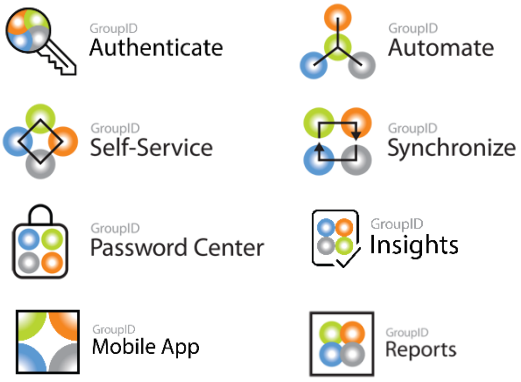
GroupID

by imanami | NOW PART OF netwrix

Version 10.2



User Guide

Authenticate

This publication applies to GroupID Version 10.2 and subsequent releases until otherwise indicated in new editions.

Contents

Chapter 1 - About GroupID Authenticate

Authenticate is a federation service for all GroupID applications. It verifies a user's identity in an identity store before allowing them to log in and use any GroupID application. With GroupID Authenticate, users are provided single sign-on support across all GroupID applications that use the same identity store.

With Authenticate, you can use GroupID both as a service provider and as an identity provider.

- **As a service provider**

  GroupID Authenticate can be extended with third party single sign-on solutions that support the SAML 2.0 standard. Supported identity providers are:

  - AD FS
  - Azure AD SSO
  - Okta
  - PingOne
  - OneLogin

  On accessing GroupID, end users would be authenticated via the configured identity provider and logged in.

  You can also implement multi-factor authentication in GroupID using a third-party single sign-on solution or with the options available in GroupID.

- **GroupID as an identity provider**

  GroupID can also be implemented as an identity provider in your organization. The administrator can configure third-party applications (service providers) with GroupID, in which case GroupID authenticates and authorizes users for those applications.

Launch GroupID Authenticate

1. In GroupID Management Console, click **Authenticate** in the left pane.

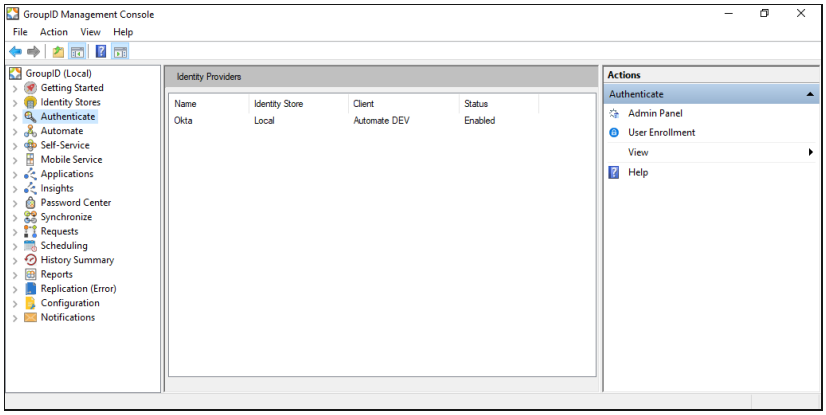


Figure 1: GroupID Authenticate

The **Identity Providers** listing displays any SAML identity providers that have been configured with GroupID.

2. Click **Admin Panel** in the **Actions** pane to launch the SSO Admin Panel for GroupID, where you can configure GroupID as a service provider as well as an identity provider.

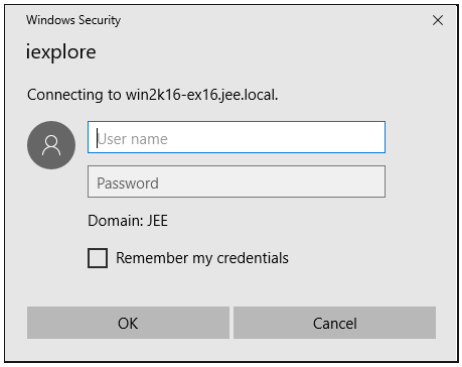


Figure 2: Windows Security dialog box

3. Provide the user name and password of a Windows or AzMan authenticated user to log into the admin panel.

   To learn about authenticated users, see Appendix A - Authenticated users in Windows AzMan on page 92.

4. Click **OK**; the GroupID Admin Panel is displayed:

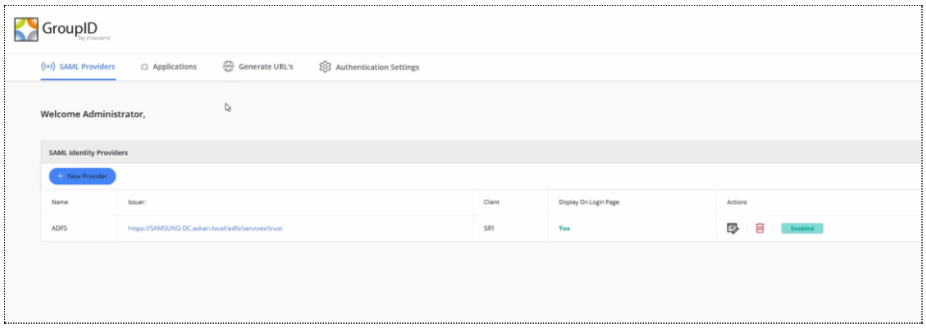


Figure 3: GroupID SSO Admin Panel

The page has four tabs. Of these, the following are used when configuring GroupID as a service provider:

- SAML Providers
  This tab displays the identity providers that have been configured for GroupID. if any. Use the **New Provider** button to add an identity provider.
- Generate URLs
  This tab contains settings (such as the consumer URL and the metadata URL) that are used to configure GroupID in an identity provider.

The following tabs are used when configuring GroupID as an identity provider:

- Applications
  This tab displays the third-party applications that have been configured to use GroupID as an identity provider. Use the **New Application** button to add a service provider.
- Authentication Settings
  This tab contains default settings that are used while configuring GroupID as an identity provider within third-party applications.

Enable Integrated Windows Authentication

To launch GroupID Authenticate successfully, you must enable Integrated Windows Authentication for the following web browsers on the GroupID machine:

- Mozilla Firefox
- Google Chrome

This is required due to high security settings on a Windows server operating system.

For Internet Explorer

Integrated Windows Authentication is enabled for Internet Explorer by default.

For Firefox:

1. Launch the Firefox browser and type *about:config* in the address bar.
2. Find the following settings and change their values as specified:

Setting	Required value
network.automatic-ntlm-auth.trusted-uris	MyIISServer.domain.com
network.automatic-ntlm-auth.allow-proxies	true
network.negotiate-auth.allow-proxies	true

Table 1: Firefox settings

For Chrome:

1. Type *regedit* in the **Run** dialog and click **OK** to launch the Registry Editor.
2. Go to the following location:
   HKEY_CURRENT_USER\Software\Policies\Google\Chrome
   (create this path if it does not exist).
3. Add the following values:

Setting	Required value
AuthSchemes	basic,digest,ntlm,negotiate
AuthServerWhitelist	MYIISSERVER.DOMAIN.COM (e.g. MachineName.DomainName, MachineName)
AuthNegotiateDelegateWhitelist	MYIISSERVER.DOMAIN.COM (e.g. MachineName.DomainName, MachineName)

Table 2: Registry settings for Chrome

It is as:

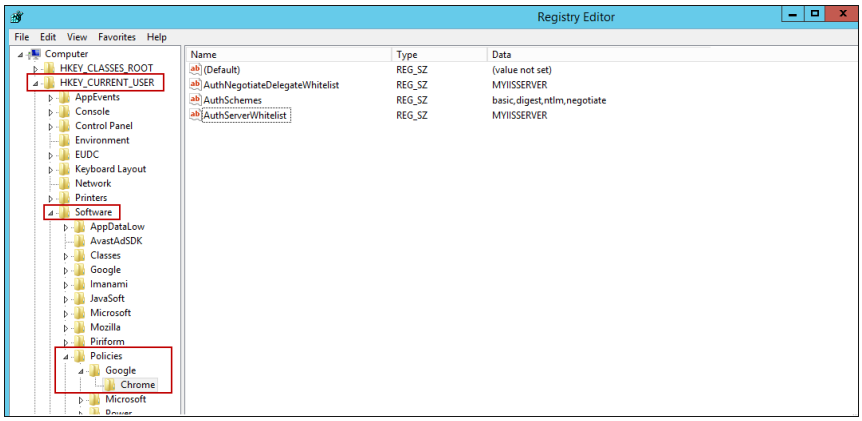


Figure 4: Registry Editor settings

4. Next, launch Control Panel and go to **Internet Options**.
5. On the **Security** tab, select **Local Intranet** and click **Custom Level**.
6. On the **Security Settings** dialog box, scroll down to **User Authentication** and set the **Logon** option to **Prompt for user name and password**.

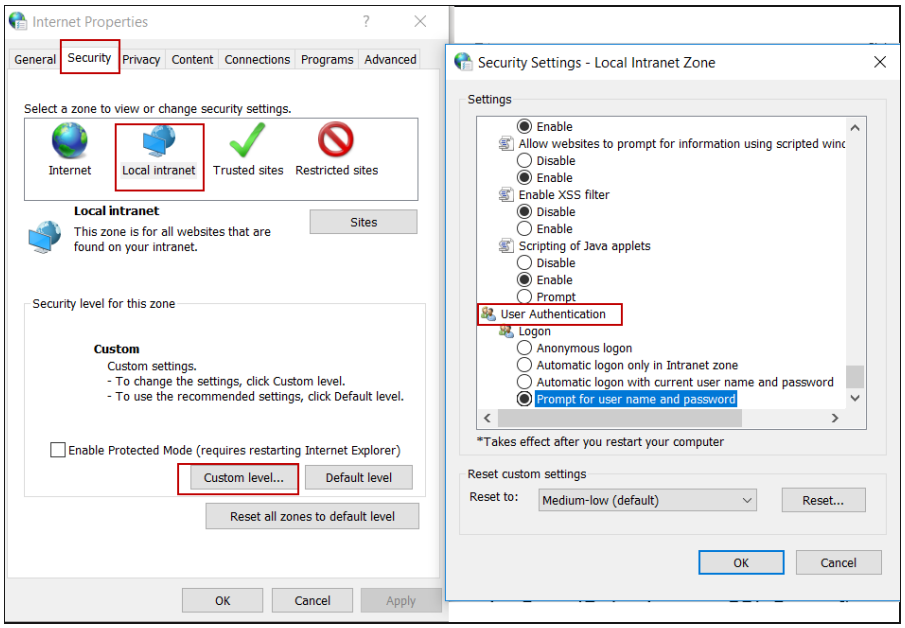


Figure 5: Settings for Internet Options

7. Click **OK**.

GroupID Security Service

GroupID Security Service is a single sign-on implantation for GroupID clients/modules. It is a web-based service responsible for authenticating and

authorizing users on different GroupID clients/modules and their functionalities in accordance with their roles.

Authentication can be done by providing a username and password in GroupID (for which multi-factor authentication can also be used) or through an external SAML provider (security endpoint is dependent on the identity provider).

Part 1 - GroupID as a Service Provider

Chapter 1 - SAML Configuration for GroupID using AD FS

Active Directory Federation Services (AD FS) is a software component developed by Microsoft that provides users with single sign-on access to systems and applications located across organizational boundaries.

The AD FS Console

Use the AD FS console to configure services and policies that are related to the deployment of a federation server.

- Manage the trust relationships of the federation service by using the **Trust Relationships** node in the AD FS console tree (Figure 8):
  - Add and configure relying party trusts.
  - Add and modify claim rules for relying party trusts.
- Configure the federation service by using the options in the **Service** node in the AD FS console tree:
  - Configure the certificates that AD FS uses for issuing and receiving tokens and publishing metadata.
  - Configure the types of claims that are supported by AD FS.

To learn more about the AD FS Console, click here.

Generate Consumer URL

The consumer URL is unique for each GroupID module (referred to as 'application' here). In GroupID Single Sign-On Admin Panel, generate the consumer URL for the GroupID application with which you want to configure AD FS. Provide this URL while creating the relying party trust in AD FS.

1. In the GroupID Single Sign-On Admin Panel (Figure 3), click **Generate URLs**.

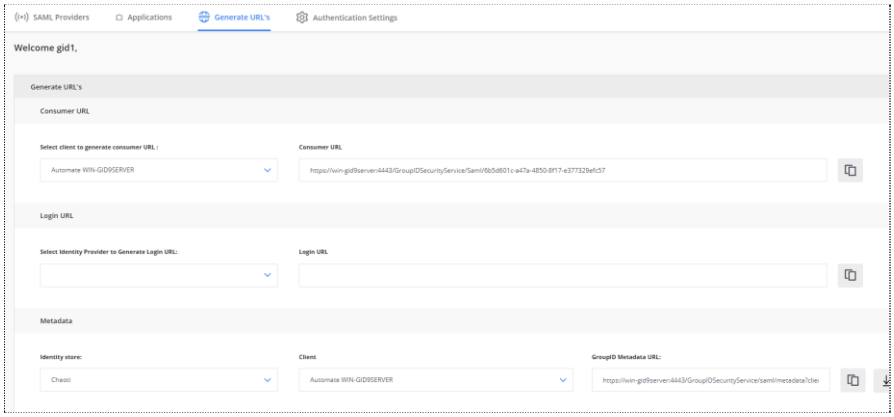


Figure 6: Generate URLs page

2. In the **Select Client to Generate Consumer URL** list, select a GroupID application to set up AD FS with it.

   This list contains all GroupID applications, namely

   - Automate
   - Management Shell
   - All Self-Service and Password Center portals created using GroupID

   As an example, let's suppose you select the Self-Service portal named *Wizard*.

3. The URL displayed in the **Consumer URL** box is a unique identifier for the selected application. It is used to set up relying party trust in AD FS. Click to copy it. Then paste it in a file, preferably a text file, to save it.

1. On upgrade to GroupID 10 SR2, you must generate the consumer URL again for the GroupID client configured with AD FS, and update it in AD FS.
2. If you lose the SQL server or the GroupID server, you will have to configure the provider again.

Generate Entity ID/Audience URL

The audience URL is unique for each GroupID module (referred to as 'application' here). In GroupID Single Sign-On Admin Panel, generate the audience URL for the GroupID application with which you want to configure AD FS. Copy this URL and paste it while creating the relying party trust in AD FS.

1. In GroupID Single Sign-On Admin Panel (Figure 3), click the **New Provider** button to add a new provider.

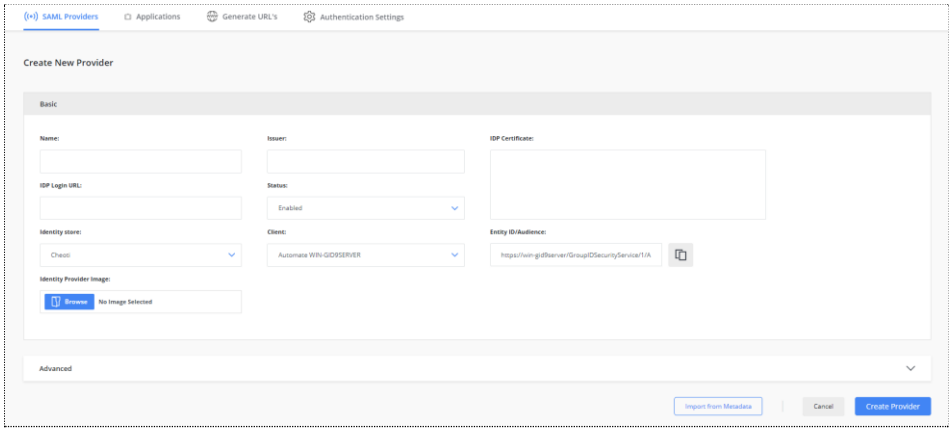


Figure 7: Add New SAML Provider page

2. In the **Client** list, select the GroupID application with which you want to set up the SAML provider.

   This list contains all GroupID applications, namely

   - Automate
   - Management Shell
   - All Self-Service and Password Center portals created using GroupID

   The application you select must be the one for which you generated the consumer URL on the **Generate URLs** page (Figure 6).

   To continue with the example, select the Self-Service portal named *Wizard* in the **Client** list.

3. The **Entity ID/Audience** box displays a URL that serves as the application ID. Click to copy it.

Configure relaying party trust in AD FS

1. Launch the AD FS console. In the left pane, select **AD FS > Trust Relationships**. Right-click **Relying Party Trusts** and click **Add Relying Party Trust** on the shortcut menu.

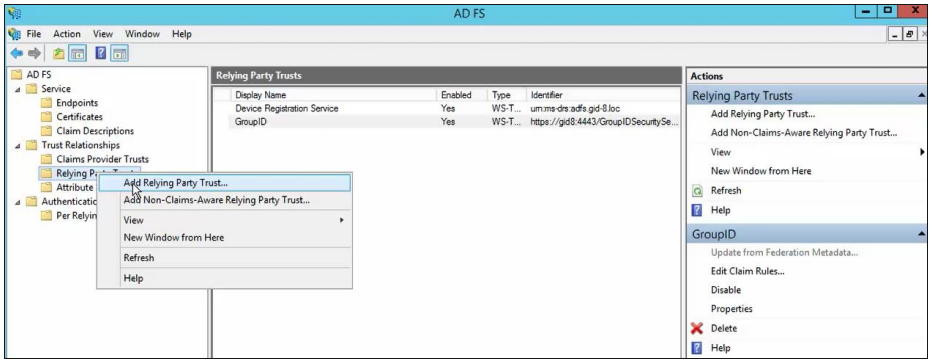


Figure 8: AD FS Console

2. The **Add Relying Party Trust** wizard opens to the **Welcome** page.

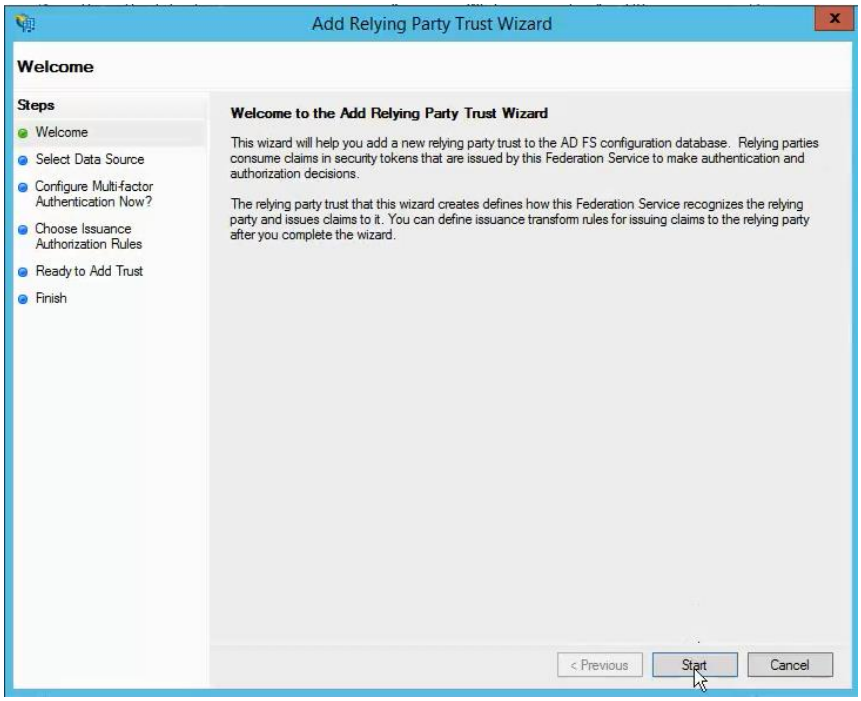


Figure 9: Welcome page

3. Read the welcome message and click **Start**.

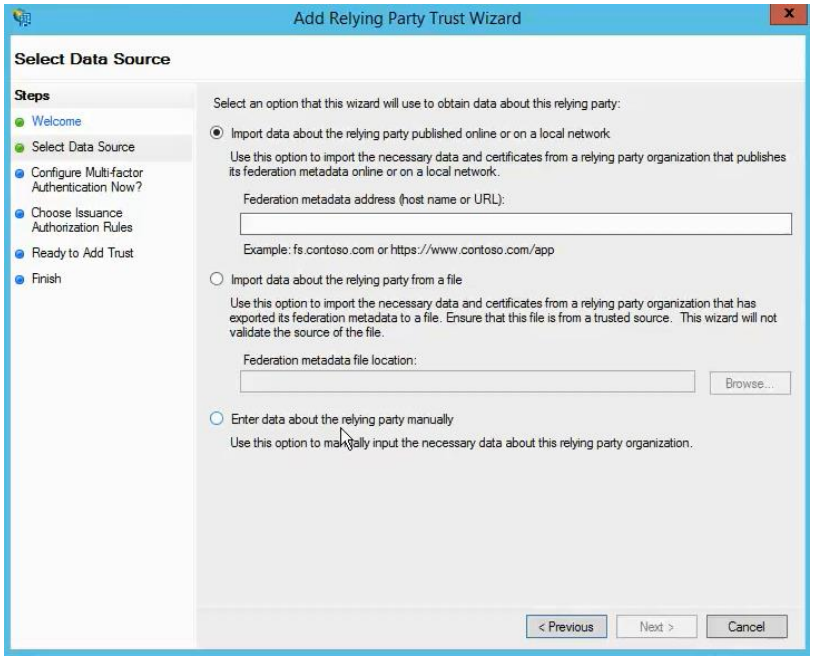


Figure 10: Select Data Source page

4. Use the options on the **Select Data Source** page to either import relying party trust data from a file, such as a metadata file, or enter the information manually.

   To enter information manually, select the **Enter data about the relying party manually** option and click **Next**.

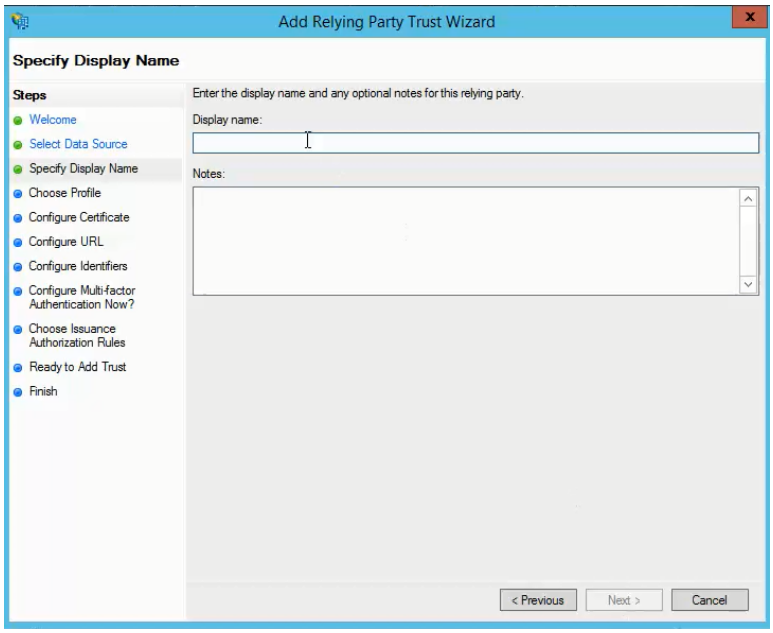


Figure 11: Specify Display Name page

5. In the **Display name** box, specify a friendly display name for this configuration.
6. Enter any additional notes in the **Notes** box.
7. Click **Next**.

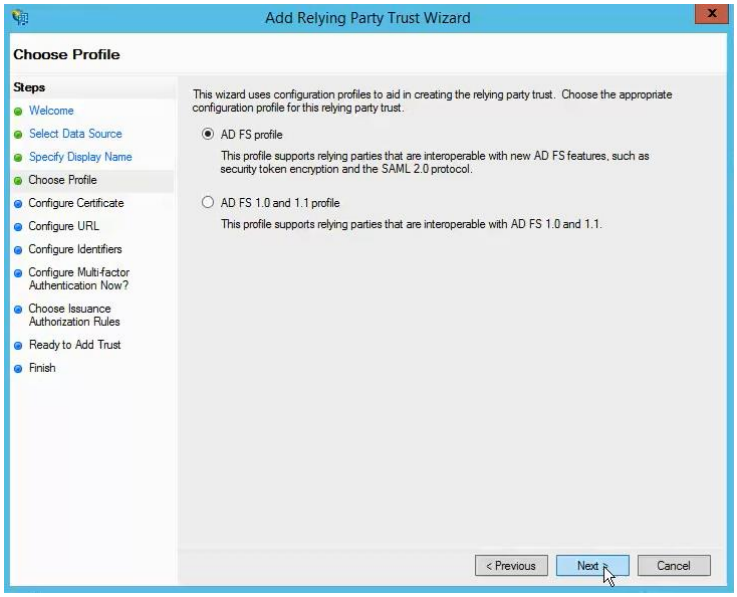


Figure 12: Choose Profile page

8. To use the SAML 2.0 protocol as profile, select the **AD FS profile** option button and click **Next**.

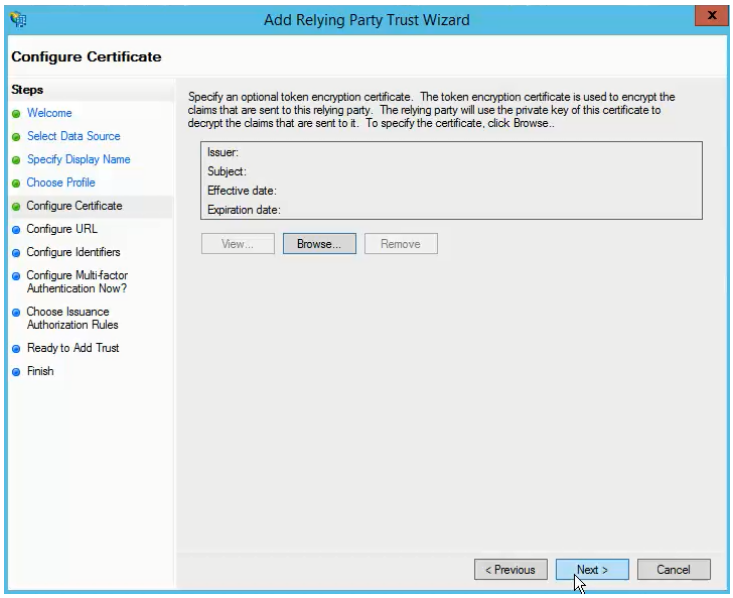


Figure 13: Configure Certificate page

9. Click **Next**.

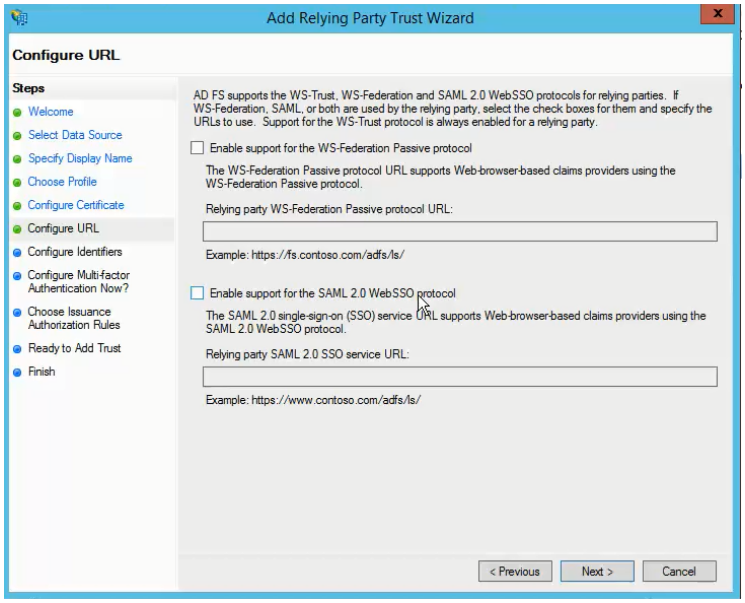


Figure 14: Configure URL page

10. Select the **Enable support for the SAML 2.0 Web SSO protocol** option button.
11. In the **Relying party SAML 2.0 SSL service URL** box, provide the consumer URL you generated on the **Generate URLs** page (Figure 6).

    The consumer URL is the relying party trust URL, used by AD FS to authenticate.
12. Click **Next**.

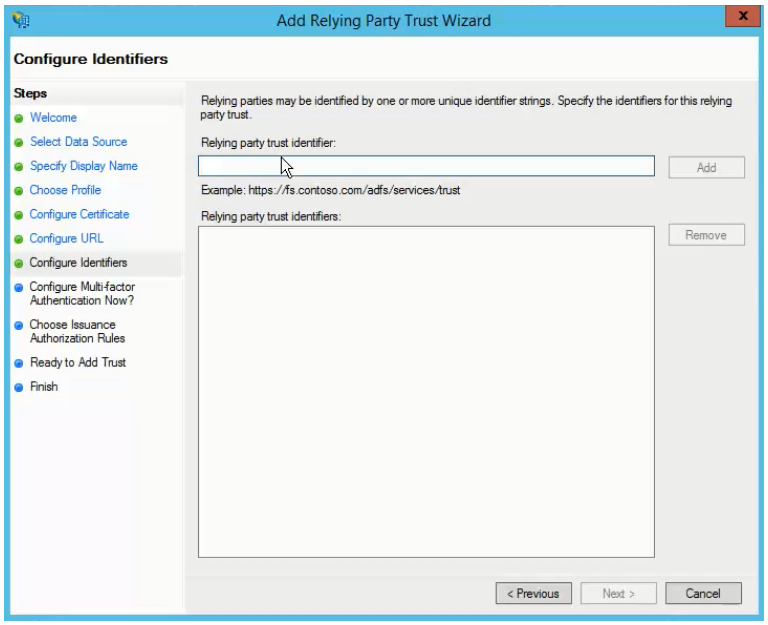


Figure 15: Configure Identifiers page

13. In the **Relying party trust identifier** box, provide the audience URL. Fetch this URL from the **Entity ID Audience** field on the **Add New SAML Provider** page (Figure 7).

14. Click **Add** next to this box and then click **Next**.

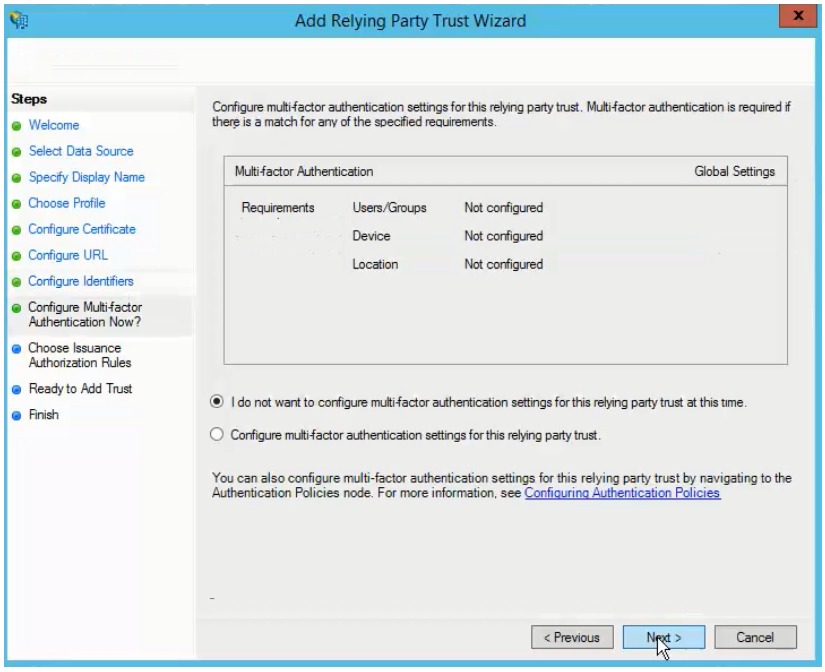


Figure 16: Configure Multi-factor Authentication Now page

15. Use the **Configure Multi-factor Authentication Now?** page to configure multi-factor authentication. At present, we will not configure it, so select the **I do not want to configure multi-factor authentications settings for this relying party trust at this time** option button and click **Next**.

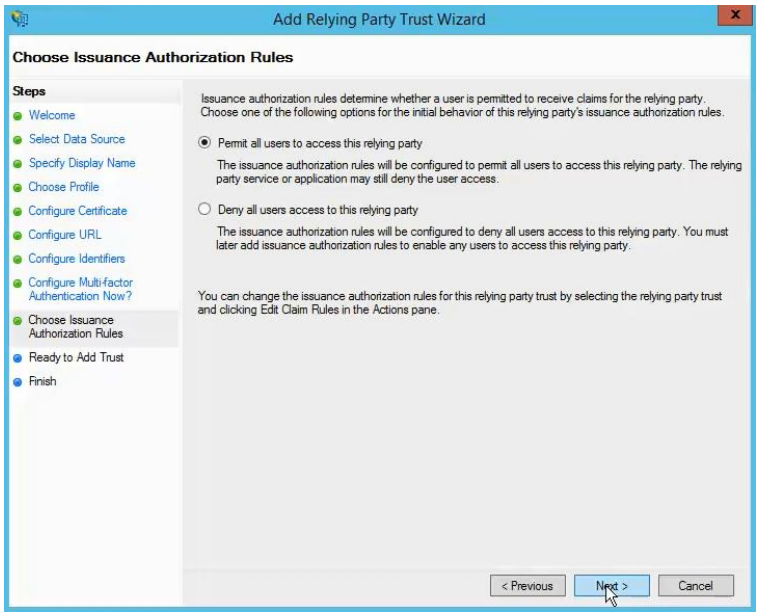


Figure 17: Choose Issuance Authorization Rules page

16. Use this page to permit all users to get authenticated on the relying party trust using AD FS. User credentials will be parsed with Active Directory.

    Select the **Permit all users to access this relying party** option button and click **Next**.

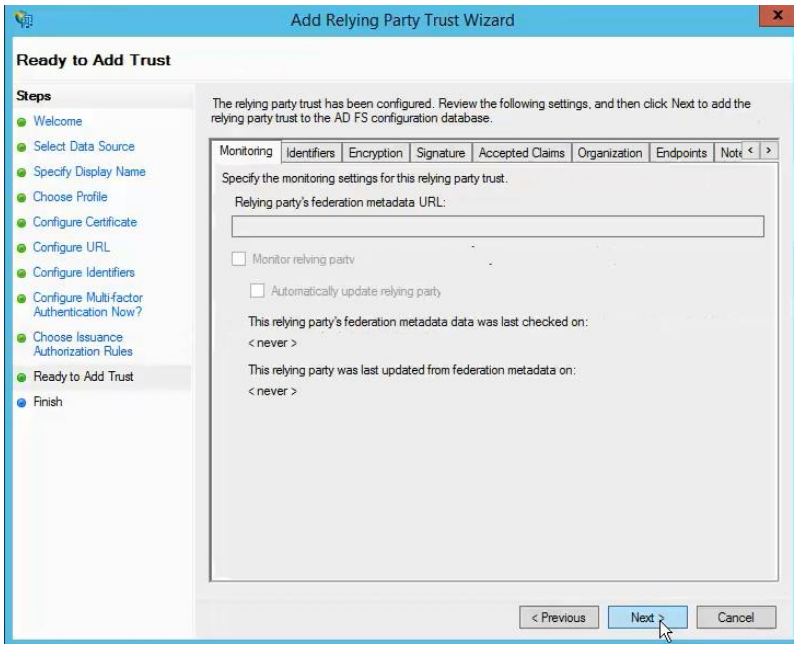


Figure 18: Ready to Add Trust page

17. Use the tabs on the **Ready to Add Trust** page to review some preconfigured settings; then click **Next**.

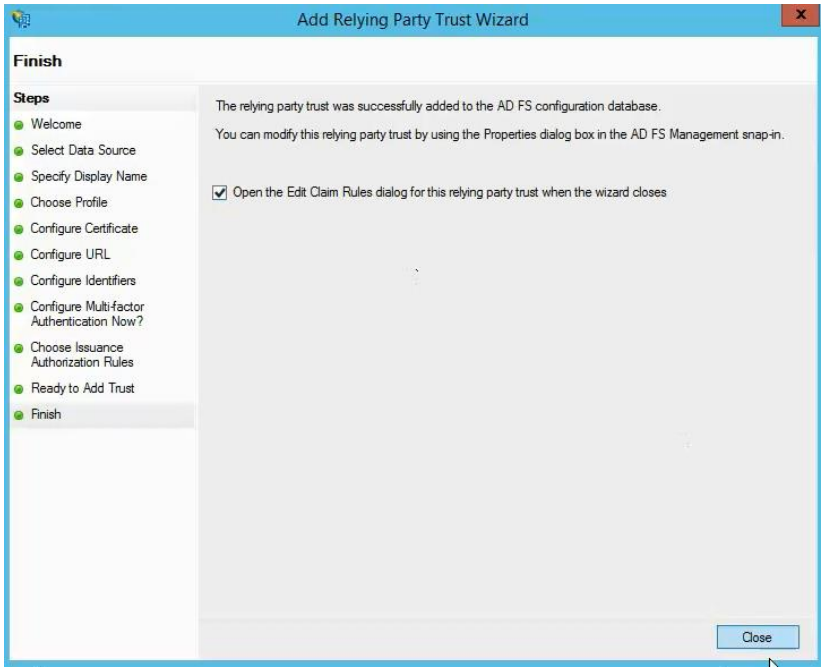


Figure 19: Finish page

18. Click **Close** to complete the wizard. The wizard closes and the following dialog box is displayed:

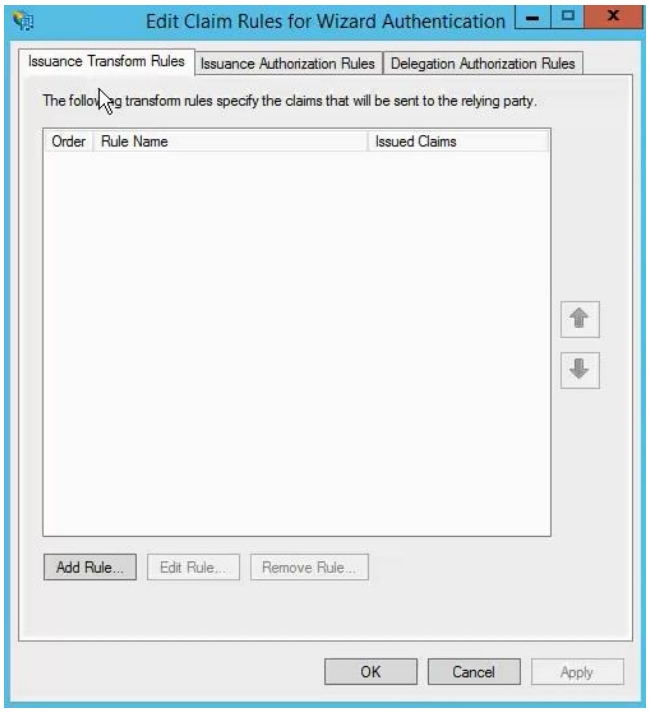


Figure 20: Edit Claim Rules dialog box

Specify claim rules for authentication

1. On the **Edit Claim Rules** dialog box (Figure 20), the **Issuance Transform Rules** option correlates to the option of authenticating using an Active Directory attribute. Click **Add Rule**.

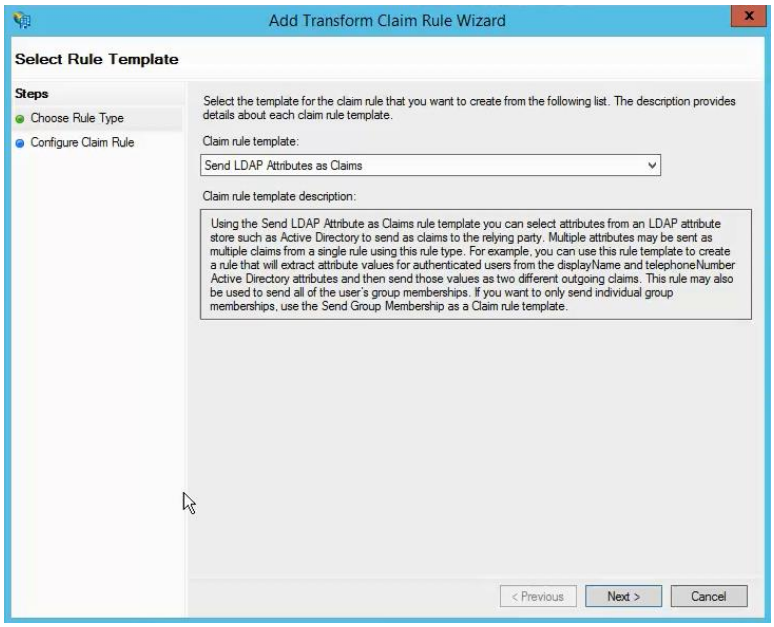


Figure 21: Choose Rule Type page

2. To add a rule, select the **Transform an Incoming Claim** option from the **Claim rule template** list and click **Next**.

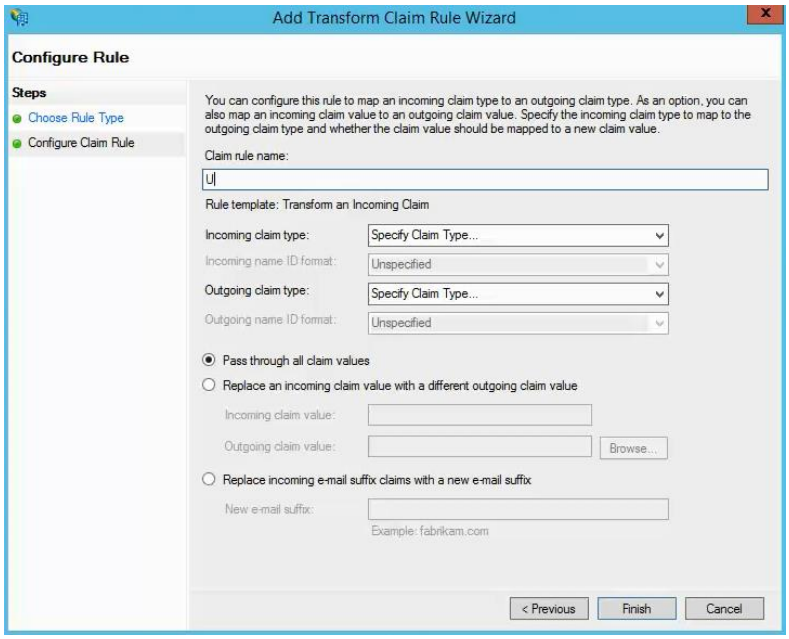


Figure 22: Configure Claim Rule

3. Specify a rule name in the **Claim rule name** box.
4. In the **Incoming claim type** and **Outgoing claim type** boxes, select an Active Directory attribute for authentication, such as the UPN attribute.

   The incoming and outgoing claim types should be the same as we will not specify a different text or different data for the logon process. It will be the exact user principal name for authentication.
5. Make sure that the **Pass through all claim values** option is selected; then click **Finish**. The new rule configuration is completed. The **Edit Claim Rules** dialog box (Figure 20) is displayed with the new rule listed on the **Issuance Transform Rules** tab.
6. Click the **Issuance Authorization Rules** tab.

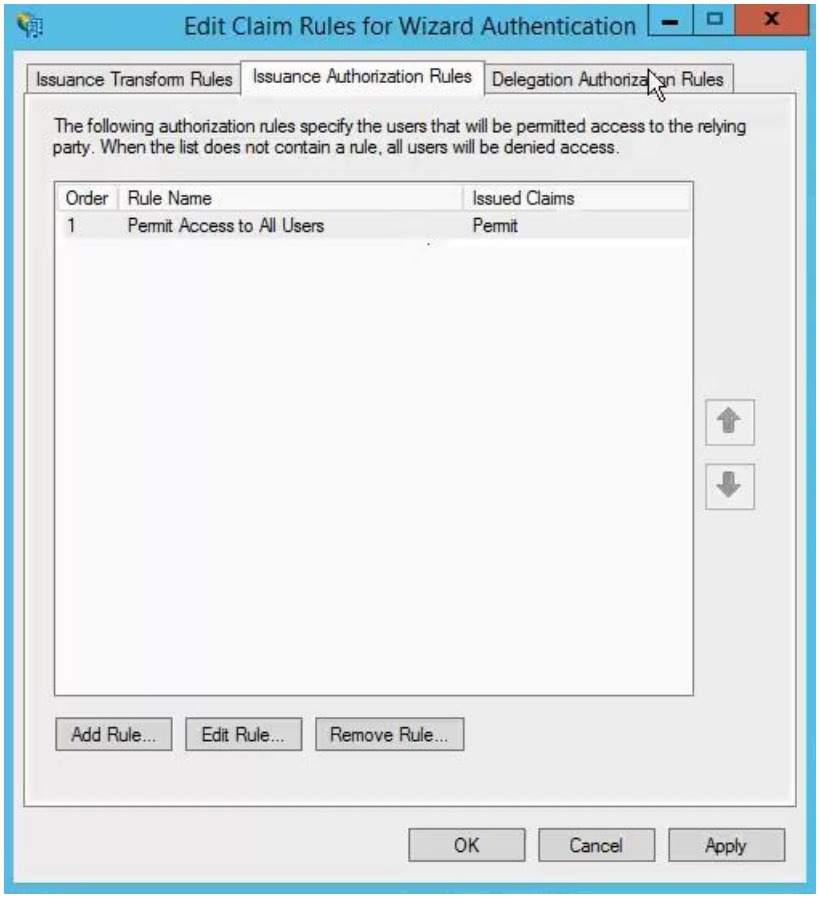


Figure 23: Issuance Authorization Rules tab

The issuance authorization rule is already completed.

7. Click the **Delegation Authorization Rules** tab.

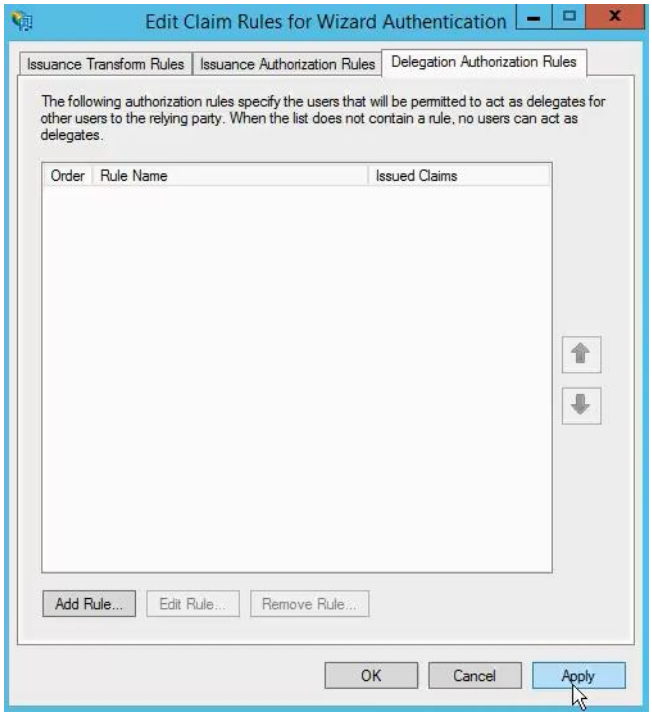


Figure 24: Delegation Authorization Rules tab

8. We do not need to delegate, so click **Apply** and then **OK**. The AD FS console (Figure 8) is displayed with the new relying party trust added.

The next step is to configure the AD FS provider in the GroupID SSO Admin Panel.

Configure the AD FS provider in GroupID

To configure the SAML provider in GroupID, go to the **Add New SAML Provider** page (Figure 7) in GroupID SSO Admin panel. The first step is to specify the Issuer URL and the IDP Login URL.

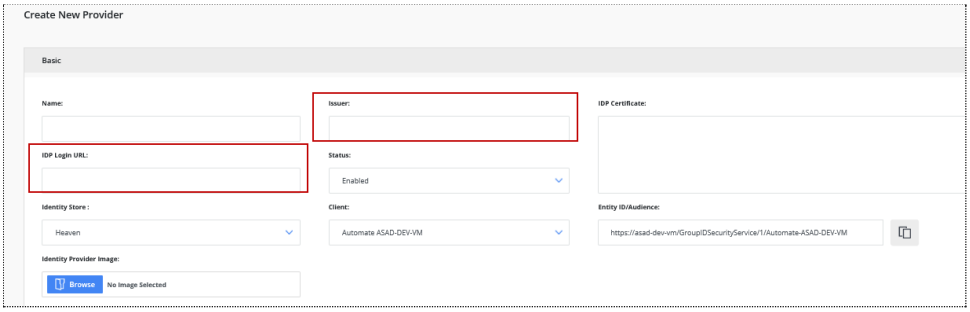


Figure 25: Add New SAML Provider page (Issuer and IDP Login URL boxes)

Provide Issuer URL

The issuer URL is provided by the federation service, i.e., AD FS. Copy this URL from AD FS and provide it in the **Issuer** box.

1. In the AD FS console, right-click **Service** and select **Edit Federation Service Properties.**

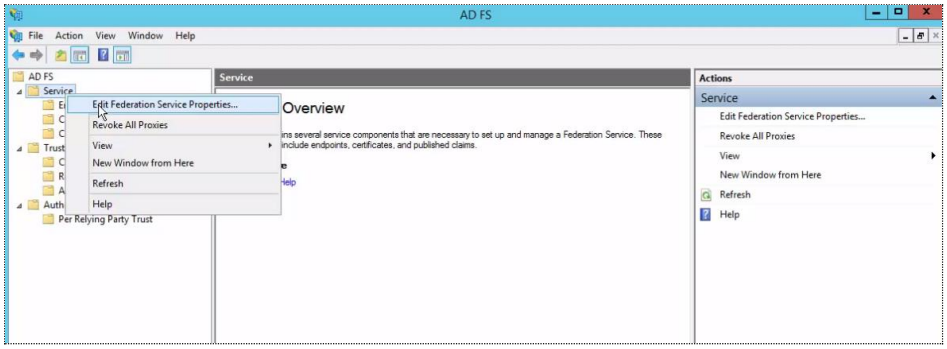


Figure 26: AD FS Console – Service node

2. The **Federation Service Properties** dialog box is displayed as follows:

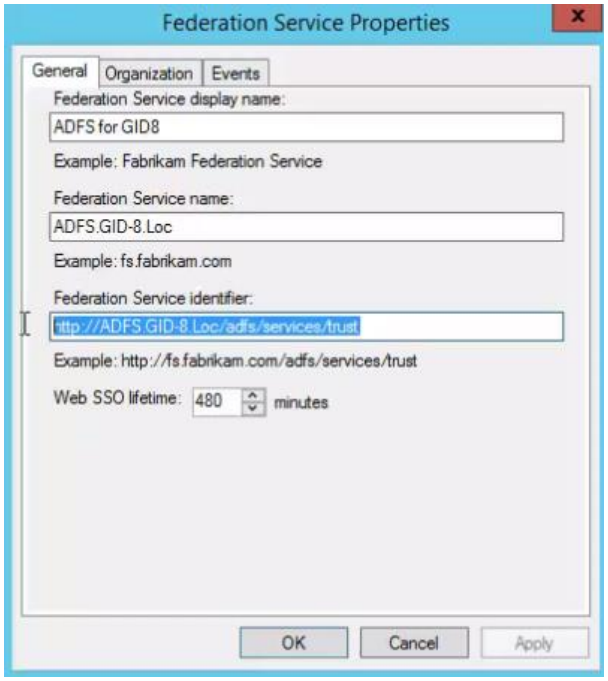


Figure 27: Federation Service Properties dialog box

3. Copy the URL displayed in the **Federation Service Identifier** box and paste it in the **Issuer** box on the **Add New SAML Provider** page (Figure 25).

Provide IDP Login URL

The IDP Login URL is the URL of the AD FS sign-in page.

1. Launch the AD FS login page and copy the URL displayed in the address bar.

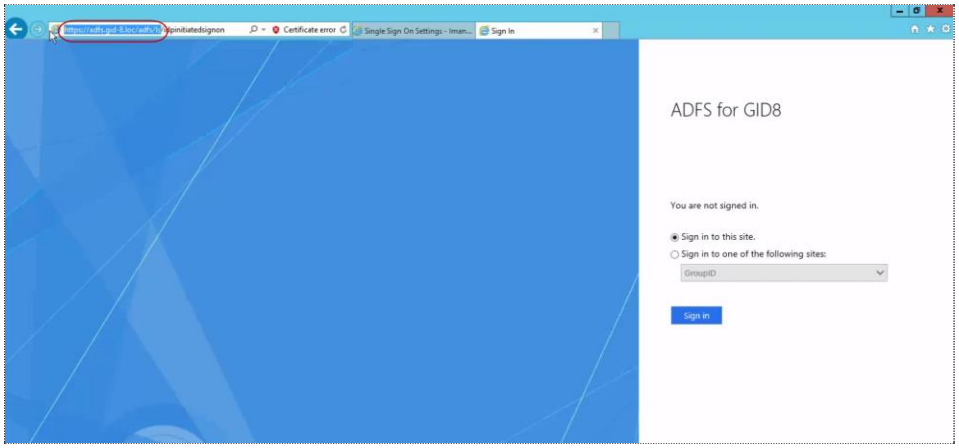


Figure 28: AD FS Authentication page

2. We only need the initial part of the URL, up to *ls*. Copy it and paste it in the **IDP Login URL** box on the **Add New SAML Provider** page (Figure 25).

Upload image for identity provider

When AD FS is configured with the GroupID application, Wizard, it will be available on Wizard's login page for single sign-on. You can choose to display the AD FS authentication option as an image or a button.

- To display the AD FS option as an image, you have to upload an image for the identity provider.

  On the **Add New SAML Provider** page (Figure 25), use the **Browse** button next to the **Identity Provider Image** box to upload an image for AD FS.

  Supported image formats are: .jpg, .bmp, .png, and .gif. Required dimensions for the image file are: 210 x 60 pixels.

OR

- If you do not want an image, AD FS authentication will be shown as a button.
  Specify a name for the button in the **Name** box (Figure 25).

Users can click the image or the button on the login page of the Self-Service portal, *Wizard* (Figure 43) for single sign-on.

Get token-signing certificate

The next step is to get the token-signing certificate from AD FS and provide it in GroupID.

1. To get the certificate, go to the AD FS console and click **Certificates**. The certificates are displayed as follows:

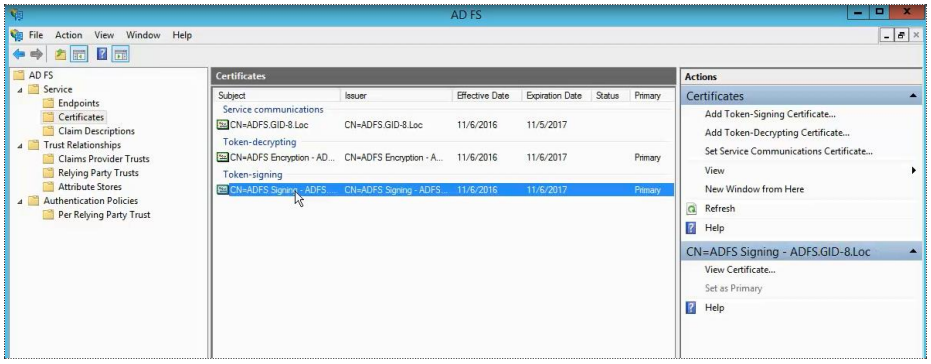


Figure 29: AS FS Console - Certificates

2. We need the token-signing certificate. Double-click this certificate to open its properties. Once the properties load, we will export the certificate to a file.

Figure 30: Certificate Properties dialog box

3. Click the **Details** tab.

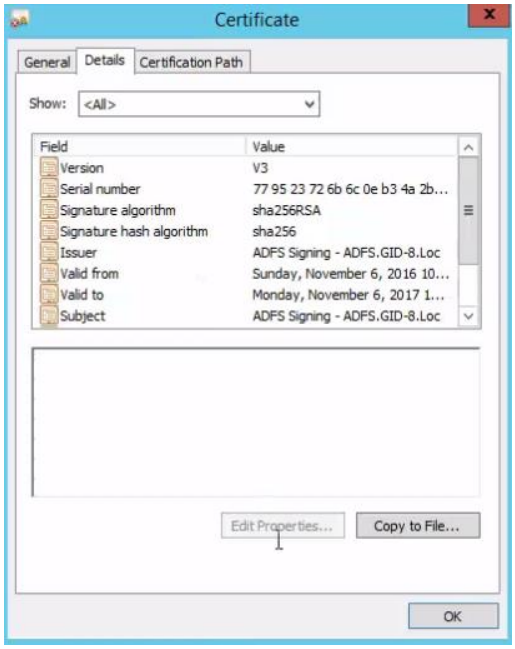


Figure 31: Details tab

4. Click the **Copy to File** button to launch the Certificate Export Wizard.

Figure 32: Certificate Export Wizard – Welcome page

5. Read the welcome message and click **Next**.

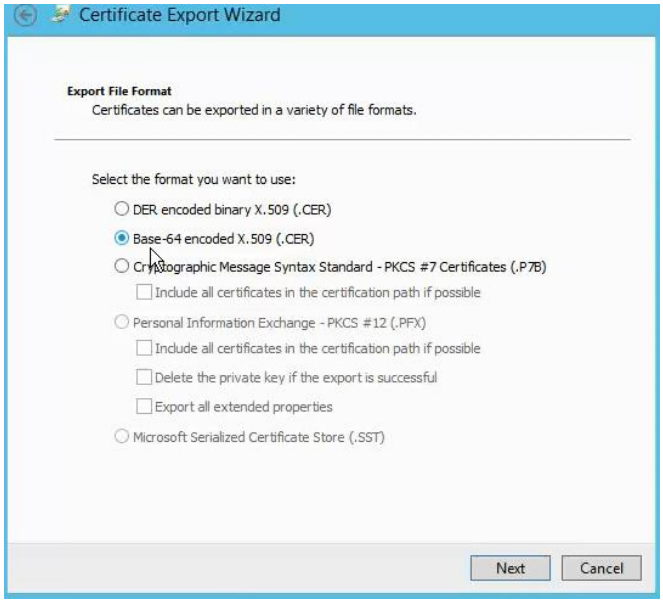


Figure 33: Export File Format page

6. On the **Export File Format** page, select the **Base-64 encoded X.509 (.CER)** option button and click **Next**.

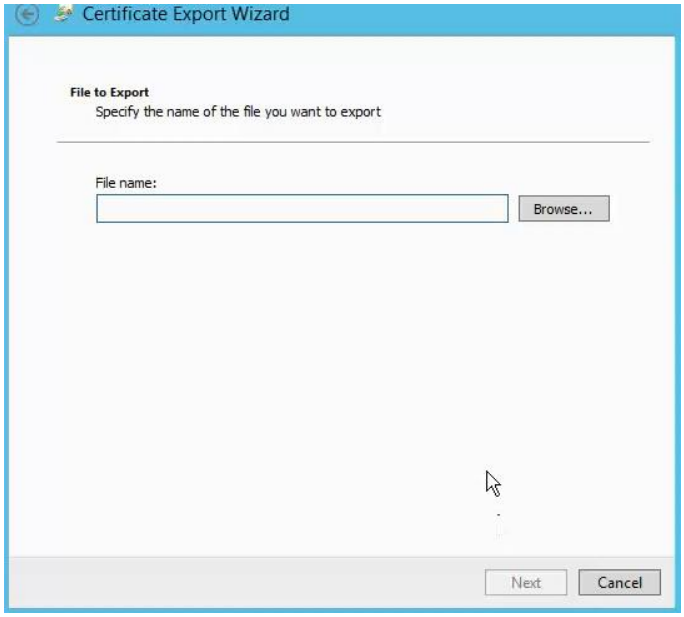


Figure 34: File to Export page

7. Specify a name for the file and click **Browse** to specify a location to save the file. Then click **Next**.

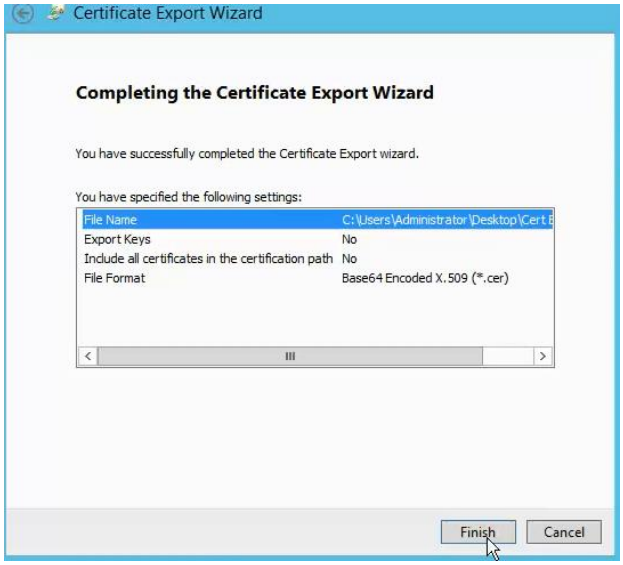


Figure 35: Completion page

8. Click **Finish** to complete the wizard.
9. Next, open the certificate file in Notepad and select the entire content.

Figure 36: Token-signing certificate

10. Copy this certificate and paste it in the **IDP Certificate** box on the **Add New SAML Provider** page (Figure 25).

Figure 37: IDP Certificate

Make sure there is no trailing space after the dashes that mark the end of the certificate.

Advanced configurations

Next, we have to do some advanced configurations for the identity provider in GroupID. Expand the **Advanced** section on the **Add New SAML Provider** page (Figure 7).

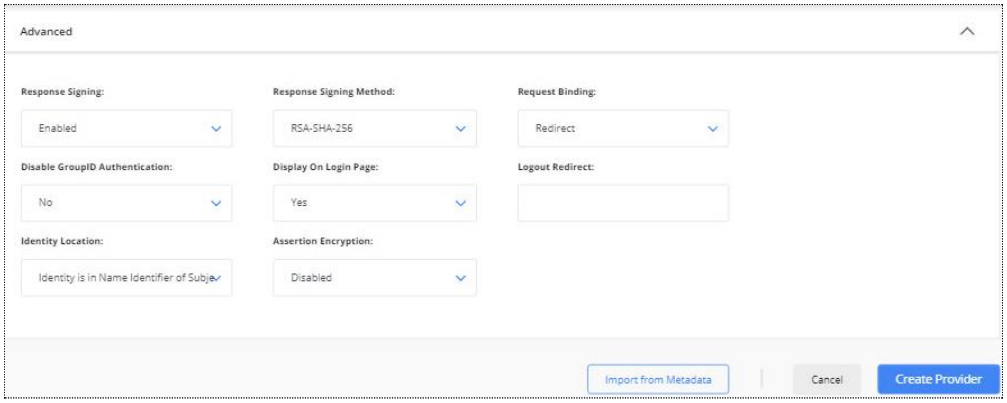


Figure 38: Add New SAML Provider page - Advanced section

1. Make sure that *RSA-SHA-256* is selected in the **Response Signing Method** box.
2. The **Disable GroupID Authentication** option indicates whether to display the GroupID authentication login on the *Wizard* portal's login page (Figure 43).
   - By default, 'No' is selected, which means that when users access the *Wizard* portal's login page, they will be shown the GroupID login and password option as well as the AD FS identity provider's button.
   - Selecting 'Yes' means that the GroupID login and password option will not be available on the *Wizard* portal's login page.

     Moreover, when a single identity store and a single SAML provider is configured, the login page for the provider is displayed rather than the *Wizard* portal's login page. (The AD FS login page is as shown in Figure 44.)
3. Select *Post* in the **Request Binding** list.

   To verify that you have selected the correct binding type, do the following:

   a. In AD FS Console (Figure 8), click **Relying Party Trust** in the left pane; the middle pane displays the relying party trusts already configured.

   b. Double-click the relying party trust that you created for the GroupID Self-Service portal, Wizard. This launches the Properties dialog box for the relying party trust.

c. Click the **Endpoints** tab and confirm that the binding type is POST.

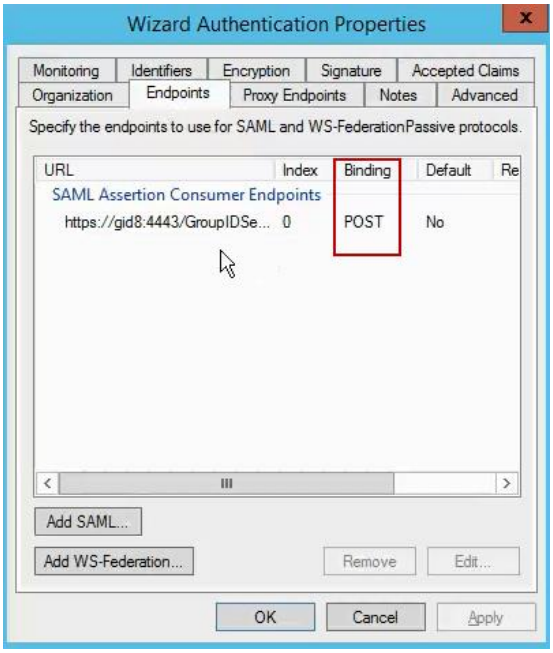


Figure 39: Endpoints tab

4. In AD FS, we configured an Active Directory attribute that the identity provider will use for authenticating users (Figure 22). In our example, we used the UPN attribute that stores the user principal name. Now in the **Advanced** section (Figure 38), we have to refer to this attribute.

   In the **Identity Location** list, select the **identity is an attribute element** option.

5. On selecting the above option, the **Identity Location Attribute** box is displayed.

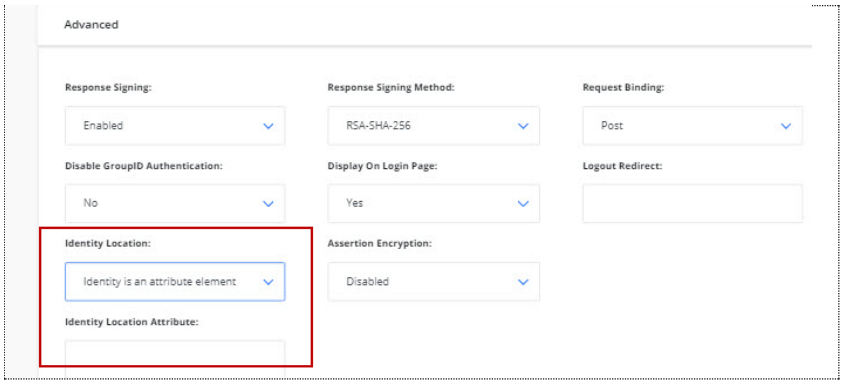


Figure 40: Identity Location Attribute box in Advanced section

The attribute location will be in the form of a URL. Get this URL from AD FS configuration.

a. In AD FS Console (Figure 8), click **Claim Descriptions** in the left pane and then select the Active Directory attribute you specified for authentication, i.e., the UPN attribute.

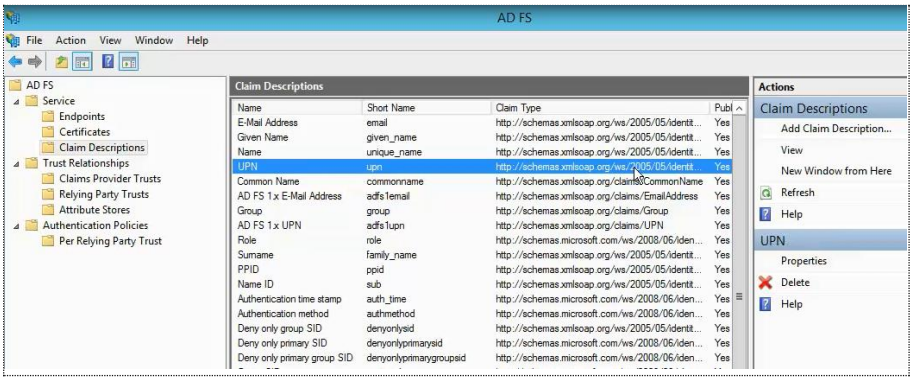


Figure 41: AD FS Console – Claim Descriptions

b. Double-click the attribute to open its properties.

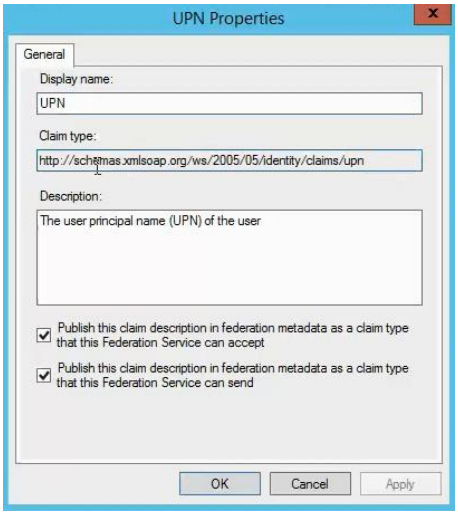


Figure 42: Attribute Properties dialog box

c. Copy the URL displayed in the **Claim type** box. Next, paste it in the **Identity Location Attribute** box in the **Advanced** section (Figure 40).

6. With all configurations completed, click the **Create Provider** button. The identity provider, i.e., AD FS, is created and displayed in the **SAML Identity Providers** grid in the GroupID SSO Admin Panel (Figure 3).

Sign-in using AD FS

We configured the ADS FS provider with the GroupID Self-Service portal, Wizard. For single sign-on using AD FS, we can choose any of the following ways:

- SP-initiated single sign-on: when the SSO operation is initiated from the SP end, i.e., from the Self-Service portal, *Wizard*.
- IdP-initiated single sign-on: when the SSO operation is initiated from the IdP end, i.e., from AD FS.

SP-initiated single sign-on

1. Launch the Self-Service portal, Wizard.

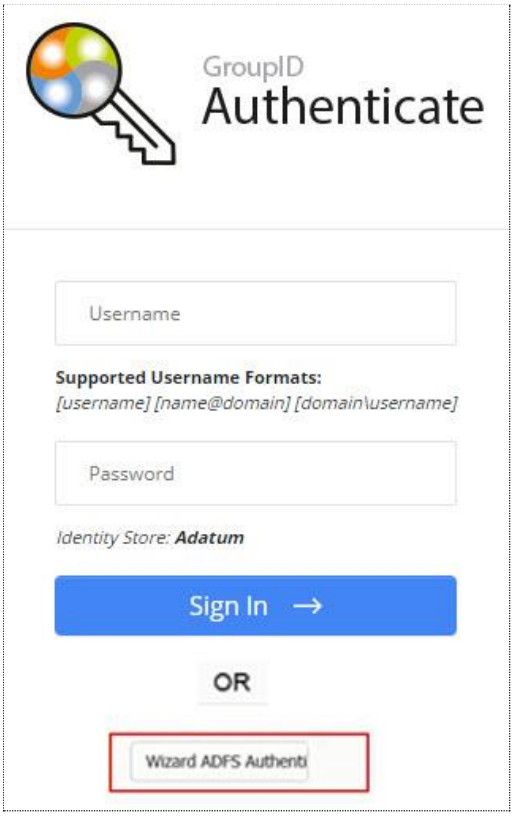


Figure 43: Login page with AD FS button

The availability of the user name and password fields depends on your selection in the **Disable GroupID Authentication** list (see Figure 38).

While creating the AD FS identity provider in GroupID, we did not upload an image using the **Identity Provider Image** box; rather, we chose to provide a name for the ADS FS button (See Upload image for identity provider).

On Wizard's login page, a button for the provider is displayed with the specified name.

2. Click the AD FS button; you will be redirected to the AD FS authentication URL you provided as the IDP login URL.

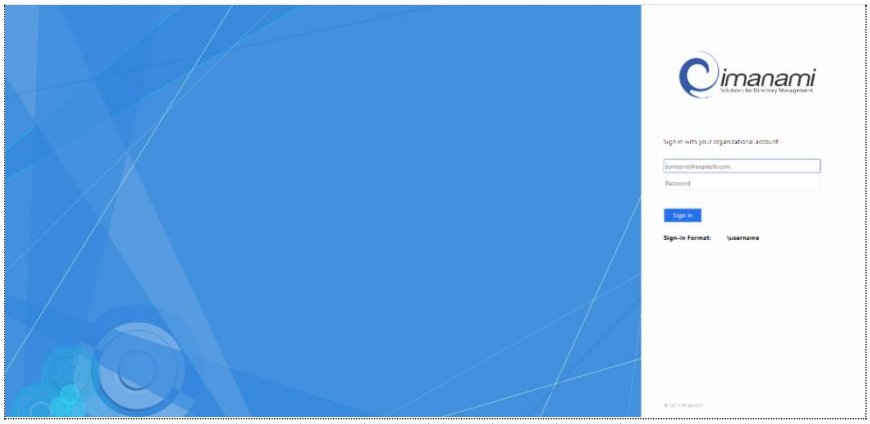


Figure 44: AD FS Sign In page

3. Log in as an Active Directory regular user. On signing in, the authentication is routed to AD FS, that will validate the user with respect to the specified attribute (i.e., user principal name – UPN in our case) and log him or her into the portal.

With single sign-on, you can now launch any GroupID application without having to sign in again.

IdP-initiated single sign-on

1. Launch the ADF FS portal using the URL provided by your organization and log in. The AD FS dashboard will be displayed.

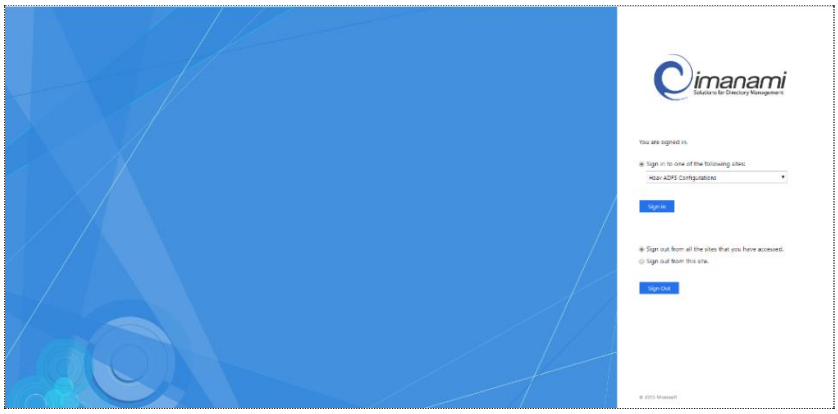


Figure 45: AD FS Dashboard

2. From the **Sign in to one of the following sites** list, select a relying party trust.
   This list contains the relying party trusts configured with AD FS for single sign-on.
3. Click **Sign in**; you will be redirected to it. Authentication will not be required.

Chapter 2 - SAML Configuration for GroupID using Azure AD SSO

Azure AD SSO enables users to conveniently access all their apps from any location, on any device, from a centralized and branded portal for a simplified user experience and better productivity.

In this chapter, we will discuss the configuration of single sign on in GroupID using Azure AD as a provider.

Generate Consumer URL

The consumer URL is unique for each GroupID module (referred to as 'application' here). In GroupID Single Sign-On Admin Panel, generate the consumer URL for the GroupID application with which you want to configure Azure AD SSO. Provide this URL while configuring the GroupID application in Azure AD.

1. Launch the GroupID Single Sign on Admin Panel (Figure 3) and click **Generate URL**. The **Generate URLs** page (Figure 6) is displayed.
2. In the **Select Client to Generate Consumer URL** list, select a GroupID application with which you want to set up Azure AD SSO for single sign-on.

   This list contains all GroupID applications, namely

   - Automate
   - Management Shell
   - All Self-Service and Password Center portals created using GroupID

   As an example, let's select the Self-Service portal named *SSO Hub*.
3. The URL displayed in the **Consumer URL** box is a unique identifier for the selected application. It is used while configuring the *SSO* Hub portal in Azure AD. Click  to copy this URL. Paste it in a file, preferably a text file, to save it.

1. On upgrade to GroupID 10 SR2, you must generate the consumer URL again for the GroupID client configured with Azure AD SSO, and update it in Azure AD SSO.

2. If you lose the SQL server or the GroupID server, you will have to configure the provider again.

Generate Entity ID/Audience URL

The audience URL is unique for each GroupID module (referred to as 'application' here). In GroupID Single Sign-On Admin Panel, generate the audience URL for the GroupID application with which you want to configure Azure AD SSO. Copy this URL and provide it while configuring GroupID in Azure AD.

1. In GroupID Single Sign-On Admin Panel (Figure 3), click the **New Provider** button to add a new provider. The **Add New SAML Provider** page (Figure 7) is displayed.
2. In the **Client** list, select the GroupID application with which you want to set up the SAML provider.

   This list contains all GroupID applications, namely

   - Automate
   - Management Shell
   - All Self-Service and Password Center portals created using GroupID

   The application you select must be the one for which you generated the consumer URL on the **Generate URLs** page (Figure 6).

   To continue with the example, select the Self-Service portal named *SSO Hub* in the **Client** list.
3. Make sure you select an identity store that is linked with the *SSO Hub* portal.
4. The **Entity ID/Audience** box displays a URL that serves as the application ID. Click  to copy it. Paste it in a file, preferably a text file, to save it.

Configure GroupID in Azure AD for SSO

1. Sign into the Azure AD portal.
2. Go to **Azure Active Directory > Enterprise Applications** and add a new application.

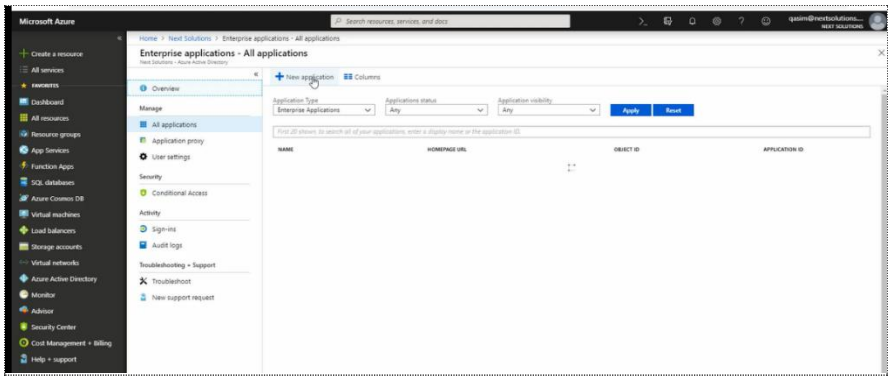


Figure 46: Azure AD Portal – Enterprise Applications page

3. In the **Add your own app** area, select **Non-Gallery application** and enter a name for it in the **Name** box (for example, Azure SSO). Then click **Add**.

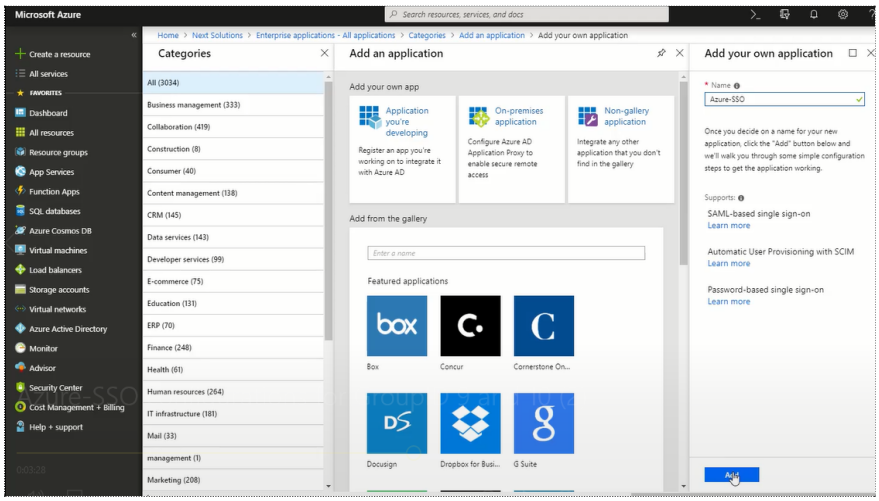


Figure 47: Add an Application page

On adding an application, the portal displays an **Overview** page for it.

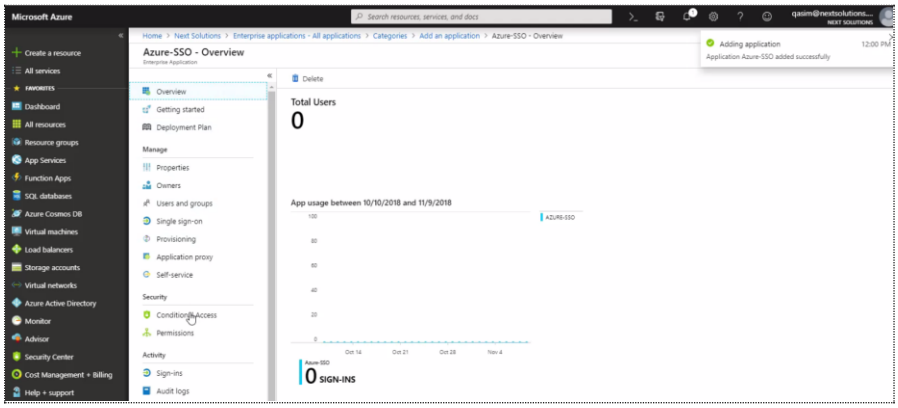


Figure 48: Application Overview page

4. Click **Properties** in the left pane to navigate to its properties.

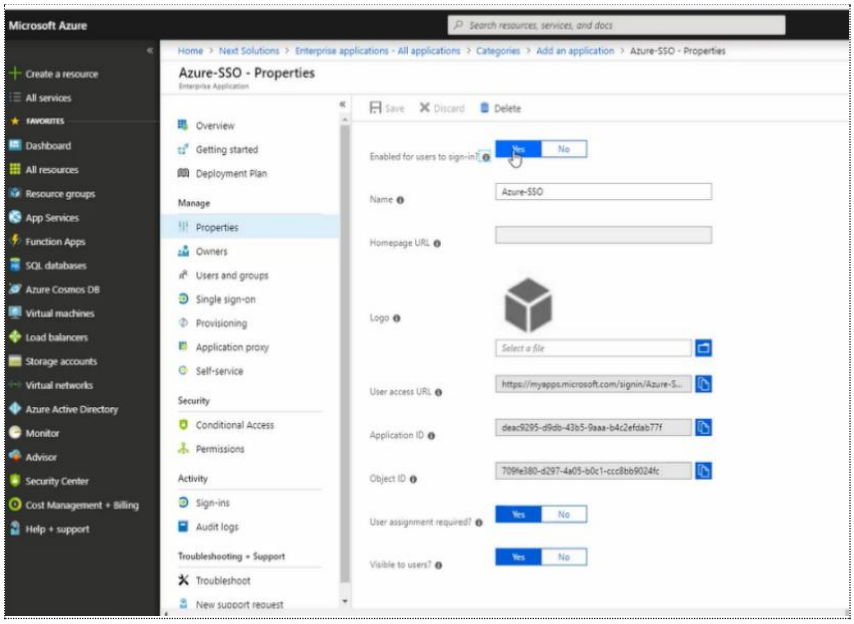


Figure 49: Application Properties page

5. Make sure the application is enabled so that users can sign in. For this, the **Enabled for Users to sign in** option should be set to **Yes.**

6. The **Name** box displays the application name.

   You can change the application logo. Your application is displayed with the logo in the Access Panel Applications.

7. Make sure **User assignment required** is enabled. We will be assigning users manually, who would be able to log into the GroupID Self-Service portal, *SSO Hub*, using Azure AD SSO.

Assign owners to the application:

8. Click **Owners** in the left pane and assign one or more users as owners of the application. For example, you can specify your service account as an owner.

   Click **Add** and search the user(s) you want to assign as owners.

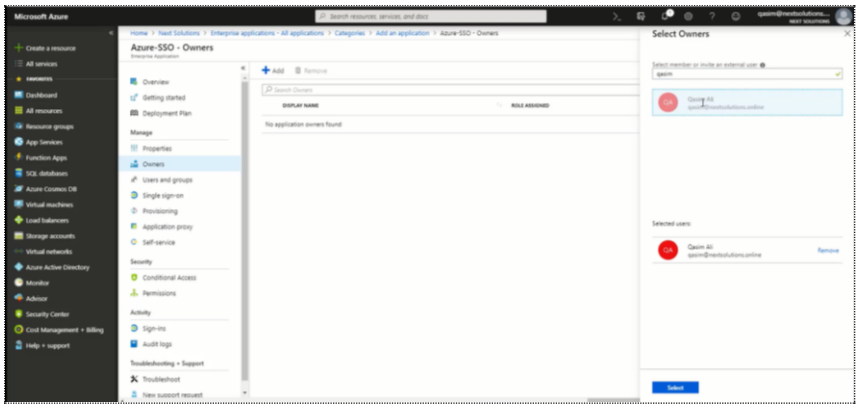


Figure 50: Application Owners page

Assign users to log into GroupID using Azure AD SSO:

9. The next step is to assign users who can log on to the Self-Service portal, *SSO Hub*, using Azure AD SSO. You can specify users and groups.

   Go to **Users and Groups** in the left pane. Search for your required user or group, select it and click **Assign.**

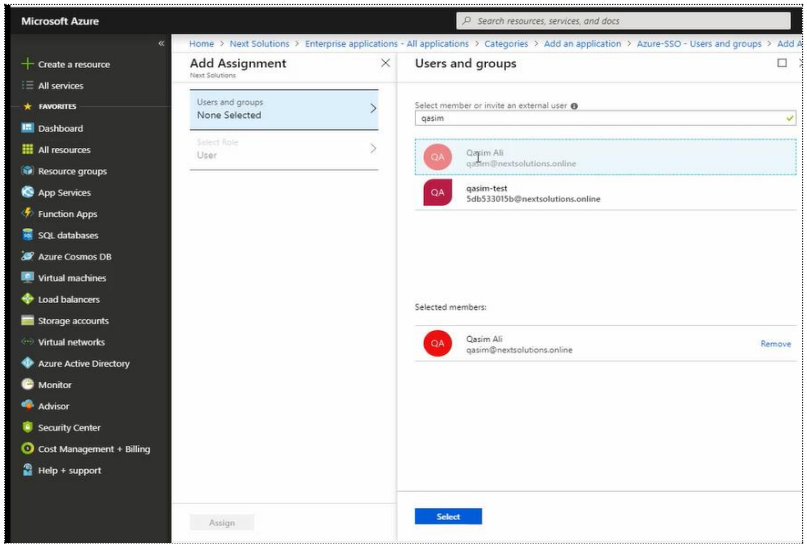


Figure 51: Users and Groups page

SAML SSO configurations for the application

1. Go to **Single Sign On** in the left pane (Figure 50). It displays different methods that Azure AD provides for single sign on. Select **SAML** as GroupID 9 and 10 support SAML 2.0.

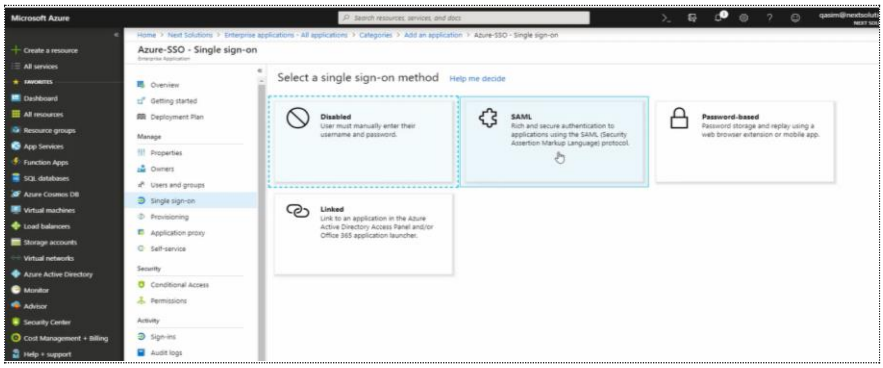


Figure 52: Azure-SSO - Single Sign-on

The following page is displayed, where you have to set single sign-on options for GroupID.

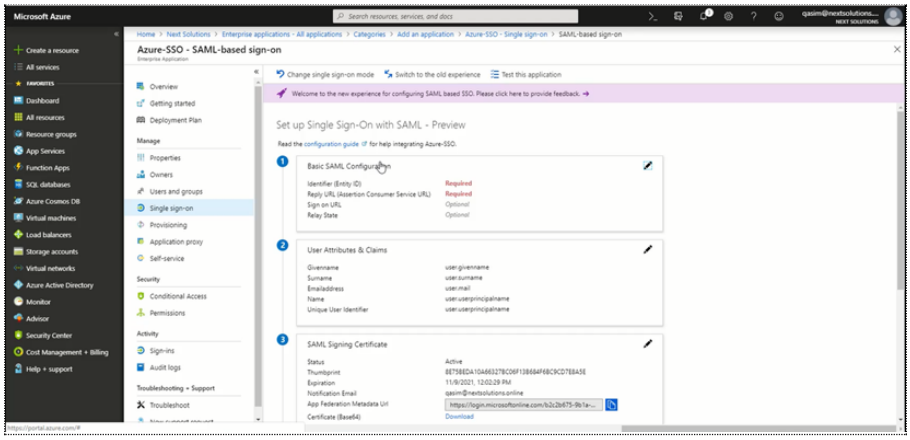


Figure 53: SAML-based sign-on settings page

2. On the **Basic SAML Configuration** card, click **Edit** ( ).

Figure 54: Basic SAML Configuration dialog box

3. Provide the Entity ID and Consumer URL that you copied earlier.

   After adding the information, click **Save**.

4. The **User Attributes and Claims** card (Figure 53) displays the attributes used for logging in. Let's keep the defaults.

5. On the **SAML Signing Certificate** card, download Certificate (Base64).

Configure the Azure AD SSO application in GroupID

1. In GroupID Single Sign-On Admin Panel (Figure 3), click the **New Provider** button to add a new provider. The **Add New SAML Provider** page (Figure 7) is displayed.

2. Assign a name to the provider, for example, Azure AD SSO.

3. Open the Certificate (Base64) file that you downloaded from the Azure AD portal and copy the certificate information.

   On the **Add New SAML Provider** page, paste it in the **IDP Certificate** box. Make sure you have not copied any trailing space.

4. In the Azure AD portal, copy the Login URL from the **Set up Azure SSO** card on the **SAML-based sign-on settings** page (Figure 53) and paste it in the **IDP Login URL** box on the **Add New SAML Provider** page.

5. Again, copy the Azure AD Identifier URL from the **Set up Azure SSO** card on the **SAML-based sign-on settings** page and paste it in the **Issuer** box on the **Add New SAML Provider** page.

Advanced settings:

6. Click **Advanced** on the **Add New SAML Provider** page (Figure 7).

   The **Advanced** section is displayed, as shown in Figure 78.

7. Select *Post* in the **Request Binding** drop-down list.

8. The **Disable GroupID Authentication** option indicates whether to display the GroupID authentication login on the *SSO Hub* portal's login page.

   - By default, 'No' is selected, which means that when users access the *SSO Hub* portal's login page, they will be shown the GroupID login and password option as well as the Azure AD SSO provider's button.
   - Selecting 'Yes' means that the GroupID login and password option will not be available on the *SSO Hub* portal's login page.

     Moreover, when a single identity store and a single SAML provider is configured, the login page for the provider (Figure 56) is displayed rather than the *SSO Hub* portal's login page.

9. Click **Create Provider** to complete the configuration.

   The new provider is listed on the **GroupID Single Sign On Admin Panel** (Figure 3).

Sign in using Azure AD SSO

We configured the Azure AD SSO with the GroupID Self-Service portal, *SSO Hub*. For single sign-on using Azure AD SSO, we can choose any of the following ways:

- SP-initiated single sign-on: when the SSO operation is initiated from the SP end, i.e., from the Self-Service portal, *SSO Hub*.
- IdP-initiated single sign-on: when the SSO operation is initiated from the IdP end, i.e., from the Azure AD SSO application.

SP-initiated single sign-on

1. Launch the Self-Service portal, *SSO Hub*.

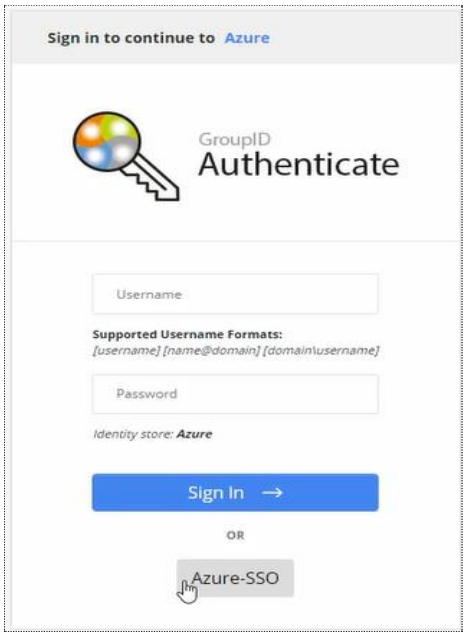


Figure 55: Login page with Azure SSO button

Notice the Azure-SSO button. You can login using your GroupID credentials or click **Azure SSO** to log in.

The availability of the user name and password fields depends on your selection in the **Disable GroupID Authentication** list in the **Advanced** section on the **Add New SAML Provider** page (Figure 7).

2. Click **Azure SSO**; the Microsoft Sign In page is displayed.

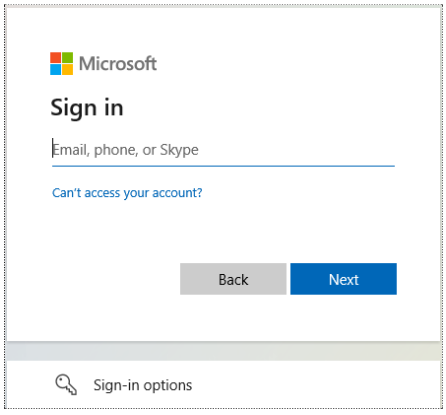


Figure 56: Microsoft Sign In page

3. Enter your credentials and click **Sign In**. You will be routed to the main page of the Self-Service portal, *SSO Hub*.

   Only users defined for our app in Azure AD can log in by entering their user names and passwords. See Assign Users to log into GroupID using Azure AD SSO.

With single sign-on, you can now launch any GroupID application without having to sign in again.

IdP-initiated single sign-on

1. Launch the Microsoft My Apps portal using the following URL and sign in.

   https://myapps.microsoft.com

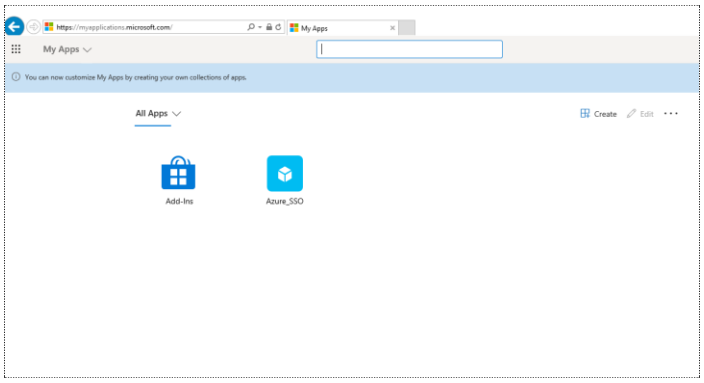


Figure 57: My App Portal

2. Click the **Azure_SSO** app (i.e., the app we created to work with the *SSO Hub* portal for single sign on) and it will redirect you to your portal.

Chapter 3 - SAML Configuration for GroupID using Okta

Okta provides secure identity management and single sign-on to any application, whether in the cloud, on-premises or on a mobile device for the employees in an organization.

In this chapter, we will discuss the configuration of single sign on in GroupID using Okta as a provider.

Generate Consumer URL

The consumer URL is unique for each GroupID module (referred to as 'application' here). In GroupID Single Sign-On Admin Panel, generate the consumer URL for the GroupID application with which you want to configure Okta. Provide this URL while configuring the GroupID application in Okta.

1. Launch the GroupID Single Sign on Admin Panel (Figure 3) and click **Generate URL**. The **Generate URLs** page (Figure 6) is displayed.
2. In the **Select Client to Generate Consumer URL** list, select a GroupID application with which you want to set up Okta for single sign-on.

   This list contains all GroupID applications, namely

   - Automate
   - Management Shell
   - All Self-Service and Password Center portals created using GroupID

   As an example, let's select the Self-Service portal named *OKTA SSO*.
3. The URL displayed in the **Consumer URL** box is a unique identifier for the selected application. It is used while configuring the portal, *OKTA SSO* in Okta. Click  to copy this URL. Then paste it in a file, preferably a text file, to save it.

1. On upgrade to GroupID 10 SR2, you must generate the consumer URL again for the GroupID client configured with Okta and update it in Okta.

2. If you lose the SQL server or the GroupID server, you will have to configure the provider again.

Generate Entity ID/Audience URL

The audience URL is unique for each GroupID module (referred to as 'application' here). In GroupID Single Sign-On Admin Panel, generate the audience URL for the GroupID application with which you want to configure Okta. Copy this URL and provide it while configuring GroupID in Okta.

1. In GroupID Single Sign-On Admin Panel (Figure 3), click the **New Provider** button to add a new provider. The **Add New SAML Provider** page (Figure 7) is displayed.
2. In the **Client** list, select the GroupID application with which you want to set up the SAML provider.

   This list contains all GroupID applications, namely

   - Automate
   - Management Shell
   - All Self-Service and Password Center portals created using GroupID

   The application you select must be the one for which you generated the consumer URL on the **Generate URLs** page (Figure 6).

   To continue with the example, select the Self-Service portal named *OKTA SSO* in the **Client** list.
3. The **Entity ID/Audience** box displays a URL that serves as the application ID. Click  to copy it.

Configure GroupID in Okta

1. Launch Okta.

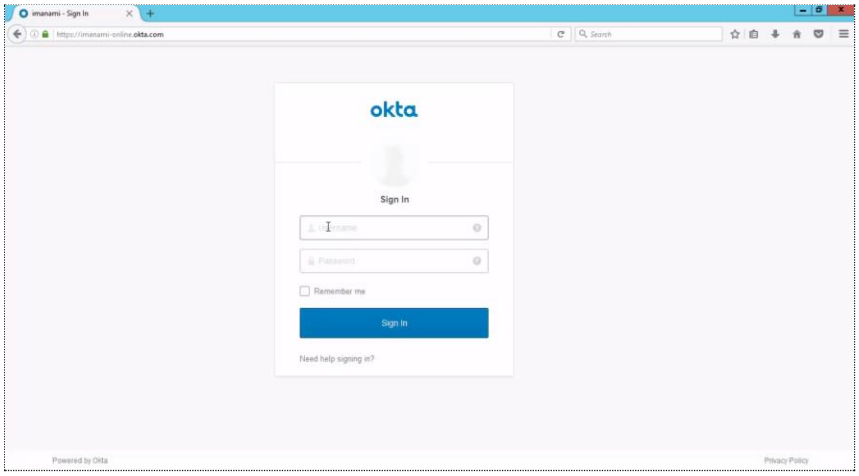


Figure 58: Okta login page

2. This is the provider's login page; use it to sign into Okta.

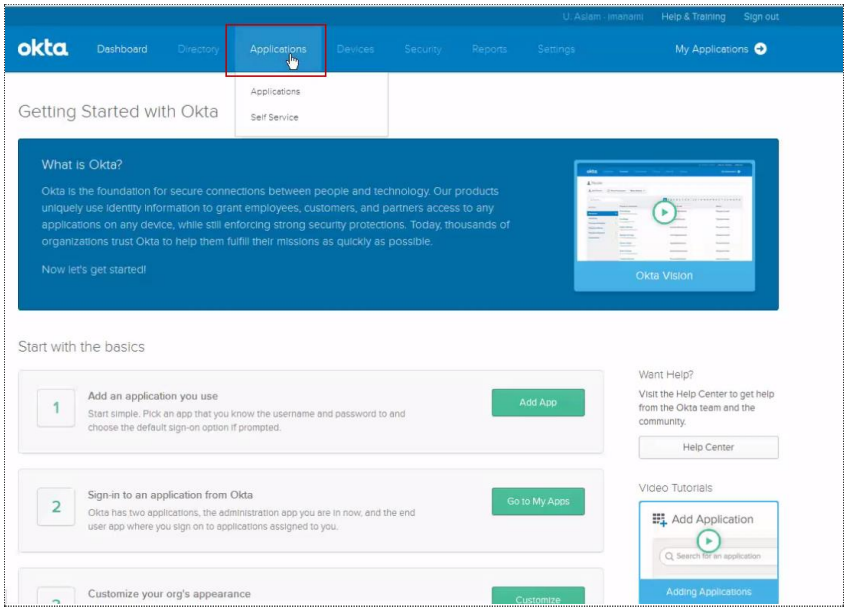


Figure 59: Okta Dashboard

3. This is the dashboard for OKTA. To configure the GroupID application *OKTA SSO*, click **Applications** in the blue bar at the top.

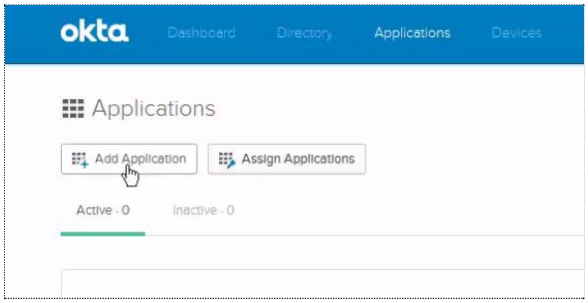


Figure 60: Applications page

4. Click the **Add Application** button.

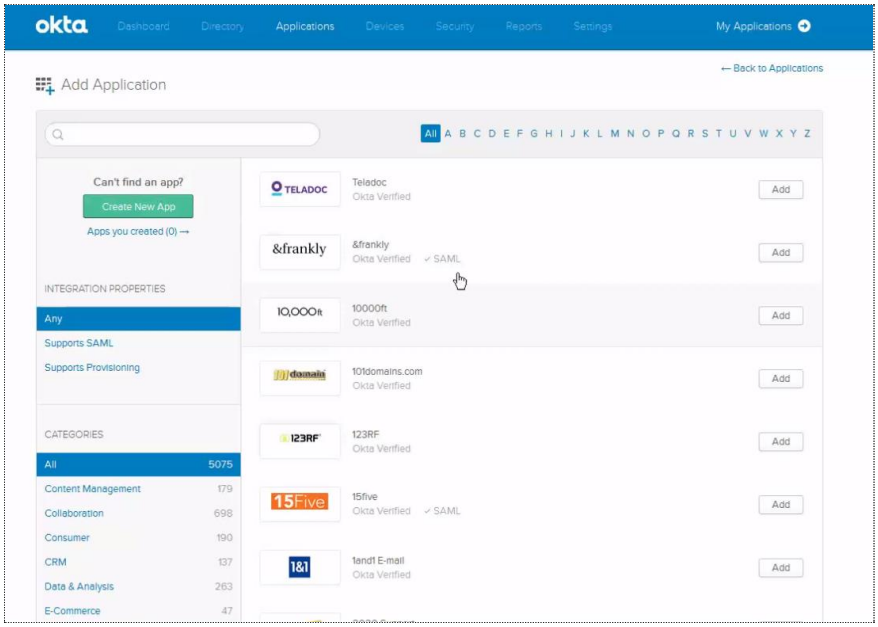


Figure 61: Add Application page

5. This page displays the preconfigured options available. Click the **Create New App** button.

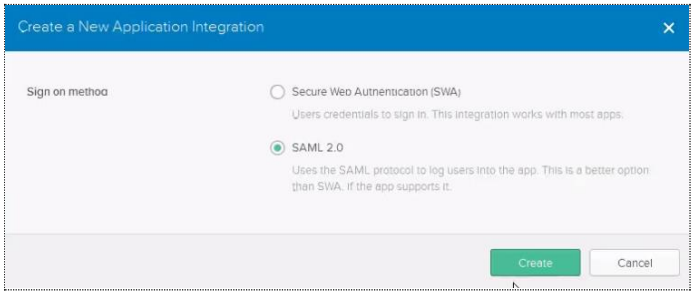


Figure 62: Create a New Application Integration dialog box

6. Select the **SAML 2.0** option button and click **Create**.

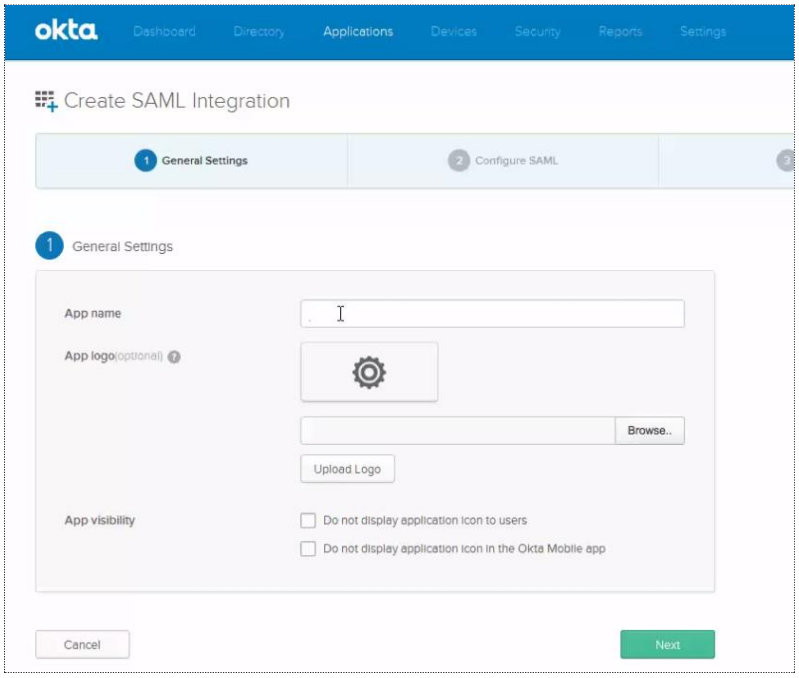


Figure 63: Create SAML Integration page

7. In the **App name** box, provide a user-friendly name for the app, for example, GroupID Okta Sign-On.
8. You can choose to upload a logo for the GroupID app. This logo will be displayed on the Okta dashboard (Figure 81).

   Every SAML provider has a user dashboard. Hence, when a user logs in to Okta, he or she will be redirected to the dashboard that may have GroupID and other applications listed for single sign-on.
9. Click **Next** to proceed to the next step.

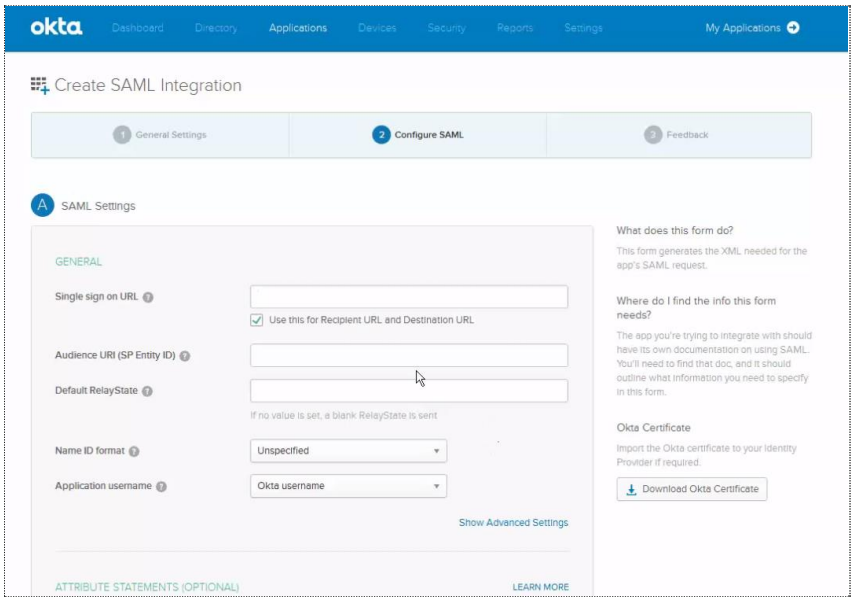


Figure 64: Create SAML Integration page (2)

10. In the **Single sign on URL** box, paste the consumer URL that you generated for the GroupID application, *OKTA SSO* (see Generate Consumer URL on page 38).
11. In the **Audience URI (SP Entity ID)** box, provide the audience URL. Fetch this URL from the **Entity ID Audience** field on the **Add New SAML Provider** page (see Generate Entity ID/Audience URL on page 40).
12. We will not specify any default relay state, so leave the **Default Relay State** field blank.
13. Leave the **Name ID format** selected to 'Unspecified'.
14. In the **Application username** list, make sure that the 'Okta username' option is selected. This implies that only users defined in Okta can authenticate on the Self-Service portal, *OKTA SSO* using the Okta single sign-on option.

    See Configure users in Okta on page 48.
15. Additional options include attribute statements within the Okta provider.

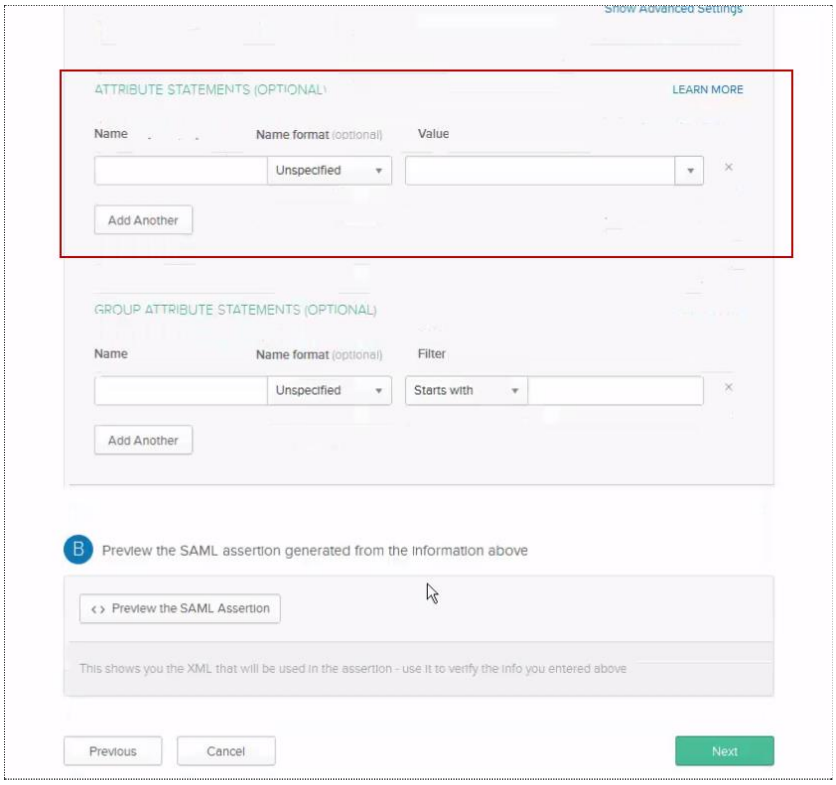


Figure 65: Create SAML Integration page (3)

The **Attribute Statements** area is for specifying an attribute that will be used to authenticate users who will be signing into GroupID using the Okta. Hence, this attribute is meant for user identification.

Skip this section and leave the selections to default. The Okta provider would authenticate users on the basis of the username.

16. Click **Next**.

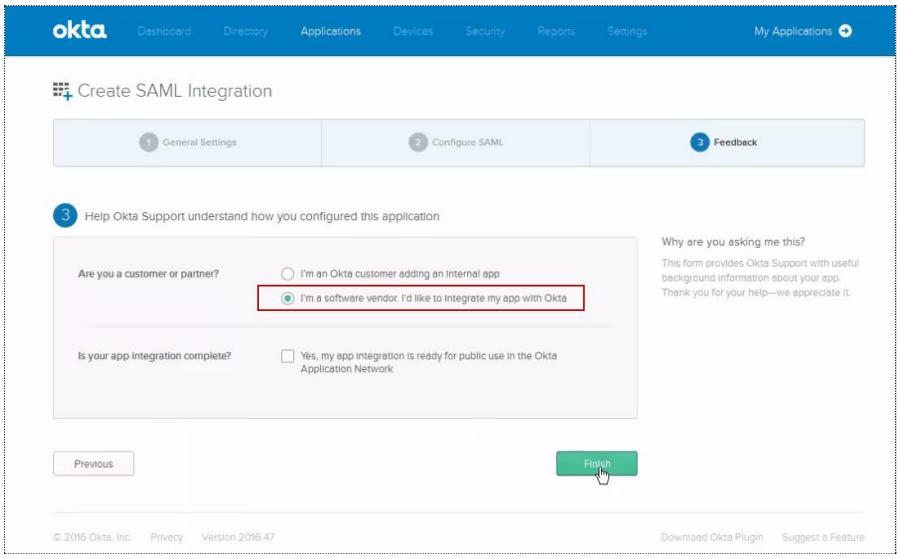


Figure 66: Create SAML Integration page (4)

17. Select the option, **I'm a software vendor. I'd like to integrate my app with Okta** and click **Finish**.

With this, the GroupID OKTA SSO app is successfully added in Okta, and the **Sign-On Settings** page for the new app is displayed as follows:

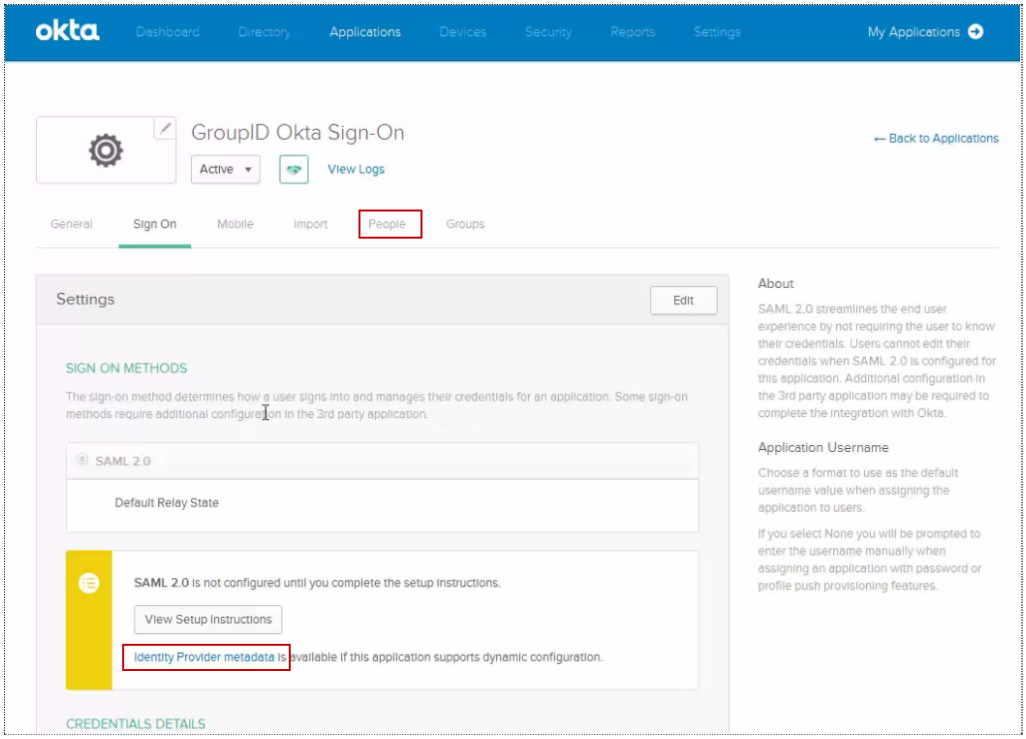


Figure 67: Sign-On Settings page

Download Okta metadata file

You can download a metadata file from Okta and import it into GroupID to configure the Okta provider in GroupID.

1. To download the metadata file, click the **Identity Provider metadata** link on the **Sign-On Settings** page (Figure 67).

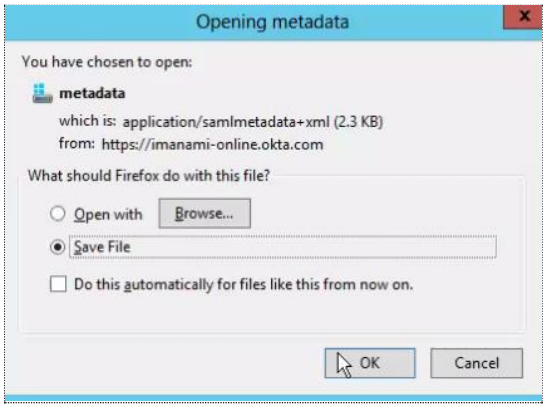


Figure 68: Opening metadata dialog box

2. Make sure that the **Save File** option is selected and click **OK**. The file downloads and the following dialog box is displayed.

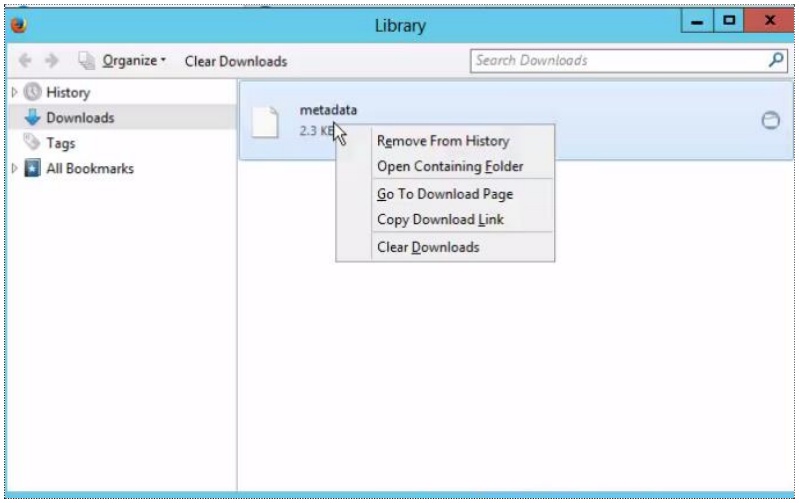


Figure 69: Library dialog box

3. Right-click the metadata file and select the **Open Containing Folder** option on the shortcut menu.

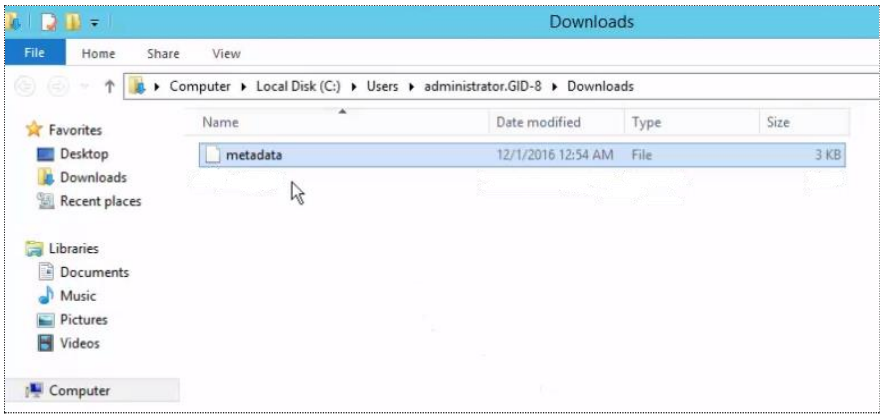


Figure 70: Downloads page

4. Either copy the metadata file to your desktop for simplicity or save its location, so that you can easily locate it for import into GroupID.

Importing the Okta metadata file into GroupID will bring in all the configurations for this provider within the SAML provider setup in GroupID.

Configure users in Okta

You must define users in Okta. Only these users can authenticate on the GroupID Self-Service portal, OKTA SSO using Okta. (See Sign-in using Okta on page 53.)

1. Click the **People** tab (Figure 67).

Figure 71: People page

Right now, no user is added here. There are multiple ways to define users in Okta, such as:

- Add users manually.
- Use a CSV file to import users.
- Use the Active Directory tool provided by Okta (that syncs Active Directory users to Okta).

For all of these, if Okta finds an existing user in its own database, it will link the GroupID application, OKTA SSO to the existing account. If not, it will create a new Okta account for the user.

For new users, a password is generated by Okta and sent to them by email.

2. To create users manually or to import them into Okta, visit https://help.okta.com/en/prod/Content/Topics/Directory/Directory_People.htm.

   To use an Active Directory tool for adding users, see https://help.okta.com/en/prev/Content/Topics/Directory/Directory_Directory_Integrations.htm?cshid=Directory_Directory_Integrations#Directory_Directory_Integrations.

3. After defining users, you must manually add these users.

   Click **People** to go to the **People** page (Figure 71). Click the **Assign to People** button to add users here.

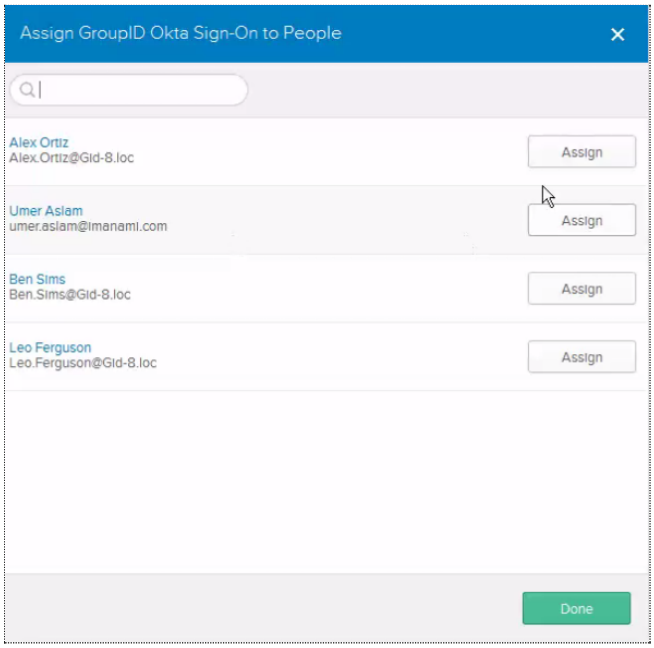


Figure 72: Assign GroupID Okta Sign-On to People dialog box

4. Click **Assign** against a user so that they can authenticate on the Self-Service portal, *OKTA SSO* using Okta.

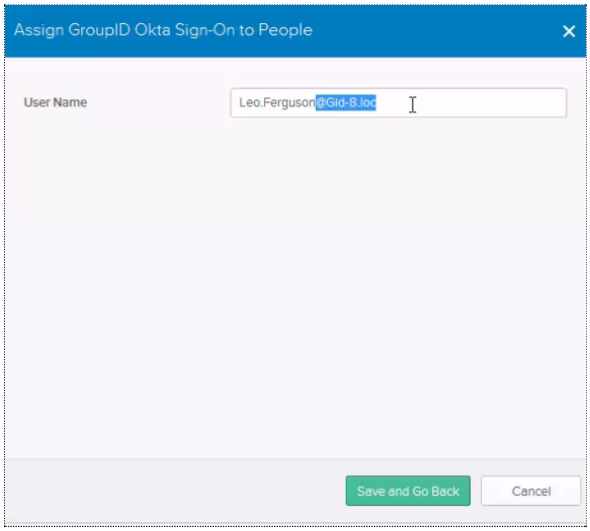


Figure 73: Assign GroupID Okta Sign-On to People dialog box (2)

   a. Remove the domain after the user's name, i.e., the part starting with '@'. After removing the domain, we are left with the user name. The user will use this name to authenticate on the portal, *OKTA SSO* using Okta.

   b. Click **Save and Go Back**.

5. Repeat step 4 for all the required users and then click **Done** on the **Assign GroupID Okta Sign-On to People** dialog box (Figure 72).

   The users will be displayed on the **People** page.

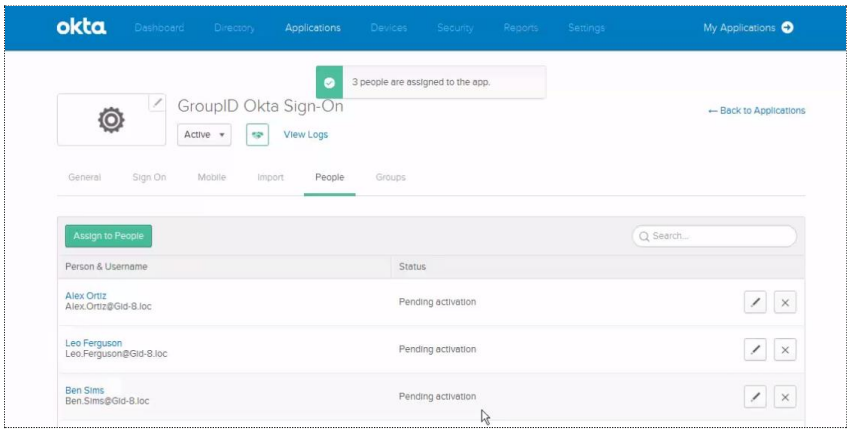


Figure 74: People page with users added

6. The next step is to activate the user accounts. Click the **Directory** link in the blue bar at the top.

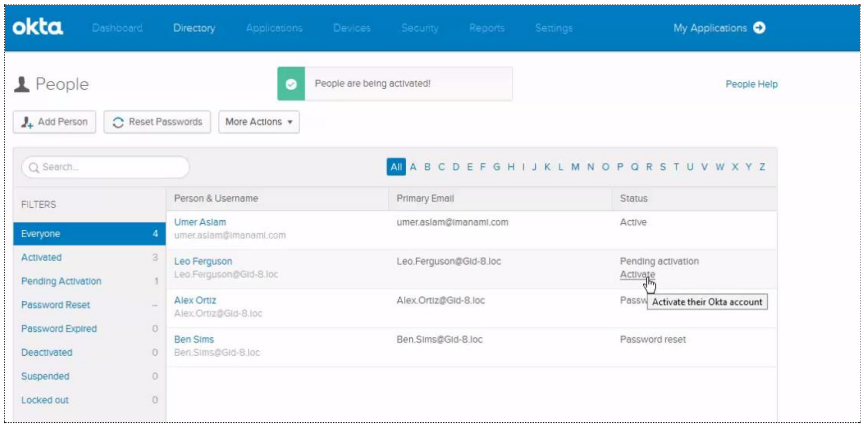


Figure 75: Directory page

7. Click the **Activate** link for the required user.

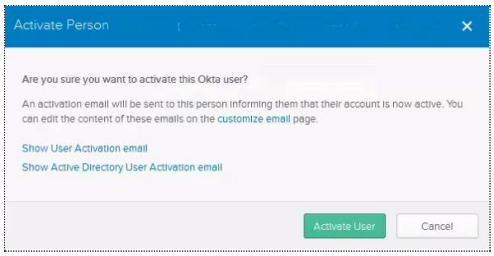


Figure 76: Activate Person dialog box

8. Click **Activate User**.

With this, we have successfully configured users within the Okta provider.

Configure the Okta provider in GroupID

While creating the Okta provider in GroupID SSO Admin Panel, you simply have to import the Okta metadata file to configure all settings for this identity provider.

1. In GroupID SSO Admin Panel, go to the **Add New SAML Provider** page (Figure 7) and make sure *OKTA SSO* is selected in the **Client** list.

   (*OKTA SSO* is the GroupID application for which we generated the audience URL, to set up Okta with it.)

2. To import the Okta metadata file, click the **Import from Metadata** button under the **Advanced** section; the following dialog box is displayed:

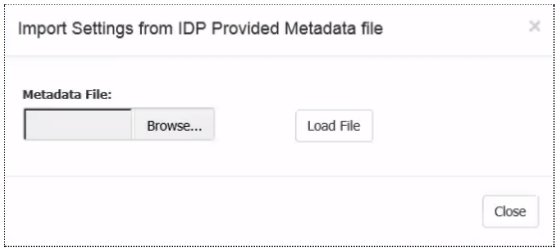


Figure 77: Import Settings from IDP provided Metadata File dialog box

3. Click **Browse** to select the Okta metadata file you downloaded earlier (see Download Okta metadata file on page 47).
4. Then click **Load File**. With this, fields on the **Add New SAML Provider** page (Figure 7) are automatically filled in.
5. When Okta is configured with the GroupID application, *OKTA SSO*, it will be available on *OKTA SSO*'s login page for single sign-on. You can choose to display the Okta authentication option as an image or a button.

   - To display the Okta option as an image, you have to upload an image for the identity provider.

     On the **Add New SAML Provider** page (Figure 7), use the **Browse** button next to the **Identity Provider Image** box to upload an image for Okta.

     Supported image formats are: .jpg, .bmp, .png, and .gif. Required dimensions for the image file are: 210 x 60 pixels.

   OR

   - If you do not want an image, Okta authentication will be shown as a button.

     Specify a name for the button in the **Name** box.

   Users can click the image or the button on the login page of the Self-Service portal, *OKTA SSO* (Figure 79) and authenticate using the Okta single sign-on process.

6. To make advanced configurations, click **Advanced** to expand the **Advanced** section.

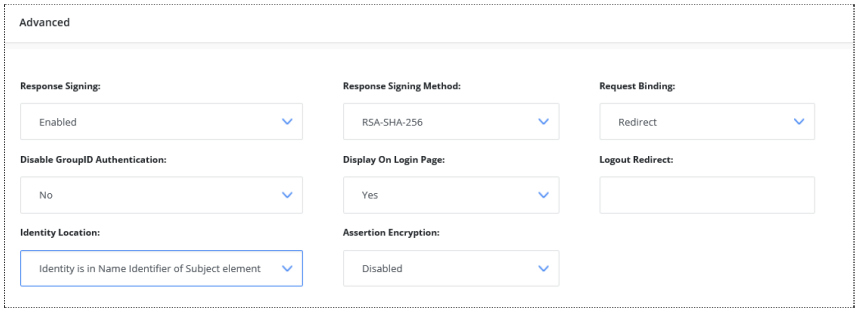


Figure 78: Advanced section

7. Leave all settings to default.
8. The **Disable GroupID Authentication** option indicates whether to display the GroupID authentication login on the *OKTA SSO* portal's login page (Figure 79).
    - By default, 'No' is selected, which means that when users access the *OKTA SSO* portal's login page, they will be shown the GroupID login and password option as well as the Okta identity provider's button.
    - Selecting 'Yes' means that the GroupID login and password option will not be available on the *OKTA SSO* portal's login page.

      Moreover, when a single identity store and a single SAML provider is configured, the login page for the provider is displayed rather than the *OKTA SSO* portal's login page. (The Okta login page is as shown in Figure 80.)
9. Click **Create Provider** to complete the configuration.

The identity provider is created and displayed in the **SAML Identity Providers** grid in the GroupID SSO Admin Panel (Figure 3).

Sign-in using Okta

We configured the Okta provider with the GroupID Self-Service portal, *OKTA SSO*. For single sign-on using Oklta, we can choose any of the following ways:

- SP-initiated single sign-on: when the SSO operation is initiated from the SP end, i.e., from the Self-Service portal, *Okta SSO*.
- IdP-initiated single sign-on: when the SSO operation is initiated from the IdP end, i.e., from Okta.

SP-initiated single sign-on

1. Launch the Self-Service portal, *Okta SSO*.

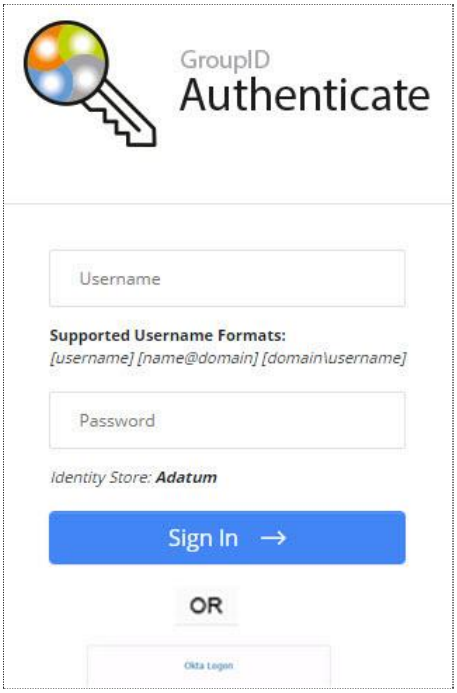


Figure 79: Login page with Okta button

The availability of the user name and password fields depends on your selection in the **Disable GroupID Authentication** list (see Figure 78).

2. Click the **Okta Logon** link; the Okta Sign In page is displayed.

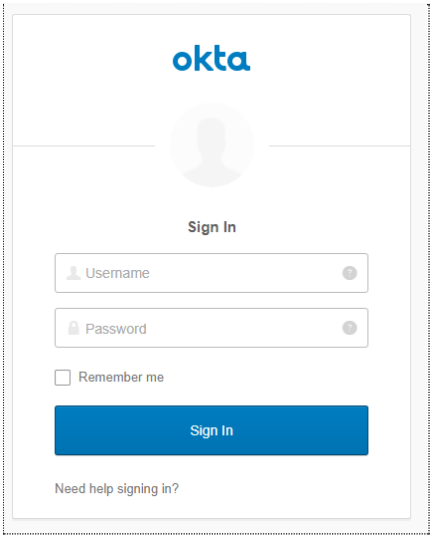


Figure 80: Okta Sign In page

3. Enter your credentials and click **Sign In**. You will be routed to the main page of the Self-Service portal, *Okta SSO*.

   Only users defined for our app in Okta can log in by entering their user names and passwords. See Configure users in Okta on page 48.

With single sign-on, you can now launch any GroupID application without having to sign in again.

IdP-initiated single sign-on

1. Launch the Okta portal using the URL provided by your organization and log in. The Okta dashboard is displayed.

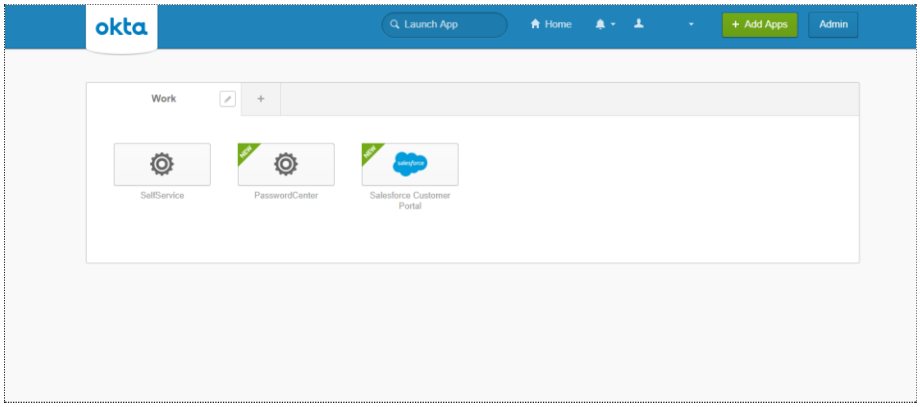


Figure 81: Okta Dashboard

   This page displays the apps configured with Okta for single sign-on.

2. On clicking an app, you will be redirected to it. Authentication will not be required.

Chapter 4 - SAML Configuration for GroupID using PingOne

PingOne is an Identity as a Service (IDaaS) solution that enables organizations to deliver single sign-on with just one username and password.

In this chapter, we will discuss the configuration of single sign on in GroupID using PingOne as a provider.

Generate GroupID metadata file

In GroupID SSO Admin Panel, you can generate a metadata file for the GroupID application with which you want to set up the PingOne identity provider.

When you import this file into PingOne, it populates all GroupID-related configurations into the provider.

Getting the metadata file is a two-step process:

- Generate the consumer URL for the GroupID application you want to set up the PingOne identity provider with
- Download the metadata file

Generate Consumer URL

The consumer URL is unique for each GroupID module (referred to as 'application' here). In GroupID Single Sign-On Admin Panel, generate the consumer URL for the GroupID application with which you want to configure PingOne. Provide this URL while configuring the GroupID application in PingOne.

1. Launch the GroupID Single Sign on Admin Panel (Figure 3) and click **Generate URL**. The **Generate URLs** page (Figure 6) is displayed.
2. In the **Select Client to Generate Consumer URL** list, select a GroupID application with which you want to set up PingOne for single sign-on.

   This list contains all GroupID applications, namely

   - Automate

- Management Shell
- All Self-Service and Password Center portals created using GroupID

As an example, let's select the Self-Service portal named *Enterprise*.

3. The URL displayed in the **Consumer URL** box is a unique identifier for the selected application. It is used to define the link of our application (i.e., the *Enterprise* portal) within the provider (i.e., PingOne). Click to copy this URL. Then paste it in a file, preferably a text file, to save it.

1. On upgrade to GroupID 10 SR2, you must generate the consumer URL again for the GroupID client configured with PingOne, and update it in PingOne.
2. If you lose the SQL server or the GroupID server, you will have to configure the provider again.

Download metadata file

Use the **Metadata** section on the **Generate URLs** page (Figure 6) to generate the metadata file for the GroupID application with which you want to set up PingOne for single sign-on.

Since we generated the consumer URL for the *Enterprise* portal, we should generate the metadata file for this same portal.

1. In the **Client** list, select *Enterprise*.
2. Select the relevant identity store in the **Identity Store** list.

   Users will be authenticated in this identity store when they use PingOne for single sign-on.

3. Click to download the metadata file on your machine.

Configure GroupID in PingOne

1. Launch the PingOne Identity dashboard. It is as follows:

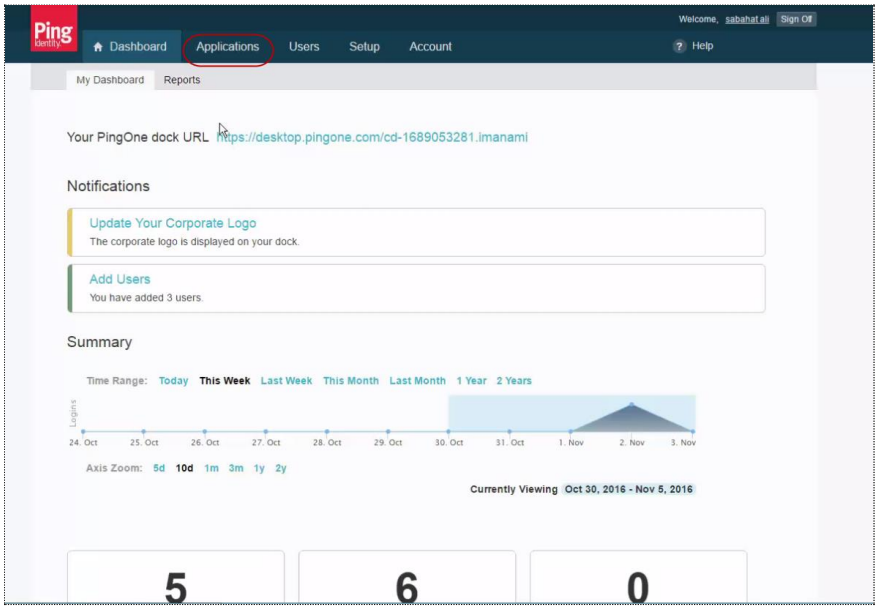


Figure 82: PingOne Identity Dashboard

2. Click the **Applications** tab.

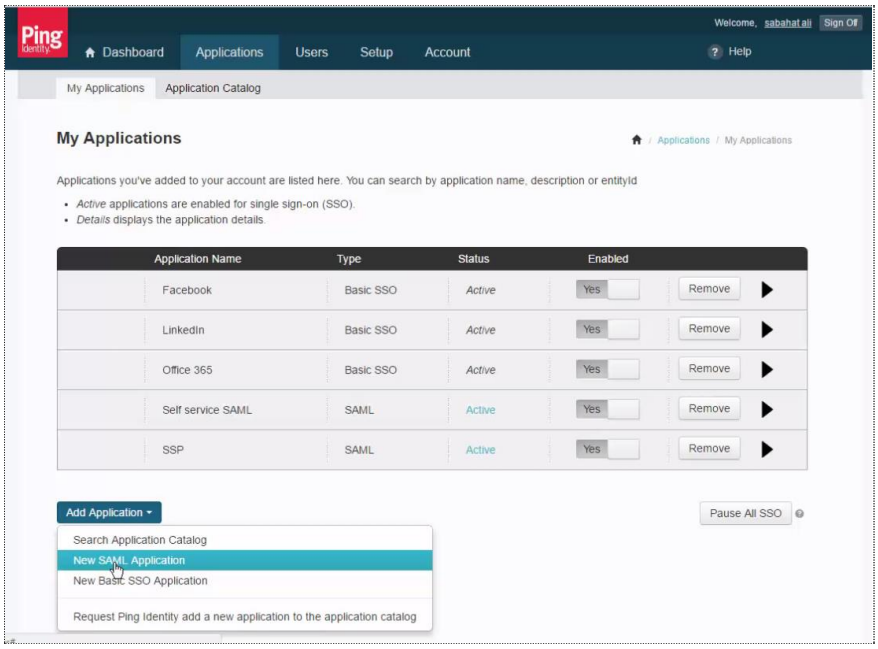


Figure 83: Applications tab

3. Click **Add Application** and select the **New SAML Application** option to configure the GroupID application, *Enterprise*, in PingOne.

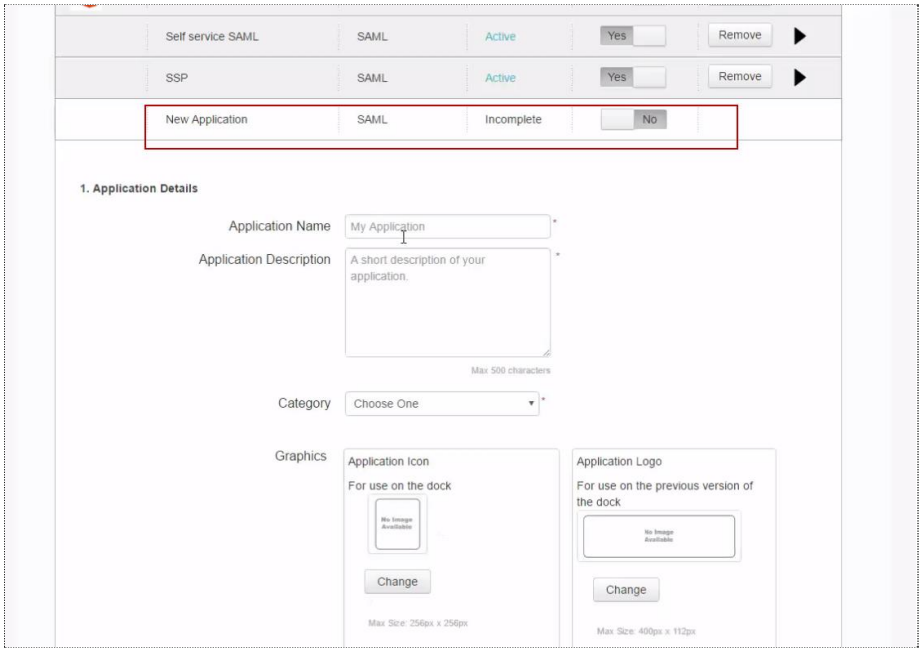


Figure 84: Application Details page

The new application is added to the grid and the **Application Details** section is displayed.

4. In the **Application Name** box, provide a friendly name for the application. For example, *Imanami GroupID App1*.

5. In the **Application Description** box, you can specify the GroupID application with which you want to set up PingOne for single sign-on. In our example, it is the Self-Service portal, *Enterprise*.

6. You can choose to upload an image for the GroupID app. This image will be displayed on the PingOne dashboard.

   Every SAML provider has a user dashboard. Hence, when a user logs in to PingOne, he or she will be redirected to the dashboard that may have GroupID and other applications listed for single sign-on.

7. Select an option from the **Category** list, for example, *Information Technology*.

   This section will appear as:

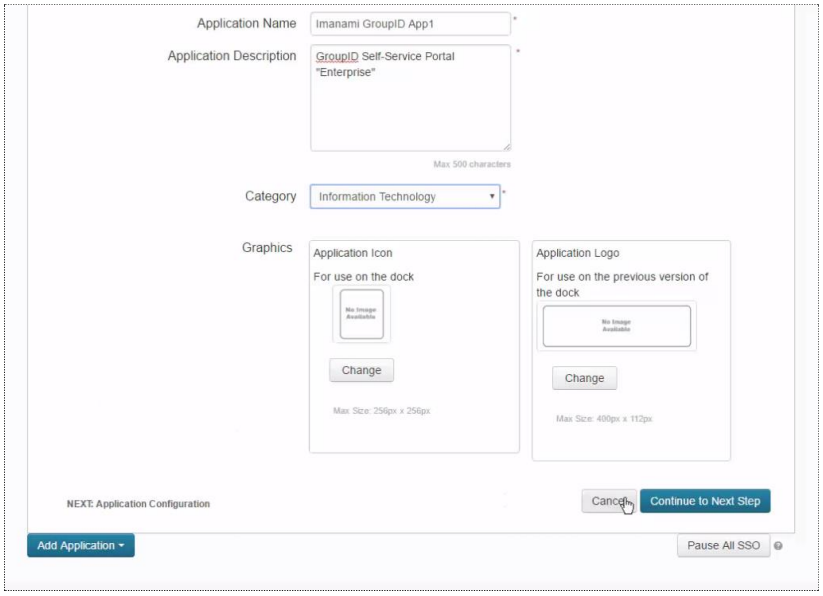


Figure 85: Application Details page (2)

8. Click the **Continue to Next Step** button.

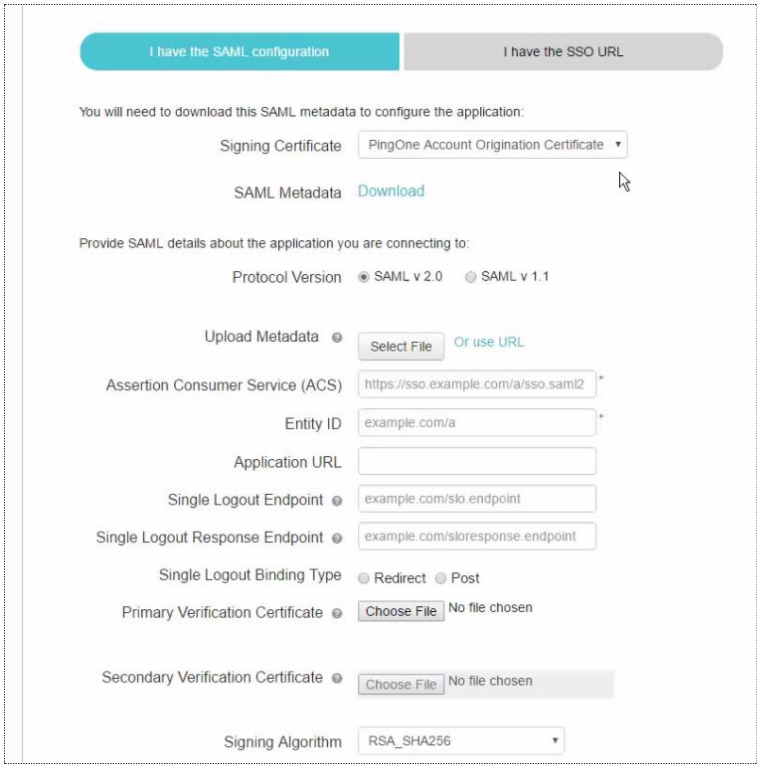


Figure 86: SAML Configurations page

9. Use the metadata file you generated for the *Enterprise* portal in GroupID Admin Panel to configure certain settings on this page.

   (See Generate GroupID metadata file on page 56.)

   Click the **Select File** button next to the **Upload Metadata** label. Simply select the metadata file and it will be uploaded, thereby bringing in the required settings to configure the GroupID application, *Enterprise*, within PingOne.

   For example, the **Entity ID** box is populated with the required URL.

10. In the **Application URL** box, copy the same URL as displayed in the **Assertion Consumer Service (ACS)** box.

11. Select the *Post* option button for the **Single Logout Binding Type**.

12. In the **Signing Algorithm** list, select the RSA_SHA256 bit encryption option.

    GroupID currently supports the following options:

    - RSA_SHA1
    - RSA_SHA256

13. Click the **Download** link next to the **SAML Metadata** label to download the metadata file from the PingOne identity provider.

    While creating the PingOne provider in GroupID, you can import this file to being in all the configurations for PingOne within the identity provider setup in GroupID.

14. No further configurations are required on this page. Scroll down and click the **Continue to Next Step** button.

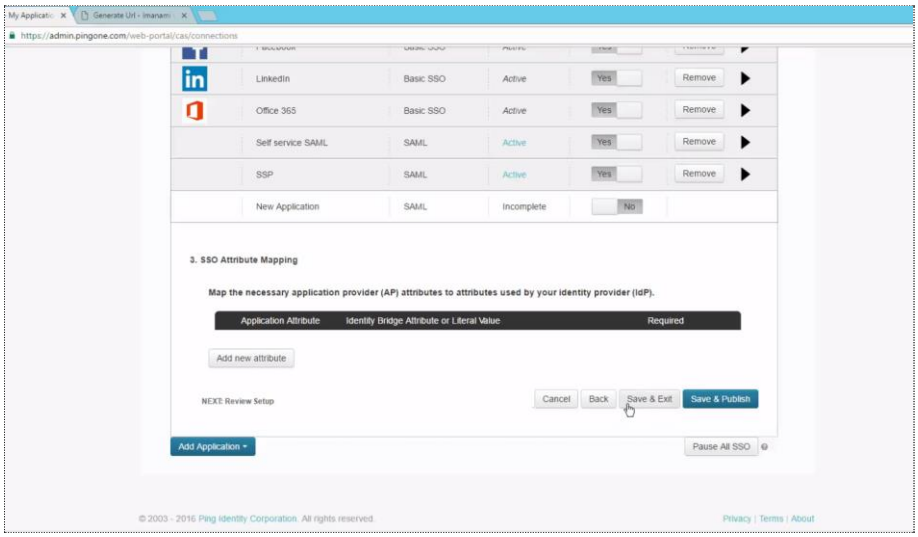


Figure 87: SSO Attribute Mapping page

Attribute mapping in PingOne

The next step is to specify an attribute that will be used to authenticate users who will be signing into GroupID using the PingOne single sign-on facility.

Hence, this attribute is meant for user identification.

1. In the **SSO Attribute Mapping** area (Figure 87), click the **Add new attribute** button. A new row is displayed.

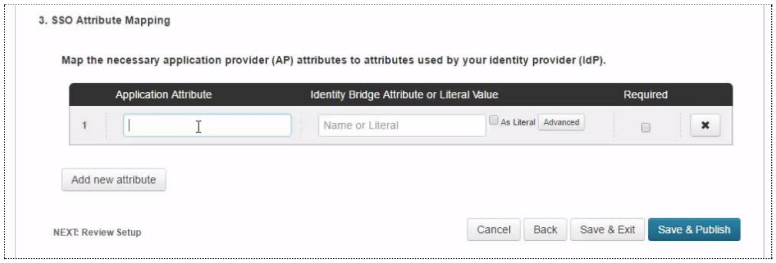


Figure 88: New row for adding authentication attribute

2. Click the **Advanced** button in this row.

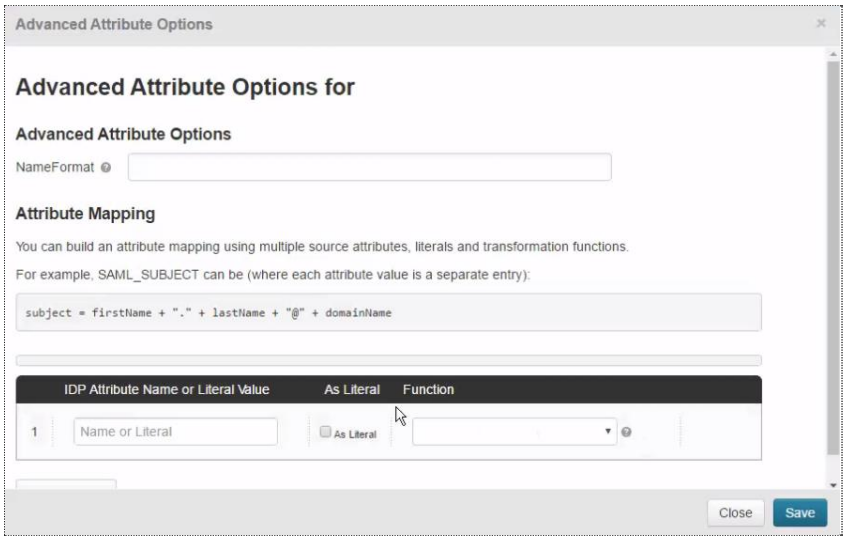


Figure 89: Advanced Attribute Options dialog box

3. In the **NameFormat** list, select the first option, as shown below:

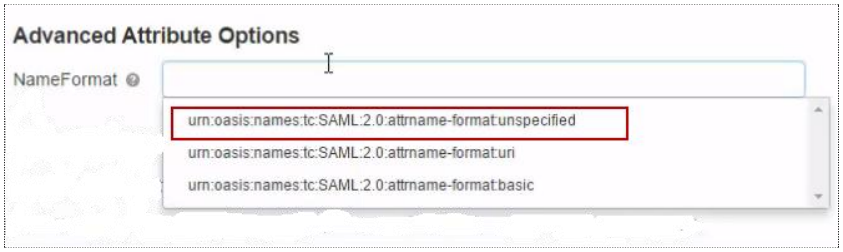


Figure 90: Name Format options

4. In the **IDP Attribute Name or Literal Value** box, type or select the Active Directory attribute you want to use for authentication. For example, E-mail. This attribute facilitates user identification.

   To define users in PingOne, see Configure users in PingOne.

5. In the **Function** list, you can select the conversion methodology. For example, you can convert the first name or last name to upper case, lower case, or even use regular expressions. We will not use any conversion methodology here.

6. Click **Save**.

7. The specified attribute is displayed in the **Identity Bridge Attribute or Literal Value** box (Figure 88). Provide a user-friendly name for the attribute in the **Application Attribute** box.

8. There is one change we have to make. For attribute mapping, the email listed should be accurate, since we selected E-*mail* as the unique identifier.

   Click the **Advanced** button in the row (Figure 88); the **Advanced Attribute Options** dialog box (Figure 89) is displayed.

9. On clicking *E-mail* in the **IDP Attribute Name or Literal Value** box, a drop-down is displayed. Select the **Email** option.

Figure 91: Email option

10. With this selected, users will be authenticated with their email address. Click **Save**.

11. Click the **Save & Publish** button (Figure 88).

12. The configurations we made in PingOne will be displayed. Click **Finish**.

    The new GroupID application you created in PingOne is displayed in the **My Applications** grid.

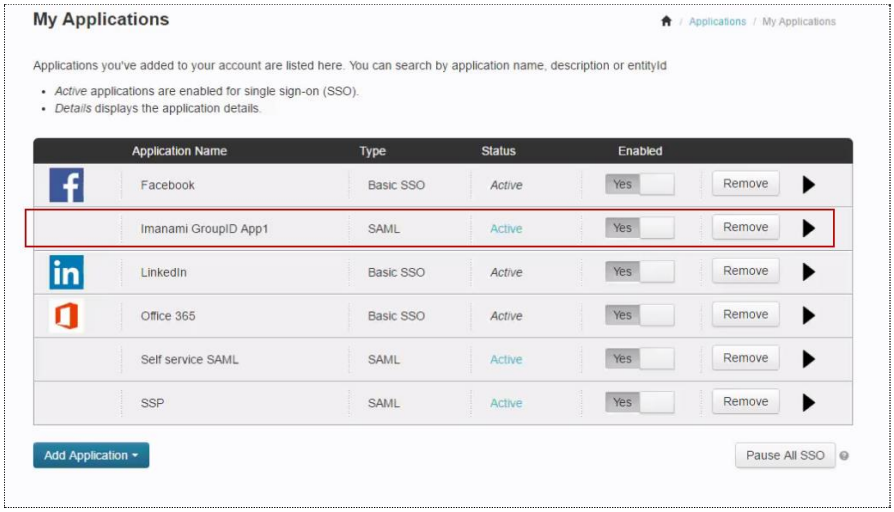


Figure 92: My Applications grid displaying the GroupID app

Configure the PingOne provider in GroupID

While creating the PingOne provider in GroupID SSO Admin Panel, you simply have to import the PingOne metadata file to configure all settings for this identity provider.

1. In GroupID SSO Admin Panel (Figure 3), click the **New Provider** button to add the PingOne provider.

   The **Add New SAML Provider** page (Figure 7) is displayed.

2. In the **Client** list, select the GroupID application with which you want to set up the SAML provider.

   This list contains all GroupID applications, namely

   - Automate
   - Management Shell
   - All Self-Service and Password Center portals created using GroupID

   The application you select must be the one for which you generated the consumer URL and the GroupID metadata file (see Generate GroupID metadata file on page 56).

To continue with the example, select the Self-Service portal named *Enterprise* in the **Client** list.

3. Click the **Import from Metadata** button under the **Advanced** section to import the PingOne metadata file.

   You downloaded this metadata file in step 13 under the heading, Configure GroupID in PingOne.

Figure 93: Import Settings from IDP provided Metadata File dialog box

4. Click **Choose File** to select the PingOne metadata file. Then click **Load File**. With this, fields on the **Add New SAML Provider** page (Figure 7) are automatically filled in.

10. When PingOne is configured with the GroupID application, *Enterprise*, it will be available on *Enterprise's* login page for single sign-on. You can choose to display the PingOne authentication option as an image or a button.

    - To display the PingOne option as an image, you have to upload an image for the identity provider.

      On the **Add New SAML Provider** page (Figure 7), use the **Browse** button next to the **Identity Provider Image** box to upload an image for PingOne.

      Supported image formats are: .jpg, .bmp, .png, and .gif. Required dimensions for the image file are: 210 x 60 pixels.

    OR

    - If you do not want an image, PingOne authentication will be shown as a button.

      Specify a name for the button in the **Name** box.

    Users can click the image or the button on the login page of the Self-Service portal, *Enterprise* (Figure 97) and authenticate using the PingOne single sign-on process.

5. To make advanced configurations, click **Advanced** to expand the **Advanced** section.

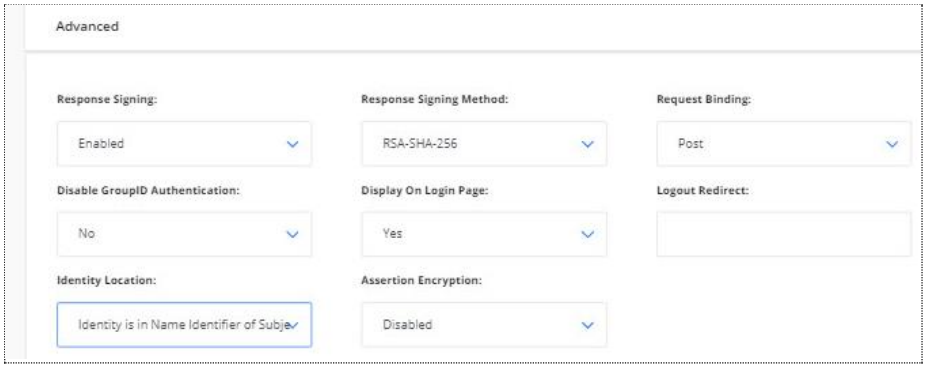


Figure 94: Advanced section for PingOne

6. The **Response Signing Method** box displays *RSA-SHA-256* as the signing method type. We configured this method as the signing algorithm in PingOne (Figure 86).
7. The **Disable GroupID Authentication** option indicates whether to display the GroupID authentication login on the *Enterprise* portal's login page (Figure 97).
   - By default, 'No' is selected, which means that when users access the *Enterprise* portal's login page, they will be shown the GroupID login and password option as well as the PingOne identity provider's button.
   - Selecting 'Yes' means that the GroupID login and password option will not be available on the *Enterprise* portal's login page.

     Moreover, when a single identity store and a single SAML provider is configured, the login page for the provider is displayed rather than the *Enterprise* portal's login page.
8. In the **Request Binding** list, select *POST*, since the **Single Logout Binding Type** is set to *Post* in PingOne (Figure 86).
9. Click the **Create Provider** button.

The PingOne identity provider is created and displayed in the **SAML Identity Providers** grid in the GroupID SSO Admin Panel (Figure 3).

Configure users in PingOne

You must define users in PingOne. These users are authenticated in GroupID on the basis of an attribute, as discussed in Attribute mapping in PingOne.

Only the users you define here can authenticate on the GroupID Self-Service portal, *Enterprise* using PingOne. (See Sign-in using PingOne on page 68.)

1. In PingOne, click the **Users** tab. The **Users** page is displayed as follows:

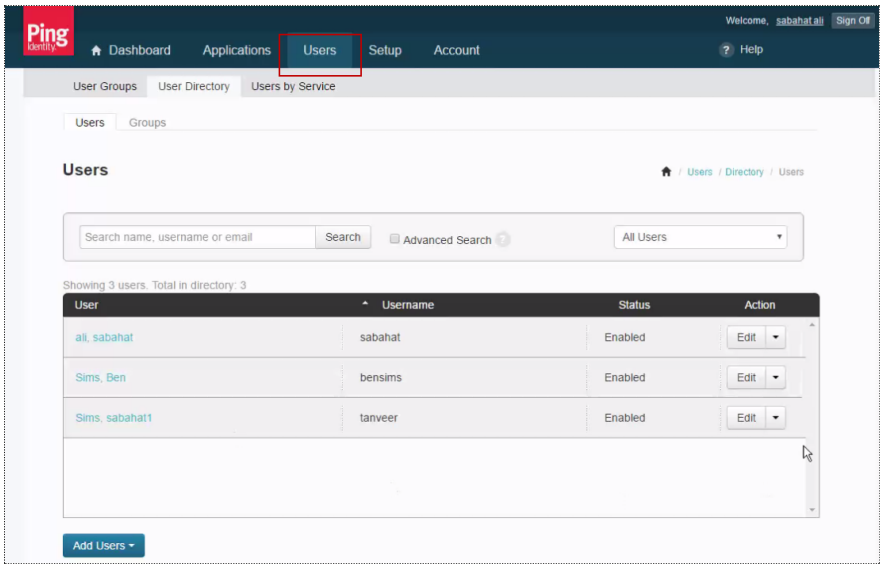


Figure 95: Users page

2. Click the **Add Users** button and select the **Create New User** option to create a user.

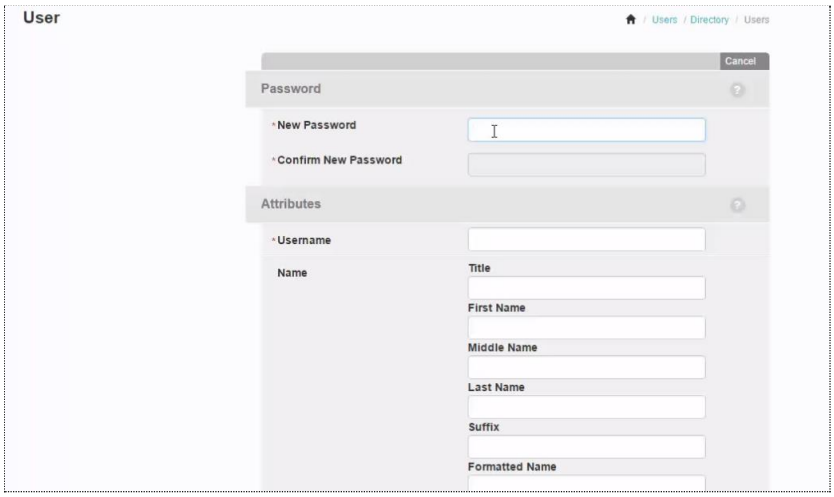


Figure 96: Create New User page

3. Specify a password in the **New Password** and **Confirm New Password** boxes.
4. Specify a user name in the **Username** box.

   The user will use this user name and password for single sign-on into GroupID using PingOne.
5. Enter other details of the user, such as first name, last name, and the email address.
6. Click **Save**. The user is created.

Sign-in using PingOne

We configured the PingOne provider with the GroupID Self-Service portal, *Enterprise*. We also created a user in PingOne who should be able to log into the *Enterprise* portal using the PingOne single sign-on option.

For single sign-on using PingOne, we can choose any of the following ways:

- SP-initiated single sign-on: when the SSO operation is initiated from the SP end, i.e., from the Self-Service portal, *Enterprise*.
- IdP-initiated single sign-on: when the SSO operation is initiated from the IdP end, i.e., from PingOne.

SP-initiated single sign-on

1. Launch the Self-Service portal, *Enterprise*.

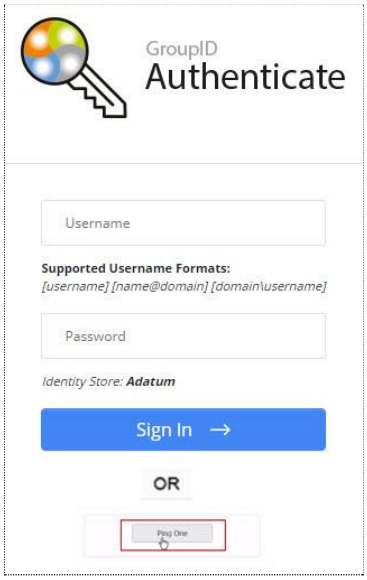


Figure 97: Login page with PingOne button

The availability of the user name and password fields depends on your selection in the **Disable GroupID Authentication** list (see Figure 94).

2. Click the PingOne button; the PingOne Sign In page is displayed.
3. Enter your credentials and log in. You will be routed to the main page of the Self-Service portal, *Enterprise*.

   Only users defined for our app in PingOne can log in using PingOne single sign-on. See Configure users in PingOne on page 67.

With single sign-on, the user can now launch any GroupID application without having to sign in again.

Even if the user closes the portal and re-launches it, he or she will directly log into the portal, without having to enter any credentials. The same behavior applies in case of an IIS reset.

IdP-initiated single sign-on

1. Launch the PingOne portal using the URL provided by your organization and log in.

   The PingOne dashboard will be displayed. It lists the apps configured with PingOne for single sign-on.
2. On clicking an app, you will be redirected to it. Authentication will not be required.

Chapter 5 - SAML Configuration for GroupID using OneLogin

OneLogin provides single sign-on and identity management for organizations that embrace cloud computing.

In this chapter, we will discuss the configuration of single sign on in GroupID using OneLogin as a provider.

Generate Consumer URL

The consumer URL is unique for each GroupID module (referred to as 'application' here). In GroupID Single Sign-On Admin Panel, generate the consumer URL for the GroupID application with which you want to configure OneLogin. Provide this URL while configuring the GroupID application in OneLogin.

1. Launch the GroupID Single Sign on Admin Panel (Figure 3) and click **Generate URL**. The **Generate URLs** page (Figure 6) is displayed.
2. In the **Select Client to Generate Consumer URL** list, select a GroupID application with which you want to set up OneLogin for single sign-on.

   This list contains all GroupID applications, namely

   - Automate
   - Management Shell
   - All Self-Service and Password Center portals created using GroupID

   As an example, let's select the Self-Service portal named *Users*.
3. The URL displayed in the **Consumer URL** box is a unique identifier for the selected application. It is used while configuring the portal, *Users* in OneLogin. Click to copy this URL. Then paste it in a file, preferably a text file, to save it.

1. On upgrade to GroupID 10 SR2, you must generate the consumer URL again for the GroupID client configured with OneLogin, and update it in OneLogin.
2. If you lose the SQL server or the GroupID server, you will have to configure the provider again.

Generate Entity ID/Audience URL

The audience URL is unique for each GroupID module (referred to as 'application' here). In GroupID Single Sign-On Admin Panel, generate the audience URL for the GroupID application with which you want to configure OneLogin. Provide this URL while configuring GroupID in OneLogin.

1. In GroupID Single Sign-On Admin Panel (Figure 3), click the **New Provider** button to add a new provider. The **Add New SAML Provider** page (Figure 7) is displayed.
2. In the **Client** list, select a GroupID application to set up the SAML provider with.

   This list contains all GroupID applications, namely

   - Automate
   - Management Shell
   - All Self-Service and Password Center portals created using GroupID

   The application you select must be the one for which you generated the consumer URL on the **Generate URLs** page (Figure 6).

   To continue with the example, select the Self-Service portal named *Users* in the **Client** list.
3. The **Entity ID/Audience** box displays a URL that serves as the application ID. Click  to copy it.

Configure GroupID in OneLogin

Configuring GroupID in OneLogin involve the following steps:

- Create an app for the GroupID Self-Service *Users* portal in OneLogin.
- Configure this app by specifying the consumer URL and audience URL.
- Specify an attribute for authenticating users who use the OneLogin single sign-on option to log into the *Users* portal.
- Define SSO settings.

You also have to:

- Define users in OneLogin, who can authenticate on the GroupID app, *Users* using OneLogin.
- Download the OneLogin metadata file, that will be used to configure the OneLogin provider in GroupID.

Create app for GroupID in OneLogin

1. Launch OneLogin.

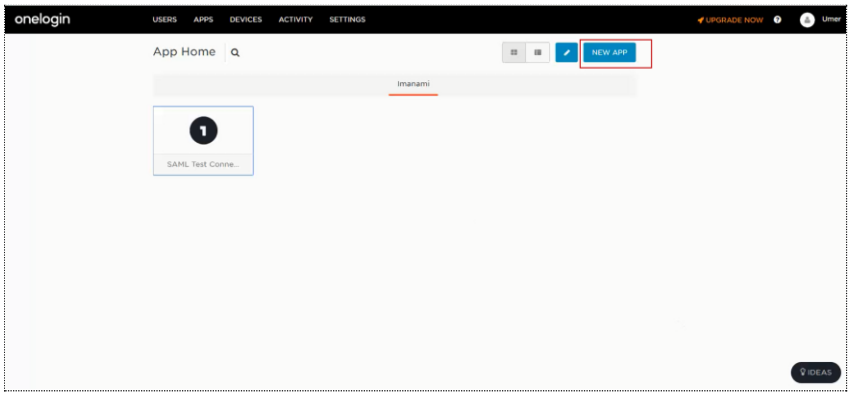


Figure 98: OneLogin – Home page

2. On the Home page, click the **New App** button to add a new application in the OneLogin control panel.

   To continue with our example, we will be adding the GroupID application, *Users*.

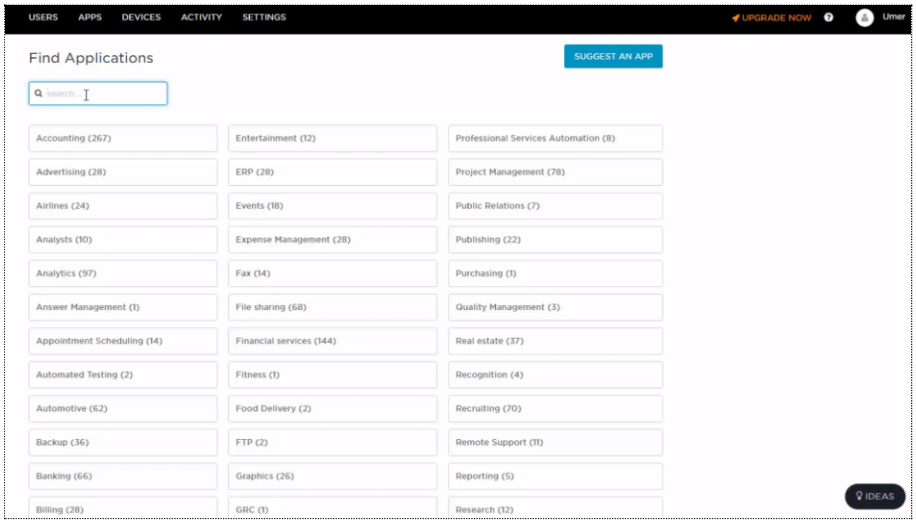


Figure 99: Find Applications page

3. A list of applications is available here. In the **Find Applications** box, type 'SAML' to search for single sign-on applications.

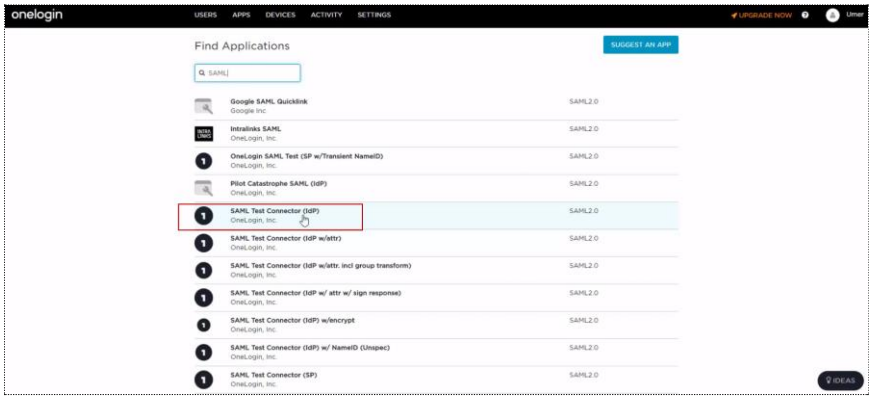


Figure 100: List of SAML applications

4. Select the **SAML Test Connector (IdP)** option (without any attributes or any sign responses).

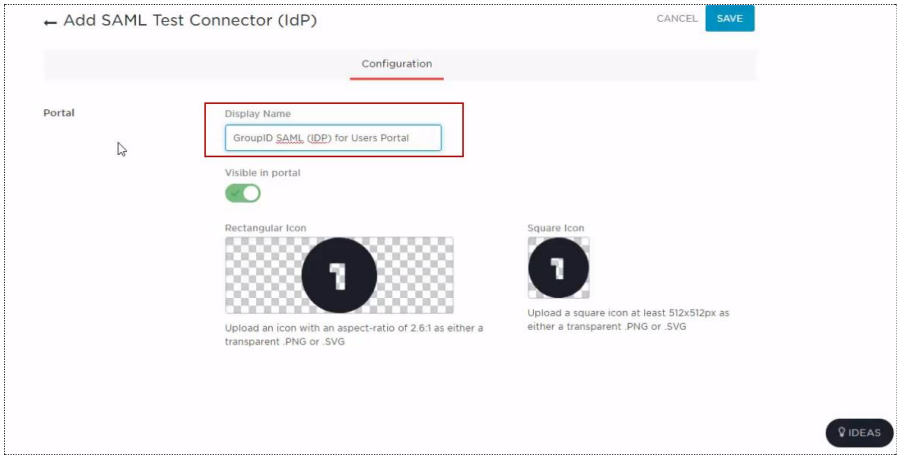


Figure 101: Create New App page

5. Specify a friendly name for the application in the **Display Name** box.
6. You can also upload an image for the GroupID app that will be displayed on the user dashboard in OneLogin (Figure 122).

   Every SAML provider has a user dashboard. Hence, when a user logs in to OneLogin, he or she will be redirected to the dashboard that may have GroupID and other applications listed for single sign-on.
7. Click **Save**.

   A message is displayed that the app is added and a few links are displayed under the message. It is as follows:

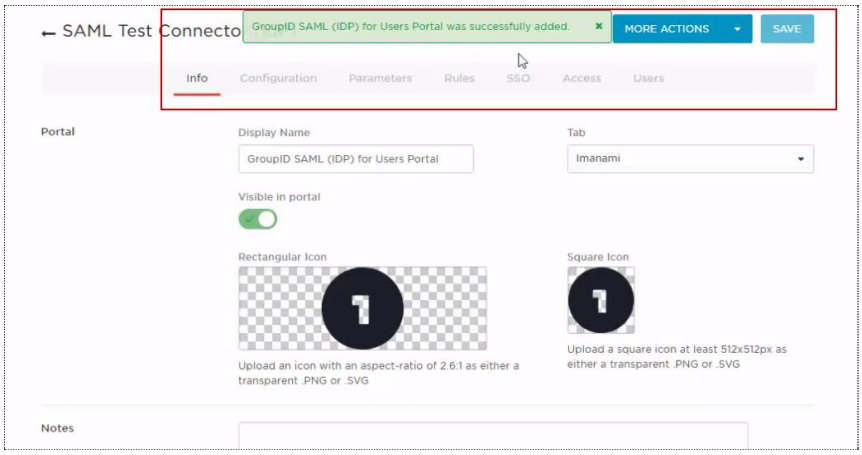


Figure 102: Create New App page (2)

Set Consumer URL and Audience URL

8. Click the **Configurations** link (Figure 102). The **Configurations** page for the new app is displayed as follows:

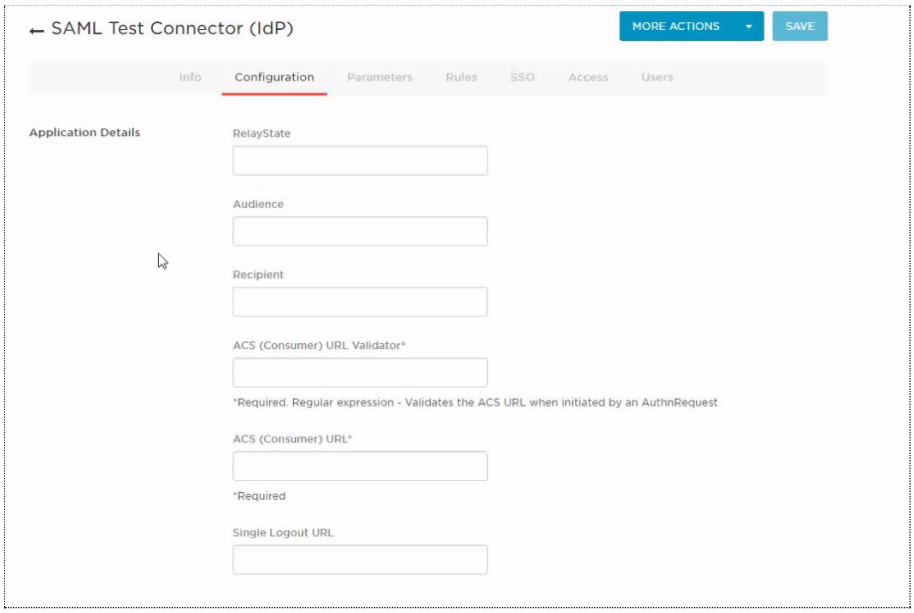


Figure 103: New App Configurations page

9. In the **ACS (Consumer) URL Validator** and **ACS (Consumer) URL** boxes, provide the consumer URL that you generated for the GroupID application, *Users* (see Generate Consumer URL on page 70).

10. Provide the audience URL in the **Audience** box. Fetch this URL from the **Entity ID Audience** field on the **Add New SAML Provider** page (see Generate Entity ID/Audience URL on page 71).

Specify attribute for user authentication

11. Click the **Parameters** link.

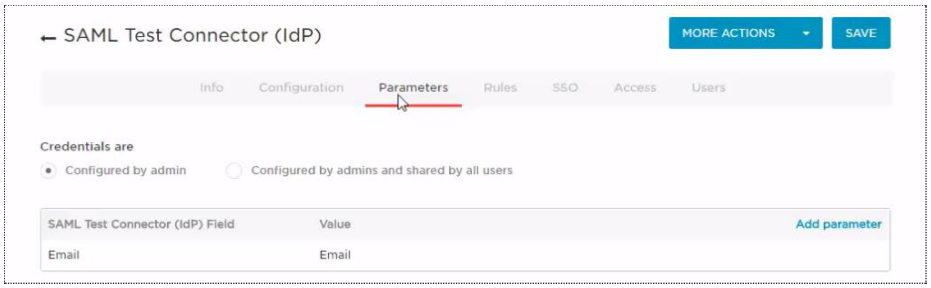


Figure 104: Parameters page

12. *Email* is already set as the entity ID that will be used for authenticating users who opt to sign into GroupID using the OneLogin single sign-on option. Leave all settings to default.

    Hence, the *Email* attribute is meant for user identification.

Configure SSO settings

13. Click the **SSO** link.

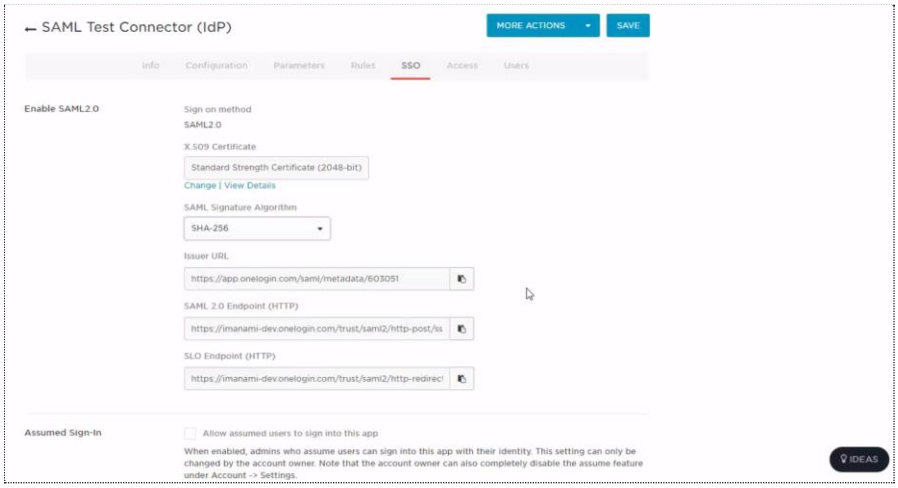


Figure 105: SSO page

14. In the **SAML Signature Algorithm** list, select *SHA-256*.

15. The page also displays the Issuer URL and the endpoint URLs for both the post and redirect methods. You will have to provide these URLs while configuring the OneLogin provider in GroupID SSO Admin Panel.
    (See Configure the OneLogin provider in GroupID on page 77.)

Define users

16. Click the **Access** link. The **Policy** list displays any policies that you may have configured for users. You can select a policy to enforce it.
17. Click the **Users** link.

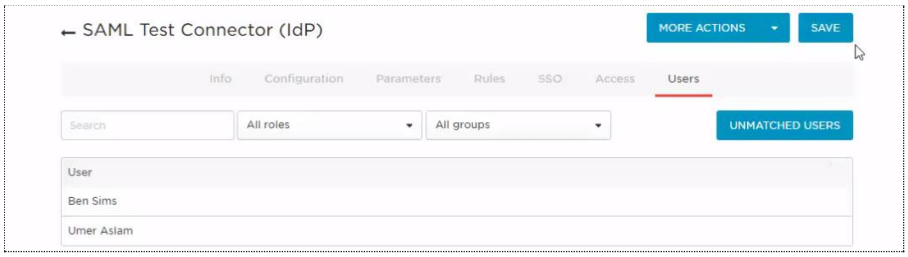


Figure 106: Users page

User management is discussed in detail in Define users in OneLogin on page 80.

18. Click **Save**.

Download OneLogin metadata file

You can download a metadata file from OneLogin and import it into GroupID to configure the OneLogin provider in GroupID.

19. Click **More Actions** and select **SAML Metadata**. This will download the OneLogin metadata file on your machine.

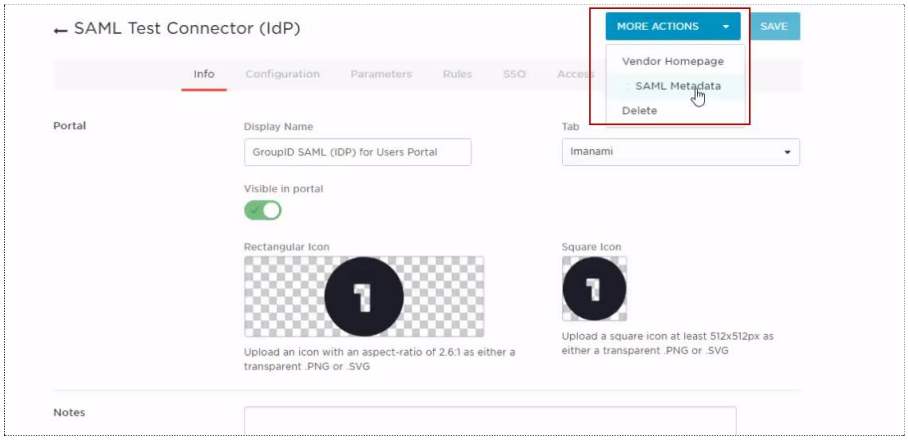


Figure 107: Download metadata file

20. For convenience, copy this file from the downloaded location to your desktop. Now you have to import this file into GroupID.

    Importing the metadata file will being in all the configurations for the OneLogin identity provider within the SAML provider setup in GroupID.

Configure the OneLogin provider in GroupID

While creating the OneLogin provider in GroupID SSO Admin Panel, you simply have to import the OneLogin metadata file to configure all settings for it.

1. In GroupID SSO Admin Panel, go to the **Add New SAML Provider** page (Figure 7) and make sure *Users* is selected in the **Client** list.

   (*Users* is the GroupID application for which we generated the audience URL, to set up OneLogin with it.)

Import OneLogin metadata file

2. Click the **Import from Metadata** button under the **Advanced** section to import the OneLogin metadata file.

   (You downloaded this metadata file in the Download OneLogin metadata file section on page 76.)

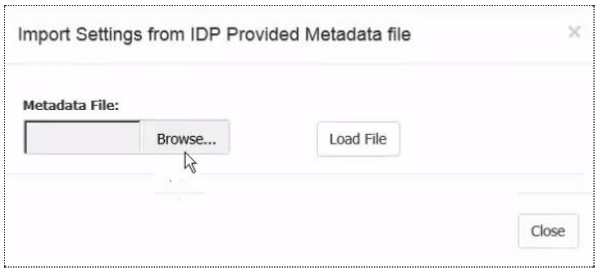


Figure 108: Import Settings from IDP provided Metadata File dialog box

3. Click **Browse** to select the OneLogin metadata file. Then click **Load File**. With this, the required fields on the **Add New SAML Provider** page (Figure 7) are automatically filled in.

   However, you still have to provide the Issuer URL and IDP Login URL.

Provide Issuer URL and IDP Login URL

4. On the **SSO** page (Figure 105), copy the URL displayed in the **Issuer URL** box and paste it in the **Issuer** box on the **Add new SAML provider** page (Figure 25).
5. For request binding, we will prefer the *post* method rather than the *redirect* method.

   Select the endpoint URL for the post method in the **SAML 2.0 Endpoint (HTTP)** box on the **SSO** page (Figure 105) and paste it in the **IDP Login URL** box on the **Add new SAML provider** page (Figure 25).

Upload image for identity provider

6. When OneLogin is configured with the GroupID application, *Users*, it will be available on *Users's* login page for single sign-on. You can choose to display the OneLogin authentication option as an image or a button.

   - To display the OneLogin option as an image, you have to upload an image for the identity provider.

     On the **Add New SAML Provider** page (Figure 7), use the **Browse** button next to the **Identity Provider Image** box to upload an image for OneLogin.

     Supported image formats are: .jpg, .bmp, .png, and .gif. Required dimensions for the image file are: 210 x 60 pixels.

   OR

   - If you do not want an image, OneLogin authentication will be shown as a button.

     Specify a name for the button in the **Name** box.

   Users can click the image or the button on the login page of the Self-Service portal, *Users* (Figure 120) and authenticate using the OneLogin single sign-on process.

Advanced settings

7. To make advanced configurations, click **Advanced** to expand the **Advanced** section.

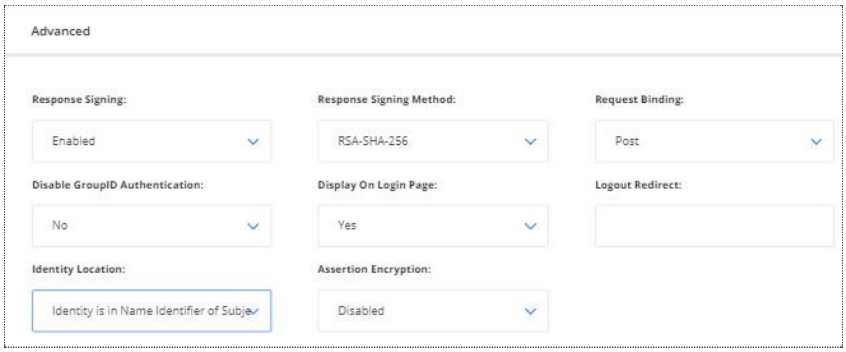


Figure 109: Advanced section for OneLogin

8. The **Disable GroupID Authentication** option indicates whether to display the GroupID authentication login on the *Users* portal's login page (Figure 120).
   - By default, 'No' is selected, which means that when users access the *Users* portal's login page, they will be shown the GroupID login and password option as well as the OneLogin identity provider's button.
   - Selecting 'Yes' means that the GroupID login and password option will not be available on the *Users* portal's login page.

     Moreover, when a single identity store and a single SAML provider is configured, the login page for the provider is displayed rather than the *Users* portal's login page. (The OneLogin login page is as shown in Figure 121.)
9. In the **Request Binding** list, select *POST*, since we used the endpoint URL for the *post* method in the **IDP Login URL** box.
10. We will not use the assertion encryption, so make sure *Disabled* is selected in the **Assertion Encryption** list.
11. In the **Response Signing Method** list, select *RSA-SHA-256*, since we configured this method as the signing algorithm in the **SAML Signature Algorithm** list on the **SSO** page (Figure 105).

Create the provider

12. Click the **Create Provider** button.

The OneLogin identity provider is created and displayed in the **SAML Identity Providers** grid in the GroupID SSO Admin Panel (Figure 3).

Define users in OneLogin

You must define users in OneLogin. Only these users can authenticate on the GroupID Self-Service portal, *Users* using OneLogin. (See Sign-in using OneLogin on page 84.)

On the **Users** page (Figure 106) in the OneLogin admin panel, let's add a new user.

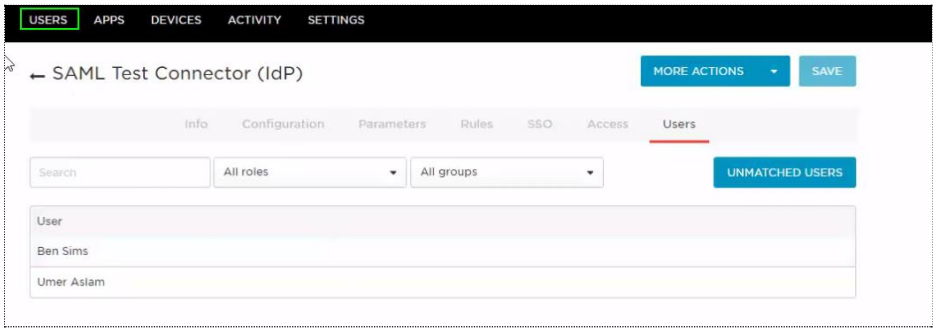


Figure 110: Users page

1. Click **Users** in the black bar at the top; the following page is displayed:

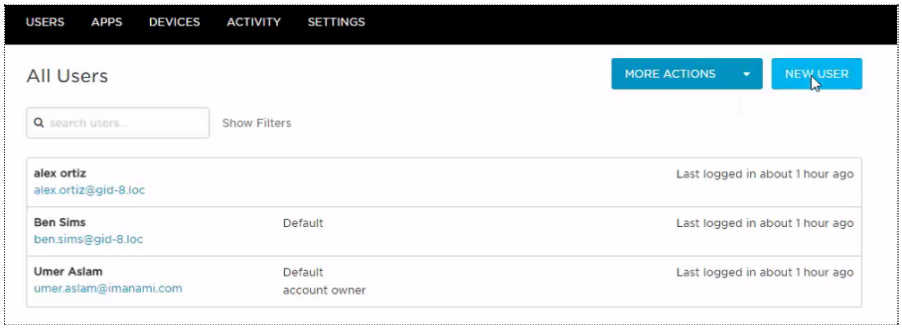


Figure 111: All Users page

2. Click the **New User** button.

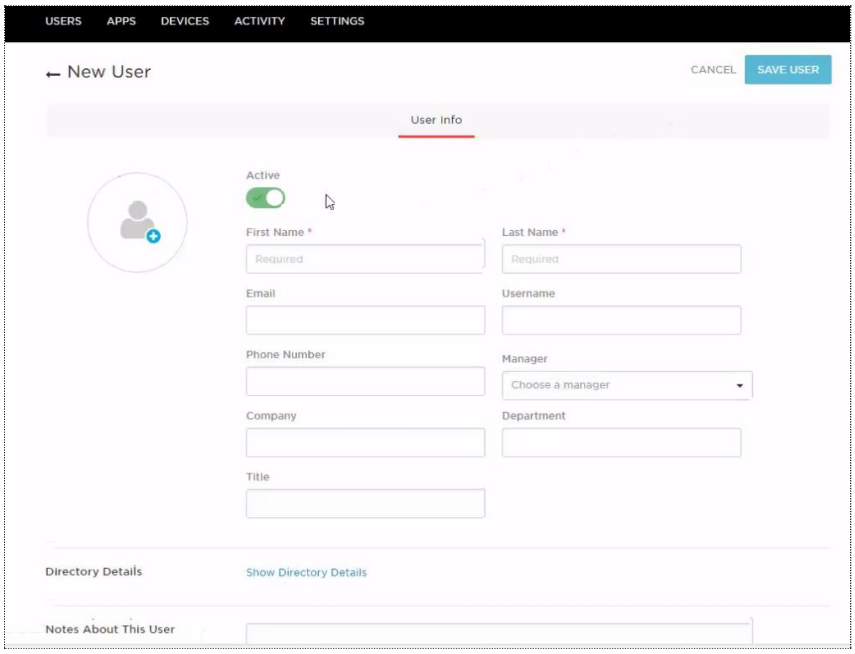


Figure 112: New User page

3. Create a new user, for example, Leo Ferguson. Enter the t=required information for this user and click **Save User** to create the user.

   Notice that we specified a user name but no password for the user. We will specify it later (Figure 118).

   A message is displayed that the user is created and a few links are displayed under the message.

4. Click the **Authentication** link.

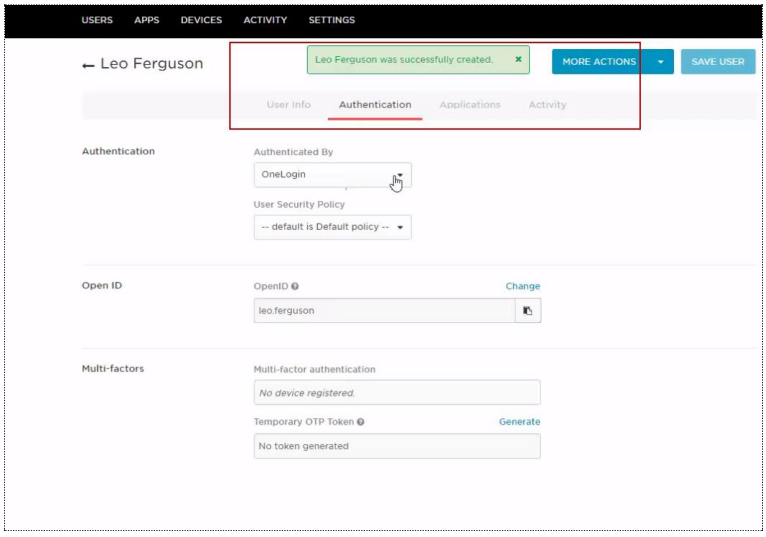


Figure 113: Authentication page

5. In the **Authenticated By** list, make sure OneLogin is selected.
6. In the **User Security Policy** list, select 'Default policy'.
7. Click the **Applications** link.

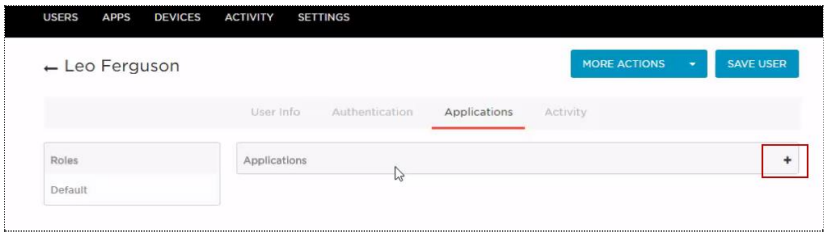


Figure 114: Applications page

8. Click + to specify the application that the user (i.e., Leo Ferguson in our example) will be able to log on to.

   The following dialog box is displayed:

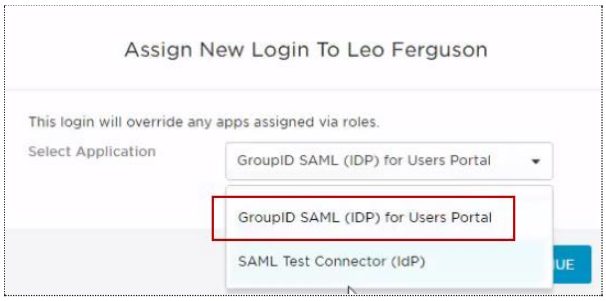


Figure 115: Assign New Login dialog box

9. In the **Select Application** list, select the application that you created for GroupID in OneLogin (Figure 101).
10. Click **Continue**. The following dialog box is displayed:

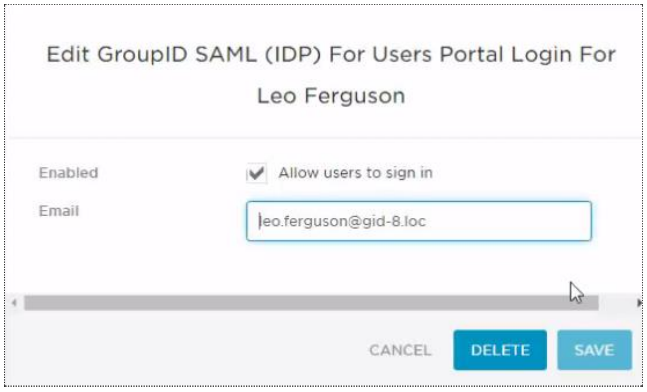


Figure 116: Edit app for User dialog box

The user's email is fetched from the **New User** page (Figure 112).

11. Click **Save**. The app is listed as:

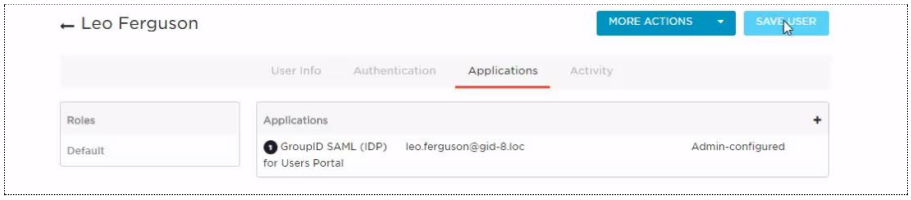


Figure 117: Applications page (2)

12. Click **Save User**.
13. Next, you have to update the user's password in OneLogin.

    On the **New User** page (Figure 112), click **More Actions** and select **Change Password**.

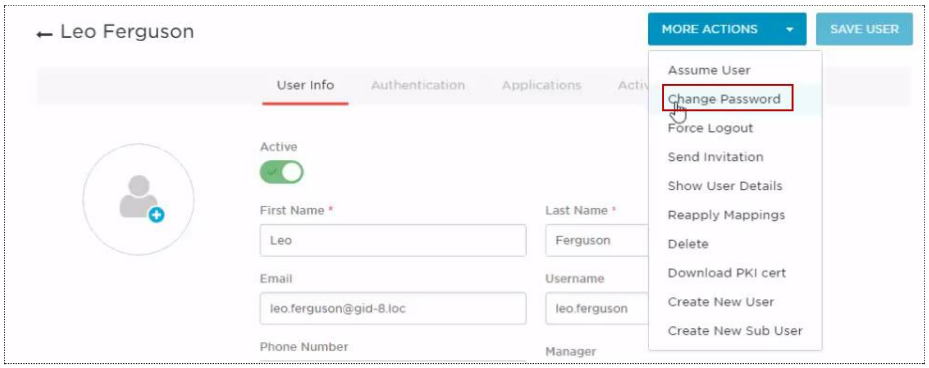


Figure 118: Change Password option

14. The following dialog box is displayed:

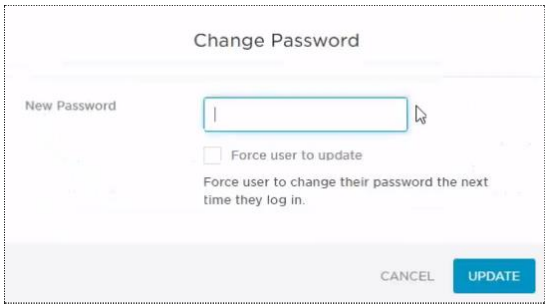


Figure 119: Change Password dialog box

15. Specify a new password for the user and click **Update**.
16. Click **Save User**.

Sign-in using OneLogin

We configured the OneLogin provider with the GroupID Self-Service portal, *Users*. We also created a user, Leo Ferguson, in OneLogin who should be able to log into the *Users* portal using the OneLogin single sign-on option.

For single sign-on using OneLogin, we can choose any of the following ways:

- SP-initiated single sign-on: when the SSO operation is initiated from the SP end, i.e., from the Self-Service portal, *Users*.
- IdP-initiated single sign-on: when the SSO operation is initiated from the IdP end, i.e., from OneLogin.

SP-initiated single sign-on

1. Launch the Self-Service portal, *Users*.

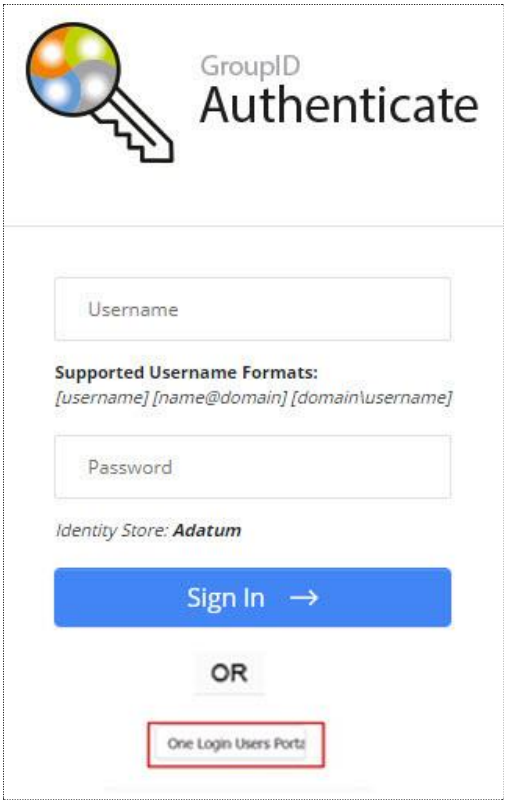


Figure 120: Login page with OneLogin button

The availability of the user name and password fields depends on your selection in the **Disable GroupID Authentication** list (see Figure 109).

2. Click the **One Login Users Portal** button; the user is redirected to the OneLogin sign in page.

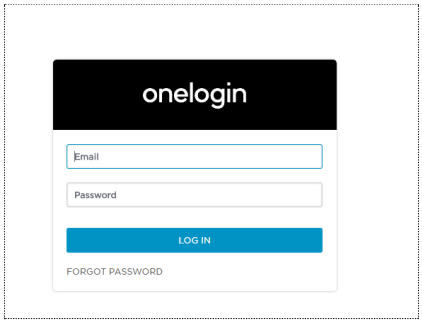


Figure 121: OneLogin sign in page

3. Enter Leo Ferguson's login name and password, and click **Login**.

   The user is successfully logged into the Self-Service portal using the OneLogin single sign on option.

   Only users defined for our app in OneLogin can log in by entering their user names and passwords. See Define users in OneLogin on page 80.

With single sign-on, you can now launch any GroupID application without having to sign in again.

IdP-initiated single sign-on

1. Launch the OneLogin portal using the URL provided by your organization and log in.
   The OneLogin dashboard will be displayed.

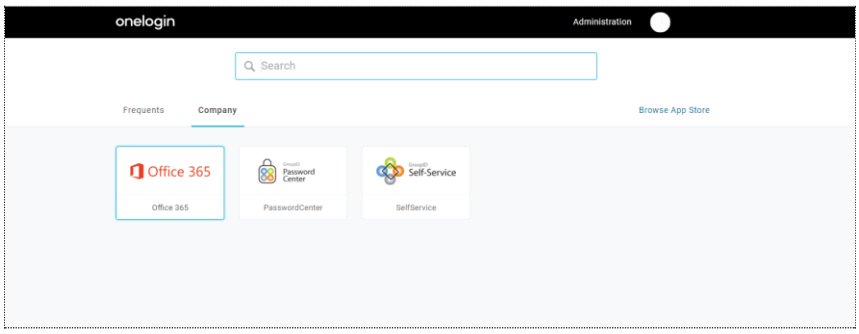


Figure 122: OneLogin Dashboard

   This page displays the apps configured with OneLogin for single sign-on.

2. On clicking an app, you will be redirected to it. Authentication will not be required.

Part 2 - GroupID as an Identity Provider

Chapter 1 - Configure GroupID as an Identity Provider

GroupID can provide the services of an identity provider. You can register a third-party application as a service provider in GroupID to authenticate users in that application through GroupID.

Register an application (service provider) in GroupID

1. Launch GroupID Authenticate.
2. In GroupID SSO Admin Panel, click the **Applications** tab.
3. Click **New Application**.

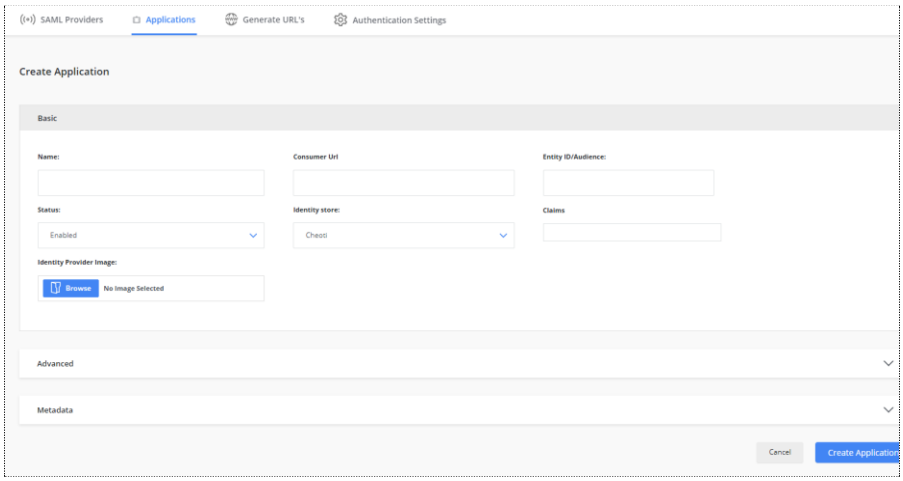


Figure 123: Create Application page

4. Enter a name for the application in the **Name** box.
   The application will be displayed on the GroupID **Login** page with this name.
5. Copy the consumer URL from the service provider and enter it In the **Consumer URL** box.
6. Copy the audience URL from the service provider and enter it In the **Entity ID/Audience** box.

7. From the **Identity store** drop-down list, select the identity store to use for authenticating users.

   For single sign-on, third-party application users must authenticate through an identity store defined in GroupID. For example, to authenticate users through Active Directory, select an AD-based identity store.

8. Next, specify an attribute as a claim. Service provider application users are authenticated in GroupID based on this attribute.

   Enter the attribute name in the **Claim** box. As you type, the system displays the attributes in the selected identity store that start with the text. Select the required attribute.

   The value of this attribute in the application would be matched to the value of this same attribute in the identity store for authentication.

9. Click **Browse** under **Identity Provider Image** to upload an image for the application, such as the application logo.

   Supported image formats: .jpg, .bmp, .png, and .gif
   Image file dimensions: 210 x 60 pixels

Specify Advanced settings for the application

10. Expand the **Advanced** section by clicking the down arrow.

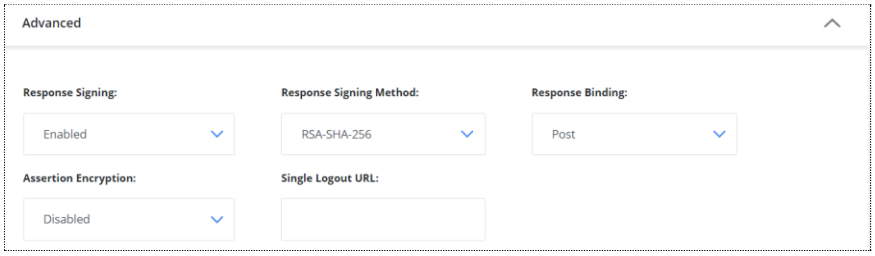


Figure 124: Create Application page – Advanced section

11. Select *Enabled* or *Disabled* in the **Response Signing** box, depending on whether it is enabled or disabled in the service provider.

12. Select a response signing method from the **Response Signing Method** drop-down list. This method should be the same for the identity provider (GroupID) and the service provider (third-party application).

13. Select *Post* or *Redirect* in the **Response Binding** list, depending on how the service provider accepts the response.

14. If you are not using assertion encryption, make sure *Disabled* is selected in the **Assertion Encryption** list.

    To use assertion encryption as an advanced security feature, select *Enabled*. Then provide the certificate, key transport algorithm, and encryption algorithm to encrypt the response.

15. Generate a logout URL in the service provider and enter it in the **Single Logout URL** box. When a user clicks this URL, he or she will be logged out of all applications that have been authenticated through GroupID (i.e., applications that he or she is single signed in through GroupID).

16. Provide the GroupID metadata in the service provider to register GroupID as an identity provider in it.

    See GroupID metadata for service provider configurations.

17. Click **Create Application** to create the service provider in GroupID.

GroupID metadata for service provider configurations

As part of registering an application in GroupID, you also have to provide GroupID metadata at the service provider end.

18. On the **Create Application** page (Figure 123), expand the **Metadata** section by clicking the down arrow.

Figure 125: Create Application page – Metadata section

19. Copy the Issuer URL and GroupID certificate from the **Provider Issuer** and **Provider Signing Certificate** boxes and paste them in the service provider.

20. Both the **Provider IDP POST Endpoint** and **Provider IDP Redirect Endpoint** are given here. Depending on how the service provider sends the request or the mechanism used, copy the appropriate URL and paste it in the service provider.

21. The **Single Logout Endpoint POST** box displays a URL.
    Requests are posted on this URL for logging out from the current and all other third-party applications configured in GroupID.

22. The **Login URL** box displays a URL for logging in.
    On clicking this URL, the user is redirected to the GroupID Login page where GroupID is acting as an identity provider. If the user is already logged into GroupID, he/she will be auto-authenticated; otherwise the user will have to provide the credentials.

Specify default metadata values

You can specify default values for the following metadata:

- Issuer URL
- Signing Certificate

To specify default values:

1. Launch GroupID Authenticate.
2. In GroupID SSO Admin Panel, click the **Authentication Settings** tab.

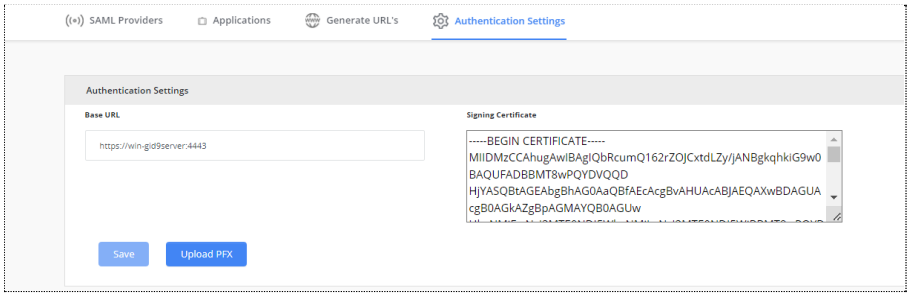


Figure 126: Authentication Settings page

Update the Issuer URL:

The **Base URL** box displays the Issuer URL. This URL is reflected in the **Provider Issuer** box on the **Create Application** page (Figure 125).

You may want to change the base/Issuer URL for any reason, for example, replace it with a sub-domain URL or a load balancer URL.

Replace or update the URL in the **Base URL** box and click **Save**.

The new URL would be reflected on the **Create Application** page (Figure 125) too.

Update the signing certificate:

The **Signing Certificate** box displays the GroupID certificate created in IIS. It displays the certificate along with the private key. This certificate is reflected in the **Provider Signing Certificate** box on the **Create Application** page (Figure 125), though without the private key.

You may choose to use this certificate or create a custom certificate and use that in third-party applications.

1. Create your custom certificate and export it to a PFX file.
2. On the **Authentication Settings** page (Figure 126), click **Upload PFX**.

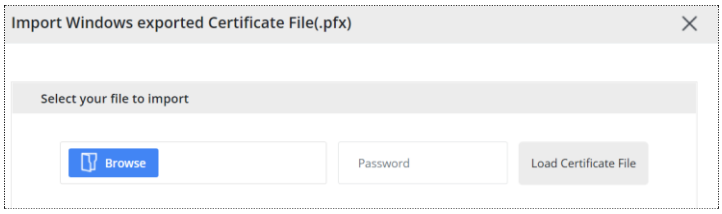


Figure 127: Import Certificate File dialog box

3. Click **Browse** to select the exported certificate file. As it is password protected, enter the password and click **Load Certificate File**.
4. Click **Save**.
   The new certificate is displayed in the **Signing Certificate** box and reflected on the **Create Application** page (Figure 125) too.

Sign-in using GroupID

Let's assume that we configured three service providers in GroupID. Users should be able to access these applications through GroupID.

For single sign-on using GroupID, users can choose any of the following ways:

- SP-initiated single sign-on: when the SSO operation is initiated from the SP end, i.e., from any of the registered service providers.
- IdP-initiated single sign-on: when the SSO operation is initiated from the IdP end, i.e., from GroupID.

IdP-initiated single sign-on

1. Click the Login URL displayed in the GroupID metadata section.
2. On clicking it, the user is redirected to the GroupID login page where GroupID is acting as an identity provider. If the user is already logged into GroupID, he/she will be auto-authenticated; otherwise the user will have to provide the credentials.

Appendix A

Authenticated users in Windows AzMan

The GroupID administrative permissions are controlled through the Windows Authorization Manager (AzMan) console.

Only if your account has the 'GroupID Administrators' role in AzMan, you will be able to log into the GroupID Single Sign-on Admin Panel and manage SAML providers.

To view the users configured in AzMan:

1. In the **Run** dialog box, type azman.msc to launch the Authorization Manager console.

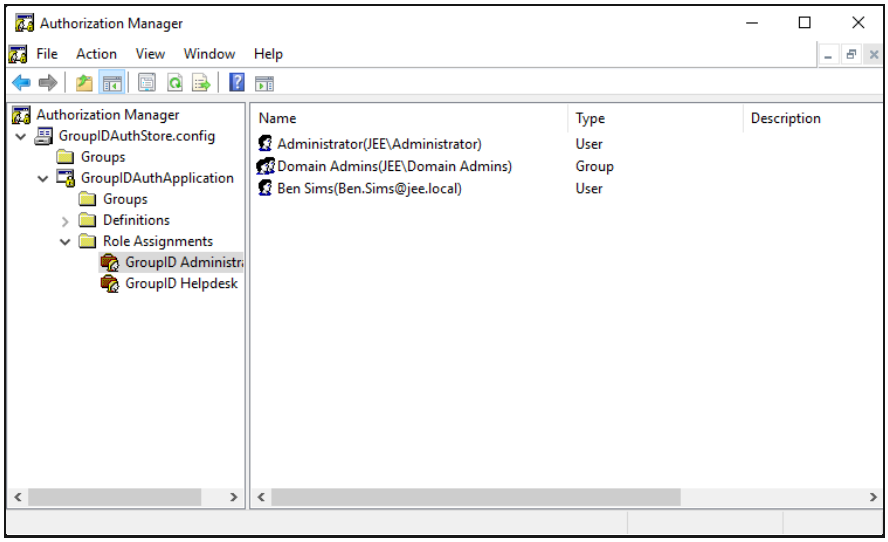


Figure 128: AzMan Console

2. Click **Authorization Manager > Role Assignments > GroupID Administrators**. Only users configured under the 'GroupID Administrators' role in AzMan (such as Ben Sims) can log into the GroupID SSO Admin Panel and configure a single sign-on entity.

Imanami | Now part of Netwrix

6160 Warren Parkway, Suite 100,
Frisco, TX 75034,
United States.
https://www.imanami.com/

Support: (925) 371-3000, Opt. 3
support@imanami.com

Sales: (925) 371-3000, Opt. 1
sales@imanami.com

Toll-Free: (800) 684-8515
Phone: (925) 371-3000
Fax: (925) 371-3001