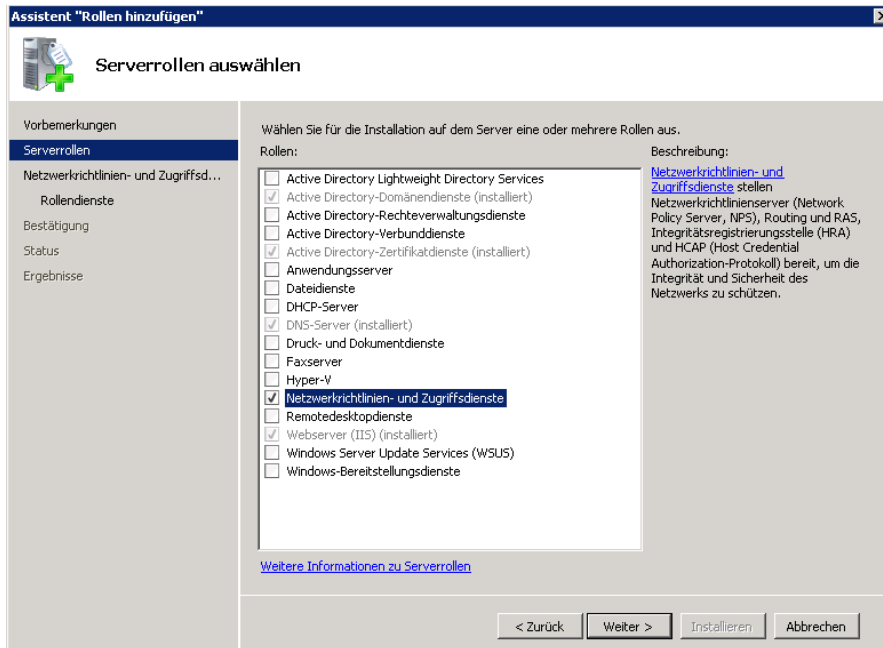


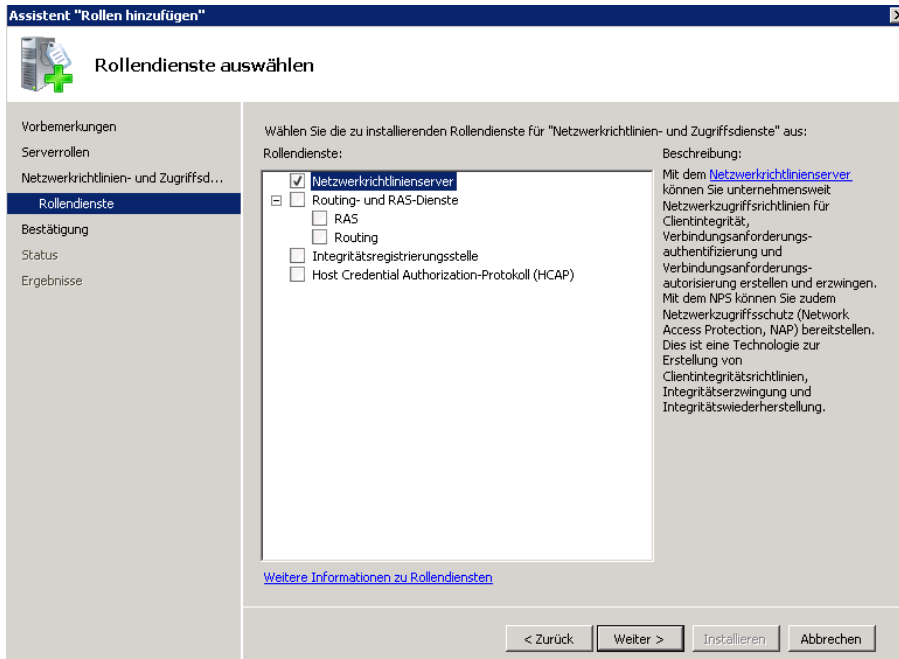
WLAN mit Zertifikaten

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

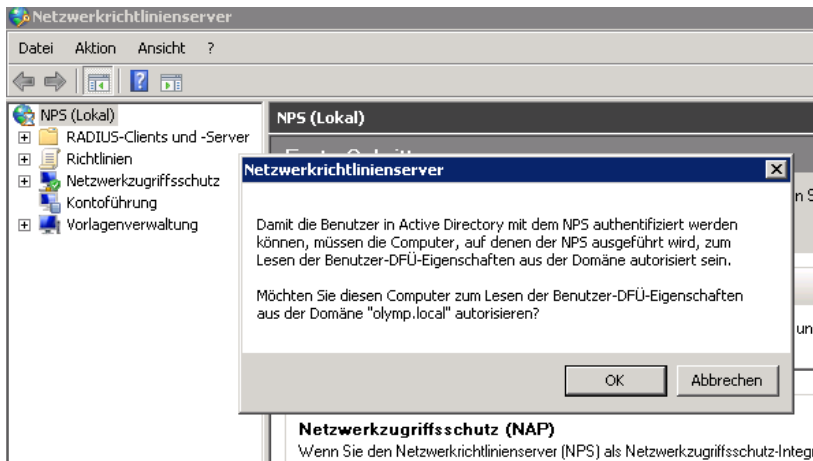
NPS Server Installation



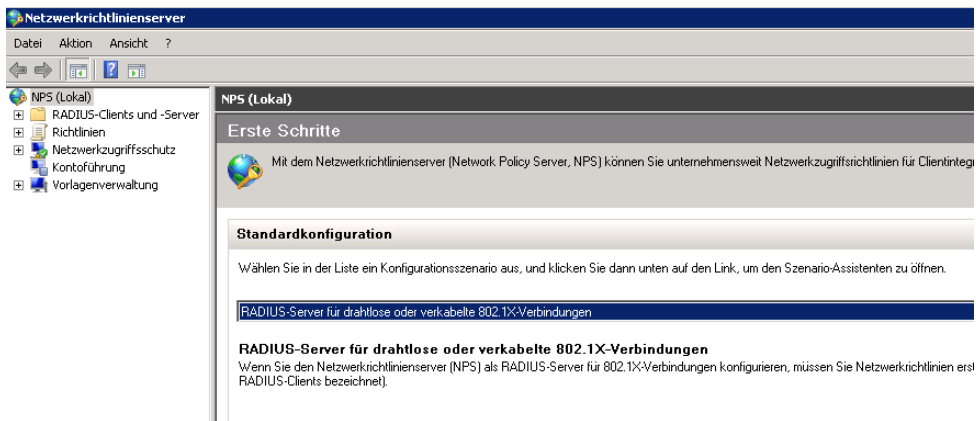
Nur die NPS Server Rolle installieren



Server im Active Directory registrieren



Netzwerkrichtlinienserver konfigurieren fuer RADIUS 802.1.X



Neue 802.1x Policy



RADIUS Client fuer die WLAN Switche / Bridges anlegen

Eigenschaften von: [Name] 09

Einstellungen | **Erweitert**

Diesen RADIUS-Client aktivieren
 Vorhandene Vorlage auswählen:

Name und Adresse
Anzeigename: [09]
Adresse (IP oder DNS): [192.168.] Überprüfen...

Gemeinsamer geheimer Schlüssel
Vorlage für gemeinsame geheime Schlüssel auswählen:
Keine

Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten.

Manuell Generieren

Gemeinsamer geheimer Schlüssel: [.....]
Bestätigen: [.....]

OK Abbrechen Übernehmen

Darauf achten, einen sicheren PSK zu verwenden

EAP Typ ist Zertifikat

802.1X konfigurieren

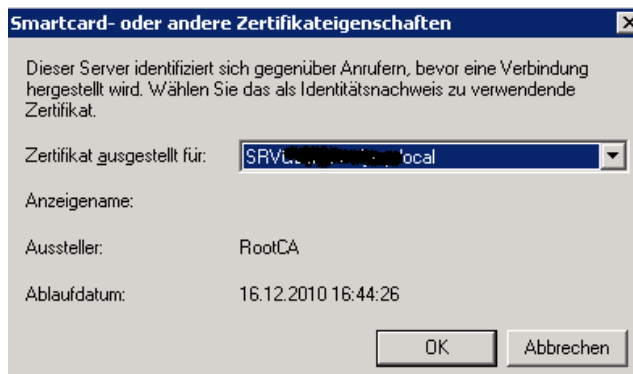
Authentifizierungsmethode konfigurieren

Wählen Sie den EAP-Typ für diese Richtlinie aus.

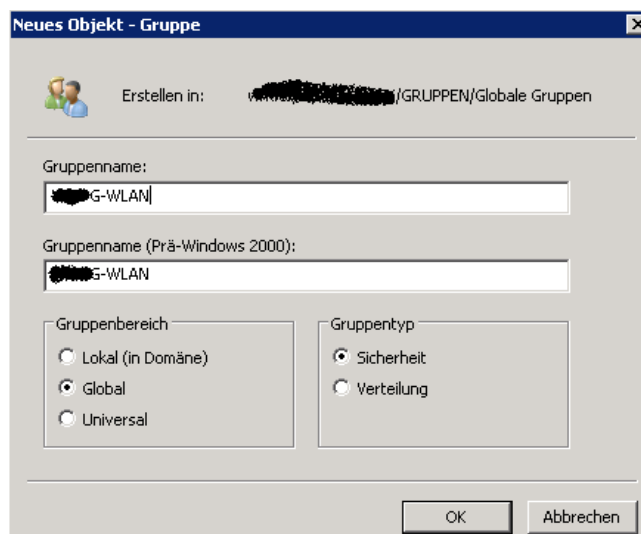
Typ (basierend auf der Zugriffsmethode und der Netzwerkkonfiguration):
Microsoft: Smartcard- oder anderes Zertifikat Konfigurieren...

Zurück Weiter Fertig stellen Abbrechen

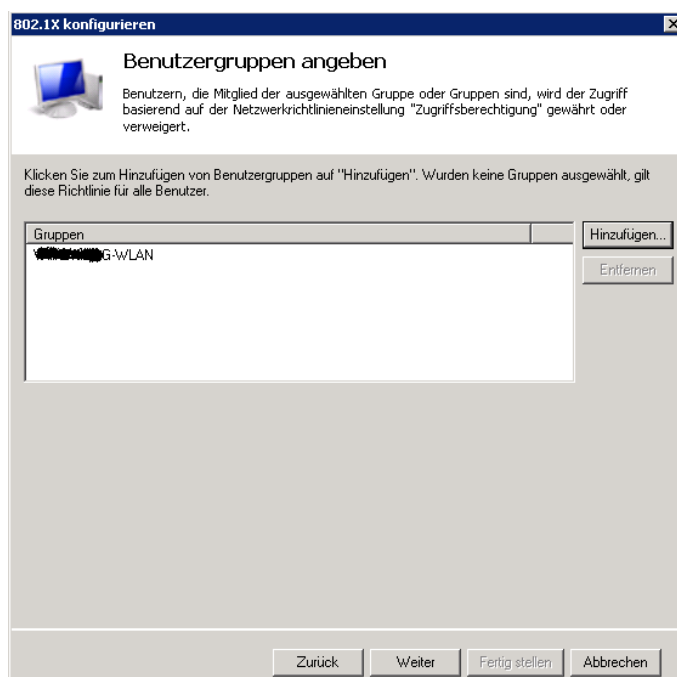
Zertifikat fuer Authentifizierung auswaehlen



Neue globale Sicherheitsgruppe mit den Computern fuer WLAN Zugriff anlegen

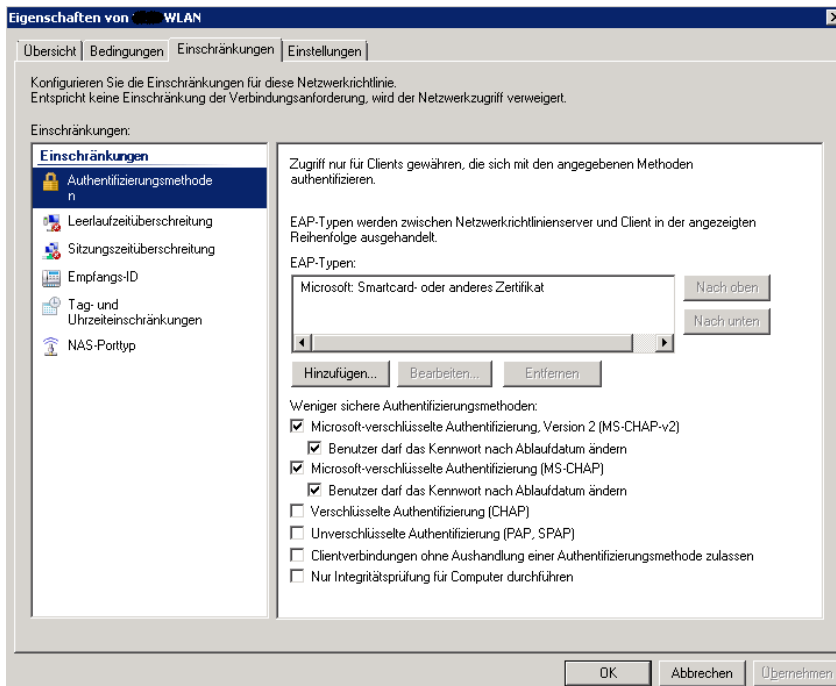


Computergruppe im NPS hinterlegen



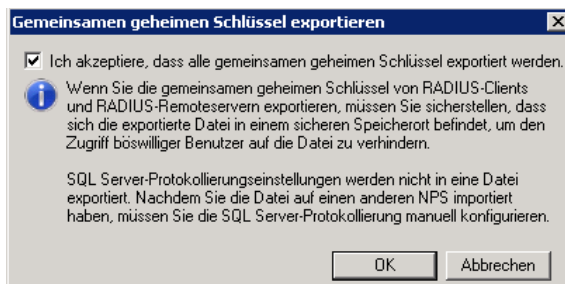
Anpassung der Netzwerkrichtlinie

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



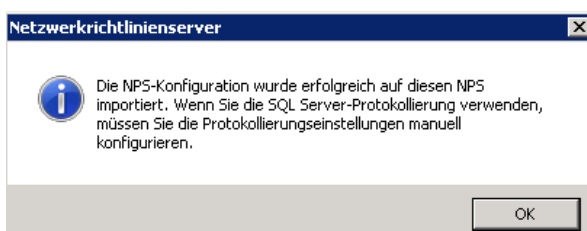
MPPE 128 Bit einstellen

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

The screenshot shows the NPS console with the 'Verbindungsanforderungsrichtlinien' (Connection Request Policies) pane selected. A table lists the policies:

Richtliniename	Status	Verarbeitungsreihenfolge	Quelle
WLAN	Aktiviert	1	Unspecified
Use Windows authentication for all users	Aktiviert	100000	Unspecified

The 'Eigenschaften von WLAN' dialog box is open, showing the 'Bedingungen' (Conditions) tab. It contains a table with one condition:

Bedingung	Wert
NAS-Porttyp	Wireless - Other OR Wireless - IEEE 802.11

Below the table, there is a description: 'Bedingungsbeschreibung: Die Bedingung "NAS-Porttyp" gibt den vom Zugriffsklient verwendeten Medientyp an, z.B. analoge Telefonleitungen, ISDN, Tunnel oder VPNs, IEEE 802.11 drahtlos und Ethernet-Switches.'

Netzwerkrichtlinien

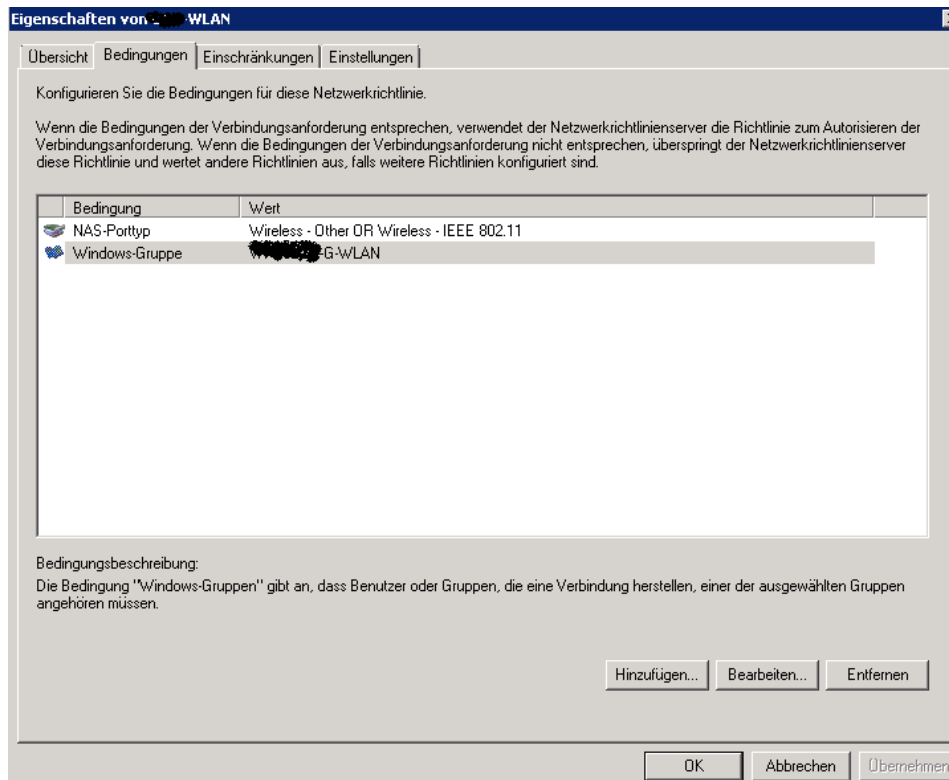
The screenshot shows the NPS console with the 'Netzwerkrichtlinien' (Network Policies) pane selected. A table lists the policies:

Richtliniename	Status	Verarbeitungsreihenfolge	Zugriffstyp	Quelle
WLAN	Aktiviert	1	Zugriff gewähren	Unspecified

The 'Eigenschaften von WLAN' dialog box is open, showing the 'Einschränkungen' (Restrictions) tab. It contains the following settings:

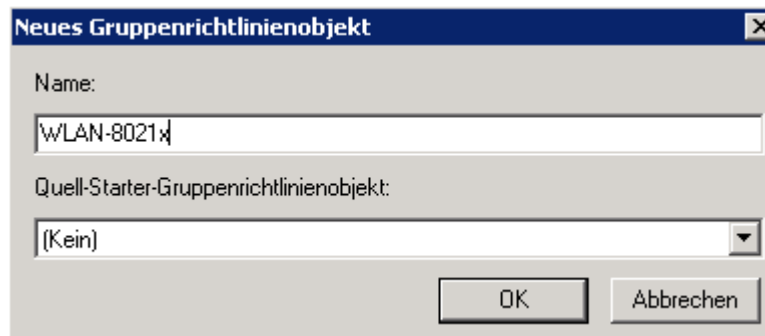
- Richtlinienstatus:** Richtlinie aktiviert
- Zugriffsberechtigung:**
 - Zugriff gewähren. Der Zugriff wird gewährt, wenn die Verbindungsanforderung dieser Richtlinie entspricht.
 - Zugriff verweigern. Der Zugriff wird verweigert, wenn die Verbindungsanforderung dieser Richtlinie entspricht.
 - Benutzerkonto-Einwähleigenschaften ignorieren. Wenn die Verbindungsanforderung den Bedingungen und Einschränkungen dieser Netzwerkrichtlinie entspricht und die Richtlinie den Zugriff gewährt, wird die Autorisierung nur mit der Netzwerkrichtlinie ausgeführt. Die Einwähleigenschaften der Benutzerkonten werden nicht ausgewertet.
- Netzwerkverbindungsmethode:**
 - Typ des Netzwerkzugriffsservers: Unspecified
 - Herstellerspezifisch: 10

Bedingungen sind WLAN 802.11 und die globale Computergruppe

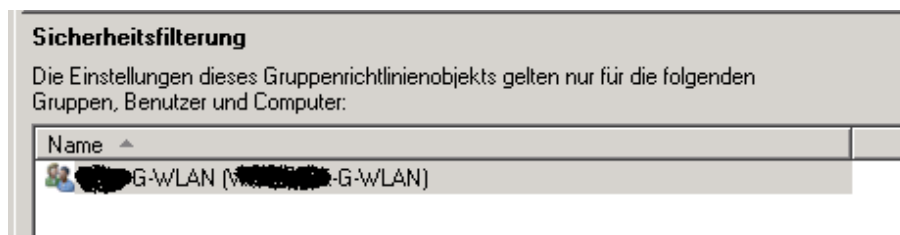


Autoenrollment fuer Zertifikate konfigurieren

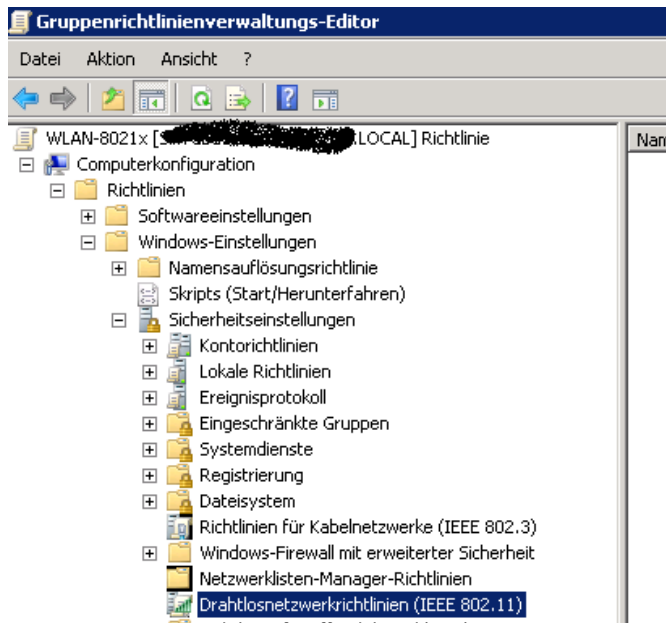
Neues Gruppenrichtlinienobjekt erstellen



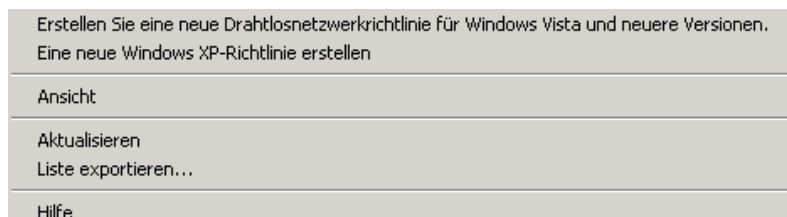
Sicherheitsfilterung auf die globale Gruppe mit den WLAN Computerkonten



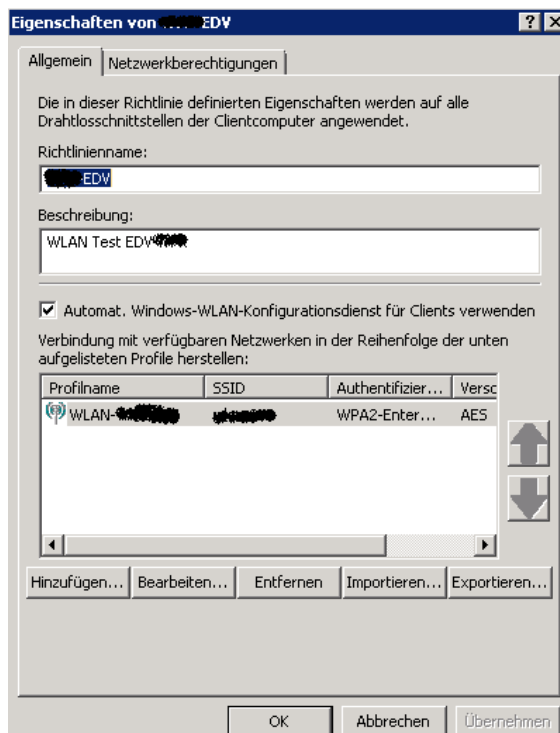
Neue Drahtlosnetzwerkrichtlinie konfigurieren

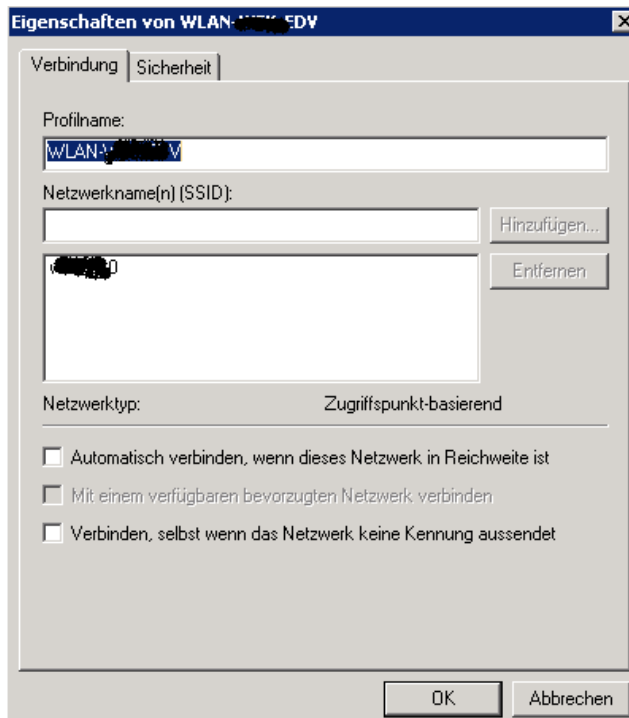


Versionspezifisch

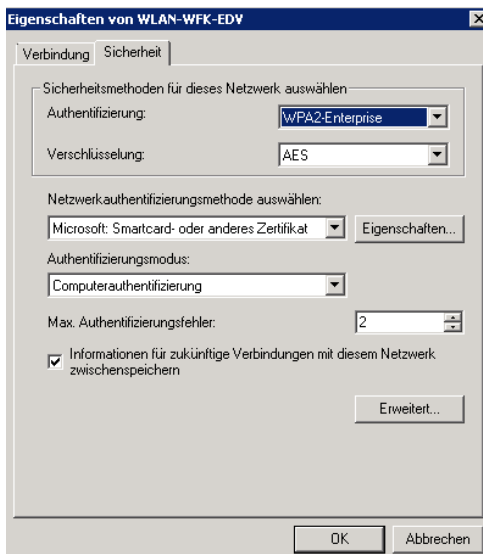


Neue Einstellungen fuer WLAN

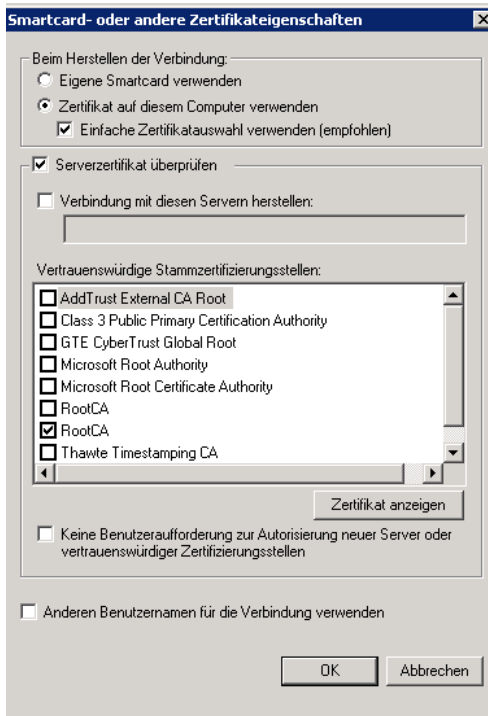




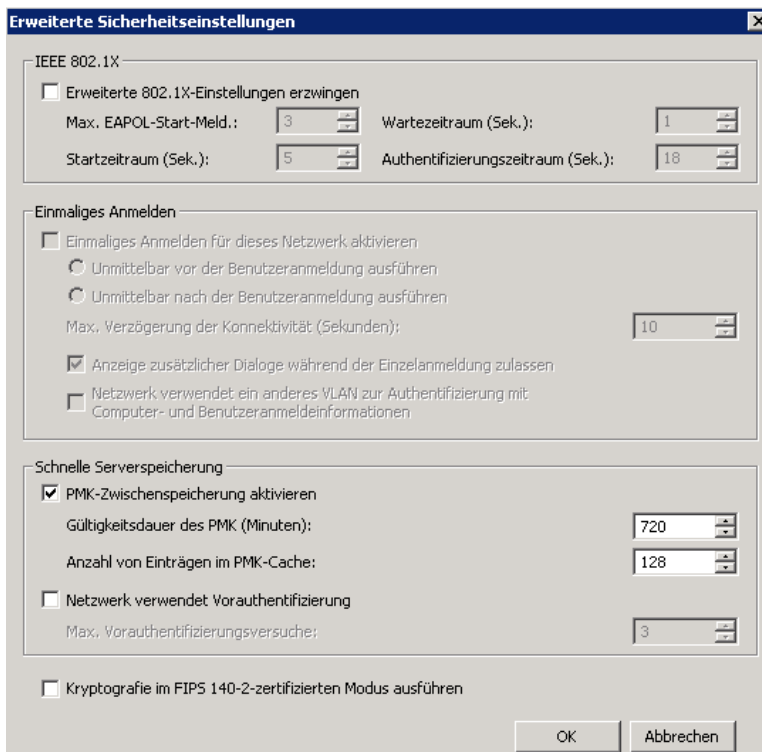
Sicherheitseinstellungen



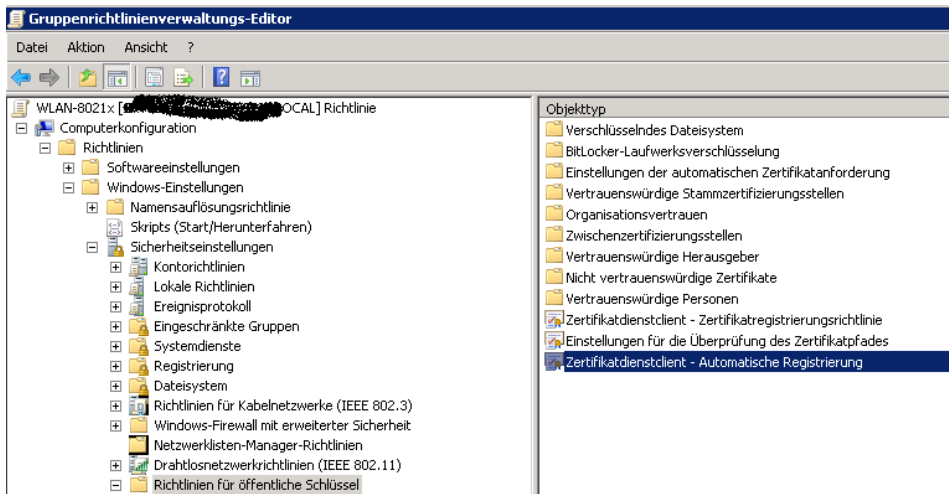
Zugriff auf die interne Zertifizierungsstelle beschaenken



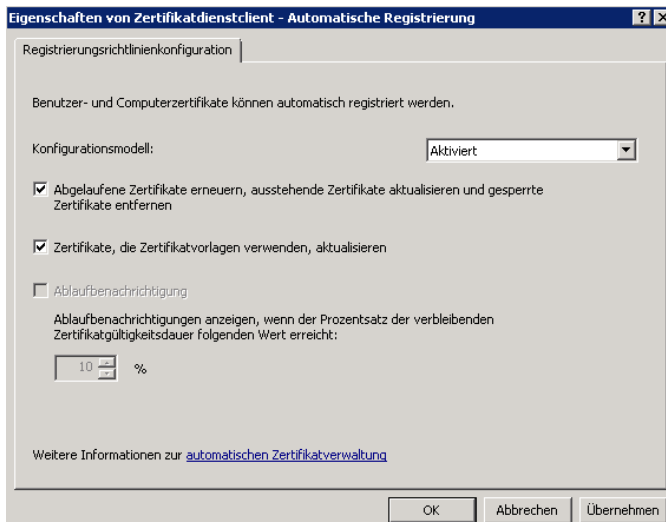
Erweiterte Sicherheitseinstellungen



Autoenrollment fuer Zertifikate in der Gruppenrichtlinie aktivieren



Erweiterte Einstellungen



Neue Zertifikatvorlage fuer 802.1x Authentifizierung

Vorlagenanzzeige	Unterstützte Zertifizierungsstellen (Min.)	Version	Besabsichtigte Zwecke
Administrator	Windows 2000	4.1	
Arbeitsstationsauthentifizierung	Windows Server 2003 Enterprise	101.0	Clientauthentifizierung
Authentifizierte Sitzung	Windows 2000	3.1	
Basis-EFS	Windows 2000	3.1	
Benutzer	Windows 2000	3.1	
CEP-Verschlüsselung	Windows 2000	4.1	
CodeSignatur	Windows 2000	3.1	
Computer	Windows 2000	5.1	
Domänencontroller	Windows 2000	4.1	
Domänencontrollerauthentifizierung	Windows Server 2003 Enterprise	110.0	Clientauthentifizierung, Serverauthentifizierung, Smartcard-Anmeldung
EFS-Wiederherstellungs-Agent	Windows 2000	6.1	
E-Mail-Verschlüsselung	Windows Server 2008 Enterprise	100.6	Sichere E-Mail
E-Mail-Verschlüsselung-XP	Windows Server 2003 Enterprise	100.6	Sichere E-Mail
Exchange-Benutzer	Windows 2000	7.1	
Exchange-Registrierungs-Agent (Offlineinfo...	Windows 2000	4.1	
IPSec	Windows 2000	8.1	
IPSec (Offlineanforderung)	Windows 2000	7.1	
Kerberos-Authentifizierung	Windows Server 2003 Enterprise	110.0	Clientauthentifizierung, Serverauthentifizierung, Smartcard-Anmeldung, KDC-Authentifizierung
Kreuzzertifizierungsstelle	Windows Server 2003 Enterprise	105.0	
Nur Benutzersignatur	Windows 2000	4.1	
Nur Exchange-Signatur	Windows 2000	6.1	
OCSP-Antwortsignatur	Windows Server 2008 Enterprise	101.0	OCSP-Signatur
RAS- und IAS-Server	Windows Server 2003 Enterprise	101.0	Clientauthentifizierung, Serverauthentifizierung
Registrierungs-Agent	Windows 2000	4.1	
Registrierungs-Agent (Computer)	Windows 2000	5.1	
Router (Offlineanforderung)	Windows 2000	4.1	
Schlüsselwiederherstellungs-Agent	Windows Server 2003 Enterprise	105.0	Key Recovery Agent
Smartcard-Anmeldung	Windows 2000	6.1	
Smartcard-Benutzer	Windows 2000	11.1	
Stammzertifizierungsstelle	Windows 2000	5.1	
Untergeordnete Zertifizierungsstelle	Windows 2000	5.1	
Vertrauensitzensignatur	Windows 2000	3.1	
Verzeichnis-E-Mail-Replikation	Windows Server 2003 Enterprise	115.0	Verzeichnisdienst-E-Mail-Replikation
Webserver	Windows 2000	4.1	
Zertifizierungsstellenaustausch	Windows Server 2003 Enterprise	106.0	Archivierung des privaten Schlüssels

Doppelte Vorlage der Computerzertifikatvorlage

Gultigkeit 2 Jahre

Eigenschaften der neuen Vorlage

Antragstellername	Server	Ausstellungsvoraussetzungen
Abgelöste Vorlagen	Erweiterungen	Sicherheit
Allgemein	Anforderungsverarbeitung	Kryptografie

Vorlagenanzzeige:

Unterstützte Zertifizierungsstellen (Min.): Windows Server 2008 Enterprise

Vorlagenname:

Gültigkeitsdauer: Jahre

Erneuerungszeitraum: Wochen

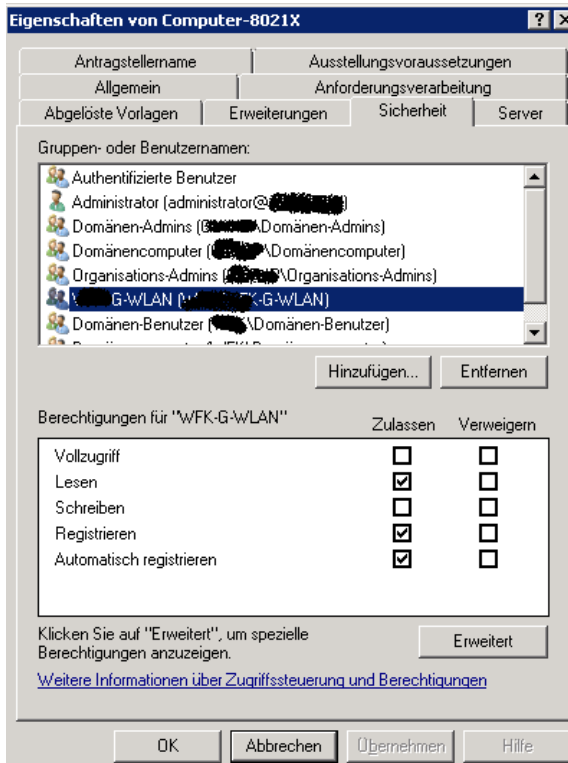
Zertifikat in Active Directory veröffentlichen

Nicht automatisch neu registrieren, wenn ein identisches Zertifikat bereits in Active Directory vorhanden ist

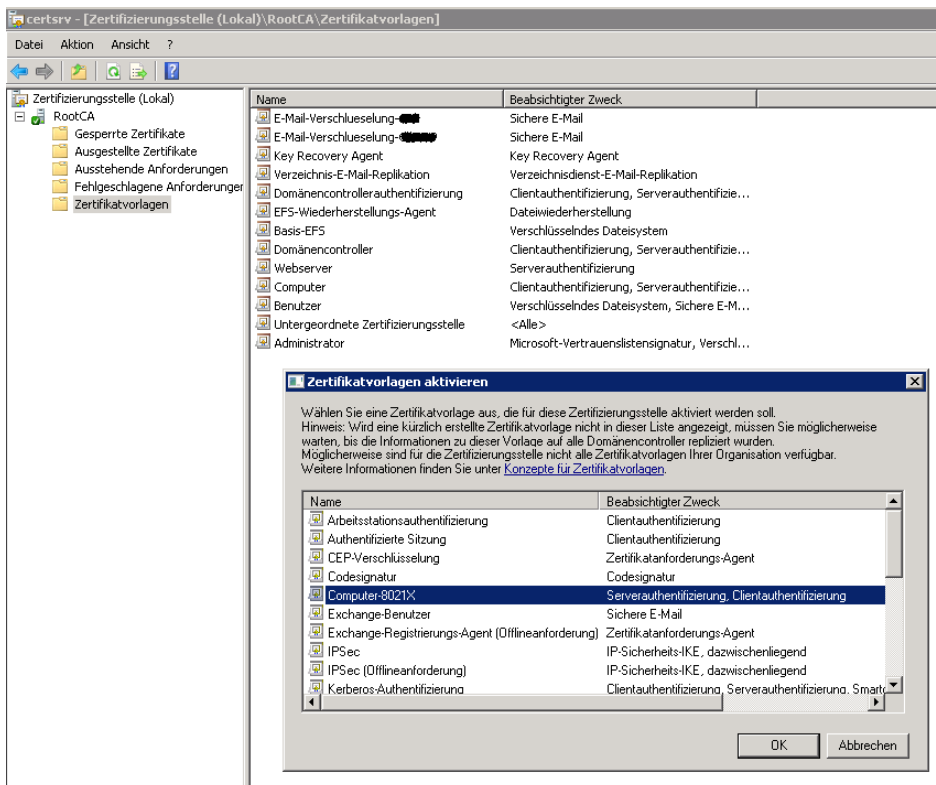
Vorhandenen Schlüssel für automatische Erneuerung von Smartcardzertifikaten verwenden, falls Erstellung eines neuen Schlüssel nicht möglich ist

OK Abbrechen Übernehmen Hilfe

Autoenrollment fuer die Computergruppe erlauben



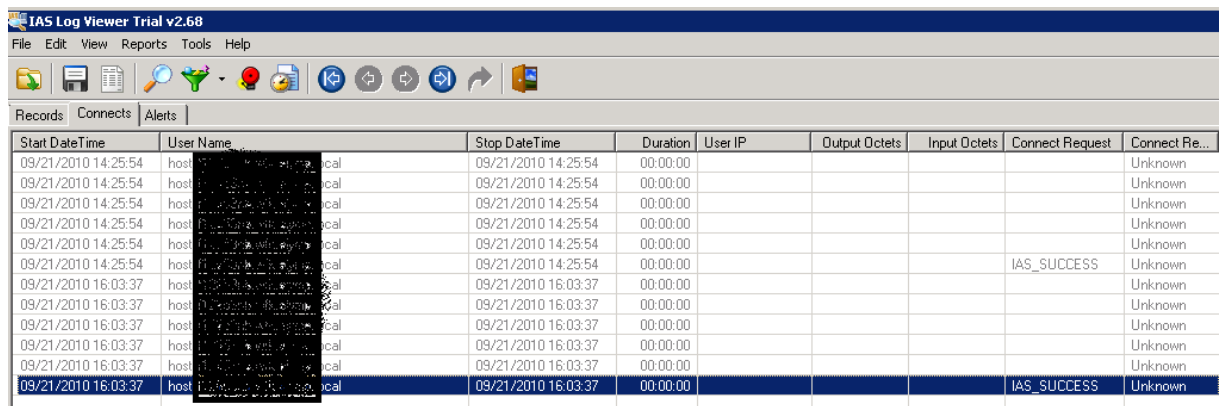
Zertifikatvorlage aktivieren



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



The screenshot shows the IAS Log Viewer interface with a table of log entries. The table has columns for Start DateTime, User Name, Stop DateTime, Duration, User IP, Output Octets, Input Octets, Connect Request, and Connect Re... (truncated). The User Name column contains redacted information. The Connect Request column shows 'IAS_SUCCESS' for two entries.

Start DateTime	User Name	Stop DateTime	Duration	User IP	Output Octets	Input Octets	Connect Request	Connect Re...
09/21/2010 14:25:54	host	09/21/2010 14:25:54	00:00:00					Unknown
09/21/2010 14:25:54	host	09/21/2010 14:25:54	00:00:00					Unknown
09/21/2010 14:25:54	host	09/21/2010 14:25:54	00:00:00					Unknown
09/21/2010 14:25:54	host	09/21/2010 14:25:54	00:00:00					Unknown
09/21/2010 14:25:54	host	09/21/2010 14:25:54	00:00:00				IAS_SUCCESS	Unknown
09/21/2010 16:03:37	host	09/21/2010 16:03:37	00:00:00					Unknown
09/21/2010 16:03:37	host	09/21/2010 16:03:37	00:00:00					Unknown
09/21/2010 16:03:37	host	09/21/2010 16:03:37	00:00:00					Unknown
09/21/2010 16:03:37	host	09/21/2010 16:03:37	00:00:00					Unknown
09/21/2010 16:03:37	host	09/21/2010 16:03:37	00:00:00				IAS_SUCCESS	Unknown

Weitere optionale Moeglichkeiten:

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