Inhoudsopgave

Azure AD Fortigate SSL VPN SSO Applicatie

SSO Applicatie aanmaken voor de vpn aanmaken:

Voor dat we SSO kunnen gaan instellen moeten we op azure ad een applicatie voorzien die authenticatie kan afhandelen met een saml en het best ook een Security user groep voorzien voor de vpn users.

Dit doen we door in azure ad naar ‘applications’ te gaan en dan naar ‘enterprise applications’

We maken dan een nieuwe applicatie aan, we hebben twee keuzes

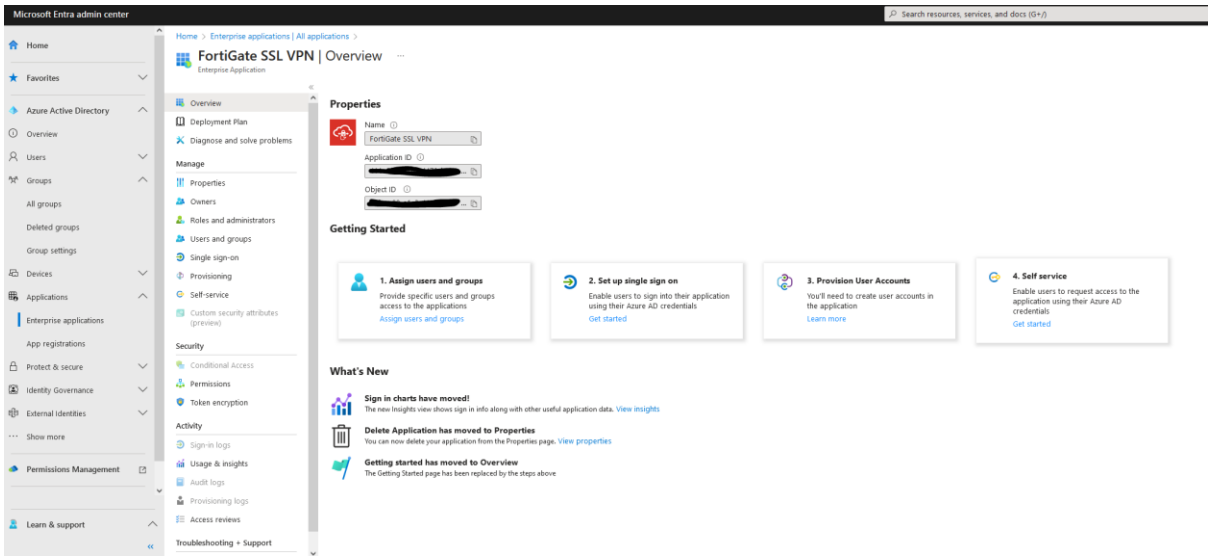
1. We gebruiken de built in fortigate ssl vpn applicatie in de azure ad gallery

2. of we maken een custom applicatie.

Omdat we een built in fortigate ssl vpn applicatie in de azure ad gallery hebben, gebruiken we deze dan ook, dit geeft een beter overzicht.

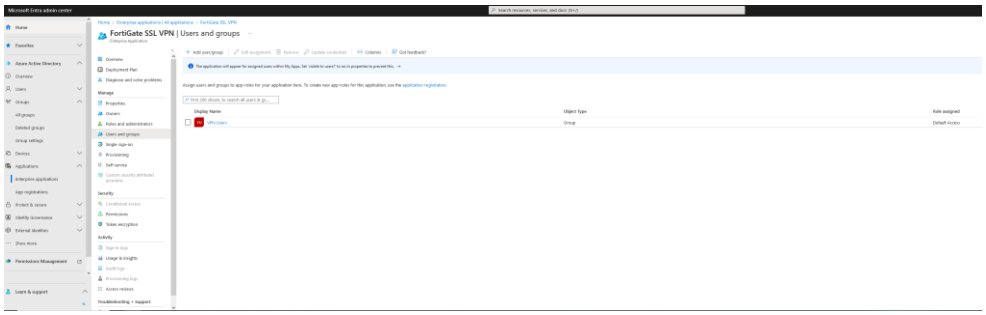
Nadat de applicatie is aangemaakt op azure dan maken we een security groep aan op de azure ad bv. ‘VPN users’ waaronder we alle gebruikers plaatsen die via de SSO kunnen inloggen om de vpn te kunnen gebruiken.

Nu we een groep hebben waaronder de vpn gebruikers vallen kunnen we via het overview menu van de applicatie in azure punt 1. Assign users and groups doen en punt 2. Set up single sign on.



VPN Groep toewijzen aan applicatie:

Als je in het menu gaat van de single sign on, dan krijg je een stappenplan, waar je kan doorlopen.
Stap 1. Is de user/groepen toewijzen.



Hier voegen we de azure ad groep toe dat via SSO de sign in mag doen voor de vpn.

Single Sign On opstellen:

Als je in het menu gaat van de single sign on, dan krijg je een stappenplan, waar je kan doorlopen.

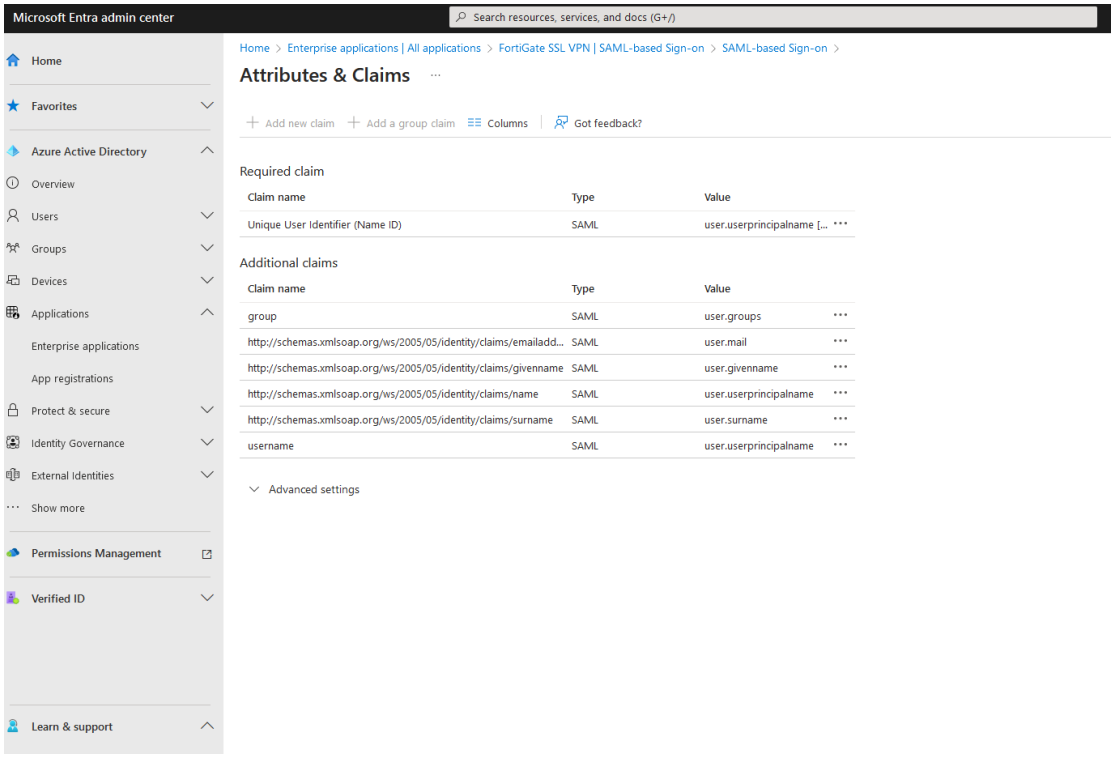
Bij stap 1. Basic SAML Configuration geven we het adres of de FQDN van de fortigate die via het publiek internet te bereiken is en de poort waarop de fortigate VPN server bereikbaar is. (let wel op dat het protocol bv. https overeen komt!)
Dit wordt dan opgevolgd met het pad “/remote/saml/metadata” voor het veld “Identfier (Entity ID)

Voor de Reply URL (Assertion Consumer Service URL) is de FQDN/IP hetzelfde en het pad is “/remote/saml/login”.

Voor de Sign on URL is de FQDN/IP ook hetzelfde en he pad is “/remote/saml/login”.

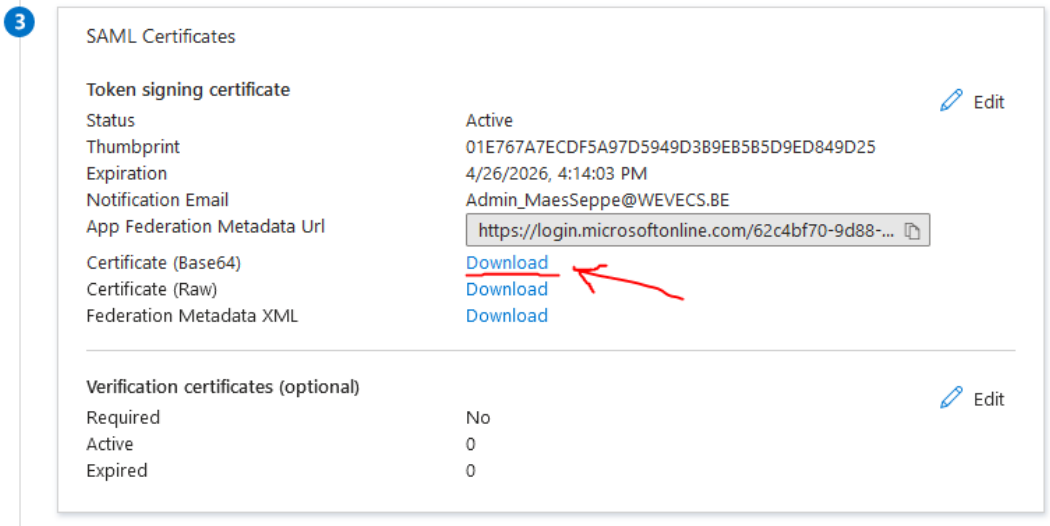
In dit geval hebben we geen Relay State.

Voor de Logout URL is de FQDN/IP ook hetzelfde en het pad is “/remote/saml/logout”.

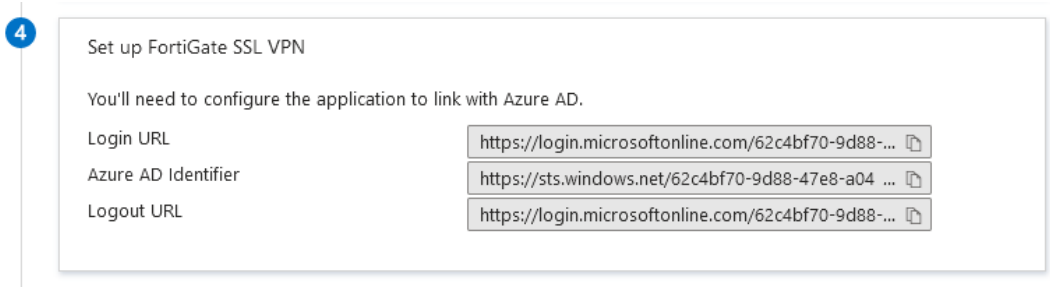


Bij “Attributes & Claims” is het belangerijk dat we twee additional claims instellen, een hiervan is de claim “group” met als waarde “user.groups” en een claim “username” met als waarde “user.userprinciplename”.

Deze claims zijn nodig zodat de fortigate en de azure ad authenticatie met elkaar kunnen uitwisselen een SAML token kan meerdere claims bevatten maar in dit geval moet de fortigate/azure ad alleen mar de username en group claim doorsturen met de token voor de authenticatie te kunnen verrichten.



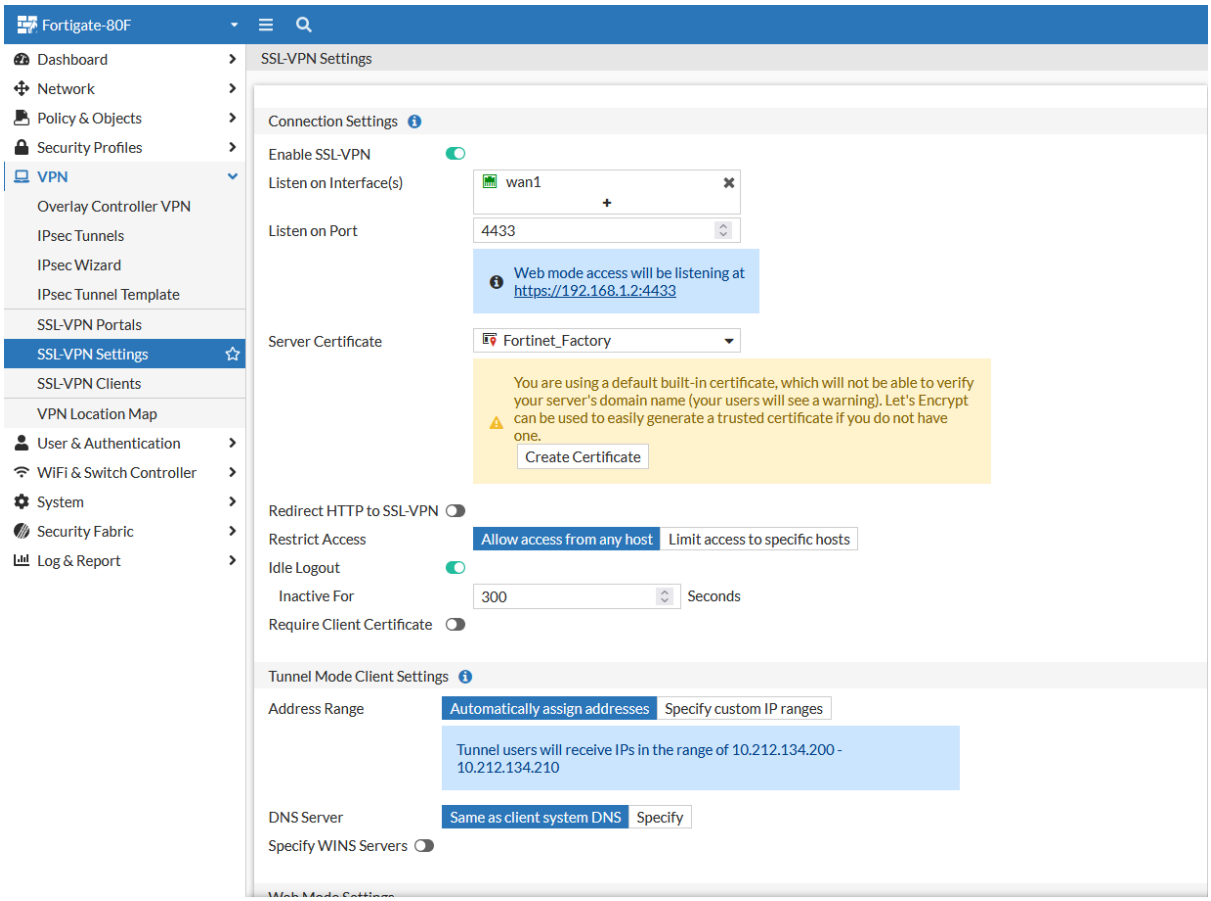
In het derde puntje “SAML Certificates” downloaden we het “Base64” Certificaat, dit gaan we later nodig hebben voor als we SSO instellen op de fortigate.



Bij het vierde puntje kopiëren we de “Login URL”, de “Azure AD Identifier” en de “Logout URL”. Deze gaan we later ook nodig hebben als we de configuratie voor SSO op de fortigate firewall gaan doen.

FortiGate GUI:

SSL-VPN Settings:



Enable SSL-VPN: Eerst schakelen we De VPN server in door op ‘Enable SSL-VPN’ op aan te zetten.

Listen on Interface(s): Als ‘Listen on Interfaces(s) gebruiken we de Interface(s) waarop de clients binnekomen, in ons geval is dit op de Wan1 interface die naar het internet gericht staat.

Listen on Port: Als ‘Listen on port’ selecteren we een poort naar keuzen waarop de clients verbinding gaan maken met de VPN, deze poort mag niet een poort zijn die al wordt gebruikt op de fortigate, in dit geval gebruiken we poort 4433 omdat poort 443(default) al gebruikt wordt.

Server Certificate: Als ‘Server Certificate’ gebruiken we het built in ‘Fortinet_Factory’ Certificaat, je kan evengoed een signed Certificaat door een eigen of publieke CA gebruiken of een van let’s encrypt via de fortigate zelf laten aanmaken. (Zorg wel dat voor het let’s encrypt certificaat dat let’s encrypt de fortigate kan bereiken via ACME op de benodigde poort(en) (TCP/80))

Restrict Access: plaatsen we op ‘Allow access from any host’ omdat de vpn gaat dienen als een algemene remote access vpn voor als de gebruiker buiten het bedrijf is bv. Op een ander bedrijf/openbare plaats, etc.

Hierdoor kunnen we moeilijk een host ip gebruiken voor access te limiteren aangezien dit dynamisch is.

Idle Logout: in dit geval staat de idle logout ingesteld na 5min. Dit is de tijd nadat de server de vpn verbinding met de host sluit moest de host inactief zijn.

Require Client Certificate: ‘Require Client Certificate staat uit in ons geval omdat we al via azure SSO authenticatie uitvoeren met 2FA waardoor een Certificaat authenticatie per apparaat niet nodig is.

Address range: Voor de ‘Address Range’ gebruiken we de built in ‘Automatically assign addresses’ range van 10.22.134.200 – 210, dit doen we omdat deze range genoeg is voor het aantal gebruikers dat de vpn actief gaan gebruiken.

DNS Server: Same as client system DNS

Authentication/Portal Mapping: zorgen we ervoor dat de VPN Users groep ‘Tunnel-access’ heeft.

SSL-VPN Portals:

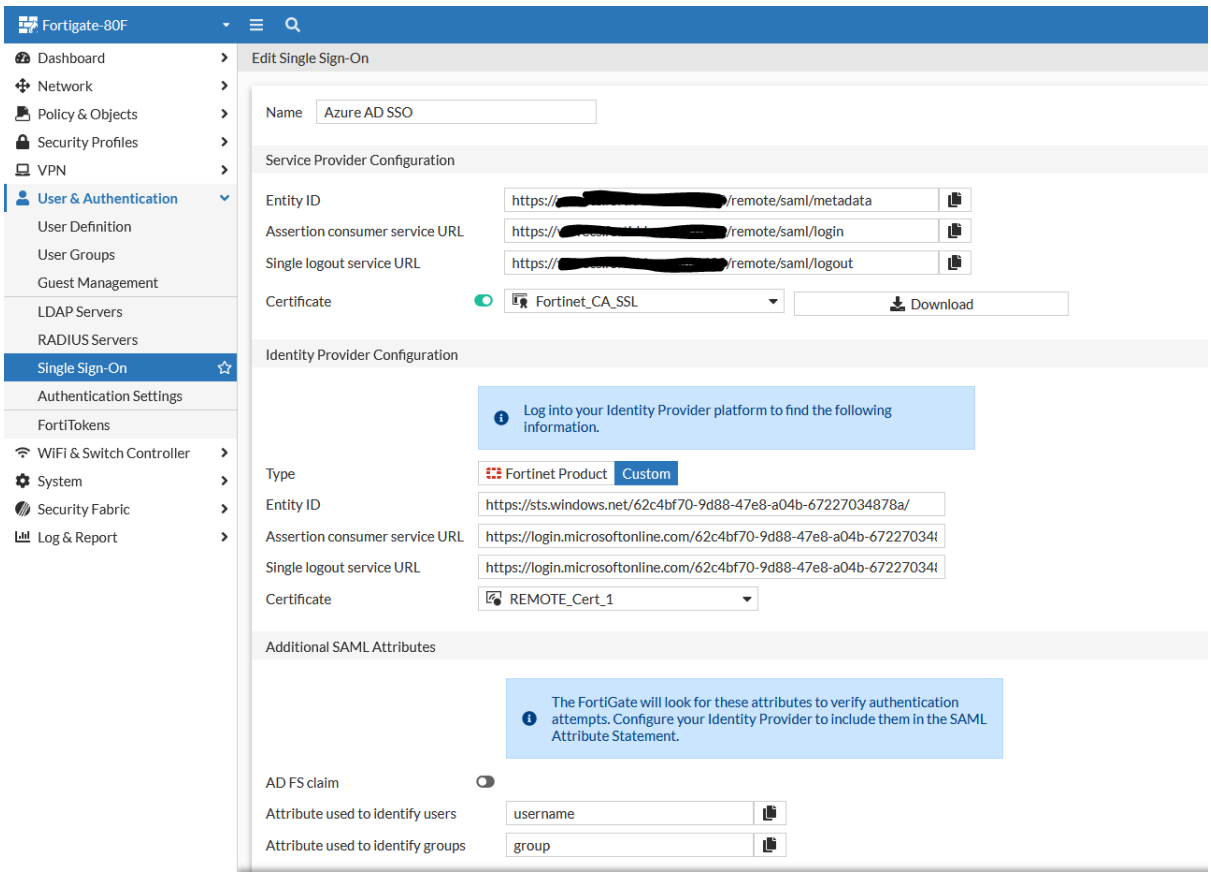
In de ‘SSL-VPN Portals’ tab kan je de access groepen bepalen en welk type access ze krijgen.

In ons geval heeft de built in ‘web access’ geen toegang tot zowel web mode als tunnel mode, omdat we de ‘web access’ niet gebruiken.

‘Tunnel access’ heeft alleen recht op tunnel mode.

We gebruiken in onze situatie alleen tunnel mode omdat al onze clients de forticlient vpn gepushed krijgen via intune.

Single Sign-On:



Name:

In het name field vul je de logische naam in voor de SSO instelling/verbinding

Service Provider Configuration:

Het veld Entity ID, Assertion consumer service URL en Single logout service URL verwijzen in dit geval naar de bestanden/waarden die de client moet aaspreken op de fortigate.

Het adres kan zowel een ip adres als een FQDN zijn, in dit geval is er een DDNS van fortinet gebruikt om het dynamisch ip “statisch” te houden doormiddel van een domeinnaam.

Als Certificate gebruiken we in dit geval als voorbeeld het built in “Fortinet_CA_SSL” certificaat, maar dit kan evengoed een signed certificaat zijn van een provider of een let’s encrypt certificaat dat aangevraagd is met fortigate zijn built in service.

Identity Provider Configuration:

Als type selecteren we in dit geval “Custom” omdat we als provider microsoft azure willen gebruiken omdat we SSO willen toepassen via onze azure ad gebruikers.

De EntityID, Assertion Consumer service URL, Single logout service URL en Certificate kunnen worden teruggevonden in de aangemaakte single sign on applicatie op azure ad, zie hiervoor het document, “(Fortigate SSL VPN) applicatie maken op azure”.

Nadat je dit hebt gedaan en de nodige velden vanuit de applicatie hebt genomen dan kan je deze overzetten in de fortigate.

Additional SAML Attributes:

Identify users: identify users moet “userame” zijn

Identify groups : identify groups moet “group” zjn

Deze waarden zijn belangrijk en moeten overeenkomen met de waarden ingesteld op de azure ad applicatie voor SSO (fortigate SSL VPN)

User Groups:

In de tab ‘User Groups’ passen we de aangemaakte VPN Users groep aan en voegen we een Remote Group toe, als remote server selecteren we de “Azure AD SSO” dat we hebben aangemaakt op Single Sing-On op de fortigate. (zie puntje Single Sign-On)

En als ‘Groep Name’ gebruik je de Object id van de groep op azure ad die toegang heeft tot de Fortigate SSL VPN applicatie op azure ad dit hebbe we nodig omdat we een match met een lokale groep en een remote groep moeten hebben voor onze policies op de firewall.

(moest dit niet lukken via de GUI dan kan je met de volgende commando chain hetzelfde toekomen.

```
config user group
  edit "VPN Users"
    set member "Azure AD SSO"
    config match
      edit 1                                    ---> match = 1 !!!
        set server-name "Azure AD SSO"          ---> naam voor remote ldp (Azure) aangemaakt in GUI
        set group-name "1ae6f576-0d66-4dd7-a627-519d0df24c86"  ---> Object id van user group in azure ad
```