paedML® – stabil und zuverlässig vernetzen

Unsupported HowTo

Radius-Server im WLAN konfigurieren

Stand 03.06.2019

paedML® Linux

Version: 7.1

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, 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: 2019

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.

Darüber hinaus kann die Radius-Authentifizierung auch für 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.

Zielgruppe	**Schwierigkeitsgrad**
Händler, Administratoren	Mittel

ACHTUNG:

In der paedML Linux 7.1 wird Freeradius in der Version 3.0 eingesetzt. Die Konfigurationsdatei „clients.conf“ älterer Versionen (zum Beispiel aus der paedML Linux 7.0) kann nicht verwendet werden, da sich die Syntax verändert hat.

Eine automatisierte Migration der „clients.conf“ aus der paedML Linux 7.0 in die paedML Linux 7.1 beim Upgradevorgang findet daher nicht statt.

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“.*

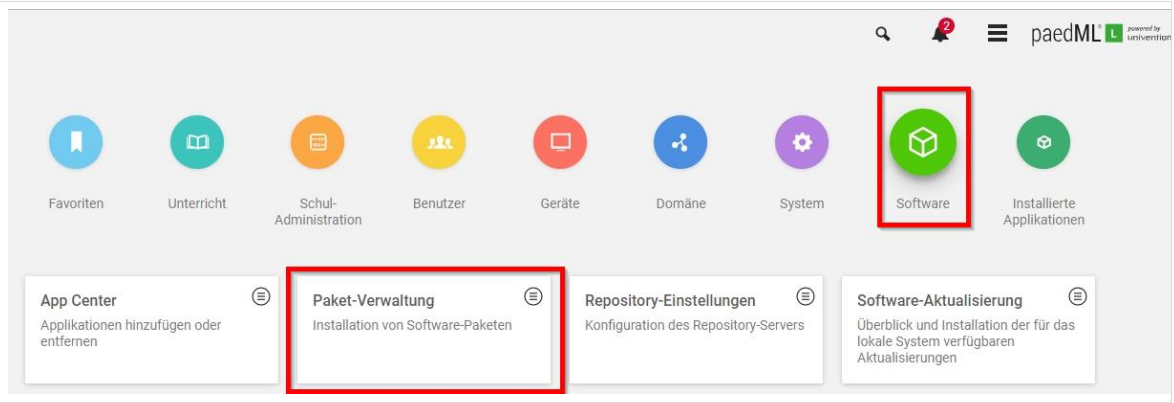

Abb. 1: Aufrufen der Paketverwaltung

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

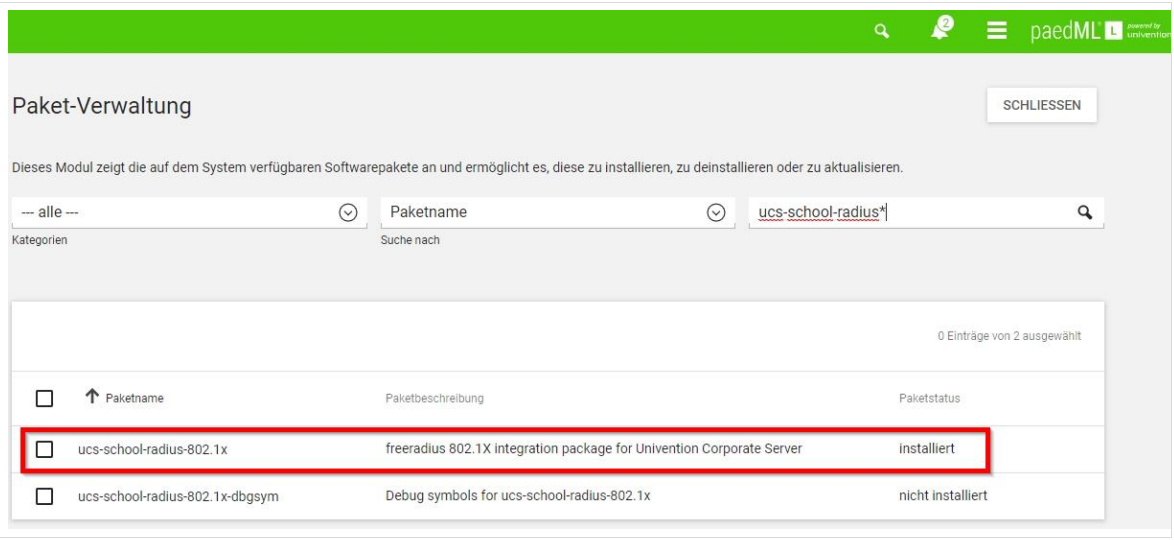

Abb. 2: Aufrufen der Paketverwaltung

2. Konfiguration des RADIUS-Servers

Die Integration der Access-Points in das pädagogische Netz geschieht über die Aufnahme der Geräte in der Schulkonsole *(„Geräte mit IP-Adresse“)*. Dies wird im Administrationshandbuch im Kapitel *„Verwaltung von Geräten“* beschrieben. Accesspoints können auch im Gästenetz betrieben werden. Beachten Sie diesbezüglich die konzeptionellen Hinweise und die Einrichtung von Accesspoints in der Anleitung „WLAN in der paedML Linux“:

http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux/howtos/wlan-in-der-paedmlr-linux-60.html

Das weitere Vorgehen wird anhand eines Access-Points im pädagogischen Netz beschrieben, der nach der Aufnahme in der Schulkonsole mit den folgenden Parametern erscheint:

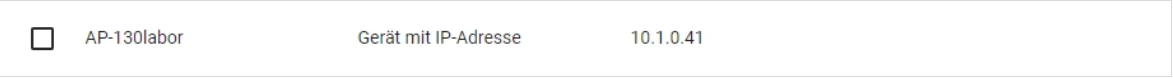

Abb. 3: AP in der Rechnerliste der Schulkonsole.

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/3.0/clients.conf“* auf dem Server ein neuer Eintrag angehängt und das *„Secret“* (hier *EinGeheimerSchluessel!*) für die Adresse/n der Accesspoints eingetragen:

```
#client example.org{
#<---->ipaddr<><---->=radius.example.org
#<---->secret<><---->=testing123
#}

client AP-130labor {
ipaddr=10.1.0.41/24
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.

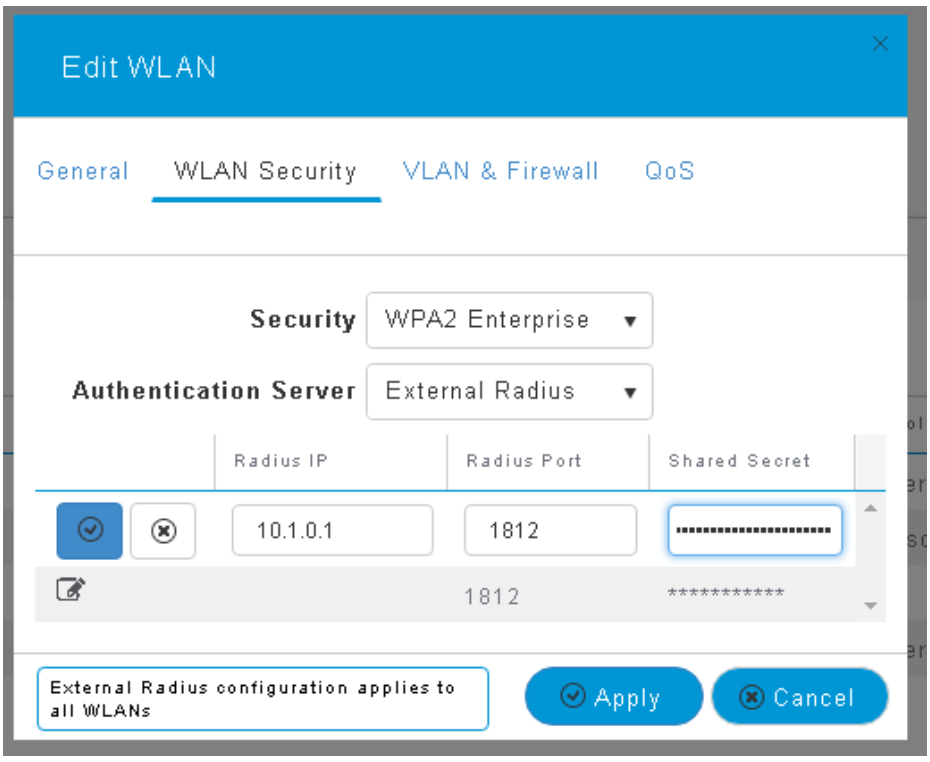

Abb. 4: Radius-IP, Radius-Port und Shared-Secret im Accesspoint (Cisco AIR-AP1832I) eintragen

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.

Im folgenden Beispiel wird zunächst eine Internetregel mit dem Namen *„Radius Test“* 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.

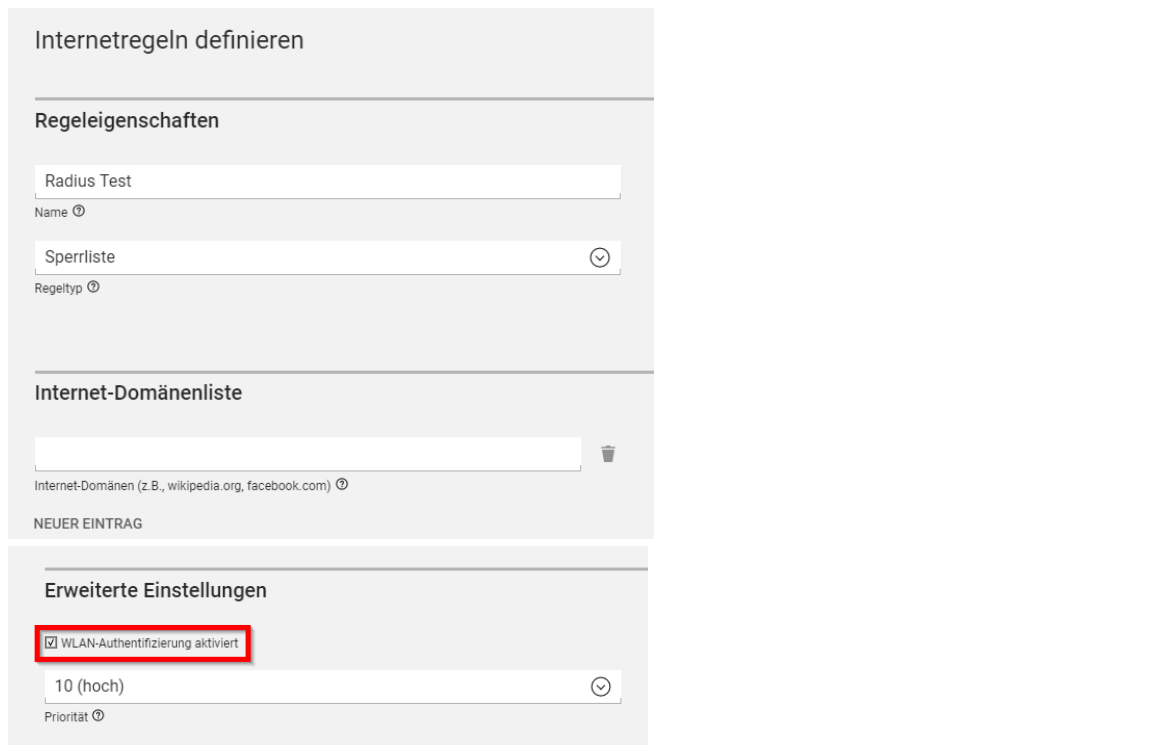

Abb. 5: Internetregel definieren

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.

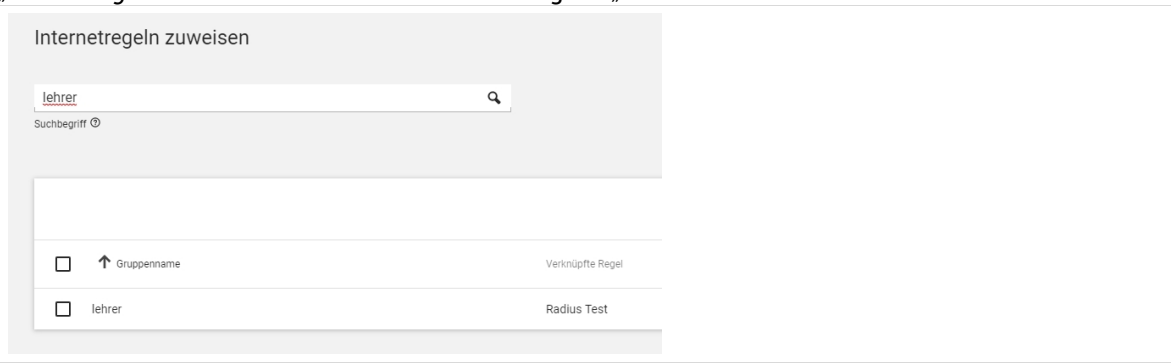

Abb. 6: Internetregel zuweisen

Für die Computerauthentifizierung muss sich 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.

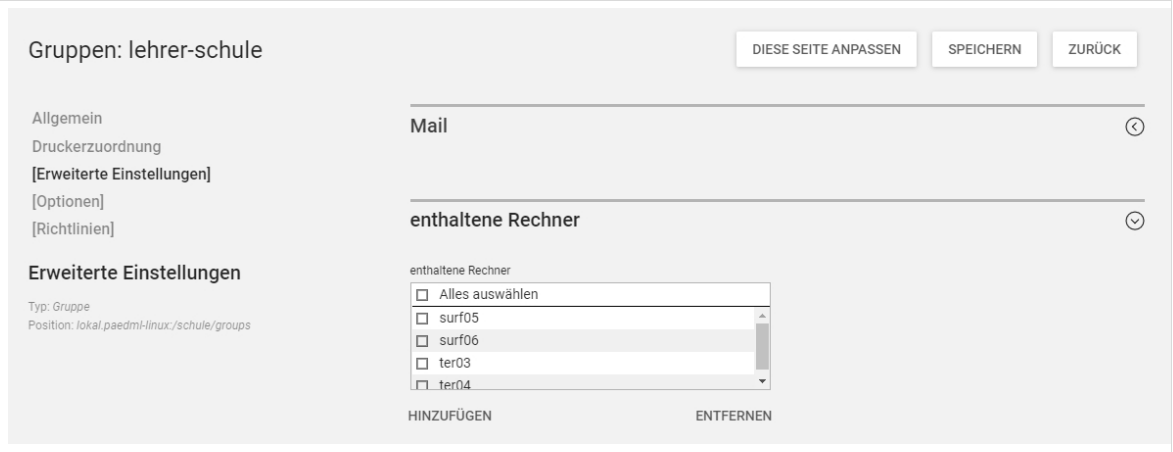

Abb. 7: Rechner einer Gruppe zuweisen

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. 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:
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

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

5. 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