NACVIEW

OBSŁUGA SYSTEMU NACVIEW

Szkolenie dla administratorów sieci

NACVIEW

Spis treści

1. Wprowadzenie

Szkolenie obejmuje podstawowy zakres funkcjonalności systemu NACVIEW. Umożliwia naukę korzystania z interfejsu systemu oraz weryfikacji poprawności działania skonfigurowanych usług.

Dokumentacja szkoleniowa zawiera wszystkie aspekty jakie są niezbędne, aby wdrożyć w pełni działający system w organizacji w celu zabezpieczenia dostępu do sieci wewnętrznej.

1.1. Opis systemu

System NACVIEW to narzędzie do zarządzania dostępem użytkowników i urządzeń do sieci. Pozwala kontrolować urządzenia końcowe oraz tożsamości, które próbują uzyskać dostęp do zasobów sieciowych zarówno z sieci przewodowych, bezprzewodowych, jak i poprzez VPN.

Zasady dostępu są tworzone przy użyciu prostego interfejsu. Wszystkie zdarzenia są dostępne w formie graficznej, dzięki czemu monitorowanie aktywności poszczególnych użytkowników i urządzeń w sieci jest czytelne i przejrzyste.

System NACVIEW można wdrożyć w już istniejących sieciach, dzięki możliwości integracji z systemami zewnętrznymi (np. z AD lub z zaimplementowaną własną strukturą PKI). Wbudowane serwery (np. własny serwer CA, serwer DHCP, wewnętrzna baza użytkowników itp.) to z kolei świetne rozwiązanie dla dopiero powstających sieci, w których infrastruktura sieciowa wciąż wymaga implementacji.

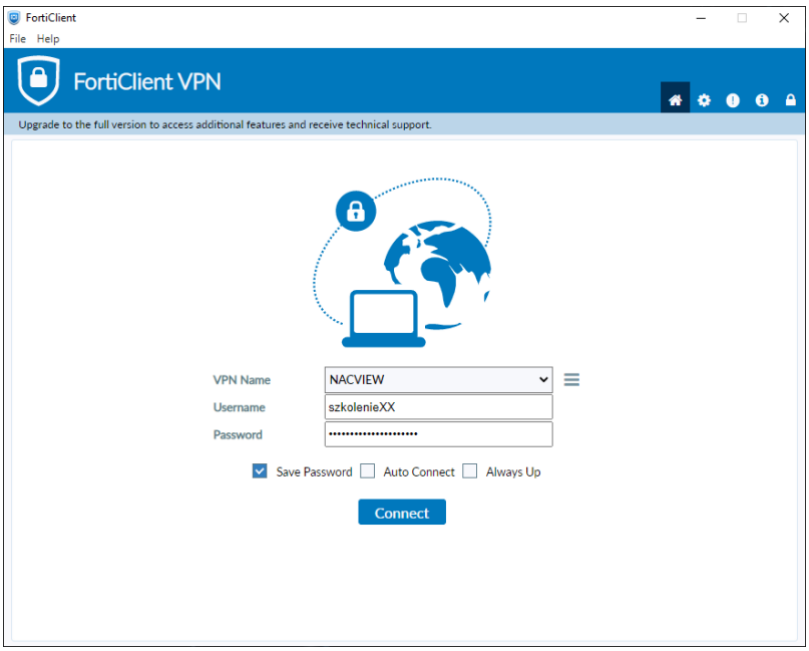
Ponadto, system NACVIEW umożliwia zarządzanie urządzeniami sieciowymi, na których przeprowadzana jest autoryzacja. Dzięki temu, administrowanie całą infrastrukturą sieciową jest możliwe w ramach jednej platformy.

1.2. Instalacja

1.2.1. Połączenie zdalne do środowiska szkoleniowego

Podłącz się swoim komputerem poprzez połączenie VPN do środowiska szkoleniowego NACVIEW. Pobierz **FortiClientVPNOnlineInstaller.exe** i zainstaluj. Skonfiguruj poświadczenia dla połączenia zgodnie z otrzymanymi danymi (Uwaga - w polu *Username* wpisz prawidłową nazwę użytkownika dla danego środowiska). Może być wymagany restart komputera, aby program działał prawidłowo.

W kolejnym kroku kliknij dwukrotnie niebieską ikonkę FortiClient znajdującą się w tray-u, wpisz hasło i uruchom połączenie przyciskiem Connect.



1.2.2. Instalator CLI

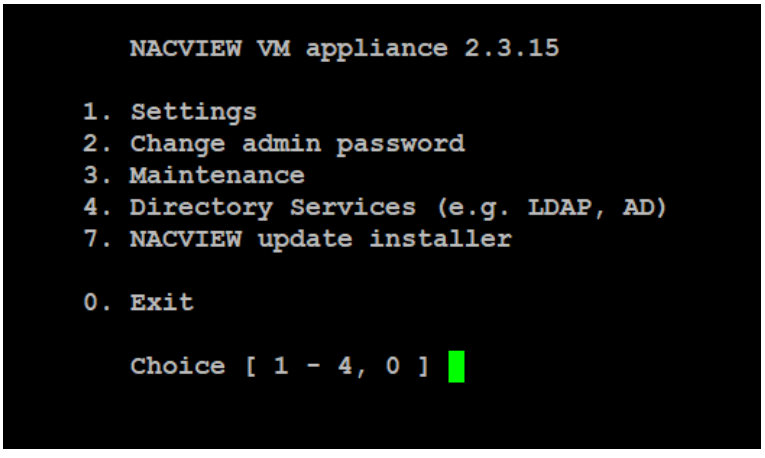
Uruchom przeglądarkę www i połącz się do Proxmox (dane dostępowe w tabeli 1.4). Wpisz adres **https://10.XX.166.9:8006** (login: admin, hasło: NACVIEW_SZKOLENIE22). Po zalogowaniu się do Proxmox przejdź do hosta **XX-MS** (master systemu NACVIEW).

Następnie wywołaj konsolę i zaloguj się do systemu, korzystając z poniższych danych.

Domyślne dane logowania do systemu:

- **Login**: admin
- **Hasło**: NACVIEW

Na ekranie powinno pojawić się główne menu instalatora. Wybierz opcję ***Settings***, wpisując odpowiednią cyfrę z menu.



Uzupełnij wyświetlony formularz, podając parametry:

- **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**: (brak)

Po zatwierdzeniu ustawionych parametrów przyciskiem ***Enter,*** na ekranie pojawi się podsumowanie. Jeśli wszystkie dane się zgadzają wpisz „***y***" i znów zatwierdź swoją odpowiedź przyciskiem ***Enter***. Wyjdź z instalatora wpisując „***y***" potwierdzając przyciskiem ***Enter***.

1.2.3. Instalator WWW

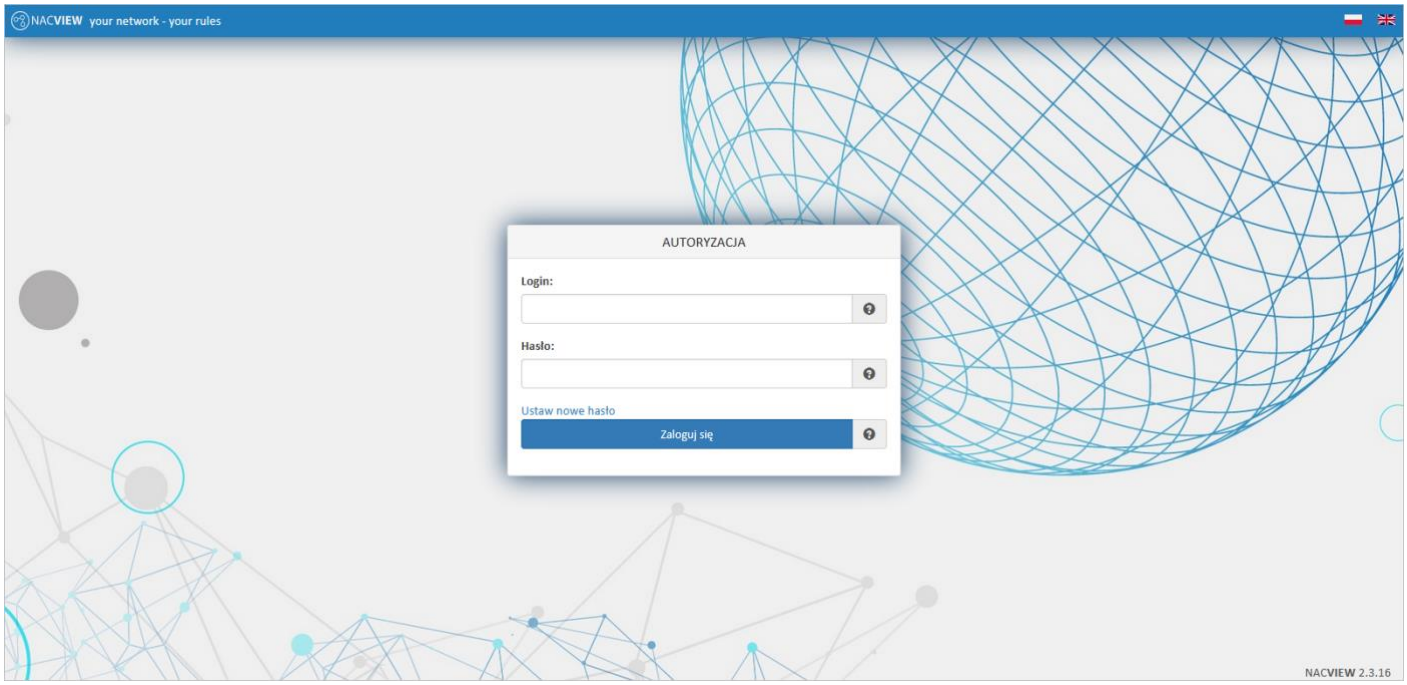
Po zakończeniu procesu instalacji za pomocą instalatora CLI, należy zalogować się do instalatora WWW i dokończyć instalację systemu. W tym celu należy skorzystać ze zdefiniowanego w konfiguratorze CLI adresu IP, loginu konta administracyjnego oraz hasła.

W oknie przeglądarki należy wpisać: **https://10.XX.166.4**

Domyślne dane logowania do panelu:

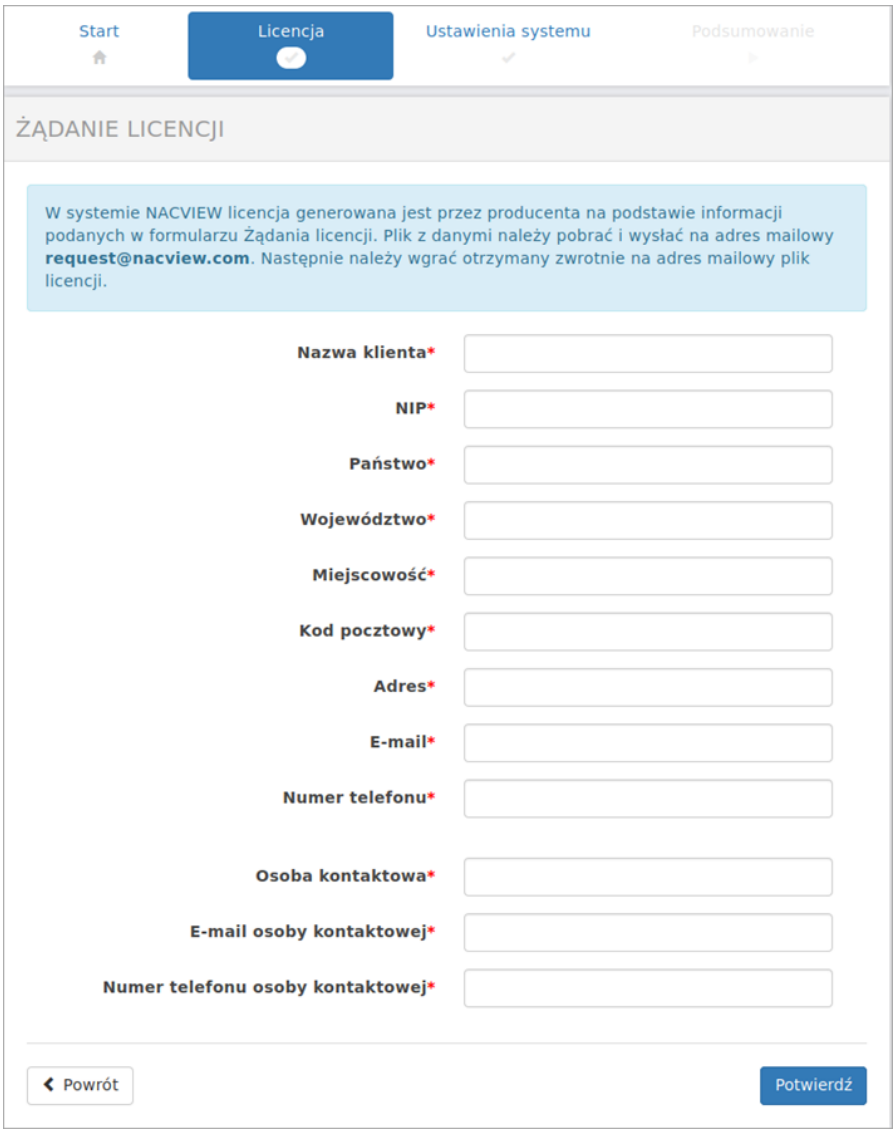
- **Login**: admin@nacview.com

- **Hasło**: NACVIEW

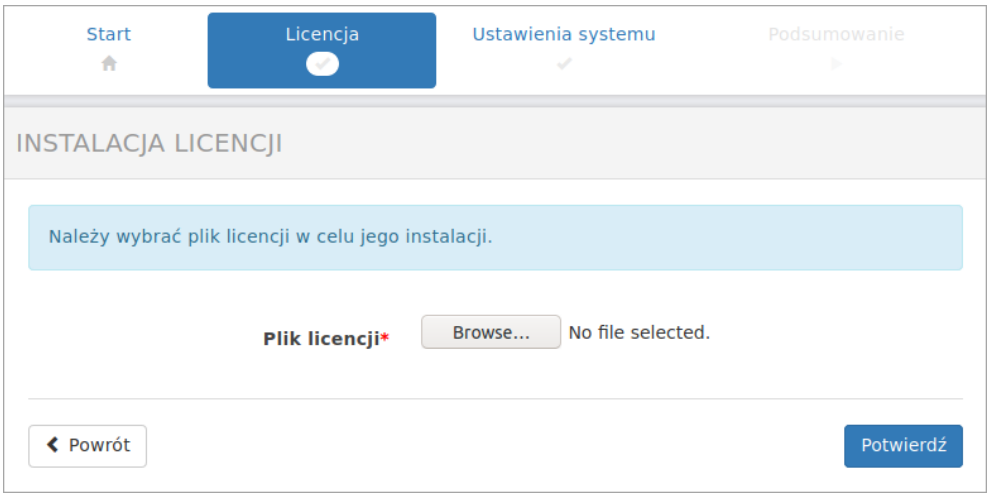


Po zalogowaniu pojawi się okno z menu instalatora WWW. W celu przejścia do Instalatora WWW, kliknij *Instalacja systemu*.

Kliknij w przycisk ***Licencja***, a następnie ***Żądanie licencji***. Uzupełnij wszystkie pola wyświetlonego formularza i zapisz wprowadzone dane. **Uwaga - jeśli posiadasz już plik licencyjny (np. otrzymany na potrzeby szkolenia) - zainstaluj go. Nie wypełniaj poniższego formularza, tylko wgraj otrzymany plik, jak pokazano na kolejnej stronie instrukcji.**

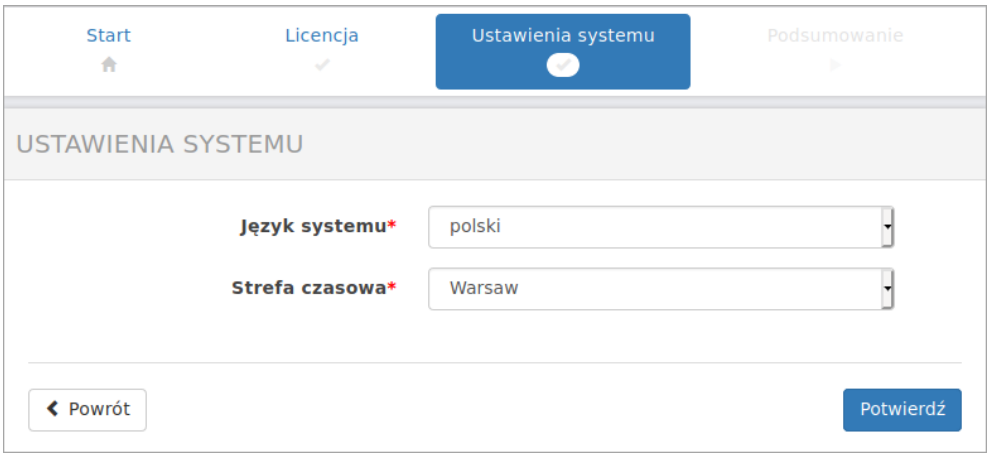


Pobierz na dysk wypełniony formularz. Następnie, wgraj do systemu plik z licencją. W tym celu kliknij ***Instalacja licencji*** i wybierz z dysku odpowiedni plik.



Kliknij ***Potwierdź***. Po poprawnym zainstalowaniu klucza licencyjnego, obok przycisku ***Instalacja licencji*** powinien pojawić się status: *skonfigurowano*. Powróć do okna ***Instalacja systemu***.

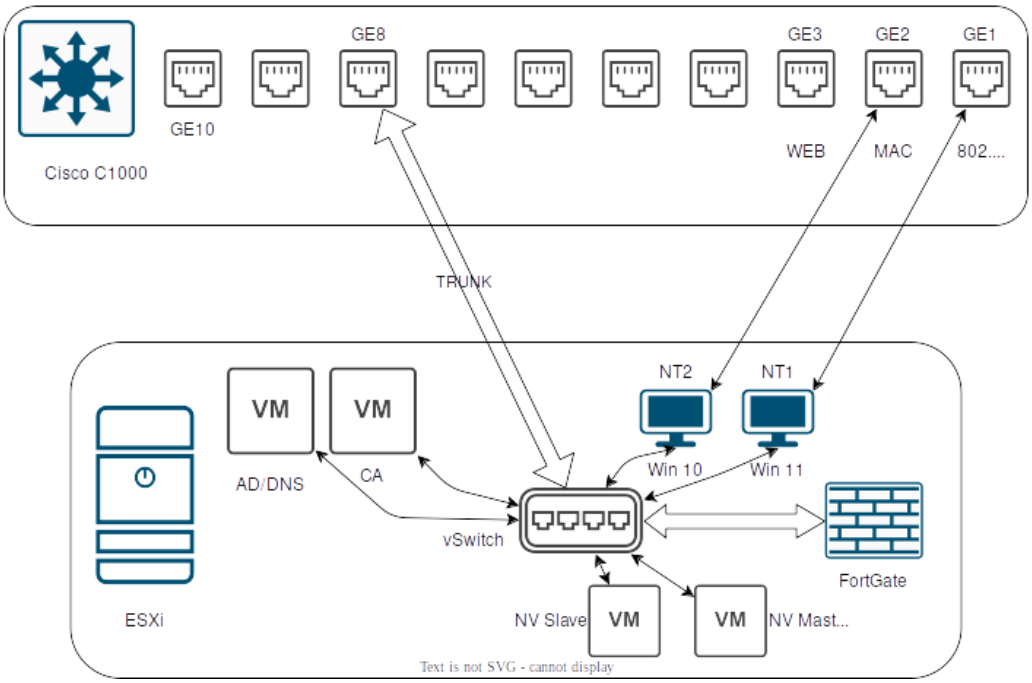
Ostatnim etapem konfiguracji są ustawienia systemu. W tym miejscu możesz określić jaki będzie domyślny język systemu NACVIEW, a także wybrać strefę czasową, w której będzie pracował system.



Po przejściu wszystkich etapów konfiguracji zostanie odblokowany przycisk ***Podsumowanie***. W oknie podsumowania wyświetlą się informacje skonfigurowane w poszczególnych etapach. Jeśli wszystkie dane się zgadzają, kliknij ***Instaluj***. Proces instalacji może trwać ok. 10 minut. W trakcie instalacji nie należy wyłączać maszyny.

1.3. Struktura połączeniowa środowiska szkoleniowego

1.3.1. Schemat



1.3.2. Adresacja

Nazwa	Adres IP
Cisco C1000 (Gateway)	10.XX.166.1
alpha.enterprise.test (AD / DNS, XX-DC)	10.XX.166.2
Adres IP VRRP dla HA	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
Serwer wirtualizacji Proxmox	10.XX.166.9:8006
FortiGate (XX-FTG)	10.XX.166.21
Resources	10.XX.166.1/24
Autoryzacja I	10.XX.80.1/24
Autoryzacja II	10.XX.88.1/24
Autoryzacja V	10.XX.126.1/24
CP L2	10.XX.96.1/24
CP L3	10.XX.104.1/24
Sieć gościnna	10.XX.120.1/24

1.4. Dane dostępowe

Nazwa	Użytkownik	Hasło	Adres IP	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	-	-	-
Kontroler domeny: ENTERPRISE	administrator@enterprise.test	NACVIEW_SZKOLENIE22	10.XX.166.2	-	-	-
Urządzenie sieciowe (Cisco C1000, FortiGate)	admin	NACVIEW_SZKOLENIE22	10.XX.166.1	NACVIEW_SZKOLENIE22	NVPrivate	NACVIEW_SZKOLENIE22
Użytkownik testowy (OU Reserach and Development)	ENTERPRISE\TesterR&D	NACVIEW_SZKOLENIE22	-	-	-	-
Użytkownik testowy (OU NetworkOperations)	ENTERPRISE\TesterNO	NACVIEW_SZKOLENIE22	-	-	-	-
Użytkownik testowy (grupa Accounting)	ENTERPRISE\AccountantOne	NACVIEW_SZKOLENIE22	-	-	-	-
Hyperwizor Proxmox	admin	NACVIEW_SZKOLENIE22	10.XX.166.9:8006	-	NVPrivate	-

2. Kreatory

2.1. Certyfikat zewnętrzny

Kliknij na przycisk ***Kreatory***  , znajdujący się na górnym pasku strony. Z rozwiniętej listy kreatorów wybierz opcję ***Urząd certyfikacji CA***, a następnie kliknij ***Dodaj nową pozycję***. W kolejnym oknie wybierz ***Zewnętrzny urząd CA + zapytanie CSR***.

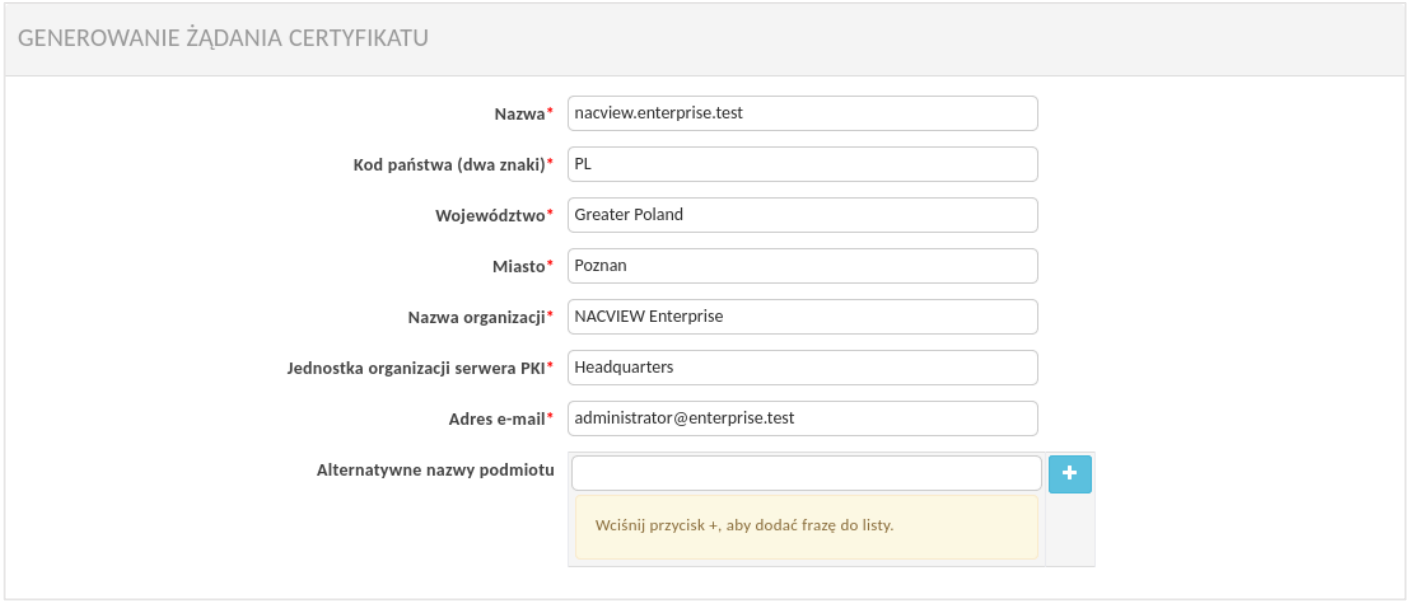
Kliknij ***Edytuj ustawienia*** i wypełnij formularz następującymi danymi:

- **Aktywny:** Tak
- **Czy domyślny:** Nie
- **Aktywny dla obiektów:** Nie
- **Wykorzystywany dla WWW:** Nie
- **Czy OCSP aktywne**: Nie
- **Czy SCEP aktywny:** Nie
- **URL for CRL:** http://beta.enterprise.test/CertEnroll/enterprise-BETA-CA.crl

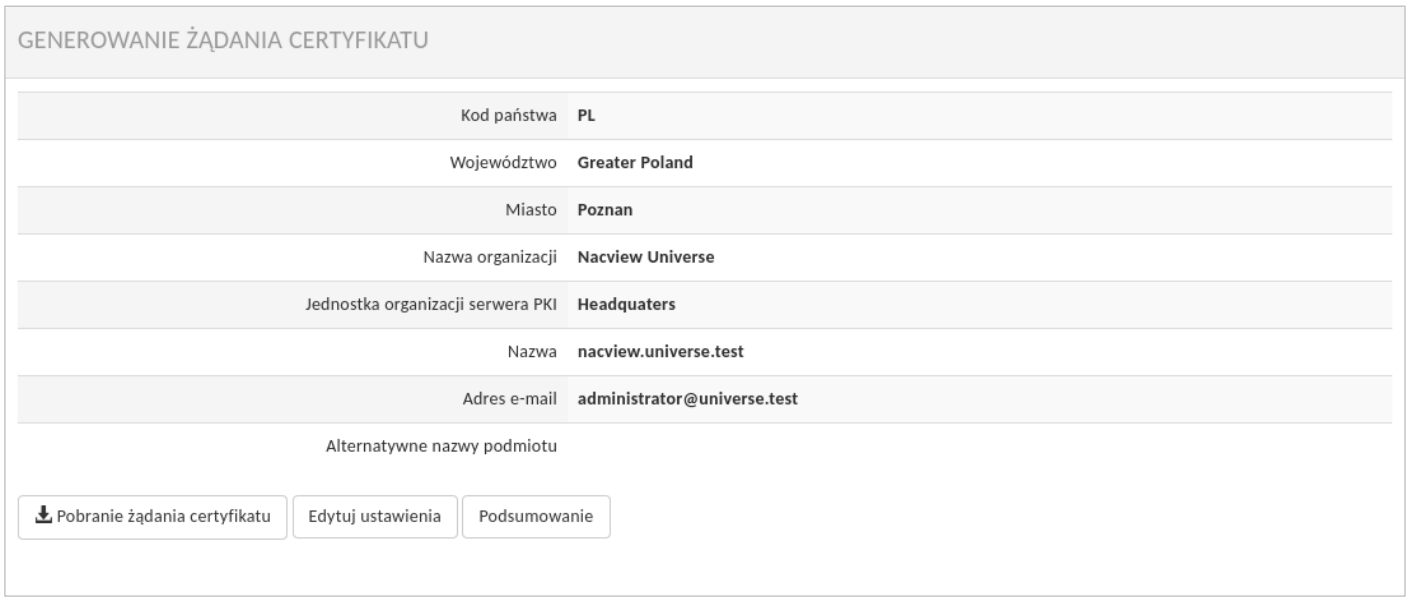
Zapisz wprowadzone zmiany.

Po zaimportowaniu pliku certyfikatu zmienia się kolor ramki na zielony oraz wyświetla się informacja, jaki plik został wgrany.

Zacznij od skonfigurowania żądania podpisania certyfikatu (kliknij ostatni przycisk na podświetlonej na czerwono liście).



Zatwierdź przyciskiem ***Potwierdź*** u dołu ekranu. Kolejnym krokiem jest podpisanie CSR. W tym celu należy pobrać CSR przyciskiem ***Pobranie żądania certyfikatu***.



Następnie wejdź na adres http://beta.enterprise.test/certsrv (**http://10.XX.166.6/certsrv)** i wybierz opcję ***Request a certificate***. Jeśli strona wymaga podania danych logowania, wpisz login: **ENTERPRISE\Administrator** oraz hasło: **NACVIEW_SZKOLENIE22**

Z wyświetlonych opcji wybierz *submit an* ***advanced certificate request***.

W pole ***Saved request*** wklej zawartość pobranego CSR - można go otworzyć np. za pomocą narzędzia Notepad++. W dalszej kolejności z listy możliwych certyfikatów wybierz ***Web server*** i zatwierdź przyciskiem ***Submit***. Uzyskany certyfikat należy pobrać w formacie ***Base64.***

Z okna żądania certyfikatu wyjdź przyciskiem ***Podsumowanie***. Certyfikat CA można uzyskać, wchodząc na adres http://beta.enterprise.test/certsrv (**http://10.XX.166.6/certsrv)** i wybierając ***Download a CA certificate, certificate chain, or CRL***. Następnie wybierz urząd certyfikacji (***pki.enterprise.test***) oraz kodowanie ***Base64***. Certyfikat pobierz za pomocą przycisku ***Download CA certificate***. Następnie dodaj odpowiednie pliki do systemu (na dole okna) przechodząc kolejno ścieżki:

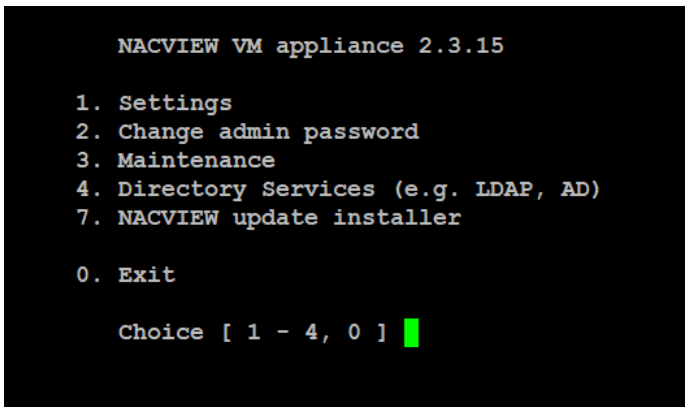
Certyfikat CA →Wybierz plik → Prześlij pliki →Podsumowanie

Certyfikat serwera → Wybierz plik → Prześlij pliki → Podsumowanie

Po poprawnym wgraniu wszystkich plików, na dole okna powinien pojawić się przycisk ***Zatwierdź konfigurację.*** Naciśnij go, aby zainstalować pliki. System w ciągu 5 minut ustawi żądane parametry.

Aby dokończyć wprowadzanie zmian, przejdź ponownie do kreatora ***Urzędy certyfikacji CA*** i kliknij przycisk ***Zainstaluj konfiguracje***, znajdujący się w prawym górnym rogu. W nowo otwartym oknie naciśnij ***Zastosuj konfiguracje***. Poczekaj około 10 minut na wprowadzenie zmian.

2.2. Klaster HA



Przejdź do drugiego noda NACVIEW (maszyna XX-SL).

Następnie zaloguj się do konsoli. Wybierz opcję ***Settings***, wpisując odpowiednią cyfrę z menu.

Uzupełnij wyświetlony formularz, podając parametry:

- **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**: (brak)

Po zatwierdzeniu ustawionych parametrów przyciskiem ***Enter,*** na ekranie pojawi się podsumowanie. Jeśli wszystkie dane się zgadzają wpisz „***y***" i znów zatwierdź swoją odpowiedź przyciskiem ***Enter***. Wyjdź z instalatora wpisując „***y***" potwierdzając przyciskiem ***Enter***.

Przejdź do systemu NACVIEW. Z listy kreatorów wybierz opcję ***Klaster HA***. Przejdź do edycji i dodaj konfigurację dla węzła Slave. W tym celu uzupełnij formularz następującymi danymi:

- **Adres IP:** 10.XX.166.5
- **Typ noda:** HA
- **Login:** admin
- **Hasło:** NACVIEW
- **Strefa czasowa:** Warsaw
- **DNS IP:** 10.XX.166.2
- **Adres IP VRRP:** 10.XX.166.3
- **Prefiks podsieci VRRP:** 24

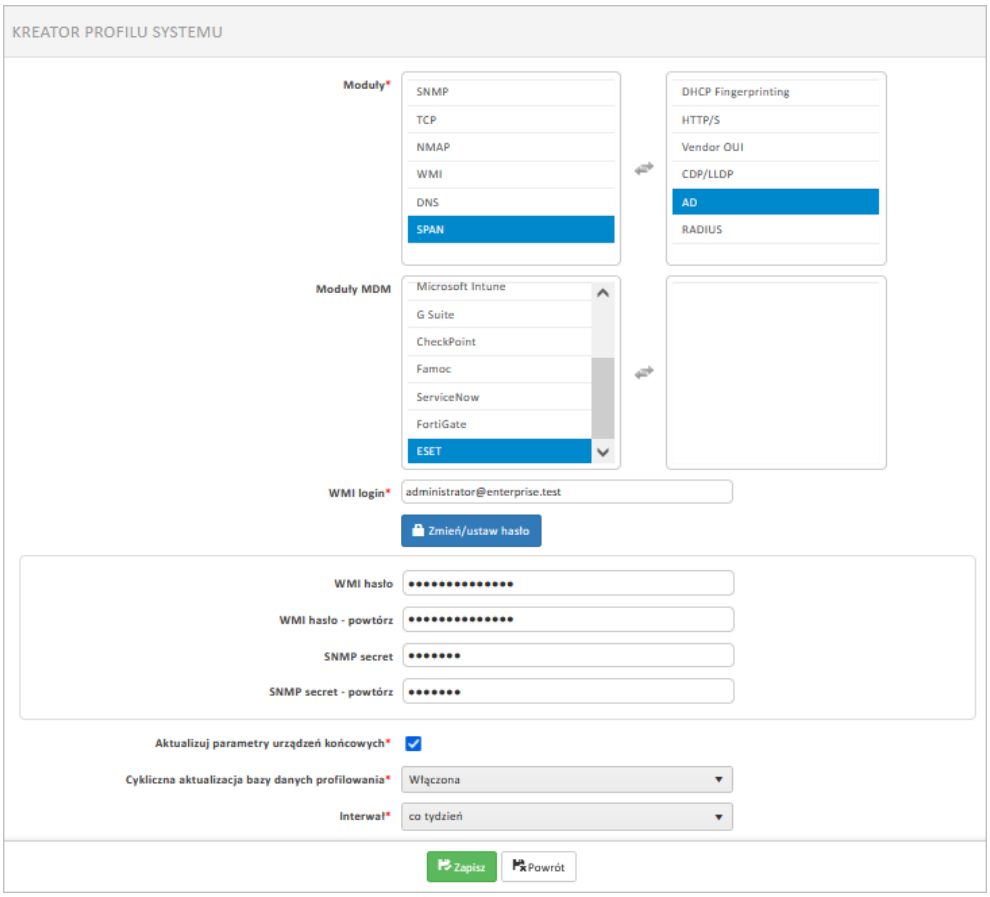
Zapisz ustawione wartości. Aby wgrać zmiany do systemu, naciśnij przycisk ***Zastosuj konfigurację.*** System w ciągu 10 minut ustawi żądane parametry.

2.3. Profil systemu

Z listy kreatorów wybierz opcję ***Profilowanie.*** Przejdź do edycji. Uzupełnij formularz. Do listy ***Modułów*** dodaj: ***RADIUS***, ***AD***, ***CDP/LLDP***, ***VENDOR OUI***, ***DHCP Fingerprinting*** oraz ***HTTP/S***.

Uzupełnij pozostałe pola:

- **WMI login:** administrator@enterprise.test (tak samo ustaw w: **WinRM login** oraz **ONVIF login**)
- **SNMP secret**: NVPrivate
- **WMI password:** NACVIEW_SZKOLENIE22



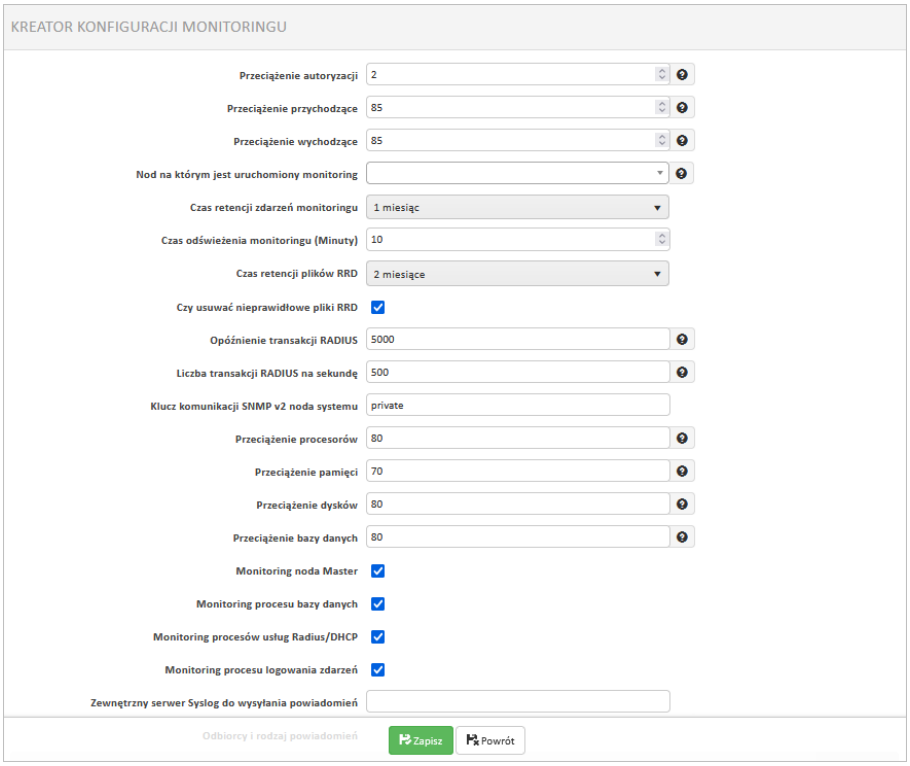
Zapisz ustawione wartości. Aby wgrać zmiany do systemu, naciśnij przycisk ***Zastosuj konfigurację.*** System w ciągu 10 minut ustawi żądane parametry.

2.4. Ustawienia monitoringu

Z listy kreatorów wybierz opcję ***Monitoring***. Przejdź do edycji. Uzupełnij formularz, podając parametry związane z przeciążeniem portów:

- **Przeciążenie autoryzacji:** 2
- **Przeciążenie przychodzące**: 85
- **Przeciążenie wychodzące:** 85
- **Czas odświeżenia monitoringu**: 5
- **Monitoring noda Master:** Tak
- **Monitoring procesu bazy danych:** Tak
- **Monitoring procesów usług Radius/DHCP**: Tak
- **Monitoring procesów logowania zdarzeń:** Tak

Pozostałe wartości ustaw, jak pokazano na poniższym obrazku.



Zapisz ustawione wartości. Aby wgrać zmiany do systemu, naciśnij przycisk ***Zastosuj konfigurację.*** System w ciągu 10 minut ustawi żądane parametry.

2.5. Active Directory

2.5.1. Konfiguracja Active Directory

Z listy kreatorów wybierz opcję ***Usługi katalogowe LDAP/AD***. Kliknij ***Dodaj nową pozycję***. Uzupełnij formularz, podając dane według poniższej tabeli:

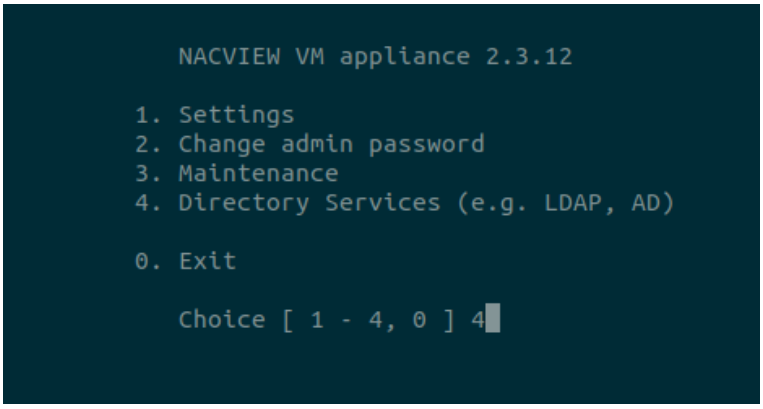
Pole	Dane
Nazwa	Enterprise
Aktywny	Tak
Czy domyślny	Tak
Czy domyślny dla VPN	Nie
Czy domyślny dla OTP	Nie
Nazwa NetBios	ENTERPRISE
Nazwa domenowa DNS	enterprise.test
Nazwy domenowe lub IP serwerów AD	alpha.enterprise.test
DNS IP	10.XX.166.2
Czy przeglądać inne współdzielone domeny	Tak
Czy wyłączyć w nazwie hostname ID	Nie
PKI CA	pki.enterprise.test

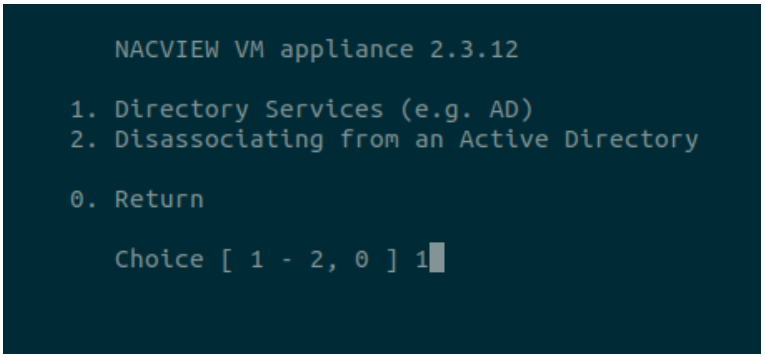
Zapisz ustawione wartości. Aby wgrać zmiany do systemu, naciśnij przycisk ***Zainstaluj konfigurację.*** System w ciągu 5 minut ustawi żądane parametry.

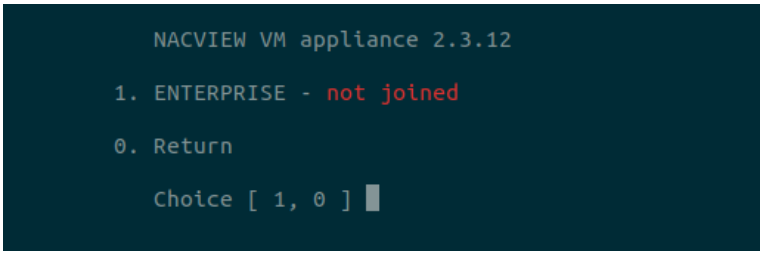
2.5.2. Wiersz poleceń (CLI/SSH)

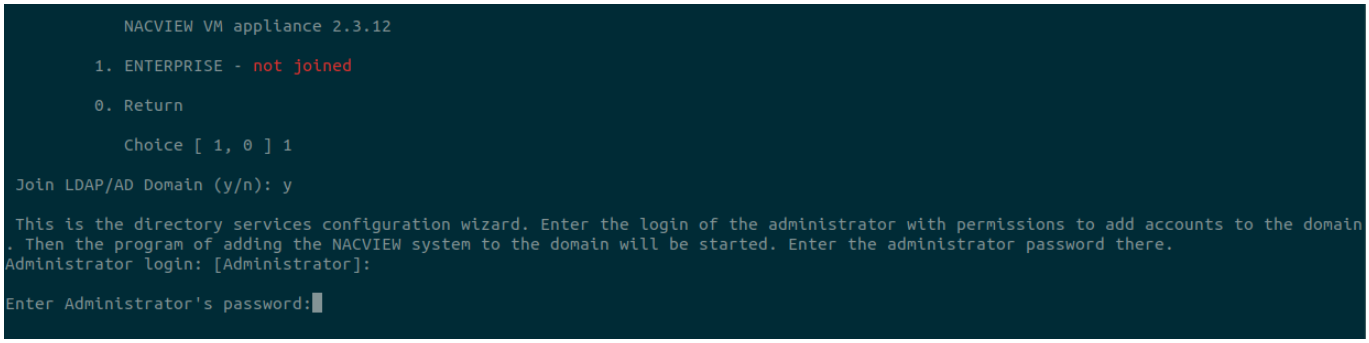
Otwórz wiersz poleceń maszyny XX-MS. Jako użytkownik ***admin*** (hasło: NACVIEW) wybierz opcję ***Directory Services (e.g. LDAP, AD),*** następnie opcję Directory Services (e.g. AD), a na końcu odpowiednią domenę (ENTERPRISE). Uruchom usługę, podając poświadczenia umożliwiające dodanie systemu do AD:

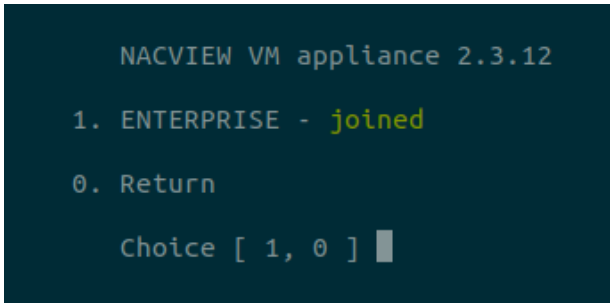
- Login: Administrator
- Hasło: NACVIEW_SZKOLENIE22











Uwaga! Sprawdź, czy nie trzeba na serwerze master wykonać aktualizacji konfiguracji nodów, po czym **te same czynności powtórz dla drugiego noda** (slave). Maszyna **XX-SL**.

3. Administracja

3.1. Konfiguracja SMTP

Z listy kreatorów wybierz opcję ***SMTP*** i przejdź do edycji formularza. Uzupełnij go, podając dane:

- **Nazwa nadawcy**: NACVIEW System
- **E-mail nadawcy**: szkolenie22@nacview.com
- **Protokół połączenia**: SMTP
- **Serwer poczty:** poczta.nacview.com
- **Nazwa użytkownika:** szkolenie22@nacview.com
- **Hasło:** Nv_SZKOLENIE22
- **Rodzaj autoryzacji**: login
- **Port połączenia** 587
- **Szyfrowanie**: TLS

Zapisz ustawione wartości. Aby wgrać zmiany do systemu, naciśnij przycisk ***Zainstaluj konfigurację.*** System w ciągu 5 minut ustawi żądane parametry.

3.2. Konfiguracja systemu

Z menu głównego wybierz ***Konfiguracja systemu*** *(*sekcja ***Administracja****)*. W sekcji ***Konfiguracja podstawowa*** kliknij ***Edytuj***. Uzupełnij formularz, podając następujące dane:

- **Domyślny prefix Tożsamości**: user_
- **Pierwszy serwer DNS:** 10.XX.166.2
- **Powiadamianie administratorów:** admin@nacview.com
- **Wysyłanie powiadomień:** miesiąc przed
- **Domyślny okres przeszukiwania historii zdarzeń:** 1 tydzień
- **Czas retencji zdarzeń DHCP**: 2 lata

Zapisz ustawione wartości.

3.3. Konta administracyjne

Z menu głównego wybierz ***Konta administracyjne*** *(*sekcja ***Administracja****)*. Kliknij ***Dodaj nową pozycję***, aby utworzyć nowe konto. Uzupełnij formularz, podając dane dla konta 1 z poniższej tabeli. Zapisz ustawienia. Powtórz dla kont numer 2 oraz 3 z tabeli.

Konto administracyjne	1	2	3
Serwery autoryzacji	Local database	Local database	Local database
Login	sekretariat	audyt	netAdmin
Hasło	NACVIEW2022	AUDYT2022	NVNET2022
Imię	Konto	Konto	Konto
Nazwisko	Sekretariatu	Audytoryjne	NOC
E-mail	sekretariat@enterprise.test	audyt@enterprise.test	noc@enterprise.test

3.4. Grupy administracyjne

Z menu wybierz ***Grupy administracyjne*** *(*sekcja ***Administracja****)*. Kliknij ***Dodaj nową pozycję***. Uzupełnij formularz, podając dane dla konta 1 z poniższej tabeli. Zapisz ustawienia. Powtórz dla kont numer 2 oraz 3 z tabeli.

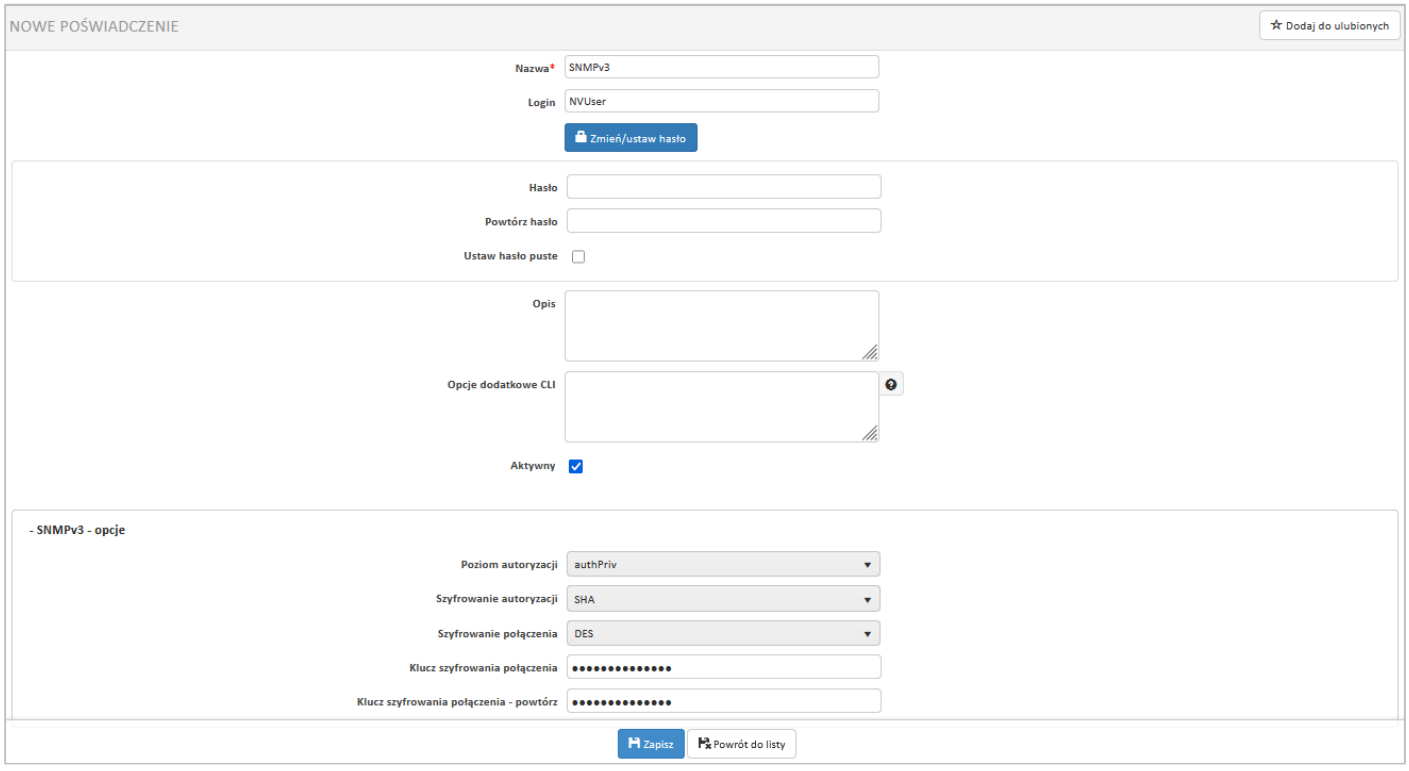
Grupa administracyjna	1	2	3
Nazwa	Sekretariat	Audyt	NOC
Role	Voucher accounts creating Voucher accounts deleting Voucher accounts displaying Voucher accounts editing Voucher accounts preview window access Standard Identities creating Standard Identities deleting Standard Identities displaying Standard 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
Konta administracyjne	sekretariat@enterprise.test	audyt@enterprise.test	noc@enterprise.test
Szczegółowe uprawnienia	Tożsamości: • Dodanie • Podgląd • Edycja • Listowanie Urządzenia końcowe • Podgląd • Listowanie		

Po ustawieniu ww. ról dla grup administracyjnych wyloguj się z panelu administracyjnego NACVIEW i zaloguj kolejno na poszczególne konta w celu weryfikacji uprawnień.

3.5. Poświadczenia urządzeń

Z menu głównego wybierz ***Poświadczenia urządzeń*** *(*sekcja ***Administracja****)*. Kliknij ***Dodaj nową pozycję*** i uzupełnij formularz, wpisując dane poświadczenia 1 z poniższej tabeli. Zapisz ustawione wartości. Powtórz czynności dla poświadczenia 2, 3 i 4.

Poświadczenie	1	2	3	4
Nazwa	SNMPv2	SNMPv3	cisco-SSH	SSH
Login	private	NVUser	admin	admin
Hasło	NVPrivate	NACVIEW_SZKOLENIE22	NACVIEW_SZKOLENIE22	NACVIEW_SZKOLENIE22
Opcje dodatkowe CLI (SSH)			-oKexAlgorithms=diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1 -o HostKeyAlgorithms=ssh-rsa	
SNMPv3 - opcje		Poziom autoryzacji: AuthPriv, Szyfrowanie autoryzacji: SHA, Szyfrowanie połączenia: DES, Klucz szyfrowania: NACVIEW_SZKOLENIE22		



3.6. Grupy obiektów

Z menu głównego wybierz ***Grupy obiektów*** *(*sekcja ***Administracja****)*. Kliknij ***Dodaj nową pozycję***. Uzupełnij formularz wpisując kolejno nazwy:

- *Komputery,*
- *Pracownicy,*
- *Księgowość,*
- *Managerowie,*
- *Młodsi Inżynierowie Sieciowi,*
- *Starsi Inżynierowie Sieciowi,*
- *MAC adresy,*
- *Drukarki,*
- *Urządzenia sieciowe,*
- *Telefony VoIP.*

4. Sieć

4.1. Podsieci

4.1.1. Dodawanie podsieci

Z menu głównego wybierz ***Podsieci IPv4*** *(*sekcja ***Sieć****)*. Kliknij ***Dodaj nową pozycję*** i uzupełnij formularz, wpisując dane podsieci 1 z poniższej tabeli. Zapisz ustawione wartości. Powtórz czynności dla podsieci 2-7.

Podsieć	1	2	3	4
Nazwa	NET_166	NET_80	NET_88	NET_126
Nazwa wyświetlana na mapie podsieci	10.XX.166.0/24	10.XX.80.0/24	10.XX.88.0/24	10.XX.126.0/24
Adres podsieci	10.XX.166.0	10.XX.80.0	10.XX.88.0	10.XX.126.0
Maska podsieci	24	24	24	24
DHCP włączony	Nie	Tak	Tak	Tak

Podsieć	5	6	7
Nazwa	NET_96	NET_104	NET_120
Nazwa wyświetlana na mapie podsieci	10.XX.96.0/24	10.XX.104.0/24	10.XX.120.0/24
Adres podsieci	10.XX.96.0	10.XX.104.0	10.XX.120.0
Maska podsieci	24	24	24
DHCP włączony	Tak	Tak	Tak

4.1.2. Konfiguracja DHCP

Znajdź na liście podsieci: 10.XX.80.0/24. Kliknij na  w wierszu, w którym się znajduje i wybierz ***Edytuj***. Rozwiń formularz klikając ***+DHCP*** (w lewym dolnym rogu).

- **DHCP włączony:** Tak
- **Czas dzierżawy:** 1800
- **Czy monitorować użycie DHCP**: Tak
- **Próg procentowy użycia DHCP:** 85
- **Próg procentowy ramek DHCP DECLINE**: 5
- **Zarejestruj urządzenie końcowe:** Nie

Zapisz ustawione wartości. Po zapisaniu zmian serwer DHCP zaczyna już działać.

Otwórz okno podglądu podsieci, klikając na  . Naciśnij  i wybierz ***Parametry DHCP***. Kliknij w ***Nowy parametr*** i uzupełnij pola formularza:

- **Nazwa parametru**: DHCP-Name-Service-Search
- **Wartość:** enterprise.test
- **Łącznik parametru i wartość:** =
- **Aktywny:** tak

Zapisz ustawione wartości.

W kolejnym kroku znajdź na liście podsieci: 10.XX.96.0/24. Kliknij na  w wierszu, w którym się znajduje i wybierz ***Edytuj***. Rozwiń formularz klikając ***+DHCP*** (w lewym dolnym rogu).

Uwaga! Tu ustaw **Czas dzierżawy DHCP** na bardzo krótki, np. **30**. Sieć 10.XX.96.0/24 to sieć dla połączeń do Captive Portalu.

4.1.3. Przydział adresów IP

Z menu głównego wybierz ***Adresy IPv4*** *(*sekcja ***Sieć****)*. Zaznacz adresy: od 10.XX.80.10 do 10.XX.80.20 (z podsieci 10.XX.80.0/24), kliknij w ***Akcje grupowe*** i wybierz ***Ustaw statyczny przydział***. Powtórz to dla wszystkich pozostałych sieci z uruchomioną usługą DHCP.

4.2. VLAN

Z menu głównego wybierz ***VLAN***. Kliknij ***Dodaj nową pozycję*** i uzupełnij formularz, wpisując dane VLAN-u 1 z poniższej tabeli. Zapisz ustawione wartości. Powtórz czynności dla VLAN-ów 2-7.

VLAN	1	2	3	4	5	6	7
Nazwa	Autoryzacja I	Autoryzacja II	Autoryzacja V	CP L2	CP L3	Sieć gościnna	Resources
Tag	80	88	126	96	104	120	166
Identyfikator koloru	Dowolna wartość	Dowolna wartość	Dowolna wartość	Dowolna wartość	Dowolna wartość	Dowolna wartość	Dowolna wartość
Podsieci	NET_80	NET_88	NET_126	NET_96	NET_104	NET_120	NET_166

4.3. Urządzenia sieciowe

4.3.1. Przełącznik Cisco C1000

Skonfiguruj urządzenie sieciowe. W tym celu zaloguj się do C1000 za pomocą klienta SSH jako admin, podając 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
```

- Konfiguracja portów - 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
```

- Konfiguracja portów - 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
```

Następnie wróć do panelu administracyjnego NACVIEW i dodaj skonfigurowane urządzenie. W tym celu z menu głównego wybierz ***Urządzenia sieciowe***. Kliknij ***Dodaj nową pozycję*** i uzupełnij formularz, wpisując dane urządzenia z poniższej tabeli.

Urządzenie sieciowe	Parametry
Model urządzenia	Network device
Liczba portów	10
Nazwa	Cisco C1000
Adres IP	10.XX.166.1
Oprogramowanie	Cisco IOS
Grupy obiektów	Urządzenia sieciowe

Zapisz ustawione wartości. Powinno wyświetlić się okno z ustawieniami poświadczeń. Naciśnij przy wierszu z protokołem SSH i wybierz ***Edytuj***. Uzupełnij formularz następującymi danymi:

- **Protokół połączenia:** SSH
- **Login i hasło:** cisco-SSH admin

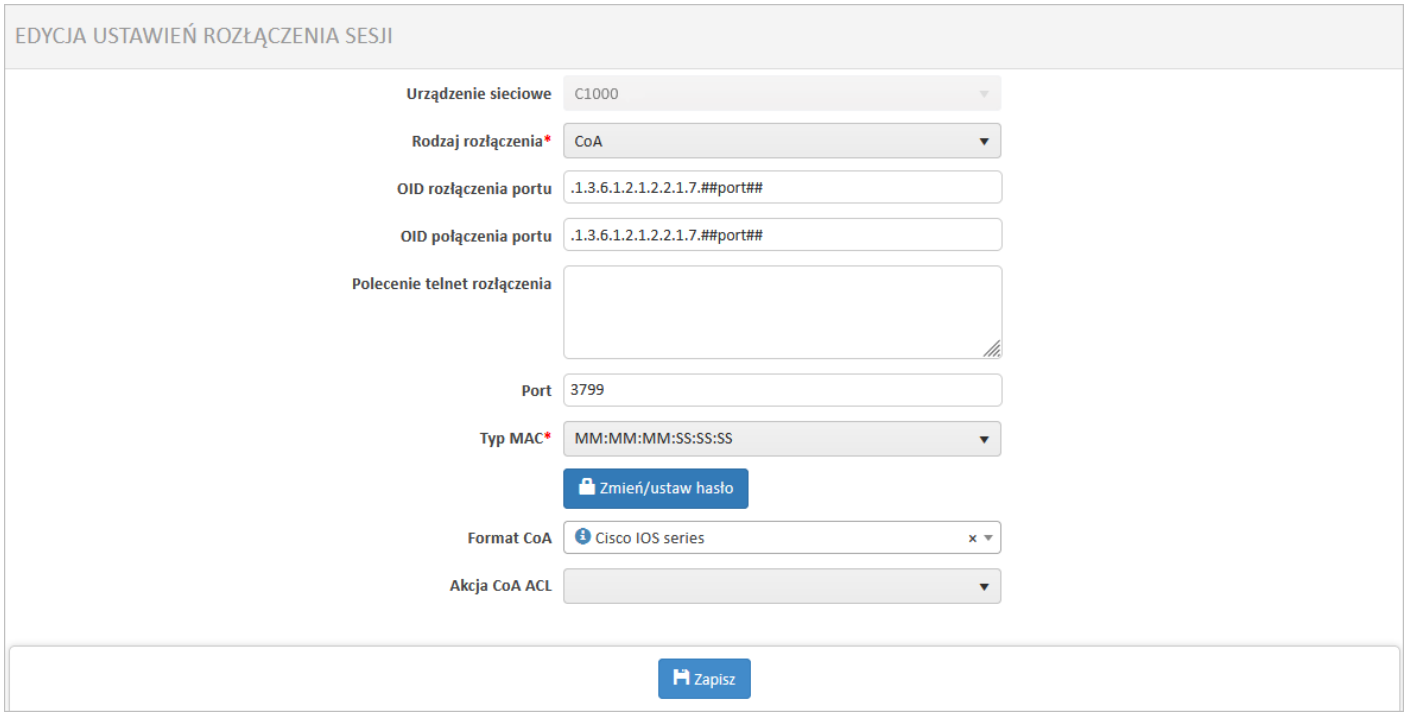
Zapisz. Powtórz dla protokołu SNMP, podając dane:

- **Protokół połączenia**: SNMPv3
- **Login i hasło**: SNMPv3 NVUser

Przejdź ***Dalej*** i kliknij ***Monitoring***. W wyświetlonym oknie pojawi się tabela z danymi konfiguracyjnymi monitoringu. Kliknij ***Zapisz*** w celu ich zatwierdzenia, a następnie zamknij okno.

Dane z urządzenia zostaną zebrane po maksymalnie 10 minutach, a gdy to się stanie - kliknij przycisk ***Edycja nazw portów***. Uzupełnij wyświetlony formularz i zapisz ustawione wartości.

W celu ustawienia mechanizmu rozłączania sesji kliknij przycisk ***Edycja rozłączania***. Wybierz rodzaj rozłączenia CoA, port 3799, format MAC rozdzielany dwukropkiem, podaj hasło **NACVIEW_SZKOLENIE22,** wybierz format CoA: Cisco iOS series i zapisz ustawione wartości.



Teraz należy zmienić domyślne hasło Radius, które zostało wygenerowane do komunikacji między systemem NACVIEW a urządzeniem sieciowym. W tym celu wejdź w edycję dodanego urządzenia (> ***Edytuj***), kliknij ***Zmień/ustaw hasło*** i uzupełnij pole ***Klucz komunikacji Radius***: zgodnie z danymi pkt. 1.4. Zapisz zmiany i powróć do listy.

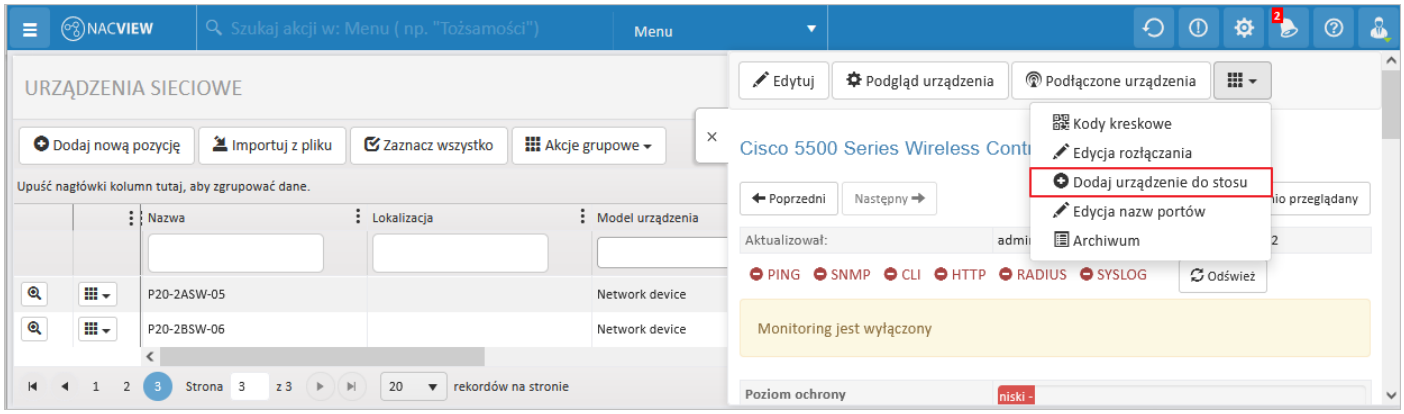
4.4. Urządzenia sieciowe - stack

Aby dodać przełączniki w stosie, w pierwszej kolejności należy dodać i skonfigurować główne urządzenie sieciowe. W tym celu przejdź do ***Urządzenia sieciowe > Dodaj nową pozycję***. Uzupełnij dane:

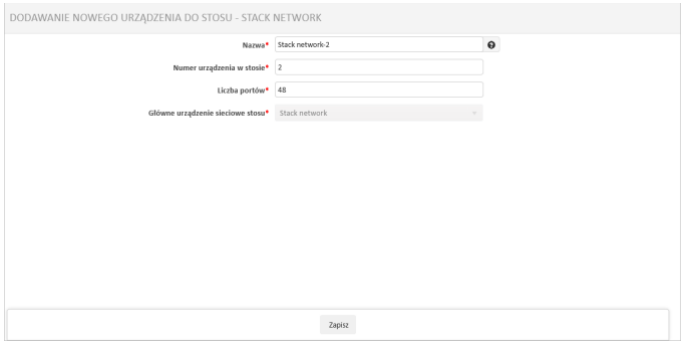
- **Model urządzenia:** Network device
- **Nazwa:** Stack network
- **Liczba portów:** 48
- **Adres IP:** 10.XX.166.19

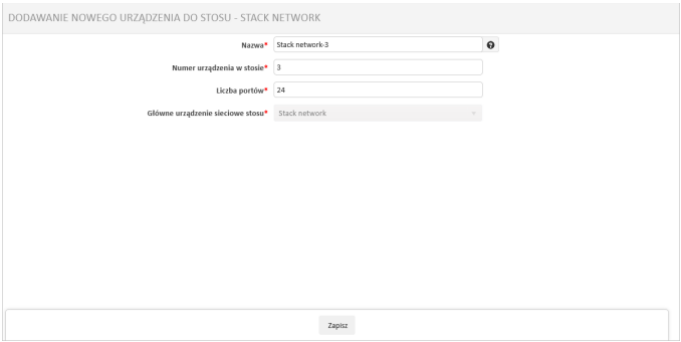
Zapisz wprowadzone zmiany.

Znajdź na liście nowo utworzony przełącznik (domyślnie powinien znajdować się na końcu listy). Otwórz podgląd, klikając przycisk: w wierszu danego przełącznika. W oknie otworzonym po prawej stronie, z menu rozwijanego wybierz opcję ***Dodaj urządzenie do stosu***.



W formularzu, jako numer urządzenia w stosie wybierz 2, natomiast jako liczbę portów wpisz 48. ***Zapisz*** ustawienia. Powtórz czynności dla trzeciego urządzenia w stosie o liczbie portów 24.





4.5. Wi-Fi

Z menu głównego wybierz ***Sieci WiFi*** *(*sekcja ***Sieć****)*. Kliknij ***Dodaj nową pozycję*** i uzupełnij formularz, wpisując dane sieci 1 z poniższej tabeli. ***Zapisz*** ustawione wartości. Powróć do listy i powtórz czynności dla sieci 2.

Sieć WiFi	1	2
Nazwa	WiFi_EAP	WiFi_MAC
SSID sieci	NACVIEW_22_EAP	NACVIEW_22_MAC

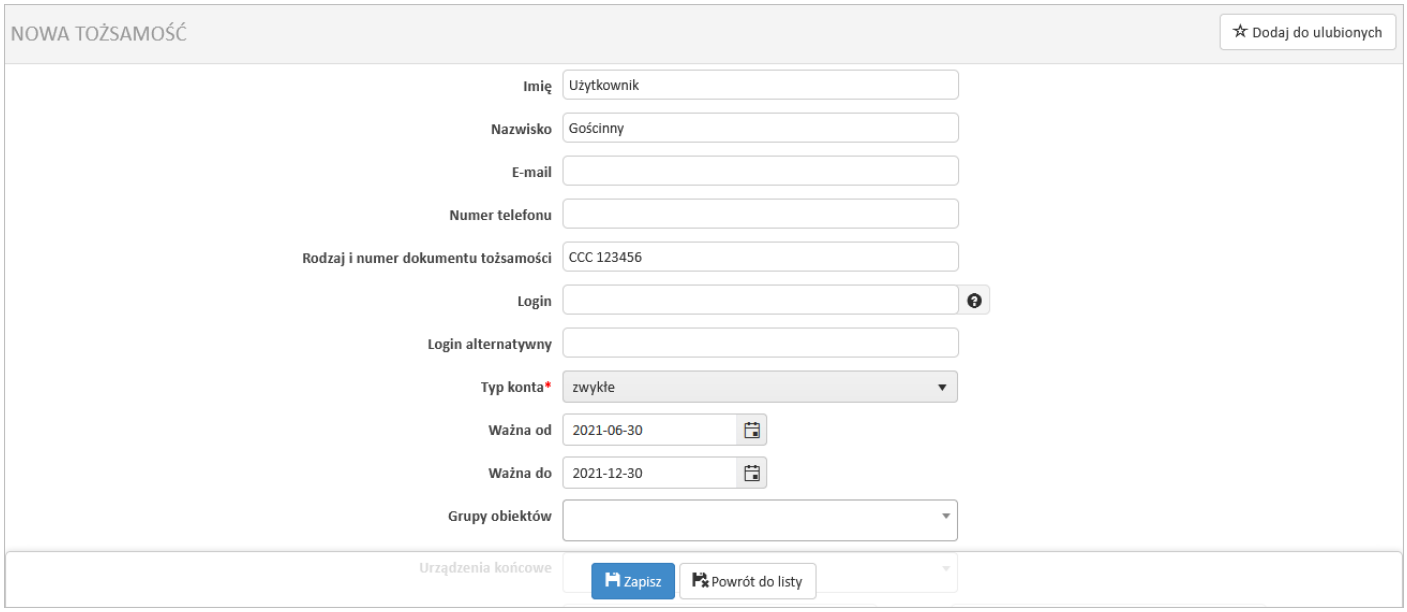
5. Obiekty

5.1. Tożsamości

5.1.1. Tworzenie tożsamości

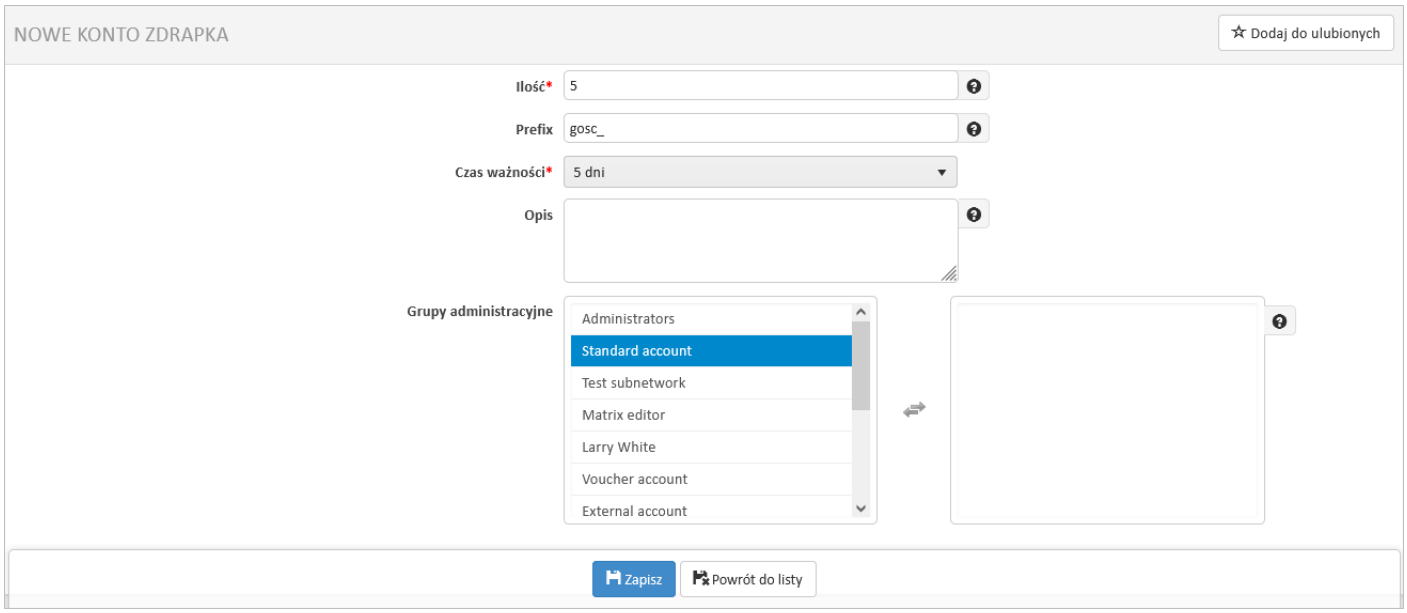
Z menu głównego wybierz ***Tożsamości*** *(*sekcja ***Obiekty****)*. Kliknij ***Dodaj nową pozycję*** i uzupełnij formularz, wpisując następujące dane:

- **Imię**: Użytkownik
- **Nazwisko:** Gościnny
- **Rodzaj i numer dokumentu tożsamości**: CCC 123456
- **Typ konta:** zwykłe
- **Ważna do**: 2026-03-21
- **Grupy obiektów:** Pracownicy



Zapisz ustawione wartości. Pozostając w sekcji ***Tożsamości***, kliknij ***Dodaj konta zdrapki*** i uzupełnij pola formularza:

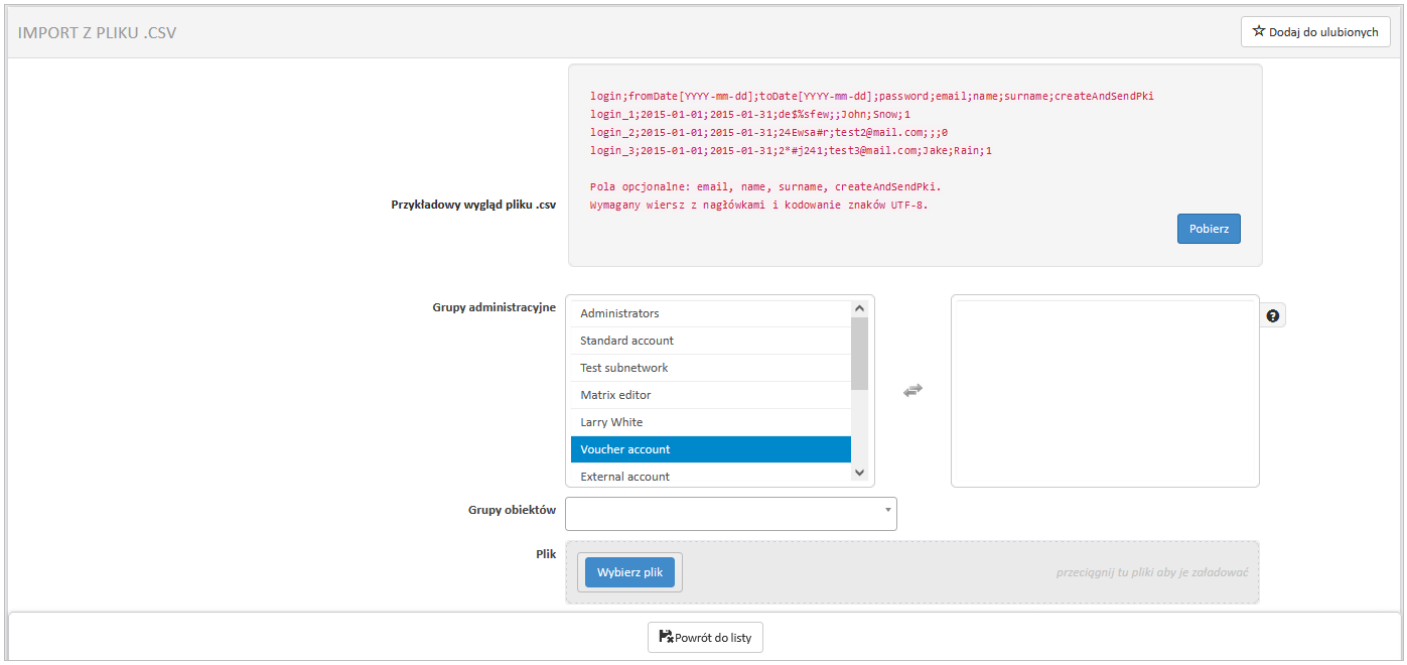
- **Ilość**: 10
- **Prefix**: gosc_
- **Czas ważności**: 5 dni



Zapisz ustawione wartości.

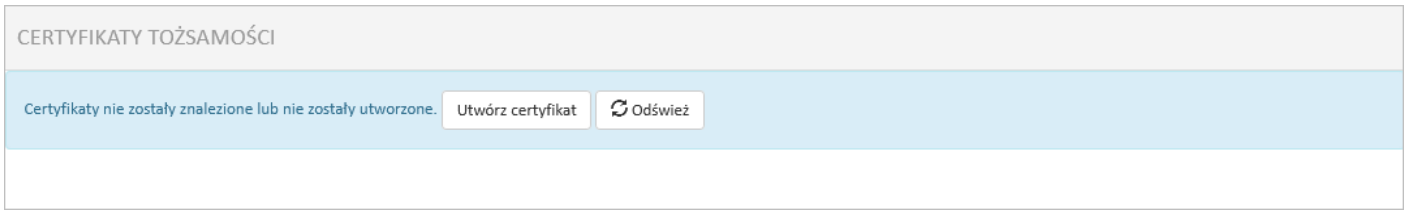
5.1.2. Import z pliku

Kliknij ***Importuj z pliku***, a następnie ***Pobierz***. Zapisz plik na dysku lokalnym. Kliknij ***Wybierz plik*** i otwórz pobrany przed chwilą plik. Plik został wgrany.



5.1.3. Certyfikaty

Naciśnij przy wybranej tożsamości i wybierz ***Certyfikaty***. Kliknij ***Utwórz certyfikat*** i po chwili ***Odśwież***. Certyfikat został wygenerowany.



5.2. Urządzenia końcowe

Z menu głównego wybierz ***Urządzenia końcowe*** *(*sekcja ***Obiekty****)*. Kliknij ***Dodaj nową pozycję*** i uzupełnij formularz, wpisując dane urządzenia 1 z poniższej tabeli. ***Zapisz*** ustawione wartości. Powróć do listy i powtórz czynności dla urządzenia 2.

Urządzenie końcowe	1	2
Nazwa	Telefon VoIP	Drukarka
Typ urządzenia	telefon/smartfon	drukarka
Grupy obiektów	Telefony VoIP	Drukarki
Parametry	-	-

5.3. Adresy MAC

Z menu głównego wybierz ***Mac adresy***. Kliknij ***Dodaj nową pozycję*** i uzupełnij formularz, wpisując dane adresu MAC 1 z poniższej tabeli. ***Zapisz*** ustawione wartości. Powróć do listy i powtórz czynności dla adresu 2. Następnie powtórz, dodając rzeczywisty adres MAC karty sieciowej komputera NT1. Odczytaj go używając poleceń np. **cmd**, następnie: **ipconfig /all** lub też łatwiej: **getmac**

Adres MAC	1	2
MAC	2E:B4:7E:A0:CA:9B	AB:B2:86:44:6B:FD
Domyślny adres IP	-	-
Urządzenie końcowe	Drukarka	Telefon VoIP
Grupy obiektów	Drukarki	Telefony VoIP

6. Konfiguracja

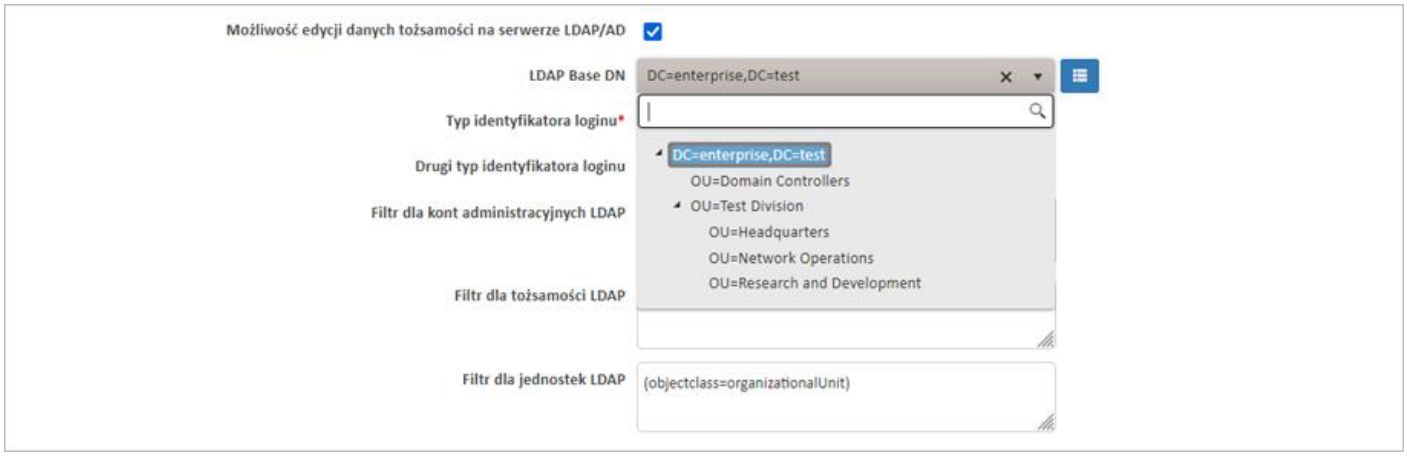
6.1. Serwery autoryzacji

Z menu głównego wybierz ***Serwery autoryzacji*** (z sekcji ***Konfiguracja***). Kliknij ***Dodaj nową pozycję***. Uzupełnij formularz danymi serwera 1 z poniższej tabeli. Kliknij ***Więcej opcji*** i w polu ***Typ identyfikatora loginu*** zaznacz *Account name*. Opcjonalnie możesz również uzupełnić pole ***Filtr dla tożsamości LDAP***. Zapisz ustawienia. Powtórz czynności dla serwera 2.

Serwer autoryzacji	1	2
Przeznaczenie	Tożsamości	Urządzenia końcowe
Rodzaj autoryzacji	Autoryzacja LDAP/AD	Autoryzacja LDAP/AD
Nazwa	Pracownicy_AD	Komputery_AD
Host	alpha.enterprise.test	alpha.enterprise.test
Login do usługi	administrator@enterprise.test	administrator@enterprise.test
Hasło	NACVIEW_SZKOLENIE22	NACVIEW_SZKOLENIE22
Typ identyfikatora loginu	Account name (sAMAccountName)	DNS Host name (dnsHostName)
Drugi typ identyfikatora loginu	Principal name (userPrincipalName)	Common name (cn)

Znajdź na liście serwerów autoryzacji serwer 1 i kliknij w przycisk  . Wybierz ***Edytuj***. Kliknij ***Więcej opcji*** i w polu ***LDAP Base DN*** zaznacz ***DC=enterprise,DC=test.*** Zapisz ustawienia.

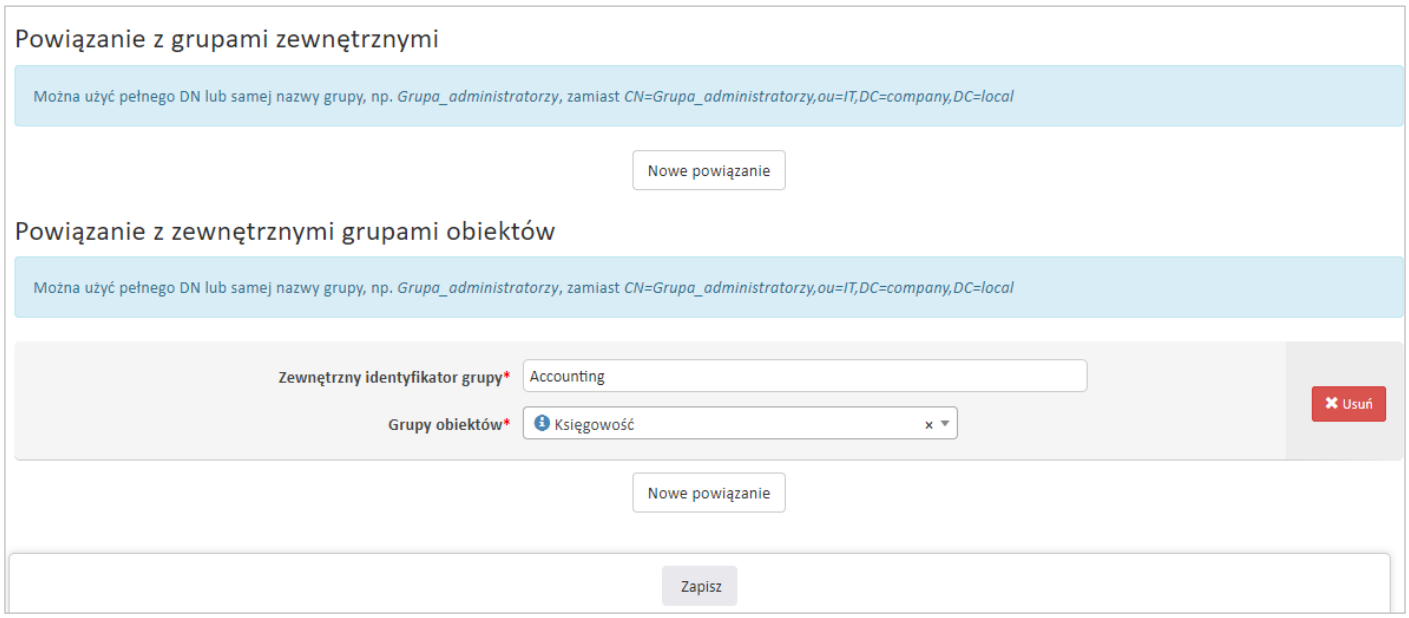
Jeśli dany serwer autoryzacji jest nieaktywny, kliknij w  i wybierz ***Aktywuj***.



W wierszu przy serwerze autoryzacji 1 (*Pracownicy_AD*) kliknij przycisk . W oknie, które otworzyło się po prawej stronie wybierz opcję ***Parametry dodatkowe importu***. W sekcji ***Powiązanie z zewnętrznymi grupami obiektów*** (u dołu okna) kliknij przycisk ***Nowe powiązanie***. W polu ***Zewnętrzny identyfikator grupy*** wpisz ***Accounting***, a w polu ***Grupy obiektów*** wybierz ***Księgowość***. W ten sam sposób dodaj jeszcze kolejne 3 grupy:

- Department Managers - Managerowie
- Junior Network Engineers - Młodsi Inżynierzy Sieciowi
- Senior Network Engineers - Starsi Inżynierzy Sieciowi

Zapisz ustawienia.



Znajdź teraz na liście serwer autoryzacji 2. Kliknij przycisk i w nowo otwartym oknie ponownie wybierz opcję ***Parametry dodatkowe importu***. W polu ***Domyślna grupa obiektów*** wybierz: ***Komputery***. Zapisz ustawienia. Następnie, w przypadku obu serwerów kliknij przycisk i wybierz opcję ***Synchronizuj***.

Z menu głównego wybierz ***Tożsamości*** (z sekcji ***Obiekty***). Sprawdź, czy obiekty się zaimportowały i czy mają przypisane ustalone wcześniej, zmapowane grupy.

6.2. Polityki dostępu

6.2.1. Tworzenie polityk

Z menu głównego wybierz ***Polityki dostępu***. Kliknij przycisk ***Dodaj regułę***. W wyświetlonym formularzu, wpisz dane polityki 1, znajdujące się w tabeli poniżej. Zapisz ustawienia. Powtórz czynności dla polityk 2-6.

Polityka dostępu	1	2	3	4
Nazwa	Host_Access	EAP_Access_Group	EAP_Access_OU_I	EAP_Access_OU_II
Metoda uwierzytelniania do sieci	Host	EAP	EAP	EAP
Akcja	Dostęp do VLAN-u	Dostęp do VLAN-u	Dostęp do VLAN-u	Dostęp do VLAN-u
Czy odsyłać nr VLAN-u	☑	☑	☑	☑
VLAN	Autoryzacja V	Autoryzacja I	Autoryzacja I	Autoryzacja II
Brak zdefiniowanych urządzeń użytkownika oznacza	Obojętnie jakie Urządzenie	-	-	
Brak zdefiniowanych Tożsamości oznacza	-	Dowolna Tożsamość	Dowolna Tożsamość	Dowolna Tożsamość
Dowolna Tożsamość oznacza		Dowolna aktywna Tożsamość zdefiniowana w systemie	Dowolna aktywna Tożsamość zdefiniowana w systemie	Dowolna aktywna Tożsamość zdefiniowana w systemie
Grupy obiektów Tożsamości		Księgowość, Managerowie	-	-
Serwery autoryzacji urządzeń końcowych	Komputery_AD	-	-	-
Jednostki organizacyjne Tożsamości	-	brak	Network Operations	Research and Development
Serwery autoryzacji Tożsamości		Pracownicy_AD	Pracownicy_AD	Pracownicy_AD
Logika warunków dla tożsamości		And	And	And
Urządzenia sieciowe	C1000	C1000	C1000	C1000

Polityka dostępu	5	6
Nazwa	MAC Telefony i Drukarki	Captive Portal
Metoda uwierzytelniania do sieci	MAC	MAC
Akcja	Dostęp do VLAN-u	Dostęp do VLAN-u
Czy odsyłać nr VLAN-u	☑	☑
VLAN	Autoryzacja II	Sieć gościnna
Lokalny Captive Portal	-	☑
Brak zdefiniowanych urządzeń użytkownika oznacza	Obojętnie jakie Urządzenie	
Grupy obiektów adresów MAC lub urządzeń końcowych	Drukarki, Telefony VoIP	
Urządzenia sieciowe	C1000	C1000

Po dodaniu polityk, wgraj je do systemu. W tym celu kliknij w przycisk ***Zainstaluj listę***. Zatwierdź, naciskając ***Zainstaluj***.

6.2.2. Testowanie polityk

Kliknij na przycisk ***Testowanie polityk***, znajdujący się w prawym górnym rogu okna Polityk dostępu. Uzupełnij pola formularza danymi kolumny 1 z poniższej tabeli. Kliknij ***Prześlij***. Pod formularzem powinien pojawić się wynik autoryzacji (pozytywny lub negatywy). Powtórz czynności dla danych z kolumn 2 i 3.

Dane	1	2	3
Rodzaj autoryzacji	MAC	Host (EAP)	EAP
Sprawdź dla	Urządzenie końcowe	Urządzenie końcowe	Tożsamości
Tożsamość	-	-	AccountantOne
Urządzenie końcowe	Komputer	NT1.enterprise.test	-
Urządzenie sieciowe	C1000	C1000	C1000
MAC adres klienta	AB:B2:86:44:6B:FD	-	-

6.3. Definicje zdarzeń

Z menu głównego wybierz ***Definicje zdarzeń***. Kliknij przycisk ***Dodaj nową pozycję*** i uzupełnij pola następującymi danymi:

- **Nazwa**: Alarm konfiguracji
- **Źródło**: Zdarzenia syslog
- **Szukane frazy:** VLAN mismatch
- **Akcja**: Powiadom
- **Konta administracyjne do powiadomienia:**
  - admin@nacview.com
  - sekretariat@nacview.com

Zapisz ustawione wartości. Następnie kliknij przycisk  i wybierz opcję **Zobacz logi**.

6.4. Captive Portal

Z menu głównego wybierz ***Captive Portal*** (sekcja ***Konfiguracja***). Kliknij przycisk ***Edytuj*** przy pozycji o typie portalu ***Autoryzacja***. Następnie zmień dane:

- **Nazwa:** Captive
- **Aktywny:** Tak
- **Certyfikat**: wewnętrzny (pki.enterprise.test)
- **Adres IP**: 10.XX.96.1
- **Port HTTP**: 80
- **Port HTTPS**: 443
- **Adres URL**: https://captive.enterprise.test
- **Regulamin**: Tekst regulaminu dla pracownika

\+ Ustawienia logowania i rejestracji:

- **Ręczna aktywacja tożsamości**: Nie
- **Ręczna aktywacja urządzeń końcowych**: Nie
- **Przesłanie hasła do tożsamości**: Instant
- **Grupy przypisane podczas rejestracji**: Pracownicy

Zapisz ustawione wartości. Następnie kliknij ***Zainstaluj konfiguracje*** (prawy górny róg okna). Wejdź teraz do edycji podsieci 10.XX.96.0/24 i ustaw ***Adres serwera DNS 1***: 10.XX.96.1. Zapisz ustawione wartości.

6.4.1 Test działania

CP możesz sprawdzić logując się do komputera z Windows 10 **(NT2)**. Wyłącz pierwszą kartę sieciową komputera i włącz drugą. Po wywołaniu przeglądarki i wpisaniu jakiegokolwiek adresu powinieneś zostać przekierowany do portalu, gdzie po prawidłowym podaniu danych logowania zostaniesz rozłączony, otrzymasz inny adres IP i zostaniesz przeniesiony do innego VLAN-u zgodnie z ustaloną wcześniej polityką. Cały proces możesz przeanalizować w sekcji **Raporty** > **Zdarzenia autoryzacji**.

Na urządzeniu sieciowym można podejrzeć proces autoryzacji oraz VLAN przypisany do portu za pomocą poleceń: *show mab all summary, show mab interface gigabitEthernet 1/0/2 details, show vlan brief.*

6.5. Grupy TACACS+

6.5.1. Konfiguracja na urządzeniu sieciowym

Zaloguj się za pomocą klienta SSH do C1000 jako admin. Aby ustawić TACACS+ na przełączniku, skonfiguruj go za pomocą poniższych komend, wchodząc w tryb edycji *configure terminal*:

```
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. Hasło TACACS+

Z menu głównego wybierz ***Konta administracyjne*** *(*sekcja ***Administracja****)*. Kliknij w przycisk  przy koncie administracyjnym (sekretariat@enterprise.test) i wybierz ***Edytuj***. Kliknij w Zmień/ustaw hasło i uzupełnij pole ***Hasło TACACS+:*** NACVIEW_SZKOLENIE22. Zapisz ustawione wartości.

Z menu głównego wybierz ***Urządzenia sieciowe***. Kliknij w przycisk  przy wybranym urządzeniu sieciowym i wybierz ***Edytuj***. Kliknij w Zmień/ustaw hasło i uzupełnij pole ***Klucz TACACS+*** zgodnie z danymi z pkt. 1.4. (wpisz hasło: NACVIEW_SZKOLENIE22). Zapisz ustawione wartości.

6.5.3. Konfiguracja TACACS+

Z menu głównego wybierz ***Serwery TACACS+*** *(*sekcja ***Konfiguracja****)*. Kliknij przycisk ***Dodaj nową pozycję.*** Uzupełnij formularz następującymi danymi:

- **Nazwa**: Role1
- **Domyślne uprawnienia**: permit
- **Użytkownicy**: sekretariat@enterprise.test
- **Urządzenia sieciowe**: C1000

Zapisz ustawione wartości. Znajdź na liście dodaną przed chwilą grupę i kliknij przycisk  , a następnie w otwartym po prawej stronie oknie ***Edycja ustawień TACACS+.*** Naciśnij ***Dodaj ustawienie*** i uzupełnij formularz, wprowadzając komendy:

- **Polecenie:** show running-config
- **Uprawnienie**: deny
- **Aktywny**: Tak

Zapisz ustawione wartości, a następnie kliknij ***Zainstaluj konfigurację i zaczekaj na koniec procesu instalacji***.

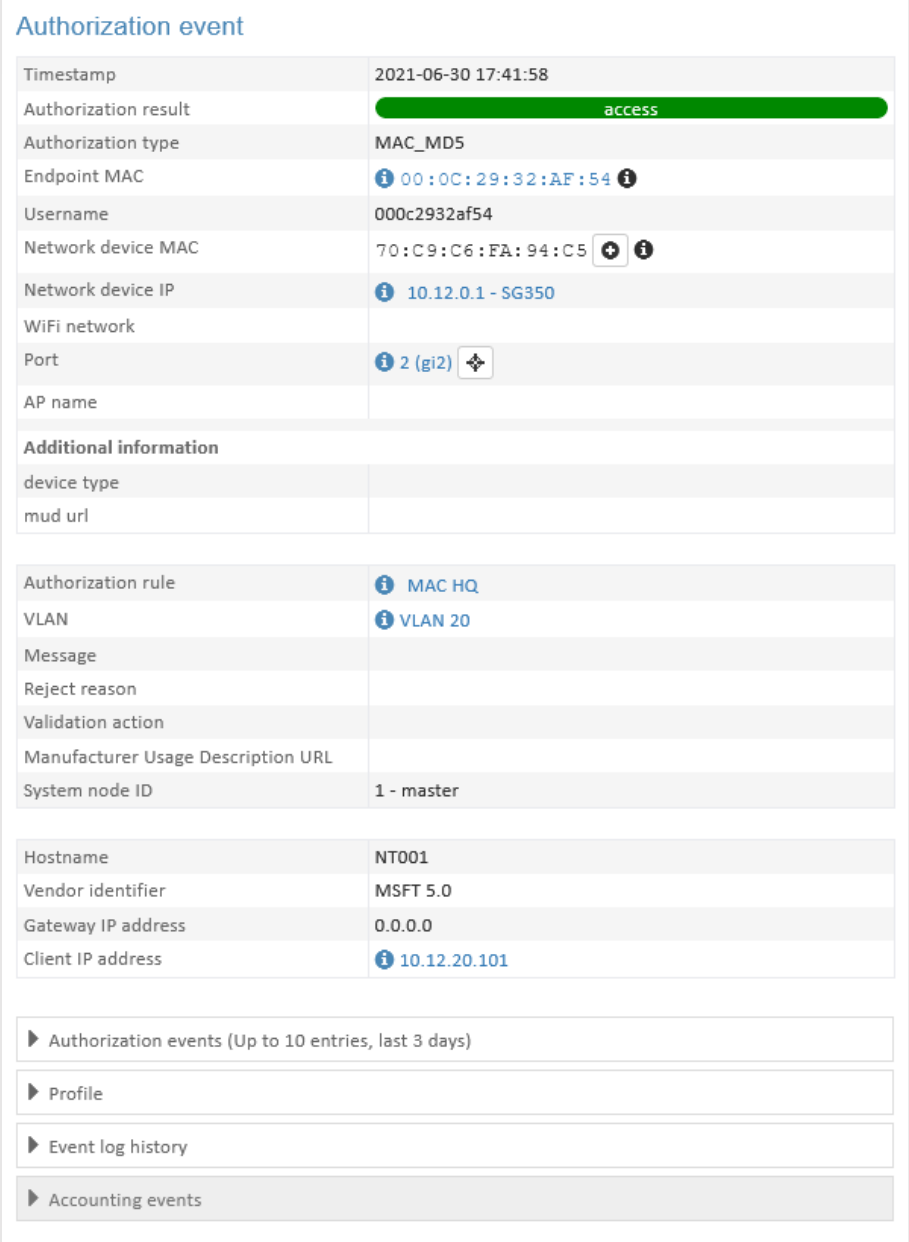
Zaloguj się poprzez SSH do C1000 jako użytkownik sekretariat i podaj hasło TACACS administratora. Wykonaj polecenie: *show running-config*. Przejdź w NACVIEW do sekcji ***Zdarzenia TACACS*** i sprawdź informacje o zalogowaniu się do urządzenia sieciowego i blokadzie wykonania komendy. Popraw ustawienie, zmieniając parametr *deny* na *permit*. ***Zainstaluj konfiguracje i zaczekaj na koniec procesu instalacji***.

Ponownie wykonaj w C1000 komendę *show running-config*. Zweryfikuj wykonanie komendy w ***Zdarzeniach TACACS.***

7. Raporty - przegląd sekcji

7.1.1. Weryfikacja działania polityk

Zweryfikuj użyte polityki logowania . W tym celu z menu głównego wybierz ***Zdarzenia autoryzacji*** (sekcja ***Raporty***). W ***Zdarzeniach autoryzacji*** zobacz szczegóły i użytą autoryzację . W ***Zdarzeniach DHCP*** (sekcja ***Raporty***) sprawdź nadany adres IP.

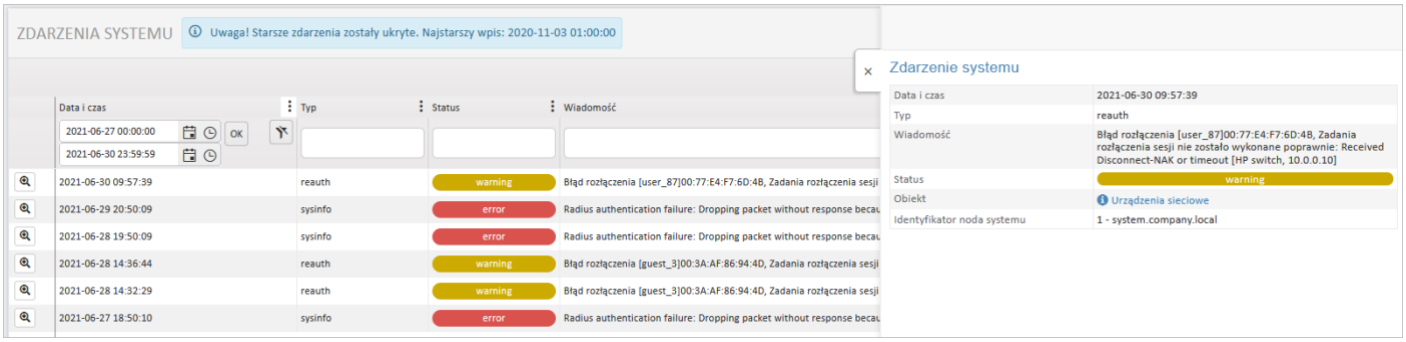


7.1.2. Rozłączenie sesji

Z menu głównego NACVIEW wybierz ***Zdarzenia autoryzacji***. Znajdź ostatnią autoryzację na liście i naciśnij przycisk  , znajdujący się w tym samym wierszu. W oknie otwartym po prawej stronie kliknij ***Rozłączanie sesji***. Uzupełnij wyświetlony formularz następującymi danymi:

- **Czy rozłączyć sesję:** Tak
- **Do jakich grup dodać adres MAC i tożsamość**: Quarantine
- **Adres MAC:** wybrana ze zdarzenia
- **Tożsamość**: wybrana ze zdarzenia

Zapisz ustawione wartości. Przejdź teraz do ***Zdarzeń systemu*** i sprawdź wynik rozłączenia.



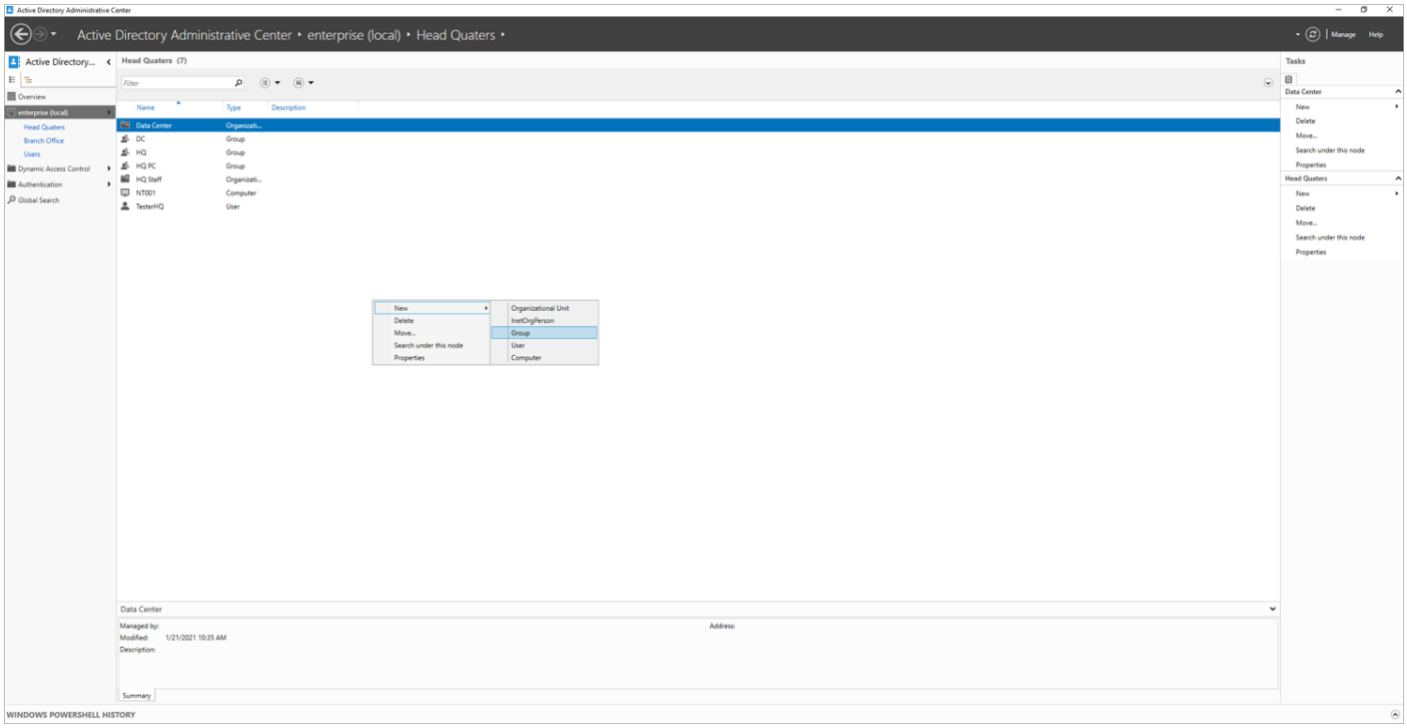
8. Konfiguracja usług na serwerze i klientach Windows

8.1. Publikacja certyfikatów przez GPO

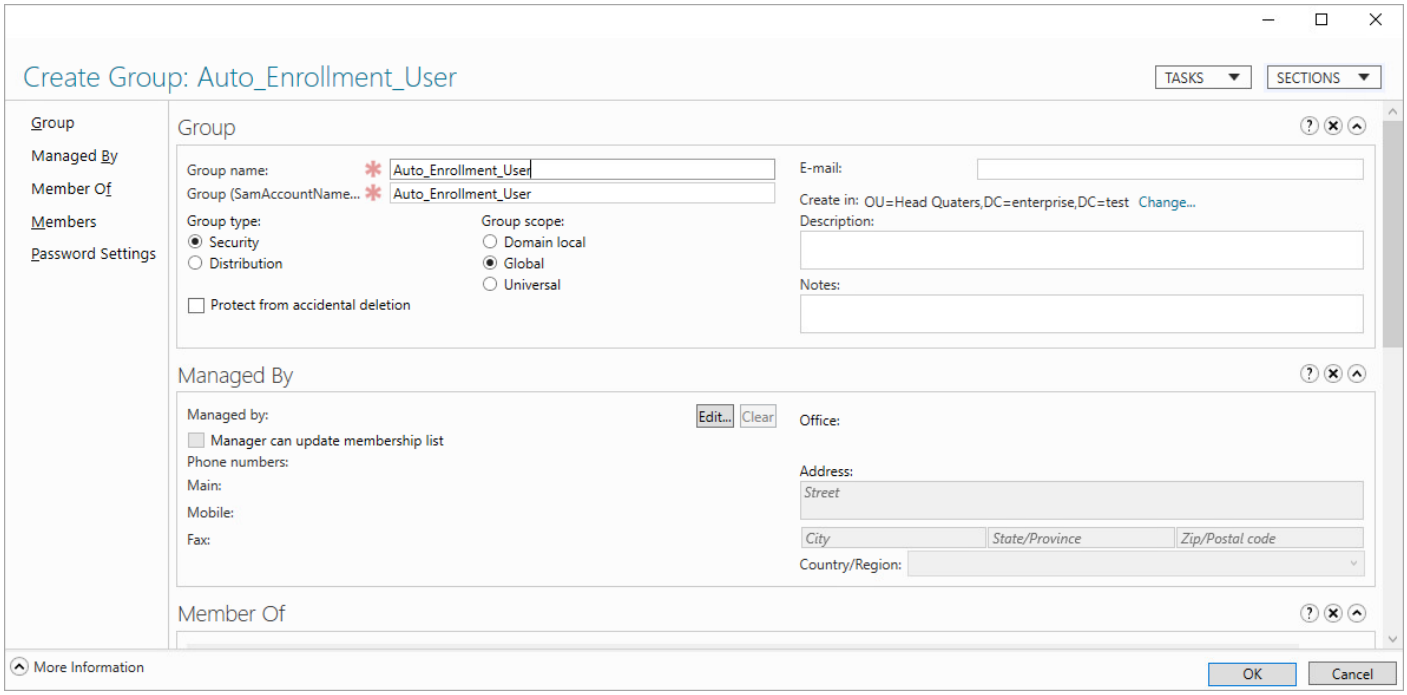
8.1.1. Tworzenie grup bezpieczeństwa dla użytkowników

Otwórz ***Active Directory Administrative Center*** na serwerze z możliwością zarządzania domeną **(maszyna XX-DC).**

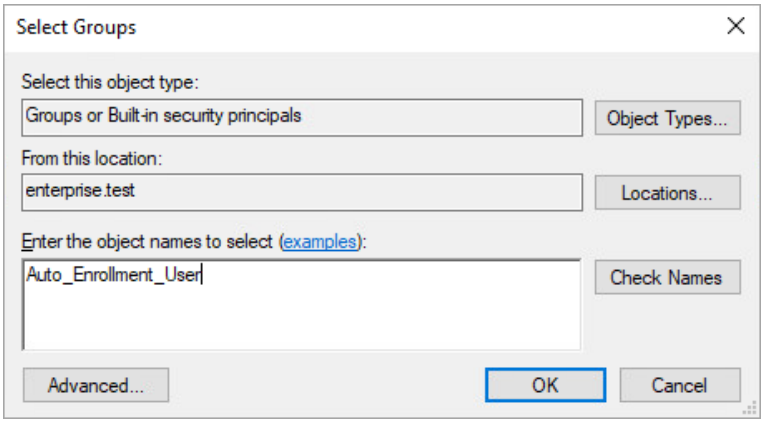
W OU *Enterprise Divisionsion* stwórz grupę bezpieczeństwa. W tym celu kliknij prawym przyciskiem myszy i wybierz *New > Group*. Użytkownicy należący do tej grupy będą uczestniczyć w tzw. *auto-enrollment*.



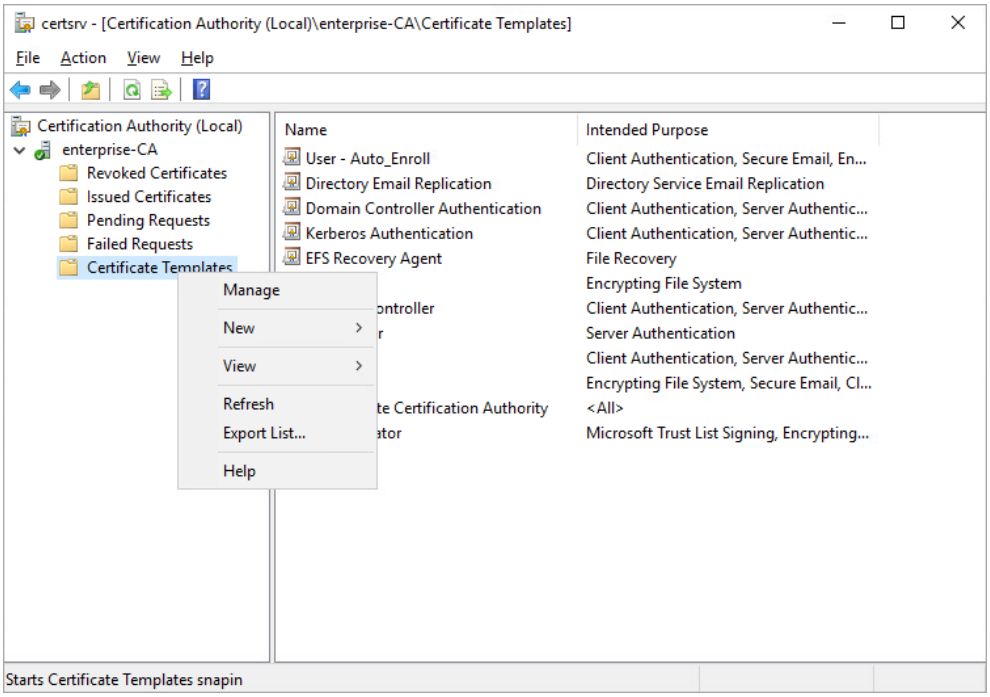
Wprowadź nazwę grupy (np. *Auto_Enrollment_User*). Zapisz, klikając ***OK***.



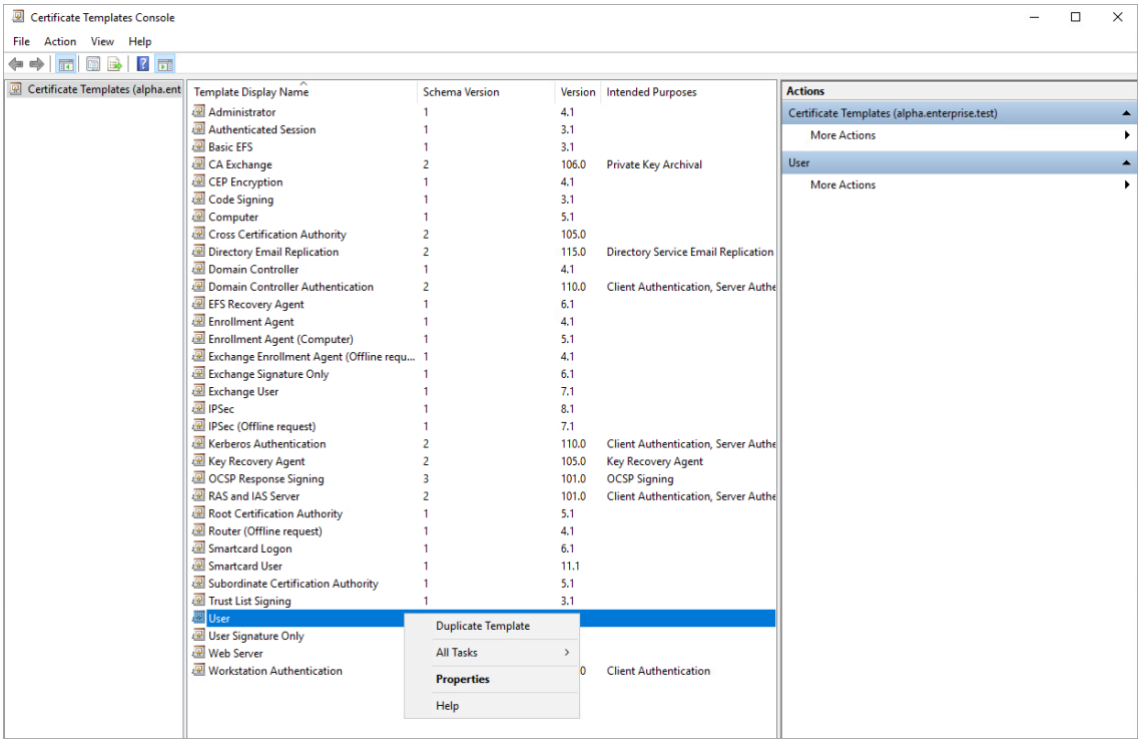
Dodaj użytkowników do utworzonej przed chwilą grupy. W tym celu kliknij prawym przyciskiem myszy na wybranego użytkownika i wybierz ***Add to group…*** Wpisz nazwę utworzonej wcześniej grupy. Zatwierdź przyciskiem ***OK***.



Zamknij AD AC na maszynie XX-DC, a następnie przejdź do maszyny wirtualnej **XX-CA** i otwórz narzędzie ***Certification Authority*** (***Server Manager > Tools > Certification Authority***). Kliknij prawym przyciskiem myszy na ***Certificate Templates***, a następnie wybierz ***Manage.***

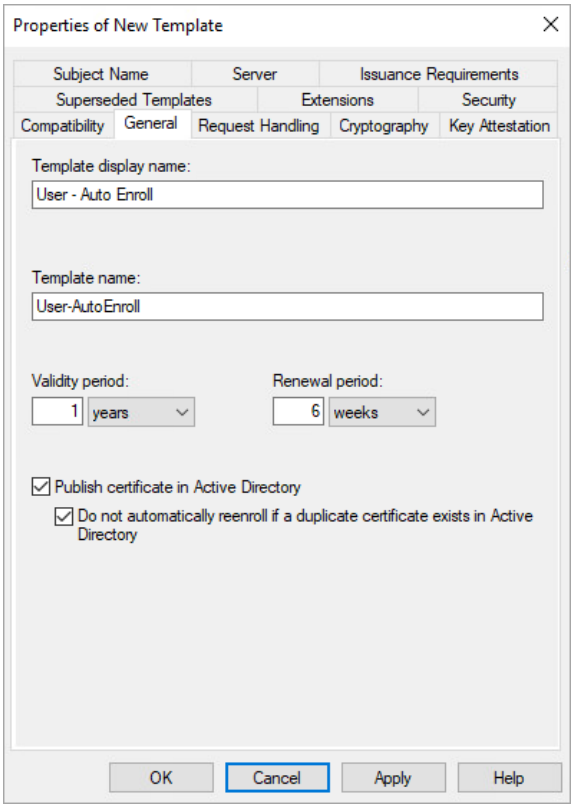


W panelu po prawej stronie powinny pojawić się szablony certyfikatów. Kliknij prawym przyciskiem myszy na szablon o nazwie ***User*** i wybierz ***Duplicate Template***.

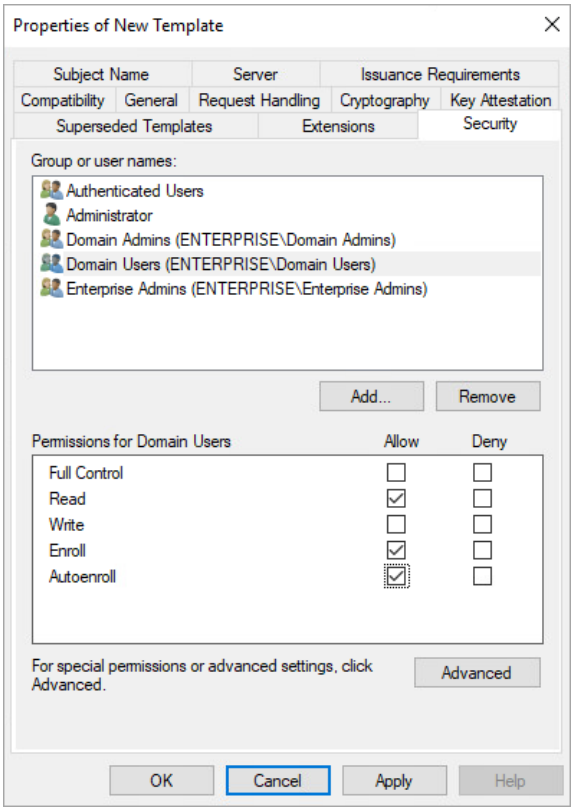


Wprowadź zmiany w zakładkach wg poniższych zaleceń:

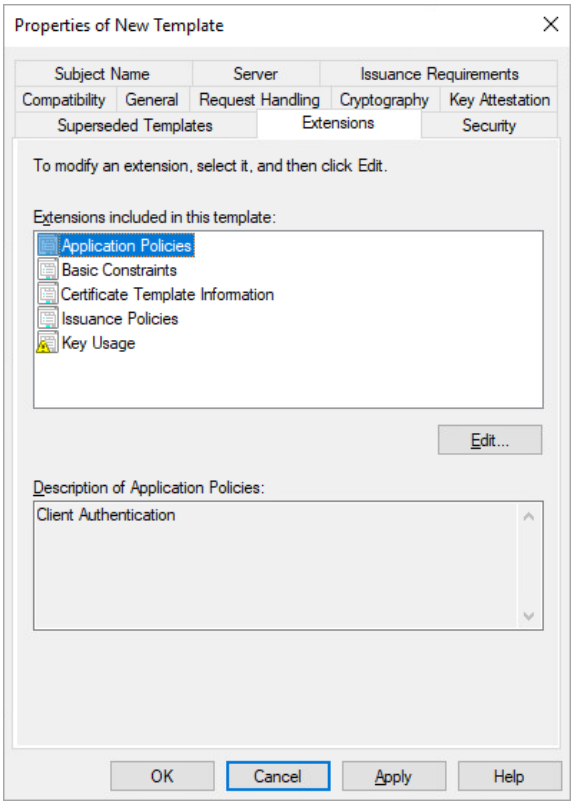
- ***Compatibility:*** wybierz właściwy system operacyjny dla urzędu certyfikacji oraz odbiorcy certyfikatu. Powinna to być najniższa wersja systemu operacyjnego funkcjonującego w środowisku.
- ***General:*** Zmień nazwę (tu: User - Auto Enroll) oraz ustaw okres ważności wg. zasad organizacji (zalecamy odnawianie nie częściej niż raz na rok). Zaznacz opcję ***Publish certificate in Active Directory*** oraz ***Do not automatically reenroll if a duplicate exists in Active Directory***.



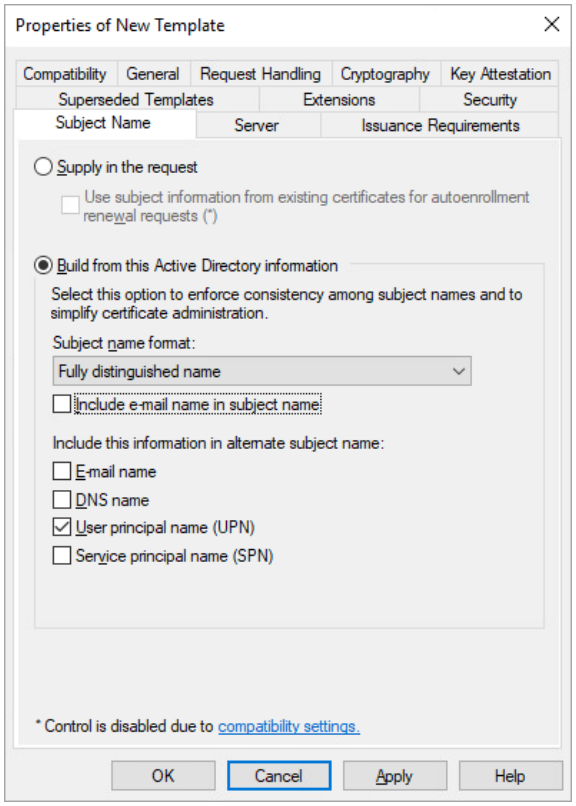
- ***Cryptography***: zalecene min. 2048 bitowy klucz, a dla ważnych grup 4096.
- ***Security***: w sekcji ***Permissions for Domain Users*** zaznacz opcje tak jak na poniższym zdjęciu.



- ***Extensions***: dla ***Application Policies*** wybierz opcję ***Client Authentication*** (usuń inne opcje), a dla ***Key Usage*** zaznacz: ***Digital Signature*** oraz ***Signature is proof of origin***.

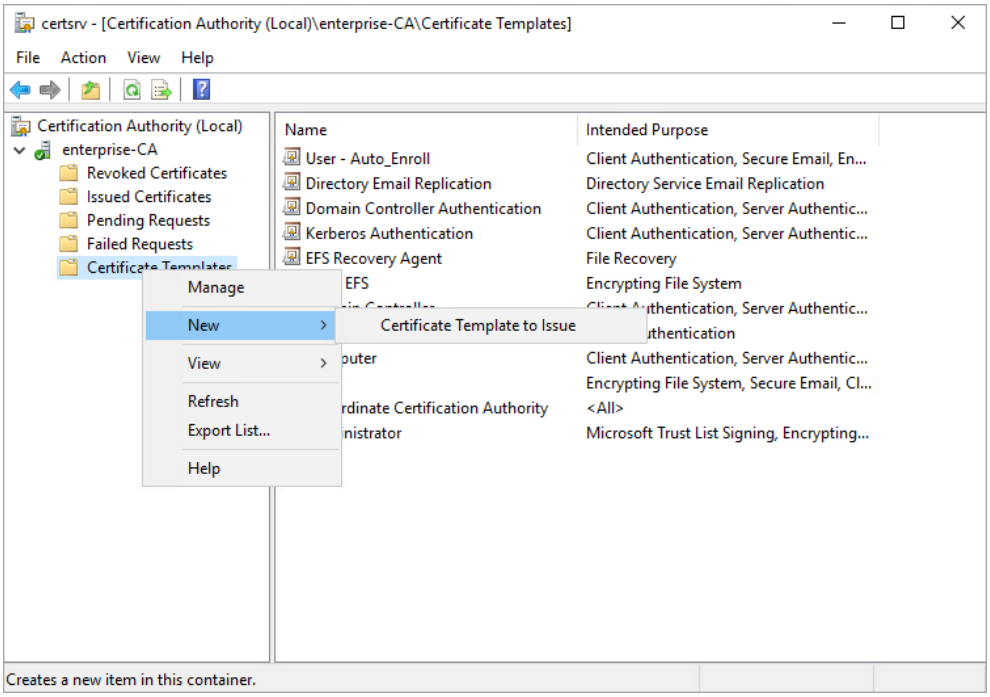


- ***Subject Name***: Zaznacz opcję ***User principal name (UPN)***.



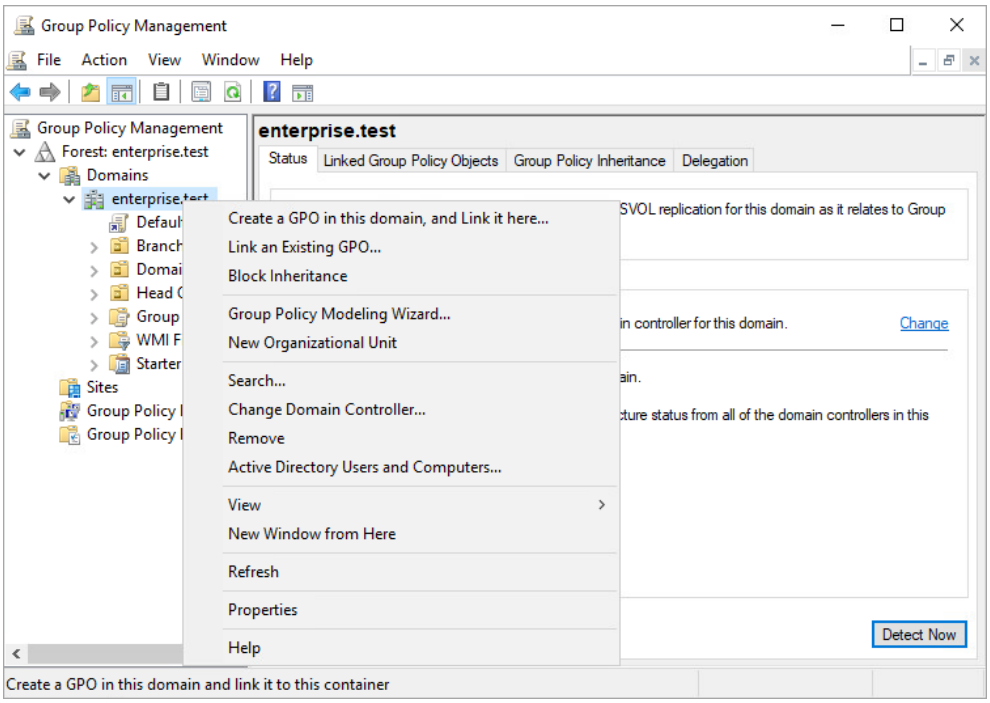
Wartości w pozostałych zakładkach pozostaw domyśle. Zatwierdź zmiany przyciskiem ***OK*** i zamknij panel zarządzania szablonami certyfikacji.

Dodaj nowo utworzony szablon do aktywnych szablonów. W tym celu kliknij prawym przyciskiem myszy na ***Certificate Templates*** i wybierz ***New*** > ***Certificate Template to Issue***.

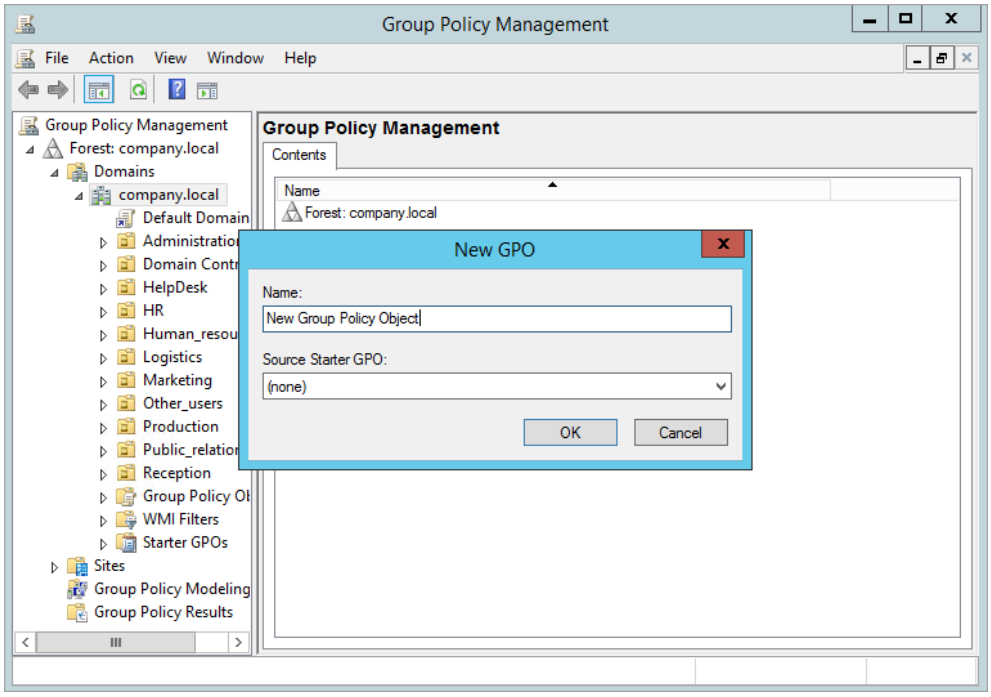


8.1.2. Publikacja certyfikatów dla użytkowników

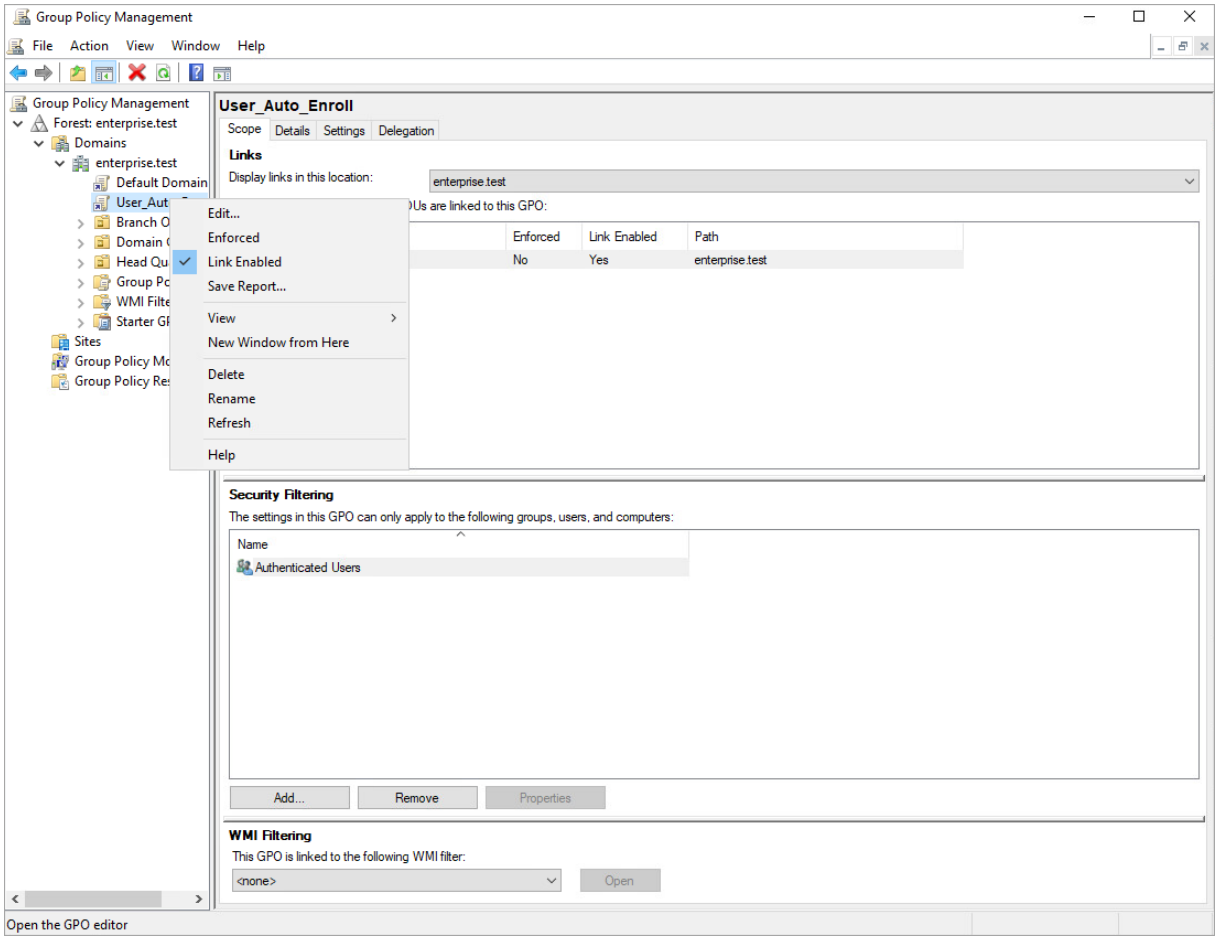
Na kontrolerze domeny **(maszyna XX-DC)** wyszukaj i otwórz ***Group Policy Management.*** W oknie struktury domeny rozwiń: ***Forest*** > ***Domains > enterprise.test > Enterprise Divisionsion***. Kliknij na wybrane OU prawym przyciskiem myszy i wybierz ***Create a GPO in this domain, and Link it here…***



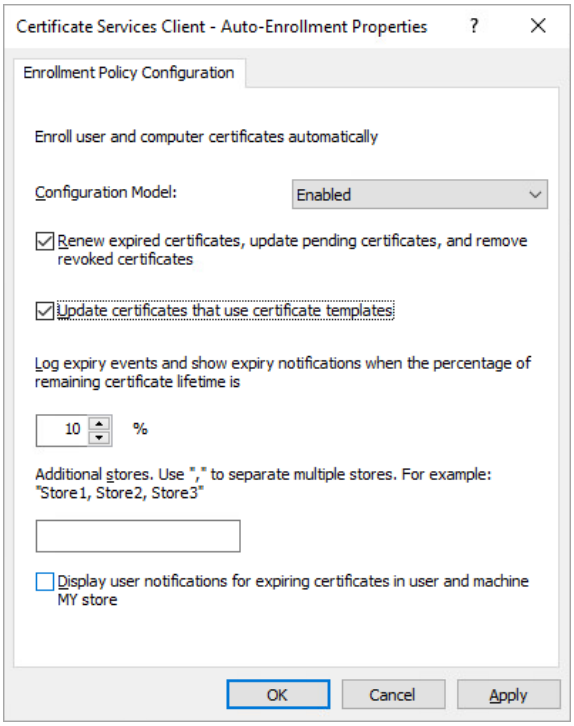
W wyświetlonym okienku wpisz nazwę dla nowego GPO i kliknij ***OK.***



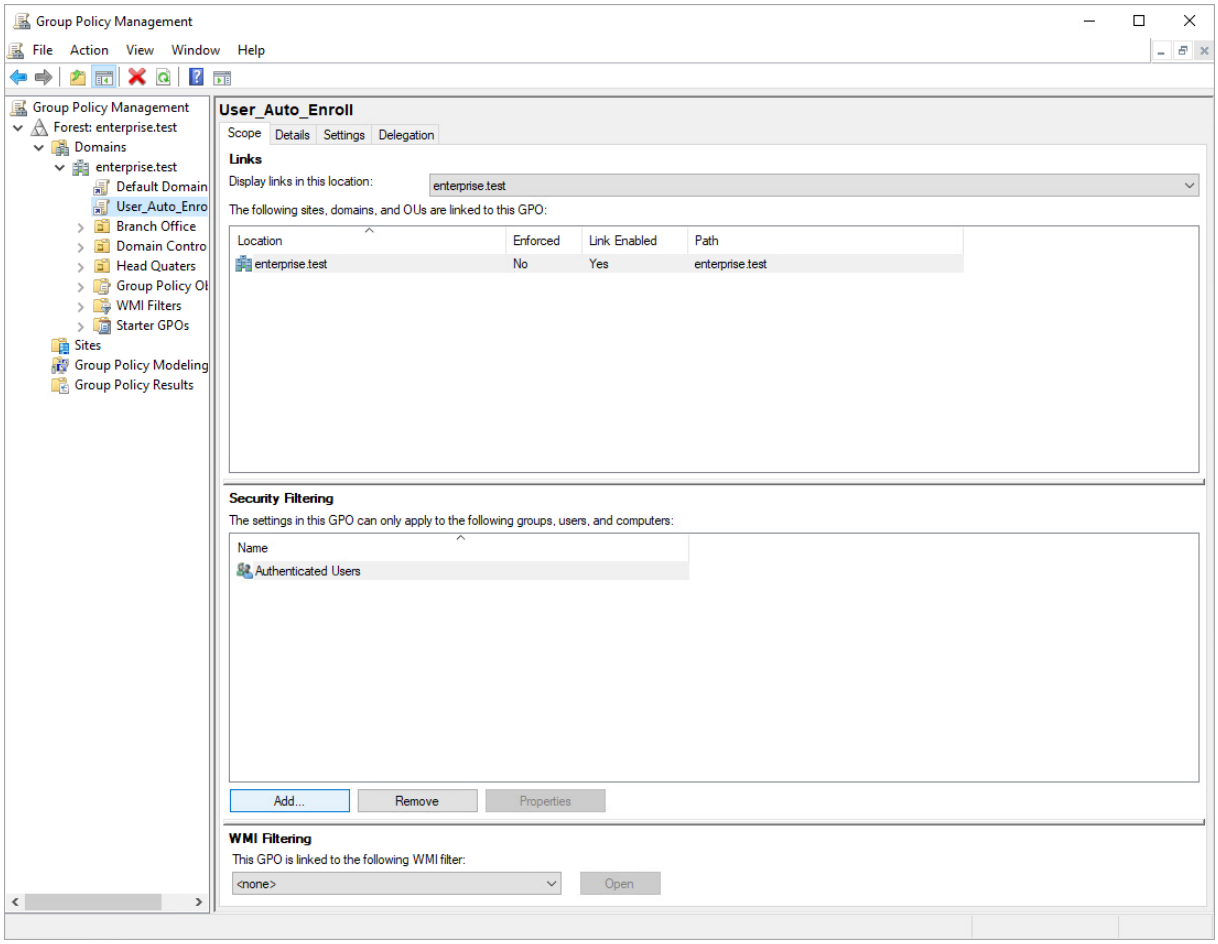
Kliknij prawym przyciskiem na dodane GPO i wybierz ***Edit***.



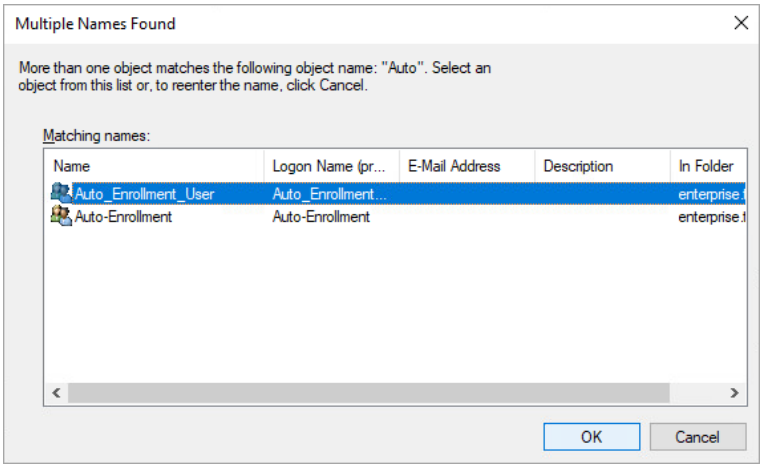
Przejdź do ***User Configuration*** > ***Policies*** > ***Windows Settings*** > ***Security Settings*** > ***Public Key Policies***. W zakładce ***Object Type*** wybierz ***Certificate Sercices Client - Auto-Enrollment***. Ustaw wartości tak jak na poniższym przykładzie.



Zatwierdź zmiany przyciskiem ***OK***, a następnie zamknij ***GPO Editor***. Przejdź do zakładki ***Scope*** nowo utworzonej polityki.



W sekcji ***Security Filtering*** dodaj utworzoną w poprzednim grupę bezpieczeństwa dedykowaną użytkownikom.

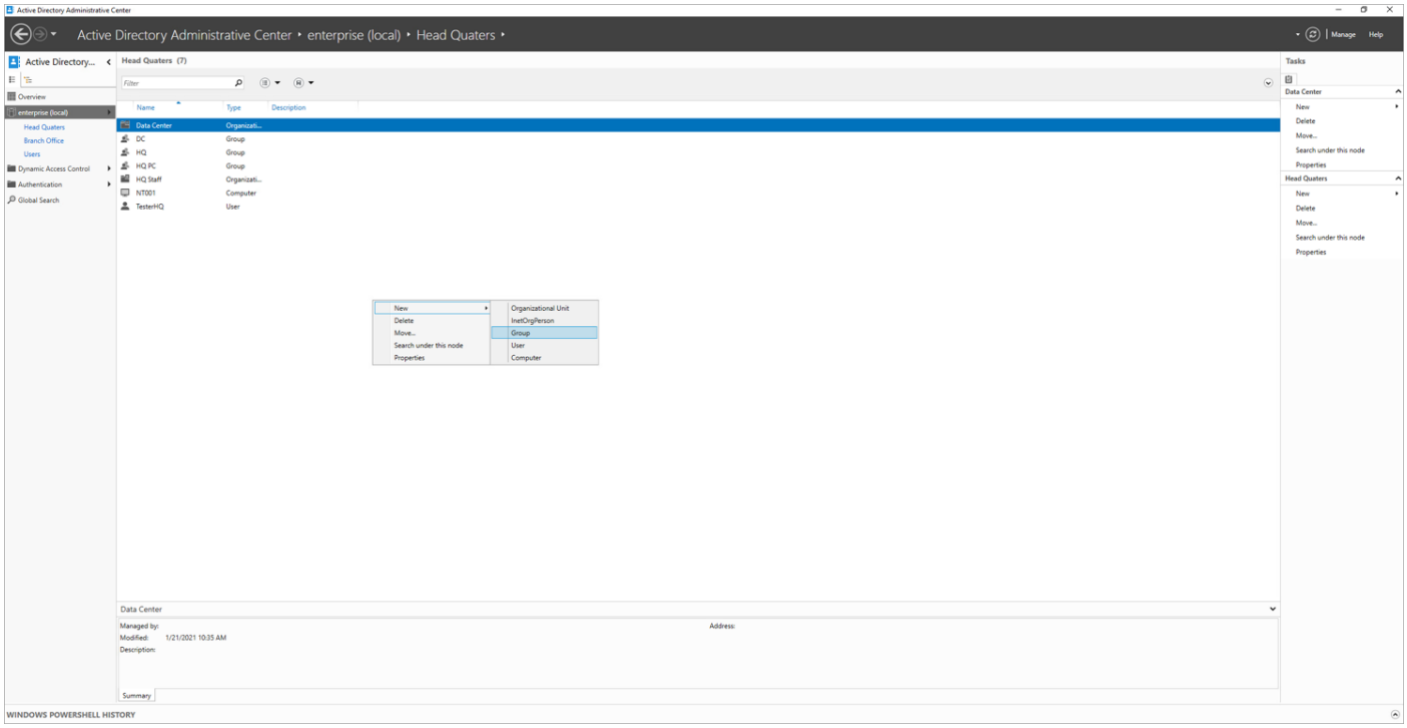


Zatwierdź przyciskiem ***OK*** i zamknij. Przy kolejnym logowaniu, certyfikat powinien zostać automatycznie wystawiony.

8.1.3. Tworzenie grup bezpieczeństwa dla urządzeń

Otwórz ***Active Directory Administrative Center*** na serwerze z możliwością zarządzania domeną **(maszyna XX-DC).**

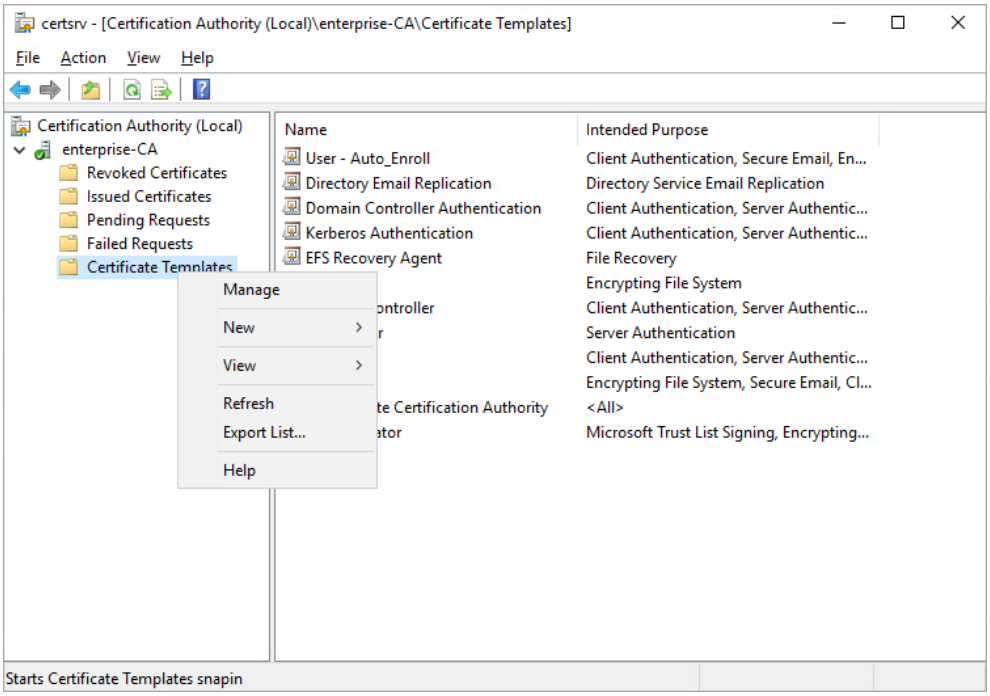
W OU *Enterprise Divisionsion* stwórz grupę bezpieczeństwa. W tym celu kliknij prawym przyciskiem myszy i wybierz *New > Group*. Komputery należące do tej grupy będą uczestniczyć w tzw. *auto-enrollment*.



Podobnie jak wcześniej dla użytkowników, teraz wprowadź nazwę grupy dla urządzeń (np. *Auto_Enrollment_Host*). Zapisz, klikając ***OK***.

Teraz dodaj komputer do utworzonej przed chwilą grupy. W tym celu kliknij prawym przyciskiem myszy na wybranym hoście i wybierz ***Add to group…*** Wpisz nazwę utworzonej wcześniej grupy. Zatwierdź przyciskiem ***OK***.

Zamknij AD AC, a następnie otwórz ***Certification Authority*** na serwerze z możliwością zarządzania AD CS (***Server Manager > Tools > Certification Authority,*** **maszyna XX-CA**). Kliknij prawym przyciskiem myszy na ***Certificate Templates***, a następnie wybierz ***Manage.***



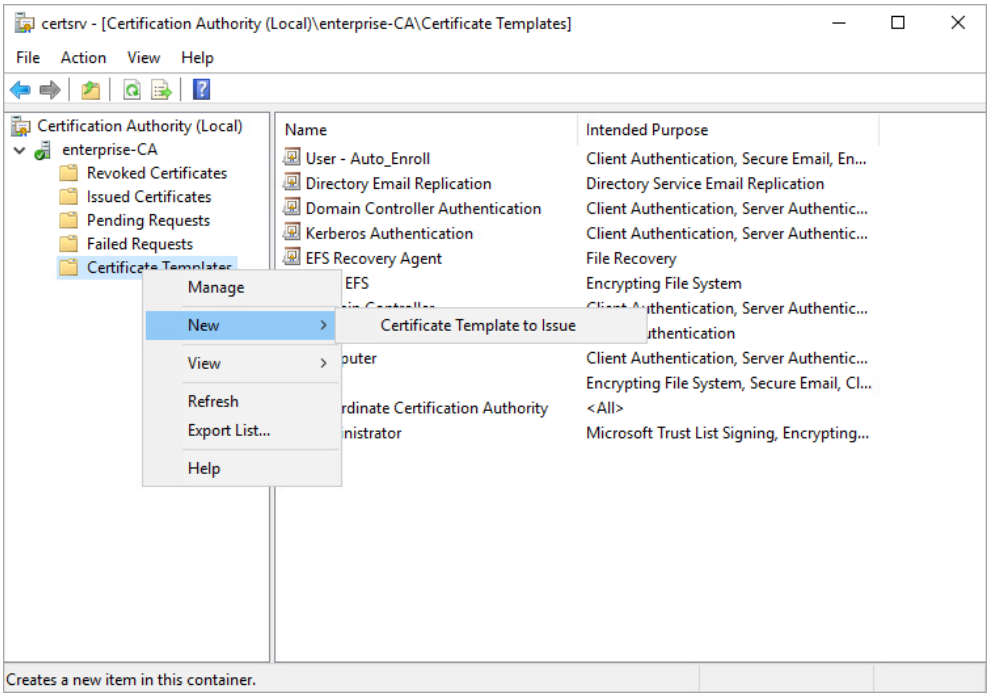
W panelu po prawej stronie powinny pojawić się szablony certyfikatów. Kliknij prawym przyciskiem myszy na szablon o nazwie ***Computer*** i wybierz ***Duplicate Template***.

Wprowadź zmiany w zakładkach wg poniższych zaleceń:

- ***Compatibility:*** wybierz właściwy system operacyjny dla urzędu certyfikacji oraz odbiorcy certyfikatu. Powinna to być najniższa wersja systemu operacyjnego funkcjonującego w środowisku.
- ***General:*** Zmień nazwę (np. Host - Auto Enroll) oraz ustaw okres ważności wg. zasad organizacji (zalecamy odnawianie nie częściej niż raz na rok). Zaznacz opcje ***Publish certificate in Active Directory*** oraz ***Do not automatically reenroll if a duplicate exists in Active Directory***.
- ***Cryptography***: zalecene min. 2048 bitowy klucz, a dla ważnych grup 4096.
- ***Security***: w sekcji ***Permissions for Domain Computers*** zaznacz opcje analogicznie, jak wcześniej dla użytkownika: Allow: Read, Enroll, Autoenroll.

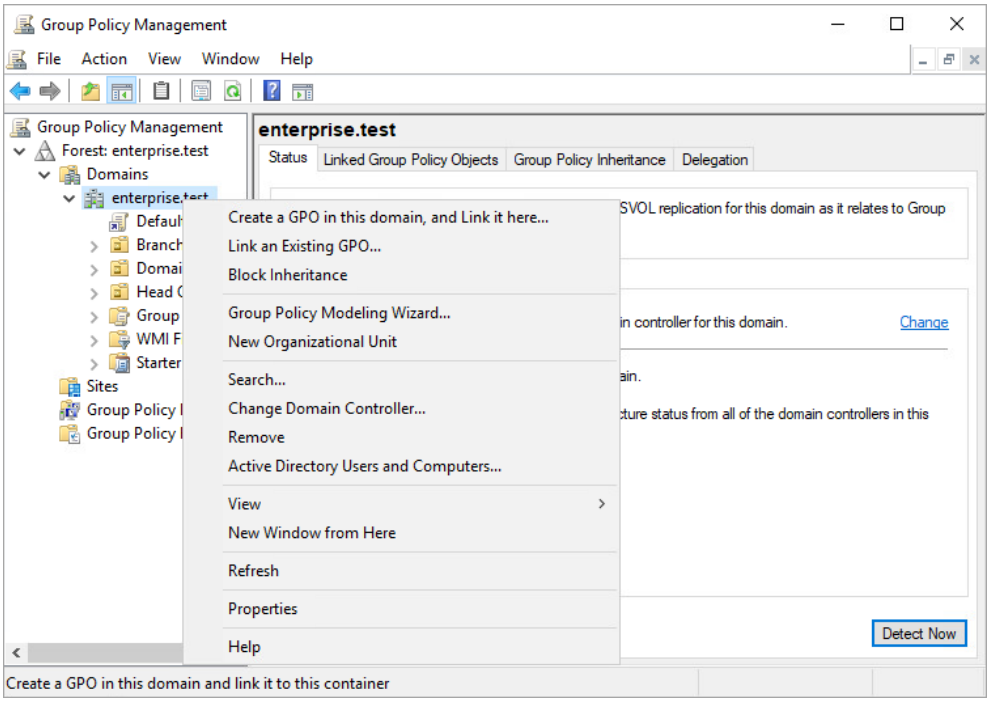
Wartości w pozostałych zakładkach pozostaw domyśle. Zatwierdź zmiany przyciskiem ***OK*** i zamknij panel zarządzania szablonami certyfikacji.

Dodaj nowo utworzony szablon do aktywnych szablonów. W tym celu kliknij prawym przyciskiem myszy na ***Certificate Templates*** i wybierz ***New*** > ***Certificate Template to Issue***.

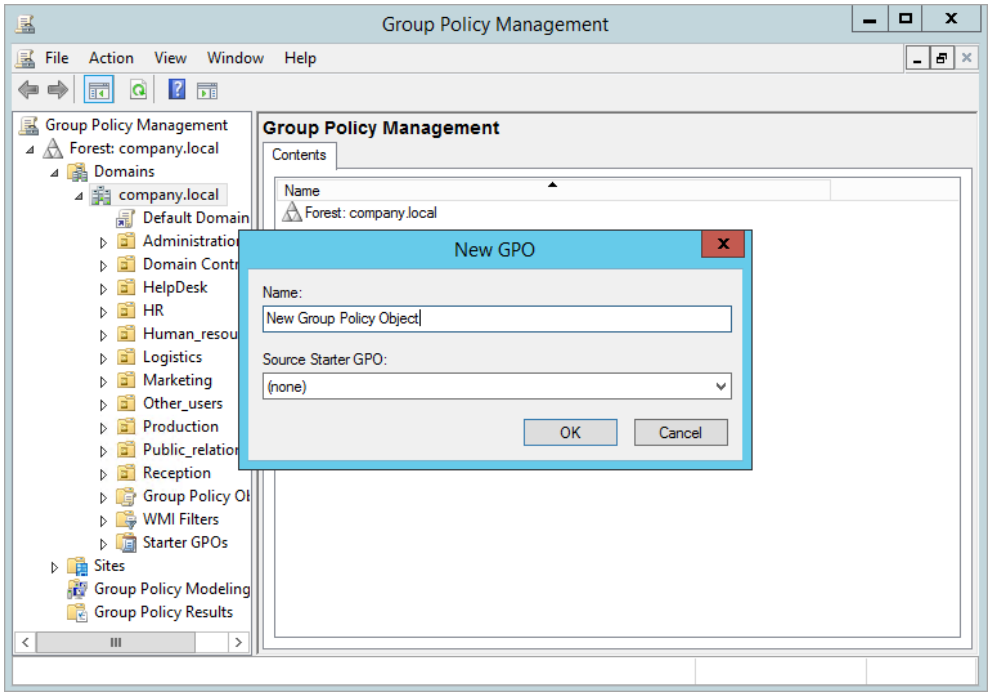


8.1.4. Publikacja certyfikatów dla urządzeń

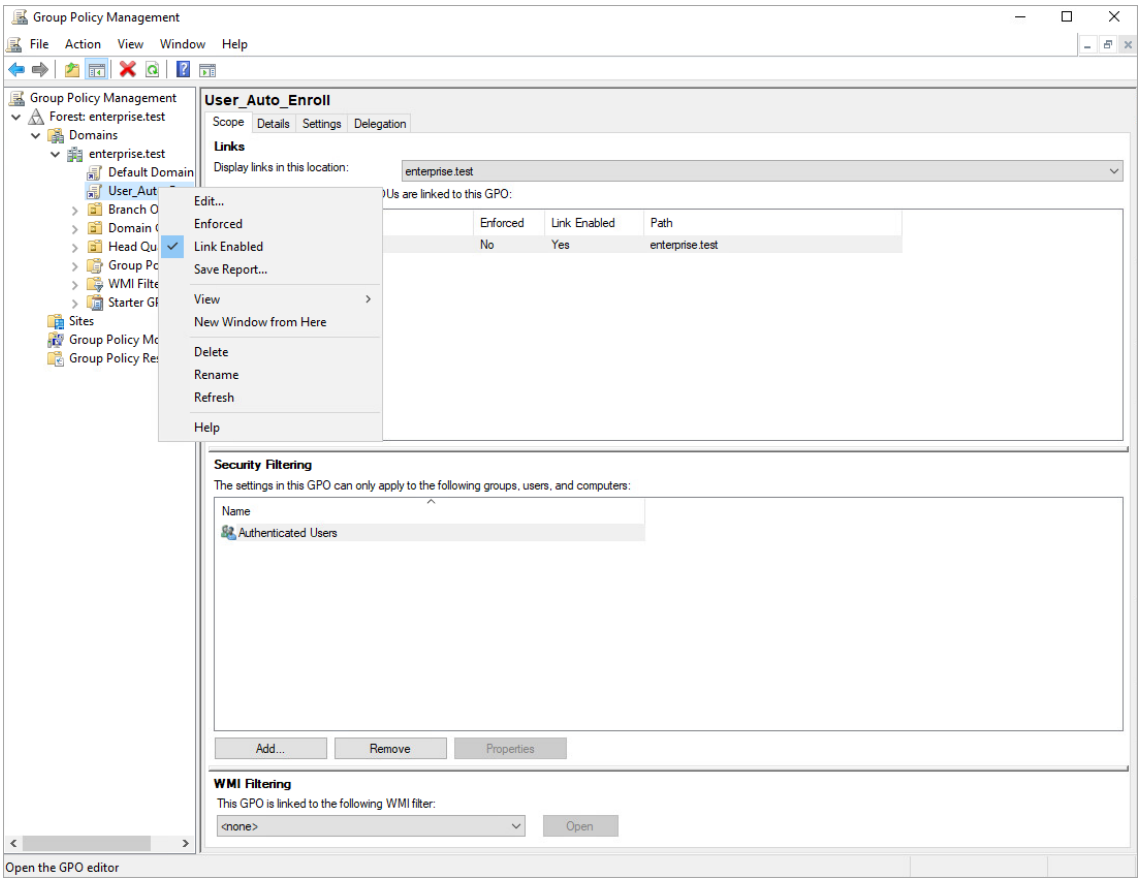
Na kontrolerze domeny **(maszyna XX-DC)** wyszukaj i otwórz ***Group Policy Management.*** W oknie struktury domeny rozwiń: ***Forest*** > ***Domains > enterprise.test > Enterprise Divisionsion***. Kliknij na wybrane OU prawym przyciskiem myszy i wybierz ***Create a GPO in this domain, and Link it here…***



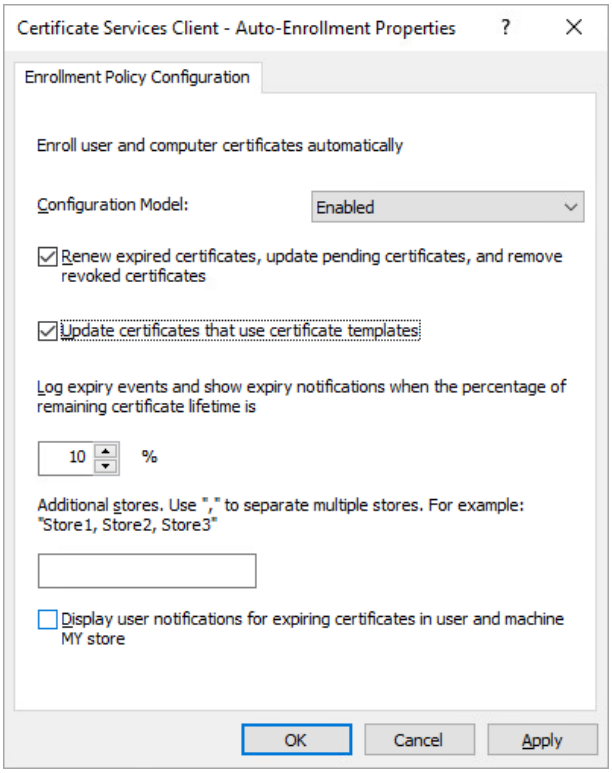
W wyświetlonym okienku wpisz nazwę dla nowego GPO i kliknij ***OK.***



Kliknij prawym przyciskiem na dodane GPO i wybierz ***Edit***.



Przejdź do ***Computer Configuration*** > ***Policies > Windows Settings*** > ***Security Settings*** > ***Public Key Policies***. W zakładce ***Object Type*** wybierz ***Certificate Services Client - Auto-Enrollment***. Ustaw wartości tak jak na poniższym przykładzie.



Zatwierdź zmiany przyciskiem ***OK***, a następnie zamknij ***GPO Editor***. Przejdź do zakładki ***Scope*** nowo utworzonej polityki.

W sekcji ***Security Filtering*** dodaj utworzoną w poprzednim grupę bezpieczeństwa dedykowaną urządzeniom.

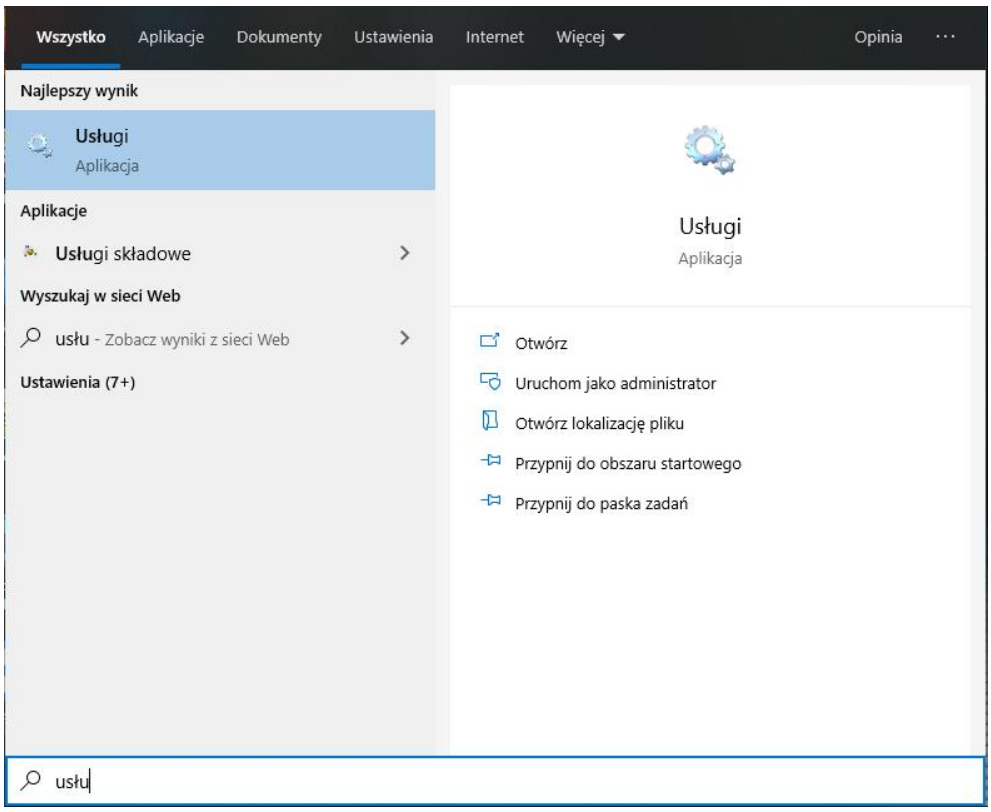
Zatwierdź przyciskiem ***OK*** i zamknij. Przy kolejnym logowaniu, certyfikat powinien zostać automatycznie wystawiony.

8.2. Konfiguracja klienta PEAP

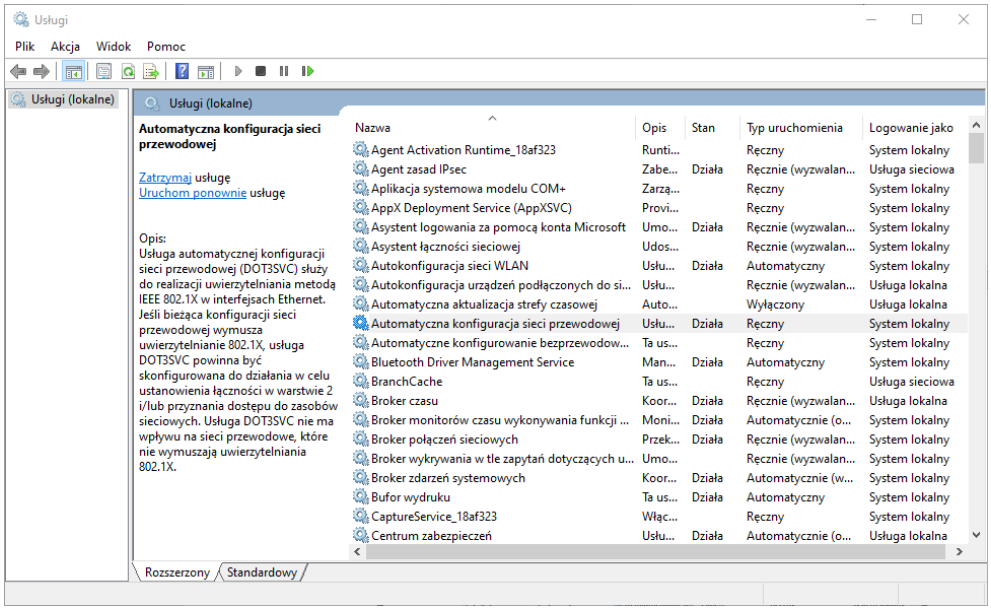
8.2.1. Konfiguracja ręczna klienta PEAP

W celu poprawnej komunikacji PEAP zalecane jest, aby zaimportować oraz zainstalować na komputerze certyfikat główny CA. W przypadku, gdy PKI jest na AD - nie jest to wymagane.

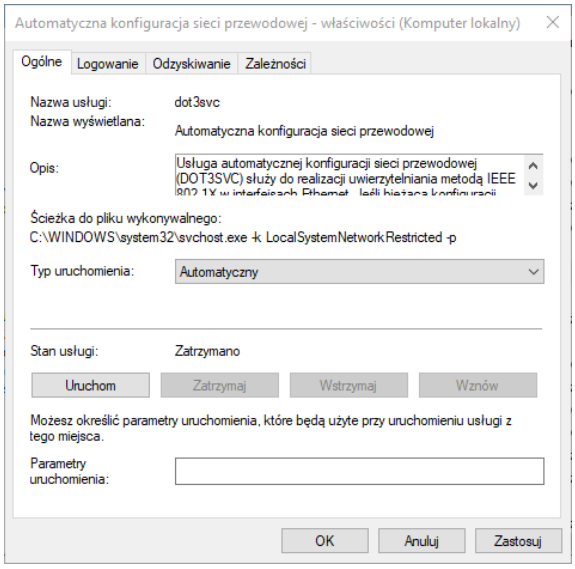
Na maszynie z Windows 11 **(NT1)** wyszukaj w systemie aplikację ***Usługi (Services)*** i otwórz ją.



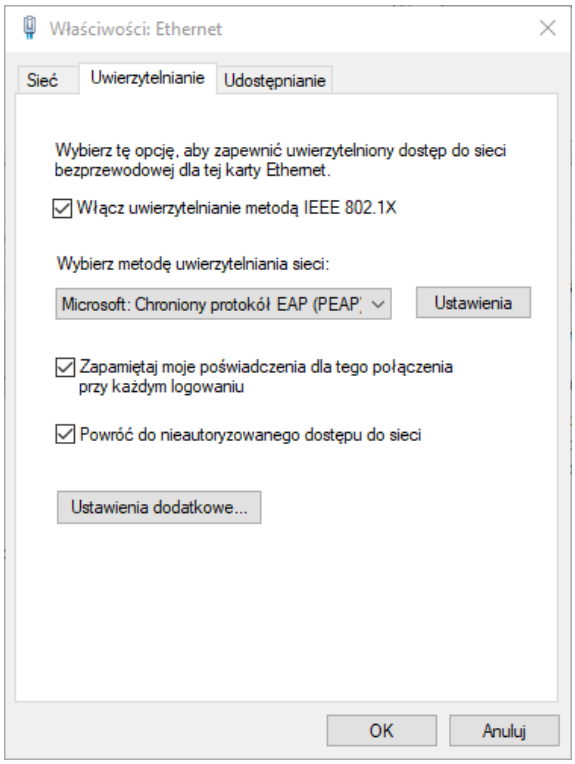
Na liście usług znajdź ***Automatyczna konfiguracja sieci przewodowej (Wired AutoConfig)*** i kliknij na nią dwukrotnie.



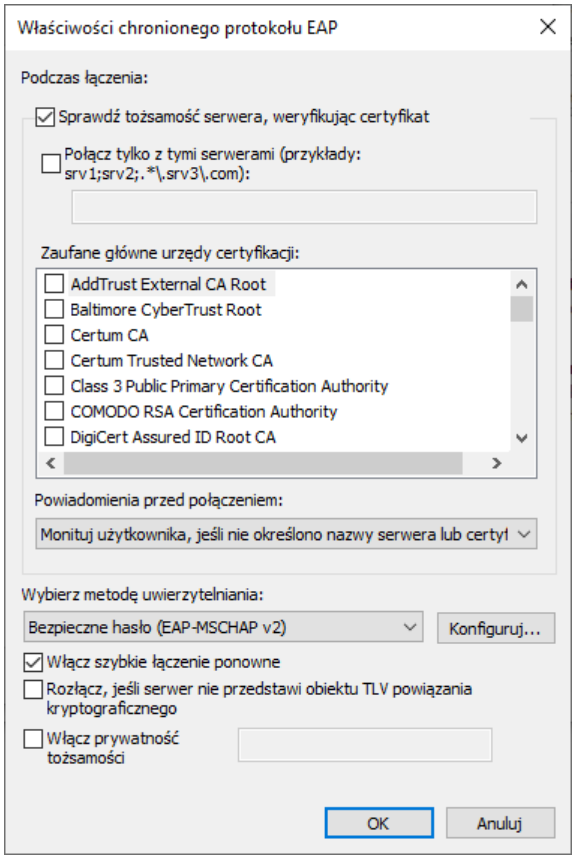
W wyświetlonym oknie w polu ***Typ uruchomienia*** wybierz ***Automatyczny***. Kliknij przycisk ***Uruchom*** i zatwierdź przyciskiem ***OK***.



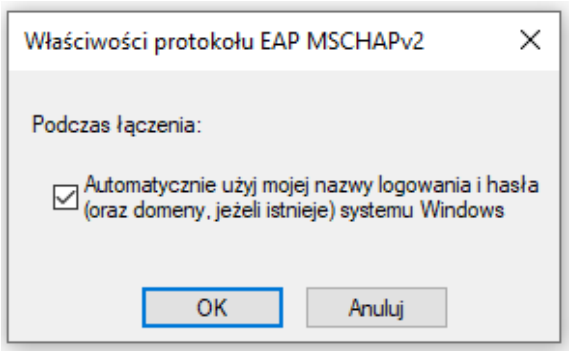
Wyszukaj w systemie ***Centrum sieci i udostępniania*** (Panel sterowania > Sieć i Internet > Centrum sieci i udostępniania. Z paska po lewej stronie wybierz ***Zmień ustawienia karty sieciowej***. Kliknij prawym przyciskiem myszy na sieć przewodową (druga karta sieciowa), którą chcesz skonfigurować i wejdź w jej ***Właściwości***. W wyświetlonym okienku przejdź do zakładki ***Uwierzytelnianie***.



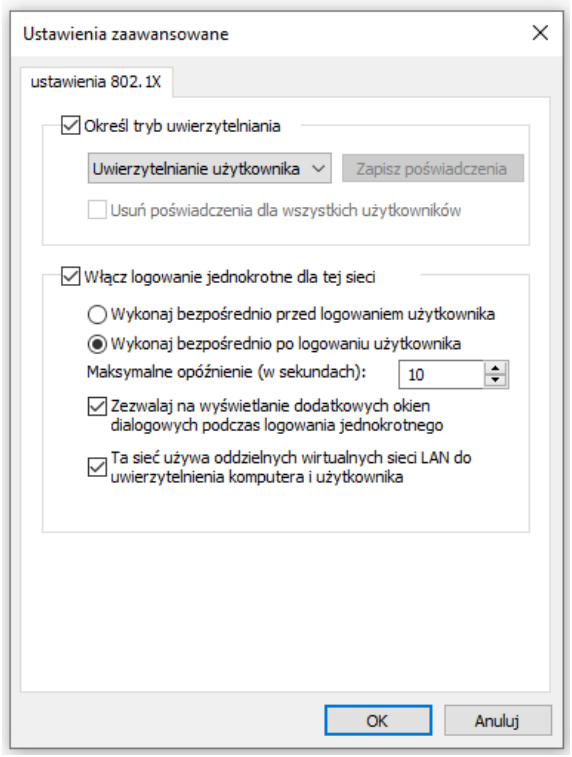
Jako metodę uwierzytelniania sieci wybierz ***Microsoft: Chroniony protokół EAP (PEAP)*** i kliknij ***Ustawienia***. W kolejnym oknie ponownie ustaw pola, jak na poniższym ekranie.



Kliknij ***Konfiguruj…*** i zaznacz opcję ***Automatycznie użyj mojej nazwy logowania i hasła (oraz domeny, jeżeli istnieje) systemu Windows***.



Zatwierdź dwukrotnie przyciskiem **OK**. Wejdź w ***Ustawienia dodatkowe…***. Zaznacz ***Określ tryb uwierzytelniania*** i z rozwijanej listy wybierz ***Uwierzytelnianie użytkownika lub komputer***. Zaznacz opcję ***Włącz logowanie jednokrotne do tej sieci.***



Kliknij ***Zapisz poświadczenia***. Zatwierdź przyciskiem ***OK*** wszystkie otwarte okna. Możesz połączyć się z siecią.

8.2.2. Weryfikacja działania polityk

Po poprawnej konfiguracji ustawień sieciowych na maszynie testowej Windows 11 **(NT1)** sprawdź na karcie sieciowej czy nastąpiło połączenie. Wyłącz pierwszą kartę sieciową komputera i włącz drugą. Zweryfikuj w ***Zdarzeniach autoryzacji*** czy pojawił się zapis o poprawnej autoryzacji oraz jaki typ został użyty. Sprawdź jaka polityka dopuściła, jaki VLAN, oraz jaki adres IP został nadany.

Zaloguj się do urządzenia sieciowego i wykonaj polecenia:
`show dot1x all summary` oraz `show dot1x interface gigabitEthernet 1/0/1 details`.

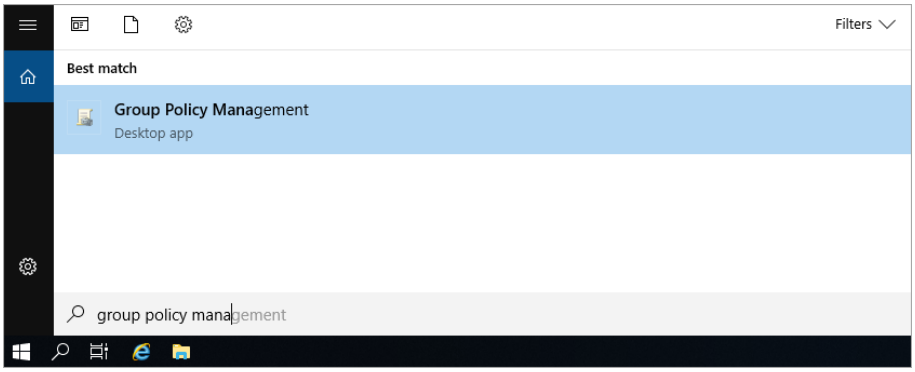
Więcej szczegółów w Cisco C1000: `show authentication sessions interface gi1/0/1 det`

Następnie wyloguj użytkownika z systemu i powtórz powyższe czynności.

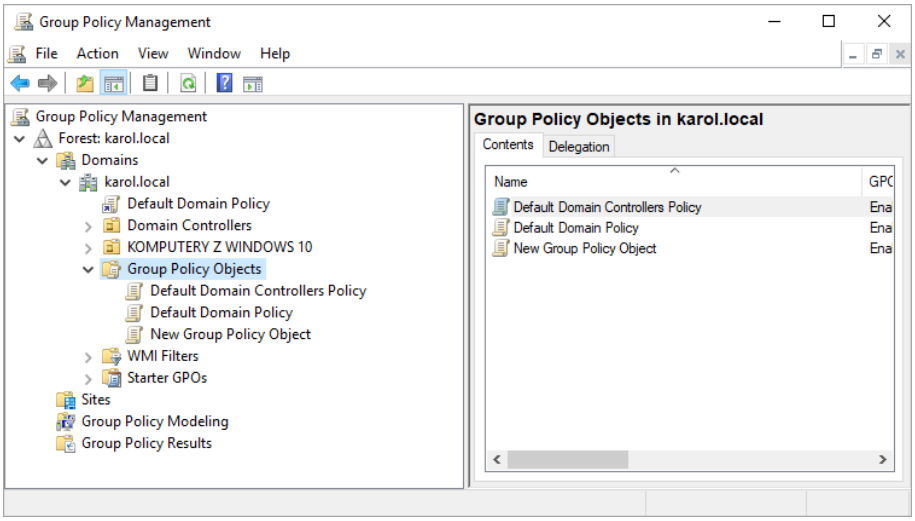
8.3. Konfiguracja klienta TLS

8.3.1. Konfiguracja klienta TLS poprzez GPO

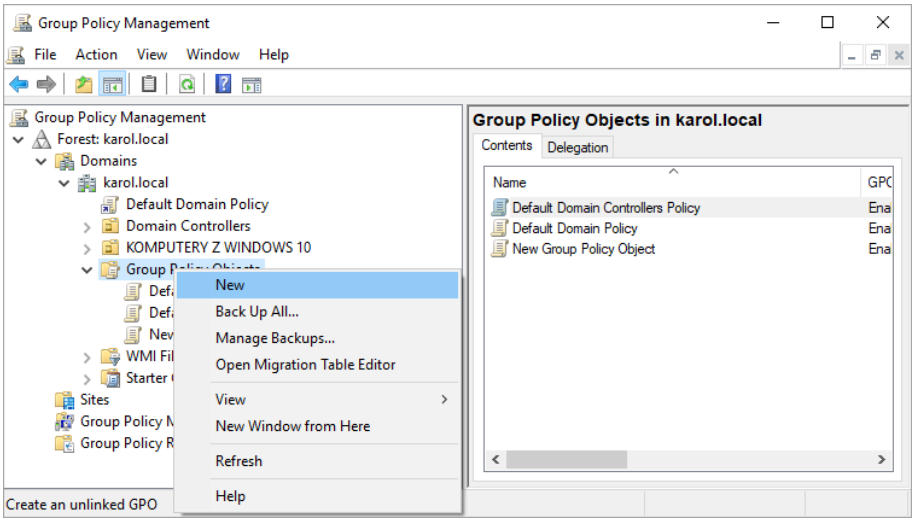
Na kontrolerze domeny (maszyna **XX-DC**) wyszukaj i otwórz ***Group Policy Management.***



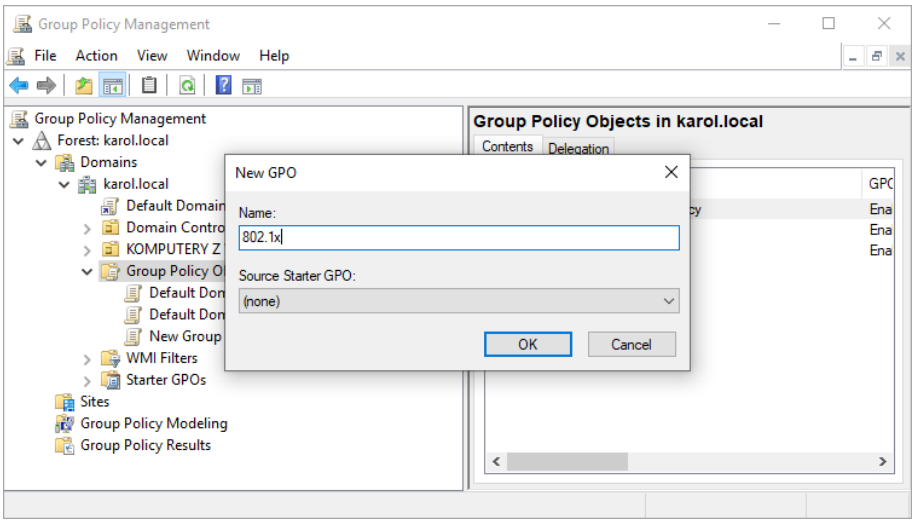
Przejdź do ***Group Policy Objects*** - w tym celu w oknie struktury domeny rozwiń: ***Forest > Domains >*** *wybrana domena lub jednostka organizacyjna*.



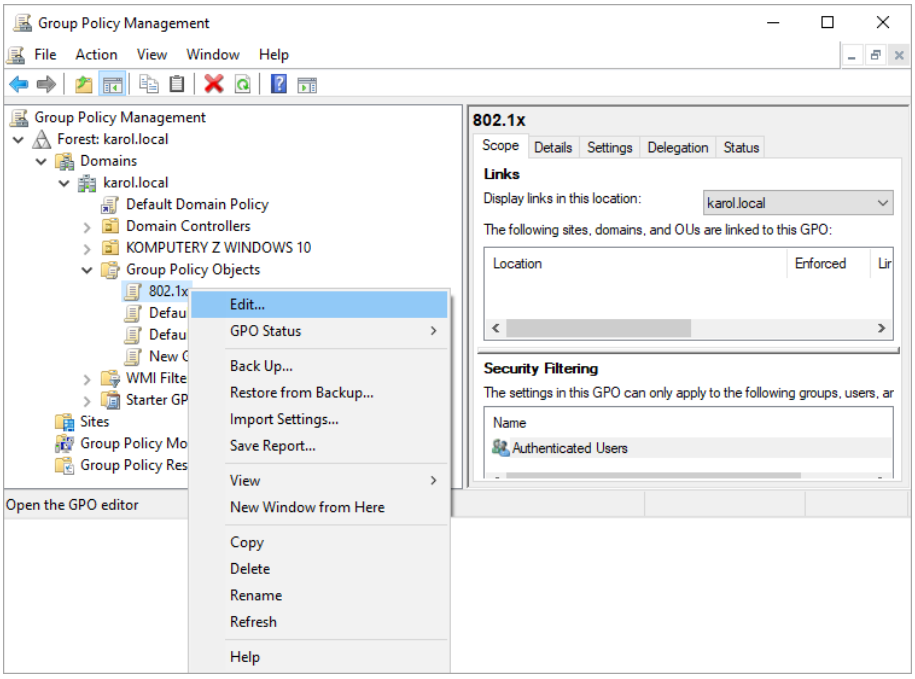
Kliknij prawym przyciskiem myszy na ***Group Policy Object*** i wybierz ***New***.



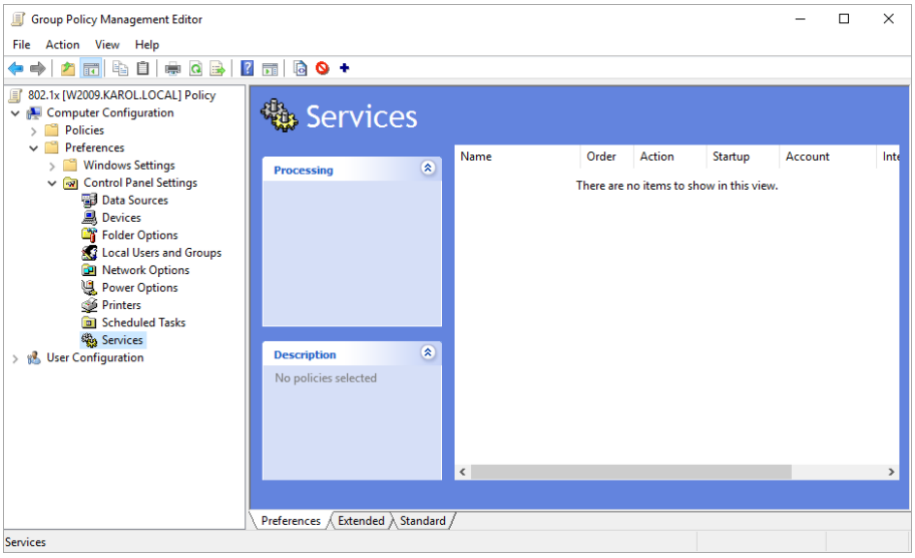
W wyświetlonym okienku wpisz nazwę dla nowego GPO i kliknij ***OK***.



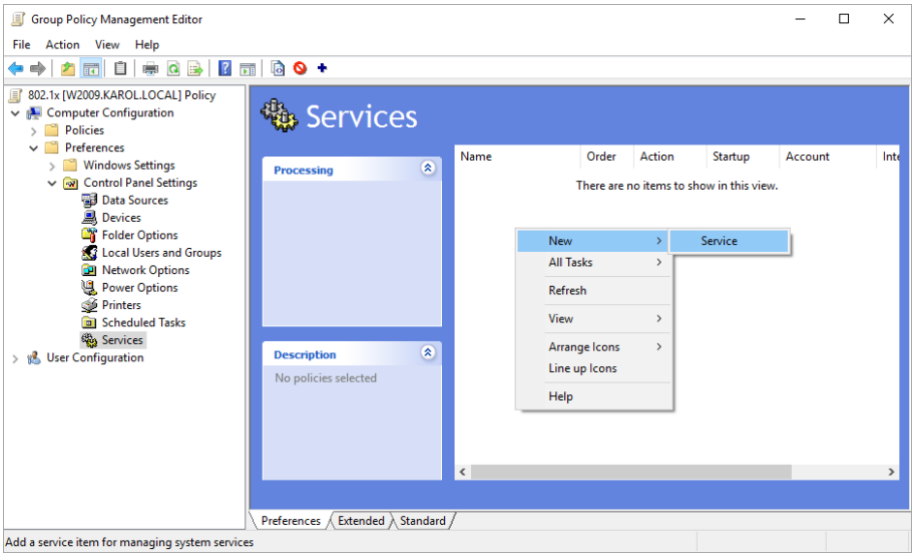
Z menu kontekstowego wybierz opcję ***Edit…*** dla nowego GPO.



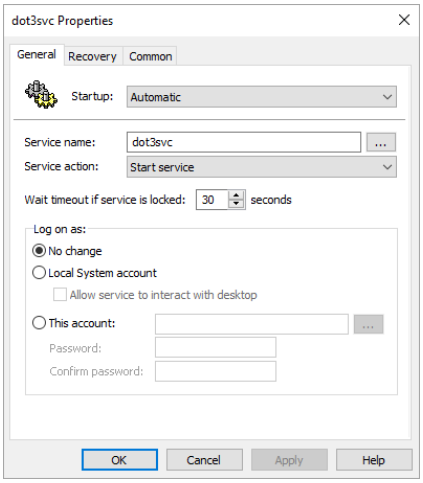
W oknie Group Policy Management Editor wyszukaj opcję ***Services*** (***Computer Configuration > Preferences > Control Panel Settings > Services***).



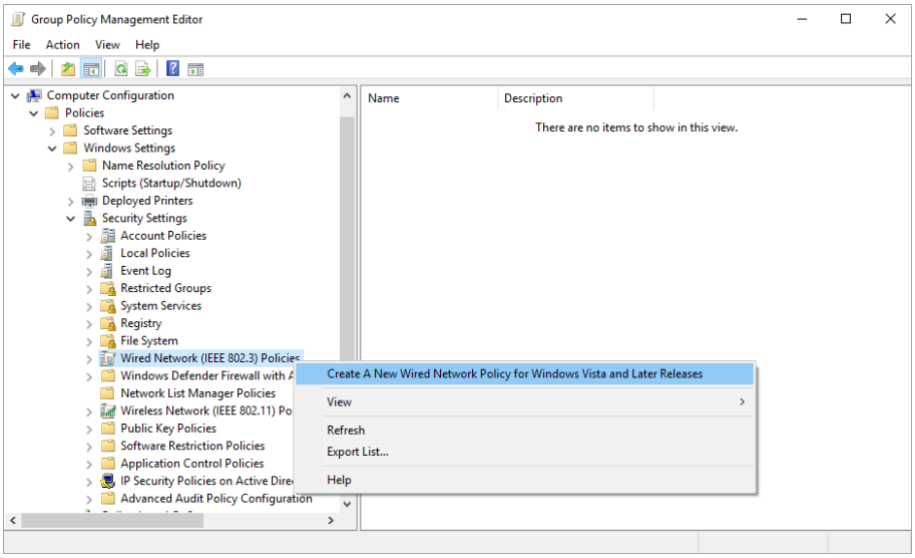
Z menu kontekstowego wybierz opcję ***New***, a następnie ***Service***.



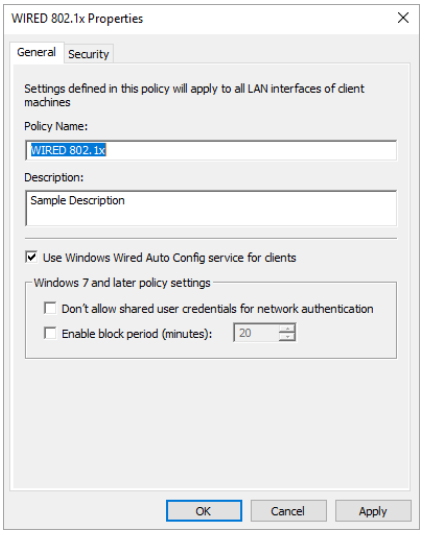
Ustaw parametry jak na ekranie poniżej, by skonfigurować automatyczne uruchomienie usługi suplikanta na komputerach użytkowników końcowych z systemem Windows. Zakładki ***Recovery*** oraz ***Common*** pozostaw bez zmian.



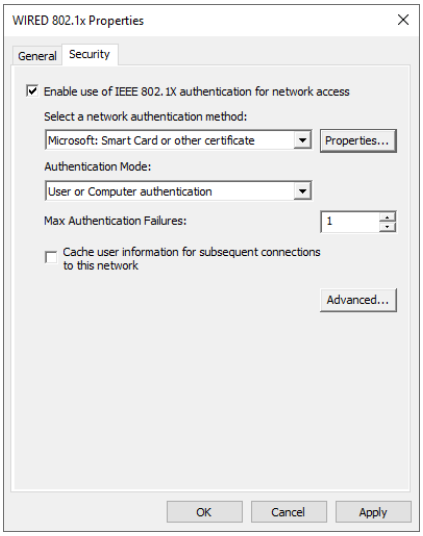
Przejdź do ustawień zabezpieczeń (***Computer Configuration > Policies > Windows Settings > Security Settings***), kliknij prawym przyciskiem myszy na ***Wired Network (IEEE 802.3) Policies***, a następnie wybierz ***Create A New Wired Network Policy for Windows Vista and Later Releases.***



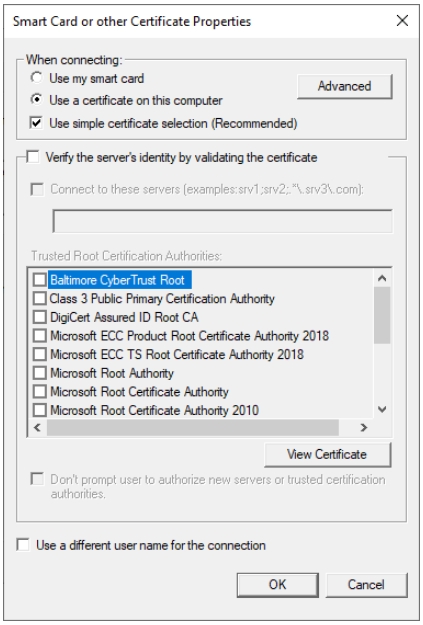
W wyświetlonym okienku, w zakładce ***General*** nadaj nazwę nowej polityce.



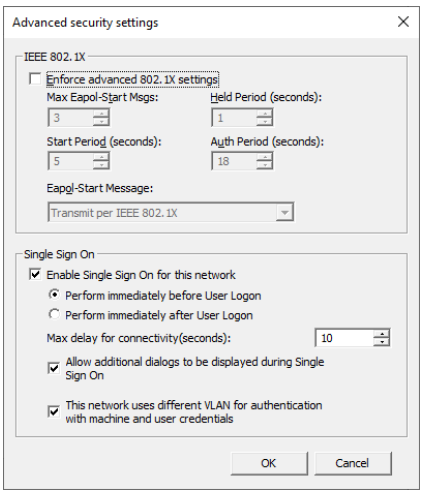
Przejdź do zakładki ***Security*** i ustaw parametry jak na ekranie poniżej.



Naciśnij przycisk ***Properties…***, ustaw parametry zgodnie z poniższym ekranem, zaznacz na liście certyfikat **pki.enterprise.test** i kliknij ***OK***.

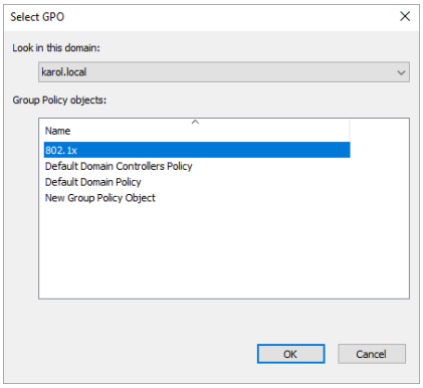


Kliknij na ***Advanced…*** i ustaw parametry jak na poniższym ekranie.

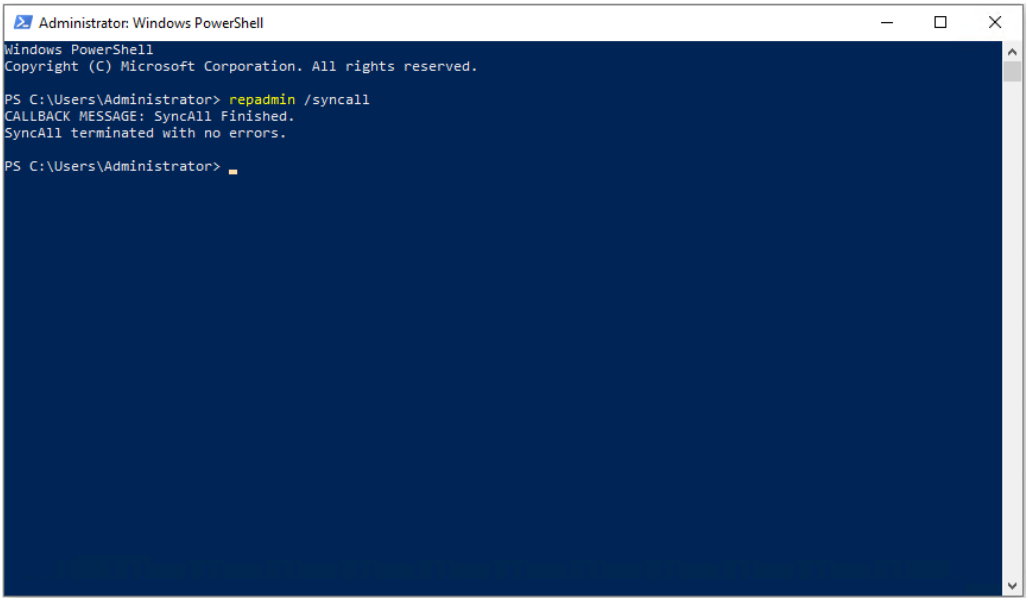


GPO jest gotowe. Zamknij wszystkie modalne okna, zatwierdzając przyciskiem ***OK***.

Podłącz nowe GPO do istniejącej grupy obiektów (Enterprise Divisionsion), do których nowe ustawienia mają być zastosowane. W tym celu kliknij prawym przyciskiem myszy na daną grupę obiektów, a następnie wybierz ***Link an Existing GPO…*** Wybierz konfigurowane przed chwilą GPO i kliknij ***OK***.



Aby przyspieszyć replikację nowego GPO, uruchom (z uprawnieniami administratora) program PowerShell na serwerze, na którym go skonfigurowałeś. Użyj polecenia ***repadmin /syncall*** i zatwierdź komendę. Jeżeli replikacja się powiedzie, zobaczysz komunikat o powodzeniu operacji („SyncAll terminated with no errors").



Poczekaj na rozpropagowanie ustawień wśród komputerów w domenie. Od tej pory suplikant na urządzeniach końcowych jest skonfigurowany. Dla większej sieci możesz dodać więcej polityk w celu przydziału odpowiednich zasobów w zależności od tożsamości, rodzaju autoryzacji i/lub grup obiektów.

Aby można było z powodzeniem uwierzytelniać komputery i użytkowników za pomocą NACVIEW w oparciu o ich certyfikaty, zażądaj (z poziomu stacji roboczej) osobnych certyfikatów dla tych obiektów.

8.3.2. Weryfikacja działania polityk

Po poprawnej konfiguracji ustawień sieciowych na maszynie testowej Windows 11 **(NT-1)** sprawdź na karcie sieciowej czy nastąpiło połączenie. Zweryfikuj w ***Zdarzeniach autoryzacji*** czy pojawił się zapis o poprawnej autoryzacji oraz jaki typ został użyty. Sprawdź jaka polityka dopuściła, jaki VLAN, oraz jaki adres IP został nadany.

```
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)#
```

Zaloguj się do urządzenia sieciowego i wykonaj polecenia: **`show dot1x all summary`** oraz **`show dot1x interface gigabitEthernet 1/0/1 details`**.

Więcej szczegółów w Cisco C1000: **`show authentication sessions interface gi1/0/1 det`**

Następnie wyloguj użytkownika z systemu i powtórz powyższe czynności.

9. Pozostałe ustawienia

9.1. Backup

Z listy kreatorów wybierz opcję ***Backup***. Skonfiguruj kopię zapasową danych oraz logów na zdalną lokalizację. W tym celu przejdź do edycji i uzupełnij formularz, wpisując następujące dane:

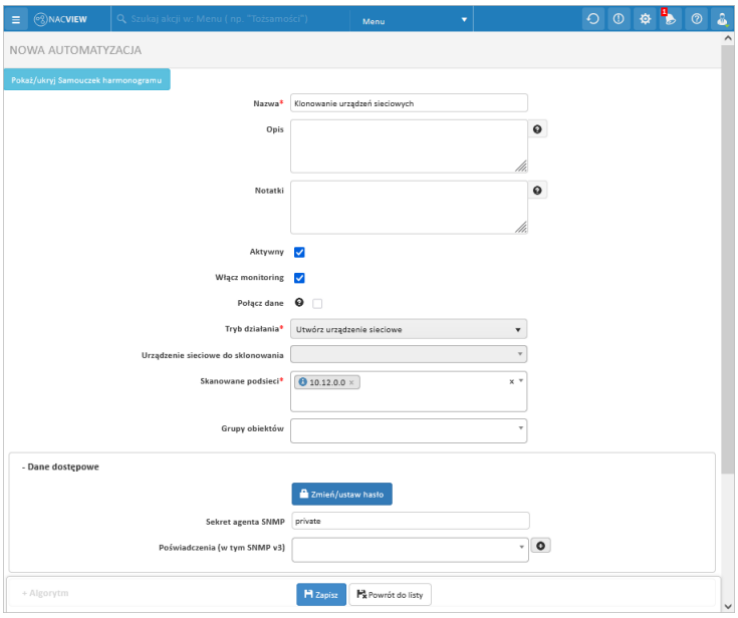
- **Protokół komunikacji**: SMB
- **Wersja protokołu komunikacji:** 3.0
- **Zdalny host:** 10.XX.166.2
- **Katalog**: \NV_Backup
- **Nazwa użytkownika:** administrator@enterprise.test
- **Hasło**: NACVIEW_SZKOLENIE22
- **Cykliczna kopia zapasowa:** Włączona
- **Interwał**: co miesiąc
- **Uwzględniaj logi**: Nie

Zapisz ustawione wartości. Aby wgrać zmiany do systemu naciśnij ***Zastosuj konfigurację***. System w ciągu 5 minut ustawi żądane parametry.

9.2. Automatyzacja

Z menu głównego NACVIEW wybierz ***Automatyzacja*** *(*sekcja ***Konfiguracja****)*. Kliknij ***Dodaj nową pozycję***, a następnie ***Automatyzacja uzupełniająca***. Uzupełnij formularz następującymi danymi:

- **Nazwa**: Klonowanie urządzeń sieciowych
- **Tryb działania**: Utwórz urządzenie sieciowe
- **Skanowanie podsieci**: 10.XX.166.0/24
- **Sekret agenta SNMP**: NVPrivate
- **Powiadomienie:** admin@nacview.com



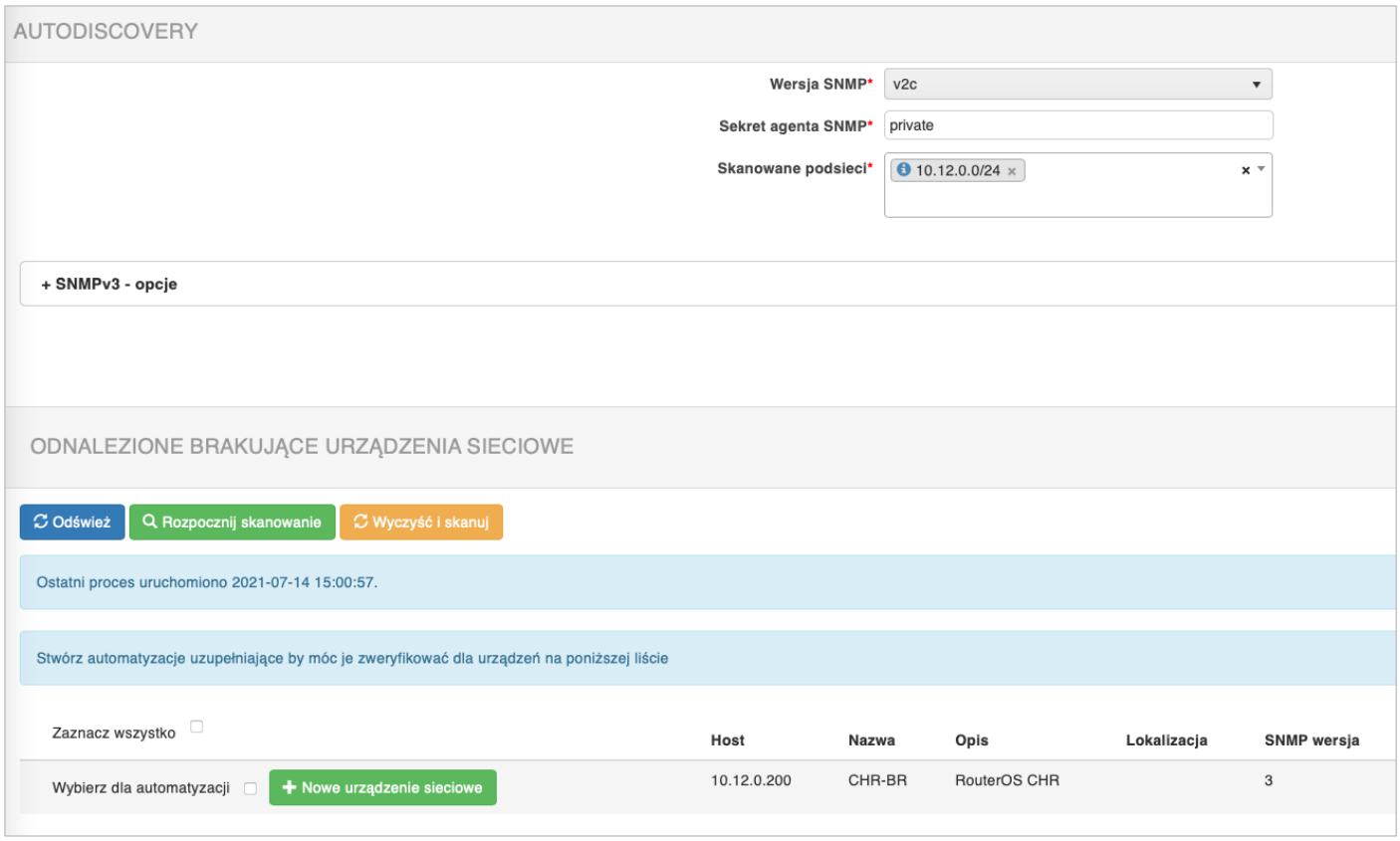
Zapisz ustawione wartości.

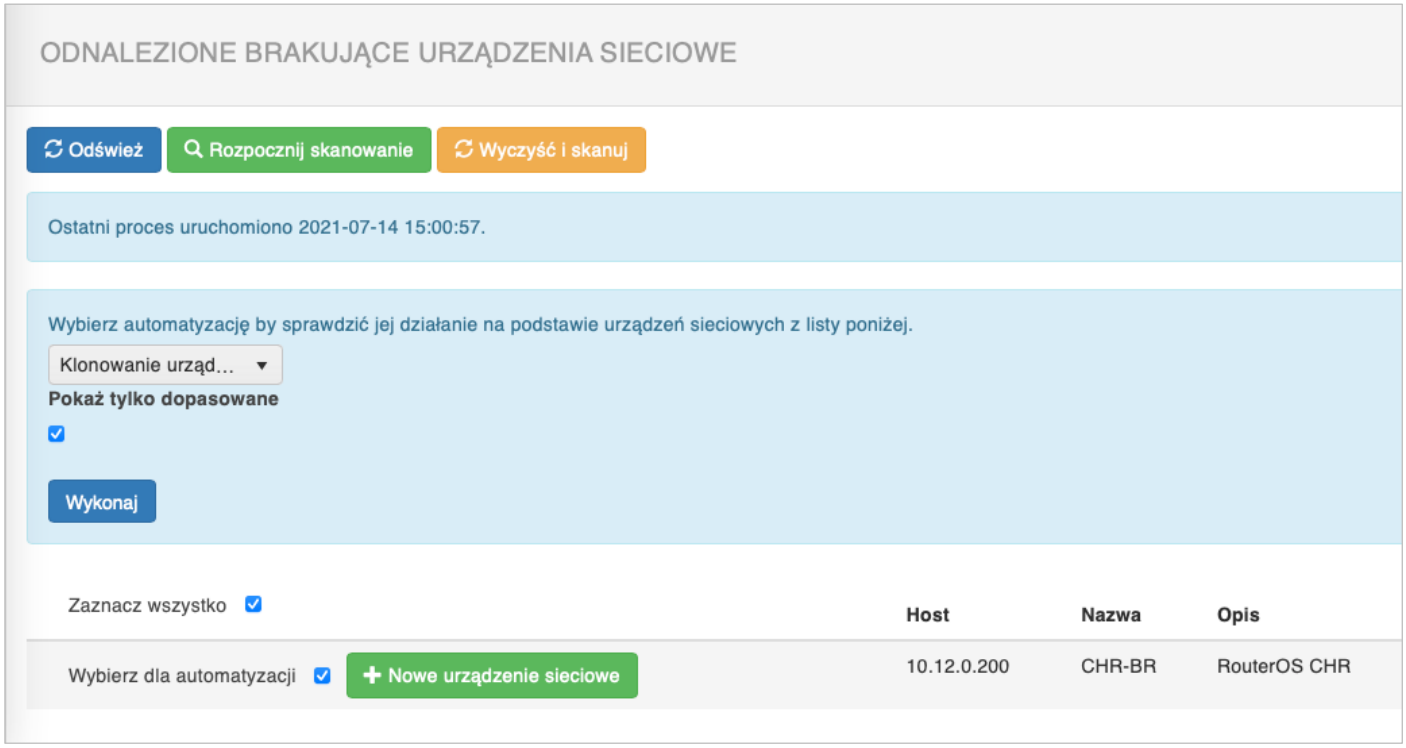
9.3. Autodiscovery

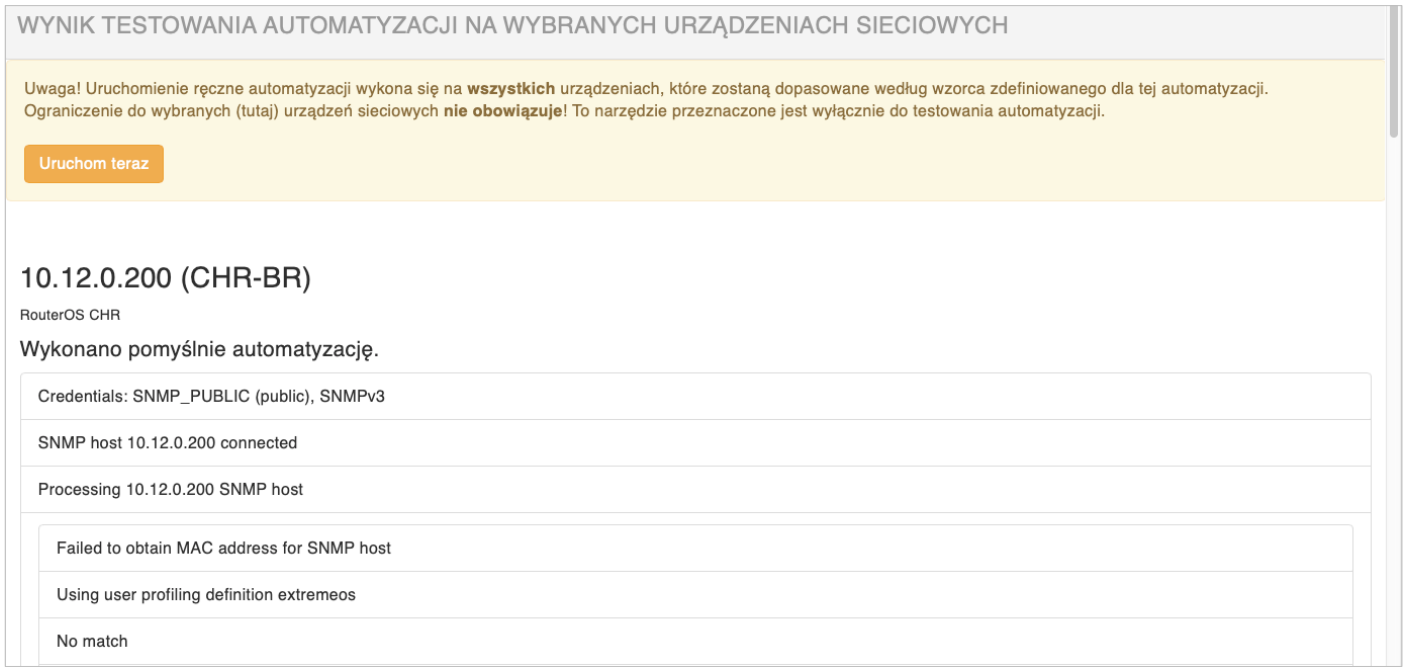
Z menu głównego wybierz Autodiscovery. Uzupełnij pola formularza:

- **Wersja SNMP**: v2c
- **Sekret agenta SNMP**: NVPrivate
- **Skanowanie podsieci**: 10.XX.166.0/24

Kliknij ***Zapisz***, a następnie Rozpocznij skanowanie. Powinien wyświetlić się komunikat: “Proces wyszukiwania urządzeń w podsieciach jest aktywny!". Aby zobaczyć znalezione obiekty, kliknij ***Odśwież***. Zaznacz znalezione obiekty polem ***Zaznacz wszystko***, a następnie z rozwijanego menu wybierz ***Klonowanie urządzeń sieciowych***. Kliknij ***Wykonaj***. W nowo otwartym oknie, uruchom symulację automatyzacji, klikając ***Uruchom teraz***.



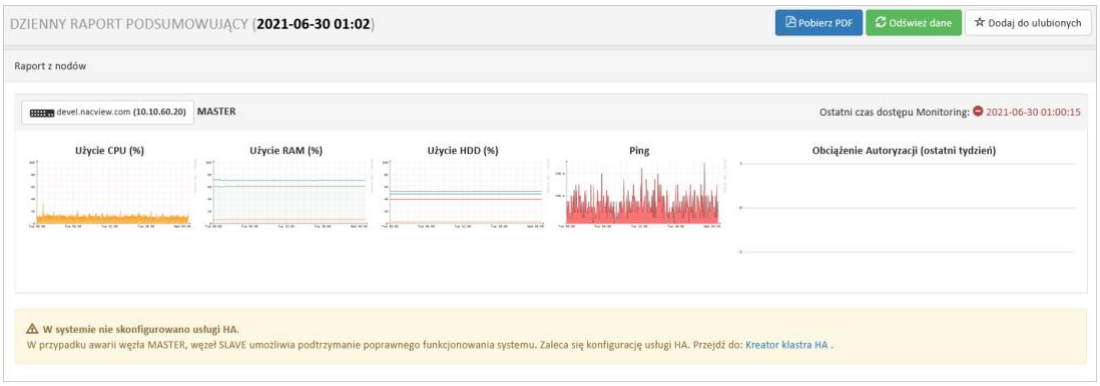




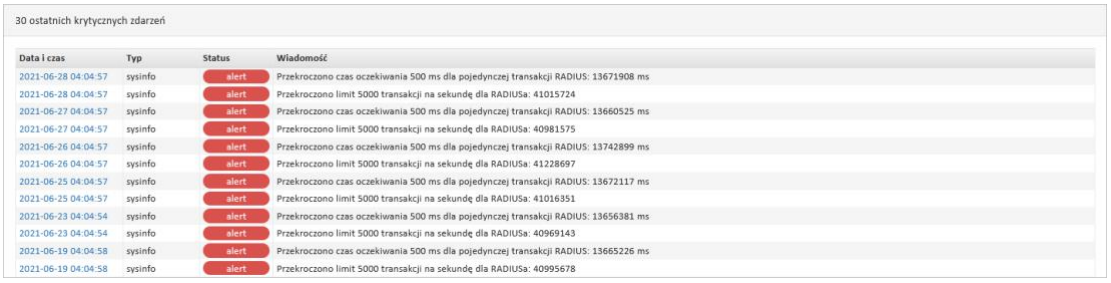
9.4. Raport dobowy, status systemu

Aby przejść do raportu dobowego, z menu głównego z sekcji ***Pulpit*** wybierz ***Raport podsumowujący***. Przeanalizuj kolejno wszystkie sekcje znajdujące się w raporcie.

Raport z nodów

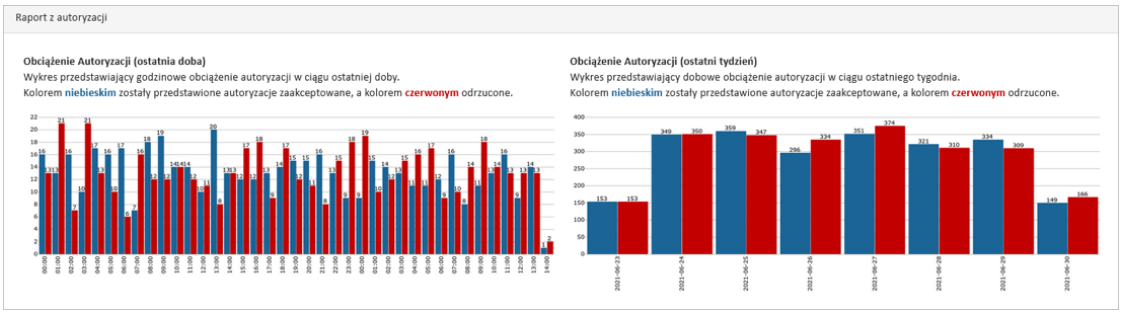


30 ostatnich krytycznych zdarzeń

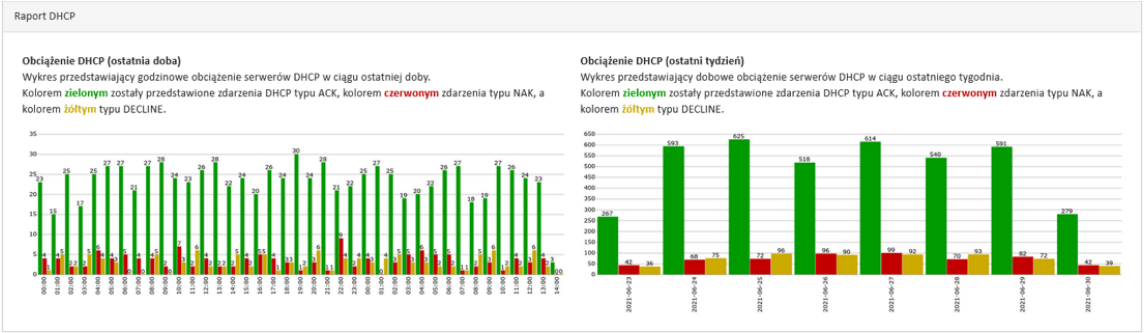


Data i czas	Typ	Status	Wiadomość
2021-06-28 04:04:57	sysinfo	alert	Przekroczono czas oczekiwania 500 ms dla pojedynczej transakcji RADIUS: 13671908 ms
2021-06-28 04:04:57	sysinfo	alert	Przekroczono limit 5000 transakcji na sekundę dla RADIUSa: 41015724
2021-06-27 04:04:57	sysinfo	alert	Przekroczono czas 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

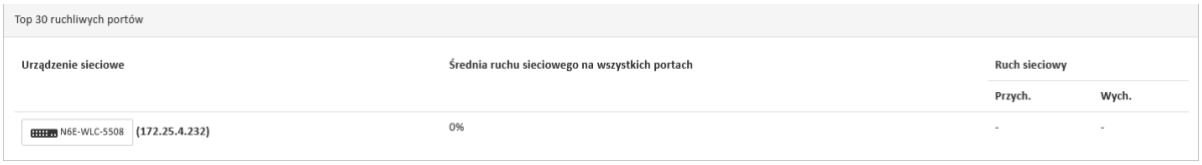
Raport z autoryzacji



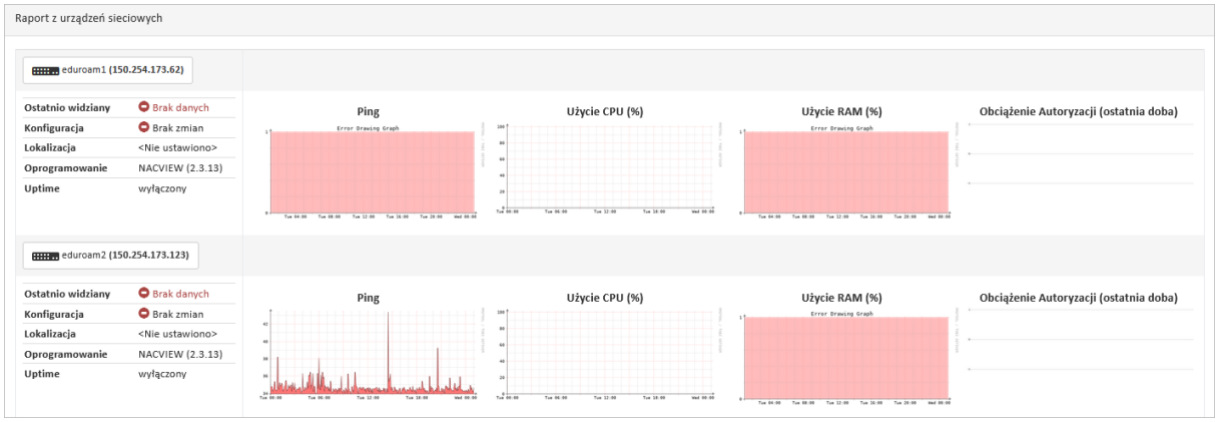
Raport DHCP



Top 30 ruchliwych portów

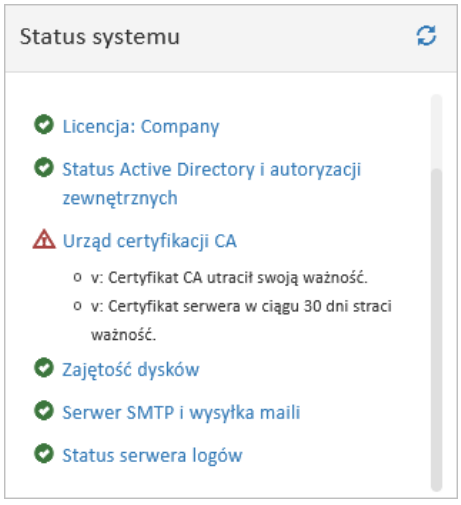


Raport z urządzeń sieciowych



Niezaufane serwery DHCP

Aby podejrzeć status systemu, z paska nawigacyjnego wybierz przycisk  . Przeanalizuj poszczególne elementy znajdujące się w tej sekcji.



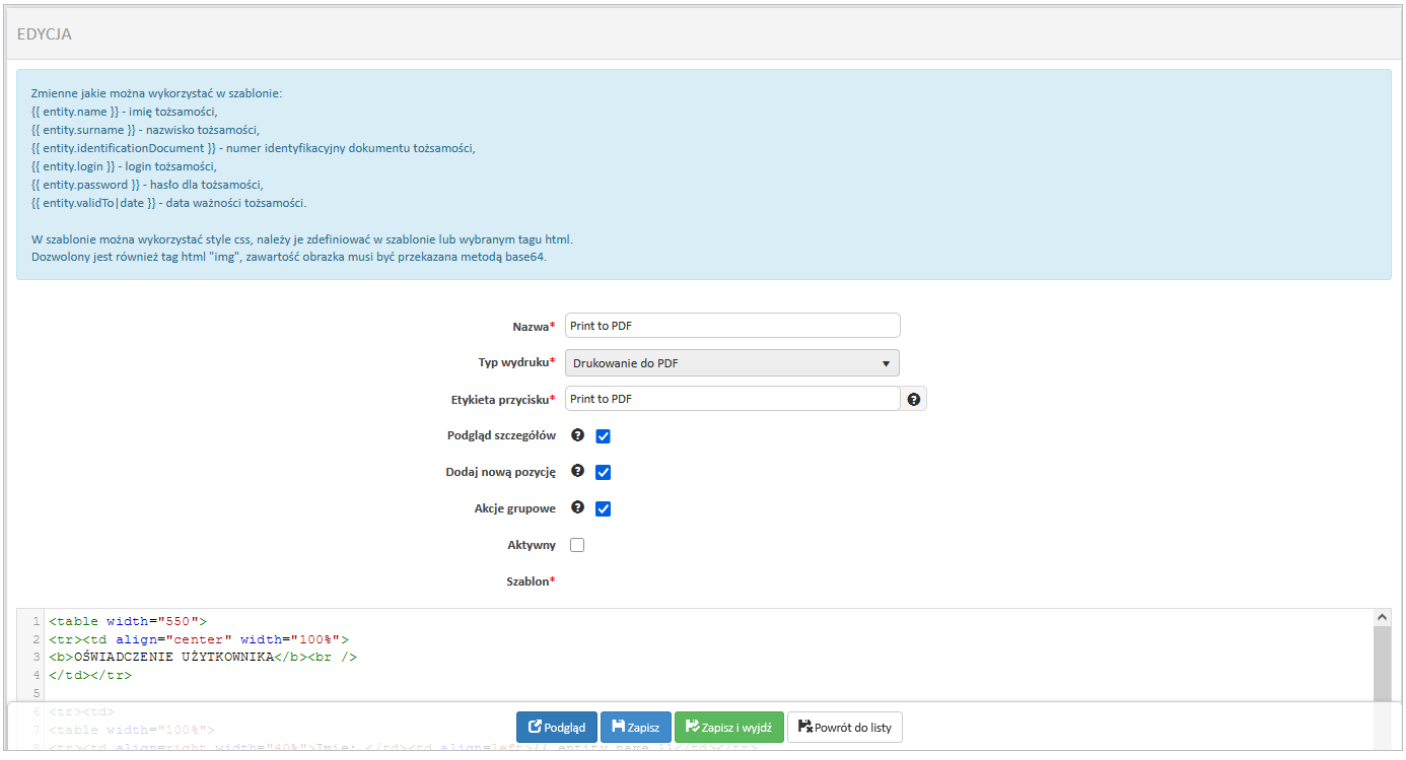
9.5. Szablony e-mail

Z menu głównego wybierz ***Szablony e-mail*** (sekcja ***Administracja***) potem przejdź do ***Zarządzanie szablonami globalnymi.*** Aby zmodyfikować wartość, kliknij w przycisk edycji () dla języka ***PL*** - znajduje się tam domyślnie ustawiony szablon wiadomości, napisany w HTML. Możesz go dowolnie modyfikować, pamiętając o zachowaniu kodu: {% block content %}{% endblock %}, który zawiera treść wiadomości. Zmodyfikuj zawartość szablonu i kliknij ***Podgląd*** w celu sprawdzenia wprowadzonych zmian.

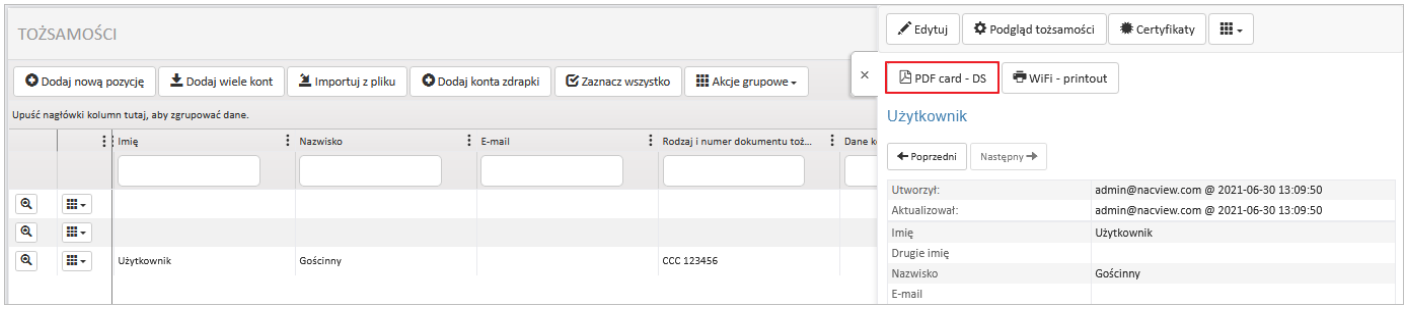
Zakończ edycję, zapisując szablon.

9.6. Szablony wydruków

Z menu głównego wybierz ***Szablony wydruków*** (sekcja ***Administracja***). Następnie wybierz istniejący szablon i kliknij ***Edytuj***. W szablonie zmień dowolną wartość i kliknij ***Podgląd*** w celu sprawdzenia wprowadzonych zmian.



Następnie z menu głównego wybierz ***Tożsamości***. Kliknij przycisk  i wybierz opcję ***Drukuj kartę***.



Wróć do szablonu wydruku, zmień typ wydruku na ***Drukowanie do HTML*** i sprawdź rezultat jak powyżej.

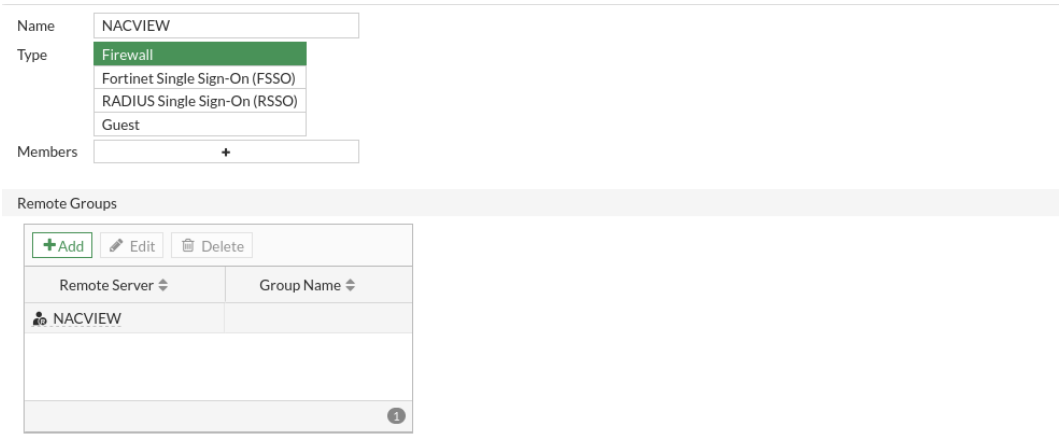
10. OTP Fortigate

10.1. Konfiguracja FortiGate i NACVIEW

Po zalogowaniu się do konsoli CLI Fortigate 10.XX.166.21 (admin/NACVIEW_SZKOLENIE22), wykonaj następujące komendy:

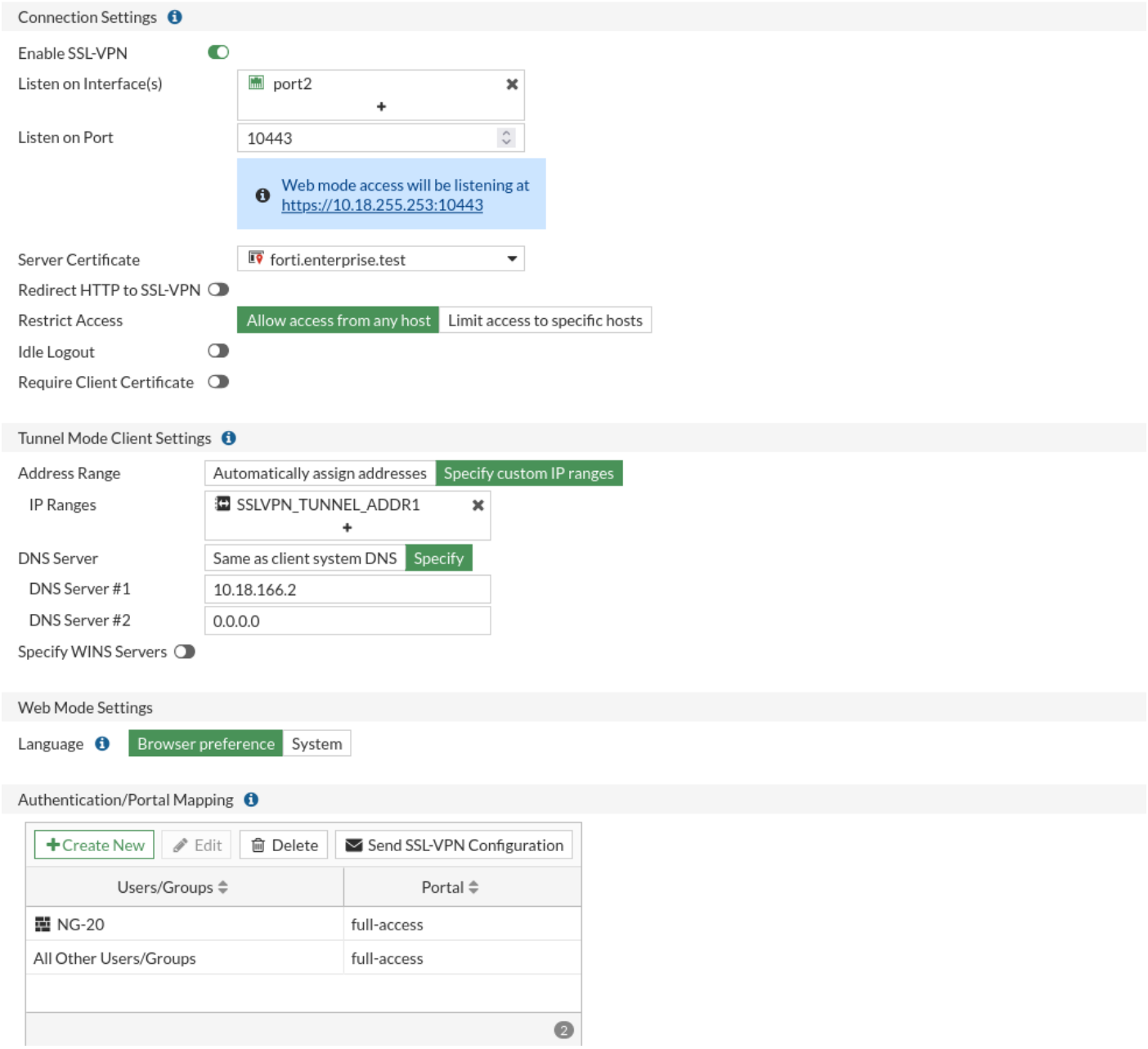
```
config system global
     set remoteauthtimeout 30
 end
 config user radius
 edit NACVIEW
        set server "10.XX.166.3"
        set secret NACVIEW_SZKOLENIE22
        set radius-port 1817
        set auth-type pap
    next
 end
```

Po zalogowaniu się do panelu GUI Fortigate https://10.XX.166.21 (admin/NACVIEW_SZKOLENIE22), przejdź do menu ***User & Authentication***, następnie do zakładki ***User Groups***. Utwórz nową grupę przyciskiem ***+Create New***. Następnie ustaw parametry jak na poniższym zdjęciu:

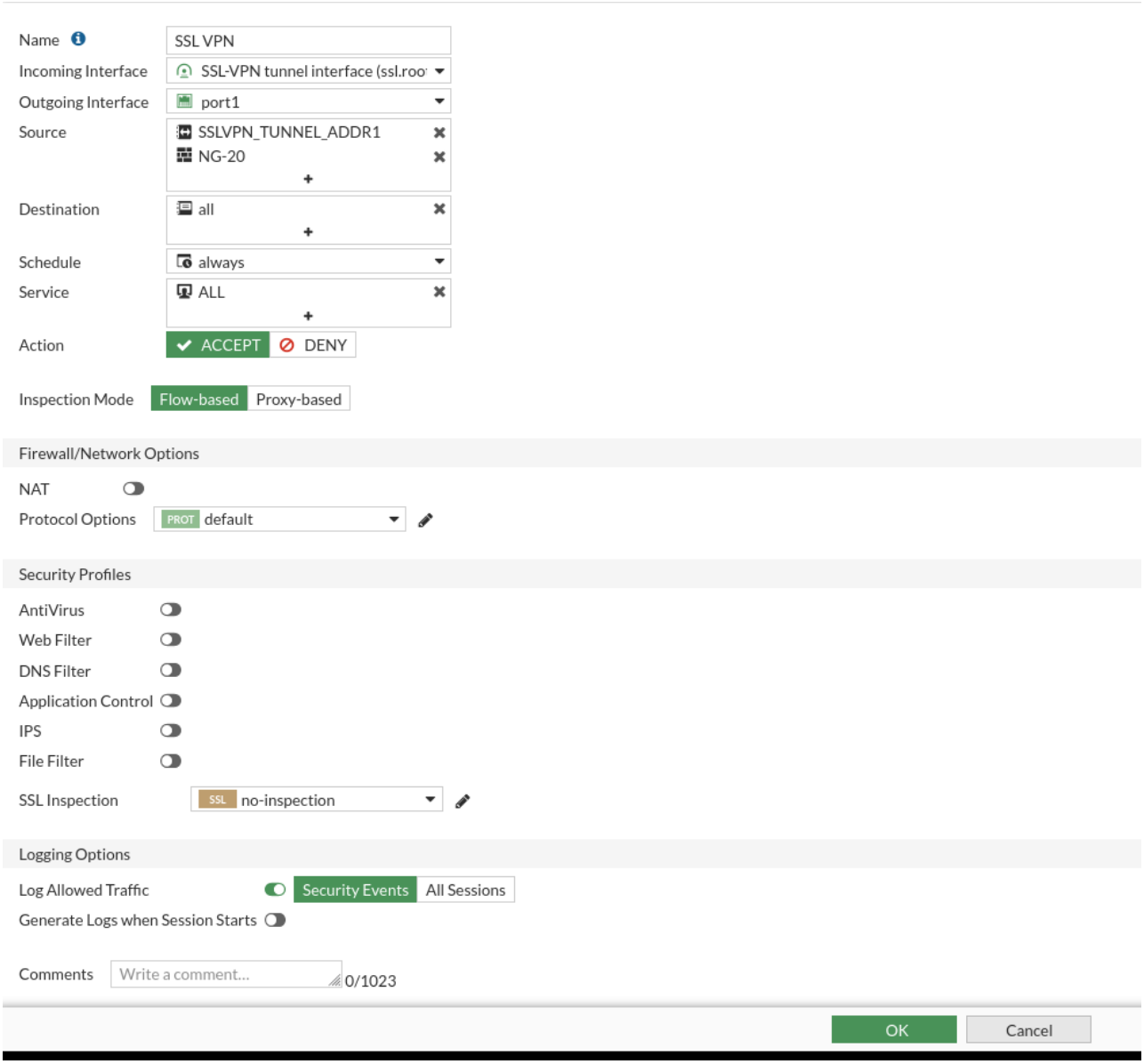


Przejdź do menu ***VPN***, otwórz zakładkę ***SSL-VPN Settings*** i skonfiguruj ustawienia połączenia VPN jak na poniższym zdjęciu.

Wygeneruj nowy certyfikat dla połączeń, nazwij go np. **forti.enterprise.test**



W kolejnym kroku przejdź do menu ***Policy & Objects***, do zakładki ***Firewall Policy***. Dodaj nową zasadę zapory sieciowej przyciskiem ***+Create New***. Skonfiguruj ustawienia tak, jak na poniższym zdjęciu:



Zatwierdź przyciskiem ***OK***.

Teraz wróć do systemu ***NACVIEW***. Otwórz menu i wybierz ***Urządzenia sieciowe*** *(*sekcja ***Sieć****)*. Kliknij ***Dodaj nową pozycję***. Uzupełnij pola: ***Adres IP, Klucz komunikacji Radius*** (po kliknięciu w przycisk ***Zmień/ustaw hasło***), ***Opcje OTP*** (rozwijana lista na końcu formularza), wprowadzając dane dla systemu FortiGate.

Ilość portów: **3**

Adres IP: **10.XX.166.21**

Nazwa: **XX-FTG**

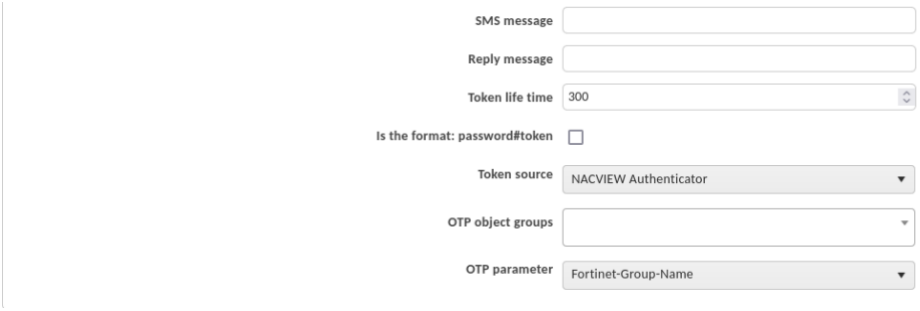
Klucz komunikacji RADIUS: **NACVIEW_SZKOLENIE22**

+ Opcje OTP:

Generowanie tokenu: **NACVIEW Authenticator**

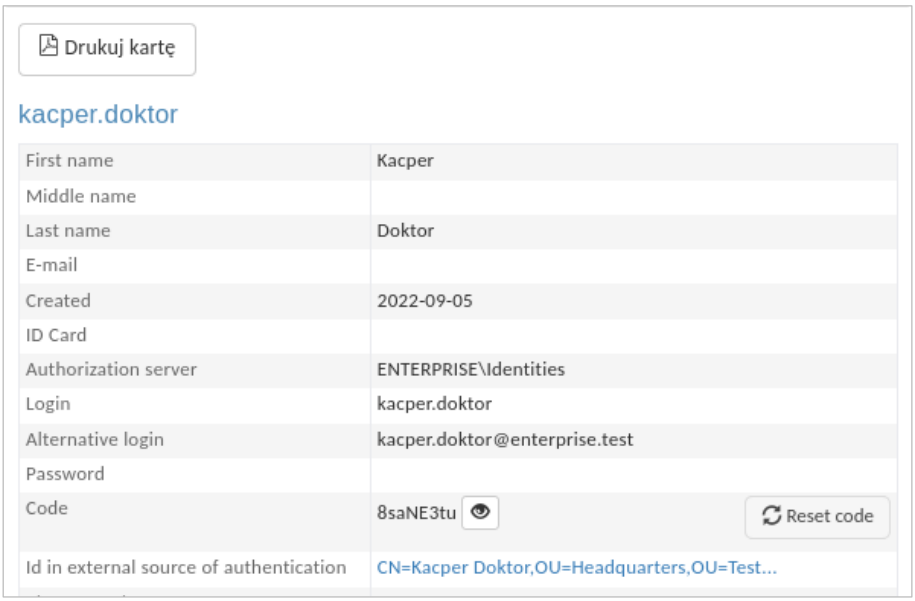
Parametr OTP: **Fortinet-Group-Name**

Zapisz ustawione wartości.



10.2. Konfiguracja aplikacji Nacview Authenticator

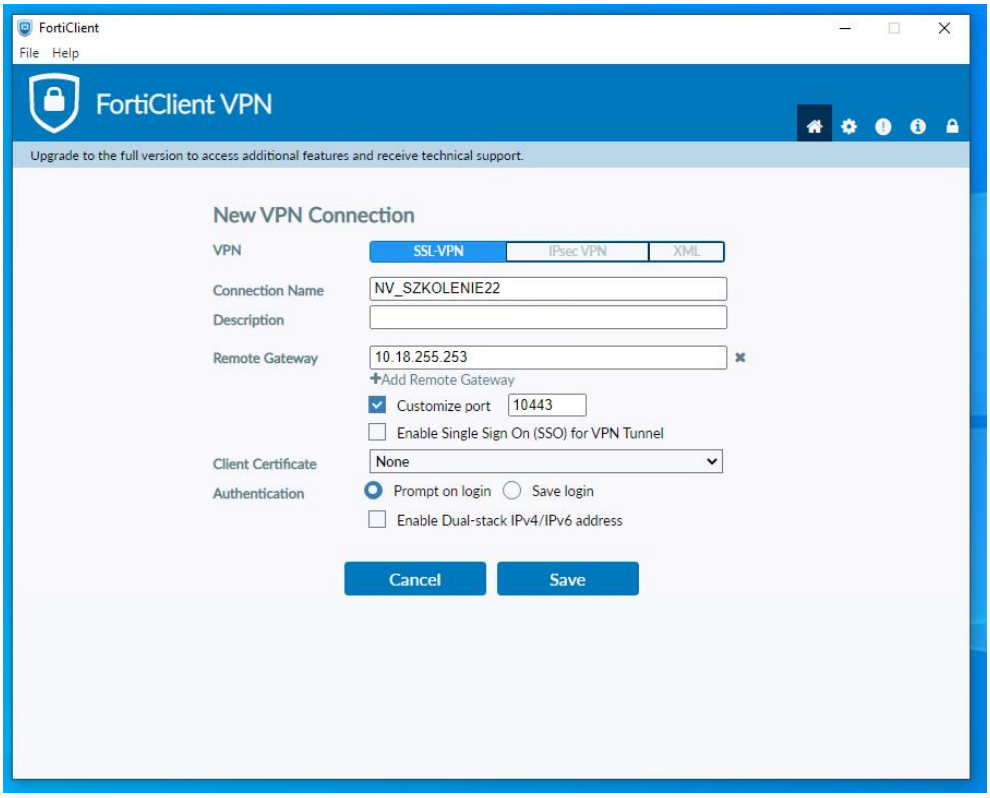
W aplikacji Nacview Autheticator należy podać login oraz kod, który można sprawdzić w ***Obiekty → Tożsamości → Szczegóły tożsamości (tu chodzi o dwu klik na konkretną tożsamość) → Kod.*** Kod ten można znaleźć również w podmenu ***Autoryzacja dwuetapowa.*** Należy także podać kod PIN zabezpieczający dostęp do aplikacji. Po skonfigurowaniu konta można za pomocą przycisku ***Generate*** wygenerować jednorazowy kod dostępu.



10.3. Konfiguracja klienta VPN

Po zalogowaniu się na maszynę **XX-NT3** (login: TesterVPN, hasło: NACVIEW_SZKOLENIE22) włącz FortiClient VPN i wybierz ***Configure VPN***.

Podaj dane połączeniowe i kliknij ***Save***.



Następnie wprowadź dane użytkownika uprzednio skonfigurowane w NACVIEW Authenticator i kliknij *Connect.*