ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik & Security

fh st.pölten

Übung3

BCN

IT Security - VZ

Kevin Lopci 2410410042

Stand: 07. August 2025

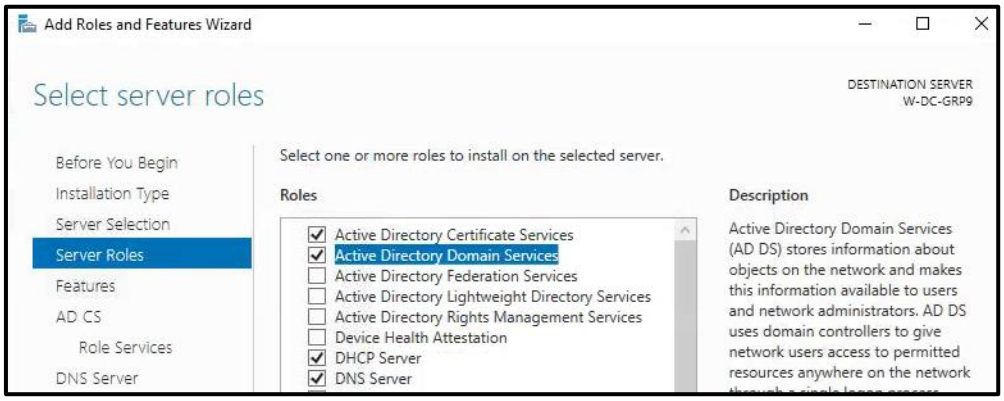
Inhaltsverzeichnis / Table of Contents

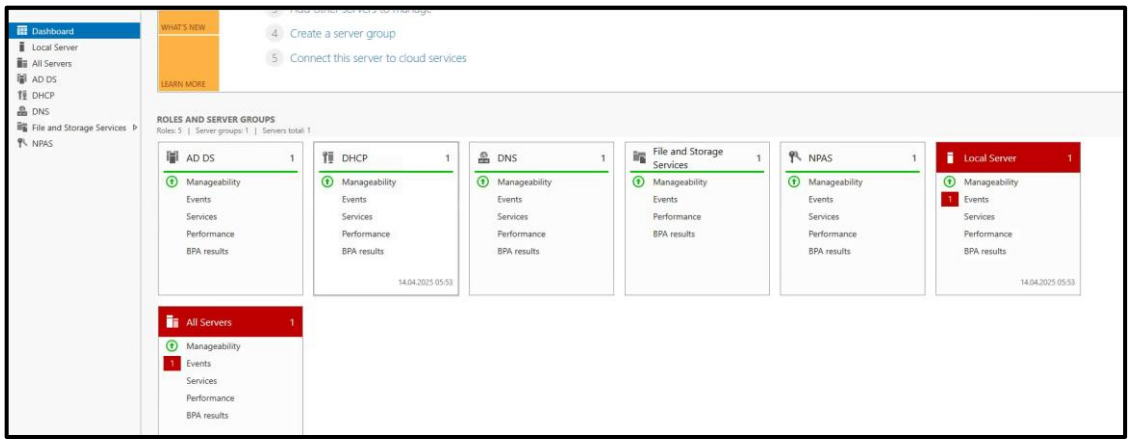
2 Infrastructure Requirements

Server infrastructure

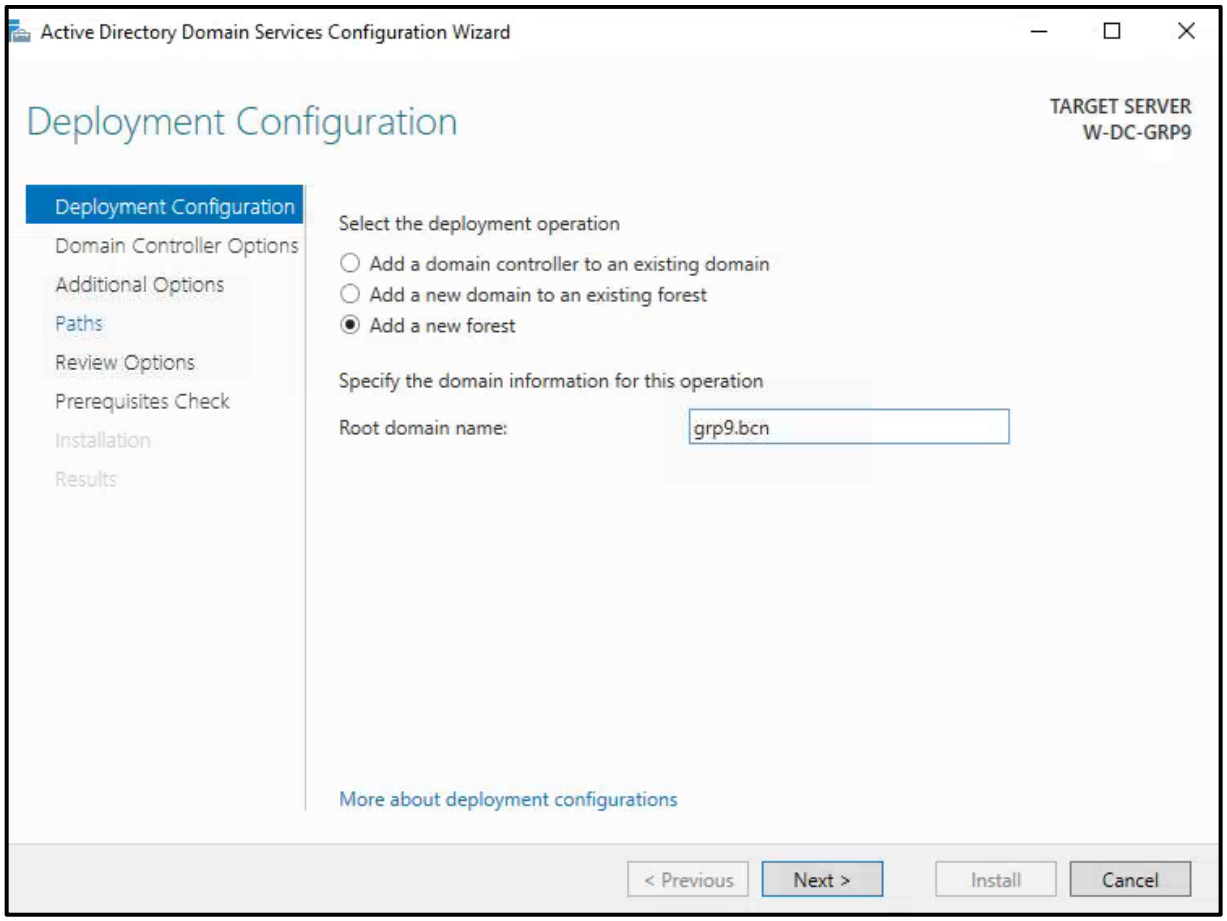
1.The Windows Server handles the DC (Domain Controller), DNS, DHCP and PKI services. The domain name (= DNS name) must be “grpY.bcn”, where Y is your group number (as found on eCampus). Create all users and groups in the OU “GrpY” and use self-explanatory names for them.

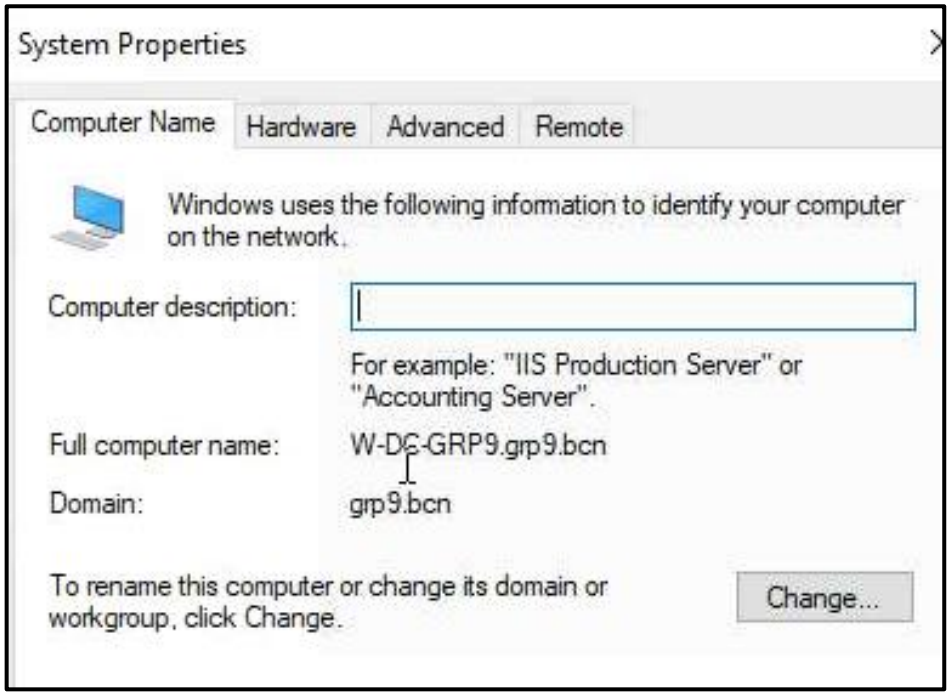
The above-mentioned roles are installed on DC seen.





Then we need to create the domain grp9.bcn on our DC server. We promote the server to a DC first by clicking the flag on top when the service is installed and click “configure as Domain Controller” the following wizard will pop up. Just follow along the instructions.

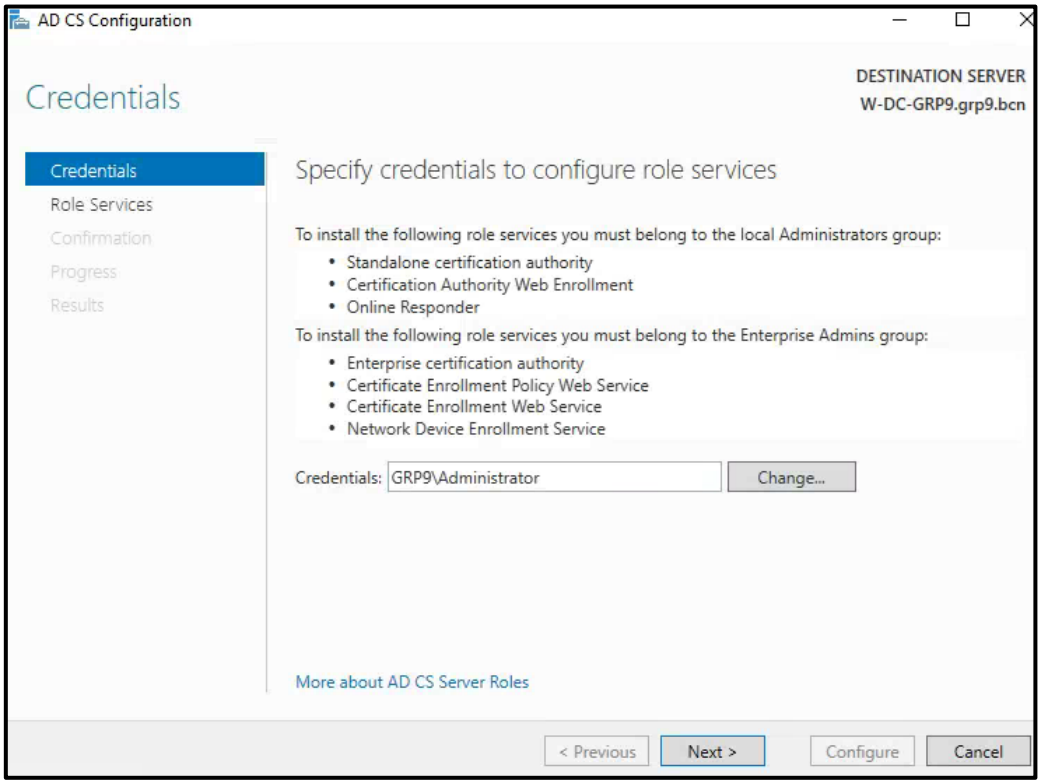


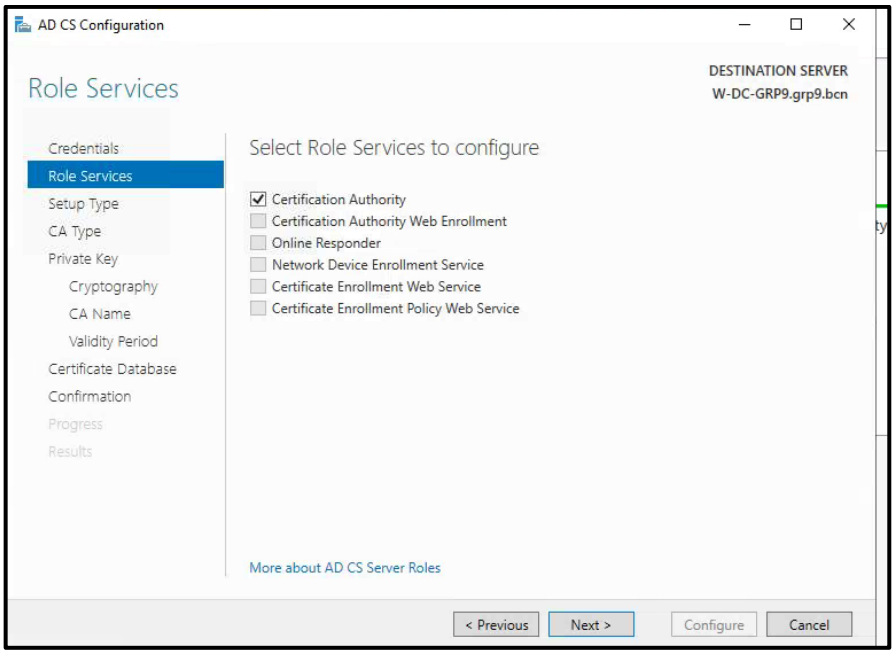


Kevin Lopci 2410410042

2.CA for 802.1x installieren und konfigurieren mit Template.

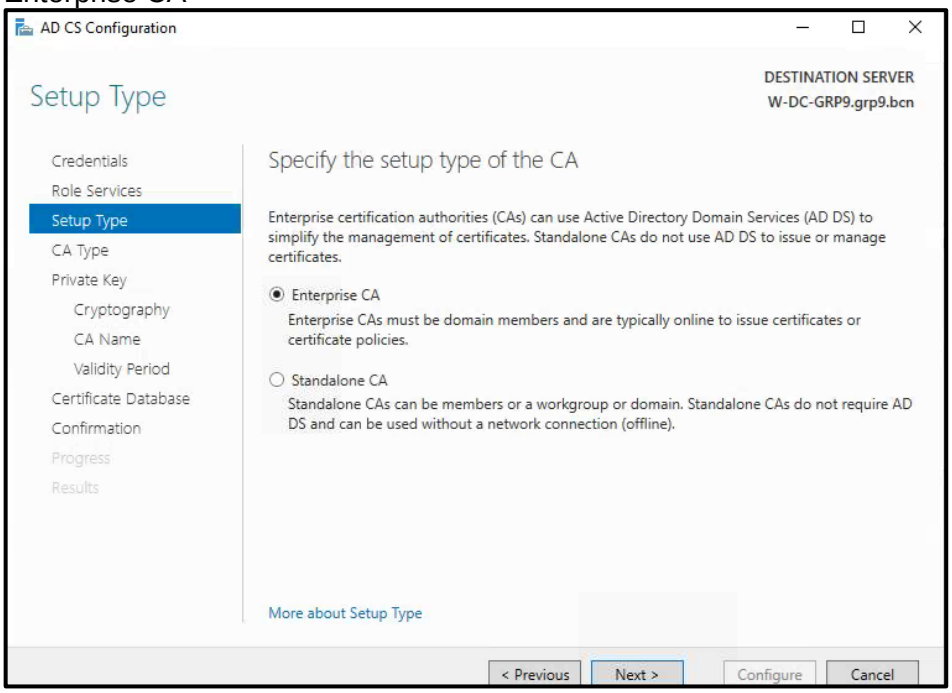
Certificate Authority needs to be installed on our Server in order for machine authentication to work..



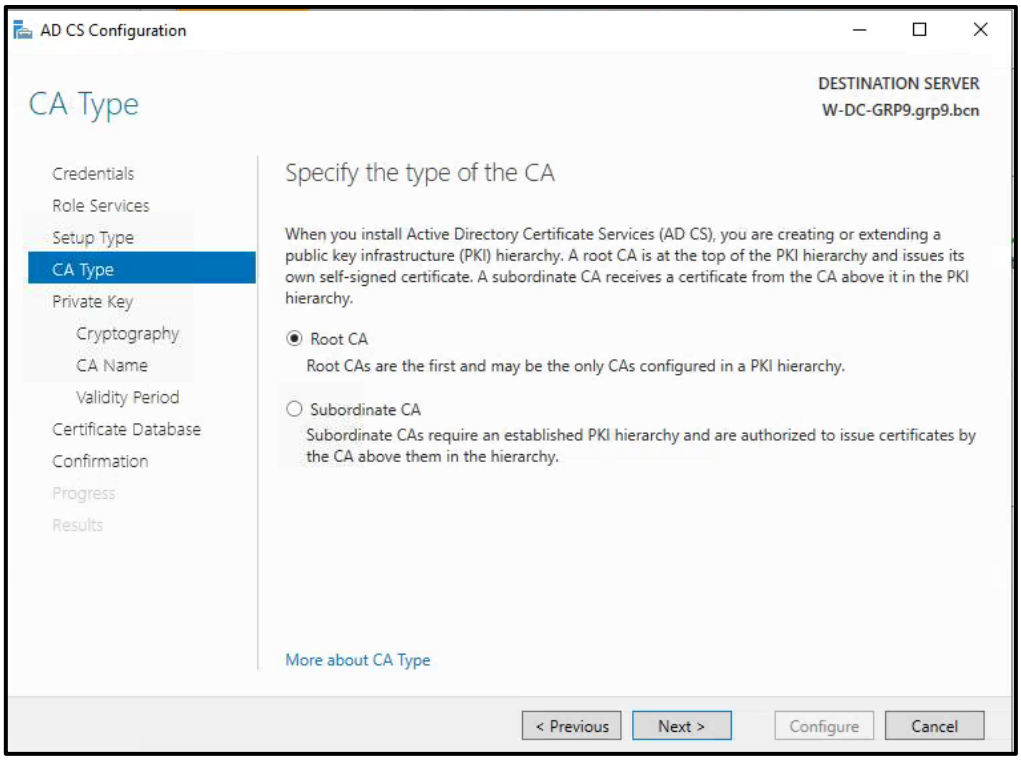


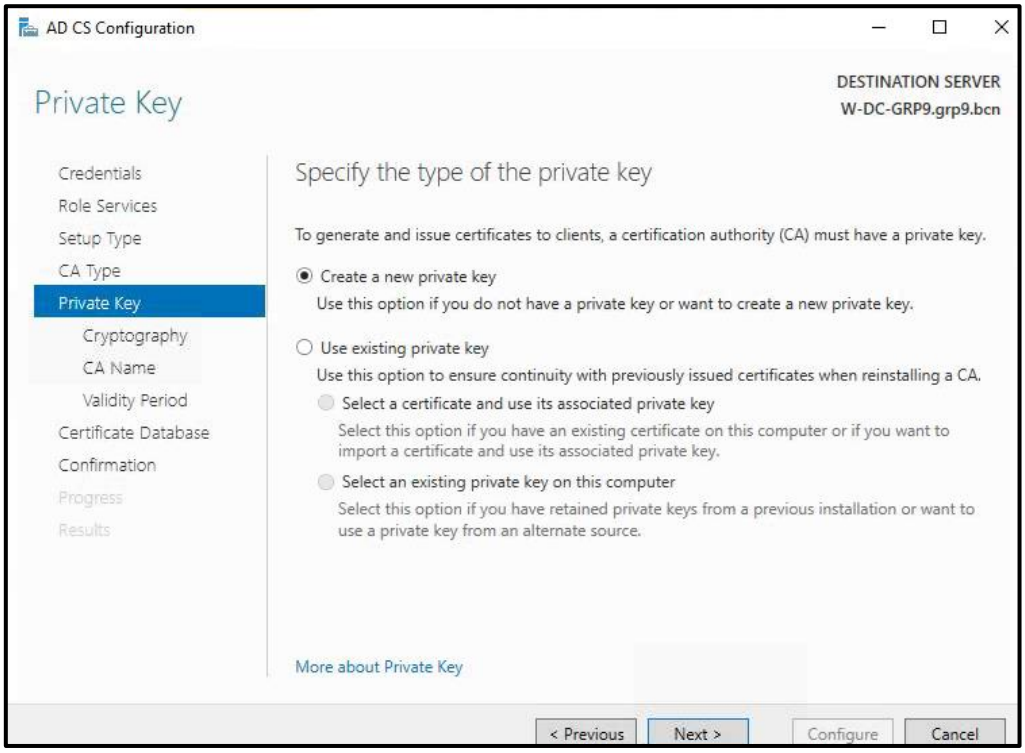
CA wählen

Enterprise CA

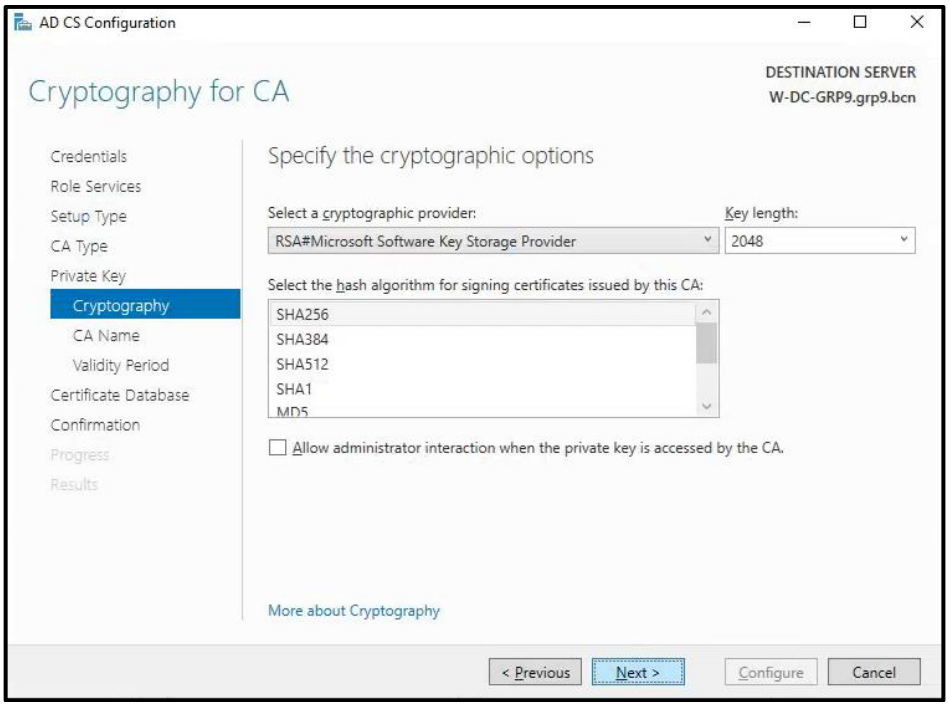


Root CA

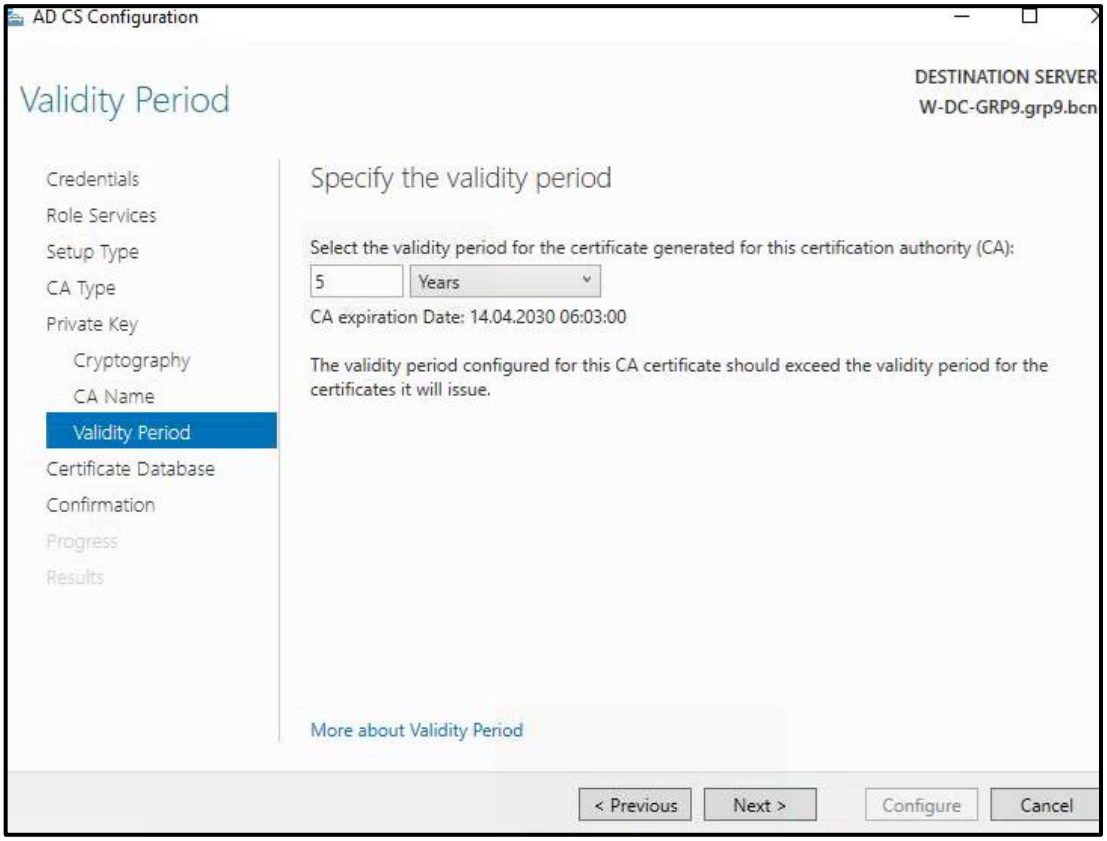




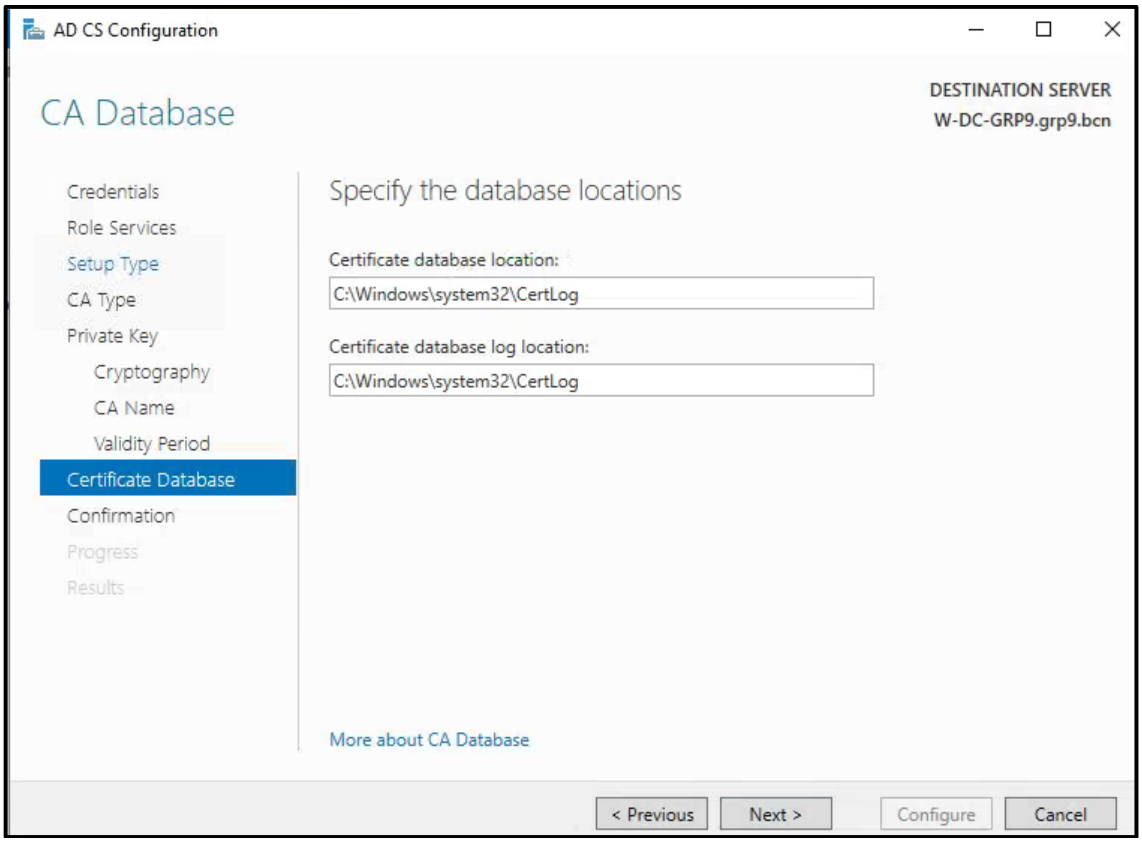
SHA 256 wählen


AD CS Configuration
Cryptography for CA
DESTINATION SERVER
W-DC-GRP9.grp9.bcn
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the cryptographic options
Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider
Key length:
2048
Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1
MD5
Allow administrator interaction when the private key is accessed by the CA.
More about Cryptography
< Previous
Next >
Configure
Cancel

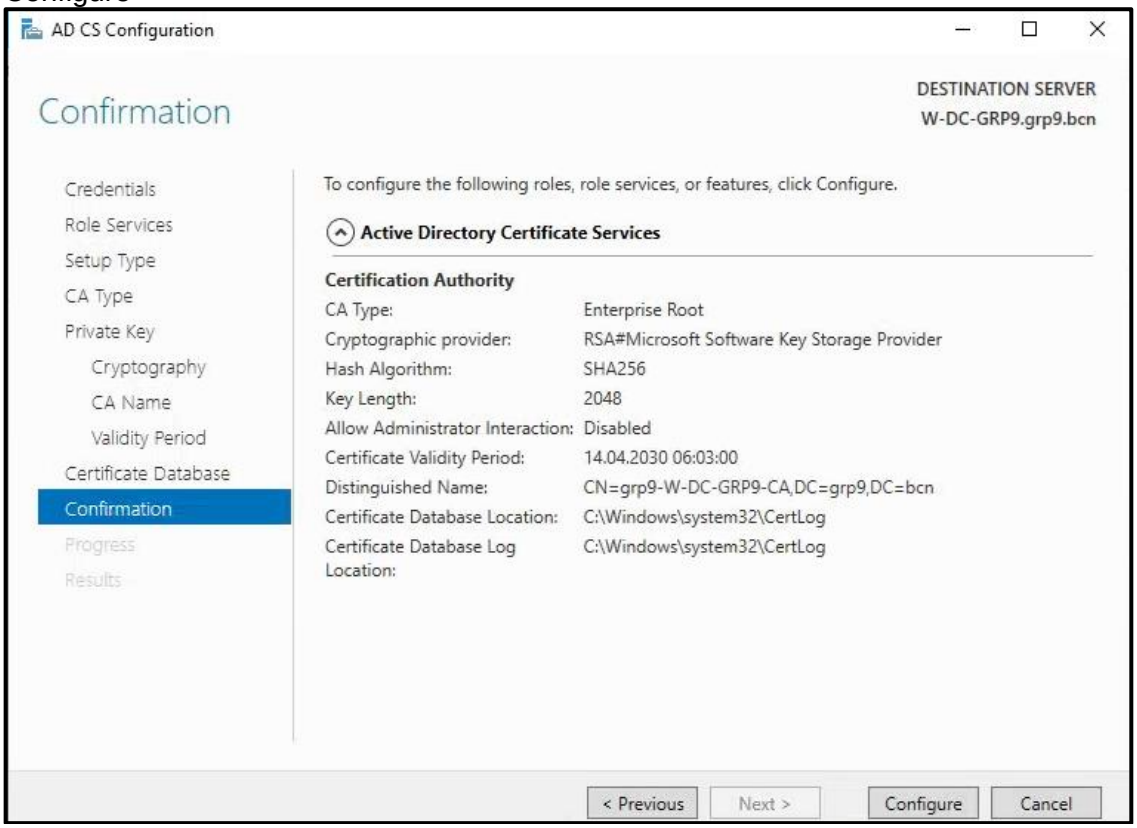
Next


AD CS Configuration
Validity Period
DESTINATION SERVER
W-DC-GRP9.grp9.bcn
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the validity period
Select the validity period for the certificate generated for this certification authority (CA):
5
Years
CA expiration Date: 14.04.2030 06:03:00
The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.
More about Validity Period
< Previous
Next >
Configure
Cancel

Next



Configure

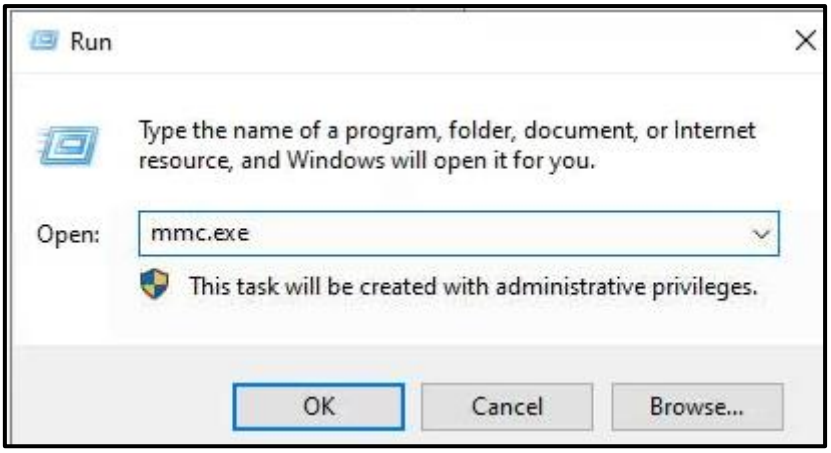


Am Ende Configure klicken.

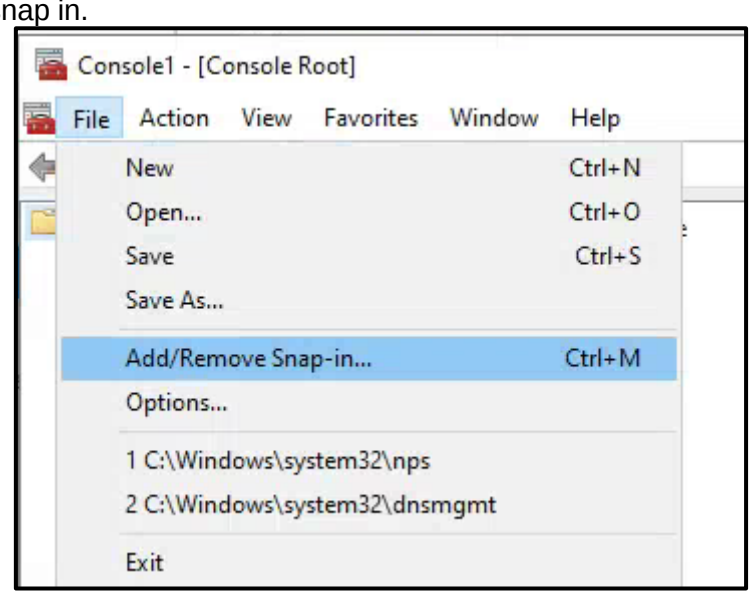
When we open CA, it should be listed here:

Kevin Lopci 2410410042

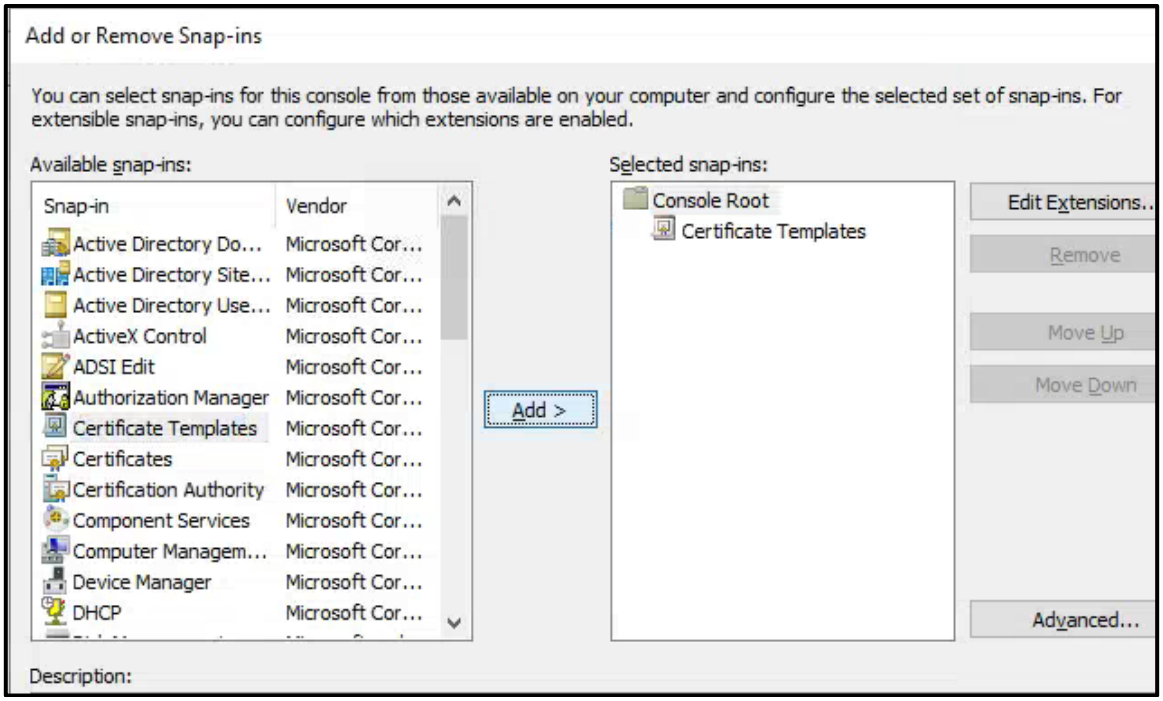
Now that we have configured our root CA we need to create a template to use.
We open the console.



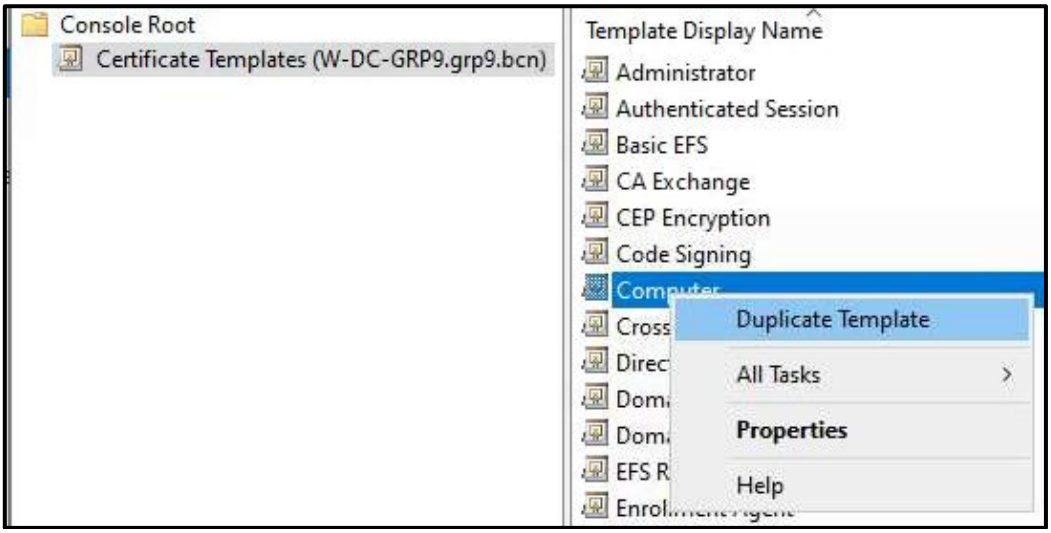
Click Add / remove snap in.



Add certificiate templates.

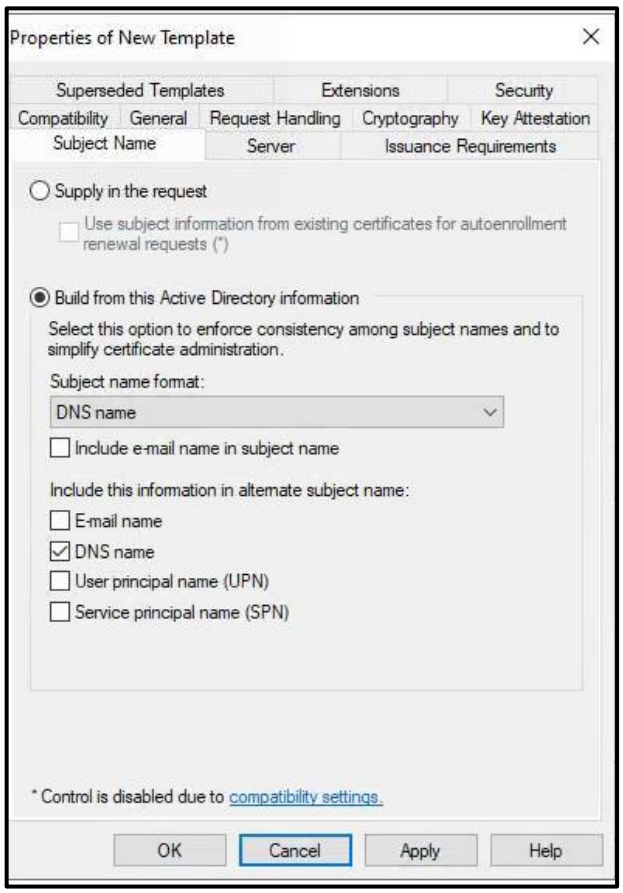


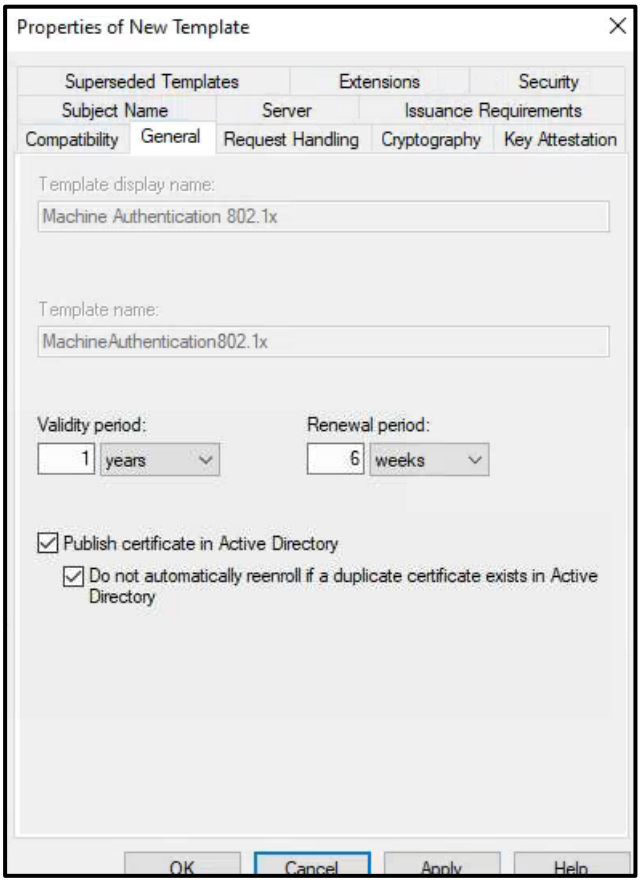
Duplicate template.



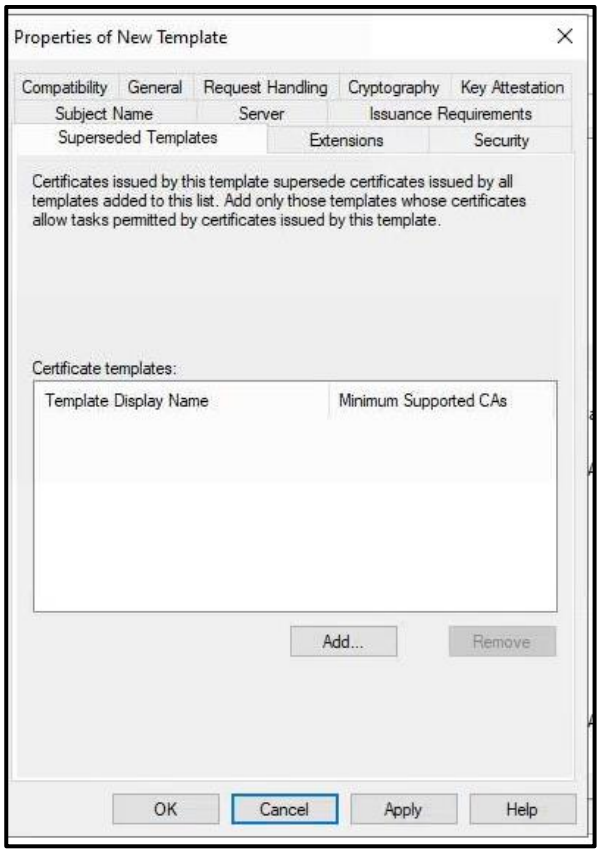
Kevin Lopci 2410410042

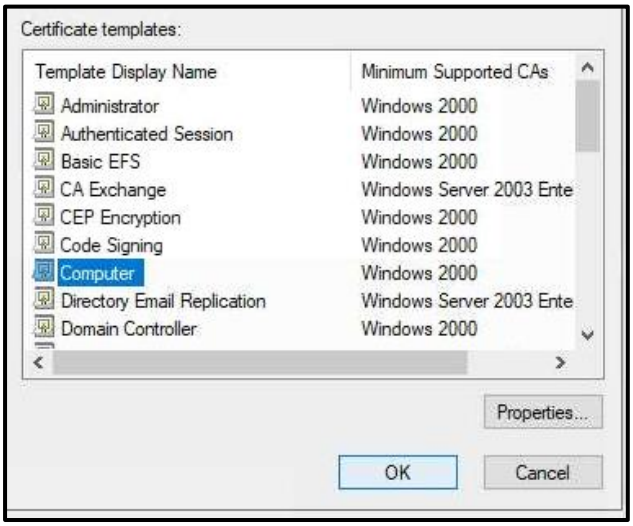
Choose DNS Name. In the general tab,give it a name,Publish it in AD, and make sure to tick the other option as well so that a machine doesn't get a new certificate everytime it boots.



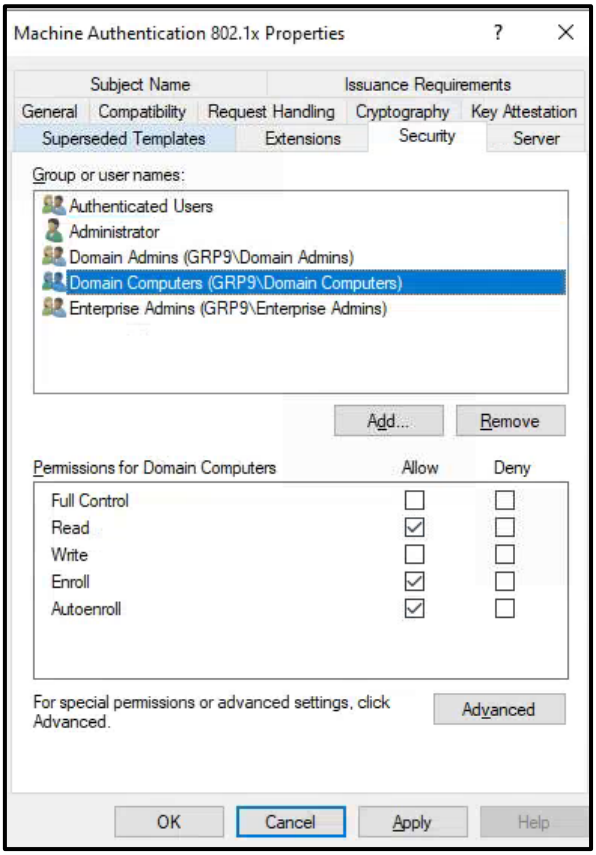


Switch to suspended templates,click on computer and press ok.



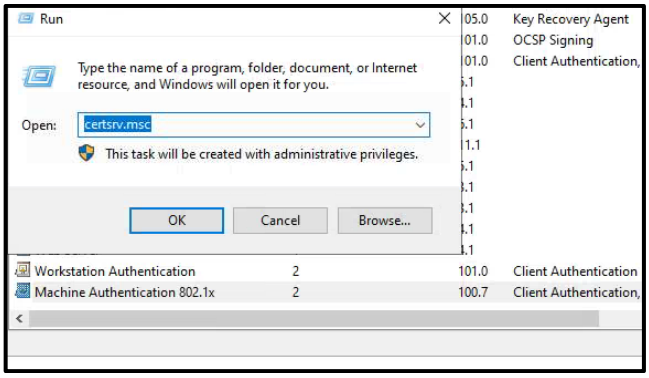


In the security tab, Domain Coputers,should be able to read,enroll and autoenroll. Click apply and ok.

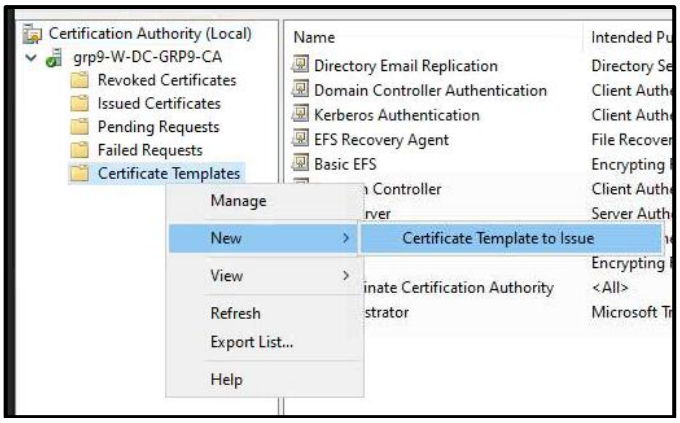


Kevin Lopci 2410410042

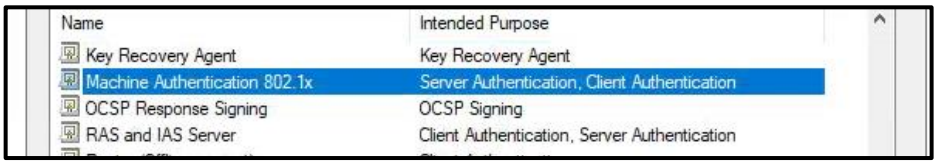
Run this command to open Certificate Authority Server



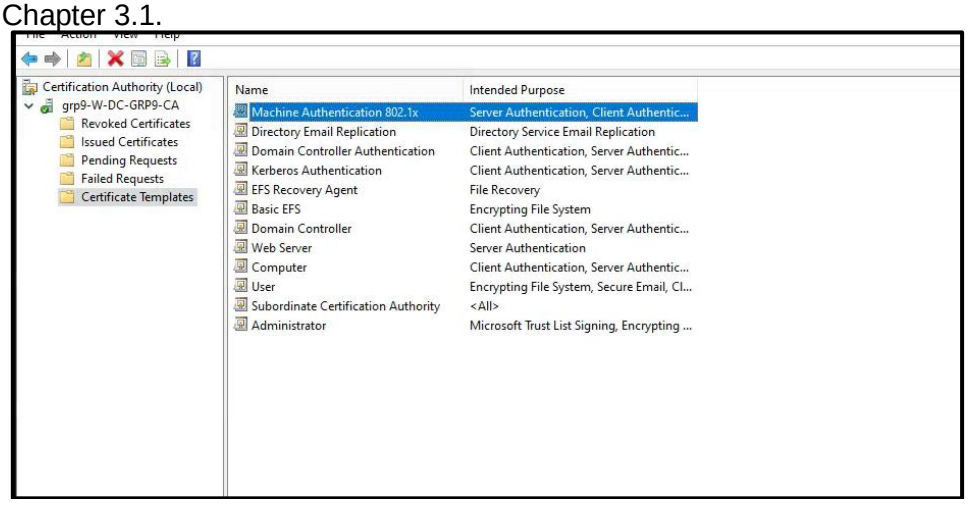
We need to issue our new 802.1x machine authentication certificate.



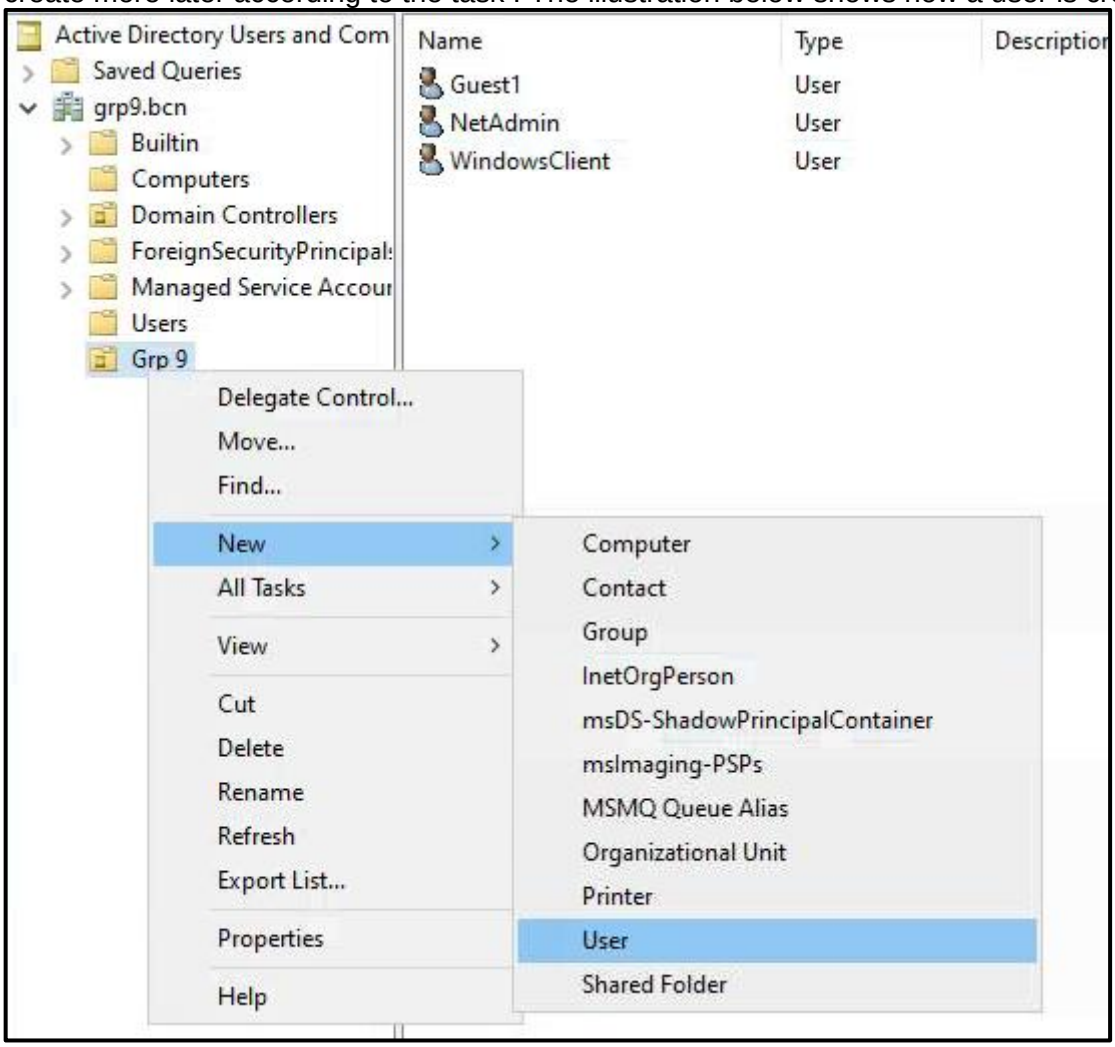
Find it and press ok.



Now that the Certificate is enabled , we need to configure a GPO for the auto-enrollment , this will be shown in Chapter 3.1.



„Grp 9“ OU is created, and for now these are the test users that we have in plan of creating. We will create more later according to the task . The illustration below shows how a user is created in AD.



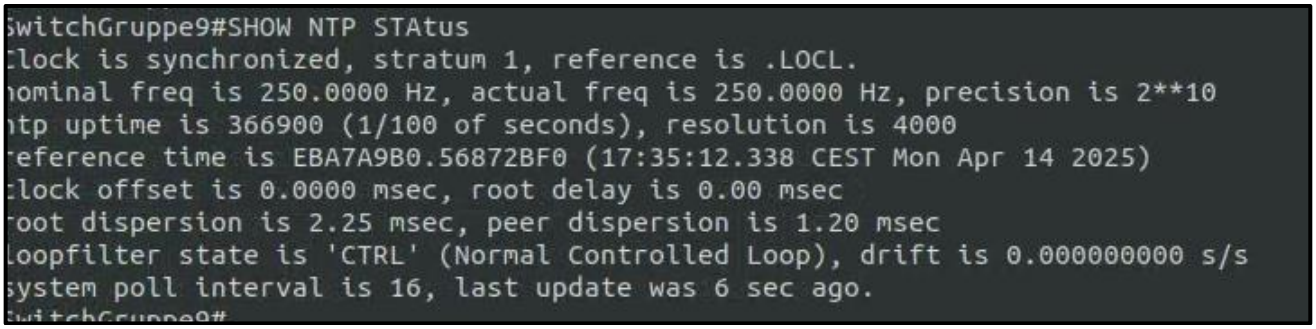
You must set and sync the current time on all core network components and servers. Use NTP (Network Time Protocol, time zone: CET) and the L3 switch as NTP server for this.

On Switch , NTP Master 1 means that Switch will operate as Master for NTP , clock timezone is set to CET 1

```
Conf
ntp server 130.88.202.49 prefer
ntp master 1
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
ex
clock set 16:37:00 14 Apr 2025
```

Kevin Lopci 2410410042

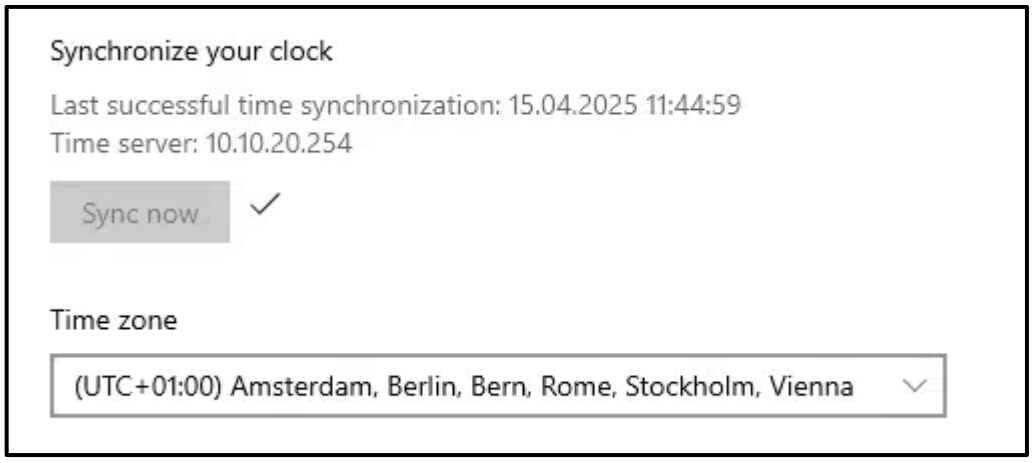
With show ntp status we can see that the stratum is 1,this is like the priority for NTP to be set as Master,clock is unsynchronized, because it needs to be connected with an external NTP Server but that was not asked in this LAB,and the time is accurate.



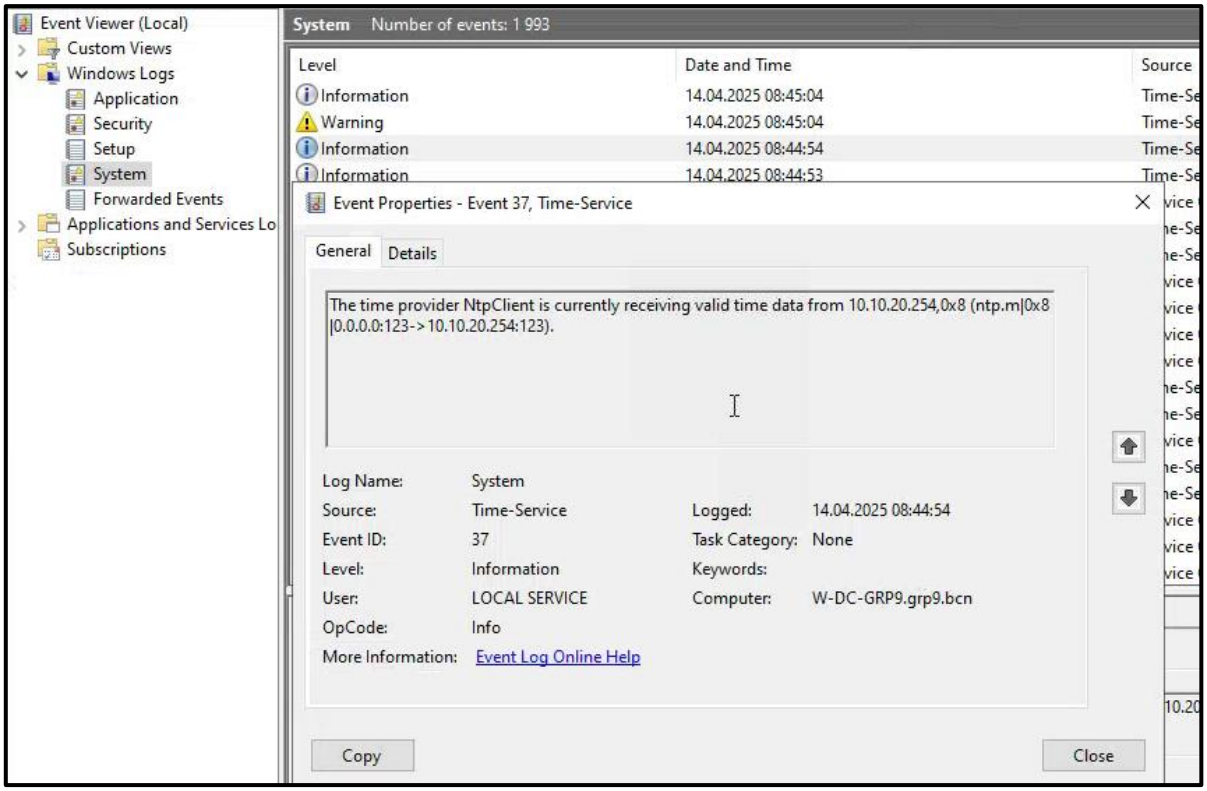
Now on the DC, the Switch needs to be configured as NTP Master on the DC.

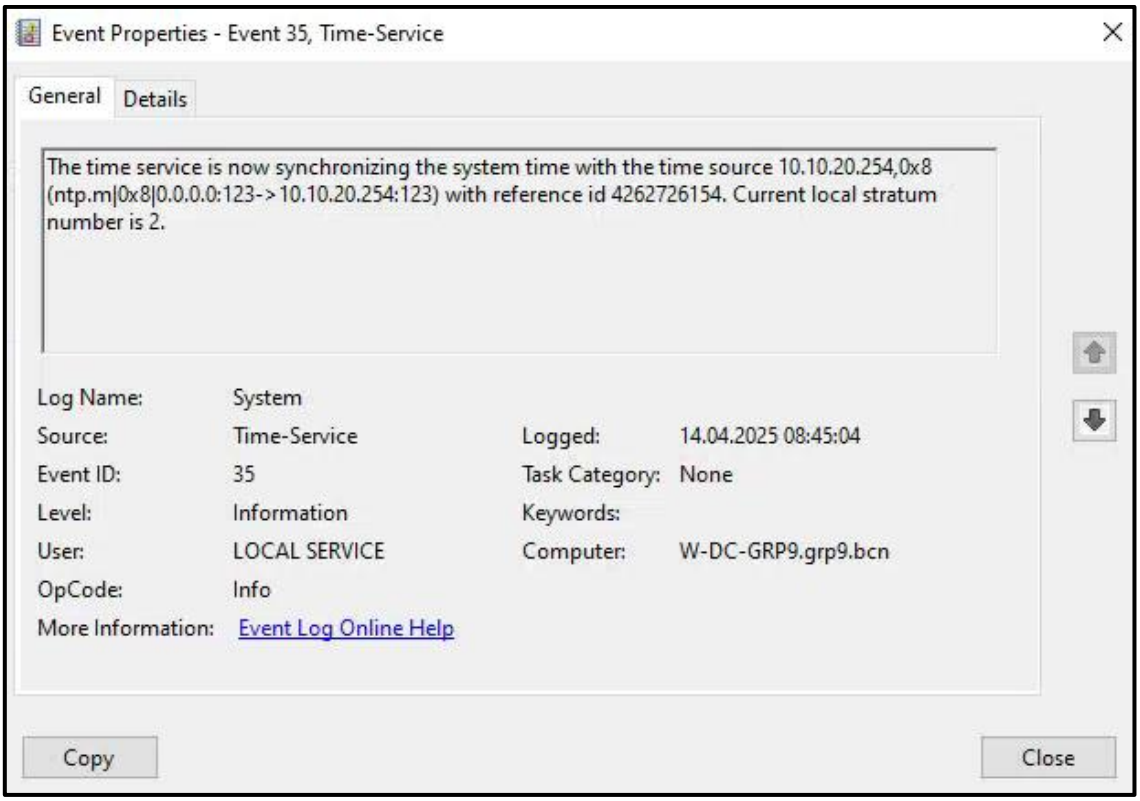
```
C:\Users\Administrator>w32tm /config /manualpeerlist:"10.10.20.254",0x8
/syncfromflags:MANUAL
The command completed successfully.

C:\Users\Administrator>net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.


C:\Users\Administrator>net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.


C:\Users\Administrator>w32tm /resync
Sending resync command to local computer
The command completed successfully.
```

Also set the timezone on DC



As said on the documentation on E Campus we should get following event IDs. The images show that the DC was learning NTP Information from the L3Switch and now it is a reliable source of time.





Windows Client will also be automatically synced when joined into a Domain just have to change the time zone to UTC+1

DMZ NTP

```
sudo nano /etc/systemd/timesyncd.conf
```

```
#
#  systemd is free software; you can redistribute it and/or modify it under the
#  terms of the GNU Lesser General Public License as published by the Free
#  Software Foundation; either version 2.1 of the License, or (at your option)
#  any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file, or by creating "drop-ins" in
# the timesyncd.conf.d/ subdirectory. The latter is generally recommended.
# Defaults can be restored by simply deleting this file and all drop-ins.
#
# See timesyncd.conf(5) for details.

[Time]
NTP=10.10.80.254
#FallbackNTP=ntp.ubuntu.com
#RootDistanceMaxSec=5
#PollIntervalMinSec=32
#PollIntervalMaxSec=2048
~
~
~
~
```

```
Timedatectl set-timezone Europe/Vienna
Systemctl restart system-timesyncd
```

Kevin Lopci 2410410042

```
GMT
root@studend-server:/home/student# timedatectl set-timezone Europe/Vienna
root@studend-server:/home/student# systemctl restart systemd-timesyncd
root@studend-server:/home/student# timedatectl status
               Local time: Tue 2025-04-15 17:56:46 CEST
           Universal time: Tue 2025-04-15 15:56:46 UTC
                 RTC time: Tue 2025-04-15 15:57:33
                Time zone: Europe/Vienna (CEST, +0200)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
root@studend-server:/home/student# _
```

WLS

```
(Cisco Controller) config>time ntp server 10.10.20.254
(Cisco Controller) config>time timezone location 14
(Cisco Controller) >show time

Time..................................... Wed Apr 16 12:59:18 2025

Timezone delta..................................... 0:0
Timezone location.............................. (GMT +1:00) Amsterdam, Berlin, Rome,
Vienna

NTP Servers
    NTP Version.................................     3
    NTP Polling Interval........................     600

     Index     NTP Key Index                  NTP Server                Status
NTP Msg Auth Status
    -------  ------------------------------------------------------------------------
       1              0                                  10.10.41.254     In Sync
AUTH DISABLED
```

```
(Cisco Controller) >show time

Time..................................... Wed Apr 16 12:59:18 2025

Timezone delta..................................... 0:0
Timezone location.............................. (GMT +1:00) Amsterdam, Berlin, Rome, Vienna

NTP Servers
    NTP Version.................................     3
    NTP Polling Interval........................     600

     Index     NTP Key Index                  NTP Server                Status         NTP Msg Auth Status
    -------  ------------------------------------------------------------------------
       1              0                                  10.10.41.254     In Sync             AUTH DISABLED
```

MAB Coffee Maschine NTP

Open the file to the NTP Configuration ,and give the timeserver as 10.10.50.254 .

```
vim /etc/systemd/timesyncd.conf
```

```
root@student-virtual-machine:/home/student# timedatectl show-timesync --all
LinkNTPServers=
SystemNTPServers=10.10.50.254
FallbackNTPServers=ntp.ubuntu.com
ServerName=10.10.50.254
ServerAddress=10.10.50.254
RootDistanceMaxUSec=5s
PollIntervalMinUSec=32s
PollIntervalMaxUSec=34min 8s
PollIntervalUSec=32s
```

```
systemctl restart systemd-timesyncd.service
```

2.2 Layer 2/3 infrastructure Create a VLAN for each client use case and your infrastructure/backend systems (SSIDs, management, APs, servers, DMZ, clients, etc.)

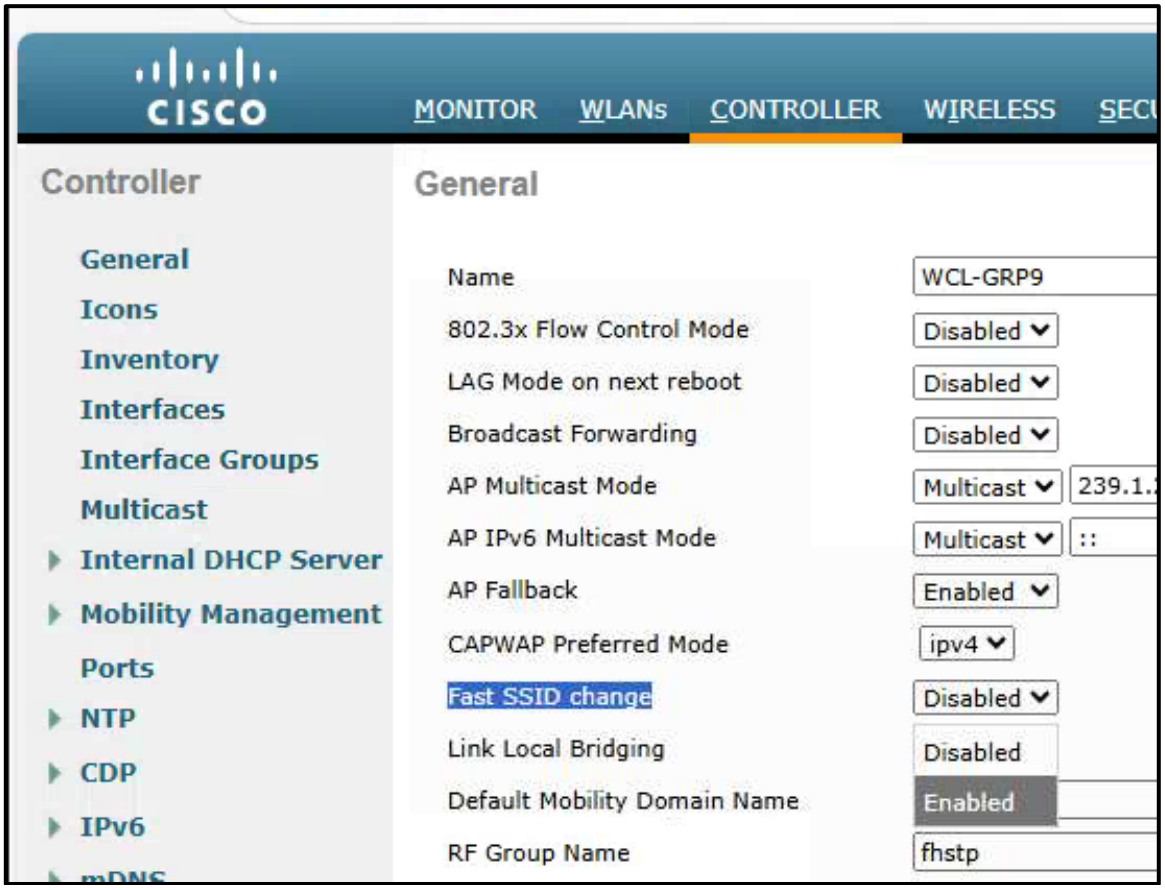
VLAN ID,VLAN Name,IP Subnet,Device/Use Case,Interface,Device IP,PC+Port
10,MGMT-SWITCH,10.10.10.0/24,Switch MGMT,-,10.10.10.1 PC20
20,DC,10.10.20.0/24,Windows Server (DC),Gi1/0/4,10.10.20.1 PC19 Green
30,WindowsClient,10.10.30.0/24,Windows Client,Gi1/0/5,10.10.30.1 PC19 Yellow
40,AP,10.10.40.0/24,Access Point,Gi1/0/2,10.10.40.1
41,WLC,10.10.41.0/24,WLAN Controller,Gi1/0/34,10.10.41.1
50,Coffe-IOT,10.10.50.0/24,Coffee Machine,Gi1/0/7,10.10.50.1 PC18 green
60,STAFF,10.10.60.0/24,WLAN User (Staff),via AP
61,STAFF-ADMIN,10.10.61.0/24,WLAN-Staff-Admin,via AP
70,WLAN-GUEST,10.10.70.0/24,WLAN Guest,via AP
80,DMZ-Webserver,10.10.80.0/24,Web Server,Gi1/0/6,10.10.80.1 PC 18 yellow
(kein VLAN)INTERNET_LOOP,13.13.13.13/24,Simulated Internet,Loopback1,13.13.13.13
(kein VLAN)Coffe_LOOP,7.7.7.7/24,Coffee Order Server,Loopback0,7.7.7.7

2.3 WLAN Infrastructure

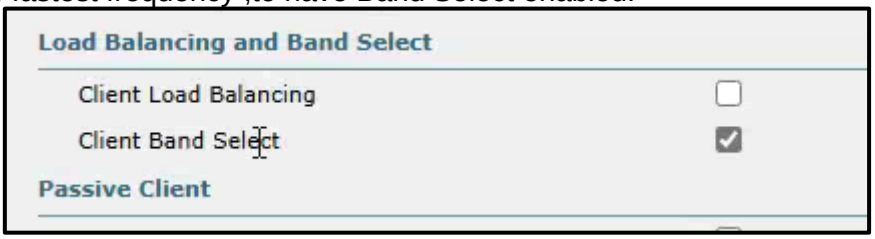
1. All SSIDs must be optimized for the highest possible data throughput in the 5 GHz frequency band.

2. Activate “Fast SSID Change” on the WLC (best practice setting, and not only useful in the lab)

On WLS GUI, click “Controller” and select “Enabled” on Fast SSID change.



Since Staff uses both 2.4 and 5 GHz frequencies, we need to make sure that for it in order to be optimized for the fastest frequency ,to have Band Select enabled.



3. Use a separate VLAN for each use case / each SSID and use dynamic VLAN assignment for this.

(Point 4)

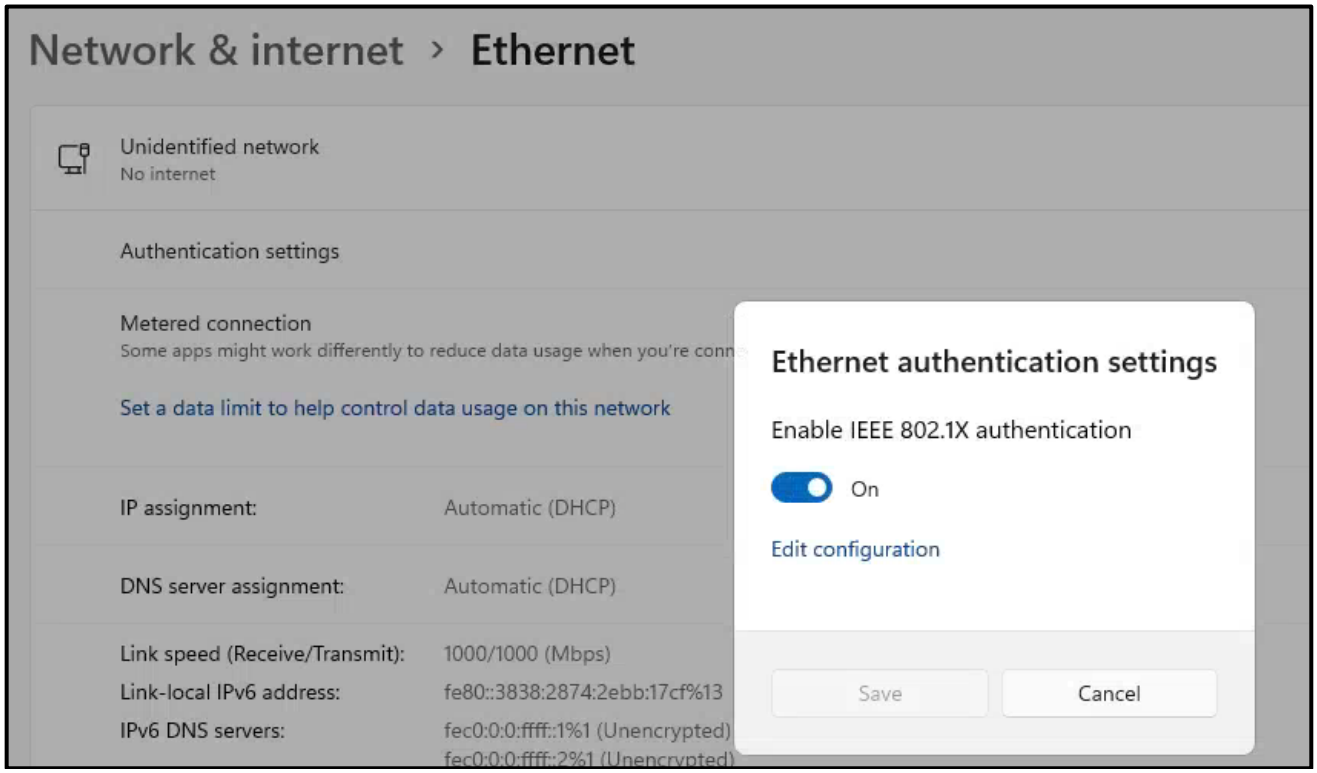
Kevin Lopci 2410410042

3 LAN Authentication

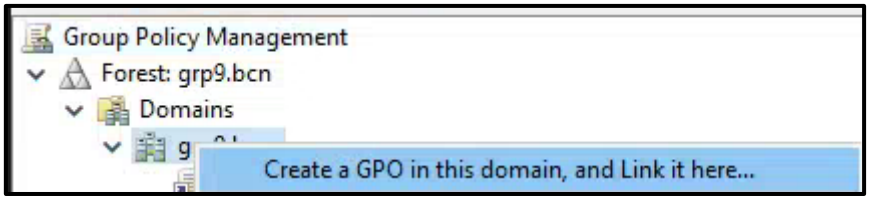
3.1 Via Certificate (802.1X Machine Auth):

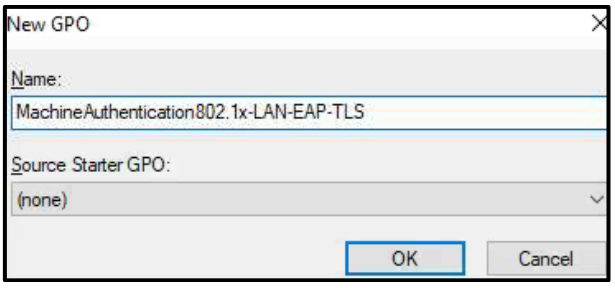
1. Implement LAN EAP-TLS authentication for a Windows 11 client (VM).
a. Configure the EAP-LAN settings for your Domain clients via Windows Group Policy
2. For LAN access to the network, the client must have a computer account in the domain and a valid certificate from the internal PKI.
a. Distribute the certificates for the clients automatically via Windows Group Policy
3. Under no circumstances may the clients attempt to authenticate themselves with RADIUS servers out side the company!

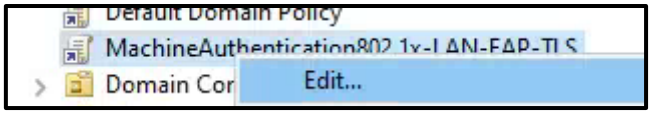
Before we begin make sure to enable 802.1x authentication on the Client ,otherwise you wont be able to authenticate and be removed from the domain.



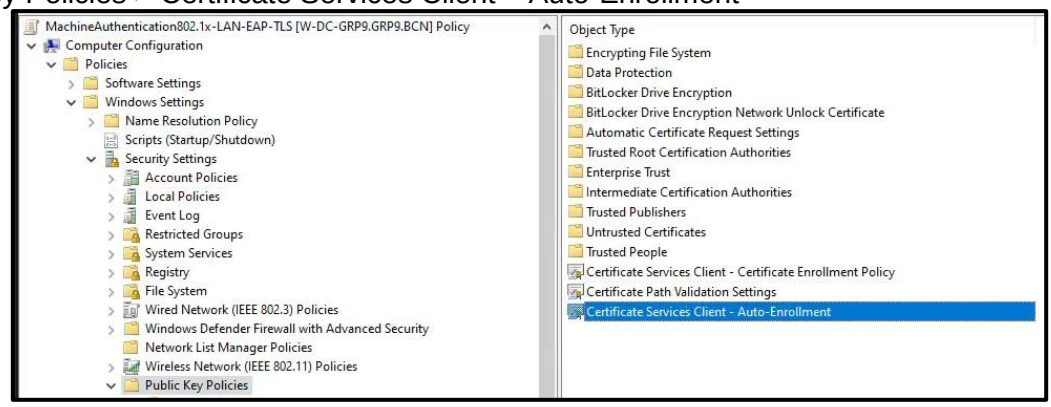
As shown on “CA for 802.1x installieren und konfigurieren mit template.” ,we have already set up the template, we need to now configure the GPO for the auto enrollment of the Certificate. We follow the guide on E-campus.



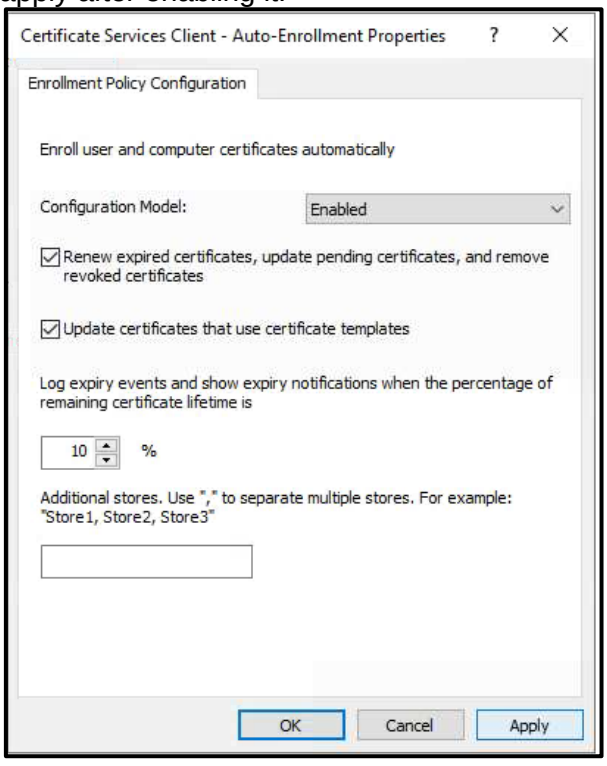




After opening it to edit it we got to:
Computer Configuration > Policies > Windows Settings > Security Settings
From here
Public Key Policies > Certificate Services Client – Auto-Enrollment

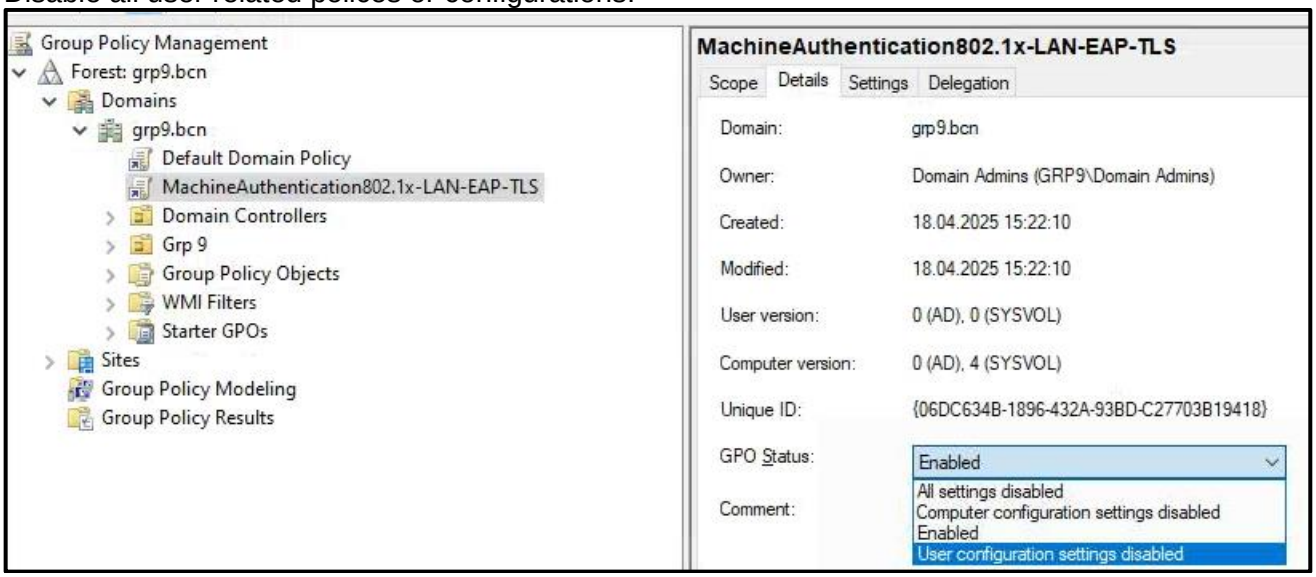


Click the options and click apply after enabling it.

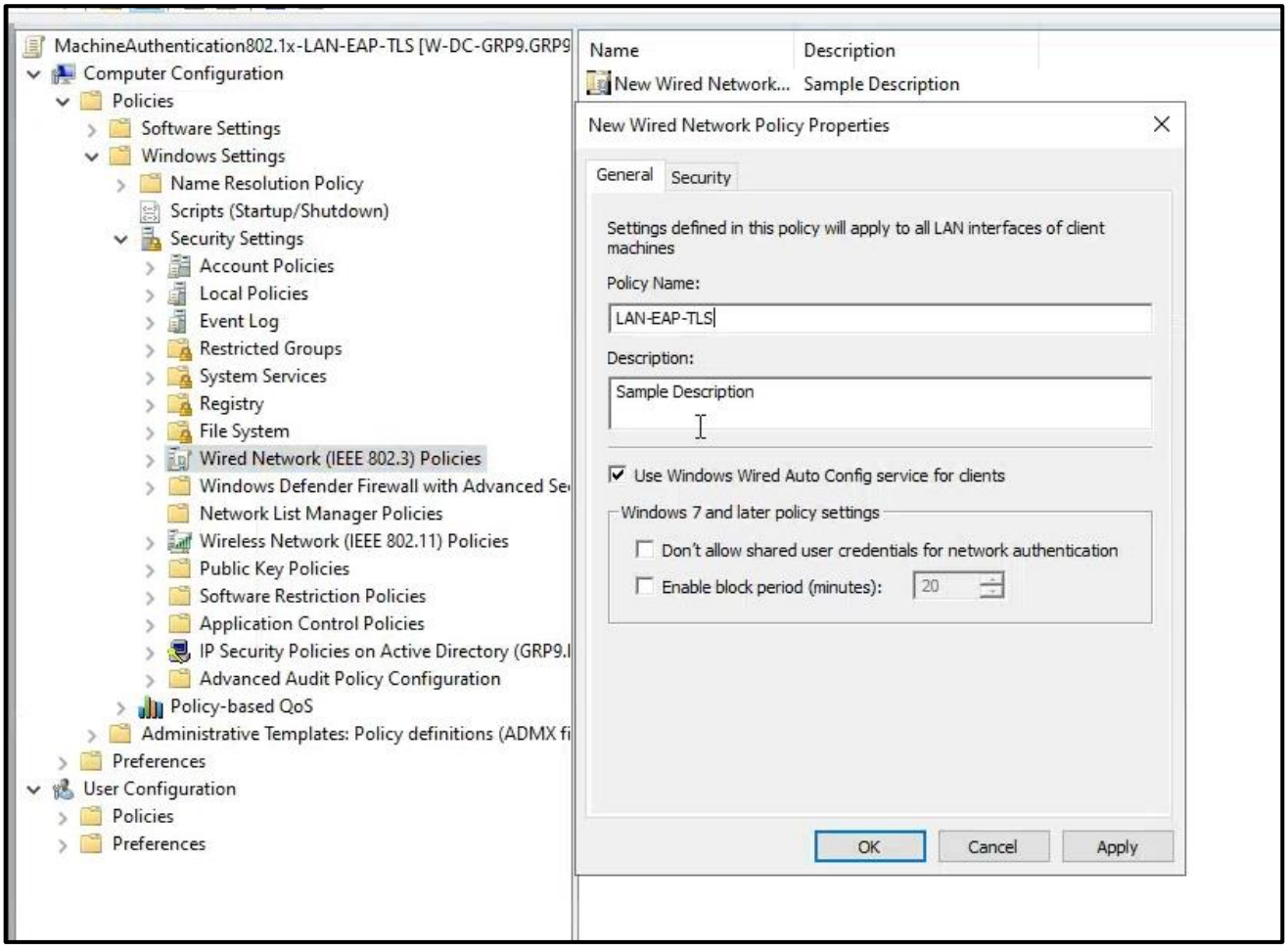


Kevin Lopci 2410410042

Disable all user related polices or configurations.

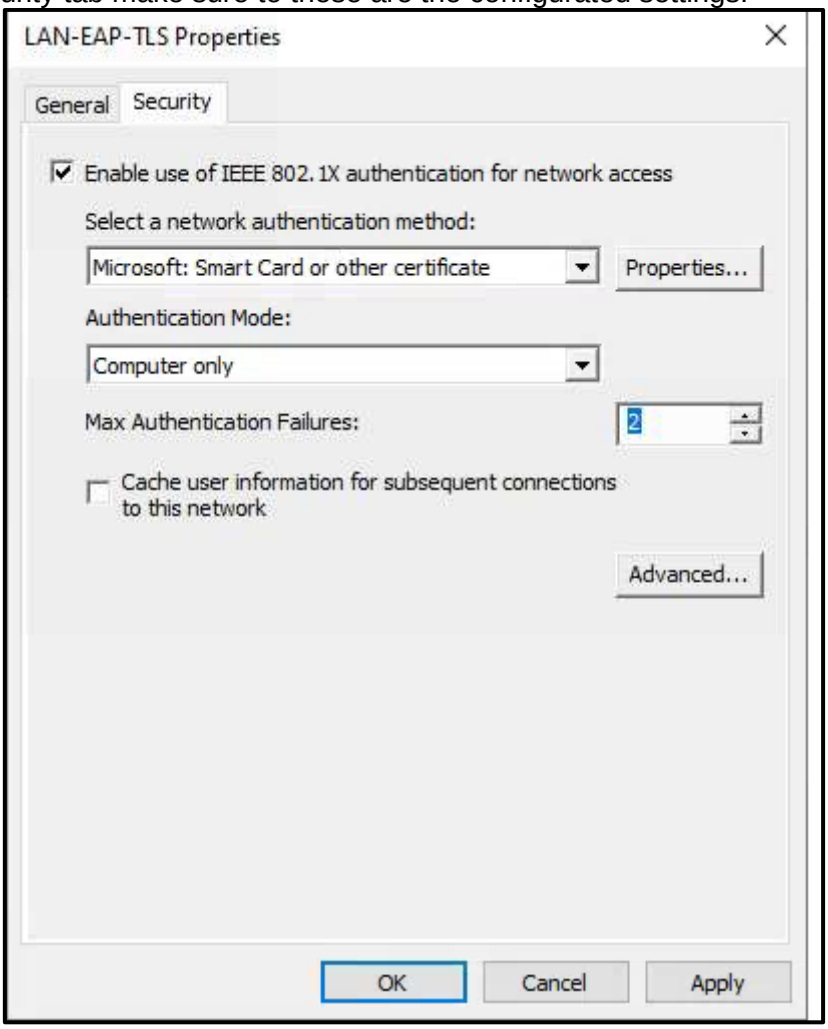


Make sure that also a wired network policy is properly configured otherwise,authentication will also fail. This will make sure that the Computer only uses Computer authentication and not user.
We go to Computer Configuration > Policies > Windows Settings > Security Settings > Wired Network (IEEE 802.3) Policies
And create a new policy



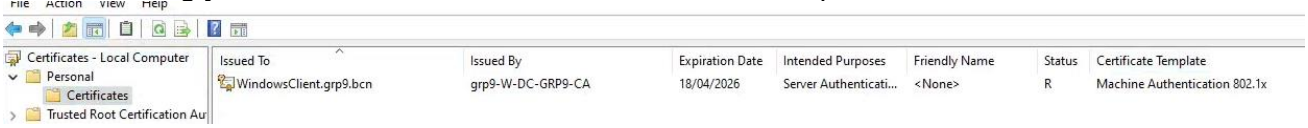
Kevin Lopci 2410410042

Name it,in the security tab make sure to these are the configurated settings.

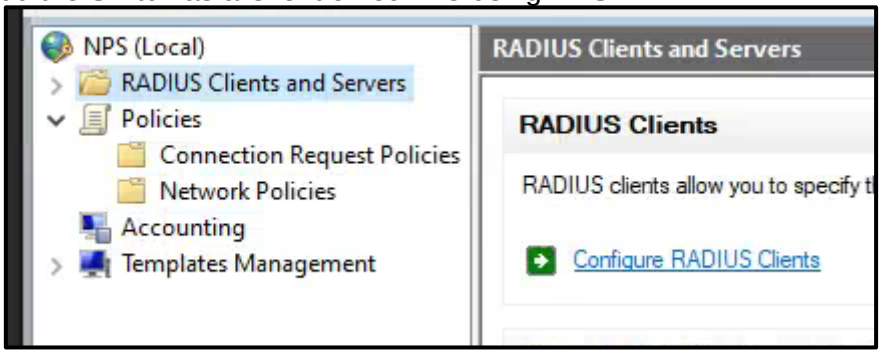


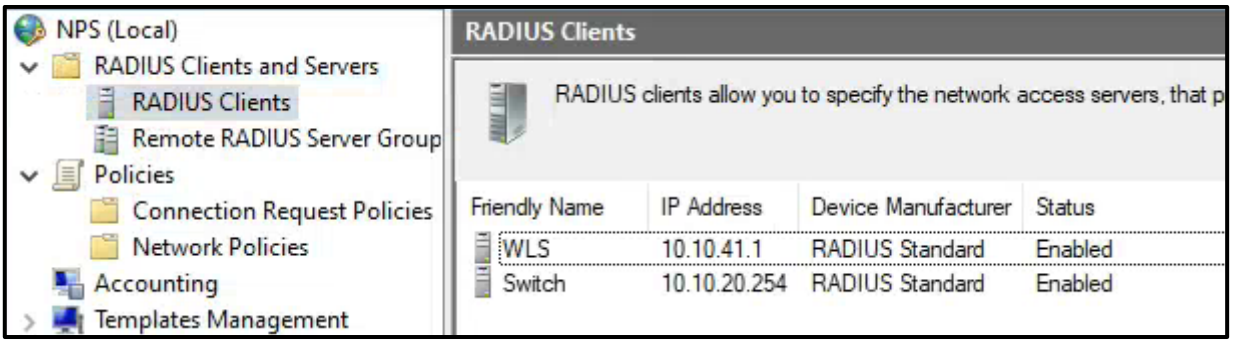
Here we made sure that EAP-TLS is used as an authentication method,and that it is only a machine or computer authentication.

After restarting your windows Machine, it should show here on personal certificates.

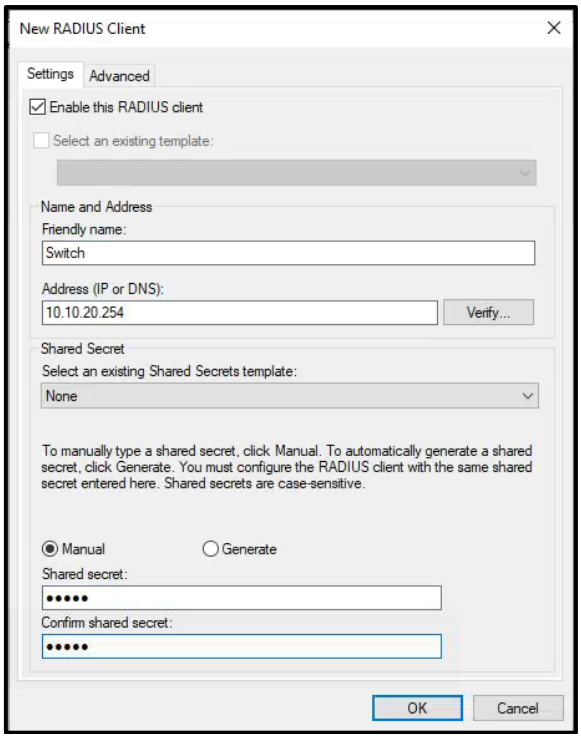


Now we need to configure the Switch as an Authenticator.
To do this, we add the Switch as a Client on our DC using NPS.





Add Switch as a Client, use a reachable ip address,in this case I will use 10.10.20.254, a friendly name and the shared password.

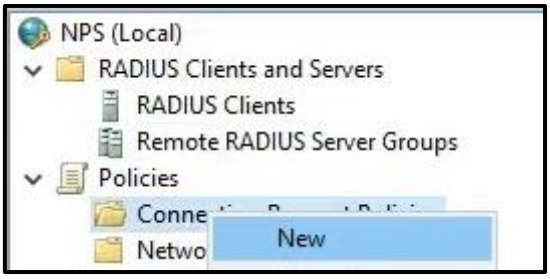


Now we will configure the switch according to the guide in e campus.

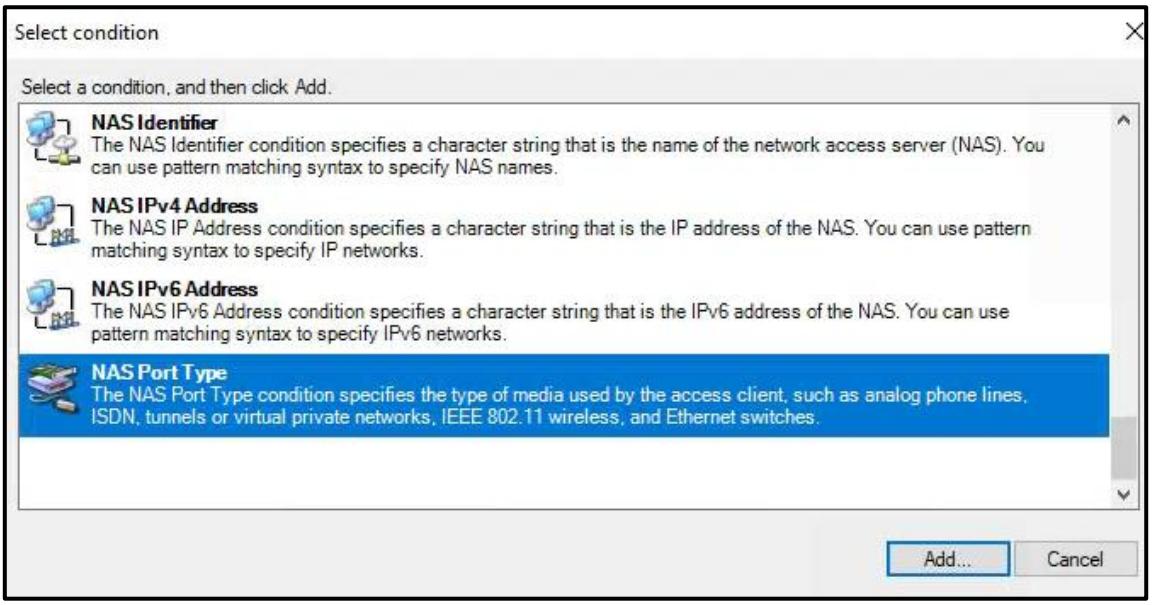
```
SwitchGruppe9(config)#aaa new-model
SwitchGruppe9(config)#radius server NPS
SwitchGruppe9(config-radius-server)#address ipv4 10.10.20.1
SwitchGruppe9(config-radius-server)#key 427Al
SwitchGruppe9(config-radius-server)#exit
SwitchGruppe9(config)#aaa group server radius MY-NPS-SERVERS
SwitchGruppe9(config-sg-radius)#server name NPS
SwitchGruppe9(config-sg-radius)#exit
SwitchGruppe9(config)#aaa authentication dot1x default group MY-NPS-SERVERS
SwitchGruppe9(config)#aaa authorization network default group MY-NPS-SERVERS
SwitchGruppe9(config)#dot1x system-auth-control
SwitchGruppe9(config)#int g1/0/5
SwitchGruppe9(config-if)#dot1x pae authenticator
SwitchGruppe9(config-if)#authentication port-control auto
SwitchGruppe9(config-if)#exit
```

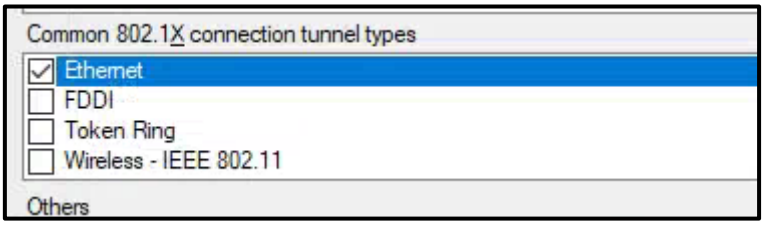
Kevin Lopci 2410410042

Now on the DC we create Connection Request Policy and Network policy.



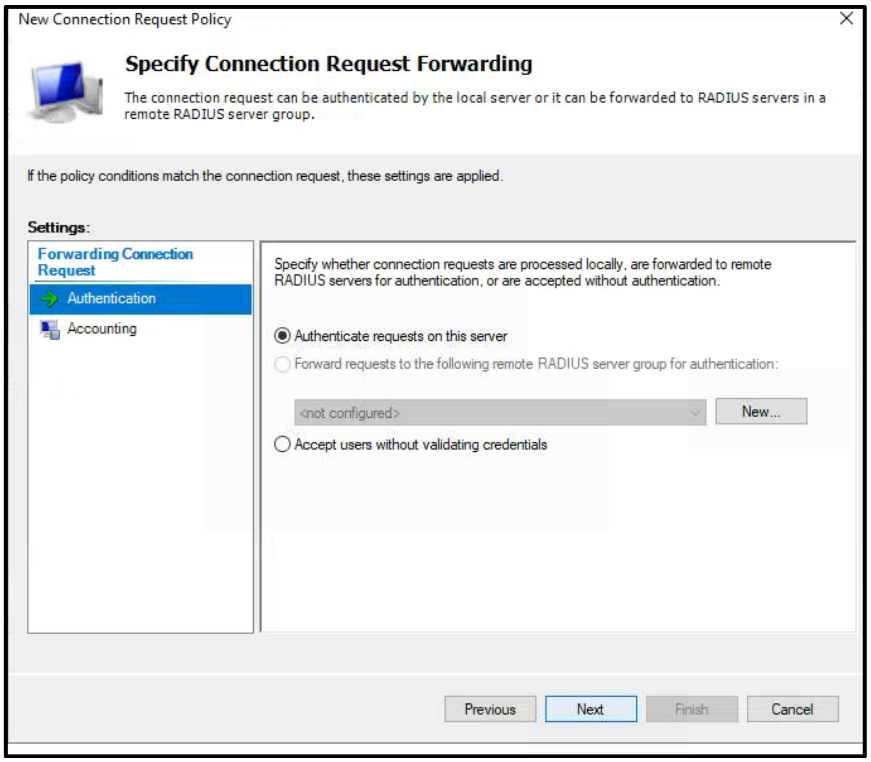
On Conditions, NAS Port type must be set to ethernet,since this is LAN authentication.



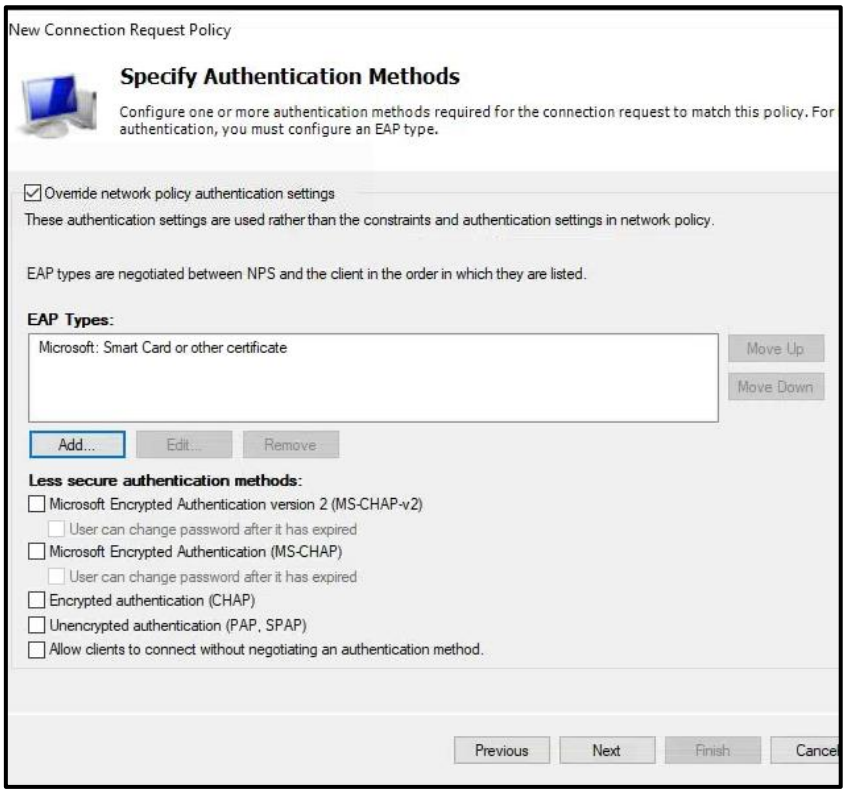


Select it, click ok and then next.

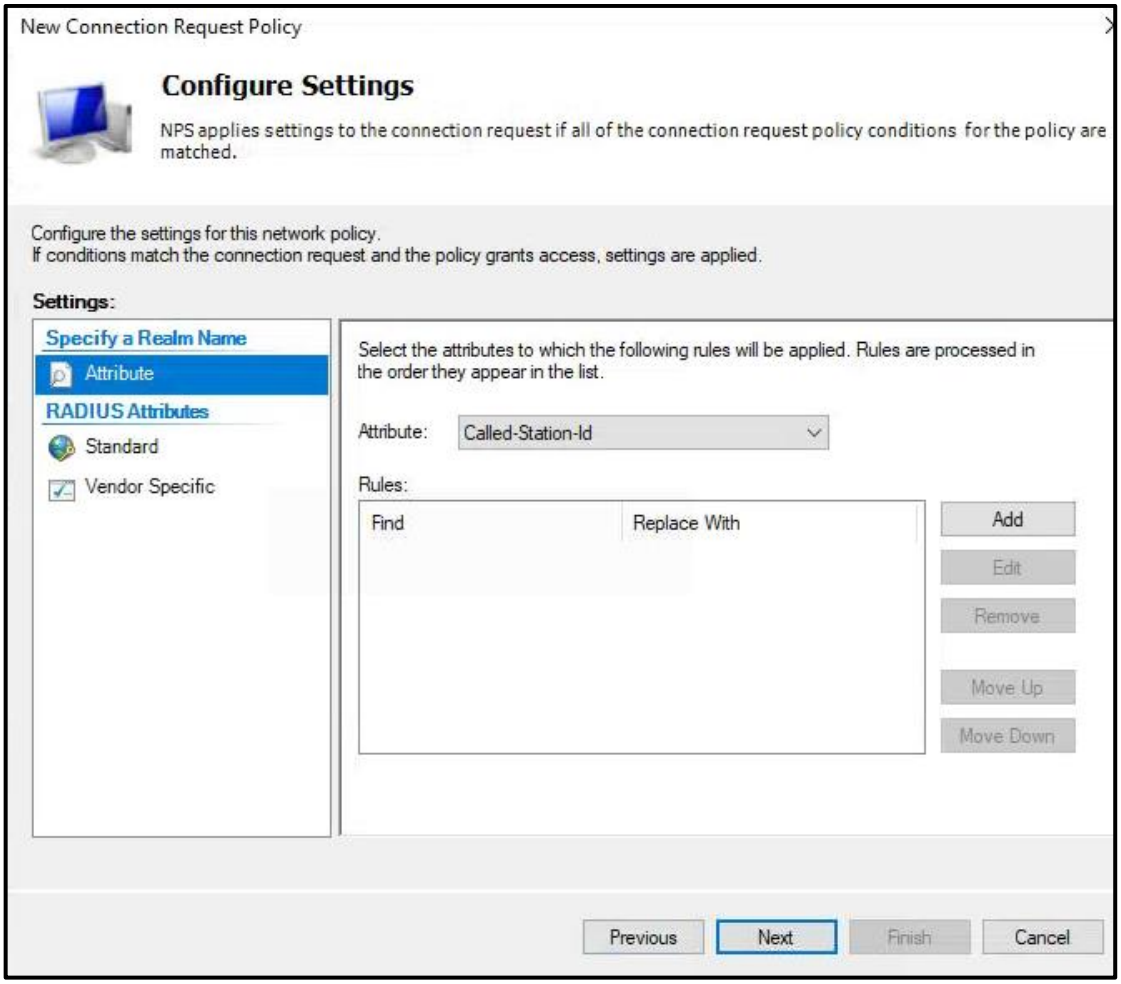
Next again



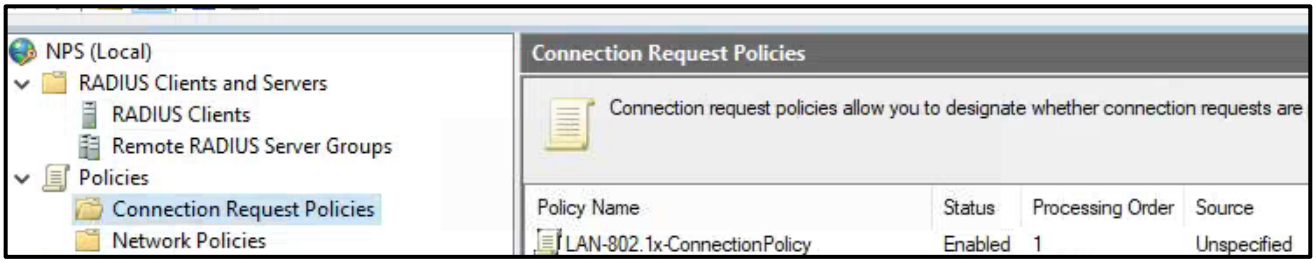
Add Microsoft Smart Card or another certificate to enable EAP-TLS and click next.



Next again.

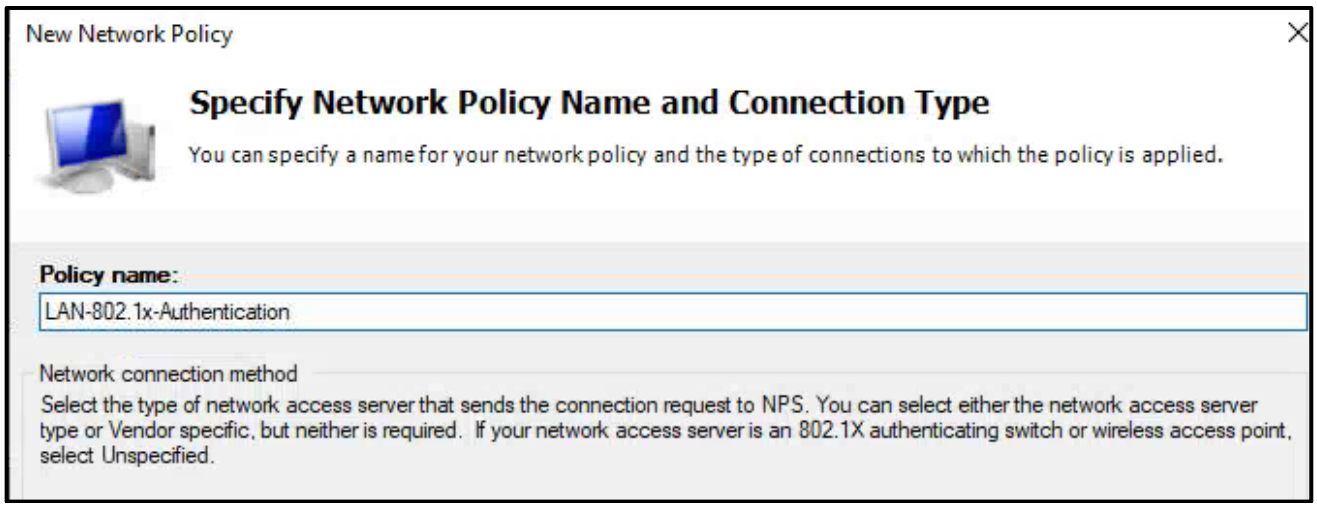


Should show here at the end.

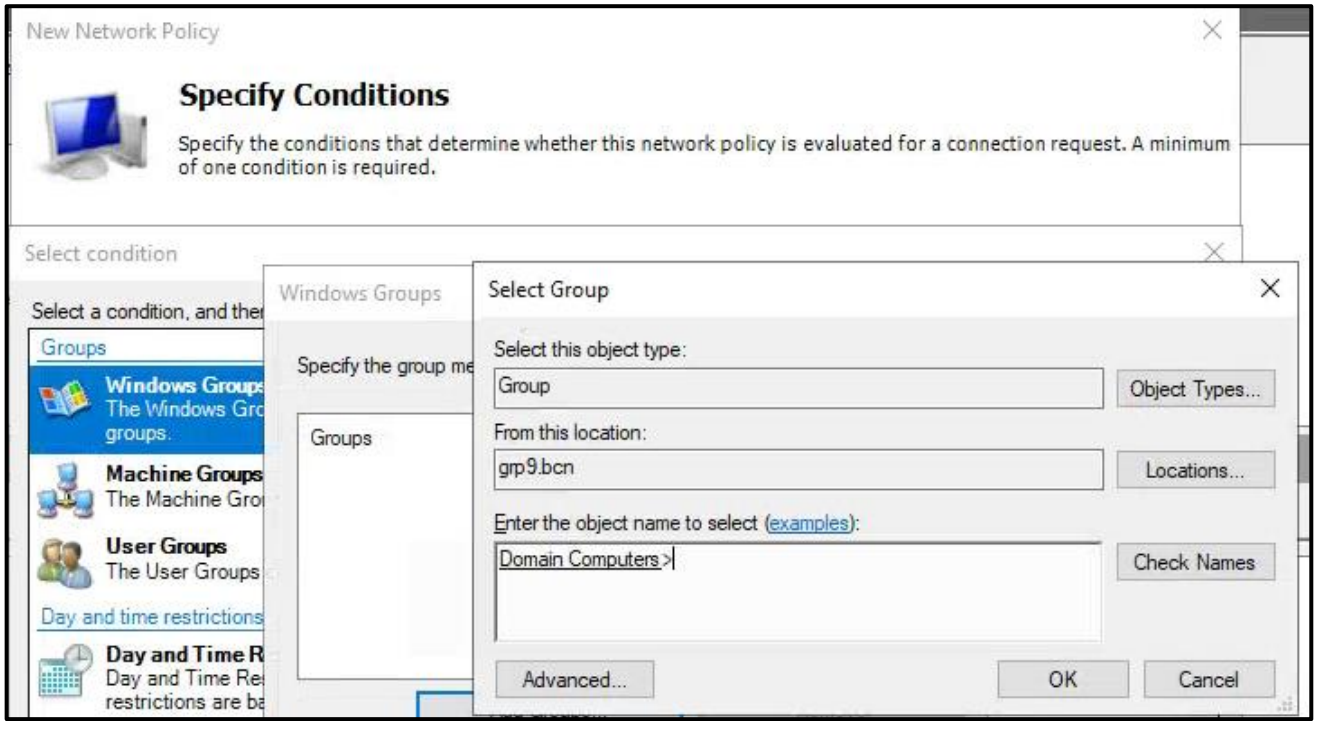


Kevin Lopci 2410410042

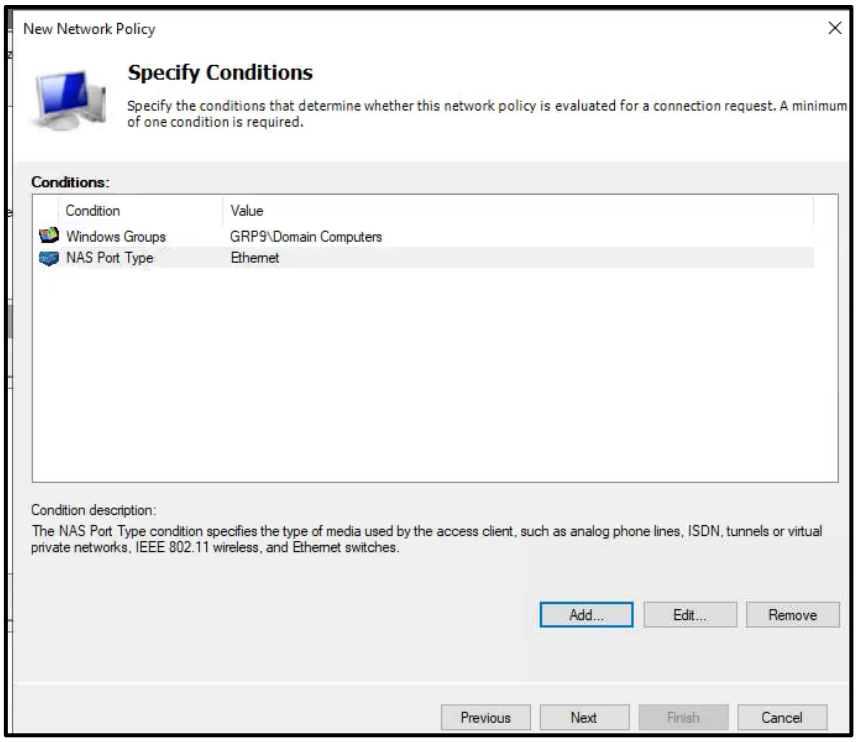
Now we configure the NP. We need to configure both because, Connection Request Policies handle how and where the Authentication needs to be handled, and Network policies decide if a request is allowed or denied.



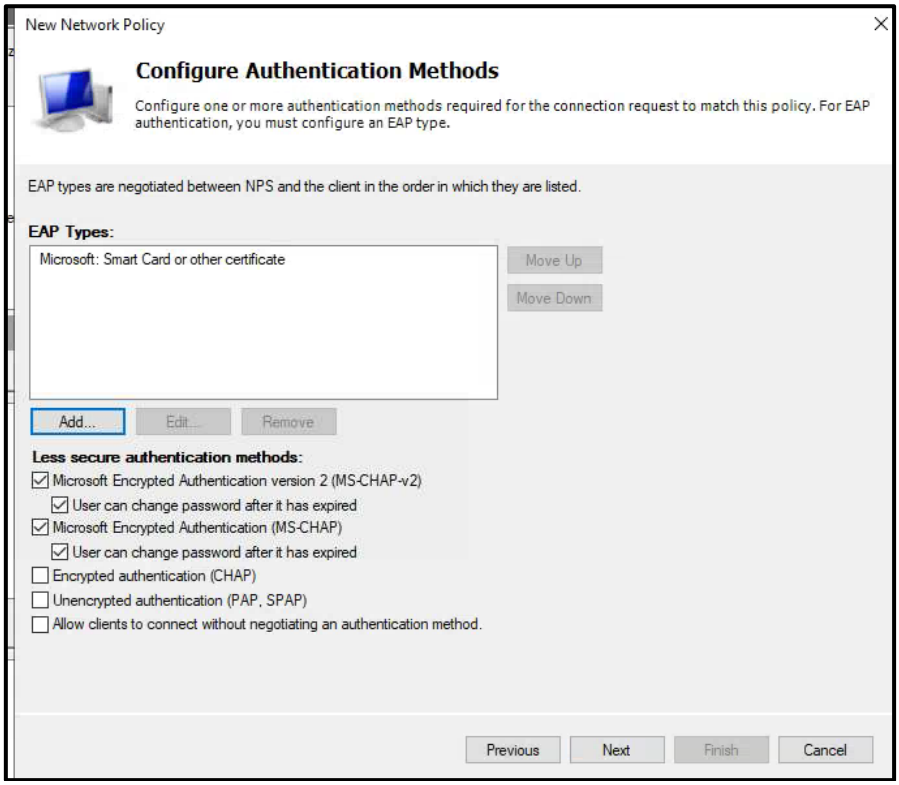
In Conditions Groups and NAS port type need to be defined. Groups is Domain Computers, and NAS port type is ethernet.



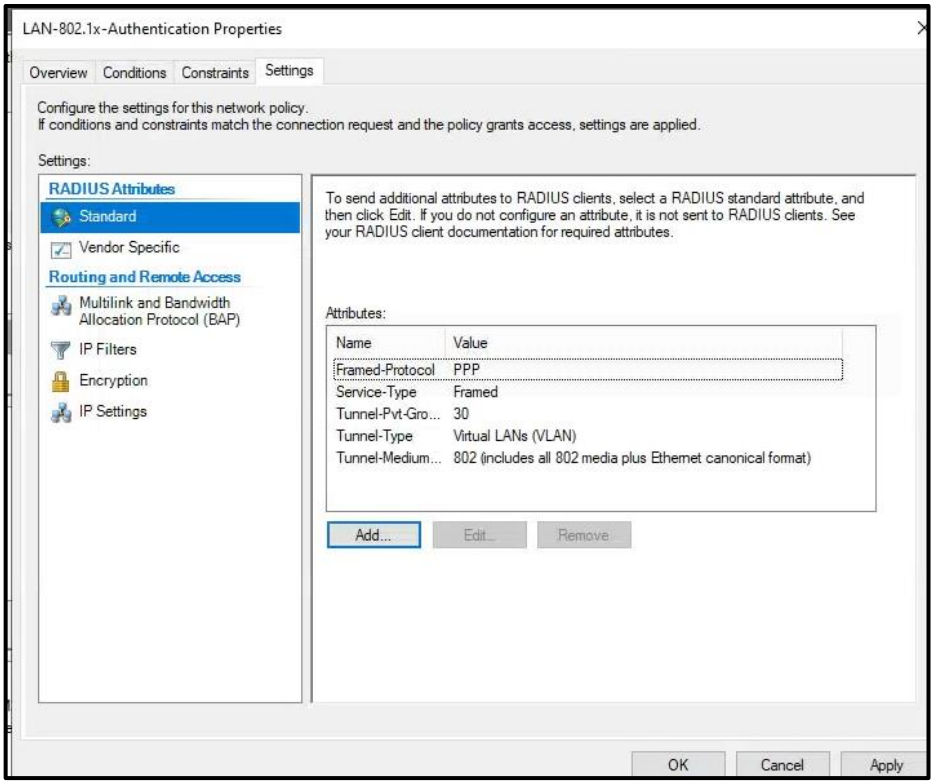
Next



Next until, authentication methods, EAP-TLS needs to be enabled.

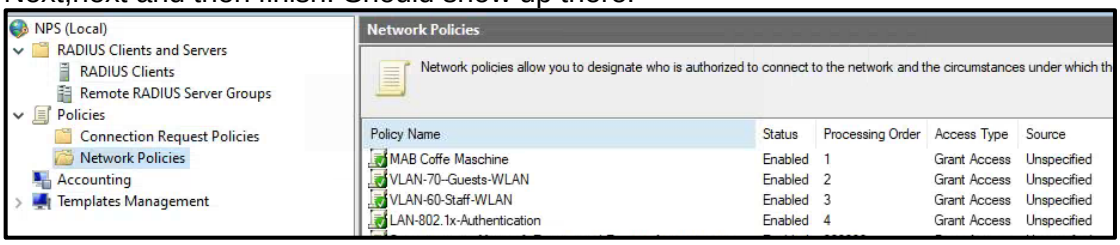


Made sure to specify dynamic VLAN assignment 30,since the client with a valid machine certificate belongs in this VLAN 30.

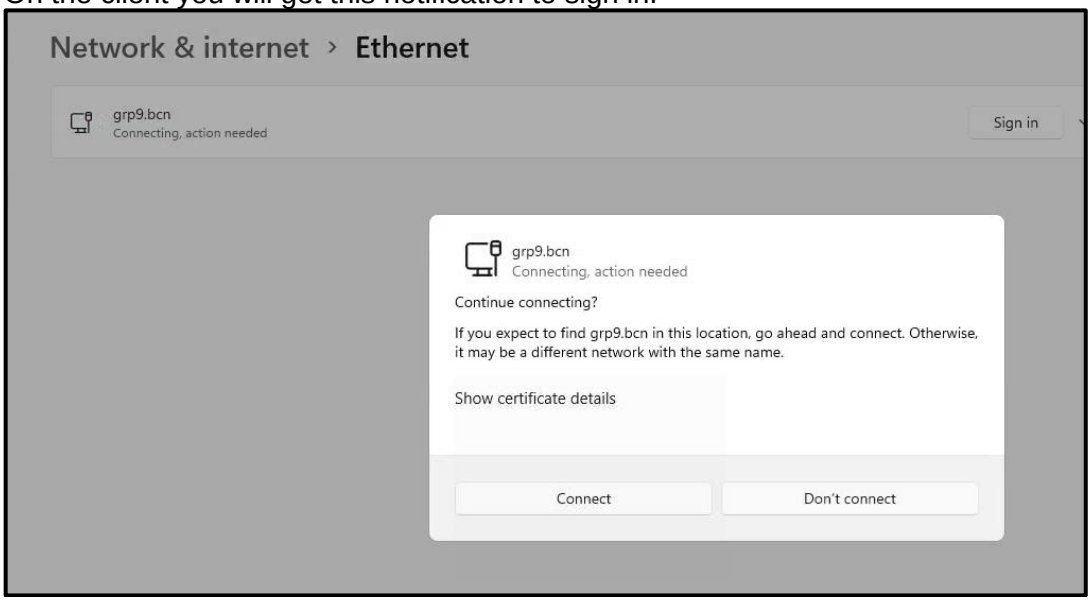


And then finish.

Next,next and then finish. Should show up there.

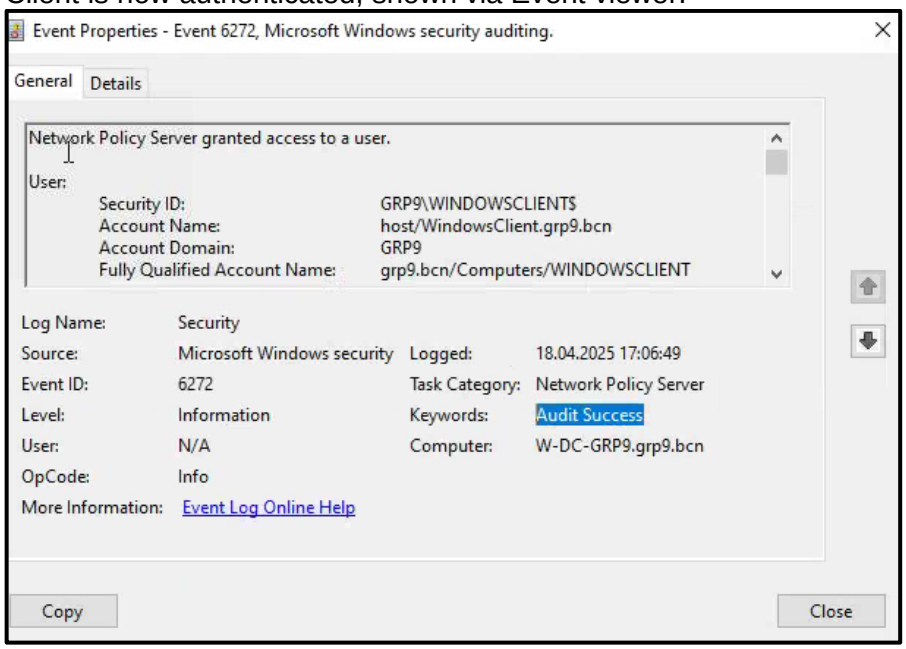


On the client you will get this notification to sign in.



Kevin Lopci 2410410042

Client is now authenticated, shown via Event viewer.




```
SwitchGruppe9#show run interface g1/0/5
Building configuration...

Current configuration : 220 bytes
!
interface GigabitEthernet1/0/5
 description WC
 switchport access vlan 30
```

```
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
 spanning-tree bpduguard enable
end
SwitchGruppe9#
SwitchGruppe9#show authentication session int g1/0/5 details
Apr 18 15:15:42.092: %SYS-5-CONFIG_I: Configured from console by console
            Interface:  GigabitEthernet1/0/5
               IIF-ID:  0x19CB58B2
          MAC Address:  000c.2965.0243
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  host/WindowsClient.grp9.bcn
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0A0A14FE0000000E497134CF
      Acct Session ID:  Unknown
               Handle:  0xa0000004
       Current Policy:  POLICY_Gi1/0/5


Local Policies:
      Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecured

Server Policies:
      Vlan Group:  Vlan: 30

Method status list:
       Method           State
        dot1x           Authc Success

SwitchGruppe9#show mac address-table interface g1/0/5
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  30    000c.2965.0243    STATIC      Gi1/0/5
Total Mac Addresses for this criterion: 1
```

4.Make sure that (by using ACLs):

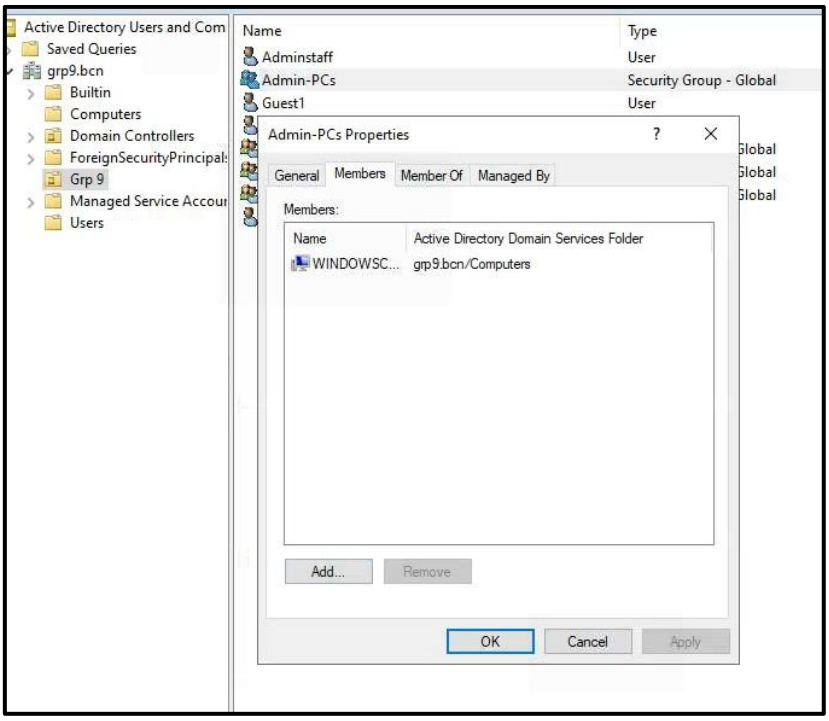
a. Clients with valid certificates have full access to the DMZ and server subnets.
b. Clients with valid certificates have access to “the internet” via HTTP/HTTPS.
c. No AD client has access to the management and AP subnets.

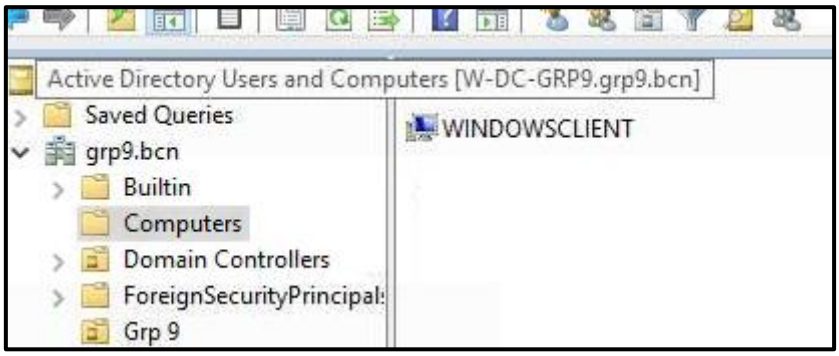
On L3 Switch, made sure to allow server subnets in this case VLAN-20 , DMZ VLAN-80, internet via HTTP / S Blocking access to AP, WLS, and its subnets , while not blocking any DNS, DHCP or RADIUS services.

```
SwitchGruppe9(config)#ip access-list extended VLAN30-POLICY
SwitchGruppe9(config-ext-nacl)#deny ip 10.10.30.0 0.0.0.255 10.10.10.0 0.0.0.255
SwitchGruppe9(config-ext-nacl)#deny ip 10.10.30.0 0.0.0.255 10.10.40.0 0.0.0.255
SwitchGruppe9(config-ext-nacl)#deny ip 10.10.30.0 0.0.0.255 10.10.41.0 0.0.0.255
SwitchGruppe9(config-ext-nacl)#deny ip 10.10.30.0 0.0.0.255 10.10.60.0 0.0.0.255
SwitchGruppe9(config-ext-nacl)#deny ip 10.10.30.0 0.0.0.255 10.10.70.0 0.0.0.255
SwitchGruppe9(config-ext-nacl)#deny ip 10.10.30.0 0.0.0.255 10.10.61.0 0.0.0.255
SwitchGruppe9(config-ext-nacl)#permit udp 10.10.30.0 0.0.0.255 any eq 67
SwitchGruppe9(config-ext-nacl)#permit udp any eq 68 10.10.30.0 0.0.0.255
SwitchGruppe9(config-ext-nacl)#permit udp 10.10.30.0 0.0.0.255 any eq 53
SwitchGruppe9(config-ext-nacl)#permit udp 10.10.30.0 0.0.0.255 host 10.10.20.1 eq 1812
SwitchGruppe9(config-ext-nacl)#permit ip 10.10.30.0 0.0.0.255 10.10.20.0 0.0.0.255
SwitchGruppe9(config-ext-nacl)#permit ip 10.10.30.0 0.0.0.255 10.10.80.0 0.0.0.255
SwitchGruppe9(config-ext-nacl)#permit tcp 10.10.30.0 0.0.0.255 host 13.13.13.13 eq 80
SwitchGruppe9(config-ext-nacl)#permit tcp 10.10.30.0 0.0.0.255 host 13.13.13.13 eq 443
SwitchGruppe9(config-ext-nacl)#deny ip any any
SwitchGruppe9(config-ext-nacl)#interface Vlan30
SwitchGruppe9(config-if)# ip access-group VLAN30-POLICY in
SwitchGruppe9(config-if)#
```

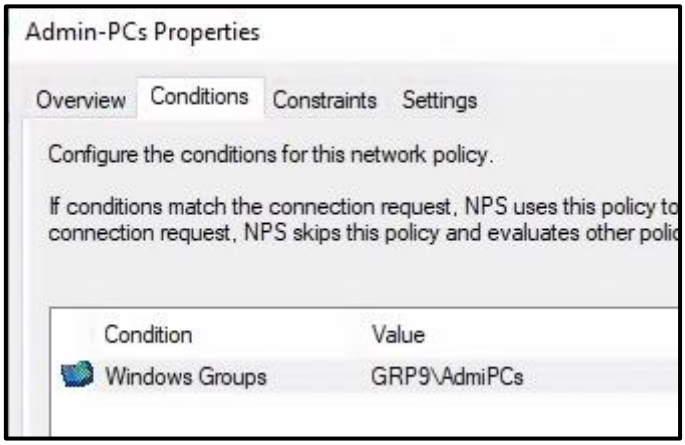
5.Extend your configuration so that - in contrast to common AD clients - computers in the AD group “Admin PCs” automatically join a VLAN from which full access to the network is permitted.

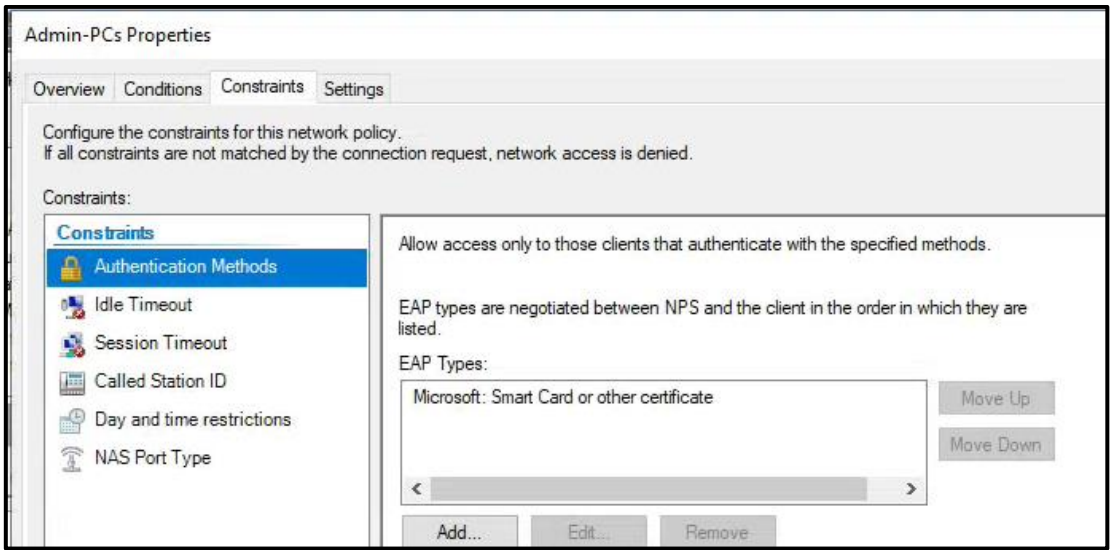
Created a group where the computer will temporarily be part of it just to test it.

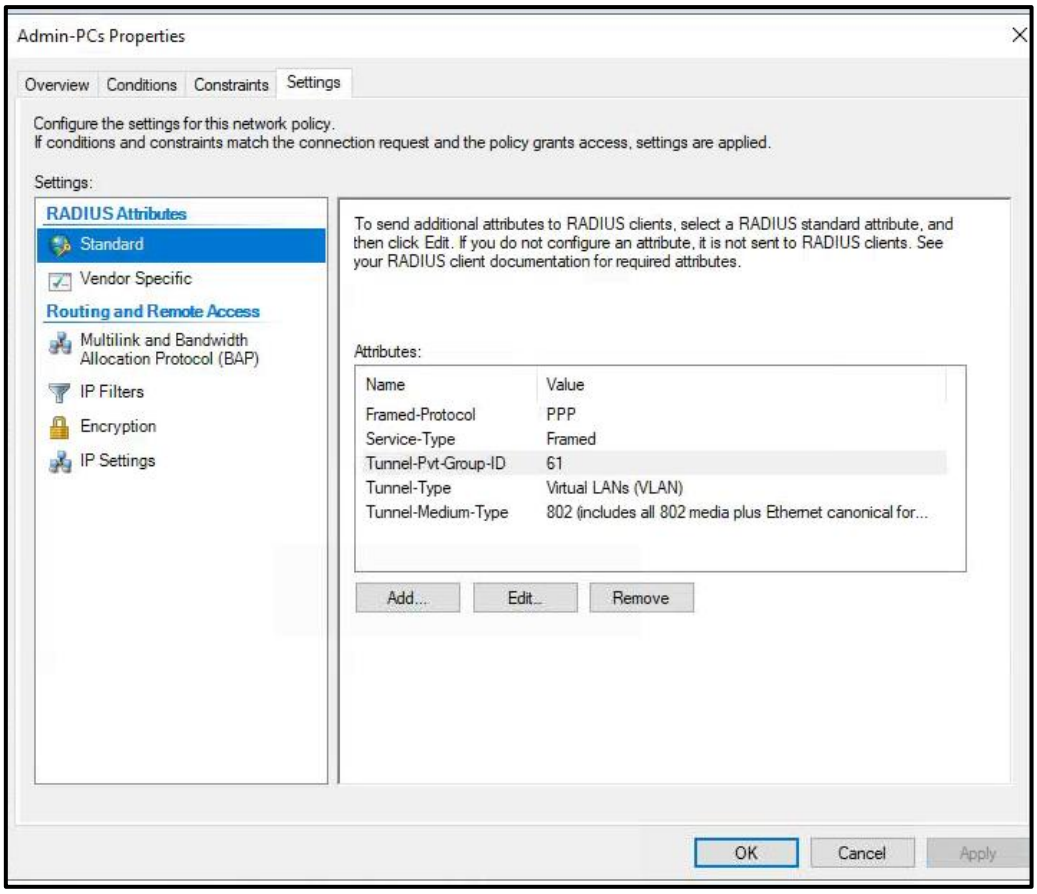


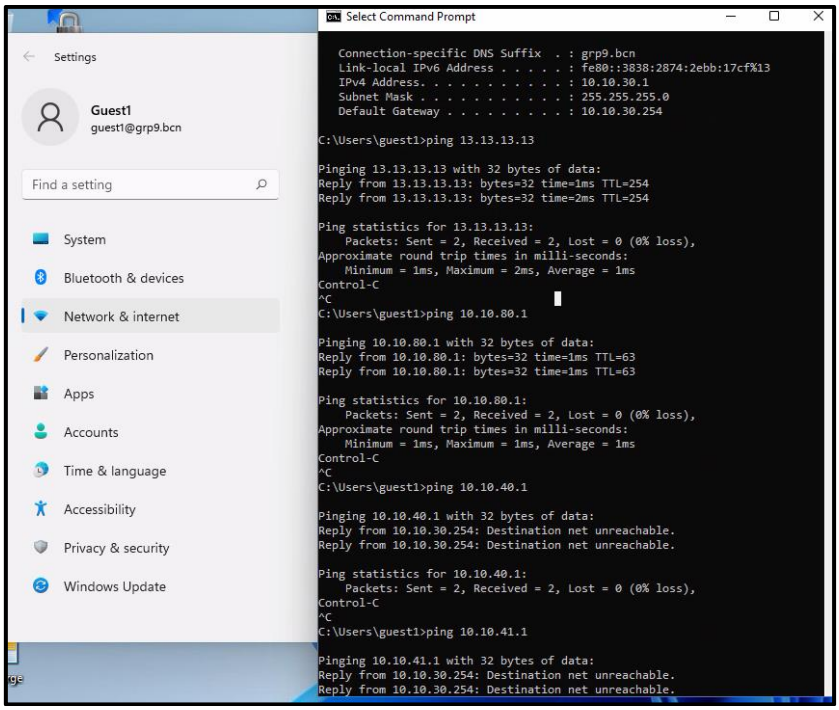


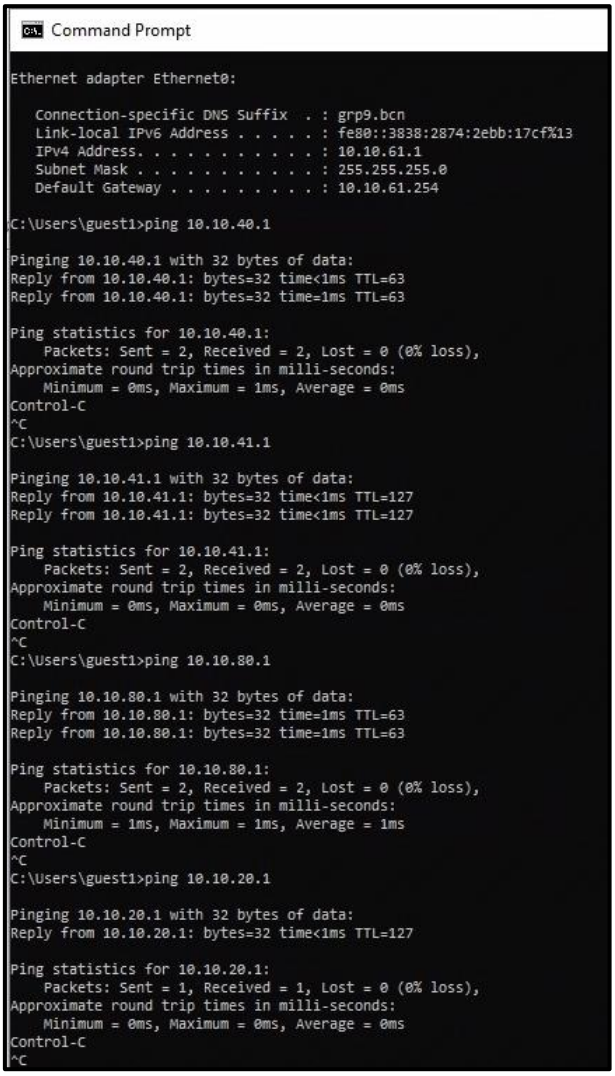
Created this policy to join VLAN 61 (Staff-Admins) automatically, since it is not restricted to anything. These are the settings.




Admin-PCs Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Smart Card or other certificate
Move Up
Move Down
Add...
Edit...
Remove

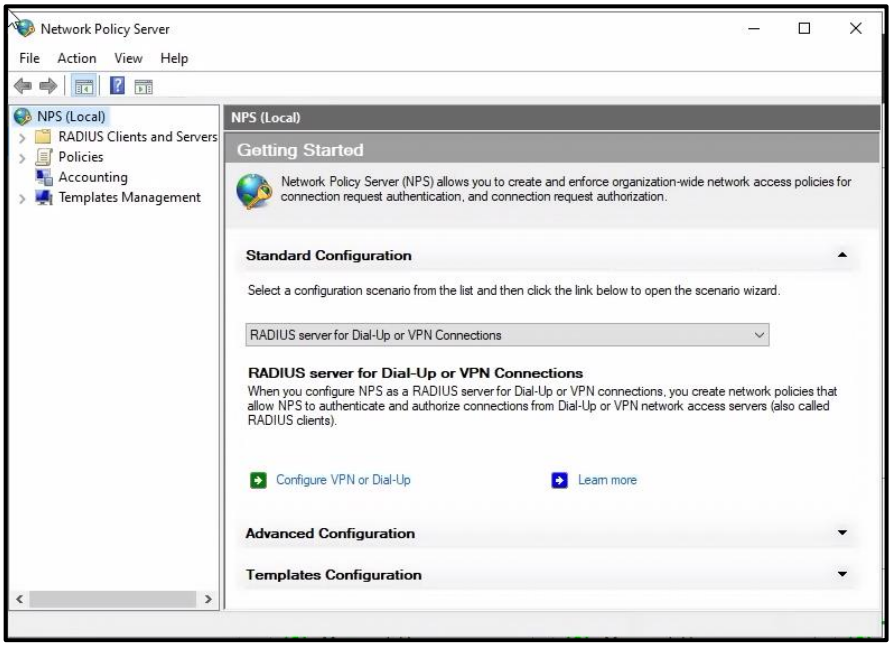

Admin-PCs Properties
Overview
Conditions
Constraints
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
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
Framed-Protocol
PPP
Service-Type
Framed
Tunnel-Pvt-Group-ID
61
Tunnel-Type
Virtual LANs (VLAN)
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Add...
Edit...
Remove
OK
Cancel
Apply


Settings
Guest1
guest1@grp9.bcn
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Accessibility
Privacy & security
Windows Update
Select Command Prompt
Connection-specific DNS Suffix . : grp9.bcn
Link-local IPv6 Address . . . . . : fe80::3838:2874:2ebb:17cf%13
IPv4 Address. . . . . : 10.10.30.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.30.254
C:\Users\guest1>ping 13.13.13.13
Pinging 13.13.13.13 with 32 bytes of data:
Reply from 13.13.13.13: bytes=32 time=1ms TTL=254
Reply from 13.13.13.13: bytes=32 time=2ms TTL=254
Ping statistics for 13.13.13.13:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
Control-C
^C
C:\Users\guest1>ping 10.10.80.1
Pinging 10.10.80.1 with 32 bytes of data:
Reply from 10.10.80.1: bytes=32 time=1ms TTL=63
Reply from 10.10.80.1: bytes=32 time=1ms TTL=63
Ping statistics for 10.10.80.1:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
^C
C:\Users\guest1>ping 10.10.40.1
Pinging 10.10.40.1 with 32 bytes of data:
Reply from 10.10.30.254: Destination net unreachable.
Reply from 10.10.30.254: Destination net unreachable.
Ping statistics for 10.10.40.1:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Control-C
^C
C:\Users\guest1>ping 10.10.41.1
Pinging 10.10.41.1 with 32 bytes of data:
Reply from 10.10.30.254: Destination net unreachable.
Reply from 10.10.30.254: Destination net unreachable.

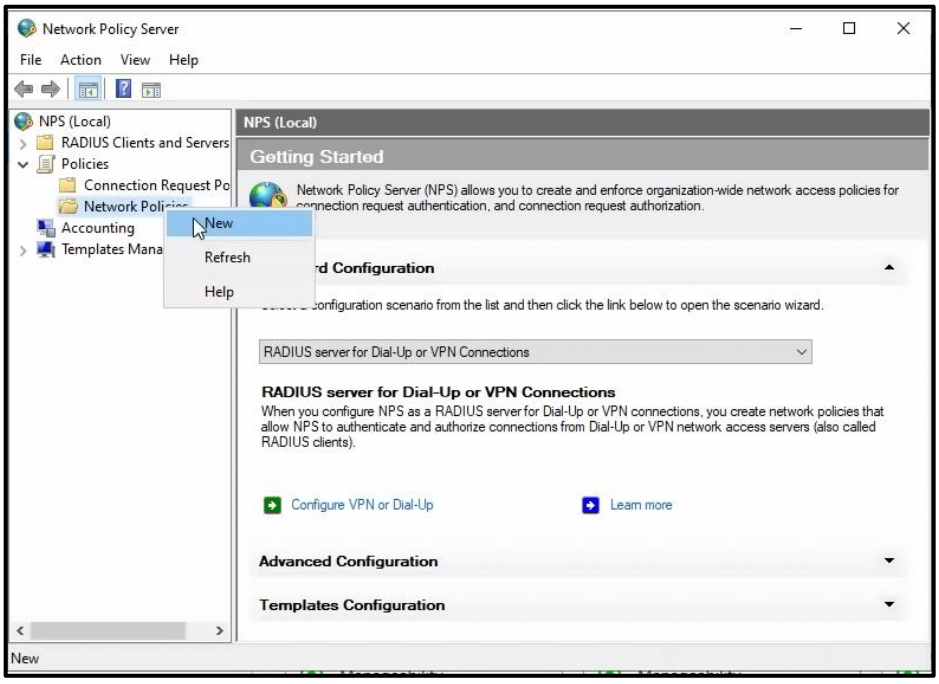

Command Prompt
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : grp9.bcn
Link-local IPv6 Address . . . . . : fe80::3838:2874:2ebb:17cf%13
IPv4 Address. . . . . : 10.10.61.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.61.254
C:\Users\guest1>ping 10.10.40.1
Pinging 10.10.40.1 with 32 bytes of data:
Reply from 10.10.40.1: bytes=32 time<1ms TTL=63
Reply from 10.10.40.1: bytes=32 time=1ms TTL=63
Ping statistics for 10.10.40.1:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\guest1>ping 10.10.41.1
Pinging 10.10.41.1 with 32 bytes of data:
Reply from 10.10.41.1: bytes=32 time<1ms TTL=127
Reply from 10.10.41.1: bytes=32 time<1ms TTL=127
Ping statistics for 10.10.41.1:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\guest1>ping 10.10.80.1
Pinging 10.10.80.1 with 32 bytes of data:
Reply from 10.10.80.1: bytes=32 time=1ms TTL=63
Reply from 10.10.80.1: bytes=32 time=1ms TTL=63
Ping statistics for 10.10.80.1:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
^C
C:\Users\guest1>ping 10.10.20.1
Pinging 10.10.20.1 with 32 bytes of data:
Reply from 10.10.20.1: bytes=32 time<1ms TTL=127
Ping statistics for 10.10.20.1:
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C

3.2 Via MAC Address (MAB)

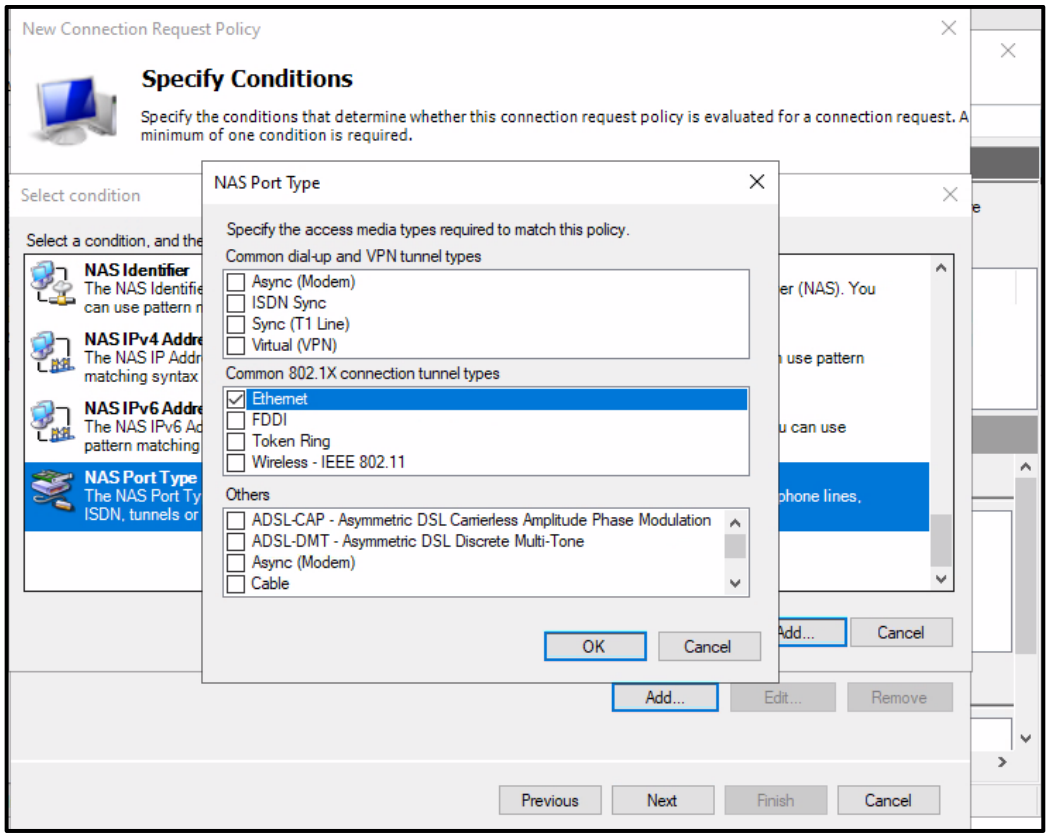
Connected Coffee Machine VM to the switch on port Gi1/0/7
I configured the switch to support 802.1X with fallback to MAB by enabling AAA defining a RADIUS server group linked to the NPS server applying dot1x and MAB settings on interface Gi1/0/7 also VLAN 50 and ensuring the port dynamically authenticates the coffee machine based on its MAC address
On the Windows Server NPS
Created RADIUS Client for the switch 10.10.20.254 with shared secret 427Alb



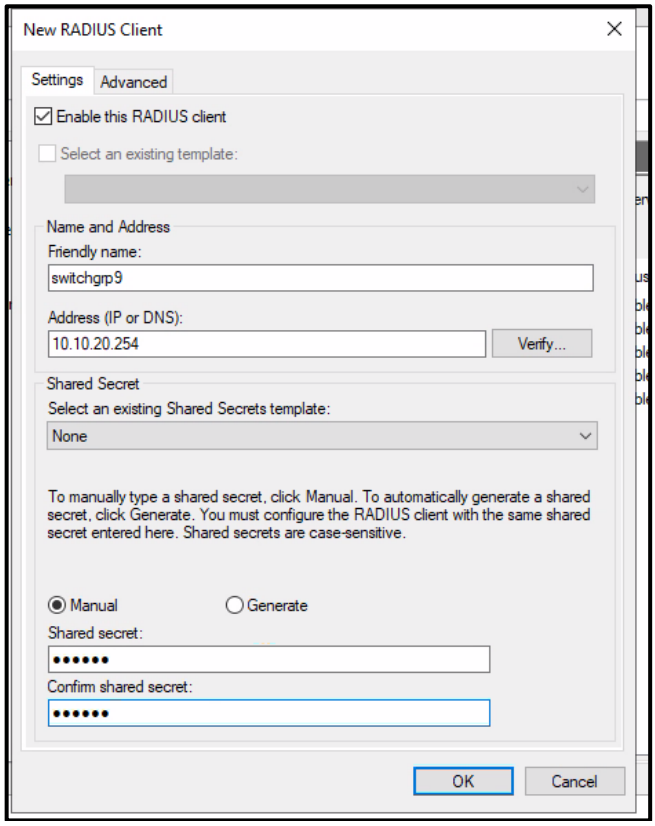
Created a Network Policy named MAB Coffee Maschine



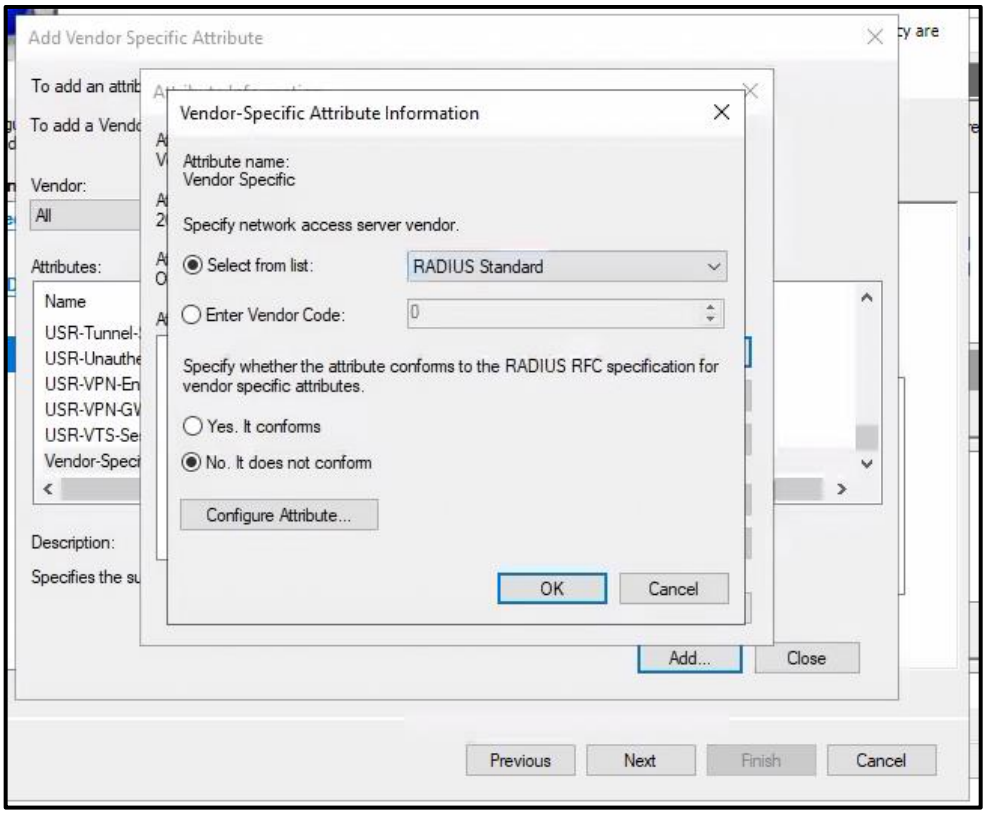
Right click and click new



Then I needed to specify the conditions for this policy

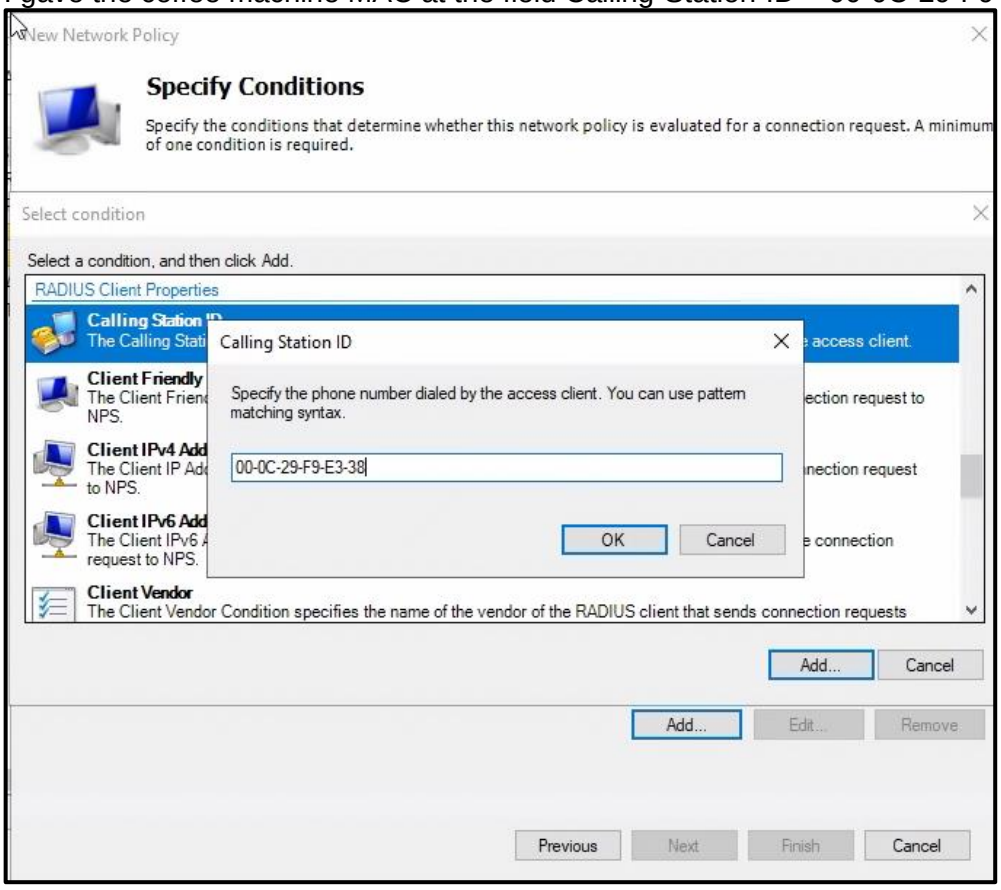


Kevin Lopci 2410410042

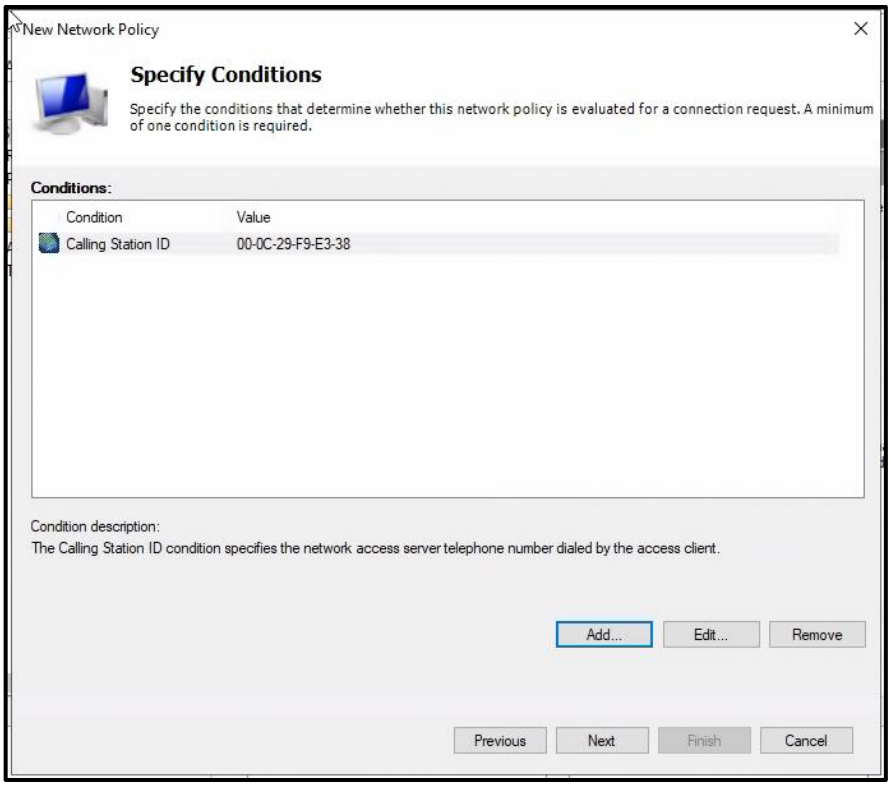


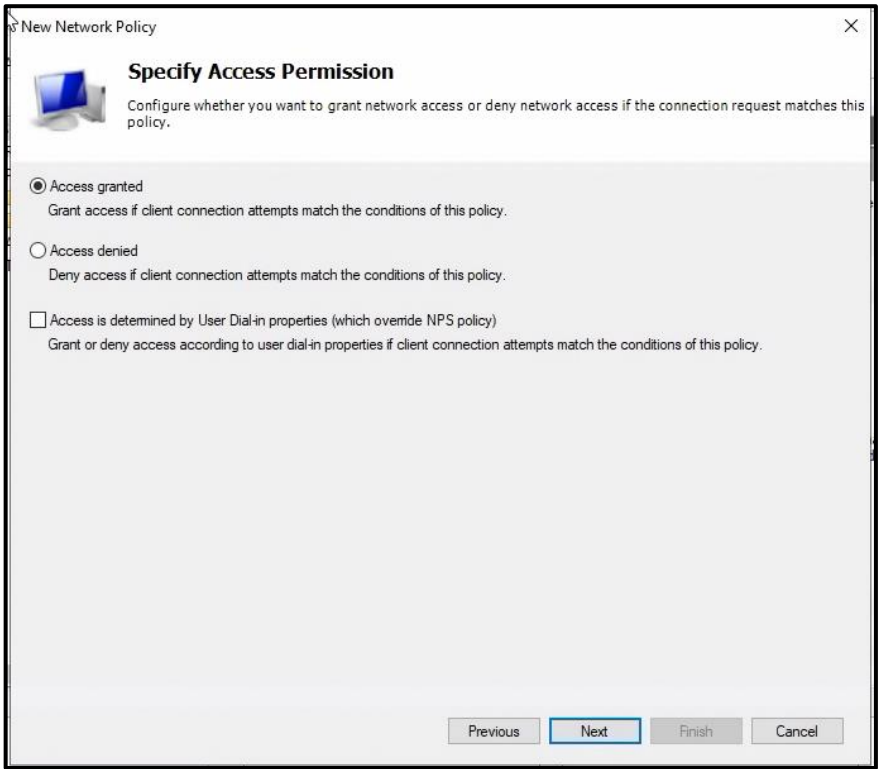
I put a shared key same as I putted it to the switch and the following IP.

I gave the coffee machine MAC at the field Calling-Station-ID = 00-0C-29-F9-E3-38

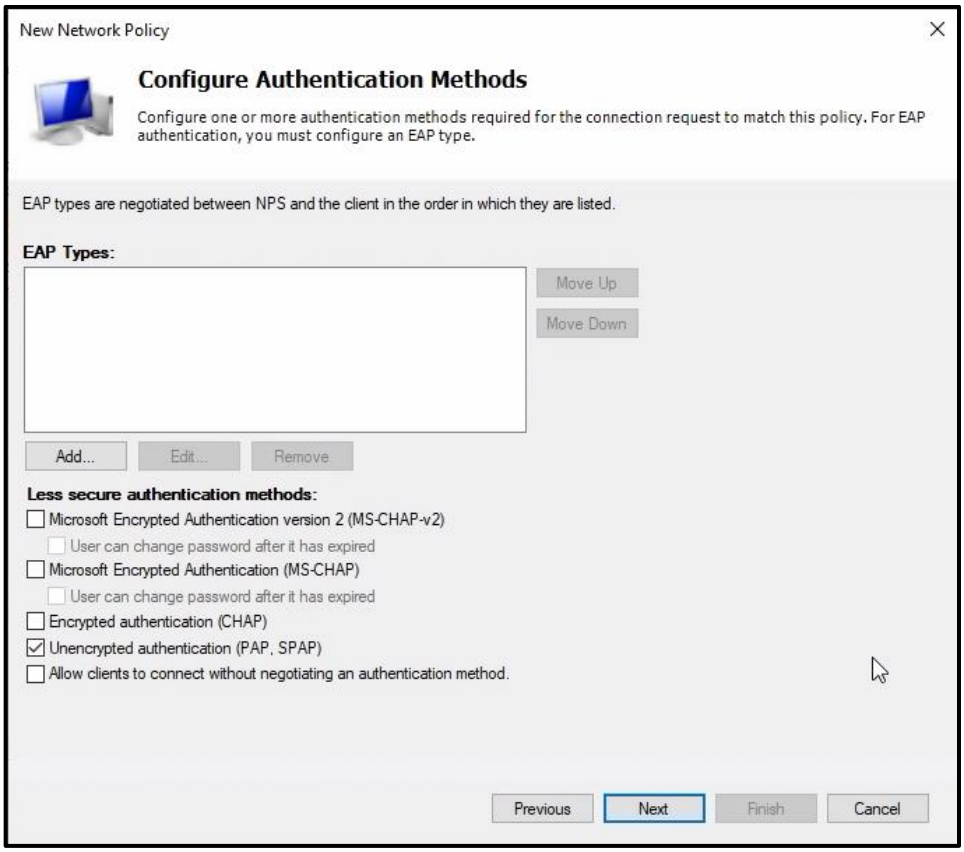


Kevin Lopci 2410410042

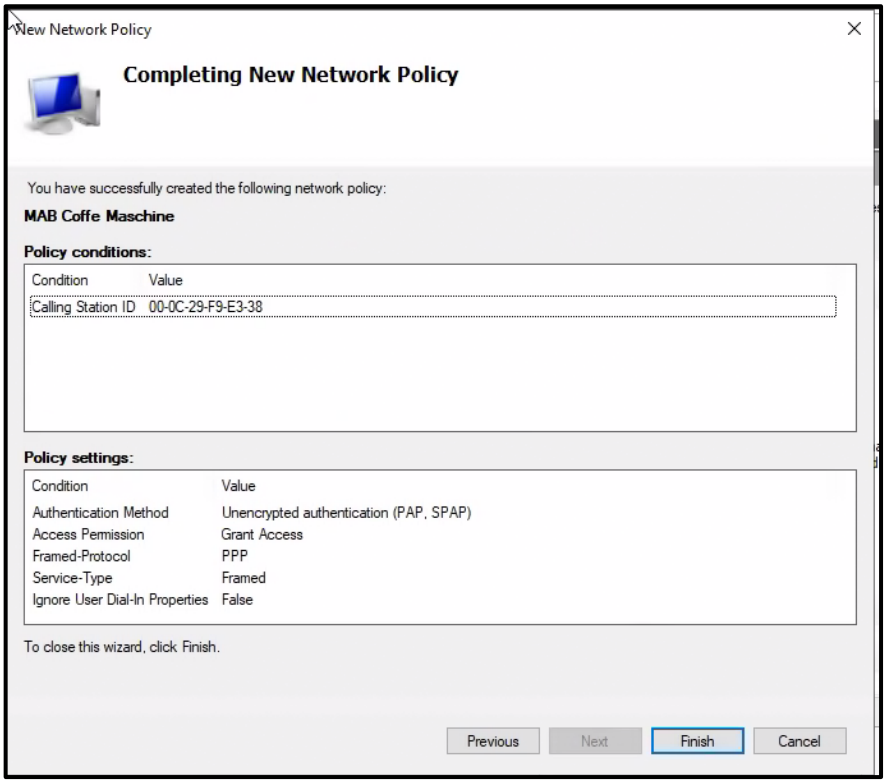




The policy should be Granted access for it to work



Configured constraints so only Unencrypted Authentication PAP and SPAP allowed



Then I clicked finish.
On the Coffee Machine VM MAC address verified as 00:0c:29:f9:e3:38 and received static IP 10.10.50.1 in VLAN 50

Kevin Lopci 2410410042

```
student@student-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:f9:e3:38 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.10.50.1/24 brd 10.10.50.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::d20a:2313:3ebc:2c1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
student@student-virtual-machine:~$
```

Ping tests show that's after MAB was finally configured the pings were successful

```
student@student-virtual-machine:~$ ping 7.7.7.7
PING 7.7.7.7 (7.7.7.7) 56(84) bytes of data.
64 bytes from 7.7.7.7: icmp_seq=2 ttl=254 time=1.64 ms
64 bytes from 7.7.7.7: icmp_seq=3 ttl=254 time=1.49 ms
^C
--- 7.7.7.7 ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.488/1.562/1.637/0.074 ms
student@student-virtual-machine:~$ ping 13.13.13.13
PING 13.13.13.13 (13.13.13.13) 56(84) bytes of data.
64 bytes from 13.13.13.13: icmp_seq=1 ttl=254 time=1.74 ms
64 bytes from 13.13.13.13: icmp_seq=2 ttl=254 time=1.91 ms
^C
--- 13.13.13.13 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.736/1.822/1.908/0.086 ms
student@student-virtual-machine:~$ ping 10.10.20.1
PING 10.10.20.1 (10.10.20.1) 56(84) bytes of data.
64 bytes from 10.10.20.1: icmp_seq=1 ttl=127 time=0.554 ms
64 bytes from 10.10.20.1: icmp_seq=2 ttl=127 time=0.473 ms
^C
--- 10.10.20.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1060ms
rtt min/avg/max/mdev = 0.473/0.513/0.554/0.040 ms
```

Ran show authentication sessions interface Gi1/0/7 to verify it was working

```
:ichGruppe9 show authentication sessions interface Gi1/0/7
 MAC Address     Method     Domain      Status Fg    Session ID
 000c.29f9.e338  mab        DATA        Authorized   90AA14FE0000008
ey to Session Events Flags:
  A Applying Policy (multi-line status for details)
  B Authc Success
  C Authz Success
  I Allocated IP Address
  P Pushed Session Policy
  X-Unknown Identiver
unable methods list
  Priority     List       Priority
  15           dot        1x
  10           mab        15
vitschGruppe9#
```

MAB Clients only have access to the order server IP via port 1337/tcp, and no other subnet.

```
ip access-list extended COFFEE_MAB
 10 permit tcp any host 7.7.7.7 eq 1337
 20 deny   ip  any any
```

Then apply it inbound on the switchport where the coffee-machine sits:

```
interface GigabitEthernet1/0/7
  switchport mode access
  switchport access vlan 50
  ip access-group COFFEE_MAB in
```

That ensures only TCP/1337 to 7.7.7.7 is permitted; everything else is dropped.

Kevin Lopci 2410410042

4 WLAN Authentication

4.1 Via AD Account (802.1X User Auth / WPA2-Enterprise)

1. Employees are allowed to connect their smartphones and other private devices to the corporate WLAN with the SSID “Staff-GrpY”. This is achieved by using 802.1X authentication with their AD account.

2. The SSID should be accessible regardless of which frequency bands the connecting devices support.

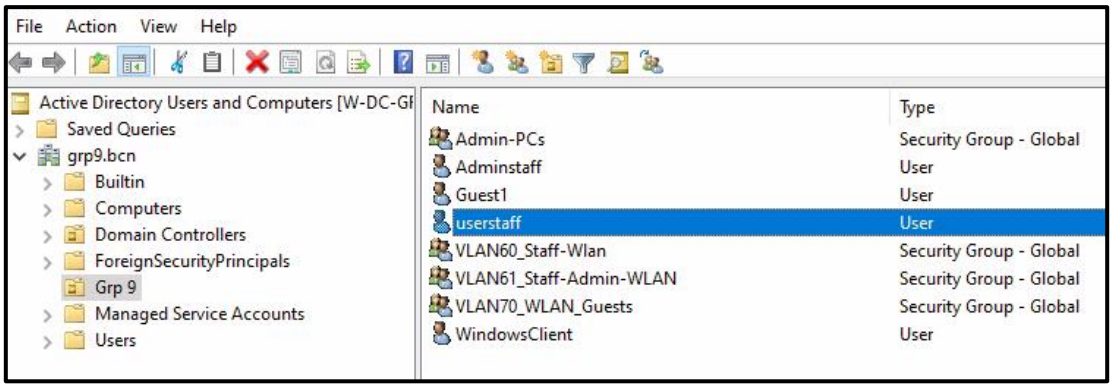
3. Employees have different permissions in and access to the network, based on their work position:

a. Create two new groups in your Active Directory, one for Users and one for Admins.

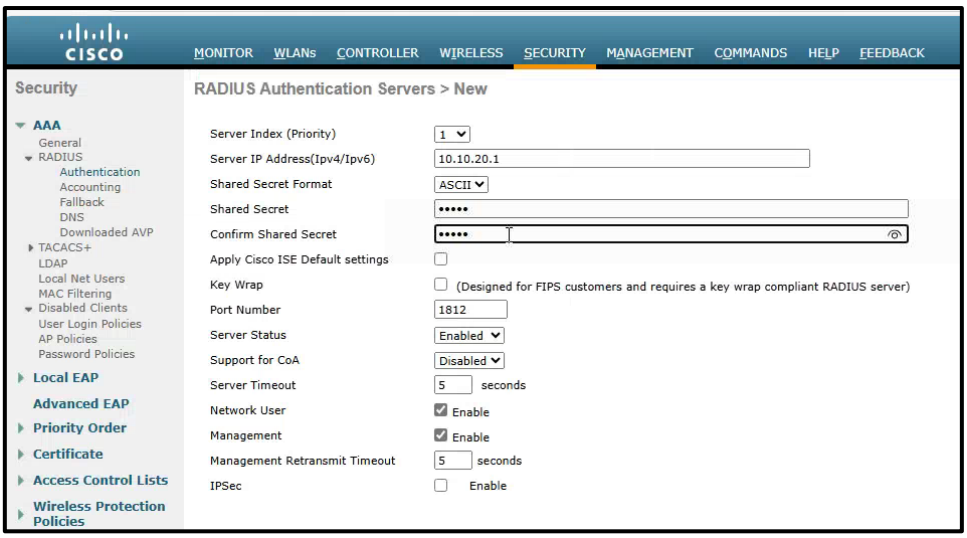
b. Create at least one user account in each of the 2 groups.

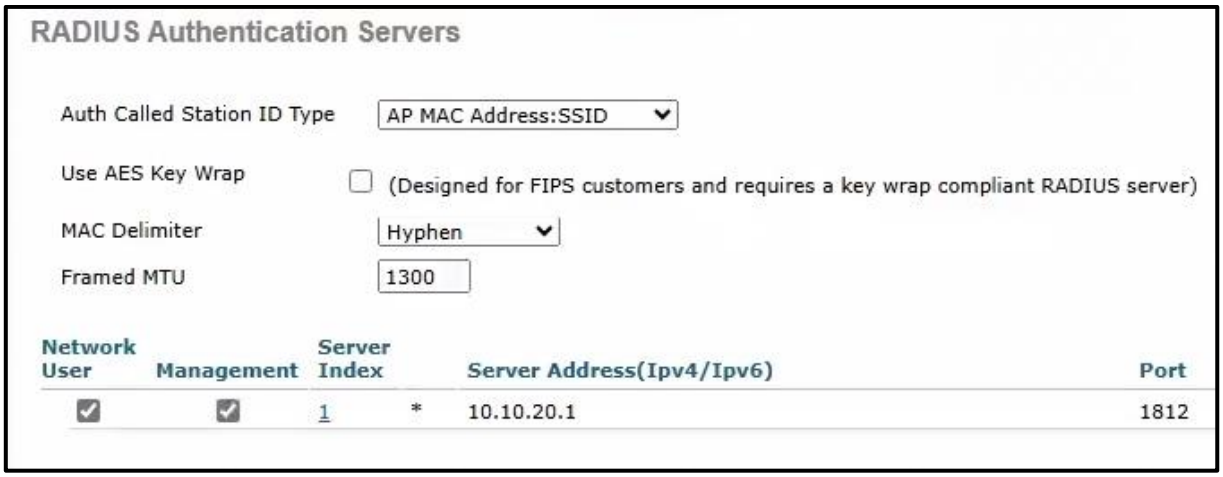
c. Based on the group membership, the user must be assigned to the correct VLAN automatically

Before we begin, these are our users, each of them are assigned to their corresponding group.
Guest1-> VLAN 70
Staffuser-> VLAN 60
Adminstaff-> VLAN 61



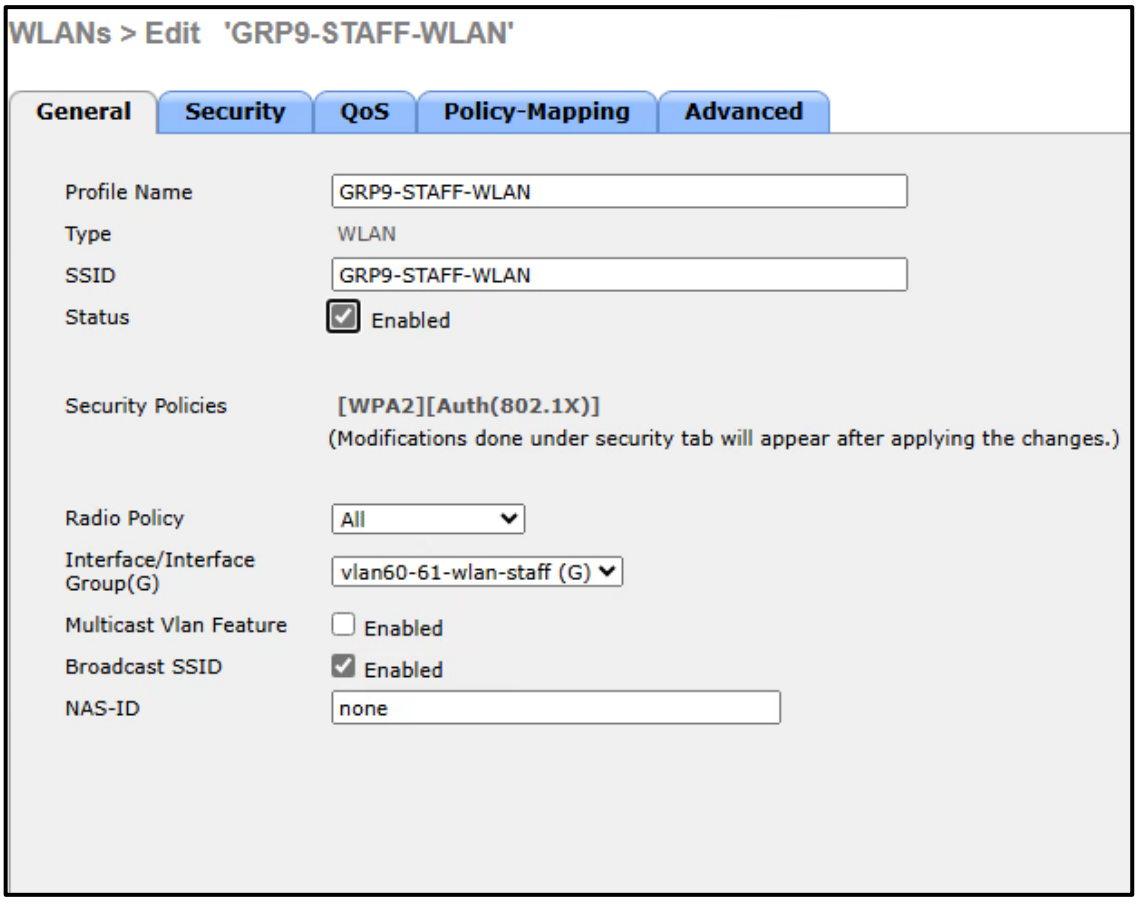
To complete this task, we need to first enable AAA to override on our WLANs via WLS GUI.
And add DC 10.10.20.1 as our AAA Server and set a shared secret.
First, we add our DC as a RADIUS Server on WLS, we go to “Security”->Radius->Authentication and click new.



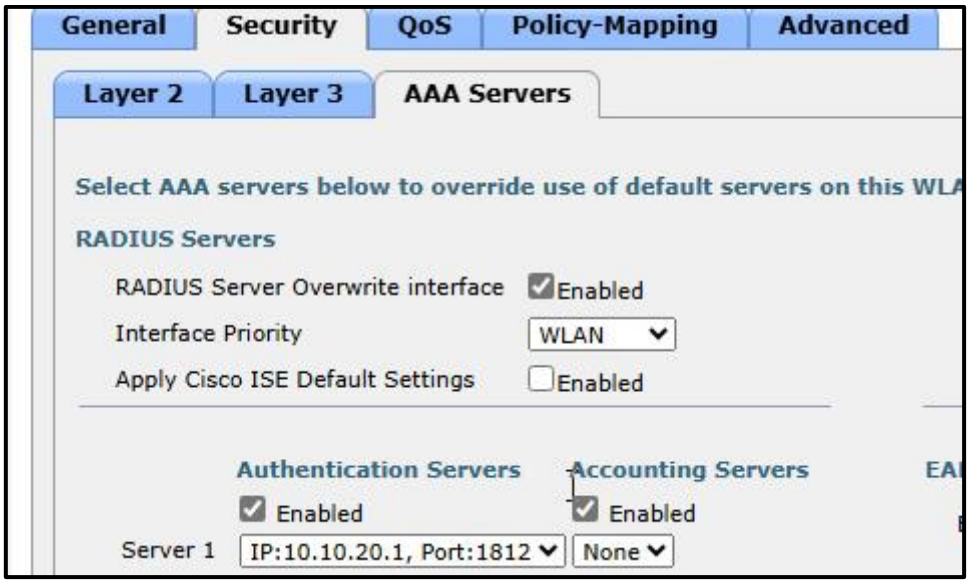


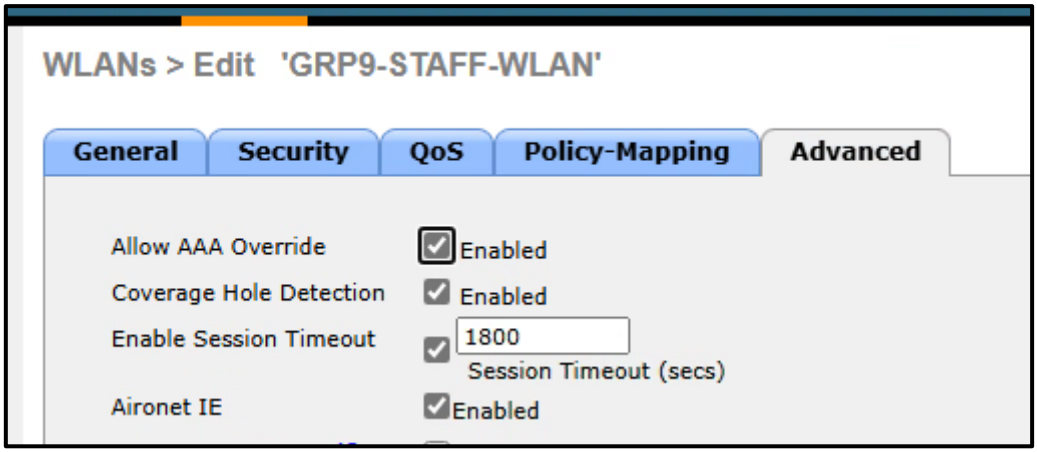
Documentation WLC SSID Settings

Create Staff WLAN, radio policy to allow any frequency band.



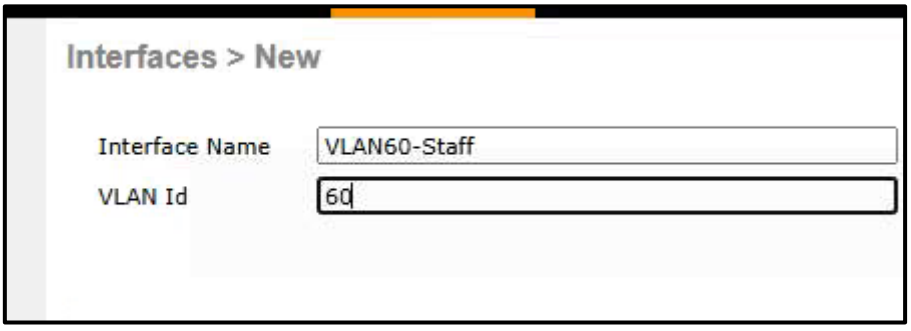
Enable RADIUS Server overwrite interface, Interface priority WLAN, and the IP Address of the DC.



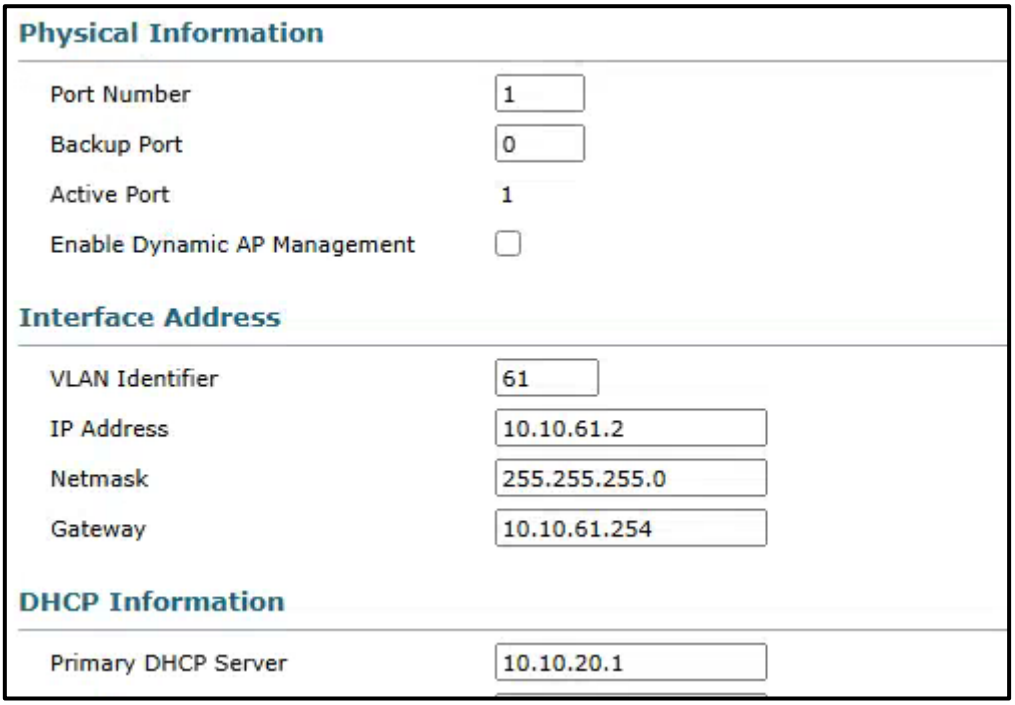


Documentation global WLC settings

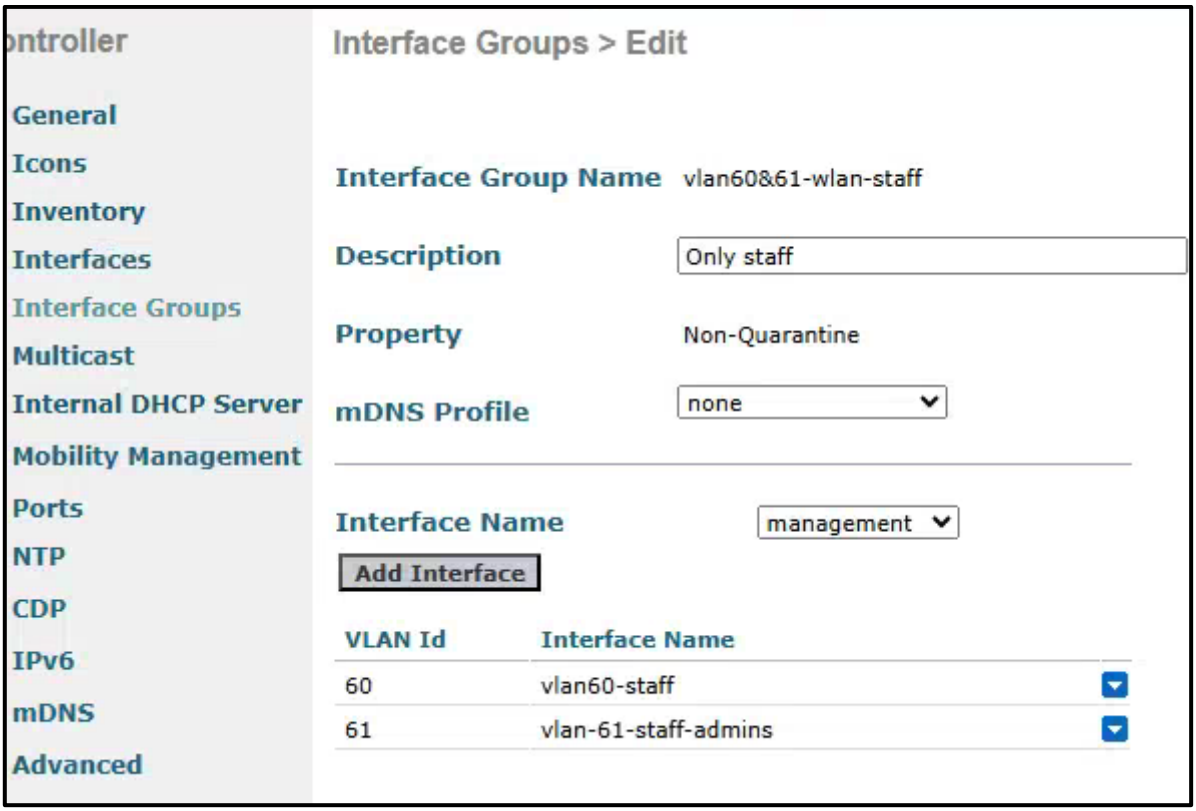
We need to create 2 VLAN interfaces on WLS, for Staff-Users is VLAN 60, and make sure



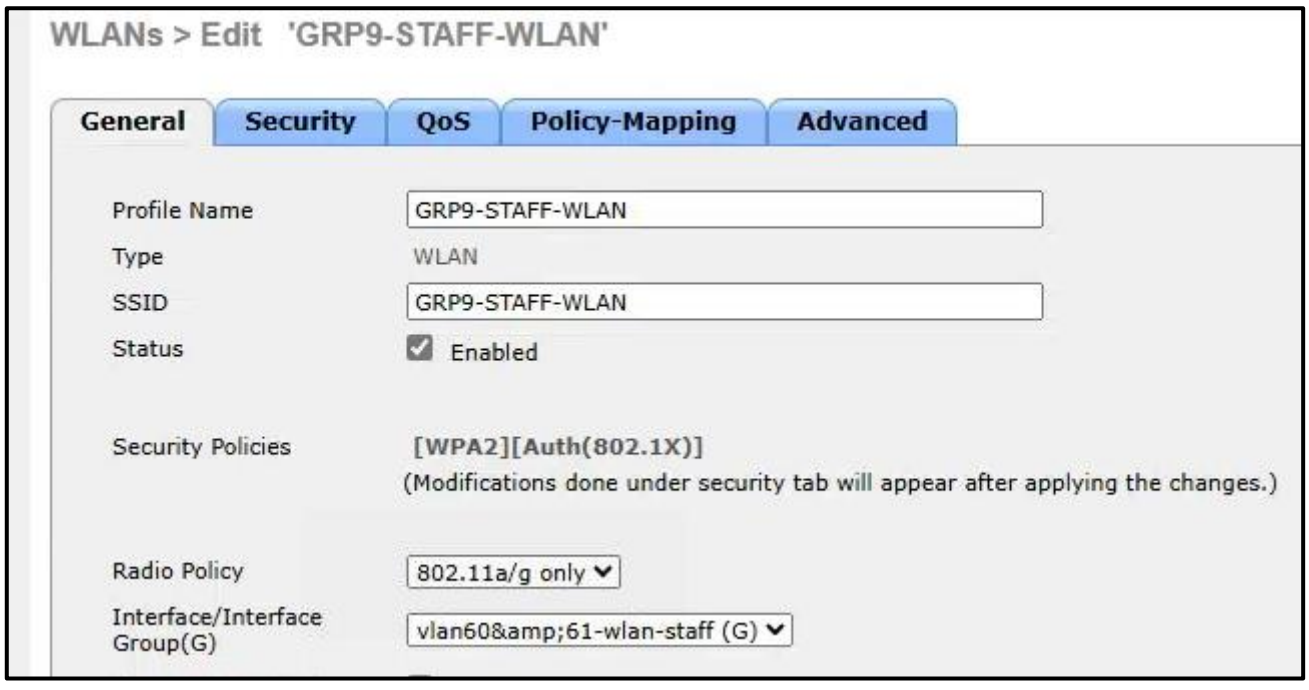
The same for VLAN -61



After this in order to make sure that WLAN-Staff is only assigning users from VLAN 60 or 61 according to the account they log in with, we need to also configure the interface group for that WLAN.

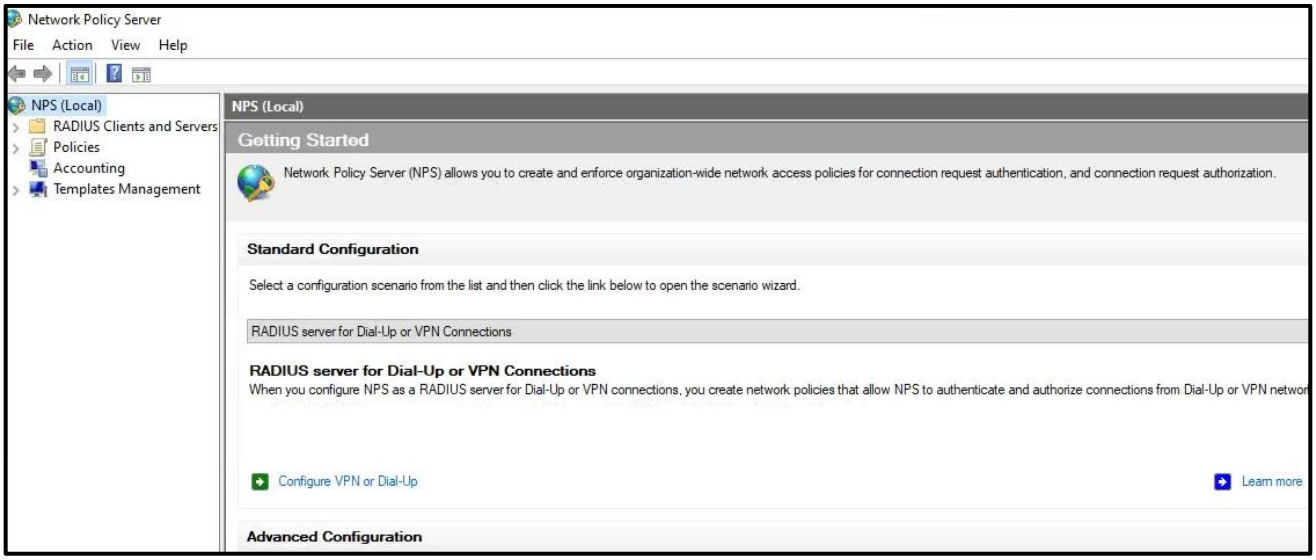


Supports both 2.4GHz and 5GHz.

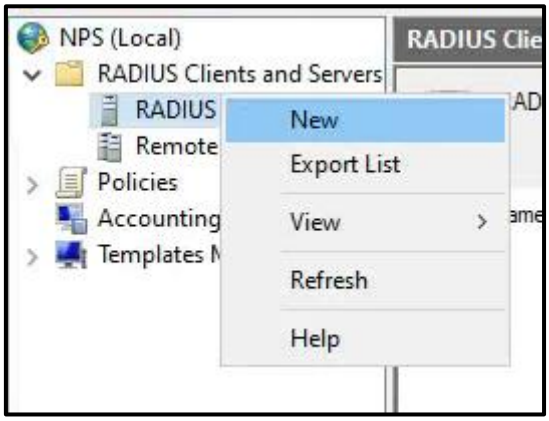


Now on the WS DC. Make sure NPS is installed as it is required to manage RADIUS.
We need to configure the WLS as a RADIUS Client because it forwards the Users requests to the NPS.

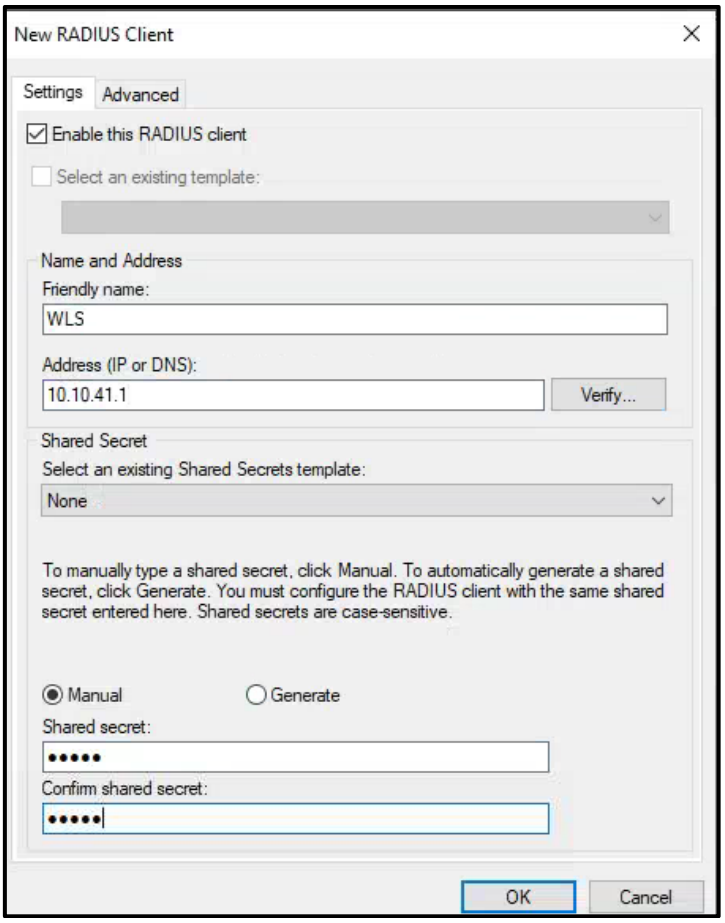
Documentation NPS settings for WLAN 802.1X



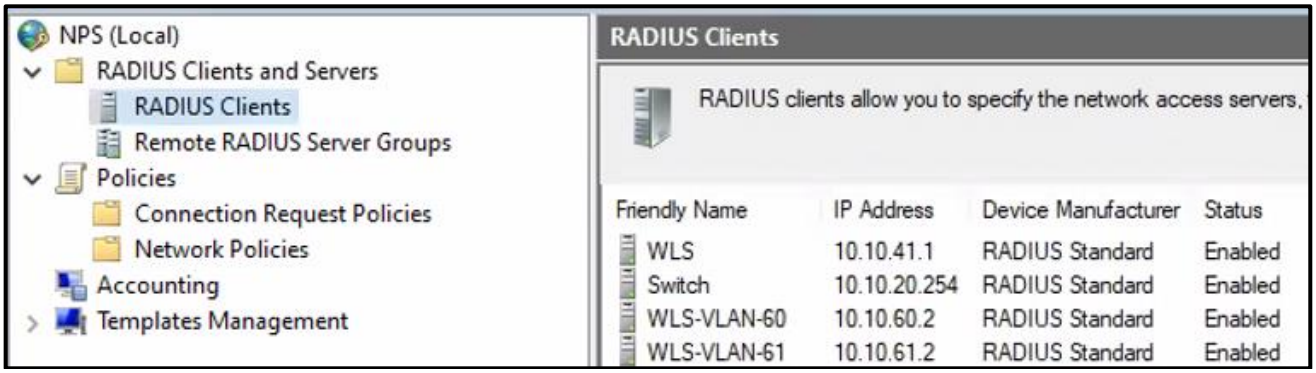
Radius Clients and Servers - > Configure Radius Clients



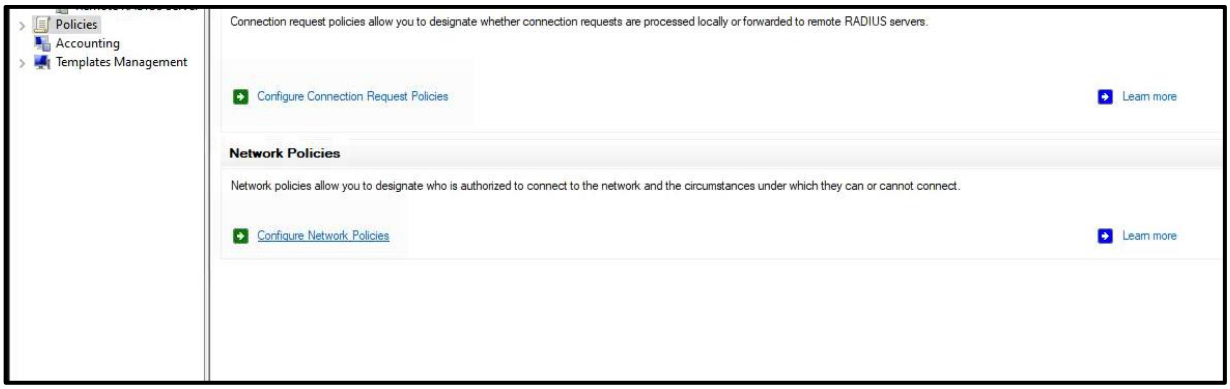
Give it a name, make it sure it can resolve or reach the WLS via DNS or IP ,make sure to add the shared Secret.



Should show it here. Do the same for all dynamic interfaces,because WLS may prefer dynamic interfaces due to priority misconfiguration to make authenticator requests via dynamic interfaces. Make sure to reserve these addresses in DHCP due to security reasons.

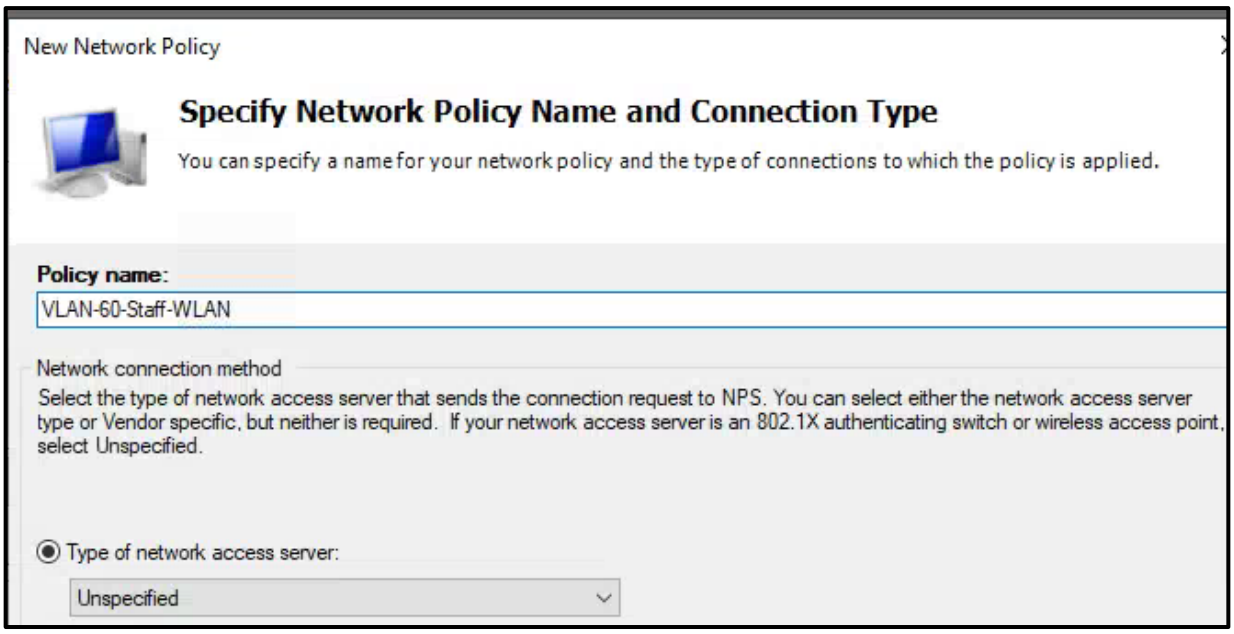


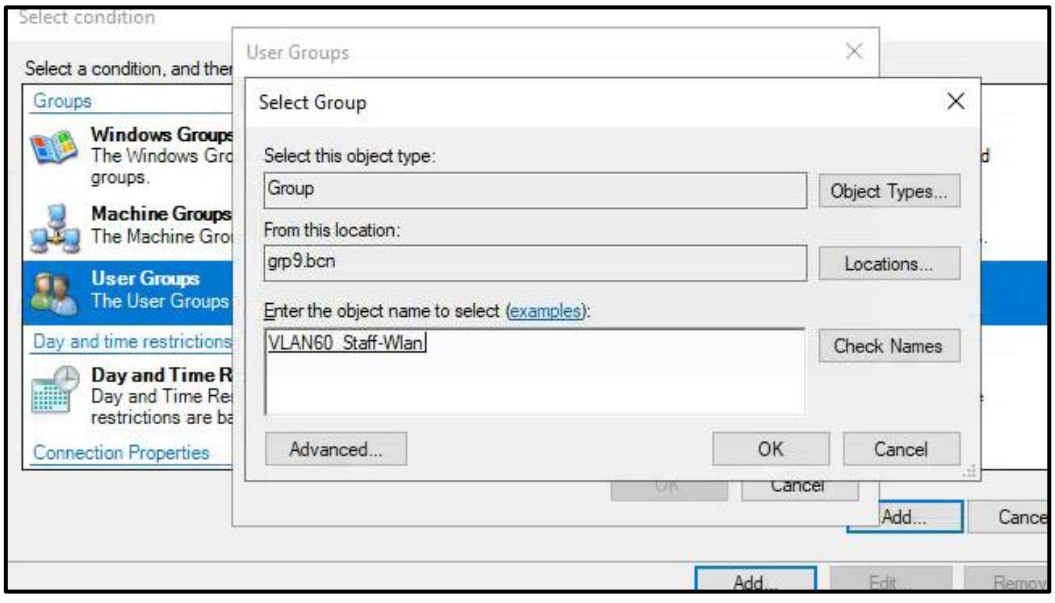
A new network policy needs to be created for each instance of VLAN to enable dynamic VLAN assignment.



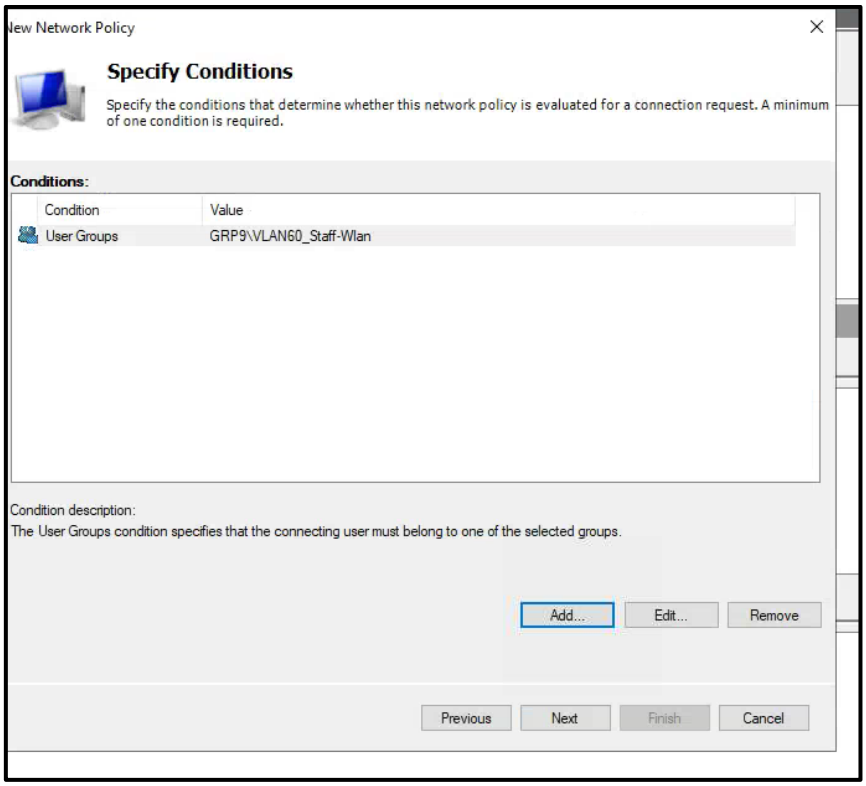
VLAN 60

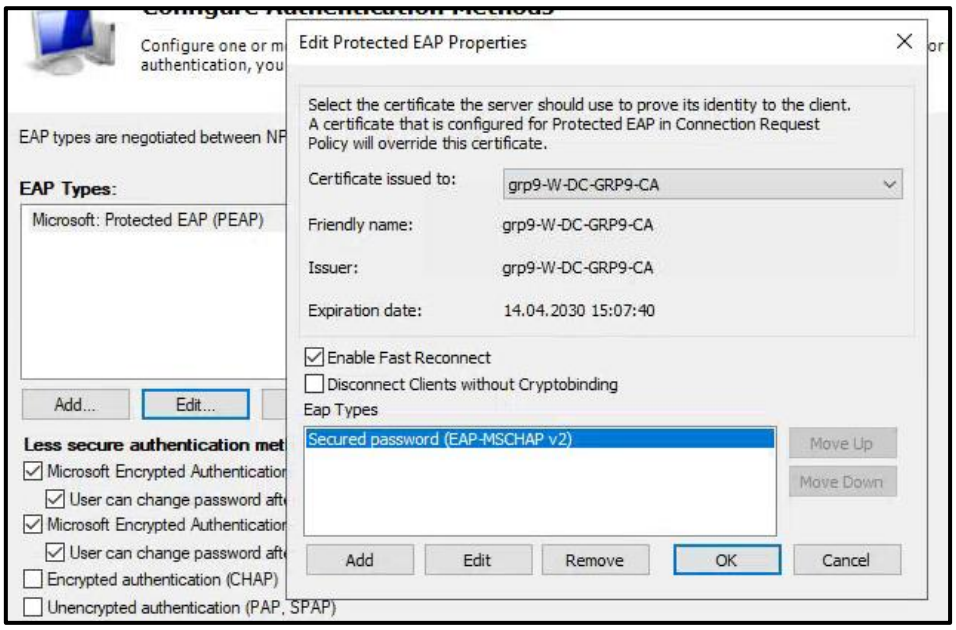
Procedure for VLAN-60-Staff



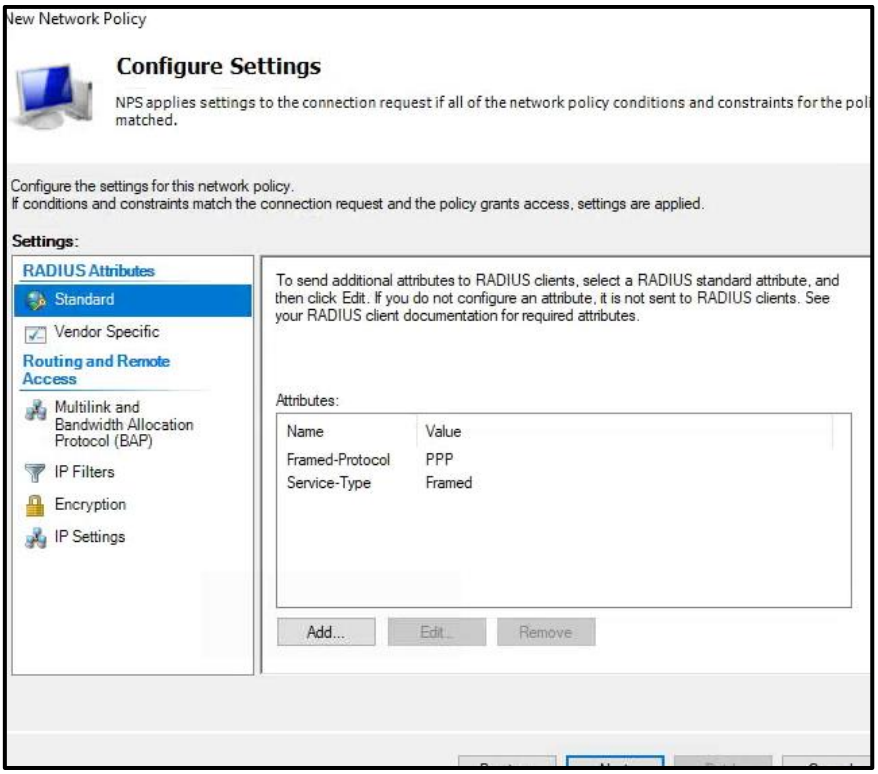


Kevin Lopci 2410410042

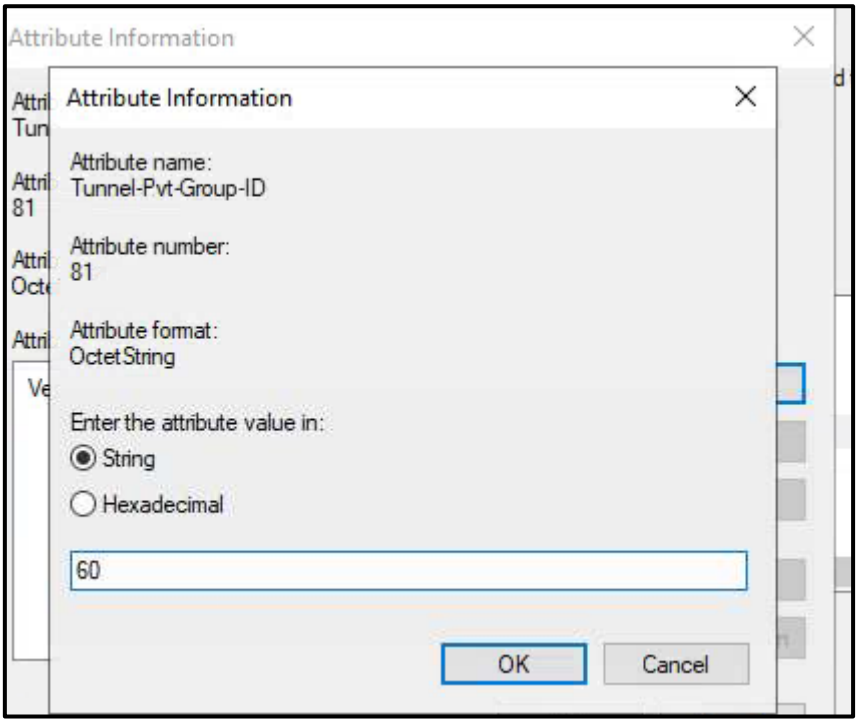




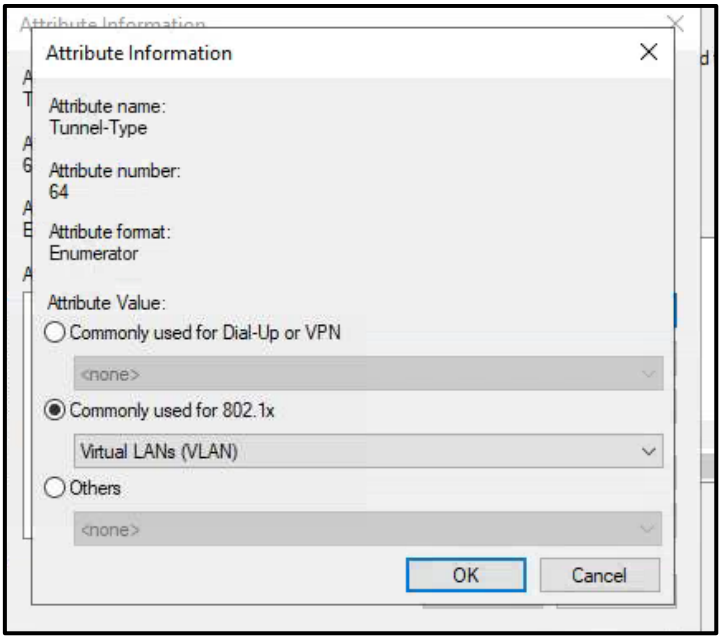
Click next until “Configure Settings”



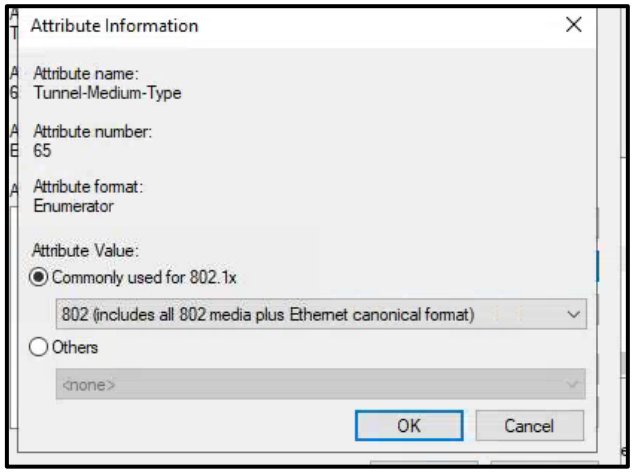
Add VLAN 60 for Tunnel-PVT-Group-ID



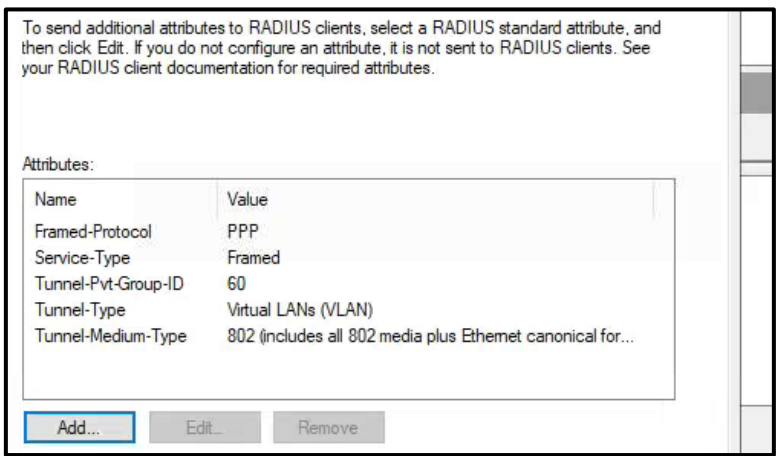
Tunnel type



Tunnel medium type: 802.1x (vlans)

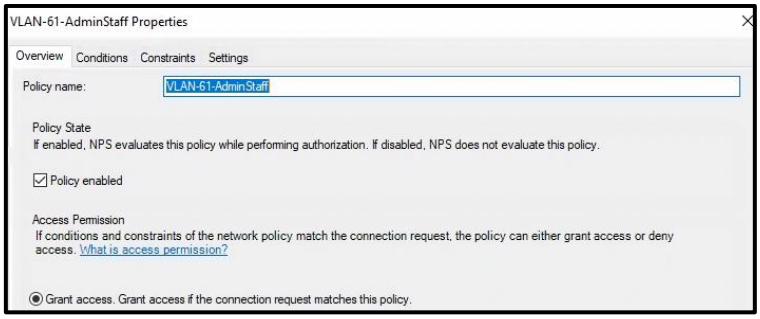


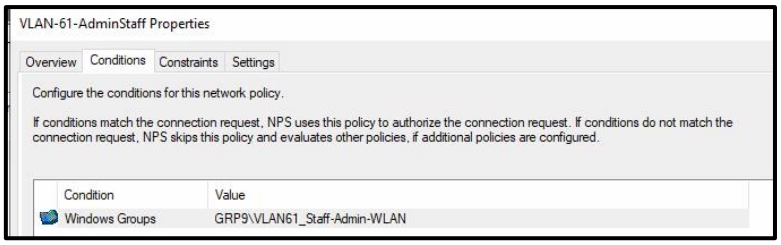
Tunnel middle type

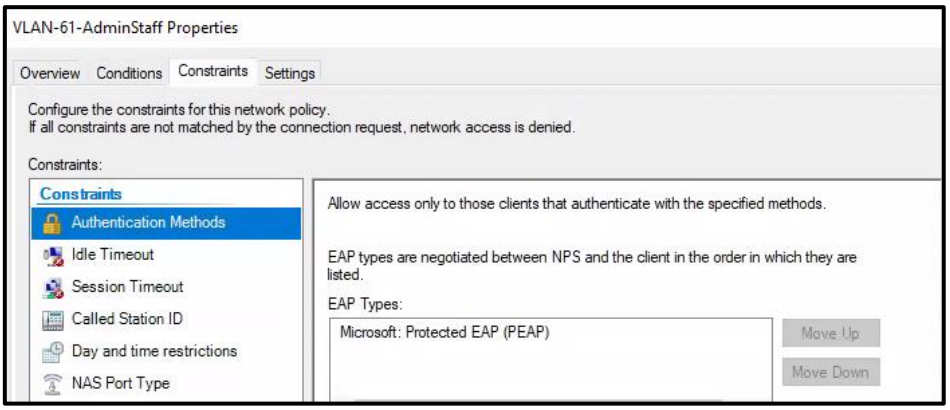


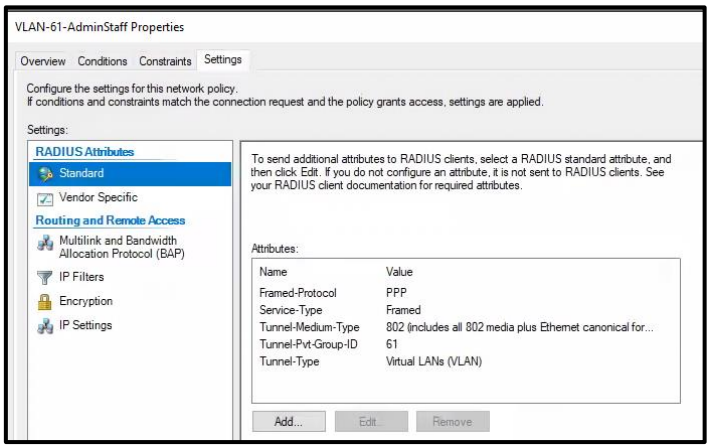
Kevin Lopci 2410410042

And then finish.
Do the same for VLAN 61.

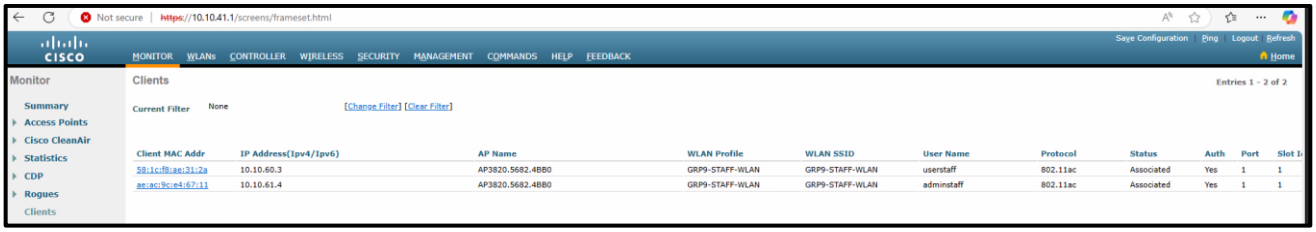


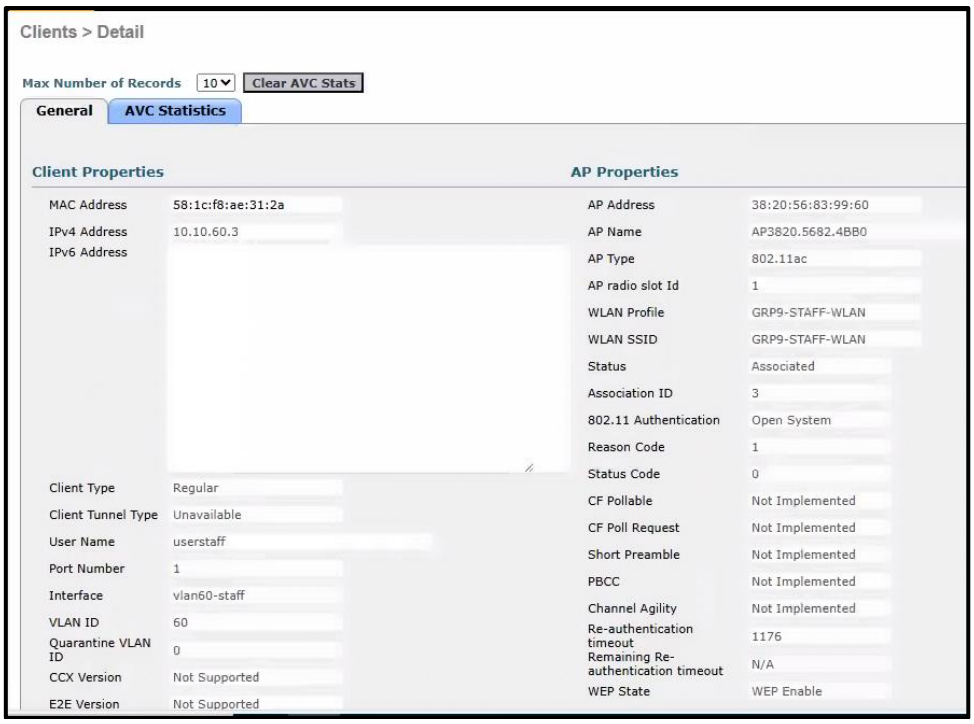


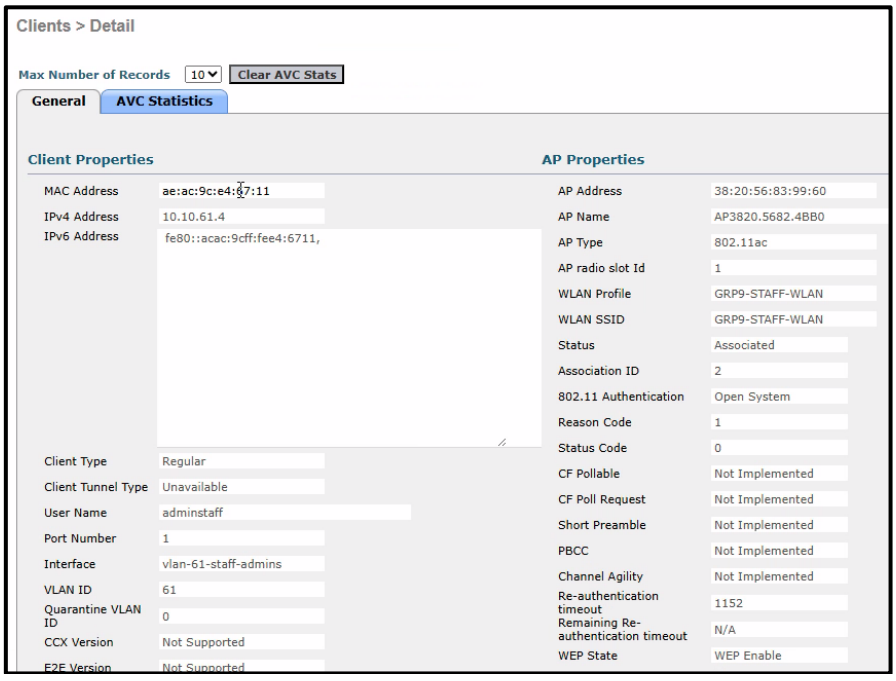


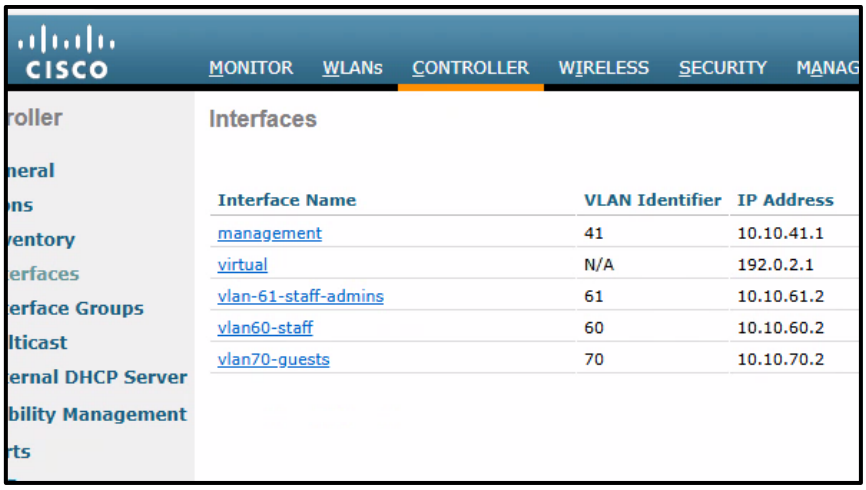


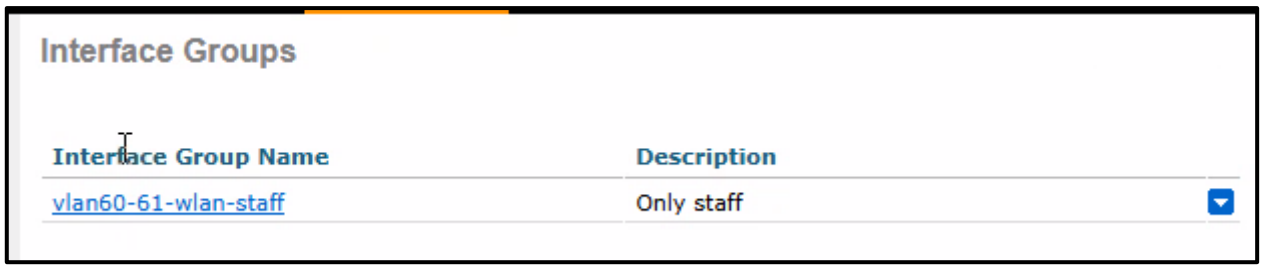
Documentation WLC Client Status (Monitor - Clients) -> IP, VLAN, Security, etc.



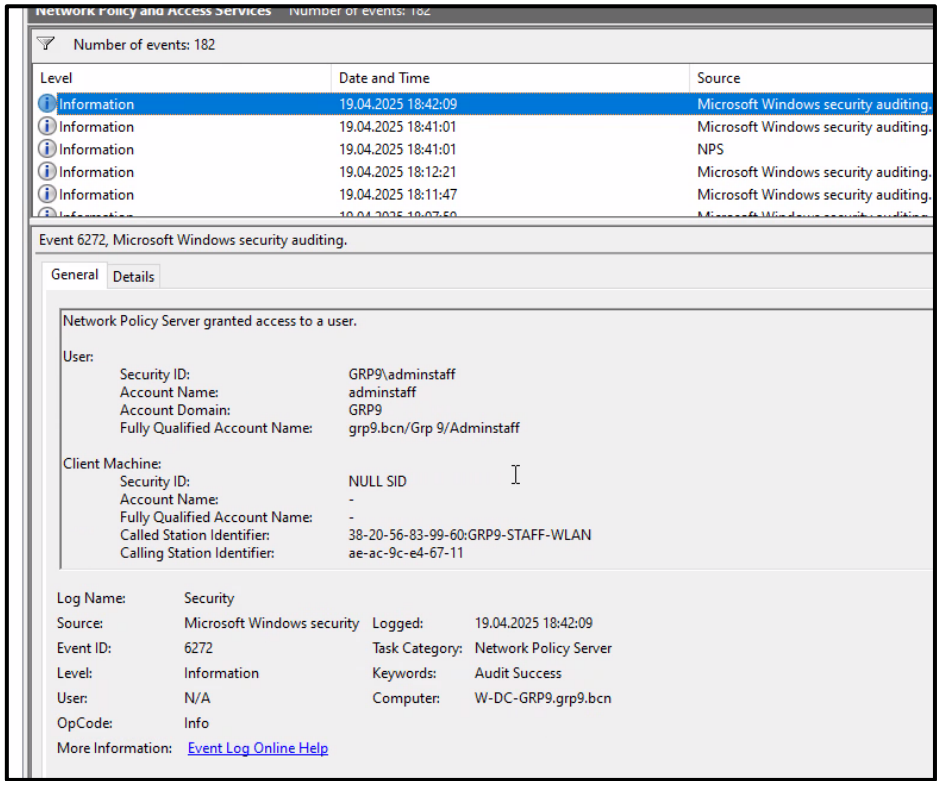


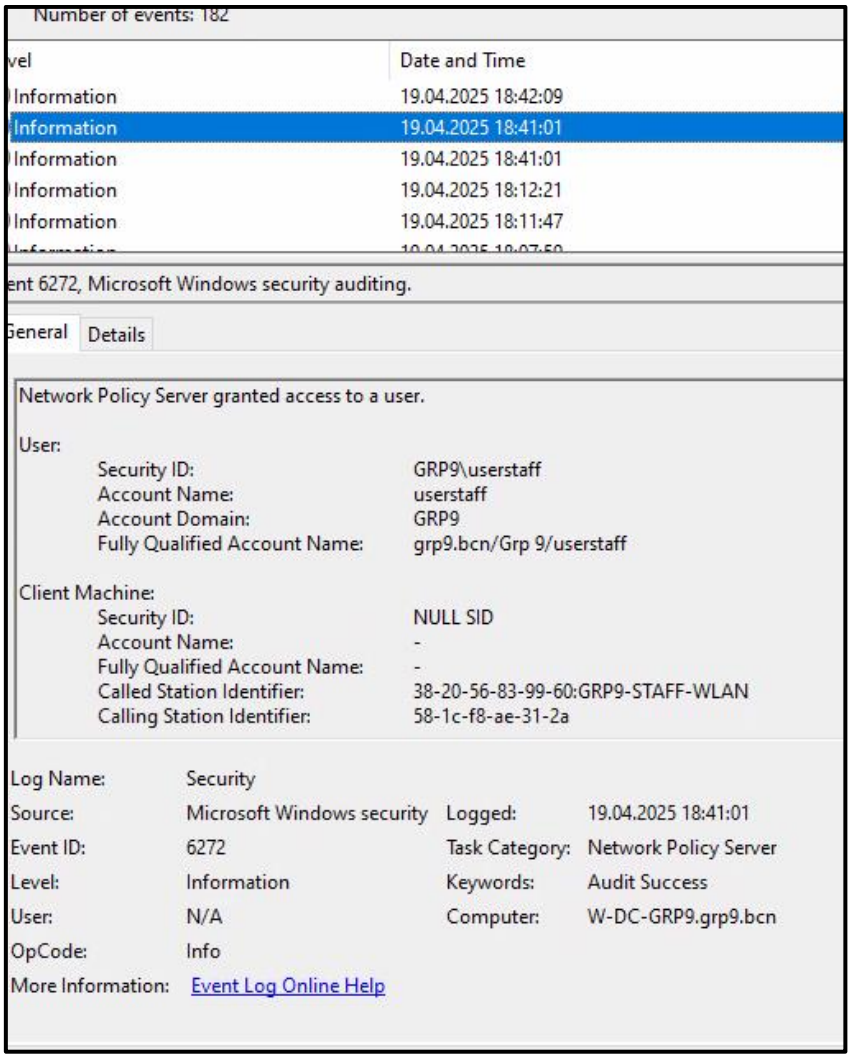






Documentation ISE Authentication Report

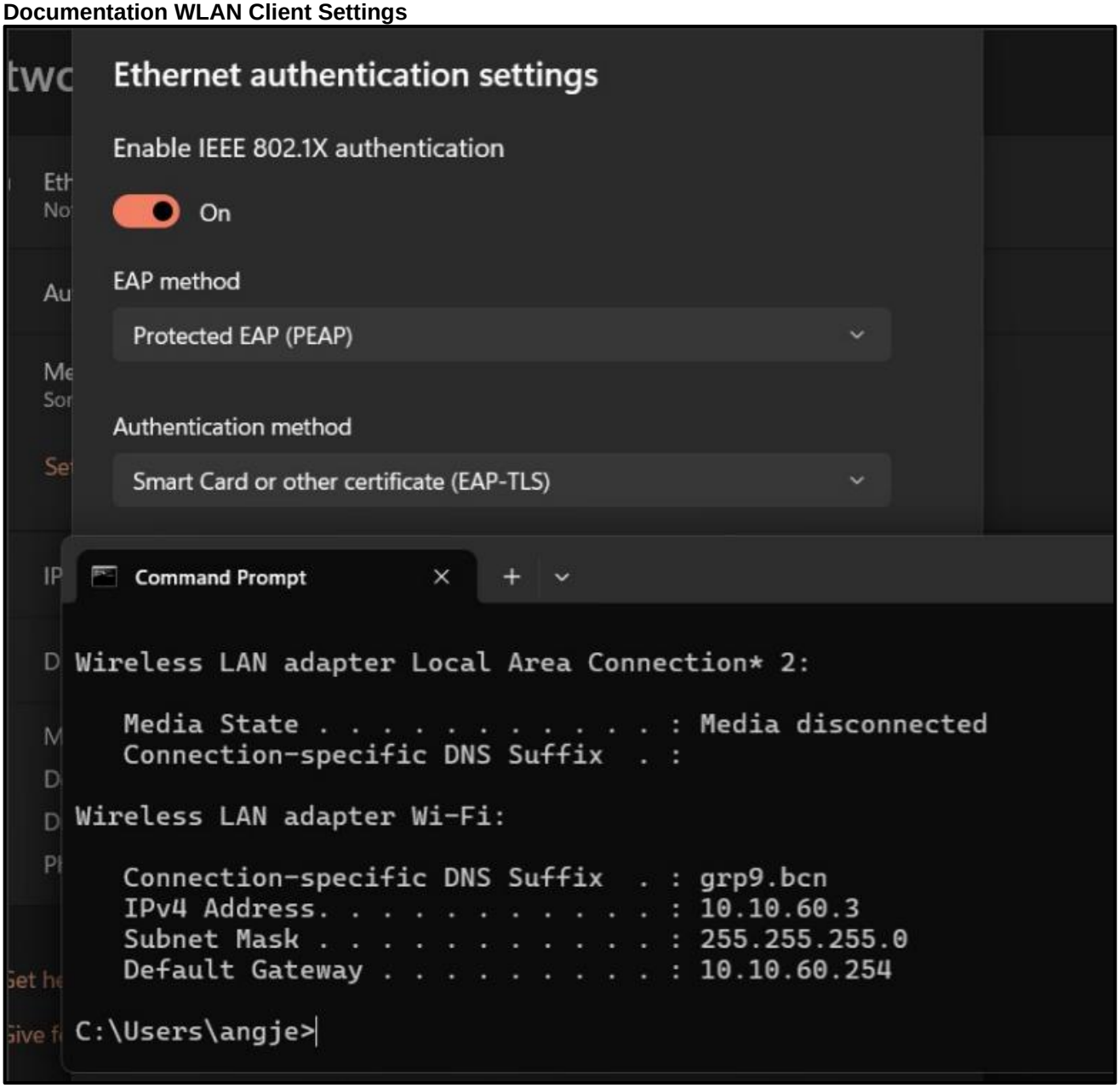



Number of events: 182
vel
Date and Time
Information 19.04.2025 18:42:09
Information 19.04.2025 18:41:01
Information 19.04.2025 18:41:01
Information 19.04.2025 18:12:21
Information 19.04.2025 18:11:47
ent 6272, Microsoft Windows security auditing.
General
Details
Network Policy Server granted access to a user.
User:
Security ID: GRP9\userstaff
Account Name: userstaff
Account Domain: GRP9
Fully Qualified Account Name: grp9.bcn/Grp 9/userstaff
Client Machine:
Security ID: NULL SID
Account Name: -
Fully Qualified Account Name: -
Called Station Identifier: 38-20-56-83-99-60:GRP9-STAFF-WLAN
Calling Station Identifier: 58-1c-f8-ae-31-2a
Log Name: Security
Source: Microsoft Windows security
Logged: 19.04.2025 18:41:01
Event ID: 6272
Task Category: Network Policy Server
Level: Information
Keywords: Audit Success
User: N/A
Computer: W-DC-GRP9.grp9.bcn
OpCode: Info
More Information: Event Log Online Help

Documentation Switchport Settings of WLAN components & Switch MAC Address Table (Switchports of APs and WLC)

```
SwitchGruppe9#show run interface Gi1/0/2
Building configuration...

Current configuration : 161 bytes
!
interface GigabitEthernet1/0/2
 description AP
 switchport access vlan 40
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
end

SwitchGruppe9#show run interface Gi1/0/34
Building configuration...

Current configuration : 125 bytes
!
interface GigabitEthernet1/0/34
 description WLC
 switchport trunk allowed vlan 40,41,60,61,70
 switchport mode trunk
end
SwitchGruppe9#show mac address-table interface Gi1/0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  40    3820.5682.4bb0    DYNAMIC     Gi1/0/2
Total Mac Addresses for this criterion: 1
SwitchGruppe9#show mac address-table interface Gi1/0/34
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  41    0059.dcb5.de20    DYNAMIC     Gi1/0/34
  41    0059.dcb5.de24    DYNAMIC     Gi1/0/34
  60    581c.f8ae.312a    DYNAMIC     Gi1/0/34
  61    aeac.9ce4.6711    DYNAMIC     Gi1/0/34
Total Mac Addresses for this criterion: 4
SwitchGruppe9#
```

Documentation WLAN Client Settings



4. Make sure that (by using ACLs):

a. Admins have: • access to all subnets

(Note: This is not a very secure way to authenticate Admins! We use it as a demon stration example to assign multiple VLANs via only one SSID. Consider TEAP or EAP-TLS for admin access in productive environments!)

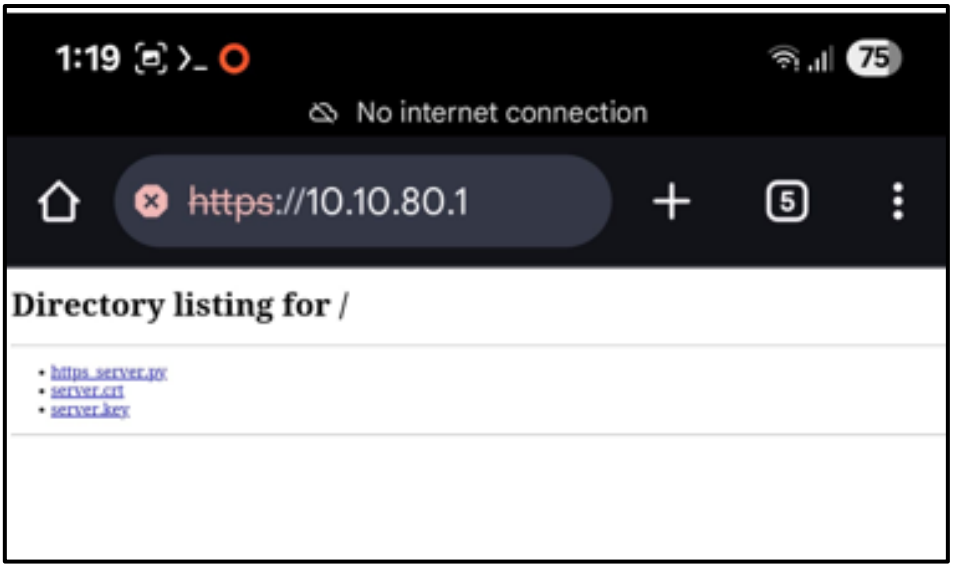
b. Users have:

• https access to the DMZ web server • http/https access to the “Internet”

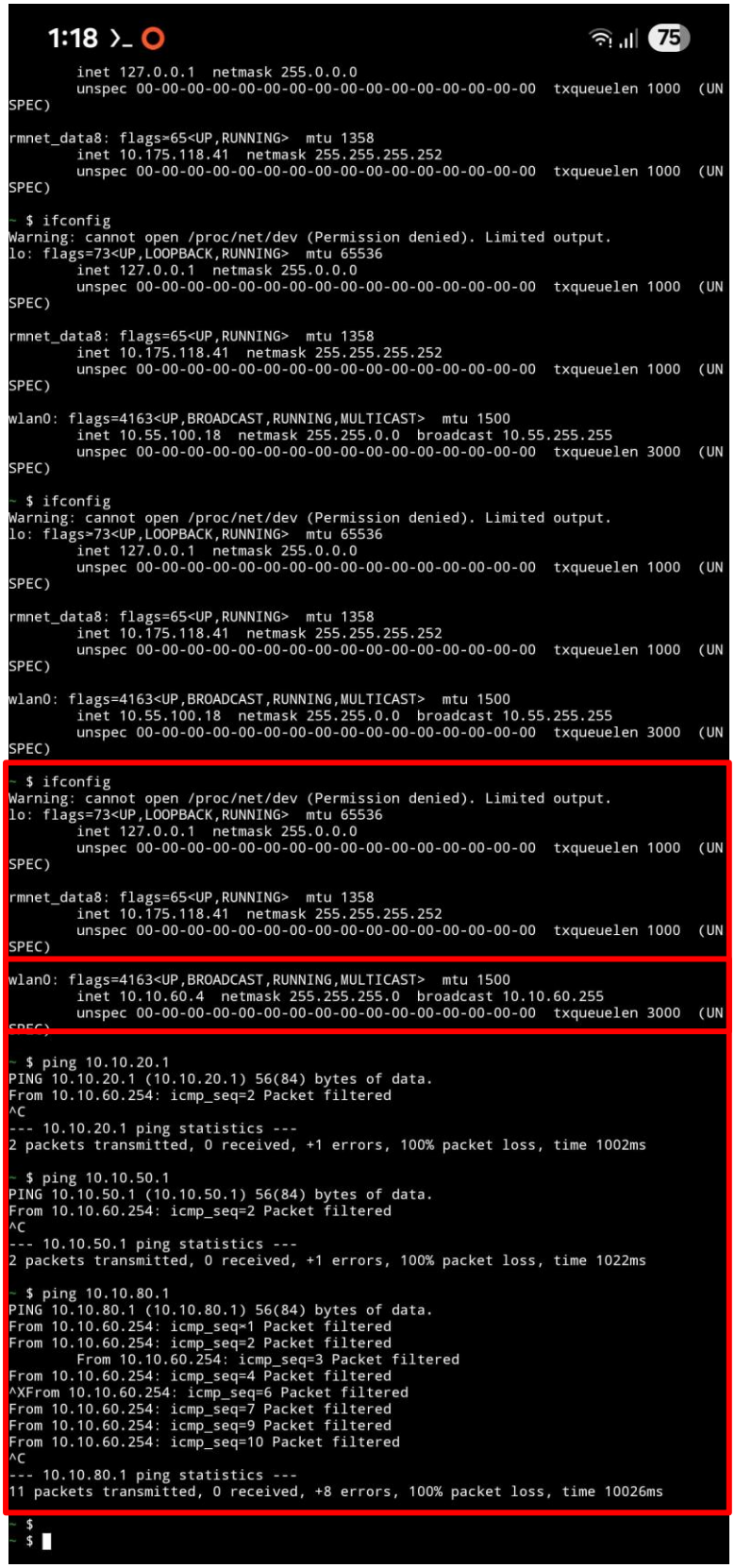
• no access to any other subnet.

```
SwitchGruppe9(config)#ip access-list extended VLAN61-ADMIN-FULL
SwitchGruppe9(config-ext-nacl)#permit ip 10.10.61.0 0.0.0.255 any
SwitchGruppe9(config-ext-nacl)#exit
SwitchGruppe9(config)#
SwitchGruppe9(config)#ip access-list extended VLAN60-USERS-RESTRICTED
SwitchGruppe9(config-ext-nacl)#permit tcp 10.10.60.0 0.0.0.255 host 10.10.80.1 eq 443
SwitchGruppe9(config-ext-nacl)#permit tcp 10.10.60.0 0.0.0.255 host 13.13.13.13

SwitchGruppe9(config-ext-nacl)#permit tcp 10.10.60.0 0.0.0.255 host 13.13.13.13 eq 80
SwitchGruppe9(config-ext-nacl)#permit tcp 10.10.60.0 0.0.0.255 host 13.13.13.13 eq 443
SwitchGruppe9(config-ext-nacl)#deny ip 10.10.60.0 0.0.0.255 any
SwitchGruppe9(config-ext-nacl)#Exit
SwitchGruppe9(config)#
SwitchGruppe9(config)#interface Vlan60
SwitchGruppe9(config-if)# ip access-group VLAN60-USERS-RESTRICTED in
SwitchGruppe9(config-if)#Exit
SwitchGruppe9(config)#
SwitchGruppe9(config)#interface Vlan61
SwitchGruppe9(config-if)# ip access-group VLAN61-ADMIN-FULL in
SwitchGruppe9(config-if)#exit
```

Testing with Clients

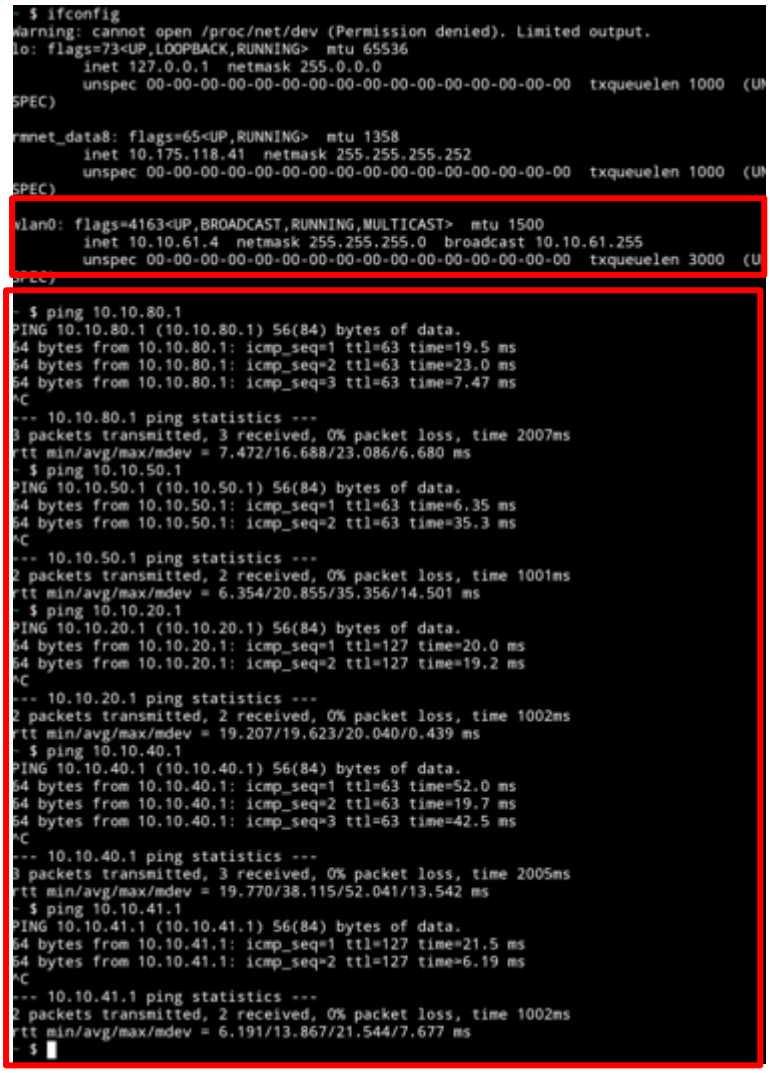


```
~ $
~ $ ifconfig
Warning: cannot open /proc/net/dev (Permission denied). Limited output.
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UN
SPEC)

rmnet_data8: flags=65<UP,RUNNING>  mtu 1358
        inet 10.175.118.41  netmask 255.255.255.252
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UN
SPEC)

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.60.4  netmask 255.255.255.0  broadcast 10.10.60.255
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 3000  (UN
SPEC)

~ $ ping 13.13.13.13
PING 13.13.13.13 (13.13.13.13) 56(84) bytes of data.
64 bytes from 13.13.13.13: icmp_seq=1 ttl=254 time=59.1 ms
64 bytes from 13.13.13.13: icmp_seq=2 ttl=254 time=23.7 ms
^C
--- 13.13.13.13 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 23.706/41.409/59.113/17.704 ms
~ $
```


1:18
75
inet 127.0.0.1 netmask 255.0.0.0
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
rmnet_data8: flags=65<UP,RUNNING> mtu 1358
inet 10.175.118.41 netmask 255.255.255.252
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
~ $ ifconfig
Warning: cannot open /proc/net/dev (Permission denied). Limited output.
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
rmnet_data8: flags=65<UP,RUNNING> mtu 1358
inet 10.175.118.41 netmask 255.255.255.252
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.55.100.18 netmask 255.255.0.0 broadcast 10.55.255.255
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 3000 (UNSPEC)
~ $ ifconfig
Warning: cannot open /proc/net/dev (Permission denied). Limited output.
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
rmnet_data8: flags=65<UP,RUNNING> mtu 1358
inet 10.175.118.41 netmask 255.255.255.252
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.55.100.18 netmask 255.255.0.0 broadcast 10.55.255.255
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 3000 (UNSPEC)
~ $ ifconfig
Warning: cannot open /proc/net/dev (Permission denied). Limited output.
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
rmnet_data8: flags=65<UP,RUNNING> mtu 1358
inet 10.175.118.41 netmask 255.255.255.252
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.60.4 netmask 255.255.255.0 broadcast 10.10.60.255
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 3000 (UNSPEC)
~ $ ping 10.10.20.1
PING 10.10.20.1 (10.10.20.1) 56(84) bytes of data.
From 10.10.60.254: icmp_seq=2 Packet filtered
^C
--- 10.10.20.1 ping statistics ---
2 packets transmitted, 0 received, +1 errors, 100% packet loss, time 1002ms
~ $ ping 10.10.50.1
PING 10.10.50.1 (10.10.50.1) 56(84) bytes of data.
From 10.10.60.254: icmp_seq=2 Packet filtered
^C
--- 10.10.50.1 ping statistics ---
2 packets transmitted, 0 received, +1 errors, 100% packet loss, time 1022ms
~ $ ping 10.10.80.1
PING 10.10.80.1 (10.10.80.1) 56(84) bytes of data.
From 10.10.60.254: icmp_seq=1 Packet filtered
From 10.10.60.254: icmp_seq=2 Packet filtered
From 10.10.60.254: icmp_seq=3 Packet filtered
From 10.10.60.254: icmp_seq=4 Packet filtered
^XFrom 10.10.60.254: icmp_seq=6 Packet filtered
From 10.10.60.254: icmp_seq=7 Packet filtered
From 10.10.60.254: icmp_seq=9 Packet filtered
From 10.10.60.254: icmp_seq=10 Packet filtered
^C
--- 10.10.80.1 ping statistics ---
11 packets transmitted, 0 received, +8 errors, 100% packet loss, time 10026ms
~ $
~ $

As a host of VLAN 60 you cannot reach any other subnets,but you can ping 13.13.13.13 (po port-specific ping since you cant place ports on loopbacks) and you can access DMZ web interface.

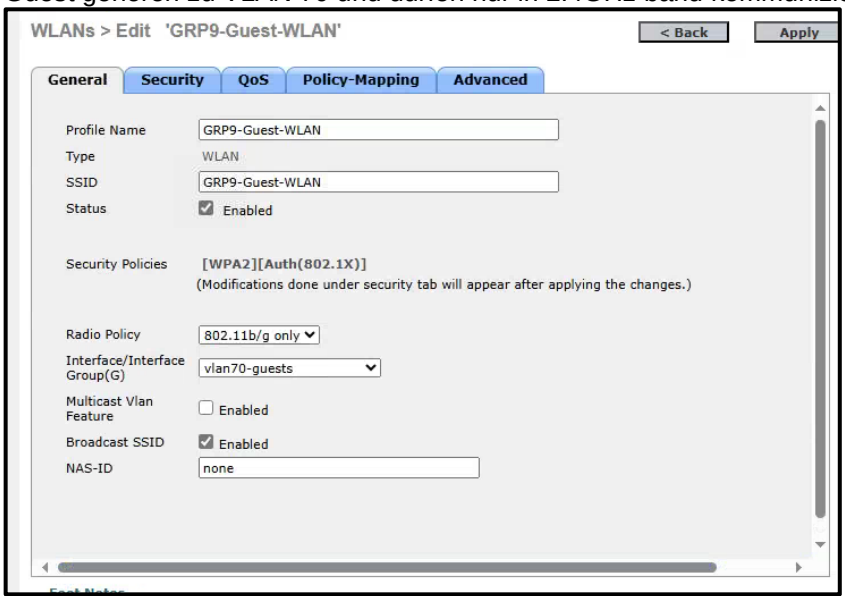
As a host of vlan 61 also staff admins, you can ping any subnet and access the web interface of DMZ.



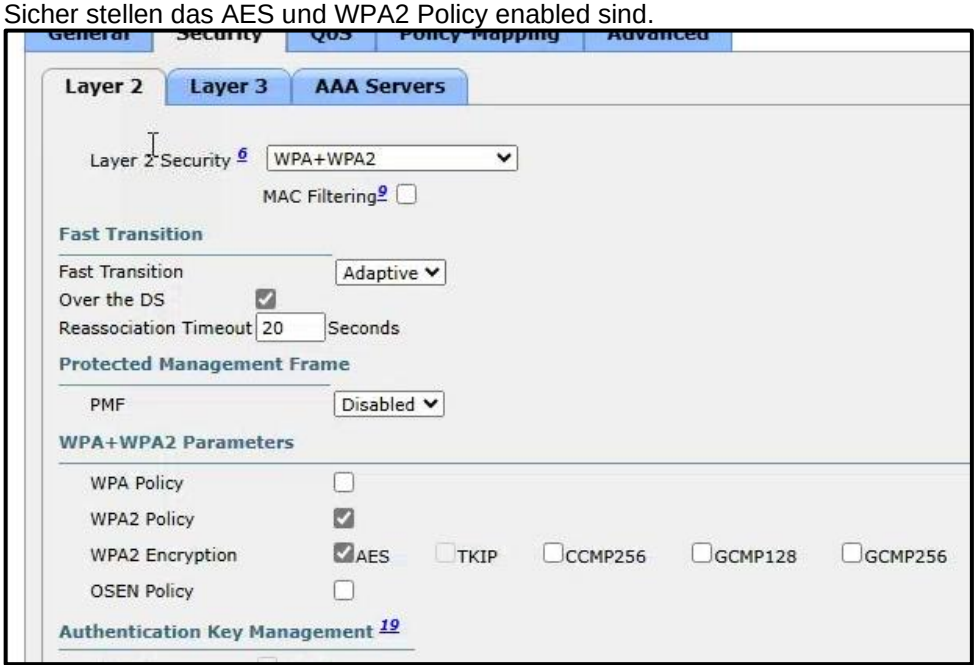
4.2 Via PSK (Guest Auth / WPA2-Personal)

1. Configure a custom SSID “Guest-GrpY” for your guests.
2. The guest WLAN is secured using a WPA2-AES PSK.
3. All guests should only use 2.4 GHz as the common frequency band.
4. Guests should not be able to reach each other.

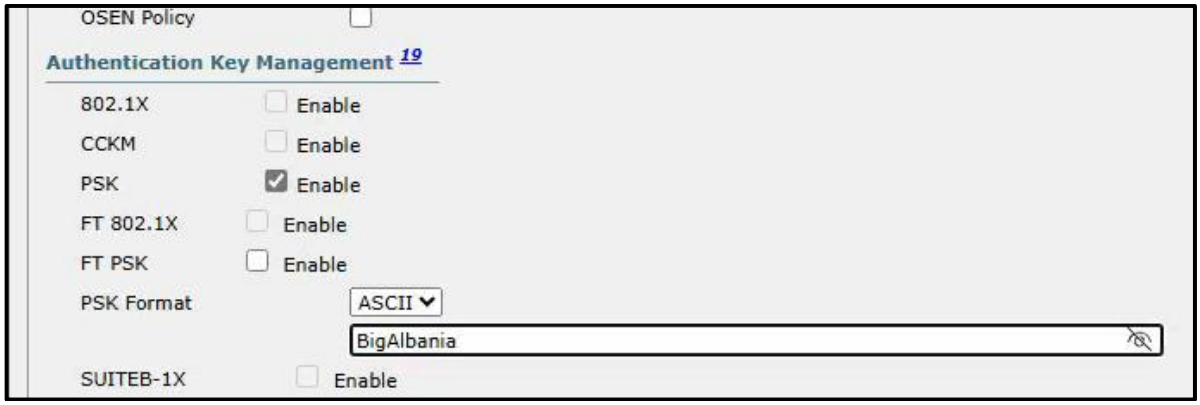
Guest gehören zu VLAN 70 und dürfen nur in 2.4GHz band kommunizieren.



Sicher stellen das AES und WPA2 Policy enabled sind.

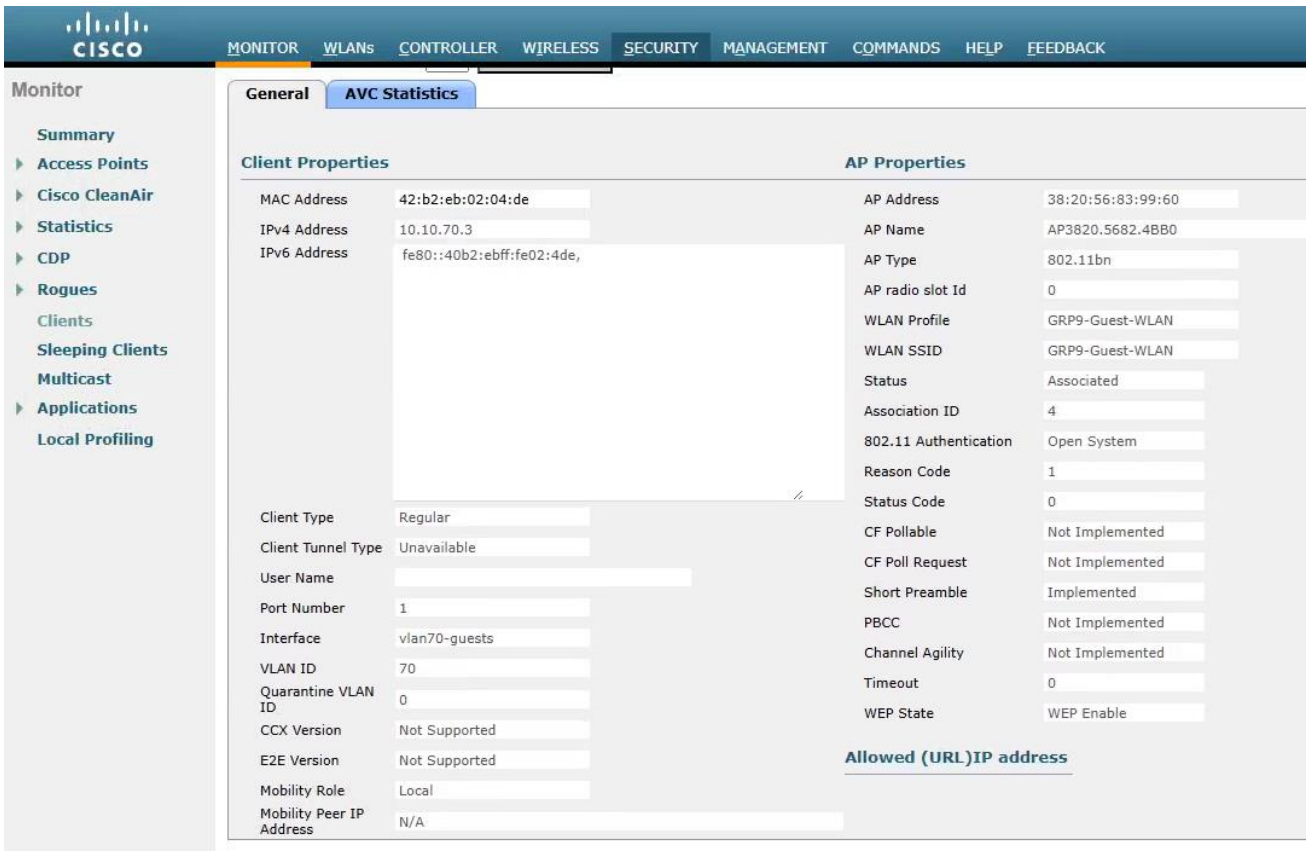


PSK enablen und ein password geben,



In Advanced-> Peer-2-Peer blocking , drop damit Guests nicht miteinander kommunizieren können.

Documentation WLC Client Status



Kevin Lopci 2410410042

5. Make sure that (by using ACLs): a. Guests have http/https access to “the Internet”. b. No Guest has access to any other subnet.

```
SwitchGruppe9(config)#ip access-list extended VLAN70-GUEST-ACL
SwitchGruppe9(config-ext-nacl)#permit tcp 10.10.70.0 0.0.0.255 host 13.13.13.13 eq 80
SwitchGruppe9(config-ext-nacl)#permit tcp 10.10.70.0 0.0.0.255 host 13.13.13.13 eq 443
SwitchGruppe9(config-ext-nacl)#deny ip 10.10.70.0 0.0.0.255 10.10.0.0 0.0.255.255
SwitchGruppe9(config-ext-nacl)#permit ip any any

SwitchGruppe9(config)#interface Vlan70
SwitchGruppe9(config-if)#ip access-group VLAN70-GUEST-ACL in
```

Client Test

5. Administra ents

To ensure secure and controlled administrative access, SSH access to the switch is configured to use centralized RADIUS-based authentication (NPS), with fallback to a local account in case the RADIUS server is unreachable.

5.1 SSH Access via Central AAA (RADIUS)

To secure SSH access to the switch using Microsoft NPS (RADIUS):

1. I enabled AAA on the switch (`aaa new-model`).
2. I configured a RADIUS server (`10.10.20.1`) and grouped it under `MY-NPS-SERVERS`.
3. I created a custom AAA method list named `SSH-LOGIN`, which first tries RADIUS and falls back to the local user.
4. I configured all VTY lines (`0-15`) to use this method list.
5. I enabled SSH on the switch by generating RSA keys and specifying SSH-only access on the VTY lines.
6. I successfully tested login with an AD user via SSH.

Switch Configuration:

```
! Enable AAA
aaa new-model

! Define RADIUS server
radius server NPS
 address ipv4 10.10.20.1 auth-port 1645 acct-port 1646
 key 427Al

! Group the server
aaa group server radius MY-NPS-SERVERS
 server name NPS

! AAA login method: try RADIUS, fallback to local
aaa authentication login SSH-LOGIN group MY-NPS-SERVERS local

! (Used in other steps – for 802.1X and authorization)
aaa authentication dot1x default group MY-NPS-SERVERS
aaa authorization network default group MY-NPS-SERVERS

! Use common session ID format
aaa session-id common
```

SSH Setup and VTY Line Binding:

```
! Configure SSH
ip domain-name grp9.bcn
crypto key generate rsa modulus 2048
ip ssh version 2

! Apply SSH-LOGIN AAA method to all VTY lines
line vty 0 4
 login authentication SSH-LOGIN
 transport input ssh
line vty 5 15
 login authentication SSH-LOGIN
 transport input ssh
```

Test and Result

I connected from my Linux VM using:

```
ssh is241031@switch.lab -p 3005
```

Result:

```
(is241031@switch.lab) Password:
Switch>
```

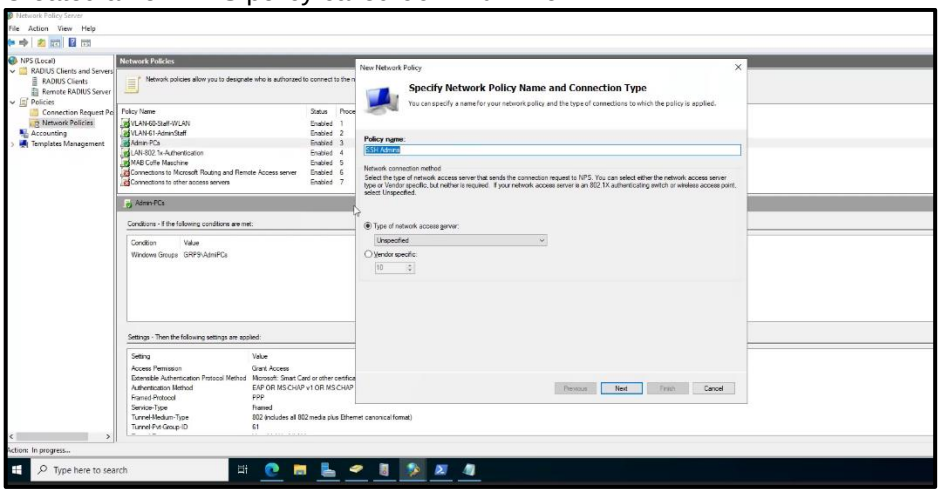
- The login prompt confirmed that the switch used RADIUS.
- I reached user exec mode (`Switch>`) indicating successful authentication via NPS.

5.2 Auto-Enable Mode via RADIUS

To ensure administrators are placed in privileged EXEC mode (`Switch#`) immediately after logging in via SSH, the NPS server was configured to return the Cisco-specific RADIUS attribute `shell:priv-lvl=15`.

What I Did:

- Created a new NPS policy called `SSH Admins`



- Applied a condition to match AD group `SSH-Admins`
- Under **RADIUS Attributes > Vendor Specific**, added:

```
Vendor Code: 9 (Cisco)
Attribute: shell:priv-lvl=15
```

- Added the following command on the switch:

```
aaa authorization exec default group MY-NPS-SERVERS if-authenticated
```

Result:

After successful login via SSH, users are automatically placed in enable mode:

```
$ ssh is241031@switch.lab -p 3005
(is241031@switch.lab) Password:
SwitchGruppe9#
```

Privilege level 15 confirmed with show privilege.

```
SwitchGruppe9#show privilege
Current privilege level is 15
SwitchGruppe9#
```

5.3 Local Fallback User (in case RADIUS is down)

To ensure administrative access is still possible if the RADIUS server is unreachable, a local fallback user account was configured on the switch. This user has privilege level 15 and can access the device via SSH.

What I Did:

- Created a local user with enable privileges:

```
SwitchGruppe9(config)#username fallbackadmin privilege 15 secret F@llb@ck2025
```

- Ensured the AAA login method falls back to local:

```
aaa authentication login SSH-LOGIN group MY-NPS-SERVERS local
```

- Confirmed that login still works if the RADIUS server becomes unavailable (e.g., shut down NPS or block traffic to 10.10.20.1).

Test Output:

```
$ ssh fallbackadmin@switch.lab -p 3005
Password:
SwitchGruppe9#
SwitchGruppe9#show privilege
Current privilege level is 15
SwitchGruppe9#
```

Kevin Lopci 2410410042

- Local login works
- User enters privileged EXEC mode automatically