

MICROSOFT NETWORK POLICY SERVER

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security.

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

Microsoft Network Policy Server

[NPS](#) [Network Policy Server](#) [RDS](#) [Remote Desktop Services](#) [RDWeb](#) [RDGateway](#) [Session Host](#) [RemoteApp](#) [Remote Application](#) [Remote Desktop](#) [Remote Desktop Gateway](#)

1. Overview

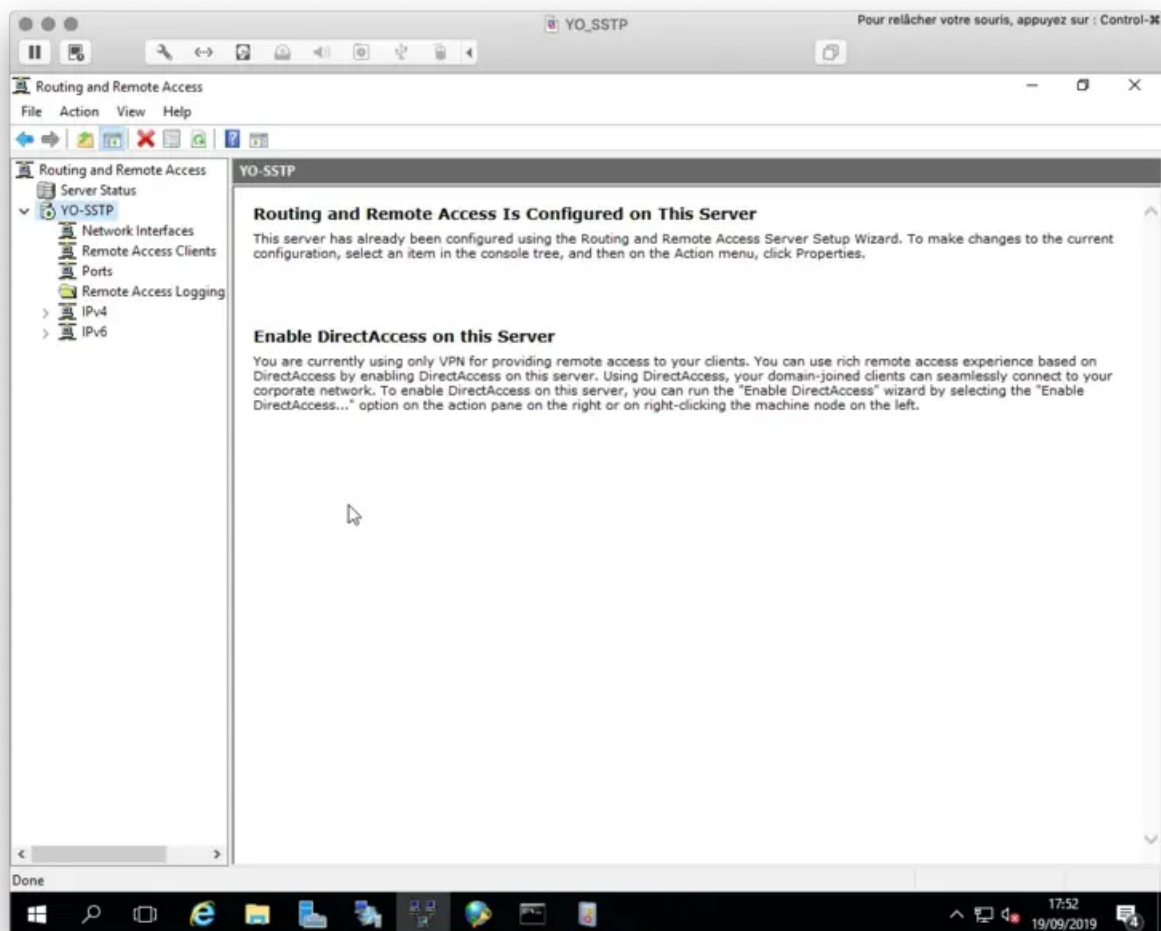
In that documentation, we will explain how to configure OpenOTP multi-factor authentication on your Microsoft Network Policy Server. As a practical example, we will configure NPS with Microsoft Remote Access Server for VPN use.

For this recipe, you will need to have a WebADM, OpenOTP and Radius Bridge installed and configured. Please refer to [WebADM Installation Guide](#), [WebADM Manual](#) and [Radius Bridge Manual](#) for instructions on these. Your Microsoft Network Policy Server and Remote Access Server should be installed and configured for VPN (PPTP, SSTP) use.

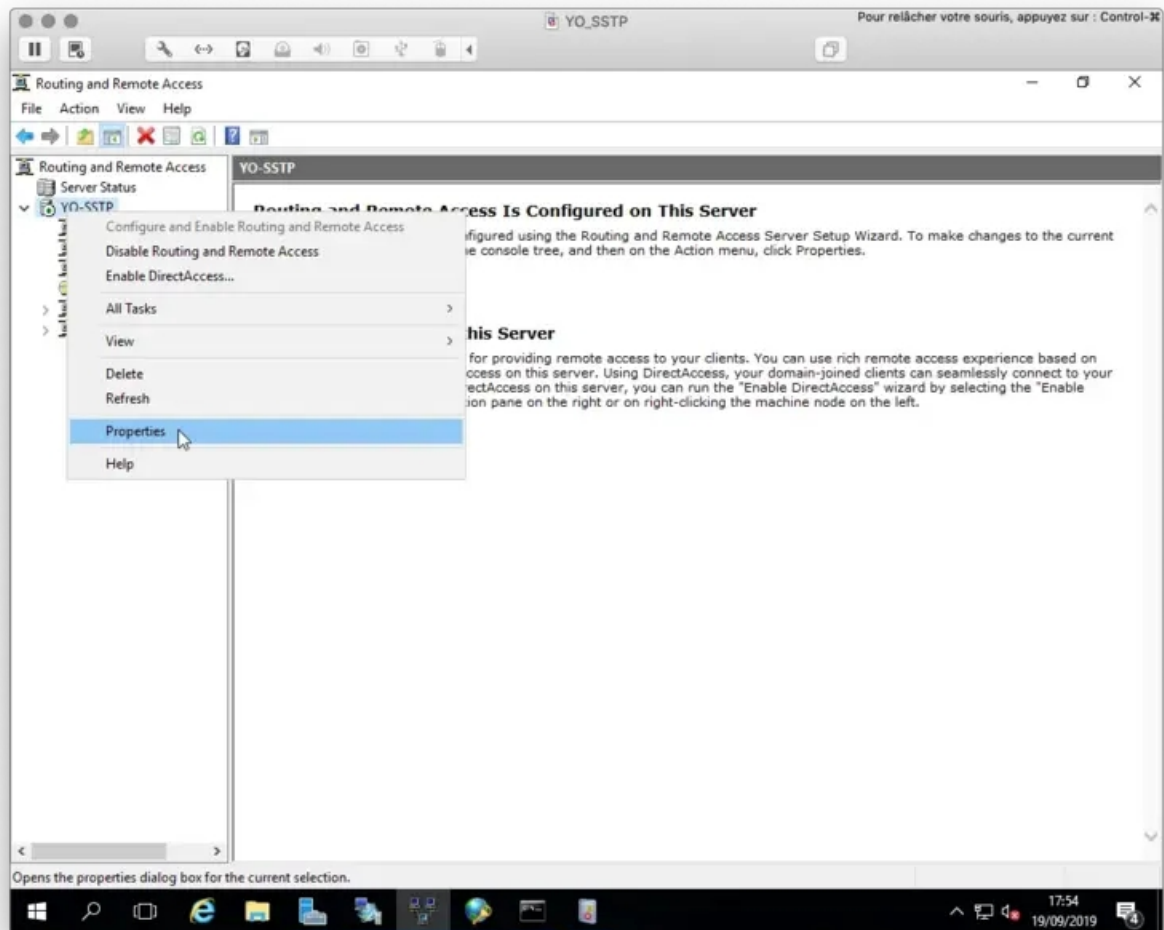
Note that only two multifactor authentication methods can be used to authenticate your Windows VPN client with OpenOTP: Simple push “Accept/Reject” or concatenated LDAP+OTP password. NPS supports RADIUS challenge, but Windows VPN Client does not, so you can not prompt additional credentials during the authentication request to ask for the OTP.

2. Configure MS VPN with NPS

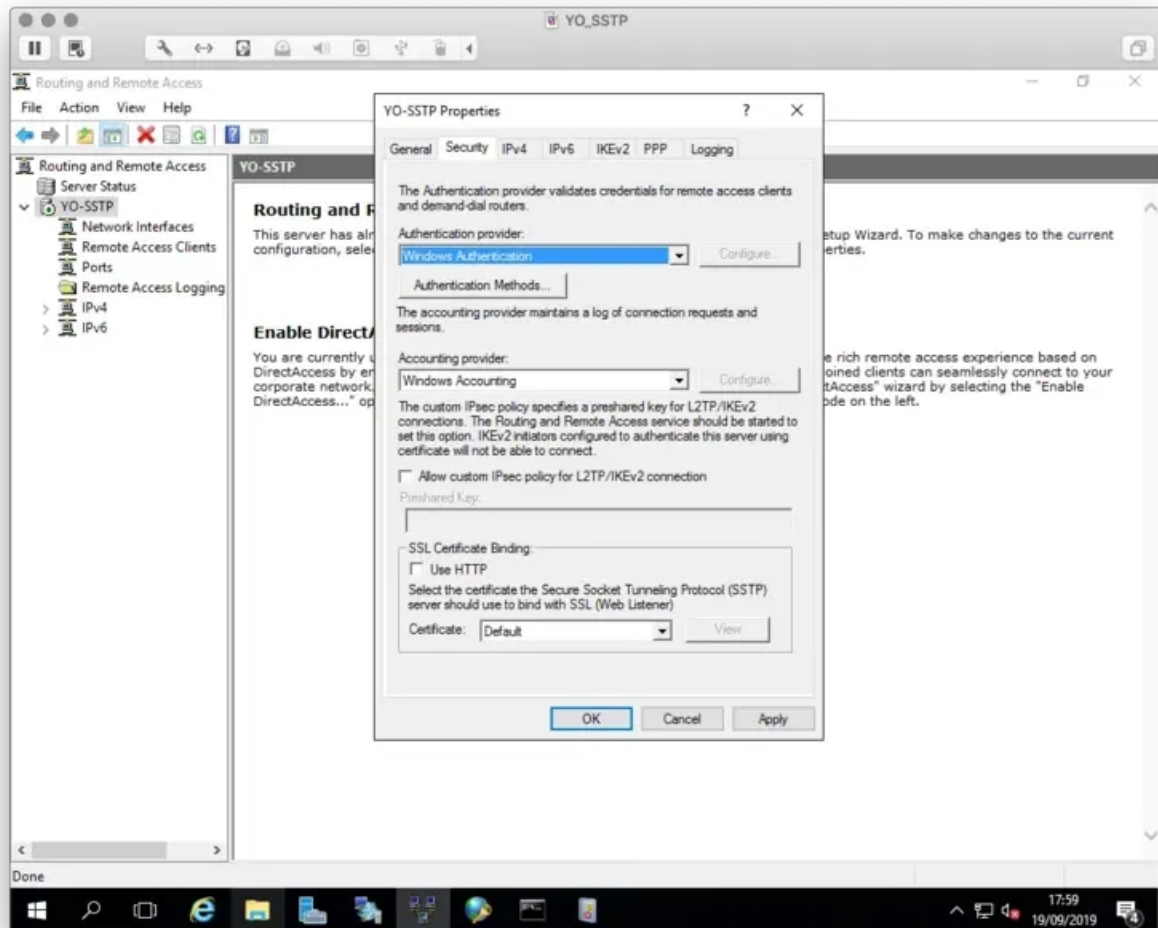
Open the Routing and Remote Access console from your Windows VPN server



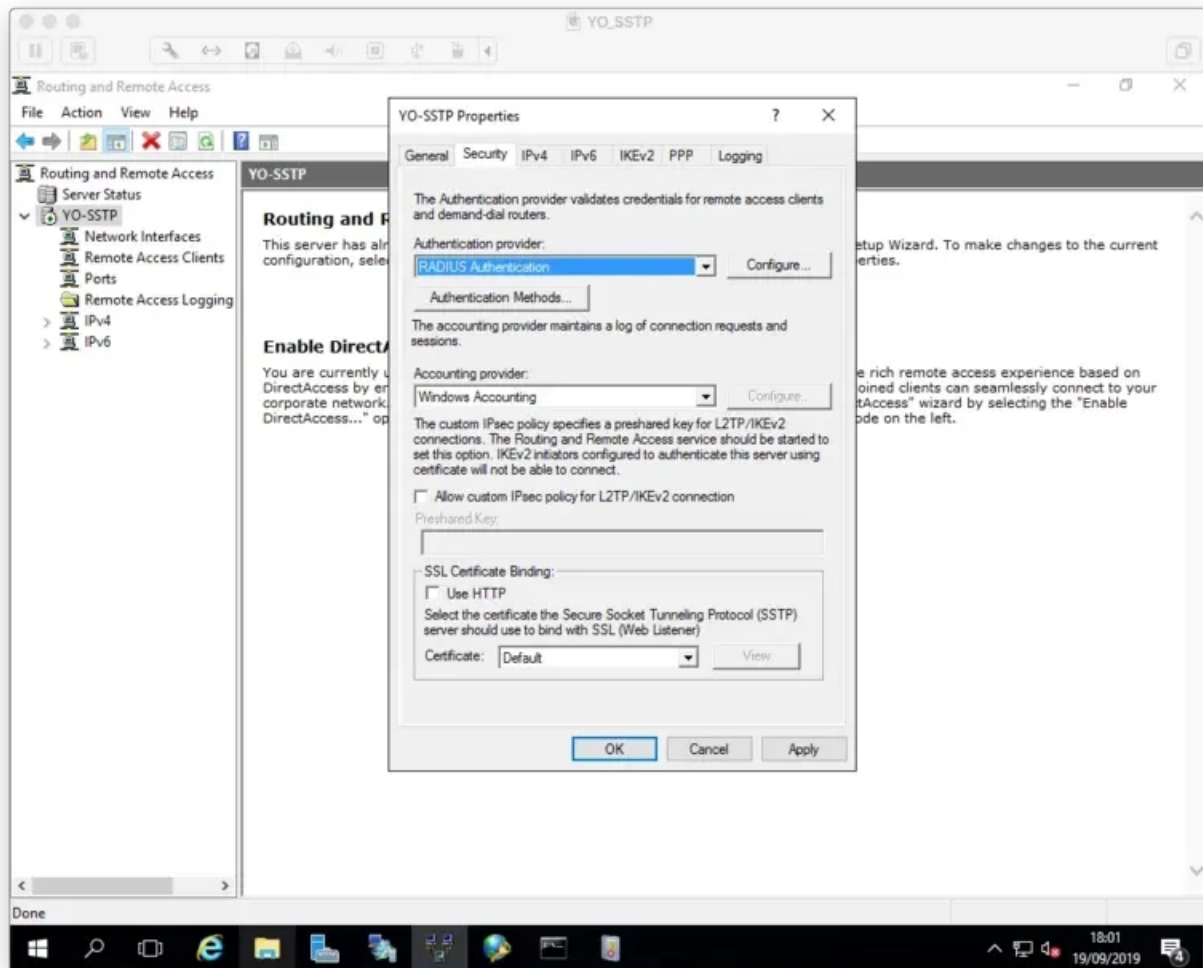
Right-click on your VPN > **Properties**



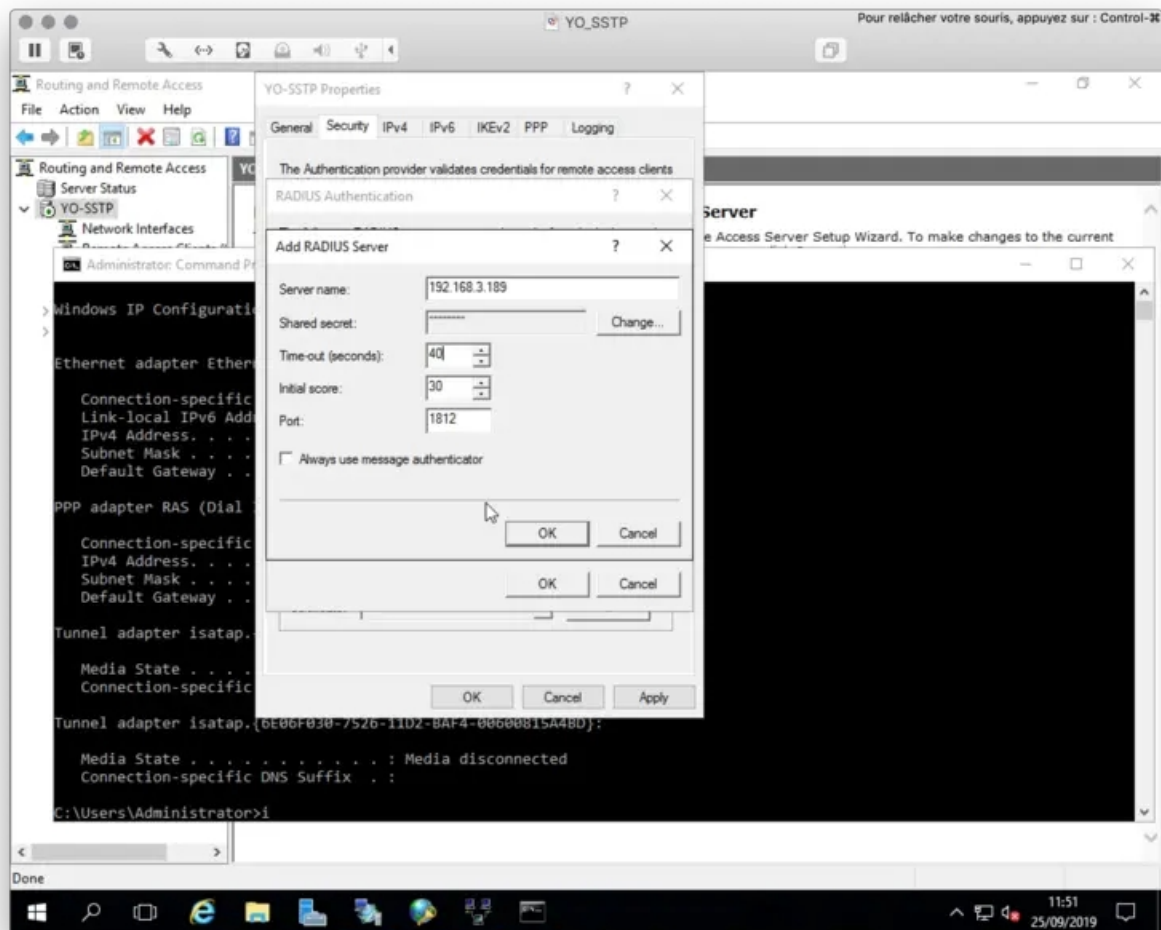
Click on **Security** tab



We will now change the **Authentication Provider** from Windows Authentication to RADIUS Authentication and click on **Configure** button.



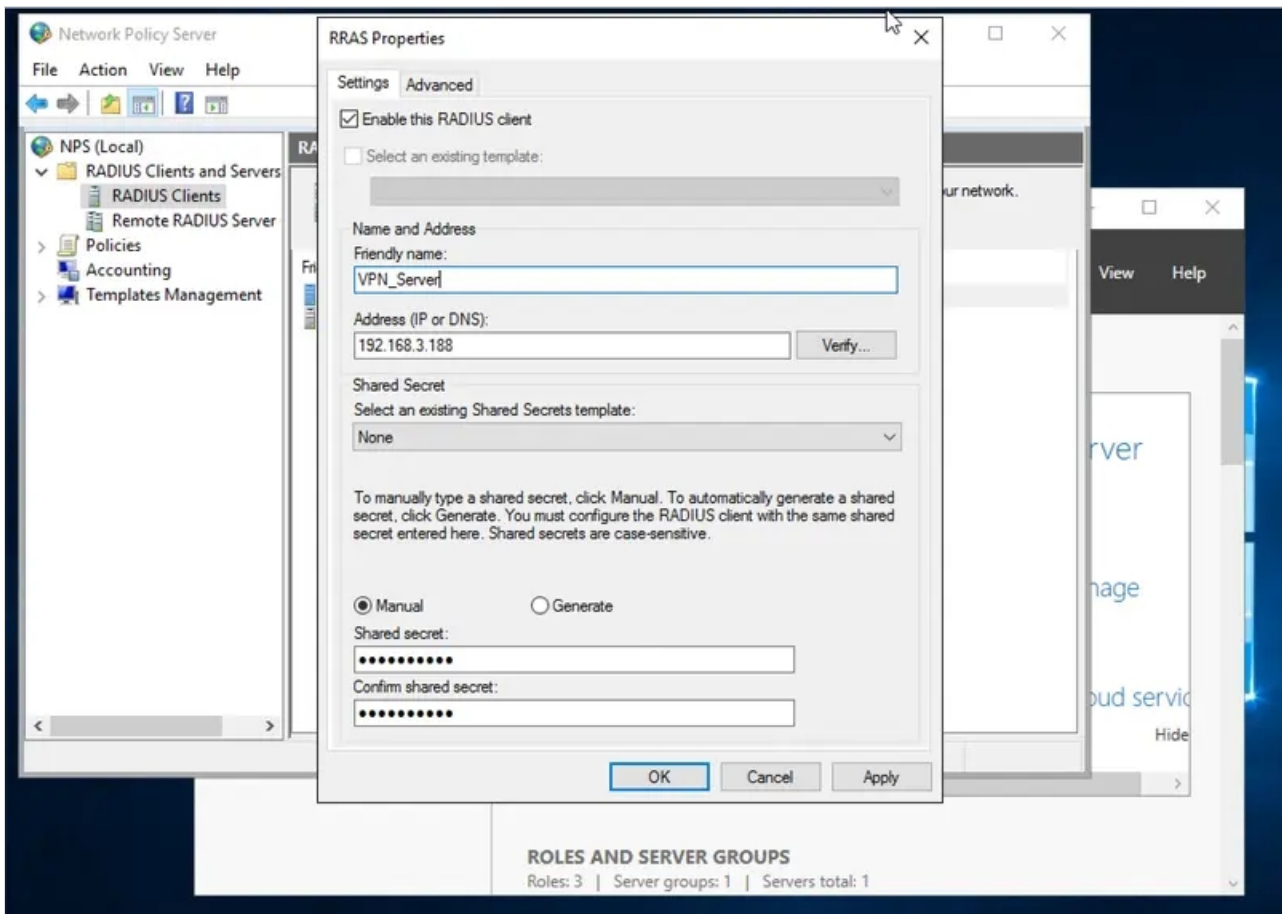
On the following screen, configure the IP of your NPS server and a secret. Adjust the timeout according to the screenshot. If you are using Simple Push based authentication, it is important that the timeout exceeds the push timeout configured in WebADM.



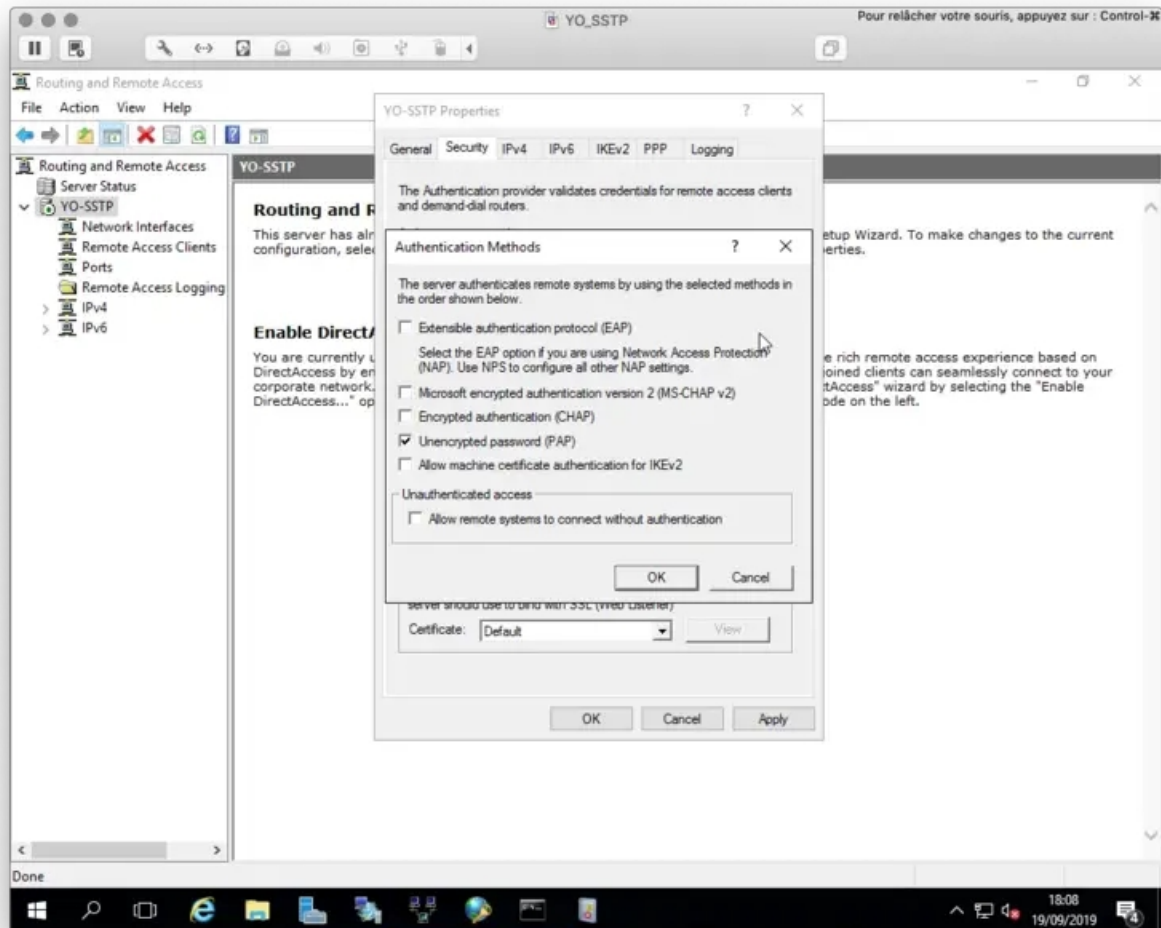
3. NPS Configuration

3.1 Add your VPN server as RADIUS Client

On NPS your VPN server is configured as a Radius client.



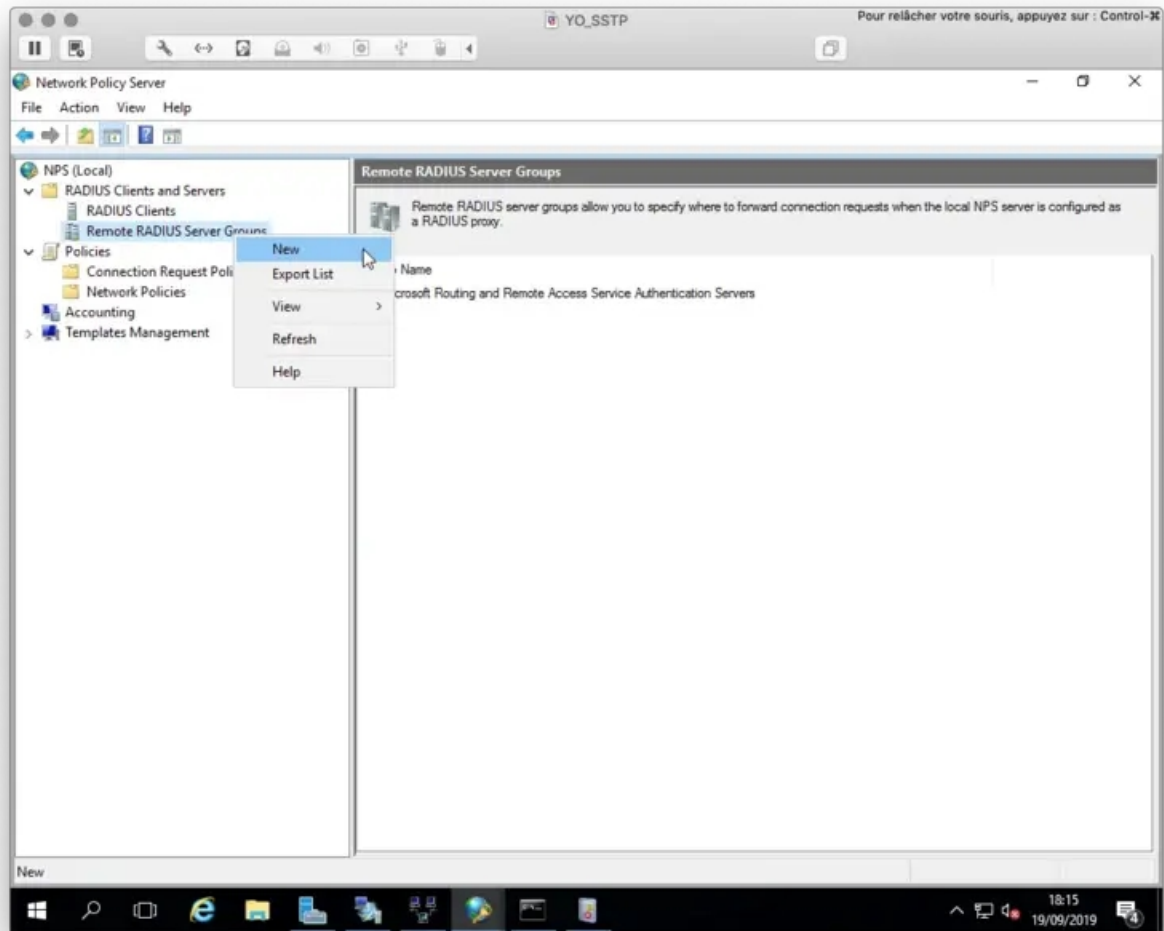
The secret must be the same as the one you configured on your VPN server. Go back to your VPN properties and click on **Authentication Methods** button. Configure **PAP** as **Authentication Method** like below:



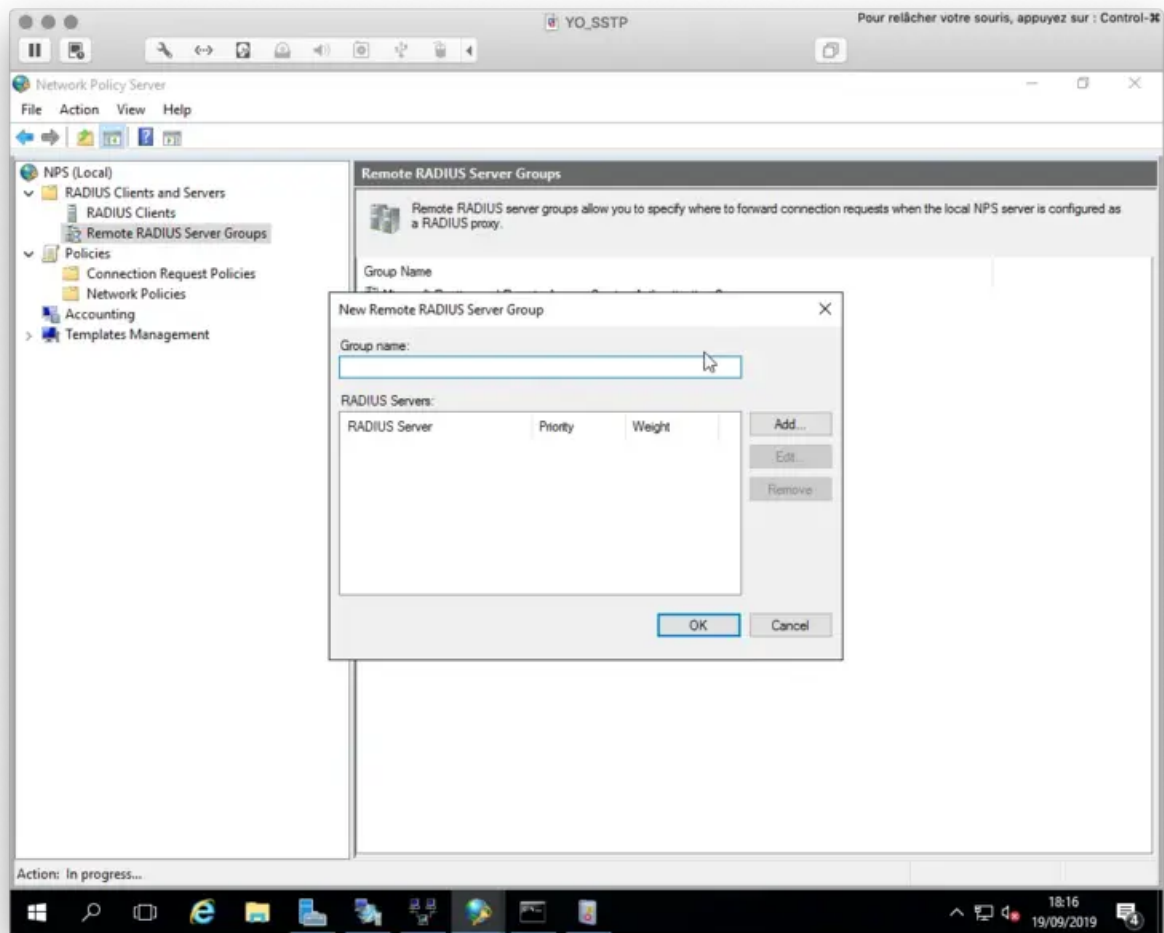
Apply the configuration. This concludes the VPN server part.

3.2 Add a new Remote RADIUS Server

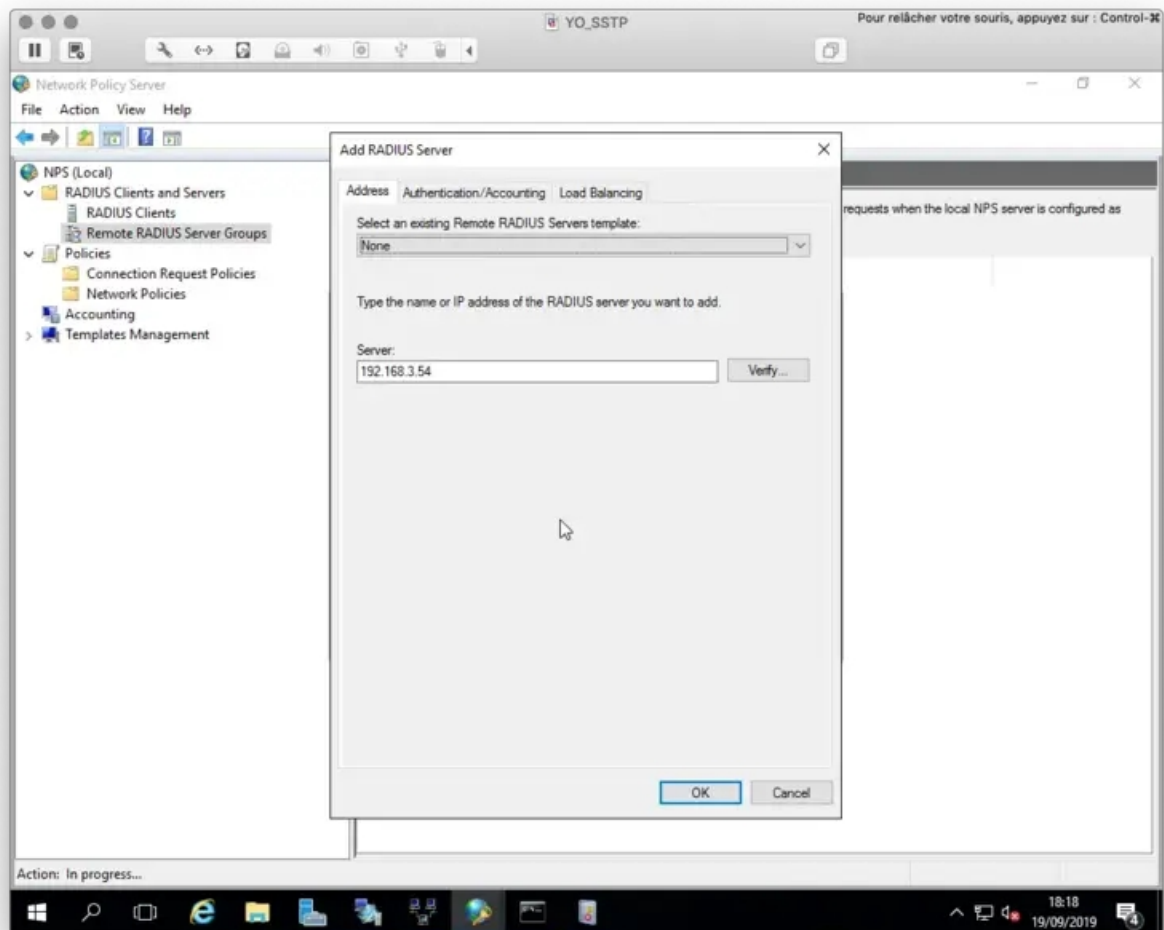
Open the NPS console, we will now configure a **Remote RADIUS Server**. Right click on **Remote RADIUS Server Group** > **New**



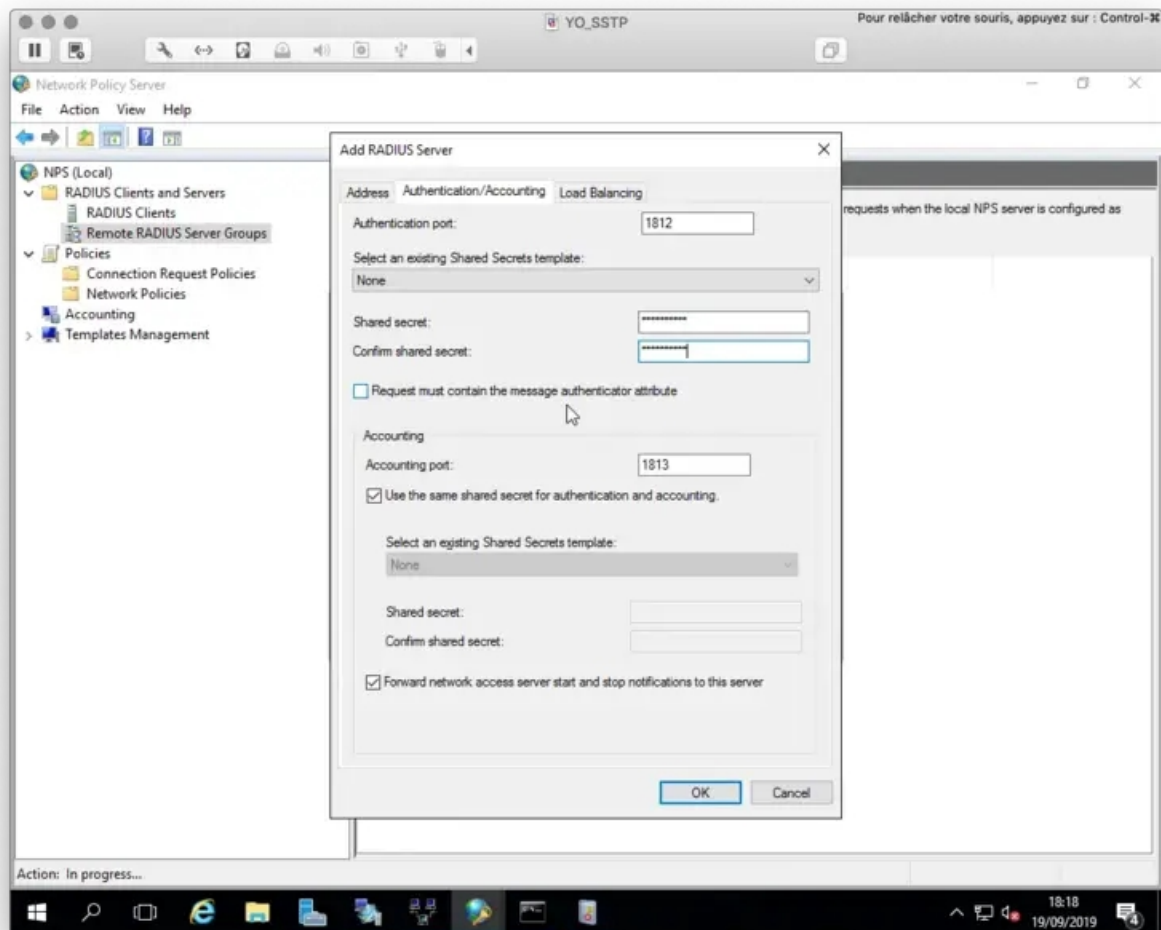
Click **Add** button



On the next page, add the IP address of your Radius Bridge.



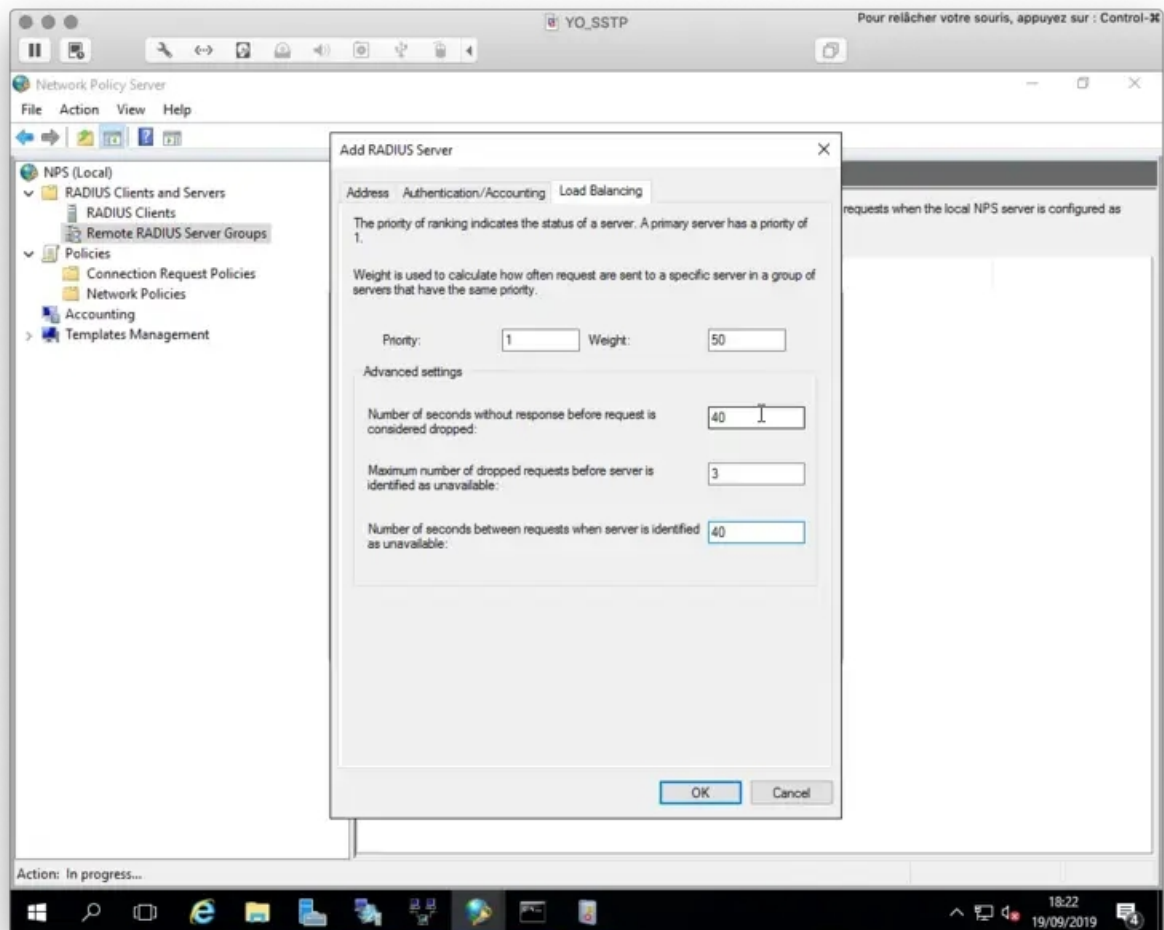
On the next tab, you have to configure the secret, which must match a client definition in your RADIUS bridge clients.conf:



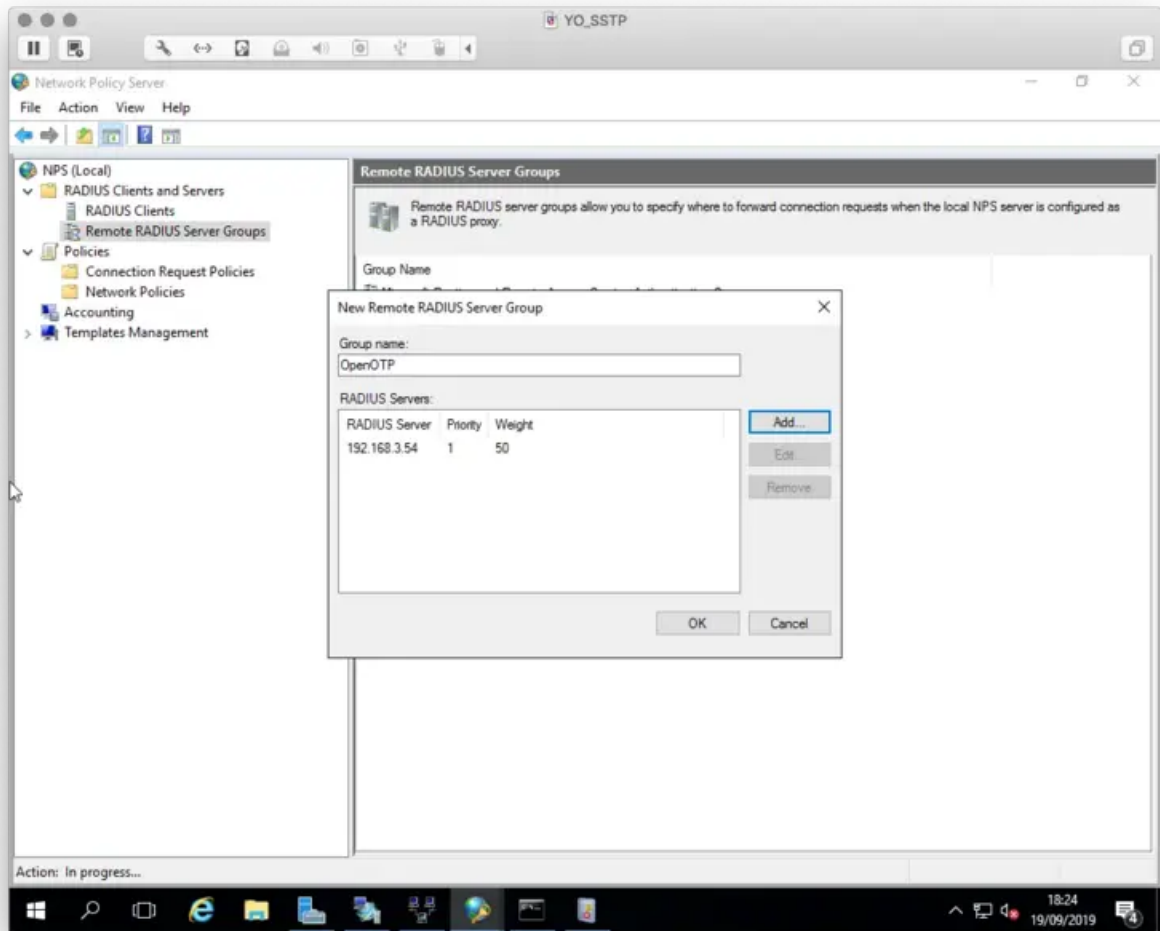
NPS server IP needs to be configured as Radius client in `/opt/radius/conf/clients.conf` :

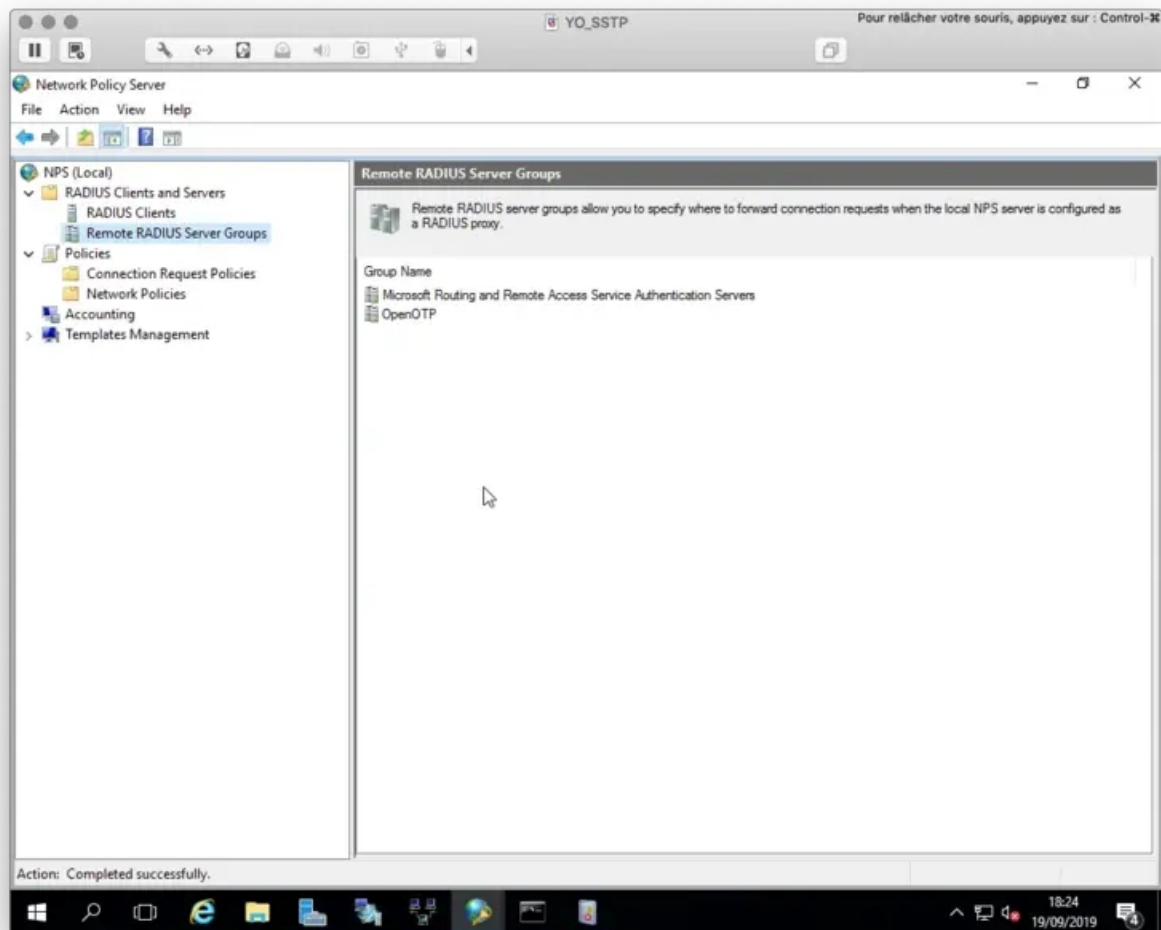
```
client NPS_Server {  
    ipaddr = 192.168.3.189  
    secret = testing123  
}
```

On the `Load Balancing` tab, you need to configure the timeouts like below. Again they must exceed the push timeout:



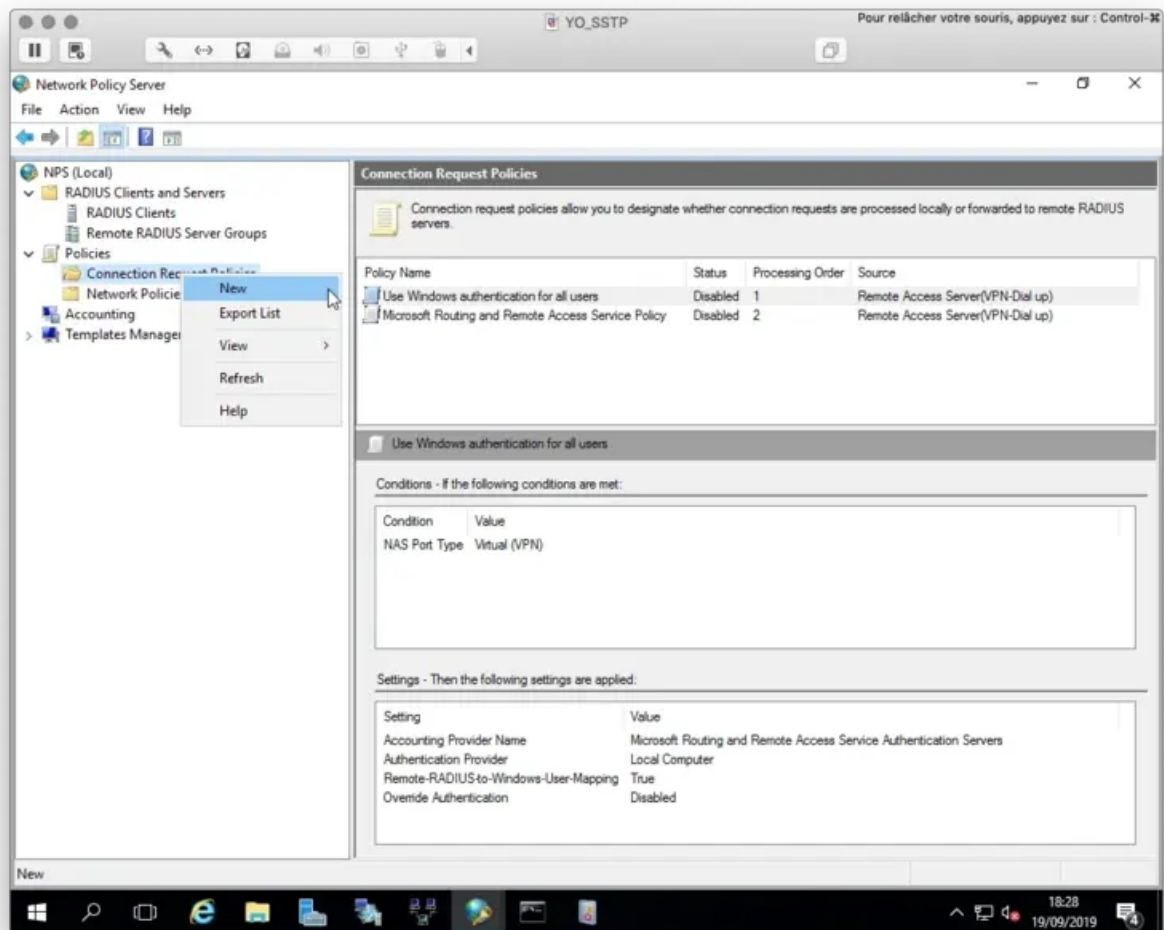
Click **Ok** twice when your configuration is done.



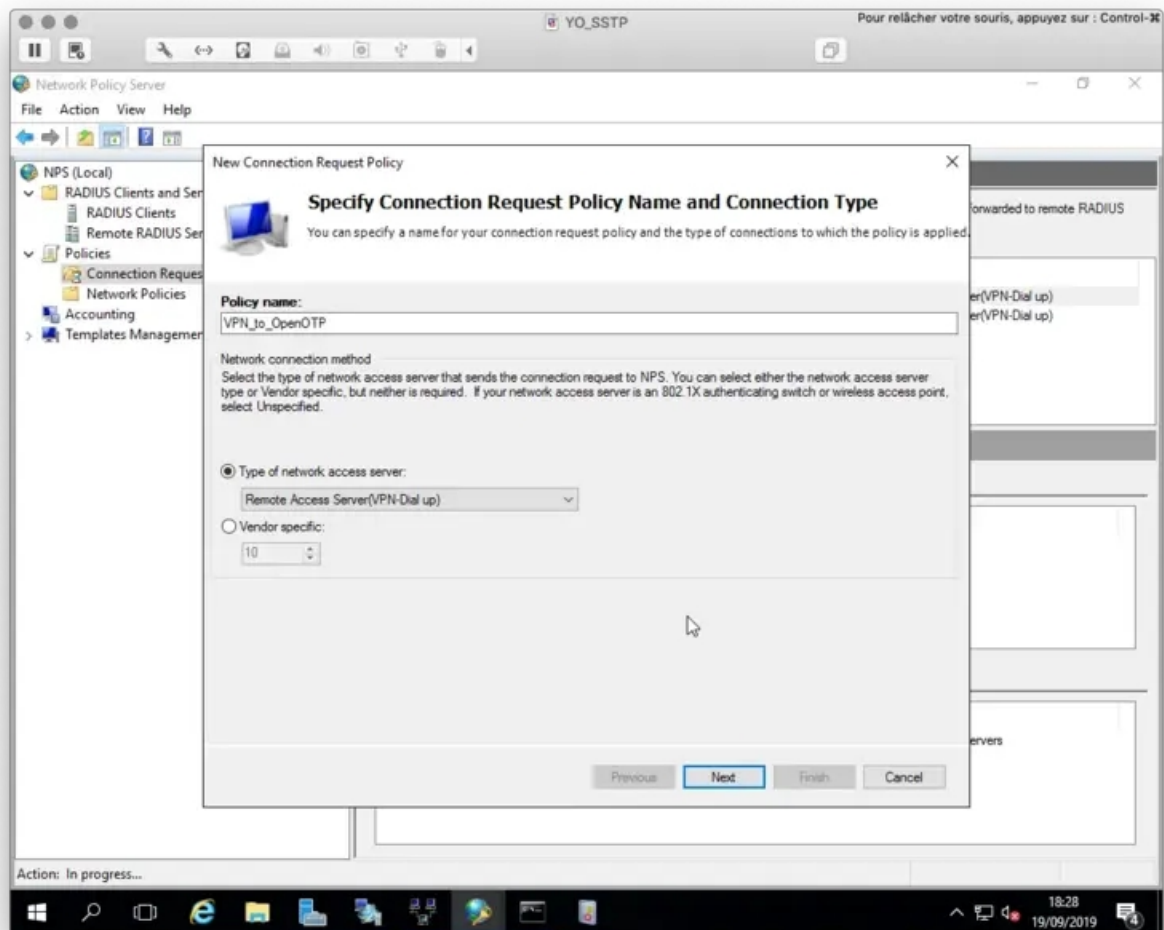


3.3 Connection request Policies

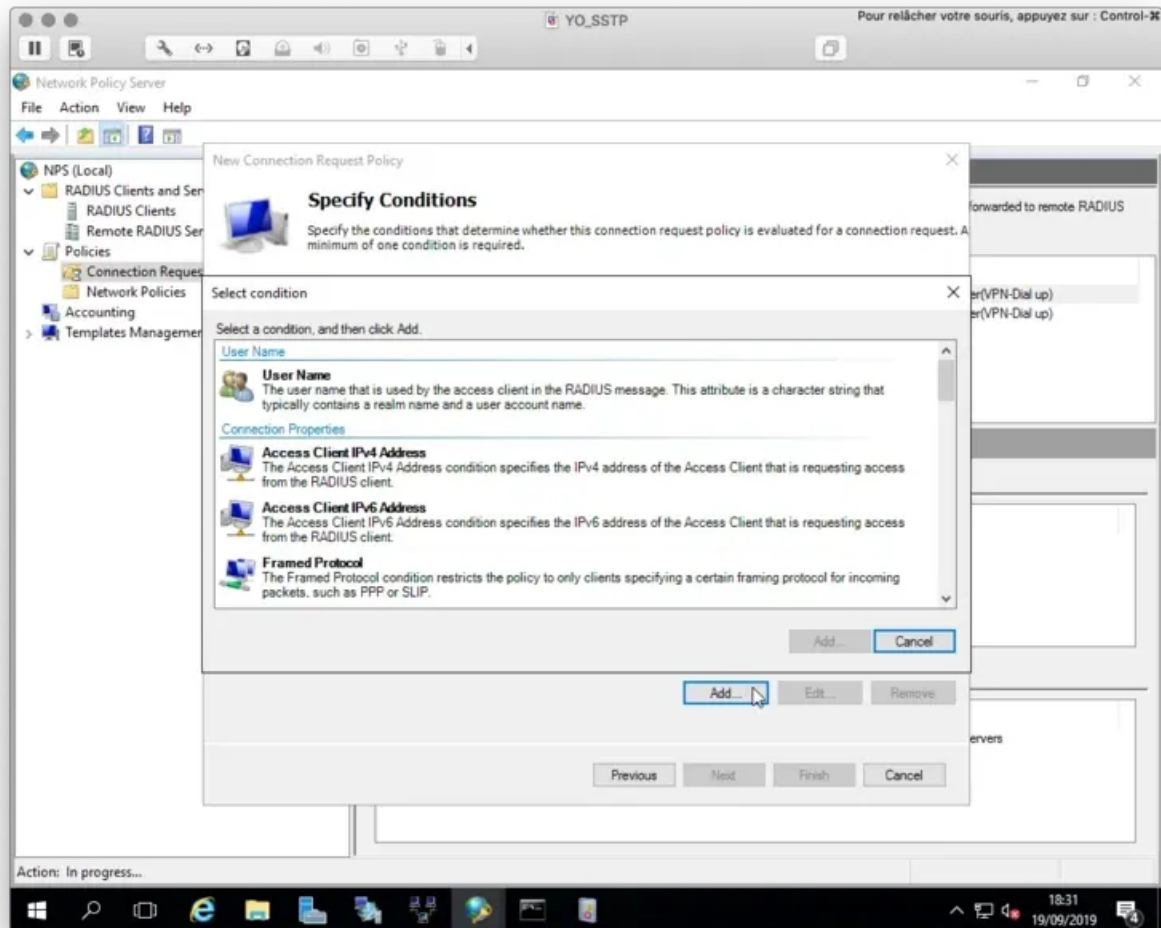
Now we need to configure a **Connection Request Policy** in order to forward authentication request to Radius Bridge.
Right click on **Connection Request Policy** > **New**



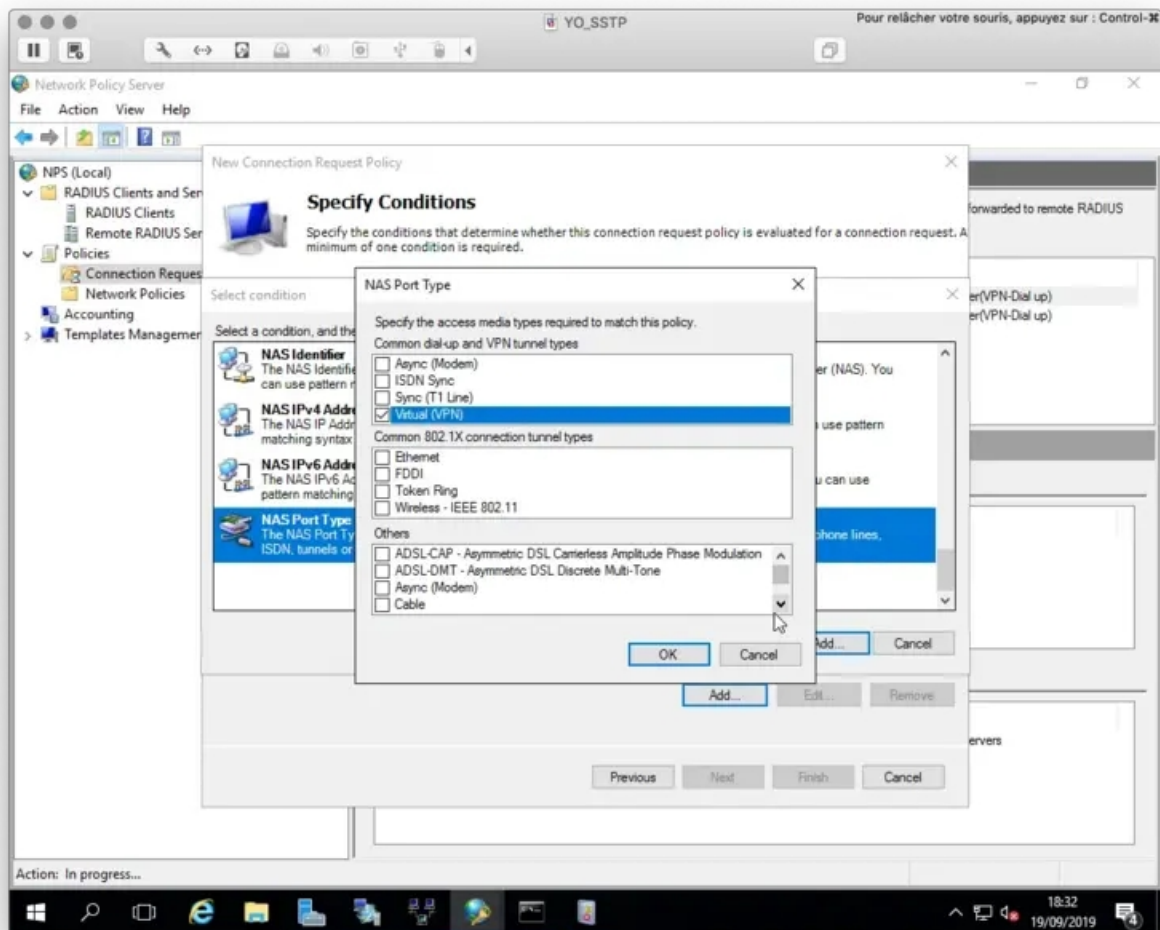
Name your policy, define the **Type of Network access server** to **Remote Access Server** and then click **Next**.

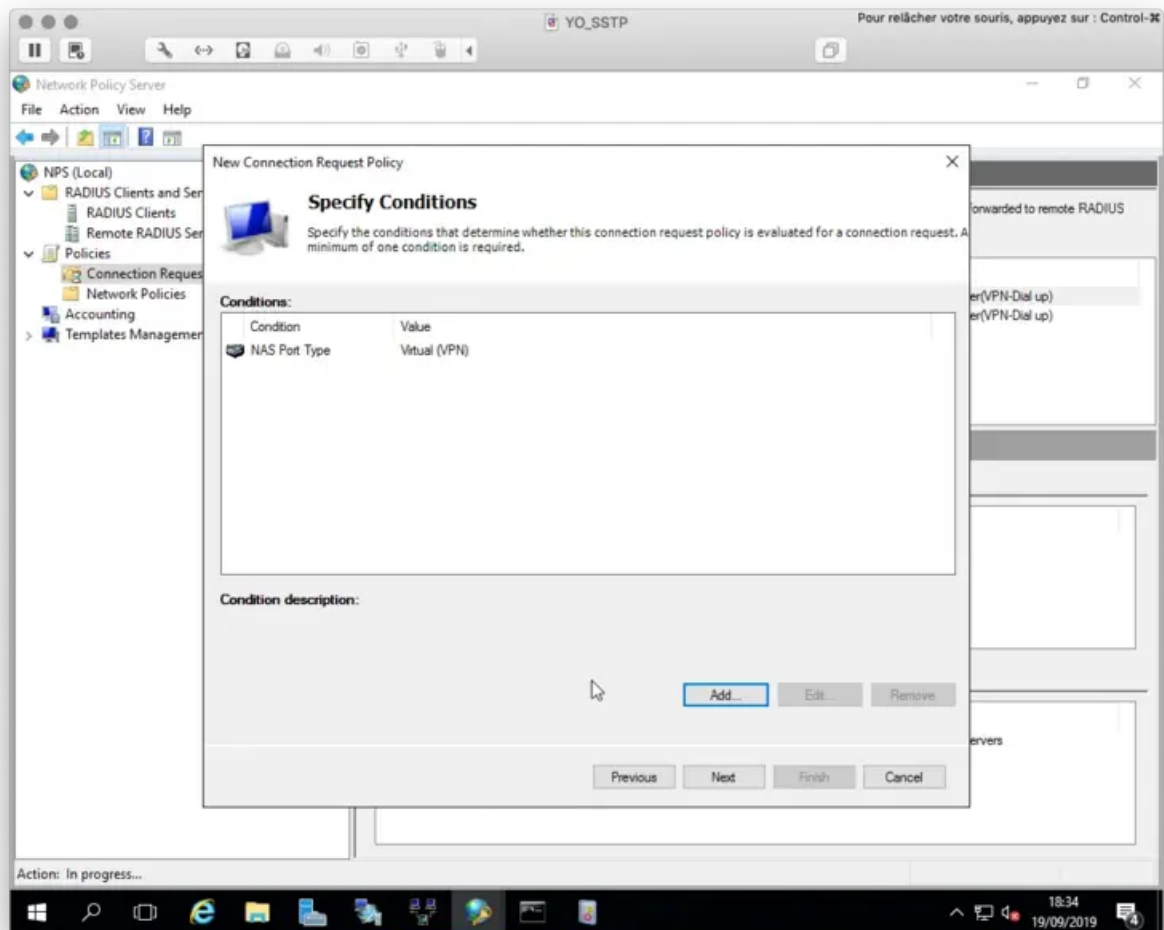


On the next page, define your Access Conditions.



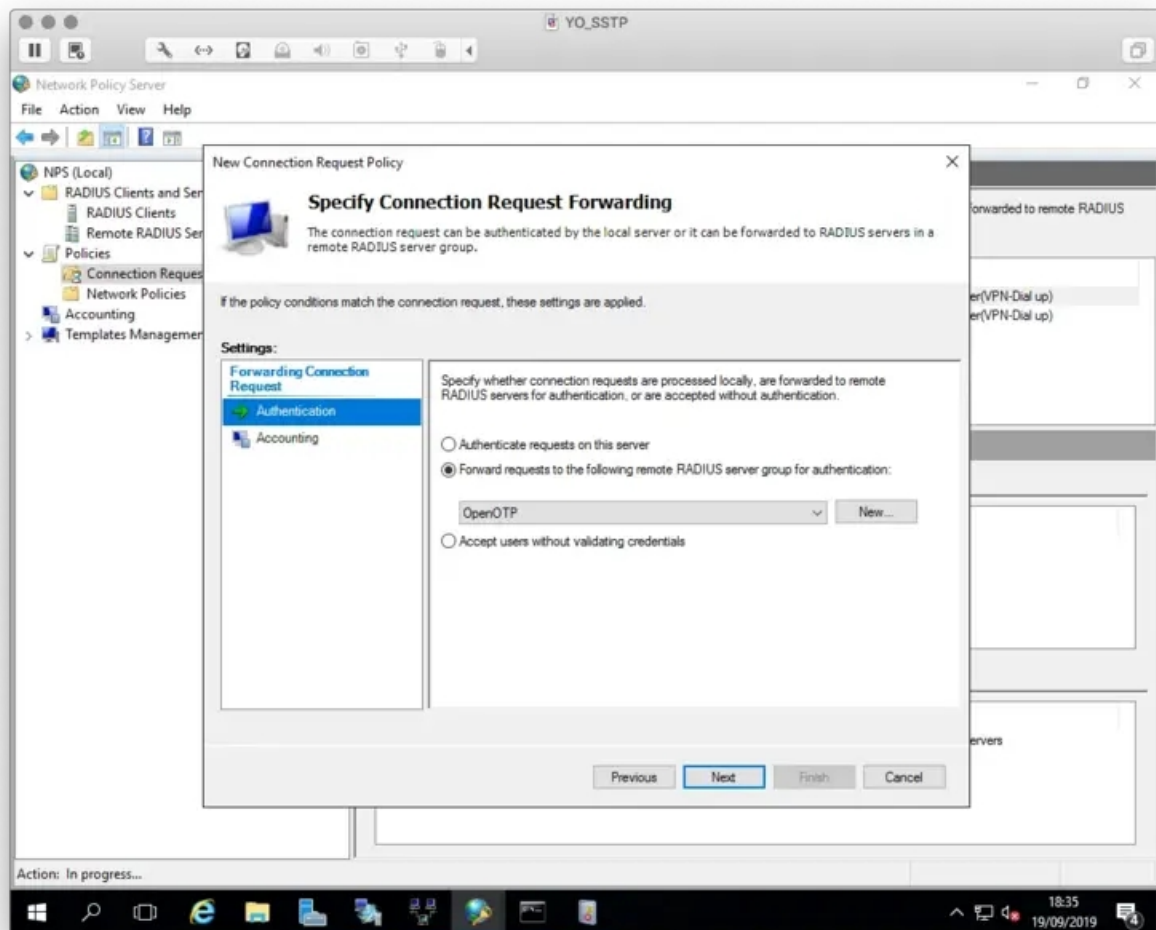
On my side, I only defined the **NAS Port Type** to **VPN(Virtual)** . This means the policy is applied to VPN connections.





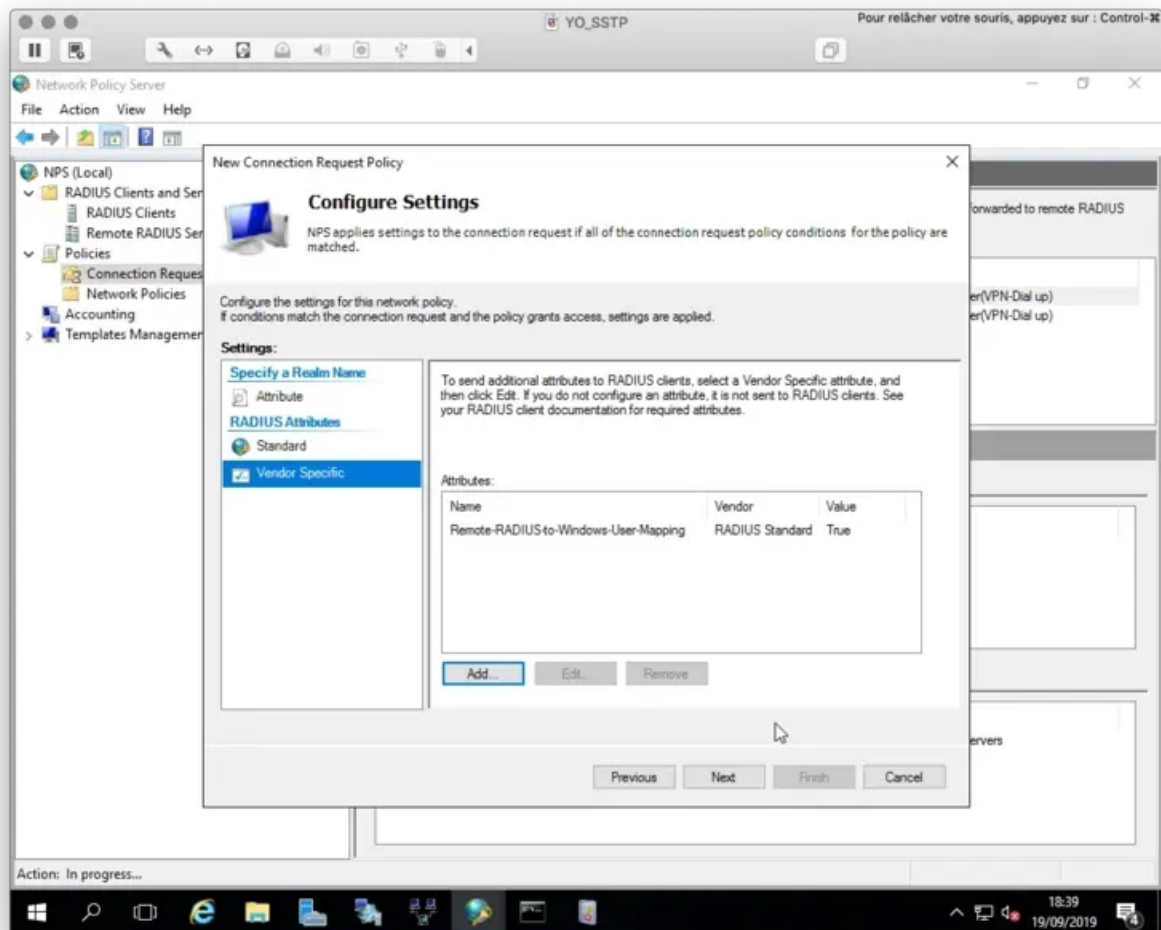
Click **Next** when all of your conditions are defined.

Next page we finally define the Authentication mechanism for the requests. On the Authentication tab switch to **Forward requests to the following RADIUS server group for authentication** and choose the Server group we defined earlier.

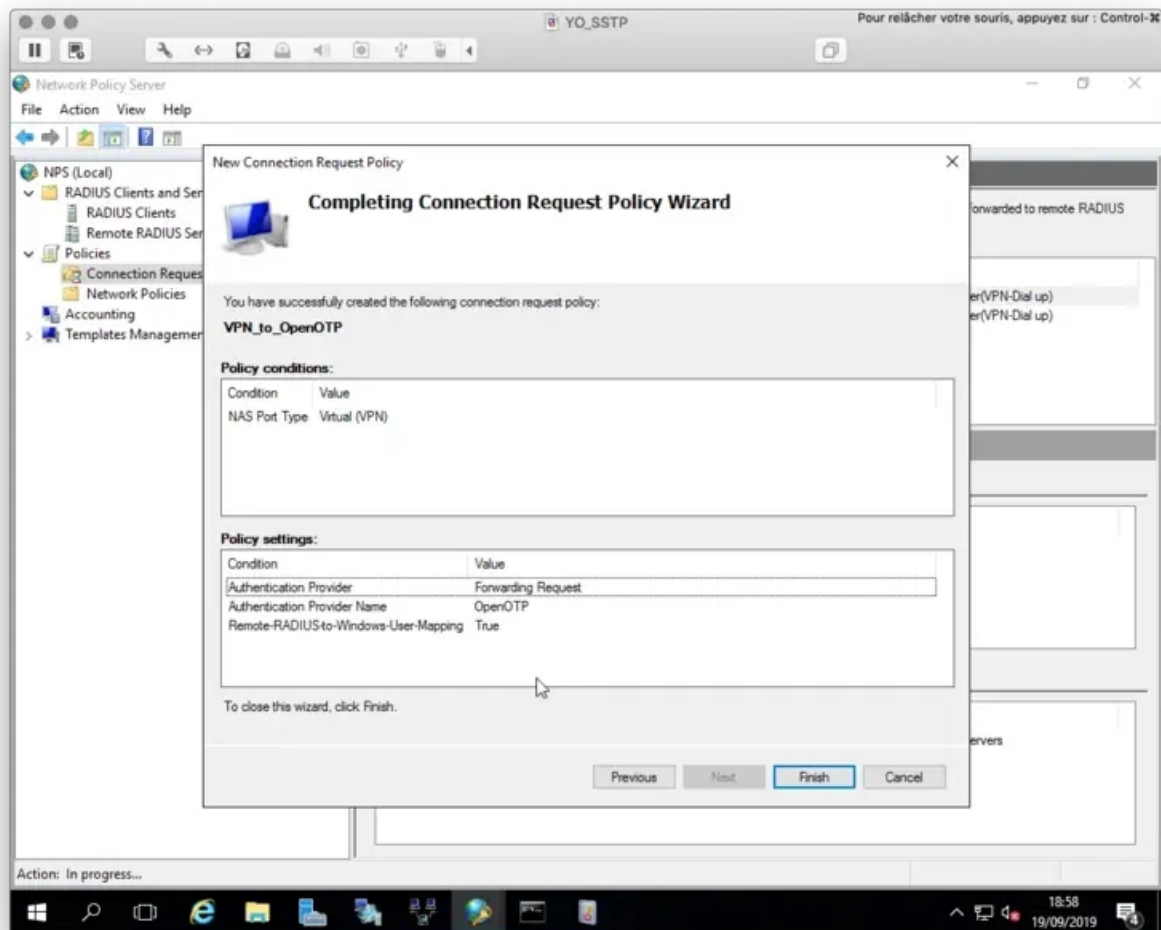


The accounting part can be kept by default because Radius Bridge does not support RADIUS accounting. Click **Next**.

On the next page, there is one small but important setting to be considered. If you wish to implement Network Policies (for example user/group specific network access rules) in NPS, you must configure the following RADIUS attribute set to **True**. This attribute means NPS sends the defined Network Policies back to VPN server. Without it all Network Policies are ignored.

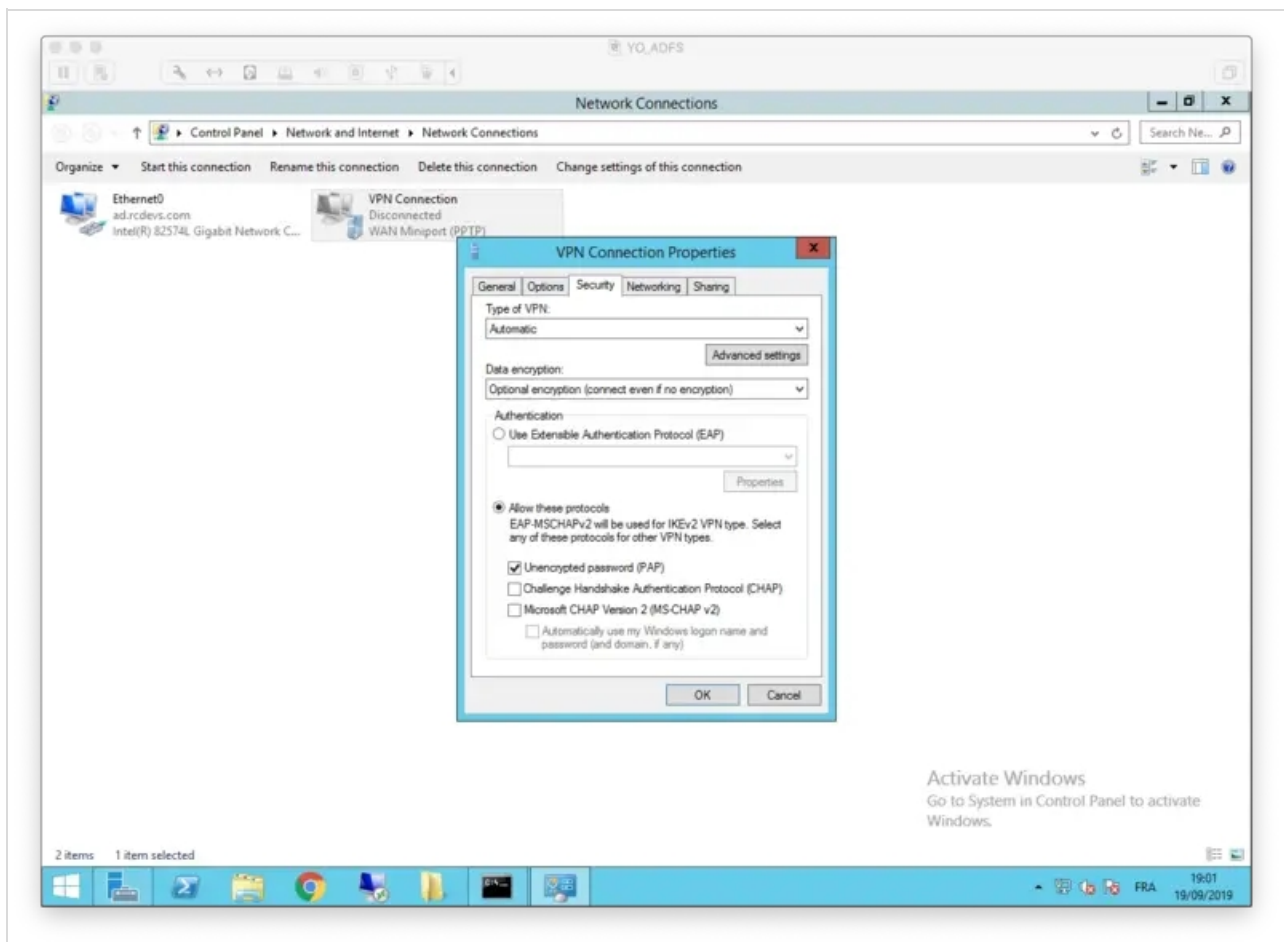


Click **Next** and finish.



4. VPN client configuration

On the VPN Client configuration we need to configure PAP as supported protocol. Edit your VPN Connection Properties and configure it as below :



That concludes the VPN client configuration.

5. WebADM Client Policy

As mentioned, Windows VPN client doesn't support RADIUS Challenge. For this reason, you have to create a WebADM client policy for your VPN, disabling the challenge mode support for the requests from MS VPN server.

Login on **WebADM Admin GUI** > **Admin tab** > **Client Policy**

YO_AD-DC (Active Directory)

- DC=yorcdevs (36)
 - CN=Builtin
 - CN=Computers
 - CN=ForeignSecurityPrincip...
 - CN=FreeIPA
 - CN=Infrastructure
 - CN=LostAndFound
 - CN=Managed Service Account...
 - CN=MountPoints
 - CN=MyGroup
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=TPM Devices
 - CN=Users (64)
 - CN=2fatestuser
 - CN=AZERTYUIQ
 - CN=Administrateur
 - CN=Administrateurs de l'e...
 - CN=Administrateurs du sch...
 - CN=Administrator
 - CN=Admins du domaine
 - CN=Contrôleurs de domaine...
 - CN=Contrôleurs de domaine...
 - CN=Contrôleurs de domaine...
 - CN=Contrôleurs de domaine
 - CN=DnsAdmins
 - CN=DnsUpdateProxy
 - CN=Groupe de réplication ...
 - CN=Groupe de réplication ...
 - CN=ITWeb
 - CN=Invité
 - CN=Invités du domaine
 - CN=Ordinateurs du domaine
 - CN=Propriétaires créateur...
 - CN=Protected Users
 - CN=RCDevs

WebADM Enterprise Edition v1.7.6-2

Copyright © 2010-2019 RCDévs SA, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

WebADM Server Administration

WebADM v1.7.6-2 (64bit) running on server webadm1.yorcdevs.com (192.168.3.54) in cluster mode (2 servers). Currently handling 1 connection(s).

Server Version Details: Apache/2.4.41 PHP/7.2.22 OpenSSL/1.1.1d
Internal Server Time: 2019-09-19 19:03:54 Europe/Berlin (NTP check Ok)
Hardware Modules: No HSM Connected
WebADM Features: WebApps (Enabled), WebSrvs (Enabled), Manager (Enabled)

Active LDAP Server:	YO_AD-DC (192.168.3.50)	Active SQL Server:	SQL Server (192.168.3.58)
Active Session Server:	Session Server 1 (192.168.3.54)	Active PKI Server:	PKI Server (192.168.3.54)
Active License Server:	License Server (91.134.128.157)	Active Mail Server:	SMTP Server (78.141.172.203)
Active Push Server:	Push Server (91.134.128.157)		

User Domains (8)
Associate domain names with LDAP user search bases.

Client Policies (15)
Define custom policy settings for consumer applications.

Access Devices (0)
Hardware devices for badging and physical access control.

LDAP Mount Points (9)
Connect secondary LDAP servers to the tree view.

LDAP Option Sets (1)
Define LDAP tree constraints for your "other" administrators.

Administrator Roles (1)
Create admin role templates for your "other" administrators.

Licensing and Configurations

- Software License Details
- LDAP Server Details
- LDAP Server Schema
- Memory Usage Details
- Hardware Modules Details
- Remote Manager Interface
- Config Object Statuses
- Network Service Statuses
- WebADM Base Settings

Runtime Actions

- Download WebADM CA Certificate
- Download WebADM SSL Certificate
- Issue Server or Client SSL Certificate
- Clear Admin Session Cache (6 KB)
- Clear WebADM License Cache
- Clear WebADM System Caches (617 KB)
- Flush WebADM Session Data (853 KB)
- Reload WebADM Configurations

Click on **Add Client** button, name your client policy and click **Proceed** button :

Create Configuration Object of Type Client

Mandatory attributes

Container Select

Common Name

WebADM Object Type

Optional attributes

Description / Note

WebADM Settings You can edit this attribute once object is created.

Proceed

Click on **Create Object** :

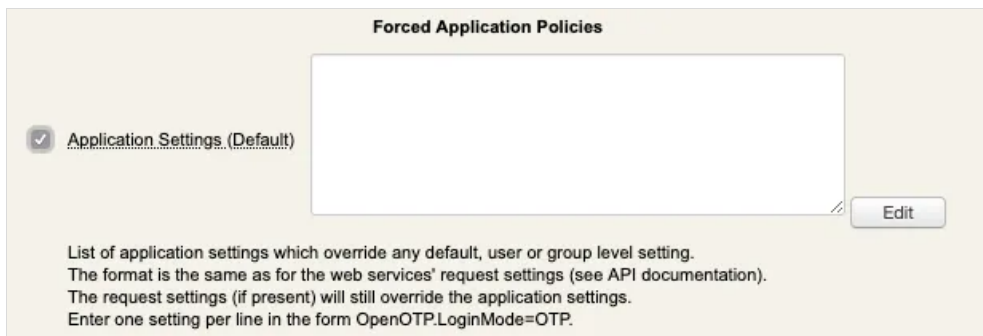
Create Configuration Object of Type Client

Confirm object creation for cn=Microsoft NPS,cn=Clients,cn=WebADM,dc=...

Attribute	Value
DN	cn=Microsoft NPS,cn=Clien...
Common Name	Microsoft NPS
WebADM Object Type	Client

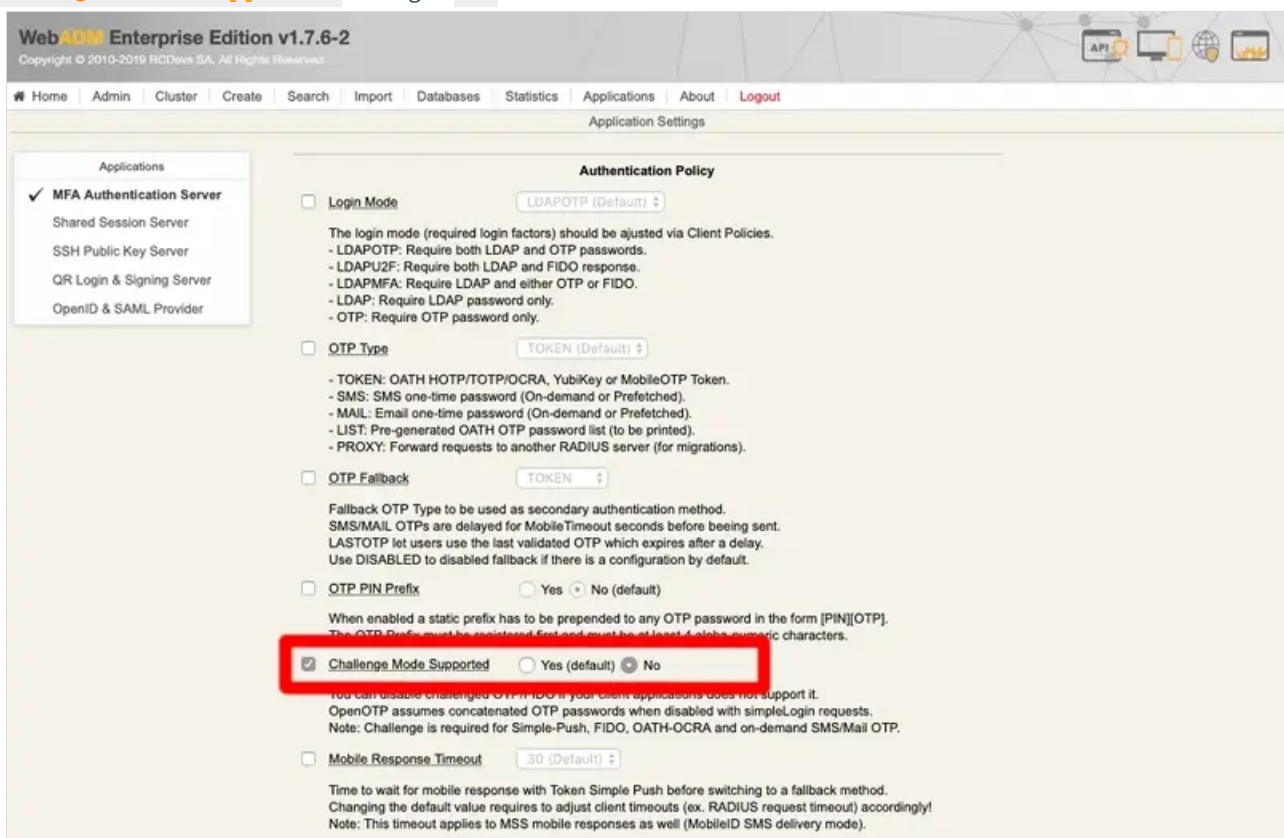
Create Object

You are now on the configuration page of your client policy. Scroll down to find the **Forced Application Policies** section :



Enable the setting and click **Edit** button :

In the **Application** box on the top left, select **MFA Authentication Server** switch the **Challenge Mode Supported** setting to **No** :



On the same page you can also configure **Push Login** setting to **yes** if you have a push login infrastructure available and wish to use this method.

Scroll down to apply the configuration, and you will be redirected to the client policy configuration page. You should have the following :

Forced Application Policies

OpenOTP.ChallengeMode=No
OpenOTP.PushLogin=Yes

☒ **Application Settings (Default)**

[Edit](#)

List of application settings which override any default, user or group level setting.
The format is the same as for the web services' request settings (see API documentation).
The request settings (if present) will still override the application settings.
Enter one setting per line in the form OpenOTP.LoginMode=OTP.

For OpenOTP match the policy with NPS and your VPN, you must configure the IP addresses of your VPN and NPS servers in the Client Name Aliases setting. On my side, both are running on the same server so I configured only one IP address:

WebADM Enterprise Edition v1.7.7
Copyright © 2010-2019 RCDev SA, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

Object Settings for CN=Microsoft NPS,CN=Clients,CN=WebADM,DC=yorcdevs,...

- ☐ **Disable Client** ☐ Yes ☒ No (default)
When disabled, client requests using this client policy will be refused.
- ☐ **Default Domain** AD
This domain is automatically selected when no domain is provided.
- ☐ **Friendly Name**
Friendly client name or short description to be used for %CLIENT% in user messages.
- ☒ **Client Name Aliases** 192.168.3.182
Comma-separated list of alternative client IDs.
- ☐ **UID Attributes** [Edit](#)
Restricted list of LDAP login attributes replacing the attributes configured via uid_attrs in webadm.conf.

Press **Apply** to save your client policy.

Microsoft NPS (CN=Microsoft NPS,CN=Clients,CN=WebADM,DC=...)
[i]

Status: Enabled [\[CONFIGURE\]](#) [\[RENAME\]](#) [\[REMOVE\]](#)

Aliases: 192.168.3.182

Application Settings: OpenOTP: 2

Configuration is now complete.

With this policy, when your users will try to log in from the VPN client, they must use the push login to be able to log in (if push login infrastructure is configured with OpenOTP) or use LDAP and OTP passwords concatenation :

- > LDAP Username : Administrator
- > LDAP Password : password
- > OTP : 123456
- > **LDAP Password+OTP concatenation : password123456**

6. OpenOTP logs

6.1 Push login logs

```

[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] New openotpSimpleLogin SOAP request
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] > Username: administrator
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] > Password: xxxxxxxx
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] > Source IP: 192.168.3.189
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] > Options: RADIUS,-U2F
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Enforcing client policy: Microsoft NPS
(matched client IP)
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Registered openotpSimpleLogin request
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Resolved LDAP user:
CN=Administrator,CN=Users,OU=TESTING,DC=yorcdevs,DC=com (cached)
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Resolved LDAP groups: group policy creator
owners,domain admins,enterprise admins,schema admins,administrators,denied rod password
replication group
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Started transaction lock for user
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Found user fullname: Administrator
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Found 46 user settings:
LoginMode=LDAPOTP,OTPTType=TOKEN,PushLogin=Yes,ExpireNotify=MAIL,ChallengeMode=No,ChallengeTim
1:HOTP-SHA1-6:QN06-
T1M,DeviceType=FIDO2,SMSType=Normal,SMSMode=Ondemand,SecureMail=No,MailMode=Ondemand,Pre
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Found 5 user data:
TokenType,TokenKey,TokenState,TokenID,TokenSerial
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Found 1 registered OTP token (TOTP)
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Challenge mode disabled (checking
concatenated passwords)
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Requested login factors: LDAP & OTP
[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] LDAP password Ok
[2019-09-19 16:50:34] [192.168.3.54] [OpenOTP:8ENCNNEB] Sent push notification for token #1
[2019-09-19 16:50:34] [192.168.3.54] [OpenOTP:8ENCNNEB] Waiting 27 seconds for mobile response
[2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] Received mobile authentication response
from 192.168.3.192
[2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] > Session: SeNAdV4FltKKVKIJ
[2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] > Password: 16 Bytes
[2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] Found authentication session started 2019-
09-19 16:50:33
[2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] PUSH password Ok (token #1)
[2019-09-19 16:50:37] [192.168.3.54] [OpenOTP:8ENCNNEB] Updated user data
[2019-09-19 16:50:37] [192.168.3.54] [OpenOTP:8ENCNNEB] Sent login success response

```

6.2 Concatenated LDAP password and OTP logs

[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] New openotpSimpleLogin SOAP request
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] > Username: administrator
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] > Password: xxxxxxxxxxxxxxxx
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] > Source IP: 192.168.3.189
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] > Options: RADIUS,-U2F
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Enforcing client policy: Microsoft NPS
(matched client IP)
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Registered openotpSimpleLogin request
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Resolved LDAP user:
CN=Administrator,CN=Users,OU=TESTING,DC=yorcdevs,DC=com (cached)
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Resolved LDAP groups: group policy creator
owners,domain admins,enterprise admins,schema admins,administrators,denied rod password
replication group
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Started transaction lock for user
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Found user fullname: Administrator
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Found 46 user settings:
LoginMode=LDAPOTP,OTPTType=TOKEN,PushLogin=No,ExpireNotify=MAIL,ChallengeMode=No,ChallengeTim
1:HOTP-SHA1-6:QN06-
T1M,DeviceType=FIDO2,SMSType=Normal,SMSMode=Ondemand,SecureMail=No,MailMode=Ondemand,Pre

[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Found 5 user data:
TokenType,TokenKey,TokenState,TokenID,TokenSerial
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Found 1 registered OTP token (TOTP)
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Challenge mode disabled (checking
concatenated passwords)
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Requested login factors: LDAP & OTP
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] LDAP password Ok
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] TOTP password Ok (token #1)
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Updated user data
[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Sent login success response

This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved