Procédure d’installation et configuration de OpenVPN Access Server

Auteur : Arthur GUILET
Reference : Assurmer
Date : 20/04/2022

DIFFUSION et VISAS

Diffusion				
Société / Entité	**Destinataires**	**Fonction**	**Diffusion**	**Pour info**
Assumer	Service IT	Procédure	Réseau	

Visas			
Société/Entité	**Nom**	**Fonction**	

SUIVI DES VERSIONS

Version	Date	Auteur	Raison	Nombre de page
V1.0	07/04/2023	Arthur GUILET	Installation et configuration de OpenVPN Access Server	9

COORDONNEES

Contacts		
Nom	**E-mail**	**Téléphone**
Arthur GUILET	arthur.guilet@assurmer.fr	01.54.23.79.02

SOMMAIRE

-Prérequis	page 4
-Installation d’OpenVPN Acces Server	page 5
-Configuration d’OpenVPN Acces Server	page 7
-LDAP OpenVPN Acces Server	page 10

Prérequis

-Il vous faut une serveur linux installer et configurer

-Désactiver les firewalls

-Paramétrer son adresses IP en statique et son DNS à lui même

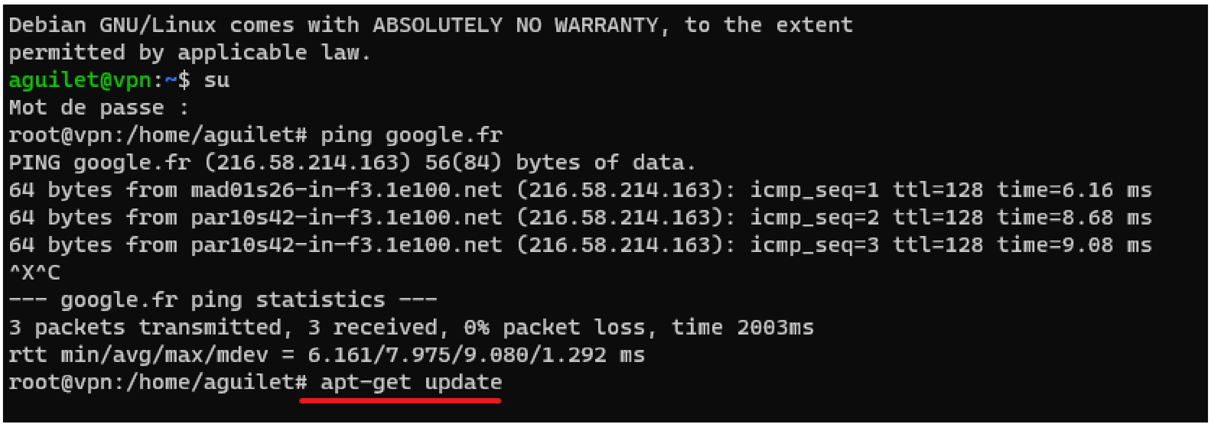
-Il faut que votre serveur soit relié un switch

-Vous devez installer et configurer un activer directory

-Configurer votre DNS

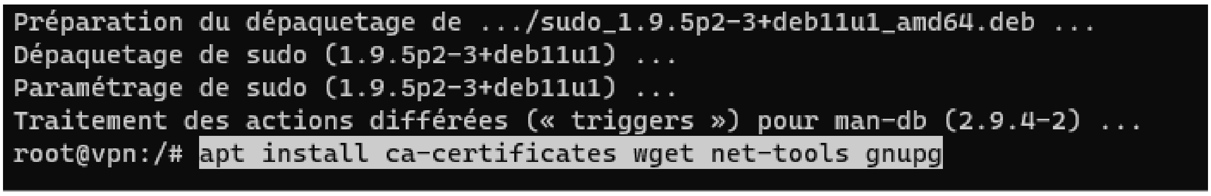
Installation d’OpenVPN Acces Server

1. Mettez à jour votre machine avec
-apt update
-apt upgrade



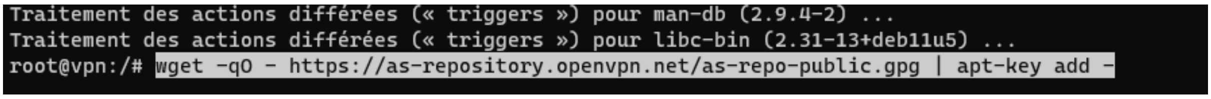
```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
aguilet@vpn:~$ su
Mot de passe :
root@vpn:/home/aguilet# ping google.fr
PING google.fr (216.58.214.163) 56(84) bytes of data.
64 bytes from mad01s26-in-f3.1e100.net (216.58.214.163): icmp_seq=1 ttl=128 time=6.16 ms
64 bytes from par10s42-in-f3.1e100.net (216.58.214.163): icmp_seq=2 ttl=128 time=8.68 ms
64 bytes from par10s42-in-f3.1e100.net (216.58.214.163): icmp_seq=3 ttl=128 time=9.08 ms
^X^C
--- google.fr ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 6.161/7.975/9.080/1.292 ms
root@vpn:/home/aguilet# apt-get update
```

2. Installer une dépendance
-apt install ca-certificates wget net-tools gnupg



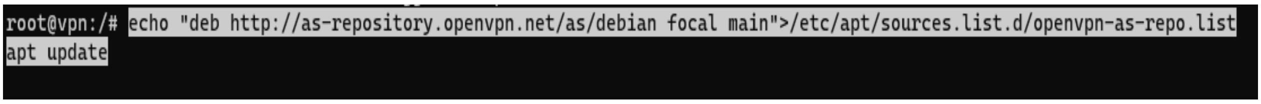
```
Préparation du dépaquetage de .../sudo_1.9.5p2-3+deb11u1_amd64.deb ...
Dépaquetage de sudo (1.9.5p2-3+deb11u1) ...
Paramétrage de sudo (1.9.5p2-3+deb11u1) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
root@vpn:/# apt install ca-certificates wget net-tools gnupg
```

3.Installer le reposetory list
-wget -qO - https://as-repository.openvpn.net/as-repo-public.gpg | apt-key add -



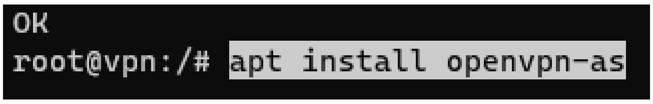
```
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.31-13+deb11u5) ...
root@vpn:/# wget -qO - https://as-repository.openvpn.net/as-repo-public.gpg | apt-key add -
```

4. Modifier une source list :
- echo "deb http://as-repository.openvpn.net/as/debian bullseye main">/etc/apt/sources.list.d/openvpn-as-repo.list



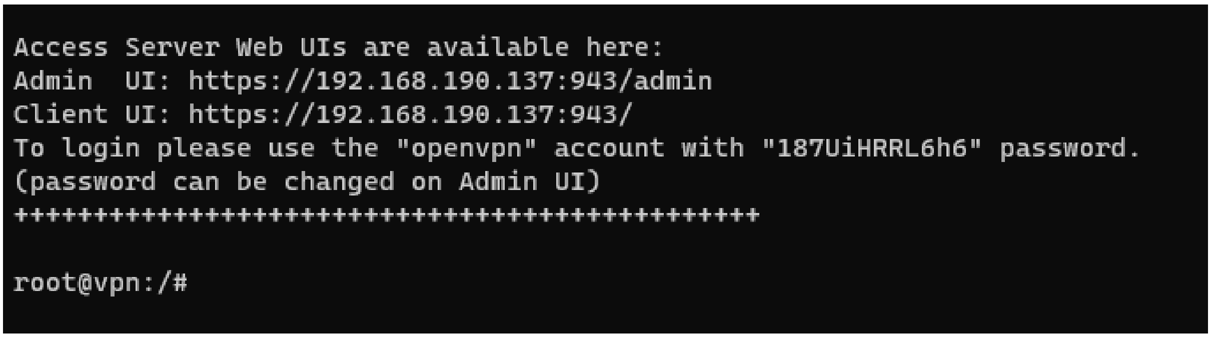
```
root@vpn:/# echo "deb http://as-repository.openvpn.net/as/debian focal main">/etc/apt/sources.list.d/openvpn-as-repo.list
apt update
```

5. Installer la solution OpenVPN access server.



```
OK
root@vpn:/# apt install openvpn-as
```

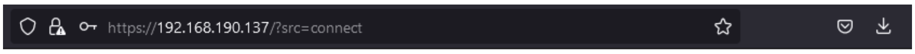
6. Votre un mot de passe pour l’utilisateur admin : openvpn rentrer l’url ensuite l’utilisateur saisissez le mot de passe



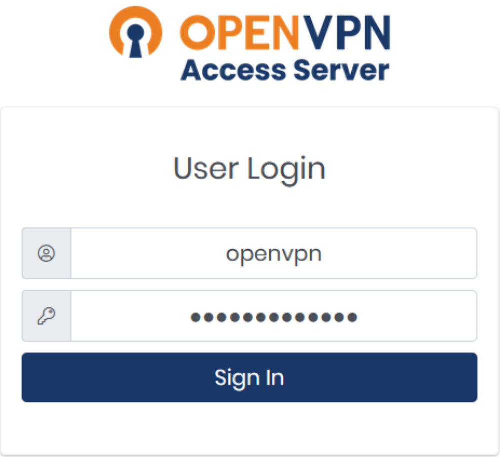
```
Access Server Web UIs are available here:
Admin  UI: https://192.168.190.137:943/admin
Client UI: https://192.168.190.137:943/
To login please use the "openvpn" account with "187UiHRRL6h6" password.
(password can be changed on Admin UI)
+++++++++++++++++++++++++++++++++++++++++++++++

root@vpn:/#
```

Configuration d’OpenVPN Acces Server

7. Connectez-vous



https://192.168.190.137/?src=connect



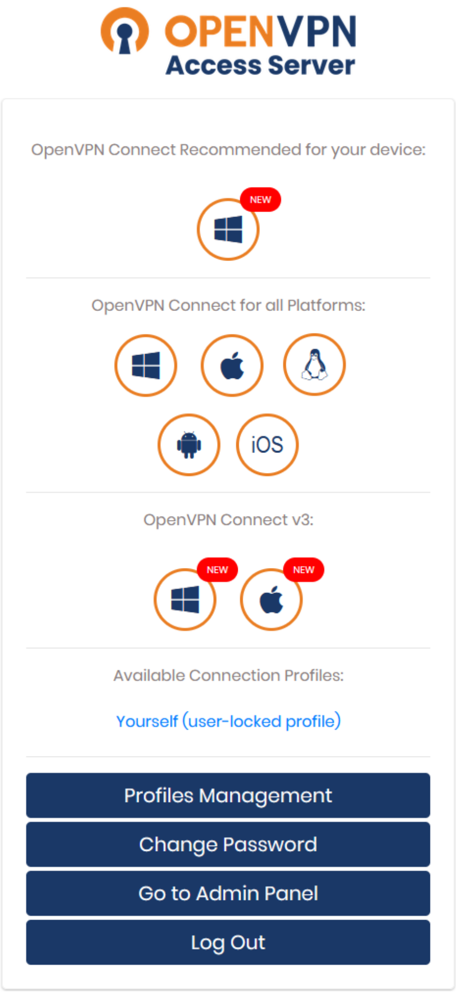
User Login

openvpn

●●●●●●●●●●●●●

8. Installer le client openvpn

9. Ensuite allé dans l'admin panel



OPENVPN Access Server

OpenVPN Connect Recommended for your device:

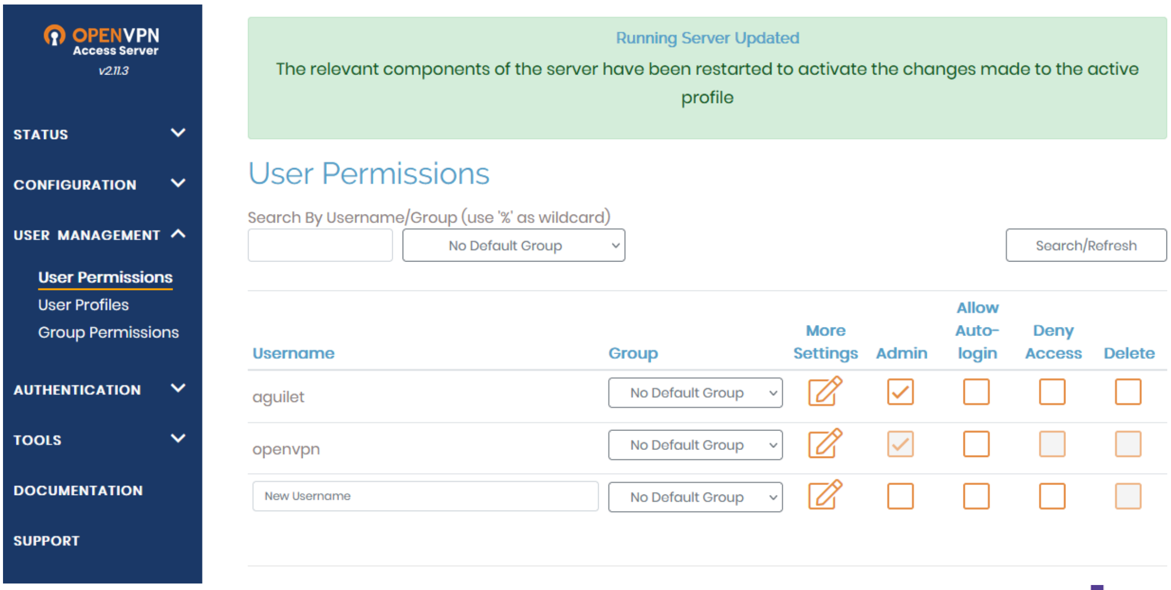
OpenVPN Connect for all Platforms:

OpenVPN Connect v3:

Available Connection Profiles:

Yourself (user-locked profile)

10. Créez-vous un identifiant admin



Running Server Updated

The relevant components of the server have been restarted to activate the changes made to the active profile

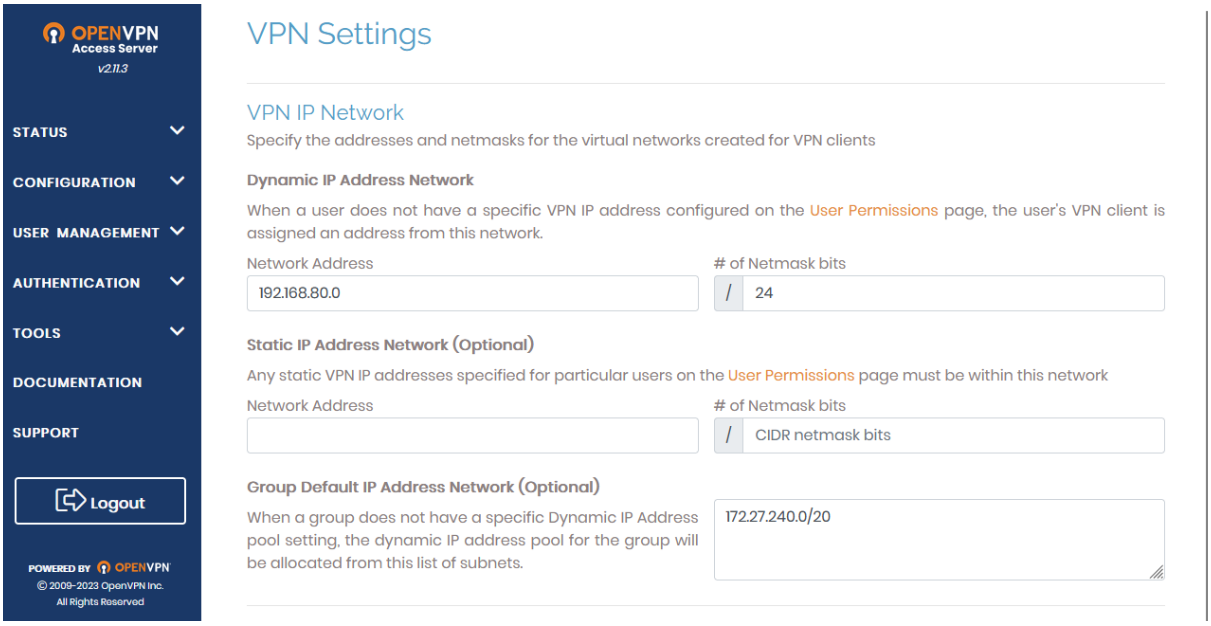
User Permissions

Search By Username/Group (use '%' as wildcard)

No Default Group

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
aguilet	No Default Group	✎	☑	□	□	□
openvpn	No Default Group	✎	☑	□	□	□
New Username	No Default Group	✎	□	□	□	□

11. Vous-devez indiquer le réseau du VPN dans notre cas il est sur notre VLAN 80



VPN Settings

VPN IP Network

Specify the addresses and netmasks for the virtual networks created for VPN clients

Dynamic IP Address Network

When a user does not have a specific VPN IP address configured on the User Permissions page, the user's VPN client is assigned an address from this network.

Network Address: 192.168.80.0

# of Netmask bits: / 24

Static IP Address Network (Optional)

Any static VPN IP addresses specified for particular users on the User Permissions page must be within this network

Network Address:

# of Netmask bits: / CIDR netmask bits

Group Default IP Address Network (Optional)

When a group does not have a specific Dynamic IP Address pool setting, the dynamic IP address pool for the group will be allocated from this list of subnets.

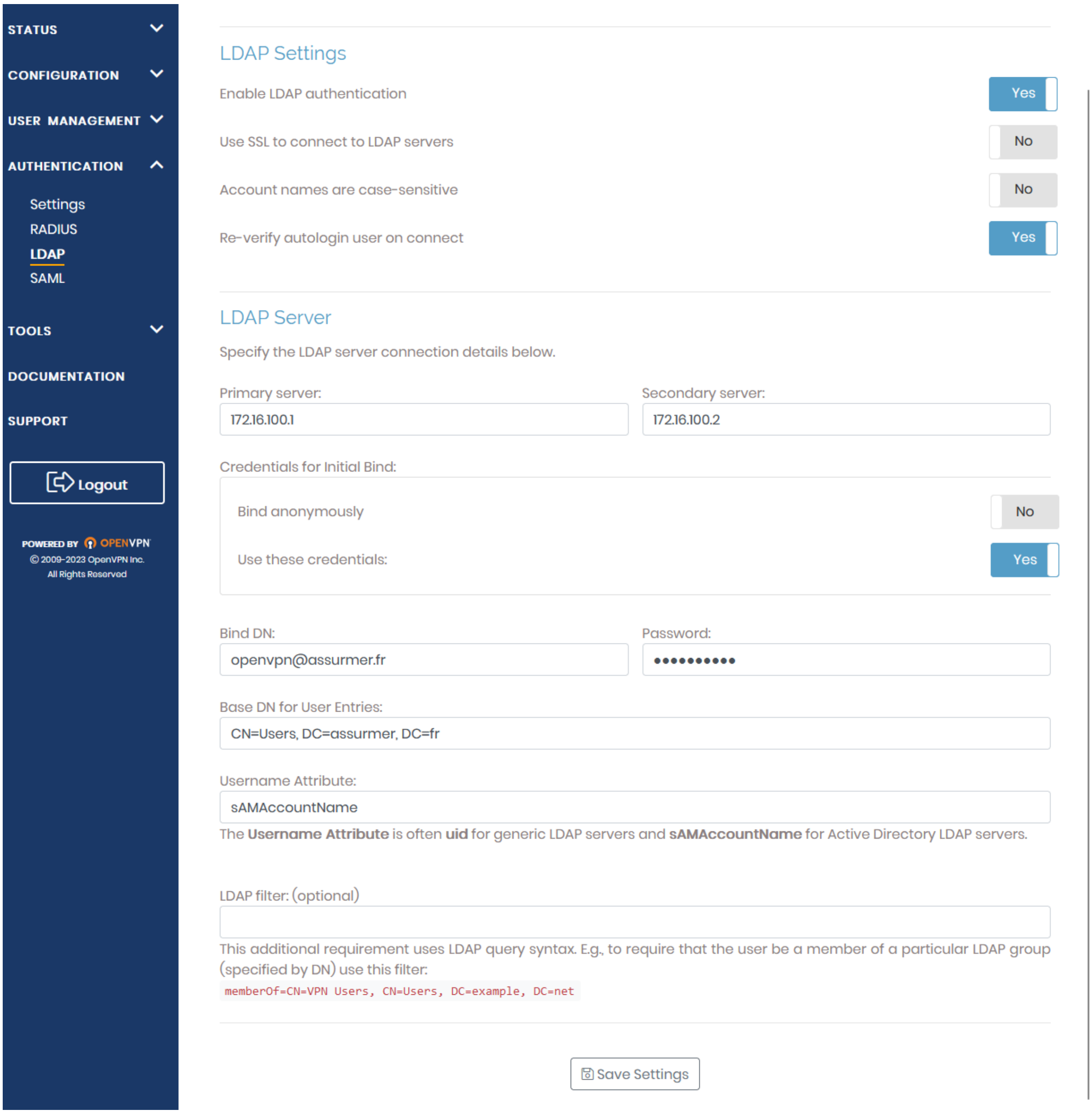
172.27.240.0/20

LDAP OpenVPN Acces Server

12. Activer le LDAP

13. Indiquer l'ip de votre serveur AD

14. Enfin un utilisateur et l'OU de l'AD



LDAP Settings

Enable LDAP authentication: Yes

Use SSL to connect to LDAP servers: No

Account names are case-sensitive: No

Re-verify autologin user on connect: Yes

LDAP Server

Specify the LDAP server connection details below.

Primary server: 172.16.100.1

Secondary server: 172.16.100.2

Credentials for Initial Bind:

Bind anonymously: No

Use these credentials: Yes

Bind DN: openvpn@assurmer.fr

Password: ●●●●●●●●●●

Base DN for User Entries: CN=Users, DC=assurmer, DC=fr

Username Attribute: sAMAccountName

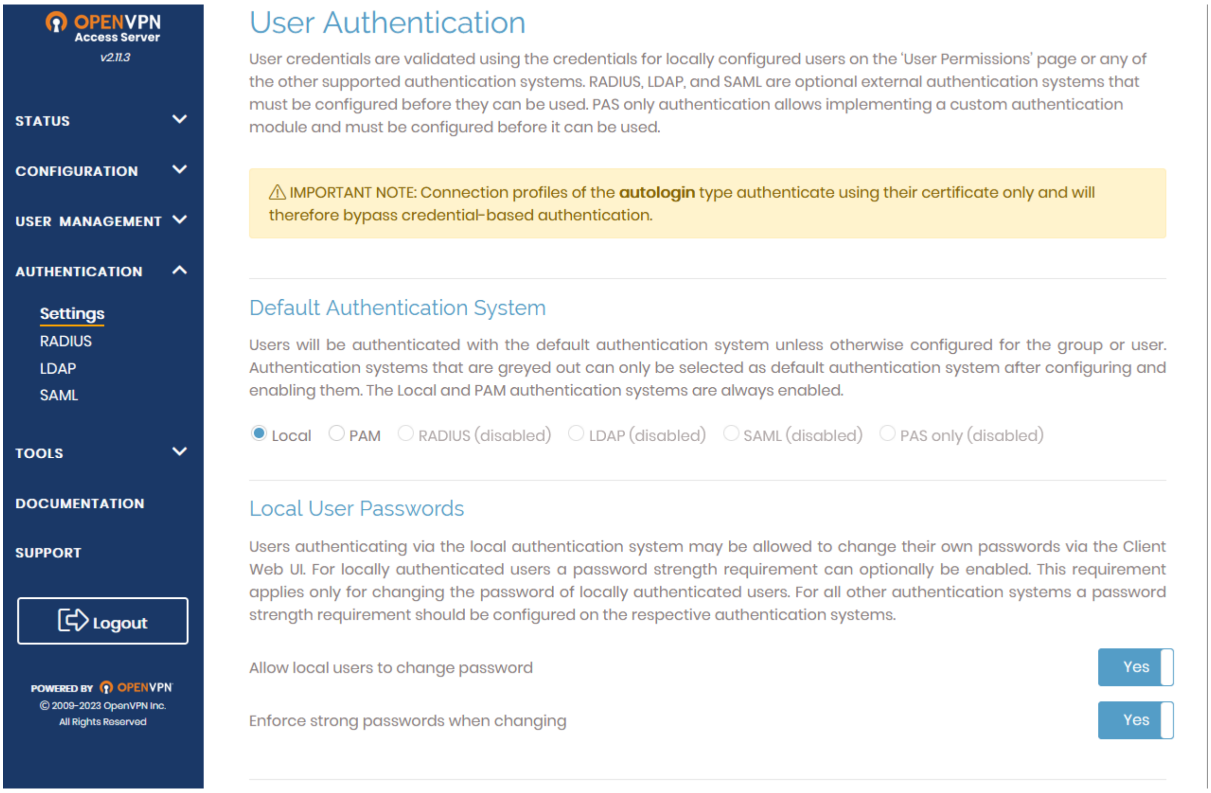
The **Username Attribute** is often **uid** for generic LDAP servers and **sAMAccountName** for Active Directory LDAP servers.

LDAP filter: (optional)

This additional requirement uses LDAP query syntax. E.g., to require that the user be a member of a particular LDAP group (specified by DN) use this filter:

```
memberOf=CN=VPN Users, CN=Users, DC=example, DC=net
```

15. Enfin activer le LDAPcomme système d'authentification et vous avez terminé



User Authentication

User credentials are validated using the credentials for locally configured users on the 'User Permissions' page or any of the other supported authentication systems. RADIUS, LDAP, and SAML are optional external authentication systems that must be configured before they can be used. PAS only authentication allows implementing a custom authentication module and must be configured before it can be used.

⚠ IMPORTANT NOTE: Connection profiles of the **autologin** type authenticate using their certificate only and will therefore bypass credential-based authentication.

Default Authentication System

Users will be authenticated with the default authentication system unless otherwise configured for the group or user. Authentication systems that are greyed out can only be selected as default authentication system after configuring and enabling them. The Local and PAM authentication systems are always enabled.

● Local ○ PAM ○ RADIUS (disabled) ○ LDAP (disabled) ○ SAML (disabled) ○ PAS only (disabled)

Local User Passwords

Users authenticating via the local authentication system may be allowed to change their own passwords via the Client Web UI. For locally authenticated users a password strength requirement can optionally be enabled. This requirement applies only for changing the password of locally authenticated users. For all other authentication systems a password strength requirement should be configured on the respective authentication systems.

Allow local users to change password: Yes

Enforce strong passwords when changing: Yes