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

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

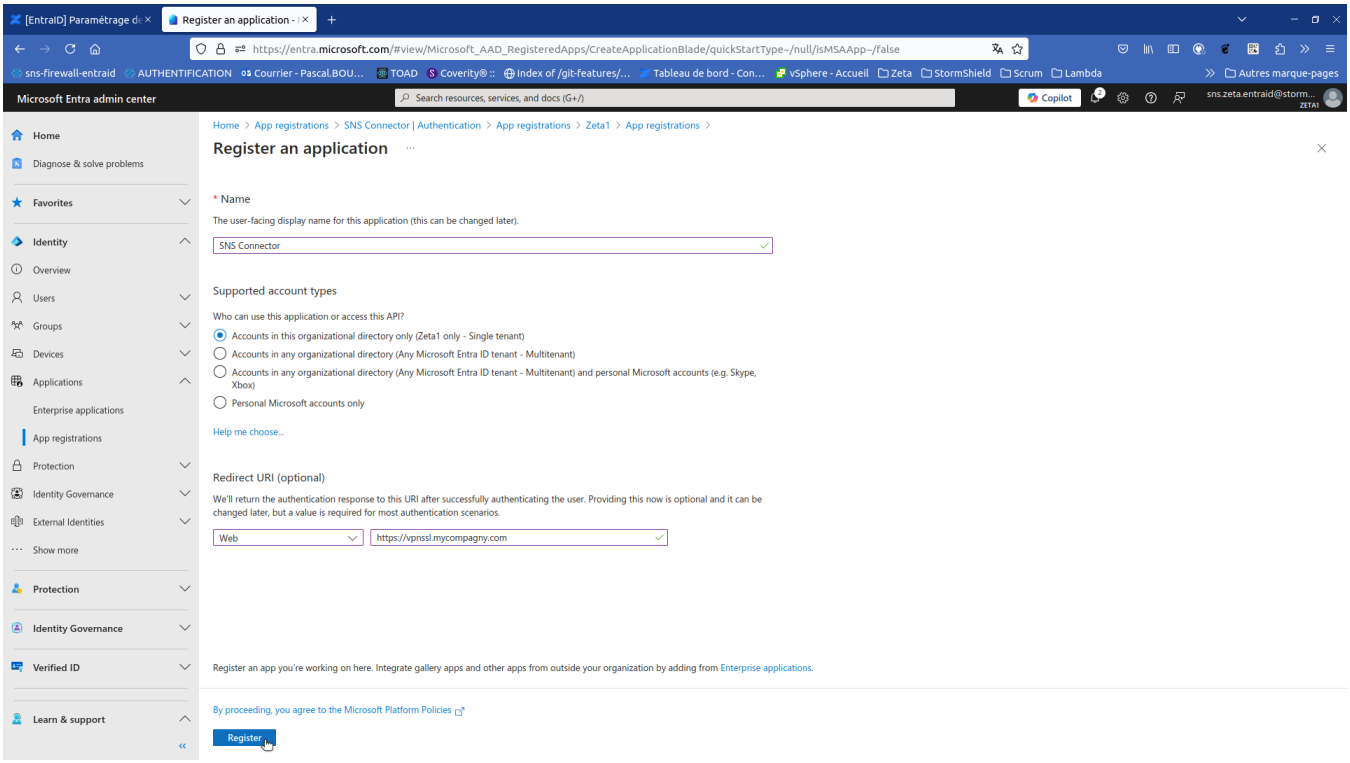
Creation of the application

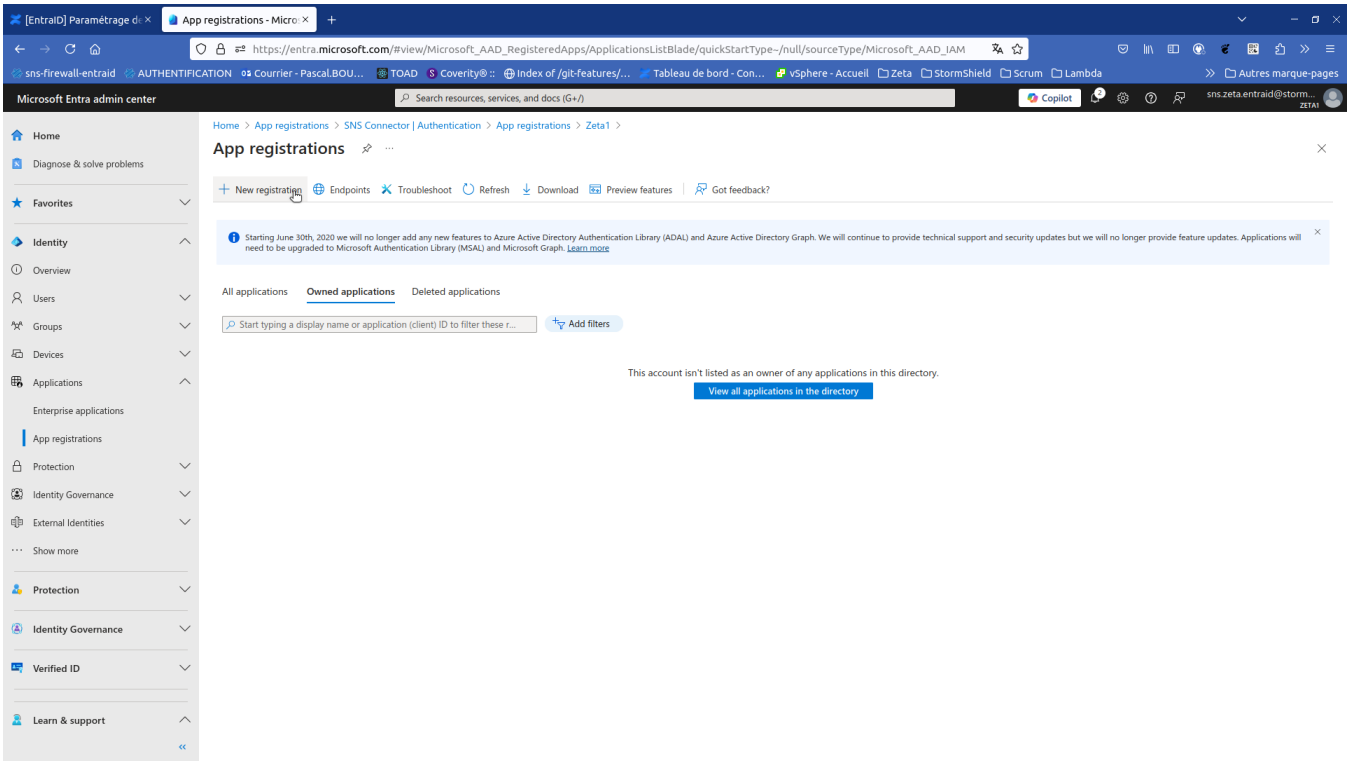
Configuration of the SNS application in EntraID

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

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

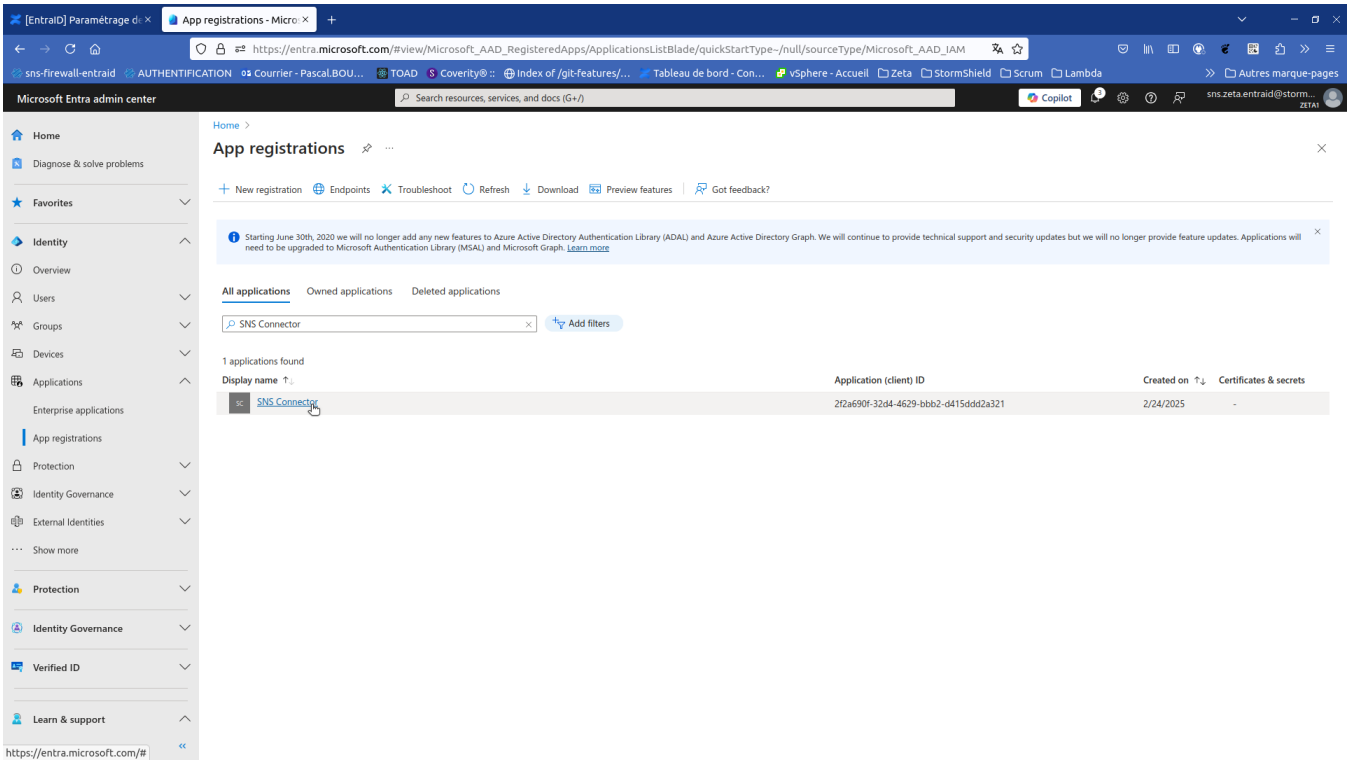
and enter the public URL of the SNS for example: "https://vpnssl.mycompany.com **/auth/v1/oidc/token/sslvpn**"



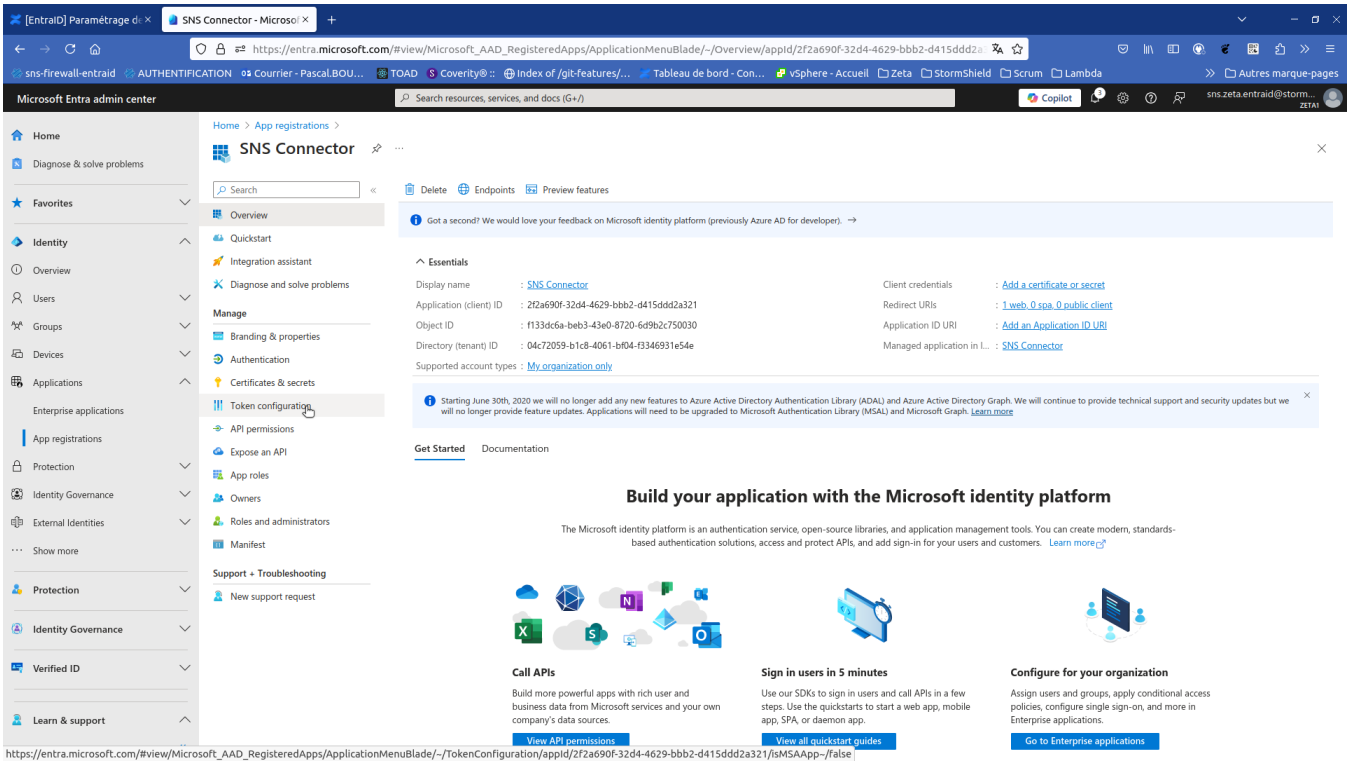


Token Configuration

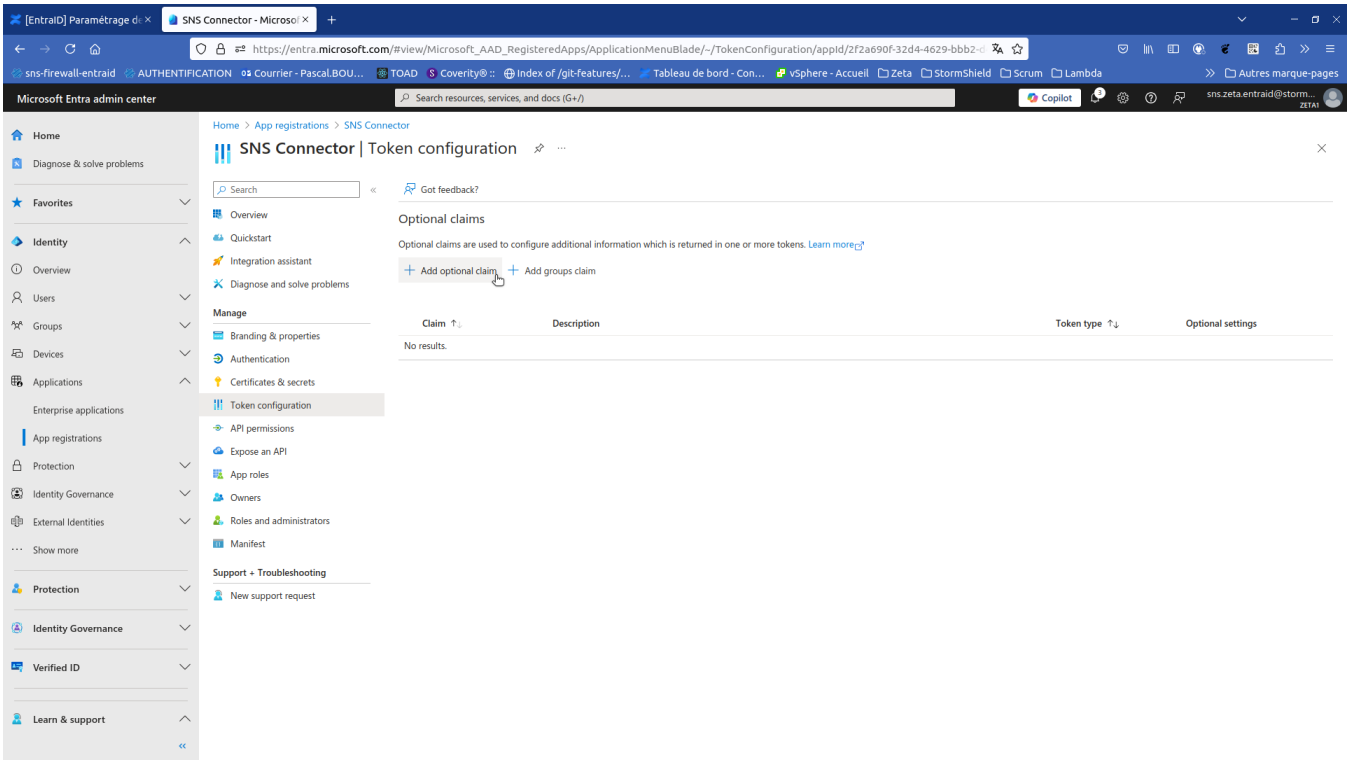
1/ Go to "Application Registration" ; click on "Display all applications in the directory" and select the SNS connector application, then "Token Configuration"

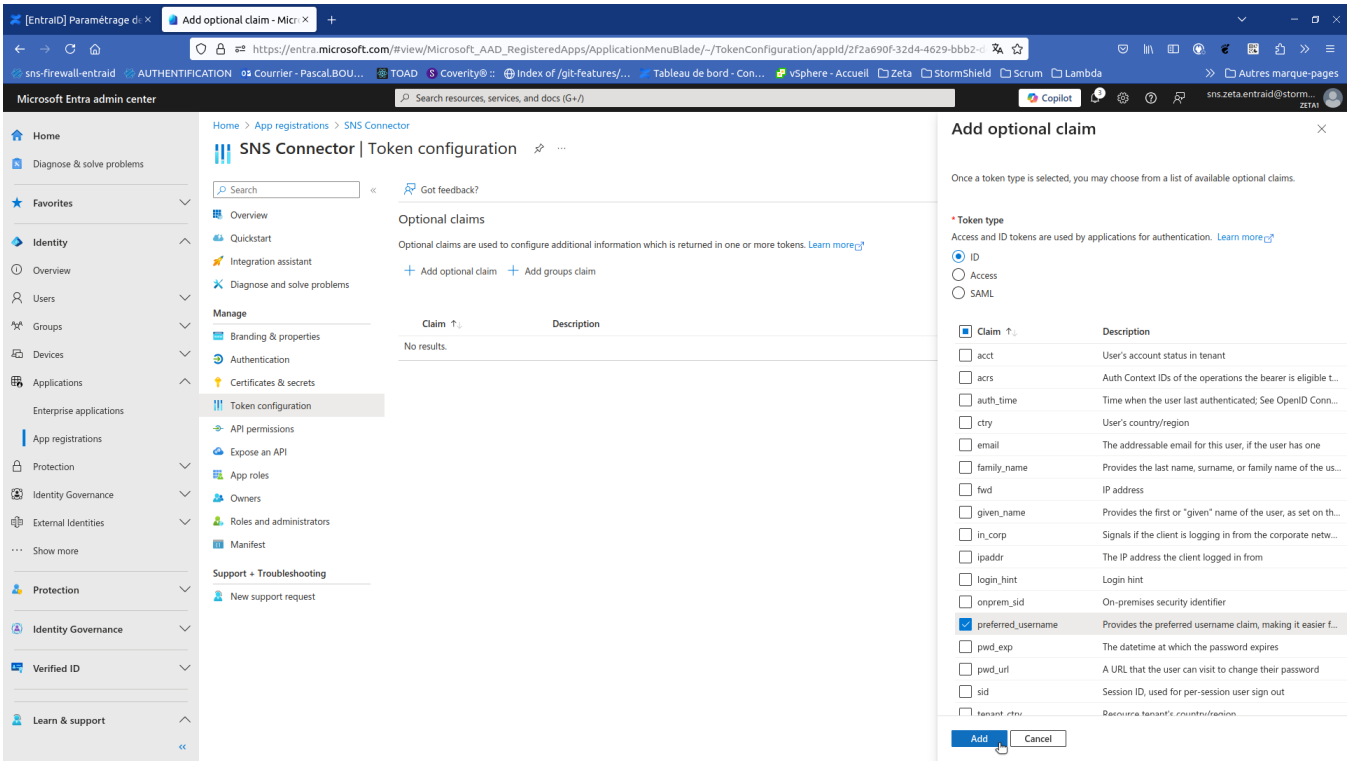


Token configuration :



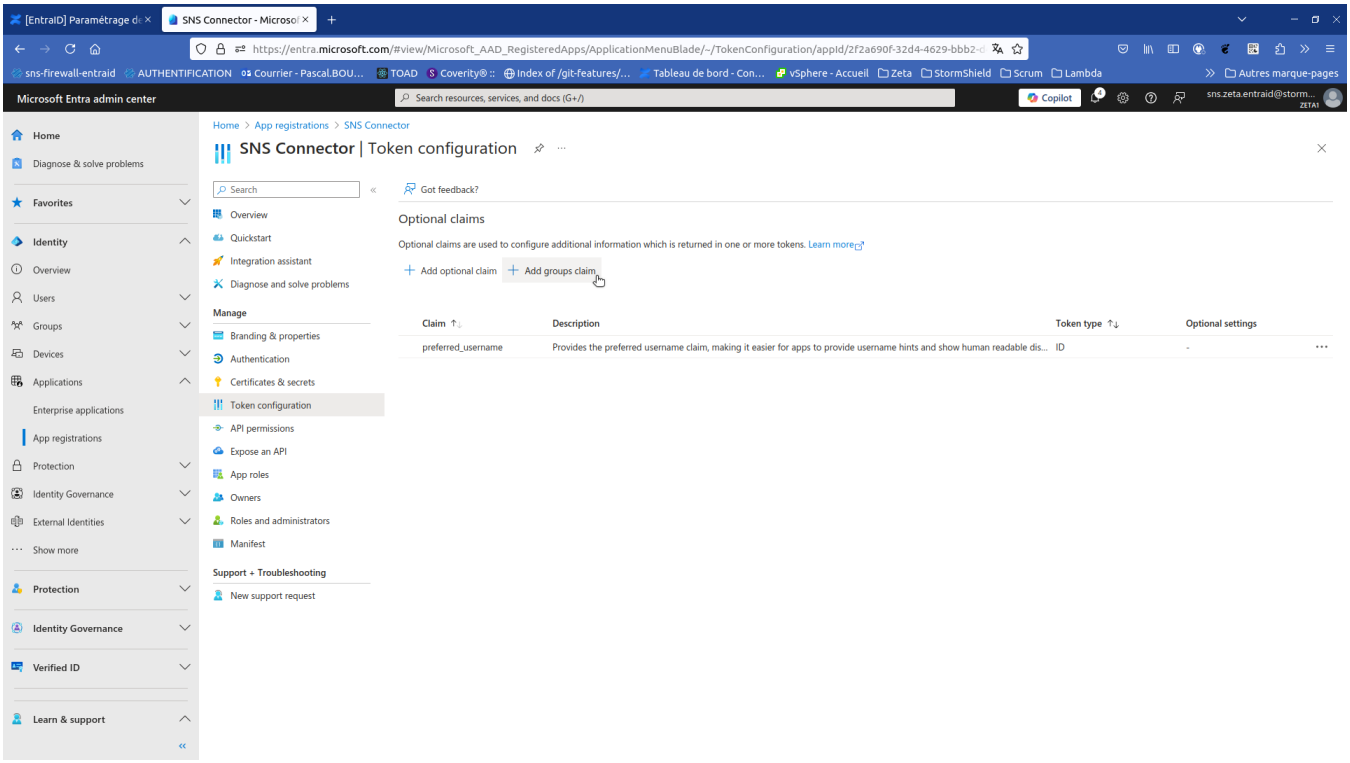
2/ Add the optional "preferred_username" claim for the ID Token (⚠️ mandatory for SNS)

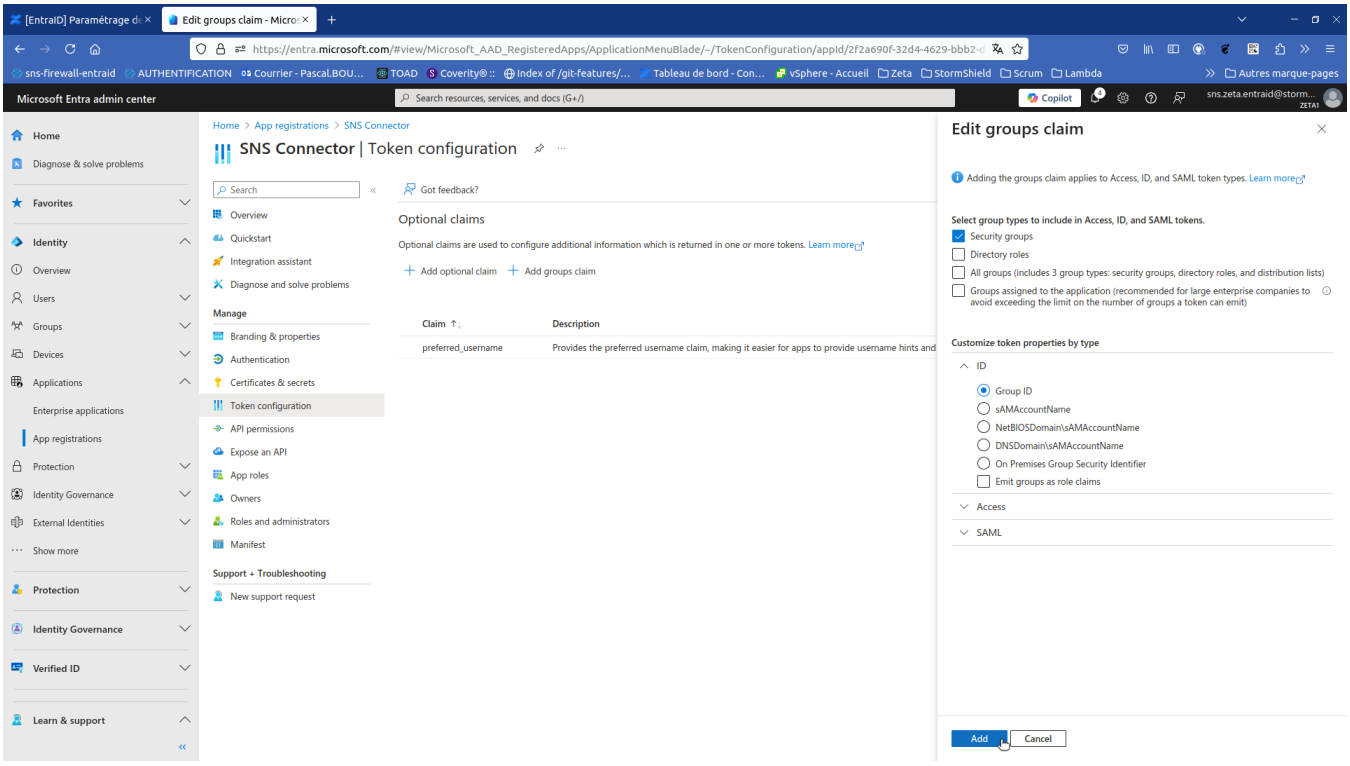




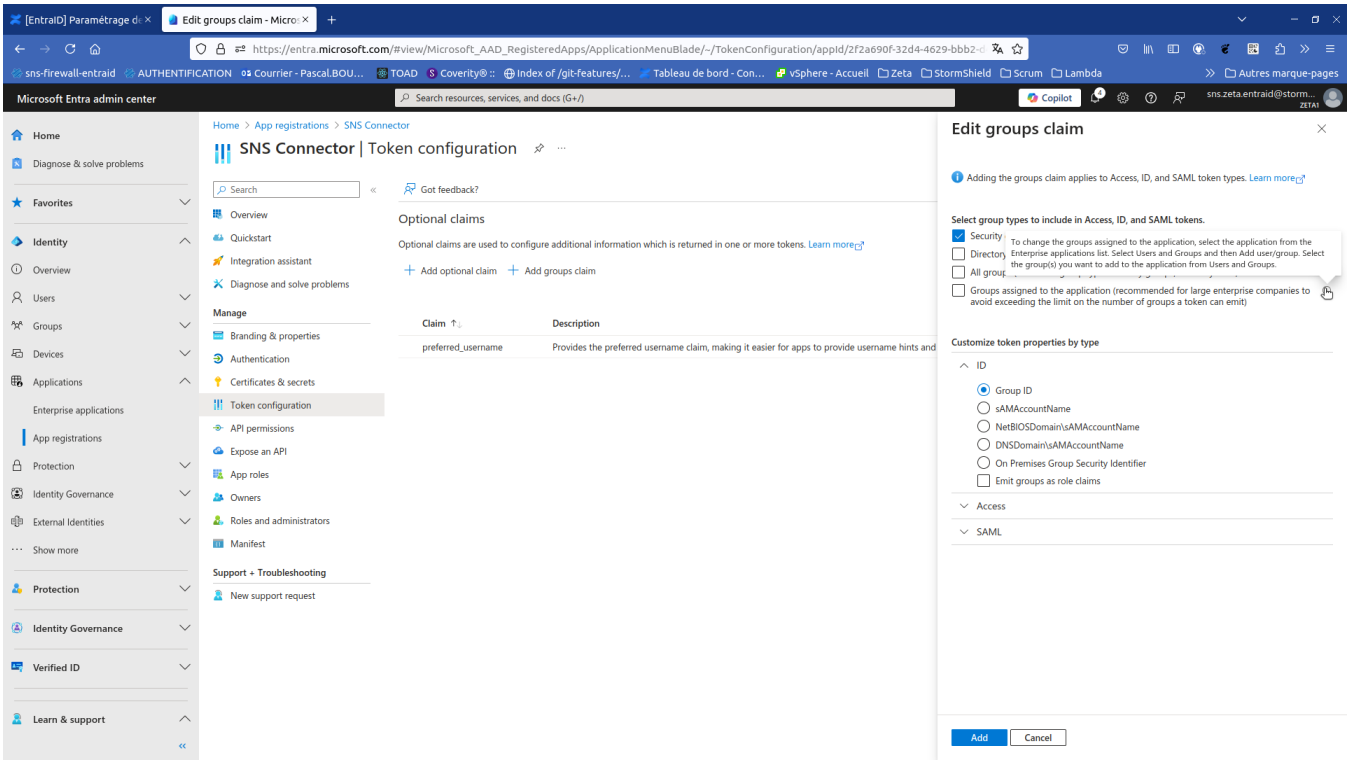
3/ For "Add Group Claim", and in the "Edit Group Claim" section, check "Security Groups" with ID on "Group ID".

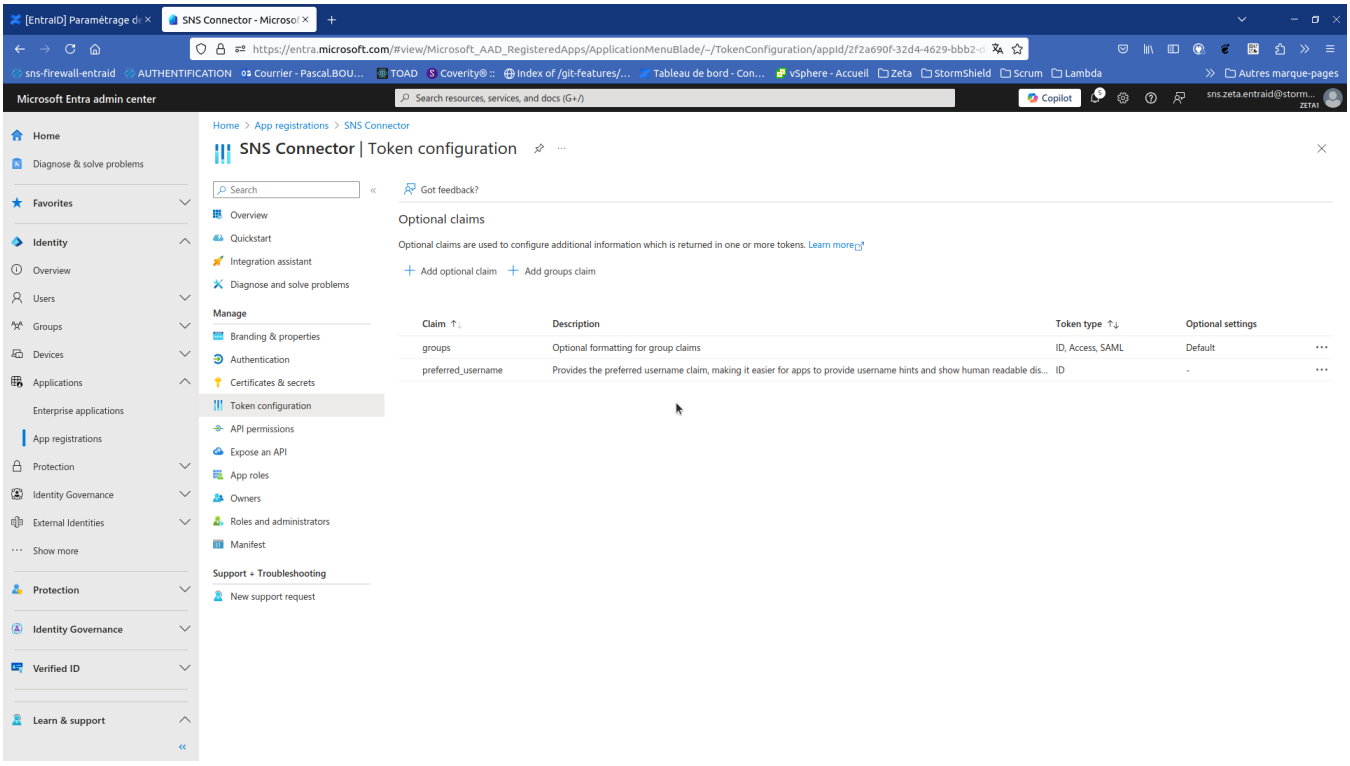
Optional for SNS but strongly recommended in order to benefit from UAC/AAC/filtering and authentication policies on security groups.





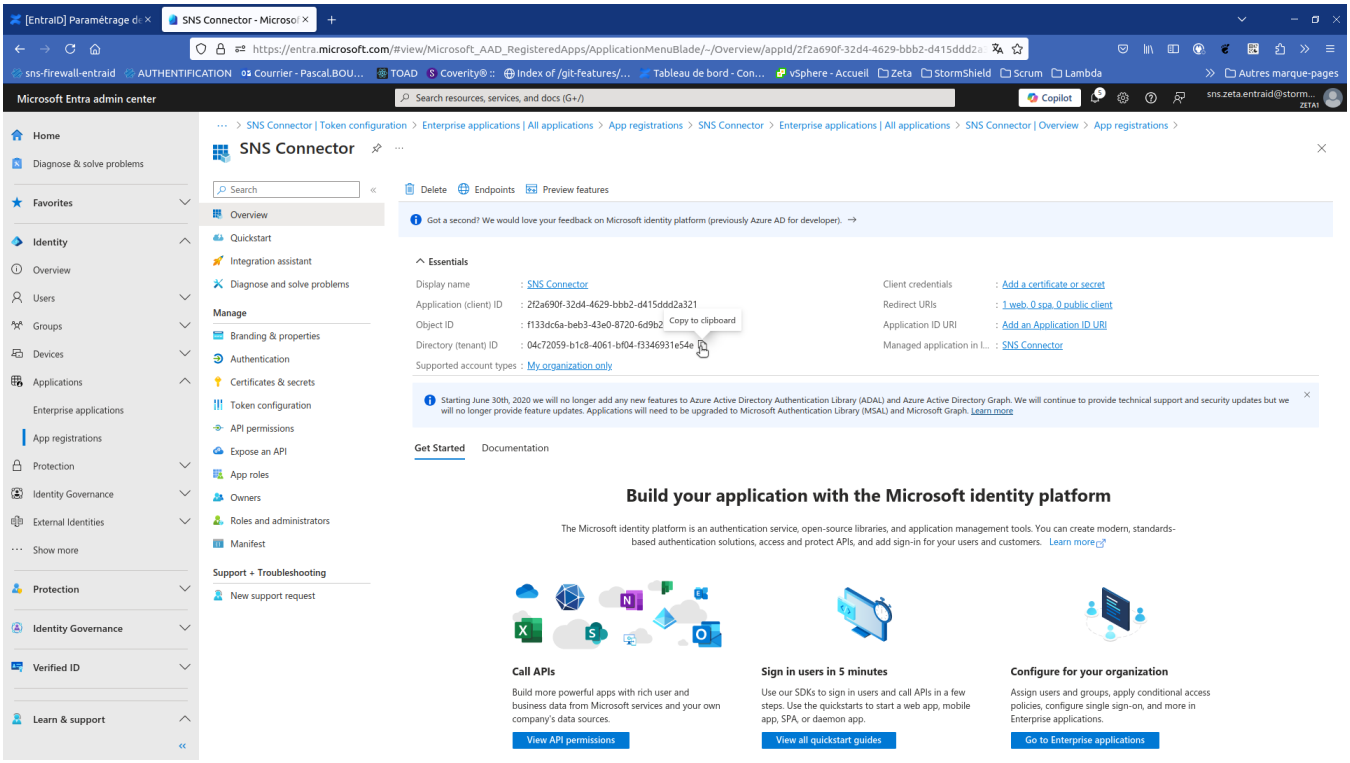
Note that it is possible to limit the groups included in the ID Token to those assigned to the application, but this is subject to a P1 subscription.

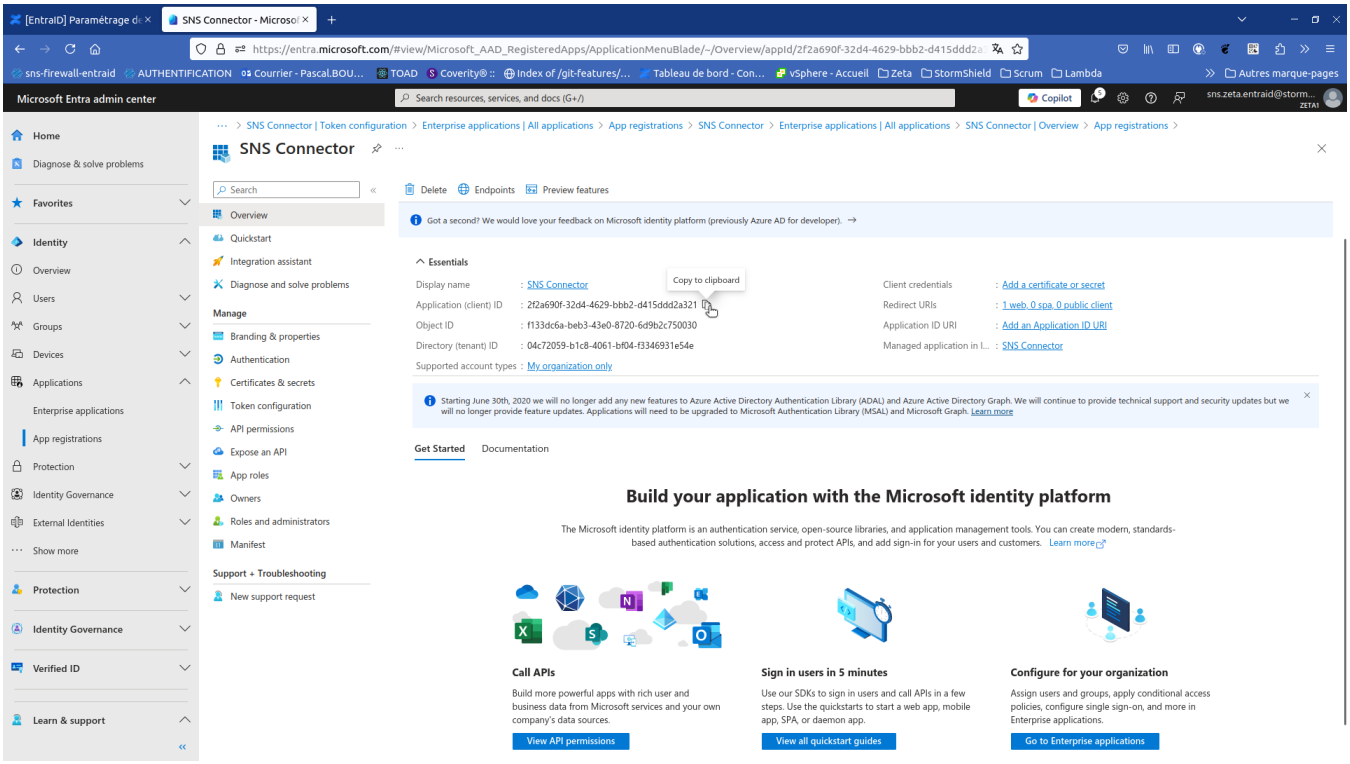




4/ From App registrations SNS Connector Overview

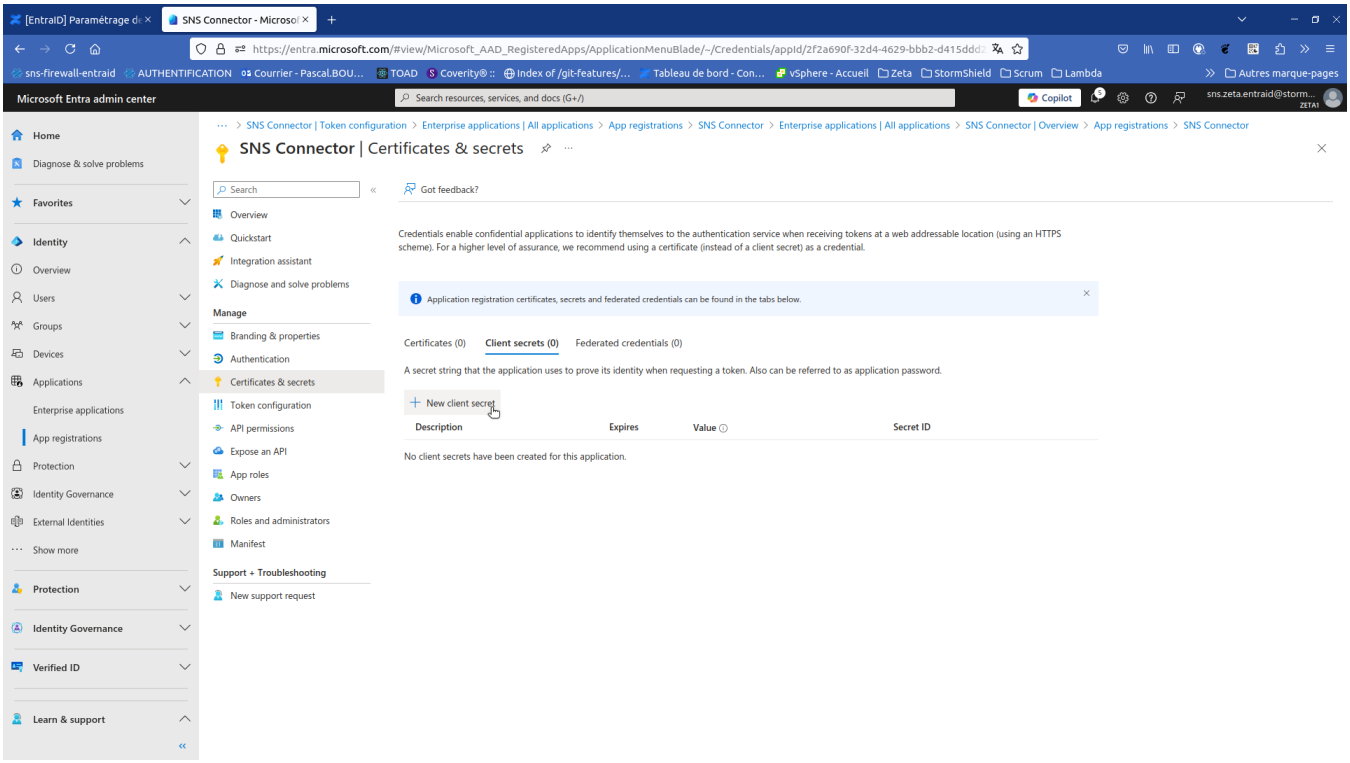
- Copy the value of "Directory (tenant) ID" to fill in the "IssuerID" in the SNS configuration.
- Copy the value of "Application (client) ID" to fill in the "ClientID" in the SNS configuration.

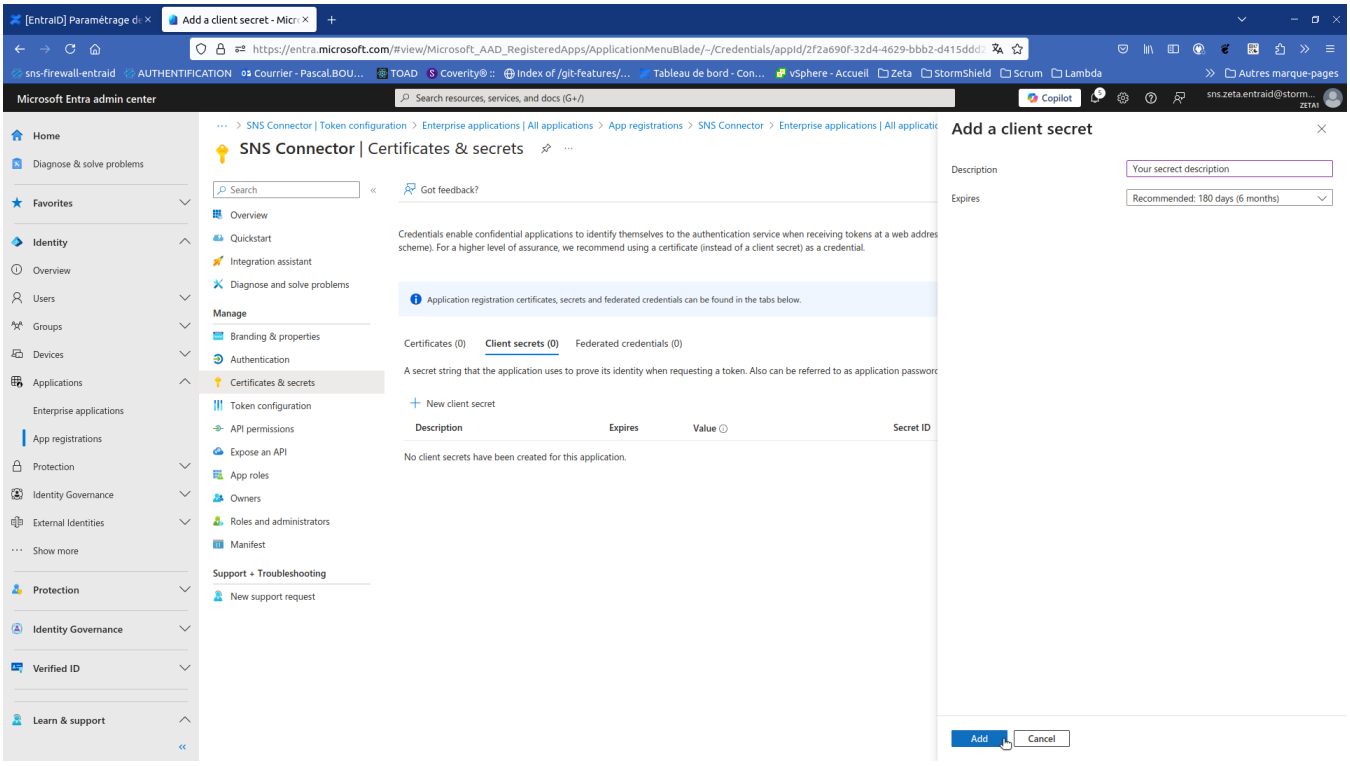


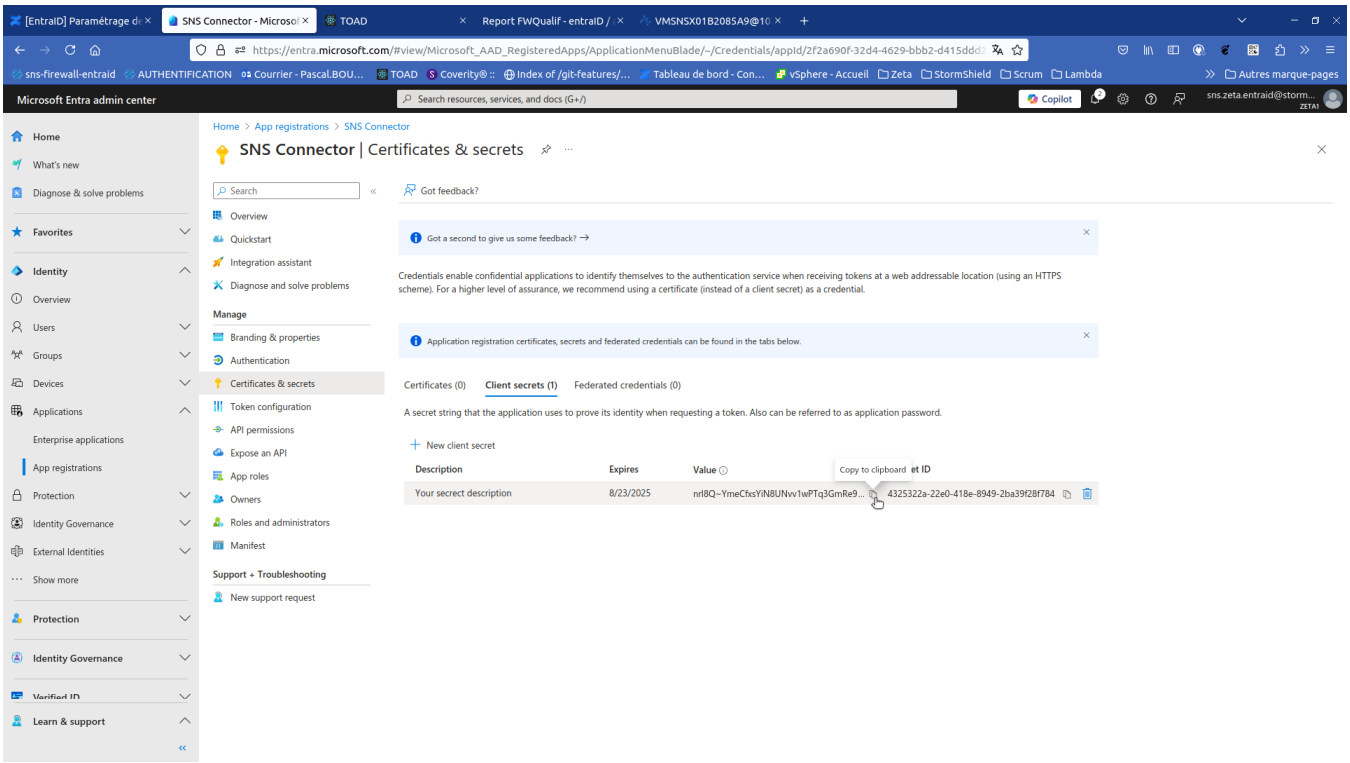


Creation of the secret

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


[EntraID] Paramétrage d
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 d
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 applicati
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
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

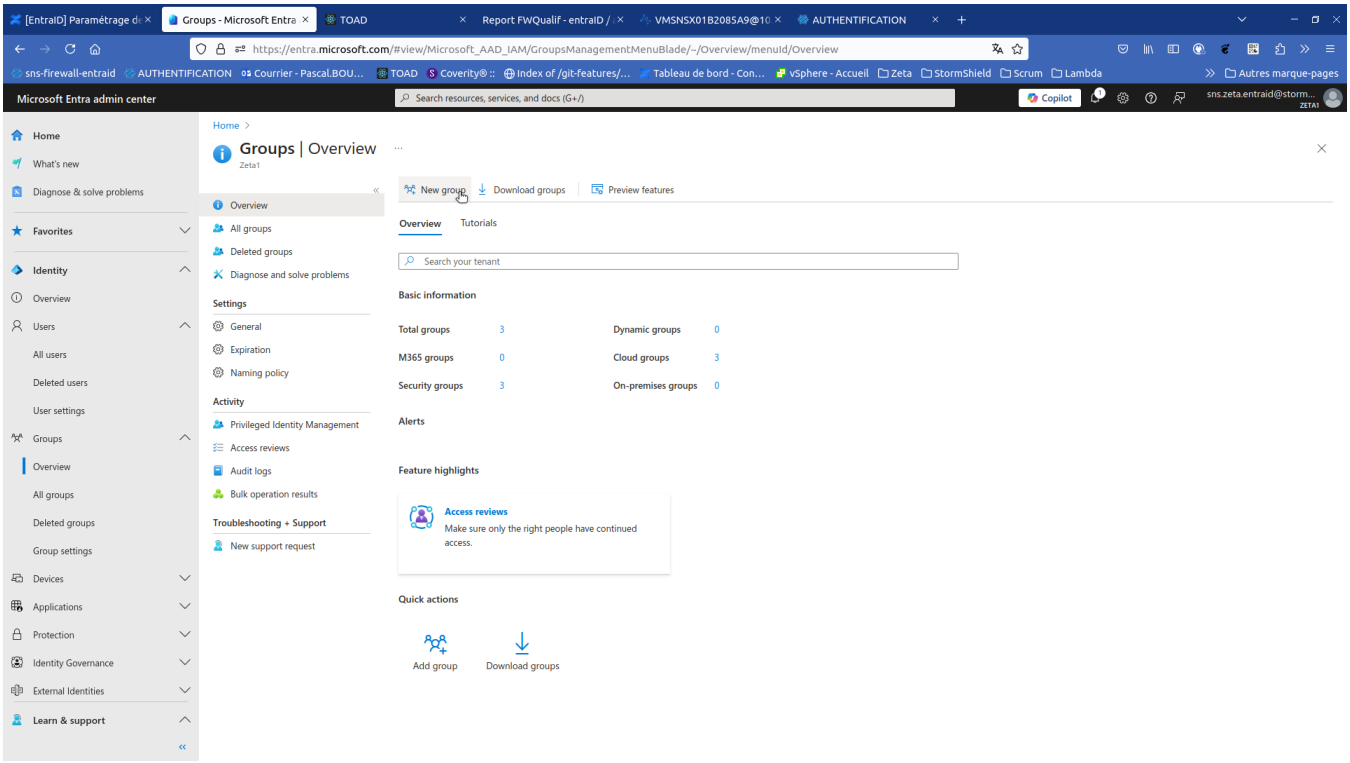


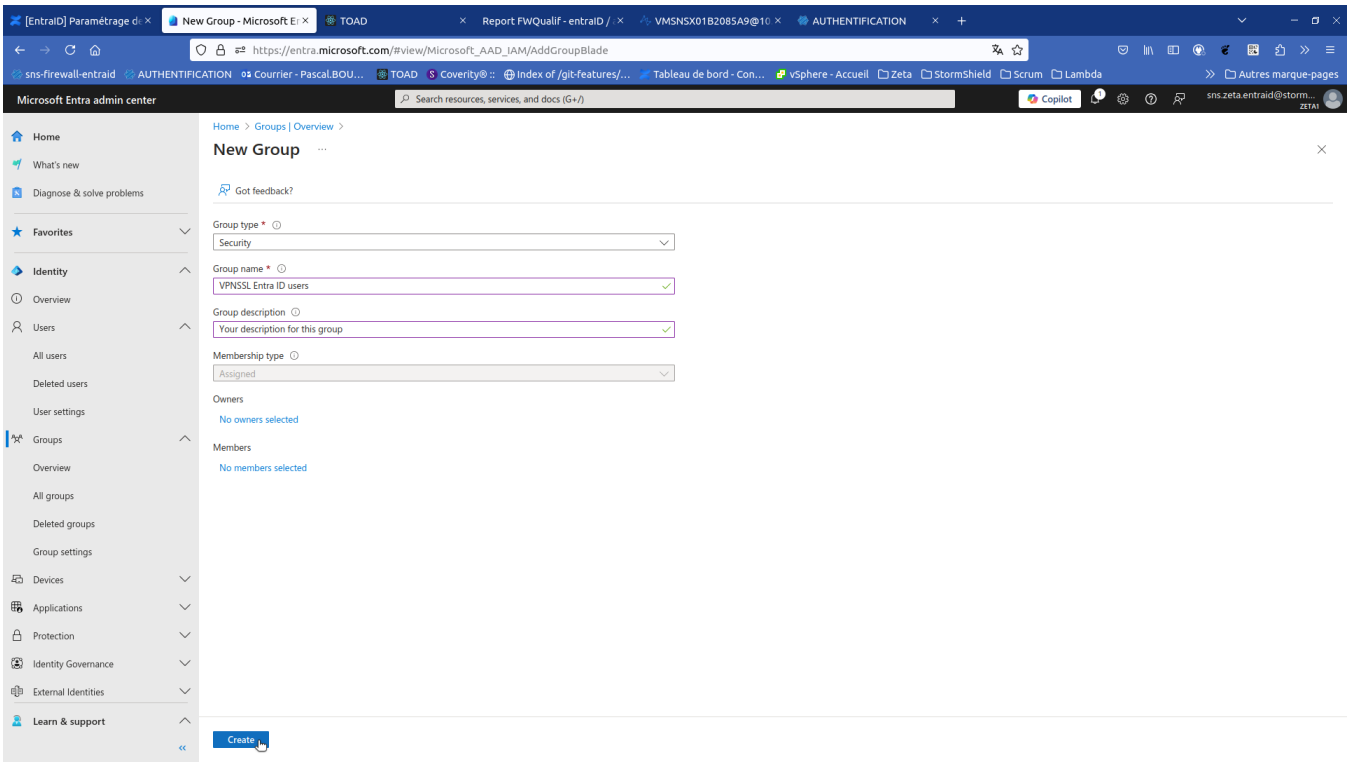
2/ Copy the secret value to then fill in the "ClientSecret" in the SNS configuration.

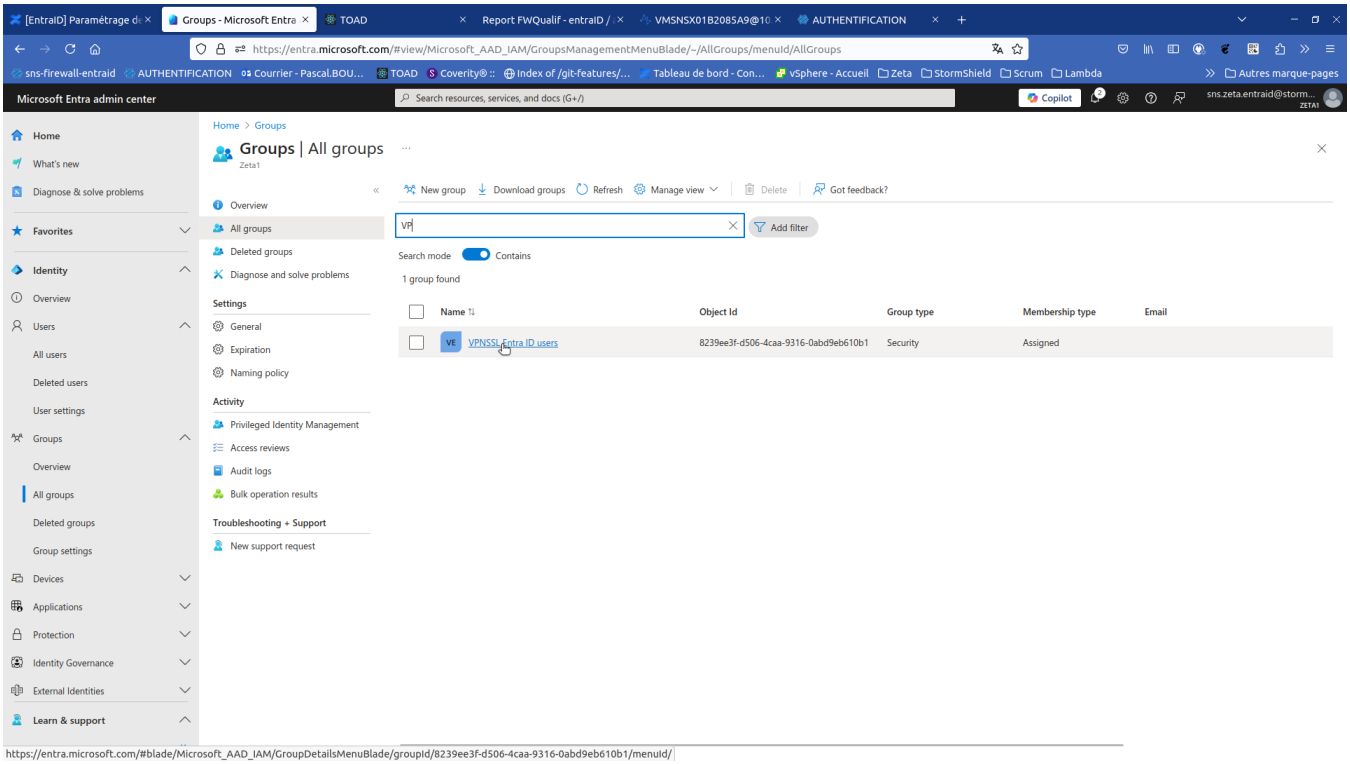
User Association

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

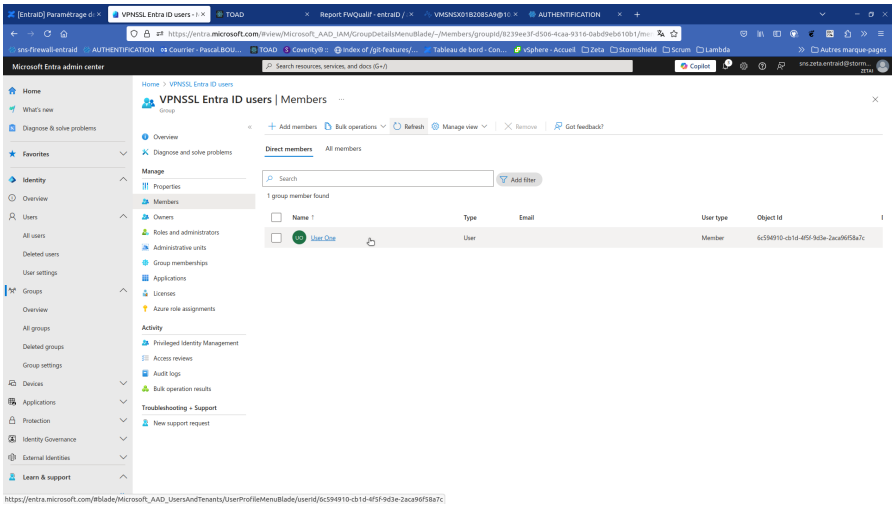
1/ Go to "Groups" and create a security group named 'VPNSSL EntraID Users'

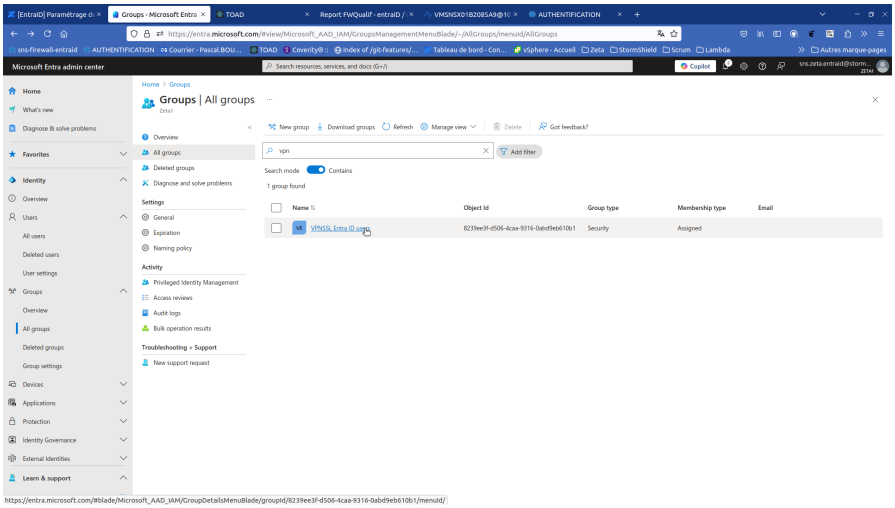


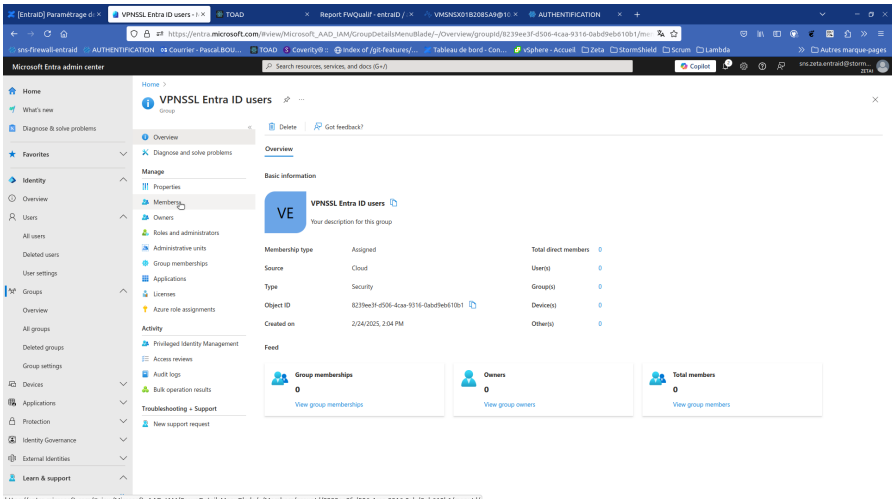


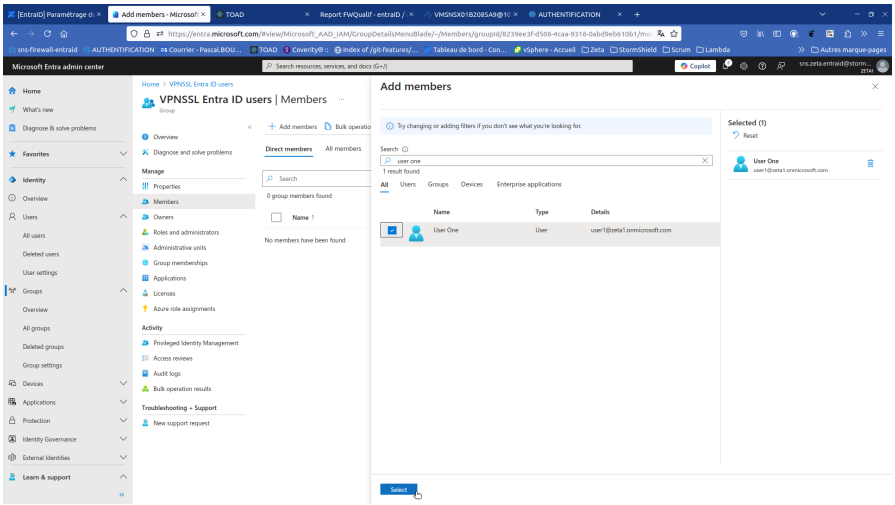


2/ Associate with this group, the users who will be authorized to set up an SSL VPN tunnel (ℹ several methods possible)

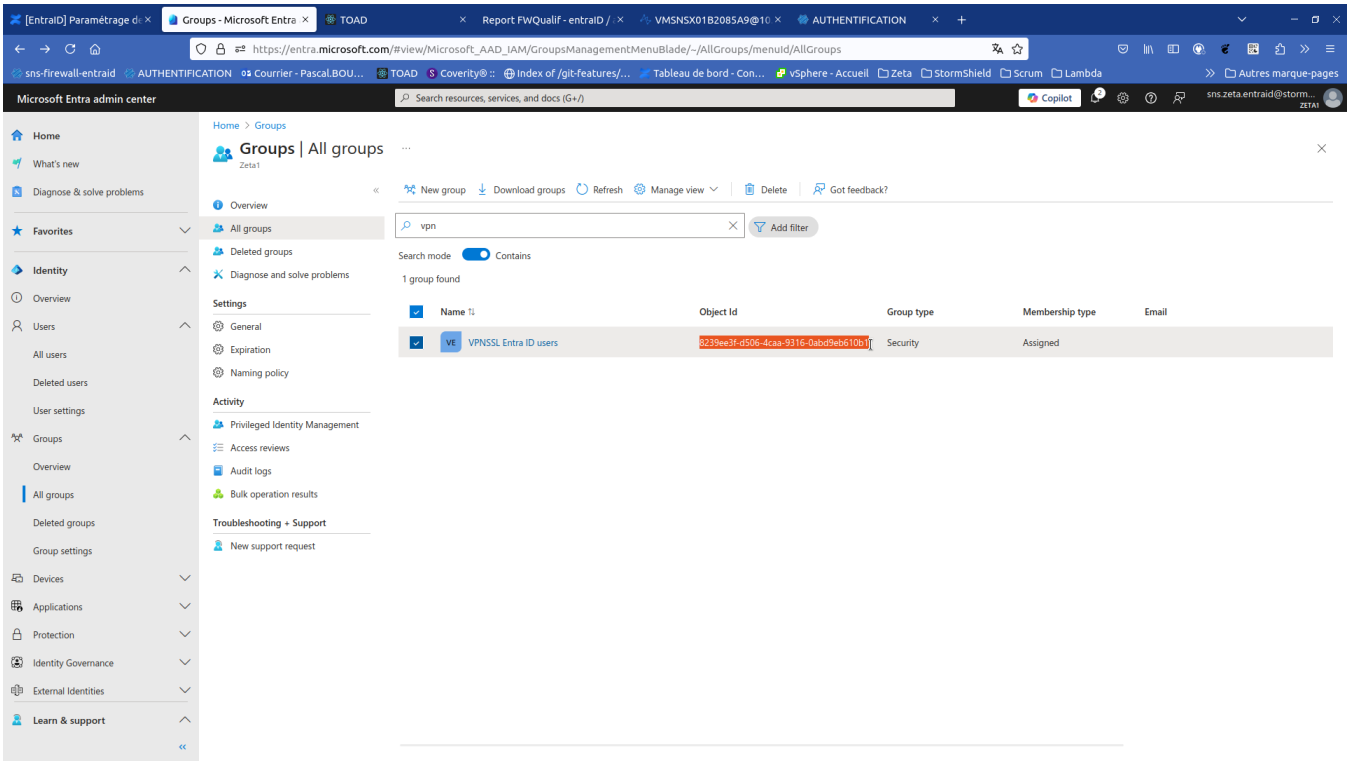

VPNSSL Entra ID users | Members
Group
Home > VPNSSL Entra ID users
Add members
Bulk operations
Refresh
Manage view
Remove
Got feedback?
Direct members
All members
Search
Add filter
1 group member found
Name
Type
Email
User type
Object Id
User One
User
Member
6c594910-cb1d-4f5f-9d3e-2aca96f58a7c
Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Roles and administrators
Administrative units
Group memberships
Applications
Licenses
Azure role assignments
Activity
Privileged Identity Management
Access reviews
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
https://entra.microsoft.com/#blade/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/userId/6c594910-cb1d-4f5f-9d3e-2aca96f58a7c


Groups | All groups
Home > Groups
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
Overview
All groups
Deleted groups
Diagnose and solve problems
Settings
General
Expiration
Naming policy
Activity
Privileged Identity Management
Access reviews
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
https://entra.microsoft.com/#blade/Microsoft_AAD_IAM/GroupDetailsMenuBlade/groupId/8239ee3f-d506-4caa-9316-0abd9eb610b1/menuId/


VPNSSL Entra ID users
Group
Home >
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
0
View group memberships
Owners
0
View group owners
Total members
0
View group members
Diagnose and solve problems
Manage
Properties
Members
Owners
Roles and administrators
Administrative units
Group memberships
Applications
Licenses
Azure role assignments
Activity
Privileged Identity Management
Access reviews
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/GroupDetailsMenuBlade/~/Members/groupId/8239ee3f-d506-4caa-9316-0abd9eb610b1/menuId/

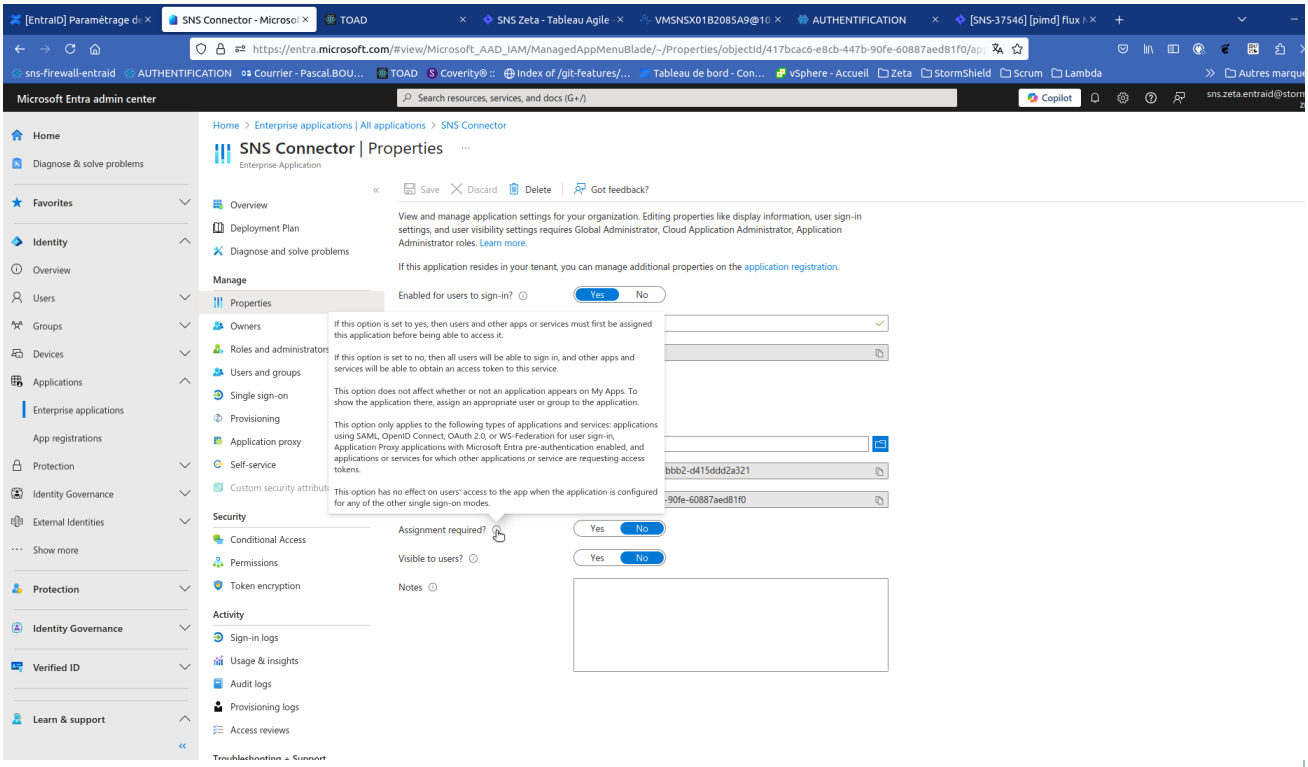


3/ In the "All groups" view, copy the "Object ID" value to enter the group's UID in the SNS configuration.

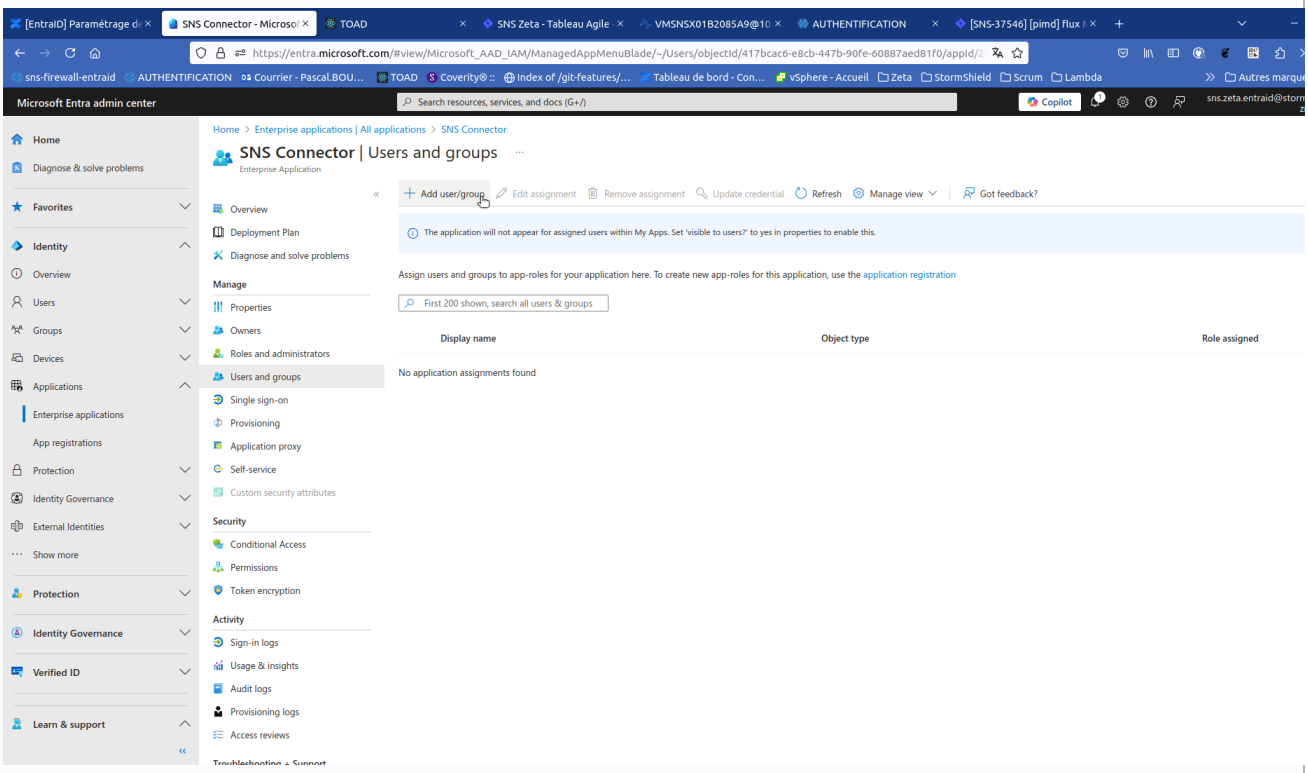


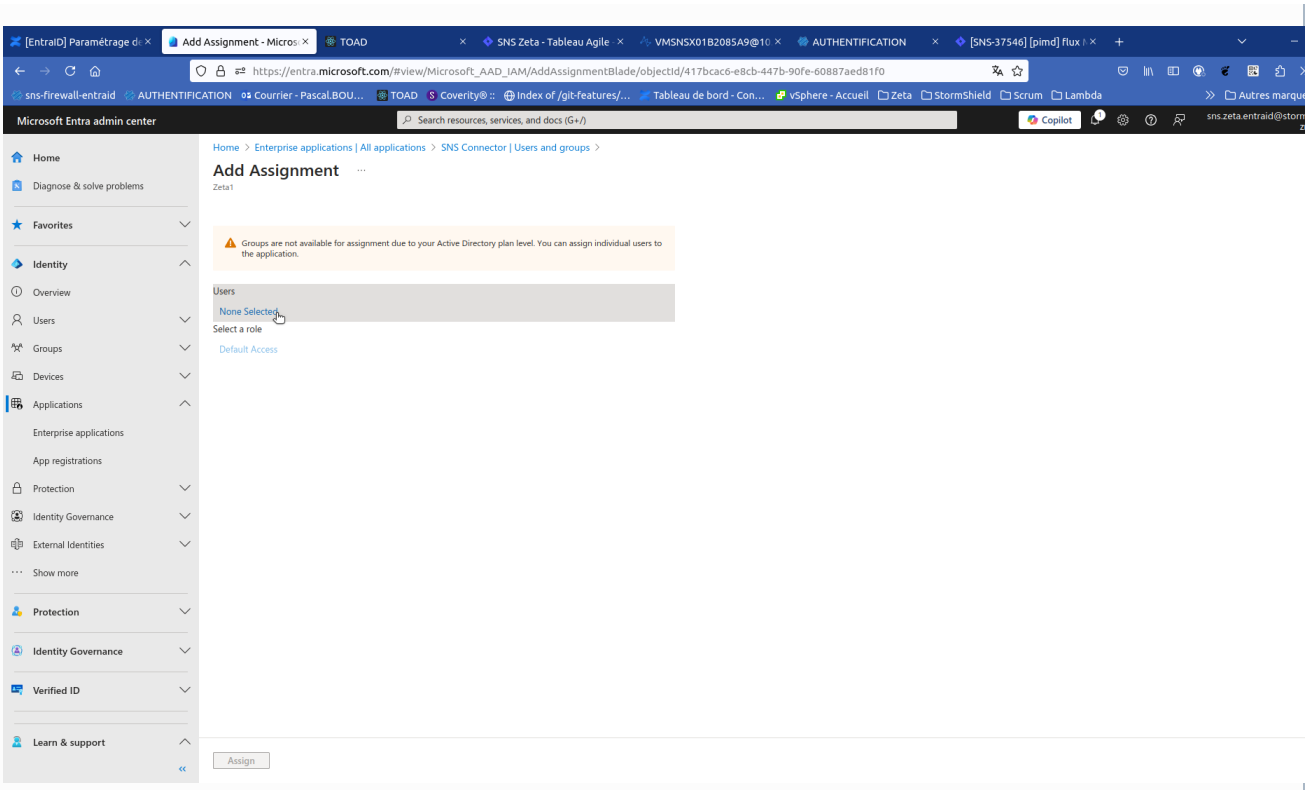
Assignement des utilisateurs à l'application

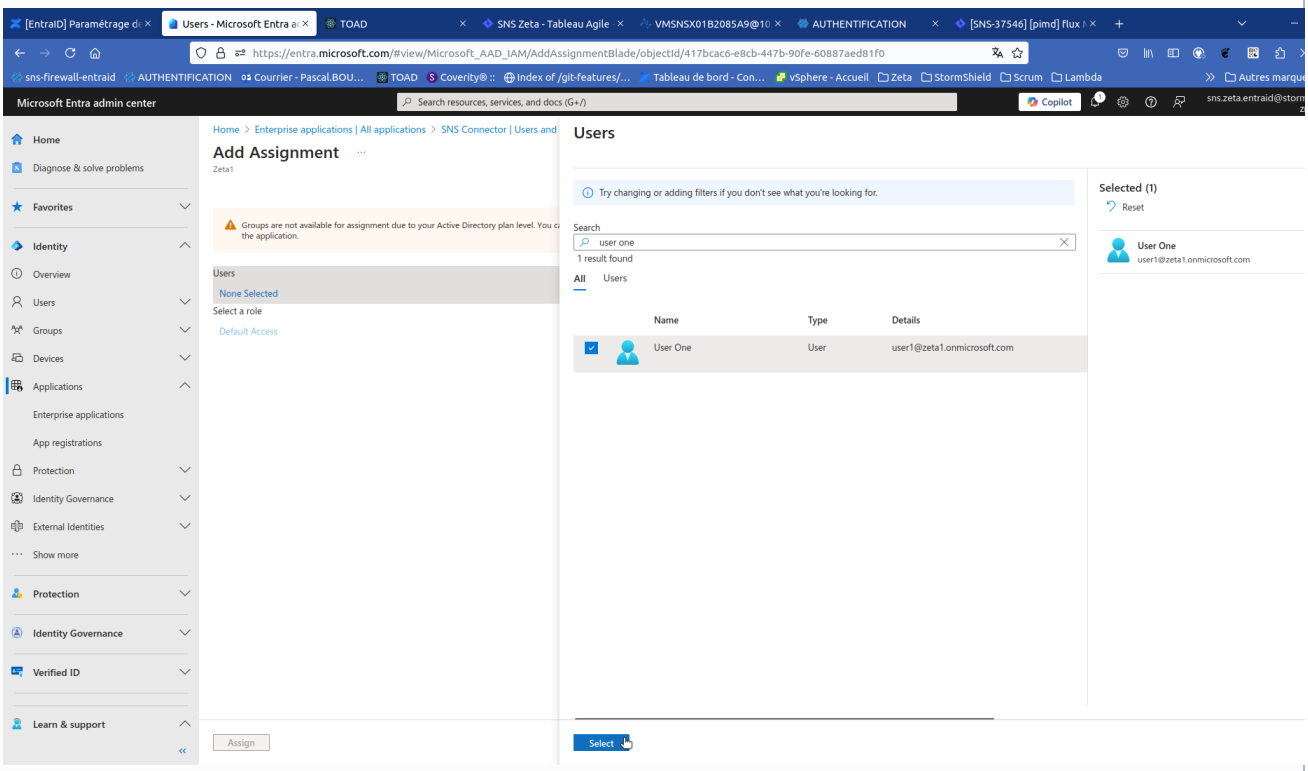
Via **Enterprise applications SNS Connector Properties**, it is possible to allow access to the application to all users of the tenant or to limit its access to a list of users.

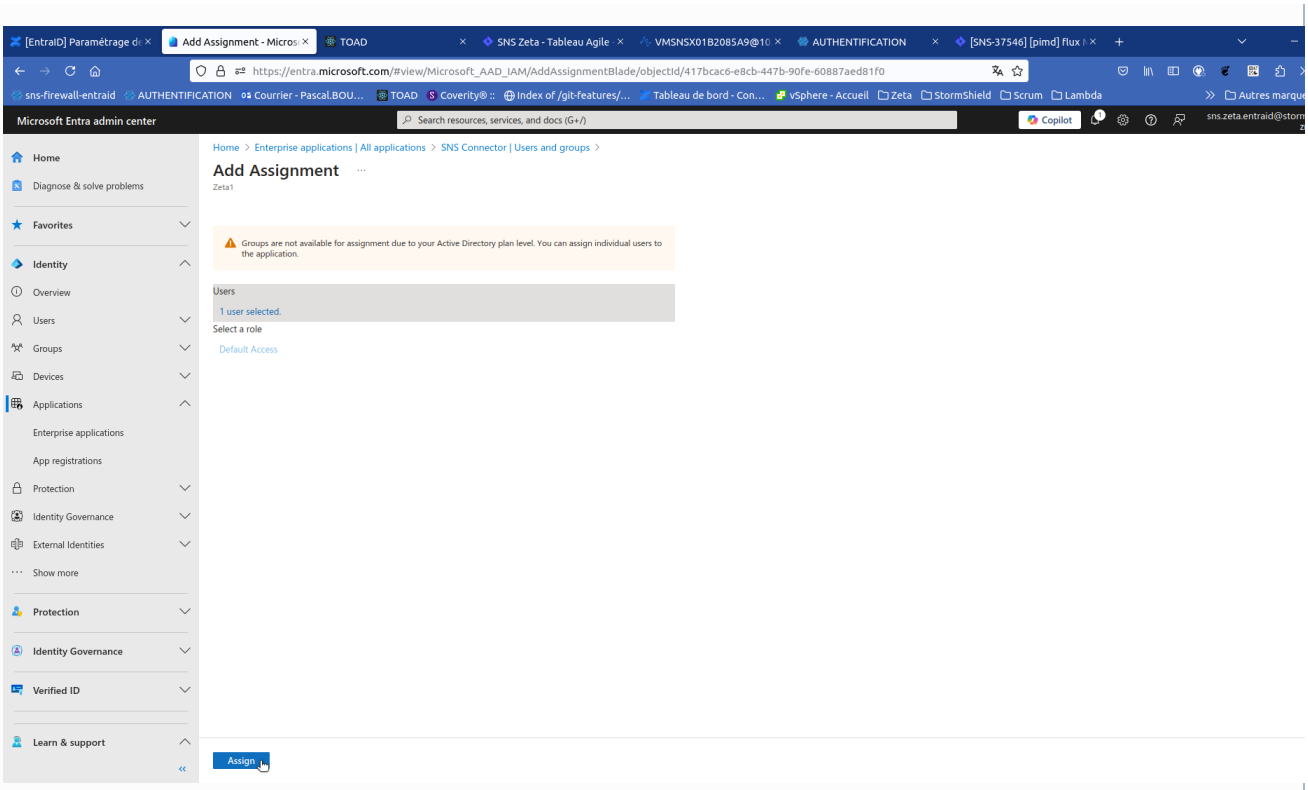


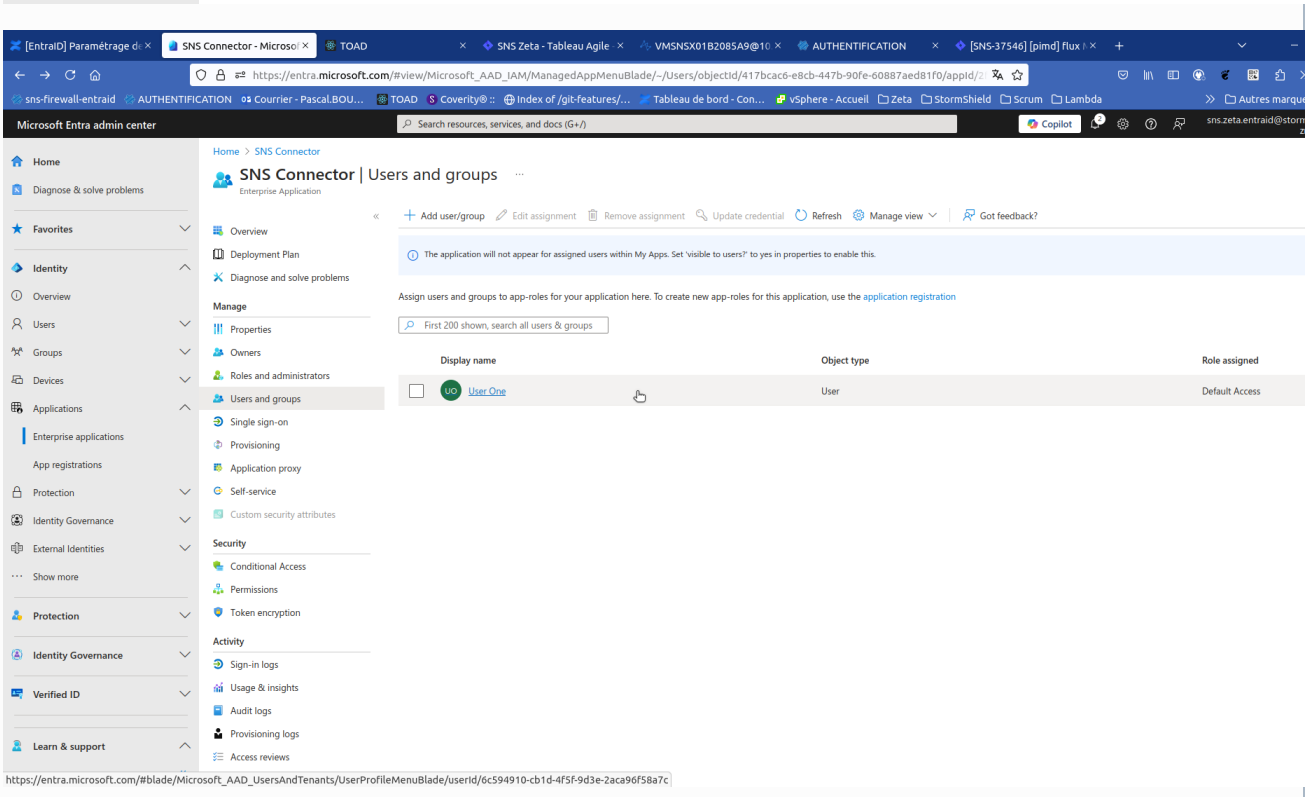
In the case where this option is set to **Yes**, you must assign the users you want to authorize via **Users and groups**




Add Assignment - Micros
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/417bcac6-e8cb-447b-90fe-60887aed81f0
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
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
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


Users - Microsoft Entra a
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/417bcac6-e8cb-447b-90fe-60887aed81f0
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home > Enterprise applications | All applications > SNS Connector | Users and
Add Assignment
Zeta1
Groups are not available for assignment due to your Active Directory plan level. You c
the application.
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
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





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.

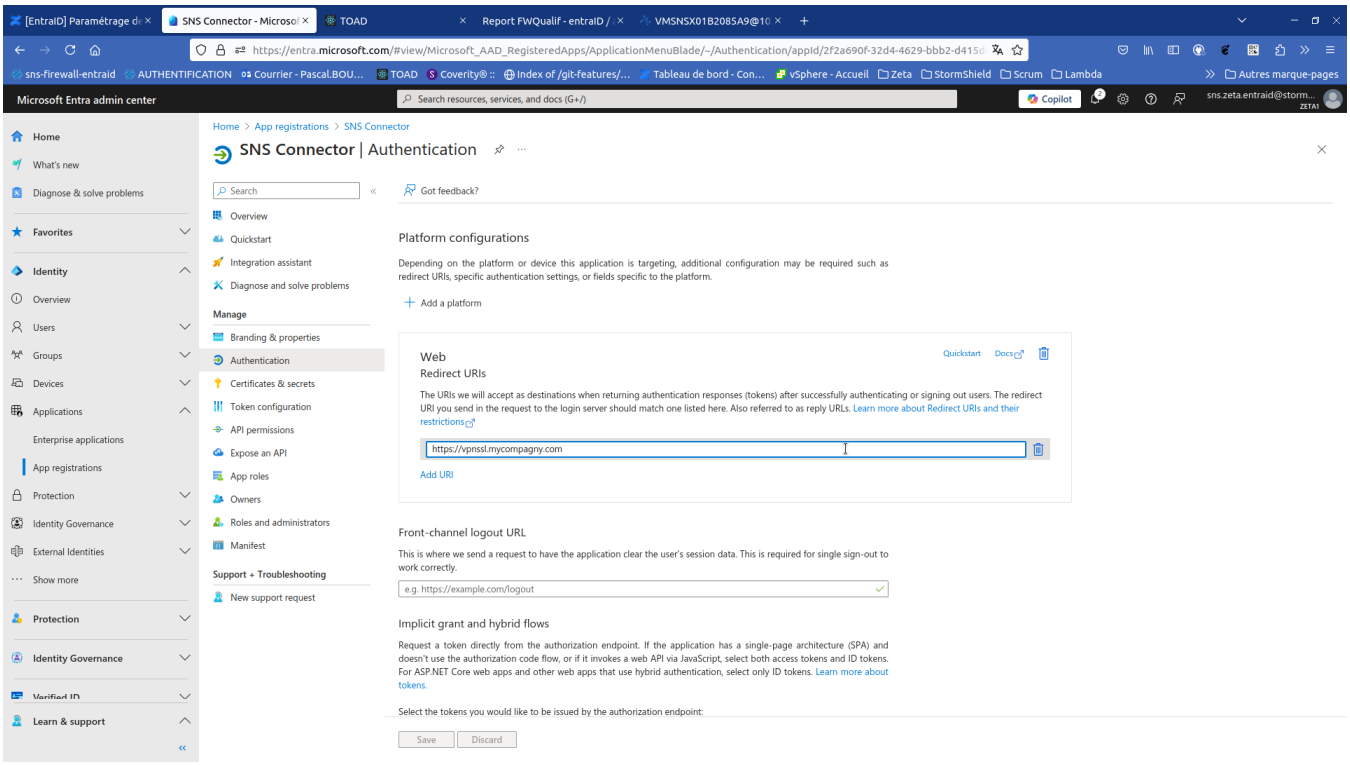
ⓘ The "IssuerID" parameter will be built as: "https://login.microsoftonline.com/$TENANTID/v2.0"

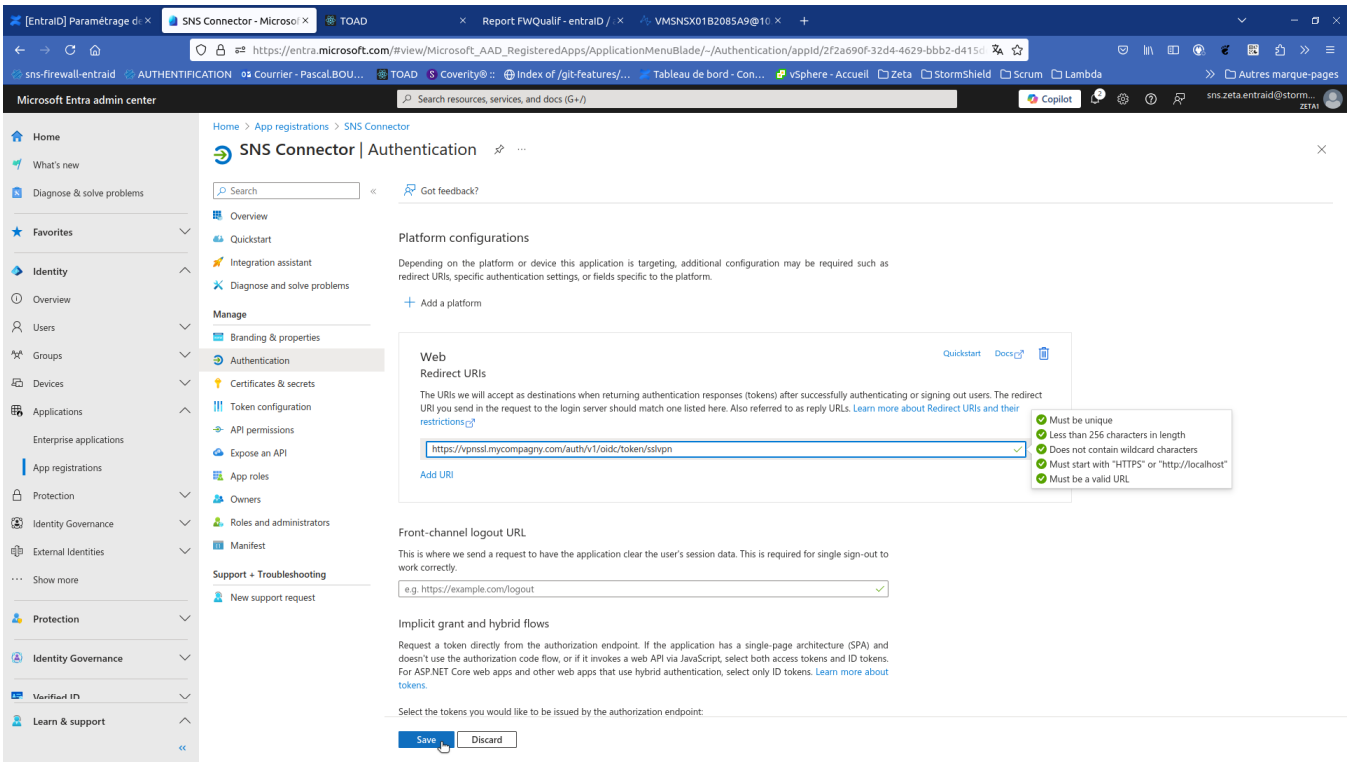
The redirect URLs are built from the Captive Portal configuration (System/Configuration -> General Configuration -> Advanced Configuration -> Captive Portal)

Configuration of Redirect URLs in EntraID

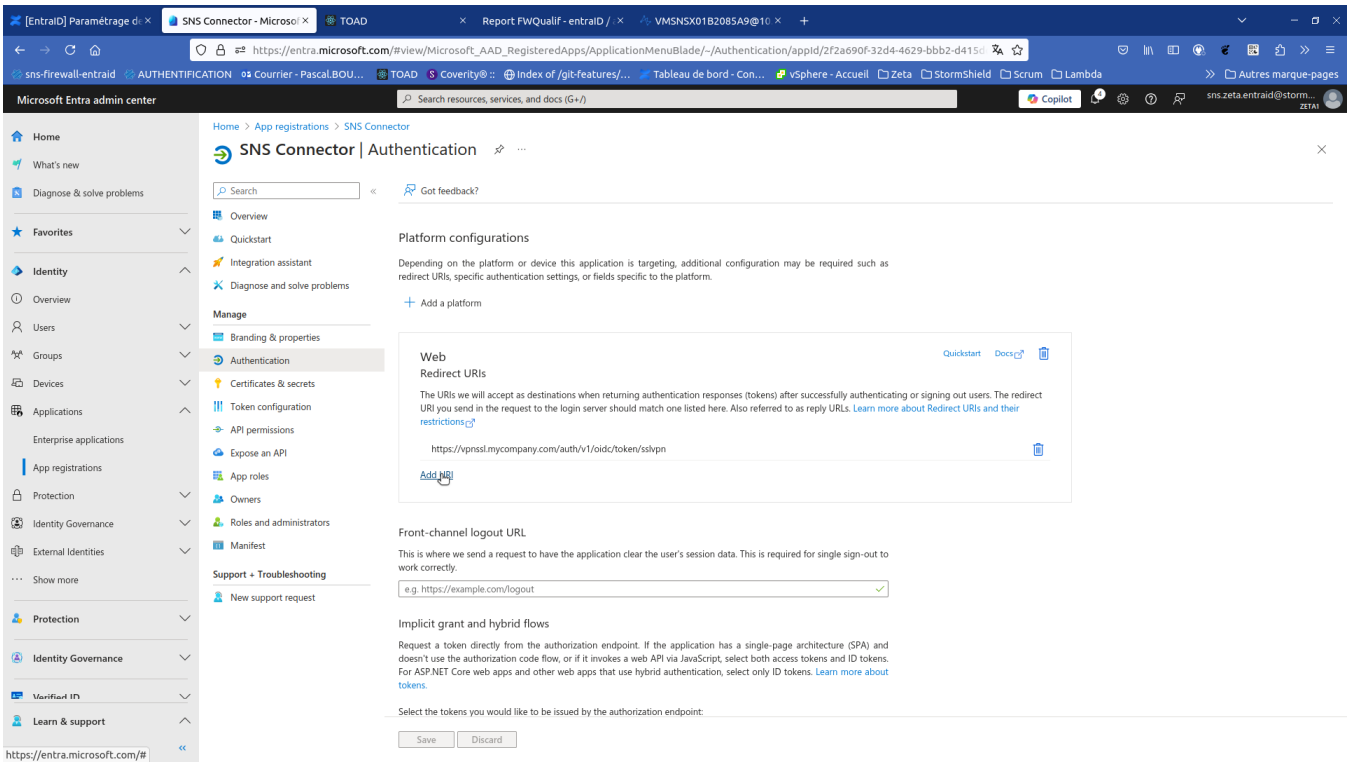
Update the desired redirect URI in the SNS Connector application from the proposed ones

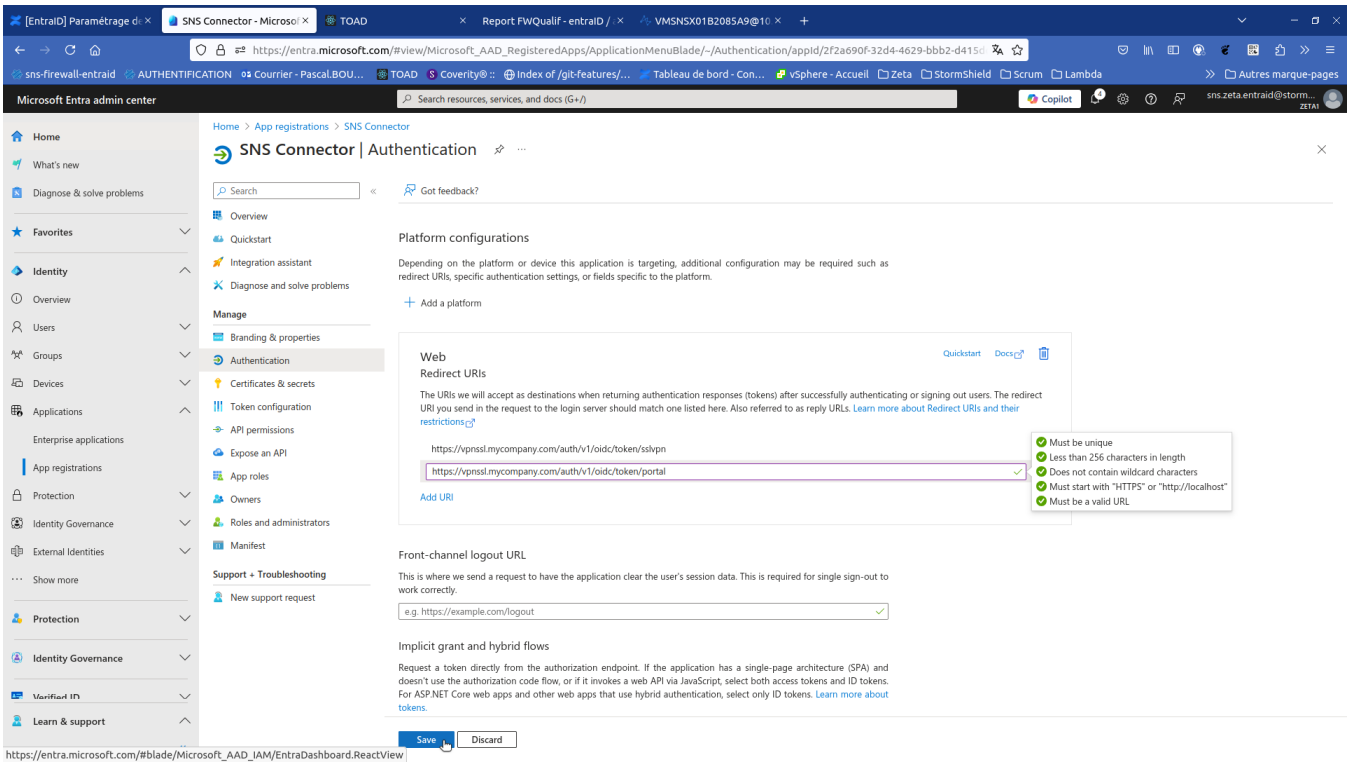
1/ Update the existing redirect URI





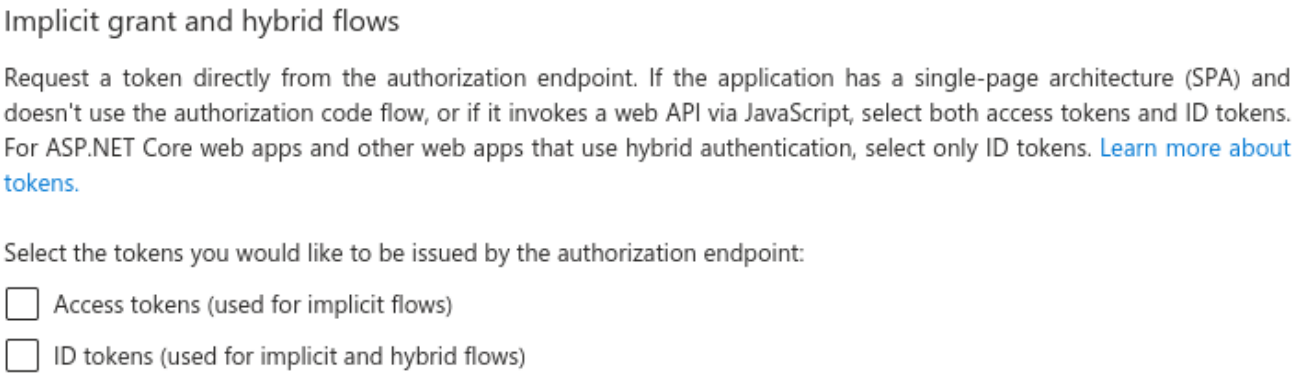
2/ Add if necessary the redirect URI to allow authentication via the SNS captive portal

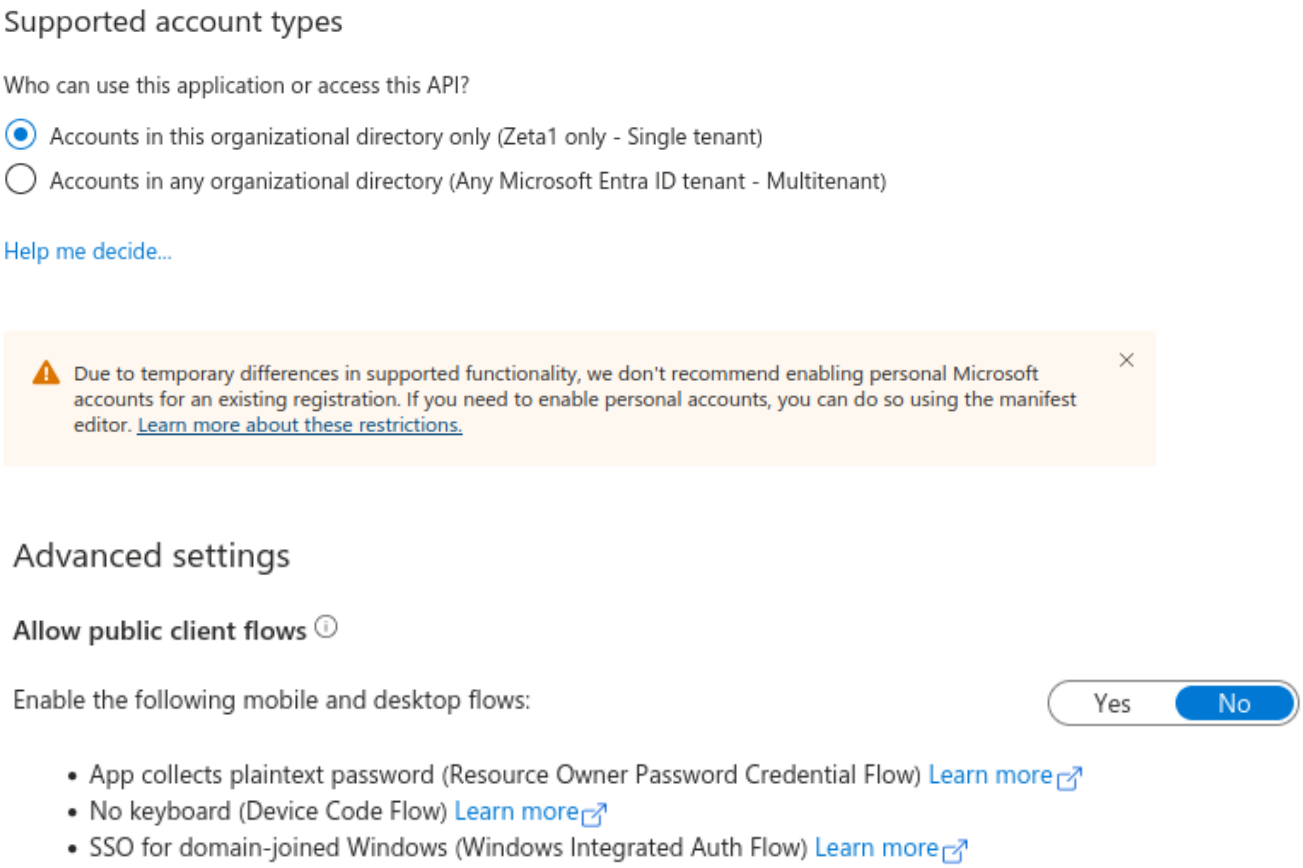




3/ On this same page, take the opportunity to check the following configurations:

- 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**".

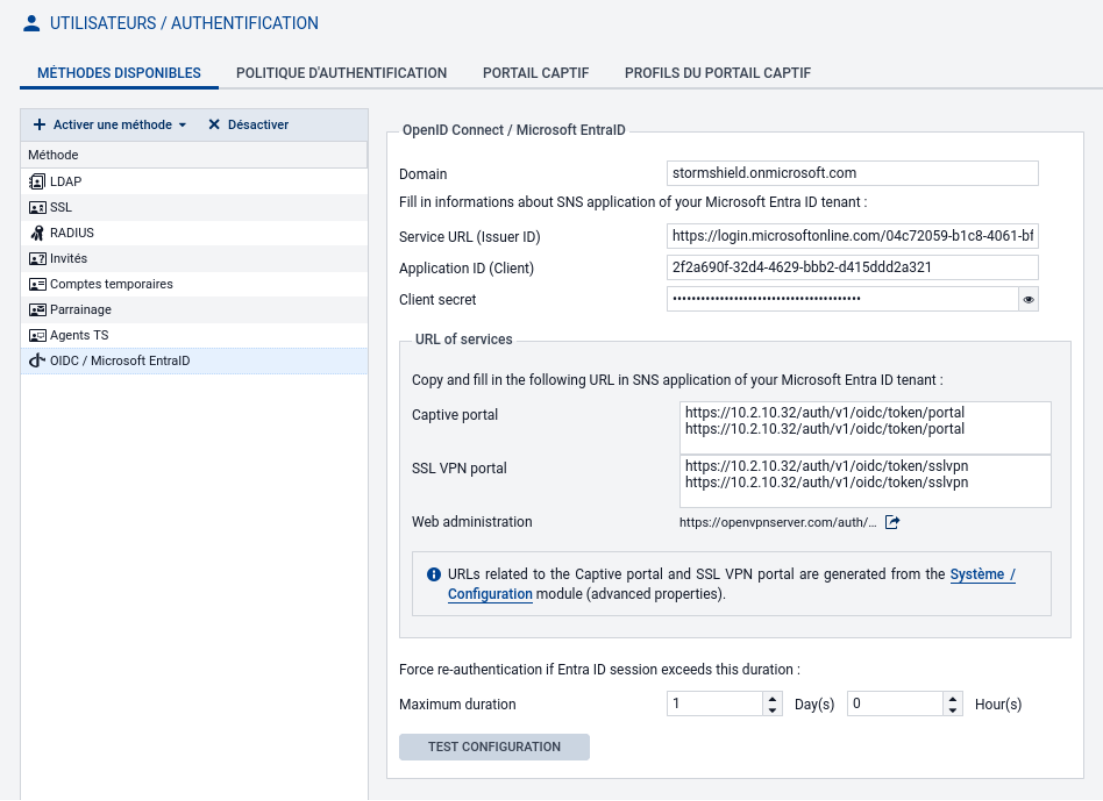




Re-check the SNS configuration

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



Importing EntraID Security Groups

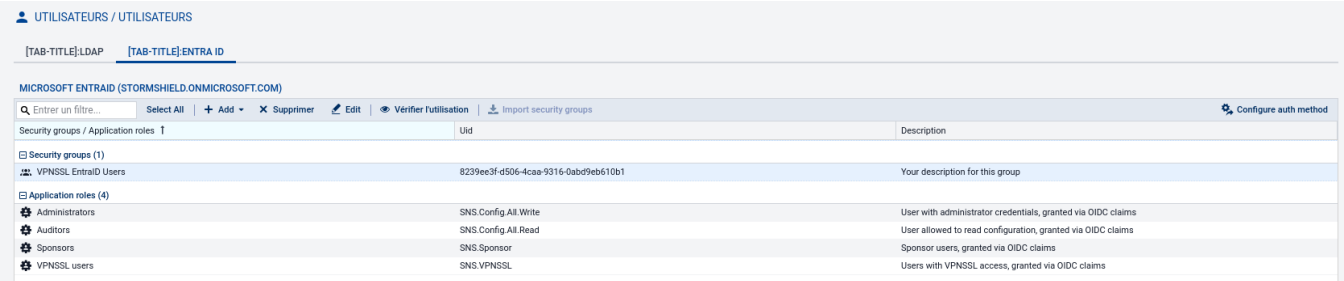
1/ Creation of an OIDC group corresponding to VPNSSL users

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

Add a security group and apply the configuration

Example :

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



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

Creation of an authentication rule

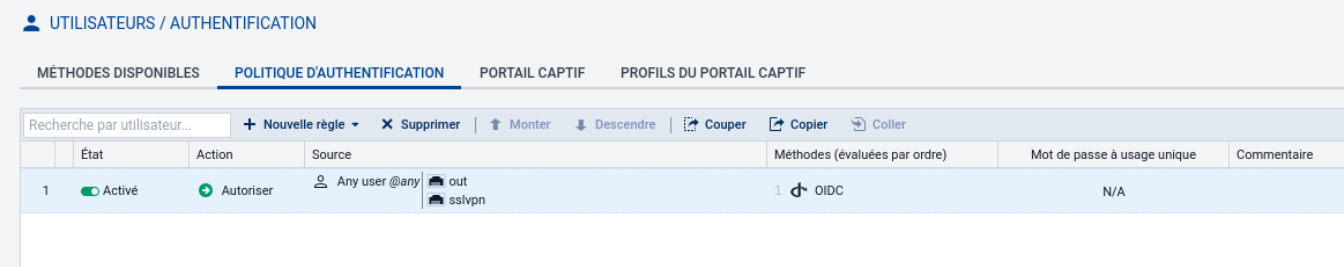
The authentication rule must apply to the "out" interfaces to allow access to the captive portal, but also "sslvpn" to allow the establishment of SSL VPN tunnels for this type of user.

"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

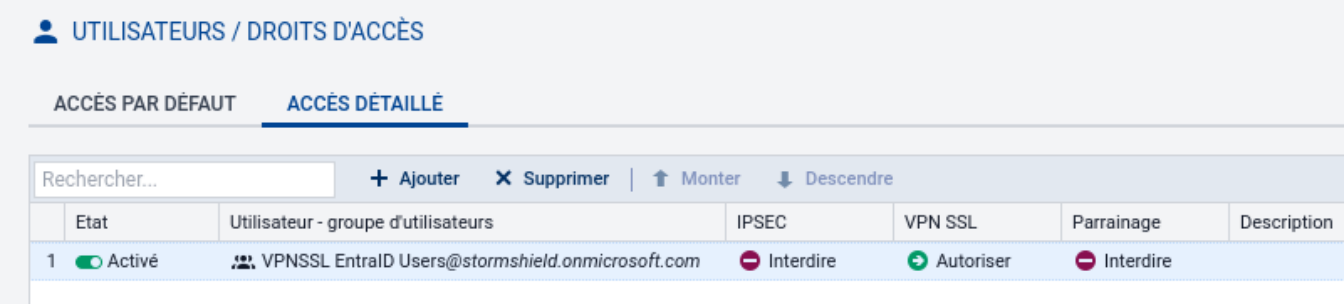


Creation of an access rule

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

Example:

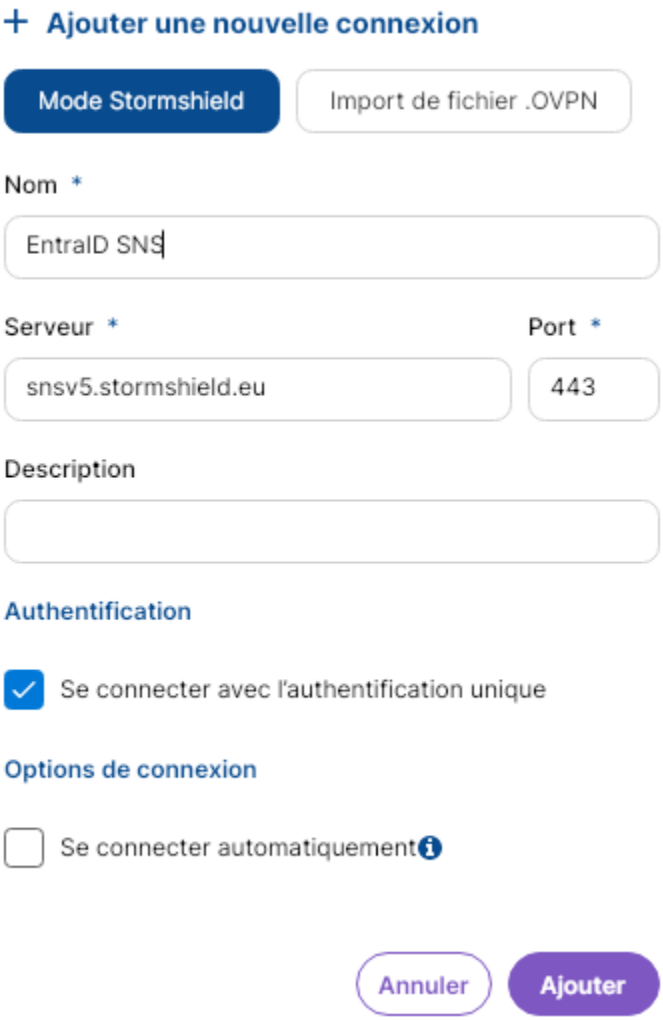
- User= "VPNSSL EntraID Users"
- Domain = stormshield.onmicrosoft.com
- SSL VPN = Allow



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"

> 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 *
EntraID SNS
Serveur *
Port *
snsv5.stormshield.eu
443
Description
Authentification
Se connecter avec l'authentification unique
Options de connexion
Se connecter automatiquement
Annuler
Ajouter