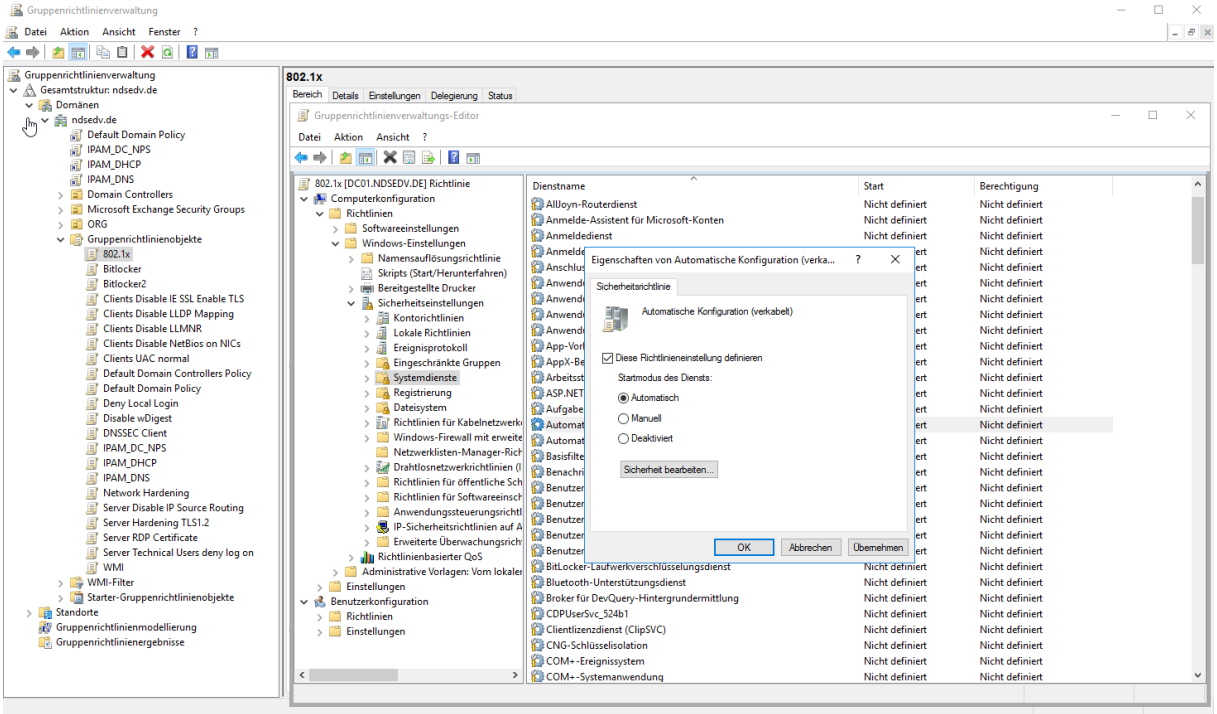
Einfache Port-Security umsetzen

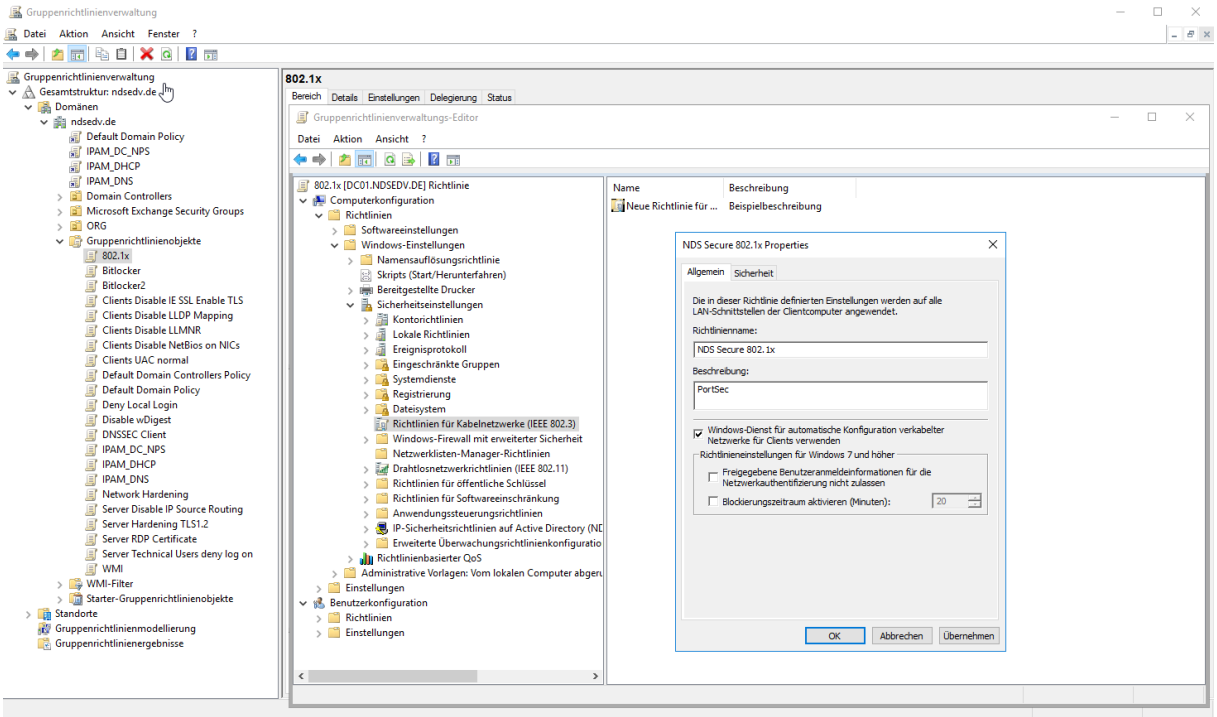
Ich setze jetzt voraus, das der/die Switch(e) z.B. Cisco Catalyst 3560-CG entsprechend für die Port-Security vorbereitet sind, genauso wie die Windows Server Rolle „Netzwerkrichtlinien- und Zugriffsdienste" konfiguriert sind. Als nächstes erstellen wir ein neues GPO und nehmen folgende Konfiguration vor.

Hinweis: 802.1x schützt ausschließlich den Zugang zum physikalischen Netzwerk

Aktivieren den lokalen Dienst „Automatische Konfiguration (verkabelt)" auf den Clientsystemen.

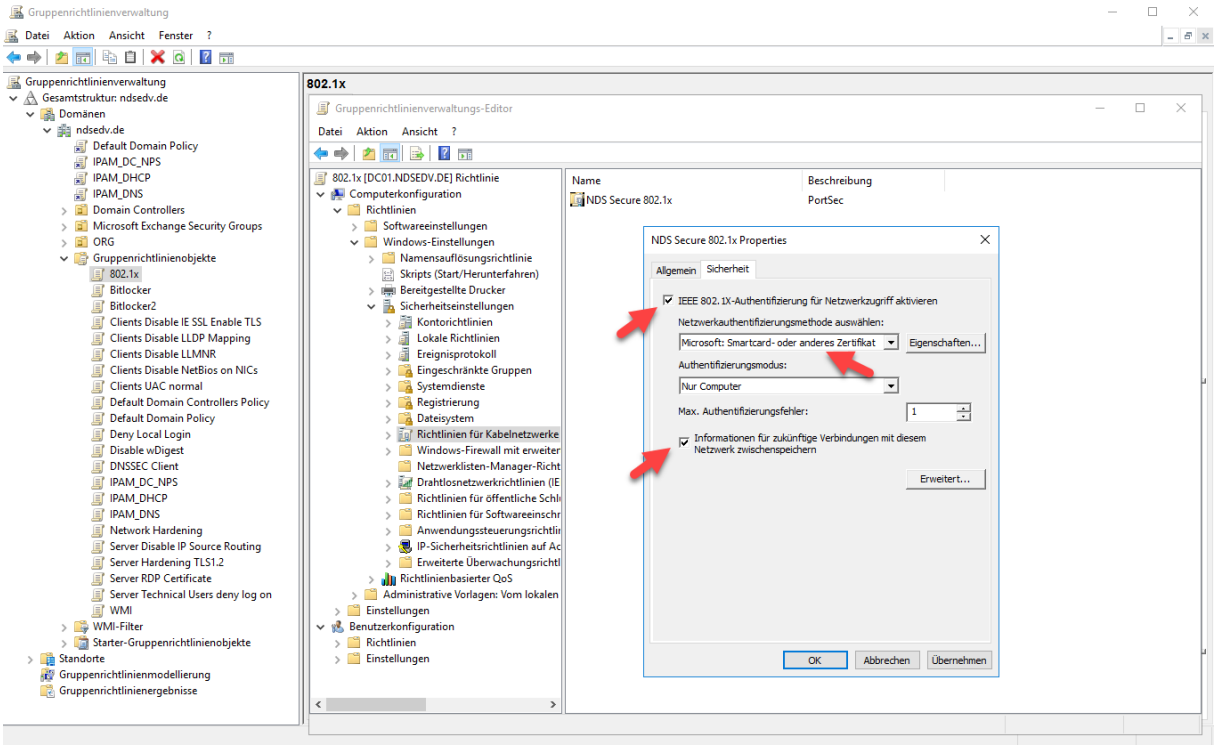


Die Richtlinien für Kabelnetzwerke (IEEE 802.3) nehmen wir wie folgt vor:

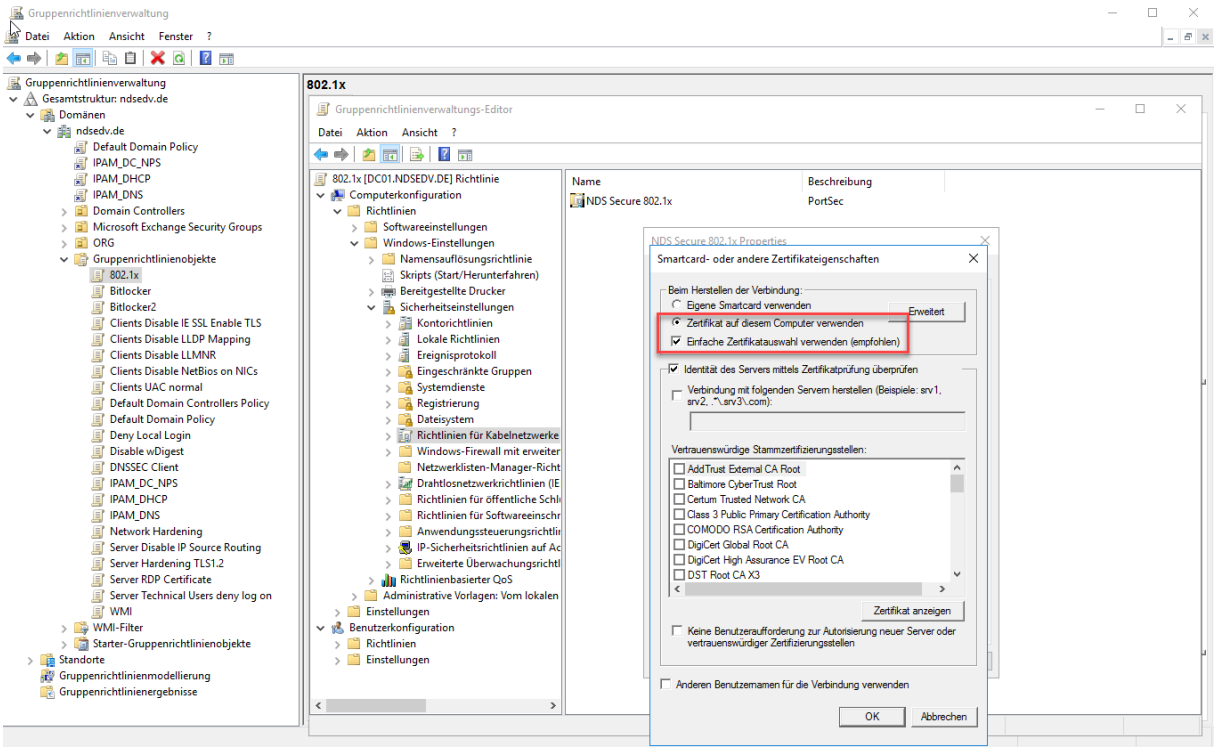


Einfache Port-Security umsetzen

Über den Reiter Sicherheit setzen wir folgende Optionen und Einstellungen fest.

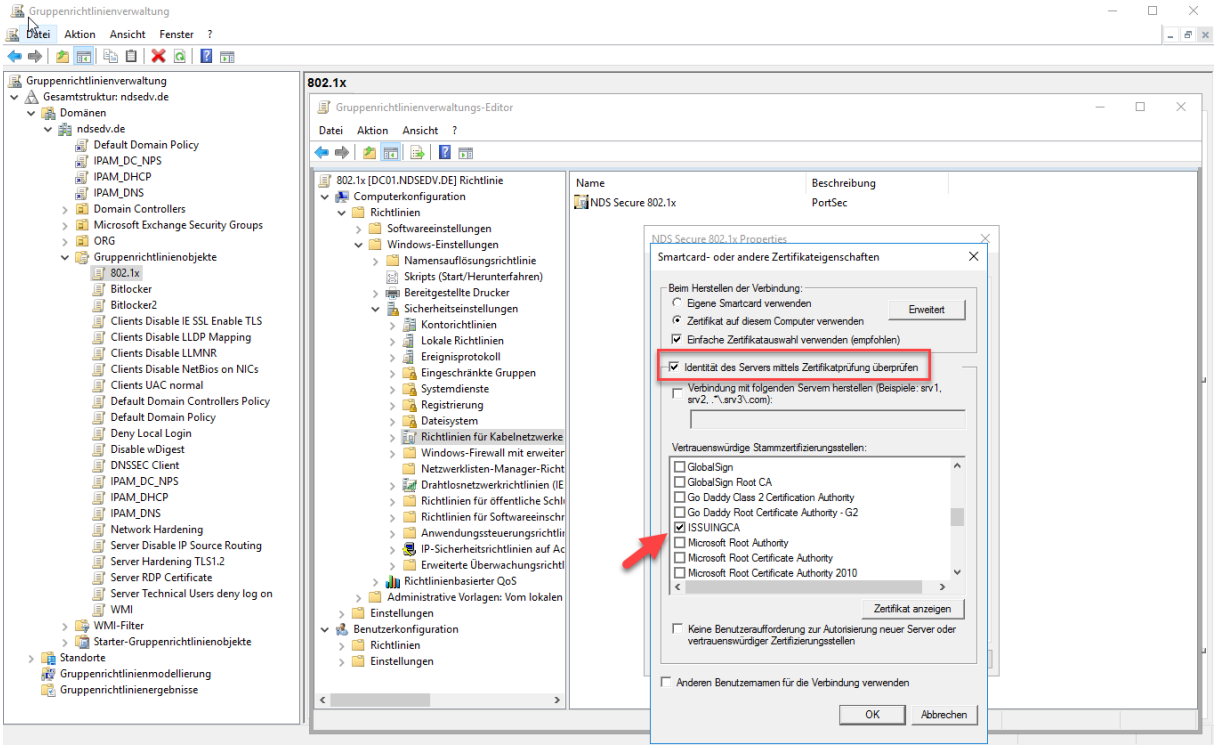


Über Eigenschaften nehmen wir weitere Einstellungen vor und zwar die zertifikatsbasierte Authentifizierung.

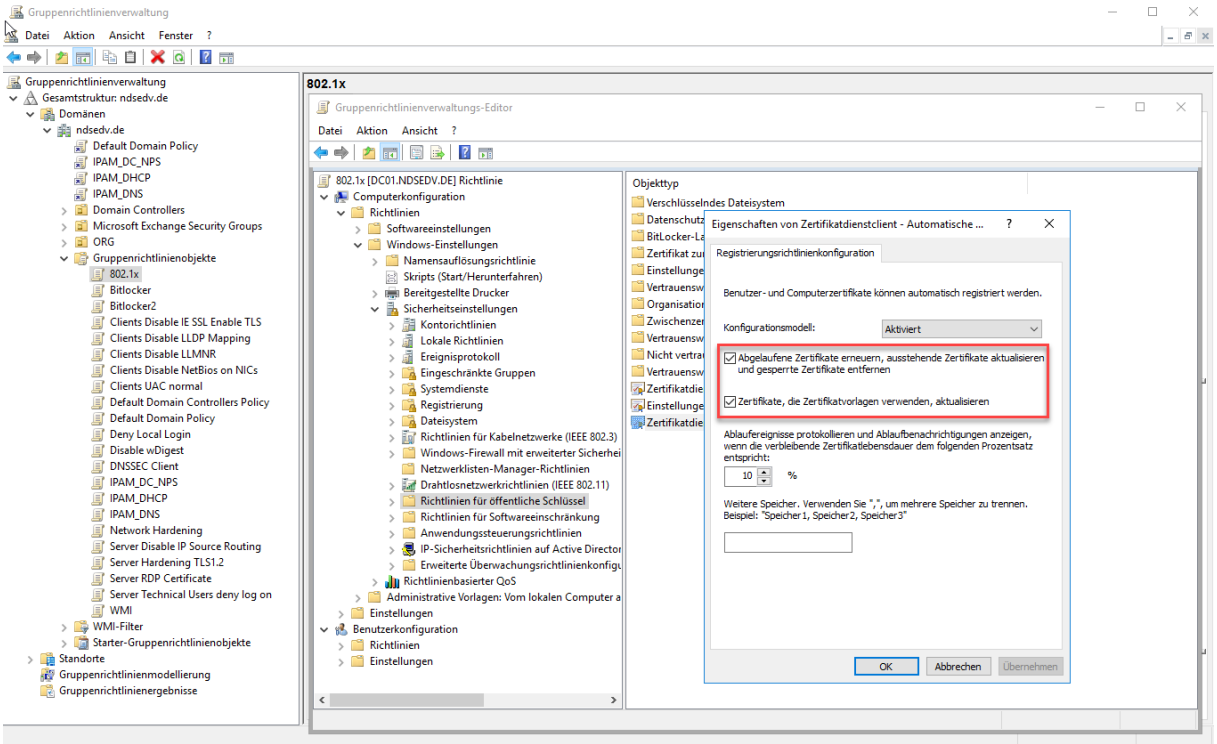


Einfache Port-Security umsetzen

Aktivieren das Zertifikat der internen CA.



Aktivieren die automatische Zertifikatserneuerung.



Einfache Port-Security umsetzen

Nachfolgend der Bericht des neuen GPO 802.1x.

802.1x
Daten ermittelt am: 27.12.2017 17:10:05

Alle ausblenden

Allgemein

Ausblenden

Details

Ausblenden

Domäne	ndsedv.de
Besitzer	NDSEDV\Domänen-Admins
Erstellt	27.12.2017 16:58:12
Geändert	27.12.2017 17:07:14
Benutzerrevisionen	1 (AD), 1 (SYSVOL)
Computerrevisionen	6 (AD), 6 (SYSVOL)
Eindeutige ID	{1CC1A385-9265-45D9-A151-1DA56318EE93}
GPO-Status	Benutzereinstellungen deaktiviert

Verknüpfungen

Ausblenden

Standort	Erzwungen	Verknüpfungsstatus	Pfad
Keine			

Die Liste enthält Verknüpfungen zur Domäne des Gruppenrichtlinienobjekts.

Sicherheitsfilterung

Ausblenden

Die Einstellungen dieses Gruppenrichtlinienobjekts können nur auf folgenden Gruppen, Benutzer und Computer angewendet werden:

Name
NT-AUTORITÄT\Authentifizierte Benutzer

Delegierung

Ausblenden

Folgende Gruppen und Benutzer haben die angegebene Berechtigung für das Gruppenrichtlinienobjekt

Name	Zulässige Berechtigungen	Geerbt
NDSEDV\Domänen-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NDSEDV\Organisations-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NT-AUTORITÄT\Authentifizierte Benutzer	Lesen (durch Sicherheitsfilterung)	Nein
NT-AUTORITÄT\DOMÄNENCONTROLLER DER ORGANISATION	Lesen	Nein
NT-AUTORITÄT\SYSTEM	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein

Computerkonfiguration (Aktiviert)

Ausblenden

Richtlinien

Ausblenden

Windows-Einstellungen

Ausblenden

Sicherheitseinstellungen

Ausblenden

Systemdienste

Ausblenden

Automatische Konfiguration (verkabelt) (Startmodus: Automatisch)

Ausblenden

Berechtigungen
Keine Berechtigungen angegeben

Überwachung
Keine Überwachung angegeben

Richtlinien für verkabeltes Netzwerk (802.3)

Ausblenden

NDS Secure 802.1x

Ausblenden

Name	NDS Secure 802.1x
Beschreibung	PortSec

Globale Einstellungen

Ausblenden

Einstellung	Wert
Windows-Netzwerkdienste für verkabeltes LAN verwenden	Aktiviert
Freigegebene Benutzeranmeldeinformationen für die Netzwerkauthentifizierung	Aktiviert

Netzwerkprofil

Ausblenden

Sicherheitseinstellungen

Ausblenden

Verwendung der IEEE 802.1X-Authentifizierung für den Netzwerkzugriff aktivieren	Aktiviert
Verwendung der IEEE 802.1X-Authentifizierung für den Netzwerkzugriff erzwingen	Deaktiviert

IEEE 802.1X-Einstellungen

Ausblenden

Computerauthentifizierung	Nur Computer
Maximale Anzahl an Authentifizierungsfehlern	1
Maximale Anzahl an gesendeten EAPOL-Startmeldungen	
Wartezeitraum (Sekunden)	
Startzeitraum (Sekunden)	
Authentifizierungszeitraum (Sekunden)	

Eigenschaften für Netzwerkauthentifizierungsmethode

Ausblenden

Authentifizierungsmethode	Smartcard oder Zertifikat
Serverzertifikat überprüfen	Aktiviert
Verbindung mit folgenden Servern herstellen	
Keine Benutzeraufforderung zur Autorisierung neuer Server oder vertrauenswürdiger Zertifizierungsstellen	Deaktiviert
Zertifikat auf diesem Computer verwenden	Aktiviert
Einfache Zertifikatauswahl verwenden	Aktiviert
Anderen Benutzernamen für die Verbindung verwenden	Deaktiviert

Richtlinien für öffentliche Schlüssel/Zertifikatdienstclient - Einstellung für die automatische Registrierung

Ausblenden

Richtlinie	Einstellung
Automatische Zertifikatverwaltung	Aktiviert

Option	Einstellung
Neue Zertifikate registrieren, abgelaufene Zertifikate erneuern, ausstehende Anforderungen für Zertifikate verarbeiten und gesperrte Zertifikate entfernen	Aktiviert
Zertifikate, die Zertifikatvorlagen von Active Directory verwenden, aktualisieren und verwalten	Aktiviert

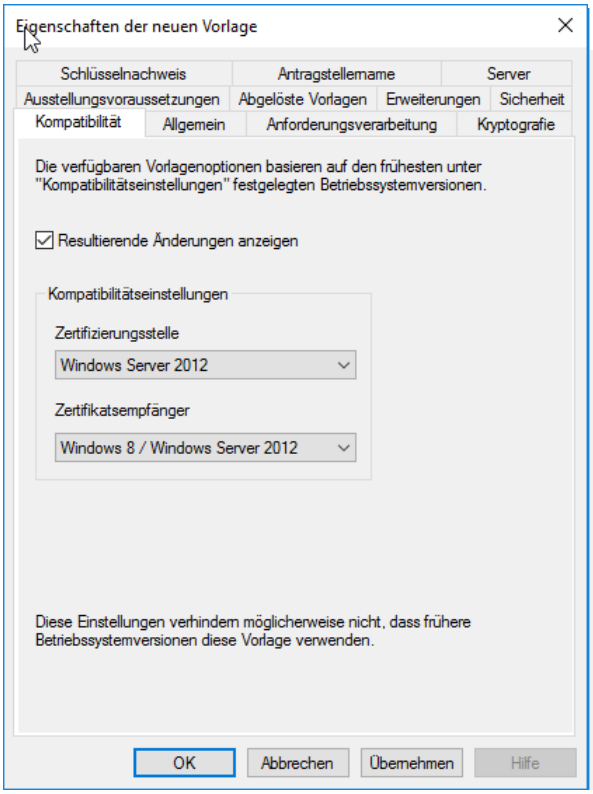
Benutzerkonfiguration (Deaktiviert)

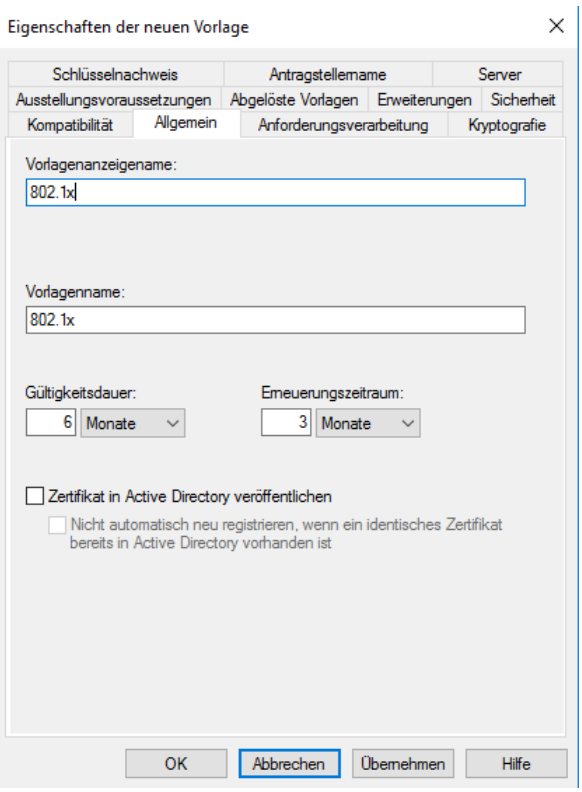
Ausblenden

Keine Einstellungen definiert

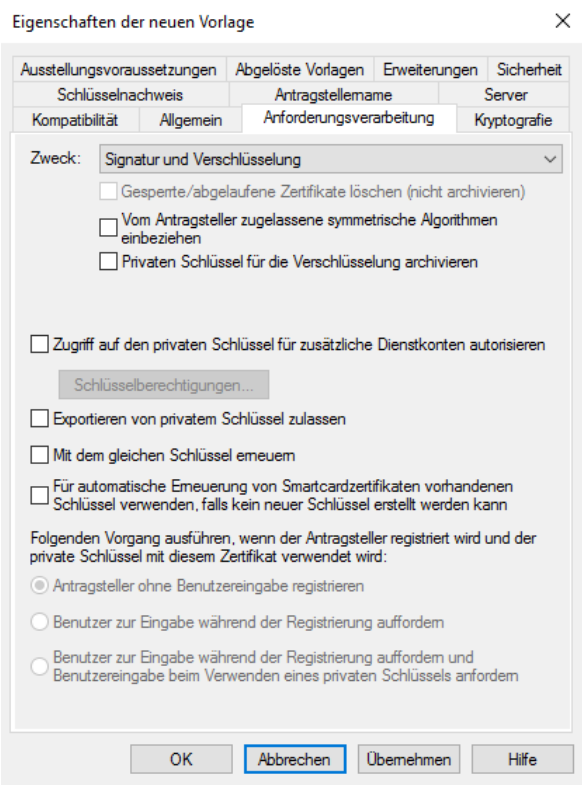
Einfache Port-Security umsetzen

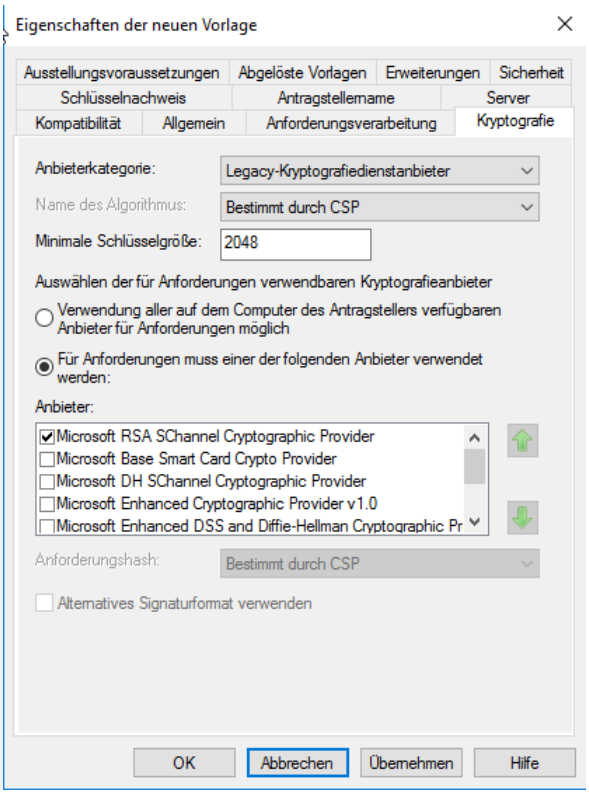
Erstellen auf der CA ein neues Template und setzen die Einstellungen in etwas so. Abhängig von der lokalen Infrastruktur.





Bei der Kryptografie muss man auf die Kompatibilität der Infrastruktur schauen.

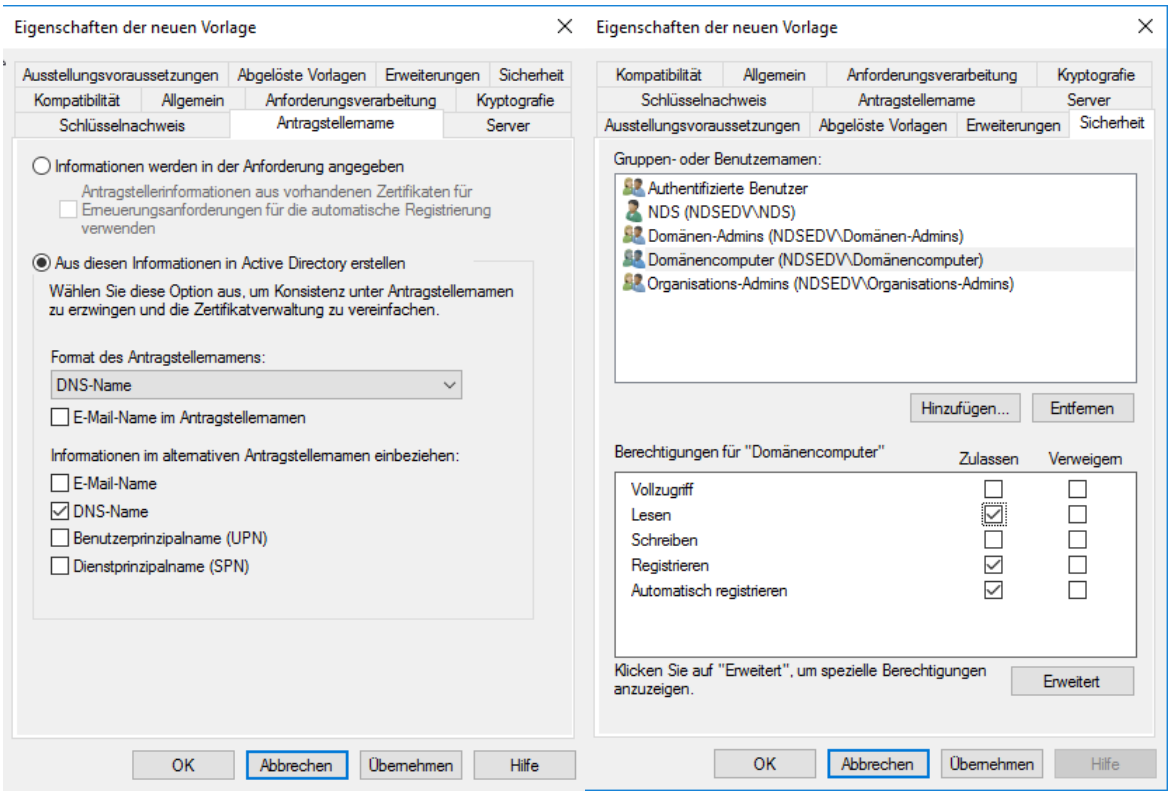




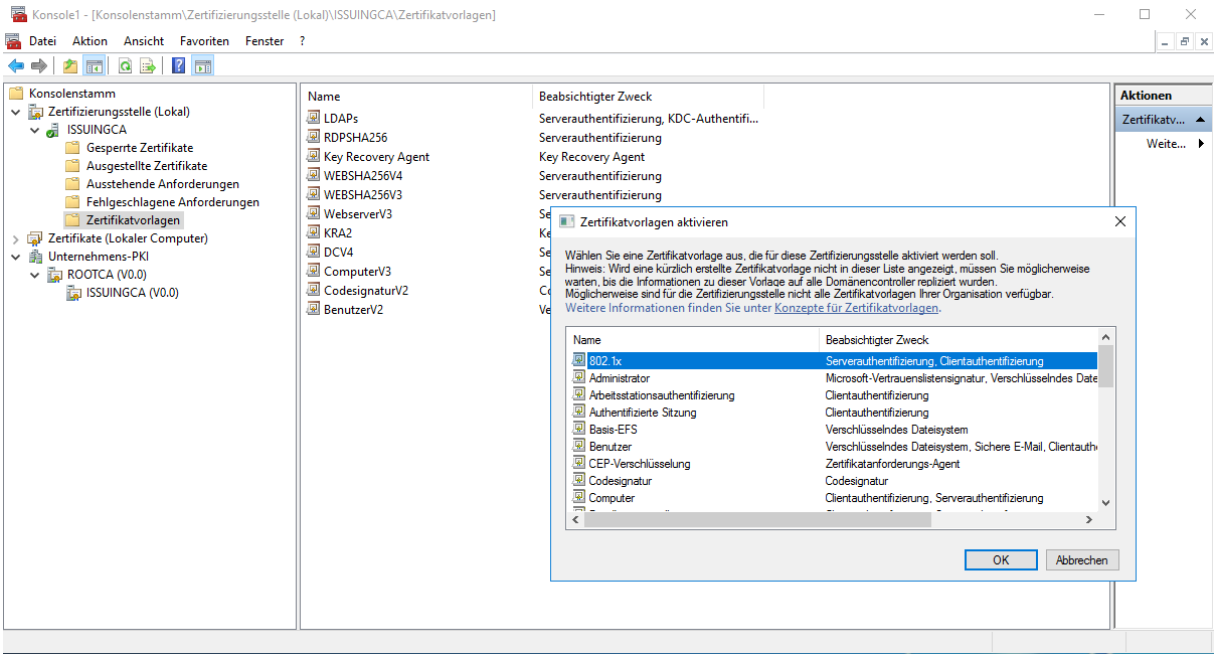
Einfache Port-Security umsetzen

Für den automatischen roll-out benötigt der Client das Recht für die automatische Registrierung und das Zertifikat muss mit dem DNS Namen des Clients erstellt werden.

Ich erstelle grundsätzlich immer eine neue Sicherheitsgruppe und füge die Clientsysteme hinzu und berechtige diese dann auf das Template.

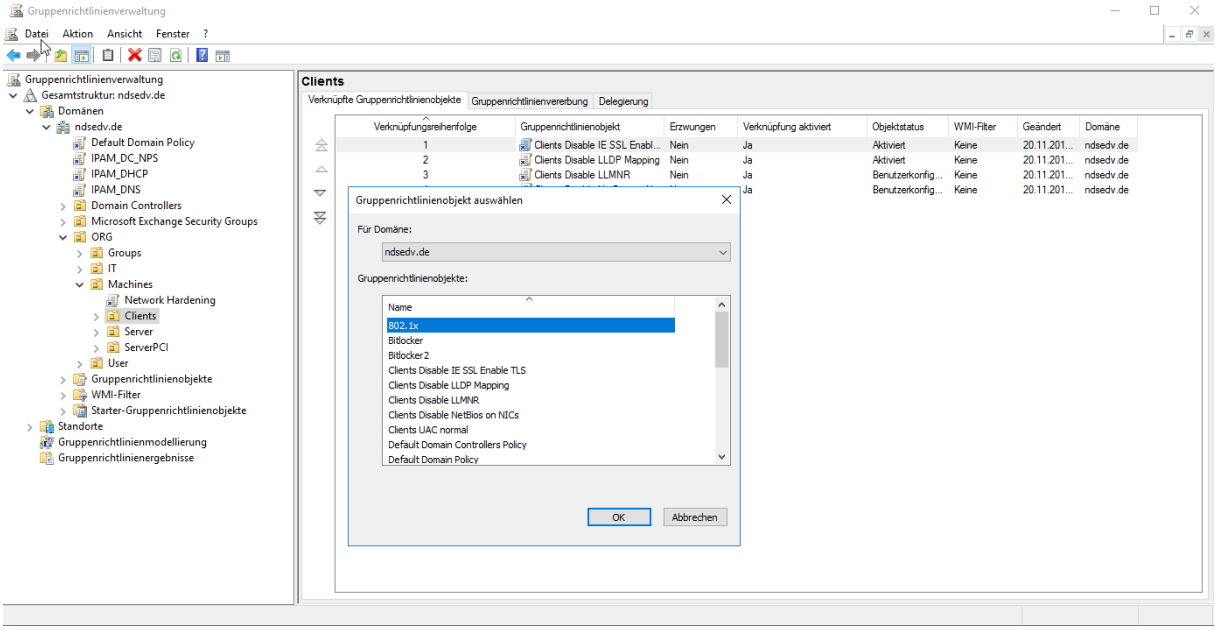


Template zum Abschluss noch veröffentlichen.

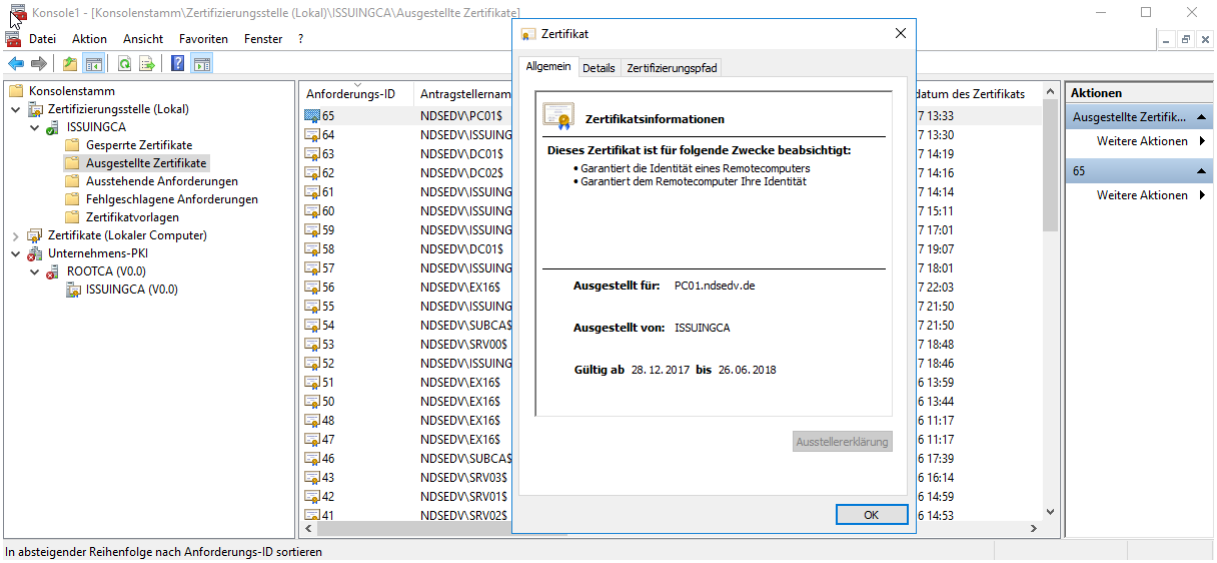


Einfache Port-Security umsetzen

Das neue GPO muss nur noch auf die entsprechende OU verlinkt werden.

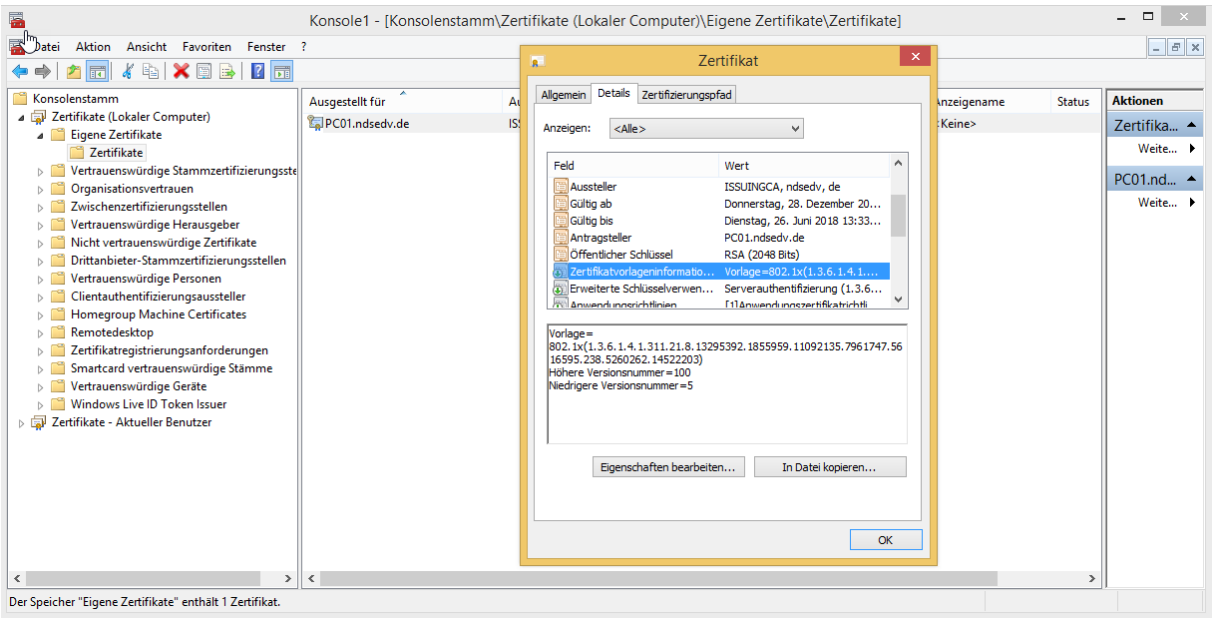
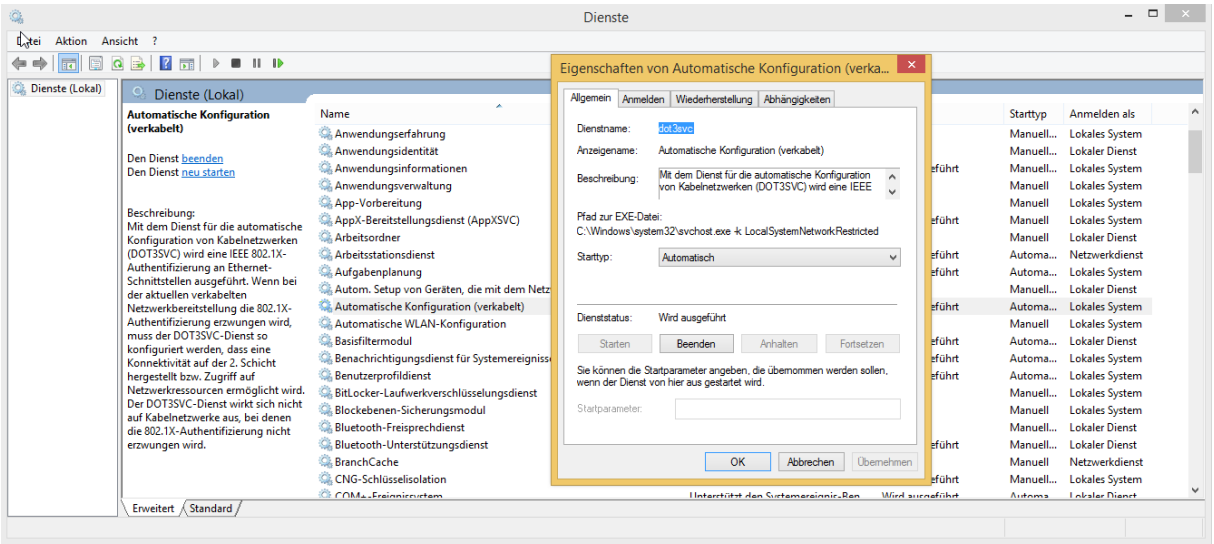


Nach einem Neustart der Clients bekommen diese automatisch ein Zertifikat ausgestellt.



Einfache Port-Security umsetzen

Auf dem Client PC01 die MMC gestartet und das Snap-In Zertifikate hinzugefügt.



Auch der Dienst „Automatische Konfiguration (verkabelt)" wurde gestartet und auf den Starttyp „Automatisch" gestellt.