# Configuring Single Sign-On Using SAML Authentication

https://campus.barracuda.com/doc/46896088/

Single sign-on (SSO) is a mechanism where a single set of user credentials is used for authentication and authorization to access multiple applications across different web servers and platforms, without having to re-authenticate. For more information, see How to Configure Single Sign-On.

**Case 1**

SSO between two applications with different virtual IP (VIP) addresses configured on the same Barracuda Web Application Firewall.

1. Create two HTTPS services on the **BASIC > Services** page by following the steps mentioned in Step 2 in the Configuring SAML on the Barracuda Web Application Firewall article. As an example, consider **App1** and **App2** are the two HTTPS services created on the Barracuda Web Application Firewall.
2. Add a SAML IdP authentication service on the **ACCESS CONTROL > Authentication Services** page by following the steps mentioned in Step 3 in the Configuring SAML on the Barracuda Web Application Firewall article. You can add multiple identity providers to a SAML IdP authentication service (if required). See "Configuring Multiple Identity Providers" in the Advanced Configuration for SAML Authentication article..
3. Configure the authentication policy for both the services (**App1** and **App2**) by following the steps below:
    1. Go to the **ACCESS CONTROL > Authentication Policies** page, **Authentication Policies** section.
    2. Click **Edit Authentication** next to **App1** (HTTPS service created in Step 1).
        1. On the **Edit Authentication Policies** page, do the following configuration:
            - **Status** – Set to *On*.
            - **Authentication Service** - Select the SAML IdP authentication service created in Step 2.

              It is recommended that both the services in the SSO setup have the same SAML IdP authentication service. However, you can associate different SAML IdP authentication services with the applications if the SAML IdP authentication services have the same server configuration in it.
            - Specify values for the parameters under **SAML Service Provider Configuration**, and click **Save**. See Step 4 in the Configuring SAML on the Barracuda Web Application Firewall article.
    3. Repeat Step 3 for **App2** (HTTPS service created in Step 1).
    4. Configure the authorization policy for both the services (App1 and App2) by following the steps mentioned in Step 5 in the Configuring SAML on the Barracuda Web Application Firewall article.

## How the SSO Setup Works

1. Open your web browser and access the protected resource of the first service.
2. If the SAML IdP authentication service associated with the service is configured with only one IdP server detail, the Barracuda Web Application Firewall redirects the user to the configured identity provider and challenges the user to provide login credentials.
3. If multiple identity providers are configured, the Barracuda Web Application Firewall displays an identity provider selection page where the user can select the identity provider for authentication.
4. After successful authentication, the user is allowed to access the requested URL.
5. Access the protected resource of the second application.
6. If the SAML IdP authentication service associated with the service is configured with only one IdP server details, then the user is allowed to access the requested URL without being challenged to provide login credentials.
7. Both the services are now in an SSO environment.
8. If multiple identity providers are configured, the Barracuda Web Application Firewall displays an identity provider selection page where the user can select the identity provider for authentication. In this case:
    1. If the user selects the same identity provider that was selected for first service, the user is allowed to access the requested URL without being challenged to provide login credentials.
    2. If the user selects a different identity provider for authentication, the user is allowed to access the requested URL upon successful authentication, but the service remains independent and not in an SSO environment.

**Case 2**

SSO between two applications that are configured on different Barracuda Web Application Firewalls with different virtual IP (VIP) addresses.

1. On the Barracuda Web Application Firewall 1, complete the following configuration:
    1. Create an HTTPS service on the **BASIC > Services** page by following the steps mentioned in Step 2 in the Configuring SAML on the Barracuda Web Application Firewall article.
    2. Add a SAML IdP authentication service on the **ACCESS CONTROL > Authentication Services** page by following the steps mentioned in Step 3 in the Configuring SAML on the Barracuda Web Application Firewall page. You can add multiple Identity Providers to a SAML IdP authentication service (if required). See "Configuring Multiple Identity Providers" in the Advanced Configuration for SAML Authentication article.
    3. Configure an authentication and authorization policy for the service created in Step 1 by following the steps mentioned in Steps 4 and 5 in the Configuring SAML on the Barracuda Web Application Firewall article.
2. On the Barracuda Web Application Firewall 2, repeat Step 1a., 1b., and 1c.

Ensure that you add a SAML IdP authentication service with the same server configuration as that of the Barracuda Web Application Firewall 1.