

## Anexo 4

# Provisionado y autenticación de identidades con Azure AD

**Jordi Guillem Ferrer Bozzano**

Máster Universitario en Ciberseguridad y Privacidad  
Seguridad empresarial

**Iñaki Moreno Fernández**

**Víctor García Font**

10 de enero de 2023

# Índice

<b>1. PROVISIÓN DE USUARIOS NETSKOPE SCIM</b> .....	<b>3</b>
1.1. CREACIÓN DEL TOKEN OAuth EN NETSKOPE.....	3
1.2. CREAR APLICACIÓN EMPRESARIAL EN AZURE AD .....	4
1.3. COMPROBACIÓN DEL PROVISIONADO EN NETSKOPE.....	6
<b>2. AUTENTICACIÓN SAML PARA NETSKOPE FORWARD PROXY</b> .....	<b>8</b>
2.1. OBTENER CONFIGURACIÓN SAML DE NETSKOPE .....	8
2.2. CONFIGURAR APLICACIÓN EMPRESARIAL DE AZURE AD .....	8
2.3. AÑADIR UNA CUENTA DE AZURE AD EN NETSKOPE.....	10
<b>3. AUTENTICACIÓN SAML PARA NETSKOPE ADMIN CONSOLE</b> .....	<b>12</b>
3.1. OBTENER LA CONFIGURACIÓN DE NETSKOPE PARA EL SSO.....	12
3.2. CREAR LA APLICACIÓN EMPRESARIAL PARA NETSKOPE ADMIN CONSOLE EN AZURE AD.....	12
3.3. AÑADIR LA CONFIGURACIÓN SSO DE AZURE EN EL TENANT DE NETSKOPE .....	16

# Índice de ilustraciones

Ilustración 1: Inicio de sesión en Netskope (Provisión identidades).....	3
Ilustración 2: Creación Token OAuth (Provisión identidades) .....	3
Ilustración 3: Acceso al portal Azure (Provisión identidades).....	4
Ilustración 4: Añadir aplicación empresarial SCIM (Provisión identidades) .....	4
Ilustración 5: Búsqueda aplicación Netskope User Authentication (Provisión identidades) .....	5
Ilustración 6: Provisioning de aplicación empresarial (Provisión identidades).....	6
Ilustración 7: Grupos de provisioning (Provisión identidades).....	6
Ilustración 8: Grupos provisionados en Netskope (Provisión identidades) .....	7
Ilustración 9: Configuración SAML Forward Proxy de Netskope .....	8
Ilustración 10: Configuración SAML de aplicación Netskope SCIM en Azure AD .....	8
Ilustración 11: Edición de configuración SAML de aplicación Netskope SCIM en Azure AD.....	9
Ilustración 12: Descarga certificado Base 64 de SAML.....	9
Ilustración 13: Inicio de sesión de Netskope (Forward Proxy) .....	10
Ilustración 14: Nueva cuenta SSO en Netskope (Forward Proxy).....	10
Ilustración 15: Comprobación nueva cuenta SSO en Netskope (Forward Proxy) .....	11
Ilustración 16: Inicio de sesión de Netskope (Admin console) .....	12
Ilustración 17: Obtener información SSO de Netskope (Admin console).....	12
Ilustración 18: Añadir aplicación empresarial Netskope Administración Console.....	13
Ilustración 19: Crear nueva aplicación empresarial en Azure AD.....	13
Ilustración 20: Crear nueva aplicación empresarial Netskope Administration Console .....	14
Ilustración 21: Editar SAML de aplicación Netskope Administration Console en Azure AD.....	14
<i>Ilustración 22: Edición de SAML de aplicación Netskope Administration Console en Azure AD</i> .....	15
Ilustración 23: Seleccionar grupo para autenticar en Netskope Administration Console.....	15
Ilustración 24: Editar Claim para los usuarios administradores en Azure AD.....	16
<i>Ilustración 25: Inicio de sesión en Netskope (Admin Console) .....</i>	16
<i>Ilustración 26: Añadir configuración SAML en Netskope .....</i>	16

# 1. Provisión de usuarios Netskope SCIM

## 1.1. Creación del Token OAuth en Netskope<sup>1</sup>

1.1.1. Iniciar sesión en la consola de administración de Netskope:

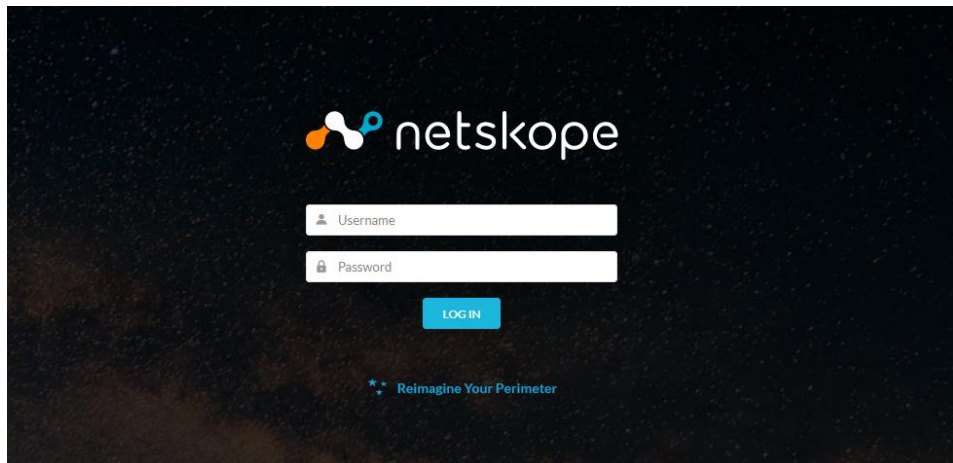


Ilustración 1: Inicio de sesión en Netskope (Provisión identidades)

1.1.2. Crear el *Token OAuth* para la integración SCIM desde **Settings > Tools > Directory Tools > SCIM Integration > Add Token**

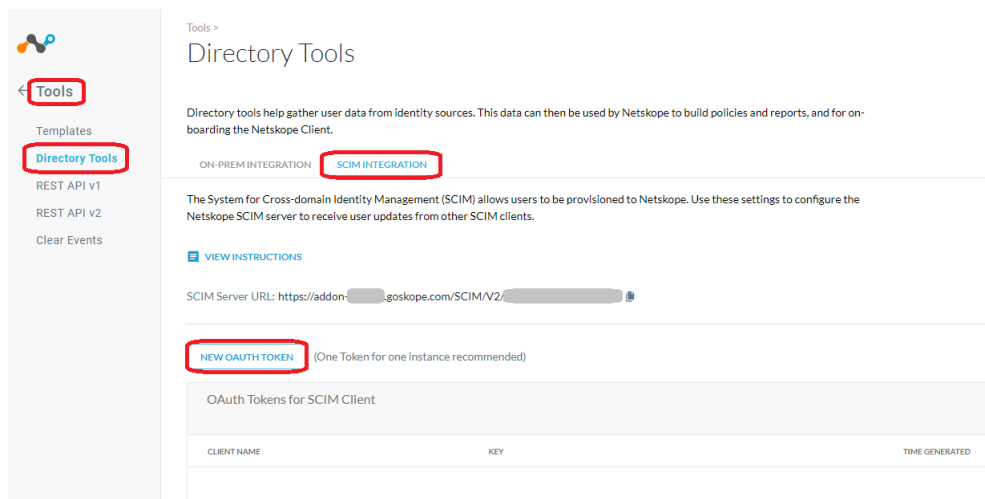


Ilustración 2: Creación Token OAuth (Provisión identidades)

<sup>1</sup> <https://docs.netskope.com/en/configure-netskope-oauth-token-for-azure-scim-integration.html>

1.1.3. Una vez generado el *OAuth Token* será utilizado en el siguiente punto para que Azure AD pueda conectarse a la API SCIM de Netskope y sincronizar información de identidades.

## 1.2. Crear aplicación empresarial en Azure AD<sup>2</sup>

1.2.1. Iniciar sesión en el *tenant* de Azure y dirigirse a la consola de *Active Directory Admin Service*: <https://aad.portal.azure.com>

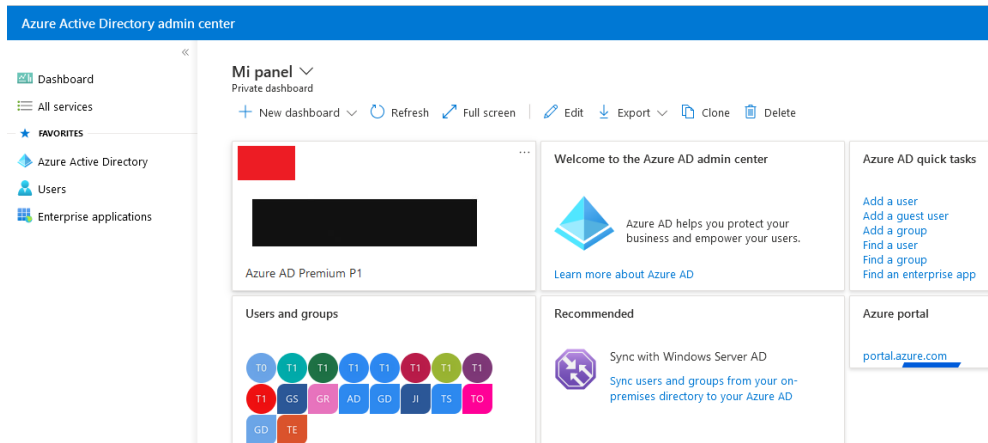


Ilustración 3: Acceso al portal Azure (Provisión identidades)

1.2.2. Crear la aplicación de aprovisionamiento de identidades con nombre **Netskope SCIM** dentro de **Enterprise applications > New Application**:

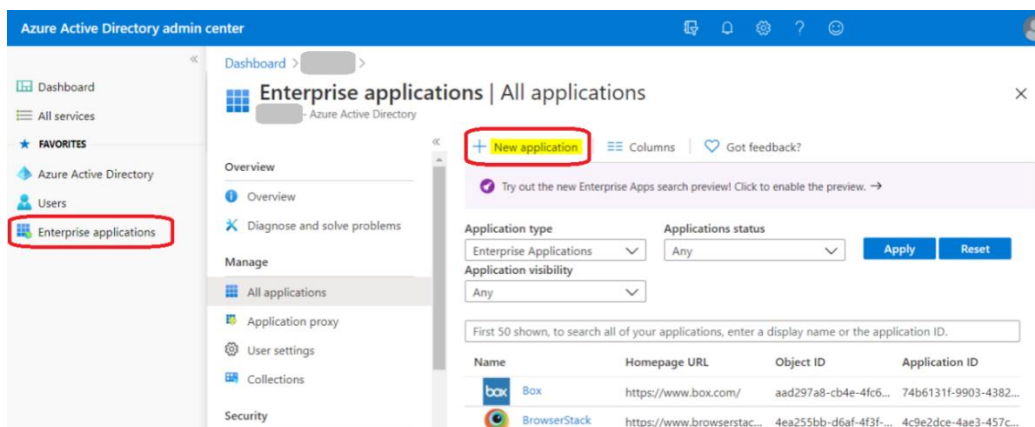


Ilustración 4: Añadir aplicación empresarial SCIM (Provisión identidades)

1.2.3. Buscar la aplicación **Netskope User Authentication** en la lista:

<sup>2</sup> <https://docs.netskope.com/en/user-provisioning-with-azure-ad.html>

## Browse Azure AD Gallery

+ Create your own application | Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Azure AD Gall

Netskope User Authentication x Single Sign-on : All User Account Management : All Categories : All

Federated SSO Provisioning

Showing 2 of 2 results

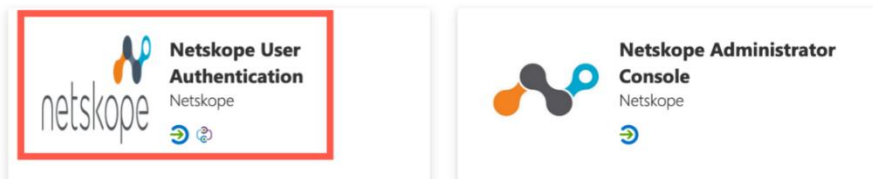


Ilustración 5: Búsqueda aplicación Netskope User Autenticación (Provisión identidades)

- 1.2.4. Añadir el nombre de la aplicación que será **Netskope SCIM** y seguidamente añadir con el botón **Add**.
- 1.2.5. Dentro de la aplicación empresarial **Netskope SCIM** dirigirse a **Provisioning** y añadir el *Token OAuth* obtenido en la sección anterior de la siguiente manera:

## Provisioning

Save Discard

This provisioning connector is in preview. Please click here to provide us feedback.

Provisioning Mode

Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Netskope SCIM based on user and group assignment.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to Netskope SCIM's API and synchronize user data.

Tenant URL \* ⓘ

https://addon[redacted].goskope.com/SCIM/V2/[redacted]

Secret Token

[redacted]

^ Mappings


Mappings  
Mappings allow you to define how data should flow between Azure Active Directory and Netskope.


Name	Enabled
<a href="#">Provision Azure Active Directory Groups</a>	Yes
<a href="#">Provision Azure Active Directory Users</a>	Yes


Restore default mappings

---

^ Settings

Send an email notification when a failure occurs  
Notification Email 

Prevent accidental deletion   
Accidental deletion threshold

Scope 

Sync only assigned users and groups

Ilustración 6: Provisioning de aplicación empresarial (Provisión identidades)

1.2.6. Activar el provisionado estableciendo el **Provisioning status** con el valor a **On**

1.2.7. Añadir las identidades que se quieran provisionar desde dentro de la aplicación empresarial **Netskope SCIM > Users and Groups**:

1.2.8. Añadir a los grupos GS\_AZUREAD\_NETSKOPE y GS\_AZUREAD\_NETSKOPE\_ADMINS:


Display Name	Object Type
<input type="checkbox"/>  GS_AZUREAD_NETSKOPE_ADMINS	Group
<input type="checkbox"/>  GS_AZUREAD_NETSKOPE_USERS	Group

Ilustración 7: Grupos de provisioning (Provisión identidades)

## 1.3. Comprobación del provisionado en Netskope

1.3.1. Comprobar el provisionado de los grupos dentro del menú **Security Cloud Platform > Groups**:

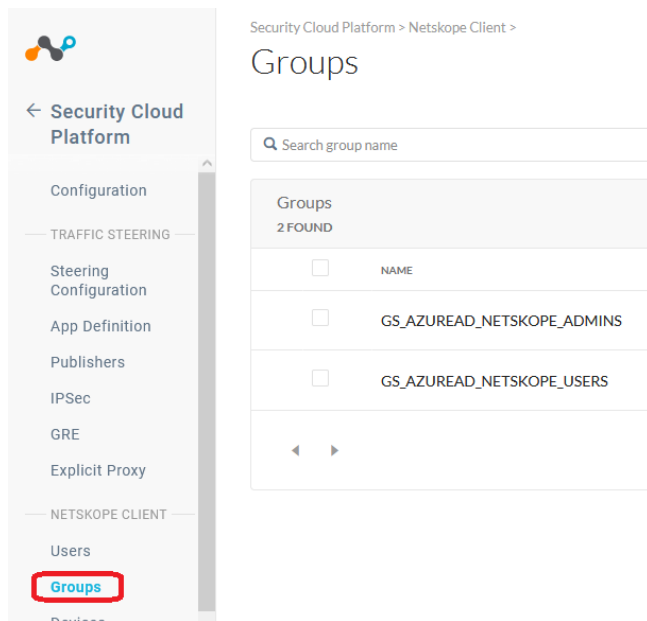


Ilustración 8: Grupos provisionados en Netskope (Provisión identidades)

1.3.2. Todas las identidades miembros de los anteriores grupos podrán ser utilizadas en Netskope para poder crear políticas de seguridad.



## 2. Autenticación SAML para Netskope Forward Proxy

### 2.1. Obtener Configuración SAML de Netskope<sup>3</sup>

2.1.1. Dirigirse a la consola de administración de Netskope, Settings > **Security Cloud Platform** > **Forward Proxy** > **SAML**:

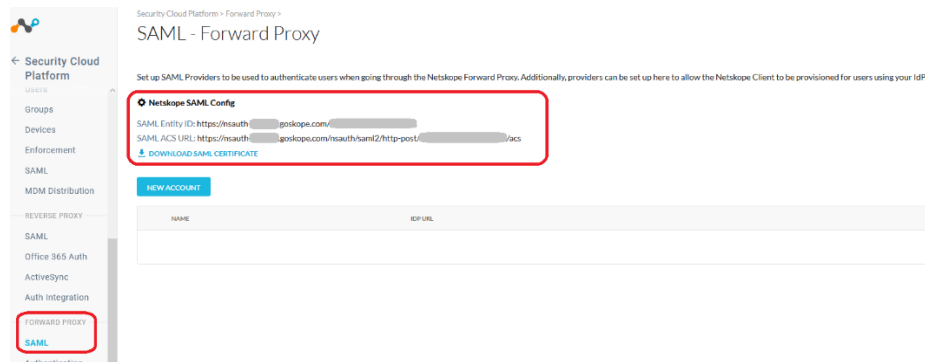


Ilustración 9: Configuración SAML Forward Proxy de Netskope

2.1.2. Guardarse estos valores para poder posteriormente configurar el SSO en la aplicación empresarial de Azure AD.

### 2.2. Configurar aplicación empresarial de Azure AD<sup>4</sup>

2.2.1. Dirigirse a la aplicación empresarial Netskope SCIM creada en el provisionado de identidades anteriormente, **Netskope SCIM** > **Single Sign On** > **Basic SAML Configuration** > **Edit**

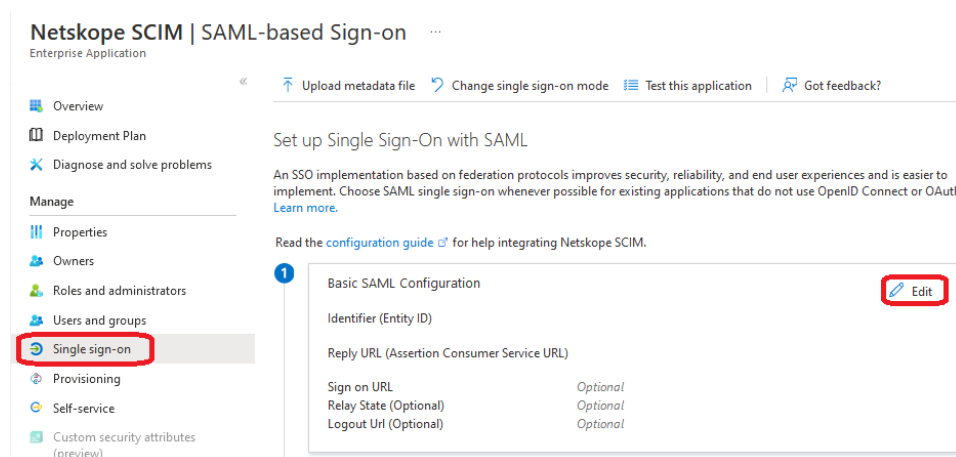


Ilustración 10: Configuración SAML de aplicación Netskope SCIM en Azure AD

<sup>3</sup> <https://docs.netskope.com/en/get-netkskope-saml-settings.html>

<sup>4</sup> <https://docs.netskope.com/en/configure-an-enterprise-application-in-microsoft-azure-active-directory-for-saml-auth.html>

2.2.2. Introducir la información obtenida de la configuración de SAML de Netskope y añadirla en los campos **Entity ID** y **Reply URL (Assertion Consumer Service)**:

### Basic SAML Configuration

Save | Got feedback?

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) \* ⓘ  
The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default  
https://nsauth-...gосkope.com/... ✓ ⓘ 🗑️  
Add identifier  
Patterns: netskope-customertenant-specific-value

Reply URL (Assertion Consumer Service URL) \* ⓘ  
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default  
https://nsauth-...gосkope.com/nsauth/saml2/http-post/... ✓ ✓ ✓ ⓘ 🗑️  
Add reply URL  
Patterns: https://nsauth-<TENANT>.gосkope.com/nsauth/saml2/http-post/<CUSTOM\_STRING>

Ilustración 11: Edición de configuración SAML de aplicación Netskope SCIM en Azure AD

2.2.3. Descargar el certificado en formato Base64 y copiar los campos **Login URL** y **Azure ID Identifier** para poder posteriormente configurar el forward proxy de Netskope:

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Self-service

3

### SAML Certificates

Token signing certificate		<a href="#">Edit</a>
Status	Active	
Thumbprint	...	
Expiration	10/10/2025, 9:59:25 AM	
Notification Email	...	
App Federation Metadata Url	https://login.microsoftonline.com/...	
<b>Certificate (Base64)</b>	<a href="#">Download</a>	
Certificate (Raw)	<a href="#">Download</a>	
Federation Metadata XML	<a href="#">Download</a>	

Ilustración 12: Descarga certificado Base 64 de SAML

## 2.3. Añadir una cuenta de Azure AD en Netskope<sup>5</sup>

2.3.1. Iniciar sesión en la consola de administración de Netskope:

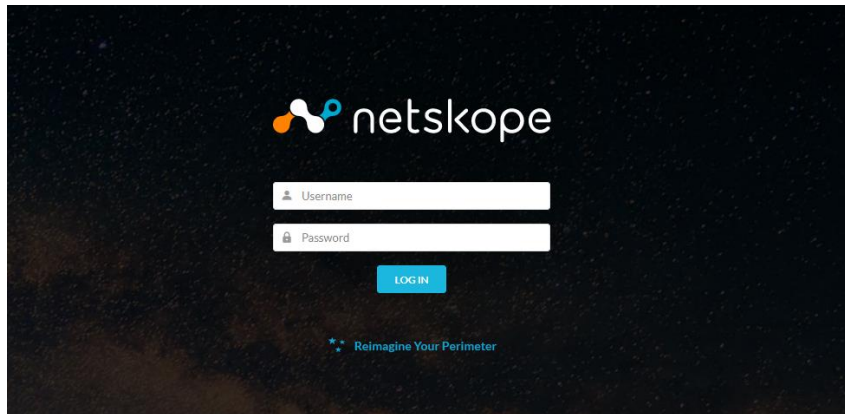


Ilustración 13: Inicio de sesión de Netskope (Forward Proxy)

2.3.2. Dirigirse a **Settings > Security Cloud Platform > Forward Proxy > SAML** y seleccionar **New Account**, especificar un nombre AzureAD e introducir la información del **Login URL**, **Azure ID Identifier** y el certificado en formato Base64 obtenidos de la anterior sección:

Ilustración 14: Nueva cuenta SSO en Netskope (Forward Proxy)

2.3.3. Se comprueba que la cuenta se ha creado correctamente:

<sup>5</sup> <https://docs.netskope.com/en/add-an-azure-ad-account-in-netskope-saml---forward-proxy.html>

⚙️ Netskope SAML Config

SAML Entity ID: <https://nsauth-tous.eu.goskope.com/a89OI97mgnk3r54v4jA>

SAML ACS URL: <https://nsauth-tous.eu.goskope.com/nsauth/saml2/http-post/a89OI97mgnk3r54v4jA/acs>

[📄 DOWNLOAD SAML CERTIFICATE](#)

[NEW ACCOUNT](#)

NAME	IDP URL
AzureAD	<a href="https://login.microsoftonline.com/[redacted]/saml2">https://login.microsoftonline.com/[redacted]/saml2</a>

Ilustración 15: Comprobación nueva cuenta SSO en Netskope (Forward Proxy)

## 3. Autenticación SAML para Netskope Admin Console

### 3.1. Obtener la configuración de Netskope para el SSO

3.1.1. Iniciar sesión en la consola de administración de Netskope:

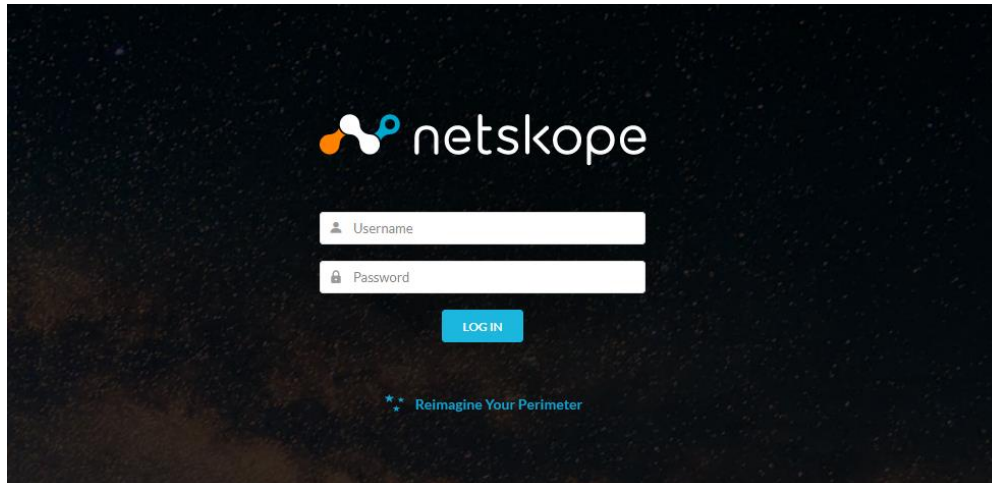


Ilustración 16: Inicio de sesión de Netskope (Admin console)

3.1.2. Obtener la configuración de SSO de Netskope SSO para poder configurar una aplicación empresarial en Azure AD:

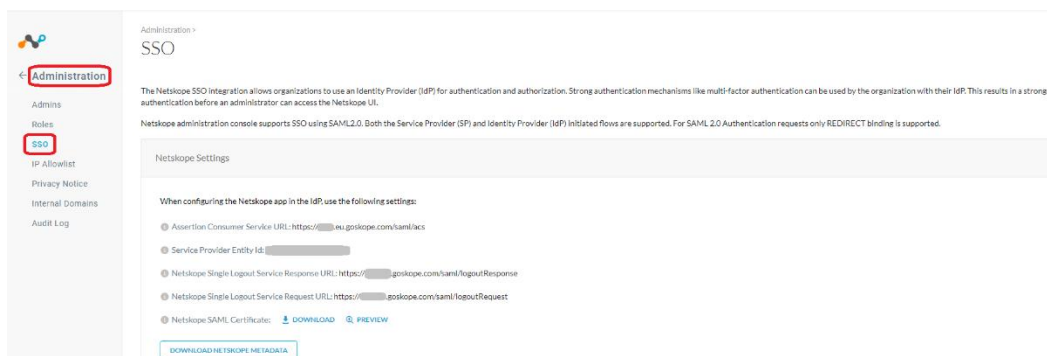


Ilustración 17: Obtener información SSO de Netskope (Admin console)

### 3.2. Crear la aplicación empresarial para Netskope Admin Console en Azure AD

3.2.1. Iniciar sesión en el *tenant* de Azure y dirigirse a la consola de *Active Directory Admin Service*: <https://aad.portal.azure.com>

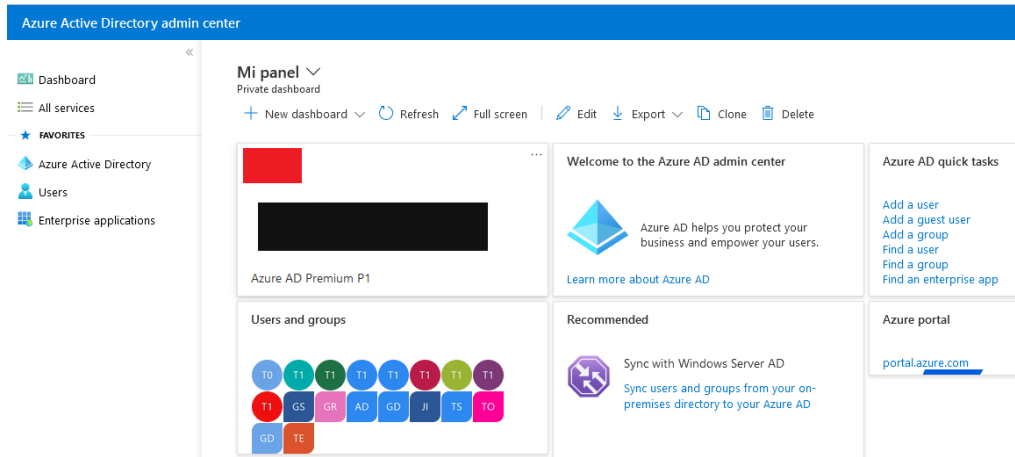


Ilustración 18: Añadir aplicación empresarial Netskope Administracion Console

### 3.2.2. Crear la aplicación de aprovisionamiento de identidades con nombre **Netskope Administration Console** dentro de **Enterprise applications > New Application**:

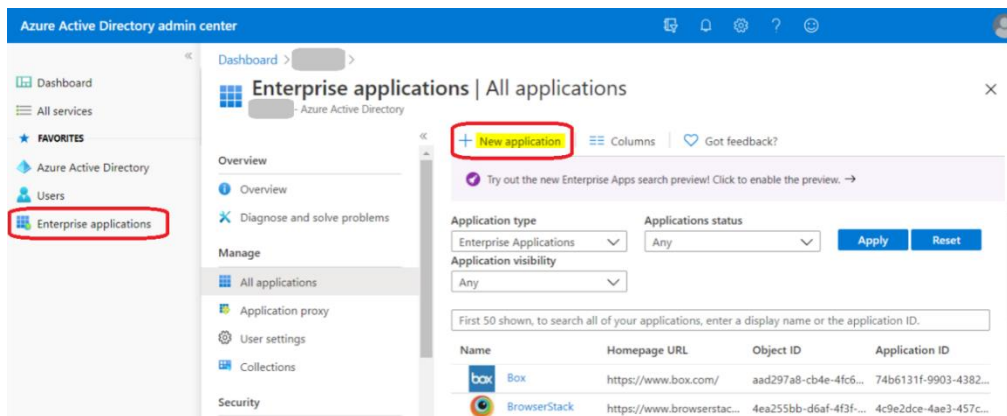


Ilustración 19: Crear nueva aplicación empresarial en Azure AD

### 3.2.3. Buscar la aplicación **Netskope Administration Console** en la lista:

## Browse Azure AD Gallery

+ Create your own application | Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Azure AD Gall

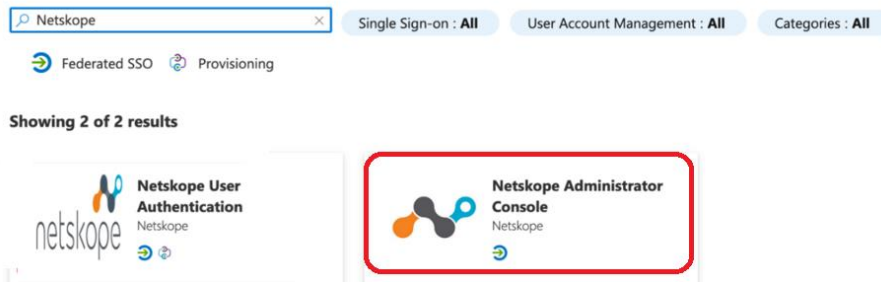


Ilustración 20: Crear nueva aplicación empresarial Netskope Administration Console

3.2.4. Añadir el nombre de la aplicación que será **Netskope Administration Console** y seguidamente añadir con el botón **Add**.

3.2.5. Dentro de la aplicación empresarial Netskope Administration Console dirigirse a **Single sign-on > Basic SAML Configuration > Edit**

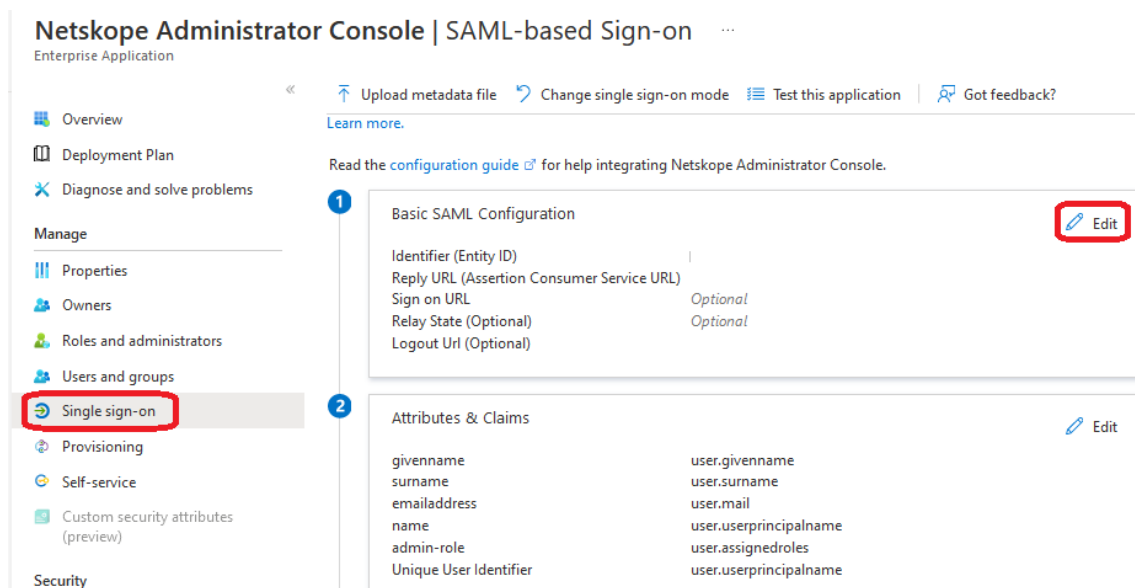


Ilustración 21: Editar SAML de aplicación Netskope Administration Console en Azure AD

3.2.6. Configurar el SAML con la configuración obtenida del SSO de Netskope:

## Basic SAML Configuration

Save | Got feedback?

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) \*

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

gskope.com

Add identifier

Patterns: https://\*.gskope.com

Reply URL (Assertion Consumer Service URL) \*

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

https://\*.gskope.com/saml/acs

Add reply URL

Patterns: https://<TENANTNAME>.gskope.com/saml/acs

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

https://\*.gskope.com/saml/logoutResponse

Ilustración 22: Edición de SAML de aplicación Netskope Administration Console en Azure AD

- 3.2.7. Añadir el grupo de administradores GS\_AZUREAD\_NETSKOPE\_ADMINS, este grupo contendrá los usuarios que podrán administrar la consola de Netskope a través de SSO, para ello es necesario dirigirse dentro de la aplicación **Netskope Administration Console > User and groups > Add user/group**

Netskope Administrator Console | Users and groups ...

Enterprise Application

Overview  
Deployment Plan  
Diagnose and solve problems

Manage

Properties  
Owners  
Roles and administrators  
**Users and groups**  
Single sign-on  
Provisioning

+ Add user/group | Edit | Remove | Update Credentials | Columns | Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & groups, enter a display name.

	Display Name	Object Type
<input type="checkbox"/>	GS GS_AZUREAD_NETSKOPE_ADMINS	Group

Ilustración 23: Seleccionar grupo para autenticar en Netskope Administration Console

- 3.2.8. Añadir el *claim* para el *tenant* de Netskope, dentro de **Manage Claim**, seleccionar el grupo **GS\_AZUREAD\_NETSKOPE\_ADMINS** y selecciona el valor **"Tenant Admin"**:



**Manage claim** ...

Save | Discard changes | Get feedback?

Name:

Namespace:

Choose name format (Preview)

Source:  Attribute  Transformation

Source attribute:

Claim conditions

Returns the claim only if all the conditions below are met.

Multiple conditions can be applied to a claim. When adding conditions, order of operation is important. [Read the documentation](#) for more information.

User type:  | Scopes:  | Source:  Attribute  Transformation | Value:

Ilustración 24: Editar Claim para los usuarios administradores en Azure AD

### 3.3. Añadir la configuración SSO de Azure en el tenant de Netskope

#### 3.3.1. Iniciar sesión en la consola de administración de Netskope:

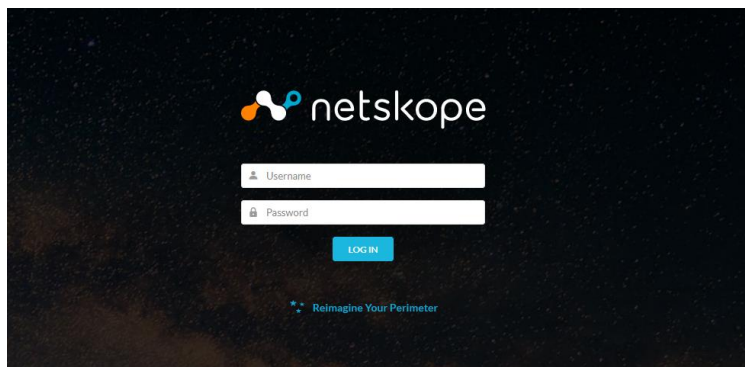


Ilustración 25: Inicio de sesión en Netskope (Admin Console)

#### 3.3.2. Dirigirse a **Settings > Administration > SSO** y crear una configuración

#### 3.3.3. Añadir la configuración del SSO de Azure AD obtenida de la aplicación empresarial **Netskope Administration Console**:

Settings

SSO

Enable SSO

Sign SSO Authentication Request

Disable Force Authentication

IDP URL:

IDP ENTITY ID:

IDP CERTIFICATE:

SLO

Enable SLO

Sign SLO Request/Response

ADFS?

CANCEL | SUBMIT

Ilustración 26: Añadir configuración SAML en Netskope