

Configurando servidor RADIUS

Breve descrição do RADIUS:

O RADIUS é um protocolo que visa a autenticação, autorização e gestão de utilizadores, para acesso à rede ou serviços de rede (conceito AAA). RADIUS é normalmente usado para gerir e tornar mais seguro o acesso à Internet ou a redes internas. O Protocolo RADIUS baseia-se num sistema cliente/servidor. O Servidor de RADIUS utiliza o conceito AAA para gerir o acesso à rede. Este conceito refere-se aos processos de autenticação e autorização e contabilização (accounting) que são utilizados para estabelecer uma ligação à Internet ou utilizar aplicações de acesso à rede. Uma rede ou serviço de rede que utilize o protocolo RADIUS necessita de autenticação para permitir a ligação deste utilizador/dispositivo a esta. Após autenticação é determinado quais são os privilégios a que o utilizador autenticado está autorizado, e é contabilizado (accounting) e gravado o acesso deste no servidor RADIUS, de modo a haver uma melhor gestão e controle de acessos. O RADIUS tornou-se assim uma ferramenta necessária para controlo e segurança de acessos à rede de Internet ou redes internas. — Fonte: paginas.fe.up.pt

Requisitos:

Serviços Necessários:

1. [Active Directory Domain Services](#)
2. [AD Certificate Services](#)
3. [Network Policy and Access Services](#)

Portas:

Porta	Protocolo	Descrição
1645	UDP	RADIUS Authentication
1646	UDP	RADIUS Accounting
1812	UDP	RADIUS Authentication default port
1813	UDP	radius-acct, radacct, RADIUS accounting

Passo 1

Instalar e configurar o [Active Directory Domain Services](#)

Passo 2

Instalar o [Active Directory Certificate Services](#) e configurar o servidor como autoridade certificadora

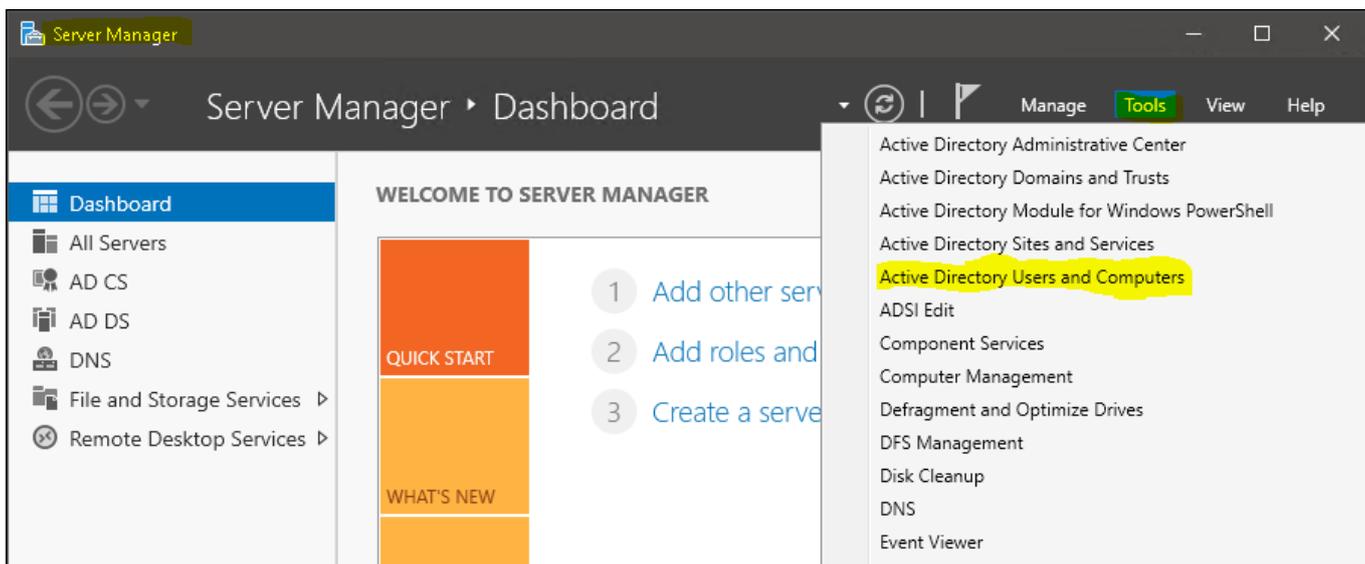
Passo 3

Instalar o **Network Policy and Access Services** e registra-lo no **Active Directory**

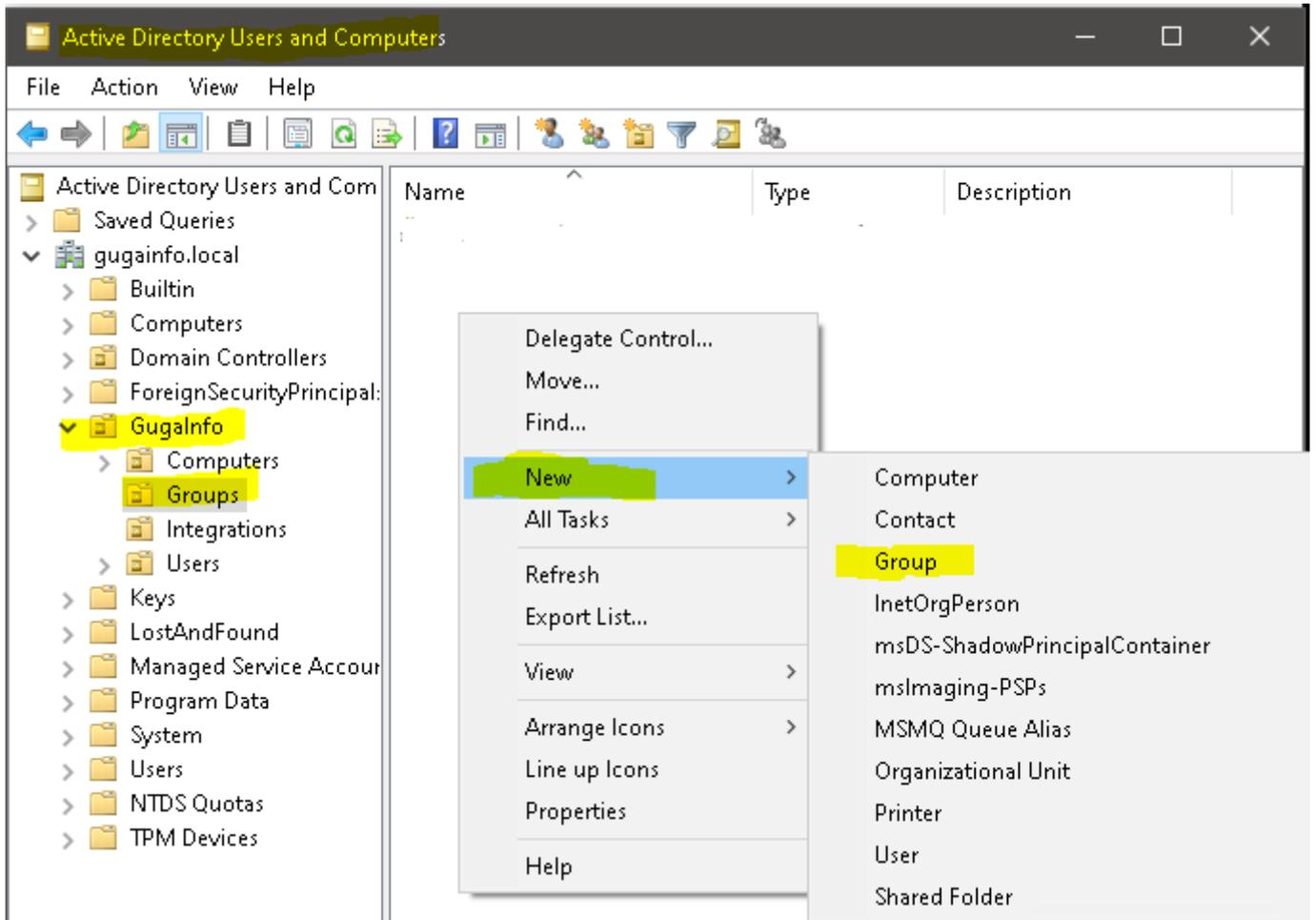
Passo 4

Criar grupo para computadores que terão permissão para conexão através do RADIUS

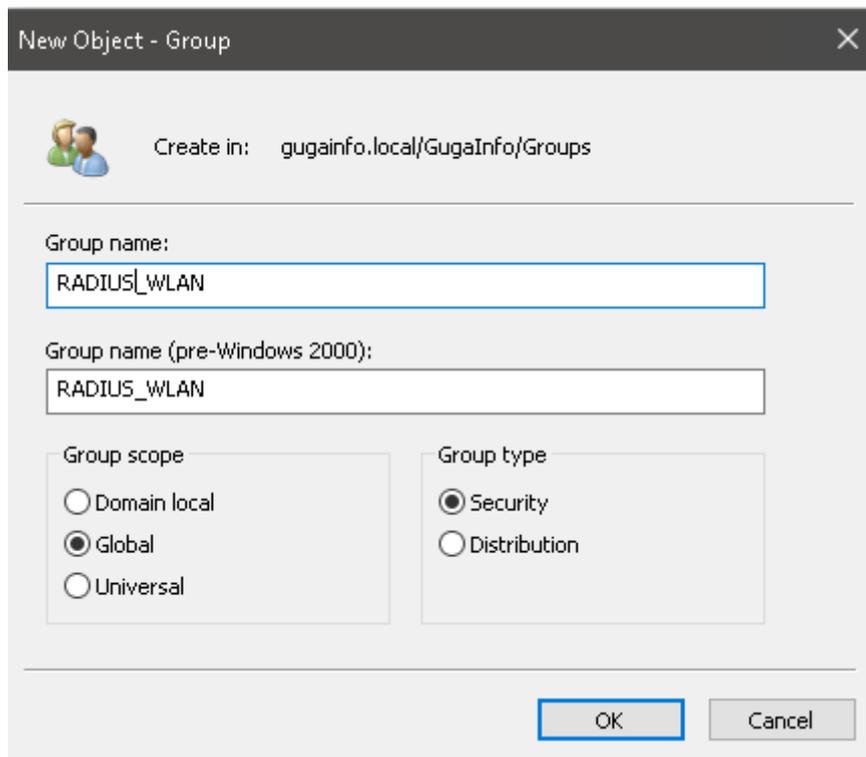
Gerenciador do Servidor » Ferramentas » Usuários e computadores do Active Directory



Escolher OU de sua Preferência, clicar com o botão direito -> Novo -> Grupo



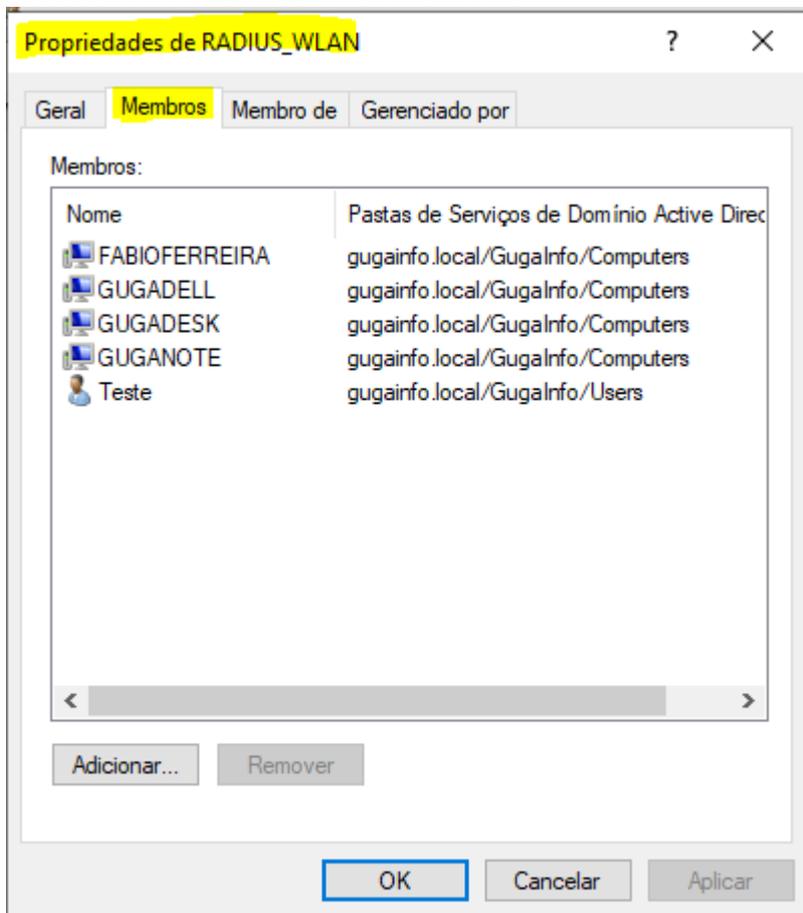
Dar nome ao grupo, ok



Passo 5

Adicionar membros ao grupo criado para acesso através do RADIUS

- **Usuários** → Podem ser utilizado para dispositivos que não façam parte do domínio
- **Computadores** → Permitindo que computadores do domínio se autenticuem sem necessidade de inserir credenciais



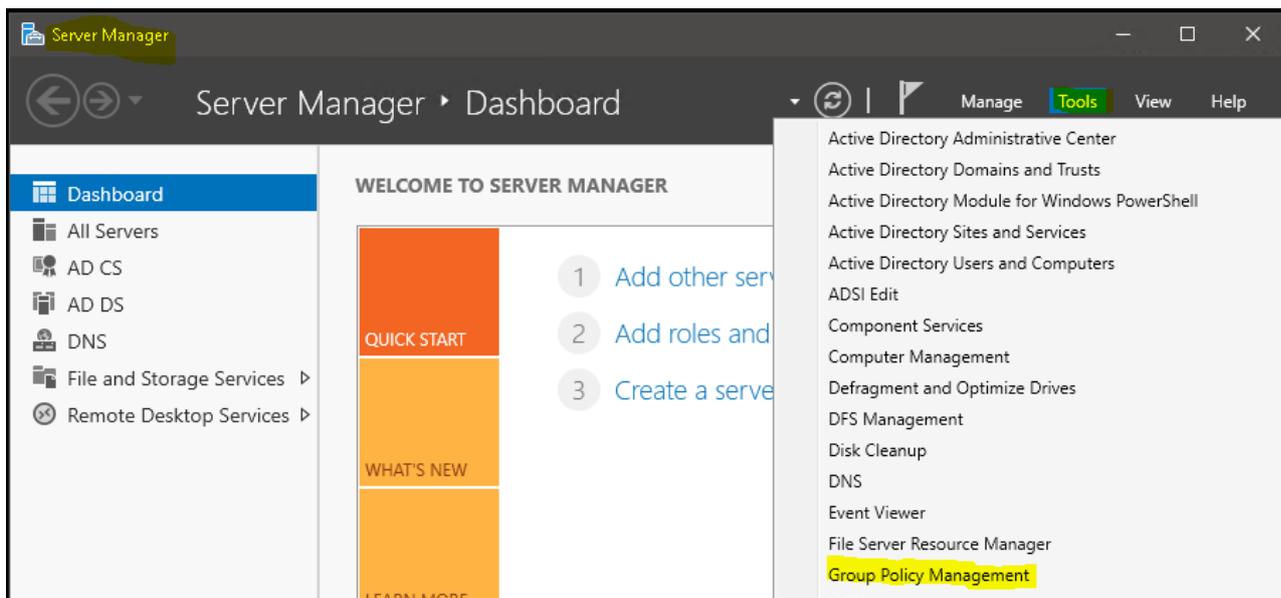
Passo 6

Liberar portas no firewall do Windows para comunicação com o RADIUS

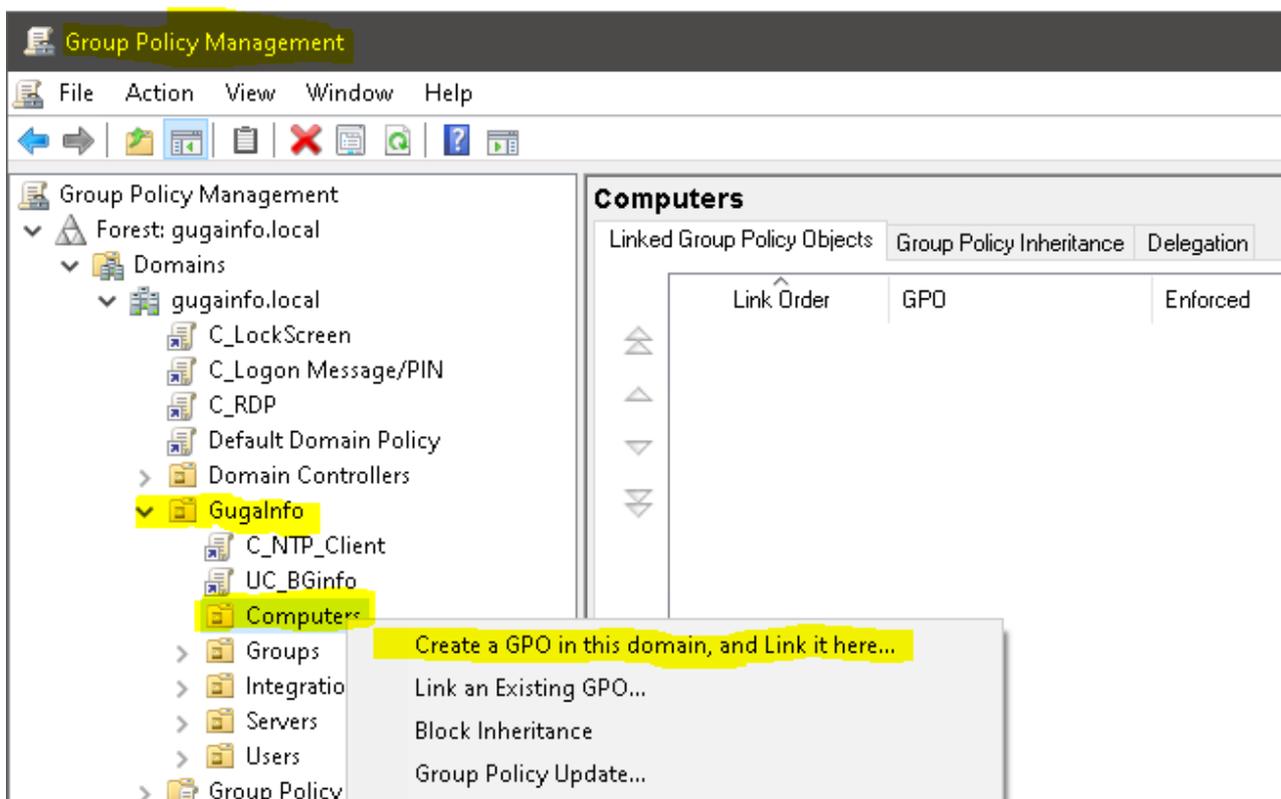
- **CMD:**
 - netsh advfirewall firewall add rule name="Permir RADIUS" dir=in action=allow protocol=UDP localport=1645-1646,1812-1813 enable=yes

Passo 7

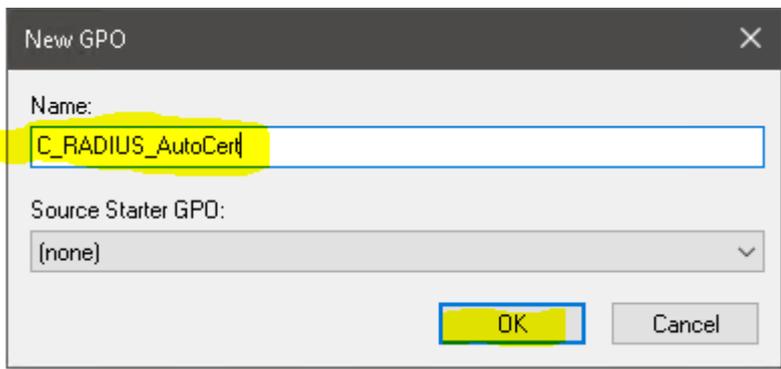
Criar GPO para geração automática de certificado digital para as máquinas que se autenticarão através do RADIUS.



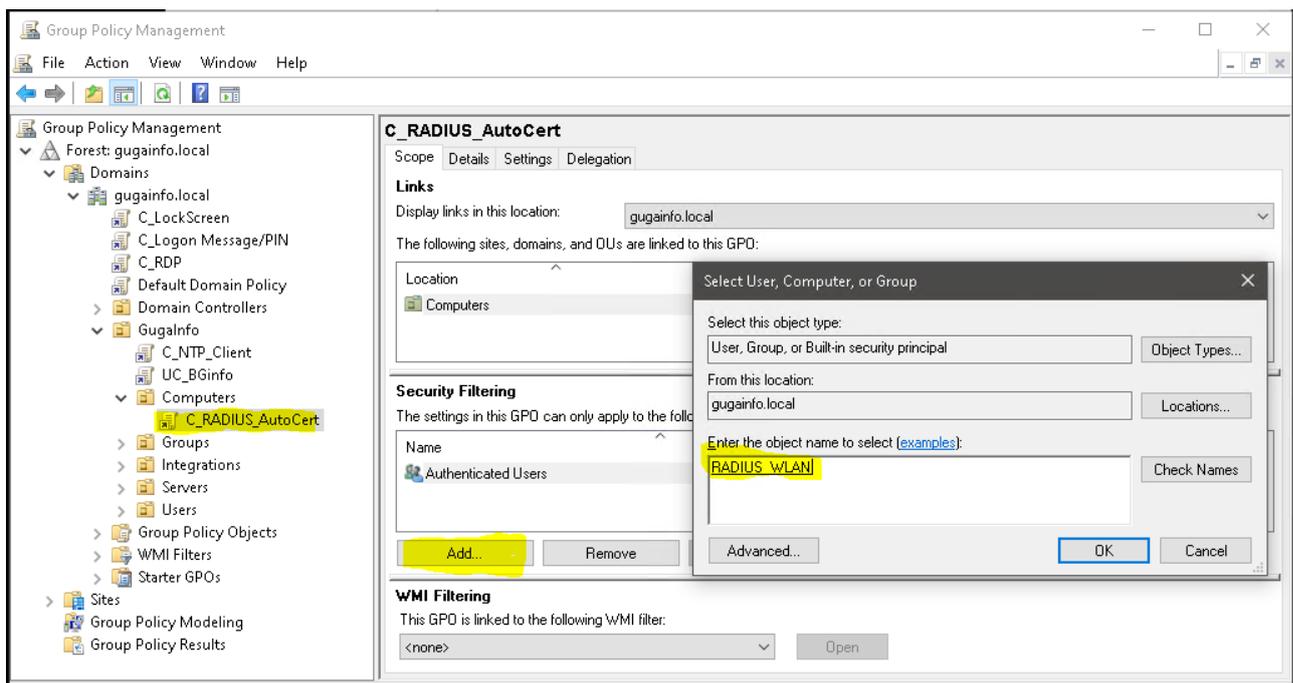
Criar GPO na mesma OU onde ficam os computadores



Defina um nome como preferir

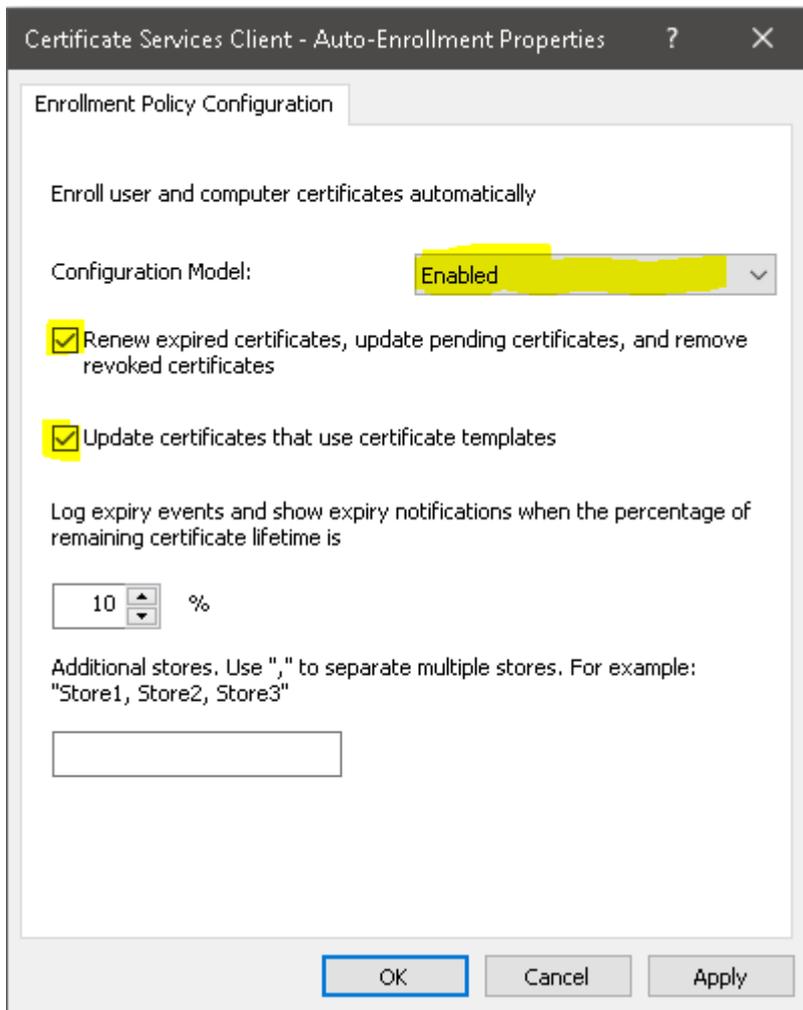


Adicione o grupo criado anteriormente ao filtro de segurança da GPO



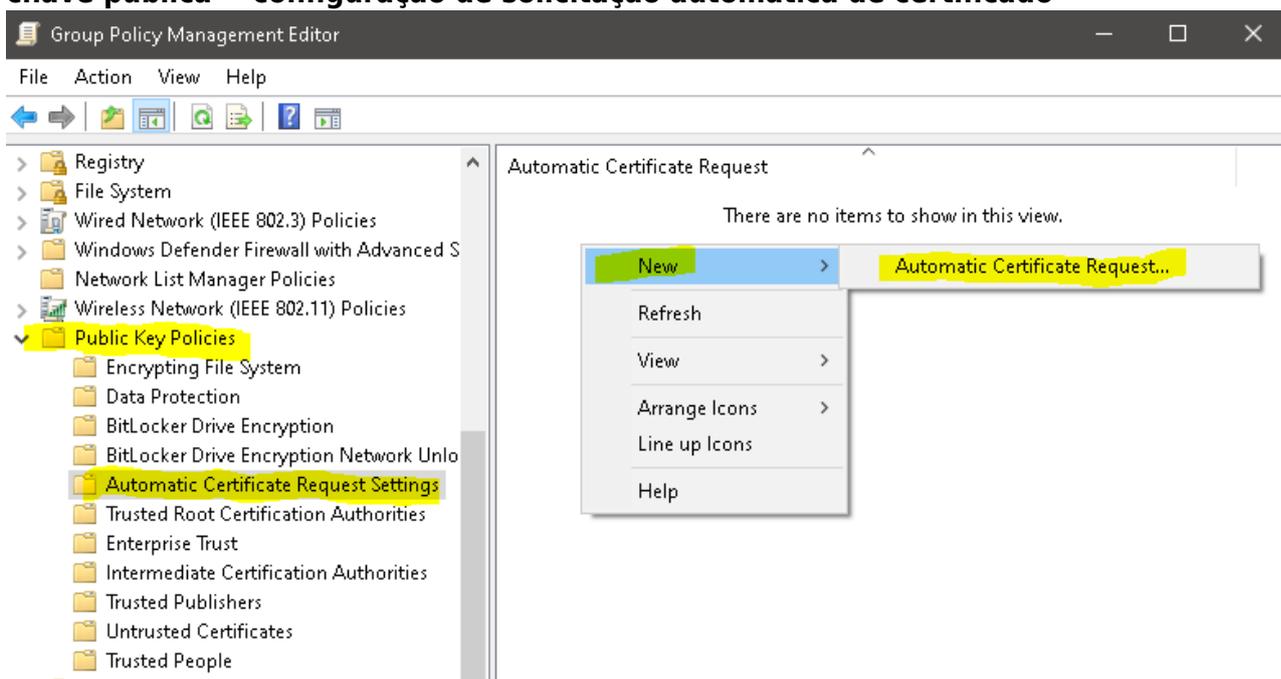
Editar GPO para ativar "Cliente Serviços Certificado - Registro Autom."

- Configuração de computador → Políticas → Configurações de Segurança → Políticas de chave pública
- Habilitar e marcar as opções “Renovar certificados expirados” e “Atualizar certificados que usam modelos”

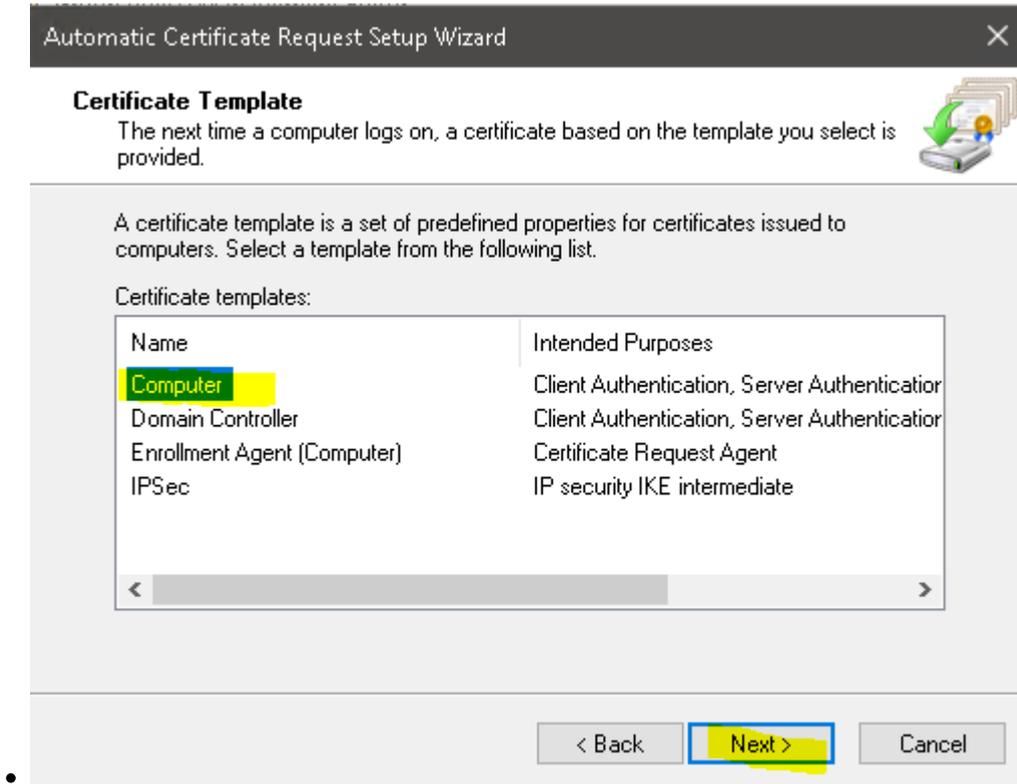


Criar nova configuração de solicitação automática de certificado

- **Configuração de computador → Políticas → Configurações de Segurança → Políticas de chave pública → configuração de solicitação automática de certificado**



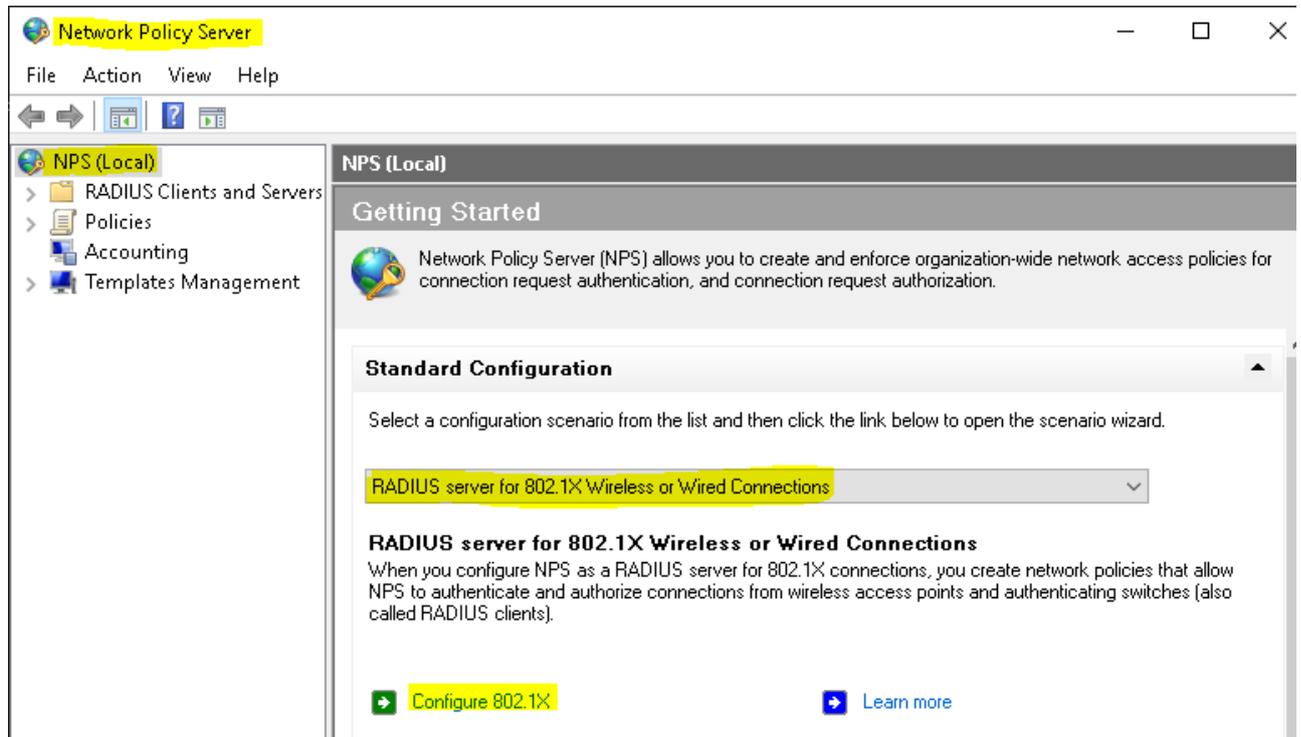
Avançar, escolher a opção "Computador", avançar e concluir



Passo 8

Configurar o Servidor de Políticas de Rede (NPS)

- Iniciar → Ferramentas administrativas → Servidor de Políticas de Rede
- Selecionar Uma situação de configuração na lista
 - Escolher a opção: Servidor RADIUS para Conexões 802.1X com/sem Fio



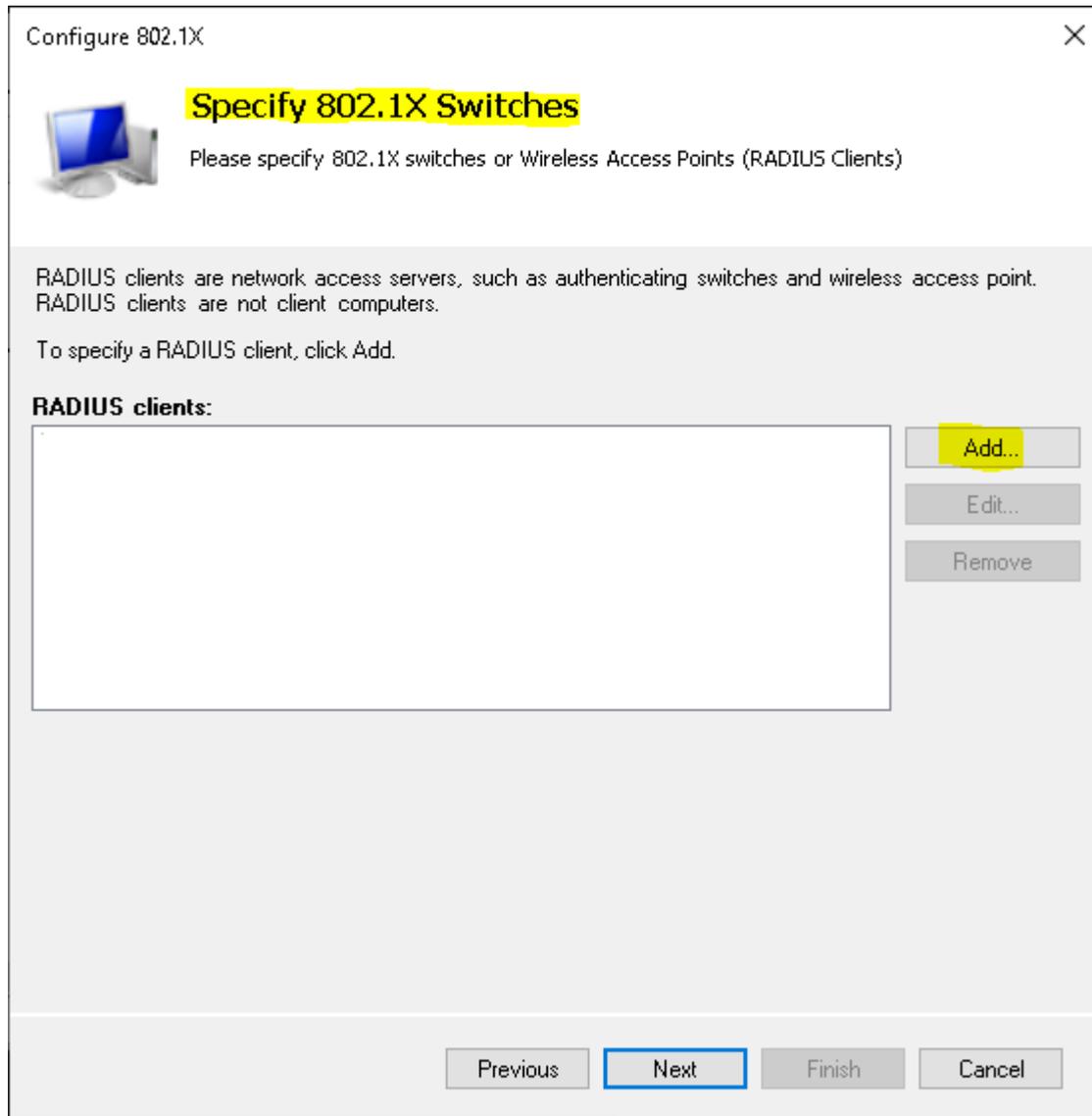
Configurar 802.1X

- **Selecionar Tipo de Conexões 802.1X**
 - **Conexão sem Fio Seguras**
 - **Definir um nome como preferir**

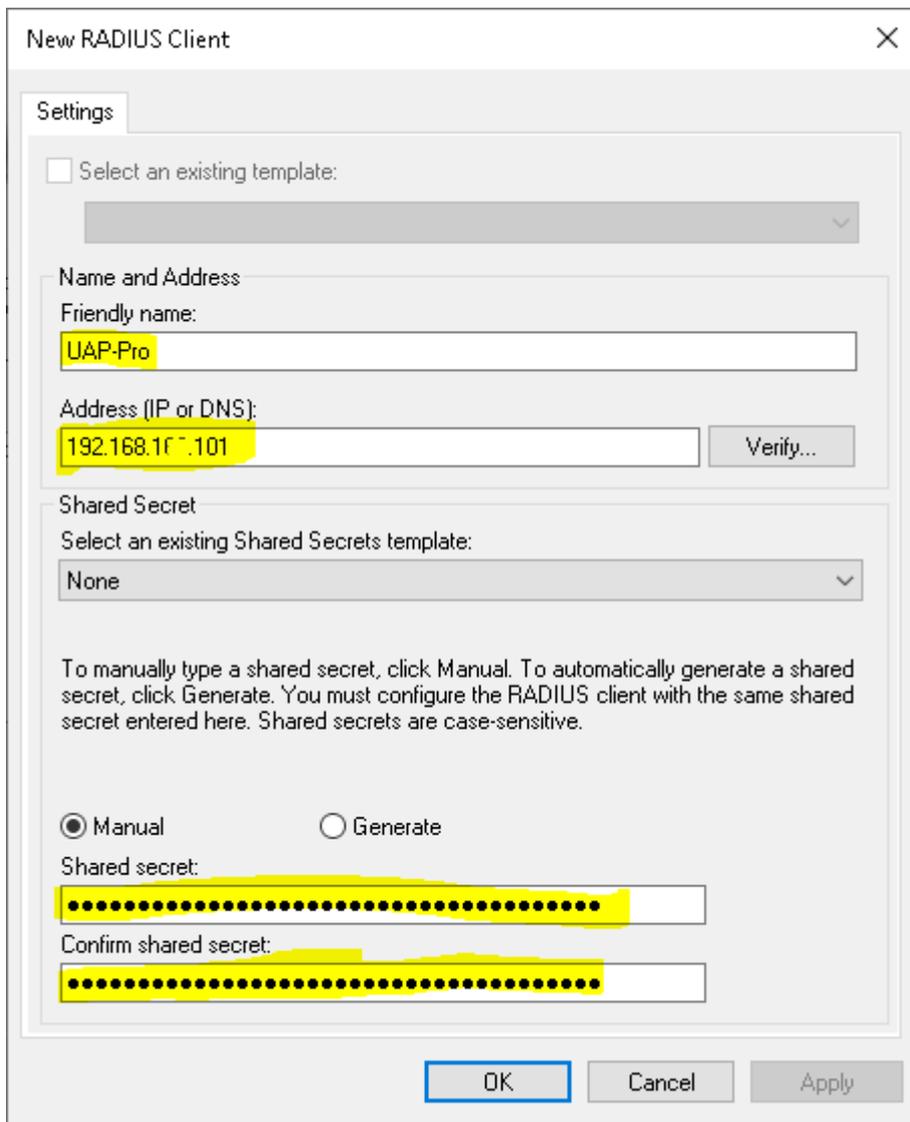


Especificar Switches 802.1X

- Adicionar Clientes RADIUS

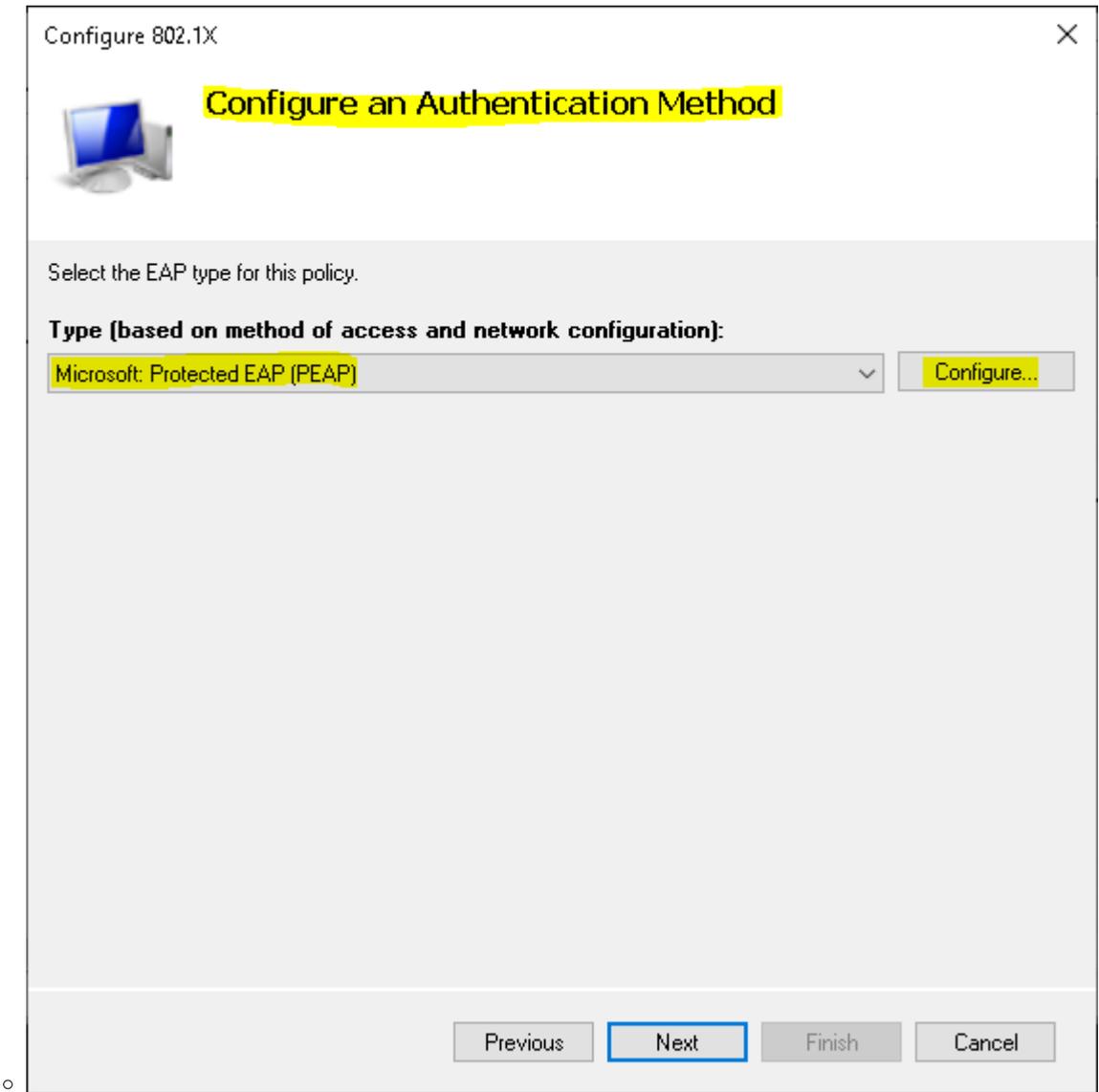


- **Inserir nome amigável**
- **Inserir Endereço IP do dispositivo (AP) que se conectará ao servidor RADIUS**
- **Definir manualmente ou gerar uma senha para esta comunicação entre o cliente (AP) e o servidor RADIUS**

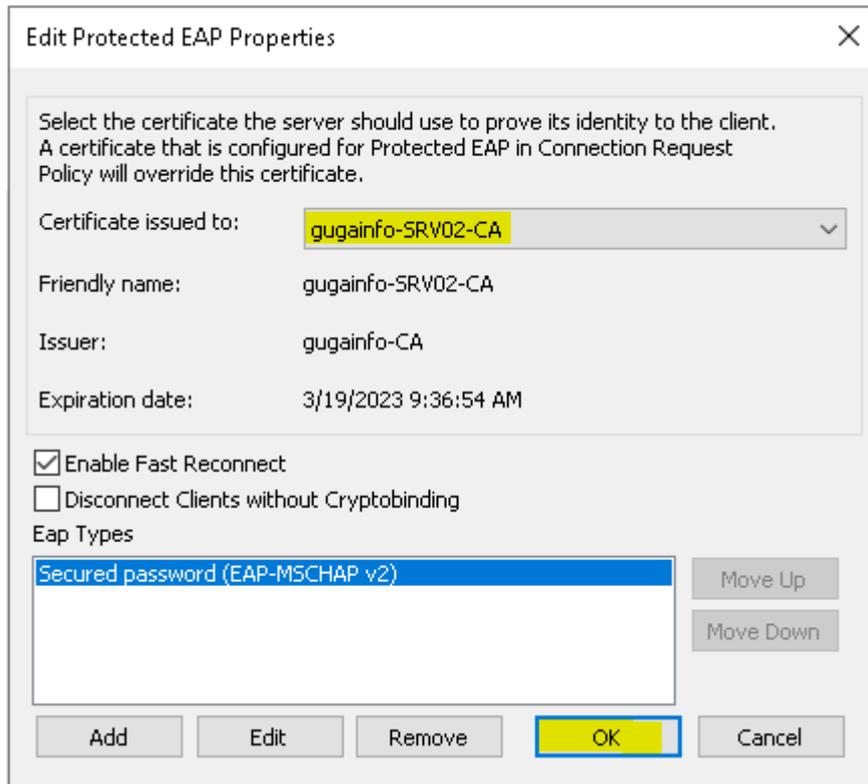


Configurar um Método de Autenticação

- Escolher o tipo
 - Selecionar o: **“Microsoft Protected EAP (PEAP)”**



- **Editar Propriedades do PEAP**
- **Em: "Certificado emitido para:" Escolher sua Autoridade certificadora (CA) criada anteriormente**



Especificar Grupos

- Adicionar Grupo que criamos anteriormente para acesso ao RADIUS

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

GUGAINFO\RADIUS_WLAN

Add... Remove

Select Group

Select this object type:
Group Object Types...

From this location:
gugainfo.local Locations...

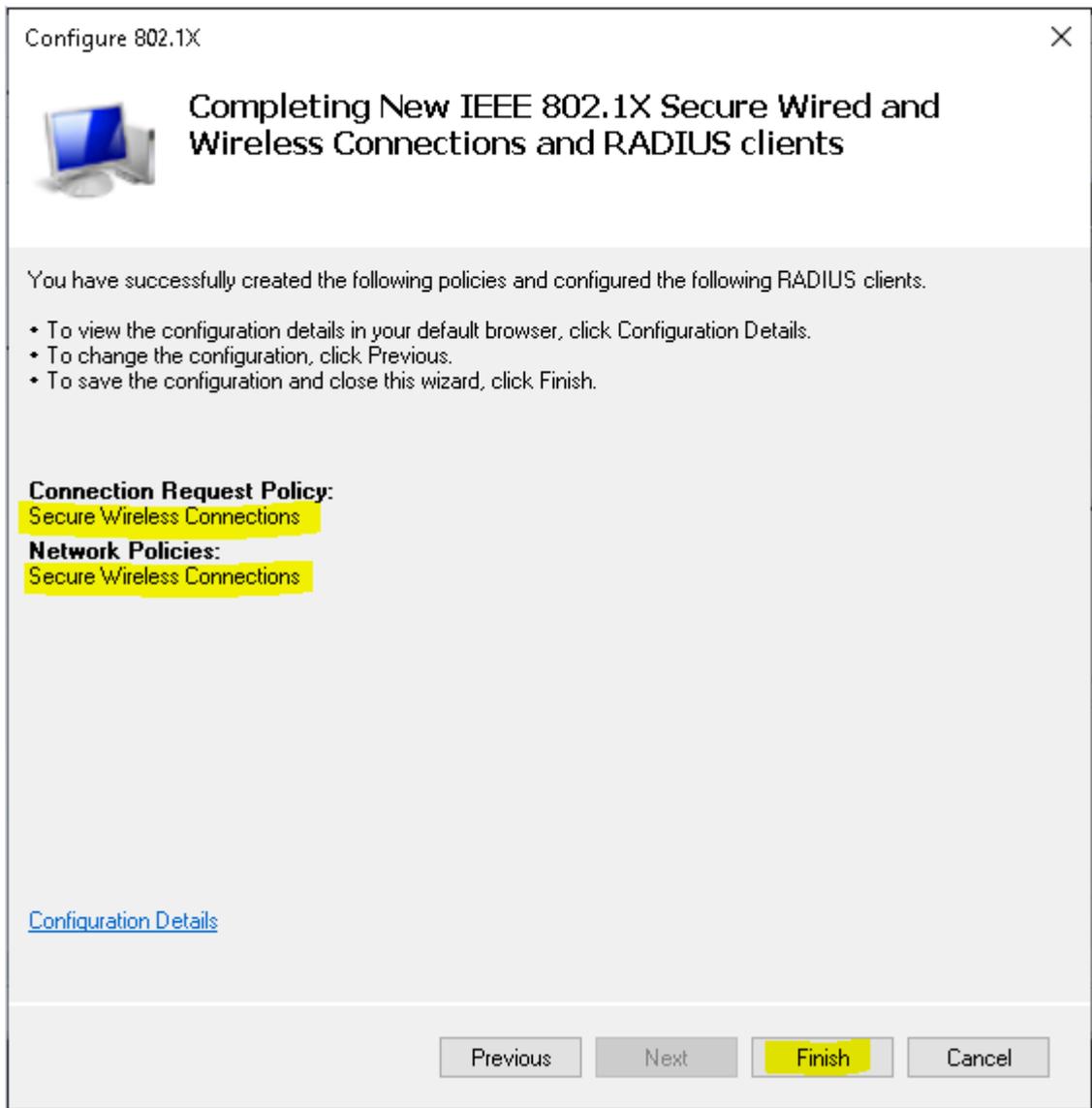
Enter the object name to select (examples):
RADIUS_WLAN Check Names

Advanced... OK Cancel

Previous Next Finish Cancel

Handwritten annotations: 1 (pointing to Add...), 2 (next to RADIUS_WLAN), 3 (next to OK), 4 (next to Finish)

Avançar e finalizar



Configurar Clientes

Exemplo de configuração de cliente RADIUS Unifi

From:
<https://gugainfo.com.br/> - **Gugainfo**

Permanent link:
https://gugainfo.com.br/doku.php?id=windows:win_server_2019:radius

Last update: **2022/03/26 12:00**

