NACVIEW

NACVIEW
SYSTEM MANAGMENT

Training for network administrators

NACVIEW

Table of contents

1. Introduction

The following training covers the basic functionalities of the NACVIEW system. It allows you to learn how to use the system interface and verify the correct operation of the configured services.

The training documentation contains all aspects that are necessary to implement a fully operational system in the organization to secure access to the internal network.

1.1. Description of the NACVIEW system

The NACVIEW system is a tool for the user and devices access management to the network. It allows you to control end devices and identities, that try to access network resources from both wired and wireless networks, as well as via VPN.

Access policies are created using a simple interface. All events are available in a graphical form, and this results in clarity and transparency in monitoring all activity of individual users and devices in the network.

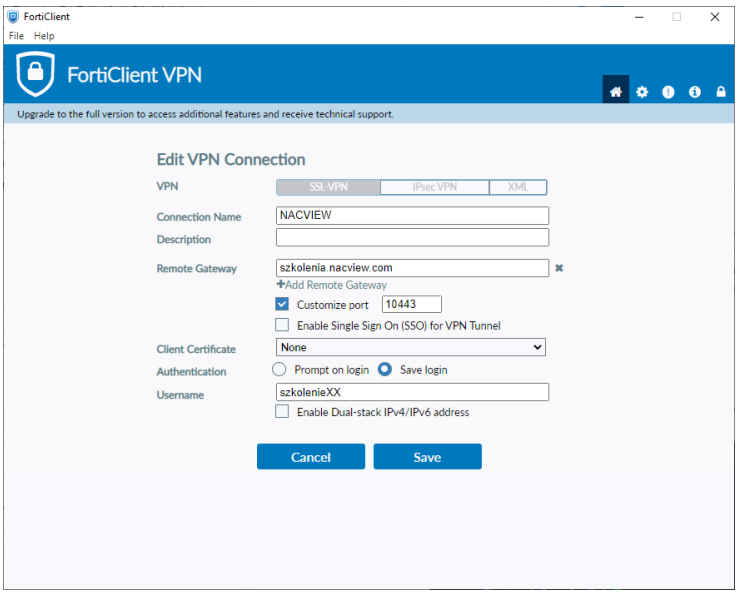
The NACVIEW system can be implemented in already existing networks, thanks to the possibility of integration with external systems (e.g. with AD or with its own PKI structure implemented). On the other hand, built-in servers (e.g. own CA server, DHCP server, internal user database, etc.) are a great solution for emerging networks where the network infrastructure still needs to be implemented.

Moreover, the NACVIEW system enables the management of network devices on which authorization is carried out. Thanks to this, the administration of the entire network infrastructure is possible within one platform.

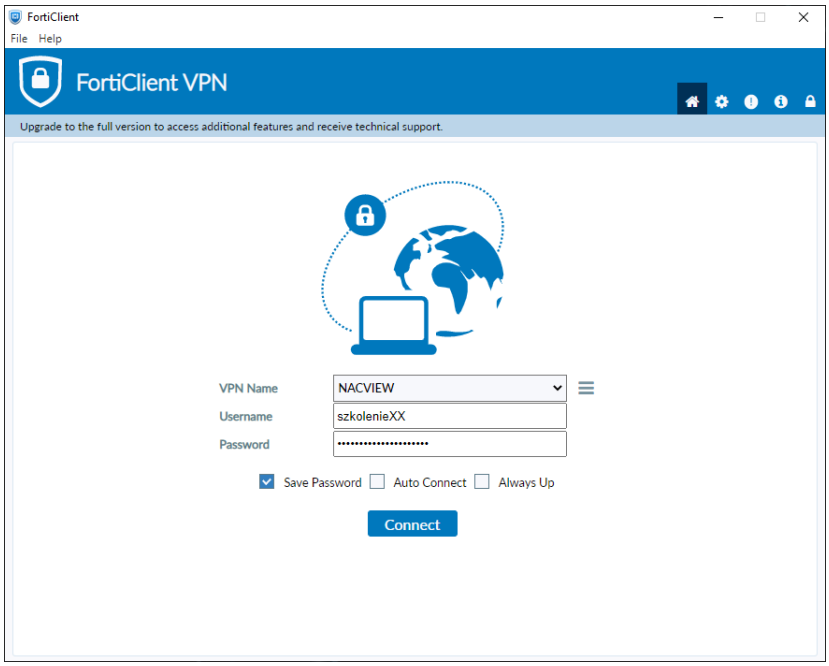
1.2. Installation

1.2.1. Remote connection to the training environment

Connect your computer via VPN connection to the NACVIEW training environment. Download **FortiClientVPNOnlineInstaller.exe** and install. Configure the credentials for the connection according to the received data (Note - in the *Username* field, enter the correct username for the given environment). A computer restart may be required for the program to work properly.



In the next step double-click the blue FortiClient icon in the tray, enter the password and start the connection with the ***Connect*** button.



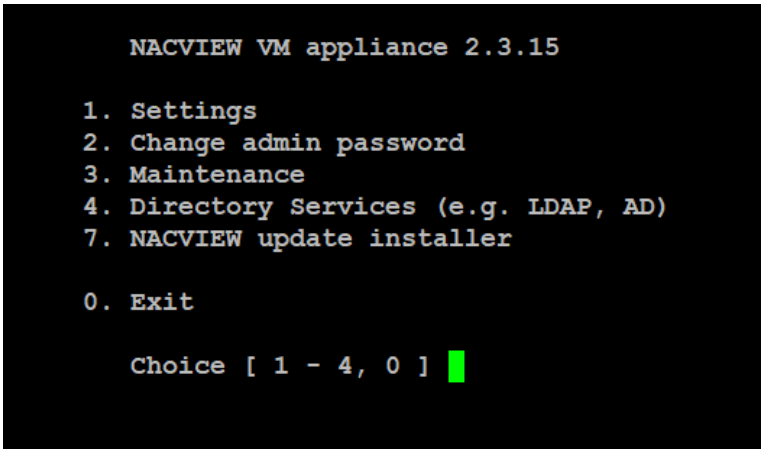
1.2.2. CLI installer

Launch a web browser and connect to PROXMOX (access data in table 1.4). Enter the address **https://10.XX.166.9:8006** (login: admin, password: NACVIEW_SZKOLENIE22). After logging into PROXMOX, go to the **XX-MS** host (NACVIEW system master). Then call up the console and log in to the system using the details below.

Default system login details:

- **Login**: admin
- **Password**: NACVIEW

The installer main menu should appear on the screen. Select the ***Settings*** option by entering the appropriate number from the menu:



Complete the displayed form with the following parameters:

- **Hostname**: master
- **IP address**: 10.XX.166.4
- **Netmask**: 24
- **IP default gateway**: 10.XX.166.1
- **Nameserver**: 10.XX.166.2
- **NTP addresses:** 10.XX.166.2 162.159.200.123
- **PROXY address**: (none)

Once the set parameters get confirmed with the ***Enter*** button, a summary will appear on the screen. If all the details are correct, enter '***y***' and confirm your answer again with the ***Enter*** button. Exit the installer by typing '***y***' and confirming with ***Enter***.

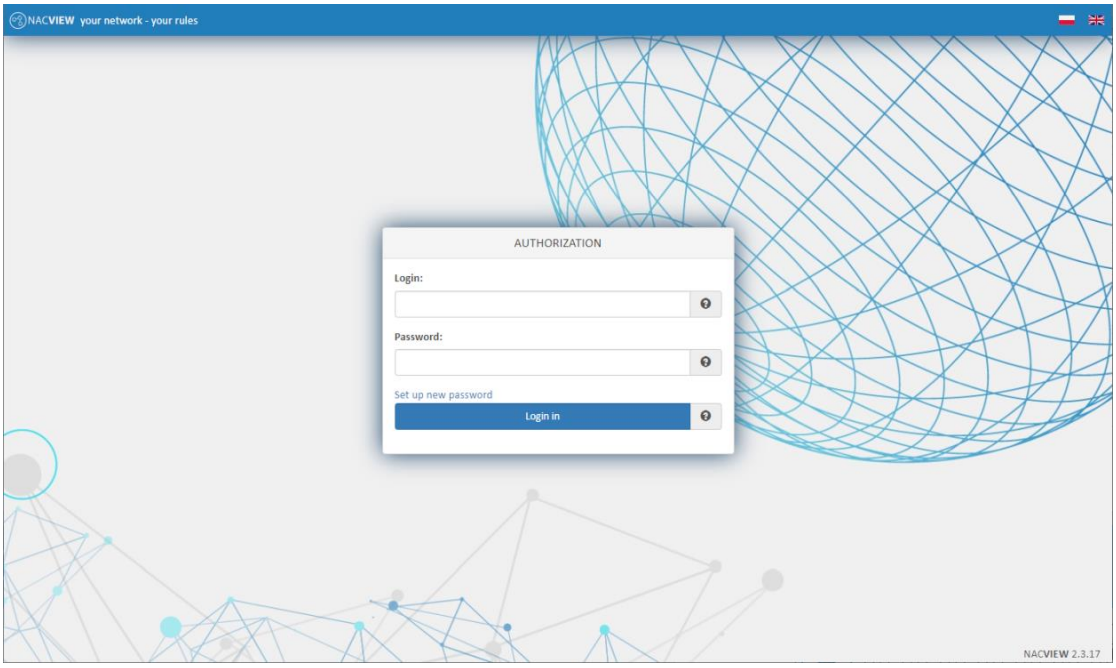
1.2.3. The web installer

After completing the installation process using the CLI installer, log in to the web installer and complete the system installation. To do this, use the IP address, administrative account login and password defined in the CLI configurator.

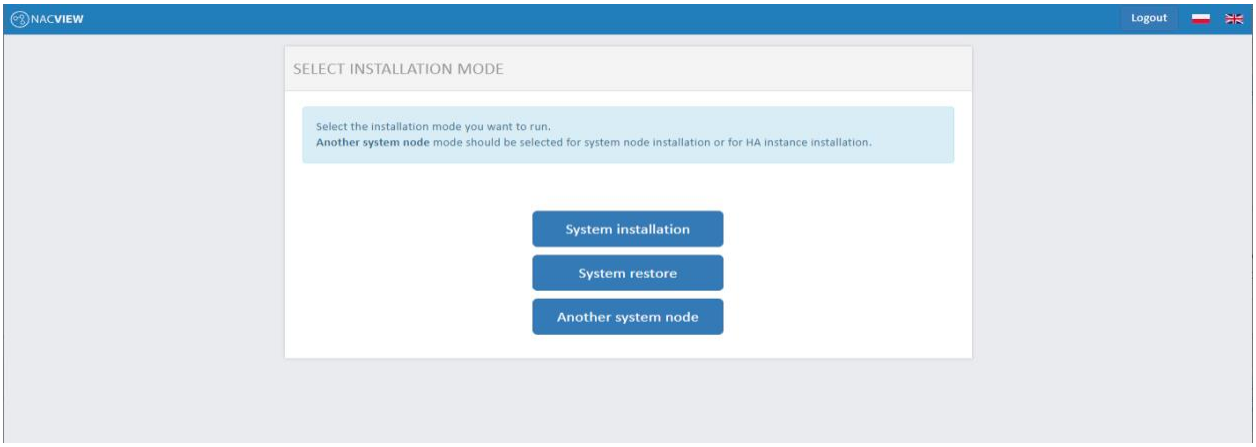
In the browser window, enter: **https://10.XX.166.4**

Default system login details:

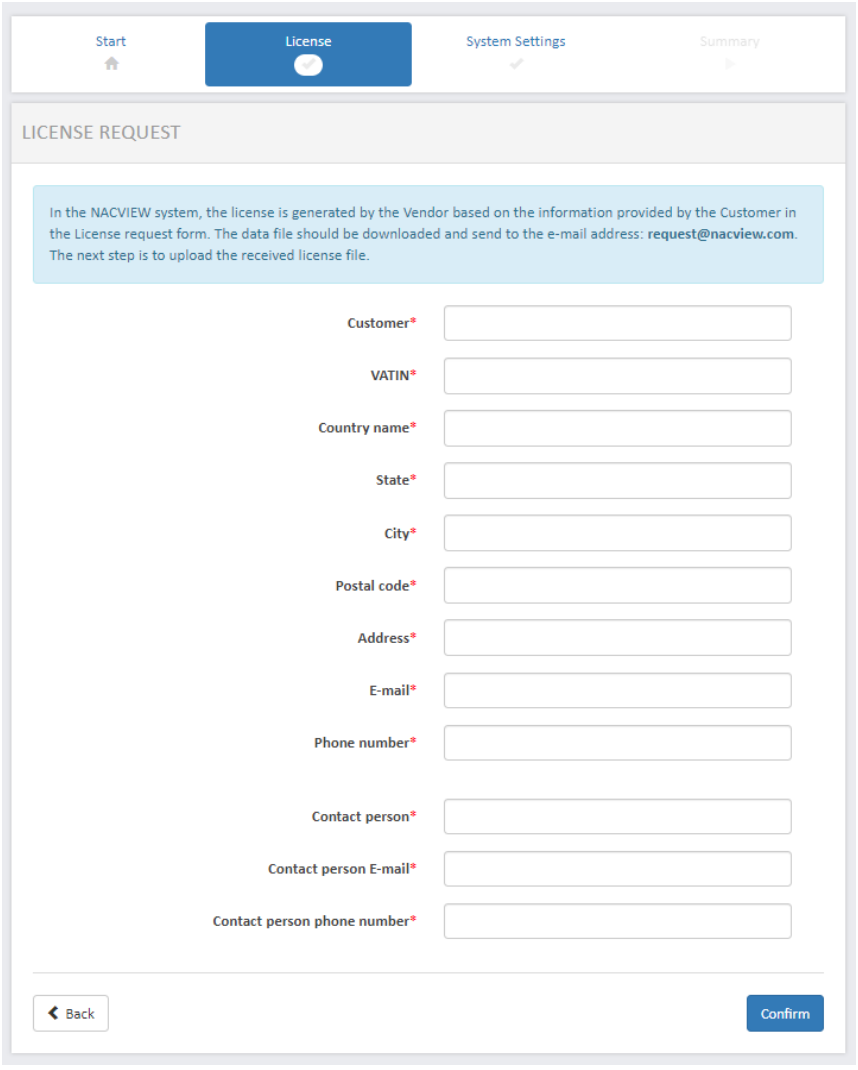
- **Login**: admin@nacview.com
- **Password**: NACVIEW



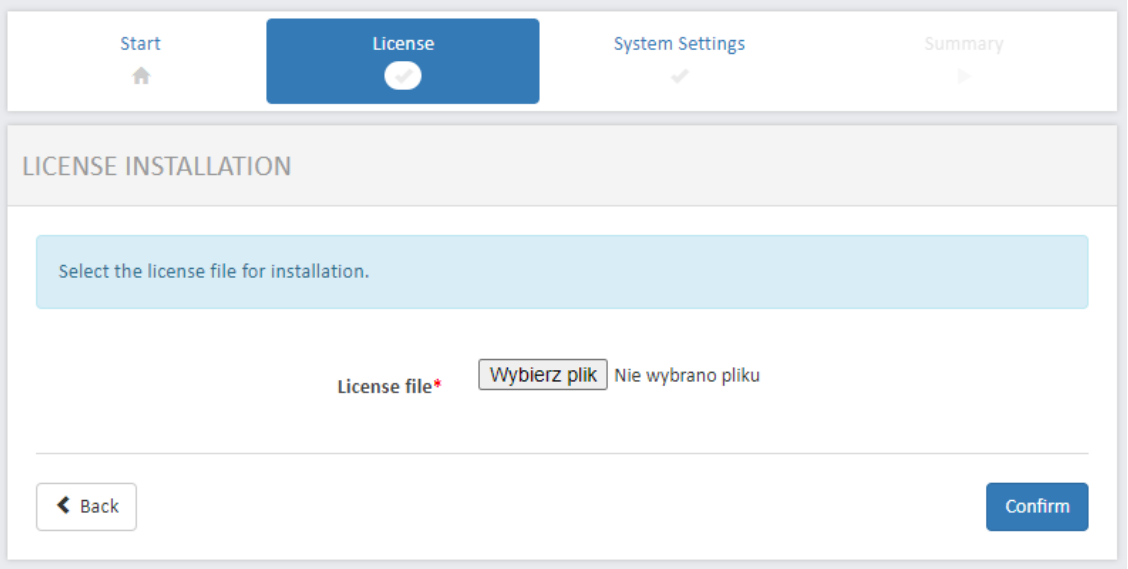
After logging in, this window with the web installer menu will appear. To go to the Web Installer, click ***System installation***.



Click the ***License*** button, then ***License Request***. Complete all fields of the displayed form and save the entered data. **Note - if you already have a license file (e.g. received for training purposes) - install it. Do not fill out the form below, just upload the received file as shown on the next page of the instruction.**

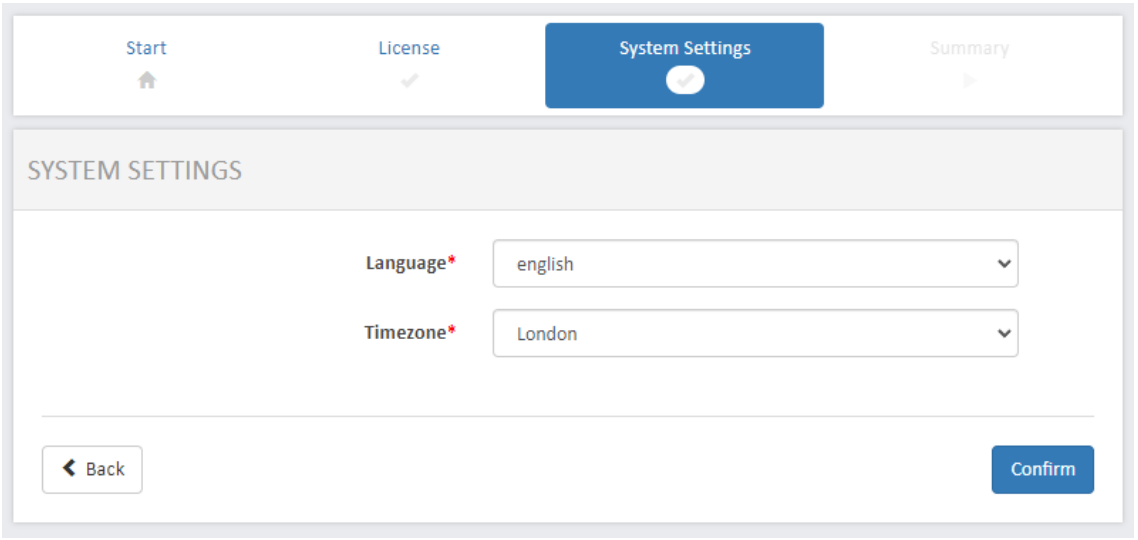


Download the completed form. Next, upload the license file to the system. To do this, click ***License installation*** and select the appropriate file from the disk:



Now click: ***Confirm***. After the license key has been correctly installed, the status: *configured* should appear next to the ***License installation*** button. Return to the ***System Installation*** window.

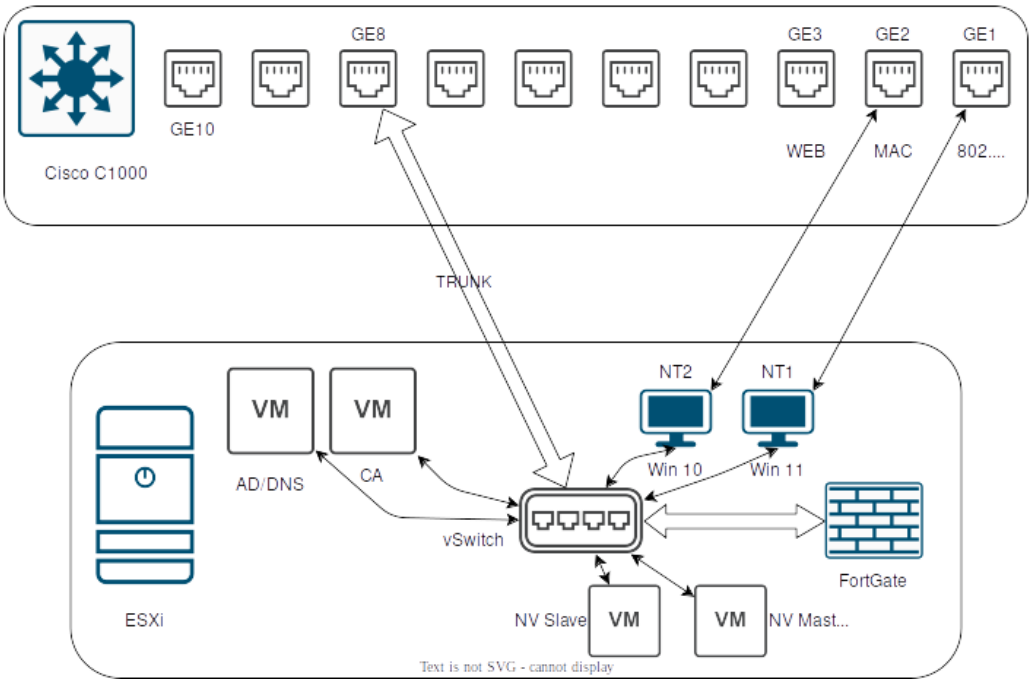
The last stage of configuration is the system settings. Here you can specify the default language of the NACVIEW system, and also you can select the time zone in which the system will operate.



After all setup steps get completed, the ***Summary*** button will get unlocked. The summary window will display the information configured in each step. If everything is correct, click ***Install***. The installation process may take approximately 10 minutes. Do not turn off the machine during your installation.

1.3. The connection structure of training environment

1.3.1. The diagram



1.3.2. Adressing

Nazwa	Adres IP
Cisco C1000 (Gateway)	10.XX.166.1
alpha.enterprise.test (AD / DNS, XX-DC)	10.XX.166.2
HA IP Address VRRP	10.XX.166.3
NACVIEW HA Master (XX-MS)	10.XX.166.4
NACVIEW HA Slave (XX-SL)	10.XX.166.5
beta.enterprise.test (XX-CA)	10.XX.166.6
PROXMOX virtualization server	10.XX.166.9:8006
FortiGate (XX-FTG)	10.XX.166.21
Resources	10.XX.166.1/24
Authorization I	10.XX.80.1/24
Authorization II	10.XX.88.1/24
Authorization V	10.XX.126.1/24
CP L2	10.XX.96.1/24
CP L3	10.XX.104.1/24
Guest Network	10.XX.120.1/24

1.4. The access data

Name	User	Password	IP Address	RADIUS Secret	SNMPv2	TACACS+ Secret
NACVIEW WEB LOGIN	admin@nacview.com	NACVIEW	10.XX.166.3	-	-	-
NACVIEW SSH LOGIN	admin	NACVIEW	10.XX.166.3	-	-	-
Domain Controller: ENTERPRISE	administrator@ enterprise.test	NACVIEW_ SZKOLENIE 22	10.XX.166.2	-	-	-
Network Device: (Cisco C1000, FortiGate)	admin	NACVIEW_ SZKOLENIE 22	10.XX.166.1	NACVIEW_ SZKOLENIE 22	NVPrivate	NACVIEW_ SZKOLENIE 22
Test User (OU Reserach and Development)	ENTERPRISE\ TesterR&D	NACVIEW_ SZKOLENIE 22	-	-	-	-
Test User (OU NetworkOperations)	ENTERPRISE\ TesterNO	NACVIEW_ SZKOLENIE 22	-	-	-	-
Test User (Accounting Group)	ENTERPRISE\ AccountantOne	NACVIEW_ SZKOLENIE 22	-	-	-	-
Hypervisor PROXMOX	admin	NACVIEW_ SZKOLENIE 22	10.XX.166.9:8006	-	NVPrivate	-

2. Wizards

2.1. External certificate

Click on the ***Wizards*** button  (top bar of the screen). From the expanded list of wizards, select ***CA Certification Authority***, and then click button: ***Create New***. In the next window, select: ***External CA CSR***.

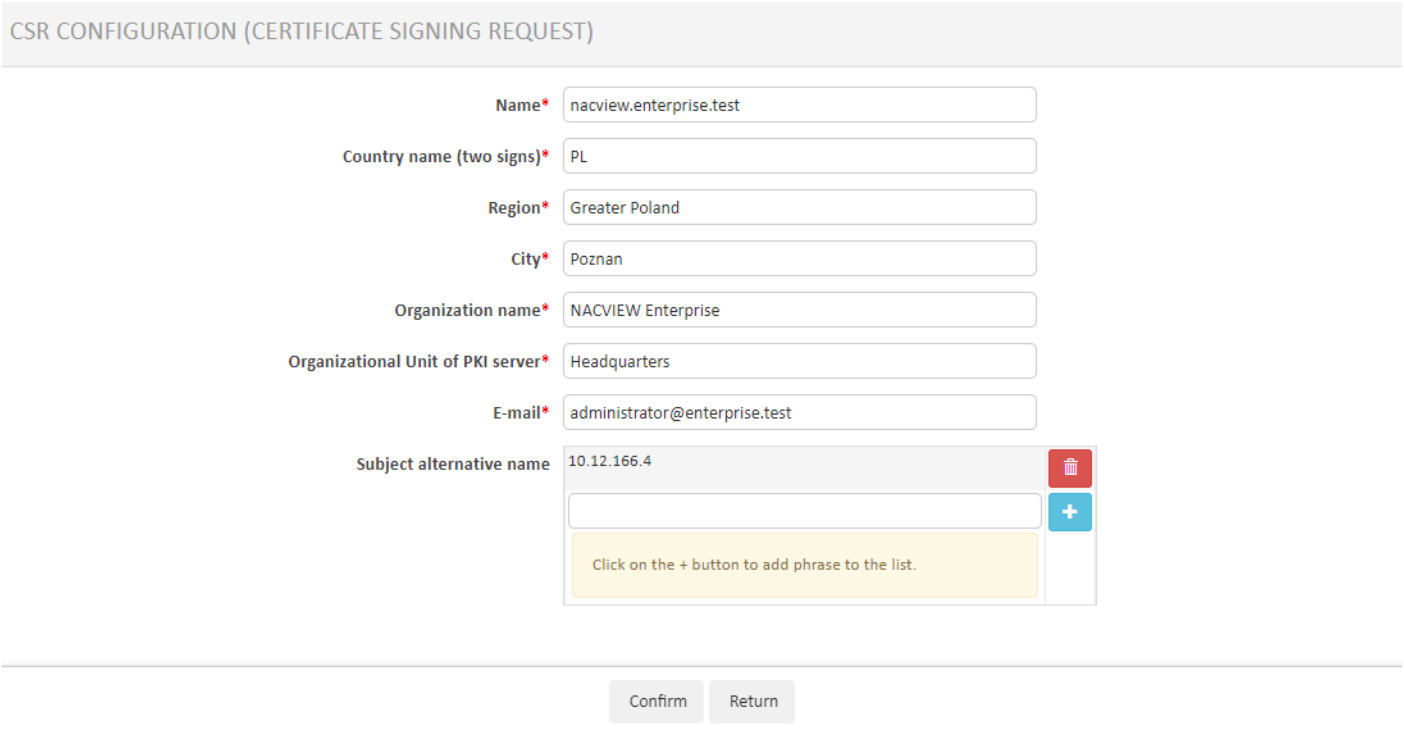
Click ***Edit configuration*** and fill out the form with the following details:

- **Active:** Yes
- **Is it default:** No
- **Active for objects:** No
- **Used for WWW:** No
- **Is OCSP active**: No
- **Is SCEP active:** No
- **URL for CRL:** http://beta.enterprise.test/CertEnroll/enterprise-BETA-CA.crl

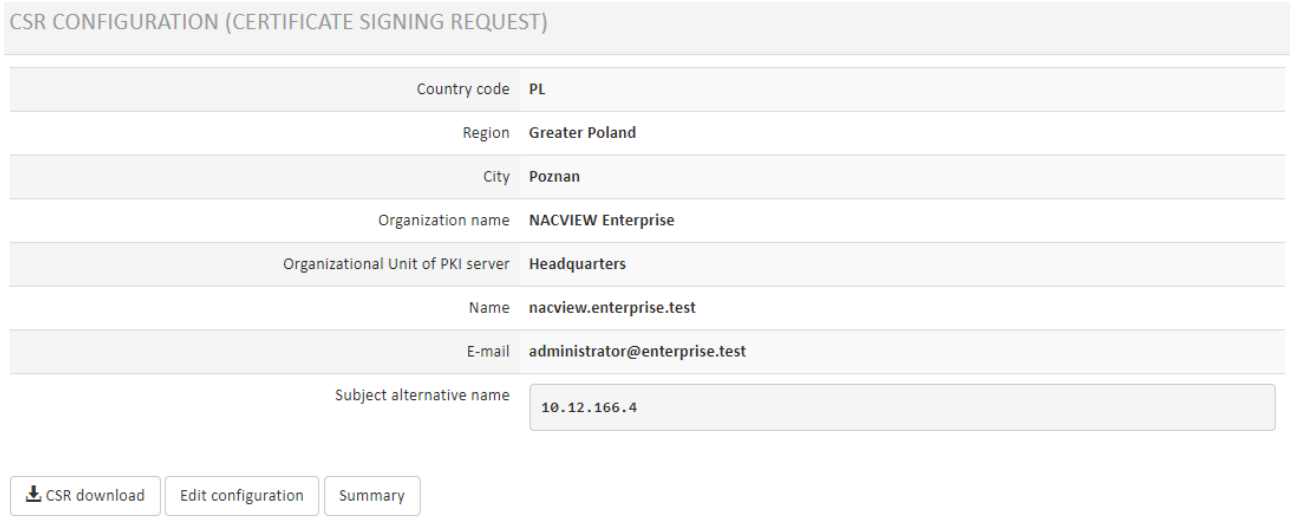
Now save your settings.

<u>After the certificate file gets imported, the colour of the frame will change to green and information about the uploaded file will get displayed.</u>

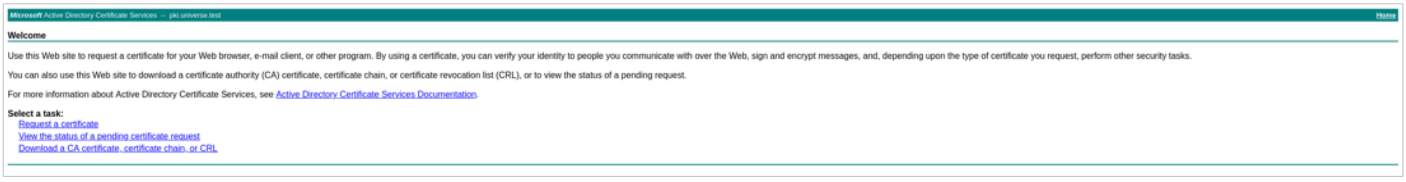
Now start from the setting up certificate signing request (click the last button in the red marked list):



Click now ***Confirm*** (at the bottom of the screen). Your next step is to sign CSR. To do this, download the CSR using the ***CSR Download*** button.



Then go to http://beta.enterprise.test/certsrv (http://10.XX.166.6/certsrv) and select: *Request a certificate*. If the website requires login details, enter login: ENTERPRISE\Administrator and password: NACVIEW_SZKOLENIE22



Among the displayed options select: *submit an advanced certificate request*.

Paste the content of the downloaded CSR into the *Saved request* - it can be opened, for example, using the Notepad++ tool. Next, from the list of accessible certificates, select: *Web server* and save it with the *Submit* button. The obtained certificate should be downloaded in the *Base64* format.

Exit the certificate request window with the *Summary* button. You can obtain a CA certificate by going to: http://beta.enterprise.test/certsrv (http://10.XX.166.6/certsrv) and select:

Download a CA certificate, certificate chain, or CRL. And next, select the certification authority (*pki.enterprise.test*) and *Base64* encoding. Download the certificate using the *Download CA certificate* button. Then add the appropriate files to the system (at the bottom of the window) by the following paths:

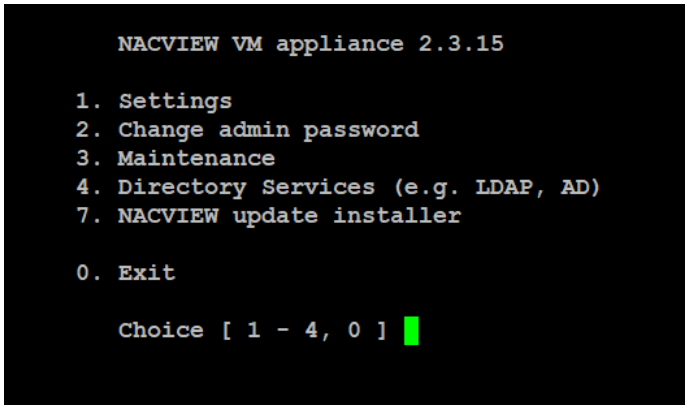
Server certificate → *Select file* → *Upload files* → *Summary*

CA Certificate chain → *Select file* → *Upload files* → *Summary*

After all the files have got successfully uploaded, the *Confirm configuration* button should appear at the bottom of the window. Press it to install the files. The system will set the required parameters within 5 minutes.

In order to complete your changes, go back to the ***CA Certification Authorities*** wizard and click: ***Install Configurations*** in the upper right corner. In the newly opened window, press: ***Apply configurations***. Wait about 10 minutes for the changes to take effect.

2.2. HA cluster



Now go to the second NACVIEW node (**XX-SL** machine). Verify that the network interfaces are connected to the appropriate networks: Resources, CPL2, and SPAN.

Then log into the console. Select the ***Settings*** option by entering the appropriate number from the menu.

Complete the displayed form with the following parameters::

- **Hostname**: slave
- **IP address**: 10.XX.166.5
- **Netmask**: 24
- **IP default gateway**: 10.XX.166.1
- **Nameserver**: 10.XX.166.2
- **NTP addresses**: 10.XX.166.2 162.159.200.123
- **PROXY address**: (none)

After you get your set parameters confirmed with ***Enter***, the summary will appear on the screen. If all the details are correct, enter 'y' and confirm your answer again with the ***Enter*** button. Exit the installer by typing 'y' and confirming with ***Enter***.

Now go to the NACVIEW system. From the list of wizards, select ***HA Cluster***. Go to editing and add the configuration for the Slave node. To do this, click button ***Create new*** and complete the form with the following data:

- **IP address:** 10.XX.166.5
- **Node type:** HA
- **Login:** admin
- **Password:** NACVIEW
- **Timezone:** Warsaw
- **DNS IP:** 10.XX.166.2
- **VRRP IP address:** 10.XX.166.3
- **VRRP subnetwork prefix:** 24

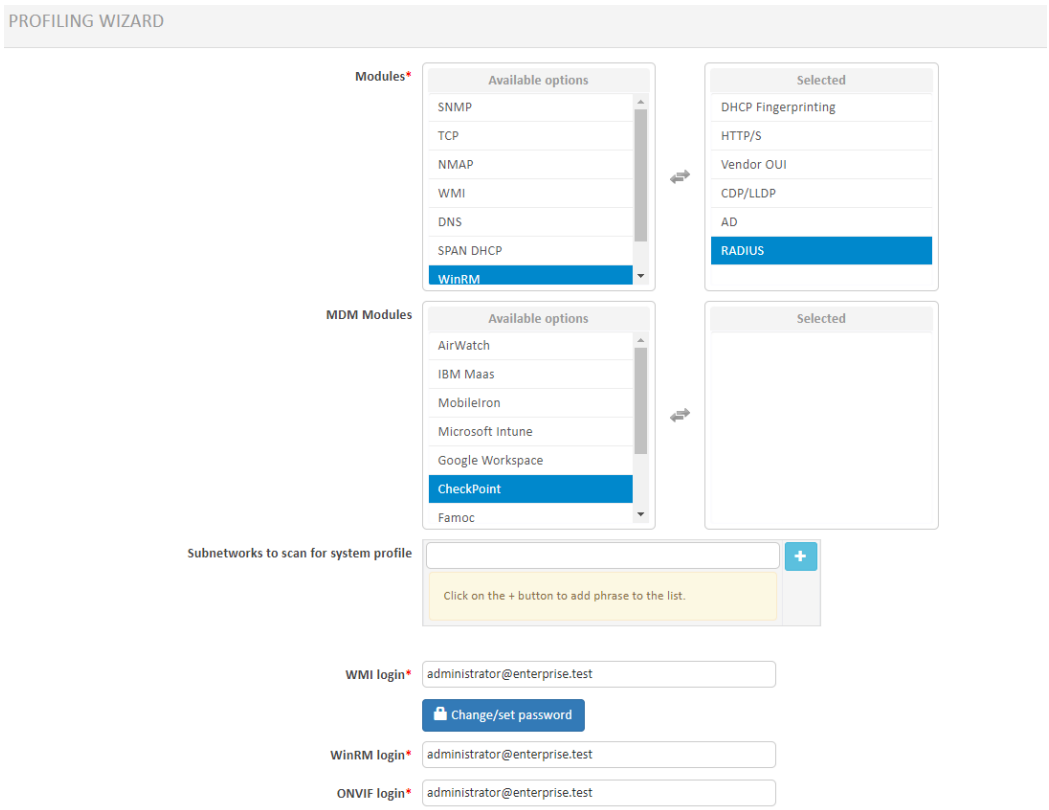
Save your set values. To upload changes to the system, press the ***Apply configuration*** button. The system will set the required parameters within 10 minutes.

2.3. The system profile

From the wizards list, select ***Profiling.*** Now go to editing. Complete the form. To the ***List of modules*** add: ***RADIUS***, ***AD***, ***CDP/LLDP***, ***VENDOR OUI***, ***DHCP Fingerprinting*** and also ***HTTP/S***.

Now complete the remaining fields:

- **WMI login:** administrator@enterprise.test (set also in: **WinRM login** and **ONVIF login**)
- **SNMP secret**: NVPrivate
- **WMI password:** NACVIEW_SZKOLENIE22



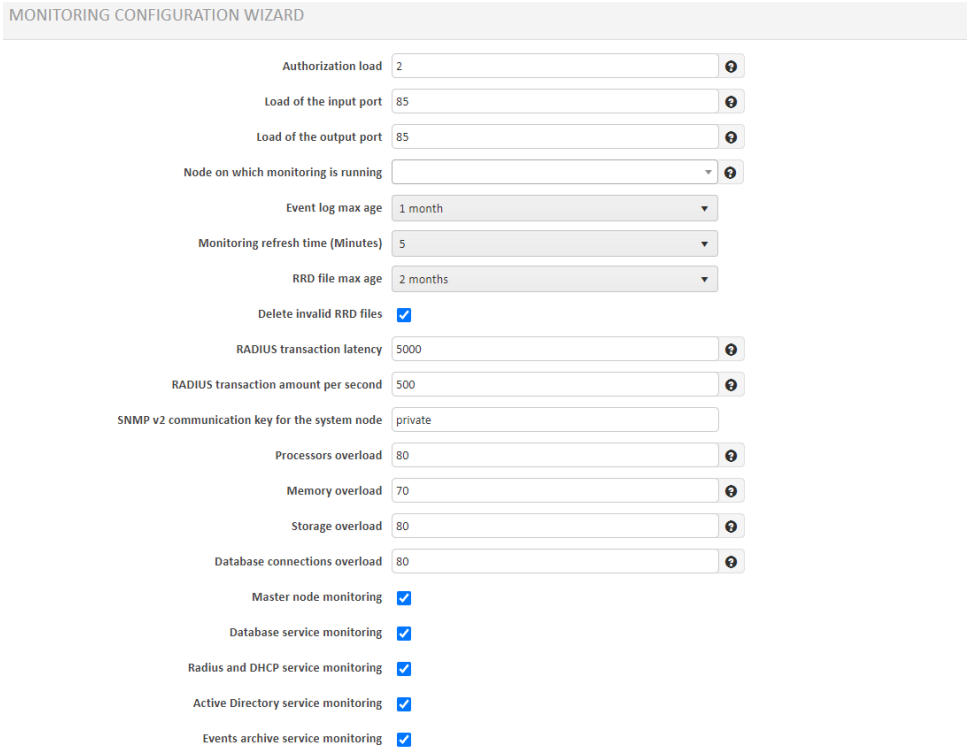
Save your set values. To upload changes to the system, press the ***Apply configuration*** button. The system will set your required parameters within 10 minutes.

2.4. Monitoring settings

From the wizards list select ***Monitoring***. Now go to editing. Complete the form with parameters related to the port overload:

- **Authorization load:** 2
- **Load of the input port:** 85
- **Load of the output port:** 85
- **Monitoring refresh time**: 5
- **Master node monitoring:** Yes
- **Database service monitoring:** Yes
- **Radius and DHCP service monitoring** : Yes
- **Events archive service monitoring:** Yes

  Set the other values as shown in the picture below.



Save the set values. To upload changes to the system, press the ***Apply configuration*** button. The system will set the required parameters within 10 minutes.

2.5. Active Directory

2.5.1. Active Directory configuration

From the list of wizards, select LDAP/AD Directory Services. Click ***Create new*** . Complete the form by providing the data according to the table below:

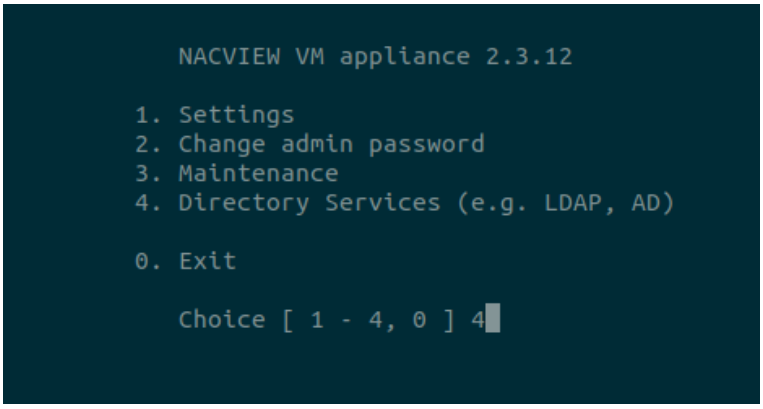
Field	Value
Name	Enterprise
Active	Yes
Is default	Yes
Is default for VPN	No
Is default for OTP	No
NetBIOS name	ENTERPRISE
DNS domain name	enterprise.test
Domain names or IP of AD servers	alpha.enterprise.test
DNS IP	10.XX.166.2
Allow LDAP referrals	Yes
Is exclude id in hostname	No
PKI CA	pki.enterprise.test

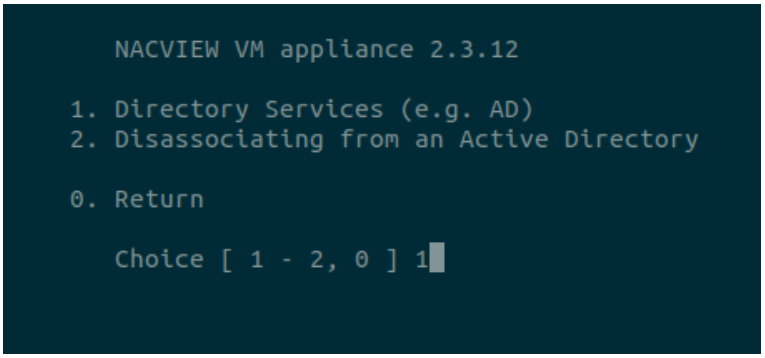
Save your set values. To upload changes to the system, press the ***Install configuration*** button. The system will set the required parameters within 5 minutes.

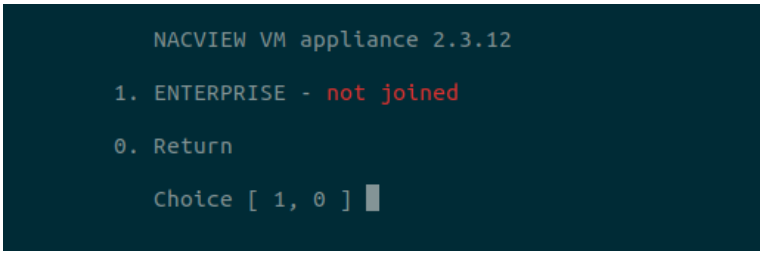
2.5.2. The Command line (CLI/SSH)

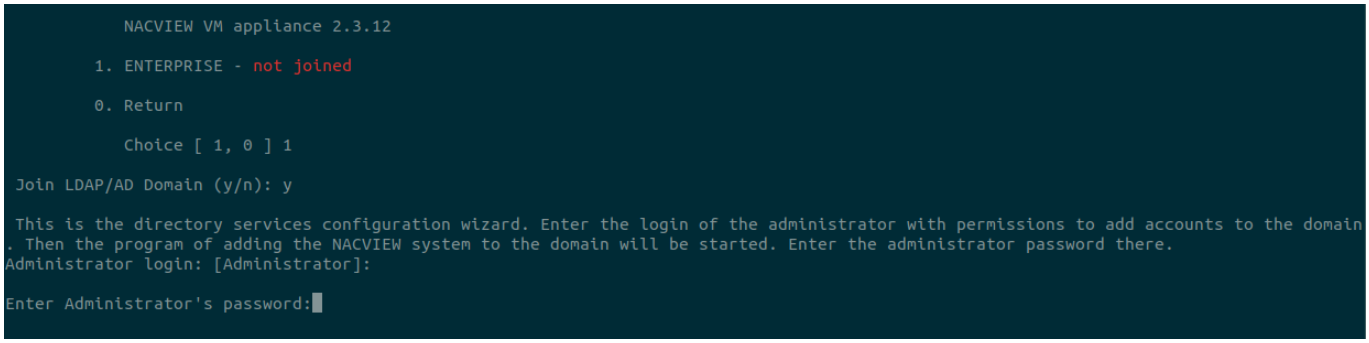
Open the **XX-MS** machine's command line. As the admin user (password: **NACVIEW**), select Directory Services (e.g. *LDAP*, *AD*), then Directory Services (e.g. AD), and finally the appropriate domain (**ENTERPRISE**). Start the service by providing the credentials to add the system to AD: umożliwiające dodanie systemu do AD:

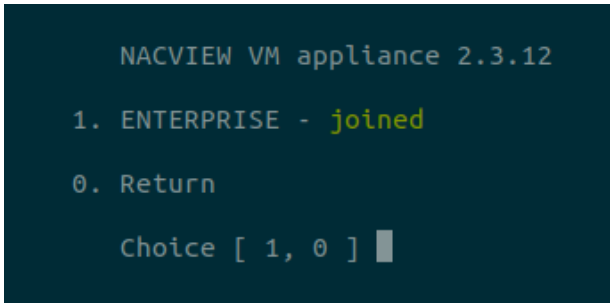
- **Login**: Administrator
- **Hasło**: NACVIEW_SZKOLENIE22











Bare in mind that you need to check if the node configuration needs its update on the master server, **then repeat the same steps for the second node** (slave). Machine **XX-SL**.

3. Administration

3.1. SMTP configuration

From the list of wizards, select the ***SMTP*** option and proceed to editing the form. Complete it with the following data:

- **Sender's name**: NACVIEW System
- **Sender's e-mail**: szkolenie22@nacview.com
- **Connection protocol**: SMTP
- **Mail server**: poczta.nacview.com
- **Username**: szkolenie22@nacview.com
- **Password**: Nv_SZKOLENIE22
- **Authorization type**: login
- **Connection port**: 587
- **Encryption**: TLS

Save your set values. To upload changes to the system, press the ***Install configuration*** button. The system will set the required parameters within 5 minutes.

3.2. System configuration

From the main menu, select ***System configuration*** (***Administration*** section). In the Basic configuration section on top, click ***Edit***. Complete the form with the following data:

- **Default Identity prefix**: user_
- **DNS primary server:** 10.XX.166.2
- **Notifications for administrators:** admin@nacview.com
- **Sending notifications:** month before
- **Default interval for events history search:** 1 week
- **DHCP events retention time**: 2 years (you will find in section below: + Events retention time)

Now save your set values.

3.3. Admin accounts

From the main menu, select ***Administrator Accounts*** (***Administration*** section). Click ***Create new*** to create a new account. Complete the form with data for account 1 from the table below. Save your settings. Now do the same for accounts number 2 and 3 from the table:

Administration Account	1	2	3
Authorization server	Local database	Local database	Local database
Login	sekretariat	audyt	netAdmin
Password	NACVIEW2022	AUDYT2022	NVNET2022
Name	Konto	Konto	Konto
Surname	Sekretariatu	Audytoryjne	NOC
E-mail	sekretariat@enterprise.test	audyt@enterprise.test	noc@enterprise.test

3.4. Admin groups

From the menu select ***Administration groups*** (***Administration*** section). Click ***Create new***. Complete the form with data for account 1 from the table below. Save the settings. Repeat for accounts number 2 and 3 in the table:

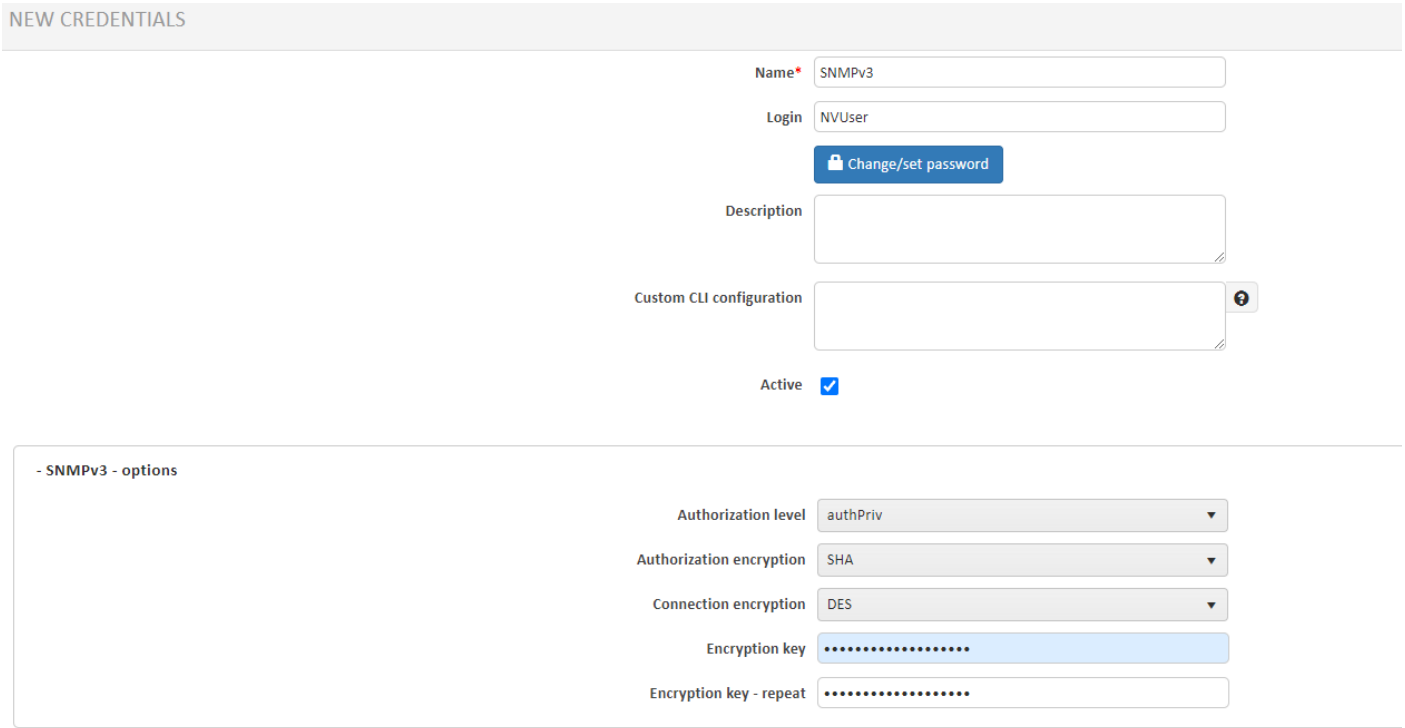
Administration Group	1	2	3
Name	Sekretariat	Audyt	NOC
Roles	Voucher accounts creating Voucher accounts deleting Voucher accounts displaying Voucher accounts editing Voucher accounts preview window access Standard Identities creating Standard Identities deleting Standard Identities displaying Standard Identities editing Notifications admin	Notification admin Audit of administrators admin	Notifications admin IPv4 addresses admin Network devices admin Ports admin Subnetworks admin VLANs admin WiFi networks admin MAC addresses admin Administrator accounts admin Administration groups admin System events access DHCP events access Authorization events access Activity access
Administrator accounts	sekretariat@enterprise.test	audyt@enterprise.test	noc@enterprise.test
Detailed permissions	Identities: • Create • Preview • Edit • List Endpoints • Preview • List		

After you have set the above-mentioned roles for administration groups, log out of the NACVIEW administration panel and log in to individual accounts in order to verify permissions.

3.5. Device credentials

From the main menu, select ***Device credentials*** (***Administration*** section). Click ***Create new*** and complete the form with credentials 1 from the table below. Save your set values. Now repeat steps for credential 2, 3 and 4.

Credentials	1	2	3	4
Name	SNMPv2	SNMPv3	cisco-SSH	SSH
Login	private	NVUser	admin	admin
Password	NVPrivate	NACVIEW_SZKOLENIE22	NACVIEW_SZKOLENIE22	NACVIEW_SZKOLENIE22
Custom CLI configuration			-oKexAlgorithms=diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1 -o HostKeyAlgorithms=ssh-rsa	
SNMPv3 - options		Authorization level: AuthPriv, Authorization encryption: SHA, Connection encryption: DES, Encryption key: NACVIEW_SZKOLENIE22		



3.6. Object groups

From the main menu, select ***Object groups*** (***Administration*** section). Click ***Create new***. Complete the form by entering the names in turn:

- *Computers,*
- *Employees,*
- *Accounting,*
- *Managers,*
- *Junior Network Engineers,*
- *Senior Network Engineers,*
- *MAC addresses,*
- *Printers,*
- *Network devices,*
- *VoIP Phones.*

4. The network

4.1. Subnets

4.1.1. Subnets adding

From the main menu select ***Network IPv4*** (***Network*** section). Click ***Create new*** and complete the form with subnet 1 details from the table below. Save the set values. Repeat the same for 2-7 subnets.

Subnet	1	2	3	4
Name	NET_166	NET_80	NET_88	NET_126
Name displayed on subnets map	10.XX.166.0/24	10.XX.80.0/24	10.XX.88.0/24	10.XX.126.0/24
Network address	10.XX.166.0	10.XX.80.0	10.XX.88.0	10.XX.126.0
Subnets mask	24	24	24	24
DHCP enabled	No	Yes	Yes	Yes

Subnet	5	6	7
Name	NET_96	NET_104	NET_120
Name displayed on subnets map	10.XX.96.0/24	10.XX.104.0/24	10.XX.120.0/24
Network address	10.XX.96.0	10.XX.104.0	10.XX.120.0
Subnets mask	24	24	24
DHCP enabled	Yes	Yes	Yes

4.1.2. DHCP configuration

In the list of subnets find: 10.XX.80.0/24. Now click on the row  (in which it is) and select ***Edit***. Expand the form by clicking ***+DHCP*** (in the lower left corner):

- **DHCP enabled:** Yes
- **Lease time:** 1800
- **Monitoring DHCP:** Yes
- **DHCP usage warning level:** 85
- **DHCP decline warning level**: 5
- **Link endpoint with identity:** No

Save your set values. After you got your changes saved, the DHCP server is already operational.

Open the subnet view window by clicking on  . Press  and select: ***DHCP options.*** Click: ***Add*** and complete the form fields as follow:

- **Parameter key**: DHCP-Name-Service-Search
- **Value**: enterprise.test
- **Key to parameter connector**: =
- **Active**: Yes

Now save your set values.

In the next step, find in the list of subnets: 10.XX.96.0/24. Click on  (the row where it is in) and then select ***Edit***. Expand the form by clicking ***+DHCP*** (in the lower left corner).

Please be mindful that here you need to set the DHCP **Lease time** to a very short one, eg 30. Network 10.XX.96.0/24 is the network for Captive Portal connection.

4.1.3. IP addresses allocation

From the main menu, select ***IPv4 addresses*** (the ***Network*** section). Select the addresses: from 10.XX.80.10 to 10.XX.80.20 (from the subnet 10.XX.80.0/24), click on ***Group actions*** and select ***Make static assignment***. Repeat this for all other networks running DHCP.

4.2. VLAN

Select VLANs from the main menu. Click ***Create new*** and complete the form by entering VLAN 1 data from the table below. Save your set values. Repeat this for VLANS: 2 - 7.

VLAN	1	2	3	4	5	6	7
Name	Authorization I	Authorization II	Authorization V	CP L2	CP L3	Guest Network	Resources
Tag	80	88	126	96	104	120	166
Color identifier	Any value	Any value	Any value	Any value	Any value	Any value	Any value
Subnetworks	NET_80	NET_88	NET_126	NET_96	NET_104	NET_120	NET_166

4.3. Network devices

4.3.1. Cisco C1000 switch

Configure your network device. To do this, log in to the C1000 using the SSH client as admin, specifying IP: 10.XX.166.1.

- SNMPv3

```
configure terminal
snmp-server enable traps
snmp-server group NVGroup v3 priv context vlan- match prefix
snmp-server group NVGroup v3 priv write v1default
snmp-server ifindex persist
snmp-server trap-source vlan 166
snmp-server source-interface informs vlan 166
snmp-server source-interface traps vlan 166
snmp-server user NVUser NVGroup v3 auth sha NACVIEW_SZKOLENIE22 priv des NACVIEW_SZKOLENIE22
snmp-server host 10.XX.166.3 inform version 3 priv NVUser
snmp-server host 10.XX.166.3 traps version 3 priv NVUser
```

- RADIUS

```
configure terminal
aaa new-model
radius-server vsa send authentication
radius-server vsa send accounting
aaa group server radius NVRadius
server-private 10.XX.166.3 auth-port 1812 acct-port 1813 key NACVIEW_SZKOLENIE22
ip radius source-interface vlan 166
exit
aaa authentication dot1x default group NVRadius
aaa accounting dot1x default start-stop group NVRadius
aaa authorization network default group NVRadius
dot1x system-auth-control
```

- Change of Authority (CoA)

```
configure terminal
aaa server radius dynamic-author
client 10.XX.166.3 server-key NACVIEW_SZKOLENIE22
port 3799
```

- SYSLOG

```
configure terminal
logging host 10.XX.166.3
logging source-interface vlan 166
logging on
```

- Port configuration - 802.1x + MAC

```
configure terminal
interface gigabitEthernet 1/0/1
spanning-tree portfast edge
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode single-host
authentication periodic
authentication violation replace
mab eap
authentication order dot1x mab
authentication priority dot1x mab
```

- Port configuration - MAC - CPL2

```
configure terminal
interface gigabitEthernet 1/0/2
spanning-tree portfast edge
switchport mode access
authentication port-control auto
authentication host-mode multi-auth
authentication periodic
authentication violation shutdown
mab eap
authentication order mab
authentication priority mab
```

Then return to the NACVIEW user panel and add the configured device. To do this, select ***Network devices*** from the menu. Now click ***Create new*** and complete the form by entering the device data from the table below:

Network Device	Value
Device model	Network device
Number of ports	10
Name	Cisco C1000
IP address	10.XX.166.1
Device software	Cisco IOS
Object groups	Network devices

Save your set values. The ***Credential Settings*** window should appear. Click  on the line with the SSH protocol and select ***Edit***.

Now complete the form with the following data:

- **Connection protocol**: SSH
- **Login and password**: cisco-SSH admin

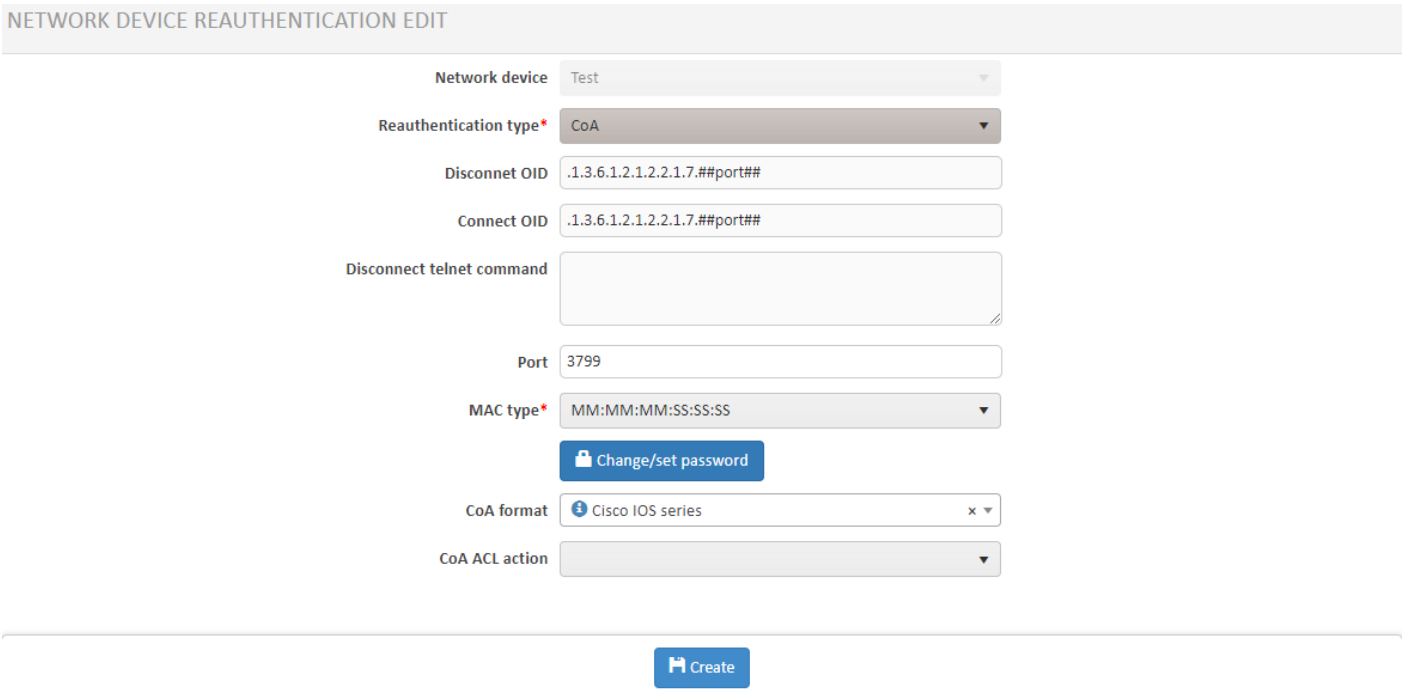
Save it now. Repeat the same for SNMP with these details:

- **Connection protocol**: SNMPv3
- **Login and password**: SNMPv3 NVUser

Go ***Next*** and click ***Monitoring***. A table with monitoring configuration data will appear in the displayed window. Click ***Save*** to confirm , then close the window.

Data from the device will get collected after a maximum of 10 minutes, and when this happens - click the ***Edit ports names*** button. Complete the displayed form and save the set values.

In order to set the session disconnection mechanism, click the ***Reathentication edit*** button. Select the type of CoA disconnection, port 3799, MAC format separated by a colon, enter the password **NACVIEW_SZKOLENIE22**, select the CoA format: Cisco iOS series and save your set values.



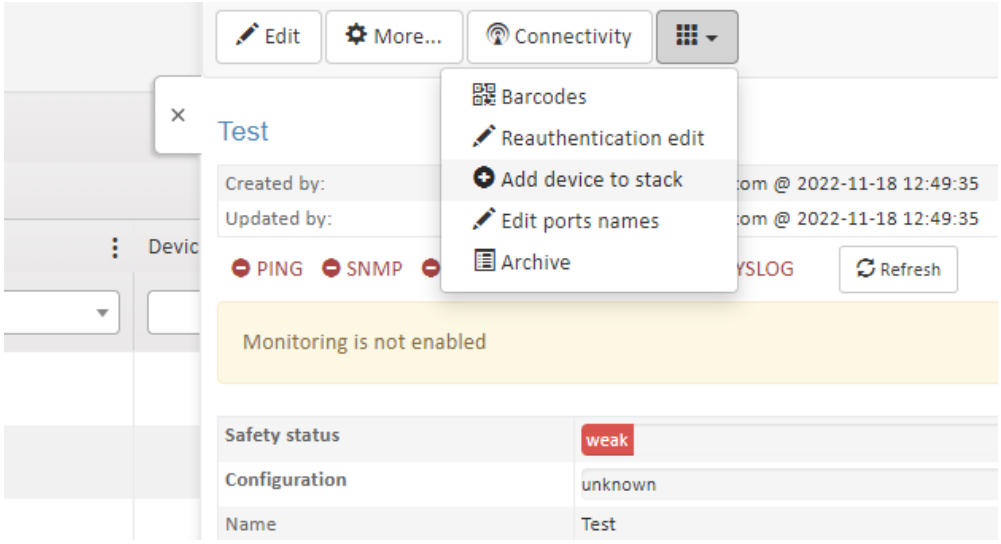
Now you need to change the default Radius password that was generated for communication between the NACVIEW system and the network device. To do this, enter the edition of the added device (> ***Edit***), click: ***Change/set password*** and complete the ***Key for communication RADIUS*** field - in accordance with the data at 1.4. point (NACVIEW_SZKOLENIE22). Save the changes now and return to the list.

4.4. Network devices - stack

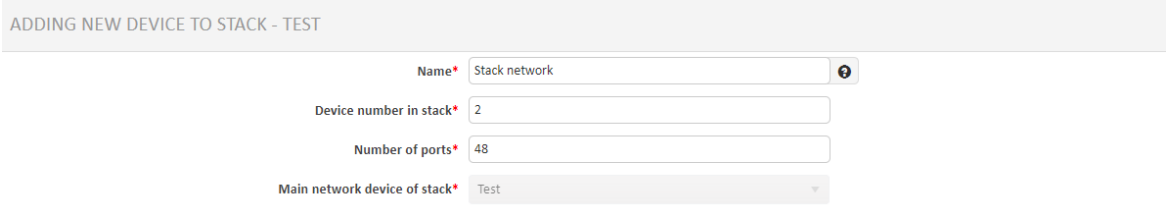
To add switches in a stack, you must first add and configure the root network device. To do this, go to ***Network devices > Create new***. Complete the data:

- **Device model**: Network device
- **Name**: Stack network
- **Port number**: 48
- **IP address**: 10.XX.166.19

Save all your set values. Find the newly created switch in the list (it should be at the end of the list by default). Open the preview by clicking: in the row of your switch. In the window that opens on the right, select the ***Add device to stack*** option from the drop-down menu:



In the form: select 2 as the device number in the stack and enter 48 as the number of ports. ***Save*** your settings. Repeat for the third device in the 24-port stack:



4.5. Wi-Fi

From the main menu, select ***WiFi networks*** (***Network*** section). Click ***Create new*** and complete the form by entering network 1 data from the table below. Save your set values. Return to the list and repeat the steps for network 2:

WiFi Network	1	2
Name	WiFi_EAP	WiFi_MAC
Network SSID	NACVIEW_22_EAP	NACVIEW_22_MAC

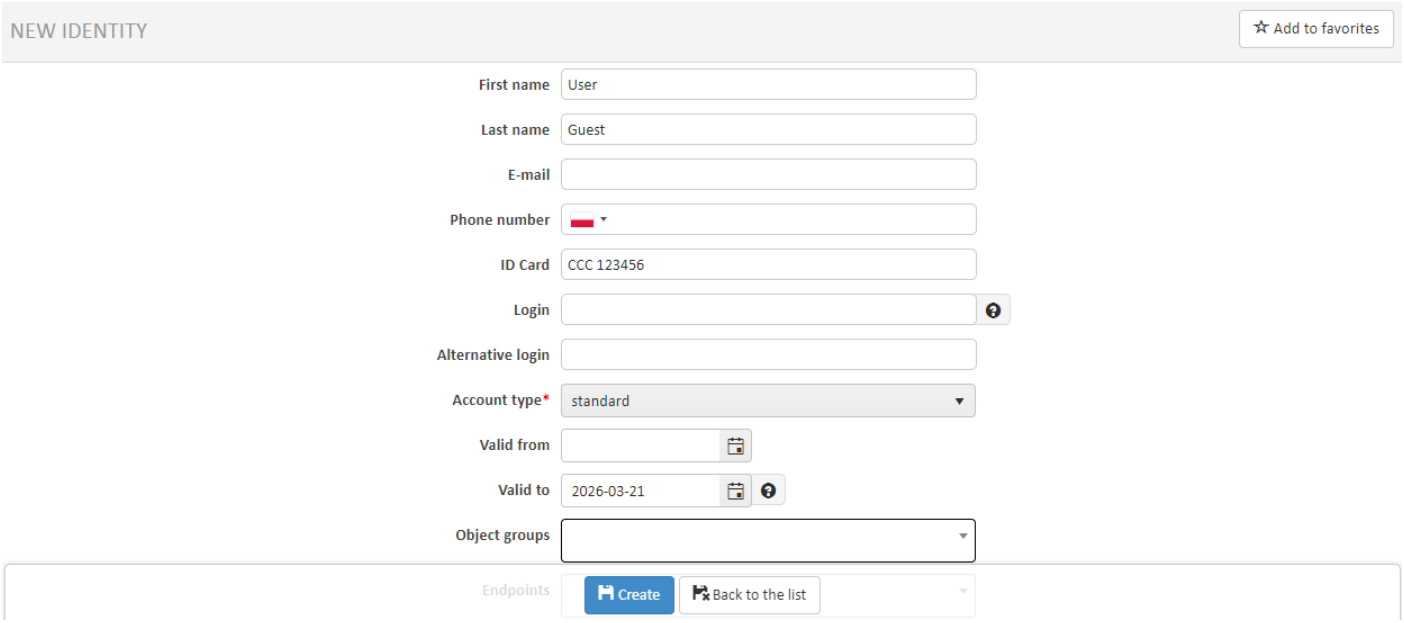
5. Objects

5.1. Identities

5.1.1. Identities creation

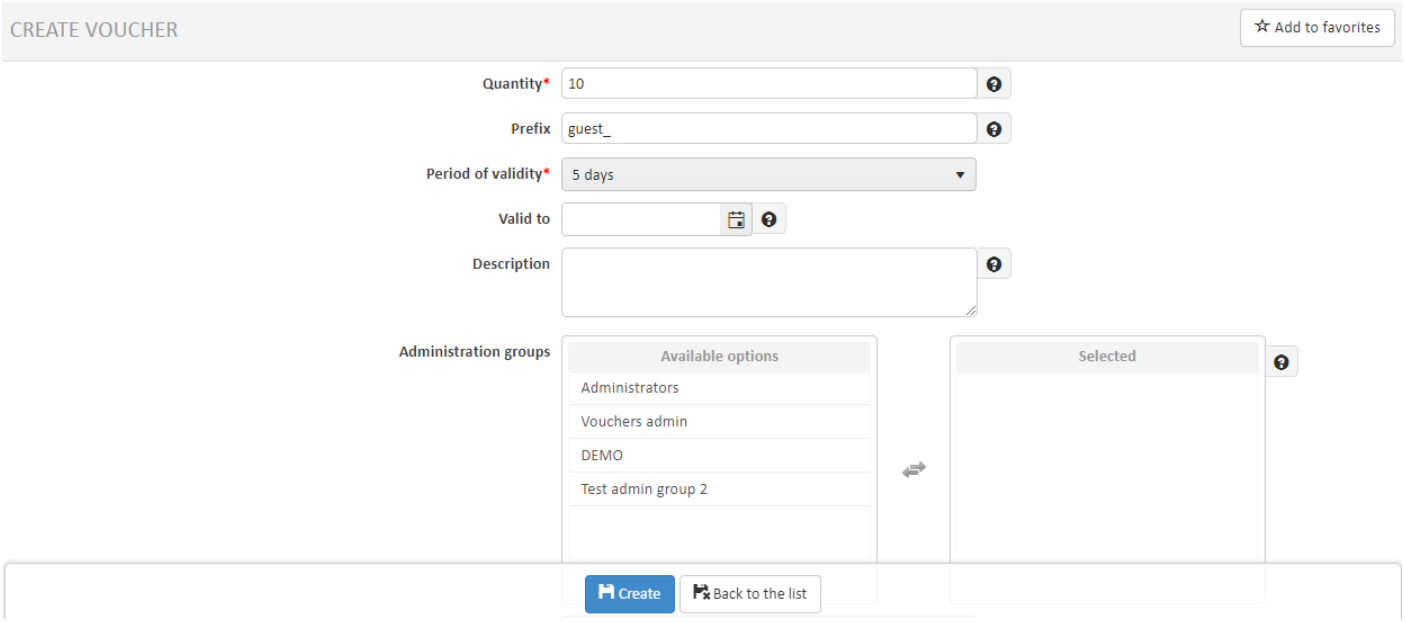
In the main menu select: ***Identities*** *(*in ***Objects****)*. Click ***Create new*** and complete the form by entering the following data:

- **First name**: User
- **Last name:** Guest
- **ID Card**: CCC 123456
- **Account type**: standard
- **Valid to**: 2026-03-21
- **Object groups**: Employees



Now save your set values. Staying in the ***Identities*** section, click button ***Create voucher*** and complete the form fields:

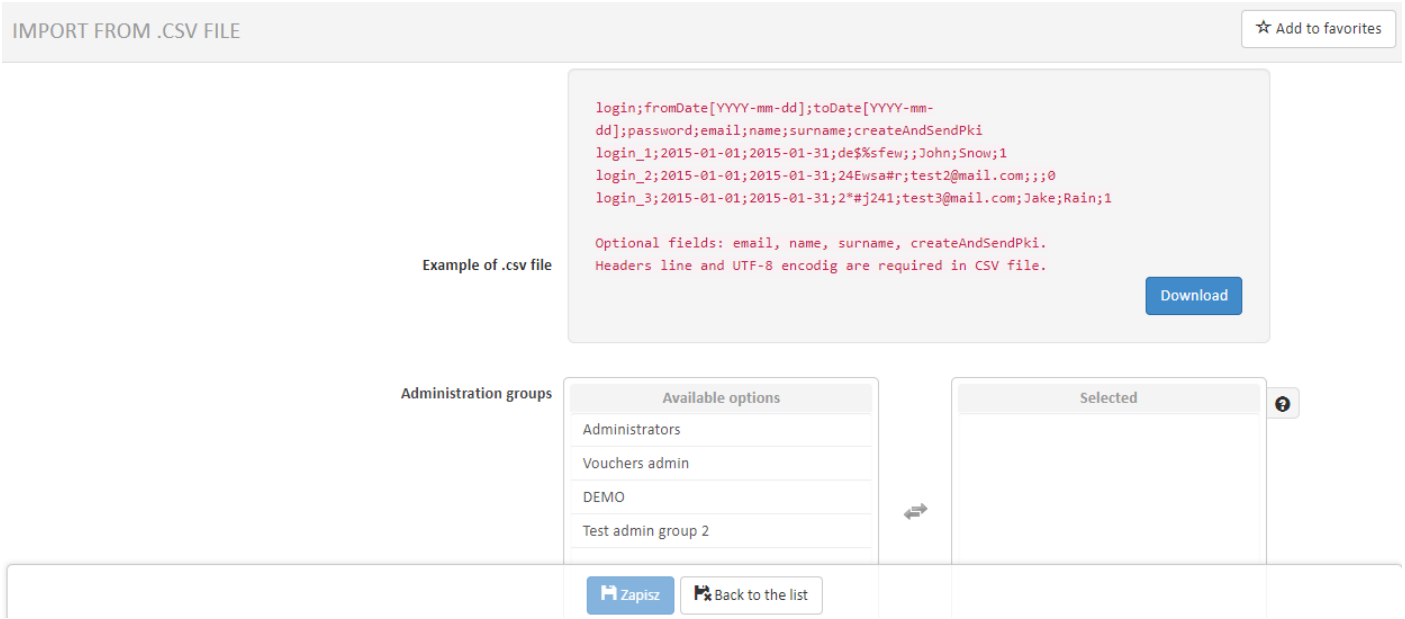
- **Quantity**: 10
- **Prefix**: guest_
- **Period of validity:** 5 days



Save your set values (click Create button below).

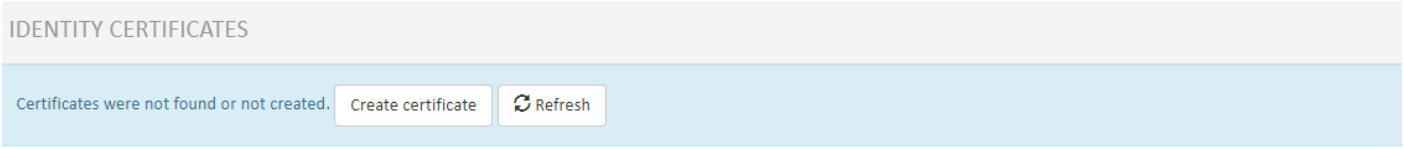
5.1.2. Import from File

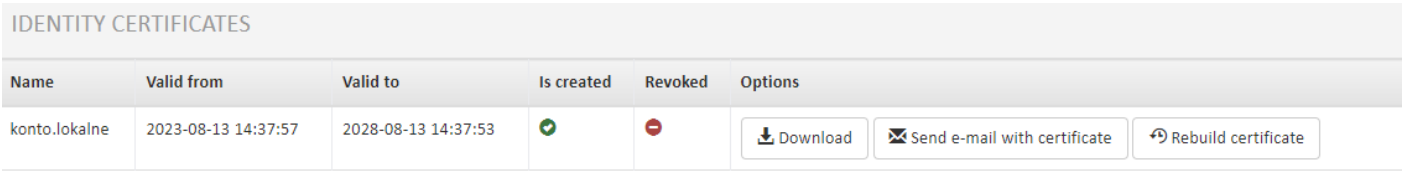
Staying still in the ***Identities*** section, click ***Import from file*** and then ***Download***. Save the file to your local drive. Click ***Select file*** and open the file you just downloaded. The file has been uploaded.



5.1.3. Certificates

Click click on the selected identity and select Certificates. Click: ***Create certificate*** button and, after a while: ***Refresh***. The certificate has been successfully generated.





5.2. Endpoints

From the main menu select: ***Endpoints*** *(*the ***Objects*** section*)*. Click: ***Create new*** and fill in the form by entering device data 1 from the table below. Click ***Save*** for the set values. Return to the list and repeat the steps for device 2:

Endpoint	1	2
Name	VoIP phone	Printer
Endpoint type	phone/smartphone	printer
Object groups	VoIP Phones	Printers
Parameters	-	-

5.3. MAC addresses

From the main menu select ***MAC addresses.*** Click: ***Create new*** and complete the form, by entering the MAC Address 1 information from the table below. Then save your set values. Now go back to the list and repeat the steps for the address 2. Then repeat that, also adding the actual MAC address of the NT1 computer network card. Read it using commands such as **cmd**, then: **ipconfig /all** or easier: **getmac**

MAC Address	1	2
MAC	2E:B4:7E:A0:CA:9B	AB:B2:86:44:6B:FD
Default IP address	-	-
Endpoint	Printer	VoIP phone
Object groups	Printers	VoIP Phones

6. Configuration

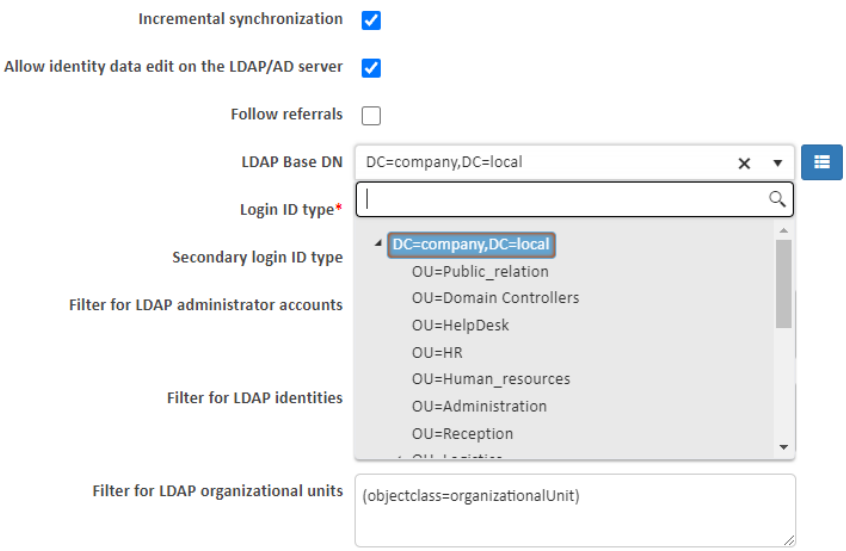
6.1. Authorization servers

From the main menu, select ***Authorization servers*** (from the ***Configuration*** section). Click: ***Create new***. Complete the form with server 1 data from the table below. Create and edit again. Click: ***More options*** and in the ***Login ID type*** field, select *Account name*. Optionally, you can also complete the field: ***Filter for the LDAP identity***. Save your settings. Repeat that for server 2:

Authorization server	1	2
Purpose	Identities	Endpoints
Authorization type	Authorization LDAP/AD	Authorization LDAP/AD
Name	Employees_AD	Computers_AD
Host	alpha.enterprise.test	alpha.enterprise.test
Service login	administrator@enterprise.test	administrator@enterprise.test
Service password	NACVIEW_SZKOLENIE22	NACVIEW_SZKOLENIE22
Login ID type	Account name (sAMAccountName)	DNS Host name (dnsHostName)
Secondary login ID type	Principal name (userPrincipalName)	Common name (cn)

In the list of authorization servers find server 1 and click the button:  Now select ***Edit***. Click ***More Options*** and in the ***LDAP Base DN*** field, select: ***DC=enterprise,DC=test***. Save these settings.

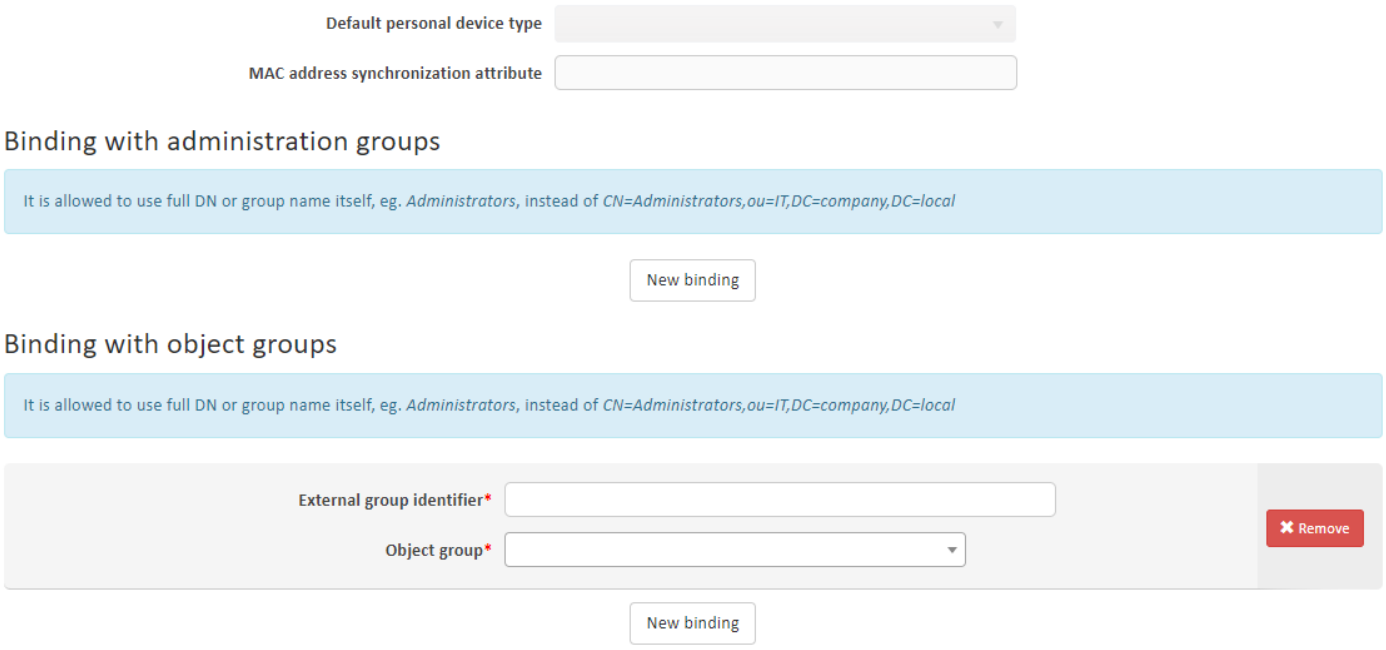
If any authorization server is inactive, click:  and select: ***Activate***.



In the row at authorization server 1 (Employees_AD) click:  . In the window that opens on the right, select: ***Import settings***. In the ***Binding with object groups*** section (at the bottom of the window), click the ***New binding*** button. In the ***External group ID*** field, enter: ***Accounting***, and in the ***Object group*** field, select Accounting. In the same way, add 3 other groups

- Managers
- Junior Network Engineers
- Senior Network Engineers

Now save your settings.



Find authorization server 2 in the list now. Click:  and in the newly opened window choose again: ***Import settings***. In the ***Default object group*** field, select: ***Computers***. Save your settings. Next, for both servers click  and select the ***Sync*** option.

From the main menu, select ***Identities*** (from the ***Objects*** section). Check whether the objects have been imported and if they have predetermined, mapped groups assigned.

6.2. Access policies

6.2.1. Policies creating

From the main menu select: ***Acces policies***. Click the ***Add Rule*** button. In the form that appears, enter the details of policy 1, found in the table below. Save the settings. Repeat the same for policies 2-6:

Access policies	1	2	3	4
Name	Host_Access	EAP_Access_Group	EAP_Access_OU_I	EAP_Access_OU_II
Authorization method	Host	EAP	EAP	EAP
Action	Access to vlan	Access to vlan	Access to vlan	Access to vlan
Send VLAN tag back	☑	☑	☑	☑
Vlan	Authorization V	Authorization I	Authorization I	Authorization II
Undefined Endpoints means	Any Endpoints	-	-	
No defined Identities means	-	Any Indetities	Any Indetities	Any Indetities
Any Identities means		Any active Identities defined in system	Any active Identities defined in system	Any active Identities defined in system
Group of Identities		Accountants, Managers	-	-
Endpoints of authorization servers	Computers_AD	-	-	-
Identities of unit	-	none	Network Operations	Research and Development
Identities of authorization servers		Employees_AD	Employees_AD	Employees_AD
Accounts conditions logic		And	And	And
Network device	C1000	C1000	C1000	C1000

Access policies	5	6
Name	MAC Phones and Printers	Captive Portal
Authorization method	MAC	MAC
Action	Access to vlan	Access to vlan
Send VLAN tag back	☑	☑
Vlan	Authorization II	Guest Network
Local CaptivePortal	-	☑
Undefined Endpoints means	Any Endpoints	
MAC addresses or Endpoints group	Printers, VoIP Phones	
Network device	C1000	C1000

After adding all policies, upload them to the system. To do this, click the ***Install list*** button. Confirm it by clicking: ***Install***.

6.2.2. Policies testing

Click: ***Policy Testing***, located in the upper right corner of the **Access Policies** window. Complete the form fields with the column 1 data from the table below. Now click: ***Send.*** The authorization result (positive or negative) should appear under the form. Repeat the same for columns 2 and 3 also.

Dane	1	2	3
Authorization type	MAC	Host (EAP)	EAP
Check for	Endpoints	Endpoints	Identity
Identity	-	-	AccountantOne
Endpoints	Computer	NT1.enterprise.test	-
Network device	C1000	C1000	C1000
Client MAC address	AB:B2:86:44:6B:FD	-	-

6.3. Events definitions

From the main menu select: ***Events definitions***. Now click ***Create new*** and complete the fields with the following data:

- **Name**: Configuration alert
- **Source:** Syslog events
- **Phrases:** VLAN mismatch
- **Action:** Notify
- **Users to notify**:
  - admin@nacview.com
  - sekretariat@nacview.com

Now save your settings. Then click:  and select: ***Matched logs***.

6.4. Captive Portal

From the main menu, select ***Captive Portal*** (***Configuration*** section). Click the ***Edit*** button next to the entry with the portal type ***Authorization***. Then adjust the data:

- **Name**: Captive
- **Active**: Yes
- **Certificate**: internal (pki.enterprise.test)
- **IP address**: 10.XX.96.1
- **HTTP port**: 80
- **HTTPS port**: 443
- **URL address**: https://captive.enterprise.test
- **End user agreement**: The text of the regulations for the employee

+ Authorization and registration settings:

- **Manual identities activation**: No
- **Manual endpoints activation**: No
- **Password notification type:** Instant
- **Add this groups after registration**: Employees

Save your set values. Then click ***Install configurations*** (upper right corner of the window). Now edit subnet 10.XX.96.0/24 and set ***DNS server address 1***: 10.XX.96.1. Save your settings.

6.4.1 Functional test

You can check the CP by logging into any Windows 11 (**NT2**) computer. Disable the first network card of the computer and enable the second. After opening the browser and entering any address, you should be redirected to the portal where, after entering the login details correctly, you will be disconnected. Then you should receive a different IP address and you will be transferred to another VLAN – according to the previously established policy. You can analyze the entire process in the ***Reports > Authorization events*** section.

On the network device, you can view the authorization process and the VLAN assigned to the port using the following commands: *show mab all summary, show mab interface gigabitEthernet 1/0/2 details, show vlan brief*.

6.5. TACACS+ Groups

6.5.1. Network device configuration

Log in using the SSH Client to the C1000 as Admin. To set TACACS+on a switch, configure it with the following commands by entering the configure terminal edit mode:

```
aaa group server tacacs+ NVTac
server-private 10.XX.166.3 key NACVIEW_SZKOLENIE22
accounting acknowledge broadcast
ip tacacs source-interface vlan 166
exit
aaa authentication login default group NVTac local
aaa authorization exec default group NVTac if-authenticated
aaa authorization commands 0 default group NVTac none
aaa authorization commands 1 default group NVTac none
aaa authorization commands 15 default group NVTac none
aaa accounting exec default start-stop group NVTac
```

6.5.2. TACACS+ Password

From the main menu, select ***Administrator accounts*** (***Administration*** section). Click on  next to the administrative account (sekretariat@enterprise.test) and select ***Edit***. Click Change/set password and fill in the TACACS+ Password field: NACVIEW_SZKOLENIE22. Save the set values.

From the main menu, select ***Network devices***. Click on this  next to the selected network device and select ***Edit***. Click Change/set password and fill in the ***TACACS+ key*** field in accordance with the data from point 1.4. (enter password: NACVIEW_SZKOLENIE22). Save your settings.

6.5.3. TACACS+ Configuration

From the main menu, select ***TACACS+ servers*** (***Configuration*** section). Click the ***Create new*** button. Complete the form with the following data:

- **Name**: Roles1
- **Default service**: permit
- **Users**: sekretariat@enterprise.test
- **Network devices**: C1000

Save the set values. Find the group you have just added in the list and click the button  and then, in the ***Edit TACACS+ settings*** window that opens on the right. Press ***Add setting*** and complete the form by entering the following commands:

- **Command**: show running-config
- **Privilege**: deny
- **Active**: Yes

Save your settings, then click ***Install Configuration*** and wait for the end of the installation process.

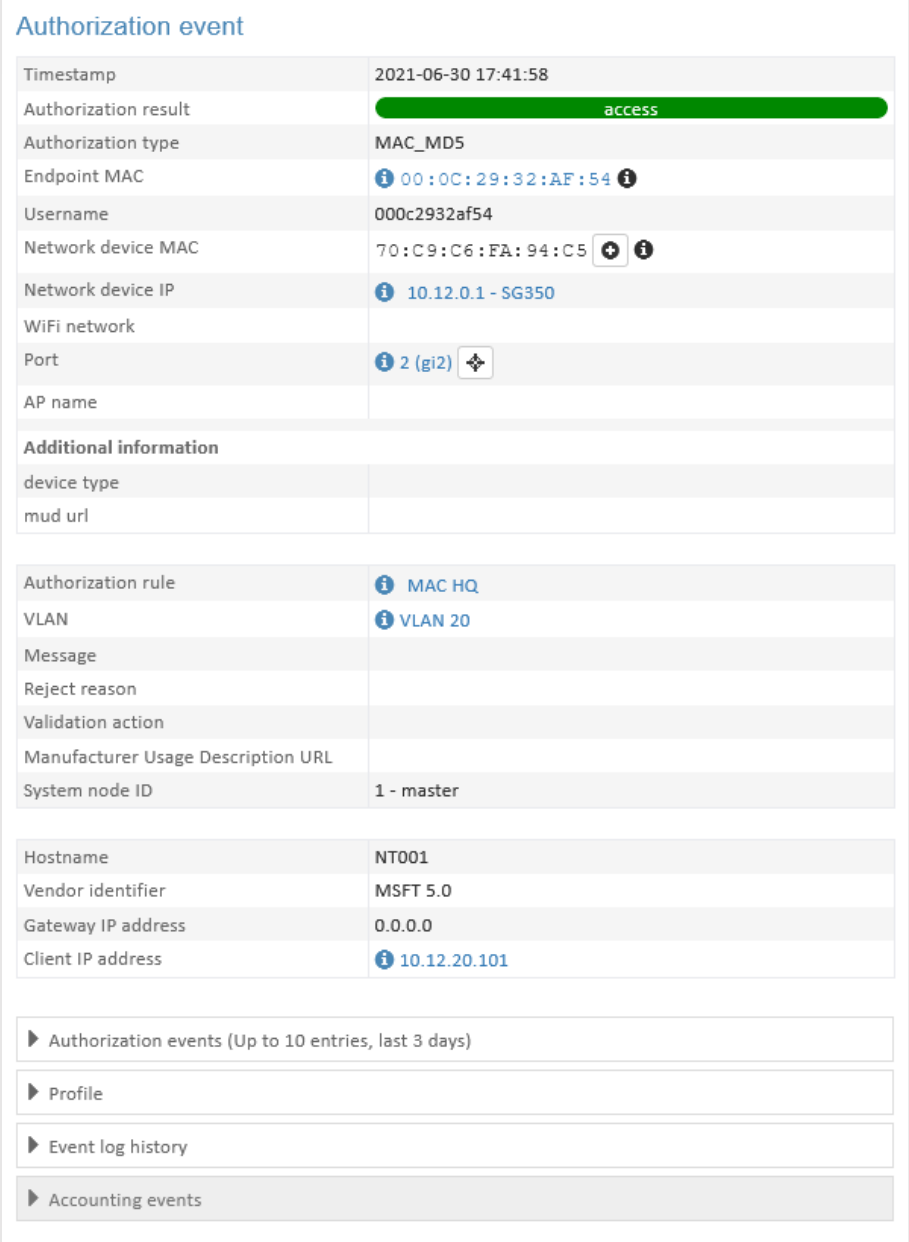
Log in via SSH to C1000 as the sekretariat user and enter the TACACS administrator password. Execute the command: *show running-config*. In NACVIEW go to the ***TACACS events*** section and check the information about logging into the network device and blocking the execution of the command. Adjust the setting by changing the deny parameter to permit. Install the configurations and wait for the end of the installation process.

Now run the show running-config command on the C1000 again. Verify the execution of the command in ***TACACS events.***

7. Reports - section overview

7.1.1. Verification of policies operation

Verify the login policies used. To do this, select ***Authorization events*** from the main menu (***Reports*** section). In ***Authorization events***, see details and used authorization. In ***DHCP Events*** (***Reports*** section) check the assigned IP address:

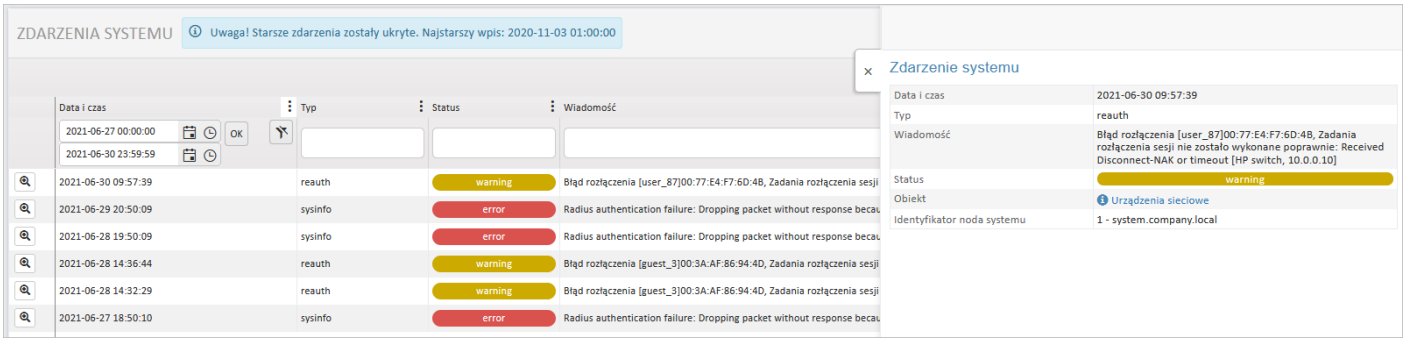


7.1.2. Session disconnection

From the NACVIEW main menu, select ***Authorization events***. Find the last authorization in the list and press the button  on the same line. In the window that opens on the right, click ***Reathentication***. Complete the displayed form with the following data:

- **Disconnect the session**: Yes
- **What groups to add the MAC address and identity to**: Quarantine
- **MAC address**: selected from the event
- **Identity**: selected from the event

Now save your settings. Go to: ***System events*** and check the disconnect result.



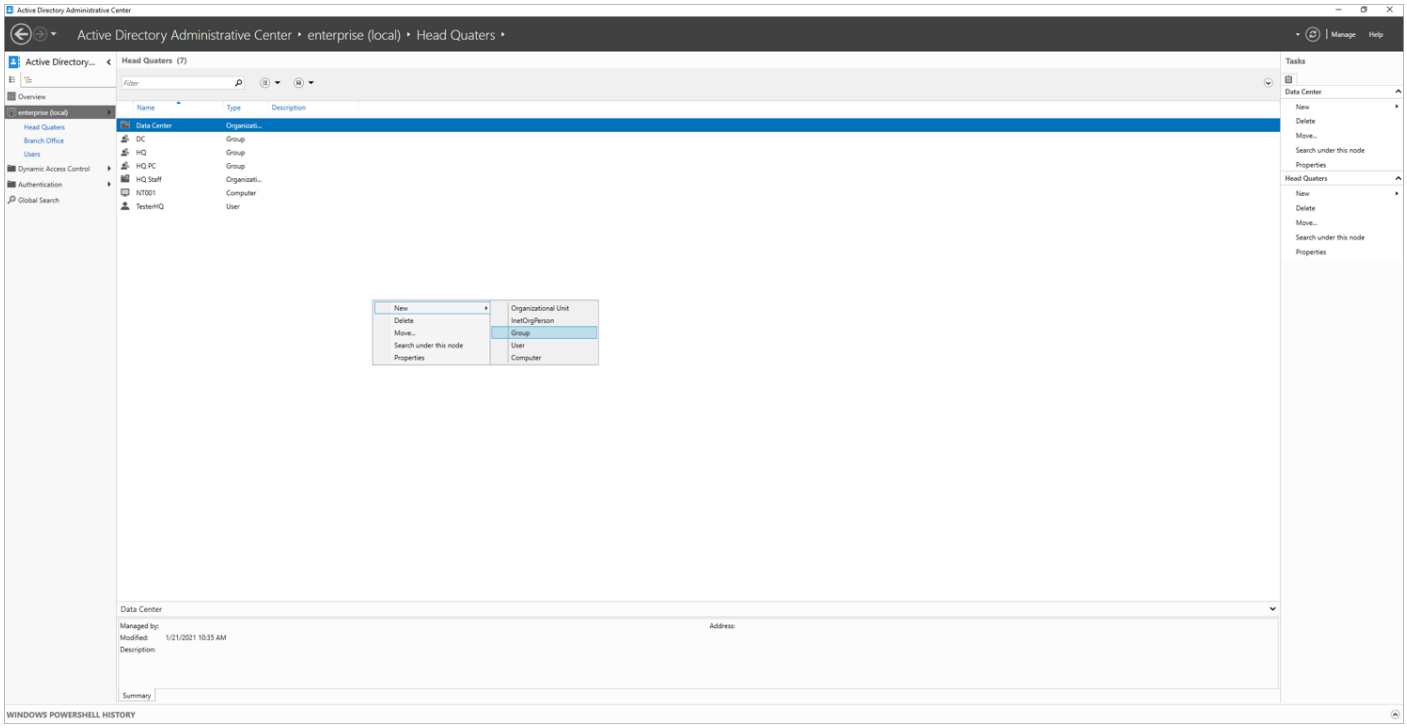
8. Service configuration on the Windows Server and Clients

8.1. Certificates publication via GPO

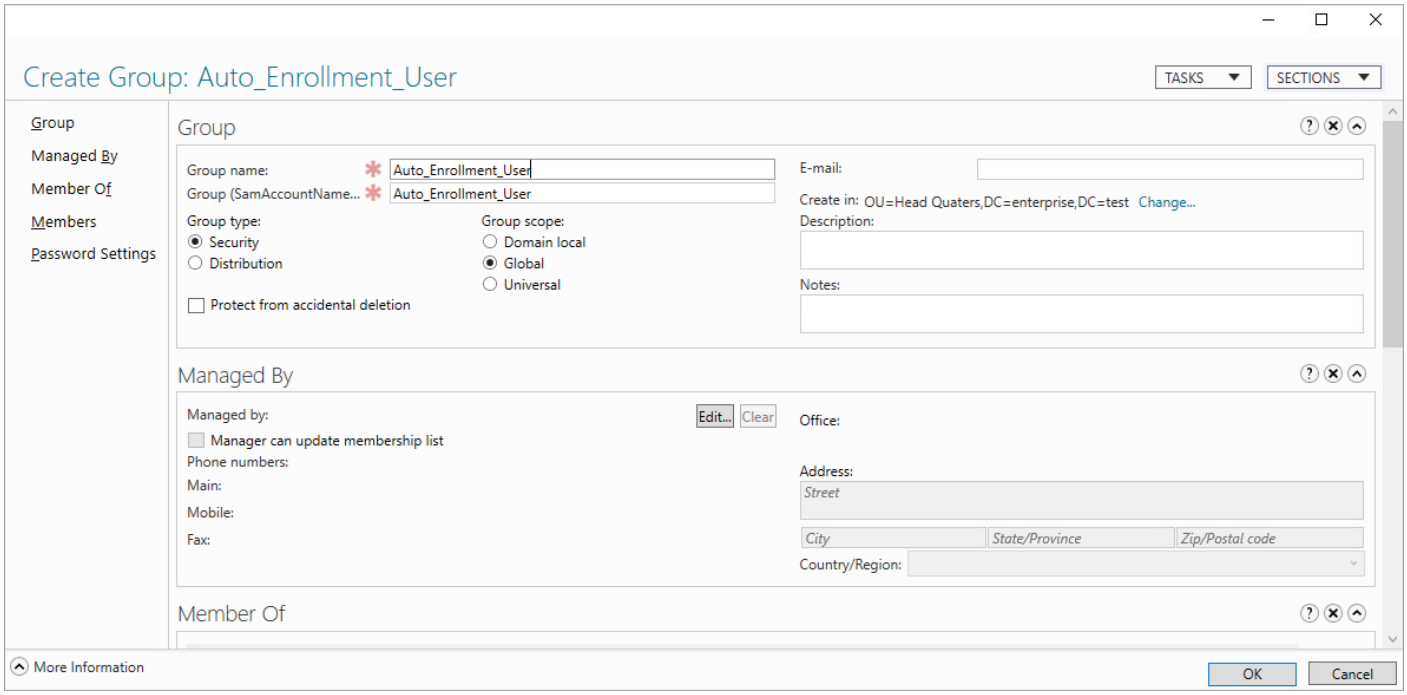
8.1.1. Creating security groups for the user

Open the ***Active Directory Administrative Center*** on the domain manageable server (**machine XX-DC**).

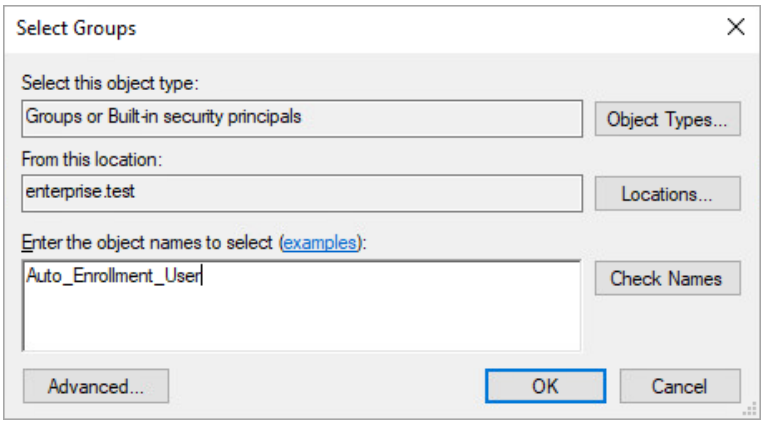
In ***OU Test Division***, create a security group. To do this, right-click and select ***New > Group***. Users belonging to this group will participate in the so-called *auto-enrollment*.



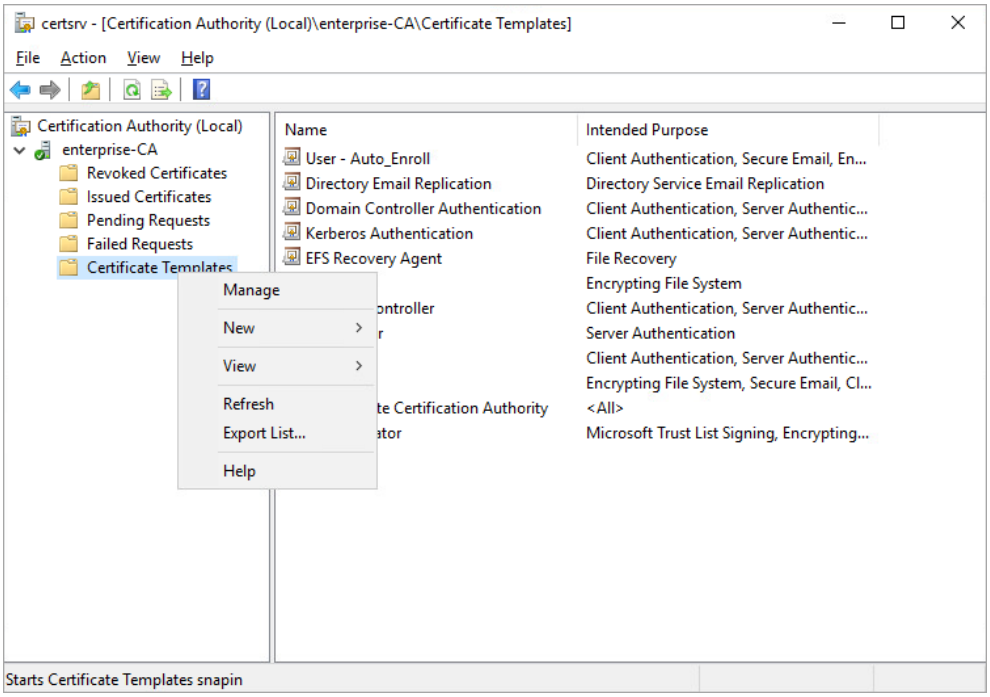
Enter a group name (e.g. *Auto_Enrollment_User*). Save it with ***OK*** click.



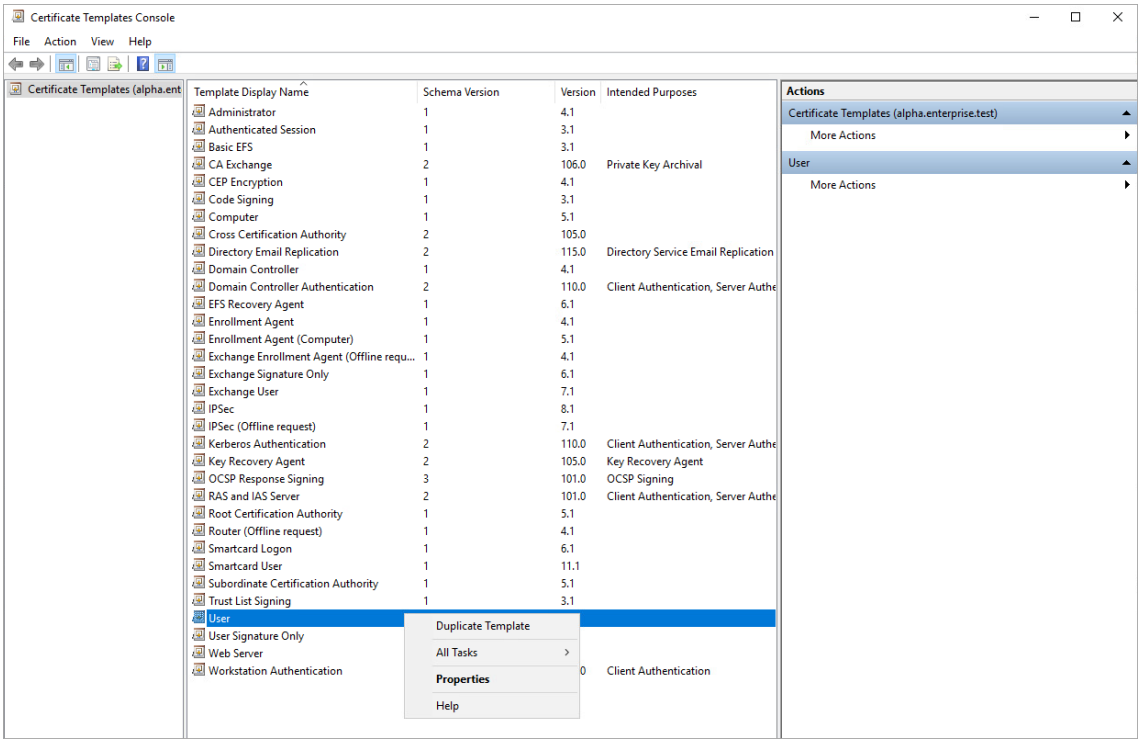
Add users to the group you have just created. To do this, right-click on the selected user and select ***Add to group…***. Enter the name of the previously created group. Confirm with ***OK.***



Shut down AD AC on the **XX-DC** machine, then go to the **XX-CA** VM and open this tool: **XX-CA** ***Certification Authority*** (***Server Manager > Tools > Certification Authority***). Right click on ***Certificate Templates***, and select: ***Manage.***

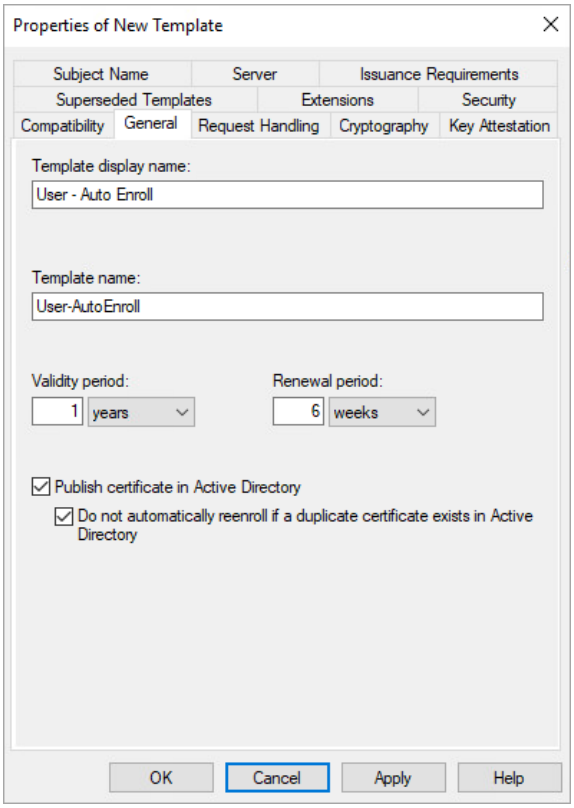


Certificate templates should appear in the panel on the right. Right click on the template named ***User*** and then select: ***Duplicate Template***.

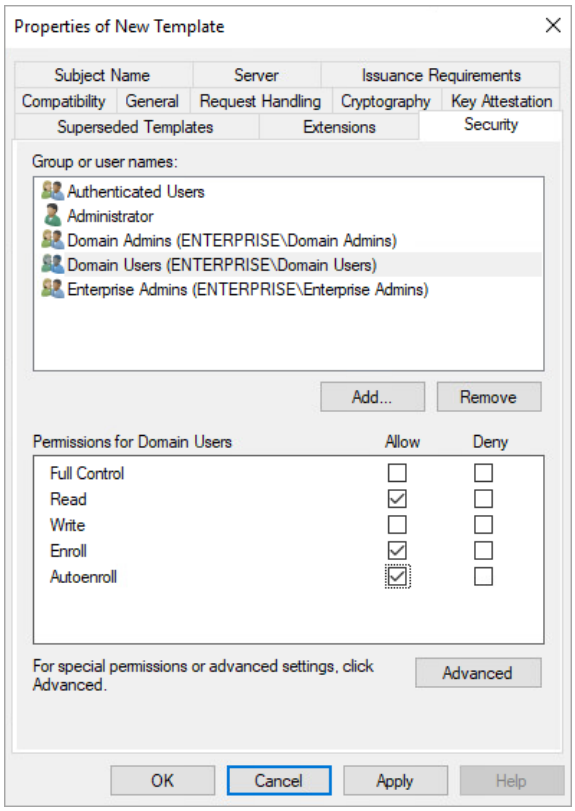


Make changes to the tabs as follows:

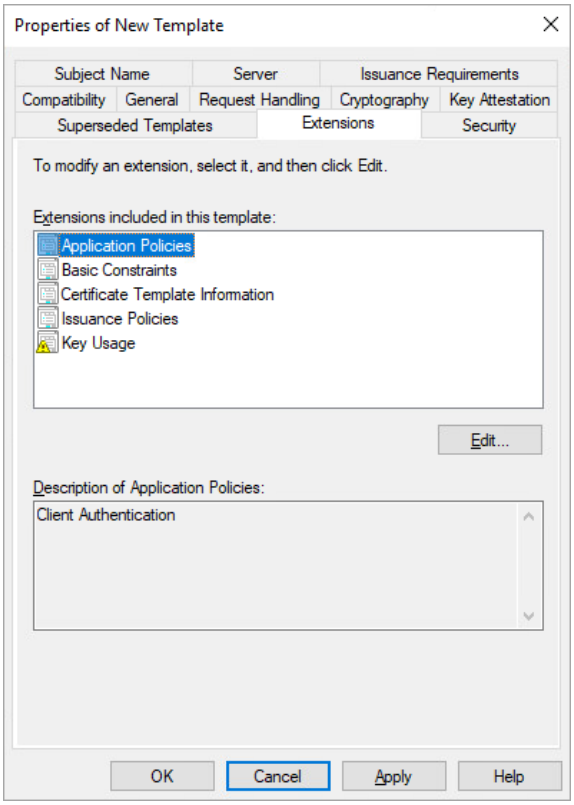
- ***Compatibility:*** select the correct operating system for the certification authority and certificate recipient. This should be the lowest version of the operating system in your environment.
- ***General:*** Change the name (here: User - Auto Enroll) and set the validity period according to organization policies (we recommend renewing no more than once a year. Check the option: ***Publish certificate in Active Directory*** and ***Do not automatically reenroll if a duplicate exists in Active Directory***.



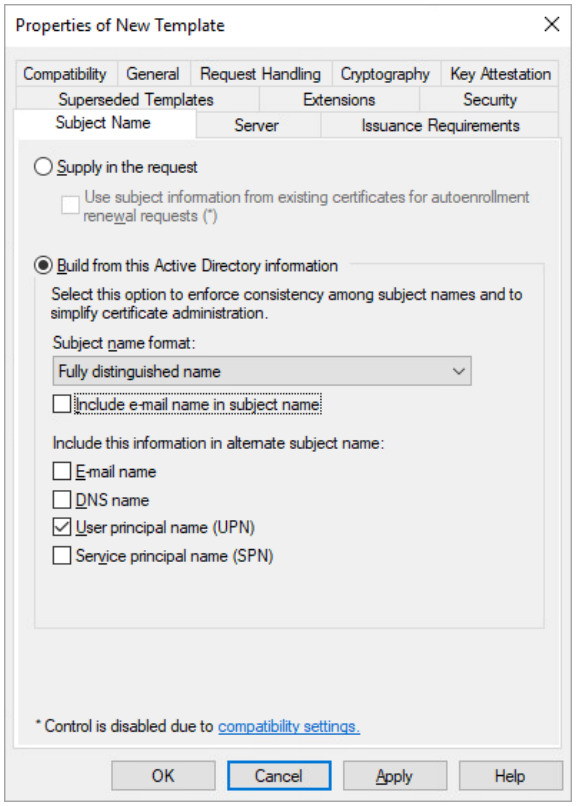
- ***Cryptography***: recommended min. 2048 bit key, and 4096 for important groups.
- ***Security***: in ***Permissions for Domain Users*** section select the options as the picture below:



- ***Extensions***: For ***Application Policies*** select: ***Client Authentication*** (delete other options), and for ***Key Usage*** check: ***Digital Signature*** and also: ***Signature is proof of origin***.

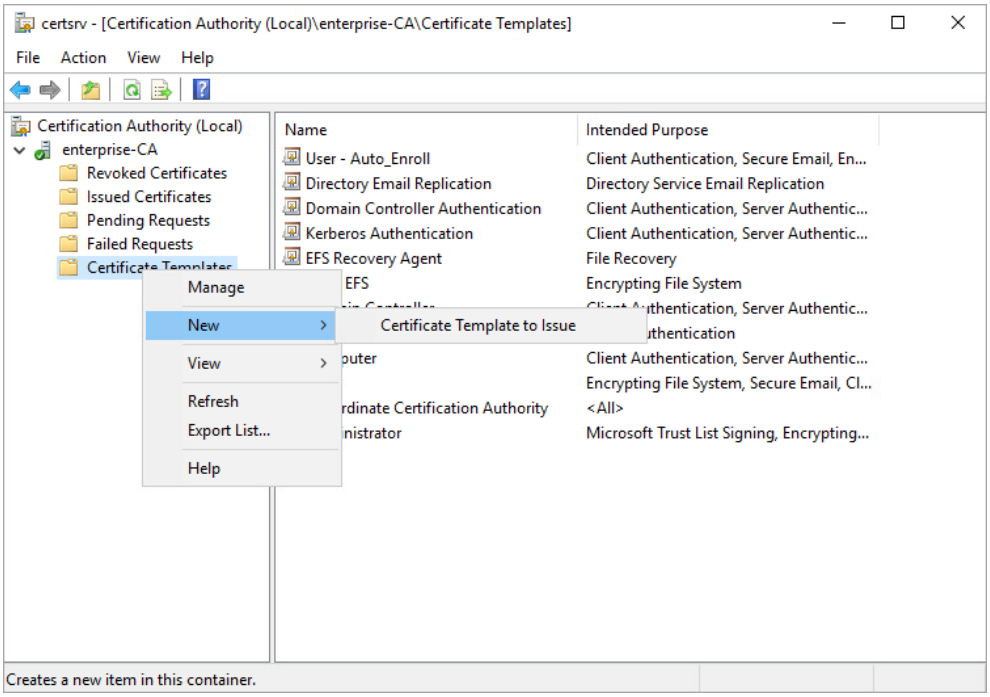


- ***Subject Name***: check ***User principal name (UPN)*** option and if the rest options are unchecked.



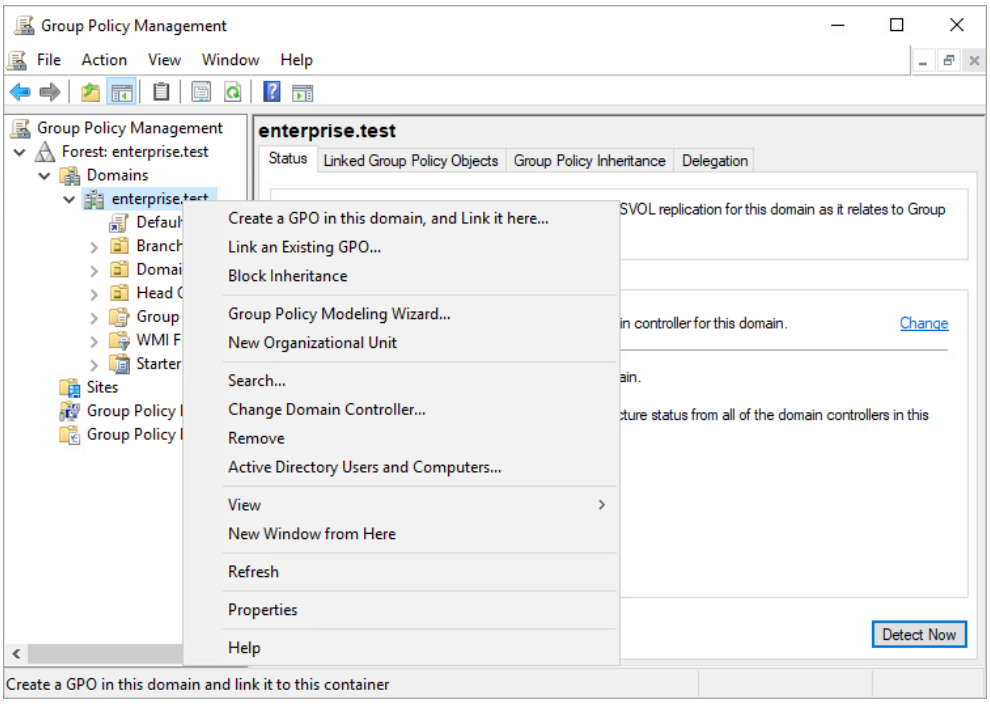
Leave the values in the other tabs as default. Confirm the changes with the ***OK*** button and close the certification template management panel.

Add the newly created template for active templates. To do this, right-click on ***Certificate Templates*** and select ***New > Certificate Template to Issue***.

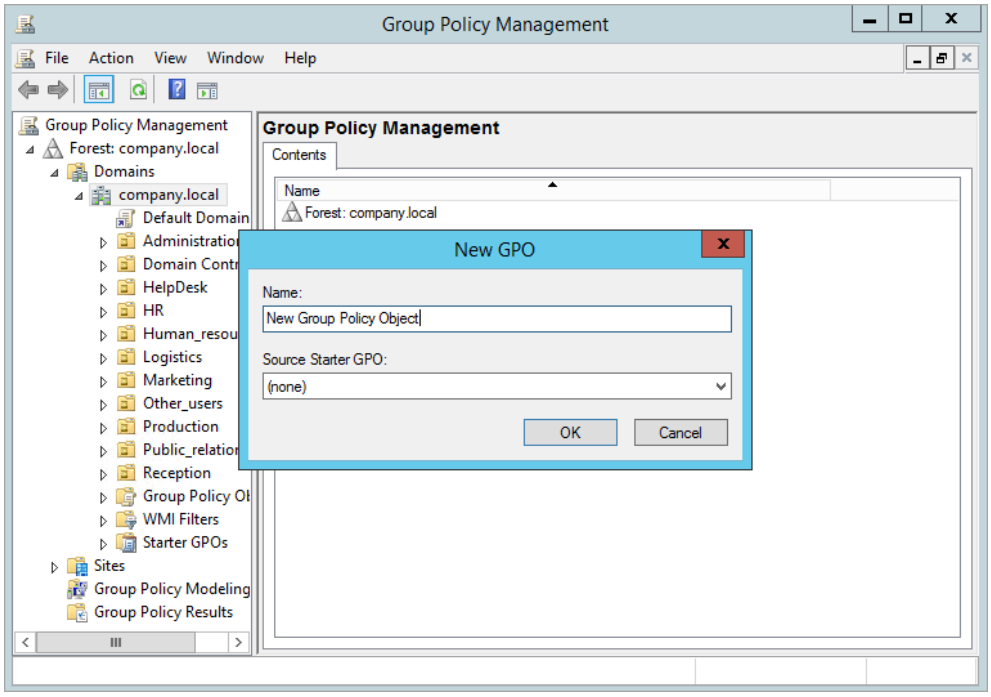


8.1.2. Certificates publication for the user

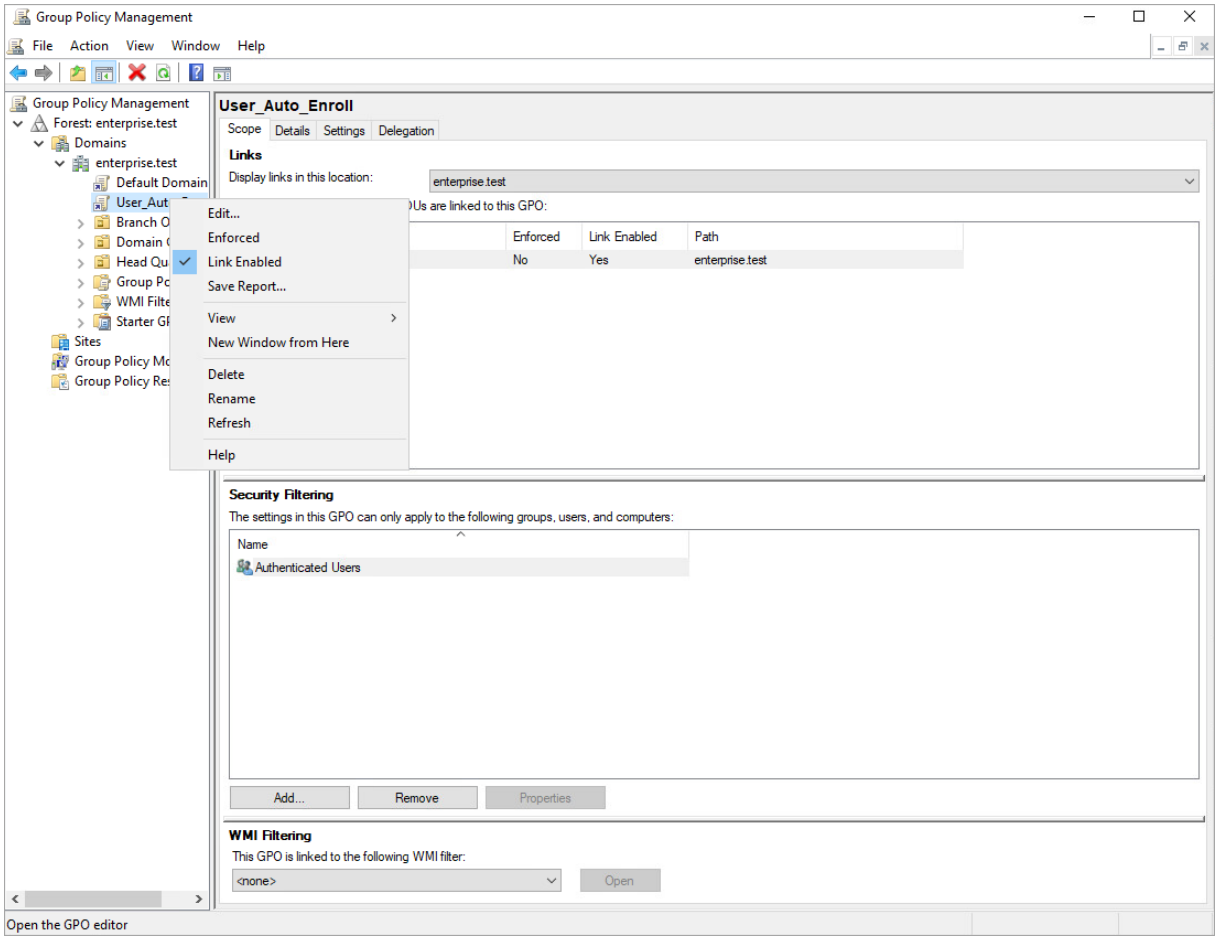
On the domain controller (**machine XX-DC**), search and open: ***Group Policy Management.*** In the domain structure window, expand: ***Forest*** > ***Domains > enterprise.test > Test Division***. Right-click on the selected OU and select: ***Create a GPO in this domain, and Link it here…***



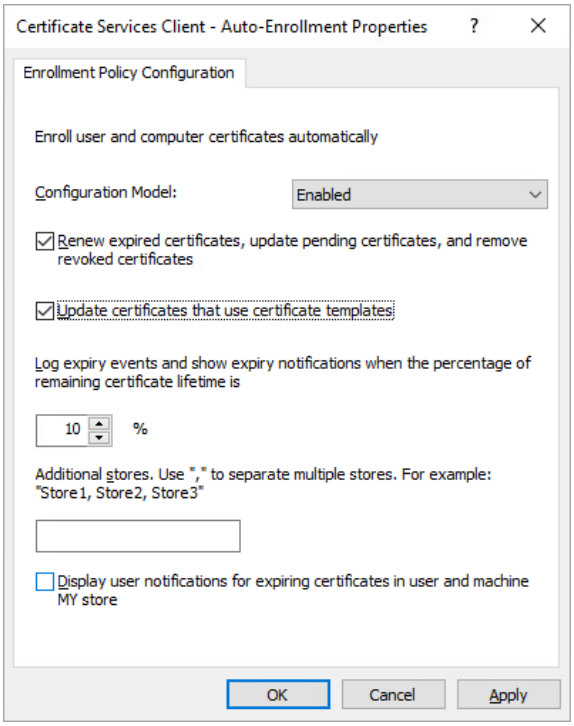
In the window that appears, enter a name for the new GPO and click ***OK.***



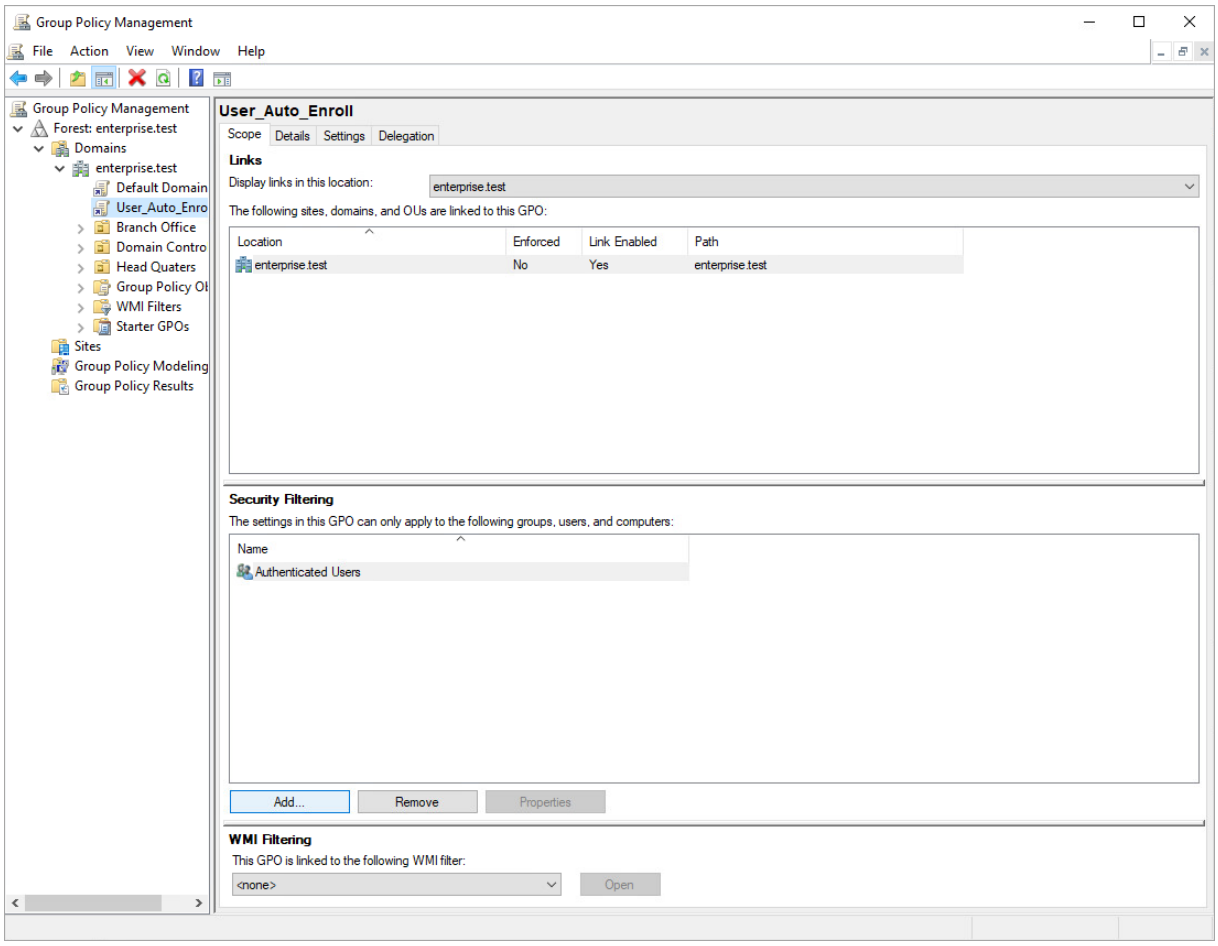
Now right click on the added GPO and select ***Edit***.



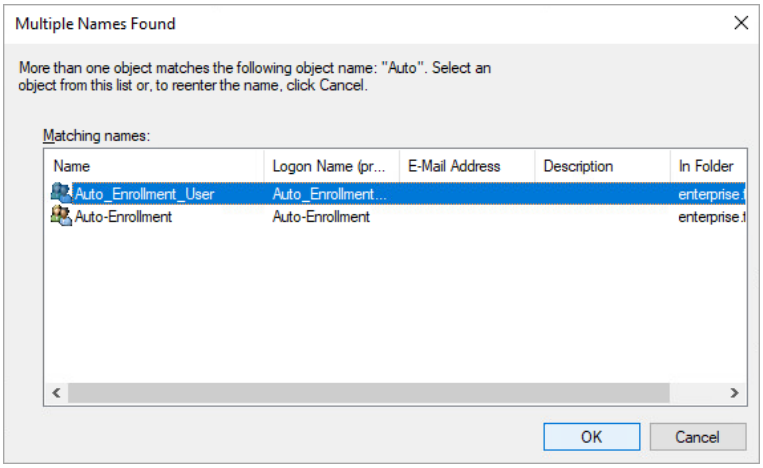
Go to: ***User Configuration*** > ***Policies > Windows Settings*** > ***Security Settings*** > ***Public Key Policies***. In the ***Object Type*** tab select: ***Certificate Sercices Client - Auto-Enrollment***. Set the values as in the example below:



Save you settings with ***OK***, and next shut ***GPO Editor***. Now go to the ***Scope*** - the newly created policy tab.



In the ***Security Filtering*** section add the security group created in the previous step, dedicated to users.



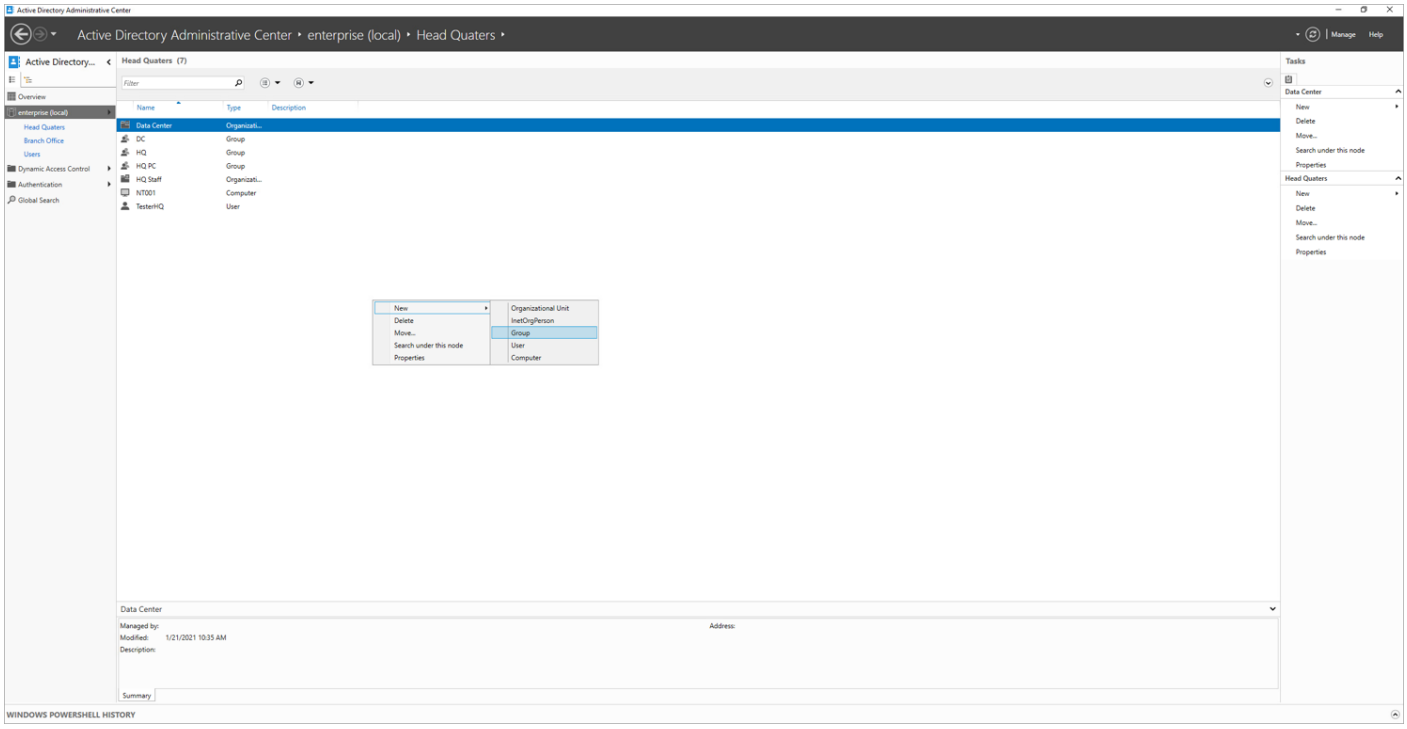
Confirm with ***OK*** and close. The next time you log in, the certificate should be automatically issued.

8.1.3. Creating security groups for devices

Open ***Active Directory Administrative Center*** on the domain management server **(XX-DC Machine).**

In OU ***Test Division*** create a security group. To do this, right-click and select: ***New > Group***.

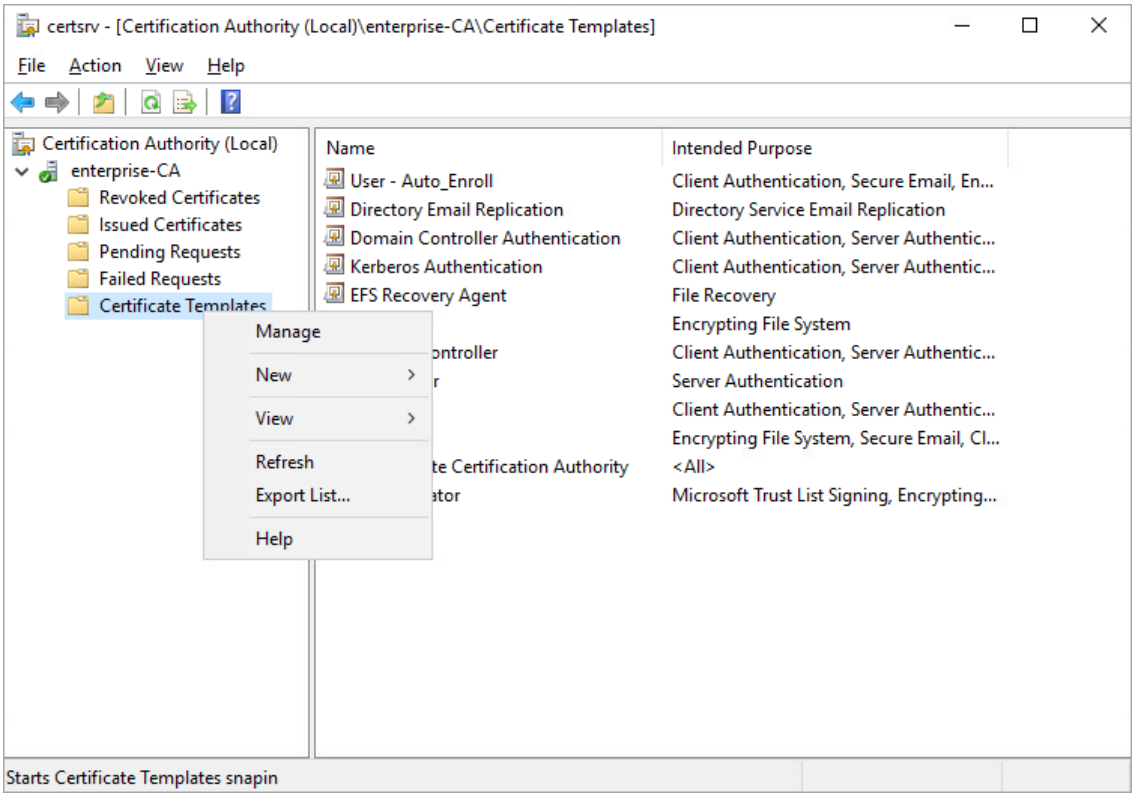
Computers belonging to this group will participate in the so-called *auto-enrollment*.



As before for users, now enter a group name for devices (e.g. *Auto_Enrollment_Host*). Save it all with ***OK***.

Now add the computer to the group you have just created. To do this, right-click on the selected host and select: ***Add to group...*** Enter the name of the previously created group. Confirm with ***OK***.

Now shut AD AC, and then open: ***Certification Authority*** on your server with the ability to manage AD CS (***Server Manager > Tools > Certification Authority, XX-CA Machine***). Right click on: ***Certificate Templates***, and next select: ***Manage.***



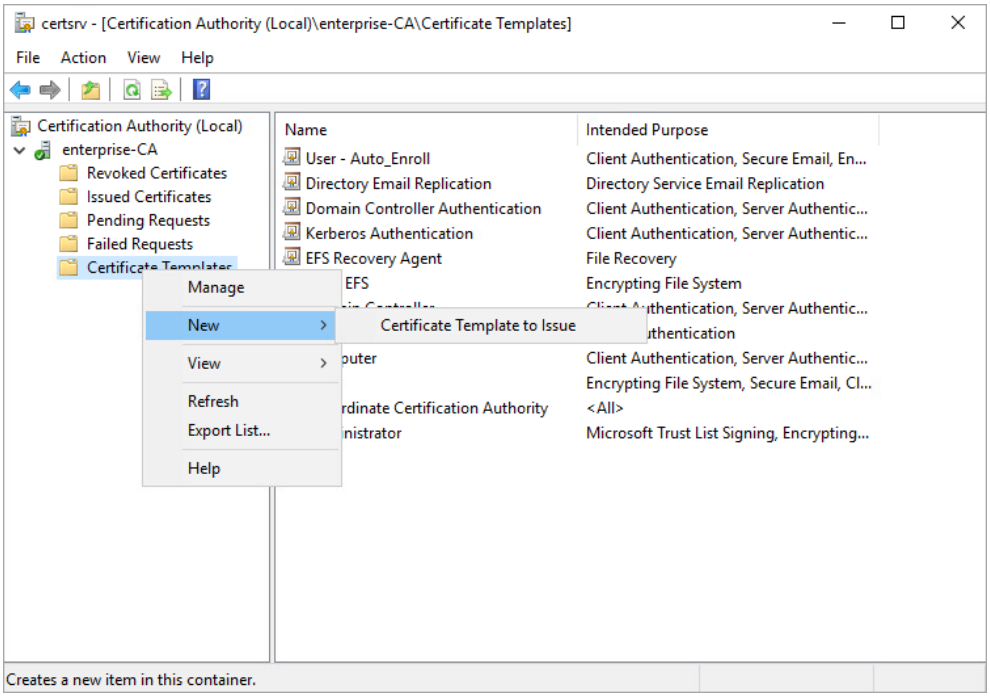
Certificate templates should appear in the panel on the right. Right click on the template named ***Computer*** and select ***Duplicate Template***.

Make changes to the tabs as follows:

- ***Compatibility:*** select the correct operating system for the certification authority and the certificate recipient. This should be the lowest version of the operating system in your environment.
- ***General***: Change the name (e.g. Host - Auto Enroll) and set the validity period according to organization policies (we recommend renewing no more than once a year). Check options: ***Publish certificate in Active Directory*** and also: ***Do not automatically reenroll if a duplicate exists in Active Directory***.
- ***Cryptography***: recommended min. 2048 bit key, and 4096 for important groups.
- ***Security***: in the ***Permissions for Domain Computers*** section select the options the same way as done before for the user: Allow: Read, Enroll, Autoenroll.

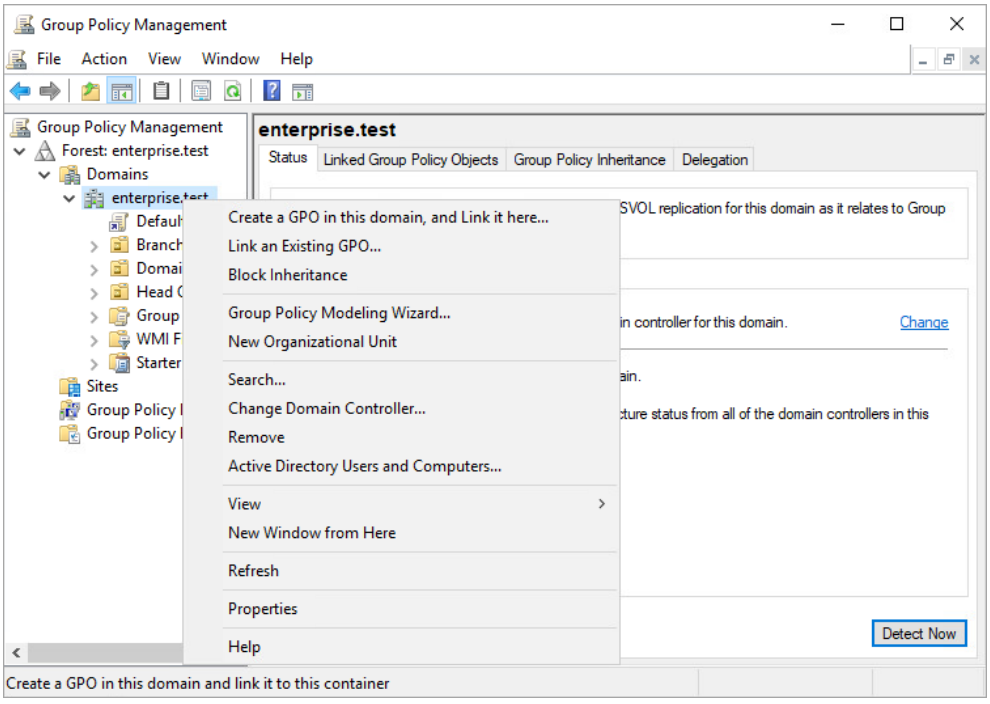
Leave the values in the other tabs as default. Confirm the changes with the ***OK*** button and close the certification template management panel.

Add your newly created template to active templates. To do this, right click on ***Certificate Templates*** and select: ***New*** > ***Certificate Template to Issue***.

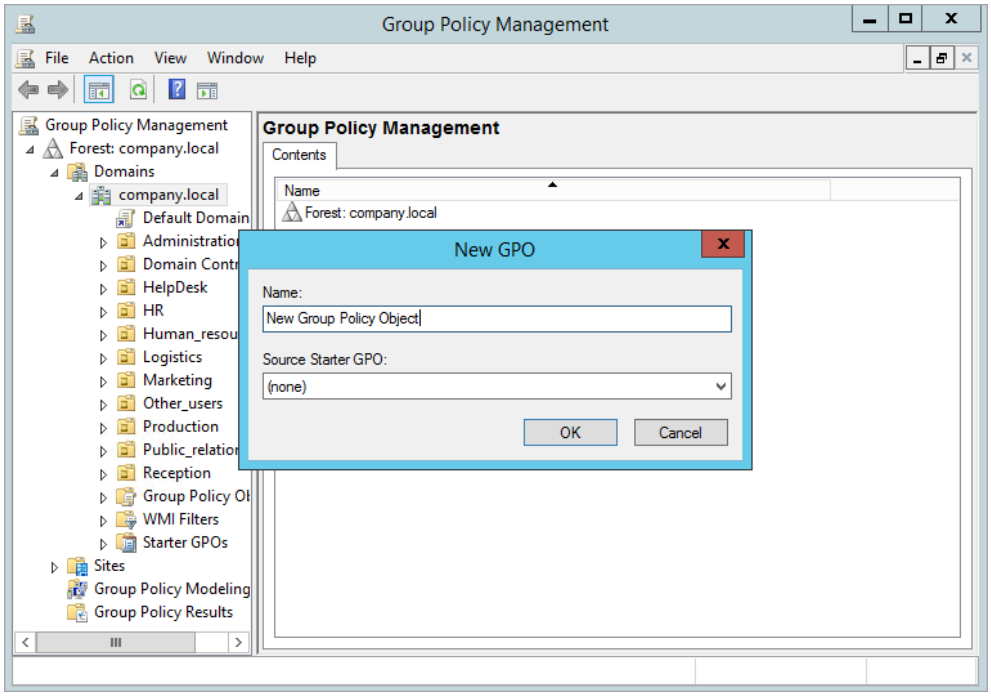


8.1.4. Certificates publication for devices

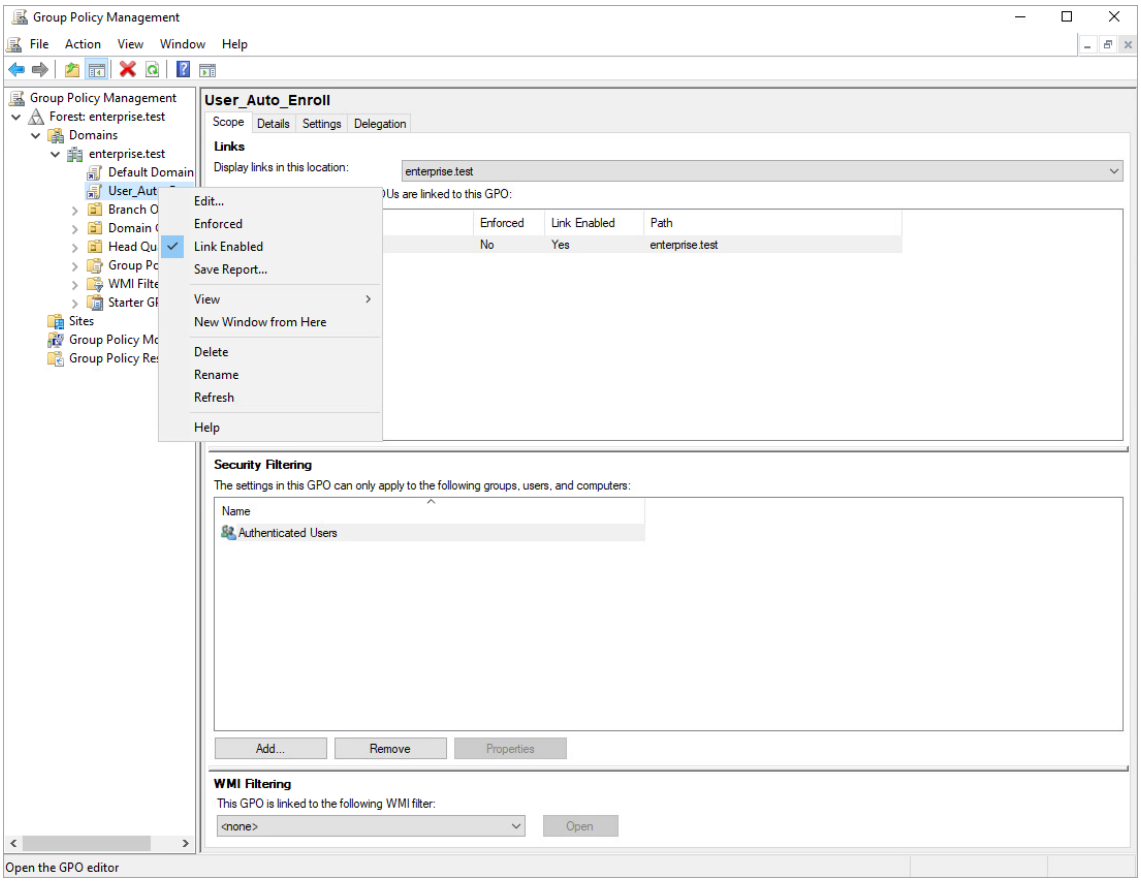
On your domain controller **(XX-DC Machine)** find and open: ***Group Policy Management.*** In the domain structure window expand: ***Forest*** > ***Domains > enterprise.test > Test Division***. Right click on the chosen OU and select ***Create a GPO in this domain, and Link it here…***



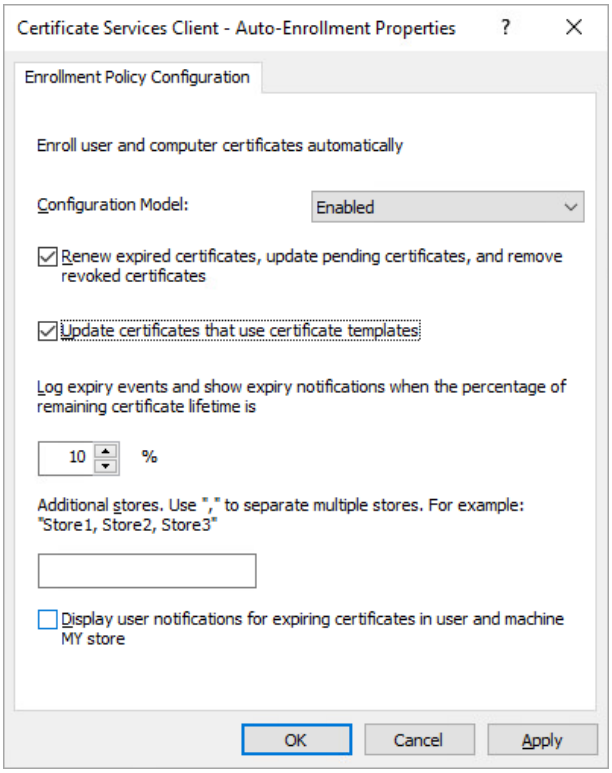
In the window that appears, enter a name for the new GPO and click ***OK*** to confirm.



Right click on the added GPO and select ***Edit***.



Now to go: ***Computer Configuration*** > ***Policies > Windows Settings*** > ***Security Settings*** > ***Public Key Policies***. In the ***Object Type*** tab select: ***Certificate Services Client - Auto-Enrollment***. Set the values as in the example below:



Save your set values with ***OK***, and next close ***GPO Editor***. Go to the ***Scope*** tab – your newly created policy. ***In the Security Filtering*** section add the security group created in the previous section dedicated to devices. Confirm all with ***OK*** and close. Next time you log in, the certificate should be automatically issued.

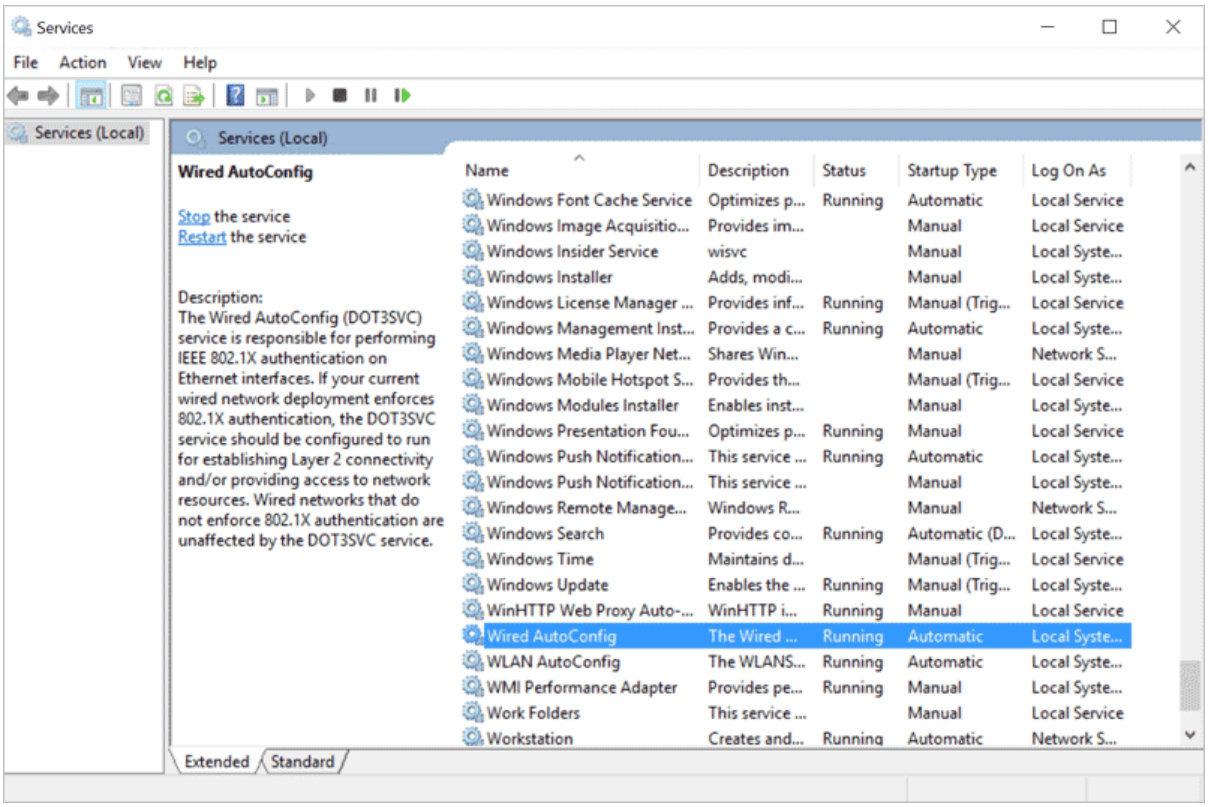
8.2. PEAP client configuration

8.2.1. Manual configuration of the PEAP client

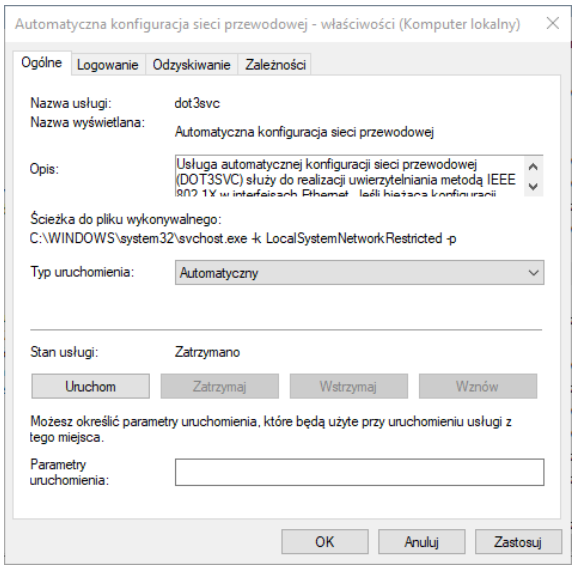
For the proper PEAP communication, it is recommended to import and install the root CA certificate on the computer. In case the PKI is on AD - it is not required.

On the Windows 11 (NT1) Machine, search the system for the ***Services*** application and open it.

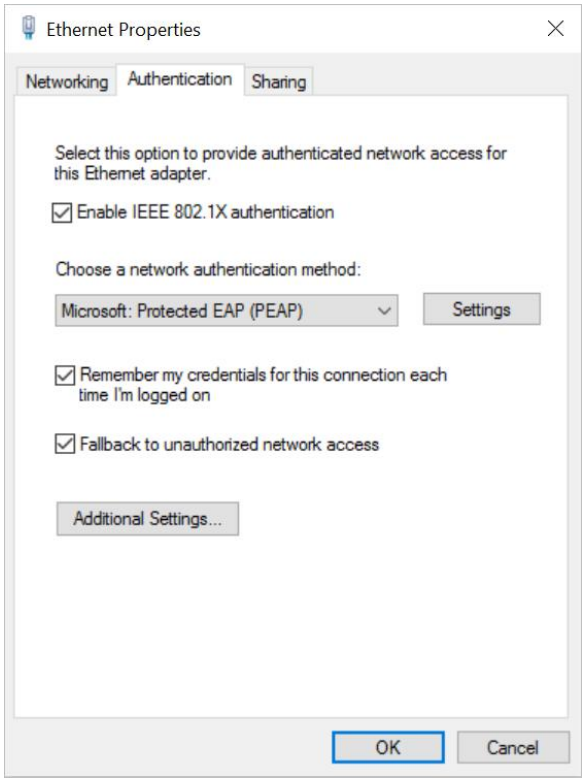
In the list of services, find ***Wired AutoConfig*** and double click on it:



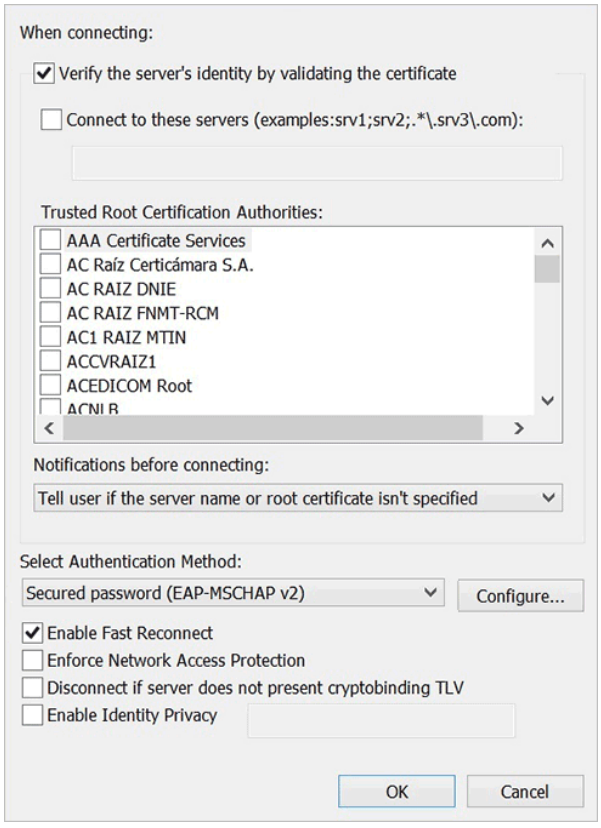
In the window that appears, in the Startup type field, select ***Automatic***. Click the ***Run*** button and confirm with the ***OK*** button.



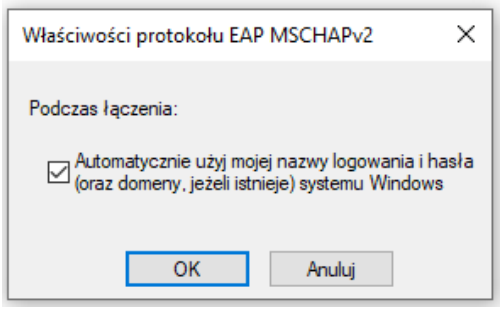
Search the system for the ***Network and Sharing Center*** (Control Panel > Network and Internet > Network and Sharing Center). From the left sidebar, select: ***Change adapter settings***. Right click on the wired network (second adapter) you want to configure and enter its ***Properties***. In the window that appears, go to the ***Authentication*** tab:



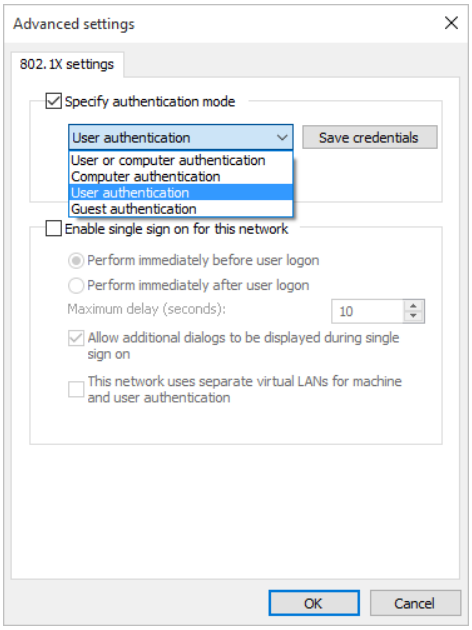
Select Microsoft as the network authentication method ***Microsoft: Protected EAP (PEAP)*** and click: ***Settings***. In the next window set the fields again, as shown in the screen below:



Click ***Configure…*** and check: ***Automatically use my Windows login and password*** (and Windows **domain**, if any):



Confirm twice with the ***OK*** button. Go to ***Additional settings...*** Check: ***Specify authentication mode*** and select ***User or computer authentication*** from the drop-down list. Select ***Enable single log-in to this network***.



Click: ***Save Credentials***. Confirm all open windows with the ***OK*** button. You can now connect to the network.

8.2.2. Verification of policies operation

After the correct configuration of network settings on the Windows 11 (**NT1**) test machine, check on the network card whether the connection has been established. Disable the first network card of the computer and enable the second. Verify in ***Authorization Events*** whether there was a record of correct authorization and what type was used. Check what policy allowed, what VLAN, and what IP address was assigned.

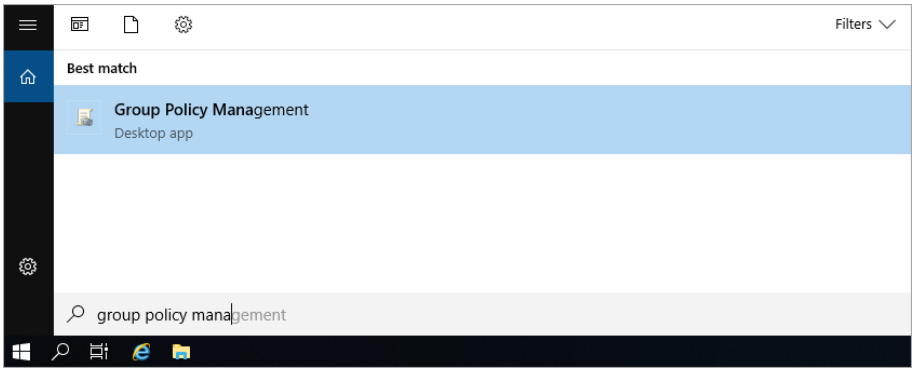
Log in to the network device and execute these commands:
`show dot1x all summary` oraz **`show dot1x interface gigabitEthernet 1/0/1 details`**.
More details in Cisco C1000: **`show authentication sessions interface gi1/0/1 det`**

Then log off the user from the system and repeat the steps above:

8.3. TLS Client configuration

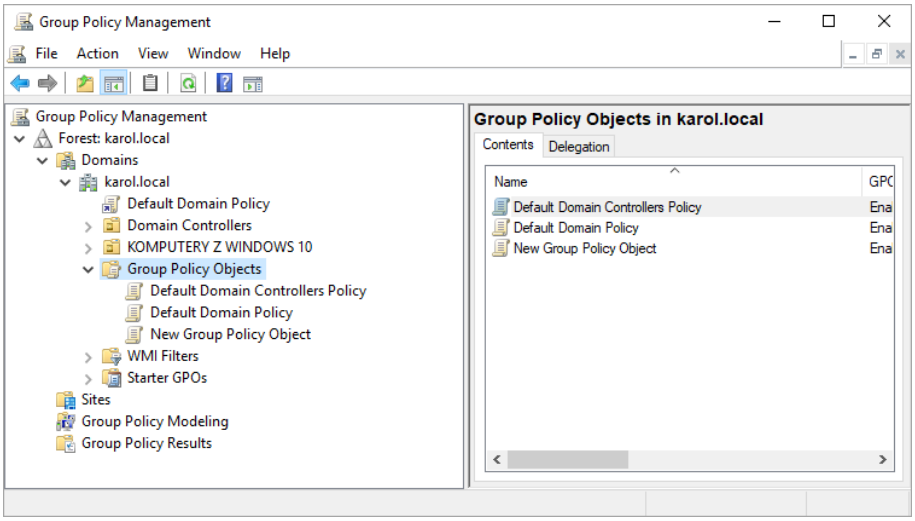
8.3.1. TLS client configuration via GPO

On the domain controller (XX-DC Machine), search and open: ***Group Policy Management.***

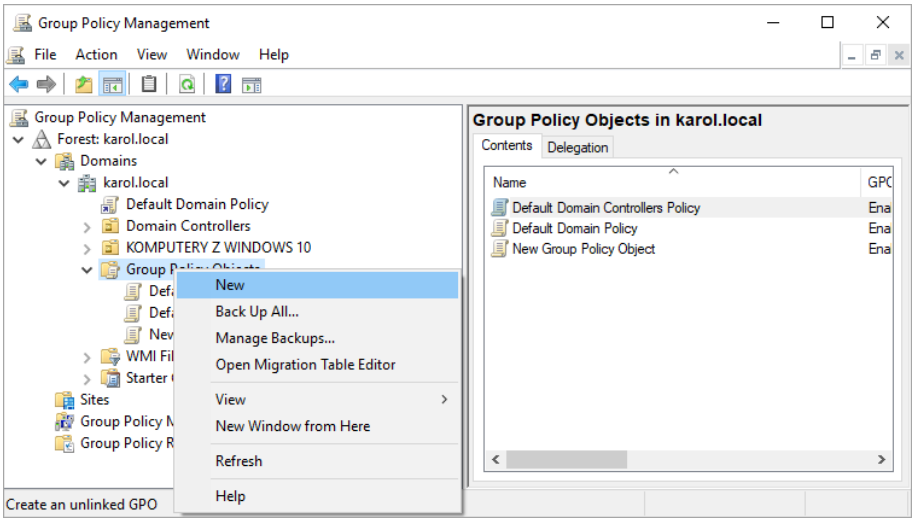


Go to ***Group Policy Objects*** – in order to do this, in the domain structure window, expand:

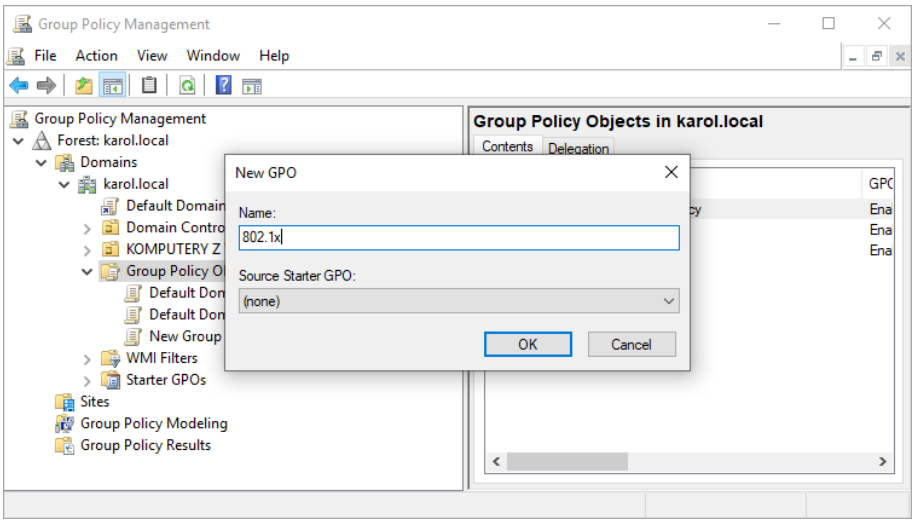
Forest > Domains > *selected domain or organizational unit.*



Right click on ***Group Policy Object*** and select: ***New***.

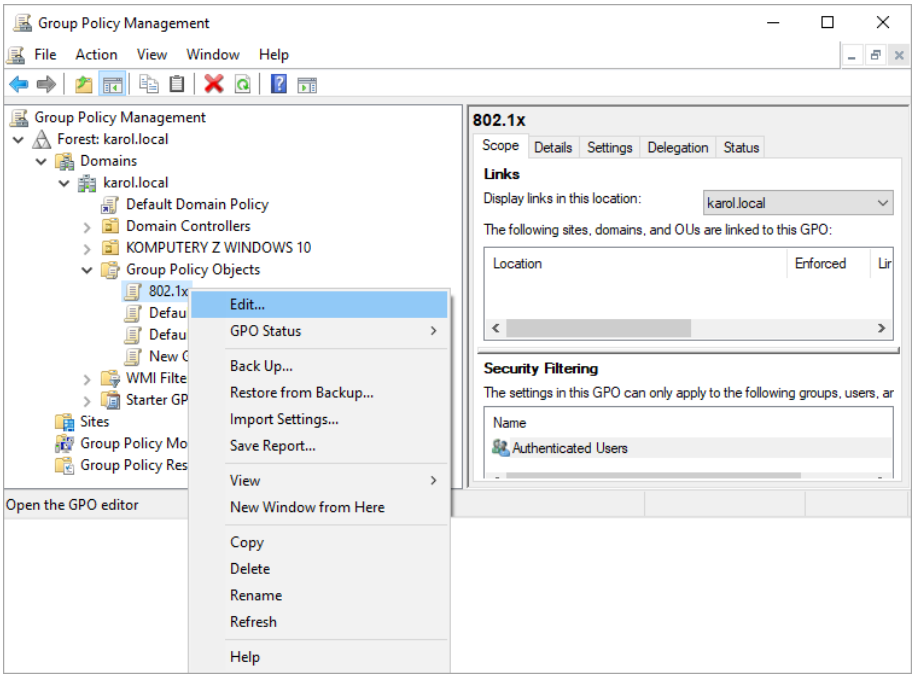


In the window that appears, enter a name for the new GPO and click ***OK***.

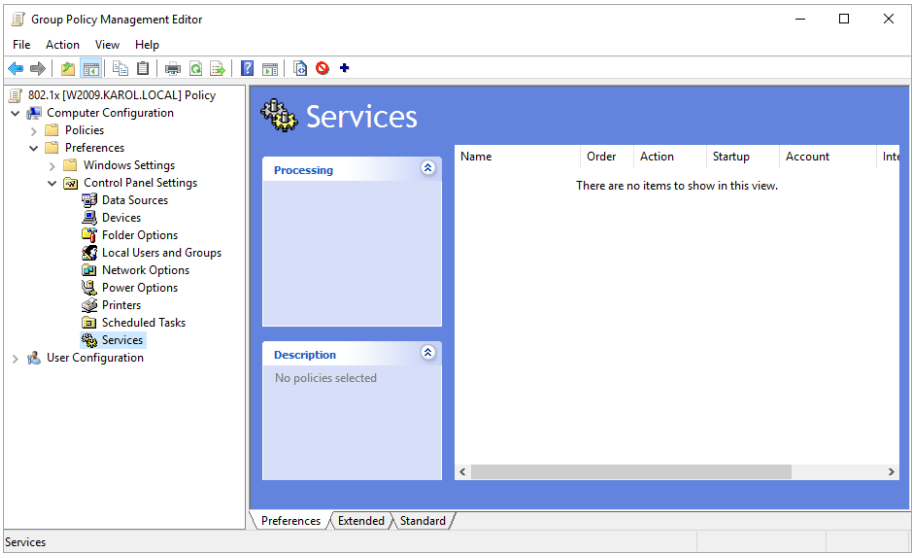


Select an option from the context menu and select: ***Edit…*** for the new

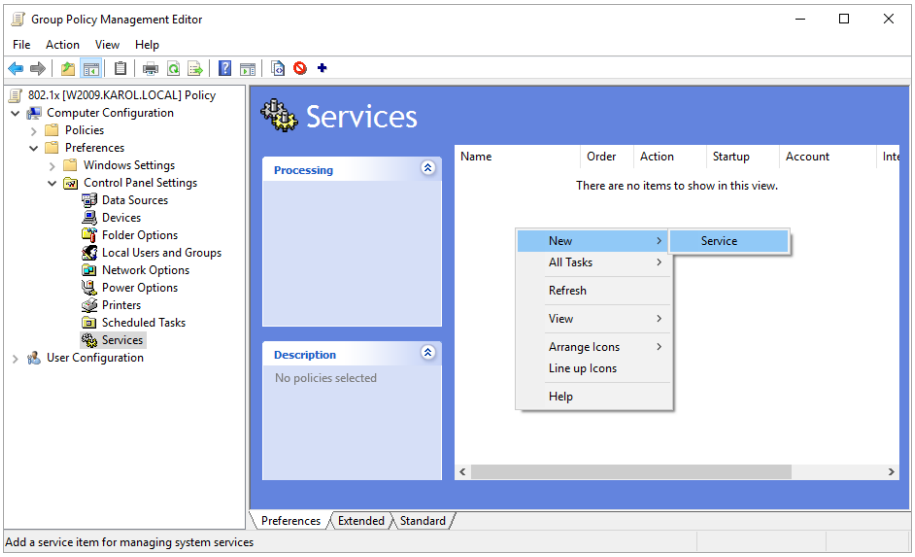
GPO:



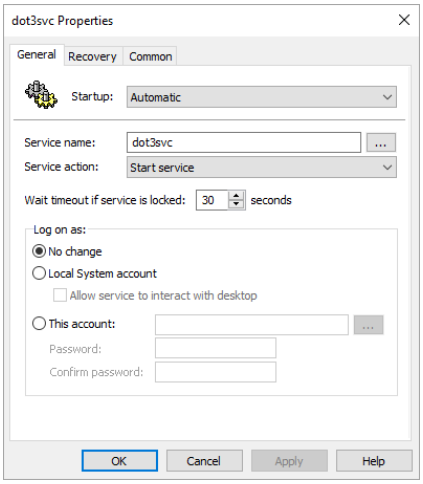
In the ***Group Policy Management Editor*** search for: ***Services*** (***Computer Configuration > Preferences > Control Panel Settings > Services***).



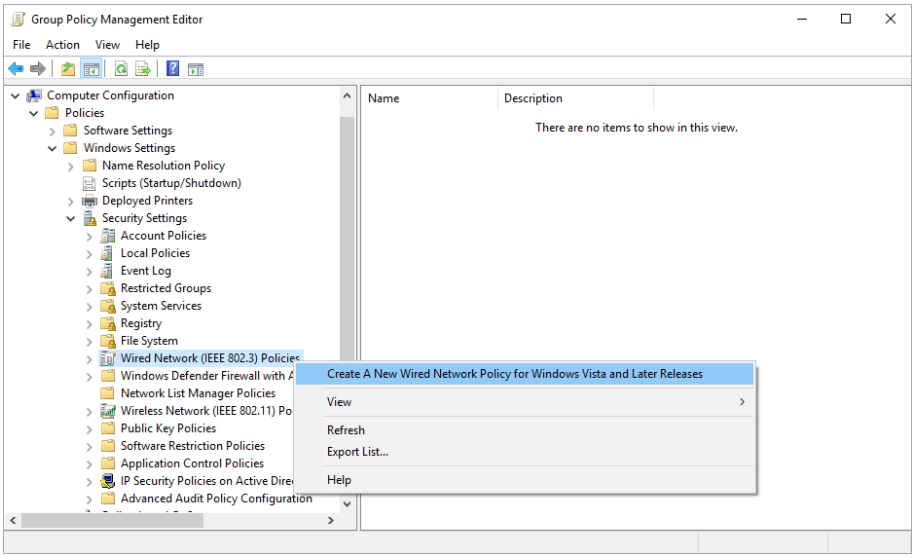
Select an option from the context menu select the ***New*** option and next: ***Service***.



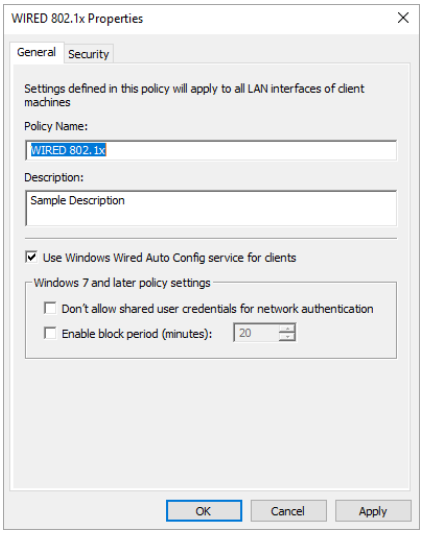
Set the parameters as on the screen below to configure the automatic start of the supplicant service on end-user computers with Windows. Leave the ***Recovery*** and ***Common*** tabs unchanged:



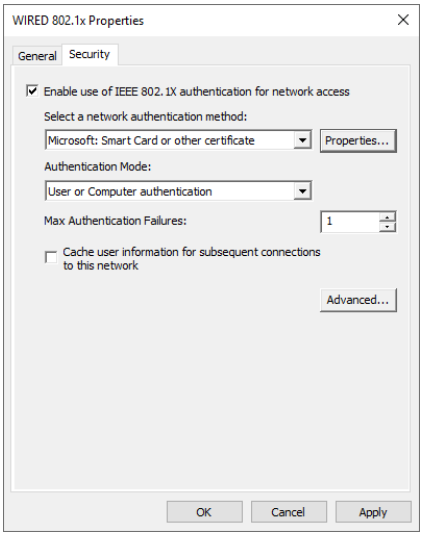
Go to security settings (***Computer Configuration > Policies > Windows Settings > Security Settings***), right click on ***Wired Network (IEEE 802.3) Policies*** and select: ***Create A New Wired Network Policy for Windows Vista and Later Releases.***



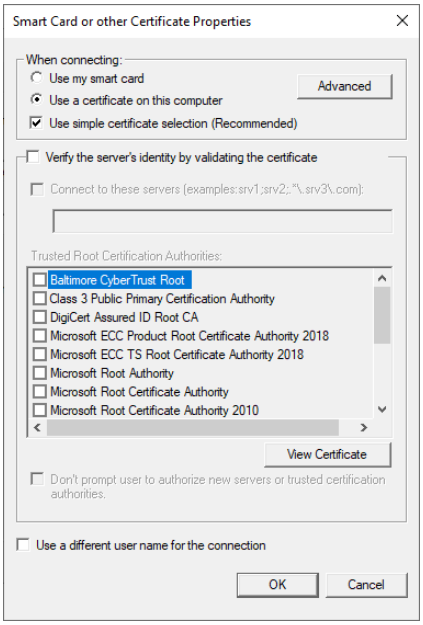
In the window that appears, in the ***General*** tab, give the new policy a name:



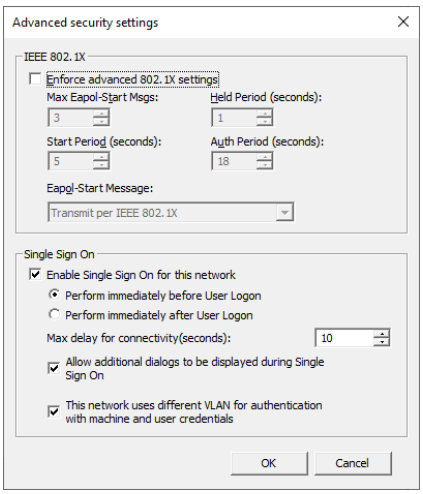
Now go to the ***Security*** tab and set parameters as shown on the screen below:



Click the ***Properties...*** button, then set parameters according to the screen below. Select a certificate from the list: **pki.enterprise.test** and confirm with ***OK***.

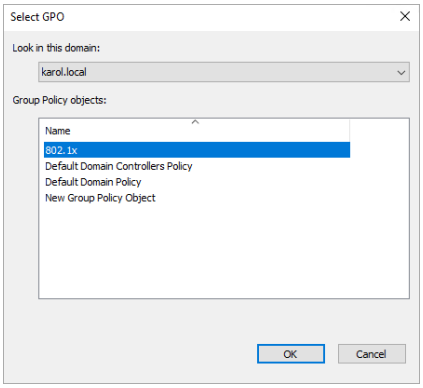


Click on ***Advanced…*** and set your parameteres as the below screen shows:

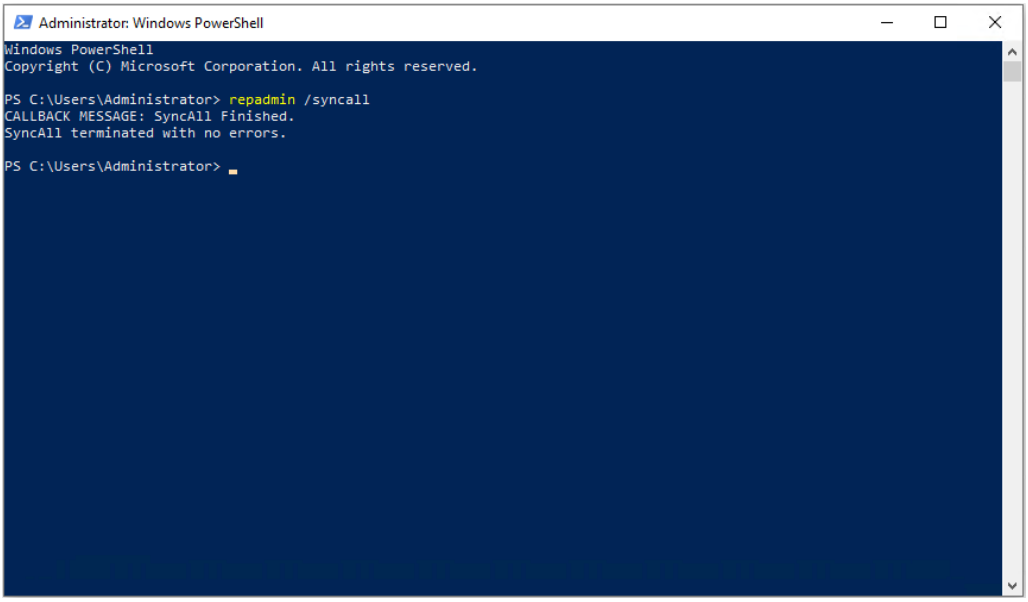


GPO is operational now. Close all modal windows now and confirm with ***OK***.

Now connect the new GPO to the existing group of objects (Test Division) to which the new settings are to be applied. To do this, right click on the given group of objects, and then select: ***Link an Existing GPO…*** Select the GPO you have just configured and click ***OK***:



In order to speed up the replication of the new GPO, run (with administrator privileges) PowerS-hell on the server where you configured it. Use the ***repadmin /syncall*** command and confirm. If replication is successful, you will see a message saying: '*SyncAll terminated with no errors*':



Wait for the settings to propagate to computers in the domain. From now on, the supplicant on the end devices is configured. For a larger network, you can add more policies to allocate appropriate resources based on identity, authorization type, and/or object groups.

To successfully authenticate computers and users with NACVIEW based on their certificates, request (from the workstation) separate certificates for these objects.

8.3.2. Verification of policies operation

After the correct configuration of network settings on the Windows 11 (NT-1) Test Machine, check on the network card whether the connection has been established. Verify in ***Authorization events*** whether there was a record of correct authorization and what type was used. Check what policy allowed, what VLAN, and what IP address was assigned.

```
cisco12(config-if)#do show dot1x users

                        MAC                Auth   Auth   Session         VLAN
Port     Username       Address            Method Server Time
-------- -------------- ------------------ ------ ------ --------------- ----
gi1      ENTERPRISE\Teste 00:0c:29:72:a6:1d 802.1X Remote 00:52:58       20
         rB
gi2      000c2932af54   00:0c:29:32:af:54 MAC    Remote 00:06:46       20
gi2      005056536a81   00:50:56:53:6a:81 MAC    Remote 00:52:04       20
cisco12(config-if)#
```

Log in to the network device and follow the instructions: **`show dot1x all summary`** oraz **`show dot1x interface gigabitEthernet 1/0/1 details`**.

More details in Cisco C1000: **`show authentication sessions interface gi1/0/1 det`**

Then log off the user from the system and repeat the steps as explained above.

9. Other settings

9.1. Backup

Select ***Backup*** from the list of wizards. Configure data and log backup to a remote location. To do this, go to editing and complete the form by entering the following data:

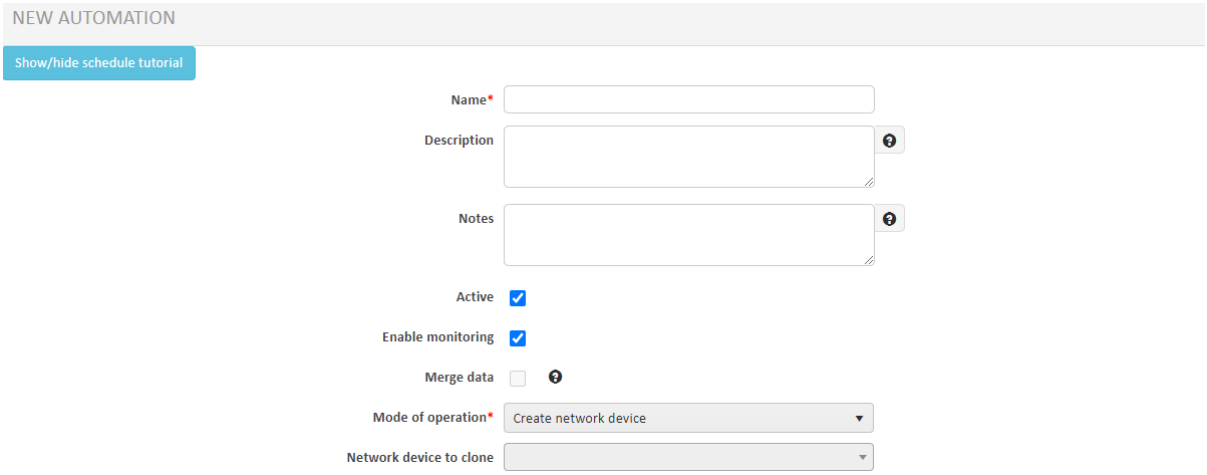
- **Protocol**: SMB
- **Protocol version**: 3.0
- **Remote host**: 10.XX.166.2
- **Directory**: \NV_Backup
- **Username**: administrator@enterprise.test
- **Password**: NACVIEW_SZKOLENIE22
- **Backup rotation**: enabled
- **Interval**: every month
- **Include logs**: No

Save your set values. To upload changes to the system, press: ***Run configuration***. The system will set the required parameters within 5 minutes.

9.2. Automation

From the NACVIEW main menu select: ***Automation*** (***Configuration*** section). Now click: ***Create new***, and next: ***Supplemetal Automation***. Complete the form with the following data:

- **Name**: Clone network devices
- **Mode of operation**: Create a network device
- **Subnetworks**: 10.XX.166.0/24
- **SNMP agent secret**: NVPrivate
- **Notification**: admin@nacview.com



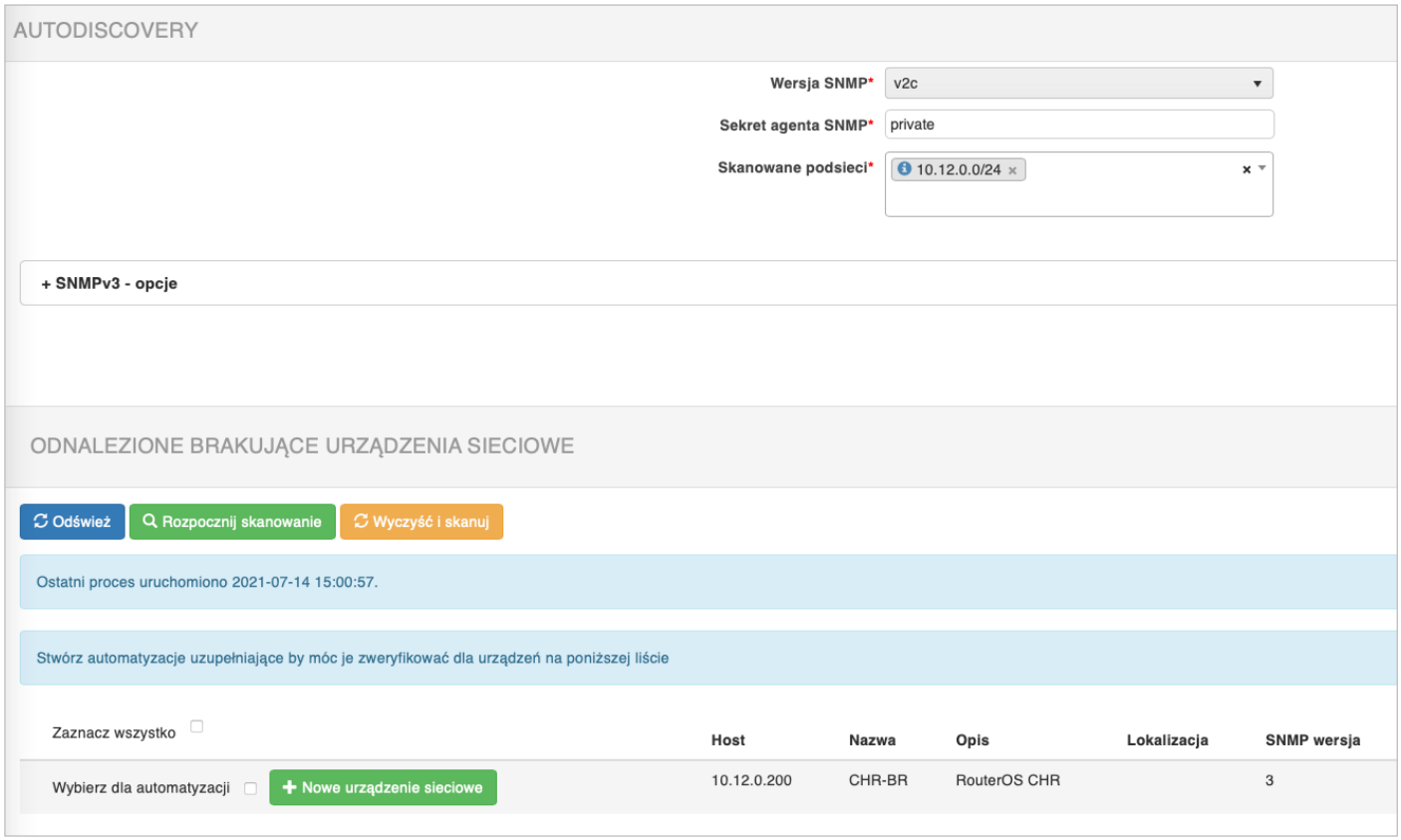
Now click ***Save*** to confirm your settings.

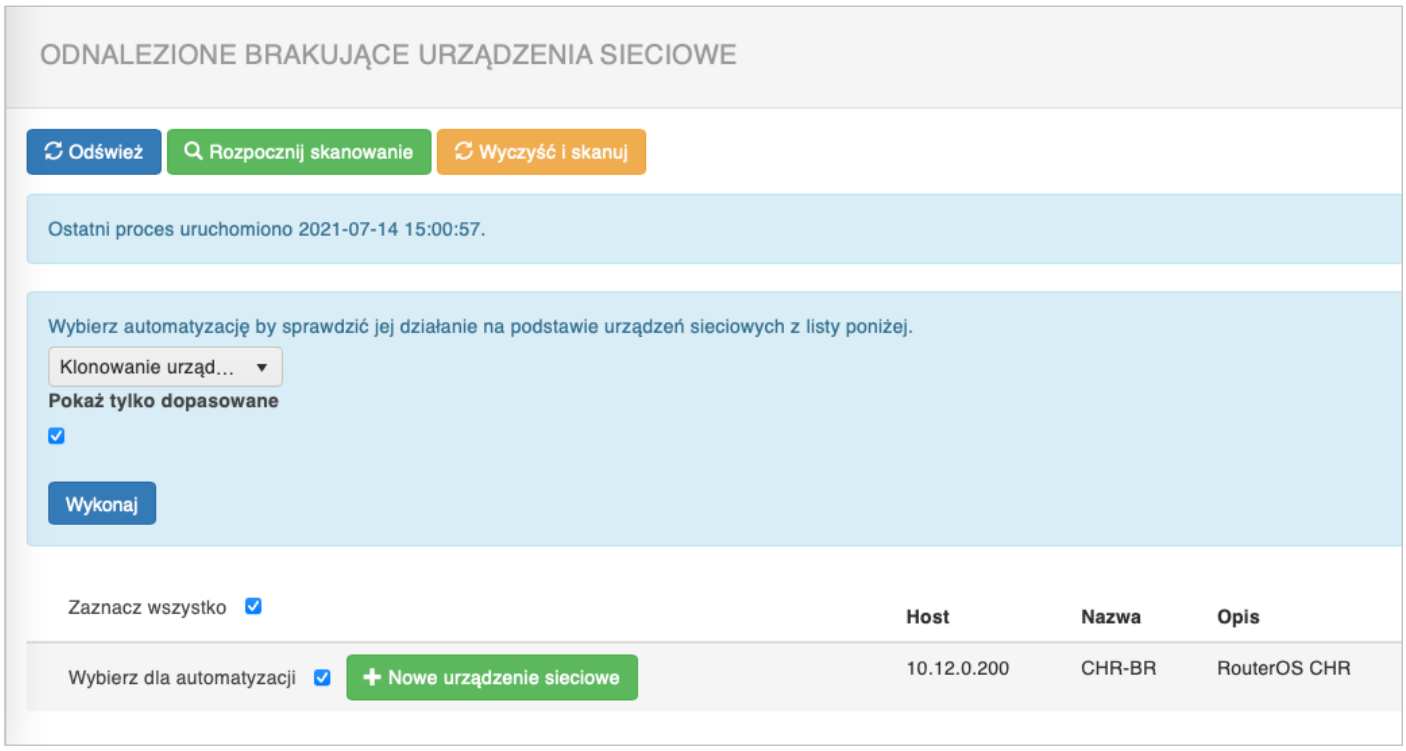
9.3. Autodiscovery

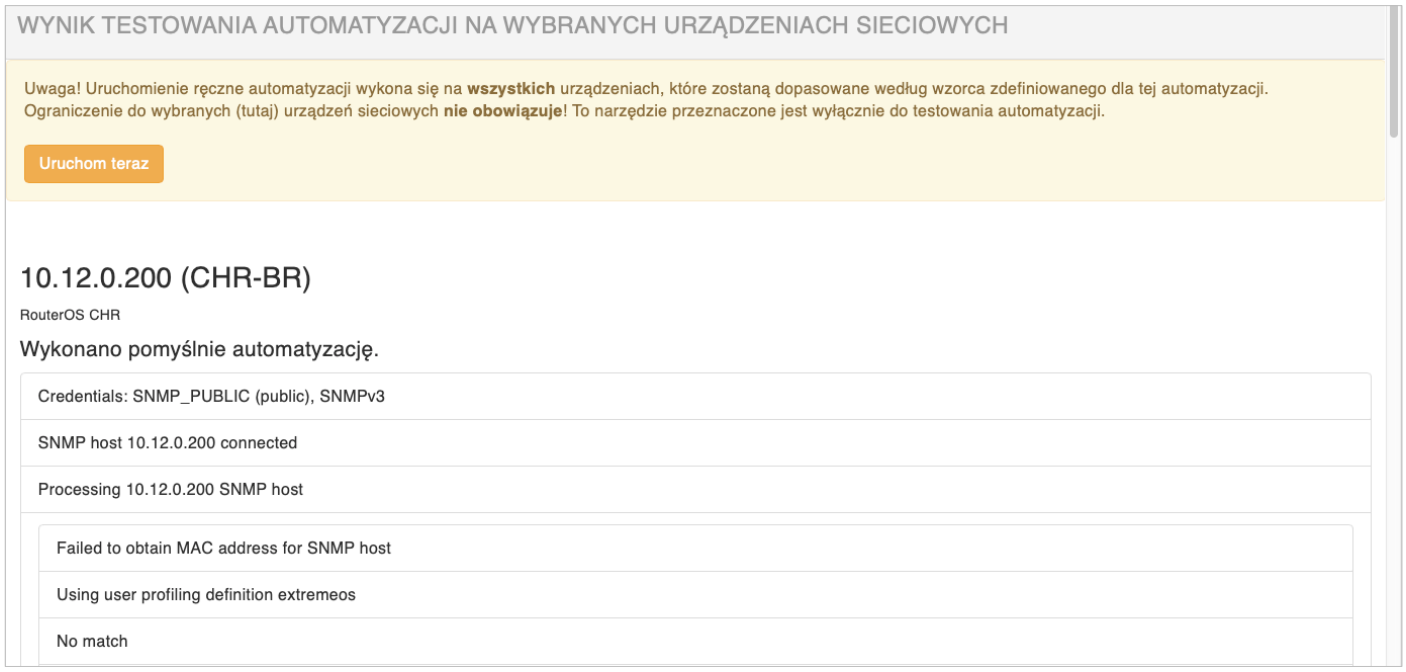
From the mani menu select: ***Autodiscovery***. Then filli in the form:

- **SNMP version**: v2c
- **SNMP agent secret**: NVPrivate
- **Subnetworks**: 10.XX.166.0/24

Click ***Save***, and next start scanning. The following message should be appear: '*The searching process for devices in subnets is active*!'. To see the found objects, click ***Refresh***. Select the found objects with the ***Select all*** box, and then select: ***Clone network devices*** from the drop-down menu. Click: ***Execute***. In the newly opened window, run automation simulation by clicking: ***Run now***.



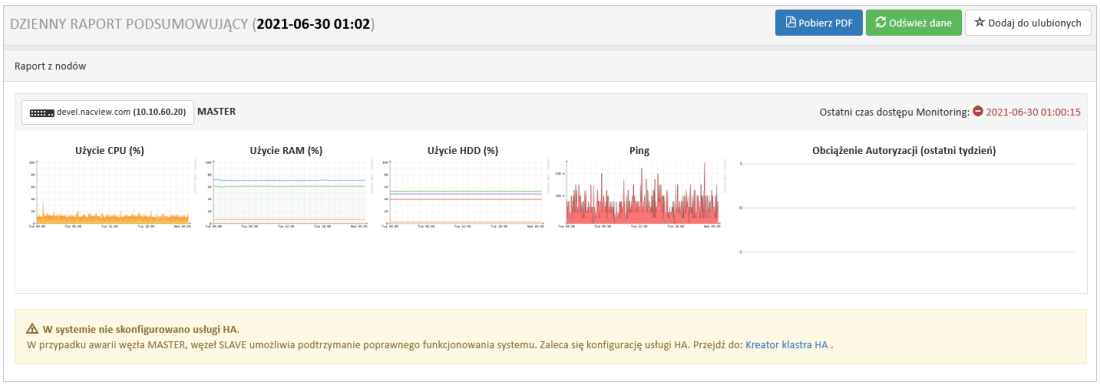




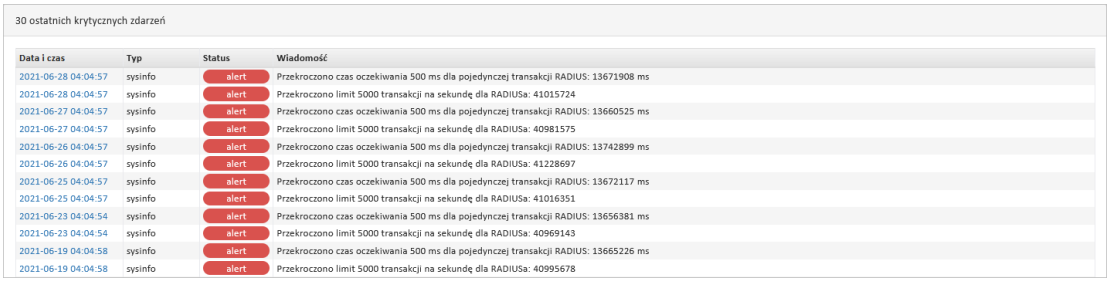
9.4. Daily report (system status)

In order to go to the daily report, select ***Summary report*** from the main menu in the ***Dashboard*** section. Go through all the sections in the report:

Nodes Report

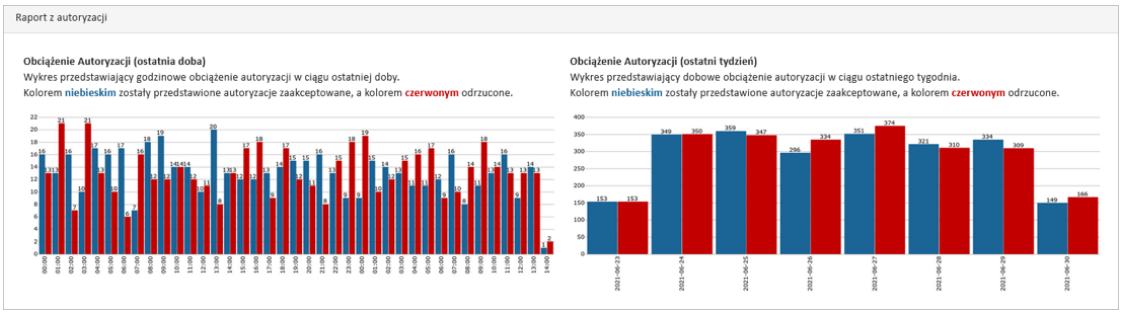


30 most recent critical events

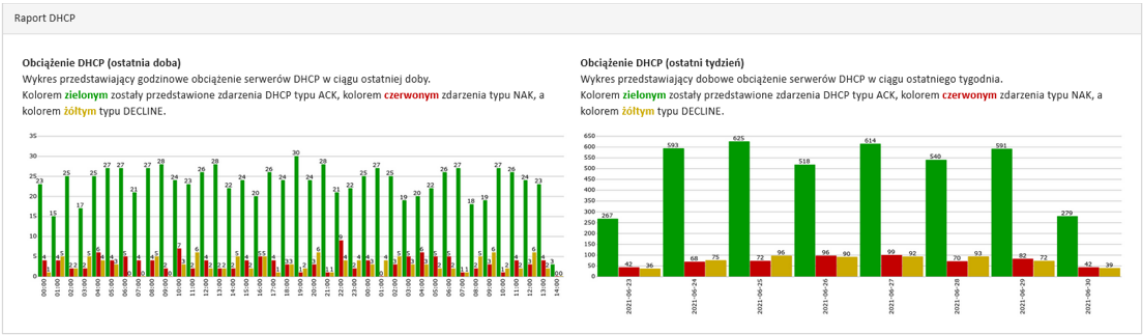


Data i czas	Typ	Status	Wiadomość
2021-06-28 04:04:57	sysinfo	alert	Przekroczono czas oczekiwania 500 ms dla pojedynczej transakcji RADIUS: 13671908 ms
2021-06-28 04:04:57	sysinfo	alert	Przekroczono limit 5000 transakcji na sekundę dla RADIUSa: 41015724
2021-06-27 04:04:57	sysinfo	alert	Przekroczono czas oczekiwania 500 ms dla pojedynczej transakcji RADIUS: 13660525 ms
2021-06-27 04:04:57	sysinfo	alert	Przekroczono limit 5000 transakcji na sekundę dla RADIUSa: 40981575
2021-06-26 04:04:57	sysinfo	alert	Przekroczono czas oczekiwania 500 ms dla pojedynczej transakcji RADIUS: 13742899 ms
2021-06-26 04:04:57	sysinfo	alert	Przekroczono limit 5000 transakcji na sekundę dla RADIUSa: 41228697
2021-06-25 04:04:57	sysinfo	alert	Przekroczono czas oczekiwania 500 ms dla pojedynczej transakcji RADIUS: 13672117 ms
2021-06-25 04:04:57	sysinfo	alert	Przekroczono limit 5000 transakcji na sekundę dla RADIUSa: 41016351
2021-06-23 04:04:54	sysinfo	alert	Przekroczono czas oczekiwania 500 ms dla pojedynczej transakcji RADIUS: 13656381 ms
2021-06-23 04:04:54	sysinfo	alert	Przekroczono limit 5000 transakcji na sekundę dla RADIUSa: 40969143
2021-06-19 04:04:58	sysinfo	alert	Przekroczono czas oczekiwania 500 ms dla pojedynczej transakcji RADIUS: 13665226 ms
2021-06-19 04:04:58	sysinfo	alert	Przekroczono limit 5000 transakcji na sekundę dla RADIUSa: 40995678

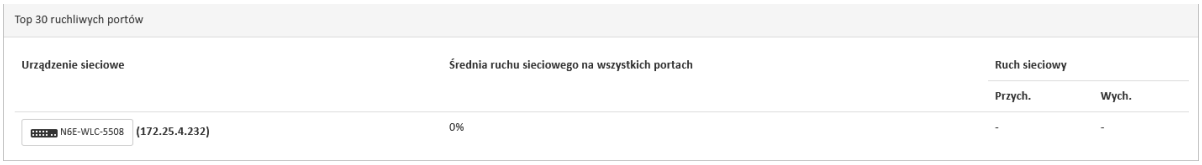
Authorization report



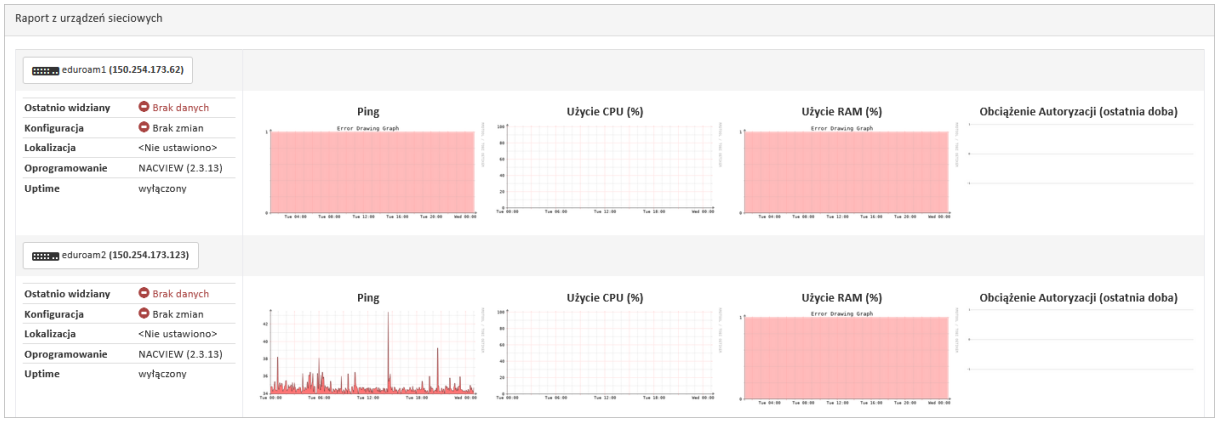
DHCP Report



Top 30 Busy Ports

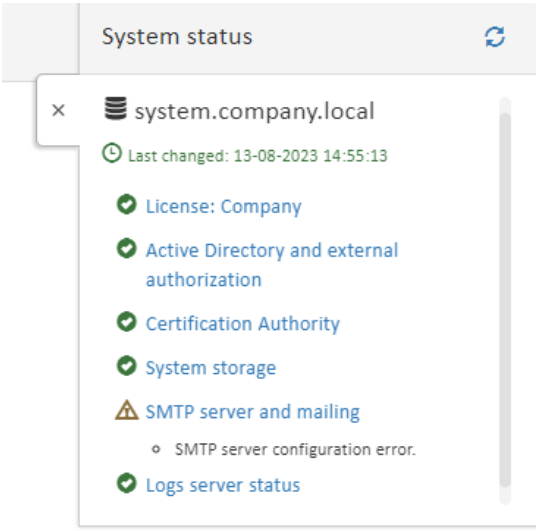


Network devices report



DHCPU untrusted servers

To view the system status, select  . the button from the navigation bar. Analyze the individual elements in this section.



9.5. E-mail templates

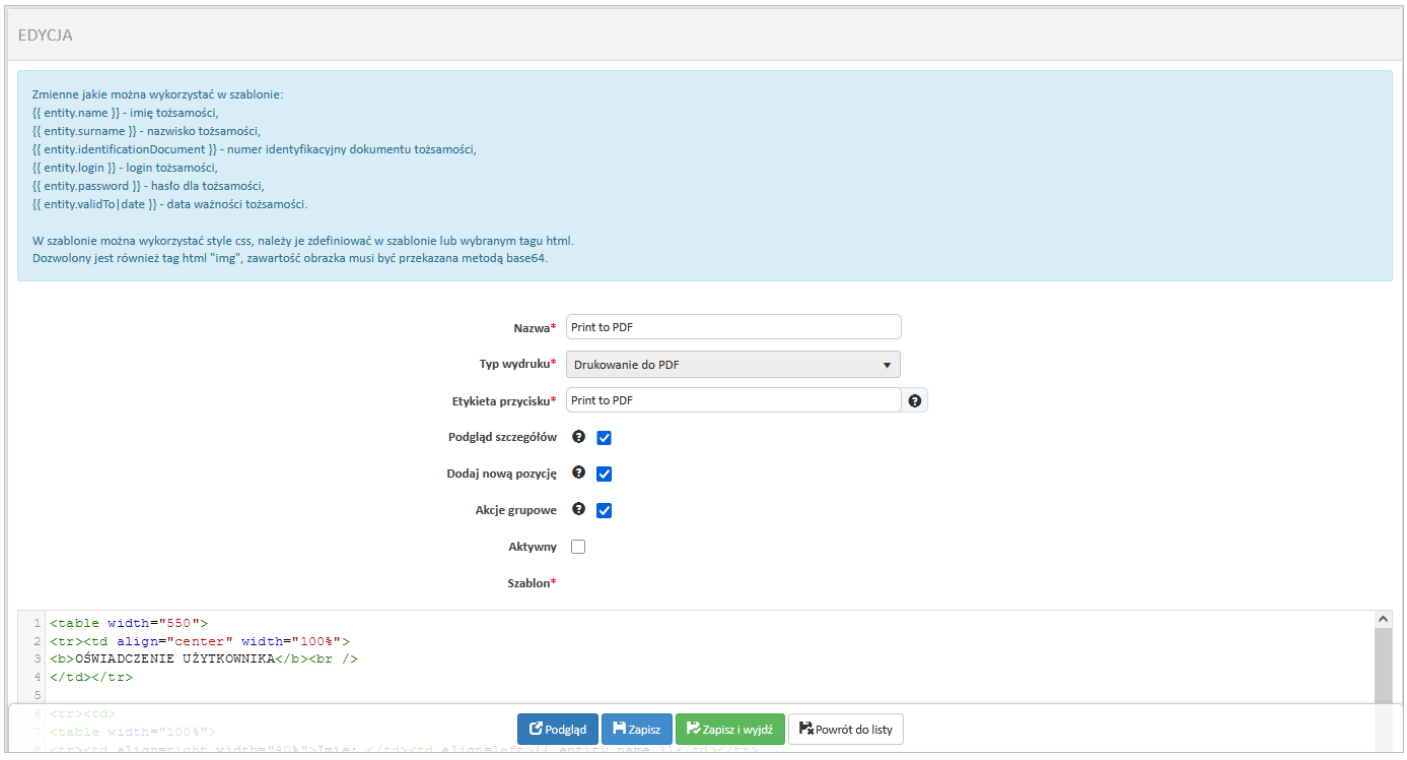
From the main menu select: ***E-mail template*** (***Administration*** section), and then, go to:

Manage global templates. To modify the value, click the edit button ( ) for the **PL** language - there is a default message template there, in HTML. You can freely modify it - just remember to keep the following code: {% block content %}{% endblock %}, which contains the content of the message. Modify the template content and click ***Preview*** to check your changes.

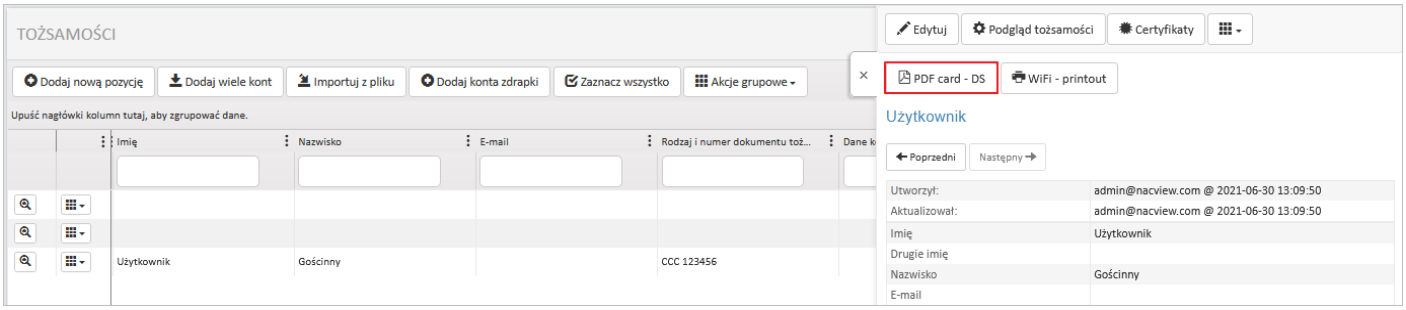
Finish editing by saving the template.

9.6. Printout templates

From the main menu select: ***Print Template*** (***Administration*** section). Then select the existing template and click ***Edit***. Change any value in the template and click ***Preview*** to check your changes:



Then select ***Identities*** from the main menu. Now click: and select: ***Print Card***.



Go back to the print template, change the print type to: ***Print to HTML*** and check the result as shown above.

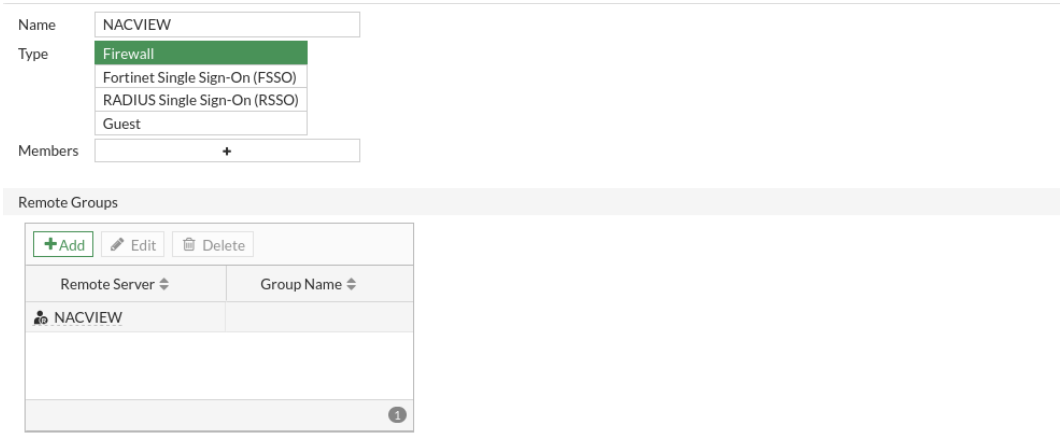
10. OTP Fortigate

10.1. FortiGate and NACVIEW Configuration

After you have got logged into the Fortigate 10.XX.166.21 CLI console (admin/NACVIEW_SZKOLENIE22), execute the following commands:

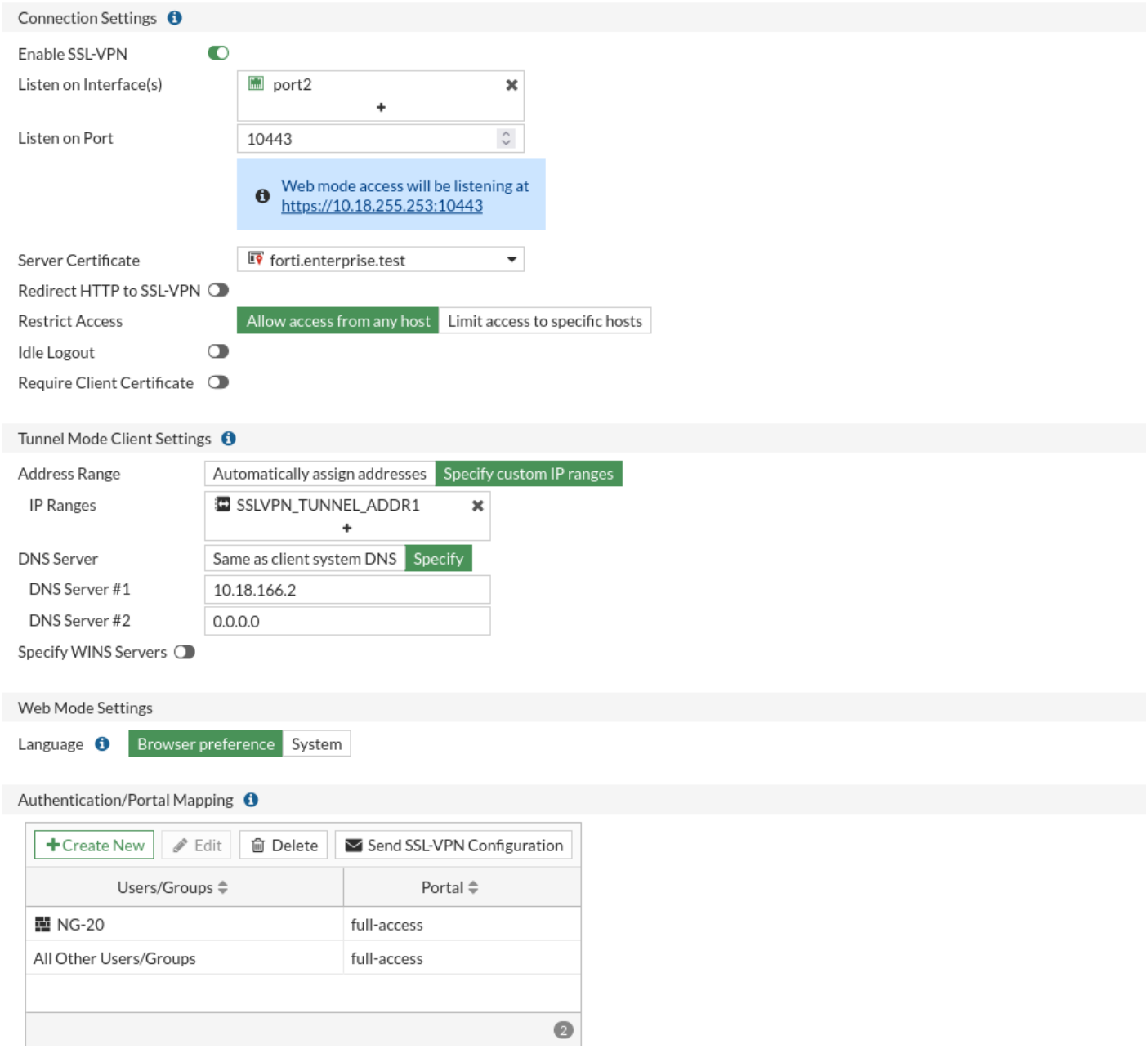
```
config system global
     set remoteauthtimeout 30
 end
 config user radius
 edit NACVIEW
        set server "10.XX.166.3"
        set secret NACVIEW_SZKOLENIE22
        set radius-port 1817
        set auth-type pap
    next
 end
```

After you have got logged into the GUI Fortigate https://10.XX.166.21 (admin/NACVIEW_SZKOLENIE22), go to menu: ***User & Authentication***, and next - to the ***User Groups*** tab. Create a new group with the ***+Create New*** button. Then set the parameters as shown in the picture below:

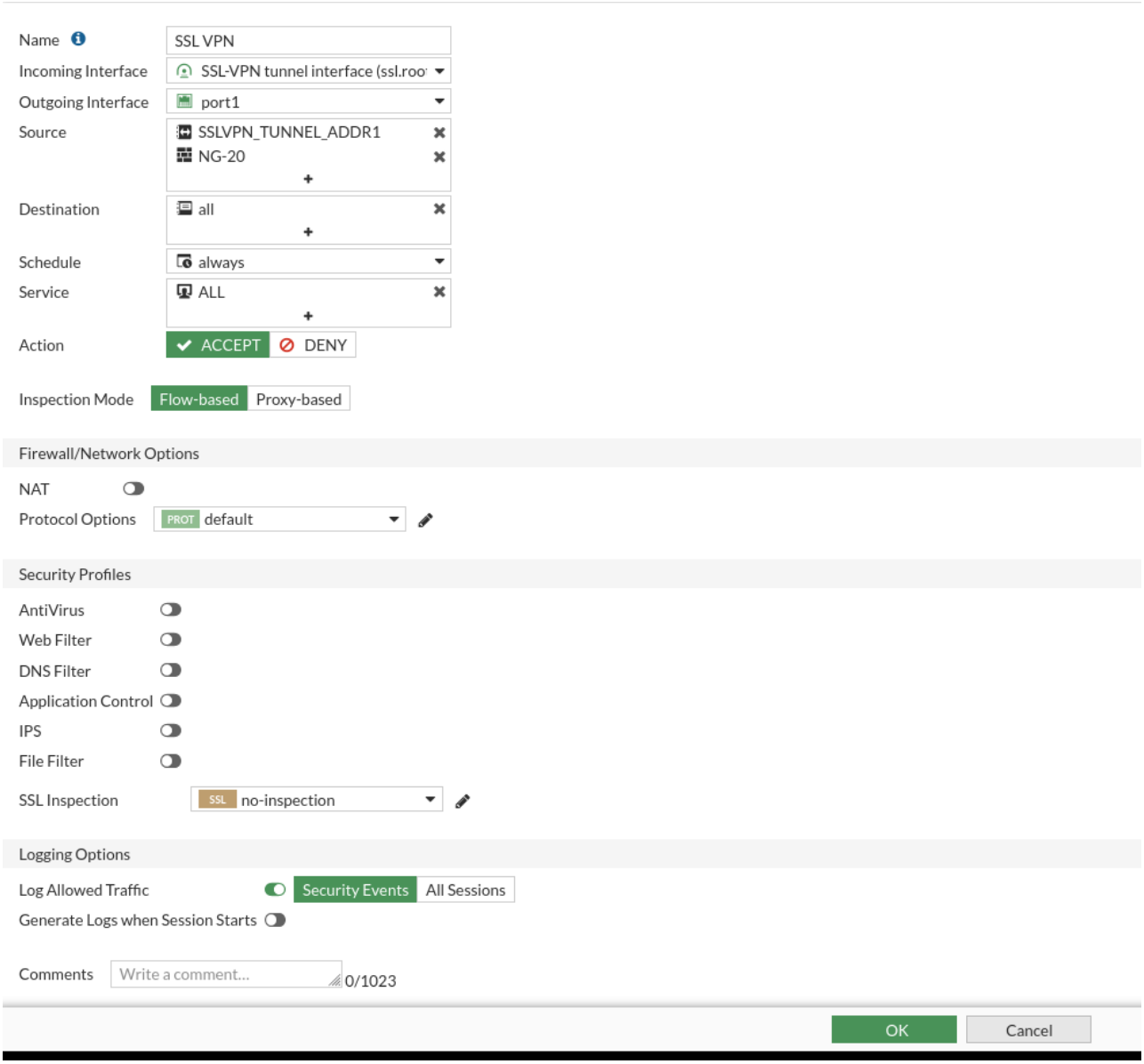


Go to the ***VPN*** menu, open the ***SSL-VPN Settings*** tab and configure the VPN connection settings as in the picture below. Go to the VPN menu, open the SSL-VPN Settings tab and configure the VPN connection settings as in the picture below.

Generate a new certificate for connections, name it e.g. **forti.enterprise.test**



In the next step, go to the ***Policy & Objects*** menu, to ***Firewall Policy*** tab. Add a new firewall rule with the buton. Add a new firewall rule with the ***+Create New*** button. Configure the settings as shown in the picture below:



Now confirm with ***OK***.

Go back to ***NACVIEW*** now. Open the menu and select: ***Network Devices*** (***Network*** section). Click: ***Create new Item***. Complete the fields: ***IP address***, ***Radius communication key*** (after clicking the ***Change/set password*** button), ***OTP Options*** (drop-down list at the end of the form), entering data for the FortiGate system:

Number of ports: **3**

IP address: **10.XX.166.21**

Name: **XX-FTG**

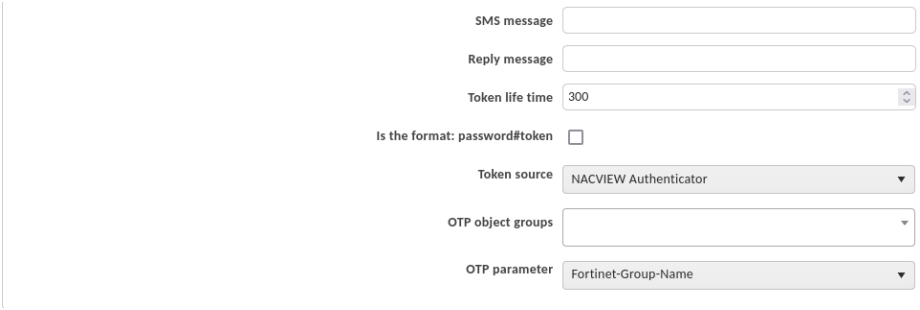
RADIUS key: **NACVIEW_SZKOLENIE22**

+OTP options:

Token source: **NACVIEW Authenticator**

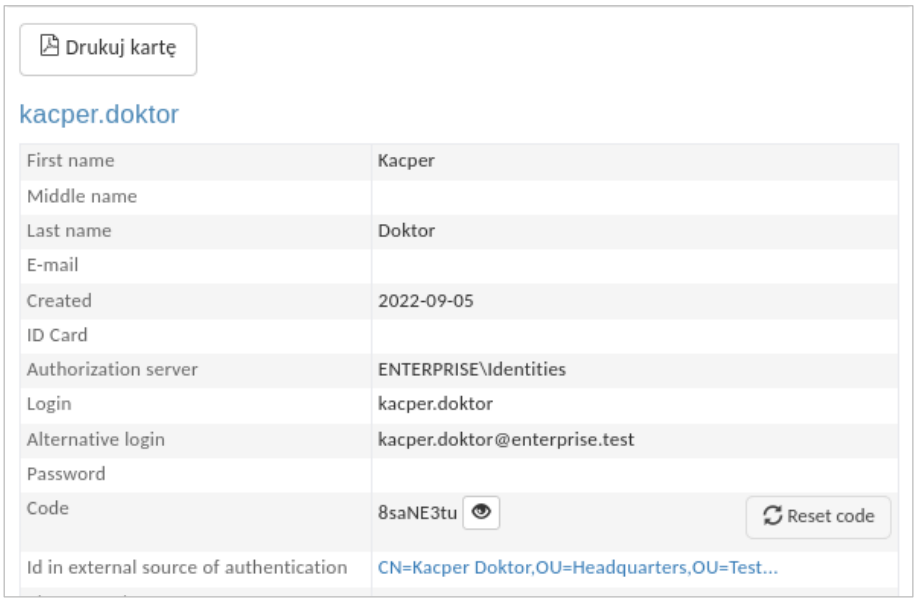
OTP parameter: **Fortinet-Group-Name**

Now save your set values.



10.2.Configuration of Nacview Authenticator application

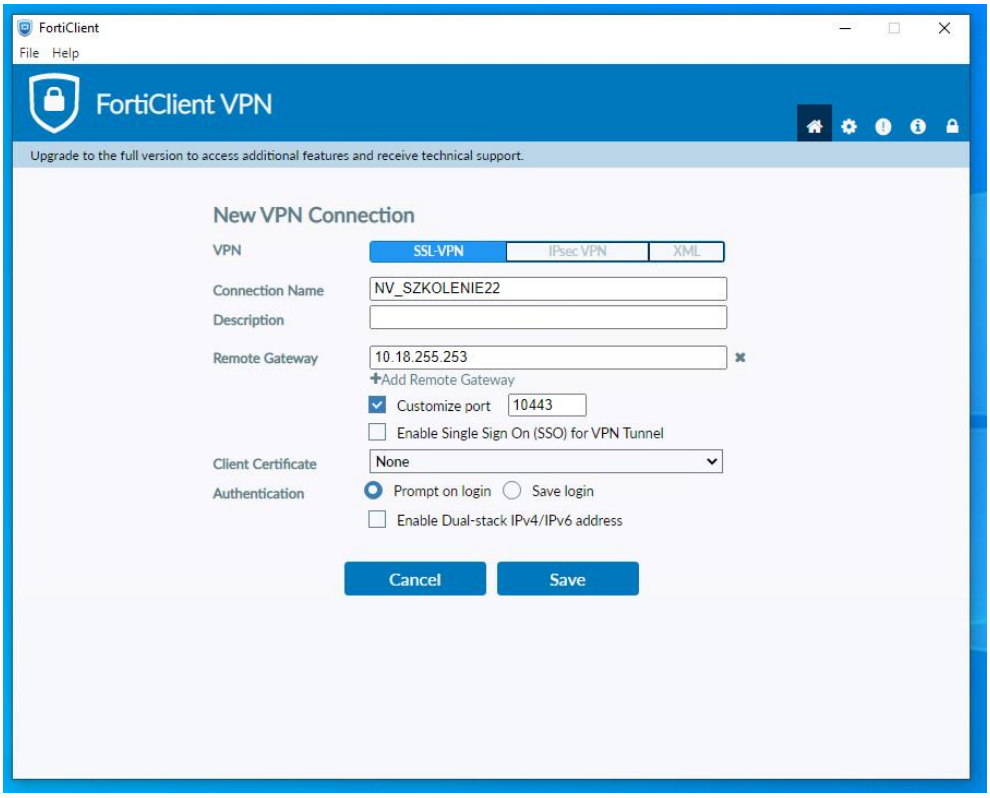
In the Nacview Authenticator application, you need to enter the login and the code, which can be checked in *Objects* → *Identities* → *Identity Details* (double-click on a specific identity) → *Code*. This code can also be found in the *Two-factor authentication* submenu. You must also provide a PIN to secure access to the application. After configuring the account, you can generate a one-time access code using the ***Generate*** button.



10.3. VPN Client Configuration

After you got logged in to the **XX-NT3** machine (login: TesterVPN, password: NACVIEW_SZKOLENIE22), enable FortiClient VPN and select: ***Configure VPN***.

Enter your connection details and click **Save**.



Afterwards, enter the user details previously configured in the NACVIEW Authenticator and click: *Connect.*