

Network Access Protection

mit Windows Server 2012 – Funktion 802.1x

Inhaltsverzeichnis

1	VORBEREITUNGEN	3
2	ACTIVE DIRECTORY	4
2.1	Installation	4
2.2	Konfiguration	8
2.3	Aufbau der OU-Struktur	11
3	ROLLE CA	11
4	CLIENT	19
5	DHCP	20
5.1	Installation	20
5.2	Konfiguration	24
6	ZERTIFIKAT	28
7	NETWORK POLICY SERVER	31
7.1	Installation	31
7.2	Konfiguration NPS	34
7.3	Gruppenrichtlinie	45
8	SWITCH	49
8.1	Cisco	49
8.2	Switch	52
8.3	Zyxel	53
9	ERGEBNIS	54
10	KONTROLLEN	55

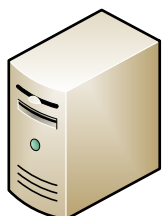
1 Vorbereitungen

Vorausgesetzt werden zwei Windows Server 2012 und ein Windows 8 Client sowie ein Switch. Der erste Windows Server 2012 erhält die fixe IP-Adresse 192.168.15.10, der zweite die IP-Adresse 192.168.15.15. Der Switch wird mit der IP-Adresse 192.168.15.20 konfiguriert.

Zwei VLANs werden angelegt:

- VLAN2: NonCompliant
- VLAN3: Compliant

Die Ports 1-4 des Switches werden auf VLAN3 konfiguriert, der Port 5 wird per Radius / NPS zugewiesen.



192.168.15.10

Installierte Rollen:

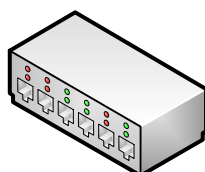
- Active Directory
- DNS
- Certificate Authority



192.168.15.15

Installierte Rollen:

- DHCP
- NPS



Switch

192.168.15.20

VLAN 2: NonCompliant

VLAN 3: Compliant

Ports 1-4: VLAN3

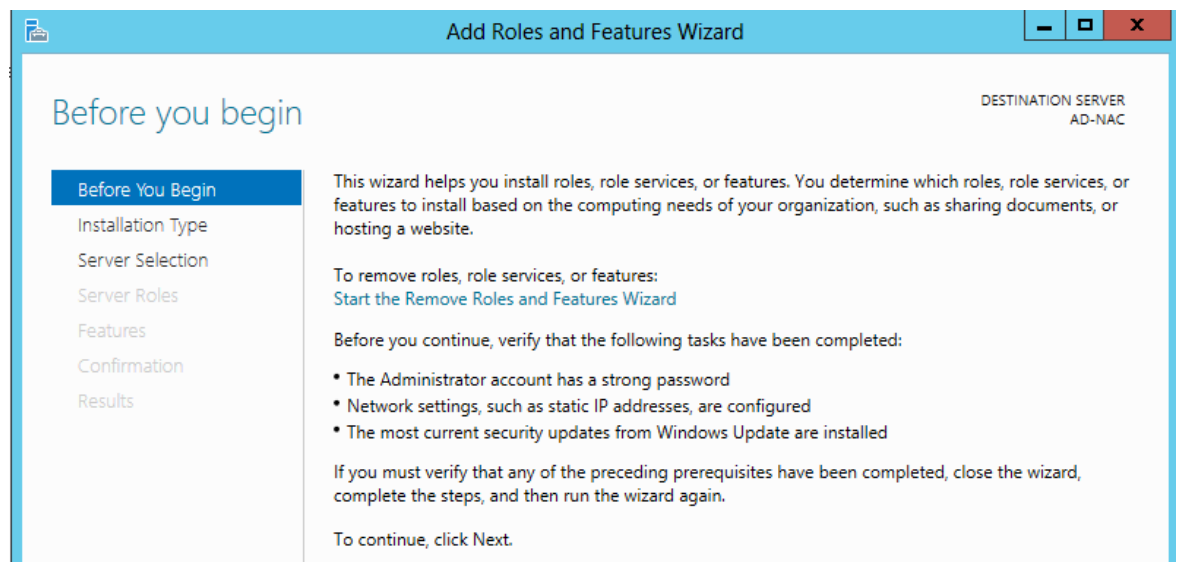
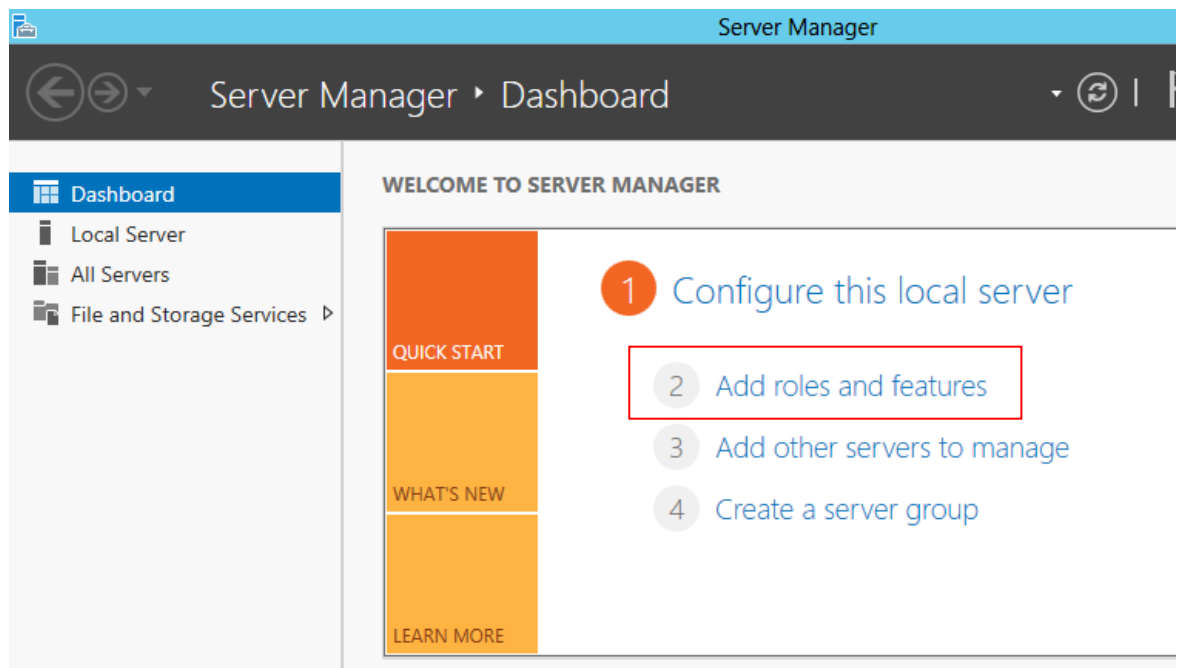
Port 5: per Radius/NPS



2 Active Directory

2.1 Installation

Als erstes wird im Server Manager die Rolle Active Directory Domain Services ausgewählt und installiert.



Die Rolle wird für diesen Server installiert.

Add Roles and Features Wizard

DESTINATION SERVER
AD-NAC

Select installation type

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Add Roles and Features Wizard

DESTINATION SERVER
AD-NAC

Select destination server

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
AD-NAC	192.168.15.10	Microsoft Windows Server 2012 Standard Evaluation

Die Rolle „Active Directory Domain Services“ wird angewählt,

Add Roles and Features Wizard

DESTINATION SERVER
AD-NAC

Select server roles

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

Select one or more roles to install on the selected server.

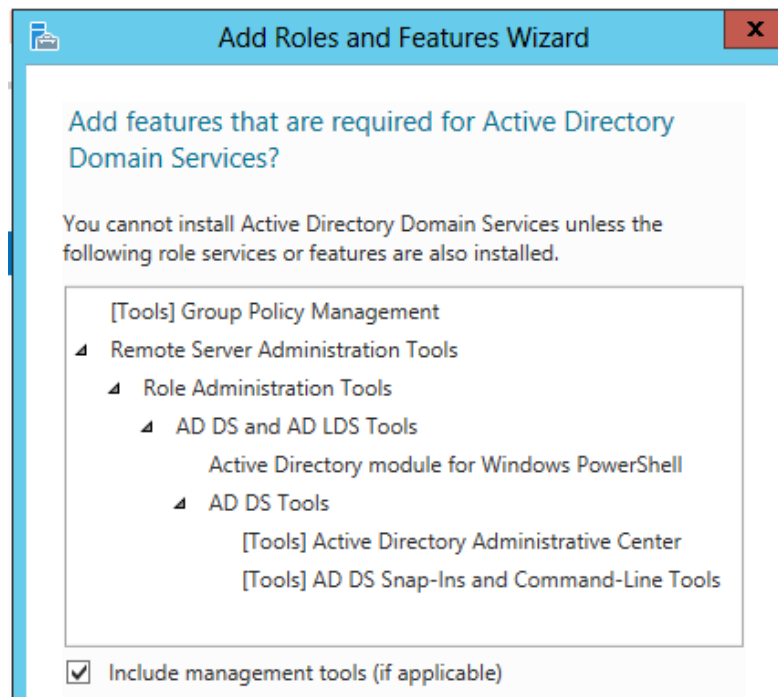
Roles

☐ Active Directory Certificate Services
☒ **Active Directory Domain Services**
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Application Server
☐ DHCP Server

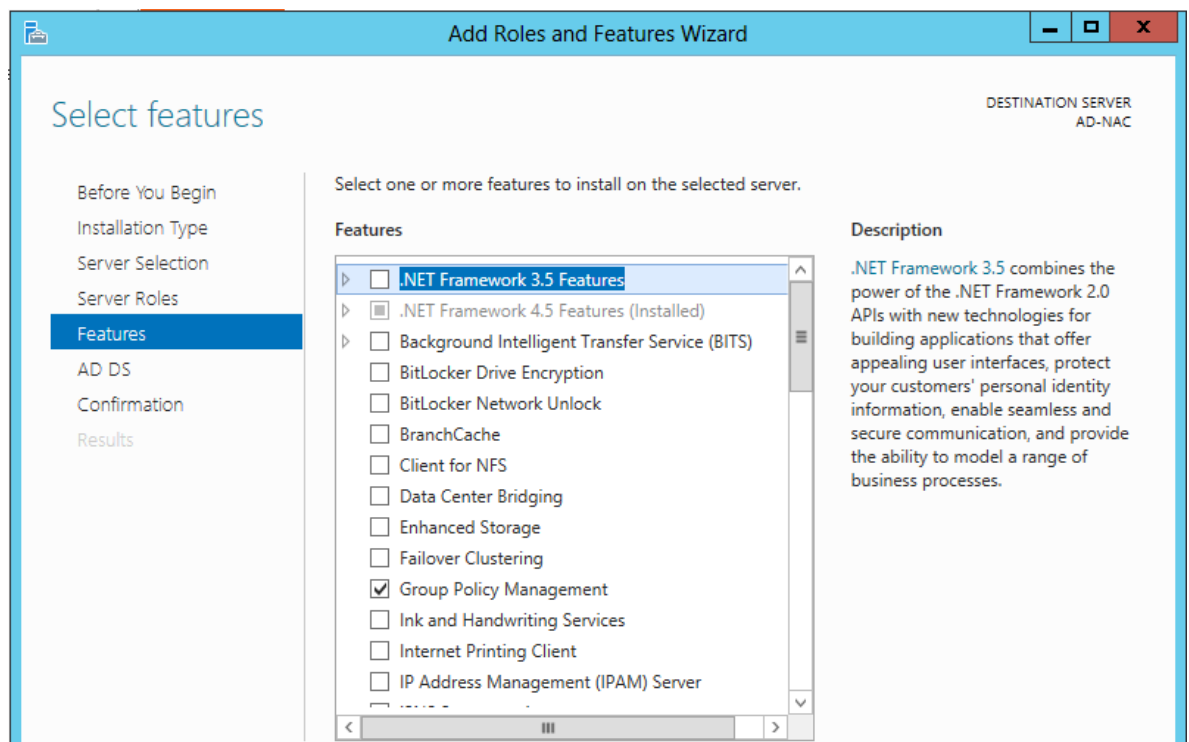
Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

und die notwendigen Features übernommen.



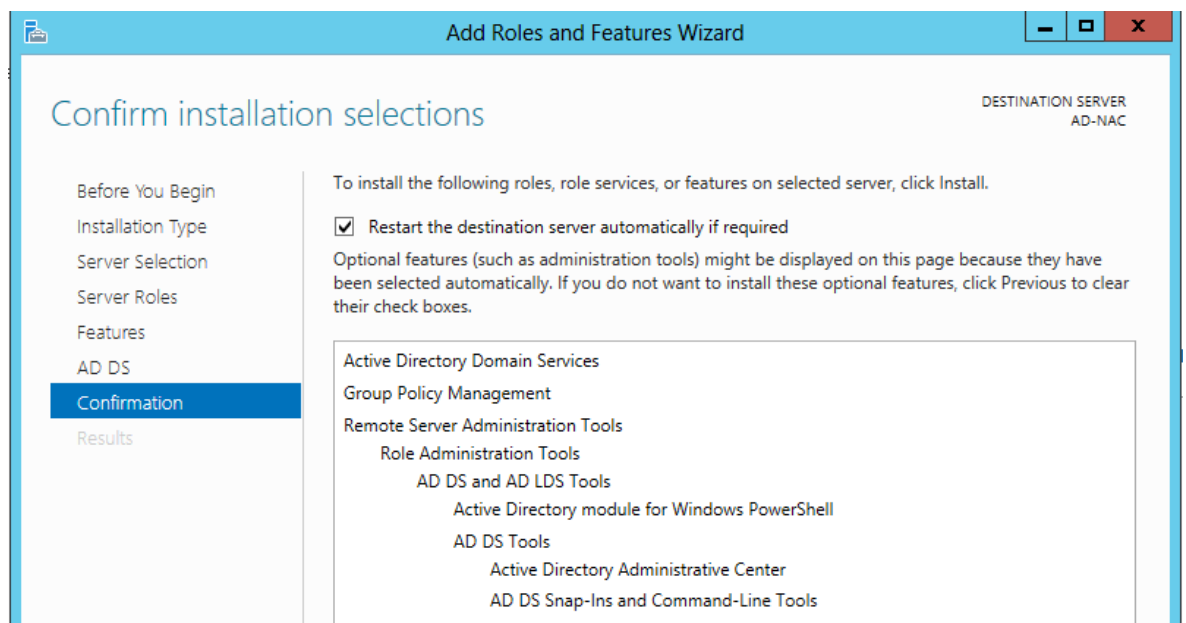
Und anschliessend die vorgeschlagenen Features übernehmen.



Danach folgen die Informationen zur Rolle „Active Directory Domain Services“...



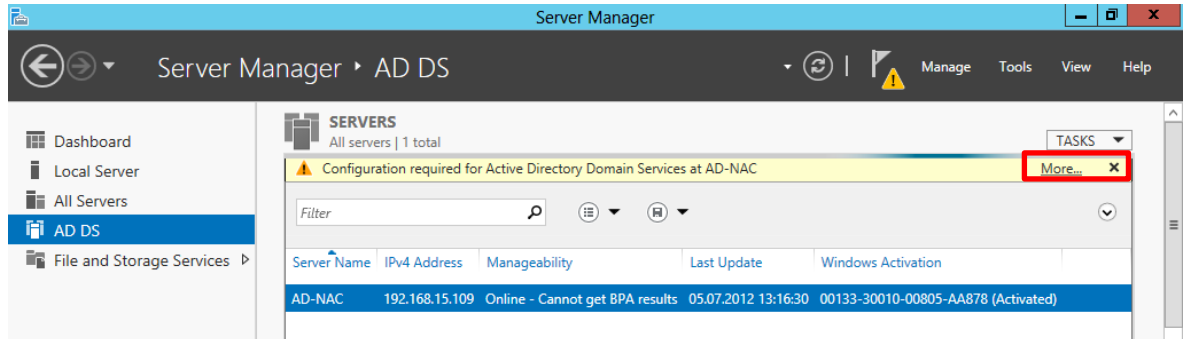
... die im nächsten Schritt zusammengefasst und bestätigt werden können. Falls notwendig, wird der Server bei gesetztem Häkchen automatisch neu gestartet.



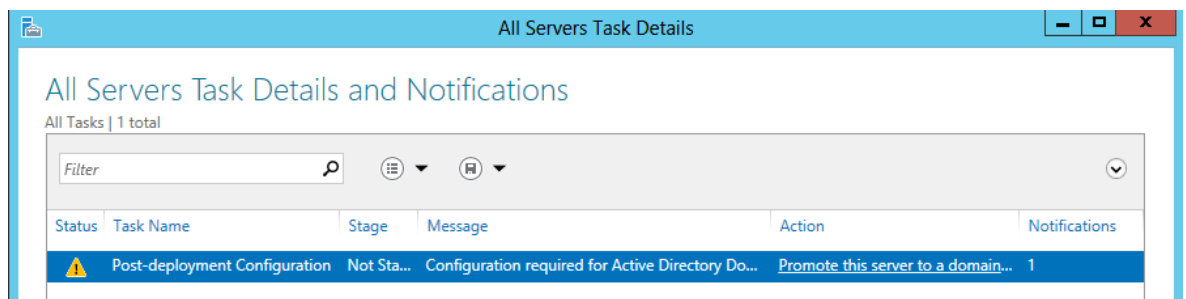
Nach Abschluss der Installation kann die Rolle AD DS konfiguriert werden.

2.2 Konfiguration

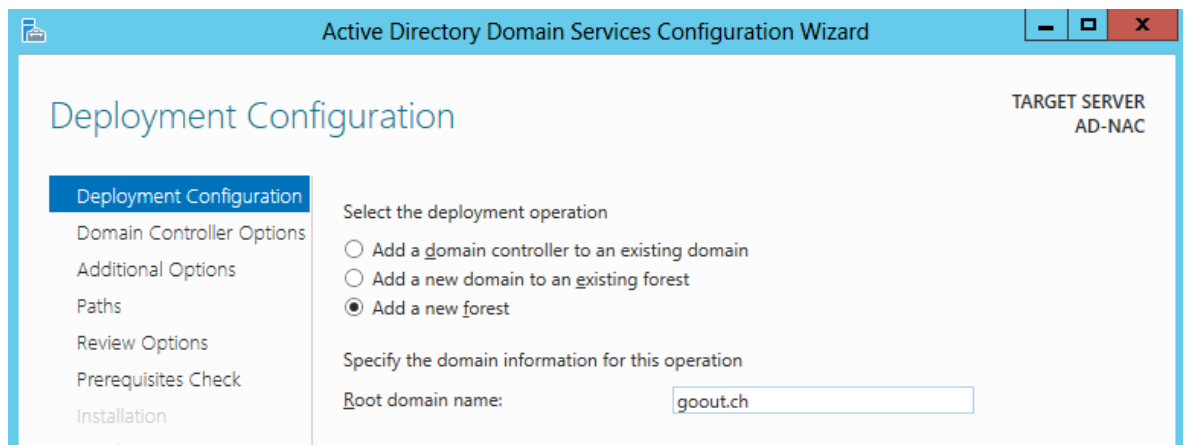
Um den AD Dienst zu konfigurieren, wird auf „More..“ im gelben Kästchen geklickt.



Mit einem Klick auf „Promote this server to a domain controller“ wird der Vorgang gestartet.



Es wird eine neue Domäne mit dem Namen „goout.ch“ angelegt.



Der Funktionslevel der Domäne und des Forest werden auf „Windows Server 2012“ belassen. Zusätzlich wird der DNS Server installiert.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
AD-NAC

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012

Domain functional level: Windows Server 2012

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

Die Fehlermeldung ist „normal“ und kann ignoriert werden.

Active Directory Domain Services Configuration Wizard

DNS Options

TARGET SERVER
AD-NAC

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Specify DNS delegation options

☐ Create DNS delegation

A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... Show more

Der vorgeschlagene NetBIOS Name wird übernommen.

Active Directory Domain Services Configuration Wizard

Additional Options

TARGET SERVER
AD-NAC

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: GOOUT

Auch die Standardpfade werden übernommen.

Active Directory Domain Services Configuration Wizard

Paths

TARGET SERVER
AD-NAC

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

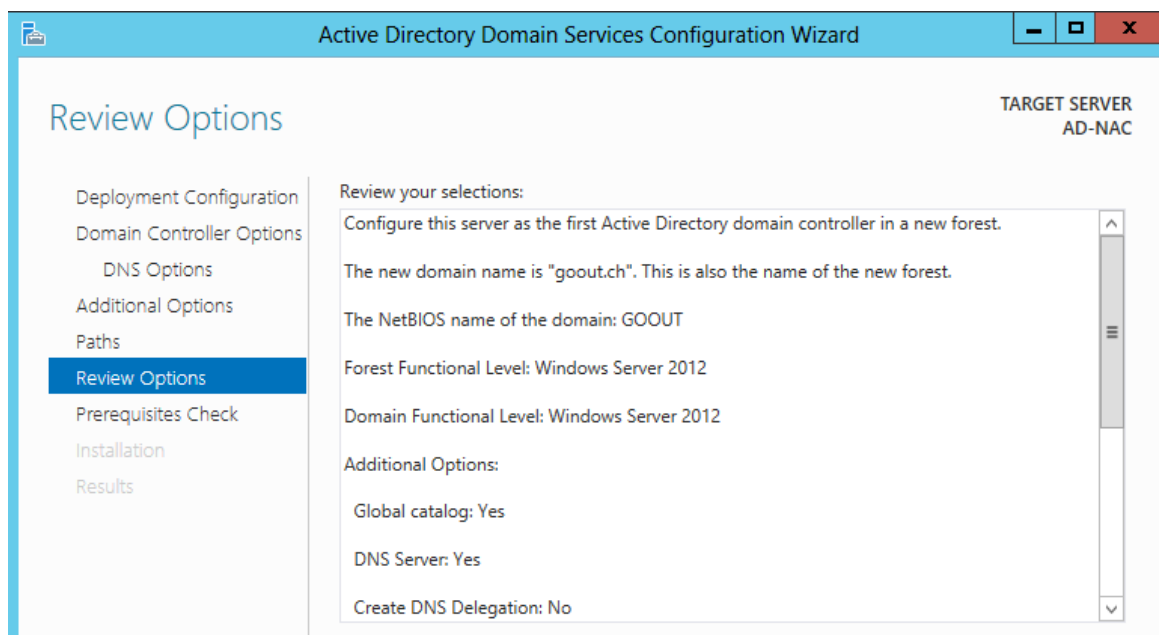
Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS

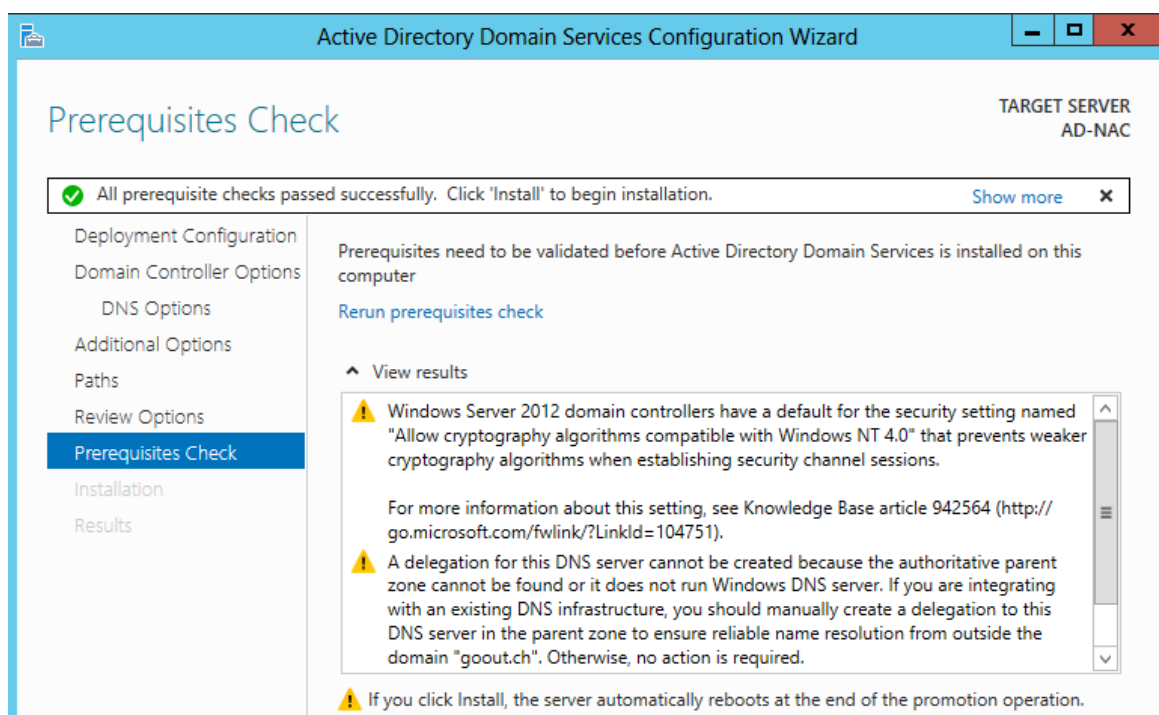
Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

Die gemachten Angaben werden nochmals angezeigt.

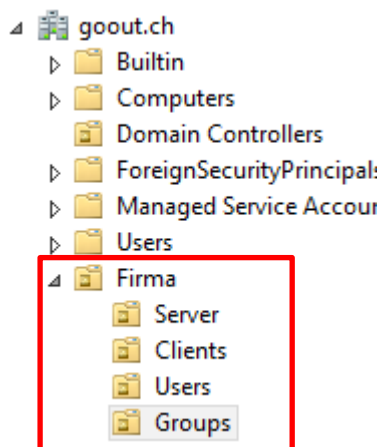


Die Abhängigkeiten werden überprüft und angezeigt. Danach kann die Installation gestartet werden.



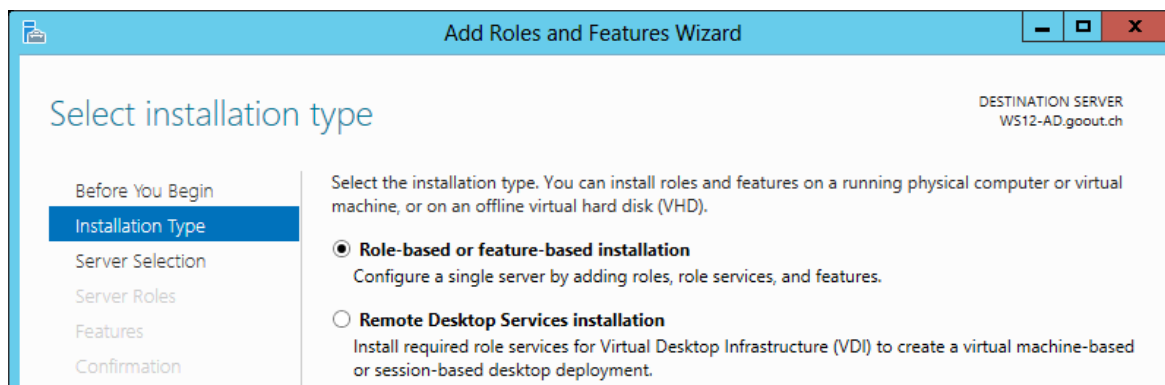
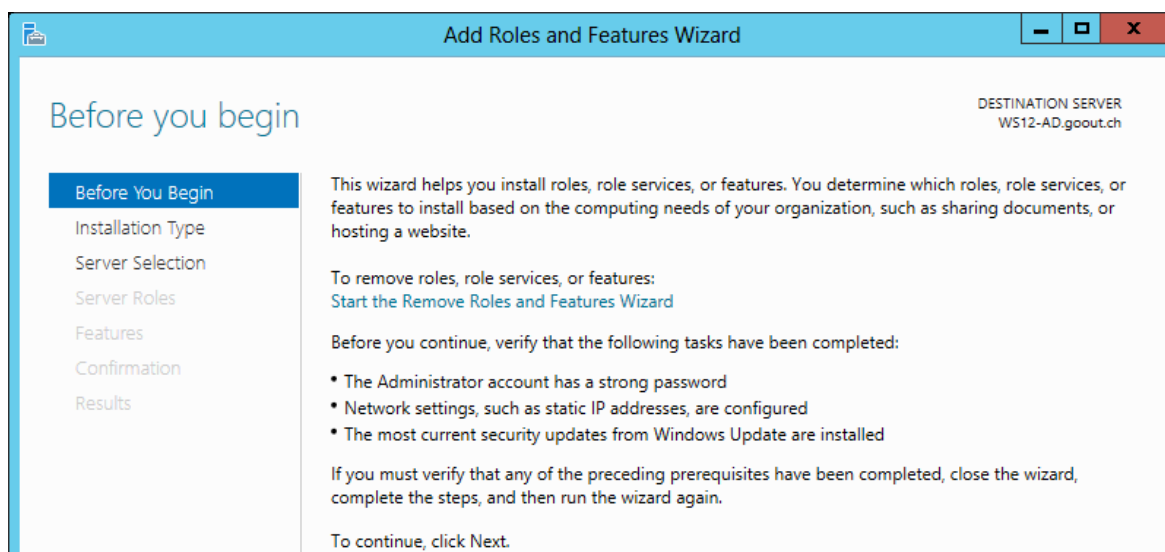
2.3 Aufbau der OU-Struktur

Folgende OU-Struktur wurde aufgebaut:



3 Rolle CA

Auf dem Domain Controller wird zusätzlich die Rolle „Active Directory Certificate Service“ installiert.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WS12-AD.goout.ch

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
WS12-AD.goout.ch	192.168.15.10	Microsoft Windows Server 2012 Release Candidate Data

Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WS12-AD.goout.ch

Before You Begin
Installation Type
Server Selection
Server Roles
Features

Select one or more roles to install on the selected server.

Roles

☒ Active Directory Certificate Services
☒ Active Directory Domain Services (Installed)
☐ Active Directory Federation Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue

Die Auswahl wird bestätigt.

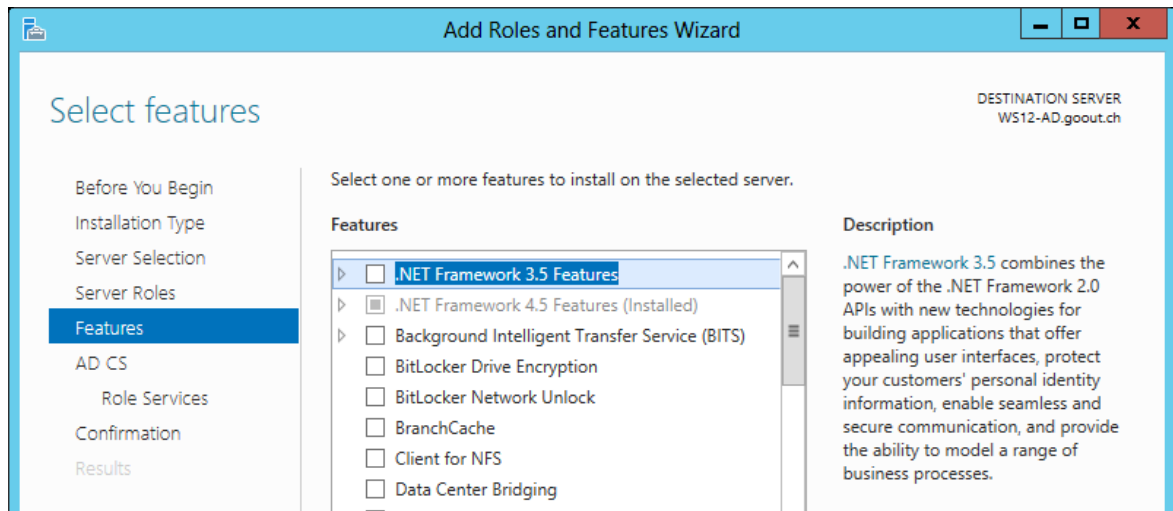
Add Roles and Features Wizard

Add features that are required for Active Directory Certificate Services?

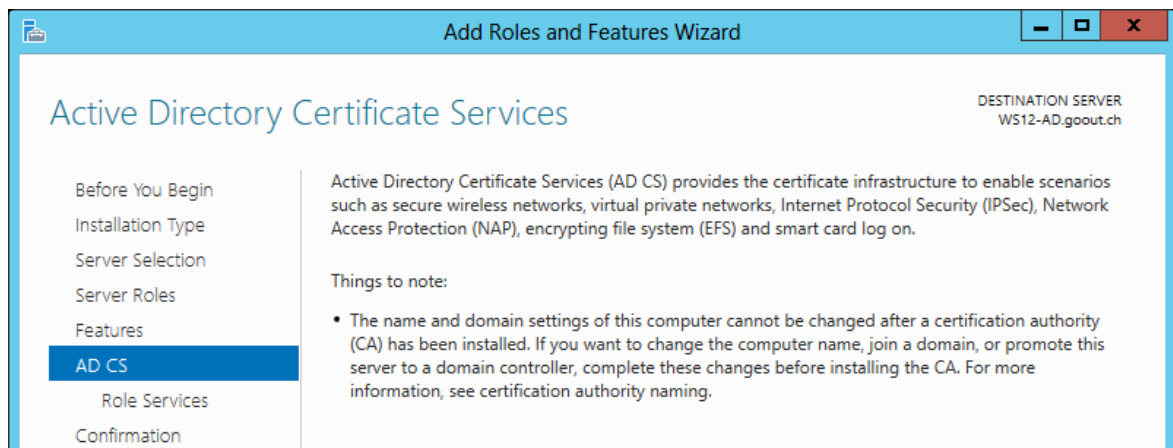
The following tools are required to manage this feature, but do not have to be installed on the same server.

- ▴ Remote Server Administration Tools
 - ▴ Role Administration Tools
 - ▴ Active Directory Certificate Services Tools
 - [Tools] Certification Authority Management Tools

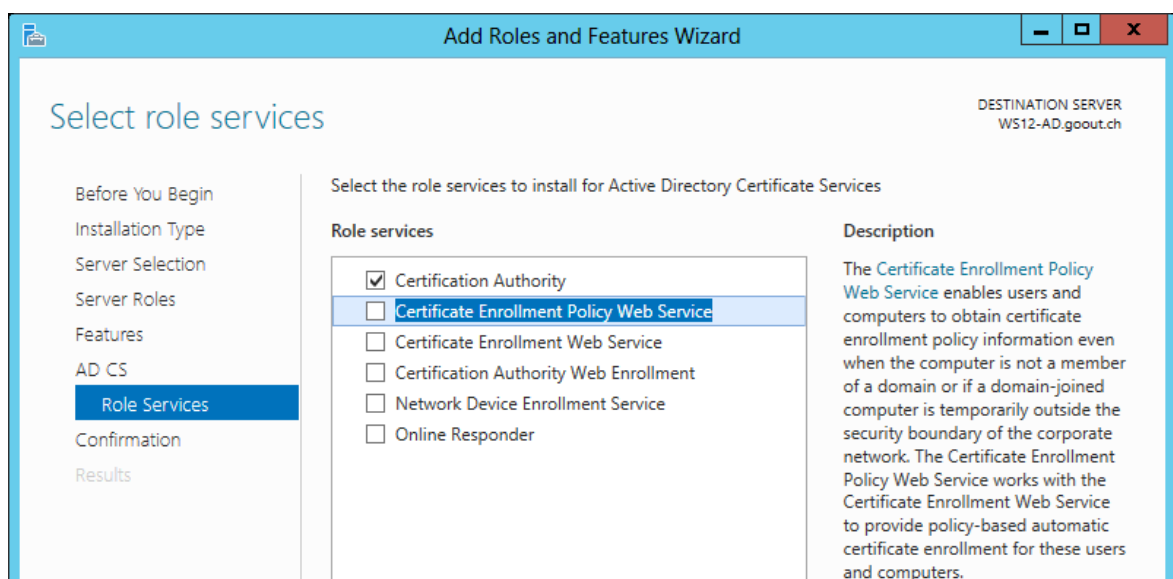
Es sind keine zusätzlichen Features notwendig.



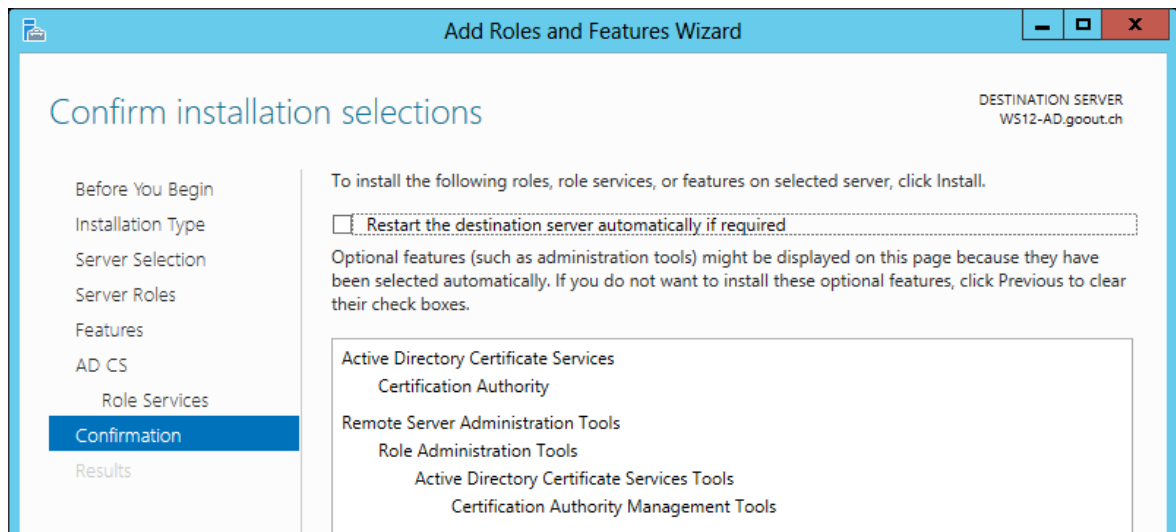
Die Rolleninformationen erscheinen.



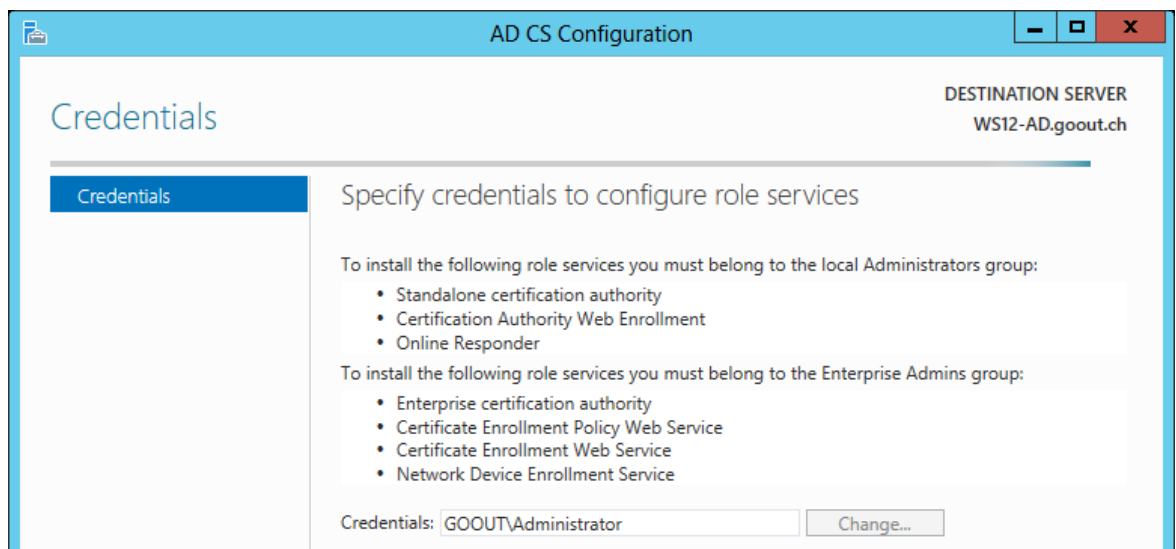
Für unsere Übung ist lediglich die Certification Authority notwendig.



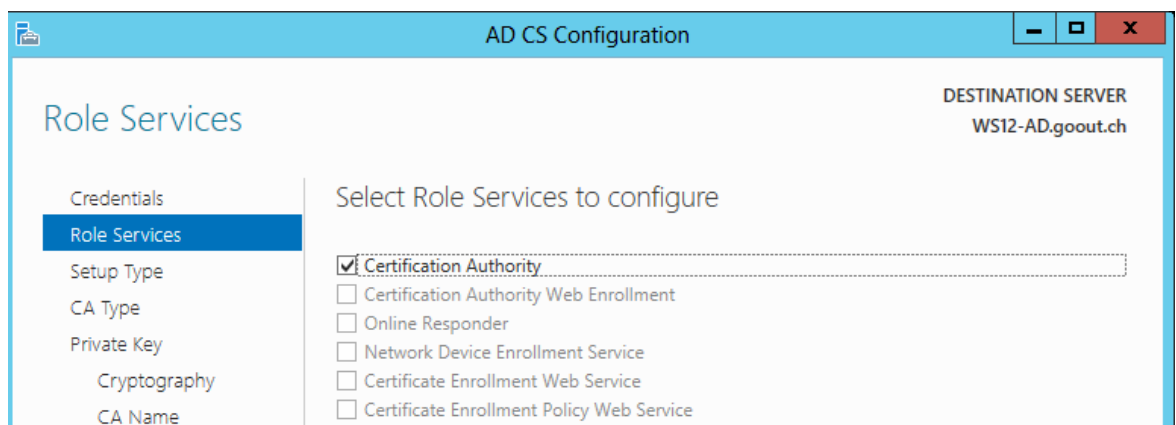
Die gemachten Eingaben werden noch bestätigt und anschliessend die Installation gestartet.



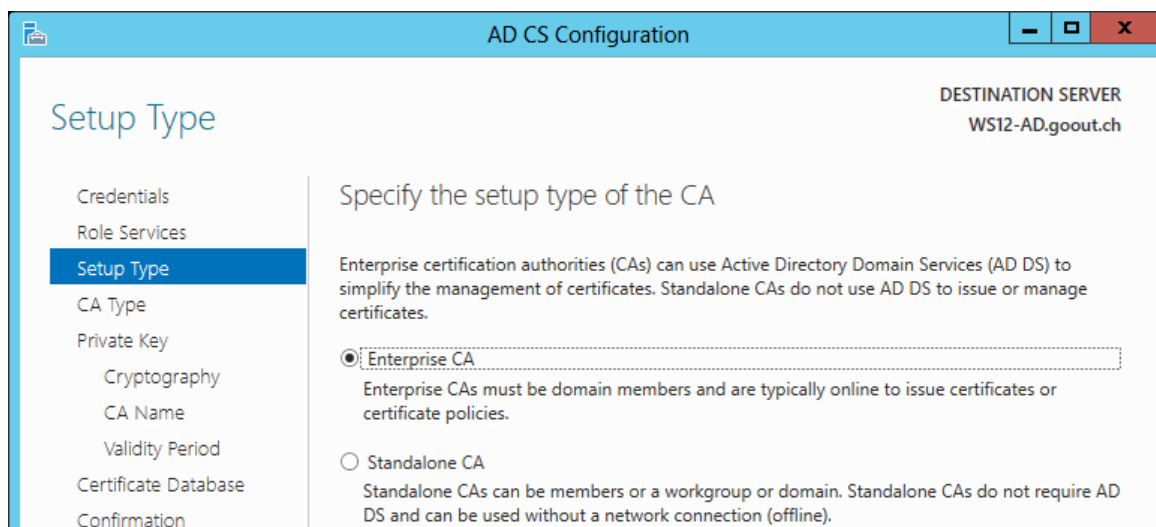
Nach der Installation wird angegeben, mit welchem Benutzer die CA läuft. Für unsere Übung ist dies der Administrator der Domäne.



Die installierte Rolle wird anschliessend konfiguriert.

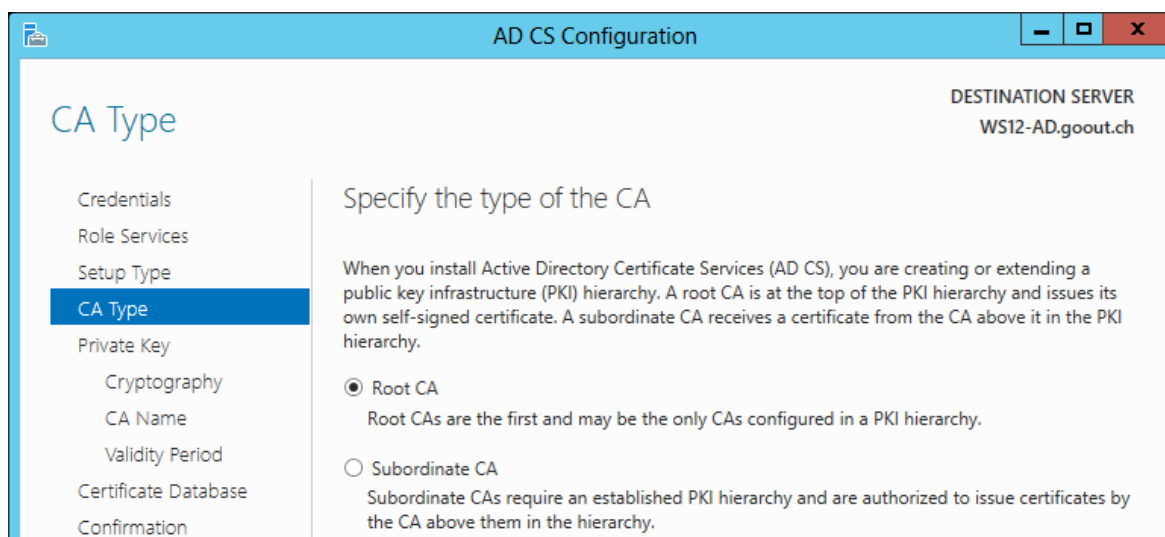


Unsere CA wird in die Domäne integriert.



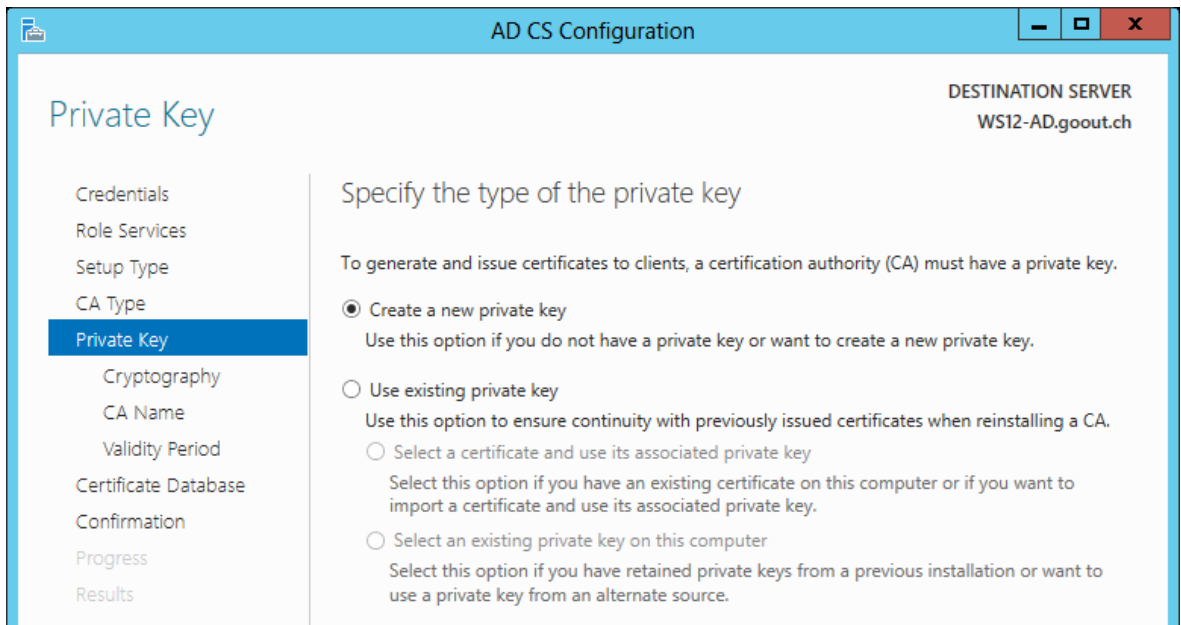
The screenshot shows the 'AD CS Configuration' window with the 'Setup Type' tab selected. The 'DESTINATION SERVER' is 'WS12-AD.goout.ch'. The left sidebar lists 'Credentials', 'Role Services', 'Setup Type' (selected), 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', and 'Confirmation'. The main area is titled 'Specify the setup type of the CA'. It explains that Enterprise CAs use Active Directory Domain Services (AD DS) to simplify certificate management, while Standalone CAs do not. The 'Enterprise CA' option is selected with a radio button. Below it, text states: 'Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.' The 'Standalone CA' option is unselected.

Sie stellt die Root CA dar.



The screenshot shows the 'AD CS Configuration' window with the 'CA Type' tab selected. The 'DESTINATION SERVER' is 'WS12-AD.goout.ch'. The left sidebar lists 'Credentials', 'Role Services', 'Setup Type', 'CA Type' (selected), 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', and 'Confirmation'. The main area is titled 'Specify the type of the CA'. It explains that when installing Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy. The 'Root CA' option is selected with a radio button. Below it, text states: 'Root CAs are the first and may be the only CAs configured in a PKI hierarchy.' The 'Subordinate CA' option is unselected.

Die notwendigen Schlüssel werden neu erstellt.



AD CS Configuration

DESTINATION SERVER
WS12-AD.goout.ch

Private Key

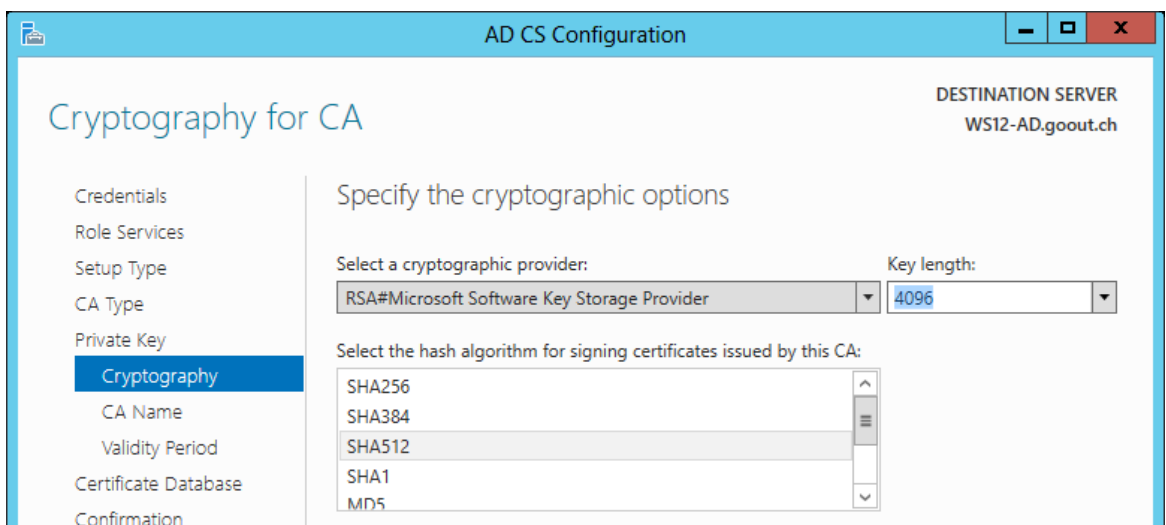
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

- ☒ **Create a new private key**
Use this option if you do not have a private key or want to create a new private key.
- ☐ **Use existing private key**
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
 - ☐ **Select a certificate and use its associated private key**
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
 - ☐ **Select an existing private key on this computer**
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

Die Schlüssel werden optimal gewählt.



AD CS Configuration

DESTINATION SERVER
WS12-AD.goout.ch

Cryptography for CA

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation

Specify the cryptographic options

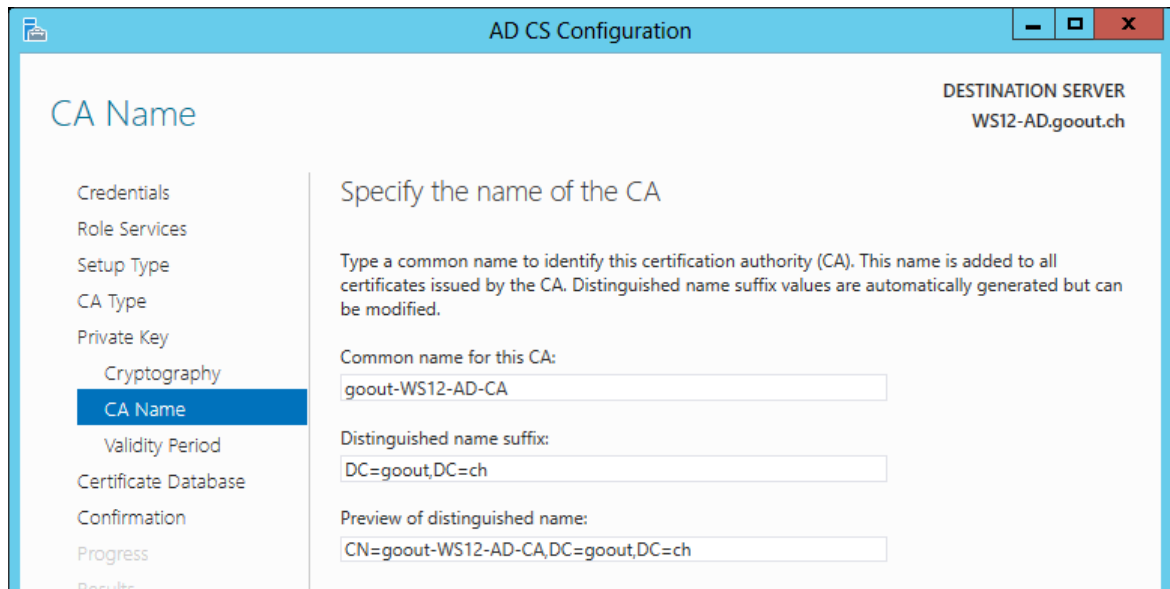
Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 4096

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512**
- SHA1
- MD5

Die vorgeschlagenen Namen übernommen.



AD CS Configuration

DESTINATION SERVER
WS12-AD.goout.ch

CA Name

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Back

Specify the name of the CA

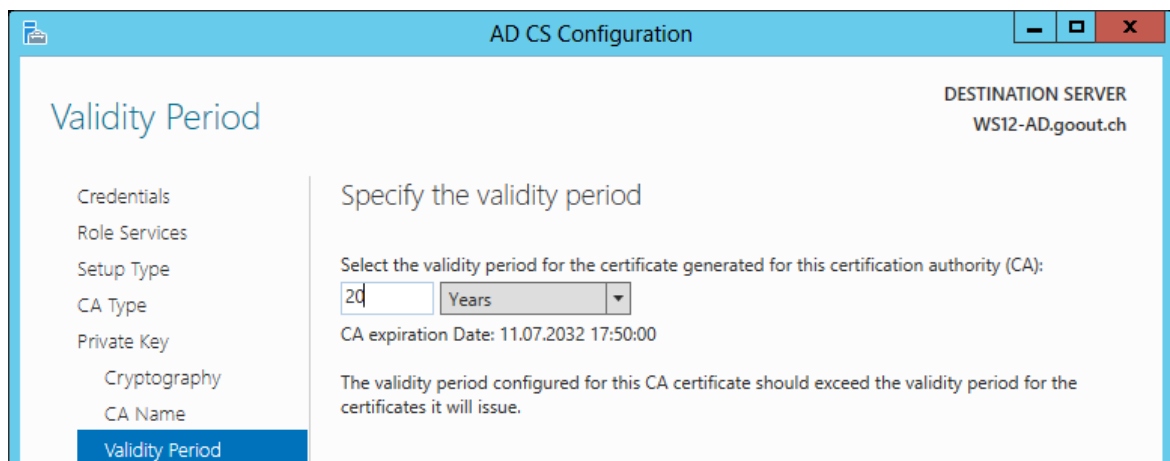
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

Distinguished name suffix:

Preview of distinguished name:

Nun kann noch die Schlüsseldauer gewählt werden. Da unsere Schlüsselvorgaben hoch gewählt wurden, kann auch eine lange Lebensdauer definiert werden (Randbemerkung: eine Verlängerung oder Erneuerung des Schlüssels ist keine grosse Herausforderung).



AD CS Configuration

DESTINATION SERVER
WS12-AD.goout.ch

Validity Period

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

CA expiration Date: 11.07.2032 17:50:00

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

Die Standardpfade können übernommen werden.

AD CS Configuration

CA Database

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name
- Validity Period
- Certificate Database**

Specify the database locations

Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

Die gemachten Angaben werden nochmals bestätigt.

AD CS Configuration

Confirmation

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name
- Validity Period
- Certificate Database
- Confirmation**
- Progress
- Results

To configure the following roles, role services, or features, click Configure.

^ **Active Directory Certificate Services**

Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA512
Key Length:	4096
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	11.07.2032 17:50:00
Distinguished Name:	CN=goout-WS12-AD-CA,DC=goout,DC=ch
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Die erfolgreiche Installation wird bestätigt.

AD CS Configuration

Results

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key

The following roles, role services, or features were configured:

^ **Active Directory Certificate Services**

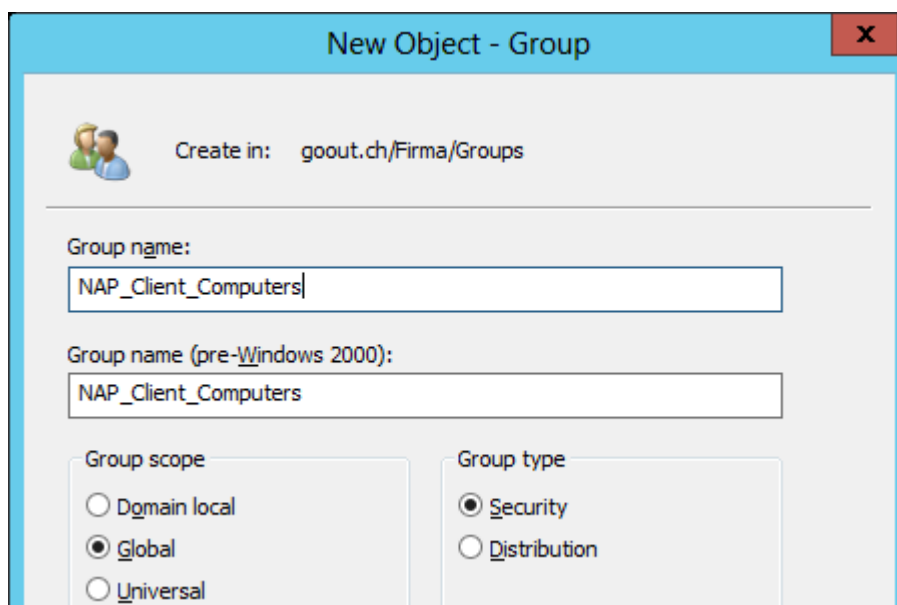
Certification Authority ✔ Configuration succeeded

[More about CA Configuration](#)

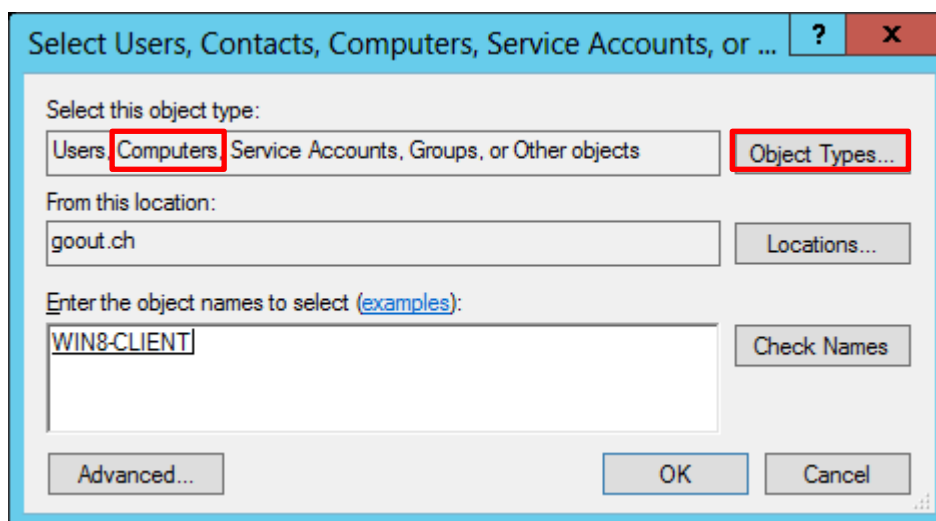
4 Client

Als Client-Betriebssystem wurde ein Windows 8 installiert. Anschliessend wurde der Client mit dem Namen WIN8-CLIENT in die Domäne goout.ch aufgenommen und in der OU Firma-Clients abgelegt.

Anschliessend wurde der Client in die Gruppe NAP_Client_Computers aufgenommen.



Damit der Objekttyp „Computers“ angezeigt wird, muss er unter dem Button „Object Types...“ angewählt werden.

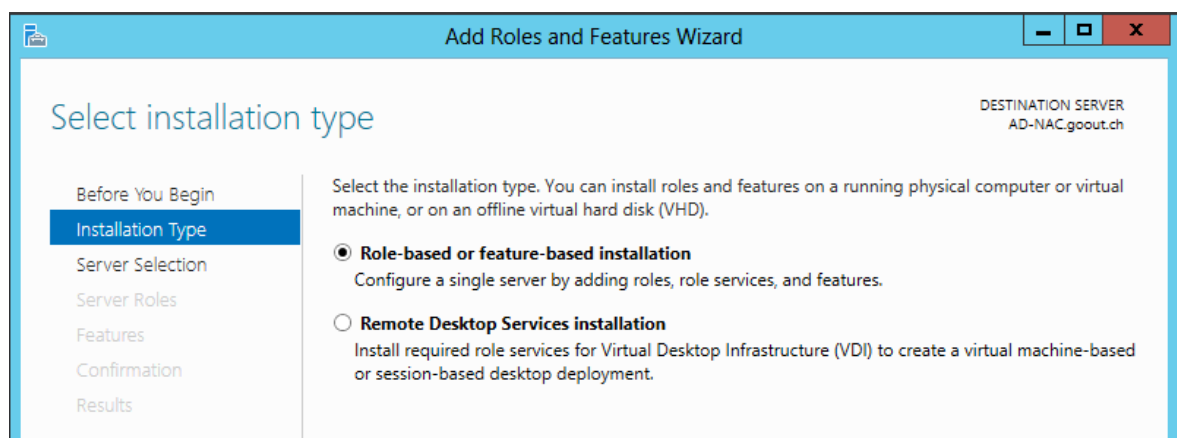
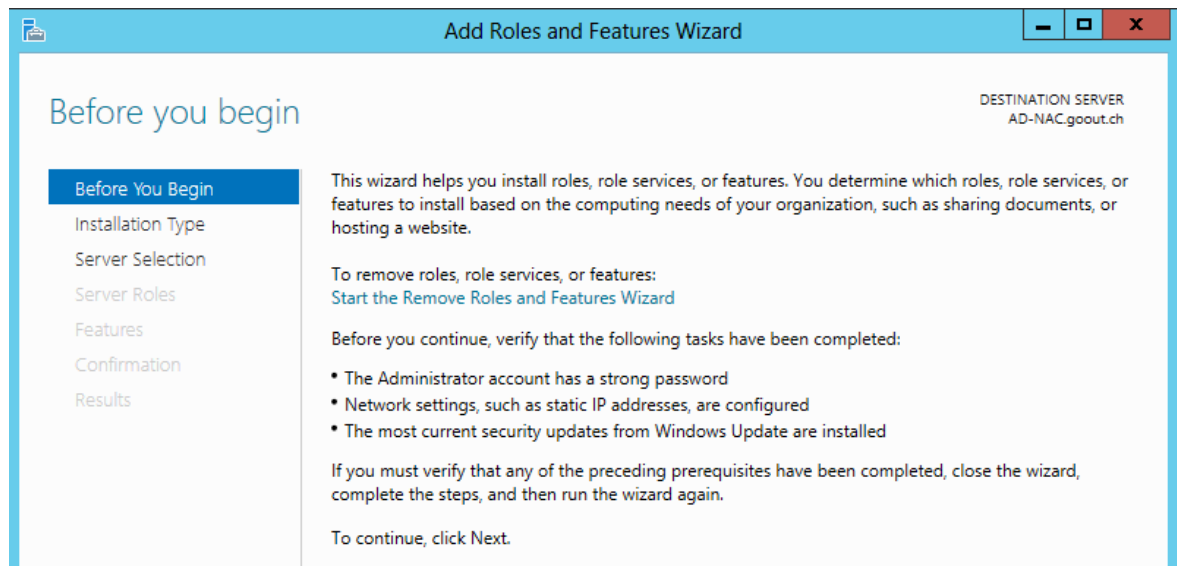


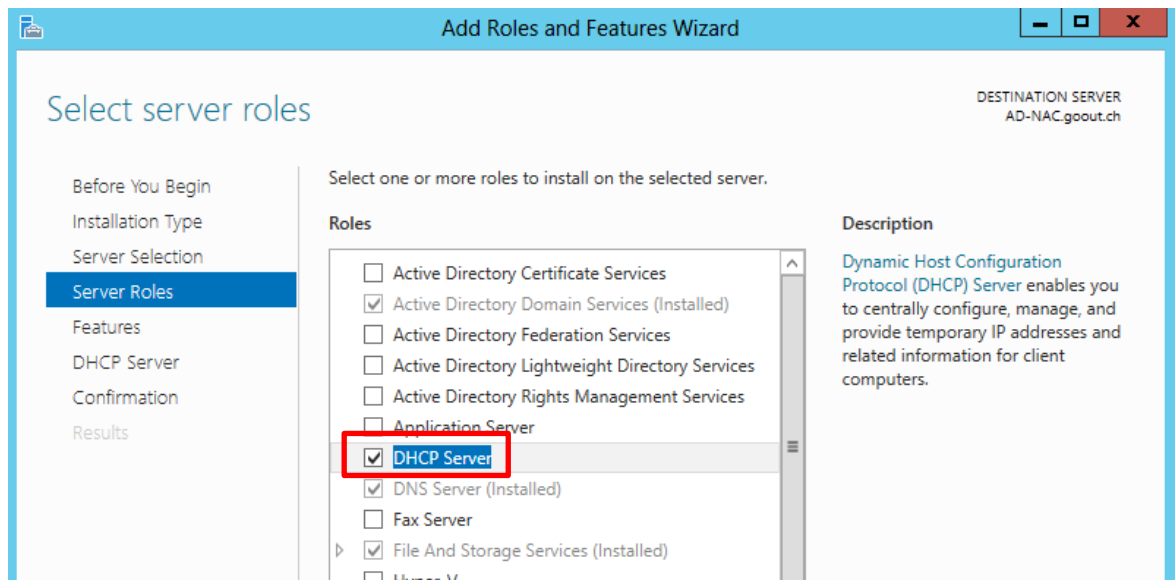
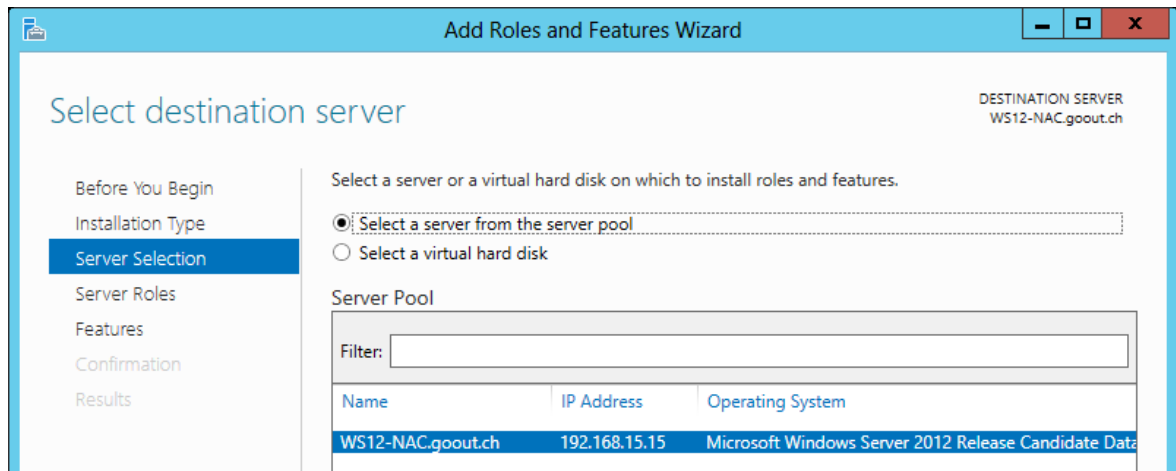
5 DHCP

Auf dem zweiten Windows Server 2012 werden die Rollen DHCP und NPS installiert.

5.1 Installation

Als erstes wird die Rolle „DHCP“ installiert. Dazu wird im Server Manager wiederum “Add roles and features” ausgewählt.

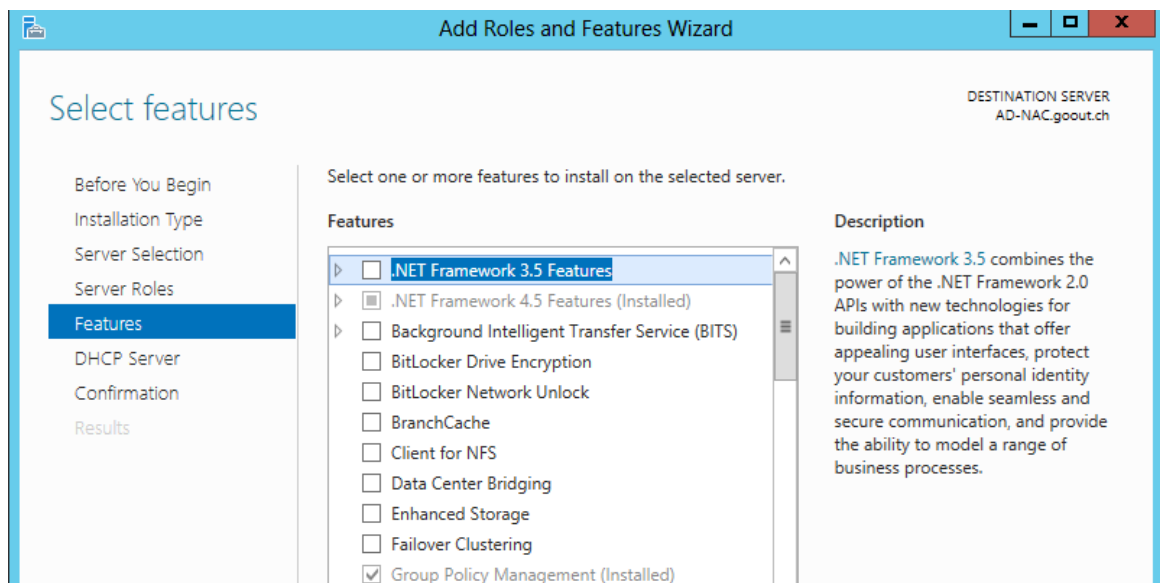




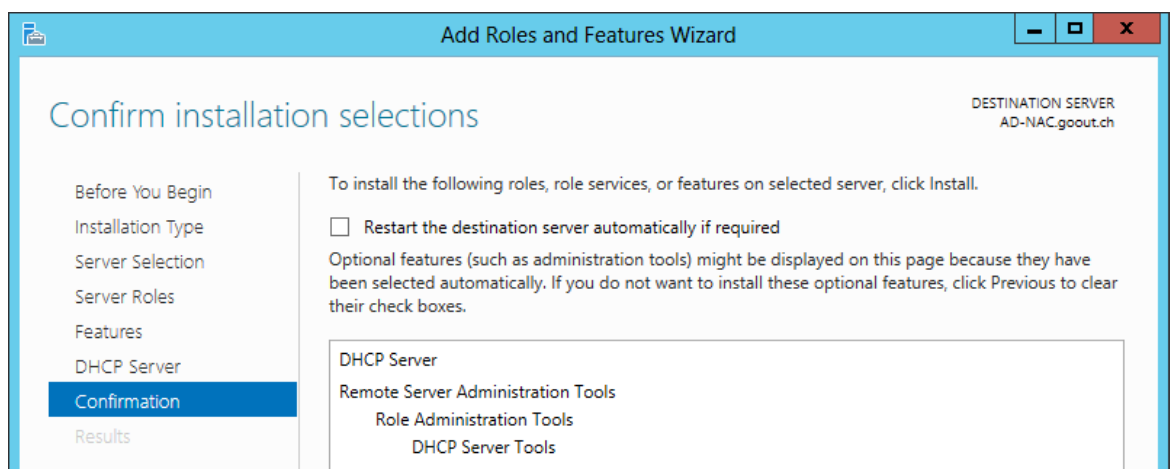
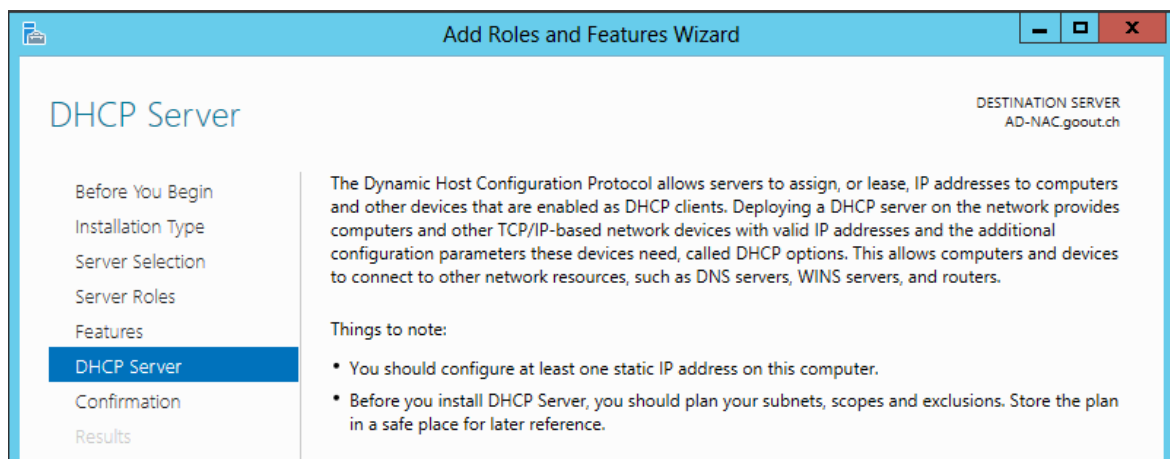
Anschliessend den Dialog „Add Roles and Features Wizard“ bestätigen.



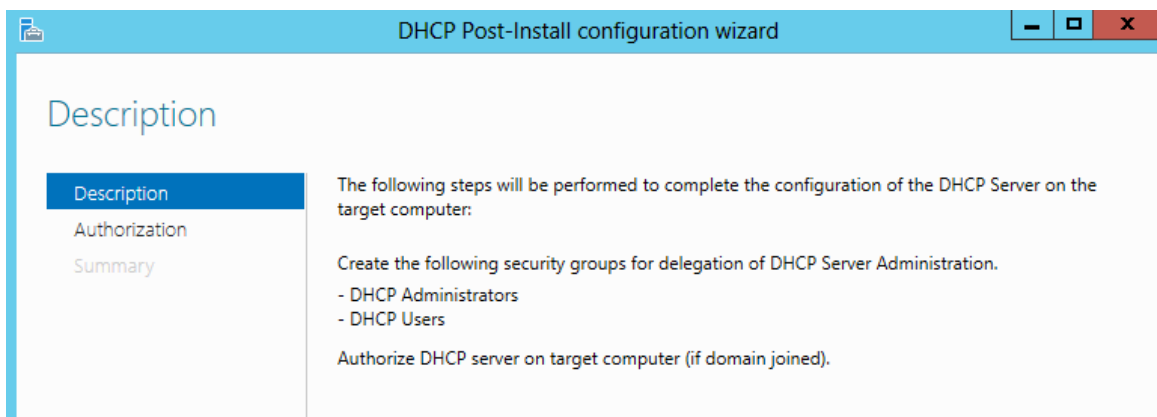
Zusätzliche Features sind nicht notwendig.



Anschließend folgt die die Bestätigung und die Zusammenfassung.



Vor der Installation kann die Rolle „DHCP Server“ noch ins AD integriert werden.



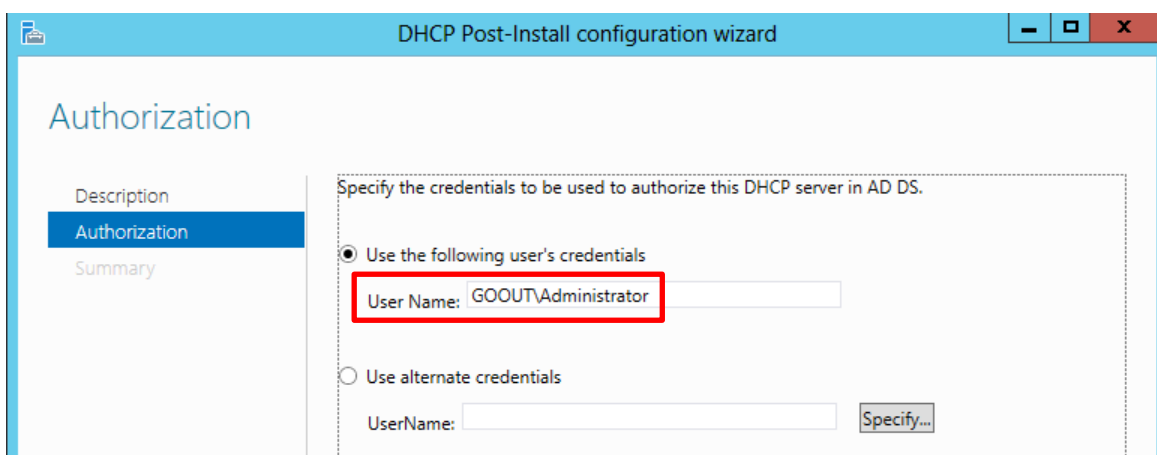
Description

The following steps will be performed to complete the configuration of the DHCP Server on the target computer:

Create the following security groups for delegation of DHCP Server Administration.

- DHCP Administrators
- DHCP Users

Authorize DHCP server on target computer (if domain joined).



Authorization

Specify the credentials to be used to authorize this DHCP server in AD DS.

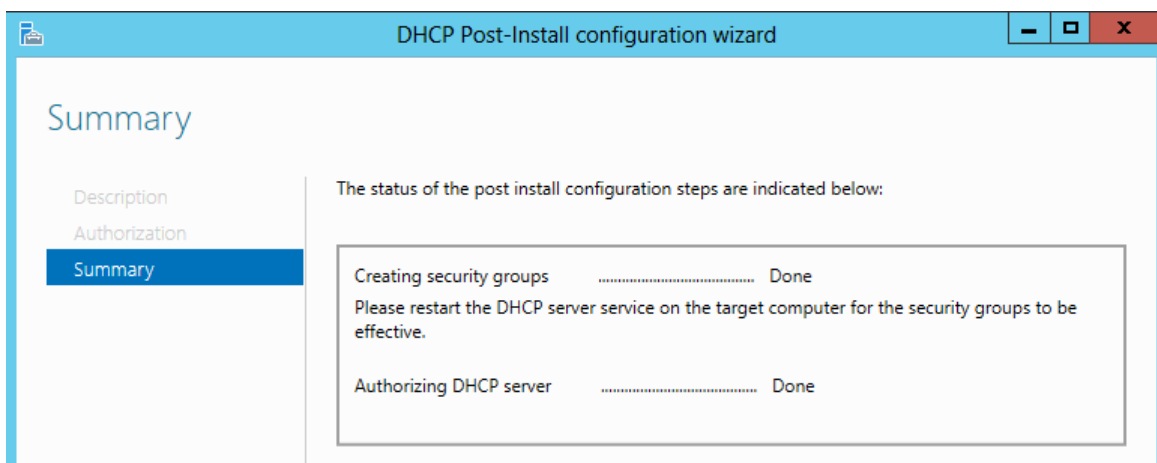
☒ Use the following user's credentials

User Name: GOOUT\Administrator

☐ Use alternate credentials

UserName: Specify...

Falls erfolgreich, erscheint die Bestätigung.



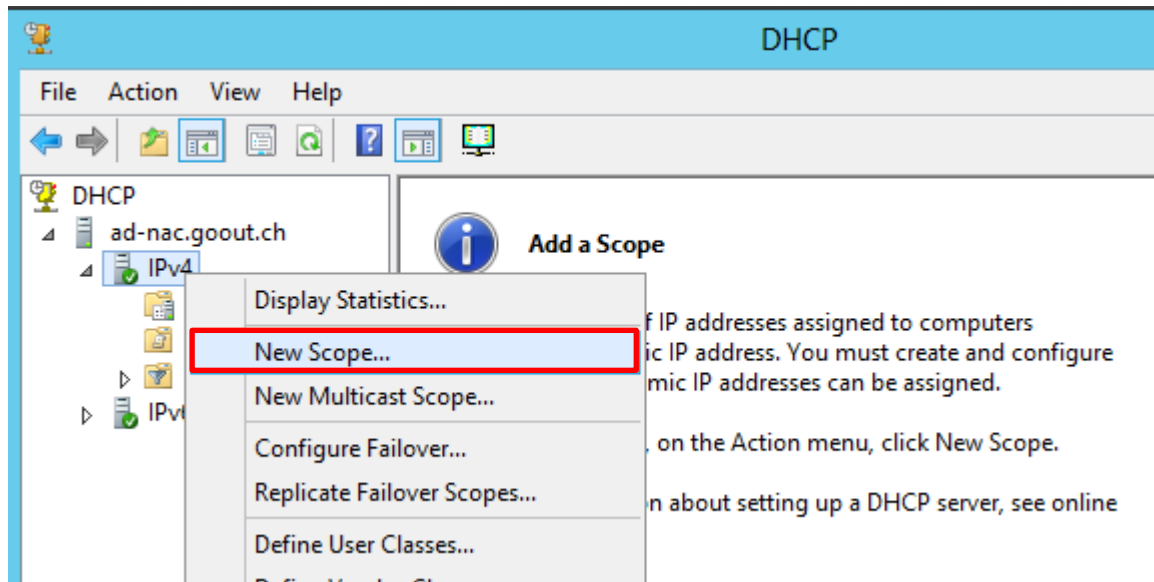
Summary

The status of the post install configuration steps are indicated below:

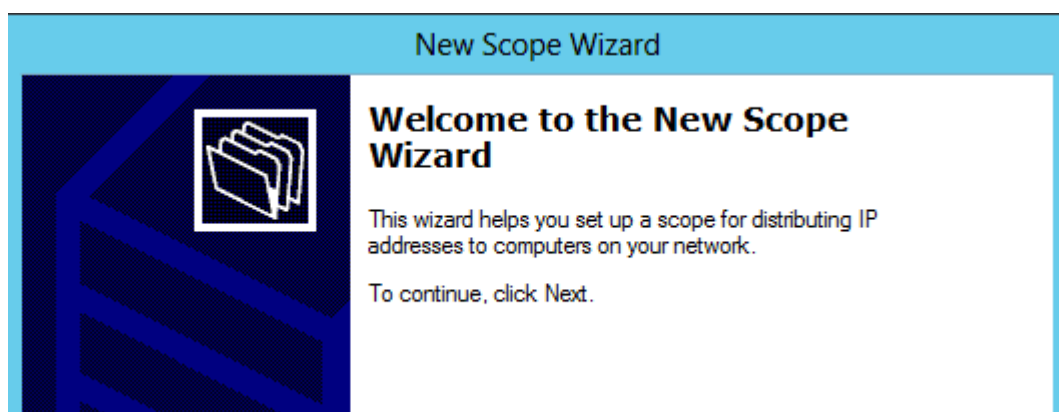
Creating security groups	Done
Please restart the DHCP server service on the target computer for the security groups to be effective.	
Authorizing DHCP server	Done

5.2 Konfiguration

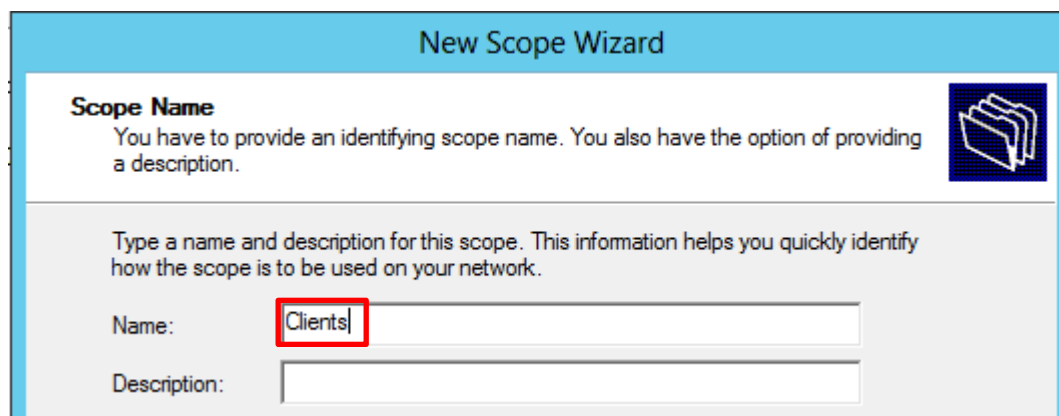
Im DHCP Server wird anschliessend ein neuer Bereich angelegt.



Der Wizard führt nun Schritt-für-Schritt durch die Konfiguration.



Für diese Übung heisst der neue Bereich „Clients“.



Der Client-Bereich ist von 192.168.15.100-149 (50 Adressen).

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 15 . 100

End IP address: 192 . 168 . 15 . 149

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Ausnahmen werden keine getätigt.

New Scope Wizard

Add Exclusions and Delay
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: | . . . End IP address: . . . Add

Excluded address range: Remove

Subnet delay in milli second: 0

Die Lease-Dauer wird auf dem Standardwert von 8 Tagen belassen.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

Die zusätzlichen Informationen werden gleich mit dem Wizard definiert.

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

Als Default Gateway wird der Router mit der Adresse 192.168.15.1 definiert.

New Scope Wizard

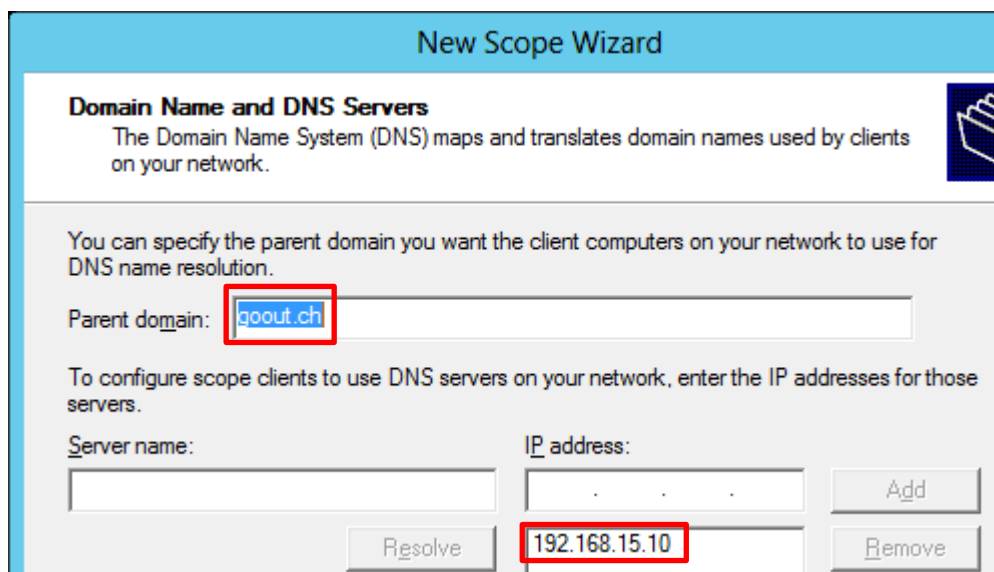
Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

Der DNS Server ist unser AD-Server mit der IP-Adresse 192.168.15.10.



New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

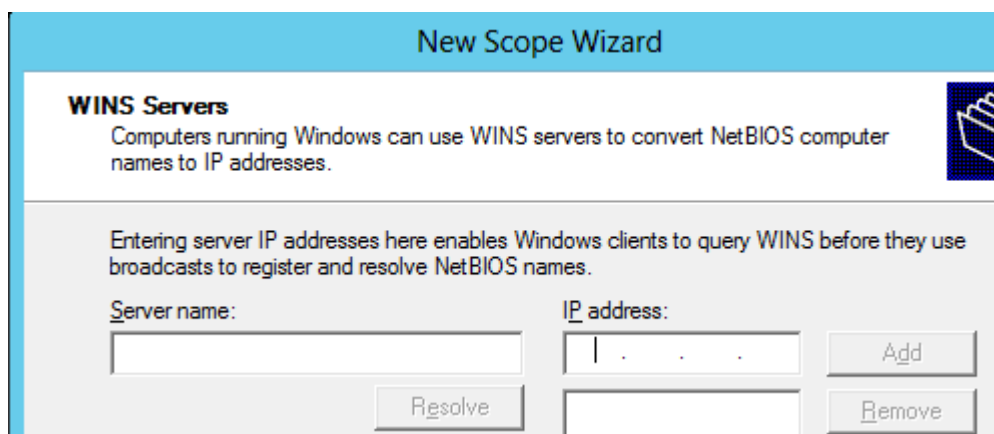
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
	192.168.15.10	Add
Resolve		Remove

WINS wird für diese Übung nicht benötigt.



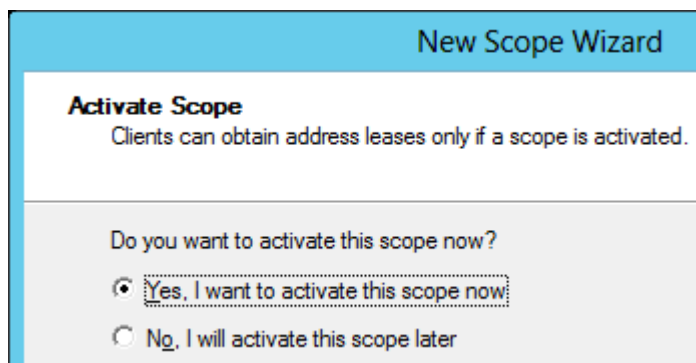
New Scope Wizard

WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:	IP address:	
	1 . . .	Add
Resolve		Remove

Der neue Bereich „Clients“ wird direkt aktiviert.



New Scope Wizard

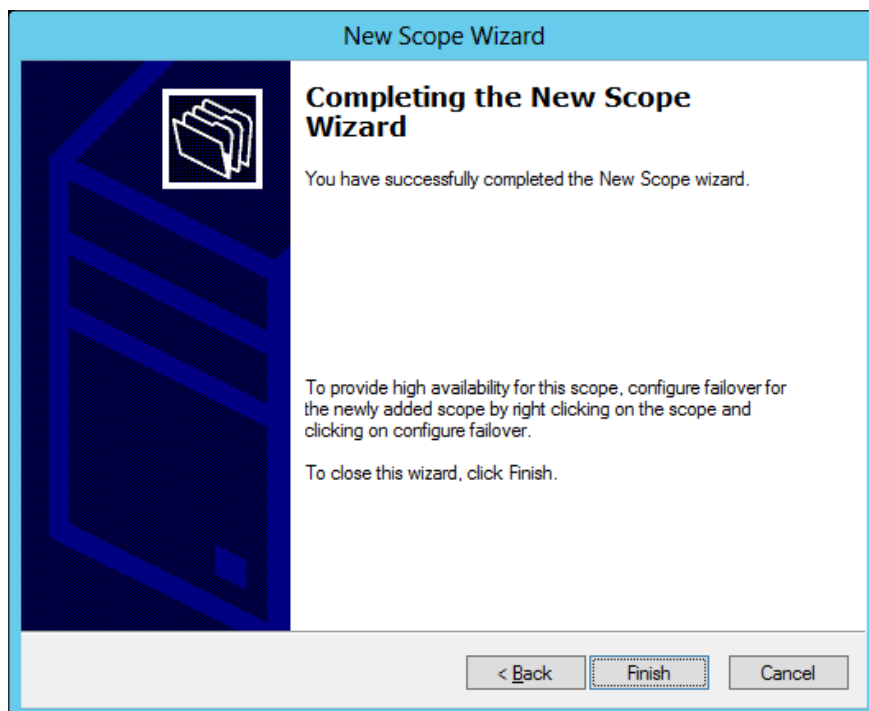
Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

☒ Yes, I want to activate this scope now

☐ No, I will activate this scope later

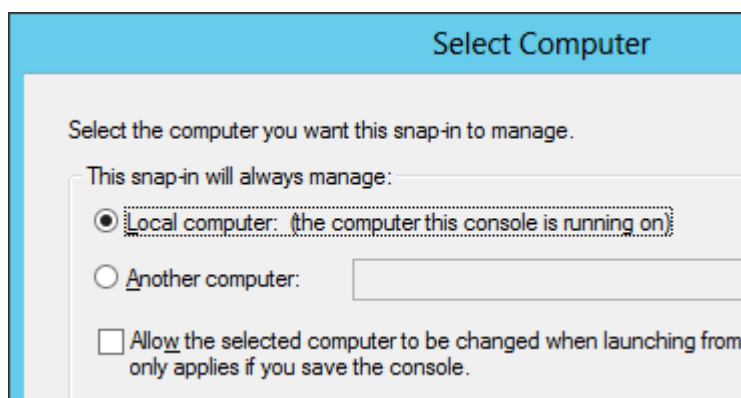
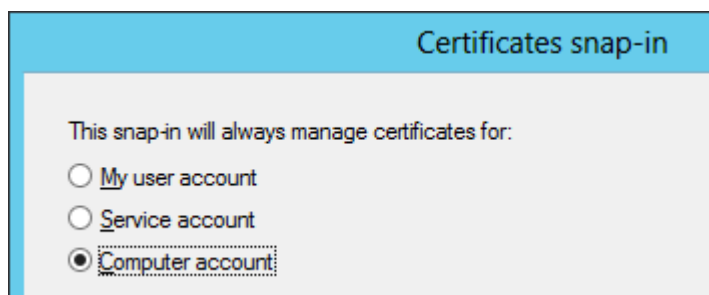
Und der Wizard-Konfigurationsvorgang ist abgeschlossen.



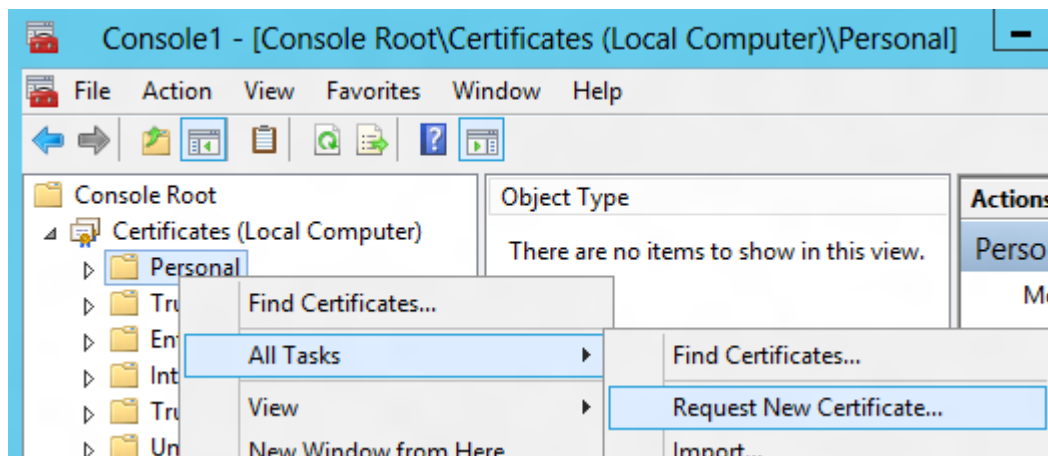
6 Zertifikat

Auf dem zweiten Windows Server 2012 muss noch ein Zertifikat installiert werden, damit der NPS Dienst mit dem Active Directory Daten austauschen kann.

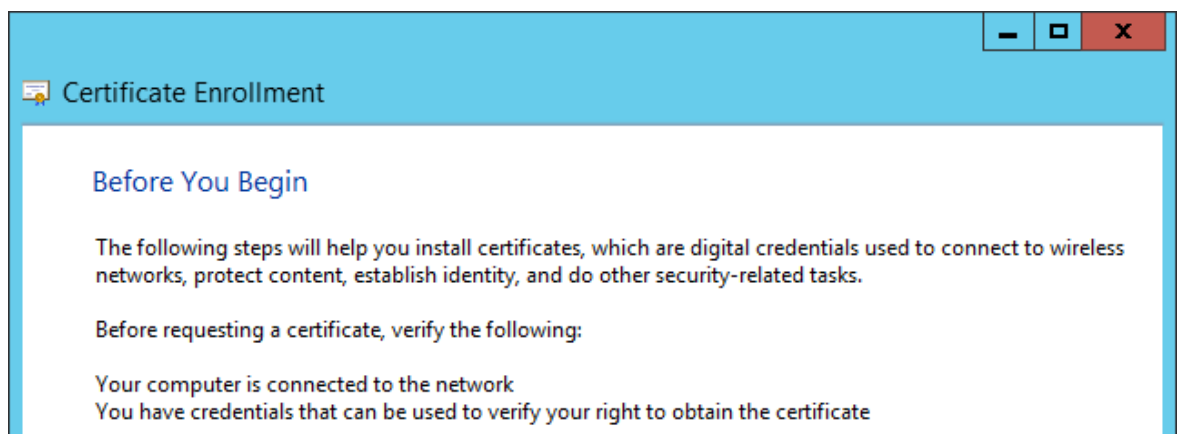
Dazu wird mit dem Befehl mmc die Management-Konsole gestartet und das Snap-In „Certificate“ ausgewählt. Das Zertifikat soll für den Computer gelten:



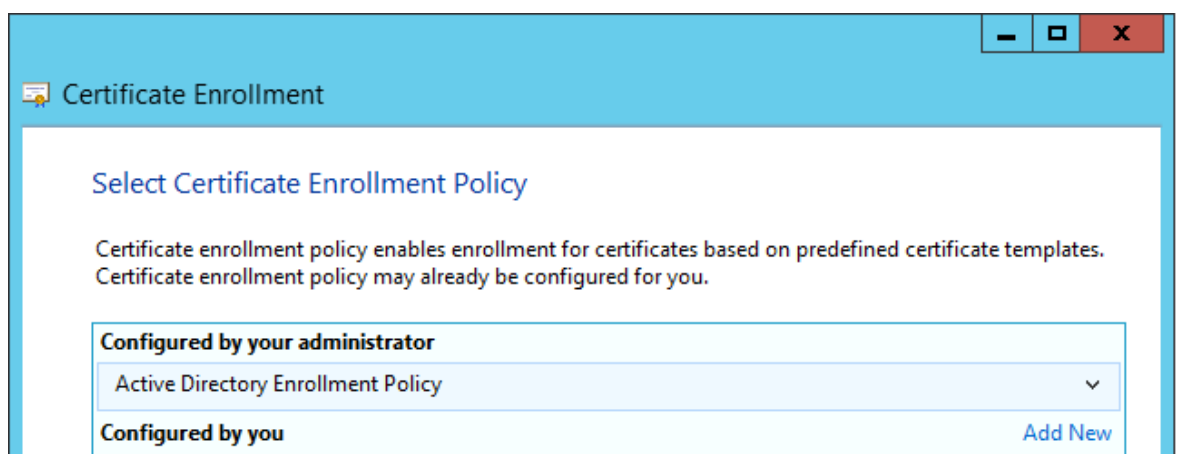
Nun wird ein Zertifikat beantragt



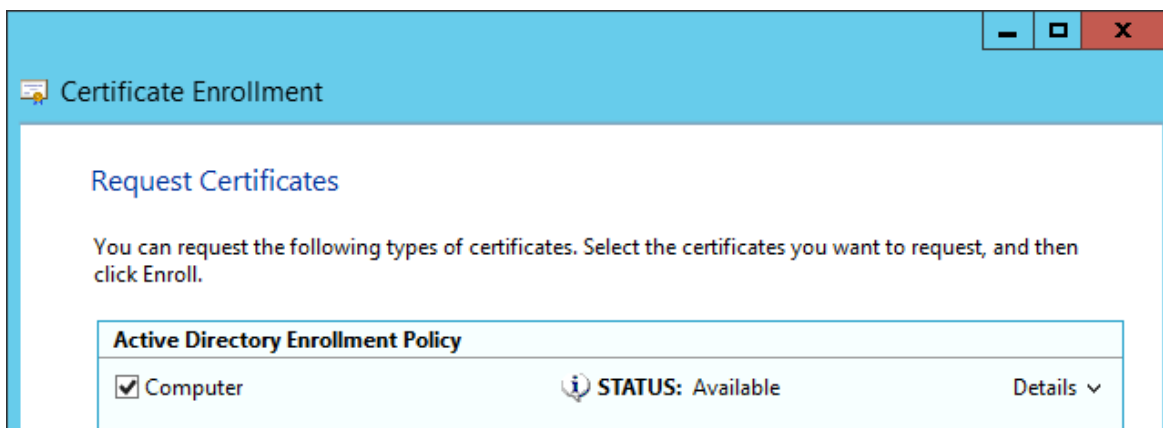
Der entsprechende Wizard startet.



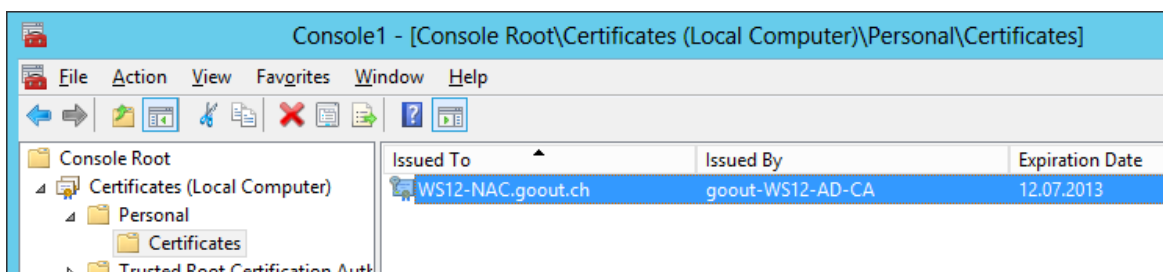
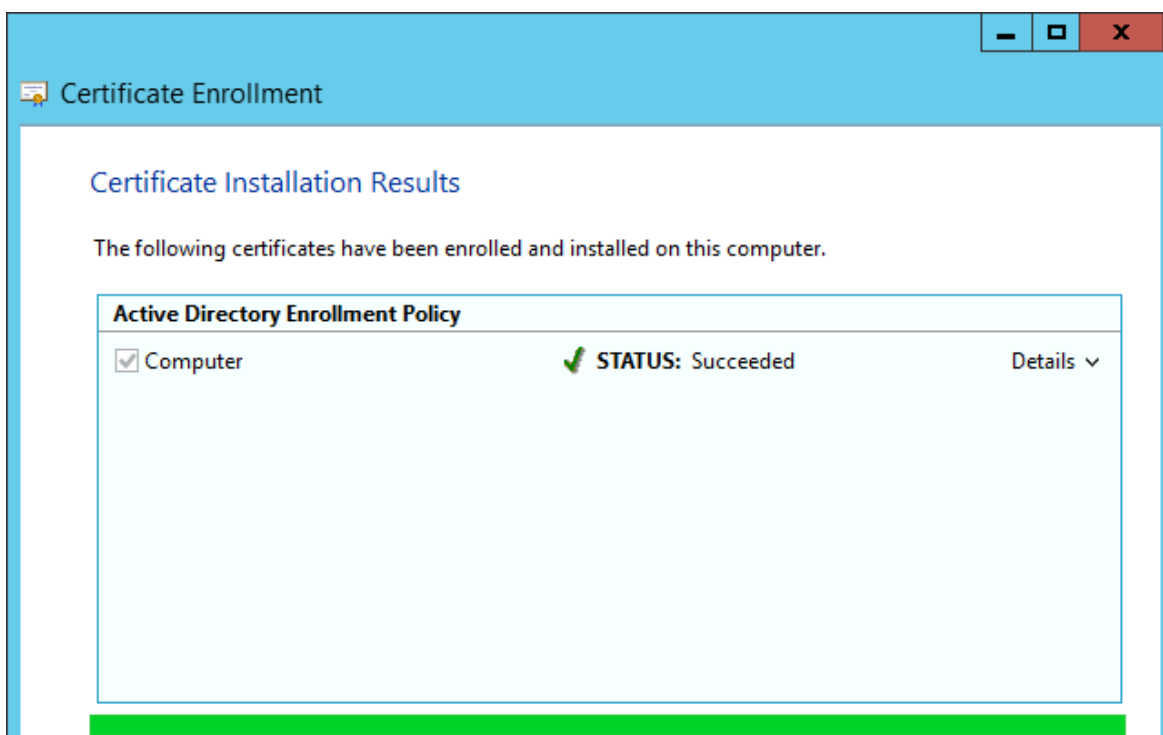
Das Zertifikat wird automatisch von der CA auf dem Domain Controller „geholt“.



Mit Enroll wird das Zertifikat im Anschluss „geholt“.



Nach wenigen Augenblicken ist das Zertifikat lokal installiert.

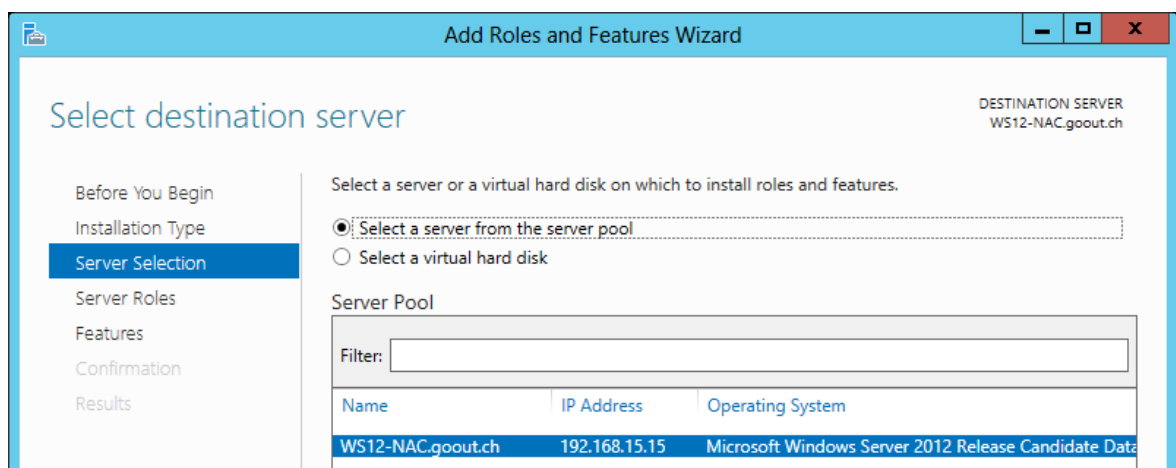
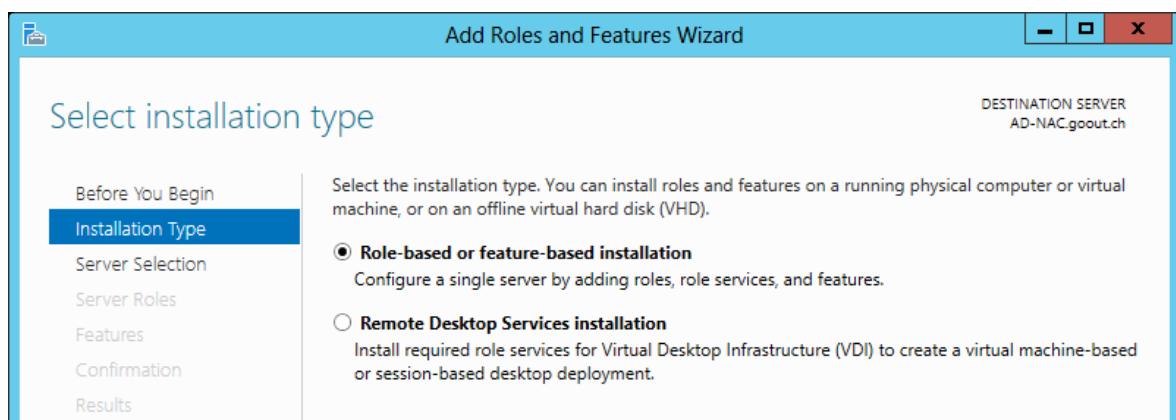
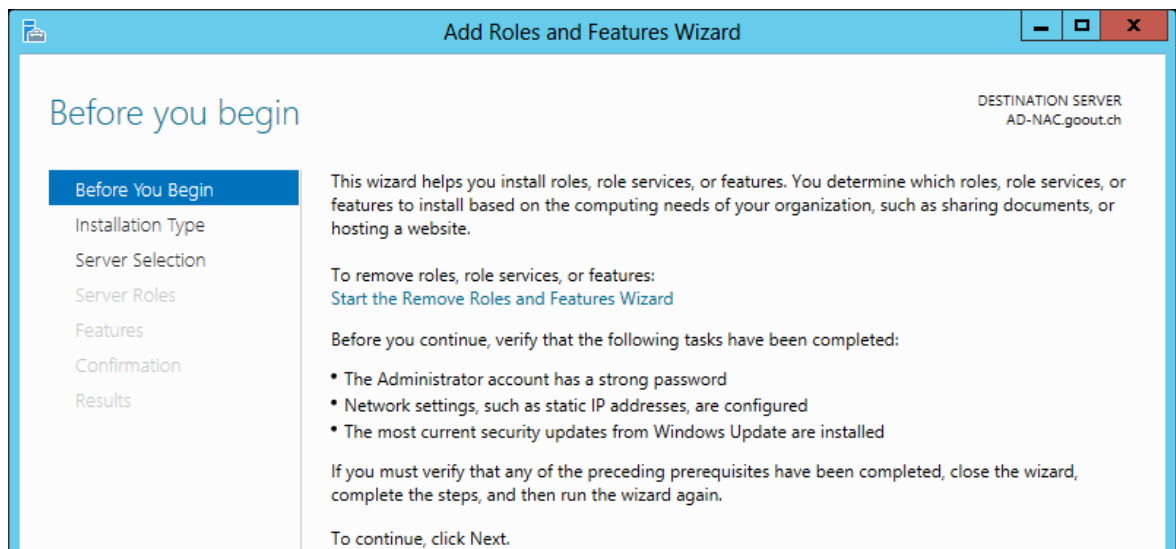


Die Konsole kann anschliessend ohne Speicherung geschlossen werden.

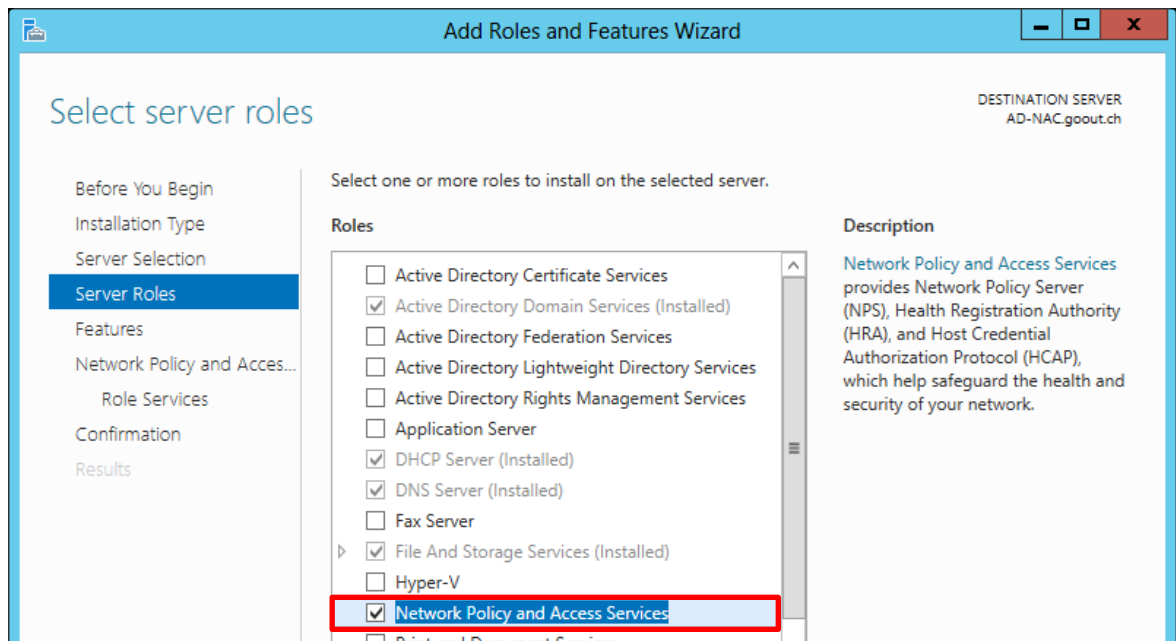
7 Network Policy Server

7.1 Installation

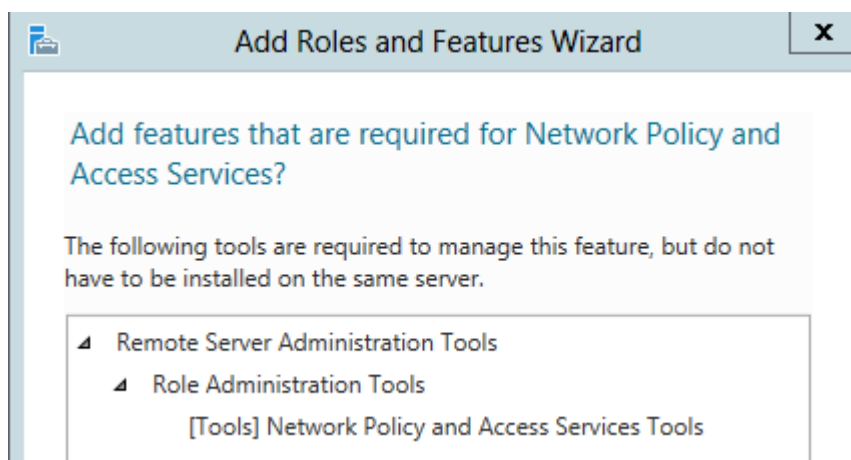
Nun wird die Rolle „NPS – Network Policy Server“ installiert. Dazu wird der Wizard im Rollenmanager „Add new roles and features“ gestartet.



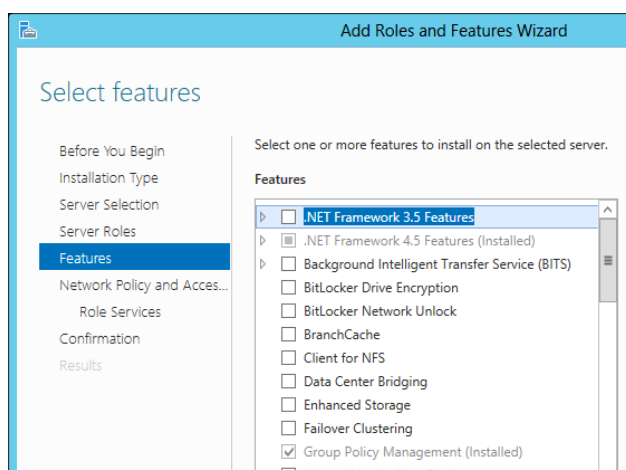
Und die Rolle „Network Policy and Access Services“ ausgewählt.



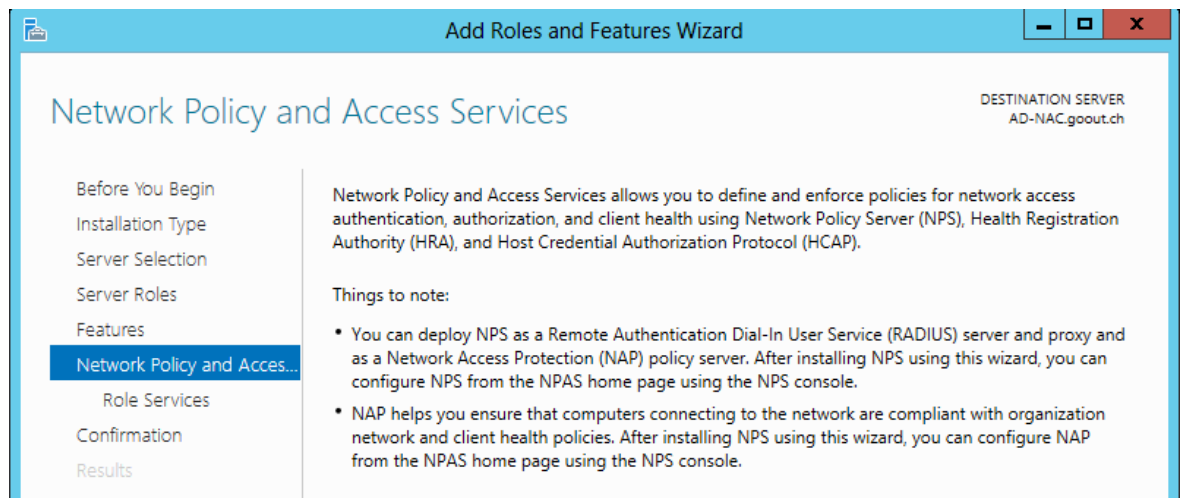
Und der Vorschlag übernommen.



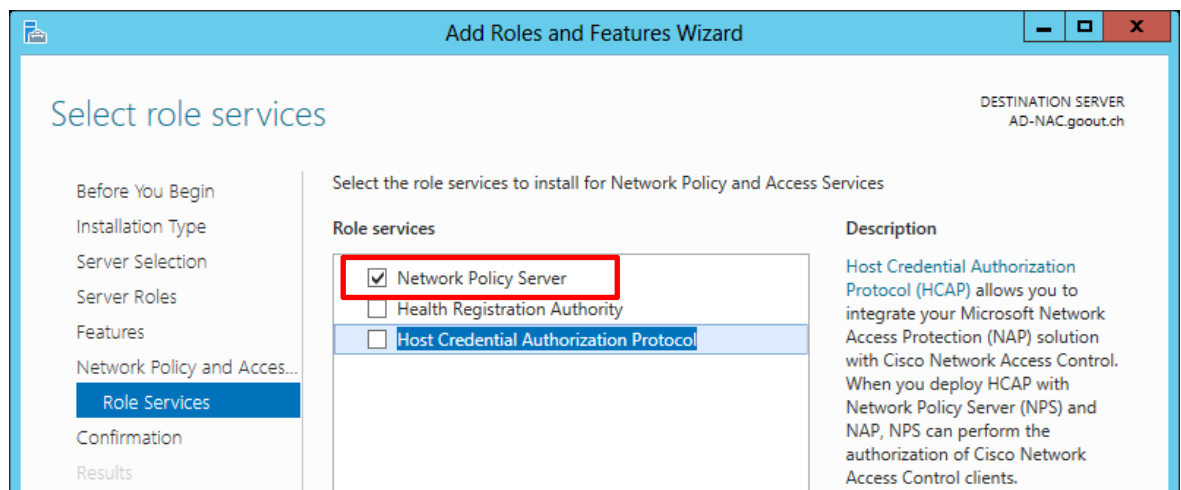
Zusätzliche Features sind nicht notwendig.



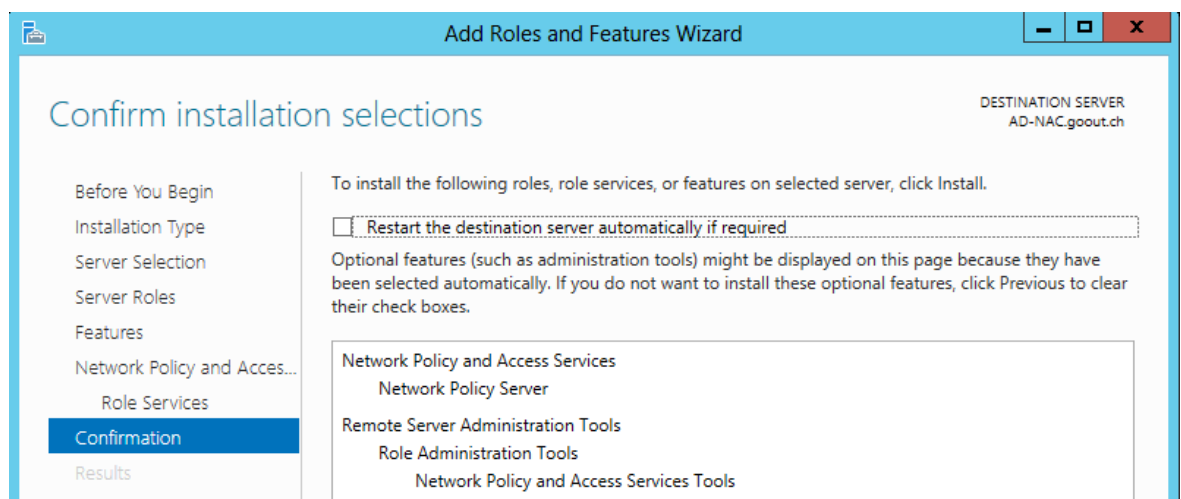
Nun startet der NPS Wizard.



Für unsere Übung ist nur der Network Policy Server notwendig.

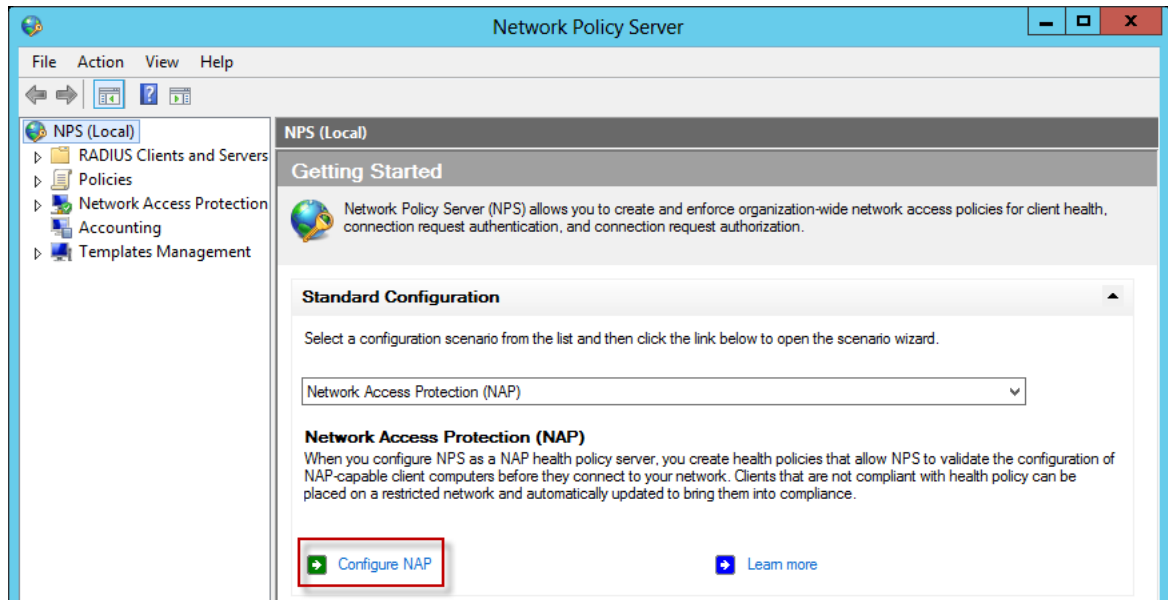


Es folgt eine Bestätigung der Eingaben.

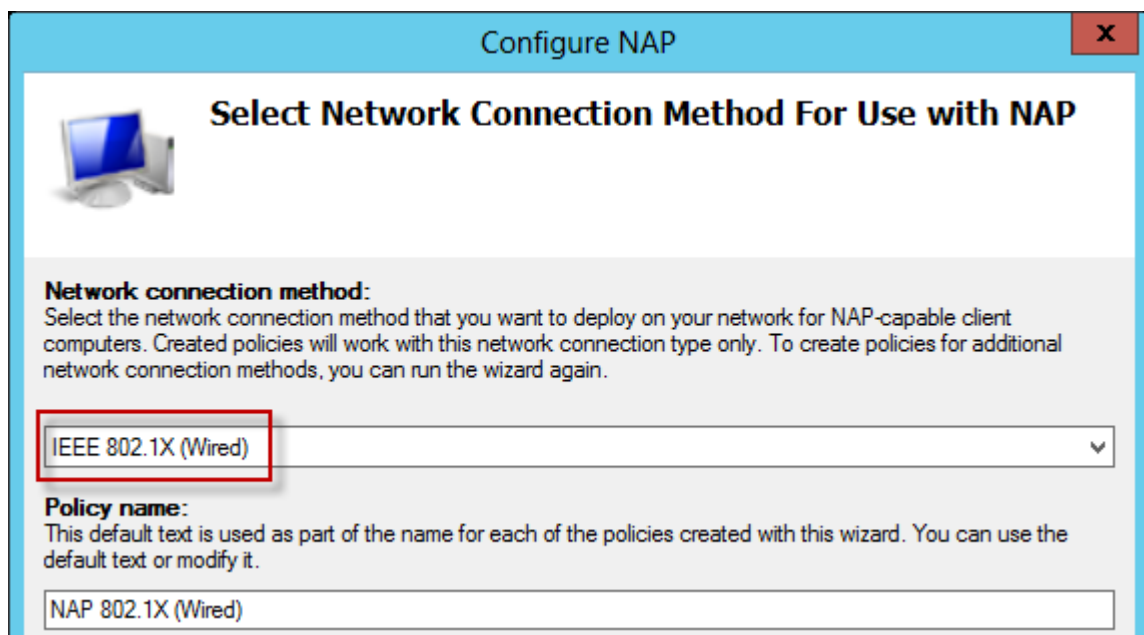


7.2 Konfiguration NPS

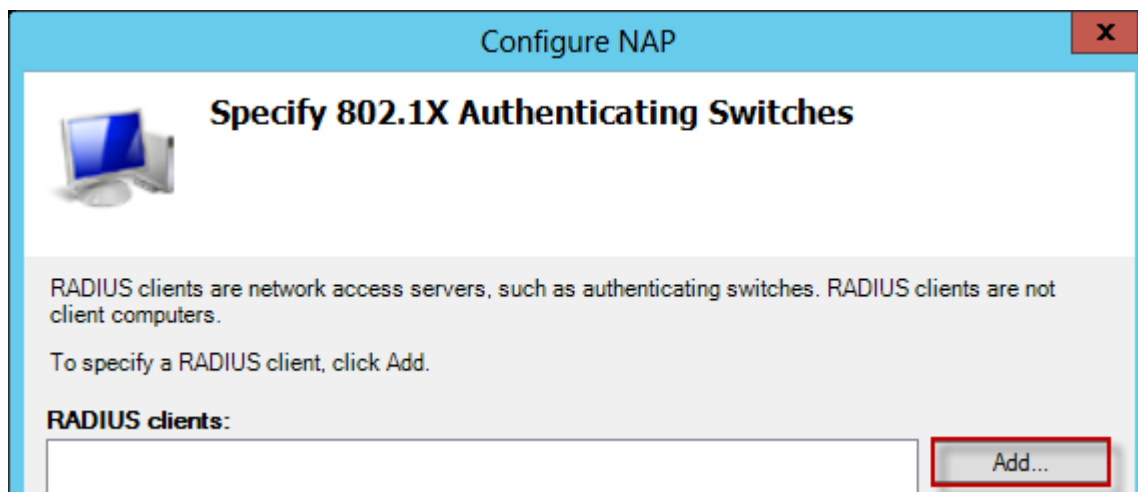
Im nächsten Schritt wird eine NPS Richtlinie erstellt.



Für dieses Szenario wird die Methode IEEE 802.1X (Wired) ausgewählt.



Im nächsten Schritt fügen wir einen Radius-Client (Switch) hinzu.



Configure NAP

Specify 802.1X Authenticating Switches

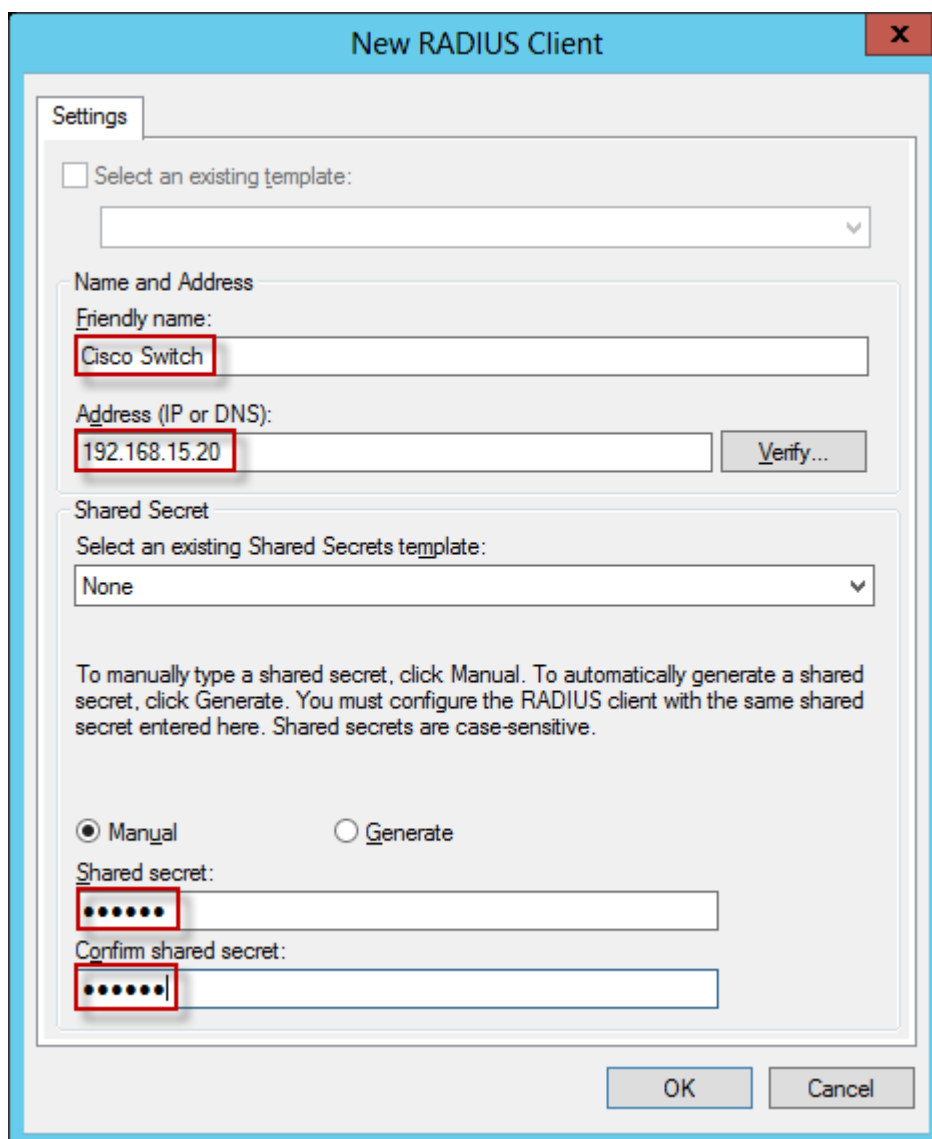
RADIUS clients are network access servers, such as authenticating switches. RADIUS clients are not client computers.

To specify a RADIUS client, click Add.

RADIUS clients:

Add...

Unser Radius Client (Switch) hat die IP-Adresse 192.168.15.20. Das Passwort benötigen wir anschliessend auch auf dem Switch. Für diese Übung lautet es „secret“.



New RADIUS Client

Settings

☐ Select an existing template:

Name and Address

Friendly name:
Cisco Switch

Address (IP or DNS):
192.168.15.20

Verify...

Shared Secret

Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

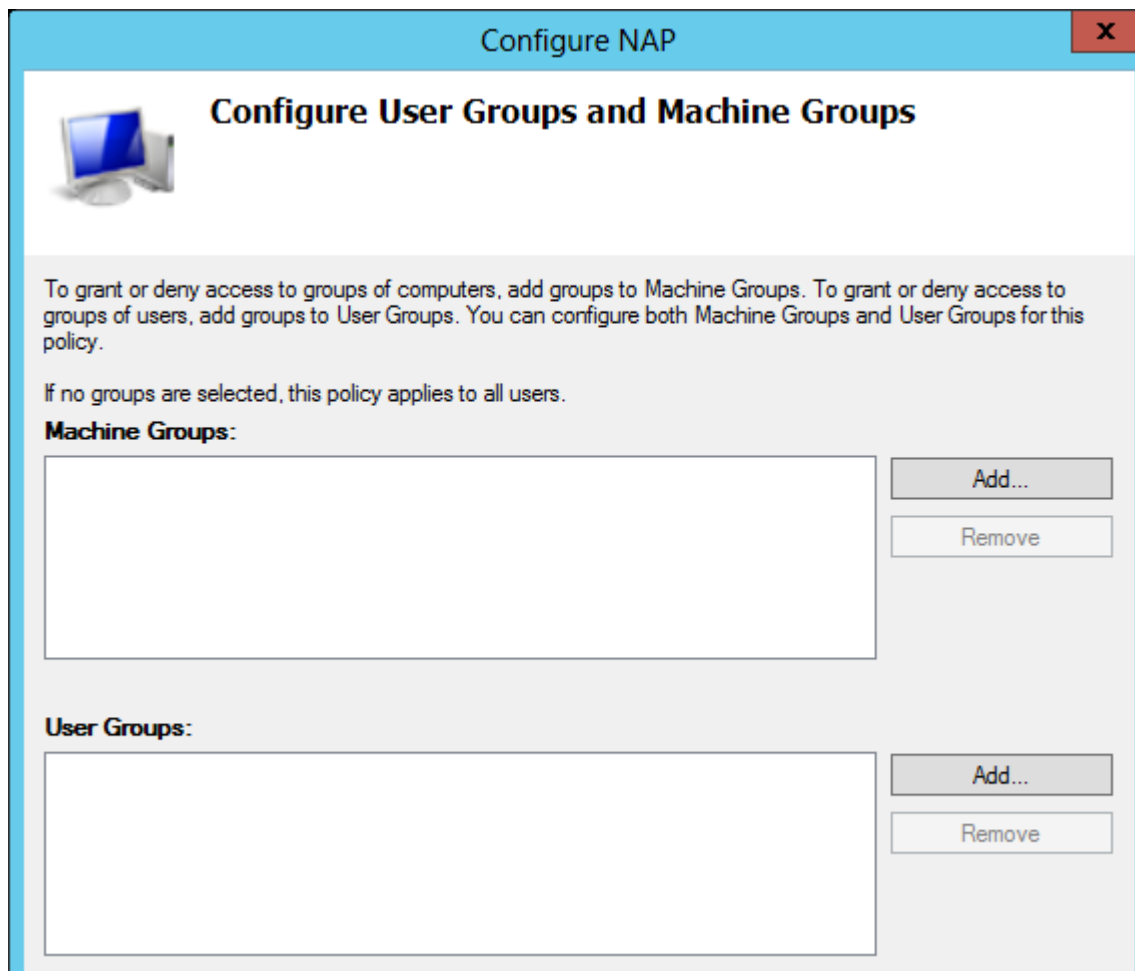
☒ Manual ☐ Generate

Shared secret:
.....

Confirm shared secret:
.....

OK Cancel

Den nächsten Schritt lassen wir momentan offen und konfigurieren diesen im Anschluss von Hand.



The screenshot shows a window titled "Configure NAP" with a close button (X) in the top right corner. Inside the window, there is a section titled "Configure User Groups and Machine Groups" with a small icon of a computer monitor. Below the title, there is a text block explaining that groups can be added to Machine Groups or User Groups to grant or deny access. It also states that if no groups are selected, the policy applies to all users. There are two main sections: "Machine Groups:" and "User Groups:". Each section has a large empty rectangular box for listing groups. To the right of each box are two buttons: "Add..." and "Remove".

Das Zertifikat für die Kommunikation mit dem Domain Controller wird automatisch erkannt und angezeigt.

Configure NAP

Configure an Authentication Method

Protected Extensible Authentication Protocol (PEAP) is the authentication method used with wireless access points and authenticating switches. To configure PEAP, you must select a server certificate on the NPS server and you must configure an authentication type.

NPS Server Certificate

To select a server certificate issued by your organization trusted root certification authority (CA) or a public CA that is trusted by client computers, click Choose. To view the selected certificate, click View.

WS12-NAC.goout.ch (Valid until 7/12/2013 3:49:09 PM)

View... Choose...

EAP types:
Select EAP types to use with PEAP. The authentication type determines the kind of credentials that NPS can accept from client computers and users (either user name and password or a certificate).

☒ Secure Password (PEAP-MS-CHAP v2). This authentication type permits users to type password-based credentials during authentication.

☐ Smart Card or other certificate (EAP-TLS). This authentication type requires certificates on smart cards or in the client computer certificate store. For this authentication type you must deploy your own trusted root CA.

Im ersten Schritt konfigurieren wir die notwendigen Angaben, wenn der Client die Anforderungen des NPS erfüllt.

Configure NAP

Configure Traffic Controls

Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. Examples of traffic controls include virtual LANs (VLANs) or access control lists (ACLs). Your RADIUS client might also support other traffic control attributes. To configure these attributes, enter values for the full access network and the restricted access network.

If you do not use traffic controls or will configure them later, click Next.

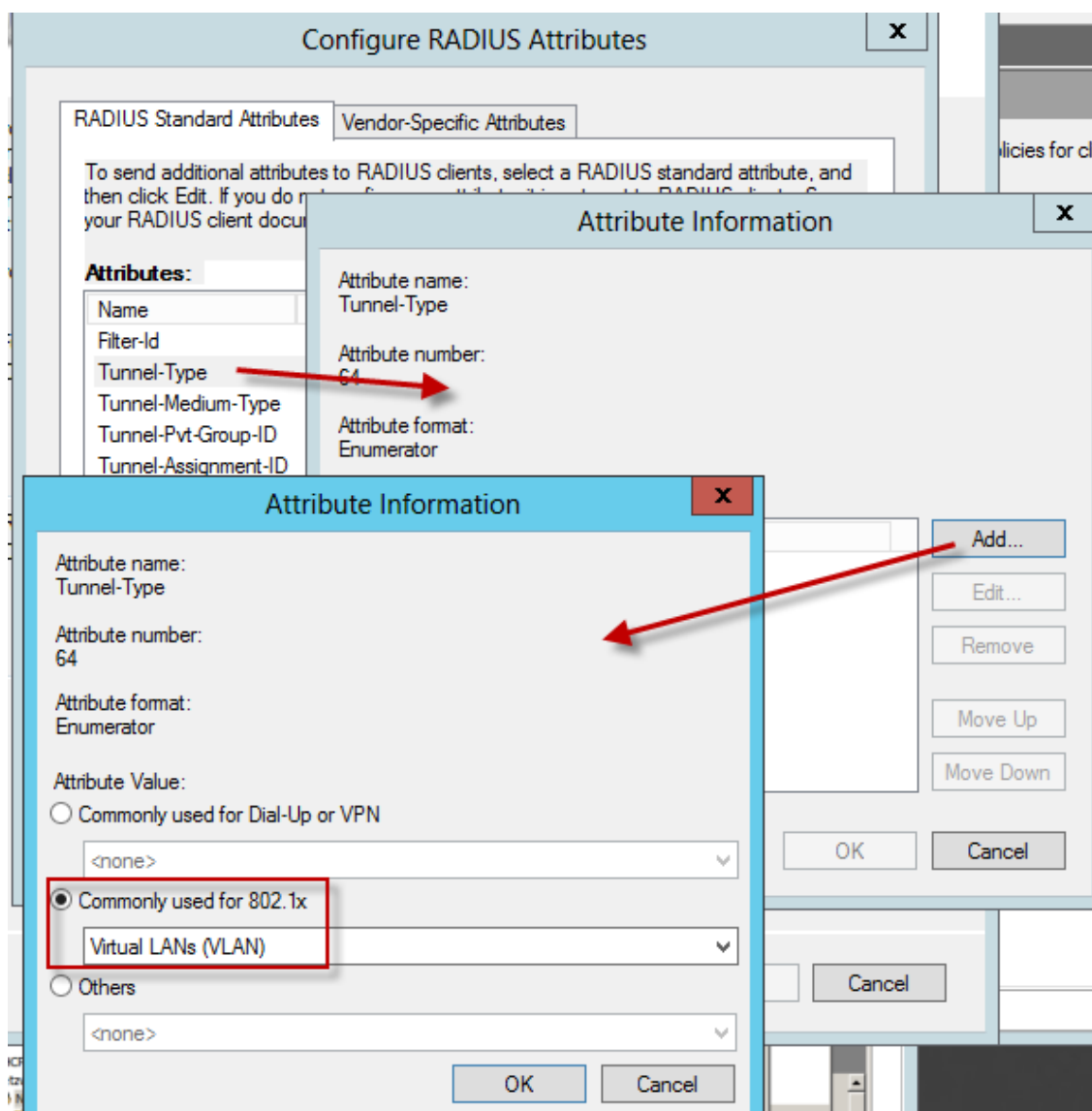
Full access network
Configure RADIUS attributes for computers that are granted full network access.

Configure...

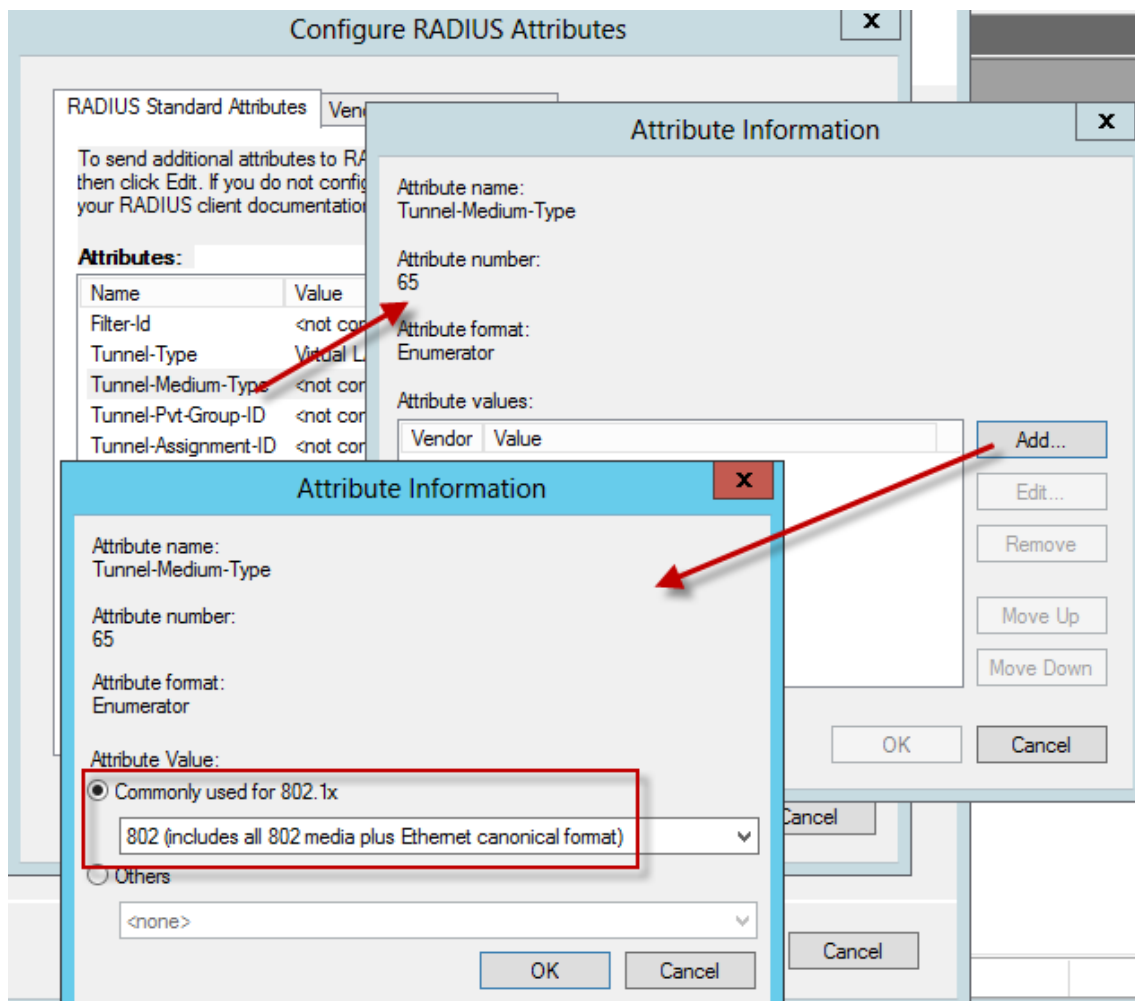
Restricted access network
Configure RADIUS attributes for computers that are granted restricted network access.

Configure...

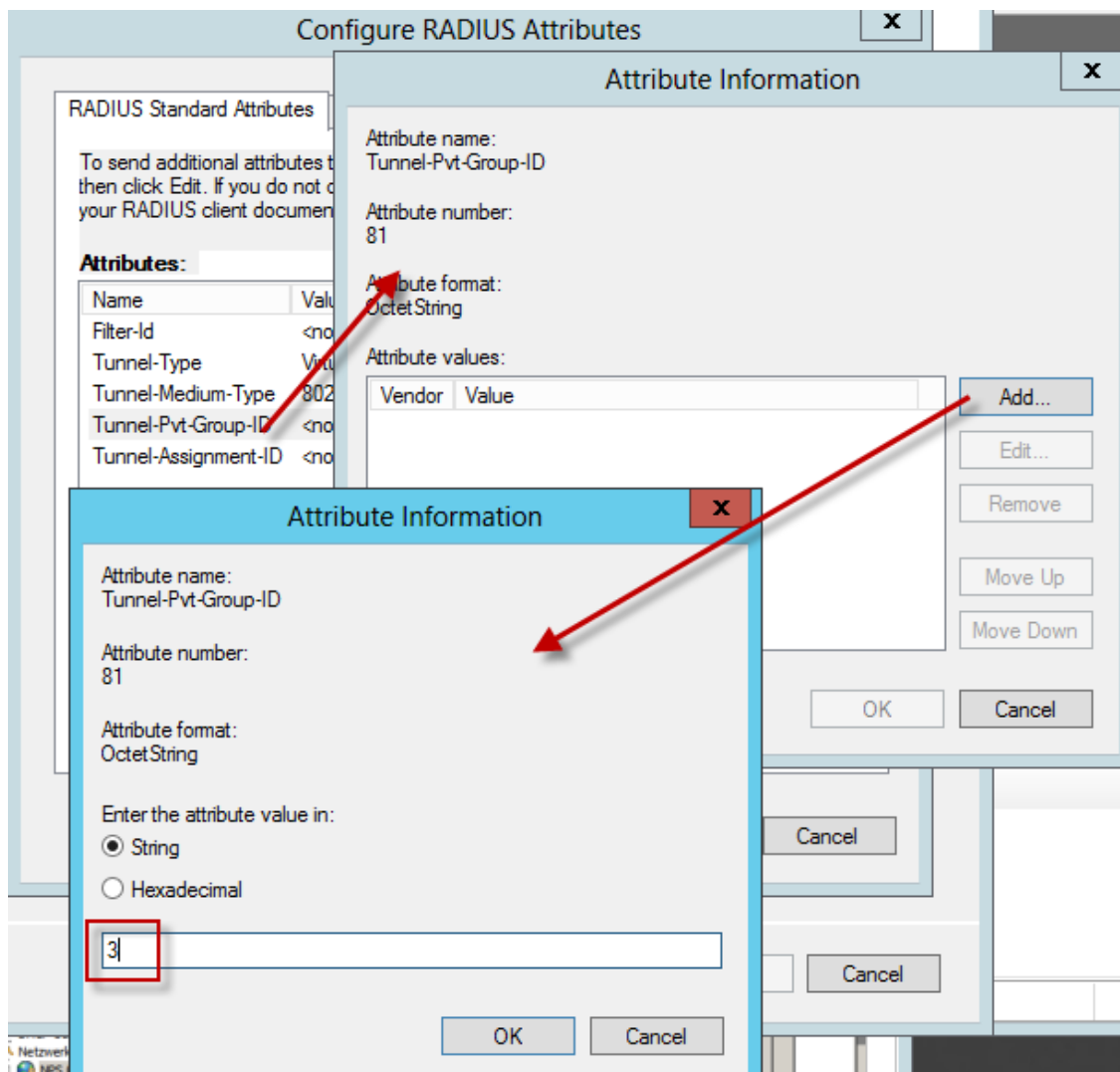
Zuerst wird der Tunnel-Typ ausgewählt (VLAN).



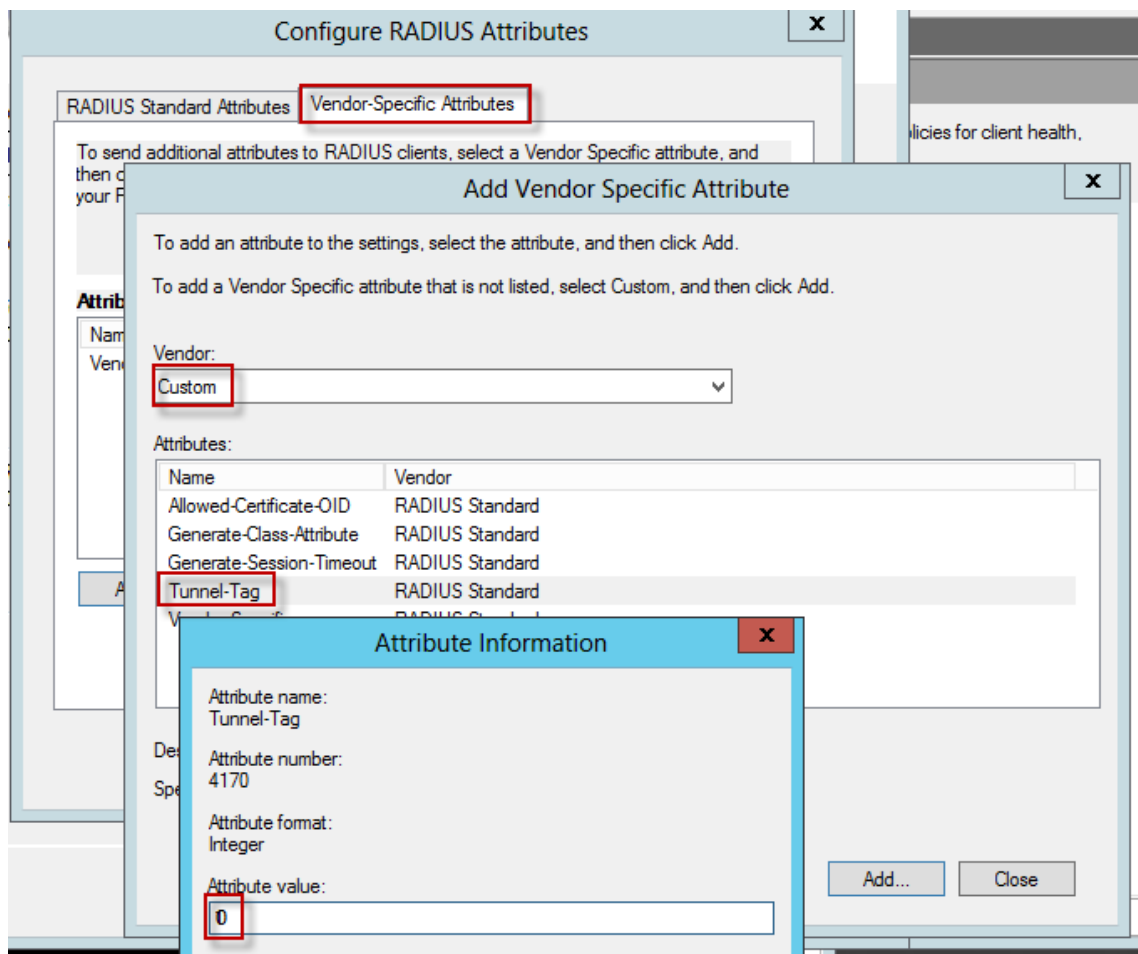
Im zweiten Schritt der Tunnel-Medium-Type (802.1x)



Der dritte Schritt umfasst die Tunnel-Pvt-Group-ID (entsprechendes VLAN). In unserem Beispiel ist dies das VLAN 3.



Für den nächsten Schritt muss unbedingt das Handbuch des Switches beachtet werden. Je nach Gerät kann der Wert 0 oder 1 sein!



Im zweiten Schritt wird das eingeschränkte Netzwerk definiert.

Configure NAP

Configure Traffic Controls

Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. Examples of traffic controls include virtual LANs (VLANs) or access control lists (ACLs). Your RADIUS client might also support other traffic control attributes. To configure these attributes, enter values for the full access network and the restricted access network.

If you do not use traffic controls or will configure them later, click Next.

Full access network

Configure RADIUS attributes for computers that are granted full network access.

Configure...

Restricted access network

Configure RADIUS attributes for computers that are granted restricted network access.

Configure...

Das Vorgehen ist analog den gemachten Schritten, jedoch wird das VLAN 2 zugewiesen.

Configure RADIUS Attributes

RADIUS Standard Attributes | **Vendor-Specific Attributes**

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Filter-Id	<not configured>
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	2
Tunnel-Assignment-ID	<not configured>

Wichtig ist der untere Abschnitt des folgenden Bildes. Was geschieht mit Geräten, die kein NAP können. Hier unbedingt „Deny full network access“ anwählen.

Configure NAP X



Define NAP Health Policy

The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy.

Name
☒ Windows Security Health Validator

☒ Enable auto-remediation of client computers

If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers.

If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated.

Network access restrictions for NAP-ineligible client computers:

☒ Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only.

☐ Allow full network access to NAP-ineligible client computers.

Nun werden alle notwendigen Policies erstellt.

Configure NAP



Completing NAP Enforcement Policy and RADIUS Configuration

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

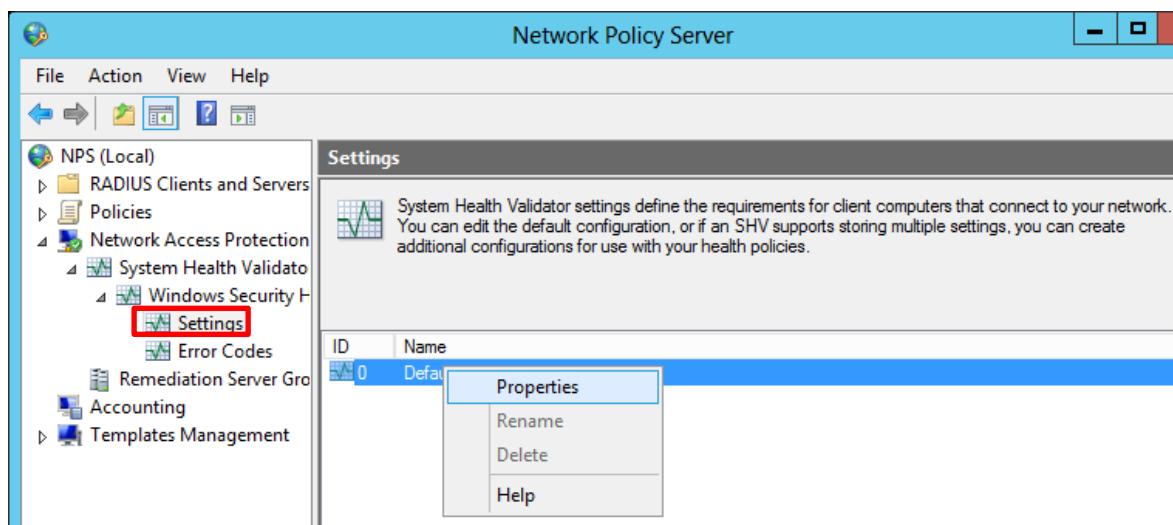
RADIUS clients:
Cisco Switch (192.168.15.20)

Health Policies:
NAP 802.1X (Wired) Compliant
NAP 802.1X (Wired) Noncompliant

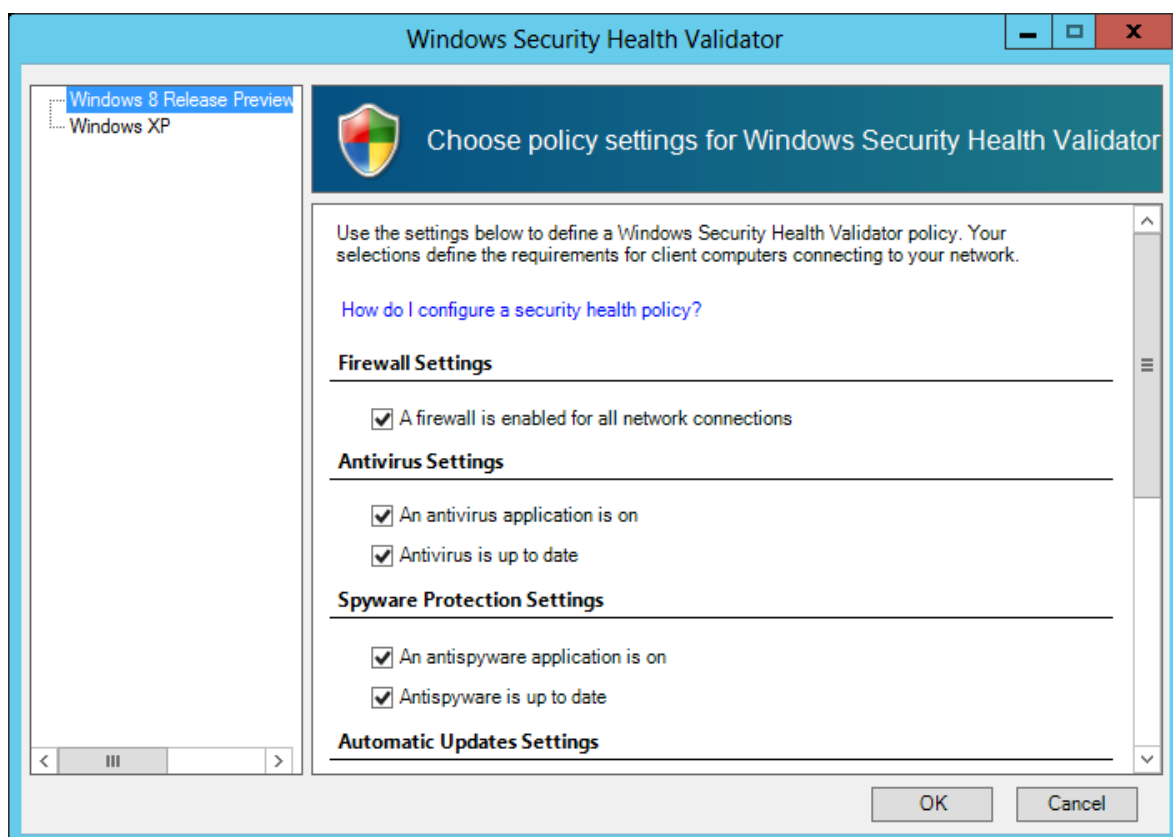
Connection Request Policy:
NAP 802.1X (Wired)

Network Policies:
NAP 802.1X (Wired) Compliant
NAP 802.1X (Wired) Noncompliant
NAP 802.1X (Wired) Non NAP-Capable

Nun können noch die erzwungenen Vorgaben definiert werden.

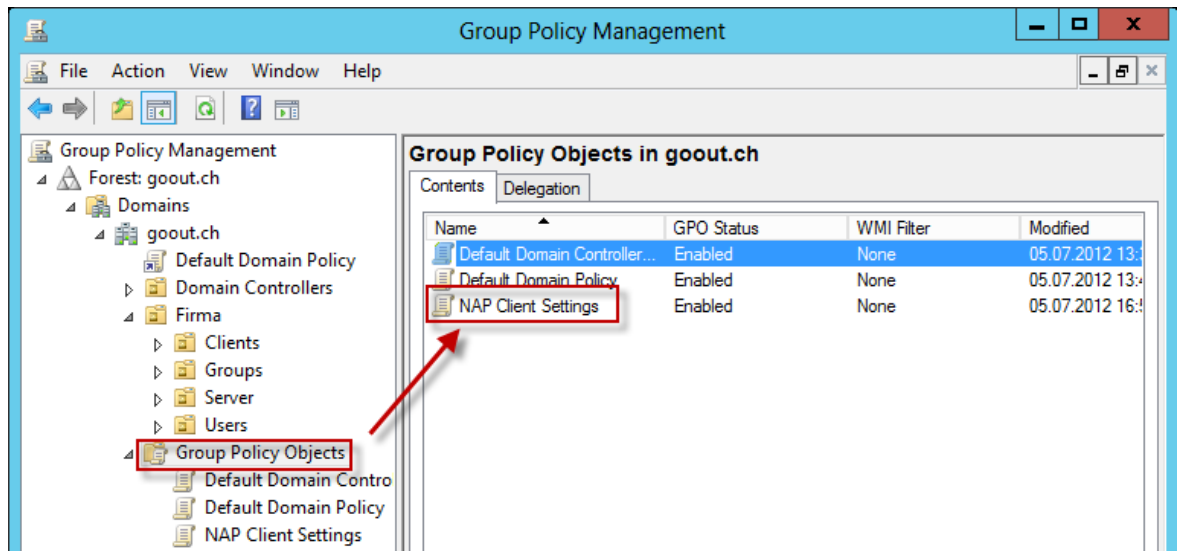


Folgende Kontrollen können durchgeführt werden. Hinweis: Windows XP muss separat konfiguriert werden, da hier keine Antispyware Software vorhanden ist (Windows Defender wurde erst mit Windows Vista eingeführt).

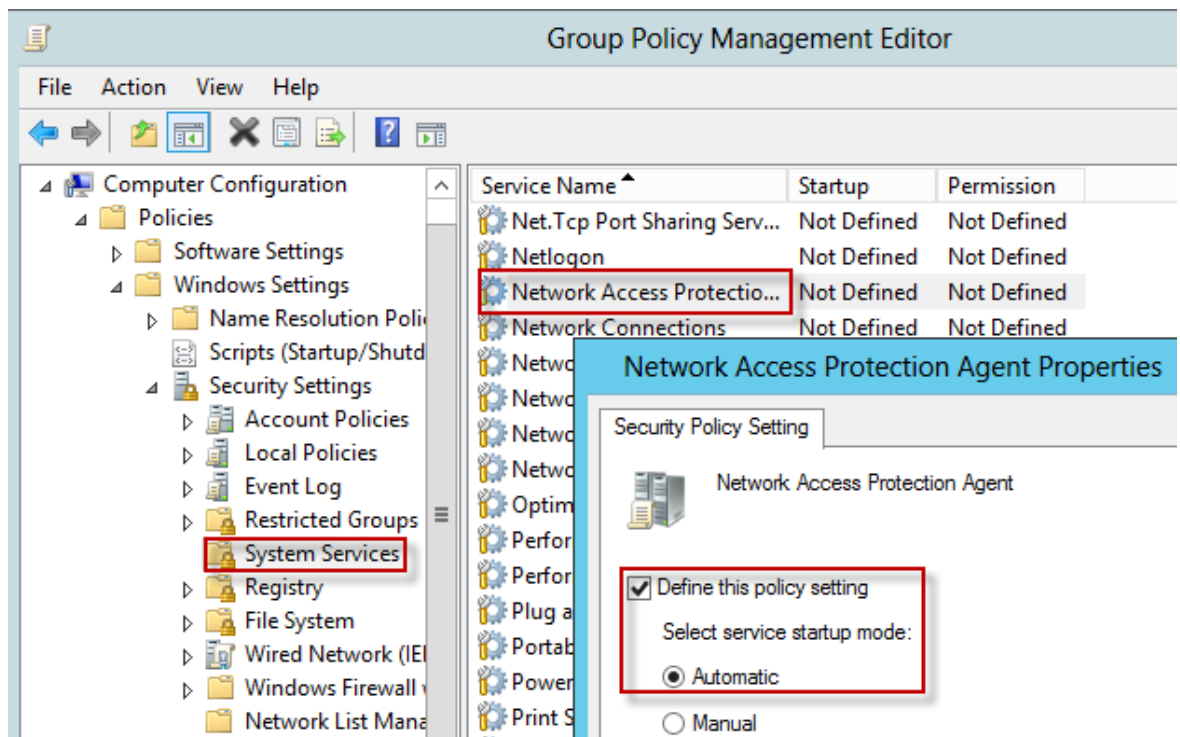


7.3 Gruppenrichtlinie

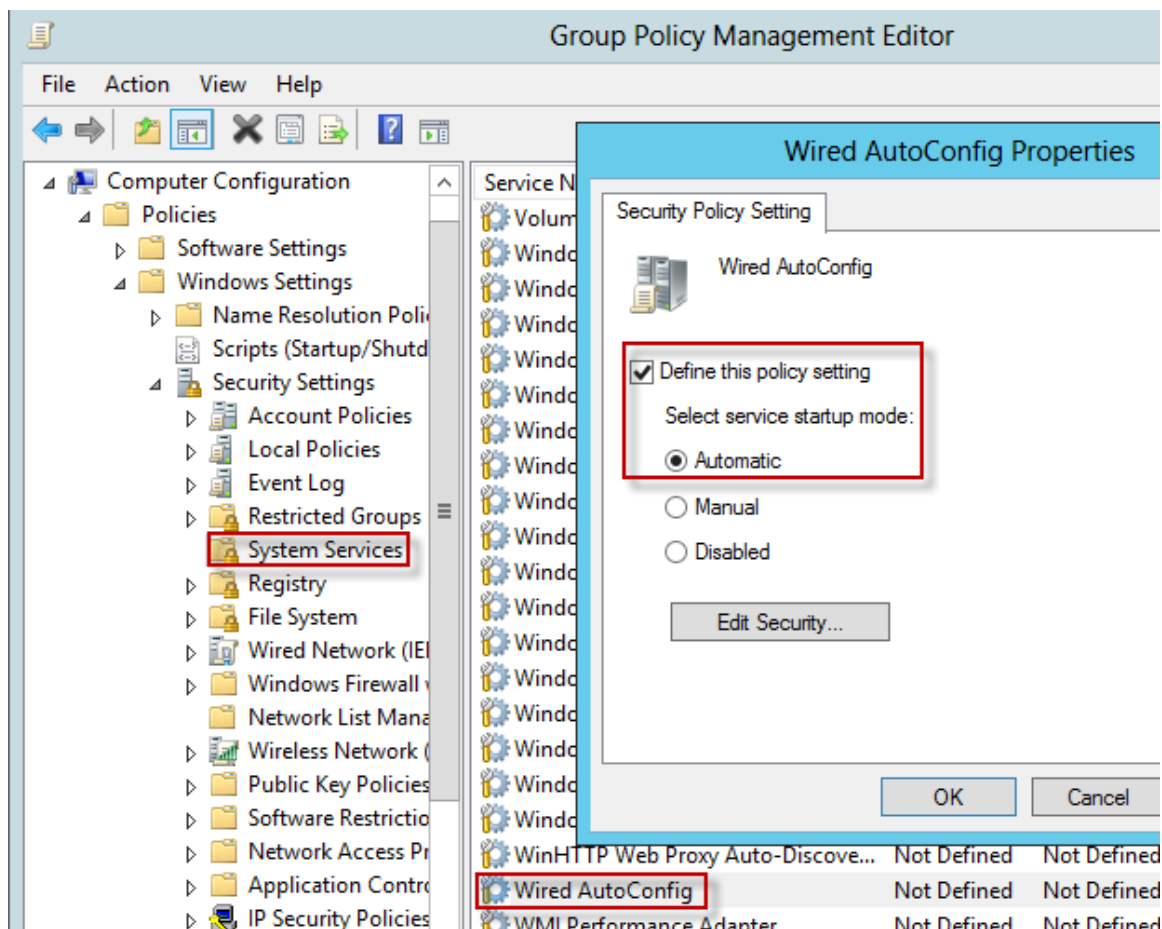
Für die Vorgaben an den Client wird eine neue Gruppenrichtlinie mit dem Namen „NAP Client Settings“ erstellt.



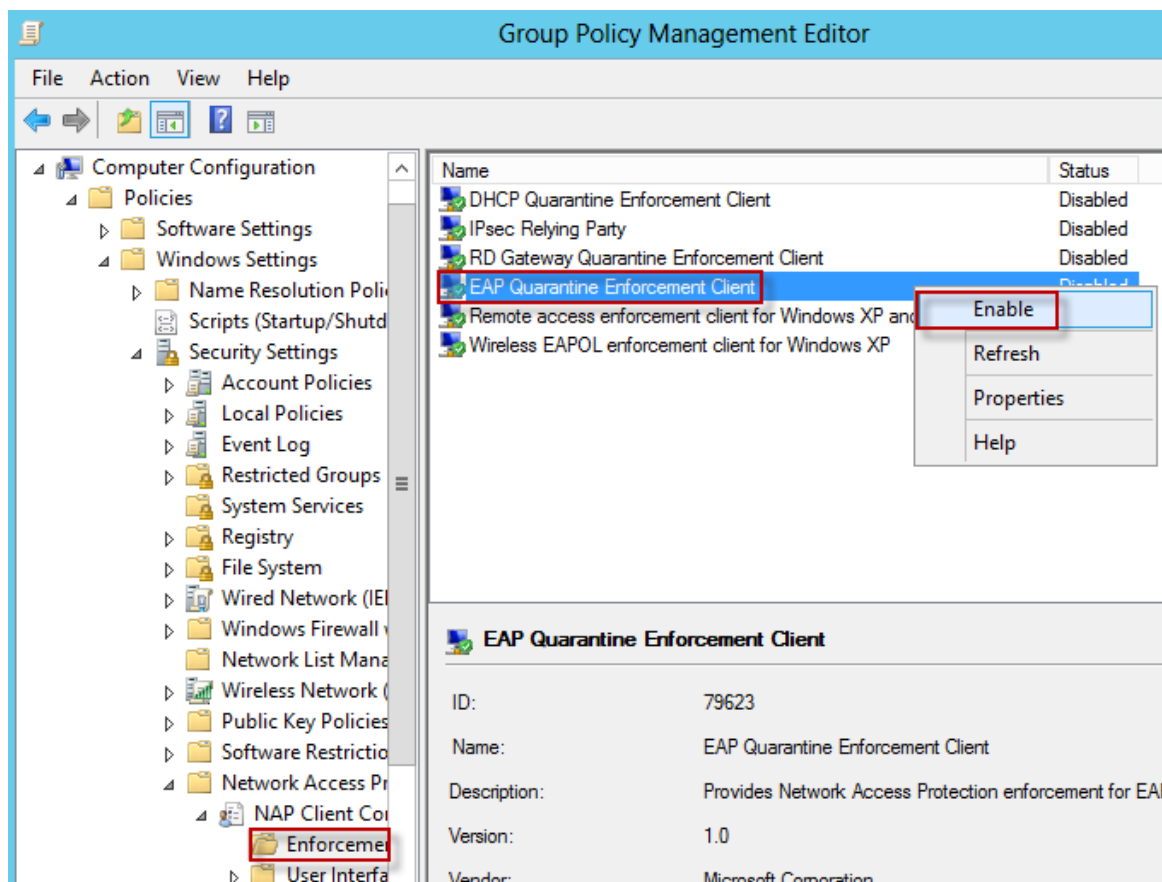
Auf dem Client muss der Dienst „Network Access Protection Agent“ auf „Automatisch“ gesetzt sein.



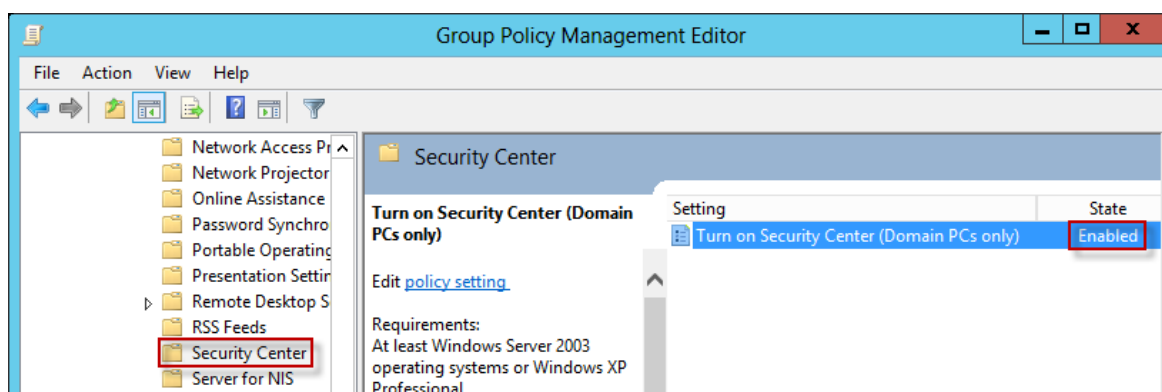
Weiter wird der Wired AutoConfig Dienst auf automatisch gesetzt.



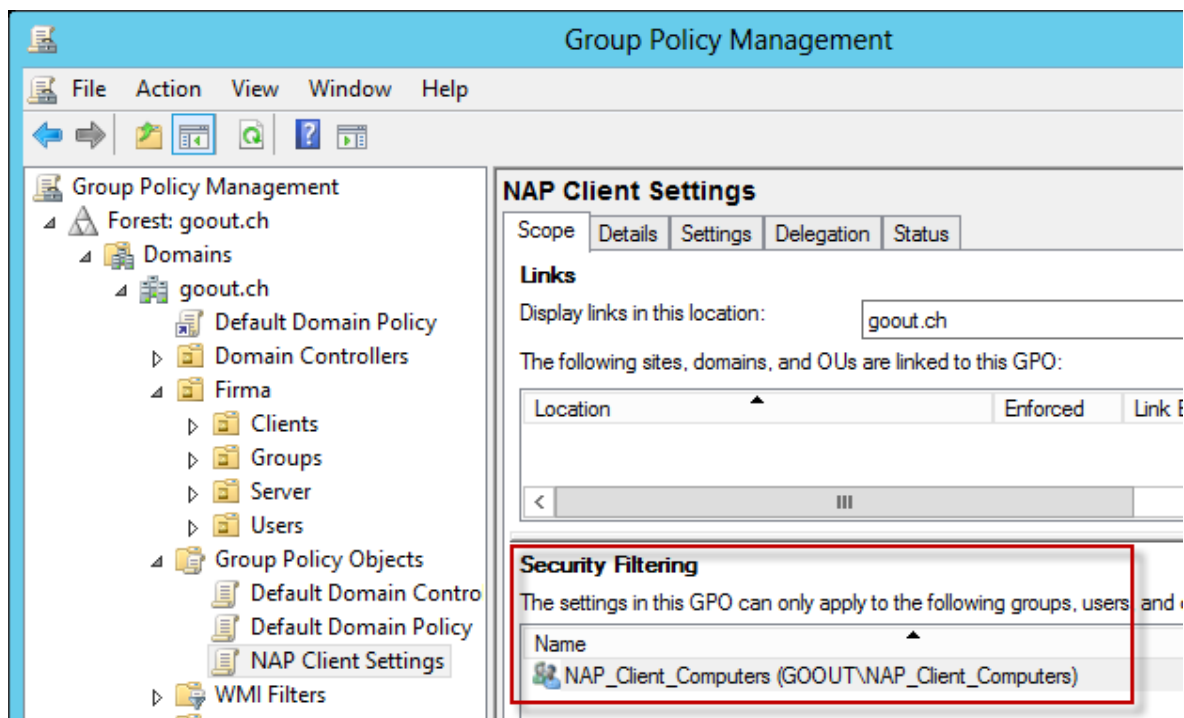
Damit die Kontrollen auf dem Client ausgeführt werden, muss der EAP Quarantine Enforcement Client aktiviert werden.



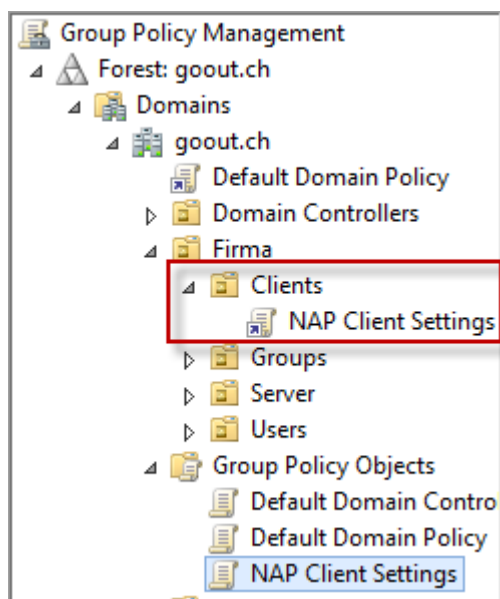
Zudem muss das Security Center aktiviert werden (ist bei domänenintegrierten Clients deaktiviert. Hinweis: Administrative Vorlagen – Windows Komponenten – Sicherheitscenter



Die Gruppenrichtlinie wird nur auf die oben erstellte Gruppe „NAP_Client_Computers“ zugewiesen.



Nun muss die Gruppenrichtlinie noch der entsprechenden OU zugewiesen werden.



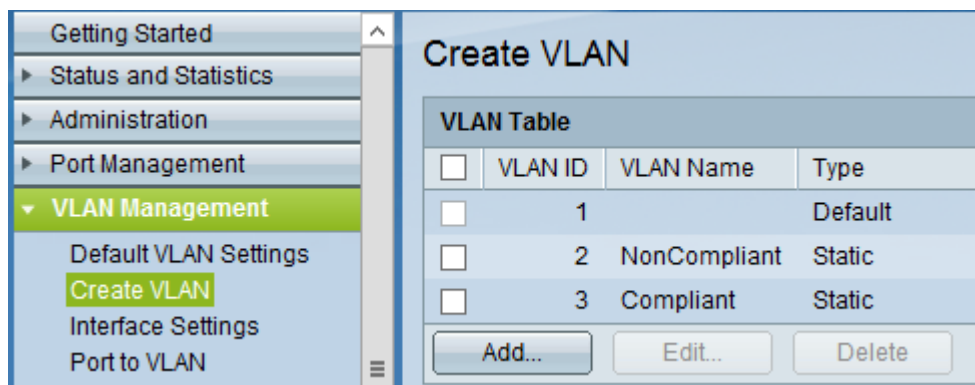
Nachdem der Client neu gestartet wurde, greifen die Richtlinien.

8 Switch

8.1 Cisco

Die folgenden Screenshots zeigen einen Switch der Small Business Reihe.

Zuerst werden die beiden VLANs eingerichtet:

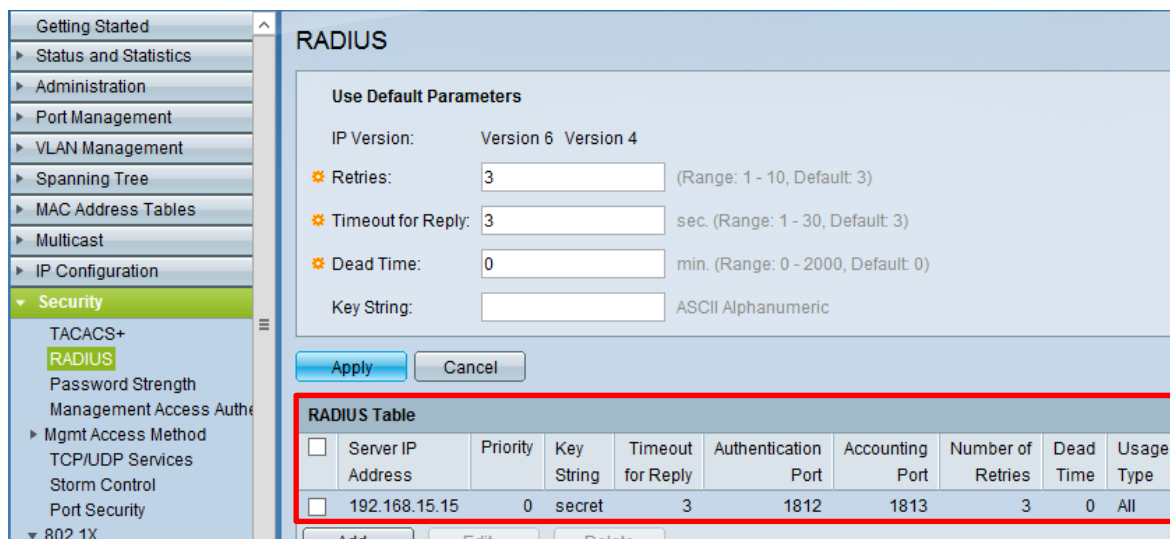


The screenshot shows the 'Create VLAN' configuration page. On the left, a sidebar menu has 'VLAN Management' expanded, with 'Create VLAN' highlighted. The main area is titled 'Create VLAN' and contains a 'VLAN Table' with the following data:

☐	VLAN ID	VLAN Name	Type
☐	1		Default
☐	2	NonCompliant	Static
☐	3	Compliant	Static

Below the table are three buttons: 'Add...', 'Edit...', and 'Delete'.

Im zweiten Schritt werden die Verbindungsdaten zum NPS eingestellt.



The screenshot shows the 'RADIUS' configuration page. On the left, a sidebar menu has 'Security' expanded, with 'RADIUS' highlighted. The main area is titled 'RADIUS' and contains the following configuration options:

- Use Default Parameters**
 - IP Version: Version 6 Version 4
 - Retries: 3 (Range: 1 - 10, Default: 3)
 - Timeout for Reply: 3 sec. (Range: 1 - 30, Default: 3)
 - Dead Time: 0 min. (Range: 0 - 2000, Default: 0)
 - Key String: (Empty field) ASCII Alphanumeric
- RADIUS Table** (highlighted with a red box)

☐	Server IP Address	Priority	Key String	Timeout for Reply	Authentication Port	Accounting Port	Number of Retries	Dead Time	Usage Type
☐	192.168.15.15	0	secret	3	1812	1813	3	0	All

At the bottom of the 'RADIUS' section are 'Apply' and 'Cancel' buttons.

Nun wird 802.1x mit Radius aktiviert.

Properties

Port-Based Authentication: ☒ Enable

Authentication Method: ☐ RADIUS, None
☒ RADIUS
☐ None

Guest VLAN: ☐ Enable

Guest VLAN ID:

Guest VLAN Timeout: ☒ Immediate
☐ User defined

VLAN Authentication Table			
	VLAN ID	VLAN Name	Authentication
☐	2	NonCompliant	Enabled
☐	3	Compliant	Enabled

Damit unter der Small Business Reihe 802.1x greift, muss auch auf dem entsprechenden Port (hier Port 5), Multiple Sessions aktiviert werden.

Edit Host and Session Authentication - G

192.168.15.20/netauthen/security_network_multipleHost

Port:

Host Authentication: ☐ Single
☐ Multiple Host (802.1X)
☒ Multiple Sessions

Action on Violation: ☒ Discard
☐ Forward
☐ Shut Down

Traps: ☐ Enable

* Trap Frequency sec. (

Nun kann auf dem gewünschten Port (hier Port 5) Radius VLAN Assignment aktiviert werden.

SG 300-10 T

- Getting Started
- Status and Statistics
- Administration
- Port Management
- VLAN Management
- Spanning Tree
- MAC Address Tables
- Multicast
- IP Configuration
- Security**
 - TACACS+
 - RADIUS
 - Password Strength
 - Management Access Authen
 - Mgmt Access Method
 - TCP/UDP Services
 - Storm Control
 - Port Security
 - 802.1X
 - Properties
 - Port Authentication**
 - Host and Session Authen
 - Authenticated Hosts
 - Time Range

Port: **g5**

User Name: **GOOUTwiser**

Current Port Control: **Authorized**

Administrative Port Control: ☐ Force Unauthorized ☒ Auto ☐ Force Authorized

RADIUS VLAN Assignment: ☒ Enable

Guest VLAN: ☐ Enable

Authentication Method: ☒ 802.1x Only ☐ MAC Only ☐ 802.1x and MAC

Periodic Reauthentication: ☒ Enable

Reauthentication Period: **300** sec.

Reauthenticate Now: ☐

Authenticator State: **Authenticated**

Time Range: ☐ Enable

Time Range Name: **g5**

Quiet Period: **60** sec.

Resending EAP: **30** sec.

Max EAP Requests: **2** (Rar)

Ports 1-4 sind fix auf VLAN3 gesetzt, Port 5 wird automatisch zugewiesen.

Interface Settings

Filter: *Interface Type* equals to **Port** **Go**

	Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingr Filter
☐	1	g1	Trunk	3	Admit All	Ena
☐	2	g2	Trunk	3	Admit All	Ena
☐	3	g3	Trunk	3	Admit All	Ena
☐	4	g4	Trunk	3	Admit All	Ena
☐	5	g5	Trunk	2	Admit All	Ena

8.2 Switch

Die Konfiguration per Konsole sieht wie folgt aus:

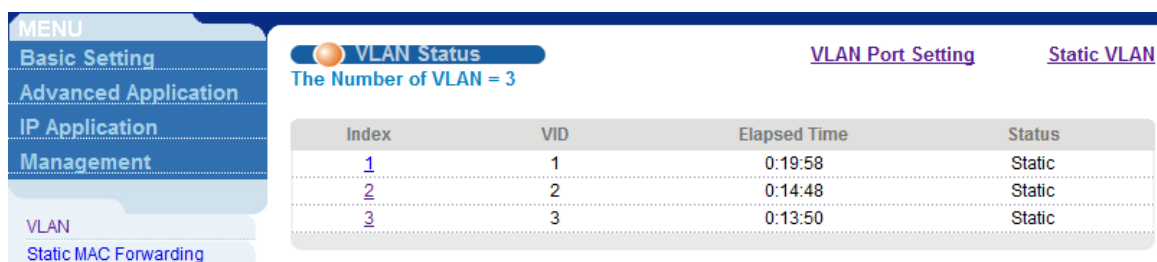
```
hostname NPS-Switch
!
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
errdisable recovery cause security-violation
errdisable recovery interval 30
ip subnet-zero
!
vtp mode transparent
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
dot1x system-auth-control
!
vlan 3
name COMPLIANT
!
vlan 2
name NONCOMPLIANT
!
interface FastEthernet0/1
switchport access vlan 3
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/2
switchport access vlan 3
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/3
switchport access vlan 3
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/4
switchport access vlan 3
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/5
switchport access vlan 2
switchport mode access
dot1x port-control auto
no cdp enable
spanning-tree portfast
!
interface Vlan2
ip address 172.16.0.20 255.255.255.0
!
```

```

interface Vlan3
ip address 192.168.15.20 255.255.255.0
ip default-gateway 192.168.15.1
ip classless
ip http server
!
radius-server host 192.168.15.15 auth-port 1812 acct-port 1813 key secret
radius-server retransmit 3
  
```

8.3 Zyxel

Zuerst werden die beiden VLANs definiert.



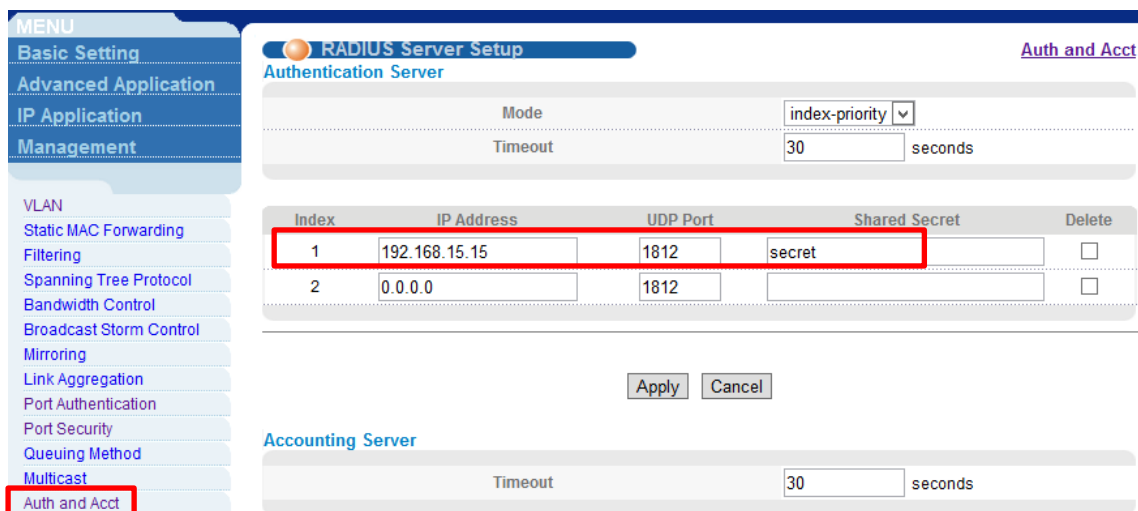
MENU
Basic Setting
Advanced Application
IP Application
Management
VLAN
Static MAC Forwarding

VLAN Status
The Number of VLAN = 3

Index	VID	Elapsed Time	Status
1	1	0:19:58	Static
2	2	0:14:48	Static
3	3	0:13:50	Static

[VLAN Port Setting](#) [Static VLAN](#)

Danach werden die Angaben vom NPS Server eingetragen.



MENU
Basic Setting
Advanced Application
IP Application
Management
VLAN
Static MAC Forwarding
Filtering
Spanning Tree Protocol
Bandwidth Control
Broadcast Storm Control
Mirroring
Link Aggregation
Port Authentication
Port Security
Queuing Method
Multicast
Auth and Acct

RADIUS Server Setup
[Auth and Acct](#)

Authentication Server

Mode: index-priority
Timeout: 30 seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	192.168.15.15	1812	secret	☐
2	0.0.0.0	1812		☐

Apply Cancel

Accounting Server

Timeout: 30 seconds

Die Port Authentication wird auf Port 5 aktiviert.

MENU
 Basic Setting
 Advanced Application
 IP Application
 Management
 VLAN
 Static MAC Forwarding
 Filtering
 Spanning Tree Protocol
 Bandwidth Control
 Broadcast Storm Control
 Mirroring
 Link Aggregation
 Port Authentication

802.1x
 Port Authentication
 Active ☒

Port	Active	Reauthentication	Reauthentication Timer
*	☐	On ▾	seconds
1	☐	On ▾	3600 seconds
2	☐	On ▾	3600 seconds
3	☐	On ▾	3600 seconds
4	☐	On ▾	3600 seconds
5	☒	On ▾	3600 seconds

9 Ergebnis

Wird beim Client die Firewall deaktiviert, wird automatisch ins VLAN2 umgeschaltet, da die automatische Reaktivierung eingeschaltet ist, wird die Firewall automatisch wieder aktiviert und der Client zurück ins VLAN3 verschoben. Ein Ping geht dabei verloren.

```

Reply from 173.194.32.127: bytes=32 time=2ms TTL=57
Reply from 173.194.32.127: bytes=32 time=2ms TTL=57
Reply from 173.194.32.127: bytes=32 time=2ms TTL=57
Reply from 192.168.15.103: Destination host unreachable.
Reply from 173.194.32.127: bytes=32 time=3ms TTL=57
Reply from 173.194.32.127: bytes=32 time=2ms TTL=57
Reply from 173.194.32.127: bytes=32 time=2ms TTL=57
Reply from 173.194.32.127: bytes=32 time=2ms TTL=57
  
```

Kontrolle auf dem Switch. Firewall deaktiviert:

g4	Trunk	3	3U
g5	Trunk	2	2U
g6	Trunk	1	1U

Firewall ist wieder aktiviert:

g3	Trunk	3	3U
g4	Trunk	3	3U
g5	Trunk	2	3U
g6	Trunk	1	1U

Es ist schön ersichtlich, mit welchem Benutzer der Port 5 momentan verbunden ist.

Port Authentication Table									
	Entry No.	Port	User Name	Current Port Control	RADIUS VLAN Assignment	Guest VLAN	Authentication Method	Periodic Reauthentication	Rea
☐	1	g1		Authorized	Disabled	Disabled	802.1x Only	Disabled	
☐	2	g2		Authorized	Disabled	Disabled	802.1x Only	Disabled	
☐	3	g3		Authorized	Disabled	Disabled	802.1x Only	Disabled	
☐	4	g4		N/A	Disabled	Disabled	802.1x Only	Disabled	
☒	5	g5	GOOUTwiser	Authorized	Enabled	Disabled	802.1x Only	Enabled	
☐	6	g6		N/A	Disabled	Disabled	802.1x Only	Disabled	
☐	7	g7		N/A	Disabled	Disabled	802.1x Only	Disabled	
☐	8	g8		N/A	Disabled	Disabled	802.1x Only	Disabled	
☐	9	g9		N/A	Disabled	Disabled	802.1x Only	Disabled	
☐	10	g10		N/A	Disabled	Disabled	802.1x Only	Disabled	

Untenstehend die Logdaten aus dem Zyxel Switch.

MENU

- Basic Setting
- Advanced Application
- IP Application
- Management
- Maintenance
- Access Control
- Diagnostic

Diagnostic

```

51 Thu Aug 09 17:51:34 2012 PP15 WARN 802.1x
Authentication - retransmit EAPOL-START packet [User-Name
GOOUT\wisler] [NAS-Port 5]
52 Thu Aug 09 17:51:36 2012 PP15 WARN 802.1x
Authentication - retransmit EAPOL-START packet [User-Name
GOOUT\wisler] [NAS-Port 5]
55 Thu Aug 09 17:52:30 2012 PP15 WARN 802.1x
Authentication - retransmit EAPOL-START packet [User-Name
GOOUT\wisler] [NAS-Port 5]
56 Thu Aug 09 17:52:33 2012 PP15 WARN 802.1x

```

10 Kontrollen

Mit dem Befehl „nap client show state“ kann überprüft werden, ob NAP aktiv ist (d.h. der Dienst ist gestartet).

```

Id                = 79623
Name              = EAP Quarantine Enforcement Client
Description       = Provides Network Access Protection enforcement for EAP
authenticated network connections, such as those used with 802.1X and UPN techno
logies.
Version           = 1.0
Vendor name       = Microsoft Corporation
Registration date  =
Initialized       = Yes

```

Mit „netsh nap client show group policy“ kann zusätzlich überprüft werden, ob die Gruppenrichtlinie sauber greift.

```

Name              = EAP Quarantine Enforcement Client
ID               = 79623
Admin             = Enabled

```