

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 <u>Base Licensing and Subscriptions</u>.

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 application	ons Overview
cudazure - Microsoft Entra ID for workfo	irce
Overview A	+ New application 🖗 Got feedback?
() Overview	Overview Tutorials
X Diagnose and solve problems	Search your tenant
Manage	
All applications	Basic information
7. The Browse Microsoft Entra Ga	Illery blade opens. Click Create your own application.
Home > Enterprise applications Ov	verview >
Browse Microsoft En	tra Gallery
browse interosoft En	tra Gallery
+ Create your own application	Sot feedback?
The Microsoft Entra App Gallery is a cat	alog of thousands of apps that make it eas
their apps. Browse or create your own a	pplication here. If you are wanting to publ
Search application	Single Sign-on : All
9 Enter the name of your application	n and select Integrate any other application you den't
find in the gallery (Non-gallery	v).
Create your own application	×
🖗 Got feedback?	
What's the name of your app?	
Campus-Saml	
What are you looking to do with your application?	
 Contigure Application Proxy for secure remote access to an on-premises a Register an application to integrate with Microsoft Entra (App you're deve 	loping)
Integrate any other application you don't find in the gallery (Non-gallery)]

Campus-S	ml 🗸
What are yo	I looking to do with your application?
Config	re Application Proxy for secure remote access to an on-premises applicatio
🔿 Registe	an application to integrate with Microsoft Entra (App you're developing)
	e any other application you don't find in the calleny (Non-calleny)
 Integra 	e any other application you don't find in the gallery (Non' gallery)
We fou We rec	nd the following applications that may match your entry mmend using gallery applications when possible.
We fou We rec	and the following applications that may match your entry mmend using gallery applications when possible.

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**.

Barracuda CloudGen Firewall



Deployment Plan			
	Name ①		
× Diagnose and solve problems	mpittracher-saml		
Manane	Application ID ①		
	d7d43b7e-a478-4116-b525 D		
A Queer	Object ID		
A Palor and administrators	22640104-2007-4003-8414 12		
	Getting Started		
Osers and groups			
Single signion			
Provisioning	1. Assign users and groups	2. Set up single sign on Table upset to size into their application	3. Provision User Accounts
Application proxy	to the applications	using their Azure AD credentials	accounts in the application
Generation Self-service	Assign users and groups	Get started	Get started
 Custom security attributes (preview) 			
Security		C. I. Sultannin	
Conditional Access	4. Conditional Access	Enable users to request access to the	
Permissions	Secure access to this application with a customizable access policy.	application using their Azure AD	
Token encryption	Create a policy	Get started	
Activity			

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.

Barracuda CloudGen Firewall



Campus-Samil (SAML-based Sign-on			
Conviction Conviction Conviction Conversion C	Campus-Saml SAML-bas	ed Sign-on	
	Overview	↑ Upload metadata file	sign-on mode 1 Test this application A Got feedback?
Stata Active Stata Active Thombyers Special Thombyers Stata Active Thombyers Special Thombyers Special Thompyers Special Thombyers Special Thompyers Special Thompyers Special Thompyers Spec	Deployment Plan	Token signing certificate	1.
A of your and usune processor Your and usune procesor Your and usune processor Your and usune procesor You	× Simmer and other meltions	Status	Active
Marage Instruction famil methods/relations/action IP Properties The finance in Maradia to U methods/relations/actions/a	 Dragnose and some problems 	Thumbprint	D994292775296E30185D819A5C4265F255744CE2
If Properties App Federation Metabla UI <u>Http://grappm.microsoftnorime.com/42/2eeft-6/fraD</u> If Owers Certificite (aso4) Download Void read owers 0 Download If Owers 0 Download Owers Download Download Owers Download	Manage	Notification Email	mpittracher@barracuda.com
Control Based Control	III Properties	App Federation Metadata Url	https://login.microsoftonline.com/4c2cee7c-97ca
Control Environmentations Solves and groups Sol		Certificate (Base64)	Download
	A Owners	Certificate (Raw)	Download
	& Roles and administrators	Federation Metadata XML	Download
	Users and groups	Verification certificates (optional) (Pr	eview)
Develoaning Active 0 Experied Active 0	Single sign-on	Required	No
Specification procy Set service Set up mpittracher-saml Vour area to configure the application to link with Azure A.D Login UR: Set up mpittracher-saml Conditional Access Conditional Access Conditional Access Text single sign-on with mpittracher-saml Text single sign-on us working. Users will need to be added to Users and groups before they can sign in. Sign-in hogs: Set up mpittra Text single sign-on us working. Users will need to be added to Users and groups before they can sign in. Text single sign-on is working. Users will need to be added to Users and groups before they can sign in. Text to required fields in they 1	Provisioning	Active	0
Serieserke Set op mpittacher-sami Set of the splitation to link with Acure AC. (cogin GL, http://tigmmicrosoftwrite.com/42/set/c-976C, http://tigmmicrosoftwrite.com/42/set/set/c-976C, http://tigmmicrosoftwrite.com/42/set/c-976C, htt	Application proxy	Expired	u u
Conditional Access Conditional	G Self-service	Set up mnittracher-saml	
purners) Total and the departure and the second and the departure and t	Custom security attributes	Veriff and to confirm the evolution	and the second and
Sacuthy Login co. Ittp://gruphicosoftmile.com/42ceef-0fra0 & Conditional Access Acara AD identifier Ittp://gruphicosoftmile.com/42ceef-0fra0 & Conditional Access Login AL identifier Ittp://gruphicosoftmile.com/42ceef-0fra0 B By International Access Test single sign-on with mpittracter-saml Test single sign-on with mpittracter-saml Test to see if single sign-on is working. User will need to be added to Users and groups before they can sign in. In Usage A ministic	(preview)	tou in need to considere the apprication	D ID ID IN WITH AZDIE AD.
Conditional Access Actine au Determine Integr/(tig) windows.met/accestr2/stra-ut2-steel Deterministors Text single sign-on with implituacter-saml Text single sign-on with implituacter-saml Text to see if single sign-on is working. Uses will need to be added to Users and groups before they can sign in. Text to see if single sign-on is working. Uses will need to be added to Users and groups before they can sign in. Text to see if single sign-on is working. Uses will need to be added to Users and groups before they can sign in. Text to see if single sign-on is working. Uses will need to be added to Users and groups before they can sign in. Text to see if single sign-on is working.	Security	LOGIN UKL	https://login.microsoftonline.com/4c2cee7c-97ca
termissions termissions termissions Total single sign-on with mpittrader-sam! Text single sign-on with mpittrader-sam! Text single sign-on is working. Users will need to be added to Users and groups before they can sign in. A fill dur required fields in they 1 Text Text	Conditional Access	Azure Au identifier	https://sts.windows.net/4c2cee7c;97ca-4f42-88ea
token excryption Test single sign-on with mphtracher-sam! Test single sign-on with mphtracher-sam! Test to see single sign-on with mphtracher-sam! Test Test	A Permissions	Logour one	nttps://login.microsottonine.com/4c2cee7c-97ca
Activity Test single sigm-on with mpittacher-sam! 9 Sigm-in logs 11 Usage & insights Test to see if single sigm-on su working. Users will need to be added to Users and groups before they can sign in. A Fil bus regime fields in Step 1 Test Test Test Test Test Test Test Test	Token encryption	•	
Signini logs Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in. All out required fields in Step 1 Test	Activity	Test single sign-on with mpittrache	r-saml
Charge & insights Test	Sign-in logs	Test to see if single sign-on is working	Users will need to be added to Users and groups before they can sign in.
Test	A Design & Installate	A Hill out required fields in Step 1	
	in obage or inorgino	Test	

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.

	inte i campao cami i civine casca sign on i		
U	ser Attributes & Claims		
Н	⊢ Add new claim 🕂 Add a group claim 📰 Columns 🗏 🔊 Got feedback?		
Re	quired claim		
C	llaim name	Value	
L	Inique User Identifier (Name ID)	user.userprincipalname [nameid-for	•••
٨	Iditional claims		
AC			
C	claim name	Value	
h	ttp://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail •	•••
h	ttp://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	•••
h	ttp://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	•••
	a and a subsequence of the second		

- 2
- 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	\sim
Advanced options	
Customize the name of the group claim	
Name (required)	
Namespace (optional)	
Emit groups as role claims ①	
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 feed	back?	
Required claim		
Claim name	Value	

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 <u>Claims in SAML</u> 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 <u>Configure group claims for applications by using Microsoft Entra ID</u>.

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.

 In the Identity Provider section, click Ex/Import. Then, click Import from File... and select the file retrieved in Step 1.

 Configuration 	SAML General Information			
MSAD Authentication	Activate Scheme	Yes	✓ Ē*	
MSAD DC Client	Method	SAML	∨ Ē*	
MS-CHAP Authentication SAML/ADFS Authenticat	Number of Processes	5	Ēv	
LDAP Authentication RADIUS Authentication				
TACACS+ Authentication	SAML Configuration			
RSA-ACE Authentication NGF Local Authentication	Service Provider Entity ID	http://sso.barracudafirewall.local/2wf-3Tv-iNt	Ē	
MSNT Authentication				
Web Security Gateway TS Agent Authentication	Identity Provider			
Wi-Fi AP Authentication	Identity Provider Metadata	Ex/Import	=~	
TOTP Authentication OCSP Validation	IDP Entity ID	×	◯ Other 📳	
Certificate Validation				

- 7. Click Send Changes.
- 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:nameidformat: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		Ē
Service Provider Certificate for Encryp	<explicit></explicit>	▼ ⊝
Service Provider Private Key for Encry	No Key present	¢.∼
Explicit Service Provider Certificate for	No Certificate present	Ö.
Certificate Chain	No Certificate Chain present	¢.∼
Enable Assertion Signing (recommen		Ēv
Service Provider Certificate for Signing	<explicit></explicit>	▼
Service Provider Private Key for Signing	No Key present	Ö.
Explicit Service Provider Certificate for	No Certificate present	¢.~
Certificate Chain	No Certificate Chain present	\$4~

- 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.





22. Click Send Changes and Activate.

Step 3. Finalize the SAML Configuration in Microsoft Azure

- 1. Log into the Azure portal: <u>https://portal.azure.com</u>
- 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.

Barracuda CloudGen Firewall



Campus-SAML-Enc Enterprise Application	lpoint S	AML-based Sign-on		
	≪ ⊼	Upload metadata file 均 Change si	ngle sign-on mode 🛛 🗐	Test this application ···
👢 Overview	0			
Deployment Plan	•	Basic SAML Configuration		🖉 Edit
		Identifier (Entity ID)	Required	
Manage		Reply URL (Assertion Consumer S rvice URL)	e Required	
Properties		Sign on URL	Optional	
🎎 Owners		Relay State	Optional Optional	
🤱 Roles and administrators (Previe	ew)	Logour on	Optional	
Select the file downloade	ed in Step	2 and click Add .		
Home > Enterprise applications > Car	mpus-SAML-Endr	point >		
Campus-SAML-Endpo	int SAML	-based Sign-on		×
Overview	↑ Upload n	netadata file 🂙 Change single sign-on m	ode 🛛 🗮 Test this application	on
Deployment Plan	Upload m	etadata file.		
	Values for the	e fields below are provided by Campus-S/	ML-Endpoint. You may ei	ther enter those
Manage	Endpoint.	my, or upload a pre-comigured SAME me	tadata me n provided by (ampus-same-
Properties	"serviceProvi	derMetadata.xml"		Р
Owners	- Add	Canad		
Roles and administrators (Preview)	Add	Cancer		
Users and groups	2 Use	r Attributes & Claims		7 Edit
Single sign-on	give	nname user.givenna	me	
-		2		
Click Save.				
Click Save. Basic SAML Configuration		×		
Click Save. Basic SAML Configuration		×		
Click Save. Basic SAML Configuration Set of the obset Mentifier (Entity ID) * The addout identifier will be the audience of the SAML response for ID+-induced 350	Refusit	×		
Click Save. Basic SAML Configuration Save R of treeback Media identifier (Entity ID) * © The default identifier will be the oudernee of the SAML response for IDP-initiated SSO Integrity/ssobaracudatirewall.local/vie-866-10E	Default	×		
Click Save. Basic SAML Configuration So of tredback Mentifer (Entity ID) * © The default identifier will be the audience of the SAML response for IDP-initiated SSO Metry/Stac barracudatfreewall local/vei-866-1UE	Default	×		
Click Save. Basic SAML Configuration © See @ Contreatback Merging See @ Contreatbac	Default	×		
Click Save. Basic SAML Configuration Configuratio	Default Default Default Default	×		
Click Save. Basic SAML Configuration Configu	Default Default Default Default	×		
Click Save Basic SAML Configuration	Default Default Default U	×		
Click Save. Basic SAML Configuration Configurati	Default Default Default 0 0 0	×		
Click Save. Basic SAML Configuration Configu	Default Default Default	×		

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.



«	$ar{\uparrow}$ Upload metadata file $^{>}$ Change single sign-on	mode 📧 Test this application 🎘 Got feedback?	
4 Overview			
Deployment Plan	Set up Single Sign-On with SAML		
Manage	Read the configuration guide 🖒 for help integrating Ca	impus-Saml.	
Properties	Basis SAMI Configuration		
A Owners	base skille configuration		0
 Roles and administrators (Preview) 	Identifier (Entity ID)	http://sso.barracudafirewall.local/vvi-BE6-1UE	
	Sign on URI	Ontional	
Users and groups	Relay State	Optional	
Single sign-on	Logout Url	Optional	
Provisioning			
Application proxy	User Attributes & Claims		1
 Self-service 	givenname	user.givenname	-
	surname	user.sumame	
Security	emailaddress	user.mail	
Conditional Access	name	user.userprincipalname	
A Darmissions	Group	user.oserprincipalitame user.oroups	
 Token encryption 	0		
Activity	SAML Signing Certificate		0
Sign-in logs	Status	Active	
🙀 Usage & insights	Thumbprint Expiration	12/20/2025 9:50:17 PM	
	Notification Email		
Audit logs	App Federation Metadata Url	https://login.microsoftonline.com//	2
Provisioning logs	Certificate (Base64)	Download	_
= Acress reviews	Certificate (Raw)	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	Ex/Import 🗸 DATA set	Ē×
IDP Entity ID	Export to File Clear)7-41d3-b313-d385 🗸 🗌 Other Ē∵
	Import from File	
A AL-MAN AND A		

Attributes

- 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.
- 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	Ø	<explicit></explicit>	•
Private key	Ø	Hash: PKOECK 2048 Bits	Ö ~
Certificate	Ø	Hash: PKOECK 2048 Bits (self signed)	Ö-

- 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.

IPv4 IPv6 Enabled Advertise Route Network Address 10.245.245.0/24	
Network Address 10.245.245.0/24 Network Address	vertise Route
Gateway 10.245.245.1 Gateway	
IP Range Base IP Range Base	

- 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.

Clie	ent to Site - VPN	(vpn)		
Barracuda V	PN CA External CA	Message	es Pictures 💕	Registry 🛛 😅 V
Group Polic	y Rules 🛛 🖓 Hide	Advanced	Configuration	
Click here	for options			
Disabled	Name	Secure	Network	Routes
			_	
	New Group Po	licy		
	Show/Edit			
	Remove			
	Group Match	Settings		
	Tools		>	

- 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.

mmon Setting	s VPNClient	Barracuda - Set	tings:	VPNCh	ent
atistic Name		Enforce Wir	ndows Security Sett	ings (Vista and ne	ewer only)
	COSVENIN-Invest 10 24E	245.0 .vv	Network		
	C25VFININEIMOIF10.245	243.0 V	r VPN	-	
IS IPv4	8.8.8.8	Always On		lo lo	
S IPv6		E Grawall But	lae .	~	
NS		VPN Client N	AC k	nore	
		VPN		,	
twork Routes	Network Routes	Offline			
	10.11.0.0/24	Firewall Alway	s ON N	lo	
		Login Mess	age		
		Message			
		Bitmap			
cess Control it (ACL)	Access Control List		Algorithms		
cess Control it (ACL) PSec Attributes	Access Control List		Algorithms		
cess Control It (ACL) PSec Attributes	Access Control List		Algorithms		
icess Control it (ACL) PSec Attributes Universal Tr Internal Domai	Access Control List		Algorithms		
cess Control t (ACL) PSec Attributes Internal Domai (comma separa	Access Control List		Algorithms		
cess Control t (ACL) PSec Attributes Universal Tr Internal Domai (comma separa	Access Control List affic Selectors Names ted		Algorithms		
cess Control t (ACL) PSec Attributes Universal Tr Internal Domai (comma separ sup Policy Cr	Access Control List affic Selectors Names sted		Algorithms		
cess Control t (ACL) PSec Attributes Internal Domai (comma separa oup Policy Co xternal Group	Access Control List affic Selectors Names Selector Selectors Client Client	×509 Subject	Cett Policy / DID	Peer	
cess Control t (ACL) PSec Attributes Universal Tr Internal Domai (comma separi oup Policy Cr xternal Group	Access Control List affic Selectors Names Client	X509 Subject	Agonithms	Peer	

- 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.



Assigned VPN G	roup	VPNClient			\sim
External Group Cond	dition (from	external auther	ntication)		
Group Pattern	ðf				Lookup
exampl	le: membe	rOf: CN=group	1,CN=Users,I	DC=smard,DC=	est
	Pattern	1: *CN=Users	> * substitut	es for any zero	or more characters
	Pattern	2: CN=group?	> ? substitut	es for any one	character
Use One-Time P	assword				
X509 Certificate Co	nditions				
Subject					Edit/Show
	_				
Certificate Policy					(UID: 2.5.29.32)
Generic v3 OID				~	
	Conten	t			
Client Condition					
Barracuda Client		IPSec C	lient		
Peer Address/Netw	ork 🗔				
		ddr/Mask			
Add Delete					
/ du Delete					

- 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 <u>How to Configure the Barracuda VPN Client for</u> <u>Windows</u>.
- For the configuration of the macOS client, see <u>How to Configure the Barracuda VPN Client for</u> <u>macOS</u>.
- For more information on establishing VPN connections, see <u>How to Establish a VPN Connection</u> <u>Using Barracuda VPN Client for Windows</u> or <u>How to Establish a VPN Connection Using Barracuda</u> <u>VPN Client for macOS</u>.

Further Information

- For more information on client-to-site configuration, see <u>Client-to-Site VPN</u>.
- 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.