

<u>Procédure Configuration WIFI + RADIUS</u>  Procédure configuration Wifi & Radius	HUYNH Michael SAKO Bah FRANCAIS Benjamin 2B-SISR
---	--

ASSURMER

Version	Auteur	Date	Nombre de pages	À l'attention	Mode de diffusion	Valideur
1.0	FRANCAIS Benjamin ; SAKO BAH ;HUYNH Michael	31/01/2025	29	Assurmer-IT	.pdf	FRANÇAIS Benjamin

Sommaire

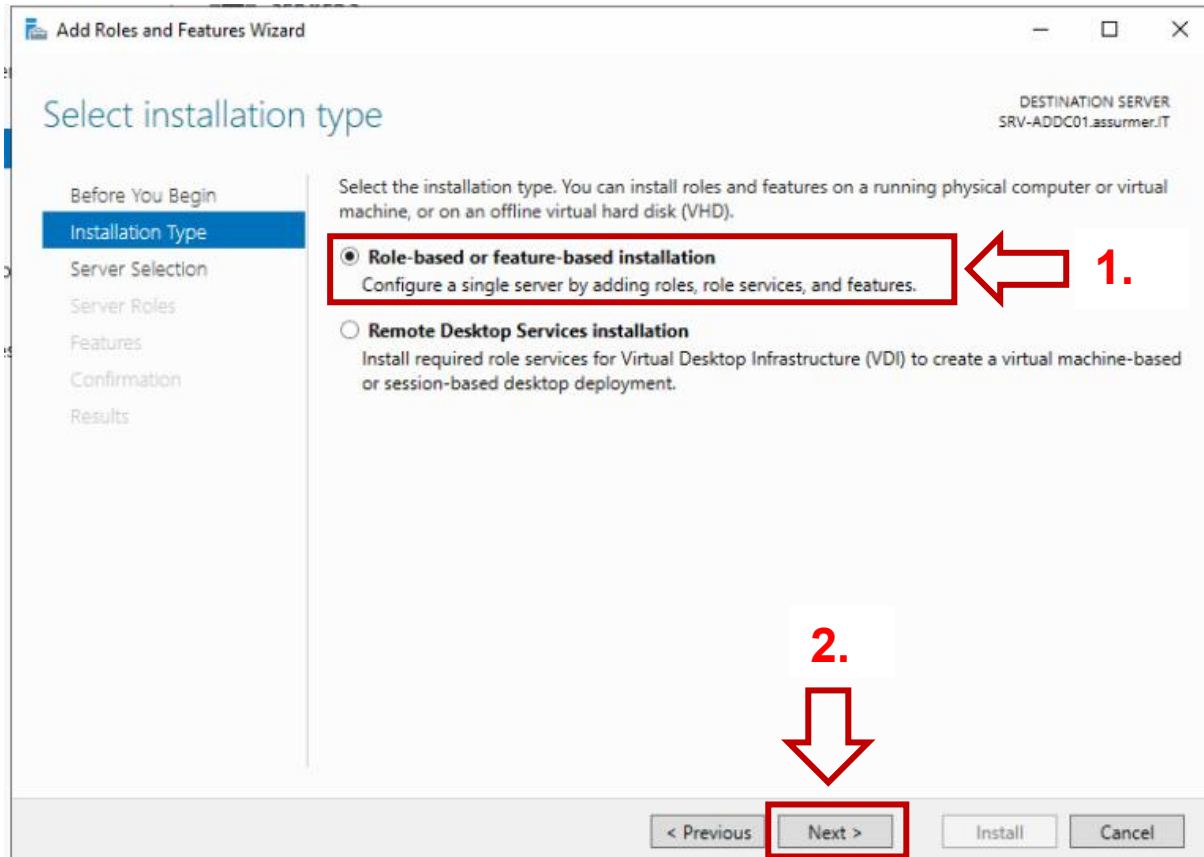
PREREQUIS :	2
INSTALLATION « NETWORK POLICY SERVER » :	3
Liaison NPS et AD :	6
CONFIGURATION RADIUS :	8
Liaison Borne WiFi et AD :	8
CONFIGURATION « AD CERTIFICATE SERVICES »	15
CONFIGURATION 802.1X :	23
CONFIGURATION BORNE WIFI POUR RADIUS :	27

Prérequis :

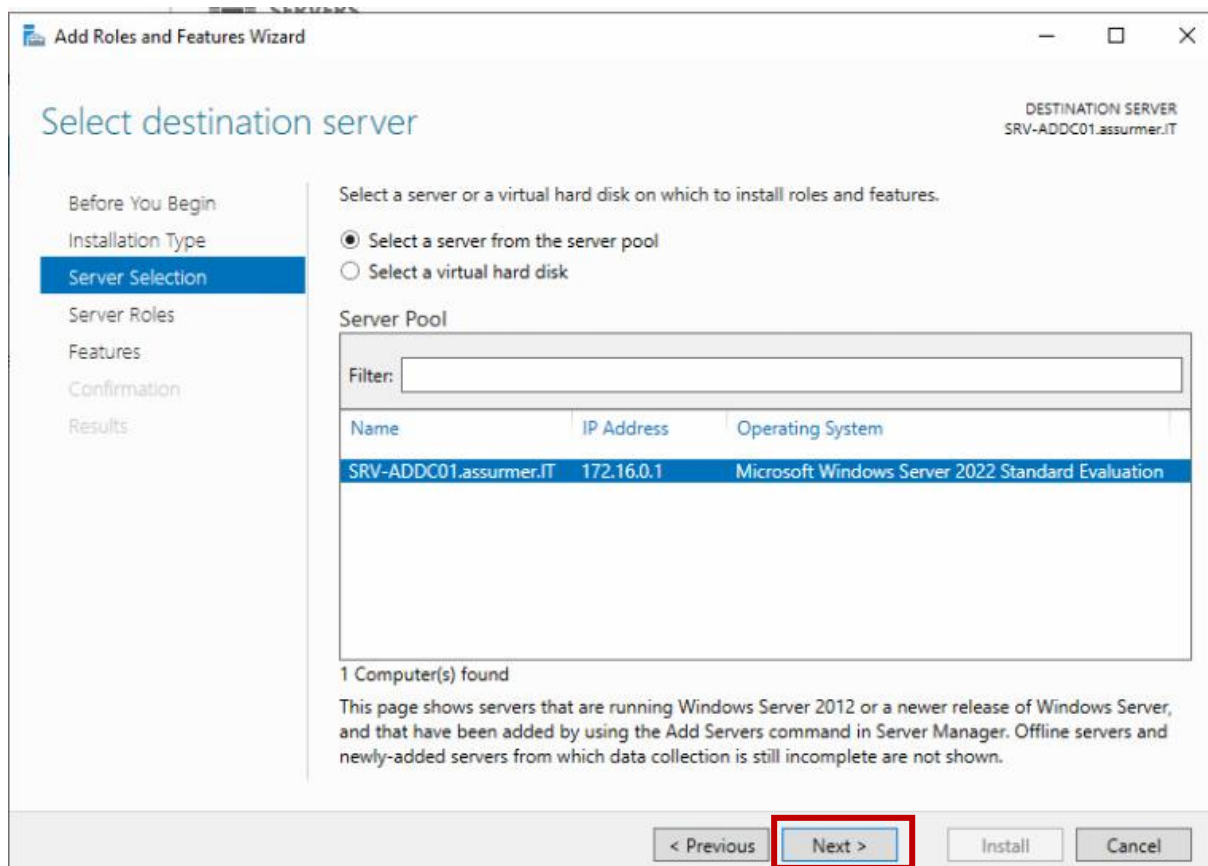
- 1 serveur AD; 1 Borne Wifi
- Compte Administrateur

Installation « Network Policy Server » :

- Cliquer sur « Add Roles and Features Wizard » dans le « Server Manager » puis sélectionner « Role-based or feature-based installation »

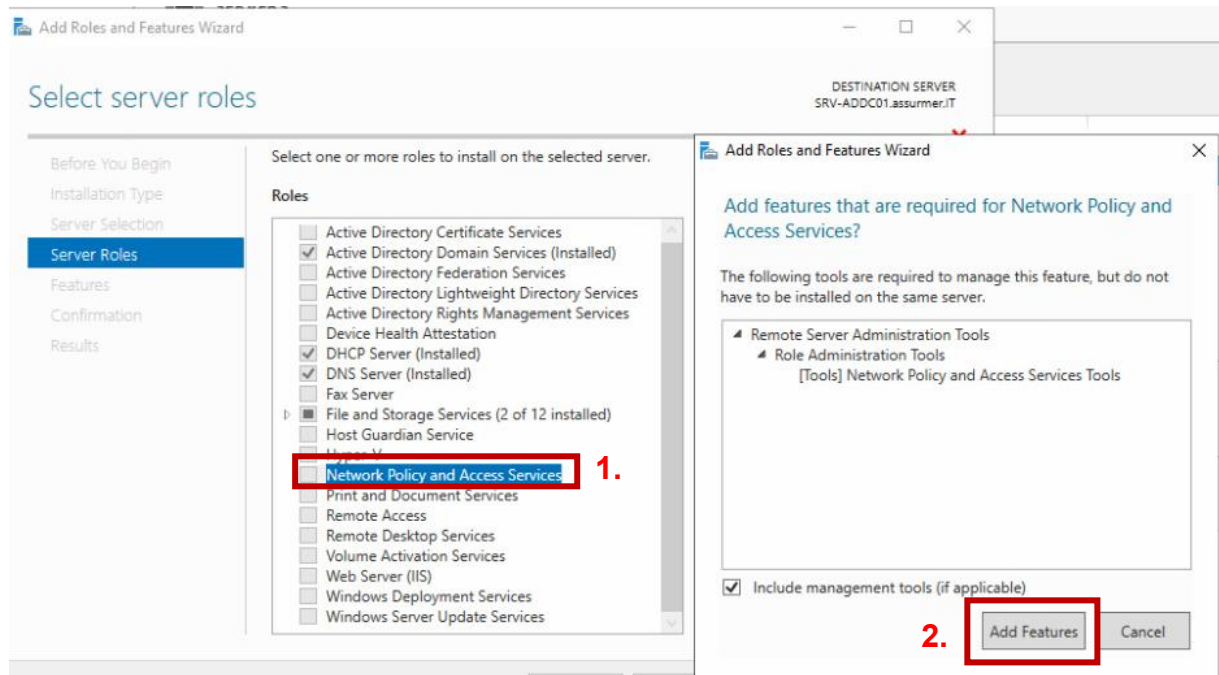


- Sélectionner le serveur concerné

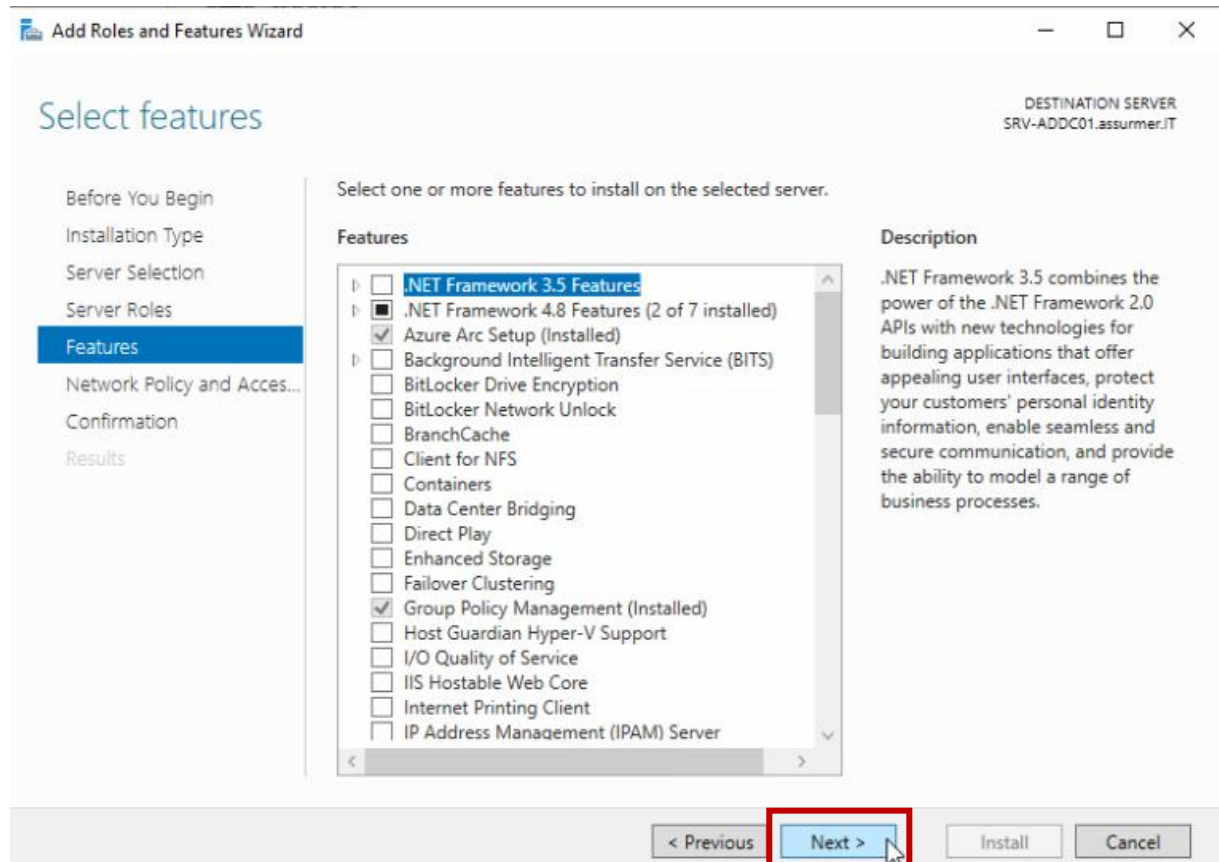


[Procédure] Configuration WiFi & RADIUS

- Sélectionner « Network Policy and Access Services »

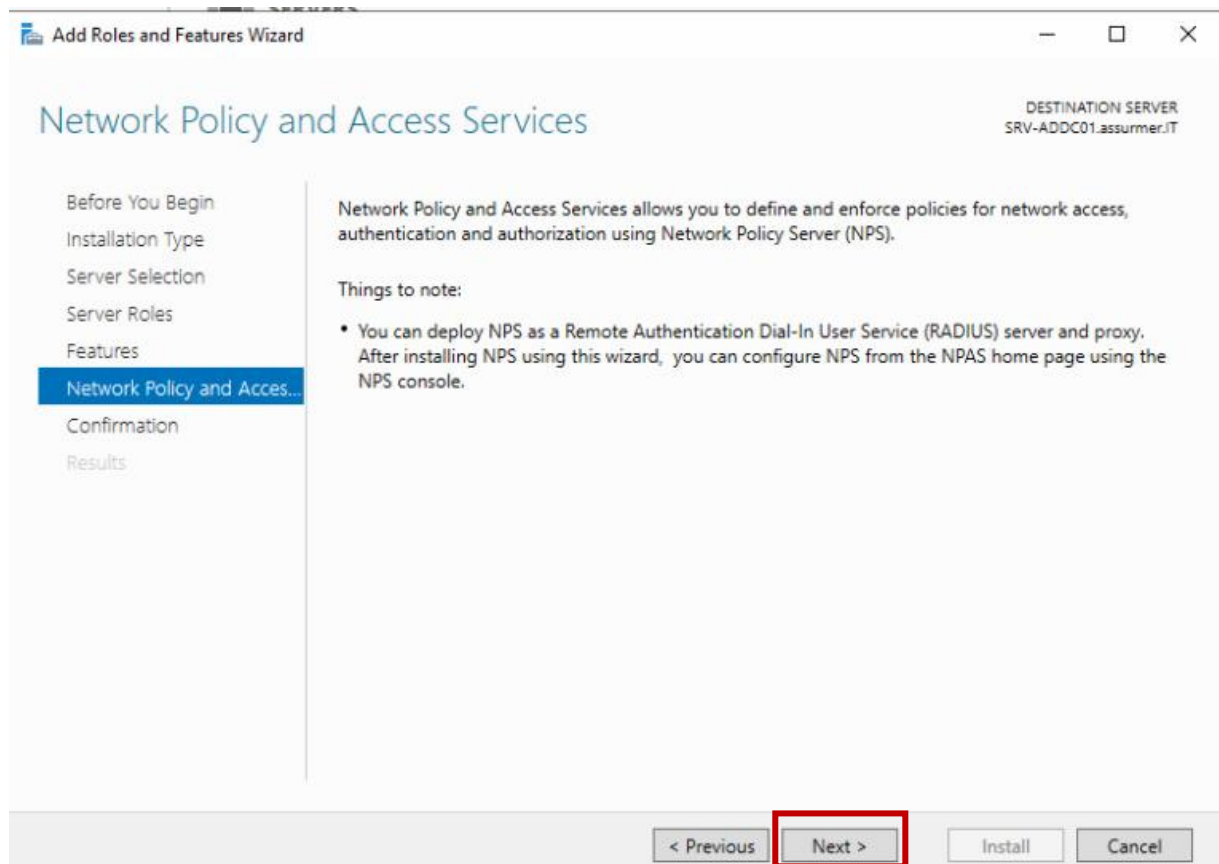


- Cliquer sur « Next »

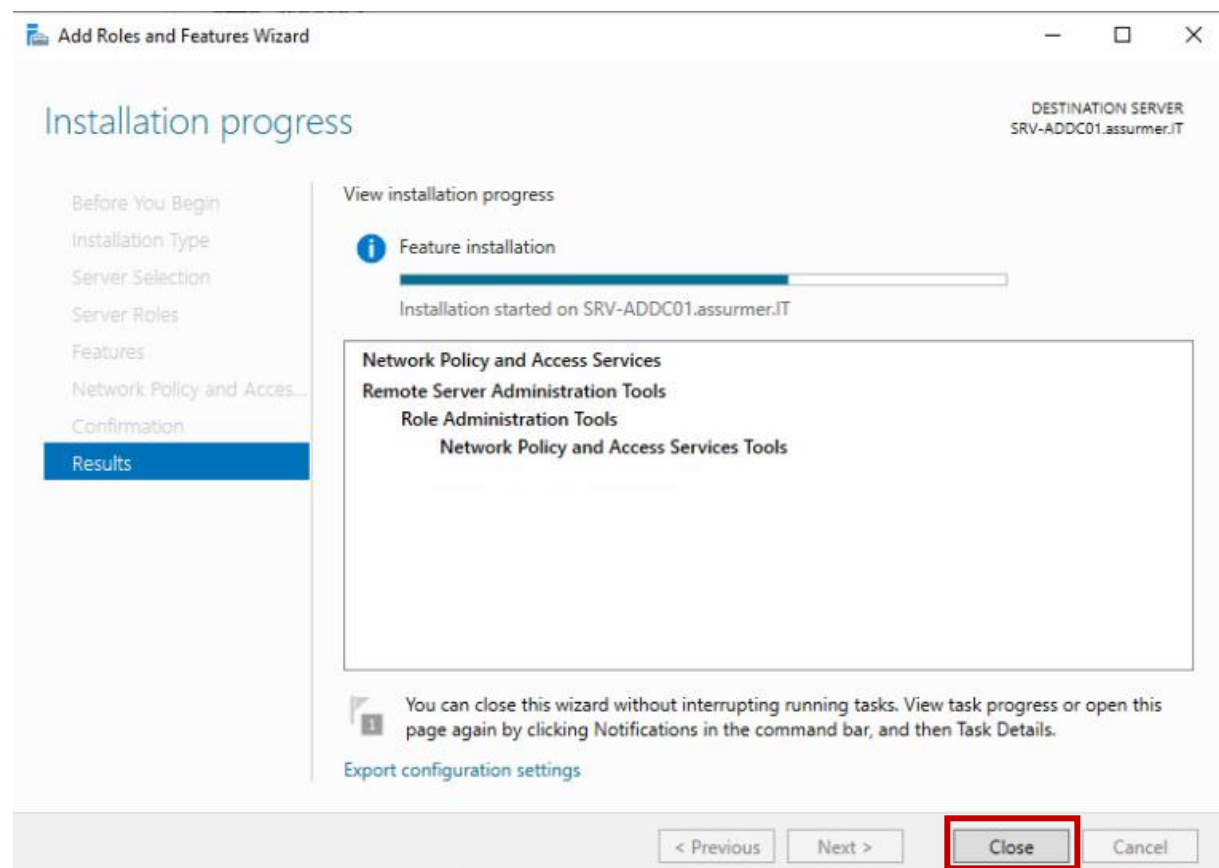


[Procédure] Configuration WiFi & RADIUS

- Cliquer sur « Next »

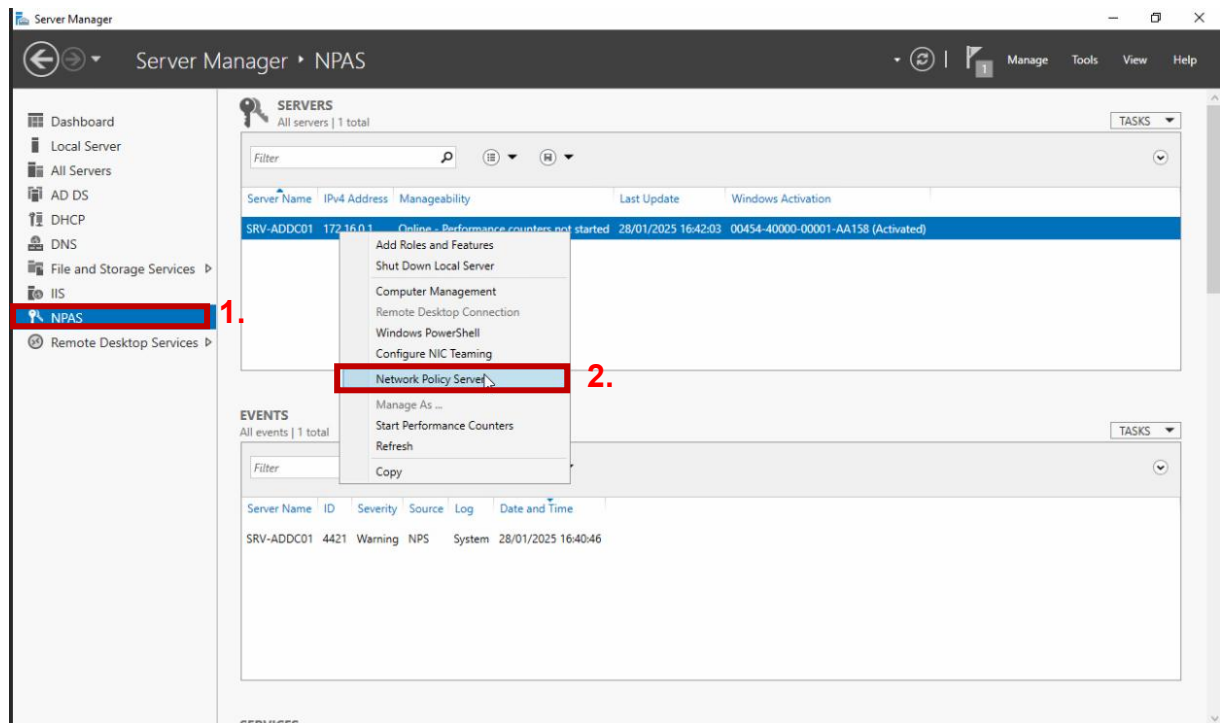


- Cliquer sur « Close »

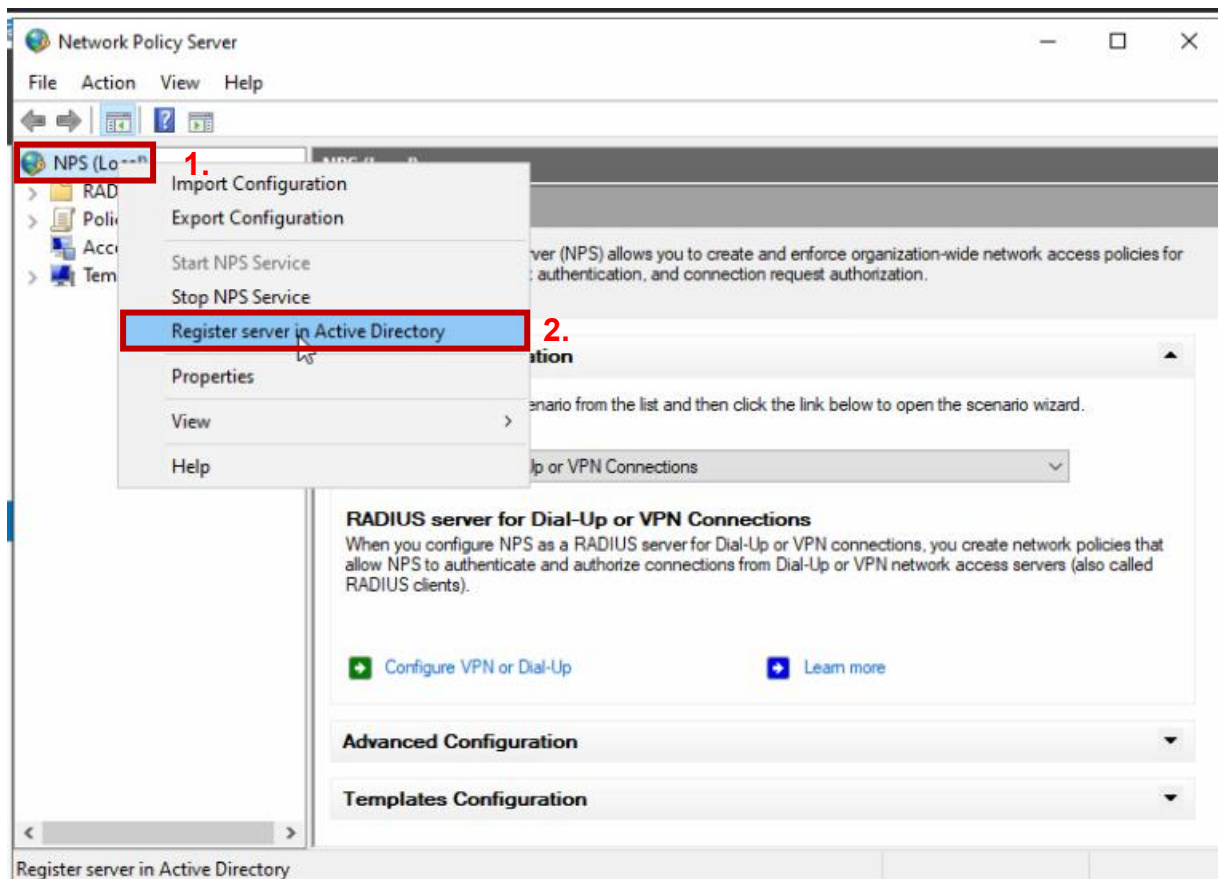


Liaison NPS et AD :

- Sur le « Server Manager », aller dans « NPAS » et faire un clic-droit sur le serveur. Puis sélectionner « Network Policy Server »

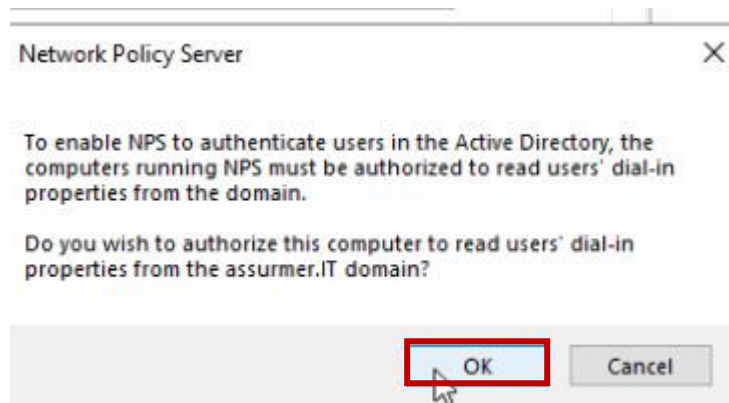


- Faire un clic droit sur « NPS » et sélectionner « Register server in Active Directory »



[Procédure] Configuration WiFi & RADIUS

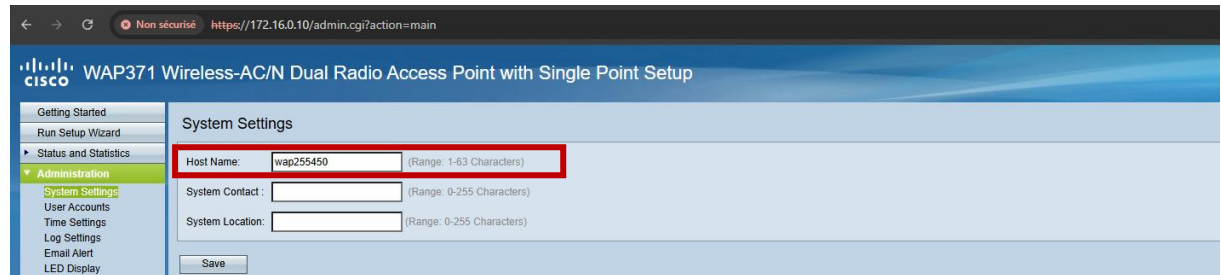
- Cliquer sur « OK »



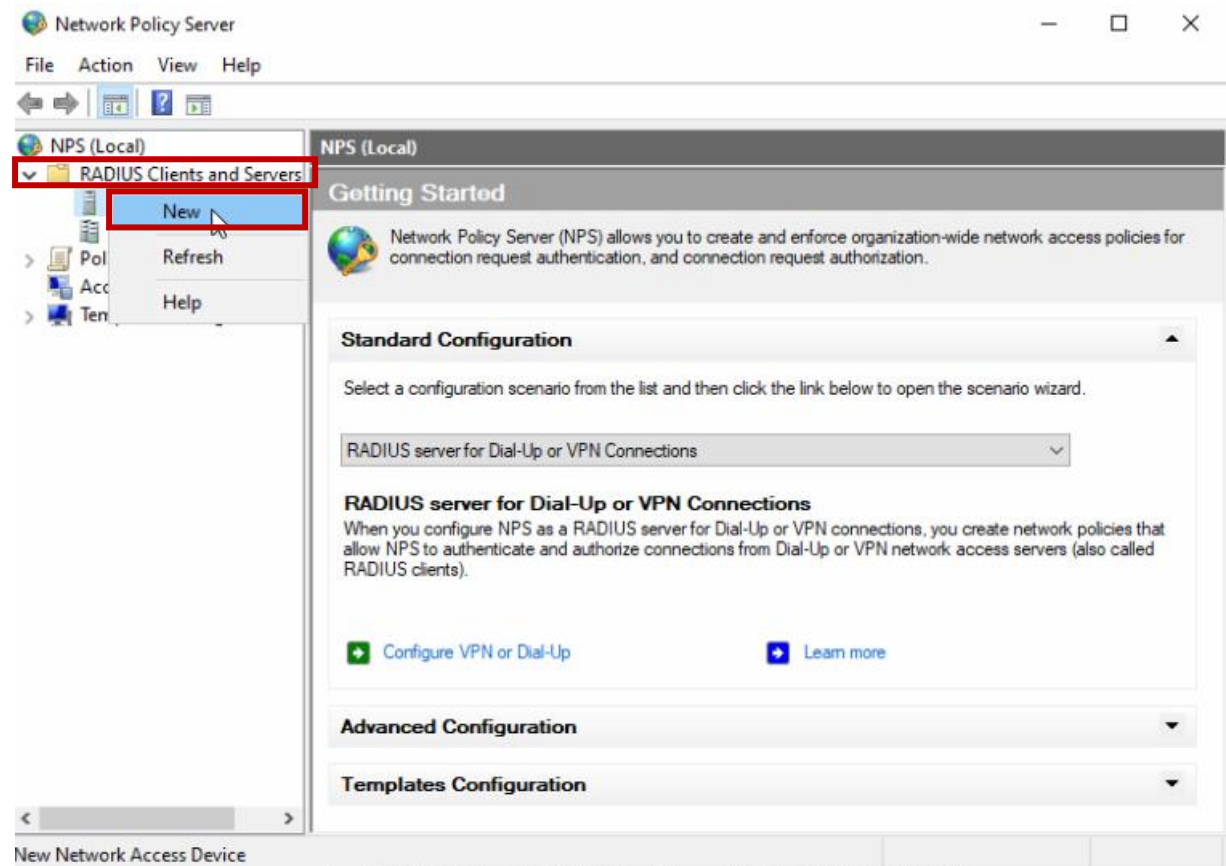
Configuration RADIUS :

Liaison Borne WiFi et AD :

- Récupérer le « Host name » de la borne sur l'interface en ligne de la borne :



- Retourner sur NPS et clic-droit sur « RADIUS CLIENTS » et « New »



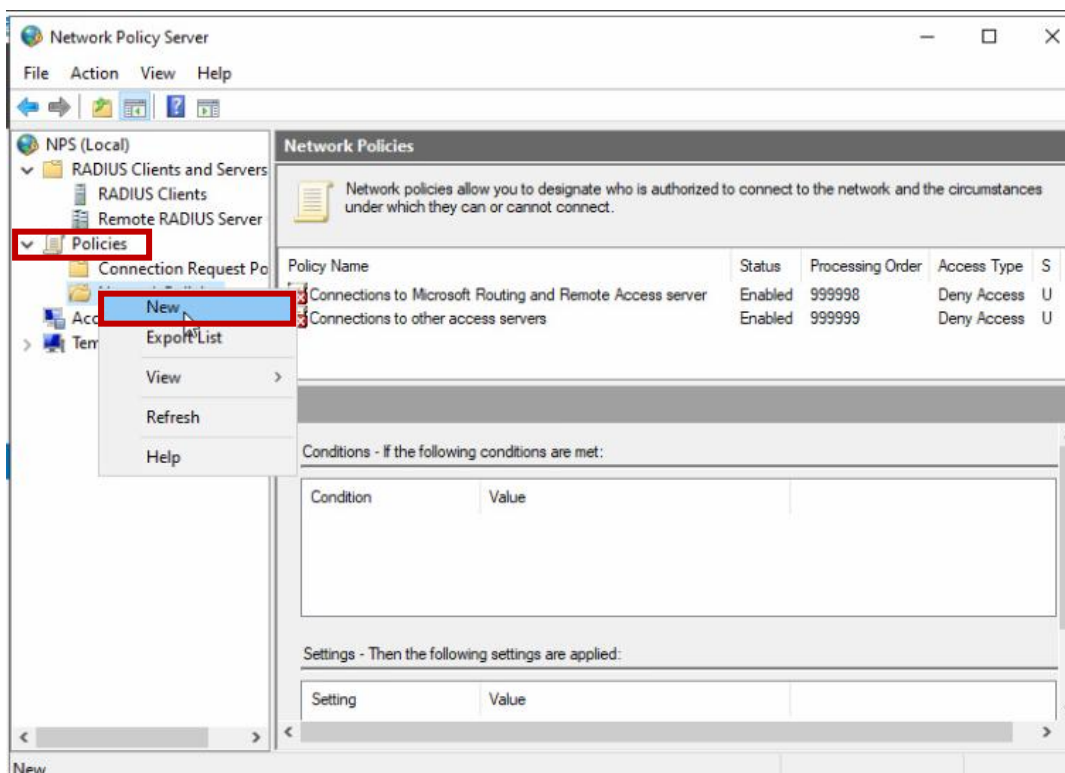
•

[Procédure] Configuration WiFi & RADIUS

- Rentrer les informations relatives à la borne Wifi

The 'New RADIUS Client' dialog box is shown with the 'Settings' tab selected. The 'Enable this RADIUS client' checkbox is checked. Under 'Name and Address', the 'Friendly name' is 'wap255450' and the 'Address (IP or DNS)' is '172.16.0.10'. Under 'Shared Secret', the 'Manual' radio button is selected, and the 'Shared secret' and 'Confirm shared secret' fields are filled with masked characters. The 'OK' button is highlighted.

- Développer Politiques puis clic-droit sur « Network Policies » et « New »



[Procédure] Configuration WiFi & RADIUS

- Nommer la politique en « SSID »

New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
SSID

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

Previous Next Finish Cancel

- Cliquer sur « Add »

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
-----------	-------

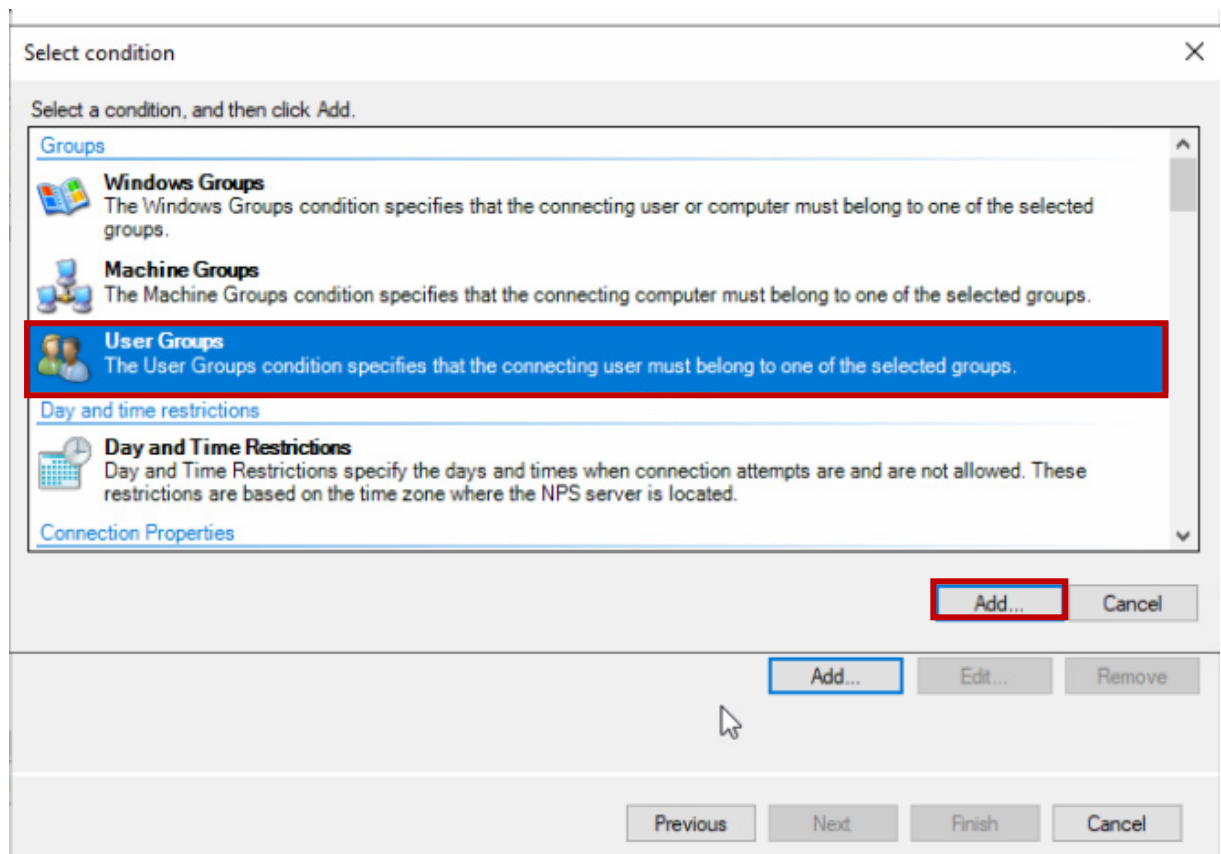
Condition description:

Add Edit... Remove

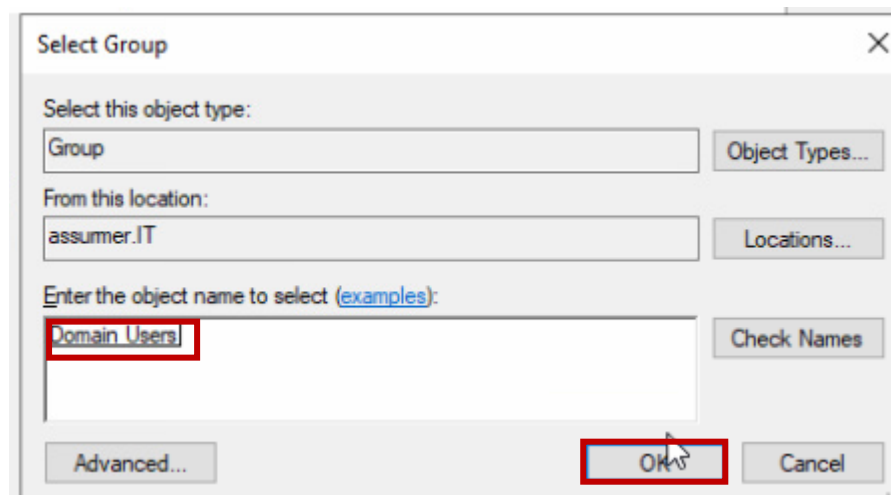
Previous Next Finish Cancel

[Procédure] Configuration WiFi & RADIUS

- Choisir « User Groups »

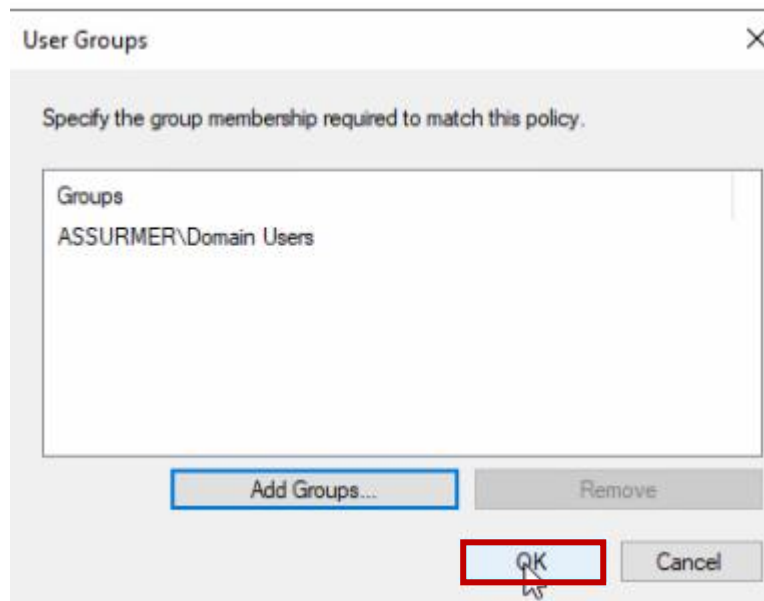


- On rajoute le groupe de sécurité « Domain User »

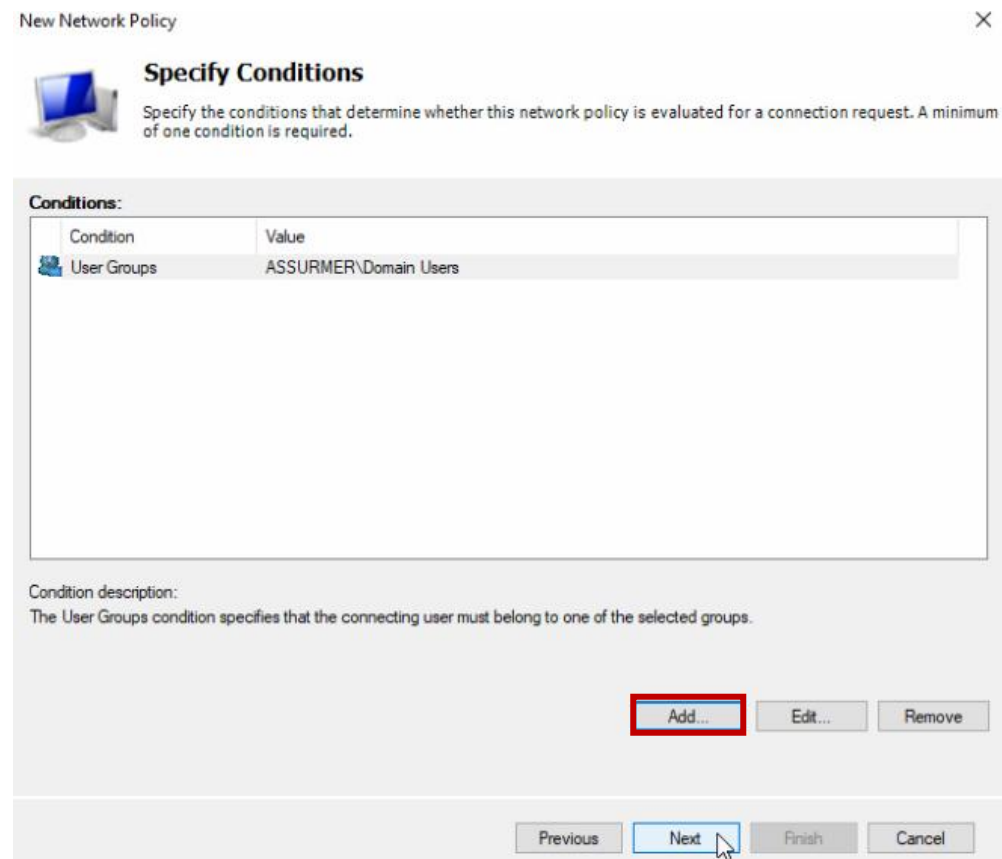


[Procédure] Configuration WiFi & RADIUS

- Cliquer sur « OK »

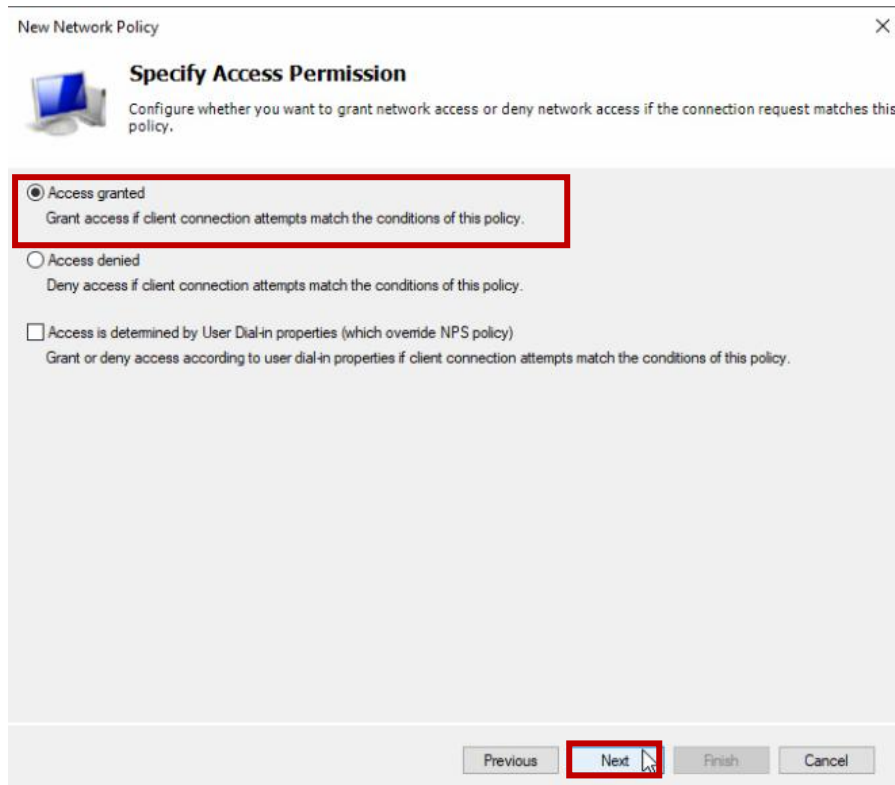


- Cliquer sur « Next »



[Procédure] Configuration WiFi & RADIUS

- Sélectionner « Access granted » puis « Next »



New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

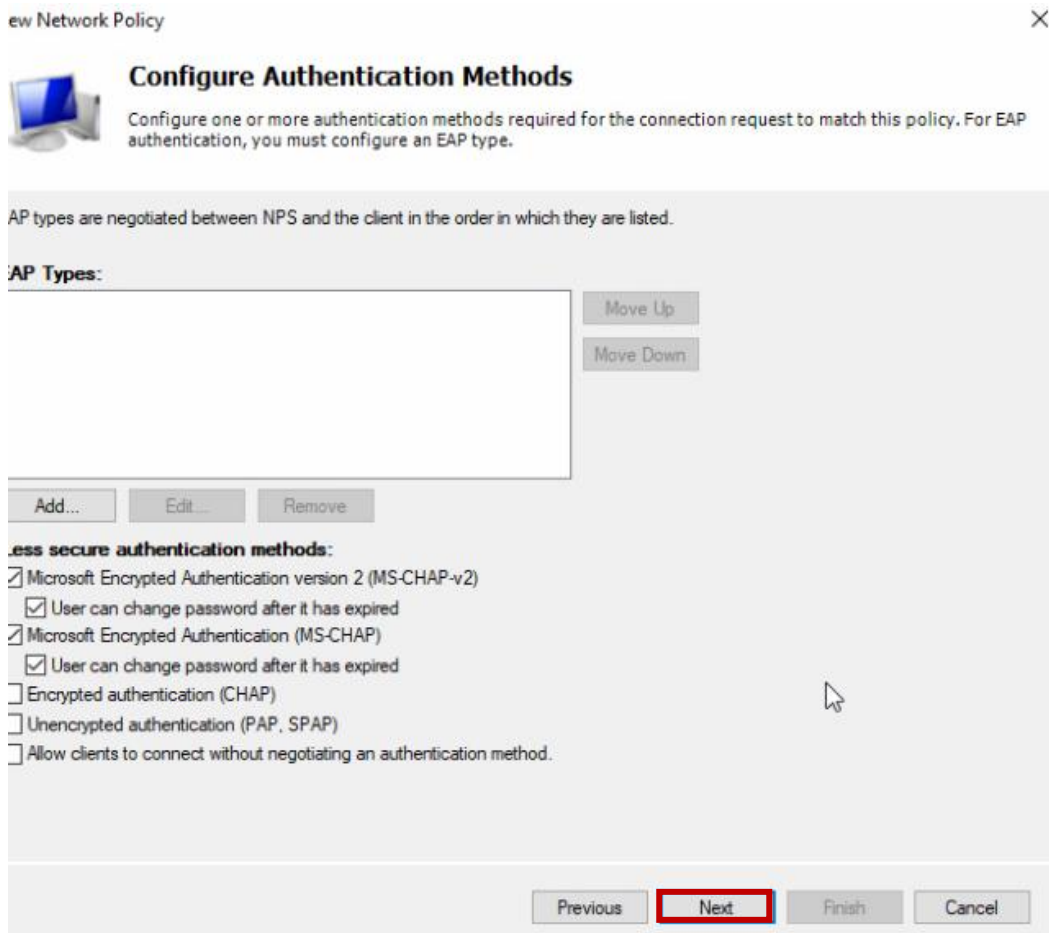
☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

- Cliquer « Next »



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

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

AP Types:

Move Up
Move Down

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.

Previous Next Finish Cancel

[Procédure] Configuration WiFi & RADIUS

- Cliquer « Finish »

New Network Policy ×

 **Completing New Network Policy**

You have successfully created the following network policy:

SSID

Policy conditions:

Condition	Value
User Groups	ASSURMER\Domain Users

Policy settings:

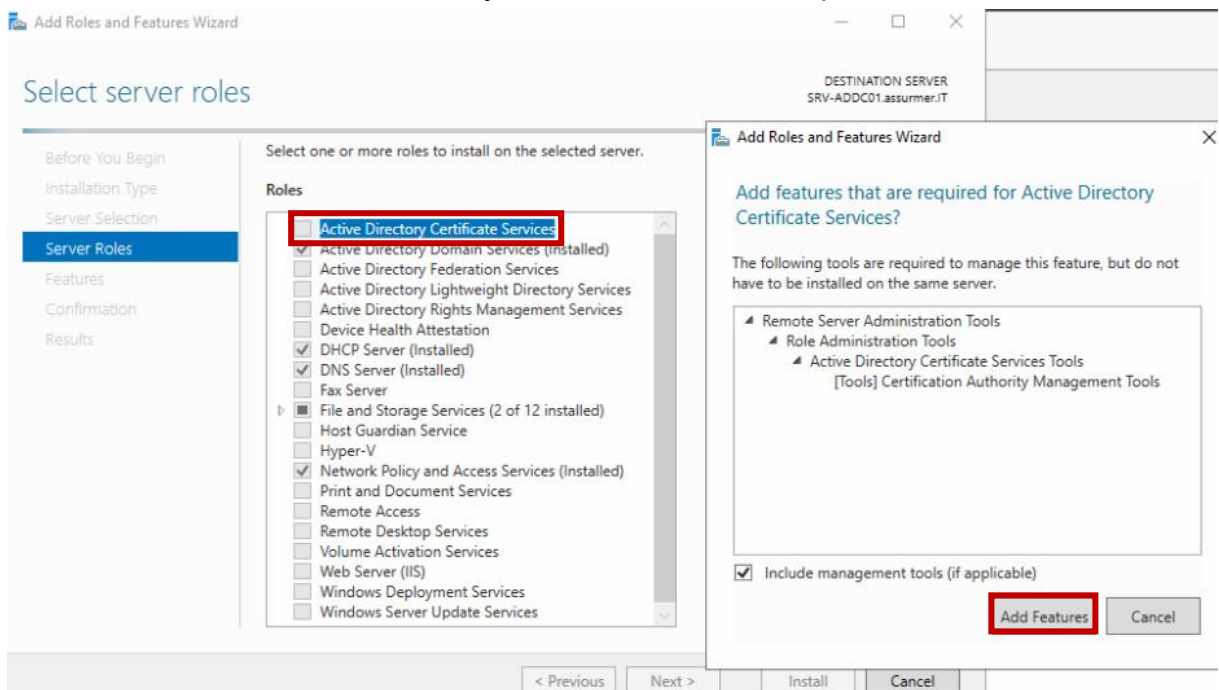
Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False

To close this wizard, click Finish.

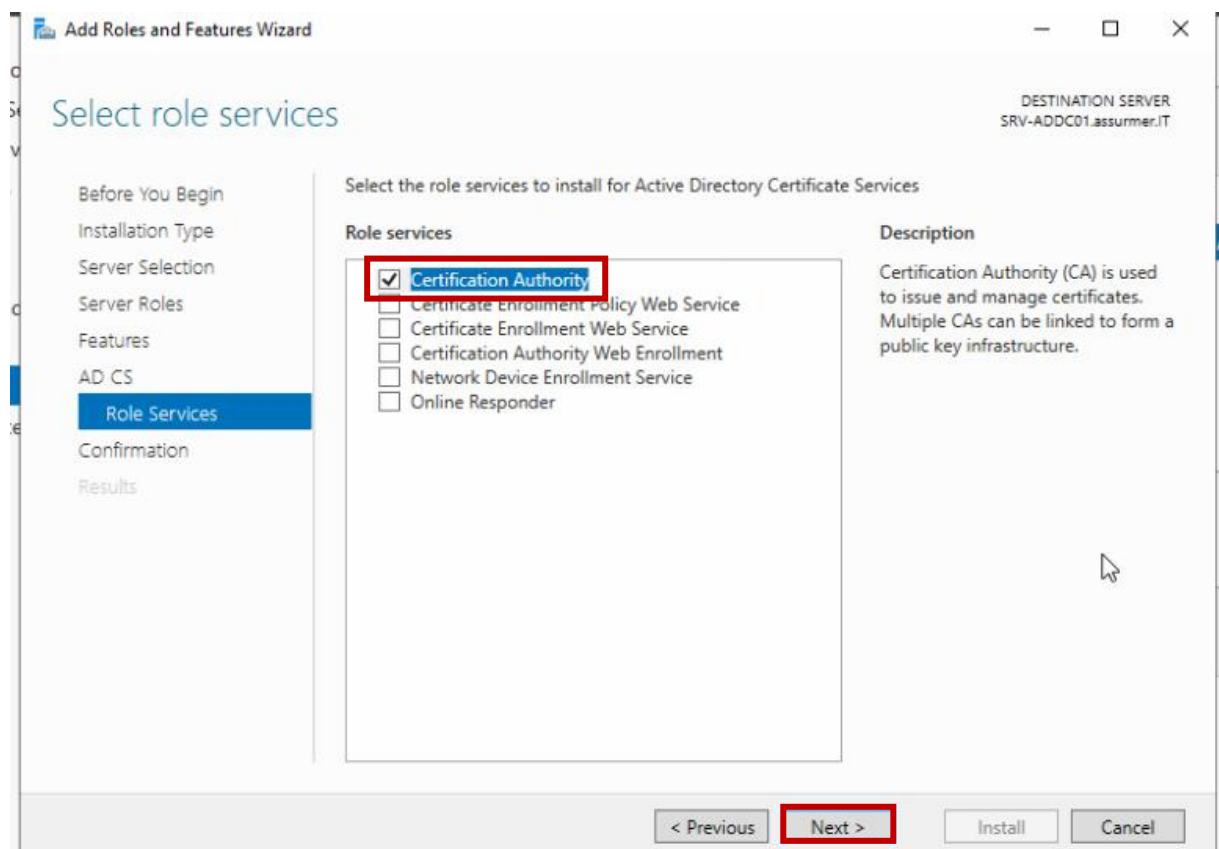
Previous Next **Finish** Cancel

Configuration « AD Certificate Services »

- Sélectionner « Active Directory Certificate Services » puis « Add Features »

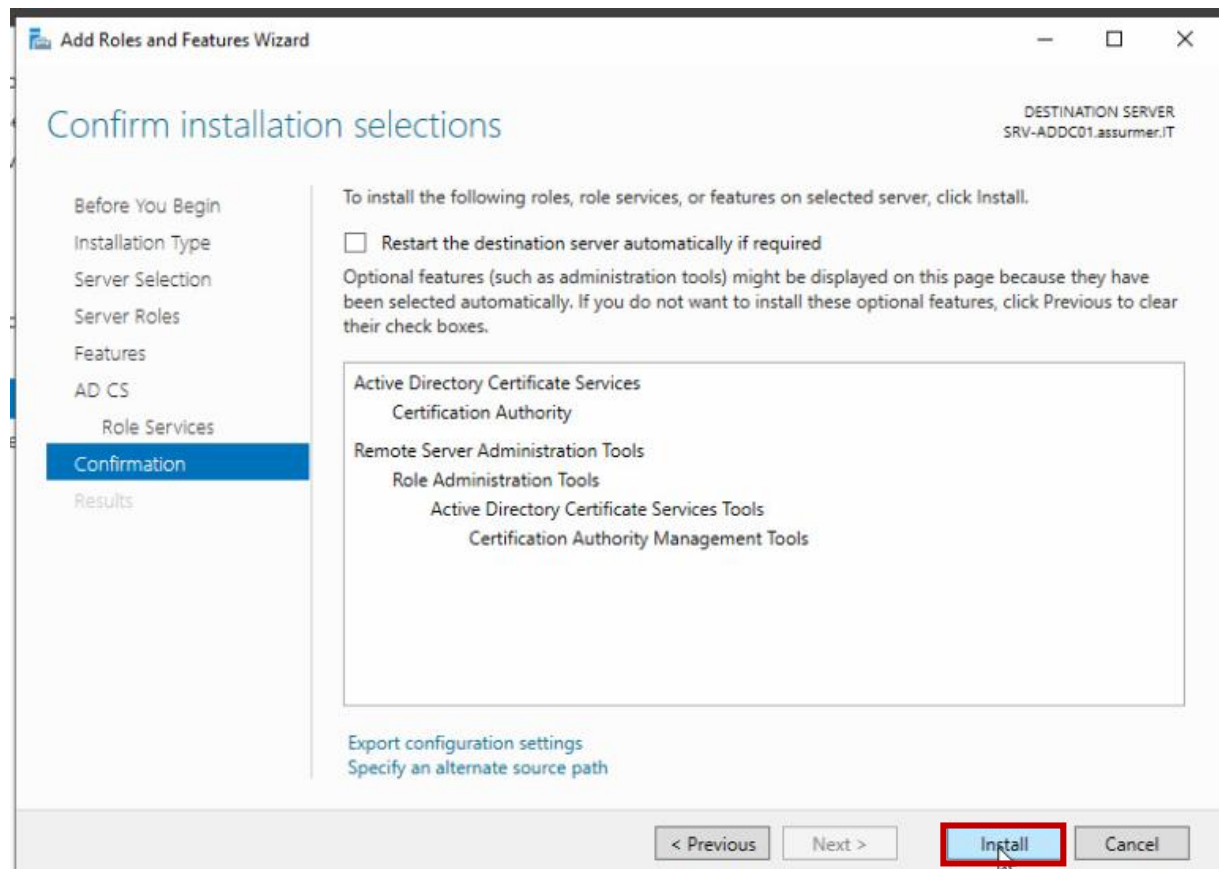


- Sélectionner « Certification Authority » puis « Next »

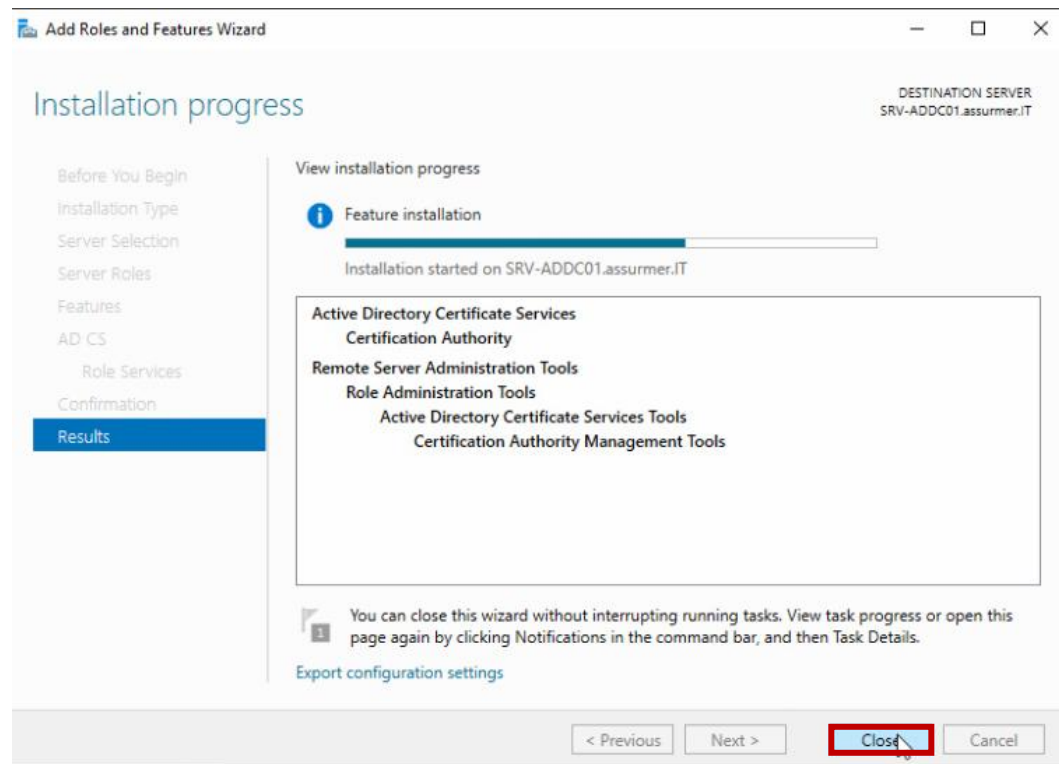


[Procédure] Configuration WiFi & RADIUS

- Cliquer « Install »

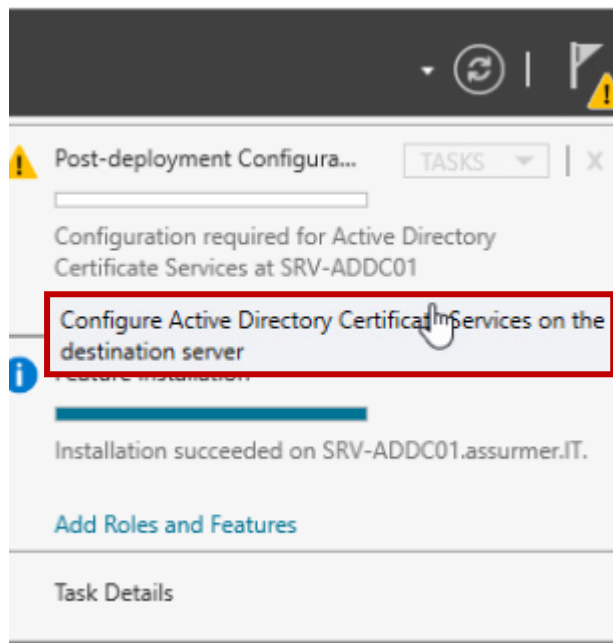


- A la fin de l'installation cliquer sur « Close »

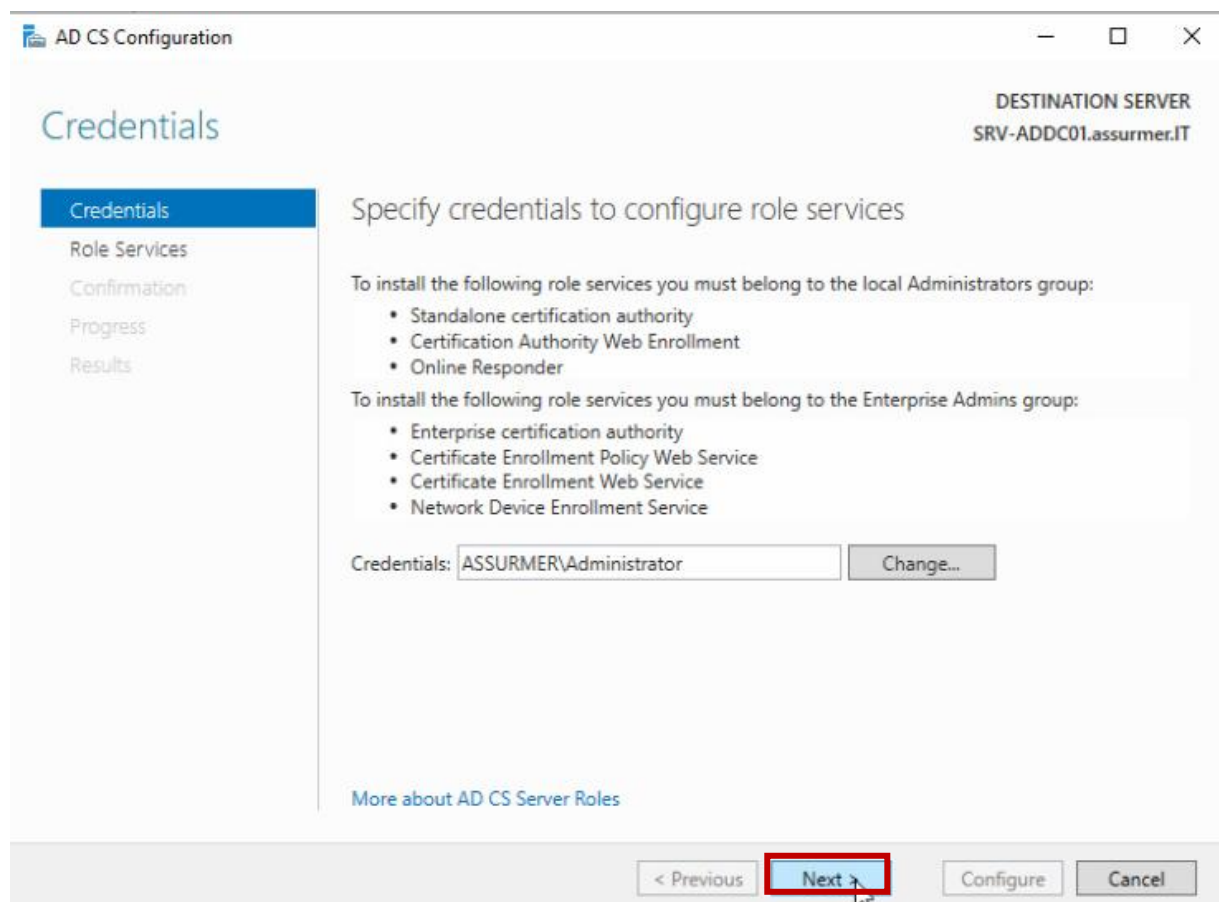


[Procédure] Configuration WiFi & RADIUS

- Configurer le service précédemment installer

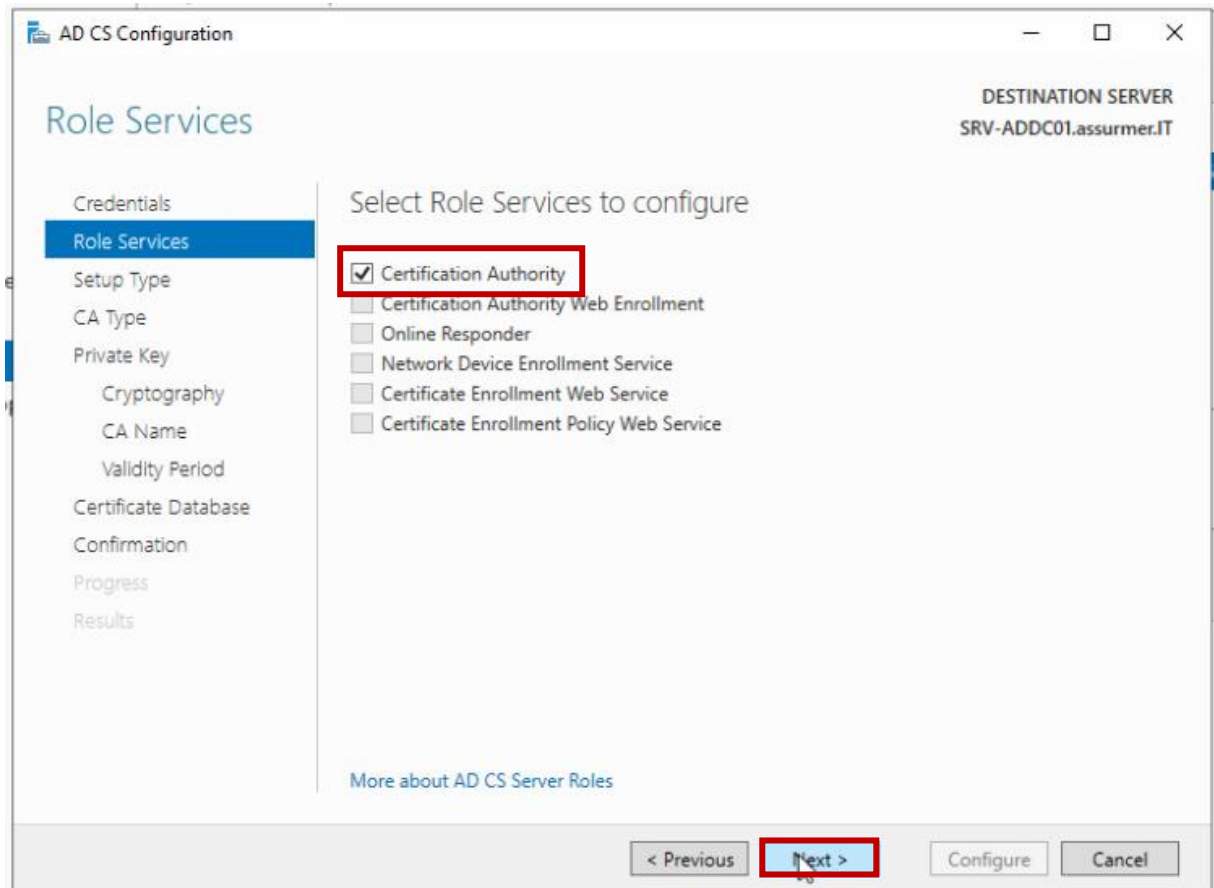


- Cliquer « Next »

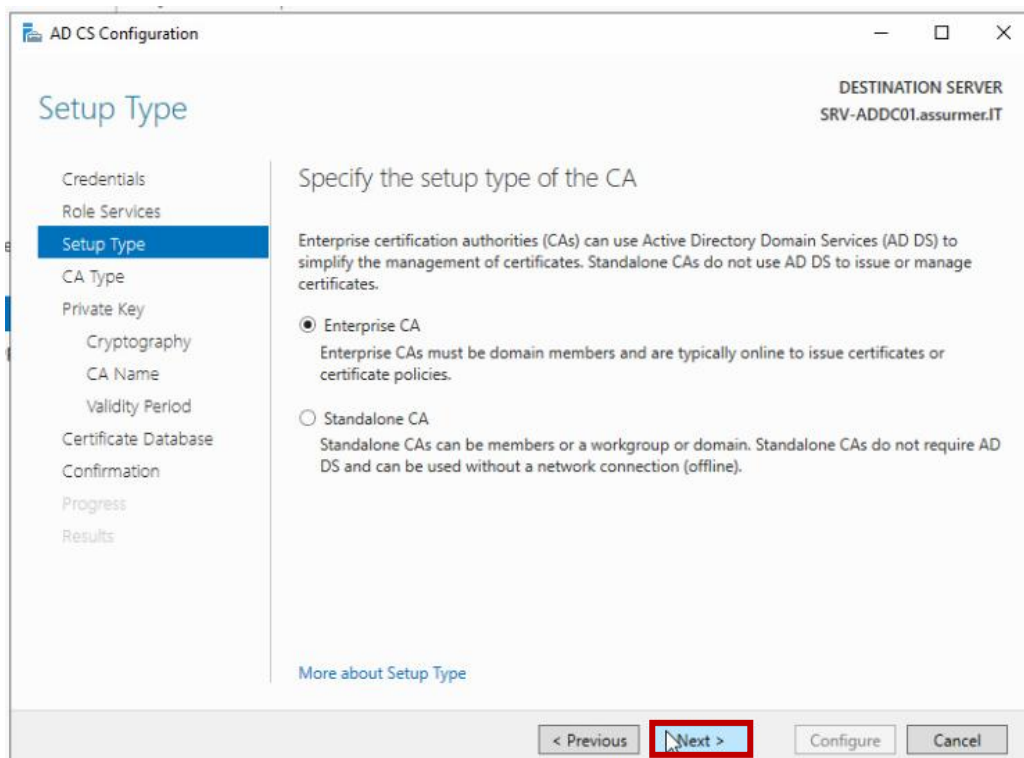


[Procédure] Configuration WiFi & RADIUS

- Sélectionner « Certification Authority »



- Sélectionner « Enterprise CA » puis « Next »



[Procédure] Configuration WiFi & RADIUS

- Sélectionner « Root CA » puis « Next »

AD CS Configuration

DESTINATION SERVER
SRV-ADDC01.assurmer.IT

CA Type

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.

[More about CA Type](#)

< Previous **Next >** Configure Cancel

- Sélectionner « Create a new private key » puis « Next »

AD CS Configuration

DESTINATION SERVER
SRV-ADDC01.assurmer.IT

Private Key

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.

[More about Private Key](#)

< Previous **Next >** Configure Cancel

[Procédure] Configuration WiFi & RADIUS

- Cliquer « Next »

The screenshot shows the 'Cryptography for CA' step in the 'AD CS Configuration' wizard. The left sidebar lists various configuration steps, with 'Cryptography' currently selected. The main area is titled 'Specify the cryptographic options'. It includes a dropdown for 'Select a cryptographic provider' set to 'RSA#Microsoft Software Key Storage Provider', a 'Key length' dropdown set to '2048', and a list for 'Select the hash algorithm for signing certificates issued by this CA:' with options SHA256, SHA384, SHA512, SHA1, and MD5. A checkbox for 'Allow administrator interaction when the private key is accessed by the CA.' is unchecked. At the bottom, the 'Next >' button is highlighted with a red box.

- Cliquer « Next »

The screenshot shows the 'CA Name' step in the 'AD CS Configuration' wizard. The left sidebar shows 'CA Name' selected. The main area is titled 'Specify the name of the CA'. It contains instructions: '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.' Below this are three text boxes: 'Common name for this CA:' with the value 'assumer-SRV-ADDC01-CA', 'Distinguished name suffix:' with the value 'DC=assumer,DC=IT', and 'Preview of distinguished name:' with the value 'CN=assumer-SRV-ADDC01-CA,DC=assumer,DC=IT'. At the bottom, the 'Next >' button is highlighted with a red box.

[Procédure] Configuration WiFi & RADIUS

- Choisir la durée du certificat puis cliquer « Next »

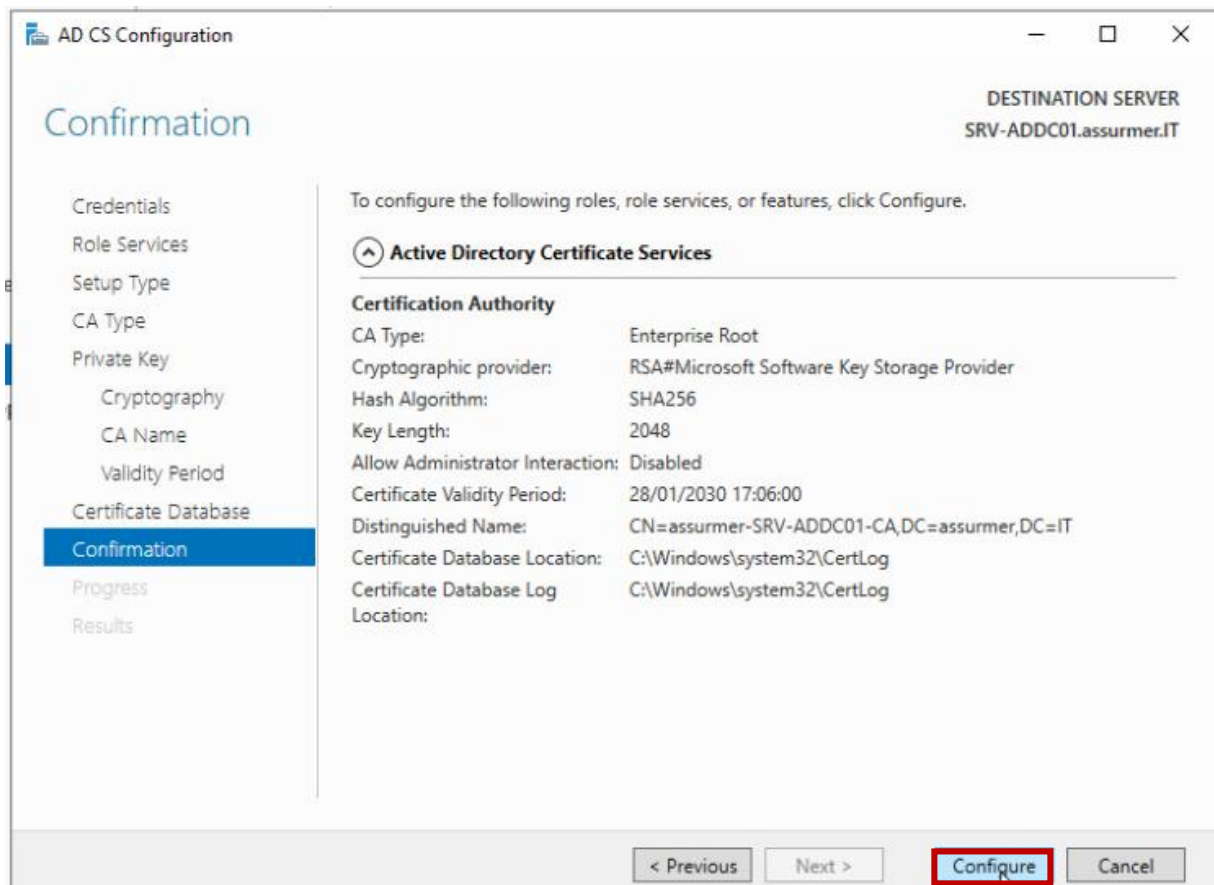
The screenshot shows the 'AD CS Configuration' window with the 'Validity Period' step selected in the left-hand navigation pane. The main area is titled 'Specify the validity period'. It contains a text box with '5' and a dropdown menu set to 'Years'. Below this, it says 'CA expiration Date: 28/01/2030 17:06:00'. A note states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' At the bottom right, there is a 'DESTINATION SERVER' label with the value 'SRV-ADDC01.assurmer.IT'. The bottom navigation bar has buttons for '< Previous', 'Next >' (highlighted with a red box), 'Configure', and 'Cancel'.

- Laisser les chemins par défauts et cliquer « Next »

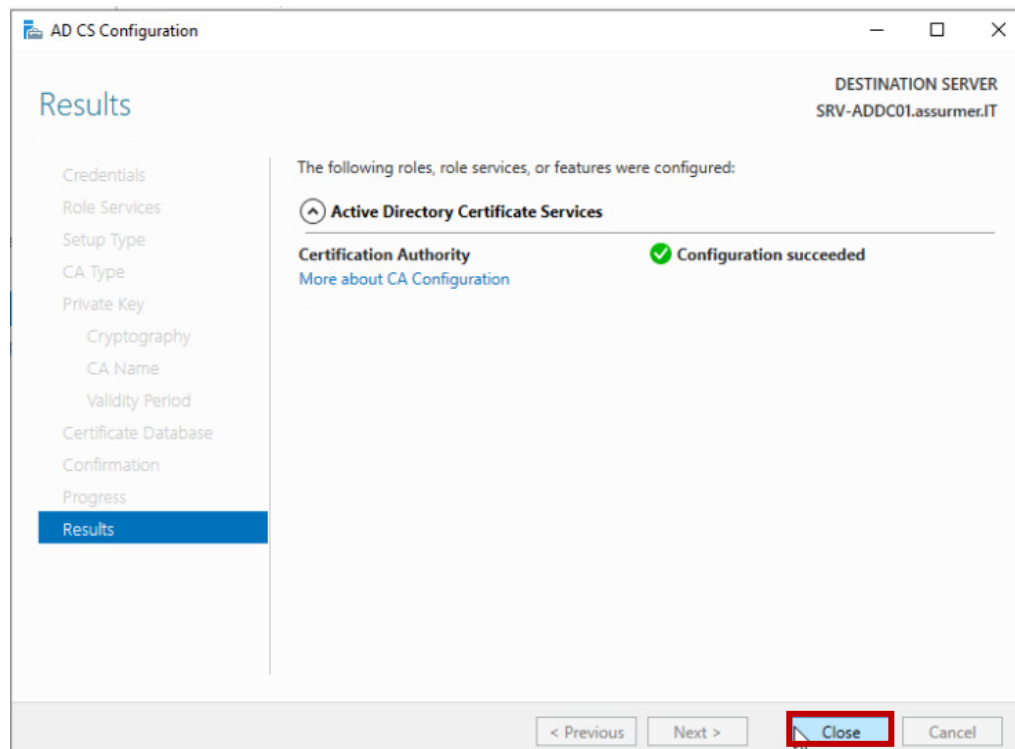
The screenshot shows the 'AD CS Configuration' window with the 'CA Database' step selected in the left-hand navigation pane. The main area is titled 'Specify the database locations'. It contains two text boxes: 'Certificate database location:' with the default path 'C:\Windows\system32\CertLog' and 'Certificate database log location:' with the default path 'C:\Windows\system32\CertLog'. At the bottom right, there is a 'DESTINATION SERVER' label with the value 'SRV-ADDC01.assurmer.IT'. The bottom navigation bar has buttons for '< Previous', 'Next >' (highlighted with a red box), 'Configure', and 'Cancel'.

[Procédure] Configuration WiFi & RADIUS

- Cliquer sur « Configure »

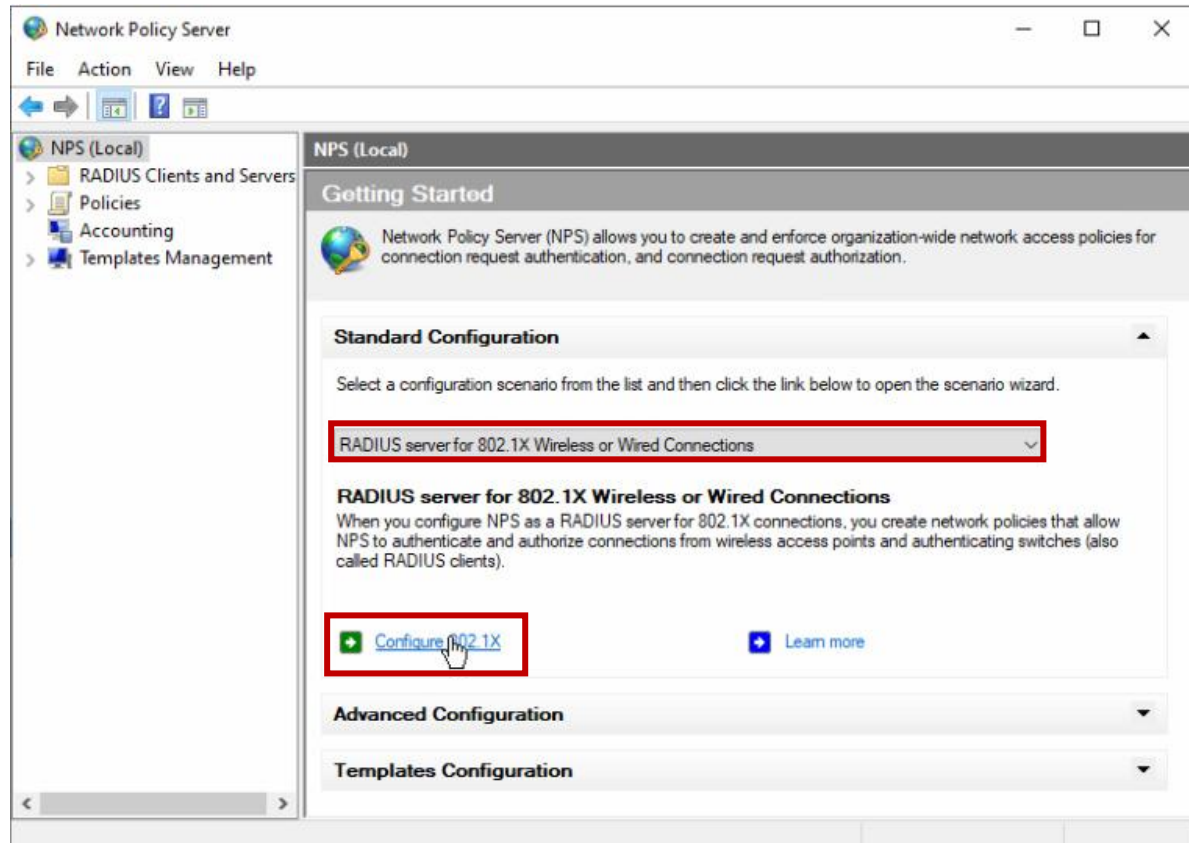


- Cliquer sur « Close »

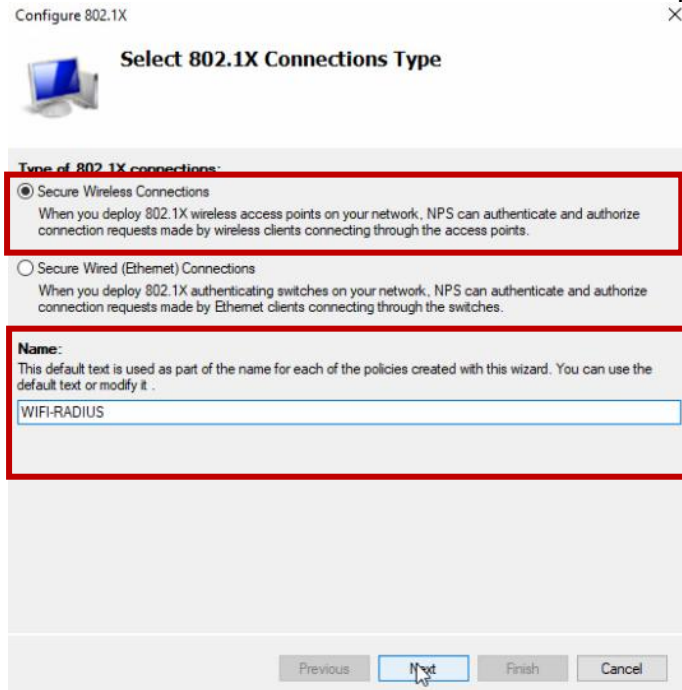


Configuration 802.1X :

- Dans NPS sélectionner « RADIUS server for 802.1X ... » puis « Configure 802.1X »

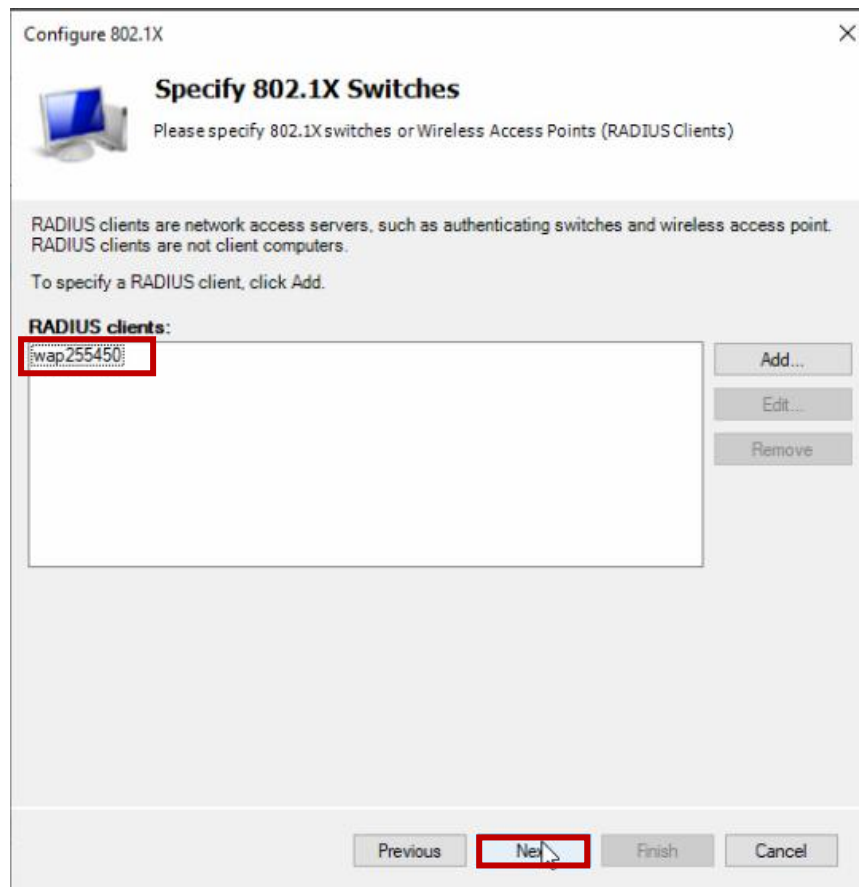


- Sélectionner « Secure Wireless Connections » puis choisir un nom

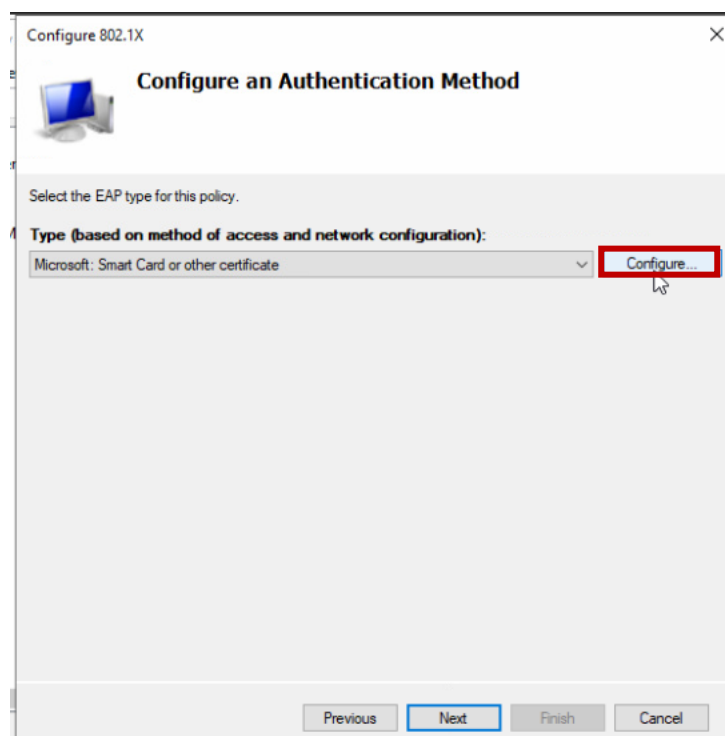


[Procédure] Configuration WiFi & RADIUS

- Ensuite la borne sera identifiée et cliquer « Next »

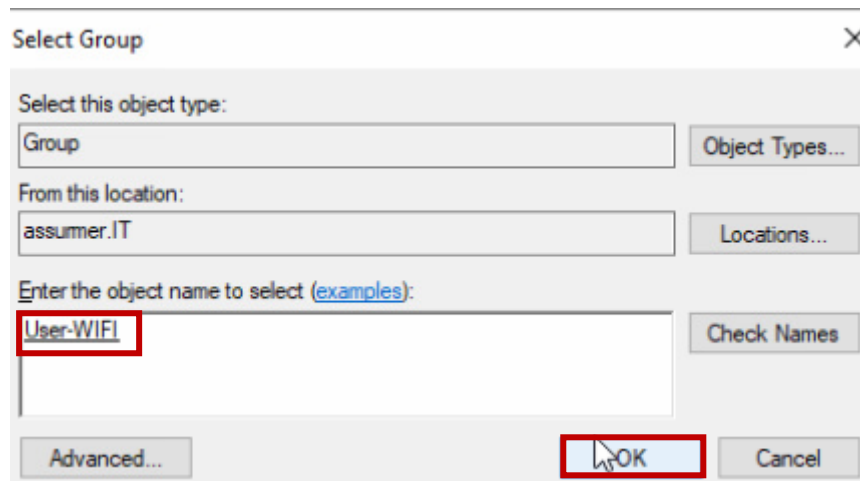


- Sélectionner « Microsoft Smart ... » dans le menu déroulant puis cliquer sur « Configure »



[Procédure] Configuration WiFi & RADIUS

- Choisir le groupe de sécurité qui doit avoir accès au WiFi



Select Group

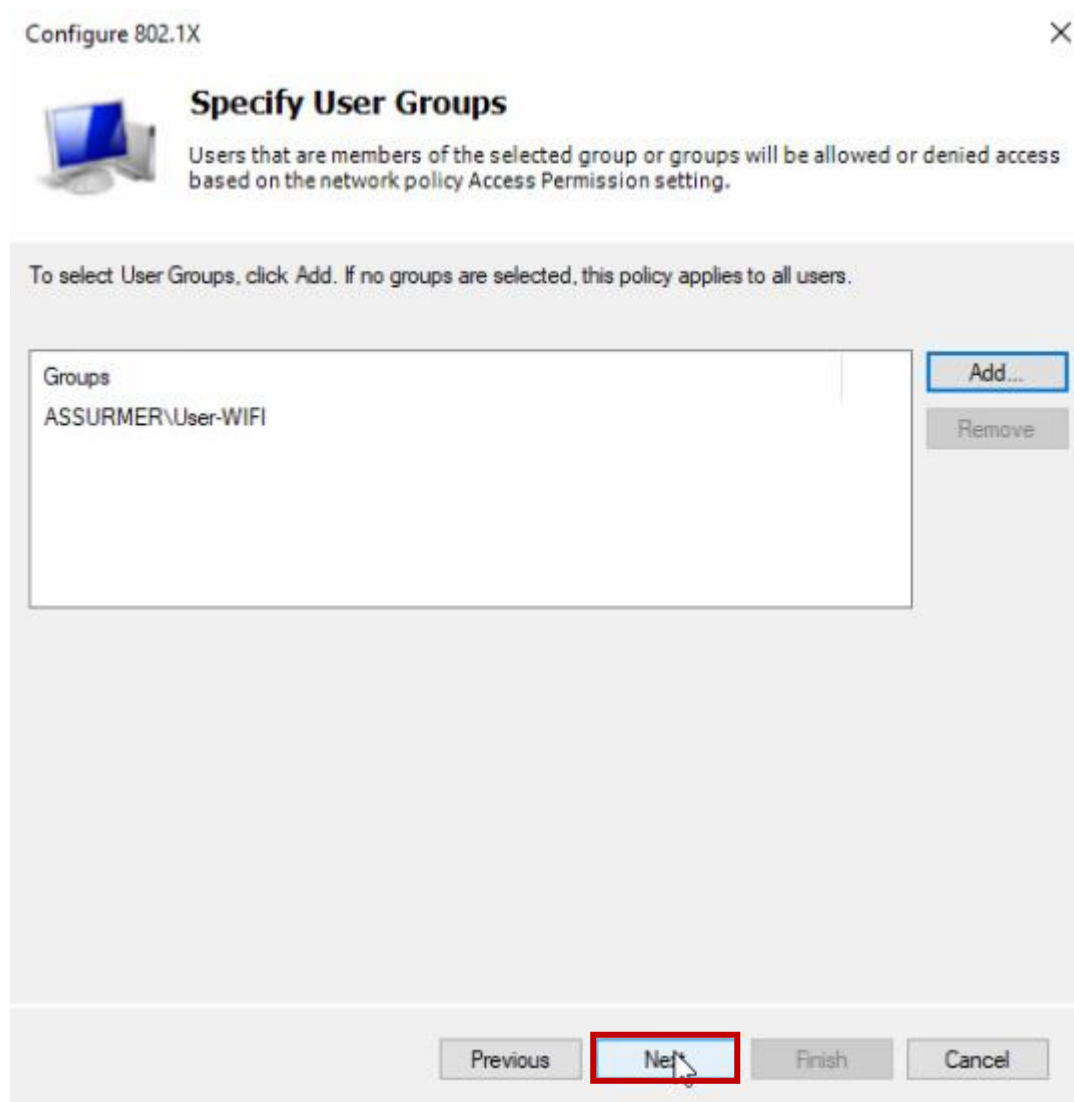
Select this object type:
Group

From this location:
assumer.IT

Enter the object name to select (examples):
User-WIFI

Advanced... OK Cancel

- Cliquer « Next »



Configure 802.1X

Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

Groups
ASSURMER\User-WIFI

Add... Remove

Previous Next Finish Cancel

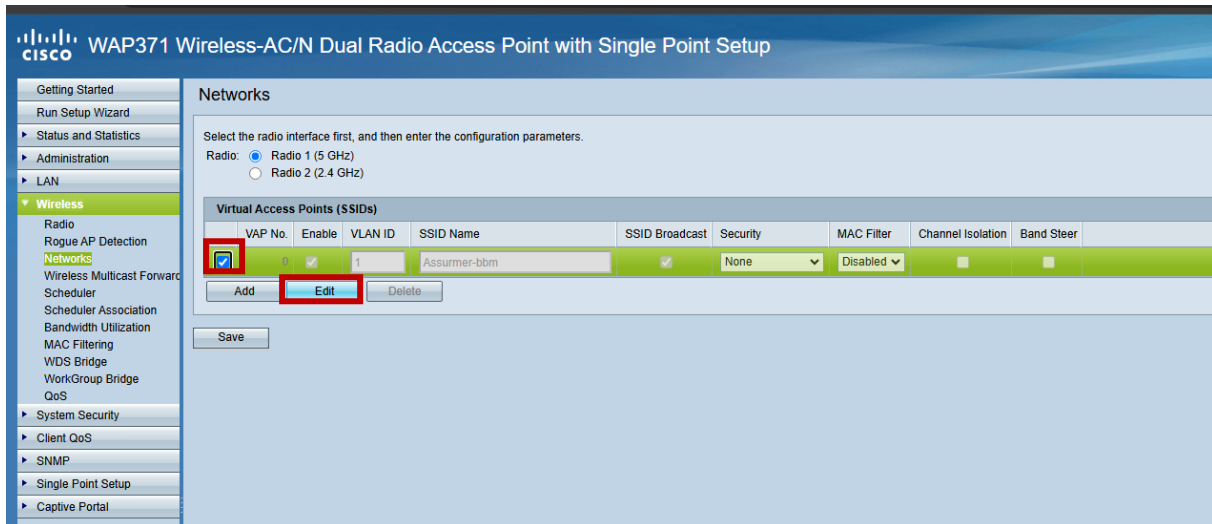
[Procédure] Configuration WiFi & RADIUS

- Cliquer « Finish »



Configuration borne WiFi pour RADIUS :

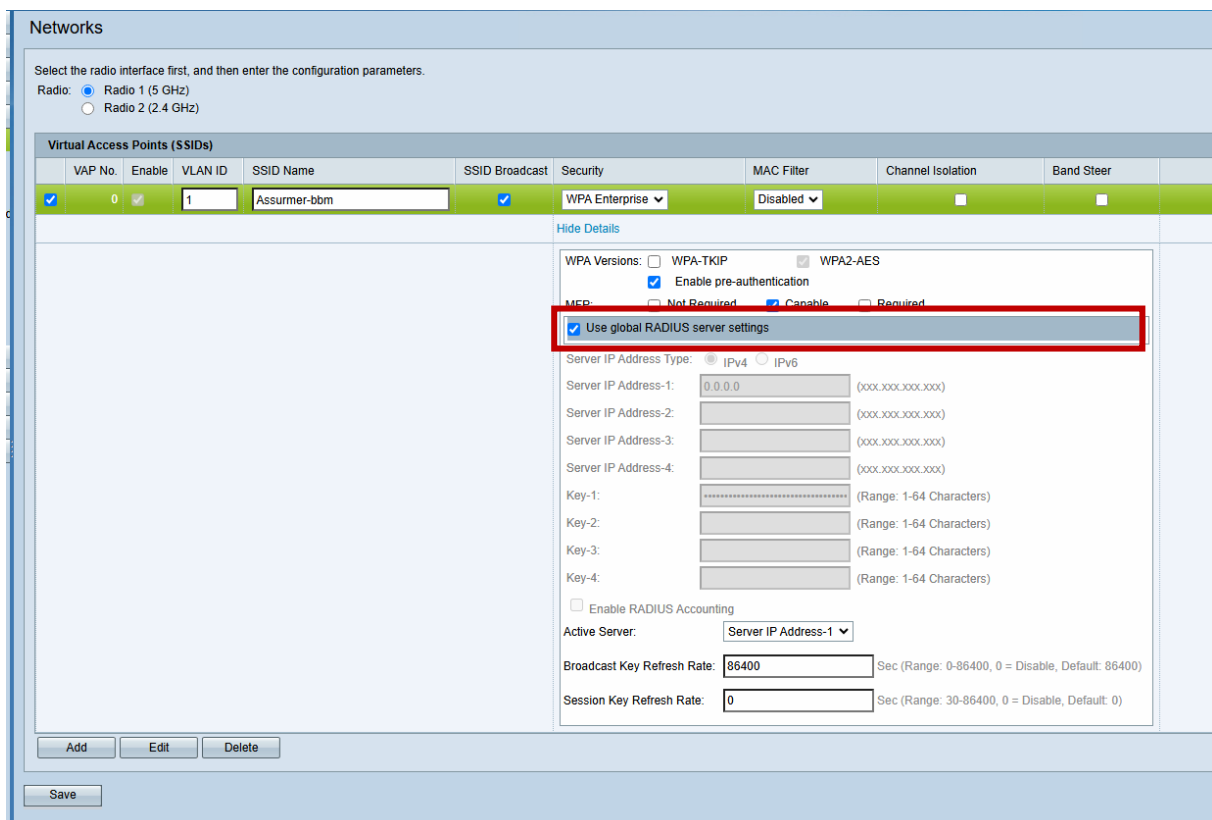
- Sur l'interface Web, sélectionner « Edit »



The screenshot shows the Cisco WAP371 configuration interface. On the left, the 'Wireless' menu is expanded, and 'Networks' is selected. The main area is titled 'Networks' and contains a table of Virtual Access Points (SSIDs). The first row is selected, and the 'Edit' button is highlighted with a red box. The table has columns for VAP No., Enable, VLAN ID, SSID Name, SSID Broadcast, Security, MAC Filter, Channel Isolation, and Band Steer.

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
0	☒	1	Assumer-bbm	☒	None	Disabled	☐	☐

- Cocher « Use global RADIUS server settings »

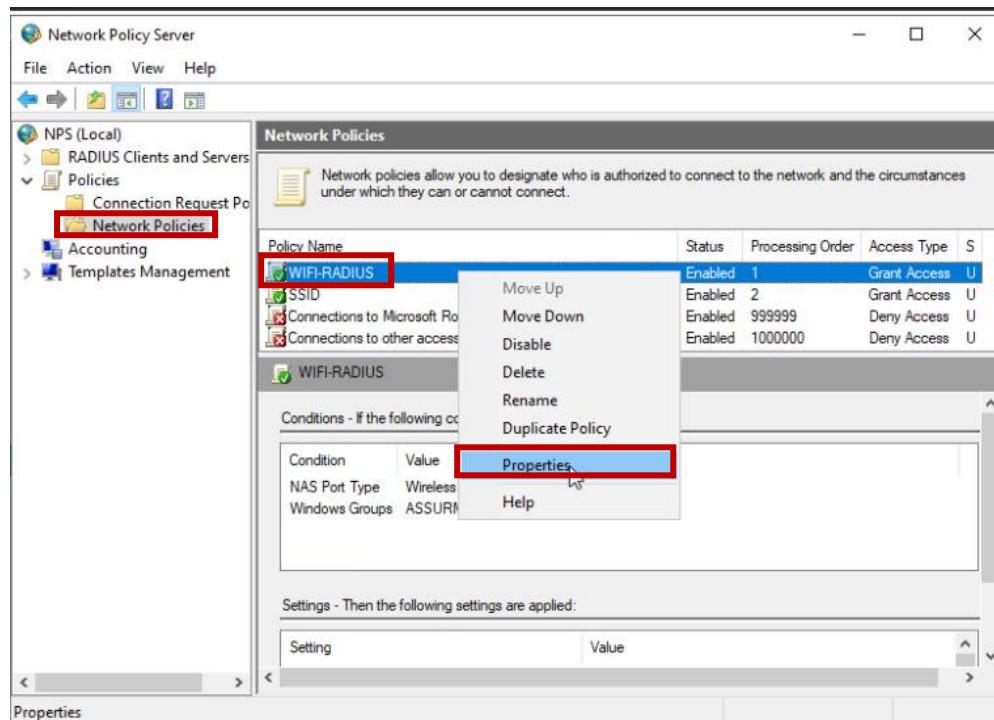


The screenshot shows the 'Hide Details' section of the configuration page. The 'Use global RADIUS server settings' checkbox is checked and highlighted with a red box. Below this, there are fields for Server IP Address Type (IPv4/IPv6), Server IP Address-1 through -4, Key-1 through -4, and Broadcast Key Refresh Rate. The 'Active Server' dropdown is set to 'Server IP Address-1'.

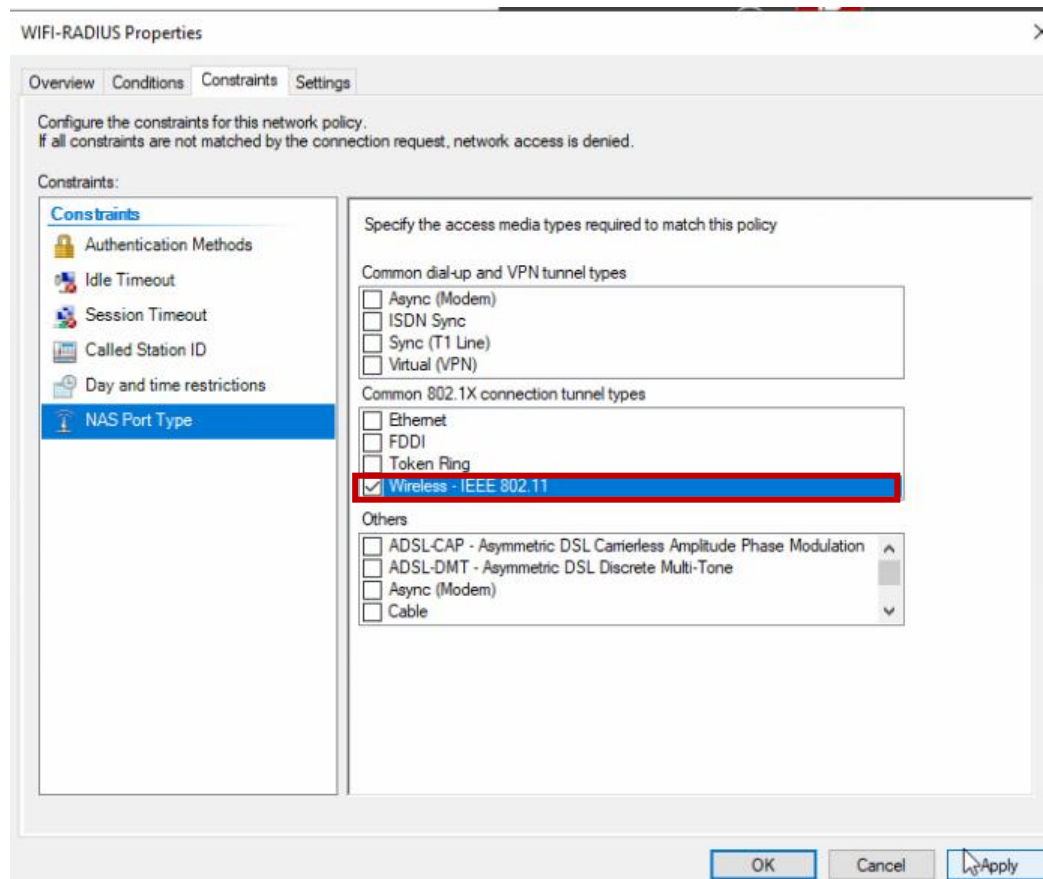
WPA Versions: ☐ WPA-TKIP ☒ WPA2-AES
☒ Enable pre-authentication
MFP: ☐ Not Required ☒ Capable ☐ Required
☒ Use global RADIUS server settings
Server IP Address Type: ☒ IPv4 ☐ IPv6
Server IP Address-1: 0.0.0.0 (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)
Key-1: (Range: 1-64 Characters)
Key-2: (Range: 1-64 Characters)
Key-3: (Range: 1-64 Characters)
Key-4: (Range: 1-64 Characters)
☐ Enable RADIUS Accounting
Active Server: Server IP Address-1
Broadcast Key Refresh Rate: 86400 Sec (Range: 0-86400, 0 = Disable, Default: 86400)
Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

[Procédure] Configuration WiFi & RADIUS

- Retourner sur NPS puis « Network Polities » puis clic-droit sur la politique RADIUS



- Sélectionner « Wireless – IEEE 802.11 » puis « Apply » et « OK »



[Procédure] Configuration WiFi & RADIUS

- Sur NPS et « Network Policies », supprimer les politiques par défaut

