Configuring Identity Provider (IdP) for SAML Authentication

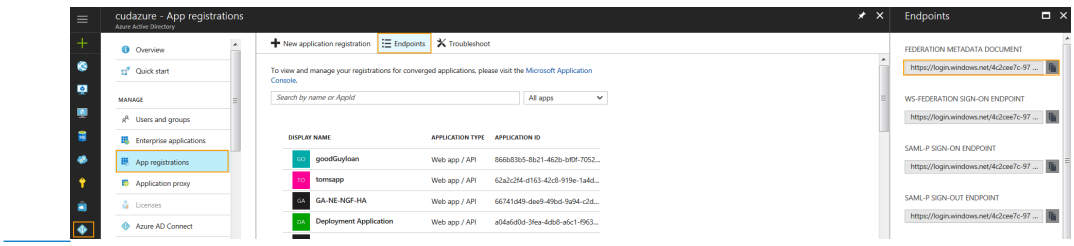
https://campus.barracuda.com/doc/45024465/

An IdP is a service/website that certifies user identities using security tokens. The Identity Provider may be an on premises Active Directory Federation Services (AD FS) setup, or an Active Directory (AD) located in Azure cloud.

Configuring Azure Active Directory (AD) for SAML Authentication in the New Microsoft Azure Portal

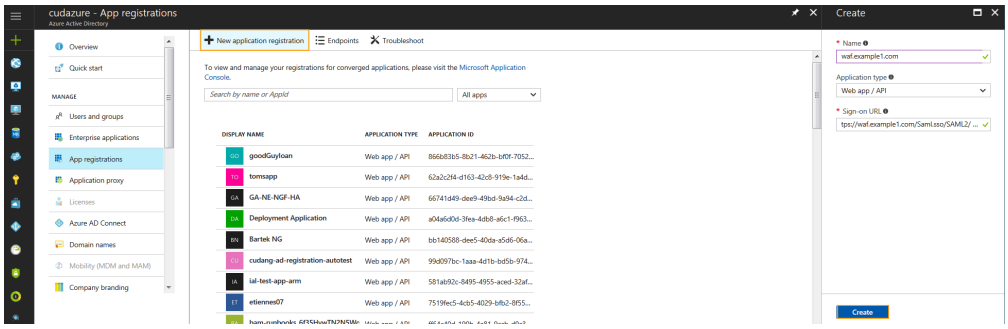
Azure Active Directory (AD) is the Identity Provider responsible for authenticating users accessing web applications hosted on the Microsoft Azure cloud. Azure AD manages user identities along with applications. You should configure the SAML endpoints in Azure AD for web applications requiring protection from the Barracuda Web Application Firewall. Perform the following steps to configure Azure AD:

1. Log into the Microsoft Azure Portal.
2. In the left pane, select **Azure Active Directory** and then **App registrations** under **MANAGE**.
3. In the **App registrations** page, click **Endpoints**.
4. In the **Endpoints** page, copy the **FEDERATION METADATA DOCUMENT** link. This is the **Identity Provider Metadata URL** to be configured on the Barracuda Web Application Firewall in the **ACCESS CONTROL > Authentication Services** page, **New Authentication Service** section > **SAML Identity Provider**. Example: https://login.windows.net/4c2cee7c-97ca-4f42-88ea-6acf44978369/federationmetadata/2007-06/federationmetadata.xml

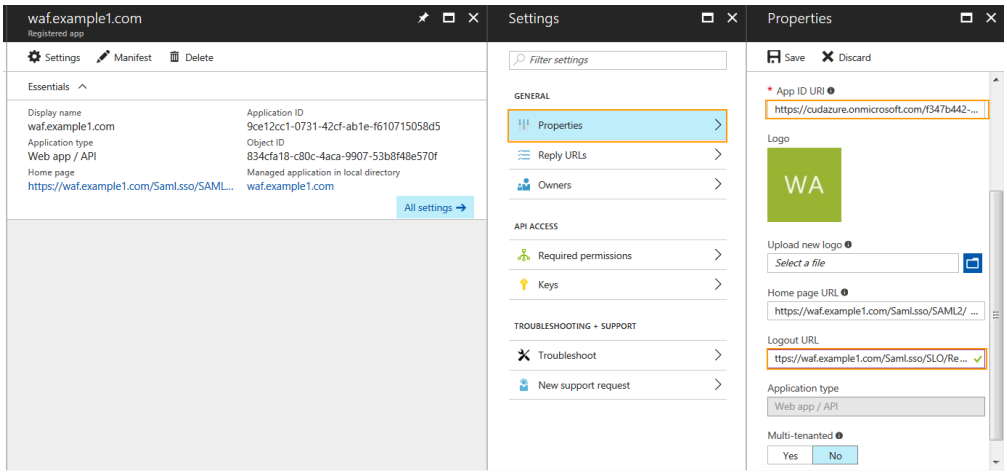


5. Now, go back to the **App registration** page and click **New application registration**.
6. In the **Create** page, do the following:
   1. **Name**: Enter a name for the application. **Example**: waf.example1.com

2. **Application type**: Keep the default option i.e. Web app/API
3. **Sign-on URL**: Enter https://waf.example1.com/Saml.sso/SAML2/POST.
4. Click **Create**.



7. In the **App registrations** page, locate the application you created in step **6** and click on the application.
8. In the application's **Settings** page, click **Properties** under **GENERAL**.
9. In the **Properties** page, do the following:
    1. **App ID URI**: Enter https://waf.example.com/saml.sso or keep the default value. Note: If the **App ID URI** is left with the default value, ensure the same is configured as **SP Entity ID** on the Barracuda Web Application Firewall in the **ACCESS CONTROL > Authentication Policies** page, **Authentication Policies** section. Click **Edit Authentication** next to the service and enter **SP Entity ID** under **SAML SP Configuration**.
    2. **Logout URL**: Enter https://waf.example.com/Saml.sso/SLO/Redirect.
    3. Click **Save**.



Configuring Azure Active Directory (AD) for SAML Authentication in the Classic Microsoft Azure Portal

1. Log into the Azure Management Portal.

2. In the left pane, select **ACTIVE DIRECTORY**.
3. Select an Active Directory from the **active directory** list, and click **APPLICATIONS**.
4. Click **ADD**.
5. In the pop-up window, click **Add an application my Organization is developing**.
6. In the **Tell us about your application** window, enter a **Name** for the application. **Example**: waf.example.com
7. Keep the default option, **WEB APPLICATION AND/OR WEB API**, and click **Next** to continue.
8. In the **App properties** window, do the following:
    1. **SIGN-ON URL** – Enter https://waf.example.com/Saml.sso/SAML2/POST as sign-on URL.
    2. **APP ID URI** – Enter https://waf.example.com/saml.sso as app Id URI, and click the tick mark to complete.
9. After the application is added, click **CONFIGURE.** Scroll down to the **single sign-on** section; verify that **App ID URI** is the same as in step **8.b** i.e. https://waf.example.com/saml.sso.

    This is the unique **Service Provider (SP) EntityID** to be configured on the Barracuda Web Application Firewall.
10. Click **VIEW ENDPOINTS** at the bottom of the screen. The **App Endpoints** window displays the list of endpoints. Note that the **Federation Metadata Document** URL is the Metadata URL for this application. **Example**: https://login.windows.net/fed64a10-d698-4693-9ad4-/federationmetadata/2007-06/federationmetadata.xml.

    Use the same Metadata URL while configuring **IDP Metadata** on the Barracuda Web Application Firewall. IDP Metadata can be configured on the **ACCESS CONTROL > Authentication Services** page.
11. Copy the **Federation Metadata Document** URL and open it in a new browser.

    The **Federation Metadata Document** URL is an XML file that contains the Metadata details. If the Barracuda Web Application Firewall can be reached via internet, you can use the same URL and configure it on the Barracuda Web Application Firewall. If not, you can download this XML file and upload it in the **SAML IDP** tab on the **ACCESS CONTROL > Authentication Services** page.
12. In the XML file, note the following:
    1. **entityID** - This is the IDP Entity ID that needs to be configured on the Barracuda Web Application Firewall. Example: “entityID=https://sts.windows.net/fed64a10-d698-4693-95b4-61f4ddd86b64/”
13. Close the **VIEW ENDPOINTS** page by clicking the tick mark.
14. Click **MANAGE MANIFEST** at the bottom of the screen, and select **Download Manifest**.
15. In the **Download Manifest** window, click **Download manifest** and save the file to your local machine.
    1. Open the file in a notepad from the saved location and search for “**logoutUrl**”.
    2. Configure the logoutUrl as: "logoutUrl": "https://waf.example.com/Saml.sso/SLO/Redirect",
    3. Save the file.
16. Click **MANAGE MANIFEST** at the bottom of the screen, and select **Upload Manifest**.
17. In the **Upload Manifest** window, browse and upload the file you saved in step **15.c**.

Configuring Active Directory Federation Services (AD FS) 2.0 for SAML

Authentication

Active Directory Federation Services (AD FS) is the Identity Provider responsible for authenticating users accessing the web applications hosted on the Microsoft Windows server. Perform the following steps to configure AD FS 2.0:

1. Download the IdP Metadata from the AD FS server.
2. Use the IdP metadata information and create a SAML IDP authentication service on the **ACCESS CONTROL > Authentication Services** page.
3. Continue with steps **3** to **6** under Configuring SAML on the Barracuda Web Application Firewall in the SAML Authentication article.
4. Go to the **ACCESS CONTROL > Authentication Policies** page, and generate the Service Provider (SP) Metadata file by following the steps in **Step 6 - Generate Service Provider (SP) Metadata** in the Configuring SAML on the Barracuda Web Application Firewall article.
5. Save the Metadata file to the location you desire on the AD FS server.
6. Log into the AD FS server, and do the following:
    1. Click the **Start** menu and select **AD FS 2.0 Management**.
    2. On the AD FS 2.0 window, expand the **Trust Relationships** folder under the **AD FS 2.0** root directory by clicking the plus button.
    3. Right click on **Relying Party Trusts** and select **Add Relying Party Trust**. The **Add Relying Party Trust Wizard** appears.
    4. In the **Add Relying Trust Wizard** window, click **Start**.
    5. In the **Select Data Source** step:
        1. Select **Import data about the relying party published from a file**.
        2. Click **Browse** and select the SP Metadata file saved in step **5**.
        3. Click **Next**.
        4. The message "**Some of the content in the federation metadata was skipped because it is not supported by AD FS 2.0**" may appear. Click **OK**.
    6. In the **Specify Display Name** step:
        1. Enter the service provider domain in **Display Name**. Example: service1.domain.com
        2. Click **Next**.
    7. In the **Choose Issuance Authorization Rules** step, keep the default settings and click **Next**.
    8. Click **Next** in the **Ready to Add Trust** step, and then click **Close**. The **Edit Claim Rules window** appears.
    9. In the **Edit Claim Rules** window, add, edit or remove rules and click **OK**.
    10. The added trust displays in the **Relying Party Trusts** list.

Configuring SAML Attributes on the AD FS 2.0 server

To illustrate how to configure SAML attributes on the AD FS server, the LDAP attributes **User-Principal-Name** and **Token-Groups – Unqualified Names** are used as examples in this section.

Perform the following steps to configure SAML attributes on the AD FS server:

1. Log into the AD FS server.
2. Click the **Start** menu and select **AD FS 2.0 Management**.
3. In the AD FS 2.0 window, expand the **Trust Relationships** folder under the **AD FS 2.0** root directory by clicking the plus button.
4. Click on **Relying Party Trusts** folder. The **Relying Party Trusts** list appears in the right pane.
5. Right click on the relying party application you created, and select **Edit Claim Rules**. For example, service1.domain.com
6. In the **Edit Claim Rules** window, click **Add Rule** in the **Issuance Transform Rules** tab.
7. In the **Add Transform Claim Rule Wizard** window:
    1. Select **Send LDAP Attributes as Claims** in the **Choose Rule Type** step, and click **Next**.
8. In the **Configure Claim Rule** step:
    1. Enter a name in **Claim rule name**.
    2. Select **Active Directory** from the **Attribute store** list.
    3. Under **Mapping of LDAP attributes to outgoing claim types**, create mappings for the attributes that need to be allowed in the SAML IdP response. **Example**:

LDAP Attribute	Outgoing Claim Type
User-Principal-Name	UPN
Token-Groups – Unqualified Names	Group

    4. Click **Finish**.
9. Create transform rules for the attributes added in step **8.c** (i.e. User-Principal-Name and Token-Groups – Unqualified Names).
10. To add a transform rule for the attribute **User-Principal-Name**, repeat step **6** and **7**, and then continue with the steps below.
11. Select **Send Claims Using a Custom Rule** in the **Choose Rule Type** step and click **Next**.
12. In the **Configure Claim Rule** step:
    1. Enter a name in **Claim rule name**. **Example**: Transform UPN to epPN.
    2. Type or copy and paste the following in the **Custom rule** text box:

```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
 => issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.6", Value =
c.Value,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimpro
perties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-
format:uri");
```

    3. Click **Finish**.
14. To add a transform rule for the attribute **Token-Groups – Unqualified Names**, repeat step **6** and **7,** and then continue with the steps below.

15. Select **Send Claims Using a Custom Rule** in the **Choose Rule Type** step and click **Next**.
16. In the **Configure Claim Rule** step:
    1. Enter a name in **Claim rule name**. **Example**: Transform Group to epSA
    2. Type or copy and paste the following in the **Custom rule** text box:

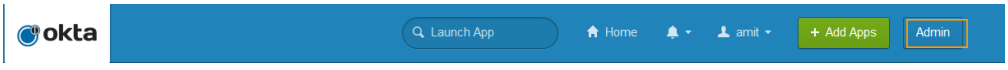
```
c:[Type == "http://schemas.xmlsoap.org/claims/Group", Value ==
"Domain Users"]
 => issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.9", Value =
"member@domain.com ",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimpro
perties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-
format:uri");
```

       The **domain.com** name above should be the domain name of the AD FS Server configured.
    3. Click **Finish**, and then **OK**.
17. The added rules display under the **Issuance Transform Rules** tab.

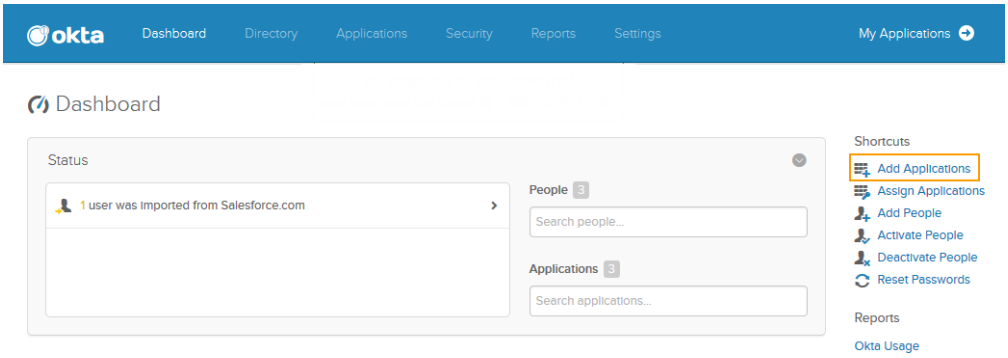
Configuring Okta for SAML Authentication

The Barracuda Web Application Firewall can authenticate users configured on Okta using SAML Single Sign-On. Okta is as an SAML IDP Provider and the Barracuda Web Application Firewall is the Service Provider to authenticate users. Perform the following steps to configure Okta:

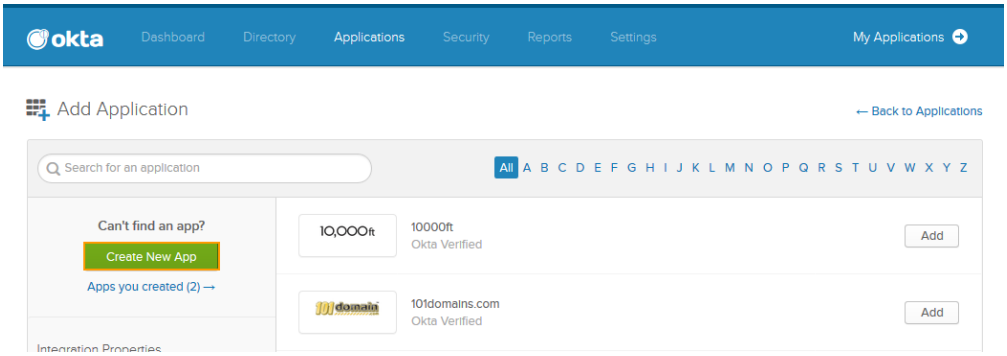
1. Download the IdP Metadata from the Okta.
2. Use the IdP metadata information and create a SAML IDP authentication service on the **ACCESS CONTROL > Authentication Services** page.
3. Continue with steps **3** to **6** under **Configuring SAML on the Barracuda Web Application Firewall** in the SAML Authentication article.
4. Go to the **ACCESS CONTROL > Authentication Policies** page, and generate the Service Provider (SP) Metadata file by following the steps under **Generate Service Provider (SP) Metadata** in the SAML Authentication article.
5. Save the Metadata file to your desktop.
6. Open the Metadata file and note the following:
    1. Entity ID
    2. AssertionConsumerService Location
7. Log into the Okta application, and do the following:
8. Click **Admin** on the Okta home page.



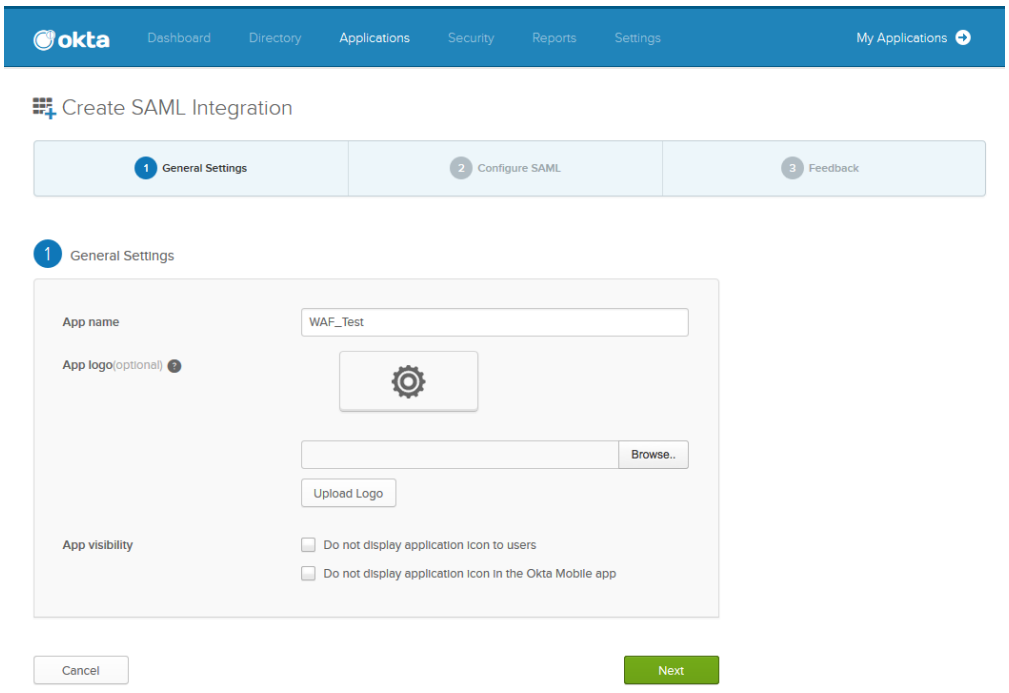
9. On the Okta **Dashboard**, click **Add Applications** under **Shortcuts**.



10. On the **Add Application** page, click **Create New App** and do the following**:**
    1. Select **SAML 2.0** in the **Create a New Application Integration** window and click **Create**.

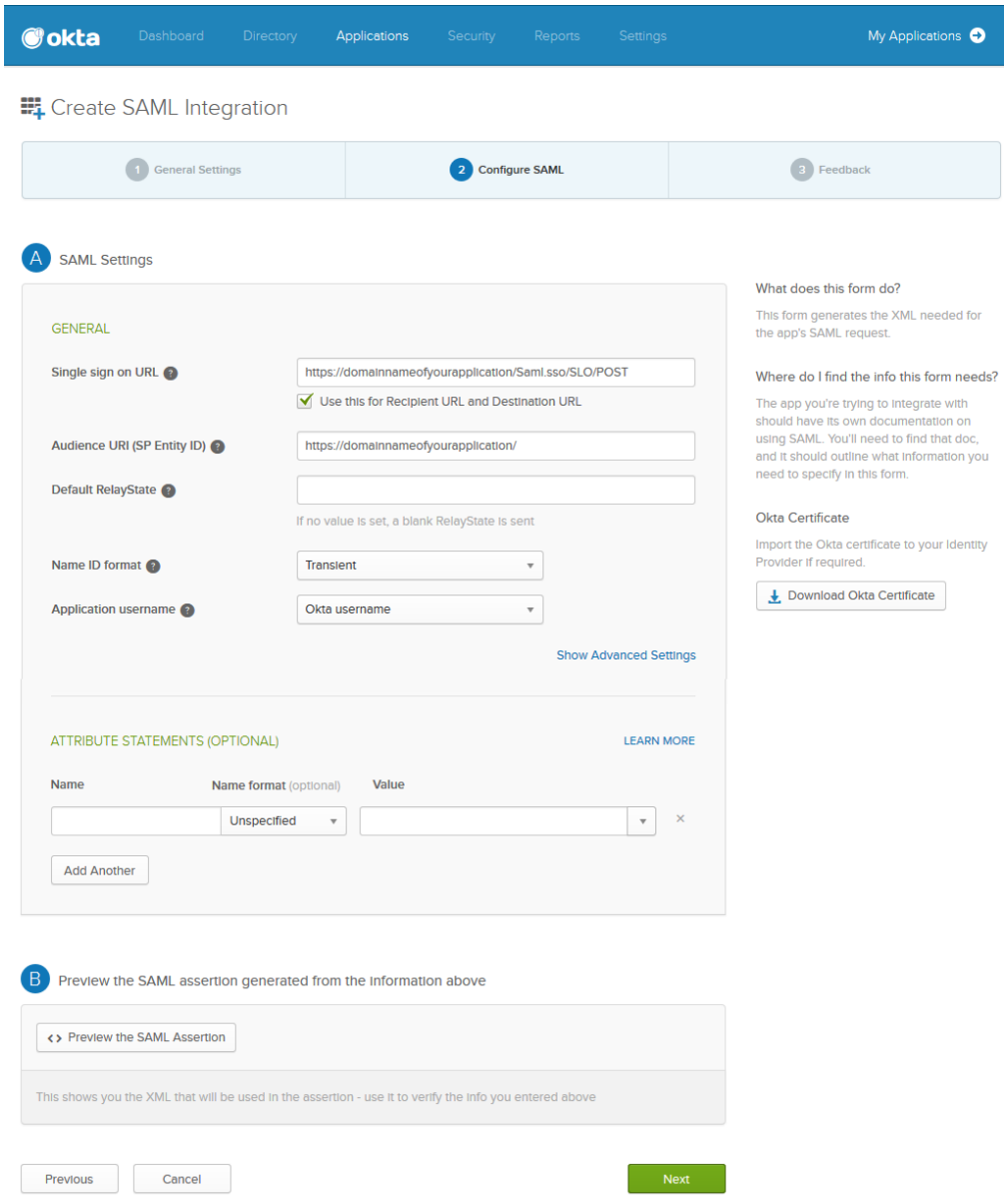


    2. In the **Create SAML Integration** page**:**
    3. Under **General Settings**, enter a name for the application in the **App name** field and click **Next**.

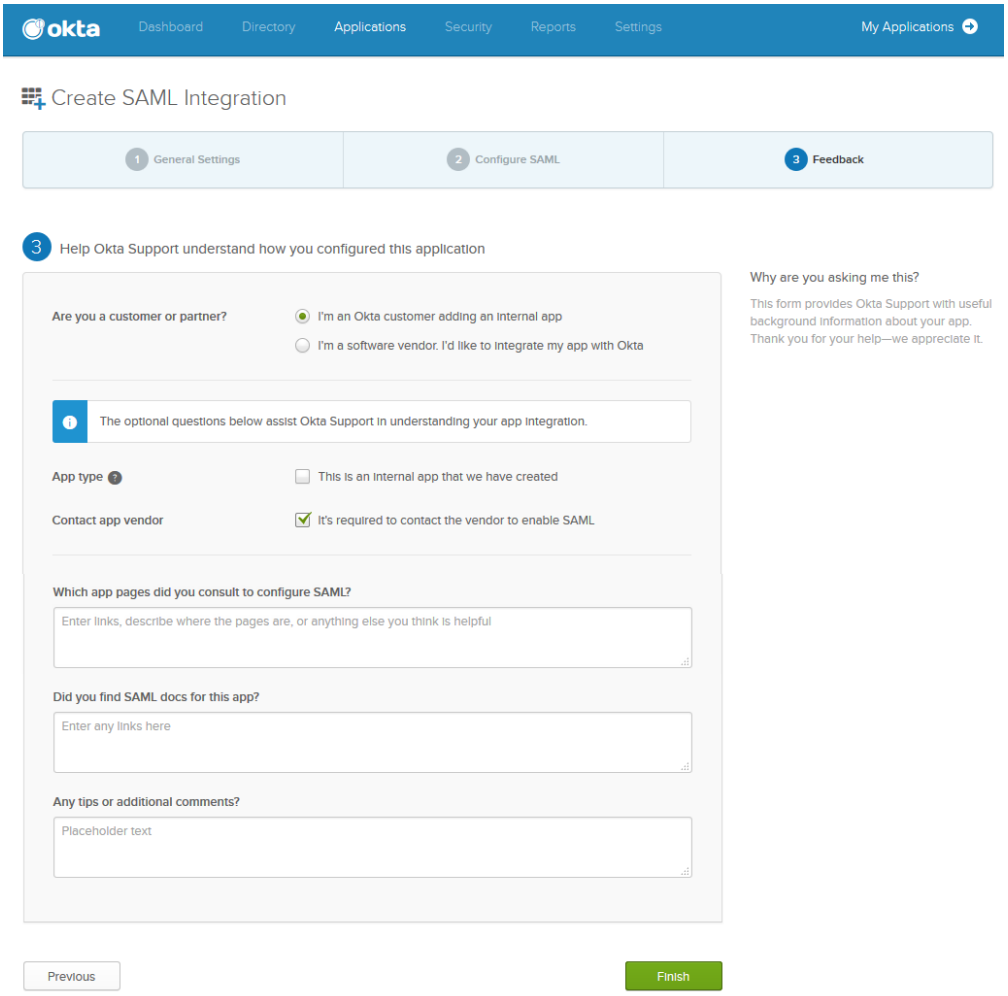


    4. Under **Configure SAML:**

1. Specify the **AssertionConsumerService Location** noted in step **6** in the **Single sign on URL** field. Verify **Use this for Recipient URL and Destination URL** is selected.
2. Specify the **Entity ID** noted in step **6** in the **Audience URI (SP Entity ID).**
3. Select **Transient** as **Name ID format**.
4. Click **Next**.



5. Under **Feedback**:
   1. Select **I'm an Okta customer adding an internal app** next to **Are you a customer or partner?**.
   2. Select **It's required to contact the vendor to enable SAML** next to **Contact app vendor**.



6. Click **Finish**.

Figures

1. Endpoints.png
2. New_App_registration.png
3. Properties.png
4. Admin.png
5. Add Applications.png
6. Create_New_App.png
7. General_Settings.png
8. Configuring_SAML.png
9. Feedback.png