MikroTik Warsaw
Training Center

MikroTik CAPsMAN
WPA2 Enterprise z Microsoft AD

MBUM#4
22 listopad 2019r

Piotr Wasyk

mwtc

- ✓ **Największe centrum MikroTik szkoleniowe w Polsce**
  - ✓ Warszawa/ Kraków / inne …
  - ✓ Pełna ścieżka certyfikacji MikroTik
  - ✓ Szkolenia dofinansowane (nawet do 100%)

MikroTik TRAINING CENTER

- ✓ **Projektowanie i wdrażanie sieci bezprzewodowych (indoor)**
- ✓ **Wdrożenia systemów monitorowania infrastruktury IT** *(partner Zabbix)*

ZABBIX

- ✓ **Konsulting IT**

Agenda

- ✓ Co to jest CAPsMAN?
- ✓ Dlaczego CAPsMAN?

- ✓ Radius – centralna baza użytkowników
- ✓ Microsoft NPS

- ✓ CAPsMAN WPA2EAP
- ✓ Jedno SSID wiele sieci (VLAN)

Co to jest CAPsMAN?

- ✓ **MikroTik CAPsMAN** to jedna z funkcjonalności systemu pracującego na urządzeniach MikroTik – RouterOS

- ✓ Odpowiedzialny za dostarczanie konfiguracji do punktów dostępowych (provisioning)
  - ✓ ustawienia modułów radiowych
  - ✓ aktualizacji oprogramowania

- ✓ MikroTik umożliwia wykonanie badania propagacji fal (narzędzie spectral-history)

Dlaczego CAPsMAN?

- ✓ Szerokie możliwości konfiguracji, stabilność działania
- ✓ Szeroki wybór urządzeń AP (zarówno indoor jak i outdoor)
- ✓ Estetyka i jakość wykonania AP
- ✓ Wygodne zarządzenie za pomocą: aplikacji Winbox / WWW / CLI / mobile App
- ✓ Rozbudowana funkcja hotspot (strony powitalne)
- ✓ Opcja konfiguracji w wariancie HA
- ✓ Zastosowanie CAPsMAN w „chmurze”

- ✓ Niska cena urządzeń
- ✓ Brak opłat licencyjnych (w tym także brak opłat za możliwość aktualizacji)

Centralna baza użytkowników

- ✓ W rozbudowanych środowiskach, w szczególności, gdy występuje wiele lokalizacji (np. oddziałów firmy, hoteli czy restauracji w sieci) zalecane jest zastosowanie centralnej, współdzielonej bazy użytkowników.

- ✓ Do tego celu wykorzystuje się serwer Radius. MikroTik posiada własną implementację Radius dostępną jako paczka dodatkowa (extra package) do systemu RouterOS – **user manager** (interfejs WWW)
- ✓ Użycie user manager nie jest licencjonowane
- ✓ Może być zainstalowany na dowolnym urządzeniu MikroTik jak i na maszynie wirtualnej

- ✓ RouterOS może być klientem dowolnego serwera AAA, np. FreeRadius, Dalo, Microsoft NPS (Network Policy Server)

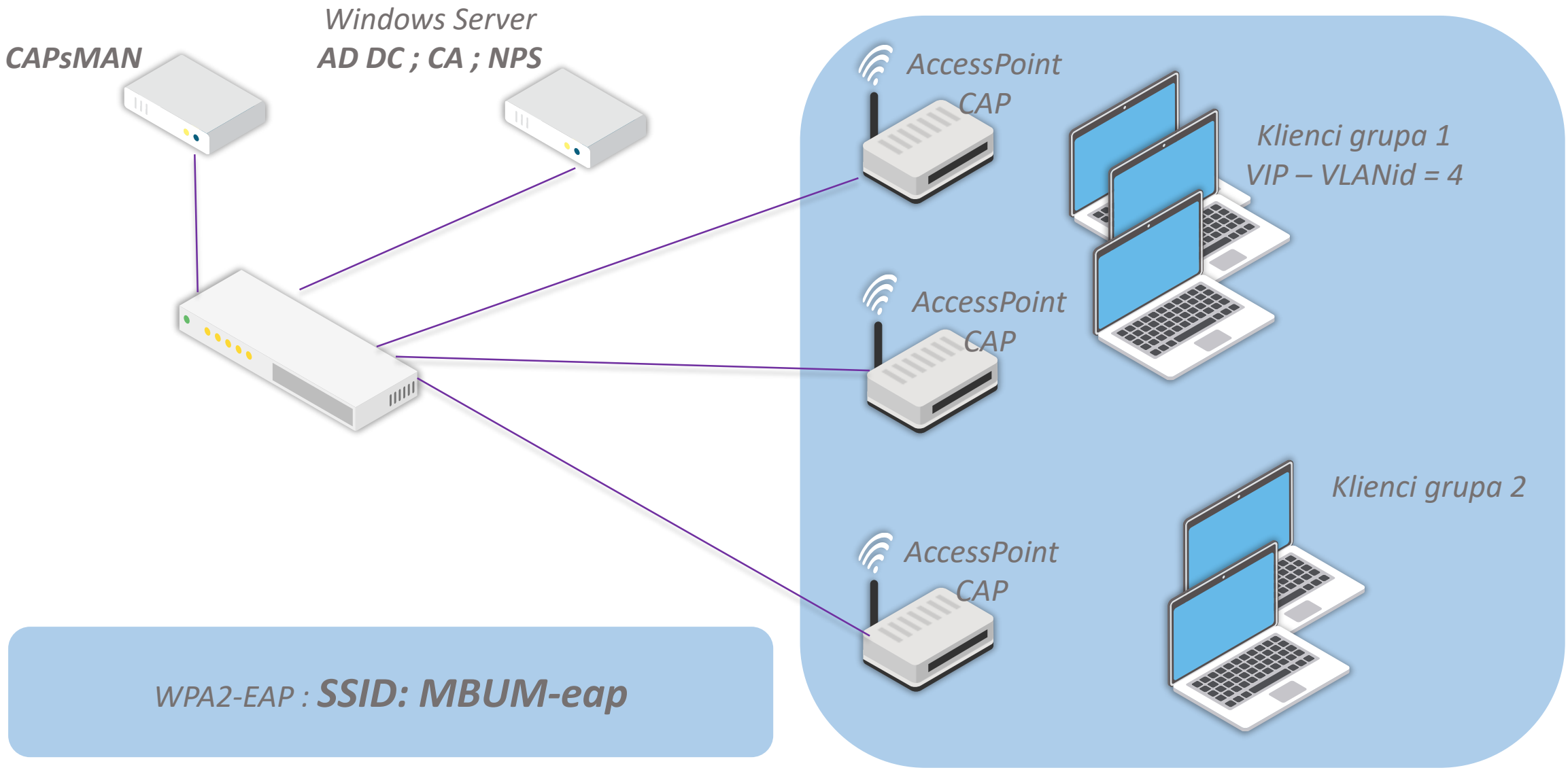
Scenariusz praktyczny

Wielooddziałowa firma, od 1 do > 150AP w każdym oddziale , kontroler CAPsMAN w chmurze (redundantny), MikroTik jako router brzegowy, NPS (Microsoft Network Policy Server)

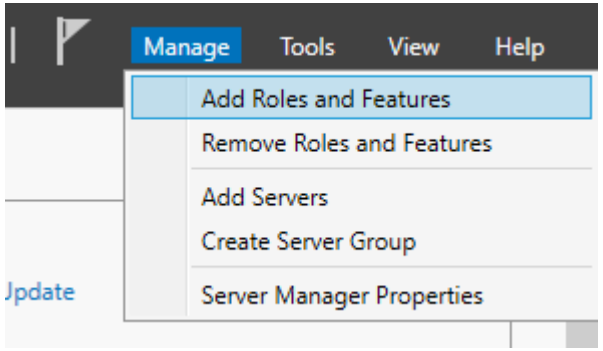
Wymagania:

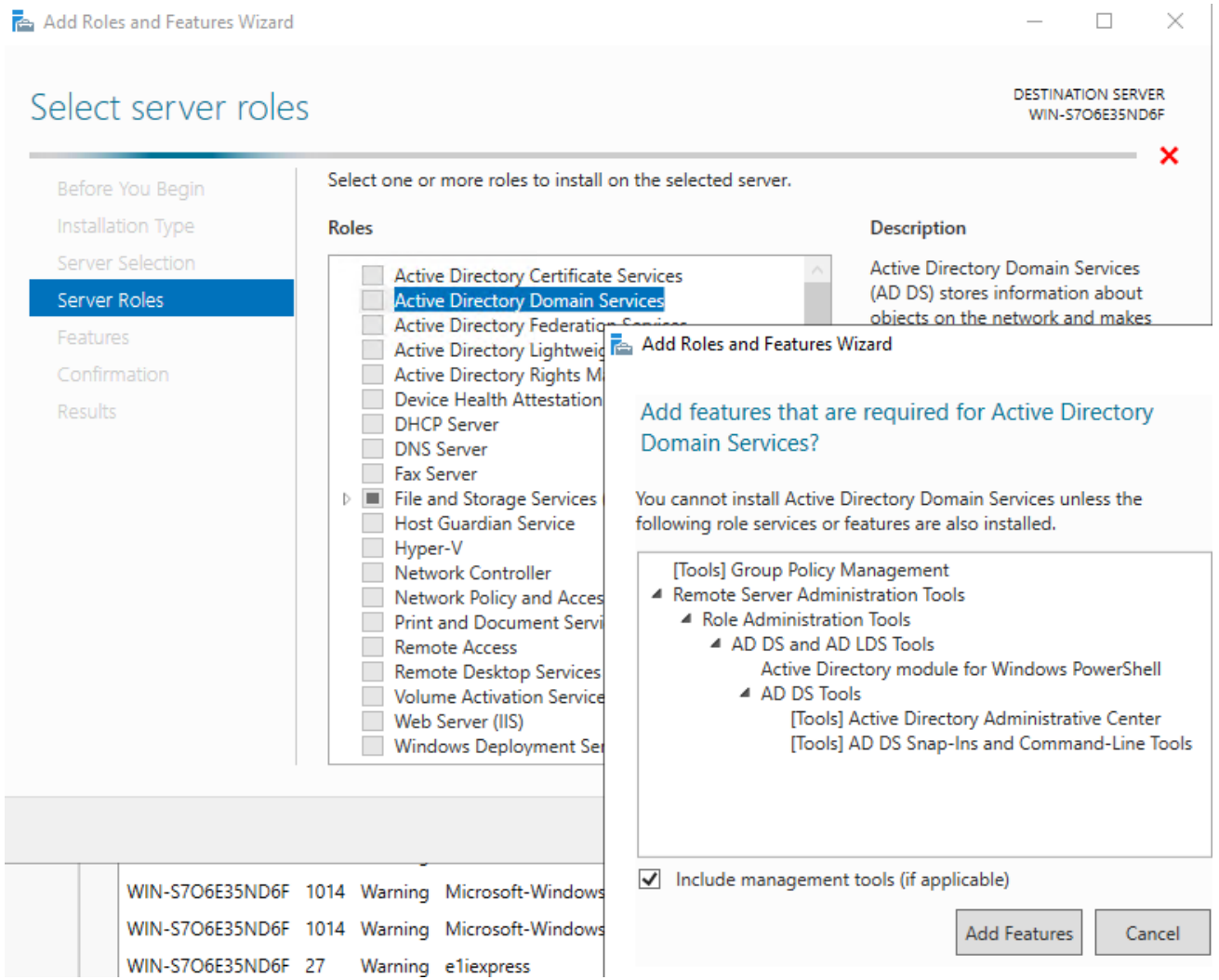
- Sieć WPA2-EAP dla pracowników – uwierzytelnienie do sieci za pomocą konta w usługach katalogowych (np. Microsoft Active Directory)
- W zależności od przynależności do odpowiedniej grupy AD użytkownik kierowany do odpowiedniego VLAN (grup > 20). Rozgłaszanie tylko jednego SSID

Scenariusz praktyczny

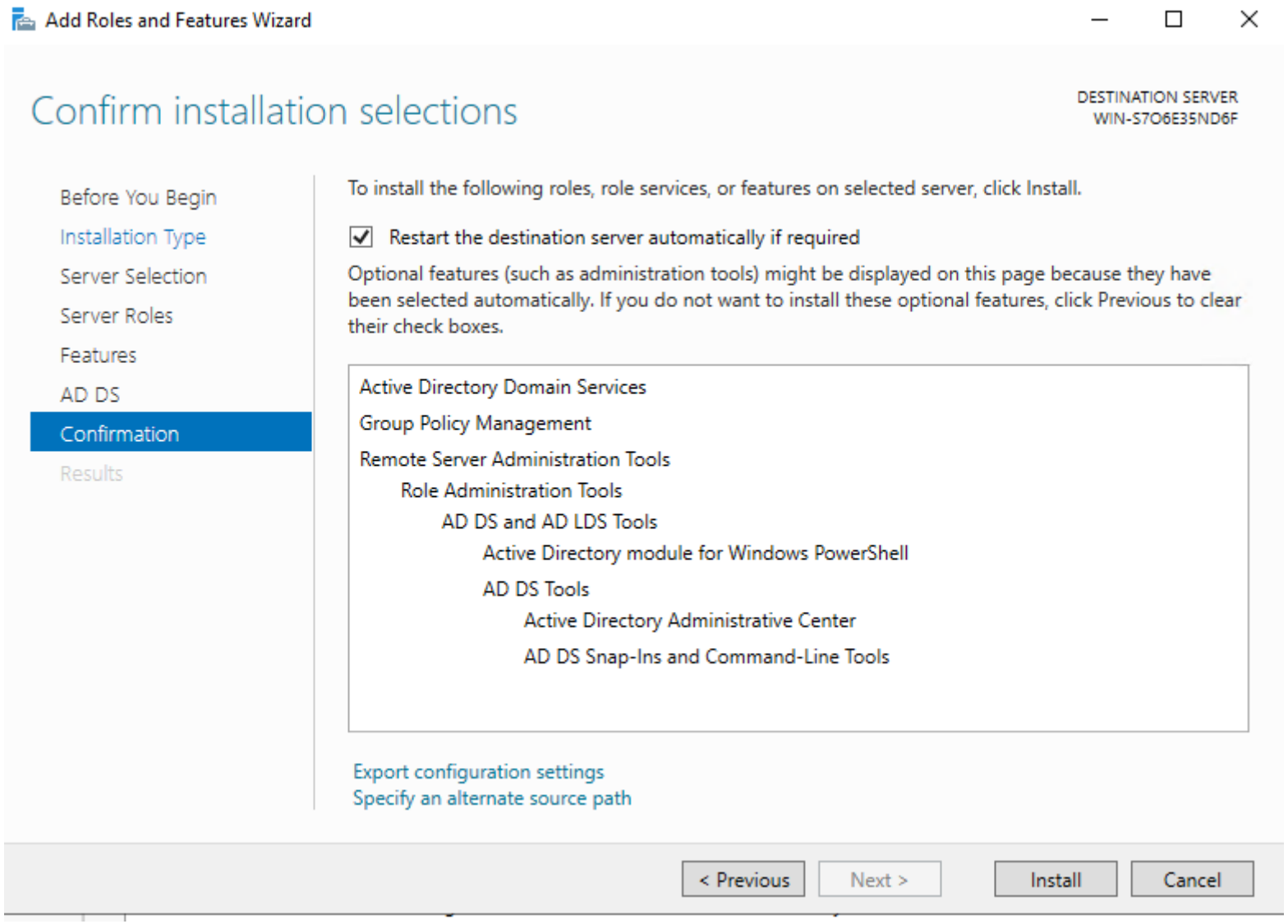


Instalacja Active Directory Services

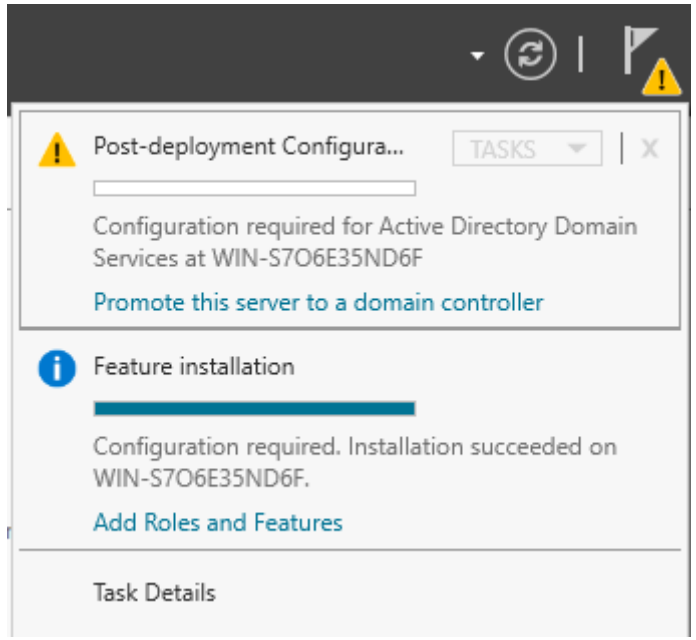


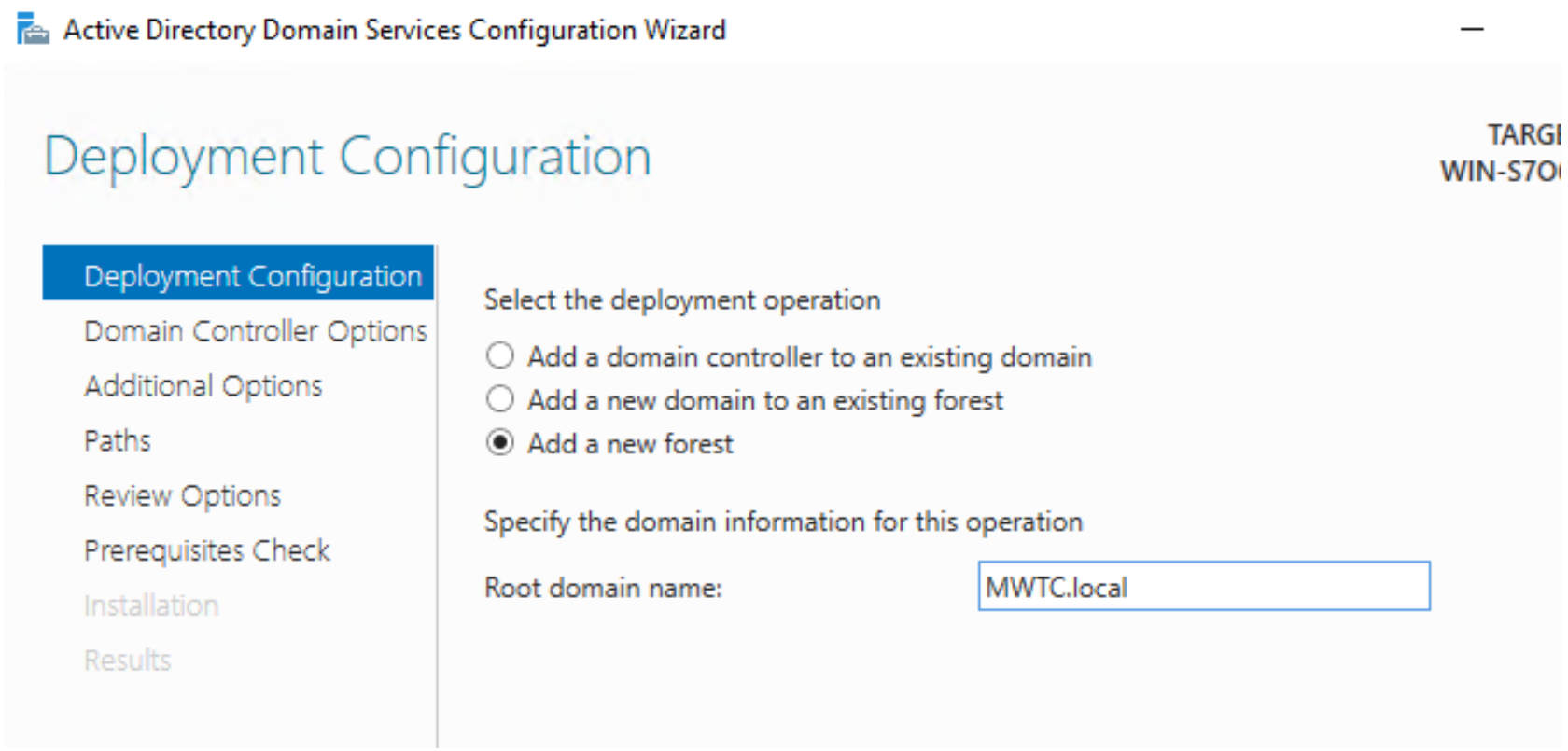


Instalacja Active Directory Services

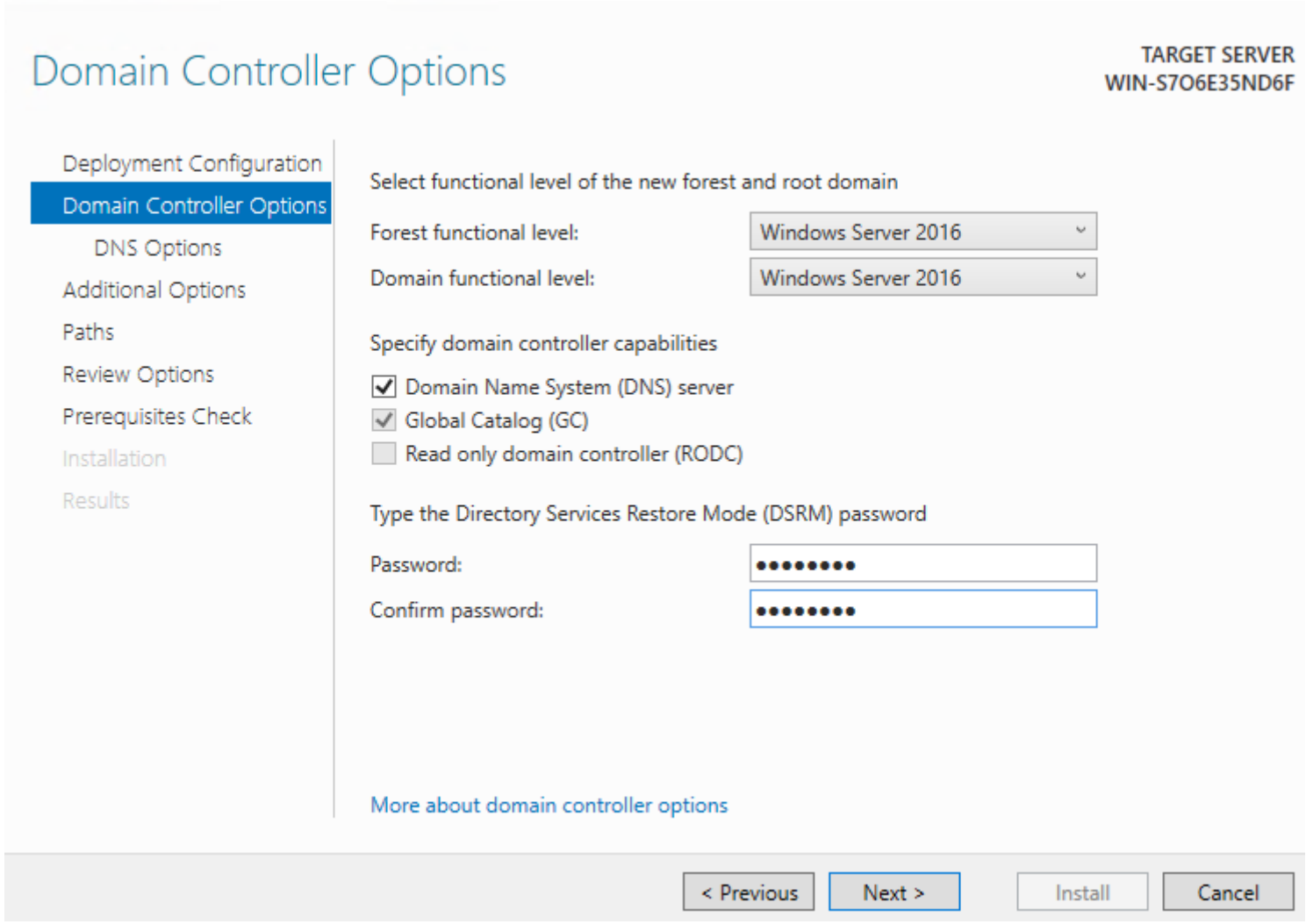


Promocja serwera do roli DC

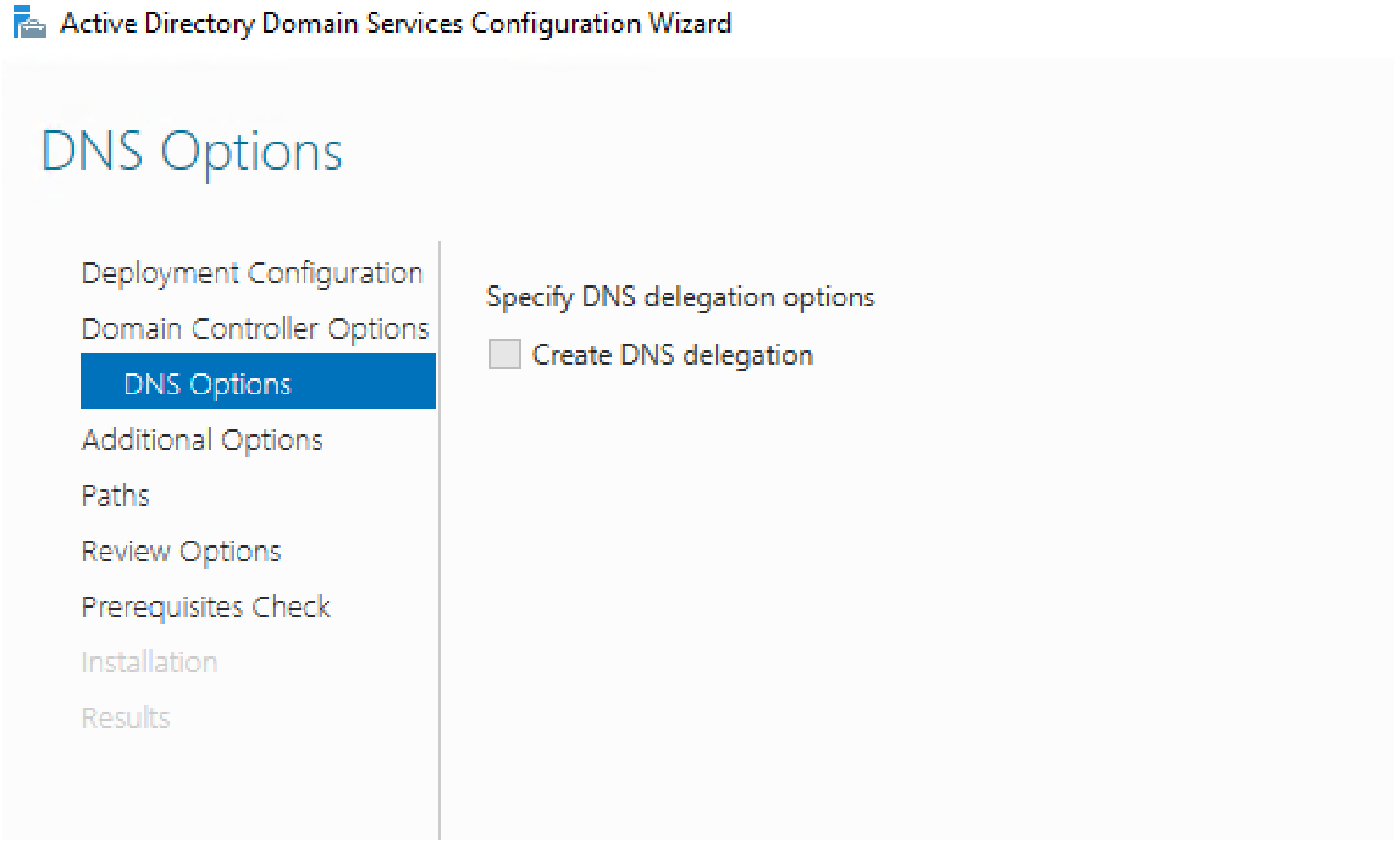




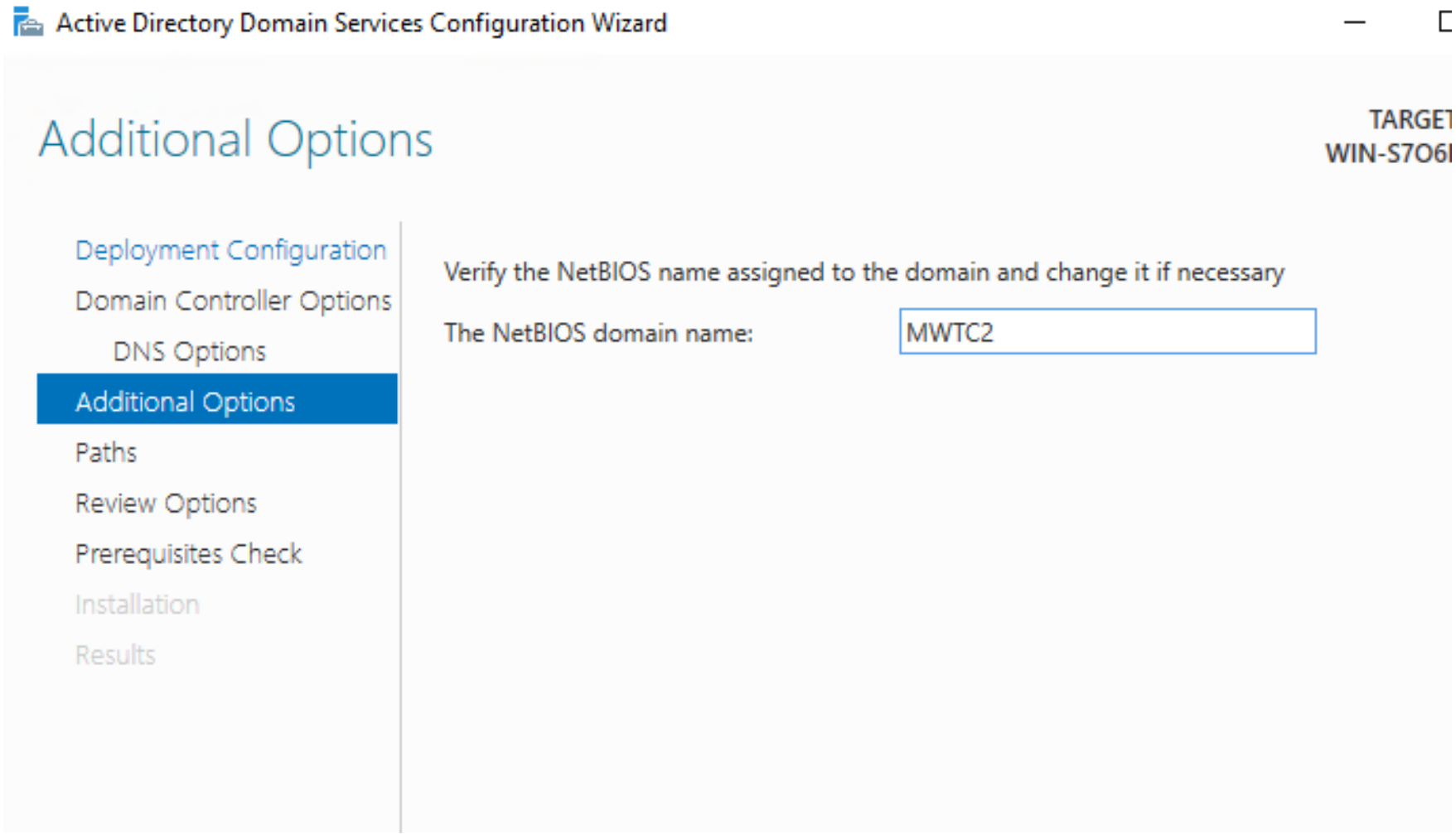
Promocja serwera do roli DC



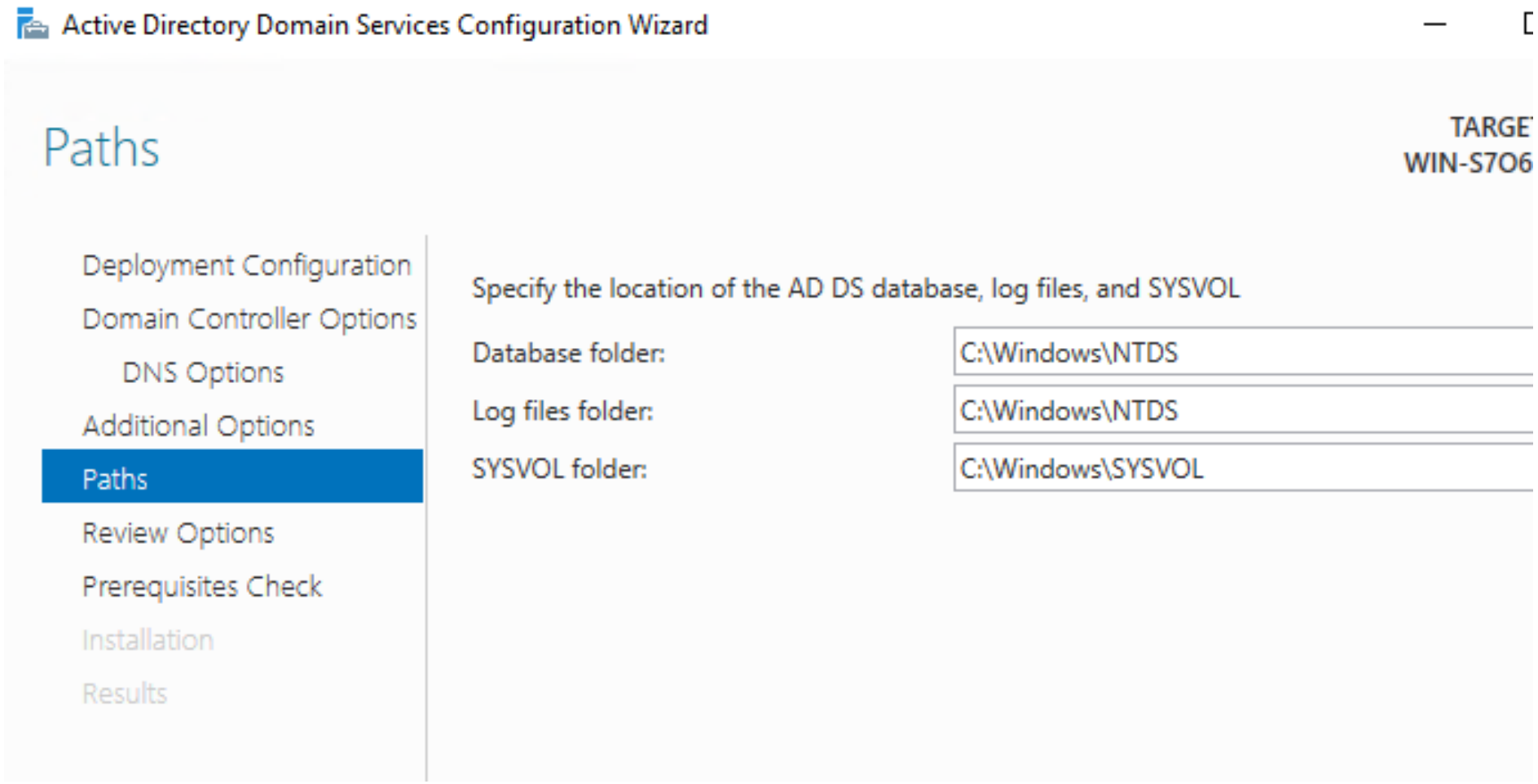
Promocja serwera do roli DC



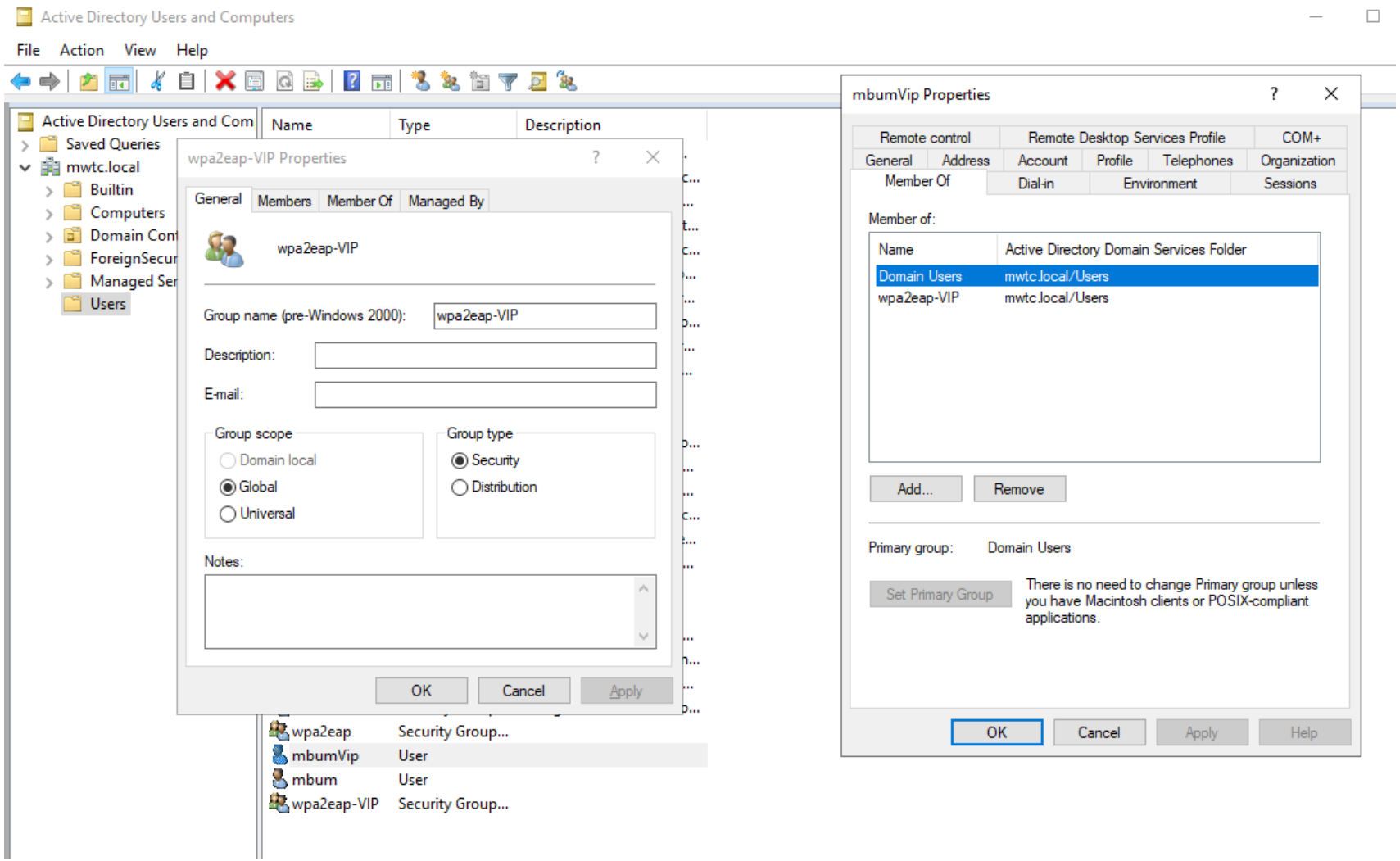
Promocja serwera do roli DC



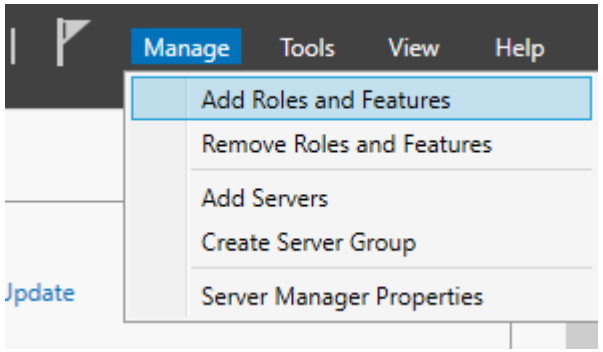
Promocja serwera do roli DC

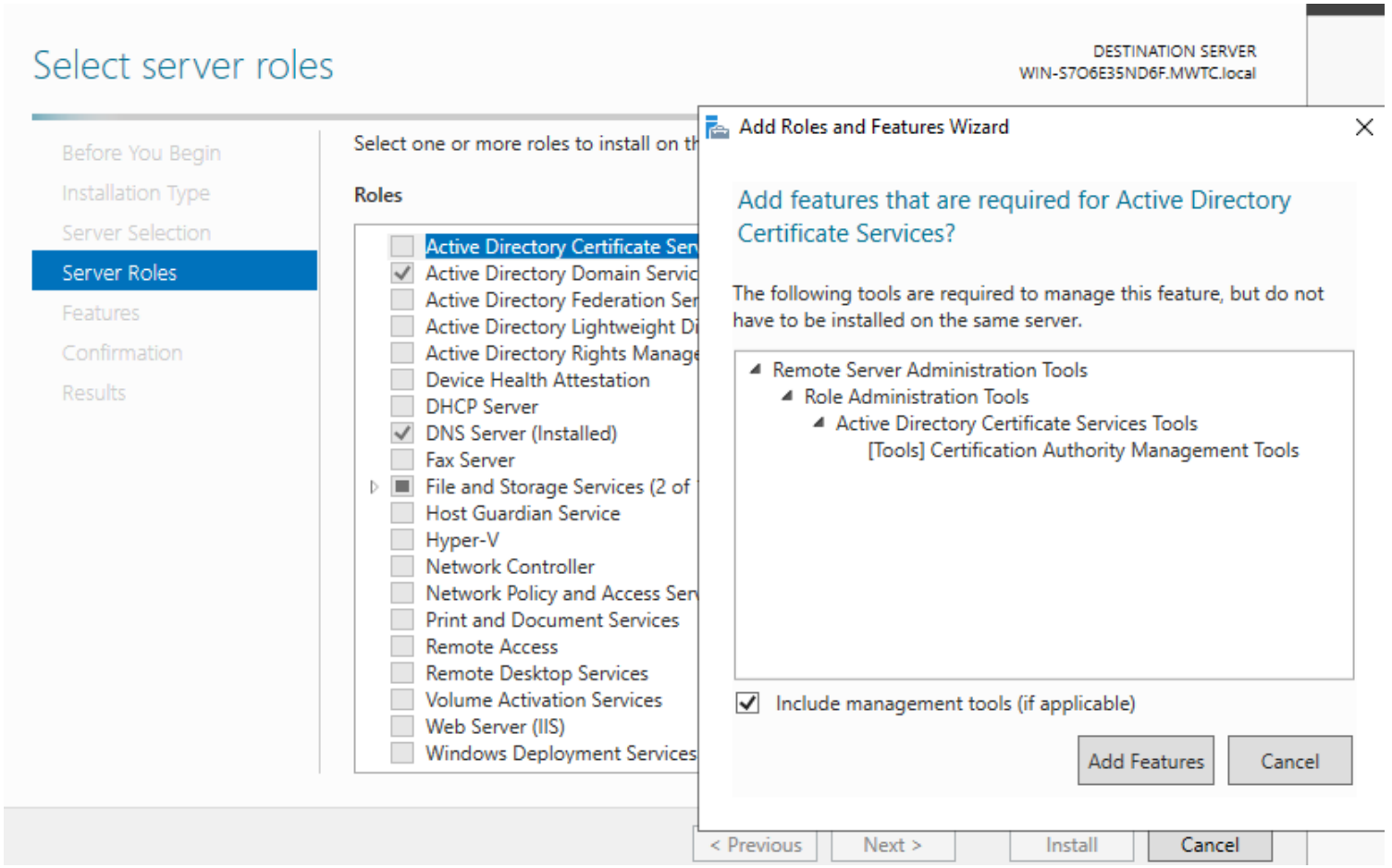


Dodanie grup i użytkowników

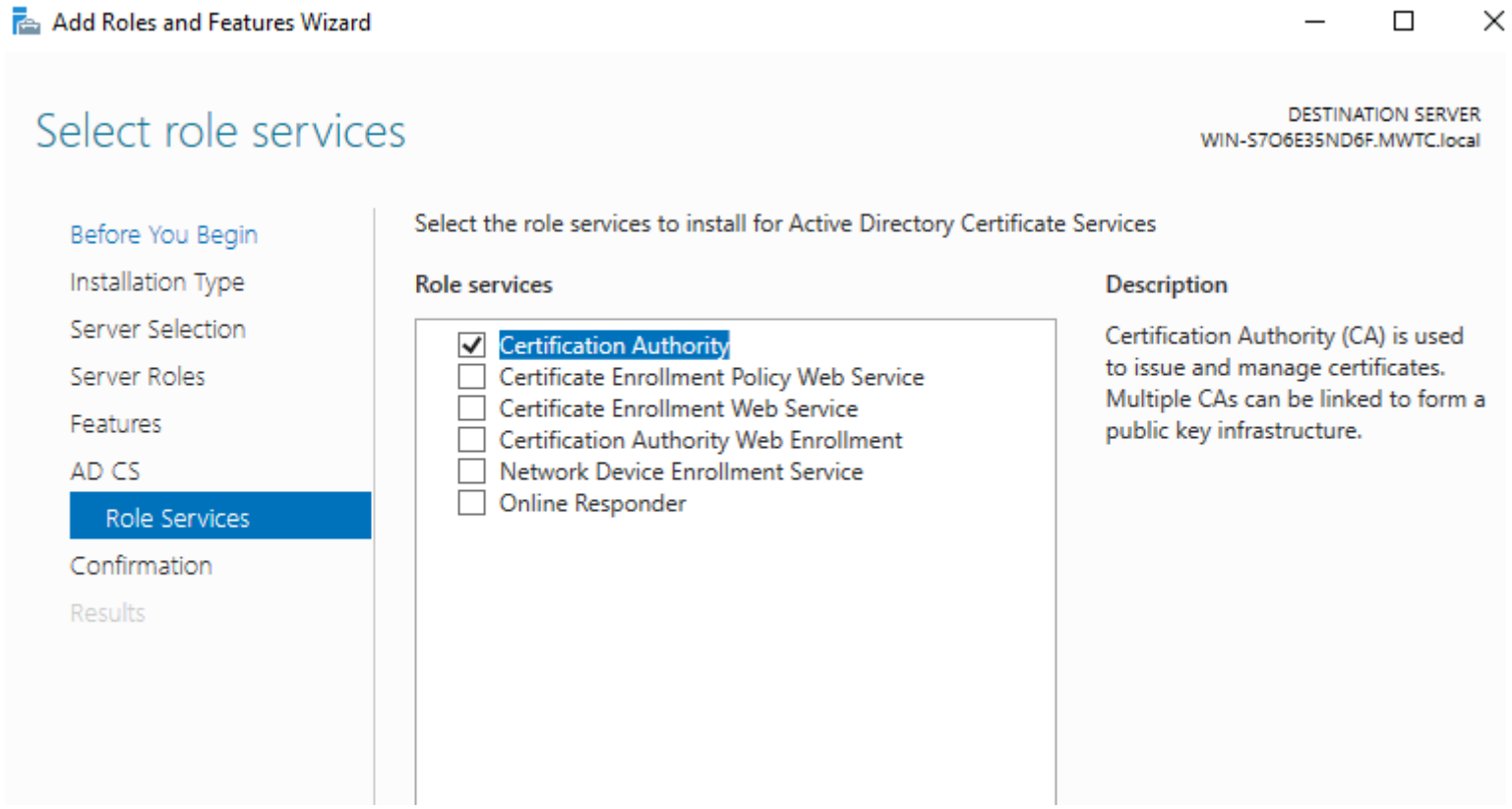


Instalacja Active Directory Certificates Services

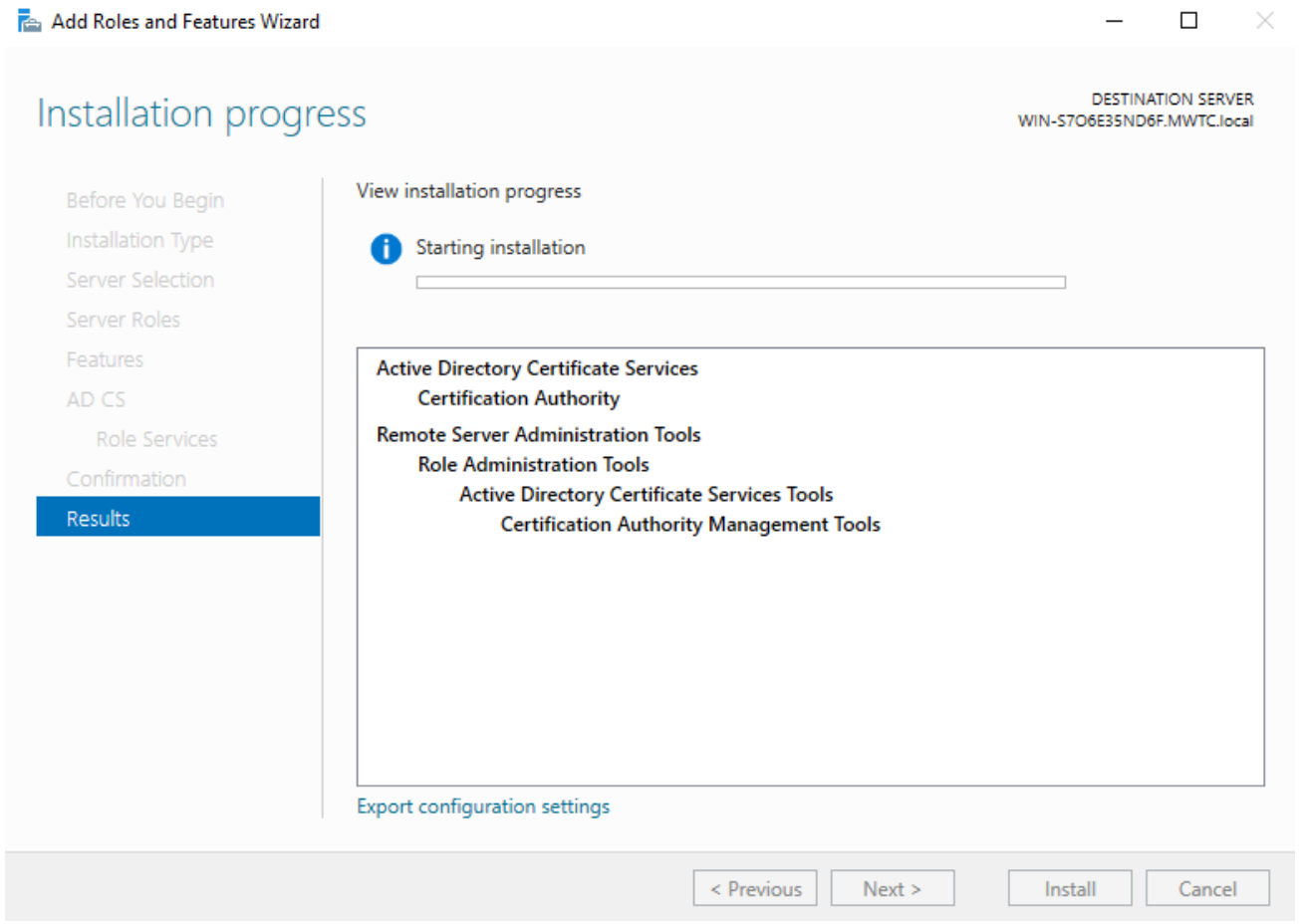




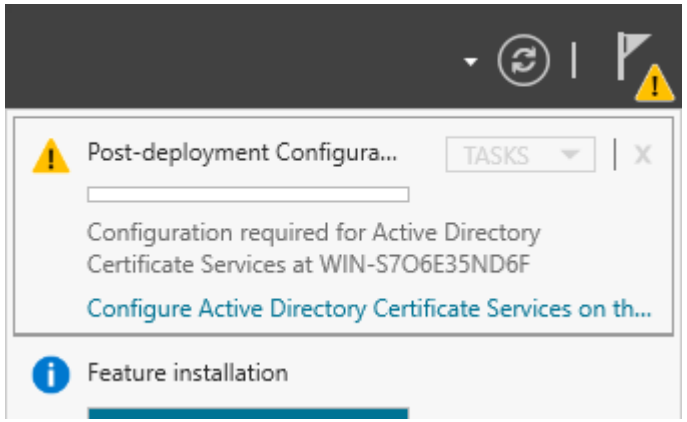
Instalacja Active Directory Certificates Services

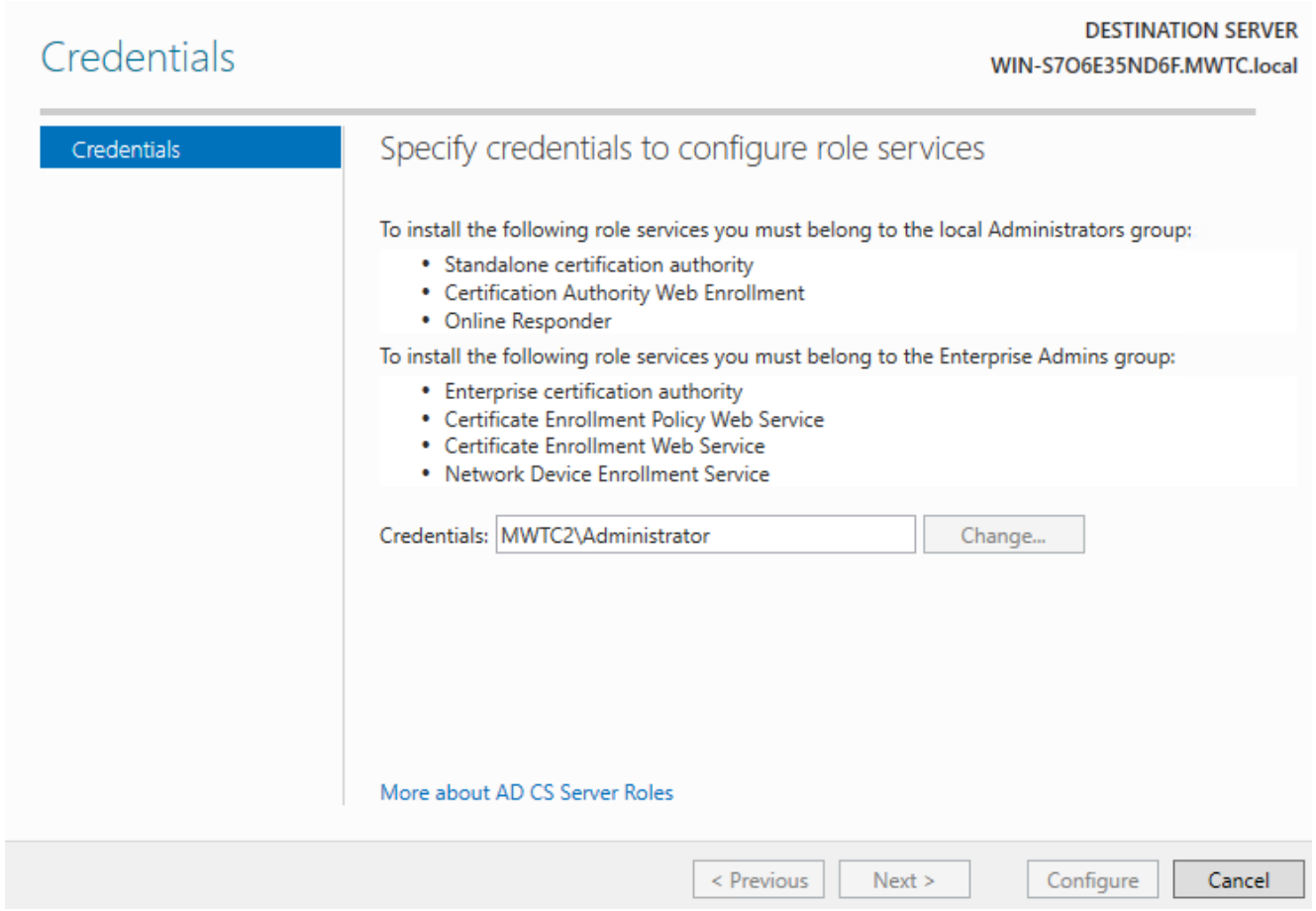


Instalacja Active Directory Certificates Services

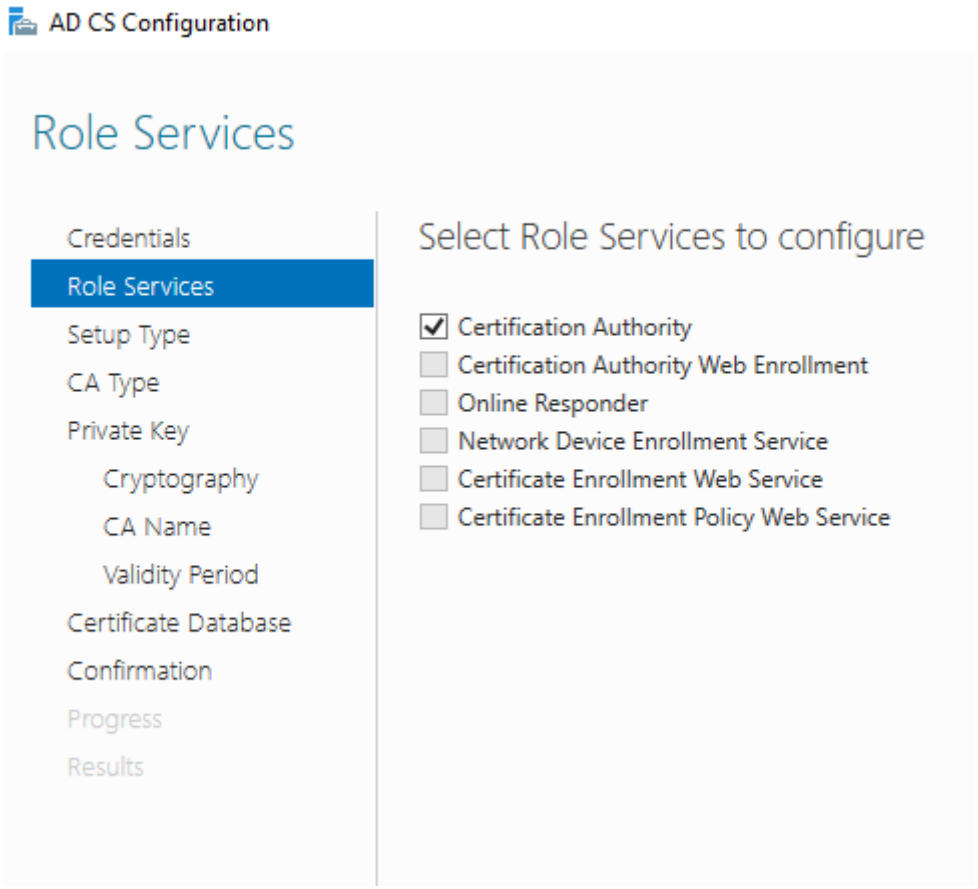


Konfiguracja Active Directory Certificates Services

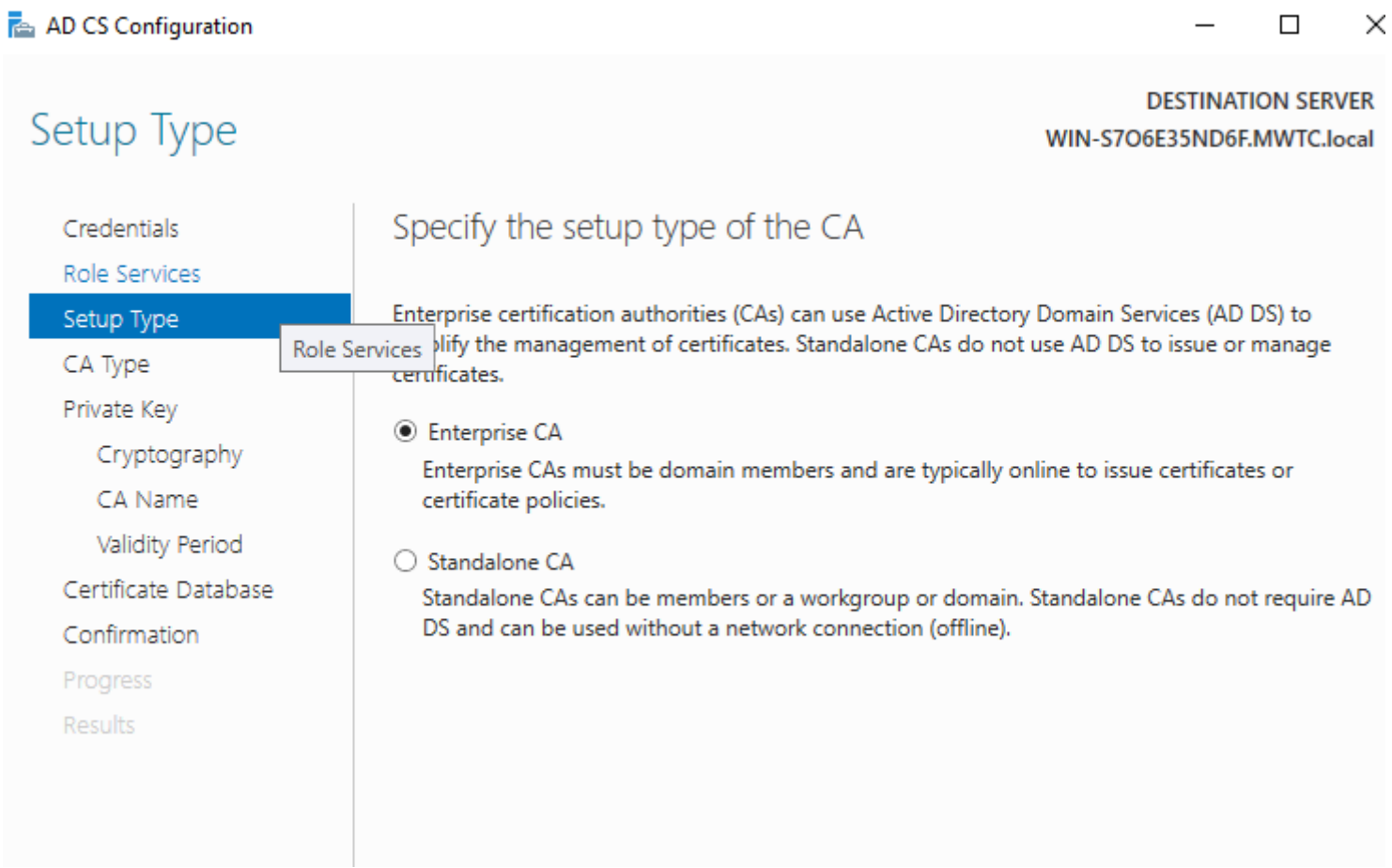




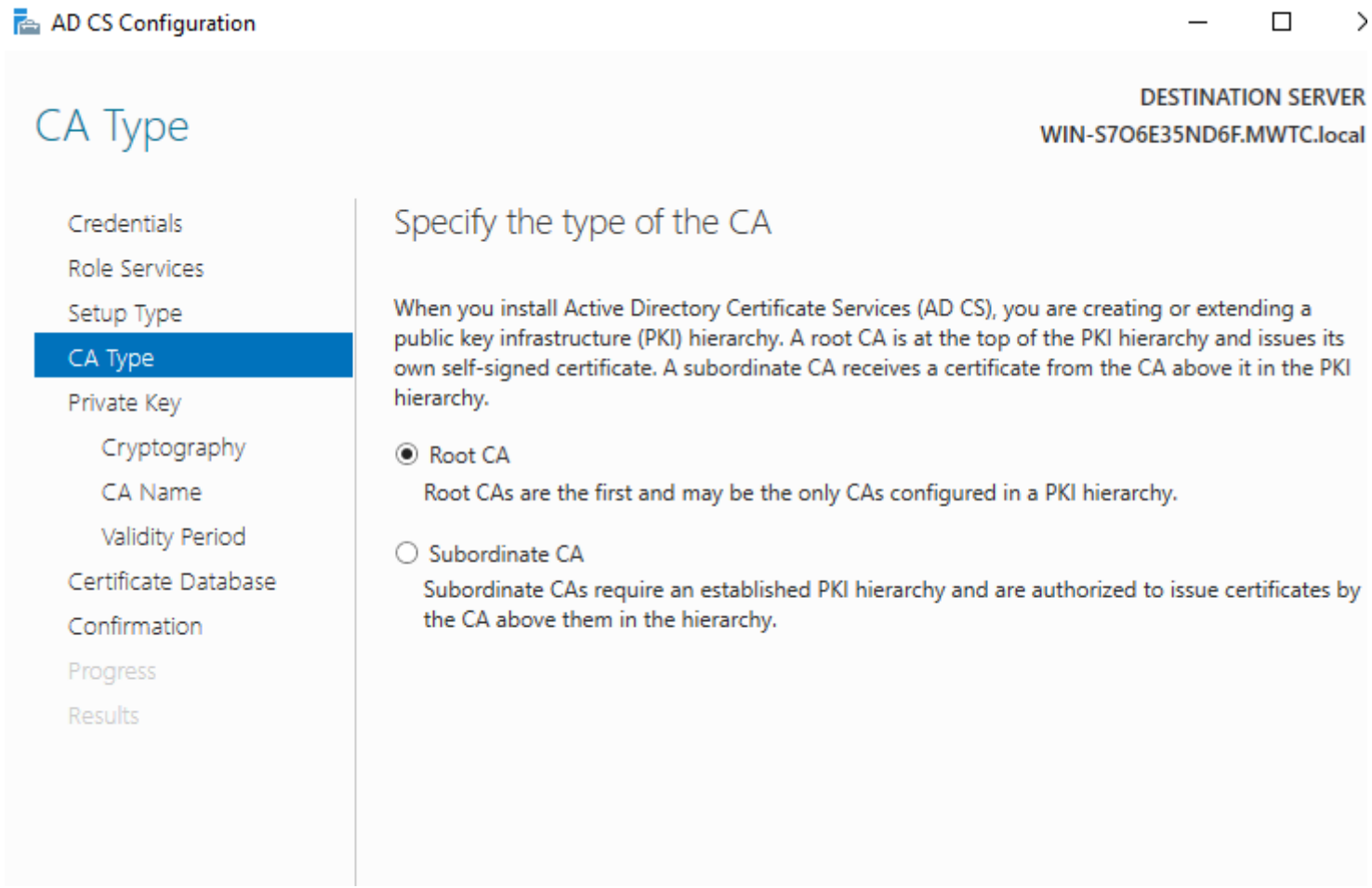
Konfiguracja Active Directory Certificates Services



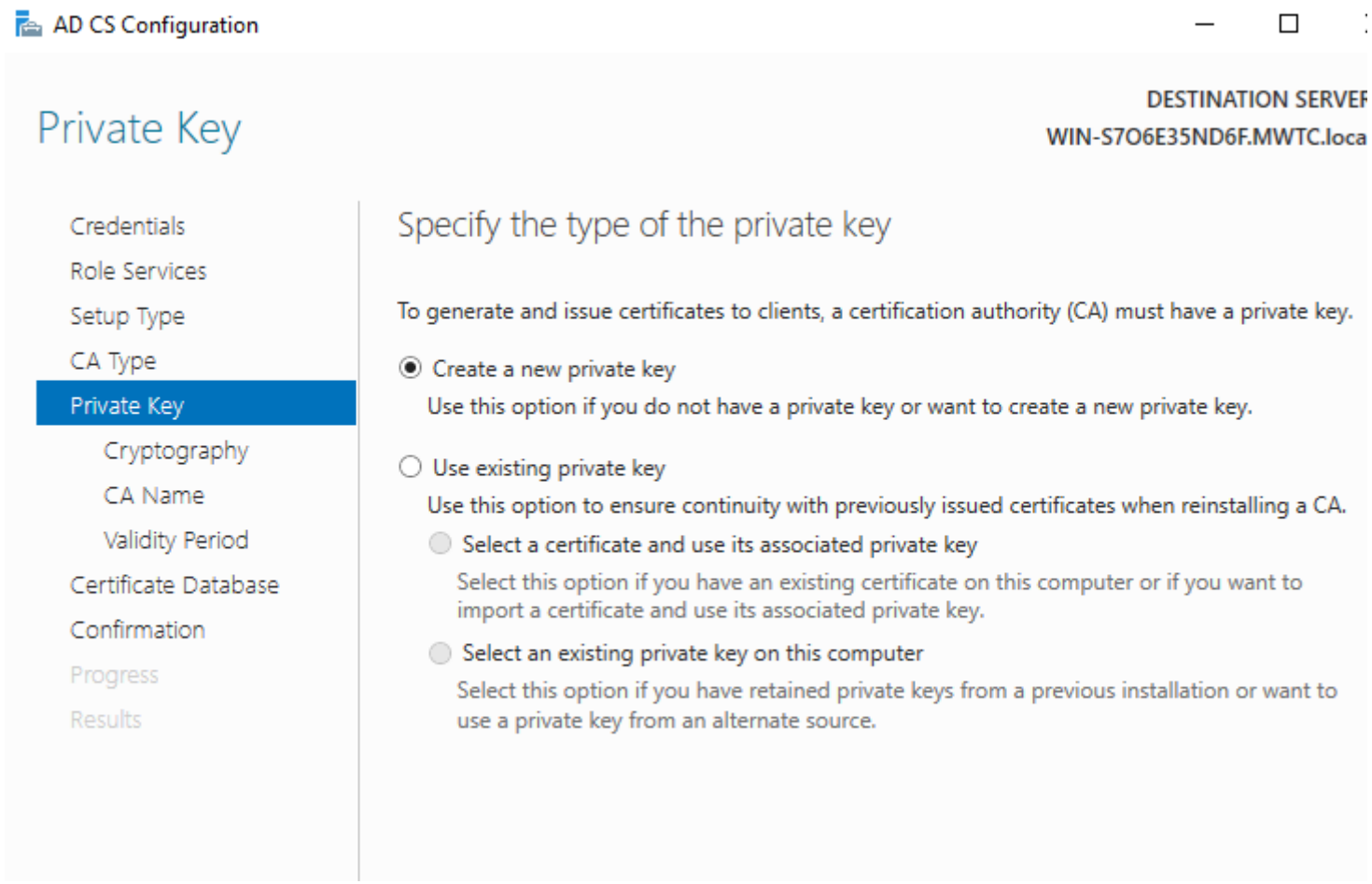
Konfiguracja Active Directory Certificates Services



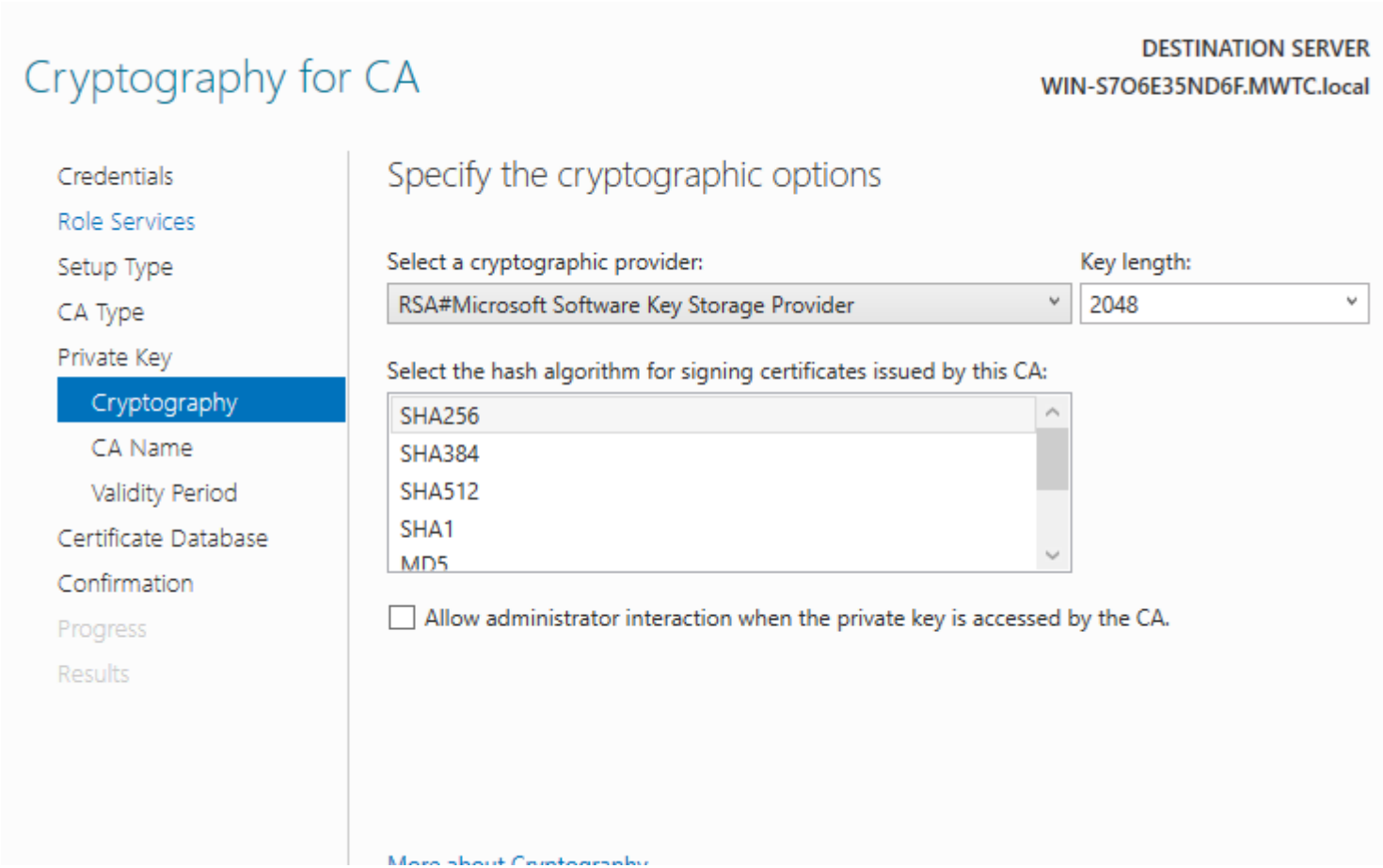
Konfiguracja Active Directory Certificates Services



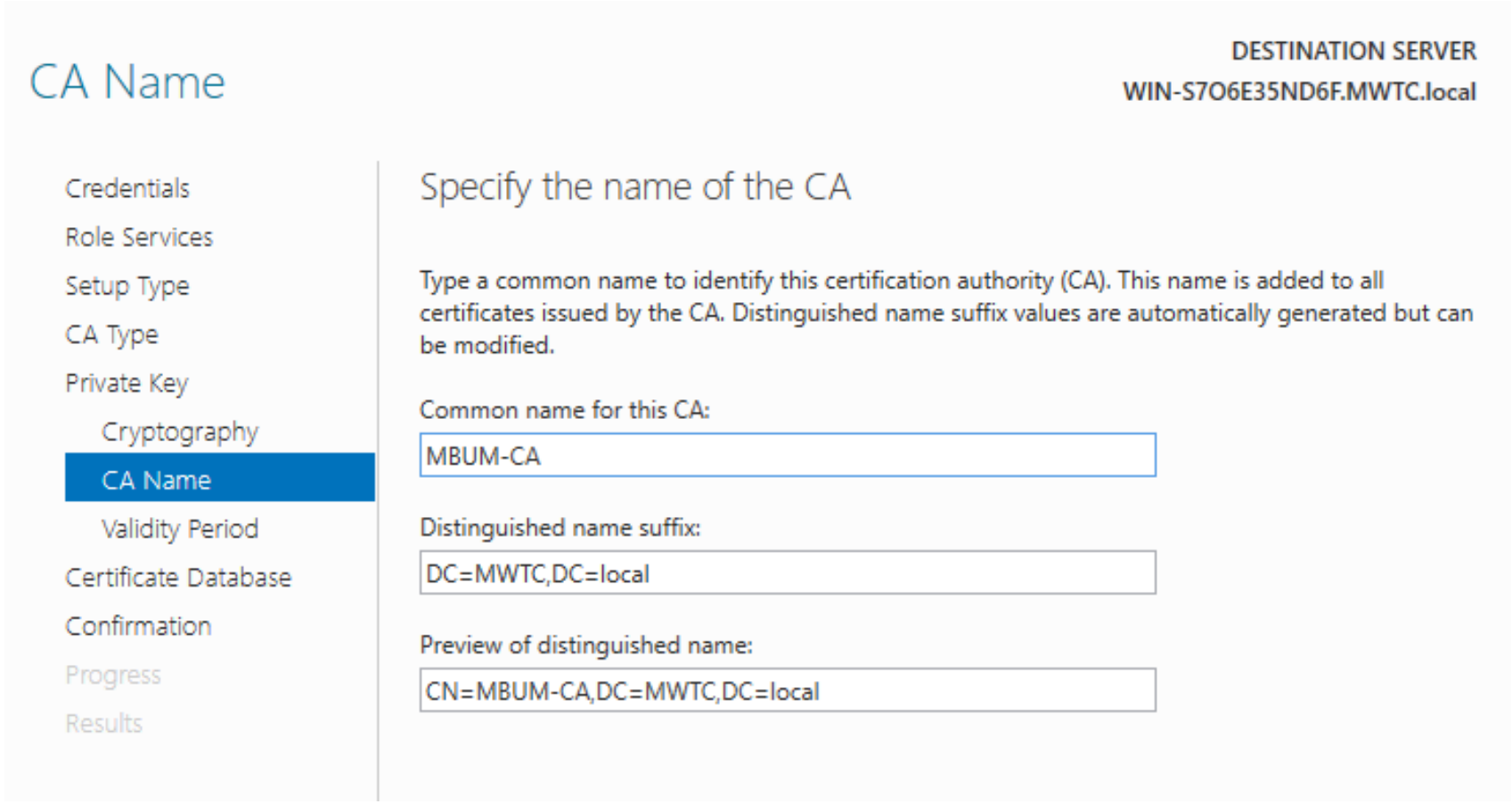
Konfiguracja Active Directory Certificates Services



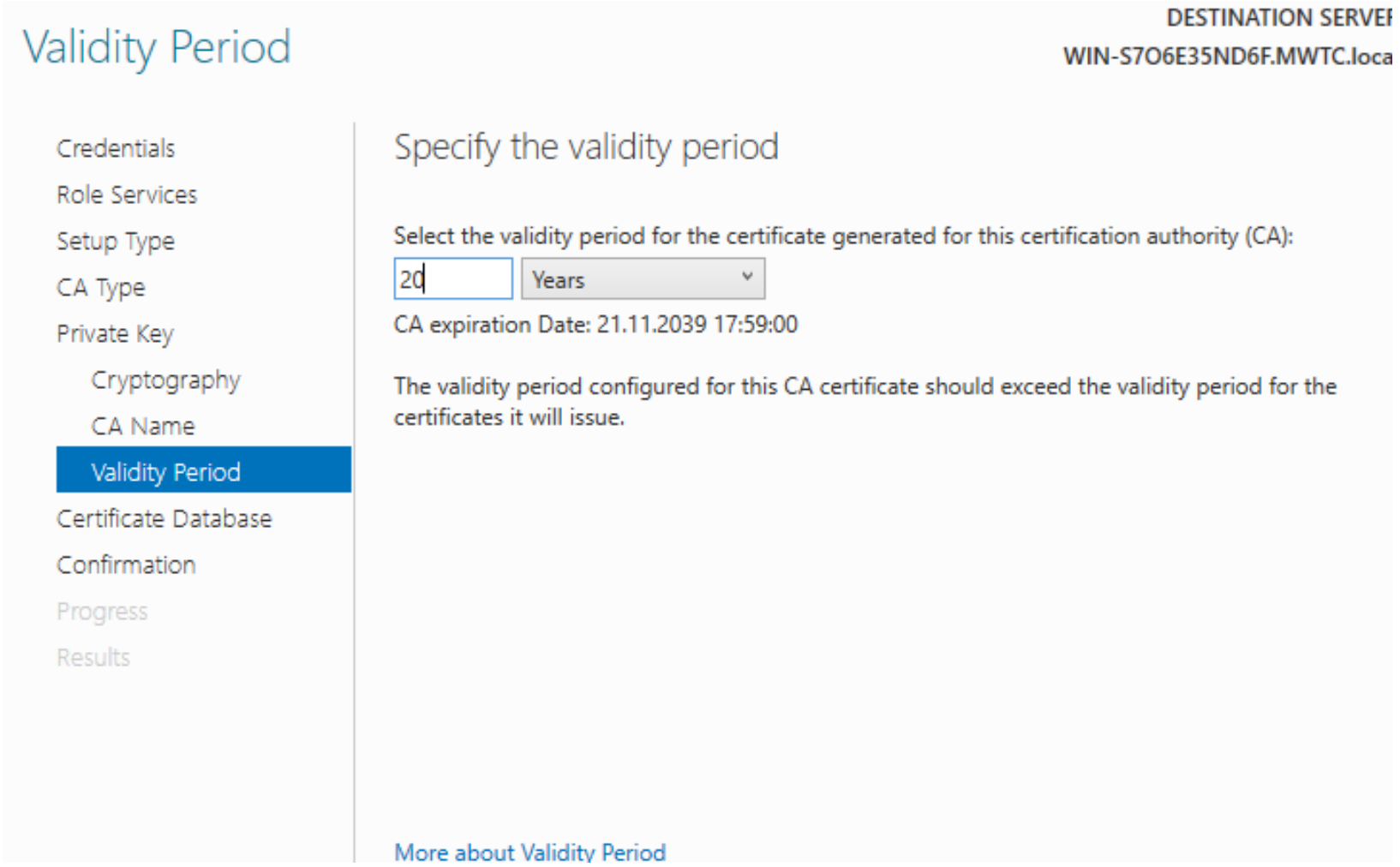
Konfiguracja Active Directory Certificates Services



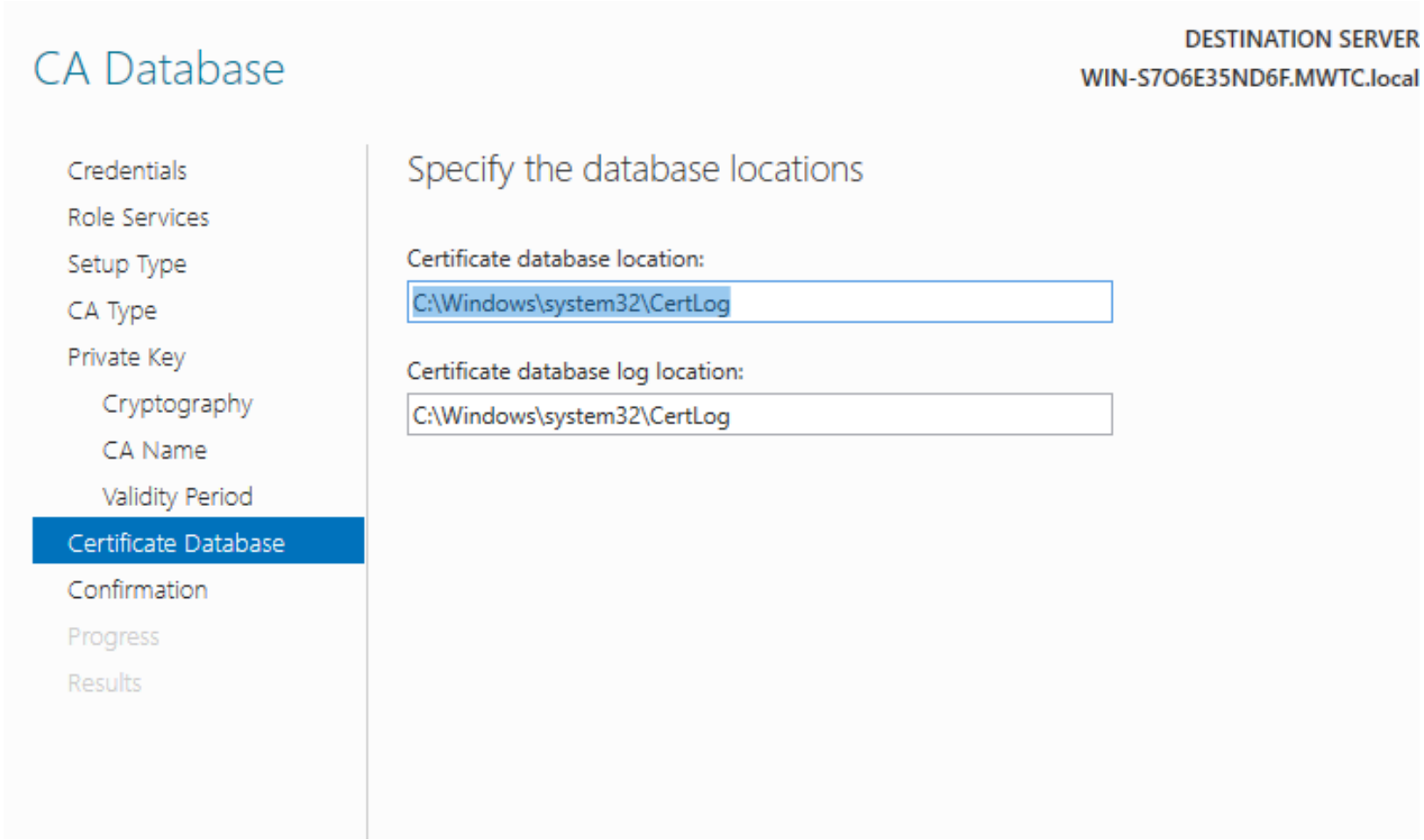
Konfiguracja Active Directory Certificates Services



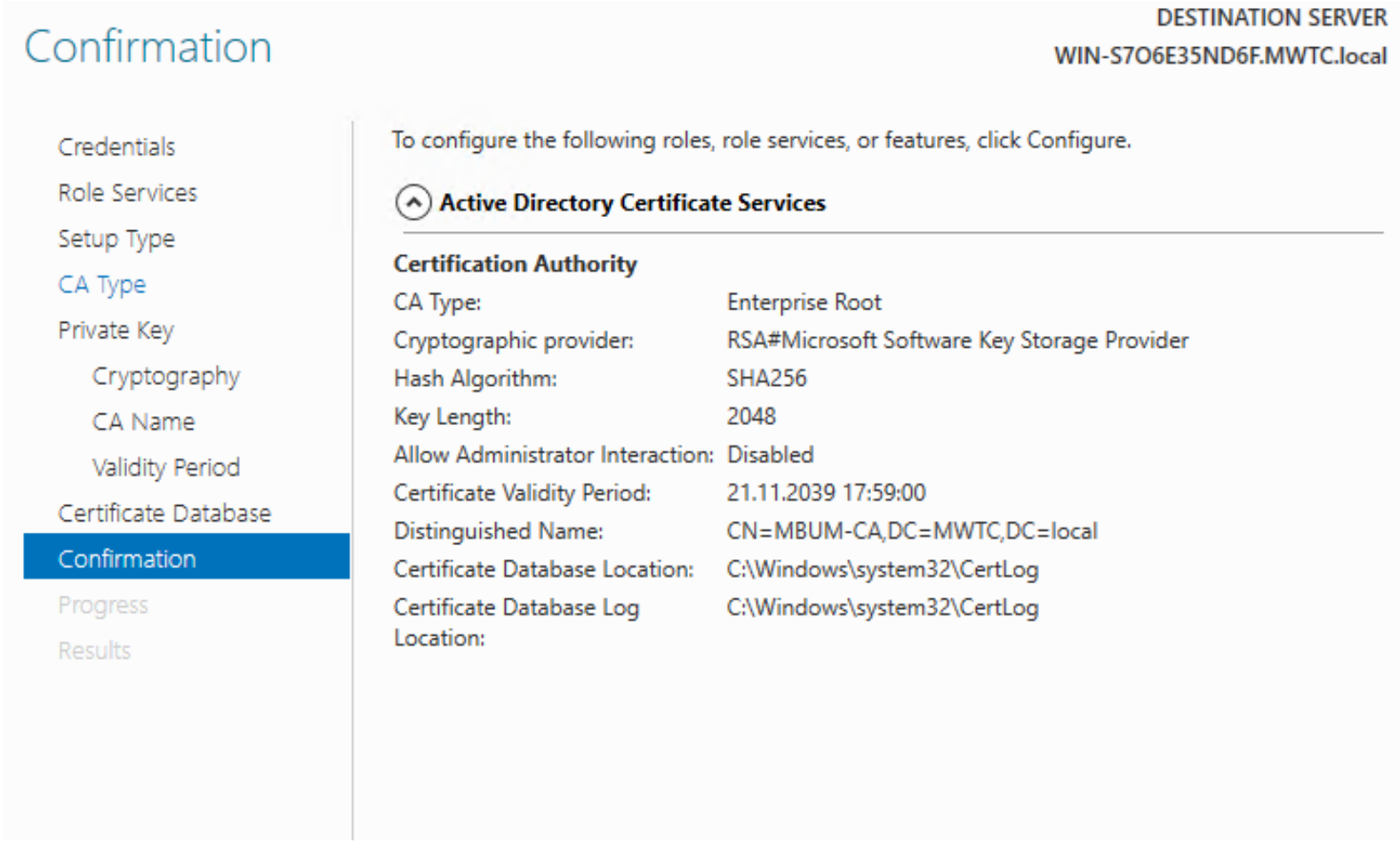
Konfiguracja Active Directory Certificates Services



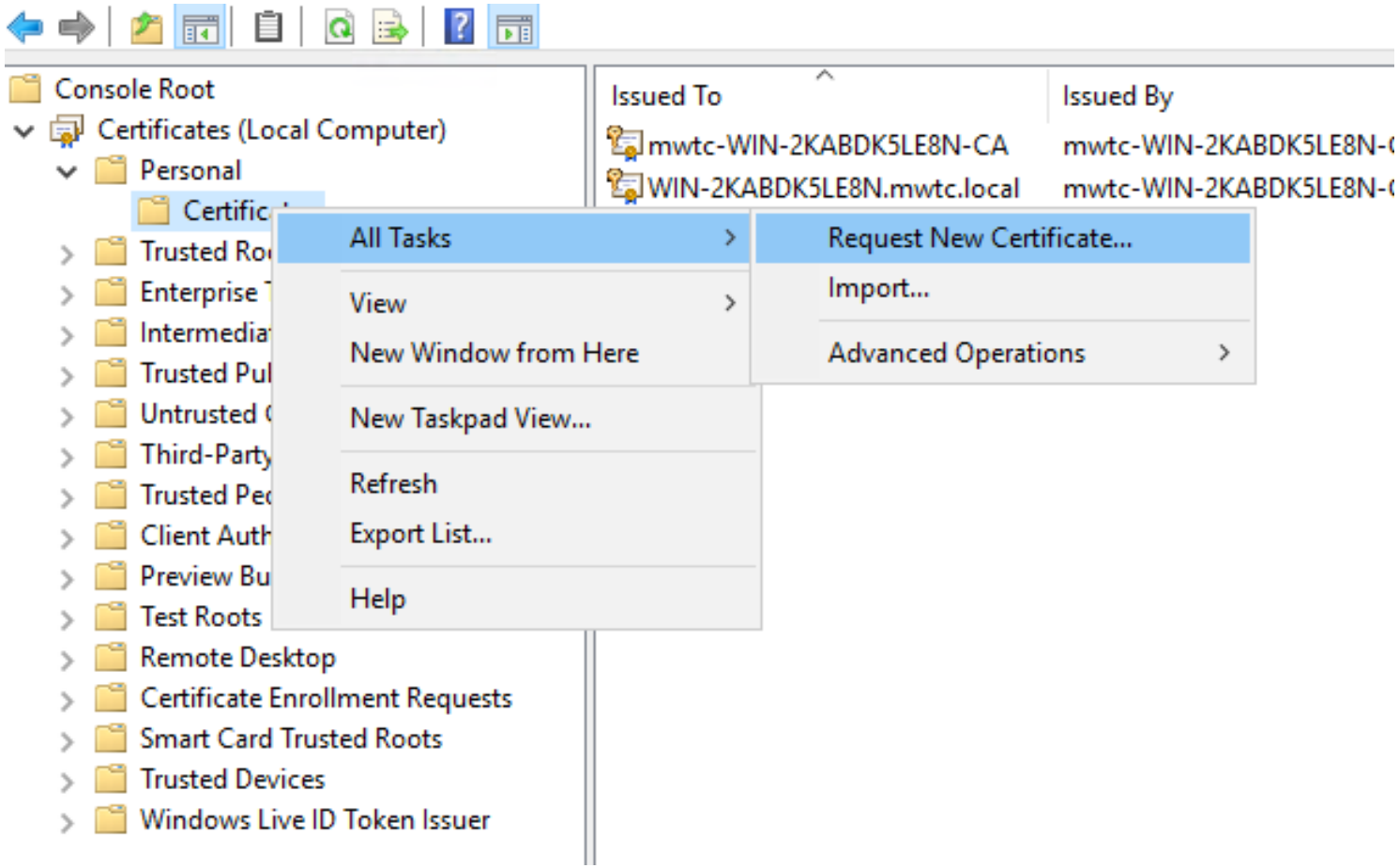
Konfiguracja Active Directory Certificates Services



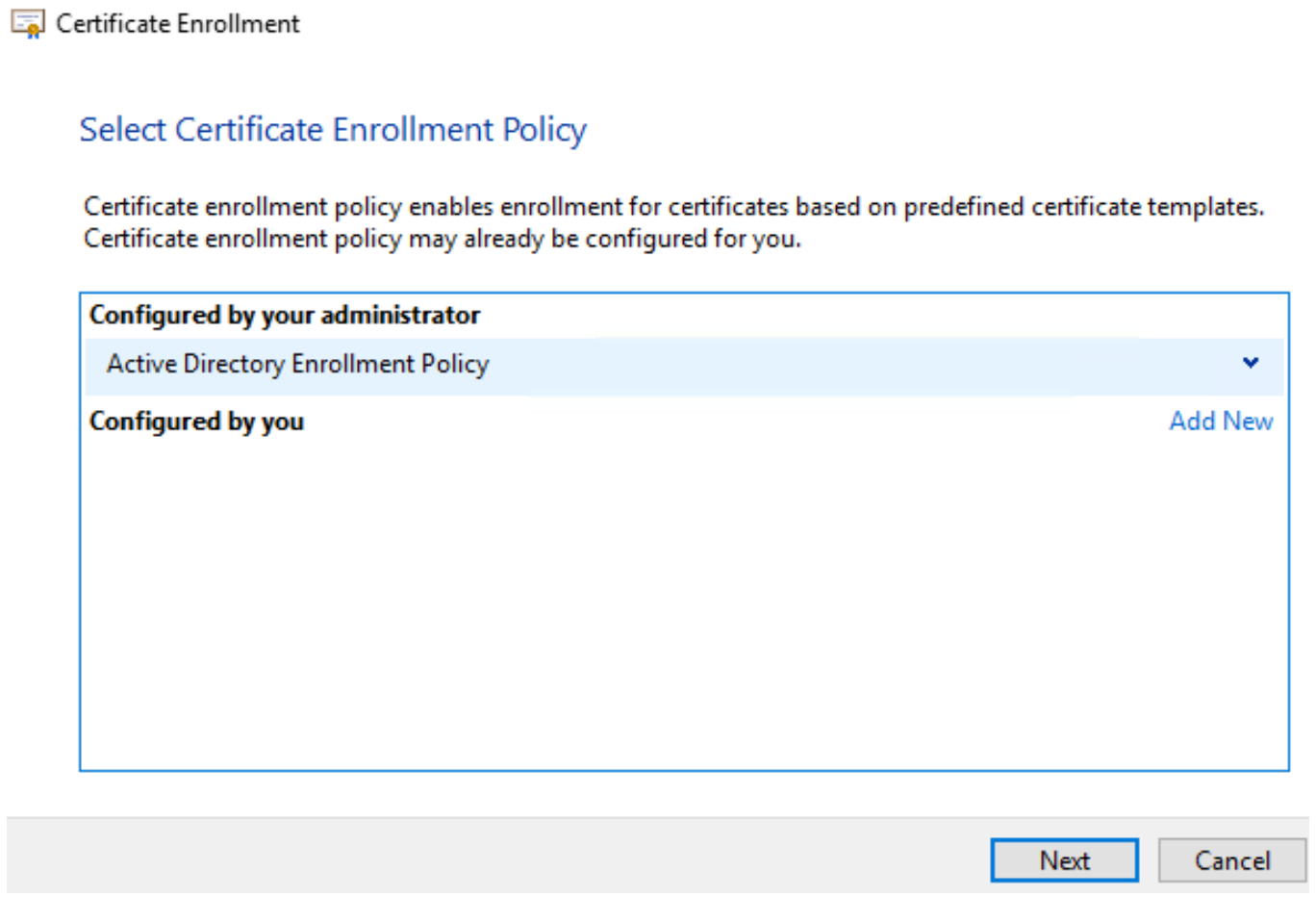
Konfiguracja Active Directory Certificates Services



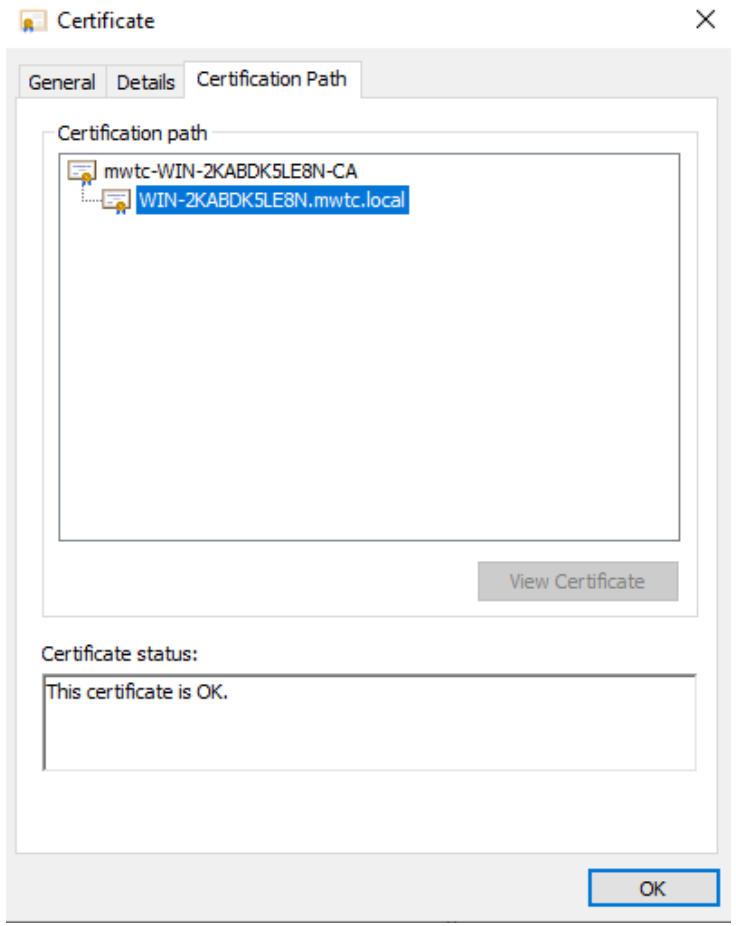
Konfiguracja Active Directory Certificates Services



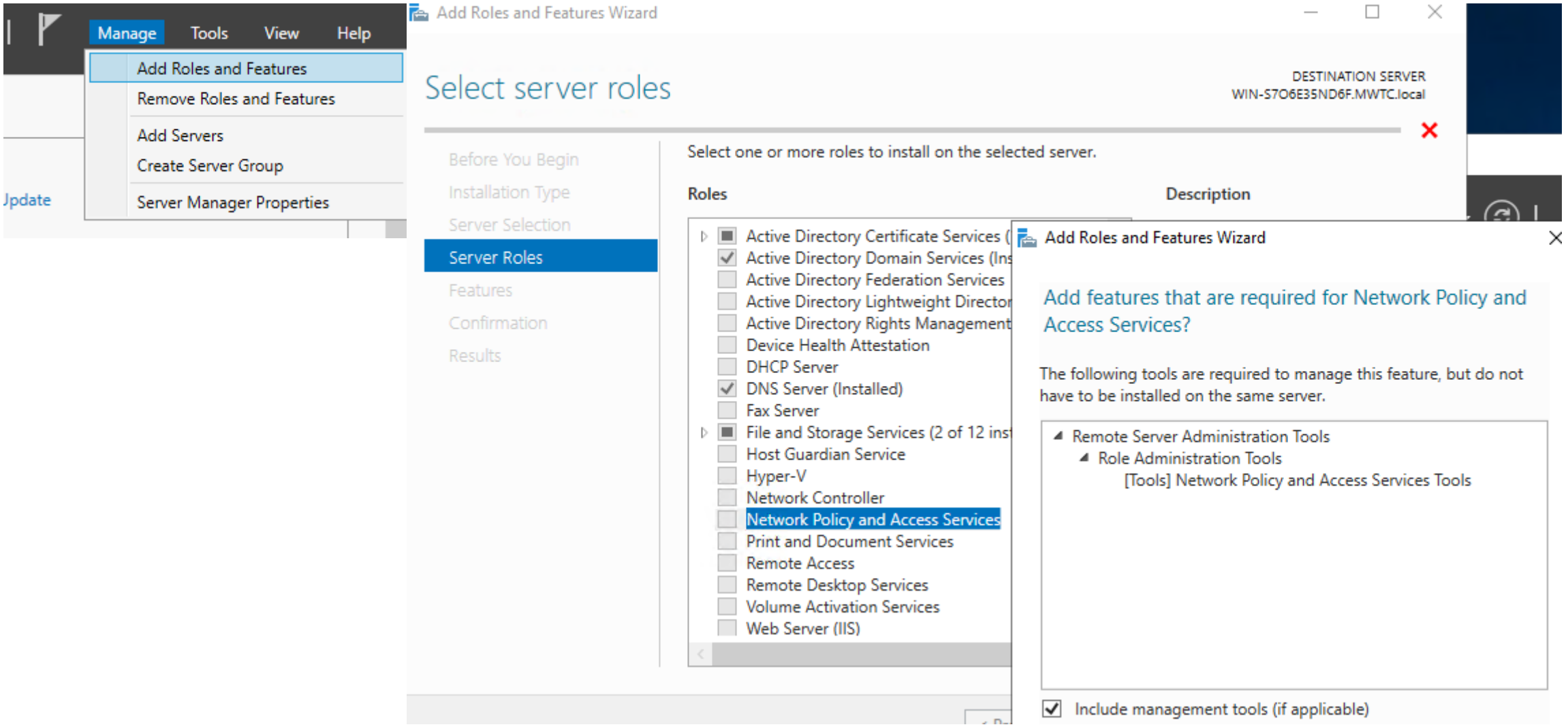
Konfiguracja Active Directory Certificates Services



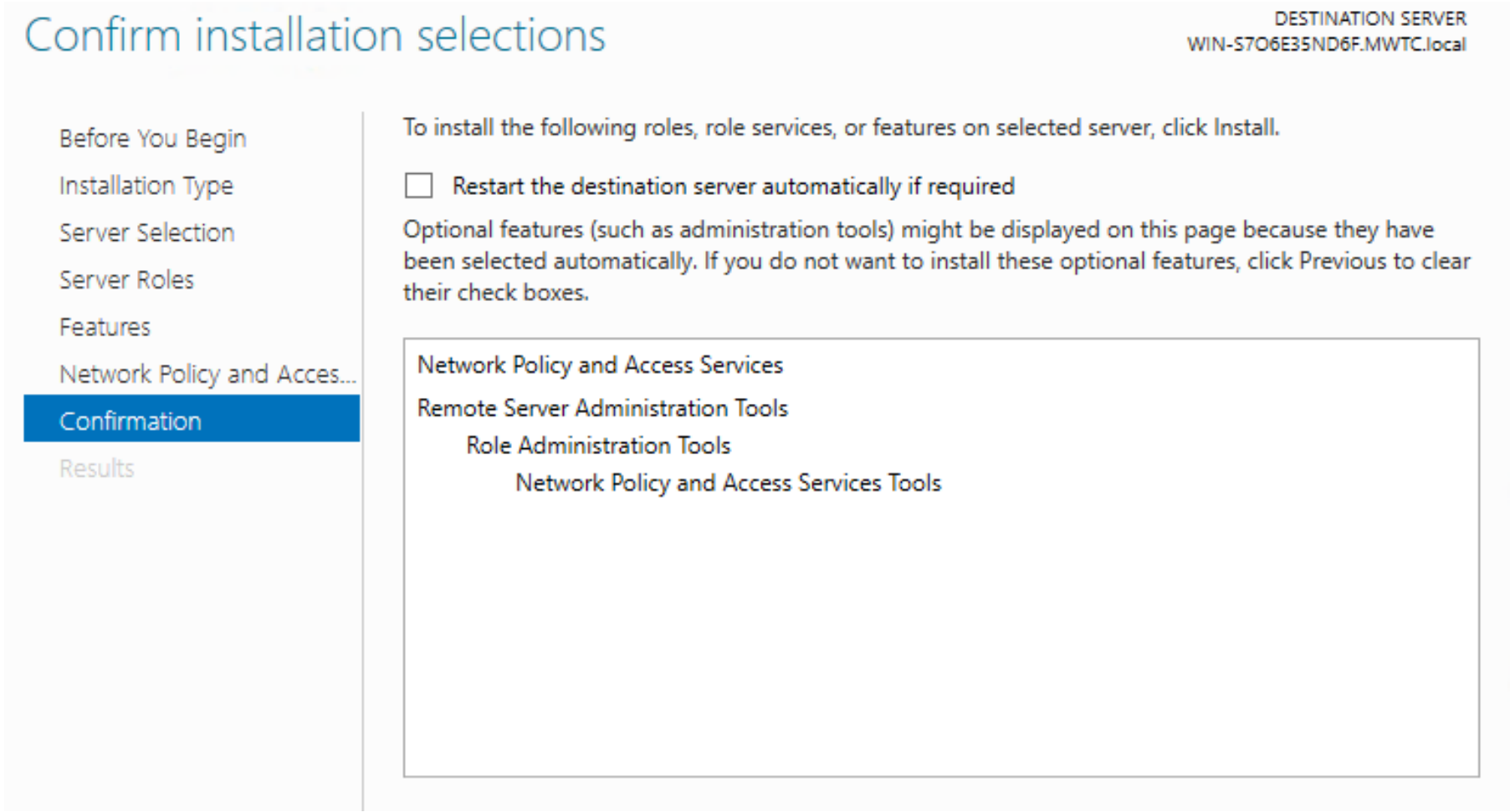
Konfiguracja Active Directory Certificates Services



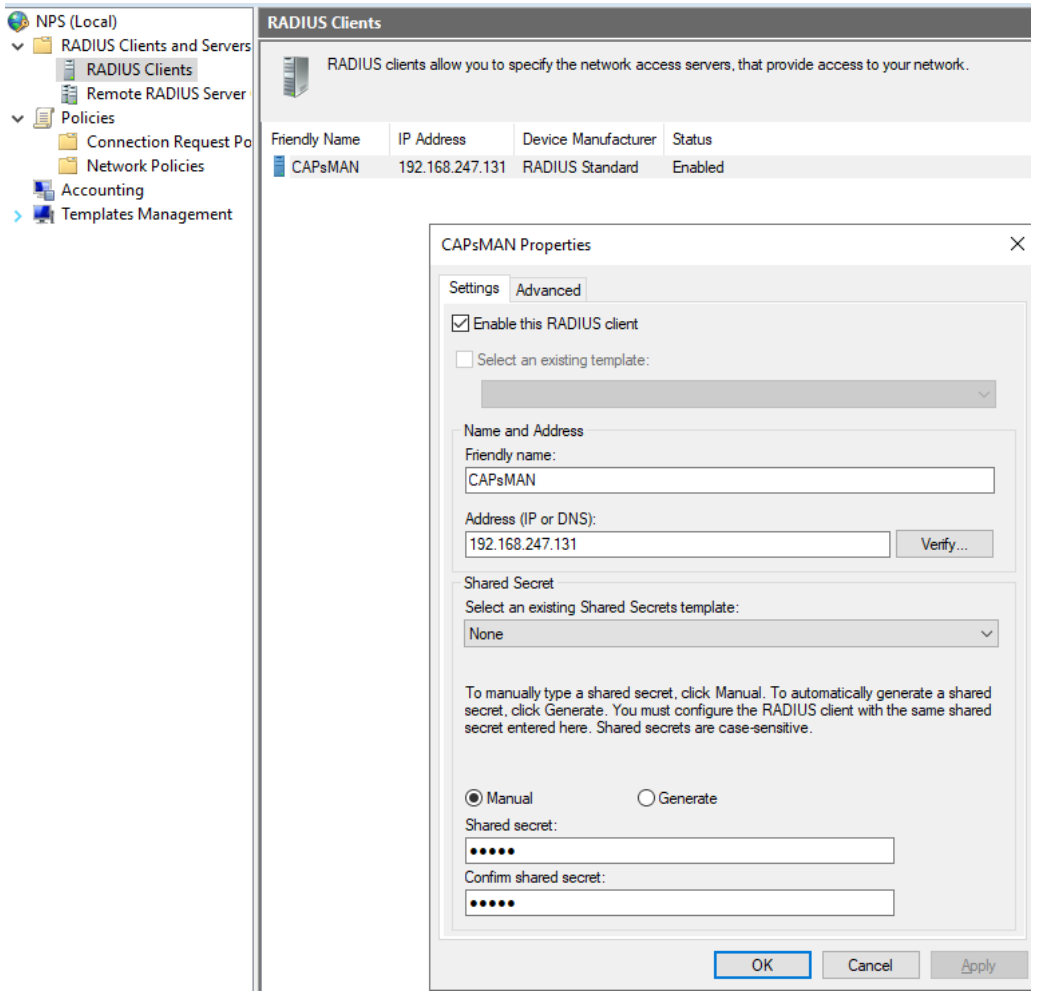
Instalacja Network Policy Server



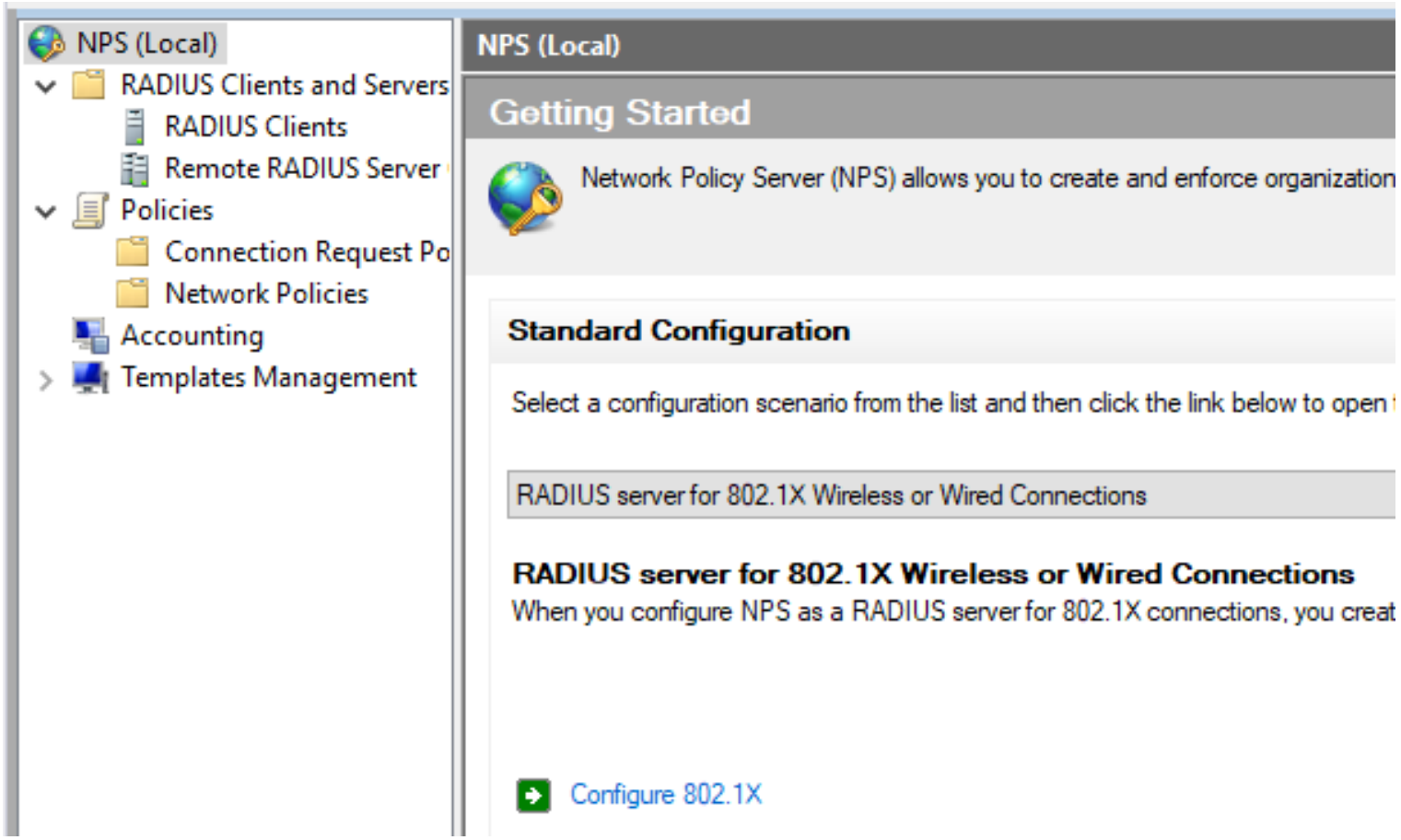
Instalacja Network Policy Server



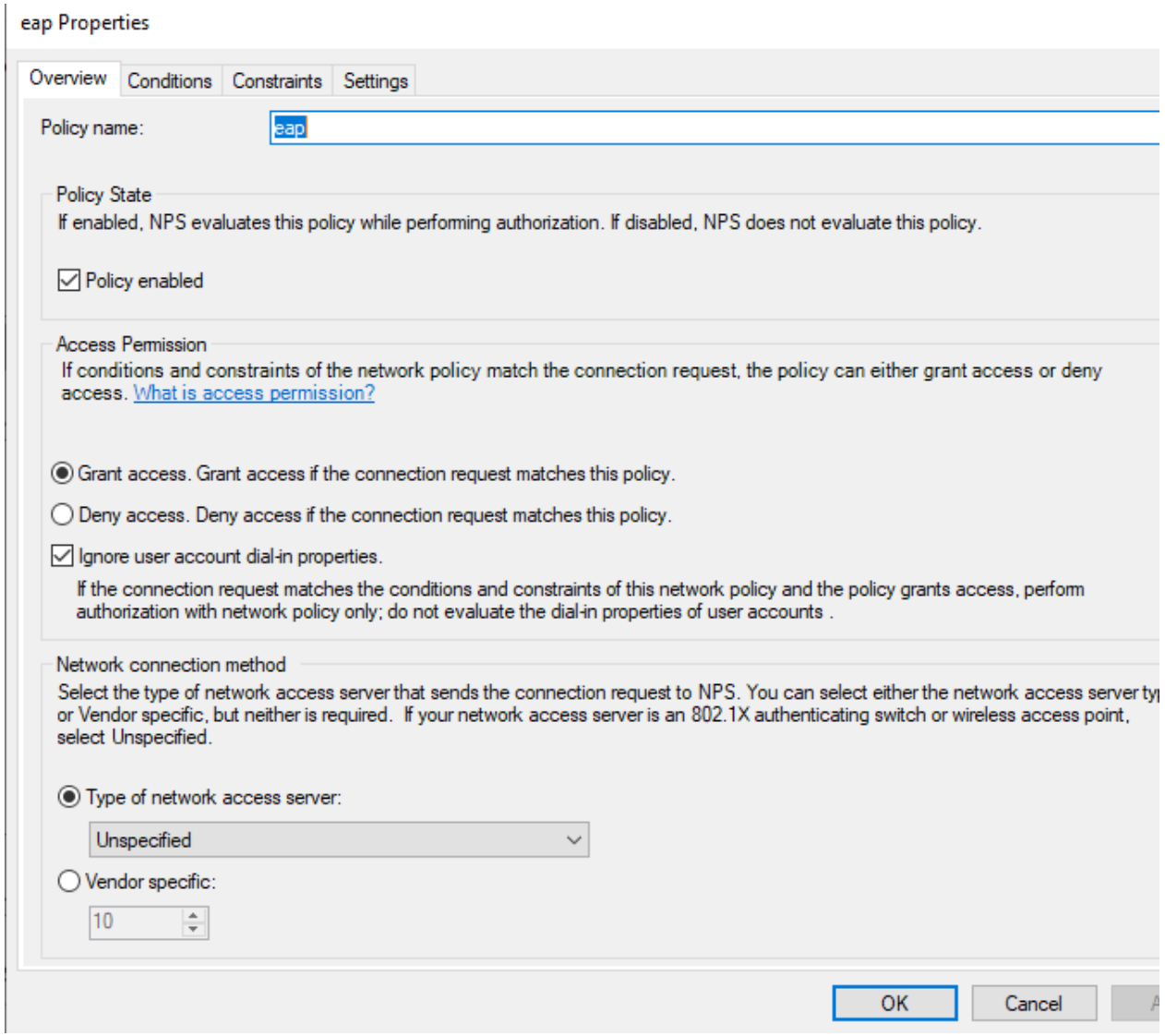
Konfiguracja NPS – Radius Clients



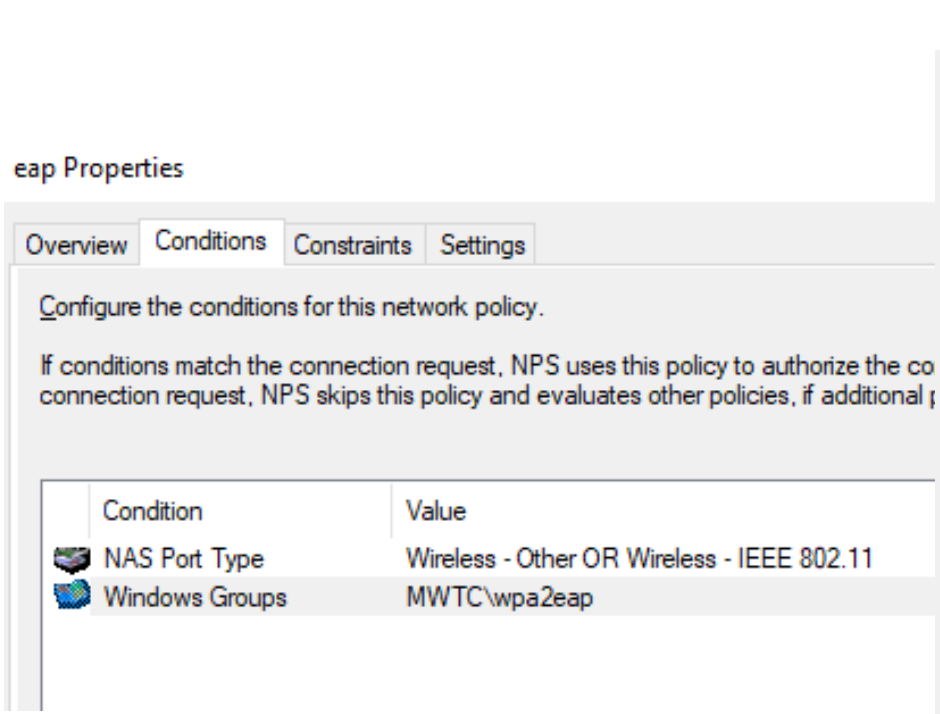
Konfiguracja NPS – Polityka 802.1x

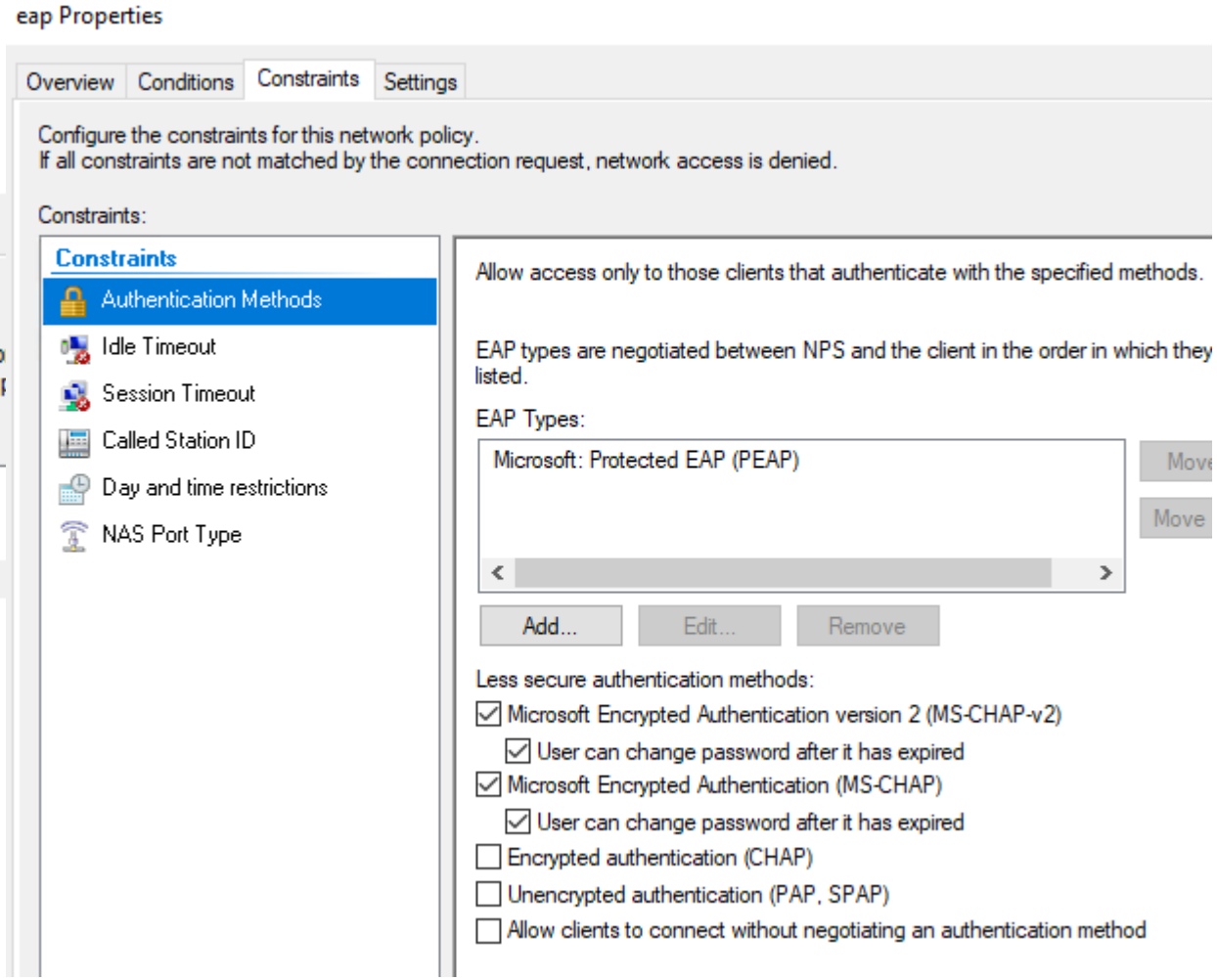


Konfiguracja NPS – Polityka 802.1x

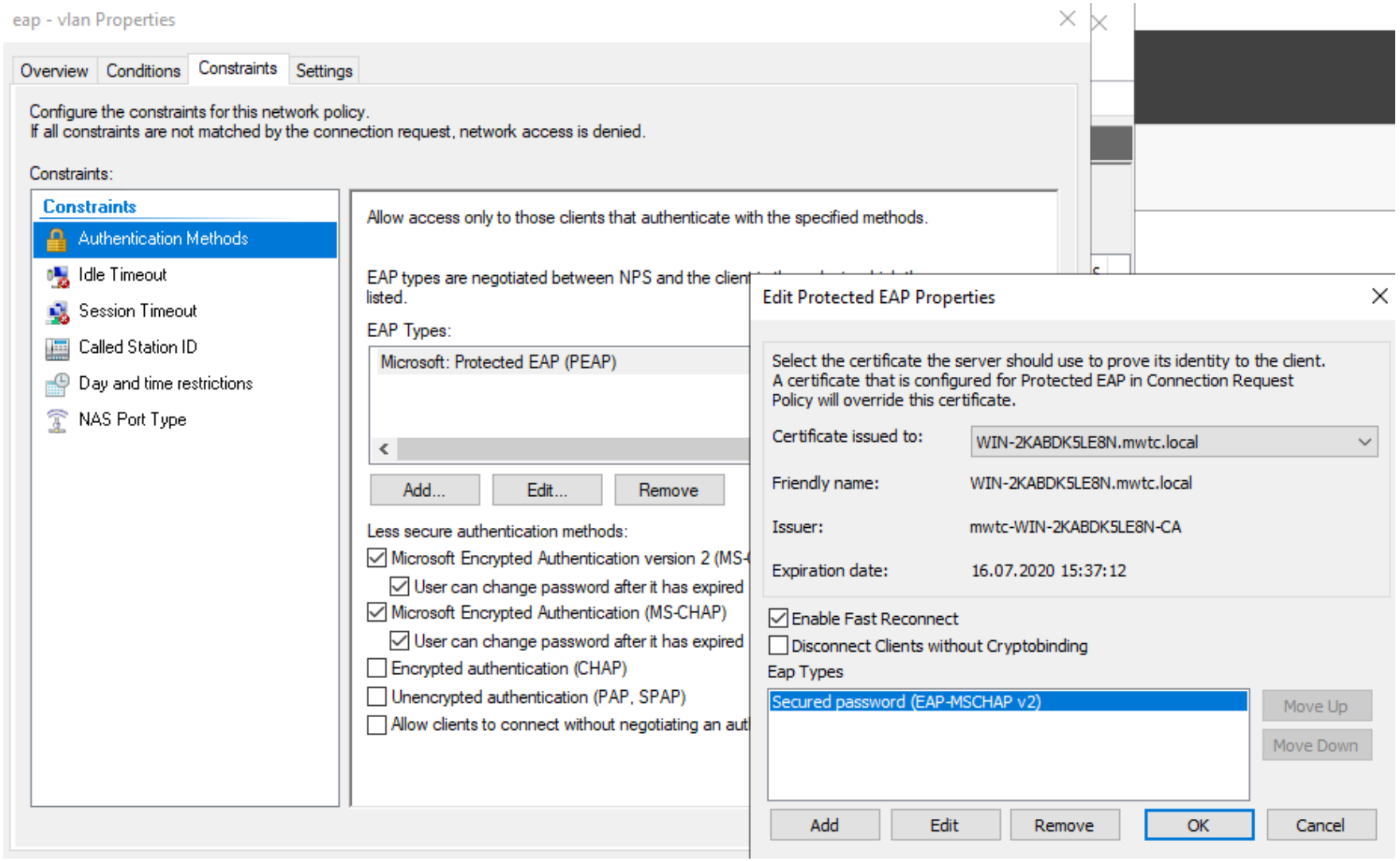


Konfiguracja NPS – Polityka 802.1x

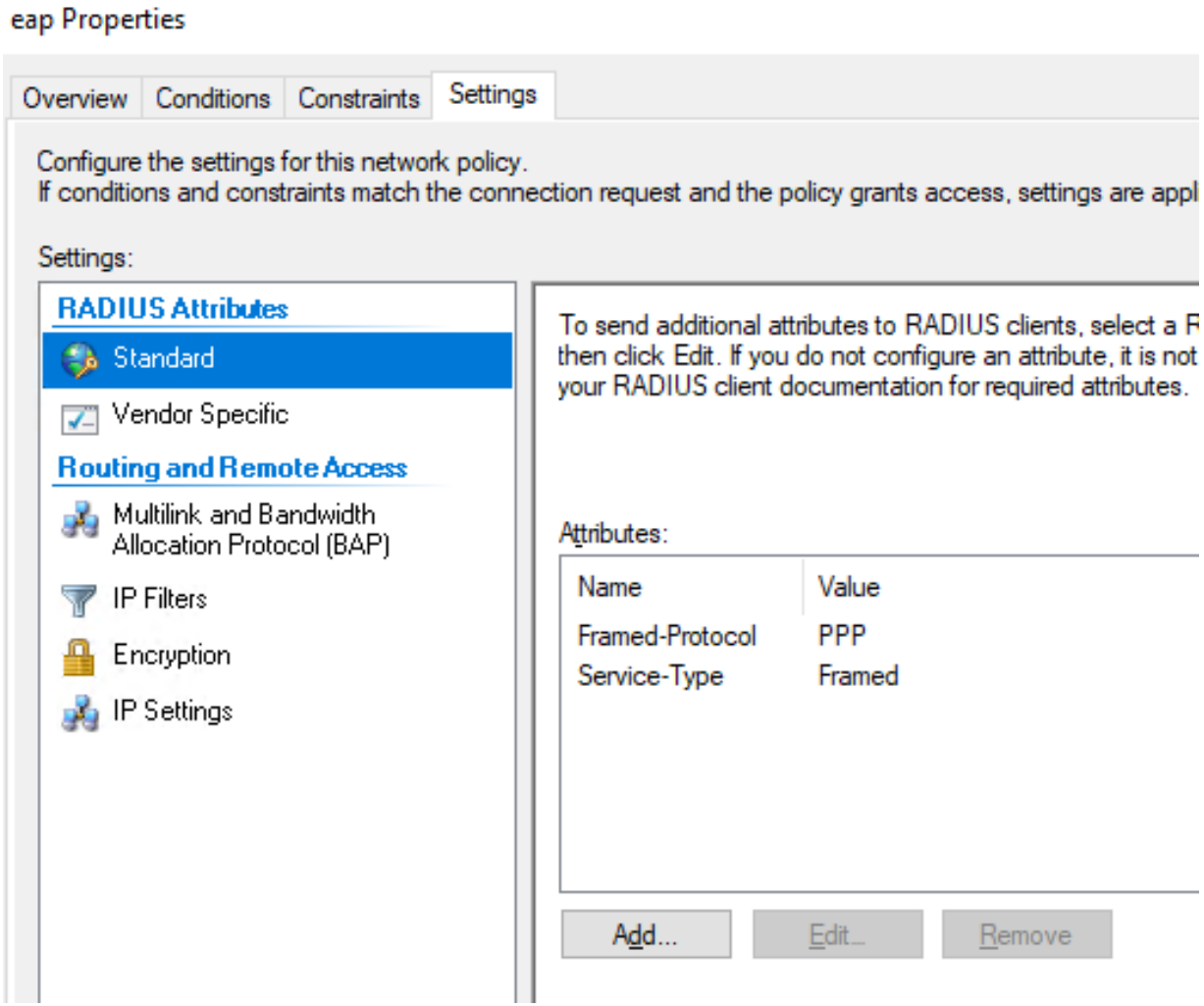




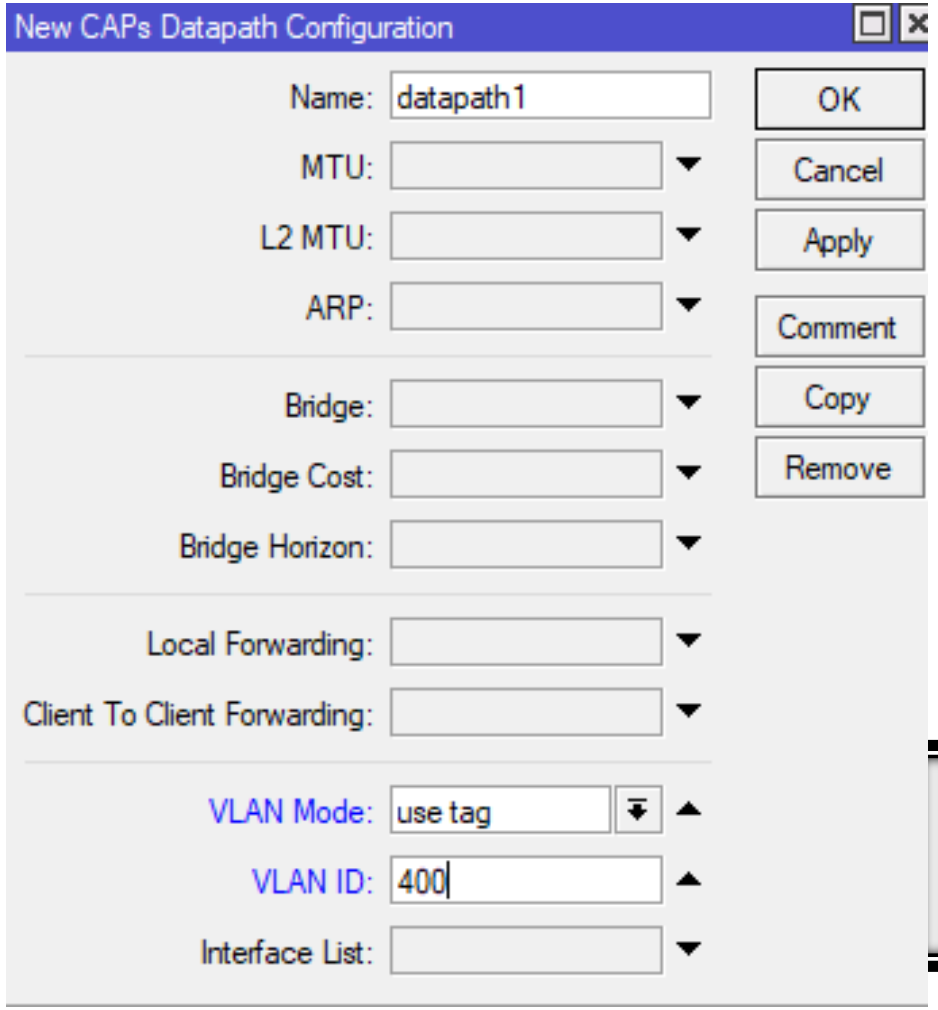
Konfiguracja NPS – Polityka 802.1x



Konfiguracja NPS – Polityka 802.1x



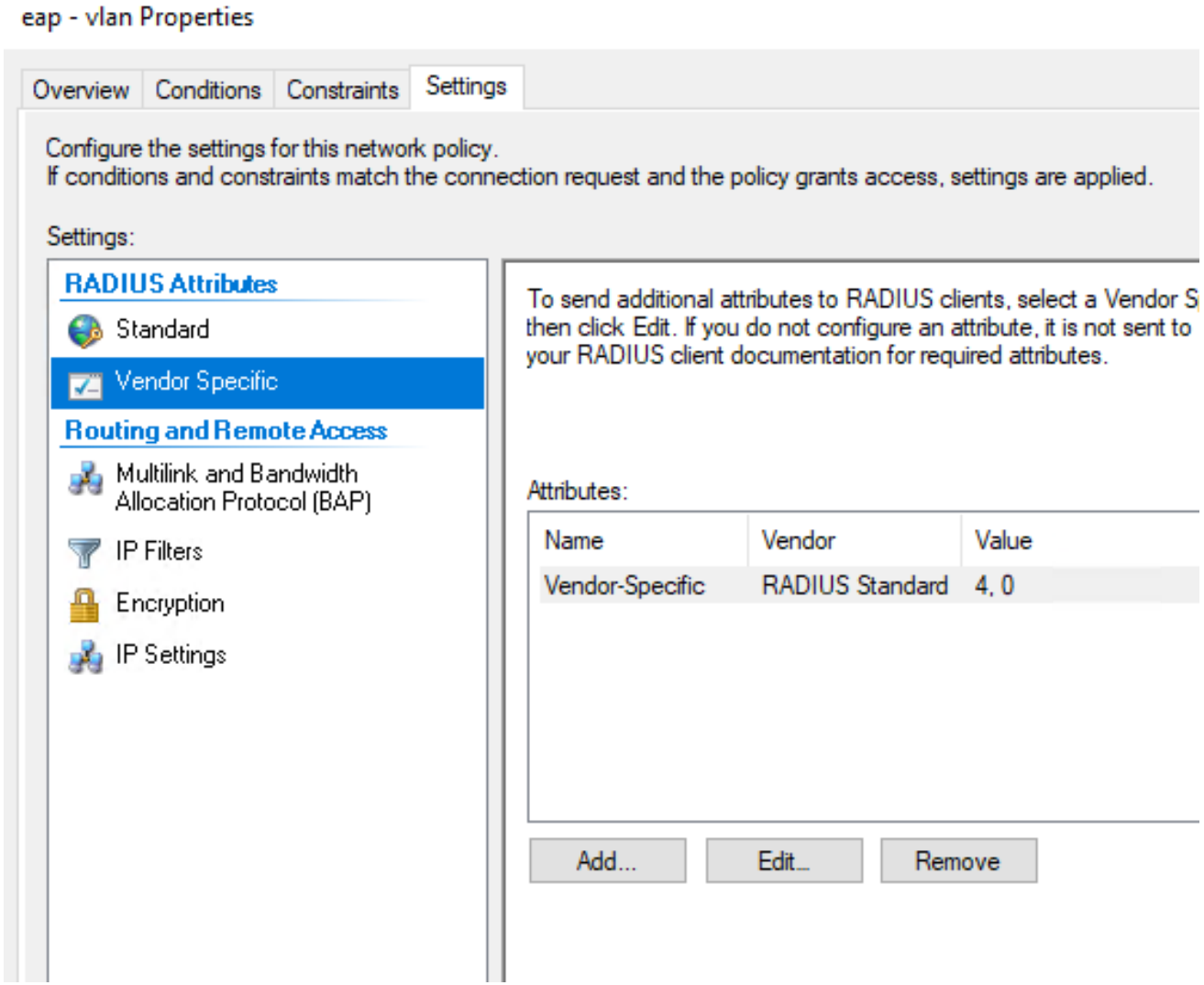
Konfiguracja NPS – Polityka 802.1x (z VLAN)



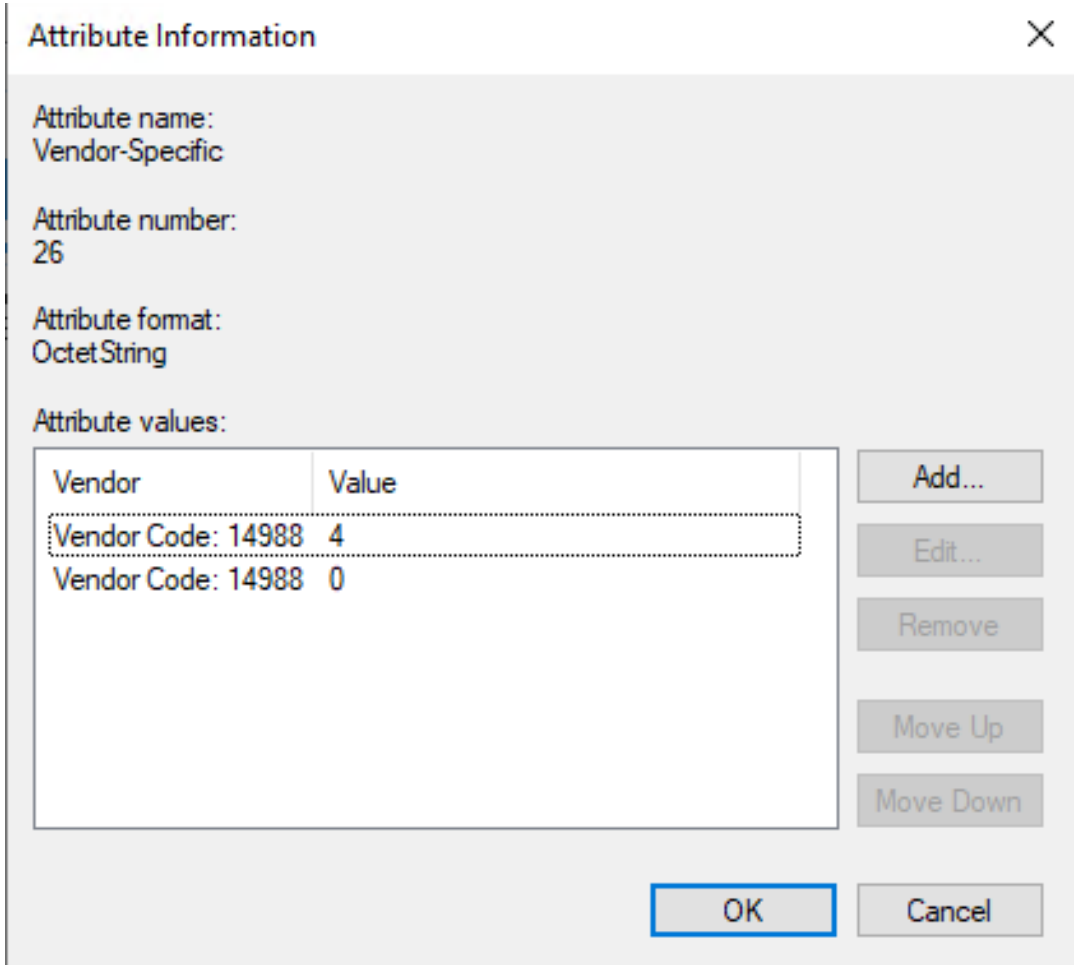
https://wiki.mikrotik.com/wiki/Manual:RADIUS_Client

MIKROTIK_WIRELESS_VLANID	14988	26
MIKROTIK_WIRELESS_VLANIDTYPE	14988	27

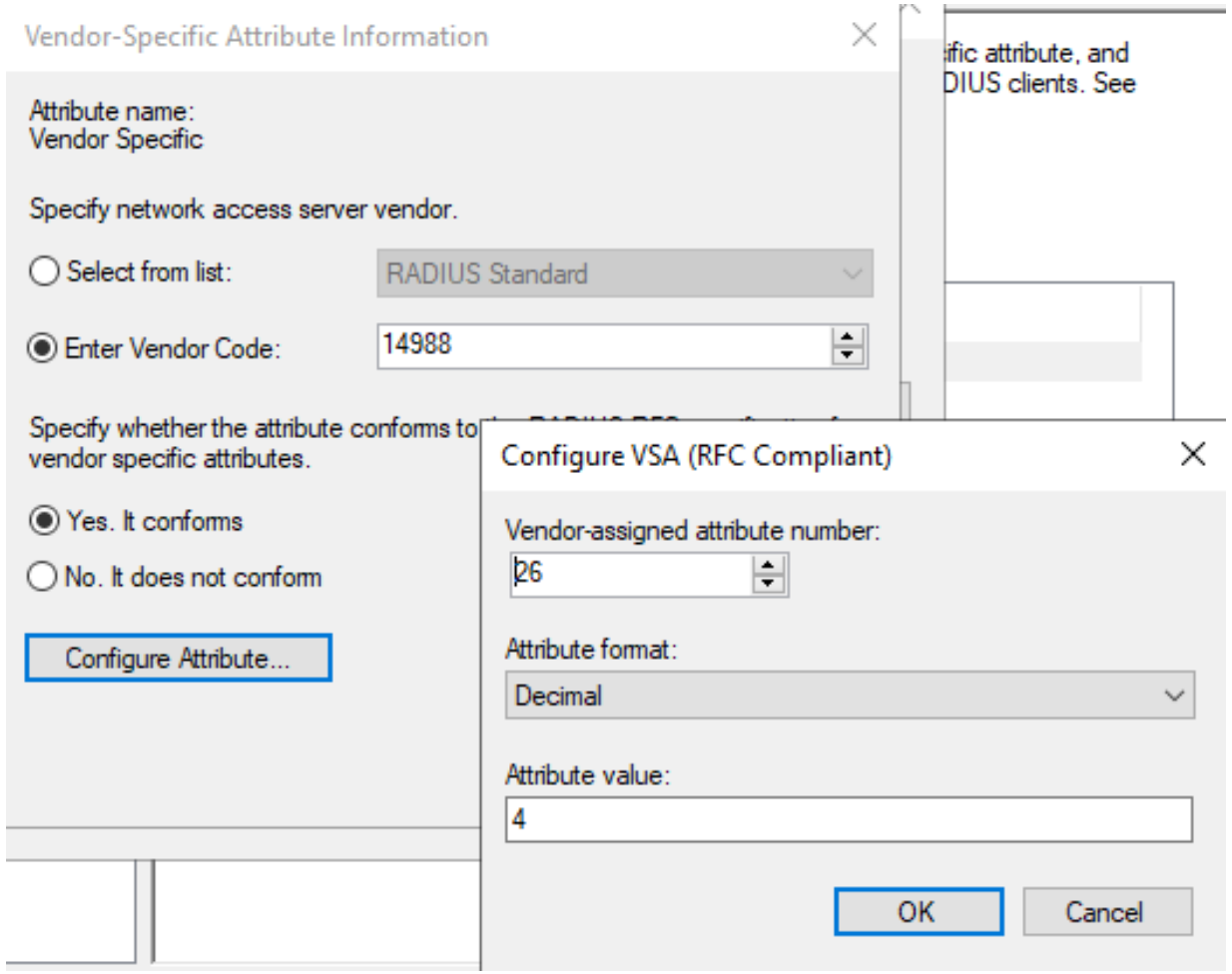
Konfiguracja NPS – Polityka 802.1x (z VLAN)



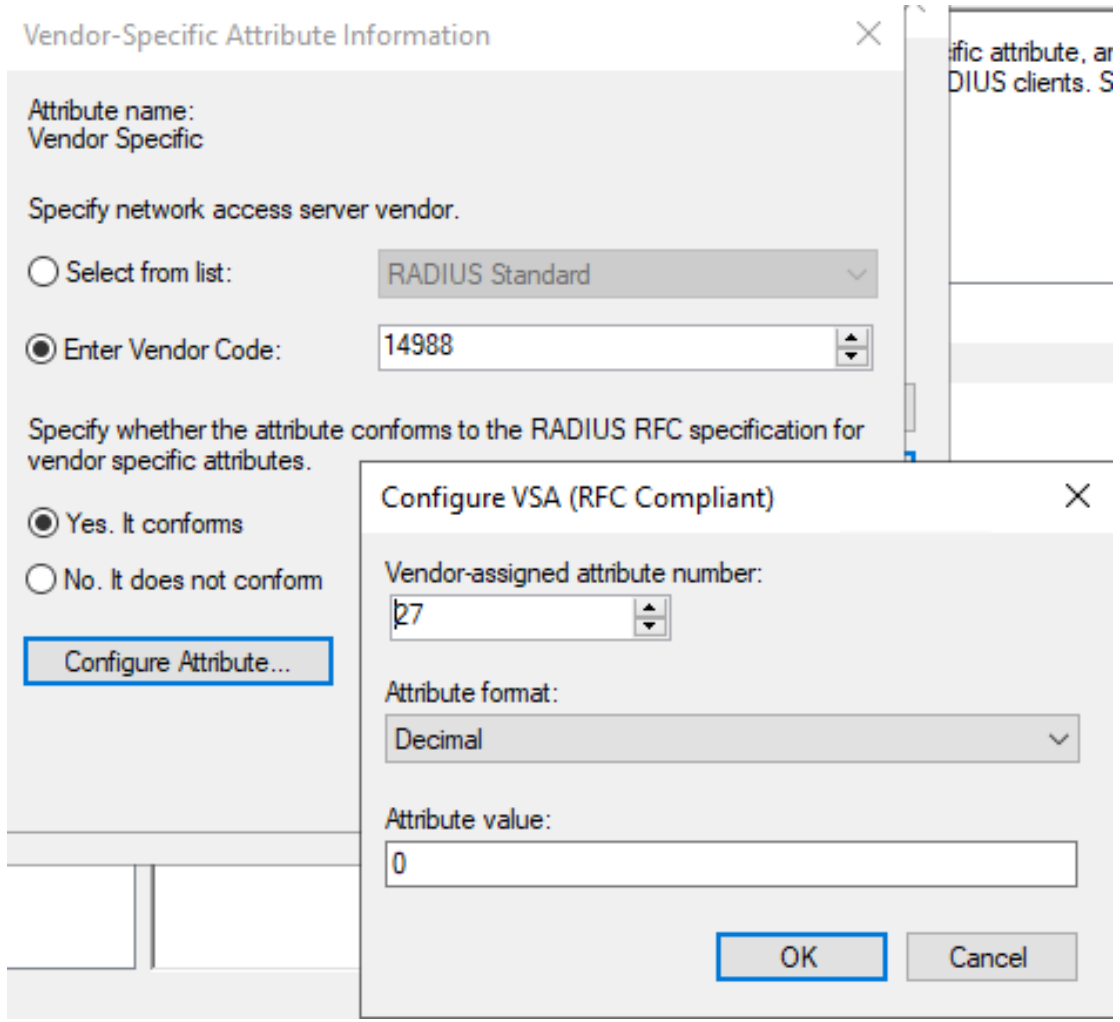
Konfiguracja NPS – Polityka 802.1x (z VLAN)



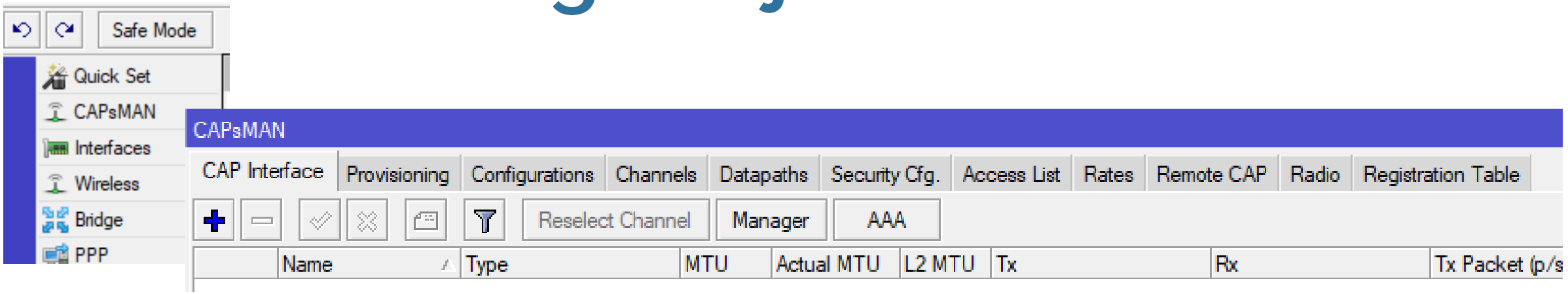
Konfiguracja NPS – Polityka 802.1x (z VLAN)



Konfiguracja NPS – Polityka 802.1x (z VLAN)

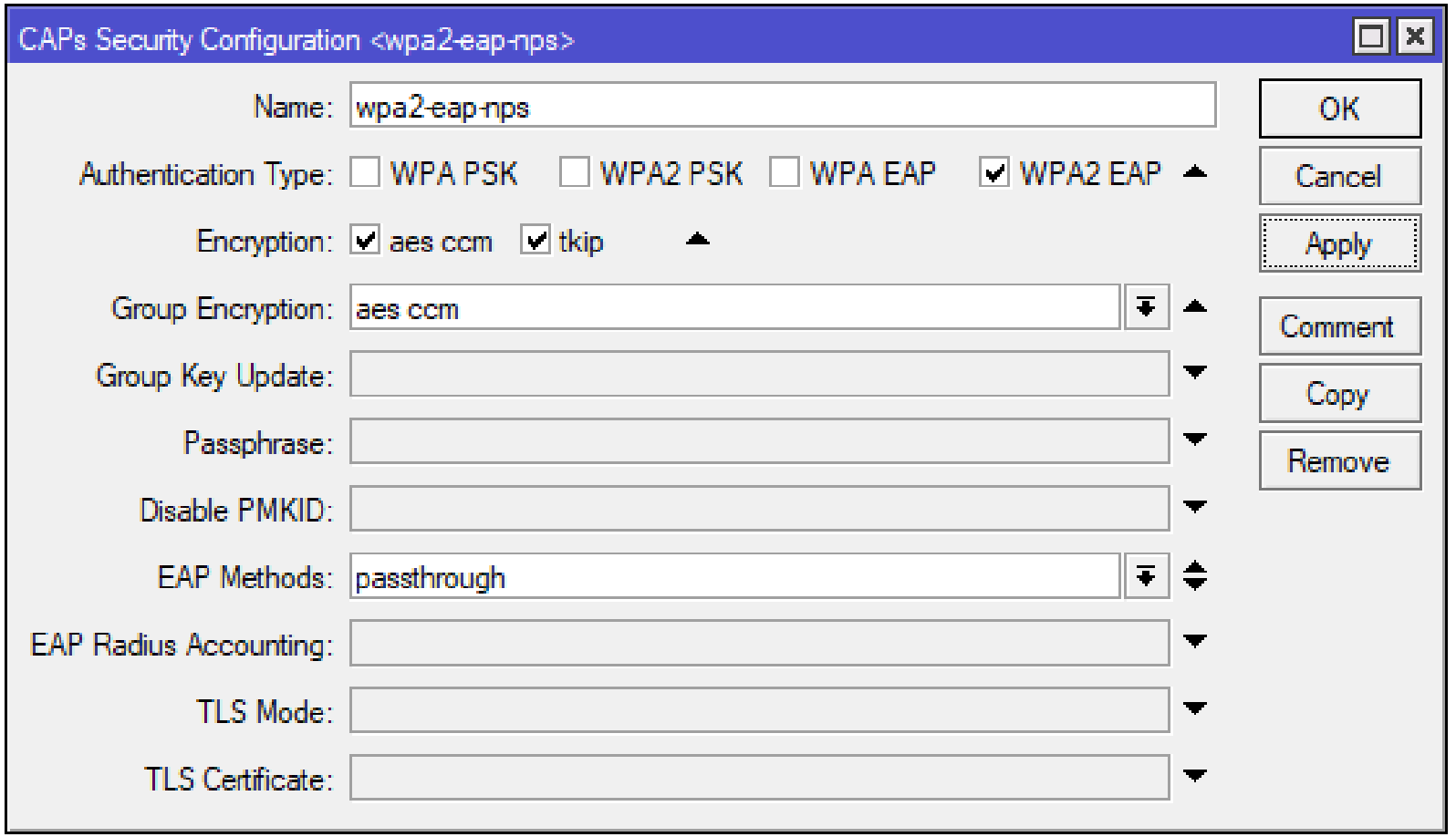


Konfiguracja CAPsMAN

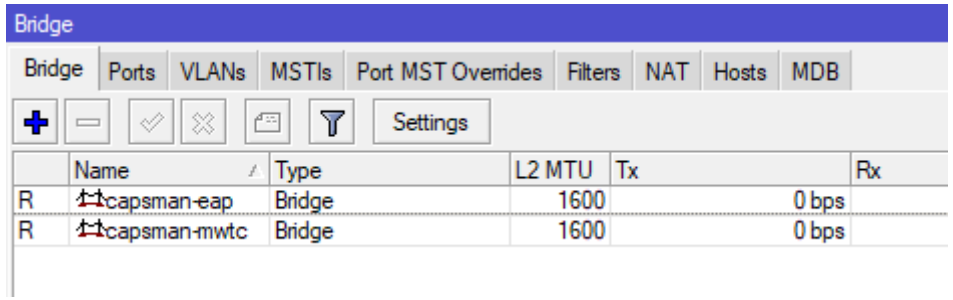


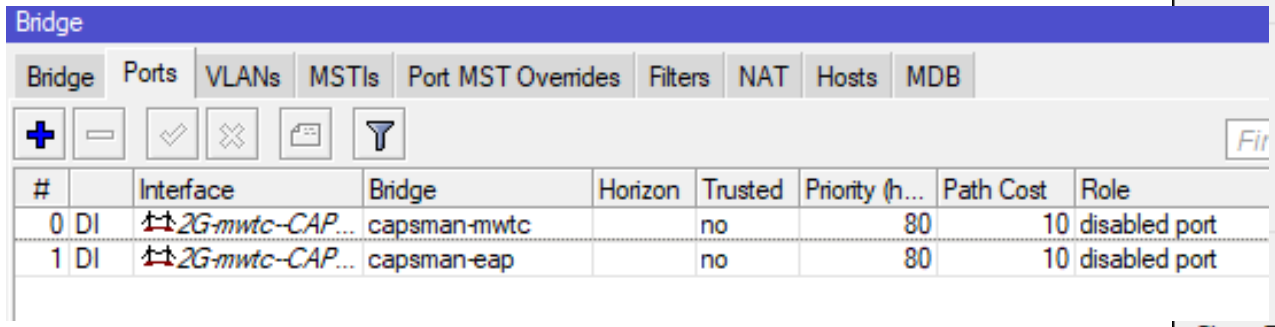
- ✓ **CAP Interface** – interfejsy odpowiadające SSID i modułom radiowym punktów dostępowych
- ✓ **Provisioning** –zarządzanie dystrybucją konfiguracji do punktów dostępowych
- ✓ **Configurations** – konfiguracje modułów radiowych (łączące dane z innych zakładek)
- ✓ **Channels** – ustawienia dotyczące częstotliwości
- ✓ **Datapaths** – konfiguracja jak obsługiwany będzie ruch klientów
- ✓ **Security Cfg** – ustawienie zabezpieczenia sieci, np. współdzielonego hasła (jeśli używane)
- ✓ **Access List** – dodatkowe reguły do secutity Cfg
- ✓ **Registration Table** – informacje o połączonych klientach

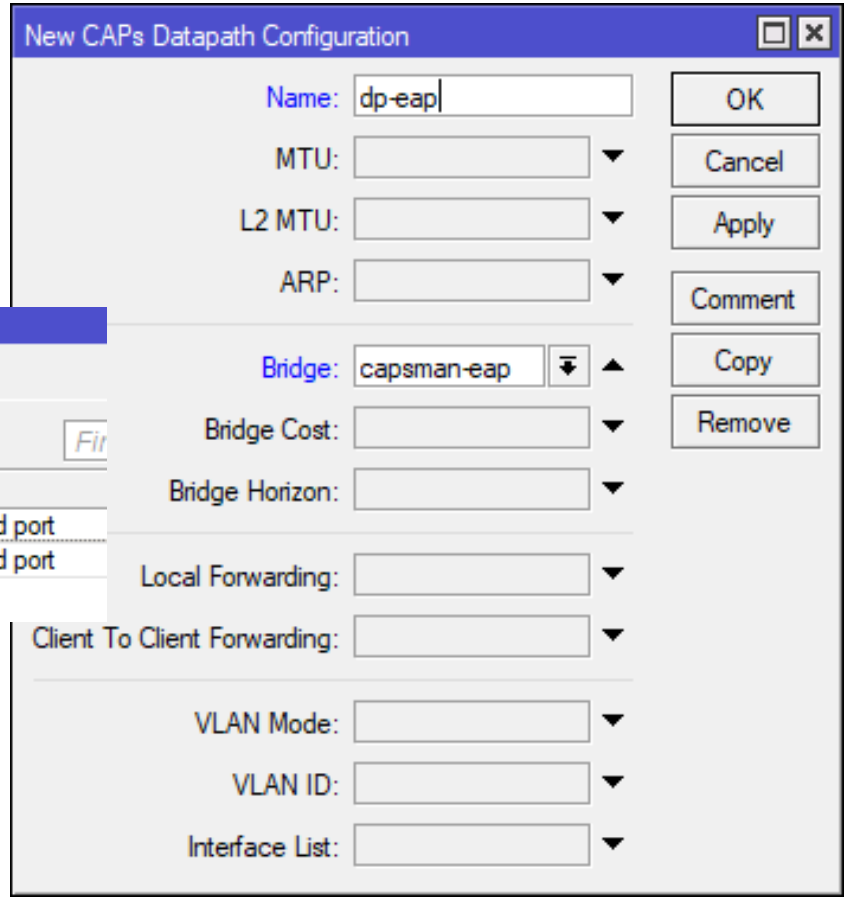
Konfiguracja CAPsMAN



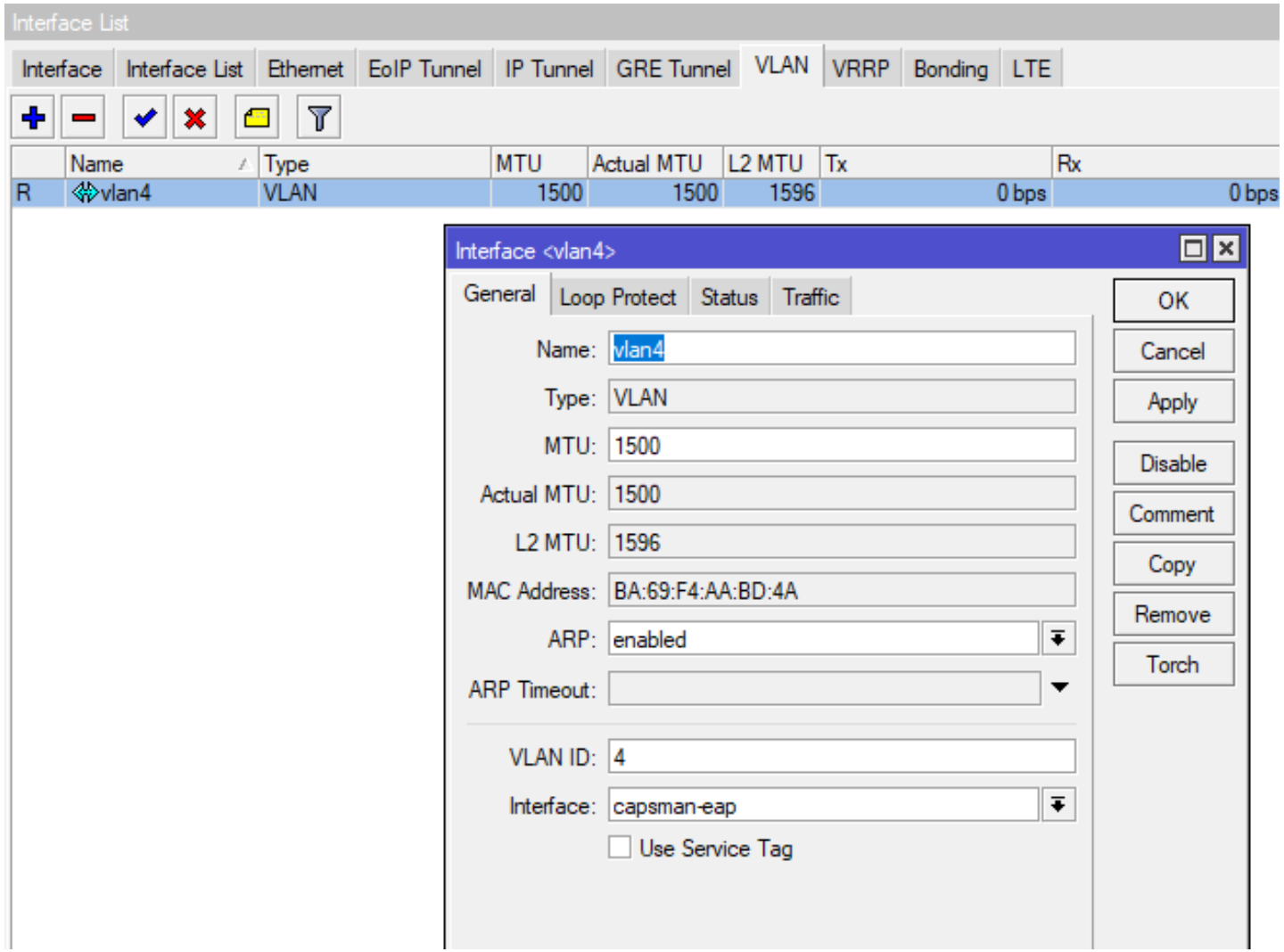
Konfiguracja CAPsMAN - bridge



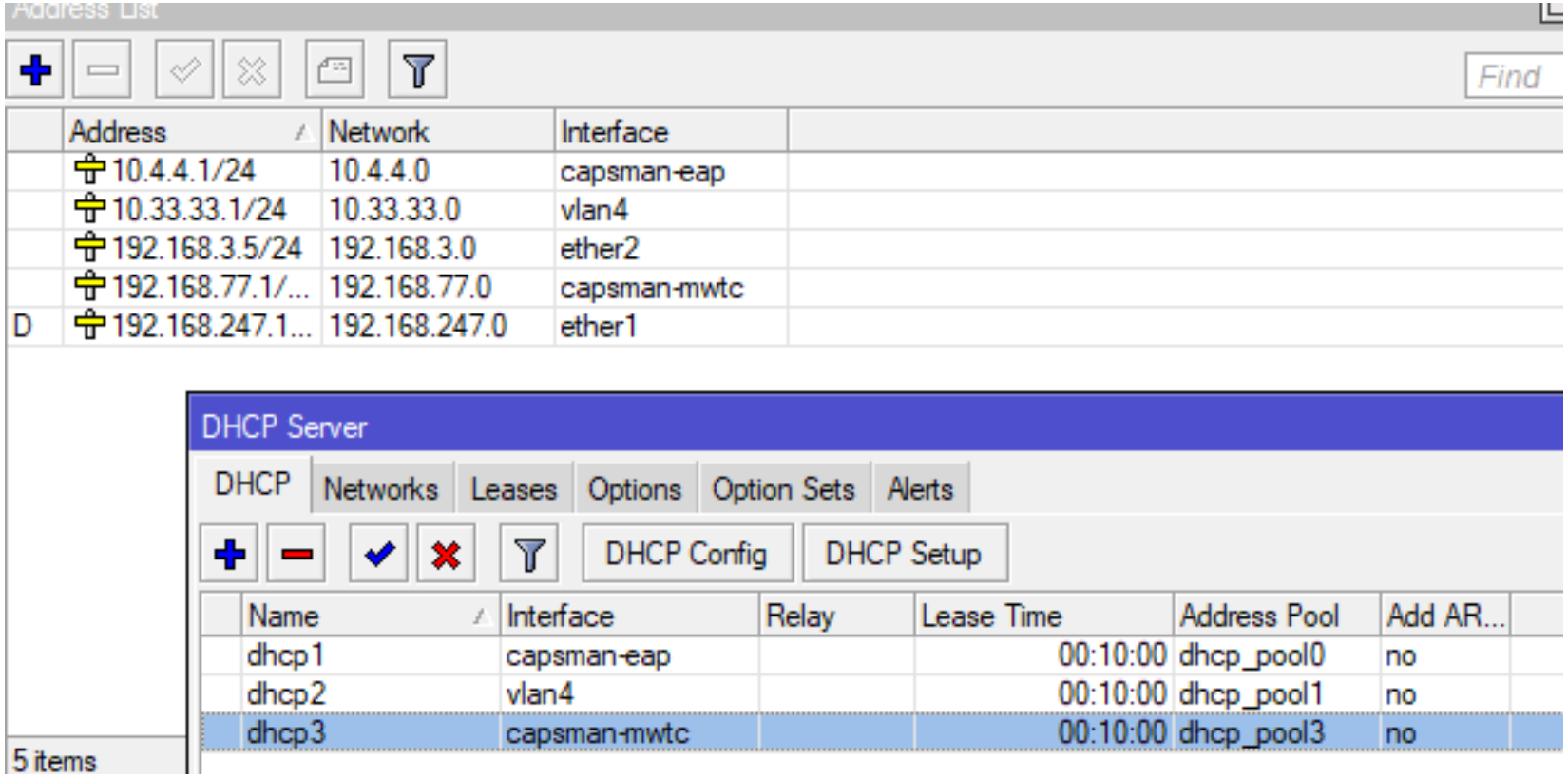




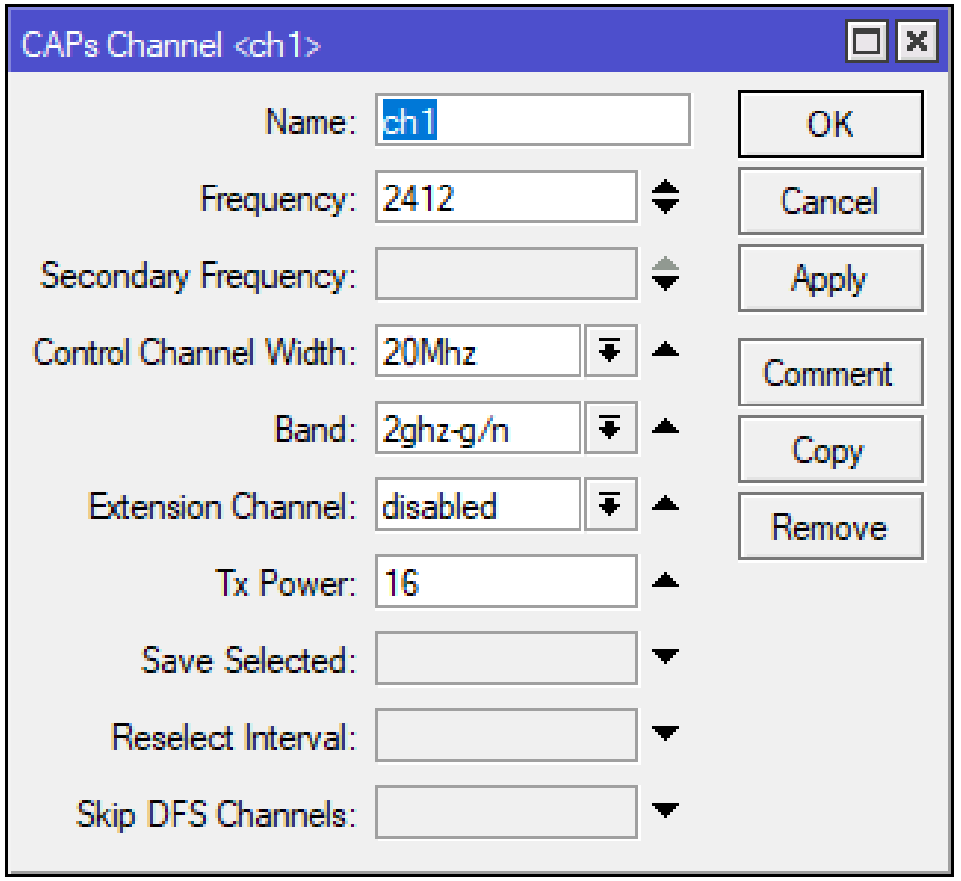
Konfiguracja - VLAN



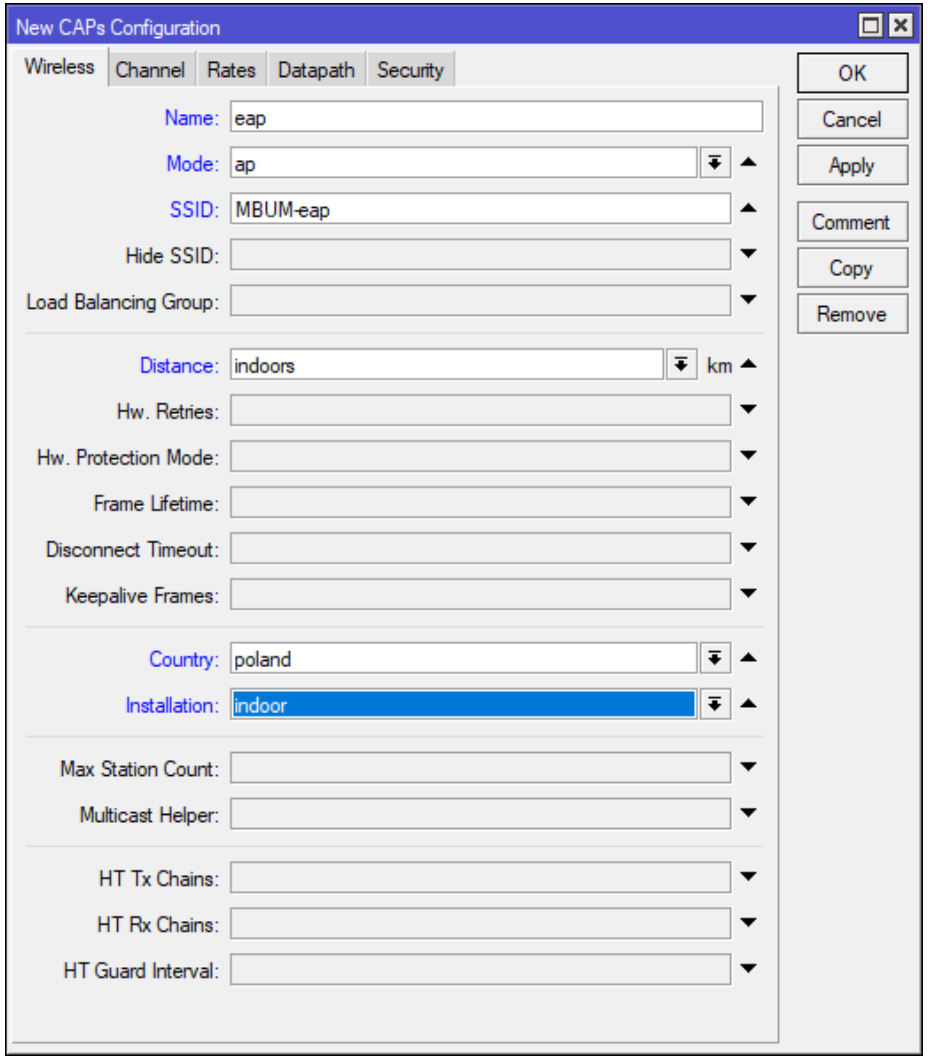
Konfiguracja – adresacja IP/ dhcp-server …



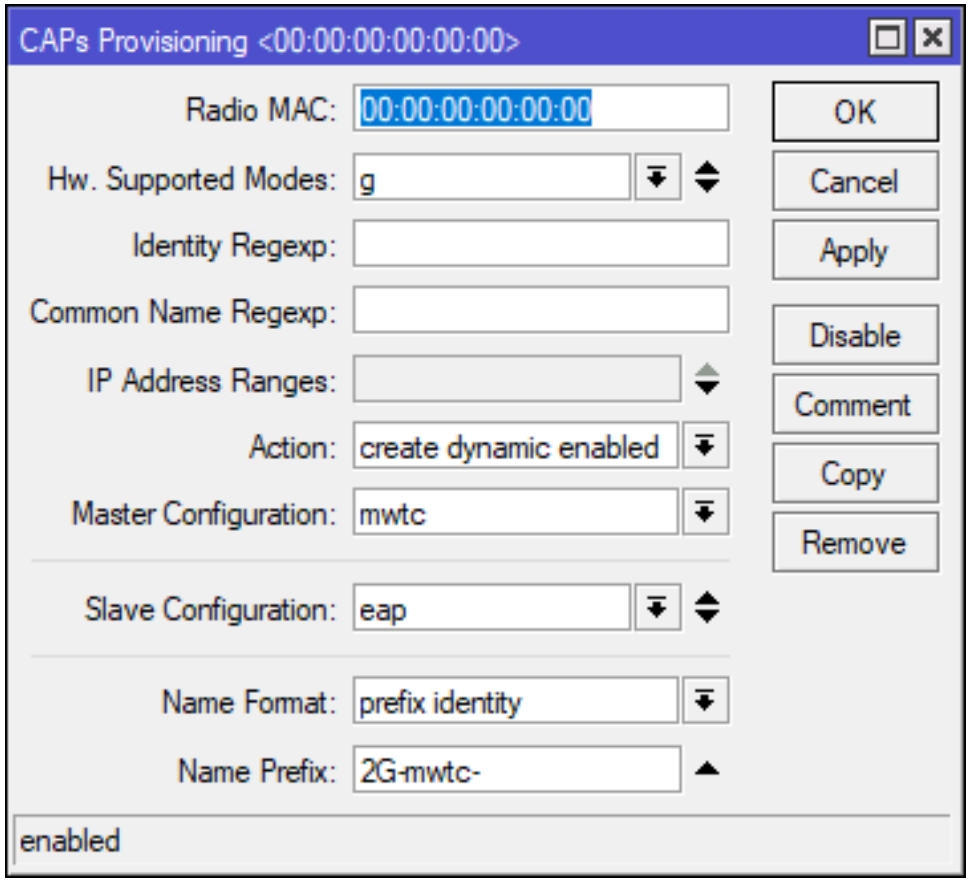
Konfiguracja CAPsMAN - channel



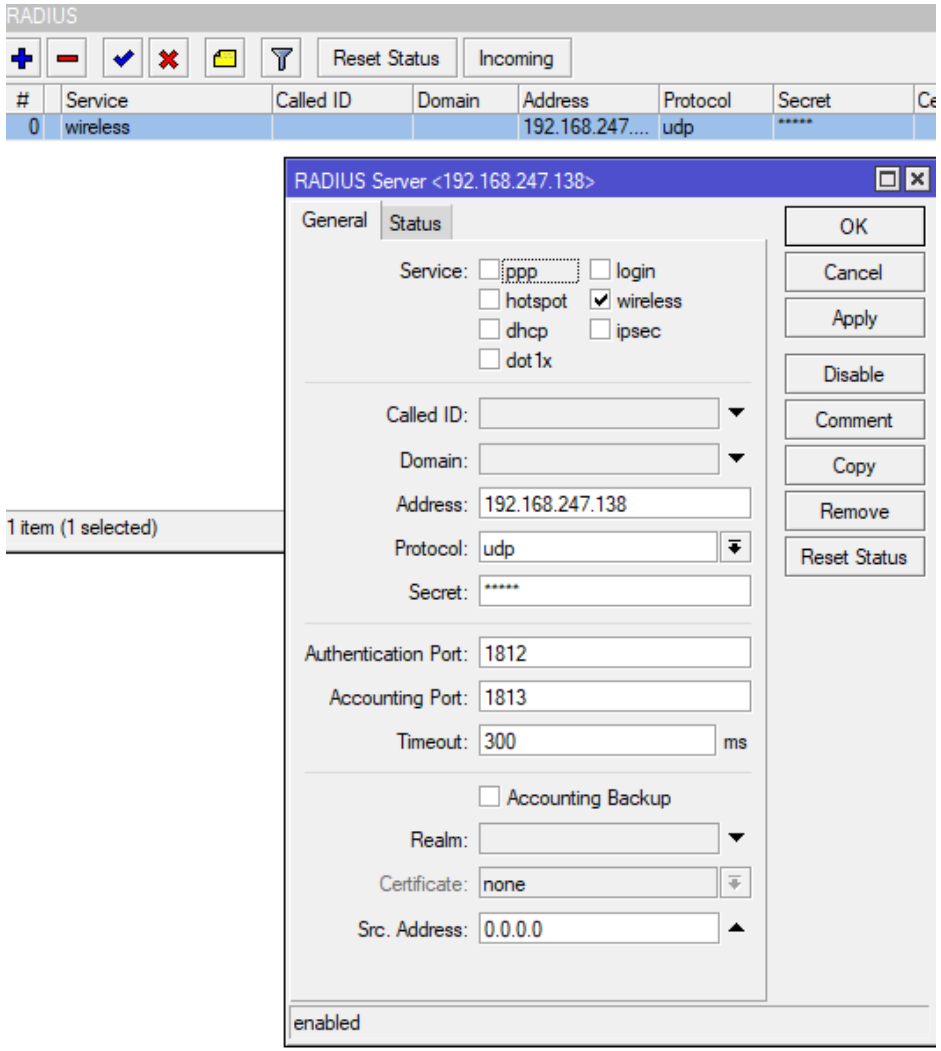
Konfiguracja CAPsMAN - configuration

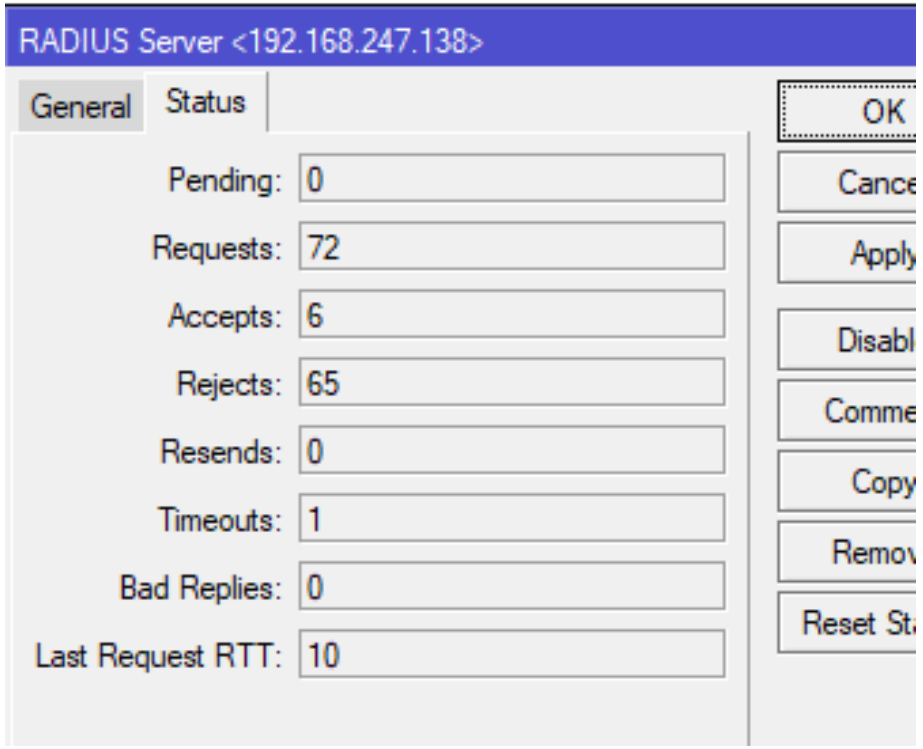


Konfiguracja CAPsMAN - provisioning

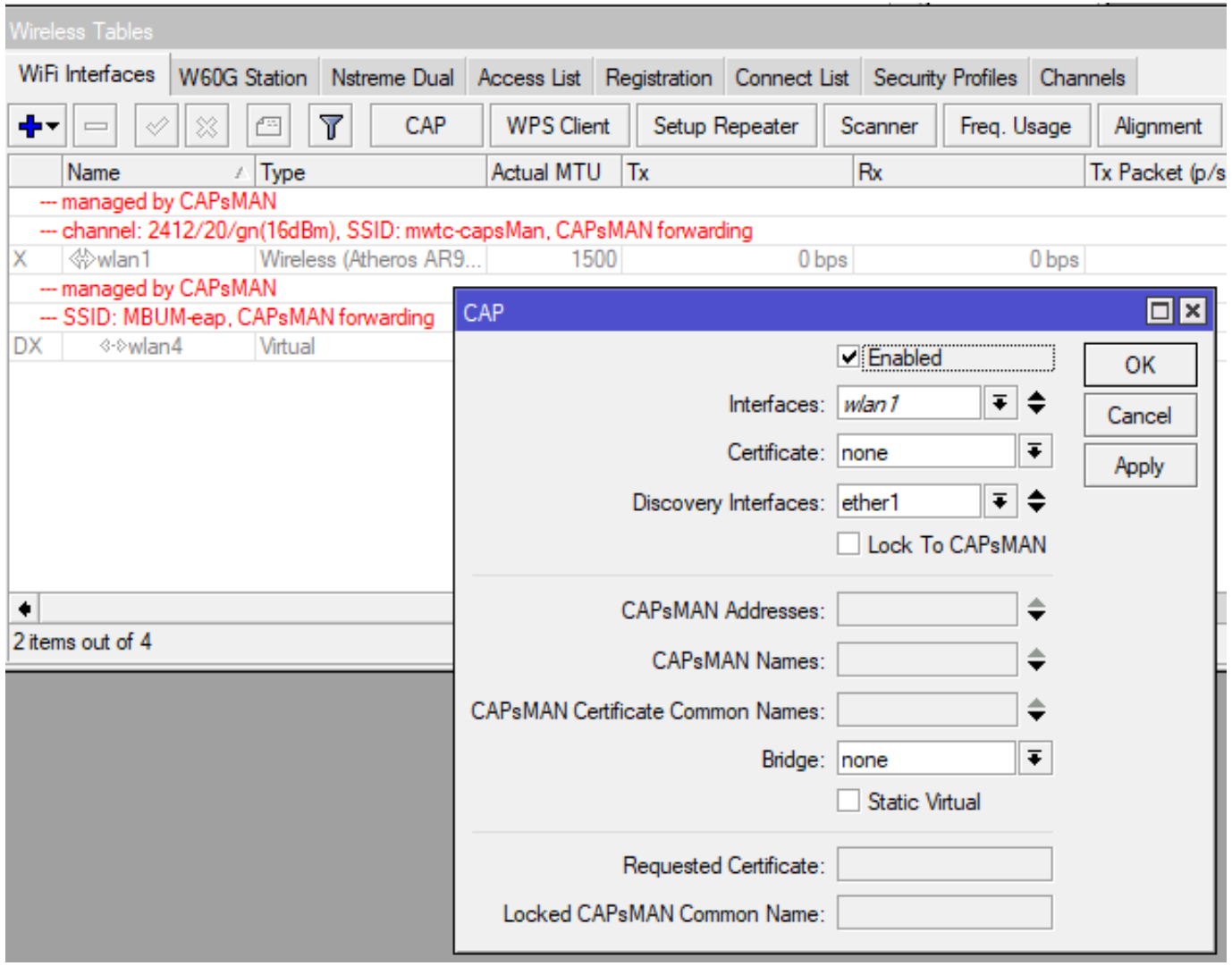


Konfiguracja CAPsMAN – radius Client

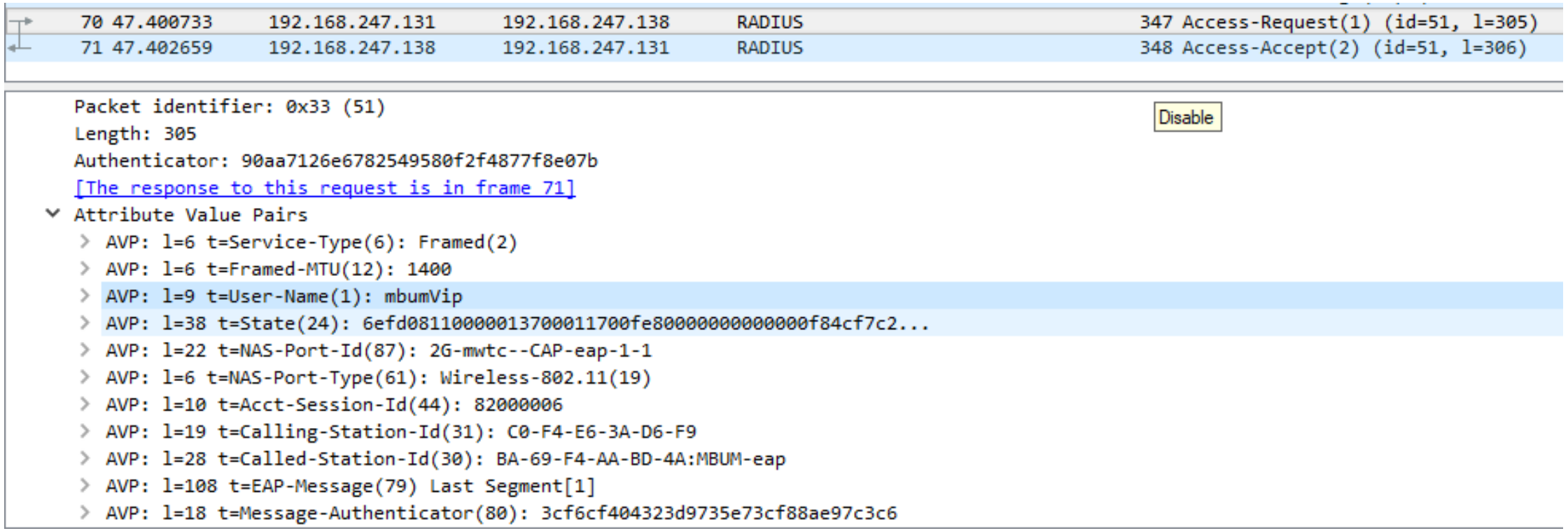




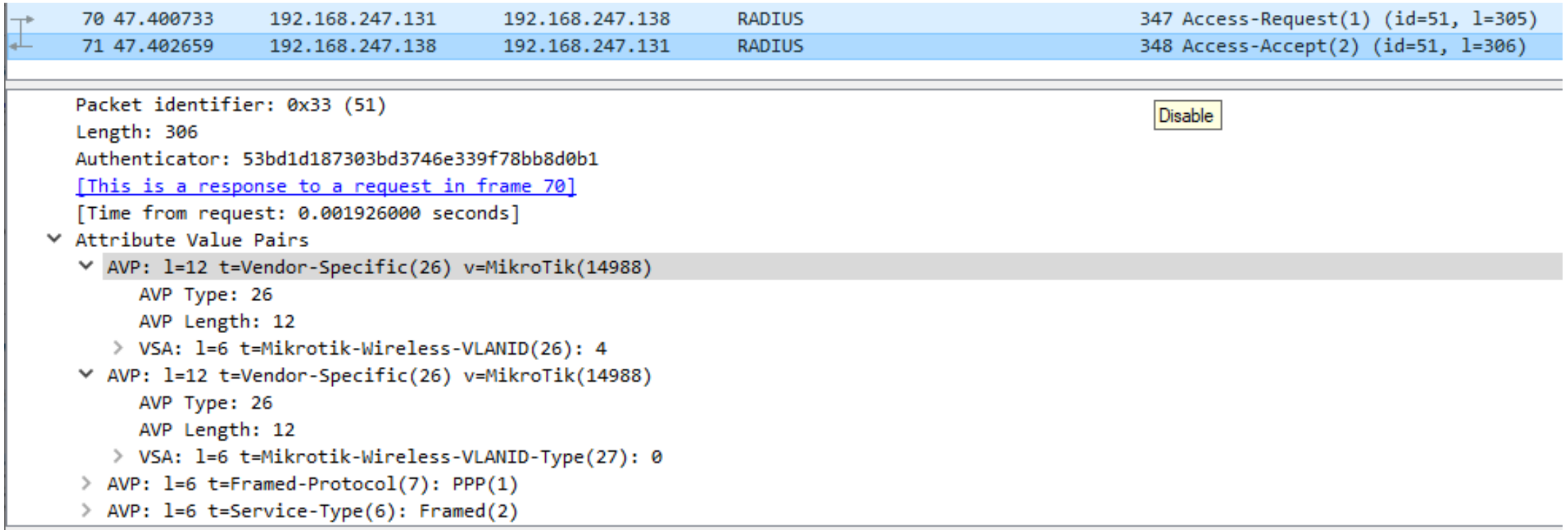
Konfiguracja CAP



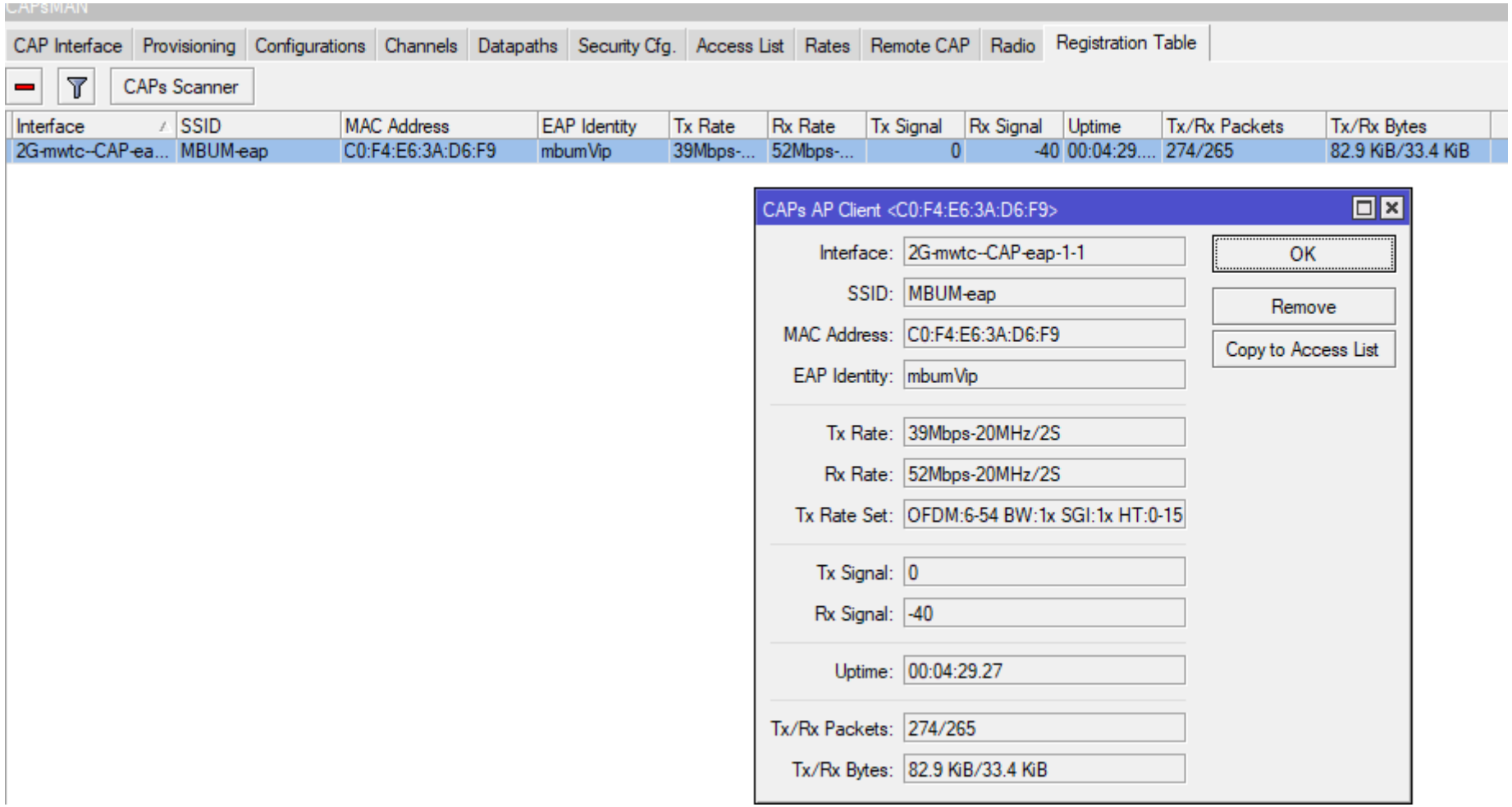
Szczegóły request Radius



Szczegóły response Radius



Podłączeni klienci



Gdzie szukać informacji o MikroTik i CAPsMAN

MikroTik Warsaw Training Center
https://mwtc.pl

Oficjalna dokumentacja nt. CAPsMAN

Grupa FaceBook MikroTikPolishGroup

MikroTikAcademy.pl

Pytania?

Piotr Wasyk
piotr@mwtc.pl