind. In der paedML Linux/GS sind die Drucker jedoch in der Regel im Netzwerk „PAEDAGOGIK“, bekommen also eine IP-Adresse der Form 10.1.0.* während die iPads in der Regel im MDM-Netz liegen und eine mit 172.23 beginnende Adresse haben.

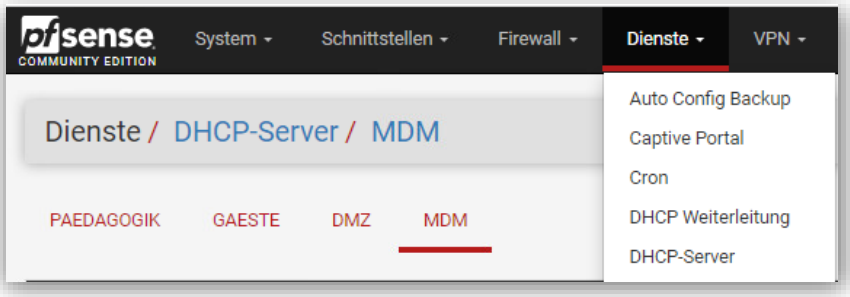
Um Drucker nun gleichzeitig für die Clients der paedML Linux und iPads im MDM-Netz verwenden zu können, müssen die Drucker also im MDM-Netzwerk sein. Dort können diese dann direkt von den iPads gefunden und verwendet werden. In der Regel muss man durch zuweisen von entsprechenden VLANs an den Switchen den Netzwerkanschluss der Drucker entsprechend anpassen. Die Umsetzung hängt von der verbauten Hardware ab, kontaktieren Sie gegebenenfalls Ihren Dienstleister.

Die Druckaufträge aus der paedML werden über den Server vermittelt, d.h. es reicht, wenn der Server auf die Drucker in dem anderen Netzwerk zugreifen kann. Im Auslieferungszustand der Firewall kann der Server die Adressen aus dem MDM-Netz erreichen und umgekehrt können Geräte im MDM-Netz auch den Server erreichen, es sind also dort keine weiteren Einstellungen notwendig.

Das Problem ist nun noch, dass die Drucker im MDM-Netz ihre IP-Adressen nicht vom paedML DHCP zugewiesen bekommen, sondern von der Firewall.

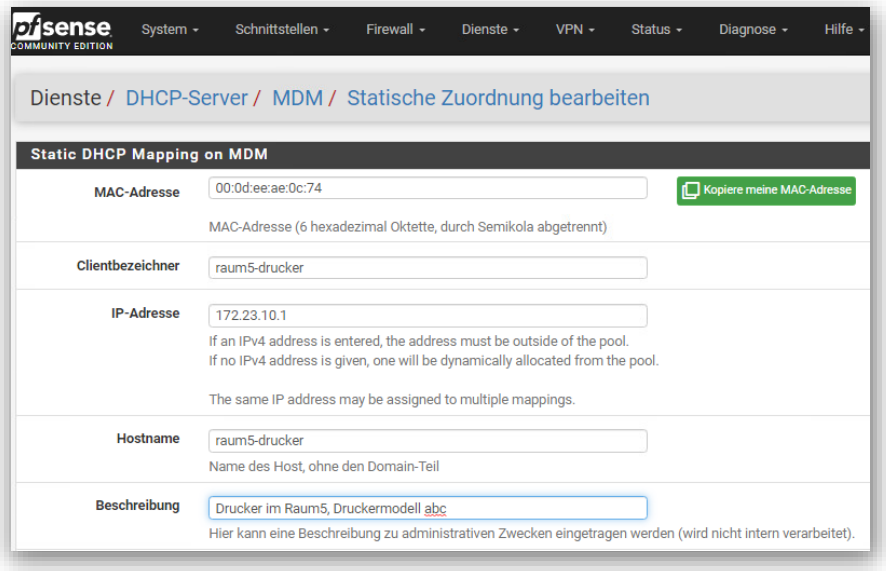
Um Druckern eine feste Adresse im MDM-Netz (oder auch einem anderen WLAN-Netz) zu geben, öffnen Sie die Oberfläche der Firewall (im Browser: firewall.paedml-linux.lokal oder firewall/ oder 10.1.0.1) und melden sich als Administrator an.

Öffnen Sie über „Dienste“ –> „DHCP-Server“ –> „MDM“ die Konfigurationsseite des DHCP-Dienstes.

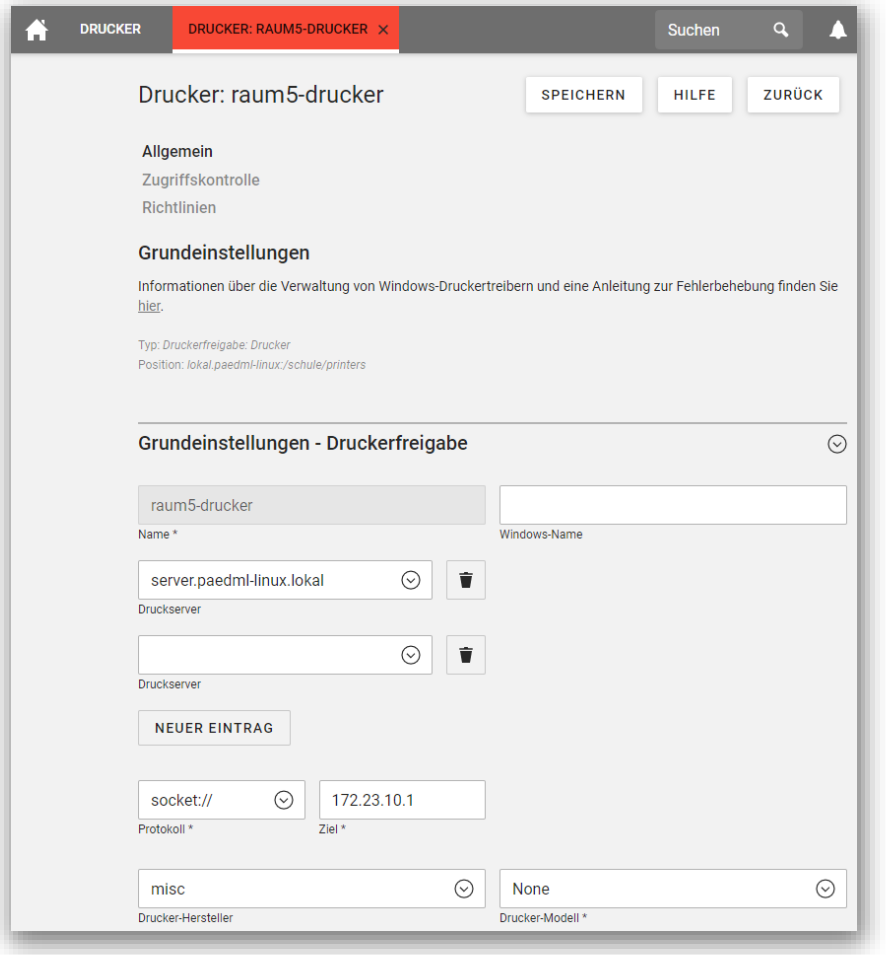


Auf dieser Seite können Sie nun ganz unten bei „DHCP statische Zuordnung für diese Schnittstelle“ auf „+ Hinzufügen“ klicken.

Tragen Sie die MAC-Adresse des Druckers ein und vergeben eine Adresse aus dem MDM-Adressbereich, z.B. 172.23.10.*, Hostname und Beschreibung sind optional.



Nun muss der Drucker noch unter seiner neuen Adresse dem Server bekannt gemacht werden. Auf der Schulkonsole unter „Geräte“ – „Drucker“ öffnen Sie den betreffenden Drucker und ändern Sie unter „Ziel *“ die IP-Adresse auf die neue Adresse des Druckers. Somit sollte der Drucker nun sowohl für iPads als auch für Computer erreichbar sein.



Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart