How to Set Up Microsoft Entra ID Integration for the Barracuda Web Application Firewall Management Access

https://campus.barracuda.com/doc/95263386/

Microsoft Entra ID Integration

Perform the following steps to set up Microsoft Entra ID integration for the Barracuda Web Application Firewall Management Access:

Step 1. Service Provider (SP) Configuration on the Barracuda Web Application Firewall

1. Log into the Barracuda Web Application Firewall web interface and go to **ADVANCED > Admin Access Control**.
2. Scroll down to the **Single Sign-On** section, and click **SAML Service Provider Information** to expand the section.
3. In the **SAML Service Provider Information** section, specify values for the following:
    1. **Realm Name** - Enter a name for the SAML Service Provider.
    2. **Organization Name** - Enter the name of the service provider organization that is used in the SAML metadata.
    3. **Organization URL** - Enter the URL of the service provider organization. The URL should be a Fully Qualified Domain Name (FQDN).
    Example: *http://domain/url* or *https://domain/url* .
    4. **Organization Display Name** - Enter the name of the service provider that is displayed to the users who are accessing this service.
    5. **SP Entity ID** - Enter a unique ID for Service Provider Entity.
    6. **Host Name** - Enter the hostname that can be used to access the Barracuda Web Application Firewall web interface.
    7. **Privacy Policy**
        1. **Signing Certificate** - The certificate that needs to be used by the service provider for signing the messages to the Identity Provider. Click the drop-down list and select Generate Certificate to create a new certificate or select Upload Certificate to upload a signed certificate. If you have already created or uploaded the certificate, select the certificate from the drop-down list.
        2. **Digest Algorithm** - The digest algorithm used for generating signature. This will further be used for signing SAML Authentication Request.

8. **Advanced Settings**:
    1. **Logout Processor Path** - The URL handled by the Barracuda WAF for performing Logout. *Example:* Saml.sso/SLO/Redirect.
    2. **Post Processor Path** - The URL that is handled by the Barracuda WAF for SAML POST operations. *Example*: Saml.sso/SAML2/POST.
9. Click **Save** to save the configuration.
10. Click **Generate** to download the Service Provider metadata.

Step 2. Identity Provider (IdP) Configuration on Azure

1. Log into the Azure portal.
2. Go to **Microsoft Entra ID > Enterprise Application**.
3. On the **Enterprise Applications | All Applications** page, click **New application** and then click **Create your own application**.
4. Enter a name for the application and click **Create**.
5. After the application is created, click **Single Sign-On** under **Manage**.
6. On the **Single Sign-On** page, select **SAML** as the Single Sign-On method.
7. On the **SAML-based Sign-On** page, click **Edit** next to **Basic SAML Configuration** under **Set up Single Sign-On with SAML**.
8. Click **Upload Metadata File**, and choose the file downloaded in the **Service Provider (SP) Configuration on the Barracuda Web Application Firewall** section. The **Basic SAML Configuration** page opens.
9. On the **Basic SAML Configuration** page, add the **Reply URL** (Assertion Consumer ServiceURL) by copying the 'AssertionConsumerService' from the SP metadata. Other data automatically gets updated from the SP metadata file upload. Click **Save**.
10. On the **Basic SAML Configuration** page, add the SP Entity ID, SP Assertion Consumer Service URL, and SP logout endpoint, and click **Save**.
    Entity ID can be a string or a URL.
    Before you add the Assertion Consumer Service URL, you must know the hostname to access the Barracuda Web Application Firewall.
11. On the **SAML-based Sign-On** page, copy the **App Federation Metadata URL** in the **SAML Signing Certificate** section under **Set up Single Sign-On with SAML**.

Step 3. Identity Provider (IdP) Configuration on the Barracuda Web Application Firewall

1. Log into the Barracuda Web Application Firewall web interface and go to **ADVANCED > Admin Access Control**.
2. Io the **Single Sign-On** section, click **Add SAML Identity Provider**.
3. In the **SAML SSO Identity Provider Configuration** section, specify values for the following:
    - **Identity Provider Name** – Enter the name of the identity provider.
    - **Identity Provider Metadata Type** - Choose **URL** as the Identity Provider Metadata

Type.
- **Metadata URL** – Enter the App Federation Metadata URL that you copied in **Step 11** in the **Identity Provider (IdP) Configuration on Azure** section.

4. In the **SAML Claims/Attributes Mapping** section, specify values for the following:
   - **Claim/Attribute Name** – Enter the attribute name used for mapping.
   - **Local ID** - Enter the name, email and groups shared by IdP.

     The Barracuda Web Application Firewall web interface (UI) access needs three (3) attributes from IDP in the Assertion. The following attributes MUST be provided by the IDP:
     -- User name
     -- Email address
     -- Groups info.
     Following are the example attribute names from the Microsoft Entra ID IDP:

     http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
     http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
     http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
5. In the **Role Association** section, specify values for the following:
   1. **Default Role** - Select a role from the drop-down list for the user. You can assign the role to individual users and/or users of a group that are not associated with any specific user role. When set to **None**, users are not allowed to access the system. By default, the Default Role is set to **None**.
   2. **Group Mapping** - Set to **Yes** to view the group mapping configuration. The group names can be specified in **Associated IdP Groups** next to the desired role. The users of the group specified in **Associated IdP Groups** are associated with the role next to which they are configured, and can perform the operations that are granted to the role. For example, consider a group is associated with the Audit-Manager role. The users of that group are allowed to view logs on the system and are prevented from accessing any other objects.

      Multiple groups can be mapped to a single role by specifying the group names separated with a comma (,).
      -- If a user belongs to multiple groups and those groups are mapped to different roles, then based on the Priority the user will assume the Role.
      -- If a user does not belong to any **Group**, **Default Role** is assigned to the user.
      -- If the **Default Role** is set to **None**, access to the Barracuda Web Application Firewall web interface is denied to the user.
6. Click **Save**.