

## How to Create a SAML Endpoint in Microsoft Azure and Client-to-Site SAML Configuration

<https://campus.barracuda.com/doc/98210143/>

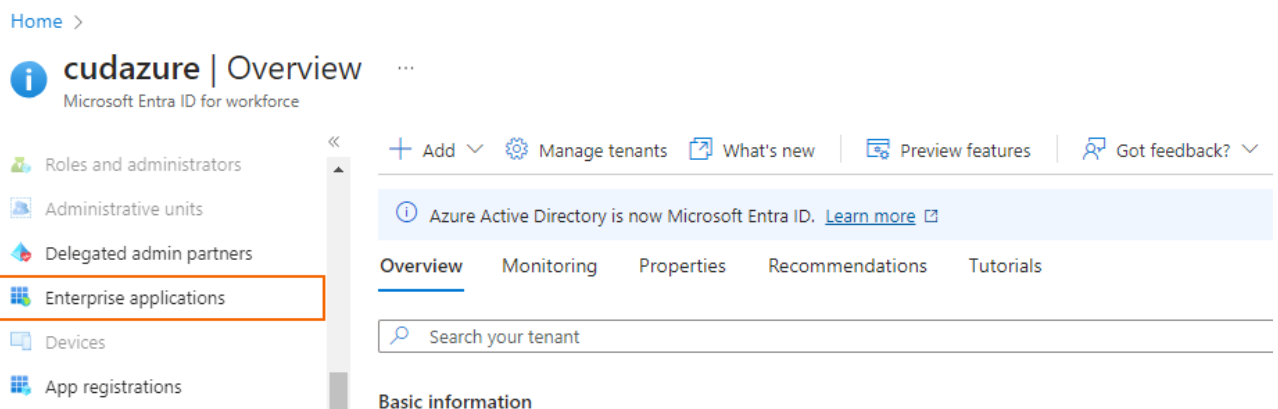
Follow the guide below to create a SAML endpoint in Microsoft Azure and to configure a Barracuda CloudGen Firewall to use SAML authentication for the client-to-site VPN service.

### Before You Begin

- Create and configure a VPN service. For more information, see [VPN](#).
- You must have an existing user group in Microsoft Entra ID. For more information, see <https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups>.
- An Advanced Remote Access subscription is required. For more information on subscriptions, see [Base Licensing and Subscriptions](#).

### 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](#) >

## Enterprise applications | Overview

cudazure - Microsoft Entra ID for workforce

Overview

[Overview](#)[Diagnose and solve problems](#)

Manage

[All applications](#)[+ New application](#)[Got feedback?](#)[Overview](#)[Tutorials](#)[Search your tenant](#)

Basic information

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

[Microsoft Azure](#)[Home](#) > [Enterprise applications | Overview](#) >

## 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 find and integrate their apps. Browse or create your own application here. If you are wanting to publish your app, you can also create a new app here.

[Search application](#)Single Sign-on : **All**

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?

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 Microsoft Entra (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

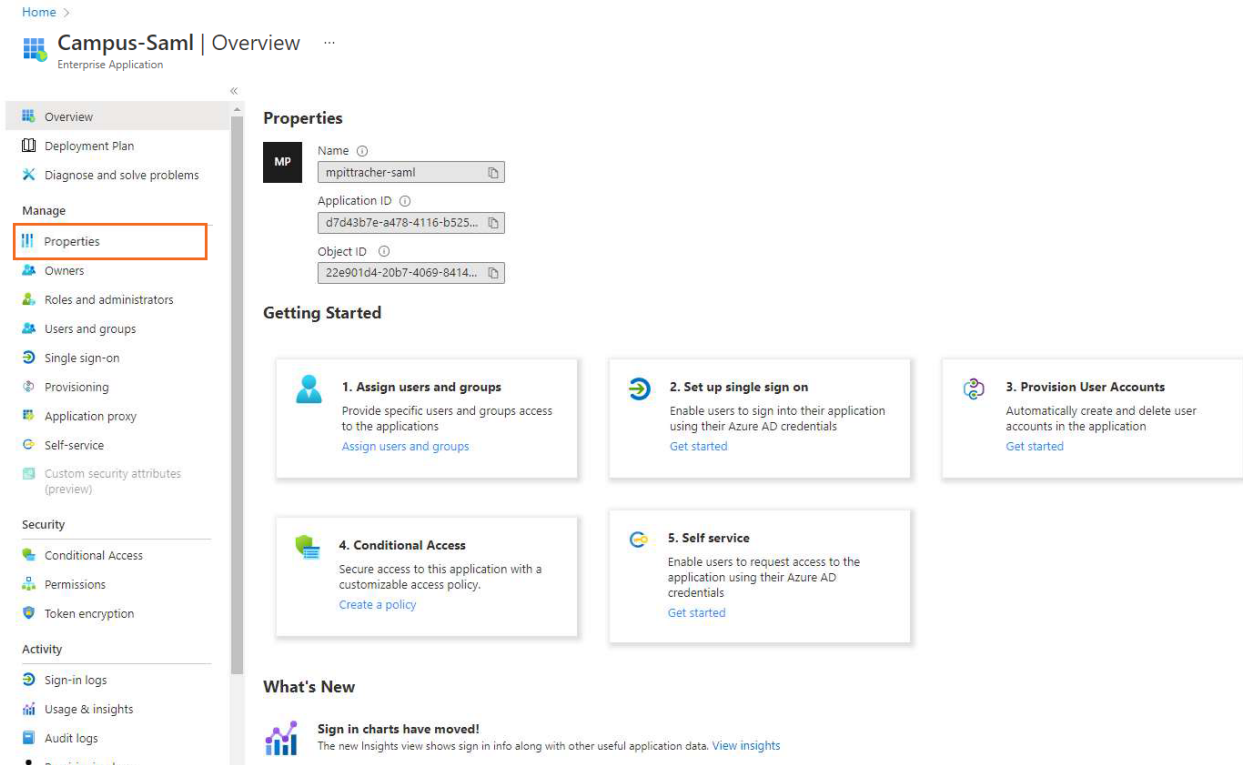
We found the following applications that may match your entry  
We recommend using gallery applications when possible.

[OU Campus](#)[Create](#)

9. Click **Create**.

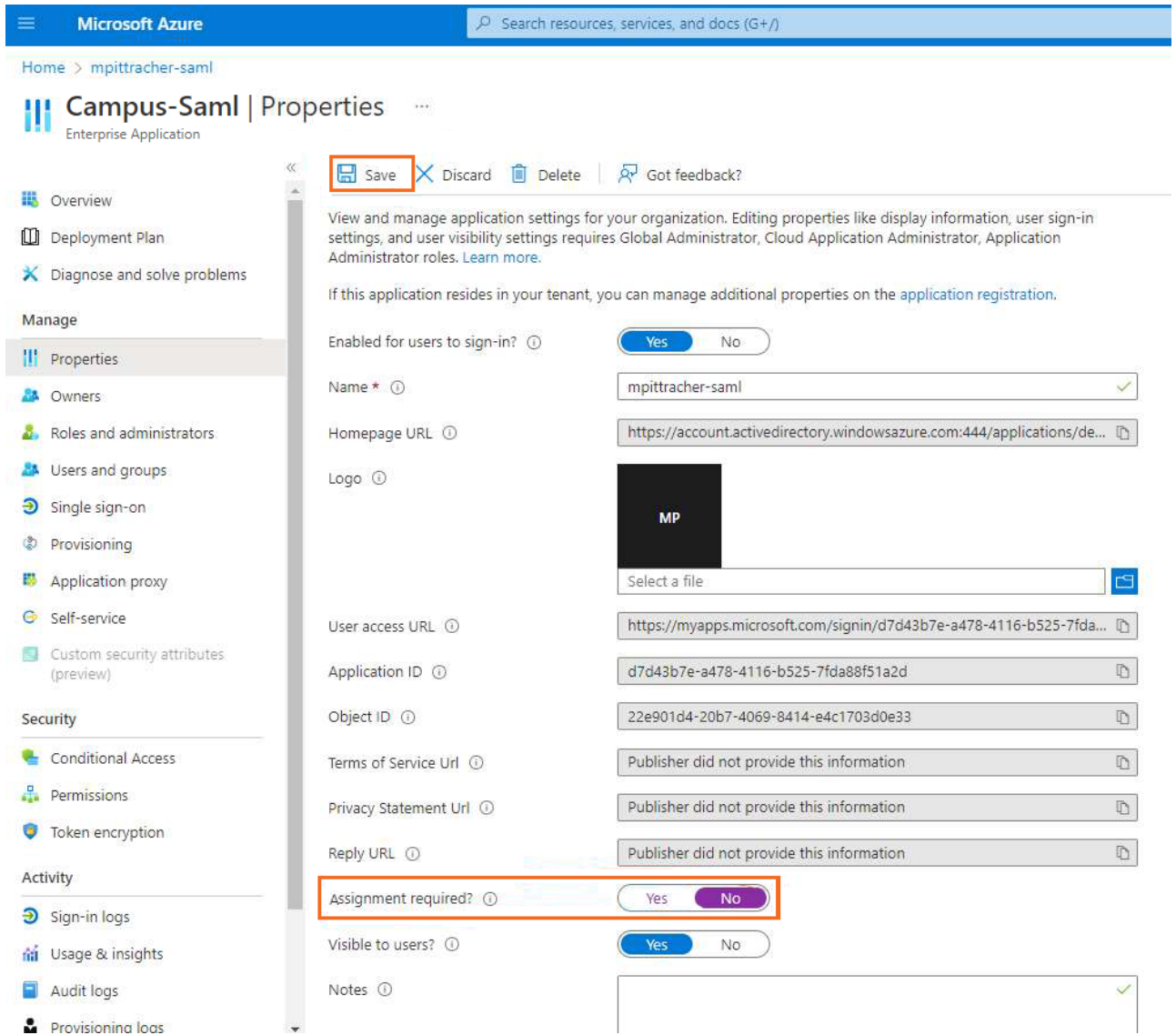
After the application is successfully deployed, it automatically opens the **Overview** blade of the created application.

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



The screenshot shows the Microsoft Azure portal interface. On the left, the 'Campus-Saml' application is selected, and the 'Properties' blade is active in the left-hand menu. The main content area displays the 'Properties' section for the application, which includes fields for Name, Application ID, and Object ID. Below this, there is a 'Getting Started' section with five numbered steps: 1. Assign users and groups, 2. Set up single sign on, 3. Provision User Accounts, 4. Conditional Access, and 5. Self service. Each step has a brief description and a 'Get started' link. At the bottom, there is a 'What's New' section with a message about 'Sign in charts have moved!' and a link to '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. The top navigation bar includes the Microsoft Azure logo and a search bar. The left sidebar contains a navigation menu with sections like Overview, Deployment Plan, Diagnose and solve problems, Manage, Security, and Activity. The 'Manage' section is expanded, showing 'Properties' as the selected option. The main content area displays the 'Campus-Saml' application properties. 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 'Assignment required?' toggle is highlighted with a red box and is currently set to 'No'. Other settings include 'Enabled for users to sign-in?' (Yes), 'Name' (mpitracher-saml), 'Homepage URL' (https://account.activedirectory.windowsazure.com:444/applications/de...), 'Logo' (MP), 'User access URL' (https://myapps.microsoft.com/signin/d7d43b7e-a478-4116-b525-7fda...), 'Application ID' (d7d43b7e-a478-4116-b525-7fda88f51a2d), 'Object ID' (22e901d4-20b7-4069-8414-e4c1703d0e33), 'Terms of Service URL' (Publisher did not provide this information), 'Privacy Statement URL' (Publisher did not provide this information), and 'Reply URL' (Publisher did not provide this information). The 'Visible to users?' toggle is set to 'Yes'.



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 & insights (Preview) Audit logs Provisioning logs (Preview) Access reviews<< **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.

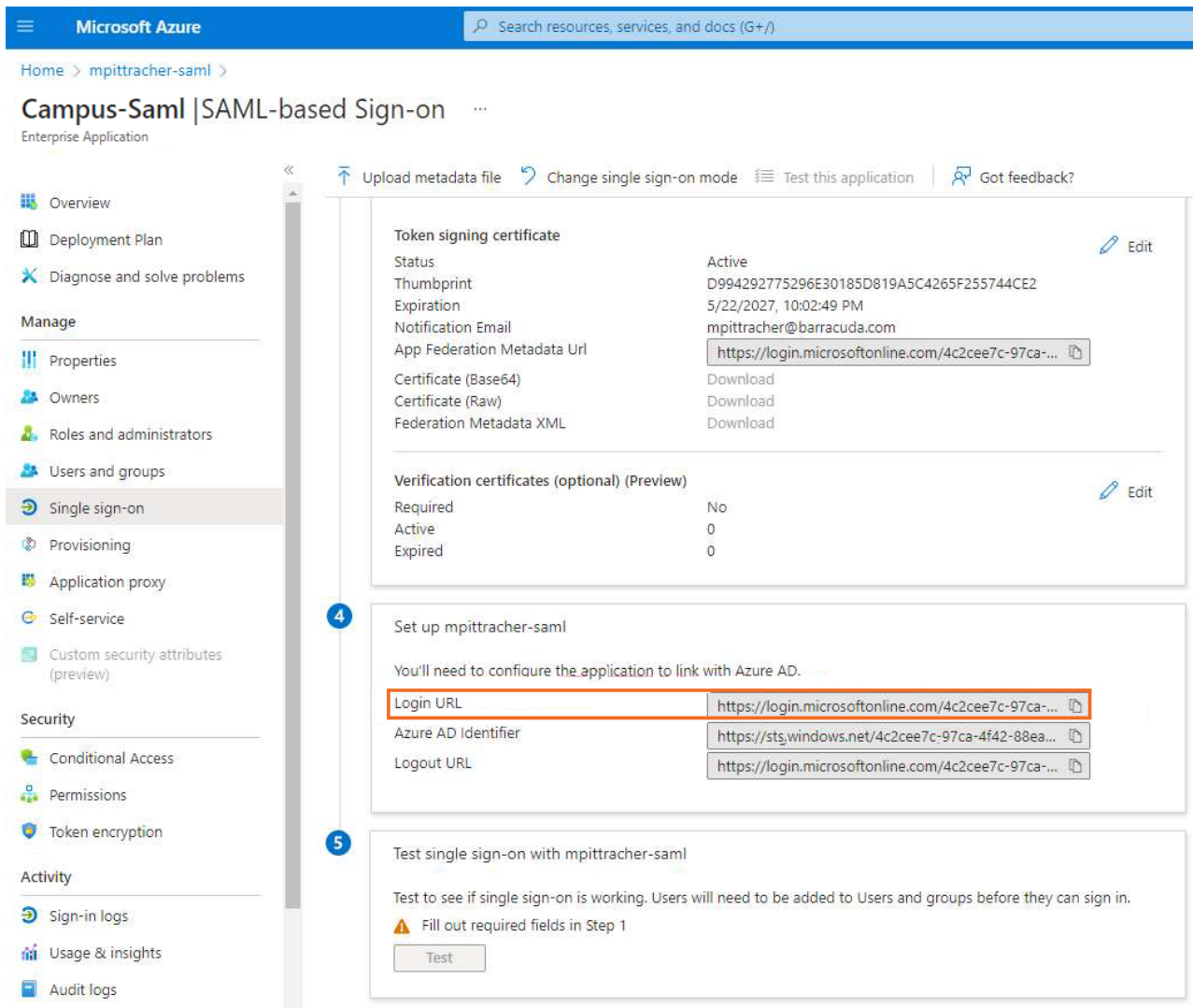
**Password-based**

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**.



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

Activity

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

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

#### Token signing certificate

Active [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)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

#### 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>

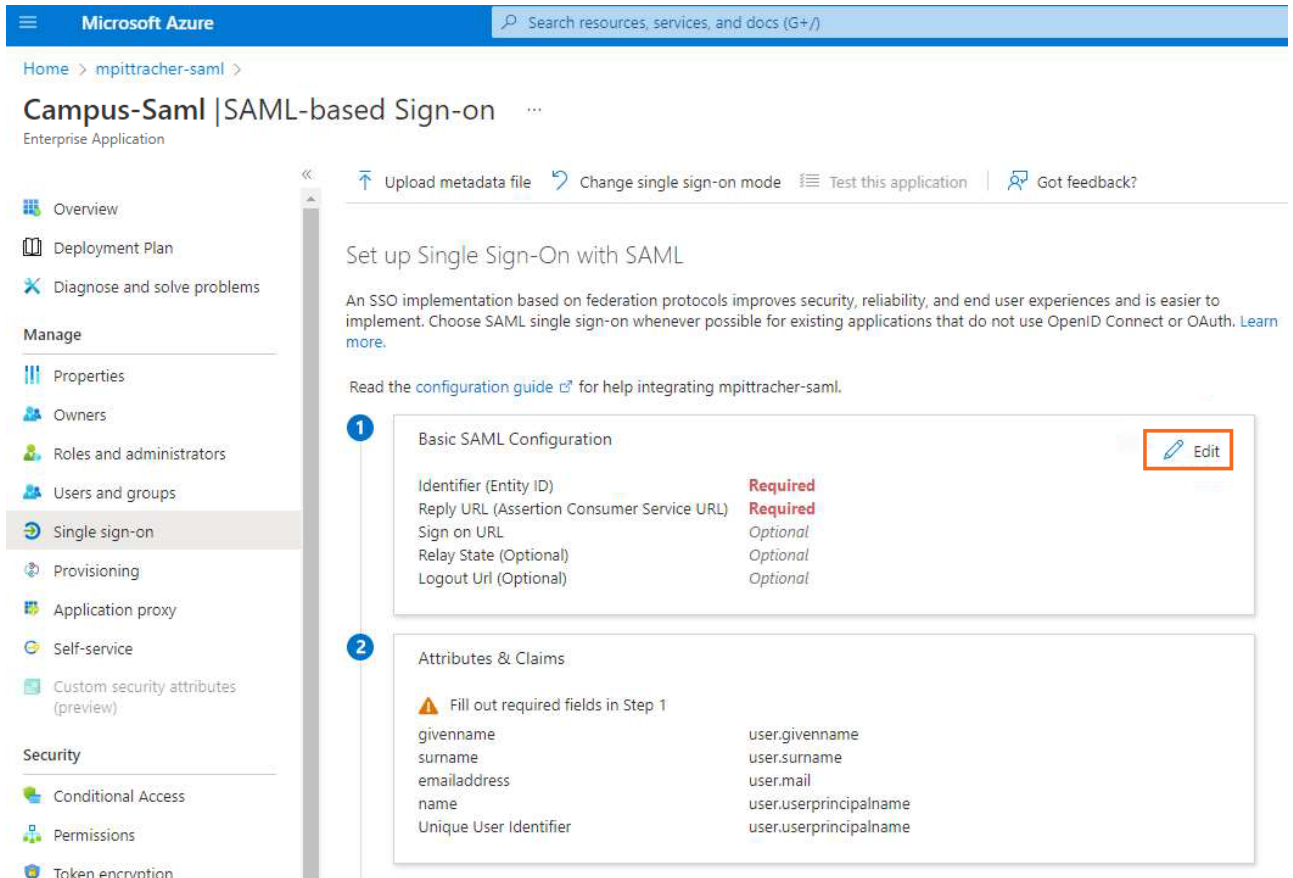
#### 5 Test single sign-on with mpitracher-saml

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**

[Test](#)

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



Home > mpitracher-saml >

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

Enterprise Application

Upload metadata file Change single sign-on mode Test this application Got feedback?

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

### 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

Identifier (Entity ID) **Required**

Reply URL (Assertion Consumer Service URL) **Required**

Sign on URL **Optional**

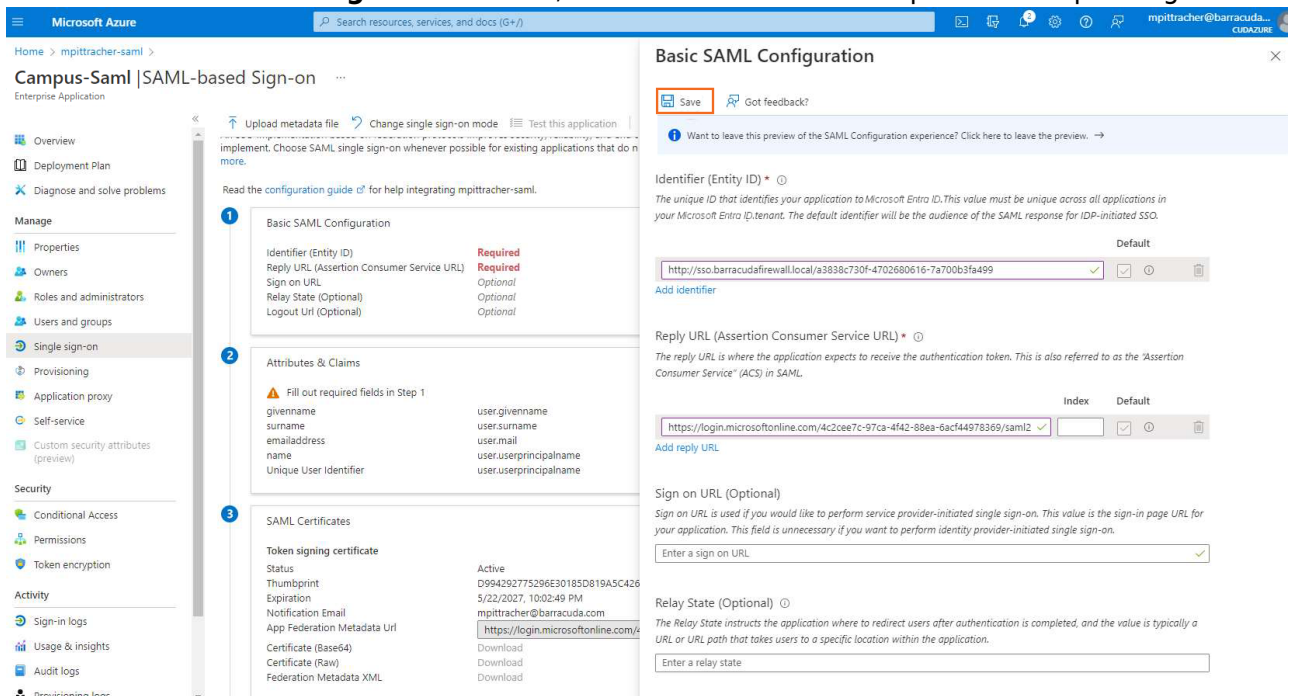
Relay State (Optional) **Optional**

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 CloudGen Firewall, and copy the **Service Provider Entity ID**.
- In the **Basic SAML Configuration** blade, click **Add identifier** and paste the copied login URL.



Home > mpitracher-saml >

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

Enterprise Application

Upload metadata file Change single sign-on mode Test this application Got feedback?

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

### 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 Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra ID tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

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.

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.

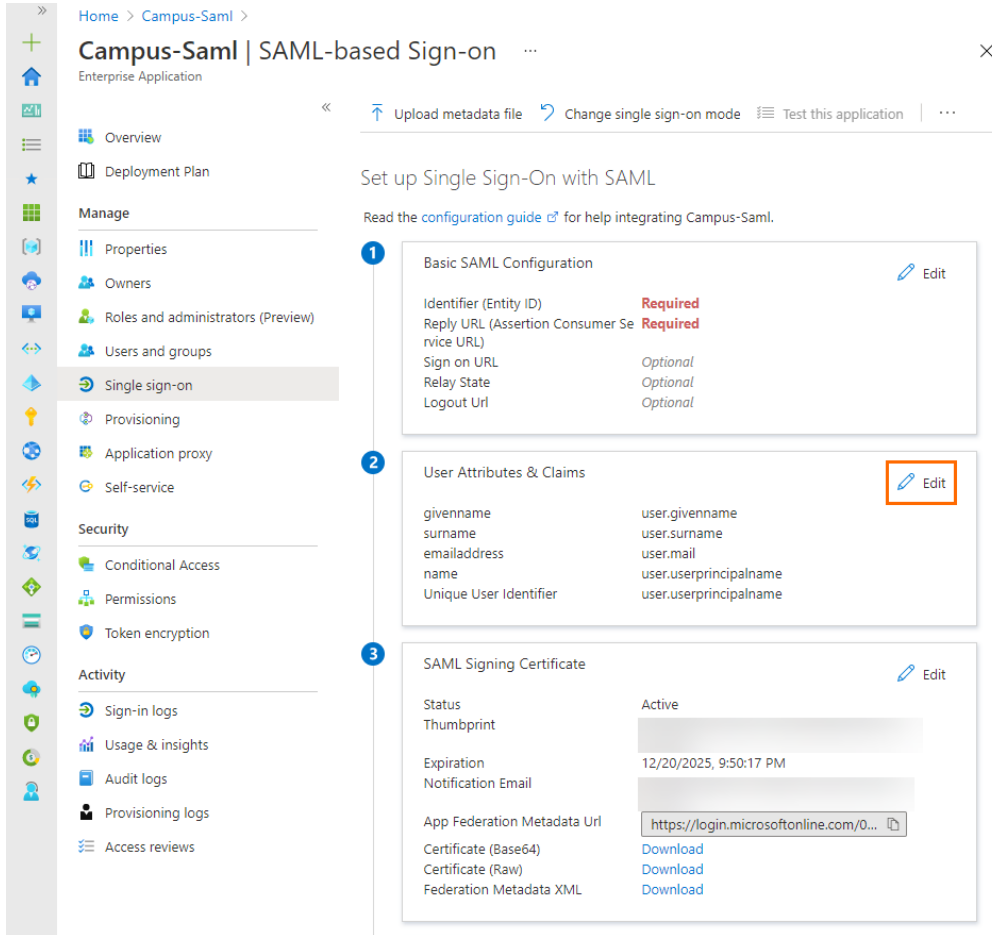
Enter a relay state

- 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

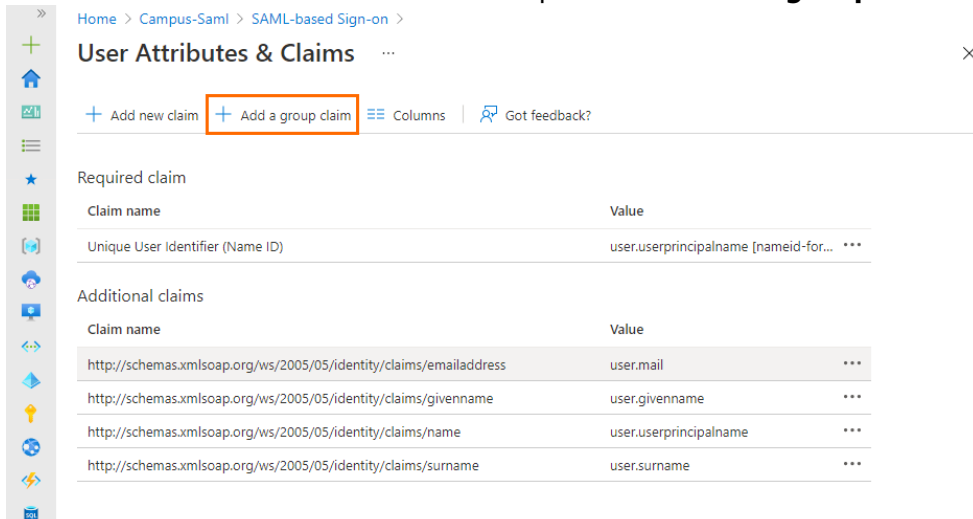
Read the [configuration guide](#) for help integrating Campus-Saml.

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

Attribute Name	Value
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- 3 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>

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
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a>	user.mail
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a>	user.givenname
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>	user.userprincipalname
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a>	user.surname

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



## Group Claims



Manage the group claims used by Microsoft Entra ID 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)	<b>Required</b>
Reply URL (Assertion Consumer Service URL)	<b>Required</b>
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](#)

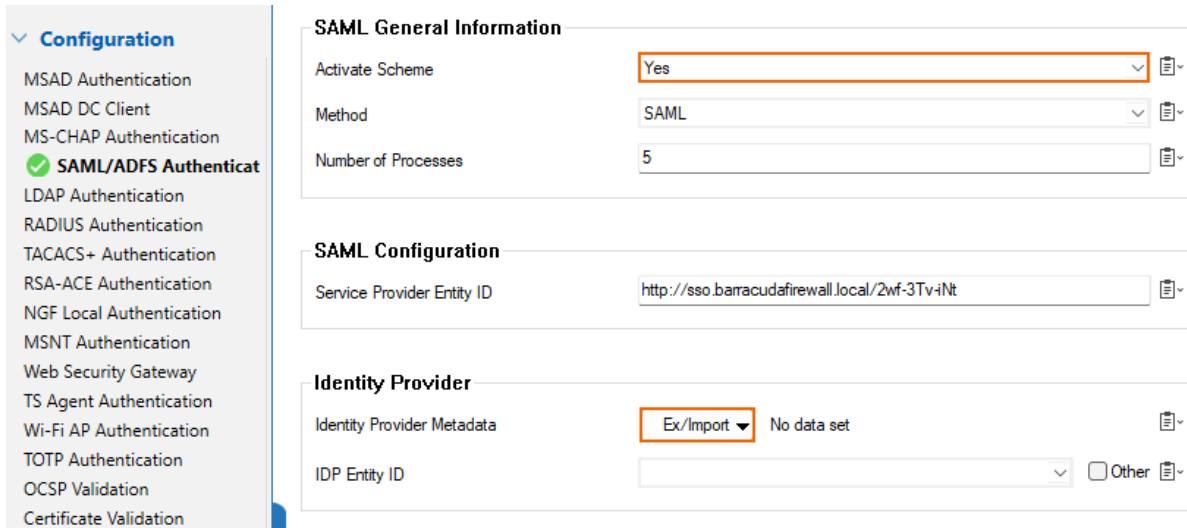
Status	Active
Thumbprint	
Expiration	12/20/2025, 9:50:17 PM
Notification Email	
App Federation Metadata Url	<a href="https://login.microsoftonline.com/0...">https://login.microsoftonline.com/0...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata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

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

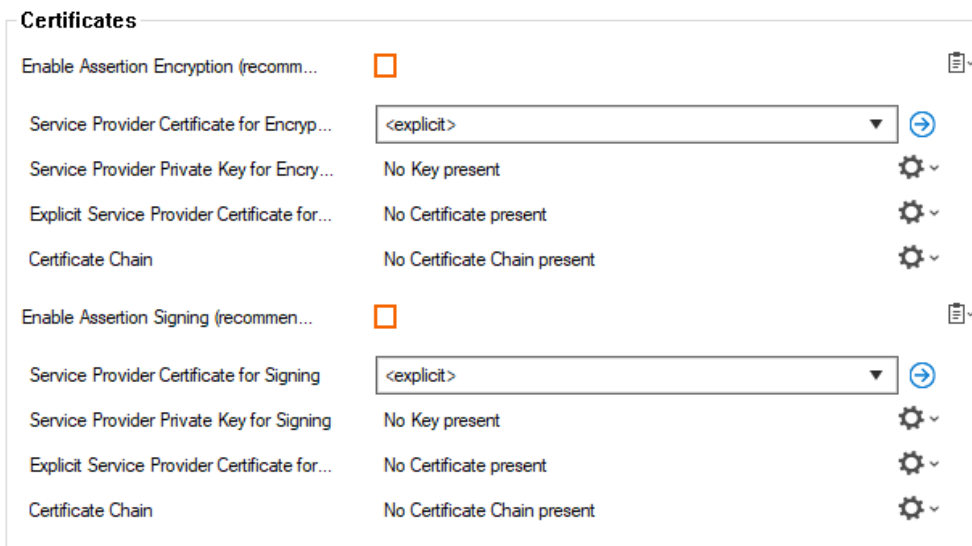
26. Save the file to your local machine.

## Step 2. Configure the Barracuda CloudGen Firewall to Use SAML Authentication

1. Connect to your Barracuda CloudGen Firewall and log in.
2. Go to **CONFIGURATION > Configuration Tree > Infrastructure Services > Authentication Service**.
3. In the left menu, click **SAML/ADFS Authentication**.
4. Click **Lock**.
5. In the **SAML General Information** section, set **Activate Scheme** to **yes**.
6. In the **Identity Provider** section, click **Ex/Import**. Then, click **Import from File...** and select the file retrieved in Step 1.

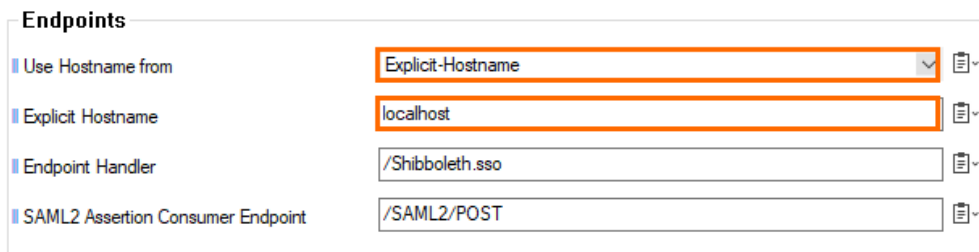


7. Click **Send Changes**.
8. In the **Attributes** section, specify the **Assertion Name ID** and select **um:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** from the drop-down menu.
9. Click **Send Changes**.
10. Specify values for the following:
  - **User Attribute** – Select **Name ID (um:oasis:names:tc:SAML:1.1:nameid-format:emailAddress)** from the drop-down menu.
  - **Group Attribute** – Select **Attribute(Groups)** from the drop-down menu.
11. In the **Certificates** section, specify values for the following:
  - **Enable Assertion Encryption** – Clear the check box.
  - **Enable Assertion Signing** – Clear the check box.

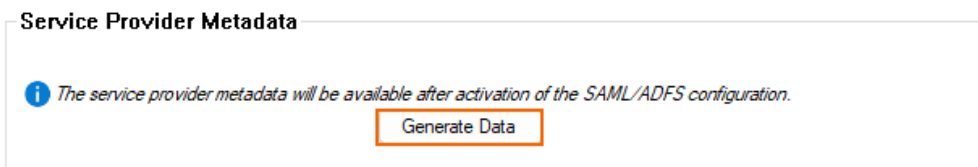


12. In the left menu of the **SAML/ADFS Authentication** window, click **Configuration Mode** and select **Switch to Advanced**.
13. In the **Endpoints** section, specify values for the following if SAML/ADFS is not used for Firewall Authentication. Otherwise, you can skip this step.
  - **Use Hostname from** – Select **Explicit-Hostname** from the drop-down menu.

- **Explicit Hostname** - Enter localhost.



- Click **Send Changes** and **Activate**.
- On the firewall, go to **CONTROL > Services > Box Services**.
- Restart the authentication daemon (phibs).  
 For High Availability (HA) setups, you must restart the service on both units.
- Go back to **CONFIGURATION > Configuration Tree > Infrastructure Services > Authentication Service**.
- In the left menu, click **SAML/ADFS Authentication**.
- Click **Lock**.
- In the **Service Provider Metadata** section, export the metadata by clicking **Generate Data**.



- Copy the information and save it to your local machine in an .xml file. This file has to be uploaded in Azure at a later stage.  
 Specify the hostname only if SAML/ADFS is not used for Firewall Authentication.
- Click **Send Changes** and **Activate**.

### Step 3. Finalize the SAML Configuration in Microsoft Azure

- Log into the Azure portal: <https://portal.azure.com>
- In the left menu, click **All services** and search for **Microsoft Entra ID**.
- Click **Microsoft Entra ID**. The **Microsoft Entra ID** blade opens.
- In the left menu, select **Enterprise applications**.
- In the **Enterprise applications** blade, click **All applications**.
- Click on the application you created in Step 1, e.g., *Campus-SAML-Endpoint*.
- In the left menu, click **Single sign-on**.
- Select **SAML**. The **Single sign-on** blade opens.
- 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

Identifier (Entity ID) **Required**

Reply URL (Assertion Consumer Service URL) **Required**

Sign on URL *Optional*

Relay State *Optional*

Logout Url *Optional*

[Edit](#)

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://localhost/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

« [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*

2

User Attributes & Claims

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

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](#)

## Step 4. Finalize the Barracuda CloudGen Firewall SAML Configuration

1. Connect to your Barracuda CloudGen Firewall and log in.
2. Go to **CONFIGURATION > Configuration Tree > Infrastructure Services > Authentication Service**.
3. In the left menu, click **SAML/ADFS Authentication**.
4. Click **Lock**.
5. In the **Identity Provider** section, click **Ex/Import**.
6. From the drop-down menu, select **Clear**.

**Identity Provider**

Identity Provider Metadata

IDP Entity ID

**Ex/Import** DATA set

Export to File...

**Clear**

Import from File...

07-41d3-b313-d385

Other

7. In the **Identity Provider** section, click **Ex/Import**.
8. From the drop-down menu, select **Import from File**.
9. Select the file downloaded in Step 3 and import it.
10. Click **Send Changes** and **Activate**.
11. Restart the authentication daemon (phibs) in **CONTROL > Services > Box Services**.

For High Availability (HA) setups, you must restart the service on both units.

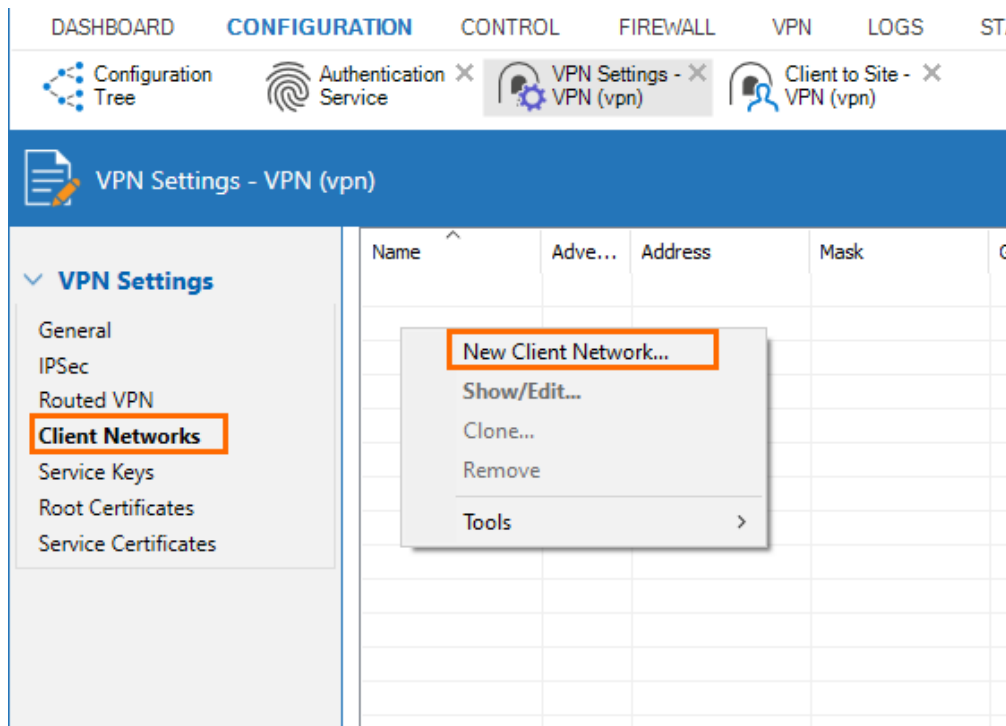


## Step 5. VPN Configuration of the Barracuda CloudGen Firewall

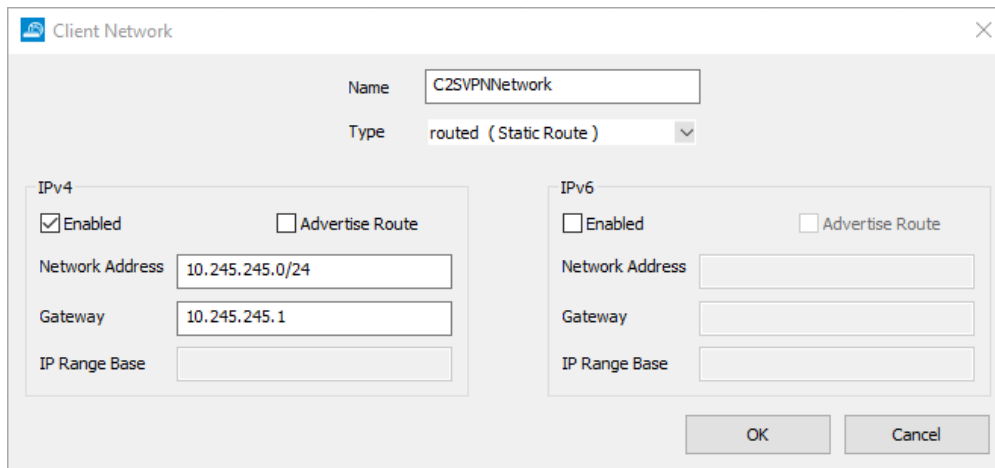
1. Connect to your Barracuda CloudGen firewall and log in.
2. Go to **CONFIGURATION > Configuration Tree > Assigned Services > VPN (VPN-Service) > VPN Settings**.
3. In the left menu, click **General**.
4. Click **Lock**.
5. In the **Service** section, specify values for the following:
  - **Private key** - Click to generate a new private key. Select a key length and click **OK**.
  - **Certificate** - Click to generate a new certificate. Enter a name and click **OK**.

Default Server Certificate		<explicit>	
Private key		Hash: PKOECK 2048 Bits	
Certificate		Hash: PKOECK 2048 Bits (self signed)	

6. Click **Send Changes** and **Activate**.
7. In the left menu, click **Client Networks**.
8. Click **Lock**.
9. In the right menu, right-click in the table and select **New Client Network** from the drop-down menu.

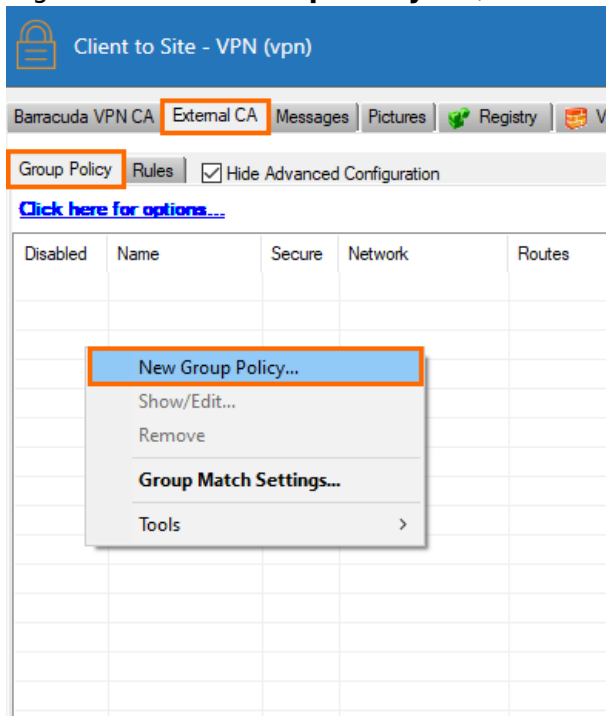


10. The **Client Network** window opens. Specify values for the following:
  - **Name** - Enter a name.
  - **Network Address** - Enter the network address.
  - **Gateway** - Enter the gateway.

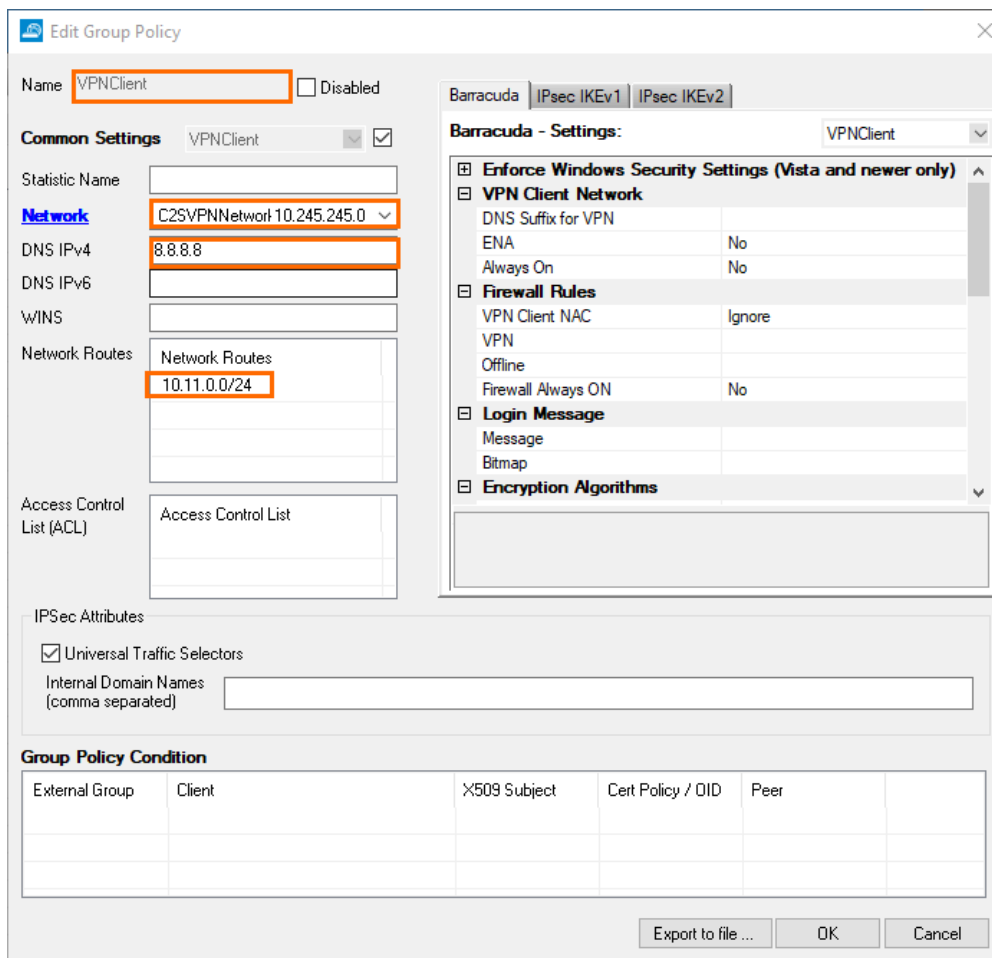


The 'Client Network' window shows configuration for a network named 'C2SVPNNetwork'. The 'Type' is set to 'routed (Static Route)'. Under the 'IPv4' section, 'Enabled' is checked, 'Advertise Route' is unchecked, 'Network Address' is '10.245.245.0/24', 'Gateway' is '10.245.245.1', and 'IP Range Base' is empty. The 'IPv6' section has 'Enabled' unchecked, 'Advertise Route' unchecked, and all other fields are empty. 'OK' and 'Cancel' buttons are at the bottom right.

11. Click **OK**.
12. Click **Send Changes** and **Activate**.
13. Go to **CONFIGURATION > Configuration Tree > Assigned Services > VPN (VPN-Service) > Client to Site**.
14. Click **Lock**.
15. Open the **External CA** tab.
16. Select **Click here for options**.
17. Select the check-box to **Enable SAML support**.
18. Click **OK**.
19. Right-click in the **Group Policy** tab, and select **New Group Policy** from the drop-down menu.



20. The **Edit Group Policy** window opens. Specify values for the following:
  - **Name** - Enter a name.
  - **Network** - Select the client network created before.
  - **DNS IPv4** - Enter a DNS server.
  - **Network Routes** - Enter one or more routes if applicable.



**Edit Group Policy**

Name: **VPNClient** ☐ Disabled

**Common Settings** VPNClient ☒

Statistic Name:

**Network** C2SVPNNetwork-10.245.245.0

DNS IPv4: 8.8.8.8

DNS IPv6:

WINS:

Network Routes: Network Routes

10.11.0.0/24

Access Control List (ACL): Access Control List

IPSec Attributes

☒ Universal Traffic Selectors

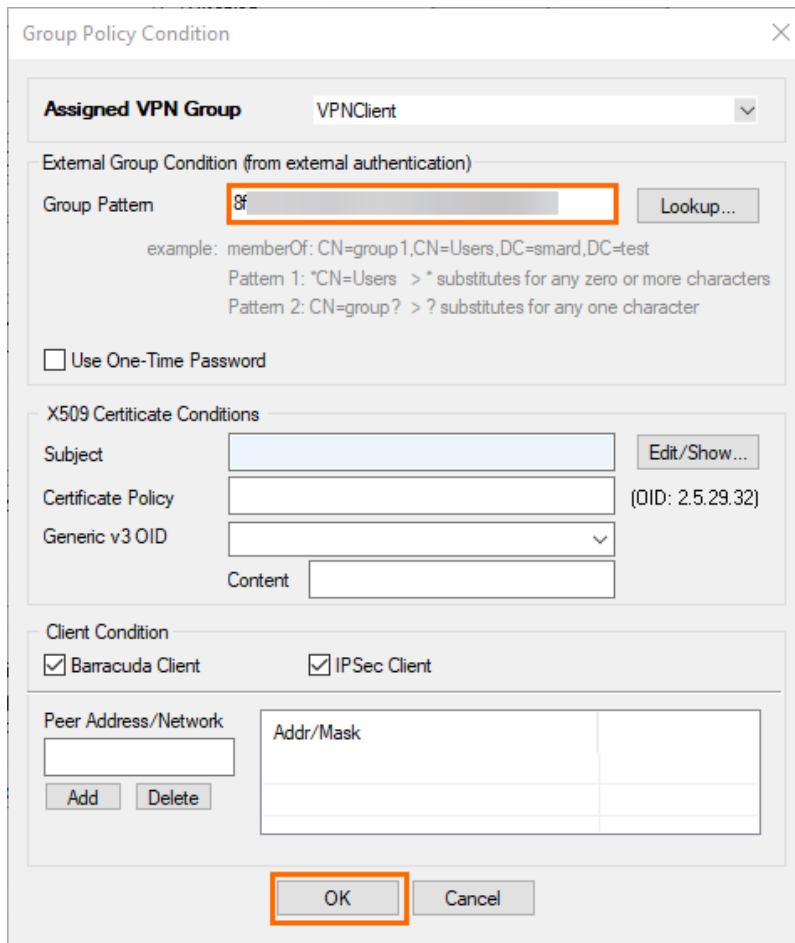
Internal Domain Names (comma separated):

**Group Policy Condition**

External Group	Client	X509 Subject	Cert Policy / OID	Peer	

Export to file ... OK Cancel

21. Stay in the **Edit Group Policy** window. In the **Group Policy Condition** section, double-click to add a new entry.
22. The **Group Policy Condition** window opens. Specify values for the following:
  - **Group Pattern** - Enter the object ID of your Microsoft Entra ID group that will be enabled to use client-to-site VPN.



The image shows a 'Group Policy Condition' dialog box. At the top, 'Assigned VPN Group' is set to 'VPNClient'. Under 'External Group Condition (from external authentication)', the 'Group Pattern' field contains '&' and is highlighted with an orange box. Below it, there is an example: 'memberOf: CN=group1,CN=Users,DC=smard,DC=test' and two pattern rules. A 'Use One-Time Password' checkbox is unchecked. The 'X509 Certificate Conditions' section has fields for 'Subject', 'Certificate Policy', and 'Generic v3 OID', with an 'Edit/Show...' button. The 'Client Condition' section has checkboxes for 'Barracuda Client' and 'IPSec Client', both of which are checked. Below this is a 'Peer Address/Network' section with a table for 'Addr/Mask' and 'Add/Delete' buttons. The 'OK' button at the bottom is highlighted with an orange box.

23. Click **OK**.
24. Click **OK**.
25. Click **Send Changes** and **Activate**.

## Step 6. Configuration of the VPN Client

- In the VPN configuration, you must select **SAML** as **Authentication Method**.
- Transport mode for the VPN tunnel must be either **TCP** or **Optimized** to guarantee 100% functionality.

- For the configuration of the Windows client, see [How to Configure the Barracuda VPN Client for Windows](#).
- For the configuration of the macOS client, see [How to Configure the Barracuda VPN Client for macOS](#).
- For more information on establishing VPN connections, see [How to Establish a VPN Connection Using Barracuda VPN Client for Windows](#) or [How to Establish a VPN Connection Using Barracuda VPN Client for macOS](#).

---

## Further Information

---

- For more information on client-to-site configuration, see [Client-to-Site VPN](#).
- For more information on the VPN client, see [Overview - VPN Client & Network Access Client 5.x](#).

## Figures

1. select\_enterprise.png
2. add\_new\_app.png
3. create\_own\_app.png
4. create\_own\_2.png
5. overview\_properties.png
6. assignment\_required.png
7. sso\_saml.png
8. copy\_url.png
9. edit\_basic.png
10. add\_identifier\_ui.png
11. user\_attributes.png
12. add\_gclaim.png
13. claim\_sg.png
14. close\_uac.png
15. download\_fed\_metadata.png
16. enable\_saml.png
17. cert\_settings.png
18. endpoints.png
19. generate\_data.png
20. upload\_metadata.png
21. add\_file.png
22. cgf\_saml\_conf.png
23. fed\_metadata\_download2.png
24. clear.png
25. vpn\_key.png
26. create\_client\_networks1.png
27. c2s\_network.png
28. group\_policy1.png
29. group\_policy2.png
30. group\_policycondition.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.