

---

## How to Configure Allowed VPN User Groups

<https://campus.barracuda.com/doc/94539562/>

Barracuda CloudGen WAN allows you to restrict access to the [User Connectivity & Personal Security](#) feature based on users and groups.

### Before You Begin

---

- Synchronize your Azure Active Directory with Barracuda Cloud Control. For more information, see [How to Connect Your Azure Active Directory with Barracuda Cloud Control](#).
- Create a SAML endpoint in Microsoft Azure and provide a basic configuration of the User Connectivity & Personal Security feature. For more information, see [How to Create a SAML Endpoint in Microsoft Azure and Basic User Connectivity & Personal Security Configuration](#).

### Step 1. Group Claims in Microsoft Azure

---

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and search for **Azure Active Directory**.
3. Click **Azure Active Directory**.
4. In the left menu of the **Azure Active Directory** blade, click **Enterprise applications**.

Home >

## cudazure | Overview

Azure Active Directory

Overview

Getting started

Preview hub

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units


**Enterprise applications**

Devices

Switch tenant

Delete tenant

+

 Azure Active Directory can help you enable more

### cudazure

Search your tenant

Tenant information

Your role  
Global administrator [More info](#)

License  
Azure AD Premium P2

Tenant ID

5. In the **Enterprise applications** blade, click **All applications**.
6. Click on the application you created, e.g., Campus-SAML-Endpoint.
7. Click **Single sign-on**.
8. The **Set up Single Sign-On with SAML** blade opens.
9. In the **User Attributes & Claims** section, click **Edit**.

Home > cudazure > Enterprise applications > Campus-SAML-Endpoint >

### Campus-SAML-Endpoint | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

**Single sign-on**

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption

Upload metadata file

Change single sign-on mode

Test this application

Got feedback?

#### Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Campus-SAML-Endpoint.

1

**Basic SAML Configuration**

Identifier (Entity ID)  
https://cloudgenwan.barracudanetworks.com/4126c000-7cdc-4138-98f8-cfebaa554865

Reply URL (Assertion Consumer Service URL)  
https://localhost/sso/acs

Sign on URL  
Optional

Relay State  
Optional

Logout Url  
Optional

2

**User Attributes & Claims**

givenname  
user.givenname

surname  
user.surname

emailaddress  
user.mail

name  
user.userprincipalname

Unique User Identifier  
user.userprincipalname

Edit

10. The **User Attribute and Claims** blade opens.
11. Click **Add a group claim**.

[Home](#) > [Campus-SAML-Endpoint](#) > [SAML-based Sign-on](#) >

## User Attributes & Claims

[+ Add new claim](#) [+ Add a group claim](#) [≡ Columns](#)

### Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***

### Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***

12. The **Group claim blade** opens. Specify values for the following:

- **Which groups associated with the user should be returned in the claim?** – Select **Security groups**.
- **Source attribute** – Select **Group ID**.

## Group Claims

×

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

☐ None

☐ All groups

☒ Security groups

☐ Directory roles

☐ Groups assigned to the application

Source attribute \*

Group ID

### Advanced options

☐ Customize the name of the group claim

Name (required)

Namespace (optional)

☐ Emit groups as role claims ⓘ

Save

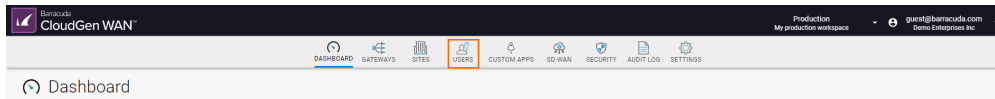
13. Click **Save**.

## Step 2. Configuration in Barracuda CloudGen WAN

1. Go to <https://cloudgenwan.barracudanetworks.com/> and log in with your existing Barracuda

Cloud Control account.

2. Click **USERS**.



3. The **Personal Access** window opens.


4. Go to the **AZURE AD INTEGRATION** section.

- **Allowed VPN User Group** - Type to search for users or groups you want to grant permission to use [Personal Access](#). Only users and groups added here are allowed to use Personal Access.


**AZURE AD INTEGRATION**

To configure Point-to-Site VPN, you must connect CloudGen WAN to your Azure AD Enterprise App, by exchanging metadata below.

*i* Service Provider Metadata

 **DOWNLOAD METADATA**

*i* Enterprise App Federation Metadata Url \*

 **RE-SYNC**

To use Site Authentication and User/Group rules in Security, you must configure and sync your Azure AD into your Barracuda Account [here](#). Instructions for setting up Azure AD in Barracuda can be found [here](#).

*i* Allowed VPN User Group

5. Click **Save**.

## Further Information

- For more information on Personal Access and Site Authentication, see [User Connectivity & Personal Security](#).

## Figures

1. ent\_app.png
2. edit\_user\_claim.png
3. add\_group\_claim.png
4. group\_claim.png
5. main\_menu82.png
6. allowed\_vpn.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.