HowTo mise en place d'EntraID (via GUI)

- Cinématique de configuration par l'administrateur de l'autorisation des comptes EntraID à monter des tunnels VPNSSL.
- Application SNS dans EntraID
  - Création de l'application
    - Configuration de l'application SNS dans EntraID
    - Configuration du jeton
    - Création du secret
  - Association des utilisateurs
- Configuration du SNS
  - Configuration de la méthode OIDC pour EntraID
    - Mettre à jour le profil d'authentification OIDC
  - Configuration des URL de redirection dans EntraID
    - Renseigner dans l'application SNS Connector, les URI de redirection souhaitée à partir de celles proposées
    - Vérifier de nouveau la configuration du SNS
  - Importation des groupes de sécurité d'EntraID
  - Configuration du groupe de sécurité dans les UAC pour autoriser le VPNSSL
    - Création d'une règle d'authentification
    - Création d'une règle d'accès
  - Utilisation du client VPN SSL 5.1

> Cette procédure décrit l'ensemble des opérations de configuration à réaliser à la fois dans EntraID et sur le SNS.
>
> Néanmoins, il est fortement recommander d'avoir au préalable des notions sur la solution EntraID et les possibilités offres par l'authentification via une application "OpenID Connect".

Cinématique de configuration par l'administrateur de l'autorisation des comptes EntraID à monter des tunnels VPNSSL.

Déroulement :

1. Sur EntraID, configuration de l'application SNS dans EntraID
2. Sur EntraID, association des utilisateurs, dont celui de test, à un groupe de sécurité qui sera autorisé pour le VPNSSL.
3. Sur EntraID, exportation des groupes de sécurité d'EntraID concernés par le SNS.
4. Sur le SNS, configuration de la méthode OIDC pour EntraID
5. Sur le SNS, importation des groupes de sécurité d'EntraID
6. Sur le SNS, configuration du groupe de sécurité dans les UAC pour autoriser le VPNSSL.
7. Sur le Client VPNSSL, monter le tunnel avec un compte de test
8. Sur le SNS, validation dans le monitoring des utilisateurs et des tunnels VPNSSL.

Application SNS dans EntraID

> L'ensemble des manipulations sont à réaliser dans la partie 'Identité'

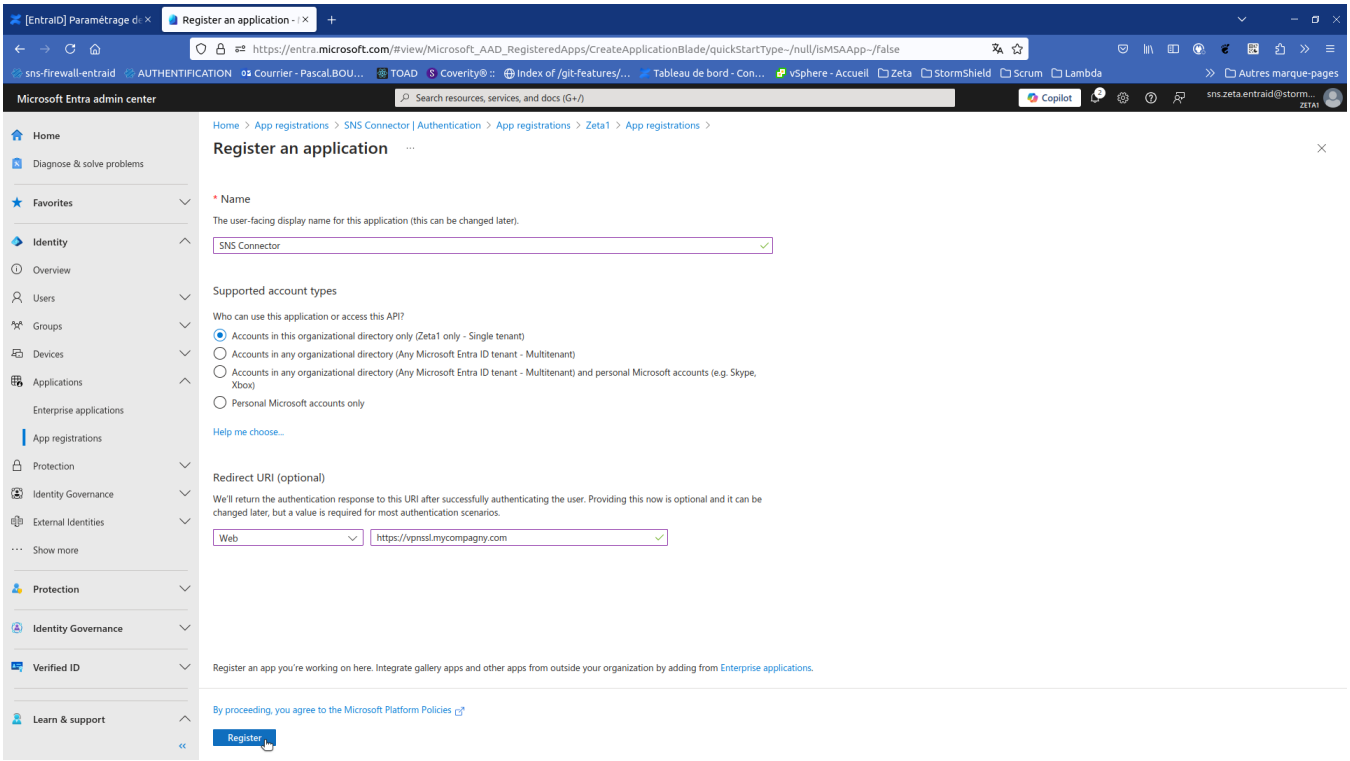
Création de l'application

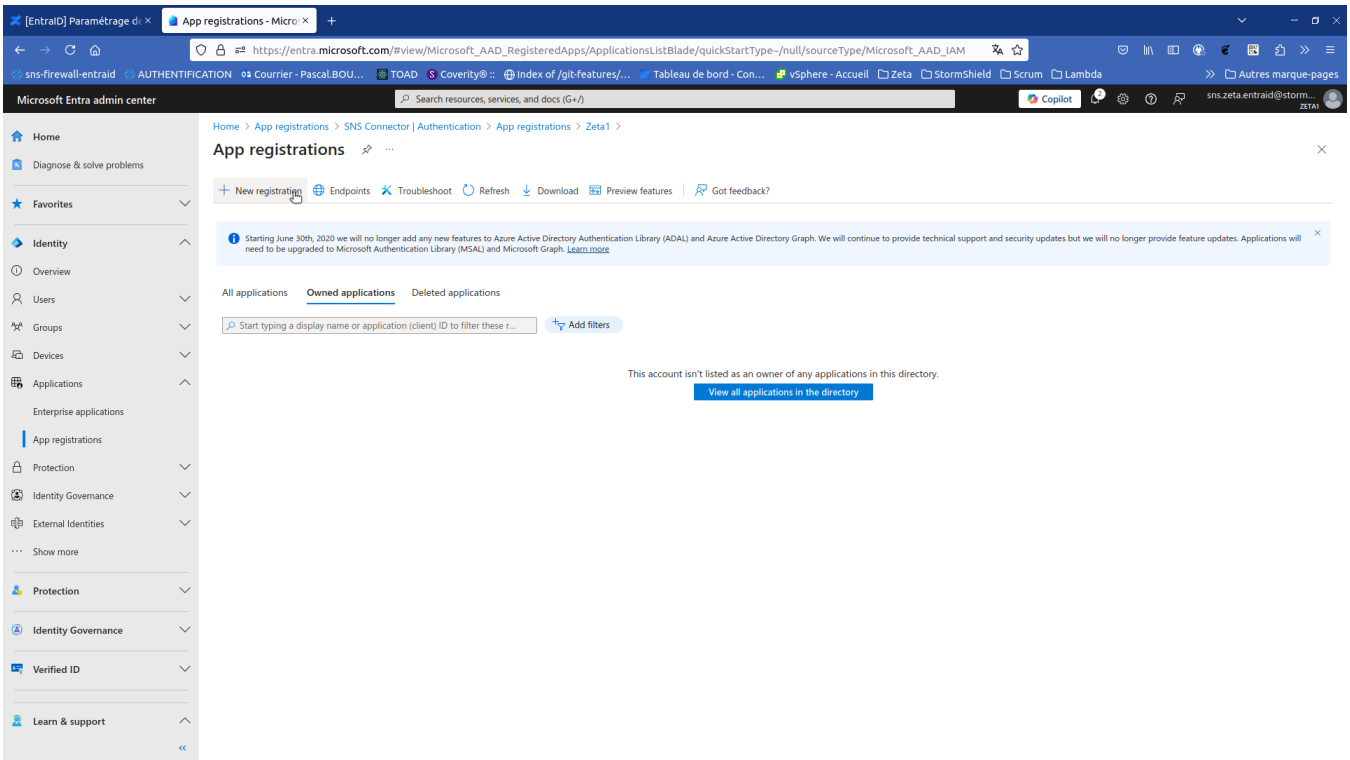
Configuration de l'application SNS dans EntraID

Depuis l'interface d'administration de votre espace EntraID "Inscrire une application" nommée "**SNS Connector**"

avec "URI de redirection (facultatif)" en mode "**Web**"

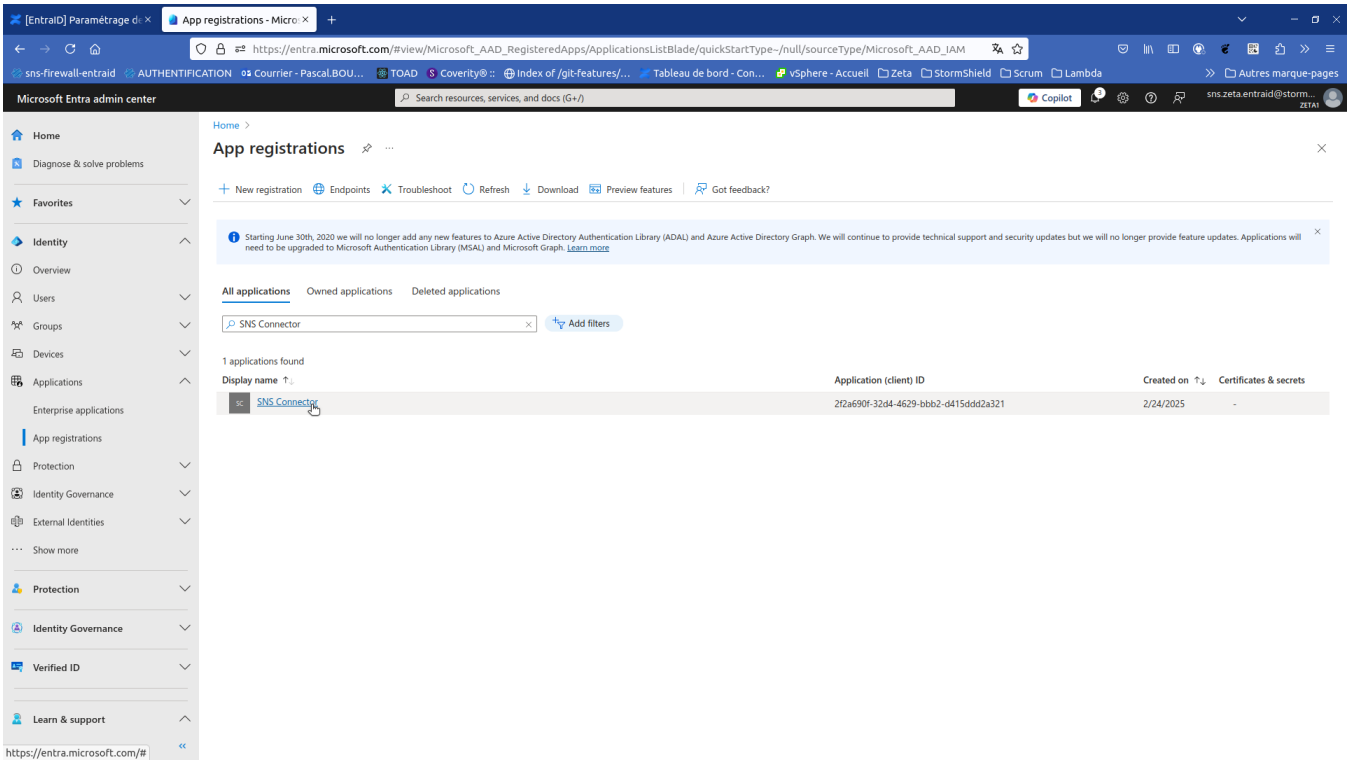
et mettre l'URL publique du SNS par exemple : "https://vpnssl.mycompany.com**/auth/v1/oidc/token/sslvpn**"



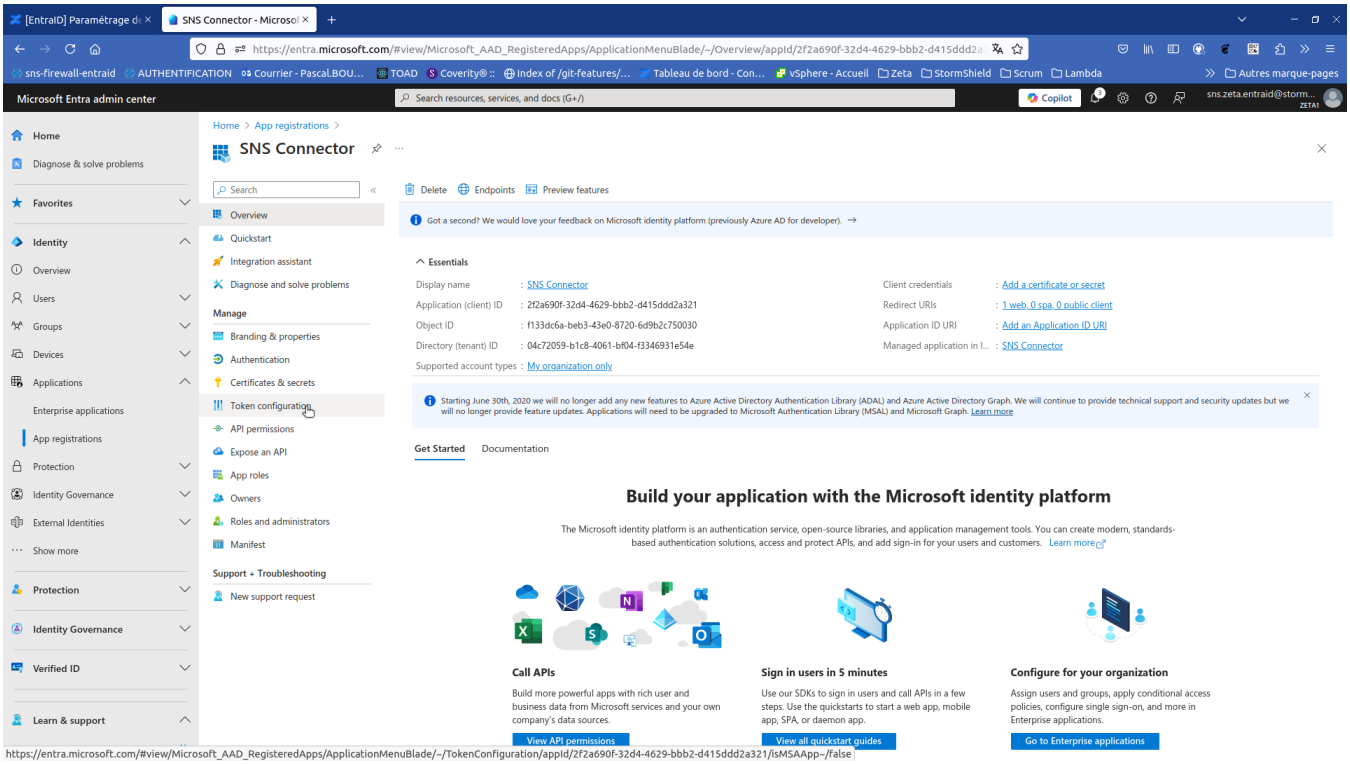


Configuration du jeton

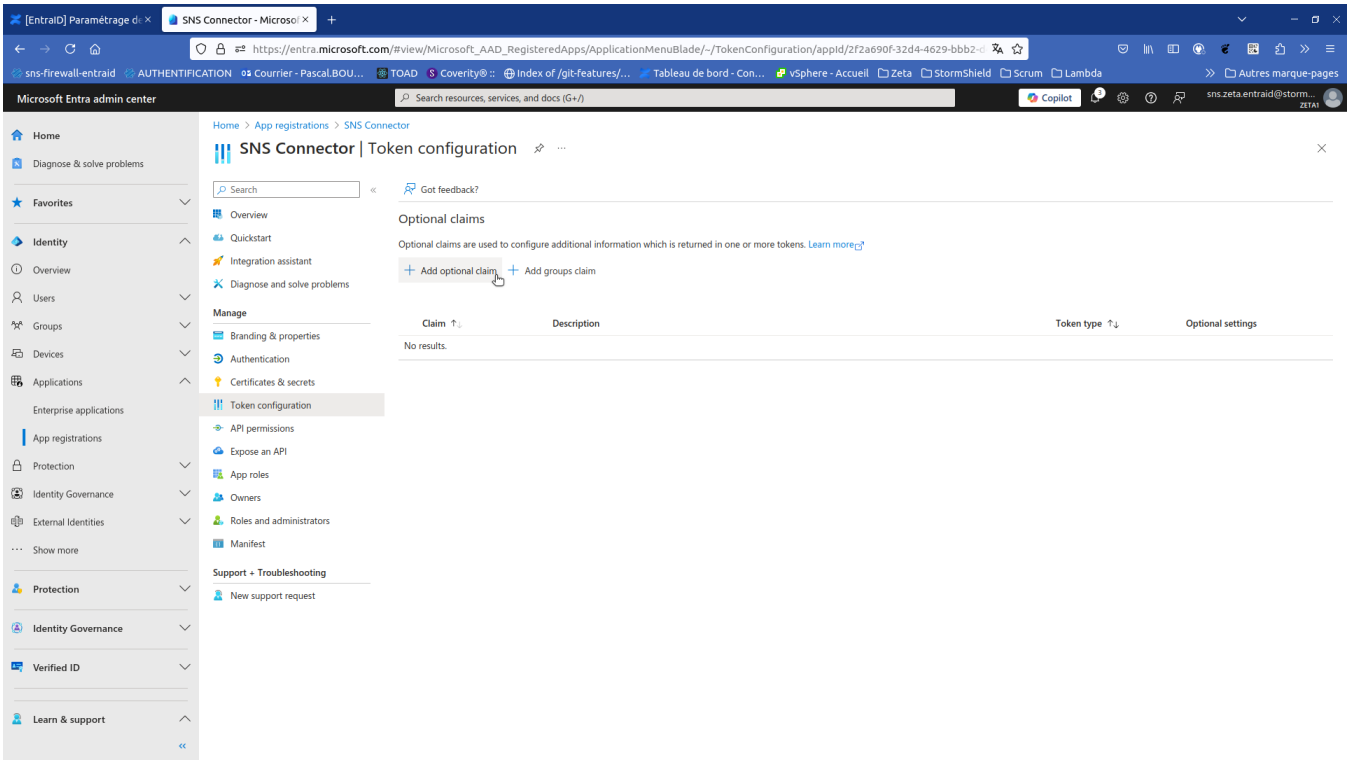
1/ Aller dans "Inscription d'application" ; cliquer sur "Afficher toutes les applications dans l'annuaire" et sélectionner l'application SNS connector, puis "Configuration des jetons"

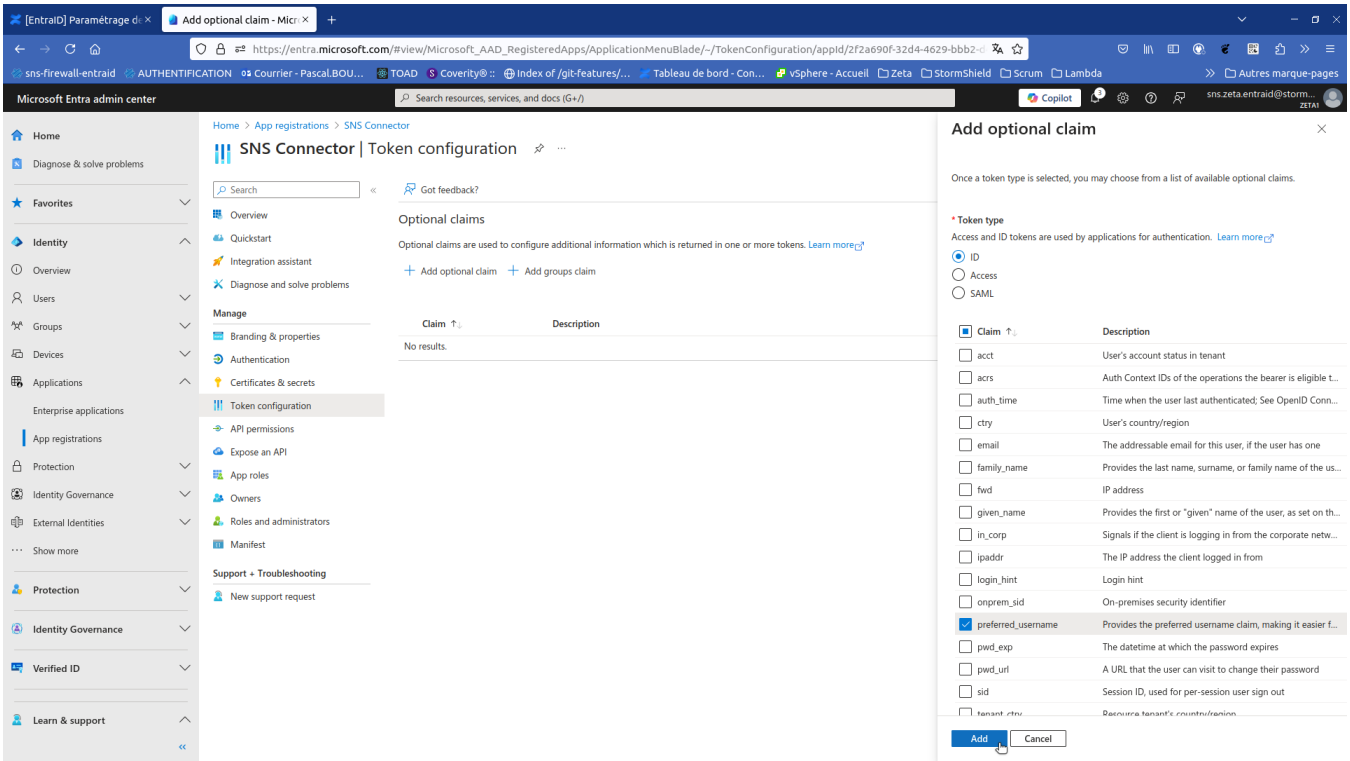


Token configuration :



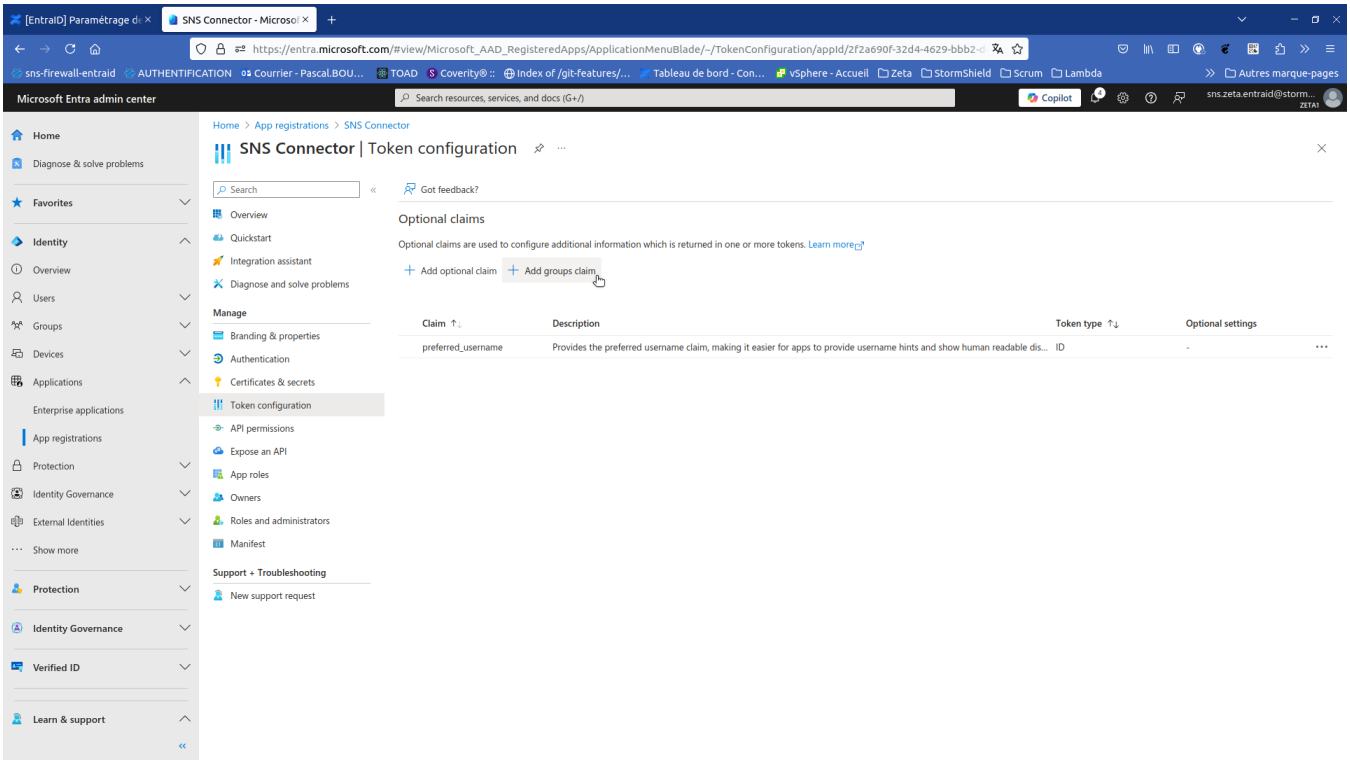
2/ Ajouter la revendication optionnelle "preferred_username" pour l'ID Token (⚠️ **obligatoire pour SNS**)

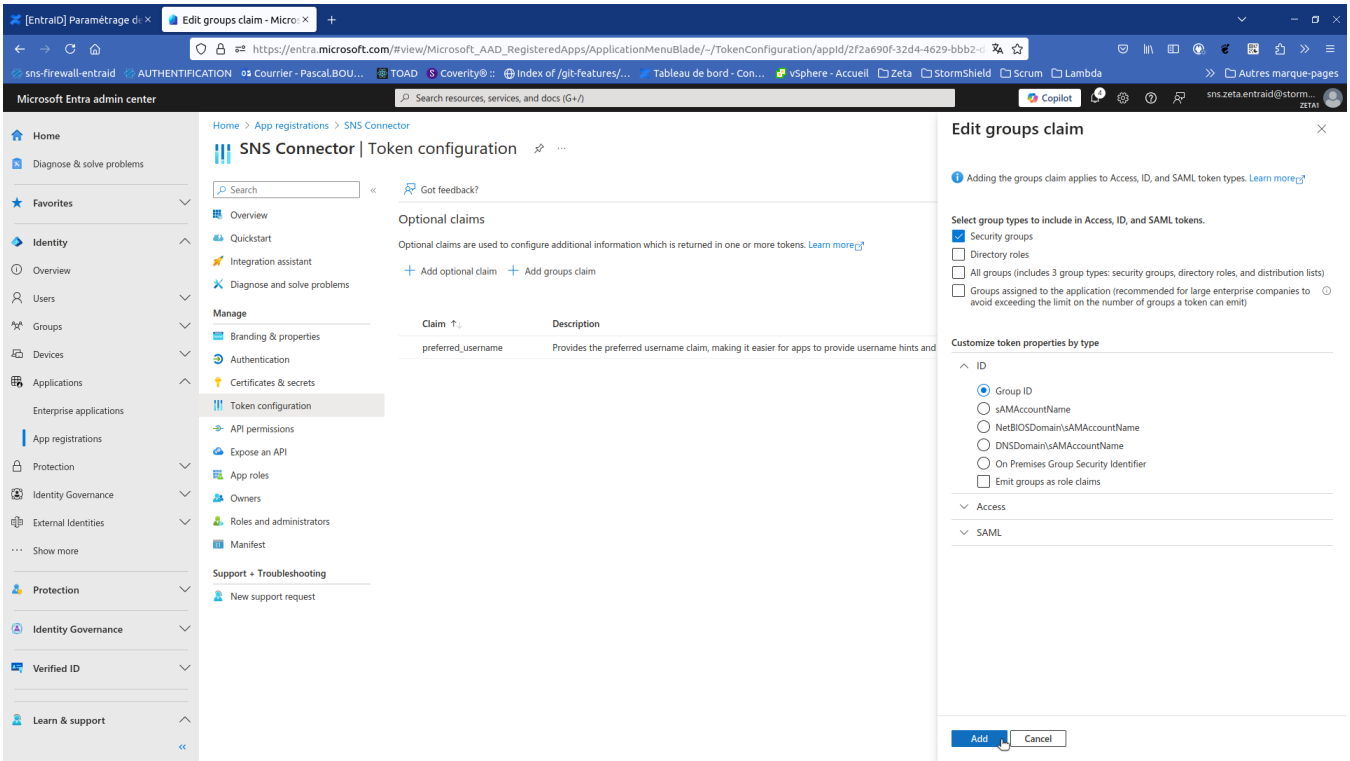




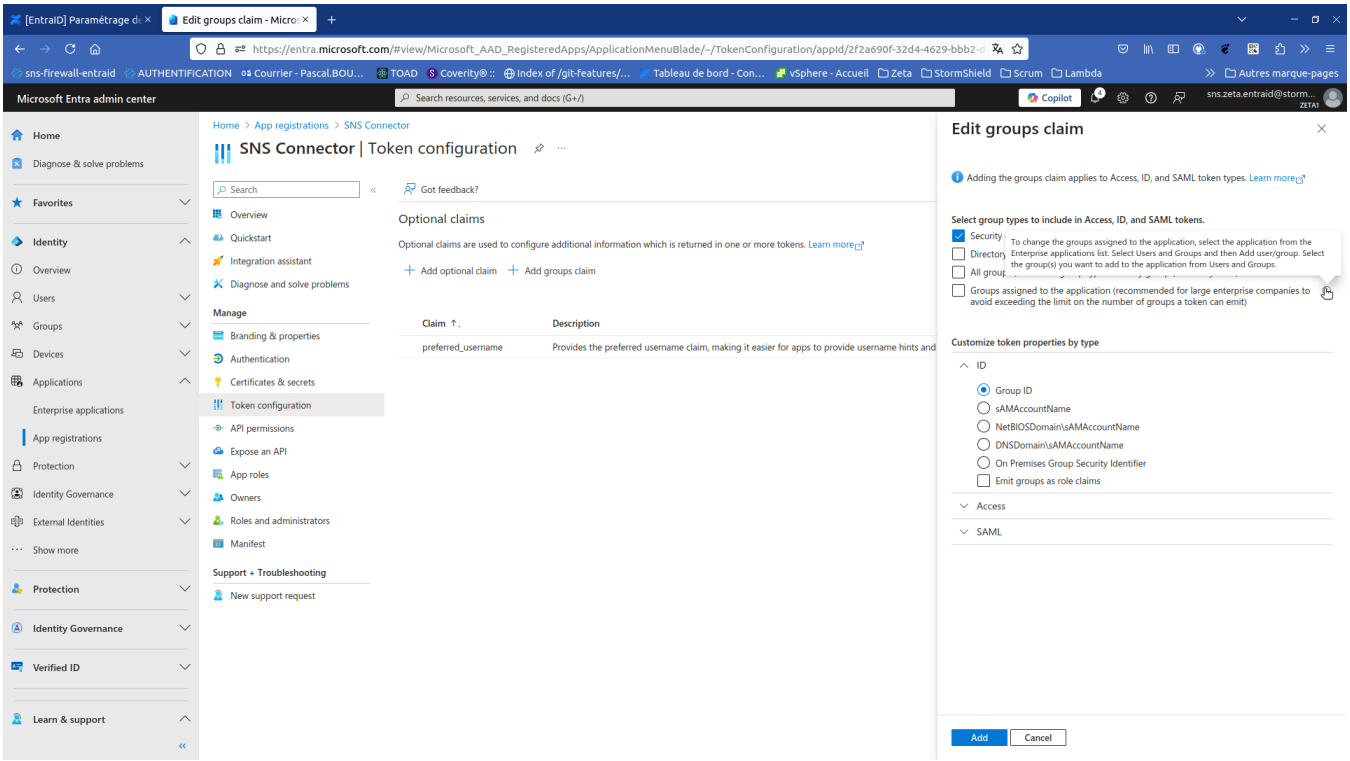
3/ Pour "Ajouter une revendication de groupes", et dans l'encart "Modifier la revendication de groupes", cocher "Groupes de sécurité" avec ID sur "ID de groupe".

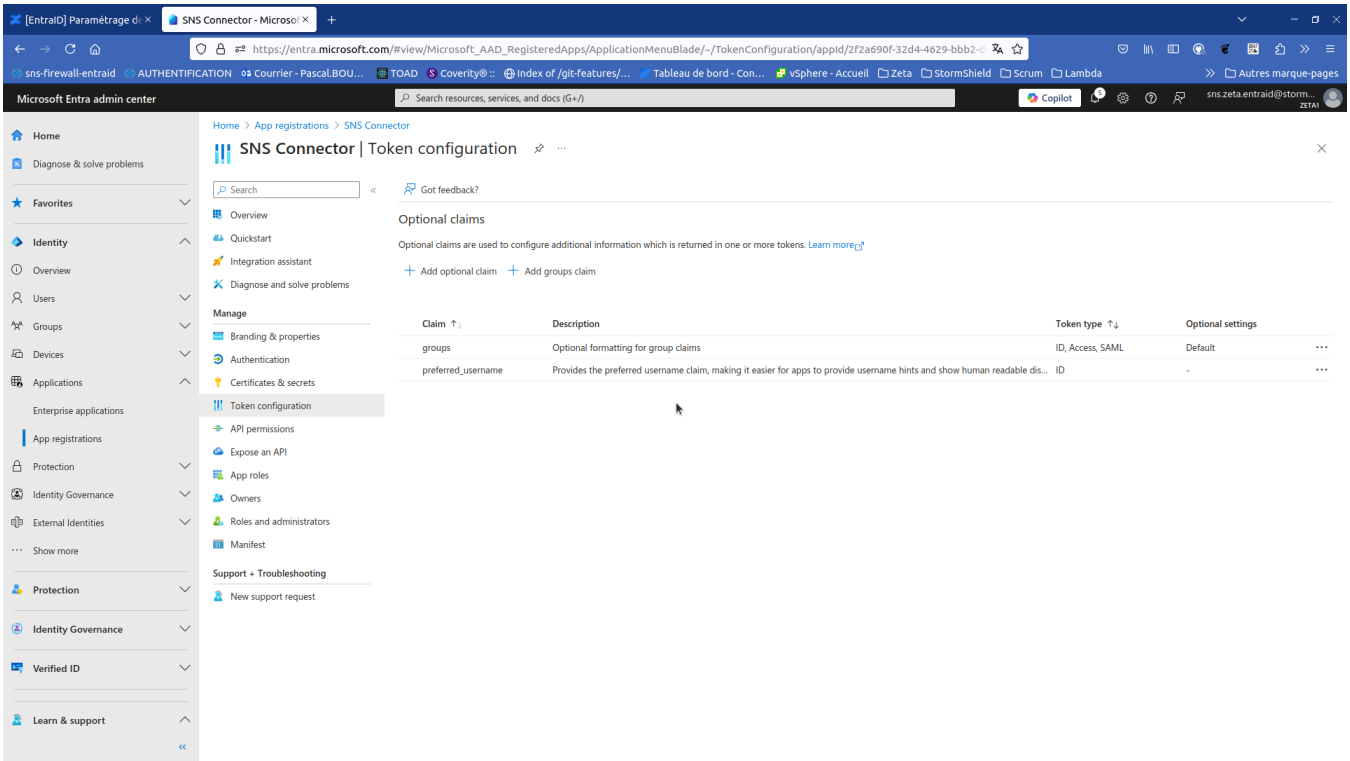
optionnel pour SNS mais fortement recommandé afin de pouvoir bénéficier des UAC/AAC/politiques de filtrages et d'authentification sur les groupes de sécurité.





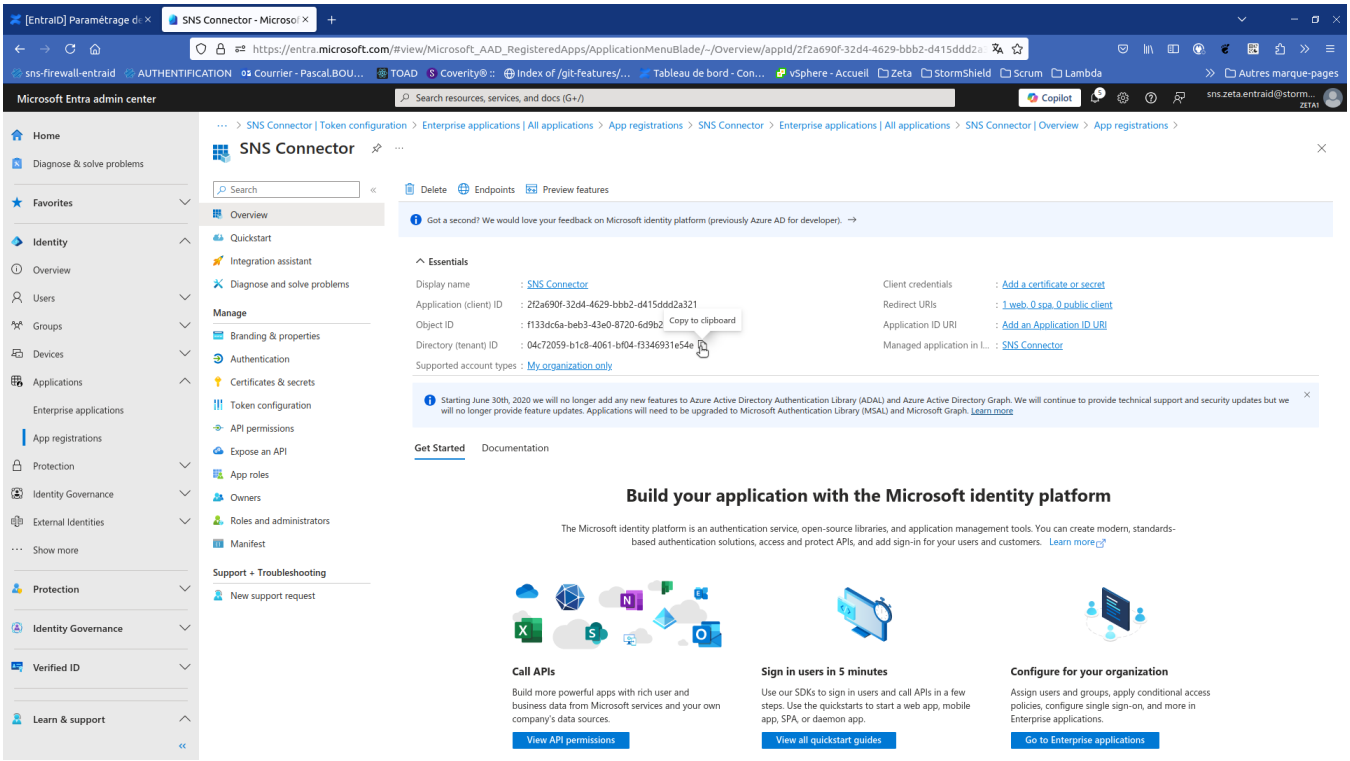
A noter qu'il est possible de limiter les groupes à inclure dans l'ID Token à ceux assignés à l'application, mais cela est conditionné à abonnement P1.

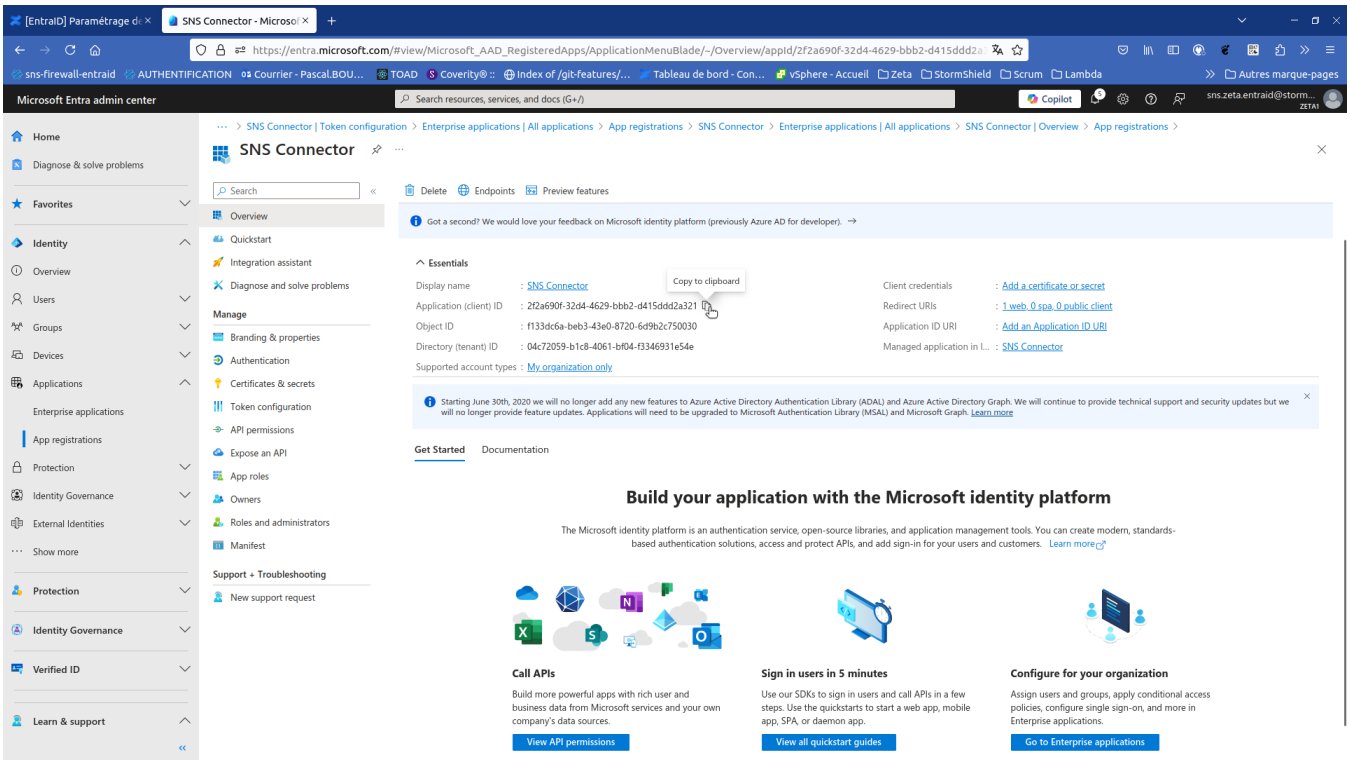




4/ À partir de App registrations SNS Connector Overview

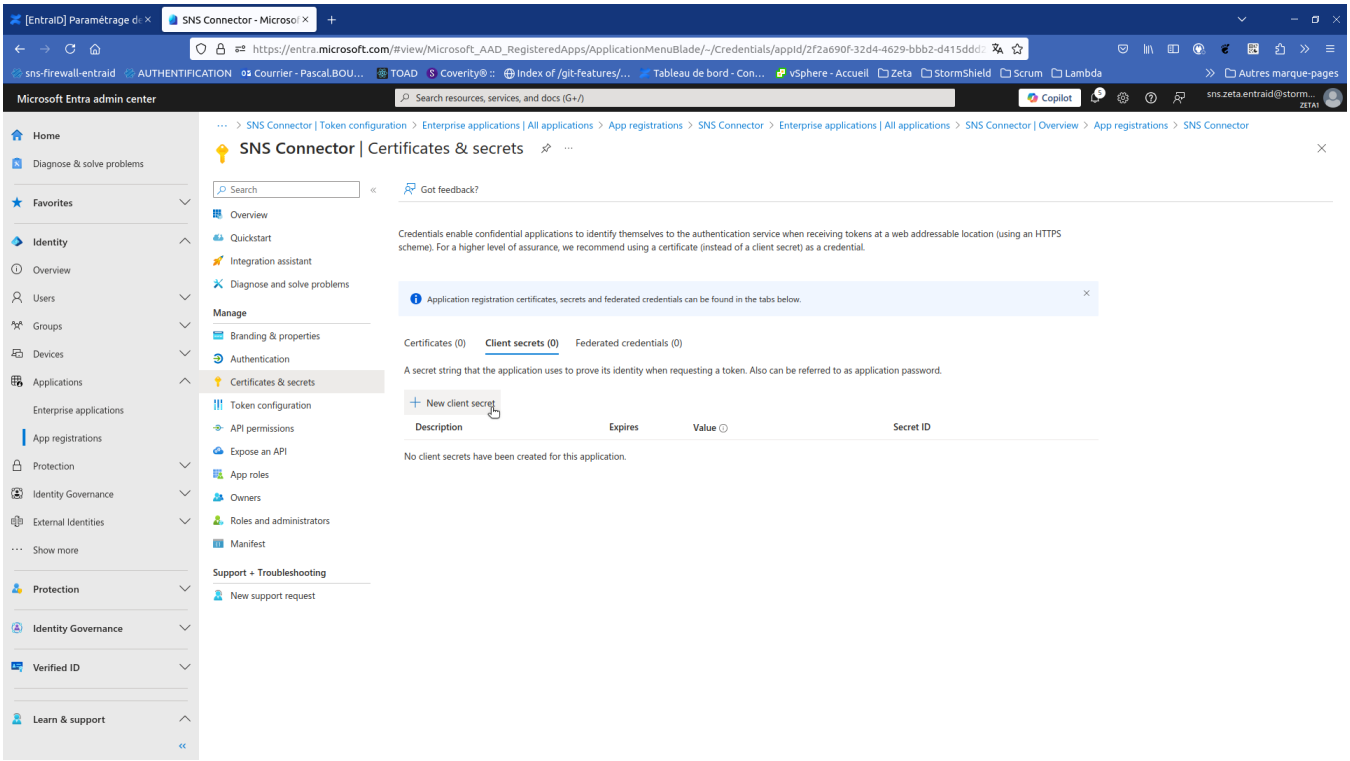
- Copier la valeur du "ID de l'annuaire (locataire)" pour renseigner le "IssuerID" dans la configuration du SNS.
- Copier la valeur du "ID d'application (client)" pour renseigner le "ClientID" dans la configuration du SNS.

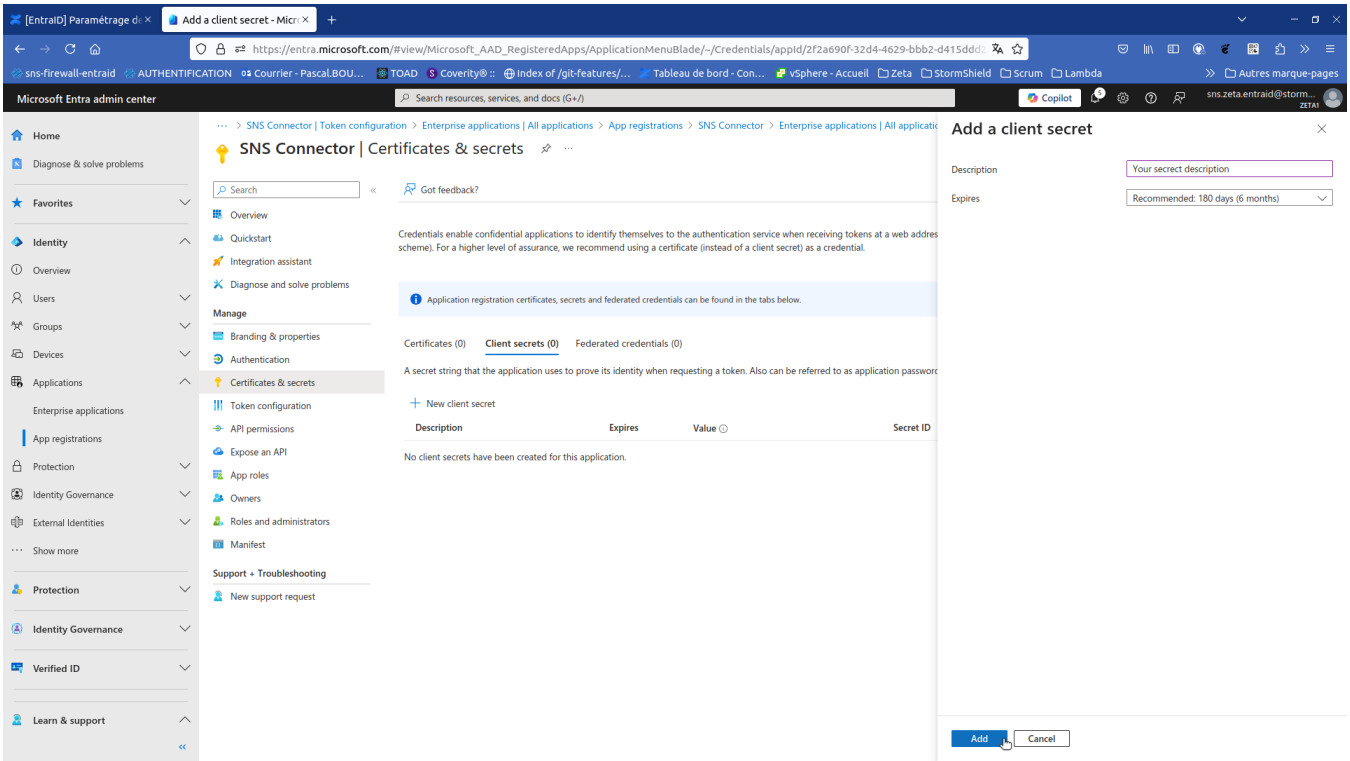


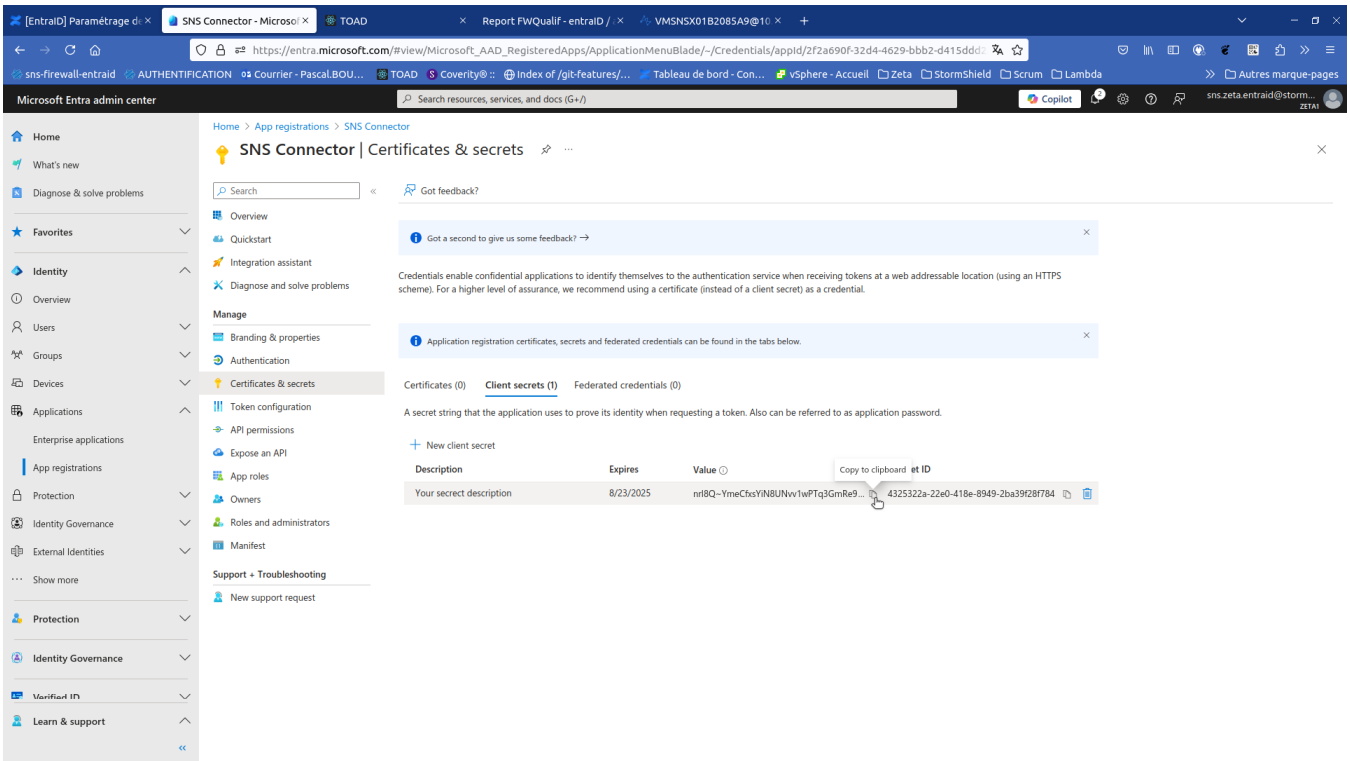


Création du secret

1/ Dans le menu "Certificats & secrets", onglet '"Secrets client", créer un "nouveau secret client"


[EntraID] Paramétrage de
SNS Connector - Microso
https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/appId/2f2a690f-32d4-4629-bbb2-d415ddd
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
SNS Connector | Token configuration > Enterprise applications | All applications > App registrations > SNS Connector > Enterprise applications | All applications > SNS Connector | Overview > App registrations > SNS Connector
SNS Connector | Certificates & secrets
Got feedback?
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
Application registration certificates, secrets and federated credentials can be found in the tabs below.
Certificates (0)
Client secrets (0)
Federated credentials (0)
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
New client secret
Description
Expires
Value
Secret ID
No client secrets have been created for this application.
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
New support request
Home
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Enterprise applications
App registrations
Protection
Identity Governance
External Identities
Show more
Protection
Identity Governance
Verified ID
Learn & support


[EntraID] Paramétrage de
Add a client secret - Micr
https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/appId/2f2a690f-32d4-4629-bbb2-d415ddd
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
SNS Connector | Token configuration > Enterprise applications | All applications > App registrations > SNS Connector > Enterprise applications | All applicatio
SNS Connector | Certificates & secrets
Got feedback?
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addres
scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
Application registration certificates, secrets and federated credentials can be found in the tabs below.
Certificates (0)
Client secrets (0)
Federated credentials (0)
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application passwor
New client secret
Description
Expires
Value
Secret ID
No client secrets have been created for this application.
Add a client secret
Description
Your secret description
Expires
Recommended: 180 days (6 months)
Add
Cancel

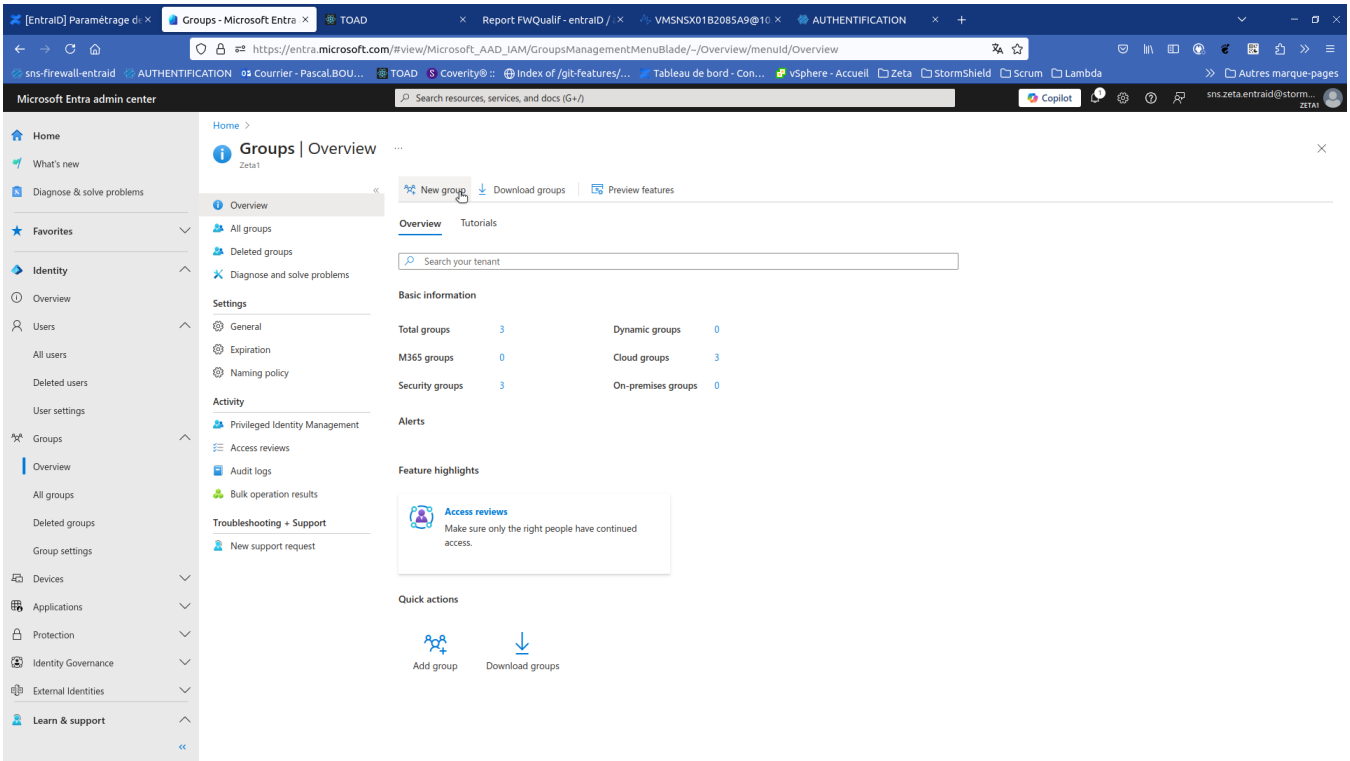


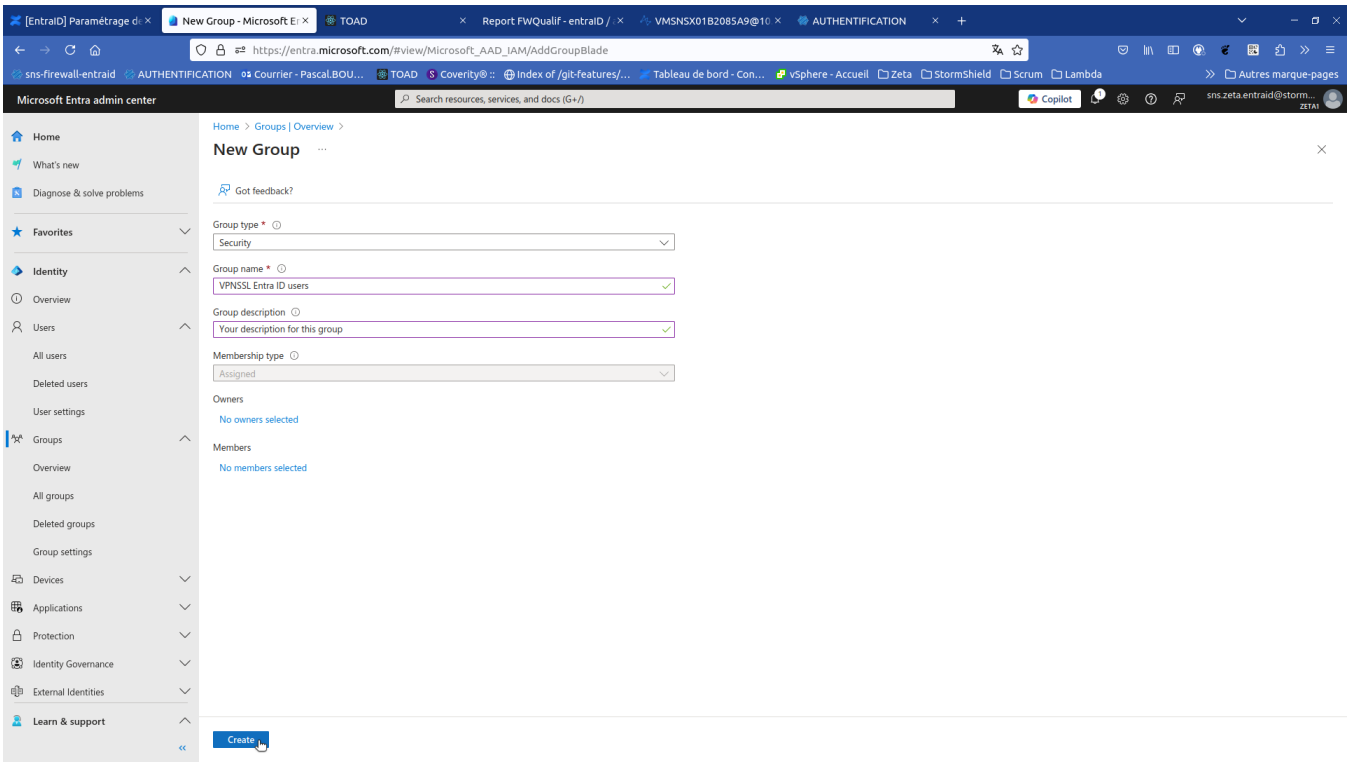
2/ Copier la valeur du secret pour par la suite renseigner le "ClientSecret" dans la configuration du SNS.

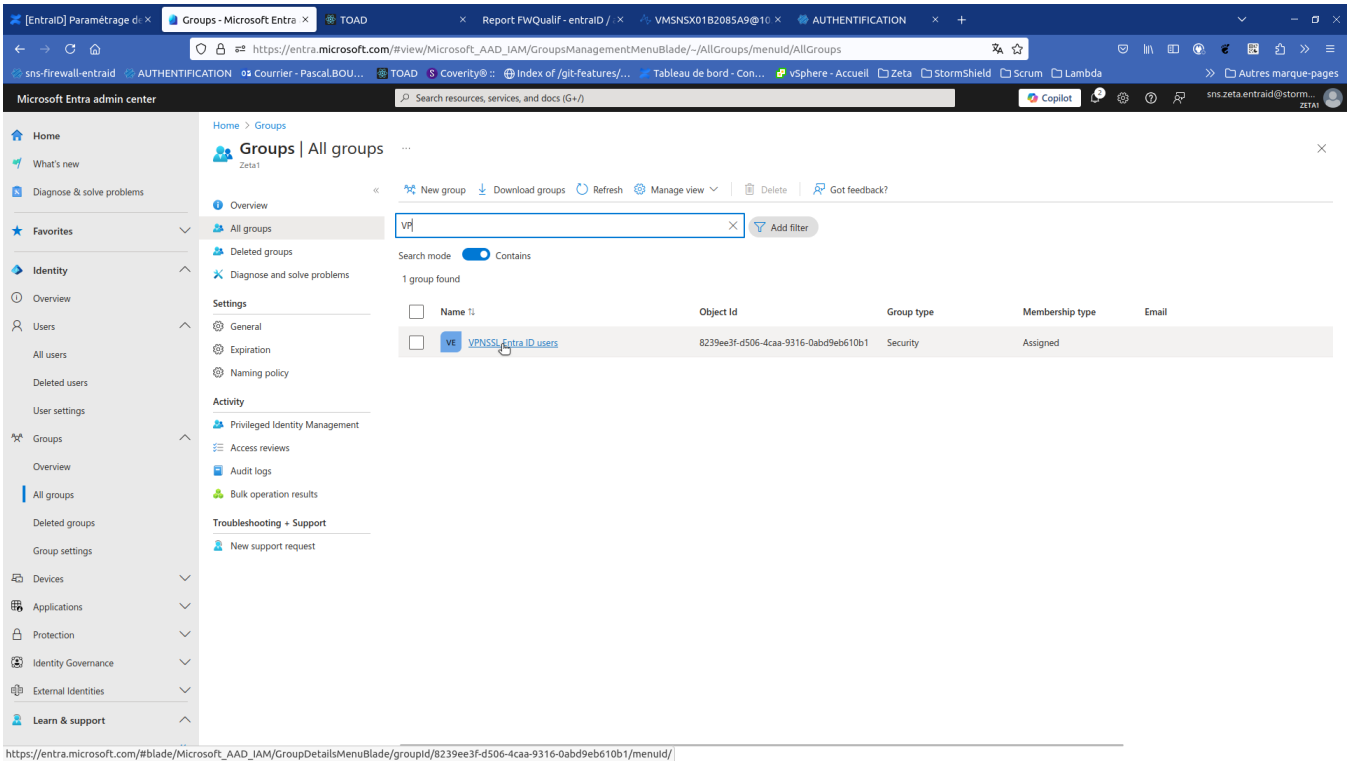
Association des utilisateurs

Association des utilisateurs à un groupe de sécurité qui sera autorisé pour le VPNSSL.

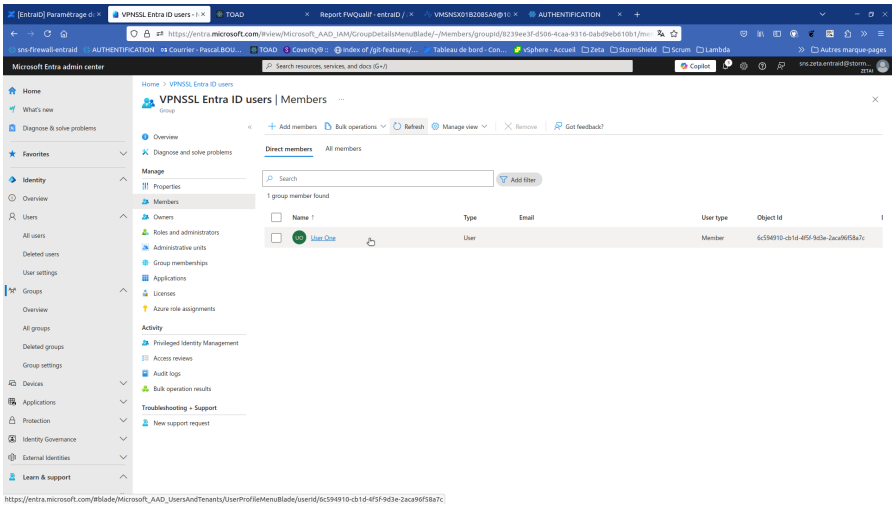
1/ Aller dans "Groupes" et créer un groupe de sécurité nommé 'VPNSSL EntraID Users'

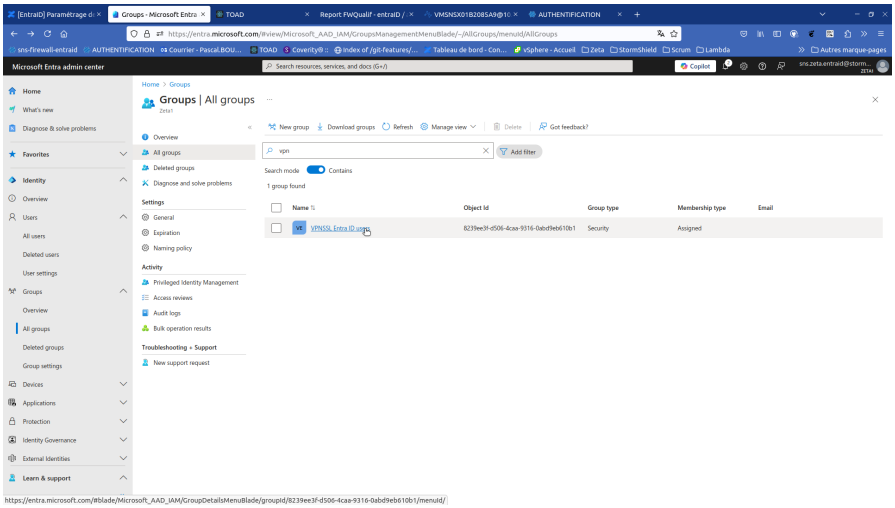


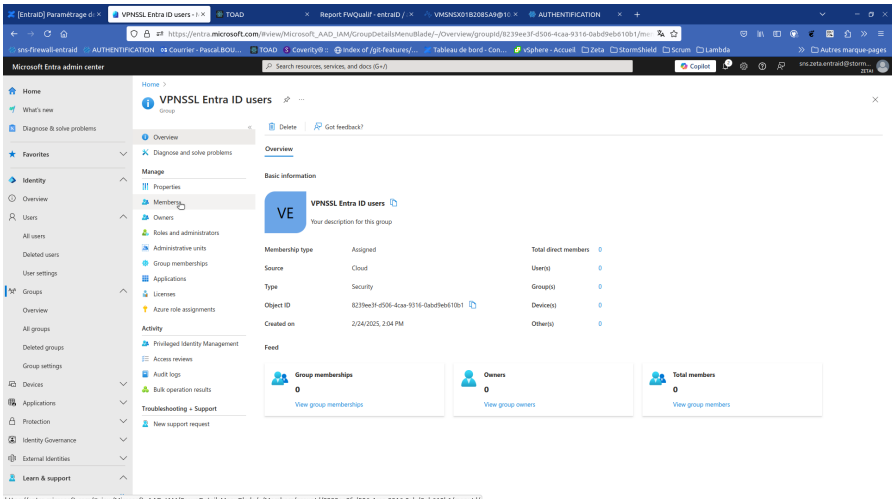


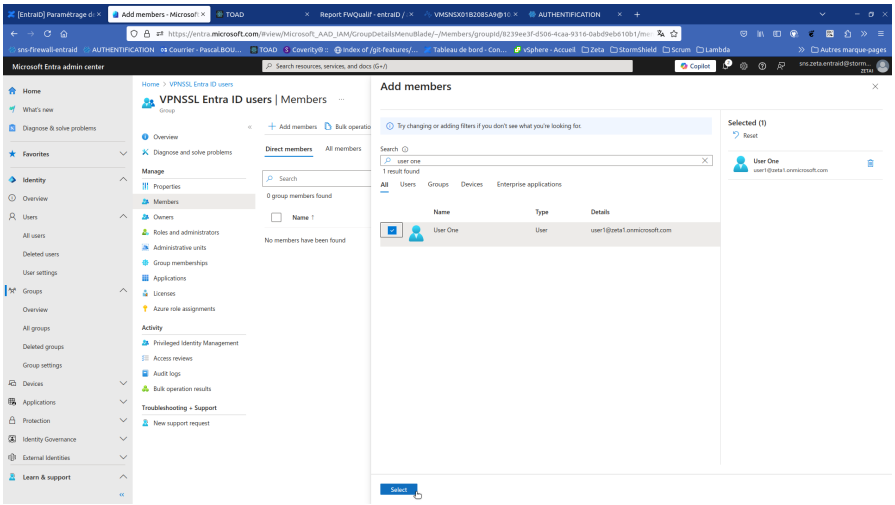


2/ Associer à ce groupe, les utilisateurs qui seront autorisés à monter un tunnel VPN SSL (ℹ plusieurs méthodes possibles)

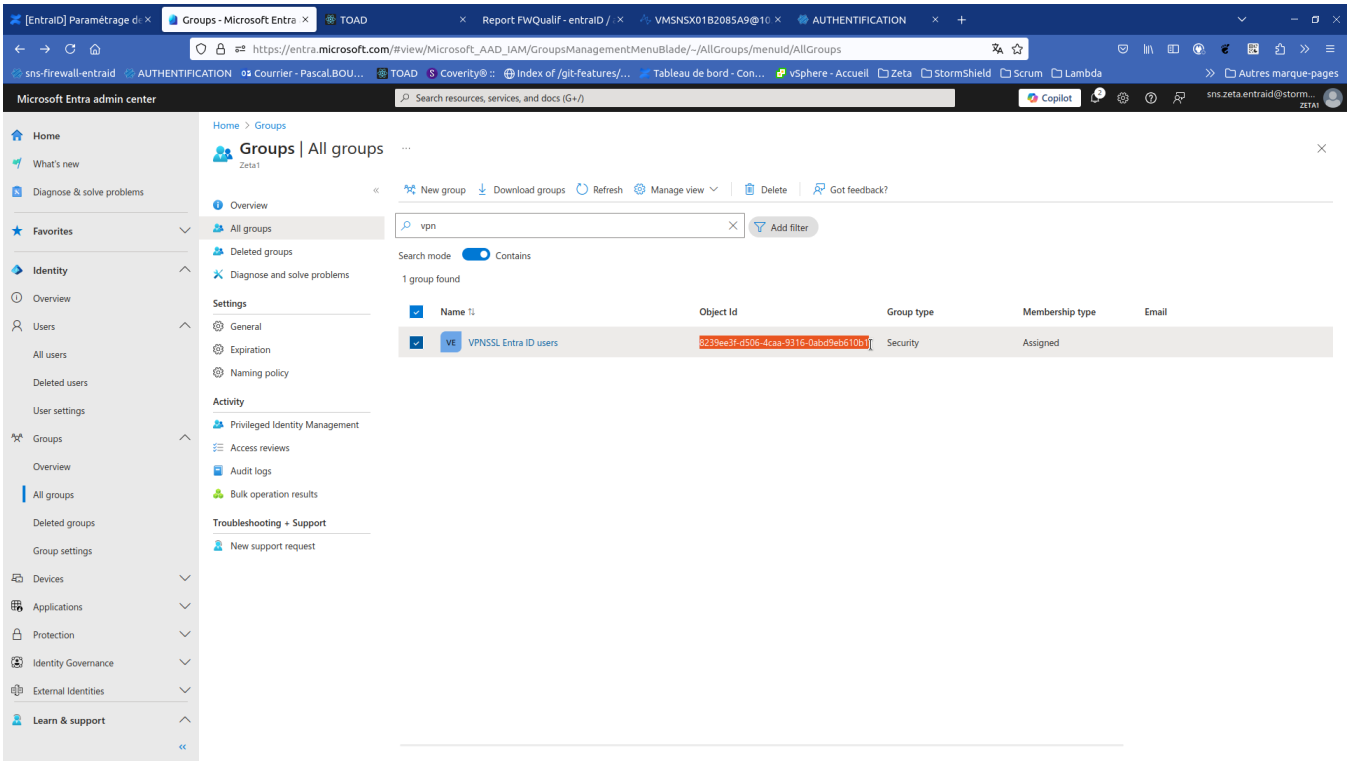

VPNSSL Entra ID users | Members
Group
Home > VPNSSL Entra ID users
Microsoft Entra admin center
Add members
Bulk operations
Refresh
Manage view
Remove
Got feedback?
Direct members
All members
Search
Add filter
1 group member found
Name
Type
Email
User type
Object Id
User One
User
Member
6c594910-cb1d-4f5f-9d3e-2aca96f58a7c
https://entra.microsoft.com/#blade/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/userId/6c594910-cb1d-4f5f-9d3e-2aca96f58a7c


Groups | All groups
Zeta1
Home > Groups
Microsoft Entra admin center
New group
Download groups
Refresh
Manage view
Delete
Got feedback?
vpn
Add filter
Search mode
Contains
1 group found
Name
Object Id
Group type
Membership type
Email
VPNSSL Entra ID users
8239ee3f-d506-4caa-9316-0abd9eb610b1
Security
Assigned
https://entra.microsoft.com/#blade/Microsoft_AAD_IAM/GroupDetailsMenuBlade/groupId/8239ee3f-d506-4caa-9316-0abd9eb610b1/menuId/


VPNSSL Entra ID users
Group
Home >
Microsoft Entra admin center
Delete
Got feedback?
Overview
Basic information
VE
VPNSSL Entra ID users
Your description for this group
Membership type
Assigned
Source
Cloud
Type
Security
Object ID
8239ee3f-d506-4caa-9316-0abd9eb610b1
Created on
2/24/2025, 2:04 PM
Total direct members
User(s)
Group(s)
Device(s)
Other(s)
Feed
Group memberships
Owners
Total members
View group memberships
View group owners
View group members
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/GroupDetailsMenuBlade/~/Members/groupId/8239ee3f-d506-4caa-9316-0abd9eb610b1/menuId/

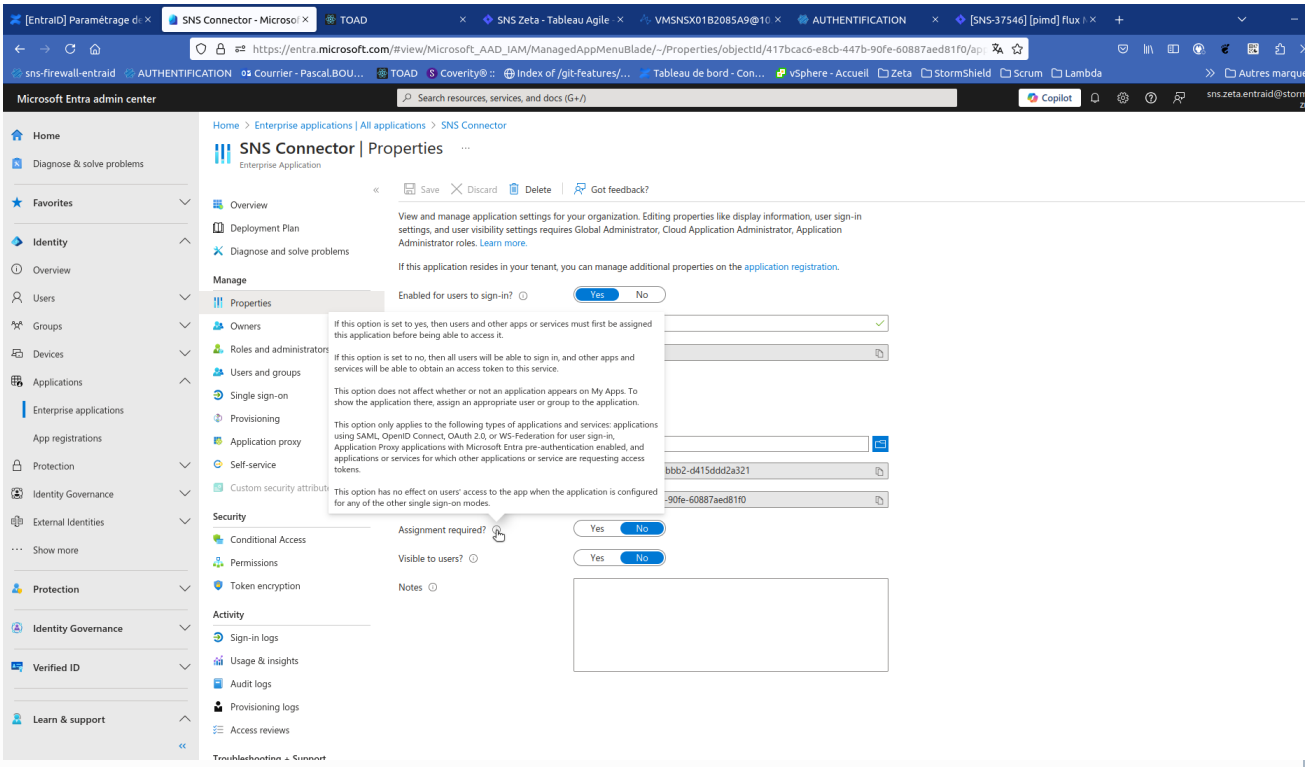


3/ Dans la vue "Tous les groupes", copier la valeur "ID d'objet" pour renseigner le UID du groupe dans la configuration du SNS.

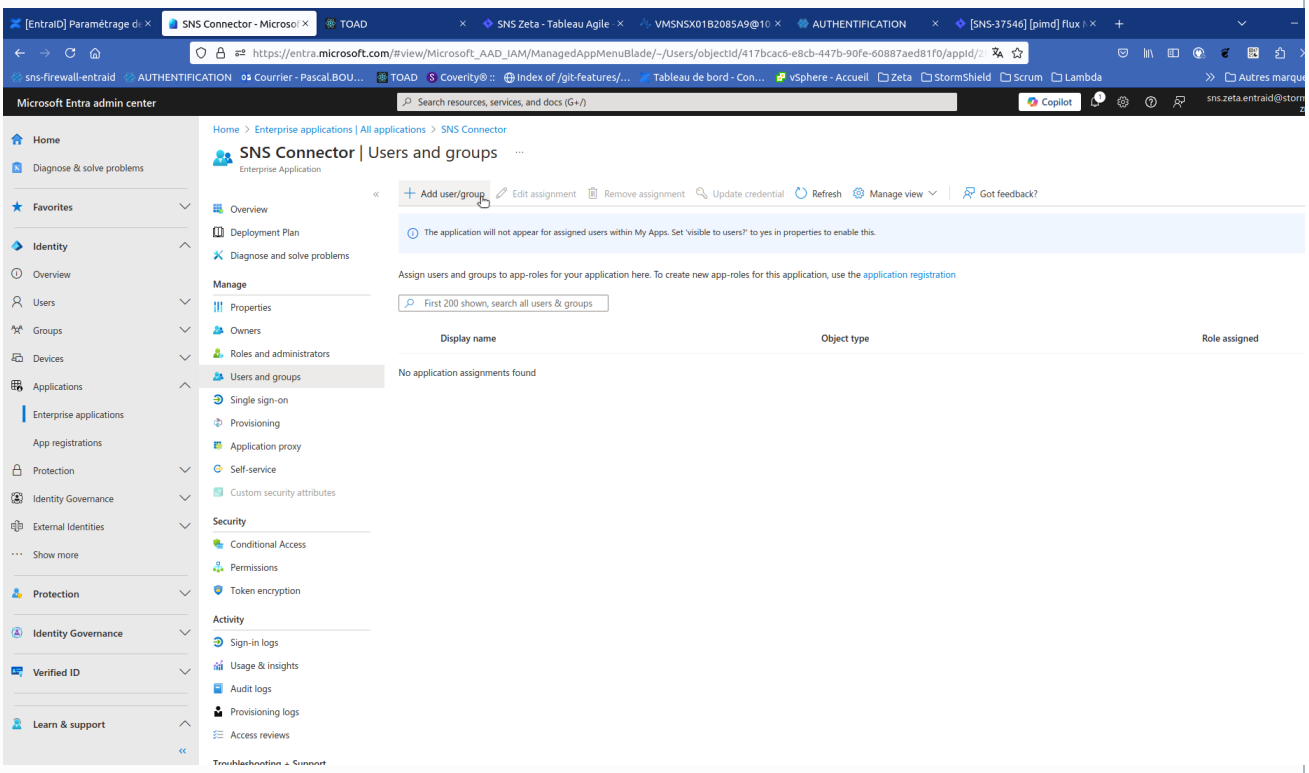


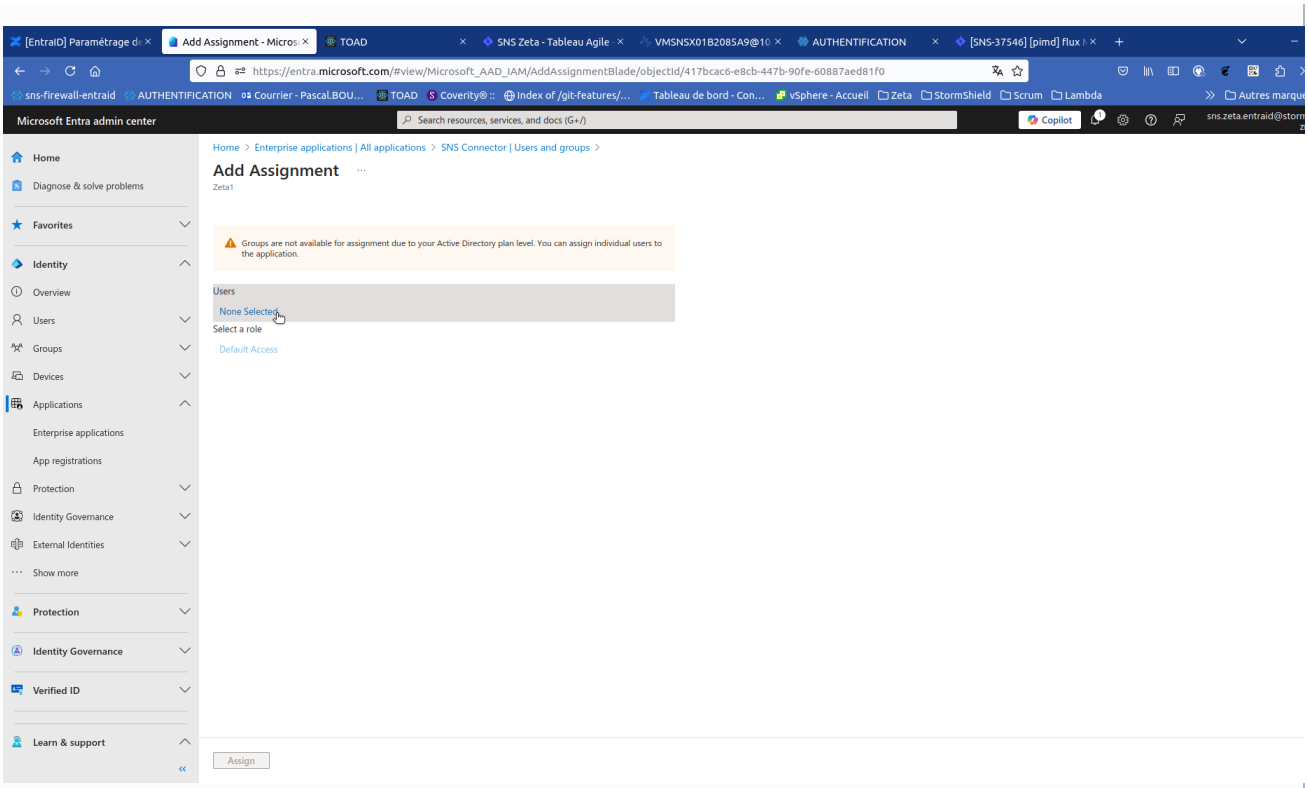
Assignement des utilisateurs à l'application

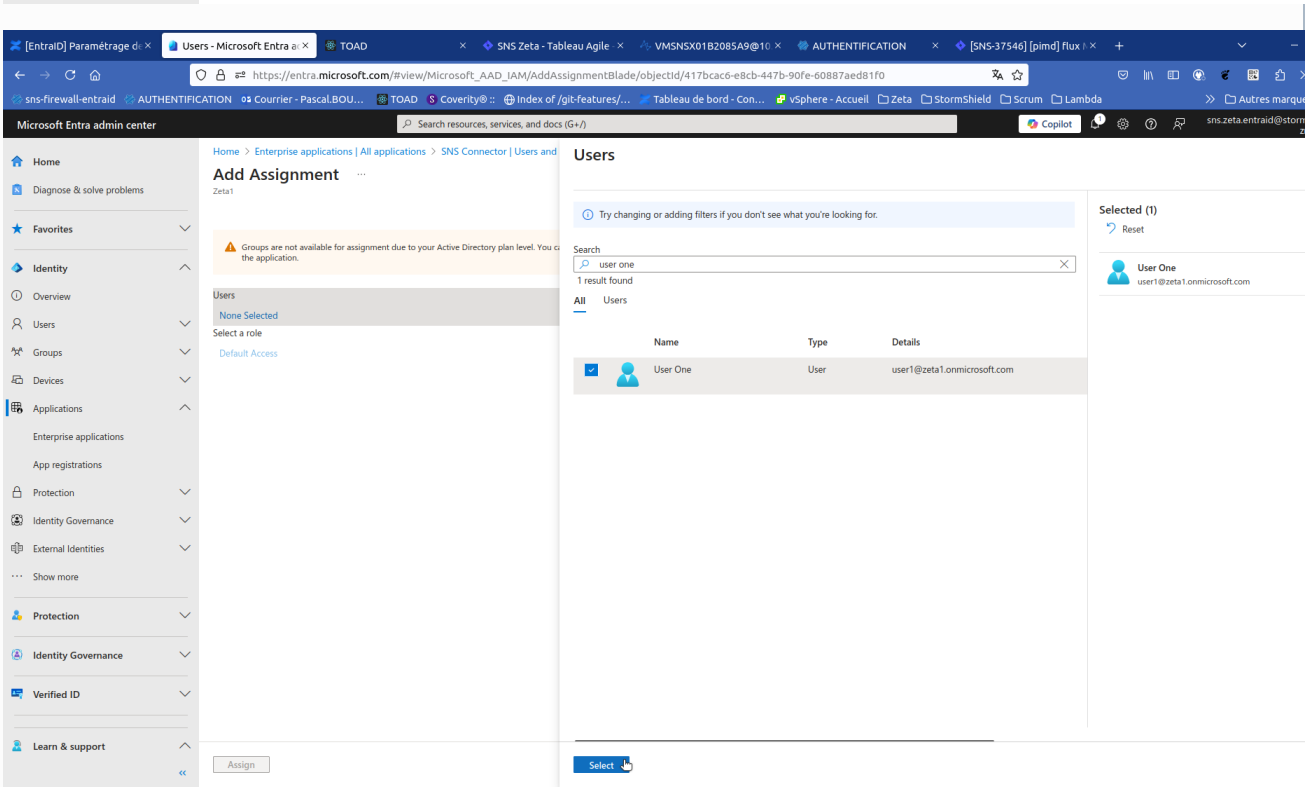
Via **Entreprise applications SNS Connector Properties**, il est possible d'autoriser l'accès à l'application à tous les utilisateurs du locataire ou de limiter son accès à une liste d'utilisateur.

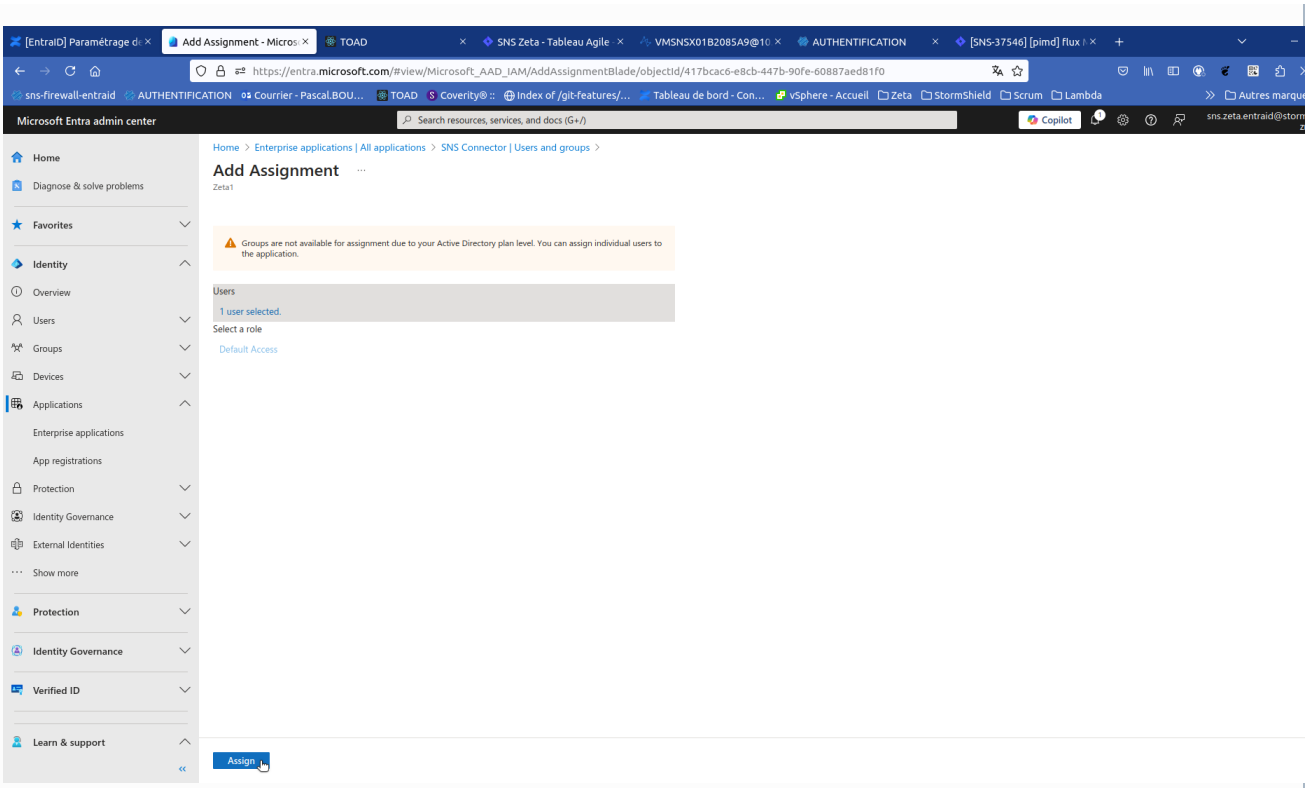


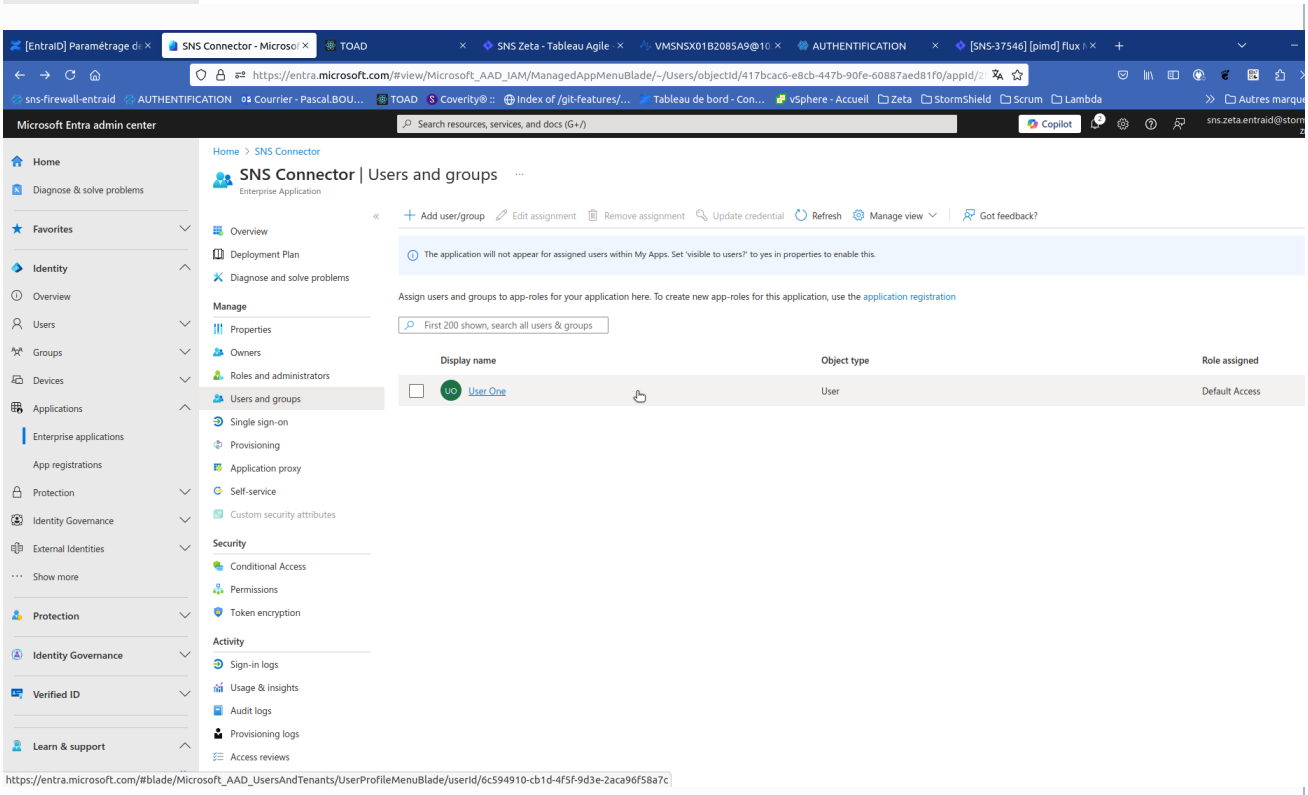
Dans le cas où cette option est positionnée sur **Yes**, il faut assigner les utilisateurs que l'on souhaite autorisés via **Users and groups**




Add Assignment - Micros
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/417bcac6-e8cb-447b-90fe-60887aed81f0
Microsoft Entra admin center
Home > Enterprise applications | All applications > SNS Connector | Users and groups >
Add Assignment
Zeta1
Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.
Users
None Selected
Select a role
Default Access
Assign


Users - Microsoft Entra a
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/417bcac6-e8cb-447b-90fe-60887aed81f0
Microsoft Entra admin center
Add Assignment
Zeta1
Users
None Selected
Select a role
Default Access
Assign
Users
Try changing or adding filters if you don't see what you're looking for.
Search
user one
1 result found
All
Users
Name
Type
Details
User One
User
user1@zeta1.onmicrosoft.com
Selected (1)
Reset
User One
user1@zeta1.onmicrosoft.com
Select





Il est possible d'assigner les utilisateurs à l'application via leur groupe de sécurité, mais cette option est soumis à abonnement P1.

Configuration du SNS

Configuration de la méthode OIDC pour EntraID

Pour cela il faut recopier les éléments suivants de la configuration d'EntraID (vue d'ensemble, voir étapes précédentes) :

- TenantID : ID de l'annuaire (locataire)
- ClientID : ID d'application (client)
- ClientSecret : Présent comme "Secrets client"

Mettre à jour le profil d'authentification OIDC

Dans l'interface d'administration Web, aller dans le panneau 'Authentification'.

Dans le menu 'Activer une méthode', choisir 'OIDC / Entra ID'

Recopier les éléments de la configuration d'EntraID dans l'assistant.

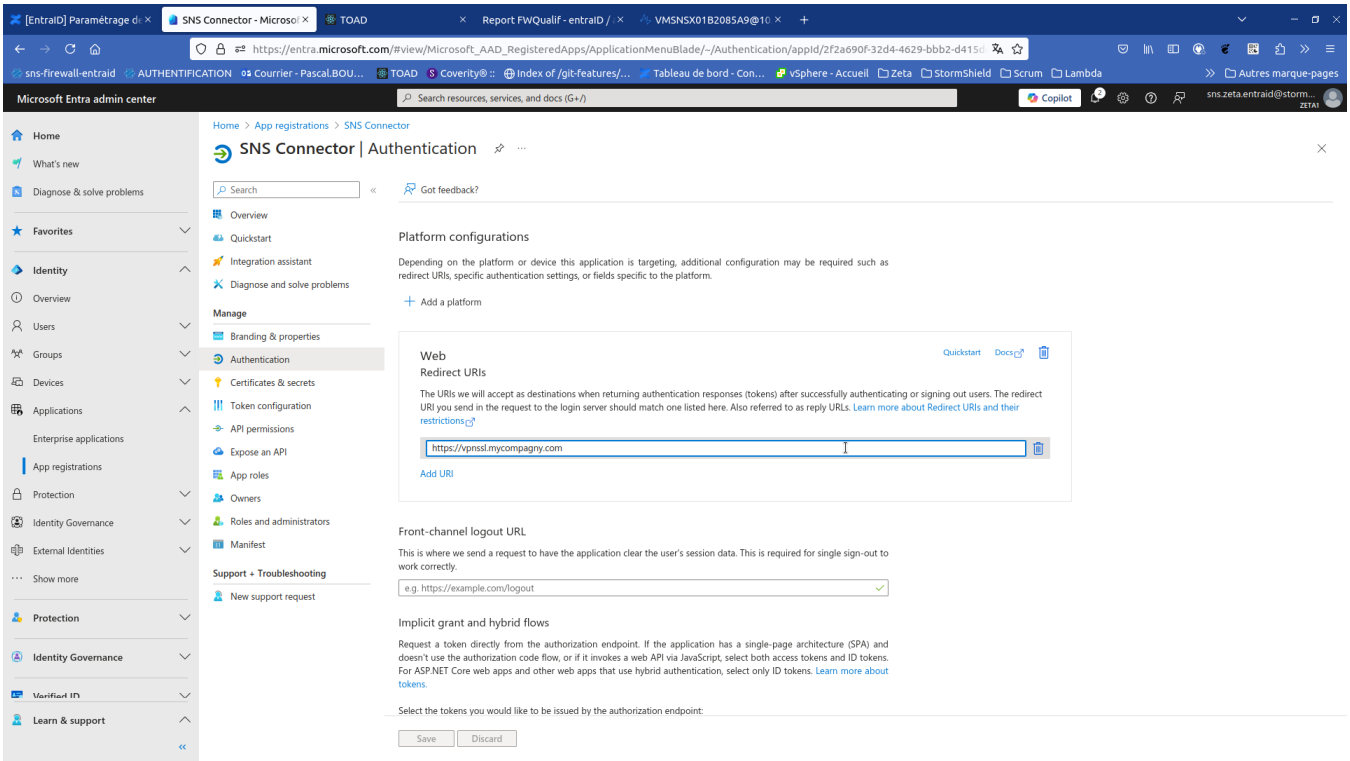
⚠️ Passer à la configuration des URLs de redirection avant de terminer l'assistant.

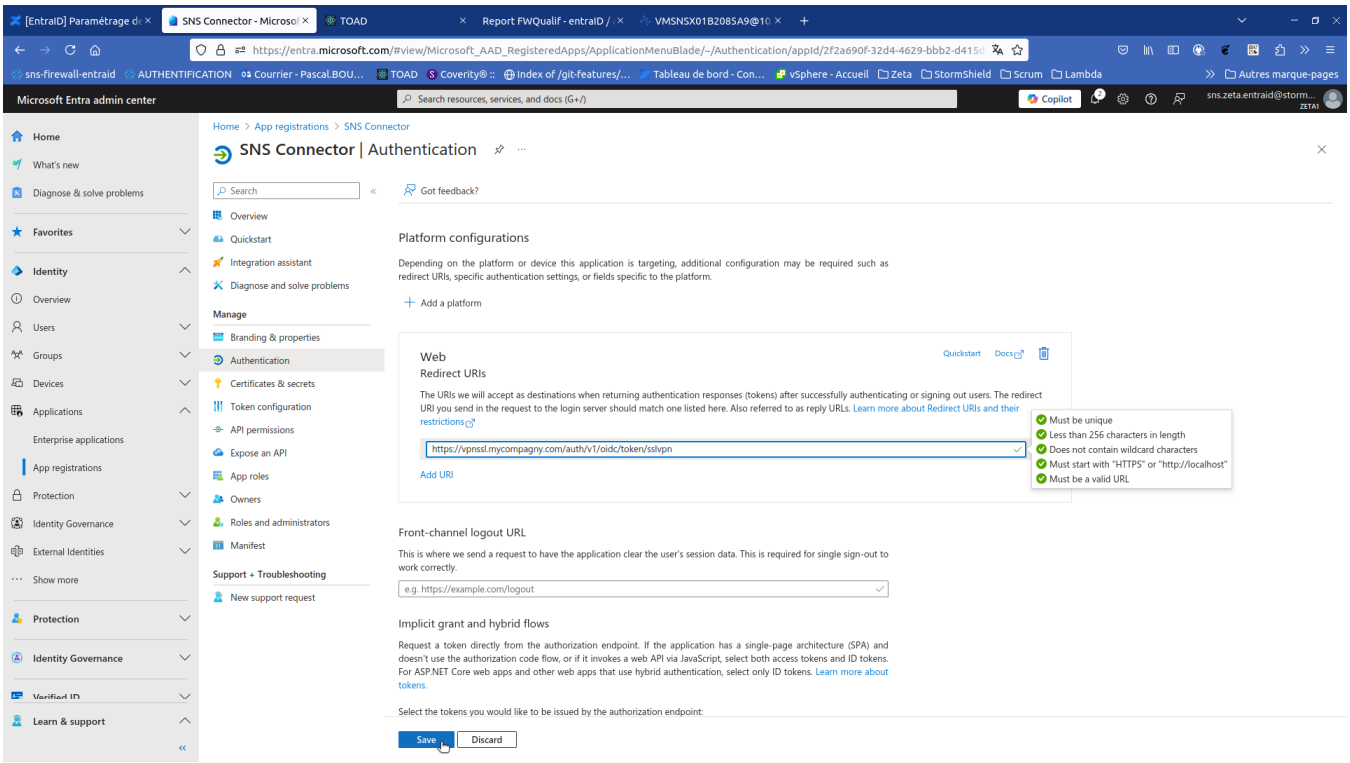
> ⓘ Le paramètre "IssuerID" sera construit tel que : "https://login.microsoftonline.com/$TENANTID/v2.0"
>
> Les URL de redirection sont construites à partir de la configuration du Portail Captif (Système/Configuration -> Configuration générale -> Configuration avancée -> Portail captif)

Configuration des URL de redirection dans EntraID

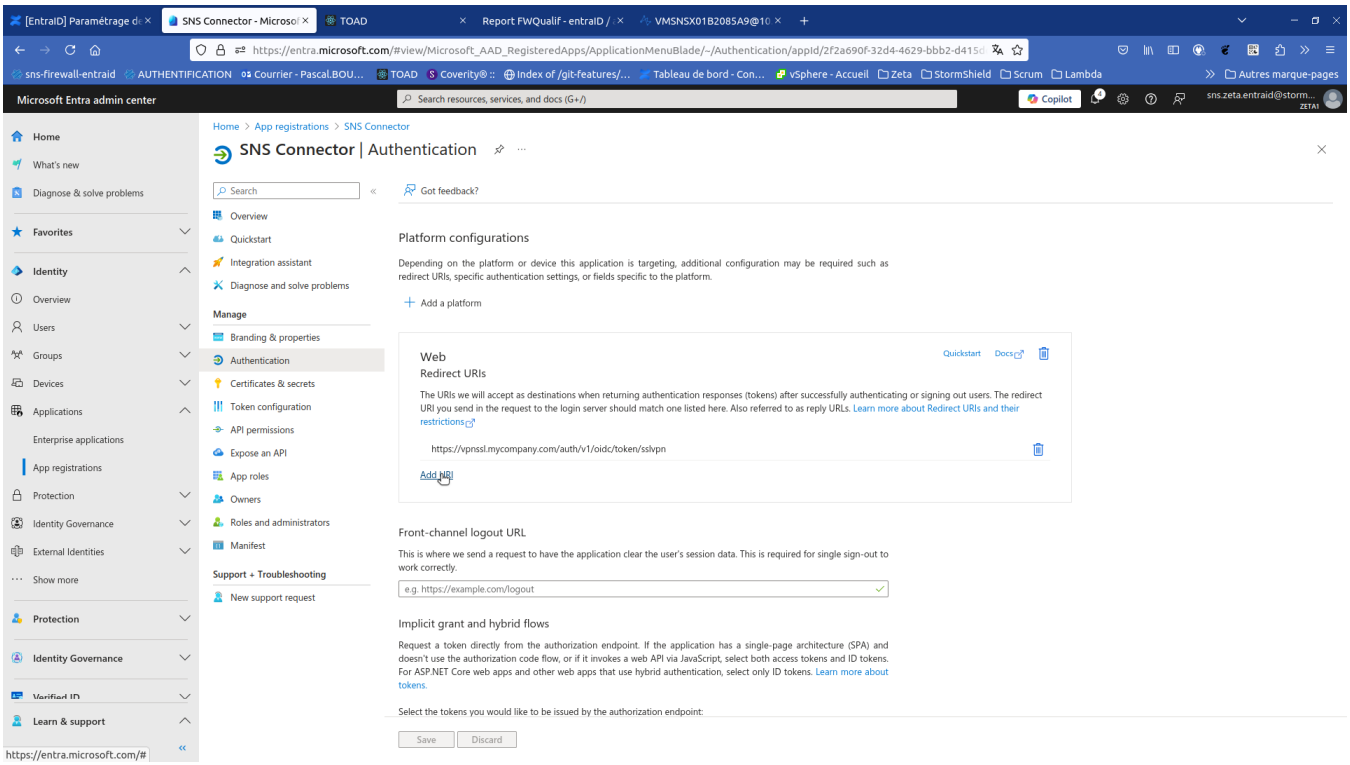
Renseigner dans l'application SNS Connector, les URI de redirection souhaitée à partir de celles proposées

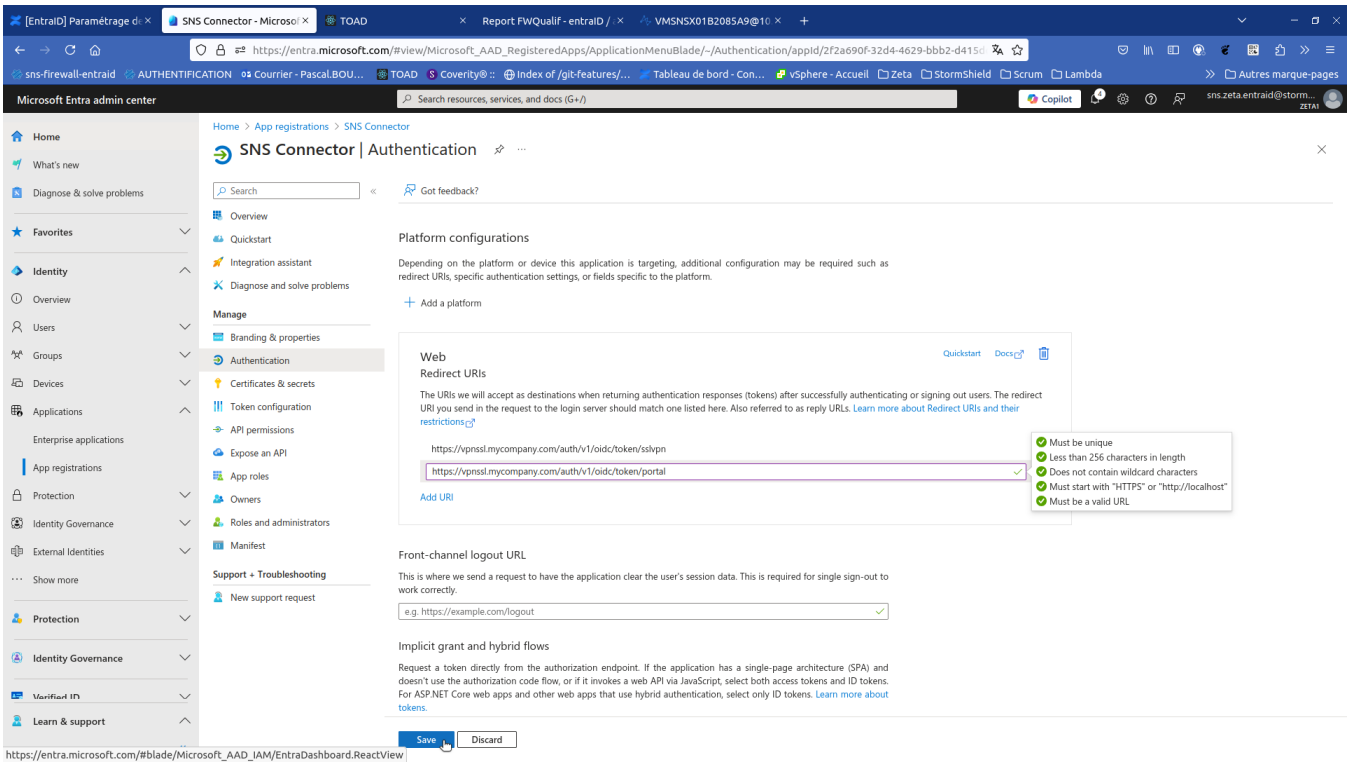
1/ Mettre à jour l'URI de redirection déjà présente





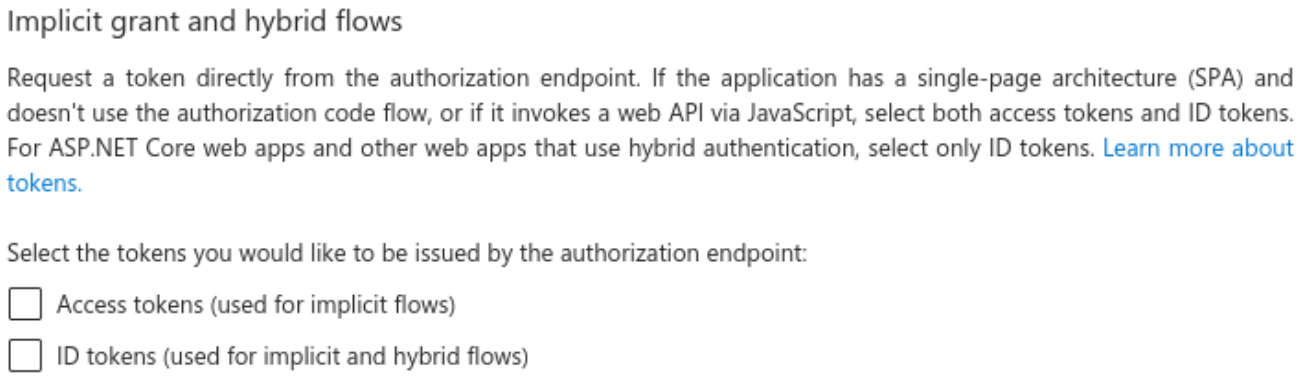
2/ Ajouter si nécessaire l'URI de redirection pour autoriser l'authentification via le portal captif du SNS

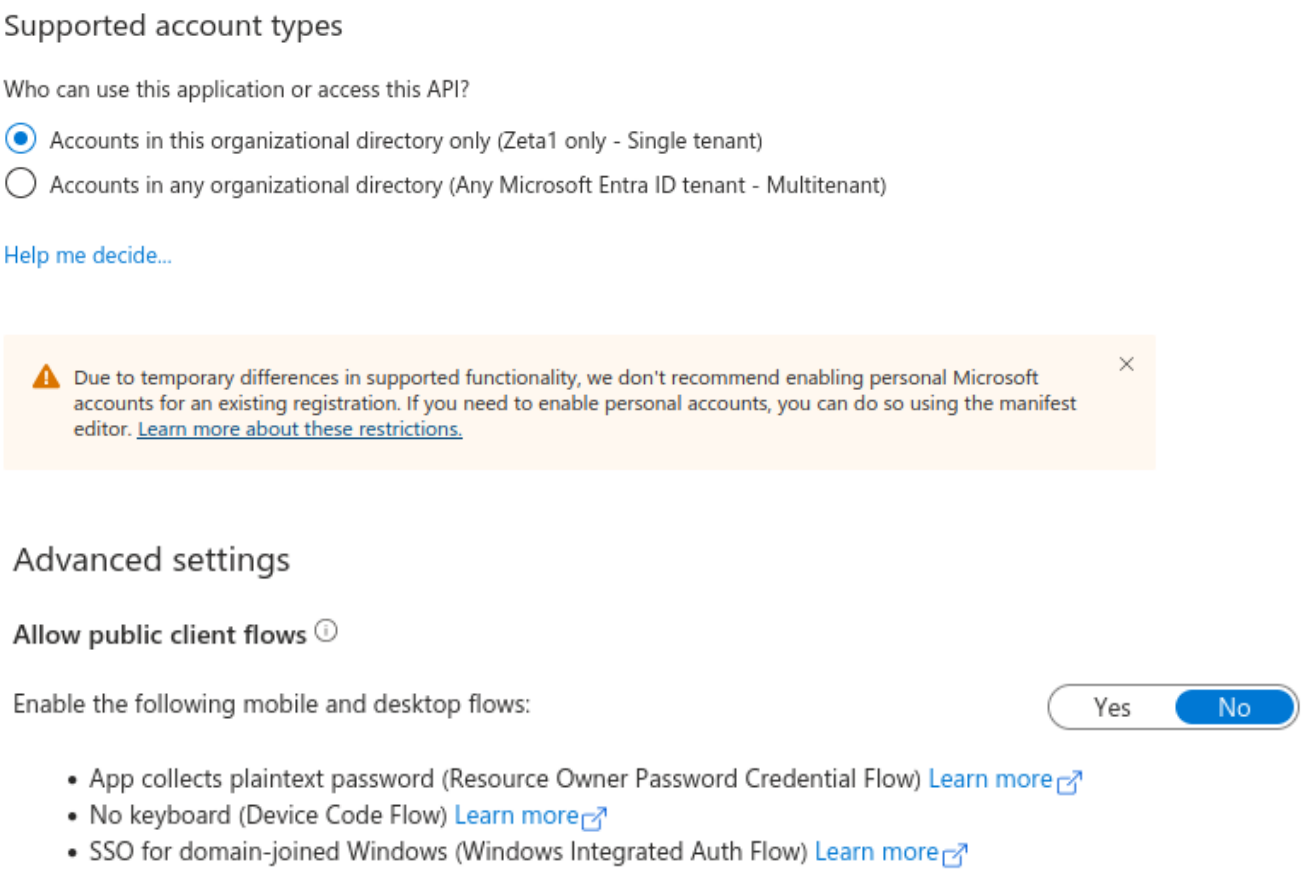




3/ Sur cette même page, en profiter pour vérifier les configurations suivantes :

- S'assurer que les options "**Access tokens (used for implicit flows)**" et "**ID tokens (used for implicit and hybrid flows)**" ne sont pas cochées afin de garantir que l'application n'utilise ni le flux implicite ni le flux hybride, conformément aux bonnes pratiques de sécurité.
- L'option "**Accounts in this organizational directory only (Single tenant)**" doit être sélectionnée. Les autres options n'ayant pas fait l'objet de tests internes, leur fonctionnement ne peut être garanti et elles ne sont pas officiellement supportées.
- L'application utilise des redirect URI et ne repose pas sur des flux de type public client. L'option "**Allow public client flows**" doit donc être définie sur "**No**".

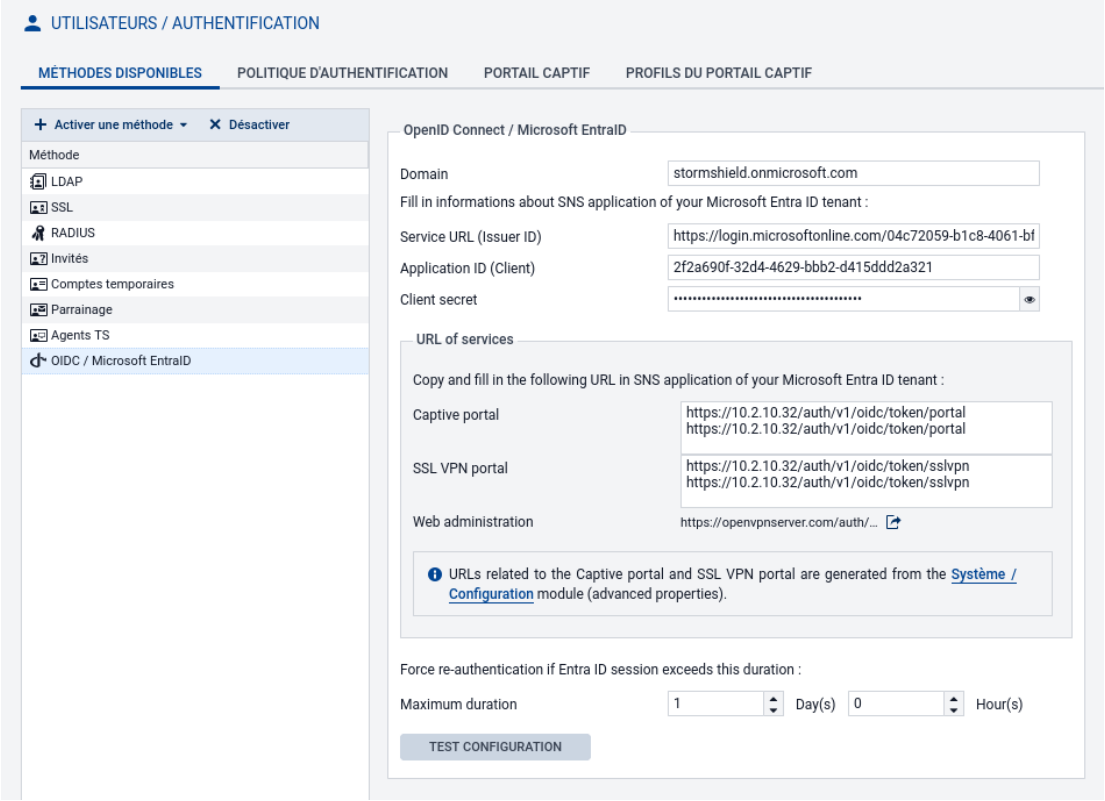




Vérifier de nouveau la configuration du SNS

Si toutes les **URI de redirection** listées par SNS ont été renseignées dans l'application **SNS Connector** coté EntraID alors plus aucun warning ne sera affiché et la configuration sera considérée comme valide.

⚠️ Terminer l'assistant de configuration



Importation des groupes de sécurité d'EntraID

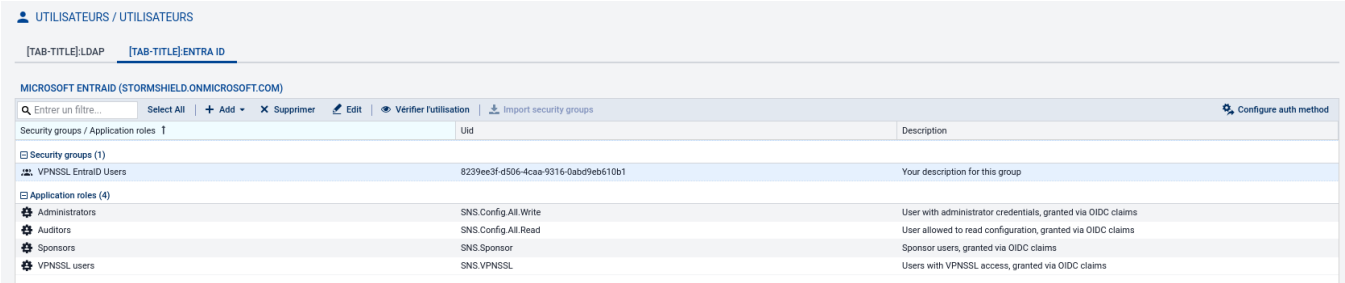
1/ Création d'un groupe OIDC correspondant aux utilisateurs du VPNSSL

Se rendre dans le panneau 'Utilisateurs' et l'onglet 'ENTRA ID'

Ajouter un groupe de sécurité et appliquer la configuration

Exemple :

- Name="VPNSSL EntraID Users"
- UID="8239ee3f-d506-4caa-9316-0abd9eb610b1"
- Description="Your description for this group"



Configuration du groupe de sécurité dans les UAC pour autoriser le VPNSSL

Création d'une règle d'authentification

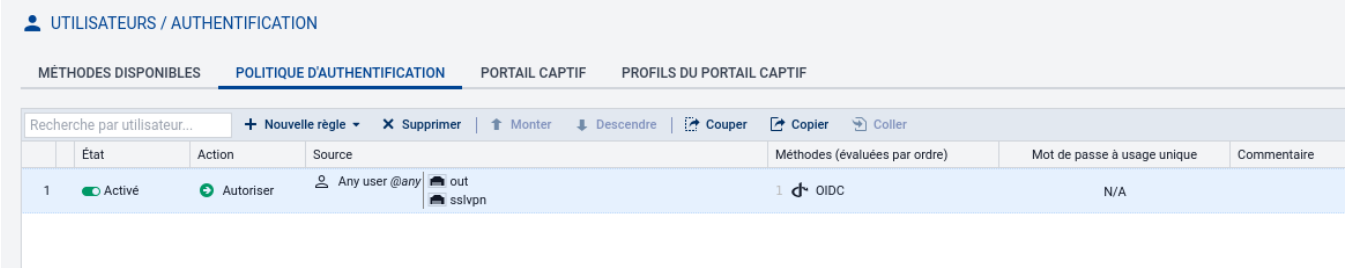
La règle d'authentification doit porter sur les interfaces "out" pour permettre l'accès au portail captif, mais également "sslvpn" pour autoriser la monter des tunnels VPNSSL pour ce type d'utilisateur.

Panneau "Authentification", onglet "Politique d'authentification" pour créer une règle portant sur la méthode OIDC et appliquer la configuration.

Exemple :

- Action = Autoriser
- Source = "any@any"

- Interface = "out, sslvpn"
- Méthode = OIDC



Création d'une règle d'accès

Panneau "Droits d'accès", onglet "Accès détaillé" pour valider ou rééditer la règle autorisant les accès au VPNSSL.

Exemple :

- Utilisateur = "VPNSSL EntraID Users"
- Domaine = stormshield.onmicrosoft.com
- VPN SSL = Autoriser

Utilisation du client VPN SSL 5.1

Lors de la configuration de la passerelle (en connexion directe ou en tant que connexion enregistrée), en mode "Stormshield", cochez la case "Se connecter avec l'authentification unique"

> Le champ Serveur doit nécessairement renseigner le FQDN du SNS qui correspond à l'URL de redirection préalablement configurée dans le SNS et EntraID.
>
> En particulier, renseigner directement une adresse IP du SNS retournera une erreur "interne".

+ Ajouter une nouvelle connexion

Mode Stormshield | Import de fichier .OVPN

Nom *

EntraID SNS

Serveur *

snsv5.stormshield.eu

Port *

443

Description

Authentification

☑ Se connecter avec l'authentification unique

Options de connexion

☐ Se connecter automatiquement

Annuler | Ajouter