



STORMSHIELD



TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

CONFIGURE OIDC / MICROSOFT ENTRA ID AUTHENTICATION

Product concerned: SNS v5 and higher

Document last updated: September 19, 2025

Reference: sns-en-configure_OIDC_Microsoft_ENTRA_ID_authentication_technical_note



Table of contents

Change log	4
Getting started	5
Requirements	5
SNS/Microsoft Entra ID OIDC authentication	6
Understanding how OIDC/Microsoft Entra ID authentication works	7
Adding the SNS application to your Microsoft Entra ID tenant	8
Creating the SNS application in the Microsoft Entra ID tenant	8
Adding more redirect URLs to your application (optional)	8
Creating a client secret for the application	8
Creating an application token containing the necessary claims	9
Granting administrator consent to the application for the entire tenant	9
Creating application roles and assigning them to Microsoft Entra ID tenant users (optional)	9
Adding users/groups to your Microsoft Entra ID tenant	11
Adding users to your tenant	11
Assigning specific permissions to a user on the tenant	11
Assigning roles to users or groups in the application (optional)	11
Creating a group and assigning members to it	12
Downloading user groups to import them into the SNS firewall	12
Retrieving the Microsoft Entra ID information required to configure the firewall	13
Retrieving the domain name and tenant ID	13
Downloading the Application ID (client)	13
Configuring the firewall for OIDC/Microsoft Entra ID authentication	14
Setting the firewall FQDN for access to the captive portal	14
Creating a server identity based on this FQDN	14
Enabling the OIDC/Microsoft Entra ID authentication method	15
Creating the authentication rule	16
Configuring the captive portal	17
Viewing/importing Microsoft Entra ID security groups	18
Creating or editing application roles on the firewall (optional)	18
Creating an application role	19
Editing an application role	19
Allowing SSL VPN for users authenticated through Microsoft Entra ID	19
Allowing administrators authenticated through Microsoft Entra ID to access the web administration interface	20
Viewing OIDC/Microsoft Entra ID authentication monitoring components	21
Accessing connection events	21
Accessing details of users connected via Microsoft Entra ID	21
Resolving incidents - Common errors	22
Checking the consistency of the firewall and Microsoft Entra ID tenant configurations	22
The URL of the Microsoft Entra ID service (Issuer ID) in the firewall configuration is incorrect	22
The application ID (client) in the firewall configuration is incorrect	22
The client secret in the firewall configuration is incorrect	22



A redirect URI is invalid or was not declared in the Microsoft Entra ID tenant application	22
None of the redirect URIs are valid or have been declared in the Microsoft Entra ID tenant application	23
Other cases	23
Other common errors	23
The configured time or time zone on the firewall is incorrect	23
The <preferred_username> claim is missing from the Microsoft Entra ID tenant configuration	23
The Microsoft Entra ID servers cannot be reached	23
A group received by the identity provider (Microsoft Entra ID) was not declared on the firewall ...	23



Change log

Date	Description
September 19, 2025	New document



Getting started

As of SNS version 5, the firewall offers seamless, secure integration with Microsoft Entra ID through the OpenID Connect (OIDC) protocol. This feature is designed to centralize and optimize the management of access to your network infrastructure.

By connecting your SNS firewall to Microsoft Entra ID, you can:

- Centrally monitor who has access to your SSL VPN directly from Microsoft Entra ID.
- Allow your users to be automatically authenticated on the SNS firewall (for the captive portal or filter policies) simply by using their existing Microsoft Entra ID accounts.
- Manage your SNS administration accounts from a single location, thereby improving the security and consistency of your access policies.

The directory that groups users and the applications that are accessible to these users through Microsoft Entra ID is known as a "tenant" in the Microsoft Entra ID administration interface, and in the rest of this document.

Requirements

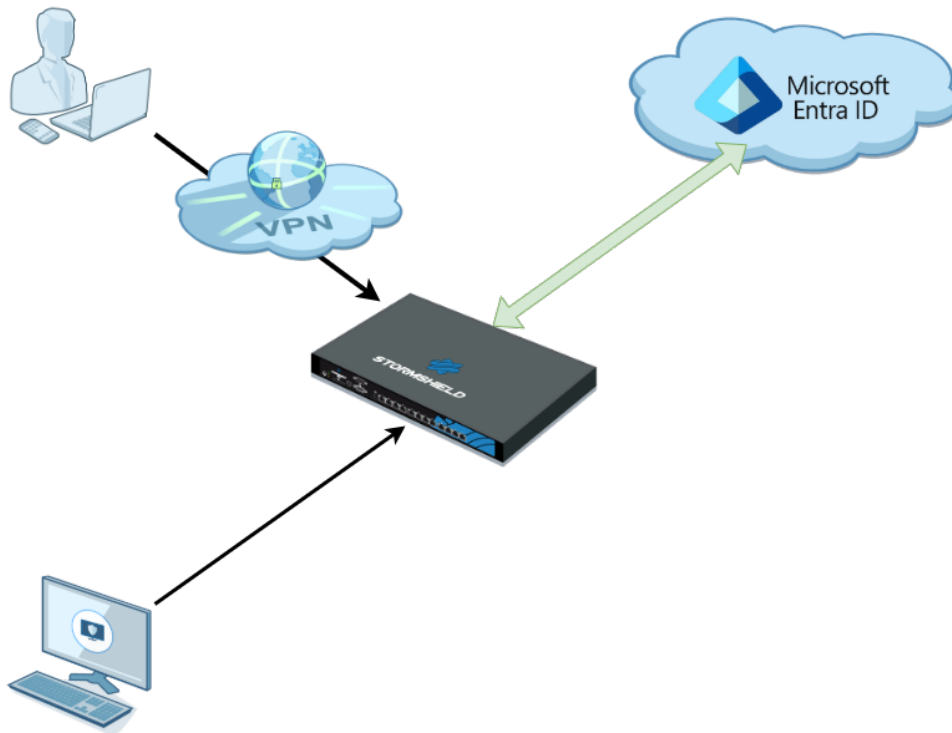
- A Microsoft Entra ID subscription including the tenant.
- An administrator account for the tenant in question.
- An SNS firewall in version 5.0.1 or higher with a fully qualified domain name (FQDN) that can be accessed from the Internet (e.g., myfirewall.mycompany.com, sslvpn.mycompany.com, etc.).
- The date and time on this firewall have to be up to date in order for OIDC/Microsoft Entra ID authentication to work.
To ensure optimal operation, you are strongly advised to [enable NTP time synchronization](#) on the firewall.
- A Stormshield SSL VPN client in version 4.1 or higher if users authenticated via OIDC/Microsoft Entra ID are allowed to set up SSL VPN tunnels with the firewall.



SNS/Microsoft Entra ID OIDC authentication

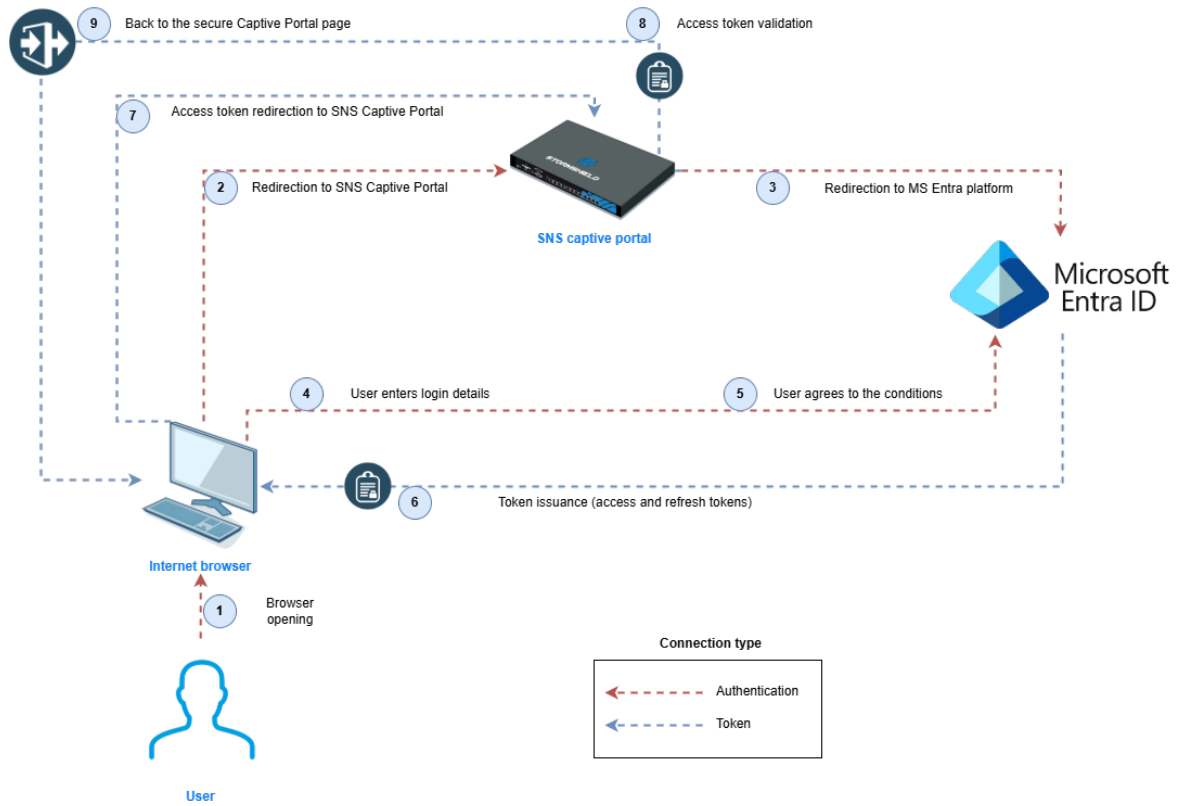
This document explains the SNS and Microsoft Entra ID configurations that are required to allow:

- Remote users to set up an SSL VPN tunnel by authenticating through Microsoft Entra ID.
- Administrators to connect to the firewall administration web interface by authenticating through Microsoft Entra ID.





Understanding how OIDC/Microsoft Entra ID authentication works





Adding the SNS application to your Microsoft Entra ID tenant

Log in to the Microsoft Entra ID administration center, then access the **Identity > Applications > Application registrations** menu.

Creating the SNS application in the Microsoft Entra ID tenant

1. Go to **Identity > Applications > Application registrations**.
2. Click on **New registration**.
3. Name the application (e.g., SNS Connector).
4. Under **Supported account types**, select **Accounts in this organization directory only**.
5. For the redirect URI, select **Web** as the type and a first redirect URI in one of the following forms:
 - SSL VPN: `https://<firewall_fqdn>/auth/v1/oidc/token/sslvpn`
 - Web administration interface: `https://<firewall_fqdn>/auth/v1/oidc/token/webadmin`



NOTE

An initial redirect URI must be entered for any new application.

6. Click on **Register**.

Adding more redirect URIs to your application (optional)

If you would like to add other redirect URIs to your application in order to access additional services:

1. In the **Databases** section, click on the link to **Web redirect URIs**.
2. In the **Web** section, enter the URI in one of the following forms:
 - SSL VPN: `https://<firewall_fqdn>/auth/v1/oidc/token/sslvpn`
 - Web administration interface: `https://<firewall_fqdn>/auth/v1/oidc/token/webadmin`
3. Click on **Add a URI** to set an additional URI.
4. Click on **Save** to confirm your configuration.

Creating a client secret for the application

This operation consists of generating a secret that will be entered on the SNS firewall to allow it to access the application.

1. In **Certificates & secrets > Client secrets** tab, click on **New client secret**.
2. Enter a description and select an **Expiry date** for the secret.
The default value is 6 months (180 days).
3. Confirm.
The secret will appear in the list.



IMPORTANT

Click on the **Copy to the clipboard** icon next to the value of the secret and keep it until



you add it to the Entra ID configuration on the firewall.
This secret can no longer be displayed once you exit the Microsoft Entra ID module.
If you forgot to copy the secret before exiting the module, you will need to create a new secret.

Creating an application token containing the necessary claims

When the user authenticates on Microsoft Entra ID, the firewall receives a token containing the user's name, the groups in which the user is a member, and the application roles that were assigned to the user (optional) in order to determine user authorizations.

1. In the **Token configuration** menu, click on **Add an optional claim**.
2. Select the **ID token**.
The list of claims appears.
3. Select the **preferred_username** checkbox.
This makes it possible to include the user's identity information (first and last names) in the token.
4. Click on **Add**.
5. Click on **Add a group claim**.
6. Select the **Security groups** checkbox.
7. Ensure that the ID associated with this token is set to **Group ID**.
This makes it possible for the token to include the list of groups in which the user is a member. Note that for free licenses, this option is restricted to the first 200 groups to which the user belongs.

i NOTE

The number of groups to be included in the token can be restricted to the groups affected by the application, by selecting the option **Groups assigned to the application (recommended for large companies to avoid exceeding the maximum number of groups that a token can issue)**. This option exists only with a paid P1 license.

Granting administrator consent to the application for the entire tenant


When users connect to Microsoft Entra ID for the first time, they are asked to consent to sharing <preferred_username> information with the application. The administrator of the tenant may give overall consent for all users of the tenant.

1. In **Security > Permissions**, click on **Grant admin consent for <application_name>**.
A window appears, asking you to accept the permissions.
2. Click on **Accept**.

Creating application roles and assigning them to Microsoft Entra ID tenant users (optional)

Application roles can be defined to grant specific access privileges to users.



For example: allowing a user to access the firewall configuration in read-only or read/write mode, allowing a user to sponsor ( more information on the [sponsorship](#) feature in the [SNS user guide](#)), granting users permissions to set up SSL VPN tunnels, etc.

There are four default application roles on the firewall:

- **Administrators:** access in read/write to the firewall web administration interface.
- **Auditors:** access to the firewall web administration interface in read-only mode.
- **Sponsors:** permission to sponsor temporary users.
- **SSLVPN users:** permission to set up an SSL VPN tunnel with the firewall.

IMPORTANT

If you choose to use application roles for permissions, they must have an identical UID on the Microsoft Entra ID tenant and on the SNS firewall that uses OIDC/Microsoft Entra ID authentication (e.g., SNS.Config.All.Write or SNS.SSLVPN).

The configuration of application roles on the firewall is covered in the section [Configuring the firewall for OIDC/Microsoft Entra ID authentication](#).

1. Specify the **Role display name**.
2. Select the **Users/Groups** checkbox.
3. In the **Value** field, specify the permissions assigned through this role as a sequence of SNS permissions (e.g., SNS.Config.All.Write or SNS.SSLVPN).
4. Select the checkbox **Enable this application role?** if you wish to use this role in your Microsoft Entra ID application.
5. Repeat steps 2 to 7 to create all the desired roles.



Adding users/groups to your Microsoft Entra ID tenant

Log in to the Microsoft Entra ID administration center to access your tenant.

Adding users to your tenant

1. In **Identity > Users > All users**, click on **New user**, then on **Create a user**.
2. In the **Main username** field, enter the desired user name (e.g., john.doe).
The suffix corresponding to the tenant is added automatically (e.g., @snsdoc.onmicrosoft.com).
The full username will be the ID to be used to connect to the tenant (e.g., john.doe@snsdoc.onmicrosoft.com).
3. Specify the user's **Display name** (e.g., John Doe).
4. You can manually enter the **Password** for this user or **Automatically generate password** by selecting the checkbox of the same name.
5. Click on **Review + Create** and confirm by clicking on **Create**.
The user is then created.
6. Repeat steps 2 to 6 to create all users on the tenant.

Assigning specific permissions to a user on the tenant

1. In **Identity > Users > All users**, click on the name of the user to whom you wish to assign permissions.
2. In the menu on the left, click on **Roles assigned**.
3. Click on **Add assignments** and select the desired permissions (e.g., General administrator).
4. Click on **Add**.

Assigning roles to users or groups in the application (optional)

NOTE

In order to assign roles to groups, a paid Microsoft Entra ID subscription is required. Free subscriptions only make it possible to assign roles to users.

1. In **Identity > Enterprise applications**, click on the name of your application (e.g., SNS Connector).
2. Go to **Manage > Users and groups**.
3. Click on **Add user/group**.
4. Under **Users**, click on **No selection**.
5. Select the users to whom you wish to assign the role.
6. Click on **Select**.
7. Under **Select a role**, click **No selection**.
8. Select the desired role, and click on **Select**.
9. Click on **Assign**.



Users and their roles will then appear in the grid.

10. Repeat steps 2 to 7 to assign all the roles.

Creating a group and assigning members to it

1. In **Identity > Groups > Overview**, click on **New group**.
2. For the **Group type**, select **Security**.
3. Specify the **Name** of the group (e.g., SNS Authentication).
You can add a **Group description** if needed.
4. Click on **No members selected**, and select the users to be added to this group (e.g., John Doe).
5. Confirm by clicking on **Select**.
6. Click on **Create**.

Downloading user groups to import them into the SNS firewall

1. In **Identity > Groups > All groups**, select the groups to be exported, then click on **Download groups**.
2. Change the name of the suggested CSV file if needed, then click on **Start download..** The CSV file will then be created.
3. When the CSV file is ready, click on the link **The file is ready! Click here to download**, and save the CSV file on your workstation.



Retrieving the Microsoft Entra ID information required to configure the firewall

Go to your Microsoft Entra ID administration center to retrieve the following information, which is required to configure the OIDC/Microsoft Entra ID method on the SNS firewall.

Retrieving the domain name and tenant ID

1. Go to **Identity > Overview**.
2. Retrieve the value of the **Main domain** field.
3. Retrieve the value of the **Tenant ID** field.

Downloading the Application ID (client)

1. Go to **Identity > Applications > Application registrations > All applications** tab.
2. Click on the name of your SNS application (e.g., SNS Connector).
3. Retrieve the value of the **Application ID (client)** field.



Configuring the firewall for OIDC/Microsoft Entra ID authentication

Log in to the web administration interface of the firewall.

Setting the firewall FQDN for access to the captive portal

Browsers on client workstations must be able to resolve this FQDN.

In **System > Configuration > General configuration** tab > **Captive portal** section:

1. In the **Redirect to the captive portal** field, select the value **Specify a domain name (FQDN)**.
2. In the **Domain name (FQDN)** field, enter the full name of the firewall (example: documentation-firewall.stormshield.eu).

! IMPORTANT

This FQDN must be identical to the one used when [declaring URIs in the Stormshield application](#) defined in the Microsoft Entra ID tenant.

Creating a server identity based on this FQDN

The certificate of this server identity is meant to be used by the firewall's captive portal.

i NOTE

In SSL VPN access, it is preferable for the captive portal identity to come from a public CA, as it is already integrated into browsers.

In **Objects > Certificates and PKI**:

1. Click on **Add**, then select **Server identity**.
2. In the **Fully Qualified Domain Name (FQDN)** field, enter the FQDN specified in step [Setting the firewall FQDN for access to the captive portal](#) (e.g., documentation-firewall.stormshield.eu).
3. The ID suggested by default for this identity corresponds to the FQDN defined in step 2. This name can be changed.
4. Click on **Next**.
5. Select the **Parent authority** that signs this identity, and enter the password for this CA. This identity must be known to the browsers used for authentication.
6. Click on **Next**.
7. Change the **Validity (days)**, **Key type** and **Key size (bits)** fields if necessary. The default values are those relating to the parent CA.
8. Click on **Next**.
9. Aliases can be added to this identity.
10. Click on **Next**. You will be shown a summary of this identity's properties.
11. Confirm these properties by clicking on **Finish**.



Enabling the OIDC/Microsoft Entra ID authentication method

In **Users > Authentication > Available methods** tab:

1. Click on **Enable a method**.
2. Select **OIDC/Microsoft Entra ID**.
A configuration wizard will automatically launch:
3. **Domain name**: indicate the main domain name [retrieved from your Microsoft Entra ID administration center](#) (e.g., snsdoc.onmicrosoft.com).
4. **Tenant ID**: enter the ID [retrieved from your Microsoft Entra ID administration center](#) in this field.
5. **Application ID (client)**: enter the value [retrieved from your Microsoft Entra ID administration center](#) in this field.
6. **Client secret**: enter the value retrieved and saved when [Creating a secret for the application](#) during the creation of the SNS application on your Microsoft Entra ID tenant. If you did not save this value, you need to delete the **Client secret** that was created earlier for your application, and generate a new one, by following the procedure described in [this step](#).
7. Change the **Authentication duration** if necessary. This is how long an authenticated Microsoft Entra ID user will stay connected before needing to enter their login details again. The default setting is 1 day.
8. Click on **Next**.
The wizard suggests URLs that correspond to the captive portal service, the SSL VPN service, and access to the firewall's web administration interface. These URLs can be copied directly from this wizard to be entered as redirect URLs in your Microsoft Entra ID administration center if necessary.
They are also available in the OIDC/Microsoft Entra ID method editing panel.
9. If you do not wish to import user groups in the next step of the wizard, select the **Skip group import** checkbox and go directly to step 15 of this procedure.
10. Click on **Next**.
11. Select the CSV file containing the groups in your Microsoft Entra ID tenant, which was downloaded when [Downloading user groups to import them into the SNS firewall](#), then click on **Next**. A summary of the group import operation then appears.
12. Click on **Next**.
Configuring the firewall for OIDC/ authentication If an error is detected, click on **Fix**: you will be redirected to the configuration step in which the error was detected.
13. Fix the error and click on **Next** several times to return to the configuration verification step.
14. Confirm your configuration by clicking on **Finish**.
You will be redirected to the OIDC/Microsoft Entra ID authentication method editing panel.
15. Click on **Apply** to save the configuration of the Microsoft Entra ID authentication method on the firewall.



In this example, the configuration of the OIDC/Microsoft Entra ID method on the firewall will therefore resemble the following:

OpenID Connect / Microsoft Entra ID - SNS Doc

Domain name

Fill in information about the SNS application on your Microsoft Entra ID tenant:

URL of the MS Entra ID service (Issuer ID)

Application ID (client)

Client secret

Service URL

Copy the following URLs to enter them in the SNS application on your Microsoft Entra ID tenant

Captive portal

SSL VPN

Web administration interface

URLs relating to the captive portal and SSL VPN are generated from the [System / Configuration](#) module (Advanced configuration).

Force re-authentication of a Microsoft Entra ID session when its duration exceeds:

Maximum duration Day(s) Hour(s)

TEST THE CONFIGURATION

Creating the authentication rule

Go to **Configuration > Users > Authentication > Authentication policy** tab:

1. Click on **New rule** and select **Standard rule**.
2. Select **All users** in the **Users** menu.
Permissions to connect to the captive portal, web administration interface or SSL VPN by authenticating through Microsoft Entra ID will be granted according to the privileges set in the tenant.
3. In the **Sources** menu: add the network interfaces through which users authenticated by Microsoft Entra ID will be presenting on the firewall. In this example, the following interfaces are used:
 - in: interface to access the internal captive portal to authenticate administrators via the web administration interface,
 - out: interface to access the external captive portal that SSL VPN clients use for retrieving their configuration files and setting up tunnels,
 - sslvpn: interface used by SSL VPN clients to access the firewall's SSL VPN service when the tunnel is set up.
4. In the **Authentication methods** menu: click on **Enable a method** and select the **OIDC** method.
5. Likewise, add the other authentication methods for your users (e.g.: **LDAP**).
6. Confirm this authentication rule by clicking on **OK**.
The rule will be added to the authentication policy but will not be enabled by default.
7. In the authentication rule grid, double click on the status of the rule to enable it.

The authentication rule will then look like this:



Status	Action	Source	Methods (assess by order)	One-time password
Enabled	Allow	any @any in out sslvpn	1. OIDC 2. LDAP	<input type="checkbox"/>

NOTE

During an authentication, rules are scanned in order of their appearance in the list. As such, ensure that you organize them using the **Up** and **Down** buttons when necessary, as well as the associated actions (**Allow/Block**).

The firewall's captive portal will now offer **Microsoft Entra ID** authentication:

Configuring the captive portal

In **Configuration > Users > Authentication > Captive portal** tab:

1. Add the **in** and **out** interfaces to respectively associate them with the **Internal** and **External** profiles of the captive portal.
2. Select the server identity certificate based on the firewall's FQDN.

The captive portal configuration will then look like this:



USERS / AUTHENTICATION

AVAILABLE METHODSAUTHENTICATION POLICYCAPTIVE PORTALCAPTIVE PORTAL PROFILES

Captive portal

AUTHENTICATION PROFILE AND INTERFACE MATCH

+ Add X Delete

Interface	Profile	Default method or directory
in	Internal	Directory (stormshield.eu)
out	External	Directory (stormshield.eu)

SSL server

Certificate (private key)documentation-firewall.stormshield.eu

Viewing/importing Microsoft Entra ID security groups

Go to **Configuration > Users > Users and Groups > Microsoft Entra ID** tab.

The list of imported Microsoft Entra ID groups and their group IDs are displayed in the grid.

When you add or edit groups in your Microsoft Entra ID administration center, you can import these groups into this module by using the **Import groups** button, and selecting the CSV file that was exported from your Microsoft Entra ID tenant when [Downloading user groups to import them into the SNS firewall](#).

i NOTE

If custom groups were added through this module, they will not be overwritten when a CSV file is imported. If an imported group has the same name as a custom group, they will be differentiated by their unique identifiers (UIDs), and can coexist in the configuration.

Creating or editing application roles on the firewall (optional)

To use application roles to manage user permissions, these roles must have identical configurations on the firewall and in the Microsoft Entra ID tenant application.

Go to **Users > Users > Microsoft Entra ID** tab.



Creating an application role

1. Click on **Add**, then on **Application role**.
2. Fill in the following fields:
 - The **Application role name** (any text).
 - The **Application role UID**, which has to use syntax in Actions.Permissions format (e.g., SNS.Config.All.Write, SNS.Config.All.Read).
 - The optional **Description** (any text).

! IMPORTANT

The role UID must be unique on the firewall, and identical to the UID of the corresponding application role that was created in your Microsoft Entra IDtenant.

3. Click on **Apply** to confirm the creation of the role.
4. Click on **Apply** to save changes to the configuration.

Editing an application role

1. Select the role to edit, and click on **Edit**.
2. Change the following parameters according to your requirements:
 - The **Application role name** (any text).
 - The **Application role UID**, which has to use syntax in Actions.Permissions format (e.g., SNS.Config.All.Write, SNS.Config.All.Read).
 - The optional **Description** (any text).

! IMPORTANT

The role UID must be unique on the firewall, and identical to the UID of the corresponding application role that was created in your Microsoft Entra IDtenant.

3. Click on **Apply** to confirm the creation of the role.
4. Click on **Apply** to save changes to the configuration.

Allowing SSL VPN for users authenticated through Microsoft Entra ID

In **Configuration > Users > Access privileges > Detailed access** tab:

1. Click on **Add**.
2. Enable **Microsoft Entra ID** and select a group that has been imported from Microsoft Entra ID, a custom group or an application role.
3. Click on **Apply**.
A rule is added to the grid.
4. Click in the **SSL VPN** column of this rule and select **Allow**.
5. Double-click in the **Status** column of this rule to enable it.
6. Click on **Apply**, then **Save** to confirm changes to the configuration.



USERS / ACCESS PRIVILEGES

DEFAULT ACCESS

DETAILED ACCESS

Searching...

+ Add

✕ Delete

↑ Up

↓ Down

Status	User - user group	IPSEC	SSL VPN	Sponsorship	Description
1 <div>Enabled</div>	<div></div> SNS Authentication@snsdoc.onmicrosoft.com	<div>Block</div>	<div>Allow</div>	<div>Block</div>	

Allowing administrators authenticated through Microsoft Entra ID to access the web administration interface

In **System > Administrators**:

1. Click on **Add an administrator**.
2. Select the type of permissions to be granted to the administrator group.
3. Click on **Microsoft Entra ID**, then select a security group that was imported from Microsoft Entra ID, a custom security group or an application role.
4. Confirm your selection by clicking on **Apply**.
5. Click on **Apply** to confirm changes to the configuration.

SYSTEM / ADMINISTRATORS

ADMINISTRATORS

ADMINISTRATOR ACCOUNT

TICKET MANAGEMENT

Add an administrator

Delete

Copy privileges

Paste privileges

Grant all privileges

Switch to advanced view

	User - User group	System	Network	Users	Firewall	Monitoring	Temporary accounts	API keys
1	SNS Authentication@snsdoc.on...							



Viewing OIDC/Microsoft Entra ID authentication monitoring components

Log in to the web administration interface of the firewall.

Accessing connection events

1. Go to the **Monitoring** tab > **Logs - Audit logs** menu.
2. Click on **Users**.
Lines regarding Microsoft Entra ID authentication contain the keyword "OIDC" in the **Method** column.

Example:

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 malformed

This example illustrates the fact that before the firewall date and time were synchronized, OIDC/Microsoft Entra ID authentication was not working ("ID Token with an invalid 'exp' claim" messages - see section [Resolving incidents - Common errors](#)).

Accessing details of users connected via Microsoft Entra ID

1. Go to the **Monitoring** tab > **Monitoring** menu.
2. Click on **Users**.
Lines regarding Microsoft Entra ID authentication contain the keywords "OpenID Connect (OIDC)" in the **Auth method** column.

Example:

Name	IP address	Directory	Group	Expiry date	Auth. method	Client workst...	One-time passw...	Administrator	Sponsor	SSL VPN	iPsec VPN
@snsdoc.ormicrosoft.com	10.10.10.10	snsdoc.ormi...	sns administrators,sns authentication,vpnsl users,ad...	2h 11m 56s	OpenID Connect (OIDC)	N/A		✓		✓	
@snsdoc.ormicrosoft.com	172.16.17.17	snsdoc.ormi...	sns authentication,sns administrators,vpnsl users,ad...	1h 22m 16s	OpenID Connect (OIDC)	N/A		✓		✓	



Resolving incidents - Common errors

Checking the consistency of the firewall and Microsoft Entra ID tenant configurations

Go to **Configuration > System > CLI console** and type the following command:
`CONFIG AUTH OIDC CHECK DomainName=<Microsoft_EntraID_domain_name>.`

The URL of the Microsoft Entra ID service (Issuer ID) in the firewall configuration is incorrect

One of the following messages appears:

```
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"
```

The application ID (client) in the firewall configuration is incorrect

The following message appears:

```
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>
```

The client secret in the firewall configuration is incorrect

The following message appears:

```
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>
```

The **Users** log file (**Monitoring > Logs - Audit logs**) also contains a line resembling:

```
id=firewall time="2025-01-09 19:59:53" fw="documentation-
firewall.stormshield.eu" tz="+0100" starttime="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"
```

A redirect URI is invalid or was not declared in the Microsoft Entra ID tenant application

The following message appears:

```
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>
```



None of the redirect URIs are valid or have been declared in the Microsoft Entra ID tenant application

The following message appears:

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

Other cases

The following generic message appears:

```
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>
```

Other common errors

The configured time or time zone on the firewall is incorrect

This error causes a log line to be written in **Monitoring > Logs - Audit logs > Users** with the following message:

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

The <preferred_username> claim is missing from the Microsoft Entra ID tenant configuration

This error causes a visible log line to be written in **Monitoring > Logs - Audit logs > Users** with the following message:

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

The Microsoft Entra ID servers cannot be reached

This error causes a visible log line to be written in **Monitoring > Logs - Audit logs > Users** with the following message:

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

A group received by the identity provider (Microsoft Entra ID) was not declared on the firewall

This error causes a visible log line such as the following to be written in **Monitoring > Logs - Audit logs > System events**:

```
Attempt to authenticate with the following undeclared GUIDs: GUID="<GUID_reference>"
```



STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.