NOTE TECHNIQUE
PRODUCT NAME

CONFIGURER L'AUTHENTIFICATION OIDC / MICROSOFT ENTRA ID

Produits concernés : SNS v5 et supérieures

Dernière mise à jour du document : 19 septembre 2025

Référence : sns-fr-configurer_authentification_OIDC_Microsoft_ENTRA_ID_note_technique

Table des matières

Historique des modifications

Date	Description
19 septembre 2025	Nouveau document

Avant de commencer

A partir de la version 5 de SNS, le firewall offre une intégration transparente et sécurisée avec Microsoft Entra ID via le protocole OpenID Connect (OIDC). Cette fonctionnalité est conçue pour centraliser et optimiser la gestion des accès à votre infrastructure réseau.

En connectant votre Firewall SNS à Microsoft Entra ID, vous pouvez :

- Contrôler de façon centralisée qui a accès à votre VPN SSL directement à partir de Microsoft Entra ID.
- Permettre à vos utilisateurs d'être automatiquement authentifiés sur le firewall SNS (pour le portail captif ou les politiques de filtrage) en utilisant leurs comptes Microsoft Entra ID existants.
- Gérer vos comptes d'administration SNS à partir d'un seul endroit, améliorant ainsi la sécurité et la cohérence de vos politiques d'accès.

L'annuaire regroupant les utilisateurs et les applications accessibles à ces utilisateurs via Microsoft Entra ID est nommé *tenant* dans l'interface d'administration Microsoft Entra ID ainsi que dans la suite de ce document.

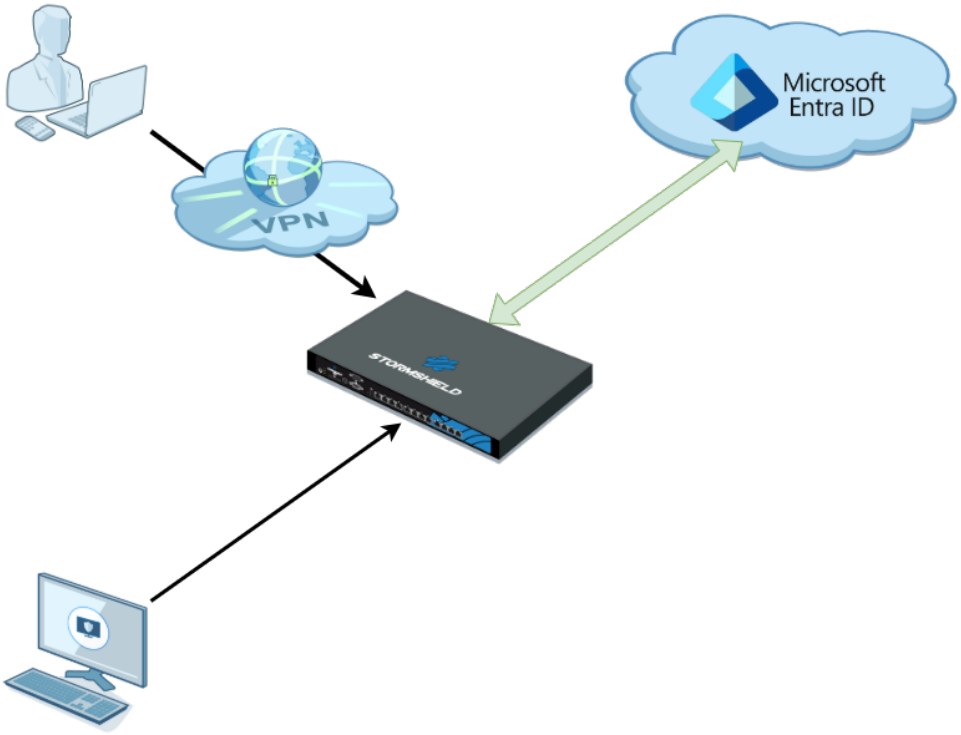
Prérequis

- Un abonnement Microsoft Entra ID comportant le *tenant.*
- Un compte administrateur du *tenant* considéré.
- Un firewall SNS en version 5.0.1 ou supérieure disposant d'un nom de domaine qualifié (FQDN) accessible depuis Internet (exemples : myfirewall.mycompany.com, vpnssl.mycompany.com...).
- L'heure et la date de ce firewall doivent être à jour pour que l'authentification OIDC / Microsoft Entra ID fonctionne.
  Pour garantir un fonctionnement optimal, il est donc fortement recommandé d'activer la synchronisation de temps via NTP sur le firewall.
- Un client Stormshield VPN SSL en version 4.1 ou supérieure si les utilisateurs authentifiés via OIDC / Microsoft Entra ID sont autorisés à établir des tunnels VPN SSL avec le firewall.

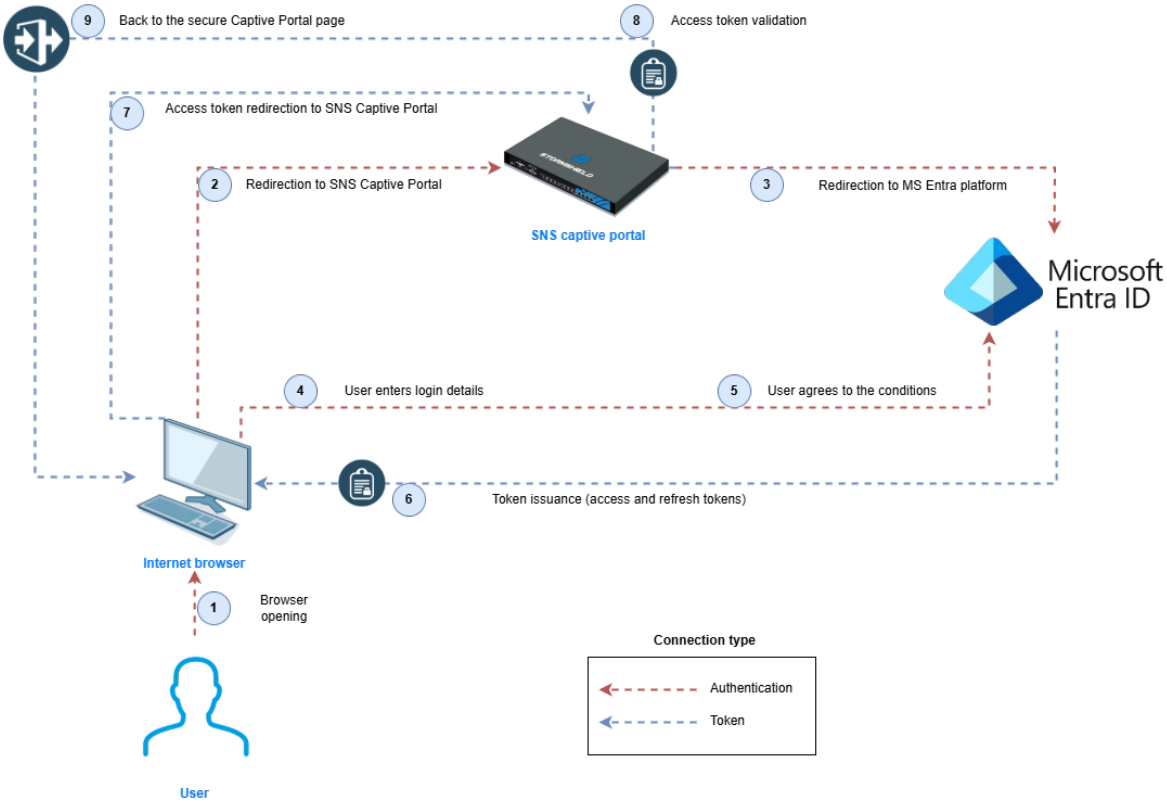
Authentification SNS / OIDC Microsoft Entra ID

Ce document présente les configurations SNS et Microsoft Entra ID nécessaires pour autoriser :

- Des utilisateurs distants à établir un tunnel VPN SSL en s'authentifiant via Microsoft Entra ID.
- Des administrateurs à se connecter à l'interface Web d'administration du firewall en s'authentifiant via Microsoft Entra ID.



Comprendre le fonctionnement de l'authentification OIDC / Microsoft Entra ID



Ajouter l'application SNS dans votre *tenant* Microsoft Entra ID

Connectez-vous au centre d'administration Microsoft Entra ID puis accédez au menu **Identité** > **Applications** > **Inscriptions d'applications**.

Créer l'application SNS au sein du tenant Microsoft Entra ID

1. Accédez au menu **Identité** > **Applications** > **Inscriptions d'applications**.
2. Cliquez sur **Nouvelle inscription**.
3. Nommez l'application (exemple : SNS Connector).
4. Dans la rubrique **Types de comptes pris en charge**, sélectionnez impérativement **Comptes dans cet annuaire d'organisation uniquement**.
5. Pour l'URI de redirection, sélectionnez le type **Web** ainsi qu'une première URI de redirection sous l'une des formes suivantes :
   - VPN SSL : https://<firewall_fqdn>/auth/v1/oidc/token/sslvpn
   - Interface Web d'administration : https://<firewall_fqdn>/auth/v1/oidc/token/webadmin

   > **NOTE**
   > Vous devez saisir une première URI de redirection pour toute nouvelle application.
6. Cliquez sur **S'inscrire**.

Ajouter des URI de redirection supplémentaires à votre application (optionnel)

Si vous souhaitez ajouter à votre application d'autres URI de redirection pour accéder à des services supplémentaires :

1. Dans le cadre **Bases**, cliquez sur le lien vers les **URI de redirection** de type **Web**.
2. Dans le cadre **Web**, saisissez l'URI sous l'une des formes suivantes :
   - VPN SSL : https://<firewall_fqdn>/auth/v1/oidc/token/sslvpn
   - Interface Web d'administration : https://<firewall_fqdn>/auth/v1/oidc/token/webadmin
3. Cliquez sur **Ajouter une URI** pour définir une URI supplémentaire.
4. Cliquez sur **Enregistrer** pour valider votre configuration.

Créer un secret client pour l'application

Cette opération consiste à générer un secret qui sera renseigné sur le firewall SNS pour l'autoriser à accéder à l'application.

1. Dans le menu **Certificats & secrets** > onglet **Secrets client**, cliquez sur **Nouveau secret client**.
2. Saisissez une description et sélectionnez une **Date d'expiration** du secret.
   La valeur proposée par défaut est de 6 mois (180 jours).
3. Validez.
   Le secret apparaît dans la liste.

IMPORTANT
Cliquez sur l'icône **Copier dans le Presse-papier** à côté de la valeur du secret et conservez cette dernière en attendant de l'ajouter dans la configuration Entra ID du firewall.
En effet, ce secret n'est plus affichable dès lors que vous quittez ce module Microsoft Entra ID.
Si vous avez oublié de copier le secret avant de quitter ce module, vous devrez en recréer un nouveau.

Créer un jeton d'application contenant les revendications nécessaires

Lorsque l'utilisateur s'authentifie sur Microsoft Entra ID, le firewall reçoit un jeton comprenant le nom de l'utilisateur, les groupes auxquels il appartient ainsi que les rôles applicatifs qui lui ont été attribués (optionnel) afin de déterminer les autorisations des utilisateurs.

1. Dans le menu **Configuration du jeton**, cliquez sur **Ajouter une revendication facultative**.
2. Sélectionnez le jeton **ID**.
   La liste des revendications apparaît.
3. Cochez la case **preferred_username**.
   Cela permet d'inclure dans le jeton les informations d'identité (Nom - Prénom) de l'utilisateur.
4. Cliquez sur **Ajouter**.
5. Cliquez sur **Ajouter une revendication de groupe**.
6. Cochez la case **Groupes de sécurité**.
7. Vérifiez que l'ID associée à ce jeton est positionnée sur **ID de groupe**.
   Cela permet d'inclure dans le jeton la liste des groupes auxquels appartient l'utilisateur.
   Notez que pour les licences gratuites, cette option se limite aux 200 premiers groupes auxquels l'utilisateur appartient.

NOTE
Il est possible de limiter le nombre de groupes à inclure dans le jeton aux groupes concernés par l'application en cochant l'option **Groupes affectés à l'application (recommandé pour les grandes entreprises pour ne pas dépasser la limite du nombre de groupes qu'un jeton peut émettre)**. Cette option n'est présente que pour une licence payante de type P1.

Accorder à l'application un consentement d'administrateur pour l'ensemble du *tenant*

Lorsqu'un utilisateur se connecte pour la première fois à Microsoft Entra ID, il lui est demandé de consentir à partager les informations de type <preferred_username> à l'application.
L'administrateur du *tenant* peut donner un consentement général pour l'ensemble des utilisateurs de ce *tenant*.

1. Dans le menu **Sécurité** > **Autorisations**, cliquez sur **Accorder un consentement d'administrateur pour (Grant admin consent for)** <nom_de_l_application>.
   Une fenêtre demandant d'accepter les autorisations est affichée.
2. Cliquez sur **Accepter**.

Créer des rôles applicatifs et les attribuer aux utilisateurs du *tenant* Microsoft Entra ID (optionnel)

Il est possible de définir des rôles applicatifs pour accorder des droits d'accès spécifiques aux utilisateurs. Par exemple : autoriser un utilisateur à accéder à la configuration du firewall en lecture seule ou en lecture / écriture, autoriser un utilisateur à parrainer (plus d'informations sur la fonctionnalité de parrainage dans le Manuel Utilisateur SNS), accorder à un utilisateur le droit d'établir un tunnel VPN SSL ...

Quatre rôles applicatifs existent par défaut dans le firewall :

- **Administrators** : accès en lecture / écriture à l'interface Web d'administration du firewall.
- **Auditors** : accès en lecture seule à l'interface Web d'administration du firewall.
- **Sponsors** : droit à parrainer des utilisateurs temporaires.
- **VPNSSL users** : droit à établir un tunnel VPN SSL avec le firewall.

IMPORTANT
Si vous choisissez d'utiliser des rôles applicatifs pour les autorisations, ils doivent disposer d'un UID identique dans le *tenant* Microsoft Entra ID et sur le firewall SNS utilisant l'authentification OIDC / Microsoft Entra ID (exemple : SNS.Config.All.Write ou SNS.VPNSSL).
La configuration des rôles applicatifs sur le firewall est abordée dans la section Configurer le firewall pour l'authentification OIDC / Microsoft Entra ID.

1. Précisez le **Nom d'affichage du rôle**.
2. Cochez la case **Utilisateurs/Groupes**.
3. Dans le champ **Valeur**, indiquez les droits attribués au travers de ce rôle sous la forme d'une suite de droits SNS (exemple : SNS.Config.All.Write ou SNS.VPNSSL).
4. Cochez la case **Voulez-vous activer ce rôle d'application ?** si vous souhaitez pouvoir utiliser ce rôle dans votre application Microsoft Entra ID.
5. Répétez les étapes 2 à 7 pour créer l'ensemble des rôles souhaités.

Ajouter des utilisateurs / groupes dans votre *tenant* Microsoft Entra ID

Connectez-vous au centre d'administration Microsoft Entra ID pour accéder à votre *tenant*.

Ajouter un utilisateur à votre *tenant*.

1. Dans le menu **Identité** > **Utilisateurs** > **Tous les utilisateurs**, cliquez sur **Nouvel(le) Utilisateur(-trice)** puis sur **Créer un utilisateur**.
2. Dans le champ **Nom d'utilisateur principal**, indiquez le nom d'utilisateur souhaité (exemple : john.doe).
   Le suffixe correspondant au *tenant* est ajouté automatiquement (exemple : @snsdoc.onmicrosoft.com).
   Le nom d'utilisateur complet sera l'identifiant à utiliser pour se connecter au *tenant* (exemple : john.doe@snsdoc.onmicrosoft.com).
3. Précisez le **Nom d'affichage** de l'utilisateur (exemple : John Doe).
4. Vous pouvez indiquer manuellement le **Mot de passe** de cet utilisateur ou lui **Générer automatiquement le mot de passe** en cochant la case du même nom.
5. Cliquez sur le bouton **Vérifier + Créer** puis validez en cliquant sur **Créer**.
   L'utilisateur est créé.
6. Répétez les étapes 2 à 6 pour créer tous les utilisateurs du *tenant*.

Attribuer des droits spécifiques sur le *tenant* à un utilisateur

1. Dans le menu **Identité** > **Utilisateurs** > **Tous les utilisateurs**, cliquez sur le nom de l'utilisateur auquel vous souhaitez ajouter des droits.
2. Dans le menu de gauche, cliquez sur **Rôles affectés**.
3. Cliquez sur **Ajouter des affectations** et sélectionnez les droits souhaités (exemple : Administrateur général).
4. Cliquez sur **Ajouter**.

Attribuer des rôles aux utilisateurs ou aux groupes dans l'application (optionnel)

> **NOTE**
> L'attribution de rôles à des groupes nécessite un abonnement Microsoft Entra ID payant.
> Les abonnements gratuits n'autorisent l'assignation de rôles qu'aux utilisateurs.

1. Dans le menu **Identité** > **Applications d'entreprise**, cliquez sur le nom de votre application (exemple : SNS Connector).
2. Allez dans le menu **Gérer** > **Utilisateurs et groupes**.
3. Cliquez sur **Add user/group**.
4. Sous **Utilisateurs**, cliquez sur **Aucune sélection**.
5. Sélectionnez les utilisateurs auxquels assigner le rôle.
6. Cliquez sur **Sélectionner**.
7. Sous **Sélectionner un rôle**, cliquez sur **Aucune sélection**.

8. Sélectionnez le rôle souhaité puis cliquez sur **Sélectionner**.
9. Cliquez sur **Attribuer**.
   Les utilisateurs et leur rôle sont affichés dans la grille.
10. Répétez les étapes 2 à 7 pour réaliser l'ensemble des attributions de rôles.

Créer un groupe et lui affecter des membres

1. Dans le menu **Identité** > **Groupes** > **Vue d'ensemble**, cliquez sur **Nouveau groupe**.
2. Pour le **Type de groupe**, sélectionnez la valeur **Sécurité**.
3. Précisez le **Nom** du groupe (exemple : SNS Authentication).
   Vous pouvez ajouter une **Description du groupe** si vous le souhaitez.
4. Cliquez sur **Aucun membre sélectionné** et sélectionner les utilisateurs à ajouter à ce groupe (exemple : John Doe).
5. Validez en cliquant sur **Sélectionner**.
6. Cliquez sur **Créer**.

Télécharger les groupes d'utilisateurs en vue de leur import dans le firewall SNS

1. Dans le menu **Identité** > **Groupes** > **Tous les groupes**, cochez les groupes à exporter puis cliquez sur **Télécharger des groupes**.
2. Modifiez le nom du fichier CSV proposé si vous le souhaitez puis cliquez sur **Démarrer le téléchargement.**
   La création du fichier CSV est lancée.
3. Lorsque le fichier CSV est prêt, cliquez sur le lien **Le fichier est prêt ! Cliquez ici pour télécharger** et enregistrez le fichier CSV sur votre poste de travail.

Récupérer les informations Microsoft Entra ID nécessaires au paramétrage du firewall

Rendez-vous dans votre centre d'administration Microsoft Entra ID pour récupérer les informations suivantes. Elles sont nécessaires pour paramétrer la méthode OIDC / Microsoft Entra ID sur le firewall SNS.

Récupérer le nom du domaine et l'ID du tenant

1. Allez dans le menu **Identité** > **Vue d'ensemble**.
2. Récupérez la valeur du champ **Domaine principal**.
3. Récupérez la valeur du champ **ID de tenant**.

Récupérer l'ID d'application (client)

1. Allez dans le menu **Identité** > **Applications > Inscriptions d'applications** > onglet **Toutes les applications**.
2. Cliquez sur le nom de votre application SNS (exemple : SNS Connector).
3. Récupérez la valeur du champ **ID d'application (client)**.

Configurer le firewall pour l'authentification OIDC / Microsoft Entra ID

Connectez-vous à l'interface Web d'administration du firewall.

Définir le FQDN du firewall pour l'accès au portail captif

Les navigateurs des postes clients doivent être capables de résoudre ce FQDN.

Dans le module **Système** > **Configuration** > onglet **Configuration générale** > cadre **Portail captif** :

1. Pour le champ **Redirection vers le portail captif**, choisissez la valeur **Préciser un nom de domaine (FQDN)**.
2. Dans le champ **Nom de domaine (FQDN)**, renseignez le nom complet du firewall (exemple : documentation-firewall.stormshield.eu).

> **IMPORTANT**
> Ce FQDN doit être identique à celui utilisé lors de la déclaration des URI dans l'application Stormshield définie dans le *tenant* Microsoft Entra ID.

Créer une identité serveur basée sur ce FQDN

Le certificat de cette identité serveur est destiné à être utilisé par le portail captif du firewall.

> **NOTE**
> Dans le cas des accès VPN SSL, il est préférable que l'identité du portail captif soit issue d'une CA publique puisque celle-ci est déjà intégrée aux navigateurs.

Dans le module **Objets** > **Certificats et PKI** :

1. Cliquez sur **Ajouter** puis sélectionnez **Identité serveur**.
2. Dans le champ **Nom de domaine qualifié (FQDN)**, indiquez le FQDN précisé lors de l'étape Définir le FQDN du firewall pour l'accès au portail captif (exemple : documentation-firewall.stormshield.eu).
3. L'identifiant proposé par défaut pour cette identité correspond au FQDN défini à l'étape 2. Vous pouvez le modifier.
4. Cliquez sur **Suivant**.
5. Sélectionnez l'**Autorité parente** devant signer cette identité, et renseignez le mot de passe de cette CA.
   Cette identité doit être connue des navigateurs procédant à l'authentification.
6. Cliquez sur **Suivant**.
7. Modifiez si vous le souhaitez les champs **Validité (jours)**, **Type de clé** et **Taille de clé (bits)**.
   Les valeurs proposées par défaut sont celles liées à la CA parente.
8. Cliquez sur **Suivant**.
9. Vous pouvez ajouter des alias à cette identité.
10. Cliquez sur **Suivant**.

Un résumé des caractéristiques de cette identité vous est proposé.

11. Validez ces caractéristiques en cliquant sur **Terminer**.

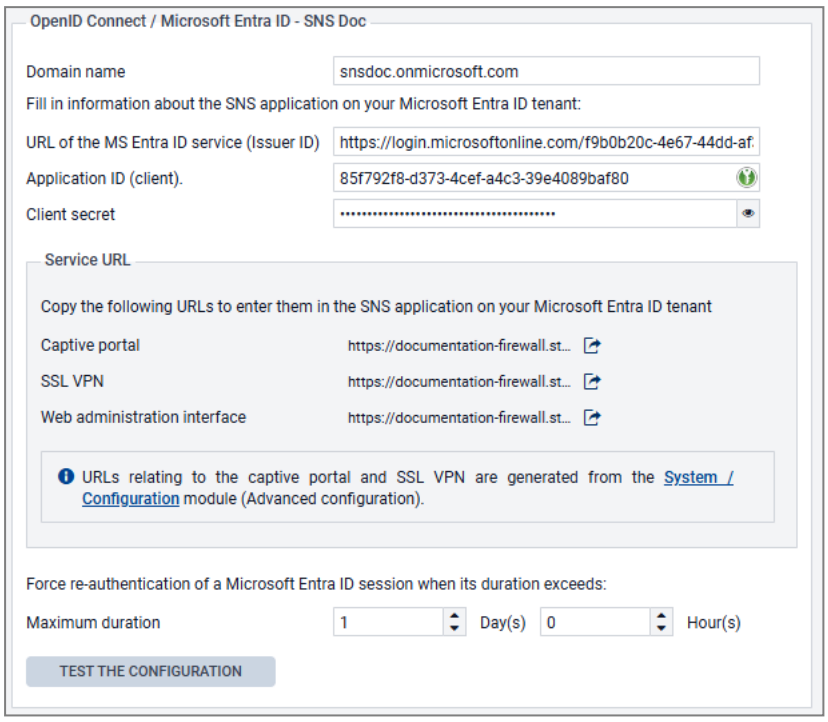
Activer la méthode d'authentification OIDC / Microsoft Entra ID

Dans le module **Utilisateurs** > **Authentification** > onglet **Méthodes disponibles** :

1. Cliquez sur **Activer une méthode**.
2. Sélectionnez **OIDC / Microsoft Entra ID**.
   Un assistant de configuration se lance automatiquement.
3. **Nom de domaine** : indiquez le nom de domaine principal récupéré dans votre centre d'administration Microsoft Entra ID (exemple : snsdoc.onmicrosoft.com).
4. **ID du tenant** : indiquez dans ce champ l'identifiant récupéré dans votre centre d'administration Microsoft Entra ID.
5. **ID d'application (client)** : indiquez dans ce champ la valeur récupérée dans votre centre d'administration Microsoft Entra ID.
6. **Secret client** : indiquez dans ce champ la valeur récupérée et sauvegardée lors de l'étape Créer un secret pour l'application de la création de l'application SNS dans votre tenant Microsoft Entra ID. Si vous n'aviez pas sauvegardé cette valeur, vous devez supprimer le **Secret client** précédemment créé pour votre application et en générer un nouveau en suivant la procédure décrite dans cette étape.
7. Vous pouvez modifier, si vous le souhaitez, la **Durée d'authentification**. Il s'agit de la durée pendant laquelle un utilisateur Microsoft Entra ID authentifié n'aura pas besoin de ressaisir ses informations de connexion. Cette durée est positionnée par défaut sur 1 jour.
8. Cliquez sur **Suivant**.
   L'assistant propose les URL correspondant au service de portail captif, au service VPN SSL et à l'accès à l'interface Web d'administration du firewall. Elles peuvent être copiées directement depuis cet assistant afin de les renseigner comme URL de redirection dans votre centre d'administration Microsoft Entra ID si nécessaire.
   Elles sont également disponibles dans le panneau d'édition de la méthode OIDC / Microsoft Entra ID.
9. Si vous ne souhaitez pas importer les groupes d'utilisateurs dans l'étape suivante de l'assistant, cochez la case **Passer l'import de groupes** et allez directement à l'étape 15 de cette procédure.
10. Cliquez sur **Suivant**.
11. Sélectionnez le fichier CSV contenant les groupes de votre *tenant* Microsoft Entra ID, téléchargé lors de l'étape Télécharger les groupes d'utilisateurs en vue de leur import dans le firewall SNS puis cliquez sur **Suivant**. Un résumé de l'opération d'import de groupes est affiché.
12. Cliquez sur **Suivant**.
    Un résumé de l'état de la configuration est affiché. Si une erreur est détectée, cliquez sur le bouton **Corriger** : vous êtes redirigé à l'étape de configuration pour laquelle l'erreur a été détectée.
13. Corrigez l'erreur et cliquez plusieurs fois sur le bouton **Suivant** pour retourner à l'étape de vérification de la configuration.
14. Validez votre configuration en cliquant sur **Terminer**.
    Vous êtes redirigé vers le panneau d'édition de la méthode d'authentification OIDC / Microsoft Entra ID.

15. Cliquez sur **Appliquer** pour enregistrer la configuration de la méthode d'authentification Microsoft Entra ID sur le firewall.

Dans cet exemple, la configuration de la méthode OIDC / Microsoft Entra ID sur le firewall prend donc la forme suivante :



Créer la règle d'authentification

Rendez-vous dans le module **Configuration** > **Utilisateurs** > **Authentification** > onglet **Politique d'authentification** :

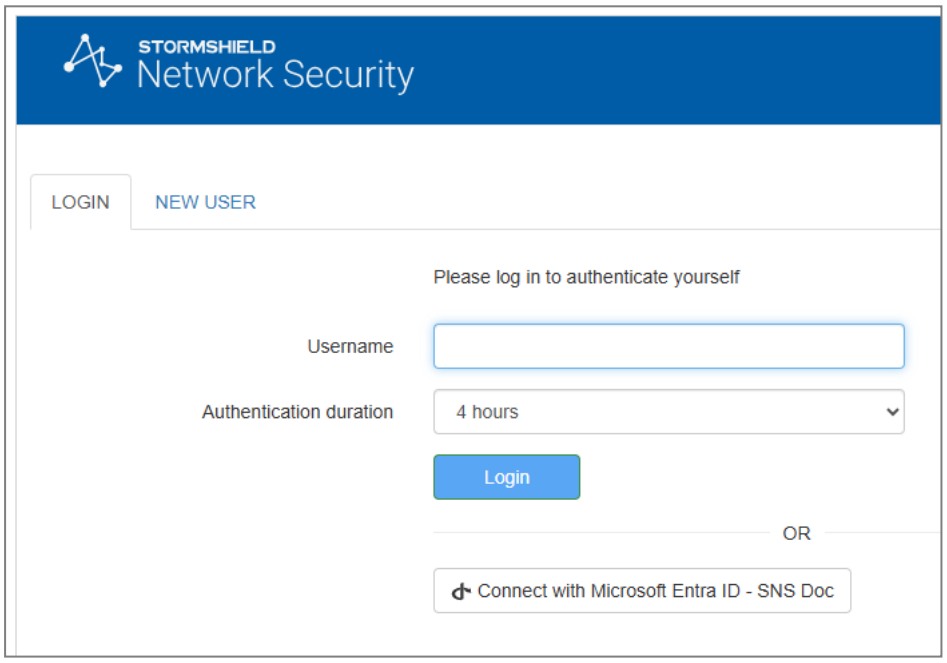
1. Cliquez sur **Nouvelle règle** et sélectionnez **Règle standard**.
2. Dans le menu **Utilisateurs** : cochez **Tous les utilisateurs**.
   Les autorisations de se connecter au portail captif, à l'interface Web d'administration ou au VPN SSL en s'authentifiant via Microsoft Entra ID seront accordées en fonction des droits définis dans le *tenant*.
3. Dans le menu **Sources** : ajoutez les interfaces réseau par lesquelles les utilisateurs authentifiés par Microsoft Entra ID se présentent au firewall. Dans cet exemple, les interfaces suivantes sont utilisées :
   - in : interface d'accès au portail captif interne pour l'authentification des administrateurs via l'interface Web d'administration,
   - out : interface d'accès au portail captif externe utilisée pour la récupération de leur fichier de configuration par les clients VPN SSL et l'établissement du tunnel,
   - sslvpn : interface utilisée par les clients VPN SSL pour accéder au service VPN SSL du firewall lorsque le tunnel est établi.
4. Dans le menu **Méthodes d'authentification** : cliquez sur **Activer une méthode** et sélectionnez la méthode **OIDC**.
5. De la même manière, ajoutez les autres méthodes d'authentification pour vos utilisateurs (exemple : **LDAP**).
6. Validez cette règle d'authentification en cliquant sur **OK**.
   La règle est ajoutée à la politique d'authentification mais n'est pas activée par défaut.

7. Dans la grille des règles d'authentification, double-cliquez sur l'état de cette règle pour l'activer.

La règle d'authentification prend donc la forme suivante :

NOTE
Lors d'une authentification, les règles sont examinées dans l'ordre de leur numérotation. Veillez donc à les organiser à l'aide des boutons **Monter** et **Descendre** selon vos besoins et les actions associées (**Autoriser** / **Interdire**).

Le portail captif du firewall propose désormais l'authentification via **Microsoft Entra ID** :

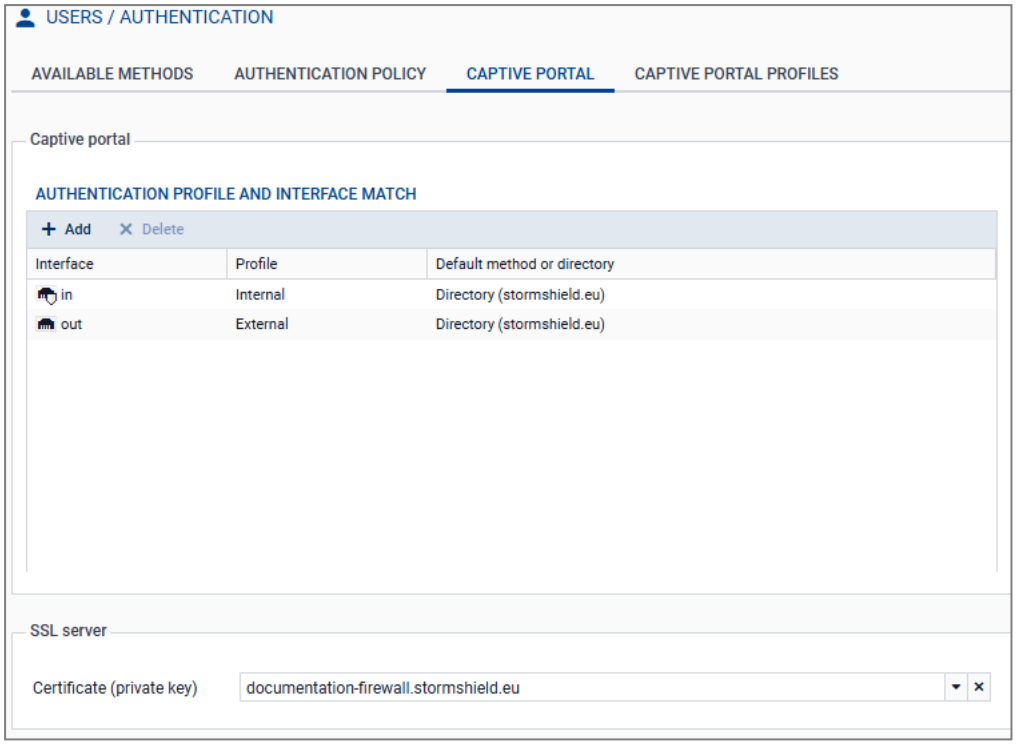


Configurer le portail captif

Dans le module **Configuration** > **Utilisateurs** > **Authentification** > onglet **Portail captif** :

1. Ajoutez les interfaces **in** et **out** pour les associer respectivement aux profils **Internal** et **External** du portail captif.
2. Sélectionnez le certificat de l'identité serveur basée sur le FQDN du firewall.

La configuration du portail captif prend donc la forme suivante :



Visualiser / importer des groupes de sécurité Microsoft Entra ID

Rendez-vous dans le module **Configuration** > **Utilisateurs** > **Utilisateurs et groupes** > onglet **Microsoft Entra ID**.
La liste des groupes Microsoft Entra ID importés et leurs identifiants de groupe sont affichés dans la grille.

Lorsque vous ajoutez ou modifiez des groupes dans votre centre d'administration Microsoft Entra ID, vous pouvez importer ces groupes dans ce module à l'aide du bouton **Importer des groupes** et en sélectionnant le fichier CSV exporté depuis votre *tenant*Microsoft Entra ID lors de l'étape Télécharger les groupes d'utilisateur en vue de leur import dans le firewall SNS.

NOTE
Si des groupes personnalisés ont été ajoutés via ce module, ils ne sont pas remplacés lors d'un import de fichier CSV. Si un groupe importé possède le même nom qu'un groupe personnalisé, ils sont différenciés par leur identifiant unique (UID) et peuvent coexister dans la configuration.

Créer ou modifier des rôles applicatifs sur le firewall (optionnel)

L'utilisation des rôles applicatifs pour la gestion des droits utilisateurs impose que ces rôles soient définis à l'identique sur le firewall et dans l'application du *tenant* Microsoft Entra ID.

Rendez-vous dans le module **Utilisateurs** > **Utilisateurs** > onglet **Microsoft Entra ID**.

Créer un rôle applicatif

1. Cliquez sur **Ajouter** puis **Rôle applicatif**.
2. Renseignez les champs suivants :
   - Le **Nom du rôle applicatif** (texte libre).
   - L'**UID du rôle applicatif** dont la syntaxe doit être de la forme Actions.Droits (exemple : SNS.Config.All.Write, SNS.Config.All.Read).
   - La **Description** optionnelle (texte libre).

   IMPORTANT
   L'UID du rôle doit être unique sur le firewall et identique à l'UID du rôle applicatif correspondant créé dans votre tenant Microsoft Entra ID.
3. Cliquez sur **Appliquer** pour valider la création du rôle.
4. Cliquez sur **Appliquer** pour enregistrer la modification de configuration.

Modifier un rôle applicatif

1. Sélectionnez le rôle à modifier et cliquez sur **Éditer**.
2. Modifiez selon vos besoins :
   - Le **Nom du rôle applicatif** (texte libre).
   - L'**UID du rôle applicatif** dont la syntaxe doit être de la forme Actions.Droits (exemple : SNS.Config.All.Write, SNS.Config.All.Read).
   - La **Description** optionnelle (texte libre).

   IMPORTANT
   L'UID du rôle doit être unique sur le firewall et identique à l'UID du rôle applicatif correspondant créé dans votre tenant Microsoft Entra ID.
3. Cliquez sur **Appliquer** pour valider la création du rôle.
4. Cliquez sur **Appliquer** pour enregistrer la modification de configuration.

Autoriser le VPN SSL pour les utilisateurs authentifiés via Microsoft Entra ID

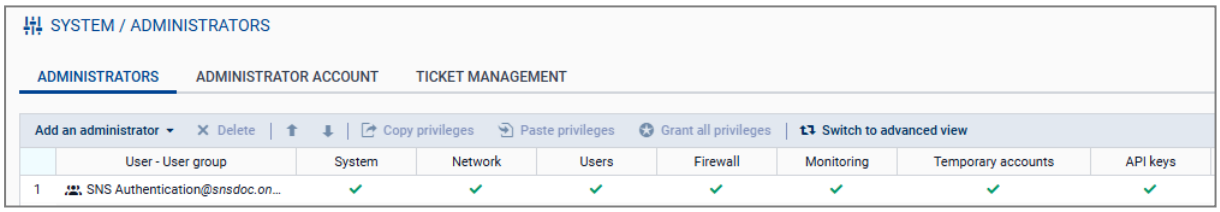
Dans le module **Configuration** > **Utilisateurs** > **Droits d'accès** > onglet **Accès détaillé** :

1. Cliquez sur **Ajouter**.
2. Cochez **Microsoft Entra ID** et sélectionnez un groupe importé depuis Microsoft Entra ID, un groupe personnalisé ou un rôle applicatif.
3. Cliquez sur **Appliquer**.
   Une règle est ajoutée dans la grille.
4. Cliquez dans la colonne **VPN SSL** de cette règle et sélectionnez **Autoriser**.
5. Double-cliquez dans la colonne **État** de cette règle pour l'activer.
6. Cliquez sur **Appliquer** puis **Sauvegarder** pour valider la modification de configuration.

Autoriser l'accès à l'interface Web d'administration pour les administrateurs authentifiés via Microsoft Entra ID

Dans le module **Système** > **Administrateurs** :

1. Cliquez sur **Ajouter un administrateur**.
2. Sélectionnez le type de droits à accorder au groupe d'administrateurs.
3. Cliquez sur **Microsoft Entra ID** puis sélectionnez un groupe de sécurité importé depuis Microsoft Entra ID, un groupe de sécurité personnalisé ou un rôle applicatif.
4. Validez ce choix en cliquant sur **Appliquer**.
5. Cliquez sur **Appliquer** pour valider la modification de configuration.



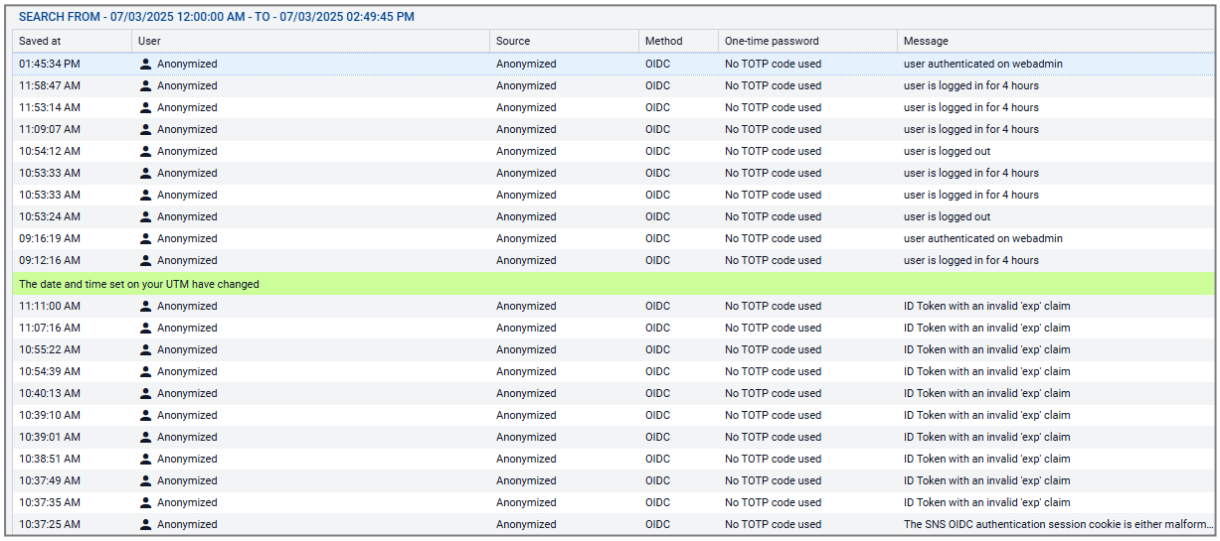
Consulter les éléments de surveillance de l'authentification OIDC / Microsoft Entra ID

Connectez-vous à l'interface Web d'administration du firewall.

Accéder aux événements de connexion

1. Placez-vous dans l'onglet **Monitoring** > menu **Logs - Journaux d'audit.**
2. Cliquez sur **Utilisateurs**.
   Les lignes concernant l'authentification Microsoft Entra ID contiennent le mot-clé "OIDC" dans la colonne **Méthode.**

Exemple :



SEARCH FROM - 07/03/2025 12:00:00 AM - TO - 07/03/2025 02:49:45 PM

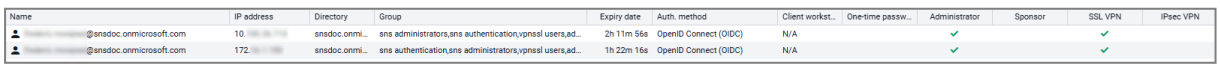
Saved at	User	Source	Method	One-time password	Message
01:45:34 PM	Anonymized	Anonymized	OIDC	No TOTP code used	user authenticated on webadmin
11:58:47 AM	Anonymized	Anonymized	OIDC	No TOTP code used	user is logged in for 4 hours
11:53:14 AM	Anonymized	Anonymized	OIDC	No TOTP code used	user is logged in for 4 hours
11:09:07 AM	Anonymized	Anonymized	OIDC	No TOTP code used	user is logged in for 4 hours
10:54:12 AM	Anonymized	Anonymized	OIDC	No TOTP code used	user is logged out
10:53:33 AM	Anonymized	Anonymized	OIDC	No TOTP code used	user is logged in for 4 hours
10:53:33 AM	Anonymized	Anonymized	OIDC	No TOTP code used	user is logged in for 4 hours
10:53:24 AM	Anonymized	Anonymized	OIDC	No TOTP code used	user is logged out
09:16:19 AM	Anonymized	Anonymized	OIDC	No TOTP code used	user authenticated on webadmin
09:12:16 AM	Anonymized	Anonymized	OIDC	No TOTP code used	user is logged in for 4 hours
The date and time set on your UTM have changed					
11:11:00 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
11:07:16 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
10:55:22 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
10:54:39 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
10:40:13 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
10:39:10 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
10:39:01 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
10:38:51 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
10:37:49 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
10:37:35 AM	Anonymized	Anonymized	OIDC	No TOTP code used	ID Token with an invalid 'exp' claim
10:37:25 AM	Anonymized	Anonymized	OIDC	No TOTP code used	The SNS OIDC authentication session cookie is either malform...

Cet exemple illustre le fait qu'avant la synchronisation du firewall en termes de date et heure, l'authentification OIDC / Microsoft Entra ID ne fonctionnait pas (messages "ID Token with an invalid 'exp' claim" - voir la section Résoudre les incidents - Erreurs communes).

Accéder au détail des utilisateurs connectés via Microsoft Entra ID

1. Placez-vous dans l'onglet **Monitoring** > menu **Supervision**.
2. Cliquez sur **Utilisateurs**.
   Les lignes concernant l'authentification Microsoft Entra ID contiennent les mots-clés "OpenID Connect (OIDC)" dans la colonne **Méthode d'auth.**

Exemple :



Name	IP address	Directory	Group	Expiry date	Auth. method	Client workst...	One-time passw...	Administrator	Sponsor	SSL VPN	IPsec VPN
@snsdoc.onmicrosoft.com	10.	snsdoc.onmi...	sns administrators,sns authentication,vpnssl users,ad...	2h 11m 56s	OpenID Connect (OIDC)	N/A		✓		✓	
@snsdoc.onmicrosoft.com	172.	snsdoc.onmi...	sns authentication,sns administrators,vpnssl users,ad...	1h 22m 16s	OpenID Connect (OIDC)	N/A		✓		✓	

Résoudre les incidents - Erreurs communes

Vérifier la cohérence entre les configurations du firewall et du *tenant* Microsoft Entra ID

Placez-vous dans le module **Configuration** > **Système** > **Console CLI** et tapez la commande suivante :

```
CONFIG AUTH OIDC CHECK DomainName=<Microsoft_EntraID_domain_name>.
```

L'URL du service Microsoft Entra ID (Issuer ID) est incorrecte dans la configuration du firewall

L'un des messages suivants est affiché :

```
type=warning code=1 domain="<domain name>" token="IssuerID" msg="Error
when trying to get OIDC Provider Metadata document"
type=warning code=1 domain="<domain name>" token="IssuerID" msg="Error
when trying to get OIDC Provider Metadata document (timeout)"
value0="timeout"
type=warning code=1 domain="<domain name>" token="IssuerID" msg="Error
when trying to get OIDC Provider Metadata document (invalid peer
certificate)" value0="invalid peer certificate"
```

L'ID d'application (client) est incorrecte dans la configuration du firewall

Le message suivant est affiché :

```
type=warning code=2 domain="<domain name>" token="ClientID" msg="Error
with ClientID when testing connection to SNS OpenID application : <OpenID
Provider error code>/<OpenID Provider error message>" value0=<OpenID
Provider error code> value1=<OpenID Provider error message>
```

Le secret client est incorrect dans la configuration du firewall

Le message suivant est affiché :

```
type=warning code=3 domain="<domain name>" token="ClientSecret" msg="Error
with ClientSecret when testing connection to SNS OpenID application :
<OpenID Provider error code>/<OpenID Provider error message>"
value0=<OpenID Provider error code> value1=<OpenID Provider error message>
```

Le fichier de logs **Utilisateurs** (module **Monitoring** > **Logs - Journaux d'audit**) contient également une ligne du type :

```
id=firewall time="2025-01-09 19:59:53" fw="documentation-
firewall.stormshield.eu" tz=+0100 startime="2025-01-09 19:59:53"
user="unknown" src=10.100.17.85 domain="mycompanyinternal.onmicrosoft.com"
confid=0 ruleid=0 method="OIDC" totp="no" error=5 msg="error to get token
response"
```

Une URI de redirection est invalide ou n'est pas déclarée dans l'application du tenant Microsoft Entra ID

Le message suivant est affiché :

```
type=info code=4 domain="<domain name in section>" msg="Error with
redirect_uri <redirect_uri> when testing connection to SNS OpenID
application" value0=<redirect_uri>
```

Aucune URI de redirection n'est valide ou n'a été déclarée dans l'application du tenant Microsoft Entra ID

Le message suivant est affiché :

```
type=warning code=5 domain="<domain name>" msg="Error : No working
redirect_uri"
```

Autres cas

Le message générique suivant est affiché :

```
type=warning code=6 domain="<domain name>" msg="Error when testing
connection to SNS OpenID application : <OpenID Provider error
code>/<OpenID Provider error message>" value0=<OpenID Provider error code>
value1=<OpenID Provider error message>
```

Autres erreurs courantes

La configuration de l'heure ou du fuseau horaire sur le firewall n'est pas correcte

Cette erreur provoque l'écriture d'une ligne dans le module **Monitoring** > **Logs - Journaux d'audit** > **Utilisateurs** avec le message suivant :

```
"ID Token with an invalid 'exp' claim"
```

La revendication <preferred_username> est absente de la configuration du *tenant* Microsoft Entra ID

Cette erreur provoque l'écriture d'une ligne visible dans le module **Monitoring** > **Logs - Journaux d'audit** > **Utilisateurs** avec le message suivant :

```
ID Token with an invalid or missing 'preferred_username' claim
```

Les serveurs Microsoft Entra ID sont injoignables

Cette erreur provoque l'écriture d'une ligne visible dans le module **Monitoring** > **Logs - Journaux d'audit** > **Utilisateurs** avec le message suivant :

```
Error while retrieving the OIDC Provider Metadata document
```

Un groupe reçu par le fournisseur d'identité (Microsoft Entra ID) n'a pas été déclaré dans le firewall

Cette erreur provoque l'écriture d'une ligne visible dans le module **Monitoring** > **Logs - Journaux d'audit** > **Événements système** du type :

```
Tentative d'authentification par les GUIDs suivants non déclarés :
GUID="<GUID_reference>"
```

documentation@stormshield.eu