

Configuring Identity Provider (IdP) for SAML Authentication

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

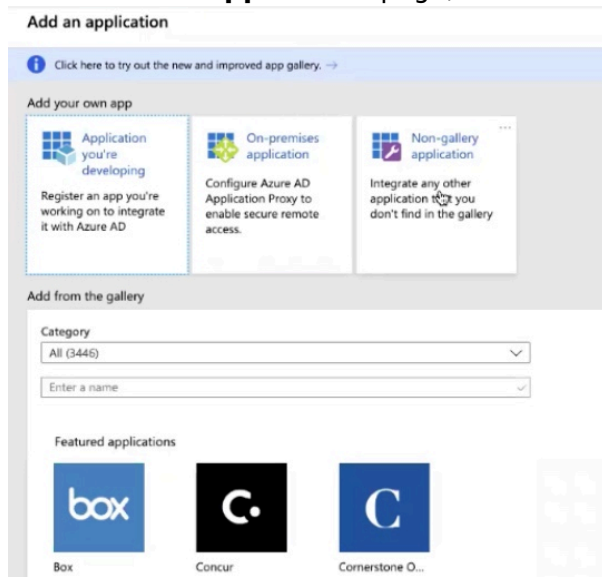
An IdP is a service/website that certifies user identities using security tokens. The identity provider may be an on-premises Active Directory Federation Services (AD FS) setup, or an Active Directory (AD) located in the Azure cloud.

- Configuring Azure AD as IdP:
 - [Configuring Azure AD as IdP in the New Microsoft Azure Portal](#)
- [Configuring AD FS 2.0 as IdP](#)
- [Configuring Okta as IdP](#)
- [Configuring Duo Single Sign-On](#)

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. Select **Azure Active Directory** and then from the left pane select **Enterprise application**.
3. In the **Enterprise applications** page, click + **New application**.
4. In the **Add an application** page, click **Non-gallery application**.

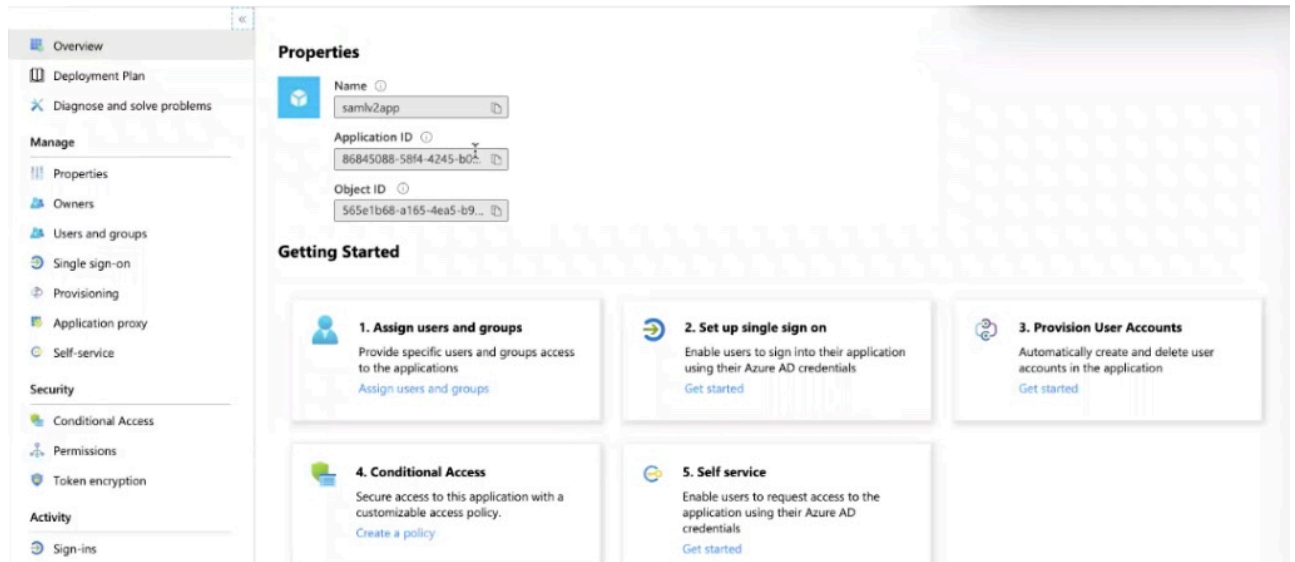


5. In the **Add your own application** page, enter a name for the application and then click **Add**.

For example: samlv2app

The application page is created.

6. In the **Overview** page, click **1. Assign users and groups**.



7. Click **Add users > Users and groups** and from the right pane, select the user who has to be part of the application.
8. Go to the **Overview** page and then click **Set up single sign on**.
9. Select SAML, scroll down, and then copy the **App Federation Metadata Url** link. This is the **Identity Provider Metadata URL** to be configured on the Barracuda Web Application Firewall in the **ACCESS CONTROL > Authentication Services > New Authentication Service > SAML Identity Provider** page. Example: https://login.microsoftonline.com/<AzureADtenantID>/federationmetadata/2007-06/federationmetadata.xml?appid=<app_ID>
10. Use the IdP metadata information and create a SAML IDP authentication service on the **ACCESS CONTROL > Authentication Services** page. Also, verify that the SP Entity ID is the same and then click **Save** to save the metadata file to your desktop.
11. Continue with Steps 3 to 6 under **Configuring SAML on the Barracuda Web Application Firewall** in the [SAML Authentication](#) article.
12. Use the SAML identity provider created in the previous steps and create an authorization policy in the **ACCESS CONTROL > Authentication Policies** page.
13. Click **Generate** to generate an XML file. For more information on how to generate the service provider (SP) metadata file, refer to, **Generate Service Provider (SP) Metadata** in the [SAML Authentication](#) article.
14. Go to the **SAML-based sign on** page, click **Upload metadata file**, select the XML file to upload and then click **Save**.
15. Verify the same in [Microsoft Azure Portal](#) page.

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:

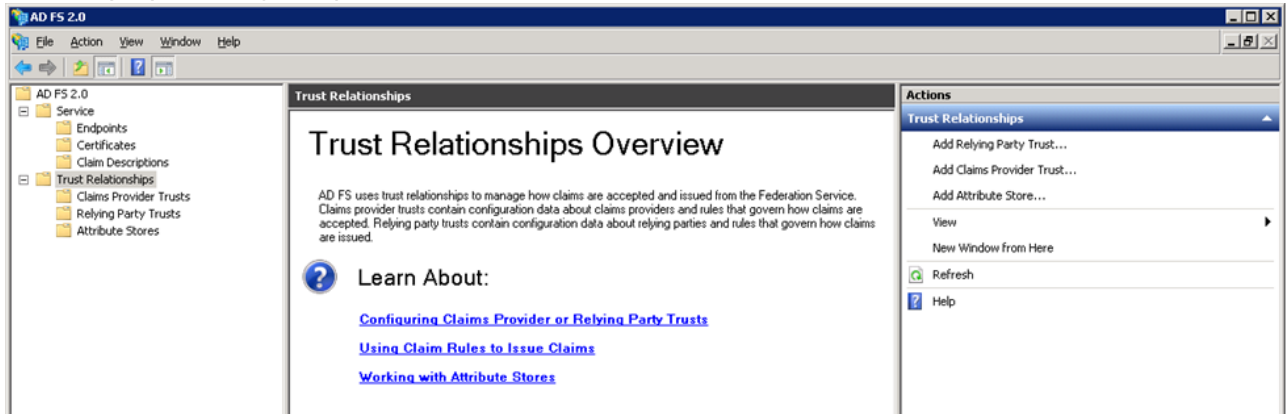
1. Download the IdP metadata from the AD FS server.
2. Use the IdP metadata information and create a SAML IDP authentication service on the **ACCESS CONTROL > Authentication Services** page.
3. Continue with Steps 3 to 6 under [Configuring SAML on the Barracuda Web Application Firewall](#) in the [SAML 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 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 **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

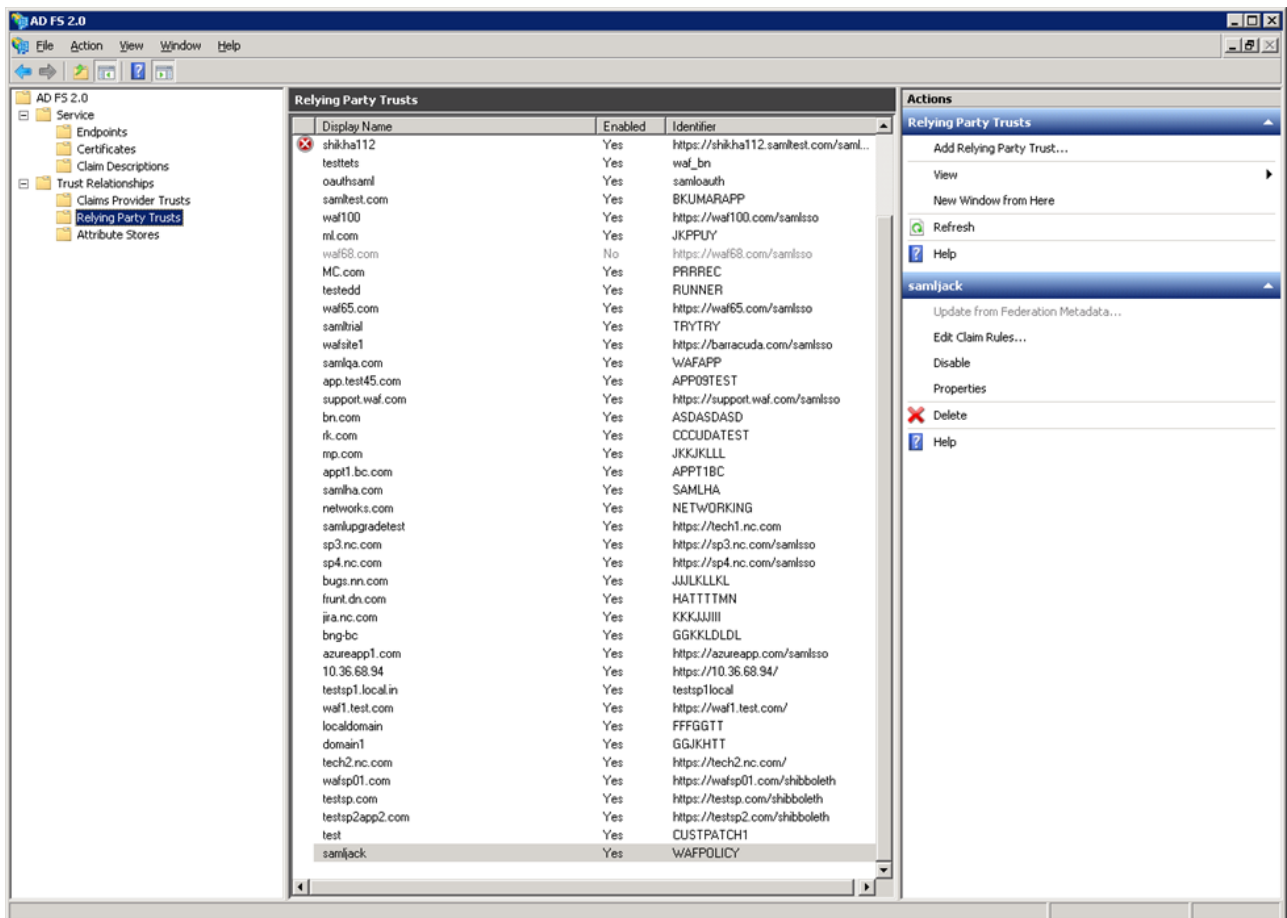
To illustrate how to configure SAML attributes on the AD FS server, the LDAP attributes **User-Principal-Name** and **Token-Groups - Unqualified Names** are used as examples in this section.

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

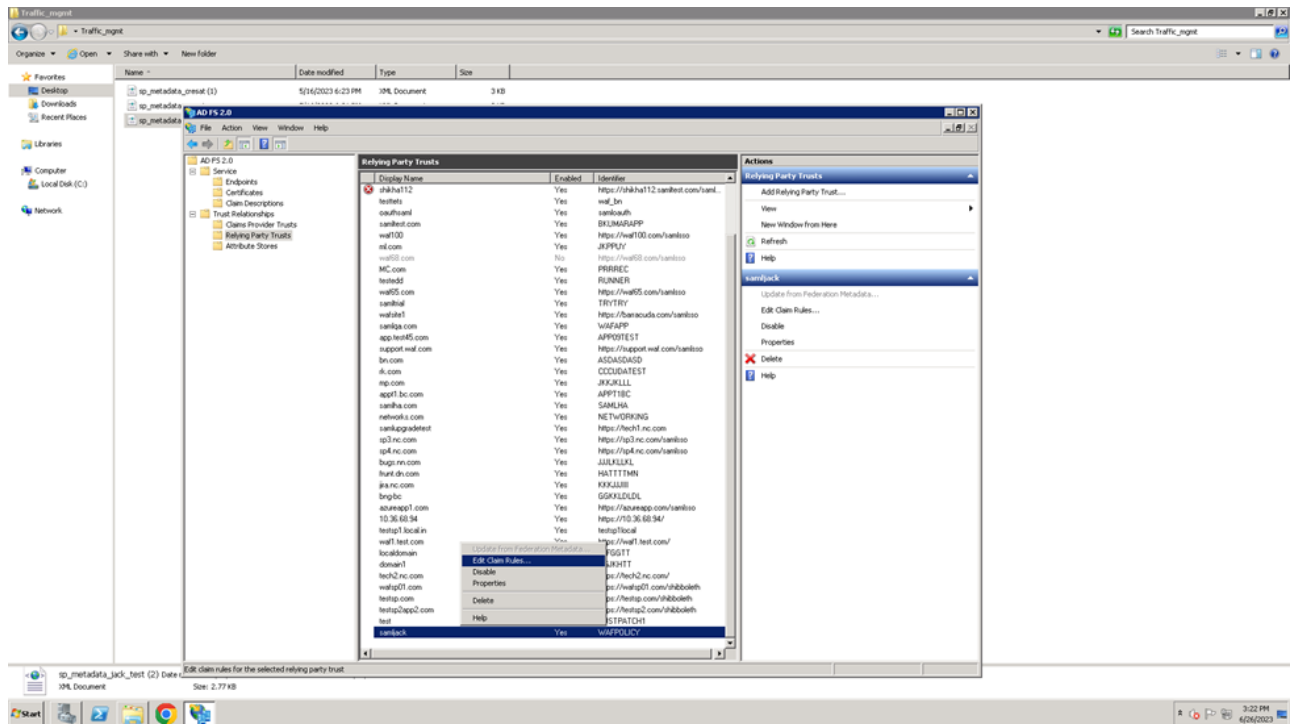
1. Log into the AD FS server.
2. Click the **Start** menu and select **AD FS 2.0 Management**.
3. In the AD FS 2.0 window, expand the **Trust Relationships** folder under the **AD FS 2.0** root directory by clicking the plus (+) button.



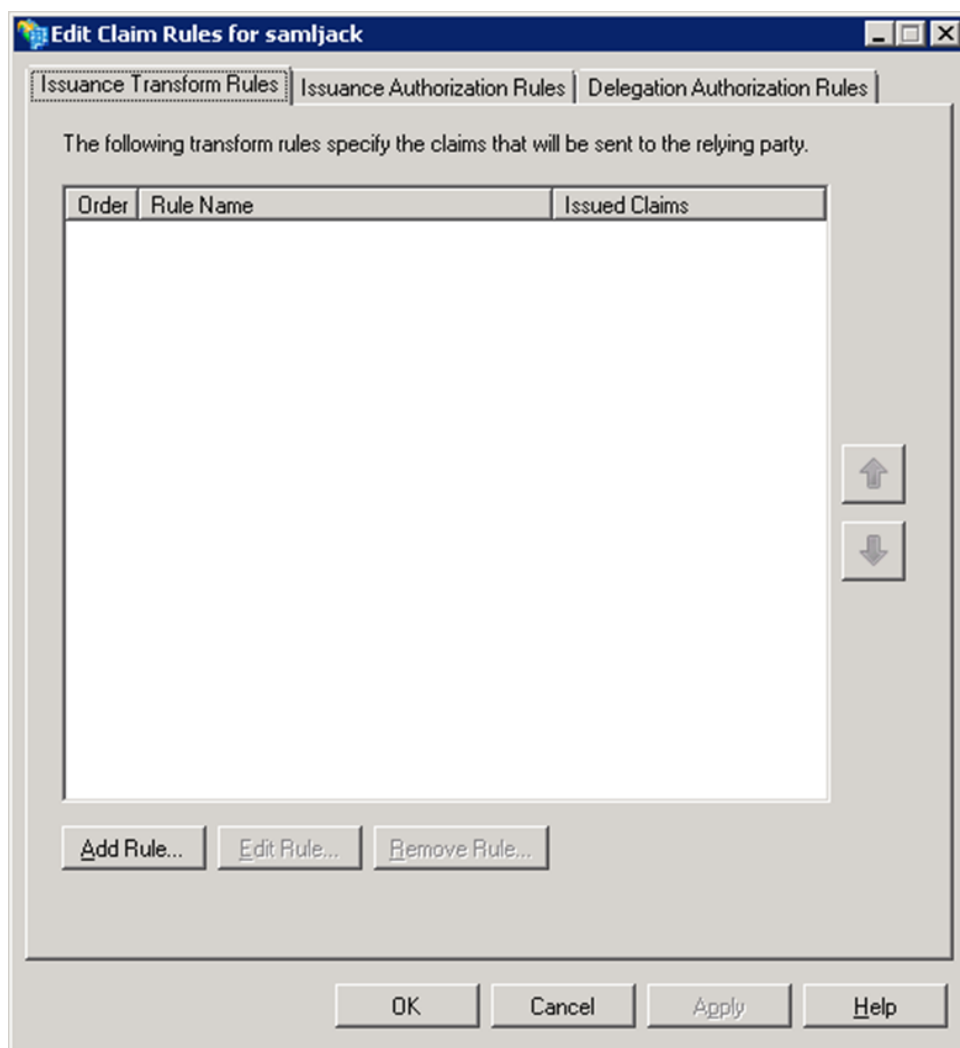
4. Click on the **Relying Party Trusts** folder. The **Relying Party Trusts** list appears in the right pane.



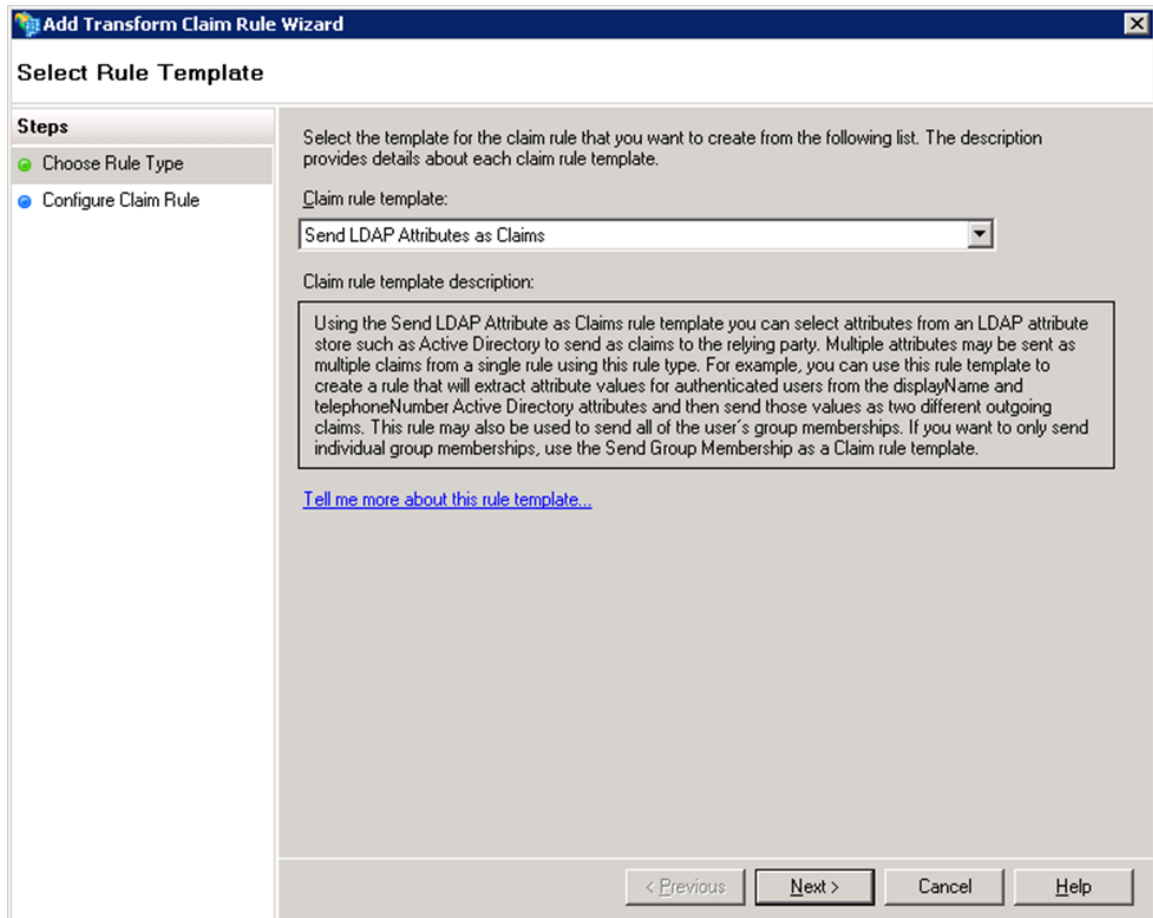
5. Right-click on the relying party application you created, and select **Edit Claim Rules**. For example, service1.domain.com



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**.



The screenshot shows the 'Add Transform Claim Rule Wizard' window, specifically the 'Select Rule Template' step. The 'Steps' pane on the left shows 'Choose Rule Type' as the current step. The main area contains a dropdown menu for 'Claim rule template' with 'Send LDAP Attributes as Claims' selected. Below this is a text box for the 'Claim rule template description' which explains that this template allows sending multiple LDAP attributes as claims. At the bottom are buttons for '< Previous', 'Next >', 'Cancel', and 'Help'.

Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

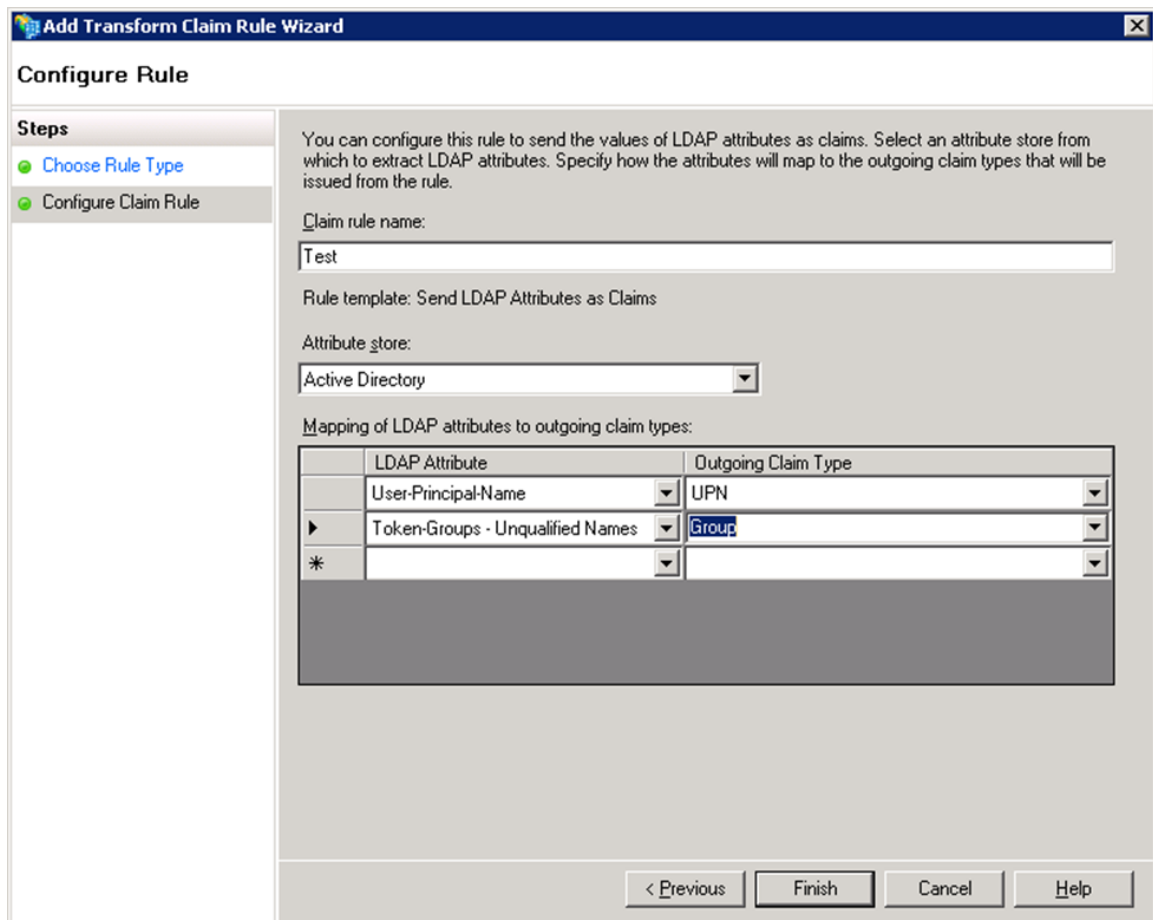
[Tell me more about this rule template...](#)

< Previous Next > Cancel Help

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



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

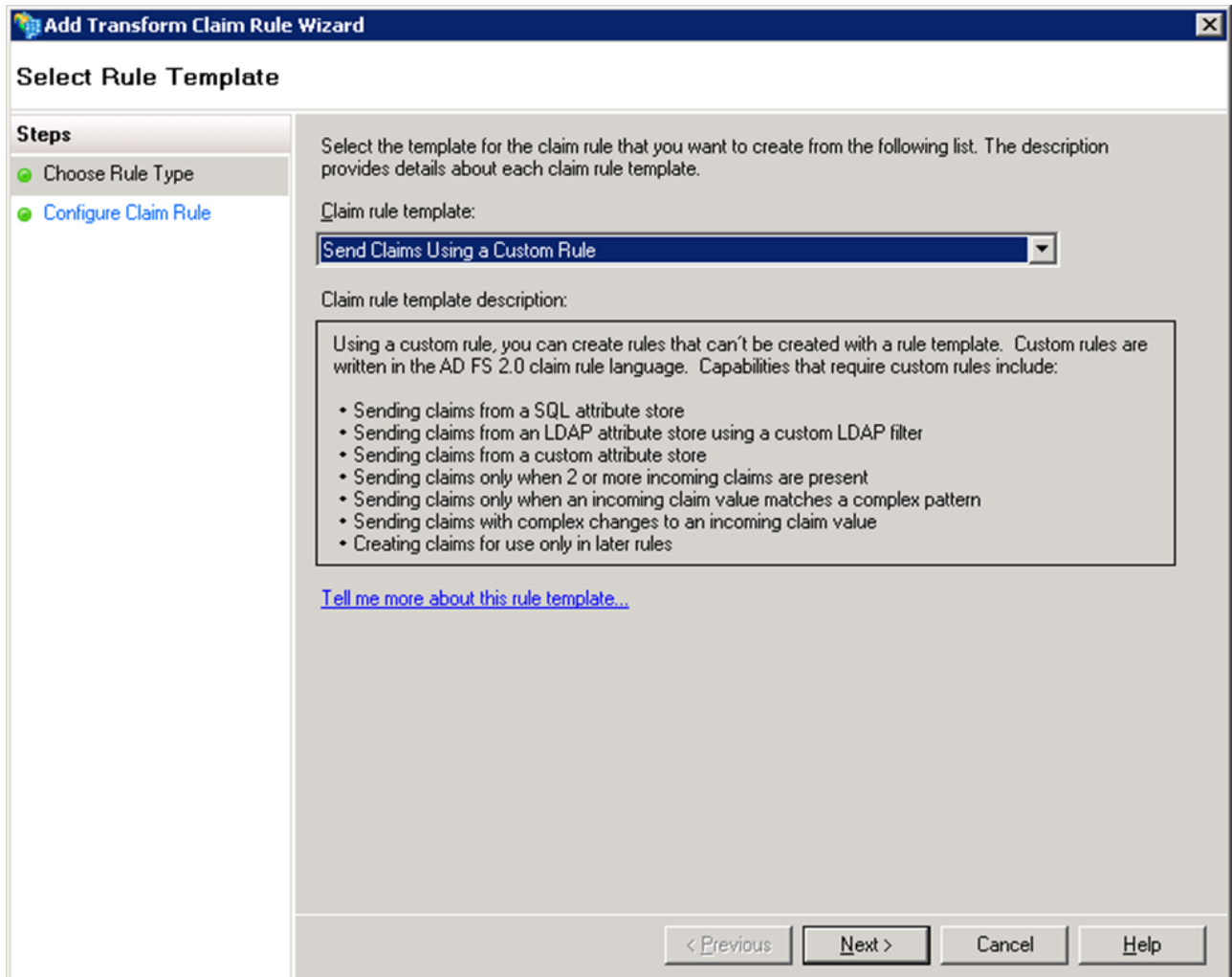
Mapping of LDAP attributes to outgoing claim types:

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

< Previous Finish Cancel Help

4. Click **Finish**.

9. Create transform rules for the attributes added in Step 8c (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**.

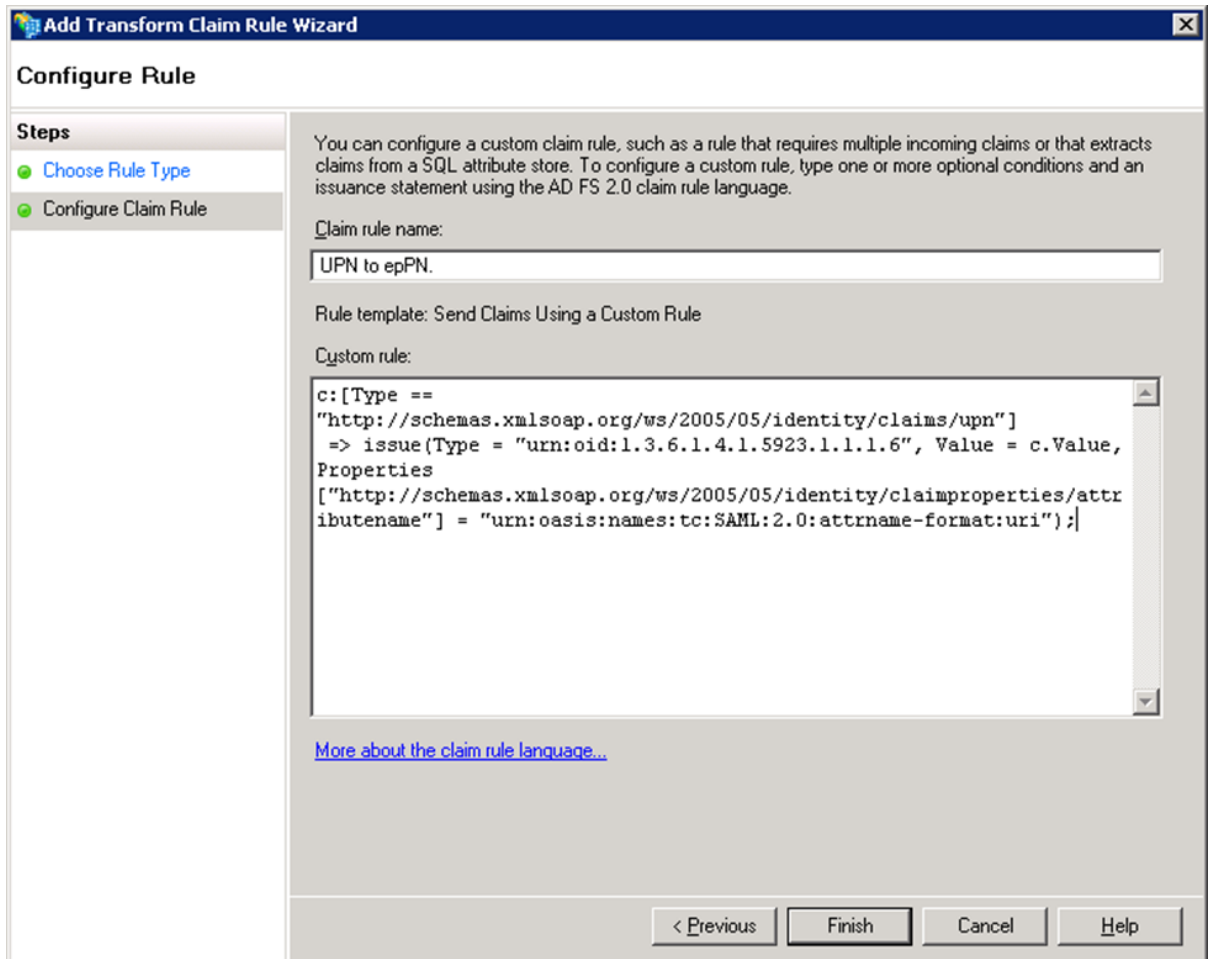


12. In the **Configure Claim Rule** step:

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**.



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.

Claim rule name:
UPN to epPN.

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
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/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

[More about the claim rule language...](#)

< Previous Finish Cancel Help

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/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

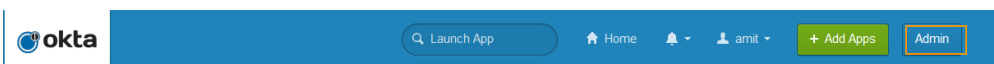
The **domain.com** name above should be the domain name of the AD FS Server configured.

3. Click **Finish**, and then **OK**.
17. The added rules display under the **Issuance Transform Rules** tab.

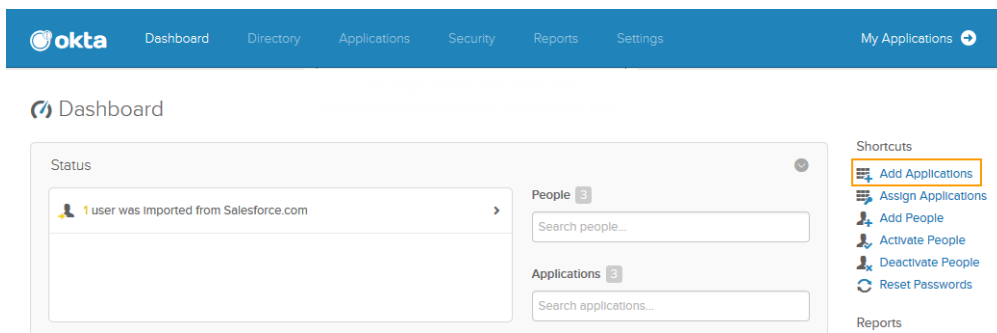
Configuring Okta for SAML Authentication

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:

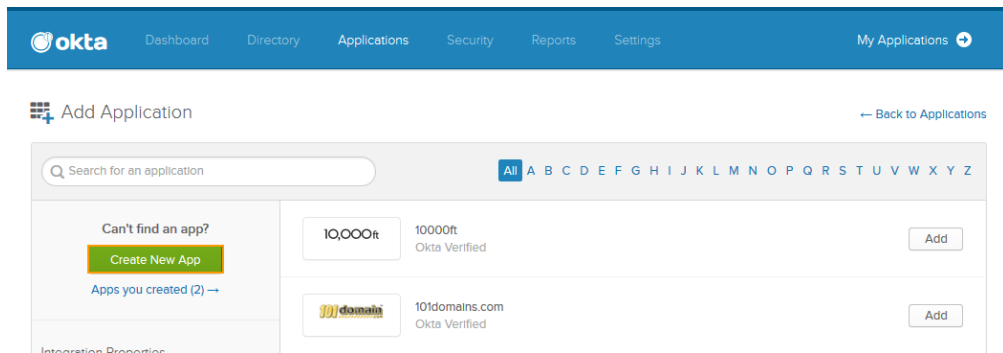
1. Download the IdP metadata from the Okta.
2. Use the IdP metadata information and create a SAML IDP authentication service on the **ACCESS CONTROL > Authentication Services** page.
3. Continue with Steps 3 to 6 under **Configuring SAML on the Barracuda Web Application Firewall** in the [SAML Authentication](#) 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.
8. Click **Admin** on the Okta homepage.



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

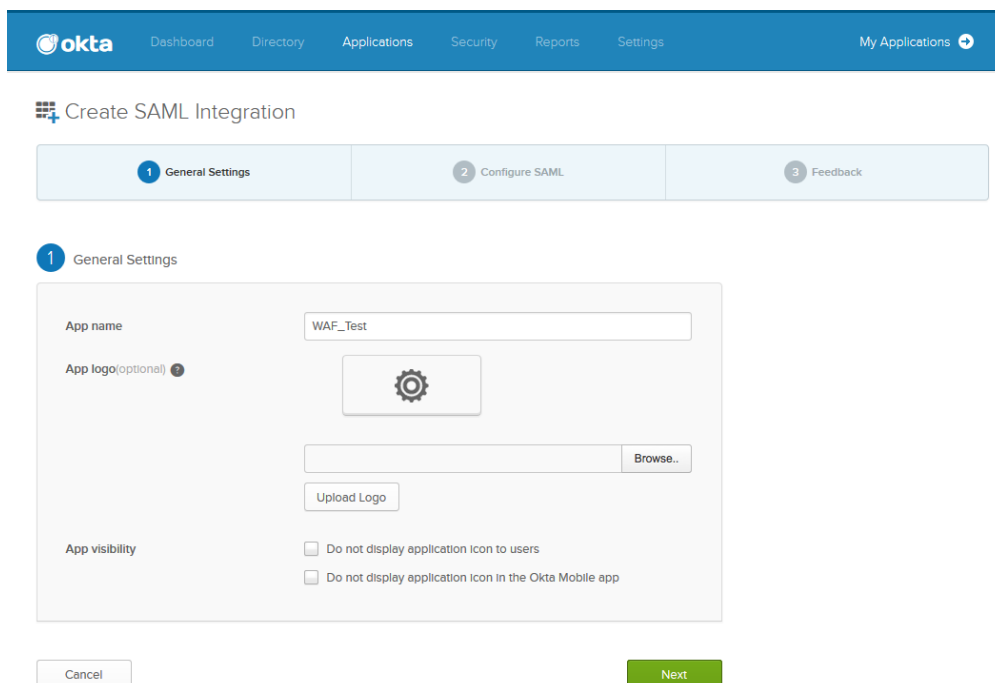


10. On the **Add Application** page, click **Create New App** and do the following:
 1. Select **SAML 2.0** in the **Create a New Application Integration** window and click **Create**.



The screenshot shows the 'Add Application' page in the Okta admin console. The top navigation bar includes 'Dashboard', 'Directory', 'Applications', 'Security', 'Reports', 'Settings', and 'My Applications'. The main heading is 'Add Application' with a 'Back to Applications' link. A search bar is present with the text 'Search for an application'. Below the search bar, there are two columns of application cards. The first column has a 'Can't find an app?' section with a 'Create New App' button and a link to 'Apps you created (2)'. The second column shows two application cards: '10,000ft' (Okta Verified) and '101domains.com' (Okta Verified), each with an 'Add' button.

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





The screenshot shows the 'Create SAML Integration' page in the Okta admin console. The top navigation bar is the same as the previous screenshot. The main heading is 'Create SAML Integration' with a progress bar showing three steps: '1 General Settings', '2 Configure SAML', and '3 Feedback'. The 'General Settings' step is active. The form contains the following fields and options:

- App name**: A text field with the value 'WAF_Test'.
- App logo(optional)**: A section with a gear icon, a text input field, and a 'Browse...' button.
- Upload Logo**: A button.
- App visibility**: Two checkboxes:
 - ☐ Do not display application icon to users
 - ☐ Do not display application icon in the Okta Mobile app

At the bottom, there are 'Cancel' and 'Next' buttons.

3. 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**.

 Dashboard Directory Applications Security Reports Settings My Applications 

Create SAML Integration


1 General Settings

2 Configure SAML


3 Feedback


A SAML Settings

GENERAL


Single sign on URL 

☒ Use this for Recipient URL and Destination URL


Audience URI (SP Entity ID) 


Default RelayState 

If no value is set, a blank RelayState is sent


Name ID format 

Transient



Application username 



Okta username



Show Advanced Settings

ATTRIBUTE STATEMENTS (OPTIONAL)

LEARN MORE

Name	Name format (optional)	Value
<input type="text"/>	<div>Unspecified</div> <div></div>	<div><input type="text"/></div> <div></div>

Add Another

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

B Preview the SAML assertion generated from the information above

< > Preview the SAML Assertion

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

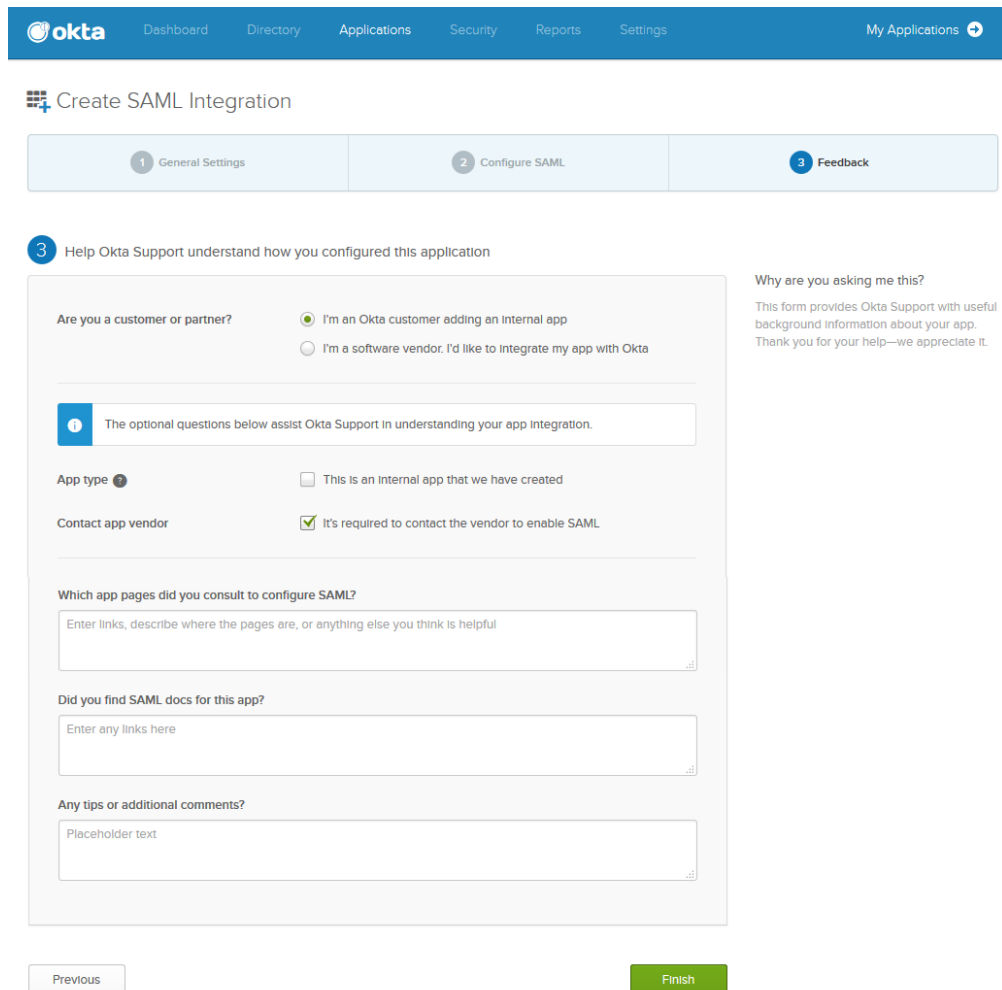
Previous

Cancel

Next

4. 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**.



okta Dashboard Directory Applications Security Reports Settings My Applications ➔

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

☒ I'm an Okta customer adding an internal app

☐ I'm a software vendor. I'd like to integrate my app with Okta

i The optional questions below assist Okta Support in understanding your app integration.

App type ⓘ ☐ This is an internal app that we have created

Contact app vendor ☒ It's required to contact the vendor to enable SAML

Which app pages did you consult to configure SAML?

Enter links, describe where the pages are, or anything else you think is helpful

Did you find SAML docs for this app?

Enter any links here

Any tips or additional comments?

Placeholder text

Previous Finish

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

5. Click **Finish**.

Configuring Duo Single Sign-On (SSO) Using SAML Authentication

To configure the Barracuda Web Application Firewall with Duo SSO using SAML Authentication, see the article [Duo Single Sign-On for Barracuda Web Application Firewall](#) .

Figures

1. saml2.jpg
2. saml3.jpg
3. Trust_Relationships.png
4. Relying_Party_Trusts.png
5. Edit_Claim_Rules.png
6. Issuance_Transform_Rules.png
7. Select_Rule_Template.png
8. Configure_Rule.png
9. Send_Claims_Using_a_Custom_Rule.png
10. Claim_Rule_Name.png
11. Admin.png
12. Add_Applications.png
13. Create_New_App.png
14. General_Settings.png
15. Configuring_SAML.png
16. Feedback.png

© Barracuda Networks Inc., 2024 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.