How to Set Up ADFS IdP Integration for the Barracuda Web Application Firewall Management Access

https://campus.barracuda.com/doc/95263391/

Perform the following steps to set up ADFS IdP 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 the 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 later be used for signing the 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 ADFS

1. Open the **ADFS Management** on your system.
2. On the **AD FS** window, right-click on **Relying Party Trust** and select **Add**.
3. On the **Add Relying Party Trust Wizard**:
    1. Ensure that the **Claims aware** is selected and click **Next**.
    2. Click **Select Data Source** under **Steps** and select the **Import data about the relying party from a file** radio button.
    3. Click **Browse**. **Locate** and select the metadata file. Click **Next**.
    4. Specify a name in the **Display Name** text field.
    5. Choose **Access Control Policy** window, and select **Permit Everyone**
    6. In the **Ready to Add Trust** window, check if the signature and endpoints are properly imported from the metadata.
    7. Click **Next** and click **Finish**
4. On the **Relying Party Trusts** window, select the relying trust rule added in Step **3** and click **Edit Claim Issuance Policy** in the **Actions** panel.
5. On the **Edit Claim Issuance Policy** window, click **Add Rule**.
    1. Under **Select Rule Template**, select **Send LDAP Attributes as Claims** from the **Claim rule template** drop-down list and click **Next**.
    2. Under **Configure Rule**:
        1. Enter a name in the **Claim rule name** text box.
        2. Select **Active Directory** from the **Attribute Store** drop-down list, add LDAP attributes and the Outgoing Claim Type for those attributes. The Barracuda Web Application Firewall requires the following attributes:
            1. User name or UPN
            2. Email Address
            3. Groups
    3. Click **Finish**.
6. Click on the rule again and select **Edit Claim Issuance Policy**.
7. On the **Edit Claim Issuance Policy** window, click **Add Rule**.
    1. Under S**elect Rule Template**, select **Transform an Incoming Claim** from the **Claim rule template** drop-down list and click **Next**.
    2. Under **Configure Rule**:
        1. Enter a name in the **Claim rule name** text box.
        2. Configure the rule by selecting the **Incoming claim type** as **Email address**, **Outgoing claim type** as **NameID** and **Outgoing name ID format** as **unspecified**.
        3. Click **OK** and click **Apply** on the **Issuance Transform Rules** window.
8. On the **AD FS Management** window, expand the **AD FS** folder, click **Service** and select **Endpoints**.

9. Under **Endpoints**, copy the Metadata URL and use the URL or download the Metadata and save it in a file.

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. In 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 Metadata URL that you copied in Step 9 in the **Identity Provider (IdP) Configuration on ADFS** 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 attributes are as follows:
   -- Username
   -- Email address
   -- Group
   Following are the example attribute names from ADFS IDP:
   http://schemas.xmlsoap.org/claims/UPN
   http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
   http://schemas.xmlsoap.org/claims/Group
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**.