



MikroTik Warsaw  
Training Center

---

# MikroTik CAPsMAN WPA2 Enterprise z Microsoft AD

MBUM#4  
22 listopad 2019r

Piotr Wasyk



✓ **Największe centrum MikroTik szkoleniowe w Polsce**

- ✓ Warszawa/ Kraków / inne ...
- ✓ Pełna ścieżka certyfikacji MikroTik
- ✓ Szkolenia dofinansowane (nawet do 100%)

✓ **Projektowanie i wdrażanie sieci bezprzewodowych (indoor)**

✓ **Wdrożenia systemów monitorowania infrastruktury IT (*partner 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 zarządzanie 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 W/W/W)
- ✓ 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)

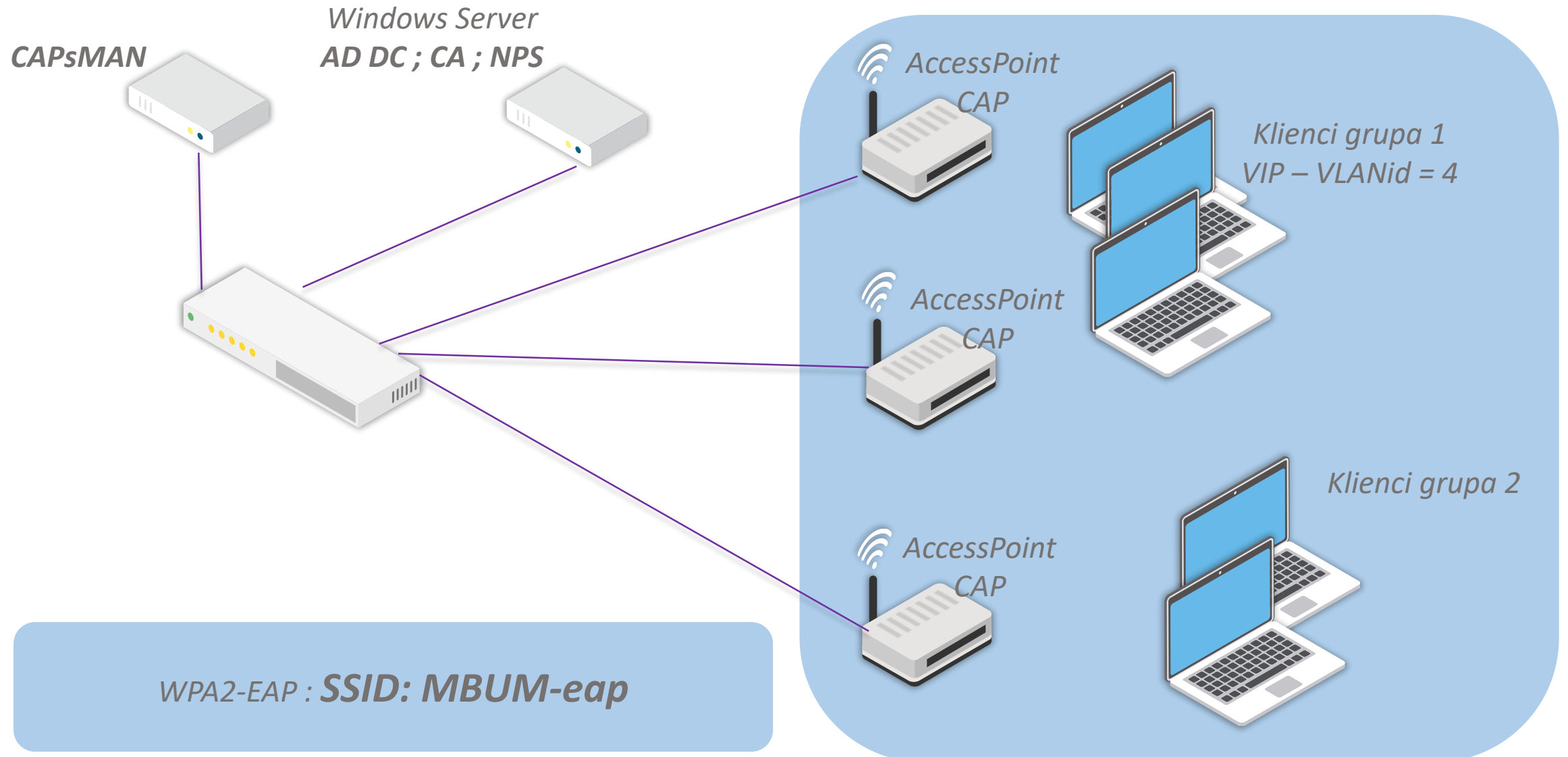
# Scenariusz praktyczny

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

Wymagania:

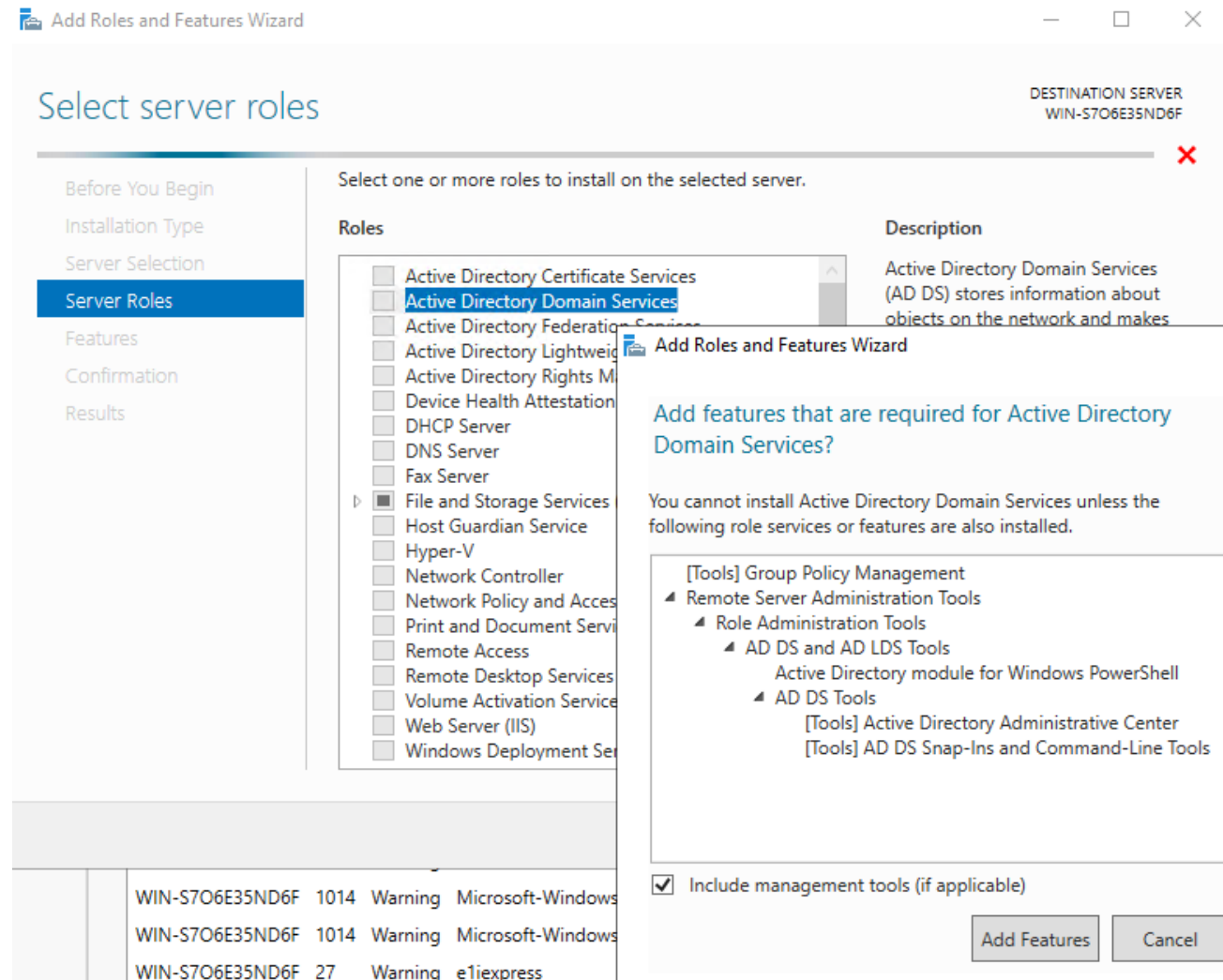
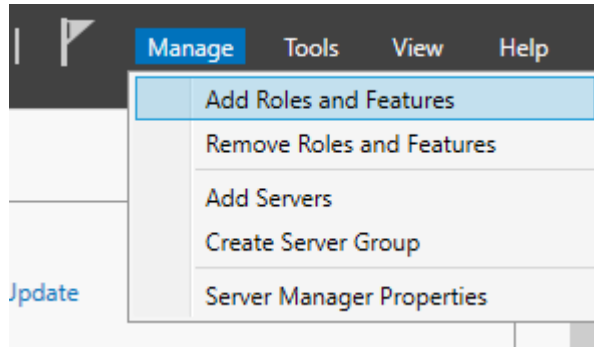
- Sieć WPA2-EAP dla pracowników – uwierzytelnienie do sieci za pomocą konta w usługach katalogowych (np. Microsoft Active Directory)
- W zależności od przynależności do odpowiedniej grupy AD użytkownik kierowany do odpowiedniego VLAN (grup > 20). Rozgłaszanie tylko jednego SSID

# Scenariusz praktyczny





# Instalacja Active Directory Services



# Instalacja Active Directory Services

Add Roles and Features Wizard

— □ ×

## Confirm installation selections

DESTINATION SERVER  
WIN-S7O6E35ND6F

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Domain Services  
Group Policy Management  
Remote Server Administration Tools  
    Role Administration Tools  
        AD DS and AD LDS Tools  
            Active Directory module for Windows PowerShell  
            AD DS Tools  
                Active Directory Administrative Center  
                AD DS Snap-Ins and Command-Line Tools

[Export configuration settings](#)  
[Specify an alternate source path](#)

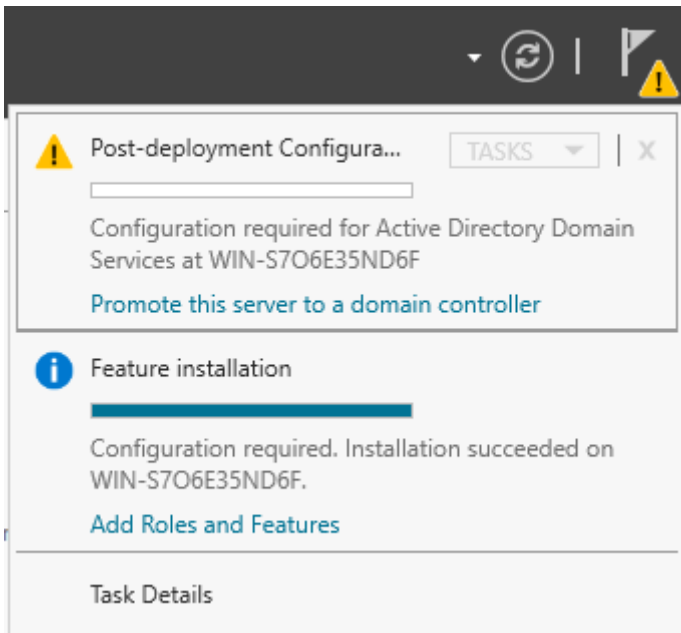
< Previous

Next >

Install

Cancel

# Promocja serwera do roli DC



## Active Directory Domain Services Configuration Wizard

### Deployment Configuration

#### Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

- ☐ Add a domain controller to an existing domain
- ☐ Add a new domain to an existing forest
- ☒ Add a new forest

Specify the domain information for this operation

Root domain name:

MWTC.local

TARGET  
WIN-S7O6E35ND6F

# Promocja serwera do roli DC

Domain Controller Options

TARGET SERVER  
WIN-S7O6E35ND6F

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: .....

Confirm password: .....

[More about domain controller options](#)

< Previous

Next >

Install

Cancel

# Promocja serwera do roli DC

 Active Directory Domain Services Configuration Wizard

## DNS Options

Deployment Configuration

Domain Controller Options

**DNS Options**

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify DNS delegation options

☐ Create DNS delegation

# Promocja serwera do roli DC

Active Directory Domain Services Configuration Wizard

— [

## Additional Options

TARGET  
WIN-S7O6I

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

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

The NetBIOS domain name:

# Promocja serwera do roli DC



Active Directory Domain Services Configuration Wizard

— [

## Paths

TARGET  
WIN-S7O6

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

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

Database folder:

C:\Windows\NTDS

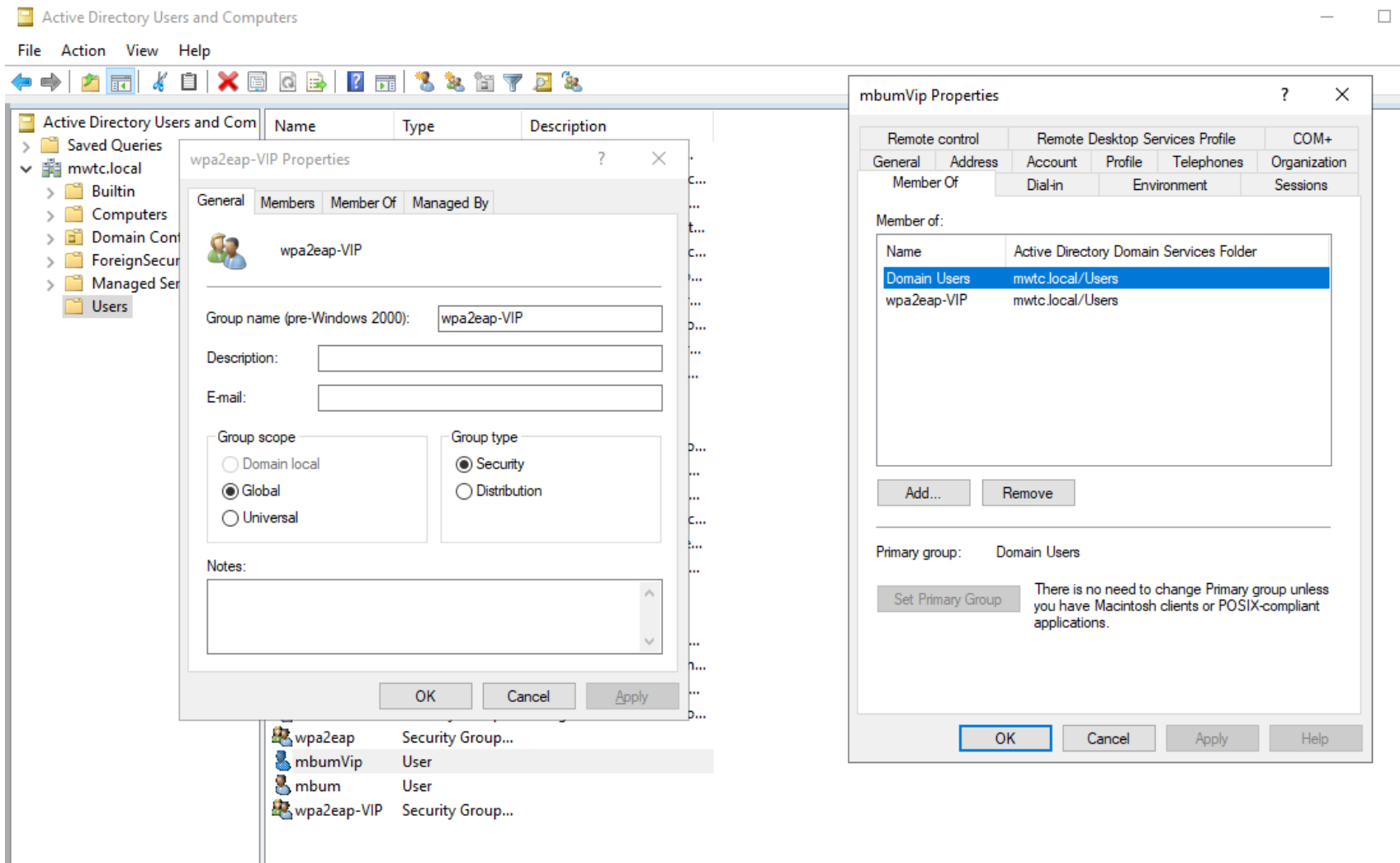
Log files folder:

C:\Windows\NTDS

SYSVOL folder:

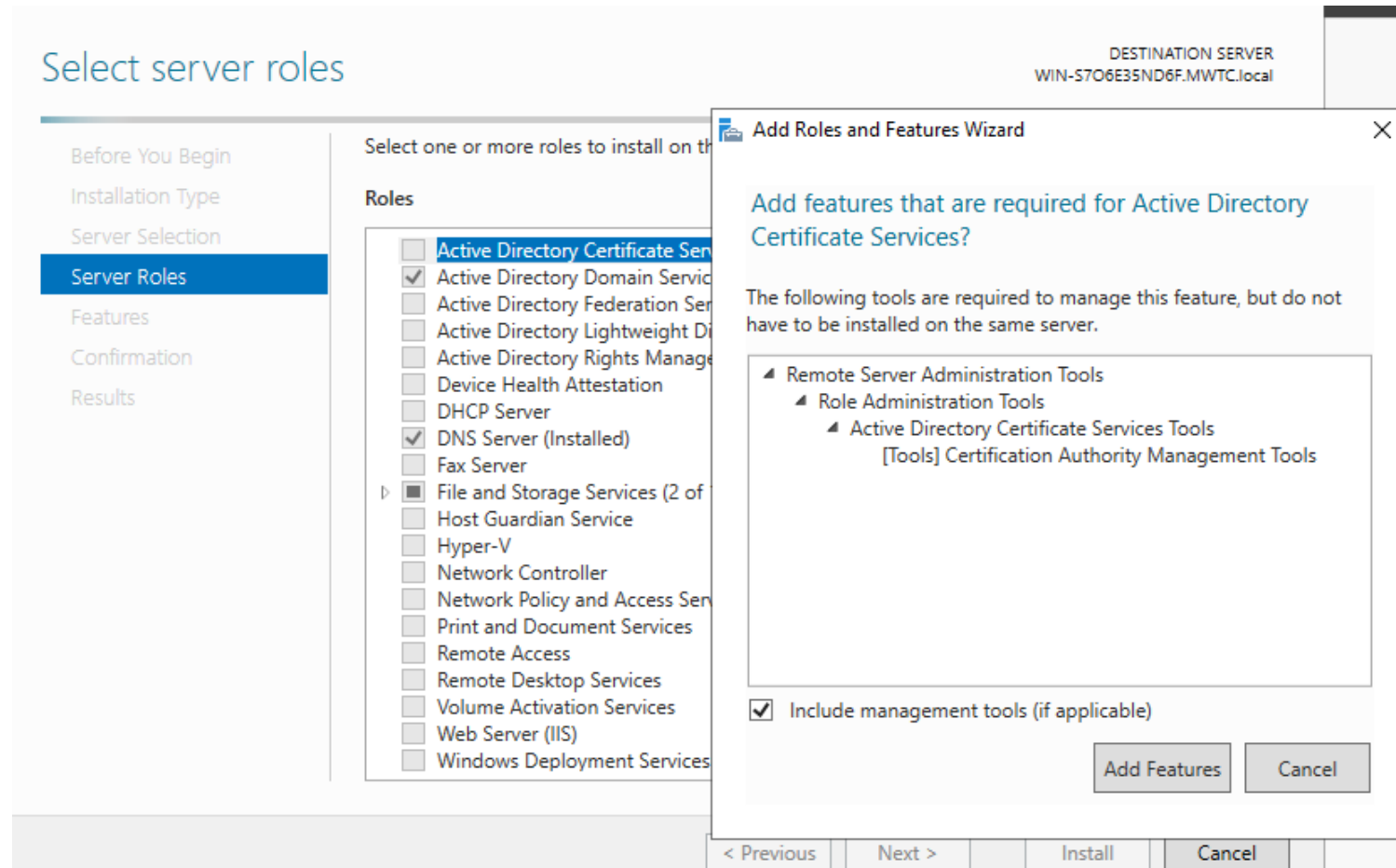
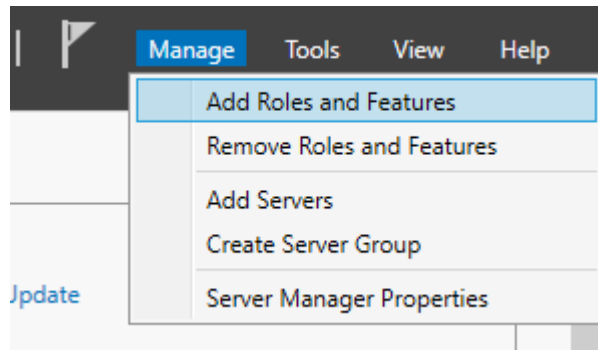
C:\Windows\SYSVOL

# Dodanie grup i użytkowników





# Instalacja Active Directory Certificate Services



# Instalacja Active Directory Certificates Services

Add Roles and Features Wizard

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

## Select role services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

**Role Services**

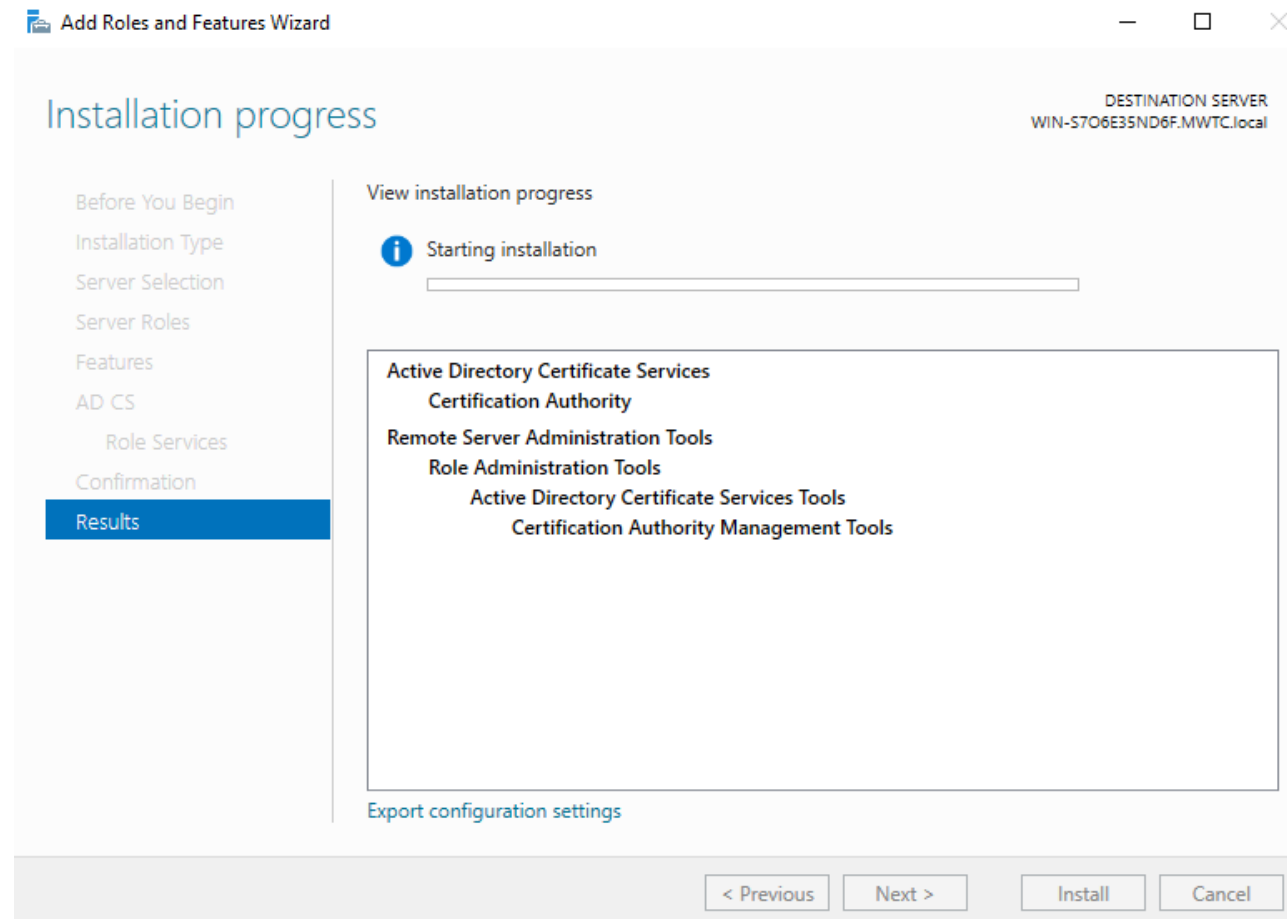
Confirmation

Results

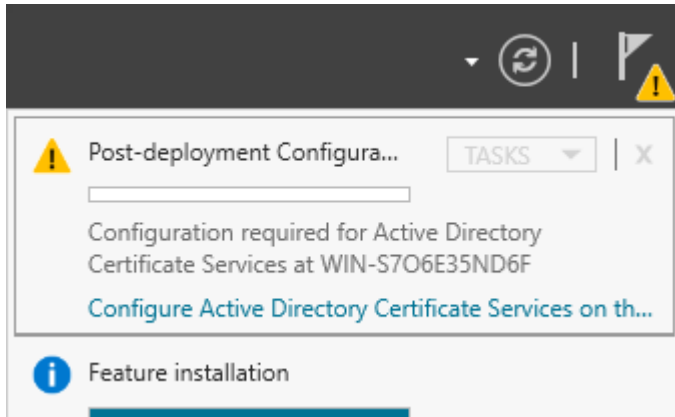
Select the role services to install for Active Directory Certificate Services

Role services	Description
<input checked="" type="checkbox"/> <b>Certification Authority</b>	Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
<input type="checkbox"/> Certificate Enrollment Policy Web Service	
<input type="checkbox"/> Certificate Enrollment Web Service	
<input type="checkbox"/> Certification Authority Web Enrollment	
<input type="checkbox"/> Network Device Enrollment Service	
<input type="checkbox"/> Online Responder	

# Instalacja Active Directory Certificates Services



# Konfiguracja Active Directory Certificates Services



Credentials

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

Credentials

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:


- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: MWTC2\Administrator

[More about AD CS Server Roles](#)

< Previous Next >

# Konfiguracja Active Directory Certificates Services

 AD CS Configuration

## Role Services

Credentials

**Role Services**

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

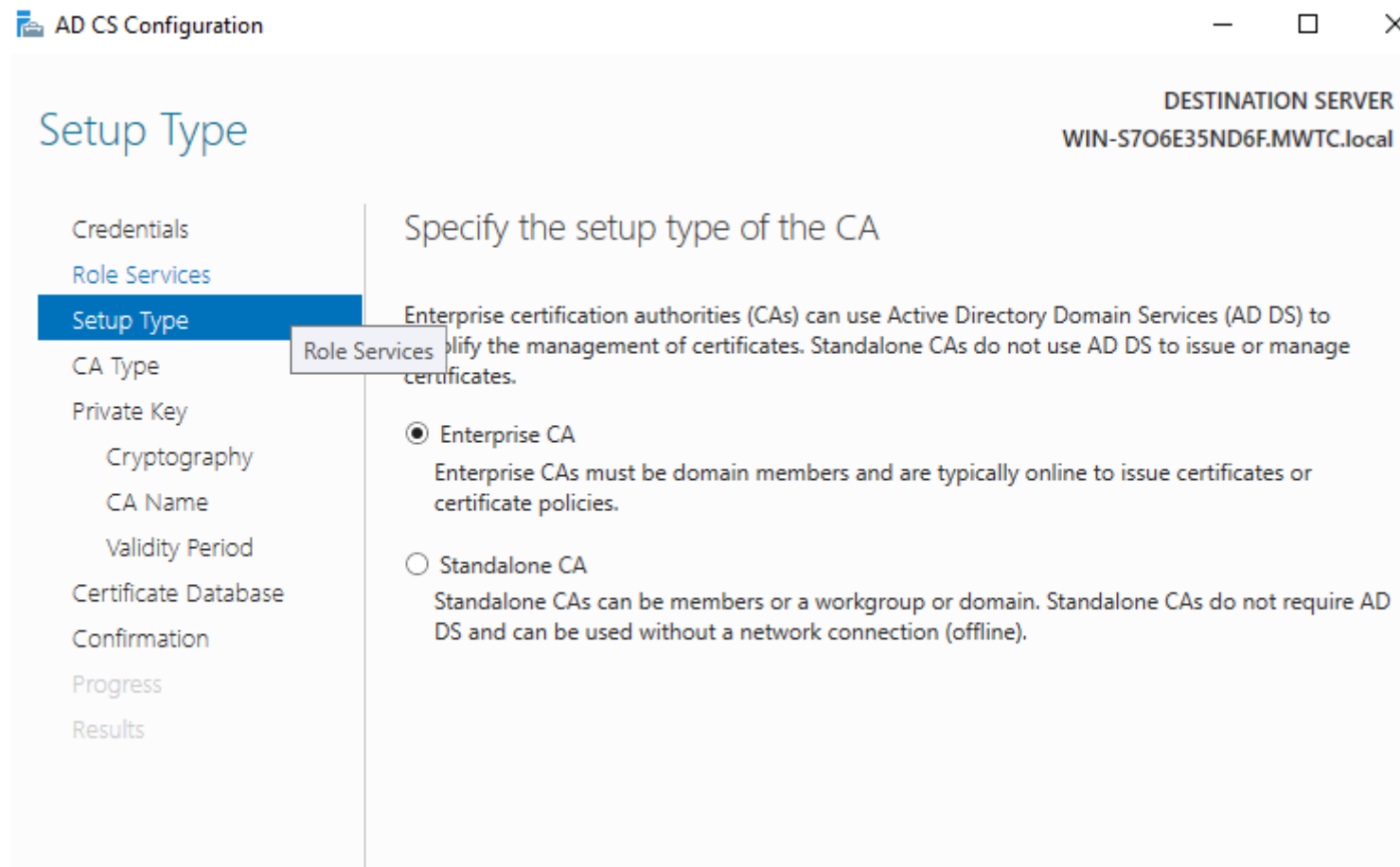
Progress

Results

### Select Role Services to configure

- ☒ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

# Konfiguracja Active Directory Certificates Services



The screenshot shows the 'AD CS Configuration' console window. The left-hand navigation pane lists the following steps: Credentials, Role Services, Setup Type (highlighted in blue), CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main pane is titled 'Specify the setup type of the CA'. In the top right corner, it displays 'DESTINATION SERVER' as 'WIN-S7O6E35ND6F.MWTC.local'. The main content area explains that Enterprise certification authorities (CAs) use Active Directory Domain Services (AD DS) to simplify certificate management, while Standalone CAs do not. Two radio buttons are present: 'Enterprise CA' (which is selected) and 'Standalone CA'. A tooltip is visible over the 'Role Services' link in the left pane.

AD CS Configuration

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

## Setup Type

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

☒ Enterprise CA  
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

☐ Standalone CA  
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

# Konfiguracja Active Directory Certificates Services

AD CS Configuration

— □ >

## CA Type

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

### Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

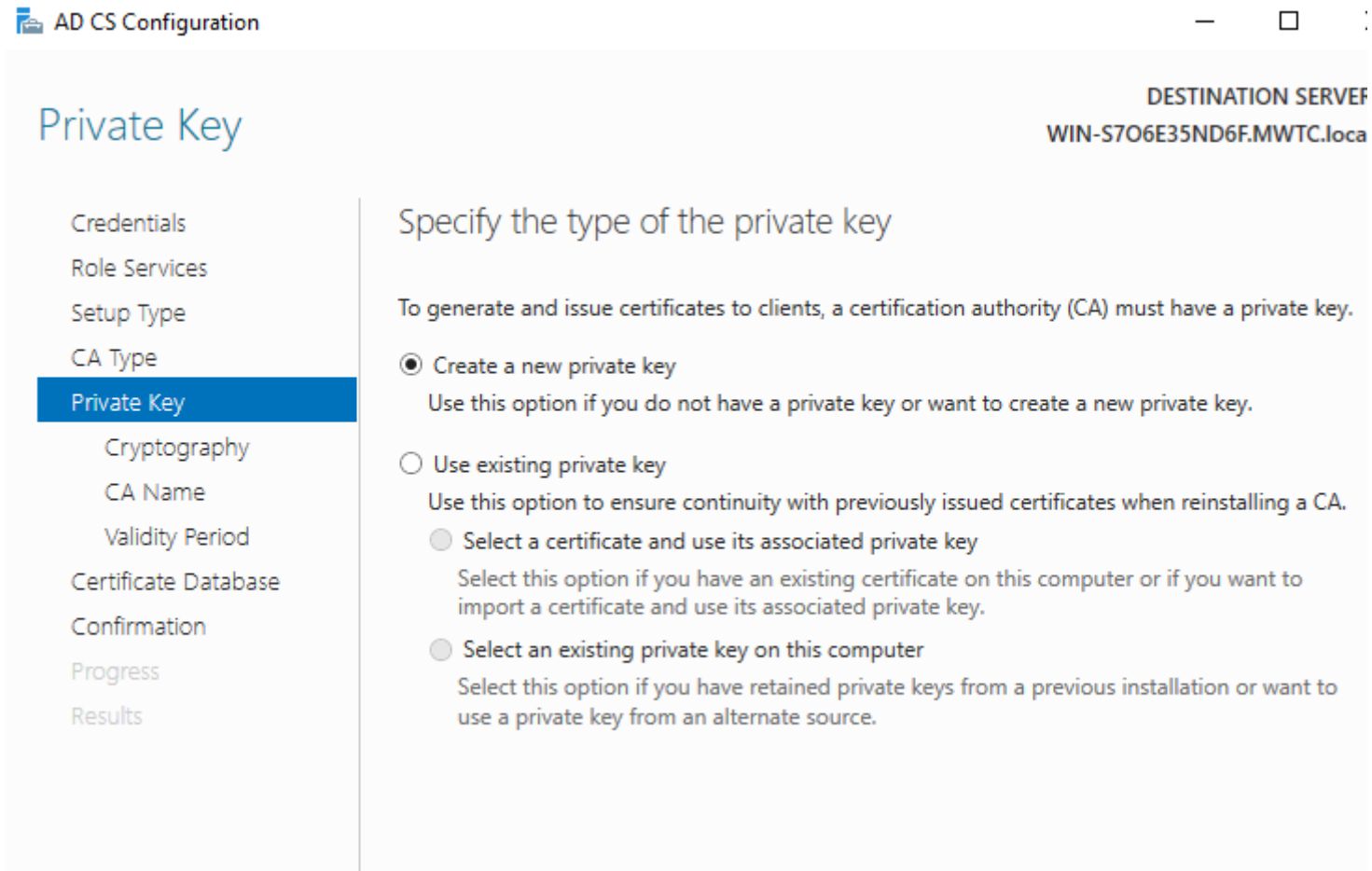
☒ Root CA

Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ Subordinate CA

Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

# Konfiguracja Active Directory Certificates Services



AD CS Configuration

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

## Private Key

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

### Specify the type of the private key

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

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



# Konfiguracja Active Directory Certificates Services

## Cryptography for CA

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

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

### Specify the cryptographic options

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

Key length: 2048

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

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

[More about Cryptography](#)

# Konfiguracja Active Directory Certificates Services

## CA Name

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

**CA Name**

Validity Period

Certificate Database

Confirmation

Progress

Results

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

Specify the name of the CA

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

Common name for this CA:

Distinguished name suffix:

Preview of distinguished name:

# Konfiguracja Active Directory Certificates Services

## Validity Period

DESTINATION SERVER

WIN-S7O6E35ND6F.MWTC.local

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

### Specify the validity period

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

 Years

CA expiration Date: 21.11.2039 17:59:00

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

[More about Validity Period](#)

# Konfiguracja Active Directory Certificates Services

CA Database

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

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

### Specify the database locations

Certificate database location:

Certificate database log location:

# Konfiguracja Active Directory Certificates Services

## Confirmation

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

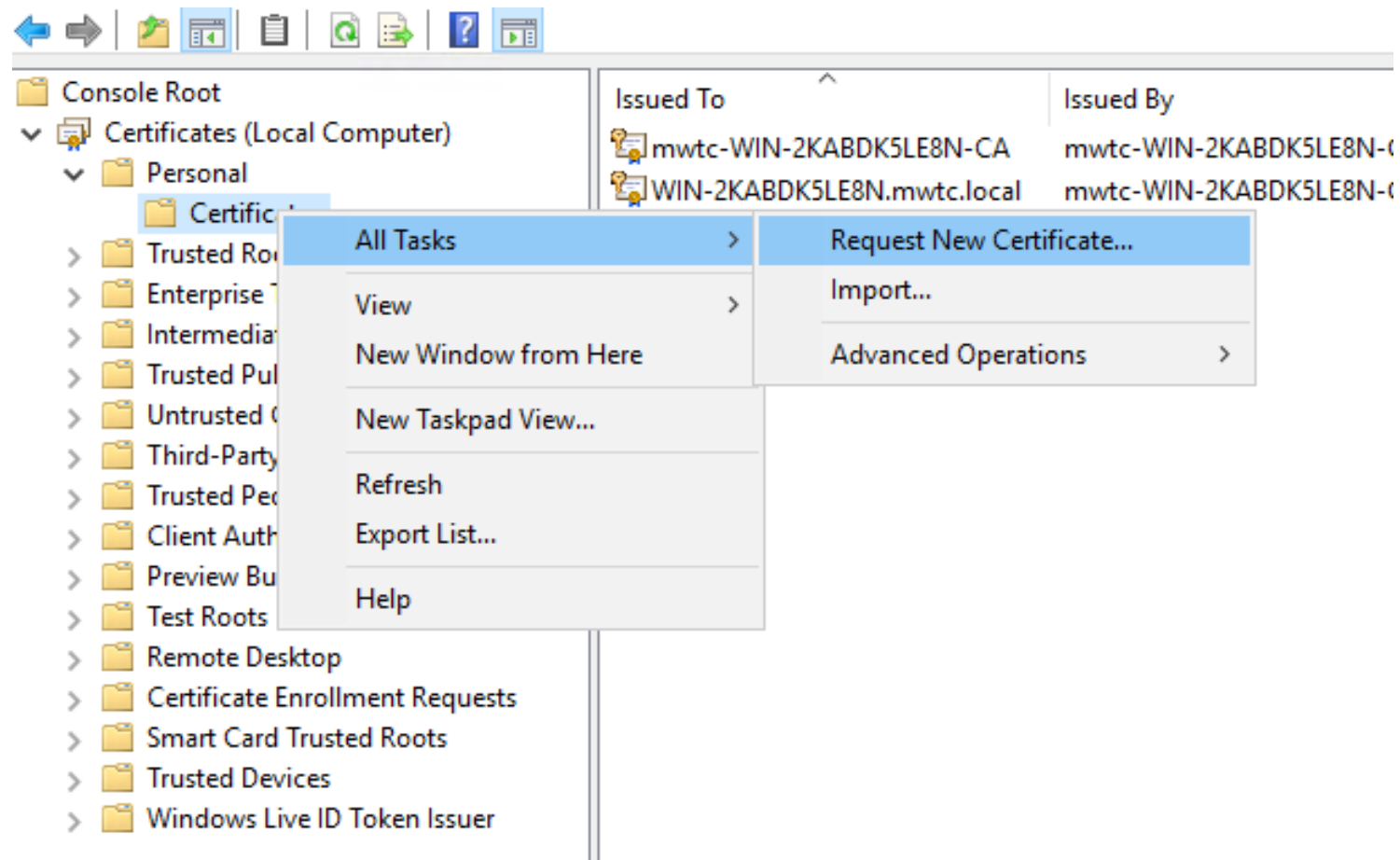
To configure the following roles, role services, or features, click Configure.

### ⤴ Active Directory Certificate Services


#### Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	21.11.2039 17:59:00
Distinguished Name:	CN=MBUM-CA,DC=MWTC,DC=local
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

# Konfiguracja Active Directory Certificates Services



# Konfiguracja Active Directory Certificates Services

 Certificate Enrollment

## Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

### Configured by your administrator

Active Directory Enrollment Policy



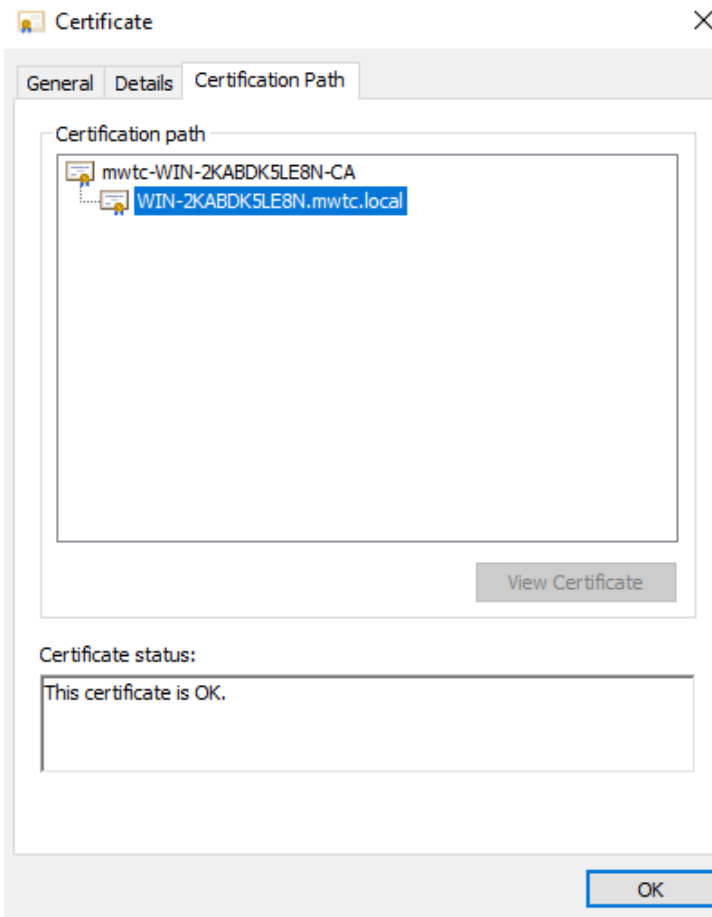
### Configured by you

[Add New](#)

Next

Cancel

# Konfiguracja Active Directory Certificates Services





# Instalacja Network Policy Server

The screenshot displays the 'Add Roles and Features Wizard' in Windows Server. The main window is at the 'Select server roles' step, showing a list of roles for the destination server 'WIN-S7O6E35ND6F.MWTC.local'. The 'Network Policy and Access Services' role is highlighted. A secondary window titled 'Add Roles and Features Wizard' is open, asking 'Add features that are required for Network Policy and Access Services?'. It lists 'Remote Server Administration Tools' and 'Role Administration Tools' as required, with a checkbox for 'Include management tools (if applicable)' which is checked.

**Manage** Tools View Help

- Add Roles and Features
- Remove Roles and Features
- Add Servers
- Create Server Group
- Server Manager Properties

Update

**Add Roles and Features Wizard**

Select server roles

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

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

Roles	Description
<input type="checkbox"/> Active Directory Certificate Services (AD CS)	
<input checked="" type="checkbox"/> Active Directory Domain Services (AD DS)	
<input type="checkbox"/> Active Directory Federation Services (AD FS)	
<input type="checkbox"/> Active Directory Lightweight Directory Services (AD LDS)	
<input type="checkbox"/> Active Directory Rights Management Services (AD RMS)	
<input type="checkbox"/> Device Health Attestation	
<input type="checkbox"/> DHCP Server	
<input checked="" type="checkbox"/> DNS Server (Installed)	
<input type="checkbox"/> Fax Server	
<input type="checkbox"/> File and Storage Services (2 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Controller	
<input checked="" type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	

**Add Roles and Features Wizard**

Add features that are required for Network Policy and Access Services?

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

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] Network Policy and Access Services Tools

☒ Include management tools (if applicable)

# Instalacja Network Policy Server

## Confirm installation selections

DESTINATION SERVER  
WIN-S7O6E35ND6F.MWTC.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Network Policy and Acces...

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

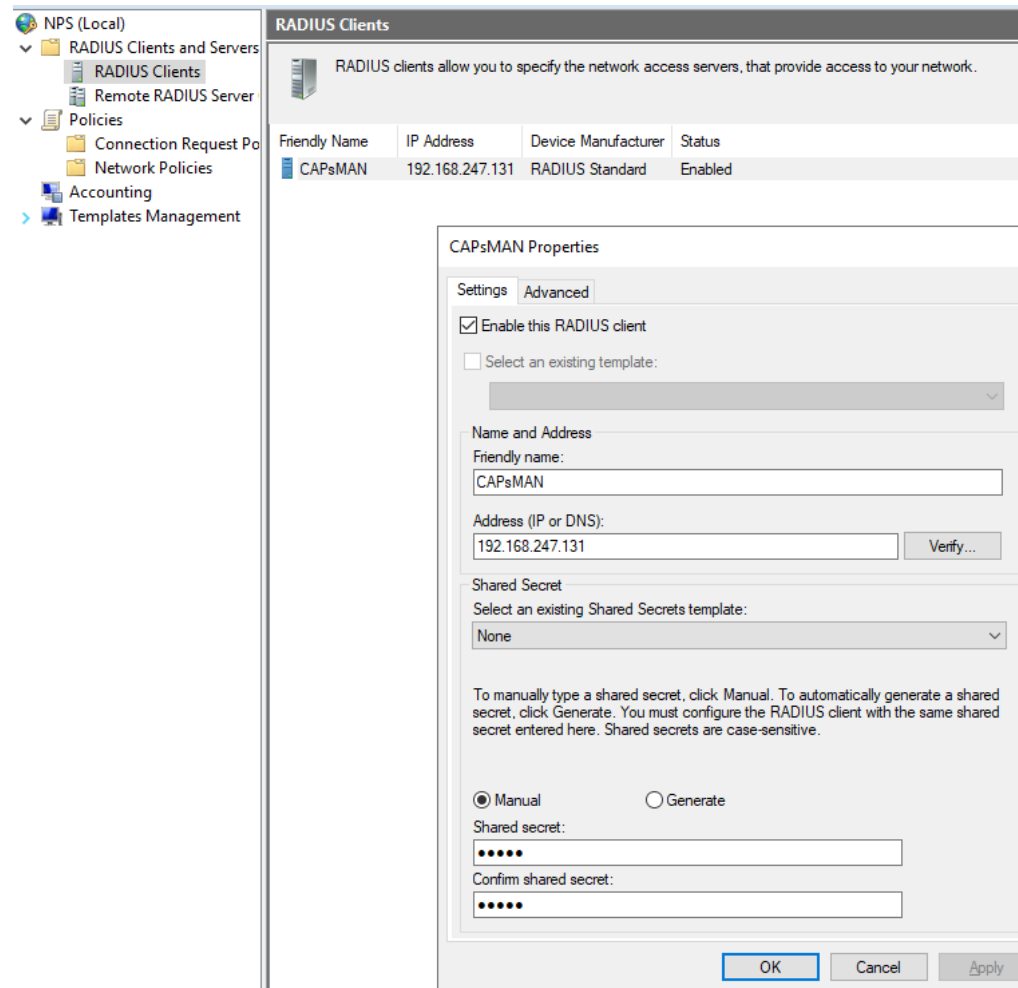
Network Policy and Access Services

Remote Server Administration Tools

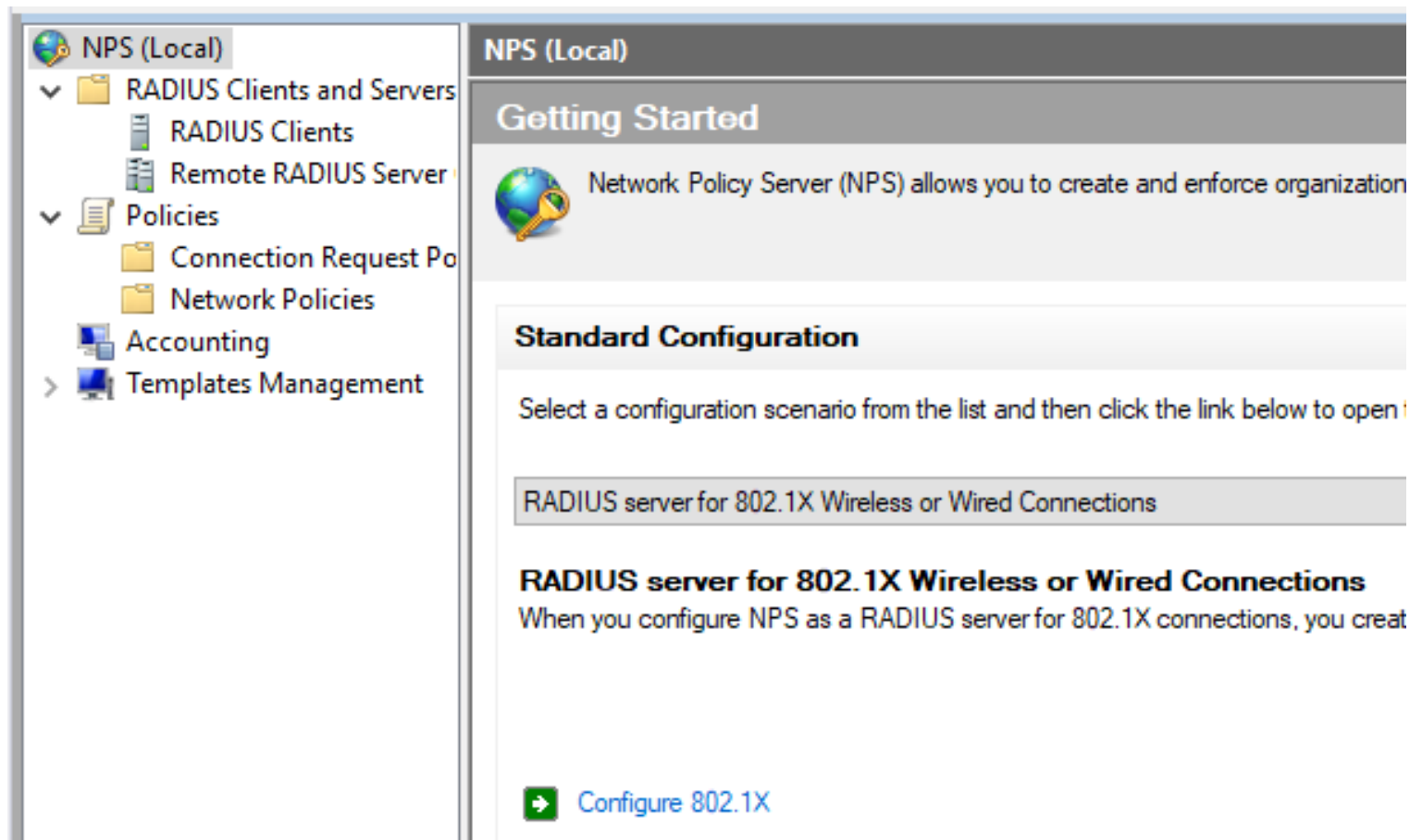
Role Administration Tools

Network Policy and Access Services Tools

# Konfiguracja NPS – Radius Clients



# Konfiguracja NPS – Polityka 802.1x



# Konfiguracja NPS – Polityka 802.1X

eap Properties

Overview Conditions Constraints Settings

Policy name: eap

**Policy State**  
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

**Access Permission**  
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

☒ Grant access. Grant access if the connection request matches this policy.

☐ Deny access. Deny access if the connection request matches this policy.

☒ Ignore user account dial-in properties.  
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

**Network connection method**  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:  
Unspecified

☐ Vendor specific:  
10

OK Cancel

# Konfiguracja NPS – Polityka 802.1x

eap Properties

Overview Conditions Constraints Settings

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	MWTC\wpa2eap

eap Properties

Overview Conditions Constraints Settings

Configure the constraints for this network policy.  
If all constraints are not matched by the connection request, network access is denied.

Constraints:

**Constraints**

- Authentication Methods
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Protected EAP (PEAP) Move

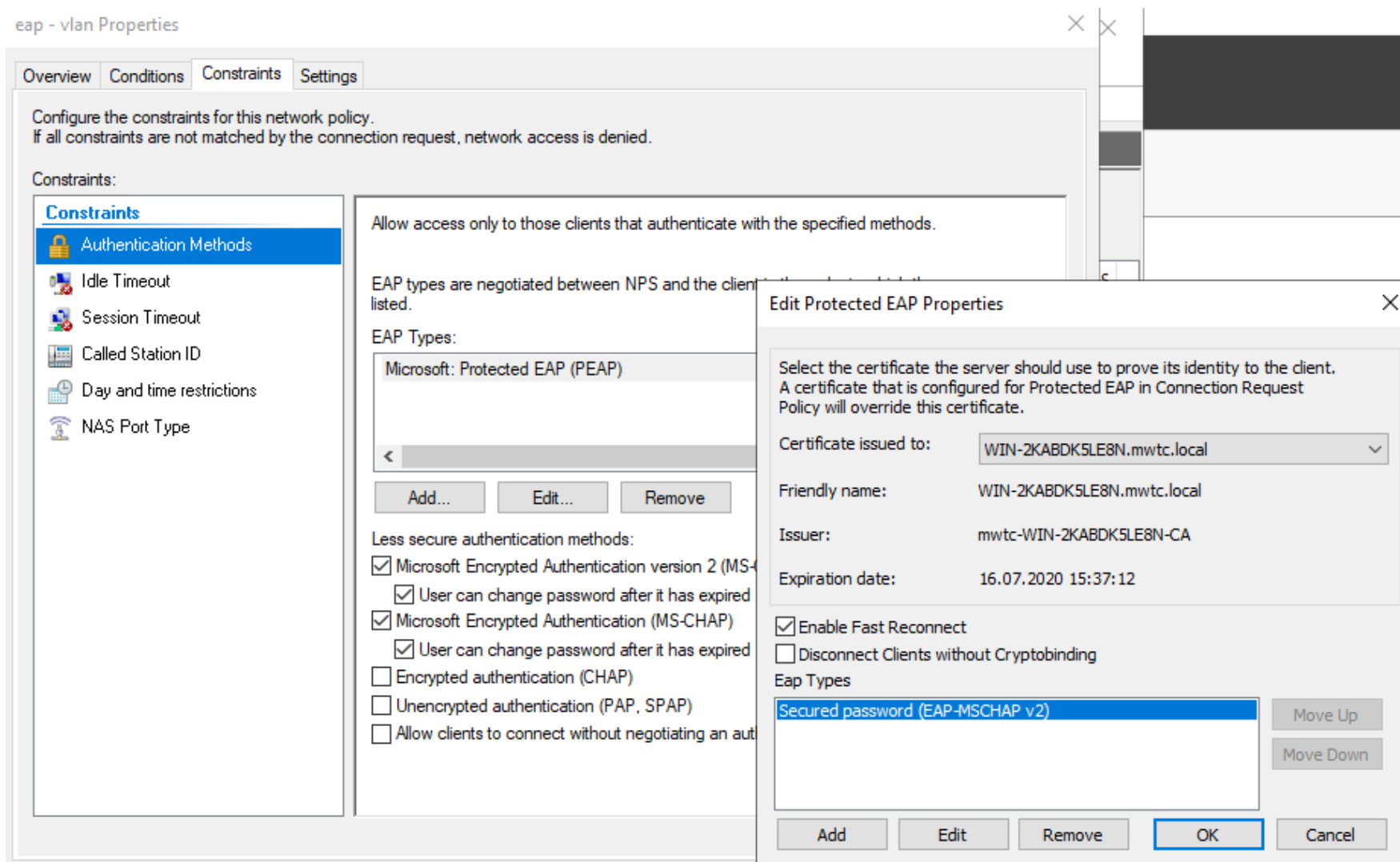
< > Move

Add... Edit... Remove

Less secure authentication methods:

- ☒ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - ☒ User can change password after it has expired
- ☒ Microsoft Encrypted Authentication (MS-CHAP)
  - ☒ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method

# Konfiguracja NPS – Polityka 802.1x



# Konfiguracja NPS – Polityka 802.1x

eap Properties

Overview

Conditions


Constraints

Settings

Configure the settings for this network policy.  
If conditions and constraints match the connection request and the policy grants access, settings are appl


Settings:


**RADIUS Attributes**


 Standard


☒ Vendor Specific

**Routing and Remote Access**

 Multilink and Bandwidth Allocation Protocol (BAP)

 IP Filters

 Encryption

 IP Settings

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

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add...

Edit...

Remove



# Konfiguracja NPS – Polityka 802.1x (z VLAN)

New CAPs Datapath Configuration

Name: datapath1

MTU:

L2 MTU:

ARP:

Bridge:

Bridge Cost:

Bridge Horizon:

Local Forwarding:

Client To Client Forwarding:

VLAN Mode: use tag

VLAN ID: 400

Interface List:

OK

Cancel

Apply

Comment

Copy

Remove

[https://wiki.mikrotik.com/wiki/Manual:RADIUS Client](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)

eap - vlan Properties

Overview

Conditions


Constraints

Settings

Configure the settings for this network policy.  
If conditions and constraints match the connection request and the policy grants access, settings are applied.


Settings:


**RADIUS Attributes**


 Standard


☒ **Vendor Specific**

**Routing and Remote Access**

 Multilink and Bandwidth Allocation Protocol (BAP)

 IP Filters

 Encryption

 IP Settings

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

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	4, 0

Add...

Edit...

Remove

# Konfiguracja NPS – Polityka 802.1x (z VLAN)

Attribute Information ✕

Attribute name:  
Vendor-Specific

Attribute number:  
26

Attribute format:  
OctetString

Attribute values:

Vendor	Value
Vendor Code: 14988	4
Vendor Code: 14988	0

Add...

Edit...

Remove

Move Up

Move Down

OK

Cancel

# Konfiguracja NPS – Polityka 802.1x (z VLAN)

The image shows two overlapping windows from the Network Policy Server (NPS) configuration tool. The background window is titled "Vendor-Specific Attribute Information" and contains the following fields:

- Attribute name: Vendor Specific
- Specify network access server vendor:
  - ☐ Select from list: RADIUS Standard
  - ☒ Enter Vendor Code: 14988
- Specify whether the attribute conforms to vendor specific attributes:
  - ☒ Yes. It conforms
  - ☐ No. It does not conform
- Configure Attribute... button

The foreground window is titled "Configure VSA (RFC Compliant)" and contains the following fields:

- Vendor-assigned attribute number: 26
- Attribute format: Decimal
- Attribute value: 4
- OK button
- Cancel button

# Konfiguracja NPS – Polityka 802.1x (z VLAN)

Vendor-Specific Attribute Information

Attribute name:  
Vendor Specific

Specify network access server vendor.

☐ Select from list: RADIUS Standard

☒ Enter Vendor Code: 14988

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

☒ Yes. It conforms

☐ No. It does not conform

Configure Attribute...

Configure VSA (RFC Compliant)

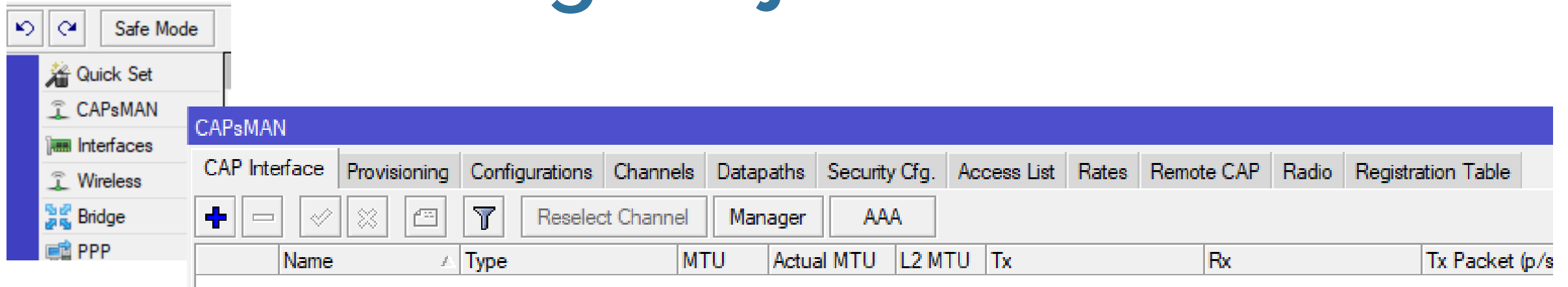
Vendor-assigned attribute number:  
27

Attribute format:  
Decimal

Attribute value:  
0

OK Cancel

# 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 security Cfg
- ✓ **Registration Table** – informacje o połączonych klientach

# Konfiguracja CAPsMAN

CAPs Security Configuration <wpa2-eap-nps>

Name:

Authentication Type: ☐ WPA PSK ☐ WPA2 PSK ☐ WPA EAP ☒ WPA2 EAP ▲

Encryption: ☒ aes ccm ☒ tkip ▲

Group Encryption:  ▼ ▲

Group Key Update:  ▼

Passphrase:  ▼

Disable PMKID:  ▼

EAP Methods:  ▼ ▲

EAP Radius Accounting:  ▼

TLS Mode:  ▼

TLS Certificate:  ▼

OK  
Cancel  
Apply  
Comment  
Copy  
Remove

# Konfiguracja CAPsMAN - bridge

Bridge						
Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB						
+ - ✓ ✗ [icon] [icon] Settings						
	Name	Type	L2 MTU	Tx	Rx	
R	↕↕capsman-eap	Bridge	1600		0 bps	
R	↕↕capsman-mwtc	Bridge	1600		0 bps	

Bridge								
Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB								
+ - ✓ ✗ [icon] [icon] Fit								
#		Interface	Bridge	Horizon	Trusted	Priority (h...	Path Cost	Role
0	DI	↕↕2G-mwtc-CAP...	capsman-mwtc		no	80	10	disabled port
1	DI	↕↕2G-mwtc-CAP...	capsman-eap		no	80	10	disabled port

New CAPs Datapath Configuration

Name:

MTU:

L2 MTU:

ARP:

Bridge:

Bridge Cost:

Bridge Horizon:

Local Forwarding:

Client To Client Forwarding:

VLAN Mode:

VLAN ID:

Interface List:

OK

Cancel

Apply

Comment








Copy

Remove



# Konfiguracja - VLAN

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
	     								
	Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx		
R	 vlan4	VLAN	1500	1500	1596		0 bps		0 bps

Interface <vlan4>

General Loop Protect Status Traffic

Name:


Type:


MTU:

Actual MTU:


L2 MTU:

MAC Address:

ARP:  

ARP Timeout:  

VLAN ID:

Interface:  

☐ Use Service Tag

OK Cancel Apply Disable Comment Copy Remove Torch

# Konfiguracja – adresacja IP/ dhcp-server ...

Address List				
<div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div>Find</div></div>				
	Address	Network	Interface	
	10.4.4.1/24	10.4.4.0	capsman-eap	
	10.33.33.1/24	10.33.33.0	vlan4	
	192.168.3.5/24	192.168.3.0	ether2	
	192.168.77.1/...	192.168.77.0	capsman-mwtc	
D	192.168.247.1...	192.168.247.0	ether1	

DHCP Server

DHCP

Networks

Leases

Options

Option Sets

Alerts

DHCP Config

DHCP Setup


	Name	Interface	Relay	Lease Time	Address Pool	Add AR...	
	dhcp1	capsman-eap		00:10:00	dhcp_pool0	no	
	dhcp2	vlan4		00:10:00	dhcp_pool1	no	
	dhcp3	capsman-mwtc		00:10:00	dhcp_pool3	no	


5 items



# Konfiguracja CAPsMAN - channel



CAPs Channel <ch1>



Name:


Frequency:  


Secondary Frequency:  


Control Channel Width:   


Band:   

Extension Channel:   

Tx Power:  

Save Selected:  

Reselect Interval:  

Skip DFS Channels:  

OK  
Cancel  
Apply  
Comment  
Copy  
Remove

# Konfiguracja CAPsMAN - configuration

New CAPs Configuration

Wireless Channel Rates Datapath Security

Name: eap

Mode: ap

SSID: MBUM-eap

Hide SSID:

Load Balancing Group:

Distance: indoors km

Hw. Retries:

Hw. Protection Mode:

Frame Lifetime:

Disconnect Timeout:

Keepalive Frames:

Country: poland

Installation: indoor

Max Station Count:

Multicast Helper:

HT Tx Chains:

HT Rx Chains:

HT Guard Interval:

OK

Cancel

Apply

Comment

Copy

Remove

# Konfiguracja CAPsMAN - provisioning

CAPs Provisioning <00:00:00:00:00:00>

Radio MAC: 00:00:00:00:00:00

Hw. Supported Modes: g

Identity Regexp:

Common Name Regexp:

IP Address Ranges:

Action: create dynamic enabled

Master Configuration: mwtc

Slave Configuration: eap

Name Format: prefix identity

Name Prefix: 2G-mwtc-

enabled

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove

# Konfiguracja CAPsMAN – radius Client

RADIUS

+ - ✓ ✗ 📁 🔍 Reset Status Incoming

#	Service	Called ID	Domain	Address	Protocol	Secret	Ce
0	wireless			192.168.247....	udp	*****	

1 item (1 selected)

RADIUS Server <192.168.247.138>

General Status OK Cancel Apply Disable Comment Copy Remove Reset Status

Service: ☐ ppp ☐ login  
☐ hotspot ☒ wireless  
☐ dhcp ☐ ipsec  
☐ dot1x

Called ID:

Domain:

Address: 192.168.247.138

Protocol: udp

Secret: \*\*\*\*\*

Authentication Port: 1812

Accounting Port: 1813

Timeout: 300 ms

☐ Accounting Backup

Realm:

Certificate: none

Src. Address: 0.0.0.0

enabled

RADIUS Server <192.168.247.138>

General Status OK Cancel Apply Disable Comment Copy Remove Reset Status

Pending: 0

Requests: 72

Accepts: 6

Rejects: 65

Resends: 0

Timeouts: 1

Bad Replies: 0

Last Request RTT: 10

# Konfiguracja CAP

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profiles Channels

+ - ✓ ✕ [Icon] [Icon] CAP WPS Client Setup Repeater Scanner Freq. Usage Alignment

	Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/s)
	--- managed by CAPsMAN					
	--- channel: 2412/20/gn(16dBm), SSID: mwtc-capsMan, CAPsMAN forwarding					
X	wlan1	Wireless (Atheros AR9...	1500	0 bps	0 bps	
	--- managed by CAPsMAN					
	--- SSID: MBUM-eap, CAPsMAN forwarding					
DX	wlan4	Virtual				

2 items out of 4

☒ Enabled

Interfaces: wlan1

Certificate: none

Discovery Interfaces: ether1

☐ Lock To CAPsMAN

CAPsMAN Addresses:

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: none

☐ Static Virtual

Requested Certificate:

Locked CAPsMAN Common Name:

OK Cancel Apply

# Szczegóły request Radius

70	47.400733	192.168.247.131	192.168.247.138	RADIUS	347 Access-Request(1) (id=51, l=305)
71	47.402659	192.168.247.138	192.168.247.131	RADIUS	348 Access-Accept(2) (id=51, l=306)

Packet identifier: 0x33 (51)

Length: 305

Authenticator: 90aa7126e6782549580f2f4877f8e07b

[\[The response to this request is in frame 71\]](#)

▼ Attribute Value Pairs

- > AVP: l=6 t=Service-Type(6): Framed(2)
- > AVP: l=6 t=Framed-MTU(12): 1400
- > AVP: l=9 t=User-Name(1): mbumVip
- > AVP: l=38 t=State(24): 6efd08110000013700011700fe8000000000000f84cf7c2...
- > AVP: l=22 t=NAS-Port-Id(87): 2G-mwtrc--CAP-eap-1-1
- > AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
- > AVP: l=10 t=Acct-Session-Id(44): 82000006
- > AVP: l=19 t=Calling-Station-Id(31): C0-F4-E6-3A-D6-F9
- > AVP: l=28 t=Called-Station-Id(30): BA-69-F4-AA-BD-4A:MBUM-eap
- > AVP: l=108 t=EAP-Message(79) Last Segment[1]
- > AVP: l=18 t=Message-Authenticator(80): 3cf6cf404323d9735e73cf88ae97c3c6

Disable



# Szczegóły response Radius

70	47.400733	192.168.247.131	192.168.247.138	RADIUS	347 Access-Request(1) (id=51, l=305)
71	47.402659	192.168.247.138	192.168.247.131	RADIUS	348 Access-Accept(2) (id=51, l=306)

Packet identifier: 0x33 (51)	<a href="#">Disable</a>
Length: 306	
Authenticator: 53bd1d187303bd3746e339f78bb8d0b1	
<a href="#">[This is a response to a request in frame 70]</a>	
[Time from request: 0.001926000 seconds]	
▼ Attribute Value Pairs	
▼ AVP: l=12 t=Vendor-Specific(26) v=MikroTik(14988)	
AVP Type: 26	
AVP Length: 12	
> VSA: l=6 t=Mikrotik-Wireless-VLANID(26): 4	
▼ AVP: l=12 t=Vendor-Specific(26) v=MikroTik(14988)	
AVP Type: 26	
AVP Length: 12	
> VSA: l=6 t=Mikrotik-Wireless-VLANID-Type(27): 0	
> AVP: l=6 t=Framed-Protocol(7): PPP(1)	
> AVP: l=6 t=Service-Type(6): Framed(2)	

# Podłączeni klienci

CAPSMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table

— Y CAPs Scanner

Interface	SSID	MAC Address	EAP Identity	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime	Tx/Rx Packets	Tx/Rx Bytes
2G-mwtc-CAP-ea...	MBUM-eap	C0:F4:E6:3A:D6:F9	mbumVip	39Mbps-...	52Mbps-...	0	-40	00:04:29...	274/265	82.9 KiB/33.4 KiB

CAPs AP Client <C0:F4:E6:3A:D6:F9>

Interface: 2G-mwtc-CAP-eap-1-1 OK

SSID: MBUM-eap Remove

MAC Address: C0:F4:E6:3A:D6:F9 Copy to Access List

EAP Identity: mbumVip

Tx Rate: 39Mbps-20MHz/2S

Rx Rate: 52Mbps-20MHz/2S

Tx Rate Set: OFDM:6-54 BW:1x SGI:1x HT:0-15

Tx Signal: 0

Rx Signal: -40

Uptime: 00:04:29.27

Tx/Rx Packets: 274/265

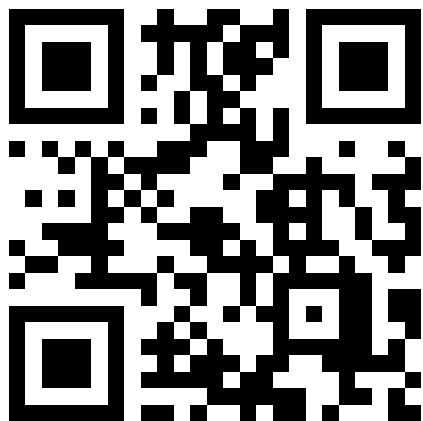
Tx/Rx Bytes: 82.9 KiB/33.4 KiB

# 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