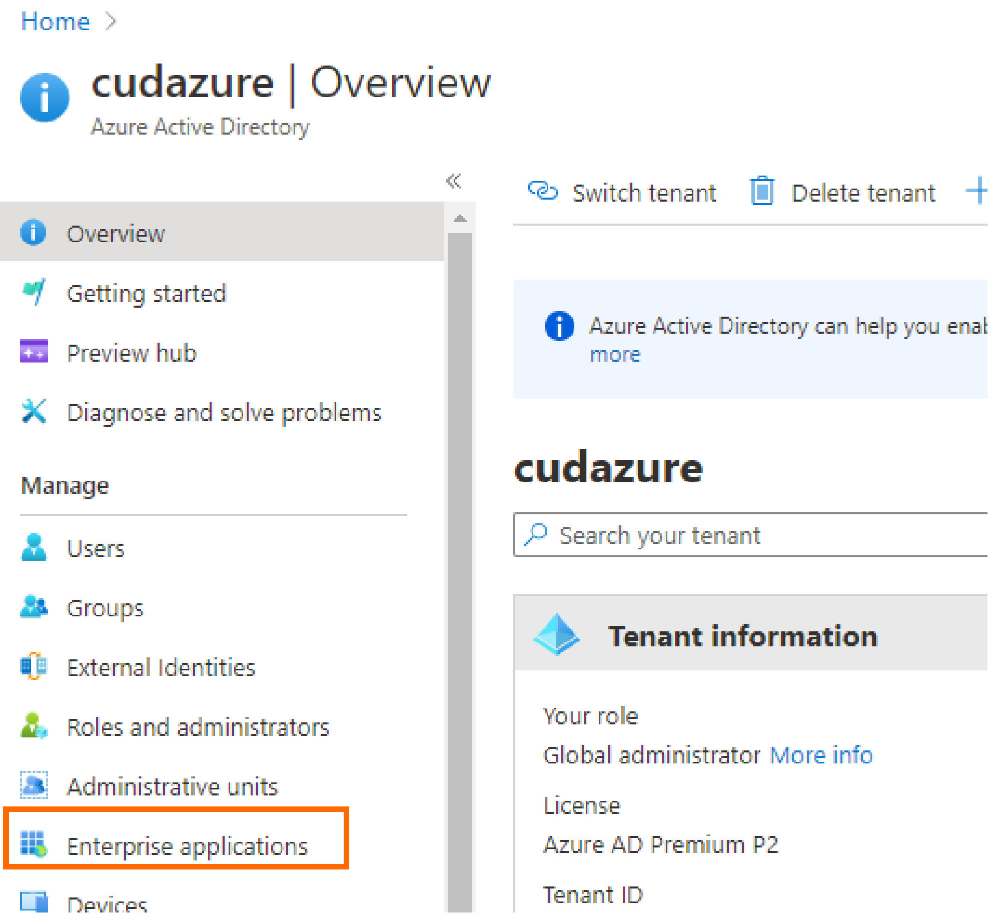
# How to Create a SAML Endpoint in Microsoft Azure and Basic User Connectivity & Personal Security Configuration

https://campus.barracuda.com/doc/94539352/

For Barracuda CloudGen WAN User Connectivity & Personal Security, you must configure a SAML endpoint in Microsoft Azure. In order to save the SAML configuration in Barracuda CloudGen WAN, you must also provide basic configuration details for User Connectivity & Personal Security.

## Step 1. Create a SAML Endpoint in Microsoft Azure

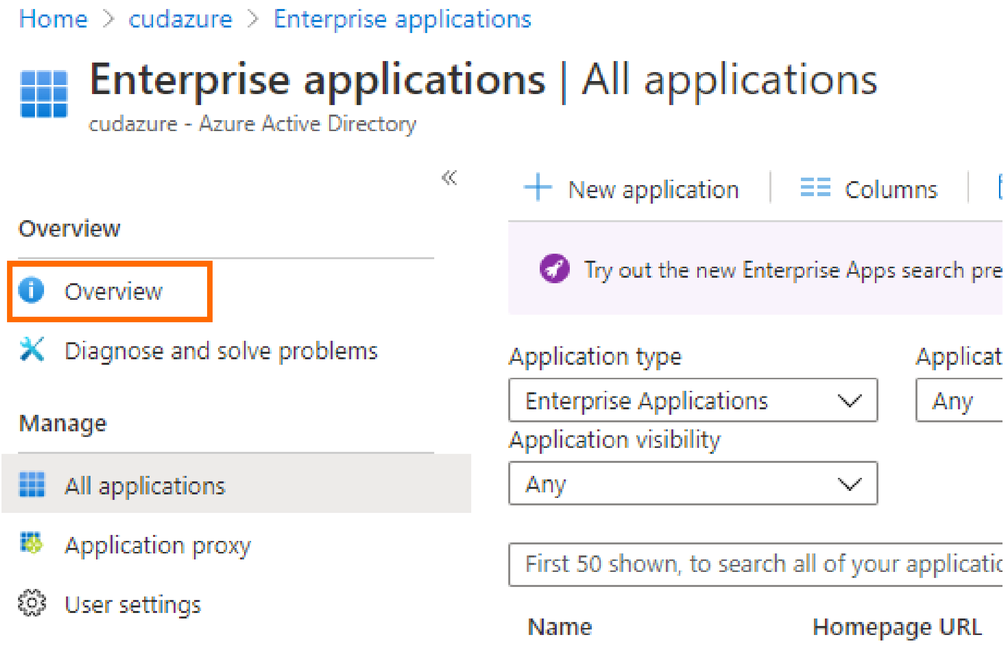
1. Log into the Azure portal: https://portal.azure.com
2. In the left menu, click **All services** and search for **Azure Active Directory**.
3. Click **Azure Active Directory**.
4. In the left menu of the **Azure Active Directory** blade, click **Enterprise applications**.



Your role
Global administrator More info

License
Azure AD Premium P2

5. In the **Enterprise applications** blade, click **Overview**.



Home > cudazure > Enterprise applications

Enterprise applications | All applications

cudazure - Azure Active Directory

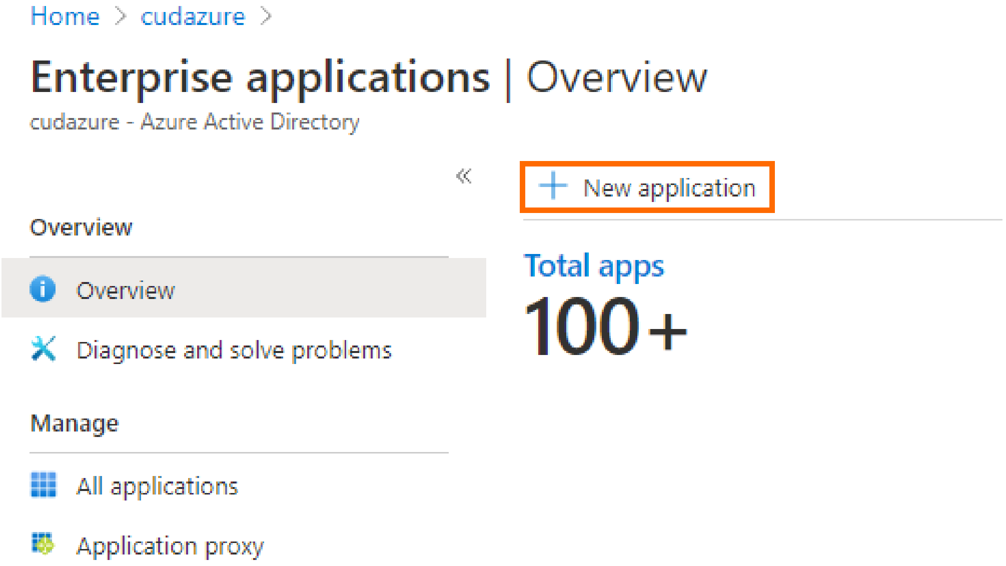
Application type: Enterprise Applications

Applicat: Any

Application visibility: Any

First 50 shown, to search all of your applicatic

6. In the **Overview** blade, click **+ New application**.



Home > cudazure >

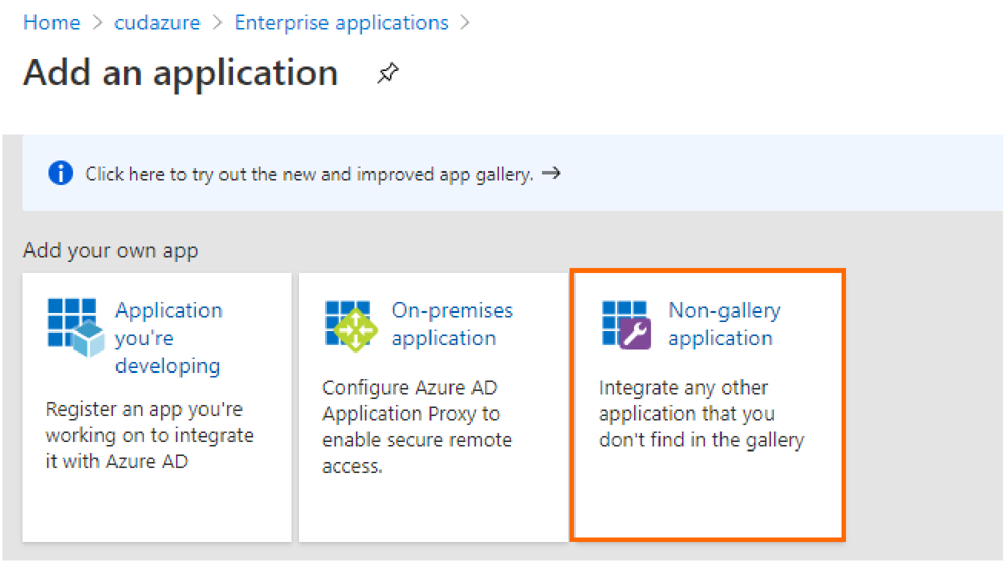
Enterprise applications | Overview

cudazure - Azure Active Directory

Total apps

100+

7. The **Add an application** blade opens. Select **Non-gallery application**.



Home > cudazure > Enterprise applications >

Add an application

Click here to try out the new and improved app gallery. →

Add your own app

Application you're developing

Register an app you're working on to integrate it with Azure AD

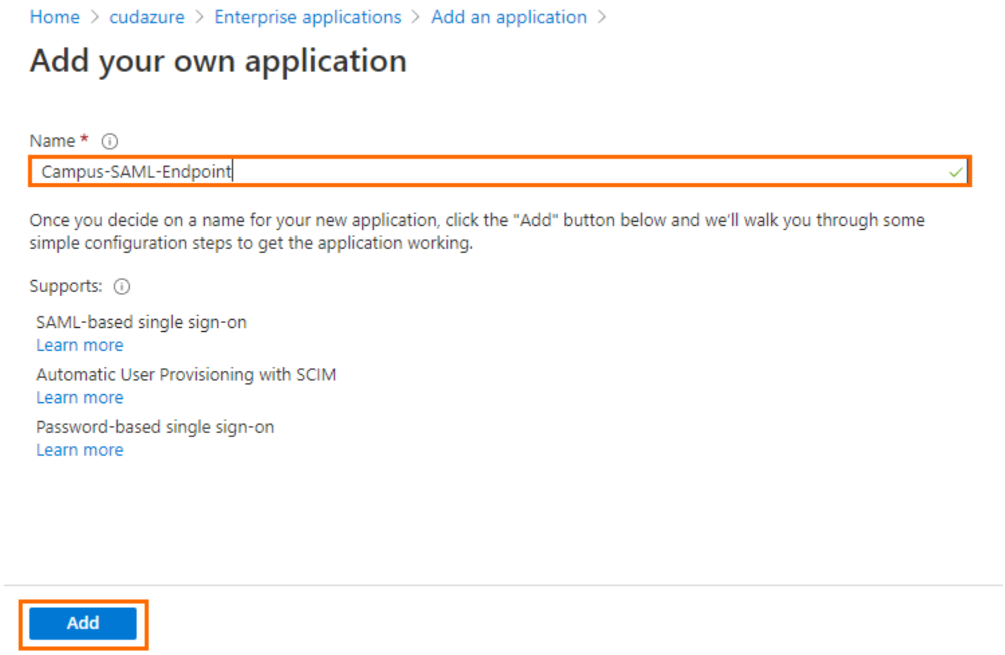
On-premises application

Configure Azure AD Application Proxy to enable secure remote access.

Non-gallery application

Integrate any other application that you don't find in the gallery

8. The **Add your own application blade** opens. Enter a name for the application, e.g., `Campus-SAML-Endpoint` and click **Add** .



Home > cudazure > Enterprise applications > Add an application >

Add your own application

Name *

Campus-SAML-Endpoint

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

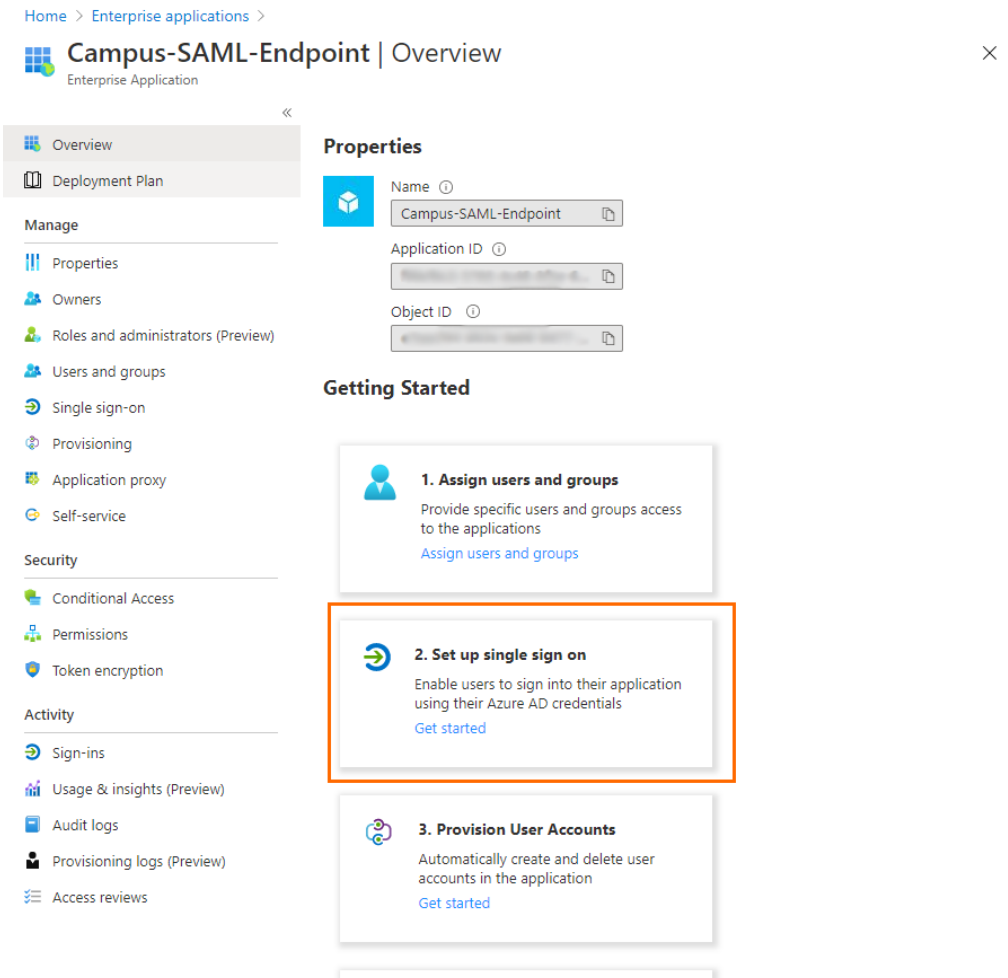
Supports:

SAML-based single sign-on
Learn more

Automatic User Provisioning with SCIM
Learn more

Password-based single sign-on
Learn more

9. After the deployment of the application is finished, open your application.
10. In the **Enterprise applications** blade, click **All applications**.
11. Click on the application you just created, e.g., Campus-SAML-Endpoint.
12. The application **Overview** blade opens. Click **2. Set up single sign on** .



Home > Enterprise applications >

Campus-SAML-Endpoint | Overview

Enterprise Application

**Properties**

Name: Campus-SAML-Endpoint

Application ID: [redacted]

Object ID: [redacted]

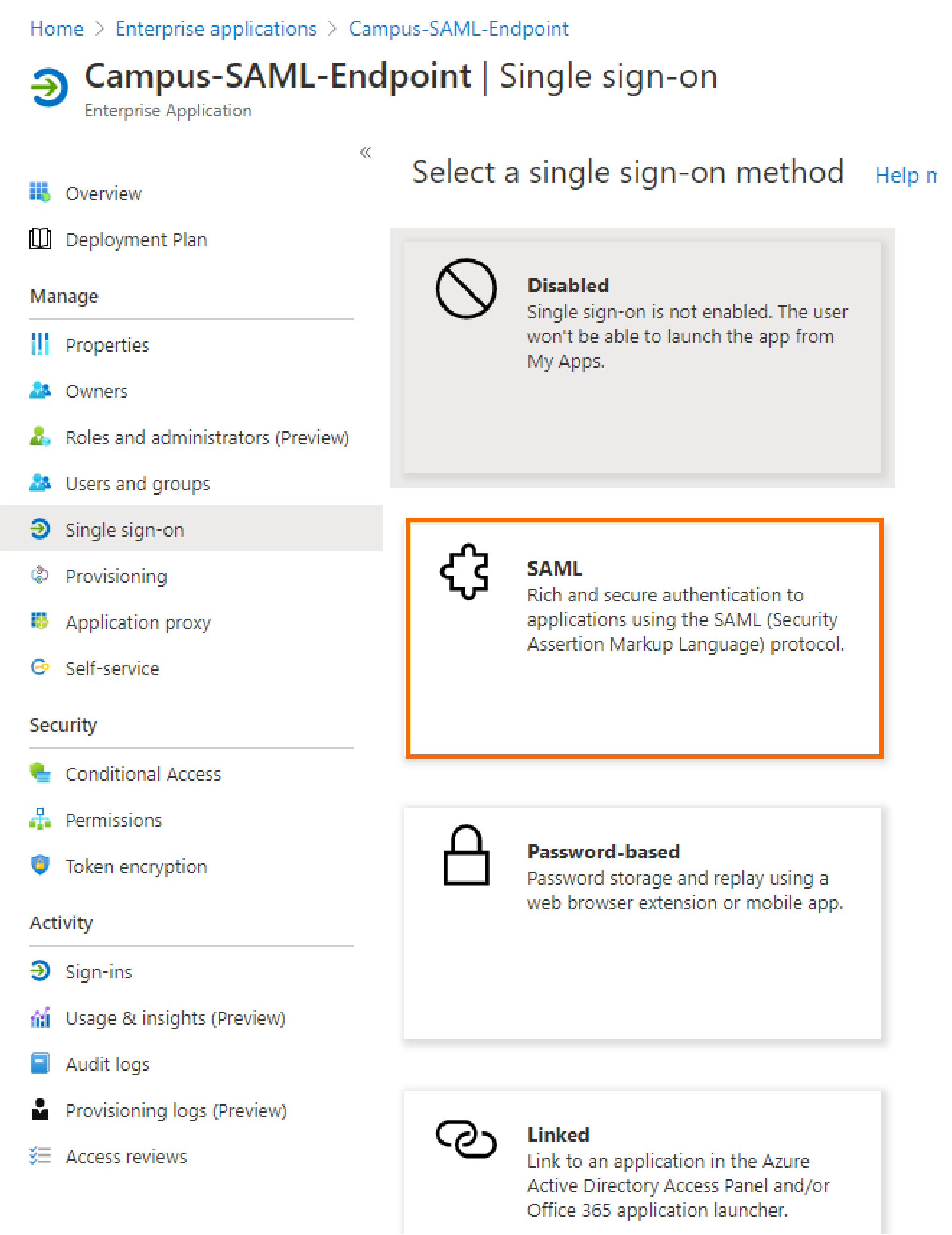
**Getting Started**

**1. Assign users and groups**
Provide specific users and groups access to the applications
Assign users and groups

**2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
Get started

**3. Provision User Accounts**
Automatically create and delete user accounts in the application
Get started

13. The **Single sign-on** blade opens. Click **SAML** .



Campus-SAML-Endpoint | Single sign-on

Enterprise Application

Select a single sign-on method

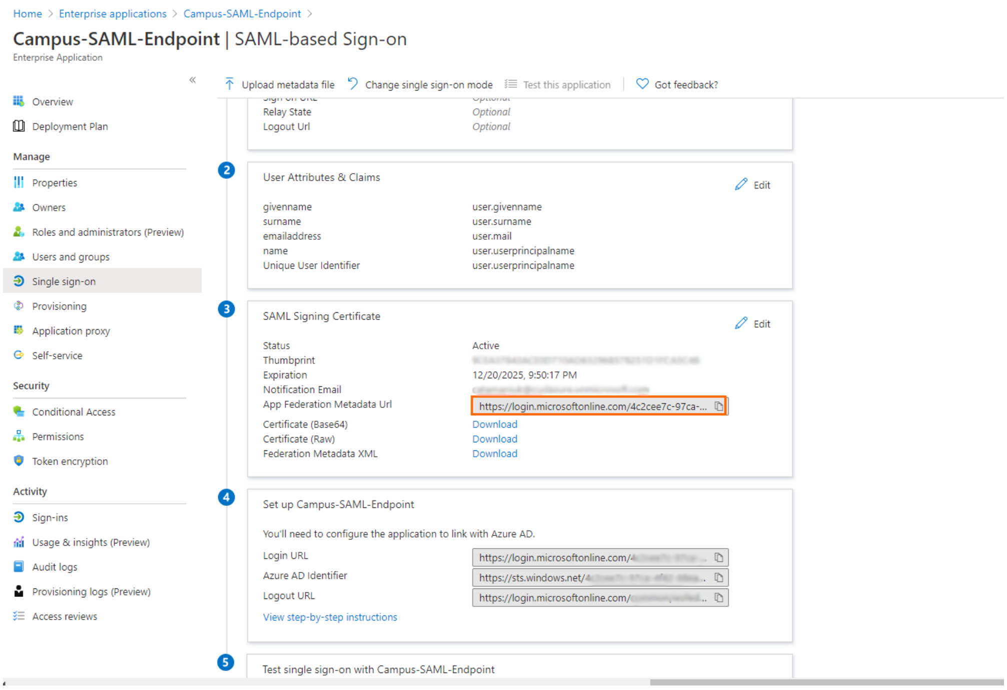
**Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

**SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

**Password-based**
Password storage and replay using a web browser extension or mobile app.

**Linked**
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

14. Copy the **App Federation Metadata Url** to your clipboard.



**Campus-SAML-Endpoint** | SAML-based Sign-on
Enterprise Application

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

3 SAML Signing Certificate

Status: Active
Thumbprint: [redacted]
Expiration: 12/20/2025, 9:50:17 PM
Notification Email: [redacted]
App Federation Metadata Url: https://login.microsoftonline.com/4c2cee7c-97ca-...
Certificate (Base64): Download
Certificate (Raw): Download
Federation Metadata XML: Download

4 Set up Campus-SAML-Endpoint

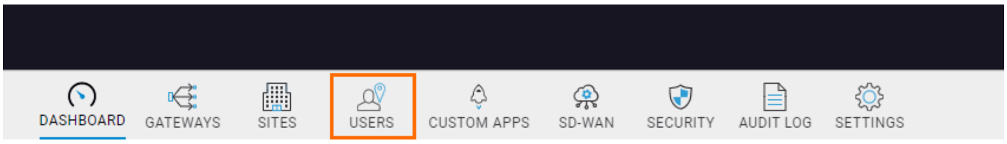
You'll need to configure the application to link with Azure AD.

Login URL: https://login.microsoftonline.com/4[redacted]
Azure AD Identifier: https://sts.windows.net/4[redacted]
Logout URL: https://login.microsoftonline.com/[redacted]
View step-by-step instructions

5 Test single sign-on with Campus-SAML-Endpoint

## Step 2. Basic 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**.

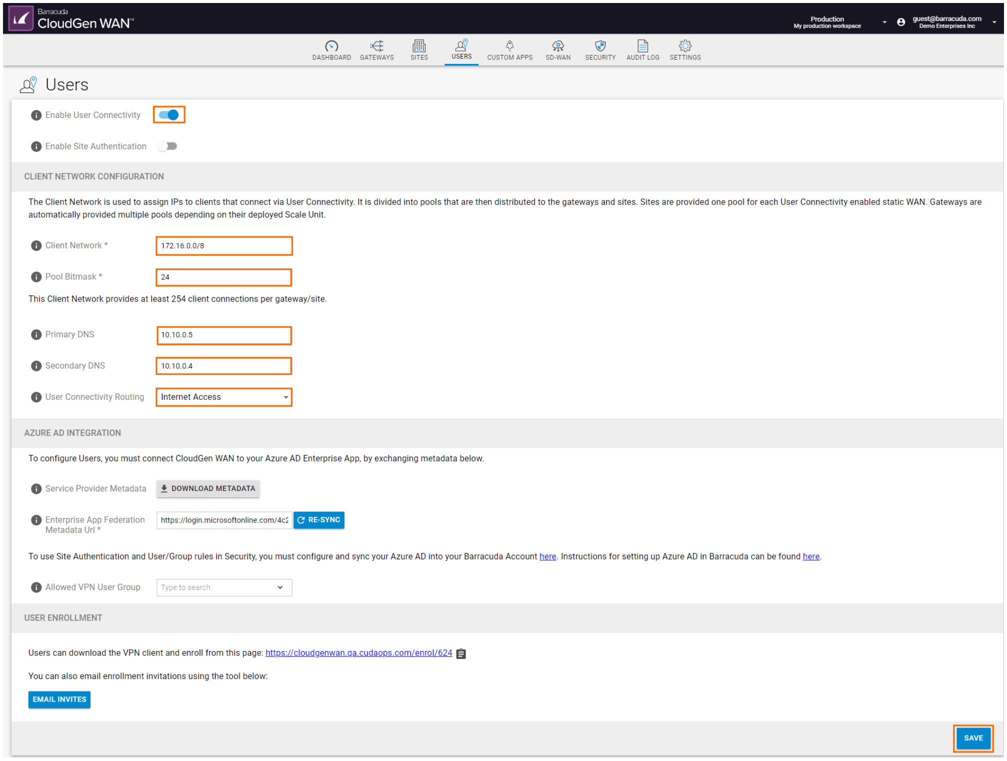


3. The **USERS** window opens. Specify values for the following:
   - **Enable Point-to-Site VPN** – Click to enable.
   - **Enable Site Autentication** – Cick to enable. Site authentication allows devices physically located within the network to authenticate against the Barracuda CloudGen WAN service to enforce Security Policies.
   - **Client Network** – Enter the network used for the clients.
   - **Pool Bitmask** – Enter the bitmask of the network pool to allocate to each VPN access point.

> Barracuda Networks recommends you to allocate an address space that is twice as large as the number of desired clients because the client network is automatically divided into pools. The pools are assigned equally to the gateways and must therefore be sized according to the largest number of clients. For example: If you have 2 gateways in 2 regions, and a large headquarters and a small branch office, both will receive an equal number of pools. For this reason, the client network must

be sized according to the size of your headquarters location.

- **Primary DNS** – Enter a primary DNS address for the VPN clients to use or leave blank to use the standard configuration.
- **Secondary DNS** – Enter a secondary DNS address for the VPN clients to use, or leave blank to use the standard configuration.
- **User Connectivity Routing** – Select either **Internal Network** or **Internet Access** from the drop-down menu. The option **Internal Network** routes only the networks learned via BGP through the CloudGen WAN gateway**,** and the option **Internet Access** sends all traffic through the gateway. **Internet Access** can be used to inspect all traffic by CloudGen WAN.
- **Enterprise App Federation Metadata Url*** – Paste the **App Federation Metadata Url** retrieved in Step 1.



Enable User Connectivity: on

Enable Site Authentication: off

CLIENT NETWORK CONFIGURATION

The Client Network is used to assign IPs to clients that connect via User Connectivity. It is divided into pools that are then distributed to the gateways and sites. Sites are provided one pool for each User Connectivity enabled static WAN. Gateways are automatically provided multiple pools depending on their deployed Scale Unit.

Client Network *: 172.16.0.0/8

Pool Bitmask *: 24

This Client Network provides at least 254 client connections per gateway/site.

Primary DNS: 10.10.0.5

Secondary DNS: 10.10.0.4

User Connectivity Routing: Internet Access

AZURE AD INTEGRATION

To configure Users, you must connect CloudGen WAN to your Azure AD Enterprise App, by exchanging metadata below.

Service Provider Metadata: DOWNLOAD METADATA

Enterprise App Federation Metadata Url *: https://login.microsoftonline.com/4c2 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.

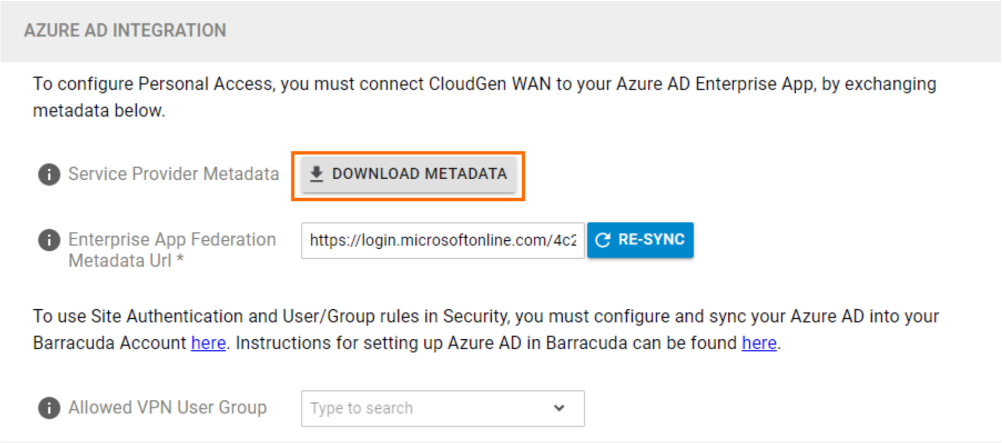
Allowed VPN User Group: Type to search

USER ENROLLMENT

Users can download the VPN client and enroll from this page: https://cloudgenwan.qa.cudaops.com/enrol/624

You can also email enrollment invitations using the tool below:

4. Click **Save**.
5. Stay in the **USERS** window.
6. Click **DOWNLOAD METADATA**.



AZURE AD INTEGRATION

To configure Personal Access, you must connect CloudGen WAN to your Azure AD Enterprise App, by exchanging metadata below.

Service Provider Metadata

Enterprise App Federation Metadata Url *: https://login.microsoftonline.com/4c2

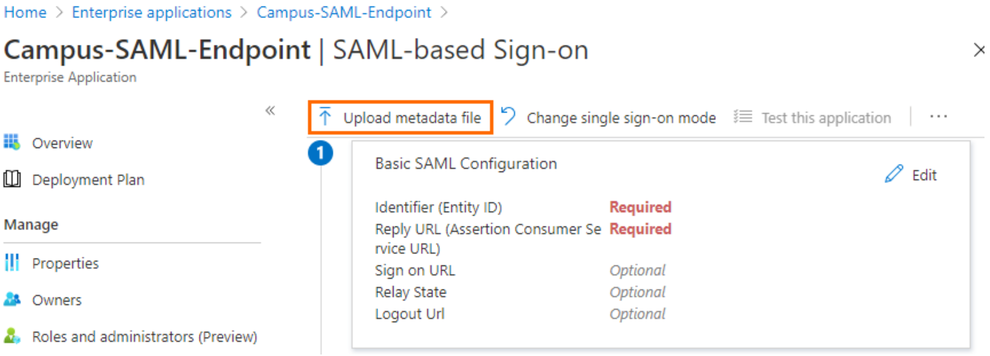
To use Site Authentication and User/Group rules in Security, you must configure and sync your Azure AD into your Barracuda Account here. Instructions for setting up Azure AD in Barracuda can be found here.

Allowed VPN User Group: Type to search

7. Save the file to your local disk.

## Step 3. Finalize SAML Configuration 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**.
5. In the **Enterprise applications** blade, click **All applications**.
6. Click on the application you created in Step 1, e.g., Campus-SAML-Endpoint.
7. In the left menu, click **Single sign-on** .
8. The **Single sign-on** blade opens.
9. Click **Upload metadata file**.



Home > Enterprise applications > Campus-SAML-Endpoint >

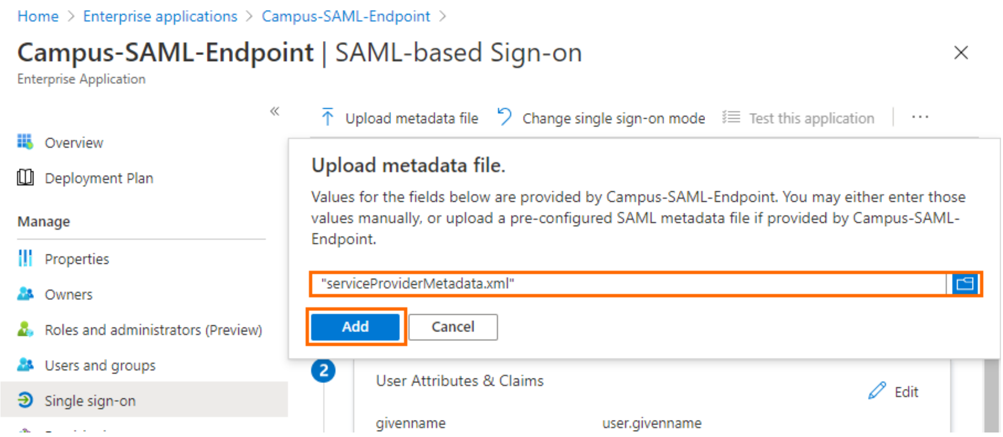
Campus-SAML-Endpoint | SAML-based Sign-on

Enterprise Application

Basic SAML Configuration

| | |
|---|---|
| Identifier (Entity ID) | Required |
| Reply URL (Assertion Consumer Service URL) | Required |
| Sign on URL | Optional |
| Relay State | Optional |
| Logout Url | Optional |

10. Select the file downloaded in Step 2 and click **Add** .

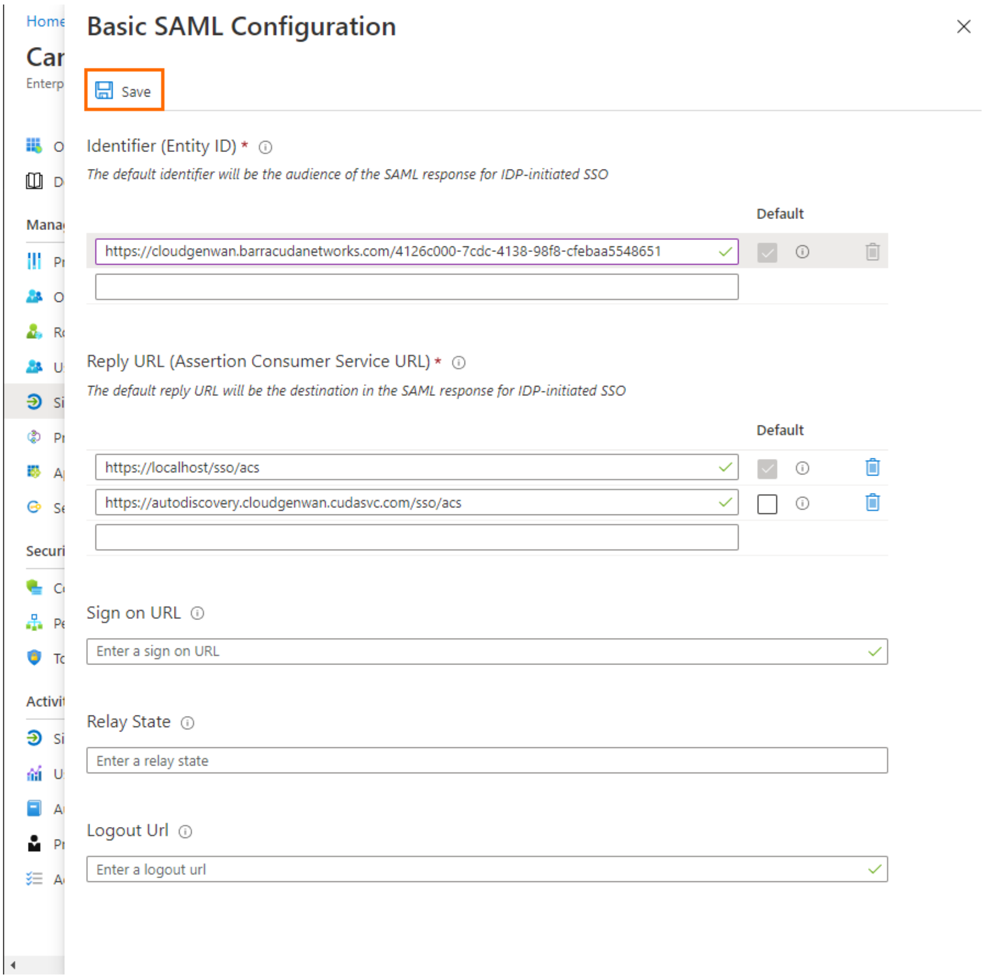


Upload metadata file.

Values for the fields below are provided by Campus-SAML-Endpoint. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by Campus-SAML-Endpoint.

"serviceProviderMetadata.xml"

11. Click **Save**.



Identifier (Entity ID) *

*The default identifier will be the audience of the SAML response for IDP-initiated SSO*

https://cloudgenwan.barracudanetworks.com/4126c000-7cdc-4138-98f8-cfebaa5548651

Reply URL (Assertion Consumer Service URL) *

*The default reply URL will be the destination in the SAML response for IDP-initiated SSO*

https://localhost/sso/acs

https://autodiscovery.cloudgenwan.cudasvc.com/sso/acs

Sign on URL

Enter a sign on URL

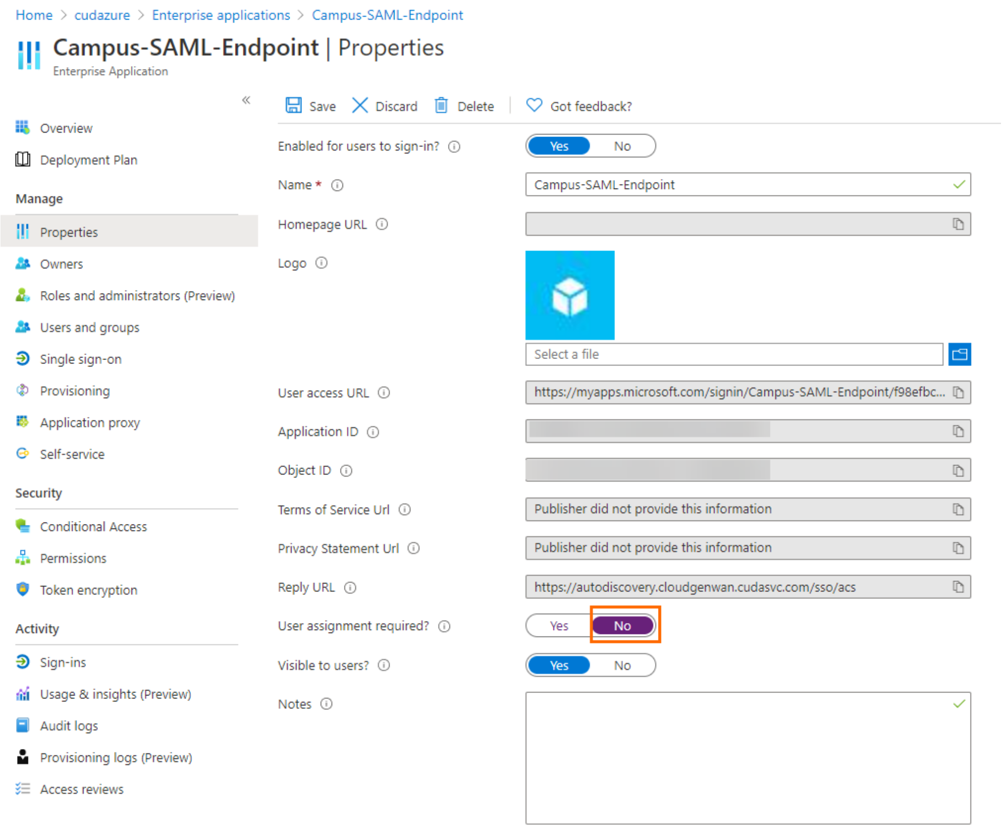
Relay State

Enter a relay state

Logout Url

Enter a logout url

12. The **Enterprise applications** blade opens.
13. Click **Properties** and set **User assignment required?** to **No**.

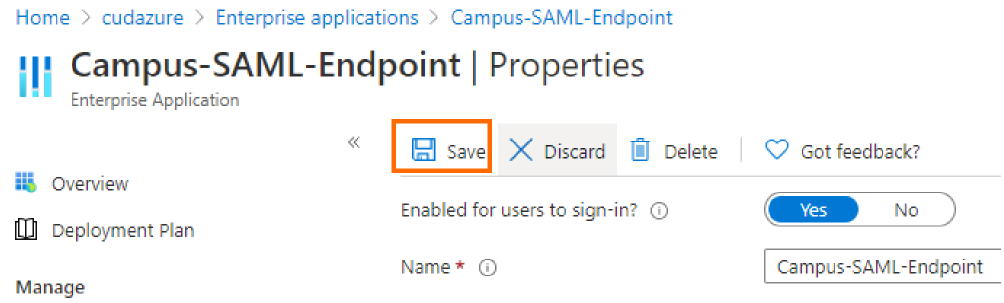


Home > cudazure > Enterprise applications > Campus-SAML-Endpoint

Campus-SAML-Endpoint | Properties
Enterprise Application

Enabled for users to sign-in? Yes
Name * Campus-SAML-Endpoint
Homepage URL
Logo
User access URL https://myapps.microsoft.com/signin/Campus-SAML-Endpoint/f98efbc...
Application ID
Object ID
Terms of Service Url Publisher did not provide this information
Privacy Statement Url Publisher did not provide this information
Reply URL https://autodiscovery.cloudgenwan.cudasvc.com/sso/acs
User assignment required? No
Visible to users? Yes
Notes

14. Click **Save**.



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

Campus-SAML-Endpoint | Properties
Enterprise Application

Enabled for users to sign-in? Yes
Name * Campus-SAML-Endpoint

## Further Information

- For more information on Personacl Access and Site Authentication, see User Connectivity & Personal Security.
- For more information on allowed VPN users and groups, see How to Configure Allowed VPN User Groups.

## Figures