

HowTo - Setup EntraID with SNS (by GUI) - EN

- Configuration cinematics by the administrator of EntraID account authorization to mount VPN SSL tunnels.
- SNS Application in EntraID
 - Creation of the application
 - Configuration of the SNS application in EntraID
 - Token Configuration
 - Creation of the secret
 - User Association
- SNS Configuration
 - Configuration of the OIDC method for EntraID
 - Update the OIDC authentication profile
 - Configuration of Redirect URLs in EntraID
 - Update the desired redirect URI in the SNS Connector application from the proposed ones
 - Re-check the SNS configuration
 - Importing EntraID Security Groups
 - Configuration of the security group in the UAC to allow SSL VPN
 - Creation of an authentication rule
 - Creation of an access rule
 - Using the SSL VPN Client 5.1



This procedure describes all the configuration operations to be performed both in EntraID and on the SNS.

However, it is strongly recommended to have prior knowledge of the EntraID solution and the possibilities offered by authentication via an "OpenID Connect" application.

Configuration cinematics by the administrator of EntraID account authorization to mount VPN SSL tunnels.

Overall Procedure:

1. On EntraID, configure the SNS application in EntraID
2. On EntraID, associate users, including the test user, to a security group that will be authorized for VPNSSL.
3. On EntraID, export the security groups from EntraID that are relevant to SNS.
4. On the SNS, configure the OIDC method for EntraID
5. On the SNS, import the security groups from EntraID
6. On the SNS, configure the security group in the UAC to authorize VPNSSL.
7. On the VPNSSL Client, establish the tunnel with a test account
8. On the SNS, validate the users and VPNSSL tunnels in the monitoring.

SNS Application in EntraID



All manipulations are to be performed in the 'Identity' section

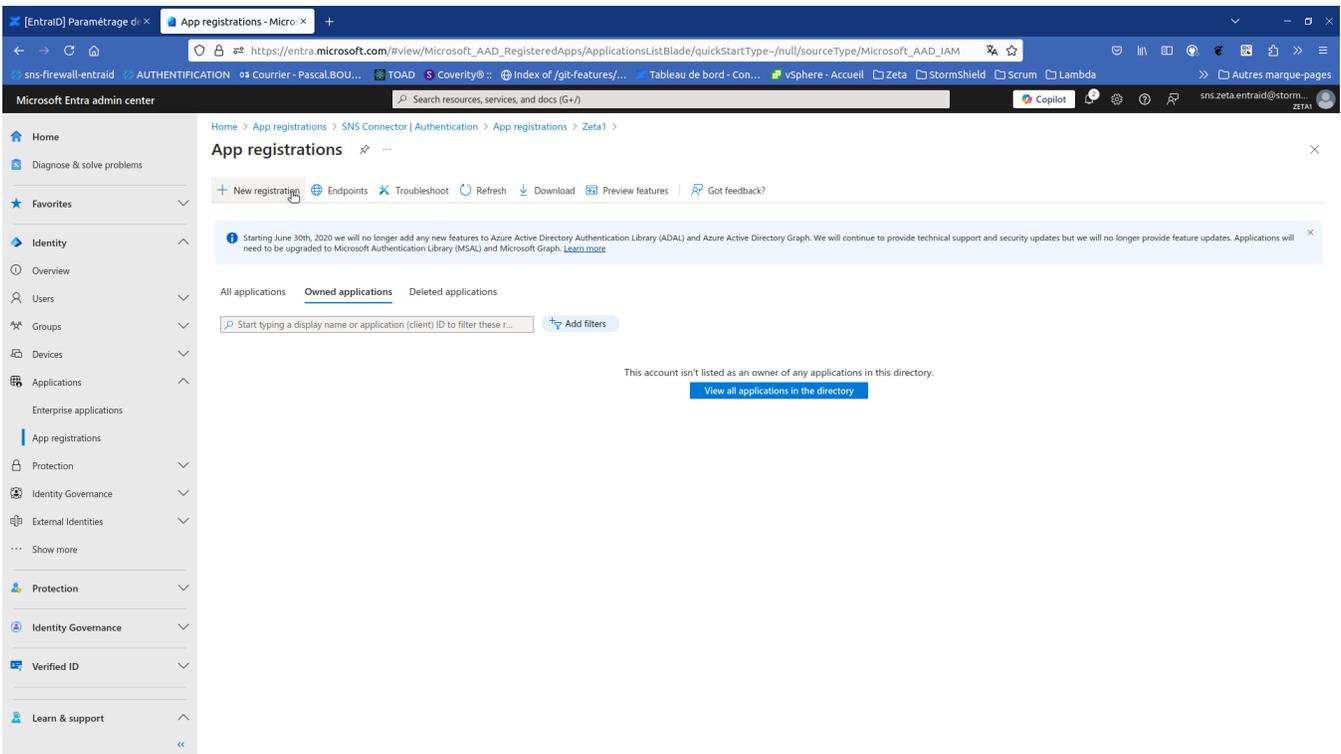
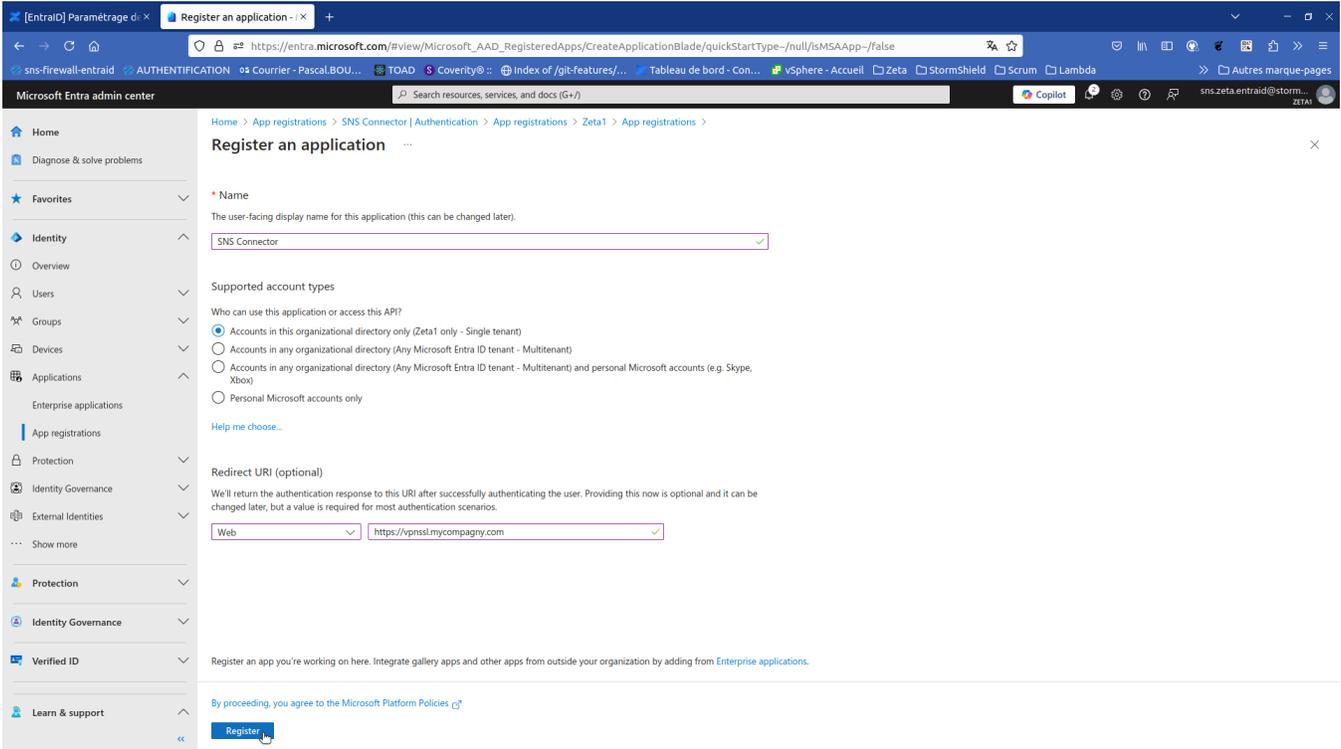
Creation of the application

Configuration of the SNS application in EntraID

From the administration interface of your EntraID space "Register an application" named "**SNS Connector**"

with "Redirect URI (optional)" in "**Web**" mode

and enter the public URL of the SNS for example: "<https://vpnsll.mycompany.com/auth/v1/oidc/token/sslvpn>"



Token Configuration

1/ Go to "Application Registration"; click on "Display all applications in the directory" and select the SNS connector application, then "Token Configuration"

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane is visible, with 'App registrations' selected. The main content area displays the 'App registrations' page for 'SNS Connector'. A table lists the application with the following details:

Display name	Application (client) ID	Created on	Certificates & secrets
SNS Connector	2f2a690f-32d4-4629-bbb2-d415ddd2a321	2/24/2025	-

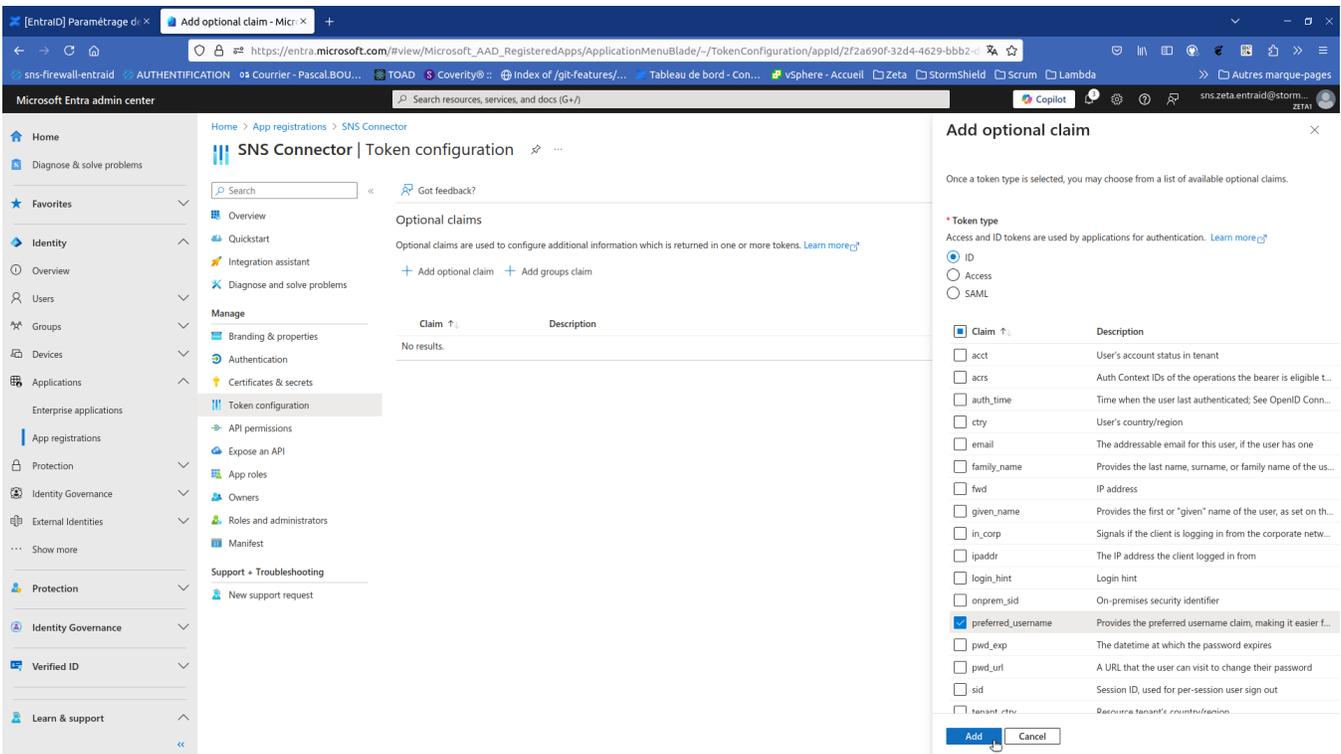
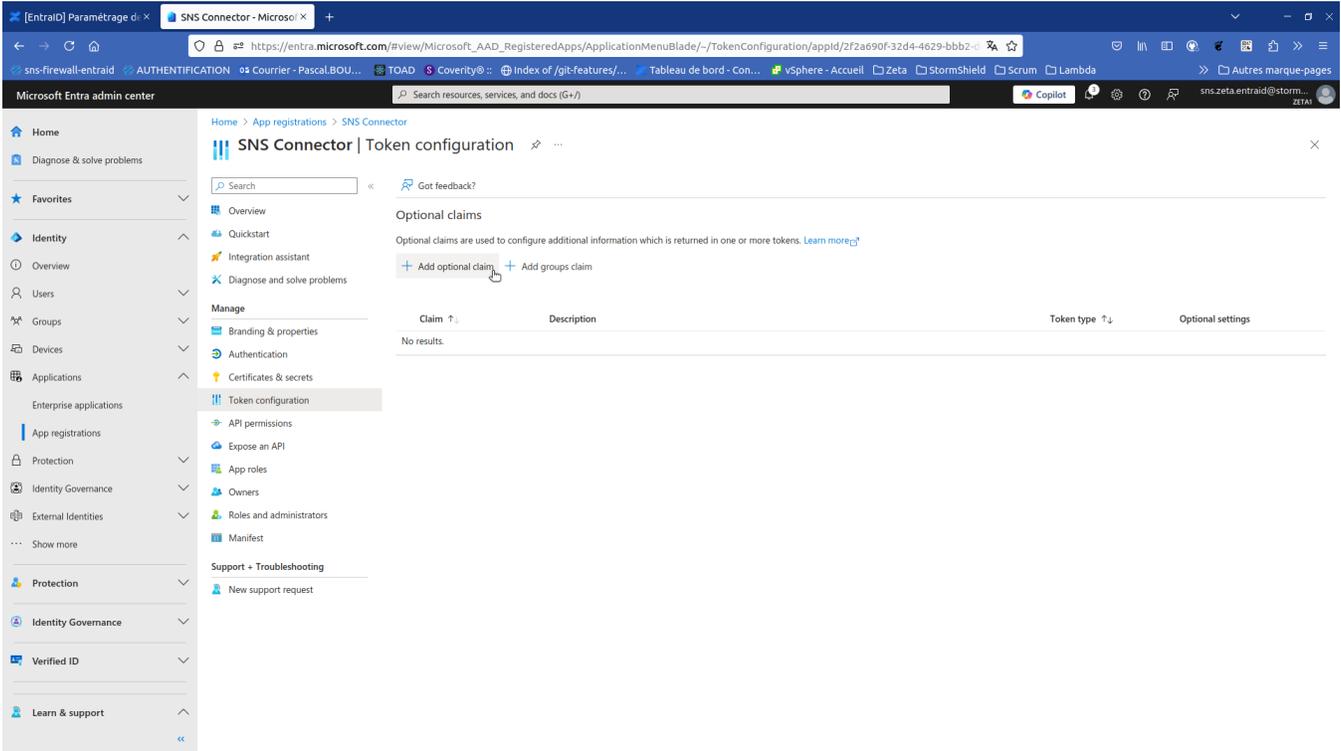
Token configuration :

The screenshot shows the 'Token configuration' page for the 'SNS Connector' application. The 'Essentials' section contains the following information:

- Display name: SNS Connector
- Application (client) ID: 2f2a690f-32d4-4629-bbb2-d415ddd2a321
- Object ID: f1334c6a-beb3-43e0-8720-649b2c750030
- Directory (tenant) ID: 04c72059-b1e8-4061-bf04-f3346931e54e
- Supported account types: My organization only

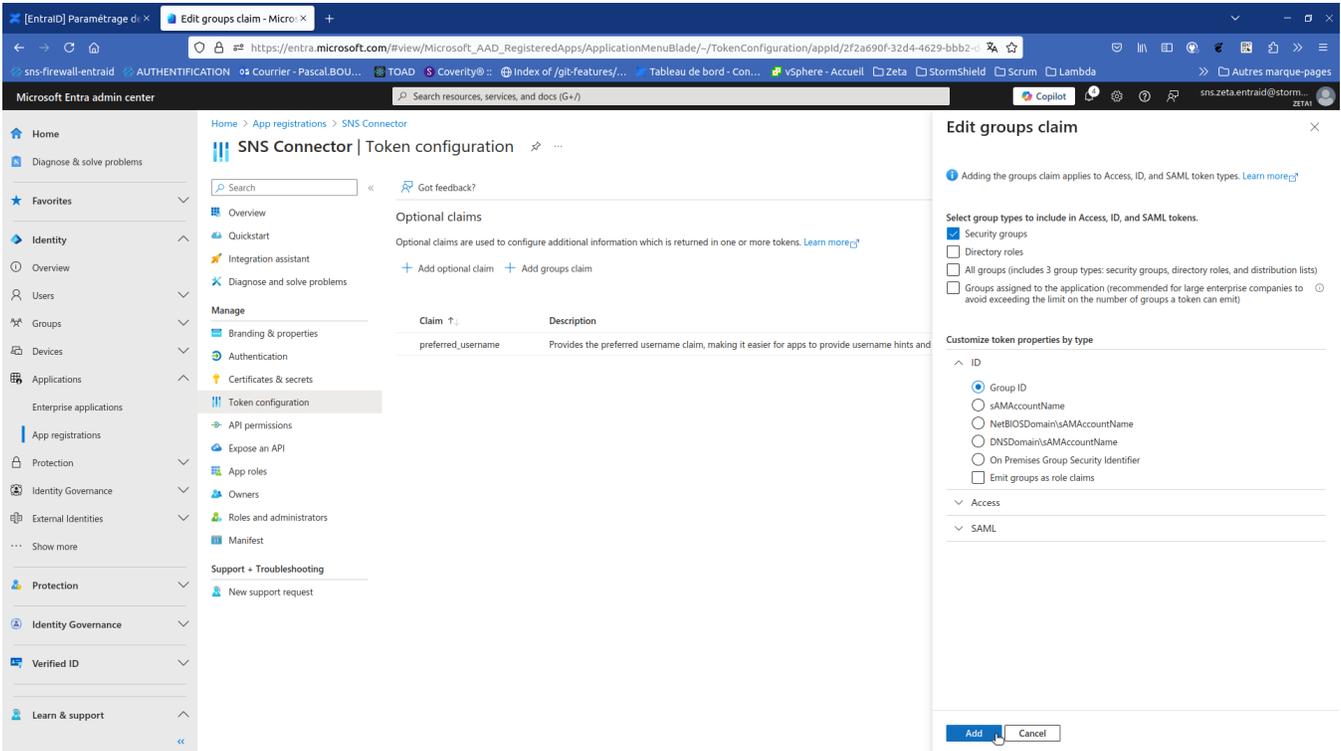
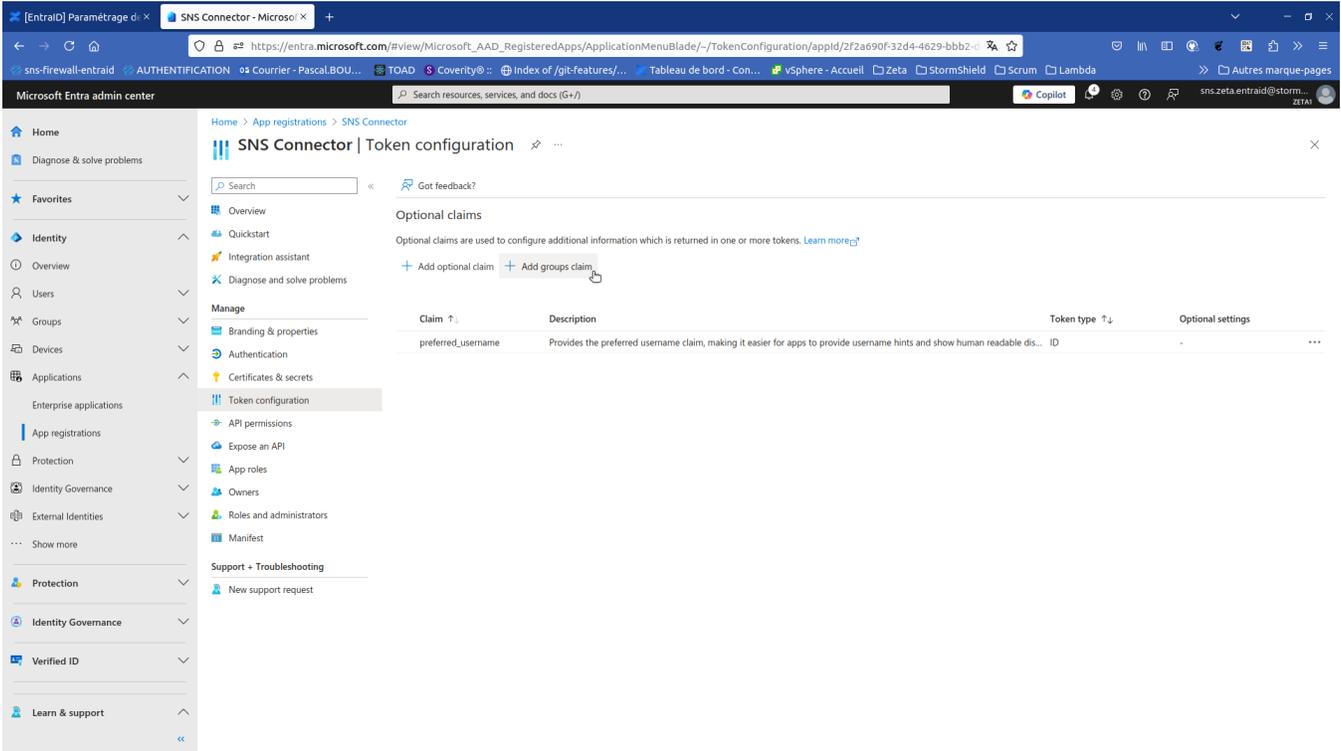
The 'Get Started' section provides guidance on building applications with the Microsoft identity platform, including links for 'Call APIs', 'Sign in users in 5 minutes', and 'Configure for your organization'.

2/ Add the optional "preferred_username" claim for the ID Token (⚠️ mandatory for SNS)

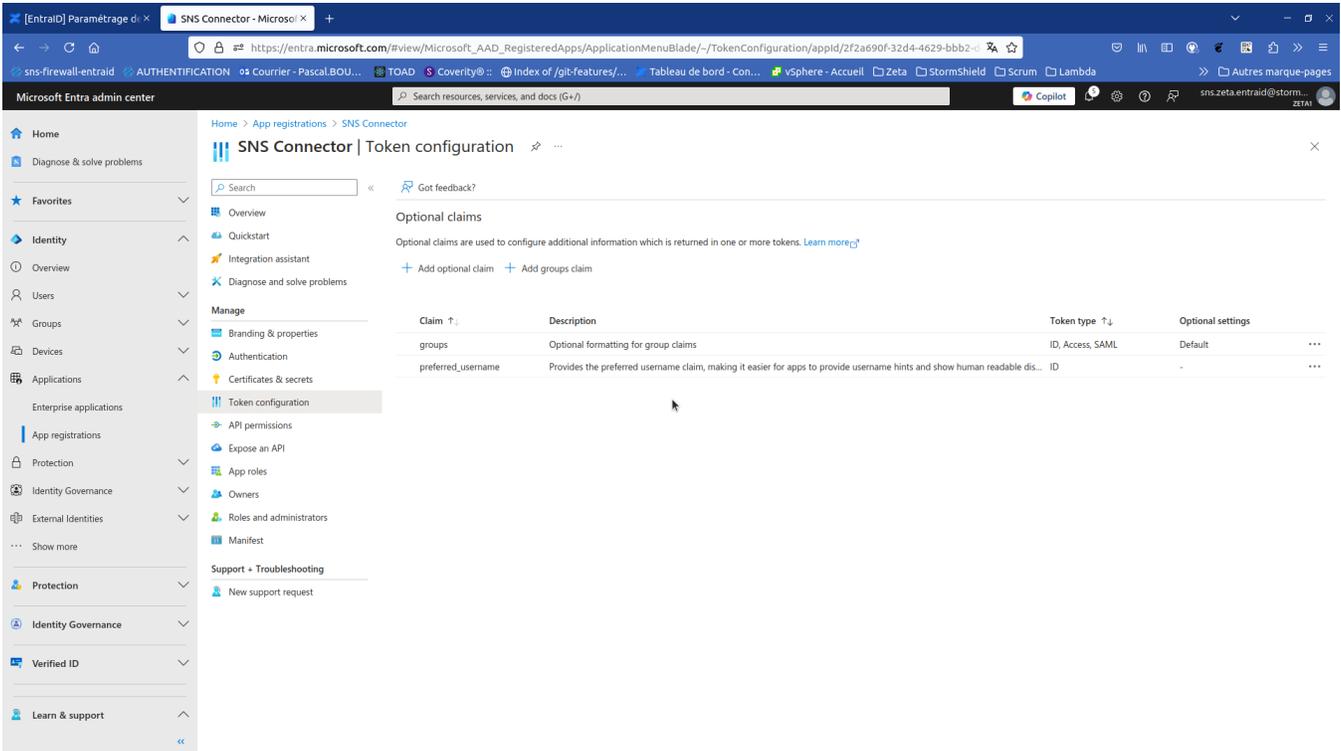
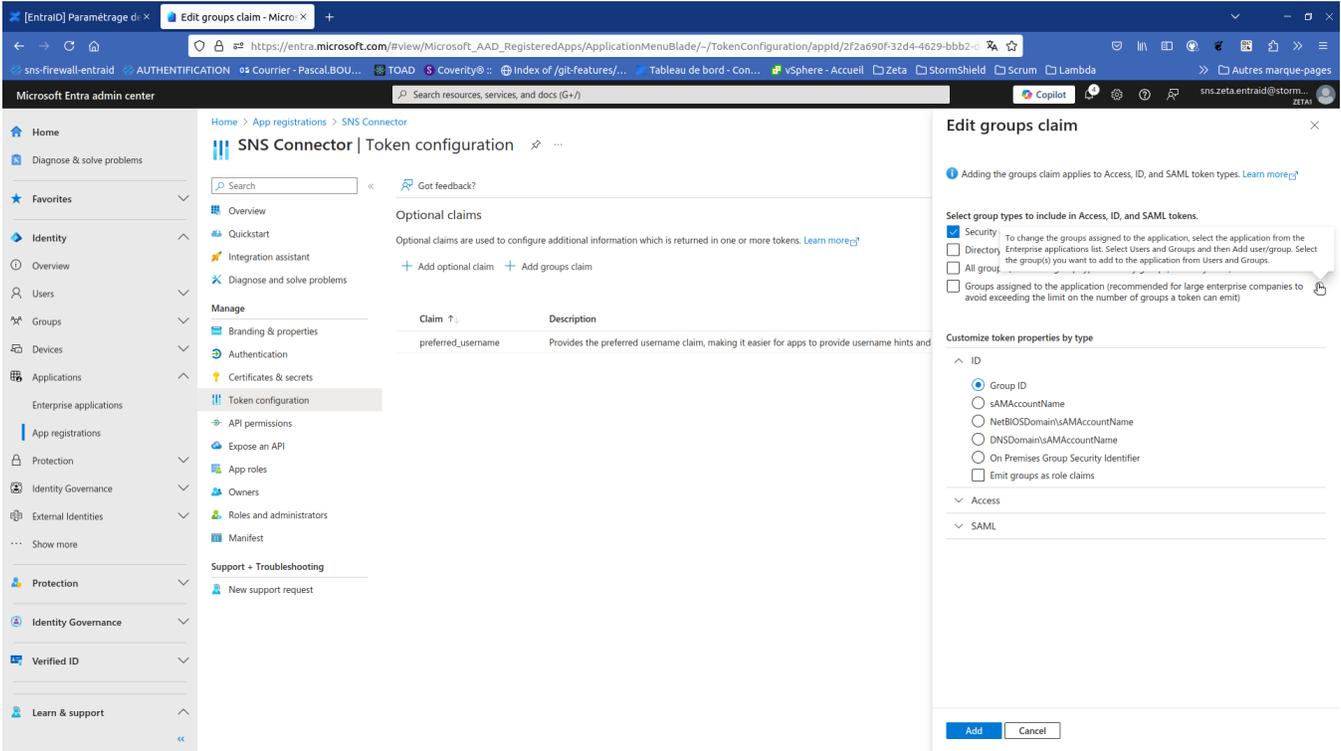


3/ For "Add Group Claim", and in the "Edit Group Claim" section, check "Security Groups" with ID on "Group ID".

i Optional for SNS but strongly recommended in order to benefit from UAC/AAC/filtering and authentication policies on security groups.



i Note that it is possible to limit the groups included in the ID Token to those assigned to the application, but this is subject to a P1 subscription.



4/ From App registrations SNS Connector Overview

- Copy the value of "Directory (tenant) ID" to fill in the "IssuerID" in the SNS configuration.
- Copy the value of "Application (client) ID" to fill in the "ClientID" in the SNS configuration.

Microsoft Entra admin center

SNS Connector | Token configuration > Enterprise applications | All applications > App registrations > SNS Connector > Enterprise applications | All applications > SNS Connector | Overview > App registrations

Search resources, services, and docs (G+)

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: SNS Connector	Client credentials	: Add a certificate or secret
Application (client) ID	: 2f2a690f-32d4-4629-bbb2-d415ddd2a321	Redirect URIs	: 1 web, 0 spa, 0 public client
Object ID	: f133dc6a-bbb3-43e0-8720-6d9b2c750030	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 04c72059-b1c8-4061-bf04-f3346931e54e	Managed application in L.	: SNS Connector

Supported account types : [My organization only](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

- Call APIs**
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources. [View API permissions](#)
- Sign in users in 5 minutes**
Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app. [View all quickstart guides](#)
- Configure for your organization**
Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications. [Go to Enterprise applications](#)

Microsoft Entra admin center

SNS Connector | Token configuration > Enterprise applications | All applications > App registrations > SNS Connector > Enterprise applications | All applications > SNS Connector | Overview > App registrations

Search resources, services, and docs (G+)

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: SNS Connector	Client credentials	: Add a certificate or secret
Application (client) ID	: 2f2a690f-32d4-4629-bbb2-d415ddd2a321	Redirect URIs	: 1 web, 0 spa, 0 public client
Object ID	: f133dc6a-bbb3-43e0-8720-6d9b2c750030	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 04c72059-b1c8-4061-bf04-f3346931e54e	Managed application in L.	: SNS Connector

Supported account types : [My organization only](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

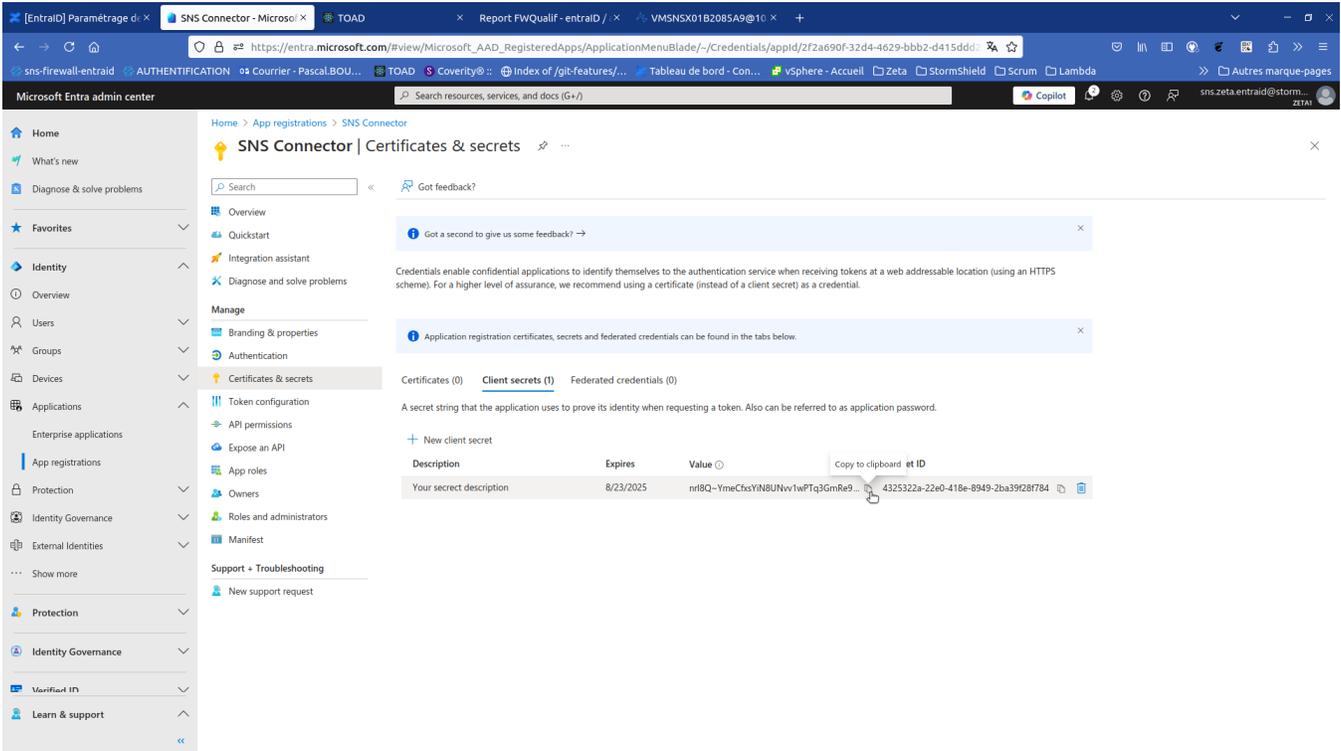
- Call APIs**
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources. [View API permissions](#)
- Sign in users in 5 minutes**
Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app. [View all quickstart guides](#)
- Configure for your organization**
Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications. [Go to Enterprise applications](#)

Creation of the secret

1/ In the "Certificates & Secrets" menu, "Client Secrets" tab, create a "new client secret"

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane is visible, with 'Applications' expanded and 'Enterprise applications' selected. The main content area displays the 'Certificates & secrets' page for an SNS Connector application. The page includes a search bar, a 'Got feedback?' link, and a list of tabs: 'Certificates (0)', 'Client secrets (0)', and 'Federated credentials (0)'. A blue information banner states: 'Application registration certificates, secrets and federated credentials can be found in the tabs below.' Below the tabs, there is a text description: '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.' A 'New client secret' button is highlighted with a mouse cursor. Below this button is a table with columns: 'Description', 'Expires', 'Value', and 'Secret ID'. The table is currently empty, with the text 'No client secrets have been created for this application.' below it.

The screenshot shows the 'Add a client secret' dialog box overlaid on the previous page. The dialog has a title bar 'Add a client secret' and a close button. It contains two input fields: 'Description' with the placeholder text 'Your secret description' and 'Expires' with a dropdown menu showing 'Recommended: 180 days (6 months)'. At the bottom of the dialog, there are two buttons: 'Add' and 'Cancel'.

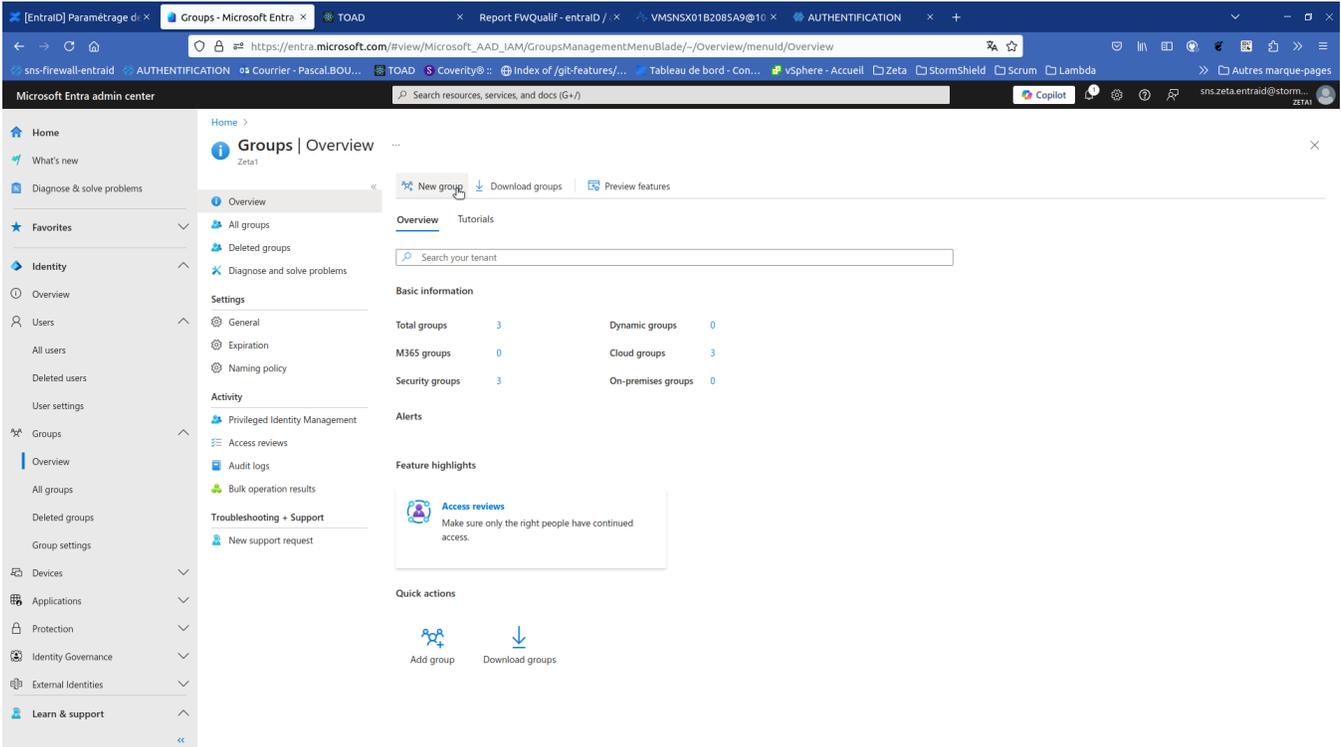


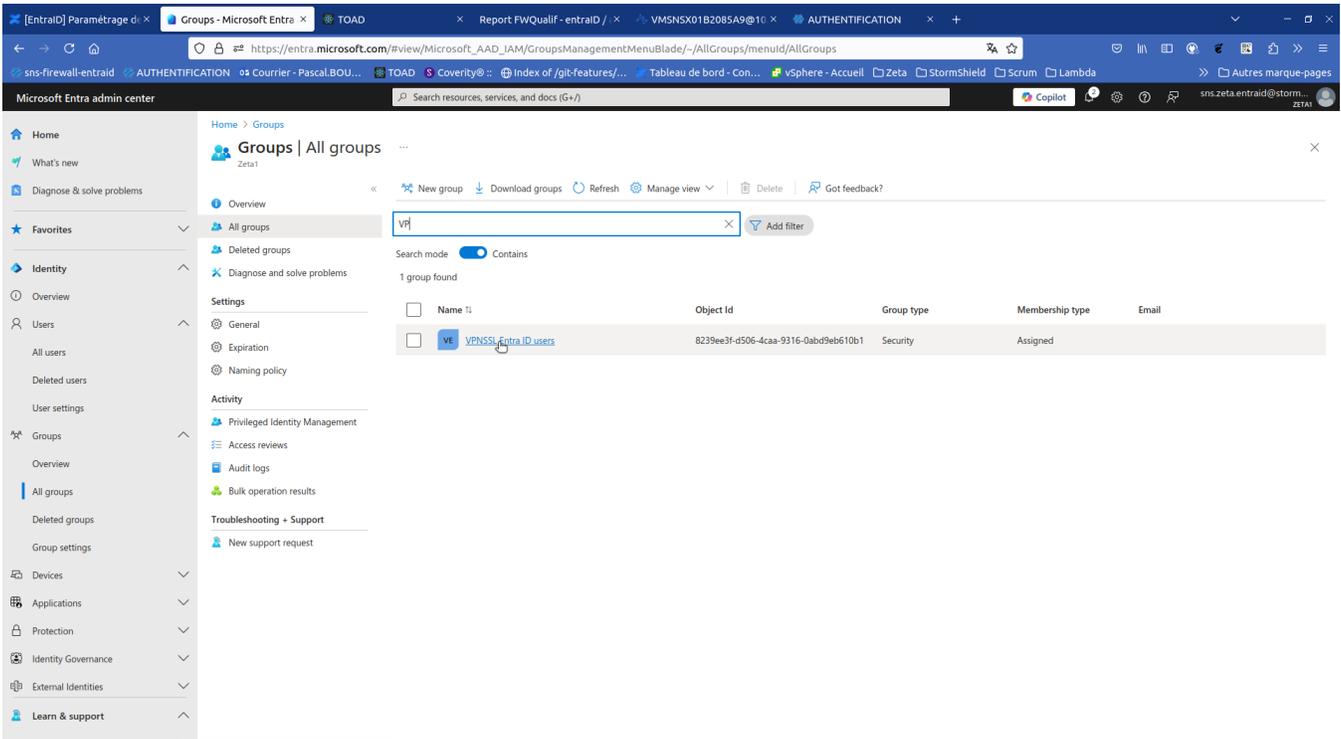
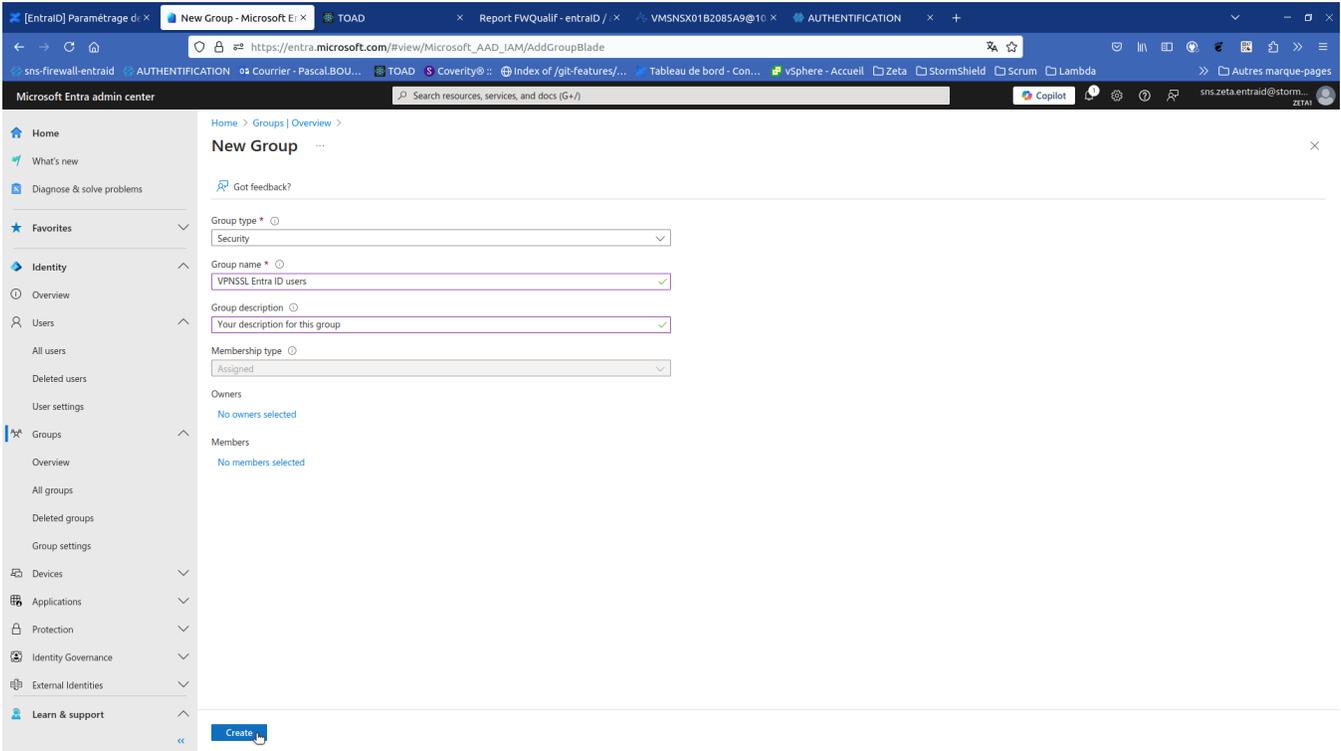
2/ Copy the secret value to then fill in the "ClientSecret" in the SNS configuration.

User Association

Associating users to a security group that will be authorized for SSL VPN.

1/ Go to "Groups" and create a security group named 'VPNSSL EntraID Users'





https://entra.microsoft.com/#blade/Microsoft_AAD_IAM/GroupDetailsMenuBlade/groupid/8239ee3f-d506-4caa-9316-0abd9eb610b1/menuid/

2/ Associate with this group, the users who will be authorized to set up an SSL VPN tunnel (i several methods possible)

The screenshot shows the Microsoft Entra admin center interface. The main content area displays the 'Members' page for the 'VPNSSL Entra ID users' group. It includes a search bar, a table with one member, and various management options.

Name	Type	Email	User type	Object ID
Umar Durr	User		Member	6c59810-cb14-4f51-8d3e-2ac06f587c7c

The screenshot shows the 'All groups' page in the Microsoft Entra admin center. A search filter 'vp' is applied, resulting in one group found: 'VPNSSL Entra ID users'.

Name	Object ID	Group type	Membership type	Email
VPNSSL Entra ID users	8239e3f-d506-4caa-9316-0abdf6b10b1	Security	Assigned	

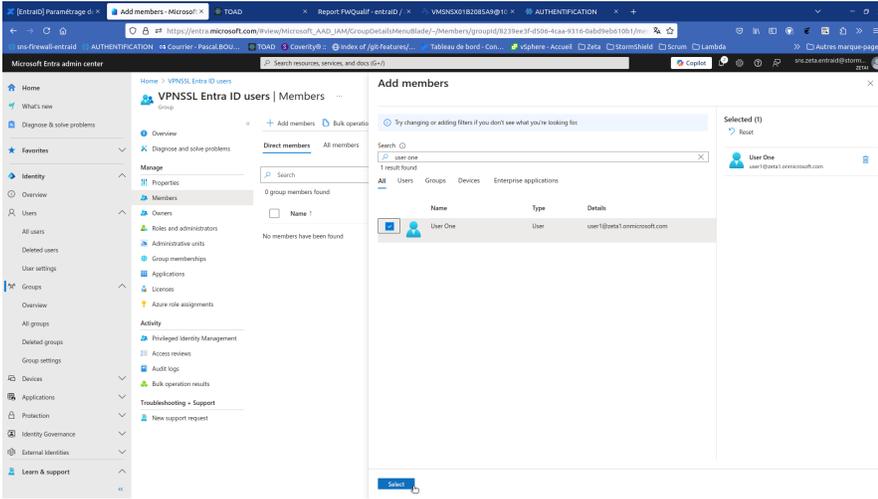
The screenshot shows the 'Overview' page for the 'VPNSSL Entra ID users' group. It displays basic information such as membership type, source, type, object ID, and creation date. Summary cards for group memberships, owners, and total members are also visible.

Basic Information

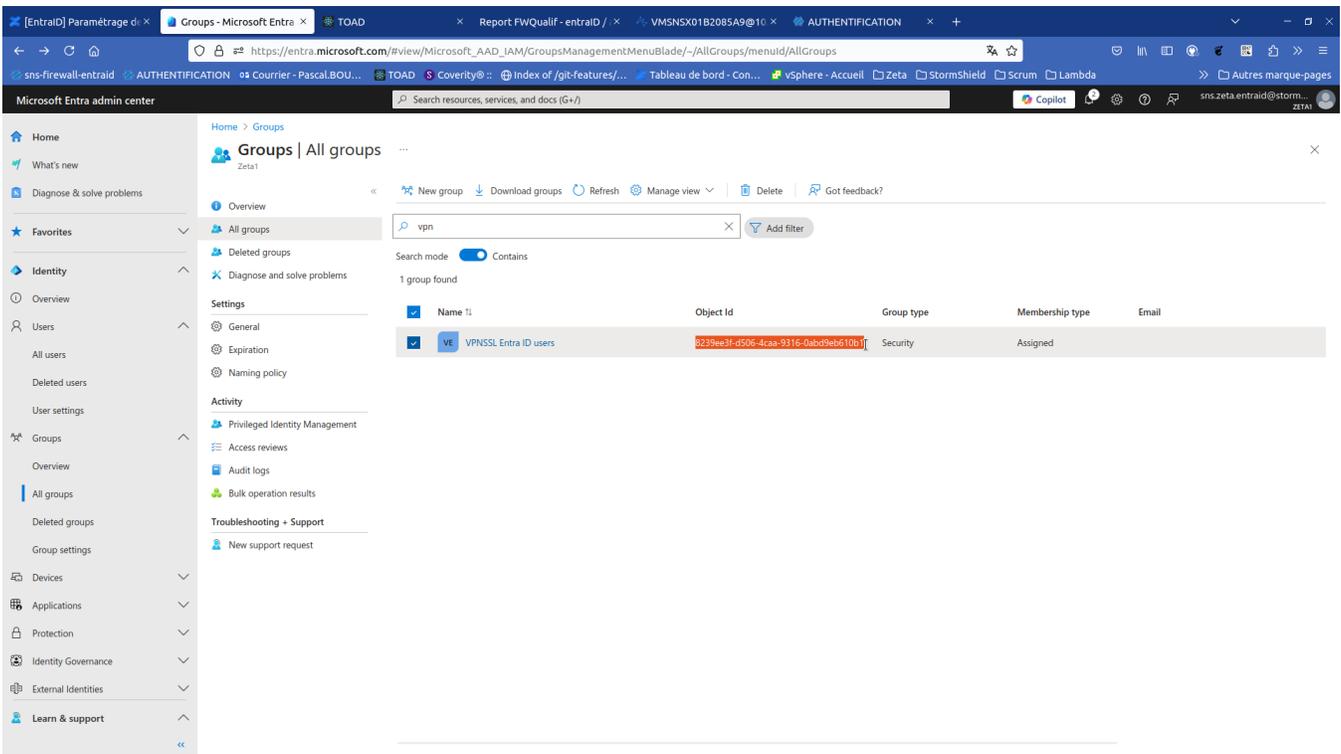
Membership type	Assigned	Total direct members	0
Source	Cloud	Users	0
Type	Security	Groups	0
Object ID	8239e3f-d506-4caa-9316-0abdf6b10b1	Devices	0
Created on	2/24/2023, 2:04 PM	Others	0

Summary Cards:

- Group memberships: 0
- Owners: 0
- Total members: 0

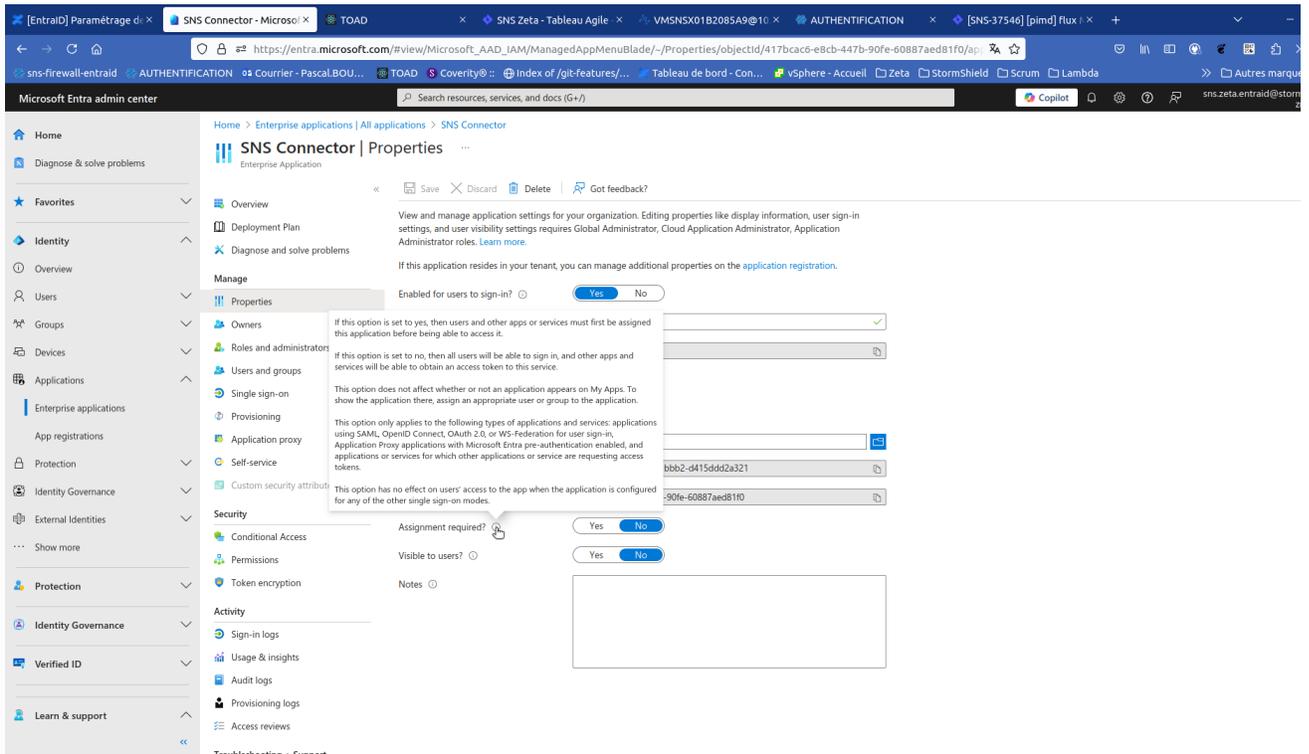


3/ In the "All groups" view, copy the "Object ID" value to enter the group's UID in the SNS configuration.

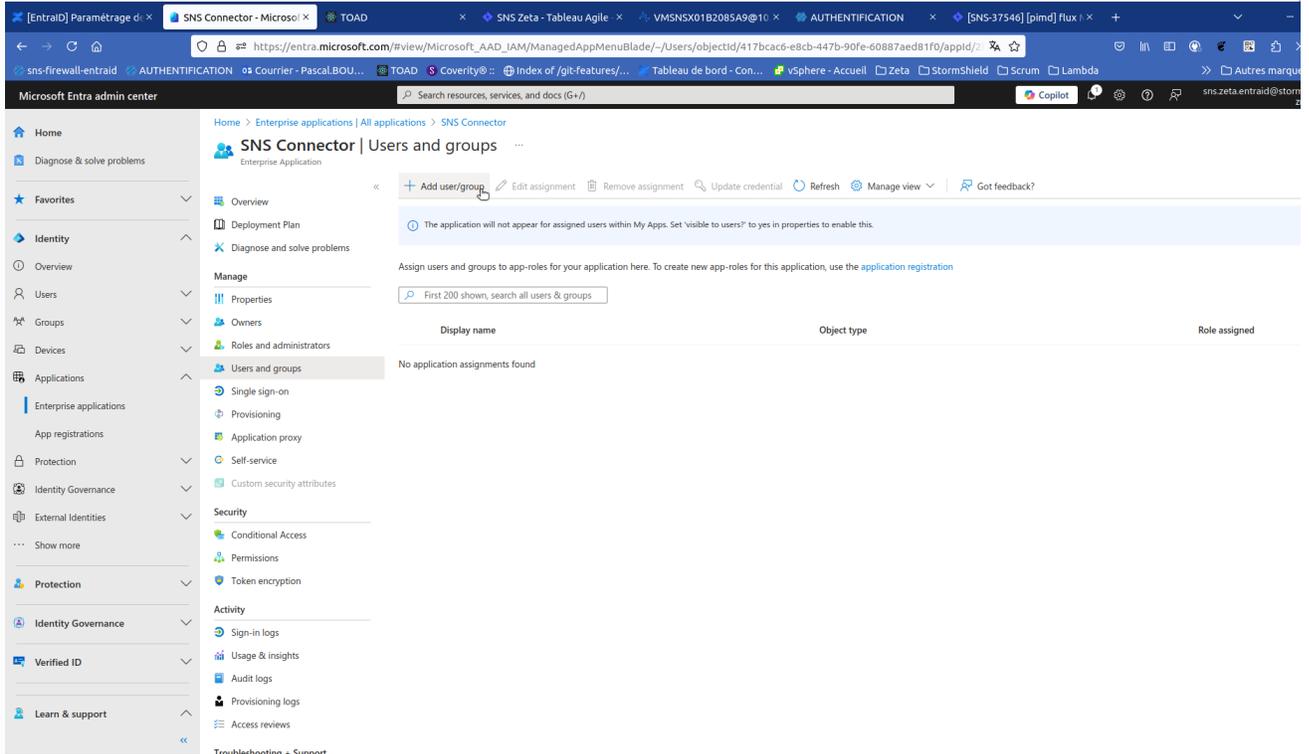


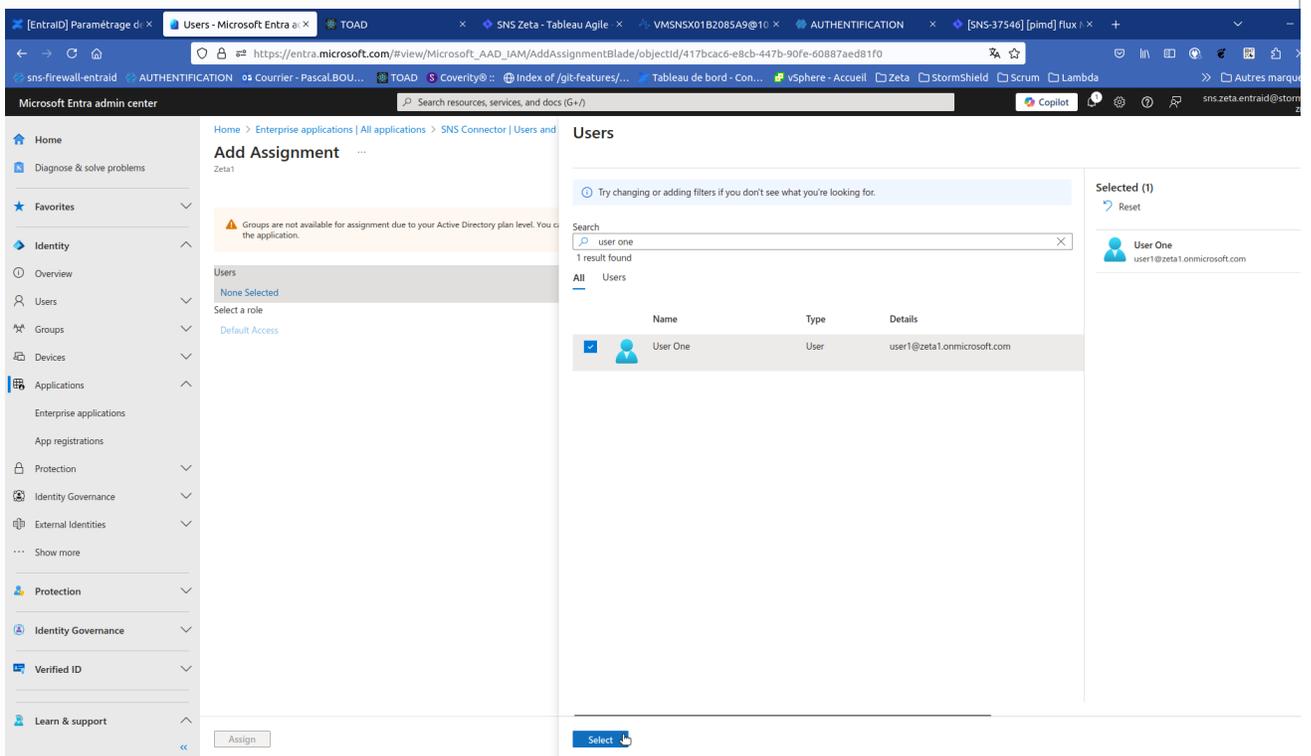
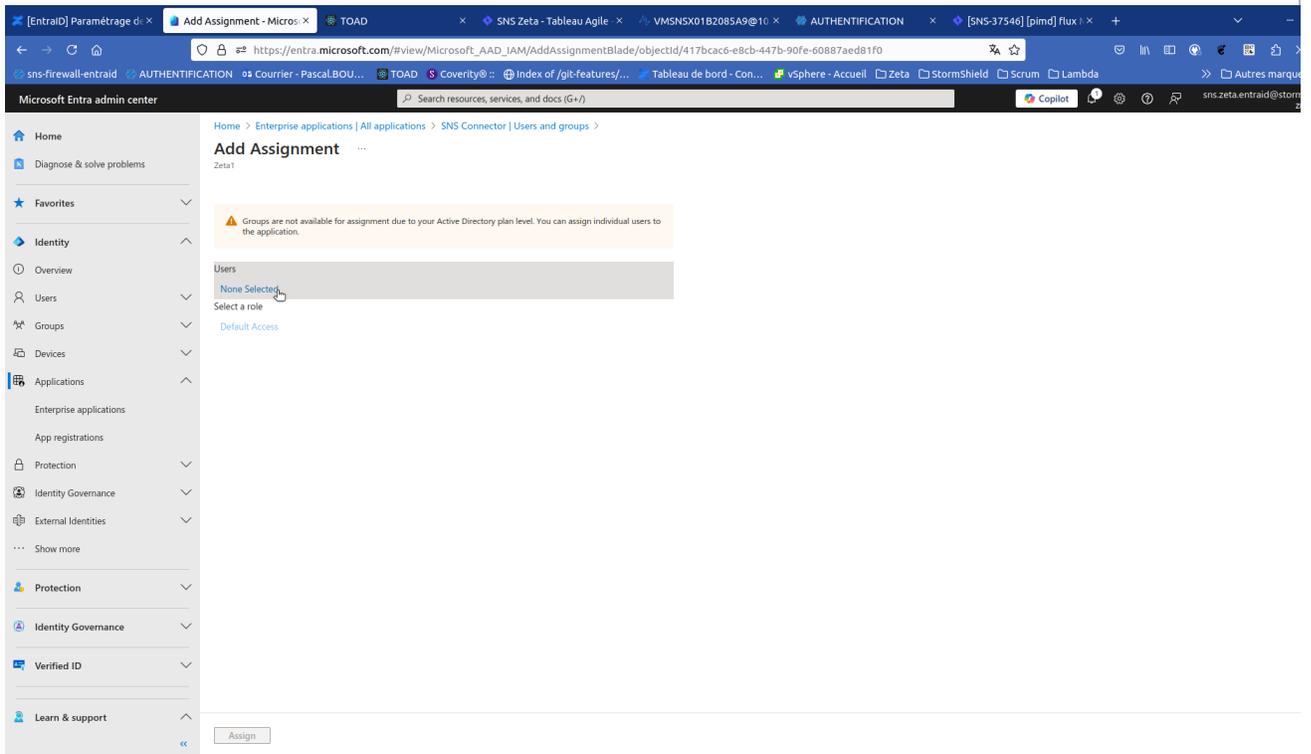
Assignment des utilisateurs à l'application

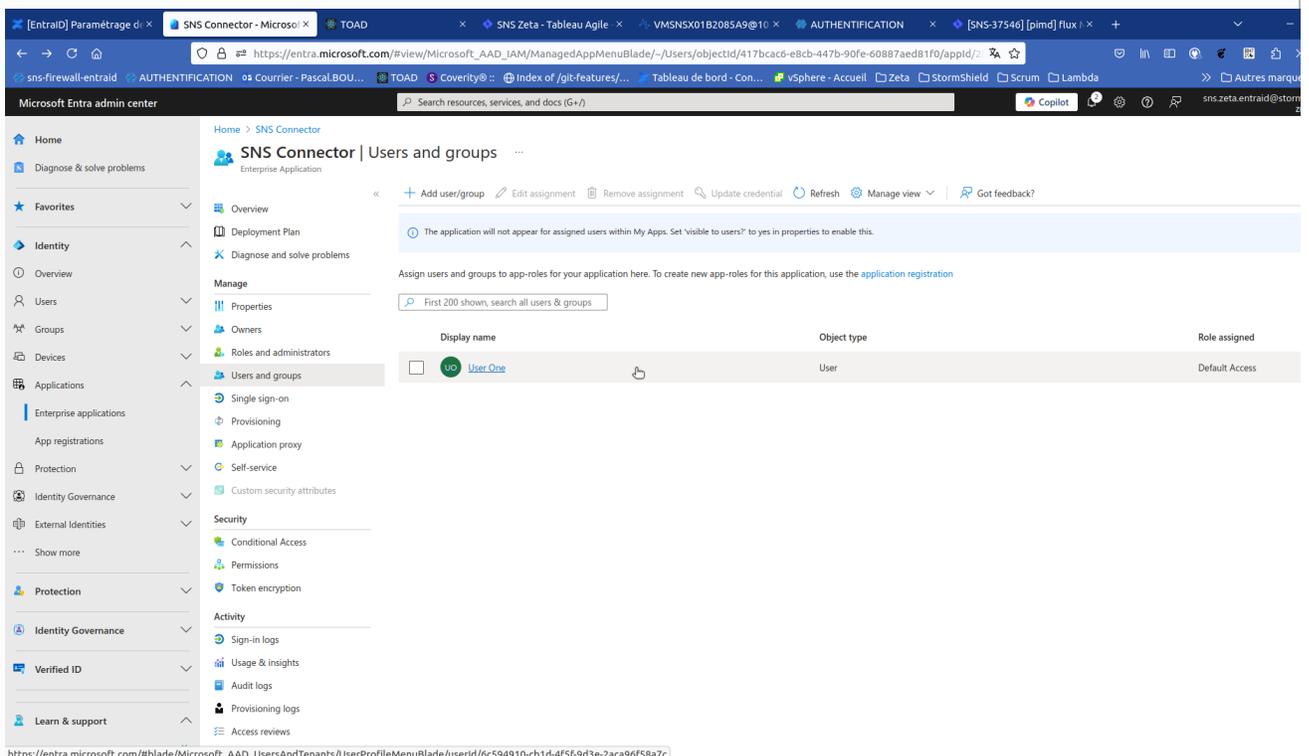
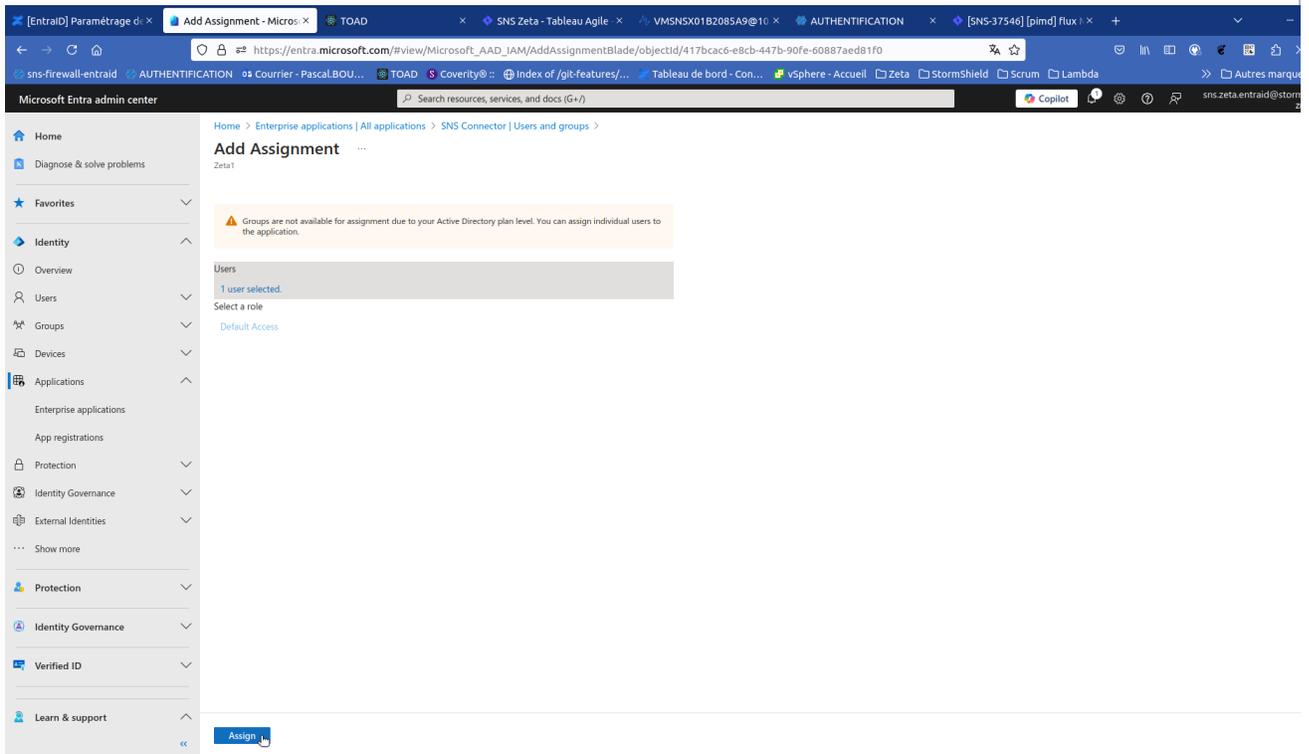
Via **Enterprise applications SNS Connector Properties**, it is possible to allow access to the application to all users of the tenant or to limit its access to a list of users.



In the case where this option is set to **Yes**, you must assign the users you want to authorize via **Users and groups**







It is possible to assign users to the application via their security group, but this option is subject to a P1 subscription.

SNS Configuration

Configuration of the OIDC method for EntraID

To do this, you need to copy the following elements from the EntraID configuration (overview, see previous steps):

- TenantID: Directory ID (tenant)
- ClientID: Application ID (client)
- ClientSecret: Displayed as "Client Secrets"

Update the OIDC authentication profile

In the web administration interface, go to the 'Authentication' panel.

In the 'Activate a method' menu, choose 'OIDC / Entra ID'

Copy the EntraID configuration elements into the assistant.

! Proceed to configure the redirect URLs before finishing the assistant.

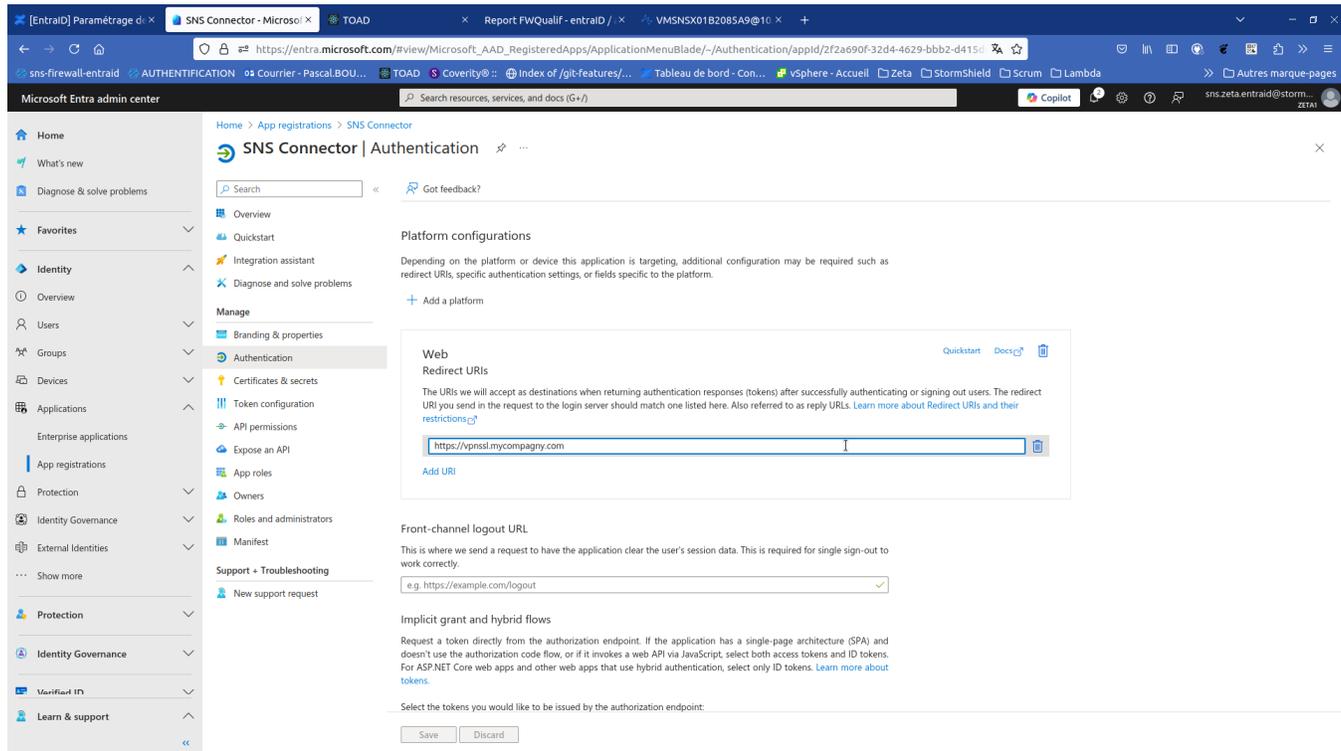
i The "IssuerID" parameter will be built as: "[https://login.microsoftonline.com/\\$TENANTID/v2.0](https://login.microsoftonline.com/$TENANTID/v2.0)"

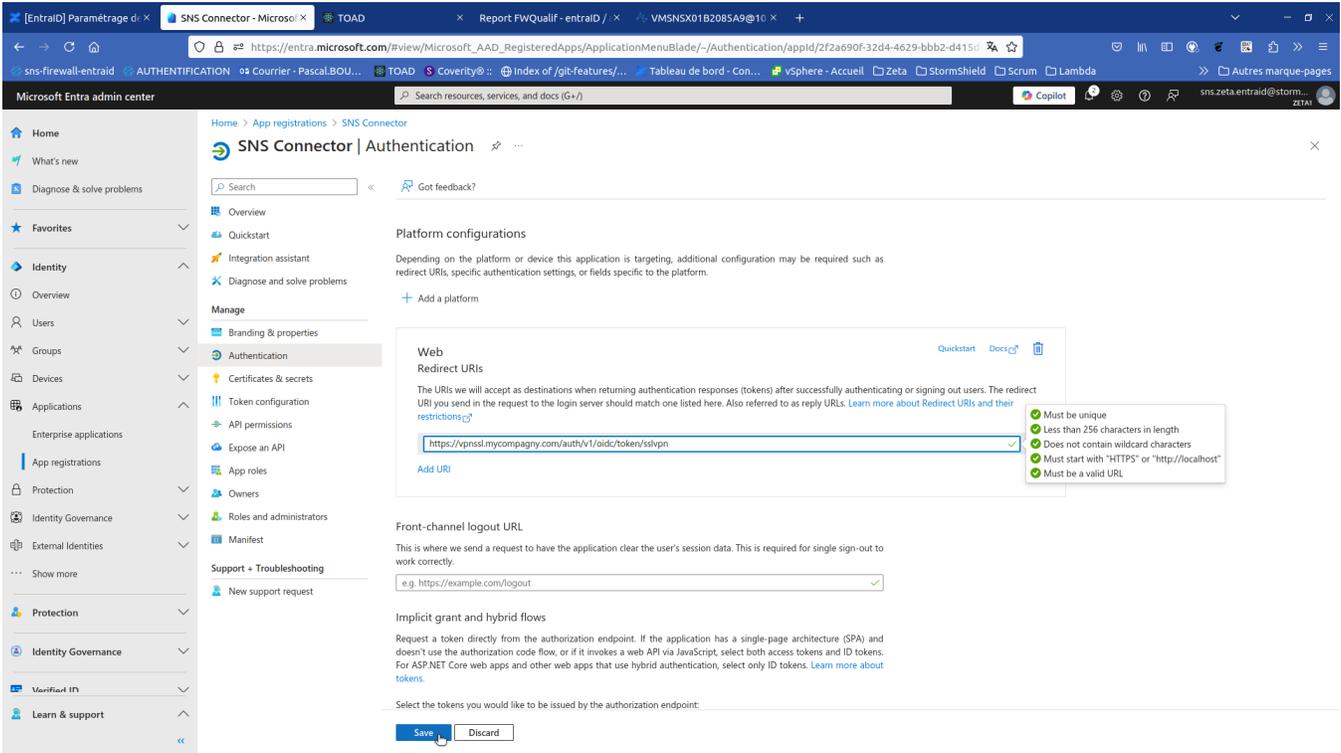
The redirect URLs are built from the Captive Portal configuration (System/Configuration -> General Configuration -> Advanced Configuration -> Captive Portal)

Configuration of Redirect URLs in EntraID

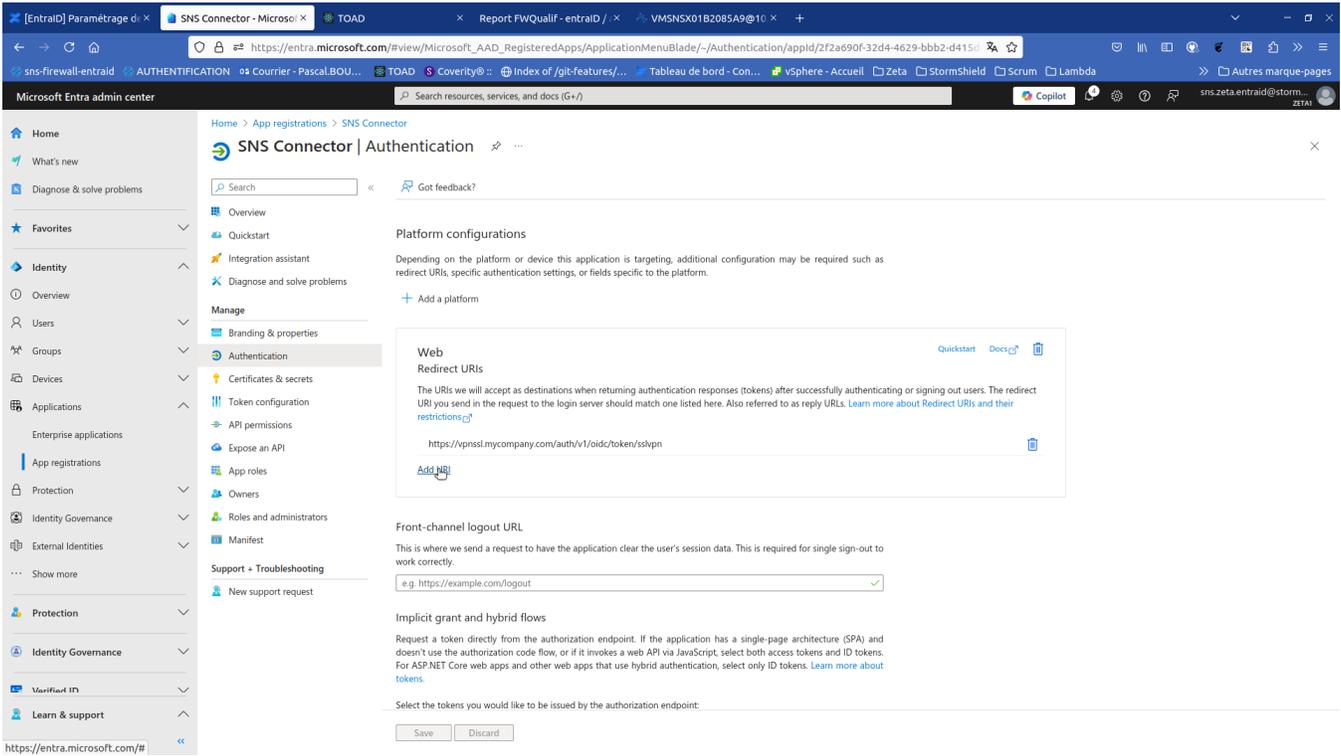
Update the desired redirect URI in the SNS Connector application from the proposed ones

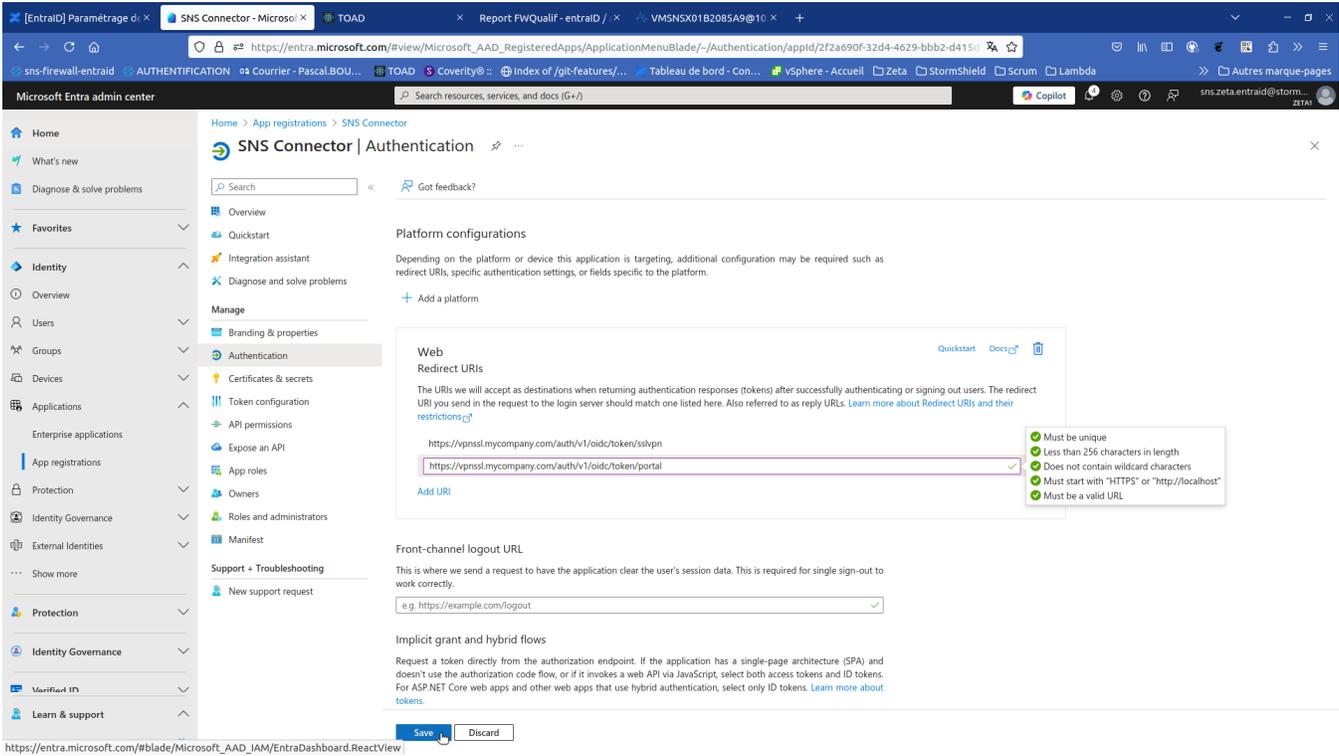
1/ Update the existing redirect URI





2/ Add if necessary the redirect URI to allow authentication via the SNS captive portal





3/ On this same page, take the opportunity to check the following configurations:

- Ensure that the options **"Access tokens (used for implicit flows)"** and **"ID tokens (used for implicit and hybrid flows)"** are not checked to ensure that the application does not use either the implicit flow or the hybrid flow, in accordance with security best practices.
- The option **"Accounts in this organizational directory only (Single tenant)"** must be selected. The other options have not been internally tested, their operation cannot be guaranteed and they are not officially supported.
- The application uses redirect URIs and does not rely on public client flows. The **"Allow public client flows"** option must therefore be set to **"No"**.

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

- Access tokens (used for implicit flows)
- ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Zeta1 only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

[Help me decide...](#)

 Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#) ✕

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

Yes No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#) 
- No keyboard (Device Code Flow) [Learn more](#) 
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#) 

Re-check the SNS configuration

If all the **redirect URIs** listed by SNS have been entered in the **SNS Connector** application on the EntraID side, then no warning will be displayed and the configuration will be considered valid.

 [Finish configuration assistant](#)

UTILISATEURS / AUTHENTIFICATION

MÉTHODES DISPONIBLES POLITIQUE D'AUTHENTIFICATION PORTAIL CAPTIF PROFILS DU PORTAIL CAPTIF

+ Activer une méthode X Désactiver

Méthode

- LDAP
- SSL
- RADIUS
- Invités
- Comptes temporaires
- Parrainage
- Agents TS
- OIDC / Microsoft EntraID**

OpenID Connect / Microsoft EntraID

Domain:

Fill in informations about SNS application of your Microsoft Entra ID tenant :

Service URL (Issuer ID):

Application ID (Client):

Client secret:

URL of services

Copy and fill in the following URL in SNS application of your Microsoft Entra ID tenant :

Captive portal:

SSL VPN portal:

Web administration:

URLs related to the Captive portal and SSL VPN portal are generated from the [Système / Configuration](#) module (advanced properties).

Force re-authentication if Entra ID session exceeds this duration :

Maximum duration: Day(s) Hour(s)

TEST CONFIGURATION

Importing EntraID Security Groups

1/ Creation of an OIDC group corresponding to VPNSL users

Go to the 'Users' panel and the 'ENTRA ID' tab

Add a security group and apply the configuration

Example :

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

UTILISATEURS / UTILISATEURS

[TAB-TITLE]LDAP [TAB-TITLE]ENTRA ID

MICROSOFT ENTRAID (STORMSHIELD.ONMICROSOFT.COM)

Enter un filtre... Select All + Add X Supprimer Edit Verifier l'utilisation Import security groups Configure auth method

Security groups / Application roles	Uid	Description
Security groups (1)		
VPNSL EntraID Users	8239ee3f-d506-4caa-9316-0abd9eb610b1	Your description for this group
Application roles (4)		
Administrators	SNS.Config.All.Write	User with administrator credentials, granted via OIDC claims
Auditors	SNS.Config.All.Read	User allowed to read configuration, granted via OIDC claims
Sponsors	SNS.Sponsor	Sponsor users, granted via OIDC claims
VPNSL users	SNS.VPNSL	Users with VPNSL access, granted via OIDC claims

Configuration of the security group in the UAC to allow SSL VPN

Creation of an authentication rule

The authentication rule must apply to the "out" interfaces to allow access to the captive portal, but also "sslvpn" to allow the establishment of SSL VPN tunnels for this type of user.

"Authentication" panel, "Authentication Policy" tab to create a rule based on the OIDC method and apply the configuration.

Example:

- Action = Allow
- Source = "any@any"

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

UTILISATEURS / AUTHENTIFICATION

MÉTHODES DISPONIBLES **POLITIQUE D'AUTHENTIFICATION** PORTAIL CAPTIF PROFILS DU PORTAIL CAPTIF

Recherche par utilisateur... + Nouvelle règle X Supprimer | Monter Descendre | Couper Copier Coller

	État	Action	Source	Méthodes (évaluées par ordre)	Mot de passe à usage unique	Commentaire
1	Activé	Autoriser	Any user @any out sslvpn	1 OIDC		N/A

Creation of an access rule

"Access Rights" panel, "Detailed Access" tab to validate or edit the rule allowing VPNSSL access.

Example:

- User= "VPNSSL EntraID Users"
- Domain = stormshield.onmicrosoft.com
- SSL VPN = Allow

UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT **ACCÈS DÉTAILLÉ**

Rechercher... + Ajouter X Supprimer | Monter Descendre

	Etat	Utilisateur - groupe d'utilisateurs	IPSEC	VPN SSL	Parrainage	Description
1	Activé	VPNSSL EntraID Users@stormshield.onmicrosoft.com	Interdire	Autoriser	Interdire	

Using the SSL VPN Client 5.1

When setting up the gateway (in direct connection or as a registered connection), in "Stormshield" mode, check the box "Log on with single authentication"

i The Server field must necessarily specify the FQDN of the SNS that corresponds to the redirect URL previously configured in the SNS and EntraID.

In particular, directly entering an IP address of the SNS will return an "internal" error.

+ Ajouter une nouvelle connexion

Mode Stormshield

Import de fichier .OVPN

Nom *

EntralD SNS

Serveur *

snsv5.stormshield.eu

Port *

443

Description

Authentification

Se connecter avec l'authentification unique

Options de connexion

Se connecter automatiquement 

Annuler

Ajouter