

Configuring Google for OpenID Connect on the Barracuda Web Application Firewall

<https://campus.barracuda.com/doc/92767333/>

The Barracuda Web Application Firewall can authenticate users configured on Google using OpenID Connect. Google is the OpenID provider and the Barracuda Web Application Firewall is the service provider to authenticate users. The authentication should be done before you are allowed to access the application protected by the service on the WAF.

Perform the following steps to configure Google 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 Metadata URL for Google OpenID Connect Provider

- Ensure that you have an active account created on Google.
- Make a note of the *client ID* and *Client Secret* strings that are displayed on your screen when configuring Google.
- Use the discovery URL - <https://accounts.google.com/.well-known/openid-configuration>

Step 3 - Configuring the Google OpenID Connect Provider on the Barracuda Web Application Firewall

1. Navigate to **ACCESS CONTROL > Authentication Services** and click the **OpenID Connect** tab.
2. In the **Realm Name** box, specify a name to identify the OpenID Connect.
3. In the **Open ID Connect Alias** box, specify the OpenID Connect alias name to identify the OpenID Connect provider on the Barracuda Web Application Firewall. Example: GoogleOIDC.
4. Choose **Discovery URL** to fill the end point URLs from metadata URL automatically.
5. Specify the metadata URL of the Google OpenID Connect.
Example: <https://accounts.google.com/.well-known/openid-configuration>
6. Click **Retrieve** to display the end point URLs in the fields by default (except for client/clientsec).
7. Configure the client ID and client secret that you noted down while performing the Google configuration. Also, ensure that the Scope field has the OpenID displayed.
8. Click **Add**. The Google OpenID Connect authentication service is displayed in the **Existing Authentication Service** section.

Step 4 - Configure the Authentication Policy for the Service

1. Go to the **ACCESS CONTROL > Authentication Policies** page.

2. In the **Authentication Policies** section, for the service to which you want to enable authentication, click the drop-down list and select **Edit Authentication** from the **Options** column.
3. In the **Edit Authentication Policies** window, configure the following:
 1. Set Status to **On**.
 2. From the **Authentication Service** drop-down list, select the authentication service realm.
 3. Enter the redirect URL. Ensure that you use the same redirect URL that was configured on the Google server. For example, if the redirect URL configured on the Google server is *https://www.oauthtest.com/redirect.html*, then you can use */redirect.html* here.
4. The login page is selected by default in the **Access Control Pages** section.
5. In the **OpenID Connect Claim Configuration** section, specify the claim name and local ID received from the identity provider that needs to be sent to the application server. However, this is an optional step.
6. Click **Save**.

Step 5 - Configure the Authorization Policy for the Service

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

© 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.