

Configuring AzureAD for Open ID Connect on the Barracuda Web Application Firewall

<https://campus.barracuda.com/doc/92767250/>

Azure Active Directory (AD) is the identity provider responsible for authenticating users accessing web applications hosted on the Microsoft Azure cloud. Azure AD manages user identities along with applications. You should configure the Open ID Connect endpoints in Azure AD for web applications requiring protection from the Barracuda Web Application Firewall.

Perform the Following Steps to Configure Azure AD on the Barracuda Web Application Firewall

Step 1 - Create an HTTPS Service on the Barracuda Web Application Firewall.

For more information on how to create a HTTPS service, see [Creating an HTTPS Service](#)

Step 2 - Generate Azure AD Identity Provider Metadata URL

1. Log into the [Microsoft Azure Portal](#).
2. In the left pane, select **Azure Active Directory > App registrations > New registration**.
3. Specify the name for the application.
4. Specify the redirect URI to redirect the user back to the application. Retain the other settings to default.
5. Click **Register**.
6. Click **Endpoints** and copy the **OpenID Connect METADATA DOCUMENT** link.

This is the **Identity Provider Metadata URL** to be configured on the Barracuda Web Application Firewall in the **ACCESS CONTROL > Authentication Services > New Authentication Service > OpenID Connect** page. Example:

https://login.microsoftonline.com/<tenant_id>/v2.0/.well-known/openid-configuration

Step 3 - Configuring the Azure AD Open ID Connect Provider on Barracuda Web Application Firewall

1. In the **Real Name** box, specify a name to identify the Open ID Connect provider on the Barracuda Web Application Firewall. *Example: AzureAD*
2. Choose **Discovery URL** as the mode to identify the provider's endpoint configuration.
3. Specify the metadata URL of the Azure AD Open ID Connect. Example:
<https://dev-9wh7d1r1.auth0.com/.well-known/openid-configuration>
4. Click **Retrieve** to display all other details by default.



- Configure the client ID and client secret that you had noted down while performing the Azure AD configuration and then click **Add**. AzureAD Open ID Connect authentication service is displayed in the **Existing Authentication Service** section.



NAME	TYPE	SERVICE	CLIENT ID	CLIENT SECRET	STATUS	EDIT	DELETE
Internal	LDAP		127.0.0.1		Add	Edit	Delete
OAuth	OPENIDCONNECT		Okta		Add	Edit	Delete
			Auth0		Add	Edit	Delete
			azure_ad		Add	Edit	Delete
			Google		Add	Edit	Delete
Automation_managed	OPENIDCONNECT	OAuth2Service,OAuth2	Keycloak		Add	Edit	Delete
			Google		Add	Edit	Delete
			Auth0_server		Add	Edit	Delete
			Okta_server		Add	Edit	Delete

Step 4 - Configure the Authentication Policy for the Service

- Go to the **ACCESS CONTROL > Authentication Policies** page.
- In the **Authentication Policies** section, click on **Edit Authentication** next to the service to which you want to enable authentication.
- In the **Edit Authentication Policies** window, configure the following:
 - Set Status to **On**.
 - Select the AzureAD authentication service created from the **Authentication Service** drop-down list.
 - Verify the Redirect URL.
- The login page is selected by default in the **Access Control Pages** section.
- Click **Save**.

Step 5 - Configure the Authorization Policy for the Service

- Go to the **ACCESS CONTROL > Authentication Policies** page.
- In the **Authentication Policies** section, click on **Add Authorization** next to the service to which you want to enable authorization.
- In the **Add Authorization Policy** section, configure the following:
 - Policy Name** - Enter a name for the policy.
 - Set Status to **On**.
 - URL Match** - Enter the URL that needs to be matched in the request. For example `/*`
 - Host Match** - Enter the host name to be matched against the host in the request. For

example, *openid.selahcloud.in*



Add Authorization Policy		Help
Service	Oauthinstantsl	
Policy Name	<input type="text" value="test"/> <small>The name of the authorization policy. Must not include spaces.</small>	
Status	<input checked="" type="radio"/> On <input type="radio"/> Off <small>Enable or disable the authorization policy for this service.</small>	
URL Match	<input type="text" value="*"/> <small>The matching criterion for URL field in the Request. This should start with a "*" and can have a maximum of one "*", which is treated as a wildcard.</small>	
Host Match	<input type="text" value="*"/> <small>Enter a host name to be matched against the host in the request. This can be either a specific host match or a wildcard host match with a single "*" anywhere in the URL. Examples: * *.example.com www.example.com</small>	
Extended Match	<input type="text" value="*"/> <small>Define an expression that consists of a combination of HTTP headers and/or query string parameters. This expression is used to match against special attributes in the HTTP headers or query string parameters in the requests.</small>	
Extended Match Sequence	<input type="text" value="1000"/> <small>Specifies an order for matching the extended match rule.</small>	
Login Method	<input checked="" type="radio"/> HTML Form <input type="radio"/> HTTP Basic Authentication <small>Select the login method to be used to authenticate the user.</small>	
Use Persistent Cookie	<input type="radio"/> Yes <input checked="" type="radio"/> No <small>Use Persistent Cookie instead of Session Cookie</small>	
Persistent Cookie Timeout	<input type="text" value="15"/> <small>Persistent Cookie Timeout interval in minutes.</small>	
Comments	<input type="text"/>	

4. Click **Save**.

Step 5 - Verify by Logging into the Microsoft Application.

Figures

1. AzureAD1.png
2. image2020-5-26 15:27:59.png
3. AzureAD2.png

© Barracuda Networks Inc., 2020 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.