Kapitel 10. Authentifizierung des WLAN-Zugriffs über RADIUS

RADIUS ist ein Authentifizierungsprotokoll für Rechner in Computernetzen. Es wird in UCS@school für die Authentifizierung von Rechnern für den Wireless-LAN-Zugriff eingesetzt.

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.

10.1. Installation und Konfiguration des RADIUS-Servers

Um RADIUS-Unterstützung einzurichten muss das Paket ucs-school-radius-802.1x auf dem Schulserver der Schule installiert werden, in der WLAN-Authentifizierung eingerichtet werden soll. Außerdem muss das Paket ucs-school-webproxy auf dem Schulserver installiert sein.

Nun müssen alle *Access Points* der Schule in der Konfigurationsdatei `/etc/freeradius/clients.conf` registriert werden. Pro *Access Point* sollte ein zufälliges Passwort erstellt werden. Dies kann z.B. mit dem Befehl `makepasswd` geschehen. Die Kurzbezeichnung ist frei wählbar. Ein Beispiel für einen solchen Eintrag für einen *Access Point*:

```
client 192.168.100.101 {
    secret = a9RPAeVG
    shortname = AP01
}
```

10.2. Konfiguration der *Access Points*

Nun müssen die *Access Points* konfiguriert werden. Die dafür nötigen Schritte unterscheiden sich je nach Hardwaremodell, prinzipiell müssen die folgenden vier Optionen konfiguriert werden:

- Der Authentifizierungmodus muss auf RADIUS-Authentifzierung umgestellt werden (diese Option wird oft auch als *WPA Enterprise* bezeichnet)
- Die IP-Adresse des Schulservers muss als RADIUS-Server angegeben werden
- Der Radius-Port ist 1812 (sofern kein abweichender Port in FreeRADIUS konfiguriert wurde)
- Das in der `/etc/freeradius/clients.conf` hinterlegte Passwort

10.3. Konfiguration der zugreifenden Clients

Der zugreifende Client muss zunächst das UCS-Wurzelzertifikat importieren. Es kann z.B. von der Startseite des Domänencontroller Master unter dem Link "Wurzelzertifikat" bezogen werden. Anschließend muss er eine Netzwerkverbindung mit den folgenden Parametern konfigurieren:

- Authentifizierung per WPA und TKIP als Verschlüsselungsverfahren
- `PEAP` und `MSCHAPv2` als Authentifizierungsprotokoll

Die Konfiguration unterscheidet sich je nach Betriebssystem des Clients. Im Univention Wiki findet sich eine exemplarische Schritt-für-Schritt-Anleitung für die Einrichtung unter Windows XP: http://wiki.univention.de/index.php?title=Einrichtung-WLAN-Authentifizierung-WinXP, sowie für die Einrichtung unter Windows 7: http://wiki.univention.de/index.php?title=Einrichtung-WLAN-Authentifizierung-Win7.

10.4. Freigabe des WLAN-Zugriffs in der Univention Management Console

In der Grundeinstellung ist der WLAN-Zugriff nicht zugelassen. Um einzelnen Benutzergruppen WLAN-Zugriff zu gestatten, muss in der Univention Management Console im Modul Internetregeln definieren eine Regel hinzugefügt - oder eine bestehende editiert werden -, in der die Option WLAN-Authentifizierung aktiviert aktiviert ist.

Weiterführende Dokumentation zur Freigabe des WLAN-Zugriffs finden sich in der UCS@school-Lehrerdokumentation [ucs-school-teacher].

10.5. 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`.