Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

# Unsupported HowTo

Radius-Server im WLAN konfigurieren

Stand 05.02.2018

## paedML® Linux

Version: 7.0

paedML L

lmz Landesmedienzentrum Baden-Württemberg

**Herausgeber**

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

70190 Stuttgart

**Autoren**

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

Johannes Albani

**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: 2018

# Inhaltsverzeichnis

# Vorwort

*RADIUS* ist ein Authentifizierungsprotokoll für Rechner in Computernetzen. Es wird in *UCS@school* für die Authentifizierung von Rechnern für den Wireless-LAN-Zugriff eingesetzt. Im Heimbereich wird normalerweise *„WPA-Personal“* als WLAN-Verschlüsselungsmethode verwendet. Die Verbindung zu diesem WLAN wird hergestellt, indem die SSID ausgewählt wird und ein vorher festgelegter einheitlicher WPA-Schlüssel eingetragen wird. Wird der Schlüssel verloren oder vergessen, muss ein neuer Schlüssel erzeugt werden und bei allen Geräten eingetragen werden.

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.

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.

| **Zielgruppe** | **Schwierigkeitsgrad** |
|---|---|
| Händler, Administratoren | mittel |

# 1. Installation des Radius-Servers

Überprüfen Sie, ob das Paket *„ucs-school-radius-802.1x“* installiert ist. Melden Sie sich dazu als *Administrator* an der Schulkonsole des Servers an und klicken Sie in der Kategorie *„Software“* auf *„Paket-Verwaltung“.*

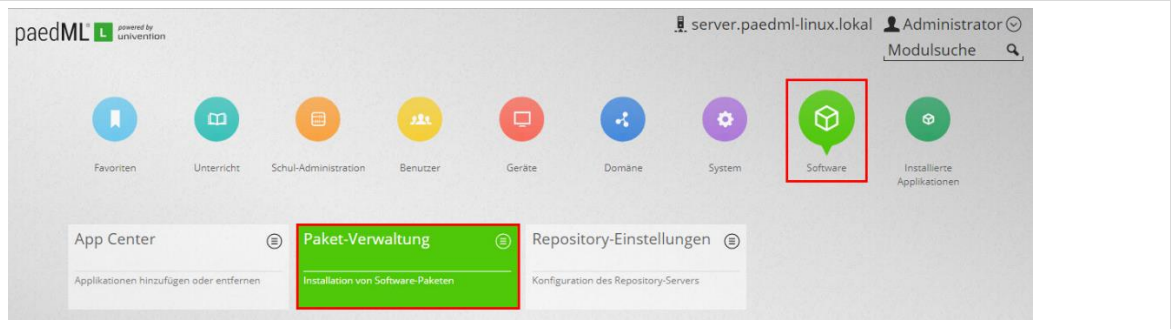


*Abb. 1: Aufrufen der Paketverwaltung*

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

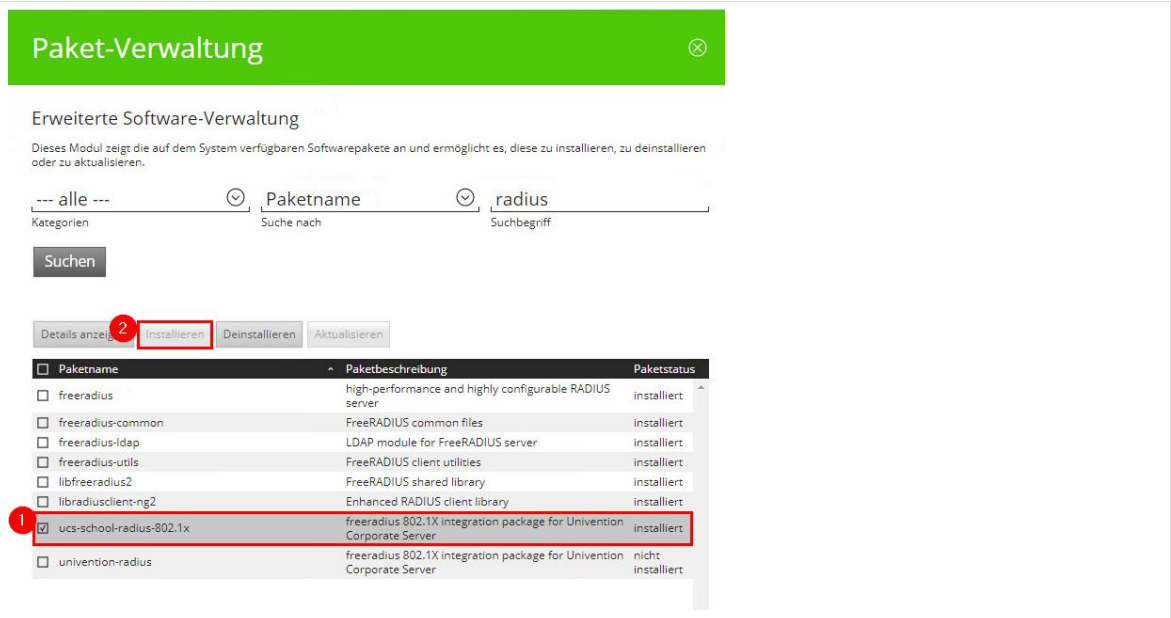


*Abb. 2: Aufrufen der Paketverwaltung*

# 2. Konfiguration des RADIUS-Servers

Die Integration der Access-Points geschieht über die Aufnahme der Geräte in der Schulkonsole (*„Geräte mit IP-Adresse“*). Dies wird im Administrationshandbuch im Kapitel *„Verwaltung von Geräten“* beschrieben.

Für den Aufbau eines sicheren Tunnels zwischen Schulserver und den Accesspoints wird ein *„Secret“ (Pre-Shared-Key)* zwischen dem RADIUS-Server und den Access Points ausgetauscht. Dazu wird in der Datei *„/etc/freeradius/clients.conf“* auf dem Server ein neuer Eintrag angehängt und das *„Secret“* für die Adresse/n der Accesspoints eingetragen:

```
client 10.200.22.0/24 {
secret = EinGeheimerSchluessel!
}
```

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 *„clients.conf“*-Datei des Servers entsprechen.

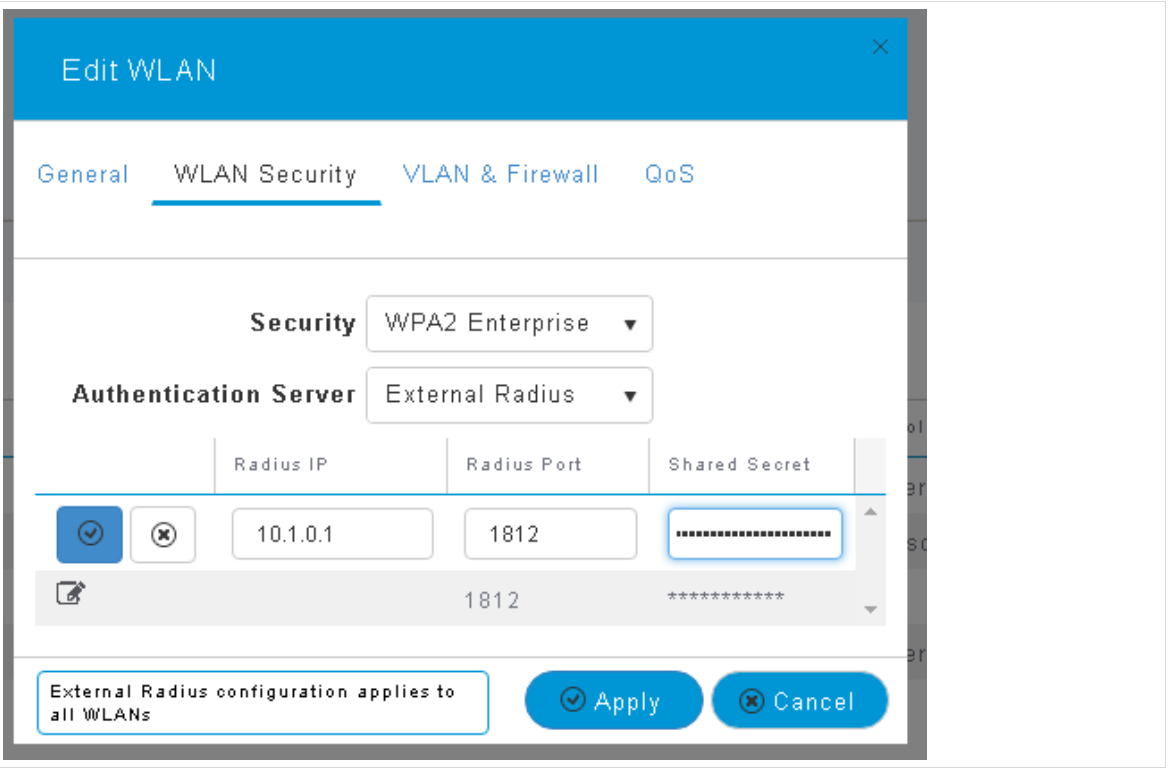


*Abb. 3: Radius-IP, Radius-Port und Shared-Secret im Accesspoint (Cisco AIR-AP1832I) eintragen*

## 3. WLAN Zugriff aktivieren

Damit der Radiusserver einen Benutzer authentifizieren kann, muss dieser zu einer Gruppe oder Klasse gehören. Dieser Gruppe muss eine Internetregel mit der Option *„WLAN-Authentifizierung aktiviert“* zugewiesen werden.

Weitere Informationen zu *„Gruppen“* in der *paedML Linux* finden Sie im Handbuch für Lehrkräfte in Kapitel 5.3. *„Informationen zu Internetregeln“* sind im Administratorhandbuch in Kapitel 16.1 und 16.2 zu finden.

In dem Beispiel unten wird zunächst eine Internetregel mit dem Namen *„Internet und WLAN Lehrer“* angelegt. Diese Funktion ist in der Schulkonsole, angemeldet als *„Administrator“* unter *„Schul-Administration“* zu finden. In *„Erweiterte Einstellungen“* muss die Option *„WLAN-Authentifizierung aktiviert“* ausgewählt werden.

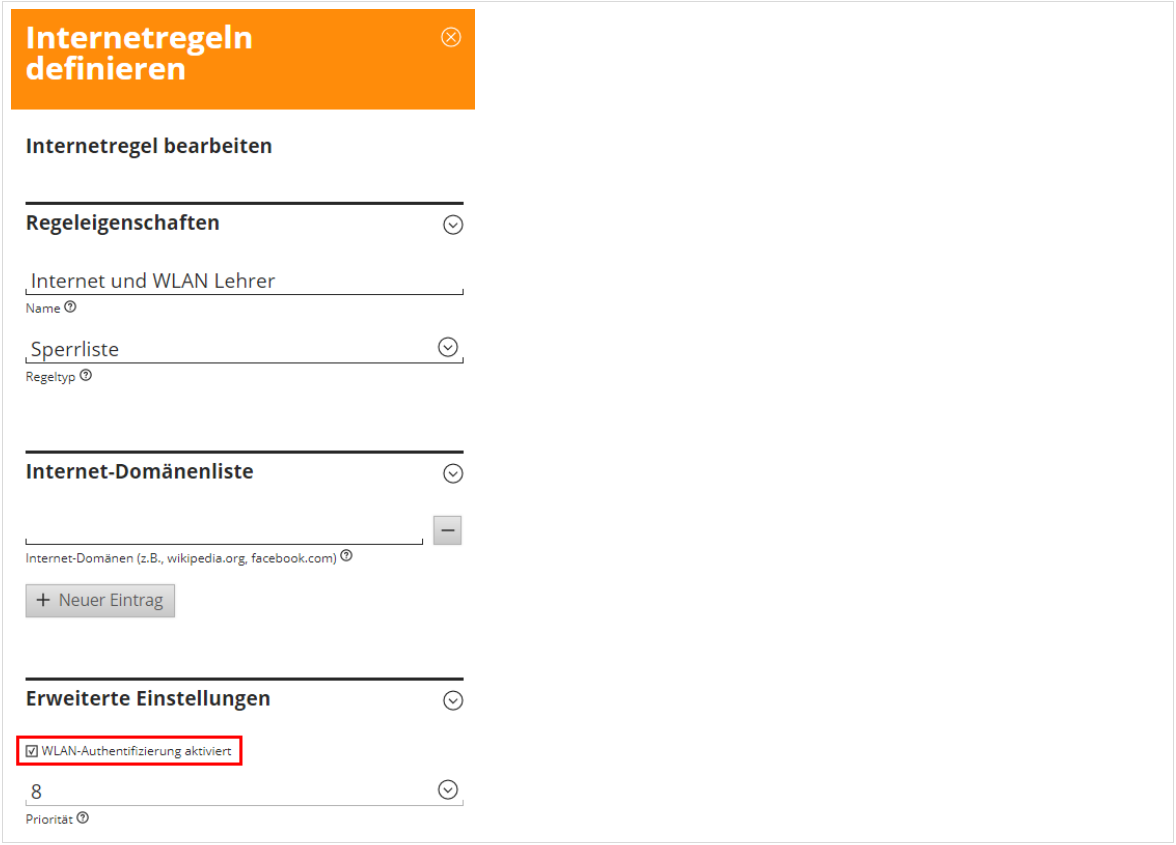


*Abb. 4: Internetregel definieren*

Dann muss die Internetregel der Gruppe zugewiesen werden, in diesem Beispiel der Gruppe *„Lehrer“*. *„Internetregeln zuweisen“* ist ebenfalls in der Kategorie *„Schul-Administration“* zu finden.

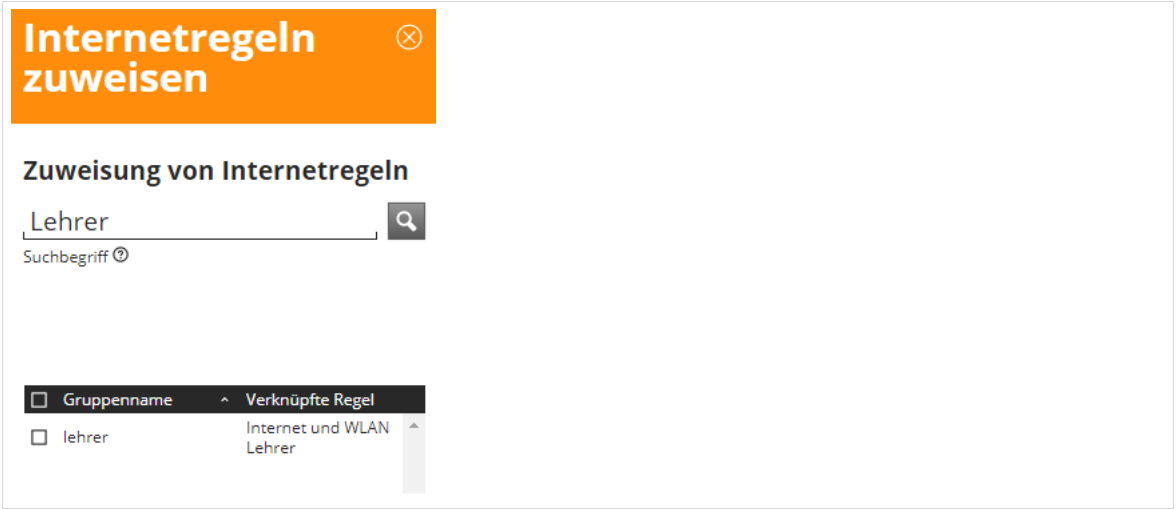


*Abb. 5: Internetregel zuweisen*

Für die Computerauthentifizierung muss jedes zu authentifizierende Gerät in einer Gruppe oder Klasse mit Internetregel *„WLAN Authentifizierung aktiviert“* befinden. In der Schulkonsole unter *Benutzer | Gruppen | Erweiterte Einstellungen | enthaltene Rechner* können Rechner einer Gruppe oder Klasse zugewiesen werden.

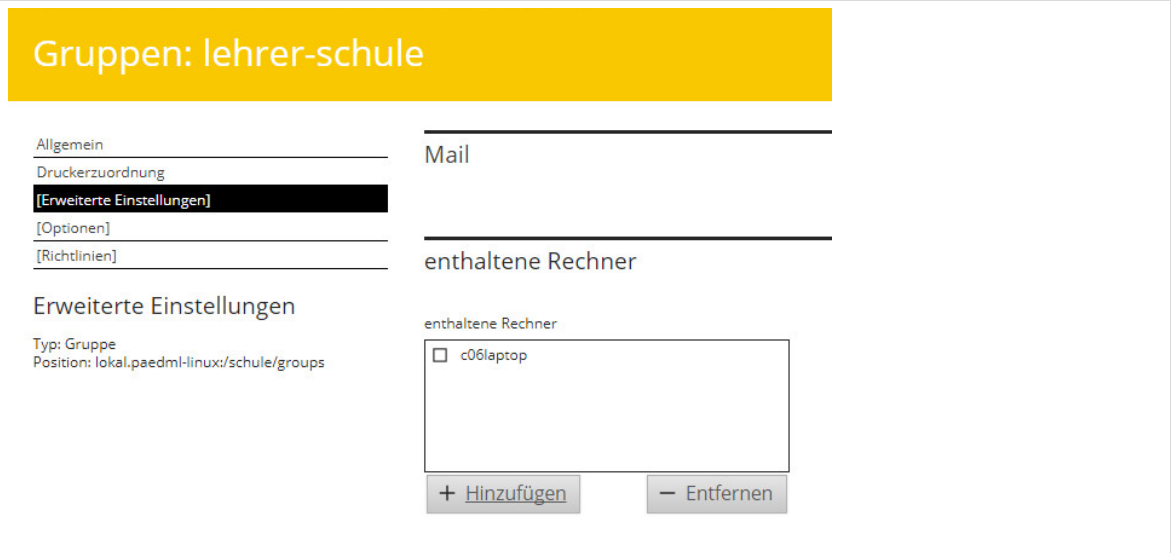


*Abb. 6: Rechner einer Gruppe zuweisen*

**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!

# 4. Funktionstest

Zum Testen der Installation legen Sie bitte einen neuen Benutzer, z.B. *„testbenutzer“* und einen Testcomputer, z.B. *„testcomputer“* an und legen ein Passwort fest. Bitte beachten Sie, dass dieses Passwort beim Testen im Klartext erscheint.

Der Benutzer *„testbenutzer“* kann in der Schulkonsole mithilfe der Funktion *„Benutzer (Schulen)“* angelegt werden.

Der Rechner *„testrechner“* kann in der Schulkonsole unter *„Rechner (Schulen)“* mit dem Namen *„testrechner“* und einer beliebigen MAC-Adresse, z.B. 75-18-5D-AD-67-6B, erstellt werden. Um die Authentifizierung zu testen, können Sie das Rechnerkennwort neu festlegen. Suchen die den Rechner unter *„Rechner (Schulen)“* und klicken Sie ihn an. Ein Klick auf Erweiterte Einstellungen bringt Sie in das LDAP-Verzeichnis für *„testrechner“.* Klicken Sie hier auf *„Erweiterte Einstellungen“*, dann auf *„Konto“,* um ein beliebiges Passwort festzulegen. Klicken Sie anschließend auf das Diskettensymbol zum Übernehmen des Passworts.

**Vorsicht: Der Server handelt mit jedem Rechner des Schulnetzes ein eigenes Passwort aus. Ein Zurücksetzen dieses Passworts ist für reale Rechner im Schulnetz nicht geeignet!**

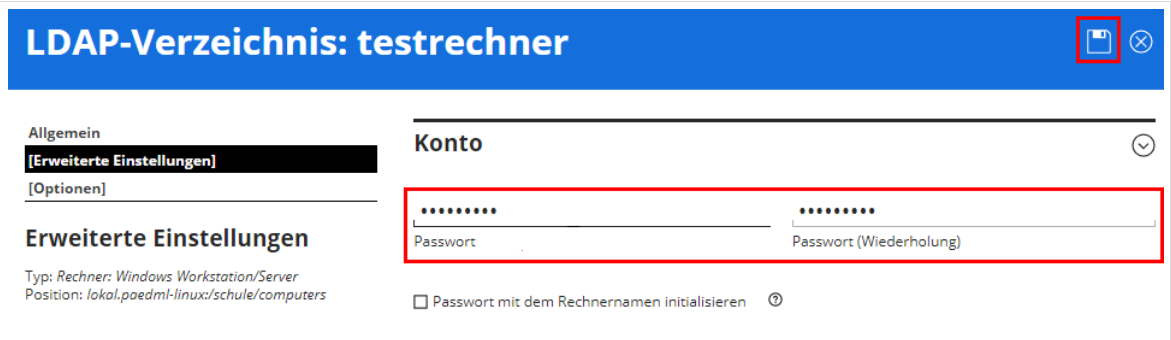


*Abb. 7: Passwort festlegen*

Nun müssen Sie *„testnutzer“* und *„testcomputer“* einer Gruppe mit einer Internetregel für WLAN zuordnen wie in Kapitel 3: *„WLAN Zugriff aktivieren“* ab Seite 6 beschrieben.

Um das Anmelden am Radiusserver zu testen verbinden Sie sich mit Putty auf den Server.

Stoppen Sie nun den Service Freeradius:

```
$ service freeradius stop
```

und starten Sie den Debug-Modus:

```
$ freeradius -X
```

Mit folgenden Befehlen auf der Kommandozeile können Sie nun die RADIUS-Konfiguration testen. Achten Sie darauf, dass Sie bei Rechnerkonten dem Namen immer ein „$“anhängen müssen. Das ist wichtig, um dem Server deutlich zu machen, dass es sich um ein Rechnerkonto handelt.

Reine LDAP-Authentifizierung:

```
$ radtest testbenutzer passwort localhost 10 testing123
$ radtest testrechner$ passwort localhost 10 testing123
```

Als Ausgabe muss eine Access-Accept-Antwort ausgegeben werden:

```
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=246,
length=20
```

Sollte es eine Access-Reject-Antwort geben, prüfen Sie bitte Benutzernamen und Passwort erneut:

```
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=129,
length=20
```

LDAP-Authentifizierung und Internetregelprüfung:

```
 $ radtest -t mschap testbenutzer passwort localhost 10 testing123
 $ radtest -t mschap testrechner$ passwort localhost 10 testing123
```

Als Ausgabe muss eine Access-Accept-Antwort ausgegeben werden:

```
 rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=198,
length=84
 MS-CHAP-MPPE-Keys =
0x000000000000000d5194e85da278bd6a55144941cbdc1f8000000000000000
 MS-MPPE-Encryption-Policy = 0x00000002
 MS-MPPE-Encryption-Types = 0x00000004
```

Internetregelprüfung schlägt fehl:

```
 rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=44,
length=38
 MS-CHAP-Error = "\000E=691 R=1"
```

Die zugewiesene Internetregel lässt kein WLAN zu (Checkbox WLAN-Aktivierung nicht ausgewählt).

# 5. Einrichtung des WLAN-Zugriffs an den Clients

Die Authentifizierung von Benutzern benötigt keine weiteren Arbeiten.

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

**Vorgehensweise für Windows 7 Clients:**
http://wiki.univention.de/index.php?title=Einrichtung_des_WLAN-Zugriffs_%C3%BCber_RADIUS_f%C3%BCr_Windows_7

# 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.

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

**70190 Stuttgart**