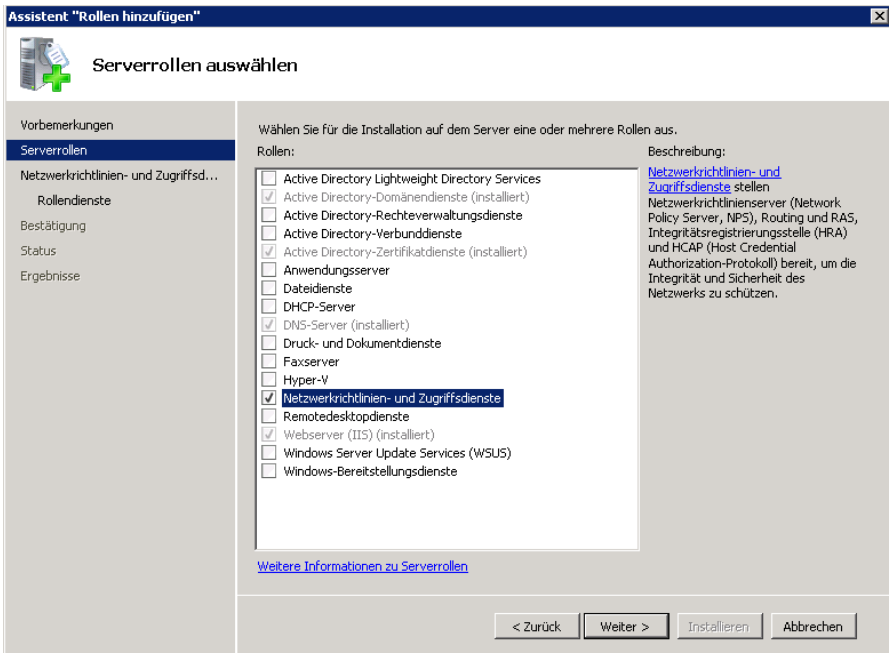
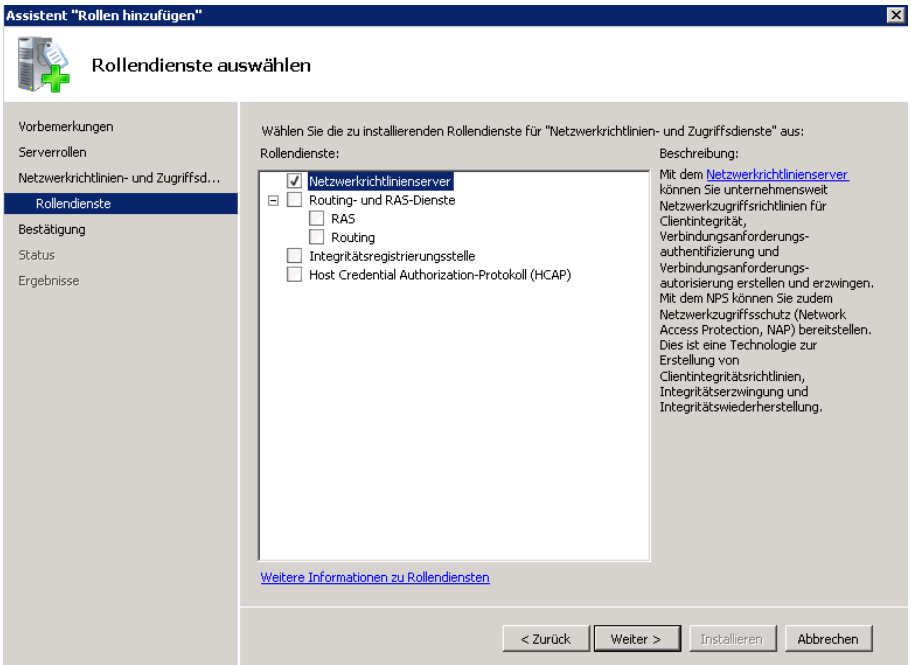
WLAN mit Zertifikaten

Ziel ist es, eine WLAN Authentifizierung mit Computerzertifkaten durchzufuehren und die entsprechenden WLAN Einstellungen per Gruppenrichtlinie zu verteilen und die Zertifikate mit Autoenrollment zu verteilen.

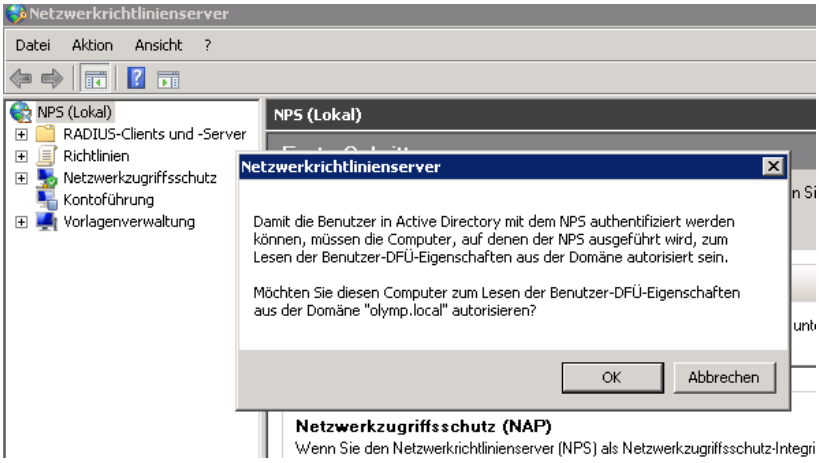
NPS Server Installation



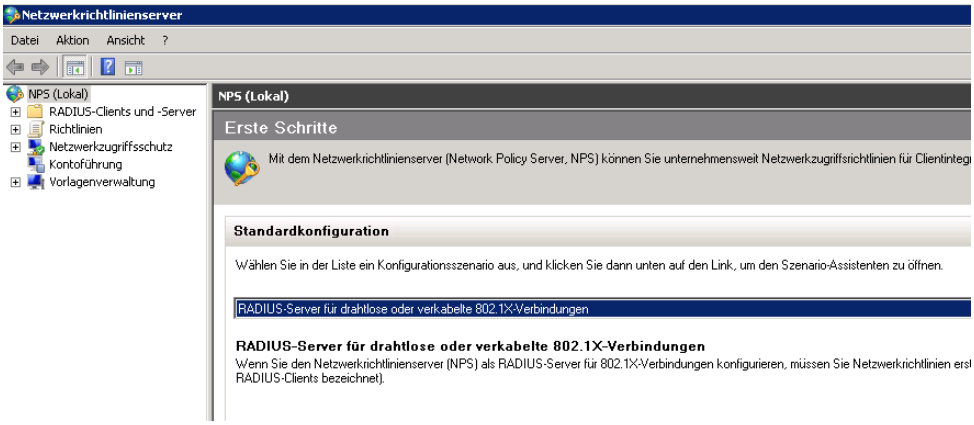
Nur die NPS Server Rolle installieren



Server im Active Directory registrieren

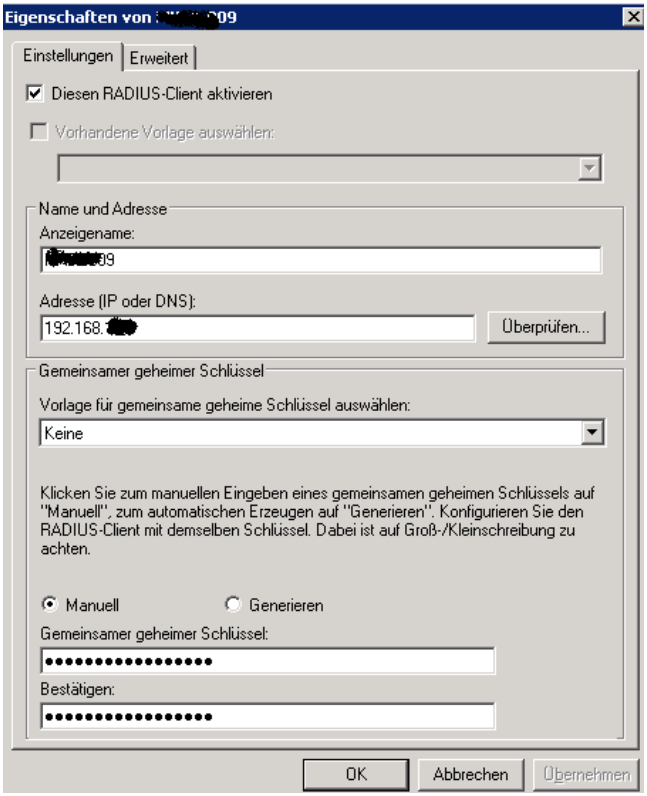


Netzwerkrichtlinienserver konfigurieren fuer RADIUS 802.1.X



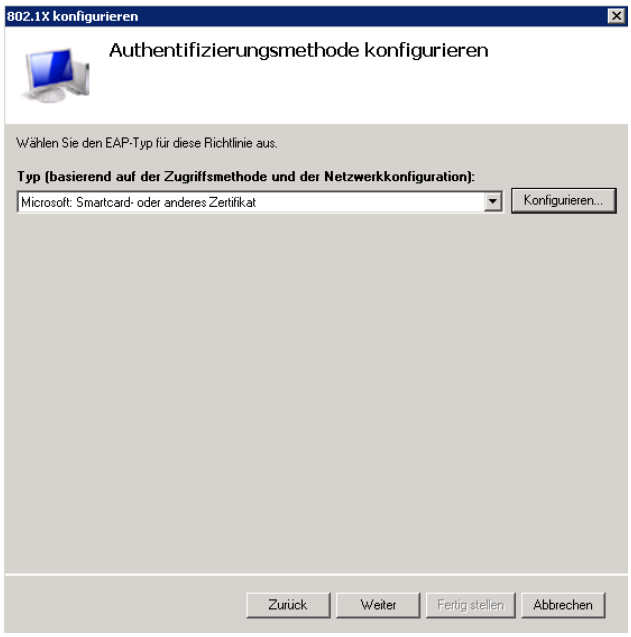
Neue 802.1x Policy

RADIUS Client fuer die WLAN Switche / Bridges anlegen

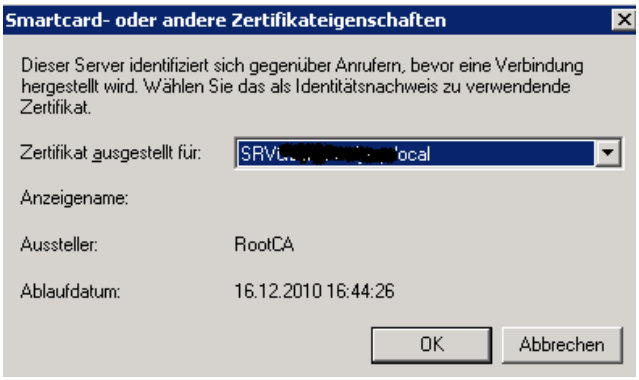


Darauf achten, einen sicheren PSK zu verwenden

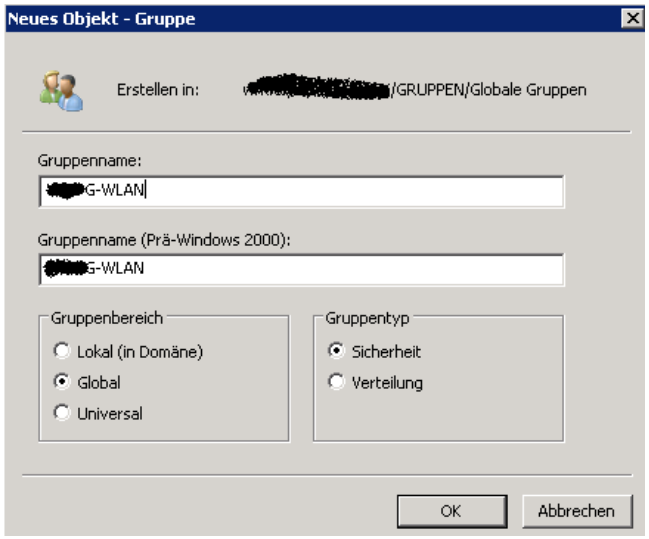
EAP Typ ist Zertifikat



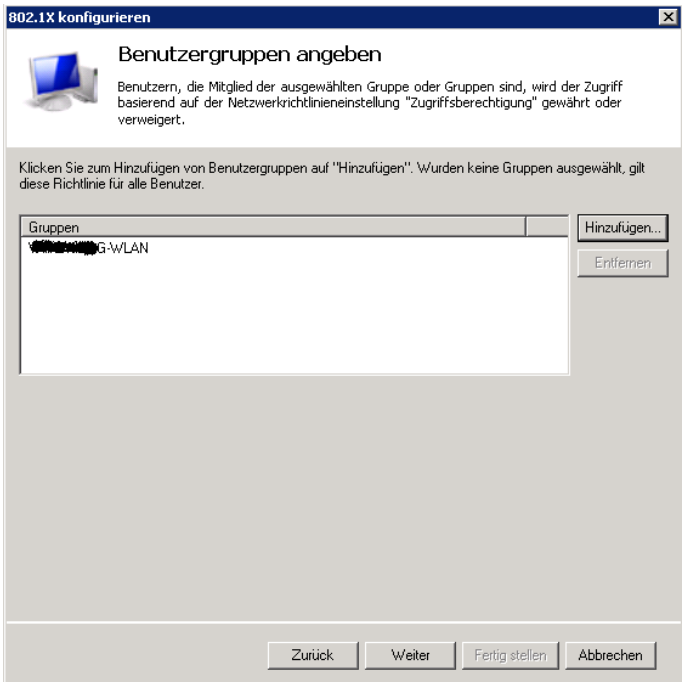
Zertifikat fuer Authentifizierung auswaehlen



Neue globale Sicherheitsgruppe mit den Computern fuer WLAN Zugriff anlegen

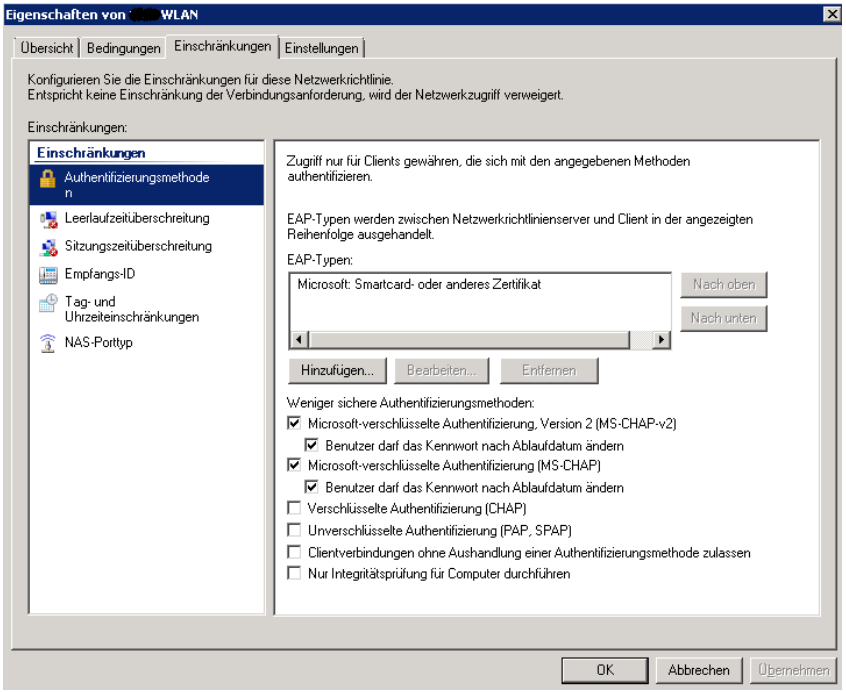


Computergruppe im NPS hinterlegen



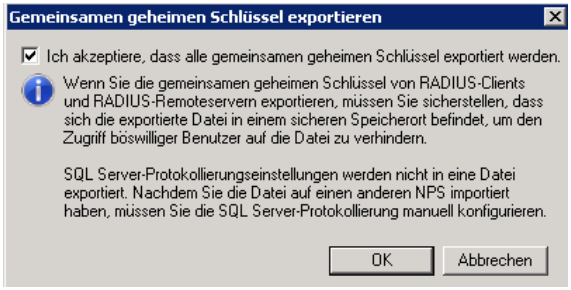
Anpassung der Netzwerkrichtlinie

MS-CHAP von den unterstuetzten Authentifizierungsmethoden entfernen. EAP-Type ist Zertifikat



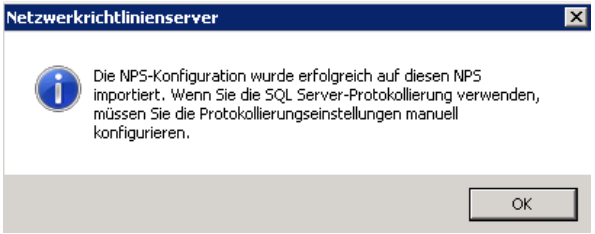
MPPE 128 Bit einstellen

Konfiguration exportieren und auf dem anderen NPS Server importieren.

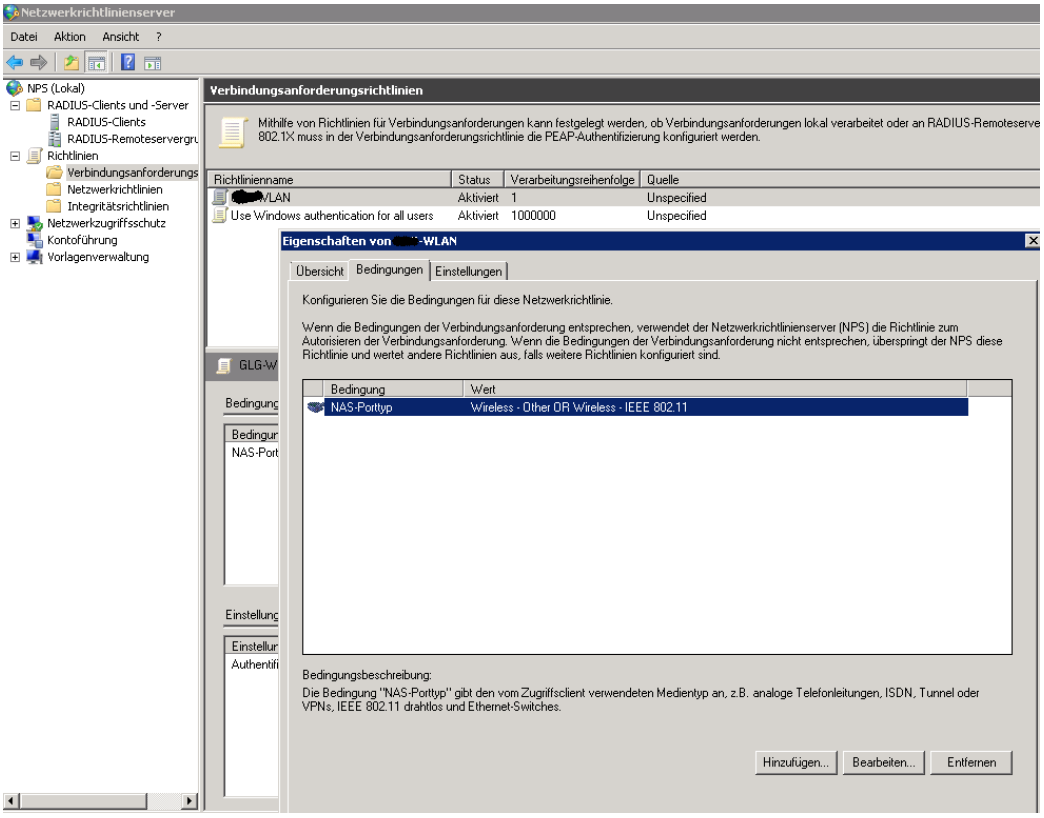


WICHTIG: Die beiden NPS Server synchronisieren die Konfiguration NICHT automatisch. Dazu muesste mit einem RADIUS-Server und RADIUS-Proxy Servern gearbeitet werden. Zum jetzigen Zeitpunkt muessen also Aenderungen an der NPS-Konfiguration auf beiden Servern manuell durchgefuehrt werden.

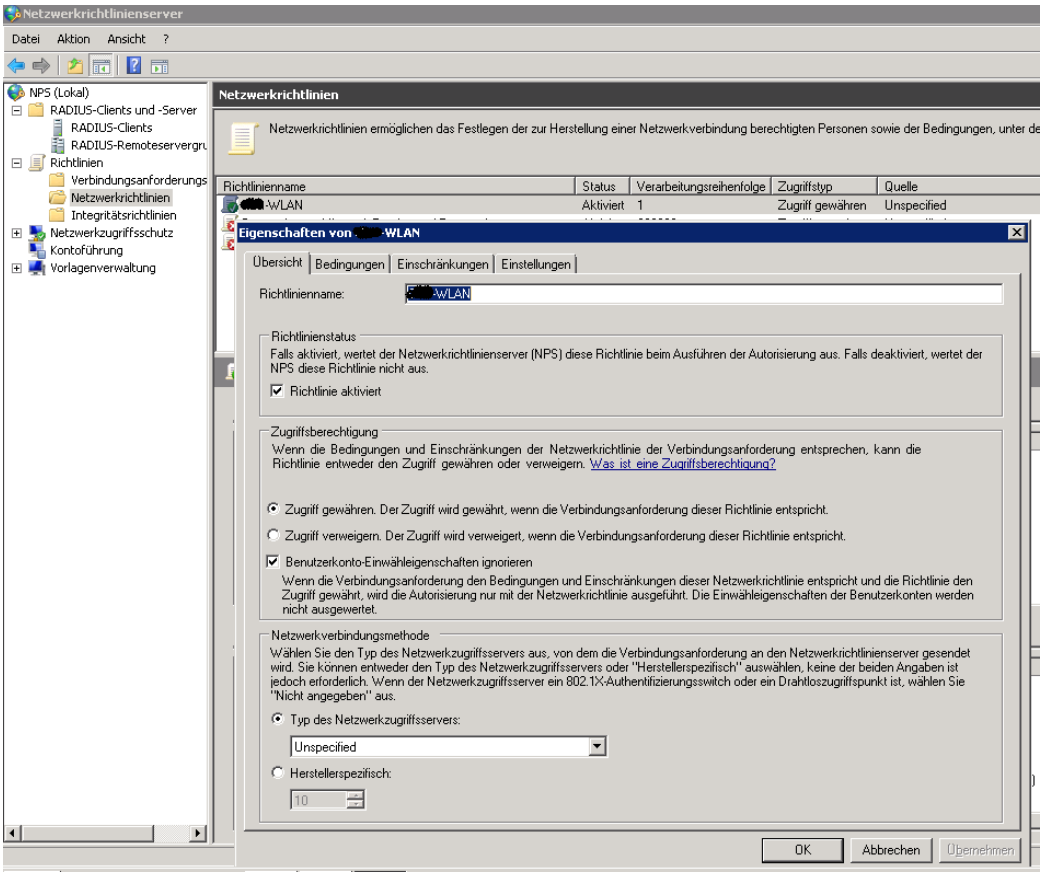
Konfiguration auf dem anderen NPS Server importieren



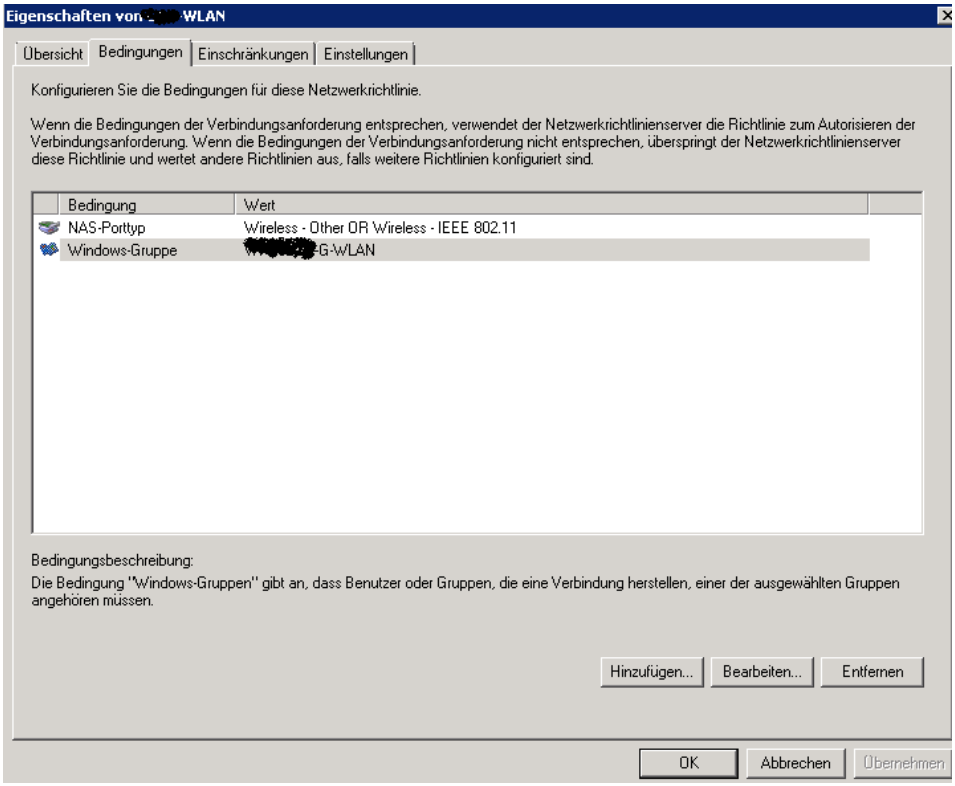
Verbindungsanforderungsrichtlinien



Netzwerkrichtlinien

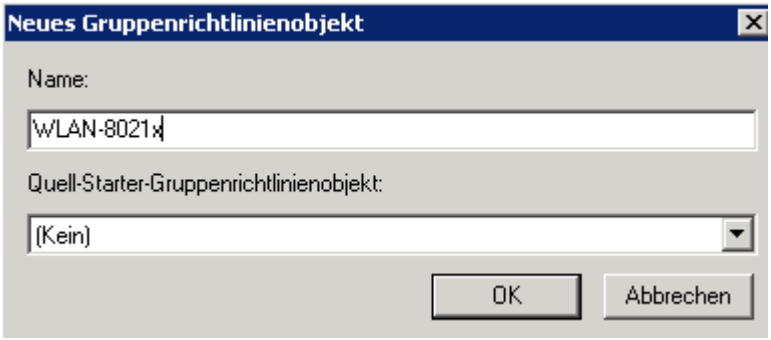


Bedingungen sind WLAN 802.11 und die globale Computergruppe

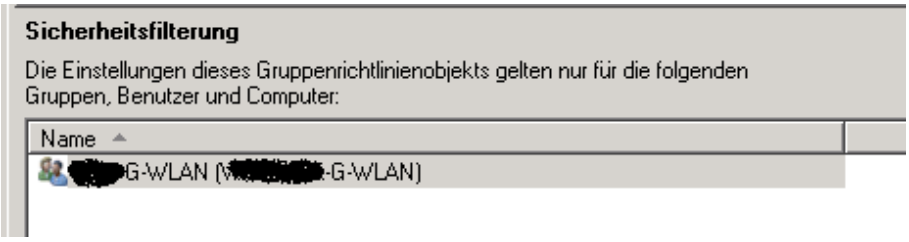


Autoenrollment fuer Zertifikate konfigurieren

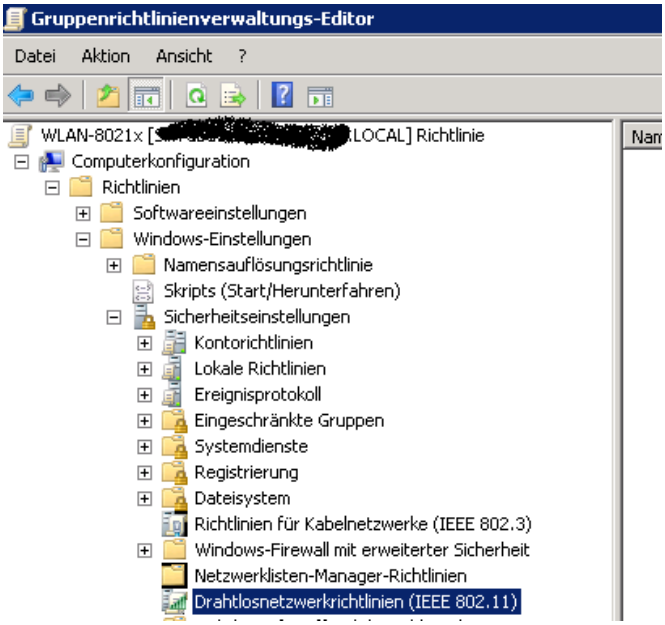
Neues Gruppenrichtlinienobjekt erstellen



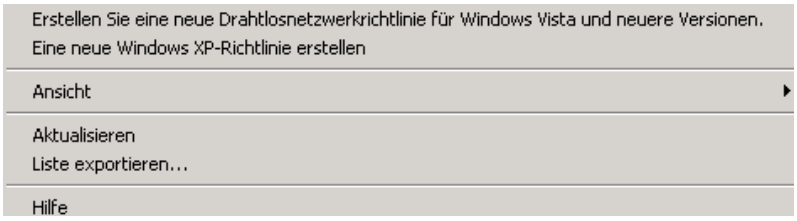
Sicherheitsfilterung auf die globale Gruppe mit den WLAN Computerkonten



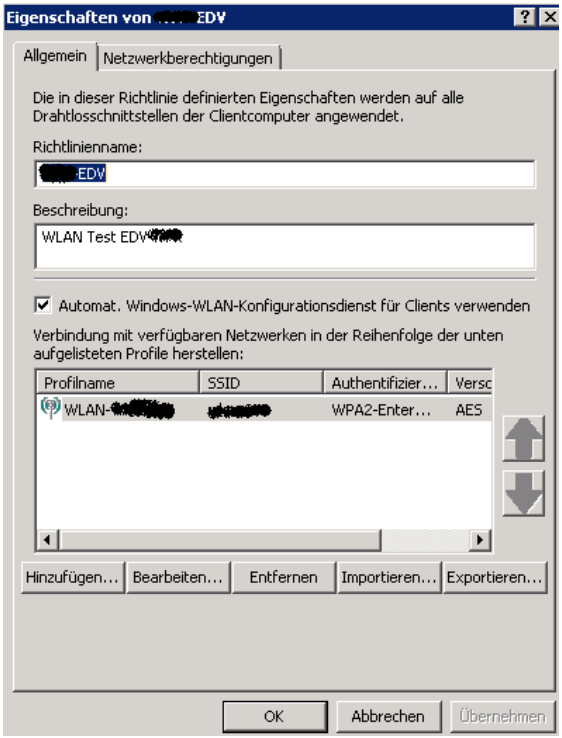
Neue Drahtlosnetzwerkrichtlinie konfigurieren

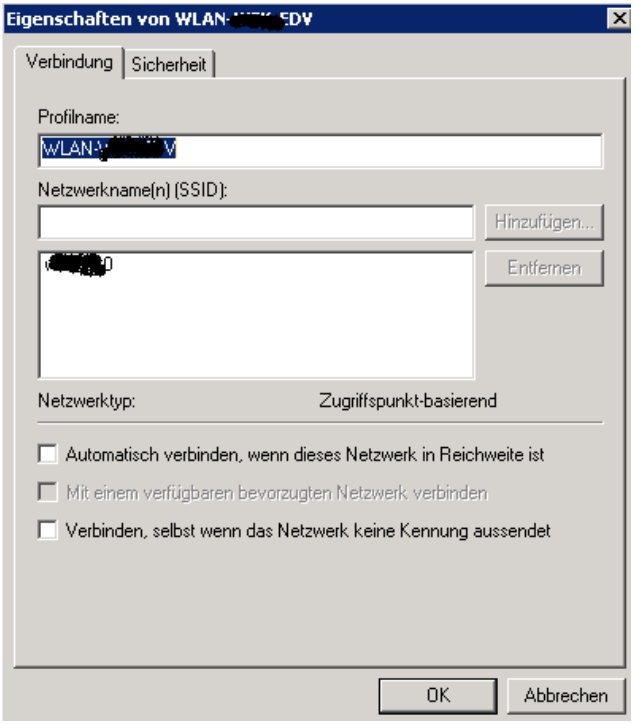


Versionsspezifisch

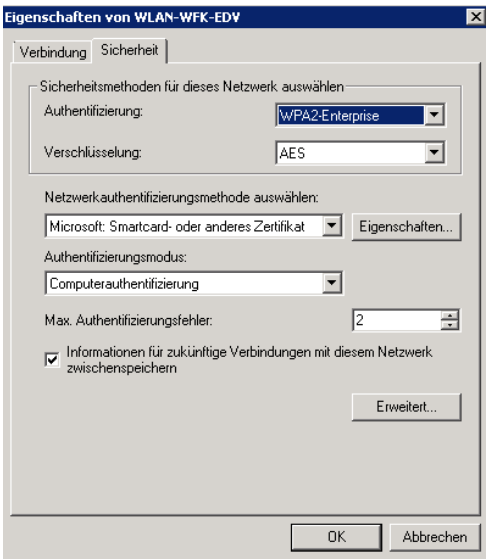


Neue Einstellungen fuer WLAN

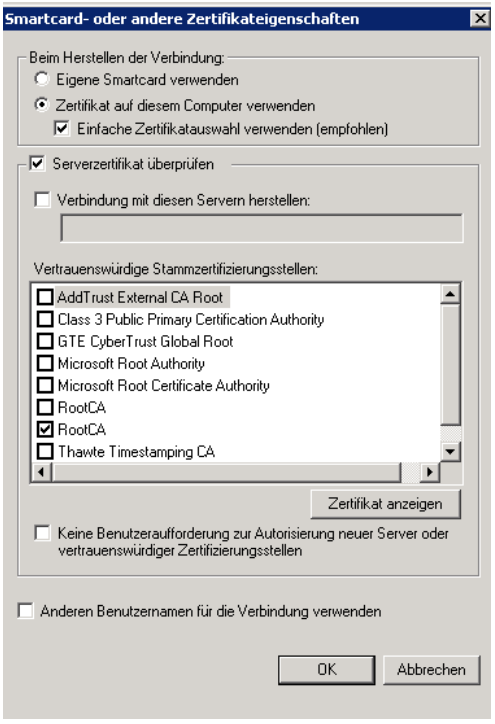




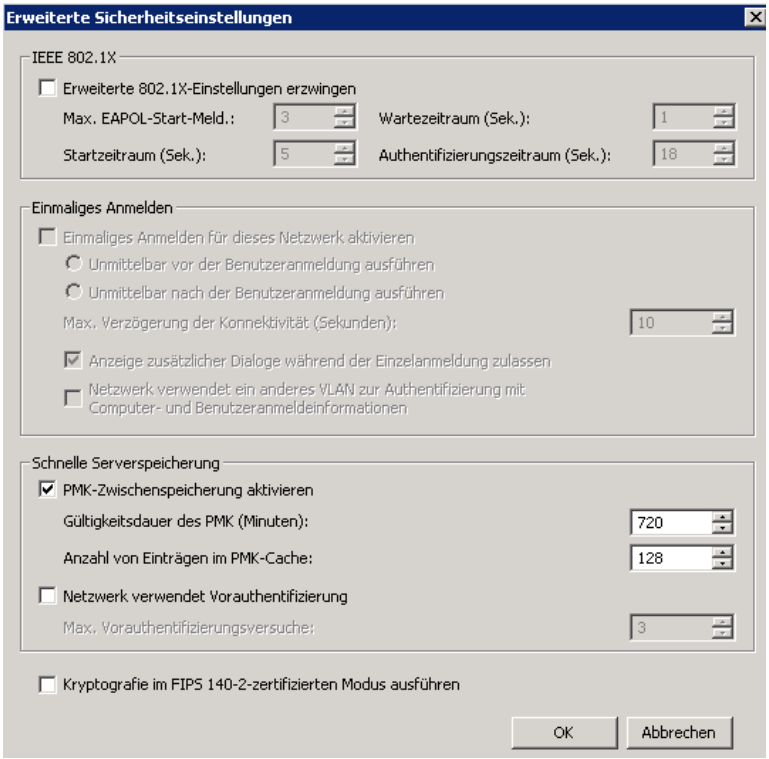
Sicherheitseinstellungen



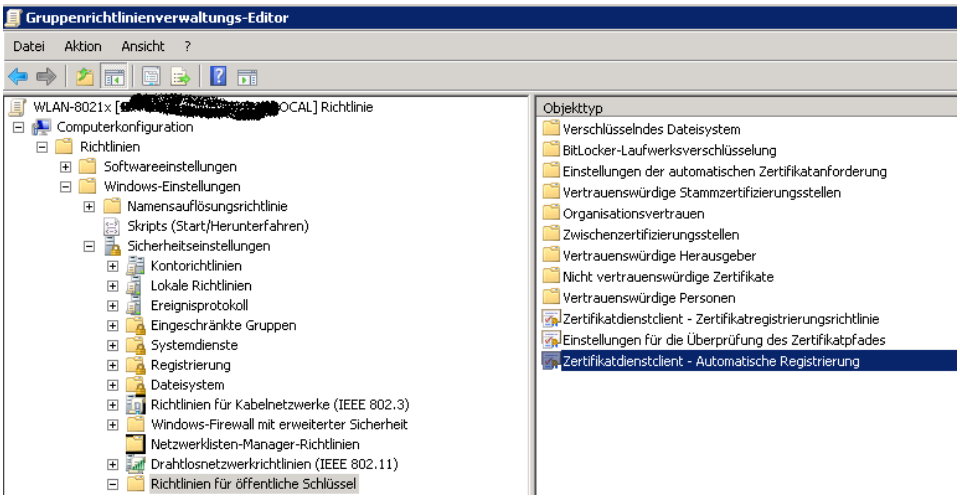
Zugriff auf die interne Zertifizierungsstelle beschraenken



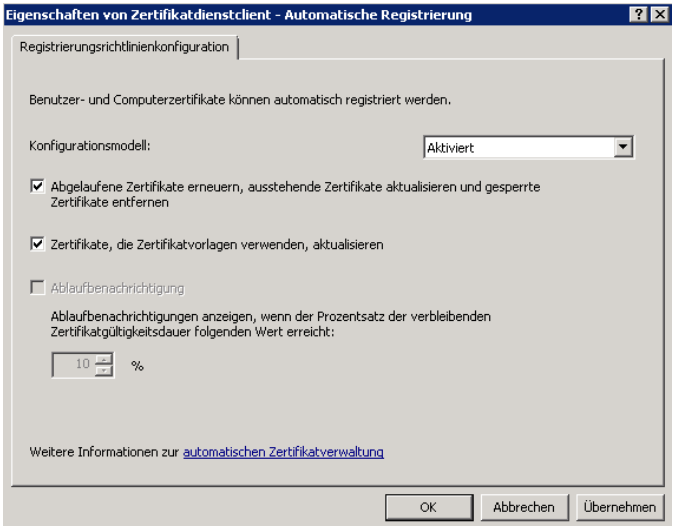
Erweiterte Sicherheitseinstellungen



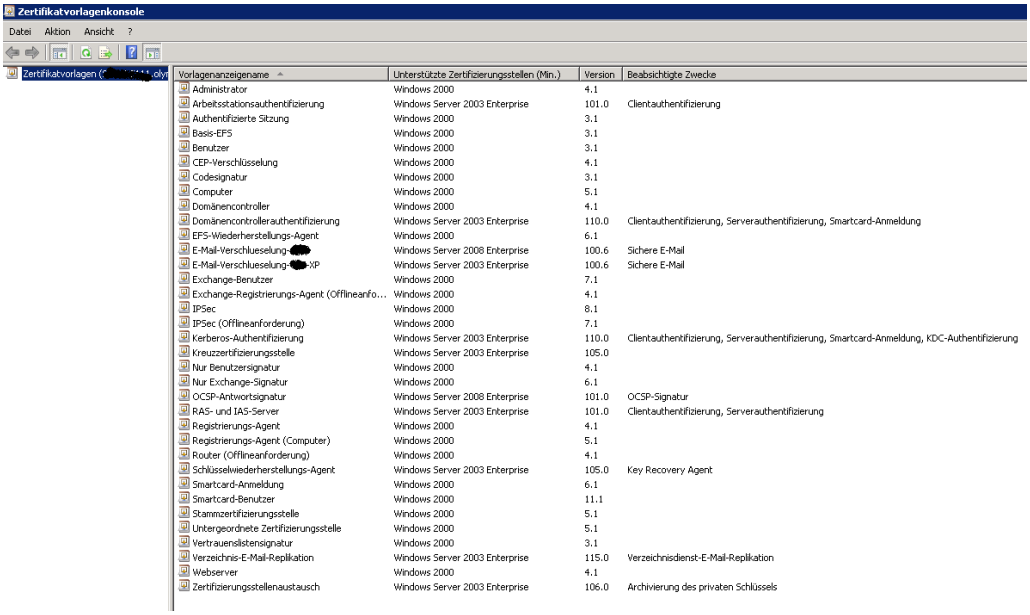
Autoenrollment fuer Zertifikate in der Gruppenrichtlinie aktivieren



Erweiterte Einstellungen

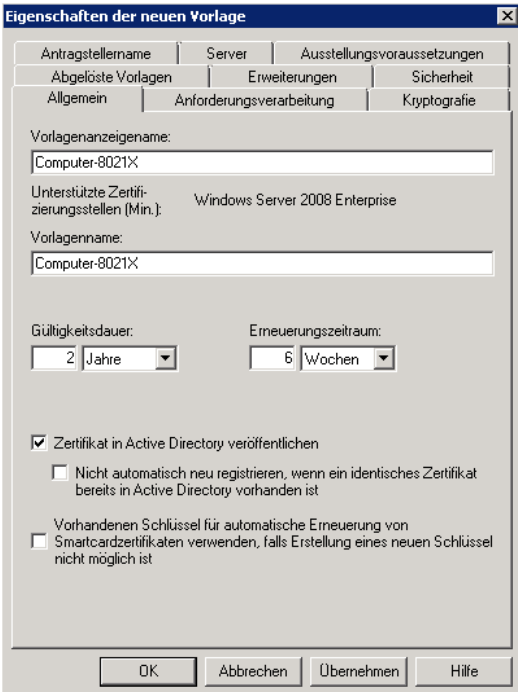


Neue Zertifikatvorlage fuer 802.1x Authentifizierung

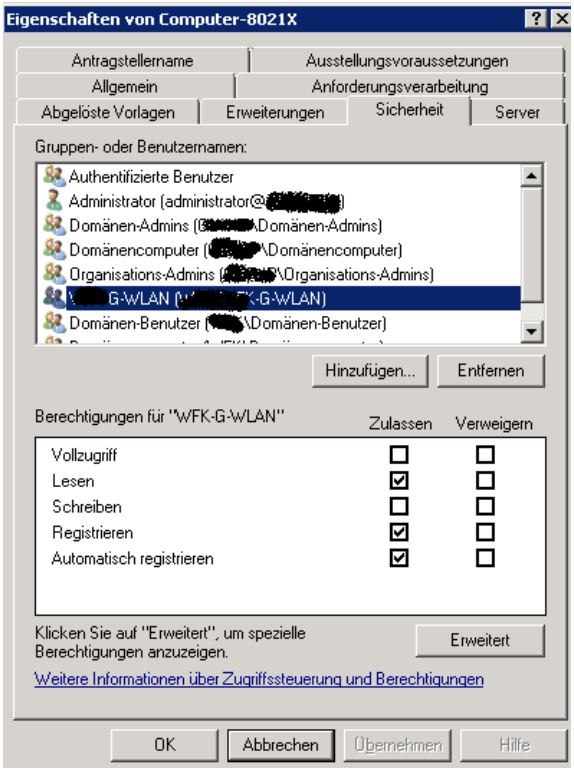


Doppelte Vorlage der Computerzertifikatvorlage

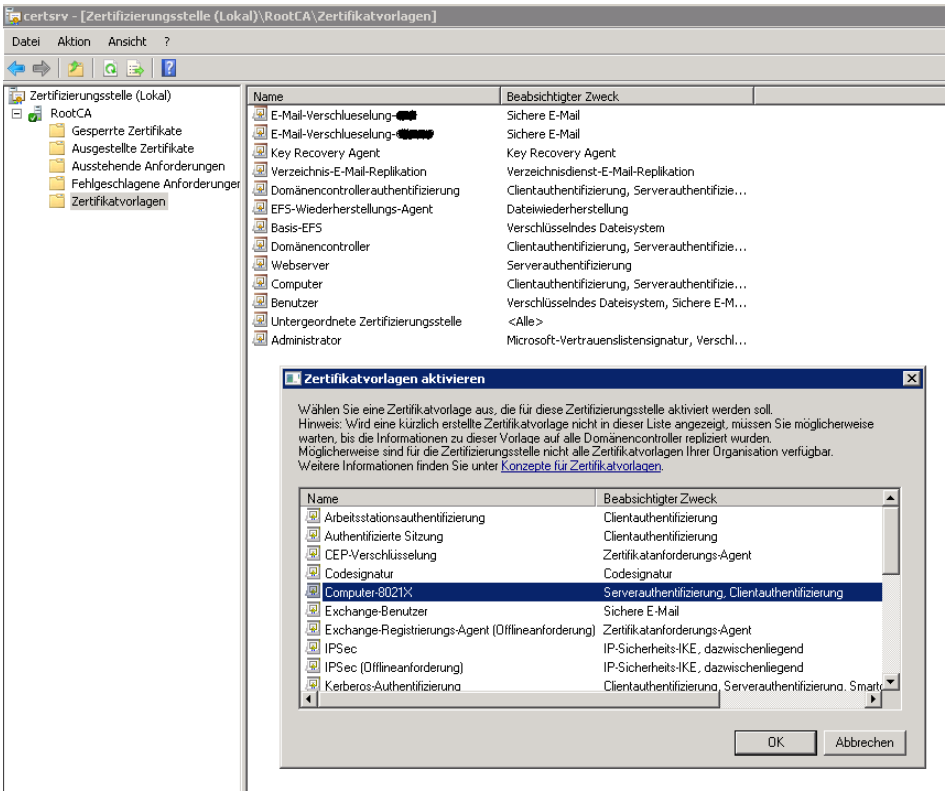
Gueltigkeit 2 Jahre



Autoenrollment fuer die Computergruppe erlauben



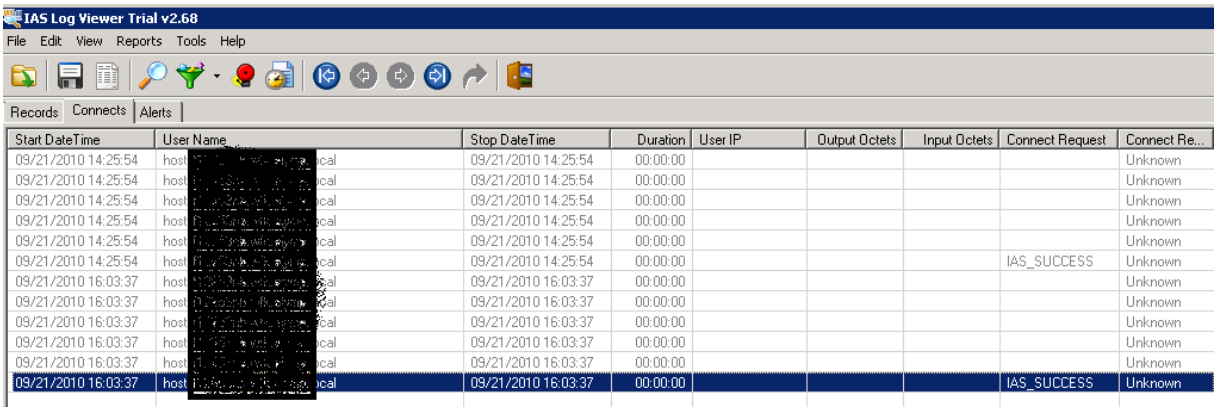
Zertifikatvorlage aktivieren



Client Seite:

Auf der Client-Seite muss der entsprechende WLAN-Client nur in die globale Windows Gruppe aufgenommen werden und die Anwendung der Gruppenrichtlinieneinstellungen abgewartet werden oder mit GPUPDATE /FORCE forciert werden.

IAS Log Viewer zur Anzeige der RADIUS Requests am NPS



Weitere optionale Moeglichkeiten:

- Einrichtung von NAP fuer die WLAN-Clients
- Einrichtung RADIUS-Server und RADIUS-Proxy fuer Zentralkonfiguration