



paedML Die Musterlösung
Baden-Württemberg

Windows 2003 paedML[®] Windows 2.1 für schulische Netzwerke



**WLAN in der paedML[®] Windows
unter Nutzung der Radius-Technologie**

Installationsanleitung für

paedML[®] Windows 2.1 für Windows 2003 Server

Stand: 22.12.2011

Impressum

Herausgeber

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

Autoren

der Firma Raab OHG
www.raabonline.com

Dirk Reister,
Daniel Heinrich

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

Erstveröffentlichung: Tamer Berber (14.03.2008)
1. überarbeitete Version: Peter Klein (25.02.2009)
2. überarbeitete Version: Markus Maier (22.12.2011)

Endredaktion

Birgit Mikley

Weitere Informationen

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

Veröffentlicht: **2011**

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1.	Allgemeines zur Erweiterung „Radius-Server“	3
1.1.	Drahtloser Zugang für schulische und private Notebooks	3
1.1.1.	Funktionsweise: Radius-Server in der paedML Windows	3
1.2.	Private Notebooks im Schulnetz zulassen – Hinweis auf Virenschutz	5
1.3.	Hinweise zur Anleitung	5
1.3.1.	Mobiler Zugriff auf das Schulnetz	6
1.3.2.	Sicherheitsaspekte und eingesetzte Sicherheitsstandards	6
1.3.1.1.	Standards und Komponenten für die Zugriffskontrolle	6
1.3.2.1.	Standards für die Verschlüsselung	7
1.3.3.	Systemvoraussetzungen WLAN Clients	7
1.3.4.	Systemvoraussetzungen WLAN-Access-Points	8
2.	Installation	9
2.1.	Planung und Konzeption der WLAN-Zugriffspunkte	9
2.1.1.	Funkstandard 802.11b/g oder 802.11a?	9
2.1.2.	Hinweise zum „Ausleuchten“ von Räumlichkeiten	10
2.1.1.1.	Vorbereitungen treffen	10
2.1.2.1.	Messung vor Ort	10
2.2.	Access-Points einrichten und als Radius-Clients einbinden	11
2.2.1.	Allgemeine Hinweise zur Einrichtung der Access-Points	11
2.2.2.	Grundeinstellungen der Access-Points in Kürze	12
2.2.3.	Beispieleinrichtung anhand Access-Point D-Link DWL-2100AP	12
2.2.3.1.	Access-Point D-Link DWL-2100AP	12
2.3.	Installation von Zertifikatdiensten und IAS (RADIUS) auf S1	15
2.3.1.	Zertifikatdienste installieren	15
2.3.2.	IAS-Komponente installieren	18
2.4.	IAS konfigurieren	19
2.4.1.	Radius Clients eintragen	19
2.4.2.	RAS-Richtlinien anlegen	20
2.4.1.1.	Eine RAS-Richtlinie für alle Schul-Notebooks erstellen	21
2.4.2.1.	Notebooks der Schule per GPO als WLAN-Clients deklarieren	25
2.4.3.	RAS-Richtlinien für private WLAN-Clients	31
2.4.4.	RAS-Richtlinie für Benutzer, die mit privaten Clients auf das WLAN zugreifen dürfen	31
2.4.5.	RAS-Richtlinie mit additiver MAC-Adressenüberprüfung	32

3.	Links, Tools, Patches, weiterführende Informationen	37
3.1.	Microsoft Technet	37
3.2.	Literatur	37
3.3.	Tools für WLAN-Ausleuchtung	37
3.4.	Microsoft Updates für Windows XP – Client-PC's	38
3.5.	Microsoft Updates für Windows 2000 – Client-PC's	38

1.

Allgemeines zur Erweiterung „Radius-Server“

1.1.

Drahtloser Zugang für schulische und private Notebooks

Im Zusammenhang mit Notebook-Klassenzimmern erhalten Schulen oftmals WLAN-Lösungen, die nur die gelieferten Notebooks berücksichtigen, aber kein Gesamtkonzept für ein ganzes Schulnetzwerk einbeziehen. Für die flexible anderweitige Nutzung im Schulnetz sind sie also in der Regel nicht ausgelegt. Hierzu werden die Dienste von geeigneten Systemhäusern und Händlern benötigt. Leider kennen diese nicht immer die schulischen Anforderungen, da es vielen Schulen schwer fällt, ihre spezifischen Ansprüche anzugeben.

Durch die Erweiterung zum Radius-Server werden elementare, schulische Anforderungen abgedeckt. Das sind:

- Einfache Administration mit zentralen Konfigurationen
- Das „normale“ Netzwerk muss davon unbeeinflusst bleiben
- Skalierbarkeit: Weitere Zugriffspunkte („Access-Points“) hinzufügen, vorhandene Zugriffspunkte austauschen, Berechtigungen zentral und einfach steuern
- Nutzung möglichst hoher Sicherheitsstandards (Industriestandards)
- Nutzung von Bordmitteln, um Zusatzkosten zu sparen
- Support durch die zentrale Hotline
- ...

1.1.1.

Funktionsweise: Radius-Server in der paedML[®] Windows

Zu den Komponenten der Radius-Server-Lösung gehören:

- WLAN-Clients:
Zu den WLAN-Clients zählen schulische oder private Notebooks. Aber auch PDAs können auf diesem Weg Zugriff erhalten. Die Drahtlos-Netzwerkadapter dieser Geräte verfügen über die Unterstützung von IEEE802.1X und der WPA-Verschlüsselung.
- Access-Points:
Die Access-Points (-es kann auch nur einer sein-) müssen ebenfalls die Standards unterstützen, die für die WLAN-Clients gelten. Die Access-Points werden als „Radius-Clients“ auf dem Server registriert. Dies geschieht unter anderem über einen geheimen Schlüssel auf beiden Seiten (Access-Point und Radius-Server), durch den die gegenseitige Identifizierung gewährleistet ist.

- Radius-Server:

Nach der Installation der Komponente IAS (Internet Authentication Services) auf dem paedML-Server überprüft das Active-Directory die Anmeldeinformationen. In dieser Lösung wird die Zugriffsberechtigung über zwei zentrale Richtlinien gesteuert.

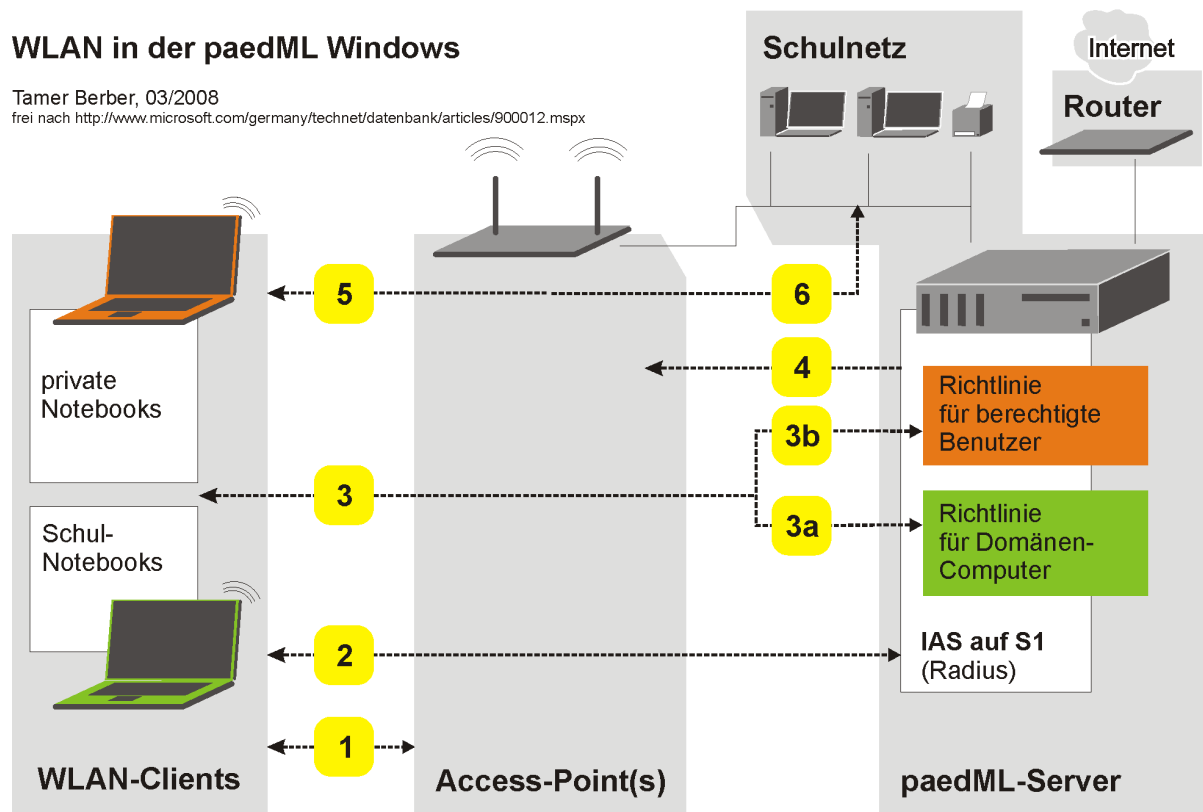
 - Richtlinie für Domänencomputer:

Jede Authentizität eines Domänencomputers berechtigt zum WLAN-Zugriff.
 - Richtlinie für berechtigte Benutzer:

Private Geräte benötigen eine Benutzer-Authentizität. Berechtigt für den Zugriff ist eine Gruppe, deren Mitglieder über die Schulkonsole verwaltet werden können.

- Schulnetz mit paedML-Server:

Werden die Zugriffsrichtlinien erfüllt, erhält der WLAN-Client vom DHCP-Server ein Lease (geliehene IP-Adresse), damit Zugriff ins Schulnetz und somit Zugriff auf entsprechende Speicherpfade, Drucker und Internet.



1. Der WLAN-Client befindet sich im Empfangsbereich eines Access-Points und versucht eine Verbindung zum Schulnetz herzustellen.
2. Der Access-Point leitet die Anfrage über einen eingeschränkten Kanal (Tunnel) an den Radius-Server weiter. Für diesen Tunnel wird ein Serverzertifikat benötigt, das zuvor auf dem Client installiert sein muss. Dieses Zertifikat kann von der (auf dem Server) installierten Zertifizierungsstelle heruntergeladen und auf den privaten Clients installiert werden. Schulische Clients erhalten das Zertifikat über eine GPO automatisch beim Hochfahren. Der Radius-Server prüft die Anmeldeinformationen gegen-

über dem Active-Directory.

3. War die Anmeldung/Authentifizierung erfolgreich, prüft der Radius-Server anhand der Anmeldeinformationen, ob die Bedingungen der Richtlinien erfüllt sind:

3a: Die Schul-Notebooks authentifizieren sich über ihr Computerkonto in der Schuldomäne. So erhält der WLAN-Client schon vor einer Benutzeranmeldung Verbindung zum Schulnetz. Nun kann sich jeder Benutzer des Schulnetzes anmelden.

3b: Bei privaten Notebooks verweigert die Richtlinie für Domänencomputer den Zugriff. Sie werden deshalb beim Verbindungsversuch nach Anmeldeinformationen gefragt. Gehört dieser Benutzer einer berechtigten Gruppe an, lässt die zweite Richtlinie für berechnigte Benutzer die Anfrage durch.

4. Der Radius-Server autorisiert den Access-Point, die Verbindung zuzulassen.
5. Der WLAN-Client stellt eine verschlüsselte Verbindung zum Schulnetz her.
6. In der Regel benötigt der WLAN-Client eine DHCP-Lease vom paedML-Server. Sobald diese IP-Adresse erteilt wurde, ist die Verbindungsprozedur abgeschlossen und der WLAN-Client kann auf die Netzwerkressourcen zugreifen.

1.2.

Private Notebooks im Schulnetz zulassen – Hinweis auf Virenschutz

Der Zugriff von privaten Notebooks ins Schulnetz birgt Sicherheitsrisiken. **Wir empfehlen Ihnen deswegen dringend, nur solchen Geräten den Zugriff zu gewähren, die einen aktuellen Virens Scanner installiert haben.** Benutzer, die mit ihren privaten Notebooks das Schulnetz nutzen möchten, sollten mindestens über eine Benutzerordnung darauf aufmerksam gemacht werden.

1.3.

Hinweise zur Anleitung

Diese Installationsanleitung wendet sich an Computerfachbetriebe und ggf. an erfahrene Netzwerkberater. Voraussetzung zur Installation sind fundierte Computerkenntnisse.

Die Anleitung beschreibt die Vorgehensweise für die Ein-Server-Lösung, das heißt, alle Schritte werden immer auf S1 ausgeführt. Die Installationsschritte für Zwei- und Drei-Server-Lösungen unterscheiden sich nicht.

1.3.1.

Mobiler Zugriff auf das Schulnetz

Mit der Einführung einer drahtlosen Zugangstechnik ins Schulnetz können flexibel mobile Endgeräte Zugang zu den gleichen Netzwerkdiensten wie kabelgebundene Desktop-Geräte erlangen. Das heißt:

- Zugriff auf Verzeichnisse und Dateien, auf die der Benutzer per NTFS berechtigt ist
- Internetzugang
- RDP-Session zu einem eventuell vorhandenen Terminalserver
- Zugriff auf die Schulkonsole

Hierbei ist eine besondere Absicherung des Funkzugangs erforderlich, um folgenden Missbrauch zu vermeiden:

- Nutzung der Infrastruktur durch Unbefugte
- Abhören der Kommunikation
- Manipulation der Kommunikation
- Beeinträchtigung der Verfügbarkeit

Herkömmliche WLAN- Absicherungsmechanismen bergen folgende Probleme:

- WEP-Verschlüsselung kann "geknackt" werden
- Sichere WPA oder WPA2-Verschlüsselung mit PSK (Pre-Shared-Key) sind durch statische Schlüsselvergabe auf den Clients unpraktisch im Schulalltag.

1.3.2.

Sicherheitsaspekte und eingesetzte Sicherheitsstandards

1.3.1.1.

Standards und Komponenten für die Zugriffskontrolle

Um Zugriff auf das Wireless LAN (WLAN) zu bekommen, muss zuvor eine passwortbasierte Authentifizierung erfolgen. Somit können sich nur im System (Schulkonsole / Active Directory) angelegte Benutzer oder Computerkonten nach korrekter Anmeldung in das WLAN einbuchten.

Hierfür werden folgende Komponenten eingesetzt:

- 802.1x (IEEE (Institute of Electrical and Electronic Engineers) Standard)
- PEAP (Protected Extensible Authentication Protocol)
- MS-CHAP V2

Dies erfordert eine RADIUS (Remote Authentication Dial-In User Service) -fähige WLAN-Infrastruktur:

- WLAN Clients mit mindestens WPA 802.1x-Unterstützung

- WLAN-Access-Points (AP), welche mind. WPA 802.1x unterstützen (meist alle aktuellen AP's unterstützen dies).
- RADIUS-Server zur Authentifizierung für die Access-Points/Clients
Hierfür wird die Windows 2003 Server (Standard) Komponente IAS (Internet Authentication Service) eingesetzt.
Hinweis: Der IAS des Windows 2003 Server Standard ist auf maximal 50 AP's (802.1x Clients) begrenzt.
- Zertifizierungsdienste zwischen WLAN-Client und IAS
Für die erforderliche CA (Certificate Authority) werden wiederum die Zertifikatdienste des Windows 2003 Server Standard verwendet.

1.3.2.1.

Standards für die Verschlüsselung

Als WLAN-Verschlüsselung wird WPA (WiFi Protected Access) eingesetzt. Abhörsicherheit ist hiermit im Gegensatz zu statischem WEP (Wired Equivalent Privacy) gewährleistet.

WPA2 ist nicht erforderlich und wird vorerst nicht empfohlen: Zum jetzigen Zeitpunkt ist es noch nicht möglich, per Gruppenrichtlinie von einem Windows 2003 SP2 Server die WPA2-WLAN Einstellungen für die Clients per Gruppenrichtlinie zu verteilen. Sie können jedoch WPA mit AES anstelle von WEP-TKIP (RC4) verwenden.

1.3.3.

Systemvoraussetzungen WLAN Clients

- WLAN-Karten:
Integrierter oder externer (USB, Cardbus/PCMCIA) WLAN-Adapter nach 802.11b, 802.11g oder 802.11a – Standard
WPA Unterstützung mit 802.1x
- Betriebssysteme
 - Windows XP mit Service Pack 3 (Seit Anfang 2008 verfügbar) oder
 - Service Pack 2 und zusätzlich 802.11i/WPA2 Unterstützung durch das Update für Windows XP SP2 (KB917021)
siehe Kapitel 3 „Links, Tools, Patches, weiterführende Informationen“
 - Windows 2000
Siehe „Using 802.1x authentication on client computers“
siehe Kapitel 3 „Links, Tools, Patches, weiterführende Informationen“: Sonstige WLAN-Clients mit WPA/802.1x/PEAP Unterstützung (PDA's, ...)

Sowohl Professional als auch Home-Versionen von Windows XP sind möglich. Bei den „Home“-Varianten muss auf automatische Konfiguration der WLAN-Einstellungen sowie auf automatisches Vertrauen des IAS-Zertifikats verzichtet werden.

1.3.4.

Systemvoraussetzungen WLAN-Access-Points

- Unterstützung Standard 802.11b/g (2,4GHz) oder zusätzlich 802.11a (5 GHz)
- Unterstützung von WPA erforderlich bzw. 802.11i
- Authentifizierungsmöglichkeit über RADIUS Server: 802.1x (meist alle aktuellen AP's unterstützen dies).

Empfehlung: Mit „günstigen“ Access-Points wurden zum Teil erhebliche Probleme festgestellt, da auch die aktuellen Firmware-Updates sich als fehlerhaft erwiesen. Wir raten Ihnen deswegen, die Wahl der Access-Points dem installierenden Unternehmen zu überlassen.

2. Installation

Verwenden Sie diese Installationsanleitung, um ein abgesichertes WLAN für die paedML 2.1 für Windows 2003 Server zu installieren.

Die Einrichtung erfolgt in folgenden Schritten:

- Planung und Konzeption der WLAN-Zugriffspunkte (Access Points)
- Installation von Zertifikatsdiensten
- Installation und Konfiguration von IAS (RADIUS-Komponente)
- Konfiguration der WLAN-Clients über Richtlinien oder manuell

Folgender Datenträger muss für die Installation von IAS und CA vorhanden sein:

- Installations-DVD *PAEDML_W2K3*
insbesondere: Windows 2003 Standard Edition mit integriertem SP2.

2.1. Planung und Konzeption der WLAN-Zugriffspunkte

2.1.1. Funkstandard 802.11b/g oder 802.11a?

Eine Frage der geplanten oder vorhandenen WLAN-Clients und Access-Points als Hilfe:

- Die meisten WLAN-Komponenten unterstützen entweder ein drahtloses Netzwerk im 2,4 GHz Frequenzband gemäß Standards 802.11b (bis 11 Mbps) oder zusätzlich 802.11g (bis 54 Mbps).
- Wenige WLAN-Komponenten unterstützen ausschließlich 802.11a (bis 54 Mbps), d.h. 5 GHz Frequenzband.
- Viele WLAN-Komponenten unterstützen auch beide, zueinander inkompatible Standards b/g und a.

Beachten Sie auch, dass oft spezielle Antennen benötigt werden, und auch diese je nach Standard für 2,4 oder 5 GHz (oder beides) ausgelegt sein müssen, z.B.:

- Gerichtete Antennen, um das Funkfeld in bestimmten Bereichen zu verbessern;
- Deckenantennen, um Access-Points in der Decke zu verstecken.
- ...

2.1.2.

Hinweise zum „Ausleuchten“ von Räumlichkeiten

2.1.1.1.

Vorbereitungen treffen

- Besorgen Sie sich einen Grundriss-Plan für das zu testende Gelände.
- Bereiten Sie den Test AP vor (am Besten vom selben Modell, das später verbaut werden soll):
Test IP, Kanäle und Verschlüsselung einrichten
- Bereiten Sie zwei Testnotebooks vor:
 - Vergeben Sie Test IPs auf WLAN und LAN-Schnittstelle (gleiches Netz wie AP)
 - Installieren Sie das Tool „netio“: Kostenloses Tool zum Messen der Übertragungsgeschwindigkeit; siehe auch Kapitel 3 „Links, Tools, Patches, weiterführende Informationen“
 - Installieren Sie das Tool „Network Stumbler“: Ebenfalls kostenloses Tool, mit dem Sie sich die WLAN-Signalstärke anzeigen lassen können (siehe Anhang).
- Mit Hilfe des Grundriss-Planes können Sie schon einmal im Vorfeld grob einplanen, wo und wie viele AP's nötig sind. Die genauen Plätze müssen Sie aber vor Ort abklären und austesten, da sie stark von baulichen Begebenheiten und möglichen Kabelwegen abhängen.
- Führen Sie einen Testlauf der Messung/Referenzmessung durch:
Die Ping und Netio-Messungen sind einmal mit und einmal ohne laufendem „Network Stumbler“ zu ermitteln. Bei Unterschieden müssen Sie die Messungen ohne „Network Stumbler“ durchführen. Dieser wird dann lediglich zum Begehen des Funkfeldes und zum Ermitteln der SNR-Werte (Signal-Rauschabstand) eingesetzt.

2.1.2.1.

Messung vor Ort

1. Deaktivieren Sie auf dem ersten Notebook die WLAN-Schnittstelle und verbinden Sie das Notebook über LAN mit dem AP.
2. Starten Sie auf dem ersten Notebook Netio im Servermodus („netio.exe -t -s“)
3. Schalten Sie das zweite Notebook an und verbinden Sie über WLAN mit dem AP.
4. Nun müssen Sie dauerhaft das erste Notebook anpingen (über *Verbindung + Stabilität*)
5. Starten Sie „Network Stumbler“ (über *Signalstärke | Werte und –Grafiken*)

Reichweite ermitteln

6. Stellen Sie den WLAN AP an eine der vorgeplanten Positionen
7. Lassen Sie anhand von „Network Stumbler“ (4.) Werte und Grafiken und Ping (5.) Grenzen und kritische Örtlichkeiten auslaufen.

Hauptmessung: Messpunkte im Reichweitenbereich (7.) erfassen

8. Starten Sie *Netio* im Clientmodus mit der IP des ersten Notebooks („netio.exe -t ip-notbook1“).Klicken Sie auf *effektiver Netzwerkdurchsatz*.

9. Nun notieren Sie pro Messpunkt im Grundriss-Plan
 - das Netio-Ergebnis,
 - die dazugehörige Signalstärke (vom „Network Stumbler“),
 - eventuelle Pingverluste während der Messung.

Weitere AP-Standorte

10. Wiederholen Sie 8. bis 9. für drei bis vier andere Punkte im Funkbereich, welche von diesem AP abgedeckt werden sollen. Es muss eine Verbindung von min. 1 MBit/s = 150 kByte/s für die Internetbenutzung möglich sein; für den Datentransfer wären mindestens 8 MBit/s = 1 MByte/s wünschenswert. Wenn nicht überall ausreichende Werte erreicht werden, muss der AP versetzt sowie die Messungen wiederholt oder ein weiterer AP-Standort eingeplant und vermessen werden.
11. Wiederholen Sie 6. bis 10. für alle AP's bis der Geländebereich ausreichend ausgeleuchtet ist.
12. Zum Schluss tragen Sie alle neuen bzw. überprüften Standorte der AP's in einen frischen Grundriss-Plan (für die Montage und Dokumentation) ein.

2.2.

Access-Points einrichten und als Radius-Clients einbinden

2.2.1.

Allgemeine Hinweise zur Einrichtung der Access-Points

- Sie sollten das Standard-Passwort des Access-Points ändern bzw. überhaupt erst einmal ein Passwort setzen.
- Die Zugriffskontrollliste (ACL = Access Control List) kann deaktiviert bleiben. Diese Maßnahme stellt kaum einen wirklichen Sicherheitsgewinn dar, da MAC-Adressen manipulierbar sind.
- Die SSID des Access-Points sollte keine Rückschlüsse auf verwendete Hardware, Einsatzzweck oder Einsatzort zulassen.
- Die Deaktivierung der SSID-Übermittlung (Broadcasting) empfehlen wir nicht, denn die SSID kann auch bei deaktiviertem Broadcasting mit einem Sniffer ausgelesen werden!
- Sie sollten regelmäßige Firmware-Aktualisierungen des Access-Points durchführen, um sicherheitsrelevante Verbesserungen zu erhalten. Bitte beachten Sie, dass ein Firmware Upgrade NICHT über die Funkverbindung ausgeführt werden sollte, da es bei Funkstörungen zu Beschädigungen und damit zum Ausfall des Produktes kommen kann. Firmware Upgrades sollten generell über eine verkabelte Netzwerkverbindung ausgeführt werden.
- Im Access-Point sollte, sofern vorhanden, die Fernkonfiguration über WLAN abgeschaltet werden.

2.2.2.

Grundeinstellungen der Access-Points in Kürze

Einstellung	Anmerkung	Werte
IP-Adressen Access-Points	Bereich 10.1.5.1 - 10.1.5.9 wird meist für Switches verwendet.	10.1.5.11 - 10.1.5.19
Funkkanal	Bei 802.11 b/g: Verwenden Sie bei benachbarten AP's keine überlappenden Funkkanäle. Bei 802.11a: Die Kanalwahl erfolgt automatisch.	1, 6 oder 11
SSID:	„Name“ der Funkzellen, - bei allen AP's gleich einzustellen	SCHULE
Authentifizierung und Verschlüsselung	Verschiedene Bezeichnungen – NICHT: „WPA-PSK“; meist „WPA-Enterprise“ oder „WPA-802.1x“	WPA-EAP ; 802.1x; RADIUS und AES
RADIUS	IP des RADIUS-Servers „Gemeinsamer geheimer Schlüssel“ zwischen AP's und IAS-Server, siehe <i>Seite 20</i>	10.1.1.1 _____

2.2.3.

Beispieleinrichtung anhand Access-Point D-Link DWL-2100AP

Im Auslieferungszustand sind Access-Points meist auf eine Adresse aus dem Bereich 192.168.x.x voreingestellt. Um diese Adresse ändern zu können, muss sich auch der Konfigurationsrechner temporär in diesem Adressbereich befinden.

Im Folgenden wird die Einrichtung an einem konkreten Access-Point beschrieben:

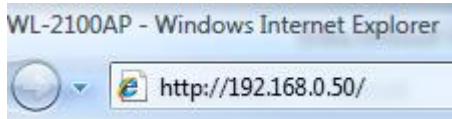
2.2.3.1.

Access-Point D-Link DWL-2100AP

(Firmware Version: v2.40de)

- Geben Sie auf dem Konfigurationsrechner die manuelle IP-Adresse ein: 192.168.0.123 Subnetzmaske 255.255.255.0

- Starten Sie den Webbrowser und stellen Sie eine Verbindung her mit IP: 192.168.0.50



- Benutzername = admin ; Kennwort leer



- Klicken Sie auf der linken Navigationsleiste auf *Drahtlos* und nehmen Sie folgende Einstellungen vor:



- Modus: *Access-Point*
- SSID: *SCHULE*
- Kanal: wie bei AP-Ausleuchtung vergeben (min 2-4 Kanäle Abstand)
Bei überlappenden Bereichen, bei automatischer Kanalwahl kann es zu Problemen mit einzelnen Notebooks kommen, die amerikanische WLAN-Karten-Treiber haben (US=Kanal 1-12, EU=Kanal 1-13). Das heißt, Sie wählen in diesem Fall entweder Kanal 1, 6 oder 11.
- Authentifizierung: *WPA-EAP*
- Cipher Type: *AES*
- Radius Server: *10.1.1.1 (S1)*
- RADIUS-Schlüssel: _____
Empfehlung: Benutzen Sie hier einen Passwortgenerator und vergeben Sie mind. >20 Zeichen (groß/klein/Zahlen)
- Zugriff über Funk: *EIN*
- Klicken Sie auf *Anwenden*. Der AP wird neu gestartet. Melden Sie sich neu am AP an.
- Gehen Sie auf die obere Navigationsleiste *Werkzeuge* und klicken Sie bei *Login* auf *neues Kennwort vergeben* („muster“).

Login	
Benutzername	<input type="text" value="admin"/>
Altes Kennwort	<input type="password"/>
Neues Kennwort	<input type="password" value="•••••"/>
Neues Kennwort bestätigen	<input type="password" value="•••••"/>

- Klicken Sie auf *Anwenden* und melden Sie sich mit neuem Kennwort am AP an.
- Gehen Sie auf die obere Navigationsleiste *Startseite* und klicken Sie auf der linken Navigationsleiste auf *LAN*.
- Vergeben Sie eine neue IP-Adresse im Bereich von 10.1.5.11 – 10.1.5.19
Vergeben Sie jeder AP eine andere IP;
Subnetzmaske: 255.255.0.0 ;
Gateway 10.1.1.1 (in der Mehr-Server-Lösung 10.1.1.2 bzw. 10.1.1.3)



The screenshot shows the configuration interface for a DWL-2100AP. On the left, there are three buttons: 'Assistent', 'Drahtlos', and 'LAN'. The 'LAN' button is highlighted in yellow. The main area shows the 'Startseite' (Home) tab selected, with sub-tabs for 'Erweitert', 'Werkzeuge', 'Status', and 'Hilfe'. Under 'LAN-Einstellungen', the following settings are visible:

IP-Zuweisung	Statisch (Manuell)
IP-Adresse	10.1.5.11
Subnetzmaske	255.255.0.0
Standard-Gateway	10.1.1.1

At the bottom right, there are three status icons: a green checkmark, a red X, and a red plus sign, with the labels 'Anwenden', 'Abbrechen', and 'Hilfe' respectively.

Klicken Sie auf *Anwenden* | *AP startet neu* | *AP an seinen benötigten Platz anbringen und ans Netz anschließen*.

- Gehen Sie genauso bei allen anderen AP's vor, nur jeweils mit einer anderen IP-Adresse.
Konfigurieren Sie weitere AP's.

2.3.

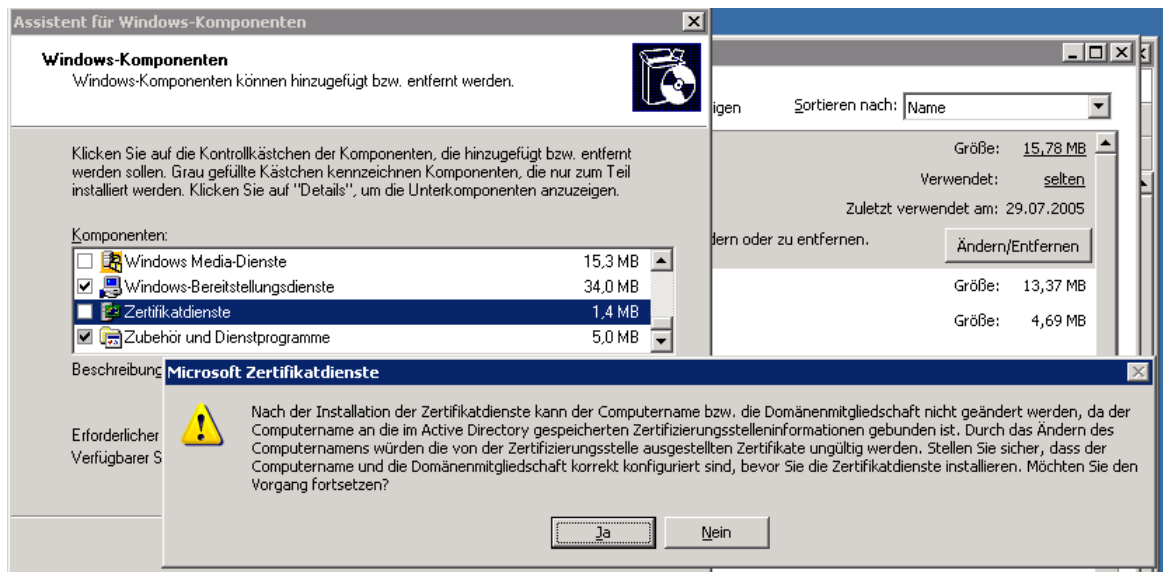
Installation von Zertifikatdiensten und IAS (RADIUS) auf S1

Sämtliche Installationsschritte werden auf S1 durchgeführt.

2.3.1.

Zertifikatdienste installieren

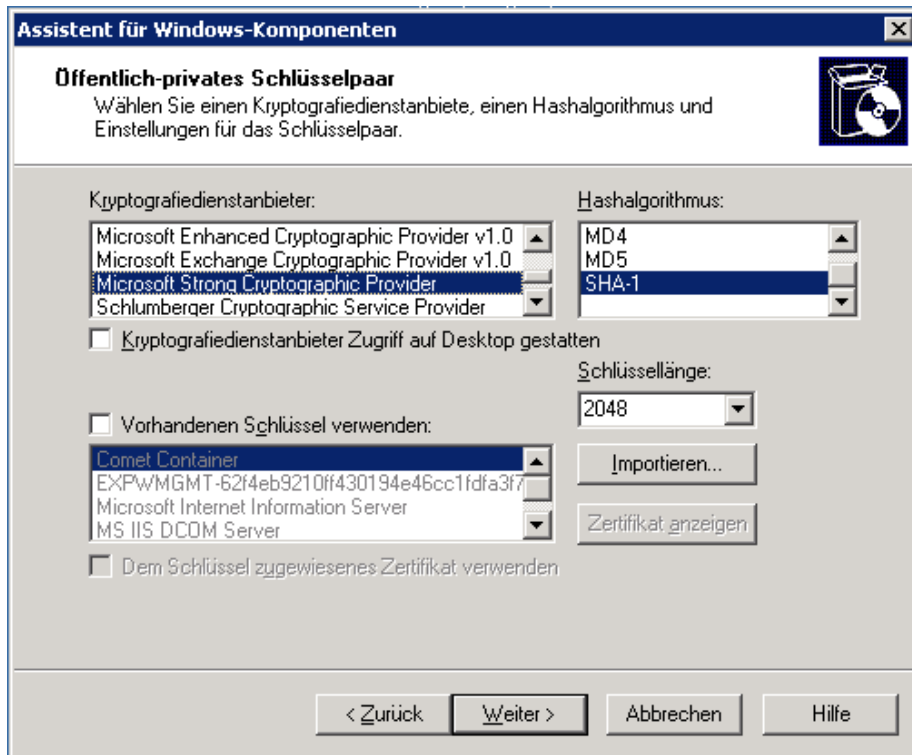
- Gehen Sie auf *Systemsteuerung | Software | Windows-Komponenten | Zertifikatdienste*



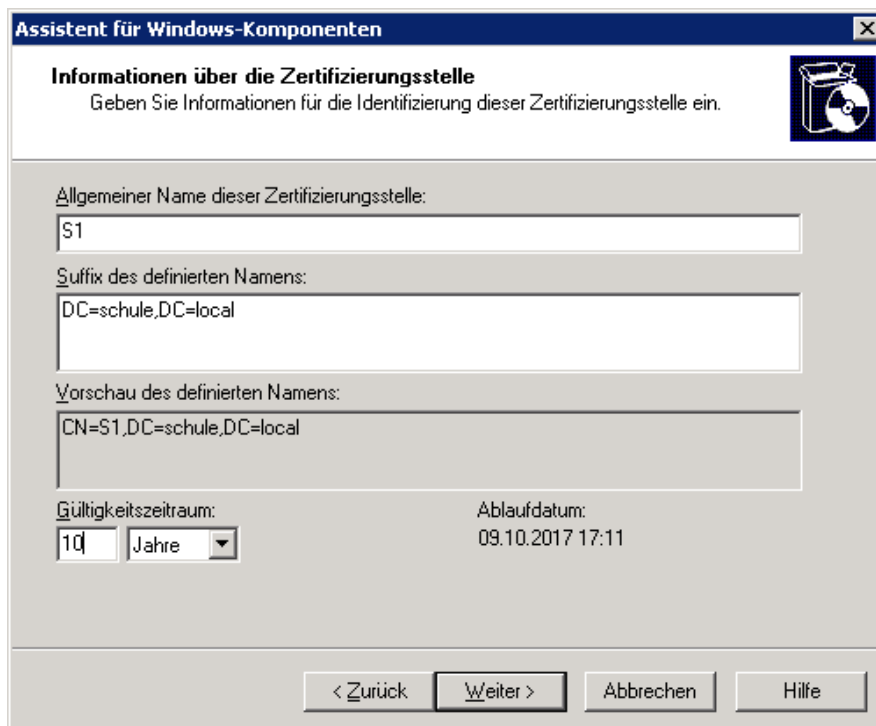
- Setzen Sie den Haken bei „Schlüsselpaar und ein Zertifizierungsstellenzertifikat ... erstellen“ und klicken Sie dann auf *Weiter*.



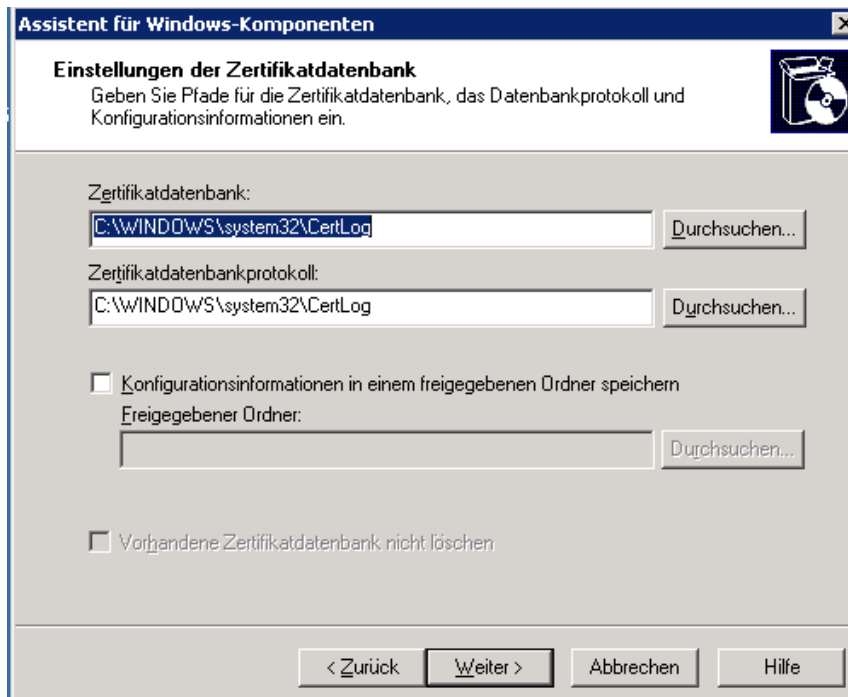
- Übernehmen Sie die Einstellungen und klicken Sie auf *Weiter...*



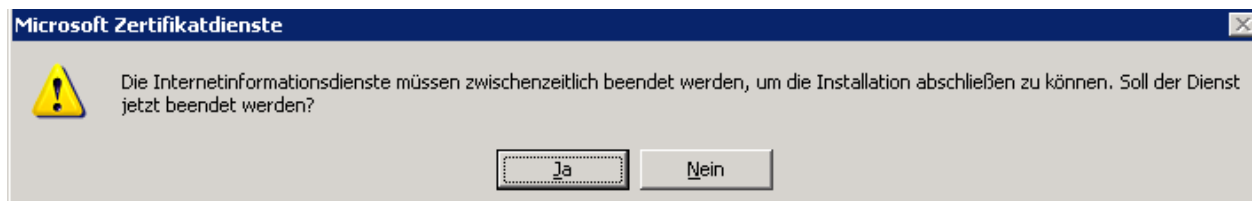
- Erhöhen Sie den Gültigkeitszeitraum auf *10 Jahre* und klicken Sie auf *Weiter...*



- Klicken Sie *Weiter...*

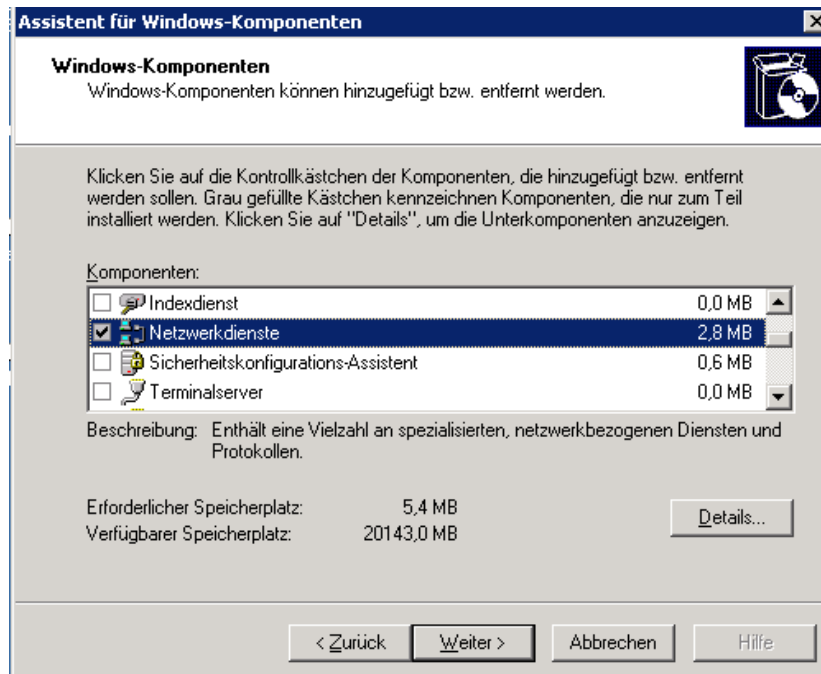


- Bestätigen Sie mit *Ja*.

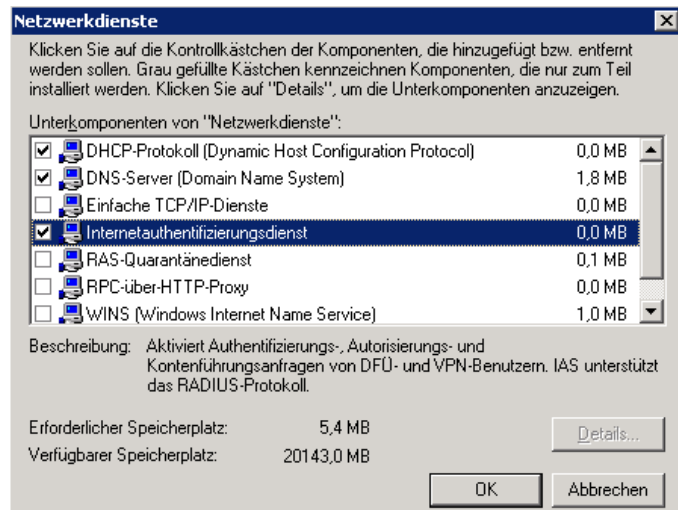


2.3.2. IAS-Komponente installieren

- Gehen Sie auf *Netzwerkdienste | Internetauthentifizierungsdienst*



- Gehen Sie mit Doppelklick auf *Netzwerkdienste*



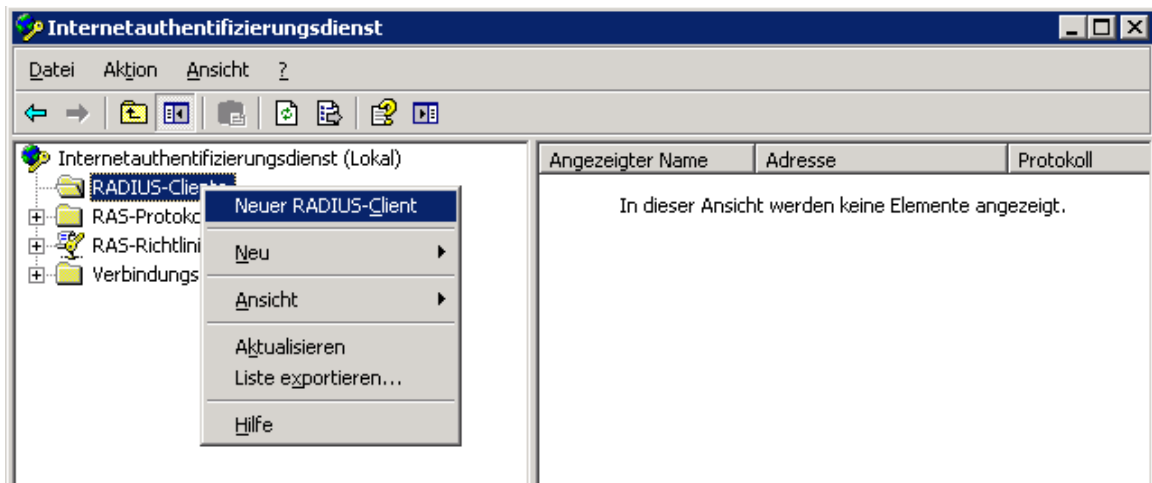
Bestätigen Sie mit *OK*, *Weiter* und *Fertigstellen*.

- Starten Sie den Server neu!

2.4. IAS konfigurieren

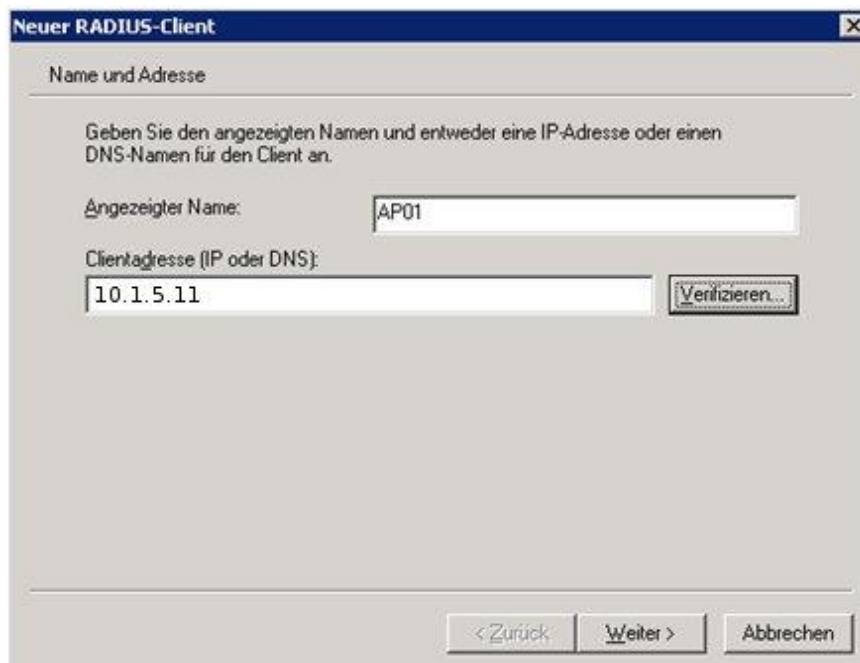
2.4.1. Radius Clients eintragen

- Starten Sie auf S1 *Internetauthentifizierungsdienst Konsole* (über *Start | Programme | Verwaltung | Internetauthentifizierungsdienst*).



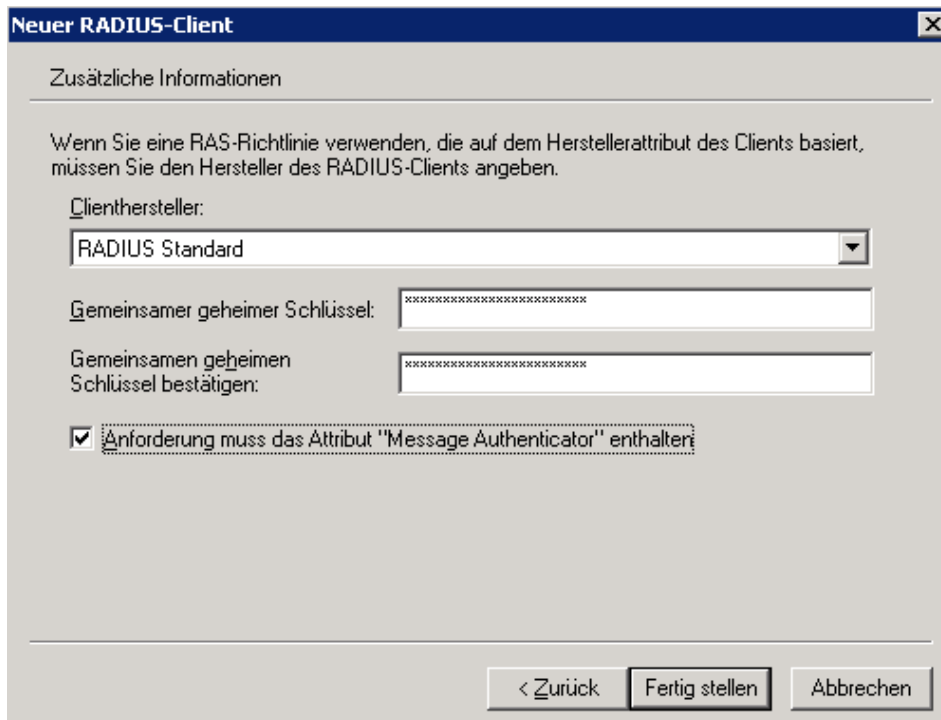
Gehen Sie auf *RADIUS-Clients | neuer Radius-Client*.

- Geben Sie dem AP (APxx) einen Namen und tragen Sie die zugehörige IP-Adresse ein.



Bestätigen Sie mit *Weiter*.

- Unter *Neuer RADIUS-Client* tragen Sie zusätzliche Informationen ein:



- Clienthersteller: *RADIUS Standard*
 - Gemeinsamer geheimer Schlüssel: siehe Kapitel "Access-Points einrichten und als Radius-Clients einbinden" (Seite 11)
 - Aktivieren Sie *Message Authenticator*
- Wiederholen Sie den Vorgang für die anderen Access-Points.

2.4.2. RAS-Richtlinien anlegen

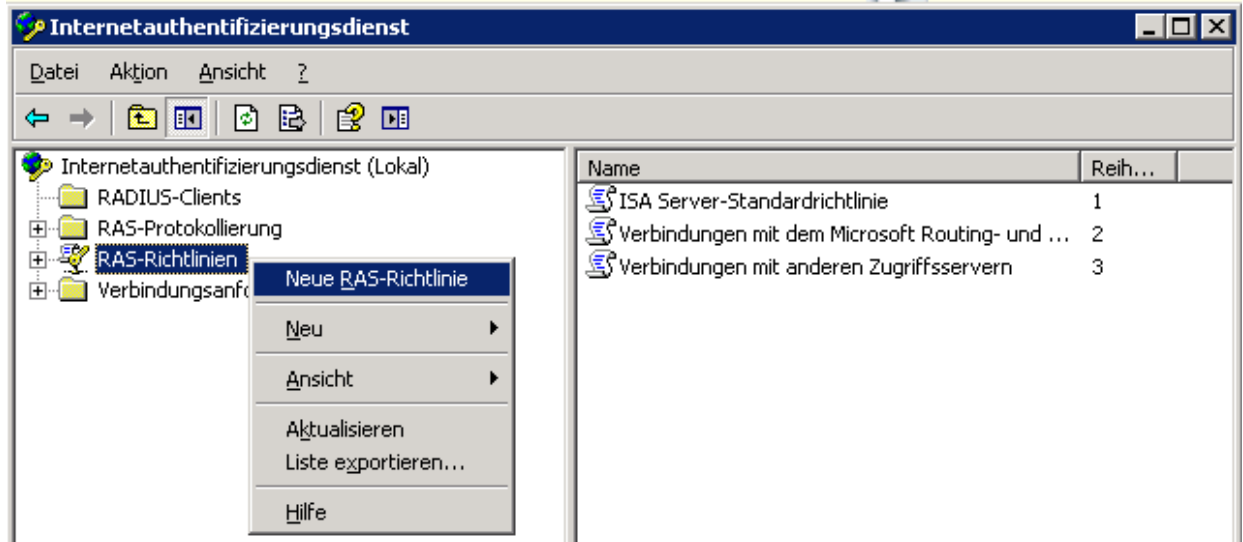
Die RAS-Richtlinien regeln den Zugriff auf die WLAN-Zugriffspunkte. Diese Konzeption sieht folgende Regeln vor:

- **Für den WLAN-Zugriff aller Schul-Notebooks:**
Erlaubt allen Domänen-Computern den WLAN-Zugriff. Das benötigte Zertifikat wird per GPO vorgegeben. Weitere Sicherheitsüberprüfungen (MAC-Adressen-Prüfung, Benutzerauthentifizierung, ...) sind nicht nötig.
- **Für WLAN-Zugriff privater Notebooks:**
Da die Hardware im Netz nicht bekannt ist, wird der Zugriff über eine Gruppenmitgliedschaft geregelt. Das heißt, die berechtigten Benutzer müssen Mitglied einer eingestellten Gruppe sein. Das zusätzlich benötigte Zertifikat können sich die Benutzer von einem beliebigen Client im Schulnetz auf einen USB-Stick speichern. Optional können Sie hierbei auch additiv die MAC-Adresse jedes einzelnen privaten Notebooks überprüfen.

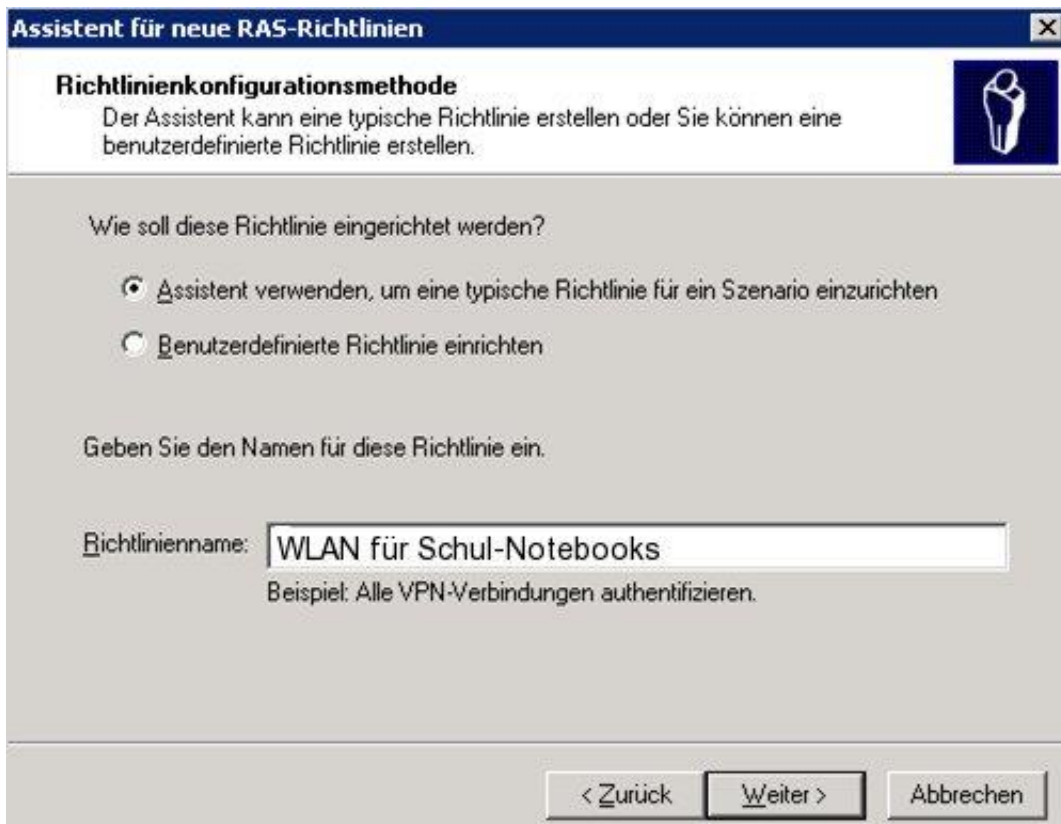
2.4.1.1.

Eine RAS-Richtlinie für alle Schul-Notebooks erstellen

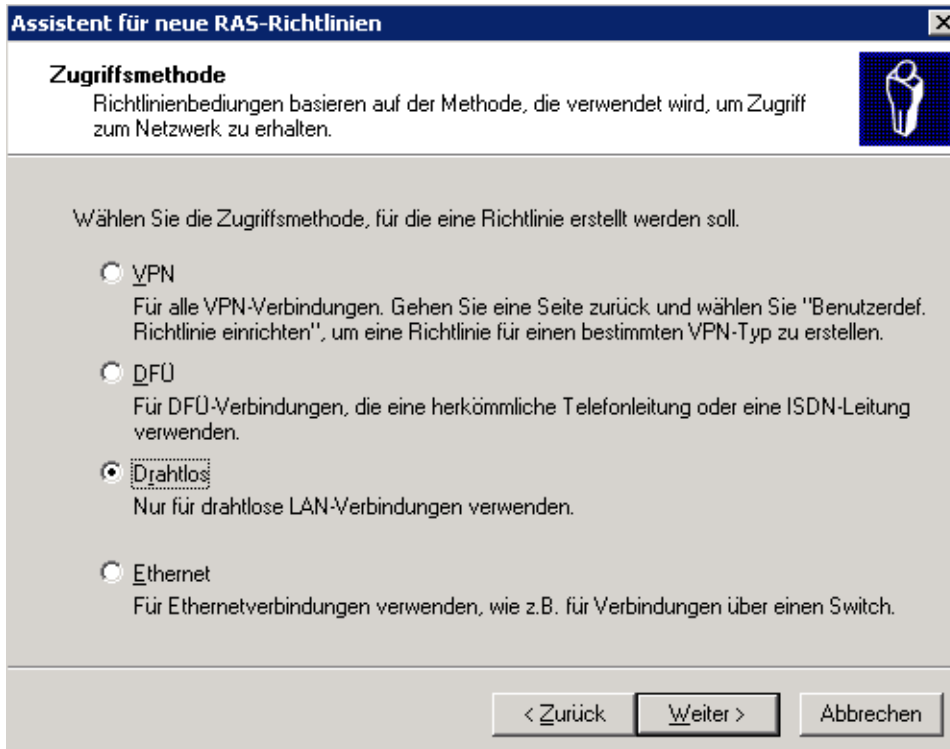
1. Gehen Sie über Internetauthentifizierungsdienst *Console* | *RAS-Richtlinie* | *Neue RAS-Richtlinie*.



2. Aktivieren Sie den Assistenten (wie angezeigt) und vergeben Sie einen Richtliniennamen (z.B. WLAN für Schul-Notebooks)



3. Bei *Zugriffsmethode* aktivieren Sie „Drahtlos“.



Assistent für neue RAS-Richtlinien

Zugriffsmethode
Richtlinienbedingungen basieren auf der Methode, die verwendet wird, um Zugriff zum Netzwerk zu erhalten.

Wählen Sie die Zugriffsmethode, für die eine Richtlinie erstellt werden soll.

VPN
Für alle VPN-Verbindungen. Gehen Sie eine Seite zurück und wählen Sie "Benutzerdef. Richtlinie einrichten", um eine Richtlinie für einen bestimmten VPN-Typ zu erstellen.

DFU
Für DFU-Verbindungen, die eine herkömmliche Telefonleitung oder eine ISDN-Leitung verwenden.

Drahtlos
Nur für drahtlose LAN-Verbindungen verwenden.

Ethernet
Für Ethernetverbindungen verwenden, wie z.B. für Verbindungen über einen Switch.

< Zurück Weiter > Abbrechen

4. Bei *Zugriff gewähren, basierend auf:* wählen Sie „Gruppen“ aus und fügen *Domänencomputer* hinzu.



Assistent für neue RAS-Richtlinien

Benutzer- oder Gruppenzugriff
Sie können individuellen Benutzern oder ausgewählten Gruppen Zugriff gestatten.

Zugriff gewähren, basierend auf:

Benutzern
Benutzerzugriffsberechtigungen werden in dem Benutzerkonto spezifiziert.

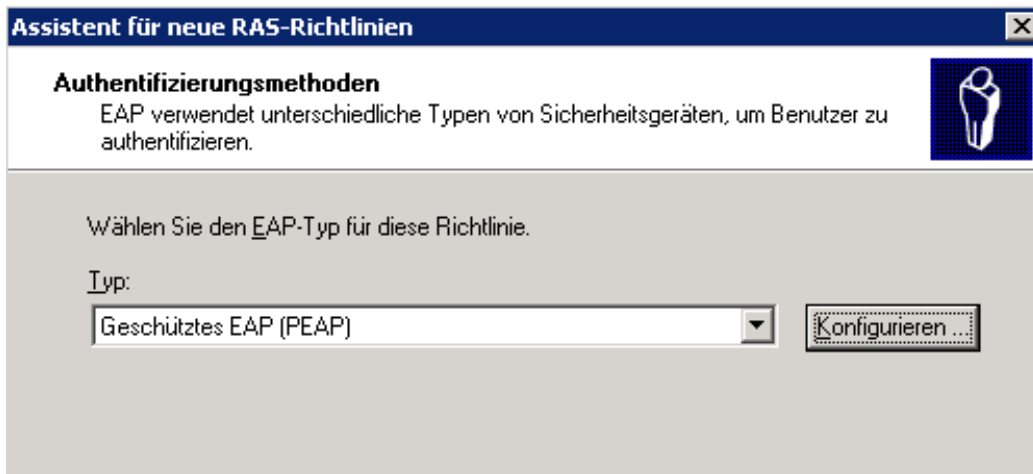
Gruppen
Individuelle Benutzerberechtigungen setzen Gruppenberechtigungen außer Kraft.

Gruppenname:
SCHULE\Domänencomputer

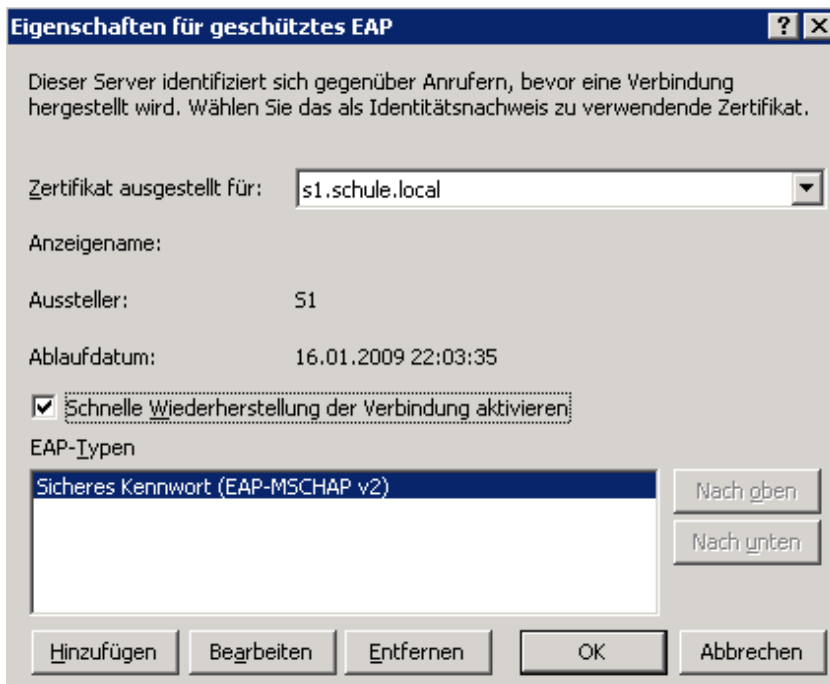
Hinzufügen...
Entfernen

< Zurück Weiter > Abbrechen

5. Geben Sie Geschütztes EAP (PEAP) ein und klicken Sie auf *Konfigurieren*.

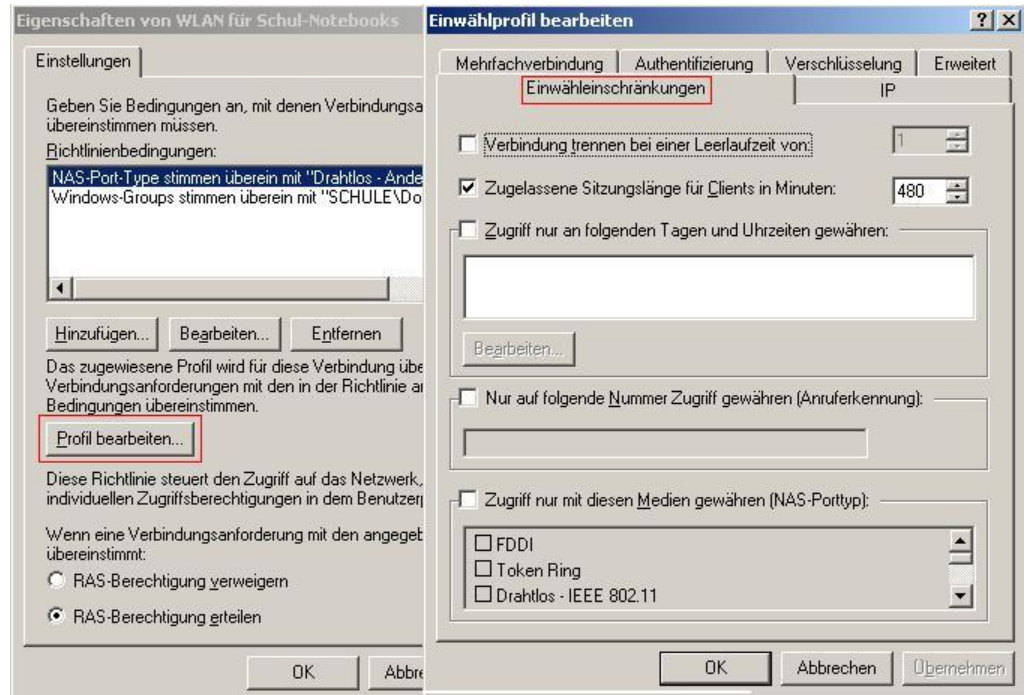


6. Setzen Sie den Haken bei „Schnelle Wiederherstellung der Verbindung aktivieren“ und klicken Sie dann auf *OK*.

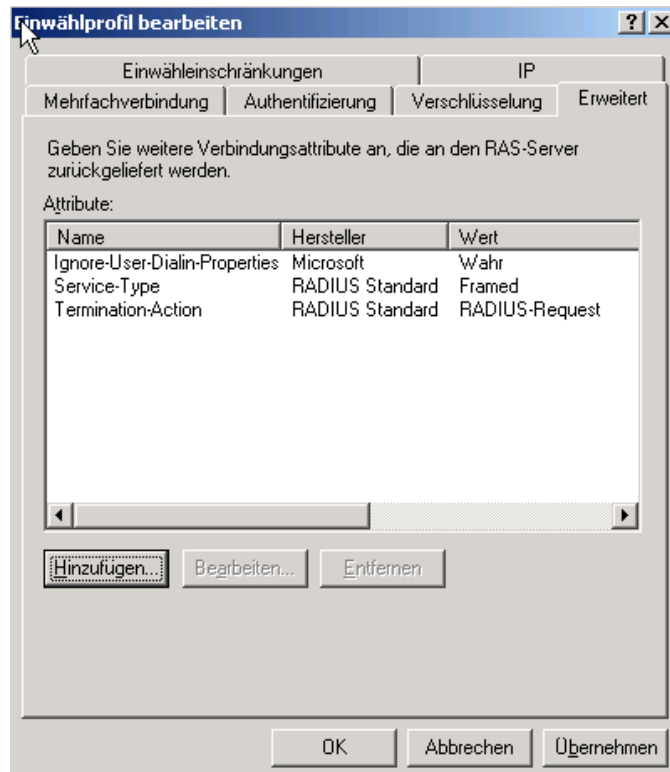


7. Klicken Sie auf *Fertigstellen*.
8. Nun müssen in der eben erstellten RAS-Richtlinie noch einige Änderungen vorgenommen werden. Klicken Sie hierzu im rechten Fenster mit der rechten Maustaste auf die Richtlinie „WLAN für Schulnotebooks“ und wählen Sie Eigenschaften. Im Eigenschaftsfenster der Richtlinie „WLAN für Schulnotebooks“ klicken Sie bitte auf den Button *Profil bearbeiten* und wählen anschließend die Registerkarte „Einwahlbeschränkungen“ aus:

- Setzen Sie den Haken bei „Zugelassene Sitzungslänge für Clients in Minuten“ und wählen Sie 480



- Wechseln Sie in das Register *Erweitert* und klicken Sie auf *Hinzufügen*.



Ignore-User-Dialin-Properties	Wahr
Service-Type	Framed
Termination-Action	Radius-Request

2.4.2.1.

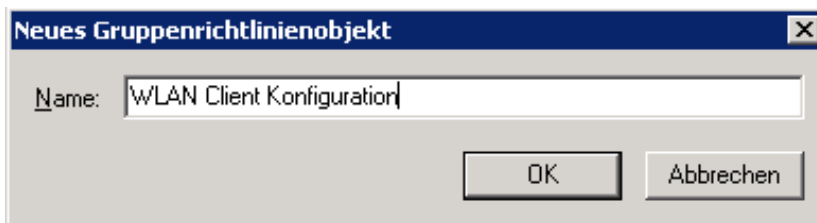
Notebooks der Schule per GPO als WLAN-Clients deklarieren

Die *WLAN-Konfiguration* der Notebooks erfolgt über *Gruppenrichtlinien* (eine neue GPO) im Active Directory derzeit nur für Windows XP Professional SP2 (Regelfall für schuleigene Notebooks).

Automatische Konfiguration über Gruppenrichtlinien

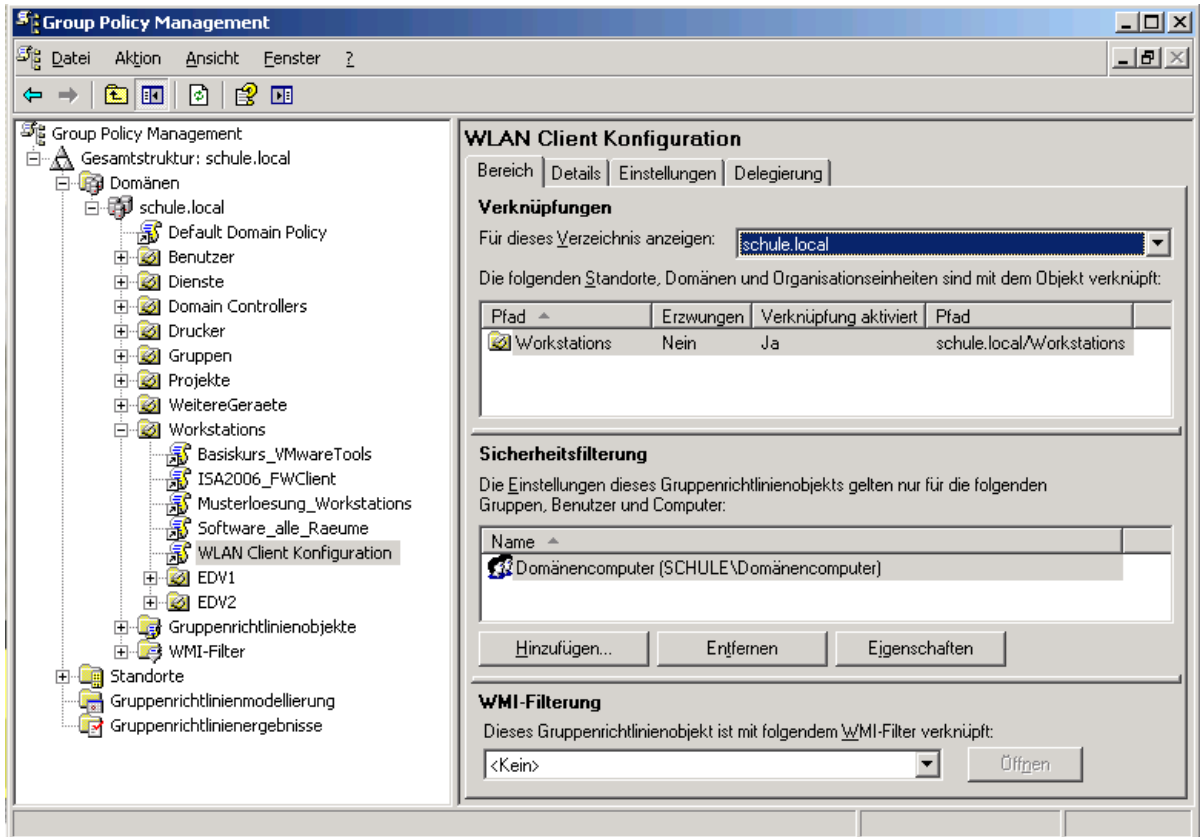
Auf S1:

- Gehen Sie auf *Start | Programme | Verwaltung | Gruppenrichtlinienverwaltung*
- Mit Rechtsklick gehen Sie auf die Ordnergruppe *Workstations | Gruppenrichtlinienobjekt hier erstellen und verknüpfen*.



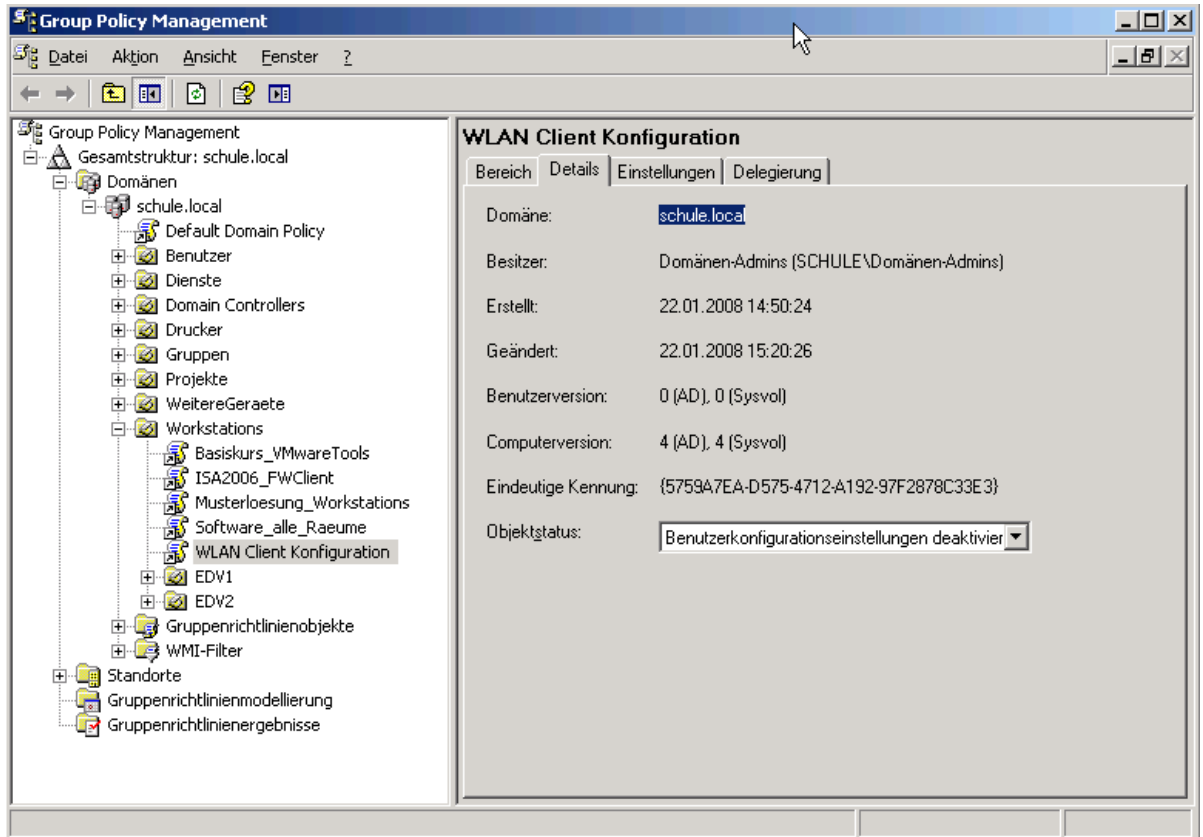
Bei *Name*: geben Sie *WLAN Client Konfiguration* ein.

- Markieren Sie das neue *WLAN Client Konfiguration* Objekt. Bei *Sicherheitsfilterung* löschen Sie die *Authentifizierten Benutzer* und fügen stattdessen *Domänencomputer* hinzu ¹

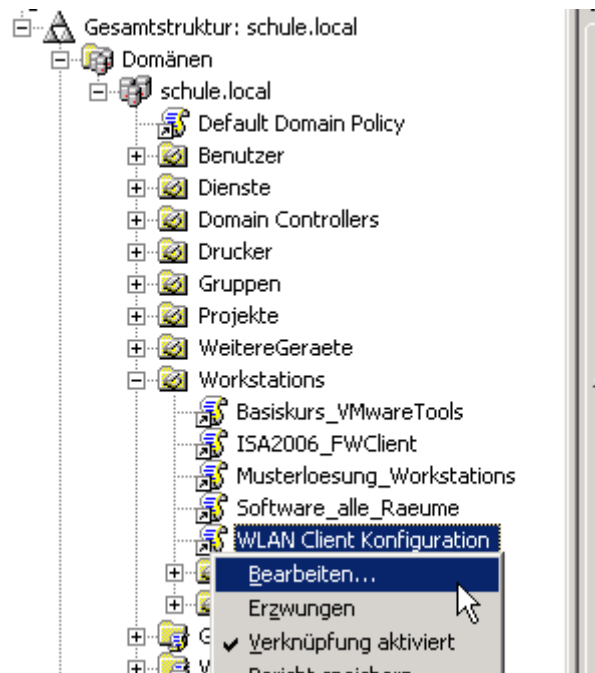


¹ Die Einstellungen dieser GPO werden sich lediglich auf die WLAN-Einstellungen im Zusammenhang mit dem bereitgestellten Zertifikat beziehen. Diese Richtlinie soll von den Clients bereits beim Hochfahren übernommen werden.

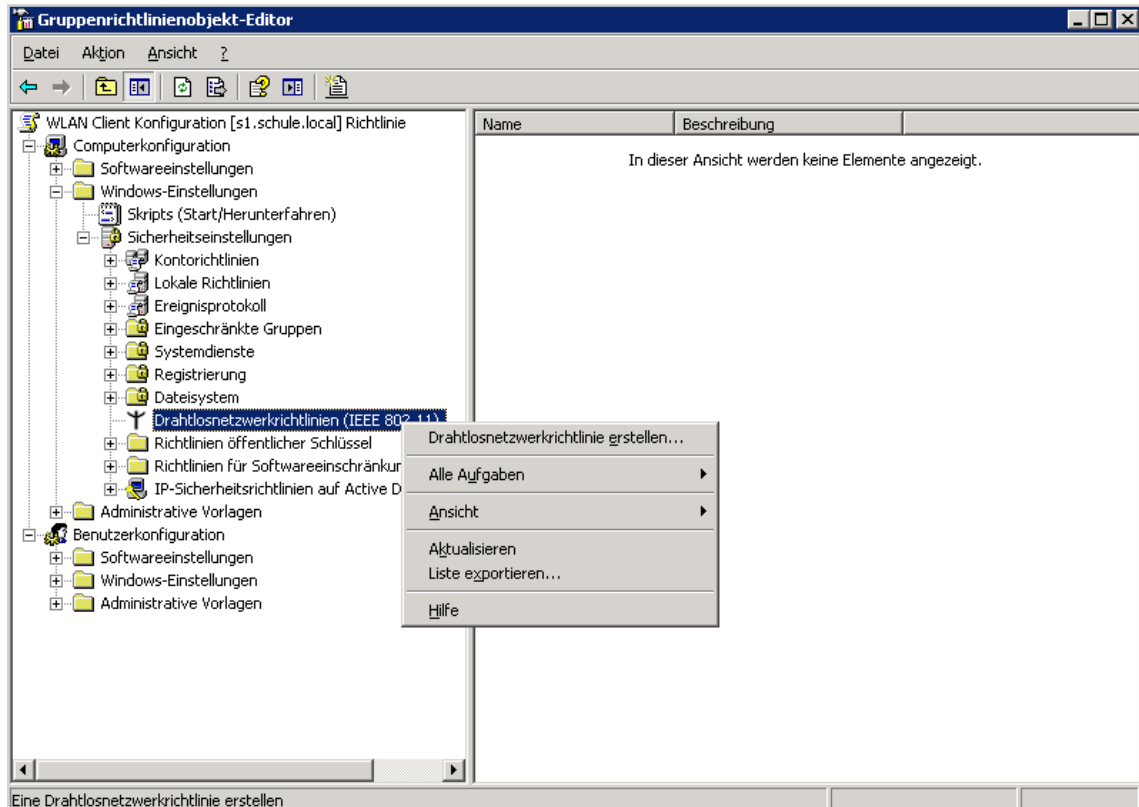
- Wechseln Sie in das Register *Details* und nehmen Sie bei *Objektstatus*: die Einstellung *Benutzerkonfigurationseinstellungen deaktiviert* vor ...



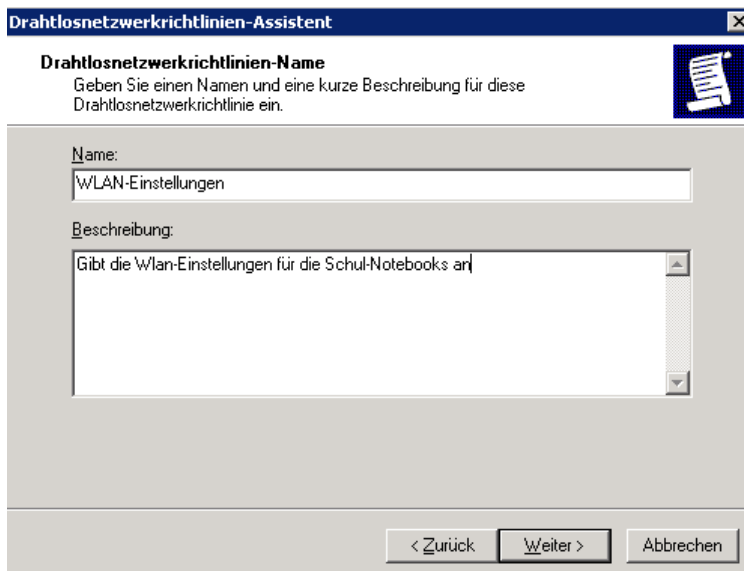
- Gehen Sie in der linken Fensterhälfte auf *WLAN Client Konfiguration* und mit Rechtsklick auf *Bearbeiten*.



- Gehen Sie unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* auf *Drahtlosnetzwerkrichtlinien* und dann mit Rechtsklick auf *Drahtlosnetzwerkrichtlinie* erstellen.

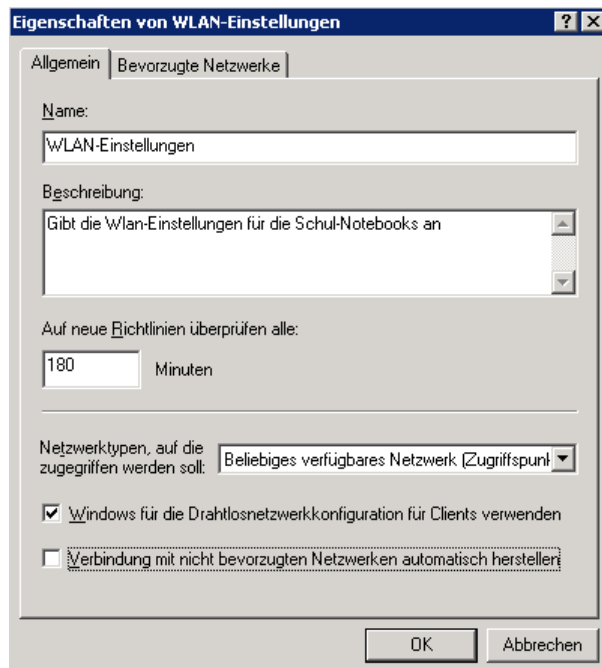


- Klicken Sie im Assistenten auf *Weiter*. Unter *Drahtlosnetzwerkrichtlinien-Name*: tragen Sie *WLAN-Einstellungen* ein. Klicken Sie dann auf *Weiter*.

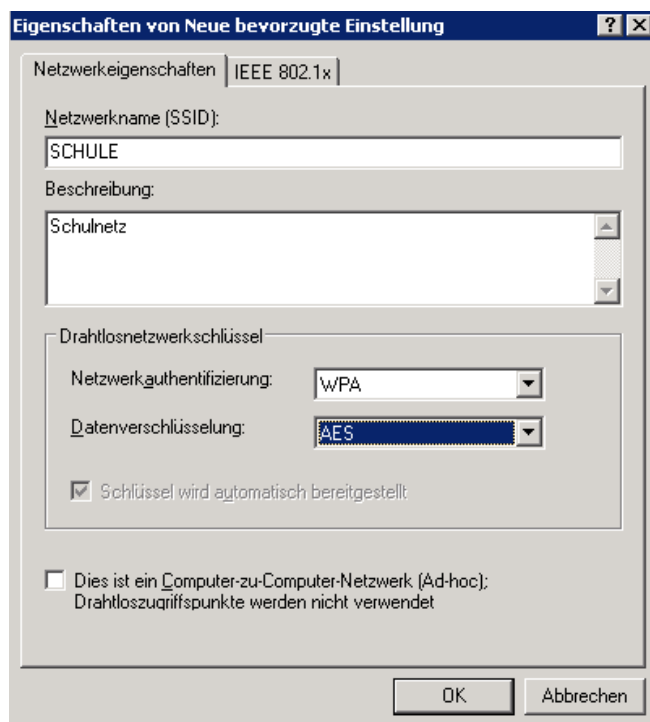


- Diese Drahtlosrichtlinie wird nun angepasst mit *Eigenschaften bearbeiten*. Wechseln Sie unter *Eigenschaften von WLAN-Einstellungen* in den Reiter *Allgemein*. Belassen Sie die

Einstellungen auf Standard.



- Klicken Sie im Reiter *Bevorzugte Netze* auf *Hinzufügen* und wechseln Sie in den Reiter *Netzwerkeigenschaften*

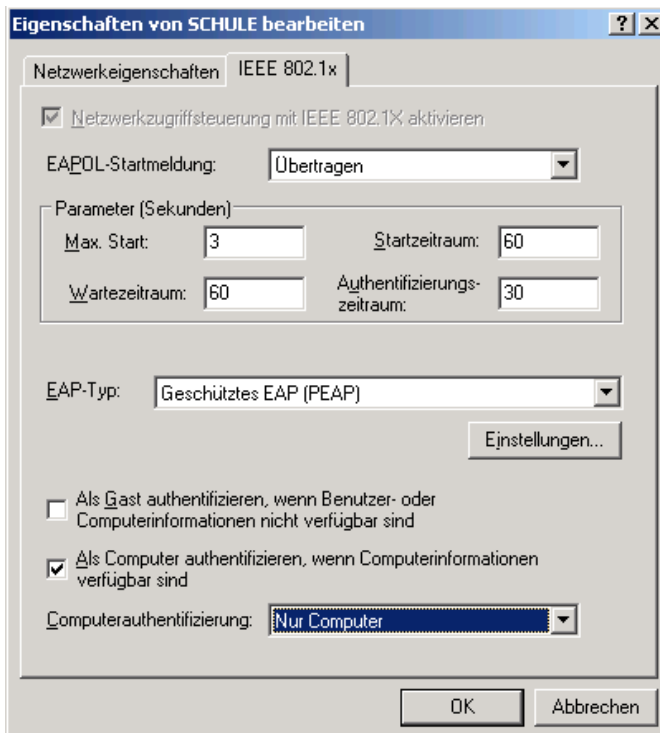


Netzwerkname (SSID): *SCHULE*

Netzwerkauthentifizierung: *WPA*

Datenverschlüsselung: *AES*

- Wechseln Sie in den Reiter *IEEE 802.1x*



Eigenschaften von SCHULE bearbeiten [?] [X]

Netzwerkeigenschaften IEEE 802.1x

Netzwerkzugriffsteuerung mit IEEE 802.1X aktivieren

EAPOL-Startmeldung: Übertragen

Parameter (Sekunden)

Max. Start:	<input type="text" value="3"/>	Startzeitraum:	<input type="text" value="60"/>
Wartezeitraum:	<input type="text" value="60"/>	Authentifizierungszeitraum:	<input type="text" value="30"/>

EAP-Typ: Geschütztes EAP (PEAP) [Einstellungen...]

Als Gast authentifizieren, wenn Benutzer- oder Computerinformationen nicht verfügbar sind

Als Computer authentifizieren, wenn Computerinformationen verfügbar sind

Computerauthentifizierung: Nur Computer

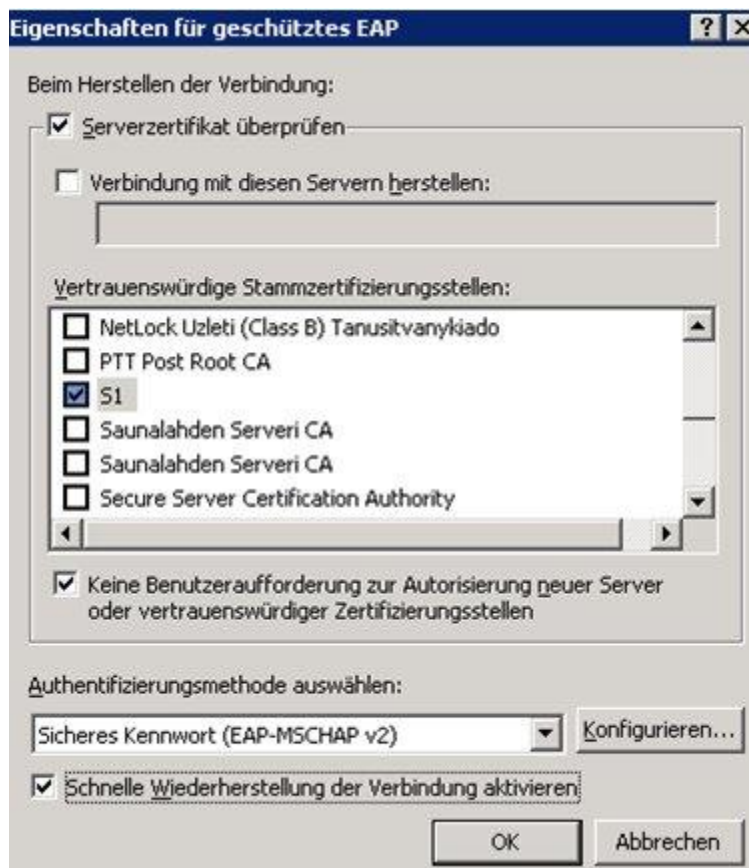
[OK] [Abbrechen]

EAPOL-Startmeldung: *Übertragen*

EAP-Typ: *Geschütztes EAP (PEAP)*

Computerauthentifizierung: *Nur Computer*

Bei EAP-Typ klicken Sie *Einstellungen* an.



Eigenschaften für geschütztes EAP [?] [X]

Beim Herstellen der Verbindung:

Serverzertifikat überprüfen

Verbindung mit diesen Servern herstellen:

Vertrauenswürdige Stammzertifizierungsstellen:

- NetLock Uzleti (Class B) Tanusitvanykiado
- PTT Post Root CA
- S1
- Saunalahden Serveri CA
- Saunalahden Serveri CA
- Secure Server Certification Authority

Keine Benutzeraufforderung zur Autorisierung neuer Server oder vertrauenswürdiger Zertifizierungsstellen

Authentifizierungsmethode auswählen:

Sicheres Kennwort (EAP-MSCHAP v2) [Konfigurieren...]

Schnelle Wiederherstellung der Verbindung aktivieren

[OK] [Abbrechen]

Setzen Sie den Haken bei „Serverzertifikat überprüfen“

Bei *Vertrauenswürdige Stammzertifizierungsstellen*: aktivieren Sie für alle „S1“

Setzen Sie den Haken bei „Keine Benutzeraufforderung zur Autorisierung neuer Server oder Zertifizierungsstellen“ sowie bei „Schnelle Wiederherstellung der Verbindung aktivieren“.

- Bestätigen Sie alles, um abzuschließen. Danach müssen sich die Notebooks nur einmal über LAN an der Domäne anmelden, damit die Gruppenrichtlinie aktiv wird.

2.4.3.

RAS-Richtlinien für private WLAN-Clients

Der Zugriff für private Clients erfolgt über eine weitere RAS-Richtlinie. Diese Richtlinie erlaubt den Zugriff über die Prüfung einer Gruppenmitgliedschaft. Dazu muss eine neue Gruppe angelegt werden, in welcher die Lehrer oder Schüler aufgenommen werden:

1. Legen Sie unter den OU *Gruppen* eine neue Gruppe *G_WLANZugriff* an.
2. Legen Sie nun mit der Schulkonsole ein neues Projekt mit dem Namen *PrivateWLAN-Nutzer* an.
3. Erklären Sie diese Projektgruppe zum Mitglied der Gruppe *G_WLANZugriff*.
4. Mitglieder der Projektgruppe sind alle Benutzer, denen der WLAN-Zugriff über private Notebooks gewährt werden soll (Die Mitglieder dieser Gruppe können einfach über die Oberfläche der Schulkonsole verwaltet werden).

Hinweis:

Entscheiden Sie, ob Sie den Zugriff zusätzlich auch über die MAC-Adressenprüfung gewähren möchten.

- Wenn ja, befolgen Sie die Richtlinienerstellung unter 2.4.5.
- Andernfalls führen Sie die Schritte unter 2.4.4 durch.

2.4.4.

RAS-Richtlinie für Benutzer, die mit privaten Clients auf das WLAN zugreifen dürfen

Erstellen Sie wie unter 2.4.1.1 eine neue Richtlinie. Abweichend davon ...

1. nennen Sie diese Richtlinie *WLAN für private Geräte*
2. Wählen Sie unter *Gruppen* anstelle von SCHULE\Domänencomputer die Gruppe *G_WLAN-Zugriff* aus.
3. Achten Sie darauf, dass sich die berechtigten Benutzer in der Projektgruppe *PrivateWLAN-Nutzer* befinden.

2.4.5.

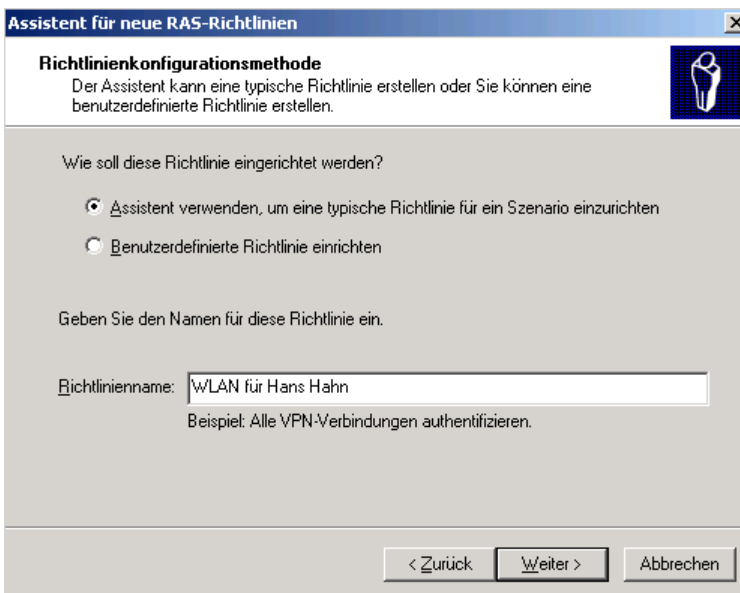
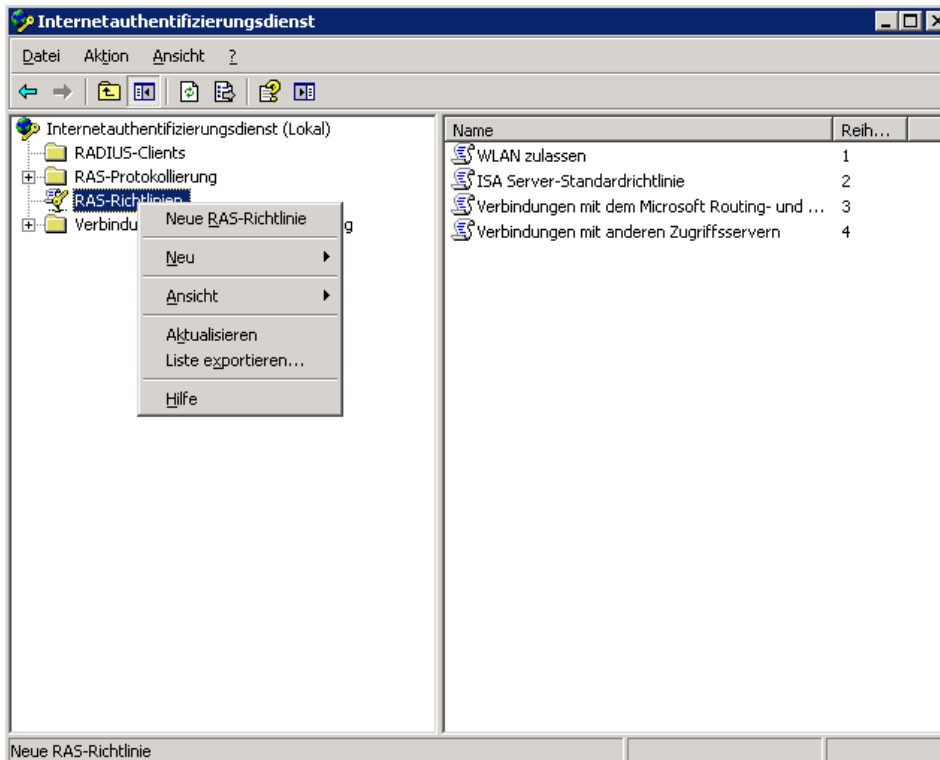
RAS-Richtlinie mit additiver MAC-Adressenüberprüfung

Wenn Sie den Zugriff nicht generell für alle privaten Geräte zulassen möchten, empfiehlt es sich zusätzlich die MAC-Adresse zu überprüfen. Dazu benötigen Sie von den Benutzern die MAC-Adresse des privaten Rechners. Die Benutzer können diese mit einem Befehl (*Start | Ausführen*) in eine Datei schreiben lassen und Ihnen übergeben, z.B.: `ipconfig /all C:\ipconf.txt`

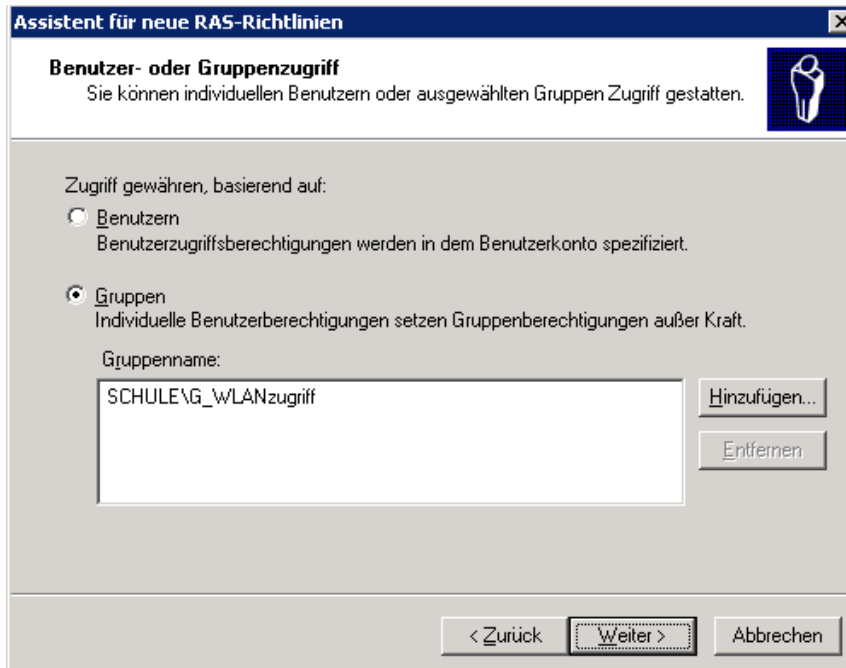
In der so erstellten Textdatei wählen Sie die MAC-Adresse des *Drahtlosadapters* für die Regel aus.

Bei dieser Form der Überprüfung müssen Sie für jeden Benutzer eine eigene Regel erstellen:

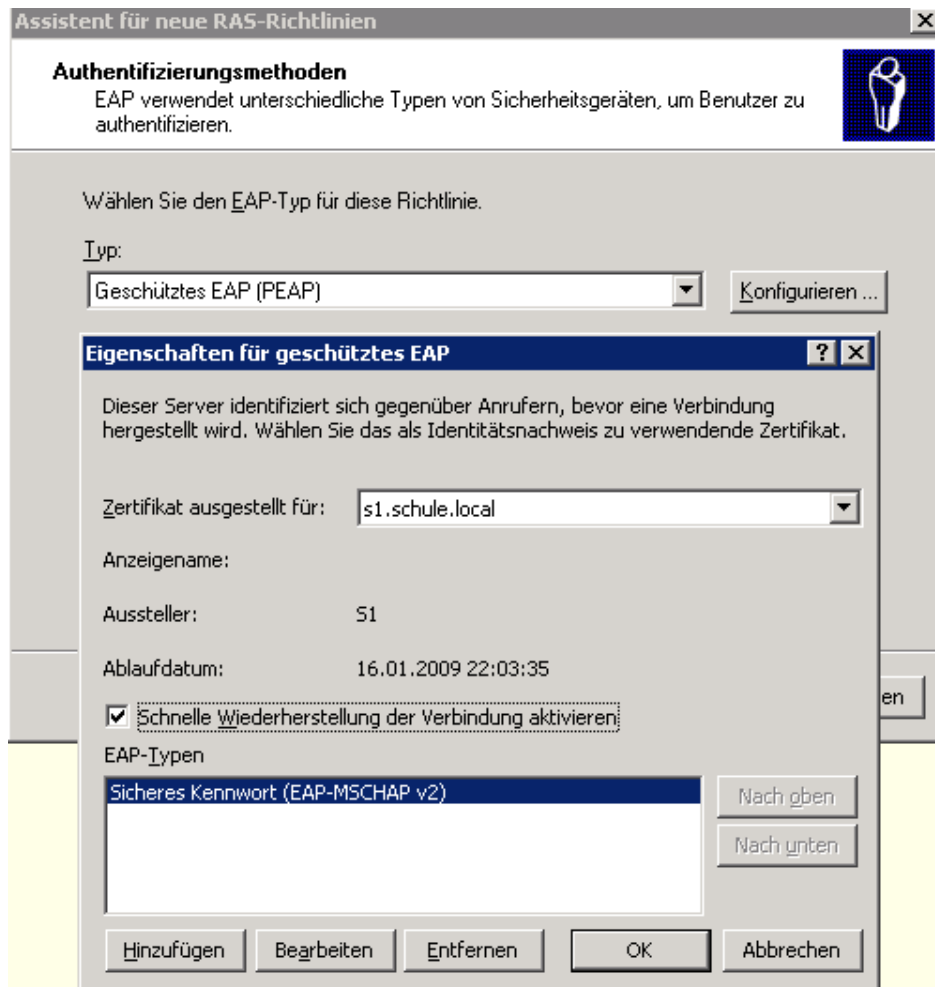
1. Erstellen Sie wie unter 2.4.4 eine neue Regel.



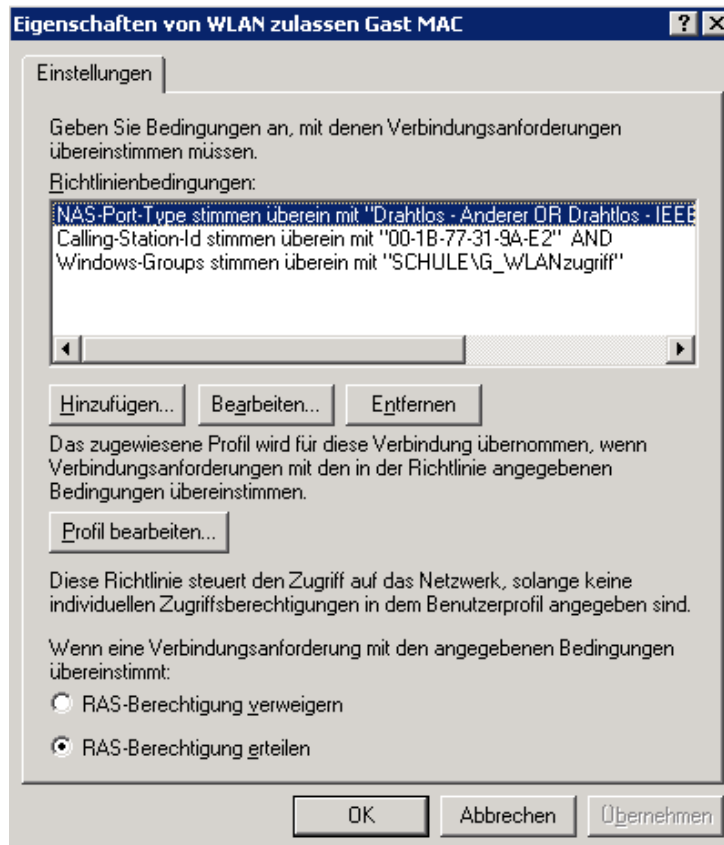
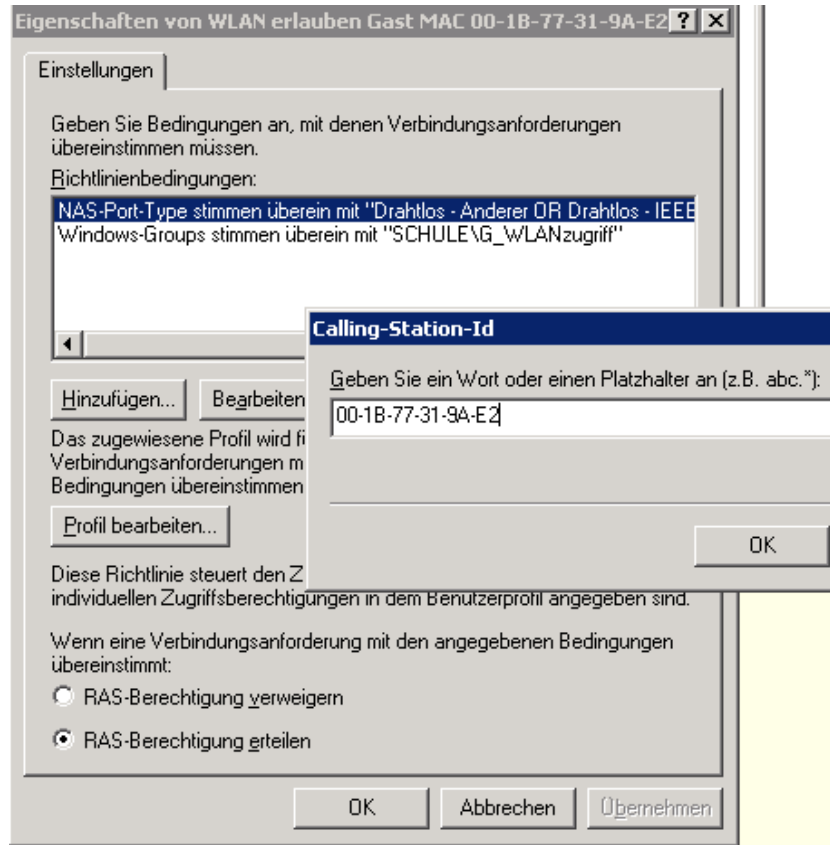
2. Achten Sie darauf, dass sich der berechnete Benutzer in der Projektgruppe *PrivateWLAN-Nutzer* befindet.
3. Wählen Sie als Zugriffsmethode „Drahtlos“ aus.
4. Wählen Sie die Gruppe *G_WLANZugriff* als berechnete Gruppe aus.



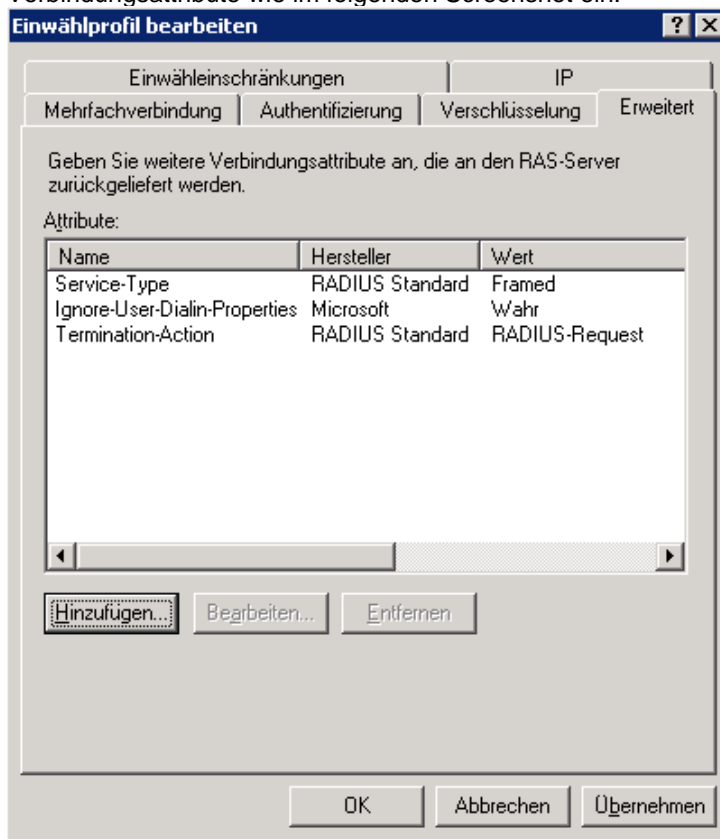
5. Wählen Sie als Authentifizierungsmethode *Geschütztes EAP (PEAP)* aus. Klicken Sie auf *Konfigurieren* und aktivieren Sie die Option „Schnelle Wiederherstellung der Verbindung aktivieren“ wie im Screenshot:



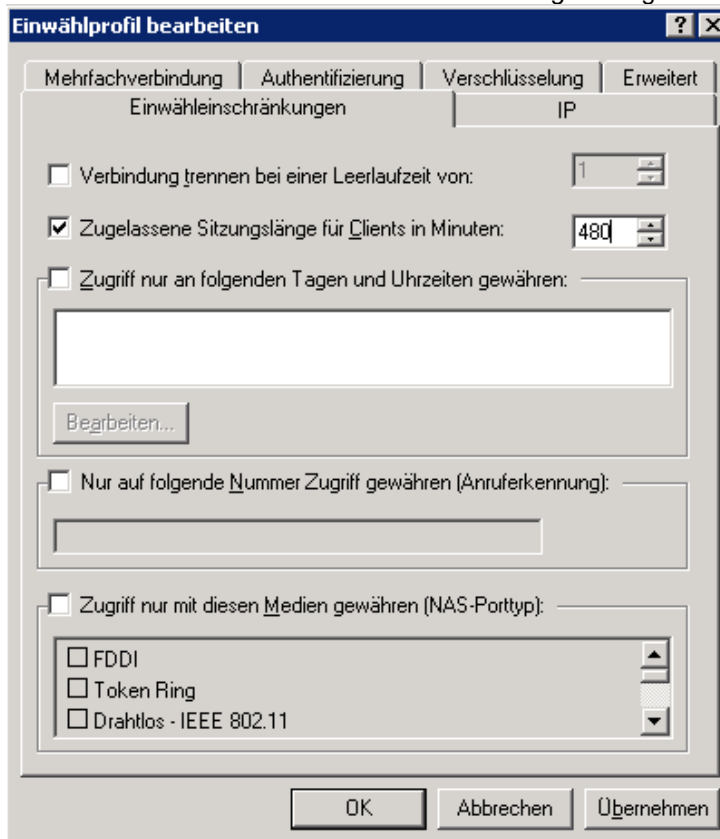
6. Bestätigen Sie die Einstellungen mit *Fertig stellen* und wechseln Sie mit einem rechten Mausklick auf die neue Regel im Register *Eigenschaften*.
 - Klicken Sie hier auf *Hinzufügen*.
 - Wählen Sie hier das Attribut *Calling-Station-Id* und klicken Sie auf *Hinzufügen...*
 - Geben Sie nun die MAC-Adresse des privaten Gerätes ein (Beachten Sie die Schreibweise mit einem „-“ nach jedem zweiten Zeichen).



- Klicken Sie nun auf *Profil bearbeiten ...* und wechseln Sie über den Reiter *Erweitert* die erweiterten Verbindungsattribute wie im folgenden Screenshot ein:



- Stellen Sie über den Reiter *Einwählbeschränkungen* die gewünschte zugelassene Sitzungslänge ein:



3. Links, Tools, Patches, weiterführende Informationen

3.1. Microsoft Technet

- Sichern von WLANs mit PEAP und Kennwörtern (aktualisiert: 18. Juni 2004)
online: <http://www.microsoft.com/germany/technet/datenbank/articles/900010.msp>
Download (Englisch): Securing Wireless LANs with PEAP and Passwords (V1.61 vom 22.6.2007)
<http://go.microsoft.com/fwlink/?LinkId=23481> (incl. div. Tools)
- The Cable Guy-May 2005 : Wi-Fi Protected Access 2 (WPA2) Overview
[http://technet.microsoft.com/de-de/library/bb878054\(en-us\).aspx](http://technet.microsoft.com/de-de/library/bb878054(en-us).aspx)
- Networking and Access Technologies (Overview): Wireless Networking
[http://technet.microsoft.com/de-de/network/bb530679\(en-us\).aspx](http://technet.microsoft.com/de-de/network/bb530679(en-us).aspx)
- IAS (Internet Authentication Service) Dump/restore (Netsh)
<http://technet2.microsoft.com/windowsserver/en/library/8f5c89d5-fdaf-430c-9ef4-318f8c15baf11033.msp?mfr=true>
- IAS Tools and Settings
<http://technet2.microsoft.com/WindowsServer/en/library/bdaf817f-dc50-48f0-b2a8-3cea5bd6d8031033.msp>

3.2. Literatur

- Joseph Davies „Drahtlose Netzwerke mit Microsoft Windows“ Microsoft Press
Theorie und Praxis sicherer 802.11-Wireless-LANs mit Microsoft Technologien
ISBN 3-86063-963-3

3.3. Tools für WLAN-Ausleuchtung

- Netstumbler <http://www.netstumbler.com/>
- NetIO <http://freshmeat.net/projects/netio/> oder <http://www.ars.de/ars/ars.nsf/docs/netio>

3.4.

Microsoft Updates für Windows XP – Client-PCs

- 802.11i/WPA2 Unterstützung durch das Update für Windows XP SP2:
 - Knowledge base: <http://support.microsoft.com/?kbid=917021>
 - Download: Update für Windows XP (KB917021) (17.10.2007)
<http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=2726f32f-d52b-4f84-ace8-f7fc20195769>
Hinweis: alte Version; Update für Windows XP (KB893357) (29.4.2005)

3.5.

Microsoft Updates für Windows 2000 – Client-PCs

- “Using 802.1x authentication on client computers that are running Windows 2000”
<http://support.microsoft.com/kb/313664/en-us>