

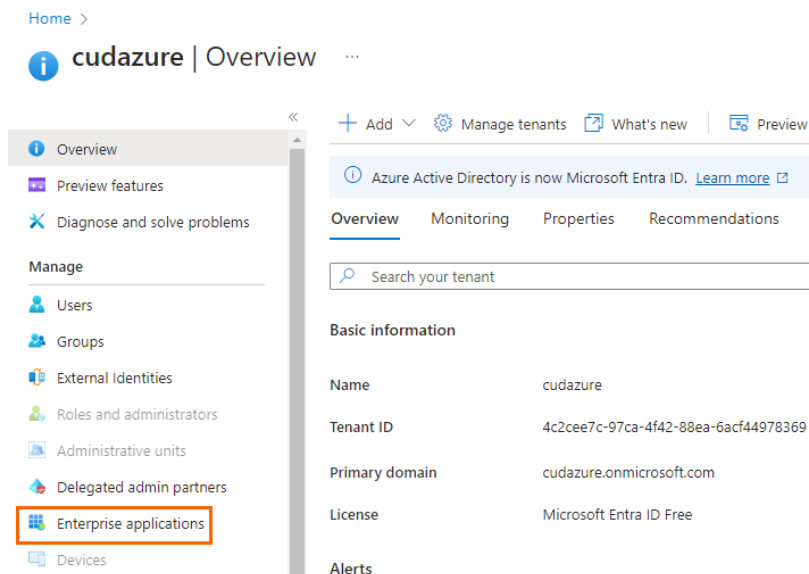
## How to Create a SAML Endpoint in Microsoft Azure and Basic User Connectivity & Personal Security Configuration

<https://campus.barracuda.com/doc/98223662/>

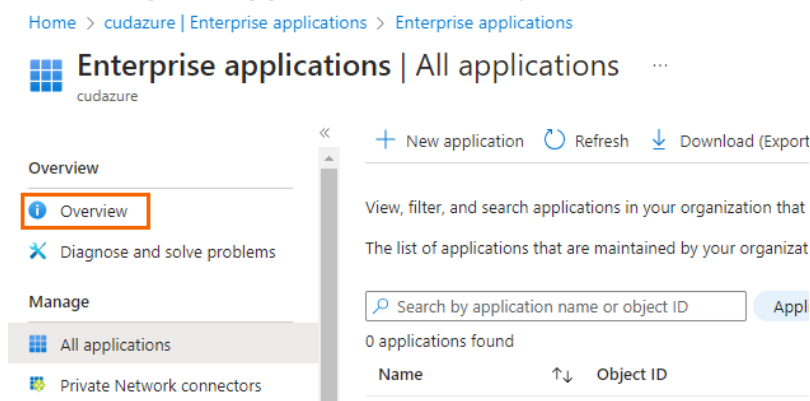
For Barracuda SecureEdge User Connectivity & Personal Security, you must configure a SAML endpoint in Microsoft Azure. In order to save the SAML configuration in Barracuda SecureEdge, you must also provide basic configuration details for User Connectivity & Personal Security.

### 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 **Microsoft Entra ID**.
3. Click **Microsoft Entra ID**.
4. In the left menu of the **Microsoft Entra ID** blade, click **Enterprise applications**.

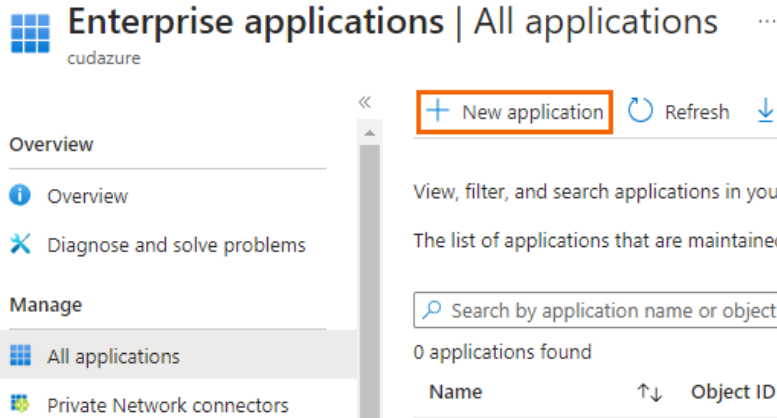


5. The **Enterprise applications** blade opens. Click **Overview**.



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

Home > cudazure | Enterprise applications > Enterprise applications



**Enterprise applications | All applications** ...

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Private Network connectors

+ New application Refresh

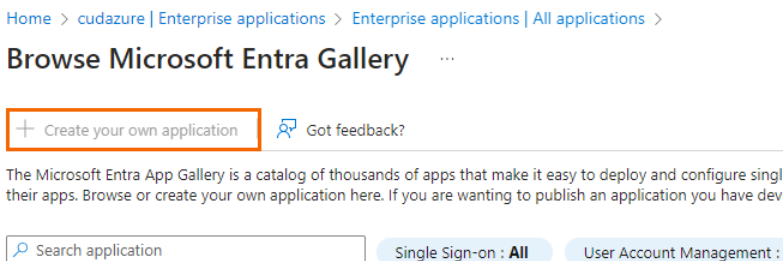
View, filter, and search applications in your organization. The list of applications that are maintained in the Microsoft Entra App Gallery.

Search by application name or object ID

0 applications found

Name	Object ID
------	-----------

7. The **Browse Microsoft Entra Gallery** blade opens. Click **Create your own application**.



Home > cudazure | Enterprise applications > Enterprise applications | All applications >

**Browse Microsoft Entra Gallery** ...

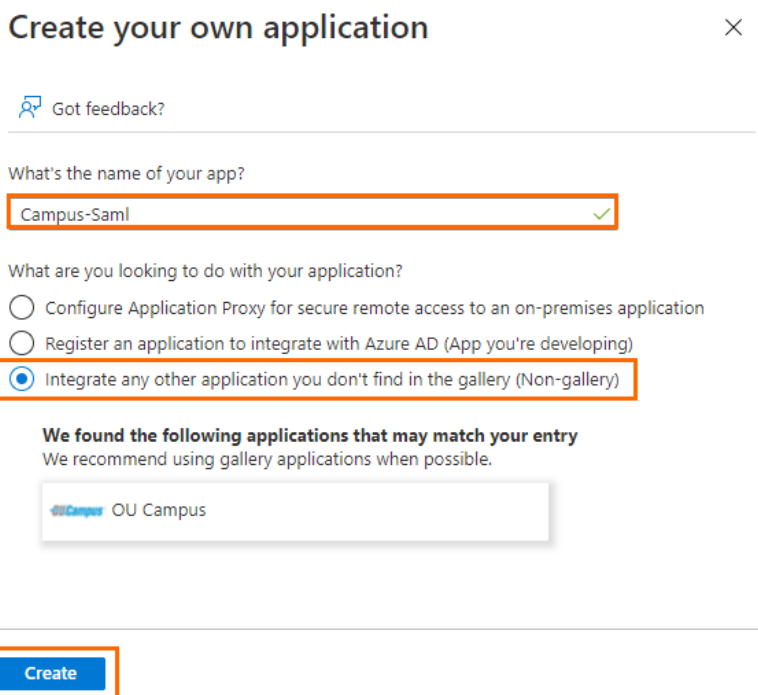
+ Create your own application Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on for your apps. Browse or create your own application here. If you are wanting to publish an application you have developed, click on the 'Publish' button.

Search application

Single Sign-on : All User Account Management :

8. Enter the name of your application, and select **Integrate any other application you don't find in the gallery (Non-gallery)**.



**Create your own application** ×

Got feedback?

What's the name of your app?

Campus-Saml ✓

What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Azure AD (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry  
We recommend using gallery applications when possible.

OU Campus

Create

9. Click **Create**.

After the application is successfully deployed, it automatically opens the **Overview** blade of the created application.

10. In the left menu, select **Properties**.

Home > Campus-Saml | Overview ...

Enterprise Application

Overview

- Deployment Plan
- Diagnose and solve problems

Manage

- Properties**
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes (preview)



Security



- Conditional Access
- Permissions
- Token encryption



Activity

- Sign-in logs
- Usage & insights
- Audit logs

**Properties**

Name  mpitracher-saml 


Application ID  d7d43b7e-a478-4116-b525... 

Object ID  22e901d4-20b7-4069-8414... 

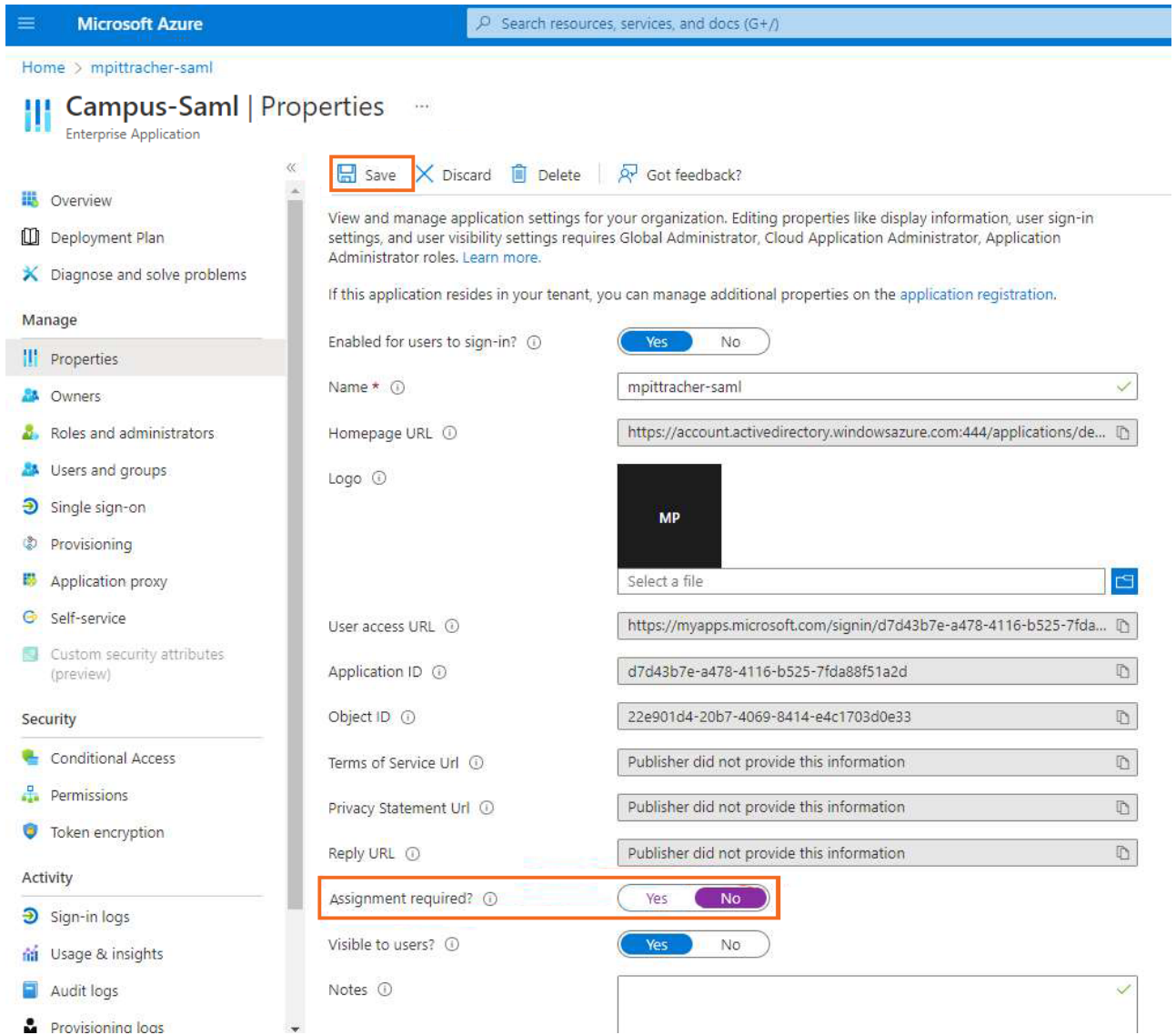
**Getting Started**

- 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](#)
- 4. Conditional Access**  
Secure access to this application with a customizable access policy.  
[Create a policy](#)
- 5. Self service**  
Enable users to request access to the application using their Azure AD credentials  
[Get started](#)

**What's New**

 **Sign in charts have moved!**  
The new Insights view shows sign in info along with other useful application data. [View insights](#)

11. In the **Properties** blade, disable **Assignment required** and click **Save**.



The screenshot shows the Microsoft Azure portal interface for managing an application named 'Campus-Saml'. The left-hand navigation pane includes sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (with sub-items like Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, and Custom security attributes), Security (with sub-items like Conditional Access, Permissions, and Token encryption), and Activity (with sub-items like Sign-in logs, Usage & insights, Audit logs, and Provisioning logs). The 'Single sign-on' option is highlighted in the Manage section. The main content area displays the 'Properties' of the 'Campus-Saml' application. At the top of this area, there are buttons for 'Save', 'Discard', 'Delete', and 'Got feedback?'. The 'Save' button is highlighted with a red box. Below these buttons, there is a description of the application and its settings. The 'Enabled for users to sign-in?' toggle is set to 'Yes'. The 'Name' field is 'mpitracher-saml'. The 'Homepage URL' is 'https://account.activedirectory.windowsazure.com:444/applications/de...'. The 'Logo' field shows a placeholder image with the letters 'MP'. The 'User access URL' is 'https://myapps.microsoft.com/signin/d7d43b7e-a478-4116-b525-7fda...'. The 'Application ID' is 'd7d43b7e-a478-4116-b525-7fda88f51a2d'. The 'Object ID' is '22e901d4-20b7-4069-8414-e4c1703d0e33'. The 'Terms of Service URL', 'Privacy Statement URL', and 'Reply URL' are all set to 'Publisher did not provide this information'. The 'Assignment required?' toggle is highlighted with a red box and is currently set to 'No'. The 'Visible to users?' toggle is set to 'Yes'. The 'Notes' field is empty.

12. In the left menu, click **Single sign-on**.

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

[Home](#) > [Enterprise applications](#) > [Campus-SAML-Endpoint](#)**Campus-SAML-Endpoint | Single 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

**Activity**

Sign-ins

Usage &amp; insights (Preview)

Audit logs

Provisioning logs (Preview)

Access reviews

&lt;&lt;

Select a single sign-on method [Help n](#)**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.

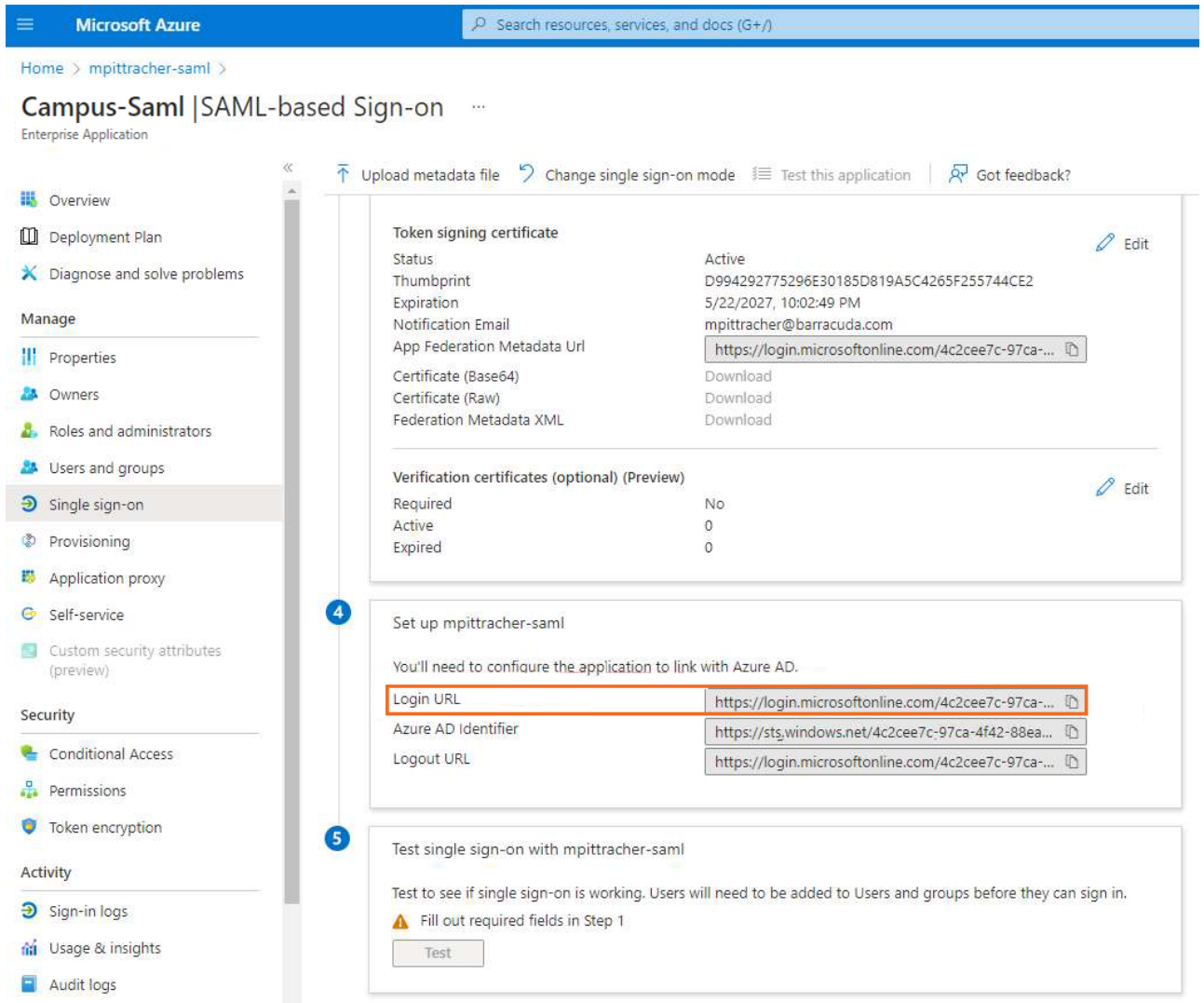
**Password-based**

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. The **SAML-based Sign-on** blade opens. Copy the **Login URL**.



The screenshot shows the Microsoft Azure portal interface for configuring a SAML-based sign-on for the 'Campus-Saml' application. The left sidebar contains navigation links for Overview, Deployment Plan, Diagnose and solve problems, and a Manage section with links to Properties, Owners, Roles and administrators, Users and groups, Single sign-on (selected), Provisioning, Application proxy, Self-service, and Custom security attributes (preview). The main content area is titled 'Campus-Saml | SAML-based Sign-on' and includes a search bar and a list of actions: Upload metadata file, Change single sign-on mode, Test this application, and Got feedback?.

The configuration details are as follows:

Token signing certificate		Edit
Status	Active	
Thumbprint	D994292775296E30185D819A5C4265F255744CE2	
Expiration	5/22/2027, 10:02:49 PM	
Notification Email	mpitracher@barracuda.com	
App Federation Metadata Url	<a href="https://login.microsoftonline.com/4c2cee7c-97ca-...">https://login.microsoftonline.com/4c2cee7c-97ca-...</a>	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Verification certificates (optional) (Preview)		Edit
Required	No	
Active	0	
Expired	0	

**4** Set up mpitracher-saml

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

Login URL	<a href="https://login.microsoftonline.com/4c2cee7c-97ca-...">https://login.microsoftonline.com/4c2cee7c-97ca-...</a>
Azure AD Identifier	<a href="https://sts.windows.net/4c2cee7c-97ca-4f42-88ea-...">https://sts.windows.net/4c2cee7c-97ca-4f42-88ea-...</a>
Logout URL	<a href="https://login.microsoftonline.com/4c2cee7c-97ca-...">https://login.microsoftonline.com/4c2cee7c-97ca-...</a>

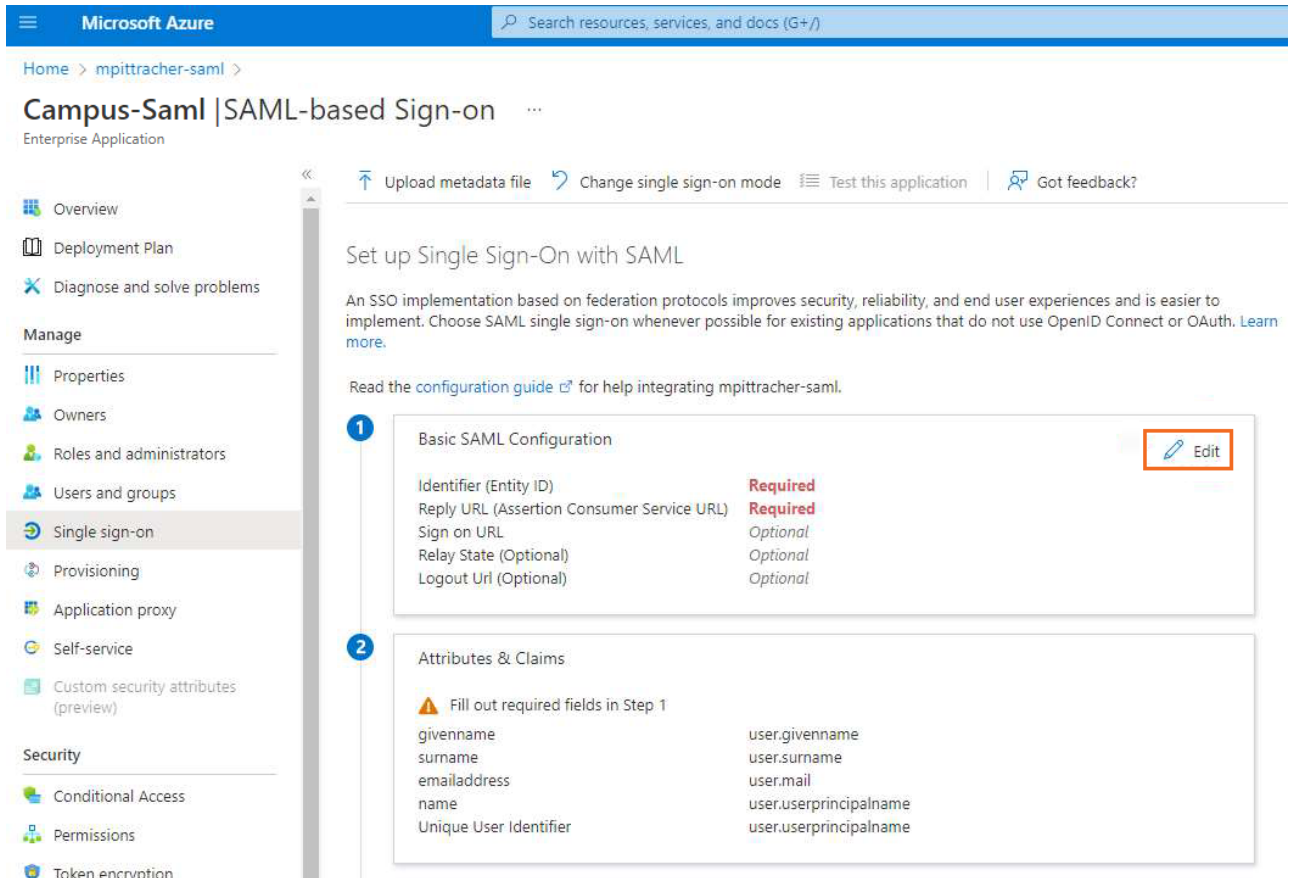
  

**5** Test single sign-on with mpitracher-saml

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

⚠ Fill out required fields in Step 1

15. Click **Edit** next to **Basic SAML Configuration**.



Microsoft Azure

Home > mpitracher-saml >

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

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

**Single sign-on**

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

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

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating mpitracher-saml.

- #### Basic SAML Configuration

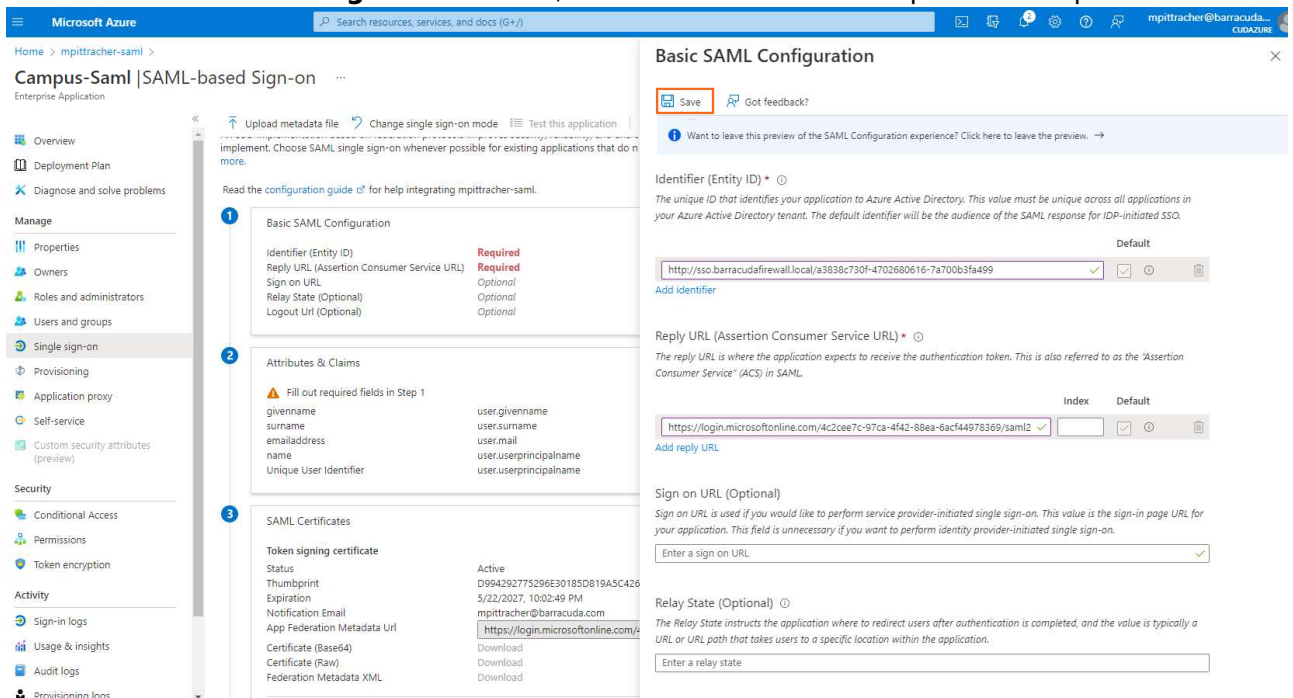
[Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- #### Attributes & Claims

Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

- Click **Add reply URL** and paste the copied URL.
- Open the SAML configuration on your Barracuda SecureEdge, and copy the **Service Provider Entity ID**.
- In the **Basic SAML Configuration** blade, click **Add identifier** and paste the copied ID.



Microsoft Azure

Home > mpitracher-saml >

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

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

**Single sign-on**

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Token encryption

Upload metadata file

Change single sign-on mode

Test this application

Got feedback?

### 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

[http://sso.barracudafirewall.local/a3838c730f-4702680616-7a700b3fa499](#) ✓ [Add identifier](#)

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://login.microsoftonline.com/4c2cee7c-97ca-4f42-88ea-6ac44978369/saml2](#) ✓ [Add reply URL](#)

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

Token signing certificate

Status Active

Thumbprint D994392775326630185D019A5C426

Expiration 5/22/2027, 10:02:49 PM

Notification Email mpitracher@barracuda.com

App Federation Metadata Url [https://login.microsoftonline.com/4c2cee7c-97ca-4f42-88ea-6ac44978369/saml2](#)

Certificate (Base64) Download

Certificate (Raw) Download

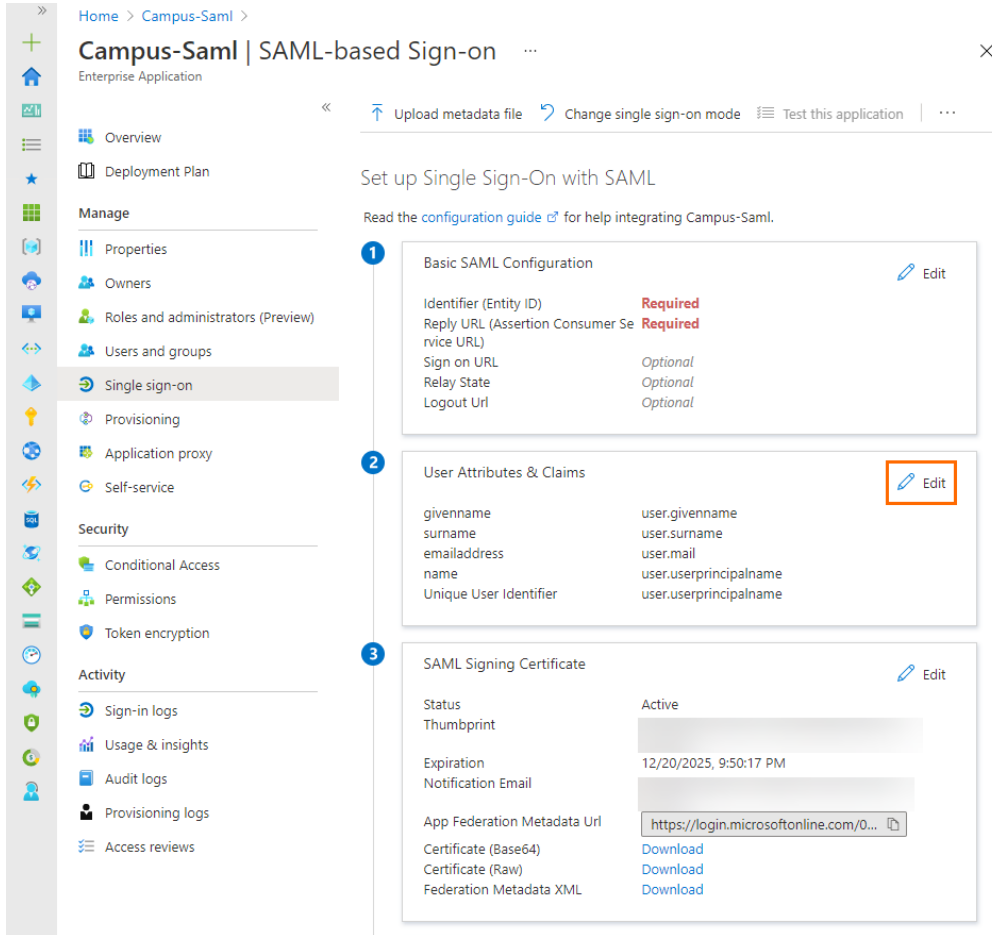
Federation Metadata XML Download

- Click **Save**.



20. Click **X** to close the **Basic SAML Configuration** blade.

21. In the **User Attribute & Claims** section, click **Edit**.



Home > Campus-Saml >

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

Enterprise Application

« Upload metadata file Change single sign-on mode Test this application ...

Set up Single Sign-On with SAML

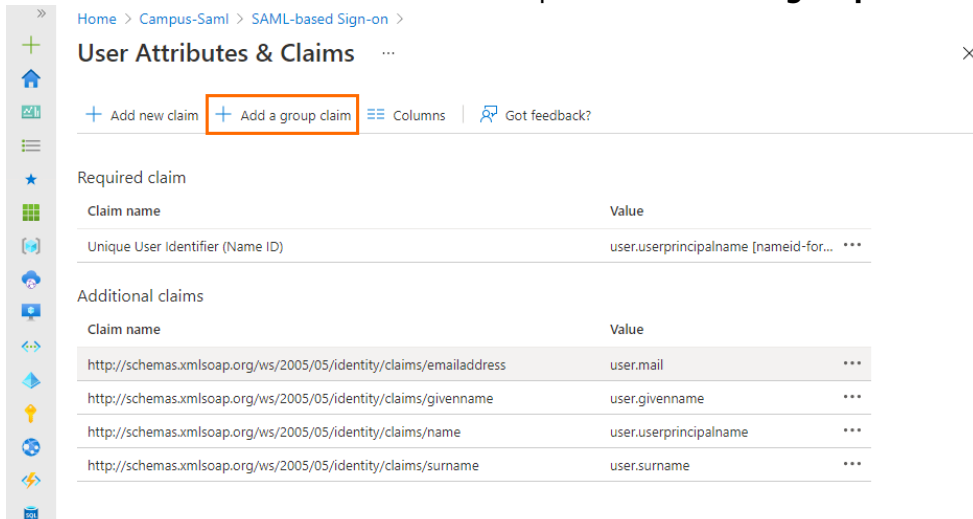
Read the [configuration guide](#) for help integrating Campus-Saml.

- 1 Basic SAML Configuration [Edit](#)
- 2 User Attributes & Claims [Edit](#)
- 3 SAML Signing Certificate [Edit](#)

**User Attributes & Claims**

Attribute	Value
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

22. The **User Attributes & Claims** blade opens. Click **Add a group claim**.



Home > Campus-Saml > SAML-based Sign-on >

## User Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

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

23. The **Group Claims** blade opens. Select **Security groups** and click **Save**.



## 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

24. Click **X** to close the **User Attributes & Claims** blade.

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

## User Attributes & Claims

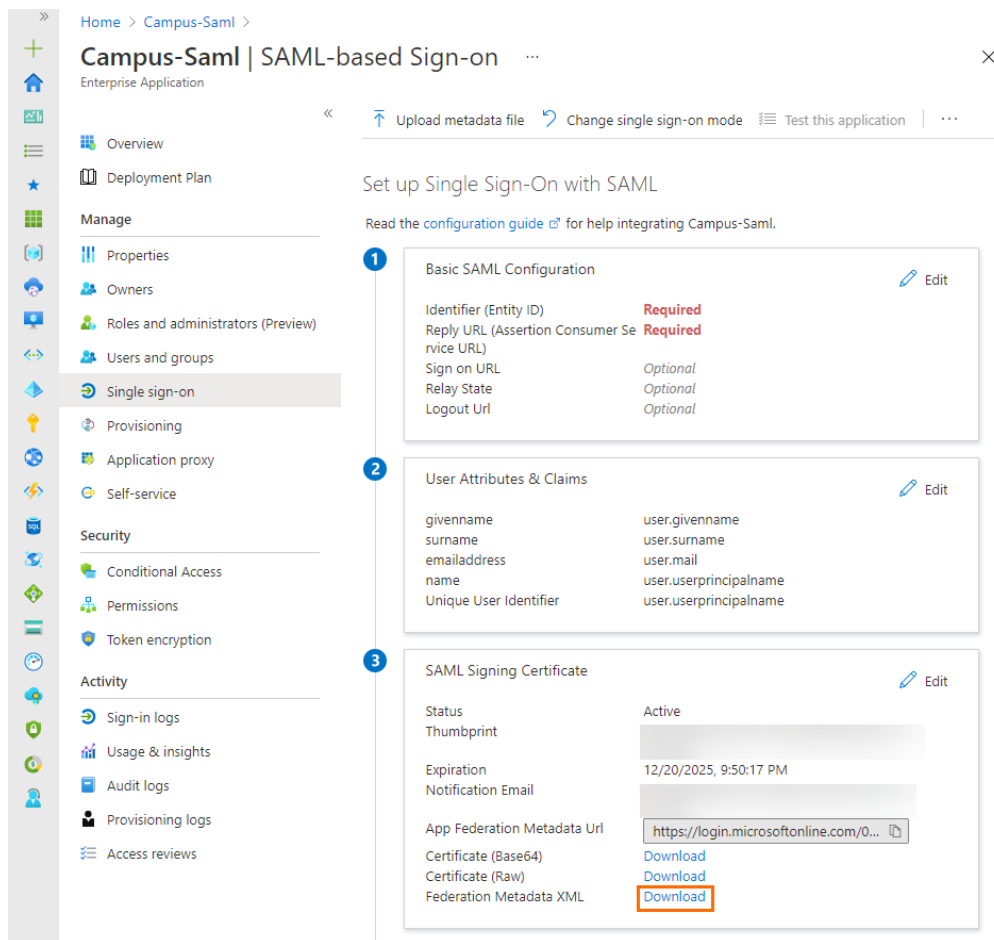
[+](#) Add new claim [+](#) Add a group claim [≡](#) Columns | [🗨️](#) Got feedback?

### Required claim

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

If the number of groups a user is in exceeds a certain limit (150 for SAML, 200 for JWT) then an overage claim will be added, the claim sources pointing at the graph endpoint containing the list of groups for the user. (For detailed information, see [Claims in SAML tokens](#) in the Microsoft documentation.) The firewall does not use this link to extract user groups and therefore generates a "DENY: Group did not match" security entry in the VPN logs in this case, as no group policy containing a group filter will match. This can be avoided by creating a group filter, preventing Microsoft from sending a link pointing to the groups. For more information, see [Configure group claims for applications by using Microsoft Entra ID](#).

25. In the **SAML-based Sign-on** blade, click **Download** to download the *Federation Metadata XML*.



Home > Campus-Saml > **Campus-Saml | SAML-based Sign-on** ...

Enterprise Application

« ↑ Upload metadata file ↶ Change single sign-on mode ⌵ Test this application | ...

### Set up Single Sign-On with SAML

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

- Basic SAML Configuration** [Edit](#)
  - Identifier (Entity ID) **Required**
  - Reply URL (Assertion Consumer Service URL) **Required**
  - Sign on URL *Optional*
  - Relay State *Optional*
  - Logout URL *Optional*
- User Attributes & Claims** [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Signing Certificate** [Edit](#)

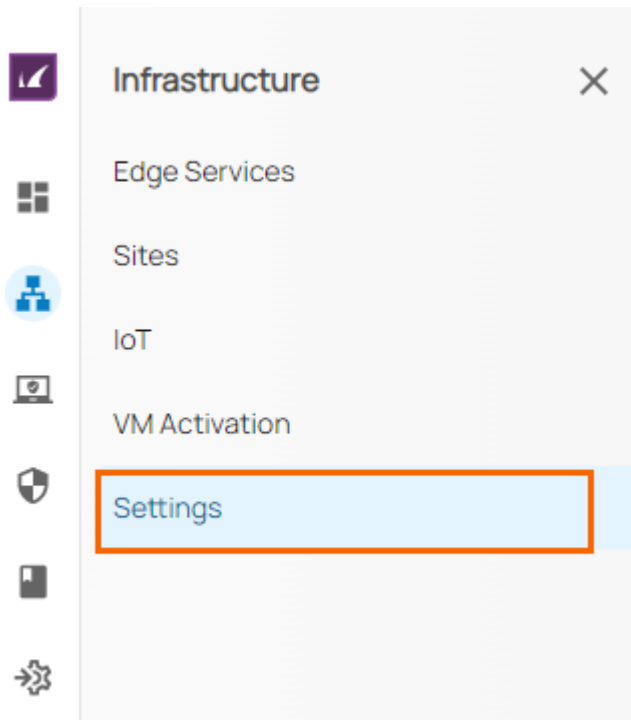
Status	Active
Thumbprint	
Expiration	12/20/2025, 9:50:17 PM
Notification Email	
App Federation Metadata Url	<a href="https://login.microsoftonline.com/0...">https://login.microsoftonline.com/0...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

Note that some browsers might block the \*.xml file.

26. Save the file to your local machine.

## Step 2. Basic Configuration in Barracuda SecureEdge

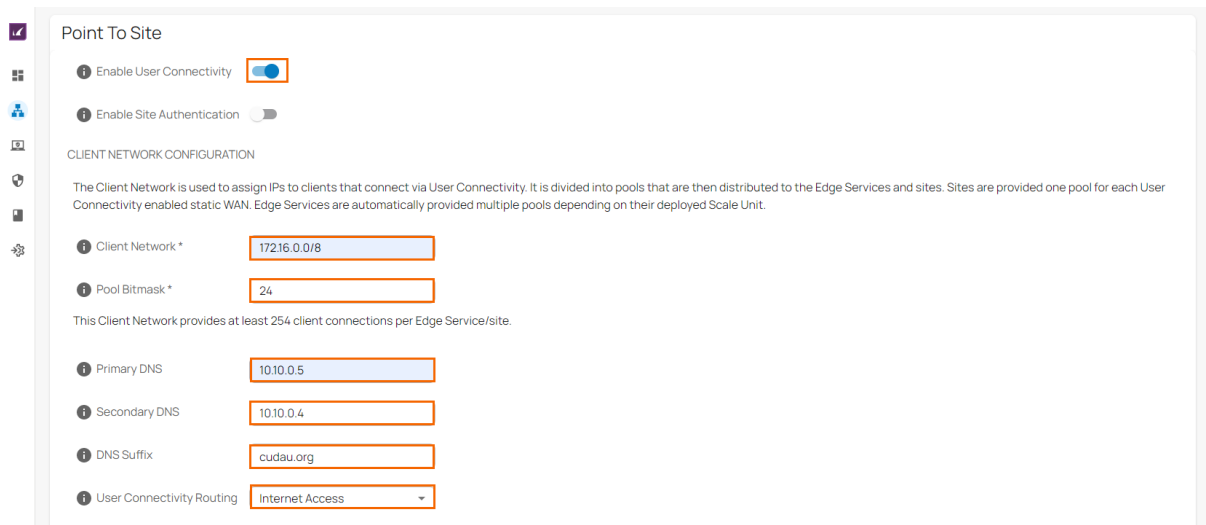
1. Go to <https://se.barracudanetworks.com/> and log in with your existing Barracuda Cloud Control account.
2. Go to **Infrastructure > Settings**.



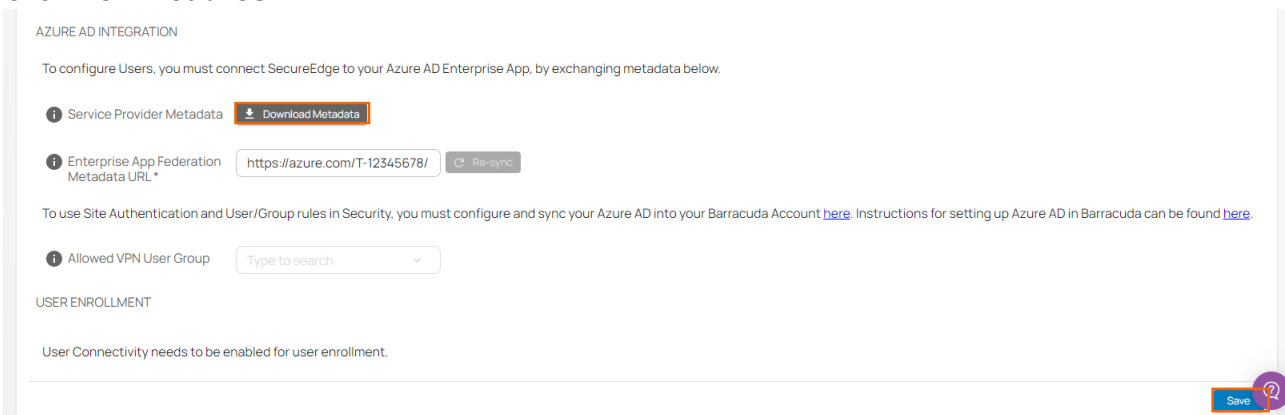
3. The user configuration window opens. Specify values for the following:

- **Enable Site Authentication** – Click to enable. Site authentication allows devices physically located within the network to authenticate against the Barracuda SecureEdge 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** – (optional) Enter a secondary DNS address for the VPN clients to use.
- **DNS Suffix** – Enter a DNS suffix to be used for the VPN client network.
- **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 SecureEdge gateway, and the option **Internet Access** sends all traffic through the gateway. **Internet Access** can be used to inspect all traffic by SecureEdge.
- **Enterprise App Federation Metadata Url\*** – Paste the **App Federation Metadata Url** retrieved in Step 1.



4. Click **Save**.
5. Stay in the user configuration window, and scroll down to **AZURE AD INTEGRATION**.
6. Click **Download CSV**.



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 **Microsoft Entra ID**.
3. Click **Microsoft Entra ID**.
4. In the left menu of the **Microsoft Entra ID** 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

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

« **Upload metadata file** Change single sign-on mode Test this application ...

**1** Basic SAML Configuration Edit

Identifier (Entity ID)	<b>Required</b>
Reply URL (Assertion Consumer Service URL)	<b>Required</b>
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

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

[Home](#) > [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

« **Upload metadata file** Change single sign-on mode Test this application ...

**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.

📎



**Add** Cancel

**2** User Attributes & Claims Edit

givenname	user.givenname
-----------	----------------


11. Click **Save**.

### Basic SAML Configuration

 Save |  Got feedback?


Identifier (Entity ID) \* ⓘ  
*The default identifier will be the audience of the SAML response for IDP-initiated SSO*

http://sso.barracudafirewall.local/vvi-BE6-1UE ✓

Default ☒ ⓘ 

Reply URL (Assertion Consumer Service URL) \* ⓘ  
*The default reply URL will be the destination in the SAML response for IDP-initiated SSO*

https://127.0.0.2/Shibboleth.sso/SAML2/POST ✓

Default ☒ ⓘ 

Sign on URL ⓘ  

Enter a sign on URL ✓

Relay State ⓘ  

Enter a relay state

Logout Url ⓘ  

Enter a logout url ✓

12. Close the **Basic SAML Configuration** blade.

You are now back in the **Single sign-on** blade.

13. Click **Download** to download the *Federation Metadata XML file* and save it to your local machine.

[Home](#) > [Default Directory](#) > [Enterprise applications](#) > [Campus-Saml](#) >

## Campus-Saml | 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

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

« [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.

1

Basic SAML Configuration

Identifier (Entity ID)

http://sso.barracudafirewall.local/vvi-BE6-1UE

Reply URL (Assertion Consumer Service URL)

**Required**

Sign on URL

Optional

Relay State

Optional

Logout Url

Optional

Edit

2

User Attributes & Claims

givenname

user.givenname

surname

user.surname

emailaddress

user.mail

name

user.userprincipalname

Unique User Identifier

user.userprincipalname

Group

user.groups

Edit

3

SAML Signing Certificate

Status

Active

Thumbprint

Expiration

12/20/2025, 9:50:17 PM

Notification Email

App Federation Metadata Url

<https://login.microsoftonline.com/>

Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)

Federation Metadata XML

[Download](#)

Edit

## Further Information

- For more information on Personal Access and Site Authentication, see [Point-to-Site](#).
- For more information on allowed VPN users and groups, see [How to Configure Allowed VPN User Groups](#).



## Figures

1. enterprise\_application.png
2. overview\_ent\_app.png
3. new\_application.png
4. create\_own\_app.png
5. create\_own2.png
6. overview\_properties.png
7. assignment\_required.png
8. sso\_saml.png
9. copy\_url.png
10. edit\_basic.png
11. add\_identifier.png
12. user\_attributes.png
13. add\_gclaim.png
14. claim\_sec.png
15. close\_uac.png
16. download\_fed\_metadata.png
17. goto-infrast-setting.png
18. pt-to-site-menu.png
19. azure-AD-integration.png
20. upload\_metadata.png
21. add\_file.png
22. cgf\_saml.png
23. fed\_metadata\_download2.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.