

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

<https://campus.barracuda.com/doc/112167358/>

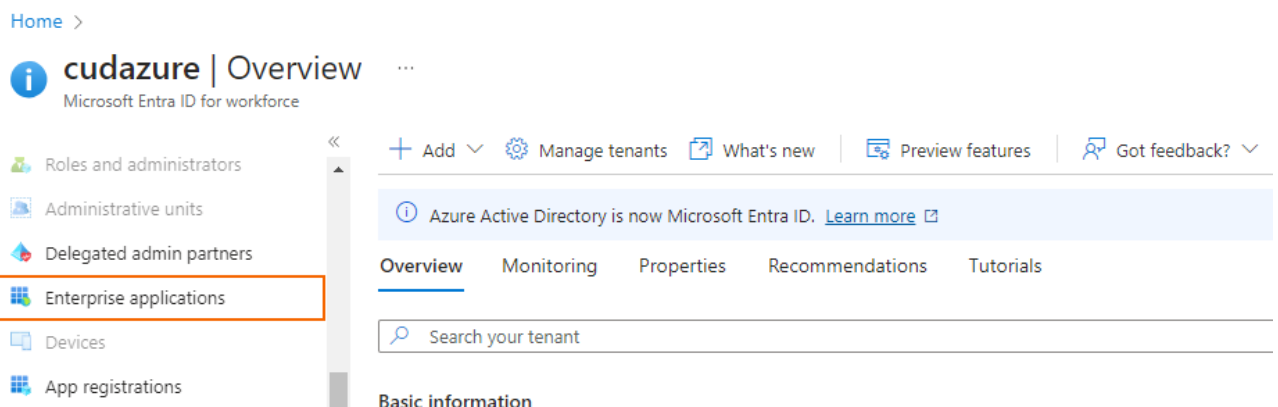
Follow the guide below to create a SAML endpoint in Microsoft Azure and to configure a Barracuda CloudGen Firewall to use SAML authentication for the client-to-site VPN service.

Before You Begin

- Create and configure a VPN service. For more information, see [VPN](#).
- You must have an existing user group in your 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](#)

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

[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)

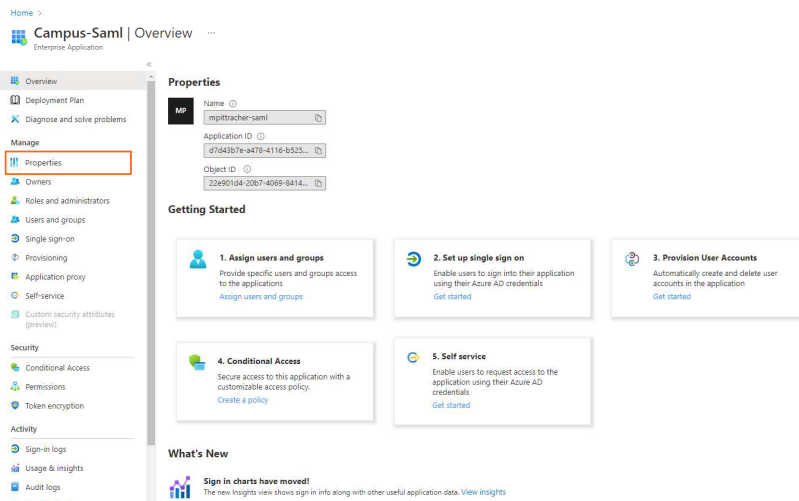
We found the following applications that may match your entry
We recommend using gallery applications when possible.

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

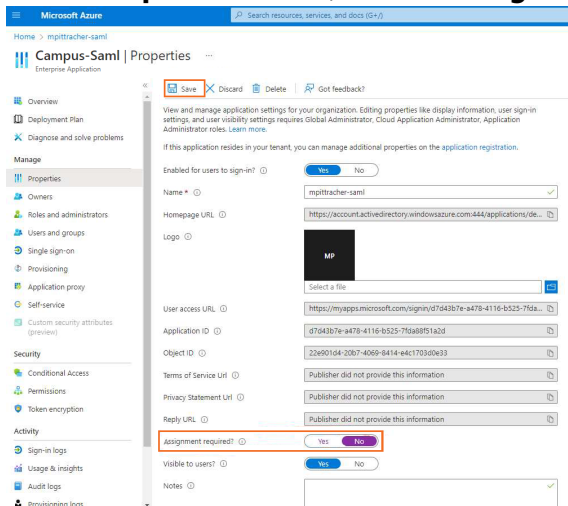
9. Click **Create**.

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

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

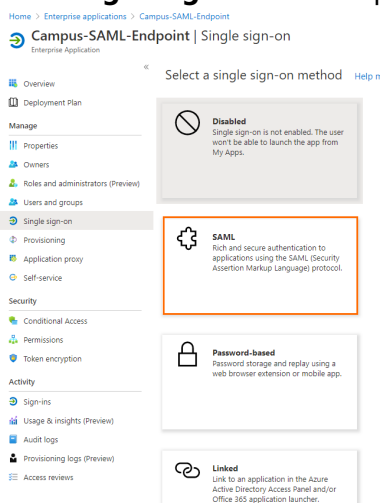


11. In the **Properties** blade, disable **Assignment required** and click **Save**.

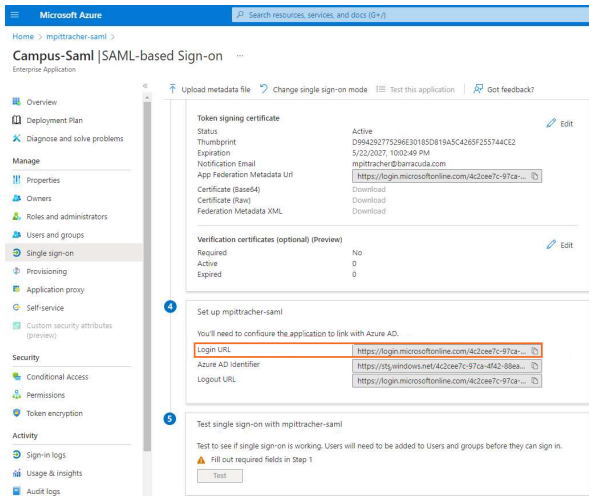


12. In the left menu, click **Single sign-on**.

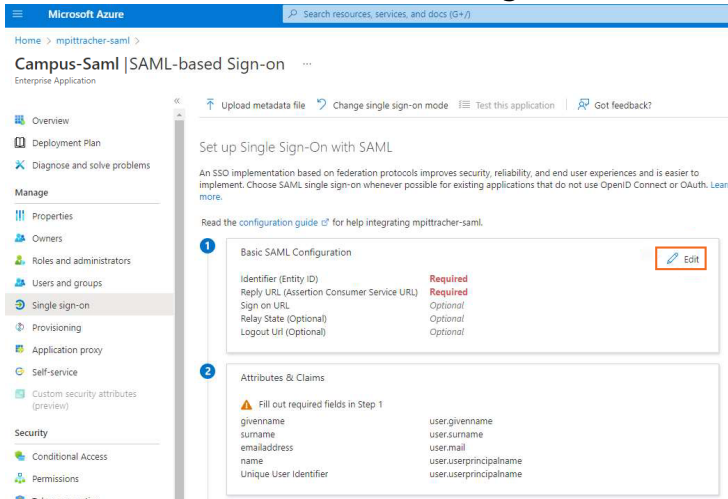
13. The **Single sign-on** blade opens. Select **SAML**.



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



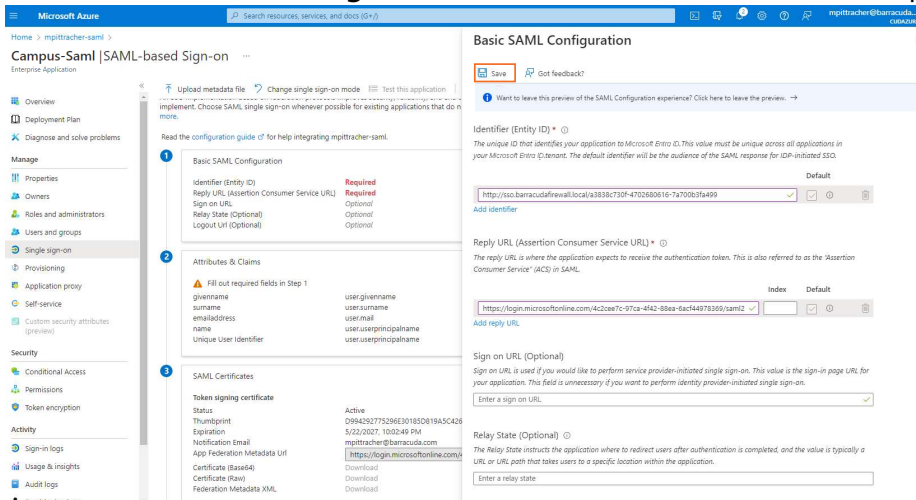
15. Click **Edit** next to **Basic SAML Configuration**.



16. Click **Add reply URL** and paste the copied URL.

17. Open the SAML configuration on your Barracuda CloudGen Firewall, and copy the **Service Provider Entity ID**.

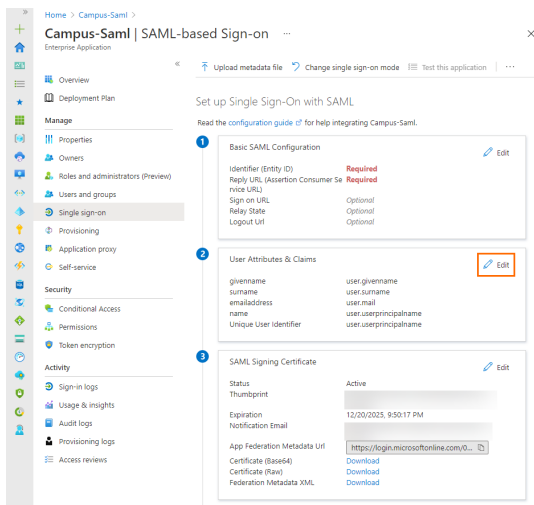
18. In the **Basic SAML Configuration** blade, click **Add identifier** and paste the copied login URL.



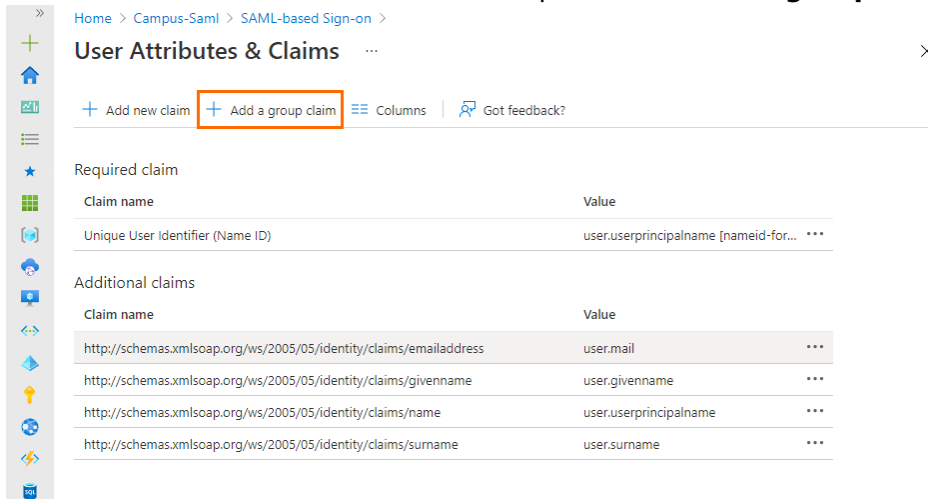
19. Click **Save**.

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

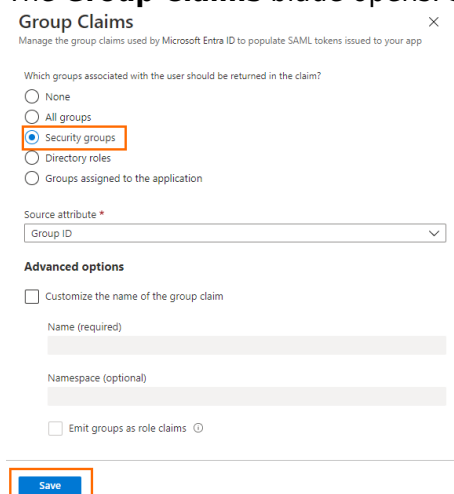
21. In the **User Attribute & Claims** section, click **Edit**.



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



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



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

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

User Attributes & Claims ...

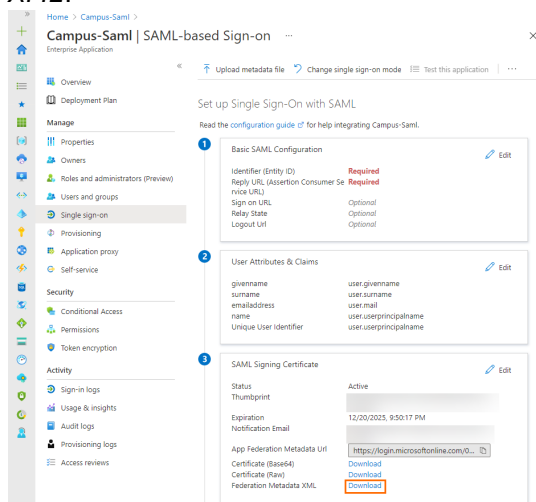

[+ Add new claim](#) | [+ Add a group claim](#) | [Columns](#) | [Got feedback?](#)

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*.



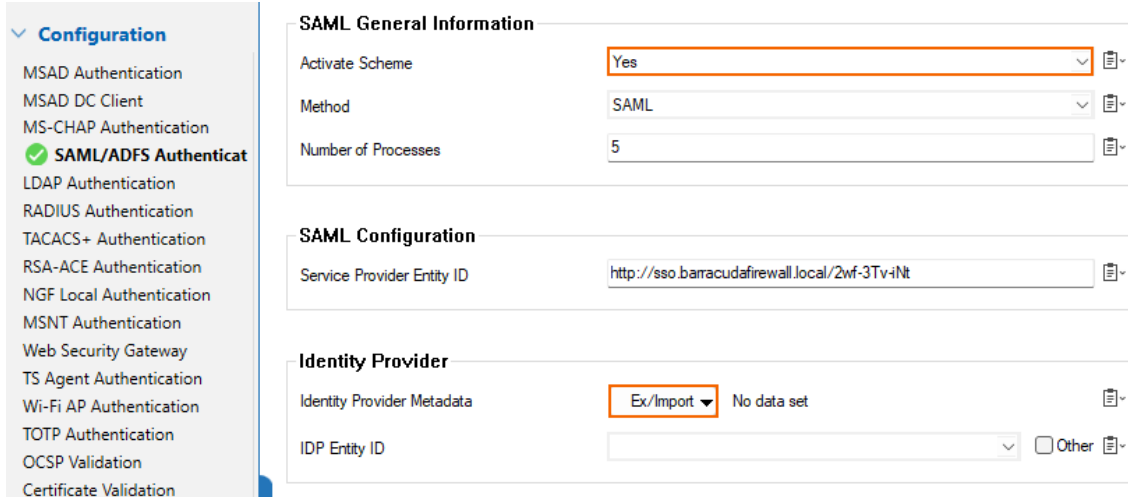
Note that some browsers might block the *.xml file.

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.



Configuration

- MSAD Authentication
- MSAD DC Client
- MS-CHAP Authentication
- SAML/ADFS Authentication**
- LDAP Authentication
- RADIUS Authentication
- TACACS+ Authentication
- RSA-ACE Authentication
- NGF Local Authentication
- MSNT Authentication
- Web Security Gateway
- TS Agent Authentication
- Wi-Fi AP Authentication
- TOTP Authentication
- OCSP Validation
- Certificate Validation

SAML General Information

Activate Scheme	Yes
Method	SAML
Number of Processes	5

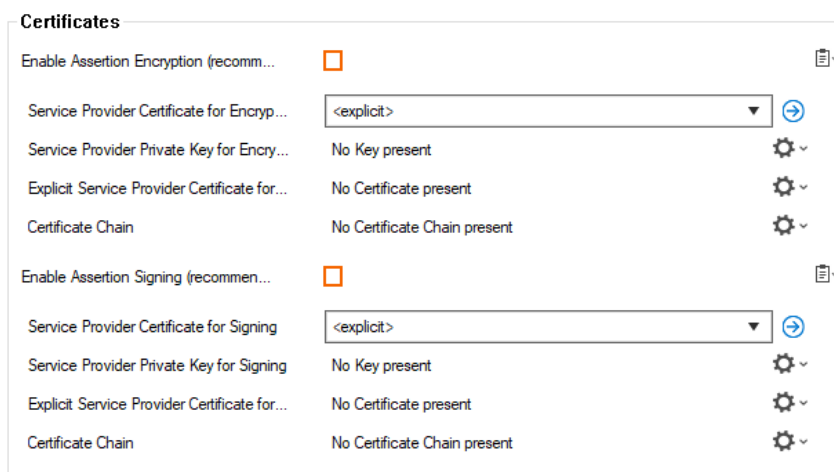
SAML Configuration

Service Provider Entity ID	http://sso.barracudafirewall.local/2wf-3Tv-iNt
----------------------------	--

Identity Provider

Identity Provider Metadata	Ex/Import	No data set
IDP Entity ID		Other

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.

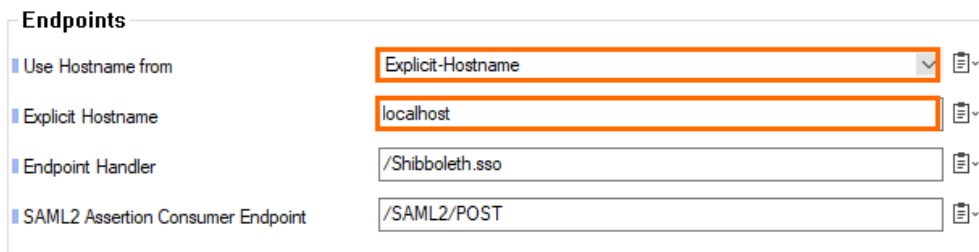


Certificates

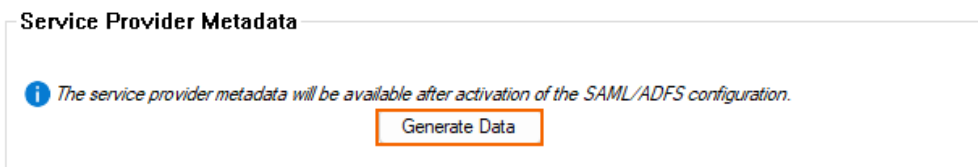
Enable Assertion Encryption (recomm...	<input type="checkbox"/>
Service Provider Certificate for Encryp...	<explicit>
Service Provider Private Key for Encry...	No Key present
Explicit Service Provider Certificate for...	No Certificate present
Certificate Chain	No Certificate Chain present
Enable Assertion Signing (recommen...	<input type="checkbox"/>
Service Provider Certificate for Signing	<explicit>
Service Provider Private Key for Signing	No Key present
Explicit Service Provider Certificate for...	No Certificate present
Certificate Chain	No Certificate Chain present

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.



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



21. 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.
22. Click **Send Changes** and **Activate**.

Step 3. Finalize the 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**. The **Microsoft Entra ID** blade opens.
4. In the left menu, select **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. Select **SAML**. 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)	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**.

[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.

"serviceProviderMetadata.xml"

Add

Cancel

2

User Attributes & Claims

Edit

givenname

user.givenname

11. Click **Save**.

Basic SAML Configuration

Save

Get feedback?

Identifier (Entity ID) *

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

Default
http://sso.barracudafirewall.local/vni-8E6-1UE

Reply URL (Assertion Consumer Service URL) *

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

Default
https://localhost/Shibboleth.sso/SAML2/POST

Sign on URL

Enter a sign on URL

Relay State

Enter a relay state

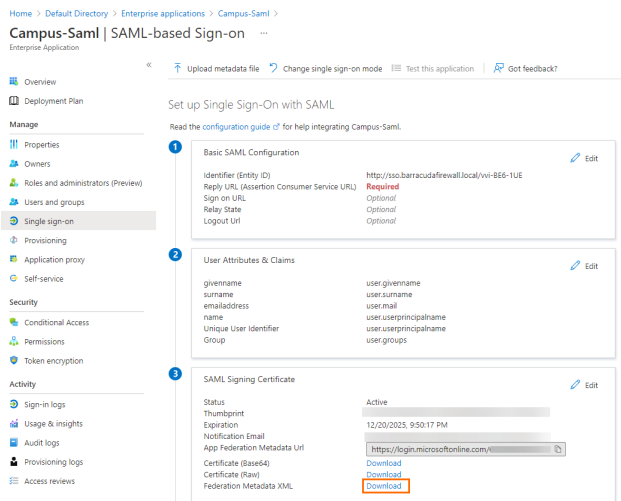
Logout URL

Enter a logout url

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

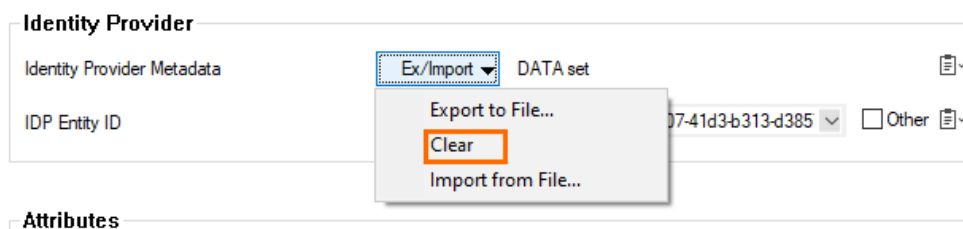
You are now back in the **Single sign-on** blade.

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



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**.





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.

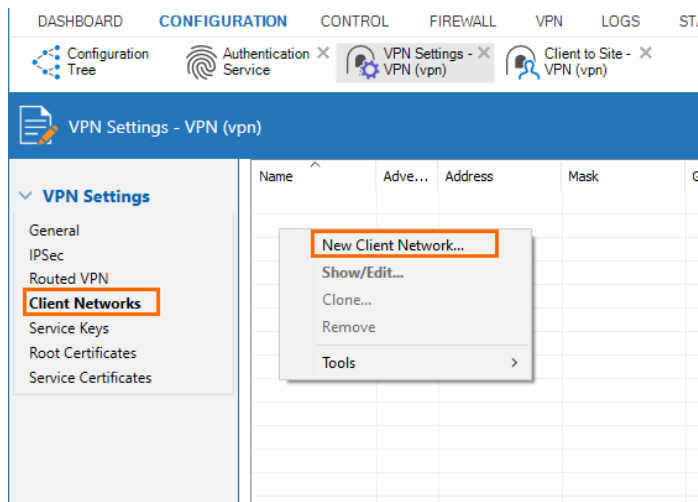
Step 5. VPN Configuration of the Barracuda CloudGen Firewall

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**.

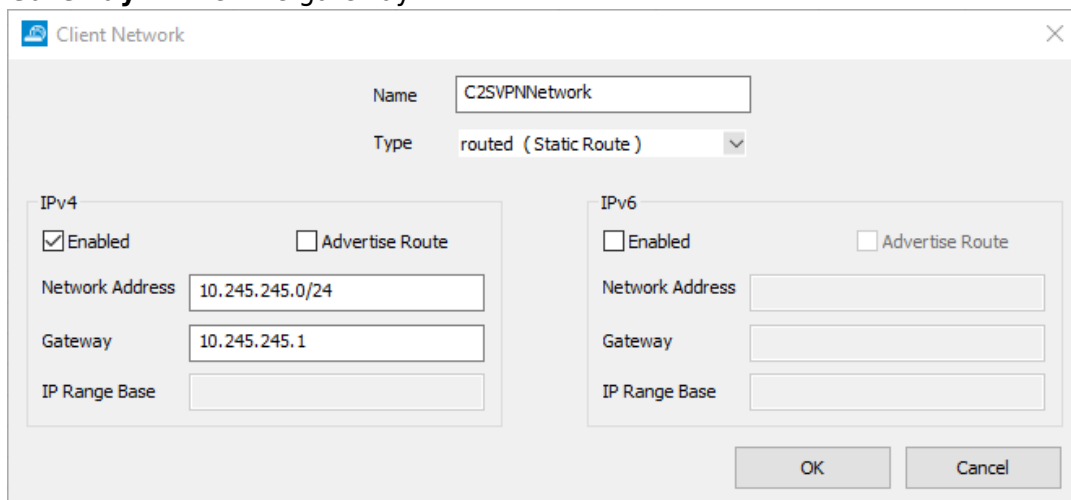
4. Click **Lock**.
5. In the **Service** section, specify values for the following:
 - **Private key** – Click to generate a new private key. Select a key length and click **OK**.
 - **Certificate** – Click to generate a new certificate. Enter a name and click **OK**.

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.

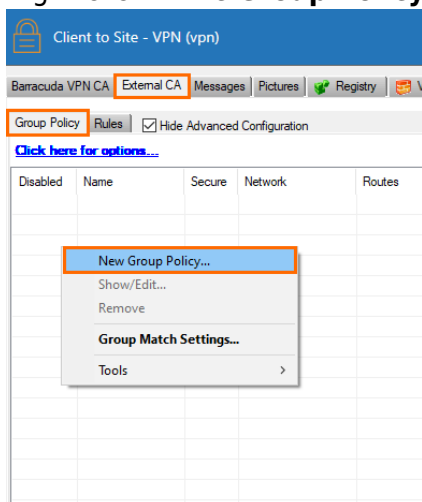


10. The **Client Network** window opens. Specify values for the following:
 - **Name** – Enter a name.
 - **Network Address** – Enter the network address.
 - **Gateway** – Enter the gateway.

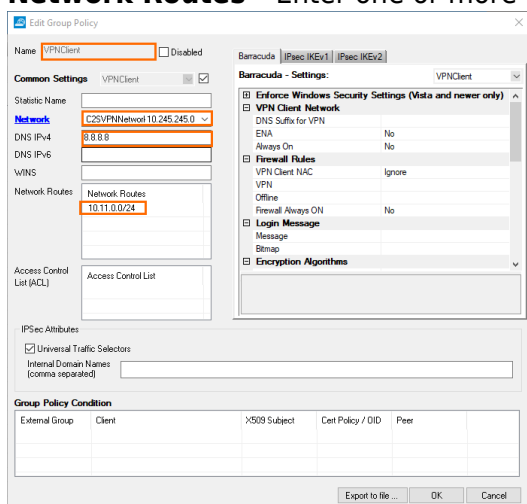


11. Click **OK**.
12. Click **Send Changes** and **Activate**.

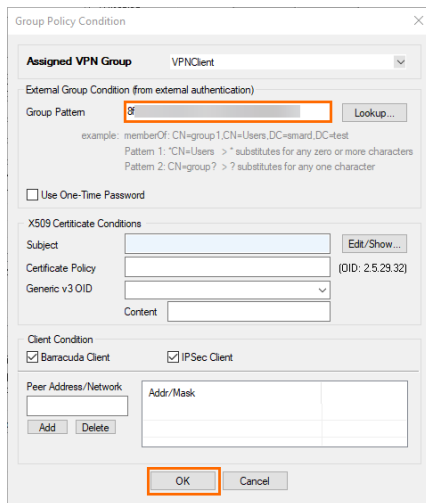
13. Go to **CONFIGURATION > Configuration Tree > Assigned Services > VPN (VPN-Service) > Client to Site**.
14. Click **Lock**.
15. Open the **External CA** tab.
16. Select **Click here for options**.
17. Select the check-box to **Enable SAML support**.
18. Click **OK**.
19. Right-click in the **Group 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.



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.



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.