
Configuring a Gluu Server for OpenID Connect on the Barracuda Web Application Firewall

<https://campus.barracuda.com/doc/92767456/>

The Barracuda Web Application Firewall can authenticate users configured on a Gluu server using OpenID Connect.

Perform the following steps to configure a Gluu Server 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 Gluu Server's Client ID and Client Secret

1. Log into the Gluu Server Administrator Console and provide administrator username and password.
2. In the left pane, select **Add Realm** and specify the name of the realm. Example: *Test*.
3. Select the realm that you added.
4. Click **Clients > Create** to create a client. Example, *adc-user*. The client is displayed in the client ID column.
5. Select the client that you created and configure Redirect URI for the client in the Valid Redirect URI box.
6. Save the configuration.

Step 3 - Configure the Gluu OpenID Connect Provider on the Barracuda Web Application Firewall

1. Go to the **ACCESS CONTROL > Authentication Policies** page.
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: Gluu*
4. Choose **Discovery URL** to automatically fill the end point URLs from metadata URL.
5. Specify the metadata URL of the Gluu server OpenID Connect. Example, *https://<Gluu OpenID server IP>/well-known/openid-configuration*
6. Click **Retrieve** to display the end point URLs by default (except for client/clientsec).

7. Configure the client ID and client secret that you had noted down while performing the Gluu server configuration. Also, ensure that the Scope field has the OpenID displayed.
8. Click **Add**. The Gluu 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:
 - Set Status to **On**.
 - From the **Authentication Service** drop-down list, select the authentication service realm.
 - Enter the redirect URL. Ensure that you use the same redirect URL that was configured on the Gluu Server. For example, if the redirect URL configured on Gluu server is <https://www.oauthtest.com/redirect.html>, you can use `/redirect.html` here.
4. The login page is selected by default in the **Access Control Pages** section.
5. (Optional) 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.
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:
 - **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.
4. Click **Save**.

© Barracuda Networks Inc., 2022 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.